

# Novell eDirectory™

8.8

[www.novell.com](http://www.novell.com)

管理ガイド

2005年9月15日



Novell®

## 法令通知

米国 Novell, Inc. およびノベル株式会社は、本書の内容または本書を使用した結果について、いかなる保証、表明または約束も行っておりません。また、本書の商品性、および特定の用途への適合性について、いかなる黙示的保証も否認し、排除します。また、本書の内容は予告なく変更されることがあります。

米国 Novell, Inc. およびノベル株式会社は、すべてのノベル製ソフトウェアについて、いかなる保証、表明または約束も行っておりません。また、ノベル製ソフトウェアの商品性、および特定の用途への適合性について、いかなる黙示的保証も否認し、排除します。米国 Novell, Inc. およびノベル株式会社は、ノベル製ソフトウェアの内容を変更する権利を常に留保します。

すべての製品または技術情報はこの同意の下に提供され、米国の輸出管理および他国の通商法の制約を受けます。輸出管理規制に従って必要なライセンスを取得するか、または配送品の分類(輸出、再輸出、輸入)を取得することに同意します。現在の米国の輸出除外リストに掲載されているか、または米国の輸出管理法で指定されているエンティティに対して、貿易が禁止されている国またはテロリストの国に輸出または再輸出しないことに同意します。禁止されている核兵器、ミサイル、または最終化学生物兵器を配送しないことに同意します。Novell ソフトウェアを国外へ輸送する詳細については、[www.novell.com/info/exports/](http://www.novell.com/info/exports/) を参照してください。Novell は、輸出時に必要な承認を取得できなかったことによる問題について一切責任を負わないものとします。

Copyright © 2005, Novell, Inc. All rights reserved. 本書の一部または全体を無断で複写・転載することは、その形態を問わず禁じます。

本書に記載された製品で使用されている技術に関連する知的所有権は、弊社に帰属します。これらの知的所有権は、<http://www.novell.com/company/legal/patents/> に記載されている 1 つ以上の米国特許、および米国ならびにその他の国における 1 つ以上の特許または出願中の特許を含む場合があります。

Novell, Inc.  
404 Wyman Street, Suite 500  
Waltham, MA 02451  
U.S.A.

[www.novell.com](http://www.novell.com)

Novell eDirectory 8.8 管理ガイド  
2005 年 9 月 15 日

**オンラインドキュメント**：本製品およびその他の Novell 製品のオンラインマニュアルにアクセスする場合や、アップデート版を取得する場合は、<http://www.novell.com/documentation/japanese> を参照してください。

## Novell の商標

Client32 は、米国 Novell, Inc. の商標です。

eDirectory は、米国 Novell, Inc. の商標です。

NetWare は、米国 Novell, Inc. の米国ならびに他の国々における登録商標です。

NetWare Core Protocol および NCP は、米国 Novell, Inc. の商標です。

NMAS は、米国 Novell, Inc. の商標です。

Novell は、米国 Novell, Inc. の米国ならびに他の国々における登録商標です。

Novell Client は、米国 Novell, Inc. の商標です。

Novell Directory Services および NDS は、米国 Novell, Inc. の米国ならびに他の国々における登録商標です。

Ximiam は、米国 Novell, Inc. の米国ならびに他の国々における登録商標です。

ZENworks は、米国 Novell, Inc. の米国ならびに他の国々における登録商標です。

## サードパーティの商標

サードパーティ各社とその製品の商標は、所有者であるそれぞれの会社に所属します。

この製品には、OpenSSL プロジェクトが開発した OpenSSL Toolkit (<http://www.openssl.org>) で使用するソフトウェアが含まれています。





# 目次

|           |    |
|-----------|----|
| このガイドについて | 15 |
|-----------|----|

|                                 |           |
|---------------------------------|-----------|
| <b>1 Novell eDirectory について</b> | <b>17</b> |
| Novell eDirectory               | 18        |
| Novell iManager の便利な管理機能        | 18        |
| 強力なツリー構造                        | 19        |
| Web ベースの管理ユーティリティ               | 21        |
| シングルログインと認証                     | 22        |
| オブジェクトクラスとプロパティ                 | 22        |
| オブジェクトのリスト                      | 23        |
| コンテナオブジェクトクラス                   | 25        |
| リーフオブジェクトクラス                    | 29        |
| コンテキストと命名規則                     | 39        |
| 識別名                             | 40        |
| タイプ付きの名前                        | 40        |
| ネームレゾリューション                     | 40        |
| 現在のワークステーションのコンテキスト             | 41        |
| 先頭ピリオド                          | 41        |
| 相対命名                            | 41        |
| 後続ピリオド                          | 42        |
| Linux および UNIX でのコンテキストと命名規則    | 42        |
| スキーマ                            | 42        |
| スキーマ管理                          | 43        |
| スキーマクラス、属性、および構文                | 43        |
| 必須属性およびオプション属性について              | 48        |
| スキーマのサンプル                       | 48        |
| スキーマを設計する                       | 49        |
| パーティション                         | 49        |
| パーティション                         | 50        |
| パフォーマンス向上のためにレプリカを分散する          | 50        |
| パーティションと WAN リンク                | 51        |
| レプリカ                            | 52        |
| レプリカのタイプ                        | 53        |
| フィルタ済みレプリカ                      | 56        |
| NetWare バインダリエミュレーション           | 57        |
| レプリカリングでのサーバの同期                 | 58        |
| リソースへのアクセス                      | 58        |
| eDirectory での権利                 | 59        |
| トラスティ割り当ておよびターゲット               | 59        |
| eDirectory での権利の概念              | 59        |
| 新規サーバのデフォルト権                    | 65        |
| 管理の委託                           | 65        |
| 権利の管理                           | 66        |

|          |   |           |
|----------|---|-----------|
| <b>2</b> | <b>Novell eDirectory ネットワークの設計</b>                              | <b>73</b> |
|          | eDirectory 設計の基本  | 73        |
|          | ネットワークのレイアウト  | 73        |
|          | 組織の構造   | 74        |
|          | eDirectory 設計の準備をする   | 74        |
|          | eDirectory ツリーの設計   | 74        |
|          | 命名標準ドキュメントを作成する   | 74        |
|          | Tree の上位層を設計する  | 77        |
|          | ツリーの下位層を設計する  | 79        |
|          | ツリーのパーティション化のガイドライン   | 80        |
|          | ツリーの上位層におけるパーティションを決定する   | 81        |
|          | ツリーの下位層におけるパーティションを決定する   | 81        |
|          | パーティションサイズを決定する   | 81        |
|          | ネットワーク変数について  | 82        |
|          | ツリーのレプリカ作成に関するガイドライン  | 82        |
|          | ワークグループのニーズ   | 83        |
|          | 障害対策  | 83        |
|          | レプリカ数を決定する  | 84        |
|          | Tree パーティションのレプリカを作成する  | 84        |
|          | 管理用にレプリカを作成する   | 84        |
|          | NetWare のバインダリサービスの必要性に対応させる                                    | 84        |
|          | WAN トラフィックを管理する   | 85        |
|          | ユーザ環境についてのプランニング  | 85        |
|          | ユーザの必要条件を検討する   | 85        |
|          | アクセスに関するガイドラインを作成する   | 85        |
|          | e ビジネスに対応する eDirectory の設計                                      | 86        |
|          | Novell Certificate Server について                                  | 87        |
|          | Novell Certificate Server でタスクを実行するのに必要な権利                      | 87        |
|          | Linux、Solaris、AIX、および HP-UX システムでの eDirectory 操作に関するセキュリティを確保する | 88        |
|          | ネットワーク時刻の同期   | 91        |
|          | NetWare サーバで時刻を同期する   | 92        |
|          | Windows サーバで時刻を同期する   | 93        |
|          | Linux、Solaris、AIX、または HP-UX システムで時刻を同期する                        | 93        |
|          | 時刻同期を確認する   | 93        |
|          | セキュリティ上の考慮事項  | 94        |
| <b>3</b> | <b>オブジェクトの管理</b>  | <b>95</b> |
|          | オブジェクトに関連する一般的なタスク  | 95        |
|          | eDirectory ツリーを参照する   | 96        |
|          | オブジェクトを作成する   | 98        |
|          | オブジェクトのプロパティを変更する   | 99        |
|          | オブジェクトをコピーする  | 99        |
|          | オブジェクトを移動する   | 99        |
|          | オブジェクトを削除する   | 100       |
|          | オブジェクトをリネームする   | 100       |
|          | ユーザアカウントを管理する   | 100       |
|          | ユーザアカウントを作成および変更する  | 101       |
|          | オプションのアカウント機能を設定する  | 102       |
|          | ログインスクリプトを設定する  | 104       |
|          | リモートユーザのログイン時間制限  | 105       |
|          | ユーザアカウントを削除する   | 106       |
|          | 役割ベースサービスを設定する  | 106       |
|          | RBS 役割を定義する   | 108       |
|          | カスタム RBS タスクを定義する   | 110       |
|          | 同期  | 111       |
|          | 同期の特徴   | 112       |

|   |            |
|---|------------|
| 通常同期またはレプリカ同期                                 | 113        |
| 優先度同期   | 115        |
| <b>4 スキーマの管理</b>                              | <b>123</b> |
| スキーマの拡張                                       | 124        |
| クラスを作成する                                      | 124        |
| クラスを削除する                                      | 124        |
| 属性を作成する                                       | 125        |
| クラスへオプション属性を追加する                              | 125        |
| 属性を削除する                                       | 126        |
| 補助クラスを作成する                                    | 126        |
| 補助クラスのプロパティでオブジェクトを拡張する                       | 126        |
| オブジェクトの補助プロパティを変更する                           | 127        |
| オブジェクトから補助プロパティを削除する                          | 127        |
| スキーマの表示                                       | 128        |
| クラス情報を参照する                                    | 128        |
| 属性情報を表示する                                     | 128        |
| 手動でスキーマを拡張する                                  | 128        |
| NetWare でスキーマを拡張する                            | 129        |
| Windows でスキーマを拡張する                            | 129        |
| Linux、Solaris、AIX、または HP-UX システムでスキーマを拡張する    | 129        |
| eDirectory 8.7 に追加されたスキーマフラグ                  | 131        |
| eMBox クライアントを使用してスキーマ操作を実行する                  | 133        |
| DSSchema eMTool を使用する                         | 133        |
| DSSchema eMTool オプション                         | 134        |
| <b>5 パーティションおよびレプリカの管理</b>                    | <b>135</b> |
| パーティションの作成                                    | 136        |
| パーティションのマージ                                   | 137        |
| パーティションの移動                                    | 138        |
| パーティションの作成操作またはマージ操作のキャンセル                    | 139        |
| レプリカの管理                                       | 140        |
| レプリカを追加する                                     | 140        |
| レプリカを削除する                                     | 141        |
| レプリカタイプを変更する                                  | 142        |
| フィルタ済みレプリカを設定し管理する                            | 143        |
| フィルタ処理済レプリカウィザードを使用する                         | 143        |
| パーティションスコープを定義する                              | 144        |
| サーバフィルタを設定する                                  | 145        |
| パーティションおよびレプリカを表示する                           | 146        |
| サーバのパーティションを表示する                              | 146        |
| パーティションレプリカを表示する                              | 146        |
| パーティションに関する情報を表示する                            | 147        |
| パーティションの階層を表示する                               | 147        |
| レプリカに関する情報を表示する                               | 147        |
| <b>6 Novell eDirectory 管理ユーティリティ</b>          | <b>149</b> |
| Novell インポート / エクスポート変換ユーティリティ                | 149        |
| Novell iManager インポート / エクスポート変換ウィザードを使用する    | 150        |
| コマンドラインインタフェースを使用する                           | 158        |
| 変換ルール   | 176        |
| LBURP (LDAP Bulk Update/Replication Protocol) | 185        |
| LDAP ディレクトリ間でスキーマを移行する                        | 186        |
| LDIF のインポートを高速化する                             | 186        |
| インデックスマネージャ                                   | 188        |
| インデックスを作成する                                   | 189        |
| インデックスを削除する                                   | 189        |

|  |            |
|--|------------|
| インデックスをオフラインにする . . . . .                                | 190        |
| 他のサーバ上でインデックスを管理する . . . . .                             | 190        |
| Novell インポート / エクスポート変換ユーティリティを使用してインデックスを管理する . . . . . | 191        |
| プレディケートデータ . . . . .                                     | 193        |
| プレディケートデータを管理する . . . . .                                | 193        |
| eDirectory Service Manager . . . . .                     | 194        |
| eMBox クライアントのサービスマネージャ eMTool を使用する . . . . .            | 194        |
| Novell iManager でサービスマネージャプラグインを使用する . . . . .           | 195        |
| <b>7 Novell iMonitor 2.1 の使用</b>                         | <b>197</b> |
| システム要件 . . . . .   | 198        |
| プラットフォーム . . . . .                                       | 198        |
| 監視できる eDirectory のバージョン . . . . .                        | 199        |
| iMonitor へアクセスする . . . . .                               | 199        |
| iMonitor のアーキテクチャ . . . . .                              | 199        |
| iMonitor ページの構成 . . . . .                                | 200        |
| 動作モード . . . . .  | 201        |
| すべてのページからアクセス可能な iMonitor の機能 . . . . .                  | 202        |
| NetWare Remote Manager との統合 . . . . .                    | 202        |
| 環境設定ファイル . . . . .                                       | 203        |
| iMonitor の機能 . . . . .                                   | 206        |
| eDirectory サーバのヘルス情報の表示 . . . . .                        | 206        |
| パーティション同期ステータスの表示 . . . . .                              | 207        |
| サーバ接続情報の表示 . . . . .                                     | 207        |
| 認識されているサーバの表示 . . . . .                                  | 208        |
| レプリカ情報の表示 . . . . .                                      | 208        |
| DS エージェントを制御および環境設定する . . . . .                          | 209        |
| トレースを環境設定する . . . . .                                    | 210        |
| プロセスステータス情報の表示 . . . . .                                 | 211        |
| エージェントアクティビティの表示 . . . . .                               | 211        |
| トラフィックパターンの表示 . . . . .                                  | 212        |
| バックグラウンドプロセスの表示 . . . . .                                | 212        |
| eDirectory サーバエラーの表示 . . . . .                           | 212        |
| DSRepair 情報の表示 . . . . .                                 | 213        |
| エージェントのヘルス情報を表示する . . . . .                              | 213        |
| ツリー内のオブジェクトの参照 . . . . .                                 | 213        |
| 同期またはパージのためのエントリの表示 . . . . .                            | 214        |
| Novell Nsure Identity Manager の詳細の表示 . . . . .           | 214        |
| レプリカの同期ステータスの表示 . . . . .                                | 215        |
| レポートの設定と表示 . . . . .                                     | 215        |
| スキーマ、クラス、および属性定義の表示 . . . . .                            | 217        |
| オブジェクトの検索 . . . . .                                      | 217        |
| ストリームビューアの使用 . . . . .                                   | 218        |
| DIB セットのクローン . . . . .                                   | 218        |
| セキュリティ保護された iMonitor 操作の実現 . . . . .                     | 224        |
| <b>8 Novell eDirectory ツリーのマージ</b>                       | <b>225</b> |
| eDirectory ツリーのマージ . . . . .                             | 226        |
| 前提条件 . . . . .   | 226        |
| ターゲットツリーの要件 . . . . .                                    | 226        |
| スキーマの要件 . . . . .  | 227        |
| ソースツリーをターゲットツリーへマージする . . . . .                          | 227        |
| パーティションの変化 . . . . .                                     | 227        |
| ソースツリーとターゲットツリーを準備する . . . . .                           | 228        |
| マージする前の時刻の同期 . . . . .                                   | 229        |
| 2 つのツリーのマージ . . . . .                                    | 230        |
| <b>8 Novell eDirectory 8.8 管理ガイド</b>                     |            |

|                                       |            |
|---------------------------------------|------------|
| マージ後の作業                               | 231        |
| サーバツリーの結合                             | 232        |
| コンテキスト名の変更について                        | 234        |
| ソースツリーとターゲットツリーを準備する                  | 234        |
| ソースツリーとターゲットツリーを結合する                  | 237        |
| ツリー名の変更                               | 237        |
| eMBox クライアントを使用したツリーのマージ              | 238        |
| DSMerge eMTool を使用する                  | 238        |
| DSMerge eMTool オプション                  | 239        |
| <b>9 eDirectory のデータを暗号化する</b>        | <b>241</b> |
| 暗号化属性                                 | 241        |
| 暗号化方式を使用する                            | 243        |
| 暗号化属性ポリシーを管理する                        | 243        |
| 暗号化属性にアクセスする                          | 247        |
| 暗号化属性を表示する                            | 248        |
| バックアップデータを暗号化 / 復号化する                 | 248        |
| 暗号化属性を含む DIB ファイルセットのクローンを作成する        | 249        |
| レプリカリングに eDirectory 8.8 サーバを追加する      | 249        |
| 下位互換性                                 | 249        |
| 暗号化属性に移行する                            | 249        |
| 暗号化属性のレプリカを作成する                       | 249        |
| 暗号化レプリケーション                           | 250        |
| 暗号化複製を有効にする                           | 251        |
| 新しいレプリカをレプリカリングに追加する                  | 255        |
| 同期と暗号化複製                              | 260        |
| 暗号化複製ステータスを表示する                       | 260        |
| データを暗号化するときデータの完全な安全性を確保する            | 261        |
| 完全に新しい設定でデータを暗号化する                    | 262        |
| 既存の設定でデータを暗号化する                       | 262        |
| まとめ                                   | 264        |
| <b>10 Novell eDirectory データベースの修復</b> | <b>265</b> |
| 基本修復操作の実行                             | 266        |
| 標準修復を実行する                             | 267        |
| ローカルデータベースの修復の実行                      | 269        |
| 外部参照のチェック                             | 269        |
| 単一オブジェクトの修復                           | 270        |
| 不明なリーフオブジェクトの削除                       | 270        |
| 修復ログファイルの表示と設定                        | 271        |
| ログファイルを開く                             | 271        |
| ログファイルオプションを設定する                      | 271        |
| Novell iMonitor での修復の実行               | 272        |
| レプリカの修復                               | 272        |
| すべてのレプリカを修復する                         | 273        |
| 選択したレプリカを修復する                         | 273        |
| タイムスタンプを修復する                          | 273        |
| このサーバを新しいマスタレプリカに設定する                 | 274        |
| 選択したレプリカを削除する                         | 275        |
| レプリカリングを修復する                          | 275        |
| すべてのレプリカリングを修復する                      | 276        |
| 選択したレプリカリングを修復する                      | 276        |
| リング内のすべてのサーバにすべてのオブジェクトを送信する          | 276        |
| マスタから選択したレプリカへすべてのオブジェクトを受信する         | 277        |
| レプリカリングからこのサーバを削除する                   | 277        |
| スキーマの保守                               | 278        |

|  |            |
|--|------------|
| ツリーからスキーマを要求する                                     | 278        |
| ローカルスキーマをリセットする                                    | 278        |
| Post-NetWare 5 スキーマの更新を実行する                        | 279        |
| オプションスキーマ拡張機能を実行する                                 | 279        |
| リモートスキーマをインポートする                                   | 280        |
| 新規スキーマエポックを宣言する                                    | 280        |
| サーバのネットワークアドレスの修復                                  | 281        |
| すべてのネットワークアドレスを修復する                                | 281        |
| サーバのネットワークアドレスを修復する                                | 281        |
| 同期化操作を実行する   | 282        |
| 選択したレプリカをこのサーバで同期する                                | 282        |
| このサーバの同期ステータスをレポートする                               | 283        |
| すべてのサーバの同期ステータスをレポートする                             | 283        |
| 時刻同期を実行する  | 284        |
| 即時同期をスケジュールする                                      | 284        |
| DSRepair の詳細オプション                                  | 285        |
| eDirectory サーバ上で DSRepair を実行する                    | 285        |
| DSRepair コマンドラインオプション                              | 286        |
| DSRepair 詳細設定スイッチの使用                               | 288        |
| eMBox クライアントを使用したデータベースの修復                         | 289        |
| DSRepair eMTool を使用する                              | 289        |
| DSRepair eMTool のオプション                             | 290        |
| <b>11 WAN トラフィックマネージャ</b>                          | <b>293</b> |
| WAN トラフィックマネージャについて                                | 293        |
| LAN エリアオブジェクト                                      | 295        |
| WAN トラフィックポリシー                                     | 297        |
| WAN トラフィックを制限する                                    | 301        |
| コストファクタを割り当てる                                      | 302        |
| WAN トラフィックマネージャポリシーグループ                            | 303        |
| 1-3AM.WMG  | 303        |
| 7AM-6PM.WMG  | 304        |
| COSTLT20.WMG                                       | 304        |
| IPX.WMG  | 304        |
| NDSTTYP.S.WMG                                      | 305        |
| ONOSPOOF.WMG                                       | 317        |
| OPNSPOOF.WMG                                       | 317        |
| SAMEAREA.WMG                                       | 317        |
| TCPIP.WMG  | 318        |
| TIMECOST.WMG                                       | 318        |
| WAN ポリシーの構成  | 319        |
| 宣言セクション  | 319        |
| セレクタセクション  | 321        |
| プロバイダセクション   | 321        |
| ポリシーセクションで使用される構文                                  | 322        |
| <b>12 LDAP Services for Novell eDirectory について</b> | <b>327</b> |
| LDAP サービスの主な用語                                     | 328        |
| クライアントとサーバ   | 328        |
| オブジェクト   | 328        |
| 参照   | 329        |
| LDAP と eDirectory の連携について                          | 331        |
| LDAP から eDirectory に接続する                           | 331        |
| クラスと属性のマッピング                                       | 334        |
| 非標準スキーマ出力を有効にする                                    | 337        |
| 構文の相違  | 338        |

|   |            |
|---|------------|
| サポートされる Novell LDAP コントロールおよび拡張   | 339        |
| Linux、Solaris、AIX、または HP-UNIX 環境での LDAP ツールの使用                          | 340        |
| LDAP ツール  | 341        |
| 拡張可能一致検索フィルタ  | 350        |
| <b>13 LDAP Services for Novell eDirectory の環境設定</b>                     | <b>353</b> |
| LDAP Services for eDirectory をロードおよびアンロードする                             | 353        |
| LDAP サーバがロードされているか確認する  | 354        |
| LDAP サーバが実行されているか確認する   | 355        |
| シナリオ  | 355        |
| LDAP サーバが実行されているか確認する   | 356        |
| デバイスが受信待機していることを確認する  | 358        |
| LDAP オブジェクトを環境設定する  | 358        |
| Linux、Solaris、AIX、HP-UX システム上で、LDAP サーバオブジェクトおよび LDAP グループオブジェクトを環境設定する | 360        |
| LDAP サーバをリフレッシュする   | 363        |
| 認証とセキュリティ   | 364        |
| パスワードとの単純バインドに TLS を要求する  | 364        |
| TLS を開始 / 停止する  | 365        |
| TLS のサーバを環境設定する   | 366        |
| TLS のクライアントを環境設定する  | 367        |
| ルート認証局をエクスポートする   | 367        |
| クライアント証明書で認証を受ける  | 368        |
| サードパーティプロバイダの証明書を使用する   | 368        |
| LDAP プロキシユーザを作成および使用する  | 369        |
| SASL を使用する  | 370        |
| LDAP サーバを使ってディレクトリを検索する   | 372        |
| 検索制限を設定する   | 372        |
| 参照を使用する   | 373        |
| フィルタ済みレプリカを検索する   | 378        |
| 上方参照を設定する   | 379        |
| シナリオ：連結ツリーでの上方参照  | 379        |
| 信頼されていない領域を作成する   | 380        |
| 参照データを指定する  | 381        |
| LDAP で参照情報を更新する   | 382        |
| 影響を受ける操作  | 382        |
| 上方参照のサポートの有無を確認する   | 383        |
| 持続的検索：eDirectory イベントの設定  | 383        |
| 持続的検索の管理  | 384        |
| イベントの監視拡張操作の使用を制御する   | 385        |
| LDAP サーバの情報を取得する  | 386        |
| <b>14 Novell eDirectory のバックアップと復元</b>                                  | <b>389</b> |
| eDirectory のバックアップ処理に関する確認事項  | 390        |
| バックアップサービスおよび復元サービスについて   | 393        |
| eDirectory Backup eMTool について   | 393        |
| eDirectory 8.7.3 のバックアップ / 復元機能で変更された事項                                 | 394        |
| Backup eMTool による復元作業の概要  | 396        |
| バックアップファイルのヘッダ書式  | 397        |
| バックアップログファイルの書式   | 401        |
| DSMASTER サーバによる災害対策   | 402        |
| 遷移ベクトルと復元後の検証処理   | 403        |
| 復元後の検証については eDirectory 8.5 以降のみで互換性がある                                  | 403        |
| NetWare のファイルシステムデータを復元する際のアクセス権の保存                                     | 404        |
| ロールフォワードログを使用する   | 405        |
| ロールフォワードログ機能を使用する上での注意事項  | 406        |

|  |            |
|--|------------|
| ロールフォワードログの保存先   | 407        |
| ロールフォワードログのバックアップと削除                                     | 408        |
| 注意：eDirectory を削除するとロールフォワードログも削除される問題                   | 409        |
| 復元処理の準備  | 409        |
| 復元作業の前提条件  | 409        |
| 復元に必要なバックアップファイルの収集                                      | 411        |
| Novell iManager を使ったバックアップ / 復元作業                        | 412        |
| iManager による手動バックアップ                                     | 413        |
| iManager によるロールフォワードログの設定                                | 415        |
| iManager によるバックアップファイルの復元作業                              | 417        |
| eMBox クライアントを使ったバックアップ / 復元作業                            | 420        |
| eMBox クライアントによる手動バックアップ                                  | 420        |
| バッチファイルと eMBox クライアントによる無人バックアップ                         | 423        |
| eMBox クライアントによるロールフォワードログの設定                             | 426        |
| eMBox クライアントによるバックアップファイルの復元作業                           | 428        |
| バックアップ / 復元のコマンドラインオプション                                 | 431        |
| NetWare で DSBK.NLM を使用する                                 | 438        |
| サーバ固有情報のバックアップに関する変更事項 (NetWare のみ)                      | 438        |
| 復元後の検証処理に失敗した場合の対処方法                                     | 440        |
| レプリカリングをクリーンアップする  | 441        |
| サーバの復旧とレプリカの再追加  | 442        |
| バックアップ / 復元の運用例  | 444        |
| シナリオ：単一サーバ構成のネットワークで、eDirectory を格納しているハードディスクが故障した場合    | 445        |
| シナリオ：複数サーバ構成のネットワークで、eDirectory を格納しているハードディスクが故障した場合    | 446        |
| シナリオ：複数サーバ構成のネットワークで、1 台のサーバが完全に使えなくなった場合                | 448        |
| シナリオ：複数サーバ構成のネットワークで、数台のサーバが使えなくなった場合                    | 449        |
| シナリオ：複数サーバ構成のネットワークで、すべてのサーバが使えなくなった場合                   | 449        |
| NICI のバックアップと復元  | 451        |
| UNIX   | 452        |
| NetWare の場合  | 454        |
| Windows の場合  | 454        |
| <b>15 Novell eDirectory の SNMP サポート</b>                  | <b>457</b> |
| SNMP に関する用語の定義   | 457        |
| SNMP サービスについて  | 458        |
| eDirectory と SNMP  | 460        |
| eDirectory の管理に SNMP を使う利点                               | 460        |
| eDirectory での SNMP の機能について                               | 461        |
| eDirectory の SNMP サービスのインストールと設定                         | 464        |
| SNMP サーバモジュールのロードとアンロード                                  | 464        |
| サブエージェントの設定  | 465        |
| eDirectory の SNMP サービスの設定                                | 467        |
| SNMP による eDirectory の監視                                  | 478        |
| トラップ   | 479        |
| トラップに関する設定   | 494        |
| 統計情報   | 506        |
| トラブルシューティング  | 511        |
| <b>16 Novell eDirectory のメンテナンス</b>                      | <b>513</b> |
| eDirectory のパフォーマンスの改善                                   | 513        |
| エントリキャッシュとブロックキャッシュでメモリを配分する                             | 514        |
| デフォルトのキャッシュ設定を使用する                                       | 514        |
| LDAP for eDirectory をチューニングする                            | 519        |
| Linux、Solaris、AIX、および HP-UX システムでの eDirectory パフォーマンスの改善 | 522        |
| eDirectory サーバを微調整する                                     | 522        |
| eDirectory のキャッシュを最適化する                                  | 523        |



|  |            |
|--|------------|
| Novell eDirectory 用に Solaris OS をチューニングする          | 526        |
| eDirectory のパフォーマンスの改善                             | 528        |
| eDirectory キャッシュの設定                                | 528        |
| LBURP トランザクションサイズの設定                               | 529        |
| ICE の非同期要求の数を増やす                                   | 529        |
| LDAP 書き込みスレッド数の増加                                  | 530        |
| ICE のスキーマ検証を無効にする                                  | 530        |
| ACL テンプレートを無効にする                                   | 531        |
| バックリンカ   | 532        |
| インラインキャッシュを有効 / 無効にする                              | 532        |
| LBURP のタイムアウト周期の拡大                                 | 533        |
| eDirectory の正常な動作の維持                               | 533        |
| ヘルスチェックを実行する時期                                     | 533        |
| ヘルスチェックの概要   | 534        |
| iMonitor を使用した eDirectory のヘルスチェック                 | 534        |
| 詳細情報   | 535        |
| 監視のためのリソース   | 536        |
| ハードウェアのアップグレードやサーバの交換                              | 536        |
| サーバを交換しないでハードウェアまたは記憶デバイスを計画的にアップグレードする            | 536        |
| サーバの計画的な交換   | 540        |
| ハードウェア障害後の eDirectory の復元                          | 543        |
| <b>17 DHost iConsole Manager</b>                   | <b>545</b> |
| DHost について   | 546        |
| DHost iConsole の実行                                 | 547        |
| NetWare で DHost iConsole を実行する                     | 547        |
| Windows で DHost iConsole を実行する                     | 547        |
| Linux、Solaris、AIX、および HP-UX で DHost iConsole を実行する | 548        |
| eDirectory モジュールの管理                                | 548        |
| NetWare でモジュールをロードまたはアンロードする                       | 549        |
| Windows でモジュールをロードまたはアンロードする                       | 549        |
| Linux、Solaris、AIX、および HP-UX でモジュールをロードまたはアンロードする   | 549        |
| DHost 情報の照会  | 550        |
| 環境設定パラメータを表示する                                     | 550        |
| プロトコル情報を表示する                                       | 550        |
| 接続プロパティを表示する                                       | 551        |
| スレッドプールの統計情報を表示する                                  | 551        |
| プロセススタック   | 552        |
| SAdmin パスワードを設定する                                  | 552        |
| NetWare で SAdmin パスワードを設定する                        | 552        |
| Windows で SAdmin パスワードを設定する                        | 553        |
| Linux、Solaris、AIX、および HP-UX で SAdmin パスワードを設定する    | 553        |
| <b>18 eDirectory Management Toolbox</b>            | <b>555</b> |
| eMBox コマンドラインクライアントの使用                             | 555        |
| コマンドラインヘルプを表示する                                    | 556        |
| eMBox コマンドラインクライアントを対話式モードで実行する                    | 556        |
| eMBox コマンドラインクライアントをバッチモードで実行する                    | 560        |
| eMBox コマンドラインクライアントのオプション                          | 563        |
| eMBox クライアントを使用してセキュア接続を確立する                       | 564        |
| eDirectory ポート番号を確認する                              | 564        |
| eMBox ログの記録の使用                                     | 566        |
| eMBox ログの記録コマンドラインクライアントを使用する                      | 567        |
| Novell iManager で eMBox ログの記録機能を使用する               | 567        |

|          |   |            |
|----------|---|------------|
| <b>A</b> | <b>NMAS の注意事項</b>                                     | <b>569</b> |
|          | 独立したパーティションとしてのセキュリティコンテナの設定                          | 569        |
|          | 複数のセキュリティコンテナを持つツリーのマージ                               | 569        |
|          | ツリーのマージ前に実行する製品固有の操作                                  | 570        |
|          | ツリーのマージを実行する  | 573        |
|          | ツリーのマージ後に実行する製品固有の操作                                  | 573        |
| <b>B</b> | <b>Novell eDirectory の Linux および UNIX 用コマンドとその使用法</b> | <b>575</b> |
|          | 一般ユーティリティ   | 575        |
|          | LDAP 固有のコマンド  | 579        |
| <b>C</b> | <b>OpenSLP for eDirectory の設定</b>                     | <b>581</b> |
|          | Service Location Protocol                             | 581        |
|          | SLP の基本   | 581        |
|          | Novell Service Location Providers                     | 582        |
|          | ユーザエージェント   | 583        |
|          | サービスエージェント  | 583        |
|          | 環境設定パラメータ   | 584        |
| <b>D</b> | <b>Novell eDirectory が DNS を使用する際の動作について</b>          | <b>585</b> |
| <b>E</b> | <b>eDirectory での GSSAPI の設定</b>                       | <b>587</b> |
|          | 前提条件  | 587        |
|          | ネットワークの特性に関する前提                                       | 588        |
|          | iManager 用の Kerberos プラグインのインストール                     | 588        |
|          | Kerberos の LDAP 拡張の追加                                 | 590        |
|          | ルート認証局証明書のエクスポート                                      | 591        |
|          | SASL-GSSAPI メソッドの設定                                   | 592        |
|          | SASL-GSSAPI メソッドを使用して設定された eDirectory ツリーをマージする       | 592        |
|          | SASL-GSSAPI メソッドの管理                                   | 592        |
|          | Kerberos スキーマの拡張                                      | 592        |
|          | Kerberos レルムオブジェクトの管理                                 | 593        |
|          | サービスプリンシパルの管理   | 594        |
|          | 外部プリンシパルの編集   | 599        |
|          | ログインシーケンスの作成  | 599        |
|          | LDAP での SASL-GSSAPI の使用方法                             | 599        |
|          | エラーメッセージ  | 599        |

# このガイドについて

このガイドでは、Novell® eDirectory™ 8.8 の管理および設定の方法について説明します。このガイドはネットワーク管理者を対象にし、次のセクションから構成されています。

- ◆ 17 ページの第 1 章「Novell eDirectory について」
- ◆ 73 ページの第 2 章「Novell eDirectory ネットワークの設計」
- ◆ 95 ページの第 3 章「オブジェクトの管理」
- ◆ 123 ページの第 4 章「スキーマの管理」
- ◆ 135 ページの第 5 章「パーティションおよびレプリカの管理」
- ◆ 149 ページの第 6 章「Novell eDirectory 管理ユーティリティ」
- ◆ 197 ページの第 7 章「Novell iMonitor 2.1 の使用」
- ◆ 225 ページの第 8 章「Novell eDirectory ツリーのマージ」
- ◆ 241 ページの第 9 章「eDirectory のデータを暗号化する」
- ◆ 265 ページの第 10 章「Novell eDirectory データベースの修復」
- ◆ 293 ページの第 11 章「WAN トラフィックマネージャ」
- ◆ 327 ページの第 12 章「LDAP Services for Novell eDirectory について」
- ◆ 353 ページの第 13 章「LDAP Services for Novell eDirectory の環境設定」
- ◆ 389 ページの第 14 章「Novell eDirectory のバックアップと復元」
- ◆ 457 ページの第 15 章「Novell eDirectory の SNMP サポート」
- ◆ 513 ページの第 16 章「Novell eDirectory のメンテナンス」
- ◆ 545 ページの第 17 章「DHost iConsole Manager」
- ◆ 555 ページの第 18 章「eDirectory Management Toolbox」
- ◆ 569 ページの付録 A「NMAP の注意事項」
- ◆ 575 ページの付録 B「Novell eDirectory の Linux および UNIX 用コマンドとその使用法」
- ◆ 581 ページの付録 C「OpenSLP for eDirectory の設定」
- ◆ 585 ページの付録 D「Novell eDirectory が DNS を使用する際の動作について」
- ◆ 587 ページの付録 E「eDirectory での GSSAPI の設定」

## 補足マニュアル

eDirectory のインストール手順については、『[Novell eDirectory 8.8 インストールガイド](http://www.novell.com/documentation/edir88/index.html)』(<http://www.novell.com/documentation/edir88/index.html>) を参照してください。

eDirectory 管理ユーティリティに関するマニュアルについては、『[Novell iManager 2.5 管理ガイド](http://www.novell.com/documentation/imanager25/index.html)』(<http://www.novell.com/documentation/imanager25/index.html>) を参照してください。

## マニュアルの更新

このガイドの最新版については、『[Novell eDirectory 8.8 管理ガイド](http://www.novell.com/documentation/edir88/index.html)』(<http://www.novell.com/documentation/edir88/index.html>) を参照してください。

## マニュアルの表記規則

このマニュアルでは、不等号 (>) を使用して、操作手順の動作、およびクロスリファレンスパス内の項目を区切ります。

「®」、「™」などの商標記号は、Novell の商標を示します。アスタリスク (\*) はサードパーティの商標を示します。

パス名に円記号 (¥) が使用されるプラットフォームやスラッシュ (/) が使用されるプラットフォームがありますが、パス名は円記号で表記されています。Linux や UNIX\* など、スラッシュを必要とするプラットフォームでは、ソフトウェアの必要に応じてスラッシュを使用してください。

# 1

## Novell eDirectory について

Novell® eDirectory™ は、高い拡張性を持ち、高性能で、安全性の高いディレクトリサービスです。ユーザ、アプリケーション、ネットワークデバイス、およびデータなど、多量のオブジェクトを格納および管理できます。Novell eDirectory が提供する安全な識別情報管理ソリューションは、複数のプラットフォーム間で実行され、インターネット規模の高い拡張性を持っています。

また、識別情報管理、インフラストラクチャ、インターネット上のセキュリティ、および拡張性が 1 つに集約されて、ファイアウォール越しに実行されるすべてのアプリケーションで利用できます。Novell eDirectory には、Web ベースのワイヤレスな管理機能が搭載されており、Web ブラウザおよびさまざまな携帯用デバイスから、ディレクトリやユーザ、アクセス権、およびネットワークリソースにアクセスしたり、それらを管理したりすることができます。

eDirectory では、ディレクトリ標準 LDAP (Lightweight Directory Access Protocol) バージョン 3 がネイティブでサポートされ、OpenSSL ソースコードに基づいた TLS/SSL サービスがサポートされています。

eDirectory エンジンの詳細については、[eDirectory Process Requests \(http://developer.novell.com/research/sections/netmanage/dirprimer/2002/august/p020801.htm\)](http://developer.novell.com/research/sections/netmanage/dirprimer/2002/august/p020801.htm) を参照してください。

このセクションでは、次の情報について説明します。

- ◆ 18 ページの「Novell eDirectory」
- ◆ 18 ページの「Novell iManager の便利な管理機能」
- ◆ 22 ページの「オブジェクトクラスとプロパティ」
- ◆ 39 ページの「コンテキストと命名規則」
- ◆ 42 ページの「スキーマ」
- ◆ 49 ページの「パーティション」
- ◆ 52 ページの「レプリカ」
- ◆ 57 ページの「NetWare バインダリエミュレーション」
- ◆ 58 ページの「レプリカリングでのサーバの同期」
- ◆ 58 ページの「リソースへのアクセス」
- ◆ 59 ページの「eDirectory での権利」

# Novell eDirectory

簡単に言うと、Novell eDirectory は、ネットワークユーザ、サーバ、プリンタ、プリントキュー、アプリケーションなどのネットワークリソースを表すオブジェクトのリストです。図 1 は、Novell iManager 管理ユーティリティで表示されるオブジェクトの一部を示しています。

図 1 iManager での eDirectory オブジェクト



eDirectory サーバで設定された実際のスキーマや eDirectory を実行するオペレーティングシステムによっては、使用できないオブジェクトクラスもあります。

オブジェクトの詳細については、22 ページの「オブジェクトクラスとプロパティ」を参照してください。

ネットワークに複数の eDirectory サーバがある場合、ディレクトリは複数のサーバに複製できます。

## Novell iManager の便利な管理機能

Novell eDirectory では、ネットワークリソースを、容易に、強力に、またフレキシブルに管理できます。eDirectory は、グループウェアやその他アプリケーションのユーザ情報のリポジトリとしても機能します。これらのアプリケーションは、業界標準の LDAP (Lightweight Directory Access Protocol) を使用して、ディレクトリにアクセスします。

eDirectory の便利な管理機能には、強力なツリー構造、統合管理ユーティリティ、およびシングルログインと認証機能があります。

Novell iManager では、Web ブラウザやさまざまな携帯用デバイスから、ディレクトリやユーザ、ディレクトリ内のアクセス権やネットワークリソースを管理できます。iManager への eDirectory プラグインによって、基本的なディレクトリ管理タスクや、DSRepair、DSMerge、バックアップおよび復元などの、以前は eDirectory サーバで実行する必要のあった eDirectory 管理ユーティリティにアクセスすることができます。

詳細については、『Novell iManager 2.5 管理ガイド』(<http://www.novell.com/documentation/imanager25/index.html>) を参照してください。

## 強力なツリー構造

Novell eDirectory では、ツリー構造内にオブジェクトが編成されます。最上部の Tree オブジェクトには、ツリー名が付けられます。

eDirectory サーバで動作するオペレーティングシステムが NetWare、Linux、UNIX、Windows のどれであっても、すべてのリソースを同じツリー内に保管できます。オブジェクトの作成や、権利の付与、パスワードの変更、アプリケーションの管理のために、それぞれのサーバやドメインに個別にアクセスする必要はありません。

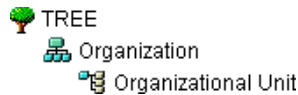
ツリーの階層構造によって、極めて柔軟で強力な管理が可能になっています。このような管理機能は、主に次の 2 つの機能で実現できます。


- ◆ 19 ページの「コンテナオブジェクト」
- ◆ 20 ページの「継承」


## コンテナオブジェクト


コンテナオブジェクトを利用することによって、オブジェクトを個々に扱うのではなく、オブジェクトのまとまりとして扱うことができます。図 2 に示すように、コンテナオブジェクトには、3 つの共通クラスがあります。

図 2 コンテナオブジェクトの共通クラス




 Tree オブジェクトは、ツリー内の最上部のコンテナオブジェクトです。通常、このコンテナには、その会社の組織オブジェクトが格納されます。

 組織は通常、Tree オブジェクトの直下に位置するコンテナクラスです。一般に、組織オブジェクトには会社名に基づく名前が付けられます。小規模な会社の場合は、管理を容易化するために、他のオブジェクトをすべて組織オブジェクトの直下に配置します。

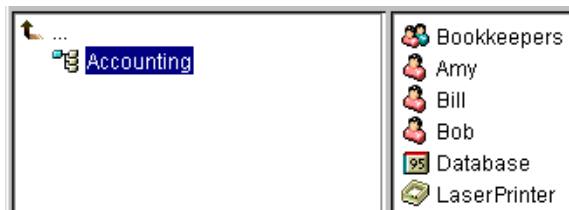
 組織の下に部門オブジェクトを作成し、異なった地区、ネットワークキャンパス、または個々の部署を表すことができます。部門の下にさらに部門を作成して、ツリーを細分化することもできます。

その他、コンテナオブジェクトには、カントリクラスと地域クラスがあります。これらのクラスは通常、複数の国にまたがるネットワークでのみ使用されます。

 ドメインオブジェクトは、Tree オブジェクトの下、または組織、部門、カントリ、および地域オブジェクトの下に作成されます。

コンテナ内のすべてのオブジェクトに対してなんらかの処理を行う場合、コンテナオブジェクトに処理を行えば1回の実行で済みます。たとえば、Accounting コンテナ内のすべてのオブジェクトに対する管理制御権を、Amy という名前のユーザに与えます。( 図 3 を参照してください。)

図 3 コンテナオブジェクト



この場合、Accounting オブジェクトを右クリックして [オブジェクトのトラスティ] を選択し、Amy をトラスティとして追加します。次に、Amy に与える権利を選択して [OK] をクリックします。これで Amy に、Database アプリケーション、Bookkeepers グループ、LaserPrinter プリンタ、および Amy、Bill、Bob のユーザオブジェクトを管理する権利が与えられました。

## 継承

eDirectory のもう 1 つの強力な機能は、権利の継承です。継承とは、ツリー内の上位層のコンテナの権利が、それぞれの下位層のすべてのコンテナに受け継がれることを意味します。この機能によって、権利の割り当て回数を少なくすることができます。たとえば、20 ページの 図 4 に示すオブジェクトに対する管理権を与えます。

図 4 eDirectory オブジェクトの例



次の割り当てのいずれかを行うことができます。

- ◆ ユーザに Allentown に対する権利を与えると、そのユーザは Allentown コンテナ内のオブジェクトのみ管理できます。
- ◆ ユーザに East に対する権利を与えると、そのユーザは East、Allentown、および Yorktown コンテナ内のオブジェクトを管理できます。
- ◆ ユーザに YourCo に対する権利を与えると、そのユーザは図中のすべてのコンテナのすべてのオブジェクトを管理できます。

権利の割り当ての詳細については、59 ページの「eDirectory での権利」を参照してください。



## Web ベースの管理ユーティリティ

Novell iManager はブラウザベースのツールで、eDirectory オブジェクトを運用、管理、設定するために使用します。iManager を使用すると、ユーザに特定のタスクや責任を割り当てたり、それらのタスクを実行するために必要なツールおよびそれに伴う権利だけを付与したりすることができます。

iManager を実行するには、Microsoft Internet Explorer 6.0 SP1 以降 (推奨)、Mozilla 1.7 以降、または Mozilla Firefox 0.9.2 を搭載したワークステーションが必要です。

**重要:** これら以外の Web ブラウザでも iManager にアクセスできる場合がありますが、完全な機能は保証されません。

iManager を使用すると、次のようなスーパーバイザの作業を実行できます。

- ◆ eDirectory への LDAP および XML ベースのアクセス設定
- ◆ ネットワークユーザ、デバイス、およびリソースを表すオブジェクトの作成
- ◆ 新規ユーザアカウント作成用のテンプレートの定義
- ◆ ネットワークオブジェクトの検索、変更、移動、および削除
- ◆ 管理権を委託する権利と職種の定義
- ◆ カスタムオブジェクトタイプとプロパティを作成するための eDirectory スキーマの拡張
- ◆ 複数のサーバでの eDirectory データベースのパーティション化とレプリカの作成
- ◆ DSRepair、DSMerge、バックアップおよび復元などの eDirectory 管理ユーティリティの実行

その他にも、iManager にロードされたプラグインに基づいた管理機能を実行できます。iManager 2.5 でインストールされるのは、次の eDirectory プラグインです。

- ◆ eDirectory Backup and Restore
- ◆ eDirectory Log Files
- ◆ eDirectory Merge
- ◆ eDirectory Repair
- ◆ eDirectory Service Manager
- ◆ eGuide コンテンツ
- ◆ iManager 基本コンテンツ
- ◆ インポート変換エクスポートウィザード
- ◆ インデックス管理
- ◆ iPrint
- ◆ LDAP
- ◆ ユニバーサルパスワードの強制
- ◆ 優先度同期
- ◆ 暗号化属性
- ◆ 暗号化レプリケーション
- ◆ NLS

- ◆ NMAS
- ◆ PKI/Certificate
- ◆ フィルタ処理済レプリカ環境設定ウィザード
- ◆ SNMP
- ◆ WANトラフィックマネージャ

iManager のインストール、設定、および実行についての詳細は、『[Novell iManager 2.5 管理ガイド](http://www.novell.com/documentation/imanager25/index.html)』(<http://www.novell.com/documentation/imanager25/index.html>) を参照してください。

## シングルログインと認証

eDirectory では、ユーザはグローバルディレクトリにログインするため、ユーザごとに複数のサーバやドメインを管理する必要はありません。また、ドメイン間の信頼関係や通過時の認証を管理する必要もありません。

ディレクトリのセキュリティ機能の 1 つは、ユーザの認証です。ユーザがログインするためには、あらかじめユーザオブジェクトがディレクトリ内に作成されている必要があります。ユーザオブジェクトには、名前やパスワードといった、特定のプロパティがあります。

ユーザがログインすると、eDirectory は入力されたパスワードとディレクトリに格納されているそのユーザのパスワードを照合し、一致した場合にアクセスを許可します。

## オブジェクトクラスとプロパティ

eDirectory オブジェクトの各タイプの定義を、オブジェクトクラスといいます。たとえば、「ユーザ」や「組織」は、オブジェクトクラスです。オブジェクトの各クラスには、それぞれ特定のプロパティがあります。たとえば、ユーザオブジェクトでは、名、姓、および他の多くのプロパティがあります。

スキーマでは、オブジェクトクラスとプロパティ、および包含ルール(どのコンテナにどのオブジェクトを保管するか)が定義されます。eDirectory にはベーススキーマが付属しています。このベーススキーマは、ユーザまたはユーザが使用するアプリケーションによる拡張が可能です。スキーマの詳細については、[42 ページの「スキーマ」](#)を参照してください。

コンテナオブジェクトは、他のオブジェクトを格納し、ツリーをさまざまな分岐に分割するために使用されます。一方、リーフオブジェクトはネットワークリソースを表します。












## オブジェクトのリスト







次の表に、eDirectory のオブジェクトクラスを示します。サービスを追加した場合は、表内のオブジェクトクラス以外のオブジェクトクラスが eDirectory 内に新たに作成されることがあります。

### eDirectory コンテナオブジェクトクラス

| iManager アイコン   | コンテナオブジェクト (略語) | 説明  |
|---|-----------------|---|
|    | ツリー             | ツリーの開始点を表します。詳細については、 <a href="#">25 ページの「ツリー」</a> を参照してください。   |
|    | カントリ (C)        | ネットワークが存在する国を表します。その下には、国内の他のディレクトリオブジェクトが編成されます。詳細については、 <a href="#">28 ページの「国」</a> を参照してください。   |
|    | ライセンスコンテナ (LC)  | NLS (Novell Licensing Services) 技術を使用して、ライセンス許可証をインストールした場合や課金許可証を作成した場合に自動的に作成されます。NLS 対応のアプリケーションをインストールすると、LC コンテナオブジェクトがツリーに追加され、ライセンス許可証リーフオブジェクトがそのコンテナに追加されます。 |
|   | 組織 (O)          | ディレクトリ内の他のオブジェクトの編成に使用されます。組織オブジェクトは、カントリオブジェクトの直下に配置されます(カントリオブジェクトを作成している場合)。詳細については、 <a href="#">26 ページの「組織」</a> を参照してください。  |
|  | 部門 (OU)         | ディレクトリ内の他のオブジェクトをさらに細かく編成するために使用されます。部門オブジェクトは、組織オブジェクトの直下に配置されます。詳細については、 <a href="#">27 ページの「部門」</a> を参照してください。   |
|  | ドメイン (DC)       | ディレクトリ内の他のオブジェクトをさらに細かく編成するために使用されます。ドメインオブジェクトは、Tree オブジェクトの下、または組織、部門、カントリ、および地域オブジェクトの下に作成されます。詳細については、 <a href="#">28 ページの「ドメイン」</a> を参照してください。                   |


## eDirectory リーフオブジェクトクラス

| iManager アイコン   | リーフオブジェクト | 説明  |
|---|-----------|---|
|    | AFP サーバ   | eDirectory ネットワーク内のノードとして機能する、AppleTalk* ファイリングプロトコルサーバを表します。通常、複数の Macintosh* コンピュータに対する NetWare ルータおよび AppleTalk サーバとしても機能します。                  |
|    | Alias     | ディレクトリ内にあるオブジェクトの実際の位置を指します。別名を使用することによって、ディレクトリ内のディレクトリオブジェクトを、実際の場所とは異なる場所に存在するように表示できます。詳細については、 <a href="#">36 ページの「Alias」</a> を参照してください。     |
|    | アプリケーション  | ネットワークアプリケーションを表します。アプリケーションオブジェクトによって、権利の割り当て、ログインスクリプトのカスタマイズ、およびアプリケーションの起動のような、管理作業を簡素化できます。  |
|    | コンピュータ    | ネットワーク内のコンピュータを表します。  |
|    | ディレクトリマップ | ファイルシステム内のディレクトリを表します。詳細については、 <a href="#">38 ページの「ディレクトリマップ」</a> を参照してください。  |
|  | Group     | ディレクトリ内のユーザオブジェクトのリストに名前を割り当てます。各ユーザに権利を割り当てる代わりに、グループに権利を割り当てることによって、グループ内の各ユーザに権利を与えることができます。詳細については、 <a href="#">32 ページの「Group」</a> を参照してください。 |
|  | ライセンス許可証  | プロダクトライセンス許可証をデータベースのオブジェクトとしてインストールするために、NLS 技術とともに使用されます。NLS 対応アプリケーションをインストールすると、ライセンス許可証オブジェクトがライセンスプロダクトコンテナに追加されます。                         |
|  | 職種        | 組織内での地位や職種を定義します。   |
|  | プリントキュー   | ネットワークのプリントキューを表します。  |
|  | プリントサーバ   | ネットワークのプリントサーバを表します。  |
|  | プリンタ      | ネットワークのプリンタを表します。   |

| iManager アイコン   | リーフオブジェクト | 説明   |
|---|-----------|--|
|  | プロファイル    | 共通のログインスクリプトコマンドを共有するユーザグループが使用するログインスクリプトを表します。これらのユーザは同じコンテナに属する必要はありません。詳細については、 <a href="#">39 ページの「プロファイル」</a> を参照してください。 |
|  | サーバ       | 任意のオペレーティングシステムが動作するサーバを表します。詳細については、 <a href="#">29 ページの「サーバ」</a> を参照してください。  |
|  | テンプレート    | 新しいユーザオブジェクトに適用する標準のユーザオブジェクトプロパティを表します。   |
|  | 不明        | iManager にカスタムアイコンが存在しないオブジェクトを表します。   |
|  | ユーザ       | ネットワークを使用する人を表します。詳細については、 <a href="#">30 ページの「ユーザ」</a> を参照してください。   |
|  | ボリューム     | ネットワーク上の物理的なボリュームを表します。詳細については、 <a href="#">29 ページの「ボリューム」</a> を参照してください。  |

## コンテナオブジェクトクラス

### ツリー

 ネットワーク内のサーバに eDirectory を初めてインストールすると、Tree コンテナ (以前の [Root] コンテナ) が作成されます。最上位のコンテナである Tree コンテナには、通常、組織オブジェクト、カントリオブジェクト、または別名オブジェクトが格納されます。

#### Tree が表す内容


Tree コンテナはツリーの最上部を表します。

#### 使用法

Tree は、包括的な権利の割り当てに使用します。Tree に対して行った権利の割り当ては、継承機能によって、ツリー内のすべてのオブジェクトに適用されます。[59 ページの「eDirectory での権利」](#)を参照してください。デフォルトで、トラステイ [Public] は Tree に対するブラウズ権を所有し、Admin は Tree に対するスーパーバイザ権を所有します。

#### 重要なプロパティ

Tree オブジェクトは名前プロパティを持っています。名前プロパティは、最初のサーバのインストール時に指定されたツリー名を表します。ツリー名は iManager の階層に表示されます。

 ネットワークのサーバに eDirectory をインストールすると、組織コンテナオブジェクトが作成されます。通常、組織コンテナは最上部の Tree コンテナの直下に作成され、コンテナ内には部門オブジェクトとリーフオブジェクトが格納されます。

デフォルトでは、最初の組織コンテナに、Admin という名のユーザオブジェクトが作成されます。

### 組織オブジェクトが表す内容

通常、組織オブジェクトは会社を表しますが、Tree の下に組織オブジェクトを追加作成することもできます。一般的に、組織オブジェクトの追加作成は、さまざまな地区で構成されるネットワークや、独立した複数の eDirectory ツリーがマージされているネットワークで行われます。

### 使用法

ツリーでの組織オブジェクトの運用方法は、ネットワークのサイズと構造により異なります。小規模のネットワークでは、1つの組織オブジェクトの下にすべてのリーフオブジェクトを配置します。

大規模なネットワークでは、組織オブジェクトの下に部門オブジェクトを作成します。これにより、リソースの検索と管理を容易化できます。たとえば、社内の各部署や事業部ごとに部門オブジェクトを作成できます。

複数のサイトがあるネットワークでは、組織オブジェクトの下に各サイトを表す部門オブジェクトを作成します。ディレクトリを分割するためのサーバ数が十分にあれば、このようにサイトの境界で論理的にパーティションを区切ることができます。

プリンタ、ボリューム、アプリケーションといった、社内全体で使用するリソースを共有しやすくするために、組織の直下に、対応するプリンタ、ボリューム、アプリケーションのオブジェクトを作成します。

### 重要なプロパティ

組織オブジェクトの最も有用なプロパティを次に示します。名前プロパティは必須です。すべてのプロパティの一覧を表示するには、iManager で組織オブジェクトを選択します。プロパティの各ページの説明を表示するには、[ヘルプ] をクリックします。

#### ◆ 名前


通常、名前プロパティは会社名と同じです。簡素化のために短くすることもできます。たとえば、会社名が Your Shoe Company の場合、YourCo とすることができます。

組織名は、その下に作成されるすべてのオブジェクトのコンテキストの一部として使用されます。

#### ◆ ログインスクリプト

ログインスクリプトプロパティには、組織の直下にあるユーザオブジェクトが実行するコマンドが格納されます。これらのコマンドは、ユーザのログイン時に実行されます。

## 部門

 部門 (OU) コンテナオブジェクトを作成することによって、ツリーを細分化できます。部門は、iManager で、組織、カントリ、または別の部門オブジェクトの下に作成されます。

部門には、ユーザオブジェクトやアプリケーションオブジェクトといった、他の部門やリーフオブジェクトを格納できます。

### 部門オブジェクトが表す内容

通常は、部門オブジェクトは1つの部署を表し、互いにアクセスする必要があるオブジェクトのセットを格納します。部門オブジェクトの主な格納内容として、ユーザのセット、およびユーザが使用するプリンタ、ボリューム、アプリケーションなどを挙げることができます。

部門オブジェクトの最上位レベルに配置された各部門は、WAN リンクごとに区切られたネットワークの各サイトを表します。

### 使用法

ツリーでの部門オブジェクトの運用方法は、ネットワークのサイズと構造により異なります。小規模のネットワークでは、部門オブジェクトを作成する必要がない場合もあります。

大規模なネットワークでは、組織オブジェクトの下に部門オブジェクトを作成します。これにより、リソースの検索と管理を容易化できます。たとえば、社内の各部署や事業部ごとに部門オブジェクトを作成できます。ユーザオブジェクトと、ユーザが頻繁に使用するリソースを一緒に部門オブジェクトに格納すると、管理が最も容易になります。

複数のサイトがあるネットワークでは、組織オブジェクトの下に各サイトを表わす部門オブジェクトを作成します。ディレクトリを分割するためのサーバ数が十分にあれば、このようにサイトの境界で論理的にパーティションを区切ることができます。

### 重要なプロパティ

部門オブジェクトの最も有用なプロパティを次に示します。名前プロパティは必須です。すべてのプロパティの一覧を表示するには、iManager で部門オブジェクトを選択します。プロパティの各ページの説明を表示するには、[ヘルプ] をクリックします。


#### ◆ 名前

通常、名前プロパティは部署名と同じです。簡素化のために短くすることもできます。たとえば、部署名が **Accounts Payable** の場合、省略して **AP** とすることができます。

部門名は、その下に作成されるすべてのオブジェクトのコンテキストの一部として使用されます。

#### ◆ ログインスクリプト

ログインスクリプトプロパティには、部門の直下にあるユーザオブジェクトが実行するコマンドが格納されます。これらのコマンドは、ユーザのログイン時に実行されます。

 国オブジェクトは、iManager を使用して、Tree オブジェクトの直下に作成できます。国オブジェクトは、特定の X.500 グローバルディレクトリに接続する場合にのみ必要です。

### 国オブジェクトが表す内容

国オブジェクトは、ツリーの分岐の国名を表します。

### 使用法


ネットワークが複数の国に渡っている場合でも、管理者は通常、国オブジェクトを作成しません。これは、国オブジェクトがツリーに不要なレベルを追加するだけだからです。ネットワークが複数の国家で構成されている場合は、必要に応じて、Tree オブジェクトの下に 1 つ以上の国オブジェクトを作成できます。国オブジェクトには、組織オブジェクトのみ格納できます。

国オブジェクトを作成していない場合でも、後で必要になった時には、随時ツリーを変更して国オブジェクトを追加できます。

### 重要なプロパティ

国オブジェクトには、2 文字の名前プロパティがあります。国オブジェクト名には、US、UK、または DE といった、2 文字の標準コードが使用されます。

## ドメイン

 ドメインオブジェクトは、iManager を使用して Tree オブジェクトの直下に作成できます。また、組織、部門、国、および地域オブジェクトの下にも作成できます。

### ドメインオブジェクトが表す内容

ドメインオブジェクトは、DNS のドメインコンポーネントを表します。ドメインオブジェクトを使用すると、ドメインネームシステムによって示されるサービスリソースレコードの場所 (DNS SRV) に基づいて、ツリー内のサービスを検索できます。

ドメインオブジェクトを使用すると、ツリーは次のように表されます。

DS=Novell.DC=Provo.DC=USA

この例では、すべてのサブコンテナがドメインになっています。次のように、異なるツリーが混在する場合にもドメインオブジェクトを使用できます。

DC=Novell.O=Provo.C=USA

または

OU=Novell.DC=Provo.C=USA

通常、先頭のドメインは Tree 全体を表し、サブドメインはその Tree の下位の部分を表します。たとえば `machine1.novell.com` をツリーで表すと、`DC=machine1.DC=novell.DC=com` となります。ドメインは、eDirectory ツリーの設定で使用される一般的な方法です。コンテナおよびサブコンテナがすべて DC オブジェクトである場合は、オブジェクトを検索するときに、C、O、または OU を意識する必要はありません。



## 使用法

NetWare 4 および 5 のツリーでは、ドメインオブジェクトをツリーの最上位にすることはできません。NetWare 4 および 5 では、NCP サーバオブジェクトを組織、国、部門、または地域コンテナに配置できます。ドメインコンテナには配置できません。ただし NetWare 6 では、ドメインオブジェクトをツリーの最上位にすることができます。また NCP サーバオブジェクトをドメインコンテナに配置できます。

NetWare の以前のインストール (4 など) を使用している場合、NetWare 5 以降のインストールやアップグレードに備えてツリーを設定するときに、nds500.sch ファイルが自動的に実行されます。最初のサーバをツリーにインストールすると、このファイルによりスキーマが拡張され、任意の場所にドメインコンテナを作成し、ほとんどのディレクトリオブジェクトを格納できます。

## リーフオブジェクトクラス

### サーバ



サーバに eDirectory をインストールすると、そのサーバに対応するサーバオブジェクトが、ツリー内に自動作成されます。このオブジェクトクラスは、eDirectory が動作しているいずれかのサーバを表します。

NetWare 2 または NetWare 3 バインダリサーバを表すサーバオブジェクトを作成することもできます。

### サーバオブジェクトが表す内容

サーバオブジェクトは、eDirectory が動作しているサーバ、またはバインダリベース (NetWare 2 または NetWare 3) のサーバを表します。

### 使用法

サーバオブジェクトはレプリケーション処理のリファレンスポイントの役目を果たします。バインダリベースのサーバを表すサーバオブジェクトでは、iManager でそのサーバのボリュームを管理できます。

### 重要なプロパティ

サーバオブジェクトの主なプロパティとして、ネットワークアドレスプロパティがあります。ネットワークアドレスプロパティには、そのサーバのポートとアドレス番号が表示されます。これはパケットレベルでのトラブルシューティングに役立ちます。

すべてのプロパティの一覧を表示するには、iManager でサーバオブジェクトを選択します。プロパティの各ページの説明を表示するには、[ヘルプ] をクリックします。

### ボリューム



サーバ上に物理ボリュームを作成すると、ツリー内にボリュームオブジェクトが自動作成されます。デフォルトでは、サーバ名にアンダースコアと物理ボリューム名を追加したものが、ボリュームオブジェクトの名前になります (「YOSERVER\_SYS」など)。

ボリュームオブジェクトは NetWare でのみ作成できます。Linux および UNIX ファイルシステムのパーティションは、ボリュームオブジェクトを使用して管理することはできません。

## ボリュームオブジェクトが表す内容

ボリュームオブジェクトは、サーバ上の物理ボリューム (書き込み可能ディスクや CD などの記憶媒体) を表します。eDirectory 内のボリュームオブジェクトには、そのボリューム内のファイルやディレクトリに関する情報は含まれませんが、iManager を使用すれば、それらの情報にアクセスできます。ファイルおよびディレクトリに関する情報は、ファイルシステム自体に保存されます。

## 使用法

iManager で [ボリューム] アイコンをクリックすると、そのボリュームにあるファイルやディレクトリを管理できます。iManager により、ボリュームの空きディスク容量、ディレクトリエントリ領域、および圧縮の統計に関する情報が提供されます。

ツリー内に、NetWare 2 や NetWare 3 ボリュームのボリュームオブジェクトを作成することもできます。

## 重要なプロパティ

必須の名前プロパティおよびホストサーバプロパティに加えて、ボリュームオブジェクトには他にも重要なプロパティがあります。

- ◆ 名前  
ツリー内のボリュームオブジェクトの名前です。デフォルトでは、この名前は物理ボリュームの名前に基づいて付けられますが、変更も可能です。
- ◆ ホストサーバ  
ボリュームが存在するサーバの名前です。
- ◆ バージョン  
ボリュームの格納先であるサーバの NetWare または eDirectory のバージョンです。

## ユーザ



ログインにはユーザオブジェクトが必要です。ツリーに最初のサーバが導入されると、Admin というユーザオブジェクトが作成されます。初回ログイン時には、Admin としてログインします。

ユーザオブジェクトの作成またはインポートには、次の機能を使用できます。

- ◆ iManager  
iManager の詳細については、『[Novell iManager 2.5 管理ガイド](http://www.novell.com/documentation/imanager25/index.html)』 (<http://www.novell.com/documentation/imanager25/index.html>) を参照してください。
- ◆ データベースファイルからのバッチ処理  
バッチファイルの使用の詳細については、[74 ページの「eDirectory ツリーの設計」](#) を参照してください。
- ◆ NetWare アップグレードユーティリティ  
既存のバインダリサーバからのユーザのインポートなど、アップグレードユーティリティの詳細については、[74 ページの「eDirectory ツリーの設計」](#) を参照してください。

## ユーザオブジェクトが表す内容

ユーザオブジェクトはネットワークを使用するユーザを表します。

## 使用法

ネットワークを使用するユーザ全員に対して、ユーザオブジェクトを作成します。ユーザオブジェクトは個別に管理することもできますが、次のようにすると時間の節約になります。

- ◆ テンプレートオブジェクトを使用して、通常のユーザオブジェクトのデフォルトのプロパティを設定する。新しく作成するユーザに対して、自動的にテンプレートが適用されます(既存のユーザには適用されません)。
- ◆ ユーザのセットを一括管理するためのグループオブジェクトを作成する。
- ◆ コンテナオブジェクトをトラスティとして使用して、権利を割り当てる。これにより、権利の割り当てをコンテナ内のユーザオブジェクトすべてに適用できます。
- ◆ 複数のユーザオブジェクトは、<Shift> または <Ctrl> を押してクリックすると選択できます。これにより、選択したすべてのユーザオブジェクトのプロパティ値を一度に変更できます。

## 重要なプロパティ

ユーザオブジェクトには 80 を超えるプロパティがあります。すべてのプロパティの一覧を表示するには、iManager でユーザオブジェクトを選択します。プロパティの各ページの説明を表示するには、[ヘルプ] をクリックします。

ログイン名プロパティと姓プロパティは必須です。これら必須のプロパティおよび、他の有用なプロパティを次に示します。

- ◆ [Account Expiration Date] では、ユーザアカウントの有効期限を設定できます。有効期限を過ぎた後は、アカウントはロックされ、ユーザはログインできなくなります。
- ◆ [アカウント使用不可] には、アカウントがロックされ、ユーザがログインできない状態であることを示すシステム生成の値があります。ロックは、アカウントの有効期限が切れた場合や、ユーザが不正なパスワードを連続して何度も入力した場合などに発生します。
- ◆ [定期的なパスワード強制変更] によって、一定期間ごとにパスワードの変更をユーザに要求し、セキュリティの強化を図ることができます。
- ◆ [グループメンバーシップ] は、ユーザがメンバーとして含まれているすべてのグループオブジェクトを示します。
- ◆ [ホームディレクトリ] は、NetWare ボリュームと、ユーザ自身のファイルまでのファイルシステムのパスを表します。多くの管理者がこのようなディレクトリを作成し、ユーザの作業ファイルがネットワーク上に維持されるようにします。  
このプロパティが表すディレクトリは、ユーザオブジェクトの作成時に自動作成することもできます。
- ◆ [最終ログイン時刻] はシステムが生成するプロパティで、ユーザが最後にログインした日時を示します。
- ◆ [姓] は必須ですが、eDirectory が直接使用することはありません。eDirectory ネームベースを利用するアプリケーションが、名、役職、位置、Fax 番号など、他の識別プロパティとともに、このプロパティを使用する場合があります。

- ◆ [同時接続数の制限] では、ユーザがネットワークで開くことができるセッションの最大数を設定できます。
- ◆ [ログイン名] は **iManager** で [ユーザ] アイコンによって表示される名前です。また、ログイン時にユーザが入力する名前でもあります。

**eDirectory** では、各コンテナ内で固有のログイン名を使用する必要がありますが、ネットワーク内の別のコンテナ間では同じログイン名を使用できます。ただし、社内全体で固有のログイン名を使用した方が、管理を単純化できます。


一般に、ログイン名には姓と名の組み合わせが使用されます。たとえば、**Steve Jones** の場合は、**STEVEJ** や **SJONES** のようになります。

- ◆ [ログインスクリプト] では、個々のユーザオブジェクトの特定のログインコマンドを作成できます。ユーザのログイン時には、最初にコンテナのログインスクリプトが実行されます。次に、ユーザオブジェクトがプロファイルオブジェクトのメンバーシップリストに登録されている場合は、プロファイルのログインスクリプトが実行されます。最後に、ユーザのログインスクリプトが実行されます (スクリプトが存在する場合)。

管理に要する時間を節約するため、ログインコマンドのほとんどの部分はコンテナのログインスクリプトに保管するようにします。ユーザログインスクリプトを編集すると、共通の必要条件に対する例外に対処できます。

- ◆ [ログイン時間制限] では、ユーザがログインできる時刻と曜日を設定できます。
- ◆ [ネットワークアドレス] には、ユーザのログイン元である **IPX™** アドレスや **IP** アドレスをすべて示したシステム生成の値が格納されます。これらの値は、パケットレベルでのネットワークの問題のトラブルシューティングに役立ちます。
- ◆ [パスワード要求] では、パスワードの入力をユーザに要求するかどうかを指定できます。他の関連プロパティでは、パスワード長などの一般的なパスワード制限を設定できます。
- ◆ [Rights to Files and Directories] は、ユーザに割り当てられた、**NetWare** ファイルシステムに対するすべての権利を示します。**iManager** を使用して、ファイルおよびディレクトリに対するユーザの有効な権利 (他のオブジェクトから継承されたものを含む) を確認することもできます。

## Group

 グループオブジェクトを作成すると、ユーザオブジェクトのセットを容易に管理できます。

### グループオブジェクトが表す内容

グループオブジェクトは、ユーザオブジェクトのセットを表します。

### 使用法

コンテナオブジェクトではコンテナ内のすべてのユーザオブジェクトを管理でき、グループオブジェクトでは1つまたは複数のコンテナ内のサブセットを管理できます。

グループオブジェクトは、次の2つの主な目的に対して使用されます。

- ◆ 多数のユーザオブジェクトに、一度に権利を与える。
- ◆ **IF MEMBER OF** 構文を使用して、ログインスクリプトコマンドを指定する。

## スタティックグループ

スタティックグループでは、メンバーオブジェクトを明示的に指定します。各メンバーは、グループに明示的に割り当てられます。

これらのグループでは固定したメンバーのリストが示され、また、グループのメンバーリストと、オブジェクト上で属性を持つメンバーとの間の参照整合性を提供しません。グループメンバーシップは、メンバーの属性によって明示的に管理されます。

## ダイナミックグループ

ダイナミックグループでは、LDAP URL を使用して規則のセットを定義します。この規則に従って、eDirectory のユーザオブジェクトに一致したときに、グループのメンバーが定義されます。ダイナミックグループのメンバーは、URL に指定された検索フィルタによって定義される共通の属性を共有します。LDAP URL の形式に関する詳細は、[RFC 2255 を参照してください \(http://www.cis.ohio-state.edu/cgi-bin/rfc/rfc2255.html\)](http://www.cis.ohio-state.edu/cgi-bin/rfc/rfc2255.html)。

ダイナミックグループを使用すると、グループのメンバーシップを評価する際に使用される条件を指定できます。グループの実際のメンバーは、eDirectory によって動的に評価されます。つまり、論理的にグループ化することでグループのメンバーを定義するため、eDirectory はグループのメンバーを自動的に追加または削除できます。この拡張性の高いソリューションによって、管理コストを低減でき、LDAP の通常のグループに高い柔軟性を補うことができます。

eDirectory を使用すると、任意の属性に基づいてユーザを自動的にグループ化する場合、または一致する DN を含むグループに対して ACL を適用する場合に、ダイナミックグループを作成できます。たとえば、部署 = マーケティングという属性を持つすべての DN を自動的に含むグループを作成できます。部署 = マーケティングという検索フィルタを適用すると、部署 = マーケティングの属性を持つすべての DN を含むグループが検索結果として返されます。その後、このフィルタに基づく検索結果からダイナミックグループを定義できます。部署 = マーケティングという条件に一致するユーザがディレクトリに追加されると、このグループにも自動的に追加されます。部署が他の値に変更されたユーザ (またはディレクトリから削除されたユーザ) は、グループから自動的に削除されます。

eDirectory でダイナミックグループを作成するには、`objectclass=dynamicGroup` というタイプのオブジェクトを作成します。スタティックグループオブジェクトをダイナミックグループに変換するには、補助クラス `dynamicGroupAux` をグループオブジェクトに関連付けます。ダイナミックグループは、グループに関連付けられた `memberQueryURL` 属性を持ちます。

`dgIdentity` 属性は、ダイナミックグループオブジェクト上で、グループのダイナミックメンバーを拡張するために使用される証明書と権利を持つエントリの識別名に設定することができます。

グループは、`memberQueryURL` を使用して管理されます。基本的な `memberQueryURL` には、ベース DN、スコープ、フィルタ、およびオプション拡張があります。ベース DN は検索ベースを指定します。スコープはベース内の検索レベルを指定します。フィルタは、指定したスコープ内で選択されたエントリに基づく検索フィルタです。

**注:** `memberQueryURL` によって作成されたリストに例外を設定するため、ダイナミックグループでもユーザを明示的に含めたり、除外したりできます。

ダイナミックグループは、Novell iManager を使用して作成および管理できます。ダイナミックグループ管理タスクには、[役割およびタスク] ページの [ダイナミックグループ] 役割をクリックしてアクセスできます。

また、LDAP コマンドを使用してもグループを管理できます。ダイナミックグループに関連付けられた最も有用なプロパティは、`dgIdentity` および `memberQueryURL` です。

## 重要なプロパティ

グループオブジェクトの最も有用なプロパティは、メンバープロパティとファイル/ディレクトリへの権利プロパティです。すべてのプロパティの一覧を表示するには、iManager でグループオブジェクトを選択します。プロパティの各ページの説明を表示するには、[ヘルプ] をクリックします。

- ◆ **dgAllowDuplicates**

ダイナミックグループメンバーの印刷で重複が許されるかどうかを指定します。デフォルトは「TRUE」です。

- ◆ **dgIdentity**

このプロパティは DN を保持します。ダイナミックグループは、この DN の識別子を検索時の認証用に使用します。識別子は、ダイナミックグループと同じパーティション上に存在する必要があります。dgIdentity によって指定されたオブジェクトは、memberQueryURL 属性で指定された検索を実行するのに必要な権利を持っている必要があります。

たとえば、memberQueryURL が次のような値であるとします。

```
"ldap:///o=nov??sub?(title=*)"
```

この場合、dgIdentity は、コンテナ o=nov 以下の属性タイトルの読み込み/比較権利を持っている必要があります。

- ◆ **dgTimeout**

このプロパティは、サーバがタイムアウトになるまでにかかるメンバーの属性の読み込みまたは比較の最大所要時間を指定します。サーバがこの dgTimeout 値を超えると、-6016 エラーが表示されます。

- ◆ **memberQueryURL**

このプロパティは、グループメンバーの属性と照合する規則のセットを定義します。

memberQueryURL は、そのスキーマ定義に従って複数の値を持つ属性です。

memberQueryURL は複数の値を持ちますが、eDirectory 8.6.1 では、memberQueryURL の最初の値のみが使用されていました。

例：

管理者によって作成されたダイナミックグループに、次のような 2 つの memberQueryURL 値があるとします。

```
"ldap:///o=nov??sub?cn=*"
"ldap:///o=org??sub?cn=*"
```

eDirectory 8.6.x サーバは、グループのメンバーの比較のために「ldap:///o=nov??sub?cn=\*」を使用します。複数のクエリが許可されますが、読み込まれるのは最初のクエリだけです。

この限界は、eDirectory 8.7.3 で克服されています。eDirectory 8.7.3 サーバは、すべての memberQueryURL 値に基づいてメンバーを計算するため、そのメンバーは個々の memberQueryURL 値を使用して計算されたメンバーを統合したものになります。

上の例では、結果としてダイナミックグループのメンバーは、o=org および o=nov の場合に cn 値を持つすべてのエントリとなります。

- ◆ member

このプロパティは、グループ内のすべてのオブジェクトを示します。グループオブジェクトに割り当てられた権利は、そのグループのすべてのメンバーに適用されます。ダイナミックグループの **member** プロパティに値を追加すると、ダイナミックグループにスタティックメンバーが追加されます。この方法は、個別にメンバーを追加する場合に使用できます。

- ◆ excludedMember

このプロパティは、ダイナミックグループのメンバーシップリストから特に除外された DN を格納します。これは、ダイナミックグループの除外リストを作成するのに使用できます。

**excludedMember** によって、DN をダイナミックグループのダイナミックメンバーから除外されるようにします。

こうすると、**memberQueryURL** によって指定されたメンバーの基準で選択された場合にのみ、DN はダイナミックグループのダイナミックメンバーになり、**excludedMember** としてリストされたり、**uniqueMember** や **member** に明示的に追加されたりすることはありません。

- ◆ staticMember

このプロパティは、ダイナミックグループのスタティックメンバーを読み込むだけでなく、DN がダイナミックグループのスタティックメンバーかどうかを判断します。また、DN が唯一のスタティックメンバーであるダイナミックグループを探し、ダイナミックメンバーを持っているが、スタティックメンバーを持たないグループを探すこともできます。

このプロパティを既存のダイナミックグループに追加するには、**dgstatic.sch** を使用するスキーマを拡張します。

## eDirectory 8.6.1 以前のデータベースのダイナミックグループを更新する

ダイナミックグループがローカルで作成されるか、同期の一部として取得されると、ダイナミックグループオブジェクトが作成されますが、ダイナミックグループの機能は、そのオブジェクトに格納されるいくつかの内部値を必要とします。

古いサーバでもダイナミックグループを格納できますが、値を生成することはできません。ダイナミックグループは eDirectory 8.6.1 で導入されたためです。

eDirectory 8.6.2 では、eDirectory 8.6.1 データベースに適合させるために、8.6.1 以前のデータベースのダイナミックグループオブジェクトが自動で更新されました。

## memberQueryURL の追加構文のサポート

**memberQueryURL** 属性は、ダイナミックグループのメンバーを計算するために eDirectory サーバが使用する検索フィルタを格納できます。

eDirectory 8.6.1 では、フィルタで使用される属性の構文は、次の基本的な文字列型にのみ制限されていました。

- ◆ SYN\_CE\_STRING
- ◆ SYN\_CI\_STRING
- ◆ SYN\_PR\_STRING
- ◆ SYN\_NU\_STRING
- ◆ SYN\_CLASS\_NAME

- ◆ SYN\_TEL\_NUMBER
- ◆ SYN\_INTEGER
- ◆ SYN\_COUNTER
- ◆ SYN\_TIME
- ◆ SYN\_INTERVAL
- ◆ SYN\_BOOLEAN
- ◆ SYN\_DIST\_NAME
- ◆ SYN\_PO\_ADDRESS
- ◆ SYN\_CI\_LIST
- ◆ SYN\_FAX\_NUMBER
- ◆ SYN\_EMAIL\_ADDRESS


eDirectory 8.7.3 以降では、次の属性構文が `memberQueryURL` の値として追加でサポートされています。

- ◆ SYN\_PATH
- ◆ SYN\_TIMESTAMP
- ◆ SYN\_TYPED\_NAME

eDirectory 8.6.1 および eDirectory 8.7.x の両方では、`SYN_OCTET_STRING` や `SYN_NET_ADDRESS` のようなバイナリ構文は、`memberQueryURL` 検索フィルタでサポートされません。

詳細については、[How to Manage and Use Dynamic Groups in Novell eDirectory](http://developer.novell.com/research/appnotes/2002/april/05/a020405.htm) (<http://developer.novell.com/research/appnotes/2002/april/05/a020405.htm>) を参照してください。

## Alias

 ツリー内の別のオブジェクトをポイントする別名オブジェクトを作成できます。別名オブジェクトによって、ユーザは自分の属するコンテナの外部にあるオブジェクトに、ローカル名を付けることができます。

コンテナの名前を変更するときには、必要に応じて、元のコンテナの位置に新しい名前をポイントする別名を作成できます。これにより、コンテナ内のオブジェクトを参照するログインスクリプトコマンドやワークステーションは、コンテナ名が更新されていなくても対象のオブジェクトにアクセスできます。

### 別名オブジェクトが表す内容

別名オブジェクトは、コンテナやユーザなど、ツリー内の別のオブジェクトを表します。別名オブジェクト自体にはトラスティ権はありません。別名オブジェクトに与えられたトラスティ権は、その別名オブジェクトが示している実際のオブジェクトに適用されます。ただし、別名をトラスティ割り当ての対象とすることもできます。

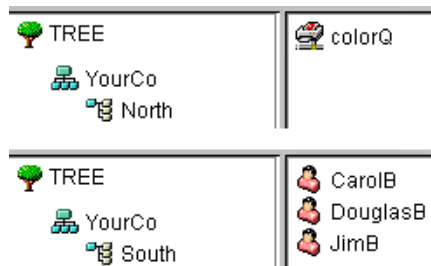


## 使用法

別名オブジェクトを作成すると、名前の解決が容易になります。オブジェクトの命名規則では、現在のコンテキストのオブジェクトに対する命名が最も簡単のため、現在のコンテキストに、現在のコンテキストの外部のリソースをポイントする別名オブジェクトを作成します。

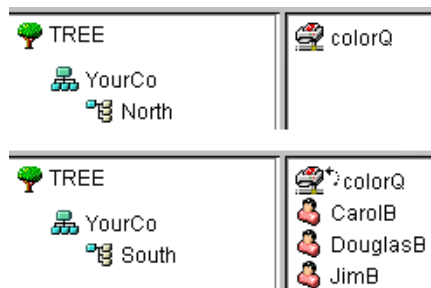
たとえば、[図 5](#) に示すように、ユーザが South コンテナにログインし、現在のコンテキストを確立する場合に、North コンテナの ColorQ というプリントキューオブジェクトにアクセスする必要があるとします。

**図 5** コンテナの例



[図 6](#) に示されるように、South コンテナに別名オブジェクトを作成できます。

**図 6** eDirectory コンテナの別名オブジェクト




別名オブジェクトによって、元の ColorQ オブジェクトがポイントされるため、South コンテナでは ColorQ をローカルオブジェクトとして印刷設定できます。

## 重要なプロパティ

別名オブジェクトには別名元オブジェクトプロパティがあり、このプロパティによって、別名オブジェクトと元のオブジェクトとが関連付けられます。

## ディレクトリマップ

 ディレクトリマップオブジェクトは、サーバのファイルシステム内のパスへのポインタです。これにより、ディレクトリをより簡単に参照できます。

ネットワークに NetWare ボリュームがない場合は、ディレクトリマップオブジェクトを作成することはできません。

### ディレクトリマップオブジェクトが表す内容

ディレクトリマップオブジェクトは、NetWare ボリューム上のディレクトリを表します (それに対し、別名オブジェクトはオブジェクトを表します)。

### 使用法

ディレクトリマップオブジェクトは、ログインスクリプトでのドライブマッピングを単純化するために作成します。ディレクトリマップオブジェクトを使用すると、複雑なファイルシステムパスを簡単な名前にすることができます。


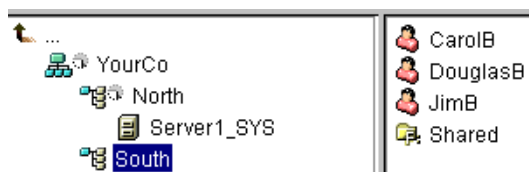
また、ファイルの場所を変更した場合でも、新しい場所を参照するように、ログインスクリプトやバッチファイルを変更する必要がありません。ディレクトリマップオブジェクトを編集するだけです。たとえば、 7 に示すように、South コンテナのログインスクリプトを編集するとします。

図 7 eDirectory コンテナの例



ドライブをボリューム sys: 上の Shared ディレクトリにマッピングするコマンドは、次のようになります。

```
MAP N:=sys.North.:Shared
```

共有ディレクトリマップオブジェクトを作成した場合、マップコマンドは、次のようにさらに簡単になります。

```
MAP N:=Shared
```

### 重要なプロパティ

ディレクトリマップオブジェクトには、次のようなプロパティがあります。

- ◆ 名前

ディレクトリ内のオブジェクト (たとえば、Shared) を指定します。名前プロパティは MAP コマンドで使用されます。


- ◆ ボリューム

Sys.North.YourCo のような、ディレクトリマップオブジェクトが参照するボリュームオブジェクトの名前が格納されます。

- ◆ パス

public¥winnt¥nls¥english のように、ディレクトリをボリュームのルートからのパスとして指定します。

## プロファイル

 プロファイルオブジェクトはログインスクリプトの管理に役立ちます。

### プロファイルオブジェクトが表示内容

プロファイルオブジェクトは、コンテナログインスクリプトの後、およびユーザログインスクリプトの前に実行されるログインスクリプトを表します。

### 使用法

特定のユーザのみを対象にログインスクリプトコマンドを実行したい場合は、プロファイルオブジェクトを作成します。対象のユーザには、同一コンテナ内のユーザだけでなく、異なるコンテナ内のユーザも指定できます。プロファイルオブジェクトを作成した後は、プロファイルのログインスクリプトプロパティにコマンドを指定します。続いて、該当のユーザオブジェクトをプロファイルオブジェクトのトラスティに指定し、それらのユーザオブジェクトのプロファイルメンバーシッププロパティにそのプロファイルオブジェクトを追加します。

### 重要なプロパティ

プロファイルオブジェクトには、次の2つの重要なプロパティがあります。

- ◆ ログインスクリプト

そのプロファイルのユーザに対して実行するコマンドを格納します。

- ◆ ファイル/ディレクトリへの権利

ログインスクリプトに INCLUDE ステートメントを使用した場合は、プロファイルオブジェクトに、ファイル/ディレクトリへの権利プロパティに指定されているファイルに対する権利を与える必要があります。

## コンテキストと命名規則

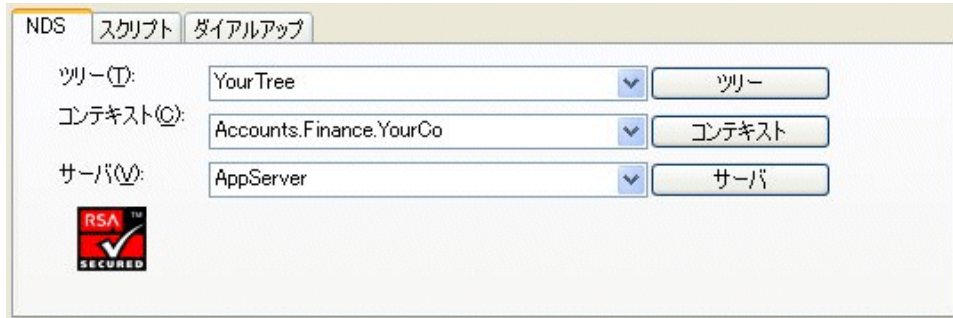
オブジェクトのコンテキストは、ツリー内でのそのオブジェクトの位置を表します。コンテキストは、NDS ドメインとほぼ同じです。

次の図は、ユーザ Bob は部門 Accounts にあり、部門 Accounts は部門 Finance にあり、部門 Finance は組織 YourCo にあることを示しています。

図 8 eDirectory コンテナの例



ただし、オブジェクトのコンテキストを eDirectory ユーティリティで表現する必要がある場合もあります。たとえば、40 ページの図 9 に示すように、Bob のワークステーションを設定するときには、名前のコンテキストを指定する必要があります。



コンテキストは、対象のオブジェクトと Tree の最上部との間に存在する各コンテナをピリオドで区切ったリストとして指定します。この例では、ユーザオブジェクト **Bob** はコンテナ **Accounts** にあり、コンテナ **Accounts** はコンテナ **Finance** にあり、コンテナ **Finance** はコンテナ **YourCo** にあります。

## 識別名

オブジェクトの識別名とは、オブジェクト名にコンテキストを付けたものです。たとえば、ユーザオブジェクト **Bob** の識別名は、**Bob.Accounts.Finance>YourCo** です。

## タイプ付きの名前

タイプ付きの名前が、eDirectory ユーティリティに表示されることがあります。タイプ付きの名前には、次の表に示されたようなオブジェクトタイプの略語があります。

| オブジェクトクラス        | タイプ       | 略語      |
|------------------|-----------|---------|
| すべてのリーフオブジェクトクラス | 共通名       | CN      |
| 組織               | 組織        | O       |
| 部門               | 部門        | OU      |
| 国                | 国         | C       |
| 地域               | 地域または都道府県 | L または S |

eDirectory では、タイプ付きの名前の作成に、タイプの略語、等号、およびオブジェクト名を使用します。たとえば、**Bob** のタイプ付きの名前は、**CN=Bob** となります。**Bob** のタイプ付きの完全な名前は、**CN=Bob.OU=Accounts.OU=Finance.O=YourCo** となります。eDirectory ユーティリティにおいて、タイプ付きの名前は、タイプなしの名前と互換性があります。

## ネームレゾリューション

ディレクトリツリー内のオブジェクトの位置を見つけるために eDirectory が使用するプロセスのことを、**ネームレゾリューション**(名前解決)といいます。eDirectory ユーティリティでオブジェクト名を使用すると、eDirectory は、現在のコンテキストまたはツリーの最上部を基準として名前の解決を行います。

## 現在のワークステーションのコンテキスト

ネットワークソフトウェアの実行時には、ワークステーションにはコンテキストが設定されます。このコンテキストによって、ネットワーク内のワークステーションの位置が相対的に指定されます。たとえば、Bob のワークステーションでは、現在のコンテキストが次のように設定されます。

Accounts.Finance.YourCo

次のセクションで説明するように、現在のコンテキストは、先頭のピリオド、相対命名、および後続ピリオドの使用法を理解するうえで重要です。

## 先頭ピリオド

現在のコンテキストがどこに設定されているかに関わりなく、ツリーの最上部から名前を解決するには、先頭ピリオドを使用します。次の例では、先頭ピリオドが CX (コンテキストの変更) ユーティリティに、ツリーの最上部を基準として名前を解決するよう指定しています。

CX .Finance.YourCo

eDirectory はこのコマンドを、「ツリーの最上部から名前を解決を行い、YourCo コンテナにある Finance コンテナにコンテキストを変更する」と解釈します。

## 相対命名

相対命名とは、ツリーの最上部ではなく、ワークステーションの現在のコンテキストを基準に、名前を解決することを意味します。先頭ピリオドはツリーの最上部からの名前解決を表すため、相対命名の場合は先頭ピリオドを使用しません。

たとえば、ワークステーションの現在のコンテキストが Finance に設定されているとします。( 図 10 を参照してください。)

図 10 eDirectory コンテナの例



Bob の相対オブジェクト名は、次のようになります。

Bob.Accounts

eDirectory は、この名前を「現在のコンテキスト Finance から解決される Accounts に属する Bob」と解釈します。

## 後続ピリオド

後続ピリオドは、相対命名でのみ使用されます。したがって、先頭ピリオドと後続ピリオドの両方を使用することはできません。後続ピリオドは、eDirectory が名前解決を開始するコンテナを変更します。

後続ピリオド 1 つにつき、解決地点がツリーの上に向かって 1 コンテナずつ引き上げられます。たとえば、42 ページの 図 11 の例は、ワークステーションの現在のコンテキストを Timmins から Allentown に変更する場合を示しています。

図 11 eDirectory コンテナの例



この場合の適切な CX コマンドでは、次に示すように、後続ピリオドを付けた相対命名を使用します。

```
CX Allentown.East..
```

eDirectory はこのコマンドを、「現在のコンテキストの 2 つ上にあるコンテナから名前前の解決を行い、East にある Allentown にコンテキストを変更する」と解釈します。

同様に、Bob が Allentown コンテナに属し、ワークステーションの現在のコンテキストが Timmins の場合、Bob の相対名は次のようになります。

```
Bob.Allentown.East..
```

## Linux および UNIX でのコンテキストと命名規則

Linux および UNIX のユーザアカウントを eDirectory に移行した場合、ユーザの命名に eDirectory のコンテキストは使用されません。

## スキーマ

スキーマでは、ツリー内に作成できるオブジェクトのタイプ (ユーザ、プリンタ、グループなど)、およびオブジェクトの作成時に指定する必須情報とオプション情報が定義されます。各オブジェクトには、そのオブジェクトタイプのスキーマクラスが定義されています。

製品に元から付属しているスキーマは、ベーススキーマといいます。新しいクラスや属性の追加など、なんらかの形でベーススキーマが変更されると、そのスキーマは拡張スキーマとみなされます。

スキーマは必ずしも拡張する必要はありませんが、拡張も可能です。iManager のスキーマ役割を使用すれば、運用条件に合わせてスキーマを拡張できます。たとえば、従業員に特殊な履き物が必要で、従業員の靴のサイズを記録しなければならない場合などに、スキーマを拡張します。この場合は、「靴のサイズ」という属性を新たに作成し、ユーザクラスに追加します。

詳細については、123 ページの第 4 章「スキーマの管理」を参照してください。

## スキーマ管理

Novell iManager のスキーマ役割によって、ツリーへのスーパーバイザ権を持っているユーザは、そのツリーのスキーマをカスタマイズできます。スキーマ役割、およびその関連タスクは、iManager の役割およびタスクページに表示されています。

スキーマ役割の使用目的

- ◆ スキーマ内のすべてのクラスおよび属性の一覧を表示する。
- ◆ 構文やフラグなどの属性についての情報を表示する。
- ◆ 既存のスキーマにクラスまたは属性を追加して、スキーマを拡張する。
- ◆ 名前を付けてから、属性、フラグ、追加できるコンテナ、および属性の継承元のペアレントクラスを指定して、クラスを作成する。
- ◆ 名前を付けてから、構文およびフラグを設定して、属性を作成する。
- ◆ 既存のクラスにオプションの属性を追加する。
- ◆ 使用されていない、または必要のなくなったクラスや属性を削除する。

## スキーマクラス、属性、および構文

### クラス

クラスとは、ディレクトリオブジェクトのテンプレートのようなものです。ディレクトリオブジェクトとは、データを挿入されたクラスです。つまり、次のように表すことができます。

CLASS + DATA = DIRECTORY OBJECT

各クラスは、クラス名、継承クラス (そのクラスがクラス階層の最上位である場合を除く)、クラスフラグ、および属性のグループを持っています。クラスは、ディレクトリオブジェクト (ユーザ、プリンタ、キュー、サーバなど) と同じように命名されますが、単なる構造であり内容はありません。

継承クラスとは、他のオブジェクトクラスを定義するときの開始点となるクラスです。継承クラスの属性はすべて、クラス階層でそのクラスの下位に位置するクラスへ継承されます。

クラス階層は、あるクラスがどのようにペアレントクラスと関連付けられているかを示します。クラス階層により、類似したクラスが関連付けられ、属性の継承が可能になります。また、クラスを格納できる有効なコンテナのタイプも定義されます。

クラスの作成時には、クラス階層と追加属性を使用して各クラスをカスタマイズできます。継承クラスを指定することによって、階層内の上位のクラスからその属性とフラグのすべてを新しいクラスに継承できます。さらに、継承された属性クラスに追加する属性を1つまたは複数選択することによって、新しいクラスをカスタマイズできます。追加の属性は、必須属性、ネーミング属性、またはオプション属性として選択できます。

オプションの属性を追加して、既存のクラスを変更することもできます。

## 属性

属性とは、eDirectory データベース内のデータフィールドのことです。たとえば、クラスが記入用紙のようなものだとなれば、属性は記入用紙における 1 つの記入欄です。属性は、作成時に、名前 ( 姓や社員番号など ) を付けられ、構文のタイプ ( 文字列や数字など ) が指定されます。その後、その属性はスキーママネージャの属性リストで使用できるようになります。

## 構文

構文にはいくつかの選択可能なオプションがあります。これらの構文オプションは、各属性で入力するデータのタイプを指定するために使用されます。構文は属性の作成時にのみ指定できます。後から構文を変更することはできません。利用可能な構文は次のようなものです。

- ◆ バックリンク

オブジェクトを参照する他のサーバの追跡に使用されます。また、eDirectory の内部管理目的で使用されます。

- ◆ ブール

TRUE(1) または FALSE(0) の値をとる属性に使用されます。この構文タイプには、単一の値のフラグが設定されます。

- ◆ 大文字小文字を区別する文字列

比較演算で大文字 / 小文字が区別される Unicode 文字列を値としてとる属性に使用されます。2 つの「大文字小文字を区別する文字列」は、長さが等しく、対応する文字 ( 大文字 / 小文字の区別を含む ) が同一の場合に一致とみなされます。

- ◆ 大文字小文字を無視するリスト

比較演算で大文字 / 小文字が区別されない Unicode 文字列の順序列を値としてとる属性に使用されます。2 つの「大文字小文字を無視するリスト」は、文字列の数が等しく、対応するすべての文字列が同じ場合 ( つまり、長さに対応する文字が同一の場合 ) に一致とみなされます。

- ◆ 大文字小文字を無視する文字列

比較演算で大文字 / 小文字が区別されない Unicode 文字列を値としてとる属性に使用されます。2 つの「大文字小文字を無視する文字列」は、長さが等しく、対応する文字があらゆる面で ( ただし、大文字 / 小文字の区別を除く ) 同一の場合に一致とみなされます。

- ◆ クラス名

オブジェクトクラスの名前を値としてとる属性に使用されます。2 つのクラス名は、長さが等しく、対応する文字があらゆる面で ( ただし、大文字 / 小文字の区別を除く ) 同一の場合に一致とみなされます。

- ◆ カウンタ

増分変更された符号付き整数を値としてとる属性に使用されます。カウンタによって定義された属性は、単一の値の属性です。カウンタは、この構文の属性に値が追加されると足し算で合計に追加され、この構文の属性から値が削除されると引き算で合計から差し引かれるという点で、整数とは異なります。



- ◆ 識別名
 

eDirectory ツリー内のオブジェクト名を値としてとる属性に使用されます。DN ( 識別名 ) では大文字 / 小文字が区別されませんが、ネーミング属性の 1 つでは大文字 / 小文字が区別されます。
- ◆ 電子メールアドレス
 

バイナリ情報の文字列を値としてとる属性によって使用されます。eDirectory は、この構文の内容の内部構造については想定しません。
- ◆ Fax 番号
 

国際電話番号と、推奨 T.20 に従って形式設定されたオプションのビット文字列の格納を規定する E.123 標準に準拠した文字列を指定します。2 つの Fax 番号値は、長さが等しく、対応する文字列が同一 ( ただし、比較処理で無視されるスペースとハイフンを除く ) の場合に、一致とみなされます。
- ◆ 保持
 

符号付き整数の値を持つアカウント数量の属性に使用されます。この構文は、アカウント数量 ( トランザクションが完了するまでの間、サブジェクトのクレジット限度に対して暫定的に保持される金額 ) を表します。保持量は、カウンタ構文と同じように扱われ、新しい値がベース合計に加算されるか、ベース合計から減算されます。計算された保持量が 0 になると、保持レコードは削除されます。
- ◆ 整数
 

符号付き数値として表される属性に使用されます。2 つの整数値は、値が同一である場合に一致とみなされます。順序付けの比較では、符号付き整数ルールが使用されます。
- ◆ 間隔
 

符号付き整数を値としてとり、時間の間隔を表す属性に使用されます。間隔構文では、整数構文と同じ表現が使用されます。間隔値は、時間間隔での秒数を表します。
- ◆ ネットアドレス
 

サーバ環境でのネットワークレイヤアドレスを表します。このアドレスは、バイナリ形式です。2 つのネットアドレスは、各アドレスのタイプ、長さ、および値が一致する場合に、一致とみなされます。
- ◆ 数値文字列
 

CCITT X.208 定義で数値文字列として定義されている数値整数を値としてとる属性に使用されます。2 つの数値文字列は、長さが等しく、対応する文字が同一の場合に一致とみなされます。数値文字列文字セットにおいて有効な文字は、数字 ( 0 ~ 9 ) およびスペースのみです。
- ◆ オブジェクト ACL
 

アクセス制御リスト ( ACL ) エントリを表す値をとる属性に使用されます。オブジェクト ACL 値は、オブジェクトを保護する場合と、属性を保護場合があります。
- ◆ オクテットリスト
 

バイナリ情報またはオクテット文字列の順序付き文字列シーケンスを表します。オクテットリストは、保存済みリストのサブセットである場合に、保存済みリストと一致するとみなされます。2 つのオクテットリストは、長さが等しく、対応するビット列 ( オクテット ) が同一の場合に一致とみなされます。

- ◆ オクテット文字列

eDirectory によって解釈されないバイナリ情報の文字列を値としてとる属性に使用されます。これらのオクテット文字列は、非 Unicode 文字列です。2つのオクテット文字列は、長さが等しく、対応するビット列(オクテット)が同一の場合に一致とみなされます。

- ◆ パス

ファイルシステムパスを表す属性であり、サーバ上でファイルを見つけるために必要なすべての情報が格納されます。2つのパスは、長さが等しく、対応する文字(大文字/小文字の区別を含む)が同一の場合に、一致とみなされます。

- ◆ 住所

住所を表す Unicode 文字列を値としてとる属性に使用されます。通常、住所の属性値は、推奨 F.401 に従って MHS Unformatted Postal O/R Address Specification バージョン 1 から選択された属性で構成されます。この値は、30 文字 6 行(国名を含む)に制限されます。2つの住所は、文字列の数が等しく、対応するすべての文字列が同じ場合(つまり、長さに対応する文字が同一の場合)に一致とみなされます。

- ◆ 印刷可能文字列

CCITT X.208 に定義されている印刷可能文字列を値としてとる属性に使用されます。印刷可能文字セットは、次のものから構成されます。

- ◆ 英大文字および英小文字
- ◆ 数字 (0 ~ 9)
- ◆ スペース
- ◆ アポストロフィ (')
- ◆ 左カッコおよび右カッコ ( )
- ◆ プラス記号 (+)
- ◆ コンマ (,)
- ◆ ハイフン (-)
- ◆ ピリオド (.)
- ◆ スラッシュ (/)
- ◆ コロン (:)
- ◆ 等号 (=)
- ◆ 疑問符 (?)

2つの印刷可能文字列は長さが等しく、対応する文字が同一の場合に一致とみなされます。大文字/小文字は区別されます。

- ◆ レプリカポインタ

パーティションレプリカを表す値をとる属性に使用されます。eDirectory ツリーのパーティションでは、複数のサーバにレプリカを置くことができます。この構文は、次の 6 つのコンポーネントで構成されます。

- ◆ サーバ名
- ◆ レプリカタイプ ( マスタ、セカンダリ、読み込み専用、サブオーディネートリファレンス )
- ◆ レプリカ番号
- ◆ レプリカルート ID
- ◆ アドレスの数
- ◆ アドレスレコード

- ◆ ストリーム

任意のバイナリ情報を表します。ストリーム構文を使用すると、ファイルサーバ上のファイルから eDirectory 属性を作成できます。この構文は、ログインスクリプトやその他のストリーム属性で使用されます。ストリームファイルに格納されているデータには、構文は一切適用されません。この構文は単に任意のデータであり、個別のアプリケーションで作成、定義および使用されます。

- ◆ 電話番号

電話番号を値としてとる属性に使用されます。電話番号は、1 ~ 32 文字の長さの文字列です。2 つの電話番号は、長さが等しく、対応する文字列が同一 ( ただし、比較処理で無視されるスペースとハイフンを除く ) の場合に、一致とみなされます。

- ◆ 時間

符号なし整数を値としてとり、秒単位の時間を表す属性に使用されます。

- ◆ タイムスタンプ

特定のイベントが発生した時刻を示す値をとる属性に使用されます。特定のイベントが発生すると、eDirectory サーバによってタイムスタンプ値が生成され、そのイベントに関連付けられます。各タイムスタンプ値は、eDirectory パーティション内で固有です。これにより、同一パーティションのレプリカを保持しているすべてのサーバで発生したイベントを 1 つにまとめて順序付けできます。

- ◆ タイプ付きの名前

オブジェクトに関連付けられたレベルおよび間隔を表す値をとる属性に使用されます。この構文は、eDirectory オブジェクトを指定し、次の 2 つの数値を当該オブジェクトにアタッチします。

- ◆ 優先番号を示す属性レベル
- ◆ イベント間の秒数、または参照の頻度を表す間隔

- ◆ 不明

スキーマから削除されている属性定義をもつ属性に使用されます。この構文は、バイナリ情報の文字列を表します。

## 必須属性およびオプション属性について

オブジェクトにはどれも、オブジェクトのタイプに合わせて定義されたスキーマクラスがあります。クラスとは、意味のある方法で組織された属性のグループを指します。これらの属性の一部は必須で、一部はオプションです。

### 必須属性

必須属性とは、オブジェクトの作成時に指定する必要がある属性です。たとえば、社員番号が必須属性であるユーザクラスで新しいユーザを作成する場合、社員番号を入力せずに新しいユーザオブジェクトを作成することはできません。

### オプション属性

オプション属性とは、必要に応じて指定できる属性を指します。たとえば、ニックネームがオプション属性となっているユーザクラスで新しいユーザオブジェクトを作成するとします。この場合、この属性が入力されてもされなくてもユーザオブジェクトは作成できます。属性を入力するかどうかは、新しいユーザにニックネームが付いているかどうかによって左右されます。

例外的にオプション属性が命名に使用される場合がありますが、その場合は属性が必須になります。

## スキーマのサンプル

48 ページの [図 12](#) は、スキーマの一部の例で、基本のスキーマに類似しているかもしれませんが、この図は、組織クラスについての情報を表しています。この画面に表示されているほとんどの情報は、クラスが作成されたときに指定されたものです。オプションの属性のいくつかは後に追加されました。





 このアイコンは、ベーススキーマの拡張部分であるすべてのクラスおよび属性に割り当てられます。

図 12 iManager のクラス情報ページ






クラスフラグ:

|         |                             |
|---------|-----------------------------|
| コンテナクラス | <a href="#">新しい属性を追加します</a> |
| 有効なクラス  | <a href="#">上位クラスの表示</a>    |
| 非リムーバブル |                             |

クラスを格納できるコンテナ:

|   |  |
|---|--|
|  [Nothing] |  |
|  Country   |  |
|  domain    |  |

属性:

|   |                          |                          |
|---|--------------------------|--------------------------|
|  <a href="#">teletexTerminalIdentifier</a> | <input type="checkbox"/> | <input type="checkbox"/> |
|  <a href="#">telexNumber</a>               | <input type="checkbox"/> | <input type="checkbox"/> |
|  <a href="#">x121Address</a>               | <input type="checkbox"/> | <input type="checkbox"/> |
|  <a href="#">Account Balance</a>           | <input type="checkbox"/> | <input type="checkbox"/> |
|  <a href="#">Allow Unlimited Credit</a>    | <input type="checkbox"/> | <input type="checkbox"/> |

ASN1 ID:  
2.5.6.4

閉じる

## スキーマを設計する

最初にスキーマの設計を行うと、長期的に見た場合、時間と労力を節約できます。ベーススキーマを表示して、それが実際の必要条件に見合うか、あるいは変更が必要かを判断できます。変更が必要な場合は、スキーママネージャを使用してスキーマを拡張します。詳細については、[124 ページの「スキーマの拡張」](#) および [128 ページの「スキーマの表示」](#) を参照してください。

## パーティション

パーティションは、eDirectory データベースの論理区分です。各ディレクトリパーティションは、ディレクトリ情報を格納するツリー内の個別のデータユニットとなります。

パーティションを分割すると、ディレクトリの一部を 1 つのサーバから切り離し、別のサーバに置くことができます。

WAN リンクが遅い場合や信頼性に乏しい場合、またはディレクトリに多量のオブジェクトがあるためにサーバが処理しきれず、アクセスが遅くなる場合は、ディレクトリをパーティション分割することを検討してください。パーティションの詳細な説明については、[135 ページの第 5 章「パーティションおよびレプリカの管理」](#) を参照してください。

各ディレクトリパーティションは、コンテナオブジェクト、それに含まれるすべてのオブジェクト、およびそれらのオブジェクトに関するデータのセットから構成されます。パーティションには、ファイルシステムに関する情報、またはパーティションに含まれるディレクトリやファイルに関する情報はありません。

パーティション分割は、Novell iManager を使用して行います。iManager では、パーティションは、[パーティション] アイコン (🗄️) によって識別されます。

図 13 サーバのレプリカビュー



この上の例では、[パーティション] アイコンは Tree オブジェクトの横にあります。この場合は、Tree オブジェクトが、パーティション内の最上位のコンテナであることを意味します。他のコンテナではパーティションが表示されていないため、このパーティションが唯一のパーティションになります。

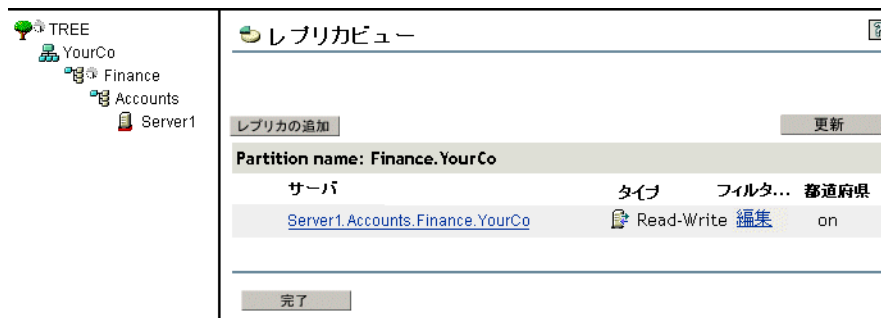
これはデフォルトの eDirectory パーティションで、ディレクトリ全体を 1 つのパーティションにまとめています。

この例では、Server1 のレプリカビューが表示されていることに注意してください。iManager でサーバのレプリカビューを表示すると、そのサーバに保持されているすべてのレプリカが右に表示されます。この場合、Server1 には唯一のパーティションのレプリカが保持されています。詳細については、[52 ページの「レプリカ」](#) および [144 ページの「eDirectory サーバのレプリカを表示する」](#) を参照してください。

## パーティション

パーティションには、その最上位のコンテナの名前が付けられます。図 14 では、Tree および Finance という名前の 2 つのパーティションがあります。パーティション Finance は Tree から分割されたため、このパーティションは Tree のチャイルドパーティションと呼ばれます。また Tree は、Finance のペアレントパーティションと呼ばれます。

図 14 パーティションのレプリカビュー



ディレクトリに大量のオブジェクトがあるためにサーバが処理しきれず、eDirectory へのアクセスが遅くなる場合、このように新しいパーティションを作成すると便利です。新しいパーティションを作成すると、データベースを分割し、その分岐のオブジェクトを異なるサーバに渡すことができます。

上の例では、Finance パーティションのレプリカビューが表示されています。iManager でパーティションのレプリカビューを表示すると、そのパーティションのレプリカを持つサーバはすべて右側に表示されます。この場合、Server1 には、Finance パーティションの読み書き可能レプリカが保持されています。詳細については、146 ページの「パーティションレプリカを表示する」を参照してください。

## パフォーマンス向上のためにレプリカを分散する

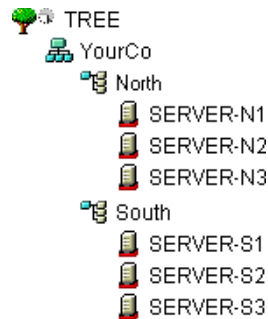
前の例で、Server1 サーバに、Tree パーティションと Finance パーティションの両方のレプリカが保管されているとします。この場合、パーティション分割後も Server1 はディレクトリ全体 (両パーティションのレプリカ) をまだ保持しているため、パーティション分割による eDirectory のパフォーマンスの向上は実現されません。

パフォーマンスを向上させるには、レプリカの 1 つを別のサーバに移動する必要があります。たとえば、Tree パーティションを Server2 へ移動すると、Tree および YourCo コンテナにあるすべてのオブジェクトが Server2 に移動します。Server1 は、Finance および Accounts コンテナのオブジェクトだけを格納することになります。Server1 と Server2 への負荷は、パーティション分割を行っていないときに比べて、いずれも軽くなります。

## パーティションと WAN リンク

ネットワークが、WAN リンクで分割された North サイトと South サイトの 2 つのサイトに渡っている場合を考えてみます。各サイトには、それぞれ 3 つのサーバがあります。

図 15 eDirectory コンテナの例



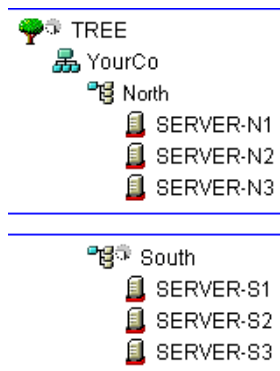
このケースでは、ディレクトリを 2 つのパーティションに分割すると、eDirectory はより高速になり、信頼性も向上します。

パーティションが 1 つしかないと、レプリカは 1 つのサイトに保存されるか、2 つのサイトに分散されます。この場合、次の 2 つの問題点があります。

- ◆ たとえば、North サイトにすべてのレプリカが保存されているとすると、South サイトでは、ログインやリソースへのアクセスに時間がかかります。また、リンクが停止した場合、South サイトのユーザは、ログインまたはリソースにアクセスすることができなくなります。
- ◆ レプリカが 2 つのサイトに分散されていると、ユーザはローカルでディレクトリにアクセスできます。ただし、サーバ間のレプリカの同期は WAN リンクを通して行われるので、リンクの信頼性が低い場合には、eDirectory エラーが発生する可能性があります。ディレクトリに加えられた変更を WAN 経由で伝えるには、時間がかかります。

51 ページの 図 16 に示した 2 つのパーティションによるソリューションは、WAN リンクでのパフォーマンスと信頼性の問題を解決します。

図 16 パーティションの例



Tree パーティションのレプリカは、North サイトのサーバに保存されています。South パーティションのレプリカは、[図 17](#) に示すように、South サイトのサーバに保存されています。

**図 17** パーティション、サーバ、およびレプリカの例

| Partition | Server    | Replica Type |
|-----------|-----------|--------------|
| TREE      | SERVER-N1 | Master       |
|           | SERVER-N2 | Read/write   |
|           | SERVER-N3 | Read/write   |
| South     | SERVER-S1 | Master       |
|           | SERVER-S2 | Read/write   |
|           | SERVER-S3 | Read/write   |

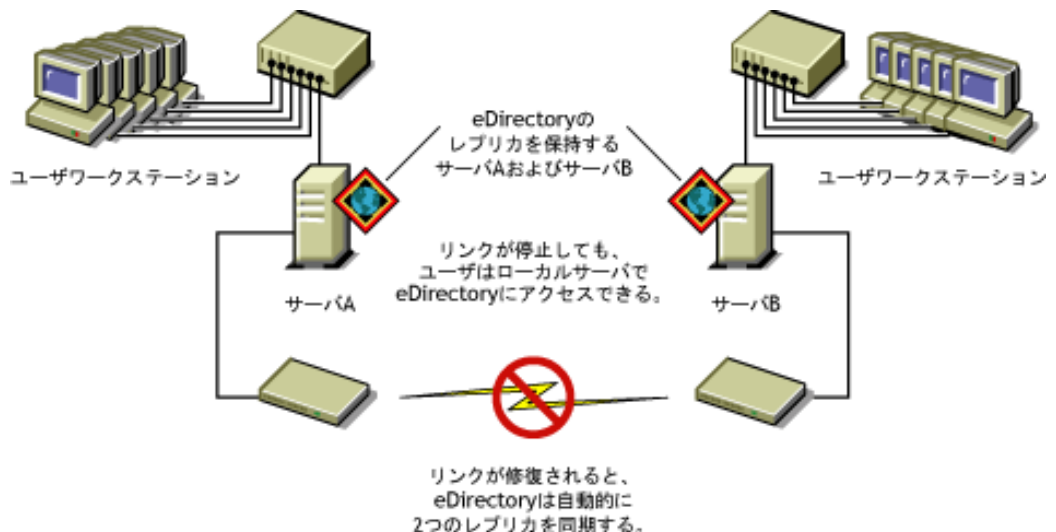
各サイトでは、ローカルリソースを表すオブジェクトは、ローカルで保存されています。サーバ間の同期トラフィックは、通信速度が遅く信頼性の低い WAN リンクではなく、LAN 上でローカルに行われます。

ただし、異なるサイトのオブジェクトにユーザや管理者がアクセスする場合は、WAN リンク上での eDirectory トラフィックが発生します。

## レプリカ

レプリカは、eDirectory サーバに分配されたユーザ定義済みのパーティションのコピーまたはインスタンスです。ネットワークに複数の eDirectory サーバがある場合、ディレクトリのレプリカ (コピー) を複数保存しておくことができます。これにより、あるサーバやそのサーバに対するネットワークリンクが機能しなくなった場合でも、ユーザが残りのネットワークリソースにログインして使用できます ([52 ページの 図 18](#) を参照)。

**図 18** eDirectory レプリカ





それぞれのサーバは、65,000以上のeDirectoryレプリカを格納できますが、同じユーザ定義済みのパーティションのレプリカで、同じサーバ上に格納できるのは1つだけです。レプリカの詳細な説明については、135ページの第5章「パーティションおよびレプリカの管理」を参照してください。

eDirectoryの障害対策として、レプリカを3つ保存しておくことをお勧めします(レプリカを保存するeDirectoryサーバが3箇所あると想定した場合)。単独のサーバに、複数のパーティションのレプリカを保存することもできます。

レプリカサーバは、eDirectoryレプリカのみを格納する専用サーバです。このタイプのサーバは、DSMASTERサーバとも呼ばれます。この環境設定は、多くの単一サーバリモートオフィスを使用する企業などでよく利用されます。レプリカサーバを使用すると、リモートオフィスの場所のパーティション用として追加のレプリカを格納できます。(402ページの「DSMASTERサーバによる災害対策」で説明されているように、それは障害回復計画の一部にもなります。)

eDirectoryのレプリケーションでは、サーバファイルシステムの障害対策は提供されません。eDirectoryオブジェクトに関する情報のみが、複製されます。ファイルシステムの障害対策には、TTS™ (Transaction Tracking System™)、ディスクのミラーリング/二重化、RAID、またはNRS (Novell Replication Services)を使用します。

バインダリサービスを提供するNetWareサーバでは、マスタレプリカ、または読み書き可能レプリカが必要になります。

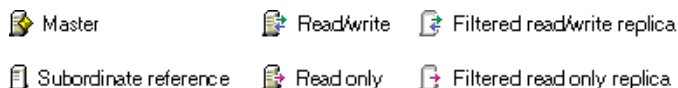
ユーザがWAN経由でeDirectory情報に定期的にアクセスしている場合は、必要な情報を含んだレプリカをサーバに配置し、ユーザがローカルでアクセスできるようにすることで、アクセス時間とWANトラフィックを減らすことができます。

LANにおいても、ある程度は同じことが当てはまります。ネットワーク上の複数のサーバにレプリカを分散すると、情報は、通常、最も近くにある使用可能なサーバから取得されます。

## レプリカのタイプ


eDirectoryでは、次の図に示したレプリカのタイプがサポートされます。

図 19 レプリカのタイプ



- ◆ 54ページの「マスタレプリカ」
- ◆ 54ページの「読み書き可能レプリカ」
- ◆ 55ページの「読み込み専用レプリカ」
- ◆ 55ページの「フィルタ済み読み書き可能レプリカ」
- ◆ 55ページの「フィルタ済み読み込み専用レプリカ」
- ◆ 56ページの「サブオーディネートリファレンスレプリカ」

## マスタレプリカ

 マスタレプリカはオブジェクトやパーティションへの変更を開始するのに使用される、書き込み可能なレプリカタイプです。マスタレプリカは、次のタイプの eDirectory パーティション操作を管理します。

- ◆ レプリカのサーバへの追加
- ◆ レプリカのサーバからの削除
- ◆ eDirectory ツリーの新しいパーティションの作成
- ◆ eDirectory ツリーの既存のパーティションの削除
- ◆ eDirectory ツリーのパーティションの移動

マスタレプリカは、次のタイプの eDirectory オブジェクト操作にも使用されます。


- ◆ eDirectory ツリーへの新しいオブジェクトの追加
- ◆ eDirectory ツリーの既存のオブジェクトの削除、リネーム、または移動
- ◆ eDirectory ツリーへのオブジェクトの認証
- ◆ eDirectory ツリーへの新しいオブジェクト属性の追加
- ◆ 既存の属性の変更または削除

デフォルトでは、ネットワークの最初の eDirectory サーバが、マスタレプリカを保持します。マスタレプリカは、各パーティションに同時に 1 つだけ存在します。別のレプリカを作成すると、デフォルトで読み書き可能レプリカになります。

マスタレプリカを保持しているサーバを 1 ～ 2 日以上ダウンさせる場合は、読み書き可能レプリカのうち 1 つをマスタレプリカにすることができます。オリジナルのマスタレプリカは、自動的に読み書き可能レプリカになります。


ネットワーク上にマスタレプリカがない場合、eDirectory で新しいレプリカやパーティションの作成などの操作を行うことはできません。

## 読み書き可能レプリカ

 eDirectory では、読み書き可能レプリカおよびマスタレプリカのオブジェクト情報にアクセスして、変更できます。すべての変更内容は、すべてのレプリカに自動的に伝えられます。

WAN リンクの通信速度が遅い場合やルータが使用中の場合など、ネットワークインフラストラクチャに遅延が起きてユーザへの eDirectory の反応が遅い場合は、必要なユーザの近くに読み書き可能レプリカを作成できます。読み書き可能レプリカは、サーバにいくつでも作成できますが、レプリカが増えると、同期を取るためにトラフィックの量が増加します。

## 読み込み専用レプリカ


 読み込み専用レプリカは、パーティションの境界ですべてのオブジェクトに関する情報を読み込むのに使用される、読み込み可能なレプリカタイプです。読み込み専用レプリカは、マスタレプリカと読み書き可能レプリカからの同期更新は受け入れませんが、クライアントからの直接の変更は受け入れません。

このレプリカタイプは、バインダリエミュレーションを提供できませんが、eDirectory ツリーの障害対策を提供しています。マスタレプリカおよびすべての読み書き可能なレプリカが破壊または破損すると、読み込み専用レプリカを新しいマスタレプリカに昇格させることができます。

また、NDS オブジェクトの読み込みやパーティションの境界内のすべてのオブジェクトを含むフォールトトレランス、およびパーティションルートオブジェクトを含む NDS ディレクトリツリーへの接続も提供します。

クライアントは常に読み書き可能レプリカにアクセスし、変更を加え続けることができるため、ツリー内のセキュリティポリシーを確立してオブジェクトの変更を制限する目的のために読み込み専用レプリカを使用することは避けてください。権利継承フィルタの使用のように、この目的でディレクトリに存在するメカニズムは他にもあります。詳細については、[64 ページの「IRF \(権利継承フィルタ\)」](#)を参照してください。


## フィルタ済み読み書き可能レプリカ

 フィルタ済み読み書き可能レプリカには、フィルタ済みオブジェクトセットまたはオブジェクトクラスが、これらのオブジェクトのフィルタ済み属性セットおよび値とともに格納されます。このレプリカの内容は、ホストサーバのレプリケーションフィルタに特定された eDirectory オブジェクトおよびプロパティのタイプに制限されません。ユーザはレプリカの内容を読み取ったり、変更することができ、eDirectory は選択されたオブジェクト情報にアクセスしたり、変更することができます。選択された変更内容は、すべてのレプリカに自動的に伝えられます。

フィルタ済みレプリカの場合、サーバごとにフィルタを1つだけ指定できます。つまり、あるサーバで定義されているフィルタは、そのサーバ上のすべてのフィルタ済みレプリカに適用されます。フィルタ済みレプリカは、サーバにいくつでも作成できますが、レプリカが増えると、同期を取るためのトラフィックの量が増加してしまいます。

詳細については、[56 ページの「フィルタ済みレプリカ」](#)を参照してください。

## フィルタ済み読み込み専用レプリカ

 フィルタ済み読み込み専用レプリカには、フィルタ済みオブジェクトセットまたはオブジェクトクラスが、これらのオブジェクトのフィルタ済み属性セットおよび値とともに格納されます。フィルタ済み読み込み専用レプリカは、マスタレプリカと読み書き可能レプリカからの同期更新は受け入れませんが、クライアントからの直接の変更は受け入れません。ユーザはこのレプリカの内容を読み込むことができますが、変更はできません。このレプリカの内容は、ホストサーバのレプリケーションフィルタに特定された eDirectory オブジェクトおよびプロパティのタイプに制限されます。

詳細については、[56 ページの「フィルタ済みレプリカ」](#)を参照してください。

## サブオーディネートリファレンスレプリカ

サブオーディネートリファレンスレプリカは、システム生成のレプリカで、マスタレプリカや読み書き可能レプリカのオブジェクトをすべて含んでいるわけではありません。したがって、サブオーディネートリファレンスレプリカは、障害対策を提供していません。サブオーディネートリファレンスレプリカは、eDirectory によるパーティションの境界を超えた名前の解決に必要な情報のみを格納するために生成される内部ポインタです。

サブオーディネートリファレンスレプリカを削除することはできません。不要になった時点で、eDirectory が自動的に削除します。サブオーディネートリファレンスレプリカは、ペアレントパーティションのレプリカを保持し、チャイルドパーティションのレプリカを保持していないサーバでのみ作成されます。

チャイルドパーティションのレプリカが、ペアレントのレプリカを保持するサーバにコピーされた場合、サブオーディネートリファレンスレプリカは自動的に削除されます。

## フィルタ済みレプリカ

フィルタ済みレプリカには、フィルタ済みオブジェクトセットまたはオブジェクトクラスが、これらのオブジェクトのフィルタ済み属性セットおよび値とともに格納されます。たとえば、eDirectory ツリーのさまざまなパーティション内のユーザオブジェクトのみを格納するフィルタ済みレプリカのセットを、1つのサーバ上に作成できます。また、ユーザオブジェクトのデータ(名、姓、電話番号など)のサブセットのみを格納するレプリカを作成することもできます。

フィルタ済みレプリカを使用して、1つのサーバ上に eDirectory データのビューを構築できます。そのために、フィルタ済みレプリカでは、スコープとフィルタを作成できます。これにより、ツリー内の数多くのパーティションから 1つの eDirectory サーバに、適切に定義されたデータセットを格納することが可能になります。

サーバのスコープとデータフィルタの説明は eDirectory に格納され、iManager のサーバオブジェクトを通して管理できます。

1つまたは複数のフィルタ済みレプリカを格納するサーバは、レプリケーションフィルタを1つだけ保持します。そのため、そのサーバ上のすべてのフィルタ済みレプリカは、それぞれのパーティションからの情報の同じサブセットを格納します。フィルタ済みレプリカのマスタパーティションレプリカは、eDirectory 8.5 以降が動作する eDirectory サーバに保管する必要があります。

フィルタ済みレプリカは、次の目的に使用できます。

- ◆ 他のサーバから複製する必要があるデータ量が減ることによる、サーバへの同期トラフィックの削減。
- ◆ Novell Nsure Identity Manager によってフィルタリングする必要があるイベント量の削減。

Novell Nsure Identity Manager の詳細については、『[DirXML 管理ガイド](#)』(<http://www.novell.com/documentation/dirxml20/index.html>) を参照してください。

- ◆ ディレクトリデータベースのサイズの縮小。

レプリカの数が増えれば、その分データベースのサイズが増大します。完全なレプリカを作成するのではなく、特定のクラスのデータのみを格納するフィルタ済みレプリカを作成することによって、ローカルデータベースのサイズを小さくすることができます。

たとえば、ツリーに 10,000 のオブジェクトが含まれていても、そのうちユーザオブジェクトの占める割合がわずかであれば、10,000 すべてのオブジェクトを格納する完全なレプリカではなく、ユーザオブジェクトのみを格納するフィルタ済みレプリカを作成できます。

ローカルデータベースに格納されているデータをフィルタリングできるという特徴を別にすれば、フィルタ済みレプリカは通常の eDirectory レプリカと同じであり、必要なときはいつでも完全なレプリカに戻すことができます。

**注:** デフォルトでフィルタ済みのレプリカは、必須のフィルタとして組織および部門を持つこととなります。

フィルタ済みレプリカの設定と管理の詳細については、[143 ページの「フィルタ済みレプリカを設定し管理する」](#)を参照してください。

## NetWare バインダリエミュレーション

プリント サーバやバックアップソフトウェアなどの多くのアプリケーションは、NetWare 4 以前のバージョンの NetWare 用に作成されており、これらのアプリケーションでは、ネットワークアクセスやオブジェクトの操作に、eDirectory ではなく、NetWare バインダリを使用していました。

バインダリとは、ユーザ、グループ、およびボリュームといった、指定したサーバに認識されているオブジェクトの単純なデータベースです。バインダリは、サーバ固有かつサーバ中心です。

NETX バインダリシェルなど、以前の NetWare クライアントソフトウェアはバインダリログイン手順を使用しており、ユーザは特定のサーバにしかログインできませんでした。複数のサーバにアクセスするには、複数のユーザアカウントを使用して、ログインを何度も行う必要がありました。

eDirectory では、バインダリ用に作成されたアプリケーションを、バインダリサービスを使用して実行できます。バインダリサービスでは、1 つ以上の eDirectory コンテキスト (最大 12) を、eDirectory サーバの仮想バインダリとして設定できます。設定したコンテキストは、サーバのバインダリコンテキストといいます。

バインダリサービスに関する重要な情報を次に示します。

- ◆ バインダリサービスを使用するには、eDirectory サーバにバインダリコンテキストを設定する必要があります。
- ◆ オブジェクトすべてが、バインダリオブジェクトにマップされるわけではありません。別名オブジェクトのように、オブジェクトの多くは、バインダリと互換性がありません。
- ◆ ほとんどのバインダリアプリケーションは、eDirectory で動作するようにアップグレードされています。アプリケーションの製造元に確認し、最新バージョンを取得します。
- ◆ バインダリコンテキストを含む各 eDirectory サーバは、バインダリコンテキストを含むパーティションのマスタレプリカ、または読み書き可能レプリカを保持している必要があります。

## レプリカリングでのサーバの同期

複数のサーバが、同じパーティションのレプリカを保持している場合、それらのサーバはレプリカリングとみなされます。同期は、あるレプリカから他のレプリカへのディレクトリ情報の伝播であるため、各パーティションの情報は他のパーティションの情報と整合性を保ちます。eDirectory は自動的にそれらのサーバの同期を維持します。詳細については、[111 ページの「同期」](#)を参照してください。

eDirectory 同期のタイプは、次のとおりです。

- ◆ [通常同期およびレプリカ同期](#)
- ◆ [優先度同期](#)

## リソースへのアクセス

eDirectory は、デフォルトの権利に従って基本レベルのネットワークアクセスセキュリティを構築します。アクセス制御をより強化するための方法を、次に示します。

- ◆ 権利の割り当て

ユーザがネットワークリソースへのアクセスを試みると、システムはそのリソースに対するユーザの有効な権利を計算します。明示的なトラスティ割り当て、同等セキュリティの付与、および継承される権利に対するフィルタ処理を行うことによって、ユーザがリソースに対する適切で有効な権利を持つように設定できます。

権利の割り当てを単純化するため、グループおよび職種オブジェクトを作成した後に、グループや職種にユーザを割り当てることができます。

- ◆ ログインセキュリティの追加

ログインセキュリティは、デフォルトでは設定されていません。ログインセキュリティ方法の設定にはいくつかあります。ログインパスワード、ログインする場所および時間の制限、同時ログインセッションの制限、不正侵入者検出、およびログインの禁止があります。

- ◆ ロールベース管理の設定

特定のオブジェクトプロパティに対して管理者を設定し、これらのプロパティに対してのみ、権利を許可します。これにより、特定の責任を担う管理者を作成できます。この責任はどのコンテナオブジェクトの下位のオブジェクトへも継承できます。ロールベースの管理者は、従業員の情報やパスワードに関連したプロパティのような、特定のプロパティに対して責任を持ちます。

ロールベースサービスの設定の手順については、『[Novell iManager 2.5 管理ガイド](#)』の「[RBS のインストール](#)」([http://www.novell.com/documentation/imanager25/imanager\\_admin\\_25/data/am757mw.html#bu1rlq9](http://www.novell.com/documentation/imanager25/imanager_admin_25/data/am757mw.html#bu1rlq9))を参照してください。

管理者がロールベースの管理アプリケーションを実行できるように、特定のタスクに基づいて役割を定義することもできます。詳細については、[106 ページの「役割ベースサービスを設定する」](#)を参照してください。



## eDirectory での権利

ツリーを作成すると、デフォルトの権利割り当てによって、ネットワークへの汎用アクセスとセキュリティが与えられます。デフォルトの割り当てには、次のようなものがあります。

- ◆ ユーザ **Admin** はツリーの最上位に対してスーパーバイザ権を持ちます。これにより、**Admin** はディレクトリ全体を完全に制御できます。**Admin** は、**NetWare** サーバオブジェクトに対してもスーパーバイザ権を持ち、サーバ上のどのボリュームに対しても完全に制御できます。
- ◆ **[Public]** はツリーの最上位のブラウザ権を持ちます。これにより、すべてのユーザが、パブリックアクセスを通して、ツリー内のすべてのオブジェクトを表示する権利を持つこととなります。
- ◆ **NetWare** での移行、印刷アップグレード、または **Windows NT** でのユーザ移行などのアップグレードプロセスを通して作成したオブジェクトは、ほとんどの場合、適切なトラスティを割り当てられます。

## トラスティ割り当ておよびターゲット

権利の割り当てには、トラスティとターゲットとなるオブジェクトが関係します。トラスティとは、認証されているユーザまたはユーザのグループを表します。ターゲットとは、ユーザが権利を持っているネットワークリソースです。

- ◆ 別名をトラスティにする場合、権利は別名が示すオブジェクトにのみ適用されません。ただし、別名オブジェクトを明示的にターゲットにすることは可能です。
- ◆ ファイルシステム権は **eDirectory** 内ではなく、ファイルシステム自体に保存されていますが、**NetWare** ファイルシステム内のファイルまたはディレクトリも、ターゲットにすることができます。

注： **[Public]** トラスティは、オブジェクトではありません。すべてのネットワークユーザに対して与えられる、権利割り当てに関連するトラスティです。

## eDirectory での権利の概念

eDirectory での権利についてより良く理解していただくために、次に各権利の概念について説明します。

- ◆ [60 ページの「オブジェクト \( エントリ \) 権」](#)
- ◆ [60 ページの「プロパティ権」](#)
- ◆ [61 ページの「有効な権利」](#)
- ◆ [61 ページの「有効な権利を計算する方法」](#)
- ◆ [64 ページの「同等セキュリティ」](#)
- ◆ [64 ページの「ACL \( アクセス制御リスト \)」](#)
- ◆ [64 ページの「IRF \( 権利継承フィルタ \)」](#)

## オブジェクト(エン트리)権

トラスティ割り当てを作成するときには、オブジェクト権とプロパティ権を与えることができます。オブジェクト権はオブジェクト全体の操作に適用されますが、プロパティ権は一定のオブジェクトプロパティにのみ適用されます。オブジェクト権は、eDirectory データベース内でエントリが提供されるため、エントリ権と呼ばれます。

各権利について、次に説明します。

- ◆ **スーパーバイザ** オブジェクトおよびそのオブジェクトのすべてのプロパティに対する、すべての権利が含まれます。
- ◆ **参照** ツリー内のオブジェクトを参照する権利です。オブジェクトのプロパティを参照する権利は含まれていません。
- ◆ **作成** ターゲットオブジェクトがコンテナの場合にのみ適用されます。トラスティがコンテナの下に新規オブジェクトを作成する権利のことで、ブラウズ権も含まれます。
- ◆ **削除** ディレクトリからターゲットを削除する権利です。
- ◆ **リネーム** ターゲット名を変更する権利です。

## プロパティ権

トラスティ割り当てを作成するときには、オブジェクト権とプロパティ権を与えることができます。オブジェクト権はオブジェクト全体の操作に適用されますが、プロパティ権は一定のオブジェクトプロパティにのみ適用されます。

iManager では、プロパティ権の管理用に次の 2 つのオプションが用意されています。

- ◆ [すべての属性権] 項目が選択されている場合は、すべてのプロパティを管理できます。
- ◆ 特定のプロパティが選択されている場合は、選択された個々のプロパティを管理できます。

各権利について、次に説明します。

- ◆ **スーパーバイザ** トラスティにプロパティの完全な制御権を与えます。
- ◆ **比較** トラスティは、プロパティの値と任意の値を比較できます。この権利によって検索が可能になります。検索では、TRUE または FALSE の結果のみ返されます。トラスティは、プロパティの値を実際に参照することはできません。
- ◆ **読み込み** トラスティはプロパティの値を参照することができます。この権利には、比較権が含まれます。
- ◆ **書き込み** トラスティはプロパティの値を作成、変更、および削除できます。
- ◆ **自己追加** トラスティ自身をプロパティの値として追加または削除する権利です。この権利は、メンバーシップリストまたは ACL (アクセス制御リスト) などのような、値としてオブジェクト名を持つプロパティに適用されます。



## 有効な権利

ユーザは、明示的なトラスティ割り当て、継承、および同等セキュリティなどのさまざまな方法で権利を受け取ることができます。権利は、権利継承フィルタにより制限され、下位レベルのトラスティ割り当てによって変更、または取り消すこともできます。このような操作による最終的な結果、つまりユーザが実際に行使できる権利を、*有効な権利*といいます。

ユーザがいずれかの操作を実行しようとするたびに、該当のオブジェクトに対するそのユーザの有効な権利が計算されます。

## 有効な権利を計算する方法

ユーザがネットワークリソースにアクセスを試みるたびに、eDirectory は次の手順でそのターゲットリソースに対するユーザの有効な権利を計算します。

1. 計算で考慮される権利を持ったトラスティをリストします。考慮されるトラスティには次のものがあります。

- ◆ ターゲットリソースにアクセスしようとしているユーザ
- ◆ ユーザが同等セキュリティとなっているオブジェクト

2. リスト内の各トラスティに対して、次のように有効な権利を決定します。

- a. まず、ツリーの最上位に対してトラスティが継承可能な権利を持っているかどうかチェックします。

eDirectory は Tree オブジェクトのオブジェクトトラスティ (ACL) プロパティをチェックして、該当のトラスティが登録された項目があるかどうか調べます。該当のトラスティが登録された項目が見つかり、その権利が継承可能な場合、eDirectory はそれらの項目に指定された権利を、該当のトラスティの有効な権利の初期セットとして使用します。

- b. ツリー内の、ターゲットリソースが含まれている分岐を 1 レベル下に移動します。
- c. このレベルでフィルタリングされるすべての権利を削除します。

eDirectory はこのレベルの ACL をチェックし、該当のトラスティの有効な権利のタイプ (オブジェクト、すべてのプロパティ、または特定のプロパティ) と一致する IRF (権利継承フィルタ) がないか調べます。検出された場合は、eDirectory は該当のトラスティの有効な権利から、これらの IRF によって継承を阻止されるすべての権利を削除します。

たとえば、上位のレベルで、トラスティの有効な権利にすべてのプロパティに対する書き込み権の割り当てが含まれていても、このレベルの IRF によってその継承を阻止された場合、すべてのプロパティに対する書き込み権はトラスティの有効な権利から削除されます。

- d. このレベルで割り当てられた継承可能な権利があれば追加し、必要に応じて他の割り当てを無効化します。

eDirectory はこのレベルの ACL をチェックし、該当のトラスティが登録された項目があるかどうかチェックします。該当のトラスティが登録された項目が見つかり、その権利が継承可能な場合、eDirectory はそれらの項目の権利をトラスティの有効な権利にコピーし、必要に応じて他の割り当てを無効化します。

たとえば、上位のレベルで、トラスティの有効な権利に作成および削除オブジェクト権が含まれ、プロパティ権についてはまったく含まれていないときに、このレベルの ACL に、該当のトラスティに対する 0 オブジェクト権の割り当てとすべてのプロパティの書き込み権の割り当てが含まれている場合、トラスティの既存のオブジェクト権 (作成および削除) は 0 権利と置き換えられ、新たにすべてのプロパティ権が追加されます。

- e. ツリーの各レベル (ターゲットリソースのレベルを含む) で、フィルタリングと追加の手順 (c および d) を繰り返します。
- f. ターゲットリソースで割り当てられた継承不可能な権利があれば追加し、必要に応じて他の割り当てを無効化します。

eDirectory は手順 2d と同じ処理を行います。その結果作成される権利セットが、該当のトラスティの有効な権利になります。

3. リスト内のすべてのトラスティの有効な権利を次のように結合します。

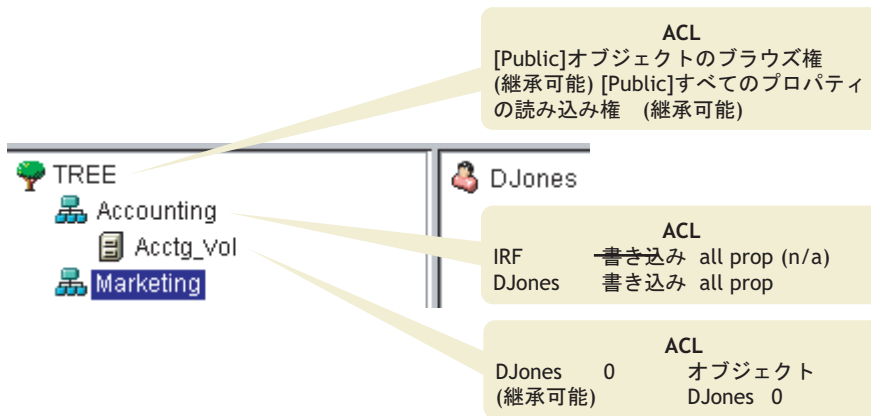
- a. eDirectory はリスト内のいずれかのトラスティが所有している権利をすべて含めます。リスト内のどのトラスティも所有していない権利のみ除外します。権利タイプは混在させません。たとえば、特定のプロパティに対する権利を、すべてのプロパティに対する権利に追加したり、その逆を行うことはありません。
- b. 現在有効な権利に暗黙に含まれる権利を追加します。

権利の設定により、ターゲットリソースに対するユーザの有効な権利が作られます。

## 例

ユーザ DJones が、ボリューム Acctg\_Vol にアクセスしようとしています (図 20 を参照してください)。

図 20 トラスティ権の例



次の手順は、eDirectory が Acctg\_Vol に対する DJones の有効な権利を計算する方法を示したものです。

1. 計算で考慮される権利を持ったトラスティは、DJones、Marketing、Tree、および [Public] です。

ここでは、DJones がどのグループまたは役割にも所属せず、どの同等セキュリティにも明示的に割り当てられていないと仮定しています。

2. 各トラスティの有効な権利は、次のとおりです。

- ◆ DJones : 0 オブジェクト、0 すべてのプロパティ

Acctg\_Vol で 0 すべてのプロパティ権を割り当てられることで、Accounting でのすべてのプロパティに対する書き込み権の割り当ては無効化されます。

- ◆ Marketing : 0 すべてのプロパティ

ツリーの最上位にあるすべてのプロパティに対する書き込み権の割り当ては、Accounting での IRF によって除外されます。

- ◆ Tree : 権利なし

Tree には、関連するどのツリー分岐でも、権利はまったく割り当てられません。

- ◆ [Public] : オブジェクトのブラウズ権、すべてのプロパティの読み込み権

これらの権利はルートで割り当てられ、関連するツリー分岐のどの位置でも、フィルタリングも無効化もされません。

3. これらすべてのトラスティの権利を結合することによって、次のようになります。

DJones : オブジェクトのブラウズ権、すべてのプロパティの読み込み権

4. すべてのプロパティの読み込み権に伴って暗黙で割り当てられるすべてのプロパティの比較権を追加することで、最終的に Acctg\_Vol に対する DJones の有効な権利は次のようになります。

DJones : オブジェクトのブラウズ権、すべてのプロパティの読み込み、比較権

### 有効な権利のブロック

有効な権利の計算方法では、IRF に頼らずに特定の権利を特定のユーザに対してブロックする方法は、必ずしも明確ではありません (IRF はすべてのユーザの権利をブロックします)。

特定の権利を IRF に頼らずにユーザに対してブロックするには、次のような方法があります。

- ◆ ターゲットリソース、およびツリー内のターゲットリソースよりも上位のレベルで、該当のユーザおよびそのユーザと同等セキュリティになるオブジェクトにそれらの権利を割り当てないようにする。
- ◆ 該当のユーザまたはそのユーザが同等セキュリティになるいずれかのオブジェクトにそれらの権利が実際に割り当てられている場合は、ツリーの下位レベルに、それらの権利の割り当てを阻止する何らかの割り当てをそのオブジェクトに対して与えるようにする。不適切な権利を持つすべての (ユーザと関連する) トラスティに対して、これを実行します。

## 同等セキュリティ

同等セキュリティとは、別のオブジェクトと同じ権利を持つことを意味します。あるオブジェクト (オブジェクト A) を別のオブジェクト (オブジェクト B) と同等セキュリティにすると、オブジェクト A の有効な権利の計算時には、オブジェクト B の権利がオブジェクト A に追加されます。

たとえば、ユーザオブジェクト **Joe** を **Admin** オブジェクトと同等セキュリティにするとします。同等セキュリティを割り当てた後は、**Joe** は、ツリーおよびファイルシステムに対して、**Admin** が持つ権利と同じ権利を持つこととなります。

同等セキュリティには、次の3つのタイプがあります。

- ◆ 明示的：割り当てによる
- ◆ 自動：グループのメンバーシップまたは役割による
- ◆ 暗黙的：すべてのペアレントコンテナおよび **[Public]** トラストティと同等

同等セキュリティは、1ステップにかぎり有効です。たとえば、さらに別のユーザを上例の **Joe** と同等セキュリティにした場合、このユーザは **Joe** の権利は受け取りますが、**Admin** の権利は受け取りません。

同等セキュリティは、該当のユーザオブジェクトの同等セキュリティプロパティの値として **eDirectory** に記録されます。

ユーザオブジェクトを職種オブジェクトにその職種の担当者として追加すると、そのユーザは自動的にその職種オブジェクトと同等セキュリティになります。ユーザをグループオブジェクトに追加した場合も同様です。

## ACL (アクセス制御リスト)

ACL (アクセス制御リスト) は、オブジェクトトラスティプロパティとも呼ばれます。トラスティを割り当てると、そのトラスティは値としてターゲットのオブジェクトトラスティ (ACL) プロパティに追加されます。

このプロパティは、次の理由から、ネットワークのセキュリティに大きく影響します。

- ◆ オブジェクトのオブジェクトトラスティ (ACL) プロパティに対する書き込み権またはスーパーバイザ権を持つユーザは、そのオブジェクトのトラスティが誰であるかを知ることができる。
- ◆ オブジェクトのオブジェクトトラスティ (ACL) プロパティに対して自己追加権を持つユーザは、そのオブジェクトに対する自分の権利を変更できる。たとえば、そのユーザは自分にスーパーバイザ権を与えることができます。

このため、コンテナオブジェクトのすべてのプロパティに対して自己追加権を与える場合は、慎重に行う必要があります。自己追加権を割り当てられたトラスティは、該当のコンテナ、その中のすべてのオブジェクト、およびその下のコンテナ内のすべてのオブジェクトに対してスーパーバイザとなることができます。

## IRF (権利継承フィルタ)

権利継承フィルタにより、**eDirectory** ツリーの低位レベルへの権利の継承をブロックできます。このフィルタの設定の詳細については、**70 ページの「eDirectory オブジェクトまたはプロパティへの権利継承をブロックする」**を参照してください。

## 新規サーバのデフォルト権


新規サーバオブジェクトをツリーにインストールすると、次のトラスティ割り当てが作成されます。

| デフォルトトラスティ                           | デフォルト権   |
|--------------------------------------|--|
| Admin ( ツリー内の最初の eDirectory サーバ )    | Tree オブジェクトに対するスーパーバイザオブジェクト権。<br><br>Admin は、NetWare サーバオブジェクトに対してスーパーバイザオブジェクト権を持ちます。これは、Admin がサーバ上に存在するあらゆるボリュームのファイルシステムのルートディレクトリに対してもスーパーバイザ権を持つことを意味します。 |
| [Public] ( ツリー内の最初の eDirectory サーバ ) | Tree オブジェクトに対するブラウザオブジェクト権。  |
| Tree                                 | すべてのボリュームオブジェクトのホストサーバ名プロパティおよびホストリソースプロパティに対する Tree 読み込みプロパティ権。<br><br>これにより、すべてのオブジェクトが物理ボリューム名および物理サーバ名にアクセスできるようになります。                                       |
| コンテナオブジェクト                           | sys:¥public に対する読み込みおよびファイルスキャン権。これにより、コンテナの下のユーザオブジェクトは、¥public の NetWare ユーティリティにアクセスできるようになります。   |
| ユーザオブジェクト                            | ユーザ用にホームディレクトリが自動的に作成されると、ユーザにはそのディレクトリに対するスーパーバイザ権が与えられます。  |


## 管理の委託

eDirectory では、自分が管理するツリーの分岐に対する管理権を無効にして、その分岐の管理を他の人物に委託できます。たとえば、特別なセキュリティ要件により、ツリーの分岐を完全に制御する管理者を個別に置かなければならないような場合には、管理権の委託というこの方法をとることが必要になります。

管理権を委託するには、次を実行します。

- 1 委託先のユーザに、該当のコンテナに対するスーパーバイザオブジェクト権を与えます。
  - 1a Novell iManager で、[役割およびタスク] ボタン  をクリックします。
  - 1b [権利] > [トラスティの変更] の順にクリックします。
  - 1c アクセスを制御するコンテナオブジェクトの名前およびコンテキストを入力して、[OK] をクリックします。
  - 1d [割り当てられた権利] をクリックします。
  - 1e 目的のプロパティの [スーパーバイザ] チェックボックスをオンにします。
  - 1f [完了] をクリックし、[OK] をクリックします。

**2** 継承を阻止したいスーパーバイザ権や他の権利をフィルタリングするための IRF を、そのコンテナに対して作成します。

**2a** Novell iManager で、[役割およびタスク] ボタン  をクリックします。

**2b** [権利] > [権利継承フィルタの変更] の順にクリックします。

**2c** 変更する権利継承フィルタを持つオブジェクトの名前およびコンテキストを指定して、[OK] をクリックします。

**2d** 必要に応じて権利継承フィルタのリストを編集します。

フィルタのリストを編集するには、オブジェクトの ACL プロパティへのスーパーバイザ権またはアクセス制御権を持っている必要があります。オブジェクトの継承された権利を全体的にブロックするフィルタは、オブジェクトのすべてのプロパティおよび個々のプロパティに対して設定できます。

**注:** フィルタによって、このオブジェクトのトラスティに明示的に付加された権利がブロックされることはありません。これらの権利は継承されるものではないからです。

**2e** [OK] をクリックします。

**重要:** ユーザオブジェクトに管理を委託した後に、そのオブジェクトが削除されると、その分岐を管理する権利を持つオブジェクトはなくなります。

パスワードの管理など、特定の eDirectory プロパティの管理を委託するには、[68 ページの「同等セキュリティを付与する」](#)を参照してください。

ルールベース管理アプリケーションの特定の機能の使用を委託するには、[106 ページの「役割ベースサービスを設定する」](#)を参照してください。

## 権利の管理

- ◆ [66 ページの「権利を明示的に割り当てる」](#)
- ◆ [68 ページの「同等セキュリティを付与する」](#)
- ◆ [70 ページの「eDirectory オブジェクトまたはプロパティへの権利継承をブロックする」](#)
- ◆ [70 ページの「eDirectory オブジェクトまたはプロパティへの有効な権利を参照する」](#)


### 権利を明示的に割り当てる

eDirectory ツリーでデフォルトで割り当てられた権利によって、ユーザが必要以上にリソースにアクセスできたり、アクセスが不十分であったりする場合は、権利を明示的に作成して割り当てたり、それを変更したりできます。権利の割り当てを作成または変更するには、まず最初にアクセスを制御しているリソースやトラスティ (権利を所有している、またはこれから所有する eDirectory オブジェクト) を選択します。

**ヒント:** ユーザの権利を個々にではなく集団で管理するには、グループ、役割、またはコンテナオブジェクトをトラスティにします。すべてのユーザについてリソースへのアクセスを全体的に制限するには、[70 ページの「eDirectory オブジェクトまたはプロパティへの権利継承をブロックする」](#)を参照してください。

- ◆ [67 ページの「リソースに基づいて Novell eDirectory へのアクセスを制御する」](#)
- ◆ [67 ページの「トラスティに基づいて Novell eDirectory へのアクセスを制御する」](#)

## リソースに基づいて Novell eDirectory へのアクセスを制御する


- 1 Novell iManager で、[役割およびタスク] ボタン  をクリックします。
- 2 [権利] > [トラスティの変更] の順にクリックします。
- 3 アクセスを制御する eDirectory リソース(オブジェクト)の名前およびコンテキストを指定して、[OK] をクリックします。

コンテナの下のすべてのオブジェクトへのアクセスを制御するには、そのコンテナを選択します。
- 4 トラスティのリストおよび権利の割り当てを必要に応じて編集します。
  - 4a トラスティの権利の割り当てを変更するには、トラスティを選択し、[割り当てられた権利] をクリックして、必要に応じて権利の割り当てを変更してから、[完了] をクリックします。
  - 4b トラスティとしてオブジェクトを追加するには、[トラスティの追加] をクリックし、オブジェクトを選択し、[OK] をクリックします。次に、[割り当てられた権利] をクリックしてトラスティを割り当て、[完了] をクリックします。

権利の割り当てを作成または変更する場合、オブジェクト全体に対しても、オブジェクトのすべてのプロパティまたは個々のプロパティに対しても、アクセスを付与したり拒否したりすることができます。
  - 4c トラスティとなっているオブジェクトを削除するには、そのトラスティを選択し、[トラスティの削除] をクリックします。

削除されたトラスティには、オブジェクトやプロパティに対する明示的な権利はすでにありませんが、継承や同等セキュリティによる有効な権利はまだ存在する可能性があります。
- 5 [OK] をクリックします。

## トラスティに基づいて Novell eDirectory へのアクセスを制御する

- 1 Novell iManager で、[役割およびタスク] ボタン  をクリックします。
- 2 [権利] > [他のオブジェクトに対する権利] の順にクリックします。
- 3 権利を変更するトラスティ(権利を所有している、またはこれから所有するオブジェクト)の名前やコンテキストを入力します。
- 4 [検索範囲のコンテキスト] フィールドで、トラスティが現在権利を割り当てられている eDirectory オブジェクトを検索する eDirectory ツリーの一部を指定します。
- 5 [OK] をクリックします。

検索の進行状況を表す画面が表示されます。検索が終了すると、[他のオブジェクトに対する権利] ページに検索結果が表示されます。
- 6 トラスティの eDirectory 権利の割り当てを必要に応じて編集します。
  - 6a 権利の割り当てを追加するには、[オブジェクトの追加] をクリックし、アクセスを制御するオブジェクトを選択して、[OK] をクリックします。次に、[割り当てられた権利] をクリックして、トラスティの権利を割り当ててから [完了] をクリックします。



- 6b** 権利の割り当てを変更するには、アクセスを制御するオブジェクトを選択し、[割り当てられた権利] をクリックして、必要に応じてトラスティの権利の割り当てを変更してから、[完了] をクリックします。

権利の割り当てを作成または変更する場合、オブジェクト全体に対しても、オブジェクトのすべてのプロパティまたは個々のプロパティに対しても、アクセスを付与したり拒否したりすることができます。

- 6c** 権利の割り当てを削除するには、アクセスを制御するオブジェクトを選択して、[オブジェクトの削除] をクリックします。

トラスティには、オブジェクトやプロパティに対する明示的な権利はすでにありませんが、継承や同等セキュリティによる有効な権利はまだ存在する可能性があります。

- 7** [OK] をクリックします。

## 同等セキュリティを付与する

別の eDirectory オブジェクトに対して同等セキュリティとなっているユーザは、事実上そのオブジェクトのすべての権利を持っています。ユーザは自動的に、所属するグループや役割に対して同等セキュリティになります。すべてのユーザは、[Public] トラスティ、および Tree オブジェクトなど、eDirectory ツリーのユーザオブジェクトの上にある個々のコンテナに対して、暗黙で同等セキュリティとなります。また、任意の eDirectory オブジェクトに対して同等セキュリティを明示的に付与することもできます。

**注:** このセクションのタスクを実行すると、eDirectory 権利を通じて管理権限を委託することができます。ロールベースサービス (RBS) 役割を使用する管理アプリケーションがある場合、それらの役割にユーザメンバーシップを割り当てることで管理権限を委託することもできます。

- ◆ [68 ページの「メンバーシップに基づいて同等セキュリティを付与する」](#)
- ◆ [69 ページの「明示的に同等セキュリティを付与する」](#)
- ◆ [69 ページの「オブジェクト固有の eDirectory プロパティの管理者を設定する」](#)

### メンバーシップに基づいて同等セキュリティを付与する

- 1** まだ完了していない場合は、ユーザを同等セキュリティにするグループまたは役割オブジェクトを作成します。

詳細については、[98 ページの「オブジェクトを作成する」](#)を参照してください。

- 2** グループや役割に、ユーザに必要な eDirectory 権利を与えます。

詳細については、[66 ページの「権利を明示的に割り当てる」](#)を参照してください。

- 3** グループや役割のメンバーシップを編集して、グループや役割の権利を必要とするユーザを追加します。



- ◆ グループオブジェクトには、[メンバー] プロパティページを使用します。

Novell iManager で、[eDirectory 管理] > [オブジェクトの変更] の順にクリックし、グループオブジェクトの名前とコンテキストを指定して [OK] をクリックし、次に [メンバー] タブをクリックします。

- ◆ 職種オブジェクトには、[担当者] プロパティページの [担当者] フィールドを使用します。


Novell iManager で、[eDirectory 管理] > [オブジェクトの変更] の順にクリックし、rbsRole オブジェクトの名前とコンテキストを指定して [OK] をクリックし、次に [全般] タブで [担当者] をクリックします。



- ◆ rbsRole オブジェクトには、[iManager のメンバーを変更] ページを使用します。  
Novell iManager で、[設定] ボタン  をクリックし、[役割の設定] > [iManager の役割を変更] の順にクリックします。次に、変更する役割の左にある [メンバーの変更] ボタン  をクリックしてから、[iManager のメンバーを変更] ページのオプションを使用して役割のメンバーを追加または削除します。

4 [OK] をクリックします。


#### 明示的に同等セキュリティを付与する

- 1 Novell iManager で、[役割およびタスク] ボタン  をクリックします。
- 2 [eDirectory 管理] > [オブジェクトの変更] の順にクリックします。
- 3 ユーザを同等セキュリティとするユーザまたはオブジェクトの名前およびコンテキストを入力して、[OK] をクリックします。
- 4 [セキュリティ] タブをクリックし、次のように同等セキュリティを付与します。
  - ◆ ユーザを選択し、[同等セキュリティ] をクリックします。次に、ユーザを同等セキュリティとするオブジェクトの名前とコンテキストを入力して <Enter> を押し、[OK] をクリックします。
  - ◆ ユーザを同等セキュリティとするオブジェクトを選択する場合は、[同等セキュリティ保有者] をクリックし、オブジェクトを同等セキュリティとするユーザの名前とコンテキストを入力して <Enter> を押し、[OK] をクリックします。

これらの 2 つのプロパティ ページのコンテキスト は、システムによって同期されます。


5 [OK] をクリックします。

#### オブジェクト固有の eDirectory プロパティの管理者を設定する

- 1 まだ完了していない場合、オブジェクト固有のプロパティのトラスティを作成するユーザ、グループ、役割、またはコンテナオブジェクトを作成します。  
トラスティとしてコンテナを作成する場合、コンテナ内またはその下のすべてのオブジェクトに権利が付与されます。プロパティは継承可能なものにする必要があります。そうしないと、コンテナおよびそのメンバーは下位レベルへの権利を持たなくなりません。  
詳細については、98 ページの「オブジェクトを作成する」を参照してください。
- 2 Novell iManager で、[役割およびタスク] ボタン  をクリックします。
- 3 [権利] > [トラスティの変更] の順にクリックします。
- 4 管理者による管理を必要とする最高レベルのコンテナの名前とコンテキストを指定し、[OK] をクリックします。
- 5 [トラスティの変更] ページで、[トラスティの追加] をクリックし、管理者を表すオブジェクトを選択して [OK] をクリックします。
- 6 追加したトラスティの [割り当てられた権利] をクリックし、[プロパティの追加] をクリックします。
- 7 プロパティリストに追加するプロパティを選択して、[OK] をクリックします。
- 8 管理者が管理するそれぞれのプロパティについて、必要な権利を割り当てます。それぞれの権利の割り当ての [継承可能] チェックボックスをオンにします。
- 9 [完了] をクリックし、[OK] をクリックします。

## eDirectory オブジェクトまたはプロパティへの権利継承をブロックする

eDirectory では、コンテナの権利の割り当ては、継承可能な場合とそうでない場合があります。NetWare のファイルシステムでは、フォルダ上のすべての権利の割り当ては継承可能です。eDirectory および NetWare では、個々の下位アイテムについてこのような継承をブロックして、トラスティになるユーザーに関係なく、これらのアイテム上では権利を無効にすることができます。例外として、NetWare ファイルシステムではスーパーバイザ権はブロックできません。

- 1 Novell iManager で、[役割およびタスク] ボタン  をクリックします。
- 2 [権利] > [権利継承フィルタの変更] の順にクリックします。
- 3 変更する権利継承フィルタを持つオブジェクトの名前およびコンテキストを指定して、[OK] をクリックします。

これで、すでにオブジェクトに設定された権利継承フィルタのリストが表示されます。


- 4 プロパティページで、必要に応じて権利継承フィルタのリストを編集します。  
フィルタのリストを編集するには、オブジェクトの ACL プロパティへのスーパーバイザ権またはアクセス制御権を持っている必要があります。オブジェクトの継承された権利を全体的にブロックするフィルタは、オブジェクトのすべてのプロパティおよび個々のプロパティに対して設定できます。

注：フィルタによって、このオブジェクトのトラスティに明示的に付加された権利がブロックされることはありません。これらの権利は継承されるものではないからです。

- 5 [OK] をクリックします。

## eDirectory オブジェクトまたはプロパティへの有効な権利を参照する

有効な権利は、ユーザーが特定のネットワークリソース上で実行できる実際の権利です。有効な権利は、明示的な権利の割り当て、継承、および同等セキュリティを基に、eDirectory によって計算されます。システムにクエリを設定すると、リソースへのユーザーの有効な権利が決定されます。

- 1 Novell iManager で、[役割およびタスク] ボタン  をクリックします。
- 2 [権利] > [有効な権利の表示] の順にクリックします。
- 3 参照する有効な権利を持つトラスティの名前とコンテキストを入力し、[OK] をクリックします。
- 4 次のオプションから選択します。

| オプション                | 説明  |
|----------------------|---|
| プロパティ名               | <p>トラスティが有効な権利を持つプロパティを表示します。プロパティは eDirectory から読み込まれるため、通常英語で表示されます。リストの個々のアイテムは次のタイプのいずれかです。</p> <p>[すべての属性権] – オブジェクトのすべてのプロパティを表示します。</p> <p>[エントリ権] – オブジェクト全体を表示します。スーパーバイザの場合を除き、このアイテムへの権利にはプロパティの権利は含まれません。</p> <p>特定のプロパティ – トラスティが個々に権利を持つ特定のプロパティです。デフォルトでは、このオブジェクトクラスのプロパティのみが表示されます (次を参照)。</p> |
| 有効な権利                | <p>eDirectory で計算されたとおりに、選択されたプロパティへのトラスティの有効な権利を表示します。</p>   |
| スキーマ内のすべてのプロパティを表示する | <p>このチェックボックスをオフにしておくと、このオブジェクトクラスのプロパティのみが表示されます。</p> <p>eDirectory スキーマで定義されたすべてのクラスのプロパティを表示するには、このチェックボックスをオンにします。追加のプロパティが有効になるのは、このオブジェクトがコンテナである場合、またはそれが拡張されて補助クラスのプロパティを含む場合のみです。追加のプロパティの横には行頭文字は表示されません。</p>   |

5 [完了] をクリックします。



# 2

## Novell eDirectory ネットワークの設計

Novell® eDirectory™ の設計は、事実上、ネットワークのすべてのユーザおよびリソースに影響を与えます。eDirectory の設計が良ければ、ネットワークの効率性、耐障害性、安全性、拡張性、機能性が高まり、それによってネットワーク全体のパフォーマンスと価値が向上します。この章では、eDirectory ネットワーク設計上のヒントについて説明します。

- ◆ 73 ページの「eDirectory 設計の基本」
- ◆ 74 ページの「eDirectory ツリーの設計」
- ◆ 80 ページの「ツリーのパーティション化のガイドライン」
- ◆ 82 ページの「ツリーのレプリカ作成に関するガイドライン」
- ◆ 85 ページの「ユーザ環境についてのプランニング」
- ◆ 86 ページの「e ビジネスに対応する eDirectory の設計」
- ◆ 87 ページの「Novell Certificate Server について」
- ◆ 91 ページの「ネットワーク時刻の同期」

### eDirectory 設計の基本

効率のよい eDirectory 設計の基盤となるのは、ネットワークのレイアウト、会社の組織構造、および適切な準備です。

e ビジネス用に eDirectory を設計する場合は、86 ページの「e ビジネスに対応する eDirectory の設計」を参照してください。

### ネットワークのレイアウト

ネットワークのレイアウトとは、ネットワークの物理的な設定のことです。効率のよい eDirectory を設計するには、次の項目について考慮する必要があります。

- ◆ WAN リンク
- ◆ リモートアクセスを必要とするユーザ
- ◆ ネットワークリソース (サーバ数など)
- ◆ 頻繁な停電など、ネットワークの状態
- ◆ 予測されるネットワークレイアウトの変更

## 組織の構造

組織の構造は、eDirectory の設計に影響します。効率的な eDirectory を設計するには、次が必要になります。

- ◆ 組織図および運営形態についての理解
- ◆ eDirectory の設計および実装を完了するのに必要な技能のある担当者  
次の技能を持った担当者を選出する必要があります。
  - ◆ eDirectory 設計の焦点およびスケジュールの管理
  - ◆ eDirectory の設計、設計標準、およびセキュリティについての理解
  - ◆ 物理的なネットワーク構造の理解および管理
  - ◆ インターネットワークのバックボーン、テレコミュニケーション、WAN 設計、およびルータ配置の管理

## eDirectory 設計の準備をする

eDirectory の設計に実際に着手する前に、次を実行します。

- ◆ スコープおよびスケジュールの現実的な見積もりの設定
- ◆ eDirectory 実装の設計によって影響があるすべてのユーザへの連絡
- ◆ 73 ページの「ネットワークのレイアウト」および 74 ページの「組織の構造」の情報の参照

## eDirectory ツリーの設計

ネットワークの設計と実装で最も重要な作業は、eDirectory ツリーの設計です。ツリーの設計には、次の作業が含まれます。

- ◆ 74 ページの「命名標準ドキュメントを作成する」
- ◆ 77 ページの「Tree の上位層を設計する」
- ◆ 79 ページの「ツリーの下位層を設計する」

## 命名標準ドキュメントを作成する

オブジェクト名などの標準名を規定すると、ユーザと管理者の両方が、ネットワークをより直感的に理解できるようになります。書き出された標準では、管理者による、電話番号や住所などの他のプロパティ値の設定方法も指定できます。

ディレクトリの検索とブラウズでは、名前やプロパティ値の整合性が重要になります。

また、標準的な名前を使用することで、Novell Nsure Identity Manager では、eDirectory とその他のアプリケーションの間でデータを容易に移動することもできます。Novell Nsure Identity Manager の詳細については、『*DirXML 管理ガイド*』(<http://www.novell.com/documentation/dirxml20/index.html>) を参照してください。

### オブジェクト

- ◆ コンテナ内では、重複する名前を使用することはできません。たとえば、同じコンテナ内で Debra Jones と Daniel Jones の両方に「DJONES」という名前を付けることはできません。
- ◆ 特殊文字を使用できます。ただし、プラス記号 (+)、等号 (=)、およびピリオド (.) を使用する場合は、直前に円記号 (¥) を入力する必要があります。サーバオブジェクトと国オブジェクトのほか、バインダリサービスおよび多言語環境には、追加の命名規則が適用されます。
- ◆ 大文字と小文字、およびアンダースコアとスペースは、入力時にはそのまま表示されますが、実際には区別されません。たとえば、「Manager\_Profile」と「MANAGER PROFILE」は同一と見なされます。
- ◆ 名前をコマンドラインやログインスクリプトに入力するときにスペースを使用する場合は、名前全体を引用符で囲む必要があります。

### サーバオブジェクト

- ◆ 新しいサーバをインストールすると、サーバオブジェクトが自動的に作成されます。
- ◆ 既存の NetWare® や NT サーバ、および他のツリーの eDirectory サーバに対して、追加のサーバオブジェクトを作成できますが、それらはすべてバインダリオブジェクトとして扱われます。
- ◆ サーバオブジェクトを作成するとき、その名前は物理サーバ名と一致していなければなりません。また、サーバ名には次の規定があります。
  - ◆ ネットワーク全体で固有である
  - ◆ 2～47 文字の長さである
  - ◆ A～Z までの文字、0～9 までの数字、ハイフン (-)、ピリオド (.)、およびアンダースコア (\_) のみを含む
  - ◆ 最初の文字にピリオドを使用しない
- ◆ 一度付けたサーバオブジェクト名は、iManager で変更することはできません。サーバで名前を変更すると、新しい名前が自動的に iManager に表示されます。

### 国オブジェクト

国オブジェクトは、2 文字の標準 ISO カントリーコードに従って命名します。

詳細については、[ISO 3166 Code Lists \(http://www.iso.ch/iso/en/prods-services/iso3166ma/02iso-3166-code-lists/list-en1.html\)](http://www.iso.ch/iso/en/prods-services/iso3166ma/02iso-3166-code-lists/list-en1.html) を参照してください。

### バインダリオブジェクト

NetWare 2 または NetWare 3 からバインダリサービス経由でオブジェクトにアクセスする場合は、次の制限が適用されます。

- ◆ 名前に使用されているスペースは、アンダースコアに置き換えられる。
- ◆ 名前は 47 文字で切り捨てられる。
- ◆ 次の文字は使用できない。スラッシュ (/)、円記号 (¥)、コロン (:)、コンマ (,)、アスタリスク (\*)、および疑問符 (?)。

**重要:** バインダリエミュレーションは、Linux、Solaris、AIX、HP-UX プラットフォームではサポートされていません。

## 多言語環境の注意事項

複数の言語で稼動しているワークステーションがある場合は、必要に応じて、オブジェクト名に使用する文字を、すべてのワークステーションで表示できる文字のみに制限します。たとえば、ワークステーションを日本語環境で使用している場合には、ヨーロッパの言語で表示できない文字を名前に使用しないよう制限します。

HP-UX は英語のみをサポートします。

**重要:** Tree 名は必ず英語で指定するようにします。

## 標準ドキュメントの例

次は、最もよく使用される一部のプロパティに関する標準ドキュメントの例です。使用しないプロパティについては、標準を規定する必要はありません。標準ドキュメントは、オブジェクトの作成または修正を担当するすべての管理者に配布します。

| オブジェクトクラス   プロパティ [標準] | 例  | 理由  |
|------------------------|--|---|
| ユーザ   ログイン名            | ファーストネームのイニシャル、ミドルネームのイニシャル(ある場合)、姓の組み合わせ(すべて小文字)。最大 8 文字です。各共通名はすべて、社内全体で固有のものにします。 | msmith, bjohnson<br>eDirectory では会社全体で固有の名前を使用する必要はありませんが、固有にすると、同じコンテキスト(またはバインダリコンテキスト)内での不整合を避けることができます。 |
| ユーザ   姓                | 姓(通常の大文字/小文字表記)。   | Smith<br>メールラベルの生成に使用されます。  |
| 電話番号および Fax 番号         | ハイフンで区切られた番号。  | 米国: 123-456-7890<br>その他: 44-344-123456<br>自動ダイヤルソフトウェアで使用されます。  |
| 複数のクラス   地域            | 2 文字の地域コード(大文字)、ハイフン、メール配達地点の組み合わせ。  | BA-C23<br>社内のメール配達で使用されます。  |
| 組織   名前                | すべてのツリーに与える会社名。  | YourCo<br>独立したツリーがある場合、標準の組織名を使用することで、将来ツリーのマージができます。   |
| 部門   名前(地域に基づく)        | 2 または 3 文字の地域コードで、すべて大文字。  | ATL, CHI, CUP, LA, BAT, BOS, DAL<br>短く、標準的な名前を使用することで、効率的に検索できます。   |
| 部門   名前(部署に基づく)        | 部署名または略語。  | Sales, Eng<br>短く、標準的な名前を使用することで、どの部署で使用しているコンテナが見分けやすくなります。   |
| グループ   名前              | 識別名。   | Project Managers<br>ユーティリティによってはすべて表示できない場合があるため、極端に長い名前は避けます。  |
| ディレクトリマップ   名前         | ディレクトリマップが示すディレクトリの内容。   | DOSAPPS<br>短く、標準的な名前を使用することで、どの部署で使用しているコンテナが見分けやすくなります。  |



| オブジェクトクラス   プロパティ [標準] |                               | 例          | 理由  |
|------------------------|-------------------------------|------------|---|
| プロファイル   名前            | プロファイルの目的。                    | MobileUser | 短く、標準的な名前を使用することで、どの部署で使用しているコンテナが見分けやすくなります。 |
| サーバ   名前               | SERV、ハイフン、部署、ハイフン、固有番号の組み合わせ。 | SERV-Eng-1 | eDirectory では、ツリー内で固有のサーバ名を使用する必要があります。       |

## Tree の上位層を設計する

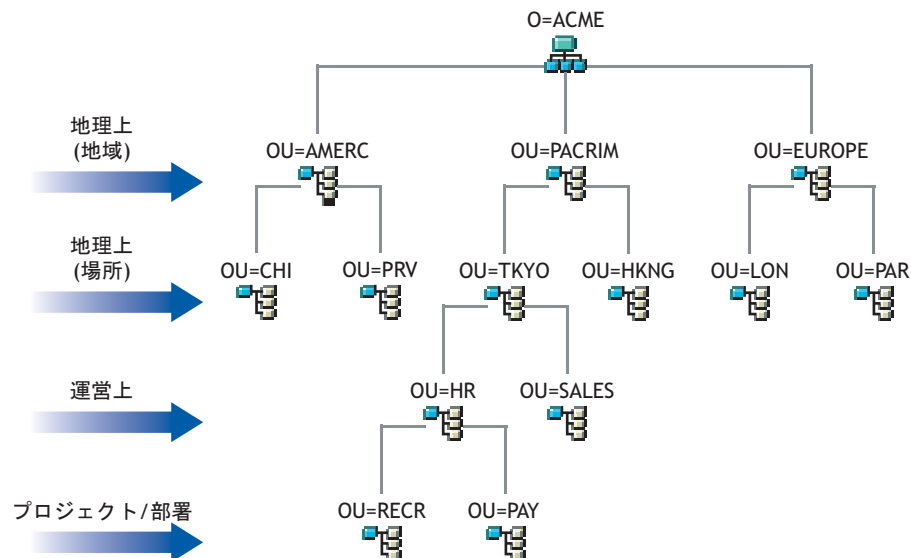
ツリーの上位層を変更するとツリーの残りの部分すべてに影響するため、ツリーの上位層は慎重に設計します。WAN リンクがある場合は、特に注意する必要があります。ツリーの最上部は、後からの変更がなるべく必要でないように設計します。

eDirectory ツリーの作成時には、次の eDirectory 設計規則に従います。

- ◆ ピラミッド型の設計を使用する。
- ◆ eDirectory ツリーは 1 つにし、固有の名前を付ける。
- ◆ 組織オブジェクトを 1 つ作成する。
- ◆ 物理的なネットワーク構造を表す第 1 レベルの部門群を作成する。

図 21 は、eDirectory 設計規則を示しています。

図 21 eDirectory 設計規則



ツリーの上位層を作成するには、98 ページの「オブジェクトを作成する」および 99 ページの「オブジェクトのプロパティを変更する」を参照してください。

## ピラミッド型の設計の使用

ピラミッド型の eDirectory では、管理や、大きなグループに対する変更、および論理パーティションの作成をより容易に実行できます。

ピラミッド型以外の設計として、フラットツリー型があります。この場合、すべてのオブジェクトがツリーの最上部に置かれます。eDirectory をフラットツリー型に設計することも可能ですが、管理やパーティション化がより難しくなります。

## 固有の名前を持つ単一の eDirectory ツリーの使用

ほとんどの組織では、ツリーを 1 つにするのが最適です。デフォルトでは、ツリーは 1 つだけ作成されます。ツリーが 1 つだけだと、ネットワーク内のユーザの識別を統一でき、セキュリティ管理もより容易になります。また、1 箇所で集中管理できます。

業務では単一のツリーの使用を推奨しますが、追加のツリーのテストや開発を否定するわけではありません。

組織によっては、法的または政治的な問題、あるいは社内の事情から、複数のツリーが必要になる場合もあります。たとえば、自立した 7 つの組織から構成される組織では、7 つのツリーが必要になることも考えられます。組織で複数のツリーが必要な場合は、Novell Nsure Identity Manager を使用して管理を容易化することを検討してください。Novell Nsure Identity Manager の詳細については、『[DirXML 管理ガイド](http://www.novell.com/documentation/dirxml20/index.html)』 (<http://www.novell.com/documentation/dirxml20/index.html>) を参照してください。

**注：** HP-UX は Novell Nsure Identity Manager をサポートしていません。

ツリーには、他のツリー名と重複しない、固有の名前を付けます。「EDL-TREE」のように、短くてわかりやすい名前を指定します。

同じネットワーク内に同じ名前のツリーが存在すると、次のような問題が発生する場合があります。

- ◆ 更新内容が、対象のツリーとは別のツリーに適用される
- ◆ リソースが消失する
- ◆ 権利が消失する
- ◆ データが破損する

ツリー名は、DSMerge ユーティリティで変更できますが、変更は十分に注意して行ってください。ツリー名の変更はネットワーク全体に影響します。ツリー名を変更した場合は、新しいツリー名でクライアントを再設定する必要があります。

## 単一の組織オブジェクトの作成

通常、1 つの eDirectory ツリーには、1 つの組織オブジェクトを作成します。デフォルトでは、組織オブジェクトが 1 つ作成され、それに会社名に基づいた名前が付けられます。これにより、会社全体に適用される変更をツリー内の 1 箇所から設定できます。

たとえば、ZENworks<sup>®</sup> を使用して、組織オブジェクトの下に、ワークステーションインポートポリシーオブジェクトを作成できます。このポリシーは、eDirectory 内にワークステーションオブジェクトを作成するときの命名方法を定義するもので、組織全体に影響します。

組織コンテナには、次のオブジェクトが作成されます。

- ◆ 管理者
- ◆ サーバ
- ◆ ボリューム

eDirectory が実行されている Windows、Linux、Solaris、AIX、または HP-UX サーバのみを含むネットワークには、ボリュームオブジェクトはありません。

次のようなケースでは、組織オブジェクトを複数作成することが必要になる場合があります。

- ◆ 複数の会社から構成される企業で、それぞれの会社が個別にネットワークを構成している。
- ◆ 社内で、独立した業務単位または組織を表す必要がある。
- ◆ 各部門が独立した形態をとることを規定する社内ガイドラインやポリシーがある。

## 物理的なネットワークを表す部門を作成する

第 1 レベルの部門設計は、eDirectory の効率性とパーティション化に影響するため重要です。

LAN または WAN を使用して複数のビルや場所などにまたがって構成されているネットワークでは、所在地に基づいて第 1 レベルの部門オブジェクトを設計します。これにより、1 つのパーティション内のすべてのオブジェクトが 1 箇所に維持されるように、eDirectory を分割できます。また、各場所でのセキュリティの設定や管理者の割り当ても容易になります。

## ツリーの下位層を設計する

ツリーの下位層は、ネットワークリソースの編成に基づいて設計します。eDirectory ツリーの下位層の設計は同じ場所に存在するオブジェクトにのみ影響するため、下位層は上位層よりも自由に設計できます。

ツリーの下位層を作成するには、[98 ページの「オブジェクトを作成する」](#) および [99 ページの「オブジェクトのプロパティを変更する」](#) を参照してください。

## コンテナ、ツリー、およびデータベースのサイズを決定する

作成する下位層のコンテナオブジェクトの数は、ツリー内のオブジェクトの総数、空きディスク容量、およびディスクの入出力速度制限によって決まります。eDirectory は、1 つの eDirectory ツリー内に 10 億以上のオブジェクトを格納できることがテストで確認されているため、実際の制約項目は、空きディスク容量とディスクの入出力速度、およびパフォーマンスを維持するための RAM です。大規模なツリーの場合は、レプリカの同期処理が大きく影響することにも注意が必要です。

eDirectory 内の一般的なオブジェクトのサイズは 3 ~ 5KB です。この数値に基づいて、現在保持している、または新たに作成するすべてのオブジェクトの保管に必要な空きディスク容量をすばやく計算できます。オブジェクトのサイズは、データに付属する属性の数や、データの内容に対応して大きくなります。画像やサウンド、または生物統計学などの BLOB (バイナリラージオブジェクト) データを格納するオブジェクトの場合、そのサイズは増加します。

パーティションのサイズが大きくなるほど、レプリケーションのサイクルは遅くなります。ZENworks や DNS/DHCP サービスなど、eDirectory の使用を必要とする製品を使用する場合、これらの製品によって作成された eDirectory オブジェクトにより、格納先のコンテナのサイズが影響を受けます。場合によっては、DNS/DHCP など、管理目的のみで使用するオブジェクトは固有のパーティションに格納することを検討します。パーティションを別にすれば、レプリカの同期処理の速度の低下によってユーザのアクセスが支障をきたすことを避けることができます。また、パーティションとレプリカの管理も容易になります。

必要な場合は、eDirectory データベースまたは DIB (ディレクトリ情報ベース) セットのサイズを簡単に判別できます。

- ◆ NetWare の場合は、Novell Support Web サイト (<http://support.novell.com>) から toolbox.nlm をダウンロードして、サーバ上の sys:\_netware ディレクトリを表示します。
- ◆ Windows の場合は、¥novell¥nds¥dibfiles にある DIB セットを参照します。
- ◆ Linux、Solaris、AIX、または HP-UX の場合は、インストール時に指定したディレクトリにある DIB セットを参照してください。

## 作成するコンテナを決定する

通常、同じ必要性からアクセスされる eDirectory オブジェクトをまとめて格納するコンテナを作成します。それにより、1つのトラスティ割り当てまたはログインスクリプトで多くのユーザにサービスを提供できます。特にログインスクリプトをより効率的にすることを目的としてコンテナを作成できるほか、1つのコンテナに2つの部署を割り当てることによって、ログインスクリプトの管理をより容易にすることもできます。

ネットワーク内のトラフィックを制限するため、ユーザは各自が必要とするリソースの近くに配置するようにします。たとえば、同じ部署で働く社員は、通常、隣り合った位置で作業します。それらの社員は同じファイルシステムにアクセスし、同じプリンタを使用して印刷します。

一般的なワークグループ境界の例外については、容易に対処できます。たとえば、2つのワークグループが共通のプリンタを使用するような場合は、一方のワークグループのプリンタに対して別名オブジェクトを作成します。グループオブジェクトを作成することによって、1つのワークグループ内だけでなく、複数のワークグループに存在する一部のユーザオブジェクトをまとめて管理できます。また、固有のログインスクリプト要件を持つ、一部のユーザ用のプロファイルオブジェクトも作成できます。

## ツリーのパーティション化のガイドライン

eDirectory にパーティションを作成すると、データベースの各部分は複数のサーバに分割して格納されます。パーティション化によって、eDirectory データ処理と保管の負荷がネットワーク内の複数のサーバに分散されるため、ネットワークの使用を最適化できます。デフォルトでは、パーティションは1つだけ作成されます。パーティションの詳細については、[49 ページの「パーティション」](#)を参照してください。パーティションの作成については、[135 ページの第 5 章「パーティションおよびレプリカの管理」](#)を参照してください。

次のガイドラインは、ほとんどのネットワークに適用できる一般的な規則です。特定の環境設定、ハードウェア、およびトラフィックの処理量など、それぞれのネットワークの運用条件に合わせて若干の調整が必要になる場合もあります。

## ツリーの上位層におけるパーティションを決定する

ツリーをピラミッド型に設計すると同じように、パーティションもピラミッド型に構成します。パーティションの構造は、ツリーの最上位に少数のパーティションがあり、下位になるに従ってパーティションの数が増えていくようにします。このような設計では、下位層より上位層のほうがパーティション数が多いツリー構造に比べて、作成されるサブオーディネートリファレンスの数が少なくなります。

ツリーをピラミッド型に設計するには、常にリーフオブジェクト (特にユーザ) の比較的近くにパーティションを作成するようにします (インストール時にツリーのルートに作成されるパーティションについては例外です)。

上位層のパーティションを設計する場合は、次の点を考慮します。

- ◆ WAN インフラストラクチャに基づいて、ツリーの最上部をパーティション化する。ツリーの最上部にはパーティションを少なめに配置し、下位になるに従ってパーティションの数を増やします。

WAN リンクによって区切られている各サイトのコンテナを作成し (各サーバオブジェクトをそのローカルコンテナに格納)、その後、各サイトのパーティションを作成します。

- ◆ WAN リンクを持つネットワークでは、パーティションが複数の場所にまたがらないようにする。

パーティションを場所ごとに作成すれば、異なるサイト間のレプリケーショントラフィックによって WAN 帯域幅が不必要に消費されることはありません。

- ◆ ローカルサーバを中心にパーティションを作成する。物理的に離れた場所にあるサーバは別のパーティションに格納します。

WAN トラフィック管理の詳細については、[293 ページの第 11 章「WAN トラフィックマネージャ」](#)を参照してください。

## ツリーの下位層におけるパーティションを決定する

eDirectory ツリーの下位層のパーティションを設計する場合は、次を考慮します。

- ◆ 下位層のパーティションは、事業部、部署、およびワークグループと、それらに関連するリソースに基づいて定義する。
- ◆ 各パーティションについて、パーティション内のすべてのオブジェクトが同じ場所にあるようにする。それによって、eDirectory への更新がローカルサーバで行われるようになります。

## パーティションサイズを決定する

eDirectory では、パーティションのサイズについて次の設計制限を推奨しています。

| エレメント           | 制限   |
|-----------------|--|
| パーティションのサイズ     | 無制限のオブジェクト<br>レプリカ DIB (ディレクトリ情報ベース) は 1TB に制限 |
| ツリー内のパーティションの総数 | 無制限  |

| エレメント                        | 制限                   |
|------------------------------|----------------------|
| ペアレントパーティションごとのチャイルドパーティション数 | 150                  |
| パーティションごとのレプリカ数              | 50<br>レプリカ DIB による制限 |
| レプリカサーバごとのレプリカ数              | 250                  |

NDS® 6 および 7 からのこの設計ガイドラインの変更は、NDS 8 におけるアーキテクチャの変更によるものです。これらの推奨値は、企業などの分散環境に適用されます。ただし、これらは e ビジネスやアプリケーションには適用されない場合があります。

一般的な e ビジネスユーザに対しては、すべてのデータが単一のサーバに保管されていることが必要ですが、eDirectory では、ツリー内のさまざまなエリアに属するオブジェクトや属性の一部を格納するフィルタ済みレプリカを作成できます。この機能を利用すると、1 つのサーバにすべてのデータを保管しなくても、同じように e ビジネスに対応できます。詳細については、[56 ページの「フィルタ済みレプリカ」](#)を参照してください。

## ネットワーク変数について

パーティションを設計する場合は、次のネットワーク変数について考慮します。

- ◆ サーバの数および速度
- ◆ ネットワークアダプタ、ハブ、ルータなどのネットワークインフラストラクチャの速度
- ◆ ネットワークトラフィックの量

## ツリーのレプリカ作成に関するガイドライン

複数の eDirectory パーティションを作成するだけでは、耐障害性やディレクトリのパフォーマンスは向上しません。耐障害性やパフォーマンスの向上は、複数のレプリカを効果的に使用することで可能になります。レプリカの配置は、アクセスや耐障害性にとってきわめて重要です。eDirectory のデータには、できるだけすばやくアクセスできるようにする必要があります。また、eDirectory のデータは障害対策用に複数の場所にコピーする必要があります。レプリカの作成については、[135 ページの第 5 章「パーティションおよびレプリカの管理」](#)を参照してください。

レプリカの配置計画では、次のガイドラインを参考にしてください。

- ◆ [83 ページの「ワークグループのニーズ」](#)
- ◆ [83 ページの「障害対策」](#)
- ◆ [84 ページの「レプリカ数を決定する」](#)
- ◆ [84 ページの「Tree パーティションのレプリカを作成する」](#)
- ◆ [84 ページの「管理用にレプリカを作成する」](#)
- ◆ [84 ページの「NetWare のバインダリサービスの必要性に対応させる」](#)
- ◆ [85 ページの「WAN トラフィックを管理する」](#)

## ワークグループのニーズ

各パーティションのレプリカを、そのパーティション内の情報を使用するワークグループに物理的に近いサーバ上に作成します。WAN リンクの一方向の側のユーザが他方の側のサーバに格納されているレプリカに頻繁にアクセスする場合は、WAN リンクの両端のサーバ上にそれぞれレプリカを作成します。

レプリカは、ユーザ、グループ、およびサービスによるアクセスが最も多い場所に配置します。2つの独立したコンテナ内の各ユーザグループが別のパーティション境界内の同じオブジェクトにアクセスする必要がある場合は、これらのユーザグループが属する2つのコンテナより1つ上のレベルにあるコンテナ内のサーバ上にレプリカを配置します。

## 障害対策

ディスクがクラッシュしたり、サーバがダウンした場合、別の場所にあるサーバ上のレプリカによりユーザのネットワークへの認証を行い、使用不能になったサーバに格納されているパーティション内のオブジェクトの情報を取得できます。

いくつかのサーバに同じ情報が配布されていると、ユーザのネットワークへの認証やログインなどのサービスを提供するために、1つのサーバに依存する必要がありません。

耐障害性を確保するには、ディレクトリツリーに十分な数のサーバがあれば、各パーティションについて3つのレプリカを作成します。ローカルパーティションのローカルレプリカは、最低2つは必要です。他の場所にあるデータへのアクセスを確保する場合や、負荷分散および障害対策用にデータのインスタンスを複数維持する必要があるアプリケーションを使用している場合、またeビジネスを展開している場合を除いて、通常は、レプリカの作成は3つまでで十分です。

マスタレプリカは1つだけ保持できます。その他のレプリカは、読み書き可能、読み込み専用、またはフィルタ済みレプリカとして使用します。通常、ほとんどのレプリカは、読み書き可能レプリカとして使用されます。読み書き可能レプリカは、マスタレプリカ同様、オブジェクトの表示、オブジェクトの管理、およびユーザのログインを処理できます。変更があったときは、同期化情報を送信します。

読み込み専用レプリカには、書き込みはできません。読み込み専用レプリカは、オブジェクトを検索および表示できます。また、パーティションのレプリカの同期が実行されると、更新されます。

サブオーディネートリファレンスレプリカやフィルタ済みレプリカは、障害対策用にはなりません。サブオーディネートリファレンスはポイントであり、パーティションのルートオブジェクト以外のオブジェクトは格納されません。フィルタ済みレプリカには、パーティション内の特定の一部のオブジェクトのみが格納されます。

eDirectory では、パーティションごとに数に制限なくレプリカを作成できますが、レプリカの数が増えるに従って、ネットワークトラフィックの量も増大します。障害対策とネットワークパフォーマンス、それぞれの必要性をバランスよく配慮します。

サーバ上の各パーティションには、レプリカを1つだけ格納できます。1つのサーバには、複数のパーティションのレプリカを格納できます。

障害発生によって、特定の場所のすべてのデータまたはその中のいずれかのサーバ上のデータが失われた場合、その組織の障害回復計画に基づくネットワーク再構築のほとんどの作業は、パーティションのレプリカを使用して行うことができます。サーバが1つしかない場所では、eDirectory を定期的にバックアップします(一部のバックアップソフトウェアでは、eDirectory のバックアップアップが実行されません)。障害対策用のレプリカを作成するための、追加サーバの購入を検討してください。



## レプリカ数を決定する

複数のレプリカの作成を制限する要素となるのは、それぞれのレプリカの同期で必要となる処理時間とトラフィックの量です。オブジェクトが変更されると、変更内容がレプリカリング内のすべてのレプリカに伝達されます。レプリカリング内のレプリカの数が多いほど、変更内容の同期に必要なデータの伝送量も増えます。WAN リンク経由でレプリカを同期する必要がある場合、同期にかかる時間のコストが高くなります。

地理上の多くの場所のパーティションを作成した場合、一部のサーバでサブオーディネートリファレンスレプリカが数限りなく生成されることになります。eDirectory では、地域のパーティションを作成することによって、これらのサブオーディネートリファレンスをより多くのサーバに分散させることができます。

## Tree パーティションのレプリカを作成する

Tree パーティションは eDirectory ツリー内の最も重要なパーティションです。このパーティションの唯一のレプリカが破損した場合、そのパーティションが修復されるか、eDirectory ツリー全体が再構築されるまで、ネットワークの機能が停止します。また、Tree に関連する設計の変更はまったくできなくなります。

Tree パーティションのレプリカの作成時には、サブオーディネートリファレンスの同期にかかるコストを考慮しながら、レプリカ数を決めてください。

## 管理用にレプリカを作成する

パーティションの変更はマスタレプリカからのみ発生するため、中央サイトのネットワーク管理者のすぐ近くにあるサーバに各マスタレプリカを保管するようにします。一見、それぞれのリモートサイトにマスタを保管するほうが適切のように思えますが、マスタレプリカはパーティションの操作が行われる場所に保管するのが妥当です。

パーティション作成などの重要な eDirectory の操作は、中央サイトの特定の管理者または管理者グループが担当することを推奨します。担当者を限定することによって、eDirectory の動作を悪化させるエラーの発生の可能性を制限できるほか、マスタレプリカを中央で一括してバックアップできます。

ネットワーク管理者は、ネットワークトラフィックが少ない時間帯を選んで、レプリカの作成などのコストの高い操作を実行します。

## NetWare のバインダリサービスの必要性に対応させる

NetWare で eDirectory を使用する場合に、ユーザがバインダリサービスを通してサーバにアクセスする必要があるときは、そのサーバにバインダリコンテキストを格納するマスタレプリカまたは読み書き可能レプリカが保管されている必要があります。バインダリコンテキストは、autoexec.ncf 内の SET BINDERY CONTEXT ステートメントによって設定されます。

ユーザは、実オブジェクトがそのサーバ上に存在する場合のみ、バインダリサービスを提供するオブジェクトにアクセスできます。パーティションのレプリカをサーバに追加すると、サーバに実オブジェクトが追加されます。それにより、そのパーティションにユーザオブジェクトを持つユーザは、バインダリ接続によってサーバにログインできるようになります。

バインダリサービスの詳細については、57 ページの「[NetWare バインダリエミュレーション](#)」を参照してください。



## WAN トラフィックを管理する

現在、ユーザが WAN リンクを使用して特定のディレクトリ情報にアクセスしている場合、必要な情報を格納するレプリカをユーザのローカルサーバに作成することによって、ユーザのアクセス時間と WAN トラフィックの量を削減できます。

マスタレプリカをリモートサイトに複製する場合や、アクセスの提供や障害対策用に WAN 経由でレプリカを配置する場合には、レプリカの同期処理で使用される帯域幅について考慮します。

推奨する 3 つのレプリカの作成がローカルサイトで不可能な場合に耐障害性を確保するため、アクセス可能性を高めるため、またマスタレプリカを中央で一括して管理および保管するためにのみ、ローカルサイト以外の場所にレプリカを作成します。

WAN リンク上の eDirectory トラフィックのレプリケーションを制御するには、WAN マネージャを使用できます。詳細については、[293 ページの第 11 章「WAN トラフィック マネージャ」](#)を参照してください。

## ユーザ環境についてのプランニング

eDirectory ツリーの基本構造を設計し、パーティションとレプリカを設定した後は、管理を単純化し、ネットワークリソースへのアクセスを容易にするためのユーザ環境の設定プランを立てます。ユーザ環境プランを立てるには、各ユーザの必要条件を検討し、エリアごとにアクセスに関するガイドラインを作成します。

### ユーザの必要条件を検討する

ユーザが必要とする条件を検討する際には、次の点について考慮します。

- ◆ プリンタやファイル保管領域など、物理的なネットワークに関する必要条件  
1 つのツリー内の複数のユーザグループ、または複数のコンテナに属する複数のユーザグループによってリソースが共有されていないか確認します。また、リモートユーザが必要とする物理的なリソースについても考慮します。
- ◆ NetWare ユーザのバインダリサービスに関する必要条件  
バインダリサービスに基づくアプリケーションはどれか、またどのユーザによって使用されるか確認します。
- ◆ アプリケーションに関する必要条件  
ユーザが必要とするアプリケーションおよびデータファイルはどれか、オペレーティングシステムは何か、またアプリケーションにアクセスする必要があるユーザまたはユーザグループは誰かを確認します。共有アプリケーションを、ZENworks などのアプリケーションによって自動で起動するのか、または手動で起動するのか確認します。

### アクセスに関するガイドラインを作成する

ユーザの必要条件についての情報を収集した後は、ユーザ環境の構成に使用する eDirectory オブジェクトを決定します。たとえば、ポリシーパッケージやアプリケーションオブジェクトを作成する場合は、作成数、およびツリー内の保管先について決定します。

また、ユーザのアクセスを制限するセキュリティの実装方法についても決める必要があります。個々のセキュリティ項目に関連する、セキュリティ上の予防措置がないか検討します。たとえば、eDirectory スーパーバイザ権はファイルシステムによって継承されるため、サーバオブジェクトに対してはスーパーバイザ権を付与しないよう、ネットワーク管理者に警告する場合があります。

## e ビジネスに対応する eDirectory の設計

eDirectory を e ビジネスに利用する場合 ( サービスのポータルを提供したり、他の企業とデータを共有する場合など )、この章ですでに説明している推奨事項は適用されないことがあります。

その場合は、e ビジネスに対応する eDirectory の設計のガイドラインとして次に示す推奨事項を代わりに使用できます。

- ◆ コンテナ数を制限したツリーを作成する。

このガイドラインは、使用するアプリケーション、および eDirectory の実装法に応じて適用します。たとえば、メッセージサーバをグローバルに展開する際には、この章の前半で説明した従来の eDirectory 設計ガイドラインを適用したほうがより適切な場合があります。また、ユーザの管理を分散させたい場合は、管理責任のエリアごとに独立した OU ( 部門 ) を作成することが必要になる場合があります。

- ◆ 最低 2 つのパーティションを維持する。

Tree レベルに作成されるデフォルトのパーティションを維持し、その他にツリーの残りの部分のパーティションを作成します。管理目的で OU を個別に作成した場合は、各 OU のパーティションを作成します。

複数のサーバに負荷を分散させる際には、パーティション数の制限を検討しますが、その場合もバックアップや障害回復用に最低 2 つのパーティションは維持します。

- ◆ 障害対策および負荷分散のために、ツリーのレプリカを最低 3 つ作成する。

LDAP は負荷の分散を自動では行いません。LDAP の負荷を分散させるには、第 4 層スイッチの使用を検討します。

- ◆ e ビジネス用のツリーを別に作成する。サーバやプリンタなど、ツリーに組み込むネットワークリソースを制限する。ユーザオブジェクトのみを格納するツリーの作成を検討する。

Novell Nsure Identity Manager を使用すると、ネットワーク情報を格納する他のツリーにこのユーザツリーをリンクさせることができます。詳細については、『[DirXML 管理ガイド](http://www.novell.com/documentation/dirxml20/index.html)』(<http://www.novell.com/documentation/dirxml20/index.html>) を参照してください。

- ◆ 補助クラスを使用して、スキーマをカスタマイズする。

カスタマやアプリケーションで標準 inetOrgPerson とは異なるユーザオブジェクトが必要となる場合は、補助クラスを使用してスキーマをカスタマイズします。補助クラスを使用すると、アプリケーションの設計時にツリーを再作成しなくても、クラスで使用する属性を変更できます。

- ◆ LDIF インポートのパフォーマンスを向上させる。

Novell インポート / エクスポート変換ユーティリティを使用すると、eDirectory は処理中に各オブジェクトに索引を付けます。それによって、LDIF インポートプロセスの処理速度が遅くなる場合があります。LDIF インポートのパフォーマンスを向上させるには、作成するオブジェクトの属性からの索引付けをいったん中止し、Novell インポート / エクスポート変換ユーティリティを使用してから、属性の索引付けを再開します。

- ◆ NDS 全体で固有の共通名 (CN) を実装する。

eDirectory では、異なるコンテナ間で同じ共通名を使用できます。ただし、全体で固有の共通名を使用すれば、共通名の検索で複数の応答を処理するロジックを実装しなくて済みます。

# Novell Certificate Server について

Novell Certificate Server™ では、セキュリティコンテナオブジェクトと組織の認証局 (CA) オブジェクトを作成することによって、デジタル証明書を作成、発行、および管理できます。組織の認証局オブジェクトにより、データを保護し、安全に伝送できるようになります。NetWare Web Manager や NetWare Enterprise Web Server などの Web 関連製品には、組織の認証局オブジェクトが必要です。eDirectory サーバを初めてインストールすると、eDirectory ツリー全体のセキュリティコンテナオブジェクトと組織の認証局オブジェクトが自動的に作成され、物理的に格納されます。どちらのオブジェクトも eDirectory ツリーの最上部に作成されます。これらのオブジェクトは、移動せずに作成時の位置にそのまま保管する必要があります。

1 つの eDirectory ツリー内に存在できる組織の認証局オブジェクトは 1 つだけです。最初のサーバ上にすでに作成されている組織の認証局オブジェクトを、別のサーバに移動することはできません。組織の認証局オブジェクトを削除したり、再作成すると、その組織の認証局に関連する証明書はすべて無効になります。

**重要:** 組織の認証局オブジェクトを永続的に保管しようとするサーバを、最初の eDirectory サーバにするようにします。組織の認証局オブジェクトの保管先のサーバは、ネットワーク内の継続して移動する部分であり、アクセス可能で、信頼性が高くなければなりません。

インストール中のサーバがネットワーク内の最初の eDirectory サーバでない場合、インストールプログラムは組織の認証局オブジェクトが存在する eDirectory サーバを探し、このサーバを参照します。インストールプログラムは、セキュリティコンテナにアクセスし、サーバ証明書オブジェクトを作成します。

ネットワーク内に組織の認証局オブジェクトがまったく存在しないと、Web 関連製品は機能しません。

## Novell Certificate Server でタスクを実行するのに必要な権利

Novell Certificate Server の設定に関連付けられたタスクを完了するには、管理者は、次の表に記載されているような権利を持っている必要があります。

| Novell Certificate Server のタスク   | 必要な権利  |
|--|--|
| 1 台目のサーバを新しいツリーにインストールするか、まだベースセキュリティをインストールしていないツリーの 1 台目のサーバをアップグレードするためのベースセキュリティ設定 | ツリーのルートのスーパーバイザ権<br>セキュリティコンテナのスーパーバイザ権                    |
| 2 台目以降のサーバをインストールするためのベースセキュリティ設定  | サーバコンテナのスーパーバイザ権<br>W0 オブジェクト (セキュリティコンテナ内) のスーパーバイザ権      |
| 組織の認証局の作成  | セキュリティコンテナのスーパーバイザ権  |
| サーバ認証オブジェクトの作成   | サーバコンテナのスーパーバイザ権<br>組織の認証局オブジェクトの NDSPK : プライベートキー属性の読み込み権 |

また、ルート管理者は、サブコンテナの管理者に次の権利を割り当てることによって、組織の認証局を使用する権限を委託することもできます。サブコンテナの管理者が SSL セキュリティを使用する Novell eDirectory をインストールするには、次のような権利が必要です。

- ◆ セキュリティコンテナにある組織の認証局オブジェクトの NDSPKI: プライベートキー属性の読み込み権。
- ◆ KAP オブジェクト内のセキュリティコンテナにある W0 オブジェクトのスーパーバイザ権。

これらの権利はグループや役割に割り当てられ、ここではすべての管理者ユーザが定義されます。Novell Certificate Server 関連の特定のタスク実行に必要な権利の詳細については、[Novell Certificate Server \(http://www.novell.com/documentation/beta/crt30/index.html\)](http://www.novell.com/documentation/beta/crt30/index.html) オンラインマニュアルを参照してください。

## Linux、Solaris、AIX、および HP-UX システムでの eDirectory 操作に関するセキュリティを確保する

eDirectory には、PKCS (パブリックキー暗号化サービス) が付属しています。PKCS には、PKI (Public Key Infrastructure) サービスを提供する Novell Certificate Server、NICI (Novell International Cryptographic Infrastructure)、および SAS\*-SSL サーバが含まれます。

次のセクションでは、eDirectory の操作におけるセキュリティの確保について説明します。

- ◆ [88 ページの「サーバ上に NICI がインストールおよび初期化されているかどうかを確認する」](#)
- ◆ [89 ページの「サーバ上の NICI モジュールを初期化する」](#)
- ◆ [90 ページの「Certificate Server \(PKI サービス\) を起動する」](#)
- ◆ [90 ページの「Certificate Server \(PKI サービス\) を停止する」](#)
- ◆ [90 ページの「組織の認証局オブジェクトを作成する」](#)
- ◆ [90 ページの「サーバ認証オブジェクトを作成する」](#)
- ◆ [91 ページの「組織の認証局の自己署名付き証明書をエクスポートする」](#)

外部認証局の使用については、『[Novell Certificate Server 管理ガイド](http://www.novell.com/documentation/beta/crt30/index.html)』 (<http://www.novell.com/documentation/beta/crt30/index.html>) を参照してください。

### サーバ上に NICI がインストールおよび初期化されているかどうかを確認する

次の条件を満たしているかチェックします。これらの条件は、NICI モジュールが正しくインストールおよび初期化されていることを表します。

- ◆ ファイル /etc/nici.cfg が存在する
- ◆ ディレクトリ /var/novell/nici が存在する
- ◆ ファイル /var/novell/nici/primenici が存在する

これらの条件を満たしていない場合、次のセクション「[サーバ上の NICI モジュールを初期化する](#)」の手順に従って操作してください。

## サーバ上の NICI モジュールを初期化する

### 1 eDirectory サーバを停止します。

- ◆ Linux では、次のコマンドを入力します。  
`/etc/init.d/ndsd stop`
- ◆ Solaris では、次のコマンドを入力します。  
`/etc/init.d/ndsd stop`
- ◆ AIX では、次のコマンドを入力します。  
`/etc/ndsd stop`
- ◆ HP-UX では、次のコマンドを入力します。  
`/sbin/init.d/ndsd stop`

**重要:** ndsd の開始と停止には、ndsmangae を使用することをお勧めします。

### 2 NICI パッケージがインストールされているかどうかを確認します。

- ◆ Linux では、次のコマンドを入力します。  
`rpm -qa | grep nici`
- ◆ Solaris では、次のコマンドを入力します。  
`pkginfo | grep NOVLniu0`
- ◆ AIX では、次のコマンドを入力します。  
`lsllpp -l | grep NOVLniu0`
- ◆ HP-UX では、次のコマンドを入力します。  
`swlist | grep NOVLniu0`

### 3 (状況によって実行) NICI パッケージがインストールされていない場合、インストールします。

NICI パッケージがインストールされていないと先に進みません。

### 4 パッケージに含まれている .nfk ファイルを /var/novell/nici ディレクトリにコピーします。

/var/novell/nici/primenici プログラムを実行します。

### 5 eDirectory サーバを開始します。

- ◆ Linux では、次のコマンドを入力します。  
`/etc/init.d/ndsd start`
- ◆ Solaris では、次のコマンドを入力します。  
`/etc/init.d/ndsd start`
- ◆ AIX では、次のコマンドを入力します。  
`/etc/ndsd start`
- ◆ HP-UX では、次のコマンドを入力します。  
`/sbin/init.d/ndsd start`

**重要:** ndsd の開始と停止には、ndsmangae を使用することをお勧めします。

## Certificate Server (PKI サービス) を起動する

PKI サービスを開始するには、次のコマンドを入力します。


```
npki -l
```

## Certificate Server (PKI サービス) を停止する

PKI サービスを停止するには、次のコマンドを入力します。

```
npki -u
```

## 組織の認証局オブジェクトを作成する

- 1 Novell iManager を起動します。
- 2 適切な権利を持った管理者として eDirectory ツリーにログインします。  
このタスクの適切な権利を参照するには、『*Novell Certificate Server 管理ガイド*』の「[Creating an Organizational CA](http://www.novell.com/documentation/beta/crt30/crtadmin/data/fbgccghh.html)」(<http://www.novell.com/documentation/beta/crt30/crtadmin/data/fbgccghh.html>) を参照してください。
- 3 [役割およびタスク] ボタン  をクリックして、[PKI Certificate Management (PKI 認証管理)] をクリックし、[認証局の作成] をクリックします。

組織の認証局オブジェクトの作成ウィザードが開始します。メッセージに従ってオブジェクトを作成します。ウィザードの各ページに関する特定の情報については、[ヘルプ] をクリックします。

注: eDirectory ツリーは組織の認証局を 1 つしか格納できません。

## サーバ認証オブジェクトを作成する

サーバ認証オブジェクトは、eDirectory サーバオブジェクトを格納するコンテナに作成されます。必要に応じて、サーバ上の個々の暗号化対応アプリケーションに、別々にサーバ認証オブジェクトを作成する場合があります。または、そのサーバで使用するすべてのアプリケーションにサーバ認証オブジェクトを 1 つ作成することもあります。

注: サーバ認証オブジェクトと暗号化キーオブジェクト (KMO) は同じ意味を示しています。eDirectory オブジェクトのスキーマ名は NDSPKI: 暗号化キーです。

- 1 Novell iManager を起動します。
- 2 適切な権利を持った管理者として eDirectory ツリーにログインします。  
このタスクの適切な権利を参照するには、『*Novell Certificate Server 管理ガイド*』の「[Creating Server Certificate Objects](http://www.novell.com/documentation/beta/crt30/crtadmin/data/fbgcdhec.html)」(<http://www.novell.com/documentation/beta/crt30/crtadmin/data/fbgcdhec.html>) を参照してください。
- 3 [役割およびタスク] ボタン  をクリックして、[PKI Certificate Management (PKI 認証管理)] をクリックし、[サーバ証明書の作成] をクリックします。


これによってサーバ証明書の作成ウィザードが開始します。メッセージに従ってオブジェクトを作成します。ウィザードの各ページに関する特定の情報については、[ヘルプ] をクリックします。

## 組織の認証局の自己署名付き証明書をエクスポートする

自己署名付き証明書は、組織の認証局の識別情報と、組織の認証局によって署名された証明書の有効性を確認するために使用できます。

組織の認証局のプロパティページでは、このオブジェクトに関連付けられた証明書とプロパティを参照できます。[自己署名付き証明書] プロパティページでは、自己署名付き証明書を、暗号化対応のアプリケーションで使用するファイルにエクスポートできます。

組織の認証局に存在する自己署名付き証明書は、組織の認証局によって署名された証明書を持つサーバ認証オブジェクトのルート認証局証明書と同じものです。組織の認証局の自己署名付き証明書をルート認証局証明書として認識するサービスでは、組織の認証局によって署名された有効なユーザやサーバが許可されます。

- 1 Novell iManager で、[役割およびタスク] ボタン  をクリックします。
- 2 [eDirectory 管理] > [オブジェクトの変更] の順にクリックします。
- 3 組織の認証局オブジェクトの名前とコンテキストを指定して、[OK] をクリックします。

組織の認証局オブジェクトはセキュリティコンテナにあります。

- 4 [証明書] タブをクリックし、[Self-Signed Certificate (自己署名付き証明書)] をクリックします。
- 5 [エクスポート] をクリックします。  
証明書のエクスポートウィザードが開始します。メッセージに従って証明書をエクスポートします。ウィザードの各ページに関する特定の情報については、[ヘルプ] をクリックします。
- 6 [証明書のエクスポートの概要] ページで、[Save the Exported Certificate to a File (エクスポートされた証明書をファイルに保存)] をクリックします。  
証明書がファイルに保存され、ルート認証局として暗号化対応アプリケーションにインポートできるようになります。
- 7 [閉じる] をクリックします。

このファイルを、eDirectory へのセキュア接続を確立するためのすべてのコマンドライン操作に組み込みます。

## ネットワーク時刻の同期

時刻同期は、ネットワーク全体で一貫したサーバ時刻を維持するためのサービスです。時刻同期は、eDirectory ではなく、サーバのオペレーティングシステムによって提供されます。eDirectory は eDirectory 自体の内部時刻に基づいて eDirectory パケットの正しい順序を維持しますが、その時刻はサーバのオペレーティングシステムから取得されます。

このセクションでは、NetWare の時刻同期と、Windows、Linux、Solaris、AIX、および HP-UX の時刻同期との統合について説明します。



## NetWare サーバで時刻を同期する

IP ネットワーク、および混合プロトコルネットワークでは、NetWare 5 サーバは IP を使用する他のサーバと時刻を同期します。NetWare 5 サーバは、`timesync.nlm` と NTP (ネットワーク時刻プロトコル) を使用してこの同期を行います。

NetWare 5 および 6 は、サーバで IP または IPX™ のみが使用されている場合も、両方のプロトコルが使用されている場合も、`timesync.nlm` を使用して時刻を同期します。`timesync.nlm` はサーバのインストール時にロードされます。NTP は `timesync.nlm` を通して設定できます。

ネットワーク内に Windows、Linux、Solaris、AIX、または HP-UX システムが含まれている場合は、時刻同期の標準である NTP を使用してサーバを同期してください。

NetWare 3 と NetWare 4 には、サードパーティの NTP 時刻サービスを使用できます。

時刻同期ソフトウェアの詳細については、[The Network Time Protocol \(http://www.ntp.org\)](http://www.ntp.org) の Web サイトを参照してください。

## NTP

NTP は、UDP プロトコルスイートの一部として機能します。UDP プロトコルスイートは、TCP/IP プロトコルスイートの一部として機能します。したがって、NTP を使用するコンピュータには、TCP/IP プロトコルスイートがロードされている必要があります。インターネットへアクセスするネットワーク内のコンピュータは、いずれもインターネット上の NTP サーバから時刻を取得できます。

NTP は、国際時刻標準である協定世界時 (UTC) と時刻を同期します。

NTP には、`stratum` (層) という概念が導入されています。`stratum-1` サーバには、電波時計または原子時計などの正確な時計が内蔵されています。`stratum-2` サーバは `stratum-1` サーバから時刻を取得します。同様に、各層のサーバは 1 つ前の層のサーバから時刻を取得します。

NetWare 5 および 6 のサーバでは、`ntp.nlm` をロードすることによって、`timesync.nlm` を通して NTP 時刻同期を実装できます。IP サーバで `timesync.nlm` によって NTP を設定すると、NTP は IP サーバと IPX サーバの両方のタイムソースとして機能するようになります。この場合、IPX サーバはセカンダリサーバとして設定する必要があります。

時刻同期の詳細については、『[Network Time Management 管理ガイド](http://www.novell.com/documentation/lg/nw65/time_enu/data/h15k6r0y.html)』 ([http://www.novell.com/documentation/lg/nw65/time\\_enu/data/h15k6r0y.html](http://www.novell.com/documentation/lg/nw65/time_enu/data/h15k6r0y.html)) および『[Network Time Protocol 管理ガイド](http://www.novell.com/documentation/lg/nw65/ntp/data/aizwub2.html)』 (<http://www.novell.com/documentation/lg/nw65/ntp/data/aizwub2.html>) を参照してください。

## TIMESYNC.NLM

`timesync.nlm` は NetWare サーバ間の時刻を同期します。`timesync.nlm` は、インターネット NTP サーバなどの外部タイムソースと併せて使用できます。また、`timesync.nlm` が実行されているサーバに合わせて時刻を更新するよう、Novell Client™ ワークステーションを設定することもできます。

時刻同期の詳細については、『[Network Time Management 管理ガイド](http://www.novell.com/documentation/lg/nw65/time_enu/data/h15k6r0y.html)』 ([http://www.novell.com/documentation/lg/nw65/time\\_enu/data/h15k6r0y.html](http://www.novell.com/documentation/lg/nw65/time_enu/data/h15k6r0y.html)) を参照してください。



## Windows サーバで時刻を同期する

Windows NT および Windows 2000 サーバの時刻同期の詳細については、オペレーティングシステムのマニュアルを参照してください。

## Linux、Solaris、AIX、または HP-UX システムで時刻を同期する

xntpd NTP (ネットワーク時刻プロトコル) デーモンを使用すると、Linux、Solaris、AIX、および HP-UX サーバの時刻を同期できます。xntpd は、インターネット標準時サーバと同期してシステム時刻を設定および保持するオペレーティングシステムデーモンです。

AIX での xntpd の実行の詳細については、『*AIX Commands Reference, Volume 6 (AIX コマンドリファレンス、第6巻)*』の「xntpd Daemon」([http://publibn.boulder.ibm.com/doc\\_link/en\\_US/a\\_doc\\_lib/cmds/aixcmds6/xntpd.htm](http://publibn.boulder.ibm.com/doc_link/en_US/a_doc_lib/cmds/aixcmds6/xntpd.htm)) を参照してください。

Solaris での xntpd の実行の詳細については、<http://docs.sun.com/?p=/doc/806-0625/6j9vfim2v&a=view#xntpd-1m-indx-2> (<http://docs.sun.com/?p=/doc/806-0625/6j9vfim2v&a=view#xntpd-1m-indx-2>) を参照してください。

HP-UX での xntpd の実行の詳細については、[http://docs.hp.com/cgi-bin/fsearch/framedisplay?top=/hpux/onlinedocs/B2355-90147/B2355-90147\\_top.html&con=/hpux/onlinedocs/B2355-90147/00/00/58-con.html&toc=/hpux/onlinedocs/B2355-90147/00/00/58-toc.html&searchterms=ntp%7cconfiguring&queryid=20030922-153023](http://docs.hp.com/cgi-bin/fsearch/framedisplay?top=/hpux/onlinedocs/B2355-90147/B2355-90147_top.html&con=/hpux/onlinedocs/B2355-90147/00/00/58-con.html&toc=/hpux/onlinedocs/B2355-90147/00/00/58-toc.html&searchterms=ntp%7cconfiguring&queryid=20030922-153023) を参照してください。

Linux での ntpd の実行の詳細については、[ntpd - Network Time Protocol \(NTP\) Daemon](http://www.eecis.udel.edu/~mills/ntp/html/ntpd.html) (<http://www.eecis.udel.edu/~mills/ntp/html/ntpd.html>) を参照してください。

## 時刻同期を確認する

ツリー内の時刻が同期されているか確認するには、Tree オブジェクトに対して読み書き可能以上の権利を持つ、Tree 内のいずれかのサーバから、DSRepair を実行します。

### NetWare の場合

- 1 サーバコンソールで、dsrepair.nlm をロードします。
- 2 [時刻同期] を選択します。

ログの解釈に関するヘルプを表示するには、<F1> を押します。

注: 次のコマンドを使用すると、時刻同期の問題を解決できます。

```
set timesync debug=7
```

### Windows の場合

- 1 [スタート] > [設定] > [コントロールパネル] > [Novell eDirectory サービス] の順にクリックします。
- 2 [dsrepair.dlm] > [開始] の順にクリックします。
- 3 [修復] > [時刻同期] の順にクリックします。

### Linux、Solaris、AIX、および HP-UX

- 1 次のコマンドを実行します。

```
ndsrepair -T
```

## セキュリティ上の考慮事項

LDAP バインドは、安全な接続を使用して実行してください。常に SSL/TLS 接続を使用することをお勧めします。使用しない場合は次の内容を考慮する必要があります。

- ◆ 回線上で転送されたキーが見破られることがあります。したがって、企業ネットワークを傍受またはパケットスニффイングから物理的に保護する必要があります。
- ◆ 権限を持つ担当者のみが物理的にアクセスできる安全な場所にサーバを配置する必要があります。
- ◆ 企業のファイアウォールの外でユーザがこの製品を使用する場合は、VPN を使用する必要があります。
- ◆ サーバが企業ネットワークの外からアクセスできる場合は、不正侵入者による直接アクセスを防ぐためにファイアウォールを使用する必要があります。
- ◆ 監視ログを定期的に確認する必要があります。
- ◆ 異なる管理任務を、別々の個人に割り当てる必要があります。
- ◆ Kerberos の管理には特定の LDAP サーバを正しいサーバとして指定することをお勧めします。サーバ名は iManager で指定できます。

**重要:** ユーザはサーバの IP アドレスではなく、DNS 名を使用して LDAP サーバにアクセスする必要があります。これは、IP アドレスから DNS 名への変換が保護されていないためです。

# 3

## オブジェクトの管理

Novell® eDirectory™ 8.8 には、Web ベースのネットワーク管理アプリケーションである Novell iManager 2.5 が含まれています。これを使用すると、eDirectory ツリーのオブジェクトを管理できます。Novell iManager の新機能および特長については、『[Novell iManager 2.5 管理ガイド](http://www.novell.com/documentation/imanager25/index.html)』(<http://www.novell.com/documentation/imanager25/index.html>) を参照してください。

eDirectory オブジェクトの管理には、オブジェクトの作成、変更、および操作が含まれます。たとえば、ユーザアカウントの作成や、ユーザの権利の管理などの作業が必要になることがあります。Novell iManager は次の場合に使用します。

- ◆ オブジェクトの参照、作成、編集、および編成などの基本的な管理を行う。
- ◆ ユーザのログイン名など eDirectory で使用される情報を指定して、ユーザアカウントを作成する。
- ◆ 権利の割り当て、同等セキュリティの付与、継承の阻止、および有効な権利の参照を行い、権利を管理する。詳細については、[66 ページの「権利の管理」](#)を参照してください。
- ◆ 役割ベースサービスオブジェクトを通じて特定の管理アプリケーションでの管理者の役割を定義し、役割ベースの管理を設定する。

この章では次のトピックについての情報を説明します。


- ◆ [95 ページの「オブジェクトに関連する一般的なタスク」](#)
- ◆ [100 ページの「ユーザアカウントを管理する」](#)
- ◆ [106 ページの「役割ベースサービスを設定する」](#)


### オブジェクトに関連する一般的なタスク

このセクションでは、eDirectory ツリーの管理で使用する基本的なタスクの手順について説明します。

- ◆ [96 ページの「eDirectory ツリーを参照する」](#)
- ◆ [98 ページの「オブジェクトを作成する」](#)
- ◆ [99 ページの「オブジェクトのプロパティを変更する」](#)
- ◆ [99 ページの「オブジェクトをコピーする」](#)
- ◆ [99 ページの「オブジェクトを移動する」](#)
- ◆ [100 ページの「オブジェクトを削除する」](#)
- ◆ [100 ページの「オブジェクトをリネームする」](#)

## eDirectory ツリーを参照する

Novell iManager の [オブジェクトの表示] ボタン () を使用すると、eDirectory ツリーのオブジェクトを検索したり参照したりできます。ツリーの構造を表示し、タスクを実行するオブジェクトを右クリックします。実行可能なタスクは、選択するオブジェクトの種類によって異なります。

オブジェクトの検索や参照は、Novell iManager の [eDirectory オブジェクトセレクタ] ページでも行えます。Novell iManager のほとんどのエン트리フィールドでは、オブジェクト名およびコンテキストを指定したり、[オブジェクトセレクタ] ボタン () をクリックしてオブジェクトを検索または参照したりできます。[eDirectory オブジェクトセレクタ] ページのオブジェクトを選択すると、エン트리フィールドにオブジェクトおよびオブジェクトのコンテキストが挿入されます。

このセクションでは、次の情報について説明します。


- ◆ 96 ページの「[オブジェクトの表示] ボタンを使用する」
- ◆ 97 ページの「[オブジェクトセレクタ] ボタンを使用する」



### [オブジェクトの表示] ボタンを使用する

次で説明する方法を使用して、管理する特定のオブジェクトを検索します。

- ◆ 96 ページの「[参照] を使用する」
- ◆ 97 ページの「[検索] を使用する」

### [参照] を使用する


- 1 Novell iManager で、[オブジェクトの表示] ボタン () をクリックします。
- 2 [参照] をクリックします。
- 3 オブジェクトを参照するには、次のオプションを使用します。

| オプション   | 説明  |
|---|---|
|  | ツリー内を 1 レベル下に移動します。   |
|  | ツリー内を 1 レベル上に移動します。   |
| コンテキスト  | 内容を表示するコンテナの名前を指定します。<br>このオプションを使用するには、コンテナの名前を指定して [適用] をクリックします。   |
| 名前  | オブジェクトの名前を指定します。<br><br>このフィールドには、ワイルドカード文字としてアスタリスク (*) を使用できます。たとえば、「g*」と入力すると、Germany や Greg など g で始まるすべてのオブジェクトが検索され、「*te」と入力すると、Kate や Corporate など te で終わるすべてのエントリが検索されます。<br><br>このオプションを使用するには、名前を入力して [適用] をクリックします。 |

| オプション | 説明   |
|-------|--|
| タイプ   | <p>検索するオブジェクトのタイプを指定します。デフォルト値は、[使用可能なすべてのタイプ] です。</p> <p>このオプションを使用するには、ドロップダウンリストでオブジェクトのタイプを選択して、[適用] をクリックします。</p> |

- 4 目的のオブジェクトを見つけたら、オブジェクトを右クリックして、実行可能なタスクのリストから選択します。

### [検索] を使用する


- 1 Novell iManager で、[オブジェクトの表示] ボタン  をクリックします。
- 2 [検索] をクリックします。
- 3 [コンテキスト] フィールドで、検索するコンテナの名前を指定します。  
[サブコンテナを検索] をクリックし、現在のコンテナにあるすべてのサブコンテナを検索対象に含めます。
- 4 [名前] フィールドで、検索するオブジェクトの名前を指定します。  
このフィールドには、ワイルドカード文字としてアスタリスク (\*) を使用できます。たとえば、「g\*」と入力すると、Germany や Greg など g で始まるすべてのオブジェクトが検索され、「\*te」と入力すると、Kate や Corporate など te で終わるすべてのエントリが検索されます。
- 5 [タイプ] ドロップダウンリストで、検索するオブジェクトのタイプを選択します。
- 6 [検索] をクリックします。
- 7 目的のオブジェクトを見つけたら、オブジェクトを右クリックして、実行可能なタスクのリストから選択します。



### [オブジェクトセレクタ] ボタンを使用する

次で説明する方法を使用して、管理する特定のオブジェクトを検索します。

- ◆ 97 ページの「[参照] を使用する」
- ◆ 98 ページの「[検索] を使用する」


### [参照] を使用する

- 1 iManager のプロパティページで [オブジェクトセレクタ] ボタン  をクリックします。
- 2 [参照] をクリックします。
- 3 オブジェクトを参照するには、次のオプションを使用します。



| オプション   | 説明                  |
|---|---------------------|
|  | ツリー内を 1 レベル下に移動します。 |
|  | ツリー内を 1 レベル上に移動します。 |

| オプション       | 説明   |
|-------------|--|
| 検索対象        | 内容を表示するコンテナの名前を指定して、[適用] をクリックします。   |
| 次のオブジェクトを検索 | <p>オブジェクトの名前を指定します。</p> <p>このフィールドには、ワイルドカード文字としてアスタリスク (*) を使用できます。たとえば、「g*」と入力すると、Germany や Greg など g で始まるすべてのオブジェクトが検索され、「*te」と入力すると、Kate や Corporate など te で終わるすべてのエントリが検索されます。</p> <p>このオプションを使用するには、名前を入力して [適用] をクリックします。</p> |



### [検索] を使用する

- 1 iManager のプロパティページで [オブジェクトセクタ] ボタン  をクリックします。
- 2 [検索] をクリックします。
- 3 [次から検索開始] フィールドで、検索するコンテナの名前を指定します。  
[サブコンテナを検索] をクリックし、現在のコンテナにあるすべてのサブコンテナを検索対象に含めます。
- 4 [次のオブジェクトを検索] フィールドで、検索するオブジェクトの名前を指定します。  
このフィールドには、ワイルドカード文字としてアスタリスク (\*) を使用できます。たとえば、「g\*」と入力すると、Germany や Greg など g で始まるすべてのオブジェクトが検索され、「\*te」と入力すると、Kate や Corporate など te で終わるすべてのエントリが検索されます。
- 5 [検索] をクリックします。

## オブジェクトを作成する


- 1 Novell iManager で、[役割およびタスク] ボタン  をクリックします。
- 2 [eDirectory 管理] > [オブジェクトの作成] の順にクリックします。
- 3 使用可能なオブジェクトクラスのリストからオブジェクトを選択し、[OK] をクリックします。
- 4 必要な情報を指定して、[OK] をクリックします。  
必要な情報は、作成するオブジェクトのタイプによって異なります。詳細については、 をクリックしてください。
- 5 [OK] をクリックします。

## オブジェクトのプロパティを変更する


- 1 Novell iManager で、[役割およびタスク] ボタン  をクリックします。
- 2 [eDirectory 管理] > [オブジェクトの変更] の順にクリックします。
- 3 変更するオブジェクトの名前およびコンテキストを指定して、[OK] をクリックします。
- 4 必要に応じてプロパティページを編集します。  
各プロパティページの詳細については、 をクリックしてください。
- 5 [OK] をクリックします。

## オブジェクトをコピーする


このオプションを使用すると、既存のオブジェクトと同じ属性値を持った新しいオブジェクトを作成したり、あるオブジェクトから別のオブジェクトに属性値をコピーしたりできます。

- 1 Novell iManager で、[役割およびタスク] ボタン  をクリックします。
- 2 [eDirectory 管理] > [オブジェクトのコピー] の順にクリックします。
- 3 [コピー元のオブジェクト] フィールドで、コピーするオブジェクトの名前およびコンテキストを指定します。
- 4 次のいずれかのオプションを選択します。
  - ◆ Create New Object and Copy Attribute Values
  - ◆ Copy Attribute Values to an Existing Object
- 5 アクセス制御リスト (ACL) の権利を、作成または変更するオブジェクトにコピーする場合、[ACL 権利のコピー] をクリックします。  
ACL 権利をコピーする場合、システムやネットワークの環境によってはさらに処理時間がかかる場合があります。
- 6 [OK] をクリックします。


## オブジェクトを移動する

- 1 Novell iManager で、[役割およびタスク] ボタン  をクリックします。
- 2 [eDirectory 管理] > [オブジェクトの移動] の順にクリックします。
- 3 [オブジェクト名] フィールドで、移動するオブジェクトの名前およびコンテキストを指定します。
- 4 [移動先] フィールドで、オブジェクトを移動するコンテナを指定します。
- 5 移動する各オブジェクトについて、元の場所に別名を作成する場合は、[移動したオブジェクトの代わりに別名を作成します] を選択します。  
これにより、移動前の場所に依存するあらゆる操作は、操作を更新して移動後の場所を反映できるようになるまで、引き続き実行されます。
- 6 [OK] をクリックします。

## オブジェクトを削除する

- 1 Novell iManager で、[役割およびタスク] ボタン  をクリックします。
- 2 [eDirectory 管理] > [オブジェクトの削除] の順にクリックします。
- 3 削除するオブジェクトの名前およびコンテキストを指定します。
- 4 [OK] をクリックします。

## オブジェクトをリネームする

- 1 Novell iManager で、[役割およびタスク] ボタン  をクリックします。
- 2 [eDirectory 管理] > [オブジェクトのリネーム] の順にクリックします。
- 3 [オブジェクト名] フィールドで、リネームするオブジェクトの名前およびコンテキストを指定します。
- 4 [新規オブジェクト名] フィールドで、オブジェクトの新しい名前を指定します。  
[新規オブジェクト名] フィールドには、オブジェクトのコンテキストは含めないでください。
- 5 リネームするオブジェクトに別名を作成する場合は、[リネームしたオブジェクトの代わりに別名を作成] を選択します。  
これにより、リネーム前のオブジェクト名に依存するあらゆる操作は、操作を更新してリネーム後のオブジェクト名を反映できるようになるまで、引き続き実行されます。
- 6 リネーム前のオブジェクト名を保存する場合、[古い名前を保存] をクリックします。  
これにより、リネーム前のオブジェクト名が、名前プロパティに未公認の値として追加されます。古い名前を保存しておくで、その名前に基づいてオブジェクトを検索できます。オブジェクトのリネーム後には、[識別] タブの [別の名前] フィールドで古い名前を表示できます。
- 7 [OK] をクリックします。

## ユーザアカウントを管理する

eDirectory のユーザアカウントの設定には、ユーザオブジェクトの作成、およびログイン制御のプロパティやユーザのネットワークコンピューティング環境の設定があります。テンプレートオブジェクトを使用すると、これらのタスクを簡単に実行できます。

ログインスクリプトを作成すると、ユーザがログインしたときに、自動的にファイルやプリンタなどの必要なネットワークリソースに接続できます。同じリソースを使用するユーザが複数いる場合、コンテナにログインスクリプトコマンドを格納して、ログインスクリプトのプロファイルを作成することができます。

このセクションでは、次の情報について説明します。

- ◆ [101 ページの「ユーザアカウントを作成および変更する」](#)
- ◆ [102 ページの「オプションのアカウント機能を設定する」](#)
- ◆ [104 ページの「ログインスクリプトを設定する」](#)
- ◆ [105 ページの「リモートユーザのログイン時間制限」](#)
- ◆ [106 ページの「ユーザアカウントを削除する」](#)





## ユーザアカウントを作成および変更する

ユーザアカウントは、eDirectory ツリー内のユーザオブジェクトです。ユーザオブジェクトによって、ユーザのログイン名など、eDirectory で使用される情報を指定して、ネットワークリソースへのユーザのアクセスを制御できます。



このセクションでは、次の情報について説明します。

- ◆ 101 ページの「ユーザオブジェクトを作成する」
- ◆ 101 ページの「ユーザアカウントを変更する」
- ◆ 101 ページの「ユーザアカウントを有効にする」
- ◆ 101 ページの「ユーザアカウントを無効にする」


### ユーザオブジェクトを作成する

- 1 Novell iManager で、[役割およびタスク] ボタン  をクリックします。
- 2 [ユーザ] > [ユーザの作成] の順にクリックします。
- 3 ユーザ名とユーザの姓を指定します。
- 4 ユーザを作成するコンテナを指定します。
- 5 オプションで追加情報を指定して、[OK] をクリックします。  
使用可能なオプションの詳細については、 をクリックしてください。
- 6 [OK] をクリックします。


### ユーザアカウントを変更する

- 1 Novell iManager で、[役割およびタスク] ボタン  をクリックします。
- 2 [ユーザ] > [ユーザの変更] の順にクリックします。
- 3 変更するユーザの名前およびコンテキストを指定して、[OK] をクリックします。
- 4 必要に応じてプロパティページを編集します。  
特定のプロパティの詳細については、 をクリックしてください。
- 5 [OK] をクリックします。

### ユーザアカウントを有効にする

- 1 Novell iManager で、[役割およびタスク] ボタン  をクリックします。
- 2 [ユーザ] > [アカウントの有効化] の順にクリックします。
- 3 ユーザの名前とコンテキストを指定して、[OK] をクリックします。



### ユーザアカウントを無効にする

- 1 Novell iManager で、[役割およびタスク] ボタン  をクリックします。
- 2 [ユーザ] > [アカウントの無効化] の順にクリックします。
- 3 ユーザの名前とコンテキストを指定して、[OK] をクリックします。



## オプションのアカウント機能を設定する

ユーザオブジェクトを作成した後、ユーザのネットワークコンピューティング環境を設定し、追加のログインセキュリティ機能を実装できます。

### ユーザのネットワークコンピューティング環境を設定する

- 1 Novell iManager で、[役割およびタスク] ボタン  をクリックします。
- 2 [ユーザ] > [ユーザの変更] の順にクリックします。
- 3 変更するユーザの名前およびコンテキストを指定して、[OK] をクリックします。
- 4 [全般] タブで、[使用環境] ページをクリックします。
- 5 プロパティページに入力します。  
特定のプロパティの詳細については、 をクリックしてください。
- 6 [OK] をクリックします。


### ユーザに追加のログインセキュリティを設定する

- 1 Novell iManager で、[役割およびタスク] ボタン  をクリックします。
- 2 [ユーザ] > [ユーザの変更] の順にクリックします。
- 3 変更するユーザの名前およびコンテキストを指定して、[OK] をクリックします。
- 4 [制限] タブで、必要なプロパティページに入力します。  
ページの詳細については、 をクリックしてください。

| ページ         | 説明  |
|-------------|---|
| パスワード制限     | ログインパスワードを設定します。  |
| ログイン制限      | <ul style="list-style-type: none"><li>◆ アカウントを有効または無効にします。</li><li>◆ 同時ログインセッション数を制限します。</li><li>◆ ログインの有効期限およびロックアウトする日付を設定します。</li></ul>  |
| ログイン時間制限    | ユーザがログインできる時間を制限します。制限を設定し、制限時間になったときにオブジェクトがログインされていると、5分間警告が表示され、5分後にまだオブジェクトがログアウトされていない場合は、そのオブジェクトをログアウトします。リモートからログインする場合は、 <a href="#">105 ページの「リモートユーザのログイン時間制限」</a> を参照してください。 |
| アドレス制限      | このユーザがログインするネットワークの場所 (ワークステーション) を制限します。このページで制限を設定しない場合、ユーザはネットワークのどの場所からでもログインできます。  |
| アカウントバランス   | このユーザのサーバ使用量を設定します。   |
| 不正侵入者ロックアウト | 不正侵入者が検出されたためにアカウントがロックされた場合、このアカウントを操作します。不正侵入者検出の設定を管理するには、親コンテナの <a href="#">[不正侵入者検出]</a> プロパティページを使用します。   |

- 5 [OK] をクリックします。

## コンテナ内のすべてのユーザの不正侵入者検出を設定する

- 1 Novell iManager で、[役割およびタスク] ボタン  をクリックします。
- 2 [eDirectory 管理] > [オブジェクトの変更] の順にクリックします。
- 3 コンテナオブジェクトの名前とコンテキストを指定して、[OK] をクリックします。
- 4 [全般] タブで、[不正侵入者検出] ページをクリックします。
- 5 次のオプションから選択します。

| オプション           | 説明  |
|-----------------|---|
| 不正侵入者を検出する      | コンテナのユーザアカウントの不正侵入者検出システムを有効にします。   |
| 不正ログイン試行回数      | 連続してログインに失敗して不正侵入者検出がアクティブになるまでのログイン試行回数を指定します。このコンテナ内のユーザアカウントのいずれかを使用して、連続してログインに失敗した回数がこの数値を超えた場合、不正侵入者検出がアクティブになります。この数値は、コンテナの [Login Intruder Limit (不正ログイン制限)] プロパティに格納されます。   |
| 不正ログイン回数のリセット間隔 | ここで指定する時間間隔の中で連続して失敗したログインが発生した場合、不正侵入者検出がアクティブになります。日、時間、および分を入力します。   |
| 検出後にアカウントをロックする | このコンテナ内のユーザアカウントで不正侵入者検出がアクティブになった場合に、ログインを無効にするかどうかを指定します。このチェックボックスがオンになっていない場合、不正侵入者検出がアクティブになってもアカウントはロックされません。このチェックボックスをオンにし、不正侵入者の検出によってユーザアカウントがロックされた場合、ユーザオブジェクトの [不正侵入者ロックアウト] プロパティの [ロックされたアカウント] チェックボックスをオフにして、アカウントのロックを解除できます。 |
| 日、時間、分          | この3つのフィールドでは、不正侵入者検出がこのコンテナ内のユーザアカウントでアクティブになった場合にログインが無効になる時間が指定されます。指定する日、時間、および分を入力するか、デフォルトの15分を使用します。指定した時間が経過すると、ユーザアカウントのログインが再度有効になります。これらのフィールドの内容は、コンテナの [アカウントロックアウト期間] プロパティに格納されます。  |

- 6 [OK] をクリックします。


## ログインスクリプトを設定する

ログインスクリプトは、ユーザがログインしたときに実行される一連のコマンドです。一般的に、ユーザとファイルやプリンタなどのネットワークリソースとの接続に使用されます。ログインスクリプトは、次の順序でユーザのワークステーション上で実行されます。

1. コンテナログインスクリプト
2. プロファイルログインスクリプト
3. ユーザログインスクリプト

ログイン中に、これらのログインスクリプトで見つからないものがある場合、次のスクリプトにスキップします。何も見つからない場合、デフォルトのスクリプトが実行され、検索ドライブがユーザのデフォルトサーバ上のフォルダにマップされます。デフォルトサーバは、ユーザオブジェクトの [使用環境] プロパティページで設定されます。

## ログインスクリプトを作成する

- 1 Novell iManager で、[役割およびタスク] ボタン  をクリックします。
- 2 [eDirectory 管理] > [オブジェクトの変更] の順にクリックします。
- 3 ログインスクリプトを作成するオブジェクトの名前とコンテキストを指定します。


| ログインスクリプトの適用先      | 作成先          |
|--------------------|--------------|
| 1人のユーザのみ           | ユーザオブジェクト    |
| まだ作成されていない1人以上のユーザ | テンプレートオブジェクト |
| 1つのコンテナ内のすべてのユーザ   | コンテナオブジェクト   |
| 1つ以上のコンテナの複数のユーザ   | プロファイルオブジェクト |

- 4 [OK] をクリックします。
- 5 [全般] タブで、[ログインスクリプト] ページを選択します。
- 6 指定するログインスクリプトコマンドを入力します。  
詳細については、『*Login Script Commands Guide*』(<http://www.novell.com/documentation/lg/noclienu/index.html>) を参照してください。
- 7 [OK] をクリックします。

## ユーザにプロフィールを割り当てる

プロフィールをユーザオブジェクトと関連付けることによって、ユーザのログイン中にそのプロフィールのログインスクリプトが実行されます。ユーザが、プロフィールオブジェクトのブラウズ権、およびプロフィールオブジェクトのログインスクリプトプロパティの読み込み権を持っていることを確認してください。


詳細については、70 ページの「[eDirectory オブジェクトまたはプロパティへの有効な権利を参照する](#)」を参照してください。

- 1 Novell iManager で、[役割およびタスク] ボタン  をクリックします。
- 2 [ユーザ] > [ユーザの変更] の順にクリックします。
- 3 ログインスクリプトを作成するユーザオブジェクトの名前とコンテキストを指定します。
- 4 [OK] をクリックします。
- 5 [全般] タブで、[ログインスクリプト] ページを選択します。
- 6 プロファイルオブジェクトをこのオブジェクトに関連付けるには、[プロフィール] フィールドにプロフィールオブジェクトの名前とコンテキストを入力します。
- 7 [OK] をクリックします。

## リモートユーザのログイン時間制限

ユーザオブジェクトの [ログイン時間制限] プロパティページで、ユーザが eDirectory にログインできる時間を制限できます。(デフォルトでは、ログイン時間は制限されていません。) ログイン時間制限が設定され、制限時間になったときにユーザがログインしていると、5 分以内にログアウトするよう警告が表示されます。ユーザが 5 分経ってもまだログインしている場合、自動的にログアウトされ、保存していないデータは失われます。

ログイン要求を処理するサーバとは異なるタイムゾーンからリモートでログインする場合、ユーザに設定されたログイン時間制限の時差は調整されます。たとえば、月曜日の午前 1 時から午前 6 時までにログインが制限されており、サーバより 1 時間遅いタイムゾーンからリモートでログインする場合、このユーザの制限は午前 2 時から午前 7 時まで有効になります。


- 1 Novell iManager で、[役割およびタスク] ボタン  をクリックします。
- 2 [ユーザ] > [ユーザの変更] の順にクリックします。
- 3 変更するユーザの名前およびコンテキストを指定して、[OK] をクリックします。
- 4 [制限] タブで、[ログイン時間制限] をクリックします。

5 次のオプションから選択します。

| オプション       | 説明   |
|-------------|--|
| タイムグリッド     | タイムグリッドのそれぞれのセルは、表示されている週の1日のうちの30分を表します。赤いセルは、このオブジェクトにログインできない制限時間を表します。灰色のセルは制限されていない時間で、このオブジェクトにログインできる時間を表します。時間制限を設定するには、指定する時間をクリックして濃い灰色にします。複数の時間を選択するには、を押しながらセルをクリックし、該当するセルまでドラッグします。設定したログイン時間制限は、このオブジェクトの [Login Allowed Time Map ( ログイン許可時間マップ )] プロパティに格納されます。 |
| ログイン時間制限の追加 | 時間制限を追加するには、灰色のセルをクリックして、このオプションを選択します。  |
| ログイン時間制限の削除 | 時間制限を削除するには、赤いセルをクリックして、このオプションを選択します。   |
| 更新          | このボタンをクリックすると選択が有効になります。   |
| リセット        | このボタンをクリックすると、このプロパティページを開く前の状態にタイムグリッドがリセットされます。  |

6 [OK] をクリックします。

## ユーザアカウントを削除する

- 1 Novell iManager で、[役割およびタスク] ボタン  をクリックします。
- 2 [ユーザ] > [ユーザの削除] の順にクリックします。
- 3 削除するユーザの名前およびコンテキストを指定します。
- 4 [OK] をクリックします。






## 役割ベースサービスを設定する


Novell iManager を使用すると、管理者は、ユーザに特定の責任を割り当てたり、これらの責任を実行するために必要なツールおよびそれに伴う権利だけを与えたりすることができます。この機能を、*役割ベースサービス (RBS)* といいます。

役割ベースサービスによって、タスクと呼ばれる機能、および役割と呼ばれるタスクの集まりによって決定されたオブジェクトといった特定の機能だけをユーザが使用できるようにします。ユーザが iManager にアクセスしたときに表示されるのは、eDirectory 内の役割の割り当てが基になっています。表示されるのは、そのユーザに割り当てられたタスクのみです。管理するオブジェクトを探すためにツリーを参照する必要はありません。そのタスクの iManager プラグインには、タスクを実行するために必要なツールとインターフェースが用意されています。

1人のユーザには複数の役割を割り当てることができます。また、複数のユーザに同じ役割を割り当てることができます。

役割ベースサービスは、eDirectory 内で定義されたオブジェクトとして表されます。基本の eDirectory スキーマは、iManager のインストール中に拡張されます。RBS オブジェクトタイプには、次の表のようなものがあります。

| オブジェクト  | 説明  |
|---|---|
|  RBS コレクション  | <p>すべての RBS 役割オブジェクトおよびモジュールオブジェクトを格納するコンテナオブジェクト。</p> <p>RBS コレクションオブジェクトは、すべての RBS オブジェクトの最上位のコンテナです。ツリーには RBS コレクションオブジェクトをいくつでも格納できます。これらのオブジェクトには、コレクションを管理する権利を持つユーザとして「所有者」が存在します。</p> <p>RBS コレクションオブジェクトは次のコンテナのいずれかに作成できます。</p> <ul style="list-style-type: none"> <li>◆ 国</li> <li>◆ ドメイン</li> <li>◆ 地域</li> <li>◆ 組織</li> <li>◆ 部門</li> </ul> |
|  rbsRole     | <p>ユーザ (メンバー) が実行を許可されたタスクを指定するコンテナオブジェクト。役割の定義には、rbsRole オブジェクトの作成や役割が実行できるタスクの指定が含まれます。</p> <p>役割メンバーには、ユーザ、グループ、組織、部門があり、ツリーの特定の範囲内の役割に関連付けられています。rbsTask オブジェクトおよび rbsBook オブジェクトは、rbsRole オブジェクトに割り当てられます。</p> <p>rbsRole オブジェクトは、RBS コレクションコンテナ内のみ作成できます。</p>   |
|  rbsModule | <p>rbsTask オブジェクトおよび rbsBook オブジェクトを格納するコンテナオブジェクトです。rbsModule オブジェクトには、タスクやブックを定義する製品の名前 (たとえば、eDirectory Maintenance Utilities、NMA Management、Novell Certificate Server Access など) を表すモジュール名の属性があります。</p> <p>rbsModule オブジェクトは、RBS コレクションコンテナ内のみ作成できます。</p>   |
|  rbsTask   | <p>ログインパスワードのリセットなど、特定の機能を表すリーフオブジェクトです。</p> <p>rbsTask オブジェクトは、rbsModule コンテナ内のみ格納されます。</p>  |
|  rbsBook   | <p>ブックに割り当てられる一連のページを含むリーフオブジェクトです。rbsBook は、1 つ以上の役割および 1 つ以上のオブジェクトクラスタイプに割り当てることができます。</p> <p>rbsBook オブジェクトは、rbsModule コンテナ内のみ格納されます。</p>   |

| オブジェクト   | 説明  |
|--|---|
|  rbsScope | <p>ユーザオブジェクトごとに割り当てずに ACL 割り当てを実行するためのリーフオブジェクトです。rbsScope オブジェクトは、役割が実行されるツリー内のコンテキストを表し、rbsRole オブジェクトに関連付けられます。このオブジェクトはグループクラスから権利を受け継ぎます。ユーザオブジェクトは rbsScope オブジェクトに割り当てられません。これらのオブジェクトは、関連付けられるツリーのスコープを参照します。</p> <p>このオブジェクトは、必要な場合は動的に作成され、不要になれば自動的に削除されます。rbsScope オブジェクトは rbsRole コンテナ内のみ格納されます。</p> <p><b>警告</b> : Scope オブジェクトの環境設定を変更してはいけません。設定を変更することによって深刻な問題が発生し、システムが故障する可能性があります。</p> |

RBS オブジェクトは、次の図に示されているように eDirectory ツリーに属しています。

図 22 eDirectory ツリー内の RBS オブジェクト



## RBS 役割を定義する

RBS 役割は、ユーザが実行を許可されるタスクを指定します。RBS 役割の定義には、rbsRole オブジェクトの作成や、役割が実行できるタスク、およびユーザ、グループ、またはこれらのタスクを実行できるコンテナオブジェクトの指定などがあります。Novell iManager プラグイン (製品パッケージ) には、変更可能な定義済み RBS 役割が提供されている場合もあります。

RBS 役割が実行できるタスクは、eDirectory ツリー内では rbsTask オブジェクトとして公開されます。これらのオブジェクトは、製品パッケージのインストールの際に自動的に追加されます。オブジェクトは 1 つ以上の rbsModule に編成され、異なる機能を持つ製品モジュールに対応するコンテナとなります。


役割へのメンバーの割り当てについての詳細は、109 ページの「RBS 役割のメンバーシップおよびスコープを割り当てる」を参照してください。

- ◆ 109 ページの「役割オブジェクトを作成する」
- ◆ 109 ページの「役割に関連付けられたタスクを変更する」
- ◆ 109 ページの「RBS 役割のメンバーシップおよびスコープを割り当てる」
- ◆ 110 ページの「役割ベースサービスオブジェクトを削除する」



## 役割オブジェクトを作成する



Create iManager Role ウィザードを使用して、新しい rbsRole オブジェクトを作成します。新しい rbsRole オブジェクトを作成する場合は、他の rbsRole オブジェクトが属している同じ RBS コレクションコンテナ (たとえば、役割ベースサービスコレクションコンテナ) 内に作成することをお勧めします。

- 1 Novell iManager で、[設定] ボタン  をクリックします。
- 2 [役割の設定] > [iManager の役割を作成] の順にクリックします。
- 3 Create iManager Role ウィザードの手順に従って操作します。

役割へのメンバーの追加についての詳細は、[110 ページの「カスタム RBS タスクを定義する」](#)を参照してください。

## 役割に関連付けられたタスクを変更する

各 RBS 役割には、それに関連付けられた使用可能なタスクがあります。特定の役割に割り当てられたタスクは、必要に応じてタスクを追加したり削除したりすることで選択できます。

- 1 Novell iManager で、[設定] ボタン  をクリックします。
- 2 [役割の設定] > [iManager の役割を変更] の順にクリックします。
- 3 役割のタスクを追加または削除するには、変更する役割の左にある [タスクの変更] ボタン  をクリックします。
- 4 [割り当てられたタスク] リストでタスクを追加または削除します。
- 5 [OK] をクリックします。

## RBS 役割のメンバーシップおよびスコープを割り当てる


所属する組織に必要な RBS 役割を定義すると、それぞれの役割にメンバーを割り当てることができます。その際、それぞれのメンバーが役割の機能を使用できるスコープを指定します。スコープは、この役割を実行できる eDirectory ツリー内の場所またはコンテキストです。


役割へのユーザの割り当ては、次の方法で行うことができます。

- ◆ 直接
- ◆ グループおよび動的グループの割り当てによる方法役割に割り当てられているグループまたは動的グループのメンバーであれば、ユーザはその役割にアクセスできます。
- ◆ 職種割り当てによる方法役割に割り当てられている職種に所属する場合は、ユーザはその役割にアクセスできます。
- ◆ コンテナ割り当てによる方法ユーザオブジェクトは、その親コンテナが割り当てられたすべての役割にアクセスできます。さらにツリーのルートまで遡るコンテナの役割にもアクセスできます。


役割との関連付けは、それぞれ異なるスコープで何度も実行できます。また、同じタスクを複数のメンバーに割り当てることもできます。

役割のメンバーシップおよびスコープを割り当てるには、次の操作を実行します。

- 1 Novell iManager で、[設定] ボタン  をクリックします。

- 2 [役割の設定] > [iManager の役割を変更] の順にクリックします。
- 3 役割のメンバーを追加または削除するには、変更する役割の左にある [メンバーの変更] ボタン  をクリックします。
- 4 [名前] フィールドには、オブジェクトの名前 ( ユーザ、グループ、またはコンテナオブジェクト ) およびコンテキストを指定します。
- 5 [スコープ] フィールドには、組織または部門オブジェクトの名前およびコンテキストを指定します。
- 6 [追加] をクリックし、[OK] をクリックします。


### 役割ベースサービスオブジェクトを削除する

- 1 Novell iManager で、[設定] ボタン  をクリックします。
- 2 [役割の設定] > [役割の削除] の順にクリックします。
- 3 削除する RBS 役割の名前およびコンテキストを指定します。
- 4 [OK] をクリックします。

### カスタム RBS タスクを定義する


- ◆ 110 ページの「iManager タスクを作成する」
- ◆ 110 ページの「サーバ管理タスクを作成する」
- ◆ 110 ページの「役割の割り当てを変更する」
- ◆ 111 ページの「タスクを削除する」

### iManager タスクを作成する


- 1 Novell iManager で、[設定] ボタン  をクリックします。
- 2 [タスクの設定] > [iManager のタスクを作成] の順にクリックします。
- 3 Task Builder の手順に従ってカスタムタスクを作成します。

### サーバ管理タスクを作成する


Create Server Administration Task ウィザードを使用してカスタムタスクを作成し、サーバのサービスにアクセスします。システム管理者は、サービスがサーバ上で使用可能かどうかを確認する必要があります。

- 1 Novell iManager で、[設定] ボタン  をクリックします。
- 2 [タスクの設定] > [サーバ管理タスクの作成] の順にクリックします。
- 3 Create Server Administration Task ウィザードの手順に従って操作します。

### 役割の割り当てを変更する

- 1 Novell iManager で、[設定] ボタン  をクリックします。
- 2 [タスクの設定] > [役割の割り当てを変更] の順にクリックします。
- 3 変更するタスクの名前およびコンテキストを指定して、[次へ] をクリックします。
- 4 割り当てを変更する役割を [使用可能な役割] カラムから [割り当て役割] カラムへ移動します。
- 5 [OK] をクリックします。

## タスクを削除する

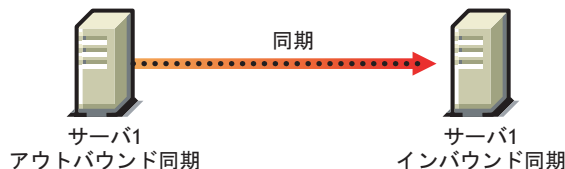
- 1 Novell iManager で、[設定] ボタン  をクリックします。
- 2 [タスクの設定] > [タスクの削除] の順にクリックします。
- 3 削除するタスクの名前およびコンテキストを指定して、[OK] をクリックします。

## 同期

同期は、あるレプリカから他のレプリカへのディレクトリ情報の伝播であるため、各パーティションの情報は他のパーティションの情報と整合性を保ちます。eDirectory は自動的にそれらのサーバの同期を維持します。

同期には、インバウンド同期とアウトバウンド同期があります。たとえば、データに加えられた変更を server1 と server2 の間で同期する必要がある場合、「アウトバウンド」という用語は、server1 から server2 に送信される同期プロセスを意味します。「インバウンド」という用語は、server2 によって受信された server1 からの同期プロセスを意味します。

図 23 アウトバウンド同期とインバウンド同期



同期には、次の 2 つのタイプがあります。

- ◆ 通常同期およびレプリカ同期
- ◆ 優先度同期 (eDirectory 8.8 以降)

次の表に、通常同期と優先度同期の比較を示します。

表 1 通常同期またはレプリカ同期と優先度同期の比較

| 通常同期またはレプリカ同期   | 優先度同期   |
|---|---|
| レプリカリング内の任意のサーバのデータに変更が加えられた場合にトリガされます。                       | 重要データとして指定しているデータに変更が加えられた場合のみトリガされます。              |
| 詳細については、113 ページの「通常同期またはレプリカ同期」を参照してください。                     | 詳細については、115 ページの「優先度同期」を参照してください。                   |
| データが変更されると、変更内容はバッファに保存されます。通常同期は、変更内容が保存されてから約 30 秒後に開始されます。 | 重要データへの変更はバッファに保存されません。優先度同期は、データが変更された直後に開始されます。   |
| eDirectory で最も重要な同期です。変更が優先度同期によって同期されているかどうかにかかわらず実行されます。    | 通常同期を補完するものです。重要な属性は優先度同期によって同期され、通常同期によって再度同期されます。 |
| eDirectory 8.8 サーバ間または以前のバージョンの eDirectory をホストするサーバ間で実行可能です。 | 同じパーティションを保持している eDirectory 8.8 サーバ間でのみ実行されます。      |

| 通常同期またはレプリカ同期   | 優先度同期  |
|---|--|
| <p>機能上、失敗することはありません。</p> <p>詳細については、<a href="#">112 ページの「同期の特徴」</a>を参照してください。</p> | <p>優先度同期が失敗した場合、重要なデータへの変更は通常同期によって同期されます。</p> <p>詳細については、<a href="#">122 ページの「優先度同期が失敗する場合」</a>を参照してください。</p> |

## 同期の特徴

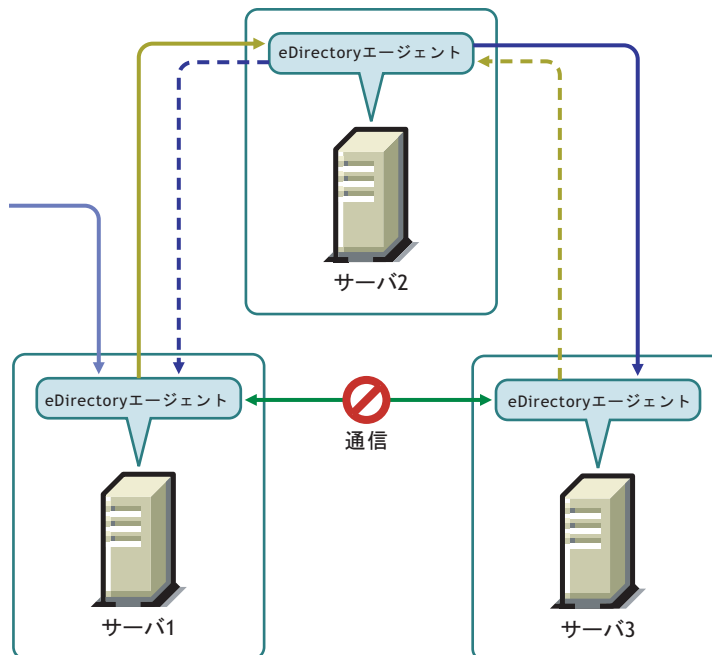
eDirectory での同期には、次のような特徴があります。

- ◆ **遷移**です。
- ◆ **オブジェクトトランザクションモデル**を維持します。
- ◆ **遷移ベクトル**、**local received up to**、および **remote received up to** などのタイムスタンプがあります。

## 遷移同期

eDirectory での同期は遷移同期です。つまり、eDirectory でデータへの変更を同期する場合、eDirectory エージェントがレプリカリング内の他のすべてのエージェントに直接接続して変更を同期する必要はありません。

図 24 遷移同期



たとえば、Server 1 でデータに変更を加えた場合、その変更は Server 1 から Server 2、および Server 2 から Server 3 に同期されます。通信上の問題のため Server 1 が Server 3 に直接接続できなかった場合でも、Server 3 は Server 2 を介してデータへの最新の変更内容を受信します。Server 3 は、変更内容を受信したことを Server 2 に通知します。次に Server 2 は、Server 3 と Server 2 が同期していることを Server 1 に通知します。

## オブジェクトトランザクションモデル

eDirectory での同期では、LDAP および X.500 準拠ディレクトリの標準であるオブジェクトトランザクションモデルが維持されます。オブジェクトトランザクションモデルでは、新しいトランザクションを同期する前に、以前のトランザクションをすべて同期する必要があります。

たとえば、サーバ上でデータに D1、D2、および D3 という変更を加えたとします。ネットワーク障害のため、これらの変更は他のサーバ間で同期されません。サーバ上で別の D4 という変更を行った場合、D1、D2、および D3 がレプリカリング内のすべてのサーバ間で同期された後でのみ、D4 が同期されます。

## 遷移ベクトル

遷移ベクトルとは、レプリカのタイムスタンプのことです。レプリカ作成時刻を 1970 年 1 月 1 日からの経過秒数で表したものと、レプリカ番号、および現在のイベント番号を組にして表示されます。たとえば次のような形をしています。

```
s3D35F377 r02 e002
```

詳細については、[403 ページの「遷移ベクトルと復元後の検証処理」](#)を参照してください。

## Local Received Up To

Local Received Up To (LRUT) は、ローカルレプリカが変更内容を受信するまでの時間です。

詳細については、[213 ページの「ツリー内のオブジェクトの参照」](#)を参照してください。

## Remote Received Up To

Remote Received Up To (RRUT) は、リモートレプリカの LRUT です。

詳細については、[213 ページの「ツリー内のオブジェクトの参照」](#)を参照してください。

## 通常同期またはレプリカ同期

通常同期またはレプリカ同期は、eDirectory における 2 つの同期プロセスの 1 つです。通常同期では、サーバ上のデータへの変更がすべて、レプリカリング内の他のサーバと同期されます。

通常同期は、同じパーティションを持つ任意のバージョンの eDirectory が実行されているすべてのサーバ間で行われます。

詳細については、[140 ページの「レプリカの管理」](#)を参照してください。

通常同期を有効または無効にするには、Novell iMonitor でアウトバウンド同期およびインバウンド同期を有効または無効にします。インバウンド同期およびアウトバウンド同期は両方とも、デフォルトでは有効になっています。通常同期を介して他のサーバ間でデータへの変更を同期するには、iMonitor で同期パラメータを設定する必要があります。詳細については、[209 ページの「DS エージェントを制御および環境設定する」](#)を参照してください。

通常同期では、データに変更が加えた場合、変更内容はサーバ間で同期される前に、バッファに保存されます。サーバの同期ステータスは、iMonitor で表示できます。詳細については、[213 ページの「ツリー内のオブジェクトの参照」](#)を参照してください。

通常同期は遷移同期であり、オブジェクトトランザクションモデルが維持されます。詳細については、101 ページの「遷移同期」および「オブジェクトトランザクションモデル」を参照してください。

## 通常同期を設定する

通常同期を設定するには、iMonitor の [エージェント同期] にある [エージェント環境設定] を使用します。

このセクションでは、次の情報について説明します。

- ◆ 114 ページの「通常同期を有効 / 無効にする」
- ◆ 114 ページの「インラインキャッシュを有効 / 無効にする」
- ◆ 114 ページの「同期スレッド」
- ◆ 115 ページの「同期メソッド」

### 通常同期を有効 / 無効にする

通常同期を有効または無効にするには、iMonitor でアウトバウンド同期およびインバウンド同期を有効または無効にします。詳細については、209 ページの「DS エージェントを制御および環境設定する」を参照してください。

アウトバウンド同期は、デフォルトで有効になっています。このオプションをサーバで無効にしている場合、このサーバ上のデータへの変更は、他のサーバと同期されません。アウトバウンド同期を無効にする期間 (単位は時間) を指定できます。デフォルト (最大時間) は 24 時間です。指定された期間が過ぎると、そのサーバでデータに加えられた変更が他のサーバと同期されるようになります。

インバウンド同期は、デフォルトで有効になっています。サーバに対してこのオプションを無効にすると、他のサーバでデータに加えられた変更がそのサーバと同期されなくなります。

### インラインキャッシュを有効 / 無効にする

サーバのインラインキャッシュ変更を有効または無効にできます。インラインキャッシュ変更は、アウトバウンド同期が無効になっている場合のみ、無効にできます。アウトバウンド同期を有効にすると、インラインキャッシュ変更も有効になります。

インラインキャッシュ変更を無効にすると、このレプリカの変更キャッシュが無効としてマークされ、[エージェント環境設定] > [パーティション] に無効なフラグが付けられます。インラインキャッシュ変更を有効にすると、変更キャッシュの再構築時に、無効な変更キャッシュのフラグが削除されます。

### 同期スレッド

アウトバウンド同期を行うには、同期スレッドを設定する必要があります。iMonitor で、[エージェント同期] の下にある [エージェント環境設定] を使用して同期スレッド数を指定します。有効な値は 1 ~ 16 です。

詳細については、209 ページの「DS エージェントを制御および環境設定する」を参照してください。

## 同期メソッド

通常、eDirectory では、レプリカおよびレプリケーションパートナーの数に基づいてメソッドが自動的に選択されます。同期メソッドは、次のとおりです。

- ◆ **パーティションごと**：データへの変更は、他のレプリカと同時に同期されます。変更の同期には複数のスレッドが使用されます。たとえば、レプリカ R1 のデータに D1、D2、および D3 という変更が加えられ、これらの変更をレプリカ R2 および R3 の間で同期させる必要がある場合、D1、D2、および D3 は R2 および R3 と同時に同期されます。
- ◆ **サーバごと**：データへの変更は順次に同期されます。変更の同期には 1 つのスレッドのみが使用されます。たとえば、レプリカ R1 のデータに D1、D2、および D3 という変更を加えたとします。これらの変更をレプリカ R2 および R3 の間で同期させる必要があります。まず、D1 が R2 および R3 と同期されます。次に、D2 が R2 および R3 と同期されます。
- ◆ **ダイナミック調整**：割り当てたシステムリソースに基づいて、eDirectory によって同期メソッドが自動的に選択されます。

iMonitor で、[エージェント同期] にある [エージェント環境設定] を使用して同期メソッドを指定できます。詳細については、[209 ページの「DS エージェントを制御および環境設定する」](#)を参照してください。

## 優先度同期

優先度同期は、eDirectory における 2 つの同期プロセスの 1 つです。eDirectory 8.8 以降では、重要なデータを直ちに同期させる必要がある場合に優先度同期を使用でき、通常同期を待つことはできません。

優先度同期は、eDirectory での通常同期プロセスを補完するものです。通常同期とは異なり、優先度同期では、変更内容はサーバ間で同期される前にバッファに保存されません。そのため、優先度同期は通常同期より高速になります。

優先度同期は、デフォルトで有効になっています。詳細については、[116 ページの「インバウンド優先度同期およびアウトバウンド優先度同期を有効/無効にする」](#)を参照してください。

優先度同期を介して重要なデータへの変更を同期するには、次の手順を実行します。

- 1 優先度同期のスレッド数を指定します。**  
詳細については、[116 ページの「優先度同期スレッド」](#)を参照してください。
- 2 優先度同期キューサイズを指定します。**  
詳細については、[117 ページの「優先度同期キューサイズ」](#)を参照してください。
- 3 優先度同期ポリシーを作成して定義するには、優先度同期を介して同期する重要な属性を指定します。**  
詳細については、[119 ページの「優先度同期ポリシーを作成および定義する」](#)を参照してください。
- 4 優先度同期ポリシーを 1 つ以上のパーティションに適用します。**  
詳細については、[120 ページの「優先度同期ポリシーを適用する」](#)を参照してください。

優先度同期プロセスでは、重要な属性への変更のみが同期されます。重要な属性を持つ新しいオブジェクトを作成した場合、作成されたオブジェクトは他のサーバと同期されません。



優先度同期では、オブジェクトトランザクションモデルが維持されます。したがって、重要ではないデータが変更され、まだ同期されていない場合、および重要なデータが同じエントリで変更された場合には、重要ではないデータが重要なデータとともに同期されます。

たとえば、ユーザが **Income**、**Employee No**、**Address**、**Cube No** という属性を持っているとします。その中の **Income** と **Address** が重要な属性です。**Employee No** および **Cube No** は変更されていますが、これらの変更はまだ同期されていません。**Income** および **Address** への変更が優先度同期を介して同期されると、**Employee No** および **Cube No** も (重要データとして指定されていませんが) 同期されます。

このセクションでは、次の情報について説明します。

- ◆ [116 ページの「インバウンド優先度同期およびアウトバウンド優先度同期を有効 / 無効にする」](#)
- ◆ [116 ページの「優先度同期スレッド」](#)
- ◆ [117 ページの「優先度同期キューサイズ」](#)
- ◆ [117 ページの「優先度同期ポリシーを管理する」](#)
- ◆ [122 ページの「優先度同期が失敗する場合」](#)

## インバウンド優先度同期およびアウトバウンド優先度同期を有効 / 無効にする

eDirectory 8.8 以降でインバウンド優先度同期およびアウトバウンド優先度同期を有効または無効にするには、iMonitor を使用します。詳細については、[209 ページの「DS エージェントを制御および環境設定する」](#) を参照してください。

インバウンド優先度同期は、デフォルトで有効になっています。インバウンド優先度同期をサーバで無効にしている場合、他のサーバ上の重要なデータへの変更は、優先度同期ではこのサーバと同期されません。ただし、変更は通常同期プロセスによって同期されます。

アウトバウンド優先度同期は、デフォルトで有効になっています。このオプションをサーバで無効にしている場合、このサーバ上の重要なデータへの変更は、優先度同期では他のサーバと同期されません。ただし、変更は通常同期プロセスによって同期されます。

## 優先度同期スレッド

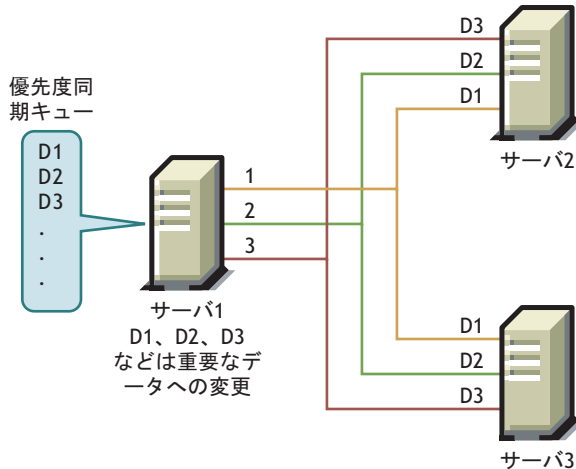
アウトバウンド優先度同期に使用するスレッド数を設定する必要があります。iMonitor で、[エージェント同期] の下にある [エージェント環境設定] を使用して、優先度同期スレッド数を指定します。詳細については、[209 ページの「DS エージェントを制御および環境設定する」](#) を参照してください。有効な値は 1 ~ 32 であり、デフォルトは 4 です。



## 優先度同期キューサイズ

これは、同期の前にキューで保持可能な、変更された重要なエントリの最大数です。重要なエントリは、変更されるとすぐに優先度同期キューに入れられ、順次に同期されます。たとえば、server1 で D1、D2、および D3 という重要なエントリが変更されており、これらのエントリを、優先度同期を介して server2 および server3 間で同期させる必要がある場合には、まず D1 が server2 および server3 と同期されます。次に D2 が server2 および server3 と同期され、その後、D3 が server2 および server3 と同期されます。キュー内の以前のエントリがサーバのいずれかと正常に同期していない場合でも、その他のエントリの同期には影響しません。

図 25 優先度同期キュー



iMonitor で優先度同期キューサイズを指定するには、[エージェント同期] の下にある [エージェント環境設定] を使用します。詳細については、209 ページの「[DS エージェントを制御および環境設定する](#)」を参照してください。

優先度同期プロセス中、多数の変更が短い間隔で行われ、キューが最大サイズに達した場合には、キューは期限切れになり、新しいキューが形成されます。まだ同期されていない古いキュー内の変更は、通常同期によって同期されます。

優先度同期のキューサイズとして有効な値の範囲は、0 ~ 232 - 1 です。デフォルト値は 232 - 1 です。優先度同期キューサイズが 0 に設定されている場合、変更は優先度同期では同期されません。これらの変更は通常同期によって同期されます。

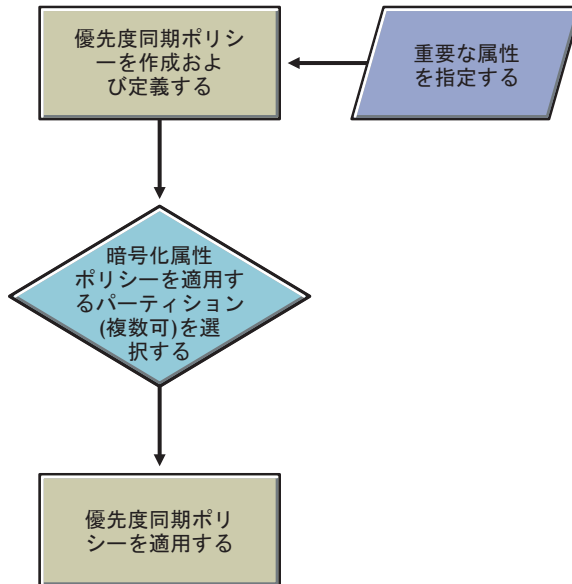
-1 を指定すると、キューサイズが無限大になります。-1 は 232 - 1 です。-3 などの負の値を指定した場合は、-3 = -1-2 となり、232 - 1-2 となります。

## 優先度同期ポリシーを管理する

優先度同期の管理は、iManager または LDAP を使用して、ポリシーを作成および定義し、パーティションに適用することで行えます。優先度同期ポリシーを定義するには、重要な属性を指定します。

注：プラグインは、Novell iManager 2.5 以降でのみ利用できます。

図 26 優先度同期プロセス



たとえば、Password および Account Number という属性が重要である場合、これらの属性を含む優先度同期ポリシー PS1 を作成できます。その後、ポリシー PS1 をパーティション P1 に適用できます。サーバ上のエントリのパスワードまたはアカウント番号を変更した場合、その変更は、パーティション P1 を持つ他のサーバと直ちに同期されます。

優先度同期が実行されるようにするには、iMonitor でアウトバウンド優先度同期およびインバウンド優先度同期が有効になっていることを確認する必要があります。インバウンド優先度同期およびアウトバウンド優先度同期は、デフォルトで有効になっています。インバウンド優先度同期およびアウトバウンド優先度同期を無効にしている場合、データへの変更は通常同期によって同期されます。

詳細については、209 ページの「DS エージェントを制御および環境設定する」を参照してください。

このセクションでは、次の情報について説明します。

- ◆ 119 ページの「優先度同期ポリシーを作成および定義する」
- ◆ 119 ページの「優先度同期ポリシーを編集する」
- ◆ 120 ページの「優先度同期ポリシーを適用する」
- ◆ 121 ページの「優先度同期ポリシーを削除する」


チャイルドパーティションを作成した場合は、ペアレントに適用されている優先度同期ポリシーがチャイルドパーティションによって継承されます。パーティションをマージした場合は、ペアレントの優先度同期ポリシーが保持されます。

## 優先度同期ポリシーを作成および定義する

優先度同期ポリシーの定義は、属性を直接選択するか、オブジェクトクラスを介して選択することで行えます。オブジェクトクラスを介して属性を選択する場合は、オブジェクトクラスの下にあるすべての属性が優先度同期に選択されます。優先度同期には、必須属性またはオプション属性を選択できます。

優先度同期ポリシーは、iManager または LDAP のいずれかを使用して、eDirectory ツリー内の任意の場所で作成できます。

### iManager を使用する場合

- 1 [役割およびタスク] ボタン  をクリックします。
- 2 [パーティションとレプリカ] > [優先度同期ポリシー] の順にクリックします。
- 3 [優先度同期ポリシー管理ウィザード] で、[作成] を選択します。
- 4 ウィザードの指示に従って、ポリシーを作成します。  
ウィザードの各段階で、[ヘルプ] が利用できます。

### LDAP を使用する場合

空の優先度同期ポリシーを作成するには、次のように指定します。

```
dn:cn=policy1,o=policies
```

```
changetype:add
```

```
objectclass:prsyncpolicy
```

優先度同期ポリシーを定義するには、優先度同期の属性をマークします。

```
dn:cn=policy2,o=policies
```

```
changetype:add
```

```
objectclass:prsyncpolicy
```


```
prsyncattributes:description
```

上の例では、Description が優先度同期としてマークされた属性です。

## 優先度同期ポリシーを編集する

優先度同期ポリシーオブジェクトの編集は、iManager または LDAP を使用して行えます。

### iManager を使用する場合

- 1 [役割およびタスク] ボタン  をクリックします。
- 2 [パーティションとレプリカ] > [優先度同期ポリシー] の順にクリックします。
- 3 [優先度同期ポリシー管理ウィザード] で、[編集] を選択します。
- 4 ウィザードの指示に従って、ポリシーを編集します。  
ウィザードの各段階で、[ヘルプ] が利用できます。

## LDAP を使用する場合

次の例では、**Description** ではなく **Surname** を優先度同期としてマークすることで、優先度同期ポリシーが変更されています。

```
dn:cn=policy2,o=policies
changetype:modify
add:prsyncattributes
prsyncattributes:surname
```

優先度同期としてマークされている属性を優先度同期ポリシーから削除するには、次のように指定します。

```
dn:cn=policy2,o=policies
changetype:modify
add:prsyncattributes
prsyncattributes:description
```


上の例では、属性 **Description** が優先度同期ポリシーから削除されています。

## 優先度同期ポリシーを適用する

1つの優先度同期ポリシーを多数のパーティションに適用できます。ただし、複数のポリシーを1つのパーティションに適用することはできません。

優先度同期ポリシーをパーティションに適用するには、iManager または LDAP を使用して行えます。

## iManager を使用する場合

- 1 [役割およびタスク] ボタン  をクリックします。
- 2 [パーティションとレプリカ] > [優先度同期ポリシー] の順にクリックします。
- 3 [優先度同期ポリシー管理ウィザード] で、[適用] を選択します。
- 4 ウィザードの指示に従って、ポリシーを適用します。  
ウィザードの各段階で、[ヘルプ] が利用できます。

## LDAP を使用する場合

優先度同期ポリシーをルートパーティションに適用するには、次のように指定します。

```
dn:
changetype:modify
add:prsyncpolicydn
prsyncpolicydn:cn=policy2,o=policies
```

上の例では、**policy2** がルートパーティションに適用されています。

優先度同期ポリシーを非ルートパーティションに適用するには、次のように指定します。

```
dn:o=org
changetype:modify
add:prsyncpolicydn
prsyncpolicydn:cn=policy2,o=policies
```

上の例では、**policy2** が非ルートパーティションに適用されています。

非ルートパーティションの優先度同期ポリシーを置き換えるには、次のように指定します。

```
dn:o=org
changetype:modify
replace:prsyncpolicydn
prsyncpolicydn:cn=policy1,o=policies
```

上の例では、**policy2** が **policy1** に置き換えられています。

優先度同期ポリシーと非ルートパーティションとの関連付けを解除するには、次のように指定します。


```
dn:o=org
changetype:modify
delete:prsyncpolicydn
```

上の例では、優先度同期ポリシーと非ルートパーティション **O=Org** との関連付けが解除されています。

### 優先度同期ポリシーを削除する

優先度同期ポリシーの削除は、iManager または LDAP を使用して行えます。

#### iManager を使用する場合

- 1 [役割およびタスク] ボタン  をクリックします。
- 2 [パーティションとレプリカ] > [優先度同期ポリシー] の順にクリックします。
- 3 [優先度同期ポリシー管理ウィザード] で、[削除] を選択します。
- 4 ウィザードの指示に従って、ポリシーを削除します。  
ウィザードの各段階で、[ヘルプ] が利用できます。

#### LDAP を使用する場合

```
dn:cn=policy1,o=policies
changetype:delete
```

## 優先度同期が失敗する場合

優先度同期は、次のような状況下で失敗する可能性があります。

- ◆ ネットワーク障害。ネットワーク障害の発生時、変更内容をリモートサーバに送信できない場合、優先度同期では変更内容が保存されません。
- ◆ 優先度同期キューサイズが最大値に達した場合。エントリ数が優先度同期キューサイズを超えた場合、優先度同期では、優先度同期キュー内の変更が無視されます。
- ◆ スキーマ同期の失敗。スキーマが同期されていない場合、優先度同期プロセスは失敗します。
- ◆ オブジェクトが他のサーバに存在していない。オブジェクトの作成が同期されていない場合、優先度同期は失敗します。
- ◆ レプリカリング内でのサーバの混在。eDirectory 8.8 および eDirectory 8.8 より前のサーバの両方を実行している場合、優先度同期は失敗します。

これらの理由のいずれかのために優先度同期が失敗した場合には、重要なデータへの変更は通常同期によって同期されます。

# 4

## スキーマの管理

Novell® eDirectory™ ツリーのスキーマには、このツリーに含めることができるオブジェクト（ユーザ、グループ、プリンタなど）のクラスを定義します。スキーマによって、各オブジェクトタイプを構成する属性（プロパティ）が指定されます。属性には、オブジェクトの作成に不可欠な必須属性と、必要に応じて指定できるオプション属性があります。

eDirectory オブジェクトはそれぞれオブジェクトクラスに属し、オブジェクトクラスはオブジェクトに関連付けることのできる属性を指定します。すべての属性は一連の属性タイプに基づくもので、属性タイプもまた、一連の標準的な属性構文に基づいています。

eDirectory スキーマは、各オブジェクトの構造を制御するだけでなく、eDirectory ツリー内でのオブジェクト間の関係も制御します。スキーマルールを設定すると、オブジェクトは他のサブオーディネートオブジェクトを含むことができます。このように、スキーマによって eDirectory ツリーの構造が決まります。

組織が必要とする情報の変化に応じて、スキーマに変更を加える必要が出てくる場合があります。たとえば、ユーザオブジェクトに、以前は FAX 番号が不要であっても、現在は必要であるとします。この場合、FAX 番号を必須属性とした新しいユーザクラスを作成し、ユーザオブジェクトの作成に、この新しいユーザクラスを使用できます。

Novell iManager でスキーマ管理の役割を持つ場合、ツリーのスーパーバイザ権を持つユーザは、そのツリーのスキーマをカスタマイズして次のようなタスクを実行できます。

- ◆ スキーマ内のすべてのクラスおよび属性の一覧を表示する。
- ◆ 既存のスキーマにクラスまたは属性を追加して、スキーマを拡張する。
- ◆ クラスを作成する。名前を付けてから、属性、フラグ、追加先コンテナ、および属性の継承元のペアレントクラスを指定することにより行います。
- ◆ 名前を付けてから、構文およびフラグを設定して、属性を作成する。
- ◆ 既存クラスへ属性を追加する。
- ◆ 使用されていない、あるいは古くなったクラスまたは属性を削除する。
- ◆ 潜在的な問題を発見および解決する。

この章では次のトピックについての情報を説明します。

- ◆ 124 ページの「スキーマの拡張」
- ◆ 128 ページの「スキーマの表示」
- ◆ 128 ページの「手動でスキーマを拡張する」
- ◆ 131 ページの「eDirectory 8.7 に追加されたスキーマフラグ」
- ◆ 133 ページの「eMBox クライアントを使用してスキーマ操作を実行する」

スキーマ情報の詳細については、『*NDS Schema Reference*』（[http://developer.novell.com/ndk/doc/ndslib/index.html?schem\\_enu/data/h4q1mn1i.html](http://developer.novell.com/ndk/doc/ndslib/index.html?schem_enu/data/h4q1mn1i.html)）を参照してください。

## スキーマの拡張

新しいクラスや属性を作成することにより、ツリーのスキーマを拡張できます。eDirectory ツリーのスキーマを拡張するには、ツリー全体に対するスーパーバイザ権が必要です。

次の作業により、スキーマを拡張できます。


- ◆ クラスを作成する
- ◆ クラスを削除する
- ◆ 属性を作成する
- ◆ クラスへオプション属性を追加する
- ◆ 属性を削除する

次の作業により、補助属性のスキーマを拡張できます。

- ◆ 補助クラスを作成する
- ◆ 補助クラスのプロパティでオブジェクトを拡張する
- ◆ オブジェクトの補助プロパティを変更する
- ◆ オブジェクトから補助プロパティを削除する

### クラスを作成する

組織の必要条件の変化に応じて、既存のスキーマに対しクラスを追加できます。

- 1 Novell iManager で、[役割およびタスク] ボタン  をクリックします。
- 2 [スキーマ] > [クラスの作成] の順にクリックします。
- 3 クラスの作成ウィザードの指示に従って、オブジェクトクラスを定義します。

ウィザードの各段階で、[ヘルプ] が利用できます。

オブジェクトクラスに追加するカスタムプロパティを定義する場合は、ウィザードを終了し、最初にカスタムプロパティを定義します。詳細については、[125 ページ](#)の「属性を作成する」を参照してください。

### クラスを削除する


使用されていないクラスは、そのクラスが eDirectory ツリーのベーススキーマの一部でない限り、削除できます。iManager では、ローカルにレプリカ作成されたパーティションで現在使用されているクラスだけは削除できません。

次のような場合に、スキーマからクラスを削除できます。

- ◆ 2 つのツリーをマージし、クラスの違いを解決した場合
- ◆ 特定のクラスが不要になった場合




クラスを削除するには、次を実行します。

- 1 Novell iManager で、[役割およびタスク] ボタン  をクリックします。
- 2 [スキーマ] > [クラスの削除] の順にクリックします。
- 3 削除するクラスを選択します。  
削除可能なクラスのみが表示されます。
- 4 [削除] をクリックします。

## 属性を作成する

独自のカスタムタイプ属性を定義し、これを既存のオブジェクトクラスのオプション属性に追加できます。ただし、既存のクラスに必須属性を追加することはできません。

- 1 Novell iManager で、[役割およびタスク] ボタン  をクリックします。
- 2 [スキーマ] > [属性の作成] の順にクリックします。
- 3 属性の作成ウィザードの指示に従って、新しい属性を定義します。  
ウィザードの各段階で、[ヘルプ] が利用できます。


## クラスへオプション属性を追加する

既存のクラスにオプションの属性を追加できます。これは、次のような場合に必要になります。

- ◆ 組織の必要とする情報が変化した場合
- ◆ ツリーのマージを準備している場合

**注:** 必須属性は、クラスの作成時にのみ定義できます。

オプション属性クラスを追加するには、次を実行します。

- 1 Novell iManager で、[役割およびタスク] ボタン  をクリックします。
- 2 [スキーマ] > [属性の追加] の順にクリックします。
- 3 属性を追加するクラスを選択して、[OK] をクリックします。
- 4 [使用可能なオプション属性] リストで、追加する属性を選択して ➡ をクリックし、[追加するオプション属性] リストにこれらの属性を追加します。

誤って属性を追加したり、後で属性を削除したい場合は、[追加するオプション属性] リストで属性を選択し、← をクリックして追加する属性のリストから削除します。

- 5 [OK] をクリックします。

このクラスにオブジェクトを作成すると、ここで追加したプロパティを含むオブジェクトが作成されます。追加したプロパティの値を設定するには、オブジェクトの [その他] 一般プロパティページを使用します。

**ヒント:** 既存のクラスは、このページにある Current Attributes リストに追加して変更できます。削除できるのは、追加してからまだ [OK] をクリックしていない属性のみです。前に追加した属性や保存した属性は削除できません。


## 属性を削除する

使用されていない属性は、その属性が eDirectory ツリーのベーススキーマの一部でない限り、削除できます。

次のような場合に、スキーマから属性を削除できます。

- ◆ 2つのツリーをマージし、属性の違いを解決した場合
- ◆ 特定の属性が不要になった場合

属性を削除するには、次を実行します。


- 1** Novell iManager で、[役割およびタスク] ボタン  をクリックします。
- 2** [スキーマ] > [属性の削除] の順にクリックします。
- 3** 削除する属性を選択します。  
削除可能な属性のみが表示されます。
- 4** [削除] をクリックします。

## 補助クラスを作成する


補助クラスとは、あるオブジェクトクラス全体ではなく、特定の eDirectory オブジェクトインスタンスに追加される一連のプロパティ (属性) です。たとえば、電子メールアプリケーション用として、eDirectory ツリーのスキーマに電子メールプロパティ補助クラスを追加し、必要に応じて、このプロパティを個別のオブジェクトに拡張できます。

スキーママネージャを使用すると、独自の補助クラスを定義できます。補助クラスで定義したプロパティを使用して、個別のオブジェクトを拡張できます。

補助クラスを作成するには、次を実行します。

- 1** Novell iManager で、[役割およびタスク] ボタン  をクリックします。
- 2** [スキーマ] > [クラスの作成] の順にクリックします。
- 3** クラス名およびオプションで ASN1 ID を指定して、[次へ] をクリックします。
- 4** クラスフラグを設定する場合は [補助クラス] をクリックし、[次へ] をクリックします。
- 5** クラスの作成ウィザードの指示に従って、新しい補助クラスを定義します。  
ウィザードの各段階で、[ヘルプ] が利用できます。

## 補助クラスのプロパティでオブジェクトを拡張する

- 1** Novell iManager で、[役割およびタスク] ボタン  をクリックします。
- 2** [スキーマ] > [オブジェクトの拡張] の順にクリックします。
- 3** 拡張するオブジェクトの名前およびコンテキストを指定して、[OK] をクリックします。

- 4 使用する補助クラスが [現在の補助クラスの拡張] の下にすでに表示されているかどうかに応じて、適切な操作を実行します。

---

**補助クラスがリストに表示 操作  
されている**


---

|     |  |
|-----|--|
| はい  | この手順を終了します。代わりに、127 ページの「 <b>オブジェクトの補助プロパティを変更する</b> 」を参照してください。 |
| いいえ | [追加] をクリックし、補助クラスを選択して、[OK] をクリックします。                            |


---

- 5 [閉じる] をクリックします。

## オブジェクトの補助プロパティを変更する

- 1 Novell iManager で、[役割およびタスク] ボタン  をクリックします。
- 2 [eDirectory 管理] > [オブジェクトの変更] の順にクリックします。
- 3 変更するオブジェクトの名前およびコンテキストを指定して、[OK] をクリックします。
- 4 [全般] タブで、[その他] ページをクリックします。
- 5 表示された画面で、必要な属性値を設定します。
  - ◆ 値のない属性をダブルクリックし、値のある属性のリストに追加します。
  - ◆ 値のある属性を選択し、[編集] をクリックして属性を編集するか、[削除] をクリックして属性を削除します。
  - ◆ 正しく設定するためには、各プロパティの構文について理解している必要があります。詳細については、[Understanding Schema Manager \(http://www.novell.com/documentation/lg/ndsv8/docui/index.html#./usnds/schm\\_enu/data/hnpkthb2.html\)](http://www.novell.com/documentation/lg/ndsv8/docui/index.html#./usnds/schm_enu/data/hnpkthb2.html) を参照してください。
- 6 [適用] をクリックし、[OK] をクリックします。

## オブジェクトから補助プロパティを削除する

- 1 Novell iManager で、[役割およびタスク] ボタン  をクリックします。
- 2 [スキーマ] > [オブジェクトの拡張] の順にクリックします。
- 3 拡張するオブジェクトの名前およびコンテキストを指定して、[OK] をクリックします。
- 4 [現在の補助クラスの拡張] のリストから、削除するプロパティが定義されている補助クラスを選択します。
- 5 [削除] をクリックし、[OK] をクリックします。

これにより、オブジェクトに最初から定義されていたプロパティを除き、補助クラスによって追加されたすべてのプロパティが削除されます。
- 6 [閉じる] をクリックします。



## スキーマの表示

スキーマが組織の情報のニーズに合ったものかどうかを評価するために、スキーマを表示したり印刷することができます。組織が大きく、また複雑になると、スキーマをカスタマイズする必要も大きくなります。しかし、小規模な組織でも、特別な記録を必要とする場合があるかもしれません。このような場合、スキーマの表示や印刷は、ベーススキーマにどのような拡張が必要かを定めるのに役立ちます。



## クラス情報を参照する

iManager の Class Information ページには、選択されたクラスに関する情報が表示され、そこで属性を追加できます。このページに表示されているほとんどの情報は、クラスが作成されたときに指定されたものです。オプション属性の中には、後で追加されたものもあります。

クラスの作成中に、そのクラスを他のクラスの属性を継承するように指定した場合は、継承された属性はペアレントクラスの中に分類されます。たとえば、オブジェクトクラスがペアレントクラスで必須属性である場合、このページには、選択されたクラスの必須属性として表示されます。

- 1 Novell iManager で、[役割およびタスク] ボタン  をクリックします。
- 2 [スキーマ] > [クラス情報] の順にクリックします。
- 3 情報を表示するクラスを選択し、[表示] をクリックします。  
詳細については、 をクリックしてください。

## 属性情報を表示する

- 1 Novell iManager で、[役割およびタスク] ボタン  をクリックします。
- 2 [スキーマ] > [属性の情報] の順にクリックします。
- 3 情報を表示する属性を選択し、[表示] をクリックします。  
詳細については、 をクリックしてください。

## 手動でスキーマを拡張する

.sch 拡張子の付いたファイルを使用して、手動で eDirectory スキーマを拡張できます。

このセクションでは、次の情報について説明します。

- ◆ 129 ページの「NetWare でスキーマを拡張する」
- ◆ 129 ページの「Windows でスキーマを拡張する」
- ◆ 129 ページの「Linux、Solaris、AIX、または HP-UX システムでスキーマを拡張する」

## NetWare でスキーマを拡張する

NWConfig.nlm を使用して、NetWare サーバのスキーマを拡張します。eDirectory に付属しているスキーマファイル (\*.sch) は、sys:¥system¥schema ディレクトリにインストールされます。

- 1 サーバコンソールで、「nwconfig」と入力します。
- 2 [ディレクトリオプション] > [スキーマの拡張] の順に選択します。
- 3 管理権を持つユーザとしてログインします。
- 4 を押して異なるパスを指定し、**sys:¥system¥schema** (または \*.sch ファイルのパス) とスキーマファイルの名前を入力します。
- 5 <Enter> キーを押します。

## Windows でスキーマを拡張する

NDSCons.exe を使用して、Windows サーバのスキーマを拡張します。eDirectory に付属しているスキーマファイル (\*.sch) は、デフォルトで C:¥Novell¥NDS ディレクトリにインストールされます。

- 1 [スタート] > [設定] > [コントロールパネル] > [Novell eDirectory サービス] の順にクリックします。
- 2 install.dlm をクリックし、[開始] をクリックします。
- 3 [追加のスキーマファイルのインストール] をクリックし、[次へ] をクリックします。
- 4 管理権を持つユーザとしてログインし、[OK] をクリックします。
- 5 スキーマファイルのパスと名前を指定します。
- 6 [完了] をクリックします。

## Linux、Solaris、AIX、または HP-UX システムでスキーマを拡張する

次のセクションでは、Linux、Solaris、AIX、および HP-UX システムでのスキーマの拡張について説明します。

- ◆ [129 ページの「ndssch ユーティリティを使用して、Linux、Solaris、AIX、または HP-UX システム上のスキーマを拡張する」](#)
- ◆ [130 ページの「RFC 2307 スキーマを拡張する」](#)

### ndssch ユーティリティを使用して、Linux、Solaris、AIX、または HP-UX システム上のスキーマを拡張する

Novell iManager のほかにも、eDirectory スキーマ拡張ユーティリティ ndssch を使用して、Linux、Solaris、AIX、または HP-UX システム上のスキーマを拡張することができます。ツリーのスキーマの変更処理では、スキーマファイル (.sch) に指定された属性とクラスが使用されます。.sch ファイルで指定した内容に従って、属性とクラスの関連付けが作成されます。

## 1 次の構文を使用します。

```
ndssch [-h ホスト名[:ポート]] [-t ツリー名] 管理者 FDN スキーマファイル...
```

```
ndssch [-h ホスト名[:ポート]] [-t ツリー名] [-d] 管理者 FDN スキーマファイル  
[スキーマの説明]...
```

| ndssch のパラメータ | 説明   |
|---------------|--|
| -h ホスト名       | スキーマを拡張するサーバの名前または IP アドレス。指定したサーバが属しているツリーのスキーマが拡張されます。スキーマを拡張するホスト上にツリーがある場合のみ、オプションで指定するパラメータです。それ以外の場合は、必須パラメータです。   |
| ポート           | サーバポート。  |
| -t ツリー名       | スキーマを拡張するツリーの名前。このパラメータの指定は任意です。/etc/opt/novell/eDirectory/conf/nds.conf ファイルに指定された値がデフォルトのツリー名として使用されます。詳細については、『Novell eDirectory 8.8 インストールガイド』の「 <a href="#">環境設定パラメータ</a> 」を参照してください。 |
| 管理者 FDN       | ツリーに対する eDirectory 管理権を持つユーザのフルコンテキスト付きの名前。  |
| スキーマファイル      | 拡張するスキーマについての情報が入力されたファイルの名前。  |
| -d, スキーマの説明   | このオプションが使用されている場合、各スキーマファイルはスキーマファイルの説明を伴っています。  |

## RFC 2307 スキーマを拡張する

RFC 2307 (<http://www.ietf.org/rfc/rfc2307.txt>) に定義されている属性とオブジェクトクラスは、ユーザまたはグループ関連、および NIS 関連のものです。ユーザまたはグループ関連の定義は、/opt/novell/eDirectory/lib/nds-modules/schema/rfc2307-usergroup.sch ファイルにコンパイルされます。NIS 関連の定義は、/opt/novell/eDirectory/lib/nds-modules/schema/rfc2307-nis.sch ファイルにコンパイルされます。それぞれに対応する LDIF 形式のファイルもあります (ユーザ/グループ関連は /opt/novell/eDirectory/lib/nds-modules/schema/rfc2307-usergroup.ldif、NIS 関連は /opt/novell/eDirectory/lib/nds-modules/schema/rfc2307-nis.ldif)。

RFC 2307 スキーマを拡張するには、ndssch ユーティリティまたは ldapmodify ツールを使用します。

- ◆ [130 ページの「ndssch ユーティリティを使用する」](#)
- ◆ [131 ページの「ldapmodify ユーティリティを使用する」](#)

### ndssch ユーティリティを使用する

次のいずれかのコマンドを入力します。

```
ndssch -t /opt/novell/eDirectory/lib/nds-schema/rfc2307-usergroup.sch
```

または

```
ndssch -t /opt/novell/eDirectory/lib/nds-schema/rfc2307-nis.sch
```

| パラメータ | 説明   |
|-------|--|
| -t    | スキーマを拡張するツリーの名前。このパラメータの指定は任意です。このパラメータが指定されていない場合、 <code>/etc/opt/novell/eDirectory/conf/nds.conf</code> ファイルに指定されたツリー名が使用されます。 |

### ldapmodify ユーティリティを使用する

次のいずれかのコマンドを入力します。

```
ldapmodify -h -D -w -f /opt/novell/eDirectory/lib/nds-schema/
rfc2307-usergroup.ldif
```

または

```
ldapmodify -h -D -w -f /opt/novell/eDirectory/lib/nds-schema/
rfc2307-nis.ldif
```

| パラメータ       | 説明   |
|-------------|--|
| -h LDAP ホスト | LDAP サーバの実行場所となっている代替ホストを指定します。  |
| -D バインドDN   | 「バインドDN」を使用して X.500 ディレクトリにバインドします。「バインドDN」には、RFC 1779 に定義されている文字列表現の DN を指定します。 |
| -w パスワード    | 簡易認証のパスワードとして、「パスワード」を使用します。   |
| -f ファイル     | エントリ情報を標準入力ではなく「ファイル」から読み出します。   |

## eDirectory 8.7 に追加されたスキーマフラグ

READ\_FILTERED および BOTH\_MANAGED スキーマフラグが、eDirectory 8.7 に追加されました。

READ\_FILTERED は、属性が LDAP オペレーショナル属性であることを示すために使用されます。LDAP がこのフラグを使用するのは、スキーマを読み込んで属性が「オペレーショナル」であることを知らせる必要がある場合です。内部定義のスキーマ属性には、このフラグが設定されたものもあります。LDAP 「オペレーショナル」定義には、3つのスキーマフラグがあります。新しい READ\_FILTERED フラグとは別に、既存のフラグとして「オペレーショナル」を示すものには READ\_ONLY フラグと HIDDEN フラグがあります。これらのフラグのいずれかがスキーマ定義に存在する場合、LDAP は属性を「オペレーショナル」として扱い、特に必要がない場合はその属性を返しません。

BOTH\_MANAGED は、セキュリティ権利を強制する新しいメカニズムです。これは識別名構文の属性にのみ重要なフラグです。この属性に設定された場合、要求している接続には、ターゲットオブジェクトと属性、およびターゲット属性によって参照されているオブジェクトの両方に対する権利が必要になります。これは、現在の WRITE\_MANAGED フラグの機能を拡張したものです。このフラグは、現在ベーススキーマ属性には設定されていません。この新しいセキュリティ動作は eDirectory 8.7.x サーバ上でのみ実行されるため、このフラグに関連する動作に矛盾がないようにするには、ツリー全体を eDirectory 8.7 以降に更新する必要があります。

eDirectory 8.7.x サーバだけがこれらの新しいフラグを認識するため、ルートパーティションのコピーを格納する eDirectory 8.7.x サーバによってのみ、これらのフラグをスキーマ定義に設定できます。これは、ルートを格納するサーバのみがスキーマを変更できるためです。通常インストールの新規サーバや、ルートパーティションを保持していない既存サーバをアップグレードしたサーバでは、これらの新しいフラグをツリー内のスキーマに追加することはできません。

これらの新しい機能のいずれかをツリーで有効にする場合は、スキーマが正常に拡張されていて、これらの新しいフラグを追加できることを確認する必要があります。確認する方法には次の 2 つがあります。1 つは、ルートパーティションの書き込み可能なコピーを持つサーバを選択して、eDirectory 8.7 以降にアップグレードすることです。これにより、自動的にスキーマが正しく拡張され、新しいフラグに対応します。

2 つ目の方法はさらに込み入ったものです。次の手順に従って操作します。

- 1** 新しく 8.7.x サーバをインストールするか、ツリー内の既存のサーバをアップグレードします。このサーバが [Root] のコピーを保持している必要はありません。
- 2** ルートパーティションのコピーをこの新しいサーバに手動で追加します。
- 3** 次に示す適切なスキーマ拡張ファイルをこのサーバ上で再実行し、スキーマを拡張します。

| プラットフォーム                | 手順   |
|-------------------------|--|
| Windows                 | install.dlm をロードし、[追加のスキーマファイルのインストール] をクリックします。   |
| NetWare                 | nwconfig をロードし、[ディレクトリオプション] > [スキーマの拡張] の順にクリックします。   |
| Linux、Solaris、AIX、HP-UX | ndssch ユーティリティを使用します。詳細については、 <a href="#">129 ページの「ndssch ユーティリティを使用して、Linux、Solaris、AIX、または HP-UX システム上のスキーマを拡張する」</a> を参照してください。 |

- 4** これらの新しいフラグが設定された新しいスキーマファイルをインストールします。
- 5** (オプション) スキーマの同期後は、このサーバからルートレプリカを削除できます。

**注:** これらの新しいスキーマフラグにより、オプションの機能が有効になります。新しい機能を必要としない場合は、スキーマ定義にこれらの新しいフラグが存在しなくても、ツリー内での eDirectory の通常操作に問題が起こることはありません。READ\_FILTERED フラグの場合は、属性の定義によっては存在しないことがあります。このため、オブジェクトのすべての属性に対する LDAP 読み込み要求によって、フラグが存在すれば読み込まないはずのデータが余分に取得される場合があります。READ\_FILTERED フラグを含む属性の中には、READ\_ONLY フラグまたは HIDDEN フラグが存在するために、やはりオペレーショナルとして扱われるものもあります。BOTH\_MANAGED フラグは、すべてのサーバがアップグレードされたツリーでのみ有効になります。その環境の中でのみ、この機能を矛盾なく操作することが可能なためです。



# eMBox クライアントを使用してスキーマ操作を実行する

eMBox (eDirectory Management Toolbox) クライアントはコマンドライン Java クライアントで、これを使用すると DSSchema 操作にリモートでアクセスできます。DSSchema eMTool を使用すると、スキーマの同期、リモートスキーマのインポート、新規スキーマエポックの宣言、ローカルスキーマのリセット、グローバルスキーマの更新などを実行できます (通常、DSRepair を使用して実行する操作です。詳細については、[278 ページの「スキーマの保守」](#)を参照してください)。

emboxclient.jar ファイルは、eDirectory の一部としてサーバにインストールされます。JVM をインストールしていれば、どのコンピュータでも実行できます。eMBox クライアントの詳細については、[555 ページの「eMBox コマンドラインクライアントの使用」](#)を参照してください。

## DSSchema eMTool を使用する

- 1 コマンドラインで次のように入力して、対話式モードで eMBox クライアントを実行します。

```
java -cp ファイルのパス/emboxclient.jar embox -i
```

(クラスパスに emboxclient.jar ファイルがすでに含まれている場合は、**java embox -i** と入力するだけです。)

eMBox Client のプロンプトが次のように表示されます。

```
eMBox Client>
```

- 2 修復するサーバにログインするには、次のように入力します。

```
login -s サーバの名前または IP アドレス -p ポート番号  
-u ユーザ名 . コンテキスト -w パスワード -n
```

ポート番号は通常 80 または 8028 です。ただし、すでにそのポートを使用している Web サーバが存在する場合は異なります。-n オプションを使用すると、非セキュア接続を開始します。

eMBox クライアントはログインが成功したかどうかを表示します。

- 3 次の構文を使用して修復コマンドを入力します。

```
dsschema. タスク オプション
```

例 :

dsschema.rst は、このサーバのスキーマを同期するようツリーのルートのみをマスタープリカに要求します。

dsschema.irs -nMyTree によって、MyTree というツリーからリモートスキーマがインポートされます。

各スイッチの間にはスペースが必要です。スイッチの順序は重要ではありません。

eMBox クライアントは修復が成功したかどうかを表示します。

DSSchema eMTool オプションの詳細については、[134 ページの「DSSchema eMTool オプション」](#)を参照してください。

- 4 eMBox クライアントからログアウトするには、次のコマンドを入力します。

```
logout
```

- 5 eMBox クライアントを終了するには、次のコマンドを入力します。

```
exit
```

## DSSchema eMTool オプション

次の表に、DSSchema eMTool オプションを示します。eMBox クライアントで `list -tdsschema` コマンドを使用して、DSSchema オプションの詳細を表示することもできます。詳細については、559 ページの「[eMTool とそのサービスを表示する](#)」を参照してください。

| オプション       | 説明  |
|-------------|---|
| rst         | ツリーのルートのマスタレプリカのスキーマをこのサーバに同期します。                 |
| irs -n ツリー名 | 別のツリーからリモートスキーマをインポートします。                         |
| dse         | ルートのマスタレプリカを持つサーバ上で新規スキーマエポックを宣言します。              |
| rls         | ローカルスキーマを、ルートパーティションのマスタレプリカがあるサーバからのコピーでリセットします。 |
| gsu         | Post NetWare 5 レベルへのグローバルスキーマ更新を実行します。            |
| scc         | ドメインクラスのスキーマサーキュラ包含ルールを追加します。                     |

# 5

## パーティションおよびレプリカの管理

パーティションは、eDirectory ツリー内の個別のデータユニットを構成する Novell® eDirectory™ データベースの論理区分です。システム管理者は、パーティションを利用して eDirectory 情報を格納し、レプリカを作成します。各パーティションは、コンテナオブジェクト、コンテナオブジェクトに含まれるすべてのオブジェクト、およびこれらのオブジェクトについての情報で構成されます。パーティションには、ファイルシステムに関する情報、またはパーティションに含まれるディレクトリやファイルに関する情報はありません。

各サーバに eDirectory データベース全体のコピーを保存する代わりに、eDirectory パーティションのコピーを作成してそれをネットワーク内の複数のサーバ上で保存できます。パーティションのそれぞれのコピーはレプリカと呼ばれます。各 eDirectory パーティションのレプリカは任意の数だけ作成することができ、任意のサーバに保存できます。レプリカのタイプには、マスタ、読み書き可能、読み込み専用、サブオーディネートリファレンス、フィルタ済み読み書き可能、およびフィルタ済み読み込み専用があります。

次の表で、レプリカタイプについて説明します。

| レプリカ                 | 説明  |
|----------------------|---|
| マスタ、読み書き可能、および読み込み専用 | 特定のパーティションのすべてのオブジェクトおよび属性が含まれます。   |
| サブオーディネートリファレンス      | ツリーの接続のために使用されます。   |
| フィルタ済みレプリカ           | <p>パーティション全体の情報のサブセットで、必要なクラスおよび属性が含まれます。必要なクラスおよび属性は、サーバのレプリケーションフィルタによって定義されます。レプリケーションフィルタは、インバウンド同期やローカルでの変更時にレプリカに含めることのできるクラスおよび属性を識別するために使用されます。</p> <p>フィルタ済みレプリカによって、管理者はまばらで断片的なレプリカを作成できます。</p> <ul style="list-style-type: none"><li>指定したオブジェクトクラスだけが含まれるスパースレプリカ</li><li>指定した属性だけが含まれる断片レプリカ</li></ul> <p>フィルタ済みレプリカの機能によって、アプリケーションが eDirectory に格納されているデータを取得するときのレスポンスが迅速になります。また、フィルタ済みレプリカを使用すると、1つのサーバにより多くのレプリカを格納できます。</p> |

| レプリカ             | 説明   |
|------------------|--|
| 読み書き可能フィルタ済みレプリカ | サーバのレプリケーションフィルタのサブセットであるクラスおよび属性をローカルで変更できます。ただし、これらのレプリカを作成できるのは、レプリケーションフィルタ内にそのクラスの必須属性がすべて含まれている場合のみです。 |
| 読み込み専用フィルタ済みレプリカ | ローカルで変更できません。  |

この章では、パーティションおよびレプリカの管理方法を説明します。

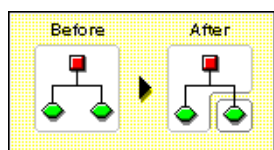
- ◆ 136 ページの「パーティションの作成」
- ◆ 137 ページの「パーティションのマージ」
- ◆ 138 ページの「パーティションの移動」
- ◆ 139 ページの「パーティションの作成操作またはマージ操作のキャンセル」
- ◆ 140 ページの「レプリカの管理」
- ◆ 143 ページの「フィルタ済みレプリカを設定し管理する」
- ◆ 146 ページの「パーティションおよびレプリカを表示する」

## パーティションの作成

パーティションを作成すると、ツリーの論理区分が作成されます。これらの論理区分は、ネットワーク内にある別の eDirectory サーバ間で複製したり配布することができます。

新しいパーティションを作成すると、ペアレントパーティションが分割されて2つのパーティションになります。新しいパーティションは、次の図で示されるように、チャイルドパーティションになります。

図 27 パーティションの分割前と分割後




たとえば、1つの部門を選択し、これを新しいパーティションとして作成すると、選択した部門およびそのサブオーディネートオブジェクトすべてがペアレントパーティションから分割されます。

選択した部門は、新しいパーティションのルートになります。新しいパーティションのレプリカは、ペアレントパーティションのレプリカと同じサーバに存在します。また、新しいパーティションのオブジェクトは、そのパーティションのルートオブジェクトに属します。

レプリカすべてを新しいパーティション情報と同期する必要があるため、パーティションの作成には時間がかかる場合があります。パーティションの作成中に別のパーティション操作を実行しようとするすると、パーティションが使用中であることを示すメッセージが表示されます。

新しいパーティションのレプリカリストを参照し、リスト内のレプリカがすべてオン  
の状態であれば、操作が完了していることがわかります。状態は自動的にリフレッ  
シュされないので、画面を定期的に手動でリフレッシュします。

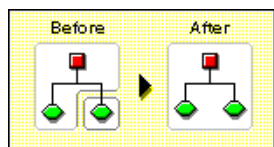
パーティションを作成するには、次の操作を行います。

- 1 Novell iManager で、[役割およびタスク] ボタン  をクリックします。
- 2 [パーティションとレプリカ] > [パーティションの作成] の順にクリックします。
- 3 新しいパーティションを作成するコンテナの名前およびコンテキストを指定して、  
[OK] をクリックします。

## パーティションのマージ

パーティションをそのペアレントパーティションにマージすると、選択したパーティ  
ションおよびそのレプリカがペアレントパーティションに結合されます。パーティ  
ションは削除できません。次の図に示されるように、パーティションはマージおよび  
作成だけを行い、ディレクトリツリーがどのように論理区分に分割されるかを定義し  
ます。

図 28 パーティションのマージ前とマージ後



パーティションとそのペアレントパーティションをマージする理由として、次のよう  
なことが考えられます。

- ◆ 2つのパーティションのディレクトリ情報が密接に関連している。
- ◆ サブオーディネートパーティションを削除する場合に、その中のオブジェクトを残  
したい。
- ◆ パーティションのオブジェクトを削除する。
- ◆ パーティションのすべてのレプリカを削除する。(パーティションのマスタレプリ  
カを削除する唯一の方法は、パーティションをそのペアレントにマージすること  
です。)
- ◆ コンテナを移動した後で(ルートパーティションにサブオーディネートパーティシ  
ョンがない場合のみ)、このコンテナをパーティションとする必要がなくなった。
- ◆ 会社の組織に変更が生じたため、パーティション構造を変更することでディレクト  
リツリーを再設計する。

パーティションが大きくなる(何百ものオブジェクトが含まれる)とネットワークの応  
答時間が遅くなるため、パーティションを分割することを検討します。

ツリーのルートパーティションは最上位のパーティションであり、マージするペア  
レントパーティションがないため、マージできません。


サーバで処理が完了すると、パーティションがマージされます。パーティションのサ  
イズ、ネットワークトラフィック、サーバの環境設定などによって異なりますが、こ  
の操作の完了にはかなり時間がかかる場合があります。

**重要:** パーティションのマージを行う前に、両パーティションの同期を点検し、続行する前にすべてのエラーを修正します。エラーを修正することにより、ディレクトリでの問題を切り離し、エラーの伝播や新しいエラーの発生を防ぐことができます。

パーティションのマージを行う前に、マージするパーティションのレプリカ (サブオーディネートリファレンスを含む) を持つサーバすべてが稼働していることを確認します。サーバが停止中の場合、eDirectory はサーバのレプリカを読み込むことができず、操作を完了できません。

パーティションのマージの処理中にエラーが表示された場合は、そのつどエラーを解決します。操作を続行してエラーを修正しないでください。さらにエラーが発生するおそれがあります。

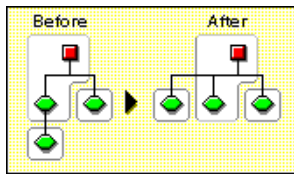
チャイルドパーティションをペアレントパーティションとマージするには、次の操作を行います。

- 1 Novell iManager で、[役割およびタスク] ボタン  をクリックします。
- 2 [パーティションとレプリカ] > [パーティションのマージ] の順にクリックします。
- 3 ペアレントパーティションとマージするパーティションの名前およびコンテキストを指定して、[OK] をクリックします。

## パーティションの移動

パーティションの移動により、ディレクトリツリー内のサブツリーを移動できます。ルートパーティションオブジェクト (コンテナオブジェクト) にサブオーディネートパーティションがない場合にのみ、このオブジェクトを移動できます。

図 29 パーティションの移動前と移動後



パーティションを移動する場合、eDirectory 包含ルールに従ってください。たとえば、部門は現在のツリーのルートの直下には移動できません。これは、ルートの包含ルールにより移動が許されているのが、地域、国、または組織であるためです。

パーティションを移動すると、eDirectory は、ルートパーティションオブジェクトへの参照すべてを変更します。オブジェクトの共通名は変更されませんが、コンテナ (およびそのサブオーディネートコンテナすべて) の完全識別名は変更されます。

パーティションを移動するときに、オプションを選択して、移動するコンテナの代わりに別名オブジェクトを作成することもできます。これにより、ユーザは引き続きネットワークにログインでき、元のディレクトリ位置にオブジェクトを見つけることができます。

作成した別名オブジェクトは、移動したコンテナと同じ共通名を持ち、そのコンテナの新しい完全識別名を参照します。

**重要:** パーティションを移動したときに、移動したパーティションの代わりとなる別名オブジェクトを作成しないと、パーティションの新しい位置を知らないユーザは元のディレクトリ位置でオブジェクトを見つけようとし、ディレクトリツリーにあるパーティションオブジェクトを見つけることが困難になります。

また、ワークステーションの NAME CONTEXT パラメータがディレクトリツリーコンテナのオリジナルの位置に設定されている場合、これにより、クライアントワークステーションがログインできないという問題が起きるおそれがあります。


オブジェクトを移動すると、オブジェクトの名前コンテキストが変更されるため、移動したオブジェクトを参照する名前コンテキストのユーザは、NAME CONTEXT パラメータを更新する必要があります。これにより、名前コンテキストは、オブジェクトの新しい名前を参照するようになります。

コンテナオブジェクトの移動の後に、ユーザの NAME CONTEXT パラメータを自動的に更新するには、NCUPDATE ユーティリティを使用します。

移動したパーティションをパーティションとして使用しない場合は、それをペアレントパーティションとマージします。

パーティションを移動する前に、ディレクトリツリーが正しく同期していることを確認します。移動元パーティションと移動先パーティションのどちらかで同期のエラーが生じた場合は、パーティションの移動操作を実行しないでください。実行する前に、同期エラーを解決します。

パーティションを移動するには、次の操作を行います。

- 1 Novell iManager で、[役割およびタスク] ボタン  をクリックします。
- 2 [パーティションとレプリカ] > [パーティションの移動] の順にクリックします。
- 3 [オブジェクト名] フィールドに移動するパーティションオブジェクトの名前およびコンテキストを指定します。
- 4 [移動先] フィールドに移動するコンテナの名前およびコンテキストを指定します。
- 5 移動するパーティションについて、元の場所に別名を作成する場合は、[移動したオブジェクトの代わりに別名を作成します] を選択します。  
これにより、移動前の場所に依存するあらゆる操作は、操作を更新して移動後の場所を反映できるようになるまで、引き続き実行されます。
- 6 [OK] をクリックします。

## パーティションの作成操作またはマージ操作のキャンセル

変更を確定する段階まで操作が到達していない場合、パーティションの作成またはマージをキャンセルできます。この機能を使用して、操作を終了できます。また、eDirectory ネットワークが、eDirectory エラーを返したり、パーティション操作に続く同期に失敗した場合にもこの機能を使用します。

ディレクトリツリーのレプリカで同期エラーが生じていると、操作を中止しても問題が解決しない場合があります。ただし、初期のトラブルシューティングオプションとして、この機能を使用できます。

サーバが停止している、またはその他の理由でサーバが使用できない場合、パーティション操作を完了できるようにサーバがネットワークから見えるようにするか、操作を中止します。データベースが壊れているために eDirectory による同期ができない場合、実行中のパーティション操作すべてを中止する必要があります。

含まれるレプリカの数、サーバの可視性、および既存のワイヤトランフィックの量によりますが、パーティション操作でネットワーク間の完全な同期を行うには、かなりの時間がかかります。

パーティションが使用中であることを示すエラーが表示されても、操作を中止する必要はありません。パーティションのサイズ、接続性の問題などによって異なりますが、通常、パーティション操作は 24 時間以内に完了します。この時間枠内で操作が完了しない場合には、操作を途中で中止します。

## レプリカの管理


レプリカの追加、削除、またはレプリカタイプの変更をする前に、ターゲットレプリカの位置を慎重に計画します。[82 ページの「ツリーのレプリカ作成に関するガイドライン」](#)を参照してください。





### レプリカを追加する

次の機能をディレクトリに提供するために、レプリカをサーバに追加します。

- ◆ 障害対策
- ◆ データへのより高速なアクセス
- ◆ WAN リンク上でのより高速なアクセス
- ◆ 設定コンテキスト中のオブジェクトへのアクセス (バインダリサービスを使用)

レプリカを追加するには、次の操作を行います。

- 1 Novell iManager で、[役割およびタスク] ボタン  をクリックします。
- 2 [パーティションとレプリカ] > [レプリカビュー] の順にクリックします。
- 3 レプリカを作成するパーティションまたはサーバの名前およびコンテキストを指定して、[OK] をクリックします。
- 4 [レプリカの追加] をクリックします。
- 5 パーティションまたはサーバの名前およびコンテキストを指定します。
- 6 次のレプリカタイプのいずれかを選択します。

| レプリカタイプ  | 説明   |
|--|--|
|  読み書き可能       | ユーザは、新しいレプリカの内容の読み込みと変更を両方行うことができます。このパーティションの eDirectory オブジェクトを管理するユーザの近くに変更可能なレプリカがない場合は、このオプションを選択します。         |
|  読み込み専用       | ユーザは、新しいレプリカの内容を読み込むことはできません、変更はできません。このパーティションの eDirectory オブジェクトを読み込むだけで、変更は行わないユーザの近くにレプリカがない場合は、このオプションを選択します。 |
|  フィルタ済み読み書き可能 | ユーザは、新しいレプリカの内容の読み込みと変更を両方行うことができますが、このレプリカの内容は、フィルタで指定された eDirectory オブジェクトとプロパティのタイプに制限されます。                     |
|  フィルタ済み読み込み専用 | ユーザは、新しいレプリカの内容を読み込んでも変更はできず、このレプリカの内容は、フィルタで指定された eDirectory オブジェクトとプロパティのタイプに制限されます。                             |

- 7 [OK] をクリックします。

詳細については、[53 ページの「レプリカのタイプ」](#)を参照してください。



## レプリカを削除する

レプリカを削除すると、パーティションのレプリカはサーバから削除されます。

サーバをディレクトリツリーから削除する場合は、その前に、レプリカをサーバから削除します。レプリカを削除することで、サーバを削除するとき起きる問題を減らすことができます。

また、レプリカの削除により、ネットワークの同期トラフィックの量も削減できます。通常、パーティションに7個以上のレプリカは必要ありません。

マスタレプリカまたはサブオーディネートリファレンスは、削除できません。



マスタレプリカを削除するには、次の2つのオプションを利用します。

- ◆ マスタレプリカをパーティションの別のレプリカを含むサーバへ移動し、そのレプリカを新しいマスタレプリカにします。  
これにより、元のマスタレプリカは自動的に読み書き可能レプリカに変更され、削除できるようになります。
- ◆ パーティションをそのペアレントパーティションとマージします。  
これにより、パーティションのレプリカとペアレントパーティションのレプリカがマージされ、そのサーバからレプリカが削除されます。マージによりパーティションの境界は削除されますが、オブジェクトは削除されません。オブジェクトは、「結合」パーティションのレプリカを持つ各サーバに残ります。

レプリカを削除する場合、次の点に注意します。

- ◆ 障害対策として、異なるサーバ上に各パーティションのレプリカを3つ以上保持します。
- ◆ レプリカを削除すると、ターゲットサーバ上のディレクトリデータベースのコピーが削除されます。  
データベースは、ネットワークの別のサーバで引き続きアクセスできます。また、レプリカが含まれていたサーバも、eDirectory で引き続き機能します。  
サブオーディネートリファレンスレプリカは、削除や管理ができません。サーバがパーティションのレプリカを含む場合、サブオーディネートリファレンスレプリカは、eDirectory により自動的にサーバ上に作成されます。ただし、サーバがパーティションのチャイルドレプリカを含む場合には、作成されません。

レプリカを削除するには、次の操作を行います。

- 1** Novell iManager で、[役割およびタスク] ボタン  をクリックします。
- 2** [パーティションとレプリカ] > [レプリカビュー] の順にクリックします。
- 3** 削除するレプリカを格納するパーティションまたはサーバの名前およびコンテキストを指定して、[OK] をクリックします。
- 4** 削除するレプリカの左にある  をクリックします。
- 5** [OK] をクリックします。

## レプリカタイプを変更する


レプリカタイプを変更して、レプリカ情報へのアクセスを制御します。たとえば、既存の読み書き可能レプリカを読み込み専用レプリカに変更して、ユーザがレプリカに書き込んだり、ディレクトリデータを変更できないようにします。




読み書き可能レプリカ、または読み込み専用レプリカのタイプを変更できます。マスタレプリカのタイプは変更できませんが、読み書き可能レプリカまたは読み込み専用レプリカは、マスタレプリカに変更できます。これにより、元のマスタレプリカは、自動的に読み書き可能レプリカに変更されます。



通常、ほとんどのレプリカは、読み書き可能レプリカとして使用されます。読み書き可能レプリカには、クライアント操作による書き込みができます。変更が加えられると、読み書き可能レプリカは同期情報を送信します。読み込み専用レプリカには、クライアント操作による書き込みができません。しかし、レプリカを同期すると、読み込み専用レプリカは更新されます。

サブオーディネートリファレンスのレプリカタイプは、変更できません。サブオーディネートリファレンスがあるサーバに、パーティションのレプリカを配置するには、レプリカの追加操作を行う必要があります。サブオーディネートリファレンスレプリカは、パーティションの完全なコピーではありません。サブオーディネートリファレンスレプリカの配置および管理は、eDirectory で制御します。サーバがパーティションのレプリカを含む場合、サブオーディネートリファレンスレプリカは、eDirectory により自動的にサーバ上に作成されます。ただし、サーバがパーティションのチャイルドレプリカを含む場合には、作成されません。

レプリカタイプを変更するには、次の操作を行います。

- 1 Novell iManager で、[役割およびタスク] ボタン  をクリックします。
- 2 [パーティションとレプリカ] > [レプリカビュー] の順にクリックします。
- 3 変更するレプリカを格納するパーティションまたはサーバの名前およびコンテキストを指定して、[OK] をクリックします。
- 4 変更するレプリカのレプリカタイプ ([タイプ] 列内) をクリックします。
- 5 新しいレプリカタイプをクリックし、[OK] をクリックします。

| レプリカタイプ  | 説明   |
|--|--|
|  マスタ    | ユーザは、このレプリカの内容の読み込みと変更を行うことができ、このレプリカは、下位パーティションの作成やマージなど、このパーティションに影響を与える将来のパーティション処理の出発点となります。マスタレプリカは、パーティションごとに1つだけ設定できます。 |
|  読み書き可能 | ユーザは新しいレプリカの内容の読み込みと変更を行うことができます。このパーティションの eDirectory オブジェクトを管理するユーザの近くに変更可能なレプリカがない場合は、このオプションを選択します。                        |
|  読み込み専用 | ユーザは新しいレプリカの内容を読み込むことができますが、変更はできません。このパーティションの eDirectory オブジェクトを読み込むだけで、変更は行わないユーザの近くにレプリカがない場合は、このオプションを選択します。              |

| レプリカタイプ  | 説明  |
|--|---|
|  フィルタ済み読み書き可能 | ユーザは新しいレプリカの内容の読み込みと変更を行うことはできますが、内容はフィルタで指定された eDirectory オブジェクトとプロパティのタイプに制限されます。 |
|  フィルタ済み読み込み専用 | ユーザは新しいレプリカの内容を読み込めても変更はできず、内容はフィルタで指定された eDirectory オブジェクトとプロパティのタイプに制限されます。       |

6 [OK] をクリックします。

詳細については、53 ページの「レプリカのタイプ」を参照してください。

## フィルタ済みレプリカを設定し管理する

フィルタ済みレプリカには、eDirectory パーティションの情報のフィルタ済みサブセット (オブジェクトまたはオブジェクトクラス、およびこれらのオブジェクトの属性と値のフィルタ済みセット) が保存されます。

管理者は、フィルタ済みレプリカのセットを保持する eDirectory サーバを作成するためにフィルタ済みレプリカ機能を使用します。フィルタ済みレプリカのセットには、同期するオブジェクトおよび属性のみが含まれます。


このため、iManager では、フィルタ済みレプリカのパーティションスコープおよびフィルタを作成できるツールが用意されています。スコープとは、単に、サーバ上でレプリカを保存するパーティションのセットです。一方、レプリケーションフィルタには、サーバのフィルタ済みレプリカセットに含める eDirectory クラスおよび属性のセットが定義されます。この結果、eDirectory サーバには、ツリー内の多くのパーティションから必要なデータを抽出し明確に定義されたデータセットが保存されることとなります。

サーバのパーティションスコープおよびレプリケーションフィルタの記述は、eDirectory に格納され、iManager のサーバオブジェクトまたは [パーティションとレプリカ] 役割によって管理できます。

- ◆ 143 ページの「フィルタ処理済レプリカウィザードを使用する」
- ◆ 144 ページの「パーティションスコープを定義する」
- ◆ 145 ページの「サーバフィルタを設定する」

## フィルタ処理済レプリカウィザードを使用する

フィルタ処理済レプリカウィザードを使用すると、サーバのレプリケーションフィルタおよびパーティションスコープを、表示される手順に従って簡単に設定できます。

- 1 Novell iManager で、[役割およびタスク] ボタン  をクリックします。
- 2 [パーティションとレプリカ] > [フィルタ処理済レプリカウィザード] の順にクリックします。
- 3 フィルタ済みレプリカを設定するサーバを指定し、[次へ] をクリックします。

- 4 選択されたサーバに設定されたフィルタのクラスおよび属性を定義するには、[\[フィルタセットの定義\]](#) をクリックします。

レプリケーションフィルタには、サーバのフィルタ済みレプリカセットに保存したい eDirectory クラスおよび属性のセットが含まれます。フィルタセットの定義の詳細については、[145 ページの「サーバフィルタを設定する」](#)を参照してください。


- 5 [\[次へ\]](#) をクリックします。
- 6 このサーバのパーティションスコープを定義するには、[\[パーティションスコープの定義\]](#) をクリックします。  
パーティションスコープの詳細については、[144 ページの「パーティションスコープを定義する」](#)を参照してください。
- 7 [\[次へ\]](#) > [\[完了\]](#) の順にクリックします。

## パーティションスコープを定義する


パーティションスコープは、サーバ上でレプリカを保存するパーティションのセットです。iManager の [\[レプリカビュー\]](#) ページには、eDirectory ツリーのパーティションの階層が表示されます。個別のパーティション、指定した分岐のパーティションセット、またはツリー内のすべてのパーティションを選択できます。次に、サーバに追加するこれらのパーティションのレプリカタイプを選択するか、既存のレプリカタイプを変更します。

サーバには、完全なレプリカもフィルタ済みレプリカも保存できます。詳細については、[56 ページの「フィルタ済みレプリカ」](#)を参照してください。


### eDirectory サーバのレプリカを表示する

- 1 Novell iManager で、[\[役割およびタスク\]](#) ボタン  をクリックします。
- 2 [\[パーティションとレプリカ\]](#) > [\[レプリカビュー\]](#) の順にクリックします。
- 3 表示するサーバの名前およびコンテキストを指定して [\[OK\]](#) をクリックし、このサーバのレプリカリストを表示します。

### eDirectory サーバにフィルタ済みレプリカを追加する

- 1 Novell iManager で、[\[役割およびタスク\]](#) ボタン  をクリックします。
- 2 [\[パーティションとレプリカ\]](#) > [\[レプリカビュー\]](#) の順にクリックします。
- 3 フィルタ済みレプリカを追加するサーバの名前およびコンテキストを指定し、[\[OK\]](#) をクリックします。
- 4 [\[レプリカの追加\]](#) をクリックします。
- 5 パーティションの名前およびコンテキストを指定します。
- 6 [\[フィルタ済み読み書き可能\]](#) または [\[フィルタ済み読み込み専用\]](#) をクリックし、[\[OK\]](#) をクリックします。

## 完全なレプリカをフィルタ済みレプリカへ変更する

- 1 Novell iManager で、[役割およびタスク] ボタン  をクリックします。
- 2 [パーティションとレプリカ] > [レプリカビュー] の順にクリックします。
- 3 変更するレプリカを格納するパーティションまたはサーバの名前およびコンテキストを指定して、[OK] をクリックします。
- 4 変更するレプリカのレプリカタイプ ( [タイプ] 列内 ) をクリックします。
- 5 [フィルタ済み読み書き可能] または [フィルタ済み読み込み専用] をクリックし、[OK] をクリックします。

## サーバフィルタを設定する


サーバレプリケーションフィルタには、サーバのフィルタ済みレプリカセットに保存したい eDirectory クラスおよび属性のセットが含まれます。どのサーバオブジェクトからでもフィルタを設定できます。フィルタ済みレプリカの場合、サーバごとにフィルタを1つだけ作成できます。つまり、ある eDirectory サーバ用に定義されているフィルタは、そのサーバ上のすべてのフィルタ済みレプリカに適用されます。ただし、完全なレプリカにはフィルタは適用されません。

サーバのフィルタは必要に応じて変更できますが、変更するとレプリカの再同期が発生するため時間がかかります。サーバの機能については、慎重に計画することを推奨します。


次の方法のいずれかで、サーバのフィルタを設定または変更できます。

- ◆ [145 ページの「レプリカビューを使用する」](#)
- ◆ [145 ページの「サーバオブジェクトを使用する」](#)

### レプリカビューを使用する

- 1 Novell iManager で、[役割およびタスク] ボタン  をクリックします。
- 2 [パーティションとレプリカ] > [レプリカビュー] の順にクリックします。
- 3 変更するレプリカを格納するパーティションまたはサーバの名前およびコンテキストを指定して、[OK] をクリックします。
- 4 変更するサーバまたはパーティションの [Edit in the Filter] 列をクリックします。
- 5 適切なクラスおよび属性を追加し、[OK] をクリックします。
- 6 [完了] をクリックします。

### サーバオブジェクトを使用する

- 1 Novell iManager で、[役割およびタスク] ボタン  をクリックします。
- 2 [eDirectory 管理] > [オブジェクトの変更] の順にクリックします。
- 3 変更するレプリカを格納するサーバの名前およびコンテキストを指定して、[OK] をクリックします。
- 4 [レプリカ] タブをクリックします。

- 5 このサーバにフィルタが定義されていなかった場合、[フィルタは空です] をクリックして [フィルタの編集] ダイアログボックスを開き、目的のクラスおよび属性を追加します。

または

[Copy Filter From] をクリックし、コピーするフィルタを持つオブジェクト (別のサーバなど) を参照します。

- 6 既存のフィルタを編集するには、フィルタ内のハイパーリンク付きアイテムをクリックし、[フィルタの編集] ダイアログボックスを開いて、目的のクラスおよび属性を追加または削除します。


## パーティションおよびレプリカを表示する

このセクションでは、次の情報について説明します。

- ◆ [146 ページの「サーバのパーティションを表示する」](#)
- ◆ [146 ページの「パーティションレプリカを表示する」](#)
- ◆ [147 ページの「パーティションに関する情報を表示する」](#)
- ◆ [147 ページの「パーティションの階層を表示する」](#)
- ◆ [147 ページの「レプリカに関する情報を表示する」](#)

## サーバのパーティションを表示する

Novell iManager では、サーバに割り当てられたパーティションを表示できます。サーバオブジェクトをディレクトリツリーから削除しようとする場合、サーバに格納されているパーティションの表示が必要となる場合があります。この場合、オブジェクトを削除する前に、削除するレプリカを表示できます。


- 1 Novell iManager で、[役割およびタスク] ボタン  をクリックします。
- 2 [パーティションとレプリカ] > [レプリカビュー] の順にクリックします。
- 3 サーバオブジェクトの名前とコンテキストを入力して、[OK] をクリックします。

## パーティションレプリカを表示する

この操作により、次を識別できます。


- ◆ パーティションのレプリカが存在するサーバ
- ◆ パーティションのマスタレプリカのホストとなっているサーバ
- ◆ 読み書き可能レプリカ、読み込み専用レプリカ、およびサブオーディネートリファレンスレプリカを含むサーバ
- ◆ 各パーティションレプリカの状態

パーティションのレプリカを表示するには、次の操作を行います。

- 1 Novell iManager で、[役割およびタスク] ボタン  をクリックします。
- 2 [パーティションとレプリカ] > [レプリカビュー] の順にクリックします。
- 3 パーティションの名前とコンテキストを入力して、[OK] をクリックします。


## パーティションに関する情報を表示する

パーティションに関する情報 ( 成功した最新の同期や最近試みた同期など ) を表示する主な目的は、パーティションの同期情報を確認することです。

- 1 Novell iManager で、[役割およびタスク] ボタン  をクリックします。
- 2 [パーティションとレプリカ] > [パーティションの情報を表示します] の順にクリックします。
- 3 パーティションの名前とコンテキストを入力して、[OK] をクリックします。

## パーティションの階層を表示する

iManager では、パーティションの階層を容易に表示できます。コンテナオブジェクトを展開して、ペアレントパーティションやチャイルドパーティションを表示できます。


パーティションのルートであるコンテナには、次のアイコンが表示されます：.

## レプリカに関する情報を表示する

レプリカに関する情報を表示する主な目的は、レプリカの状態を確認することです。eDirectory レプリカの状態は、それが実行しているパーティションや複製の操作によってさまざまです。次の表では、iManager で表示されるレプリカの状態を説明しています。

| 状態     | 説明                                    |
|--------|---------------------------------------|
| オン     | 現在パーティションや複製の操作を実行していない               |
| 新規     | サーバに新しいレプリカとして追加中                     |
| 停止中    | サーバから削除中                              |
| 停止     | サーバからの削除が完了                           |
| マスタ開始  | マスタレプリカへ変更中                           |
| マスタ完了  | マスタレプリカへの変更が完了                        |
| タイプの変更 | 他のレプリカタイプへの変更中                        |
| ロック状態  | パーティションの移動または修復の操作の準備が滞っている           |
| 移動へ移行  | パーティションの移動操作を開始中                      |
| 移動     | パーティションの移動操作中                         |
| 分割へ移行  | パーティションの分割操作 ( チャイルドパーティションの作成 ) を開始中 |
| 分割     | パーティションの分割 ( チャイルドパーティションの作成 ) 操作中    |
| 結合     | ペアレントパーティションへのマージ中                    |
| オンへ移行  | オン状態へ戻る直前                             |
| 不明     | iManager で認識できない状態                    |

レプリカの情報を表示するには、次の操作を行います。

- 1** Novell iManager で、[役割およびタスク] ボタン  をクリックします。
- 2** [パーティションとレプリカ] > [レプリカビュー] の順にクリックします。
- 3** パーティションまたはサーバの名前およびコンテキストを入力して、[OK] をクリックします。



# 6

## Novell eDirectory 管理ユーティリティ

この章では、Novell® eDirectory™ で提供されている次のユーティリティについて説明します。

- ◆ 149 ページの「Novell インポート / エクスポート変換ユーティリティ」
- ◆ 188 ページの「インデックスマネージャ」
- ◆ 193 ページの「プレディケートデータ」
- ◆ 194 ページの「eDirectory Service Manager」

### Novell インポート / エクスポート変換ユーティリティ

Novell インポート / エクスポート変換ユーティリティは次の操作に使用できます。

- ◆ LDIF ファイルから LDAP ディレクトリへのデータのインポート
- ◆ LDAP ディレクトリから LDIF ファイルへのデータのエクスポート
- ◆ LDAP サーバ間でのデータの移行
- ◆ スキーマの比較と更新の実行
- ◆ テンプレートを使用した eDirectory への情報のロード
- ◆ SCH ファイルから LDAP ディレクトリへのスキーマのインポート

Novell インポート / エクスポート変換ユーティリティは、形式に応じてデータを読み書きするための一連のハンドラを管理します。データを読み込むハンドラをソースハンドラと呼び、データを書き込むハンドラをターゲットハンドラと呼びます。1つの実行可能モジュールがソースハンドラとターゲットハンドラの両方として機能することもあります。Novell インポート / エクスポート変換エンジンは、ソースハンドラからデータを受け取ってそれを処理し、処理したデータをターゲットハンドラに渡します。

たとえば、LDIF データを LDAP ディレクトリにインポートする場合、Novell インポート / エクスポート変換エンジンは、LDIF ソースハンドラを使用して LDIF ファイルを読み込み、読み込んだデータを LDAP ターゲットハンドラを使用して LDAP ディレクトリサーバに送信します。LDIF ファイルの構文、構造およびデバッグの詳細については、「[LDIF ファイルのトラブルシューティング](#)」を参照してください。

Novell インポート / エクスポート変換クライアントユーティリティは、コマンドライン、ConsoleOne® スナップイン、または Novell iManager のインポート / エクスポート変換ウィザードから実行できます。ただし、コマンド区切りのデータに対応したハンドラは、コマンドラインユーティリティと Novell iManager でのみ使用できます。

Novell インポート / エクスポート変換ユーティリティは、次のどちらの方法でも使用できます。

- ◆ 150 ページの「Novell iManager インポート / エクスポート変換ウィザードを使用する」
- ◆ 158 ページの「コマンドラインインタフェースを使用する」

Novell インポート / エクスポート変換エンジンには、ウィザードからもコマンドラインインタフェースからもアクセスできます。ただし、ソースハンドラとターゲットハンドラの組み合わせの選択肢は、コマンドラインインタフェースを使用する場合のほうが多くなります。

NDS および eDirectory の旧バージョンで提供されていた BULKLOAD ユーティリティと ZONEIMPORT ユーティリティはどちらも、Novell インポート / エクスポート変換ユーティリティに変更されました。


## Novell iManager インポート / エクスポート変換ウィザードを使用する

インポート / エクスポート変換ウィザードは次の操作に使用できます。

- ◆ LDIF、区切りテキストファイル、スキーマファイルまたは LOAD ファイルからのデータのインポート。
- ◆ LDIF ファイルへのデータのエクスポート。
- ◆ サーバ間でのデータの移行。
- ◆ LDIF またはスキーマファイルからサーバへのデータの追加。
- ◆ あるサーバから別のサーバへのデータの追加。
- ◆ LDIF またはスキーマファイルと別の LDIF ファイルの間のデータ比較。
- ◆ サーバと LDIF ファイルの間のデータ比較。
- ◆ 順序ファイルの生成。

Novell iManager の使用方法とアクセス方法の詳細については、『[Novell iManager 2.5 管理ガイド](http://www.novell.com/documentation/imanager25/index.html)』(<http://www.novell.com/documentation/imanager25/index.html>) を参照してください。

### データをファイルからインポートする


- 1 Novell iManager で、[役割およびタスク] ボタン  をクリックします。
- 2 [eDirectory の保守] > [インポート / エクスポート変換ウィザード] の順にクリックします。
- 3 [ディスク上のファイルからデータをインポート] をクリックし、[次へ] をクリックします。
- 4 インポートするファイルのタイプを選択します。
- 5 インポートするデータが含まれているファイルの名前を指定し、適切なオプションを指定してから [次へ] をクリックします。  
このページのオプションは、選択したファイルのタイプによって異なります。使用可能なオプションの詳細については、[ヘルプ] をクリックしてください。
- 6 データのインポート先になる LDAP サーバを指定します。

- 7 次の表の説明を参照して、適切なオプションを追加します。

| オプション               | 説明   |
|---------------------|--|
| サーバの DNS 名 /IP アドレス | 相手 LDAP サーバの DNS 名または IP アドレス                                  |
| ポート                 | 相手 LDAP サーバのポート番号 ( 整数 )                                       |
| DER ファイル            | SSL 認証に使用するサーバキーが格納されている DER ファイルの名前                           |
| ログイン方法              | [ 認証ログイン ] または [ 匿名ログイン ] ( [ ユーザ DN ] フィールドに指定したエントリのログイン方法 ) |
| ユーザ DN              | サーバで指定されたバインド操作に使用されるエントリの識別名                                  |
| パスワード               | [ ユーザ DN ] フィールドで指定したエントリのパスワード属性                              |

- 8 [ 次へ ] > [ 完了 ] の順にクリックします。

### データをファイルへエクスポートする

- Novell iManager で、[ 役割およびタスク ] ボタン  をクリックします。
- [ eDirectory の保守 ] > [ インポート / エクスポート 変換ウィザード ] の順にクリックします。
- [ ディスク上のファイルにデータをエクスポート ] > [ 次へ ] の順にクリックします。
- エクスポートするエントリが格納されている LDAP サーバを指定します。  
[ 詳細設定 ] を使用して、LDAP ソースハンドラの追加オプションを設定します。  
使用可能なオプションの詳細については、[ ヘルプ ] をクリックしてください。
- 次の表の説明を参照して、適切なオプションを追加します。

| オプション               | 説明   |
|---------------------|--|
| サーバの DNS 名 /IP アドレス | ソース LDAP サーバの DNS 名または IP アドレス                                 |
| ポート                 | ソース LDAP サーバのポート番号 ( 整数 )                                      |
| DER ファイル            | SSL 認証に使用するサーバキーが格納されている DER ファイルの名前                           |
| ログイン方法              | [ 認証ログイン ] または [ 匿名ログイン ] ( [ ユーザ DN ] フィールドに指定したエントリのログイン方法 ) |
| ユーザ DN              | サーバで指定されたバインド操作に使用されるエントリの識別名                                  |
| パスワード               | [ ユーザ DN ] フィールドで指定したエントリのパスワード属性                              |

- 6 [ 次へ ] をクリックします。

- 7 エクスポートするエントリの検索条件を次のように指定します。

| オプション  | 説明   |
|--------|--|
| ベース DN | 検索要求のベース識別名<br><br>このフィールドを指定しなかった場合、デフォルトのベース DN である ""(空の文字列) が使用されます。 |
| スコープ   | 検索要求のスコープ  |
| フィルタ   | RFC 1558 準拠の検索フィルタ<br><br>デフォルトは「objectclass=*」です。                       |
| 属性     | 検索エントリごとに取得する属性  |


- 8 [次へ] をクリックします。

- 9 エクスポートするファイルのタイプを選択します。

エクスポートされたファイルは、一時的な場所に保存されます。このファイルは、インポート / エクスポート変換ウィザードの最後でダウンロードできます。

- 10 [次へ] > [完了] の順にクリックします。

## LDAP サーバ間でデータを移行する

- Novell iManager で、[役割およびタスク] ボタン  をクリックします。
- [eDirectory の保守] > [インポート / エクスポート変換ウィザード] の順にクリックします。
- [Migrate Data Between Servers] > [次へ] の順にクリックします。
- 移行するエントリが格納されている LDAP サーバを指定します。  
[詳細設定] を使用して、LDAP ソースハンドラの追加オプションを設定します。使用可能なオプションの詳細については、[ヘルプ] をクリックしてください。
- 次の表の説明を参照して、適切なオプションを追加します。


| オプション                | 説明   |
|----------------------|--|
| サーバの DNS 名 / IP アドレス | ソース LDAP サーバの DNS 名または IP アドレス                           |
| ポート                  | ソース LDAP サーバのポート番号 (整数)                                  |
| DER ファイル             | SSL 認証に使用するサーバキーが格納されている DER ファイルの名前                     |
| ログイン方法               | [認証ログイン] または [匿名ログイン] ( [ユーザ DN] フィールドに指定したエントリのログイン方法 ) |
| ユーザ DN               | サーバで指定されたバインド操作に使用されるエントリの識別名                            |
| パスワード                | [ユーザ DN] フィールドで指定したエントリのパスワード属性                          |

- 6 [次へ] をクリックします。
- 7 移行するエントリの検索条件を次のように指定します。

| オプション  | 説明   |
|--------|--|
| ベース DN | 検索要求のベース識別名<br>このフィールドを指定しなかった場合、デフォルトのベース DN である ""( 空の文字列 ) が使用されます。 |
| スコープ   | 検索要求のスコープ  |
| フィルタ   | RFC 2254 準拠の検索フィルタ<br>デフォルトは「objectclass=*」です。                         |
| 属性     | 検索エントリごとに取得する属性  |

- 8 [次へ] をクリックします。
- 9 データを移行する LDAP サーバを指定します。
- 10 [次へ] > [完了] の順にクリックします。  
注: スキーマが各 LDAP サービスで整合性を保っていることを確認します。

### スキーマをファイルから更新する


- 1 Novell iManager で、[役割およびタスク] ボタン  をクリックします。
- 2 [eDirectory の保守] > [インポート / エクスポート変換ウィザード] の順にクリックします。
- 3 [ファイルからスキーマを追加] > [次へ] の順にクリックします。
- 4 追加するファイルのタイプを選択します。  
LDIF およびスキーマファイルからタイプを選択できます。
- 5 追加するデータが含まれているスキーマの名前を指定し、適切なオプションを指定してから [次へ] をクリックします。  
追加先のサーバにスキーマを追加せずに、スキーマの比較だけをする場合は、[スキーマを追加しないで比較] を選択します。追加のスキーマは追加先サーバに追加されず、処理の最後に表示されるリンクからスキーマの相違点を確認できます。  
このページのオプションは、選択したファイルのタイプによって異なります。使用可能なオプションの詳細については、[ヘルプ] をクリックしてください。
- 6 スキーマのインポート先になる LDAP サーバを指定します。

7 次の表の説明を参照して、適切なオプションを追加します。

| オプション               | 説明   |
|---------------------|--|
| サーバの DNS 名 /IP アドレス | 相手 LDAP サーバの DNS 名または IP アドレス                            |
| ポート                 | 相手 LDAP サーバのポート番号 ( 整数 )                                 |
| DER ファイル            | SSL 認証に使用するサーバキーが格納されている DER ファイルの名前                     |
| ログイン方法              | [認証ログイン] または [匿名ログイン] ( [ユーザ DN] フィールドに指定したエントリのログイン方法 ) |
| ユーザ DN              | サーバで指定されたバインド操作に使用されるエントリの識別名                            |
| パスワード               | [ユーザ DN] フィールドで指定したエントリのパスワード属性                          |

8 [次へ] > [完了] の順にをクリックします。

### スキーマをサーバから追加する

- 1 Novell iManager で、[役割およびタスク] ボタン  をクリックします。
- 2 [eDirectory の保守] > [インポート / エクスポート 変換ウィザード] の順にクリックします。
- 3 [サーバからスキーマを追加] > [次へ] の順にクリックします。
- 4 スキーマの追加元になる LDAP サーバを指定します。
- 5 次の表の説明を参照して、適切なオプションを追加します。

| オプション               | 説明   |
|---------------------|--|
| サーバの DNS 名 /IP アドレス | 相手 LDAP サーバの DNS 名または IP アドレス                            |
| ポート                 | 相手 LDAP サーバのポート番号 ( 整数 )                                 |
| DER ファイル            | SSL 認証に使用するサーバキーが格納されている DER ファイルの名前                     |
| ログイン方法              | [認証ログイン] または [匿名ログイン] ( [ユーザ DN] フィールドに指定したエントリのログイン方法 ) |
| ユーザ DN              | サーバで指定されたバインド操作に使用されるエントリの識別名                            |
| パスワード               | [ユーザ DN] フィールドで指定したエントリのパスワード属性                          |

追加先のサーバにスキーマを追加せずに、スキーマの比較だけをする場合は、[スキーマを追加しないで比較] を選択します。追加のスキーマは追加先サーバに追加されず、処理の最後に表示されるリンクからスキーマの相違点を確認できます。


6 スキーマの追加先になる LDAP サーバを指定します。

7 次の表の説明を参照して、適切なオプションを追加します。

| オプション               | 説明   |
|---------------------|--|
| サーバの DNS 名 /IP アドレス | 相手 LDAP サーバの DNS 名または IP アドレス                                  |
| ポート                 | 相手 LDAP サーバのポート番号 ( 整数 )                                       |
| DER ファイル            | SSL 認証に使用するサーバキーが格納されている DER ファイルの名前                           |
| ログイン方法              | [ 認証ログイン ] または [ 匿名ログイン ] ( [ ユーザ DN ] フィールドに指定したエントリのログイン方法 ) |
| ユーザ DN              | サーバで指定されたバインド操作に使用されるエントリの識別名                                  |
| パスワード               | [ ユーザ DN ] フィールドで指定したエントリのパスワード属性                              |


8 [ 次へ ] > [ 完了 ] の順にをクリックします。

### スキーマファイルを比較する

- 1 Novell iManager で、[ 役割およびタスク ] ボタン  をクリックします。
- 2 [ eDirectory の保守 ] > [ インポート / エクスポート 変換 ウィザード ] の順にクリックします。
- 3 [ スキーマファイルの比較 ] > [ 次へ ] の順にクリックします。
- 4 比較するファイルのタイプを選択します。  
LDIF およびスキーマファイルから形式を選択できます。
- 5 比較するデータが含まれているスキーマの名前を指定し、適切なオプションを指定してから [ 次へ ] をクリックします。  
このページのオプションは、選択したファイルのタイプによって異なります。使用可能なオプションの詳細については、[ ヘルプ ] をクリックしてください。
- 6 比較するスキーマファイルを指定します。  
LDIF ファイルのみを選択できます。
- 7 [ 次へ ] > [ 完了 ] の順にをクリックします。

2 つのスキーマファイルの相違点は、処理の最後に表示されるリンクから確認できます。

### サーバとファイルからスキーマを比較する

- 1 Novell iManager で、[ 役割およびタスク ] ボタン  をクリックします。
- 2 [ eDirectory の保守 ] > [ インポート / エクスポート 変換 ウィザード ] の順にクリックします。
- 3 [ サーバとファイル間でスキーマファイルを比較 ] > [ 次へ ] の順にクリックします。
- 4 スキーマの比較元になる LDAP サーバを指定します。

5 次の表の説明を参照して、適切なオプションを追加します。

| オプション               | 説明   |
|---------------------|--|
| サーバの DNS 名 /IP アドレス | 相手 LDAP サーバの DNS 名または IP アドレス                                  |
| ポート                 | 相手 LDAP サーバのポート番号 ( 整数 )                                       |
| DER ファイル            | SSL 認証に使用するサーバキーが格納されている DER ファイルの名前                           |
| ログイン方法              | [ 認証ログイン ] または [ 匿名ログイン ] ( [ ユーザ DN ] フィールドに指定したエントリのログイン方法 ) |
| ユーザ DN              | サーバで指定されたバインド操作に使用されるエントリの識別名                                  |
| パスワード               | [ ユーザ DN ] フィールドで指定したエントリのパスワード属性                              |

6 比較するファイルのタイプを選択します。

7 比較するデータが含まれているファイルの名前を指定し、適切なオプションを指定してから [ 次へ ] をクリックします。


このページのオプションは、選択したファイルのタイプによって異なります。使用可能なオプションの詳細については、[ ヘルプ ] をクリックしてください。

8 [ 次へ ] > [ 完了 ] の順にをクリックします。

サーバのスキーマとスキーマファイルの相違点は、処理の最後に表示されるリンクから確認できます。

## 順序ファイルを生成する

このオプションは、区切りデータファイルからデータをインポートするために、delim ハンドラを使用する順序ファイルを生成します。ウィザードでは、特定のオブジェクトクラスの属性リストを含む順序ファイルを作成できます。

1 Novell iManager で、[ 役割およびタスク ] ボタン  をクリックします。

2 [ eDirectory の保守 ] > [ インポート / エクスポート変換ウィザード ] の順にクリックします。

3 [ 順序ファイルの生成 ]、[ 次へ ] の順にクリックします。

4 順序ファイルを生成するクラスを選択して、[ 表示 ] をクリックします。

[ 順次属性 ] リストに追加する属性を選択します。

補助クラスを選択して、[ 選択された補助クラス ] リストに追加します。

[ 順次属性 ] リストおよび [ 補助クラス ] リストの詳細については、iMonitor のオンラインヘルプを参照してください。

[ 次へ ] をクリックします。



- 5 次の表の説明を参照して、適切なオプションを追加します。

| オプション           | 説明   |
|-----------------|--|
| コンテキスト          | 作成されたオブジェクトを関連付けるコンテキスト                    |
| データファイルを選択      | データファイルの場所                                 |
| データファイルでデリミタを選択 | データファイル内で使用される区切り記号。デフォルトの区切り記号はコンマ (,) です |
| ネーミング属性を選択      | 選択したクラスで使用できるすべての属性のリストのネーミング属性            |

[詳細設定] を使用して、LDAP ソースハンドラの追加オプションを設定します。使用可能なオプションの詳細については、[ヘルプ] をクリックしてください。

[処理するレコード] を使用して、データファイルで処理するレコードを選択してください。使用可能なオプションの詳細については、[ヘルプ] をクリックしてください。

- 6 次の表の説明を参照して、適切なオプションを追加します。

| オプション               | 説明   |
|---------------------|--|
| サーバの DNS 名 /IP アドレス | 相手 LDAP サーバの DNS 名または IP アドレス                            |
| ポート                 | 相手 LDAP サーバのポート番号 ( 整数 )                                 |
| DER ファイル            | SSL 認証に使用するサーバキーが格納されている DER ファイルの名前                     |
| ログイン方法              | [認証ログイン] または [匿名ログイン] ( [ユーザ DN] フィールドに指定したエントリのログイン方法 ) |
| ユーザ DN              | サーバで指定されたバインド操作に使用されるエントリの識別名                            |
| パスワード               | [ユーザ DN] フィールドで指定したエントリのパスワード属性                          |

[詳細設定] を使用して、LDAP ソースハンドラの追加オプションを設定します。使用可能なオプションの詳細については、[ヘルプ] をクリックしてください。

- 7 [次へ] > [完了] の順にクリックします。

## コマンドラインインタフェースを使用する

Novell インポート / エクスポート変換ユーティリティのコマンドラインバージョンは、次の操作に使用できます。

- ◆ LDIF のインポート
- ◆ LDIF のエクスポート
- ◆ コンマ区切りデータのインポート
- ◆ コンマ区切りデータのエクスポート
- ◆ LDAP サーバ間でのデータの移行
- ◆ スキーマの比較と更新
- ◆ テンプレートを使用した eDirectory への情報のロード
- ◆ スキーマのインポート

Novell インポート / エクスポート変換ウィザードは、Novell iManager の一部としてインストールされます。Win32\* バージョン (ice.exe) と NetWare<sup>®</sup> バージョン (ice.nlm) の両方がインストールされます。Linux、Solaris、AIX、および HP-UX の各システムの場合、インポート / エクスポートユーティリティは、NOVLice パッケージに含まれています。

### Novell インポート / エクスポート変換構文

Novell インポート / エクスポート変換ユーティリティは、次の構文で起動します。

```
ice 標準オプション  
-S[LDIF | LDAP | DELIM | LOAD | SCH] ソースのオプション  
-D[LDIF | LDAP | DELIM] ターゲットのオプション
```

またはスキーマキャッシュを使用する場合は、次の構文になります。

```
ice -C スキーマオプション  
-S[LDIF | LDAP] ソースのオプション  
-D[LDIF | LDAP] ターゲットのオプション
```

スキーマキャッシュを使用して更新を実行する場合、LDIF ファイルはターゲットとして有効ではありません。

一般オプションの指定は任意です。ただし、指定する場合はソースハンドラオプションやターゲットハンドラオプションより前に指定します。-S (ソース) ハンドラセクションと -D (ターゲット) ハンドラセクションはどちらを先に指定してもかまいません。

利用できるソースハンドラとターゲットハンドラは次のとおりです。

- ◆ 161 ページの「LDIF ソースハンドラのオプション」
- ◆ 162 ページの「LDIF ターゲットハンドラのオプション」
- ◆ 162 ページの「LDAP ソースハンドラのオプション」
- ◆ 165 ページの「LDAP ターゲットハンドラのオプション」
- ◆ 166 ページの「DELIM ソースハンドラのオプション」
- ◆ 167 ページの「DELIM ターゲットハンドラのオプション」
- ◆ 168 ページの「SCH ソースハンドラのオプション」
- ◆ 168 ページの「LOAD ソースハンドラのオプション」

## 一般オプション

一般オプションは、Novell インポート / エクスポート変換エンジンの処理全体に影響のあるオプションです。

| オプション             | 説明  |
|-------------------|---|
| -C                | スキーマキャッシュを使用して比較および更新を実行する場合に指定します。   |
| -l ログファイル         | 出力メッセージ ( エラーメッセージなど ) を書き込むログファイルの名前を指定します。このオプションを指定しなかった場合、エラーメッセージは ice.log に出力されます。<br><br>Linux、Solaris、AIX、および HP-UX の各システムでは、このオプションを指定しなかった場合、エラーメッセージのログは記録されません。                     |
| -o                | 既存のログファイルを上書きする場合に指定します。このフラグを設定しなかった場合、メッセージは既存のログファイルの末尾に追加されます。  |
| -e LDIF エラーログファイル | 正常に処理されなかったエントリを書き込むファイルの名前を指定します。エントリは LDIF 形式で書き込まれます。このファイルは、内容を調べてエラーを修正したうえで元のディレクトリに再適用できます。  |
| -p URL            | インポート / エクスポート変換エンジンが使用する XML 配置ルールが格納されている場所を指定します。配置ルールはエントリの位置を変更するときに使用します。詳細については、 <a href="#">176 ページの「変換ルール」</a> を参照してください。  |
| -c URL            | インポート / エクスポート変換エンジンが使用する XML 作成ルールが格納されている場所を指定します。作成ルールは、インポート時にエントリを正しく作成するために必要な情報が欠落している場合にそれを補うために使用します。詳細については、 <a href="#">176 ページの「変換ルール」</a> を参照してください。                               |
| -s URL            | インポート / エクスポート変換エンジンが使用する XML スキーママッピングルールが格納されている場所を指定します。スキーママッピングルールによって、転送元サーバのスキーマエレメントを、転送先サーバ上の同等ではあるが異なるスキーマエレメントにマッピングできます。<br><br>詳細については、 <a href="#">176 ページの「変換ルール」</a> を参照してください。 |
| -b (NetWare のみ)   | 実行終了時の ICE コンソール画面で、入力を待って停止しない場合に指定します。  |
| -h または -?         | コマンドラインのヘルプを表示します。  |

## スキーマオプション

スキーマオプションでは、スキーマキャッシュを使用してスキーマの比較および更新操作を実行できます。

| オプション       | 説明                                   |
|-------------|--------------------------------------|
| -C -a       | ターゲットスキーマを更新します ( 足りないスキーマを追加します ) 。 |
| -C -c ファイル名 | 指定したファイルにターゲットスキーマを出力します。            |
| -C -n       | スキーマの事前チェックを無効にします。                  |

## ソースハンドラのオプション

ソースハンドラオプション (-S) で、インポートするデータのソースを決定します。コマンドラインには、次のうちの 1 つだけを指定できます。

| オプション   | 説明  |
|---------|---|
| -SLDIF  | LDIF ファイルをソースとして指定します。<br><br>サポートされている LDIF オプションのリストについては、 <a href="#">161 ページの「LDIF ソースハンドラのオプション」</a> を参照してください。        |
| -SLDAP  | LDAP サーバをソースとして指定します。<br><br>サポートされている LDAP オプションのリストについては、 <a href="#">162 ページの「LDAP ソースハンドラのオプション」</a> を参照してください。         |
| -SDELIM | コンマ区切りのデータファイルをソースとして指定します。<br><br>サポートされている DELIM オプションのリストについては、 <a href="#">166 ページの「DELIM ソースハンドラのオプション」</a> を参照してください。 |
| -SSCH   | スキーマファイルをソースとして指定します。<br><br>サポートされている SCH オプションのリストについては、 <a href="#">168 ページの「SCH ソースハンドラのオプション」</a> を参照してください。           |
| -SLOAD  | DirLoad テンプレートをソースとして指定します。<br><br>サポートされている LOAD オプションのリストについては、 <a href="#">168 ページの「LOAD ソースハンドラのオプション」</a> を参照してください。   |

## ターゲットハンドラのオプション

ターゲットハンドラオプション (-D) で、エクスポートするデータの書き込み先を決定します。コマンドラインには、次のうちの 1 つだけを指定できます。

| オプション   | 説明   |
|---------|--|
| -DLDIF  | LDIF ファイルを書き込み先として指定します。<br><br>サポートされているオプションのリストについては、 <a href="#">162 ページの「LDIF ターゲットハンドラのオプション」</a> を参照してください。       |
| -DLLDAP | LDAP サーバを書き込み先として指定します。<br><br>サポートされているオプションのリストについては、 <a href="#">165 ページの「LDAP ターゲットハンドラのオプション」</a> を参照してください。        |
| -DDELIM | コンマ区切りのデータファイルを書き込み先として指定します。<br><br>サポートされているオプションのリストについては、 <a href="#">167 ページの「DELIM ターゲットハンドラのオプション」</a> を参照してください。 |

## LDIF ソースハンドラのオプション

LDIF ソースハンドラは、LDIF ファイルからデータを読み込んで、それを Novell インポート / エクスポート 変換エンジンに送ります。

| オプション        | 説明   |
|--------------|--|
| -f LDIF ファイル | LDIF ソースハンドラで読み込んだ LDIF レコードを格納するファイルの名前を指定します。これらの LDIF レコードはインポート / エクスポート変換エンジンに送信されます。<br><br>Linux、Solaris、AIX、および HP-UX の各システムでは、このオプションを指定しなかった場合、入力データは stdin から読み込まれます。 |
| -a           | このオプションを設定した場合、指定した LDIF ファイル内のレコードが内容レコード (変更タイプが設定されていないレコード) であれば、これらのレコードの変更タイプは「追加」とみなされます。   |
| -c           | エラーが発生しても LDIF ソースハンドラの処理を続行したい場合に指定します。ここでいうエラーとは、LDIF 解析エラーや、ターゲットハンドラからのエラー返信などです。このオプションが設定されている場合にエラーが発生すると、LDIF ソースハンドラは、エラーを報告したうえで、LDIF ファイルの次のレコードを検出し、処理を続行します。        |
| -e           | データのエクスポートまたはインポートに応じて LDAP サーバから送受信される暗号化属性の暗号化または複合化に使用される方式 (DES/3DES) を指定します。  |
| -E           | LDIF ファイル内の暗号化属性を復号化するためのパスワードです。  |
| -n           | 実際の更新は行わず、更新を行った場合の結果を印刷して確認する場合に指定します。このオプションを設定すると、LDIF ソースハンドラは、LDIF ファイルの解析は行いますが、Novell インポート / エクスポート変換エンジンやターゲットハンドラへのレコードの送信は行いません。                                      |
| -m           | このオプションを設定した場合、指定した LDIF ファイル内のレコードが内容レコード (変更タイプが設定されていないレコード) であれば、これらのレコードの変更タイプは「変更」とみなされます。   |
| -x           | このオプションを設定した場合、指定した LDIF ファイル内のレコードが内容レコード (変更タイプが設定されていないレコード) であれば、これらのレコードの変更タイプは「削除」とみなされます。   |
| -R 値         | 処理するレコードの範囲を指定します。   |
| -v           | ハンドラの冗長モードを有効にします。   |

## LDIF ターゲットハンドラのオプション

LDIF ターゲットハンドラは、Novell インポート / エクスポート変換エンジンからデータを受け取り、そのデータを LDIF ファイルに書き込みます。

| オプション        | 説明   |
|--------------|--|
| -f LDIF ファイル | LDIF レコードの書き込み先になるファイルの名前を指定します。<br><br>Linux、Solaris、AIX、および HP-UX の各システムでは、このオプションを指定しなかった場合、出力データは stdout に送られます。 |
| -B           | バイナリ値も印刷します。   |
| -b           | LDIF データの Base64 エンコードを行いません。  |
| -e           | データのエクスポートまたはインポートに応じて LDAP サーバから送受信される暗号化属性の暗号化または複合化に使用される方式 (DES/3DES) を指定します。                                    |
| -E           | LDAP サーバから送られる暗号化属性を暗号化するためのパスワードです。   |

## LDAP ソースハンドラのオプション

LDAP ソースハンドラは、検索要求を該当する LDAP サーバに送信することによってそのサーバからデータを読み込みます。LDAP ソースハンドラは、検索操作の結果として受け取った検索エントリを Novell インポート / エクスポート変換エンジンに送ります。

| オプション    | 説明   |
|----------|--|
| -s サーバ名  | ハンドラが検索要求を送るときの送信先 LDAP サーバの DNS 名または IP アドレスを指定します。デフォルトはローカルホストです。   |
| -p ポート   | サーバ名で指定した LDAP サーバのポート番号を整数で指定します。デフォルトは 389 です。セキュリティ保護された処理の場合、デフォルトポートは 636 です。<br><br>ICE が SSL ポート (デフォルトは 636) で LDAP サーバと証明書なしで通信している場合は、サーバの証明書を信頼できるものとして許可します。このオプションは、サーバおよびクライアント間で暗号化された通信が行われ、サーバの証明書を必要としないような制御された環境でのみ使用してください。 |
| -d DN    | サーバによって指定されたバインド操作に使用するエントリの識別名を指定します。   |
| -w パスワード | DN で指定したエントリのパスワード属性を指定します。  |
| -W       | DN で指定したエントリのパスワードの入力を求めるプロンプトが表示されます。<br><br>このオプションは、Linux、Solaris、AIX、および HP-UX にのみ適用されます。  |

| オプション     | 説明   |
|-----------|--|
| -F フィルタ   | RFC 1558 準拠の検索フィルタを指定します。このオプションを指定しなかった場合、デフォルトの検索フィルタである「objectclass=*」が使用されます。  |
| -n        | 実際の検索は行わず、検索の条件などを表示して確認する場合に指定します。  |
| -a 属性リスト  | <p>検索対象の属性をコンマ区切りのリスト形式で指定します。属性名を指定するか、次の3つのうちいずれかを指定します。</p> <ul style="list-style-type: none"> <li>• 属性を検索しない場合は、「1.1」</li> <li>• すべてのユーザ属性を検索する場合は、「*」</li> <li>• オペレーショナルでない属性をすべて検索する場合は、空のリスト。</li> </ul> <p>このオプションを指定しなかった場合、属性リストは空のリスト(デフォルト)になります。</p>   |
| -o 属性リスト  | <p>LDAP サーバから受け取った検索結果をインポート/エクスポート変換エンジンに送信する前に、その検索結果から削除する属性をコンマ区切りのリスト形式で指定します。このオプションは、-a オプションでワイルドカードを指定してクラスの属性を初めにすべて検索してから、その検索結果をインポート/エクスポート変換エンジンに渡す前に一部の属性を削除したい場合に便利です。</p> <p>たとえば、「-a* -o telephoneNumber」と指定すると、ユーザレベルの属性がすべて検索された後で、その検索結果から telephoneNumber 属性が削除されます。</p>   |
| -R        | 参照結果を自動的に適用しない場合に指定します。デフォルトでは、-d および -w オプションで指定された名前とパスワードによる参照結果が自動的に適用されます。  |
| -e 値      | <p>LDAP クライアント SDK で有効にするデバッグフラグを指定します。</p> <p>詳細については、「<a href="#">LDAP SDK デバッグフラグを使用する</a>」を参照してください。</p>   |
| -b ベース DN | 検索要求のベース識別名を指定します。このオプションを指定しなかった場合、デフォルトのベース DN である ""(空の文字列)が使用されます。   |
| -c 検索スコープ | <p>検索要求のスコープを指定します。有効な値は次のとおりです。</p> <ul style="list-style-type: none"> <li>• One : この値を指定すると、ベースオブジェクトの直接のチャイルドだけが検索の対象になります。</li> <li>• Base : この値を指定すると、ベースオブジェクトのエントリだけが検索の対象になります。</li> <li>• Sub : この値を指定すると、ベースオブジェクトをルートとする LDAP サブツリー(ベースオブジェクトも含まれる)が検索の対象になります。</li> </ul> <p>このオプションを指定しなかった場合は、検索スコープのデフォルトの「Sub」が使用されます。</p> |

| オプション     | 説明  |
|-----------|---|
| -r 別名の逆参照 | <p>検索時に別名を逆参照する方法を指定します。指定できる値は次のとおりです。</p> <ul style="list-style-type: none"> <li>◆ Never : この値を指定すると、サーバは別名の逆参照を行いません。</li> <li>◆ Always : この値を指定すると、検索のベースオブジェクトを検索するときと検索フィルタに一致するエントリを評価するときの両方で、別名の逆参照が行われます。</li> <li>◆ Search : この値を指定すると、ベースオブジェクトを検出した後で検索スコープ内のエントリにフィルタを適用するときには別名の逆参照が行われますが、ベースオブジェクト自体の検索時には別名の逆参照は行われません。</li> <li>◆ Find : この値を指定すると、検索のベースオブジェクトを検索するときには別名の逆参照が行われますが、検索フィルタに一致するエントリを評価するときには別名の逆参照は行われません。</li> </ul> <p>このオプションを指定しなかった場合は、別名逆参照の方式のデフォルトである「Never」が使用されます。</p> |
| -l 制限時間   | 検索の制限時間を秒単位で指定します。  |
| -z サイズ制限  | 検索結果として取得できるエントリの最大数を指定します。   |
| -V バージョン  | 接続に使用する LDAP プロトコルのバージョンを指定します。2 または 3 を指定します。このオプションを省略した場合のデフォルト値は 3 です。  |
| -v        | ハンドラの冗長モードを有効にします。  |
| -L ファイル名  | SSL 認証に使用するサーバキーが格納されている DER 形式のファイルを指定します。   |
| -A        | 属性名だけを取得したいときに指定します。このオプションを指定した場合、出力される検索結果に属性値は含まれません。  |
| -t        | エラーが発生しても LDAP ハンドラの処理を続行したい場合に指定します。   |
| -m        | LDAP 操作は「変更」になります。  |
| -x        | LDAP 操作は「削除」になります。  |
| -k        | SSL を使用して接続します。   |
| -M        | Manage DSA IT コントロールを有効にします。  |
| -MM       | Manage DSA IT コントロールを有効にし、重要度を高く設定します。  |



## LDAP ターゲットハンドラのオプション

LDAP ターゲットハンドラは、Novell インポート / エクスポート 変換エンジンからデータを受け取り、それを LDAP サーバに送信します。データは更新操作の形で送信され、送信先サーバによって実行されます。

LDIF ファイル内のハッシュ化パスワードについては、「[LDIF ファイル内でのハッシュ化パスワードの表記](#)」を参照してください。

| オプション    | 説明   |
|----------|--|
| -s サーバ名  | ハンドラが検索要求を送る時の送信先 LDAP サーバの DNS 名または IP アドレスを指定します。デフォルトはローカルホストです。  |
| -p ポート   | サーバ名で指定した LDAP サーバのポート番号を整数で指定します。デフォルトは 389 です。セキュリティ保護された処理の場合、デフォルトポートは 636 です。   |
| -d DN    | サーバによって指定されたバインド操作に使用するエントリの識別名を指定します。   |
| -w パスワード | DN で指定したエントリのパスワード属性を指定します。  |
| -W       | DN で指定したエントリのパスワードの入力を求めるプロンプトが表示されます。<br><br>このオプションは、Linux、Solaris、AIX、および HP-UX にのみ適用されます。  |
| -B       | サーバへの更新操作の転送に非同期 LBURP (LDAP Bulk Update/Replication Protocol) 要求を使用しない場合は、このオプションを指定します。標準の同期 LDAP 更新操作要求を使用します。<br><br>詳細については、 <a href="#">185 ページの「LBURP (LDAP Bulk Update/Replication Protocol)」</a> を参照してください。 |
| -F       | 前方参照を作成可能にしたい場合は、このオプションを指定します。作成するエントリのペアレントが存在しない場合、エントリが正常に作成できるよう、そのエントリのペアレントに対応するプレースフォルダが作成されます。このプレースフォルダを前方参照といいます。以後の処理でペアレントが作成されると、前方参照は通常のエントリに変更されます。  |
| -l       | パスワード値の格納に NMAS™ (Novell Modular Authentication Service) の簡易パスワード方式を使用する場合は、このオプションを指定します。簡易パスワード方式の場合、パスワードはディレクトリ内の安全な場所で保持されますが、キーのペアはサーバ間での認証で実際に必要になるまで生成されません。これにより、パスワード情報を持つオブジェクトのロードにかかる時間を短縮できます。         |
| -e 値     | LDAP クライアント SDK で有効にするデバッグフラグを指定します。<br><br>詳細については、「 <a href="#">LDAP SDK デバッグフラグを使用する</a> 」を参照してください。  |
| -V バージョン | 接続に使用する LDAP プロトコルのバージョンを指定します。2 または 3 を指定します。このオプションを省略した場合のデフォルト値は 3 です。   |
| -L ファイル名 | SSL 認証に使用するサーバキーが格納されている DER 形式のファイルを指定します。  |

| オプション | 説明  |
|-------|---|
| -k    | SSL を使用して接続します。   |
| -M    | Manage DSA IT コントロールを有効にします。  |
| -MM   | Manage DSA IT コントロールを有効にし、重要度を高く設定します。  |
| -P    | 同時 LBURP 処理を有効にします。このオプションは、LDIF 内のすべての処理を追加する場合にだけ有効にします。-F オプションを使用する場合は、-P はデフォルトで有効になります。 |
| -Z    | 非同期要求の数を指定します。サーバから返される結果を待たずに、ICE クライアントが LDAP サーバに非同期に送信できるエントリの数を示します。                     |

## DELIM ソースハンドラのオプション

DELIM ソースハンドラはコンマ区切りのデータファイルからデータを読み込み、それをターゲットハンドラに送信します。

| オプション           | 説明  |
|-----------------|---|
| -f <i>ファイル名</i> | DELIM ソースハンドラによって読み込まれるコンマ区切りのレコードを含んだファイルの名前を指定します。これらの DELIM レコードはターゲットハンドラに送信されます。   |
| -F <i>値</i>     | -f で指定したファイルに対する属性のデータオーダを含んだファイル名を指定します。このオプションが指定されていない場合、-t を使用してこの情報を直接入力します。<br><br>詳細については、 <a href="#">172 ページの「コンマ区切りのインポートを実行する」</a> を参照してください。                                  |
| -t <i>値</i>     | カンマ区切りの属性リストです。このリストによって、-f で指定されたファイルに対する属性のデータオーダを指定します。このオプションまたは -F オプションのいずれかを指定する必要があります。<br><br>詳細については、 <a href="#">172 ページの「コンマ区切りのインポートを実行する」</a> を参照してください。                    |
| -c              | エラーが発生しても DELIM ソースハンドラの処理を続行したい場合に指定します。ここでいうエラーとは、コンマ区切りデータファイルの解析エラーや、ターゲットハンドラからのエラー返信などです。このオプションが設定されている場合にエラーが発生すると、DELIM ソースハンドラは、エラーを報告したうえで、コンマ区切りデータファイル内の次のレコードを検出し、処理を続行します。 |
| -n <i>値</i>     | 新しいオブジェクトに LDAP ネーミング属性を指定します。この属性は、-F または -t を使用して指定する属性データに含まれている必要があります。   |
| -l <i>値</i>     | RDN の追加先のパスを指定します (o=myCompany など)。DN を渡す場合は、この値は必要ありません。   |
| -o <i>値</i>     | オブジェクトクラスのコンマ区切りのリスト (入力ファイルに含まれていない場合)、または補助クラスなどその他のオブジェクトクラスを指定します。デフォルト値は「inetorgperson」です。   |

| オプション | 説明  |
|-------|---|
| -i 値  | スキップする列のコンマ区切りのリストです。この値には、スキップする列の数を整数で指定します。たとえば3列目と5列目をスキップする場合は、「i3,5」と指定します。   |
| -d 値  | 区切り記号を指定します。デフォルトの区切り記号はコンマ(,)です。<br>次に示すのは、特別な場合の区切り記号です。<br>[q] = 引用符 (二重引用符「"」1つによる区切り)<br>[t] = タブ<br>たとえば、タブを区切り記号として指定するには -d[t] を渡します。             |
| -q 値  | セカンダリ区切り記号を指定します。デフォルトのセカンダリ区切り記号は一重引用符(')です。<br>次に示すのは、特別な場合の区切り記号です。<br>[q] = 引用符 (二重引用符「"」1つによる区切り)<br>[t] = タブ<br>たとえば、タブを区切り記号として指定するには -d[t] を渡します。 |
| -v    | 冗長モードで実行します。  |

### DELIM ターゲットハンドラのオプション

DELIM ターゲットハンドラはソースハンドラからデータを受け取り、そのデータをコンマ区切りのデータファイルに書き込みます。

| オプション    | 説明  |
|----------|---|
| -f ファイル名 | コンマ区切りレコードの書き込み先になるファイルの名前を指定します。   |
| -F 値     | ソースデータの属性のデータオーダを含んだファイルの名前を指定します。このオプションが指定されていない場合、-tを使用してこの情報を直接入力する必要があります。   |
| -t 値     | コンマ区切りの属性リストです。このリストによって、ソースデータの属性のデータオーダを指定します。このオプションまたは-Fオプションのいずれかを指定する必要があります。   |
| -l 値     | RDNまたはDNのいずれかになります。ドライバによってデータ内に配置されるのが、DN全体またはRDNだけのどちらであるかを指定します。デフォルト値はRDNです。  |
| -d 値     | 区切り記号を指定します。デフォルトの区切り記号はコンマ(,)です。<br>次に示すのは、特別な場合の区切り記号です。<br>[q] = 引用符 (二重引用符「"」1つによる区切り)<br>[t] = タブ<br>たとえば、タブを区切り記号として指定するには -d[t] を渡します。 |

| オプション | 説明   |
|-------|--|
| -q 値  | セカンダリ区切り記号を指定します。デフォルトのセカンダリ区切り記号は一重引用符 ( ' ) です。<br><br>次に示すのは、特別な場合の区切り記号です。<br><br>[q] = 引用符 ( 二重引用符 「"」 1 つによる区切り )<br>[t] = タブ<br><br>たとえば、タブを区切り記号として指定するには -d[t] を渡します。 |
| -n 値  | インポート処理中に追加されるネーミング属性を指定します。たとえば cn などです。  |

### SCH ソースハンドラのオプション

SCH ハンドラは、古い NDS や eDirectory のスキーマファイル ( 拡張子 \*.sch がついたファイル ) からデータを読み込んで、それを Novell インポート / エクスポート変換エンジンに送ります。このハンドラを使用すれば、拡張子 \*.sch がついたファイルを入力として、スキーマ関連の操作を LDAP サーバに実装できます。

SCH ハンドラは、ソースハンドラだけのハンドラです。LDAP サーバに \*.sch ファイルをインポートするときには、スキーマハンドラを使用できます。ただし、\*.sch ファイルはエクスポートできません。

SCH ハンドラでサポートされているオプションを次の表に示します。

| オプション    | 説明   |
|----------|--|
| -f ファイル名 | *.sch ファイルの完全なパス名を指定します。                       |
| -c       | ( オプション ) エラーが発生しても SCH ハンドラの処理を続行したい場合に指定します。 |
| -v       | ( オプション ) 冗長モードで実行します。                         |

### LOAD ソースハンドラのオプション

DirLoad ハンドラはテンプレートのコマンドから eDirectory 情報を生成します。このテンプレートファイルは -f 引数で指定されます。また、属性仕様の情報とプログラム制御の情報が保持されています。

| オプション    | 説明   |
|----------|--|
| -f ファイル名 | すべての属性仕様とプログラムの実行を制御するすべての情報を含んだテンプレートファイルを指定します。                                |
| -c       | エラーが通知された場合、次のレコードから続行します。   |
| -v       | 冗長モードで実行します。   |
| -r       | データが追加されずに削除されるように、要求を削除要求に変更します。このオプションにより、DirLoad テンプレートを使用して追加されたレコードを削除できます。 |
| -m       | テンプレートファイル内に変更要求を作成します。  |

**属性仕様** 新しいオブジェクトのコンテキストを決定します。

次の属性仕様ファイルのサンプルを参照してください。

```
givenname: $R(first)
initial: $R(initial)
sn: $R(last)
dn:cn=$A(givenname,%1s)$A(initial,%1s)$A(sn),ou=dev,ou=ds,o=novell
objectclass: inetorgperson
telephonenumber: 1-800-$N(1-999,%03d)-$C(%04d)
title: $R(titles)
locality: Our location
```

属性仕様ファイルの形式は LDIF ファイルに似ていますが、属性仕様ファイルでは強力な構成体を使用して、詳細な情報と属性間の関係を指定することができます。

**固有の数値** 指定されたオブジェクトに対する固有の数値を属性値に挿入します。

構文: `$C[(<形式>)]`

オプションの `<形式>` には、値に適用される出力形式を指定します。形式を指定しない場合、カッコは 2 種類とも必要ありません。

```
$C
$C(%d)
$C(%04d)
```

`$C` だけを指定すると、現在の数値を属性値に挿入します。「`%d`」は、何も指定されなかった場合にプログラムが使用するデフォルト形式であるため、`$C` は `$C(%d)` と同じです。数値は各オブジェクトの後で増加するため、属性仕様で `$C` を複数回使用しても、単一オブジェクト内では数値は変わりません。開始値は、`!COUNTER= 値` の構文を使用して、設定ファイル内で指定できます。

**任意の数値** 次の構文を使用して、属性値に任意の数値を挿入します。

構文: `$N(<下限-><上限>[,<形式>])`

`<下限>` と `<上限>` では、下限値と上限値を指定します。任意の数字が生成される際に各々の値を使用します。オプションの `<形式>` には、値に適用される出力形式を指定します。

```
$N(1-999)
$N(1-999,%d)
$N(1-999,%03d)
```

**リストの任意の文字列** 次の構文を使用して、指定したリストから任意に選択された文字列を属性値に挿入します。

構文: `$R(<ファイル名>[,<形式>])`

`<ファイル名>` には、値を格納しているファイルを指定します。ファイルへのパスは絶対パスまたは相対パスのどちらでも指定できます。リストを格納しているファイルには、このパッケージに含まれているものがあります。値は改行文字で区切る必要があります。

オプションの `<形式>` には、値に適用される出力形式を指定します。

```
$A(givenname)
$A(givenname,%s)
$A(givenname,%1s)
```

前方参照は使用できませんので注意してください。属性値を使用する場合、その属性は全て、属性仕様ファイル内で現在の属性より前にある必要があります。次の例では、**dn**の一部としての**cn**が**givenname**、**initial**、**sn**から構成されています。したがって、**givenname**、**initial**、**sn**の属性は属性仕様ファイル内では**dn**の前にある必要があります。

```
givenname: $R(first)
initial: $R(initial)
sn: $R(last)
dn: o=novell,ou=dev,ou=ds,cn=$A(givenname,%.1s)$A(initial,%.1s)$A(sn)
```

**dn**はLDIFファイル内では次のような特別な処理を受けます。**dn**がどこに設定されているかに関係なく、**dn**は最初に(LDIF構文どおりに)LDIFファイルに書き込まれます。その他のすべての属性は、表示された順に書き込まれます。

**制御設定** オブジェクト作成の際の制御を追加します。すべての制御には、属性設定と区別するために、行頭の文字として感嘆符(!)が付いています。制御はファイル内の任意の場所に置くことができます。

```
!COUNTER=300
!OBJECTCOUNT=2
!CYCLE=title
!UNICYCLE=first,last
!CYCLE=ou,BLOCK=10
```

- ◆ カウンタ

固有のカウンタ値の開始値を提供します。カウンタ値は、**\$C**構文内の任意の属性に挿入されます。

- ◆ オブジェクト数

**OBJECTCOUNT**は、テンプレートから作成されるオブジェクトの数を決定します。

- ◆ サイクル

**CYCLE**は、ファイル(**\$R**構文)から任意の値を抜き出す方法を変更するときに使用できます。この設定には異なる3つの値があります。

```
!CYCLE=title
```

「title」というリスト名が使用される場合は常に、値が任意で選択されるのではなく、リストの順に次の値が抜き出されます。順番に値がすべて使用された場合には、再度リストの最初から開始します。

```
!CYCLE=ou,BLOCK=10
```

リスト「ou」のそれぞれの値が10回ずつ使用され、その後次の値に移動します。

**CYCLE**制御設定のうちで最も興味深い変数は、**UNICYCLE**です。**UNICYCLE**は、一連のソースを左から右の順序で繰り返すように指定します。このため、必要な場合に固有の値が必ず作成されます。**UNICYCLE**制御を使用する場合、**OBJECTCOUNT**制御は、オブジェクト数を、リストから作成できる固有のオブジェクトの最大数に制限するためだけに使用します。つまり、**UNICYCLE**に含まれるリストが15000オブジェクトを作成できる場合、**OBJECTCOUNT**はその数を減らすことはできませんが、増やすことはできません。

たとえば、`givenname` ファイルが 2 つの値 ( 「Doug」 および 「Karl」 ) を格納しており、かつ `sn` ファイルが 3 つの値 ( 「Hoffman」、 「Schultz」、 および 「Grieger」 ) を格納している場合、制御設定 「!UNICYCLE=givenname,sn」 および `cn` の属性定義は次のようになります。`$R (givenname) $R (sn)`。ここでは次の `cns` が作成されます。

```
cn: Doug Hoffmancn
cn: Karl Hoffmancn
cn: Doug Schultzen
cn: Karl Schultzen
cn: Doug Griegercn
cn: Karl Grieger
```

## 例

ここでは、Novell インポート / エクスポート変換ユーティリティのコマンドラインユーティリティで次の操作を行う場合のコマンドの例を紹介します。

- ◆ 171 ページの「LDIF インポートの実行」
- ◆ 171 ページの「LDIF エクスポートを実行する」
- ◆ 172 ページの「コンマ区切りのインポートを実行する」
- ◆ 172 ページの「コンマ区切りのエクスポートを実行する」
- ◆ 172 ページの「LDAP サーバ間でデータを移行する」
- ◆ 173 ページの「スキーマのインポートを実行する」
- ◆ 173 ページの「LOAD ファイルのインポートを実行する」

### LDIF インポートの実行

LDIF のインポートを実行するには、LDIF ソースハンドラと LDAP ターゲットハンドラを組み合わせて次の例のように指定します。

```
ice -S LDIF -f entries.ldif -D LDAP -s server1.acme.com -p 389 -d
cn=admin,c=us -w secret
```

コマンドラインでこのように指定すると、LDIF データが `entries.ldif` から読み込まれ、ポート 389 にある LDAP サーバ `server1.acme.com` に送られます。送信時の識別子は「`cn=admin,c=us`」、パスワードは「`secret`」になります。

### LDIF エクスポートを実行する

LDIF のエクスポートを実行するには、LDAP ソースハンドラと LDIF ターゲットハンドラを組み合わせます。例：

```
ice -S LDAP -s server1.acme.com -p 389 -d cn=admin,c=us -w password -F
objectClass=* -c sub -D LDIF -f server1.ldif
```

コマンドラインでこのように指定すると、識別子「`cn=admin,c=us`」およびパスワード「`password`」を使用してサブツリー検索が実行され、ポート 389 にある LDAP サーバ `server1.acme.com` 内のオブジェクトがすべて検出されます。結果のデータは LDIF 形式で `server1.ldif` に出力されます。

## コンマ区切りのインポートを実行する

コンマ区切りのインポートを実行するには、コマンドを次の例のように指定します。

```
ice -S DELIM -f/tmp/in.csv -F /tmp/order.csv -ncn -lo=acme -D LDAP -s
server1.acme.com -p389 -d cn=admin,c=us -w secret
```

コマンドをこのように指定すると、`/tmp/in.csv` ファイルからコンマ区切りの値が読み込まれ、`/tmp/order.csv` ファイルから属性の順序が読み込まれます。IN.CSV 内の各属性エントリに対して、ORDER.CSV で属性タイプが指定されます。たとえば、IN.CSV に次の値があるとします。

```
pat,pat,engineer,john
```

この場合、`order.csv` に含まれる値は次のようになります。

```
dn,cn,title,sn
```

`order.csv` の情報は、`-t` オプションを使用して直接指定することもできます。

次にデータは、識別子「`cn=admin,c=us`」、およびパスワード「`secret`」を使用して、ポート 389 で LDAP サーバ `server1.acme.com` に送られます。

この例では、`-n` オプションを使用して、`cn` がオブジェクトの新しい DN になるように指定し、`-l` オプションを使用して、このオブジェクトが組織コンテナ `acme` に追加されるようにします。

## コンマ区切りのエクスポートを実行する

コンマ区切りのエクスポートを実行するには、コマンドを次の例のように指定します。

```
ice -S LDAP -s server1.acme.com -p 389 -d cn=admin,c=us -w password -l
objectClass=* -c sub -D DELIM -f /tmp/server1.csv -F order.csv
```

コマンドラインでこのように指定すると、識別子「`cn=admin,c=us`」およびパスワード「`password`」を使用してサブツリー検索が実行され、ポート 389 にある LDAP サーバ `server1.acme.com` 内のオブジェクトがすべて検出されます。結果のデータはコンマ区切りの形式で `/tmp/server1.csv` ファイルに出力されます。

## LDAP サーバ間でデータを移行する

LDAP サーバ間でデータを移行するには、LDAP ソースハンドラと LDAP ターゲットハンドラを組み合わせます。例：

```
ice -S LDAP -s server1.acme.com -p 389 -d cn=admin,c=us -w password -F
objectClass=* -c sub -D LDAP -s server2.acme.com -p 389 -d cn=admin,c=us -w
secret
```

コマンドラインでこのように指定すると、識別子「`cn=admin,c=us`」およびパスワード「`password`」を使用してサブツリー検索が実行され、ポート 389 にある LDAP サーバ `server1.acme.com` 内のオブジェクトがすべて検出されます。結果のデータは、識別子「`cn=admin,c=us`」およびパスワード「`secret`」で、ポート 389 にある LDAP サーバ `server2.acme.com` に送られます。



## スキーマのインポートを実行する

スキーマファイルのインポートを実行するには、コマンドを次の例のように指定します。

```
ice -S SCH -f $HOME/myfile.sch -D LDAP -s myserver -d cn=admin,o=novell -w passwd
```

コマンドラインでこのように指定すると、スキーマデータが `myfile.sch` から読み込まれ、LDAP サーバ「`myserver`」に送られます。送信時の識別子は「`cn=admin,o=novell`」、パスワードは「`passwd`」になります。

## LOAD ファイルのインポートを実行する

LOAD ファイルのインポートを実行するには、コマンドを次の例のように指定します。

```
ice -S LOAD -f attrs -D LDIF -f new.ldf
```

次に、属性ファイル「`attrs`」の内容の例を示します。

```
#####  
# DirLoad 1.00  
#####  
  
!COUNTER=300  
  
!OBJECTCOUNT=2  
#-----  
  
# ATTRIBUTE TEMPLATE  
# -----  
  
objectclass: inetorgperson  
  
givenname: $R(first)  
  
initials: $R(initial)  
  
sn: $R(last)  
  
dn: cn=$A(givenname,%1s)$A(initial,%1s)$A(sn),ou=$R(ou),ou=dev,o=novell,  
telephonenumber: 1-800-$N(1-999,%03d)-$C(%04d)  
  
title: $R(titles)
```

コマンドプロンプトから前のコマンドを実行すると、次の LDIF ファイルが作成されます。

```
version: 1  
  
dn: cn=JohnBBill,ou=ds,ou=dev,o=novell  
  
changetype: add  
  
objectclass: inetorgperson  
  
givenname: John  
  
initials: B  
  
sn: Bill
```

```
telephonenumber: 1-800-290-0300
title: Amigo

dn: cn=BobJAmy,ou=ds,ou=dev,o=novell
changetype: add
objectclass: inetorgperson
givenname: Bob
initials: J
sn: Amy
telephonenumber: 1-800-486-0301
title: Pomo
```

コマンドプロンプトから次のコマンドを実行すると、データが LDAP ハンドラを経由して LDAP サーバに送られます。

```
ice -S LOAD -f attrs -D LDAP -s www.novell.com -d cn=admin,o=novell -w admin
```

次のコマンドラインを使用する際に前のテンプレートファイルを使用すると、前のコマンドで追加したすべてのレコードが削除されます。

```
ice -S LOAD -f attrs -r -D LDAP -s www.novell.com -d cn=admin,o=novell -w admin
```

**-m** を使用して変更する場合は、次の例のようにレコードを変更します。

```
# =====
# DirLoad 1.00
# =====
!COUNTER=300
!OBJECTCOUNT=2
#-----
# ATTRIBUTE TEMPLATE
# -----
dn: cn=$R(first),%.1s) ($R(initial),%.1s)$R(last),ou=$R(ou),ou=dev,o=novell
delete: givenname
add: givenname
givenname: test1
replace: givenname
givenname: test2
givenname: test3
```

「attrs」ファイルが上のデータを格納しているときに次のコマンドラインを使用した場合の例を示します。

```
ice -S LOAD -f attrs -m -D LDIF -f new.ldf
```

LDIF データは次のような結果になります。

```
version: 1
dn: cn=BillTSmith,ou=ds,ou=dev,o=novell
changetype: modify
delete: givenname
-
add: givenname
givenname: test1
-
replace: givenname
givenname: test2
givenname: test3
-
dn: cn=JohnAWilliams,ou=ldap,ou=dev,o=novell
changetype: modify
delete: givenname
-
add: givenname
givenname: test1
-
replace: givenname
givenname: test2
givenname: test3
-
```

## 変換ルール

Novell インポート / エクスポート変換エンジンは、ソースハンドラから受け取ったレコードをターゲットハンドラに送る前に、レコードに対して変換処理を行います。この変換処理の内容は一連のルールを使用して指定できます。これらのルールは XML で記述します (XML ファイルとして作成される場合と、XML 用ディレクトリ内に格納された XML データとして作成される場合があります)。このルールにより、LDAP ディレクトリ間でのエントリのインポート時に、次の問題が解決されます。


- ◆ 不足している情報
- ◆ 階層の違い
- ◆ スキーマの違い

次の 3 種類の変換ルールがあります。

| ルール       | 説明  |
|-----------|---|
| 配置        | <p>エントリの位置を変更します。</p> <p>たとえば、あるユーザグループをいったん「l=San Francisco, c=US」というコンテナにインポートし、インポートが終わった後で「l=Los Angeles, c=US」というコンテナに移したい場合などに、配置ルールを利用できます。</p> <p>これらのルールの形式については、<a href="#">181 ページの「配置ルール」</a>を参照してください。</p>   |
| 作成        | <p>インポート時にエントリを正しく作成するために必要な情報が欠落している場合にそれを補います。</p> <p>たとえば、LDIF データのエクスポート元サーバのスキーマではユーザエントリに必要とされる属性が cn (commonName) 属性だけであるのに対し、LDIF データのインポート先サーバのスキーマでは cn 属性の他に sn (surname) 属性も必要とされる場合が考えられます。このような場合は、作成ルールを使用することにより、インポート / エクスポート変換エンジンが各エントリを処理するときに、そのエントリにデフォルトの sn 値 (" " など) が設定されるようにできます。これにより、各エントリはインポート先サーバに送信されるときには必要な属性である sn 属性を持つことになり、エントリの正常な追加が保証されます。</p> <p>これらのルールの形式については、<a href="#">179 ページの「作成ルール」</a>を参照してください。</p> |
| スキーママッピング | <p>サーバ間でデータを転送する場合 (直接転送するか LDIF を使用するかに関係なく) で、転送元サーバのスキーマと転送先サーバのスキーマが異なっている場合、次のようにスキーママッピングを使用できます。</p> <ul style="list-style-type: none"><li>◆ エクスポート元サーバからインポートするエントリのオブジェクトクラスと属性タイプをすべて受け付けることができるように、インポート先サーバ上のスキーマを拡張します。</li><li>◆ 転送元サーバのスキーマエレメントを、転送先サーバ上の同等ではあるが異なるスキーマエレメントにマッピングします。</li></ul> <p>これらのルールの形式については、<a href="#">178 ページの「スキーママッピングルール」</a>を参照してください。</p>  |

これらの変換ルールは、Novell eDirectory インポート / エクスポートウィザードとコマンドラインインタフェースのどちらでも利用できます。XML ルールの詳細については、[178 ページの「XML ルールを使用する」](#)を参照してください。

## Novell eDirectory インポート / エクスポート変換ウィザードを使用する

- 1 Novell iManager で、[役割およびタスク] ボタン  をクリックします。
- 2 [eDirectory の保守] > [インポート / エクスポート変換ウィザード] の順にクリックします。
- 3 実行するタスクを選択します。
- 4 [詳細設定] の下の次のオプションから選択します。

| オプション   | 説明  |
|---------|---|
| スキーマルール | インポート / エクスポート変換エンジンが使用する XML スキーママッピングルールが格納されている場所を指定します。 |
| 配置ルール   | インポート / エクスポート変換エンジンが使用する XML 配置ルールが格納されている場所を指定します。        |
| 作成ルール   | インポート / エクスポート変換エンジンが使用する XML 作成ルールが格納されている場所を指定します。        |

- 5 [次へ] をクリックします。
- 6 表示される指示に従って、選択したタスクを完了します。

## コマンドラインインターフェースを使用する

コマンドラインバージョンで変換ルールを使用するには、Novell インポート / エクスポート変換ユーティリティの実行ファイルを起動するときに、使用したいルールに対応する一般オプション (-p、-c、または -s) を指定します。詳細については、[159 ページの「一般オプション」](#)を参照してください。

| オプション  | 説明  |
|--------|---|
| -p URL | インポート / エクスポート変換エンジンが使用する XML 配置ルールが格納されている場所です。        |
| -c URL | インポート / エクスポート変換エンジンが使用する XML 作成ルールが格納されている場所です。        |
| -s URL | インポート / エクスポート変換エンジンが使用する XML スキーママッピングルールが格納されている場所です。 |

すべての 3 つのオプションで、URL を次のいずれかに指定します。

- ◆ 次の形式の URL :

file://[パス/] ファイル名

ファイルは、ローカルファイルシステムに存在する必要があります。

- ◆ ベースレベルの検索を指定する RFC 2255 準拠の LDAP URL と、1 つの値の属性タイプに対して 1 つの属性記述が定義されている属性リスト。

## XML ルールを使用する

Novell インポート / エクスポート変換ルールで使用される XML 形式は、Novell Nsure Identity Manager の場合と同じです。Novell Nsure Identity Manager の詳細については、『*DirXML 管理ガイド*』(<http://www.novell.com/documentation/dirxml20/index.html>) を参照してください。

### スキーママッピングルール

スキーママッピングルールの最上位エレメントは、<attr-name-map> です。インポートスキーマとエクスポートスキーマの相互関係は、マッピングルールによって決まります。マッピングルールは、指定されたインポートクラスの定義や属性を、対応するエクスポートスキーマの定義に関連付けます。

マッピングルールは、属性名またはクラス名に対応させて設定します。

- ◆ 属性マッピングの場合、マッピングルールでは、それが属性マッピングであること、ネームスペース (**nds-name** はソース名のタグ)、eDirectory ネームスペース内の名前、および他のネームスペース (**app-name** はターゲット名のタグ) とそのネームスペース内の名前を指定する必要があります。マッピングルールでは、マッピングが特定のクラスに適用されることを指定することも、その属性を持つすべてのクラスに適用されることを指定することもできます。
- ◆ クラスマッピングの場合、マッピングルールでは、それがクラスマッピングルールであること、ネームスペース (**eDirectory** またはアプリケーション) とそのネームスペース内の名前、およびその他のネームスペースとそのネームスペース内の名前を指定する必要があります。

スキーママッピングルールの正式な DTD 定義を次に示します。

```
<!ELEMENT attr-name-map (attr-name | class-name)*>

<!ELEMENT attr-name (nds-name, app-name)>
<!ATTLIST attr-name
          class-name    CDATA    #IMPLIED>

<!ELEMENT class-name (nds-name, app-name)>

<!ELEMENT nds-name (#PCDATA)>
<!ELEMENT app-name (#PCDATA)>
```

複数のマッピングエレメントをファイルに定義できます。各エレメントは、ファイルに定義されている順番で処理されます。1 つのクラスまたは属性を複数回マッピングした場合は、最初のマッピングが優先されます。

スキーママッピングルールの作成例を次に示します。

**スキーマルール 1** : 次のルールでは、inetOrgPerson クラスについて、ソースの surname 属性をターゲットの sn 属性にマッピングします。

```
<attr-name-map>
  <attr-name class-name="inetOrgPerson">
    <nds-name>surname</nds-name>
    <app-name>sn</app-name>
  </attr-name>
</attr-name-map>
```

**スキーマルール 2 :** 次のルールでは、ソースの `inetOrgPerson` クラスの定義をターゲットの `User` クラスの定義にマッピングします。

```
<attr-name-map>
  <class-name>
    <nds-name>inetOrgPerson</nds-name>
    <app-name>User</app-name>
  </class-name>
</attr-name-map>
```

**スキーマルール 3 :** 次の例では、2種類のルールを定義します。1つ目のルールでは、`Surname` 属性を使用するすべてのクラスについて、ソースの `Surname` 属性をターゲットの `sn` 属性にマッピングします。2つ目のルールでは、ソースの `inetOrgPerson` クラスの定義をターゲットの `User` クラスの定義にマッピングします。

```
<attr-name-map>
  <attr-name>
    <nds-name>surname</nds-name>
    <app-name>sn</app-name>
  </attr-name>
  <class-name>
    <nds-name>inetOrgPerson</nds-name>
    <app-name>User</app-name>
  </class-name>
</attr-name-map>
```

**コマンド例 :** スキーマルールが `sr1.xml` ファイルに保存されている場合、次のコマンドを指定することにより、`lentry.ldf` ファイルの処理中にそのルールを使用すること、および結果をターゲットファイル `outt1.ldf` に送ることがインポート / エクスポート変換ユーティリティに指示されます。

```
ice -o -sfile://sr1.xml -SLDIF -flentry.ldf -c -DLDIF
-foutt1.ldf
```

## 作成ルール

作成ルールによって、宛先ディレクトリ内に新規エントリを作成する場合の条件が指定されます。次のエレメントがサポートされます。

- ◆ **必須属性** すべての必須属性について、追加レコードに値が必要であること、値がない場合には追加が失敗することを指定します。作成ルールでは、必須属性のデフォルト値を指定できます。レコードに属性値がない場合、そのエントリにはデフォルト値が使用されます。レコードに属性値がある場合は、そのレコード値が使用されます。
- ◆ **一致属性** 追加レコードに特定の属性が必要であり、特定の値に一致すること、そうでない場合には追加が失敗することを指定します。
- ◆ **テンプレート** `eDirectory` 内のテンプレートオブジェクトの識別名を指定します。現時点では、Novell インポート / エクスポート変換ユーティリティの作成ルールにテンプレートを指定することはできません。

作成ルールの正式な DTD 定義を次に示します。

```
<!ELEMENT create-rules (create-rule)*>

<!ELEMENT create-rule (match-attr*,
                        required-attr*,
                        template?)>

<!ATTLIST create-rule
            class-name    CDATA    #IMPLIED
            description   CDATA    #IMPLIED>

<!ELEMENT match-attr    (value)+ >
<!ATTLIST match-attr
            attr-name     CDATA    #REQUIRED>

<!ELEMENT required-attr (value)*>
<!ATTLIST required-attr
            attr-name     CDATA    #REQUIRED>

<!ELEMENT template EMPTY>
<!ATTLIST template
            template-dn   CDATA    #REQUIRED>
```

複数の作成ルールをファイルに定義できます。各ルールは、ファイルに定義されている順番で処理されます。ルールに適合しないレコードがあると、そのレコードはスキップされますが、レコードのスキップによるエラーは生成されません。

作成ルールの形式例を次に示します。

**作成ルール 1 :** 次に紹介するルールでは、`inetOrgPerson` クラスの追加レコードに次の 3 つの条件が適用されます。追加レコードには、`givenName` 属性および `Surname` 属性が必要です。追加レコードには `L` 属性が必要ですが、この属性値がない場合には、作成ルールによってデフォルト値「`Provo`」に設定されます。

```
<create-rules>
  <create-rule class-name="inetOrgPerson">
    <required-attr attr-name="givenName"/>
    <required-attr attr-name="surname"/>
    <required-attr attr-name="L">
      <value>Provo</value>
    </required-attr>
  </create-rule>
</create-rules>
```

**作成ルール 2 :** 次に紹介する作成ルールでは、ベースクラスの種類に関係なく、すべての追加レコードに次の 3 つの条件が適用されます。

- ◆ 追加レコードには、`givenName` 属性が必要です。この属性値がない場合、追加は失敗します。
- ◆ 追加レコードには、`Surname` 属性が必要です。この属性値がない場合、追加は失敗します。
- ◆ 追加レコードには、`L` 属性が必要です。この属性がない場合、`L` 属性はデフォルト値「`Provo`」に設定されます。



```

<create-rules>
  <create-rule>
    <required-attr attr-name="givenName"/>
    <required-attr attr-name="Surname"/>
    <required-attr attr-name="L">
      <value>Provo</value>
    </required-attr>
  </create-rule>
</create-rules>

```

**作成ルール 3 :** 次に紹介する作成ルールでは、ベースクラスの種類に関係なく、すべての追加レコードに次の 2 つの条件が適用されます。

- ◆ 作成ルールは、レコードに uid 属性として ratuid が指定されているかチェックします。この属性値がない場合、追加は失敗します。
- ◆ 作成ルールは、レコードに L 属性が指定されているかチェックします。この属性がない場合、L 属性はデフォルト値「Provo」に設定されます。

```

<create-rules>
  <create-rule>
    <match-attr attr-name="uid">
      <value>cn=ratuid</value>
    </match-attr>
    <required-attr attr-name="L">
      <value>Provo</value>
    </required-attr>
  </create-rule>
</create-rules>

```

**コマンド例 :** 作成ルールを `cr1.xml` ファイルに保存し、次のコマンドを指定することにより、`lentry.ldf` ファイルの処理中にそのルールを使用すること、および結果をターゲットファイル `outt1.ldf` に送ることがインポート / エクスポート変換ユーティリティに指示されます。

```

ice -o -cfile://cr1.xml -SLDIF -flentry.ldf -c -DLDIF
-foutt1.ldf

```

## 配置ルール

配置ルールによって、ターゲットディレクトリ内でエントリが作成される位置が決まります。配置ルールでは、次の 3 つの条件を使用して、エントリの配置にそのルールを適用すべきかどうかを決定します。

- ◆ **クラス一致 :** 配置ルールに `match class` エlement が定義されている場合、レコードに定義されている `objectClass` は、ルールの `class-name` 属性に一致する必要があります。一致しない場合、そのレコードには配置ルールが使用されません。
- ◆ **属性一致 :** 配置ルールに `match attribute` エlement が定義されている場合、レコードでは、`match attribute` エlement に定義されている各属性について属性値が必要です。一致しない場合、そのレコードには配置ルールが使用されません。
- ◆ **パス一致 :** 配置ルールに `match path` エlement が定義されている場合、レコードの `dn` 部分は、`match path` エlement に定義されているプリフィックスに一致する必要があります。一致しない場合、そのレコードには配置ルールが使用されません。

ルールの最後の Element によって、エントリの配置場所が決まります。配置ルールでは、必要に応じて次のオプションを指定できます。

- ◆ **解析済み文字データ** 解析済み文字データを使用して、エントリに使用するコンテナの DN を指定します。

- ◆ **名前をコピー** 古い DN のネーミング属性を、エントリの新しい DN で使用することを指定します。
- ◆ **属性をコピー** エントリの新しい DN で使用するネーミング属性を指定します。指定されたネーミング属性は、エントリのベースクラスのネーミング属性として有効でなければなりません。
- ◆ **パスをコピー** ソース DN をターゲット DN として使用することを指定します。
- ◆ **パスサフィックスをコピー** ソース DN のパスの一部をターゲット DN として使用することを指定します。**match-path** エレメントを指定した場合、古い DN のパスの一部、つまり、**match-path** エレメントのプリフィックス属性に一致しない部分だけが、エントリの DN の一部として使用されます。

配置ルールの正式な DTD 定義を次に示します。

```
<!ELEMENT placement-rules (placement-rule*)>
<!ATTLIST placement-rules
    src-dn-format      (%dn-format;)      "slash"
    dest-dn-format     (%dn-format;)      "slash"
    src-dn-delims      CDATA              #IMPLIED
    dest-dn-delims     CDATA              #IMPLIED>

<!ELEMENT placement-rule (match-class*,
    match-path*,
    match-attr*,
    placement)>
<!ATTLIST placement-rule
    description        CDATA              #IMPLIED>

<!ELEMENT match-class  EMPTY>
<!ATTLIST match-class
    class-name         CDATA              #REQUIRED>

<!ELEMENT match-path   EMPTY>
<!ATTLIST match-path
    prefix              CDATA              #REQUIRED>

<!ELEMENT match-attr   (value)+ >
<!ATTLIST match-attr
    attr-name           CDATA              #REQUIRED>

<!ELEMENT placement    (#PCDATA |
    copy-name |
    copy-attr |
    copy-path |
    copy-path-suffix)* >
```

複数の配置ルールエレメントをファイルに定義できます。各ルールは、ファイルに定義されている順番で処理されます。ルールに適合しないレコードがあると、そのレコードはスキップされますが、レコードのスキップによるエラーは生成されません。

配置ルールの形式例を次に示します。 **src-dn-format="ldap"** 属性および **dest-dn-format="ldap"** 属性によって、ソース DN およびターゲット DN のネームスペースが LDAP 形式として定義されます。

Novell インポート / エクスポート変換ユーティリティがサポートするソース名およびターゲット名は、LDAP 形式だけです。

**配置例 1 :** 次の配置ルールでは、レコードはベースクラス `inetOrgPerson` を持つ必要があります。レコードがこの条件に適合する場合、そのエントリは `test` コンテナの直下に置かれ、ソース DN の最上位コンポーネントがエントリの DN の一部として使用されます。

```
<placement-rules src-dn-format="ldap" dest-dn-format="ldap">
  <placement-rule>
    <match-class class-name="inetOrgPerson"></match-class>
    <placement>cn=<copy-name/>,o=test</placement>
  </placement-rule>
</placement-rules>
```

ベースクラス `inetOrgPerson` および次の DN を持つレコードがあるとします。

```
dn: cn=Kim Jones, ou=English, ou=Humanities, o=UofZ
```

このレコードは、例に示したルールに従って、ターゲットディレクトリ内で次の DN を持ちます。

```
dn: cn=Kim Jones, o=test
```

**配置例 2 :** 次の配置ルールでは、レコードは `sn` 属性を持つ必要があります。レコードがこの条件に適合する場合、そのエントリは `test` コンテナの直下に置かれ、ソース DN の最上位コンポーネントがエントリの DN の一部として使用されます。

```
<placement-rules src-dn-format="ldap" dest-dn-format="ldap">
  <placement-rule>
    <match-attr attr-name="sn"></match-attr>
    <placement>cn=<copy-name/>,o=test</placement>
  </placement-rule>
</placement-rules>
```

次の DN および `sn` 属性を持つレコードがあるとします。

```
dn: cn=Kim Jones, ou=English, ou=Humanities, o=UofZ
sn: Jones
```

このレコードは、例に示したルールに従って、ターゲットディレクトリ内で次の DN を持ちます。

```
dn: cn=Kim Jones, o=test
```

**配置例 3 :** 次の配置ルールでは、レコードは `sn` 属性を持つ必要があります。レコードがこの条件に適合する場合、そのエントリは `test` コンテナの直下に置かれ、`sn` 属性がエントリの DN の一部として使用されます。`copy-attr` エlement に指定された属性は、エントリのベースクラスのネーミング属性でなければなりません。

```
<placement-rules src-dn-format="ldap" dest-dn-format="ldap">
  <placement-rule>
    <match-attr attr-name="sn"></match-attr>
    <placement>cn=<copy-attr attr-name="sn"/>,o=test</placement>
  </placement-rule>
</placement-rules>
```

次の DN および `sn` 属性を持つレコードがあるとします。

```
dn: cn=Kim Jones, ou=English, ou=Humanities, o=UofZ
sn: Jones
```

このレコードは、例に示したルールに従って、ターゲットディレクトリ内で次の DN を持ちます。

```
dn: cn=Jones, o=test
```

**配置例 4 :** 次の配置ルールでは、レコードは **sn** 属性を持つ必要があります。レコードがこの条件に適合する場合、ソース DN がターゲット DN として使用されます。

```
<placement-rules src-dn-format="ldap" dest-dn-format="ldap">
  <placement-rule>
    <match-attr attr-name="sn"></match-attr>
    <placement><copy-path/></placement>
  </placement-rule>
</placement-rules>
```

**配置例 5 :** 次の配置ルールでは、レコードは **sn** 属性を持つ必要があります。レコードがこの条件に適合する場合、エントリの DN 全体が **test** コンテナにコピーされます。

```
<placement-rules src-dn-format="ldap" dest-dn-format="ldap">
  <placement-rule>
    <match-attr attr-name="sn"></match-attr>
    <placement><copy-path-suffix/>,o=test</placement>
  </placement-rule>
</placement-rules>
```

次の DN および **sn** 属性を持つレコードがあるとします。

```
dn: cn=Kim Jones, ou=English, ou=Humanities, o=UofZ
sn: Jones
```

このレコードは、例に示したルールに従って、ターゲットディレクトリ内で次の DN を持ちます。

```
dn: cn=Kim Jones, ou=English, ou=Humanities, o=UofZ, o=test
```

**配置例 6 :** 次の配置ルールでは、レコードは **sn** 属性を持つ必要があります。レコードがこの条件に適合する場合、エントリの DN 全体が **neworg** コンテナにコピーされます。

```
<placement-rules>
  <placement-rule>
    <match-path prefix="o=engineering"/>
    <placement><copy-path-suffix/>o=neworg</placement>
  </placement-rule>
</placement-rules>
```

例 :

```
dn: cn=bob,o=engineering
```

これは次のようになります。

```
dn: cn=bob,o=neworg
```

**コマンド例 :** 配置ルールが **pr1.xml** ファイルに保存されている場合、次のコマンドを指定することにより、**lentry.ldf** ファイルの処理中にそのルールを使用すること、および結果をターゲットファイル **foutt1.ldf** に送ることがインポート/エクスポート変換ユーティリティに指示されます。

```
ice -o -pfile://pr1.xml -SLDIF -flentry.ldf -c -DLDIF
-foutt1.ldf
```

## LBURP (LDAP Bulk Update/Replication Protocol)

Novell インポート / エクスポート変換ユーティリティでは、LDAP サーバへの非同期要求の送信に、LBURP を使用します。これにより、要求は常にプロトコルで指定された順序で処理されます。複数プロセッサ間の相互関係やオペレーティングシステムのスケジューラの設定によって処理順序が変わることはありません。

LBURP により、Novell インポート / エクスポート変換ユーティリティは、複数の更新操作を 1 つの要求として送信したり、これらすべての更新操作に対する応答を 1 つのレスポンスとして受け取ることができます。これにより、プロトコルのネットワーク処理効率が向上します。

LBURP は次のように機能します。

1. Novell インポート / エクスポート変換ユーティリティが LDAP サーバにバインドします。
2. サーバからクライアントにバインドレスポンスが送られます。
3. クライアントからサーバに開始 LBURP 拡張要求が送られます。
4. サーバからクライアントに開始 LBURP 拡張レスポンスが送られます。
5. 必要に応じてクライアントからサーバに LBURP 操作拡張要求が送られます。

これらの要求は非同期で送信することもできます。要求ごとに通し番号が付けられ、同じクライアントから同じ接続を介して送信された個々の要求の順序はこの通し番号によって特定されます。各要求には、少なくとも 1 つの LDAP 更新操作が設定されます。


6. サーバは、受け取った各 LBURP 操作拡張要求を通し番号に従って順番に処理し、要求ごとに LBURP 操作拡張レスポンスを送信します。
7. サーバへの更新操作の送信がすべて終了すると、クライアントはサーバに終了 LBURP 拡張要求を送ります。
8. サーバからクライアントに終了 LBURP 拡張レスポンスが送られます。

LBURP プロトコルにより、Novell インポート / エクスポート変換機能は、サーバにデータを転送するときに送信元と送信先とのネットワーク接続の限界まで転送速度を上げることができます。ネットワーク接続が十分に高速であれば、Novell インポート / エクスポート変換機能から要求が送られてくるのを待つ必要がないため、サーバはすべての処理時間を更新操作の処理だけに費やすことができます。

更新操作の処理効率をさらに上げるため、eDirectory の LBURP プロセッサは、データベースへの更新操作をグループに分けて行います。LBURP の採用により、従来の同期処理の場合と比べて、LDIF のインポート処理の効率は大幅に改善されています。

LBURP はデフォルトで有効になっていますが、LDIF のインポート中に無効にすることもできます。

LDIF のインポート中に LBURP の有効 / 無効を切り替えるには、次を実行します。

- 1 Novell iManager で、[役割およびタスク] ボタン  をクリックします。
- 2 [eDirectory の保守] > [インポート / エクスポート変換ウィザード] の順にクリックします。
- 3 [ディスク上のファイルからデータをインポート] > [次へ] の順にクリックします。
- 4 [ファイルタイプ] ドロップダウンリストから LDIF を選択し、インポートするデータが格納されている LDIF ファイルの名前を指定します。

- 5 [次へ] をクリックします。
- 6 データをインポートするLDAPサーバとログインのタイプ(匿名ログインまたは認証ログイン)を指定します。
- 7 [詳細設定] の下の [LBURP を使用] を選択します。
- 8 [次へ] をクリックし、表示される指示に従って LDIF インポートウィザードでの残りの作業を完了します。

**重要:** LBURP は比較的新しいプロトコルであるため、バージョン 8.5 よりも前の eDirectory サーバおよび eDirectory 以外のサーバの大部分は、LBURP をサポートしていません。Novell eDirectory インポート / エクスポートウィザードを使用して LBURP をサポートしていないサーバに LDIF ファイルをインポートする場合は、LDIF のインポートが正しく行われるよう、LBURP オプションを無効にします。

コマンドラインオプションを使用して、LDIF のインポート中に LBURP の有効 / 無効を切り替えることができます。詳細については、[165 ページの「-B」](#) を参照してください。

## LDAP ディレクトリ間でスキーマを移行する

LDAP ディレクトリ間でのスキーマの移行に関する詳細については、Novell Developer Portal の *NetWare Application Notes* (<http://www.developer.novell.com/research>) を参照してください。

## LDIF のインポートを高速化する

1つの LDIF ファイルに数千または数百万のレコードがある場合は、次のことを検討してください。

- ◆ [186 ページの「読み書き可能レプリカを持つサーバに直接インポートする」](#)
- ◆ [187 ページの「LBURP を使用する」](#)
- ◆ [187 ページの「データベースキャッシュを設定する」](#)
- ◆ [187 ページの「簡易パスワードを使用する」](#)
- ◆ [188 ページの「インデックスを使用する場合の注意」](#)

### 読み書き可能レプリカを持つサーバに直接インポートする

実行が可能な場合は、LDIF ファイルで示されているすべてのエントリを含む、読み書き可能レプリカを持つサーバを LDIF のインポート先に選択します。これによりネットワーク効率を大幅に高めることができます。

更新時には、インポート先サーバから他の eDirectory サーバへのチェーン接続は行わないでください。これにより、パフォーマンスはかなり低下します。ただし、一部の更新対象エントリが LDAP を実行していないサーバ上だけに存在する場合には、LDIF ファイルをインポートするためにチェーン接続が必要になることもあります。

レプリカとパーティション管理の詳細については、[135 ページの第 5 章「パーティションおよびレプリカの管理」](#) を参照してください。

## LBURP を使用する

Novell インポート / エクスポート変換機能では、ネットワークと eDirectory サーバの処理をできるだけ効率化するために、ウィザードとサーバの間でのデータ転送に LBURP を使用します。LDIF のインポート時に LBURP を使用することにより、LDIF のインポートにかかる時間が大幅に短縮されます。

LBURP の詳細については、[185 ページの「LBURP \(LDAP Bulk Update/Replication Protocol\)」](#)を参照してください。

## データベースキャッシュを設定する


eDirectory で使用できるデータベースキャッシュの容量は、LDIF インポートの処理速度に大きく影響します。特に、サーバ上のエントリの総数が多いほど影響は大きくなります。LDIF のインポートでは、インポート実行中にはできるだけ多くのメモリを eDirectory に割り当てると効率的です。インポートが完了してサーバの負荷が通常レベルに戻ったら、メモリの設定を元にもどすことができます。この方法は、eDirectory サーバで実行する処理がインポートだけの場合に特に効果があります。

eDirectory データベースキャッシュの設定の詳細については、[513 ページの第 16 章「Novell eDirectory のメンテナンス」](#)を参照してください。

## 簡易パスワードを使用する

Novell eDirectory では、パブリックキーとプライベートキーのペアを使用して認証を行います。これらのキーの生成は、CPU に大きな負荷のかかる処理です。eDirectory 8.7.3 以降では、パスワードの格納に、NMASTM (Novell Modular Authentication Service) の簡易パスワード機能を使用できます。簡易パスワードを使用する場合、パスワードはディレクトリ内の安全な場所で保持されますが、キーのペアはサーバ間での認証で実際に必要になるまで生成されません。これにより、パスワード情報を持つオブジェクトをロードする速度を大幅にアップできます。

LDIF のインポート時に簡易パスワードを有効にするには、次を実行します。

- 1 Novell iManager で、[役割およびタスク] ボタン  をクリックします。
- 2 [eDirectory の保守] > [インポート / エクスポート変換ウィザード] の順にクリックします。
- 3 [ディスク上のファイルからデータをインポート] > [次へ] の順にクリックします。
- 4 [ファイルタイプ] ドロップダウンリストから LDIF を選択し、インポートするデータが格納されている LDIF ファイルの名前を入力します。
- 5 [次へ] をクリックします。
- 6 データをインポートするLDAPサーバとログインのタイプ(匿名ログインまたは認証ログイン)を指定します。
- 7 [詳細設定] の下の [NMASTM 通常パスワード / ハッシュ化パスワードを格納する] を選択します。
- 8 [次へ] をクリックし、表示される指示に従って、LDIF インポートウィザードでの残りの作業を完了します。

パスワードの格納に簡易パスワードを使用する場合は、eDirectory ツリーへのログインおよび従来型のファイルサービスや印刷サービスへのアクセスには、NMAS 対応の Novell Client™ を使用する必要があります。またサーバには NMAS がインストールされている必要があります。名前とパスワードのバインドを行う LDAP アプリケーションは、簡易パスワード機能とスムーズに連携します。

NMAS の詳細については、『[Novell Modular Authentication Service 管理ガイド](http://www.novell.com/documentation/beta/nmas30/index.html)』 (<http://www.novell.com/documentation/beta/nmas30/index.html>) を参照してください。

## インデックスを使用する場合の注意

不要なインデックスがあると、LDIF のインポートにかかる時間が長くなります。これは、定義されているすべてのインデックスで、設定されている属性値を持つエントリごとに追加の処理が実行されるためです。LDIF をインポートする前に、不要なインデックスがないことを確認します。インデックスを作成するときは、あらかじめデータ確認済みのプレディケート統計をロードしてインデックスが本当に必要な箇所を確認すると、不要なインデックスを減らすことができます。

インデックスの調整の詳細については、[188 ページの「インデックスマネージャ」](#)を参照してください。

## インデックスマネージャ

インデックスマネージャは、サーバオブジェクトの属性の 1 つで、データベースインデックスの管理に使用します。eDirectory では、データベースインデックスを使用することによって、クエリの処理速度が大幅に向上します。

Novell eDirectory には、基本的なクエリの機能を提供する一連のインデックスが付属しています。これらデフォルトのインデックスの対象となる属性を次に示します。

|                   |               |
|-------------------|---------------|
| CN                | 別名オブジェクト名     |
| dc                | 破損通知          |
| 名                 | Member        |
| 姓                 | リファレンス        |
| uniqueID          | 同等権利保有者       |
| GUID              | NLS : 共通許可証   |
| cn_SS             | リビジョン         |
| uniqueID_SS       | extensionInfo |
| ldapAttributeList | ldapClassList |

またカスタマイズされたインデックスを作成して、ユーザの環境における eDirectory のパフォーマンスをさらに向上させることができます。たとえば、デフォルトでインデックス付けされていない属性を検索する新しい LDAP アプリケーションが組織に導入された場合、その属性に対するインデックスを作成すると便利です。


**注:** インデックスを使用することにより検索の処理速度は上がりますが、インデックスの数が増えるほど更新にかかる時間が長くなります。一般には、パフォーマンスの問題が特定のディレクトリの検索に関係すると思われる場合に、新しいインデックスを作成します。



Novell iManager を使用して、インデックスを作成または削除します。インデックス名、状態、タイプ、ルール、インデックス付き属性など、インデックスのプロパティを表示したり、管理することができます。

プレディケート統計データを使用すると、どのようなインデックスを追加したらユーザの環境で便利であるかを確認できます。プレディケート統計データは **ConsoleOne** のみ使用できます。193 ページの「**プレディケートデータ**」を参照してください。

## インデックスを作成する

1 Novell iManager で、[役割およびタスク] ボタン  をクリックします。

2 [eDirectory の保守] > [インデックス管理] の順にクリックします。

3 利用可能なサーバのリストからサーバを選択します。

4 [インデックスの変更] ページで [作成] をクリックします。

5 インデックス名を入力します。

インデックス名を入力しなかった場合は、選択した属性が自動的にインデックス名として設定されます。

**重要:** 「\$」文字は属性値の区切り記号として使用されます。インデックス名に「\$」文字を使用する場合、前に円記号 () を付けて、LDAP でインデックスを作成するときに「\$」文字をエスケープします。

6 属性を選択します。

7 インデックスのルールを選択します。

- ◆ **値** 属性の値全体または値の最初の部分を照合します。たとえば、値一致は、「Jensen」に一致する「LastName」のあるエントリの検索や、「Jen」で始まる「LastName」があるエントリの検索に使用できます。
- ◆ **存在** 特定の属性値ではなく、属性の存在のみを検索します。Login Script 属性を持つエントリをすべて検索するクエリは、存在インデックスを使用します。
- ◆ **下位文字列** 属性値文字列のサブセットを照合します。たとえば、「der」という値を含む「LastName」を検索するクエリを実行すると、「Derington」、「Anderson」、および「Lauder」が照合の結果として返されます。


下位文字列インデックスは、作成や維持を行うときに最も多くのリソースが消費されるインデックスです。

8 [OK] をクリックすると、インデックステーブルが更新されます。

9 [適用] をクリックすると、limber がバックグラウンドプロセスとして再起動され、変更内容が有効になります。

## インデックスを削除する

作成したインデックスが不要になる場合があります。必要のない、ユーザ定義または自動で作成したインデックスは、削除できます。プレディケート統計を使用して、重要度の低いインデックスを調べることができます。詳細については、193 ページの「**プレディケートデータ**」を参照してください。

1 Novell iManager で、[役割およびタスク] ボタン  をクリックします。


2 [eDirectory の保守] > [インデックス管理] の順にクリックします。

3 利用可能なサーバのリストからサーバを選択します。

- 4 [インデックスの変更] ページで、削除するユーザインデックスまたは自動追加インデックスを選択します。
- 5 [削除] をクリックすると、インデックステーブルが更新されます。
- 6 [適用] をクリックすると、limber がバックグラウンドプロセスとして再起動され、変更内容が有効になります。

## インデックスをオフラインにする

一時的にインデックスをオフラインにすることで、処理のピーク時にパフォーマンスを調整できます。たとえば、ユーザ定義のインデックスの使用をすべて中断すると、バルクロードを高速化できます。オブジェクトを追加または変更するときは定義されているインデックスを更新する必要があり、すべてのインデックスをアクティブにするとデータのバルクロードの速度が遅くなるためです。バルクロードが完了すると、再びインデックスをオンラインにできます。

- 1 Novell iManager で、[役割およびタスク] ボタン  をクリックします。
- 2 [eDirectory の保守] > [インデックス管理] の順にクリックします。
- 3 利用可能なサーバのリストからサーバを選択します。
- 4 [インデックスの変更] ページで、オフラインにするインデックスを選択して、[変更状況] をクリックします。

表示されているテーブルでは、インデックスの状態が [オンライン] から [オフライン] に変わります。インデックスは、次のいずれかの状態になります。


- ◆ **オンライン**：現在実行中です。
- ◆ **オフライン**：一時停止中です。[オンライン] をクリックすると再開します。
- ◆ **新規**：オンラインに移動するために待機中です。
- ◆ **削除済み**：インデックステーブルから削除するために待機中です。

- 5 [適用] をクリックします。

## 他のサーバ上でインデックスを管理する

あるサーバで便利に使用されているインデックスがあり、このインデックスを他のサーバでも使用する場合は、他のサーバにインデックス定義をコピーできます。またプレディケートデータを調べると、これとは逆のケースが発生する場合があります。つまり、複数のサーバで使用されていたインデックスが、そのいずれかのサーバで不要になるといったケースです。このような場合、インデックスが不要になったサーバからインデックスを削除できます。

インデックスマネージャを使用すると、他のインスタンスに影響を与えずに、インデックスの 1 つのインスタンスを処理できます。

- 1 Novell iManager で、[役割およびタスク] ボタン  をクリックします。
- 2 [eDirectory の保守] > [インデックス管理] の順にクリックします。
- 3 利用可能なサーバのリストからサーバを選択します。
- 4 同じツリーの別のサーバにインデックス定義をコピーするには、[インデックス位置の変更] をクリックします。

5 コピーするインデックス定義を選択します。

インデックスを1つ選択すると、そのインデックスを提供するツリー内のサーバが一覧表示されます。

6 このカラムを使用して、インデックスのコピーを目的のサーバに移動します。

7 [適用] をクリックします。

## Novell インポート / エクスポート変換ユーティリティを使用してインデックスを管理する

Novell インポート / エクスポート変換ユーティリティを使用してインデックスを作成または削除できます。

インデックスを作成または削除するには、LDIF ファイルを使用する必要があります。LDIF ファイルがインポートされたら、limber を開始してインデックス処理を初期化することができます。その他の場合には、インデックス処理は limber が開始されたときに自動的に行われます。

LDIF ファイルにインデックスを指定するには値が必要です。次の場合、ドル (\$) 記号で区切られた文字列は無視されます。

| 順序 | 文字列           | 説明   |
|----|---------------|--|
| 1  | Index version | 今後の使用のために予約されています。eDirectory では、常に 0 に設定します。   |
| 2  | Index name    | ユーザ定義のインデックス名 ( 姓、郵便番号など ) を指定します。文字列には、ドル (\$) 記号は使用できません。  |
| 3  | Index state   | <p>インデックスの状態を指定します。インデックスを定義する場合、このフィールドには 2 ( オンライン ) を設定します。eDirectory では次の値がサポートされています。</p> <ul style="list-style-type: none"><li>0 - 一時停止。該当するインデックスがクエリに使用されず、更新もされていない状態を示します。</li><li>1 - オンライン開始中。該当するインデックスが作成中であることを示します。</li><li>2 - オンライン。該当するインデックスが使用されていることを示します。</li><li>3 - 作成待機中。該当するインデックスの定義が完了し、バックグラウンド処理で実行されるまで待機中であることを示します。</li></ul> <p>バックグラウンドプロセスは、インデックスの構築を開始した後に状態を変更します。</p> |

| 順序 | 文字列               | 説明   |
|----|-------------------|--|
| 4  | Index rule        | <p>マッチングのタイプを指定します。</p> <ul style="list-style-type: none"> <li>0 - 値一致。値全体または値の最初の部分を含むクエリを最適化します。たとえば、「Jensen」または「Jen」ではじまる文字列と一致する surname 属性を持つエントリのクエリなどがあります。</li> <li>1 - 存在一致。属性の存在のみを含むクエリを最適化します。たとえば、surname 属性を持つすべてのエントリのクエリなどがあります。</li> <li>2 - 下位文字列一致。一致する文字列を含むクエリを最適化します。たとえば、「der」の文字列を含む surname 属性を持つエントリのクエリなどがあります。このクエリでは、「Derington」「Anderson」および「Lauder」といった surname 属性を持つエントリが返されます。</li> </ul> |
| 5  | Index type        | <p>インデックスの作成者を指定します。インデックスを定義する場合、この値を 0 に設定する必要があります。eDirectory では次の値がサポートされています。</p> <ul style="list-style-type: none"> <li>0 - ユーザ定義</li> <li>1 - 属性作成時に追加</li> <li>2 - 操作時に必要</li> <li>3 - システムインデックス</li> </ul>   |
| 6  | Index value state | <p>インデックスのソースを指定します。インデックスを定義する場合、この文字列を 1 に設定します。eDirectory では次の値がサポートされています。</p> <ul style="list-style-type: none"> <li>0 - 未初期化</li> <li>1 - サーバから追加</li> <li>2 - ローカル DIB から追加</li> <li>3 - ローカル DIB から削除</li> <li>4 - ローカル DIB から変更</li> </ul>  |
| 7  | Attribute name    | <p>属性の NDS 名を指定します。eDirectory では多くの属性が LDAP 名と NDS 名の両方を持っています。この文字列には NDS 名が必要です。</p>   |

### インデックスを作成する LDIF ファイルの例

```
dn: cn=testServer-NDS,o=Novell
changetype: modify
add: indexDefinition
indexDefinition: 0$indexName$2$2$0$1$attributeName
```

## インデックスを削除する LDIF ファイルの例

```
dn: cn=osg-nw5-7, o=Novell
changetype: modify
delete: indexDefinition
indexDefinition: 0$indexName$2$2$0$1$attributeName
```

## プレディケートデータ

プレディケートデータは、検索の対象となったオブジェクトに関する、サーバ固有の履歴を表します。このデータおよびデータの収集は、eDirectory のインストール時に作成された `ndsPredicateStats` オブジェクトを通して管理されます。`ndsPredicateStats` オブジェクトの名前は、サーバ名に「-PS」が追加されたものになります。

プレディケートデータを使用して最も頻繁に検索されているオブジェクトを識別し、そのオブジェクトのインデックスを作成して今後のアクセスを高速化できます。

## プレディケートデータを管理する

プレディケート統計は、常時実行する機能ではありません。プレディケート統計の収集は、検索のパフォーマンスに影響を与えます。また、データベースのサイズが大きい場合には、統計の収集に長時間かかります。特定のディレクトリの検索で、パフォーマンスの低下が問題になっていると思われる場合に、プレディケート統計を使用します。

ConsoleOne の [プレディケートデータ] プロパティページを使用して、データの収集を管理します。

- 1 ConsoleOne で、サーバオブジェクトを右クリックします。
- 2 [プロパティ] > [プレディケートデータ] > [プロパティ] の順にクリックします。
- 3 `ndsPredicateStats` オブジェクトに対して適切な設定を入力します。

[更新間隔] データ表示をリフレッシュし、データをディスクに書き込むまでの秒数を指定します。

[詳細] > [有効] 収集プロセスをバックグラウンドで実行するか、または実行しないかを指定します。データの収集をオフにすると、最後に収集されたデータがメモリから解放されます。[ディスクへ書き込む] を選択すると、データはディスクへ書き込まれます。

[詳細] > [ディスクへ書き込む] プレディケートデータの格納場所を決定します。常にメモリに格納するか、[更新間隔] で指定したディスクにメモリから書き込むかを指定します。

[詳細] > [値の表示] データを省略して表示するか、または完全に表示するかを選択します。省略表示では、インデックスの対象に適しているプレディケートを判断するために必要な情報が表示されます。

- 4 [OK] をクリックすると、オブジェクト設定が更新されます。

# eDirectory Service Manager

eDirectory Service Manager では、使用可能な eDirectory サービスおよびそのステータスについての情報が提供されます。また、Service Manager からこれらのサービスを開始または停止できます。

Service Manager は eDirectory サービスのみを管理します。dsservcfg.xml 設定ファイルを使用して管理を行います。このファイルには、各プラットフォームで管理できるサービスを表示します。リストにサービスを追加または削除することもできます。

eDirectory Service Manager には次の方法でアクセスできます。

- ◆ 194 ページの「eMBox クライアントのサービスマネージャ eMTool を使用する」
- ◆ 195 ページの「Novell iManager でサービスマネージャプラグインを使用する」

## eMBox クライアントのサービスマネージャ eMTool を使用する

eMBox (eDirectory Management Toolbox) クライアントはコマンドラインで実行される Java クライアントで、eDirectory Service Manager eMTool にリモートアクセスできます。emboxclient.jar ファイルは、eDirectory の一部としてサーバにインストールされます。JVM をインストールしていれば、どのコンピュータでも実行できます。eMBox クライアントの詳細については、555 ページの「eMBox コマンドラインクライアントの使用」を参照してください。

eMBox クライアントのサービスマネージャ eMTool は、次の手順で使用します。

- 1 コマンドラインで次のように入力して、対話式モードで eMBox クライアントを実行します。

```
java -cp ファイルのパス/emboxclient.jar embox -i
```

(クラスパスに emboxclient.jar ファイルがすでに含まれている場合は、**java embox -i** と入力するだけです。)

eMBox Client のプロンプトが次のように表示されます。

```
eMBox Client>
```

- 2 Service Manager を実行するサーバにログインするには、次のコマンドを入力します。

```
login -s サーバの名前または IP アドレス -p ポート番号  
-u ユーザ名 . コンテキスト -w パスワード -n
```

ポート番号は通常 80 または 8028 です。ただし、すでにそのポートを使用している Web サーバが存在する場合は異なります。-n オプションを使用すると、非セキュア接続を開始します。

eMBox クライアントはログインが成功したかどうかを表示します。

- 3 次のいずれかの Service Manager コマンドを入力します。

| コマンド  | 説明                           |
|---|------------------------------|
| <code>service.serviceList</code>            | 利用できる eDirectory サービスを表示します。 |
| <code>service.serviceStart -n モジュール名</code> | 指定された eDirectory サービスを開始します。 |
| <code>service.serviceStop -n モジュール名</code>  | 指定された eDirectory サービスを停止します。 |
| <code>service.serviceInfo -n モジュール名</code>  | 指定されたサービスに関する情報を表示します。       |

eMBox クライアントで `list -t service` コマンドを使用して、Service Manager オプションの詳細を表示することもできます。詳細については、[559 ページの「eMTool とそのサービスを表示する」](#)を参照してください。


- 4 eMBox クライアントからログアウトするには、次のコマンドを入力します。






`logout`

- 5 eMBox クライアントを終了するには、次のコマンドを入力します。

`exit`

## Novell iManager でサービスマネージャプラグインを使用する

- 1 Novell iManager で、[役割およびタスク] ボタン  をクリックします。
- 2 [eDirectory の保守] > [サービスマネージャ] の順にクリックします。
- 3 管理するサーバを指定し、[OK] をクリックします。
- 4 選択したサーバの認証を行い、[OK] をクリックします。
- 5 eDirectory サービスの状態をチェックしたり、サービスを開始または停止するには、次のアイコンを使用します。

| アイコン  | 説明                   |
|---|----------------------|
|  | サービスは実行中です。          |
|  | サービスは停止しています。        |
|  | サービスを開始します。          |
|  | サービスを停止します。          |
|  | サービスは実行中ですが、停止できません。 |





# 7

## Novell iMonitor 2.1 の使用

Novell® iMonitor は、eDirectory™ ツリー内にあるすべてのサーバに対して、複数プラットフォーム対応の監視および診断機能を提供します。Novell iMonitor ユーティリティを使用すると、ネットワーク上で Web ブラウザを使用できる場所ならどこからでもサーバを監視できます。

また iMonitor により、eDirectory 環境に対して、パーティション、レプリカ、またはサーバベースの詳細な管理が可能になります。また、実行しているタスクの種類、タスクの開始時間、結果、および実行時間を検証できます。

iMonitor は、Novell が従来提供していたサーバベースの eDirectory ツール (DSBrowse、DS トレース、DSDiag、および DSRepair が持つ診断機能など) に対して、その代わりに使用できる機能や置き換えることのできる機能を提供します。これらの機能は、Web ベースで利用できます。このため、iMonitor の機能は主にサーバで動作することに重点を置いています。つまり eDirectory ツリー全体ではなく、個々の eDirectory エージェント (ディレクトリサービスで実行しているインスタンス) の状態が、iMonitor の機能に対して重要な要素となります。

iMonitor 2.1 の機能は次のとおりです。

- ◆ eDirectory ヘルスママリ
  - ◆ 同期情報
  - ◆ 認識されているサーバ
  - ◆ エージェントの環境設定
- ◆ eDirectory ヘルスチェック
- ◆ ハイパーリンク付きの DS トレース
- ◆ エージェントの環境設定
- ◆ エージェントアクティビティおよび Verb 統計
- ◆ レポート
- ◆ エージェント情報
- ◆ エラー情報
- ◆ オブジェクト / スキーマブラウザ
- ◆ Novell Nsure Identity Manager モニタ
- ◆ 検索
- ◆ パーティションリスト
- ◆ エージェントプロセスのステータス
- ◆ バックグラウンドプロセスのスケジュール
- ◆ DSRepair
- ◆ 接続監視

iMonitor の情報は、次の要素に基づいて表示されます。

- ◆ 確立された識別情報

iMonitor で実行するすべての要求は、識別情報に基づく eDirectory 権によって制限されます。たとえば、[DSRepair] ページにアクセスするには、アクセスを行うサーバに対して、サーバの管理者またはコンソールオペレータとしてログインする必要があります。

- ◆ 監視している eDirectory エージェントのバージョン

新しいバージョンの NDS<sup>®</sup> および eDirectory には、以前のバージョンにはない機能とオプションがあります。

iMonitor に表示された情報から、ローカルサーバの状態が一目でわかります。

この章では次のトピックについての情報を説明します。

- ◆ 198 ページの「システム要件」
- ◆ 199 ページの「iMonitor へアクセスする」
- ◆ 199 ページの「iMonitor のアーキテクチャ」
- ◆ 206 ページの「iMonitor の機能」
- ◆ 224 ページの「セキュリティ保護された iMonitor 操作の実現」

## システム要件

iMonitor 2.1 を使用するには次のソフトウェアが必要です。

- ◆ Internet Explorer 5.5 以降、または Netscape 7.02 以降
- ◆ Novell eDirectory 8.7.1 以降

## プラットフォーム

iMonitor 2.1 ユーティリティは次のプラットフォームで動作します。

- ◆ NetWare<sup>®</sup> 5.1 Support Pack 4 以降  
Novell iMonitor は AUTOEXEC.NCF に格納されます。
- ◆ Windows 2000 および 2003 Server (SSL なし)
- ◆ Linux の場合
- ◆ Solaris の場合
- ◆ AIX の場合
- ◆ HP-UX の場合

NetWare および Windows では、eDirectory が実行されると、iMonitor は自動的にロードされます。Linux、Solaris、AIX、および HP-UX の場合、ndsmonitor コマンドで -l オプションを使用して iMonitor をロードできます。また、/etc/opt/novell/eDirectory/conf/ndsmonitor.conf ファイルに [ndsmonitor] を追加して、eDirectory サーバを開始する前に iMonitor を自動的にロードすることもできます。

## 監視できる eDirectory のバージョン

iMonitor を使用して監視できる NDS および eDirectory のバージョンは次のとおりです。

- ◆ NetWare 4.11 用以降のすべてのバージョンの NDS および eDirectory
- ◆ Windows 用のすべてのバージョンの NDS および eDirectory
- ◆ Linux、Solaris、AIX、および HP-UX 用のすべてのバージョンの NDS および eDirectory

## iMonitor へアクセスする

- 1 iMonitor の実行ファイルが eDirectory サーバで実行されていることを確認します。
- 2 Web ブラウザを開きます。
- 3 アドレス (URL) のフィールドに、次の形式で入力します。

**http:// サーバの TCP/IP アドレス : HTTP スタックポート /nds**

たとえば、次のように入力します。

http://137.65.135.150:8028/nds

DNS 名は、iMonitor 内でサーバの IP または IPX™ アドレス、もしくは識別名を使用できる箇所であれば常に使用できます。たとえば、次のような DNS が設定されているとします。

http://prv-gromit.provo.novell.com/nds?server=prv-igloo.provo.novell.com

これは、次の設定と同等です。

http://prv-gromit.provo.novell.com/nds?server=IP または IPX アドレス

または

http://prv-gromit.provo.novell.com/nds?server=/cn=prv-igloo,  
ou=ds,ou=dev,o=novell,t=novell\_inc

eDir HTTPS スタックが有効であれば、HTTPS を通して iMonitor を使用できます。

- 4 ユーザ名、コンテキスト、パスワードを指定します。  
すべての機能にアクセスするには、完全識別名を指定して管理者としてログインするか、管理者と同等のアクセス権でログインします。
- 5 [ログイン] をクリックします。

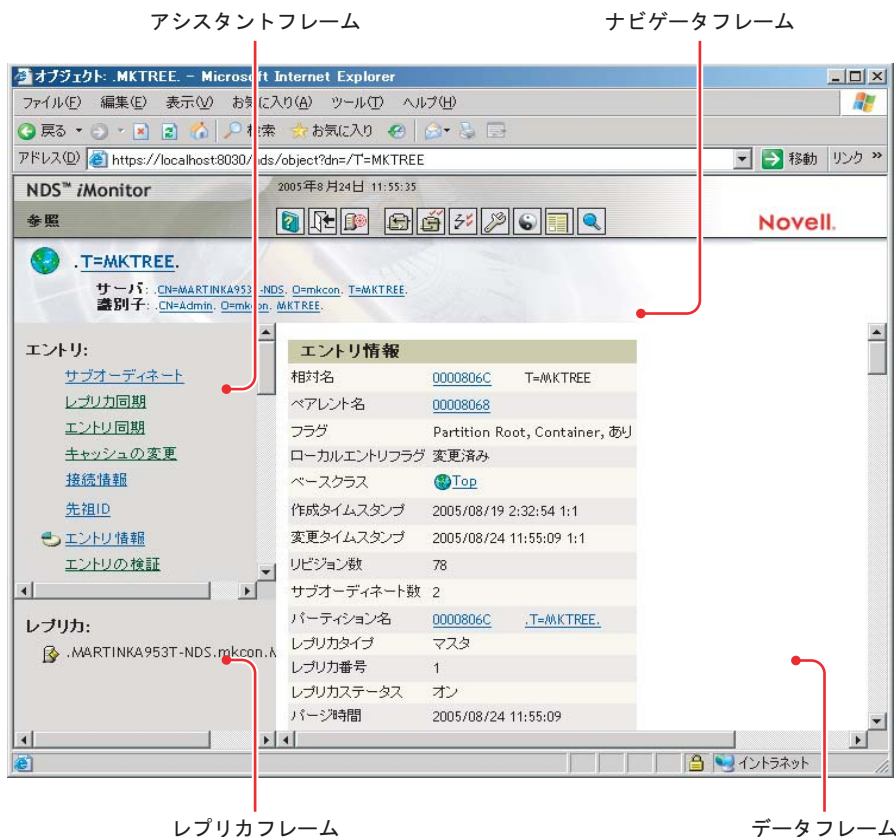
## iMonitor のアーキテクチャ

- ◆ 200 ページの「iMonitor ページの構成」
- ◆ 201 ページの「動作モード」
- ◆ 202 ページの「すべてのページからアクセス可能な iMonitor の機能」
- ◆ 202 ページの「NetWare Remote Manager との統合」
- ◆ 203 ページの「環境設定ファイル」

## iMonitor ページの構成

iMonitor の各ページは、ナビゲータフレーム、アシスタントフレーム、データフレーム、およびレプリカフレームの 4 つのフレームまたはセクションに分かれています。

図 30 iMonitor の各フレーム



**ナビゲータフレーム:** ページの上部にあります。このフレームには、データの読み込み元のサーバ名、ユーザの識別情報、および他の画面 (オンラインヘルプ、ログイン、サーバポータルなどの iMonitor ページ) にリンクするためのアイコンが表示されます。

**アシスタントフレーム:** ページの左側にあります。このフレームには、ナビゲーション用の項目 (他のページへのリンクなど)、データフレームでのデータの検索に使用する項目、および表示されているページでのデータの取得や解釈に使用する項目が含まれます。

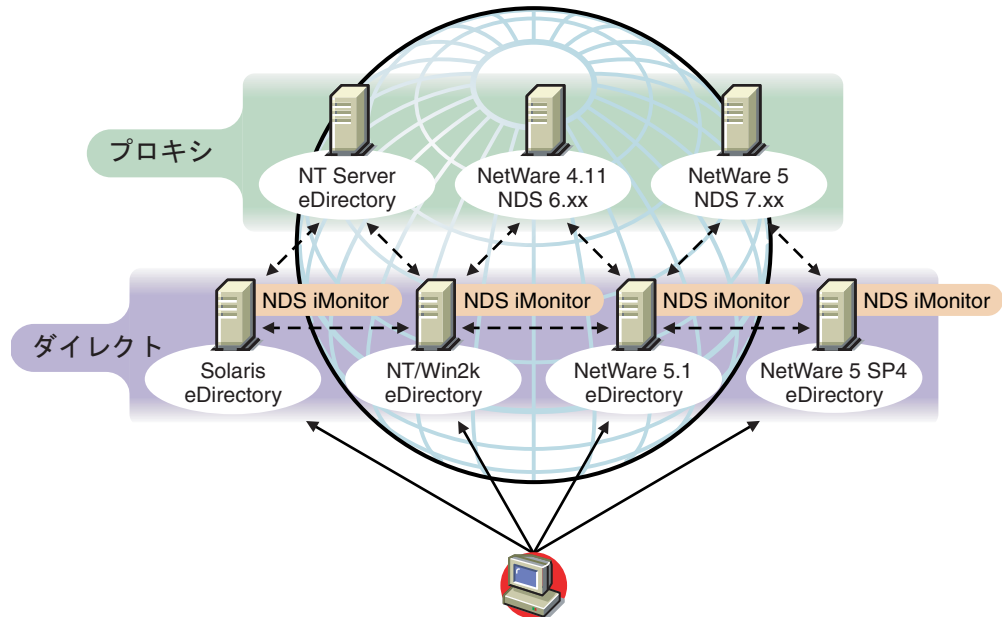
**データフレーム:** 上部にあるリンクをクリックすると、ローカルサーバに関する詳細情報が表示されます。Web ブラウザがフレームをサポートしていない場合には、このページだけが表示されます。

**レプリカフレーム:** 現在表示されているレプリカを判別できます。またリンクを使用して、現在表示されている情報が、他のサーバやレプリカを基準としたときに、どのような状態になっているかを確認できます。表示したページに、要求したデータの他のレプリカが存在する場合、またはデータフレームに表示されている情報を別の状態で表示するレプリカが存在する場合にのみ、レプリカフレームが表示されます。

## 動作モード

Novell iMonitor には、ダイレクトモードとプロキシモードという 2 種類の動作モードがあります。モードを切り替えるために環境設定情報を変更する必要はありません。モードは Novell iMonitor が自動的に切り替えますが、eDirectory ツリーのナビゲートを正しく効率的に行うために、これらのモードについて理解しておくことをお勧めします。

図 31 動作モード



**ダイレクトモード**：ダイレクトモードが使用されるのは、Web ブラウザが iMonitor の実行ファイルを実行しているコンピュータ上のアドレスまたは DNS 名を直接ポイントしていて、そのコンピュータのローカル eDirectory DIB 上の情報だけを読み込んでいる場合です。

iMonitor の機能の中にはサーバ限定のものもあります。ここでいう「サーバ限定」の機能とは、ローカルコンピュータ上で動作している iMonitor 以外からは使用できない機能のことです。サーバ限定の機能では、リモートからアクセスできないローカル API のセットを使用します。サーバ限定の iMonitor の機能には、DS トレース、DSRepair、および [バックグラウンドプロセスのスケジュール] ページなどがあります。ダイレクトモードの場合、すべての iMonitor 機能がローカルコンピュータから利用できます。

ダイレクトモードの主な特徴は次のとおりです。

- ◆ サーバ限定の機能をすべて使用できます。
- ◆ ネットワークの通信量が減少します (高速アクセスが可能)。
- ◆ eDirectory のバージョンに関係なく、プロキシによるアクセスも可能です。

**プロキシモード**：プロキシモードが使用されるのは、Web ブラウザが、1 つのコンピュータ上で実行されている iMonitor をポイントしていて、同時に他のコンピュータから情報を読み込んでいる場合です。iMonitor では、サーバ限定でない機能に対してはサーバ限定でない従来の eDirectory プロトコルを使用するため、NDS 6.x 以降の従来のバージョンの eDirectory でも監視や診断の対象にできます。ただし、サーバ限定の機能では、リモートからアクセスできない API が使用されます。

プロキシモードが有効なときに、他のサーバの動作モードをダイレクトモードに切り替えることもできます。ただし、そのサーバの eDirectory のバージョンで iMonitor がサポートされていることが条件です。プロキシによる情報収集対象のサーバ上で iMonitor が実行されている場合は、ナビゲータフレームに追加のアイコンボタンが表示されます。カーソルをこのアイコン上に移動すると、そのリモートサーバ上で実行されているリモート iMonitor へのリンクが表示されます。ただし、情報収集対象のリモートサーバで以前のバージョンの eDirectory が実行されている場合は、このアイコンは表示されません。そのリモートサーバが iMonitor をサポートしているバージョンの eDirectory にアップグレードされるまでは、そのサーバからの情報収集には常にプロキシを使用する必要があります。

プロキシモードの主な特徴は次のとおりです。

- ◆ ツリー内のすべてのサーバで iMonitor を実行しなくても、iMonitor の機能の大部分を利用できます
- ◆ 1つのサーバをアップグレードするだけで済みます
- ◆ 1つのアクセスポイントでダイヤルインが可能です
- ◆ iMonitor 自体へのアクセスには低速なリンクを使用し、iMonitor から eDirectory 情報へのアクセスには高速なリンクを使用できます
- ◆ 以前のバージョンの NDS の情報にアクセスできます
- ◆ サーバ限定の機能は、iMonitor がインストールされているコンピュータ以外では使用できません

## すべてのページからアクセス可能な iMonitor の機能

エージェントの要約、エージェント情報、エージェントの環境設定、トレースの環境設定、DSRepair、レポート、および検索の各ページには、ナビゲータフレームを使用することによってどの iMonitor ページからでもリンクできます。その他、どの iMonitor ページからでも、Novell Support Web ページにログインおよびリンクできます。

**[ログイン] ボタンと [ログアウト] ボタン**：システムにログインしていない状態では、[ログイン] ボタンが有効になります。システムにログインしている状態では [ログアウト] ボタンが表示され、これを使用するとブラウザウィンドウを閉じることができます。ブラウザウィンドウがすべて閉じられるまでは iMonitor セッションは開いたままになるので、そのつどログインし直す必要がありません。自分のログインステータスは、ナビゲータフレームに表示された識別情報を調べることによって、どのページからでも確認できます。

**Support Connection ページへのリンク**：ページ右上に表示される Novell のロゴは、Novell Support Connection Web ページへのリンクとして使用できます。ここから Novell の Web サイトに直接リンクして、最新のサーバパッチキット、更新データ、各製品に固有なサポート情報などを取得できます。

## NetWare Remote Manager との統合

NetWare 5 以降のサーバからは NetWare Remote Manager へリンクでき、NetWare サーバの監視、診断、およびトラブルシューティング情報の取得が Web ベースで実行できます。

iMonitor と NetWare Remote Manager を統合する方法を次に示します。

- ◆ NetWare Remote Manager のライトウェイト Web サーバ (httpstk.nlm) は、NetWare プラットフォームに対して、iMonitor アーキテクチャの第 1 層を割り当てます。

- ◆ iMonitor が NetWare Remote Manager (portal.nlm) に登録されます。これで、iMonitor および他の eDirectory 固有の情報へのリンクが、NetWare Remote Manager インタフェース経由で使用可能になります。

これらのリンクは、Remote Manager インタフェースの[ eDirectory の管理] セクションに表示されます。また eDirectory エージェントのヘルス情報へのリンクが、eDirectory 関連のカテゴリ内にあるヘルスマニタの [Diagnose Server (サーバの診断)] セクションに表示されます。

また、NetWare Remote Manager が eDirectory に登録されます。これにより iMonitor と NetWare Remote Manager 間のクロスリファレンスが可能になり、各ツール間の移動が、よりスムーズになります。

## 環境設定ファイル

iMonitor に含まれる環境設定ファイルを使用すると、ユーティリティのデフォルトの動作や値を変更したり、設定することができます。

環境設定ファイルはテキストファイルで、必要な値が指定された環境設定パラメータタグが含まれています。このファイルは NetWare および Windows 上では iMonitor の実行可能ファイルと同じディレクトリ (通常 Novell eDirectory の実行可能ファイルと同じ場所)、または Linux、Solaris、AIX、および HP-UX 上では /etc ディレクトリにあります。

- ◆ [203 ページの「ndsimon」](#)
- ◆ [204 ページの「ndsimonhealth」](#)

### ndsimon

ndsimon の環境設定ファイルでは、トレースファイルの設定の変更、サーバへのアクセス制御、コンテナのリスト表示または検索結果を表示する際のオブジェクトの最大表示数の設定、およびアイドル状態が何分続くと接続がログアウトするかを指定できます。

| サーバ                         | 環境設定ファイル                                     |
|-----------------------------|--|
| NetWare                     | sys:¥system¥ndsimon.ini                      |
| Windows NT および Windows 2000 | インストールディレクトリ¥novell¥NDS¥ndsimon.ini          |
| Linux, Solaris, AIX, HP-UX  | /etc/opt/novell/eDirectory/conf/ndsimon.conf |

ndsimon の環境設定ファイルに設定するパラメータには、次のような 2 種類のグループがあります。

- ◆ iMonitor の実行可能ファイル自体の実行方法に適用されるパラメータ

NetWare の場合を除き、iMonitor の実行可能ファイルはロードされると、従来の HTTP ポート 80 で受信待機します。このポートが使用中の場合は、ポート 8028 に切り替えられます。ポート 8008 も使用中の場合、iMonitor は再びポートを切り替え、番号を 2 ずつ増やしながら (8010, 8012 など) 8078 に達するまでポート番号を検索します。

SSL が設定され使用可能になっている場合も、同様のパターンでバインドが実行されます。この場合、最初にポート 81 がバインドされ、次に 8009、8011、8013 と続きます。

これにより、iMonitor と、同じサーバで実行している Web サーバとの共存が可能になります。プラットフォームによっては、インストールされた Web サーバをロードする前に iMonitor をロードできます。また、iMonitor をバインドするポートを選択することもできます。通常のポートおよび SSL ポートは、HttpPort および HttpsPort パラメータをそれぞれに使用して設定できます。付属の環境設定ファイルに、サンプルがコメントアウトされて含まれています。デフォルトでは、iMonitor は、ロードするサーバのすべての NIC アドレスにバインドされます。ただし、[アドレス] パラメータを使用して、バインドするアドレスをコンマ区切り形式のリストで指定できます。

NetWare でも、ポート選択について同様の規則が使用されますが、この規則は NetWare Remote Manager HTTP スタック (httpstk.nlm) によって制御されます。この規則の詳細は、NetWare Remote Manager のマニュアルに記載されています。

- ◆ 特定の機能またはページに適用されるパラメータ

iMonitor に付属する環境設定ファイルには、変更可能なパラメータのサンプルが含まれています。これらのパラメータの先頭にはシャープ記号 (#) が付いています。これは、パラメータがコメントアウトされていることを示していて、iMonitor が環境設定ファイルを解析するときには、これらのパラメータは無視されます。付属する環境設定ファイルでは、これらのパラメータにはすべて、内部でバインドされたデフォルト値が使用されます。これらのパラメータを使用可能にする、またはパラメータを追加するには、行の先頭の「#」を削除します。

## ndsimonhealth

ndsimonhealth の環境設定ファイルでは、[エージェントヘルス] ページのデフォルト設定を変更できます。[エージェントヘルス] オプションを有効または無効にしたり、オプションのレポートレベルおよび範囲を設定したり、サーバのレポートレベルを設定できます。

| サーバ                         | 環境設定ファイル   |
|-----------------------------|--|
| NetWare                     | sys:¥system¥ndsimonhealth.ini                      |
| Windows NT および Windows 2000 | インストールディレクトリ<br>¥novell¥NDS¥ndsimonhealth.ini      |
| Linux, Solaris, AIX, HP-UX  | /etc/opt/novell/eDirectory/conf/ndsimonhealth.conf |

ndsimonhealth の環境設定ファイルに設定するオプションには、次のような 3 種類のオプションがあります。

- ◆ オプションのみを有効または無効にする

オプションを無効にするには、オプションの前のシャープ記号 (#) を削除し、コロン (:) の後ろにリスト表示されるすべてのレベルを「OFF」に置き換えます。これらのオプションのレポートレベルを設定するには、オプションの前の「#」文字を削除し、コロン(の)後ろにレポートレベルを追加します。有効なレベルは、WARN、MARGINAL、および SUSPECT です。これらのオプションに入力できるレポートレベルは 1 つだけです。



- ◆ 設定の範囲を指定する一般オプション

これらのオプションでは、レポートレベルの設定を有効または無効にしたり、レポートレベルを設定したりできます。またレポートレベルの範囲の設定もできます。

これらのすべてのオプションのレポートレベルを設定するには、オプション名の後に `-active` と記述し、その後ろに設定するレポートレベルを記述します。たとえば、`time_delta` をアクティブに設定するには、環境設定ファイルに次の行を追加します。

```
time_delta-active: WARN
```

`time_delta` を非アクティブに設定するには、環境設定ファイルに次の行を追加します。

```
time_delta-active: OFF
```

範囲を入力する場合、指定する範囲はこのレポートレベルを表示しない範囲です。

3 つすべてのレポートレベルをアクティブにするオプションの設定方法、および範囲の設定方法については、次の `time_delta` の例を参照してください。この例では、`-2 ~ 2` の範囲外では少なくとも `marginal` のレベルが表示され、`-5 ~ 5` の範囲外では少なくとも `suspect` のレベルが表示され、`-10 ~ 10` の範囲外では `warning` のレベルが表示されます。

```
time_delta-active: WARN | SUSPECT | MARGINAL
time_delta-Min_Warn:      -10
time_delta-Min_Suspect:  -5
time_delta-Min_Marginal:  -2
time_delta-Max_Marginal:   2
time_delta-Max_Suspect:   5
time_delta-Max_Warn:     10
```

これらのオプションのヘルプを表示するには、iMonitor で次の URL を入力します。

```
http://XXX.XXX.XXX.XXX: ポート /nds/help?hbase=/nds/health/ オプション名
```

`XXX.XXX.XXX.XXX`: ポートには iMonitor がアクセスできる IP アドレスとポート、`オプション名`にはヘルプ表示するオプション名 (`time_delta` など) を入力します。

現在の設定レベルと範囲を表示するには、ブラウザを使用して表示するオプションを含むヘルスページへ進み、ブラウザの URL 行の最後に次を追加します。

```
&op=setup
```

- ◆ カスタム設定または複合設定が必要なオプション

設定できるレポートレベルには次の 3 種類があります。

- ◆ **WARN** は、すぐにアップグレードする必要があるバージョンの eDirectory を実行しているサーバを検出します。
- ◆ **SUSPECT** は、アップグレードが望まれるバージョンの eDirectory を実行しているサーバを検出します。
- ◆ **MARGINAL** は、最新バージョンではない eDirectory を実行しているサーバを検出します。

これらのオプションは、サーバのバージョンが指定された許容範囲にあるかどうかのレポートレベルを設定します。

# iMonitor の機能


このセクションでは iMonitor の機能について簡単に説明します。

iMonitor が持つ各機能の詳細については、オンラインヘルプの該当するセクションを参照してください。

- ◆ 206 ページの「eDirectory サーバのヘルス情報の表示」
- ◆ 207 ページの「パーティション同期ステータスの表示」
- ◆ 207 ページの「サーバ接続情報の表示」
- ◆ 208 ページの「認識されているサーバの表示」
- ◆ 208 ページの「レプリカ情報の表示」
- ◆ 209 ページの「DS エージェントを制御および環境設定する」
- ◆ 210 ページの「トレースを環境設定する」
- ◆ 211 ページの「プロセスステータス情報の表示」
- ◆ 211 ページの「エージェントアクティビティの表示」
- ◆ 212 ページの「トラフィックパターンの表示」
- ◆ 212 ページの「バックグラウンドプロセスの表示」
- ◆ 212 ページの「eDirectory サーバエラーの表示」
- ◆ 213 ページの「DSRepair 情報の表示」
- ◆ 213 ページの「エージェントのヘルス情報を表示する」
- ◆ 213 ページの「ツリー内のオブジェクトの参照」
- ◆ 214 ページの「同期またはパージのためのエントリの表示」
- ◆ 215 ページの「レプリカの同期ステータスの表示」
- ◆ 215 ページの「レポートの設定と表示」
- ◆ 217 ページの「スキーマ、クラス、および属性定義の表示」
- ◆ 217 ページの「オブジェクトの検索」
- ◆ 218 ページの「ストリームビューアの使用」
- ◆ 218 ページの「DIB セットのクローン」

## eDirectory サーバのヘルス情報の表示

[エージェントの要約] ページでは、同期設定、エージェントプロセスのステータス、データベースで認識されているサーバの総数など、eDirectory サーバのヘルス情報を表示できます。

**1** iMonitor で、[エージェントの要約]  をクリックします。

**2** 次のオプションから選択します。

[エージェント同期の概要] レプリカの数とタイプ、およびこれらレプリカが正常に同期されてから経過した時間を表示できます。その他、レプリカのタイプ別にエラーの数を表示することもできます。表示できるレプリカまたはパーティションが 1 つだけの場合、項目名は「パーティション同期ステータス」になります。

[エージェント同期の概要] が表示されない場合は、ユーザの識別情報に基づく権利で表示できるレプリカがないことを意味します。

[データベースで認識されているサーバ合計] ローカルデータベースが認識しているサーバのタイプと数、および各サーバが実行中であるかどうかを表示できます。

[エージェントプロセスのステータス合計] エージェント上で実行されているプロセスのステータスを、管理者に依頼せずに自分で調べることができます。ステータス情報は問題や重要な情報が発生したときに記録されます。表示される表のサイズは、記録されているステータスの数によって異なります。

## パーティション同期ステータスの表示

[エージェント同期] ページでは、パーティションの同期状態を表示できます。ページの左側のアシスタントフレームに一覧表示されているオプションから選択して、表示する情報を絞り込むこともできます。

- 1 iMonitor で、アシスタントフレームの [エージェント同期] をクリックします。
- 2 次のオプションから選択します。

[パーティション同期ステータス] パーティション、エラーの数、最終同期時刻、最大リングデルタを表示できます。

[パーティション] パーティションごとの「レプリカ同期」ページへのリンクを表示できます。

[最終同期日時] サーバから個々のパーティションのレプリカをすべて同期できたときから経過した時間を表示できます。

[最大リングデルタ] リング内にあるすべてのレプリカに対して同期できない可能性があるデータ量を表示します。たとえば、あるユーザが自分のログインスクリプトを変更してから 30 分が経過していない場合、最大リングデルタへの割り当てが 45 分であれば、このユーザのログインは正常に同期されないおそれがあります。その場合、このユーザはログイン時に前のログインスクリプトを受け取るようになります。一方、ユーザが現時点から 45 分以上前にログインスクリプトを変更した場合は、このユーザはすべてのレプリカから常に新しいログインスクリプトを受け取るようになります。

[最大リングデルタ] に [不明] が表示されている場合は、遷移同期ベクトルに不整合があり、レプリカ/パーティション操作が実行中などの理由で最大リングデルタを計算できないことを意味します。

## サーバ接続情報の表示

[エージェント情報] ページでは、ローカルサーバの接続情報を表示できます。

- 1 iMonitor で、アシスタントフレームの [エージェント情報] をクリックします。
- 2 次のオプションから選択します。

[Ping 情報] サーバからの通知先アドレスのセットに対して、iMonitor が IP Ping を送信したことを表示します。表示されるのは、応答があった場合です。

[DNS 名] iMonitor がサーバによってサポートされている IP アドレスに対してアドレスの反転を試みたことを表示します。対応する DNS 名が表示されます。

使用しているトランスポート、環境設定、およびプラットフォームによっては、この情報が表示されない場合もあります。

[接続情報] サーバの参照、タイムデルタ、一番ルート側のマスタレプリカ、およびレプリカ深さなどのサーバの情報を表示できます。

使用しているトランスポート、環境設定、およびプラットフォームによっては、この情報が表示されない場合もあります。

[サーバ照会] ローカルサーバへのアクセスに使用できるアドレスを一括して表示できます。

[時刻同期済み] レプリカの最終タイムスタンプが現在の時刻より大きい値でない限り、合成時刻や将来の時刻は使用されていないことを示します。

eDirectory では、サーバの現在時刻に基づいてタイムスタンプが正しく発行されるよう、時刻の同期が行われることが前提とされています。ただし、時刻同期プロトコルが同期状態にあることは保証されていません。

[タイムデルタ] iMonitor とリモートサーバの時刻の差を秒単位で表示できます。負の整数が表示された場合、iMonitor の時刻はリモートサーバの時刻より進んでいます。正の整数が表示された場合は、iMonitor の時刻はリモートサーバの時刻より遅れています。

[最もルートに近いマスタレプリカ] 最上位のレプリカつまりネーミングツリーのルートに最も近いレプリカがマスタレプリカであることを示します。

[レプリカ深さ] 最上位レプリカの深さ (最上位レプリカとツリーのルートの間のレベル数) を表示します。

## 認識されているサーバの表示

[認識されているサーバのリスト] には、ソースサーバのデータベースが認識しているすべてのサーバのリストが表示されます。フィルタ条件を指定して、データベースで認識されているすべてのサーバまたはレプリカリング内のすべてのサーバのリストを表示できます。サーバの横にアイコンが表示された場合、そのサーバはレプリカリングのメンバーです。

- 1 iMonitor で、アシスタントフレームの [認識サーバ] をクリックします。
- 2 次のオプションから選択します。

[エントリ ID] ローカルサーバのオブジェクト識別子を表示します。エントリ ID は、複数のサーバ間で共用することはできません。

[NDS リビジョン] 通信相手のサーバにキャッシュまたは保存されている eDirectory ビルド番号または NDS バージョンを表示します。

[ステータス] サーバのステータス (稼働中、停止中、不明) を表示します。通信相手のサーバのステータスが不明となっている場合、過去にこのサーバと通信する必要がなかったことを表します。

[最終更新時刻] 該当するサーバが相手サーバと最後に通信を試みて、その相手サーバが停止中であることを検出したときの時刻を表示します。このカラムが表示されない場合は、すべてのサーバが稼働中であることを意味しています。

## レプリカ情報の表示

[パーティション] ページでは、通信相手のサーバ上にあるレプリカに関する情報を表示できます。ページの左側のアシスタントフレームに一覧表示されているオプションから選択して、表示するページの情報を絞り込むことができます。

[サーバパーティション情報] 該当するサーバのパーティションについての情報 (エントリ ID、レプリカの状態、ページ時間、最終更新時刻など) を表示できます。

[パーティション] サーバのパーティションの Tree オブジェクトに関する情報を表示できます。


[**ページ時間**] すべてのレプリカが削除を認識しているためにすでに削除されたデータを、データベースから削除できる時間を示します。

[**最終変更時刻**] このレプリカのデータベースに書き込まれたデータの、最後に発行されたタイムスタンプを表示できます。これにより、将来の時刻が設定されていないかどうか、および合成時刻が使用されていないかどうかを確認できます。

[**レプリカ同期**] パーティションに対応する [レプリカ同期サマリ] ページを表示できます。[レプリカ同期] ページには、パーティション同期ステータスとレプリカステータスについての情報が表示されます。また、パーティションとレプリカのリストを表示することもできます。

## DS エージェントを制御および環境設定する

[**エージェント環境設定**] ページでは、DS エージェントの制御および環境設定ができます。このページで利用できる機能は、現在の識別情報に基づく権利および使用している eDirectory のバージョンによって異なります。

**1** iMonitor で、[エージェント環境設定]  をクリックします。

**2** 次のオプションから選択します。

[**エージェント情報**] ローカルサーバの接続情報を表示できます。

[**パーティション**] 通信しているサーバ上にあるレプリカを表示できます。

[**レプリケーションフィルタ**] 指定した eDirectory エージェントに対して設定されたレプリケーションフィルタを表示できます。NDS eDirectory 8.5 (ビルドバージョン 85.xx) は、フィルタ済みレプリカと呼ばれる機能を初めて実装した eDirectory バージョンです。フィルタ済みレプリカの使用と設定方法の詳細については、[56 ページの「フィルタ済みレプリカ」](#)を参照してください。

[**エージェントトリガ**] バックグラウンドプロセスを開始します。エージェントトリガは、機能的には SET DSTRACE=*option* コマンドと同じです。

[**バックグラウンドプロセス処理設定**] 特定のバックグラウンドプロセスを実行する時間間隔を変更します。バックグラウンドプロセスの設定は、機能的には SET DSTRACE=*option* コマンドと同じです。

[**エージェント同期**] インバウンド同期やアウトバウンド同期を無効または有効にします。同期を無効にする期間 (単位は時間) を指定できます。

[**データベースキャッシュ**] DS データベースエンジンが使用するデータベースキャッシュのサイズを設定します。提供されるさまざまなキャッシュ統計情報により、適切な量のキャッシュが利用可能であるかを判断できます。十分なキャッシュがないと、システムのパフォーマンスが悪化する原因となります。

[**ログイン設定**] ログイン更新のキュー登録を無効にします。更新が有効な場合、更新の時間間隔を増減することもできます。


eDirectory の最新バージョンでは、ログイン速度を向上するパフォーマンス強化機能が実装されています。NDS の以前のバージョンでは、ログイン時に変更を実行する必要があったためユーザの待機時間が発生していましたが、今回の強化により、変更がキューに登録されるようになりました。eDirectory データベースに変更を加えるときは必ずデータベースのロックが必要です。そのため使用率の高い時間帯には、データベースのロックを必要とする要求の数がその時点でいくつあるかによって、ログイン時間が非常に長くなったり予測できない場合がありました。ロックの必要性をなくし、ログイン更新をキュー登録することにより、ログイン速度が大幅に向上し、予測しやすくなりました。

このオプションでは、異なる eDirectory 環境でキュー登録の動作を制御できます。環境によっては、キュー登録されたデータが重要であれば、即時にデータベースに書き込む必要があります。その場合ユーザは、更新が実行される間待機する必要があります。また別の環境では、データは全く使用されず、無視することができます。デフォルトの動作は、多くの環境に適した設定になっています。

## トレースを環境設定する

[トレースの環境設定] ページでは、トレースを設定できます。Novell iMonitor の DS トレース機能はサーバ限定の機能です。つまり、この機能は iMonitor が動作しているサーバ以外からは起動できません。他のサーバで実行されているこの機能にアクセスするには、そのサーバで実行されている iMonitor に切り替える必要があります。

[トレースの環境設定] ページの情報にアクセスするには、サーバの管理者と同等の権利またはコンソールオペレータの権利が必要です。このページの情報にアクセスする前に、認証情報の確認のためにユーザ名とパスワードを入力する必要があります。

- 1 iMonitor で、[トレースの環境設定]  をクリックします。
- 2 次のオプションから選択します。

[更新] トレースオプションおよびトレース行プリフィックスに変更を送信できます。DS トレースがオフになっているときに [オン] ボタンをクリックすると、DS トレースがオンになります。DS トレースがすでにオンになっているときに [更新] ボタンをクリックすると、変更内容が現在のトレースに反映されます。

[オン] / [オフ] DS トレースをオンまたはオフにします。ボタン上に表示される文字列は、DS トレースが現在オンかオフかによって異なります。DS トレースがオンになっている場合、ボタン上には [トレースオフ] という文字列が表示されます。DS トレースのオンとオフを切り替えるには、このボタンをクリックします。DS トレースがオフになっているときに [トレースオン] をクリックした場合の動作は、[更新] ボタンをクリックした場合と同じです。


[トレース行プリフィックス] このオプションを使用すると、トレース行の先頭に追加するデータを選択することができます。

[DS トレースオプション] トレースを開始したローカル DS エージェント上のイベントに対して適用されます。[DS トレースオプション] を使用すると、エラーと潜在的な問題、およびローカルサーバ上の eDirectory に関する情報を表示できます。[DS トレースオプション] をオンにすると、CPU の負荷が増え、システムのパフォーマンスが低下します。このため、DS トレースオプションは診断のみに使用して、通常はオフにします。[DS トレースオプション] は、機能的には SET DSTRACE=*option* コマンドと同じですが、使い易さの点では勝っています。

[イベント環境設定] DS トレースで監視のために有効または無効にする eDirectory イベントオプションをリスト表示します。イベントシステムは、オブジェクトの追加、削除、属性値の変更など、ローカルな操作に対してイベントを生成します。個々のイベントタイプに対して、そのイベントタイプに固有の情報が含まれた構造が返されます。

[トレース履歴] 以前に実行したトレースのリストを表示できます。各トレースログは、トレースデータの収集期間によって識別されます。

[トレーストリガ] DS トレース内で、指定した DS エージェント情報を表示するために設定する必要があるフラグを表示できます。トレーストリガを有効にした場合、トレースに書き込まれる情報の量が多くなります。Novell サポートからの指示があった場合にのみ、トレーストリガを有効にすることをお勧めします。

- 3 [トレースオン] をクリックして DS トレースをオンにし、変更を送信します。
- 4 iMonitor で DS トレースを表示するには、 または [トレースライブ] をクリックします。

## プロセスステータス情報の表示

[エージェントプロセスのステータス] ページでは、バックグラウンドプロセスのステータスに関するエラーと発生した各エラーの詳細情報を表示できます。ページの左側のアシスタントフレームに一覧表示されているオプションから選択して、このページに表示する情報を絞り込むことができます。

- 1 iMonitor で、アシスタントフレームの [エージェントプロセスのステータス] をクリックします。

現在、バックグラウンドプロセスのステータスで報告される情報には、次のものが含まれます。

- ◆ スキーマの同期
- ◆ 破損通知処理
- ◆ 外部参照 /DRL
- ◆ Limber
- ◆ 修復

## エージェントアクティビティの表示

[エージェントアクティビティ] ページでは、トラフィックパターンや考えられるシステムボトルネックを調べることができます。このページでは、現在 eDirectory で処理されているバンプおよび要求が表示されます。また、これらのうち、データベースへの書き込みのために DIB ロックを取得しようとしている要求がどれかを特定したり、DIB ロックの取得待機中の要求数を調べることもできます。

Novell eDirectory 8.6 以降を実行しているサーバを表示すると、パーティションのリスト、およびナビゲータフレームで指定したサーバがあるレプリカリングを対象としているサーバも表示されます。Novell eDirectory 8.6 を導入すると、同期処理はシングルスレッドではなくなります。1つの 8.6 サーバに、1つ以上のレプリケーションパートナーへのアウトバウンドパーティションが同時に複数存在する可能性があります。このため、このような並行同期処理の監視がさらに容易になるよう、[同期アクティビティ] ページが作成されています。

- 1 iMonitor で、アシスタントフレームの [エージェントアクティビティ] をクリックします。
- 2 次のオプションから選択します。

**[Verb Activity and Statistics (バンプアクティビティおよび統計情報)]** eDirectory の最後の初期化以降に呼び出されたバンプの総数や発行された要求の数をリアルタイムで表示できます。また、現在アクティブになっている要求の数と、これらの要求を処理するための最小、最大、および平均時間 (ミリ秒単位) も表示されます。

**[Synchronization Current and Schedule (現在同期およびスケジュール)]** インバウンド同期およびアウトバウンド同期が発生したさまざまな時刻のリストを表示します。インバウンド同期またはアウトバウンド同期が現在実行中の場合、プロセスが実行中であること、そのサイクルが開始された時刻、およびそのプロセスを実行しているサーバを示すアイコンも表示されます。

インバウンド同期およびアウトバウンド同期が無効になっている場合は、現在同期が無効であることおよび再び有効になる予定の時刻を示すアイコンが表示されます。アウトバウンド同期では、次に再び有効になる予定時刻も表示されます。

[イベント] 現在アクティブな状態にあるイベント、イベントハンドラの統計情報とイベント統計情報サマリ、および呼び出された現在のイベント権利機能のリストを表示できます。

[バックグラウンド処理スケジュール] スケジュールされているバックグラウンド処理、その現在の状態、および再実行のスケジュールを表示できます。

## トラフィックパターンの表示

[Verb 統計] ページでは、トラフィックパターンや考えられるシステムボトルネックを調べることができます。このページでは、eDirectory の最後に初期化されてから呼び出されたバートの総数や発行された要求の数がリアルタイムで表示されます。その他、これら要求のうち現在アクティブなものの数や、これら要求の処理にかかる時間の最大値、平均値、最小値(それぞれミリ秒単位)も表示できます。バックグラウンドプロセス、バインダリ、および標準 eDirectory 要求が追跡されます。

このページを以前のバージョンの eDirectory で表示すると、eDirectory 8.5 以降で表示する場合より情報量が少なくなります。

## バックグラウンドプロセスの表示

[バックグラウンド処理スケジュール] ページでは、スケジュールされているバックグラウンドプロセスを、現在の状態と次回の実行予定時刻とともに表示できます。Novell iMonitor のバックグラウンド処理スケジュール機能は、サーバ限定の機能です。つまり、この機能は iMonitor が動作しているサーバ以外からは表示できません。他のサーバで実行されているバックグラウンド処理スケジュール機能にアクセスするには、そのサーバで実行されている iMonitor に切り替える必要があります。eDirectory 8.5 にアップグレードしたサーバの数が増えれば、iMonitor のサーバ限定機能の利用範囲は広がります。その他のサーバ限定機能には、[DS トレース] ページおよび [DSRepair] ページなどがあります。

[バックグラウンド処理スケジュール] ページの情報にアクセスするには、サーバの管理者と同等の権利またはコンソールオペレータの権利が必要です。このページの情報にアクセスするには、認証情報の確認のためにログインする必要があります。

## eDirectory サーバエラーの表示

[エラー索引] ページでは、eDirectory サーバ上で検出されたエラーについての情報を表示できます。検出されたエラーは、eDirectory 固有のエラー用のフィールドと、関連のあるその他のエラー用のフィールドの2つに分けて表示されます。表示されるエラーのそれぞれに説明がハイパーリンクされていて、エラーの内容、考えられる原因、回復手段などがわかります。

- 1 iMonitor で、アシスタントフレームの [エラー索引] をクリックします。

エラー索引ページからは、エラーや技術情報に関して Novell が提供している最新のドキュメントやホワイトペーパーにリンクできます。



## DSRepair 情報の表示

[DSRepair] ページでは、検出された問題を表示したり、DIB セットのバックアップやクリーンアップを実行できます。Novell iMonitor の DSRepair 機能はサーバ限定の機能です。つまり、この機能は iMonitor が動作しているサーバ以外からは起動できません。他のサーバで実行されている DSRepair 情報にアクセスするには、そのサーバで実行されている iMonitor に切り替える必要があります。eDirectory の新しいバージョンにアップグレードしたサーバの数が増えれば、iMonitor のサーバ限定機能の利用範囲は広がります。この機能以外には、[DS トレース] ページや [バックグラウンド処理スケジュール] ページなどがサーバ限定の機能です。

[DSRepair] ページの情報にアクセスするには、サーバの管理者と同等の権利またはコンソールオペレータの権利が必要です。このページの情報にアクセスするには、認証情報の確認のためにログインする必要があります。

**1** iMonitor で、[DSRepair]  をクリックします。

**2** 次のオプションから選択します。

[ダウンロード] ファイルサーバから修復関連のファイルを取得できます。DSRepair ユーティリティが実行されている場合や、iMonitor の [DSRepair] ページから修復を開始した場合には、操作が完了するまでは dsrepair.log にアクセスできません。

[古い DIB セットを削除] 赤い X をクリックすると、古い DIB セットが削除できます。

**警告:** この操作は元に戻すことができません。このオプションを選択すると、古い DIB セットがファイルシステムからパージされます。

[DS Repair 拡張スイッチ] 問題の修正、問題のチェック、データベースのバックアップ作成などを実行できます。Novell サポートから指示がない限り、[サポートオプション] フィールドには、何も入力する必要はありません。

**3** [修復の開始] をクリックして、サーバ上で DS Repair を実行します。

## エージェントのヘルス情報を表示する

[エージェントヘルス] ページでは、指定した eDirectory エージェントのヘルス情報およびそのエージェントに関連するパーティションおよびレプリカリングを表示できます。

**1** iMonitor で、アシスタントフレームの [エージェントヘルス] をクリックします。

**2** リンクをクリックすると、詳細な情報が表示されます。

## ツリー内のオブジェクトの参照

[参照] ページでは、ユーザのツリー内にある任意のオブジェクトを参照できます。ページ最上部のナビゲーションバーには、表示中のオブジェクトが存在するサーバ、およびオブジェクトへのパスが表示されます。ページの左側にある [レプリカ] フレームでは、実パーティション上にある同じオブジェクトを表示またはアクセスできます。ページ内の下線付きオブジェクトをクリックすると、オブジェクトに関する詳しい情報が表示されます。また、ナビゲータフレーム内にある名前の任意の一部分をクリックすると、ツリーの上の階層を参照できます。

このページに表示される情報は、ログイン時の eDirectory 権、参照するオブジェクトのタイプ、および実行している NDS または eDirectory のバージョンによって異なります。スーパーバイザ権でログインした場合、このページには XRef オブジェクトが表示されます。レプリカリストを使用して、レプリカの実コピーへジャンプできます。ダイナミックグループのオブジェクトを参照している場合、ダイナミックメンバーに対してタイムスタンプは表示されません。

[レプリカ同期] このオブジェクトを含むレプリカの同期ステータスを表示します。

[エン트리同期] サーバ側から見て同期が必要である属性を表示します。

[接続情報] iMonitor がこのオブジェクトの情報をどこで取得したかが表示されます。

[エン트리情報] オブジェクトの名前、フラグ、ベースクラス、変更タイムスタンプ、および接続情報のサマリを表示します。

[すべてのレプリカにエントリを送信] このエントリの属性を他のすべてのレプリカに再送信します。オブジェクトに多数の属性値がある場合、この処理には時間がかかることがあります。この処理では、そのオブジェクトの、他のすべてのコピーが同一になるわけではありません。他のレプリカが各属性を再検討できるようにするだけです。

[すべて送信] (参照しているオブジェクトがパーティションルートの場合および [カスタムモード] オプションが有効になっている場合のみ表示されます)。このパーティション内のすべてのエントリを、パーティションのレプリカを保持しているすべてのサーバに再送信します。この処理では、そのオブジェクトの、送信されたすべてのコピーが同一になるわけではありません。他のレプリカが各オブジェクトとその属性を再検討できるようにするだけです。

## 同期またはパージのためのエントリの表示

[変更キャッシュ] ページでは、同期またはパージにおいてこのサーバが検討する必要のあるエンティティのリストを表示できます。このオプションを使用できるのは、ユーザがアクセスしているサーバが eDirectory 8.6 以降を実行しており、また、表示中のオブジェクトがパーティションルートである場合だけです。このページを表示するには、NCP™ サーバに対するスーパーバイザ権が必要です。

[エン트리同期] エントリが同期を必要とする理由を判別できます。

## Novell Nsure Identity Manager の詳細の表示

[DirXML の概要] ページでは、ユーザのサーバで実行中のすべての DirXML ドライバ、各ドライバのステータス、保留中の関連付け、およびドライバの詳細のリストを表示できます。

1 iMonitor で、[DirXML の概要]  をクリックします。

2 次のオプションから選択します。

[ステータス] 指定したドライバの現在の状態を表示します。表示されるステータスは、[停止]、[開始します]、[稼働中]、[シャットダウン保留中]、および [スキーマ取得中] です。

[起動オプション] 選択したドライバの現在の起動オプションを表示します。

[保留中] まだ作成されていない関連付けの数を表示します。

[ドライバ詳細] アイコンは、ユーザのサーバで実行中の DirXML ドライバに関する、加入者および発行者の詳細、XML ルール、フィルタ、および保留中の関連付けリストを表示します。このページには、最初の 50 個の保留中オブジェクトに関する詳細も表示されます。このページに表示される XML ルールを使用すると、指定した DirXML ドライバに対するオブジェクトの作成を続行するために必要な、保留中のオブジェクト内で検索すべき情報を判断できます。

## レプリカの同期ステータスの表示

[レプリカ同期] ページでは、レプリカの同期ステータスを表示できます。

- 1 iMonitor で、アシスタントフレームの [エージェント同期] をクリックします。
- 2 表示するパーティションの [レプリカ同期] をクリックします。
- 3 このページにあるリンク、および左側のナビゲーションバーにあるリンクを使用すると、他のパーティションにアクセスしたり、レプリカリング内でジャンプすることができます。

## レポートの設定と表示




[レポート] ページでは、このサーバで直接実行されているレポートを表示および削除できます。一部のレポートでは、実行に長時間を要し、多くのリソースを消費する場合があります。

スケジュール設定されたレポートは、ユーザ認証なし、つまり [パブリック] で実行します。ユーザが実行するレポートはすべて、ユーザの権利で直接実行されます。すべてのレポートデータは、そのレポートの実行元サーバに格納されます。



[レポートの環境設定] ページでは、事前に設定されたレポート、カスタムレポート、およびスケジュール設定されたレポートのリストを表示できます。このページを使用して、レポートを変更および実行できます。また、iMonitor ページ用のカスタムレポートの作成もできます。次の表に、iMonitor 2.1 であらかじめ設定されているレポートを示します。

| レポート       | 説明   |
|------------|--|
| サーバ情報      | ツリー全体を調べて、検索可能な各 NCP サーバと通信し、検出したすべてのエラーをレポートします。このレポートを使用して、時刻同期および Limber の問題を診断できます。また、現在のサーバ自体が他のすべてのサーバと通信可能であるかどうかも知ることができます。環境設定ページで選択されている場合、このサーバはツリー内にある各サーバの NDS エージェントヘルス情報を生成することもできます。 |
| 破損通知リスティング | このサーバ上のすべての破損通知を表示します。   |
| オブジェクト統計   | オブジェクトを指定したスコープで調べて、要求される条件に一致したオブジェクトのリストを生成します。この条件には、将来の時刻、不明なオブジェクト、名前が変更されたオブジェクト、ベースクラス数、コンテナ、別名、外部参照などがあります。  |
| サービスアドバタイズ | SLP または SAP を使用して現在のサーバに認識されている、すべてのディレクトリとサーバを表示します。  |
| エージェントヘルス  | 現在のサーバのヘルス情報を収集します。  |
| 値数         | 指定した値より値数が多い属性を持つオブジェクトのリストを生成します。   |



## レポートの表示と削除

- 1 iMonitor で、[レポート]  をクリックします。
- 2 レポートを削除する場合は  を、レポートを表示する場合は  をクリックします。

## レポートを実行する



- 1 iMonitor で、[レポート]  > [レポート設定] の順にクリックします。
- 2  をクリックして、レポートを実行します。

## レポートの設定またはスケジュールを行う

- 1 iMonitor で、[レポート]  > [レポート設定] の順にクリックします。
- 2  をクリックして、レポートを設定またはスケジュールします。
- 3 目的のオプションを選択し、[デフォルトの保存] をクリックして選択したオプションを保存します。
- 4 (オプション)レポートを定期的に行うか、または後で実行するかを設定します。
  - 4a レポートの頻度、開始時刻、および開始日を指定します。
  - 4b [スケジュール] をクリックします。
- 5 [レポートの実行] をクリックして、レポートを開始します。

## カスタムレポートを作成する

カスタムレポートを作成すると、iMonitor の任意のページをレポートとして起動できます。

- 1 iMonitor で、[レポート]  > [レポート設定] の順にクリックします。
- 2 [実行可能レポートリスト] の [カスタムレポート] 行にある  をクリックします。
- 3 レポートの名前を入力し、レポートとして起動する iMonitor ページの URL を入力します。

カスタムレポートを実行する場合は、次の URL を入力します。

**/nds/ 必要なページ**

- 4 保存するレポートのバージョンの数を指定します。
- 5 (オプション) [保存] をクリックして、レポートを保存します。
- 6 (オプション)レポートを定期的に行うか、または後で実行するかを設定します。
  - 6a レポートの頻度、開始時刻、および開始日を指定します。
  - 6b [スケジュール] をクリックします。
- 7 [レポートの実行] をクリックして、レポートを開始します。

## スキーマ、クラス、および属性定義の表示

[スキーマ] ページでは、ユーザのスキーマ、クラス、および属性の定義を表示できます。すでに作成されている拡張や特定のスキーマに固有の情報 (スキーマに行った変更や拡張など) を添付して、ツリー上にロードされているスキーマを表示できます。

**1** iMonitor で、アシスタントフレームの [スキーマ] をクリックします。

**2** 次のオプションから選択します。

[同期リスト] このサーバと同期する相手のサーバを表示します。このオプションは、NDS eDirectory8.5 以降を実行しているサーバに対してのみ使用できます。この情報を表示するには、サーバに対するスーパーバイザ権が必要です。

[スキーマルート] ツリーのルートに最も近いスキーマレプリカに関する情報を表示します。

各 eDirectory サーバには、エントリ内のスキーマのレプリカが保存されています。スキーマレプリカは、ディレクトリオブジェクトを格納しているパーティションから分割されて保存されます。任意のスキーマレプリカへの変更内容は、すべてのレプリカに伝えられます。スキーマの変更は、ルートパーティションの書き込み可能なレプリカを保存するサーバを通してのみ実行できます。ルートパーティションの読み込み可能なレプリカを保存しているサーバは、スキーマ情報を読み込むことはできますが、変更はできません。


[属性定義] 各属性の名前、属性値が含まれる構文、および属性が受ける制約を表示します。左側のナビゲーションフレームを使用すると、個々の属性を参照したり、それらにアクセスすることができます。

[クラス定義] 各クラスの名前、ルール、および属性を表示します。左側のナビゲーションフレームを使用すると、個々の属性を参照したり、それらにアクセスすることができます。

## オブジェクトの検索

[検索] ページでは、さまざまなクエリオプションおよびフィルタに基づいて、オブジェクトを検索できます。検索クエリオプションおよびフィルタは、2つのレベルの検索要求フォームに分けられます。それらは、基本フォームとカスタムフォームです。基本検索要求フォームは、eDirectory の一般ユーザ向けであり、基本的な検索に使用します。カスタム検索要求フォームは、熟練ユーザ向けであり、複雑な検索に使用します。現在はサーバレベルの検索のみがサポートされています。

4つのセクション内の検索オプションおよび検索フィルタは、すべて結合可能です。空白フィールド ( 相対識別名を除く ) は無視されます。<Ctrl> キーを使用して、マルチリスト上でアイテムを選択解除したり、複数のアイテムを選択することができます。選択解除したマルチリストも無視されます。

**1** Novell iMonitor で、[検索]  をクリックします。

**2** 次のオプションから選択します。

[スコープオプション] 検索のスコープを指定できます。

[エントリフィルタ] エントリ情報に関連する検索クエリフィルタを指定できます。

[属性と値のフィルタ] 属性および値に関連する検索クエリフィルタを指定できます。

[表示オプション] 検索結果の表示形式を制御するオプションを指定できます。

**3** 検索要求フォームの一番下にある [ヘルプ] ボタンをクリックすると、そのフォームに関連する簡単なヘルプ情報が表示されます。

ヘルプ情報を消すには、[再ロード] または [更新] をクリックします。

## ストリームビューアの使用

[ストリームビューア] ページでは、次の形式で現在のストリームを表示できます。

- ◆ プレーンテキスト
- ◆ HTML
- ◆ GIF
- ◆ JPEG
- ◆ BMP
- ◆ WAV
- ◆ 16 進ダンプ
- ◆ その他

特定の形式で常に表示したいストリーム属性がある場合、[ストリームビューア] を使用してデフォルトの表示設定を選択します。

[NDS ストリーム属性セットアップ] ブラウザでストリームを表示するためのデフォルトの形式を変更します。ストリームが正しく表示されるかどうかはブラウザに依存します。ブラウザによっては、ユーザが選択した設定が適用されない場合があります。

デフォルト設定に加えた変更を適用するには、ユーザがサーバに認証される必要があります。変更内容は `streams.ini` (NetWare および Windows サーバの場合) または `streams.conf` (Solaris および Linux サーバの場合) に格納されるため、デフォルトの設定は手動で編集することもできます。

## DIB セットのクローン

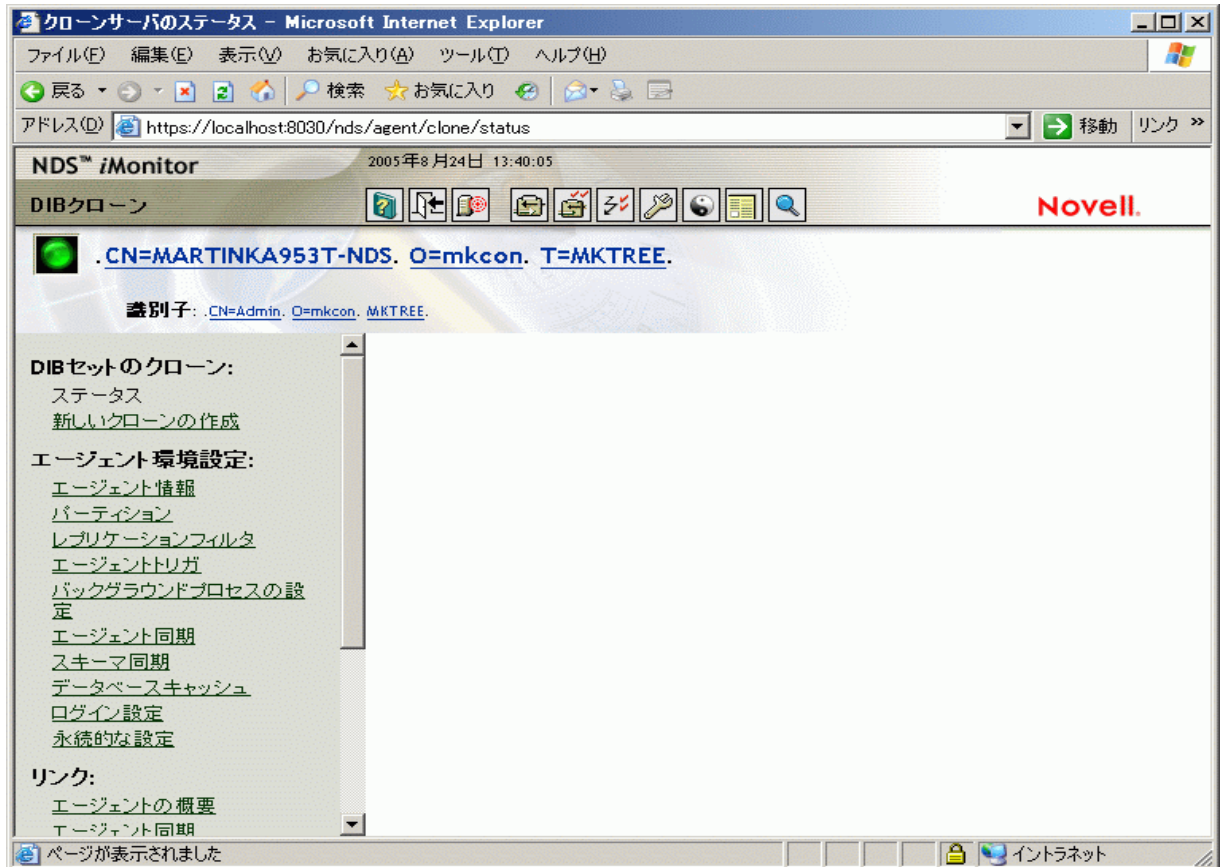
このオプションでは、1 つのサーバ (ソースサーバ) に保存されている eDirectory データベースの DIB ファイルセットを完全に複製できます。クローンは別のサーバ (ターゲットサーバ) に配置することができます。ターゲットサーバが eDirectory を開始すると、サーバは DIB ファイルセットをロードし、サーバオブジェクトのマスタレプリカに接続し、名前を解決し、クローン作成後に行われた DIB ファイルセットのすべての変更を同期します。

eDirectory DIB セットのクローンは、クローンを作成したサーバのオペレーティングシステムと同じオペレーティングシステムが稼働するサーバ上にだけ配置する必要があります。たとえば、DIB ファイルセットのクローンを Solaris サーバに復元する場合、NetWare や Windows サーバではなく、Solaris サーバ上でそのクローンを作成します。



この機能のバックエンドは eDirectory 8.7 に搭載されていましたが、eDirectory 8.7.1 で iMonitor 2.1 以降が稼働するようになるまでサポートされていませんでした。このオプションは、バージョンが 8.7 以前の Novell eDirectory や NDS では使用できません。

図 32 iMonitor の [DIB セットのクローン] ページ



このセクションでは、次の情報について説明します。

- ◆ 219 ページの「DIB セットのクローンの使用事例」
- ◆ 220 ページの「クローンを作成する」

### DIB セットのクローンの使用事例

DIB セットのクローンは次のような場合に使用します。

- ◆ すでに「オン」の状態になっているパーティションで新しいサーバを作成します。  
次の利点があります。
  - ◆ レプリカリングに新しいサーバを追加する際に、リング内のすべてのサーバが稼動中または実行中である必要がありません。
  - ◆ 新しいサーバは自動的にすべてのパーティションを保持しますが、同期する必要はありません。
  - ◆ すばやく処理できます。

◆ 障害回復

| 利点  | 欠点   |
|---|--|
| <ul style="list-style-type: none"> <li>◆ パーティションを1度コピーするだけで成功します。</li> <li>◆ 複数のパーティションをもつ大きなサーバを停止させる時間が少なくてすみます。</li> </ul> | <ul style="list-style-type: none"> <li>◆ 対象のパーティションを少なくとも1度は正しくコピーする必要があります。</li> <li>◆ SSL またはセキュリティバックアップを利用しません。</li> <li>◆ ファイルシステムを処理しません。</li> </ul> |

◆ バックアップおよび復元

| 利点   | 欠点   |
|--|--|
| <ul style="list-style-type: none"> <li>◆ 大規模のデータベースでは特に、処理に時間がかかりません。</li> </ul> | <ul style="list-style-type: none"> <li>◆ eDirectory のコアを追加するだけです。LDAP、SNMP、SSL などはインストールされません。また設定も行われません。</li> <li>◆ 最新の変更は取得されません。スナップショットのみが取得されます。ロールフォワードログは実行されません。</li> </ul> |

このような欠点があるため、バックアップ処理および復元処理のために DIB セットのクローンを使用することはお勧めできません。

## クローンを作成する

DIB ファイルセットのクローンは、元のサーバでオンラインまたはオフラインのいずれでも作成できます。オフラインで行う場合は、eDirectory を停止させておく必要があります。オンラインでは、eDirectory はロックされません。

- ◆ [220 ページの「オンラインによる方法」](#)
- ◆ [221 ページの「オフラインによる方法」](#)

### オンラインによる方法

**1** ツリーのスキーマを拡張します。

スキーマは必ず拡張してください。拡張しない場合、エラーが発生します。eDirectory のインストール時に含まれている `dibclone.sch` を使用します。これにより、iMonitor クローンユーティリティの操作に必要な属性が追加されます。

| プラットフォーム | スキーマを拡張するには、次の操作を行います。  |
|----------|---|
| NetWare  | <p>NWConfig を使用します (NWConfig.nlm&gt; [環境設定] オプション&gt; [ディレクトリ] オプション&gt; [スキーマの拡張] の順に実行します)。</p> <p><code>dibclone.sch</code> は <code>sys:¥system¥schema</code> にあります。</p>       |
| Windows  | <p>NDSCons.exe を使用します (NDSCons.exe により <code>install.dlm</code> をロードし、次に [追加のスキーマファイルのインストール] をクリックします)。</p> <p><code>dibclone.sch</code> は <code>C:¥Novell¥NDS</code> にあります。</p> |



| プラットフォーム                   | スキーマを拡張するには、次の操作を行います。  |
|----------------------------|---|
| Linux, Solaris, AIX, HP-UX | <p>ndssch を使用します。</p> <p>dibclone.sch は /opt/novell/eDirectory/lib/nds-schema にあります。</p> <p>詳細については、<a href="#">129 ページの「ndssch ユーティリティを使用して、Linux、Solaris、AIX、または HP-UX システム上のスキーマを拡張する」</a>を参照してください。</p> |

## 2 DIB ファイルセットのクローンを作成します。

### 2a iMonitor で、DIB 環境設定のクローンを実行します。

[エージェント環境設定] > 「DIB セットのクローン」 > [新しいクローンの作成] の順にクリックします。

### 2b ターゲットサーバの完全修飾名と、DIB ファイルのクローンが配置される場所のファイルパスを指定し、次に [クローンオブジェクトを作成] チェックボックスと [DIB をオンラインでクローン] チェックボックスをオンにします。

ターゲットサーバの NCP サーバ名 (クローンオブジェクト) は、ターゲットサーバの名前と一致させる必要があります。

### 2c [送信] をクリックします。

NDS クローンオブジェクトが作成され、DIB ファイルセットが指定された配置先にコピーされます。

## 3 DIB ファイルセットのクローンをターゲットサーバ上の適切なディレクトリに移動します。さらに、Linux、Solaris、AIX、および HP-UX システムの場合は、/etc/opt/novell/eDirectory/conf/nds.conf ファイルをターゲットサーバに転送し、このファイルに含まれるソースサーバへのすべての参照を、ターゲットサーバの名前に変更します。

## 4 ソースサーバ上で eDirectory を起動します。

ターゲットサーバオブジェクトのマスタレプリカが eDirectory を実行しており、使用できることを確認します。ターゲットサーバ上で eDirectory が初期化されると、eDirectory はターゲットサーバの最終的な名前が解決できるマスタレプリカと通信を行います。

## オフラインによる方法

### 1 ツリーのスキーマを拡張します。

スキーマは必ず拡張してください。拡張しない場合、エラーが発生します。eDirectory のインストール時に含まれている dibclone.sch を使用します。これにより、iMonitor クローンユーティリティの操作に必要な属性が追加されます。

| プラットフォーム | スキーマを拡張するには、次の操作を行います。  |
|----------|---|
| NetWare  | <p>NWConfig を使用します (NWConfig.nlm&gt; [環境設定] オプション&gt; [ディレクトリ] オプション&gt; [スキーマの拡張] の順に実行します)。</p> <p>dibclone.sch は sys:%system%schema にあります。</p> |
| Windows  | <p>NDSCons.exe を使用します (NDSCons.exe により install.dlm をロードし、次に [追加のスキーマファイルのインストール] をクリックします)。</p> <p>dibclone.sch は C:%Novell%NDS にあります。</p>        |

---

**プラットフォーム** スキーマを拡張するには、次の操作を行います。

---

Linux, Solaris,  
AIX, HP-UX ndssch を使用します。

dibclone.sch はインストールディレクトリ /opt/novell/eDirectory/lib/nds-schema にあります。

詳細については、[129 ページの「ndssch ユーティリティを使用して、Linux、Solaris、AIX、または HP-UX システム上のスキーマを拡張する」](#)を参照してください。

---

## 2 DIB ファイルセットのクローンを作成します。

### 2a iMonitor で、DIB 環境設定のクローンを実行します。

[エージェント環境設定] > 「DIB セットのクローン」 > [新しいクローンの作成] の順にクリックします。

### 2b ターゲットサーバの完全修飾名を指定し、[クローンオブジェクトを作成] チェックボックスをオンにして、[DIB をオンラインでクローン] チェックボックスをオフにします。

ターゲットサーバの NCP サーバ名は、ターゲットサーバの名前と一致させる必要があります。

### 2c [送信] をクリックします。

NDS クローンオブジェクトが作成されます。ソースサーバ上の eDirectory は停止しているため、eDirectory がロックされているというエラーが報告されます。

### 2d ターゲットサーバ上の配置先またはファイルセットの移動に便利なメディアに、\*.nds、nds\*、および nds.rfl/\*.\* ファイルを手動でコピーします。さらに、Linux、Solaris、AIX、および HP-UX システムの場合は、/etc/opt/novell/eDirectory/conf/nds.conf ファイルをターゲットサーバに転送し、このファイルに含まれるソースサーバへのすべての参照を、ターゲットサーバの名前に変更します。

### 2e ソースサーバ上で、eDirectory を起動します。

ファイルがコピーされる前にソースサーバ上で eDirectory が再起動された場合、このクローンは無効とみなされます。その場合は、新しい NCP サーバオブジェクトを削除してクローンを再作成する必要があります。

## 3 DIB ファイルセットのクローンをターゲットサーバ上の適切なディレクトリに移動します。

## 4 ターゲットサーバ上で eDirectory を起動します。

新しいターゲットサーバオブジェクトのマスタレプリカが eDirectory を実行しており、使用できることを確認します。ターゲットサーバ上で eDirectory が初期化されると、eDirectory はターゲットサーバの最終的な名前が解決できるマスタレプリカと通信を行います。

## eDirectory の設定を完了する

### SDIKEY

#### 1 ターゲットサーバ上で、eDirectory を停止します。

#### 2 NICISDIKEY ファイルを、ソースサーバの適切なディレクトリからターゲットサーバにコピーします。

| プラットフォーム                | ディレクトリ                                    |
|-------------------------|---|
| NetWare                 | sys:¥system¥nici¥NICISDI.KEY              |
| Windows                 | C:¥WINNT¥System32¥Novell¥NICI¥NICISDI.KEY |
| Linux、Solaris、AIX、HP-UX | /var/novell/nici/0/nicisdi.key            |

**3** ターゲットサーバ上で eDirectory を開始します。

### SAS、LDAP、および SNMP サービスを設定する

Linux、Solaris、AIX および HP-UX では、コマンドラインに次のコマンドを入力することにより、下に示すサービスを 1 回の操作で設定できます。

**ndsconfig upgrade [-a 管理者 FDN]**

#### SAS

| プラットフォーム                | コマンドまたはツール                                 |
|-------------------------|--|
| NetWare                 | iManager を使用して SAS サービスオブジェクトおよび証明書を作成します。 |
| Windows                 | iManager を使用して SAS サービスオブジェクトおよび証明書を作成します。 |
| Linux、Solaris、AIX、HP-UX | ndsconfig -t ツリー名 -o サーバコンテキスト -m sas      |

#### LDAP

| プラットフォーム                | コマンドまたはツール   |
|-------------------------|--|
| NetWare                 | iManager を使用して LDAP サーバおよびグループオブジェクトを作成します。  |
| Windows                 | iManager を使用して LDAP サーバおよびグループオブジェクトを作成します。  |
| Linux、Solaris、AIX、HP-UX | ndsconfig -t ツリー名 -o サーバコンテキスト -m ldap<br>または<br>iManager を使用して LDAP サーバおよびグループオブジェクトを作成します。 |

#### SNMP

| プラットフォーム                | コマンドまたはツール  |
|-------------------------|---|
| NetWare                 | SNMPINST -c 管理者コンテキスト パスワード サーバDN   |
| Windows                 | rundll32 snmpinst, snmpinst -c createobj -a ユーザ FDN -p パスワード -h ホスト名または IP アドレス |
| Linux、Solaris、AIX、HP-UX | ndsconfig -t ツリー名 -o サーバコンテキスト -m snmp  |

## セキュリティ保護された iMonitor 操作の実現

iMonitor 環境へのアクセスをセキュリティ保護するには、次の保護手順を実行します。

1. ファイアウォールを使用して VPN アクセスを準備します。これは、Novell iManager および、アクセス制限が必要な他のすべての Web ベースのサービスの場合も同様です。
2. ファイアウォールが設置されているかどうかに関係なく、アクセスの種類を制限することによって、iMonitor はさらに DoS (Denial of Service) 攻撃から保護されます。

iMonitor は URL 要求を経由して受け取るデータを十分に確認しますが、あらゆる不正な入力を拒否できるとは保証できません。無効な URL を通じた DoS 攻撃の危険を減らすため、**iMonitor の環境設定ファイル**を通じて 3 つのレベルのアクセスが LockMask : オプションを使用して制御されます。

| アクセスレベル   | 説明  |
|-----------|---|
| 0         | iMonitor の URL 処理において事前の認証は不要です。この場合、[Public] 識別子の eDirectory 権利がすべての要求に適用され、iMonitor が表示する情報は [Public] ユーザの権利に限定されます。ただし、iMonitor に URL を送る際に認証が不要であるため、iMonitor は、不正な URL の送信による DoS 攻撃を受けやすくなる可能性があります。  |
| 1 (デフォルト) | iMonitor が URL を処理する前に、eDirectory 識別子としての認証が必要です。この場合、その識別子の eDirectory 権利はすべての要求に適用されるため、eDirectory 権利によって制限を受けます。DoS 攻撃を受ける危険性はレベル 0 と同様ですが、DoS 攻撃は実際にサーバに認証を受けたものでないという行かないことが異なります。認証が正常に実行されるまでは、すべての iMonitor の URL 要求への返答は [ログイン] ダイアログボックスで行われます。したがってこの段階では、設定された正当性を持たないユーザによる攻撃を通さないようにする必要があります。        |
| 2         | iMonitor が URL を処理する前に、iMonitor が認証しているサーバ上のスーパーバイザに相当する eDirectory 識別子としての認証が必要です。DoS 攻撃を受ける危険性はレベル 1 と同様ですが、DoS 攻撃を行うには実際にサーバのスーパーバイザとして認証される必要があります。認証が正常に実行されるまでは、すべての iMonitor の URL 要求への返答は [ログイン] ダイアログボックスで行われます。したがってこの状態に設定されているときには、iMonitor は認証されていないユーザおよびスーパーバイザとして認証されていないユーザからの攻撃を通さないようにする必要があります。 |

レベル 1 はデフォルトです。多くの管理者はツリー内のすべてのサーバにアクセスできるスーパーバイザ権を持っていませんが、管理しているサーバと通信するサーバ上の iMonitor サービスを使用する必要が生じる可能性があるためです。

注: iMonitor には Repair、トレースなど複数の機能があり、これらの機能にアクセスするには、LockMask の設定に関係なくスーパーバイザに相当する権利が必要です。

# 8

## Novell eDirectory ツリーのマージ

Novell® eDirectory™ マージユーティリティを使用すると、2つの Novell eDirectory ツリーをマージして、単一の eDirectory ツリーを作成できます。マージされるのは Tree オブジェクトだけです。コンテナオブジェクトとそのリーフオブジェクトは、マージ後のツリー上でもそれぞれ異なるオブジェクトとして存在します。

**ヒント:** リーフオブジェクトを移動する場合や、パーティションをマージする場合には、ConsoleOne® または Novell iManager を使用します。

マージする 2 つのツリーをそれぞれソースツリーおよびターゲットツリーといいます。1 つのツリーを別のツリーにマージする前に、ターゲットツリーにあるルートパーティションのレプリカを 1 つだけ残し、その他のすべてのレプリカを削除する必要があります。ターゲットツリーにルートパーティションのレプリカが 1 つしかない場合には、マージ処理を続行できます。マージ後は、ルートパーティションのレプリカが 2 つになります。1 つはターゲットツリー上にあったレプリカで、もう 1 つはマージ操作を実行したソースツリーのサーバ上にあったレプリカです。ルートパーティションのレプリカを追加する必要がある場合は、マージが完了した後に保存することができます。

マージ時にターゲットツリーサーバにルートパーティションのレプリカが複数ある場合、マスタレプリカを保持していないサーバで、外部参照オブジェクトの位置に関する問題が発生する可能性があります。外部参照オブジェクトは、サブオーディネートリファレンスのパーティションルートに含まれています。これは、パーティションの境界を表すルートパーティションのレプリカを持つ別のサーバに配置する必要があります。ソースツリーにあるルートパーティションの下位パーティションごとに、ターゲットツリーにあるサブオーディネートリファレンスのパーティションルートを持つ必要があります。エラーが生じた場合、同期ステータスに関する eDirectory エラーコード -605 が報告されます。この場合、DSRepair を使用して、エラーが発生したサーバのローカルデータベースを修復します。詳細については、[269 ページの「ローカルデータベースの修復の実行」](#)を参照してください。

DSMerge を実行しても、コンテナ内の eDirectory 名またはコンテキストは変わりません。オブジェクト権とプロパティ権はマージ後のツリーでも保持されます。

この章では、次のトピックについて説明します。

- ◆ [226 ページの「eDirectory ツリーのマージ」](#)
- ◆ [232 ページの「サーバツリーの結合」](#)
- ◆ [237 ページの「ツリー名の変更」](#)

## eDirectory ツリーのマージ

eDirectory ツリーをマージするには、Novell iManager のツリーのマージウィザードを使用します。このウィザードでは、2 つの eDirectory ツリーのルートをマージできます。マージされるのは Tree オブジェクトだけです。コンテナオブジェクトとそのリーフオブジェクトは、マージ後のツリー上でもそれぞれ異なるオブジェクトとして存在します。

マージする 2 つのツリーはそれぞれソースツリーおよびターゲットツリーといいます。ソースツリーのマージ先ツリーがターゲットツリーです。

DSMerge を実行しても、コンテナ内のオブジェクトの名前は変わりません。オブジェクト権とプロパティ権はマージ後のツリーでも保持されます。

- ◆ [226 ページの「前提条件」](#)
- ◆ [226 ページの「ターゲットツリーの要件」](#)
- ◆ [227 ページの「ソースツリーをターゲットツリーへマージする」](#)
- ◆ [227 ページの「パーティションの変化」](#)
- ◆ [228 ページの「ソースツリーとターゲットツリーを準備する」](#)
- ◆ [229 ページの「マージする前の時刻の同期」](#)
- ◆ [230 ページの「2 つのツリーのマージ」](#)
- ◆ [231 ページの「マージ後の作業」](#)

### 前提条件


- ❑ Novell eDirectory 8.8 がソースツリーの [Root] パーティションのマスタレプリカを含むサーバにインストールされている必要があります。
- ❑ 正しい機能を維持するには、ソースツリーの他のサーバを eDirectory 8.6 以降にアップグレードする必要があります。

### ターゲットツリーの要件

- ❑ Novell eDirectory 8.8 がターゲットツリーの [Root] パーティションのマスタレプリカを含むサーバにインストールされている必要があります。このサーバで他のパーティションの NDS<sup>®</sup> または eDirectory が実行されている場合は、マージ操作が正常に完了されません。
- ❑ 正しい機能を維持するには、ターゲットツリーの他のサーバを eDirectory 8.6 以降にアップグレードする必要があります。
- ❑ ソースツリーとターゲットツリーの両方で、Tree のサブオーディネートコンテナを同じ名前でも維持することはできません。2 つのツリーをマージする前に、一方のコンテナをリネームする必要があります。
- ❑ ソースツリーとターゲットツリーの両方にセキュリティオブジェクトがある場合は、ツリーをマージする前にどちらかを削除する必要があります。

## スキーマの要件

マージ操作を実行する前に、2 つのツリーのスキーマが正確に一致している必要があります。ツリーごとに [Root] パーティションのマスタレプリカを含むサーバで DSRepair を実行する必要があります。[リモートスキーマのインポート] オプションを使用して、各ツリーで他のツリーのスキーマがすべて認識されていることを確認します。

- 1 Novell iManager で、[役割およびタスク] ボタン  をクリックします。
- 2 [eDirectory の保守] > [スキーマの保守] の順にクリックします。
- 3 スキーマメンテナンス操作を実行するサーバを指定し、[次へ] をクリックします。
- 4 指定したサーバへの認証を行い、[次へ] をクリックします。
- 5 [リモートスキーマのインポート] > [次へ] の順にクリックします。
- 6 スキーマのインポート元のツリー名を指定します。
- 7 [開始] をクリックします。

このオプションは、ソースツリーとターゲットツリーの両方でスキーマの違いが報告されなくなるまで実行する必要があります。そうでないとマージ操作は成功しません。
- 8 スキーマメンテナンス操作から戻された情報とともに「完了」メッセージが表示されたら、[閉じる] をクリックして終了します。

## ソースツリーをターゲットツリーへマージする

ツリーをマージすると、ソースツリー内のサーバがターゲットツリーに組み込まれます。

ターゲットツリーの Tree オブジェクトがソースツリー内のオブジェクトの新しい Tree オブジェクトになり、ソースツリーにあるすべてのサーバのツリー名がターゲットツリーのツリー名に変わります。

ターゲットツリー内のサーバのツリー名はマージ後も変わりません。

ソースツリーの Tree オブジェクトの下位オブジェクトは、ターゲットツリーの Tree オブジェクトの下位オブジェクトになります。

## パーティションの変化

マージ実行時には、ソースツリーの Tree オブジェクトの下にあるオブジェクトが DSMerge によって複数のパーティションに分けられます。

続いて、ソースツリー内のサーバから、Tree パーティションのレプリカがマスタレプリカを除いてすべて削除されます。ソースツリーのマスタレプリカを保持していたサーバには、ターゲットツリーの Tree パーティションのレプリカが渡されます。

図 33 および図 34 は、2つのツリーをマージした場合のパーティションの変化を示します。

図 33 マージ前の eDirectory ツリー

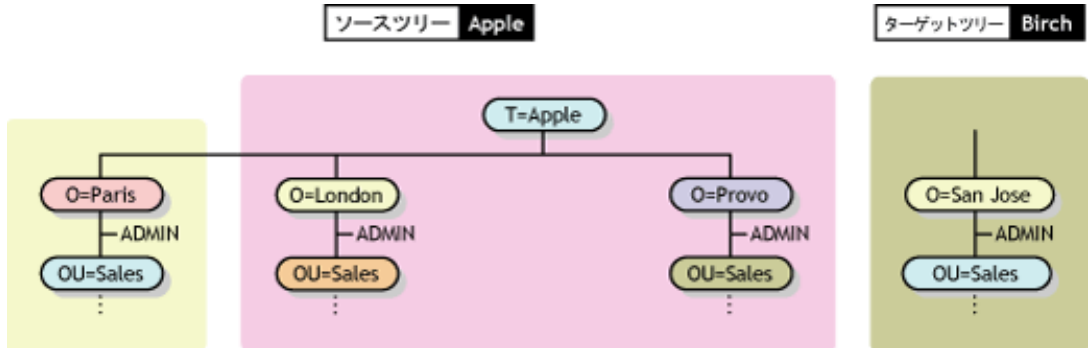
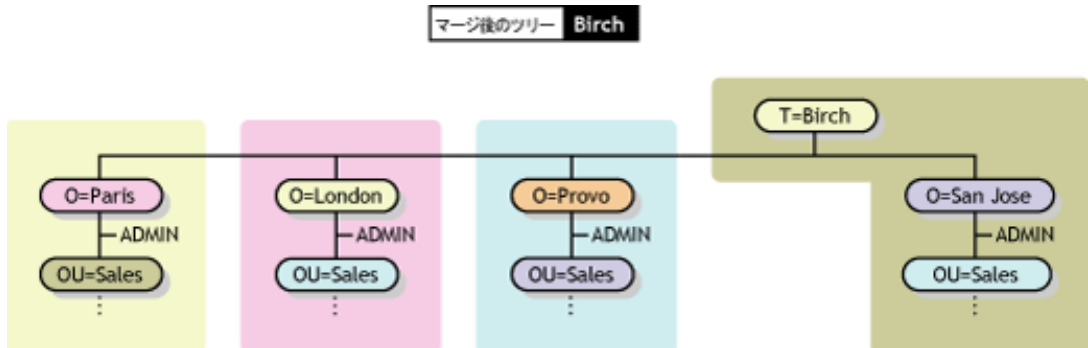


図 34 マージ後の eDirectory ツリー



## ソースツリーとターゲットツリーを準備する

マージ操作を開始する前に、そのマージ操作の影響を受けるすべてのサーバが安定した状態で同期していることを確認する必要があります。次の表で、マージ対象のソースツリーとターゲットツリーの準備に関する前提条件について説明します。

| 前提条件  | 必要な措置  |
|---|--|
| ソースツリーまたはターゲットツリーのツリーパーティションのレプリカを保持しているすべてのサーバ上で WANMAN がオフになっている。 | WANMAN ポリシーを調べて、WAN 通信の制約によるマージ操作への支障がないことを確認します。必要があれば、マージ操作を開始する前に WANMAN をオフにします。 |
| ソースツリーのツリーオブジェクトに別名またはリーフオブジェクトが存在しない。                              | ソースツリーの Tree オブジェクトに存在する別名またはリーフオブジェクトを削除します。  |



| 前提条件   | 必要な措置  |
|--|--|
| ソースツリーおよびターゲットツリーに同じ名前がない。                               | 同じ名前がある場合には、ソースツリーまたはターゲットツリーのオブジェクト名を変更します。コンテナオブジェクト名を変更したくない場合は、コンテナの1つから同じツリー内の別のコンテナにオブジェクトを移動し、空になったコンテナを DSMerge 実行前に削除します。詳細については、 <a href="#">95 ページの第 3 章「オブジェクトの管理」</a> を参照してください。<br><br>Tree オブジェクトの直下でないコンテナオブジェクトの場合は、両ツリーに同じコンテナオブジェクトがあってもかまいません。 |
| ソースツリー上にログイン接続が存在しない。                                    | ソースツリーのすべての接続を終了します。   |
| ソースツリーの eDirectory およびターゲットツリーの eDirectory のバージョンが同じである。 | ルートパーティションのレプリカを持つ、eDirectory 8.8 でないすべてのサーバをアップグレードします。   |
| ターゲットツリー内のルートレプリカのコピーが1つである。                             | ターゲットツリー上の、マスタレプリカを除いたすべてのレプリカを削除します。  |
| ソースツリーおよびターゲットツリーのスキーマが同じである。                            | DSMerge を実行します。出力されるレポートを見てスキーマに問題があることがわかった場合は、DSRepair を使用してスキーマを一致させます (詳細については、 <a href="#">280 ページの「リモートスキーマをインポートする」</a> を参照してください)。DSMerge を再実行します。   |
| 単一のツリーだけが、ツリーのルートの下位にセキュリティコンテナを保持できる。                   | ソースツリーおよびターゲットツリーの両方がセキュリティコンテナを保持している場合は、 <a href="#">569 ページの付録 A「NMAS の注意事項」</a> で説明されている手順に従って、一方のコンテナを削除します。  |

マージ操作は単独のトランザクションなので、実行中に停電やハードウェアエラーが発生しても重大な障害にはつながりません。ただし、DSMerge を実行する前に、あらかじめ eDirectory データベースの通常のバックアップをとっておくことをお勧めします。詳細については、[389 ページの第 14 章「Novell eDirectory のバックアップと復元」](#)を参照してください。

## マージする前の時刻の同期

**重要:** 時刻同期の正確な環境設定は複雑な作業です。ツリーをマージする前に、両ツリーを同期させるのに十分な時間があることを確認します。

時刻の異なる複数のタイムソースが使用されていたり、ツリー内のサーバの中に時刻が同期されていないものがあると、Novell eDirectory は正しく機能しません。

マージを実行する前に、両ツリーにあるすべてのサーバの時刻が同期されていること、およびこれらのサーバがタイムソースとして同じタイムサーバを使用していることを確認します。ただし、ターゲットツリーの時刻は 5 分以内であればソースツリーの時刻より進んでいてもかまいません。

一般に、1つのツリー上に存在できるタイムサーバは、リファレンスタイムサーバまたはシングルタイムサーバのどちらか1つだけです。同様に、マージ後のツリー上に存在できるタイムサーバも、リファレンスタイムサーバまたはシングルタイムサーバのどちらか1つだけです。

マージする両ツリーのそれぞれにリファレンスタイムサーバまたはシングルタイムサーバがある場合は、どちらかのツリーの設定をもう一方のツリーにあるリファレンスタイムサーバまたはシングルタイムサーバに変更して、マージ後のツリー上でリファレンスタイムサーバまたはシングルタイムサーバが1つだけになるようにします。

タイムサーバの種類の詳細については、『*Network Time Management 管理ガイド*』([http://www.novell.com/documentation/lg/nw65/time\\_enu/data/hl5k6r0y.html](http://www.novell.com/documentation/lg/nw65/time_enu/data/hl5k6r0y.html))を参照してください。

## 2つのツリーのマージ

すべてのメニューオプションの機能を使用できるようにするには、Tree パーティションのマスタレプリカが格納されているサーバ上で DSMerge を実行します。

マスタレプリカが格納されている場所が不明な場合は、マスタレプリカを必要とする操作を実行すると、正確なサーバ名とともに表示されます。

マージ操作を実行するには、次のどちらかの方法を使用します。

- ◆ Novell iManager
- ◆ eMBox コマンドラインクライアント

詳細については、238 ページの「**eMBox クライアントを使用したツリーのマージ**」を参照してください。

大きなツリーをマージするときは、Tree オブジェクト直下にあるオブジェクトの数が少ないほうのツリーをソースツリーとして指定したほうが、処理速度が大幅に速くなります。Tree オブジェクトの直下にあるオブジェクトすべてに対して新しいパーティションが作成されるため、この方法をとると、マージ実行時に分割されるパーティションの数が少なくすむためです。

ソースツリーの名前はマージ後には存在なくなります。したがって、場合によっては、クライアントワークステーションの環境設定を変更する必要があります。Novell Client™ for DOS/Windows を使用している場合は、net.cfg ファイルの優先ツリーステートメントおよび優先サーバステートメントを確認します。Novell Client for Windows NT/2000 または Novell Client for Windows 95/98 を使用している場合は、クライアントのプロパティページにある優先ツリーステートメントおよび優先サーバステートメントを確認します。

優先サーバが使用されている場合は、ツリーのマージやツリー名の変更を行っても、そのクライアントは名前によってサーバにログインした状態のままなので操作による影響はクライアント側にはありません。優先ツリーが使用されている場合は、ツリーのマージやツリー名の変更を行うと、元のツリー名はなくなります。マージを行った後にはターゲットツリーの名前だけが残ります。優先ツリーの名前を新しいツリー名に変更します。

**ヒント:** ターゲットツリーの名前はマージの結果作成されるツリーの名前としてそのまま残るので、アップデートする必要のあるクライアントワークステーションの数を少なくするには、クライアントワークステーションの数が多い方のツリーをターゲットツリーとして指定します。または、マージ操作の後でツリー名を変更して、最終的なツリー名が接続されているクライアントワークステーションの数が多い方のツリーに一致するようにします。詳細については、237 ページの「**ツリー名の変更**」を参照してください。


次の前提条件の一覧を使用して、マージ操作の準備ができていないか確認します。

- iManager によるソースツリーのサーバへのアクセス権があること
- マージする両ツリーの Tree オブジェクトに対するスーパーバイザオブジェクト権を持つ管理者オブジェクトの名前とパスワードがわかっていること
- 2つのツリーの eDirectory データベースがバックアップされていること
- 両ツリー内のすべてのサーバが同期されていて、同じタイムソースを使用していること
- (オプション) ツリー内のサーバがすべて動作可能であること (動作不能状態のサーバは動作可能になった時点で自動的に更新されます)
- **228 ページの「ソースツリーとターゲットツリーを準備する」**に表示された前提条件を確認すること

マージプロセス自体には2、3分しかかかりませんが、次のような場合は、付随的な作業が必要になるため、マージ操作が完了するまでに要する時間が長くなります。

- ◆ Tree オブジェクトの下に多数のオブジェクトがあり、パーティションに分ける必要がある
- ◆ ソースツリーに多数のサーバがあり、ソースツリーのツリー名を変更する必要がある

2つのツリーをマージするには、次を実行します。

- 1** Novell iManager で、[役割およびタスク] ボタン  をクリックします。
- 2** [eDirectory の保守] > [ツリーのマージ] の順にクリックします。
- 3** ソースツリーとしてマージを実行するサーバを指定し、[次へ] をクリックします。
- 4** サーバへの認証を行ってから、[次へ] をクリックします。
- 5** ソースツリーの管理者ユーザ名とパスワードを指定します。
- 6** ターゲットツリー名、管理者ユーザ名、およびパスワードを指定して [開始] をクリックします。  
ツリーのマージウィザードのステータスウィンドウが表示され、マージの進行状況が表示されます。
- 7** マージプロセスから戻された情報とともに「完了」メッセージが表示されたら、[閉じる] をクリックして終了します。

## マージ後の作業

2つのツリーをマージした後は、状況に応じて次の手順を行ってください。

- 1** すべてのツリー名が正しく変更されたことを確認します。
- 2** マージ操作によって作成された新しいパーティションを確認します。  
新しいツリーに小さいパーティションが多数存在する場合や、関連する情報が格納されたパーティションが複数存在する場合は、これらのパーティションをマージすることもできます。詳細については、**137 ページの「パーティションのマージ」**を参照してください。
- 3** DSMerge を実行する前にサーバを NetWare 5 にアップグレードしなかった場合は、NetWare 5 以外を実行しているすべてのサーバに新しいレプリカをコピーします。

**4** DSMerge 実行前にリーフオブジェクトや別名をツリーから削除した場合は、ツリーにそれらのリーフオブジェクトや別名を再作成します。

**5** eDirectory ツリーのパーティション構成を調べます。

マージ後のツリー内でのレプリカの位置はソースツリー内での位置と異なる場合があります。パーティション構成の変更や検査は慎重に行ってください。

**6** クライアントワークステーションの環境設定を更新します。

Novell Client for DOS/Windows を使用している場合は、net.cfg ファイルの優先ツリーステートメントおよび優先サーバステートメントを確認します。Novell Client for Windows NT/2000 または Novell Client for Windows 95/98 を使用している場合は、クライアントのプロパティページの優先ツリーステートメントおよび優先サーバステートメントを確認するか、またはターゲットツリーの名前を変更します。

優先サーバが使用されている場合は、ツリーのマージやツリー名の変更を行っても、そのクライアントは名前によってサーバにログインした状態のままなので操作による影響はクライアント側にはありません。優先ツリーが使用されている場合は、ツリーのマージやツリー名の変更を行うと、元のツリー名はなくなります。マージを行った後にはターゲットツリーの名前だけが残ります。優先ツリーの名前を新しいツリー名に変更します。

ソースツリーの Tree オブジェクトの ACL (アクセス制御リスト) は保持されます。したがって、この Tree オブジェクトに対してソースツリーの管理者ユーザが持つ権利は、操作後も有効です。

マージ後も、両ツリーの管理者ユーザは存在したままで、それぞれのコンテナオブジェクトによって固有のものとして識別されます。

セキュリティ上必要であれば、2つの管理者ユーザオブジェクトの一方を削除するか、両オブジェクトの権利を制限することもできます。

## サーバツリーの結合

[ツリーの結合] オプションを使用すると、単一サーバソースツリーの Tree オブジェクトを、ターゲットツリーにある指定のコンテナに結合できます。結合が完了すると、ソースツリーのツリー名は、ターゲットツリーのツリー名になります。

結合操作中に、DSMerge によってソースツリーの Tree オブジェクトのオブジェクトクラスがドメインに変更され、新しいパーティションを作成します。新しいドメインオブジェクトは、新しいパーティションのパーティションルートになります。ソースツリーの Tree オブジェクトの下位オブジェクトはすべて、ドメインオブジェクトの下に置かれます。

ターゲットツリーの管理者は、作成されたツリーのルートコンテナの権利を持つため、ソースツリーの結合されたルートの権利を持つこととなります。

**注:** 権利継承が再計算されて有効になるには、数時間かかる可能性があります。この時間は、ツリーの複雑さ、サイズ、パーティション数によって変化します。

ソースツリーの管理者は、新しく作成されたドメインオブジェクト内でのみ権利を所有します。



233 ページの  と  に、ツリーを特定のコンテナに結合した場合の変化を示します。

図 35 結合前の eDirectory ツリー

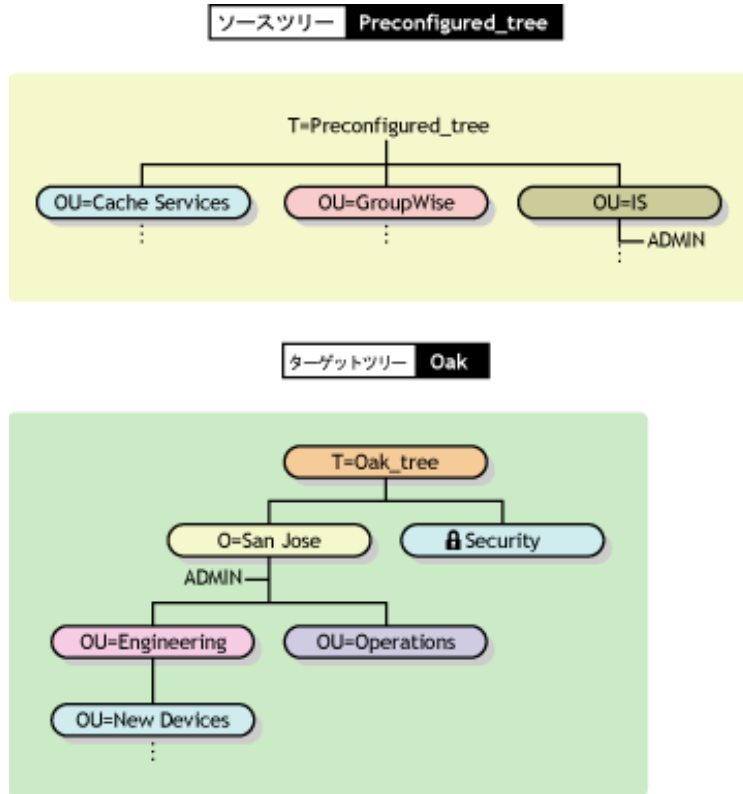
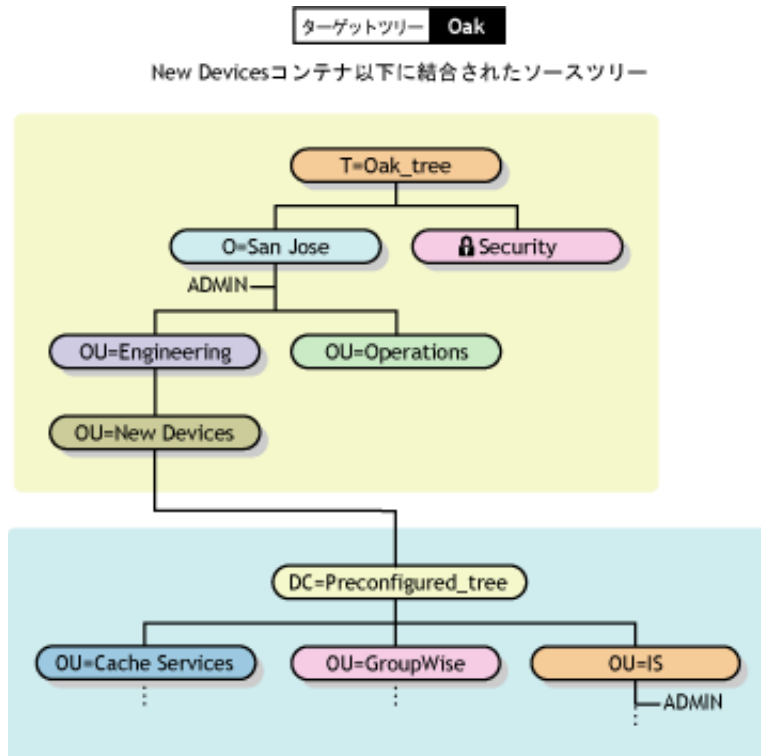


図 36 結合後の eDirectory ツリー



このセクションでは、次の情報について説明します。

- ◆ 234 ページの「コンテキスト名の変更について」
- ◆ 234 ページの「ソースツリーとターゲットツリーを準備する」
- ◆ 236 ページの「結合操作における包含要件」
- ◆ 237 ページの「ソースツリーとターゲットツリーを結合する」

## コンテキスト名の変更について

ソースツリーをターゲットツリーのコンテナに結合すると、ソースツリー内にあるオブジェクトの識別名の後ろに、ソースツリー名と、ソースツリーをマージしたターゲットツリーコンテナの識別名がこの順で追加されます。相対識別名は変わりません。

たとえば、区切り文字としてドットを使用している場合、ソースツリー `Preconfigured_tree` 内にあるオブジェクト `Admin` のタイプ付きの名前は次のようになります。

```
CN=Admin.OU=IS.T=Preconfigured_tree
```

`Preconfigured_tree` を `Oak_tree` の `New Devices` コンテナにマージした後は、`Admin` のタイプ付きの名前は次のようになります。

```
CN=Admin.OU=IS.DC=Preconfigured_tree.OU=Newdevices.  
OU=Engineering.O=Sanjose.T=Oak_tree.
```

**注：**識別名の最大長は 256 文字です。この制限は、1 つのツリーのルートをターゲットツリーの下端近くにあるコンテナに結合する場合に特に重要です。

`Oak_tree` の後にある最後のドット (`Oak_tree.`) は、この識別名を構成する最後の要素がツリー名であることを示しています。このドットを省略する場合は、ツリー名も省略します。

## ソースツリーとターゲットツリーを準備する

結合操作を開始する前に、その結合操作の影響を受けるすべてのサーバが安定した状態であることを確認する必要があります。次の表では、結合前のソースツリーとターゲットツリーの準備に関する前提条件について説明します。

| 前提条件  | 必要な措置  |
|---|--|
| ソースツリーまたはターゲットツリーのツリーパーティションのレプリカを保持しているすべてのサーバ上で WANMAN がオフになっている。 | WANMAN ポリシーを調べて、WAN 通信の制約によるマージ操作への支障がないことを確認します。必要があれば、マージ操作を開始する前に WANMAN をオフにします。 |
| ソースツリー内のサーバが 1 つである。  | ソースツリーから、1 つだけ残してすべてのサーバを削除します。  |
| ソースツリーのツリーオブジェクトに別名またはリーフオブジェクトが存在しない。                              | ソースツリーの Tree オブジェクトに存在する別名またはリーフオブジェクトを削除します。  |

| 前提条件  | 必要な措置  |
|---|--|
| 結合コンテナ内に同じ名前がない。                                      | <p>同じ名前がある場合は、ターゲットツリーの結合コンテナ内のオブジェクトまたはソースツリー内のオブジェクト名を変更します。</p> <p>オブジェクト名を変更したくない場合は、コンテナの1つから同じツリー内の別のコンテナにオブジェクトを移動し、空になったコンテナを DSMerge 実行前に削除します。詳細については、<a href="#">95 ページの第 3 章「オブジェクトの管理」</a>を参照してください。</p> <p>同じペアレントオブジェクトの直下でないコンテナオブジェクトの場合は、両ツリーに同じコンテナオブジェクトがあってもかまいません。オブジェクトは、直接のコンテナオブジェクトによって識別されます。</p> |
| ソースツリーおよびターゲットツリーの eDirectory バージョンが 8.51 SP2a 以降である。 | DSMerge は、eDirectory の適切なバージョンを検索します。許容できるバージョンが検出されない場合、DSMerge はエラーを返します。eDirectory の最新バージョンは、 <a href="http://download.novell.com">Novell Download ページ (http://download.novell.com)</a> から取得できます。   |
| ターゲットツリーを結合するコンテナがレプリカを持たないパーティション（単一サーバパーティション）にある。  | <p>ターゲットコンテナに複数のレプリカがある場合は、次のうち1つを実行します。</p> <ul style="list-style-type: none"> <li>◆ このコンテナに関連付けられたパーティションをマスタレプリカにし、その他のレプリカを削除します。</li> <li>◆ または、ターゲットツリーの結合コンテナを別のパーティションとして切り離し、レプリカを削除します。</li> </ul> <p>結合が完了した後は、パーティションの関連付けを再構築できます。</p>  |
| ターゲットコンテナを保持するサーバがルートパーティションのレプリカも保持している。             | <p>サーバがルートのレプリカを保持していない場合、ディレクトリはターゲットツリーの管理権を確認できないので、結合は失敗し、エラー「-672 アクセス権なし」が表示されます。</p> <p>iManager を使用してルートのレプリカを追加します。詳細については、<a href="#">140 ページの「レプリカを追加する」</a>を参照してください。</p>  |
| ソースツリーおよびターゲットツリーのスキーマが同じである。                         | <p>DSMerge で [結合] オプションを実行します。出力されるレポートからスキーマに問題があることがわかった場合は、ターゲットツリー上で DSRepair を実行してソースツリーからスキーマをインポートします。</p> <p>結合操作によって、自動的にスキーマがターゲットツリーからソースツリーにインポートされます。</p> <p>DSMerge を再実行します。</p>   |
| 単一のツリーだけが、ツリーのルートの下位にセキュリティコンテナを保持できる。                | ソースツリーおよびターゲットツリーの両方がセキュリティコンテナを保持している場合、 <a href="#">569 ページの付録 A「NMAS の注意事項」</a> で説明されている手順に従って、一方のコンテナを削除します。   |



| 前提条件                       | 必要な措置   |
|----------------------------|---|
| ソースツリーのタイムリファレンスが再設定されている。 | <p>ソースツリーは、ターゲットツリーのサーバからタイムソースを取得するように、セカンダリサーバとして設定される必要があります。</p> <p>Timesync を再設定するには、『<a href="http://www.novell.com/documentation/lg/nw65/time_enu/data/abzqzx2.html">Network Time Management 管理ガイド</a>』の「<a href="http://www.novell.com/documentation/lg/nw65/time_enu/data/abzqzx2.html">Configuring Timesync on Servers</a>」(<a href="http://www.novell.com/documentation/lg/nw65/time_enu/data/abzqzx2.html">http://www.novell.com/documentation/lg/nw65/time_enu/data/abzqzx2.html</a>) を参照してください。</p> |


## 結合操作における包含要件

ソースツリーをターゲットツリーのコンテナに結合するには、ターゲットツリーのコンテナでソースツリーの受け入れ準備を整えておく必要があります。ターゲットツリーのコンテナは、クラスドメインのオブジェクトを包含できなければなりません。包含に問題があると、結合操作中に「-611 不正な包含ルールです」というエラーが発生します。

次の表の情報を使用して、DSRepair を実行して包含リストを変更する必要があるかどうかを判断します。

|                 |   |
|-----------------|---|
| ターゲットツリーのコンテナ要件 | <p>ターゲットツリーのコンテナオブジェクトが、包含リスト内のドメインオブジェクトを包含していること。</p> <p>iMonitor で [スキーマ] を使用すると、この状況をチェックできます。包含リストにドメインが包含されていない場合、DSRepair を実行してスキーマを拡張します。</p>   |
| ソースツリーの要件       | <p>結合操作によって、ソースツリーのルートがクラスツリールートからクラスドメインに変更されます。Tree の下位オブジェクトはすべて、スキーマルールに従い、クラスドメインに適切に包含されている必要があります。</p> <p>iMonitor で [スキーマ] を使用すると、この状況をチェックできます。包含リストにドメインが包含されていない場合、DSRepair を実行してスキーマを拡張します。</p> |


包含要件が満たされていない場合は、DSRepair を実行してスキーマを修正します。

- 1 Novell iManager で、[役割およびタスク] ボタン  をクリックします。
- 2 [eDirectory の保守] > [スキーマの保守] の順にクリックします。
- 3 操作を実行するサーバを指定し、[次へ] をクリックします。
- 4 ユーザ名、パスワード、および操作を実行するサーバのコンテキストを指定し、[次へ] をクリックします。
- 5 [オプションスキーマ拡張機能] をクリックし、[開始] をクリックします。
- 6 表示される指示に従って、操作を完了します。



## ソースツリーとターゲットツリーを結合する

前提条件を満たしていることを確認し、DSMerge を使用して結合を実行します。

- 1 Novell iManager で、[役割およびタスク] ボタン  をクリックします。
- 2 [eDirectory の保守] > [ツリーの結合] の順にクリックします。
- 3 ソースツリーとして結合を実行するサーバを指定し、[次へ] をクリックします。
- 4 サーバへの認証を行ってから、[次へ] をクリックします。
- 5 ソースツリーの管理者名とパスワード、ターゲットツリー名、およびターゲットツリーの管理者名とパスワードを指定します。
- 6 [開始] をクリックします。

ツリーの結合ウィザードのステータスウィンドウが表示され、結合の進行状況が表示されます。結合処理から戻された情報とともに、最後に「完了」メッセージが最後に表示されます。

- 7 [閉じる] をクリックして終了します。

## ツリー名の変更

マージする 2 つのツリーの名前が同じ場合は、どちらかの名前を変更する必要があります。

ここで名前を変更できるのはソースツリーだけです。ターゲットツリーの名前を変更するには、ターゲットツリー上のいずれかのサーバで Novell iManager の [ツリー名の変更ウィザード] を実行する必要があります。

ツリー名を変更しても、バインダリコンテキストは自動的に変更されません。autoexec.ncf ファイルで設定されたバインダリコンテキストセットにもツリー名 (例: SET Bindery Context = O=n. テストツリー名) が含まれるため、ツリー名が最近変更されたサーバでは、ツリー名が変更される前のコンテキストは使用されません。

したがって、ツリー名を変更した場合、クライアントワークステーションの環境設定の変更が必要になる可能性があります。Novell Client for DOS/Windows を使用している場合は、net.cfg ファイルの優先ツリーステートメントおよび優先サーバステートメントを確認します。Novell Client for Windows NT/2000 または Novell Client for Windows 95/98 を使用している場合は、クライアントのプロパティページにある優先ツリーステートメントおよび優先サーバステートメントを確認します。

優先サーバが使用されている場合は、ツリーのマージやツリー名の変更を行っても、そのクライアントは名前によってサーバにログインした状態のままなので操作による影響はクライアント側にはありません。優先ツリーが使用されている場合は、ツリーのマージやツリー名の変更を行うと、元のツリー名はなくなります。マージを行った後にはターゲットツリーの名前だけが残ります。優先ツリーの名前を新しいツリー名に変更します。

2 つのツリーをマージする場合、ターゲットツリーの名前はマージの結果作成されるツリーの名前としてそのまま残るので、アップデートする必要があるクライアントワークステーションの数を少なくするには、クライアントワークステーションの数が多い方のツリーをターゲットツリーとして指定します。


または、マージの後でツリー名を変更して、最終的なツリー名がクライアントワークステーションの数が多い方のツリーに一致するようにすることもできます。

マージ後のツリーの名前は、元のソースツリーの名前に変更することもできます。その場合は、ターゲットツリーにあるクライアントワークステーションの `net.cfg` ファイルを更新する必要があります。

次の前提条件の一覧を使用して、リネーム操作の準備ができていないか確認します。

- ❑ ソースツリー上のサーバコンソールへのアクセス権があること、またはこのサーバとの RCONSOLE セッションが確立済みであること
- ❑ ソースツリーの Tree オブジェクトに対するスーパーバイザオブジェクト権があること
- ❑ (オプション) ツリー内のサーバがすべて動作可能であること (動作不能状態のサーバは動作可能になった時点で自動的に更新されます)

ツリー名を変更するには、次を実行します。

- 1 Novell iManager で、[役割およびタスク] ボタン  をクリックします。
- 2 [eDirectory の保守] > [ツリー名の変更] の順にクリックします。
- 3 ツリー名の変更ウィザードを実行するサーバ (ターゲットツリー内のサーバ) を指定し、[次へ] をクリックします。
- 4 サーバへの認証を行ってから、[次へ] をクリックします。
- 5 新しいツリー名、管理者ユーザ名、およびパスワードを指定します。
- 6 [開始] をクリックします。

ツリー名の変更ウィザードのステータスウィンドウが表示され、リネーム処理の進行状況が表示されます。

- 7 リネーム処理から戻された情報とともに「完了」メッセージが表示されたら、[閉じる] をクリックして終了します。

## eMBox クライアントを使用したツリーのマージ

eMBox (eDirectory Management Toolbox) クライアントはコマンドライン Java クライアントで、これを使用すると DSMerge にリモートアクセスできます。 `emboxclient.jar` ファイルは、eDirectory の一部としてサーバにインストールされます。JVM をインストールしていれば、どのコンピュータでも実行できます。eMBox クライアントの詳細については、555 ページの「[eMBox コマンドラインクライアントの使用](#)」を参照してください。

## DSMerge eMTool を使用する

- 1 コマンドラインで次のように入力して、対話式モードで eMBox クライアントを実行します。

```
java -cp ファイルのパス/emboxclient.jar embox -i
```

(クラスパスにすでに `emboxclient.jar` `file` が設定されている場合、「`java embox -i`」と入力するだけです。)

eMBox Client のプロンプトが次のように表示されます。

```
eMBox Client>
```

- 2 DSMerge を実行する (ソースツリーになる) サーバにログインするには、次のコマンドを入力します。

```
login -s サーバの名前または IP アドレス -p ポート番号  
-u ユーザ名 . コンテキスト -w パスワード -n
```

ポート番号は通常 80 または 8028 です。ただし、すでにそのポートを使用している Web サーバが存在する場合は異なります。-n オプションを使用すると、非セキュア接続を開始します。

eMBox クライアントはログインが成功したかどうかを表示します。

- 3 次の構文を使用してマージコマンドを入力します。

```
dsmerge. タスク オプション
```

例 :

「dsmerge.m -uadmin -ptest -TApple -Uadmin -Ptest」は、ターゲットツリー「Apple」を、現在ログインしているソースツリーにマージします。ターゲットツリーのユーザ名は「Admin」、ユーザパスワードは「test」です。また、ソースツリーのユーザ名も「Admin」、ユーザパスワードは「test」です。

「dsmerge.g -uadmin -ptest -TOrange -Uadmin -Ptest -CFruit」は、現在ログインしているソースツリーをターゲットツリー「Orange」内の「Fruit」コンテナに結合します。ソースツリーのユーザ名は「Admin」、ユーザパスワードは「test」です。また、ターゲットツリーのユーザ名も「Admin」、ユーザパスワードは「test」です。

各スイッチの間にはスペースが必要です。スイッチの順序は重要ではありません。

eMBox クライアントは DSMerge 操作が成功したかどうかを表示します。

DSMerge eMTool オプションの詳細については、[239 ページの「DSMerge eMTool オプション」](#)を参照してください。

- 4 eMBox クライアントからログアウトするには、次のコマンドを入力します。

```
logout
```

- 5 eMBox クライアントを終了するには、次のコマンドを入力します。

```
exit
```

## DSMerge eMTool オプション

次の表に、DSMerge eMTool オプションを示します。eMBox クライアントで list -tdsmerge コマンドを使用して、DSMerge オプションの詳細を表示することもできます。詳細については、[559 ページの「eMTool とそのサービスを表示する」](#)を参照してください。

| マージ操作                    | eMBox クライアントのコマンド  |
|--------------------------|--|
| ツリーの名前が変更できるかどうかチェックする   | dsmerge.pr -u ユーザ -p ユーザパスワード -n 新しいツリー名   |
| ツリー名を変更する                | dsmerge.r -u ユーザ -p ユーザパスワード -n 新しいツリー名  |
| 2 つのツリーがマージできるかどうかチェックする | dsmerge.pm -u ソースツリーのユーザ<br>-p ソースツリーのユーザパスワード -T ターゲットツリーの名前<br>-U ターゲットツリーのユーザ -P ターゲットツリーのパスワード |

| マージ操作                             | eMBox クライアントのコマンド  |
|-----------------------------------|--|
| 2つのツリーをマージする                      | <pre>dsmerge.m -u ソースツリーのユーザ -p ソースツリーのユーザパスワード -T ターゲットツリーの名前 -U ターゲットツリーのユーザ -P ターゲットツリーのパスワード</pre>                         |
| ソースツリーがターゲットツリーのコンテナに結合できるかチェックする | <pre>dsmerge.pg -u Source_tree_user -p ソースツリーのユーザパスワード -T ターゲットツリーの名前 -U ターゲットツリーのユーザ -P ターゲットツリーのパスワード -C ターゲットツリーのコンテナ</pre> |
| ソースツリーをターゲットツリーのコンテナに結合する         | <pre>dsmerge.g -u ソースツリーのユーザ -p ソースツリーのユーザパスワード -T ターゲットツリーの名前 -U ターゲットツリーのユーザ -P ターゲットツリーのパスワード -C ターゲットツリーのコンテナ</pre>        |
| 実行中の DSMerge 操作をキャンセルする           | cancel   |

# 9

## eDirectory のデータを暗号化する

Novell® eDirectory™ 8.8 以降では、特定のデータをディスクに保存したり、2 台以上の eDirectory 8.8 サーバ間でデータを転送する場合に、データを暗号化できます。そのため、機密データのセキュリティを強化できます。

データの暗号化の重要性と暗号化のシナリオについては、『*Novell eDirectory 8.8 What's New Guide*』(<http://www.novell.com/documentation/beta/edir88/index.html>) を参照してください。

次のものを暗号化することによって、データを保護できます。

- ◆ 属性：ディスクに格納されている機密データを保護する場合。  
[241 ページの「暗号化属性」](#) を参照してください。
- ◆ 複製：eDirectory 8.8 サーバ間の複製の実行中に機密データを保護する場合。  
[250 ページの「暗号化レプリケーション」](#)

### 暗号化属性

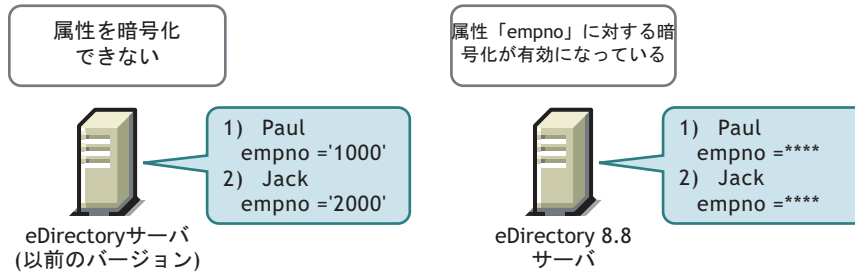
eDirectory 8.8 以降では、データがディスクに格納されている間は属性を暗号化してデータを保護できます。暗号化属性はサーバ固有の機能です。

属性を暗号化すると、属性値がエンコードされます。たとえば、DIB に保存されている属性 empno を暗号化したとします。empno=1000 である場合、属性値 (1000) はクリアテキスト形式ではディスクに保存されません。この暗号化された値は、セキュリティ保護されたチャネルからディレクトリにアクセスした場合にのみ読み取ることができます。

方式内のすべての属性に対して暗号化を有効にすることができます。ただし、共通名 (CN) 属性に対してではなく、重要なデータに対してのみ暗号化を有効にすることをお勧めします。暗号化する属性の決定については、[261 ページの「データを暗号化するときデータの完全な安全性を確保する」](#) を参照してください。

Public およびサーバが読み込める暗号化属性へのアクセスに制限はありません。つまり、クライアントはクリアテキストを使用してこれらの属性にアクセスすることができます。ユーザはこれらの暗号化用の属性に DIB レベルでマークすることができます。

図 37 暗号化属性



eDirectory 内のデータは次の方法で保存できます。

- ◆ DIB (Data Information Base) またはデータベースに保存
- ◆ バックアップデータとして保存
- ◆ LDIF ファイル

属性を暗号化するには、暗号化属性ポリシーを作成してサーバに適用します。

属性を暗号化するには、iManager で次の操作を実行します。

**1** 暗号化属性ポリシーを作成して定義します。

**1a** 暗号化する属性を選択します。

**1b** 属性の暗号化方式を選択します。

詳細については、244 ページの「暗号化属性ポリシーを作成して定義する」を参照してください。

**2** サーバに暗号化属性ポリシーを適用します。

詳細については、244 ページの「暗号化属性ポリシーを適用する」を参照してください。

LDAP を使用して属性を暗号化することもできます。詳細については、245 ページの「LDAP を使用して暗号化属性ポリシーを管理する」を参照してください。

ベストプラクティスとして、次の操作を行うことをお勧めします。

- ◆ 暗号化する属性のうち、重要な属性のみをマークします。暗号化する属性すべて (パブリックやサーバが読み込める属性など) にマークはしないでください。
- ◆ 暗号化する属性をマークする場合は、強力な暗号化アルゴリズムである AES を使用してください。

このセクションでは、次の情報について説明します。

- ◆ 243 ページの「暗号化方式を使用する」
- ◆ 247 ページの「暗号化属性にアクセスする」
- ◆ 248 ページの「暗号化属性を表示する」
- ◆ 243 ページの「暗号化属性ポリシーを管理する」
- ◆ 249 ページの「暗号化属性に移行する」

## 暗号化方式を使用する

eDirectory 8.8 では、属性のセキュリティを確保するために、次の暗号化方式がサポートされています。

- ◆ AES (Advanced Encryption Standard)
- ◆ トリプル DES
- ◆ DES (Data Encryption Standard)

1つの暗号化属性ポリシーに含まれる各属性に対して、個別に暗号化方式を選択することもできます。たとえば、EP1 という暗号化属性ポリシーに含まれる属性 `cubeno` に対しては暗号化方式として AES を選択し、属性 `empno` に対してはトリプル DES を選択することができます。詳細については、[244 ページの「暗号化属性ポリシーを作成して定義する」](#)を参照してください。

属性の暗号化方式を変更するには、暗号化属性ポリシーを編集します。すでに暗号化されている属性を復号化することもできます。詳細については、[244 ページの「暗号化属性ポリシーを編集する」](#)を参照してください。

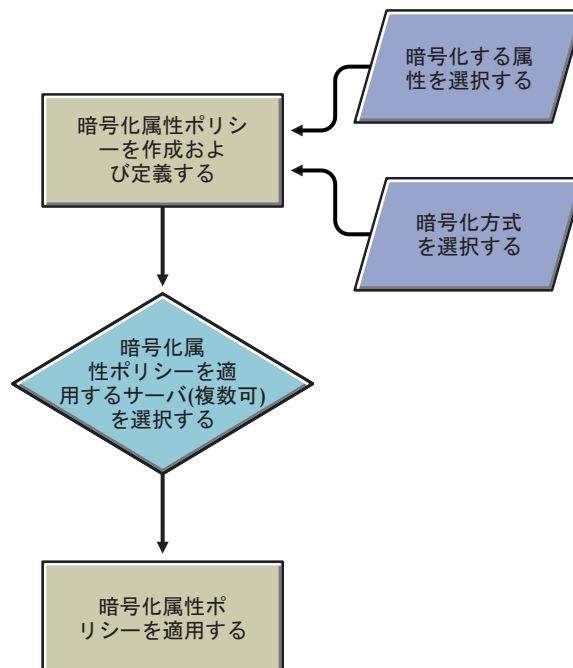
レプリカリング内の各サーバに対して、個別に暗号化方式を選択することもできます。たとえば、属性を暗号化する際に、Server1 では AES を使用し、Server2 ではトリプル DES を使用し、Server3 では暗号化方式を使用しないというような設定が可能です。

## 暗号化属性ポリシーを管理する

ポリシーを作成して定義し、サーバに適用することで、属性の暗号化を管理できます。

暗号化属性ポリシーを定義するには、暗号化する属性と暗号化方式を選択します。

図 38 属性を暗号化する



暗号化属性ポリシーの管理には、iManager を使用できます。このセクションでは、次の情報について説明します。

- ◆ 244 ページの「iManager を使用して暗号化属性ポリシーを管理する」
- ◆ 245 ページの「LDAP を使用して暗号化属性ポリシーを管理する」
- ◆ 246 ページの「暗号化属性ポリシーをコピーする」
- ◆ 246 ページの「パーティション操作」

## iManager を使用して暗号化属性ポリシーを管理する


このセクションでは、次の手順について説明します。

- ◆ 244 ページの「暗号化属性ポリシーを作成して定義する」
- ◆ 244 ページの「暗号化属性ポリシーを編集する」
- ◆ 244 ページの「暗号化属性ポリシーを適用する」
- ◆ 245 ページの「暗号化属性ポリシーを削除する」


暗号化属性が eDirectory サーバに存在する場合、iManager は次の方法で動作します。

1. クリアテキストまたはセキュリティで保護されたチャネルを介して、暗号化属性の読み込み、表示、修正を行うことはできません。
2. クリアテキストまたはセキュリティで保護されたチャネルで iManager を介して、暗号化属性以外の属性を持つエントリの属性の読み込み、表示、修正を行うことはできません。これは、エントリ全体がブロックされていることを意味します。


### 暗号化属性ポリシーを作成して定義する

- 1 Novell iManager で、[役割およびタスク] ボタン  をクリックします。
- 2 [eDirectory の暗号化] > [属性] の順にクリックします。
- 3 暗号化属性ポリシー管理ウィザードで、[作成] > [編集] > [Apply Policy] の順にクリックします。
- 4 暗号化属性ポリシー管理ウィザードの指示に従って、ポリシーを作成し定義します。ウィザードの各段階で、[ヘルプ] が利用できます。

### 暗号化属性ポリシーを編集する


- 1 Novell iManager で、[役割およびタスク] ボタン  をクリックします。
- 2 [eDirectory の暗号化] > [属性] の順にクリックします。
- 3 暗号化属性ポリシー管理ウィザードで、[ポリシーを編集します。] を選択します。
- 4 暗号化属性ポリシー管理ウィザードの指示に従って、ポリシーを編集します。ウィザードの各段階で、[ヘルプ] が利用できます。

### 暗号化属性ポリシーを適用する

- 1 Novell iManager で、[役割およびタスク] ボタン  をクリックします。
- 2 [eDirectory の暗号化] > [属性] の順にクリックします。
- 3 暗号化属性ポリシー管理ウィザードで、[Apply Policy] を選択します。
- 4 暗号化属性ポリシー管理ウィザードの指示に従って、ポリシーを適用します。ウィザードの各段階で、[ヘルプ] が利用できます。



## 暗号化属性ポリシーを削除する

- 1 Novell iManager で、[役割およびタスク] ボタン  をクリックします。
- 2 [eDirectory の暗号化] > [属性] の順にクリックします。
- 3 暗号化属性ポリシー管理ウィザードで、[ポリシーを削除します。] を選択します。
- 4 暗号化属性ポリシー管理ウィザードの指示に従って、ポリシーを削除します。  
ウィザードの各段階で、[ヘルプ] が利用できます。

## LDAP を使用して暗号化属性ポリシーを管理する

**重要:** 暗号化属性の管理には、LDAP ではなく、iManager を使用することを強くお勧めします。

このセクションでは、次の手順について説明します。

- ◆ [245 ページの「暗号化属性ポリシーを作成して定義する」](#)
- ◆ [246 ページの「暗号化属性ポリシーを編集する」](#)
- ◆ [246 ページの「暗号化属性ポリシーを適用する」](#)
- ◆ [246 ページの「暗号化属性ポリシーを削除する」](#)

**注:** LDIF で暗号化する属性をマーキングする場合は、属性と方式のリストではなく、属性と方式のペアを指定する必要があります。これは暗号化属性に付随する現行の制約です。

## 暗号化属性ポリシーを作成して定義する

- 1 暗号化属性ポリシーを作成します。

たとえば、AE Policy- test-server という暗号化属性ポリシーの場合は次のようになります。

```
dn: cn=AE Policy - test-server, o=novell
changetype: add
objectClass: encryptionPolicy
```

- 2 作成したポリシーオブジェクトに attrEncryptionDefinition 属性を追加して、暗号化する属性をマーキングします。

たとえば、暗号化する属性の名前が CRID の場合は、次のように暗号化方式と属性名を指定します。

```
dn: cn=AE Policy - test-server, o=novell
changetype: modify
add: attrEncryptionDefinition
attrEncryptionDefinition: aes$CRID
```

**注:** 属性名の指定には、その属性の NDS 名を使用します。eDirectory では多くの属性が LDAP 名と NDS 名の両方を持っています。ここでは、属性名として NDS 名を指定する必要があります。

- 3 attrEncryptionRequiresSecure 属性をポリシーに追加します。

この属性の値によって、暗号化属性にアクセスする際にセキュリティ保護されたチャネルの使用を常に要求するかどうか指定されます。この値が 0 の場合、常には要求しないことを示します。この値が 1 の場合は、常に要求することを示します。

例:

```
dn: cn=AE Policy - test-server, o=novell
changetype: modify
add: attrEncryptionRequiresSecure
attrEncryptionRequiresSecure: 0
```

#### 4 NCP サーバにポリシーを関連付けます。

test-server という NCP サーバの場合は次のようになります。

```
dn: cn=test-server, o=novell
changetype: modify
add: encryptionPolicyDN
encryptionPolicyDN: cn=AE Policy - test-server, o=novell
```

#### 暗号化属性ポリシーを編集する

次の LDIF ファイルは、attrEncryptionRequireSecure 属性の値を変更することで暗号化属性ポリシーを編集する方法を示しています。

```
dn: cn=AE Policy - test-server, o=novell
changetype: modify
replace: attrEncryptionRequiresSecure
attrEncryptionRequiresSecure: 1
```

#### 暗号化属性ポリシーを適用する

次の LDIF ファイルは、AE Policy-test-server という暗号化属性ポリシーを test-server というサーバに適用する方法を示しています。

```
dn: cn=test-server, o=novell
changetype: modify
add: encryptionPolicyDN
encryptionPolicyDN: cn=AE Policy - test-server, o=novell
```

#### 暗号化属性ポリシーを削除する

次の LDIF ファイルは、暗号化属性ポリシーを削除する方法を示しています。

```
dn: cn=AE Policy - test-server, o=novell
changetype: delete
```

#### 暗号化属性ポリシーをコピーする

eDirectory 8.8 以降では、暗号化属性ポリシーをコピーして多数のサーバに同一の設定内容を反映することができます。ポリシーは、オブジェクトとして eDirectory に保存されます。

iManager を使用してポリシーオブジェクトをコピーする手順については、[99 ページの「オブジェクトをコピーする」](#)を参照してください。

#### パーティション操作

2つのパーティションをマージすると、ペアレントのポリシーがマージ後のパーティションで保持されます。パーティションを分割すると、ペアレントのポリシーがチャイルドパーティションに継承されます。

## 暗号化属性にアクセスする

属性を暗号化すると、暗号化属性へのアクセスも保護されます。eDirectory 8.8 以降では、セキュリティ保護されたチャネル (LDAP セキュアチャネルまたは HTTP セキュアチャネル) を使用した暗号化属性へのアクセスを制限できるようになっています。

デフォルトでは、セキュリティ保護されたチャネルからしか暗号化属性にアクセスできません。

ただし、クライアントがクリアテキストで暗号化属性にアクセスできるようにするには、[常にセキュアチャネルが必要] オプションを無効にする必要があります。詳細については、[247 ページの「クリアテキストチャネルから暗号化属性へのアクセスを有効 / 無効にする」](#)を参照してください。

### クリアテキストチャネルから暗号化属性へのアクセスを有効 / 無効にする

iManager または LDAP のいずれかを使用して、[常にセキュアチャネルが必要] オプション (つまり、attrEncryptionRequireSecure 属性) を有効または無効にすることで、クリアテキストチャネルから暗号化属性へのアクセスを有効または無効にすることができます。

このセクションでは、次の情報について説明します。

- ◆ [247 ページの「iManager を使用してクリアテキストチャネルから暗号化属性へのアクセスを有効 / 無効にする」](#)
- ◆ [247 ページの「LDAP を使用してクリアテキストチャネルから暗号化属性へのアクセスを有効 / 無効にする」](#)

### iManager を使用してクリアテキストチャネルから暗号化属性へのアクセスを有効 / 無効にする

iManager を使用してクリアテキストチャネルから暗号化属性へのアクセスを有効または無効にするには、次の作業を行う際に、暗号化属性ポリシー管理ウィザードで [常にセキュアチャネルが必要] を有効または無効にします。

- ◆ [暗号化属性ポリシーを作成して定義する](#)
- ◆ [暗号化属性ポリシーを編集する](#)

### LDAP を使用してクリアテキストチャネルから暗号化属性へのアクセスを有効 / 無効にする

LDAP を使用してクリアテキストチャネルから暗号化属性へのアクセスを有効にするには、次の属性を暗号化属性ポリシーに追加します。

#### attrEncryptionRequiresSecure

この属性を 0 に設定すると、セキュリティ保護されたチャネルを必ずしも使用する必要はなくなります。つまり、クリアテキストチャネルから暗号化属性にアクセスできます。この属性を 1 に設定すると、セキュリティ保護されたチャネルの使用が常に要求されるようになります。つまり、セキュリティ保護されたチャネルからのみ暗号化属性にアクセスできます。

詳細については、[245 ページのステップ 3](#)を参照してください。

## 暗号化属性を表示する

暗号化されている属性が表示されるかどうかは、[常にセキュアチャンネルが必要] オプションが有効になっているかどうかによって決定されます。つまり、暗号化属性にアクセスする際にセキュリティ保護されたチャンネルを使用するかどうかによって決まります。

- ◆ 248 ページの「iManager を使用して暗号化属性を表示する」
- ◆ 248 ページの「DSBrowse を使用して暗号化属性を表示する」
- ◆ 248 ページの「SNMP トラップ」

### iManager を使用して暗号化属性を表示する

[常にセキュアチャンネルが必要] が有効になっている場合は、暗号化属性を表示できません。エラー「-6089」が返されます。これは、暗号化属性にアクセスする際にセキュリティ保護されたチャンネルを使用する必要があることを示しています。

[常にセキュアチャンネルが必要] が無効になっている場合は、iManager で暗号化属性値を表示できます。

詳細については、213 ページの「ツリー内のオブジェクトの参照」を参照してください。

### DSBrowse を使用して暗号化属性を表示する

[常にセキュアチャンネルが必要] オプションが有効になっている場合、つまり、暗号化属性にアクセスする際にセキュリティ保護されたチャンネルの使用が常に要求される場合は、暗号化されたエントリの属性を表示することはできません。ただし、暗号化されていないエントリの属性は表示できます。

### SNMP トラップ

暗号化属性にアクセスする際にセキュリティ保護されたチャンネルの使用を常に要求するように指定している場合は、NDS<sup>®</sup> 値イベントがブロックされます。値イベントに関連するトラップの値データは NULL になり、結果は -6089 に設定されます。これは、暗号化属性の値を取得するために、セキュリティ保護されたチャンネルを使用する必要があることを示します。次のトラップの値データは NULL になります。

- ◆ ndsAddValue
- ◆ ndsDeleteValue
- ◆ ndsDeleteAttribute

## バックアップデータを暗号化 / 復号化する

暗号化属性を含むサーバ上のデータをバックアップする際には、バックアップデータを暗号化または復号化するためのパスワードを入力するよう求められます。これは、ndsbackup ユーティリティの -E オプションを使用して簡単に指定できます。詳細については、ndsbackup の manpage を参照してください。

データのバックアップの詳細については、389 ページの第 14 章「Novell eDirectory のバックアップと復元」を参照してください。

## 暗号化属性を含む DIB ファイルセットのクローンを作成する

暗号化属性を含む eDirectory データベースのクローンを作成すると、DIB ファイルセットのクローンにも暗号化属性値が含まれます。

DIB ファイルセットのクローンに含まれる値を暗号化するには、eDirectory で使用されるキーを保護するためのパスワードを設定する必要があります。DIB ファイルセットのクローンを他のサーバに配置する際には、このパスワードの入力を求められます。

詳細については、[218 ページの「DIB セットのクローン」](#)を参照してください。

## レプリカリングに eDirectory 8.8 サーバを追加する

eDirectory 8.8 サーバは、レプリカが格納されたいずれかのサーバまたはすべてのサーバ上で属性が暗号化されているかどうか、あるいは [常にセキュアチャンネルが必要] が有効になっているかどうかに関わらず、レプリカリングに追加できます。

eDirectory 8.8 サーバをレプリカリングに追加する際の詳細については、[140 ページの「レプリカを追加する」](#)を参照してください。

## 下位互換性

暗号化属性にアクセスするには、iManager、SNMP、DirXML<sup>®</sup>、NSureAudit などのすべての eDirectory ユーティリティを、セキュリティ保護された NCP<sup>™</sup> に変更する必要があります。変更しない場合は、暗号化属性にアクセスする際にセキュリティ保護されたチャンネルの使用を要求しないように指定する必要があります。詳細については、[247 ページの「クリアテキストチャンネルから暗号化属性へのアクセスを有効 / 無効にする」](#)を参照してください。

## 暗号化属性に移行する

eDirectory 8.8 以降のバージョンにアップグレードすると、暗号化属性ポリシーを作成して定義することで、既存の属性を暗号化できます。詳細については、[243 ページの「暗号化属性ポリシーを管理する」](#)を参照してください。

## 暗号化属性のレプリカを作成する

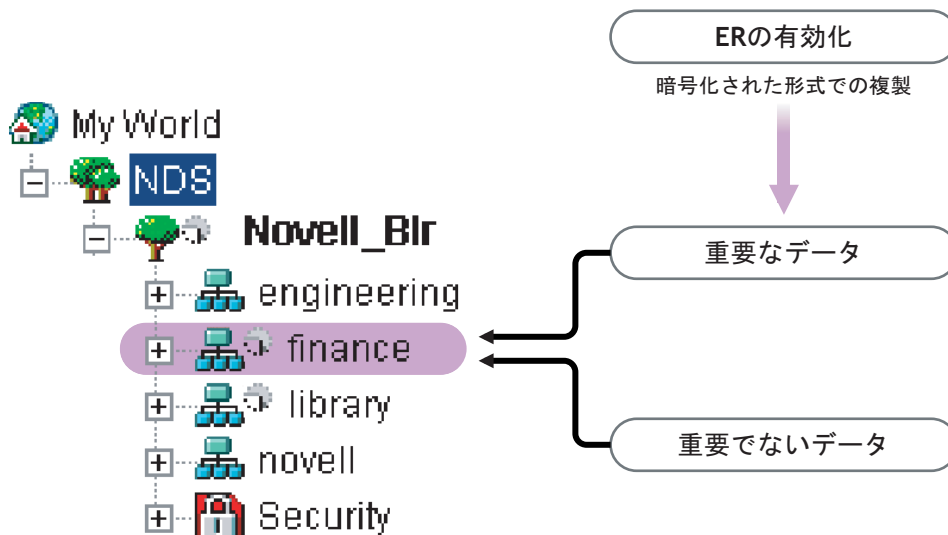
デフォルトでは、サーバに暗号化属性が存在している場合でも、暗号化複製は無効になっています。暗号化属性を安全に複製するには、暗号化複製を有効にする必要があります。暗号化複製の設定については、[250 ページの「暗号化レプリケーション」](#)を参照してください。

## 暗号化レプリケーション

Novell eDirectory 8.8 以降では、eDirectory 8.8 サーバ間を転送されるデータを暗号化できます。データがクリアテキスト形式で転送されなくなるため、複製時のセキュリティを強化できます。

複製の暗号化の重要性と暗号化のシナリオについては、『*Novell eDirectory 8.8 What's New Guide*』（<http://www.novell.com/documentation/beta/edir88/edir88new/data/bqljq11.html#bqljq11>）を参照してください。

図 39 暗号化レプリケーション



図中の「finance」と「library」は、ツリー内のパーティションです。「finance」には、複製の際に暗号化を必要とする重要データが含まれている可能性があります。その場合は、パーティション「finance」に対して暗号化複製を有効にすることができます。「library」のように重要データが含まれていないパーティションについては、暗号化複製を有効にする必要はありません。

**重要:** パーティションに対して暗号化複製を有効にすると、複製処理の速度が低下する可能性があります。

暗号化複製を有効または無効にするには、iManager を使用します。

**注:** Netware® では、暗号化複製がサポートされていません。

このセクションでは、次の情報について説明します。

- ◆ 251 ページの「暗号化複製を有効にする」
- ◆ 255 ページの「新しいレプリカをレプリカリングに追加する」
- ◆ 260 ページの「同期と暗号化複製」
- ◆ 260 ページの「暗号化複製ステータスを表示する」

## 暗号化複製を有効にする

暗号化複製を有効にするには、暗号化複製を有効にするようにパーティションを設定する必要があります。設定はパーティションの Root オブジェクトに保存されます。

暗号化複製は、パーティションレベルでもレプリカレベルでも有効にすることができます。

レプリカレベルの設定は、パーティションレベルの設定よりも優先されます。つまり、次のようになります。

- ◆ 暗号化複製がパーティションレベルで有効になっていて、特定のレプリカが無効になっている場合、それらのレプリカの間の複製はクリアテキスト形式で行われます。
- ◆ パーティションレベルで暗号化複製が無効になっていて、特定のレプリカで有効になっている場合、それらのレプリカの間の複製は暗号化された形式で行われます。

表 2 パーティションレベルの暗号化複製の設定を上書きする

| パーティションレベル | レプリカレベル | 複製      |
|------------|---------|---------|
| 有効         | 無効      | 暗号化されない |
| 無効         | 有効      | 暗号化される  |

このセクションでは、次の手順について説明します。

- ◆ [251 ページの「パーティションレベルで暗号化複製を有効にする」](#)
- ◆ [253 ページの「レプリカレベルで暗号化複製を有効にする」](#)

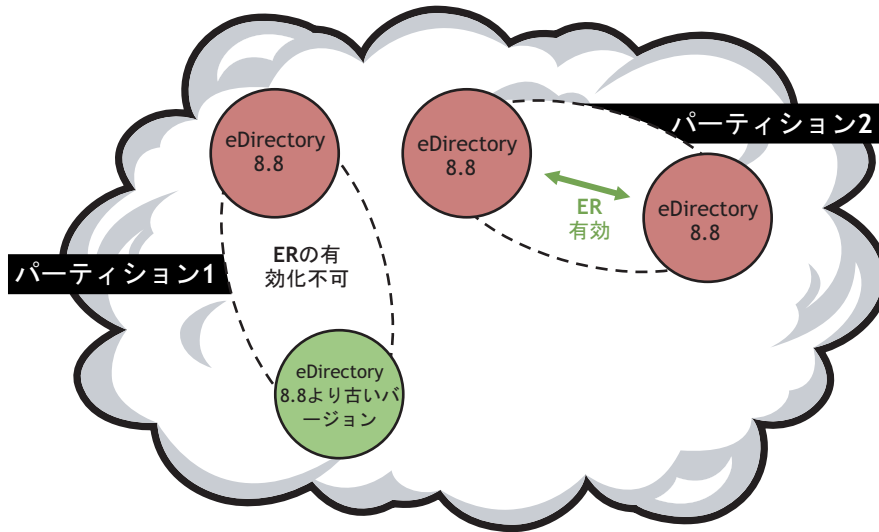
### パーティションレベルで暗号化複製を有効にする

パーティションレベルで暗号化複製を有効にすると、そのパーティションをホストしているすべてのレプリカの間で行われる複製が暗号化されます。たとえば、パーティション P1 のレプリカとして、R1、R2、R3、および R4 があるとします。その場合は、これらのレプリカの間のすべての複製（インバウンドとアウトバウンドの両方）を暗号化できます。

パーティションレベルで暗号化複製を有効にするには、そのパーティションをホストしているすべてのサーバで eDirectory 8.8 以降が実行されている必要があります。暗号化複製が有効になっていない他のパーティションは、eDirectory 8.8 より古いバージョンの eDirectory サーバでもホストできます。



図 40 パーティションレベルでの暗号化複製




レプリカレベルで暗号化複製が設定されている場合は、レプリカレベルの設定がパーティションレベルの設定よりも優先されます。[251 ページの表 2 「パーティションレベルの暗号化複製の設定を上書きする」](#)を参照してください。

下位互換性は、暗号化複製がパーティションレベルで有効になっているかどうか依存します。詳細については、[255 ページの「新しいレプリカをレプリカリングに追加する」](#)を参照してください。

パーティションレベルで暗号化複製を有効にするには、次のセクションで説明するように、iManager または LDAP を使用します。

- ◆ [252 ページの「iManager を使用してパーティションレベルで暗号化複製を有効にする」](#)
- ◆ [253 ページの「LDAP を使用してパーティションレベルで暗号化複製を有効にする」](#)
- ◆ [255 ページの「パーティション操作」](#)

### iManager を使用してパーティションレベルで暗号化複製を有効にする

- 1 [役割およびタスク] ボタン  をクリックします。
- 2 [eDirectory の暗号化] > [暗号化複製] の順にクリックします。
- 3 暗号化複製ウィザードで、[すべてのレプリカ同期を暗号化する] を選択します。  
ウィザードの各段階で、[ヘルプ] が利用できます。

**注:** パーティションレベルで暗号化複製を無効にする場合は、[すべてのレプリカ同期を暗号化する] の選択を解除します。

暗号化複製ウィザードでパーティション全体に対して暗号化複製を有効にした場合でも、特定のレプリカに対して暗号化複製を無効にできます。暗号化複製が無効になっているレプリカは、暗号化された形式のデータを送受信しません。パーティション全体に対して暗号化を無効にする場合は、[すべてのレプリカ同期を暗号化する] の選択を解除します。



## LDAP を使用してパーティションレベルで暗号化複製を有効にする

**重要:** iManager を使用して暗号化複製を有効にすることを強くお勧めします。

複製を暗号化するには、属性 `dsEncryptedReplicationConfig` を使用します。構文は次のとおりです。

有効 / 無効フラグ # ターゲットレプリカ番号 # ソースレプリカ番号

次のいずれかのフラグに置き換えます。

- ◆ 0 : 暗号化複製が無効になります
- ◆ 1 : 暗号化複製が有効になります

ソースレプリカ番号とターゲットレプリカ番号は、パーティションのソースレプリカ番号とターゲットレプリカ番号です。ソースレプリカ番号とターゲットレプリカ番号はどちらを先に指定しても構いません。レプリカ A から B への複製が暗号化されている場合は、B から A への複製も暗号化されます。

**注:** パーティションレベルのソースレプリカ番号とターゲットレプリカ番号を 0 にして、フラグを 1 に設定した場合は、すべてのレプリカで暗号化複製が有効になります。

パーティションレベルで暗号化複製を有効にするには、`dsEncryptedReplicationConfig` 属性の値を `1#0#0` に設定します。

次に、パーティションレベルで暗号化複製を有効にするための LDIF ファイルの例を示します。

```
dn: o=ou
changetype: modify
replace: dsEncryptedReplicationConfig
dsEncryptedReplicationConfig: 1#0#0
```

レプリカレベルの設定は、パーティションレベルの設定よりも優先されます。詳細については、[254 ページの「LDAP を使用してレプリカレベルで暗号化複製を有効にする」](#)を参照してください。

## レプリカレベルで暗号化複製を有効にする

レプリカレベルで暗号化複製を有効にすると、特定のレプリカの間での複製が暗号化されます。指定したレプリカの間で行われるアウトバウンドおよびインバウンドの複製が暗号化されます。

たとえば、パーティション P1 のレプリカとして、R1、R2、R3、および R4 があります。この場合、レプリカ R1 と R2 の間、または R2 と R4 の間の複製を暗号化できます。

パーティションのレプリカの間で暗号化複製を有効にするには、レプリカの間での暗号化リンクを定義する必要があります。詳細については、[254 ページの「iManager を使用してレプリカレベルで暗号化複製を有効にする」](#)を参照してください。

1 つのレプリカで暗号化複製を有効にした場合は、次のような複製が行われます。

- ◆ サーバからこのレプリカへのインバウンド同期が暗号化されます。
- ◆ このレプリカから別のサーバへのアウトバウンド同期が暗号化されます。

暗号化複製が有効になっているレプリカは、eDirectory 8.8 サーバ上に配置されている必要があります。レプリカリング内にあるレプリカのうち、暗号化複製が有効になっていない残りのレプリカは、eDirectory 8.8 より古いバージョンの eDirectory サーバ上に配置しても構いません。

特定のレプリカに対してのみ暗号化複製を有効にした場合は、eDirectory 8.8 サーバおよび eDirectory 8.8 より古いバージョンのサーバをレプリカリングに追加できます。

レプリカレベルで暗号化複製を無効にするには、iManager の暗号化複製の環境設定のウィザードで、該当するレプリカに対し [リンクを暗号化する] を無効にします。

レプリカレベルで暗号化複製を有効にするには、次のセクションで説明するように、iManager または LDAP を使用します。

- ◆ 254 ページの「iManager を使用してレプリカレベルで暗号化複製を有効にする」
- ◆ 254 ページの「LDAP を使用してレプリカレベルで暗号化複製を有効にする」


### iManager を使用してレプリカレベルで暗号化複製を有効にする

iManager を使用してレプリカレベルで暗号化複製を有効にするには、暗号化リンクを作成します。暗号化リンクで接続されたレプリカの間では、複製が暗号化されます。暗号化リンクを作成するには、レプリカレベルで暗号化複製を設定する際に、ソースレプリカと 1 つまたは複数のターゲットレプリカを選択します。

たとえば、パーティション P1 のレプリカとして、R1、R2、R3、および R4 があるとします。R1 と R2 の間の複製を暗号化するには、いずれかのレプリカをソースレプリカに指定し、他方のレプリカをターゲットレプリカに指定して暗号化リンクを作成します。

暗号化リンクを作成した後は、iManager の暗号化複製の環境設定のウィザードで [リンクを暗号化する] をオンまたはオフにすることにより、特定のレプリカに対して暗号化リンクを有効または無効にすることができます。詳細については、254 ページの「iManager を使用してレプリカレベルで暗号化複製を有効にする」を参照してください。

レプリカレベルで暗号化複製を有効にする

- 1 [役割およびタスク] ボタン  をクリックします。
- 2 [eDirectory の暗号化] > [暗号化複製] の順にクリックします。
- 3 暗号化複製ウィザードの [暗号化同期] テーブルで、[新規] を選択して暗号化リンクを定義します。
  - 3a ソースレプリカを選択します。
  - 3b ターゲットレプリカを 1 つまたは複数選択します。
  - 3c [リンクを暗号化する] を選択します。
  - 3d [OK] をクリックします。
- 4 [完了] をクリックします。

### LDAP を使用してレプリカレベルで暗号化複製を有効にする

**重要:** iManager を使用して暗号化複製を有効にすることを強くお勧めします。

複製を暗号化するには、属性 dsEncryptedReplicationConfig を使用します。構文は次のとおりです。

有効 / 無効フラグ # ターゲットレプリカ番号 # ソースレプリカ番号

この構文の詳細については、253 ページの「LDAP を使用してパーティションレベルで暗号化複製を有効にする」を参照してください。

この構文でレプリカ番号を指定すると、指定したレプリカの間での複製が暗号化されます。次に、この構文の例を示します。

- ◆ 1#0#1：レプリカ番号 1 と、他のすべてのレプリカの間で、インバウンドおよびアウトバウンドの複製が暗号化されます。
- ◆ 0#3#1：レプリカ番号 3 と 1 の間で暗号化複製が無効になります。
- ◆ 0#1#1：レプリカ番号 1 で暗号化複製が無効になります。

次に、レプリカ番号 1 と 3 の間で暗号化複製を無効にするための LDIF ファイルの例を示します。

```
dn: o=ou
changetype: modify
replace: dsEncryptedReplicationConfig
dsEncryptedReplicationConfig: 0#3#1
```

## パーティション操作

パーティションを分割すると、ペアレントパーティションの暗号化複製の設定がチャイルドパーティションに継承されます。パーティションをマージすると、ペアレントパーティションの暗号化複製の設定がマージ後のパーティションで保持されます。

## 新しいレプリカをレプリカリングに追加する

レプリカリングに新しいレプリカを追加する場合は、パーティションレベルおよびレプリカレベルで暗号化複製が有効になっているかどうかによって、それぞれ異なる影響を受けます。

レプリカをレプリカリングに追加する場合の詳細については、[140 ページの「レプリカの管理」](#)を参照してください。

次のセクションで説明するように、どちらレベルでも、レプリカリングに追加する eDirectory サーバのバージョンによって、複数のシナリオが考えられます。

- ◆ [255 ページの「パーティションレベルで暗号化複製を有効にする」](#)
- ◆ [260 ページの「レプリカレベルで暗号化複製を有効にする」](#)

## パーティションレベルで暗号化複製を有効にする

このシナリオは、追加する eDirectory サーバのバージョンによって異なります。このセクションでは、次の情報について説明します。

- ◆ [255 ページの「eDirectory 8.8 より古いバージョンのサーバをレプリカリングに追加する」](#)
- ◆ [257 ページの「eDirectory 8.8 サーバをレプリカリングに追加する」](#)

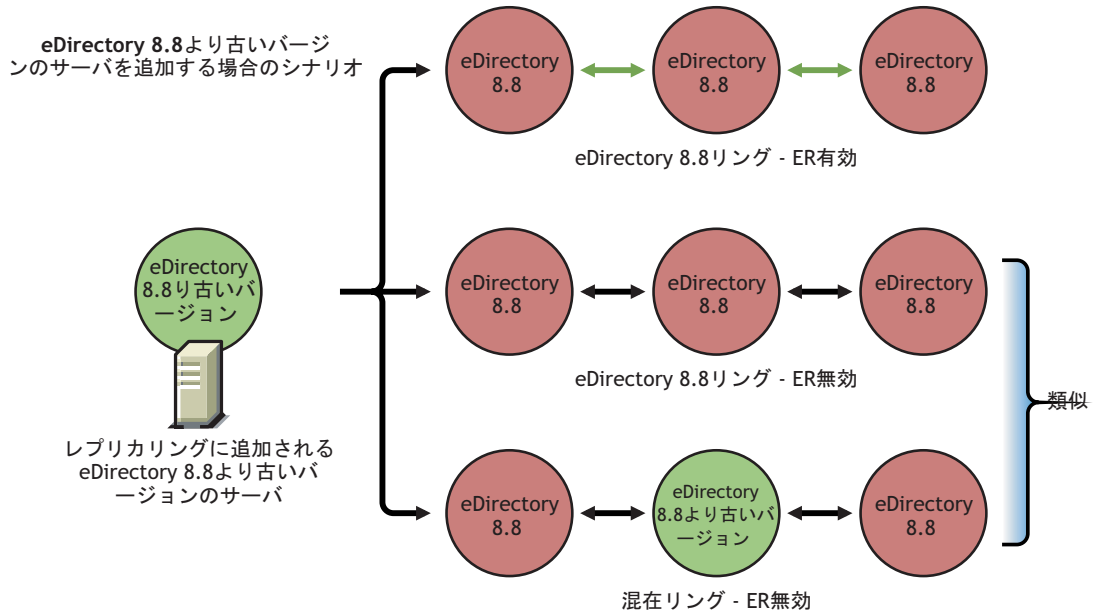
### eDirectory 8.8 より古いバージョンのサーバをレプリカリングに追加する

次の図は、eDirectory 8.8 より古いバージョンのサーバをレプリカリングに追加する場合のシナリオを示しています。

- ◆ シナリオ A
- ◆ シナリオ B
- ◆ シナリオ C

注：図中の「ER」は、暗号化複製を表しています。

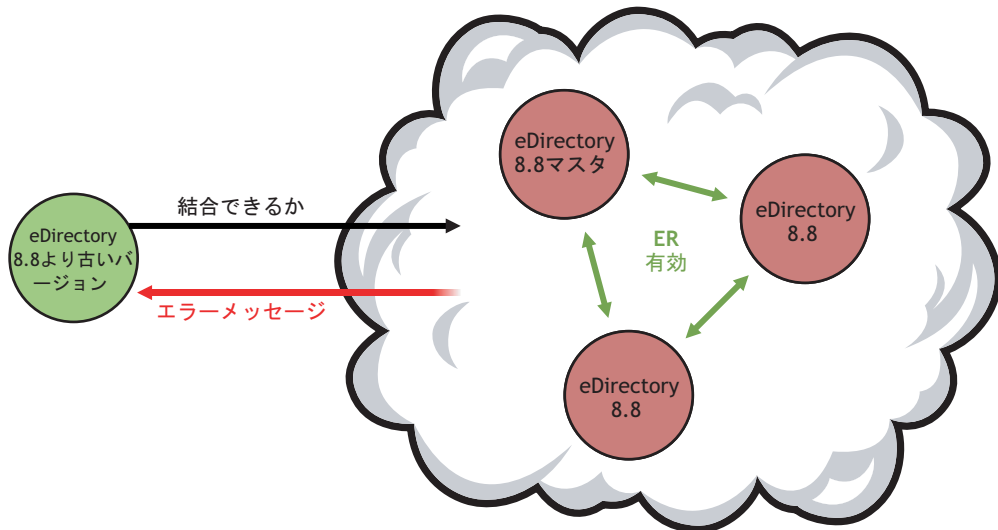
図 41 eDirectory 8.8 より古いバージョンのサーバを追加する場合のシナリオ



シナリオ A：暗号化複製が有効になっている eDirectory 8.8 レプリカリングに eDirectory 8.8 より古いバージョンのサーバを追加する

暗号化複製が有効になっている eDirectory 8.8 レプリカリングに eDirectory 8.8 より古いバージョンのサーバを追加すると、ERR\_INCOMPATIBLE\_DS エラーが返されます。レプリカリングにサーバを追加することはできますが、パーティションのレプリカをこのサーバでホストすることはできません。

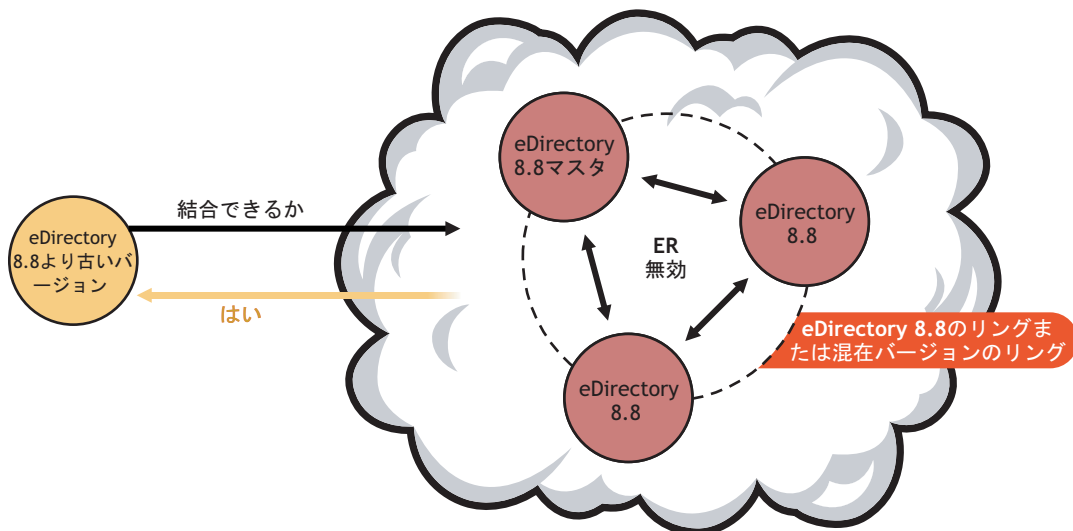
図 42 暗号化複製が有効になっている eDirectory 8.8 レプリカリングに eDirectory 8.8 より古いバージョンのサーバを追加する



シナリオ B : 暗号化複製が無効になっている eDirectory 8.8 レプリカリングに eDirectory 8.8 より古いバージョンのサーバを追加する

暗号化複製が無効になっている eDirectory 8.8 レプリカリングには、eDirectory 8.8 より古いバージョンのサーバを追加できます。

図 43 暗号化複製が無効になっているレプリカリングに eDirectory 8.8 より古いバージョンのサーバを追加する



シナリオ C : レプリケーションの暗号化が無効になっている混在レプリカリングに eDirectory 8.8 より古いバージョンのサーバを追加する

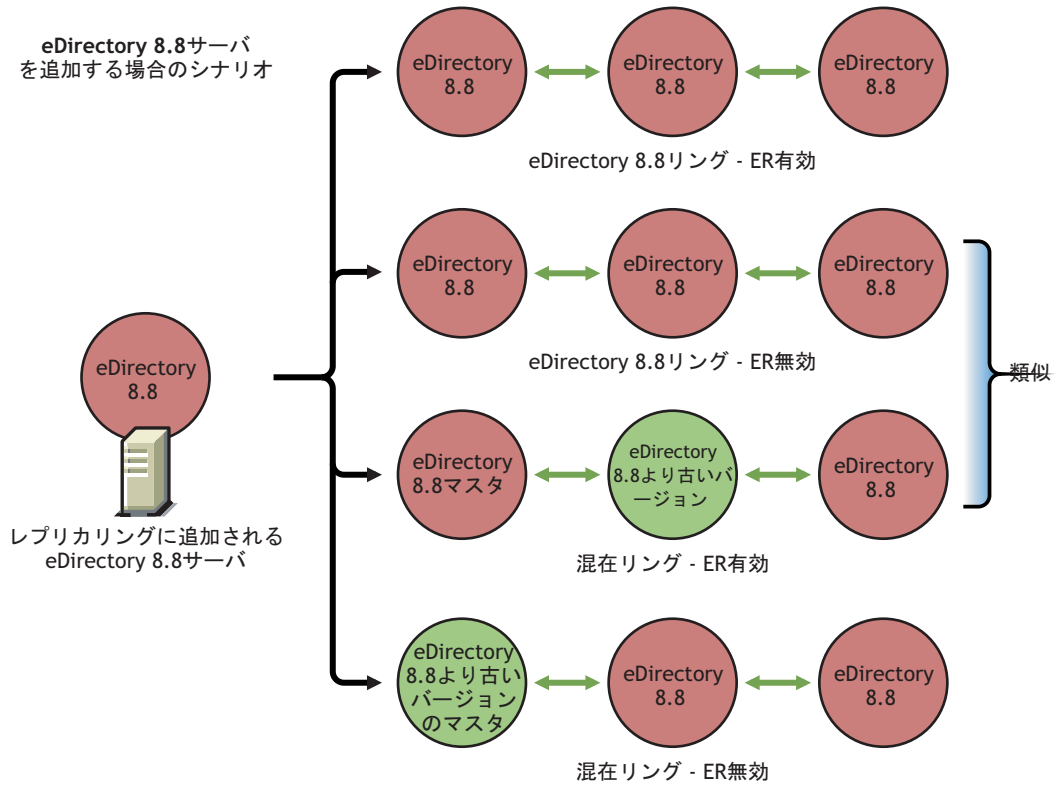
複数のバージョンの eDirectory が混在し、暗号化複製が無効になっているレプリカリングには、eDirectory 8.8 より古いバージョンのサーバを追加できます。図 43 を参照してください。

#### eDirectory 8.8 サーバをレプリカリングに追加する

次の図は、eDirectory 8.8 サーバをレプリカリングに追加する場合のシナリオを示しています。

- ◆ シナリオ A
- ◆ シナリオ B
- ◆ シナリオ C
- ◆ シナリオ D

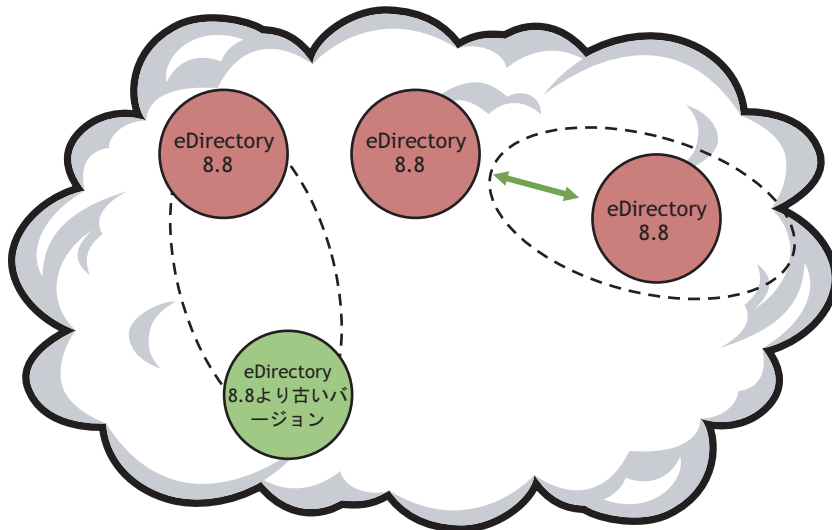
図 44 eDirectory 8.8 サーバを追加する場合のシナリオ



シナリオ A：暗号化複製が有効になっている eDirectory 8.8 レプリカリングに eDirectory 8.8 サーバを追加する

この場合は、追加された eDirectory 8.8 サーバで暗号化複製は既に有効になっています。

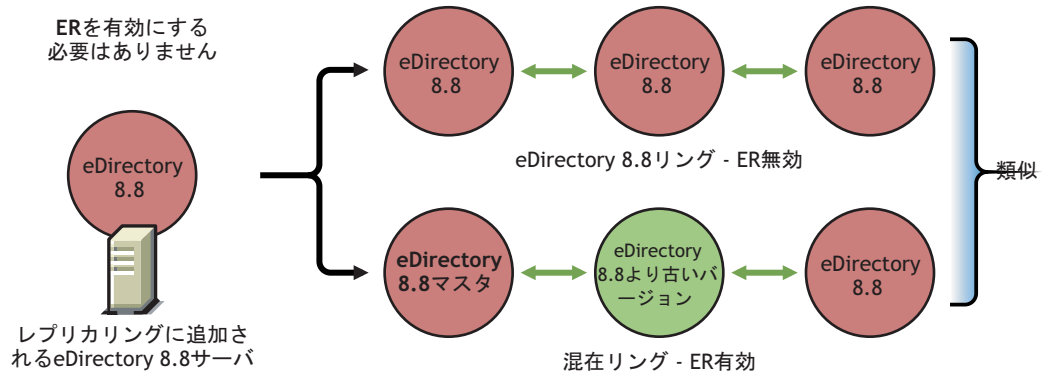
図 45 暗号化複製が有効になっている eDirectory レプリカリングに eDirectory 8.8 サーバを追加する



シナリオ B : 暗号化複製が無効になっている eDirectory 8.8 レプリカリングに eDirectory 8.8 サーバを追加する

この場合は、追加された eDirectory 8.8 サーバで暗号化複製が無効になります。

図 46 暗号化複製が無効になっているレプリカリングに eDirectory 8.8 サーバを追加する



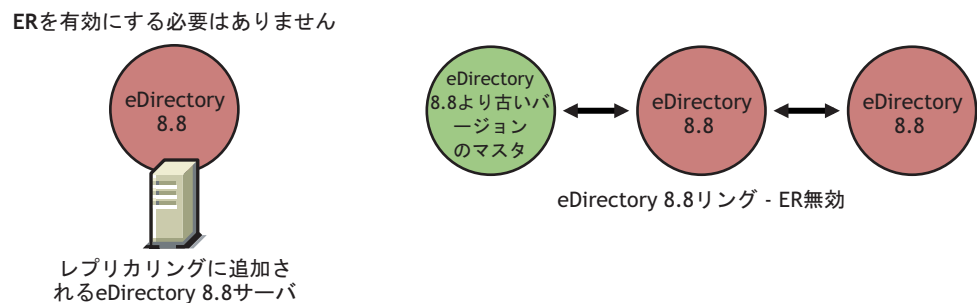
シナリオ C : マスタレプリカが eDirectory 8.8 サーバで、暗号化複製が無効になっている混在レプリカリングに eDirectory 8.8 サーバを追加する

この場合は、追加する eDirectory 8.8 サーバで暗号化複製を有効にする必要はありません。[259 ページの図 46「暗号化複製が無効になっているレプリカリングに eDirectory 8.8 サーバを追加する」](#)を参照してください。

シナリオ D : マスタレプリカが eDirectory 8.8 より古いバージョンのサーバで、暗号化複製が無効になっている混在レプリカリングに eDirectory 8.8 サーバを追加する

この場合は、追加する eDirectory 8.8 サーバで暗号化複製を有効にする必要はありません。

図 47 マスタレプリカが eDirectory 8.8 より古いバージョンのサーバであるレプリカリングに eDirectory 8.8 サーバを追加する





## レプリカレベルで暗号化複製を有効にする

ソースレプリカと特定のターゲットレプリカの間で暗号化複製が有効になっている場合は、eDirectory 8.8 サーバまたは eDirectory 8.8 より古いバージョンのサーバをレプリカリングに追加できます。

ソースレプリカと、レプリカリング内の他のすべてのレプリカの間で暗号化複製が有効になっている場合、このシナリオは当てはまりません。その場合は、パーティションレベルで暗号化複製が有効または無効になっているレプリカリングにレプリカを追加することと同じになります。詳細については、[255 ページの「パーティションレベルで暗号化複製を有効にする」](#)を参照してください。

## 追加するサーバで暗号化複製を有効にする

追加するサーバのプラットフォームが Linux または UNIX の場合は、`ndsconfig` の `-E` オプションを使用して暗号化複製を有効にできます。詳細については、`ndsconfig` の `manpage` を参照してください。

追加するサーバのプラットフォームが Windows の場合は、インストールウィザードで [暗号化複製を有効にします] オプションを選択します。

追加するサーバのプラットフォームが Linux または UNIX 以外の場合は、iManager または LDAP を使用して暗号化複製を有効にできます。詳細については、[251 ページの「暗号化複製を有効にする」](#)を参照してください。

## 同期と暗号化複製

特定のレプリカで暗号化複製を有効にして、設定の変更を他のサーバと同期しない場合、レプリカ間の複製は暗号化された形式で行われます。暗号化複製の設定変更が同期されていないレプリカでは、引き続きクリアテキスト形式で複製が行われます。

それまで暗号化複製の設定がレプリカ間で同期されていなかった場合でも、レプリカ間の複製は暗号化された形式で行われます。

## 暗号化複製ステータスを表示する

次の手順に従って、iMonitor を介して暗号化複製ステータスを表示できます。

- 1 iMonitor で、アシスタントフレームの [エージェント同期] をクリックします。
- 2 表示するパーティションの [レプリカ同期] をクリックします。

レプリカステータス情報が表示されます。現在接続されているレプリカからのリンクが暗号化されているかどうか [暗号化状態] フィールドに表示されます。

基本的に、暗号化複製 (ER) には次の 3 つのシナリオがあります。

- ◆ **パーティションレベルで ER が有効**：接続先のレプリカの暗号化状態が有効になっている場合です。  
どのレプリカに接続しているかを確認するには、レプリカフレームでハイパーリンクが付いていないレプリカを探します。そのレプリカが、現在接続しているレプリカです。他のレプリカを参照すると、そのレプリカの [暗号化状態] も [使用可能] と表示されます。
- ◆ **レプリカレベルで ER が有効**：特定のレプリカからすべてのレプリカへの (つまり 1 つからすべてへの) ER が有効になっている場合です。この場合は、そのレプリカに接続すると、レプリカの [暗号化状態] が [使用可能] と表示されます。



- ◆ **一部のレプリカで ER が有効 / 無効:**一部のレプリカで ER が有効 / 無効 – パーティション全体では ER が有効になっているが、一部のサーバでは無効になっている場合、またはその逆の場合です。

たとえば、3つのレプリカを含むパーティション A で ER が有効に設定されていて、レプリカ 1 とレプリカ 3 の間の ER が無効に設定されている場合、レプリカ 1 に接続すると、[暗号化状態] は次のように表示されます。

Server 1 使用可能

Server 2

Server 3 使用不可

これは、Server 1 からレプリカリング内のすべてのサーバへの ER は有効であるが、Server 1 から Server 3 への ER は管理者によって無効にされていることを意味します。

## データを暗号化するときデータの完全な安全性を確保する

データを暗号化するときには、まず、次の基本的な規則を守ることが重要です。

*最終的に暗号化される情報をハードディスク (またはその他の媒体) にクリアテキストの形式で書き込まないこと。*

既存のクリアテキストデータを暗号化対象としてマークすれば、そのデータは暗号化されますが、既存のクリアテキストデータは、DIB が存在するハードディスクのどこかに残る可能性があります。

次の操作を実行しようとする、データベース内のどこかのブロックにデータのクリアテキスト部分が残ります。

- ◆ 既存のクリアテキストデータを暗号化対象としてマークする
- ◆ 暗号化属性の暗号化方式を変更する

以下のセクションでは、データを暗号化するときのシナリオを想定し、暗号化データの完全な安全性を確保する手順を説明します。

- ◆ [262 ページの「完全に新しい設定でデータを暗号化する」](#)
- ◆ [262 ページの「既存の設定でデータを暗号化する」](#)
- ◆ [264 ページの「まとめ」](#)

## 完全に新しい設定でデータを暗号化する

新しい設定では、オペレーティングシステムをインストールしただけの状態では eDirectory をインストールしません。したがって、DIB が存在するハードディスク上にクリアテキストデータが存在しないことが保証されます。

eDirectory 内の暗号化データの完全な安全性を確保するには、次の手順を実行します。

- 1 どの属性をどの方式で暗号化するかをあらかじめ決めておきます。

つまり、データをクリアテキスト形式で eDirectory にアップロードする前に、暗号化する属性を決めておく必要があります。

**警告:** いったんデータをクリアテキスト形式で eDirectory にロードしたら、属性を暗号化対象としてマークしないでください。そうすることもできますが、その場合はセキュリティの問題が発生します。

- 2 eDirectory を設定し、属性に適用する暗号化方式を設定します。

- 3 既存のデータを新しいサーバにロードします。

LDIF ファイルからバルクロードすることと他のサーバから複製するという 2 つがよくあるシナリオです。バルクロードするときは、クリアテキストの LDIF ファイルを DIB が存在するハードディスクにコピーしないでください。クリアテキストデータをディスクに書き込んではいけないという規則を思い出してください。

- 4 既存のすべてのクリアテキストデータを破壊します。

クリアテキストデータが格納されているディスク (またはその他の媒体) を完全に消去してください。消去する対象には、サーバのバルクロードに使われたクリアテキストの LDIF ファイル、複製に使われた他のサーバ、古いバックアップが残っているテープなどが含まれます。

## 既存の設定でデータを暗号化する

このシナリオには次のような状況があります。

- ◆ [262 ページの「既存のクリアテキストデータを暗号化データに変換する」](#)
- ◆ [264 ページの「データの暗号化方式を変更する」](#)

### 既存のクリアテキストデータを暗号化データに変換する

クリアテキストデータを暗号化対象としてマークし、以下の方法でデータの安全性を確保できます。

- ◆ [262 ページの「複製を利用する方法」](#)
- ◆ [263 ページの「バックアップおよび復元を利用する方法」](#)

#### 複製を利用する方法

- 1 新しいサーバで次のように暗号化を設定します。

- 1a どの属性をどの方式で暗号化するかをあらかじめ決めておきます。

つまり、データをクリアテキスト形式で eDirectory にアップロードする前に、暗号化する属性を決めておく必要があります。

**警告:** いったんデータをクリアテキスト形式で eDirectory にロードしたら、属性を暗号化対象としてマークしないでください。そうすることもできますが、その場合はセキュリティの問題が発生します。

**1b** 新たにフォーマットされ、パーティションが作成されたディスクで、クリアインストール (場合によっては OS も含めて) を行います。

これは、ディスクにクリアテキストデータが存在する可能性を排除するためです。つまり、以前クリアテキストデータが保存されていた既存のコンピュータに eDirectory を再インストールすることはできません。ディスクからデータのすべての痕跡を完全に消去する必要があります。eDirectory をインストールする前に、ディスクで安全な消去用ソフトウェアを使用する、磁気バルクイレーサーを使用するなど、データを徹底的に破壊する操作を行います。

**1c** eDirectory を設定し、属性に適用する暗号化方式を設定します。

**2** 暗号化する既存のデータが存在するレプリカリングにそのサーバを移動し、複製を実行した後、古いサーバをオフラインにします。

**3** 既存のすべてのクリアテキストデータを破壊します。

クリアテキストデータが格納されているディスク (またはその他の媒体) を完全に消去してください。消去する対象には、サーバのバルクロードに使われたクリアテキストの LDIF ファイル、複製に使われた他のサーバ、古いバックアップが残っているテープなどが含まれます。

## バックアップおよび復元を利用する方法

**1** 新しいサーバで次のように暗号化を設定します。

**1a** どの属性をどの方式で暗号化するかをあらかじめ決めておきます。

つまり、データをクリアテキスト形式で eDirectory にアップロードする前に、暗号化する属性を決めておく必要があります。

**警告:** いったんデータをクリアテキスト形式で eDirectory にロードしたら、属性を暗号化対象としてマークしないでください。そうすることもできますが、その場合は Note A で説明しているセキュリティの問題が発生します。

**1b** 新たにフォーマットされ、パーティションが作成されたディスクで、クリアインストール (場合によっては OS も含めて) を行います。

これは、ディスクにクリアテキストデータが存在する可能性を排除するためです。つまり、以前クリアテキストデータが保存されていた既存のコンピュータに eDirectory を再インストールすることはできません。ディスクからデータのすべての痕跡を完全に消去する必要があります。eDirectory をインストールする前に、ディスクで安全な消去用ソフトウェアを使用する、磁気バルクイレーサーを使用するなど、データを徹底的に破壊する操作を行います。

**1c** eDirectory を設定し、属性に適用する暗号化方式を設定します。

**2** 新しいサーバで、バックアップされた DIB (既存のクリアテキストデータが格納されている) を復元します。DIB クローンまたはホットバックアップを使って DIB をバックアップできます。

**3** 既存のすべてのクリアテキストデータを破壊します。

クリアテキストデータが格納されているディスク (またはその他の媒体) を完全に消去してください。消去する対象には、サーバのバルクロードに使われたクリアテキストの LDIF ファイル、複製に使われた他のサーバ、古いバックアップが残っているテープなどが含まれます。

## データの暗号化方式を変更する

バックアップと復元を利用してこの操作を行うには、次の手順を実行します。

- 1 属性の暗号化アルゴリズムを変更します。
- 2 DIB のバックアップをとります。DIB クローンまたはホットバックアップを使って DIB をバックアップできます。
- 3 バックアップされた DIB を新しいサーバ上で復元し、古いサーバを削除します。
- 4 古いサーバ上にあるすべての既存のクリアテキストデータを破壊します。そうすることで、古い暗号化方式で暗号化されたデータの断片がハードディスクから一掃されます。

クリアテキストデータが格納されているディスク (またはその他の媒体) を完全に消去してください。消去する対象には、サーバのバルクロードに使われたクリアテキストの LDIF ファイル、複製に使われた他のサーバ、古いバックアップが残っているテープなどが含まれます。

## まとめ

ここで説明したシナリオ以外にも、この問題が発生する状況はあり得ます。「最終的に暗号化される情報をハードディスク (またはその他の媒体) にクリアテキストの形式で書き込まない」という規則を守っている限り、暗号化データの完全な安全性が確保されます。

# 10

## Novell eDirectory データベースの修復

修復ユーティリティを使用すると、Novell® eDirectory™ ツリーのデータベースを保守および修復することができます。このユーティリティでは、次の操作を実行できます。

- ◆ 不正なレコード、スキーマの不一致、不正なサーバアドレス、外部参照など、eDirectory の問題の修正
- ◆ eDirectory スキーマへの詳細な変更
- ◆ データベースの終了やユーザの介入を伴わない、自動的なデータベースの構造チェック
- ◆ データベースのオペレーショナルインデックスの確認
- ◆ 空のレコードを破棄することによる空き領域の増量
- ◆ ローカルデータベースの修復
- ◆ レプリカ、レプリカリングおよびサーバオブジェクトの修復
- ◆ 同期エラーに対する、各ローカルパーティションの各サーバの分析
- ◆ ローカルデータベース内のオブジェクトの検出と同期

すべての eDirectory データベースの問題が致命的であるというわけではなく、eDirectory によって処理を続行できる問題もあります。ただしデータベースが破損すると、ローカルデータベースを開くことができないことを知らせるメッセージがコンソールに表示されます。この場合、修復を実行するか Novell サポートに連絡します。

eDirectory に問題が発生したり Novell サポートから指示がない限り、修復操作を実行することはお勧めできません。ただし、修復ユーティリティおよび他の Novell ユーティリティ (Novell iMonitor など) の診断機能を使用することはお勧めします。詳細については、[197 ページの第 7 章「Novell iMonitor 2.1 の使用」](#)を参照してください。

Novell iManager には次の修復ウィザードが含まれています。

| ウィザード          | 説明  |
|----------------|---|
| 基本修復ウィザード      | 標準修復、ローカルデータベースの修復、または単一オブジェクトの修復を実行できます。また、外部参照をチェックして不明なリーフオブジェクトを削除できます。 |
| ログファイルウィザード    | 修復ログファイルを開いて、ログファイルオプションを設定できます。  |
| iMonitor による修復 | iMonitor を開いて、このプログラムの修復オプションを使用できます。                                       |

| ウィザード           | 説明  |
|-----------------|---|
| レプリカ修復ウィザード     | すべてまたは選択したレプリカの修復、タイムスタンプの修復と新しいエポックの宣言、現在のサーバを新しいマスターレプリカに設定、および必要に応じて選択したレプリカの削除などを実行できます。                          |
| レプリカリングの修復ウィザード | すべてまたは選択したレプリカリングの修復、リング内のすべてのサーバにすべてのオブジェクトを送信、選択したレプリカでマスターレプリカのすべてのオブジェクトを受信、および必要に応じてレプリカリングから現在のサーバの削除などを実行できます。 |
| スキーマの保守ウィザード    | ツリーからスキーマを要求、ローカルスキーマのリセット、新規スキーマエポックの宣言、オプションスキーマ拡張機能の実行、リモートスキーマのインポート、および Post NetWare® 5 スキーマの更新などを実行できます。        |
| サーバの修復ウィザード     | すべてのネットワークアドレスの修復、およびサーバのネットワークアドレスのみの修復ができます。  |
| 同期修復ウィザード       | 現在のサーバで選択したレプリカの同期、現在のサーバの同期ステータスのレポート、すべてのサーバの同期ステータスのレポート、時刻同期の実行、および即時同期のスケジュールが実行できます。                            |

ウィザードは、次のような操作のときに役立ちます。

- ◆ [266 ページの「基本修復操作の実行」](#)
- ◆ [271 ページの「修復ログファイルの表示と設定」](#)
- ◆ [272 ページの「Novell iMonitor での修復の実行」](#)
- ◆ [272 ページの「レプリカの修復」](#)
- ◆ [275 ページの「レプリカリングを修復する」](#)
- ◆ [278 ページの「スキーマの保守」](#)
- ◆ [281 ページの「サーバのネットワークアドレスの修復」](#)
- ◆ [282 ページの「同期化操作を実行する」](#)
- ◆ [285 ページの「DSRepair の詳細オプション」](#)
- ◆ [289 ページの「eMBox クライアントを使用したデータベースの修復」](#)

## 基本修復操作の実行

基本修復ウィザードでは、標準修復、ローカルデータベースの修復、または単一オブジェクトの修復を実行できます。また、外部参照をチェックして不明なリーフオブジェクトを削除できます。

- ◆ [267 ページの「標準修復を実行する」](#)
- ◆ [269 ページの「ローカルデータベースの修復の実行」](#)
- ◆ [269 ページの「外部参照のチェック」](#)
- ◆ [270 ページの「単一オブジェクトの修復」](#)
- ◆ [270 ページの「不明なリーフオブジェクトの削除」](#)

## 標準修復を実行する

標準修復では、指定されたサーバの eDirectory データベースファイルに致命的な eDirectory エラーがないかチェックし、修復します。このオプションは、実行されるたびに 8 つの主要な操作を実行します。これらの操作には、管理者が関与する必要はありません。これらの操作の中には、実行中にデータベースをロックするものがあります。標準修復では、ローカルデータベースファイルのセットが一時的に作成され、修復操作はこれらのファイルに対して実行されます。つまり、重大な問題が発生したとしても、オリジナルのファイルは無事です。

ローカルデータベースの修復で使用される対話式オプションを熟知していない場合は、この修復手段をお勧めします。標準修復を実行すると、データベースファイルが現在使用している 2 倍の容量の空きディスクが必要になる場合があります。詳細については、[269 ページの「ローカルデータベースの修復の実行」](#)を参照してください。


eDirectory が使用するオペレーショナルインデックスの再構築は、ローカルデータベースがロックされているときのみ可能です。

次の表に、標準修復の実行中に行われる操作について示します。

| 操作                     | データベースのロック | 説明   |
|------------------------|------------|--|
| データベース構造およびインデックスのチェック | する         | データベースレコードとインデックスの構造および形式を調べます。eDirectory 環境のデータベースレベルで構造的な破損が組み込まれていないことを確認します。   |
| データベース全体の再構築           | する         | 構造チェックおよびインデックスチェック中に見つかったエラーを解決します。正しいデータ構造を復元し、eDirectory データベースおよびインデックスファイルを再作成します。  |
| ツリー構造のチェックの実行          | する         | データベースレコード間のリンクを検証し、各チャイルドレコードに対して有効なペアレントレコードがあることを確認します。これは、データベースの整合性を確認するのに役立ちます。無効なレコードにはマークがつけられ、eDirectory レプリカ同期処理の実行中に別のパーティションレプリカから復元できます。  |
| すべてのローカルレプリカを修復        | する         | 各オブジェクトと属性をスキーマ定義でチェックし、eDirectory データベースの不整合を解決します。ここでは、内部データ構造の形式もすべてチェックします。<br><br>この操作では、データベースから無効なレコードを削除することにより、ツリー構造のチェック中に見つかった不整合も解決します。この結果、無効なレコードにリンクされているすべてのチャイルドレコードは、すべて孤立としてマークされます。これらの孤立レコードは失われませんが、この処理によって、データベースの再構築中に多数のエラーが発生する可能性があります。これは正常な反応で、孤立したオブジェクトはレプリカ同期の過程で自動的に再編成されます。 |
| ローカル参照をチェック            | する         | ローカル参照は、このファイルサーバ上の eDirectory データベース内で管理されているオブジェクトへのポインタです。この操作では、内部データベースのポインタを評価し、正しい eDirectory オブジェクトを指していることを確認します。無効な参照が見つかった場合は修正されます。オブジェクト間に存在する関係の数によって異なりますが、この操作は完了までにかかり時間がかかる場合があります。  |

| 操作                                  | データベースのロック | 説明  |
|-------------------------------------|------------|---|
| ネットワークアドレスの修復                       | しない        | eDirectory 内で保存しているサーバのネットワークアドレスを、ローカル SAP、SLP、または DNS テーブルで維持されている値でチェックし、eDirectory が現在も正確な情報を保持していることを確認します。矛盾が見つかった場合、eDirectory は正しい情報で更新されます。  |
| ストリームシンタックスファイルの検証                  | する         | ログインスクリプトなどのストリームシンタックスファイルは、eDirectory データベースの特殊領域に保存されます。この操作では、各ストリームシンタックスファイルが有効な eDirectory オブジェクトに関連付けられているかどうかをチェックします。関連付けられていないストリームシンタックスファイルは削除され、そのファイルを参照している属性はパージされます。  |
| メールディレクトリを検証する (NetWare のみ)         | する         | デフォルトでは、eDirectory はメールディレクトリを NetWare <sup>®</sup> サーバの sys:mail ディレクトリ内に作成します。これは以前のバインダリユーザをサポートするためです。バインダリユーザのログインスクリプトは、ユーザのメールディレクトリに保存されます。この操作では、各メールディレクトリが有効な eDirectory ユーザオブジェクトに関連付けられているかどうかをチェックします。関連付けられていない場合、メールディレクトリは削除されます。  |
| ボリュームオブジェクトとトラスティのチェック (NetWare のみ) | しない        | <p>NetWare サーバ上の各ボリュームが、eDirectory 内のボリュームオブジェクトに関連付けられていることを確認します。関連付けられていない場合、サーバが存在するコンテキストを検索し、ボリュームオブジェクトが存在しているかどうか確認します。ボリュームオブジェクトが存在しない場合は、ボリュームオブジェクトを作成します。</p> <p>ボリューム情報を検証後、トラスティ ID のリストが検証されます。eDirectory 内のすべてのオブジェクトには固有のトラスティ ID があります。この ID は、NetWare ボリュームなど eDirectory ツリー内の他のオブジェクトに権利を与える際に使用されます。この作業では、ボリュームリストにある各トラスティ ID が有効な eDirectory オブジェクトであることを確認します。そうでない場合、トラスティ ID はボリュームリストから削除されます。</p> |

標準修復を実行するには、次の操作を行います。

- 1 Novell iManager で、[役割およびタスク] ボタン  をクリックします。
- 2 [eDirectory Maintenance Utilities (eDirectory 保守ユーティリティ)] > [基本修復] の順にクリックします。
- 3 操作を実行するサーバを指定し、[次へ] をクリックします。
- 4 操作を実行するサーバのユーザ名、パスワード、およびコンテキストを指定し、[次へ] をクリックします。
- 5 [標準修復] をクリックし、[開始] をクリックします。
- 6 表示される指示に従って、操作を完了します。




## ローカルデータベースの修復の実行

eDirectory でオープンおよびアクセスできるように、この修復操作を使用してローカルデータベースの矛盾を解決します。

ローカルデータベースの修復は、一時ファイルセットに対して実行するように指定することもできます。一時ファイルセットを指定しなかった場合、修復操作はアクティブなデータベースに対して実行されます。

一時データベースファイルセットに対して修復操作を実行する場合は、この操作中はデータベースを閉じておく必要があります。操作対象を一時ファイルセットにした場合、修復結果を反映する前に、その確認を求めるメッセージが表示されます。それ以外の場合、修復結果は即座に反映されます。


修復操作が終了すると、その修復操作のログを表示して、修復を完了させるのにさらに必要な操作があるかどうかを確認できます。詳細については、[271 ページの「修復ログファイルの表示と設定」](#)を参照してください。

- 1 Novell iManager で、[役割およびタスク] ボタン  をクリックします。
- 2 [eDirectory Maintenance Utilities (eDirectory 保守ユーティリティ)] > [基本修復] の順にクリックします。
- 3 操作を実行するサーバを指定し、[次へ] をクリックします。
- 4 操作を実行するサーバのユーザ名、パスワード、およびコンテキストを指定し、[次へ] をクリックします。
- 5 [ローカルデータベースの修復] をクリックし、[次へ] をクリックします。
- 6 ローカル修復を実行するオプションを指定し、[開始] をクリックします。
- 7 表示される指示に従って、操作を完了します。

## 外部参照のチェック

この修復操作は、各外部参照オブジェクトをチェックして、そのオブジェクトを含むレプリカがあるかどうかを調べます。オブジェクトのあるパーティションのレプリカが含まれているすべてのサーバにアクセスできない場合、オブジェクトは見つかりません。オブジェクトが見つからない場合、警告が表示されます。

この操作では破損情報も表示されます。


- 1 Novell iManager で、[役割およびタスク] ボタン  をクリックします。
- 2 [eDirectory Maintenance Utilities (eDirectory 保守ユーティリティ)] > [基本修復] の順にクリックします。
- 3 操作を実行するサーバを指定し、[次へ] をクリックします。
- 4 操作を実行するサーバのユーザ名、パスワード、およびコンテキストを指定し、[次へ] をクリックします。
- 5 [外部参照のチェック] をクリックし、[開始] をクリックします。
- 6 表示される指示に従って、操作を完了します。

## 単一オブジェクトの修復

この修復操作は、eDirectory がデータへアクセスするのを妨げるような、eDirectory オブジェクトの不整合を解決します。この操作は、ユーザ作成のパーティションおよび外部参照パーティションでのみ有効です。

この操作は、アクティブなデータベースファイルに対して実行されます。破損が物理的なレベルの場合は、まず物理チェックおよび構造チェックを実行してから単一オブジェクトの修復を行います。

修復操作時点の eDirectory データベースのバックアップコピーを保持していることを確認します。


- 1 Novell iManager で、[役割およびタスク] ボタン  をクリックします。
- 2 [eDirectory Maintenance Utilities (eDirectory 保守ユーティリティ)] > [基本修復] の順にクリックします。
- 3 操作を実行するサーバを指定し、[次へ] をクリックします。
- 4 操作を実行するサーバのユーザ名、パスワード、およびコンテキストを指定し、[次へ] をクリックします。
- 5 [単一オブジェクトの修復] をクリックし、[開始] をクリックします。
- 6 修復するオブジェクトを指定し、[次へ] をクリックします。
- 7 表示される指示に従って、操作を完了します。

## 不明なリーフオブジェクトの削除

オブジェクトに必須プロパティがない場合、あるいはその他に無効な点がある場合(プロパティがオブジェクトタイプの最低要件を満たしていない場合)、修復によって一貫性のないオブジェクトが不明なオブジェクトに変更されます。不明なオブジェクトは実際のオブジェクトであり、eDirectory 側では既知のオブジェクトです。不明なオブジェクトになっているのは、オブジェクトクラスの検証が不完全なためです。疑問符アイコンで表示される不明なオブジェクトは削除できますが、簡単に元のオブジェクトタイプに戻すことはできません。

この修復操作では、ローカル eDirectory データベースのオブジェクトのうち、オブジェクトクラスが不明で、サブオーディネートオブジェクトを維持していないオブジェクトをすべて削除します。削除は eDirectory ツリーの他のレプリカと同時に後で行われます。

**重要:** この操作の意味を完全に理解しているか Novell サポートから実行の指示がない限り、この操作は実行しないでください。

- 1 Novell iManager で、[役割およびタスク] ボタン  をクリックします。
- 2 [eDirectory Maintenance Utilities (eDirectory 保守ユーティリティ)] > [基本修復] の順にクリックします。
- 3 操作を実行するサーバを指定し、[次へ] をクリックします。
- 4 操作を実行するサーバのユーザ名、パスワード、およびコンテキストを指定し、[次へ] をクリックします。
- 5 [不明なリーフオブジェクトの削除] をクリックし、[開始] をクリックします。
- 6 表示される指示に従って、操作を完了します。

## 修復ログファイルの表示と設定

修復ログファイルには、ローカルパーティションとサーバに関する詳細情報が含まれます。この情報はデータベースの破損を診断するのに役立ちます。ログファイルウィザードでは、修復ログファイルを開いてログファイルオプションを設定できます。


このセクションでは、次の操作について説明します。

- ◆ [271 ページの「ログファイルを開く」](#)
- ◆ [271 ページの「ログファイルオプションを設定する」](#)

### ログファイルを開く


この操作を行って、修復ログファイルを表示します。ログファイルのデフォルト名は dsrepair.log です。修復操作の結果は、このログファイルに書き込まれます。

ログファイル操作のオン/オフ切り替え、名前の変更、およびログファイルの削除またはリセットなどができます。詳細については、[271 ページの「ログファイルオプションを設定する」](#)を参照してください。

- 1 Novell iManager で、[役割およびタスク] ボタン  をクリックします。
- 2 [eDirectory Maintenance Utilities (eDirectory 保守ユーティリティ)] > [ログファイル] の順にクリックします。
- 3 操作を実行するサーバを指定し、[次へ] をクリックします。
- 4 操作を実行するサーバのユーザ名、パスワード、およびコンテキストを指定し、[次へ] をクリックします。
- 5 [ログファイルを開く] をクリックし、[開く] をクリックします。
- 6 表示される指示に従って、操作を完了します。

### ログファイルオプションを設定する

この操作を行って、修復ログファイルを管理します。ログファイルのオン/オフ切り替え、ログファイルの削除、追加、ファイル名の変更などが行えます。


- 1 Novell iManager で、[役割およびタスク] ボタン  をクリックします。
- 2 [eDirectory Maintenance Utilities (eDirectory 保守ユーティリティ)] > [ログファイル] の順にクリックします。
- 3 操作を実行するサーバを指定し、[次へ] をクリックします。
- 4 操作を実行するサーバのユーザ名、パスワード、およびコンテキストを指定し、[次へ] をクリックします。
- 5 [ログファイルオプション] をクリックし、[次へ] をクリックします。
- 6 表示される指示に従って、操作を完了します。

## Novell iMonitor での修復の実行

Novell iManager の [iMonitor による修復] オプションを使用して、修復機能にアクセスできます。iMonitor の [修復] ページでは、問題を表示したり、eDirectory データベースのバックアップやクリーンアップを実行できます。

iMonitor では、DSRepair 機能はサーバ限定の機能です。つまり、この機能は iMonitor が実行されているローカルサーバでのみ使用できます。他のサーバで実行されているこの機能にアクセスするには、そのサーバで実行されている iMonitor に切り替える必要があります。

[DS Repair] ページにアクセスするには、アクセスしようとするサーバの管理者またはコンソールオペレータと同等の権利が必要です。つまり、このページの情報にアクセスするには、まずログインして認証情報のチェックを受ける必要があります。

- 1 Novell iManager で、[役割およびタスク] ボタン  をクリックします。
- 2 [eDirectory Maintenance Utilities (eDirectory 保守ユーティリティ)] > [iMonitor による修復] の順にクリックします。
- 3 操作を実行するサーバを指定し、[OK] をクリックします。  
手動で iMonitor を開いて修復オプションを実行するには、[iMonitor を実行して iMonitor から修復にアクセスする] をクリックした後で [OK] をクリックします。
- 4 アクセスするサーバのユーザ名、コンテキスト、およびパスワードを指定してから [OK] をクリックし、[iMonitor 修復] ページを開きます。
- 5 修復オプションを指定し、[修復の開始] をクリックします。

iMonitor で利用可能な修復機能の詳細については、213 ページの「DSRepair 情報の表示」を参照してください。

## レプリカの修復

レプリカの修復操作では、レプリカの各オブジェクトとスキーマとの整合性が保たれているかどうか、オブジェクトの各属性とスキーマとの整合性が保たれているかどうかをチェックし、属性の構文に従ってデータをチェックします。レプリカに関連する他の内部データ構造もチェックされます。


レプリカの修復ウィザードを使用して、次の操作を実行します。

- ◆ 273 ページの「すべてのレプリカを修復する」
- ◆ 273 ページの「選択したレプリカを修復する」
- ◆ 273 ページの「タイムスタンプを修復する」
- ◆ 274 ページの「このサーバを新しいマスタレプリカに設定する」
- ◆ 275 ページの「選択したレプリカを削除する」

## すべてのレプリカを修復する

この操作では、レプリカテーブルに表示されたすべてのレプリカを修復します。


30 分前までにローカル eDirectory データベースの修復操作を行っていない場合、この操作を実行する前にローカルデータベースを修復してください。詳細については、[269 ページ](#)の「[ローカルデータベースの修復の実行](#)」を参照してください。

- 1 Novell iManager で、[役割およびタスク] ボタン  をクリックします。
- 2 [eDirectory Maintenance Utilities (eDirectory 保守ユーティリティ)] > [レプリカの修復] の順にクリックします。
- 3 操作を実行するサーバを指定し、[次へ] をクリックします。
- 4 操作を実行するサーバのユーザ名、パスワード、およびコンテキストを指定し、[次へ] をクリックします。
- 5 [すべてのレプリカの修復] をクリックし、[開始] をクリックします。
- 6 表示される指示に従って、操作を完了します。

## 選択したレプリカを修復する

この操作では、レプリカビューに表示されているレプリカのうち、選択したレプリカのみ修復します。

30 分前までにローカル eDirectory データベースの修復操作を行っていない場合、この操作を実行する前にローカルデータベースを修復してください。詳細については、[269 ページ](#)の「[ローカルデータベースの修復の実行](#)」を参照してください。

- 1 Novell iManager で、[役割およびタスク] ボタン  をクリックします。
- 2 [eDirectory Maintenance Utilities (eDirectory 保守ユーティリティ)] > [レプリカの修復] の順にクリックします。
- 3 操作を実行するサーバを指定し、[次へ] をクリックします。
- 4 操作を実行するサーバのユーザ名、パスワード、およびコンテキストを指定し、[次へ] をクリックします。
- 5 [選択したレプリカを修復する] をクリックし、[次へ] をクリックします。
- 6 修復するレプリカを指定し、[開始] をクリックします。
- 7 表示される指示に従って、操作を完了します。

## タイムスタンプを修復する

注：この操作を行う前に、同期修復ウィザードを使用して、レプリカリング内のすべてのサーバが正しく通信していることを確認します。詳細については、[282 ページ](#)の「[同期化操作を実行する](#)」を参照してください。

この操作では、選択したパーティションのレプリカをすべて最新版に更新するために、マスタレプリカの新しい参照ポイントを指定します。

この操作は、常にパーティションのマスタレプリカ上で実行されます。マスタレプリカは、このサーバのローカルレプリカである必要はありません。


オブジェクトが作成または変更されるとタイムスタンプが設定されますが、これは固有でなければなりません。マスタレプリカのすべてのタイムスタンプが検査されます。タイムスタンプが現在のネットワーク時間より遅れている場合、新しいタイムスタンプに置き換えられます。タイムスタンプが最新であれば、新しいタイムスタンプは発行されません。すべてのタイムスタンプの時刻が一致すると、新規エポックが宣言されます。

この操作は、レプリカのオブジェクト間、またはオブジェクトのプロパティ間で矛盾が生じている場合に使用します。たとえば、ログインスクリプトを更新したのにログイン時に古いログインスクリプトが表示される場合は、レプリカ間で正しく同期が取られているかどうかを確認してください。将来のタイムスタンプと現在の時刻の時間差が1分以内であれば、最終的に eDirectory 自体がその状況を修正します。新規エポックの宣言は非常に費用のかかる操作であり、定期的な使用はお勧めしていません。

Novell eDirectory はデータベースとして厳密な整合性はとられていません。したがってそのレプリカ同期の確認には5～10分かかることがあります。この操作を行うと、次の状態になります。

- ◆ 新規エポックがマスタレプリカで宣言され、その影響がマスタレプリカのすべてのオブジェクトに及ぶ可能性があります。
- ◆ すべてのタイムスタンプが調べられ、必要に応じて修復されます。
- ◆ レプリカ間の同期が取られるまで、日付の古いタイムスタンプ(エポック)を保持するレプリカからの更新内容は受け付けられません。
- ◆ レプリカは、マスタレプリカまたは新規エポックを受信済みの他のレプリカのすべてのオブジェクトのコピーを受け取ります。
- ◆ このレプリカは、マスタレプリカと同じエポックになります。
- ◆ 以前のエポックからの変更内容は失われます。
- ◆ マスタレプリカが現在のサーバに存在する必要はありませんが、この修復操作を実行するにはマスタレプリカに対するスーパーバイザ権が必要です。
- ◆ そのほかのレプリカは新しい状態になります。

タイムスタンプを修復して新規エポックを宣言するには、次の操作を行います。


- 1** Novell iManager で、[役割およびタスク] ボタン  をクリックします。
- 2** [eDirectory Maintenance Utilities (eDirectory 保守ユーティリティ)] > [レプリカの修復] の順にクリックします。
- 3** 操作を実行するサーバを指定し、[次へ] をクリックします。
- 4** 操作を実行するサーバのユーザ名、パスワード、およびコンテキストを指定し、[次へ] をクリックします。
- 5** [タイムスタンプを修復して新しいエポックを宣言する] をクリックし、[次へ] をクリックします。
- 6** 表示される指示に従って、操作を完了します。

## このサーバを新しいマスタレプリカに設定する

この操作では、選択したパーティションのローカルレプリカをマスタレプリカとして設定します。元のマスタレプリカを損失した場合には、この操作で新しいマスタレプリカを設定できます。マスタレプリカがあるサーバでハードディスク障害が発生すると、そのマスタレプリカが失われることがあります。その場合は、マスタレプリカを変更する必要があります。

Novell iManager で使用可能な通常のパーティション操作を実行するためには、このオプションを使用しないでください。詳細については、[135 ページの第 5 章「パーティションおよびレプリカの管理」](#)を参照してください。




- 1 Novell iManager で、[役割およびタスク] ボタン  をクリックします。
- 2 [eDirectory Maintenance Utilities (eDirectory 保守ユーティリティ)] > [レプリカの修復] の順にクリックします。
- 3 新しいマスタレプリカに指定するサーバを指定し、[次へ] をクリックします。
- 4 ユーザ名、パスワード、およびコンテキストを指定してサーバへの認証を行い、[次へ] をクリックします。
- 5 [このサーバを新しいマスタレプリカに設定] をクリックし、[次へ] をクリックします。
- 6 表示される指示に従って、操作を完了します。

## 選択したレプリカを削除する

この操作では、選択したレプリカをこのサーバから削除します。レプリカは削除されるか、サブオーディネートリファレンスに変更されます。

Novell iManager で使用可能な通常のパーティション操作を実行するためには、このオプションを使用しないでください。詳細については、[135 ページの第 5 章「パーティションおよびレプリカの管理」](#)を参照してください。

- 1 Novell iManager で、[役割およびタスク] ボタン  をクリックします。
- 2 [eDirectory Maintenance Utilities (eDirectory 保守ユーティリティ)] > [レプリカの修復] の順にクリックします。
- 3 削除するレプリカを含むサーバを指定し、[次へ] をクリックします。
- 4 ユーザ名、パスワード、およびコンテキストを指定してサーバへの認証を行い、[次へ] をクリックします。
- 5 [選択したレプリカを削除する] をクリックし、[次へ] をクリックします。
- 6 削除するレプリカを指定し、[次へ] をクリックします。
- 7 表示される指示に従って、操作を完了します。

## レプリカリングを修復する

レプリカリングの修復操作では、レプリカを保持する各サーバのレプリカリング情報をチェックし、リモート ID 情報を検証します。


レプリカリング修復ウィザードを使用して、次の操作を実行します。

- ◆ [276 ページの「すべてのレプリカリングを修復する」](#)
- ◆ [276 ページの「選択したレプリカリングを修復する」](#)
- ◆ [276 ページの「リング内のすべてのサーバにすべてのオブジェクトを送信する」](#)
- ◆ [277 ページの「マスタから選択したレプリカへすべてのオブジェクトを受信する」](#)
- ◆ [277 ページの「レプリカリングからこのサーバを削除する」](#)

## すべてのレプリカリングを修復する

この操作では、レプリカビューに表示されたすべてのレプリカのレプリカリングを修復します。


30分前までにローカル eDirectory データベースの修復操作を行っていない場合、この操作を実行する前にローカルデータベースを修復してください。詳細については、[269 ページ](#)の「[ローカルデータベースの修復の実行](#)」を参照してください。

- 1 Novell iManager で、[役割およびタスク] ボタン  をクリックします。
- 2 [eDirectory Maintenance Utilities (eDirectory 保守ユーティリティ)] > [レプリカリングの修復] の順にクリックします。
- 3 操作を実行するサーバを指定し、[次へ] をクリックします。
- 4 操作を実行するサーバのユーザ名、パスワード、およびコンテキストを指定し、[次へ] をクリックします。
- 5 [Repair All Replica Rings (すべてのレプリカリングを修復)] をクリックし、[次へ] をクリックします。
- 6 表示される指示に従って、操作を完了します。

## 選択したレプリカリングを修復する

この操作では、レプリカテーブルで選択したレプリカのレプリカリングを修復します。

30分前までにローカル eDirectory データベースの修復操作を行っていない場合、この操作を実行する前にローカルデータベースを修復してください。詳細については、[269 ページ](#)の「[ローカルデータベースの修復の実行](#)」を参照してください。

- 1 Novell iManager で、[役割およびタスク] ボタン  をクリックします。
- 2 [eDirectory Maintenance Utilities (eDirectory 保守ユーティリティ)] > [レプリカリングの修復] の順にクリックします。
- 3 操作を実行するサーバを指定し、[次へ] をクリックします。
- 4 操作を実行するサーバのユーザ名、パスワード、およびコンテキストを指定し、[次へ] をクリックします。
- 5 [Repair the Selected Replica Ring (選択されたレプリカリングを修復)] をクリックし、[次へ] をクリックします。
- 6 修復するレプリカを指定し、[次へ] をクリックします。
- 7 表示される指示に従って、操作を完了します。

## リング内のすべてのサーバにすべてのオブジェクトを送信する


この操作では、レプリカリング内で選択したサーバから、選択したパーティションのレプリカを含む他のすべてのサーバに、すべてのオブジェクトを送信します。

レプリカリング内で選択したサーバ上の選択したパーティションのレプリカが、レプリカリング内の他のすべてのサーバと同期していることを確かめるには、この操作を行います。該当するパーティションのサブオーディネートリファレンスレプリカのみを保持するサーバではこの操作は実行できません。

選択したサーバに保持されているレプリカとまだ同期していない他のレプリカに加えられた変更は失われます。この操作を実行する前に、同期ステータスを確認してください。

**重要:** この操作はレプリカ内のオブジェクトを再作成するため、ネットワークトラフィックの量が大幅に増加する可能性があります。これは診断操作ではありません。




- 1 Novell iManager で、[役割およびタスク] ボタン  をクリックします。
- 2 [eDirectory Maintenance Utilities (eDirectory 保守ユーティリティ)] > [レプリカリングの修復] の順にクリックします。
- 3 操作を実行するサーバを指定し、[次へ] をクリックします。
- 4 サーバのユーザ名、パスワード、およびコンテキストを指定して、[次へ] をクリックします。
- 5 [リング内の各サーバにすべてのオブジェクトを送信する] をクリックし、[次へ] をクリックします。
- 6 表示される指示に従って、操作を完了します。

## マスタから選択したレプリカへすべてのオブジェクトを受信する

この操作では、選択したサーバ上のレプリカで、マスタレプリカのすべてのオブジェクトを受信します。

レプリカリング内で選択したサーバ上の選択したパーティションのレプリカが、マスタレプリカと同期していることを確かめるには、この操作を行います。この操作は、マスタレプリカがあるサーバでは実行できません。


**重要:** この操作を行うと、ネットワークトラフィックの量が大幅に増加します。この操作を要求することにより、現在のレプリカは、サーバに新しいレプリカがあるかのように動作します。さらに、レプリカの状態は新規になります。

- 1 Novell iManager で、[役割およびタスク] ボタン  をクリックします。
- 2 [eDirectory Maintenance Utilities (eDirectory 保守ユーティリティ)] > [レプリカリングの修復] の順にクリックします。
- 3 操作を実行するサーバを指定し、[次へ] をクリックします。
- 4 サーバのユーザ名、パスワード、およびコンテキストを指定して、[次へ] をクリックします。
- 5 [マスタから選択したレプリカにすべてのオブジェクトを受信する] をクリックし、[次へ] をクリックします。
- 6 表示される指示に従って、操作を完了します。

## レプリカリングからこのサーバを削除する

この操作では、現在のサーバに保存されているレプリカのうち、選択したレプリカから特定のサーバを削除します。

**警告:** この操作を誤用すると、eDirectory データベースで致命的な破損が生じることがあります。Novell サポート担当者からの指示がない限り、この操作は実行しないでください。

- 1 Novell iManager で、[役割およびタスク] ボタン  をクリックします。
- 2 [eDirectory Maintenance Utilities (eDirectory 保守ユーティリティ)] > [レプリカリングの修復] の順にクリックします。
- 3 操作を実行するサーバを指定し、[次へ] をクリックします。
- 4 サーバのユーザ名、パスワード、およびコンテキストを指定して、[次へ] をクリックします。
- 5 [レプリカリングからこのサーバを削除] をクリックし、[次へ] をクリックします。
- 6 表示される指示に従って、操作を完了します。

# スキーマの保守

スキーマとはオブジェクト属性のルールおよび定義を体系化したもので、これにより、各オブジェクトの内容と形式が構築され、データベース内でのオブジェクト間の関係が確立されます。

スキーマの保守ウィザードには、eDirectory サーバのスキーマを [Root] のマスタに合わせるために必要なスキーマ操作がいくつか用意されています。ただし、これらの操作は必要なときだけ使用してください。スキーマは、ローカル修復操作および標準修復操作によってすでに検査されています。

eDirectory スキーマの詳細については、123 ページの第 4 章「スキーマの管理」を参照してください。


スキーマの保守ウィザードを使用して、次の操作を実行します。

- ◆ 278 ページの「ツリーからスキーマを要求する」
- ◆ 278 ページの「ローカルスキーマをリセットする」
- ◆ 279 ページの「Post-NetWare 5 スキーマの更新を実行する」
- ◆ 279 ページの「オプションスキーマ拡張機能を実行する」
- ◆ 280 ページの「リモートスキーマをインポートする」
- ◆ 280 ページの「新規スキーマエポックを宣言する」

## ツリーからスキーマを要求する

この操作を実行すると、ツリーのルートのマスタレプリカが自身のスキーマをこのサーバのスキーマに同期させます。[Root] のマスタレプリカからこのサーバのスキーマに対して行われた変更は、24 時間以内に伝達されます。


**重要:** すべてのサーバがマスタレプリカのスキーマを要求すると、ネットワークトラフィックが増加します。そのため、このオプションの使用には細心の注意を払うようにしてください。

- 1 Novell iManager で、[役割およびタスク] ボタン  をクリックします。
- 2 [eDirectory Maintenance Utilities (eDirectory 保守ユーティリティ)] > [スキーマの保守] の順にクリックします。
- 3 操作を実行するサーバを指定し、[次へ] をクリックします。
- 4 操作を実行するサーバのユーザ名、パスワード、およびコンテキストを指定し、[次へ] をクリックします。
- 5 [ツリーからスキーマを要求] をクリックし、[次へ] をクリックします。
- 6 表示される指示に従って、操作を完了します。

## ローカルスキーマをリセットする

この操作は、ローカルスキーマのタイムスタンプをクリアし、着信スキーマの同期を要求するスキーマリセット機能呼び出します。

[Root] パーティションのマスタレプリカから実行した場合、この操作はできません。ツリー内のすべてのサーバが同時にリセットされるわけではありません。

- 1 Novell iManager で、[役割およびタスク] ボタン  をクリックします。
- 2 [eDirectory Maintenance Utilities (eDirectory 保守ユーティリティ)] > [スキーマの保守] の順にクリックします。


- 3 操作を実行するサーバを指定し、[次へ] をクリックします。
- 4 操作を実行するサーバのユーザ名、パスワード、およびコンテキストを指定し、[次へ] をクリックします。
- 5 [ローカルスキーマをリセット] をクリックし、[次へ] をクリックします。
- 6 表示される指示に従って、操作を完了します。

## Post-NetWare 5 スキーマの更新を実行する

この操作では、Post-NetWare 5 DS の変更に伴い、互換性を確保するためにスキーマを拡張および変更します。

現在の eDirectory バージョンによっては、新しいバージョンにアップデートするときに、このオプションが必要な場合があります。このオプションが必要かどうかは、アップグレードする新しい eDirectory のリリースノートを参照してください。

この操作には、このサーバが [Root] パーティションのレプリカ ([Root] のマスタレプリカ推奨) を持ち、レプリカが使用可能な状態であることが必要になります。

- 1 Novell iManager で、[役割およびタスク] ボタン  をクリックします。
- 2 [eDirectory Maintenance Utilities (eDirectory 保守ユーティリティ)] > [スキーマの保守] の順にクリックします。
- 3 操作を実行するサーバを指定し、[次へ] をクリックします。
- 4 操作を実行するサーバのユーザ名、パスワード、およびコンテキストを指定し、[次へ] をクリックします。
- 5 [Post NetWare 5 スキーマの更新] をクリックし、[次へ] をクリックします。
- 6 表示される指示に従って、操作を完了します。


## オプションスキーマ拡張機能を実行する

この操作では、包含など拡張機能のためにスキーマを拡張および変更します。

この操作では、このサーバに [Root] パーティションのレプリカが含まれ、そのレプリカが使用可能な状態であることが必要になります。また、ツリー内のどの NetWare 4 サーバにも次のいずれかのバージョンの ds.nlm が搭載されている必要があります。

| サーバ        | バージョン           |
|------------|-----------------|
| 4.10       | ds.nlm v5.17 以降 |
| 4.11 / 4.2 | ds.nlm v6.01 以降 |

以前のバージョンの eDirectory では、このオプションで加えた変更の同期ができません。


- 1 Novell iManager で、[役割およびタスク] ボタン  をクリックします。
- 2 [eDirectory Maintenance Utilities (eDirectory 保守ユーティリティ)] > [スキーマの保守] の順にクリックします。
- 3 操作を実行するサーバを指定し、[次へ] をクリックします。
- 4 操作を実行するサーバのユーザ名、パスワード、およびコンテキストを指定し、[次へ] をクリックします。
- 5 [オプションスキーマ拡張機能] をクリックし、[次へ] をクリックします。
- 6 表示される指示に従って、操作を完了します。

## リモートスキーマをインポートする

この操作では、現在のツリーのスキーマに追加したいスキーマが含まれている eDirectory ツリーを選択します。

ツリーを選択すると、[Root] パーティションのマスタレプリカを保持するサーバに接続されます。現在のツリー上にあるスキーマの拡張には、そのサーバのスキーマが使用されます。

2つのツリーをマージするには、一方のツリーからもう一方のツリーへ繰り返しスキーマをインポートする必要があります。詳細については、[225 ページの第 8 章「Novell eDirectory ツリーのマージ」](#)を参照してください。

- 1 Novell iManager で、[役割およびタスク] ボタン  をクリックします。
- 2 [eDirectory Maintenance Utilities (eDirectory 保守ユーティリティ)] > [スキーマの保守] の順にクリックします。
- 3 操作を実行するサーバを指定し、[次へ] をクリックします。
- 4 操作を実行するサーバのユーザ名、パスワード、およびコンテキストを指定し、[次へ] をクリックします。
- 5 [リモートスキーマのインポート] をクリックし、[次へ] をクリックします。
- 6 表示される指示に従って、操作を完了します。

## 新規スキーマエポックを宣言する

エポックとは、基準点として任意に選択される瞬間のことです。時代や新規バージョンと同義です。エポックは、レプリカの同期を制御します。新規に宣言されると、マスタレプリカで機能します。他のレプリカは、新規エポックを持つレプリカに更新情報を送ることはできませんが、そのレプリカと完全に同期するまでは更新情報を受け取ります。


指定したパーティションの他のレプリカが更新済みレプリカと同期された場合、つまり各レプリカのエポックが同じになると、双方向の同期が再び許可されます。

新規スキーマエポックを宣言すると、[Root] パーティションのマスタレプリカを保持するサーバに接続され、スキーマレコード上の不正なタイムスタンプが修復されます。次にスキーマの新規エポックがそのサーバで宣言され、ツリー全体に影響を与えます。

他のすべてのサーバは、修復されたタイムスタンプを保持する新しいスキーマのコピーを受け取ります。

受け取る側のサーバが新規エポック内に存在しなかったスキーマを含む場合は、古いスキーマを使用するオブジェクトおよび属性が「不明」オブジェクトクラスまたは属性に変更されます。

**重要:** Novell サポートからの指示がない限り、この操作は実行しないでください。

- 1 Novell iManager で、[役割およびタスク] ボタン  をクリックします。
- 2 [eDirectory Maintenance Utilities (eDirectory 保守ユーティリティ)] > [スキーマの保守] の順にクリックします。
- 3 操作を実行するサーバを指定し、[次へ] をクリックします。
- 4 操作を実行するサーバのユーザ名、パスワード、およびコンテキストを指定し、[次へ] をクリックします。
- 5 [新規エポックの宣言] をクリックし、[次へ] をクリックします。
- 6 表示される指示に従って、操作を完了します。

## サーバのネットワークアドレスの修復

サーバの修復ウィザードでは、レプリカリングのすべてのサーバのネットワークアドレスとローカルデータベースのサーバオブジェクトを修復します。さらに、レプリカリングの指定したサーバのネットワークアドレスとローカルデータベースのサーバオブジェクトも修復できます。

サーバの修復ウィザードを使用して、次の操作を実行します。


- ◆ 281 ページの「すべてのネットワークアドレスを修復する」
- ◆ 281 ページの「サーバのネットワークアドレスを修復する」

### すべてのネットワークアドレスを修復する

この操作では、ローカル eDirectory データベース内で、すべてのサーバのネットワークアドレスをチェックします。使用できるトランスポートプロトコルに応じて、SAP テーブル、SLP ディレクトリエージェント、および DNS ローカルまたはリモート情報でサーバ名を検索します。

その後、eDirectory サーバオブジェクトのネットワークアドレス属性、およびすべてのパーティション [Root] オブジェクトの各レプリカ属性のアドレスレコードと、各アドレスが比較されます。アドレスが異なる場合は、同じになるように更新されます。


SAP テーブル、ローカル/リモート DNS 情報、または SLP ディレクトリエージェントにサーバのネットワークアドレスが見つからなければ、修復は行われません。

- 1 Novell iManager で、[役割およびタスク] ボタン  をクリックします。
- 2 [eDirectory Maintenance Utilities (eDirectory 保守ユーティリティ)] > [サーバの修復] の順にクリックします。
- 3 操作を実行するサーバを指定し、[次へ] をクリックします。
- 4 操作を実行するサーバのユーザ名、パスワード、およびコンテキストを指定し、[次へ] をクリックします。
- 5 [すべてのネットワークアドレスの修復] をクリックし、[次へ] をクリックします。
- 6 表示される指示に従って、操作を完了します。

### サーバのネットワークアドレスを修復する

この操作では、ローカル eDirectory データベース内で、選択したサーバのネットワークアドレスをチェックします。現在バインドされているトランスポートプロトコルに応じて、ローカル SAP テーブル、SLP ディレクトリエージェント、およびローカルまたはリモートの DNS 情報でサーバ名を検索します。ネットワークアドレスが見つければ、そのアドレスを eDirectory サーバオブジェクトのネットワークアドレス属性の値、およびすべてのパーティション [Root] オブジェクトのレプリカ属性のアドレスレコードと照合します。アドレスが異なる場合は、同じになるように更新されます。

SAP テーブル、SLP ディレクトリエージェント、またはローカル/リモート DNS 情報にサーバのネットワークアドレスが見つからなければ、修復は行われません。

- 1 Novell iManager で、[役割およびタスク] ボタン  をクリックします。
- 2 [eDirectory Maintenance Utilities (eDirectory 保守ユーティリティ)] > [サーバの修復] の順にクリックします。

- 3 操作を実行するサーバを指定し、[次へ] をクリックします。
- 4 操作を実行するサーバのユーザ名、パスワード、およびコンテキストを指定し、[次へ] をクリックします。
- 5 [このサーバのネットワークアドレスの修復] をクリックし、[次へ] をクリックします。
- 6 表示される指示に従って、操作を完了します。

## 問題

Novell SLP はオプションのパッケージです。認証機能は、Novell SLP パッケージの一部として実装されているわけではありません。

eDirectory は現在 OpenSLP と相互運用が可能で、OpenSLP の認証機能が使用されます。

## 同期化操作を実行する

同期修復ウィザードでは、現在のサーバで選択したレプリカの同期、現在のサーバの同期ステータスのレポート、すべてのサーバの同期ステータスのレポート、時刻同期の実行、および即時同期のスケジュールができます。

同期修復ウィザードを使用して、次の操作を実行します。


- ◆ 282 ページの「選択したレプリカをこのサーバで同期する」
- ◆ 283 ページの「このサーバの同期ステータスをレポートする」
- ◆ 283 ページの「すべてのサーバの同期ステータスをレポートする」
- ◆ 284 ページの「時刻同期を実行する」
- ◆ 284 ページの「即時同期をスケジュールする」

## 選択したレプリカをこのサーバで同期する

この操作では、選択したパーティションのレプリカを持つすべてのサーバ上で、完全な同期ステータスを確保します。

このオプションを使用して、パーティションの状態を確認できます。そのパーティションのレプリカを持つサーバがすべて正常に同期していれば、そのパーティションは異常なしと見なされます。レプリカリング内の各サーバが接続されると、次に、接続された各サーバは、レプリカリング内の他のすべてのサーバに対して、即時に同期を実行します。

サーバは、サーバ自体には同期されません。したがって、現在のサーバが所有するレプリカのステータスは「ホスト」として表示されます。

- 1 Novell iManager で、[役割およびタスク] ボタン  をクリックします。
- 2 [eDirectory Maintenance Utilities (eDirectory 保守ユーティリティ)] > [同期修復] の順にクリックします。
- 3 操作を実行するサーバを指定し、[次へ] をクリックします。
- 4 操作を実行するサーバのユーザ名、パスワード、およびコンテキストを指定し、[次へ] をクリックします。
- 5 [このサーバ上で選択したレプリカを同期する] をクリックし、[次へ] をクリックします。
- 6 表示される指示に従って、操作を完了します。




## このサーバの同期ステータスをレポートする

この操作では、現在のサーバ上にレプリカを持つすべてのパーティションのレプリカ同期ステータスをレポートします。

この操作では、パーティションのレプリカを保持する各サーバのレプリカの [Root] オブジェクトから同期ステータス属性を読み込みます。レポートには、すべてのサーバに対して正常に同期が行われた最終時刻と、最終同期以降発生したエラーが表示されます。

12 時間以内に同期が完了していない場合は、警告メッセージが表示されます。


- 1 Novell iManager で、[役割およびタスク] ボタン  をクリックします。
- 2 [eDirectory Maintenance Utilities (eDirectory 保守ユーティリティ)] > [同期修復] の順にクリックします。
- 3 操作を実行するサーバを指定し、[次へ] をクリックします。
- 4 操作を実行するサーバのユーザ名、パスワード、およびコンテキストを指定し、[次へ] をクリックします。
- 5 [Report the Sync Status on This Server (このサーバの同期ステータスのレポート)] をクリックし、[次へ] をクリックします。
- 6 表示される指示に従って、操作を完了します。

## すべてのサーバの同期ステータスをレポートする

この操作では、現在のサーバ上にレプリカを持つすべてのパーティションのレプリカ同期ステータスを確保します。

この操作では、パーティションのレプリカを保持する各サーバのレプリカの [Root] オブジェクトから同期ステータス属性を読み込みます。レポートには、すべてのサーバに対して正常に同期が行われた最終時刻と、最終同期以降発生したエラーが表示されます。

12 時間以内に同期が完了していない場合は、警告メッセージが表示されます。

- 1 Novell iManager で、[役割およびタスク] ボタン  をクリックします。
- 2 [eDirectory Maintenance Utilities (eDirectory 保守ユーティリティ)] > [同期修復] の順にクリックします。
- 3 操作を実行するサーバを指定し、[次へ] をクリックします。
- 4 操作を実行するサーバのユーザ名、パスワード、およびコンテキストを指定し、[次へ] をクリックします。
- 5 [すべてのサーバの同期ステータスのレポート] をクリックし、[次へ] をクリックします。
- 6 表示される指示に従って、操作を完了します。

## 時刻同期を実行する

この操作では、ローカル eDirectory データベースに登録されているすべてのサーバに接続し、各サーバの eDirectory と時刻同期ステータスに関する情報を要求します。

各サーバ上で実行している eDirectory のバージョンが [DS バージョン] フィールドに表示されます。


サーバに何のレプリカも含まれていない場合は、[レプリカ深さ] フィールドに「-1」と表示されます。[Root] パーティションのレプリカが含まれている場合は、「0」と表示されます。指定したサーバ上にレプリカがある場合は、[Root] に最も近いレプリカが [Root] からオブジェクト何個分離しているかを示す正の整数が表示されます。

eDirectory ツリー内のすべてのサーバは、同じタイムソースと同期している必要があります。そうしなければ、矛盾が発生したときに、レプリカ間でのオブジェクトの同期が正確に管理されなくなります。

同期修復ウィザードでは、各サーバのタイムソースはレポートできません。ただし、タイムサーバのタイプは報告します。この情報を参照すれば、時刻同期が正確に設定されているかどうかを確認できます。


**重要：**時刻同期のステータス「Nearly-In-Sync (ほぼ同期)」を監視するには、DSRepair ではなく Novell iMonitor を使用してください。詳細については、[197 ページの第 7 章「Novell iMonitor 2.1 の使用」](#)を参照してください。

詳細については、[91 ページの「ネットワーク時刻の同期」](#)を参照してください。

- 1 Novell iManager で、[役割およびタスク] ボタン  をクリックします。
- 2 [eDirectory Maintenance Utilities (eDirectory 保守ユーティリティ)] > [同期修復] の順にクリックします。
- 3 操作を実行するサーバを指定し、[次へ] をクリックします。
- 4 操作を実行するサーバのユーザ名、パスワード、およびコンテキストを指定し、[次へ] をクリックします。
- 5 [時刻同期] をクリックし、[次へ] をクリックします。
- 6 表示される指示に従って、操作を完了します。

## 即時同期をスケジュールする

この操作では、すべてのレプリカの同期を即座に行うようスケジュールします。この操作は、同期プロセスが通常のスケジュールどおりに実行されるのを待つことなく、同期情報を確認したい場合に使用します。

- 1 Novell iManager で、[役割およびタスク] ボタン  をクリックします。
- 2 [eDirectory Maintenance Utilities (eDirectory 保守ユーティリティ)] > [同期修復] の順にクリックします。
- 3 操作を実行するサーバを指定し、[次へ] をクリックします。
- 4 操作を実行するサーバのユーザ名、パスワード、およびコンテキストを指定し、[次へ] をクリックします。
- 5 [即時同期のスケジュール] をクリックし、[次へ] をクリックします。
- 6 表示される指示に従って、操作を完了します。



# DSRepair の詳細オプション

各 eDirectory プラットフォームの DSRepair ユーティリティには、Novell iManager で利用可能な修復機能のほかにも、通常の操作からは見えない拡張機能がいくつかあります。これらの拡張機能は、さまざまなプラットフォームで DSRepair ユーティリティをロードする際にスイッチを使用して利用できます。

- ◆ [285 ページの「eDirectory サーバ上で DSRepair を実行する」](#)
- ◆ [286 ページの「DSRepair コマンドラインオプション」](#)
- ◆ [288 ページの「DSRepair 詳細設定スイッチの使用」](#)

## eDirectory サーバ上で DSRepair を実行する

### NetWare の場合

DSRepair を実行するには、サーバコンソールで「**dsrepair.nlm**」と入力します。

詳細オプションで DSRepair を開くには、サーバコンソールで「**dsrepair -a**」と入力します。

### Windows の場合

**1** [スタート] > [設定] > [コントロールパネル] > [Novell eDirectory サービス] の順にクリックします。

**2** dsrepair.dlm をクリックして、[開始] をクリックします。

詳細オプションで DSRepair を開くには、Novell eDirectory Services コンソールの [起動パラメータ] フィールドに「**-a**」と入力し、dsrepair.dlm を開始します。

### Linux、Solaris、AIX、および HP-UX

DSRepair を実行するには、サーバコンソールに次の構文を使用して「**ndsrepair**」と入力します。

```
ndsrepair { -U | -E | -C | -P [-Ad] | -S [-Ad] | -N | -T | -J エントリ ID  
| --version} [-F ファイル名] [-A yes|no] [-O yes|no]
```

または

```
ndsrepair -R [-l yes|no] [-u yes|no] [-m yes|no] [-i yes|no] [-f yes|no] [-d  
yes|no] [-t yes|no] [-o yes|no] [-r yes|no] [-v yes|no] [-c yes|no] [-F ファ  
イル名] [-A yes|no] [-O yes|no]
```

**重要:** -Ad オプションは、Novell サポート担当者からの事前の指示がない限り使用しないでください。

### 例

標準修復を実行し、/root/ndsrepair.log ファイルにイベントを記録する場合 (またはログファイルがすでに存在していればそのログファイルに追加してイベントを記録する場  
合) は、次のコマンドを入力します。

```
ndsrepair -U -A no -F /root/ndsrepair.log
```

詳細オプションで DSRepair を開くには、次のコマンドを入力します。

```
ndsrepair -Ad
```

すべてのグローバルスキーマ操作とその詳細設定オプションのリストを表示するには、次のコマンドを入力します。

```
ndsrepair -S -Ad
```

データベースを強制ロックしてローカルデータベースを修復するには、次のコマンドを入力します。

```
ndsrepair -R -l yes
```

注: ndsrepair コマンドの入力内容は、オプションファイルによってリダイレクトできます。オプションファイルは、レプリカおよびパーティション操作に関連するオプションやサブオプションを含むテキストファイルです。これらはサーバに対する認証を必要としません。各オプションまたはサブオプションは、改行によって区切られます。ファイルの内容が、適切な順序で指定されていることを確認します。適切な順序になっていないと、予期しない結果が発生する場合があります。

## DSRepair コマンドラインオプション

| オプション | 説明  |
|-------|---|
| -U    | [標準修復] オプションです。ユーザの操作なしに ndsrepair を実行または終了します。Novell サポート担当者から特定の操作を手動で実行するように指示された場合を除き、この修復方法の使用をお勧めします。修復が完了したらログファイルをチェックして、ndsrepair で変更された内容を確認します。  |
| -P    | [レプリカ操作とパーティション操作] オプションです。現在のサーバの eDirectory データベースファイルにレプリカが保存されているパーティションが表示されます。[レプリカオプション] メニューには、「レプリカの修復」、「パーティション操作のキャンセル」、「同期のスケジュール」、および「ローカルレプリカをマスターレプリカとして指定」を実行するオプションがあります。  |
| -S    | [グローバルスキーマの操作] オプションです。このオプションには、このサーバのスキーマを Tree オブジェクトのマスタに準拠させるのに必要なスキーマ操作がいくつか含まれています。ただし、これらの操作は必要なときだけ使用してください。スキーマは、ローカル修復操作および標準修復操作によってすでに検査されています。  |
| -C    | [外部参照オブジェクトのチェック] オプションです。各外部参照オブジェクトをチェックして、そのオブジェクトを含むレプリカがあるかどうかを調べます。オブジェクトのあるパーティションレプリカを含むすべてのサーバがアクセス不能の場合、オブジェクトは見つかりません。オブジェクトが見つからない場合、警告が表示されます。   |
| -E    | [レプリカ同期のレポート] オプションです。現在のサーバ上にレプリカを持つすべてのパーティションのレプリカ同期ステータスをレポートします。この操作により、パーティションのレプリカを保持する各サーバ上のレプリカの Tree オブジェクトから同期ステータス属性が読み込まれます。レポートには、すべてのサーバに対して正常に同期が行われた最終時刻と、最終同期以降発生したエラーが表示されます。12 時間以内に同期が完了していない場合は、警告メッセージが表示されます。 |
| -N    | [このデータベースに認識されているサーバ] オプションです。ローカル eDirectory データベースに認識されているすべてのサーバが表示されます。現在のサーバに Tree パーティションのレプリカがある場合、このサーバには eDirectory ツリー内のすべてのサーバのリストが表示されます。サーバオプションを実行するサーバを 1 つ選択します。  |

| オプション           | 説明   |
|-----------------|--|
| -J              | ローカルサーバ上の1つのオブジェクトを修復します。修復するオブジェクトのエントリ ID (16 進形式で) を指定する必要があります。破損している1つの特定のオブジェクトを修復するには、[標準修復 (-U)] オプションの代わりに、このオプションを使用できます。データベースのサイズによっては、[標準修復] オプションの完了に何時間もかかる場合があります。このオプションを使用して、時間を節約することができます。 |
| -T              | [時刻同期] オプションです。ローカル eDirectory データベースに登録されているすべてのサーバにアクセスして、各サーバの時刻同期ステータスの情報を要求します。このサーバに Tree パーティションのレプリカがある場合は、eDirectory ツリー内のすべてのサーバがポーリングされます。各サーバ上で実行されている eDirectory のバージョンもレポートされます。                 |
| -A              | 既存のログファイルに付加します。既存のログファイルに情報が追加されます。このオプションは、デフォルトで有効に設定されています。  |
| -O              | 出力をファイルに記録します。このオプションは、デフォルトで有効に設定されています。  |
| -F <b>ファイル名</b> | 出力を指定したファイルに記録します。   |
| -R              | [ローカルデータベースの修復] オプションです。ローカル eDirectory データベースを修復します。eDirectory でオープンおよびアクセスできるように、修復操作を使用してローカルデータベースの矛盾を解決します。このオプションには、データベースの修復操作を容易にするサブオプションがあります。このオプションにはファンクション修飾子があります。ファンクション修飾子については、次の表で説明します。    |

-R オプションで使用するファンクション修飾子を次に示します。

| オプション | 説明   |
|-------|--|
| -l    | 修復操作中に eDirectory データベースをロックします。   |
| -u    | 修復操作中に一時 eDirectory データベースを使用します。  |
| -m    | 修復されていない元のデータベースを維持します。  |
| -i    | eDirectory データベース構造とインデックスをチェックします。  |
| -f    | データベースの空き領域を増やします。   |
| -d    | データベース全体を再構築します。   |
| -t    | ツリー構造のチェックを実行します。データベース内での接続状況が正しいかどうかを調べるため、ツリー構造のリンクをすべてチェックするには、「はい」を設定します。チェックを省略するには、「いいえ」を設定します。デフォルト値は「はい」です。 |
| -o    | オペレーショナルスキーマを再構築します。   |
| -r    | すべてのローカルレプリカを修復します。  |
| -v    | ストリームファイルを検証します。   |
| -c    | ローカル参照をチェックします。  |

## DSRepair 詳細設定スイッチの使用

**警告:** このセクションで説明する機能は、正しく使用しないと eDirectory ツリーが破損して元に戻せないことがあります。Novell サポート担当者からの指示がない限り、この機能は使用しないでください。

生産環境でこれらのうちのいずれかの機能を使用する前に、あらかじめサーバ上の eDirectory のフルバックアップをとっておくことをお勧めします。詳細については、[389 ページの第 14 章「Novell eDirectory のバックアップと復元」](#)を参照してください。

NetWare では、DSRepair (dsrepair -XK2 など) をロードするときに、サーバコンソールでこれらのオプションを使用します。

Linux、Solaris、AIX、および HP-UX では、「**ndsrepair -R -Ad -XK2**」と入力します。

Windows では、dsrepair.dlm を開始する前に、NDS コンソールの [起動パラメータ] フィールドにこれらのオプションを入力します。詳細については、[285 ページの「eDirectory サーバ上で DSRepair を実行する」](#)を参照してください。

| スイッチ | 説明   |
|------|--|
| -NLC | NetWare サーバで「STORE NETWORK 5 CONN SCL MLA USAGE IN NDS」セットパラメータがオンになった場合、「NLS:CERT PEAK USED POOL」属性は非常に大きい値を取得する場合があります。DSRepair を -NLC オプションで実行すると、こうした大きい値はクリアされます。 |
| -P   | タイプが不明な eDirectory オブジェクトをすべて、参照済みとしてマークします。参照されたオブジェクトは、eDirectory レプリカ同期処理の対象にはなりません。  |
| -WM  | 多くの場合、WM は次のようになります。ZENworks® 2.0 を使用すると「Registered Workstations (登録されたワークステーション)」属性は大きい値になります。DSRepair を -WM オプションで実行すると、こうした大きい値はクリアされます。                            |
| -XK2 | このサーバの eDirectory データベース内にある eDirectory オブジェクトをすべて削除します。この操作では、破損したレプリカがどんな方法を使っても削除できない場合に、破損レプリカを削除できます。   |
| -XK3 | このサーバの eDirectory データベース内にある外部参照をすべて削除します。この操作では、機能していないレプリカ内の外部参照をすべて削除できます。参照が原因で問題が発生している場合、レプリカが再度機能するために、eDirectory は参照を再作成できます。                                  |

# eMBox クライアントを使用したデータベースの修復

eMBox (eDirectory Management Toolbox) クライアントはコマンドライン Java クライアントで、これを使用すると DSRepair にリモートアクセスできます。eMBox クライアントはバッチモードで実行できるため、これを使用して eDirectory DSRepair eMTool で標準修復を行うことができます。

emboxclient.jar ファイルは、eDirectory の一部としてサーバにインストールされます。JVM をインストールしていれば、どのコンピュータでも実行できます。eMBox クライアントの詳細については、[555 ページの「eMBox コマンドラインクライアントの使用」](#)を参照してください。

## DSRepair eMTool を使用する

- 1 コマンドラインで次のように入力して、対話式モードで eMBox クライアントを実行します。

```
java -cp ファイルのパス /emboxclient.jar embox -i
```

( クラスパスに emboxclient.jar ファイルがすでに含まれている場合は、**java embox -i** と入力するだけです。)

eMBox Client のプロンプトが次のように表示されます。

```
eMBox Client>
```

- 2 修復するサーバにログインするには、次のように入力します。

```
login -s サーバの名前または IP アドレス -p ポート番号  
-u ユーザ名 . コンテキスト -w パスワード -n
```

ポート番号は通常 80 または 8028 です。ただし、すでにそのポートを使用している Web サーバが存在する場合は異なります。-n オプションを使用すると、非セキュア接続を開始します。

eMBox クライアントはログインが成功したかどうかを表示します。

- 3 次の構文を使用して修復コマンドを入力します。

```
dsrepair. タスク オプション
```

例 :

dsrepair.ufr は標準修復を実行します。

dsrepair.rld -a -v は、[すべてのローカルレプリカを修復] オプションおよび [ローカル参照をチェックする] オプションを使用して、ローカルデータベースを修復します。

各スイッチの間にはスペースが必要です。スイッチの順序は重要ではありません。

eMBox クライアントは修復が成功したかどうかを表示します。

DSRepair eMTool オプションの詳細については、[290 ページの「DSRepair eMTool のオプション」](#)を参照してください。

- 4 eMBox クライアントからログアウトするには、次のコマンドを入力します。

```
logout
```

- 5 eMBox クライアントを終了するには、次のコマンドを入力します。

```
exit
```

## DSRepair eMTool のオプション

次の表に DSRepair eMTool のオプションを示します。eMBox クライアントで **list -tdsrepair** コマンドを使用して DSRepair オプションの詳細を表示することもできます。詳細については、[559 ページの「eMTool とそのサービスを表示する」](#)を参照してください。

| オプション   | 説明  |
|---|---|
| rso<br>-o<br>-d   | 単一オブジェクトの修復<br>オブジェクト ID (16 進数)<br>オブジェクト DN   |
| rts   | 時刻の同期   |
| rss   | すべてのパーティションの同期ステータスのレポート  |
| rld<br>-l<br>-t<br>-d<br>-p<br>-i<br>-f<br>-e<br>-c<br>-o<br>-a<br>-m<br>-v | ローカルデータベースの修復<br>修復中ずっと eDirectory データベースをロック<br>修復中に一時的な eDirectory データベースを使用する<br>修復されていない元のデータベースを維持<br>データベース構造のチェックを実行<br>データベースの構造チェックとインデックスチェックを実行<br>データベースの未使用領域を増やす<br>データベース全体を再構築<br>ツリー構造のチェックを実行<br>オペレーショナルスキーマを再構築<br>すべてのローカルレプリカを修復<br>メールディレクトリおよびストリームファイルを検証<br>ローカル参照をチェック |
| ufr   | 標準修復  |
| rsn<br>-o<br>-d   | 選択したサーバのネットワークアドレスの修復<br>オブジェクト ID (16 進数)<br>オブジェクト DN   |
| ran   | すべてのネットワークアドレスの修復   |
| rsr<br>-p<br>-d   | 選択したレプリカの修復<br>パーティション ID<br>パーティション DN   |
| rer   | すべてのレプリカの修復   |
| ror<br>-p<br>-d   | 選択したレプリカリングの修復<br>パーティション ID<br>パーティション DN  |
| rar   | すべてのレプリカのレプリカリングの修復   |
| ssa<br>-p<br>-d   | すべてのサーバのレプリカ同期ステータスのレポート<br>パーティション ID<br>パーティション DN  |
| cer   | 外部参照のチェック   |

| オプション                       | 説明  |
|-----------------------------|---|
| rao<br>-p<br>-d<br>-s<br>-d | このレプリカのすべてのオブジェクトを受信<br>パーティション ID<br>パーティション DN<br>サーバ ID<br>サーバ DN        |
| sao<br>-p<br>-d<br>-s<br>-d | リング内のすべてのレプリカにすべてのオブジェクトを送信<br>パーティション ID<br>パーティション DN<br>サーバ ID<br>サーバ DN |
| dne<br>-p<br>-d             | タイムスタンプの修復と新規エポックの宣言<br>パーティション ID<br>パーティション DN                            |
| sri<br>-p<br>-d             | 即時同期のスケジュール<br>パーティション ID<br>パーティション DN<br>サーバ ID<br>サーバ DN                 |
| sks<br>-p<br>-d<br>-s<br>-d | 選択したサーバのレプリカを同期<br>パーティション ID<br>パーティション DN<br>サーバ ID<br>サーバ DN             |
| ske<br>-p<br>-d             | すべてのサーバのレプリカを同期<br>パーティション ID<br>パーティション DN                                 |
| dsr<br>-p<br>-d             | 選択したレプリカの削除<br>パーティション ID<br>パーティション DN                                     |
| xsr<br>-p<br>-d<br>-s<br>-d | レプリカリングからサーバを削除<br>パーティション ID<br>パーティション DN<br>サーバ ID<br>サーバ DN             |
| dnm<br>-p<br>-d             | このサーバを新しいマスタレプリカに設定<br>パーティション ID<br>パーティション DN                             |
| dul                         | 不明リーフオブジェクトの削除  |





# 11

## WAN トラフィックマネージャ

WAN トラフィックマネージャ (WTM) を使用して WAN リンク上のレプリケーショントラフィックを管理することにより、ネットワークコストを削減できます。WAN トラフィックマネージャは Novell® eDirectory™ のインストール時にインストールされ、次の要素から構成されます。

- ◆ WTM

レプリカリング内の各サーバ上に常駐します。eDirectory がサーバ間トラフィックを送信する前に、WTM は WAN トラフィックポリシーを読み込んで、そのトラフィックを送信するかどうかを決定します。

- ◆ WAN トラフィックポリシー

eDirectory トラフィックの生成を制御する規則です。WAN トラフィックポリシーは、サーバオブジェクトまたは LAN エリアオブジェクト、あるいはその両方に eDirectory プロパティ値として保存されるテキストです。

- ◆ WANMAN Novell iManager プラグイン

この WTM とのインタフェースは、ポリシーの作成または変更、LAN エリアオブジェクトの作成、および LAN エリアまたはサーバへのポリシーの適用のために使用します。WTM を (eDirectory インストールの一部として) インストールする場合、スキーマには LAN エリアオブジェクト、およびサーバオブジェクト上の WAN トラフィックマネージャページが含まれます。

WAN トラフィックマネージャ (NetWare® 上では wtm.nlm、Windows 上では wtm.dlm) は、トラフィックを制御する各サーバ上に常駐する必要があります。パーティションのレプリカリングに 1 つの広域リンクの両側に配置されているサーバが含まれる場合は、そのレプリカリング内のすべてのサーバ上に WAN トラフィックマネージャをインストールします。

**重要:** Linux、Solaris、AIX、または HP-UX システムでは、WAN トラフィックマネージャはサポートされていません。

## WAN トラフィックマネージャについて

eDirectory などのネットワークディレクトリにより、サーバ間トラフィックが生成されます。広域ネットワーク (WAN) リンク上のトラフィックを管理しない場合、コストが不必要に増大したり、利用率の高い時間帯に通信速度が遅い WAN リンクに過大な負荷がかかったりすることがあります。

WAN トラフィックマネージャを使用すると、eDirectory により生成された (WAN リンク上の) サーバ間トラフィックや、eDirectory ツリー内の任意のサーバ間 eDirectory トラフィックを制御できます。WTM は、トラフィックのコスト、時刻、eDirectory 操作のタイプ、あるいはそのいずれかの組み合わせに基づいてトラフィックを制限できます。

たとえば、利用率の高い時間帯には WAN リンク上の eDirectory トラフィックを制限できます。この場合には、高帯域幅のアクティビティが利用率の低い時間帯に移行します。レプリカの同期トラフィックを利用率の低い時間帯だけに制限することにより、コストを削減することもできます。

WAN トラフィックマネージャは、eDirectory により開始された定期的なイベント (レプリカの同期など) だけを制御します。管理者またはユーザにより開始されたイベントや、非 eDirectory サーバ間トラフィック (時刻の同期など) は制御しません。

サーバ間トラフィックを生成する eDirectory プロセスを次の表に示します。

| プロセス    | 説明   |
|---------|--|
| レプリカの同期 | <p>eDirectory オブジェクトへの変更がパーティションのすべてのレプリカで同期されるようにします。指定されたパーティションのコピーを保持するすべてのサーバは、変更を同期するために他のサーバと通信する必要があります。</p> <p>実行されるレプリカの同期には 2 つのタイプがあります。</p> <ul style="list-style-type: none"> <li>◆ 即時同期は、eDirectory オブジェクトが変更されるか、あるいはディレクトリツリー内でオブジェクトが追加または削除されると実行されます。</li> <li>◆ 遅延同期は、複数の eDirectory オブジェクトに共通した変更で、繰り返し実行される特定の変更 (ログインプロパティへの変更など) の後で実行されます。このような変更の例としては、ユーザがログインまたはログアウトするときのログイン時刻、最終ログイン時刻、ネットワークアドレス、およびリビジョンの各プロパティへの更新があります。</li> </ul> <p>遅延同期プロセスは、即時同期プロセスが実行されない場合にのみ実行されます。デフォルトでは、即時同期は変更が保存されてから 10 秒後に実行され、遅延同期は他の変更が発生してから 22 分後に実行されます。</p> |
| スキーマの同期 | <p>ディレクトリツリー内の各パーティションでスキーマが整合性を保ち、すべてのスキーマ変更がネットワーク上で更新されるようにします。</p> <p>デフォルトでは、このプロセスは 4 時間に 1 回実行されます。</p>   |
| ハートビート  | <p>ディレクトリオブジェクトがパーティションのすべてのレプリカで整合性を保つようにします。パーティションのコピーを持つすべてのサーバは、整合性をチェックするために、パーティションを持つ他のサーバと通信する必要があります。</p> <p>デフォルトでは、このプロセスはパーティションのレプリカを含むすべてのサーバ上で 30 分に 1 回実行されます。</p>  |


| プロセス         | 説明   |
|--------------|--|
| Limber       | <p>サーバ名またはサーバアドレスが変更されたときに、そのサーバのレプリカポインタテーブルが更新されるようにします。この変更は次のような場合に発生します。</p> <ul style="list-style-type: none"> <li>• autoexec.ncfファイルで新しいサーバ名またはIPX™ 内部アドレスを使用してサーバをリブートした。</li> <li>• プロトコルを追加するためにアドレスを追加した。</li> </ul> <p>サーバがブートされると、limber プロセスにより、サーバ名およびサーバの IPX アドレスがレプリカポインタテーブルに保存されているデータと比較されます。サーバ名とアドレスのどちらかまたは両方が一致しない場合、eDirectory は、そのサーバの項目を含むすべてのレプリカポインタテーブルを自動的に更新します。</p> <p>limber プロセスでは、レプリカリング内の各サーバのツリー名が正しいかどうかもチェックされます。</p> <p>limber プロセスはサーバがブートされてから 5 分後に実行され、その後 3 時間に 1 回実行されます。</p> |
| バックリンク       | <p>サーバ上のレプリカに保存されていない eDirectory オブジェクトへのポインタである外部参照を確認します。通常の場合、バックリンクプロセスはローカルデータベースがオープンされてから 2 時間後に実行され、その後 13 時間に 1 回実行されます。</p>  |
| 接続管理         | <p>レプリカリング内のサーバが NCP™ パケットを転送するには、セキュリティレベルの高い接続が必要です。接続管理プロセスにより、仮想クライアント接続と呼ばれる安全な接続が確立されます。</p> <p>場合によっては、接続管理プロセスにより、スキーマの同期プロセスまたはバックリンクプロセスのための仮想クライアント接続も確立する必要があります。時刻サービスの環境設定によっては、時刻の同期プロセスでも仮想クライアント接続が必要になります。</p>   |
| サーバステータスチェック | <p>サーバステータスチェックは、レプリカを持たない各サーバ上で開始されます。サーバオブジェクトを含むパーティションの書き込み可能なレプリカを保持するサーバのうち、最も近くにあるサーバへの接続が確立されます。</p> <p>サーバステータスチェックは 6 分に 1 回実行されます。</p>  |

## LAN エリアオブジェクト

LAN エリアオブジェクトを使用すると、サーバグループの WAN トラフィックポリシーを簡単に管理できます。LAN エリアオブジェクトを作成した後で、LAN エリアオブジェクトにサーバを追加したり、LAN エリアオブジェクトからサーバを削除することができます。LAN エリアに適用されたポリシーは、その LAN エリア内のすべてのサーバに適用されます。

広域リンクによって他の LAN に接続している LAN 内に複数のサーバがある場合は、LAN エリアオブジェクトを作成します。LAN エリアオブジェクトを作成しない場合は、各サーバの WAN トラフィックを個別に管理する必要があります。

## LAN エリアオブジェクトを作成する



- 1 Novell iManager で、[役割およびタスク] ボタン  をクリックします。
- 2 [WAN トラフィック] > [LAN エリアの作成] の順にクリックします。
- 3 [オブジェクトクラス] ドロップダウンリストの [WANMAN-LAN エリア] を選択します。
- 4 オブジェクトの名前とコンテキストを指定して、[作成] をクリックします。

次のいずれかのセクションに進みます。

- ◆ [296 ページの「LAN エリアオブジェクトへサーバを追加する」](#)
- ◆ [298 ページの「WAN ポリシーを適用する」](#)

## LAN エリアオブジェクトへサーバを追加する

1つのサーバは1つのLANエリアオブジェクトにのみ属することができます。追加するサーバがLANエリアオブジェクトにすでに属している場合、そのサーバはそのオブジェクトから削除され、新しいオブジェクトに追加されます。

- 1 Novell iManager で、[役割およびタスク] ボタン  をクリックします。
- 2 [WAN トラフィック] > [WAN トラフィックマネージャの概要] の順にクリックします。
- 3 [LAN エリアの表示] をクリックし、サーバを追加するLANエリアオブジェクトをクリックします。
- 4 [サーバリスト] をクリックし、[オブジェクトセレクト] ボタン  をクリックします。
- 5 目的のサーバを選択します。
- 6 追加する各サーバについて、[ステップ 4](#) から [ステップ 5](#) を繰り返します。  
WAN ポリシーをLANエリアオブジェクトに適用して、そのポリシーをグループ内のすべてのサーバに適用する方法の詳細については、[298 ページの「WAN ポリシーを適用する」](#)を参照してください。
- 7 [適用] をクリックし、[OK] をクリックします。

## LAN エリアオブジェクトへ追加情報を追加する

ConsoleOne<sup>®</sup> を使用して、LAN エリアオブジェクトに記述情報を追加できます。この機能は、Novell iMonitor では使用できません。

- 1 ConsoleOne で、LAN エリアオブジェクトを右クリックします。
- 2 [プロパティ] > [一般] の順にクリックします。
- 3 必要に応じて、所有者、説明、地域、部署、および組織の情報を追加します。
- 4 [適用] をクリックし、[OK] をクリックします。

## WAN トラフィックポリシー

WAN トラフィックポリシーは、eDirectory トラフィックの生成を制御する一連の規則です。この規則はテキストとして作成され、サーバオブジェクトまたは LAN エリアオブジェクト、あるいはその両方に eDirectory プロパティ値として保存されます。ポリシーは、単純な処理言語に基づいて解釈されます。

ポリシーは個々のサーバに適用できます。LAN エリアオブジェクトを作成して、このオブジェクトに複数のサーバを割り当てることもできます。LAN エリアオブジェクトに適用されたポリシーは、そのオブジェクトに割り当てられたすべてのサーバに自動的に適用されます。

WAN トラフィックマネージャには、いくつかの定義済みポリシーグループがあります。これらのポリシーは、そのまま使用することも、必要に応じて変更することもでき、あるいは新しいポリシーを作成することもできます。

- ◆ [298 ページの「WAN ポリシーを適用する」](#)
- ◆ [298 ページの「WAN ポリシーを変更する」](#)
- ◆ [299 ページの「既存のポリシーをリネームする」](#)
- ◆ [300 ページの「新しい WAN ポリシーを作成する」](#)

### 定義済みポリシーグループ

類似した機能を持つ定義済みポリシーのグループを次の表に示します。


| ポリシーグループ      | 説明   |
|---------------|--|
| 1-3AM.WMG     | トラフィックの送信が午前 1 時から午前 3 時までの時間帯だけに制限されます。                                     |
| 7AM-6PM.WMG   | トラフィックの送信が午前 7 時から午後 6 時までの時間帯だけに制限されます。                                     |
| COSTLT20.WMG  | コストファクタが 20 より小さいトラフィックのみ送信が許可されます。  |
| IPX.WMG       | IPX トラフィックのみ許可されます。  |
| NDSTTYP.S.WMG | さまざまな eDirectory トラフィックタイプのサンプルポリシーが提供されます。                                  |
| ONOSPOOF.WMG  | 既存の WAN 接続のみ使用が許可されます。   |
| OPNSPOOF.WMG  | 既存の WAN 接続のみ使用が許可されますが、15 分間使用されていない接続は無効と見なされます。この場合は使用できません。               |
| SAMEAREA.WMG  | 同じネットワークエリア内のトラフィックのみ許可されます。   |
| TCP/IP.WMG    | TCP/IP トラフィックのみ許可されます。   |
| TIMECOST.WMG  | すべてのトラフィックが午前 1 時から午前 1 時 30 分までの時間帯だけに制限されますが、同じロケーション内のサーバには連続的な対話が許可されます。 |

定義済みポリシーグループおよび個々のポリシーの詳細については、[303 ページの「WAN トラフィックマネージャポリシーグループ」](#)を参照してください。

## WAN ポリシーを適用する

WAN ポリシーを個々のサーバまたは LAN エリアオブジェクトに適用できます。個々のサーバに適用されたポリシーは、そのサーバの eDirectory トラフィックのみ管理します。LAN エリアオブジェクトに適用されたポリシーは、そのオブジェクトに属しているすべてのサーバのトラフィックを管理します。


WAN トラフィックマネージャは、WANMAN.INI の WAN ポリシーグループセクションに格納されている「キー=値」ステートメントを参照します。「キー」はスナップインに表示されるポリシー名で、「値」は区切られたポリシーを格納するテキストファイルへのパスです。

- 1 Novell iManager で、[役割およびタスク] ボタン  をクリックします。
- 2 [WAN トラフィック] > [WAN トラフィックマネージャの概要] の順にクリックします。
- 3 [LAN エリアの表示] をクリックし、LAN エリアオブジェクトをクリックします。  
または  
[NCP サーバの表示] をクリックし、NCP サーバオブジェクトをクリックします。
- 4 [ポリシーの追加] をクリックし、使用するポリシーグループを選択します。  
詳細については、[297 ページの「定義済みポリシーグループ」](#)を参照してください。
- 5 [OK] をクリックします。  
ポリシーグループからロードされたポリシーのリストが表示されます。
- 6 [OK] をクリックします。  
ポリシーの内容を参照したり、ポリシーを変更することができます。ポリシー内のエラーをチェックするには、[ポリシーのチェック] をクリックします。
- 7 不要なポリシーを削除するには、[ポリシー名] ドロップダウンリストでポリシーを選択し、[ポリシーの削除] をクリックします。
- 8 [適用] をクリックし、[OK] をクリックします。

## WAN ポリシーを変更する

WAN トラフィックマネージャが提供する定義済みポリシーグループは、要件に合わせて変更できます。また、独自に作成したポリシーを変更することもできます。

### サーバに適用された WAN ポリシーを変更する


- 1 Novell iManager で、[役割およびタスク] ボタン  をクリックします。
- 2 [WAN トラフィック] > [WAN トラフィックマネージャの概要] > [NCP サーバの表示] の順にクリックします。
- 3 編集するポリシーを含むサーバオブジェクトをクリックします。
- 4 [ポリシー名] ドロップダウンリストで、編集するポリシーを選択します。
- 5 [ポリシー] フィールドで必要に応じてポリシーを編集します。

WAN ポリシーの構成の詳細については、[319 ページの「WAN ポリシーの構成」](#)を参照してください。


WAN ポリシーの構文の詳細については、[322 ページの「ポリシーセクションで使用される構文」](#)を参照してください。

- 6 [ポリシーのチェック]をクリックすると、構文または構成のエラーが識別されます。  
WANトラフィックマネージャは、エラーを含むポリシーを実行しません。
- 7 変更した場合は、[適用] をクリックします。
- 8 不要なポリシーを削除するには、[ポリシー名] ドロップダウンリストでポリシーを選択し、[ポリシーの削除] をクリックします。
- 9 [適用] をクリックし、[OK] をクリックします。

#### LAN エリアオブジェクトに適用された WAN ポリシーを変更する

- 1 Novell iManager で、[役割およびタスク] ボタン  をクリックします。
- 2 [WANトラフィック] > [WANトラフィックマネージャの概要] > [LAN エリアの表示] の順にクリックします。
- 3 編集するポリシーを含む LAN エリアオブジェクトをクリックします。
- 4 [ポリシー名] ドロップダウンリストで、編集するポリシーを選択します。
- 5 [ポリシー] フィールドで必要に応じてポリシーを編集します。  
WAN ポリシーの構成の詳細については、[319 ページの「WAN ポリシーの構成」](#)を参照してください。  
WAN ポリシーの構文の詳細については、[322 ページの「ポリシーセクションで使用する構文」](#)を参照してください。
- 6 [ポリシーのチェック]をクリックすると、構文または構成のエラーが識別されます。  
WANトラフィックマネージャは、エラーを含むポリシーを実行しません。
- 7 変更した場合は、[適用] をクリックします。
- 8 不要なポリシーを削除するには、[ポリシー名] ドロップダウンリストでポリシーを選択し、[ポリシーの削除] をクリックします。
- 9 [適用] をクリックし、[OK] をクリックします。


#### 既存のポリシーをリネームする

- 1 Novell iManager で、[役割およびタスク] ボタン  をクリックします。
- 2 [WANトラフィック] > [WANトラフィックマネージャの概要] の順にクリックします。
- 3 [LAN エリアの表示] をクリックし、LAN エリアオブジェクトをクリックします。  
または  
[NCP サーバの表示] をクリックし、NCP サーバオブジェクトをクリックします。
- 4 [ポリシー名] ドロップダウンリストで、リネームするポリシーを選択します。
- 5 [ポリシーの名前の変更] をクリックし、新しい名前を指定します。  
名前は完全識別名である必要があります。
- 6 [OK] をクリックし、[適用]、[OK] の順にクリックします。


## 新しい WAN ポリシーを作成する

サーバオブジェクトまたは LAN エリアオブジェクトに適用する WAN ポリシーを作成できます。個々のサーバ用に作成されたポリシーは、そのサーバの eDirectory トラフィックのみ管理します。LAN エリアオブジェクト用に作成されたポリシーは、そのオブジェクトに属しているすべてのサーバのトラフィックを管理します。

### サーバオブジェクトの WAN ポリシーを作成する

- 1 Novell iManager で、[役割およびタスク] ボタン  をクリックします。
- 2 [WAN トラフィック] > [WAN トラフィックマネージャの概要] > [NCP サーバの表示] の順にクリックします。
- 3 新しいポリシーを作成するサーバオブジェクトをクリックし、[ポリシーの作成] をクリックします。
- 4 新しいポリシーの名前を指定し、[OK] をクリックします。  
指定する名前は完全識別名である必要があります。
- 5 [ポリシー] テキストボックスに必要な情報を指定します。  
WAN ポリシーの構成の詳細については、[319 ページの「WAN ポリシーの構成」](#)を参照してください。  
WAN ポリシーの構文の詳細については、[322 ページの「ポリシーセクションで使用する構文」](#)を参照してください。
- 6 [適用] をクリックし、[OK] をクリックします。

### LAN エリアオブジェクトの WAN ポリシーを作成する


- 1 Novell iManager で、[役割およびタスク] ボタン  をクリックします。
- 2 [WAN トラフィック] > [WAN トラフィックマネージャの概要] > [LAN エリアの表示] の順にクリックします。
- 3 WAN ポリシーを作成する LAN エリアオブジェクトをクリックし、[ポリシーの作成] をクリックします。
- 4 新しいポリシーの名前を指定し、[OK] をクリックします。  
指定する名前は完全識別名である必要があります。
- 5 [ポリシー] テキストボックスに必要な情報を指定します。  
WAN ポリシーの構成の詳細については、[319 ページの「WAN ポリシーの構成」](#)を参照してください。  
WAN ポリシーの構文の詳細については、[322 ページの「ポリシーセクションで使用する構文」](#)を参照してください。
- 6 [適用] をクリックし、[OK] をクリックします。



## WAN トラフィックを制限する

WAN トラフィックマネージャには、トラフィックを特定の時間帯だけに制限する 2 つの定義済みポリシーグループがあります ( 詳細については、[303 ページの「1-3AM.WMG」](#) および [304 ページの「7AM-6PM.WMG」](#) を参照してください)。これらのポリシーを変更すると、任意の時間帯を選択して、トラフィックをその時間帯だけに制限できます。

ここでは午前 1 時から午前 3 時までのグループを変更する場合について説明しますが、午前 7 時から午後 6 時までのグループを変更する場合でも同様の手順を使用できます。

- 1 Novell iManager で、[役割およびタスク] ボタン  をクリックします。
- 2 [WAN トラフィック] > [WAN トラフィックマネージャの概要] の順にクリックします。
- 3 [LAN エリアの表示] をクリックし、LAN エリアオブジェクトをクリックします。  
または  
[NCP サーバの表示] をクリックし、NCP サーバオブジェクトをクリックします。
- 4 [ポリシーの追加] をクリックします。
- 5 定義済みポリシーのリストの中から 1-3AM.WMG を選択し、[OK] を 2 回クリックします。

ポリシーが [ポリシー] テキストボックスに表示されるので、ここでポリシーを変更します。たとえば、トラフィックを許可する時間帯を午前 1 時から午前 3 時までではなく午前 2 時から午後 5 時までに設定するには、次のように変更します。

```
/* This policy limits all traffic to between 2 and 5 pm */
LOCAL BOOLEAN Selected;
SELECTOR
    Selected := Now.hour >= 2 AND Now.hour < 17;
    IF Selected THEN
        RETURN 50; /* between 2am and 5pm this policy has a
high priority */
    ELSE
        RETURN 1; /* return 1 instead of 0 in case there are
no other policies */
        /* if no policies return > 0, WanMan assumes
SEND */
    END
END
PROVIDER
    IF Selected THEN
        RETURN SEND; /* between 2am and 5pm, SEND */
    ELSE
        RETURN DONT_SEND; /* other times, don't */
    END
END
```

コメント行 (*/\** と *\*/* で囲まれた部分) では、午前と午後を使用して時刻を指定できます。しかし、実行コードでは 24 時間形式を使用して指定する必要があります。したがって、午後 5 時は 17 になります。

WAN ポリシーの構成の詳細については、[319 ページの「WAN ポリシーの構成」](#) を参照してください。

WAN ポリシーの構文の詳細については、[322 ページの「ポリシーセクションで使用する構文」](#) を参照してください。

- 6** 構文または構成のエラーを識別するには、ポリシーの構文を変更した後で[ポリシーのチェック] をクリックします。  
ポリシーのチェックの結果が表示されます。  
WANトラフィックマネージャは、エラーを含むポリシーを実行しません。
- 7** 元の1-3 amポリシーを変更しない場合は、新しいポリシーを別の名前で追加します。
  - 7a** [ポリシーの名前の変更] をクリックします。
  - 7b** 編集するポリシーの名前を指定し、[OK] をクリックします。
- 8** [適用] をクリックし、[OK] をクリックします。

## コストファクタを割り当てる

コストファクタにより、WANトラフィックマネージャは特定の送信先とのトラフィックのコストを比較して、WANポリシーを使用してトラフィックを管理できます。WANポリシーでは、コストファクタを使用してWANトラフィックの相対コストが決定されます。トラフィックを送信するか決定するのに、この情報を使用できます。

コストファクタは、時間単位あたりの費用として表されます。各WANトラフィックポリシーで一貫して同じ単位が使用されている限り、あらゆる単位でコストファクタを表すことができます。つまり、その比率だけを使用している限り、1時間あたりドル、1分あたりセント、1秒あたり円など任意のコスト対時間の比率を使用できます。


トラフィックの相対コストを表す送信先コストファクタを、特定のアドレス範囲に割り当てることができます。したがって、サーバのグループ全体のコストを1つの宣言で割り当てることができます。デフォルトコストファクタを割り当てることもできます。デフォルトコストファクタは、送信先のコストが指定されていない場合に使用されます。

送信先に対してコストが割り当てられていない場合は、デフォルトコストが使用されます。サーバまたはLANエリアオブジェクトに対してデフォルトコストが指定されていない場合は、-1の値が割り当てられます。



コストファクタに基づいてトラフィックを制限するサンプルポリシーの詳細については、[304 ページの「COSTLT20.WMG」](#)を参照してください。

ポリシーを変更する方法の詳細については、[298 ページの「WANポリシーを変更する」](#)を参照してください。

## デフォルトコストファクタを割り当てる

- 1** Novell iManager で、[役割およびタスク] ボタン  をクリックします。
- 2** [WANトラフィック管理] > [WANトラフィックマネージャの概要] の順にクリックします。
- 3** [LANエリアの表示] をクリックし、LANエリアオブジェクトをクリックします。  
または  
[NCPサーバの表示] をクリックし、NCPサーバオブジェクトをクリックします。
- 4** [コスト] をクリックし、[デフォルトコスト] フィールドにコストを入力します。  
コストは負以外の整数でなければなりません。指定したデフォルトコストは、サーバまたはLANエリアオブジェクトの送信先のうち、割り当てたコストの送信先アドレス範囲内に収まらないすべての送信先に割り当てられます。コストは、ドルなどの通貨単位で指定するか、または1秒あたりのパケット数で指定できます。
- 5** [適用] をクリックし、[OK] をクリックします。

## 送信先アドレス範囲へコストを割り当てる

- 1 Novell iManager で、[役割およびタスク] ボタン  をクリックします。
- 2 [WAN トラフィック管理] > [WAN トラフィックマネージャの概要] の順にクリックします。
- 3 [LAN エリアの表示] をクリックし、LAN エリアオブジェクトをクリックします。  
または  
[NCP サーバの表示] をクリックし、NCP サーバオブジェクトをクリックします。
- 4 [コスト] をクリックします。
- 5 [追加] ボタン  をクリックします。
- 6 WANMAN コストの作成ウィンドウで、[TCP/IP アドレスタイプ] または [IPX アドレスタイプ] を選択します。
- 7 範囲の開始アドレスと終了アドレスを TCP/IP または IPX の適切な形式で指定します。
- 8 [コスト] テキストフィールドで、コストを負以外の整数で指定します。
- 9 [OK] をクリックし、[適用]、[OK] の順にクリックします。

## WAN トラフィックマネージャポリシーグループ

WAN トラフィックマネージャには、次の定義済みポリシーグループがあります。

ポリシーグループを適用する方法の詳細については、[298 ページの「WAN ポリシーを適用する」](#)を参照してください。

### 1-3AM.WMG

このグループのポリシーでは、トラフィックを送信できる時間帯が午前 1 時から午前 3 時までだけに制限されます。次の 2 つのポリシーがあります。

- ◆ 1 - 3 am, NA

バックリンク、外部参照、およびログイン制限のチェック、Janitor または limber の実行、スキーマの同期がこの時間帯だけに制限されます。

- ◆ 1 - 3 am

他のすべてのトラフィックがこの時間帯だけに制限されます。

すべてのトラフィックをこの時間帯だけに制限するには、両方のポリシーを適用する必要があります。

## 7AM-6PM.WMG

このグループのポリシーでは、トラフィックを送信できる時間帯が午前 7 時から午後 6 時までだけに制限されます。次の 2 つのポリシーがあります。

- ◆ 7 am - 6 pm, NA

バックリンク、外部参照、およびログイン制限のチェック、Janitor または limber の実行、スキーマの同期がこの時間帯だけに制限されます。

- ◆ 7 am - 6 pm

他のすべてのトラフィックがこの時間帯だけに制限されます。

すべてのトラフィックをこの時間帯だけに制限するには、両方のポリシーを適用する必要があります。

## COSTLT20.WMG

このグループのポリシーでは、コストファクタが 20 未満のトラフィックのみ送信が許可されます。次の 2 つのポリシーがあります。

- ◆ Cost < 20, NA

コストファクタが 20 以上の場合、バックリンク、外部参照、およびログイン制限のチェック、Janitor または limber の実行、スキーマの同期が抑止されます。

- ◆ Cost < 20

コストファクタが 20 以上の場合、他のすべてのトラフィックが抑止されます。

コストファクタが 20 以上のトラフィックをすべて抑止するには、両方のポリシーを適用する必要があります。

## IPX.WMG

このグループのポリシーでは、IPX トラフィックのみ送信が許可されます。次の 2 つのポリシーがあります。

- ◆ IPX, NA

IPX によって生成されたトラフィック以外の場合、バックリンク、外部参照、およびログイン制限のチェック、Janitor または limber の実行、スキーマの同期が抑止されます。

- ◆ IPX

IPX によって生成されたトラフィック以外の場合、他のすべてのトラフィックが抑止されます。

IPX 以外のトラフィックをすべて抑止するには、両方のポリシーを適用する必要があります。

## NDSTTYP.S.WMG

このグループのポリシーは、さまざまな eDirectory トラフィックタイプのサンプルポリシーです。eDirectory がこのタイプの要求に渡す変数が格納されています。

- ◆ 305 ページの「Catch All with Addresses のサンプル」
- ◆ 305 ページの「Catch All without Addresses のサンプル」
- ◆ 305 ページの「NDS\_BACKLINK\_OPEN のサンプル」
- ◆ 306 ページの「NDS\_BACKLINKS のサンプル」
- ◆ 308 ページの「NDS\_CHECK\_LOGIN\_RESTRICTION のサンプル」
- ◆ 309 ページの「NDS\_CHECK\_LOGIN\_RESTRICTION\_OPEN のサンプル」
- ◆ 310 ページの「NDS\_JANITOR のサンプル」
- ◆ 311 ページの「NDS\_JANITOR\_OPEN のサンプル」
- ◆ 312 ページの「NDS\_LIMBER のサンプル」
- ◆ 313 ページの「NDS\_LIMBER\_OPEN のサンプル」
- ◆ 314 ページの「NDS\_SCHEMA\_SYNC のサンプル」
- ◆ 315 ページの「NDS\_SCHEMA\_SYNC\_OPEN のサンプル」
- ◆ 316 ページの「NDS\_SYNC のサンプル」

### Catch All with Addresses のサンプル

アドレスのあるトラフィックタイプのためのサンプルポリシーです。

### Catch All without Addresses のサンプル

アドレスのないトラフィックタイプのためのサンプルポリシーです。

### NDS\_BACKLINK\_OPEN のサンプル

NDS\_BACKLINK\_OPEN は、対応する NDS\_BACKLINKS クエリの実行中に CheckEachNewOpenConnection または CheckEachAlreadyOpenConnection が 1 に設定されていた場合にのみ使用されるトラフィックタイプです。

このクエリは、CheckEachNewOpenConnection が 1 で eDirectory がバックリンク処理のために新しい接続を確立する必要がある場合、または CheckEachAlreadyOpenConnection が 1 で eDirectory が既存の接続を再使用する必要がある場合には、常に生成されます。

- ◆ Version ( 入力のみ、タイプ INTEGER)  
eDirectory のバージョン。
- ◆ ExpirationInterval ( 入力および出力、タイプ INTEGER)

ConnectionIsAlreadyOpen が TRUE の場合、ExpirationInterval は、既存の接続ですでに設定されている有効間隔に設定されます。ConnectionIsAlreadyOpen が TRUE 以外の場合、NDS\_BACKLINKS クエリで割り当てられた ExpirationInterval に設定されます。0 の値は、デフォルト (2 時間) を使用する必要があることを示します。終了時には、この変数の値が接続の有効間隔として割り当てられます。

| 値     | 説明                    |
|-------|-----------------------|
| <0, 0 | デフォルト有効間隔を使用 (デフォルト)。 |
| >0    | この接続に割り当てる有効間隔。       |

- ◆ ConnectionIsAlreadyOpen (入力のみ、タイプ BOOLEAN)

eDirectory が既存の接続を再使用できる場合は、この変数は TRUE です。新しい接続を確立する必要がある場合は、この変数は FALSE です。

| 値     | 説明  |
|-------|---|
| TRUE  | eDirectory は、このアドレスへの接続がすでに確立されていて、再使用できると判別します。  |
| FALSE | eDirectory は、このアドレスへの接続を持たないため、新しい接続を確立する必要があります。 |

- ◆ ConnectionLastUsed (入力のみ、タイプ TIME)

ConnectionIsAlreadyOpen が TRUE の場合、ConnectionLastUsed は、この接続を使用して eDirectory から最後にパケットが送信された時点です。

ConnectionIsAlreadyOpen が TRUE 以外の場合、この値は 0 になります。

| 値     | 説明   |
|-------|--|
| TRUE  | <i>ConnectionLastUsed</i> は、この接続上で eDirectory が最後にパケットを送信した時点です。 |
| FALSE | <i>ConnectionLastUsed</i> は 0 になります。                             |

## NDS\_BACKLINKS のサンプル

eDirectory は、バックリンクまたは外部参照をチェックする前に、このアクティビティが許容される時間帯かどうかを WAN トラフィックマネージャに照会します。

NDS\_BACKLINKS には送信先アドレスがないため、NO\_ADDRESSES ポリシーが必要になります。WAN トラフィックマネージャが DONT\_SEND を返した場合は、バックリンクチェックは延期され、再度スケジュールされます。次の変数が使用できます。

- ◆ Last (入力のみ、タイプ TIME)

eDirectory 起動後にバックリンクチェックが最後に実行された時刻。eDirectory が起動されると、*Last* は 0 に初期化されます。NDS\_BACKLINKS が SEND を返した場合は、eDirectory によるバックリンク処理が完了した後で、*Last* は現在の時刻に設定されます。

- ◆ Version (入力のみ、タイプ INTEGER)

eDirectory のバージョン。

◆ ExpirationInterval (出力のみ、タイプ INTEGER)

バックリンク処理中に確立したすべての接続の有効間隔。

| 値     | 説明                    |
|-------|-----------------------|
| <0, 0 | デフォルト有効間隔を使用 (デフォルト)。 |
| >0    | この接続に割り当てる有効間隔。       |

◆ Next (出力のみ、タイプ TIME)

eDirectory が次のバックリンクチェック実行をスケジュールする時点を示します。

| 値    | 説明                 |
|------|--------------------|
| 過去、0 | デフォルトスケジューリングを使用。  |
| 将来   | バックリンクをスケジュールする時点。 |

◆ CheckEachNewOpenConnection (出力のみ、タイプ INTEGER)

バックリンクの実行中に eDirectory が新しい接続を確立する必要が生じた場合の動作を、eDirectory に指示します。

CheckEachNewOpenConnection は 0 に初期化されます。

| 値 | 説明   |
|---|--|
| 0 | WAN トラフィックマネージャを呼び出さずに成功を返します。接続は正常に続行します (デフォルト)。           |
| 1 | WAN トラフィックマネージャを呼び出します。ポリシーにより、接続を許可するかどうかが決まります。            |
| 2 | WAN トラフィックマネージャを呼び出さずに ERR_CONNECTION_DENIED を返します。接続は失敗します。 |

◆ CheckEachAlreadyOpenConnection (出力のみ、タイプ INTEGER)

この変数は、バックリンクの実行中に eDirectory がすでに確立されている接続を再使用する必要が生じた場合の動作を、eDirectory に指示します。

CheckEachAlreadyOpenConnection は 0 に初期化されます。

| 値 | 説明   |
|---|--|
| 0 | WAN トラフィックマネージャを呼び出さずに成功を返します。接続は正常に続行します (デフォルト)。           |
| 1 | WAN トラフィックマネージャを呼び出します。ポリシーにより、接続を許可するかどうかが決まります。            |
| 2 | WAN トラフィックマネージャを呼び出さずに ERR_CONNECTION_DENIED を返します。接続は失敗します。 |

## NDS\_CHECK\_LOGIN\_RESTRICTION のサンプル

eDirectory は、ログイン制限をチェックする前に、このアクティビティが許容される時間帯かどうかを WAN トラフィックマネージャに照会します。トラフィックタイプ NDS\_CHECK\_LOGIN\_RESTRICTIONS には送信先アドレスがないため、NO\_ADDRESSES ポリシーが必要になります。WAN トラフィックマネージャが DONT\_SEND を返した場合は、エラーが発生して、チェックは実行されません。

次の変数が使用できます。

- ◆ Version ( 入力のみ、タイプ INTEGER)

eDirectory のバージョン。

- ◆ Result ( 出力のみ、タイプ INTEGER)

NDS\_CHECK\_LOGIN\_RESTRICTIONS の結果が DONT\_SEND である場合、次の値がオペレーティングシステムに返されます。

| 値 | 説明                           |
|---|------------------------------|
| 0 | ログインが許可されます。                 |
| 1 | 現在の時間ブロック中は、ログインが許可されません。    |
| 2 | アカウントが無効であるか、または有効期限が切れています。 |
| 3 | アカウントが削除されています。              |

- ◆ ExpirationInterval ( 出力のみ、タイプ INTEGER)

この接続に割り当てる有効間隔です。

| 値     | 説明                      |
|-------|-------------------------|
| <0, 0 | デフォルト有効間隔を使用 ( デフォルト )。 |
| >0    | この接続に割り当てる有効間隔。         |

- ◆ CheckEachNewOpenConnection ( 出力のみ、タイプ INTEGER)

| 値 | 説明   |
|---|--|
| 0 | WAN トラフィックマネージャを呼び出さずに成功を返します。接続は正常に続行します ( デフォルト )。         |
| 1 | WAN トラフィックマネージャを呼び出します。ポリシーにより、接続を許可するかどうかが決まります。            |
| 2 | WAN トラフィックマネージャを呼び出さずに ERR_CONNECTION_DENIED を返します。接続は失敗します。 |



- ◆ CheckEachAlreadyOpenConnection (出力のみ、タイプ INTEGER)

| 値 | 説明   |
|---|--|
| 0 | WAN トラフィックマネージャを呼び出さずに成功を返します。接続は正常に続行します (デフォルト)。           |
| 1 | WAN トラフィックマネージャを呼び出します。ポリシーにより、接続を許可するかどうかが決まります。            |
| 2 | WAN トラフィックマネージャを呼び出さずに ERR_CONNECTION_DENIED を返します。接続は失敗します。 |

## NDS\_CHECK\_LOGIN\_RESTRICTION\_OPEN のサンプル

NDS\_CHECK\_LOGIN\_RESTRICTION\_OPEN は、対応する NDS\_CHECK\_LOGIN\_RESTRICTIONS クエリの実行中に CheckEachNewOpenConnection または CheckEachAlreadyOpenConnection が 1 に設定されていた場合にのみ使用されます。このクエリは、CheckEachNewOpenConnection が 1 に設定されていて eDirectory が次の操作を必要とする場合には、常に生成されます。

- ◆ limber を実行する前に新しい接続を確立する。
- ◆ ログイン制限をチェックする前に新しい接続を確立する。
- ◆ 既存の接続を再使用する。

次の変数が使用できます。

- ◆ Version (入力のみ、タイプ INTEGER)  
eDirectory のバージョン。
- ◆ ExpirationInterval (入力および出力、タイプ INTEGER)

| 値     | 説明                    |
|-------|-----------------------|
| <0, 0 | デフォルト有効間隔を使用 (デフォルト)。 |
| >0    | この接続に割り当てる有効間隔。       |

- ◆ ConnectionIsAlreadyOpen (入力のみ、タイプ BOOLEAN)

| 値     | 説明  |
|-------|---|
| TRUE  | eDirectory は、このアドレスへの接続がすでに確立されていて、再使用できると判別します。  |
| FALSE | eDirectory は、このアドレスへの接続を持たないため、新しい接続を確立する必要があります。 |

- ◆ ConnectionLastUsed ( 入力のみ、タイプ TIME)

ConnectionIsAlreadyOpen が TRUE の場合、ConnectionLastUsed は、この接続を使用して eDirectory から最後にパケットが送信された時点です。ConnectionIsAlreadyOpen が TRUE 以外の場合、この値は 0 になります。

| 値     | 説明  |
|-------|---|
| TRUE  | ConnectionLastUsed は、この接続上で eDirectory が最後にパケットを送信した時点です。 |
| FALSE | ConnectionLastUsed は 0 になります。                             |

## NDS\_JANITOR のサンプル

eDirectory は、janitor を実行する前に、このアクティビティが許容される時間帯かどうかを WAN トラフィックマネージャに照会します。NDS\_JANITOR には送信先アドレスがないため、NO\_ADDRESSES ポリシーが必要になります。WAN トラフィックマネージャが DONT\_SEND を返した場合は、janitor 作業は延期され、再度スケジュールされます。

次の変数が使用できます。

- ◆ Last ( 入力のみ、タイプ TIME)

eDirectory 起動後に janitor 作業が最後に実行された時刻。eDirectory が起動されると、Last は 0 に初期化されます。NDS\_JANITOR が SEND を返した場合は、eDirectory によるジャンタ処理が完了した後で、Last は現在の時刻に設定されます。

- ◆ Version ( 入力のみ、タイプ INTEGER)

eDirectory のバージョン。

- ◆ ExpirationInterval ( 出力のみ、タイプ INTEGER)

janitor の実行中に確立したすべての接続の有効間隔。

| 値     | 説明                      |
|-------|-------------------------|
| <0, 0 | デフォルト有効間隔を使用 ( デフォルト )。 |
| >0    | この接続に割り当てる有効間隔。         |

- ◆ Next ( 出力のみ、タイプ TIME)

janitor 作業を次回スケジュールする時点を eDirectory に示します。

| 値    | 説明                     |
|------|------------------------|
| 過去、0 | デフォルトスケジューリングを使用。      |
| 将来   | janitor 作業をスケジュールする時点。 |

- ◆ CheckEachNewOpenConnection (出力のみ、タイプ INTEGER)

janitor の実行中に eDirectory が新しい接続を確立する必要が生じた場合の動作を、eDirectory に指示します。

CheckEachNewOpenConnection は 0 に初期化されます。

| 値 | 説明   |
|---|--|
| 0 | WAN トラフィックマネージャを呼び出さずに成功を返します。接続は正常に続行します (デフォルト)。           |
| 1 | WAN トラフィックマネージャを呼び出します。ポリシーにより、接続を許可するかどうかが決まります。            |
| 2 | WAN トラフィックマネージャを呼び出さずに ERR_CONNECTION_DENIED を返します。接続は失敗します。 |

- ◆ CheckEachAlreadyOpenConnection (出力のみ、タイプ INTEGER)

janitor の実行中に eDirectory がすでに確立されている接続を再使用する必要が生じた場合の動作を、eDirectory に指示します。

CheckEachAlreadyOpenConnection は 0 に初期化されます。

| 値 | 説明   |
|---|--|
| 0 | WAN トラフィックマネージャを呼び出さずに成功を返します。接続は正常に続行します (デフォルト)。           |
| 1 | WAN トラフィックマネージャを呼び出します。ポリシーにより、接続を許可するかどうかが決まります。            |
| 2 | WAN トラフィックマネージャを呼び出さずに ERR_CONNECTION_DENIED を返します。接続は失敗します。 |

## NDS\_JANITOR\_OPEN のサンプル

NDS\_JANITOR\_OPEN は、対応する NDS\_JANITOR クエリの実行中に CheckEachNewOpenConnection または CheckEachAlreadyOpenConnection が 1 に設定されていた場合にのみ使用されます。このクエリは、CheckEachNewOpenConnection が 1 で eDirectory がバックリンク処理の前に新しい接続を確立する必要がある場合、または CheckEachAlreadyOpenConnection が 1 で eDirectory が既存の接続を再使用する必要がある場合には、常に生成されます。

次の変数が使用できます。

- ◆ Version (入力のみ、タイプ INTEGER)

eDirectory のバージョン。

- ◆ ExpirationInterval (入力および出力、タイプ INTEGER)

ConnectionIsAlreadyOpen が TRUE の場合、ExpirationInterval は、既存の接続ですでに設定されている有効間隔に設定されます。ConnectionIsAlreadyOpen が TRUE 以外の場合、NDS\_JANITOR クエリで割り当てられた ExpirationInterval に設定されます。0 の値は、デフォルト (2 時間、10 秒) を使用する必要があることを示します。終了時には、この変数の値が接続の有効間隔として割り当てられます。

| 値     | 説明                      |
|-------|-------------------------|
| <0, 0 | デフォルト有効間隔を使用 ( デフォルト )。 |
| >0    | この接続に割り当てる有効間隔。         |

◆ ConnectionIsAlreadyOpen ( 入力のみ、タイプ BOOLEAN)

eDirectory が既存の接続を再使用する必要がある場合は、この変数は TRUE です。新しい接続を確立する必要がある場合は、この変数は FALSE です。

| 値     | 説明  |
|-------|---|
| TRUE  | eDirectory は、このアドレスへの接続がすでに確立されていて、再使用できると判別します。  |
| FALSE | eDirectory は、このアドレスへの接続を持たないため、新しい接続を確立する必要があります。 |

◆ ConnectionLastUsed ( 入力のみ、タイプ TIME)

ConnectionIsAlreadyOpen が TRUE の場合、ConnectionLastUsed は、この接続を使用して eDirectory から最後にパケットが送信された時点です。ConnectionIsAlreadyOpen が TRUE 以外の場合、この値は 0 になります。

| 値     | 説明  |
|-------|---|
| TRUE  | ConnectionLastUsed は、この接続上で eDirectory が最後にパケットを送信した時点です。 |
| FALSE | ConnectionLastUsed は 0 になります。                             |

## NDS\_LIMBER のサンプル

eDirectory は、limber を実行する前に、このアクティビティが許容される時間帯かどうかを WAN トラフィックマネージャに照会します。トラフィックタイプ NDS\_LIMBER には送信先アドレスがないため、NO\_ADDRESSES ポリシーが必要になります。WAN トラフィックマネージャが DONT\_SEND を返した場合は、limber は延期され、再度スケジュールされます。

次の変数が使用できます。

◆ Last ( 入力のみ、タイプ TIME)

eDirectory 起動後に limber が最後に実行された時刻。

◆ Version ( 入力のみ、タイプ INTEGER)

eDirectory のバージョン。

- ◆ ExpirationInterval (出力のみ、タイプ INTEGER)

limber チェックの実行中に確立したすべての接続の有効間隔。

| 値     | 説明                    |
|-------|-----------------------|
| <0, 0 | デフォルト有効間隔を使用 (デフォルト)。 |
| >0    | この接続に割り当てる有効間隔。       |

- ◆ CheckEachNewOpenConnection (出力のみ、タイプ INTEGER)

| 値 | 説明   |
|---|--|
| 0 | WAN トラフィックマネージャを呼び出さずに成功を返します。接続は正常に続行します (デフォルト)。           |
| 1 | WAN トラフィックマネージャを呼び出します。ポリシーにより、接続を許可するかどうかが決まります。            |
| 2 | WAN トラフィックマネージャを呼び出さずに ERR_CONNECTION_DENIED を返します。接続は失敗します。 |

- ◆ CheckEachAlreadyOpenConnection (出力のみ、タイプ INTEGER)

| 値 | 説明   |
|---|--|
| 0 | WAN トラフィックマネージャを呼び出さずに成功を返します。接続は正常に続行します (デフォルト)。           |
| 1 | WAN トラフィックマネージャを呼び出します。ポリシーにより、接続を許可するかどうかが決まります。            |
| 2 | WAN トラフィックマネージャを呼び出さずに ERR_CONNECTION_DENIED を返します。接続は失敗します。 |

- ◆ Next (出力のみ、タイプ TIME)

次の limber チェック実行の時点。この変数を設定しないと、NDS\_LIMBER ではデフォルトが使用されます。

## NDS\_LIMBER\_OPEN のサンプル

NDS\_LIMBER\_OPEN は、対応する NDS\_LIMBER クエリの実行中に CheckEachNewOpenConnection または CheckEachAlreadyOpenConnection が 1 に設定されていた場合にのみ使用されます。このクエリは、CheckEachNewOpenConnection が 1 に設定されていて eDirectory が limber を実行する前に新しい接続を確立する必要がある場合には、常に生成されます。このクエリは、CheckEachNewOpenConnection が 1 で eDirectory がスキーマ同期の前に新しい接続を確立する必要がある場合、または CheckEachAlreadyOpenConnection が 1 で eDirectory が既存の接続を再使用する必要がある場合には、常に生成されます。

- ◆ Version ( 入力のみ、タイプ INTEGER)  
eDirectory のバージョン。
- ◆ ExpirationInterval ( 入力および出力、タイプ INTEGER)  
この接続に割り当てる有効間隔です。

| 値     | 説明                      |
|-------|-------------------------|
| <0, 0 | デフォルト有効間隔を使用 ( デフォルト )。 |
| >0    | この接続に割り当てる有効間隔。         |

- ◆ ConnectionIsAlreadyOpen ( 入力のみ、タイプ BOOLEAN)

| 値     | 説明  |
|-------|---|
| TRUE  | eDirectory は、このアドレスへの接続がすでに確立されていて、再使用できると判別します。  |
| FALSE | eDirectory は、このアドレスへの接続を持たないため、新しい接続を確立する必要があります。 |

- ◆ ConnectionLastUsed ( 入力のみ、タイプ TIME)

ConnectionIsAlreadyOpen が TRUE の場合、ConnectionLastUsed は、この接続を使用して DS から最後にパケットが送信された時点です。ConnectionIsAlreadyOpen が TRUE 以外の場合、この値は 0 になります。

| 値     | 説明  |
|-------|---|
| TRUE  | ConnectionLastUsed は、この接続上で eDirectory が最後にパケットを送信した時点です。 |
| FALSE | ConnectionLastUsed は 0 になります。                             |

## NDS\_SCHEMA\_SYNC のサンプル

eDirectory は、スキーマを同期する前に、このアクティビティが許容される時間帯かどうかを WAN トラフィックマネージャに照会します。トラフィックタイプ NDS\_SCHEMA\_SYNC には送信先アドレスがないため、NO\_ADDRESSES ポリシーが必要になります。WAN トラフィックマネージャが DONT\_SEND を返した場合は、スキーマ同期は延期され、再度スケジュールされます。

次の変数が使用できます。

- ◆ Last ( 入力のみ、タイプ TIME)  
すべてのサーバに対してスキーマの同期が最後に正常に実行された時刻。
- ◆ Version ( 入力のみ、タイプ INTEGER)  
eDirectory のバージョン。

- ◆ ExpirationInterval (出力のみ、タイプ INTEGER)

スキーマの同期中に確立したすべての接続の有効間隔。

| 値     | 説明                    |
|-------|-----------------------|
| <0, 0 | デフォルト有効間隔を使用 (デフォルト)。 |
| >0    | この接続に割り当てる有効間隔。       |

- ◆ CheckEachNewOpenConnection (出力のみ、タイプ INTEGER)

| 値 | 説明   |
|---|--|
| 0 | WAN トラフィックマネージャを呼び出さずに成功を返します。接続は正常に続行します (デフォルト)。           |
| 1 | WAN トラフィックマネージャを呼び出します。ポリシーにより、接続を許可するかどうかが決まります。            |
| 2 | WAN トラフィックマネージャを呼び出さずに ERR_CONNECTION_DENIED を返します。接続は失敗します。 |

- ◆ CheckEachAlreadyOpenConnection (出力のみ、タイプ INTEGER)

| 値 | 説明   |
|---|--|
| 0 | WAN トラフィックマネージャを呼び出さずに成功を返します。接続は正常に続行します (デフォルト)。           |
| 1 | WAN トラフィックマネージャを呼び出します。ポリシーにより、接続を許可するかどうかが決まります。            |
| 2 | WAN トラフィックマネージャを呼び出さずに ERR_CONNECTION_DENIED を返します。接続は失敗します。 |

## NDS\_SCHEMA\_SYNC\_OPEN のサンプル

NDS\_SCHEMA\_SYNC\_OPEN は、対応する NDS\_SCHEMA\_SYNC クエリの実行中に CheckEachNewOpenConnection または CheckEachAlreadyOpenConnection が 1 に設定されていた場合にのみ使用されます。このクエリは、CheckEachNewOpenConnection が 1 で eDirectory がスキーマ同期の前に新しい接続を確立する必要がある場合、または CheckEachAlreadyOpenConnection が 1 で eDirectory が既存の接続を再使用する必要がある場合には、常に生成されます。

- ◆ Version (入力のみ、タイプ INTEGER)

eDirectory のバージョン。

- ◆ ExpirationInterval ( 入力および出力、タイプ INTEGER)

この接続に割り当てる有効間隔です。

| 値     | 説明                      |
|-------|-------------------------|
| <0, 0 | デフォルト有効間隔を使用 ( デフォルト )。 |
| >0    | この接続に割り当てる有効間隔。         |

- ◆ ConnectionIsAlreadyOpen ( 入力のみ、タイプ BOOLEAN)

| 値     | 説明  |
|-------|---|
| TRUE  | eDirectory は、このアドレスへの接続がすでに確立されていて、再使用できると判別します。  |
| FALSE | eDirectory は、このアドレスへの接続を持たないため、新しい接続を確立する必要があります。 |

- ◆ ConnectionLastUsed ( 入力のみ、タイプ TIME)

ConnectionIsAlreadyOpen が TRUE の場合、ConnectionLastUsed は、この接続を使用して eDirectory から最後にパケットが送信された時点です。ConnectionIsAlreadyOpen が TRUE 以外の場合、この値は 0 になります。

| 値     | 説明  |
|-------|---|
| TRUE  | ConnectionLastUsed は、この接続上で eDirectory が最後にパケットを送信した時点です。 |
| FALSE | ConnectionLastUsed は 0 になります。                             |

## NDS\_SYNC のサンプル

eDirectory がレプリカを同期する必要がある場合は、トラフィックタイプ NDS\_SYNC を使用して、WAN トラフィックマネージャへのクエリが常に生成されます。eDirectory の WAN ポリシーでは、次の変数が使用できます。

- ◆ Last ( 入力のみ、タイプ TIME)  
このレプリカの同期が最後に正常に実行された時刻。
- ◆ Version ( 入力のみ、タイプ INTEGER)  
eDirectory のバージョン。
- ◆ ExpirationInterval ( 出力のみ、タイプ INTEGER)  
更新されたレプリカを保持するサーバへの接続の有効間隔。

| 値     | 説明                      |
|-------|-------------------------|
| <0, 0 | デフォルト有効間隔を使用 ( デフォルト )。 |
| >0    | この接続に割り当てる有効間隔。         |



## ONOSPOOF.WMG

このグループのポリシーでは、既存の WAN 接続のみ使用が許可されます。次の 2 つのポリシーがあります。

- ◆ **Already Open, No Spoofing, NA**

バックリンク、外部参照、およびログイン制限のチェック、Janitor または Limber の実行、スキーマの同期が、既存の WAN 接続上だけに制限されます。

- ◆ **Already Open, No Spoofing**

他のすべてのトラフィックが既存の WAN 接続上だけに制限されます。

すべてのトラフィックを既存の接続上だけに制限するには、両方のポリシーを適用する必要があります。

## OPNSPOOF.WMG

このグループのポリシーでは、既存の WAN 接続のみ使用が許可されますが、15 分間使用されていない接続は無効と見なされます。この場合は使用できません。次の 2 つのポリシーがあります。

- ◆ **Already Open, Spoofing, NA**

このポリシーでは、バックリンク、外部参照、およびログイン制限のチェック、Janitor または Limber の実行、スキーマの同期が、15 分以内に使用されたことがある既存の WAN 接続上だけに制限されます。

- ◆ **Already Open, Spoofing**

このポリシーでは、他のすべてのトラフィックが、15 分以内に使用されたことがある既存の WAN 接続上だけに制限されます。

すべてのトラフィックを 15 分以内に使用されたことがある既存の接続上だけに制限するには、両方のポリシーを適用する必要があります。

## SAMEAREA.WMG

このグループのポリシーでは、同じネットワークエリア内でのみトラフィックが許可されます。ネットワークエリアは、アドレスのネットワークセクションにより決定されます。WAN トラフィックマネージャは、TCP/IP アドレスをクラス C アドレスとして解釈します (クラス C アドレスとは、アドレスの最初の 3 つのセクションが同じで同じネットワークエリアに属するものです)。IPX アドレスでは、ネットワーク部分が同じアドレスはすべて同じネットワークエリアに属すると見なされます。次の 3 つのポリシーがあります。

- ◆ **Same Network Area, NA**

同じネットワークエリア内で生成されるトラフィック以外の場合、バックリンク、外部参照、およびログイン制限のチェック、Janitor または Limber の実行、スキーマの同期が抑止されます。

- ◆ **Same Network Area, TCPIP**

同じ TCP/IP ネットワークエリア内で生成される TCP/IP トラフィック以外の場合、トラフィックが制限されます。

- ◆ **Same Network Area, IXP**

同じ IPX ネットワークエリア内で生成されるトラフィック以外の場合、IPX トラフィックが制限されます。

## TCPIP.WMG

このグループのポリシーでは、TCP/IP トラフィックのみ許可されます。次の 2 つのポリシーがあります。

- ◆ TCPIP, NA

TCP/IP によって生成されたトラフィック以外の場合、バックリンク、外部参照、およびログイン制限のチェック、Janitor または Limber の実行、スキーマの同期が抑止されます。

- ◆ TCPIP

TCP/IP によって生成されたトラフィック以外の場合、他のすべてのトラフィックが抑止されます。

TCP/IP 以外のトラフィックをすべて抑止するには、両方のポリシーを適用する必要があります。

## TIMECOST.WMG

このグループのポリシーでは、すべてのトラフィックが午前 1 時から午前 1 時 30 分までの時間帯だけに制限されますが、同じロケーション内のサーバには連続的な対話が許可されます。このグループでは次のポリシーを使用します。すべてのポリシーを適用する必要があります。

- ◆ COSTLT20

NA およびアドレストラフィックの優先度は 40 です。

- ◆ Disallow Everything

トラフィックの送信がまったく許可されません。セレクタが 0 より大きい値を返したポリシーを WAN トラフィックマネージャが検出できない (0 個のポリシーを検出した) 場合、WAN トラフィックマネージャはデフォルトで SEND を設定します。このポリシーを使用すると、このような事態を抑止できます。

- ◆ NDS Synchronization

NDS\_SYNC トラフィックが午前 1 時と午前 1 時 30 分の間だけに制限されます。

- ◆ Start Rest.Procs, NA

すべてのプロセスを任意の時点に開始することが許可されますが、\*\_OPEN コールごとに WAN トラフィックマネージャに照会する必要があります。WAN トラフィックマネージャは、1 日 4 回 (1:00、7:00、13:00、および 19:00) の実行時刻に合わせてプロセスをスケジュールします。

- ◆ Start Unrest.Procs 1-1:30, NA

すべてのプロセスを午前 1 時と午前 1 時 30 分の間開始して、それ以降 WAN トラフィックマネージャに照会することなく完了するまで実行することが許可されます。プロセスは 1 日 4 回、6 時間ごとに実行されます。1:00 のプロセスはこのポリシーにより処理されますが、それ以外のプロセスは Start Rest. により処理されます。Procs, NA.

# WAN ポリシーの構成

WAN ポリシーは次の 3 つのセクションから構成されます。

- ◆ 319 ページの「宣言セクション」
- ◆ 321 ページの「セクタセクション」
- ◆ 321 ページの「プロバイダセクション」

## 宣言セクション

ポリシーの宣言セクションには、ローカル変数およびクライアントの要求を通して入力される変数の定義が含まれています。これらの定義は、セクタセクションおよびプロバイダセクションで使用されます。これらの変数は、システム定義の変数とともに保存されます。

変数の宣言はセミコロン (;) で区切られます。同じ型の宣言が複数ある場合は、組み合わせることも、複数の行に分割することもできます。行によって宣言が区別されることはありません。宣言セクションの例を次に示します。

```
REQUIRED INT R1;  
REQUIRED TIME R2;  
REQUIRED BOOLEAN R3,R4;  
REQUIRED NETADDRESS R5,R6;  
OPTIONAL INT P1 := 10;  
OPTIONAL BOOLEAN := FALSE;  
LOCAL INT L1 :=10;  
LOCAL INT L2;  
LOCAL TIME L3;  
LOCAL BOOLEAN L4 :=TRUE, L5 :=FALSE;  
LOCAL NETADDRESS L6;
```

使用される必須宣言およびオプション宣言の種類は、トラフィックタイプにより異なります。必須変数が含まれていないポリシーは実行されません。オプション宣言には、何も値が渡されない場合にデフォルトとして使用される値が指定されている必要があります。WAN トラフィックマネージャにより、すべてのトラフィックタイプで使用できるシステムシンボル (定義済み変数) が提供されます。

各宣言は次の 3 つの部分から構成されます。

- ◆ スコープ
- ◆ タイプ
- ◆ 名前とオプション値が対になっているリスト

## スコープ

有効なスコープを次の表に示します。

| スコープ     | 説明   |
|----------|--|
| REQUIRED | スコープが REQUIRED として定義された変数は複数のセクションで使用できますが、宣言セクションでは 1 回しか指定できません。<br><br>REQUIRED スコープ変数に対して値を定義することはできません。この変数の値は GetWanPolicy 要求を通して入力される必要があります。 |

| スコープ     | 説明  |
|----------|---|
| OPTIONAL | <p>スコープが OPTIONAL として定義された変数は1つのポリシーの複数のセクションで使用できますが、宣言セクションでは1回しか指定できません。</p> <p>OPTIONAL スコープ変数にはデフォルト値が割り当てられます。これらの値は初期化されません。これらは、値が渡されない場合にのみ設定されます。名前とタイプの両方が一致するパラメータへ WAN ポリシー要求から新しい値が渡されない場合、ポリシーの処理では宣言で定義された値が使用されます。</p> <p>スコープが OPTIONAL として定義された変数には値を割り当てる必要があります。TIME タイプおよび NETADDRESS タイプは宣言セクションで初期化できないため、これらの変数タイプでは OPTIONAL スコープは使用しないでください。</p> |
| LOCAL    | <p>スコープが LOCAL として定義された変数は複数のセクションで使用できますが、宣言セクションでは1回しか指定できません。</p> <p>LOCAL スコープ変数は特定のポリシーに対してのみ指定されます。つまり、これらの変数の値は呼び出し側クライアントには返されません。</p> <p>すべてのパラメータタイプを定義できます。ただし、TIME タイプおよび NETADDRESS タイプは宣言セクションで初期化できないため、これらのタイプには値を割り当てないでください。</p>  |
| SYSTEM   | <p>スコープが SYSTEM として定義された変数は複数のセクションで使用できますが、宣言セクションでは1回しか指定できません。</p>   |

## タイプ

有効なタイプを次の表に示します。

| タイプ        | 説明   |
|------------|--|
| INT        | <p>ポリシー実行を開始した GetWanPolicy 要求のトラフィックタイプを反映します。たとえば、次のポリシーでは NDS_SYNC のトラフィックタイプが指定されます。</p> <p>IF TrafficType=NDS_SYNC THEN アクションEND.</p> |
| BOOLEAN    | <p>TRUE または FALSE のいずれかの値である場合に使用します。宣言または WAN ポリシー要求で値が設定されていない場合には、値は不定です。</p>   |
| TIME       | <p>TIME スコープ変数は、セクタセクションまたはプロバイダセクションで、あるいは WAN ポリシー要求から値を受け取る必要があります。宣言では TIME スコープ変数に値を割り当てないでください。</p>                                  |
| NETADDRESS | <p>NETADDRESS スコープ変数は、セクタセクションまたはプロバイダセクションで値を受け取る必要があります。宣言では NETADDRESS スコープ変数に値を割り当てないでください。</p>  |

宣言セクションでは、TIME タイプおよび NETADDRESS タイプに値を割り当てることはできません。TIME タイプおよび NETADDRESS タイプが値を持っていない場合、これらのタイプはセクタセクションまたはプロバイダセクションで値を受け取ります。宣言セクションでは、シングルタイプのみ初期化されます。

## 名前とオプション値の対

変数名は、英数字を組み合わせた任意の長さの文字列です。最初の 31 文字だけが使用されるため、変数名の最初の 31 文字は固有の文字列にする必要があります。変数名の最初の文字は英字、または定数値として解釈されるシンボルにする必要があります。

変数名では大文字と小文字が区別されます。たとえば、変数 *R1* と変数 *r1* は異なる変数として解釈されます。変数名ではアンダースコア文字 ( `_` ) を使用できます。

宣言内の値は、変数や式ではなく、定数でなければなりません。つまり、「`LOCAL INT L2:= L3;`」という宣言は許可されません。宣言セクションで変数を初期化する値は、ポリシーのセクタセクションおよびプロバイダセクションで変更できます。

## セクタセクション

ポリシーのセクタセクションは、キーワード `SELECTOR` で始まり、キーワード `END` で終わります。セクタセクションが評価されて、どのロード済みポリシーを使用するかが決定されます。

どのポリシーのウェイトが最大かを判断するために、現在ロード済みのすべてのポリシーのセクタセクションが実行されます。評価後、セクタセクションから 0 ~ 100 の間のウェイトが返されます。0 は、このポリシーを使用しないことを意味します。1 ~ 99 は、さらに大きい値が他のポリシーから返されない限り、このポリシーを使用することを意味します。100 は、このポリシーを使用することを意味します。

セクタセクションの結果は、`RETURN` 宣言で返されます。`RETURN` 宣言がない場合、デフォルト値の 0 が返されます。セクタセクションの例を次に示します。

```
SELECTOR
RETURN 49;
END
```

複数のポリシーのセクタセクションが評価されると、複数のポリシーから同じ値が返されることがあります。この場合、どのポリシーが選択されるかは不定です。他の条件がすべて同じである場合、サーバポリシーが WAN ポリシーに優先します。

宣言を記述する方法の詳細については、[322 ページの「ポリシーセクションで使用される構文」](#)を参照してください。[321 ページの「プロバイダセクション」](#)も参照してください。

## プロバイダセクション

プロバイダセクションは、キーワード `PROVIDER` で始まり、キーワード `END` で終わります。プロバイダセクションの主要部は宣言リストで構成されます。

この宣言リストの結果は、`SEND` または `DONT_SEND` に対するポリシーの提案を表す値になります。

プロバイダセクションの結果は、`RETURN` 宣言で返されます。`RETURN` 宣言がない場合、デフォルト値の `SEND` が返されます。

プロバイダセクションの例を次に示します。

```
PROVIDER
RETURN SEND;
END
```

宣言を記述する方法の詳細については、[322 ページの「ポリシーセクションで使用される構文」](#)を参照してください。

## ポリシーセクションで使用される構文

WAN ポリシーのセレクトセクションおよびプロバイダセクションでは(宣言セクションを除く)、次のステートメントと構文を使用できます。ポリシーの宣言セクションを記述する方法の詳細については、[319 ページの「宣言セクション」](#)を参照してください。

### コメント

コメントを記述するには、行の初めに `/*` を入力し、終わりに `*/` を入力します。例：

```
/* これはコメントです。*/
```

行の終わりで `/**` に続けてコメントを記入することもできます。例：

```
IF L2 > L3 THEN /** これはコメントです。
```

### IF-THEN ステートメント

IF-THEN ステートメントを使用して、宣言ブロックを条件付きで実行します。

例：

```
IF ブール式 THEN 宣言  
END
```

```
IF ブール式 THEN 宣言  
ELSE 宣言  
END
```

```
IF ブール式 THEN 宣言  
ELSIF ブール式 THEN 宣言  
END
```

#### IF ブール式 THEN

これは IF-THEN ステートメントの最初の句です。ブール式が評価され、結果として TRUE または FALSE が返されます。TRUE の場合は、直後の宣言が実行されます。FALSE の場合は、対応する後置の ELSE、ELSIF、または END 宣言にジャンプします。

#### ELSE

対応する IF-THEN 文または ELSIF 文の結果がすべて FALSE になる場合は、ELSE で始まる宣言が実行されます。例：

```
IF ブール式 THEN ステートメント  
ELSIF ブール式 THEN ステートメント  
ELSIF ブール式 THEN ステートメント  
ELSE ステートメント  
END
```

#### ELSIF ブール式 THEN

前置の IF-THEN 宣言から FALSE が返された場合、ブール式が評価されます。ELSIF 宣言が評価され、結果として TRUE または FALSE が返されます。TRUE の場合は、直後の宣言が実行されます。FALSE の場合は、対応する後置の ELSE、ELSIF、または END 宣言にジャンプします。

例：

```
IF ブール式 THEN ステートメント  
ELSIF ブール式 THEN ステートメント  
ELSIF ブール式 THEN ステートメント  
END
```

## END

END 宣言によって IF-THEN 構文が終了します。

## RETURN

RETURN 宣言によって、セレクトアセクションおよびプロバイダセクションの結果が返されます。

### セレクトア

セレクトアセクションでは、ポリシーのウエイトとして使用される整数が RETURN 宣言によって返されます。RETURN は 0 ～ 100 の間のポリシーウエイトを返します。0 は、このポリシーを使用しないことを意味します。1 ～ 99 は、さらに大きい値が他のポリシーから返されない限り、このポリシーを使用することを意味します。100 は、このポリシーを使用することを意味します。セレクトアセクションでは RETURN 宣言がない場合、デフォルト値の 0 が返されます。

宣言を終了するにはセミコロン (;) が必要です。例：

```
RETURN 49;  
RETURN L2;  
RETURN 39+7;
```

### プロバイダ

プロバイダセクションでは、RETURN 宣言によって SEND または DONT\_SEND が返されます。RETURN 宣言がない場合、デフォルト値の SEND が返されます。

宣言を終了するにはセミコロン (;) が必要です。例：

```
RETURN SEND;  
RETURN DONT_SEND;  
RETURN L1;
```

## 割り当て

割り当て宣言では、:= 文字を使用してシンボルの値が変更されます。定義済み変数またはシステム変数を最初に指定し、:= に続いて値、変数、または演算式を指定します。代入宣言の終わりには、セミコロン (;) が必要です。例：

*変数. フィールド := 式; 変数 := 式;*

t1 と t2 はタイプ TIME、i1 と i2 はタイプ INTEGER、b1 と b2 はタイプ BOOLEAN の有効な割り当てです。

```
t1 := t2;  
b1 := t1 < t2;  
i1 := t1.mday - 15;  
b2 := t2.year < 2000
```

無効な割り当ての例を示します。

```
b1 := 10 < i2 < 12;
```

(10 < i2) はブール式です。BOOLEAN を INTEGER と比較することはできません。

b1 := (10 < i2) AND (i2 < 12); を使用します。例：

```
    b2 := i1;
```

b2 は BOOLEAN で、i1 は INTEGER です。BOOLEAN と INTEGER は型が整合しません。

代わりに、b2 := i1 > 0; を使用します。

厳密なタイプのチェックが行われます。TIME 変数に INT を割り当てることはできません。

## 算術演算子

割り当て宣言、RETURN 宣言、または IF 構文内で、算術演算子を使用できます。有効な演算子は次のとおりです。

- ◆ 加算 (+)
- ◆ 減算 (-)
- ◆ 除算 (/)
- ◆ 乗算 (\*)
- ◆ モジュール (MOD)

算術演算子とともに使用できるのは INT 変数タイプだけです。算術式で、TIME、NETADDRESS、または BOOLEAN 変数タイプは使用しないでください。

結果が -2147483648 ~ +2147483648 の範囲外の値になる演算、または 0 による除算は行わないでください。

## 関係演算子

IF 構文で関係演算子を使用できます。有効な演算子は次のとおりです。

- ◆ 等しい (=)
- ◆ 等しくない (<>)
- ◆ より大きい (>)
- ◆ 以上 (>=)
- ◆ より小さい (<)
- ◆ 以下 (<=)

関係演算子は、TIME および INT 変数タイプで使用できます。<> および = は、NET ADDRESS および BOOLEAN 変数タイプでも使用できます。



## 論理演算子

有効な演算子は次のとおりです。

- ◆ AND
- ◆ OR
- ◆ NOT
- ◆ より小さい (<)
- ◆ より大きい (>)
- ◆ 等しい (=)

## ビットワイズ演算子

INT 変数タイプでビットワイズ演算子を使用して、整数値を返すことができます。有効な演算子は次のとおりです。

- ◆ BITAND
- ◆ BITOR
- ◆ BITNOT

## 複合演算

複合演算を処理するときは、次の優先規則が適用されます。同じ優先順位の演算子には、左から右へ優先順位が付けられます。優先順位は次のとおりです。

- ◆ カッコ
- ◆ 単項 (+/-)
- ◆ BITNOT
- ◆ BITAND
- ◆ BITOR
- ◆ 乗算、除算、MOD
- ◆ 加算、減算
- ◆ 関係 (>, >=, <, <=, =)
- ◆ NOT
- ◆ AND
- ◆ OR

優先順位が明確でない場合は、カッコを使用します。たとえば、A、B、および C が整数または変数の場合、 $A < B < C$  は許可されません。A < B では、整数値ではなくブール値が返されるので、整数 C と比較することはできません。しかし、 $(A < B) \text{ AND } (B < C)$  は文法的に正しい式です。

## PRINT

PRINT 宣言を使用して、サーバの WAN トラフィックマネージャ表示画面およびログファイルに、テキストやシンボルの値を送ることができます。

PRINT ステートメントには、リテラル文字列、シンボル名やシンボルメンバー、整数値、またはブール値などの引数をコンマで区切って、いくつでも指定できます。

リテラル文字列は二重引用符 (“ ”) で囲む必要があります。PRINT 宣言の終わりには、セミコロン (;) が必要です。例：

```
PRINT "INT=",10,"BOOL=",TRUE,"SYM=",R1;
```

TIME および NETADDRESS 変数では、フォーマット化された PRINT 宣言が使用されます。TIME シンボルは次のよう出力されます。

```
m:d:y h:m
```

NETADDRESS 変数は次のよう出力されます。

*タイプ 長さ データ*

タイプは IP または IPX のいずれかで、長さはバイト数、データは 16 進のアドレス文字列です。

# 12 LDAP Services for Novell eDirectory について

LDAP (Lightweight Directory Access Protocol) は、クライアントアプリケーションでディレクトリ情報にアクセスするためのインターネット通信プロトコルです。LDAP は、X.500 DAP (Directory Access Protocol) に基づいていますが、従来のクライアントほど複雑ではなく、X.500 標準に基づくその他のディレクトリサービスと同時に使用することができます。

一般に、LDAP は最も単純なディレクトリアクセスプロトコルとして使用されます。

LDAP (Lightweight Directory Access Protocol) Services for Novell® eDirectory™ サーバアプリケーションを使用すると、eDirectory 内に格納されている情報に LDAP クライアントからアクセスできます。

LDAP サービスには、LDAP を通じて利用できる次のような eDirectory 機能が含まれます。

- ◆ プロビジョニング
- ◆ アカウント管理
- ◆ 認証
- ◆ 許可
- ◆ 識別情報管理
- ◆ 通知
- ◆ レポートニング
- ◆ 認定
- ◆ セグメンテーション

クライアントごとに異なるディレクトリアクセスレベルを設定して、ディレクトリにアクセスするための安全な接続を確立できます。このセキュリティメカニズムを利用すると、一般に公開するディレクトリ情報、組織内で利用する情報、および特定のグループまたは個人だけが利用できる情報を区別して管理できます。

各 LDAP クライアントで利用できるディレクトリ機能は、LDAP クライアントおよび LDAP サーバに組み込まれた機能により異なります。たとえば、LDAP Services for eDirectory を利用すると、LDAP クライアントは eDirectory データベース内のデータを読み書きできます。ただし、これには LDAP クライアントに必要な許可が与えられている必要があります。クライアントは、ディレクトリデータの読み書きが許可される場合と、読み込みしか許可されない場合があります。

一般的なクライアント機能を利用すると、クライアントから次のような処理を実行できます。

- ◆ 電子メールアドレスや電話番号など、特定の個人についての情報を検索する。
- ◆ 特定の姓または特定の文字で始まる姓を持つすべての個人の情報を検索する。
- ◆ 任意の eDirectory オブジェクトまたはエントリについての情報を検索する。

- ◆ 氏名、電子メールアドレス、勤務先電話番号、および自宅電話番号を取得する。
- ◆ 会社名および市町村名を取得する。

以降のセクションで、LDAP Services for eDirectory について説明します。

- ◆ 328 ページの「LDAP サービスの主な用語」
- ◆ 331 ページの「LDAP と eDirectory の連携について」
- ◆ 340 ページの「Linux、Solaris、AIX、または HP-UNIX 環境での LDAP ツールの使用」
- ◆ 350 ページの「拡張可能一致検索フィルタ」

LDAP サービスの詳細については、『*Novell LDAP Developer Documentation (Novell LDAP 開発マニュアル)*』([http://developer.novell.com/ndk/doc\\_novell\\_edirectory.htm](http://developer.novell.com/ndk/doc_novell_edirectory.htm)) を参照してください。

LDAP の詳細については、次の Web サイトを参照してください。

- ◆ ミシガン大学 (<http://www.umich.edu/~dirsvcs/ldap/ldap.html>)
- ◆ LDAP Roadmap & FAQ (<http://www.kingsmountain.com/ldapRoadmap.shtml>)
- ◆ LDAPzone.com (<http://www.ldapzone.com>)

## LDAP サービスの主な用語

### クライアントとサーバ

**LDAP クライアント** — Netscape\* Communicator\*、Internet Explorer、Novell インポート / エクスポート変換ユーティリティなどのような 1 つのアプリケーションです。

**LDAP サーバ** — nldap.nlm (NetWare® の場合)、nldap.dlm (Windows 2000/NT の場合)、libnldap.so (Linux、Solaris および AIX システムの場合)、または libnldap.sl (HP-UX システムの場合) が稼動するサーバ。

### オブジェクト

**LDAP グループオブジェクト** — LDAP サーバで Novell LDAP プロパティの設定と管理を行います。

このオブジェクトは eDirectory のインストール時に作成されます。LDAP グループオブジェクトには、複数の LDAP サーバ間で共有できる便利な設定情報が含まれています。

**LDAP サーバオブジェクト** — LDAP クライアントによる情報へのアクセスおよび使用方法の設定と管理を Novell LDAP サーバで行います。

このオブジェクトは eDirectory のインストール時に作成されます。LDAP サーバオブジェクトとは、サーバ固有の設定データのことで、

次の図は、Novell iManager の LDAP サーバオブジェクトを表したものです。

#### LDAP の概要

LDAPグループの表示 LDAPサーバの表示

 LDAP Server - LUNDI.AKRANES

## 参照

**参照** – LDAP サーバが LDAP クライアントに送信するメッセージです。このサーバからは結果がすべて提供されず、他の LDAP サーバにまだデータがある可能性をクライアントに通知します。

参照には、操作を続行するのに必要な情報がすべて含まれます。

シナリオ：LDAP クライアントが LDAP サーバに要求を送信しますが、サーバは操作のターゲットエントリをローカルで見つけることができません。その場合、LDAP サーバはパーティションおよび他のサーバに関して所有する知識参照を使用して、そのエントリについてより多くの知識を持つ別のサーバを特定します。LDAP サーバは参照情報をクライアントに送信します。

クライアントは識別されたサーバに対する新しい LDAP 接続を確立し、操作を再試行します。

参照には次の利点があります。

- ◆ LDAP クライアントが操作を制御し続けます。

常に状況を把握することにより、クライアントはよりの確な判断ができ、ユーザにフィードバックを返すことができます。また、参照を検索しない選択をしたり、検索の前にユーザに確認メッセージを表示することもできます。

- ◆ 多くの場合、参照の方がチェーンよりもリソースを効果的に使用できます。

チェーンでは、エントリの多い検索操作が要求されると、ネットワーク全体に2度送信される場合があります。1度目はデータのあるサーバからチェーンを実行するサーバへの送信です。2度目はチェーンを実行するサーバからクライアントへの送信です。

参照では、クライアントはデータのあるサーバから、1回の送信で直接データを受け取ることができます。

- ◆ エントリの格納場所がわかっている場合、クライアントは直接データのあるサーバにアクセスすることができます。

チェーンでは、クライアントは詳細を見ることはできません。エントリの格納場所がわからない場合、クライアントが直接データのあるサーバにアクセスすることはできません。

参照には次の欠点があります。

- ◆ クライアントが参照とその検索方法を認識できる能力が必要です。
- ◆ LDAPv2 クライアントでは参照結果が認識されないか、認識に古い非標準の方法が使用されます。
- ◆ すべての eDirectory パーティションに LDAP サーバのサービスが適用されていない場合があります。

適用されていない場合、参照結果をパーティションのデータに送信できません。

**上方参照** — 通信中のサーバのデータよりもツリーの高い位置にあるデータを持つサーバを参照することです。379 ページの「**上方参照を設定する**」を参照してください。

上方参照では、マルチベンダツリーで、上方または隣接した非 eDirectory パーティションにあるオブジェクトに関する要求が処理されます。

eDirectory サーバがこのタイプのツリーに含まれるようにするには、eDirectory は非信頼とマークされたパーティション内で、階層データを上方に保持するようにします。非信頼領域のオブジェクトは、正しい DN 階層を構築するのに必要なエントリのみから構成されます。これらのエントリは、X.500 の「Glue」エントリに類似しています。

eDirectory では、知識情報を LDAP 参照データの形式で非信頼領域に配置できます。この情報は、LDAP クライアントに参照を返すのに使用します。

LDAP 操作を eDirectory ツリーの信頼されていない領域で実行すると、LDAP サーバは正しい参照データを検索し、クライアントに参照を返します。

**チェーン** — サーバベースのネームレゾリューションプロトコル。

LDAP クライアントは LDAP サーバに要求を送信しますが、LDAP サーバは操作のターゲットエントリをローカルで見つけることができません。LDAP サーバ (サーバ A) は eDirectory ツリーのパーティションおよび他のサーバに関して所有する知識参照を使用して、DN についてより多くの知識を持つ、別の LDAP サーバ (サーバ B) を特定します。LDAP サーバ A は、特定された LDAP サーバ B と通信します。

必要に応じ、サーバ A がエントリのレプリカを持つサーバに接続するまでこの処理が続けられます。その後、eDirectory は詳細をすべて処理し、操作を完了します。サーバ間の処理はクライアントには表示されないため、クライアントは最初のサーバ A が要求を処理したものと判断します。

LDAP サーバにチェーンを使用した場合、次の利点があります。

- ◆ ネームレゾリューションの詳細をすべてクライアントから見えなくします。
- ◆ 自動で再認証を行います。
- ◆ クライアントのプロキシの役割を果たします。
- ◆ eDirectory ツリーに LDAP サービスをサポートしないサーバがあっても、シームレスに実行されます。

一方、チェーンには次の欠点があります。

- ◆ チェーンを使用して名前解決中には、サーバからのフィードバックがなくクライアントが待機する必要がある場合があります。
- ◆ LDAP サーバが、WAN リンク経由で多くのエントリを送信するよう要求された場合、処理に長時間かかることがあります。
- ◆ ほぼ同じ処理能力を持つサーバがいくつかある場合、別々のサーバが 2 つの要求を同じエントリ上で処理してしまうことがあります。

eDirectory は、サーバを接続コスト順にソートしようとします。負荷分散のため、eDirectory は一番コストの低いサーバの中からランダムに選択を行います。

# LDAP と eDirectory の連携について

このセクションでは次について説明します。

- ◆ [331 ページの「LDAP から eDirectory に接続する」](#)
- ◆ [334 ページの「クラスと属性のマッピング」](#)
- ◆ [337 ページの「非標準スキーマ出力を有効にする」](#)
- ◆ [338 ページの「構文の相違」](#)
- ◆ [339 ページの「サポートされる Novell LDAP コントロールおよび拡張」](#)

## LDAP から eDirectory に接続する

すべての LDAP クライアントが、次のいずれかのユーザタイプで Novell eDirectory にバインド (接続) されます。

- ◆ [Public] ユーザ (匿名バインド)
- ◆ プロキシユーザ (プロキシユーザ匿名バインド)
- ◆ NDS または eDirectory ユーザ (NDS ユーザバインド)

ユーザの認証に使用されるバインドタイプにより、LDAP クライアントがアクセスできる内容が決定されます。LDAP クライアントは、作成した要求をディレクトリに送信することにより、ディレクトリにアクセスします。LDAP クライアントが LDAP Services for eDirectory を通じて要求を送信した場合、eDirectory は、その中から LDAP クライアントが適切なアクセス権を持つ属性の要求だけを処理します。

たとえば LDAP クライアントが、読み込み権が必要なある属性値を要求したものの、その属性についてユーザに許可されているのが比較権だけである場合、この要求は拒否されます。

標準ログイン制限とパスワード制限は引き続き適用されます。ただし、制限はすべて LDAP の実行場所と関係します。時刻およびアドレス制限も適用されますが、アドレス制限は eDirectory ログインが実行された場所 (この場合は LDAP サーバ) を基準に決定されます。

### [Public] ユーザとして接続する

匿名バインドは、ユーザ名またはパスワードを使用しない接続です。サービスでプロキシユーザの使用が設定されていない場合、名前とパスワードが定義されていない LDAP クライアントで LDAP Services for eDirectory にバインドすると、ユーザは eDirectory に [Public] ユーザとして認証されます。

[Public] ユーザとは、非認証の eDirectory ユーザのことです。デフォルトでは、[Public] ユーザには eDirectory ツリー内のオブジェクトのブラウズ権が割り当てられます。

[Public] ユーザ用のデフォルトブラウズ権では、eDirectory オブジェクトを参照することはできませんが、ほとんどのオブジェクト属性にアクセスすることはできません。

多くの場合、LDAP クライアントは、デフォルトの [Public] 権だけでは不十分です。[Public] の権利は変更できますが、変更した権利はすべてのユーザに対して許可されることとなります。この問題を解決するために、プロキシユーザ匿名バインドを使用することをお勧めします。詳細については、[332 ページの「プロキシユーザとして接続する」](#)を参照してください。

[Public] ユーザによるオブジェクト属性へのアクセスを許可するには、[Public] ユーザを該当する (1 つまたは複数の) コンテナのトラスティに設定し、適切なオブジェクト権および属性権を割り当てる必要があります。

## プロキシユーザとして接続する



プロキシユーザ匿名バインドは、eDirectory ユーザ名にリンクされた匿名接続です。プロトコルでプロキシユーザの使用が設定されている場合、LDAP クライアントが LDAP for eDirectory に匿名でバインドすると、ユーザは eDirectory によりプロキシユーザとして認証されます。LDAP Services for eDirectory と eDirectory の両方でユーザ名が設定されます。

通常、匿名バインドには LDAP のポート 389 が使用されます。ただし、ポートはインストール時に手動で変更することができます。

次に、プロキシユーザ匿名バインドの概念について説明します。

- ◆ 匿名バインドを経由する LDAP クライアントアクセスは、すべてプロキシユーザオブジェクトを通して割り当てられます。
- ◆ 匿名バインドでは LDAP クライアントからパスワードが提供されないため、プロキシユーザに null パスワードを適用し、パスワード変更間隔などのパスワード制限を設定しないようにします。パスワードを強制的に有効期限切れにしたり、プロキシユーザにパスワードの変更を許可したりしないでください。
- ◆ プロキシユーザオブジェクトのアドレス制限を設定すると、ユーザがログインできるロケーションを制限できます。
- ◆ eDirectory 内にプロキシユーザオブジェクトを作成し、公開する eDirectory オブジェクトに対する権利を割り当てる必要があります。デフォルトのユーザ権では、特定のオブジェクトと属性だけに対する読み込みアクセス権が許可されます。アクセスする必要がある各サブツリー内のすべてのオブジェクトと属性に対するプロキシユーザ読み込み権および検索権を割り当てます。
- ◆ LDAP Services for eDirectory を設定する LDAP グループオブジェクトの [全般] ページで、プロキシオブジェクトを有効化する必要があります。このため、1つの LDAP グループ内のすべてのサーバに対し、プロキシユーザオブジェクトは1つしか作成できません。詳細については、[358 ページの「LDAP オブジェクトを環境設定する」](#)を参照してください。
- ◆ プロキシユーザオブジェクトに対し、すべてのプロパティ(デフォルト)か、選択したプロパティの権利を許可できます。


プロキシユーザに対して選択したプロパティの権利だけを許可するには、次を実行します。

- 1 Novell iManager で、[役割およびタスク] ボタン  をクリックします。
- 2 [権利] > [トラスティの変更] の順にクリックします。
- 3 プロキシユーザが権利を持つ最上部のコンテナの名前とコンテキストを指定するか、 をクリックし、問題のコンテナを参照して [OK] をクリックします。
- 4 [トラスティの変更] 画面で [トラスティの追加] をクリックします。
- 5 プロキシユーザのオブジェクトを参照し、[OK] をクリックします。
- 6 追加したプロキシユーザの左側にある [割り当てられた権利] をクリックします。
- 7 [すべての属性権] および [エントリ権] チェックボックスをオンにし、[プロパティの削除] をクリックします。



- 8 [プロパティの追加] をクリックし、[スキーマ内のすべてのプロパティを表示する] チェックボックスをオンにします。
- 9 メールボックス (リストの小文字のセクション) や役職など、プロキシユーザが継承可能な権利を選択し、[OK] をクリックします。  
その他の継承可能な権利を追加する場合は、手順 9 ~ 10 を繰り返します。
- 10 [完了] をクリックし、[OK] をクリックします。

プロキシユーザ匿名バインドを実装するには、eDirectory 内にプロキシユーザオブジェクトを作成し、そのユーザに適切な権利を割り当てる必要があります。アクセスする必要がある各サブツリー内のすべてのオブジェクトと属性に対するプロキシユーザ読み込み権および検索権を割り当てます。同じプロキシユーザ名を指定して、LDAP Services for eDirectory 内でプロキシオブジェクトを有効化する必要があります。

- 1 Novell iManager で、[役割およびタスク] ボタン  をクリックします。
- 2 [LDAP] > [LDAP の概要] の順にクリックします。
- 3 設定する LDAP グループオブジェクトの名前をクリックします。
- 4 [プロキシユーザ] フィールドに eDirectory ユーザオブジェクトの名前とコンテキストを指定します。
- 5 [適用] をクリックし、[OK] をクリックします。

## Linux および UNIX の ldapconfig を使用する

たとえば、LDAP Search Referral Usage で LDAP サーバによる LDAP 参照の処理方法を指定します。

- 1 システムプロンプトで、次のコマンドを入力します。  

```
ldapconfig -s "LDAP:otherReferralUsage=1"
```
- 2 ユーザ FDN (完全識別 eDirectory ユーザ名) とパスワードを入力します。

## NDS または eDirectory ユーザとして接続する

eDirectory ユーザバインドは、LDAP クライアントが完全な eDirectory ユーザ名とパスワードを使用して確立する接続です。eDirectory ユーザバインドは eDirectory により認証されます。LDAP クライアントは、その eDirectory ユーザにアクセスが許可されているすべての情報にアクセスできます。

次に、eDirectory ユーザバインドに関する重要な概念について説明します。

- ◆ eDirectory ユーザバインドは、LDAP クライアントに入力されたユーザ名とパスワードを使用して eDirectory により認証されます。
- ◆ LDAP クライアントアクセスに使用する eDirectory ユーザ名とパスワードは、NetWare クライアントが eDirectory にアクセスする場合も使用できます。
- ◆ 非 TLS 接続では、eDirectory パスワードは LDAP クライアントと LDAP Services for eDirectory の間の経路をクリアテキストデータとして転送されます。
- ◆ クリアテキストパスワードが無効に設定されている場合は、非 TLS 接続上で転送されたユーザ名またはパスワードを含む eDirectory バインド要求は、すべて拒否されます。
- ◆ eDirectory ユーザパスワードの有効期限が切れた場合、そのユーザの eDirectory バインド要求は拒否されます。

## LDAP クライアントに eDirectory 権を割り当てる

**1** LDAPクライアントがeDirectoryにアクセスするときに使用するユーザ名のタイプを決定します。

- ◆ [Public] ユーザ (匿名バインド)
- ◆ プロキシユーザ (プロキシユーザ匿名バインド)
- ◆ NDS ユーザ (NDS ユーザバインド)

詳細については、[331 ページの「LDAP から eDirectory に接続する」](#)を参照してください。

**2** ユーザが1つのプロキシユーザまたは複数の eDirectory ユーザ名でLDAPにアクセスする場合、iManager を使用して、eDirectory 内または LDAP でこれらのユーザ名を作成します。

**3** LDAP クライアントが使用するユーザ名に、適切な eDirectory 権を割り当てます。

ほとんどのユーザに割り当てられるデフォルトの権利では、ユーザ自身が持つオブジェクト以外にはアクセスできません。別のオブジェクトやその属性にアクセスするには、eDirectory で割り当てられた権利を変更する必要があります。

LDAP クライアントから eDirectory オブジェクトおよび属性へのアクセスが要求されると、eDirectory は、LDAP クライアントの eDirectory 識別情報に基づいて要求を受諾または拒否します。識別情報はバインド時に設定されます。

## クラスと属性のマッピング

クラスとは、ディレクトリ内のオブジェクトのタイプ (ユーザ、サーバ、グループなど) です。属性とは、特定のオブジェクトについての追加情報を定義するディレクトリ要素です。たとえば、ユーザオブジェクト属性にはユーザの姓、電話番号などがあります。


スキーマとは、ディレクトリで使用できるクラスと属性、およびディレクトリ構造 (クラス間の相互関係) を定義する一連の規則です。LDAP ディレクトリと eDirectory ディレクトリのスキーマが異なる場合は、LDAP クラスと属性を、適切な eDirectory オブジェクトと属性へマッピングしなければならない場合があります。これらのマッピングで、LDAP スキーマから eDirectory スキーマへの名前の変換を定義します。

LDAP Services for eDirectory にはデフォルトマッピングがあります。LDAP クラスおよび属性と、eDirectory オブジェクトタイプおよびプロパティとの対応関係は多くの場合論理的で、直観的に理解できます。ただし、実装時の条件によっては、クラスと属性のマッピングを再設定する必要が生じることもあります。

ほとんどの場合、LDAP クラスと eDirectory オブジェクトタイプとの間のマッピングは、一対一の対応関係です。ただし、LDAP スキーマでは、同じ属性を意味する CN および共通名のような別名もサポートされています。

## LDAP グループ属性をマッピングする

デフォルトの LDAP Services for eDirectory 環境設定には、定義済みのクラスと属性のマッピングが保存されています。これは、LDAP 属性のサブセットから eDirectory 属性のサブセットへのマッピングです。デフォルト環境設定でマッピングされていない属性には、自動生成されたマッピングが割り当てられます。スキーマ名がスペースまたはコロンを含まない有効な LDAP 名である場合は、マッピングは必要ありません。クラスおよび属性のマッピングを調べて、必要に応じて再設定します。

- 1 Novell iManager で、[役割およびタスク] ボタン  をクリックします。
- 2 [LDAP] > [LDAP の概要] > [LDAP グループの表示] の順にクリックします。
- 3 LDAP グループオブジェクトをクリックし、[属性マップ] をクリックします。
- 4 必要に応じて属性を追加、削除、または変更します。


LDAP 属性の種類によっては別名 (CN および共通名など) が存在する場合がありますため、複数の LDAP 属性を対応する 1 つの eDirectory 属性名にマッピングする必要があることがあります。LDAP Services for eDirectory が LDAP 属性情報を返す場合、リスト内で検出された最初の一致する属性の値が返されます。

複数の LDAP 属性を 1 つの eDirectory 属性にマッピングする場合は、属性の順序に意味があります。リスト内の順序を変更することにより、属性の優先度を変更できます。

- 5 [適用] をクリックし、[OK] をクリックします。

## LDAP グループクラスをマッピングする

LDAP クライアントが LDAP サーバに LDAP クラス情報を要求すると、サーバは対応する eDirectory クラス情報を返します。デフォルトの LDAP Services for eDirectory 環境設定には、定義済みのクラスと属性のマッピングが保存されています。

- 1 Novell iManager で、[役割およびタスク] ボタン  をクリックします。
- 2 [LDAP] > [LDAP の概要] の順にクリックします。
- 3 LDAP グループオブジェクトをクリックし、[クラスマップ] をクリックします。
- 4 必要に応じてクラスを追加、削除、または変更します。

デフォルトの LDAP Services for eDirectory 環境設定には、定義済みのクラスと属性のマッピングが保存されています。これは、LDAP クラスと属性のサブセットから eDirectory クラスと属性のサブセットへのマッピングです。デフォルト環境設定でマッピングされていない属性またはクラスには、自動生成されたマッピングが割り当てられます。

スキーマ名がスペースまたはコロンを含まない有効な LDAP 名である場合は、マッピングは必要ありません。クラスおよび属性のマッピングを調べて、必要に応じて再設定します。

- 5 [適用] をクリックし、[OK] をクリックします。

## LDAP クラスと属性をマッピングする

LDAP ディレクトリと eDirectory ディレクトリのスキーマは異なるため、LDAP クラスと属性を、適切な eDirectory オブジェクトと属性へマッピングする必要があります。これらのマッピングで、LDAP スキーマから eDirectory スキーマへの名前の変換を定義します。

有効な LDAP スキーマ名であれば、スキーマエントリに対する LDAP スキーママッピングは必要ありません。LDAP では、スキーマ名で使用できる文字は英数字とハイフン記号 (-) だけです。LDAP スキーマ名ではスペースは使用できません。

スキーマを LDAP の外部に拡張する場合、.sch ファイルなど LDAP の外部にスキーマを拡張した後でオブジェクト ID による検索を確実に実行するには、LDAP サーバ環境設定をリフレッシュする必要があります。

## 多対一マッピング

eDirectory から LDAP をサポートするために、LDAP Services は、(ディレクトリサービスレベルではなく)プロトコルレベルのマッピングを使用して、LDAP と eDirectory の間で属性とクラスを変換します。したがって、2つの LDAP クラスまたは属性を同じ eDirectory クラスまたは属性にマッピングできます。

たとえば、LDAP を使用して Cn を作成し、CommonName=Value を検索すると、Cn と属性値が同じ可能性のある commonName が返されます。

すべての属性を要求すると、そのクラスのマッピングリストの最初にある属性が返されます。名前で属性を要求すると、正しい名前が返されます。

### 多対一クラスマッピング

| LDAP クラス名                                   | eDirectory クラス名 |
|---|-----------------|
| alias<br>aliasObject                        | Alias           |
| groupOfNames<br>groupOfUniqueNames<br>group | Group           |
| mailGroup<br>rfc822mailgroup                | NSCP:mailGroup1 |

### 多対一属性マッピング

| LDAP 属性名                            | eDirectory 属性名 |
|-------------------------------------|----------------|
| c<br>countryName                    | C              |
| cn<br>commonName                    | CN             |
| uid<br>userId                       | uniqueID       |
| description<br>multiLineDescription | 説明             |

| LDAP 属性名  | eDirectory 属性名            |
|---|---------------------------|
| l<br>localityname   | L                         |
| member<br>uniqueMember  | Member                    |
| o<br>organizationname   | O                         |
| ou<br>organizationalUnitName                                  | OU                        |
| sn<br>surname   | Surname                   |
| st<br>stateOrProvinceName                                     | S                         |
| certificateRevocationList;binary<br>certificateRevocationList | certificateRevocationList |
| authorityRevocationList;binary<br>authorityRevocationList     | authorityRevocationList   |
| deltaRevocationList;binary<br>deltaRevocationList             | deltaRevocationList       |
| cACertificate;binary<br>cACertificate                         | cACertificate             |
| crossCertificatePair;binary<br>crossCertificatePair           | crossCertificatePair      |
| userCertificate;binary<br>userCertificate                     | userCertificate           |

注：;binary の付いた属性はセキュリティに関連しています。アプリケーションに必要な名前が ;binary を付けて取得される場合は、マッピングテーブルから属性を適用します。名前を ;binary を付けずに取得する場合は、マッピングの順序を変更できます。

## 非標準スキーマ出力を有効にする

eDirectory には、互換モードスイッチがあります。この機能により、非標準スキーマ出力が使用できるため、現行の ADSI クライアント および従来の Netscape\* クライアント でスキーマを読み込むことができます。このスイッチは、LDAP サーバオブジェクト内の属性を設定することにより実装されます。属性名は nonStdClientSchemaCompatMode です。通常の場合、LDAP サーバオブジェクトはサーバオブジェクトと同じコンテナ内にあります。

非標準出力は、LDAP 用の現行 IETF 規格には適合しませんが、現行バージョンの ADSI クライアントおよび従来の Netscape クライアントでは正常に処理できます。


非標準出力の出力形式は次のとおりです。

- ◆ SYNTAX OID は一重引用符で囲まれます。
- ◆ 上限は出力されません。
- ◆ X- オプションは出力されません。

- ◆ 複数の名前が存在する場合は、最初に検出された名前だけが出力されます。
- ◆ OID が定義されていない属性やクラスは、それぞれ小文字で「`attributename-oid`」、「`classname-oid`」と出力されます。
- ◆ 名前にハイフンが含まれていて OID が定義されていない属性またはクラスは出力されません。

OID またはオブジェクト識別子は、自身の属性または `objectclass` を LDAP サーバに追加するのに必要なオクテット数値の文字列です。

非標準スキーマ出力を有効化するには、次を実行します。

- 1 Novell iManager で、[役割およびタスク] ボタン  をクリックします。
- 2 [LDAP] > [LDAP の概要] の順にクリックします。
- 3 [LDAP サーバの表示] をクリックし、LDAP サーバオブジェクトをクリックします。
- 4 [検索] をクリックし、[古い ADSI および Netscape スキーマ出力を有効にする] をクリックします。  
非標準の出力は、現在 IETF が LDAP について定義している規格に準拠していませんが、現在の ADSI クライアント および以前の Netscape クライアント では動作します。
- 5 [適用]、[情報] の順にクリックし、[リフレッシュ] をクリックします。

## 構文の相違

LDAP と eDirectory では使用される構文が異なります。次のような重要な相違点があります。

- ◆ 338 ページの「コンマ」
- ◆ 338 ページの「タイプ付きの名前」
- ◆ 339 ページの「エスケープ文字」
- ◆ 339 ページの「複数のネーミング属性」

### コンマ

LDAP では、区切り記号としてピリオドではなくコンマを使用します。たとえば、eDirectory の識別名 (完全名) は次のように記述します。

CN=JANEB.OU=MKTG.O=EMA

LDAP 構文を使用すると、同じ識別名は次のようになります。

CN=JANEB,OU=MKTG,O=EMA

また、次は別の LDAP 識別名の例です。

CN=Bill Williams,OU=PR,O=Bella Notte Corp

CN=Susan Jones,OU=Humanities,O=University College London,C=GB

### タイプ付きの名前

eDirectory では、タイプなしの名前 (`JOHN.MARKETING.ABCCORP`) とタイプ付きの名前 (`CN=JOHN.OU=MARKETING.O=ABCCORP`) の両方を使用します。LDAP では、区切り記号としてコンマを使用したタイプ付きの名前 (`CN=JOHN,OU=MARKETING,O=ABCCORP`) だけを使用します。

## エスケープ文字

LDAP 識別名では、エスケープ文字として円記号 (¥) を使用します。1 つの円記号とプラス記号 (+) またはコンマ (,) を指定すると、識別名を拡張できます。

例 :

CN=Pralines¥+Cream,OU=Flavors,O=MFG (CN is Pralines+Cream)

CN=D. Cardinal,O=Lionel¥,Turner and Kaye,C=US (O は Lionel、Turner、および Kaye)

詳細については、Internet Engineering Task Force の RFC 232 (<http://www.ietf.org/rfc/rfc2253.txt?number=2253>) を参照してください。

## 複数のネーミング属性

オブジェクトは、スキーマ内の複数のネーミング属性を使用して定義できます。LDAP と eDirectory のユーザオブジェクトには、いずれも CN と UID の 2 つのネーミング属性があります。識別名の中のネーミング属性は、プラス記号 (+) で区切ります。属性に明示的なラベルが付いていない場合は、スキーマによりそれぞれの文字列に対応する属性が決定されます (eDirectory と LDAP の両方で、最初の文字列は CN、次の文字列は UID になります)。識別名の中の各部分に手動でラベルを付けると、ネーミング属性の順序を変更できます。

2 つの相対識別名の例を次に示します。

Smith (CN は Smith CN=Smith)

Smith+Lisa (CN は Smith、OU は Lisa CN=Smith UID=Lisa)

2 つの相対識別名 (Smith と Smith+Lisa) は、2 つの異なる相対識別名によって参照されるため、同じコンテキスト内に共存することができます。

## サポートされる Novell LDAP コントロールおよび拡張

LDAP クライアントと LDAP サーバは、LDAP 3 プロトコルを使用することにより、コントロールと拡張を適用して LDAP 操作を拡張できます。コントロールと拡張を使用することによって、要求や応答の一部として追加情報を指定できます。拡張された各操作は、自身の属性または `objectclass` を LDAP サーバに追加するのに必要な、オクテット数値の文字列であるオブジェクト識別子 (OID) により識別されます。LDAP クライアントは、実行したい拡張操作の OID およびその拡張操作に固有なデータを指定した拡張操作要求を送信できます。LDAP サーバはこの要求を受信すると、拡張操作を実行し、OID と追加データが設定された応答をクライアントに送信します。

たとえば、クライアントがサーバに検索要求を送信するとき、ソートを指定するコントロールをこの要求に入れることができます。サーバはこの検索要求を受け取ると、検索結果をソートしてから、その結果をクライアントに戻します。コントロールはサーバからクライアントに送ることもできます。たとえば、サーバは、クライアントにパスワード期限切れを通知する認証要求のコントロールを送ることができます。

デフォルトでは、起動直後の eDirectory LDAP サーバは、すべてのシステム拡張ならびに選択されたオプション拡張およびコントロールをロードできる状態にあります。オプション拡張に対応する LDAP サーバオブジェクトの `extensionInfo` 属性により、システム管理者は、オプション拡張およびコントロールの選択と選択解除ができます。



拡張操作を有効にするため、LDAP 3 プロトコルはルート DSE 内の supportedControl 属性および supportedExtension 属性に含まれる、サポートされているコントロールと拡張のリストをサーバに要求します。ルート DSE(DSE は DSA (Directory System Agent) Specific (固有) Entry (エントリ) の略) とは、ディレクトリ情報ツリー (DIT) のルートにあるエントリです。詳細については、[386 ページの「LDAP サーバの情報を取得する」](#)を参照してください。

サポートされている LDAP コントロールと拡張のリストについては、『*LDAP and NDS Integration Guide*』の「[LDAP Controls](http://developer.novell.com/ndk/doc/ldapover/ldap_enu/data/cchbehhc.html)」([http://developer.novell.com/ndk/doc/ldapover/ldap\\_enu/data/cchbehhc.html](http://developer.novell.com/ndk/doc/ldapover/ldap_enu/data/cchbehhc.html)) と「[LDAP Extensions](http://developer.novell.com/ndk/doc/ldapover/ldap_enu/data/a6ik7oi.html)」([http://developer.novell.com/ndk/doc/ldapover/ldap\\_enu/data/a6ik7oi.html](http://developer.novell.com/ndk/doc/ldapover/ldap_enu/data/a6ik7oi.html)) を参照してください。

## Linux、Solaris、AIX、または HP-UNIX 環境での LDAP ツールの使用

eDirectory には次の LDAP ツールが含まれており、これを使用して LDAP ディレクトリサーバを管理できます。これらのツールは /opt/novell/eDirectory/bin に格納されています。

| ツール        | 説明  |
|------------|---|
| ice        | エントリをファイルから LDAP ディレクトリにインポートし、ファイルのディレクトリ内のエントリを変更し、エントリをファイルにエクスポートし、ファイルの属性とクラス定義を追加します。   |
| ldapadd    | LDAP ディレクトリに新しいエントリを追加します。  |
| ldapdelete | LDAP ディレクトリサーバからエントリを削除します。ldapdelete ツールは、LDAP サーバとの接続を開始し、エントリのバインドと削除を行います。  |
| ldapmodify | LDAP サーバとの接続を開始し、エントリのバインド、変更、追加を行います。  |
| ldapmodrdn | LDAP ディレクトリサーバ内のエントリの相対識別名 (RDN) を変更します。LDAP サーバとの接続を開始し、エントリの RDN のバインドと変更を行います。   |
| ldapsearch | LDAP ディレクトリサーバでエントリを検索します。LDAP サーバとの接続を開始し、バインドを行い、指定されたフィルタを使用して検索を実行します。フィルタは、 <a href="http://www.ietf.org/rfc/rfc2254.txt">RFC 2254</a> ( <a href="http://www.ietf.org/rfc/rfc2254.txt">http://www.ietf.org/rfc/rfc2254.txt</a> ) で定義された LDAP フィルタの文字列表現に準拠している必要があります。 |
| ndsindex   | インデックスの作成、一覧表示、一時停止、再開、削除を行います。   |

詳細については、『*LDAP Libraries for C Guide*』の「[LDAP Tools](http://developer.novell.com/ndk/doc/cldap/ftoolenu/data/hevgtl7k.html)」(<http://developer.novell.com/ndk/doc/cldap/ftoolenu/data/hevgtl7k.html>) を参照してください。

LDAP ツールを安全に実行するには、[88 ページの「Linux、Solaris、AIX、および HP-UX システムでの eDirectory 操作に関するセキュリティを確保する」](#)を参照し、安全に eDirectory と LDAP を接続するためのコマンドラインによる LDAP 操作に DER ファイルを指定します。



## LDAP ツール

LDAP ユーティリティは、エントリの削除、変更、追加、スキーマの拡張、相対識別名の変更、エントリの新規コンテナへの異動、検索インデックスの作成、検索の実行に使用できます。

### ldapadd

ldapadd ユーティリティを使用して、新しいエントリを追加します。構文は次のとおりです。

```
ldapadd [-c] [-C] [-l] [-M] [-P] [-r] [-n] [-v] [-F] [-l 制限] [-M[M]] [-d デバッグレベル] [-e キーファイル名] [-D バインド DN] [[-W ]| [-w パスワード]] [-h LDAP ホスト] [-p LDAP ポート] [-P バージョン] [-Z[Z]] [-f ファイル]
```

**注:** NetWare サーバでは、このユーティリティは ladd と呼ばれます。

-f オプションを指定すると、ldapadd により変更がファイルから読み出されます。-f オプションを指定しない場合、ldapadd は変更を stdin から読み出します。

**ヒント:** ldap ユーティリティからの出力は stdout に送られます。出力が表示される前にユーティリティが存在する場合、出力はファイルにリダイレクトされます。例: ldapadd [オプション] > out.txt

| オプション   | 説明   |
|---------|--|
| -a      | 新しいエントリを追加します。ldapmodify のデフォルトは、既存エントリの変更です。ldapadd として呼び出されると、このフラグは常にオンになります。   |
| -r      | デフォルトでは既存の値を置換します。   |
| -c      | 連続操作モード。エラーが通知されても、ldapmodify は変更動作を続けます。デフォルトでは、エラーが通知されると終了します。  |
| -f ファイル | エントリ情報を標準入力ではなく LDIF ファイルから読み出します。レコードの最大長は 4096 行です。  |
| -F      | replica : で始まる入力行の内容に関わりなく、すべての変更を無条件で適用します (デフォルトでは、replica : 行は使用中の LDAP サーバホストおよびポートと比較され、repllog レコードを実際に適用するかどうか決定します)。 |

### すべての LDAP ツールの共通オプション

すべての LDAP ツールに共通するオプションがいくつかあります。次の表は、これらのオプションを表示したものです。

| オプション      | 説明  |
|------------|---|
| -C         | 次の参照を有効にします。(匿名バインド)  |
| -d デバッグレベル | LDAP デバッグレベルを設定します。このオプションを有効にするには、ldapmodify をコンパイルするときに LDAP_DEBUG の定義が必要です。  |
| -D バインド DN | バインド DN を使用して LDAP ディレクトリにバインドします。バインド DN には、RFC 1779 に定義されている文字列表現の DN を指定します。 |
| -e キーファイル名 | SSL バインドのため、ファイル名の確認を行います。  |

| オプション       | 説明   |
|-------------|--|
| -f ファイル     | ファイルから行を読み取り、1行ごとにLDAP検索を実行します。この場合、コマンドラインに指定されたフィルタは、%sが最初に出現した個所がファイルに指定された行で置換されるというパターンとして機能します。1つのハイフン(-)文字がファイルとして指定された場合には、標準入力から行が読み取られます。  |
| -h LDAP ホスト | LDAP サーバの実行場所となっている代替ホストを指定します。  |
| -l 制限       | 接続タイムアウト(秒)を指定します。   |
| -M          | Manage DSA IT コントロールを有効にします。(非致命的)   |
| -MM         | Manage DSA IT コントロールを有効にします。(致命的)  |
| -n          | 完了した場合の結果を表示しますが、実際にはエントリを変更しません。<br>-vと組み合わせて使用すると、デバッグ時に便利です。  |
| -p LDAP ポート | LDAP サーバが監視している代替 TCP™ ポートを指定します。  |
| -P バージョン    | LDAP のバージョン(2 または 3)を指定します。  |
| -v          | 冗長モードが設定され、多くの診断メッセージが標準出力に書き込まれます。  |
| -w パスワード    | 簡易認証のパスワードとしてパスワードを使用します。  |
| -W          | 簡易認証のプロンプトです。コマンドラインにパスワードを指定するかわりに、このオプションが使用されます。  |
| -Z          | <p>操作をバインドして実行する前に、TLS を開始します。TLS を開始する操作の途中でエラーが発生すると、エラーは無視され操作は続行されます。エラーが発生した場合に操作を中止するには、このオプションの代わりに -zz オプションの使用をお勧めします。</p> <p>このオプションでポートが指定されている場合、そのポートはクリアテキスト接続を受信する必要があります。</p> <p>サーバの識別情報を確認するには、このオプションを -e オプションと組み合わせて使用し、サーバ証明書ファイルを指定する必要があります。TLS を開始すると、これによりサーバのルート認証局証明書が確認されます。-e オプションが指定されていない場合、サーバからのすべての証明書が許可されます。</p> |
| -ZZ         | <p>操作をバインドして実行する前に、TLS を開始します。TLS を開始する操作の途中でエラーが発生すると、操作は中止されます。</p> <p>このオプションでポートが指定されている場合、そのポートはクリアテキスト接続を受信する必要があります。</p> <p>サーバの識別情報を確認するには、このオプションを -e オプションと組み合わせて使用し、サーバ証明書ファイルを指定する必要があります。TLS を開始すると、これによりサーバのルート認証局証明書が確認されます。-e オプションが指定されていない場合、サーバからのすべての証明書が許可されます。</p>   |

## 例

/tmp/entrymods ファイルが存在すると仮定すると、次のような内容になります。

```
dn: cn=Modify Me, o=University of Michigan, c=US
changetype: modify
replace: mail
mail: modme@terminator.rs.itd.umich.edu
-
add: title
title: Manager
-
add: jpegPhoto
jpegPhoto: /tmp/modme.jpeg
-
delete: description
-
```

この場合、コマンド「`ldapmodify -b -r -f /tmp/entrymods`」は、コンテンツ「`Modify Me entry`」のメール属性を「`modme@terminator.rs.itd.umich.edu`」の値に置き換え、タイトル「`Manager`」を追加し、`/tmp/modme.jpeg` ファイルの内容を `jpeg` 写真として追加し、属性記述を完全に削除します。

このような変更は、以下のように `ldapmodify` の古い入力規則を使用して実行することもできます。

```
cn=Modify Me, o=University of Michigan, c=US
mail=modme@terminator.rs.itd.umich.edu
+title=Manager
+jpegPhoto=/tmp/modme.jpeg
-description
```

コマンドは次のようになります。

```
ldapmodify -b -r -f /tmp/entrymods
```

/tmp/newentry ファイルが存在すると仮定すると、次のような内容になります。

```
dn: cn=Barbara Jensen, o=University of Michigan, c=US
objectClass: person
cn: Barbara Jensen
cn: B Jensen
sn: Jensen
title: Manager
mail: bjensen@terminator.rs.itd.umich.edu
uid: bjensen
```

この場合、/tmp/newentry ファイルからの値を使用して、コマンド「ldapadd -f/tmp/entrymods」は「B Jensen」に新しいエントリを追加します。

/tmp/newentry ファイルが存在すると仮定すると、次のような内容になります。

```
dn: cn=Barbara Jensen, o=University of Michigan, c=US
changetype: delete
```

この場合、コマンド「ldapmodify -f/tmp/entrymods」は「B Jensen」のエントリを削除します。

## ldapdelete

ldapdelete ユーティリティは、指定したインデックスを削除します。LDAP サーバとの接続を開始し、バインドしてから削除します。構文は次のとおりです。

```
ldapdelete [-n] [-v] [-c] [-r] [-l] [-C] [-M] [-d デバッグレベル] [-e キーファイル名] [-f ファイル] [-D バインド DN] [[-W] | [-w パスワード]] [-h LDAP ホスト] [-p LDAP ポート] [-Z[Z]] [dn]...
```

**注:** NetWare サーバでは、このユーティリティは、ldelete と呼ばれます。

dn パラメータは、削除するエントリの識別名のリストです。

これは、-f オプションと次のように通信します。

- ◆ コマンドラインに -f オプションがなく、コマンドラインで dn が指定されている場合、ユーティリティにより指定したエントリが削除されます。
- ◆ コマンドラインに dn と -f の両方がある場合、ユーティリティは dn のファイルを読み込んで削除して、コマンドラインの dn は無視します。
- ◆ コマンドラインに dn と -f オプションがない場合、ユーティリティは stdin から dn を読み込みます。

**ヒント:** ldap ユーティリティからの出力は stdout に送られます。出力が表示される前にユーティリティが存在する場合、出力はファイルにリダイレクトされます。例: ldapdelete [オプション] > out.txt。

| オプション   | 説明  |
|---------|---|
| -c      | 連続操作モード。エラーが通知されても、ldapdelete は削除動作を継続します。デフォルトでは、エラーが通知されると終了します。  |
| -f ファイル | ファイルから行を読み取り、1 行ごとに LDAP 検索を実行します。この場合、コマンドラインに指定されたフィルタは、%s が最初に出現した個所がファイルに指定された行で置換されるというパターンとして機能します。 |
| -r      | 再起的に削除します。  |

**注:** 共通オプションについての詳細は、341 ページの「すべての LDAP ツールの共通オプション」を参照してください。

### 例

ldapdelete のコマンド「cn>Delete Me, o=University of Michigan, c=US」では、「University of Michigan」組織のエントリの真下にある commonName「Delete Me」で指定されたエントリを削除します。この場合、削除が許可されるためには binddn および passwd を指定する必要があります (-D オプションおよび -w オプションを参照)。

## ldapmodify

ldapmodify ユーティリティを使用すると、既存エントリの属性を変更したり、新規エントリを追加することができます。構文は次のとおりです。

```
ldapmodify [-a] [-c] [-C] [-M] [-P] [-r] [-n] [-v] [-F] [-l 制限] [-M[M]]
[-d デバッグレベル] [-e キーファイル名] [-D バインド DN] [[-W] | [-w パスワード]]
[-h LDAP ホスト] [-p LDAP ポート] [-P バージョン] [-Z[Z]] [-f ファイル]
```

**注:** NetWare サーバでは、このユーティリティは lmodify と呼ばれます。

-f オプションを指定すると、ldapmodify により変更がファイルから読み出されます。  
-f オプションを指定しない場合、変更は stdin から読み出されます。

**ヒント:** ldap ユーティリティからの出力は stdout に送られます。出力が表示される前にユーティリティが存在する場合、出力はファイルにリダイレクトされます。例: ldapmodify [オプション] > out.txt。

| オプション   | 説明   |
|---------|--|
| -a      | 新しいエントリを追加します。ldapmodify のデフォルトは、既存エントリの変更です。ldapadd として呼び出されると、このフラグは常にオンになります。   |
| -r      | デフォルトでは既存の値を置換します。   |
| -c      | 連続操作モード。エラーが通知されても、ldapmodify は変更動作を続けます。デフォルトでは、エラーが通知されると終了します。  |
| -f ファイル | エントリ情報を標準入力ではなく LDIF ファイルから読み出します。レコードの最大長は 4096 行です。  |
| -F      | replica : で始まる入力行の内容に関わりなく、すべての変更を無条件で適用します (デフォルトでは、replica : 行は使用中の LDAP サーバホストおよびポートと比較され、repllog レコードを実際に適用するかどうか決定します)。 |

**注:** 共通オプションについての詳細は、[341 ページの「すべての LDAP ツールの共通オプション」](#)を参照してください。

## ldapmodrdn

ldapmodrdn を使用すると、エントリの相対識別名を変更できます。また、エントリを新しいコンテナに移動することもできます。構文は次のとおりです。

```
ldapmodrdn [-r] [-n] [-v] [-c] [-C] [-l] [-M] [-s 新規スーパーリア] [-d デバッグレ
ベル] [-e キーファイル名] [-D バインド DN] [[-W] | [-w パスワード]] [-h LDAP ホスト]
[-p LDAP ポート] [-Z[Z]] [-f ファイル] [dn 新規 RDN]
```

**注:** NetWare サーバでは、このユーティリティは <newrdn> と呼ばれます)。

ldap ユーティリティからの出力は stdout に送られます。出力が表示される前にユーティリティが存在する場合、出力はファイルにリダイレクトされます。例：ldapmodrdn [ オプション ] > out.txt。

| オプション      | 説明   |
|------------|--|
| -c         | 連続操作モード。エラーが通知されても、ldapmodify は変更動作を続けます。デフォルトでは、エラーが通知されると終了します。                              |
| -f ファイル    | エントリ変更情報を標準入力やコマンドラインではなくファイルから読み出します。古い RDN と新しい RDN の間に空白行がないか確認します。空白行がある場合、-f オプションは失敗します。 |
| -r         | エントリから旧 RDN 値を削除します。デフォルトでは、以前の値が保持されます。   |
| -s 新規スーベリア | エントリの移動先のコンテナの識別名を指定します。   |

注：共通オプションについての詳細は、341 ページの「すべての LDAP ツールの共通オプション」を参照してください。

## 例

/tmp/entrymods ファイルが存在すると仮定すると、次のような内容になります。

```
cn=Modify Me, o=University of Michigan, c=US
cn=The New Me
```

## ldapsearch

ldapsearch ユーティリティは、指定された属性とオブジェクトクラスのディレクトリを検索します。構文は次のとおりです。

```
ldapsearch [-n] [-u] [-v] [-t] [-A] [-T] [-C] [-V] [-M] [-P] [-L] [-d デバッグ
レベル] [-e キーファイル名] [-f ファイル] [-D バインド DN] [[-W] | [-w バインドパスワード]]
[-h LDAP ホスト] [-p LDAP ポート] [-b 検索基点] [-s スコープ] [-a 逆参照]
[-l 時間制限] [-z サイズ制限] [-Z[Z]] filter [属性....]
```

注：NetWare サーバでは、このユーティリティは lsearch と呼ばれます。

ldapsearch ツールは LDAP サーバとの接続を開始し、バインドを行い、フィルタを使用して検索を実行します。フィルタは、RFC 2254 (<http://www.ietf.org/rfc/rfc2254.txt>) で定義された LDAP フィルタの文字列表現に準拠している必要があります。

ldapsearch が 1 つ以上のエントリを検出すると、attrs で指定された属性が取り込まれ、エントリと値が標準出力に書き込まれます。属性がリストされない場合、すべての属性が戻ります。

ヒント：ldap ユーティリティからの出力は stdout に送られます。出力が表示される前にユーティリティが存在する場合、出力はファイルにリダイレクトされます。例：ldapsearch [ オプション ] filter [ 属性リスト ] > out.txt。

| オプション      | 説明   |
|------------|--|
| -a 逆参照     | 別名の逆参照の処理方法を指定します。次の値を使用します。 <ul style="list-style-type: none"> <li>◆ Never : ベースオブジェクトの検索時に、別名の逆参照は行われません。</li> <li>◆ Always : ベースオブジェクトの検索時に、別名の逆参照を常に行います。</li> <li>◆ Search : ベースオブジェクトのサブオーディネートの検索時は別名の逆参照を行いますが、ベースオブジェクトの検索時には行いません。</li> <li>◆ Find : ベースオブジェクトの検索時は別名の逆参照を行いますが、ベースオブジェクトのサブオーディネートの検索時には行いません。</li> </ul> |
| -A         | 値ではなく、属性のみ取り込まれます。エントリに属性が存在するかどうかを確認して、具体的な属性値を知る必要がない場合に便利です。  |
| -CC        | 次の参照を有効にします。(同じバインド DN とパスワードで認証されたバインド)   |
| -b 検索ベース   | 検索ベースを検索の開始ポイントとして使用します。   |
| -L         | エントリを LDIF 形式で出力します。   |
| -LL        | エントリを LDIF 形式で出力します。コメントは出力されません。  |
| -LLL       | エントリを LDIF 形式で出力します。コメントおよびバージョンは出力されません。  |
| -s スコープ    | 検索のスコープを指定します。スコープとして、ベースオブジェクトを示す「base」、1 レベルを示す「one」、またはサブツリー検索を示す「sub」を指定します。デフォルトは「sub」です。   |
| -S 属性      | 戻されたエントリを属性に基づいてソートします。デフォルトでは、戻ったエントリのソートを行いません。属性が長さ 0 の文字列("") の場合、エントリはその識別名のコンポーネントによりソートされます。詳細については、ldap_sort を参照してください。通常は、ldapsearch はエントリを受け取った順に出力します。-S オプションを指定するとデフォルトが無効になり、すべてのエントリが取り込まれ、ソートされてから出力されます。  |
| -t         | 検索されたバイナリ値が一時ファイルに書き込まれます。これは、jpeg の写真やオーディオなど ASCII 以外の値を扱うときに便利です。   |
| -tt        | すべての値が一時ファイルに書き込まれます。  |
| -T パス      | ファイルをパス (デフォルト : "/tmp") で指定されたディレクトリに書き出します。  |
| -u         | 識別名 (DN) をユーザにわかりやすい形式で出力します。  |
| -V         | ファイルの URL プリフィックスです。   |
| -V プリフィックス | ファイルの URL プリフィックスを指定します (デフォルト : "file://tmp/")。   |
| -z サイズ制限   | 検索が終了するまで最大サイズ制限エントリだけ待機します。   |

注 : 共通オプションについての詳細は、[341 ページの「すべての LDAP ツールの共通オプション」](#)を参照してください。

## 例

次のコマンドを実行します。

```
ldapsearch "cn=mark smith" cn telephoneNumber
```

**commonName** 「mark smith」のエントリのサブツリー検索 (デフォルトの検索ベースを使用) を実行します。 **commonName** の値および **telephoneNumber** の値が取得され、標準出力に表示されます。2つのエントリが検出された場合、次のよう出力されます。

```
cn=Mark D Smith, ou="College of Literature, Science, and the Arts",
ou=Students, ou=People, o=University of Michigan, c=US

cn=Mark Smith

cn=Mark David Smith

cn=Mark D Smith 1

cn=Mark D Smith

telephoneNumber=+1 313 930-9489

cn=Mark C Smith, ou=Information Technology Division, ou=Faculty and Staff,
ou=People,

o=University of Michigan, c=US

cn=Mark Smith

cn=Mark C Smith 1

cn=Mark C Smith

telephoneNumber=+1 313 764-2277
```

コマンド :

```
ldapsearch -u -t "uid=mcs" jpegPhoto audio
```

デフォルトの検索ベースを使用して、ユーザ ID 「mcs」のエントリのサブツリー検索を実行します。エントリの DN は、DN 自体を含む行の後にわかりやすい形式で出力されます。また、**Jpeg** の写真の値およびオーディオの値が取得され、一時ファイルに書き込まれます。要求された属性がそれぞれ1つの値をもつエントリが1つ検出された場合、次のよう出力されます。

```
cn=Mark C Smith, ou=Information Technology Division, ou=Faculty and Staff,
ou=People, o=University of Michigan, c=US

Mark C Smith, Information Technology Division, Faculty and Staff, People,
University of Michigan, US

audio=/tmp/ldapsearch-audio-a19924

jpegPhoto=/tmp/ldapsearch-jpegPhoto-a19924
```

次のコマンドは、**organizationName** が「university」で始まるすべての組織の **c=US** レベルで、1レベルの検索を実行します。

```
ldapsearch -L -s one -b "c=US" "o=university*" o description
```

検索結果は LDIF 形式で表示されます。 **organizationName** の値および記述属性の値が取得され、標準出力に書き込まれます。出力結果の例は次のようになります。



```

dn: o=University of Alaska Fairbanks, c=US
o: University of Alaska Fairbanks
description: Preparing Alaska for a brave new yesterday.
description: leaf node only
dn: o=University of Colorado at Boulder, c=US
o: University of Colorado at Boulder
description: No personnel information
description: Institution of education and research
dn: o=University of Colorado at Denver, c=US
o: University of Colorado at D

```

## ndsindex

ndsindex を使用すると、インデックスの作成、一覧表示、一時停止、再開、削除を実行できます。構文は次のとおりです。

```
ndsindex list [-h <ホスト名>] [-p <ポート>] -D <バインド DN> -W|[-w <パスワード>]
[-l 制限] -s <eDirectory サーバの DN> [-Z[Z]] [<インデックス名 1>, <インデックス
名 2>.....]
```

```
ndsindex add [-h <ホスト名>] [-p <ポート>] -D <バインド DN> -W|[-w <パスワード>]
[-l 制限] -s <eDirectory サーバの DN> [-Z[Z]] <インデックス定義 1> [<インデックス
定義 2>.....]
```

```
ndsindex delete [-h <ホスト名>] [-p <ポート>] -D <バインド DN> -W|[-w <パスワード>]
[-l 制限] -s <eDirectory サーバの DN> [-Z[Z]] <インデックス名 1> [<インデック
ス名 2>.....]
```

```
ndsindex resume [-h <ホスト名>] [-p <ポート>] -D <バインド DN> -W|[-w <パスワード>]
[-l 制限] -s <eDirectory サーバの DN> [-Z[Z]] <インデックス名 1> [<インデック
ス名 2>.....]
```

```
ndsindex suspend [-h <ホスト名>] [-p <ポート>] -D <バインド DN> -W|[-w <パスワード>]
[-l 制限] -s <eDirectory サーバの DN> [-Z[Z]] <インデックス名 1> [<インデック
ス名 2>.....]
```

**注:** NetWare サーバでは、このユーティリティは `nindex` と呼ばれます。

| オプション                 | 説明   |
|-----------------------|--|
| list                  | 指定したインデックスを表示します。インデックスが指定されていない場合、ndsindex はサーバ上のすべての既存のインデックスを表示します。 |
| add                   | 新しいインデックスを作成します。   |
| delete                | 指定したインデックスを削除します。  |
| resume                | 指定したインデックスをオフラインの状態から再開します。  |
| suspend               | 指定したインデックスを一時停止してオフラインの状態にします。   |
| -s eDirectory サーバの DN | eDirectory サーバの DN を指定します。   |

**注:** 共通オプションについての詳細は、[341 ページの「すべての LDAP ツールの共通オプション」](#)を参照してください。

## 例

サーバ **MyHost** 上のインデックスを表示するには、次のコマンドを入力します。

```
ndsindex list -h MyHost -D cn=admin, o=mycompany -w password -s cn=MyHost, o=novell
```

電子メールの属性に **MyIndex** という名前の下位文字列インデックスを作成するには、次のコマンドを入力します。

```
ndsindex add -h myhost -D cn=admin, o=mycompany -w password -s cn=myhost, o=novell "MyIndex;email address;substring"
```

市町村の属性に **MyIndex** という名前の値インデックスを作成するには、次のコマンドを入力します。

```
ndsindex add -h myhost -D cn=admin, o=mycompany -w password -s cn=myhost, o=novell "MyIndex;city;value"
```

自宅電話番号の属性に **MyIndex** という名前の存在インデックスを作成するには、次のコマンドを入力します。

```
ndsindex add -h myhost -D cn=admin, o=mycompany -w password -s cn=myhost, o=novell "MyIndex;homehone;presence"
```

**MyIndex** という名前のインデックスを削除するには、次のコマンドを入力します。

```
ndsindex delete -h myhost -D cn=admin, o=mycompany -w password -s cn=myhost, o=novell MyIndex
```

**MyIndex** という名前のインデックスを一時停止するには、次のコマンドを入力します。

```
ndsindex suspend -h myhost -D cn=admin, o=mycompany -w password -s cn=myhost, o=novell MyIndex
```

**MyIndex** という名前のインデックスを再開するには、次のコマンドを入力します。

```
ndsindex resume -h myhost -D cn=admin, o=mycompany -w password -s cn=myhost, o=novell MyIndex
```

## 拡張可能一致検索フィルタ

RFC 2251 (<http://www.cis.ohio-state.edu/cgi-bin/rfc/rfc2251.html>) で定義される LDAP 3 のコアプロトコルを指定するには、LDAP サーバが拡張可能一致検索フィルタ機能を認識できなくてはなりません。拡張可能一致検索では、LDAP クライアントは検索フィルタに次の項目を指定することができます。

- ◆ オプションの属性名
- ◆ オプションの一致ルール
- ◆ dn 属性がエントリの一部として考慮されるべきかを示すフラグ
- ◆ 一致検索に使用される値

拡張可能一致検索フィルタの文字列を次に示します。

```
extensible = attr [":dn"] [":matchingrule"] "!=" value /  
[:dn"] "":"matchingrule "!=" value
```

次の表は、拡張可能検索フィルタパラメータを表示したものです。

| パラメータ              | 説明                        |
|--------------------|---------------------------|
| attr               | 適合する属性を指定します。             |
| [":dn"]            | 一致ルールが比較一致に含まれていることを示します。 |
| [":" matchingrule] | 使用する一致ルールを指定します。          |
| ":="               | 一致ルールを指定しないと、完全一致とみなされます。 |
| value              | 比較値                       |

extensibleMatch は、LDAP 3 から導入された新しいフィルタです。matchingRule フィールドがない場合は、属性フィールドが必ず必要です。完全一致検索はその属性に対して実行されます。attribute フィールドがなく、matchingRule が存在する場合、その matchingRule をサポートするエントリ内のすべての属性が matchValue と比較され、matchingRule によりアサーション値の構文が決定されます。

フィルタ項目は次のように評価されます。

- ◆ TRUE : エントリに 1 件以上の一致があることを表します。
- ◆ FALSE : エントリに一致する属性がないことを表します。
- ◆ matchingRule を認識できなかったり、assertionValue を解析できない場合は「未定義」とされます。

matchingRule の他に type フィールドがある場合、matchingRule はその type で使用できるものでなくてはなりません。使用できない場合、フィルタ項目は定義されません。検索フィルタに : dn が指定されている場合、エントリの識別名に含まれるすべての属性に対して一致検索が適用されます。また、フィルタ項目の評価が TRUE の識別名が 1 つ以上属性を持っている場合も、評価は TRUE になります。dnAttributes フィールドを使用すると、単語の一致検索などで、1 つのルールをエントリに適用し、別のルールをエントリと dn 属性に適用するというように、一般的な一致ルールを複数設定する必要がなくなります。

拡張可能一致検索フィルタにより、LDAP クライアントでは次の 2 つのことが可能になります。

- ◆ 同じタイプのデータに対し、複数の一致ルールをサポートできます。
- ◆ 検索条件に DN 要素を含めることができます。

DN 指定により、DN の特定要素の一致検索を実行できます。

Novell eDirectory 8.7.3 以降では、DN の拡張可能な一致検索フィルタがサポートされています。拡張可能一致検索フィルタのもう一つの要素である一致ルールは未定義とみなされ、無視されます。DN 一致検索を使用すると、LDAP クライアントで eDirectory ツリーからオブジェクトを簡単に検索できます。たとえば、

```
(&(ou:dn:=sales)(objectclass=user))
```

のような複雑な LDAP 検索フィルタにより、セールスコンテナの下のセールスファンクションにあるすべてのユーザオブジェクトをリストすることができます。

## 使用例

次は、eDirectory 8.7.3 以降でサポートされている拡張可能一致検索フィルタの文字列の例です。

```
(o:dn:=Ace Industry)
```

これは `:dn` の使用例です。エントリの識別名の属性は、一致を評価するとき、エントリの一部とみなされます。これは、完全一致であることを意味します。

```
(:dn:2.4.8.10:=Dino)
```

これはエントリの属性に適用するフィルタの例です。一致ルールが `2.4.8.10` の DN の属性も考慮されます。

次は、eDirectory 8.7.3 でサポートされていない拡張可能一致検索フィルタの文字列の例です。

```
(cn:1.2.3.4.5:=John Smith)
```

この例は、属性タイプ `cn` と値 `John Smith` を指定するフィルタを表しています。一致ルール `oid 1.2.3.4.5` により、ディレクトリサーバにより一致検索が実行されます。

```
(sn:dn:2.4.6.8.10:=Barbara Jones)
```

これは `dn` の使用例です。一致ルール `2.4.6.8.10` を比較に使用して一致を評価するとき、エントリの属性の識別名はエントリの一部とみなされることを表しています。

# 13

## LDAP Services for Novell eDirectory の環境設定

eDirectory™ インストールプログラムにより、LDAP Services for Novell® eDirectory が自動的にインストールされます。eDirectory のインストールについては、『*Novell eDirectory 8.8 インストールガイド*』を参照してください。

このセクションでは次について説明します。

- ◆ 353 ページの「LDAP Services for eDirectory をロードおよびアンロードする」
- ◆ 354 ページの「LDAP サーバがロードされているか確認する」
- ◆ 355 ページの「LDAP サーバが実行されているか確認する」
- ◆ 358 ページの「LDAP オブジェクトを環境設定する」
- ◆ 363 ページの「LDAP サーバをリフレッシュする」
- ◆ 364 ページの「認証とセキュリティ」
- ◆ 372 ページの「LDAP サーバを使ってディレクトリを検索する」
- ◆ 379 ページの「上方参照を設定する」
- ◆ 383 ページの「持続的検索：eDirectory イベントの設定」
- ◆ 386 ページの「LDAP サーバの情報を取得する」

LDAP ツールの詳細については、[LDAP Tools \(http://developer.novell.com/ndk/doc/cldap/index.html?ldaplibc/data/a6eup29.html\)](http://developer.novell.com/ndk/doc/cldap/index.html?ldaplibc/data/a6eup29.html) を参照してください。

### LDAP Services for eDirectory をロードおよびアンロードする

LDAP Services for eDirectory をロードするには、次のコマンドを入力します。

| サーバ                         | コマンド  |
|-----------------------------|---|
| NetWare の場合®                | コンソールプロンプトで、次のコマンドを入力します。<br><br><code>load nldap.nlm</code>  |
| Windows                     | [DHOST (NDSCONS)] 画面で nldap.dlm を選択し、[開始] をクリックします。   |
| Linux、Solaris、AIX、または HP-UX | Linux、Solaris、AIX、または HP-UX プロンプトで、次のコマンドを入力します。<br><br><code>/opt/novell/eDirectory/sbin/nldap -l</code> |

LDAP Services for eDirectory をアンロードするには、次のコマンドを入力します。

| サーバ                        | コマンド  |
|----------------------------|---|
| NetWare                    | コンソールプロンプトで、次のコマンドを入力します。<br><br><code>unload nldap.nlm</code>  |
| Windows                    | [DHOST (NDSCONS)] 画面で <code>nldap.dlm</code> を選択し、[停止] をクリックします。  |
| Linux, Solaris, AIX, HP-UX | LDAP をアンロードするには、[DHOST リモート管理] ページで <i>LDAP v3 for Novell eDirectory 8.8</i> アクションアイコンをクリックして停止します。<br><br>または<br><br>Linux, Solaris, AIX、または HP-UX プロンプトで、次のコマンドを入力します。<br><br><code>/opt/novell/eDirectory/sbin/nldap -u</code> |

## LDAP サーバがロードされているか確認する

LDAP オブジェクトの設定を行う前に、LDAP サーバがロードされ、動作していることを確認します。この画面では、LDAP サーバがロードされているか確認する方法を説明します。サーバが動作しているか確認するには、[355 ページの「LDAP サーバが実行されているか確認する」](#)を参照してください。

### NetWare の場合

NetWare サーバに `nldap.nlm` がロードされているか確認するには、サーバコンソールに次のいずれかを入力します。

#### ◆ `ldap display activity`


`nldap.nlm` がロードされていない場合は、サーバにより「不明なコマンド」というメッセージが表示されます。

NetWare 6.x では、メッセージはコンソール画面ではなくログ画面に表示されます。

#### ◆ `ldap display config`

#### ◆ `modules nldap.nlm`


Novell iManager を使用することもできます。

- 1 [役割およびタスク] ボタン  をクリックします。
- 2 [eDirectory の保守] > [サービスマネージャ] の順にクリックします。
- 3 接続、サーバ、DNS 名、または IP アドレスを選択し、[OK] をクリックします。
- 4 パスワードを入力し、[OK] をクリックします。
- 5 LDAP Agent for Novell eDirectory 8.8 をクリックします。  
モジュール情報セクションの [ファイル名] フィールドに `nldap.nlm` と表示されます。

## Windows NT/2000 の場合

- 1 Windows サーバで、ndscons.exe を開きます。  
[スタート] > [設定] > [コントロールパネル] > [Novell eDirectory サービス] の順にクリックします。
- 2 [サービス] タブで、nldap.dlm までスクロールし、[ステータス] カラムを表示します。  
カラムに [稼働中] と表示されます。

Novell iManager を使用することもできます。

- 1 [役割およびタスク] ボタン  をクリックします。
- 2 [eDirectory の保守] > [サービスマネージャ] の順にクリックします。
- 3 接続、サーバ、DNS 名、または IP アドレスを選択し、[OK] をクリックします。
- 4 パスワードを入力し、[OK] をクリックします。
- 5 LDAP Agent for Novell eDirectory 8.8 をクリックします。  
モジュール情報セクションの [ファイル名] フィールドに nldap.nlm と表示されます。

## Linux および UNIX にロードした場合

libnldap.so または libnldap.sl を指定します。この名前は、単にバージョン情報が追加された長いファイル名のシンボリックリンクであることもあります。

また、libnldap.so または libnldap.sl ファイルは、Linux および UNIX の各プラットフォーム用の異なるバイナリファイルです。

LDAP サーバがロードされているかどうかを確認するのに、ndslog ファイルまたは ndstrace を使用することもできます。

## LDAP サーバが実行されているか確認する

LDAP サーバをロードした後で、それが実行されているか確認します。その後、デバイスが監視しているか確認します。

- ◆ [355 ページの「シナリオ」](#)
- ◆ [356 ページの「LDAP サーバが実行されているか確認する」](#)
- ◆ [358 ページの「デバイスが受信待機していることを確認する」](#)

## シナリオ

通常、LDAP サーバはロードされるとすぐに実行されます。ただし、次の 2 つのシナリオでは、サーバが正しく実行されないことがあります。

**シナリオ：サーバがゾンビ状態にある。** LDAP サーバは NetWare か DHost ローダが外部依存関係を解決できる限り、ロードを続けます。ただし、LDAP サーバは有効な設定を 2 つの設定オブジェクト (LDAP サーバと LDAP グループオブジェクト) から取得するまで、正しく動作しません。

LDAP サーバが、「ロードはされても、実行されない (ゾンビ) 状態」の場合、LDAP サーバは定期的に設定オブジェクトを探そうとします。オブジェクトの設定が失敗したり破損した場合、LDAP サーバはサーバ (nldap.nlm、nldap.dlm、libnldap.so、または libnldap.sl) をアンロードまたは終了するまで、ゾンビ状態のままになります。

ローダは、LDAP サーバがロードされているのに、nldap.nlm (または nldap.dlm、libnldap.so、libnldap.sl) により LDAP ポート (389、636) が開かれていないことを示します。また、LDAP クライアントの要求はどれも実行されていません。

定期的な試行の記録と、サーバが稼動状態にならない原因を示す DSTrace メッセージが表示されます。

**シナリオ：サービス拒否。** Digital Airlines 社のサーバは現在、長時間 (20 分以上) かかる検索を処理しています。この処理では、膨大なデータの中から検索が行われています。

この検索の実行中に、あるユーザが次のいずれかを実行します。

- ◆ 環境設定パラメータを変更し、設定オブジェクトを更新する。
- ◆ [Refresh Server Now] をクリックする。
- ◆ LDAP サーバ (nldap.nlm、nldap.dlm、libnldap.so、libnldap.sl のいずれか) をアンロードする。
- ◆ サーバ全体を終了しようとする。

LDAP サーバは、現在の処理が完了してから更新を適用します。この更新が完了するまで、新しい操作は実行されません。この遅れにより、サーバの検索が完了し、更新が適用されるまでの間、サーバが新しい要求に応答しなくなったように見えることがあります。アンロードの実行中にサーバが停止したように見えることもあります。

検索要求が長く、多くの一致項目がある場合、LDAP サーバをアンロードしようとする と検索は中止され、次の一致項目がクライアントに返される時にアンロードが実行されます。ただし、検索要求の結果、20 分間に 1 件以下しか一致する項目が見つからなかった場合、LDAP サーバは実行中の NDS<sup>®</sup> または eDirectory 要求を中止できません。

リフレッシュまたは更新の場合、クライアントに返される多くの一致レコードがあっても検索は中止されません。

## LDAP サーバが実行されているか確認する

LDAP サービスが実行されているか確認するには、Novell インポート / エクスポート 変換ユーティリティ (ICE) を使用します。ワークステーションで、コマンドラインから ice.exe を実行するか、または Novell iManager か ConsoleOne<sup>®</sup> を使用します。

### コマンドラインから実行する方法

- 1 ice.exe を含むディレクトリに移動します (例: c:\novell\consoleone\1.2\bin)。
- 2 ice.exe を実行します。

rootDSE を検索します。ソースハンドラとエクスポートハンドラを特定するパラメータを含めます。たとえば、次のように入力します。

```
ice -S LDAP -s 10.128.45.0 -p 389 -c base -a vendorname -D LDIF -f testoutput
```

| パラメータと値        | 説明   |
|----------------|--|
| -S LDAP        | LDAP をソースハンドラとして指定します。   |
| -s 10.128.45.0 | サーバの DNS 名または IP アドレスを指定します。   |
| -p 389         | LDAP ソースハンドラパラメータが識別する LDAP サーバのポート番号を指定します。デフォルトポートは 389 です。389 がインストール時に指定したポートではない場合、クリアテキストのポート番号を指定します。 |

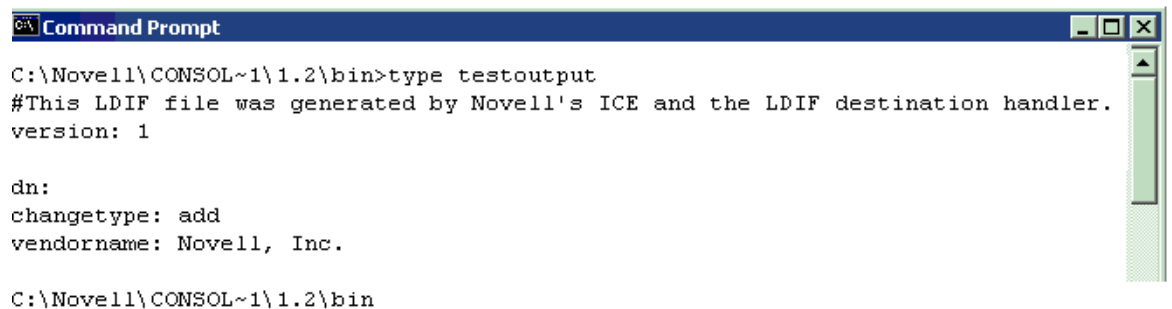


| パラメータと値  | 説明                                 |
|----------|------------------------------------|
| -c ベース   | 検索要求の範囲として、ベースオブジェクトのエントリのみを指定します。 |
| -a ベンダー名 | 検索対象に「ベンダー名」属性を指定します。              |
| -D LDIF  | LDIF をターゲットハンドラとして指定します。           |
| -f テスト出力 | LDIF レコードの書き込み先になるファイルの名前を指定します。   |

これは、出力をテスト出力ファイルに送信したときの例です。

ICE の使用方法については、149 ページの「Novell インポート / エクスポート変換ユーティリティ」を参照してください。LDAP ソースハンドラに固有の情報については、162 ページの「LDAP ソースハンドラのオプション」を参照してください。LDIF ターゲットハンドラに固有の情報については、162 ページの「LDIF ターゲットハンドラのオプション」を参照してください。

### 3 ICE コマンドの結果が表示されます。



```

C:\Novell\CONSOL~1\1.2\bin>type testoutput
#This LDIF file was generated by Novell's ICE and the LDIF destination handler.
version: 1

dn:
changetype: add
vendorname: Novell, Inc.

C:\Novell\CONSOL~1\1.2\bin

```

例 (手順 2 と 3) では rootDSE エントリからの出力をベンダ名属性のみに制限しています。この例では、情報が Novell eDirectory サーバから読み込まれたため、ベンダ情報に Novell, Inc. と表示されます。

## Novell iManager を使用する方法

Novell iManager で LDAP サーバが動作していることを確認するには、151 ページの「データをファイルへエクスポートする」の手順に従います。

IP アドレスとポート番号を入力して接続が確立された場合は、サーバは機能しています。その他の場合は、エラーメッセージが表示されます。ログファイルまたはエクスポートファイルをダウンロード (表示) してください。

## ConsoleOne を使用する方法

ConsoleOne を使用して LDAP サーバが動作していることを確認するには、171 ページの「LDIF エクスポートを実行する」を参照してください。

[ターゲット LDIF ファイルの選択] フィールドにパスとファイル名を指定します (例: c:\ldap\textoutput.txt)。ファイル名のみ入力した場合、ConsoleOne の LDAP スナップインは、ファイルをデフォルトディレクトリ (通常、c:\novell\consoleone\1.2\bin) に書き出します。

## デバイスが受信待機していることを確認する

デバイスがポート 389 で受信待機していることを確認します。

### NetWare の場合 :

- 1 サーバコンソールで次を入力します。

```
tcpcon
```

- 2 [プロトコル情報] > [TCP] > [TCP 接続] の順に選択します。

- 3 [ポート] カラムで 389 を選択します。

[状態] カラムに [リッスン] と表示された場合、デバイスはそのポートで受信待機しています。

デバイスが受信待機していない場合、そのポートは存在しません。

### Windows 2000/NT、UNIX、および Linux の場合

- 1 コマンドラインで次を入力します。

```
netstat -a
```

- 2 ローカルアドレスがサーバ名 : 389 で、状態が「リッスン中」の行を探します。

次のいずれかの状況が発生した場合は、Novell iMonitor を実行します。

- ◆ ICE ユーティリティから情報を取得できない
- ◆ LDAP サーバが LDAP 要求をハンドリングしているか確認できない

Novell iMonitor の詳細については、[203 ページの「環境設定ファイル」](#) および [210 ページの「トレースを環境設定する」](#) を参照してください。

LDAP 要求の詳細については、『*Novell eDirectory 8.8 インストールガイド*』の「[LDAP を介した eDirectory との通信](#)」を参照してください。

## LDAP オブジェクトを環境設定する

eDirectory のインストール時に、LDAP サーバオブジェクトと LDAP グループオブジェクトが作成されます。LDAP サービスのデフォルト設定は、これらの 2 つのオブジェクト上のディレクトリにあります。ConsoleOne LDAP スナップインか、Novell iManager の LDAP 管理タスクを使用して、デフォルト設定を変更できます。

LDAP サーバオブジェクトとは、サーバ固有の設定データのことです。

LDAP グループオブジェクトには、複数の LDAP サーバ間で共有できる便利な設定情報が含まれています。このオブジェクトは、共通の設定データと LDAP サーバグループを提供します。サーバは共通データを持っています。

複数の LDAP サーバオブジェクトを、LDAP グループオブジェクトと関連させることができます。関連するすべての LDAP サーバは、サーバ固有の設定を LDAP サーバオブジェクトから取得しますが、共通する情報や共有情報は LDAP グループオブジェクトから取得します。

デフォルトでは、LDAP グループオブジェクトおよび LDAP サーバオブジェクトが、eDirectory インストールプログラムによって `nldap.nlm` または `nldap.dlm` に 1 つずつインストールされます。その後、複数の LDAP サーバオブジェクトを、1 つの LDAP グループオブジェクトに関連付けることができます。

**重要:** 新しいバージョンの LDAP サーバオブジェクトを古いバージョンの LDAP グループオブジェクトに関連付けることも可能ですが、異なるバージョン間での関連付けはお勧めできません。たとえば、eDirectory 8.5 の LDAP グループオブジェクトと eDirectory 8.6 の LDAP サーバオブジェクトとの関連付けは避けるようにしてください。

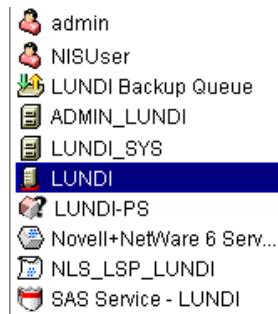
LDAP グループオブジェクトが保持する、共通情報の量は制限されています。属性に含まれるデータはほとんど共通しているため、LDAP は多くの属性を読み込む必要がありません。多くの LDAP サーバは同じデータを使用する必要があります。共通の、または共有グループオブジェクトがない場合は、各 LDAP サーバにそのデータを複製する必要があります。

LDAP サーバオブジェクトでは、LDAP グループオブジェクトよりも多くのサーバ固有の設定オプションおよびデータが許可されています。

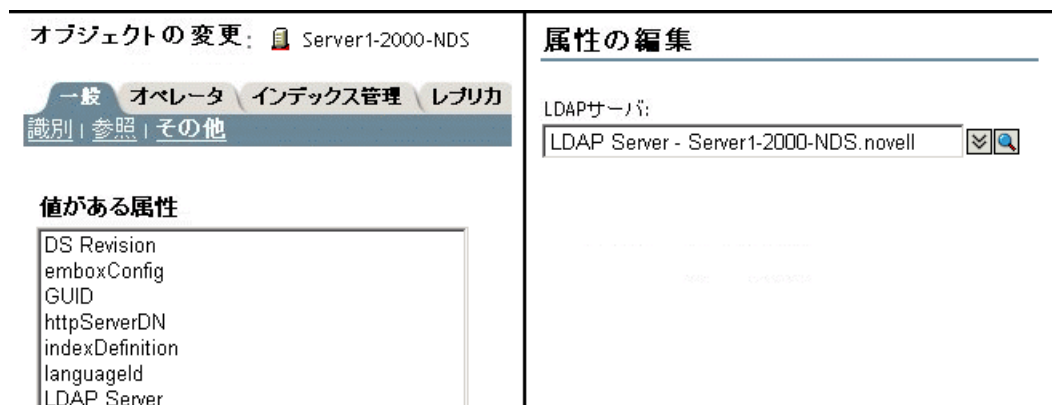
どちらのオブジェクトも、相互にポイントされた DN 構文属性を持っています。

LDAP サーバがその設定データを探せるようにするには、関連付けを追加する必要があります。関連付けは、通常の eDirectory 設定データを保持する NCP™ サーバを通じて行われます。この関連付けは、eDirectory インストールプログラムにより自動で行われます。

各 eDirectory サーバは、NCP サーバオブジェクトを持っています。次の図の「Lundi」というサーバには、このオブジェクトが iManager 上と同じように表示されています。



このオブジェクトは、特定のホスト eDirectory サーバの LDAP サーバオブジェクトを指す LDAP サーバ属性を持っています。次の図は、この属性を示しています。



通常、LDAP サーバオブジェクト、LDAP グループオブジェクト、NCP サーバオブジェクトは同じコンテナ内にあります。eDirectory のインストールで、サーバおよび管理者コンテキストを指定するときに、このコンテナを指定します。

LDAP サーバオブジェクトを移動するときは、それを書き込み可能なレプリカ上に移動する必要があります。

## Linux、Solaris、AIX、HP-UX システム上で、LDAP サーバオブジェクトおよび LDAP グループオブジェクトを環境設定する

LDAP 環境設定ユーティリティは `ldapconfig` です。Linux、Solaris、AIX、HP-UX システムで LDAP サーバオブジェクトおよび LDAP グループオブジェクトの属性を変更、表示、リフレッシュするには、`ldapconfig` を使用します。

Linux、Solaris、AIX、HP-UX システム上で LDAP 属性値を表示するには、次の構文を使用します。

```
ldapconfig get [...] | set 属性値リスト [-t ツリー名 | -p ホスト名 [: ポート]] [-w パスワード] [-a ユーザ FDN] [-f]
```

```
ldapconfig [-t ツリー名 | -p ホスト名 [: ポート]] [-w パスワード] [-a ユーザ FDN] [-V] [-R] [-H] [-f] -v 属性, 属性2...
```

Linux、Solaris、AIX、HP-UX システム上で LDAP 属性を変更するには、次の構文を使用します。

```
ldapconfig [-t ツリー名 | -p ホスト名 [: ポート]] [-w パスワード] [-a 管理者 FDN] -s 属性=値, ...
```

| パラメータ          | 説明   |
|----------------|--|
| -t ツリー名        | コンポーネントのインストール先となる eDirectory ツリーの名前。  |
| -p ホスト名        | ホストの名前です。DNS 名または IP アドレスを指定することもできます。   |
| -w             | 管理権を持つユーザのパスワード。   |
| -a             | 管理権を持つユーザの完全識別名。例：<br>cn=user.o=org1   |
| get   -V       | すべての LDAP サーバと LDAP グループの属性を表示します。   |
| get   -v 属性リスト | 属性リストにある属性の現在の値を表示します。   |
| set   -s 属性値ペア | 属性を指定した値で設定します。  |
| -v             | LDAP 属性値を表示します。  |
| -s             | インストールされたコンポーネントの属性値を設定します。  |
| -R             | LDAP サーバをリフレッシュします。  |
| -V             | 現在の LDAP 環境設定を表示します。   |
| -H             | 使用方法とヘルプを表示します。  |
| -f             | フィルタ済みレプリカ上での操作を許可します。   |
| 属性             | 設定可能な LDAP サーバ属性名またはグループ属性名。詳細については、 <a href="#">361 ページの「LDAP サーバオブジェクトの属性」</a> および <a href="#">363 ページの「LDAP グループオブジェクトの属性」</a> を参照してください。 |

## 例

属性リストの属性の値を表示するには、次のコマンドを入力します。

```
ldapconfig [-t ツリー名 | -p ホスト名[:ポート]]  
[-w パスワード] [-a ユーザFDN] -v "Require TLS for simple binds with  
password","searchTimeLimit"
```

LDAP TCP ポート番号と検索サイズの制限を 1000 に設定するには、次のコマンドを入力します。

```
ldapconfig [-t ツリー名 | -p ホスト名[:ポート]]  
[-w パスワード] [-a 管理者FDN] -s "LDAP TCP Port=389","searchSizeLimit=1000"
```

## LDAP サーバオブジェクトの属性

Novell LDAP サーバプロパティを設定および管理するために、LDAP サーバオブジェクトを使用します。

次の表に、LDAP サーバ属性の説明を示します。

| 属性                       | 説明   |
|--------------------------|--|
| LDAP Server              | eDirectory の LDAP サーバオブジェクトの完全識別名。   |
| LDAP Host Server         | LDAP サーバの実行場所となるホスト eDirectory サーバの完全識別名。  |
| LDAP Group               | eDirectory の中で、この LDAP サーバがメンバーとして属する LDAP グループオブジェクト。                                     |
| LDAP Server Bind Limit   | LDAP サーバに同時にバインドできるクライアントの数。0 を指定すると、無制限になります。   |
| LDAP Server Idle Timeout | あるクライアントと LDAP サーバの間で、ここで指定した期間無活動状態が継続すると、このクライアントと LDAP サーバの接続が切断されます。0 を指定すると、無制限になります。 |
| LDAP Enable TCP          | この LDAP サーバに対して (TLS ではなく) TCP 接続が有効であるかどうかを示します。<br>値は 1 (はい) または 0 (いいえ) です。             |
| LDAP Enable TLS          | この LDAP サーバに対して TLS 接続が有効であるかどうかを示します。<br>値は 1 (はい) または 0 (いいえ) です。                        |
| LDAP TCP Port            | (SSL でなく) TCP 接続で LDAP サーバが受信待機するポート番号。<br>範囲は 0 ~ 65535 です。                               |
| LDAP TLS Port            | TLS 接続で LDAP サーバが受信待機するポート番号。<br>範囲は 0 ~ 65535 です。これは LDAP サーバに許可されている最大接続数です。             |

| 属性                               | 説明  |
|----------------------------------|---|
| keyMaterialName                  | この LDAP サーバに関連付けられた、SSL LDAP 接続に使用する eDirectory の証明書オブジェクトの名前。  |
| searchSizeLimit                  | LDAP サーバが検索要求への応答として LDAP クライアントに返すエントリの最大数。0 を指定すると、無制限になります。  |
| searchTimeLimit                  | LDAP サーバによる LDAP 検索がタイムアウトになるまでの最大秒数。0 を指定すると、無制限になります。   |
| filteredReplicaUsage             | LDAP サーバが LDAP 検索のために、フィルタ処理されたレプリカを使用するかどうかを指定します。<br><br>値は 1 (フィルタ済みレプリカを使用) か 0 (フィルタ済みレプリカ不使用) です。   |
| sslEnableMutualAuthentication    | LDAP サーバにおいて、SSL ベースの相互認証 (証明書に基づくクライアント認証) を有効にするかどうかを指定します。   |
| ldapTLSVerifyClientCertificate   | LDAP による TLS 操作のクライアント認証の確認を有効または無効にします。  |
| ldapNonStdAllUserAttrsMode       | 非標準のすべてのユーザとオペレーショナル属性を有効または無効にします。   |
| ldapBindRestrictions             | LDAP クライアント接続で LDAP のバインド制限を設定します。LDAP クライアントから匿名バインドを許可または禁止することができます。<br><br>値は 0 か 1 です。<br><br>0 を指定すると、クライアントからの匿名バインドが許可されます。1 を指定すると、クライアントの匿名バインドが制限されます。                     |
| ldapEnablePSearch                | LDAP サーバで持続的検索機能を有効にするかどうかを指定します。<br><br>値は TRUE か FALSE です。  |
| ldapMaximumPSearchOperations     | 同時に実行できる持続的検索操作の数を制限するための整数値です。0 を指定すると、検索操作は無制限になります。  |
| ldapIgnorePSearchLimitsForEvents | 持続的検索要求によって最初の結果が返された後で、サイズと時間の制限を無視するかどうかを指定します。<br><br>値は TRUE か FALSE です。<br><br>この属性が FALSE に設定されている場合、すべての持続的検索操作は検索制限の制約を受けます。サイズと時間のいずれかの制限に達した場合、検索操作は失敗し、該当するエラーメッセージが返されます。 |

## LDAP グループオブジェクトの属性

LDAP クライアントの Novell LDAP サーバに対するアクセス方法とサーバ上の情報の使用方法を設定および管理するには、LDAP グループオブジェクトを使用します。

単純バインドに TLS が必要な場合は、[364 ページの「パスワードとの単純バインドに TLS を要求する」](#)を参照してください。この属性は、LDAP サーバが LDAP クライアントからパスワードをクリアテキストで送信することを許可するかどうかを指定します。値は 1 (はい) または 0 (いいえ) です。

デフォルトの参照および LDAP サーバによる LDAP 参照の処理方法を指定するには、[373 ページの「参照を使用する」](#)を参照してください。

## LDAP サーバをリフレッシュする

LDAP サーバの環境設定オプションや LDAP サーバの設定を変更した場合、変更を有効にするにはサーバをリフレッシュする必要があります。

ただし、LDAP 要求のサービスの実行中はサーバをリフレッシュできません。たとえば、eDirectory ツリーの処理に 15 分かかる場合には、この処理が完了するまでリフレッシュは実行されません。

同様に、LDAP サーバスレッドの実行中は、LDAP サーバを終了することはできません。

リフレッシュの実行が予定されている場合は、LDAP サーバはリフレッシュが実行されるまで新しい LDAP 要求の開始を遅らせます。

デフォルトでは、LDAP サーバは 30 分間隔で LDAP サーバオブジェクトと LDAP グループオブジェクトのタイムスタンプをチェックし、設定に変更がなかったか確認します。設定が変更されている場合、サーバはその変更を適用します。

設定のタイムスタンプが前回と変わらない場合には、リフレッシュは実行されません。(強制的にリフレッシュを実行すると、サーバはタイムスタンプを無視して変更を適用します。)

LDAP サーバをリフレッシュするには、次のいずれかを実行します。

- ◆ Novell iManager を使用する。
  1. 役割およびタスクページで、[LDAP] > [LDAP の概要] > [LDAP サーバの表示] の順にクリックします。
  2. LDAP サーバをクリックし、[リフレッシュ] をクリックします。
- ◆ サーバが次のリフレッシュ間隔で再設定されるまで待つ。
- ◆ nldap.nlm をアンロードしてから再ロードする。

nldap.nlm をアンロードする前に、前提となる NLM™ プログラムをアンロードする必要はありません。

nldap.nlm がアンロードされると、従属する NLM プログラムが再ロードされます。
- ◆ コマンドラインで、リフレッシュ間隔を変更する。

このオプションは、WAN リンクが継続して実行されていない場合に便利です。必要に応じ、一時的にサーバのハートビート処理の長さを変更できます。

この変更は持続しません。nldap.nlm をロードするたびに、コマンドを再入力する必要があります。

サーバコンソールで次を入力します。

**ldap refresh [=] [日付][時刻][間隔]**

- ◆ 日付変数の形式は、mm:dd:yyyy です。すべての日付フィールドに 0 と入力すると、現在の日付が使用されます。
- ◆ 時間変数の形式は、hh:mm:ss です。すべての時刻フィールドに 0 と入力すると、現在の時刻が使用されます。
- ◆ 間隔変数の形式は 0 または 1 ~ 2147483647 分の間です。0 と入力すると、デフォルトの 30 分が使用されます。

このコマンドは、sys:¥system ディレクトリの autoexec.ncf ファイルに追加できません。nldap.nlm をロードした行の後に、このコマンドを配置します。

## 認証とセキュリティ

このセクションでは、次の情報について説明します。

- ◆ [364 ページの「パスワードとの単純バインドに TLS を要求する」](#)
- ◆ [365 ページの「TLS を開始 / 停止する」](#)
- ◆ [366 ページの「TLS のサーバを環境設定する」](#)
- ◆ [367 ページの「TLS のクライアントを環境設定する」](#)
- ◆ [367 ページの「ルート認証局をエクスポートする」](#)
- ◆ [368 ページの「クライアント証明書で認証を受ける」](#)
- ◆ [368 ページの「サードパーティプロバイダの証明書を使用する」](#)
- ◆ [370 ページの「SASL を使用する」](#)


### パスワードとの単純バインドに TLS を要求する

SSL (Secure Socket Layer) 3.1 は Netscape でリリースされました。IETF は TLS (Transport Layer Security) 1.0 を実装することにより、SSL 標準の所有権を持っています。

TLS を使用すると、接続をセッション層で暗号化することができます。TLS 接続のために、暗号化されたポートを使用する必要はありません。また、次の方法もあります。ポート 636 は暗黙的な TLS ポートであり、クライアントがセキュアポートに接続すると、LDAP サーバは自動的に TLS 接続を開始することができます。


クライアントは、まずクリアテキストポートに接続し、後で TLS を使用して暗号化された接続にアップグレードすることもできます。

パスワードとの単純バインドに TLS を要求するには、次を実行します。

- 1** Novell iManager で、[役割およびタスク] ボタン  をクリックします。
- 2** [LDAP] > [LDAP の概要] > [LDAP グループの表示] の順にクリックします。
- 3** LDAP グループオブジェクトをクリックしてから、[全般] タブの [情報] をクリックします。



- 4 [パスワードとの単純バインドに TLS を必要とする] チェックボックスをオンにします。

LDAPグループ:  LDAP Group - LUNDI.AKRANES 

一般  
情報 | 参照 | 属性マップ | クラスマップ

認証オプション

プロキシユーザ:

パスワードとの単純バインドに TLS を必要とする

- 5 [適用] をクリックし、[OK] をクリックします。

## TLS を開始 / 停止する

LDAP 拡張オペレーション STARTTLS により、クリア接続から暗号化された接続にアップグレードすることができます。このアップグレードは、eDirectory 8.7 の新機能です。

暗号化された接続を使用すると、パケット全体が暗号化されます。このため、ネットワーク経由で送信されたデータが第三者によって診断されることはありません。

**シナリオ：STARTTLS を使用する** — ポート 389 にクリア接続し、匿名検索を行います。ただし、セキュリティ保護されたデータを扱う場合には TLS セッションに切り換えます。拡張オペレーション STARTTLS を実行し、クリア接続から暗号化された接続にアップグレードします。これでデータの安全が確保されます。

暗号化されたセッションをクリア接続に切り替えるには、TLS を停止します。クリア接続では、クライアントが送受信するデータは暗号化および解読されないため、負荷は少なくなります。そのため、クリア接続の使用時の方が、データの通信速度が速くなります。この時点で、接続は匿名にダウングレードされています。

認証を受けるには LDAP バインド操作を使用します。バインドは、ユーザの認証情報に基づいて ID を作成します。TLS を停止するときに、LDAP サービスは以前に確立された認証をすべて削除します。認証ステータスが匿名に変わります。匿名以外の状態に切り替える場合は、再認証を受ける必要があります。

**シナリオ：再認証を受ける** — あるユーザが STOPTLS を実行します。すると、そのユーザの状態が匿名に変わります。このユーザのファイルにネット上でアクセスするには、Bind コマンドを実行し、ログイン認証情報を入力します。ユーザが認証され、インターネット上でクリアテキストで作業を続行できます。

## TLS のサーバを環境設定する

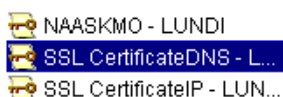
TLS セッションがインスタンス化されると、ハンドシェークが行われます。サーバとクライアントがデータを交換します。ハンドシェークの方法はサーバが決定します。サーバの正当性を証明するため、サーバは常にサーバの証明書をクライアントに送信します。このハンドシェークにより、そのサーバがクライアントに指定されたサーバであることが証明されます。

クライアントにも正当性の証明を要求するには、サーバに値を設定します。これは `ldapTLSVerifyClientCertificate` という属性です。

| 値 | 説明   |
|---|--|
| 0 | オフハンドシェーク時に、サーバがクライアントに証明書を提供します。サーバがクライアントに証明書の送信を要求することはありません。クライアントは証明書を使用することも、無視することもできます。セキュリティ保護されたセッションが確立されます。  |
| 1 | ハンドシェークの間、サーバは証明書をクライアントに送信し、クライアントからも証明書を要求します。クライアントはサーバに証明書を送信できます。クライアントの証明書が確認されます。サーバがクライアントの証明書を確認できない場合、接続は切断されます。<br><br>クライアントが証明書を送信しない場合、サーバは接続を維持します。 |
| 2 | ハンドシェークの間、サーバはクライアントから証明書を要求します。クライアントが証明書を提供しない、または証明書が確認できない場合には、接続は切断されます。  |

サーバが TLS をサポートするよりも前に、サーバの正当性の証明に使用される X.509 証明書をサーバに提供する必要があります。

この証明書は、eDirectory のインストール時に自動的に提供されます。インストール時に、パブリックキー暗号化サービス (PKI) で、キーオブジェクトと Novell Modular Authentication Services (NMASTM) が作成されます。次の図は、iManager におけるこれらのオブジェクトを示しています。



インストール中、これらの証明書の 1 つが LDAP サーバと自動的に関連付けられます。Novell iManager の LDAP サーバオブジェクトの [接続] タブに DN が表示されます。この DN は、X.509 の証明書を表しています。次の図のサーバ証明書フィールドは、この DN を示しています。

LDAPサーバ: LDAP Server - LUNDI.AKRANES

一般  
情報 | **接続** | 検索 | イベント | 追跡中 | 参照

トランスポート層セキュリティ(TLS / SSL)

サーバ証明書: SSL CertificateDNS

Novell iManager で、暗号化キーオブジェクト (KMO) 証明書を参照できます。また、ドロップダウンリストから、別の証明書に変更することもできます。DNS または IP 証明書のいずれかを使用します。

検証の際には、サーバは証明書にある名前 (ハード IP アドレスまたは DN) を確認します。

TLS 接続を確立するには、次の条件を確認します。

- ◆ LDAP サーバはそのサーバの KMO を認知している必要があります。
- ◆ クリアポートに接続してから、セキュアポートに接続するか TLS を開始します。

LDAP サーバを再設定し、サーバをリフレッシュします。**363 ページの「LDAP サーバをリフレッシュする」**を参照してください。ConsoleOne と Novell iManager は、自動的にサーバをリフレッシュします。

## TLS のクライアントを環境設定する

LDAP クライアントとは、たとえば Netscape Communicator、Internet Explorer、ICE のようなアプリケーションです。クライアントは、LDAP サーバが使用する認証局を認知している必要があります。

サーバが eDirectory ツリーに追加されると、インストールの際にデフォルトで次が作成されます。

- ◆ ツリーの認証局 (ツリー CA)
- ◆ ツリー CA からの KMO

LDAP サーバはこの認証プロバイダを使用します。

クライアントは、LDAP サーバが使用していると主張するツリー CA を確認できるよう、信頼する証明書をインポートする必要があります。この証明書をサーバからインポートしておく、サーバがその証明書を送信してきたときに、クライアントはそれを確認し正当なサーバであるかどうか確かめることができます。

クライアントが安全に接続できるよう、接続前にクライアントの環境設定をしておく必要があります。

クライアントによる証明書のインポート方法は、使用しているアプリケーションの種類によって異なります。各アプリケーションには、何らかの証明書をインポートする方法があります。Netscape ブラウザ、IE、ICE は、それぞれ別々の方法でインポートを行います。これらのインポート手段は、3つの異なる LDAP クライアントです。各クライアントは、それぞれの方法で信頼する証明書を探します。

## ルート認証局をエクスポートする

ルート認証局は、証明書サーバを受け入れるときに自動的にエクスポートできます。

ルート認証局を手動でエクスポートするには、**Exporting a Trusted Root or Public Key Certificate (<http://www.novell.com/documentation/lg/crt27/crtadmin/data/a2ebopb.html#a2ebopd>)**を参照してください。

エクスポート機能により、指定したファイルが作成されます。ファイル名は変更できませんが、オブジェクトのタイプを認識できるように、ファイル名に「DNS」または「IP」を残しておくことをお勧めします。また、サーバ名も残しておきます。

eDirectory との安全な LDAP 接続を確立するブラウザに、自己割り当て認証局をインストールします。

Internet Explorer など、Microsoft 社の製品で証明書を使用する場合は、.der 拡張子を残しておくようにします。


アプリケーションまたは SDK が証明書を要求する場合は、証明書をデータベースにインポートします。

Internet Explorer 5 の場合は、ルート証明書が自動的にエクスポートされ、レジストリが更新されます。これには、Microsoft が通常使用している .x509 拡張子が必要です。

## クライアント証明書で認証を受ける

相互認証には、TLS セッションとクライアント証明書が必要です。サーバとクライアントの両方が、それぞれが自分の主張するオブジェクトであることを証明する必要があります。クライアントの証明書がトランスポート層で確認されます。しかし、LDAP プロトコル層では、LDAP バインド要求を出すまでクライアントは匿名になります。

この時点で、クライアントはその正当性をサーバに証明しましたが、LDAP にはまだ証明されていません。クライアント証明書に含まれた ID で認証を受けたい場合は、クライアントは SASL EXTERNAL メカニズムを使ってバインドされます。

- 1 Novell iManager で、[役割およびタスク] ボタン  をクリックします。
- 2 [LDAP] > [LDAP の概要] の順にクリックします。
- 3 [LDAP サーバの表示] をクリックし、LDAP サーバオブジェクトの名前をクリックします。
- 4 [接続] をクリックします。
- 5 トランスポート層のセキュリティセクションのドロップダウンメニューから [クライアント証明書]、[必須] の順に選択します。  
これにより、相互認証が可能になります。
- 6 [適用] をクリックし、[OK] をクリックします。

## サードパーティプロバイダの証明書を使用する

eDirectory のインストール時に、LDAP サーバにツリー認証局 (CA) が提供されます。LDAP キーオブジェクトは、その CA に基づいています。クライアントが LDAP サーバに送信する証明書は、このツリー CA から確認できます。

LDAP Services for eDirectory 8.8 は、複数の認証局をサポートしています。Novell のツリー CA はそのうちの 1 つです。LDAP サーバが、他の CA を持っている場合があります (例: 外部団体の VeriSign\* など) この追加 CA もルート認証局です。

LDAP サーバが複数の認証局を使用するように環境設定するには、LDAP サーバオブジェクトの ldapTLSTrustedReaderContainer 属性を設定します。LDAP サーバが複数の認証局を参照することにより、クライアントは外部の認証局を使用できます。

## LDAP プロキシユーザを作成および使用する

Novell eDirectory は、認証されていないユーザに [Public] 識別子を割り当てます。LDAP プロトコルでは、認証されていないユーザは匿名ユーザになります。デフォルトでは、LDAP サーバは匿名ユーザに [Public] 識別子の権利を与えます。この権利により、非承認の eDirectory および匿名 LDAP ユーザは、[Public] 権を使用して eDirectory を参照することができます。

また、LDAP サーバは匿名ユーザによる別のプロキシユーザの権利の使用を許可しません。この値は LDAP グループオブジェクトにあります。Novell iManager では、この値は、[プロキシユーザ] フィールドで指定します。また ConsoleOne の場合は、[プロキシユーザ名] フィールドで指定します。次の図は、Novell iManager の [プロキシユーザ] フィールドを示しています。

LDAPグループ: LDAP Group - LUNDI.AKRANES

一般  
情報 | 参照 | 属性マップ | クラスマップ


認証オプション  
プロキシユーザ:  
 🔍  
 パスワードとの単純バインドにTLSを必要とする

プロキシユーザは識別名です。このプロキシ ID に、Public 識別子とは別の権利を与えることができます。プロキシユーザを使用すると、eDirectory ツリー内の特定コンテナへの LDAP 匿名アクセスを制御できます。

**注:** プロキシユーザのログイン制限は、すべての匿名 LDAP ユーザに適用する場合以外は設定しないでください。

**シナリオ: NLDAP プロキシユーザを設定する** — Digital Airlines 社はリサーチ会社の DataSure 社と契約を締結しています。DataSure 社は LDAP を使用して、Digital Airlines 社の NetWare 6 サーバである DigitalAir43 にアクセスし、そのリサーチを保存します。Digital Airlines 社は、DataSure 社に DigitalAir43 のディレクトリに対する [Public] 権を与えたくないとしています。

そのために、LDAP プロキシユーザを作成し、そのユーザに DataSure ディレクトリに対する特定の権利を割り当てます。LDAP グループオブジェクトにプロキシ識別名を作成し、サーバをリフレッシュします。サーバは自動的に、すべての新規または既存の匿名ユーザについて、プロキシユーザの権利の使用を開始します。

- 1 Novell iManager で、[役割およびタスク] ボタン  をクリックします。
- 2 [eDirectory 管理] > [オブジェクトの作成] の順にクリックし、プロキシユーザを作成します (例: LDAPProxy)。
- 3 ユーザに NULL パスワードを割り当てます。
- 4 (オプション) 指定したディレクトリにプロキシユーザの権利を割り当てます。
- 5 [LDAP] > [LDAP の概要] > [View LDAP グループの表示] > [LDAP グループオブジェクト] の順にクリックします。
- 6 [プロキシユーザ] フィールドで [参照] ボタンをクリックし、LDAPProxy ユーザを選択して [OK] をクリックします。

## SASL を使用する

SASL (Simple Authentication and Security Layer) は、IANA (Internet Assigned Numbers Authority) で登録する必要のあるさまざまな認証メカニズムを定義します。LDAP サーバでは次のメカニズムがサポートされます。

- ◆ DIGEST-MD5
- ◆ EXTERNAL
- ◆ NMAS\_LOGIN
- ◆ GSSAPI

これらのメカニズムは、eDirectory のインストールまたはアップグレード時に、サーバにインストールされます。ただし、Linux および UNIX の場合は nmasinst ユーティリティを実行して NMAS メソッドをインストールする必要があります。

LDAP サーバは、SASL に問い合わせた環境設定時にインストールしたメカニズムを検索し、インストールされたメカニズムを自動でサポートします。また、supportedSASLMechanisms 属性を使って rootDSE で現在サポートされている SASL メカニズムをレポートします。

これらのメカニズムは登録されているため、名前はすべて大文字で入力します。大文字で入力しない場合、LDAP サーバはメカニズムを認識しません。

LDAP バインドプロトコルでは、クライアントは認証に様々な SASL メカニズムを使用することができます。アプリケーションが LDAP バインド API を使用している場合は、単純バインドを選択し、DN とパスワードを入力するか、SASL バインドを選択し、SASL メカニズム名 (大文字) と、そのメカニズムが要求する、関連する SASL 認証情報を提供する必要があります。

### DIGEST-MD5

DIGEST-MD5 メカニズムには TLS は必要ありません。LDAP サーバは、クリア接続およびセキュア接続の両方で DIGEST-MD5 をサポートします。

LDAP は、バインド要求で SASL メカニズムをサポートします。ユーザが LDAP 単純バインド (DN およびクリアテキストパスワード) の代わりに、LDAP SASL バインドを要求すると、DN と MD5 認証情報が提供されます。

MD5 は、暗号化されたパスワードのハッシュを提供します。パスワードは、クリア接続でも暗号化されます。そのため LDAP サーバは、ポートがクリアテキストポートか暗号化されたポートかに関係なく、MD5 を使ったパスワードを受け入れます。

このパスワードが第三者によって見破られることはありません。ただし、接続全体に対してなりすましやハイジャックがなされる可能性はあります。

メカニズムは LDAP SASL バインドです (単純バインドではありません)。そのため、インストール時に [パスワードとの単純バインドに TLS を必要とする] チェックボックスがオンになっている場合、LDAP サーバはこの要求を受け入れます。



## EXTERNAL

EXTERNAL メカニズムにより、ユーザの DN および認証情報がサーバに提供されたことが LDAP サーバに通知されます。そのため、バインド要求時には DN と認証情報は必要ありません。

SASL EXTERNAL メカニズムを使用した LDAP バインド要求は、サーバに次を実行するよう要求します。

- ◆ EXTERNAL 層に認証情報を問い合わせる
- ◆ ユーザをその認証情報を持つユーザとして認証する

安全なハンドシェイクが行われます。サーバはクライアントから認証情報を要求し、クライアントはそれをサーバに渡します。LDAP サーバはクライアントから渡された証明書を受け取り、それを NMAS モジュールに渡して、ユーザを証明書にある DN として認証します。

使用できる DN の証明書を使用するには、クライアントを設定する必要があります。証明書の設定に関する詳細は、[NMAS \(http://www.novell.com/documentation/beta/nmas30/index.html\)](http://www.novell.com/documentation/beta/nmas30/index.html) オンラインマニュアルを参照してください。

クライアントが EXTERNAL メカニズムを送信しても、LDAP サーバは要求の処理に失敗することがあります。Novell iMonitor により、処理が失敗した原因が通知されます。次のような原因が考えられます。

- ◆ 接続がセキュア接続ではない。
- ◆ 接続はセキュア接続だが、クライアントがハンドシェイク時に要求された証明書を提供しなかった。
- ◆ SASL モジュールを使用できない。
- ◆ クライアントが要求を送信する前に rootDSE をチェックしなかった。

## NMAS\_LOGIN

NMAS\_LOGIN メカニズムにより、LDAP サーバに NMAS のバイOMETリック機能が提供されます。詳細については、Novell NDK を参照してください。

サーバの起動時に、LDAP サーバは SASL モジュールを初期化し、その LDAP サーバがどのメカニズムを使用できるかを SASL モジュールに問い合わせます。

クライアントは rootDSE に問い合わせ、サポートされているメカニズム属性を検索することができます。LDAP サーバはその後、サポートされているメカニズムを表示します。

## GSSAPI

GSSAPI メカニズムにより、チケットを使用して Kerberos ユーザの eDirectory サーバへの認証を行うことができます。その際に、個別の LDAP ユーザパスワードの入力は不要です。

この機能は、Kerberos インフラストラクチャがすでに配置された環境がある LDAP アプリケーションユーザ向けのものです。このようなユーザは、個別の LDAP ユーザパスワードを入力することなく、Kerberos サーバで発行されたチケットを使用して LDAP サーバへの認証を行うことができます。

GSSAPI の設定については、[587 ページの付録 E「eDirectory での GSSAPI の設定」](#)を参照してください。

# LDAP サーバを使ってディレクトリを検索する

このセクションでは、次の情報について説明します。

- ◆ 372 ページの「検索制限を設定する」
- ◆ 373 ページの「参照を使用する」
- ◆ 378 ページの「フィルタ済みレプリカを検索する」

## 検索制限を設定する

次の LDAP サーバオブジェクトの属性により、LDAP サーバのディレクトリ検索方法を指定することができます。

- ◆ 検索エントリの制限

検索のサイズを制限します。デフォルトは 0 で、サイズの制限はありません。LDAP サーバの負荷が大きくなりすぎないように、検索要求に対して LDAP サーバが返すエントリ数を制限できます。


**シナリオ：検索のサイズを制限する** — ユーザは、検索結果が何千件にもなりそうな、あるオブジェクトの検索を要求します。ただし、検索結果は 10 件に制限してあります。LDAP サーバは 10 件の検索結果を返すと検索を中止します。一致するデータがまだ存在しているが、検索が終了されたことを告げるシステムメッセージが表示されます。

- ◆ 検索時間制限

サーバが検索を行う時間を制限します。デフォルトは 0 秒です。これは時間制限がないことを表します。

次の図は、Novell iManager におけるこれらの属性を示します。

The screenshot shows the configuration page for an LDAP Server in Novell iManager. The title bar reads "LDAP サーバ: LDAP Server - LUNDI.AKRANES". Below the title bar is a navigation menu with tabs: "一般" (General), "情報" (Info), "接続" (Connections), "検索" (Search), "イベント" (Events), "追跡中" (Tracing), and "参照" (References). The "検索" (Search) tab is selected. Under the "検索" tab, there are two main sections: "最大同時持続的検索数" (Maximum concurrent persistent search count) and "制限" (Limits). The "最大同時持続的検索数" section has a text input field containing "0" and a label "操作(0=無制限)". Below it is a checked checkbox labeled "持続的検索動作の監視時にサイズと時間制限を無視する". The "制限" section has two rows: "エントリ制限" (Entry limit) with a text input field containing "0" and a label "エントリ(0=無制限)", and "時間制限" (Time limit) with a text input field containing "0" and a label "秒 (0=タイムアウトなし)".

- 1 Novell iManager で、[役割およびタスク] ボタン  をクリックします。
- 2 [LDAP] > [LDAP の概要] > [LDAP サーバの表示] の順にクリックします。
- 3 [LDAP サーバオブジェクト] > [検索] の順にクリックします。
- 4 制限セクションをスクロールして値を入力し、[OK] をクリックします。



クライアントも、検索要求に制限を設定することもできます(たとえば検索を2秒に制限するなど)。クライアントの制限がサーバの制限と競合する場合、LDAPサーバは値が小さい方の要求を採用します。

検索は、アクセス制御リスト(ACL)に基づいて実行されます。このため、匿名検索の場合は、ディレクトリに何千というエントリが存在していても、Public権で見ることのできるごく一部のエントリしか返されることがあります。

## 参照を使用する

参照は、名前を解決するためのクライアント中心の方法です。LDAPクライアントがLDAPサーバに要求を送信すると、LDAPサーバは要求操作のターゲットエントリをローカルに見つけようとします。LDAPサーバはターゲットエントリを見つけられないと、所有する知識参照を使用して、そのエントリについてのより多くの知識を持つ第2のLDAPサーバへの参照を生成します。第1のサーバは、参照情報をLDAPクライアントに送信します。

次に、LDAPクライアントは第2のLDAPサーバへ接続し、操作を再実行します。第2のLDAPサーバが操作のターゲットエントリを保持している場合は、そのサーバが操作を実行します。エントリを保持していない場合は、第2のLDAPサーバもまた参照をクライアントに送信します。この操作は、次のいずれかの状況になるまで続けられます。

- ◆ クライアントがターゲットエントリを保持するサーバと接続し、要求する操作が実行できる。
- ◆ LDAPサーバが、エントリは存在しないとのエラーを返す。
- ◆ LDAPサーバがこれ以上参照先がないことを通知する。

LDAP for eDirectory 8.7で導入された機能により、参照の動作が以前のバージョンのeDirectoryおよびNDSから少し変更されました。これにより、LDAPサービスの環境設定方法も変更されました。

## デフォルトの参照

通常、デフォルトの参照URLには、ツリーのルートを保持するサーバを指すLDAP URLが含まれています。LDAP URLの形式を次に示します。ldap://ホスト:ポート。

[デフォルト参照URL] フィールドに、デフォルトの参照先を入力します。



これまで、eDirectory LDAPサーバは、多くのフェイルオーバー時にデフォルトの参照先を送信していました。これが、この動作を予期しないユーザを混乱させる結果になっています。そこで、LDAP Services for eDirectory 8.8では、サブオーディネート参照で、デフォルトの参照先が送信される場合を指定できるようになりました。

この新しいオプションは、LDAP サーバおよび LDAP グループオブジェクトの `ldapDefaultReferralBehavior` 属性の値で指定します。値は次のビットのビットマスクである整数です。

| ビット        | 値  |
|------------|--|
| 0x00000001 | ベース DN が見つかりません                          |
| 0x00000002 | ベース DN は、利用できない eDirectory サーバ上にあります     |
| 0x00000004 | 検索スコープのエントリは、利用できない eDirectory サーバ上にあります |

LDAP サーバがその操作に対して「常に参照する」に設定されており、リストされたいずれかの条件と一致し、対応する値が設定されている場合、デフォルトの参照先が返されます。

### 検索操作の参照先を設定する

LDAP for eDirectory 8.7 で導入された機能により、参照の動作が以前のバージョンの eDirectory および NDS から少し変更されました。これにより、LDAP サービスの環境設定方法も変更されました。

eDirectory ツリー内の他の eDirectory サーバに参照先を返すように eDirectory LDAP サーバを設定することができます。デフォルトでは、LDAP サーバはユーザに代わってすべての操作を他の eDirectory サーバにチェーンし、参照先は返しません。

eDirectory 8.7 より以前は、参照先オプションの設定は LDAP グループオブジェクトでだけしか使用できませんでした。eDirectory 8.8 では、LDAP サーバオブジェクトにもこのオプションを設定することができるようになりました。LDAP サーバオブジェクトの設定により、LDAP グループオブジェクトの設定は上書きされます。

`ldapSearchReferralOption` 属性を操作することにより、照会先オプションを設定することができます。LDAP Services for eDirectory 8.7 より以前は、この属性を次のオプションに設定することができました。

- ◆ [376 ページの「チェーンを優先する」](#) (デフォルトオプション)
- ◆ [376 ページの「参照を優先する」](#)
- ◆ [377 ページの「常に参照する」](#)

これらの参照オプションは、eDirectory ツリー内の他の eDirectory サーバの参照およびチェーンでだけ使用できます。この設定は、信頼されていないパーティションからの参照は制御しません。そのため、[照会先オプション] ドロップダウンリストでオプション ( [常にチェーンする] など ) を選択しても、他のサーバの信頼されていないパーティションからは参照先が送信されます。

LDAP Services for eDirectory 8.7.a では [常にチェーンする] オプションにより、eDirectory DSA 以外の上方向参照がサポートされています。[375 ページの「常にチェーンする」](#) を参照してください。

次の図は、検索およびその他の操作に使用する [LDAP 参照] ドロップダウンリストを示しています。

LDAP サーバ: LDAP Server - LUNDI.AKRANES

---

一般

情報 | 接続 | 検索 | イベント | 追跡中 | 参照

ホームDNが存在しない

検索エントリが使用不可サーバ上にある

参照オプション

eDirectory 検索に対して:

チェーンを優先する

その他の eDirectory 操作に対して:

チェーンを優先する

eDirectory 操作にはこの他に、「追加」、「削除」、「編集」、「バインド」の各操作の参照があります。

### 常にチェーンする

[常にチェーンする] オプションは、「まったく参照しない」ように設定するオプションです。このオプションを選択すると、eDirectory LDAP サーバは、eDirectory ツリー内にある他の eDirectory サーバに参照先を返しません。LDAP サーバは、要求を出したクライアントに代わって他の LDAP サーバをチェックし、クライアントに参照先を返します。

[常にチェーンする] オプションは、eDirectory をグローバル連結ツリーのサブオーディネートサーバとして使用している場合に適しています。

この参照先オプションは、eDirectory ツリー内の参照先の処理設定にのみ使用します。このオプションが eDirectory サーバ以外のサーバの参照の動作に影響することはありません。

他のディレクトリサーバへの参照をブロックすることによりあまり意味はありませんが、これが重要になる場合もあります。eDirectory 8.7 以降のサーバ上の信頼されていないデータを古いバージョンの eDirectory サーバ上で複製すると、古いサーバを参照したときにクライアントアプリケーションのグローバルツリーが歪んで表示されることがあります。

たとえば、LDAP クライアントは LDAP サーバの参照をキャッシュし、最後に通信したサーバに要求を送信するとします。クライアントが上方参照をサポートする eDirectory サーバに要求を送信するよう設定されている場合、クライアントのグローバルツリーは正常に表示されます。

しかし、eDirectory 8.7 以前の LDAP サーバは、信頼されていない領域と上方参照を認識しません。このため、クライアントが eDirectory ツリー内の以前のバージョンの eDirectory サーバの参照に従い、要求をそのサーバに送信し続けると、以前のバージョンの LDAP サーバにより、信頼されていないデータが実際のディレクトリツリーデータであるかのように表示されてしまいます。

ただし、クライアントによっては、RootDSE の supportedFeatures 属性をチェックし、サーバが上方参照をサポートしているか確認できるものもあります。

## チェーンを優先する

[チェーンを優先する] オプションを選択すると、通常、検索操作で参照先は返されません。LDAP サーバはその代わり、すべての eDirectory DSA に対する検索操作を実行します。

ただし、持続的検索制御を設定して検索を実行する場合は例外となります。Novell の実装する持続的検索ではチェーンがサポートされていないため、検索スコープがローカルに限られていなければ参照が送信されます。

LDAP サーバが検索操作を受信します。ツリーのエントリがローカルに格納されていない場合、サーバは自動的に他のサーバにチェーンします。エントリの検出後、LDAP サーバは LDAP クライアントのプロキシとして機能します。LDAP サーバは LDAP クライアントがバインドされたものと同じ識別情報を使用してリモートサーバの認証を受け、そこで検索操作を続行します。

最初に要求を受信した LDAP サーバが、LDAP クライアントにすべての検索エントリと検索結果を送信します。この LDAP サーバが要求をすべて処理するため、LDAP クライアントからは他のサーバが関与していることはわかりません。

eDirectory でチェーンを使用すると、ある LDAP サーバに多くのデータがない場合でも、そのサーバがツリー全体のデータを保持しているかのように見えます。

[チェーンを優先する] は、パーティションに深くかかわるオプションです。

**シナリオ：他のパーティションで情報を探す** — Digital Airlines 社で、ユーザが LDAP サーバ DAir43 に [チェーンを優先する] オプションを選択しました。DAir43 はパーティション A にあります。パーティション B は A のサブパーティションで、LDAP サーバ DAir44 はこのパーティションにあります。

ある LDAP クライアントが検索を要求します。DAir43 は、エントリをローカルで検索しますが、データが一部しか見つかりません。DAir43 は、要求されたエントリを持つ DigitalAir44 に自動的にチェーンします。DAir44 は、DAir43 にデータを送信し、DAir43 は、LDAP クライアントにエントリを送信します。

[チェーンを優先する] オプションを使用すると、操作が持続的検索である場合を除き、LDAP サーバは必要に応じて検索を他のサーバにチェーンします。持続的検索の詳細については、[383 ページの「持続的検索：eDirectory イベントの設定」](#)を参照してください。

## 参照を優先する

[参照を優先する] オプションを選択すると、必要に応じ、参照の検索結果が eDirectory ツリー内の他の eDirectory サーバに返されます。この参照は、データを持つサーバが動作可能であり、LDAP サービスが稼働していることをローカルサーバが確認した場合のみ送信されます。それ以外の場合、操作は他のサーバにチェーンされるか、他のサーバが動作していない場合は処理に失敗します。

パーティションが 2 つあり、サブツリー検索を実行するとします。ローカルサーバから検索エントリがすべて検出されるまで検索が実行されます。そこで、今度は他のサーバの検索を実行します。データのレプリカ (そのパーティション) を持つサーバが nldap.nlm も実行している場合、LDAP サーバは LDAP 参照を確立し、それを LDAP クライアントに返します。

レプリカのあるサーバが nldap.nlm を実行していない場合、LDAP サーバは要求を他のサーバにチェーンし、そこで検索を完了します。

nldap.nlm が起動されると、LDAP サーバはその LDAP サーバが参照先の eDirectory と通信します。クライアントが参照を受信したのに、その参照が停止した場合は、LDAP サーバが実行されていません。

## 常に参照する

[参照を優先する] オプションは、デフォルト参照がさまざまなフェイルオーバー (たとえば、オブジェクトが見つからなかったり、サーバがダウンしているなど) の状態で送信される場合を除き、[参照を優先する] と同じロジックに従います。

残りのデータのある他のサーバで LDAP サービスが実行されていない場合、最初の LDAP サーバは要求を第 2 のサーバへチェーンしません。

[常に参照する] オプションを設定している場合には、デフォルト参照を指定することができます。[デフォルトの照会先] フィールドで 2 つの異なるベンダの LDAP サーバを結合し、独自のディレクトリツリーを構築することができます。

**シナリオ：デフォルトサーバを使用する** — 1 つの LDAP ツリーがあるとします。ツリーの一部には eDirectory のサービスが適用されています。サブオーディネイトパーティションには iPlanet のサービスが実行されています。[デフォルトの照会先] フィールドに、iPlanet サーバの URL を入力します。ある LDAP クライアントが検索を要求します。

ベース DN を解決できないため、LDAP サーバは [デフォルトの照会先] フィールドに入力された文字列をクライアントに送ります。LDAP クライアントはこの参照の URL で指定された場所を参照して iPlanet サーバに接続し、ここで検索は完了します。

デフォルトの参照が設定されており、ベース DN が見つからない場合、サーバはクライアントにデフォルト参照を返します。

参照の形式は、LDAP URL です (例：LDAP://123.23.45.6:389)。

LDAP サーバがデフォルト参照をクライアントに送信するとき (ベース DN が利用できない場合) は、サーバはこれにスラッシュ (/) とクライアントが検索中の DN を追加します。デフォルト参照と追加された情報がクライアントに送信されます。クライアントはデフォルト参照で指定したサーバに検索要求を送信します。

LDAP グループオブジェクトには、デフォルト参照の文字列フィールドがあります。LDAP サーバは、そのデータを文字列として扱います。このとき、確認は行われません。入力された文字列が、参照の先頭に追加されます。また、なんらかのデータが参照に追加されます。LDAP サーバが受け入れる文字列の形式は、URL のような形式になります。

LDAP が実行されている他の eDirectory サーバの参照がクライアントに返されるとき、クライアントは 1 つのサーバにつき 2 つの参照を受信します。

- ◆ クライアントをクリアテキストポートに導く参照
- ◆ クライアントをセキュアポートに導く参照

2 つの参照を区別するために、クリアテキスト参照には ldap://、セキュアポート照会には ldaps:// が付きます。

サーバからの参照の場合は、ポート番号を追加します。

## 他の操作の参照を設定する

履歴参照オプション設定は通常、検索操作にのみ使用します。他の処理に比較オプションを適用する場合は、ldapOtherReferralOption 属性が使用されます。この属性により、同じ値を使って検索以外の操作の動作を制御できます (参照を送信しないバインドは除きます)。

## ManageDsaIT の非サポート

LDAP Services for eDirectory 8.8 では、eDirectory ツリー内の eDirectory サーバの分散関係は、ManageDsaIT 制御以外の方法で管理されます。LDAP クライアントは、ManageDsaIT 制御を使って eDirectory サブオーディネートまたは相互参照の問い合わせや更新を実行することはできません。

### サポートされていない機能

LDAP Services for eDirectory 8.8 では、サブオーディネートリファレンスはサポートされていません。信頼されたパーティションのサブオーディネートパーティションとして信頼されていないパーティションを作成したり、そのパーティションから参照を送信させると失敗する場合があります。これを行う場合、参照は操作のベース DN を解決するときのみ送信されます。SearchResultReferences は送信されません。

信頼されていない領域のデータの分散更新はサポートされていません。ルートサーバで名前の変更があった場合、名前の変更を信頼されていない領域で同じデータを持った eDirectory サーバにコピーするような組み込みのメカニズムはありません。

## フィルタ済みレプリカを検索する

フィルタはレプリカが持つデータ量を制限します。そのため、フィルタ済みのレプリカには、ディレクトリが保持する実データが完全には表示されません。次はレプリカに適用されたフィルタの例です。


- ◆ レプリカに含まれるのはユーザオブジェクトだけです。
- ◆ レプリカにはすべてのユーザオブジェクトが含まれますが、オブジェクトには電話番号と住所しか含まれません。

フィルタ済みレプリカのデータは不完全なため、LDAP 検索の結果も制限されます。そのため、デフォルトでは、LDAP 検索要求はフィルタ済みレプリカを調べません。

次のような場合は、フィルタ済みレプリカ検索を実行しても、レプリカフィルタから何も検索結果が返されないことがあります。


- ◆ 検索フィルタに一致するオブジェクトがローカルのフィルタ済みレプリカサーバに存在しない場合、結果が完全なレプリカサーバから取得されるため、ローカルのレプリカフィルタの結果と一致しないことがあります。
- ◆ 検索ベースがフィルタ済みレプリカサーバのローカルにない場合、検索フィルタに一致するオブジェクトが完全なレプリカサーバから取得され、これがローカルレプリカのフィルタの結果と一致しないことがあります。

ただし、フィルタ済みレプリカに必要なデータがあることがわかっている場合は、LDAP サーバがフィルタ済みレプリカを検索するように設定することができます。

- 1 Novell iManager で、[役割およびタスク] ボタン  をクリックします。
- 2 [LDAP] > [LDAP の概要] の順にクリックします。
- 3 [LDAP サーバの表示] をクリックし、LDAP サーバの名前をクリックします。
- 4 [検索] をクリックします。



5 [検索にフィルタ済みレプリカに含める] を選択し、[適用] をクリックします。

LDAPサーバ:  LDAP Server - Server1-2000-NDS

一般

情報 | 接続 | **検索** | イベント | 追跡中 | 参照

### フィルタ済みレプリカ

検索にフィルタ済みレプリカを含める

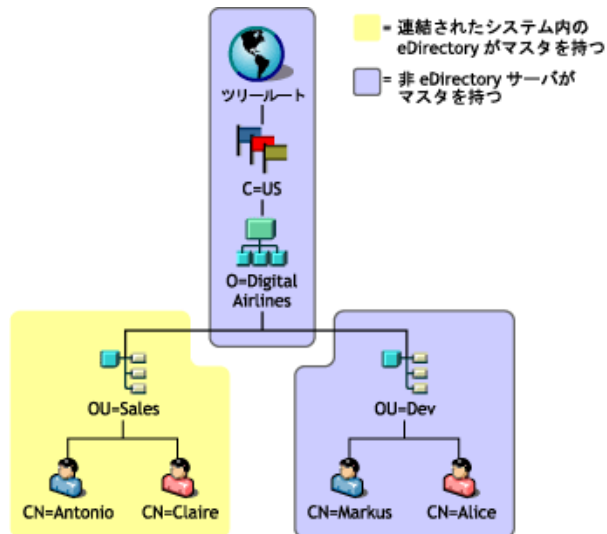
## 上方参照を設定する

組織の規模が大きくなると、さまざまなベンダの LDAP サーバソフトウェアを使用したディレクトリツリーが必要になります。このようなツリーを、グローバル連結ツリーといいます。LDAP Services for eDirectory 8.8 には、参照を連結ツリーの上方の DSA に返す機能があります。

### シナリオ：連結ツリーでの上方参照

Digital Airlines 社には、あるネットワーク担当者がいます。Digital Airlines 社のディレクトリツリーのルート (ツリーのルートから O=Digital Airlines まで) のマスタは、OpenLDAP サーバ上にあります。組織 (OU=Sales) のマスタは eDirectory サーバにあり、その他の組織 (OU=Dev) は iPlanet サーバ上にあります。

次の図は、このツリーを示します。



eDirectory にマスタがあるのは、OU=Sales のパーティション内のデータだけです。他の領域のデータのマスタは eDirectory 以外の DSA 上にあります。ネットワーク担当者は、操作の対象が O=Digital Airlines より上の領域、または OU=Sales 階層に属さない O=Digital Airlines より下の領域である場合、上方参照を返すように LDAP サービスを設定します。

ベース DN が OU=Dev,O=Digital Airlines,C=US の eDirectory LDAP サーバに操作が送信されます。そのエントリーを保持するサーバ、またはそのエントリーを保持するサーバを認知しているサーバを指す参照が返されます。

同様に、O=Digital Airlines,C=US が対象のサブツリー検索でも、ルート DSA の参照が返されます。するとルート DSA が、OU=Sales および OU=Dev のマスタである DSA の照会を返します。

LDAP サービスにより、eDirectory サーバがこのツリーに参加するのにデータ階層データを信頼されていないパーティションに持つことができます。信頼されていない領域のオブジェクトに含まれるのは、正しい DN 階層を構築するのに必要なエントリーだけです。これらのエントリーは、X.500 の“Glue”エントリーに類似しています。

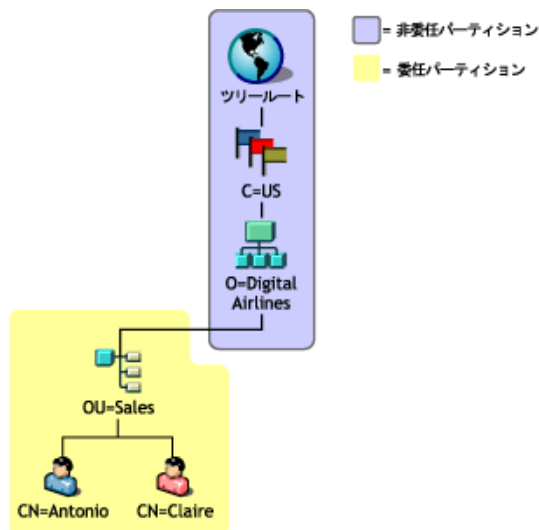
このシナリオでは、ルート、C=US、O=Digital Airlines オブジェクトは eDirectory サーバの信頼されていない領域にあります。

eDirectory では、知識情報 (参照データ) を信頼されていない領域に置くことができます。この情報は、LDAP クライアントに参照を返すのに使用します。

LDAP 操作を eDirectory ツリーの信頼されていない領域で実行すると、LDAP サーバは正しい参照データを検索し、クライアントに参照を返します。

## 信頼されていない領域を作成する

次の図は、379 ページの「シナリオ：連結ツリーでの上方参照」で示した、eDirectory サーバの連結ツリーが保持する実際のデータを示しています。



エントリーは、マスタが他の DSA 上にあっても、OU=Sales 上に配置されます。これは、eDirectory サーバが持つエントリーに適切な DN を提供できるようにするためです。

信頼されていない領域を作成するには、次を実行します。

- 1 信頼されていないデータは信頼されたデータとは切り離します。

信頼された領域の最上部に、パーティション境界を作成します。他に指定がない場合、eDirectory サーバはすべてのデータに対して信頼されたサーバであるとみなされます。



**2** ルートパーティションに信頼されていないパーティションとマークします。

**2a** 信頼属性を、パーティションの最もルートに近い属性に追加します。

**2b** 値が 0 の信頼属性を作成します。

**3** 信頼されていない領域の最下部に境界線をひきます。

このサーバの信頼されたサブツリー領域にパーティションルートを作成します。たとえば上の図の場合は、パーティションルートは OU=Sales エントリにあります。新しいパーティションには、0 に設定された信頼属性はありません。そのため、サーバはパーティションに対し信頼されたサーバであることとなります。

**4** LDAP サーバをリフレッシュします。

LDAP サーバは、その設定がリフレッシュされるたび、信頼された領域および信頼されていない領域の境界をキャッシュします。手動でサーバの設定をリフレッシュしない場合、サーバは 30 分毎のバックグラウンドタスクで自動的にリフレッシュします。

複数のパーティションがある場合は、信頼された領域のチェーンに重ねることができます。ただし、LDAP Services for eDirectory 8.8 では、すべての信頼されていないパーティションは連続していなければならない、ローカルレプリカがそれを保持している必要があります。

## 参照データを指定する

操作が信頼されていない領域で実行されていることが検出されると、LDAP サーバは参照をクライアントに返すのに使用する情報を探します。この参照情報は、次のいずれかになります。

- ◆ 信頼されていない領域のいずれか、またはすべてのエントリにある情報
- ◆ サーバの設定データを持つ LDAP サーバまたは LDAP グループオブジェクト上の、デフォルト参照として指定された情報

信頼されていない領域のエントリが持つ参照情報は、即時上方参照です。このような参照情報は、複数の値をとる ref 属性から構成されています。(この属性の詳細については、RFC 3296 (<http://www.ietf.org/rfc/rfc3296.txt>) を参照してください。) デフォルト参照設定が持つ参照情報は上方参照で、値を 1 つとります。(X.501 の immSupr および suprDSE タイプを参照してください。)

参照データは LDAP URL の形式で保持されますが、これにはホストと (オプションで) 参照先の DSA のポートだけしか指定されていません。この参照データの例は次のようになります。

```
ldap://ldap.digital_airlines.com:389
```

LDAP サーバは操作のベース DN(見つからない場合は一致した DN) を参照します。ベース DN に参照情報が含まれる場合、LDAP サーバはその情報を参照先として返します。

参照情報が見つからない場合、LDAP サーバはツリーの上方向に向かって参照情報を探します。すべてのエントリを検索しても参照情報が見つからない場合、LDAP サーバは上方参照を返します。(この参照先は、LDAP グループまたは LDAP サーバオブジェクト上のデフォルト参照設定にあります。)

## 即時上方参照の追加

`immediateSuperiorReference` と呼ばれる補助オブジェクトクラスを信頼されていない領域のエントリに追加することができます。この補助クラスは、1つ以上の LDAP URL とともに作成される `ref` 属性を追加します。それぞれの URL は DSA のホスト名と (オプションで) ポートを指します。

## 上方参照を追加する

これまで、LDAP グループオブジェクトは `ldapReferral` 属性を持っていました。この属性は、eDirectory ツリーの他の eDirectory サーバに参照を返すときに発生する、さまざまなフェイルオーバーの状況で使用されるデフォルトの参照先を保持していました。LDAP Services for eDirectory 8.8 では、この属性は、連結ツリーの上の方 DSA のデフォルト参照を 1 つ指定するのに使用します。

また、`ldapReferral` 属性が LDAP サーバオブジェクトに追加されました。`ldapReferral` 属性に LDAP サーバオブジェクトの値が含まれる場合、この設定により LDAP グループオブジェクトの同じ属性の値は上書きされます。この動作により、グループに属するすべての LDAP サーバに特定のデフォルト参照を設定し、1つか2つのサーバのデフォルト参照を別のデフォルトで上書きすることができます。

`ldapReferral` 属性の値は、LDAP URL です。URL には、ホストと参照先の DSA のポート (オプション) が含まれます。

## LDAP で参照情報を更新する

上記のステップに従い、LDAP を使ってこのタスクを実行しても、即時上方参照を追加することはできないことが多くありました。これは、ルートパーティションが既に信頼されていないとマークされており、LDAP はパーティション内のデータに対するどのような操作の参照も送信していたためです。

信頼されていない領域の情報の更新または問い合わせを行うには、LDAP 要求に `ManageDsaIT` 制御を設定する必要があります。この制御の詳細については、[RFC 3296 \(http://www.ietf.org/rfc/rfc3296.txt\)](http://www.ietf.org/rfc/rfc3296.txt) を参照してください。この制御により、LDAP サーバは信頼されていない領域全体を信頼された領域であるかのように扱うことができます。

**注:** 上方参照機能は、LDAP でのみ利用できます。他のプロトコル (NDAP など) には、信頼属性が存在することによる影響はありません。そのため、ConsoleOne または Novell iManager を使用した信頼されていない領域のデータの参照や更新が妨害されることはありません。

## 影響を受ける操作

信頼されていない領域と上方参照は、次の LDAP 操作に影響します。

- ◆ 検索と比較
- ◆ 編集と追加

DN 構文属性値はチェックされません。そのため、グループメンバー属性は、信頼されていない領域のエントリを指す DN を含むことができます。

- ◆ 削除
- ◆ 名前の変更 (`moddn`)
- ◆ 移動 (`moddn`)

親 DN が信頼されていない領域にある場合、`affectsMultipleDSAs` エラーが返されます。

- ◆ 拡張

## 上方参照のサポートの有無を確認する

上方参照は、Novell LDAP Services for eDirectory 8.7 以降でのみサポートされています。ルート DSE の supportedFeatures 属性により、eDirectory サーバがこの機能をサポートしているかどうかを確認できます。supportedFeatures 属性の値が OID 2.16.840.1.113719.1.27.99.1 である場合は、この機能はサポートされています。その他のルート DSE オブジェクトに対する確認方法では、次が変更されています。

- ◆ namingContexts

この属性は、サーバが信頼されているローカル DSA に保持されるパーティションルートだけを表示します。信頼されていないパーティションルートは表示されません。

- ◆ altServer

この属性は、ローカルサーバと信頼されていないパーティションだけを共有する他の eDirectory サーバを表示しません。

- ◆ superiorReference

この属性は、DSA の上方参照を通知します。この値は、LDAP サーバまたは LDAP グループオブジェクト上の ldapReferral 属性を更新することにより管理されます。

## 持続的検索 : eDirectory イベントの設定

Novell eDirectory では、ディレクトリ内で重大なイベントが発生したときにアプリケーションに通知するためのイベントサービスが用意されています。これには、ディレクトリサービスに関する一般イベントも含まれます。それ以外は eDirectory とその機能に固有のイベントです。

eDirectory イベントは、LDAP プロトコルに対して、次の 2 つの異なる拡張を通してアプリケーションに通知されます。

- ◆ 持続的検索制御の実装

Novell eDirectory の持続的検索機能は、最初の一致するエントリが返された後も続行される検索操作です。持続的検索は LDAP v3 の検索操作が拡張されたもので、クライアントからサーバへの検索結果内で更新をチェックする作業が不要になります。持続的検索制御により、クライアントは、ベース DN、検索スコープ、検索フィルタなどを指定する通常の LDAP 検索操作を実行することができます。その後、サーバは最後に SearchResultDone メッセージを返すのではなく、操作による接続が維持されます。このため、クライアントは検索結果に含まれるのエントリが変更されるたびに、最新のエントリを受け取ることができます。これにより、更新が発生するたびにクライアントは目的のエントリのキャッシュを維持したり、何らかのロジックをトリガすることができます。

この拡張についての詳細は、“Persistent Search” document on the Internet (<http://www.ietf.org/proceedings/01mar/I-D/ldapext-psearch-03.txt>) を参照してください。

- ◆ イベントの監視 (eDirectory 独自の拡張 LDAP 操作)



eDirectory イベントサービスを使用するアプリケーションは、ディレクトリに対する大きな計算負荷となることがあります。そこで、さまざまな属性パラメータを使用して、個々の eDirectory サーバにおけるイベントサービスの使用を制御することができます。これらのパラメータは LDAP サーバオブジェクト上に格納されます。パラメータを設定するには、ConsoleOne または Novell iManager を使用します。

イベントサービスを使用する特定のアプリケーションにより、これらのパラメータを特定の値に指定するよう要求される場合があります。特定のアプリケーション独自の要求は、そのアプリケーションのマニュアルに示されています。

詳細は、[Understanding and Using Persistent Search in Novell eDirectory](http://developer.novell.com/research/appnotes/2003/february/04/a030204.htm) (<http://developer.novell.com/research/appnotes/2003/february/04/a030204.htm>) を参照してください。

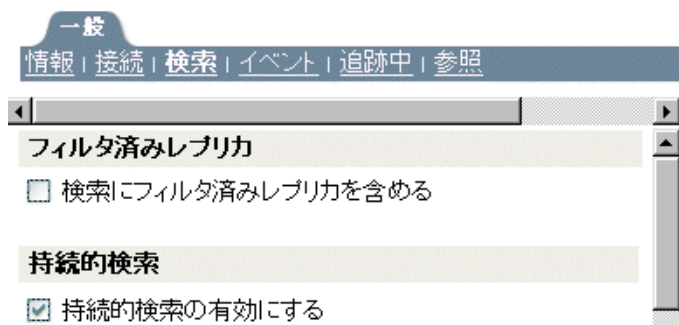
## 持続的検索の管理

Novell iManager を使用すると、持続的検索を表示または編集することができます。

- 1 Novell iManager で、[役割およびタスク] ボタン  をクリックします。
- 2 [eDirectory 管理] > [オブジェクトの変更] の順にクリックします。
- 3 変更する LDAP サーバオブジェクトの名前とコンテキストを入力するか、 をクリックし、LDAP サーバオブジェクトを参照または検索します。



- 4 [OK] をクリックし、[全般] タブの [検索] をクリックします。



- 5 持続的検索を有効にします。  
[持続的検索の有効化] チェックボックスはデフォルトでオンになっています。このサーバの持続的検索を無効にして禁止するには、チェックボックスをオフにします。  
**注:** 以前に確立された持続的検索操作を無効にすると、このオプションを無効にしてサーバをリフレッシュした後も操作が継続する場合があります。
- 6 このサーバ上の同時持続的検索の数を制御します。  
[最大同時持続的検索数] フィールドの値を指定します。0 を指定すると、同時持続的検索数は無制限になります。

### 持続的検索

- 持続的検索の有効にする
  - 最大同時持続的検索数:  操作(0=無制限)
  - 持続的検索動作の監視時にサイズと時間制限を無視する


- 7 サイズおよび時間の制限を無視するかどうかを制御します。

持続的検索要求が最初の検索結果を送信した後で、サイズおよび時間制限を無視するかどうかを指定するには、[持続的検索動作の監視時にサイズと時間制限を無視する] チェックボックスをオンにします。

このオプションを選択しない場合、すべての持続的検索操作は検索制限の制約を受けます。サイズと時間のいずれかの制限に達した場合、検索操作は失敗し、該当するエラーメッセージが返されます。

- 8 [適用] をクリックし、[OK] をクリックします。

## イベントの監視拡張操作の使用を制御する

- 1 Novell iManager で、[役割およびタスク] ボタン  をクリックします。
- 2 [LDAP] > [LDAP の概要] の順にクリックします。
- 3 [LDAP サーバの表示] をクリックし、LDAP サーバの名前をクリックします。
- 4 [イベント] をクリックします。



- 動作監視の有効化  
最大動作監視負荷  操作(0=無制限)

- 5 クライアントアプリケーションがこの LDAP サーバ上でイベントを監視できるかどうかを制御します。

クライアントアプリケーションがこの LDAP サーバ上でイベントを監視できるようにするには、[動作監視の有効化] チェックボックスをオンにします。

イベントの監視を無効にするには、チェックボックスをオフにします。

- 6 イベント 監視アプリケーションがサーバ上に置くことのできる最大負荷を制御します。

[最大動作監視負荷] フィールドに値を入力します。

イベントデータの処理と、監視対象アプリケーションへのイベント通知の送信は、LDAP サーバに対して計算負荷となります。あるイベントによるサーバへの正確な負荷は、監視されるイベントの頻度、イベントに関係したデータ、およびそのイベントを監視しているクライアントアプリケーションの数によって決まります。

[最大動作監視負荷] は、イベント監視拡張がサーバにかけることができる負荷の大きさを示す相対値です。0 を指定すると、無制限になります。この属性の適切な値を見つけるには、実際にいろいろな値を試してみてください。

- 7 [適用] をクリックし、[OK] をクリックします。

## LDAP サーバの情報を取得する

LDAP サーバについての情報を取得するには、ICE か LDAP 検索を使用します。これらのユーティリティは rootDSE (ディレクトリサービスエージェント、固有エン트리) から情報を要求します。

RootDSE は、ディレクトリツリーの擬似オブジェクトです。このオブジェクトは、ツリーのルートにある名前のないエン트리です。RootDSE は接続しているサーバに固有の情報を持っています。たとえば、rootDSE はスキーマと、スキーマがサポートする拡張およびコントロールの場所の情報を持っています。

rootDSE はツリー内の名前のないエン트리であるため、通常、LDAP サーバは検索操作で rootDSE をクライアントに返しませんが、

次の表は、rootDSE から得られる情報を表示したものです。

| 情報と説明   | 引用  |
|---|---|
| スキーマの場所 : LDAP サーバまたはツリーのスキーマの場所は、subschemaSubentry を読み込むことによって検索できます。eDirectory では、cn=schema が検索のベースになります。   | subschemaSubentry: cn=schema  |
| サポートされている拡張 : 拡張により、コンテキストの作成、マージ、新しいレプリカの追加、LDAP サーバのリフレッシュ、レプリカの削除、レプリカタイプのマスターから読み取り / 書き込みまたは読み取り専用への変更などのサーバの管理、および個別情報の管理ができます。   | supportedExtension: 2.16.840.1.113719.1.27.100.12<br>supportedExtension: 2.16.840.1.113719.1.27.100.7<br>supportedExtension: 2.16.840.1.113719.1.27.100.8 |
| 拡張の形式は ASN.1OID です。拡張の詳細については、 <a href="http://developer.novell.com/ndk/doc/ldapover/ldap_enu/data/a6ik7oi.html">LDAP Extensions (http://developer.novell.com/ndk/doc/ldapover/ldap_enu/data/a6ik7oi.html)</a> を参照してください。 |   |
| LDAP サーバを提供しているベンダ  | vendorName: Novell, Inc.  |
| LDAP サーバがサポートしているディレクトリバージョン  | vendorVersion: eDirectory v8.7.0 (10410.29)   |
| eDirectory が実行しているバージョン   | vendorVersion: eDirectory v8.7.0 (10410.29)   |
| ディレクトリサーバ名とディレクトリツリー名   | dsaname: cn=WestWindNDS,o=westwind<br>directoryTreeName: t=WESTWINDTREE   |
| サポートされている SASL メカニズム  | supported SASLMechanisms: EXTERNAL<br>supported SASLMechanisms: DIGEST-MD5<br>supported SASLMechanisms: NMAS LOGIN  |
| サポートされている LDAP サーバのバージョン  | supportedLDAPVersion: 2<br>supportedLDAPVersion: 3  |
| サーバ統計情報 : RootDSE は LDAP サーバに関するさまざまな統計情報を提供します (強力な認証バインド数など)。   | エラー : 0<br>securityErrors: 0<br>chainings: 3<br>referralsReturned: 6<br>extendedOps: 0<br>abandonOps: 0<br>wholeSubtreeSearchOps: 1                       |



rootDSE の情報は、アプリケーション開発に活用することができます。

**シナリオ：アプリケーションを開発する** — あるユーザが新しいレプリカを作成するアプリケーションを作成しています。rootDSE を読み込むと、リストに supportedExtension: 2.16.840.1.113719.1.27.100.7 と記述されています。これにより、サーバが新しいレプリカを作成するコールをサポートすることがわかります。

また、Novell iManager は rootDSE で利用できる機能をチェックし、その情報に従って動作します。

rootDSE を検索するには、ワークステーションで次を入力します。

```
ldapsearch -h ホスト名 -p 389 -b "" -s base "objectclass=*"
```

この検索は、ldap\_search API を使用したどのアプリケーションでも実行することができます。

検索のベースは NULL で、フィルタは objectclass=\* に設定されています。(このクライアントの場合、ベースは -b です。)

rootDSE の読み取り方法の詳細については、次のいずれかを参照してください。

- ◆ [LDAP Libraries for C \(http://developer.novell.com/ndk/doc/cldap/ldaplibc/data/hevgtl7k.html\)](http://developer.novell.com/ndk/doc/cldap/ldaplibc/data/hevgtl7k.html)
- ◆ [LDAP Classes for Java \(http://developer.novell.com/ndk/doc/jldap/jldapenu/data/hevgtl7k.html\)](http://developer.novell.com/ndk/doc/jldap/jldapenu/data/hevgtl7k.html)

LDAP 検索フィルタの詳細については、[LDAP Search Filters \(http://developer.novell.com/ndk/doc/ldapover/ldap\\_enu/data/a3saoeg.html\)](http://developer.novell.com/ndk/doc/ldapover/ldap_enu/data/a3saoeg.html) を参照してください。このセクションは、NDK マニュアルの「LDAP and NDS Integration」にあります。





# 14 Novell eDirectory のバックアップと復元

Novell® eDirectory™ には、レプリカ作成による障害対策機能が組み込まれています。eDirectory ツリーに属するサーバに障害があっても、別のサーバがサービスを続行できます。この意味でレプリカ作成機能は、最も重要な保護機能と位置づけられています。

ただし 1 台だけのサーバで運用している環境では、レプリカ作成は不可能です。また、レプリカを作成していても、完全に復元するのは困難な場合もあります。ハードウェア障害など、機器が破損したときや、火事や水害で何台ものサーバが動かなくなってしまう場合などです。各サーバの eDirectory をバックアップしておけば、ネットワークの耐障害性を高めることになります。

eDirectory 8.7 には、Backup eMTool という新しいバックアップ / 復元ユーティリティが付属するようになりました。これを使用すると、サーバ単位で eDirectory データベースをバックアップすることができます。これには次のような利点があります。

- **どのプラットフォームでも同じツールで操作可能。**
- **稼動中でもバックアップ可能。** eDirectory データベースを停止することなく、そのまま完全なバックアップを取ることができます。
- **個々のサーバ単位に、迅速な復元処理が可能。** ハードウェア障害からの復元には特に有用です。
- **高い拡張性。** 数千万から数億単位のオブジェクトを保持した eDirectory データベースを持つサーバでもバックアップ可能です。バックアップの処理速度は主として I/O チャンネルの帯域幅で決まります。
- **レプリカ作成機能と DSMASTER サーバを組み合わせれば、ツリー全体の復元も容易。** DSMASTER サーバを設定していない場合でも、かなりの程度まで復元できます。402 ページの「**DSMASTER サーバによる災害対策**」を参照してください。
- **リモート操作が可能。** バックアップ / 復元処理のほとんどは、iManager を使って、Web ブラウザ画面から実行可能です。ファイアウォールの内側からでも外側からでも構いません。高度な処理は、コマンドラインから実行する Java クライアントである、eMBox Client を使い、リモート操作で実行できます。ファイアウォール越しにでも、あるいは VPN 経由でも操作できます。
- **関連ファイルもバックアップ可能。** データベース以外の関連ファイルも組にしてバックアップできます。NICI セキュリティファイル、ストリームファイル、インクルードファイルで指定したファイル (autoexec.ncf など) が対象になります。
- **サーバの停止直前の状態に eDirectory を復元可能。** ただしロールフォワードログを継続的に保存していることが条件です。405 ページの「**ロールフォワードログを使用する**」を参照してください。
- **ハードウェアのアップグレードを単純化。** eDirectory データベースのコールドバックアップを取り、新しいサーバに復元して、サーバの識別情報を簡単に新ハードウェアに移行できます。RAM のアップグレードなど、機器構成を変える際の安全措置としても有効です。536 ページの「**ハードウェアのアップグレードやサーバの交換**」を参照してください。

- ◆ **分散環境での運用を考慮。** ロールフォワードログがあれば、ツリー内の他のサーバと完全に同期した状態にまで復元できます。
- ◆ **無人でのバックアップが可能。** バッチファイルを作成して、eMBox Client を使用して無人でバックアップを実行できます。

新しい eDirectory バックアップツールである Backup eMTools には、個々のサーバ単位でデータベースおよび関連ファイルのバックアップを取り、復元するために必要な機能がすべて揃っています。個々のオブジェクトやツリーの一部を単位としてバックアップ/復元することはできません。

システムバックアップ機能と組み合わせれば、eDirectory バックアップファイルをテープに保存して安全を期すことができます。

この章では、次のトピックについて説明します。

- ◆ [390 ページの「eDirectory のバックアップ処理に関する確認事項」](#)
- ◆ [393 ページの「バックアップサービスおよび復元サービスについて」](#)
- ◆ [405 ページの「ロールフォワードログを使用する」](#)
- ◆ [409 ページの「復元処理の準備」](#)
- ◆ [412 ページの「Novell iManager を使ったバックアップ / 復元作業」](#)
- ◆ [420 ページの「eMBox クライアントを使ったバックアップ / 復元作業」](#)
- ◆ [438 ページの「NetWare で DSBK.NLM を使用する」](#)
- ◆ [438 ページの「サーバ固有情報のバックアップに関する変更事項 \(NetWare のみ\)」](#)
- ◆ [440 ページの「復元後の検証処理に失敗した場合の対処方法」](#)
- ◆ [444 ページの「バックアップ / 復元の運用例」](#)
- ◆ [451 ページの「NICI のバックアップと復元」](#)

## eDirectory のバックアップ処理に関する確認事項

**複数サーバ構成のツリーで、サーバが停止していてもオブジェクトにアクセスできるようにする**

- 複数サーバ構成のツリーでは、障害対策のため、すべての eDirectory パーティションについて、複数台のサーバにレプリカが作成されていることを確認します。

レプリカの作成については、[140 ページの「レプリカを追加する」](#)を参照してください。

**個々のサーバについて、ハードウェア障害などの場合に、迅速に完全復元できるようにするための準備**

- 定期的に (週1回など) eDirectory データベースのフルバックアップを取ってください。
- 定期的に (毎晩など) インクリメンタルバックアップを取ってください。
- eDirectory のフル / インクリメンタルバックアップ終了後、すぐにファイルシステムをテープにフル / インクリメンタルバックアップしてください。

Backup eMTool は、サーバ上の指定したディレクトリにバックアップファイルを作成しますが、これを直接テープに保存する機能はありません。したがって、eDirectory のバックアップ処理後すぐにファイルシステムのバックアップを行い、安全な記録媒体であるテープに保存する必要があります。

- 必要に応じて、ロールフォワードログを残すよう設定してください。

レプリカリングに属するサーバは、ロールフォワードログ機能を有効にしておく必要があります。バックアップファイルがあっても、ロールフォワードログがなければ復元後の検証処理に失敗し、データベースを開けないこととなります。他のサーバとレプリカを共有するデータベースは、停止直前の状態にまで復元しない限りデフォルトではオープンされません。

単一サーバ環境では、ロールフォワードログがなくても復元後の検証に失敗することはありませんが、最後にバックアップを取った時の状態にしか戻りません。ロールフォワードログがあれば、システム停止直前の状態まで復元できます。

ロールフォワードログ機能を使う際の主な注意点は次のとおりです。詳細については、[405 ページの「ロールフォワードログを使用する」](#)を参照してください。

- ◆ ロールフォワードログの保存先を指定してください。初期設定を使用することはお勧めしません。

ログはサーバ上のローカルファイルとして保存する必要があります。障害対策上、eDirectory と同じディスクパーティション/ボリューム、同じ記憶デバイスは避けてください。ロールフォワードログ専用の、独立したパーティション/ボリュームを用意するとよいでしょう。

- ◆ ロールフォワードログの保存先を文書に記録しておき、障害時にはすぐわかるようにしてください。

サーバが正常に動作していれば、iManager のバックアップ環境設定画面、または eMBox Client の `getconfig` オプションで調べることができます。ただしハードウェア障害などで eDirectory が使えない状態になると、この方法でロールフォワードログの場所を調べることはできません。

- ◆ ロールフォワードログを保存しているディスクパーティション/ボリュームの空き容量を監視し、容量不足にならないようにしてください。

容量不足のためロールフォワードログが作成できなくなると、eDirectory は応答しなくなります。

- ◆ ロールフォワードログの保存先にアクセスできるユーザを制限し、権利のないユーザがログを参照できないようにしてください。

- ◆ 復元が必要となったときは、復元処理の終了後、そのサーバのロールフォワードログ設定をやり直してください。復元処理の過程で、設定が初期状態に戻るためです。ロールフォワードログを有効にしてから、改めてフルバックアップも取る必要があります。

- NICI 機能を使用している場合は、NICI セキュリティファイルもバックアップの対象として設定してください。

このファイルがないと暗号化キーを復元できないため、暗号化されたデータを読むことができなくなります。NICI セキュリティの詳細については、『[NICI Administration Guide](http://www.novell.com/documentation/beta/nici27x/index.html)』 (<http://www.novell.com/documentation/beta/nici27x/index.html>) と [TID on backing up NICI files](http://support.novell.com/cgi-bin/search/searchtid.cgi?/10098087.htm) (<http://support.novell.com/cgi-bin/search/searchtid.cgi?/10098087.htm>) を参照してください。

- 複数サーバ構成のツリーの場合、バックアップ処理に Backup eMTool を使うためには、レプリカを共有するサーバすべてを eDirectory 8.5 以降にアップグレードする必要があります。

8.5 より前の eDirectory とは、復元後の検証処理の互換性がないためです。復元検証処理の詳細については、[396 ページの「Backup eMTool による復元作業の概要」](#) および [403 ページの「復元後の検証については eDirectory 8.5 以降のみで互換性がある」](#) を参照してください。

- ❑ (NetWare® のみ) 404 ページの「NetWare のファイルシステムデータを復元する際のアクセス権の保存」を参照して、ファイルシステム上のアクセス権についても確認してください。起こりうる問題についてはあらかじめ確認し、必要に応じて予防措置を取ってください。
- ❑ 定期的にバックアップログを調べて、無人でのバックアップが正常に実行されていることを確認してください。
- ❑ サーバをアップグレードする際は、536 ページの「ハードウェアのアップグレードやサーバの交換」を参照してコールドバックアップを取ってください。
- ❑ 複数サーバ構成のツリーでは、障害対策のため、すべての eDirectory パーティションについて、複数台のサーバにレプリカが作成されていることを確認します。

パーティションのレプリカを作成しておけば、保守作業などのためサーバを停止している間もオブジェクトにアクセスできるばかりでなく、ハードウェア障害などでサーバが使えなくなった場合に備える障害対策としても役立ちます。逆に複数サーバ構成のツリーでレプリカを作成していないパーティションを保持するサーバがあると、障害時にパーティションを復元できない恐れがあります。したがって最善なのは、すべてのパーティションについてレプリカを作成しておくことです。複数サーバ構成のツリー内にレプリカを作成していないパーティションがある場合の問題点の詳細については、396 ページの「Backup eMTool による復元作業の概要」、405 ページの「ロールフォワードログを使用する」および 440 ページの「復元後の検証処理に失敗した場合の対処方法」を参照してください。

レプリカの作成については、52 ページの「レプリカ」および 135 ページの「パーティションおよびレプリカの管理」を参照してください。

- ❑ eDirectory および関連ファイルのバックアップを収めたテープは、安全な場所に保管するようにしてください。
- ❑ バックアップ計画が適切であるか、定期的に検証するようにしてください。
- ❑ (オプション) コールドバックアップ (データベースをクローズしてフルバックアップを取る作業) や高度なバックアップ / 復元操作をリモート操作で実行する場合は、リモート側コンピュータに eMBox Client をインストールしてください。また、VPN を使用するなど、ファイアウォール越しにアクセスできるように設定する必要があります。

iManager を使用すればファイアウォールの外側からでも作業が可能ですが、コールドバックアップや高度な操作はサポートされていません。

eMBox Client は、eDirectory をインストールする際、同時にインストールされます。Sun JVM 1.3.1 が動作するワークステーション上でも使えます。eMBox Client のインストールや設定の手順については、555 ページの「eMBox コマンドラインクライアントの使用」を参照してください。

#### 災害により何台ものサーバが被害を受けた場合に備える準備

- ❑ 上述の対策はすべて実施してください。
- ❑ 複数サーバ構成のツリーであれば、障害対策のために DSMASTER サーバを用意するようお勧めします。  
402 ページの「DSMASTER サーバによる災害対策」を参照してください。
- ❑ 災害からの復旧計画が適切であるか、定期的に検証するようにしてください。

## バックアップサービスおよび復元サービスについて

- ◆ 393 ページの「eDirectory Backup eMTool について」
- ◆ 394 ページの「eDirectory 8.7.3 のバックアップ / 復元機能で変更された事項」
- ◆ 396 ページの「Backup eMTool による復元作業の概要」
- ◆ 397 ページの「バックアップファイルのヘッダ書式」
- ◆ 401 ページの「バックアップログファイルの書式」
- ◆ 402 ページの「DSMASTER サーバによる災害対策」
- ◆ 403 ページの「遷移ベクトルと復元後の検証処理」
- ◆ 403 ページの「復元後の検証については eDirectory 8.5 以降のみで互換性がある」
- ◆ 404 ページの「NetWare のファイルシステムデータを復元する際のアクセス権の保存」

### eDirectory Backup eMTool について

Backup eMTool には、個々のサーバ単位で、稼動したままの状態継続的に eDirectory データベースのバックアップを取る機能があります。データベースを停止することなく、処理を始めた時点のバックアップを取ることができます。つまり、バックアップ作業はいつでも可能であり、その間も eDirectory を使い続けることができます (特に指示しなければこの「ホット」バックアップになりますが、必要であればデータベースを停止して「コールド」バックアップを取ることも可能です)。

また、ロールフォワードログを有効にすれば、最後にバックアップを取った時点以降のトランザクションをすべて記録しておけます。これを使えば、サーバが停止する直前の状態に復元することもできます。さらに、レプリカリングに属するサーバすべてについてロールフォワードログを取る必要があります。これにより、他のサーバとの同期状態も復元できます。バックアップファイルがあっても、ロールフォワードログがなければ復元後の検証処理に失敗し、データベースを開けないこととなります。ロールフォワードログの機能は、デフォルトでは無効になっています。詳細については、405 ページの「ロールフォワードログを使用する」を参照してください。

新しいバックアップツールである Backup eMTool も、eDirectory のオブジェクトをすべて一度にバックアップできるわけではありません。各サーバのパーティションが単位となります。この方式は、特定のサーバのみを復元する場合に優れているばかりでなく、TSA for NDS<sup>®</sup> を使う旧式の方法に比べて高速です。ただし、eDirectory 8.6 のマニュアルにも記載されているように、TSA for NDS は今でも使用できます。必要に応じて TSA for NDS と Backup eMTool を使い分けられます。動作の違いについては、394 ページの「eDirectory 8.7.3 のバックアップ / 復元機能で変更された事項」を参照してください。

eDirectory の新しいバックアップツールは、システムバックアップ機能と組み合わせて使用して、eDirectory バックアップファイルをテープに安全に保存する必要があります。Novell はバックアップ用製品を開発している主要企業と提携しています。一覧については、[NetWare Partner Products: Backup, Restore, & Recovery \(http://www.novell.com/partnerguides/p100004.html\)](http://www.novell.com/partnerguides/p100004.html) を参照してください。

NetWare の場合、このバックアップツールを使うためには、ファイルシステムに対する適切なアクセス権が必要です。詳細については、404 ページの「NetWare のファイルシステムデータを復元する際のアクセス権の保存」を参照してください。



iManager からは、コールドバックアップ、無人バックアップ、高度な復元機能を除くバックアップ/復元機能を実行できます。詳しくは [412 ページの「Novell iManager を使ったバックアップ/復元作業」](#) を参照してください。一方、eMBox Java コマンドラインクライアントからは、無人バックアップを含め、どんなバックアップ/復元作業でも実行できます。詳しくは [420 ページの「eMBox クライアントを使ったバックアップ/復元作業」](#) を参照してください。

iManager から実行できるバックアップ/復元オプションについては、オンラインヘルプを参照してください。eMBox Client から実行できる機能については、[431 ページの「バックアップ/復元のコマンドラインオプション」](#) を参照してください。

復元の具体的な処理過程については、[396 ページの「Backup eMTool による復元作業の概要」](#) を参照してください。

eDirectory Backup eMTool は、eMBox ツールのひとつです。eMBox は、eDirectory を構成する一部としてサーバにインストールされるサービスです。

Backup eMTool は次のファイルから成ります。

| ファイル名           | 説明   |
|-----------------|--|
| backupcr        | バックアップ/復元機能をすべて含むコアライブラリ。<br>ユーザインタフェースはなく、backuptl プログラムから動的にロード、リンクされる形で動作します。   |
| backuptl        | backupcr ライブラリを呼び出す eMTool のインタフェース部分。eMBox アーキテクチャを介してバックアップ/復元機能を提供するプログラムです。<br>iManager プラグイン、eMBox Client、Java コマンドラインクライアントを介して使用できます。 |
| dsbackup_en.xlf | Backup eMTool で表示されるメッセージの言語ファイルです。  |

Backup eMTool で作成されるバックアップファイルやログファイルの形式については、[401 ページの「バックアップログファイルの書式」](#) および [397 ページの「バックアップファイルのヘッダ書式」](#) を参照してください。

**重要:** 復元後の検証処理については、8.5 より前の eDirectory とは互換性がありません。レプリカリングに属するサーバで新しいバックアップ/復元ツールを使う場合は、これに属するサーバすべてを eDirectory 8.5 以降にアップグレードする必要があります ([403 ページの「復元後の検証については eDirectory 8.5 以降のみで互換性がある」](#) も参照してください)。

## eDirectory 8.7.3 のバックアップ/復元機能で変更された事項

eDirectory の以前のバージョンでは、バックアップ/復元ツールは、ツリーをオブジェクト単位でバックアップする方式を使用していました。

eDirectory 8.7 で組み込まれた Backup eMTool は、方式やアーキテクチャが一新されています。すなわち、ツリーではなくサーバを単位とし、個々のサーバの eDirectory データベースをバックアップする、という方式になったのです。この変更により、以前の TSA for NDS よりもバックアップ処理速度が大幅に改善されました。

TSA for NDS は今でも使用できますが、今後は新しいバックアップツールを使うようお勧めします。

サーバ固有の情報も Backup eMTool でバックアップできます。[438 ページの「サーバ固有情報のバックアップに関する変更事項 \(NetWare のみ\)」](#) を参照してください。

新旧バックアップツールの違いを次の表に示します。

| 項目                    | TSA for NDS による以前のバックアップ  | Backup eMTool による「ホットバックアップ」  |
|-----------------------|---|---|
| バックアップの対象             | ツリー全体をオブジェクト単位でバックアップ。<br><br>旧バックアップツール ( 必要ならば 8.7 でも利用可能 ) の詳細については、『Novell eDirectory 8.6 管理ガイド』の「Novell eDirectory のバックアップと復元」( <a href="http://www.novell.com/documentation/lg/ndsedir86/taoenu/data/a2n4mb6.html">http://www.novell.com/documentation/lg/ndsedir86/taoenu/data/a2n4mb6.html</a> ) を参照してください。 | サーバ単位で eDirectory データベースをバックアップ。<br><br>ツリー全体の耐障害性は主としてレプリカ作成機能で確保していますが、サーバ単位のバックアップ機能によりさらに強固になります。<br><br>災害などで何台ものサーバが停止した場合でもツリーを復元できるようにするためには、DSMASTER サーバを導入し、それに応じたレプリカ作成方針を立てる必要があります。 <b>402 ページの「DSMASTER サーバによる災害対策」</b> を参照してください。            |
| 処理速度                  | -   | 大幅に改善されています。新規バックアップツールの開発に当たっては、処理性能を最重視しました。  |
| バックアップファイルの保存先        | 直接テープに書き出し可。  | ファイルシステム上のバックアップファイルとして書き出し。<br><br>別途ファイルシステムのバックアップツールを使って、テープに書き出す必要があります。   |
| プラットフォーム間の違い          | プラットフォームによって使い方が別々。   | どのプラットフォームでも同じ使い方。  |
| 個々のサーバ単位での復元          | 考慮されていません。  | サーバ単位での復元処理が可能。ハードディスク障害時のほか、サーバ機を移行する際にも利用できます。<br><br>ロールフォワードログを使えば、停止直前の状態に復元することも可能です。これにより、レプリカリングに属する他のサーバと同期状態を揃えることができます。<br><br>eDirectory の関連ファイルもバックアップの対象とすることができます。たとえば NICI ファイルのバックアップと復元ができます。独自の関連ファイルリストを作成して、対象ファイルをバックアップに追加することもできます。 |
| NICI ファイルのバックアップ / 復元 | 考慮されていません。  | NICI ファイルのバックアップ / 復元も可能です。これにより、復元後、暗号化データにアクセスできます。復元作業の時間を大幅に短縮できるでしょう。  |
| 個々のサーバのロールフォワードログ     | 考慮されていません。  | 最後にバックアップを取った時点以降のトランザクションを、ロールフォワードログとしてすべて記録しておけます。これを使うと、停止直前の状態にまで復元することができます。複数サーバ環境では、これを使用して他のサーバと同期状態を揃えることができます。ロールフォワードログの機能は、デフォルトでは無効になっています。詳細については、 <b>405 ページの「ロールフォワードログを使用する」</b> を参照してください。   |

## Backup eMTool による復元作業の概要

復元作業に先立ち、バックアップファイルをすべて揃えておく必要があります。その手順については [409 ページの「復元処理の準備」](#) を参照してください。iManager や eMBox Client から Backup eMTool の復元機能呼び出すと、Backup eMTool で次のような処理が行われます。

1. DS エージェントをクローズします。
2. アクティブな DIB (Data Information Base) セットを、NDS から RST に切り替えます。  
既存の NDS データベースはそのままサーバに残り、復元後の検証に失敗した場合は、再びこれがアクティブな DIB セットになります。
3. 復元処理が始まります。新たに RST という DIB セットを作り、そこに復元します。
4. DIB セットをいったん無効にします。

擬似サーバのログイン無効属性をオンにします。これは、この DIB セットを使って DS エージェントがオープンされるのを避けるための措置です。

5. ロールフォワードログに関する設定をデフォルトに戻します。

したがって、復元後はロールフォワードログを書き出さない設定になります。書き出し先ファイル名の設定もデフォルトに戻ります。

このサーバでロールフォワードログ機能を使うためには、復元後に改めて有効に切り替え、障害対策のための書き出し先も設定し直して、ロールフォワードログの環境設定を再作成する必要があります。ロールフォワードログを有効にしてから、改めてフルバックアップも取る必要があります。

6. 復元された RST データベースの検証処理を行います。

復元されたデータの整合性を確認します。この確認は、レプリカを共有しているすべてのサーバにアクセスし、遷移ベクトルを比較して実行されます。

検証結果はログファイルに出力されます。

リモートサーバの遷移ベクトルの方がローカルベクトルより後の時間に作成されたものである場合は、復元されなかったデータがあるということなので、検証処理は失敗します。

あるレプリカの検証処理に失敗した場合、ログにはたとえば次のように出力されます。遷移ベクトルを比較している様子がわかります。

```
Server: ¥T=LONE_RANGER¥O=novell¥CN=CHIP
  Replica: ¥T=LONE_RANGER¥O=novell
    Status: ERROR = -6034
      Local TV          Remote TV
      s3D35F377 r02 e002  s3D35F3C4 r02 e002
      s3D35F370 r01 e001  s3D35F370 r01 e001
      s3D35F363 r03 e001  s3D35F363 r03 e001
      s3D35F31E r04 e004  s3D35F372 r04 e002
      s3D35F2EE r05 e001  s3D35F2EE r05 e001
      s3D35F365 r06 e003  s3D35F365 r06 e003
```

詳細については、[403 ページの「遷移ベクトルと復元後の検証処理」](#) を参照してください。



7. 検証に成功した場合は、RST を NDS と改名し、ログイン無効属性をオフにします。したがってこれがサーバでアクティブな eDirectory データベースになります。失敗した場合は改名しないので、元の NDS が再びアクティブな DIB セットになります。

検証に失敗した場合の復旧方法については、[440 ページの「復元後の検証処理に失敗した場合の対処方法」](#)を参照してください。高度な復元オプションを使えば、強制的に RST データベースをアクティブにし、ロックを解除することもできますが、Novell の担当者の指示がない場合はお勧めできません。

## バックアップファイルのヘッダ書式

バックアップファイルのヘッダには、次のような重要な情報が記録されています。

- ◆ バックアップファイルが作成された時点のファイル名。  
バックアップ作成後にファイル名を変更した場合にはこの情報が有用になります。
- ◆ バックアップ時点のロールフォワードログ名。  
フルバックアップと 3 回分のインクリメンタルバックアップというように複数のファイルがある場合、最後のバックアップファイルに記載されたロールフォワードログ名が重要です。バックアップファイルからの復元処理後、どのロールフォワードログから適用するかを確認するために使用されるからです。
- ◆ このサーバが保持しているレプリカのリスト。  
各レプリカをどのサーバに配置しているか記録していない場合に役立ちます。災害で何台ものサーバが停止した場合、バックアップファイルのヘッダに表示されたこの情報を見れば、最初にどのサーバを復元すべきか判断できます。
- ◆ 同時にバックアップするようユーザのインクルードファイルに指定された関連ファイル名。
- ◆ 複数のファイルに分割してバックアップする場合のファイル数。

各バックアップファイルのヘッダは XML 形式で記述されます。ヘッダ部に続き、データベース内のデータを、バイナリ形式で記録します (ファイルの末尾にバイナリデータがあると構文解析でエラーが発生しますが、XML ヘッダは XML 標準に適合しています)。バックアップが複数のファイルに分かれる場合、各ファイルに同じヘッダ情報を記録します。

**警告:** バックアップファイルを開く場合でもヘッダを確認するだけにとどめ、保存や変更はしないようにしてください。ファイルの一部が切り捨てられてしまうことがあります。ほとんどのアプリケーションではバイナリデータを正確に保存することはできません。

XML ヘッダの DTD を次に示します (この DTD は参照のため、バックアップファイルのヘッダの一部として書き込まれます)。

```
<?xml version="1.0" encoding="UTF-8" standalone="yes" ?>
<!DOCTYPE backup [
<!ELEMENT backup (file|replica)*>
<!ELEMENT file (#PCDATA)>
<!ELEMENT replica EMPTY>
<!ATTLIST backup version CDATA #REQUIRED
  backup_type (full|incremental) #REQUIRED
  idtag CDATA #REQUIRED
  time CDATA #REQUIRED
  srvname CDATA #REQUIRED
  dsversion CDATA #REQUIRED
  compression CDATA "none"
  os CDATA #REQUIRED
```

```

current_log CDATA #REQUIRED
number_of_files CDATA #IMPLIED
backup_file CDATA #REQUIRED
incremental_file_ID CDATA #IMPLIED
next_inc_file_ID CDATA #IMPLIED>
<!ATTLIST file size CDATA #REQUIRED
name CDATA #REQUIRED
encoding CDATA "base64"
type (user|nici) #REQUIRED>
<!ATTLIST replica partition_DN CDATA #REQUIRED
modification_time CDATA #REQUIRED
replica_type (MASTER|SECONDARY|READONLY|SUBREF|
SPARSE_WRITE|SPARSE_READ|Unknown) #REQUIRED
replica_state (ON|NEW_REPLICA|DYING_REPLICA|LOCKED|
CRT_0|CRT_1|TRANSITION_ON|DEAD_REPLICA|
BEGIN_ADD|MASTER_START|MASTER_DONE|
FEDERATED|SS_0|SS_1|JS_0|JS_1|MS_0|MS_1|
Unknown) #REQUIRED>
]>

```

DTD に含まれる属性について次の表で説明します。

| 属性                         | 説明   |
|----------------------------|--|
| backup version             | バックアップツールのバージョン。   |
| backup backup_type         | フルバックアップかインクリメンタルバックアップかの別 (コールドバックアップはフルバックアップとして扱います)。   |
| backup idtag               | バックアップ時刻に基づいて生成された GUID。バックアップファイル名が変わっていても、これを使えばバックアップを識別できます。   |
| backup time                | バックアップ処理の開始日時。   |
| backup srvname             | バックアップ対象サーバの識別名。   |
| backup dsversion           | サーバ上で稼動している eDirectory のバージョン。   |
| backup compression         | Backup eMTool がバックアップデータを圧縮したかどうか。対象になるのはバックアップデータ本体だけで、ヘッダは圧縮されません。   |
| backup os                  | バックアップ処理を実行したオペレーティングシステム。復元はこれと同じオペレーティングシステムのみで行うようお勧めします。   |
| backup current_log         | 復元に必要な最初のロールフォワードログ。正しく復元するために必要な情報です。   |
| backup number_of_files     | 分割してバックアップする場合のファイル数。ひとつ目のバックアップファイルにのみ記録されます。   |
| backup backup_file         | このバックアップファイル名。<br><br>複数のファイルに分けてバックアップする場合、各ファイル名には順序番号が付きませんが、それも含むファイル名が記録されます。複数のバックアップファイルのファイル名の例は、 <b>-s ファイルサイズ</b> を参照してください。 |
| backup incremental_file_ID | インクリメンタルバックアップの場合、そのファイルの ID。  |
| backup next_inc_file_ID    | これに続くインクリメンタルバックアップに与える ID。正しく復元するために必要な情報です。  |

| 属性                        | 説明  |
|---------------------------|---|
| file size                 | このファイルの <file> タグ間にあるデータ長。  |
| file name                 | バックアップファイル名およびその保存先。  |
| file encoding             | ファイルのエンコードに使ったアルゴリズム。   |
| file type                 | これが NICI ファイルか、それ以外にユーザが指定したファイルかの別。  |
| replica partition_DN      | パーティションの識別名。<br>各レプリカをどのサーバに配置しているか記録していない場合に役立ちます。災害で何台ものサーバが停止した場合、バックアップファイルのヘッダに表示されたこの情報を見れば、最初にどのサーバを復元するべきか判断できます。 |
| replica modification_time | バックアップ時点の、このレプリカの遷移ベクトル。  |
| replica replica_type      | レプリカの種別。マスタ、読み込み専用など。   |
| replica_state             | バックアップ時点でのレプリカの状態。「On」、「New Replica」など。   |

バックアップファイルのヘッダ例を次に示します。これは Windows NT サーバで作成したもので、NICI セキュリティファイルもバックアップ対象になっています。

```
<?xml version="1.0" encoding="UTF-8" standalone="yes" ?>
<!DOCTYPE backup [
<!ELEMENT backup (file|replica)*>
<!ELEMENT file (#PCDATA)>
<!ELEMENT replica EMPTY>
<!ATTLIST backup version CDATA #REQUIRED
  backup_type (full|incremental) #REQUIRED
  idtag CDATA #REQUIRED
  time CDATA #REQUIRED
  srvname CDATA #REQUIRED
  dsversion CDATA #REQUIRED
  compression CDATA "none"
  os CDATA #REQUIRED
  current_log CDATA #REQUIRED
  number_of_files CDATA #IMPLIED
  backup_file CDATA #REQUIRED
  incremental_file_ID CDATA #IMPLIED
  next_inc_file_ID CDATA #IMPLIED>
<!ATTLIST file size CDATA #REQUIRED
  name CDATA #REQUIRED
  encoding CDATA "base64"
  type (user|nici) #REQUIRED>
<!ATTLIST replica partition_DN CDATA #REQUIRED
  modification_time CDATA #REQUIRED
  replica_type (MASTER|SECONDARY|READONLY|SUBREF|
  SPARSE_WRITE|SPARSE_READ|Unknown) #REQUIRED
  replica_state (ON|NEW_REPLICA|DYING_REPLICA|LOCKED|
  CRT_0|CRT_1|TRANSITION_ON|DEAD_REPLICA|
  BEGIN_ADD|MASTER_START|MASTER_DONE|
  FEDERATED|SS_0|SS_1|JS_0|JS_1|MS_0|MS_1|
  Unknown) #REQUIRED>
]>
```

```
<backup version="2" backup_type="full" idtag="3D611DA2" time="2002-8-19'T10:32:35" srvname="¥T=MY_TREE¥O=novell¥CN=DSUTIL-DELL-NDS"
```

```

dsversion="1041081" compression="none" os="windows"
current_log="00000003.log" next_inc_file_ID="2" number_of_files="0000001"
backup_file="c:\¥backup¥header.bak">

<replica partition_DN="¥T=MY_TREE" modification_time="s3D611D95_r1_e2"
replica_type="MASTER" replica_state="ON" />

<replica partition_DN="¥T=MY_TREE¥O=part1"
modification_time="s3D611D95_r1_e2" replica_type="MASTER" replica_state="ON"
/>

<replica partition_DN="¥T=MY_TREE¥O=part2"
modification_time="s3D611D95_r1_e2" replica_type="MASTER" replica_state="ON"
/>

<replica partition_DN="¥T=MY_TREE¥O=part3"
modification_time="s3D611D96_r1_e2" replica_type="MASTER" replica_state="ON"
/>

<file size="190" name="C:¥WINNT¥system32¥novell¥nici¥bhawkins¥XARCHIVE.001"
encoding="base64" type="nici">the data is included here</file>

<file size="4228" name="C:¥WINNT¥system32¥novell¥nici¥bhawkins¥XMGRCFG.KS2"
encoding="base64" type="nici">the data is included here</file>

<file size="168" name="C:¥WINNT¥system32¥novell¥nici¥bhawkins¥XMGRCFG.KS3"
encoding="base64" type="nici">the data is included here</file>

<file size="aaac" name="C:¥WINNT¥system32¥novell¥nici¥nicintacl.exe"
encoding="base64" type="nici">the data is included here</file>

<file size="150" name="C:¥WINNT¥system32¥novell¥nici¥NICISDI.KEY"
encoding="base64" type="nici">the data is included here
</file>

<file size="4228" name="C:¥WINNT¥system32¥novell¥nici¥system¥xmgrcfg.ks2"
encoding="base64" type="nici">the data is included here
</file>

<file size="168" name="C:¥WINNT¥system32¥novell¥nici¥system¥xmgrcfg.ks3"
encoding="base64" type="nici">the data is included here
</file>

<file size="1414" name="C:¥WINNT¥system32¥novell¥nici¥xmgrcfg.wks"
encoding="base64" type="nici">the data is included here
</file>

</backup>

```

ヘッダ部に続き、データベースのバックアップデータをバイナリ形式で格納します。

## バックアップログファイルの書式

eDirectory Backup eMTool は、前回までのバックアップを含め、処理内容を細かく記録したログを残すようになっています。このログファイルにはすべてのバックアップ履歴、バックアップの開始および終了時刻、およびバックアッププロセス中に発生した考えられるエラーについての情報が含まれます。前回までのログに追記する形で記録します。書き出し先を別途指定することもできます。

無人バックアップが正常に実行されているか確認するためにも、このログは重要です。最終行を見ると、成功か失敗かの区別およびエラーコードがわかります。

Backup eMTool のログファイルには、過去のバックアップ処理の ID も記録されています。これは復元に必要なフルバックアップ、インクリメンタルバックアップのファイルを間違いなく揃えるために役立ちます。先頭の 4 行は、バックアップファイルのヘッダ情報をそのまま複写したものです。

また、同時にバックアップしたファイル名も記録します。NICI ファイルや、インクルードファイルでユーザが指定したファイルがこれに当たります。

復元処理の際は、実際に復元されたファイルを記録します。

ログファイルの出力例を次に 2 つ示します。

```
|=====DSBackup Log: Backup=====|
Backup type: Full
Log file name: sys:/backup/backup.log
Backup started: 2002-6-21'T19:53:5GMT
Backup file name: sys:/backup/backup.bak
Server name: ¥T=VIRTUALNW_TREE¥O=novell¥CN=VIRTUALNW
Current Roll Forward Log: 00000001.log
DS Version: 1041072
Backup ID: 3D138421
Backing up security file: sys:/system/nici/INITNICI.LOG
Backing up security file: sys:/system/nici/NICISDI.KEY
Backing up security file: sys:/system/nici/XARCHIVE.000
Backing up security file: sys:/system/nici/XARCHIVE.001
Backing up security file: sys:/system/nici/XMGRCFG.KS2
Backing up security file: sys:/system/nici/XMGRCFG.KS3
Backing up security file: sys:/system/nici/XMGRCFG.NIF
Starting database backup...
Database backup finished
Completion time 00:00:03
Backup completed successfully
```

```
|=====DSBackup Log: Restore=====|
Log file name: sys:/save/doc.log
Restore started: 2002-7-19'T19:1:34GMT
Restore file name: sys:/backup/backup.bak
Starting database restore...
Restoring file sys:/backup/backup.bak
Restoring file sys:/system/nici/INITNICI.LOG
Restoring file sys:/system/nici/NICISDI.KEY
Restoring file sys:/system/nici/XARCHIVE.000
Restoring file sys:/system/nici/XARCHIVE.001
Restoring file sys:/system/nici/XMGRCFG.KS2
Restoring file sys:/system/nici/XMGRCFG.KS3
Restoring file sys:/system/nici/XMGRCFG.NIF
Database restore finished
Completion time 00:00:15
Restore completed successfully
```

## DSMASTER サーバによる災害対策

複数サーバ環境で、サーバがすべて失われてしまうような災害にも備えるためには、ツリーの一部として DSMASTER サーバを導入することを検討してください。

Backup eMTool は各サーバを個別にバックアップするツールです。すなわち、ツリー全体ではなく、個々のサーバを対象とするよう設計されています。ただし DSMASTER サーバを作成しておけば、Backup eMTool でも、ツリー構造全体をバックアップできるようになります。運用例の概要については、[449 ページの「シナリオ：複数サーバ構成のネットワークで、すべてのサーバが使えなくなった場合」](#)を参照してください。

災害からの復旧で問題となるのは、同じパーティションのレプリカが複数あって、互いに整合性が取れていない場合の対処方法です。災害によってロールフォワードログも失われている場合、すべてのサーバを同じ時点の状態に復元することはできません。バックアップされたレプリカはサーバごとに異なる時点のものなので、ロールフォワードログを使わずに単純に復元しただけでは、全体をツリーとしてまとめる際に問題が起こるためです。復元後の検証処理は、このような問題を予防するために設計されています。デフォルトでは、他のレプリカとの不整合が見つければ、eDirectory データベースは復元後にはオープンされません。

DSMASTER サーバを導入すればこのような事態に備えることができます。ツリー全体のマスタコピーを作成しておき、これを復元の基準点として使用します。

DSMASTER サーバを導入する手順を次に示します。

- ◆ ある 1 台のサーバに、ツリーに属するパーティションすべてのレプリカを保持するよう設定してください。これにより、ツリー全体のコピーが、特定のサーバの eDirectory データベース中に作られるようになります。ただし、ツリーの容量が大きい場合は、複数台のキーサーバに分けても構いません。これを DSMASTER サーバと呼びます。DSMASTER サーバに作るレプリカは、マスタまたは読み書き用と設定してください。

**注：**複数台のキー DSMASTER サーバに分割する場合は、同じパーティションのレプリカが 2 台以上に作られることのないようにしてください。重複のない構成にしておけば、災害後の復元作業において、レプリカ間に不整合が生じることはありません。

災害から復旧する際に、最新のロールフォワードログは使えません。このログは各サーバのローカルファイルとして保存されるためです。したがって、複数台の DSMASTER サーバを、すべて同じ時点の状態に戻すことはできない場合があります。2 台の DSMASTER サーバに同じレプリカがあれば、これが一致せず、ツリーに不整合が生じる恐れがあります。そのため、災害対策としては、同じパーティションのレプリカを複数の DSMASTER サーバに作成することは避ける必要があります。

レプリカ全般については、[52 ページの「レプリカ」](#)を参照してください。

- ◆ DSMASTER サーバを定期的にバックアップして、ツリー全体のバックアップコピーを作成してください。災害対策としては、DSMASTER サーバのバックアップ以外にも、十分な予防措置を講じておくといでしょう。

以上のようにツリーを設計しておくことで、災害が起こっても、迅速にツリー構造を再構築し、稼働させることができます。1 台だけのサーバ（あるいは少数のキーサーバ）のみを復元し、これをマスタレプリカとして扱うようにすればよいのです。

このツリーが稼働し始めてから、フル/インクリメンタルバックアップファイルを使用して、DSMASTER 以外のサーバも順次復元していきます。ロールフォワードログがないため、他のサーバに対する復元後の検証処理は失敗します。そこで、レプリカリングからいったん外し、DSRepair を使って、すべてのレプリカ情報を外部参照に変更します。その後、DSMASTER サーバ上のコピーからレプリカを作成して、改めてサーバにレプリカを追加します。この手順については、[440 ページの「復元後の検証処理に失敗した場合の対処方法」](#)に記載されています。

災害により一部のサーバが失われた場合、操作手順はやや複雑になりますので、Novell の担当者に連絡してください。

## 遷移ベクトルと復元後の検証処理

遷移ベクトルとは、レプリカのタイムスタンプのことです。レプリカ作成時刻を 1970 年 1 月 1 日からの経過秒数で表したものと、レプリカ番号、および現在のイベント番号を組にして表示されます。たとえば次のような形をしています。

```
s3D35F377 r02 e002
```

バックアップ / 復元処理に関していえば、復元されたサーバがレプリカリング内で正しく同期しているかどうか確認するために使う、重要なデータです。

同じパーティションのレプリカを保持するサーバは、レプリカの同期を取るため、互いにデータをやり取りしています。サーバはレプリカリング内の他のサーバと通信するたびに、他のサーバの遷移ベクトルを記録しています。遷移ベクトルを使用すると、レプリカリング内の各レプリカが同期を保つためには、どのデータを送ればよいか、サーバが常に把握できます。サーバが停止するとこの通信が止まり、再び通信できるようになるまでの間、遷移ベクトルに更新や変更があっても他のサーバはそれを送信しません。

あるサーバの eDirectory を復元した後、検証処理として、復元された遷移ベクトルをレプリカリングに属する他のサーバと比較します。これは、復元されたレプリカが他のサーバと同期の取れた状態であるかどうか確認するために実行されます。

リモートサーバの遷移ベクトルの方がローカルベクトルより後の時間に作成されたものである場合は、復元されなかったデータがあるということなので、検証処理は失敗します。これは、フルバックアップまたはインクリメンタルバックアップの前に、ロールフォワードログの機能を有効にしていなかった、ロールフォワードログを使わずに復元しようとした、または必要なロールフォワードログが揃っていなかった、などが原因でデータの損失があることが考えられます。

デフォルトでは、復元した eDirectory データベースが他のレプリカと整合が取れていない場合、そのままではオープンできません。

遷移ベクトルに不整合があるログファイルの例については、[396 ページの「Backup eMTool による復元作業の概要」](#)を参照してください。

互換性の問題で検証処理に失敗することもあります。これについては、[403 ページの「復元後の検証については eDirectory 8.5 以降のみで互換性がある」](#)を参照してください。

検証に失敗した場合の対処方法については、[440 ページの「復元後の検証処理に失敗した場合の対処方法」](#)を参照してください。

## 復元後の検証については eDirectory 8.5 以降のみで互換性がある

復元後の検証処理については、8.5 より前の eDirectory とは互換性がありません。レプリカリング内に eDirectory 8.5 より前のバージョンが稼動しているサーバがあれば、復元処理は失敗します。エラーコードは -666、すなわち「DS バージョンの不整合」となります。これは、レプリカが同期していないことを示すのではなく、eDirectory のバージョンが 8.5 以前のため、遷移ベクトルの比較ができなかったことを示しているに過ぎません。

デフォルトでは、検証処理に失敗しているため、データベースがオープンされません。ただし、エラーが発生しているのが 8.5 サーバのみで、他のサーバでは問題なく検証されているのであれば、eMBox Client で上書き復元を実行することにより、安全にデータベースをオープンすることができます。

あるいは、旧バージョンのサーバをレプリカリングから外し、再度復元を試みる方法もあります。

復元処理と遷移ベクトルの詳細については、[396 ページの「Backup eMTool による復元作業の概要」](#) および [396 ページの「Backup eMTool による復元作業の概要」](#)を参照してください。



## NetWare のファイルシステムデータを復元する際のアクセス権の保存

NetWare の場合、ファイルシステム権 (トラスティの割り当て) は、eDirectory にあるトラスティオブジェクトによって決まります。そのため、eDirectory と NetWare のファイルシステムデータを復元する際には、ファイルシステム権について注意する必要があります。

eDirectory の後でファイルシステムデータを復元するようになれば、その時点でファイルシステム権も正しく復元されます。ただしこの問題を認識しておくことは必要です。起こりうる問題についてはあらかじめ確認し、必要に応じて予防措置を取ってください。

### 復元処理によりファイルシステム権に影響が及ぶ理由

eDirectory の復元作業に先立ち、eDirectory を新たにインストールし、仮のツリーを作成しておく必要があります。仮のツリーを作成するのは故障した記憶デバイスに代わる新しいデバイス上でも、サーバを移行する場合であれば新しいコンピューター上でもかまいません。

eDirectory を新規インストールした段階では、トラスティ権が割り当てられたオブジェクトはありません (復元処理の過程で、トラスティオブジェクトも復元されることになります)。

ファイルシステムデータを復元する際、eDirectory 内のトラスティオブジェクトが検索されます。しかし、復元前に新規インストールした状態のままでトラスティオブジェクトが見つからない場合、そのオブジェクトに対する権利の割り当てもファイルシステムから削除されることがあります。

### この問題への対処方法

復元とファイルシステム権利/トラスティ割り当てに関する問題には、次のように、少しずつ異なるいくつかの対処方法があります。

- ◆ 最も重要なのは、eDirectory を先に復元し、その後でファイルシステムを復元することです。

eDirectory を新たにインストールし、復元する作業に、特別な準備はいりません。これが済んでから、ファイルシステムの復元ツールを使って、ファイルシステム権利やトラスティ割り当てを元に戻すために必要なファイルを復元できます。

- ◆ バックアップの段階で、trustbar.nlm を使用してファイルシステム権利/トラスティ割り当てをバックアップできます。同等の処理ができるサードパーティ製ソフトウェアを使っても構いません。こうしておけば、eDirectory を復元した後でも、必要に応じてトラスティ割り当てを復元できます。

ファイルシステム権利/トラスティ割り当てのバックアップは、eDirectory やファイルシステムと同じスケジュールで実施することもできます。

**注:** ファイルシステム権利のバックアップのスケジュールは、サードパーティ製ソフトウェアのほか、Novell Support Web サイトで提供している cron.nlm (<http://support.novell.com/servlet/tidfinder/2939440>) でも可能です。

- ◆ ストレージシステムの構成を検討し直すことにより、eDirectory やファイルシステムデータを復元しなければならないような障害の可能性を減らすことができます。たとえば RAID 構成などにすれば、ディスクが 1 台故障した場合にデータを損失する可能性は低くなります。sys : ボリュームを冗長構成にしておけば、デバイスに障害があっても、eDirectory の新規インストールやファイルシステムの復元作業はしないで済むかもしれません。



- ◆ 何らかの理由により、先にファイルシステムデータを復元してしまい、権利が失われてしまったとしても、eDirectory を復元した後、もう一度ファイルシステムを復元すれば元に戻すことができます。
- ◆ eDirectory の復元作業が終わるまで、sys : 以外のボリュームはマウントしないでおく、という方法もあります。障害を受けたのは sys : ボリュームだけで、ほかは動作している、という場合に有効です。

確実にボリュームがマウントされないようにするためには、その記憶デバイスとサーバを結ぶケーブルを物理的に外してから NetWare や eDirectory をインストールし、復元作業の終了後、再び接続し直すようにするとよいでしょう。

eDirectory の復元後、必要に応じて sys : ボリュームのファイルシステムを復元して、権利の設定を復旧してください。

## ロールフォワードログを使用する

ロールフォワードログとは、他のデータベース製品でいう「ジャーナル」に相当する機能です。ロールフォワードログ (RFL) は、データベースの変更をすべて記録したものです。

ロールフォワードログを使用する利点は、最後のフル/インクリメンタルバックアップ以降の変更履歴が得られるため、障害で停止する直前の状態にまで eDirectory を復元できることです。ロールフォワードログを使用しないと、最後のフル/インクリメンタルバックアップを取った時点までしか eDirectory を復元できません。

eDirectory は、トランザクションをデータベースに反映する前に、その操作内容をログファイルに記録するようになっています。デフォルトでは、ログファイルはディスク容量の節約のために次々に重ね書きされるようになっているため、eDirectory の変更履歴は残りません。

継続的にロールフォワードログを取る設定にすると、変更履歴が連続したロールフォワードログファイルに保存されます。ロールフォワードログはサーバの性能には影響がありません。eDirectory がすでに作成しているログファイルのエントリを単に保存するだけです。

レプリカリングに属するサーバは、ロールフォワードログ機能を有効にしておく必要があります。バックアップファイルがあっても、ロールフォワードログがなければ復元後の検証処理に失敗し、データベースを開けないこととなります。他のサーバとレプリカを共有するデータベースは、停止直前の状態にまで復元しない限りデフォルトではオープンされません。ロールフォワードログがない場合は、[440 ページの「復元後の検証処理に失敗した場合の対処方法」](#)で説明する手順で復旧してください。

ロールフォワードログの機能は、デフォルトでは無効になっています。サーバで必要に応じて有効に切り替えてください。ロールフォワードログは、サーバの復元作業を実行すると再び無効になり、設定がデフォルトに戻ります。このため復元後に再び有効にし、設定を再作成した上で、改めてフルバックアップを取ってください。フルバックアップが改めて必要となるのは、スケジュールに従って次に無人でのフルバックアップが取られるまでに、再び障害が起こる可能性があるためです。

単一サーバ環境ではロールフォワードログがなくても構いません。しかしロールフォワードログがあれば、最後のバックアップ時ではなくシステム停止直前の状態に復元できます。

ロールフォワードログをオンにする場合、ディスクの空き容量は常に監視している必要があります。詳細については、[408 ページの「ロールフォワードログのバックアップと削除」](#)を参照してください。

このセクションでは、次のトピックについて説明します。

- ◆ 406 ページの「ロールフォワードログ機能を使用する上での注意事項」
- ◆ 407 ページの「ロールフォワードログの保存先」
- ◆ 408 ページの「ロールフォワードログのバックアップと削除」
- ◆ 409 ページの「注意: eDirectory を削除するとロールフォワードログも削除される問題」

ロールフォワードログ機能の切り替えや設定には、iManager または eMBox Client を使います。415 ページの「iManager によるロールフォワードログの設定」または 426 ページの「eMBox クライアントによるロールフォワードログの設定」を参照してください。

## ロールフォワードログ機能を使用する上での注意事項

継続的にロールフォワードログ機能を使用する場合、次のような点に注意してください。

- ◆ バックアップ処理の実行前にロールフォワードログ機能を有効にしておかないと、データベースの復元に利用することはできません。
- ◆ 障害に備えるため、eDirectory とは別の記憶デバイスにロールフォワードログを保存するようにしてください。セキュリティを考慮すれば、ログへのアクセス権も制限する必要があります。詳細については、407 ページの「ロールフォワードログの保存先」を参照してください。
- ◆ ロールフォワードログの保存先を文書に記録しておいてください。詳細については、407 ページの「ロールフォワードログの保存先」を参照してください。
- ◆ ログの保存先のディスクの空き容量を常に監視している必要があります。詳細については、408 ページの「ロールフォワードログのバックアップと削除」を参照してください。
- ◆ ロールフォワードログ機能が無効になっていたり、ログファイルを損失した場合は、有効に切り替えた後、改めてフルバックアップを取ってください。そうしなければ完全に復元できなくなる恐れがあります。次のような状況の場合に必要です。
  - ◆ 復元処理の直後。復元処理の過程で、ロールフォワードログ機能は無効になり、設定もデフォルト値に戻ってしまいます。
  - ◆ デバイス障害などにより、ロールフォワードログを保存しているディレクトリを損失した場合。
  - ◆ 意図せずにロールフォワードログ機能を無効にしてしまった場合。
- ◆ ストリームファイルのログ機能を有効にすると、ディスクの空き容量が急速に減少します。ストリームファイル(ログインスクリプトなど)のログ出力を有効にすると、変更があるたびに、ストリームファイル全体がロールフォワードログに複写されるためです。ストリームファイルのログ出力を無効にし、フル/インクリメンタルバックアップの際にのみストリームファイルをバックアップすると、ログファイルが大きくなるのを遅らせられます。
- ◆ データベースの復元で最も時間を要するのは、ロールフォワードログを参照する処理です。ロールフォワードログの容量は、ツリー構造に対して施された更新の回数に応じて増え、ストリームファイル(ログインスクリプトなど)のログ出力を有効にするとさらに増えます。

データベースが頻繁に更新されるようであれば、バックアップの頻度を上げることも検討するとよいでしょう。こうすると、復元処理の過程でロールフォワードログを参照する処理が少なくなります。

- ◆ ログファイル名を変更しないでください。ログが作成されたときとファイル名が異なる場合、ログファイルは復元処理には使用できません。
- ◆ **eDirectory** を削除するとロールフォワードログもすべて消えてしまいます。いったんデータベースを削除した後、ログファイルを使って復元するのであれば、**eDirectory** を削除する前に、別の場所にコピーしておいてください。
- ◆ 復元が必要な場合は、復元処理の終了後にそのサーバのロールフォワードログ設定を再作成してください。この機能を有効にし、ログの保存先を安全な場所に設定します。ロールフォワードログを有効にしてから、改めてフルバックアップも取る必要があります。

この手順が必要となるのは、復元処理の過程で、ロールフォワードログに関する設定はデフォルトに戻るためです。つまり、ロールフォワードログ機能は無効となり、保存先もデフォルトの場所になるからです。フルバックアップが改めて必要となるのは、スケジュールに従って次に無人でのフルバックアップが取られるまでに、再び障害が起こる可能性があるためです。

## ロールフォワードログの保存先

ロールフォワードログ機能を有効にした場合、その保存先を、**eDirectory** とは別の記憶デバイスに変更します。

保存先を設定する上で、次の点に注意してください。

- ◆ 保存先をデフォルトの場所のままにはせず、**eDirectory** とは別の記憶デバイス上に設定し直してください。こうしておけば、デバイス障害のために **eDirectory** が失われても、復元のためにロールフォワードログにアクセスできます。

たとえば NetWare の場合、デフォルトの保存先は `sys:_netware\nds.rfl` です。ただし、ロールフォワードログ機能を有効にしたら、デフォルトの保存先を使用しないでください。**eDirectory** データベースが保存されている `sys:ボリューム` にログを保存しないでください。

サーバに記憶デバイスがひとつしかない場合、デバイス障害が起こればロールフォワードログも消えてしまうので、障害対策としては役に立ちません。この機能はロールフォワードログを使用しないでおく方法もあります。

ロールフォワードログの保存先を変更するには、**iManager** のバックアップ環境設定画面、または **eMBox Client** の `setconfig` コマンドを使用してください。ロールフォワードログはサーバ上のローカルファイルとして保存する必要があります。

- ◆ 保存先を記録してください。ロールフォワードログの保存先を記録して、サーバのデータベースの復元が必要などに見つけられるようにしてください。これはサーバが正常で障害が発生する前に実行することが重要です。

サーバが正常に動作していれば、**iManager** のバックアップ環境設定画面、または **eMBox Client** の `getconfig` バックアップオプションで調べることができます。ただしハードウェア障害などで **eDirectory** が使えない状態になると、この方法でロールフォワードログの場所を調べることはできません。

サーバに障害が発生し、それを復元する場合は、**eDirectory** を新たにインストールすると、ロールフォワードログの保存先設定はデフォルトの場所に戻ります。このため、復元作業のために **eDirectory** を再インストールしたとしても、サーバの停止前にロールフォワードログをどこに保存していたか、**eDirectory** で調べることはできません。その場合は記録を参照して位置を調べる必要があります。

ロールフォワードログの保存先設定は、\_ndsdb.ini ファイルにも記録されています。しかしこれは eDirectory と同じディスクパーティション/ボリュームにあるため、eDirectory がある記憶デバイスに障害が起これば、ログの保存先を調べるために \_ndsdb.ini ファイルを使用することはできません。

- ◆ ロールフォワードログの保存先へのアクセス権を制限してください。これはセキュリティ上の問題です。見た目で中身がわかるような形式にはなっていませんが、デコードは可能なため、重要なデータが漏洩する恐れがあります。
- ◆ ディスクの空き容量が充分かどうか、常に監視している必要があります。[408 ページの「ロールフォワードログのバックアップと削除」](#)を参照してください。
- ◆ ロールフォワードログ専用のディスクパーティション/ボリュームを用意するのが最善です。こうしておけば、ディスク容量やアクセス権を監視しやすくなります。
- ◆ ログの保存先パスのうち、一番深い階層のディレクトリ名は eDirectory によって作成されます。この名前は現在の eDirectory データベース名に基づいて決まります。

たとえばログの保存先を「d:\Novell\NDS\DIBFiles」と指定した場合、eDirectory データベース名が「NDS」であれば、実際の保存先ファイルは「d:\Novell\NDS\DIBFiles\nds.rfl」となります。データベースの名前を NDS から ND1 に変更した場合、ロールフォワードログのディレクトリは d:\Novell\NDS\DIBFiles\nd1.rfl に変更されます。

保存先の設定を変えるとその時点で新しいディレクトリができますが、ログファイルは実際にトランザクションが発生するまで作成されません。

- ◆ 復元の際は、必要なロールフォワードログをすべて同じディレクトリに集めます。詳細については、[409 ページの「復元処理の準備」](#)を参照してください。

## ロールフォワードログのバックアップと削除

放置しておけばロールフォワードログは次々に蓄積され、ディスクパーティション/ボリュームがいっぱいになります。ディスク容量が不足してロールフォワードログを作成できない場合は、eDirectory はそのサーバに対して応答しなくなります。定期的にログファイルをバックアップし、サーバからは削除するようにして、常に十分なディスク容量を確保するようお勧めします。

削除しても構わないロールフォワードログを判別し、バックアップを取った上で削除するには、次の手順に従います。

- 1 「最後に使用済みになった」ロールフォワードログ名を調べてください。

最後の使用済みロールフォワードログの名前は、次のような方法で調べることができます。

- ◆ iManager で [eDirectory の保守] > [バックアップ環境設定] の順にクリックし、表示されるファイル名を調べます。
- ◆ eMBox Client で getconfig バックアップコマンドを実行します。具体的な手順については [426 ページの「eMBox クライアントによるロールフォワードログの設定」](#)を参照してください。

「最後に使用済みになった」ロールフォワードログとは、トランザクション履歴の記録が終わり、今は書き出しをしていないログファイルのうち、最新のものを表します。現在は別のもっと新しいログファイルに書き出ししているため、オープンしておく必要がないので、「最後に使用済みになった」ロールフォワードログと呼ばれます。一方、現在でもトランザクション履歴を書き出ししているログは「使用中」で、データベースに必要なものです。

- 2 ファイルシステムのバックアップ機能を使って、ロールフォワードログをテープに保存してください。
- 3 「最後に使用済みになった」ものよりも古いロールフォワードログを削除してください。

**警告:** ロールフォワードログを削除するにはより注意を払い、削除しようとするファイルが確実にバックアップされているか、繰り返し確認してください。

「最後に使用済みになった」とは、既にクローズされており、今では履歴の記録をしていないことを表します。サーバから削除しても構わないという意味ではありません。まだテープにバックアップしていないファイルは削除しないようにしてください。

テープに保存してあるロールフォワードログを復元のために使う場合は、次の点に注意してください。

- ◆ 復元に使用する他のロールフォワードログと同様に、ファイルシステムをバックアップしたテープから取得したログファイルは、他のログと合わせてひとつのフォルダに集めてください。このフォルダは、サーバからローカルにアクセスできる必要があります。
- ◆ テープおよびサーバに複製されたファイルのタイムスタンプを比較する必要があります。タイムスタンプに違いがある場合は、最新のサーバ上のファイルを使います。たとえば、ファイルシステムのバックアップ中に、データベースで使用されていたロールフォワードログファイルはテープに完全に保存されません。最新の完全なファイルはサーバに格納されています。

## 注意 : eDirectory を削除するとロールフォワードログも削除される問題

サーバから eDirectory を削除すると、ロールフォワードログのディレクトリおよびその中身もすべて削除されます。いったんデータベースを削除した後、ログファイルを使って復元するのであれば、eDirectory を削除する前に、別の場所にコピーしておいてください。

## 復元処理の準備

eDirectory データベースの復元作業で最も大切なのは、復元が完全に行われたかどうか確認することです。作業に先立ち、[409 ページの「復元作業の前提条件」](#)の説明に従って、必要な準備を行います。必要なバックアップファイルを揃える手順については、[411 ページの「復元に必要なバックアップファイルの収集」](#)を参照してください。

## 復元作業の前提条件

- 復元するサーバとレプリカを共有しているサーバはすべて、稼動状態で、通信できるようにしておかなければなりません。これは、復元後の検証処理で、同じレプリカリングに属するサーバ間の整合性を確認するために必要です。
- 必要な次のバックアップファイルをすべて収集してください。
  - ◆ フルバックアップおよびそれ以降のインクリメンタルバックアップのファイルを、復元するサーバの、1つのディレクトリ内に集めます。
  - ◆ 最後にバックアップを取って以降のロールフォワードログをすべて、同じサーバ上のもう1つのディレクトリにまとめておきます。

このサーバがレプリカリングに属している場合、最後にバックアップを取った時点以降のロールフォワードログをすべて、ひとつのディレクトリ内にまとめておきます。ファイル名はログ生成時と同じにしておかなければなりません。



411 ページの「復元に必要なバックアップファイルの収集」を参照してください。

**注:** バックアップファイルがない場合は、XBrowse を使って、サーバ情報の復元に必要な情報を eDirectory に問い合わせてください。この作業は、サーバオブジェクトやその関連オブジェクトをツリーから削除する前に実行する必要があります。Xbrowse の詳細については、[Novell Support Web site, Solution 2960653 \(http://support.novell.com/servlet/tidfinder/2960653\)](http://support.novell.com/servlet/tidfinder/2960653) を参照してください。

- ❑ eDirectory を再インストールし、仮のツリーで稼働させておきます。

最初はサーバを仮のツリーで稼働させます。最終的には障害が起きる前と同じ名前のサーバに復元しようとしているわけですが、まだ復元作業が完了していない段階で本来のツリーに組み込んでしまうと、混乱が生じてしまうからです。データベースの復元処理が完了してから、本来のツリーにサーバを組み入れることとなります。

- ❑ (状況によって実行) このサーバでロールフォワードログ機能を使うためには、復元後に改めて有効に切り替え、障害対策のための書き出し先も設定し直して、ロールフォワードログの環境設定を再作成する必要があります。ロールフォワードログを有効にしてから、改めてフルバックアップも取る必要があります。

復元処理の過程で、ロールフォワードログの機能は無効になり、ログ保存先の設定もデフォルトに戻ってしまいます。

フルバックアップが改めて必要となるのは、スケジュールに従って次に無人でのフルバックアップが取られるまでに、再び障害が起こる可能性があるためです。

- ❑ (状況によって実行) IP アドレスを指定してこのサーバにアクセスするアプリケーションやオブジェクトがある場合は、元と同じ IP アドレスを設定してください。

- ❑ (NetWare の場合のみ) 復元されたサーバの名前を、障害前と同じにしてください。同じ名前を使用しないと、復元後に「ボリュームオブジェクトが不正」などのエラーが起こる可能性があります。

復元する NetWare サーバ名を変更するには、`autoexec.ncf` ファイルを書き替え、サーバを再起動してください。

- ❑ (NetWare のみ) ファイルシステムデータおよび eDirectory を復元する際は、ファイルシステム権利を元どおりに戻せるよう、正しい手順で作業してください。eDirectory を先に復元し、その後でファイルシステムを復元してください。この手順の詳細については、404 ページの「NetWare のファイルシステムデータを復元する際のアクセス権の保存」を参照してください。

復元の過程で、eDirectory Backup eMTool はまず、フルバックアップファイルからの復元を試みます。それが済むと、Backup eMTool でインクリメンタルバックアップファイルの名前を入力するよう求められます。その際、次に適用するべきファイルの ID が提示されます。インクリメンタルバックアップファイルからの復元が終わると、今度はロールフォワードログを参照しての復元処理が始まります (396 ページの「Backup eMTool による復元作業の概要」も参照してください)。

必要なファイルをすべて揃えた後、iManager や eMBox Client から復元処理を起動します。428 ページの「eMBox クライアントによるバックアップファイルの復元作業」または 417 ページの「iManager によるバックアップファイルの復元作業」を参照してください。

## 復元に必要なバックアップファイルの収集

- 1 ファイルシステムをバックアップしたテープから、eDirectory フルバックアップファイルを、サーバ上の適当なディレクトリにコピーしてください。

最後に取ったフルバックアップの ID は、Backup eMTool のログファイルで確認できます。

- 2 同様に、一連のインクリメンタルバックアップファイルを、サーバ上の適当なディレクトリにコピーしてください。

必要なインクリメンタルバックアップファイルは、フルバックアップファイルのヘッダ部で確認できます。「next\_inc\_file\_ID」属性として、次のインクリメンタルバックアップファイルの ID が記述されています。この値は、インクリメンタルバックアップファイルのヘッダ部にある「incremental\_file\_number」属性に対応します。ヘッダの形式について詳しくは、[397 ページの「バックアップファイルのヘッダ書式」](#)を参照してください。

**警告:** バックアップファイルを開く場合でもヘッダを確認するだけにとどめ、保存や変更はしないようにしてください。ファイルの一部が切り捨てられてしまうことがあります。ほとんどのアプリケーションではバイナリデータを正確に保存することはできません。

インクリメンタルバックアップファイルにはそれぞれ、次のインクリメンタルバックアップファイルの ID が記載されています。

この ID も Backup eMTool のログファイルで確認できます。

同じ名前のファイルがいくつもあって、ひとつのディレクトリにまとめるためにファイル名を変更しているような場合、ID はその識別に不可欠です。たとえば無人でのバックアップにいつも同じバッチファイルを使っていて、バックアップファイル名が常に同じであるような場合です。ヘッダ部の ID を見れば、ファイル名が変わっていても適切なファイルを判別できます。

- 3 (状況によって実行) ロールフォワードログ機能を有効にしていた場合は、最後のバックアップ以降のロールフォワードログを、生成時のファイル名のまま、サーバ上の適当なディレクトリに集めてください。

このサーバがレプリカリングに属している場合は、ロールフォワードログを使った復元処理が必須です。ロールフォワードログがすべて揃っていない場合、復元後の検証処理で失敗してしまいます。リング内の他のレプリカと、遷移ベクトルが一致しないからです。デフォルトでは、復元した eDirectory データベースが他のレプリカと整合が取れていない場合、そのままではオープンできません。

テキストエディタで最新のバックアップファイルを開き、ヘッダの「current\_log」属性を読んで、最初に必要なロールフォワードログを特定します。この作業を繰り返して、続くすべてのロールフォワードログを集めます。

**警告:** バックアップファイルを開く場合でもヘッダを確認するだけにとどめ、保存や変更はしないようにしてください。ファイルの一部が切り捨てられてしまうことがあります。ほとんどのアプリケーションではバイナリデータを正確に保存することはできません。

必要なロールフォワードログがすべて 1ヶ所にまとまっているとは限りません。よく確認して、すべて同じディレクトリに揃えてください。ロールフォワードログは、次の理由から複数の場所に格納されている場合があります。

- ◆ 最後に eDirectory のフル/インクリメンタルバックアップを実行してから、ロールフォワードログの保存先を変更した場合。
- ◆ ファイルシステムのバックアップを使用して、ロールフォワードログをテープにバックアップした後で、空きディスク容量を確保するためにそれらのファイルを削除した場合。

テープにバックアップされたロールフォワードログを取得する場合は、データが最新のセットであることを確認してください。テープおよびサーバに複製されたファイルのタイムスタンプを比較する必要があります。ファイルシステムのバックアップ中に、データベースで使用されていたロールフォワードログファイルはテープに完全に保存されません。最新の完全なファイルはサーバに格納されています。

- ◆ 最後にバックアップを実行してから eDirectory データベースの名前を変更した (NDS から ND1 に変更した場合など)。この変更により、ロールフォワードログのパスの最後のディレクトリ名が変更されます。

たとえばログの保存先を「D:\Novell\nds\dibfiles\」と指定した場合、eDirectory データベース名が「NDS」であれば、実際の保存先ファイルはディレクトリ「D:\Novell\nds\dibfiles\nds.rfl\」となります。データベースの名前を NDS から ND1 に変更した場合、ロールフォワードログのディレクトリは D:\Novell\nds\dibfiles\nd1.rfl\ に変更されます。

**重要:** 必要なロールフォワードログがすべてそろっていることを確認してください。Backup eMTool では、ロールフォワードログがすべてそろっているかどうか確認できません。ロールフォワードログは順番に開かれて使用されます。指定したディレクトリ内に次のロールフォワードログが見つからない場合は、復元プロセスが中止されます。必要なロールフォワードログがすべてそろっていなければ復元は完了しません。

## Novell iManager を使ったバックアップ / 復元作業

バックアップやその環境設定、復元の作業は、Novell iManager から eDirectory Backup eMTool を呼び出す形で実行できます。iManager を使うことにより、ファイアウォールの外側からでも、Web ブラウザ画面で操作できます。Novell iManager の詳細については、『[Novell iManager 2.5 管理ガイド](http://www.novell.com/documentation/imanager25/index.html)』(<http://www.novell.com/documentation/imanager25/index.html>) を参照してください。

ただし、コールドバックアップ (データベースをいったん停止したフルバックアップ)、無人バックアップ、高度な復元機能は、iManager からは実行できません。こういった作業は eMBox Client で実行することになります。詳しくは [420 ページの「eMBox クライアントを使ったバックアップ / 復元作業」](#) を参照してください。

eDirectory のバックアップ / 復元作業に先立ち、[390 ページの「eDirectory のバックアップ処理に関する確認事項」](#) を参照して問題点を確認し、効率的に作業できるようにしてください。

このセクションでは、次のトピックについて説明します。

- ◆ [413 ページの「iManager による手動バックアップ」](#)
- ◆ [415 ページの「iManager によるロールフォワードログの設定」](#)
- ◆ [417 ページの「iManager によるバックアップファイルの復元作業」](#)



## iManager による手動バックアップ

iManager のブラウザ画面から [バックアップ] を使用して、eDirectory データベースをサーバにバックアップします。フルバックアップ、インクリメンタルバックアップのどちらも実行可能です。

バックアップファイルには、eDirectory をその時点の状態に復元するために必要な情報がすべて含まれています。また、処理結果は所定のログファイルに記録されます。

iManager から実行できるのは「ホット」バックアップです。つまり、バックアップ処理中も eDirectory データベースは開いたままで、通常どおり利用しながら、バックアップ開始時点の状態を完全に保存できます。

なお、コールドバックアップ (データベースを停止してのバックアップ) や無人バックアップを実行するには、eMBox Client を使用する必要があります。420 ページの「eMBox クライアントによる手動バックアップ」および 423 ページの「バッチファイルと eMBox クライアントによる無人バックアップ」を参照してください。

eDirectory のバックアップ / 復元作業に先立ち、390 ページの「eDirectory のバックアップ処理に関する確認事項」を参照して問題点を確認し、効率的に作業できるようにしてください。

### 前提条件

- eDirectory 以外にも追加でバックアップしたいファイルがあれば、それを列挙したインクルードファイルを作っておいてください。

iManager の設定画面で該当するチェックボックスをオンにすれば、NICI ファイルやストリームファイルもバックアップできます。NICI ファイルは常にバックアップするようお勧めします。

それ以外にたとえば autoexec.ncf などをバックアップしたい場合は、そのパスとファイル名をインクルードファイルに列挙します。複数のファイルがある場合はセミコロンで区切ります。改行 (ハードリターン) や空白を含めないようにしてください (例: 「sys:¥system¥autoexec.ncf;sys:¥etc¥hosts;」)。

- eDirectory のバックアップ後すぐに、ファイルシステムのバックアップ作業を行い、テープに保存できるよう準備してください (Backup eMTool による処理では、サーバ上にバックアップファイルができるだけです)。

ヒント: コピー先記憶デバイスに容量の制約がある場合は、あらかじめ eDirectory バックアップファイルの最大サイズを設定すると便利です。また、バックアップファイルの作成後、サードパーティ製ファイル圧縮ツールを使う方法もあります。80% 程度は圧縮できます。

- ロールフォワードログを作成するのであれば、バックアップを行う前にこの機能を有効にしてください。

レプリカリングに属するサーバは、ロールフォワードログ機能を有効にしておく必要があります。バックアップファイルがあっても、ロールフォワードログがなければ復元後の検証処理に失敗し、データベースを開けないこととなります。

ロールフォワードログの詳細については、405 ページの「ロールフォワードログを使用する」を参照してください。また、この機能を有効にする手順については、415 ページの「iManager によるロールフォワードログの設定」を参照してください。


- 複数サーバ環境のツリーの場合、このサーバとレプリカを共有するサーバすべてについて、eDirectory 8.5 以降にアップグレードする必要があります。

詳細については、403 ページの「復元後の検証については eDirectory 8.5 以降のみで互換性がある」を参照してください。

## 操作手順

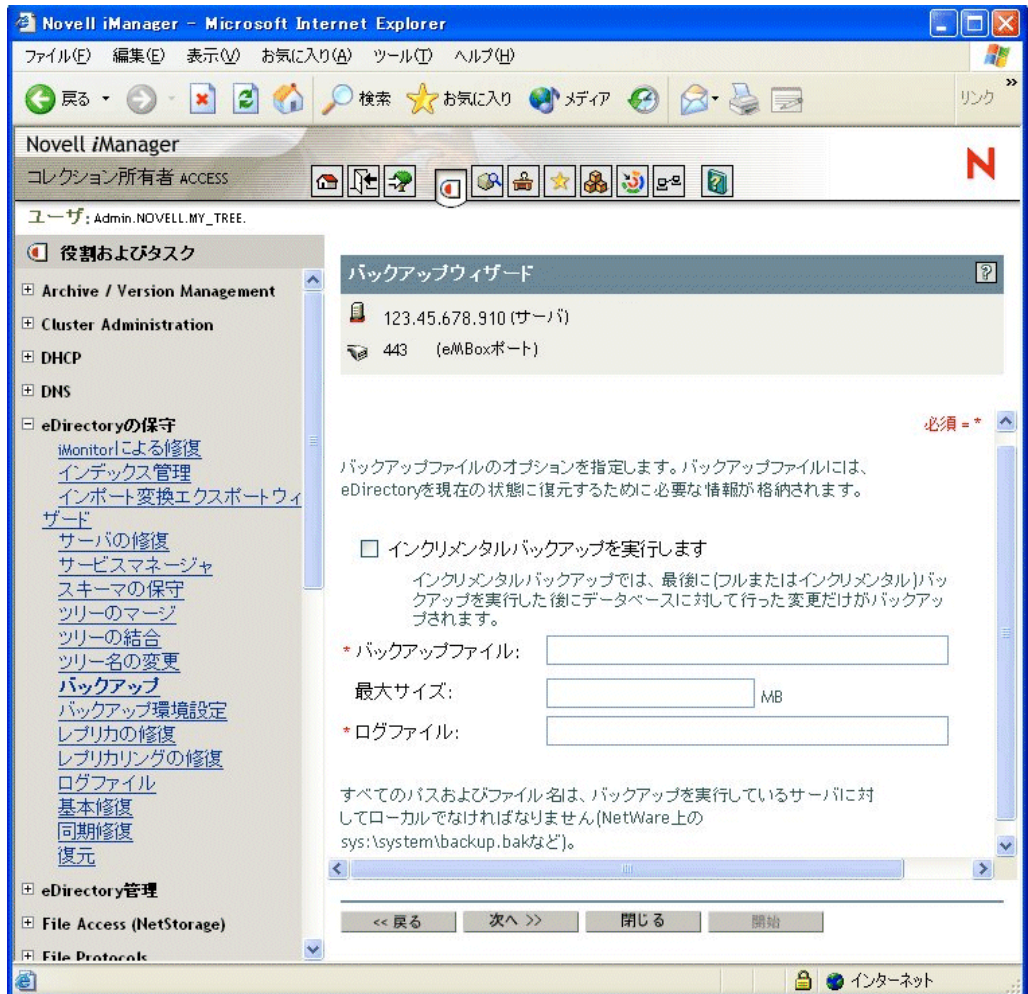
iManager を使って eDirectory データベースをバックアップする手順を次に示します。

ヒント : iManager で使用できるオプションについてはオンラインヘルプを参照してください。

- 1 [役割およびタスク] ボタン  をクリックします。
- 2 [eDirectory の保守] > [バックアップ] の順にクリックします。
- 3 バックアップの対象サーバを指定し、[次へ] をクリックします。
- 4 バックアップを実行するサーバのユーザ名、パスワード、コンテキストを指定し、[次へ] をクリックします。
- 5 バックアップファイルのオプションを指定し、[次へ] をクリックします。

最後にバックアップを実行した後の差分のみをバックアップしたい場合は、[インクリメンタルバックアップを実行します] をクリックしてください。

画面例を次に示します。

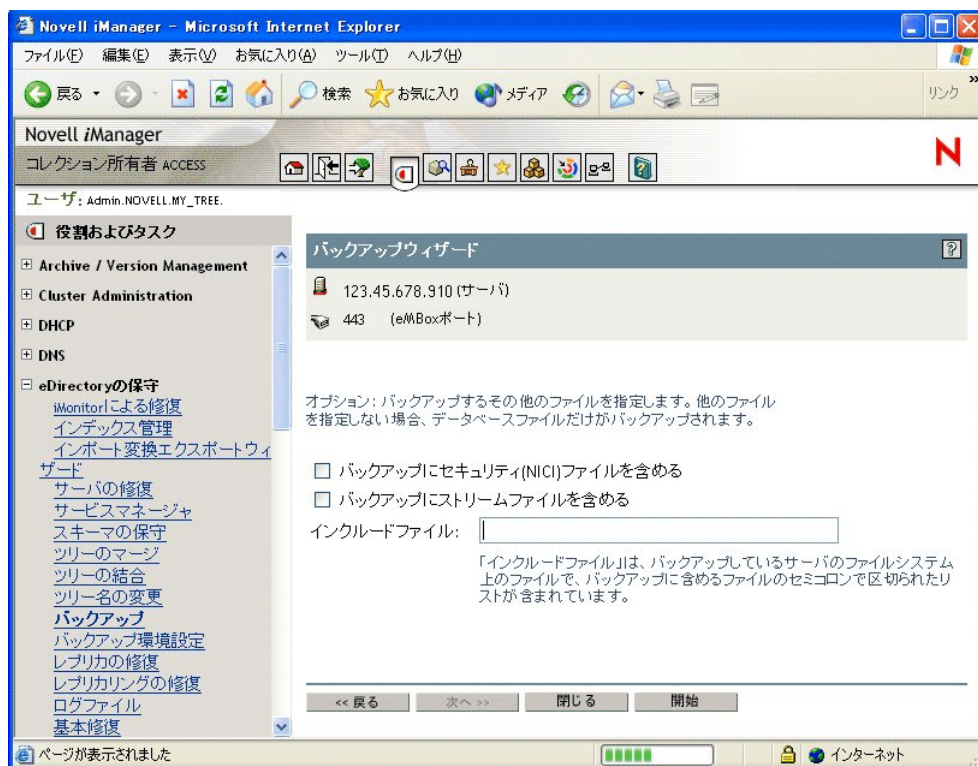


- 6 追加でバックアップしたいファイルがあればここで指定します。

追加するファイルが指定されていない場合、eDirectory データベースのみがバックアップされます。

NICI ファイルは常にバックアップするようお勧めします。

画面例を次に示します。



- 7 表示される指示に従って、バックアップを完了します。

- 8 eDirectory のバックアップ処理が終了したら、すぐにファイルシステムのバックアップ作業を行い、テープに保存します (Backup eMTool による処理では、サーバ上にバックアップファイルができるだけです)。

## iManager によるロールフォワードログの設定


ブラウザから [バックアップ環境設定] を使用して、ロールフォワードログに関する設定を変更します。次のような設定ができます。

- ◆ ロールフォワードログ機能の有効 / 無効の切り替え  
レプリカリングに属するサーバは、ロールフォワードログ機能を有効にしておく必要があります。バックアップファイルがあっても、ロールフォワードログがなければ復元後の検証処理に失敗し、データベースを開けないこととなります。
- ◆ ロールフォワードログの保存先ディレクトリの変更
- ◆ ロールフォワードログのファイルサイズの最小値、最大値の設定
- ◆ 現在使用中のログ、既書き出しを終えた最新のログの判別
- ◆ ストリームファイルをロールフォワードログに含めるかどうかの切り替え



ロールフォワードログの詳細については、405 ページの「[ロールフォワードログを使用する](#)」を参照してください。

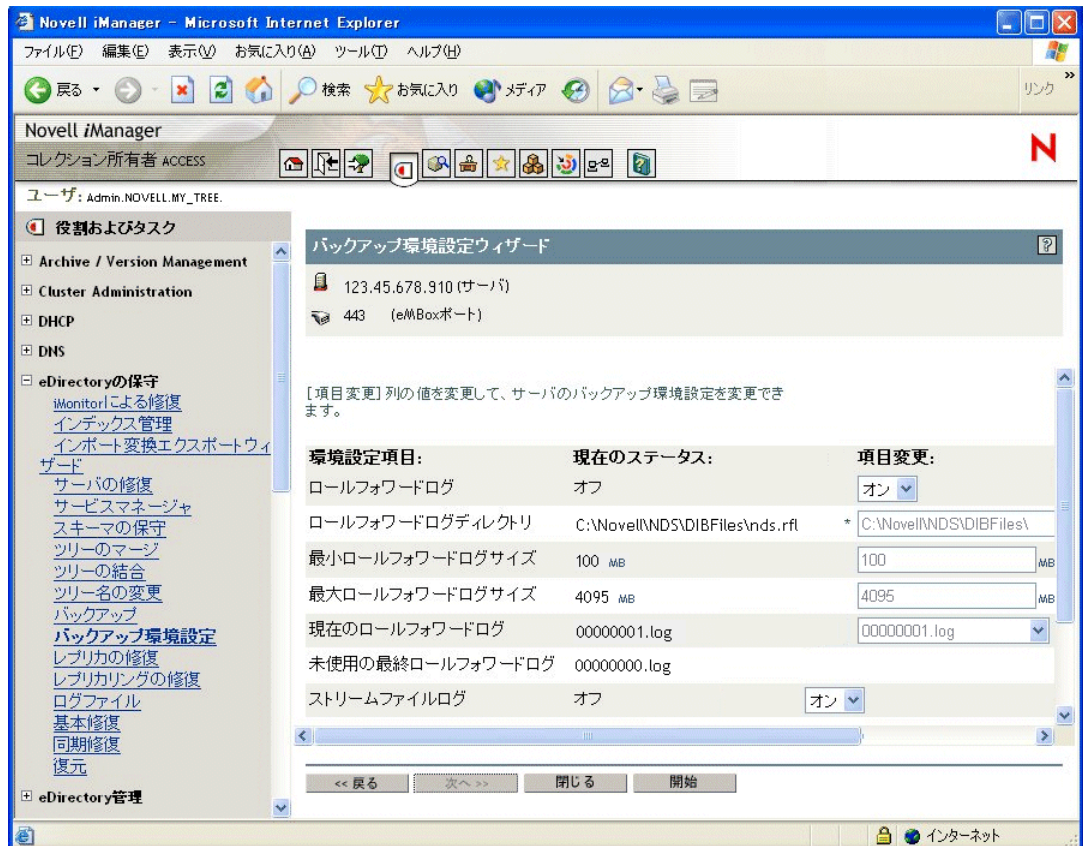
ヒント: iManager で使用できるオプションについてはオンラインヘルプを参照してください。

- 1 [役割およびタスク] ボタン  をクリックします。
- 2 [eDirectory の保守] > [バックアップ環境設定] の順にクリックします。
- 3 設定を変更するサーバを指定し、[次へ] をクリックします。
- 4 設定を変更するサーバのユーザ名、パスワード、コンテキストを指定し、[次へ] をクリックします。
- 5 必要に応じてサーバのバックアップ環境設定を変更します。

**警告:** ロールフォワードログ機能を有効にしたら、デフォルトの保存先を使用しないでください。障害対策のためには、eDirectory とは別のディスクパーティション/ボリューム、別の記憶デバイスを指定してください。ロールフォワードログディレクトリは、バックアップ環境設定を変更するサーバ上である必要があります。

**重要:** ロールフォワードログ機能を有効にする場合、ログを保存するボリュームのディスク容量を常に監視してください。これを怠ると、ログの容量は増える一方なので、ディスクパーティション/ボリュームがあふれてしまう恐れがあります。ディスク容量が不足してロールフォワードログを作成できない場合は、eDirectory はそのサーバに対して応答しなくなります。書き出しが終わったロールフォワードログは、定期的にバックアップし、サーバから削除するようお勧めします。408 ページの「[ロールフォワードログのバックアップと削除](#)」を参照してください。

画面例を次に示します。



- 6 表示される指示に従って、操作を完了します。

## iManager によるバックアップファイルの復元作業

ブラウザから [復元] を使用して、保存されたバックアップファイルのデータから eDirectory データベースを復元します。処理結果は所定のログファイルに記録されます。

復元処理の詳細については、[396 ページの「Backup eMTool による復元作業の概要」](#)を参照してください。

高度な復元機能は eMBox Client から実行する必要があります。詳しくは [420 ページの「eMBox クライアントを使ったバックアップ / 復元作業」](#)を参照してください。

### 前提条件

- ❑ 必要なバックアップファイルをすべて、復元対象サーバ上の、適当なディレクトリに集めておく必要があります。

[409 ページの「復元処理の準備」](#) および [411 ページの「復元に必要なバックアップファイルの収集」](#) を参照してください。
- ❑ eDirectory を復元対象のサーバにインストールし、稼働させておいてください。


たとえば記憶デバイスの障害の場合、デバイスを交換し、改めて eDirectory をインストールすることになります。故障したサーバごとと交換する、あるいは単に新しいサーバに移行する場合は、新しいサーバにオペレーティングシステムをインストールした上で、eDirectory も準備します。
- ❑ 復元処理の詳細については、[396 ページの「Backup eMTool による復元作業の概要」](#)を参照してください。
- ❑ (NetWare のみ) ファイルシステムデータおよび eDirectory を復元する際は、ファイルシステム権利を元どおりに戻せるよう、正しい手順で作業してください。

eDirectory を先に復元し、その後でファイルシステムを復元してください。この手順の詳細については、[404 ページの「NetWare のファイルシステムデータを復元する際のアクセス権の保存」](#)を参照してください。

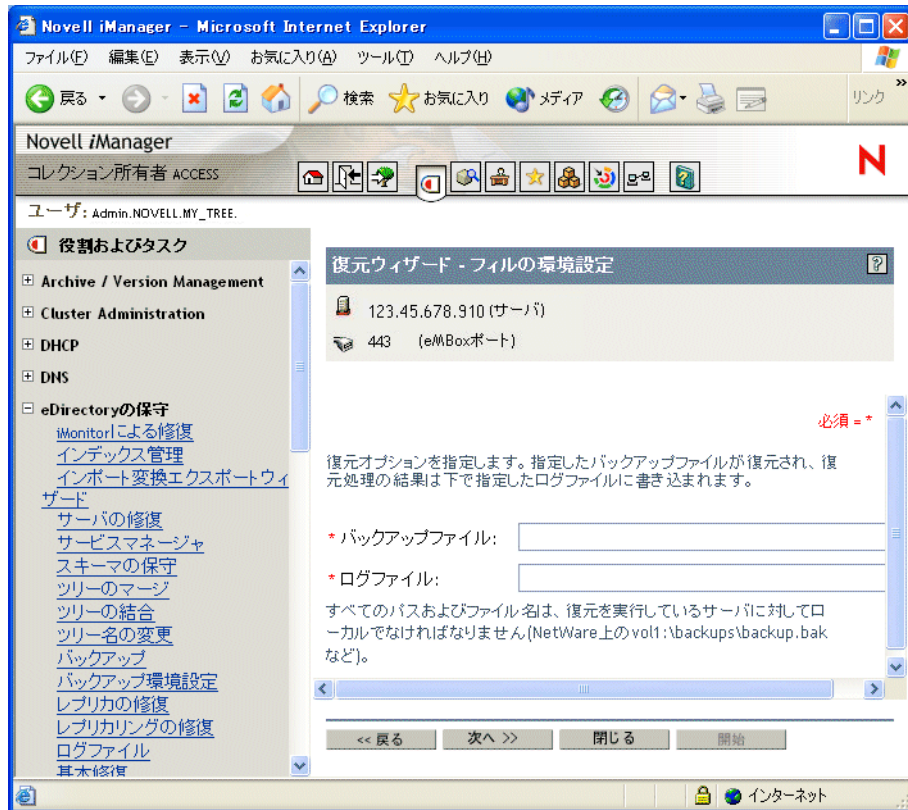
### 操作手順

ヒント: iManager で使用できるオプションについてはオンラインヘルプを参照してください。

iManager を使って eDirectory データベースを復元する手順を次に示します。

- 1** 必要なバックアップファイルを集めておきます。詳しくは [409 ページの「復元処理の準備」](#) を参照してください。
- 2** [役割およびタスク] ボタン  をクリックします。
- 3** [eDirectory の保守] > [復元] の順にクリックします。
- 4** 復元対象サーバを指定し、[次へ] をクリックします。
- 5** 復元を実行するサーバのユーザ名、パスワード、コンテキストを指定し、[次へ] をクリックします。
- 6** バックアップファイル名、ログファイル名を指定し、[次へ] をクリックします。

画面例を次に示します。



**7** 必要な復元オプションを指定し、[次へ] をクリックします。

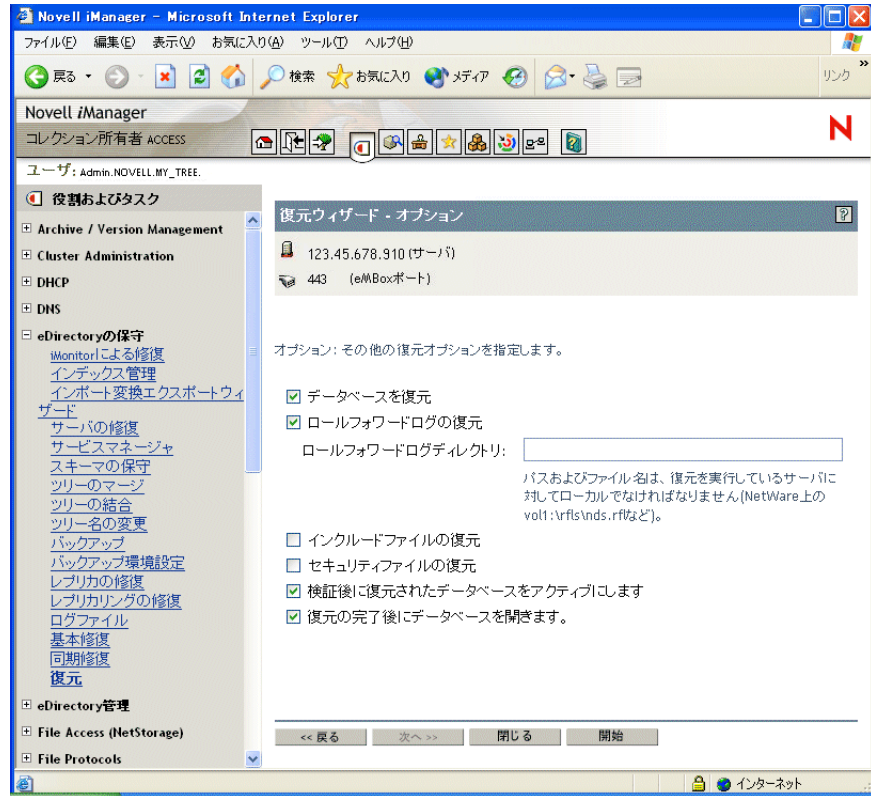
通常、少なくとも次のチェックボックスはオンにする必要があります。

- ◆ データベースを復元
- ◆ 検証後に復元されたデータベースをアクティブにします
- ◆ 復元の完了後にデータベースを開きます
- ◆ セキュリティファイルの復元 (NICI ファイルの復元)

NICI ファイルは必ずバックアップしておくようお勧めします。これがないと、復元に成功しても、暗号化されたファイルは読めません。

ロールフォワードログを使って復元する場合は、そのフルパスを指定しなければなりません。これには、eDirectory が自動的に追加するディレクトリ名 (通常は「¥nds.rfl」) も含みます。詳しくは [407 ページの「ロールフォワードログの保存先」](#) を参照してください。

画面例を次に示します。



- 8 表示される指示に従って、復元を完了します。

復元後の検証に失敗した場合の対処については、[440 ページの「復元後の検証処理に失敗した場合の対処方法」](#)を参照してください。

注：レプリカリング中に eDirectory 8.5 より前のバージョンが稼動しているサーバがある場合、復元処理は失敗します。エラーコードは -666、すなわち「DS バージョンの不整合」となります。この場合の対処方法については、[403 ページの「復元後の検証については eDirectory 8.5 以降のみで互換性がある」](#)を参照してください。

- 9 NCSI セキュリティファイルを復元した場合は、復元完了後に NCSI を再初期化するため、サーバを再起動します。
- 10 ここでサーバが通常どおり要求に応答することを確認しておきます。
- 11 (状況によって実行) このサーバでロールフォワードログ機能を使うためには、改めて有効に切り替え、障害対策のための書き出し先も設定し直して、ロールフォワードログの環境設定を再作成する必要があります。ロールフォワードログを有効にしてから、改めてフルバックアップも取る必要があります。

この手順が必要となるのは、復元処理の過程で、ロールフォワードログに関する設定はデフォルトに戻るためです。つまり、ロールフォワードログ機能は無効となり、保存先もデフォルトの場所になるからです。フルバックアップが改めて必要となるのは、スケジュールに従って次に無人でのフルバックアップが取られるまでに、再び障害が起こる可能性があるためです。

ロールフォワードログの詳細については、[405 ページの「ロールフォワードログを使用する」](#)を参照してください。

以上で復元作業が終了しました。NCSI の再初期化も済んでいるので、暗号化された情報にもアクセスできます。ロールフォワードログ機能を使用する場合は、今後の障害に備えるため、再びこの機能を有効にし、フルバックアップを取っておいてください。



## eMBox クライアントを使ったバックアップ / 復元作業

eMBox クライアントはコマンドライン Java クライアントで、これを使用すると eDirectory Backup eMTool などの eMBox ツールにアクセスできます。複数サーバ環境でも、ファイアウォール越しのアクセスができれば、1 台のコンピュータからバックアップ、復元、ロールフォワードログの設定ができます。

eMBox クライアントはバッチモードで実行できるため、eDirectory Backup eMTool を使用して無人バックアップを行うことができます。

eMBoxClient.jar ファイルは、eDirectory の一部としてサーバにインストールされます。それ以外にも、Sun JVM 1.3.1 が動作する環境であれば、eMBoxClient.jar をコピーして動かすことができます。詳細については、[555 ページの「eDirectory Management Toolbox」](#) および [557 ページの「ワークステーションで eMBox クライアントを実行する」](#) を参照してください。

eDirectory のバックアップ / 復元作業に先立ち、[390 ページの「eDirectory のバックアップ処理に関する確認事項」](#) を参照して問題点を確認し、効率的に作業できるようにしてください。

このセクションでは、次のトピックについて説明します。

- ◆ [420 ページの「eMBox クライアントによる手動バックアップ」](#)
- ◆ [423 ページの「バッチファイルと eMBox クライアントによる無人バックアップ」](#)
- ◆ [426 ページの「eMBox クライアントによるロールフォワードログの設定」](#)
- ◆ [428 ページの「eMBox クライアントによるバックアップファイルの復元作業」](#)
- ◆ [431 ページの「バックアップ / 復元のコマンドラインオプション」](#)

### eMBox クライアントによる手動バックアップ

eMBox クライアントを使って、eDirectory データベースの中身を、指定したファイルにバックアップすることができます。バックアップファイルには、eDirectory をその時点の状態に復元するために必要な情報がすべて含まれています。また、処理結果は所定のログファイルに記録されます。

eDirectory のバックアップ / 復元作業に先立ち、[390 ページの「eDirectory のバックアップ処理に関する確認事項」](#) を参照して問題点を確認し、効率的に作業できるようにしてください。

eMBox クライアントを使うと次のような作業ができます。

- ◆ データベースを開いたままで、フル / インクリメンタルバックアップ (ホットバックアップ)。  
「ホット」バックアップの場合、バックアップ処理中も eDirectory データベースは開いたままで、通常どおり利用しながら、バックアップ開始時点の状態を完全に保存できます。
- ◆ コールドバックアップ (データベースをいったん停止してフルバックアップ)。  
この機能は、ハードウェアをアップグレードする、あるいは新規サーバ (同じオペレーティングシステムが動作するもの) に移行する場合に有用です。詳しくは [536 ページの「ハードウェアのアップグレードやサーバの交換」](#) を参照してください。
- ◆ バックアップ後、データベースを閉じたままにしてロックする設定。
- ◆ バックアップファイルの最大サイズの設定。

これらの作業を無人で実行するための手順については、[423 ページの「バッチファイルと eMBox クライアントによる無人バックアップ」](#) を参照してください。



## 前提条件

- バックアップ処理を起動するコンピュータに、ファイル `eMBoxClient.jar` があることを確認してください。

このファイルは、eDirectory の一部としてサーバにインストールされます。それ以外にも、Sun JVM 1.3.1 が動作する環境であれば、`eMBoxClient.jar` をコピーして実行することができます。複数サーバ環境でも、ファイアウォール越しのアクセスが可能であれば、1 台のコンピュータからバックアップを実行できます。詳細については、555 ページの「[eMBox コマンドラインクライアントの使用](#)」を参照してください。

- ロールフォワードログを作成するのであれば、バックアップを行う前にこの機能を有効にしてください。

レプリカリングに属するサーバは、ロールフォワードログ機能を有効にしておく必要があります。バックアップファイルがあっても、ロールフォワードログがなければ復元後の検証処理に失敗し、データベースを開けないこととなります。

ロールフォワードログの詳細については、405 ページの「[ロールフォワードログを使用する](#)」を参照してください。また、この機能を有効にする手順については、426 ページの「[eMBox クライアントによるロールフォワードログの設定](#)」を参照してください。

- eDirectory 以外にも追加でバックアップしたいファイルがあれば、それを列挙したインクルードファイルを作っておいてください。

NICI ファイルやストリームファイルもスイッチを使用してバックアップできます。NICI ファイルは常にバックアップするようお勧めします。

それ以外にたとえば `autoexec.ncf` などをバックアップしたい場合は、そのパスとファイル名をインクルードファイルに列挙します。複数のファイルがある場合はセミコロンで区切ります。改行 (ハードリターン) や空白を含めないようにしてください (例: 「`sys:¥system¥autoexec.ncf;sys:¥etc¥hosts;`」)。

- eDirectory のバックアップ後すぐに、ファイルシステムのバックアップ作業を行い、テープに保存できるよう準備してください (Backup eMTool による処理では、サーバ上にバックアップファイルができるだけです)。

ヒント: コピー先記憶デバイスに容量の制約がある場合は、あらかじめ eDirectory バックアップファイルの最大サイズを設定すると便利です。その場合、バックアップコマンドの「`-s`」オプションを使い、バイト単位で指定します。また、バックアップファイルの作成後、サードパーティ製ファイル圧縮ツールを使う方法もあります。80% 程度は圧縮できます。

- コマンドラインオプションについては、431 ページの「[バックアップ / 復元のコマンドラインオプション](#)」を参照してください。

- 複数サーバ環境のツリーの場合、このサーバとレプリカを共有するサーバすべてについて、eDirectory 8.5 以降にアップグレードする必要があります。

詳細については、403 ページの「[復元後の検証については eDirectory 8.5 以降のみで互換性がある](#)」を参照してください。

## 操作手順

eMBox クライアントを使って eDirectory データベースをバックアップする手順を次に示します。

- 1 eMBox クライアントを対話式モードで起動します。
  - ◆ NetWare、UNIX の場合: コマンドラインから「`edirutil -i`」と入力します。
  - ◆ Windows: 「`ドライブ¥novell¥nds¥edirutil.exe -i`」を実行します。

edirutil ファイルは、eMBox クライアントを実行するためのショートカットです。Java の実行形式ファイルと、eMBox クライアントのインストール先ディレクトリがパラメータとして記述されているほか、NetWare の場合は「-ns」オプションもついています。(Java 実行ファイルの場所は、557 ページの「eMBox クライアント用にパスおよびクラスパスをセットアップする」で示しているように手動で入力することもできます。)

正常に起動されると、「eMBox Client」というプロンプトが現れます。eMBox Client>

- 2 バックアップの対象サーバにログインします。次のように入力してください。

**login -s サーバ名または IP アドレス -p ポート番号 -u ユーザ名 . コンテキスト -w パスワード**

たとえば Windows の場合、次のようになります。

```
login -s 151.155.111.1 -p 8009 -u admin.mycompany -w mypassword
```

セキュア接続が確立できないというエラーが表示される場合は、564 ページの「eMBox クライアントを使用してセキュア接続を確立する」に表示されている JSSE ファイルがシステム上にない可能性があります。

指定するポート番号が分からない場合は、564 ページの「eDirectory ポート番号を確認する」を参照してください。

eMBox クライアントはログインが成功したかどうかを表示します。

- 3 eMBox クライアントのプロンプトが出たら、次のような形式でバックアップコマンドを入力します。

**backup -b -f バックアップファイルの名前とパス -l バックアップログファイルの名前とパス -u インクルードファイルのファイル名とパス -t -w**

各スイッチの間にはスペースが必要です。スイッチの順序は重要ではありません。たとえば Windows の場合、次のようになります。

```
backup -b -f c:\backups¥8_20_2001.bak -l c:\backups¥backup.log -u c:\backups¥myincludefile.txt -t -w
```

この例では、フルバックアップを取ること (-b)、バックアップファイルを c:\backups¥8\_20\_2001.bak とすること、処理結果を c:\backups¥backup.log に出力すること、さらに、次のデータベース以外のファイルもバックアップすることを指定しています。

- ◆ 管理者があらかじめ作成したインクルードファイル (c:\backups¥myincludefile.txt) に列挙されたバックアップ対象のファイル (「-u」オプションで指定)。
- ◆ ストリームファイル (「-t」オプションで指定)。

さらにこの例では「-w」オプションが指定されているため、同じ名前のバックアップファイルがあれば上書きされます。

eMBox クライアントはバックアップが成功したかどうかを表示します。

- 4 サーバからログアウトするには、次のコマンドを入力します。

**logout**

- 5 eMBox クライアントを終了するには、次のコマンドを入力します。

**exit**

- 6 eDirectory のバックアップ処理が終了したら、すぐにファイルシステムのバックアップ作業を行い、テープに保存します (Backup eMTool による処理では、サーバ上にバックアップファイルができるだけです)。

## バッチファイルと eMBox クライアントによる無人バックアップ

バッチファイルを使用して、eMBox クライアントによる eDirectory の無人バックアップを実行します。たとえば週 1 回フルバックアップ、毎晩インクリメンタルバックアップを取る、といった運用が可能です。

バッチモードで eMBox クライアントを実行するには、システムバッチファイルを使う、eMBox クライアントの内蔵バッチファイルを使う、両者を組み合わせて使う、という方法があります。詳細については、[560 ページの「eMBox コマンドラインクライアントをバッチモードで実行する」](#)を参照してください。

ここではシステムバッチファイルを使う方法を解説します。

### 前提条件

- バッチファイルを自動で実行する方法については、ご使用のオペレーティングシステムのマニュアルまたはサードパーティ製スケジューリングソフトウェアのマニュアルを参照してください。

**注：**NetWare の場合、サードパーティ製ソフトウェアのほか、Novell Support Web サイトで提供している [cron.nlm \(http://support.novell.com/servlet/tidfinder/2939440\)](http://support.novell.com/servlet/tidfinder/2939440) も使えます。

- バックアップ処理を起動するコンピュータに、ファイル eMBoxClient.jar があることを確認してください。

このファイルは、eDirectory の一部としてサーバにインストールされます。それ以外にも、Sun JVM 1.3.1 が動作する環境であれば、eMBoxClient.jar をコピーして動かすことができます。複数サーバ環境でも、ファイアウォール越しのアクセスが可能であれば、1 台のコンピュータから作業できます。詳細については、[555 ページの「eMBox コマンドラインクライアントの使用」](#)を参照してください。

- ロールフォワードログを作成するのであれば、バックアップを行う前にこの機能を有効にしてください。

レプリカリングに属するサーバは、ロールフォワードログ機能を有効にしておく必要があります。バックアップファイルがあっても、ロールフォワードログがなければ復元後の検証処理に失敗し、データベースを開けないことになります。

ロールフォワードログの詳細については、[405 ページの「ロールフォワードログを使用する」](#)を参照してください。また、この機能を有効にする手順については、[426 ページの「eMBox クライアントによるロールフォワードログの設定」](#)を参照してください。

- eDirectory 以外にも追加でバックアップしたいファイルがあれば、それを列挙したインクルードファイルを作っておいてください。

NICI ファイルやストリームファイルもスイッチを使用してバックアップできます。NICI ファイルは常にバックアップするようお勧めします。

それ以外にたとえば autoexec.ncf などをバックアップしたい場合は、そのパスとファイル名をインクルードファイルに列挙します。複数のファイルがある場合はセミコロンで区切ります。改行 (ハードリターン) や空白を含めないようにしてください (例: 「sys:¥system¥autoexec.ncf;sys:¥etc¥hosts;」)。

- eDirectory のバックアップ後すぐに、ファイルシステムのバックアップ作業を行い、テープに保存できるよう準備してください (Backup eMTool による処理では、サーバ上にバックアップファイルができるだけです)。

**ヒント：**コピー先記憶デバイスに容量の制約がある場合は、あらかじめ eDirectory バックアップファイルの最大サイズを設定すると便利です。また、バックアップファイルの作成後、サードパーティ製ファイル圧縮ツールを使う方法もあります。80% 程度は圧縮できます。

- コマンドラインオプションについては、[431 ページの「バックアップ / 復元のコマンドラインオプション」](#)を参照してください。

## 操作手順

- 1 サーバをバックアップするためのシステムバッチファイルを作成します。次のような書式で、1 行に 1 サーバ分のコマンドを記述してください。

Windows、UNIX の場合、通常は次の書式を使用します。

```
java -cp パス/eMBoxClient.jar embox -s サーバ名 -p ポート番号 -u  
ユーザ名 . コンテキスト -w パスワード -t backup.backup -b -f  
バックアップファイルの名前とパス -l バックアップログファイルの名前とパス -u  
インクルードファイルのファイル名とパス -t -w
```

NetWare でも同様ですが、オプション「-nsac」を追加してください。他のプラットフォームでは、このオプションを指定してはいけません。

```
java -nsac -cp パス/eMBoxClient.jar embox -s サーバ名 -p ポート番号 -u  
ユーザ名 . コンテキスト -w パスワード -t backup.backup -b -f  
バックアップファイルの名前とパス -l バックアップログファイルの名前とパス -u  
インクルードファイルのファイル名とパス -t -w
```

具体例とその解説については、[424 ページの「無人バックアップ用システムバッチファイルの例」](#)を参照してください。

毎晩実行するインクリメンタルバックアップにも同様のバッチファイルが使えますが、オプション「-b」を削除し、代わりに「-i」を追加してください。フルバックアップとインクリメンタルバックアップで、保存先バックアップファイル名を異なるものにしておく方がよいでしょう。

指定するポート番号が分からない場合は、[564 ページの「eDirectory ポート番号を確認する」](#)を参照してください。セキュア接続を使用する場合は、[564 ページの「eMBox クライアントを使用してセキュア接続を確立する」](#)を参照してください。eMBox クライアントの内蔵バッチファイルの使い方については、[560 ページの「eMBox コマンドラインクライアントをバッチモードで実行する」](#)を参照してください。

- 2 このバッチファイルを定期的に起動するよう設定します。具体的な設定方法については、オペレーティングシステムまたはサードパーティ製ソフトウェアの資料を参照してください。
- 3 eDirectory のバックアップ後すぐに、ファイルシステムのバックアップ作業を行い、テープに保存できるよう準備してください

Backup eMTool による処理では、サーバ上にバックアップファイルができるだけです。

- 4 バックアップが正常に実行されているか、ログファイルで定期的に確認してください。

## 無人バックアップ用システムバッチファイルの例

次の 2 つの例を紹介します。

- ◆ [424 ページの「NetWare 用のバッチファイル例」](#)
- ◆ [425 ページの「Windows 用のバッチファイル例」](#)

### NetWare 用のバッチファイル例

```
java -nsac -cp sys:%system%embox%eMBoxClient.jar embox -s 10.10.1.200 -p 8008  
-u admin.mycontainer -w mypassword -n -t backup.backup -b -f  
sys:%system%backup%backup.bak -l sys:%system%backup%backup.log -u  
sys:%system%backup%includefile.txt -t -w
```

この例には次のようなオプションが指定されています。

- ◆ NetWare では、コマンド名「java」のすぐ後に「-nsac」を指定します（それ以外のプラットフォームでは指定しないでください）。

**警告:** NetWare サーバでは「-ns」も指定しなければ異常終了します。

「-ns」オプションを使用すると、新規画面が開きます。

これに続く「ac」オプションは、バッチファイルの処理が終了したらこの画面を閉じるよう指定するものです。NetWare のバッチファイルでこれを指定しないと、バックアップ処理のたびにサーバ上に画面が開き、そのまま残ってしまいます。

- ◆ フルバックアップを取る指定 (-b)。
- ◆ インクルードファイルの指定 (-u)。これは必要な場合のみ指定してください。データベース以外にもファイルをバックアップしたい場合に使います。インクルードファイルはあらかじめ用意しておいてください。
- ◆ ストリームファイル (-t) もバックアップされます。
- ◆ 同じ名前のバックアップファイルがあれば上書きする指定 (-w)。

**重要:** 同じバッチファイルを繰り返し実行するなど、同じ名前のバックアップファイルがある場合、「-w」を指定しないと正常にバックアップされません。

バッチモードでは、「-w」の指定がなければ、同じ名前のファイルが存在すると上書きを避けるため処理が中断されてしまいます。なお、対話式モードの場合は、「-w」が指定されていないと、ファイルを上書きしてよいかどうか問い合わせます。

eDirectory のフル/インクリメンタルバックアップの都度、すぐにファイルシステムのバックアップを取っているのであれば、前回のバックアップファイルはテープに保存されているはずですが、したがって上書きしても問題ありません。

- ◆ この例では安全でないポートを指定している (-p 8008) ので、それを考慮して接続するよう、「-n」オプションも指定しています。

## Windows 用のバッチファイル例

```
java -cp c:\%novell%\nds\embox\emBoxClient.jar embox -s myserver -p 8008 -u
admin.myorg -w mypassword -n -t backup.backup -b -f c:\%backup%\backup.bak -u
c:\%backup%\includes\includefile.txt -l c:\%backup%\backup.log -e -t -w
```

この例には次のようなオプションが指定されています。

- ◆ フルバックアップを取る指定 (-b)。
- ◆ インクルードファイルの指定 (-u)。これは必要な場合のみ指定してください。データベース以外にもファイルをバックアップしたい場合に使います。インクルードファイルはあらかじめ用意しておいてください。
- ◆ ストリームファイル (-t) もバックアップされます。
- ◆ 同じ名前のバックアップファイルがあれば上書きする指定 (-w)。

**重要:** 同じバッチファイルを繰り返し実行するなど、同じ名前のバックアップファイルがある場合、「-w」を指定しないと正常にバックアップされません。

バッチモードでは、「-w」の指定がなければ、同じ名前のファイルが存在すると上書きを避けるため処理が中断されてしまいます。なお、対話式モードの場合は、「-w」が指定されていないと、ファイルを上書きしてよいかどうか問い合わせます。

eDirectory のフル/インクリメンタルバックアップの都度、すぐにファイルシステムのバックアップを取っているのであれば、前回のバックアップファイルはテープに保存されているはずですが、したがって上書きしても問題ありません。

- ◆ この例では安全でないポートを指定している (-p 8008) ので、それを考慮して接続するよう、「-n」オプションも指定しています。

注：NetWare 用のバッチファイル例に含まれていた「-ns」または「ac」オプションは、NetWare プラットフォームでのみ指定するべきものです。Windows や UNIX では指定しないでください。

## eMBox クライアントによるロールフォワードログの設定

eMBox クライアントを使って、ロールフォワードログに関する設定を変更することができます。次のような設定ができます。

- ◆ 現在の設定の確認
- ◆ ロールフォワードログ機能の有効 / 無効の切り替え  
レプリカリングに属するサーバは、ロールフォワードログ機能を有効にしておく必要があります。バックアップファイルがあっても、ロールフォワードログがなければ復元後の検証処理に失敗し、データベースを開けないこととなります。
- ◆ ロールフォワードログの保存先ディレクトリの変更
- ◆ ロールフォワードログのファイルサイズの最小値、最大値の設定
- ◆ 現在使用中のログ、既書き出しを終えた最新のログの判別
- ◆ ストリームファイルをロールフォワードログに含めるかどうかの切り替え

ロールフォワードログの詳細については、[405 ページの「ロールフォワードログを使用する」](#)を参照してください。

### 前提条件

- ❑ 設定の変更処理を起動するコンピュータに、ファイル eMBoxClient.jar があることを確認してください。

このファイルは、eDirectory の一部としてサーバにインストールされます。それ以外にも、Sun JVM 1.3.1 が動作する環境であれば、eMBoxClient.jar をコピーして動かすことができます。複数サーバ環境でも、ファイアウォール越しのアクセスが可能であれば、1 台のコンピュータから作業できます。詳細については、[555 ページの「eMBox コマンドラインクライアントの使用」](#)を参照してください。

- ❑ コマンドラインオプションについては、[431 ページの「バックアップ / 復元のコマンドラインオプション」](#)を参照してください。

### 操作手順

- 1 eMBox クライアントを対話式モードで起動します。
  - ◆ NetWare、UNIX の場合：コマンドラインから「**edirutil -i**」と入力します。
  - ◆ Windows：「**ドライブ%novell%nds%edirutil.exe -i**」を実行します。

edirutil ファイルは、eMBox クライアントを実行するためのショートカットです。Java の実行形式ファイルと、eMBox クライアントのインストール先ディレクトリがパラメータとして記述されているほか、NetWare の場合は「-ns」オプションもついています。(Java 実行ファイルの場所は、[557 ページの「ワークステーションで eMBox クライアントを実行する」](#)で示しているように手動で入力することもできます。)

正常に起動されると、「eMBox Client」というプロンプトが現れます。eMBox Client>



- 2** ロールフォワードログの設定を行うサーバにログインします。次のように入力してください。

```
login -s サーバ名またはIPアドレス -p ポート番号 -u ユーザ名 . コンテキスト -w パスワード
```

たとえば Windows の場合、次のようになります。

```
login -s 151.155.111.1 -p 8009 -u admin.mycompany -w mypassword
```

セキュア接続が確立できないというエラーが表示される場合は、**564 ページの「eMBox クライアントを使用してセキュア接続を確立する」**に表示されている JSSE ファイルがシステム上にない可能性があります。

指定するポート番号が分からない場合は、**564 ページの「eDirectory ポート番号を確認する」**を参照してください。

eMBox クライアントはログインが成功したかどうかを表示します。

- 3** (オプション) 次のように入力して、現在の設定を確認します。

```
getconfig
```

オプション指定は必要ありません。

たとえば次のように表示されます。

```
Roll forward log status OFF
Stream file logging status OFF
Current roll forward log directory voll:/rfl/nds.rfl
Minimum roll forward log size (bytes) 104857600
Maximum roll forward log size (bytes) 4294705152
Last roll forward log not used 00000000.log
Current roll forward log 00000001.log
*** END ***
```

- 4** setconfig コマンドで設定を変更します。次のような形式で入力してください。

```
setconfig [-L|-l] [-T|-t] -r ロールフォワードログのパス -n 最小ファイルサイズ -m 最大ファイルサイズ
```

各スイッチの間にはスペースが必要です。スイッチの順序は重要ではありません。

たとえば NetWare の場合、次のようになります。

```
setconfig -L -r rflvolume:¥logs
```

これは、ロールフォワードログ機能を有効にし (-L スイッチ)、その保存先を「rflvolume:¥logs」以下と指定するコマンドです。ロールフォワードログ専用のディスクパーティション/ボリュームを用意するのが最善です。こうしておけば、ディスク容量やアクセス権を監視しやすくなります。ただしこの例では、ストリームファイルのログ機能は有効にしていません。

**警告:** ロールフォワードログ機能を有効にしたら、デフォルトの保存先を使用しないでください。障害対策のためには、eDirectory とは別のディスクパーティション/ボリューム、別の記憶デバイスを指定してください。ロールフォワードログディレクトリは、バックアップ環境設定を変更するサーバ上である必要があります。

**重要:** ロールフォワードログ機能を有効にする場合、ログを保存するボリュームのディスク容量を常に監視してください。これを怠ると、ログの容量は増える一方なので、ディスクパーティション/ボリュームがあふれてしまう恐れがあります。ディスク容量が不足してロールフォワードログを作成できない場合は、eDirectory はそのサーバに対して応答しなくなります。書き出しが終わったロールフォワードログは、定期的にバックアップし、サーバから削除するようお勧めします。**408 ページの「ロールフォワードログのバックアップと削除」**を参照してください。

5 サーバからログアウトするには、次のコマンドを入力します。

**logout**

6 eMBox クライアントを終了するには、次のコマンドを入力します。

**exit**

## eMBox クライアントによるバックアップファイルの復元作業

eMBox クライアントを使ってバックアップファイルに保存されたデータから eDirectory データベースを復元する手順を解説します。手動あるいはバッチ方式で残しておいたバックアップファイルから、データを復元できます。処理結果は所定のログファイルに記録されます。

eMBox クライアントを使えば、iManager では実現できない高度な復元機能も実行できます。詳しくは [431 ページの「バックアップ / 復元のコマンドラインオプション」](#) に、**restore** および **restadv** として解説します。

### 前提条件

- ❑ 復元処理を起動するコンピュータに、ファイル **eMBoxClient.jar** があることを確認してください。

このファイルは、eDirectory の一部としてサーバにインストールされます。それ以外にも、Sun JVM 1.3.1 が動作する環境であれば、**eMBoxClient.jar** をコピーして実行することができます。複数サーバ環境でも、ファイアウォール越しのアクセスが可能であれば、1 台のコンピュータから復元を実行できます。詳細については、[555 ページの「eMBox コマンドラインクライアントの使用」](#) を参照してください。

- ❑ 必要なバックアップファイルをすべて、復元対象サーバ上の、適切なディレクトリに集めておく必要があります。

[409 ページの「復元処理の準備」](#) および [411 ページの「復元に必要なバックアップファイルの収集」](#) を参照してください。

- ❑ 復元対象サーバに eDirectory をインストールし、稼働させておいてください。

たとえば記憶デバイスの障害の場合、デバイスを交換し、改めて eDirectory をインストールすることになります。故障したサーバごと交換する、あるいは単に新しいサーバに移行する場合は、新しいサーバにオペレーティングシステムをインストールした上で、eDirectory も準備します。

- ❑ コマンドラインオプションについては、[431 ページの「バックアップ / 復元のコマンドラインオプション」](#) を参照してください。

- ❑ 復元処理の詳細については、[396 ページの「Backup eMTool による復元作業の概要」](#) を参照してください。

- ❑ (NetWare のみ) ファイルシステムデータおよび eDirectory を復元する際は、ファイルシステム権利を元どおりに戻せるよう、正しい手順で作業してください。

eDirectory を先に復元し、その後でファイルシステムを復元してください。この手順の詳細については、[404 ページの「NetWare のファイルシステムデータを復元する際のアクセス権の保存」](#) を参照してください。



## 操作手順

eMBox クライアントを使って eDirectory データベースを復元する手順を示します。

- 1 必要なバックアップファイルを集めておきます。詳しくは [409 ページの「復元処理の準備」](#) を参照してください。
- 2 eMBox クライアントを対話式モードで起動します。

- ◆ NetWare、UNIX : コマンドラインから「**edirutil -i**」と入力します。
- ◆ Windows : 「**ドライブ\novell\nds\edirutil.exe -i**」を実行します。

edirutil ファイルは、eMBox クライアントを実行するためのショートカットです。Java の実行形式ファイルと、eMBox クライアントのインストール先ディレクトリがパラメータとして記述されているほか、NetWare の場合は「-ns」オプションもついています。(Java 実行ファイルの場所は、[557 ページの「ワークステーションで eMBox クライアントを実行する」](#) で示しているように手動で入力することもできます。)

正常に起動されると、「eMBox Client」というプロンプトが現れます。eMBox Client>

- 3 復元の対象サーバにログインします。次のように入力してください。

```
login -s サーバ名または IP アドレス -p ポート番号 -u ユーザ名 . コンテキスト -w パスワード
```

たとえば Windows の場合、次のようになります。

```
login -s 151.155.111.1 -p 8009 -u admin.mycompany -w mypassword
```

セキュア接続が確立できないというエラーが表示される場合は、[564 ページの「eMBox クライアントを使用してセキュア接続を確立する」](#) に表示されている JSSE ファイルがシステム上にない可能性があります。

指定するポート番号が分からない場合は、[564 ページの「eDirectory ポート番号を確認する」](#) を参照してください。

eMBox クライアントはログインが成功したかどうかを表示します。

- 4 eMBox クライアントのプロンプトが出たら、次のような形式で復元コマンドを入力します。

```
restore -r -a -o -f フルバックアップファイルのパスと名前  
-d ロールフォワードログの場所 -l 復元ログファイルのパスと名前
```

各スイッチの間にはスペースが必要です。スイッチの順序は重要ではありません。「-r」オプションを指定すれば eDirectory データベース自身、指定しなければそれ以外のファイルのみが復元の対象となります。復元処理の終了後、データベースをアクティブにし、オープンしたい場合は、「-a」および「-o」を指定してください。

ロールフォワードログを使って復元する場合は、そのフルパスを指定しなければなりません。これには、eDirectory が自動的に追加するディレクトリ名 (通常は「%nds.rfl」) も含みます。詳しくは [407 ページの「ロールフォワードログの保存先」](#) を参照してください。

例 :

```
restore -r -a -o -f sys:/backup/nds.bak -d voll:/rflidir/nds.rfl -l sys:/backups/backup.log
```

この例では、データベースを復元 (-r) し、その検証が正常終了したらアクティブにし (-a)、オープンする (-o) よう指定しています。「-f」オプションでフルバックアップファイル、「-d」オプションでロールフォワードログの保存先を指定します。また、復元処理の結果を記録するログファイルを、「-l」オプションで指定しています。

これによりフルバックアップファイルからの復元処理が実行され、次にインクリメンタルバックアップファイルの指定を求めるプロンプトが現れます。

- 5** (状況によって実行) インクリメンタルバックアップファイルから復元する場合は、プロンプトに応じて順次、そのパスとファイル名を入力します。

プロンプトには次に指定すべきファイルの ID が表示されます。これはインクリメンタルバックアップファイルのヘッダに記載されているものです。

バックアップ処理が正常終了すれば、その旨の表示が現れます。

- 6** (状況によって実行) 復元処理に失敗した場合は、ログファイルでエラーの原因を確認してください。

復元後の検証に失敗した場合の対処については、[440 ページの「復元後の検証処理に失敗した場合の対処方法」](#)を参照してください。

**注:** レプリカリング中に eDirectory 8.5 より前のバージョンが稼働しているサーバがある場合、復元処理は失敗します。エラーコードは -666、すなわち「DS バージョンの不整合」となります。この場合の対処方法については、[403 ページの「復元後の検証については eDirectory 8.5 以降のみで互換性がある」](#)を参照してください。

- 7** サーバからログアウトするには、次のコマンドを入力します。

```
logout
```

- 8** eMBox クライアントを終了するには、次のコマンドを入力します。

```
exit
```

- 9** (状況によって実行) NICI セキュリティファイルを復元した場合は、NICI を再初期化するため、サーバを再起動します。

- 10** ここでサーバが通常どおり要求に応答することを確認しておきます。

- 11** (状況によって実行) このサーバでロールフォワードログ機能を使うためには、改めて有効に切り替え、障害対策のための書き出し先も設定し直して、ロールフォワードログの環境設定を再作成する必要があります。ロールフォワードログを有効にしてから、改めてフルバックアップも取る必要があります。

この手順が必要となるのは、復元処理の過程で、ロールフォワードログに関する設定はデフォルトに戻るためです。つまり、ロールフォワードログ機能は無効となり、保存先もデフォルトの場所になるからです。フルバックアップが改めて必要となるのは、スケジュールに従って次に無人でのフルバックアップが取られるまでに、再び障害が起こる可能性があるためです。

ロールフォワードログの詳細については、[405 ページの「ロールフォワードログを使用する」](#)を参照してください。

以上で復元作業が終了しました。NICI の再初期化も済んでいるので、暗号化された情報にもアクセスできます。ロールフォワードログ機能を使用する場合は、今後の障害に備えるため、再びこの機能を有効にし、フルバックアップを取っておいてください。

## バックアップ/復元のコマンドラインオプション

eDirectory Backup eMTool のコマンドラインオプションは次の 6 つの機能に分かれています。 **backup**、**restore**、**restadv**、**getconfig**、**setconfig**、および **cancel**。

オプションはどのような順序で指定しても構いません。各オプション間は空白で区切ってください。

| オプション           | 説明   |
|-----------------|--|
| <b>backup</b>   | <b>データベースおよび関連ファイルのバックアップ</b>  |
| -f <b>ファイル名</b> | (必須) バックアップファイルの名前とパス。<br><br>Backup eMTool で作成するバックアップ先ファイル名とパスを指定します。バックアップ対象サーバ上のローカルファイルを指定してください。たとえば「 <code>backup -f vol1:¥backup¥ndsbak.bak</code> 」と指定すると、ファイル <code>vol1:¥backup¥ndsbak.bak</code> にバックアップされます。  |
| -i <b>ファイル名</b> | (必須) ログファイルの名前とパス<br><br>バックアップ処理の結果を出力するログファイルを指定します。   |
| -b              | (オプション) フルバックアップを実行<br><br>eDirectory データベースのフルバックアップを取ります。これがデフォルトの動作で、「-i」も「-c」も指定しなければフルバックアップになります。  |
| -i              | (オプション) インクリメンタルバックアップを実行<br><br>eDirectory データベースのインクリメンタルバックアップを取ります。最後に実施したフル/インクリメンタルバックアップ以降、変化した部分のみをバックアップします。  |
| -t              | (オプション) ストリームファイルもバックアップ<br><br>eDirectory データベースをバックアップする際、ストリームファイルも含める指定です。   |
| -u <b>ファイル名</b> | (オプション) インクルードファイル名およびパス<br><br>バックアップ対象に追加するファイル名を列挙した、インクルードファイルを指定します。eDirectory データベースを復元する際に必要となる重要なファイルをいっしょにバックアップしたい場合、インクルードファイルに列挙しておきます。<br><br>インクルードファイルには各ファイルのフルパスを記述し、末尾にセミコロン (;) を置いてください。たとえば <code>autoexec.ncf</code> および <code>hosts</code> を NetWare サーバのバックアップファイル対象として追加する場合、インクルードファイルは次のようになります。<br><br><code>sys:¥system¥autoexec.ncf;sys:¥etc¥hosts;</code><br><br>ファイルのリストにはスペースまたは改行 (ハードリターン) を使用しないでください。<br><br>指定どおりバックアップされたことは、ログファイルを見るか、バックアップファイルのヘッダを見れば確認できます。(401 ページの「バックアップログファイルの書式」および 397 ページの「バックアップファイルのヘッダ書式」を参照してください。)<br><br><b>警告:</b> バックアップファイルを開く場合でもヘッダを確認するだけにとどめ、保存や変更はしないようにしてください。ファイルの一部が切り捨てられてしまうことがあります。ほとんどのアプリケーションではバイナリデータを正確に保存することはできません。 |

| オプション                                 | 説明  |
|---------------------------------------|---|
| <p><code>-s</code> <b>ファイルサイズ</b></p> | <p>(オプション)バックアップファイルの最大容量(バイト単位)。</p> <p>バックアップファイルの最大容量を、バイト単位で指定します。バックアップファイルを保存する記憶媒体に容量制限がある場合、このオプションで最大容量を指定するとよいでしょう。</p> <p>最大容量に達すると新しいバックアップファイルが生成されます。ファイル名の末尾に、5桁の16進数値を追加した名前になります。この拡張の数字は、新規ファイルが作成されるたびに1ずつ増加します。</p> <p>たとえば「<code>backup -f vol1:/backup/mydib.bak -s 1000000</code>」というコマンドの場合、バックアップファイルの最大容量は1MBになります。If the database is 3.5 MB, this is the resulting set of backup files:</p> <pre>vol1:/backup/mydib.bak (容量は 1 MB) vol1:/backup/mydib.bak.00001 (容量は 1 MB) vol1:/backup/mydib.bak.00002 (容量は 1 MB) vol1:/backup/mydib.bak.00003 (容量は 0.5 MB)</pre> <p>指定できるサイズの下限は約500KBです。バックアップで作成されるファイル数によって、最初のファイルが大きくなる場合があります。</p> <p>最初のバックアップファイルには「<code>number_of_files</code>」タグが追加されます。これはバックアップファイルの総数を表します。上記の例では4となります。さらに、各ファイルのヘッダに、「<code>backup_file</code>」属性が追加されます。これは本来のバックアップファイル名を表します。(詳細については、<a href="#">397 ページの「バックアップファイルのヘッダ書式」</a>を参照してください。)</p> <p>上記の4つのバックアップファイルを使って復元する場合、コマンドは次のようになります。</p> <p><code>restore -f vol1:/backup/mydib.bak -l</code> <i>ログファイルのパスと名前</i></p> <p>ファイルが複数に分かれていることはBackup eMToolによって自動的に認識され、同じディレクトリ内にある、上記の名前のファイルが検索されます。</p> <p><b>ヒント:</b> サードパーティ製の圧縮ツールを使えば、バックアップファイルの容量を小さくすることができます。80%程度は圧縮できます。</p> |
| <p><code>-w</code></p>                | <p>(オプション)同名のバックアップファイルがあれば上書き</p> <p>「<code>-f</code>」オプションで指定されたのと同じ名前のバックアップファイルがあれば、上書きします。この指定がない場合で同名のファイルが存在すると、対話式モードであれば、Backup eMToolは上書きしてよいかどうか確認を求めます。バッチモードでは、「<code>-w</code>」の指定がなければ、同じ名前のファイルが存在すると上書きを避けるため処理が中断されてしまいます。</p> <p>eDirectoryのフル/インクリメンタルバックアップの都度、すぐにファイルシステムのバックアップを取っているのであれば、前回のバックアップファイルはテープに保存されているはずですが、したがって上書きしても問題ありません。</p> <p><b>重要:</b> バッチファイルを使って無人バックアップを行う場合、このオプションを指定してください。同じバッチファイルを繰り返し実行するなど、同じ名前のバックアップファイルがある場合、「<code>-w</code>」を指定しないと正常にバックアップされません。</p> <p>バッチモードでは、「<code>-w</code>」の指定がなければ、同じ名前のファイルが存在すると上書きを避けるため処理が中断されてしまいます。なお、対話式モードの場合は、「<code>-w</code>」が指定されていないと、ファイルを上書きしてよいかどうか問い合わせます。</p>   |

| オプション           | 説明  |
|-----------------|---|
| -c              | <p>(オプション) コールドバックアップを実行</p> <p>フルバックアップと同様ですが、いったんデータベースを停止してから実行します。「-o」または「-o-d」が指定されている場合を除き、処理終了後、データベースは再びオープンされます。</p>   |
| -o              | <p>(オプション) コールドバックアップ後、データベースを停止したままにする</p> <p>「-c」を指定した場合にのみ指定できます。コールドバックアップの終了後、データベースを停止したままにします。この機能は、ハードウェアをアップグレードする、あるいは新規サーバ(同じオペレーティングシステムが動作するもの)に移行する場合に有用です。詳しくは <a href="#">536 ページの「ハードウェアのアップグレードやサーバの交換」</a> を参照してください。</p>  |
| -d              | <p>(オプション) コールドバックアップ後、DS エージェントを無効にする</p> <p>「-c-o」を指定した場合にのみ指定できます。コールドバックアップ後、DS エージェントを無効にします。この機能は、ハードウェアをアップグレードする、あるいは新規サーバ(同じオペレーティングシステムが動作するもの)に移行する場合に有用です。詳しくは <a href="#">536 ページの「ハードウェアのアップグレードやサーバの交換」</a> を参照してください。</p> <p>擬似サーバの「login disabled」属性を設定することにより、DS エージェントを無効にします。その結果、eDirectory を起動しようとすると「-663」エラーが発生します。</p> |
| <b>restore</b>  | <b>データベースおよび関連ファイルの復元</b>   |
| -f <b>ファイル名</b> | <p>(必須) バックアップファイルの名前とパス。</p> <p>復元に使うフルバックアップファイルを指定します。このファイルは復元対象サーバ上に置いておかなければなりません。たとえば「restore -f vol1:/backup/ndsbak.bak」と指定すると、ファイル vol1:/backup/ndsbak.bak から復元されます。</p> <p>複数のファイルに分かれている場合は、すべて同じディレクトリ内に集めておいてください。</p>   |
| -l <b>ファイル名</b> | <p>(必須) ログファイルの名前とパス</p> <p>復元処理の結果を出力するログファイルを指定します。</p>   |
| -r              | <p>(オプション) DIB セットも復元。</p> <p>eDirectory データベースを復元する旨の指定です。</p> <p><b>警告:</b> このオプションを指定しなかった場合、eDirectory データベース自身は復元されません。指定した種類以外のファイルのみが復元の対象になります。</p>   |

| オプション              | 説明   |
|--------------------|--|
| -d ディレクトリ名 (オプション) | <p>ロールフォワードログのあるディレクトリ</p> <p>ロールフォワードログを集めたディレクトリを指定します。復元対象サーバ上のフルパスで指定してください。必要なロールフォワードログをすべて、作成時と同じファイル名にして、ひとつのディレクトリに集めておかなければなりません。</p> <p>バックアップファイルからの復元後、ロールフォワードログを使って、バックアップ時点以降の変更を反映させます。「-d」オプションの指定がなければ、バックアップ時にロールフォワードログ機能を有効にしている場合でも、Backup eMTool はログファイルを参照しません。</p> <p>最初に適用すべきロールフォワードログは、最新のバックアップファイルをテキストエディタで開き、「backup」タグの「current_log」属性を見れば確認できます。ここでいう最新のバックアップファイルとは、「-f」オプションで指定するフルバックアップファイルか、または復元処理で適用することになる最後のインクリメンタルバックアップファイルです。ヘッダに記述される属性について詳しくは、<a href="#">397 ページの「バックアップファイルのヘッダ書式」</a>を参照してください。</p> <p><b>警告:</b> バックアップファイルを開く場合でもヘッダを確認するだけにとどめ、保存や変更はしないようにしてください。ファイルの一部が切り捨てられてしまうことがあります。ほとんどのアプリケーションではバイナリデータを正確に保存することはできません。</p> |
| -u                 | <p>(オプション) インクルードファイルに列挙されたファイルも復元</p> <p>データベースに追加する形でバックアップしていたファイルも復元します。</p> <p>バックアップの過程で、データベース以外にもバックアップが必要なファイルを列挙したファイルを作成し、インクルードファイルとして指定することもできます。しかしその場合でも、「-u」オプションで指定しなければ復元されません。</p>  |
| -a                 | <p>(オプション) 検証後、DIB をアクティブにする指定。</p> <p>復元後の検証処理が正常終了したら、データベース名を RST から NDS に変更します。この処理については、<a href="#">396 ページの「Backup eMTool による復元作業の概要」</a>を参照してください。</p>  |
| -o                 | <p>(オプション) 処理終了後、データベースをオープンする</p> <p>復元作業が終了したら、自動的にデータベースをオープンする指定です。検証処理が正常終了すれば、データベースが自動的に開きます。失敗した場合は、復元前のデータベースが開きます。この処理については、<a href="#">396 ページの「Backup eMTool による復元作業の概要」</a>を参照してください。</p>   |
| -n                 | <p>(オプション) 復元後にデータベースを検証しない</p> <p>復元後の検証処理を省略して Backup eMTool で復元します。このサーバの遷移ベクトルをレプリカリングに属する他のサーバと比較する、という検証処理を行いません。遷移ベクトルについて詳しくは、<a href="#">403 ページの「遷移ベクトルと復元後の検証処理」</a>を参照してください。他のオプションで明示的に指定されていない限り、RST から NDS への改名もしません。</p> <p><b>重要:</b> Novell の担当者から指示を受けた場合を除き、このオプションはお勧めできません。</p>   |
| -v                 | <p>(オプション) 上書きして復元</p> <p>検証処理を行うことなく、データベース名を RST から NDS に変更します。</p> <p><b>重要:</b> Novell の担当者から指示を受けた場合を除き、このオプションはお勧めできません。</p>   |



| オプション     | 説明   |
|-----------|--|
| -k        | (オプション) データベースのロックを解除<br>NDS データベースのロックを解除します。   |
| restadv   | 高度な復元機能。(注意: これを実行する際は、DS エージェントがクローズされます。)  |
| -l ファイル名  | (必須) ログファイルの名前とパス<br>復元処理の結果を出力するログファイルを指定します。   |
| -o        | (オプション) 処理終了後、データベースをオープンする<br>復元作業が終了したら、自動的にデータベースをオープンする指定です。検証処理が正常終了すれば、データベースが自動的に開きます。失敗した場合は、復元前のデータベースが開きます。この処理については、 <a href="#">396 ページの「Backup eMTool による復元作業の概要」</a> を参照してください。  |
| -n        | (オプション) 前に失敗した復元の検証処理を起動<br>前に復元して検証に失敗した RST データベースを再度検証します。  |
| -m        | (オプション) 復元された DIB ファイルの削除<br>RST データベースが存在すれば削除します。  |
| -v        | (オプション) 上書きして復元<br>検証処理を行うことなく、データベース名を RST から NDS に変更します。<br><b>重要:</b> Novell の担当者から指示を受けた場合を除き、このオプションはお勧めできません。  |
| -k        | (オプション) データベースのロックを解除<br>NDS データベースのロックを解除します。   |
| getconfig | ロールフォワードログに関する現在の設定を表示。<br>指定できるオプションはありません。<br>現在の設定を表示します。たとえばロールフォワードログ機能が無効になっている場合、getconfig コマンドでは次のような情報が表示されます。<br><pre>Roll forward log status OFF Stream file logging status OFF Current roll forward log directory voll:/rfl/nds.rfl Minimum roll forward log size (bytes) 104857600 Maximum roll forward log size (bytes) 4294705152 Last roll forward log not used 00000000.log Current roll forward log 00000001.log *** END ***</pre> |
| setconfig | ロールフォワードログに関する設定の変更。   |

| オプション | 説明   |
|-------|--|
| -L    | <p>(オプション) ロールフォワードログ機能の有効化。</p> <p>ロールフォワードログ機能を有効にします。(デフォルトでは無効。)この機能を有効にしておけば、停止する直前の状態にまでサーバを復元できるようになります。無効のままであれば、最後のフル/インクリメンタルバックアップ時点までしか復元できません。</p> <p>レプリカリングに属するサーバについては、ロールフォワードログ機能を有効にして、他のサーバとの同期状態も復元できるようにしてください。</p> <p>ただし管理者にとっては、監視しなければならない対象が増えます。これを怠ると、ログの容量は増える一方なので、ディスクパーティション/ボリュームがあふれてしまう恐れがあります。ディスク容量が不足してロールフォワードログを作成できない場合は、eDirectoryはそのサーバに対して応答しなくなります。定期的にバックアップを取り、使わなくなったログは削除する必要があります。<a href="#">408 ページの「ロールフォワードログのバックアップと削除」</a>を参照してください。</p> <p>詳細については、<a href="#">405 ページの「ロールフォワードログを使用する」</a>を参照してください。</p> |
| -I    | <p>(オプション) ロールフォワードログ機能の無効化。</p> <p>ロールフォワードログ機能を無効にします(デフォルトでは無効)。データベースでは連続したログを保存していくのをやめ、現在のファイルに上書きしていくようになります。ロールフォワードログ作成がオフの場合、最後にフル/インクリメンタルバックアップを実行した時点までしかデータベースを復元できません。</p> <p>誤って無効にしてしまった場合、ただちに有効にすると同時に、今障害が起っても復元できるよう、改めてデータベースのバックアップを取ってください。</p> <p>詳細については、<a href="#">405 ページの「ロールフォワードログを使用する」</a>を参照してください。</p>   |
| -T    | <p>(オプション) ストリームファイルのログ出力開始</p> <p>(ロールフォワードログ機能が有効な場合のみ) ストリームファイルが更新された場合、その全体をロールフォワードログにコピーするようになります。ストリームファイルとは、ログインスクリプトなど、データベースに関する追加の情報ファイルのことです。</p> <p>ただしストリームファイルを記録すると、ディスクの空き容量が急速に減少します。ログの出力先ディスクパーティション/ボリュームの空き容量を、常に監視するようにしてください。ディスク容量が不足してロールフォワードログを作成できない場合は、eDirectoryはそのサーバに対して応答しなくなります。</p>   |
| -t    | <p>(オプション) ストリームファイルのログ出力停止</p> <p>ストリームファイルが更新されても、その全体をロールフォワードログにコピーしないようになります。この場合でも、フル/インクリメンタルバックアップの際には、ストリームファイルもバックアップできます。ストリームファイルを頻繁に更新しないのであれば、それでも充分でしょう。</p> <p>ストリームファイルを記録しないと、ログファイルの容量が急速に増えるのを抑えることにもなります。</p>   |



| オプション      | 説明   |
|------------|--|
| -r ディレクトリ名 | <p>(オプション) ロールフォワードログの出力先ディレクトリの設定。</p> <p>ロールフォワードログの出力先ディレクトリを指定します。たとえば「setconfig -r vol2:¥rfi」というコマンドを実行すると、vol2:¥rfi 以下にディレクトリが作成され、その下にログファイルができるようになります。</p> <p>このディレクトリ名は現在の eDirectory データベース名に基づいて決まります。通常はデータベース名が「NDS」なので、ログ保存先ディレクトリは「vol2:¥rfi¥nds.rfi」となります。ここでデータベース名を「ND1」に変更すると、保存先もこれに合わせて「vol2:¥rfi¥nd1.rfi」以下に変わります。</p> <p>現在の保存先設定は getconfig コマンドで確認できます。</p> <p>保存先の設定を変えるとその時点で新しいディレクトリができますが、ログファイルは実際にトランザクションが発生するまで作成されません。</p> <p><b>重要:</b> バックアップツールでは、ログの保存先ディレクトリが変わったことを認識できません。データベースを復元する際には、最後のバックアップ以降のロールフォワードログをすべて、ひとつのディレクトリに集めておく必要があります。</p> <p>詳細については、<a href="#">405 ページの「ロールフォワードログを使用する」</a>を参照してください。</p> |
| -n ファイルサイズ | <p>(オプション) ロールフォワードログの最小容量の設定</p> <p>ロールフォワードログの最小容量をバイト単位で指定します。この容量に達した後、実行中のトランザクションが終了すると、ログ出力先が新しいファイルに切り替わります。</p>   |
| -m ファイルサイズ | <p>(オプション) ロールフォワードログの最大容量の設定</p> <p>ロールフォワードログの最大容量をバイト単位で指定します。この上限に達してもトランザクションが進行中の場合は、トランザクションは次のファイルに続けて記録されます。この設定は最小サイズの設定より常に大きくする必要があります。</p>  |
| -s         | <p>(オプション) ログ出力先ファイルの強制切り替え</p> <p>実行中のトランザクションが終了した時点で、ログ出力先を新しいファイルに切り替えます。次のトランザクション開始時に新しいファイルが作成されます。</p>   |
| cancel     | <p>バックアップ/復元処理を取り消します。指定できるオプションはありません。</p>  |

## NetWare で DSBK.NLM を使用する

DSBK は、Backup eMTool と同じ操作を実行する簡易なコマンドラインパーサです。ただし、DSBK では最初にログインすることなく、サーバコンソールからバックアップを実行するか、役割ベースサービスを設定することができます (555 ページの第 18 章「eDirectory Management Toolbox」を参照)。Backup eMTool と同じコマンドラインオプションを使用してサーバ上の NLM として実行します。このユーティリティは、サーバ上の NCF ファイルを使用したスクリプトバックアップでも使用できます。

**重要:** DSBK がインクリメンタルバックアップを復元することはありません。DSBK はフルバックアップの復元のみ使用できます。

DSBK 操作が完了すると、操作の結果がファイル (dsbk.err) に書き込まれます。この dskb.err は、プログラムを使用して開き、その内容を表示することができます。操作時にエラーが発生した場合は、このファイルの最初の 4 バイトにエラーコードが記録されます。エラーが発生しなかった場合、このファイルの最初の 4 バイトには 0 が記録されます。

dsbk.nlm を使用するには、次の操作を行います。

- 1 eDirectory 8.7.3 IR3 (<http://support.novell.com/cgi-bin/search/searchtid.cgi?/2969860.htm>) をダウンロードし、インストールします。

- 2 dskb.nlm が sys:¥system ディレクトリにあることを確認します。

DSBK は、backupcr.nlm と同じディレクトリに格納されている必要があります。backupcr.nlm は、すべてのバックアップ / 復元機能を含むコアライブラリです。このライブラリにはユーザインタフェースはなく、DSBK ユーティリティから動的にロード、リンクされる形で動作します。

- 3 サーバコンソールで、431 ページの「バックアップ / 復元のコマンドラインオプション」に示されているいずれかのオプションとともに次のコマンドを実行します。

```
load dskb
```

## サーバ固有情報のバックアップに関する変更事項 (NetWare のみ)

NetWare 用インストールでは、多くの場合、サーバ固有情報もバックアップするようになっています。eDirectory 8.6 以降、eDirectory スキーマの構造が変更になりました。eDirectory 8.7 でも、さらに多くの変更が施されています。その結果、ファイルシステム TSA やサードパーティ製バックアップツールを使ってサーバ固有情報をバックアップしていた場合、そのままでは使えなくなりました。代わりに追加された Backup eMTool の「ホットバックアップ」機能を iManager から呼び出すか、または eMBox クライアントで実行するようにしてください。ファイルシステム TSA を使ってサーバ固有情報をバックアップする機能は、現在のバージョンからは削除されました。eDirectory 8.7.3 では、該当機能が「ホットバックアップ」に組み込まれています。従来と同様、ファイルシステム TSA では、dsbacker.nlm を呼び出してバックアップファイルを作成しています。しかし現在は、dsbacker.nlm が内部的に backupcr.nlm を起動し、これがさらに Backup eMTool の機能を呼び出すという形で実装されています。

NetWare および eDirectory のバージョンに応じて、次のようにバックアップ / 復元処理を行うようお勧めします。

| eDirectory のバージョン | NetWare のバージョン                                       | 推奨するバックアップ / 復元方法   |
|-------------------|--|---|
| 8.6 以前            | すべてのバージョン  | <p>ファイルシステム TSA を使ってサーバ固有情報 (SSI) を復元する場合 :</p> <ul style="list-style-type: none"> <li>停止したサーバに関連づけられているボリュームオブジェクト、サーバオブジェクトを削除しないでください。</li> <li>具体的な手順については Novell の担当者にお問い合わせください。</li> </ul> |
| 8.7               | 5.1 & 6.0  | <p>バックアップ / 復元には Backup eMTool のみを使用。</p> <p>( ファイルシステム TSA でバックアップしても復元できません。 )</p>  |
| 8.7.1 以降          | 5.1  | <p>バックアップ / 復元には Backup eMTool のみを使用。</p> <p>( ファイルシステム TSA で SSI をバックアップしても復元できません。 )</p>  |
| 8.7.1 以降          | 6.0 (SP3 を適用済み)<br>(eDirectory 8.7.1 を動かすには SP3 が必要) | Backup eMTool、ファイルシステム TSA、サードパーティ製ツールのいずれかを使用。復元処理は Backup eMTool で実行できます。   |

NetWare 6.0 上で eDirectory 8.7.1 を動かす場合、サーバ固有情報で大きく変わったのは次のような事項です。

- ◆ **ファイル長の増大** : 以前の SSI バックアップでは、データベースの一部しか対象になりませんでした。新バージョンでは、サーバ上のディレクトリオブジェクトに関する情報をすべてバックアップするようになったため、ファイル長も増大し、データベースそのものと同容量になります。
- ◆ **ユーザ定義ファイルの場所** : 以前は sys:system ディレクトリにファイル servedata.nds が生成されるだけでした。容量が小さかったため、テープにコピーするまでこのディレクトリに置いておいても問題が生じなかったのです。eDirectory 8.7.3 では、ファイルシステム TSA でデータベースのフルバックアップが可能になりました。生成されるファイルは 3 つに増えています。そのうち ssiback.bak の保存位置は、ユーザが設定できます。

| ファイル        | 説明   | 場所  |
|-------------|--|---|
| ssiback.bak | Backup eMTool で生成されるフル「ホットバックアップ」ファイルと同じです。 <a href="#">393 ページの「eDirectory Backup eMTool について」</a> を参照してください。 | <p>ユーザ定義可能。デフォルトでは sys:system になっています。</p> <p>ファイル容量が大きいので、sys : 以外のボリュームに変更するようお勧めします。</p> |

| ファイル        | 説明   | 場所         |
|-------------|--|------------|
| ssiback.ini | ファイル ssiback.bak を書き出すパスを記述したテキストファイル。デフォルトでは「sys:system」となっています。<br><br>例：<br>vol1:/backups/ssibackup.bak         | sys:system |
| ssiback.log | 前回までのバックアップ状況を分かりやすく出力したログファイルです。このログファイルにはすべてのバックアップ履歴、バックアップの開始および終了時刻、およびバックアッププロセス中に発生した考えられるエラーについての情報が含まれます。 | sys:system |

- ◆ **Backup eMTool** による復元処理：サーバ固有情報は Backup eMTool でしか復元できません。

## 復元後の検証処理に失敗した場合の対処方法

復元処理の一環として検証を行います。復元された eDirectory データベースと、レプリカリングに属する他のサーバとの間で、遷移ベクトルを比較するというものです。復元処理の詳細については、[396 ページの「Backup eMTool による復元作業の概要」](#)および [403 ページの「遷移ベクトルと復元後の検証処理」](#)を参照してください。

遷移ベクトルが合致しなければ、検証に失敗したことになります。これは一般に、復元処理に使ったファイルのデータが不足していたことを表します。たとえば次のような状況が考えられます。

- ◆ 最後にバックアップを実施した後、ロールフォワードログ機能を有効にしていなかった場合。
- ◆ ロールフォワードログを取っていたのに、復元の際これを使わなかった場合。
- ◆ ロールフォワードログが不足していた場合。

**注：**このほか、レプリカリング中に、8.5 より古い eDirectory が稼動するサーバがある場合にも、検証に失敗します。この場合の対処方法については、[403 ページの「復元後の検証については eDirectory 8.5 以降のみで互換性がある」](#)を参照してください。

デフォルトでは、復元した eDirectory データベースが他のレプリカと整合が取れていない場合、そのままではオープンできません。

バックアップファイルやロールフォワードログの指定を単に忘れてただけであれば、正しく指定してもう一度復元処理を実行すればよいはずですが、次回に復元が成功すれば、検証に成功し、データベースがオープンされるでしょう。

必要なバックアップファイルやロールフォワードログが揃っていない場合は、以下の手順でサーバを復旧してください。検証に失敗したときの復旧手順の概要を説明します。

- ◆ サーバの識別情報やファイルシステム権利は、バックアップファイルなどが不足していても復旧できるはずですが。
- ◆ バックアップからレプリカを復元できない場合でも、サーバとしては動作します。新しいレプリカが追加されたものとして扱われ、他のサーバにも影響を及ぼしてしまうのです。したがって、レプリカリングからいったんサーバを外し、高度な復元機能や DSRRepair ツールを使って元の状態に復旧してから、改めてレプリカリングに追加してください。

- ◆ このサーバにしかデータがない、すなわち他のサーバにレプリカが作られていないパーティションについては、残念ながら復元できません。

このセクションの説明により、検証に失敗した後、サーバの識別情報やファイルシステム権利を復旧し、レプリカリングからいったん外し、再び追加します。この手順でレプリケーションが終了すれば、サーバは元どおりに機能するようになるはずですが、ただしレプリカを作っていないために復元できなかったパーティションを除きます。

まず、[441 ページの「レプリカリングをクリーンアップする」](#)に従って作業してください。それが終了したら [442 ページの「サーバの復旧とレプリカの再追加」](#)に進みます。

## レプリカリングをクリーンアップする

この手順では、次の方法について説明します。

- ◆ **マスタレプリカの再割り当て。**障害が発生したサーバが、あるパーティションのマスタレプリカを保持していた場合は、DSRepair を使って、レプリカリストに属する他のサーバ上のレプリカを、マスタとして扱うよう指定します。
- ◆ **障害が発生したサーバに対するレプリカリストの参照の削除。**障害が発生したサーバを含むレプリカリングのメンバーである各サーバに対して、障害が発生したサーバが利用できなくなったことを通知する必要があります。

### 前提条件

- eDirectory そのものは、当該サーバに正常にインストールされているものとします。
- 復元を試み、検証処理で失敗したことが前提です。
- NDS データベースは稼動しており、(復元処理により作成された) RST データベースも残っているものとします。
- どのパーティションのレプリカがこのサーバに保持されていたか、は分かっているものとします。このサーバのレプリカはバックアップファイルのヘッダ部に記録されています。

### 操作手順

レプリカリングをクリーンアップするには、次の操作を行います。

- 1 DSRepair を起動します。復元対象サーバとレプリカを共有しているサーバのコンソールから、次のオプションを指定して起動してください。
  - ◆ NetWare、Windows の場合 : 「-a」 オプション。
  - ◆ UNIX の場合 : 「-Ad」 オプション。

上記のオプションについて詳しくは、[285 ページの「DSRepair の詳細オプション」](#)を参照してください。

**警告:** 「-a」 オプション、「-Ad」 オプションを指定して DSRepair を実行すると、ツリー構造が損なわれることがあります。これらのオプションの詳細については、[Novell Support Web site, Solution 2938493 \(http://support.novell.com/servlet/tidfinder/2938493\)](#) を参照してください。

- 2 レプリカ操作とパーティション操作の選択。
- 3 編集したいパーティションを選択します。このパーティションが属するレプリカリングから、障害の起こったサーバを外すこととなります。
- 4 [レプリカリングの表示] を選択して、このパーティションに関するレプリカを持つサーバのリストを表示します。
- 5 (状況によって実行) 当該サーバにマスタレプリカがあった場合、[このサーバを新しいマスタレプリカに設定] コマンドで、他のサーバにマスタを切り替えます。

この時点で、対象のレプリカリングは新しいマスタレプリカを保持しています。リングを構成するすべてのレプリカに対して、新しいマスタが存在することが通知されます。
- 6 そのまましばらく待ちます。上記のレプリカがマスタになったことが他のサーバに認識されるまで、しばらく待ちます。
- 7 [レプリカリングの表示] 画面に戻ります。障害の起こったサーバを選択して、[レプリカリングからのサーバの削除] を実行してください。

DSRepair を起動する際に「-a」または「-Ad」(プラットフォームにより選択) を指定していなかった場合、このコマンドは表示されません。

**警告:** 障害の起こったサーバをマスタレプリカに設定したままで、このコマンドを実行しないでください。リング内のサーバリストを見れば確認できます。マスタレプリカであれば、[ステップ 5](#) を参照して、他のサーバにマスタを切り替えてから、当該サーバをレプリカリングから外します。
- 8 管理者としてログインします。
- 9 説明メッセージを読み、それに対する同意を入力して処理を続行します。
- 10 DSRepair を終了します。

レプリカリングを構成するすべてのサーバに通知が行われます。
- 11 障害が発生したサーバを含んでいる各レプリカリングごとに、1つのサーバ上で、この手順を繰り返します。

続いて、障害が生じたサーバ上に、新たにレプリカを構築します。[442 ページの「サーバの復旧とレプリカの再追加」](#)に進んでください。

## サーバの復旧とレプリカの再追加

レプリカ設定を「外部参照」側書き替え、自分自身はレプリカリングに属していないものとして動作するようにします。その上でサーバからレプリカを削除すると、データベースのロックを解除できるようになります。

レプリカを削除すれば、レプリカをサーバに再追加する作業は終わりです。あとは自動的に、他のサーバから各レプリカの最新版を参照し、再追加していきます。各レプリカが再追加されたら、サーバは元と同じように機能するはずですが。

DSRepair を使用してレプリカを削除し、レプリケーション機能により再追加する手順を次に示します。

- 1 [441 ページの「レプリカリングをクリーンアップする」](#) が完了していることを確認します。



**2** eMBox クライアントの高度な復元機能を使って、上書き復元処理を行います。

**2a** eMBox クライアントを対話式モードで起動します。

- ◆ NetWare、UNIX : コマンドラインから「**edirutil -i**」と入力します。
- ◆ Windows : 「**ドライブ¥novell¥nds¥edirutil.exe -i**」を実行します。

edirutil ファイルは、eMBox クライアントを実行するためのショートカットです。Java の実行形式ファイルと、eMBox クライアントのインストール先ディレクトリがパラメータとして記述されているほか、NetWare の場合は「-ns」オプションもついています。(Java 実行ファイルの場所は、557 ページの「**ワークステーションで eMBox クライアントを実行する**」で示しているように手動で入力することもできます。)

正常に起動されると、「eMBox Client」というプロンプトが現れます。eMBox Client>

**2b** 復元の対象サーバにログインします。次のように入力してください。

**login -s サーバ名または IP アドレス -p ポート番号 -u ユーザ名 . コンテキスト -w パスワード**

たとえば Windows の場合、次のようになります。

**login -s 151.155.111.1 -p 8008 -u admin.mycompany -w mypassword**

セキュア接続が確立できないというエラーが表示される場合は、564 ページの「**eMBox クライアントを使用してセキュア接続を確立する**」に表示されている JSSE ファイルがシステム上にない可能性があります。

指定するポート番号が分からない場合は、564 ページの「**eDirectory ポート番号を確認する**」を参照してください。

eMBox クライアントはログインが成功したかどうかを表示します。

**2c** 上書き復元コマンドを、次のように実行します。併せてログファイル名も指定してください。

**restadv -v -l ログファイル名**

高度な復元機能により、RST データベース (復元したけれども検証に失敗したもの) の名前を NDS に変更します。ただしロックは解除しません。

**3** サーバコンソールで、DSRepair の高度な復元機能により、レプリカ設定をすべて外部参照に切り替えます。

- ◆ NetWare : 「**dsrepair -XK2 -rd**」というコマンドを実行してください。
- ◆ Windows : [スタート] > [設定] > [コントロールパネル] > [Novell eDirectory サービス] の順にクリックします。dsrepair.dlm を起動します。[起動パラメータ] フィールドに、「**-XK2 -rd**」と入力します。[開始] をクリックします。
- ◆ UNIX : 「**ndsrepair -R -Ad -xk2**」と入力します。

オプション「-rd」、「-R」は、ローカルデータベースとレプリカを修復する旨の指定です。


**警告** : DSRepair による高度な復元機能は、正しく使用しないとツリーが破損することがあります。これらのオプションの詳細については、[Novell Support Web site, Solution 2938493](http://support.novell.com/servlet/tidfinder/2938493) (<http://support.novell.com/servlet/tidfinder/2938493>) を参照してください。

**4** 修復が終了したら、ロックを解除してデータベースを開きます。次のように実行してください。

**restadv -o -k -l ログファイル名**

「-o」 オプションはデータベースのオープン、「-k」 オプションはロック解除を表します。

**5** iManager を使って、修復されたサーバをレプリカリングに再追加します。

**5a** Novell iManager で、[役割およびタスク] ボタン  をクリックします。

**5b** [パーティションとレプリカ] > [レプリカビュー] の順にクリックします。

**5c** レプリカを作成したいパーティションの名前とコンテキストを指定し、[OK] ボタンを押します。

**5d** [レプリカの追加] をクリックします。

**5e** [サーバ名] フィールドの横にある [参照] ボタン  をクリックし、修復されたサーバを選択します。

**5f** レプリカのタイプを選択して、[OK] をクリックし、[完了] をクリックします。

**5g** このサーバが属していた各レプリカリングについて、上記の操作を繰り返します。

**6** レプリケーション処理が終わるまでしばらく待ちます。

レプリカの状態が [新規] から [オン] に変われば、レプリケーション処理は終了です。これは iManager で確認できます。詳細については、[147 ページの「レプリカに関する情報を表示する」](#)を参照してください。

**7** NCI セキュリティファイルを復元した場合は、復元完了後に NCI を再初期化するため、サーバを再起動します。

**8** (状況によって実行) このサーバでロールフォワードログ機能を使うためには、改めて有効に切り替え、障害対策のための書き出し先も設定し直して、ロールフォワードログの環境設定を再作成する必要があります。ロールフォワードログを有効にしてから、改めてフルバックアップも取る必要があります。

この手順が必要となるのは、復元処理の過程で、ロールフォワードログに関する設定はデフォルトに戻るためです。つまり、ロールフォワードログ機能は無効となり、保存先もデフォルトの場所になるからです。フルバックアップが改めて必要となるのは、スケジュールに従って次に無人でのフルバックアップが取られるまでに、再び障害が起こる可能性があるためです。

ロールフォワードログの詳細については、[405 ページの「ロールフォワードログを使用する」](#)を参照してください。

## バックアップ / 復元の運用例

- ◆ [445 ページの「シナリオ：単一サーバ構成のネットワークで、eDirectory を格納しているハードディスクが故障した場合」](#)
- ◆ [446 ページの「シナリオ：複数サーバ構成のネットワークで、eDirectory を格納しているハードディスクが故障した場合」](#)
- ◆ [448 ページの「シナリオ：複数サーバ構成のネットワークで、1 台のサーバが完全に使えなくなった場合」](#)
- ◆ [449 ページの「シナリオ：複数サーバ構成のネットワークで、数台のサーバが使えなくなった場合」](#)
- ◆ [449 ページの「シナリオ：複数サーバ構成のネットワークで、すべてのサーバが使えなくなった場合」](#)



## シナリオ：単一サーバ構成のネットワークで、eDirectory を格納しているハードディスクが故障した場合

あるユーザは Stationery Supply 社で単一サーバ構成のネットワークを管理しています。サーバは 1 台しかないので、レプリカ機能で障害に備えるわけにはいきません。その場合、eDirectory 8.7.3 に組み込まれた新ツール Backup eMTool を使えば、eDirectory のバックアップ/復元処理が容易になります。サーバ単位で処理を行う方式であり、しかも高速だからです。

これまで Windows NT Server で eDirectory 8.6.2 を稼働させていましたが、8.7.3 にアップグレードした結果、Backup eMTool を起動するバッチファイルを用意し、定期的に無人でバックアップを行えるようになりました。

毎週日曜の夜にフルバックアップを取り、さらに平日は毎晩、インクリメンタルバックアップを取るようになりました。また、eDirectory の無人バックアップのすぐ後に、ファイルシステムのフル/インクリメンタルバックアップを取るようになります。バックアップテープには、ファイルシステムデータのほか、eDirectory の最新バックアップも保存されることになります。さらに、データ保存サービス会社と契約して、バックアップテープを社外に保管することになりました。

毎週月曜日の朝、バックアップログを調べて、正常にフルバックアップが取れていることを確認します。また、普段から時々、インクリメンタルバックアップの状況をログで調べています。

ロールフォワードログの機能は無効にしています。それは次のような理由によります。

- ◆ サーバには独立した記憶デバイスがついていないので、ロールフォワードログを有効にしてもバックアップとしては役に立ちません。記憶デバイスが故障すれば、eDirectory ばかりでなくログも消えてしまうので、いずれにしても復元には使えません。
- ◆ ツリー構成が変わることはあまりありません。また、障害が発生しても、前の晩の状態にまで復元できれば充分だと考えています。停止直前の状態まで eDirectory を復元できなくても構いません。
- ◆ サーバはレプリカリングに属して他のサーバと連携しているわけではないため、ロールフォワードログがなくても、復元後の検証処理には成功するはずですが。

Stationery Supply 社では、人事異動などによりツリー構成を大きく変える場合は、その直前と直後に、手動でバックアップすることにしています。日曜日以外でも、必要に応じて臨時のバックアップを取ろうというわけです。これがロールフォワードログに代わる措置です。

必要になればいつでもバックアップ作業ができるよう、時々テストして確かめています。テスト用にもう 1 台サーバを購入する予算はないので、市内にあるサービス会社と契約し、必要なときだけサーバを使わせてもらえるようにしました。実機と似た構成のサーバにオペレーティングシステムをインストールし、eDirectory データベースの環境もできるだけ同じように構築します。このサーバに、実機から取ったバックアップファイルを使って復元し、想定どおりに復元されていることを確認するのです。

ある水曜日の朝、eDirectory が格納されたハードディスクの故障が見つかりました。そこで新しいハードディスクを手配したほか、日曜日にとったフルバックアップファイル、月曜日および火曜日にとったインクリメンタルバックアップファイルを用意しました。次に、ハードディスクを交換し、eDirectory をインストールしました。その上に、フル/インクリメンタルバックアップファイルから復元しました。水曜日の朝、故障が起こる前にツリー構成を変更しましたが、これは復元できませんでした。ロールフォワードログを残しておかなかったからです。しかし火曜日夜の状態まで復元できたことで満足しています。ロールフォワードログを取るための管理の手間を考えれば、許容できる範囲だと考えているからです。

## シナリオ：複数サーバ構成のネットワークで、eDirectory を格納しているハードディスクが故障した場合

あるユーザが Outdoor Recreation 社で eDirectory が稼動する 10 台のサーバを管理しています。毎週日曜の夜にフルバックアップを取り、さらに平日は毎晩、インクリメンタルバックアップを取っています。eDirectory のバックアップ後すぐに、ファイルシステムバックアップによりテープに保存しています。

サーバはすべてレプリカリングに属しています。ロールフォワードログ機能は全サーバで有効です。また、その保存先は、eDirectory とは別の記憶デバイスに割り当てています。ディスクの空き容量やアクセス権は随時監視して、ロールフォワードログであふれてしまわないよう注意しています。使用済みのロールフォワードログは、時々テープにバックアップして削除し、空き容量を増やすようにしています。

もちろんロールフォワードログを有効にすると管理の手間が増えますが、それを上回る利点があると考えています。サーバがレプリカリングに属している場合、いつでも最新の状態をバックアップしておく必要があるからです。こうしておけば、障害が発生しても、他のサーバとの同期状態も含めて元どおりに復元できます。

さらに、テスト環境で定期的にバックアップファイルからの復元を試み、想定どおりに動作することを確認しています。

ある木曜日の午後 2 時、Inventory\_DB1 という Linux サーバの、eDirectory を格納しているハードディスクが故障しました。

そこでまず、最新のフルバックアップファイルとそれ以降のインクリメンタルバックアップファイルを集め、昨夜午前 1 時の状態にまでデータベースを復元します。ロールフォワードログは昨夜のバックアップ以降の変更を記録しています。そこで次に、午前 1 時以降のロールフォワードログを使って、故障が起こる直前の状態に戻さなければなりません。

次のような手順で作業を進めることにしました。

1. まず、サーバのハードディスクを交換します。
2. 日曜の夜に取ったフルバックアップのテープを用意しました。

フルバックアップ用のバッチファイルは、ファイル /adminfiles/backup/backupfull.bk にバックアップするようになっています。

ファイルの容量制限を 200MB と設定していたので、次の 2 つのファイルがありました。

backupfull.bk.00001 (250 MB)

backupfull.bk.00002 (32 MB)

3. さらに、月曜、火曜、水曜に取ったインクリメンタルバックアップのテープも用意しました。

インクリメンタルバックアップ用のバッチファイルは、ファイル /adminfiles/backup/backupincr.bk にバックアップするようになっています。

毎日同じバッチファイルを使っているため、ファイル名は常に同じです。しかし、テープからサーバにコピーする時に、ファイル名を変更しなければなりません。復元処理の際は、全ファイルを同じディレクトリに集めておく必要があるからです。

4. まず、ハードディスクを交換しました。

幸い Linux オペレーティングシステムを格納したハードディスクは故障しなかったため、Linux の再インストールは必要ありませんでした。
5. バックアップテープを使って、障害を受けたディスクパーティションを復元しました。

6. 次に eDirectory を再インストールし、仮のツリーを作りました。復元処理では、いったんこのツリー上にデータを復元してから実動ツリーに切り替えることとなります。
7. サーバ上に、バックアップファイルを集めておくためのディレクトリ /adminfiles/restore を作りました。
8. フルバックアップファイル (2 つに分割されているもの) を、このディレクトリにコピーしました。
9. さらに、月曜、火曜、水曜のインクリメンタルバックアップファイルもコピーしました。

どれも同じ backupincr.bk というファイル名なので、次のように改名します。

backupincr.mon.bk

backupincr.tues.bk

backupincr.wed.bk

**注:** インクリメンタルバックアップファイルは、必ずしもフルバックアップファイルと同じディレクトリにコピーしなくても構いません。ただし各インクリメンタルバックアップファイルはすべて同じディレクトリに置いておく必要があります。

10. 次に iManager を使って eDirectory を復元することにしました。
  - a. iManager を起動し、[eDirectory の保守] > [復元] の順にクリックします。
  - b. サーバにログインしました。コンテキストとしては、仮に作っておいたツリーを使います。
  - c. [復元ウィザード? ファイルの環境設定] 画面で次のように操作しました。

バックアップファイルの場所として、「/adminfiles/restore」を指定。

復元処理に関するログファイルの出力先として「/adminfiles/restore/restore.log」を指定。
  - d. [復元ウィザード - オプション] 画面で次のように操作しました。

[データベースを復元] チェックボックスをオン。

[ロールフォワードログの復元] チェックボックスをオン。

ロールフォワードログの保存先を入力。

これは普段ロールフォワードログを保存している場所です。eDirectory とは別のハードディスクなので、今までのロールフォワードログが残っているはずです。

[セキュリティファイルの復元] チェックボックスをオン。

[検証後に復元されたデータベースをアクティブにします] チェックボックスをオン。

[復元の完了後にデータベースを開きます] チェックボックスをオン。

これは、復元後の検証に成功したら eDirectory をオープンするための指定です。
11. 復元処理を起動し、インクリメンタルバックアップファイル名を問い合わせるメッセージが表示されたので入力しました。
12. 復元後の検証処理にも成功し、自動的にデータベースがオープンされ、従来どおりのツリーで動作するようになりました。

ロールフォワードログはそのまま残っており、その場所を正しく指定したため、停止直前の状態に復元でき、検証も成功しました。

13. 復元後、ロールフォワードログに関する設定をやり直し、改めてフルバックアップを取っておきました。

ロールフォワードログの機能は、復元処理の過程で無効に戻ってしまうため、ここで有効にする必要があります。フルバックアップが改めて必要となるのは、スケジュールに従って次に無人でのフルバックアップが取られるまでに、再び障害が起こる可能性があるためです。

サーバの稼動状況を調べ、正常に動作していることを確認しました。

## シナリオ：複数サーバ構成のネットワークで、1台のサーバが完全に使えなくなった場合

ユーザは GK Designs 社で 15 台のサーバを管理しています。毎週土曜の夜にフルバックアップを取り、さらに毎晩、インクリメンタルバックアップを取っています。eDirectory のバックアップ後すぐに、ファイルシステムバックアップによりテープに保存しています。

サーバはすべてレプリカリングに属しています。ロールフォワードログ機能は全サーバで有効です。

ある日、漏電による火事のため、ある支店のサーバが 1 台、完全に使えなくなってしまいました。幸い、このサーバのパーティションは、ひとつを除いてすべて、他のサーバにレプリカが作成されていました。ロールフォワードログ機能は有効にしていたのですが、それも使えなくなってしまいました。したがって、停止直前の状態にまで eDirectory データベースを復元することはできません。

しかしバックアップファイルがあるので、サーバの eDirectory 識別情報は再作成できます。ロールフォワードログは使えないので、他のサーバとの同期状態は元に戻せません (403 ページの「[遷移ベクトルと復元後の検証処理](#)」を参照)。検証処理には失敗するはずですが、したがって、復元処理が終わっても eDirectory データベースはオープンされません。

そこで、レプリカリングからいったんサーバを外し、DSRepair を使って、他のサーバを参照してレプリカを作る設定に変更しました。その結果、最新のレプリカを保持しているサーバからデータを参照し、最新の状態が作り出されます。具体的な手順は 440 ページの「[復元後の検証処理に失敗した場合の対処方法](#)」を参照してください。

レプリカが作られていなかったパーティションがひとつありました。これは、支店内にあるファックス/プリンタ複合機や大判カラープリンタなど、この支店内のネットワーク印刷オブジェクトを管理しているコンテナです。他のサーバにレプリカがないため、このパーティションは上述の手順では復元できません。このパーティションのオブジェクトは一から作り直さざるをえなかったため、将来に備え、これも他のサーバにレプリカを作っておくことにしました。

そこでロールフォワードログに関する設定をやり直し、改めてフルバックアップを取っておきました。ロールフォワードログの機能は、復元処理の過程で無効に戻ってしまうためです。

## シナリオ：複数サーバ構成のネットワークで、数台のサーバが使えなくなった場合

ユーザは3ヶ所に分けて設置された20台のサーバを管理しています。その1ヶ所で、水道管破裂による水漏れ事故のため、8台のうち5台が使えなくなってしまいました。

幸い、どのサーバについても、eDirectoryのバックアップを取っていました。しかし全サーバともレプリカリングに属しており、ロールフォワードログはなくなってしまったので、これを使わずに復元作業を進めなければなりません。最初にどのサーバから着手し、レプリカ間の不整合をどのように解消すればよいか、判断できませんでした。状況があまりに込み入っていたため、Novellの技術担当者に相談することになりました。

## シナリオ：複数サーバ構成のネットワークで、すべてのサーバが使えなくなった場合

ユーザとそのチームは、Human Resource Consulting社で1ヶ所に設置された50台のサーバを管理しています。

普段から障害対策のため、ツリーの各パーティションについて3つずつレプリカを作成しています。したがって、サーバが1台停止しても、そのパーティションにあるオブジェクトは他のサーバからアクセスできます。さらに、各サーバに障害があっても復元できるよう、Backup eMToolで定期的にバックアップするほか、ロールフォワードログ機能を有効にし、バックアップテープは別の建物に保管しています。

災害に備えるため、チームでは2台のサーバをDSMASTERとして割り当てています。2台を割り当てているのは、ツリーが大きすぎて、1台では全パーティションのレプリカを保持できないからです。ツリーに属するどのパーティションも、いずれかのDSMASTERサーバにレプリカが作成されています。逆に、同じパーティションのレプリカが2台のDSMASTERサーバに作成されることはないようにして、重複を避けています。これが障害対策として重要な点です。

さらにチームでは、テスト環境で定期的にバックアップファイルからの復元を試み、想定どおりに動作することを確認しています。

ある日、台風で社屋が倒壊し、データセンタにあったサーバもすべて壊れてしまいました。

台風が去った後、チームではまず、パーティションすべてのレプリカを保持する、2台のDSMASTERサーバを復元する作業に取りかかりました。最新のフルバックアップファイルおよびそれ以降のインクリメンタルバックアップファイルを使用しましたが、ロールフォワードログは使いませんでした。サーバが壊れたときに、いっしょになくなってしまったからです。DSMASTERサーバを設定する際、この2台が同じレプリカを保持することはないようにしていました。そのため、ロールフォワードログを適用しなくても、復元後の検証処理は問題なく成功したのです。DSMASTERサーバが復元されたことにより、Human Resources Consulting社のツリーに属するオブジェクトはすべてアクセスできるようになりました。

DSMASTERが復元できれば、整合性を損なうことなくツリー全体を再作成できるので、その役割は非常に重要です。

このチームは、ロールフォワードログの機能も有効にしていました。障害が発生する直前の状態にまでサーバを復元でき、レプリカリングに属する他のサーバとの同期状態に不整合が生じないからです。サーバが復旧し、他のサーバと通信できるようになると、停止していた間に行われた更新情報を自動的に受け取り、同期を取ることができます。

しかし今回はそのロールフォワードログを使えません。その場合、レプリカリングに属するサーバのうち、最初に復元処理を実施したものしか正常に復元できないこととなります。それ以外のサーバは、他のサーバと同期状態が一致しないということで、復元後の検証処理に失敗してしまうのです(403 ページの「[遷移ベクトルと復元後の検証処理](#)」を参照)。検証処理に失敗すると、この eDirectory データベースはアクティブになりません。

しかしこのチームは、このような状況もきちんと考慮していました。2 台の DSMASTER サーバを設定し、重複して保持するパーティションがないようにして、これを復元作業の起点としたのです。重複がないので検証処理に失敗することはありません。これをマスタとして順次他のサーバにコピーしていけば、レプリカリング全体が復元できることとなります。

DSMASTER サーバの復元後、他のサーバを復元するために、いくつか必要な作業があります。このチームは次のような手順で、他のサーバを順次復元していきました。

- ◆ DSMASTER サーバ上のレプリカを、マスタレプリカとして割り当てます。
- ◆ DSMASTER 以外のサーバをレプリカリングから外します。
- ◆ フル/インクリメンタルバックアップファイルを使って、DSMASTER 以外のサーバを復元します。

ロールフォワードログがないため、復元後の検証処理に失敗することは分かっています。したがって、データベースは復元されても、まだアクティブになっていません。

- ◆ 高度な復元機能を使って、データベースをアクティブにしました。ロックはまだ解除しません。
- ◆ DSRepair を使って、他のサーバを参照してレプリカを作る設定に変更しました。
- ◆ データベースのロックを解除しました。

この時点で、各サーバの識別情報は元どおりに戻っていますが、レプリカ情報を同期させようとはしません。他のサーバからレプリカのデータを受け取り、改めて構築できる状態になっています。

なお、NetWare サーバの場合、ファイルシステムの復元は eDirectory の復元後に行う必要があります。

- ◆ 各サーバは DSMASTER サーバからデータを受け取り、自動的にレプリカを復元してレプリカリングに復帰します。

各サーバにどのレプリカが置かれていたか、チームではきちんと把握していました。もっとも、最終バックアップ時点の状況は、バックアップファイルのヘッダを見れば確認できます。

- ◆ ロールフォワードログに関する設定をやり直し、改めてフルバックアップを取っておきました。ロールフォワードログの機能は、復元処理の過程で無効に戻ってしまうので、ここで有効にしたのです。改めてフルバックアップを取る必要があるのは、スケジュールに従って次に無人でのフルバックアップが取られるまでに、再び障害が起こる可能性があるためです。

具体的な手順は [440 ページの「復元後の検証処理に失敗した場合の対処方法」](#) を参照してください。

かなりの作業量でしたが、ツリー自身は比較的早期に使用できるようになり、その時点でサーバ全体を復旧する目処も立っていました。

# NICI のバックアップと復元

NICI (Novell International Cryptography Infrastructure) は、ファイルシステム内と、システムおよびユーザ固有のディレクトリやファイルに、キーとユーザデータを保存します。これらのディレクトリとファイルは、オペレーティングシステムによって提供されるメカニズムを使用して適切なアクセス権を設定することによって保護されます。この設定は、NICI インストールプログラムによって行われます。

システムから NICI をアンインストールしても、システムまたはユーザ固有のディレクトリとファイルは削除されません。したがって、これらのファイルを以前の状態に復元することが必要になるのは、重大なシステム障害や人為的エラーから回復する場合のみです。既存の NICI ユーザディレクトリおよびファイルを上書きすると、既存のアプリケーションで問題が発生する可能性があることを理解しておくことが重要です。

NICI をバックアップおよび復元するには、次の 2 つの処理を行う必要があります。

1. ディレクトリとファイルをバックアップおよび復元する。
2. これらのディレクトリとファイルの特定のユーザの権利をバックアップおよび復元する。

上記の処理を行う適切な順序は、使用しているプラットフォームによって異なります。

バックアップと復元で重要になるのは、ディレクトリとファイルの正しいアクセス権を保持することです。NICI の動作と提供されるセキュリティは、これらのアクセス権が適切に設定されているかどうかによって左右されます。

一般的な市販のバックアップソフトウェアでは、NICI システムディレクトリとユーザディレクトリおよびファイルのアクセス権を保持する必要があります。NICI のカスタムバックアップを実行する前に、お使いのバックアップソフトウェアでこの処理が行われるかどうかを確認してください。

既存の NICI ディレクトリ構造とその内容をバックアップする場合は、復元を実行する前に注意すべき点があります。まず、コンピュータキーが失われると、元に戻すことはできません。また、ユーザデータとキーはコンピュータキーを使って暗号化されている場合があるため、ユーザデータが永久に失われることになる可能性があります。

NICI の復元を行うには、復元する必要があるファイルを特定するための知識が必要になります。復元時には、所有者のアクセス権が正しく復元されることが重要になります。UNIX システムと Windows システムの場合、ユーザ固有のディレクトリの名前は所有者の ID を反映します。ただし、どちらのシステムでも、バックアップした後から復元するまでの間に所有者 ID が変更される場合があります。セキュリティ上の理由により、オペレータは、復元されるアカウントを把握し、それに応じて割り当てられるディレクトリ名とアクセス権を決定する必要があります。バックアップされた ID と同じ ID を持つユーザアカウントがシステム内に存在するからといって、現在のアカウントが復元される情報の実際の所有者であるとは限りません。

詳細については、Novell Knowledgebase の「[TID10098087, How to Backup NICI 2.7.x and 2.6.x](http://support.novell.com/cgi-bin/search/searchtid.cgi?/10098087.htm)」と「[TID10096647, How to Backup the eDirectory Database and Associated Security Services Files](http://support.novell.com/cgi-bin/search/searchtid.cgi?/10096647.htm)」を参照してください。

NICI 2.6.5 以前の場合、`/var/novell/nici` ディレクトリに、すべてのシステムディレクトリとユーザディレクトリおよびファイルが含まれています。NICI 2.7.0 以降の場合、`/var/novell/nici` は、ファイルが含まれている `/var/opt/novell/nici` ディレクトリへのシンボリックリンクになります。

使用している NICI のバージョンを特定するには、`/etc/nici.cfg` ファイルを確認します。

## バックアップの実行

次のファイルとディレクトリをバックアップする必要があります。すべてのディレクトリとファイルの権利を保持していることを確認します。

### 2.7.0 より前のバージョンの NICI の場合

| ファイル/ディレクトリ名                       | ファイルの種類と特記事項   |
|------------------------------------|--|
| <code>/etc/nici.cfg</code>         | 環境設定ファイル。  |
| <code>/usr/lib/libccs2.so</code>   | <code>/usr/lib/</code> 内の実際のライブラリへのシンボリックリンク。                            |
| <code>/usr/lib/libccs2.so.*</code> | NICI ライブラリ (ライブラリのバージョンが名前の末尾に付きます)。                                     |
| <code>/var/novell/nici</code>      | このディレクトリには、すべてのシステムキー、ユーザディレクトリとファイル/キー、および NICI の初期化に使用されるプログラムが格納されます。 |

### NICI 2.7.0 以降の場合

| ファイル/ディレクトリ名                              | ファイルの種類と特記事項   |
|---|--|
| <code>/etc/nici.cfg</code>                | <code>/etc/opt/novell/nici.cfg</code> 環境設定ファイルへのシンボリックリンク。               |
| <code>/etc/opt/novell/nici.cfg</code>     | 環境設定ファイル。  |
| <code>/usr/lib/libccs2.so</code>          | <code>/opt/novell/lib/</code> 内の実際のライブラリへのシンボリックリンク。                     |
| <code>/opt/novell/lib/libccs2.so.*</code> | NICI ライブラリ (ライブラリのバージョンが名前の末尾に付きます)。                                     |
| <code>/var/novell/nici</code>             | <code>/var/opt/novell/nici</code> ディレクトリへのシンボリックリンク。                     |
| <code>/var/opt/novell/nici</code>         | このディレクトリには、すべてのシステムキー、ユーザディレクトリとファイル/キー、および NICI の初期化に使用されるプログラムが格納されます。 |



## NICI の復元

NICI 環境設定ファイルを復元するには、最初に、`/etc/nici.cfg` ファイルまたはリンクを検索して、コンピュータに NICI がインストールされているかどうかを確認します。

- 1 NICI がシステムにすでにインストールされている場合、上記のように既存の設定のバックアップを取ります。
- 2 NICI をアンインストールし、`/var/novell/nici` または `/var/opt/novell/nici` ディレクトリ構造を削除します。  
この操作を行うのは、既存のシステムキーが復元されたセットと競合しないようにするためです。
- 3 (NICI のバージョンに応じて) バックアップストアから構造全体を復元します。アクセス権も必ず復元します。

上記の手順に従うことをお勧めします。ただし、知識が豊富なオペレータであれば、個々のファイルまたはディレクトリを復元することを選択できます。場合によっては、ファイルやディレクトリの名前を変更したり、新しいアクセス権を割り当てたりできます。この操作を行えるのは、`nicifk` ファイルと `xmgrcfg.wks` ファイルがバックアップストア上のこれらのファイルから変更されていない場合です。

NICI がコンピュータにすでにインストールされている状況で復元を行う場合は、それぞれのファイル/ディレクトリについて次のガイドラインに従うことをお勧めします。

| ファイル名                     | 操作手順   |
|---------------------------|--|
| <code>xmgrcfg.nif</code>  | 既存のファイル上に復元できます。   |
| <code>xarchive.000</code> | 既存のファイル上に復元できます。   |
| ユーザ固有のディレクトリとファイル         | <p>バックアップのユーザ ID が、コンピュータ上のユーザと同じになるようにします。ユーザディレクトリがすでに存在する場合は、そのユーザが現在のファイルを保持することを希望しているのか、以前の状態に復元することを希望しているのかを確認します。通常、ユーザの環境設定ファイルの復元は、個別にではなくまとめて行う必要があります。必ず、適切なユーザの正しいユーザ ID でユーザファイルを復元し、ユーザディレクトリとその内容の権利を復元するようにします。</p> <p>たとえば、バックアップ時には BOB に <code>userid 1000</code> が指定されて、現在は <code>userid 5000</code> が指定されている場合、バックアップされたディレクトリ 1000 内のファイルをディレクトリ 5000 に復元するか、または BOB の UID を 1000 に戻す必要があります。</p> <p>ユーザディレクトリの復元は、オペレータの入力なしに作業を進めることがないよう、計画的に行ってください。いずれの場合においても、既存の NICI ユーザディレクトリのバックアップを行う必要があります。</p> |

## NetWare の場合

NICI 2.x よりも前のバージョンでは、環境設定ファイルは `sys:¥_NetWare` に保存され、別の手順が適用されます。これらの手順は、NICI 2.x 以降でのみ有効です。

### バックアップの実行

`sys:¥system¥NICI` ディレクトリとすべてのサブディレクトリおよびアクセス権をバックアップします。NetWare では、存在するユーザが 1 人のみであるため、ユーザディレクトリのバックアップや復元は UNIX や Windows の場合のように複雑ではありません。

### NICI の復元

NICI がインストールされていない場合は、`sys:¥system¥NICI` ディレクトリとその内容を復元します。

NICI がインストールされている場合 (`sys:¥system¥NICI¥nici.cfg` ファイルが存在している場合)、既存の設定のバックアップを取り、NICI を削除します。バックアップストアからバックアップ構造全体をコピーして復元します。

選択的な復元が可能なのは、`nicifk` ファイルがバックアップストア上のファイルから変更されていない場合のみです。ファイルが変更されていない場合は、`sys:¥system¥NICI` ディレクトリ内の任意のファイルを復元します。通常、ファイルはまとめて復元する必要があります。ただし、知識の豊富なオペレータであれば、個々のファイルまたはディレクトリを復元することを選択してもかまいません。

## Windows の場合

設定情報は、次のキーの下のシステムレジストリ内に保持されます。

```
HKEY_LOCAL_MACHINE¥SOFTWARE¥Novell¥NICI
```

2 つ目のキーは、現在インストールされている NICI のバージョンを示します。例：

```
HKEY_LOCAL_MACHINE¥SOFTWARE¥Novell¥NICI (Shared) U.S./Worldwide (128 ビット)
```

### バックアップの実行

- 1 `HKEY_LOCAL_MACHINE¥SOFTWARE¥Novell¥NICI*` の下にあるレジストリ情報をすべてバックアップします。

`NICI*` は、NICI で始まるすべてのレジストリキーを表します。レジストリキーは複数存在する可能性があります。

- 2 `HKEY_LOCAL_MACHINE¥SOFTWARE¥Novell¥NICI¥ConfigDirectory` によって識別される、ディレクトリ (サブディレクトリを含む) をバックアップします。

UNIX システムの場合と同様に、ディレクトリとすべてのサブディレクトリのアクセス権を保持します。詳細については、[452 ページの「バックアップの実行」](#)を参照してください。

市販のソフトウェアを使用してバックアップする場合は、必ず、バックアッププログラム自体をシステムプロセスとして実行します。これにより、バックアッププログラムがすべてのディレクトリとサブディレクトリにアクセスできるようになります。

## NICI の復元

- 1 NICI がインストールされていない場合は、最初にすべてのレジストリ情報を復元します。  
または  
NICI がインストールされている場合は、NICI を削除し、バックアップストアからのレジストリ情報を上書きします。
- 2 オペレータによって選択されたように、  
HKEY\_LOCAL\_MACHINE¥SOFTWARE¥Novell¥NICI¥ConfigDirectory 内のファイルとディレクトリを復元します。

UNIX の場合と同様に、すべてのファイルをまとめて復元することをお勧めします。ただし、知識の豊富なオペレータであれば個々のエントリを復元することを選択してもかまいません。この操作が可能なのは、`nicifk` ファイルと `xmgrcfg.wks` ファイルがバックアップストア上のファイルから変更されていない場合のみです。その場合には、ユーザ構成ディレクトリの新しい所有者に基づいてアクセス権を調整します。個々のディレクトリにはその所有者に基づく名前が付けられますが、アクセス権は SID によって制御されます。サブディレクトリに `BOB` という名前が付けられているというだけで、現在のユーザ `BOB` が復元されている情報の正しい所有者であるとは限りません。

## Windows の特殊な場合

レジストリ値を `HKEY_LOCAL_MACHINE¥SOFTWARE¥Novell¥NICI¥UserDirectoryRoot` に設定して、ユーザの環境設定ファイルがユーザ個人の構成ディレクトリに格納されていることを示すことができます。その場合、通常のバックアップ / 復元処理の一環として、ユーザ情報をバックアップおよび復元する準備を整えます。NICI が上記のように設定されている場合は、そのことを把握し、個々のバックアップのための準備をしておく必要があります。

このような Windows の特殊な場合には、単にディレクトリパスを指定するのではなく、レジストリ値 `EnableUserProfileDirectory` を作成することによってユーザディレクトリが有効になります。ユーザアカウントを自動的に作成および削除するように Windows が設定されている場合、ユーザプロファイルディレクトリが有効になると、ディレクトリが自動的に削除されます。その場合、バックアップと復元が必要になるのは永続的な特定のユーザのみです。デフォルトのパスは、`Documents and Settings` 内のユーザのディレクトリの `Application Data¥Novell¥Nici` ディレクトリの分岐になります。



# 15

## Novell eDirectory の SNMP サポート

SNMP (Simple Network Management Protocol) は、インターネットを介してデバイスを操作および保守するための標準的なプロトコルです。管理コンソールアプリケーションと管理対象デバイスは、このプロトコルに従って管理情報をやり取りします。管理コンソールアプリケーションには、HP\* Openview、Novell® NMS、IBM\* NetView、Sun\* Net Manager などがあります。管理対象デバイスとしては、ホスト、ルータ、ブリッジ、ハブなどのほか、Novell eDirectory™ のようなネットワークアプリケーションもあります。

このセクションでは、Novell eDirectory 8.8 の SNMP サービスについて説明します。このセクションには、次のトピックが含まれています。

- ◆ [457 ページの「SNMP に関する用語の定義」](#)
- ◆ [458 ページの「SNMP サービスについて」](#)
- ◆ [460 ページの「eDirectory と SNMP」](#)
- ◆ [464 ページの「eDirectory の SNMP サービスのインストールと設定」](#)
- ◆ [478 ページの「SNMP による eDirectory の監視」](#)
- ◆ [511 ページの「トラブルシューティング」](#)

### SNMP に関する用語の定義

この章で使われる用語の定義を次の表に示します。

| 用語      | 定義   |
|---------|--|
| EMANATE | SNMP Research International, Inc. の製品。Enhanced Management Agent Through Extensions の略称です |
| SNMP    | Simple Network Management Protocol の略。ネットワークの稼動状況に関するデータをやり取りするためのプロトコルです                |
| NAA     | Native Agent Adapter の略。ネイティブエージェントアダプタ  |
| NMS     | ネットワーク管理ステーション   |
| MA      | Management Agent の略。管理エージェント   |
| SA      | サブエージェント   |
| MIB     | 管理情報ベース (MIB)  |
| NCP™    | Netware® Core Protocol™ の略   |

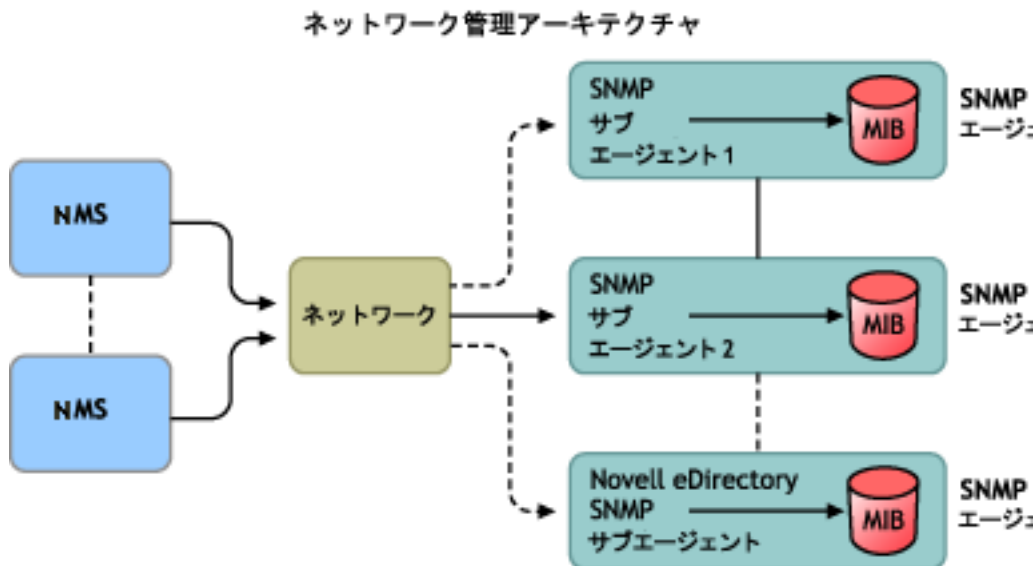
| 用語       | 定義  |
|----------|---|
| NMA      | Network Management Application の略。ネットワーク管理アプリケーション  |
| edir.mib | Novell eDirectory サーバの監視に使う MIB のこと。Novell eDirectory に関する MIB オブジェクトおよびトラップが設定されています                                     |
| トラップ     | eDirectory イベントがサーバ上で発生したときに、管理対象デバイス上のエージェントが発する警告のこと。警告を発する条件は、Novell が提供する MIB (Management Information Base) で定義されています |

## SNMP サービスについて

SNMP は「マネージャ / エージェント」アーキテクチャにもとづくプロトコルです。SNMP を使用して行われるネットワーク管理のアーキテクチャは、次のような要素から成ります。

- ◆ NMS (Network Management Station)
- ◆ 管理対象デバイス
- ◆ マスタエージェント
- ◆ サブエージェント
- ◆ MIB (Management Information Base)
- ◆ ネットワーク管理プロトコル

図 48 ネットワーク管理アーキテクチャ



## ネットワーク管理ステーション

ネットワーク管理ステーション (NMS) とは、ネットワーク管理アプリケーションがインストールされたワークステーションのことです。管理対象デバイスに関する情報をグラフィック表示します。

NMS には次のような機能があります。

- ◆ ネットワーク管理システム全体のユーザインタフェースを提供します。この機能により、ネットワーク管理の強固さ、柔軟性、および使いやすさが決まります。
- ◆ SNMP Get、Get Next、SNMP GetResponse、および Set の操作はここから実行します。また、ネットワーク上の管理対象デバイスから送られてくる SNMP トラップを捕捉するのも、やはり NMS の役割です。
- ◆ 複数のネットワーク管理アプリケーション (NMA) を同時に監視し、管理対象デバイスに関する情報をグラフィック表示します。表形式で表示する機能、ログとして記録する機能もあります。
- ◆ NMS に組み込まれている MIB コンパイラで、MIB ファイルをコンパイルすることができます。

## 管理対象デバイス

SNMP がインストールされているデバイスは、すべて管理対象デバイスとして扱うことができます。ホスト、ルータ、ブリッジ、ハブなどが管理対象デバイスになります。NMS は管理対象デバイスを監視し、またデバイスと通信します。

NMS と管理対象デバイスとの間では、サブエージェントおよびマスタエージェントという 2 種類のエージェントを介して情報をやり取りします。

## サブエージェント

サブエージェントには、管理対象デバイスに関する情報を集め、マスタエージェントに渡す役割があります。

## マスタエージェント

マスタエージェントには、さまざまなサブエージェントと NMS の間で情報を交換する役割があります。マスタエージェントは、通信相手のサブエージェントと同じホスト上で動作します。

## 管理情報ベース (MIB)

SNMP では、プロトコルデータ単位 (PDU : Protocol Data Unit) という形でネットワーク情報を交換します。PDU には、管理対象デバイスに保存されている変数に関する情報が含まれています。この変数のことを管理オブジェクトと言い、その値とオブジェクト名が NMS に渡されます。管理オブジェクトはすべて管理情報ベース (MIB) に定義されています。MIB はツリー状の階層構造で表される仮想データベースです。

## SNMP のネットワーク管理プロトコル

SNMP の基本関数を次の表に示します。

| 関数           | 説明  |
|--------------|---|
| Get          | マネージャがエージェントに情報を要求するために使用します。             |
| Get Next     | 配列や表から情報を取得する際にマネージャが使用します。               |
| Get Response | マネージャから問い合わせを受けたエージェントが、それに応答するために使用します。  |
| Set          | エージェント側の MIB にある変数の値を変更するために、マネージャが使用します。 |
| Trap         | あるイベントが発生した際、エージェントがマネージャに通知するために使用します。   |

SNMP の詳細については、次の Web サイトを参照してください。

- ◆ [NET-SNMP Home Page \(http://net-snmp.sourceforge.net\)](http://net-snmp.sourceforge.net)
- ◆ [SNMP FAQ \(http://www.faqs.org/faqs/snmp-faq/part1\)](http://www.faqs.org/faqs/snmp-faq/part1)
- ◆ [RFC 1157 \(http://www.ietf.org/rfc/rfc1157.txt\)](http://www.ietf.org/rfc/rfc1157.txt)
- ◆ [SNMPLink \(http://www.snmpLink.org\)](http://www.snmpLink.org)
- ◆ [SNMPInfo \(http://www.snmpinfo.com\)](http://www.snmpinfo.com)
- ◆ [SNMP RFC Standard MIBs and Informative Links \(http://www.wtcs.org/snmp4tpc/snmp\\_rfc.htm\)](http://www.wtcs.org/snmp4tpc/snmp_rfc.htm)
- ◆ [RFC 2605 \(http://ietf.org/rfc/rfc2605.txt?number=2605\)](http://ietf.org/rfc/rfc2605.txt?number=2605)

## eDirectory と SNMP

eDirectory には、ユーザ、アプリケーション、ネットワークデバイス、データなど、数多くのオブジェクトを格納し、管理することができます。eDirectory で管理するオブジェクトが増えてくると、オブジェクトの追加や変更に追従する必要性も増してきます。この問題を解決する手段として SNMP を使用することで、ユーザは eDirectory サーバを監視し、変化に追従できるようになります。

### eDirectory の管理に SNMP を使う利点

- ◆ eDirectory サーバをリアルタイムに監視
- ◆ サードパーティ製 SNMP MIB ブラウザから eDirectory を監視
- ◆ eDirectory が正常に稼動しているか、状況を追跡可能
- ◆ 起こりうる問題を検知時に特定し、対処が可能
- ◆ トラップや統計に関する設定により、対象を選択して監視可能
- ◆ eDirectory に対するアクセス状況をグラフ表示
- ◆ SNMP で収集した履歴データを格納し、分析可能
- ◆ SNMP の Get 要求、GetNext 要求を使った統計機能にも対応
- ◆ プラットフォームを選ばず SNMP ネイティブマスタエージェントを使用可能



## eDirectory での SNMP の機能について

SNMP を eDirectory に実装すると、アクセス状況、稼動状況、エラー、キャッシュ性能に関する eDirectory の統計情報を取得できます。また、イベントが発生すると SNMP からトラップが送信されます。トラップや統計情報は MIB に定義されています。

注：これらの属性へのアクセスには常にセキュリティ保護されたチャンネルを使用すると指定している場合は、暗号化された属性へアクセスする際にセキュリティ保護されたチャンネル以外は使用できない可能性があります。詳細については、[241 ページの「暗号化属性」](#)を参照してください。

### ディレクトリサービス監視 MIB

eDirectory の MIB には、eDirectory を監視するための統計情報やトラップが定義されています。この MIB には次の oid (オブジェクト ID) が割り当てられています。

iso(1).org(3).dod(6).internet(1).private(4).enterprise(1).novell(23).mibDoc(2).ndsMIB(98)

#### 統計情報

eDirectory MIB は、管理対象オブジェクトを次の 4 つの異なるテーブルに分けて格納しています。

- ◆ **キャッシュデータベース統計テーブル - ndsDbCacheTable** : ディレクトリサーバに関する記述と、サーバにキャッシュされたエントリに関する統計情報の要約を格納します。
- ◆ **設定データベース統計テーブル - ndsDbConfigTable** : ディレクトリサーバに関する記述と、サーバで設定されたエントリに関する統計情報の要約を格納します。
- ◆ **プロトコル統計テーブル - ndsProtoIfOpsTable** : ディレクトリサーバのアプリケーションプロトコルインタフェースごとに、アクセス状況、稼動状況、エラーに関する統計情報の要約を格納します。
- ◆ **相互通信統計テーブル - ndsServerIntTable** : 監視対象ディレクトリが通信した、あるいは通信を試みたディレクトリサーバを、最新の「N」回分記録しておきます。「N」はローカルで定義する定数です。

注：統計情報の詳細については、[506 ページの「統計情報」](#)を参照してください。

#### トラップ - ndsTrapVariables

eDirectory MIB には 119 種類のトラップが定義されています。そのうち 117 種類は eDirectory のイベントにマップされています。ほかに ndsServerStart および ndsServerStop というトラップがあり、これは SNMP サブエージェントが直接生成します。この 2 種類のトラップは設定できません。

注：トラップの詳細については、[479 ページの「トラップ」](#)を参照してください。

統計情報やトラップの詳細については、edir.mib も参照してください。

edir.mib は次のディレクトリにあります。

NetWare: sys:\$etc

Windows: <install directory>%\$SNMP

Linux および UNIX: /etc/opt/novell/eDirectory/conf/ndssnmp/

## SNMP グループオブジェクト

SNMP グループオブジェクトは、eDirectory SNMP トラップの設定や管理に使用します。インストールの過程で、「SNMP Group - サーバ名」という名前の SNMP グループオブジェクトが作られます(ここでサーバ名は、eDirectory の SNMP サービスをインストールしたサーバ名を表します)。この SNMP グループオブジェクトが作られるのは、サーバオブジェクトと同じコンテナ内です。SNMP 設定ユーティリティは、SNMP トラップの設定に使用します。

### Windows の場合

SNMP グループオブジェクトを作るには、次のコマンドを実行してください。

```
rundll32 snmpinst, snmpinst -c <createobj> -a <ユーザ FDN> -p <パスワード> -h <ホスト名または IP アドレス>
```

| パラメータ                | 説明                    |
|----------------------|-----------------------|
| -c <オブジェクト作成>        | オブジェクトの作成を示すトラップコマンド。 |
| -a <ユーザ FDN>         | 管理者権利を持つユーザの完全識別名。    |
| -p <パスワード>           | 認証に使う「ユーザ FDN」パスワード。  |
| -h <ホスト名または IP アドレス> | DNS ホスト名または IP アドレス。  |

例 :

```
rundll32 snmpinst, snmpinst -c createobj -a admin.mycontext -p mypassword -h 160.98.146.26
```

SNMP グループオブジェクトを削除するには、次のコマンドを実行してください。

```
rundll32 snmpinst, snmpinst -c <deleteobj> -a <ユーザ FDN> -p <パスワード> -h <ホスト名または IP アドレス>
```

パラメータについてはオブジェクトを作る場合と同様です。

例 :

```
rundll32 snmpinst, snmpinst -c deleteobj -a admin.mycontext -p mypassword -h 160.98.146.26
```

## NetWare の場合

SNMP グループオブジェクトの作成や削除には `snmpinst` というユーティリティを使います。これは `sys:¥system¥directory` にあります。

SNMP グループオブジェクトを作るには、次のコマンドを実行してください。

**SNMPINST -c < 管理者コンテキスト > < パスワード > < サーバ DN >**

| パラメータ         | 説明                                    |
|---------------|---------------------------------------|
| -c            | オブジェクトの作成を示すフラグコマンド。削除する場合は「-d」と指定します |
| < 管理者コンテキスト > | 管理者権利を持つユーザの完全識別名                     |
| < パスワード >     | 認証に使う「ユーザ FDN」パスワード                   |
| < サーバ DN >    | DNS ホスト名                              |

例：

```
SNMPINST -c admin.mycontext.treename mypassword myserver
```

SNMP グループオブジェクトを削除するには、次のコマンドを実行してください。

**SNMPINST -d < 管理者コンテキスト > < パスワード > < サーバ DN >**

パラメータについてはオブジェクトを作る場合と同様です。

例：

```
SNMPINST -d admin.mycontext.treename mypassword myserver
```

## Linux、UNIX の場合

SNMP グループオブジェクトを作るには、次のコマンドを実行してください。

**ndsconfig add -m < モジュール名 > -a < ユーザ FDN >**

例：

```
ndsconfig add -m snmp -a admin.mycontext
```

## eDirectory の SNMP サービスのインストールと設定

SNMP service for eDirectory は、eDirectory をインストールする際に組み込まれます。eDirectory の SNMP サービスのデフォルト設定の変更には iManager を使います。詳細については、[466 ページの「ダイナミック設定」](#)を参照してください。

SNMP Group-Object という名前の新しいオブジェクトが、eDirectory のインストール時に、ディレクトリツリーに追加されます。このオブジェクトは Novell eDirectory SNMP トラップの設定や管理に使います。詳細については、[462 ページの「SNMP グループオブジェクト」](#)を参照してください。

### eDirectory がインストールされた Windows に SNMP を組み込む手順

eDirectory のインストール時に SNMP サービスを除外した場合は、SNMP サブエージェント用ファイルがコピーされるだけで、レジストリは元のままになっています。

あとになって SNMP サービスが必要になった場合は、次のコマンドでレジストリを更新してください。

```
rundll32 snmpinst, snmpinst -c createreg
```

## SNMP サーバモジュールのロードとアンロード

SNMP サーバモジュールは手動でロード、アンロードできます。デフォルトでは、どのプラットフォームでも、自動でロードされるようになっています。Windows、Linux、および UNIX の場合は、手動でロードすることも可能です。

SNMP サーバモジュールをロードするには、次のコマンドを入力します。

| サーバ                     | コマンド   |
|-------------------------|--|
| NetWare                 | 手動でのアンロードは不可。  |
| Windows                 | [DHOST (NDSCONS)] 画面で Ndssnmp.dlm を選択し、[開始] をクリックします。  |
| Linux、Solaris、AIX、HP-UX | DHOST のリモート管理ページで、SNMP Trap Server for Novell eDirectory 8.8 アイコンをクリックすると、SNMP トラップサーバがロードされます。<br><br>または<br><br>コマンドプロンプトから「/opt/novell/eDirectory/bin/ndssnmp -1」と入力するという方法もあります。 |

SNMP サーバモジュールをアンロードするには、次のコマンドを入力します。

| サーバ                     | コマンド   |
|-------------------------|--|
| NetWare                 | 手動でのアンロードは不可。  |
| Windows                 | [DHOST (NDSCONS)] 画面で ndssnmp.dlm を選択し、[停止] をクリックします。  |
| Linux、Solaris、AIX、HP-UX | DHOST のリモート管理ページで、SNMP Trap Server for Novell eDirectory 8.8 アイコンをクリックすると、SNMP トラップサーバがアンロードされます。<br><br>または<br><br>コマンドプロンプトから「/opt/novell/eDirectory/bin/ndssnmp -u」と入力するという方法もあります。 |

## サブエージェントの設定

### スタティック設定

スタティック設定は、サブエージェントを実際に稼働させる前に行います。手動で設定する場合、Windows、Solaris、Linux、AIX ならば ndssnmp.cfg、NetWare ならば dssnmp.cfg というファイルを編集してください。ファイル ndssnmp.cfg は次のディレクトリにあります。

Windows: インストールディレクトリ ¥SNMP¥

NetWare: sys:¥etc¥

Linux および UNIX: /etc/opt/novell/eDirectory/conf/ndssnmp/

注: ndssnmp.cfg を書き替えた場合、サブエージェントを再起動する必要があります。

サブエージェントの設定は、次のような書式で記述してください。

- ◆ INTERACTIVE ステータス

ここで「ステータス」には、「on」または「off」を指定します。「on」を指定すると、サブエージェント起動時にユーザ名とパスワードを要求されるようになります。ステータスが Off の場合、ユーザ名およびパスワードはセキュリティ保護された保存データから取得されます。デフォルト値は「off」です。

例:

```
INTERACTIVE on
```

```
INTERACTIVE off
```

- ◆ INTERACTION 値

ここで「値」は、インタラクション表のエントリ数を表します。1～10の範囲で、デフォルト値は4です。

例:

```
INTERACTION 4
```

```
INTERACTION 2
```

- ◆ **MONITOR** ステータス

ここで「ステータス」には、「on」または「off」を指定します。デフォルト値は「on」です。

例：

```
MONITOR on
```

```
MONITOR off
```

- ◆ **SSLKEY** 認証ファイル

ここで「認証ファイル」は、証明書のエクスポート先パスを表します。エクスポートした証明書が実際に存在するパスを指定してください。

例：

```
SSLKEY /home/guest/snmp-cert.der (Linux、UNIX の場合)
```

```
SSLKEY c:\home\guest\snmp-cert.der (Windows NT、NetWare の場合)
```

- ◆ **SERVER** ホスト名/IP アドレス

ここで「ホスト名」は、eDirectory サーバをインストールし、設定したホスト名を表します。指定できるのは、ローカルにインストールしたサーバに限ります。

この指定は必須です。指定がなければどのサーバも監視の対象になりません。デフォルト：ローカルサーバのホスト名。

例：

```
SERVER myserver
```

```
SERVER myserver:1524
```

Linux および UNIX 上で eDirectory のインスタンスが複数存在する場合、監視するすべての eDirectory サーバを次のように指定できます。

```
SERVER myserver:1524
```

```
SERVER myserver:2524
```

```
SERVER myserver:6524
```

注：このコマンドで、コロン(:)の前にはスペースを入れないでください。

## ダイナミック設定

ダイナミック設定は、ディレクトリサービスの稼動中、いつでも次のいずれかの方法で実行できます。

### コマンドラインからの設定

トラップ設定用のコマンドラインユーティリティを使って、eDirectory の SNMP トラップを設定できます。


次のような操作が可能です。

- ◆ トラップの有効化/無効化
- ◆ トラップ間隔の設定
- ◆ エラートラップの有効化/無効化
- ◆ 有効な/無効な/すべてのトラップのリスト表示

注：詳細については、494 ページの「[トラップに関する設定](#)」を参照してください。

## iManager プラグインによる設定

トラップの設定には、Novell iManager を使う方法もあります。Novell iManager はブラウザベースのツールで、eDirectory オブジェクトを運用、管理、設定するために使用します。iManager を使用すると、ユーザに特定のタスクや責任を割り当てたり、それらのタスクを実行するために必要なツールおよびそれに伴う権利だけを付与したりすることができます。

- 1 Novell iManager で、[役割およびタスク] ボタン  をクリックします。
- 2 [SNMP Management] > [SNMP の概要] の順にクリックします。
- 3 [SNMP グループオブジェクトを表示] をクリックして、設定する SNMP グループオブジェクトの名前をクリックします。
- 4 一般ページまたはトラップページで、必要なパラメータを設定します。
- 5 [適用] をクリックし、[OK] をクリックすると、今設定した内容が保存されます。

注：詳細については Novell iManager のオンラインヘルプを参照してください。

## eDirectory の SNMP サービスの設定

eDirectory の SNMP サービスの設定は、次の手順で行います。

1. マスタエージェントの設定
2. マスタエージェントの起動
3. サブエージェントの設定
4. サブエージェントの起動

### NetWare の場合

NetWare の場合、ネイティブマスタエージェント (snmp.nlm) が、初めからオペレーティングシステムに組み込まれています。

ヒント：NetWare にはデフォルトで SNMP マスタエージェントがあります。詳細については、[SNMP Developers Components \(http://developer.novell.com/ndk/snmpcomp.htm\)](http://developer.novell.com/ndk/snmpcomp.htm) を参照してください。

### マスタエージェントの設定

コミュニティ名

- 1 コマンドプロンプトから、「**inetcfg**」と入力してください。
- 2 [Manage Configuration] オプションを選択します。
- 3 [Configure SNMP parameters] オプションを選択します。
- 4 コミュニティ名を表す文字列を編集してください。

トラップの送り先

- 1 ファイル `sys:\etc\traptarg.cfg` を編集し、トラップの送り先とするコンピュータの IP アドレスまたはホスト名を指定してください。

### マスタエージェントの起動

マスタエージェント snmp.nlm はデフォルトで起動されています。

## サブエージェントのロード

- 1 サブエージェントをロードするには、コマンドプロンプトから「**dssnmpsa**」と入力してください。  
するとダイアログボックスが現れます。[ログイン] オプション、[終了] オプションがあります。
- 2 処理を続行したい場合は[ ログイン]、中断する場合は[ 終了] を選択してください。
- 3 (状況によって実行) [ログイン] を選択した場合、ユーザ名とパスワードを求められるので入力してください。
- 4 [パスワードを保存する] に「**y**」と入力すると、パスワードを保存できます。次回からは、パスワードを入力することなくサブエージェントを起動できます。「**N**」と入力した場合は、次回からもパスワードを求められます。
- 5 いずれかを入力した後、<Enter> キーを押してください。
- 6 <F10> キーを押すとツリーにログインできます。
- 7 <Enter> キーを押して続けます。
- 8 サブエージェントが起動されます。

注: このダイアログボックスは、ファイル `sys:\etc\ndssnmp.cfg` で `INTERACTION` が「on」になっている場合に現れます。「off」ならば表示されません。

## Windows の場合

### マスタエージェントの設定

注: SNMP マスタエージェントは、eDirectory のインストールに先立って組み込んでおく必要があります。詳細については、[SNMP Installation on Windows \(http://www.microsoft.com/technet/treeview/default.asp?url=/TechNet/prodtechnolog/winttas/maintain/featusability/getting.asp\)](http://www.microsoft.com/technet/treeview/default.asp?url=/TechNet/prodtechnolog/winttas/maintain/featusability/getting.asp) を参照してください。

- 1 [Microsoft SNMP Properties] ダイアログボックスを開き、[エージェント] タブをクリックします。
- 2 接続先および場所に関する情報を入力してください。
- 3 [トラップ] タブをクリックし、コミュニティ名およびトラップの送り先に関する情報を入力します。
  - 3a コミュニティ名を入力し、[追加] をクリックします。
  - 3b トラップの送り先のコンピュータの IP アドレスまたはホスト名を入力してください。
  - 3c [追加] ボタンを押すと、ここで入力した IP アドレスまたはホスト名が追加されます。
- 4 [デスクトップとの対話をサービスに許可する] オプションを有効にします。  
このオプションが無効のままだと、Windows 上の SNMP には接続できません。
  - ◆ Windows NT の場合: [スタート] > [設定] > [コントロールパネル] > [サービス] の順にクリックします。次に [SNMP] > [起動] をクリックし、[デスクトップとの対話をサービスに許可する] を選択します。
  - ◆ Windows 2000 の場合: [スタート] > [設定] > [コントロールパネル] > [管理ツール] > [サービス] の順にクリックします。[SNMP] を右クリックし、[プロパティ] を選択します。[ログオン] タブで、[デスクトップとの対話をサービスに許可する] を選択します。



## マスタエージェントの起動

マスタエージェントを起動するには、次のいずれかの操作をしてください。

- ◆ Windows NT の場合 : [スタート] > [設定] > [コントロールパネル] > [サービス] > [SNMP] > [開始] の順にクリックします。

Windows 2000 の場合 : [スタート] > [設定] > [コントロールパネル] > [管理ツール] > [サービス] > [SNMP] > [開始] の順にクリックします。

- ◆ コマンドラインで次のように指定してください。

**Net start SNMP**

## マスタエージェントの停止

マスタエージェントを停止するには、次のいずれかの操作をしてください。

- ◆ Windows NT の場合 : [スタート] > [設定] > [コントロールパネル] > [サービス] > [SNMP] > [停止] の順にクリックします。

Windows 2000 の場合 : [スタート] > [設定] > [コントロールパネル] > [管理ツール] > [サービス] > [SNMP] > [停止] の順にクリックします。

- ◆ コマンドラインで次のように指定してください。

**Net stop SNMP**

## サブエージェントの起動

Windows の場合、マスタエージェントを起動すると、サブエージェントも自動的に起動されます。

**重要** : 最新の Service Pack は、SNMP サービスのインストール後にインストールする必要があります。

## Linux の場合

Linux (SLES 9 または OES Linux を除く) の場合は、net-snmp-5.0.9-4.rh73.i386.rpm をインストールしておく必要があります。SLES 9 (OES Linux) の場合は、システムのデフォルトのマスタエージェント (net-snmp-5.1-80.xx) が使われます。

SLES 9 (OES Linux) およびその他の Linux では、設定の手順が異なります。詳細については、を参照してください。

- ◆ [469 ページの「SLES 9 または OES Linux での SNMP サービスの設定」](#)
- ◆ [471 ページの「Linux \(SLES 9 または OES 以外\) での SNMP サービスの設定」](#)
- ◆ [473 ページの「サブエージェントの起動時の問題」](#)

## SLES 9 または OES Linux での SNMP サービスの設定

- ◆ [470 ページの「マスタエージェントの設定」](#)
- ◆ [470 ページの「マスタエージェントの起動」](#)
- ◆ [470 ページの「サブエージェントの起動」](#)
- ◆ [471 ページの「サブエージェントの停止」](#)

## マスタエージェントの設定

SLES 9 または OES Linux でマスタエージェントを設定するには、[470 ページの「snmpd.conf の変更」](#)の説明に従って snmpd.conf ファイルを変更します。

snmpd.conf ファイルは、OES Linux または SLES 9 の /etc/snmp ディレクトリ、およびその他の Linux プラットフォームの /etc ディレクトリにあります。

### snmpd.conf の変更

snmpd.conf ファイルでホスト名を設定します。

```
trapsink サーバ public
```

ここで「サーバ」は、トラップの送り先ホスト名を表します。

snmpd.conf ファイルに、次の記述を追加してください。

```
master agentx
```

また、次のように変更してください。

| 元の記述  | 変更後の記述                                       |
|---|--|
| com2sec notConfigUser default public                              | com2sec demouser default public              |
| group notConfigGroup v1 notConfigUser                             | group demogroup v1 demouser                  |
| view systemview included system                                   | view all included .1                         |
| access notConfigGroup "" any noauth exact<br>systemview none none | access demogroup "" any noauth exact all all |

上の内容が snmpd.conf ファイルに存在しない場合は追加してください。

**重要:** 設定ファイルを書き替えた場合、マスタエージェントとサブエージェントを再起動する必要があります。

### マスタエージェントの起動

マスタエージェントを起動するには、次のコマンドを実行してください。

```
/usr/sbin/snmpd -C -c /etc/snmpd.conf
```

### サブエージェントの起動

サブエージェントを起動するには、次のコマンドを実行してください。

```
/etc/init.d/ndssnmppsa start
```

**注:** サブエージェントを起動中に未定義のシンボル (EVP\_md5 エラー) が発生した場合は、[473 ページの「サブエージェントの起動時の問題」](#)を参照してください。

ユーザ名とパスワードを求められるので入力してください。正常に認証されれば、`/etc/ndssnmp/ndssnmp.cfg` で `INTERACTION = on` という設定になっている場合、次のようなメッセージが現れます。

```
Do you want to remember password?(Y/N)
```

ここで「**Y**」と入力すると、パスワードが保存されます。次回からは、パスワードを入力することなくサブエージェントを起動できます。

「**N**」と入力した場合は、次回からもパスワードを求められます。

**重要**: SLES 9 または OES Linux の場合については、サブエージェントの起動時に起きる既知の問題に関する `Readme` を参照してください。

## サブエージェントの停止

サブエージェントを停止するには、次のコマンドを実行してください。

```
/etc/init.d/ndssnmpsa stop
```

## Linux (SLES 9 または OES 以外) での SNMP サービスの設定

- ◆ [471 ページの「マスタエージェントの設定」](#)
- ◆ [471 ページの「マスタエージェントの起動」](#)
- ◆ [473 ページの「サブエージェントの起動」](#)
- ◆ [473 ページの「サブエージェントの停止」](#)

## マスタエージェントの設定

`net-snmp-5.0.9-4.rh73.i386.rpm` を <http://sourceforge.net/projects/net-snmp> (<http://sourceforge.net/projects/net-snmp>) からダウンロードします。

`net-snmp-5.0.9-4.rh73.i386.rpm` をシステムにインストールするには、`rpm-4.0.4-7x.i386.rpm` が必要です。`rpm-4.0.4-7x.i386.rpm` は、<http://rpmfind.net/linux/RPM/rpm.org/rpm/dist/rpm-4.0.x/rpm-4.0.4-7x.i386.html> (<http://rpmfind.net/linux/RPM/rpm.org/rpm/dist/rpm-4.0.x/rpm-4.0.4-7x.i386.html>) からダウンロードできます。

さらに、[470 ページの「snmpd.conf の変更」](#) の説明に従って、`snmpd.conf` ファイルを変更する必要があります。

## マスタエージェントの起動

マスタエージェントを起動するには、まず `net-snmp-5.0.9-4.rh73.i386.rpm` をインストールして設定します。

そのためには、次の 2 つのオプションのいずれかを使用します。ただし、オプション 2 ではシステムにインストールされた SNMP パッケージのアンインストールが必要となります。これはすべての従属する rpm のアンインストールも必要となるため、オプション 1 を使用することをお勧めします。

## オプション 1

- 1 net-snmp-5.0.9-4.rh73.i386.rpm および rpm-4.0.4-7x.i386.rpm を、/home/ndssnmp などの任意の場所にインストールします。

次を実行して net-snmp-5.0.9-4.rh73.i386.rpm をインストールします。

```
# cd /home/ndssnmp
# rpm2cpio net-snmp-5.0.9-4.rh73.i386.rpm | cpio -ivd
```

- 2 rpm-4.0.4-7x.i386.rpm (snmpd が必要とする従属 rpm) をインストールします。

```
# cd /home/ndssnmp
# rpm2cpio rpm-4.0.4-7x.i386.rpm | cpio -ivd
```

- 3 次を実行して、パスをエクスポートします。

```
# export LD_LIBRARY_PATH=/home/ndssnmp/usr/lib
```

- 4 次を実行してマスタエージェントを起動します。

```
# /home/ndssnmp/usr/sbin/snmpd -C -c snmpd.conf
```

たとえば、/etc ディレクトリに snmpd.conf ファイルがある場合、コマンドは次のものに似た内容となります。

```
# /home/ndssnmp/usr/sbin/snmpd -C -c /etc/snmpd.conf
```

**注:** ndssnmpsa を起動するために必要な関連情報が snmpd.conf ファイルにあることを確認します。詳細については、[469 ページの「SLES 9 または OES Linux での SNMP サービスの設定」](#)を参照してください。

- 5 (状況によって実行) マスタエージェントの起動中に、次のエラーが発生する場合があります。

```
snmpd: error while loading shared libraries: libcrypto.so.2: cannot open
shared object file: No such file or directory
```

システムに libcrypto.so.2 がインストールされていない場合に発生するエラーです。

この場合は、次のようにシステムにインストールされた暗号ライブラリへの直接のリンクを作成する必要があります。

```
# cd /usr/lib
```

さらに、次のいずれか 1 つを Linux のバージョンに応じて追加します。

- ◆ **Red Hat Advanced Server 3.0 の場合 :**

```
# ln -s libcrypto.so libcrypto.so.2
```

- ◆ **SUSE Linux Enterprise Server 8 の場合 :**

```
# ln -s libcrypto.so.0.9.6 libcrypto.so.2
```

- 6 (状況によって実行) SNMP マスタエージェントがすでにデフォルトポート #161 に設定されている場合は、次のポートでマスタエージェントを起動します。

```
# /home/ndssnmp/usr/sbin/snmpd -C -c /etc/snmpd.conf 1161
```

## オプション 2

- 1 システムにインストールされた `snmp` パッケージをアンインストールします。
- 2 SNMP パッケージがすでにインストールされており、そのバージョンが `net-snmp-5.0.9-4.rh73.i386.rpm` 以外であれば、SNMP パッケージをアンインストールして `net-snmp-5.0.9-4.rh73.i386.rpm` をインストールします。

注: 従属 RPM が必要な場合は、それらをダウンロードしてインストールしてください。

- 3 次を実行してマスタエージェントを起動します。

```
/usr/sbin/snmpd -C -c /etc/snmpd.conf
```

## サブエージェントの起動

サブエージェントを起動するには、次のコマンドを実行してください。

```
/etc/init.d/ndssnmpsa start
```

注: サブエージェントを起動中に未定義のシンボル (EVP\_md5 エラー) が発生した場合は、[473 ページの「サブエージェントの起動時の問題」](#)を参照してください。

ユーザ名とパスワードを求められるので入力してください。正常に認証されれば、`/etc/ndssnmp/ndssnmp.cfg` で `INTERACTION = on` という設定になっている場合、次のようなメッセージが現れます。

```
Do you want to remember password?(Y/N)
```

ここで「**Y**」と入力すると、パスワードが保存されます。次回からは、パスワードを入力することなくサブエージェントを起動できます。

「**N**」と入力した場合は、次回からもパスワードを求められます。

## サブエージェントの停止

サブエージェントを停止するには、次のコマンドを実行してください。

```
/etc/init.d/ndssnmpsa stop
```

## サブエージェントの起動時の問題

サブエージェントの起動時に、次のエラーが発生する可能性があります。

```
/opt/novell/eDirectory/bin/ndssnmpsa: error while loading shared libraries:  
/usr/lib/libnetsnmp.so.5: undefined symbol: EVP_md5.
```

このエラーを解決するには、`libcrypto` のパスをエクスポートする必要があります。例:

```
export LD_PRELOAD=/lib/libcrypto.so.0.9.7a:/usr/lib/libwrap.so.0
```

`libcrypto.so.0.9.7a` は、システム上で別の名前になっている可能性があります。これは、インストールされている暗号バージョンに応じて異なります。

### マスタエージェントの設定

SNMP パッケージのロードに先立ち、Solstice Enterprise master agent 1.0.3 をインストールしておく必要があります。まだであれば、[Solstice Enterprise Agents](http://www.sun.com/software/entagents) (<http://www.sun.com/software/entagents>) Web サイトからダウンロードしてください。

- 1 ファイル `/etc/snmp/conf/snmpd.conf` でホスト名を設定します。また、次の書式でトラップの設定をしておいてください。

**trap** サーバ

ここで「サーバ」は、トラップの送り先ホスト名を表します。

- 2 ファイル `/etc/snmp/conf/snmpdx.acl` のトラップパラメータ部に、次のような設定を追加してください。

トラップコミュニティ= public

hosts = サーバ {

enterprise = "Novell eDirectory"

トラップ番号= 1-117, 2001, 2002 }

ここで、「トラップコミュニティ」はトラップに使うコミュニティ名、「サーバ」はトラップの送り先ホスト名、*Novell eDirectory* はエンタープライズ MIB、「トラップ番号」はトラップの範囲を表します。

**重要:** 設定ファイルを書き替えた場合、マスタエージェントとサブエージェントを再起動する必要があります。

### マスタエージェントの起動

マスタエージェントを起動するには、次のコマンドを実行してください。

```
/usr/lib/snmp/snmpdx -y -c /etc/snmp/conf
```

### サブエージェントの設定

Solaris では、サブエージェント `ndssnmpsa` はデーモンとして動作します。

サブエージェントの設定には、`/etc/snmp/conf` 以下にある、次の設定ファイルを使います。

- ◆ `ndsmib.reg` はサブエージェントの登録ファイルです。
- ◆ `ndsmib.acl` は SNMP サブエージェントの設定ファイルです。

### サブエージェントの起動

サブエージェントを起動するには、次のコマンドを実行してください。

```
/etc/init.d/ndssnmpsa start
```

ユーザ名とパスワードを求められるので入力してください。正常に認証されれば、`/etc/ndssnmp/ndssnmp.cfg` で `INTERACTION = on` という設定になっている場合、次のようなメッセージが現れます。

```
Do you want to remember password?(Y/N)
```

ここで「**Y**」と入力すると、パスワードが保存されます。次回からは、パスワードを入力することなくサブエージェントを起動できます。

「**N**」と入力した場合は、次回からもパスワードを求められます。

### サブエージェントの停止

サブエージェントを停止するには、次のコマンドを実行してください。

```
/etc/init.d/ndssnmpsa stop
```

### マスタエージェントの設定

ファイル `/etc/snmpd.conf` で、トラップの送り先を次のように記述してください。

`trap` コミュニティ サーバ 表示名 トラップマスク

ここで、

- ◆ 「コミュニティ」はトラップパケットにエンコードされるコミュニティ名を表します。
- ◆ 「サーバ」は、トラップの送り先ホスト名を表します。
- ◆ 「表示名」は固有のオブジェクト識別子で、数値をドット (.) で区切った書式で表します。

例：1.3.6.1.4.1.23.2.98. このパラメータの指定は任意です。指定がなければ、MIB ツリー全体を表示します。

- ◆ 「トラップマスク」は 16 進数で表します。

上位ビットから順に、`coldStart`、`warmStart`、`linkDown`、`linkUp`、`authenticationFailure`、`egpNeighborLoss`、`enterpriseSpecific` の各トラップに対応します。例の中で、一番右の「98」という値には何の意味もありません。「1」になっているビットに対応したトラップが送られるようになります。それ以外のトラップはブロックされます。

例：

fe どのトラップもブロックしません (1111 1110)

7e `coldStart` トラップをブロックします (0111 1110)

be `warmStart` トラップをブロックします (1011 1110)

3e `coldStart` トラップ、`warmStart` トラップをブロックします (0011 1110)

### マスタエージェントの起動

マスタエージェントを起動するには、次のコマンドを実行してください。

```
/usr/sbin/snmpdvl
```

### サブエージェントの起動

サブエージェントを起動するには、次のコマンドを実行してください。

```
/etc/ndssnmpsa start
```

ユーザ名とパスワードを求められるので入力してください。正常に認証されれば、`/etc/ndssnmp/ndssnmp.cfg` で `INTERACTION = on` という設定になっている場合、次のようなメッセージが現れます。

```
Do you want to remember password?(Y/N)
```

ここで「**y**」と入力すると、パスワードが保存されます。次回からは、パスワードを入力することなくサブエージェントを起動できます。

「**N**」と入力した場合は、次回からもパスワードを求められます。

### サブエージェントの停止

サブエージェントを停止するには、次のコマンドを実行してください。

```
/etc/ndssnmpsa stop
```

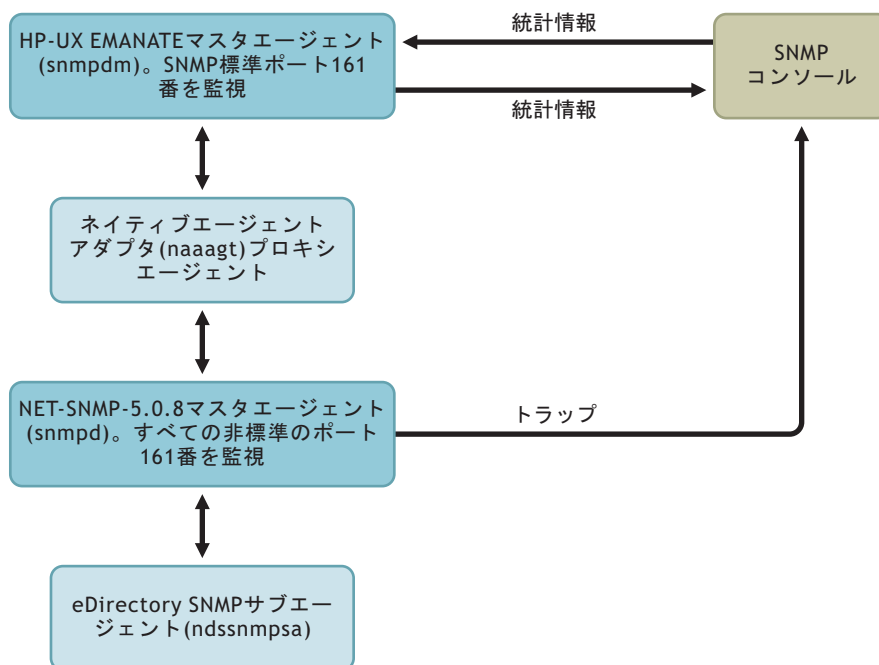
## HP-UX の場合

HP-UX の場合、EMANATE SNMP というネイティブマスタエージェントがあります。マスタエージェントを設定する場合、プロキシ SNMP エージェントの設定も必要です。プロキシエージェントの設定には NAA (Native Adapter Agent) を使います。NAA には、サードパーティ製 SNMP エージェントが、HP-UX SNMP マスタエージェント (snmpdm) と協調して動作できるようにする働きがあります。ここでは NET-SNMP マスタエージェントが、サードパーティ製 SNMP エージェントに相当します。NET-SNMP マスタエージェントは、NAA の設定と同じ非標準 UDP ポートを監視する必要があります。

詳しくは、[477 ページの「ネイティブエージェントアダプタ \(NAA\) の起動と設定」](#)および [477 ページの「NET-SNMP マスタエージェントの起動/設定」](#)を参照してください。

eDirectory SNMP サブエージェント、NET-SNMP マスタエージェント、NAA エージェント、HP-UX EMANATE マスタエージェント、SNMP コンソール間のデータの流れを図に示します。

図 49 SNMP データの流れ



### HP-UX SNMP マスタエージェントの起動

HP-UX SNMP マスタエージェントを起動するには、次のコマンドを実行してください。

```
/etc/snmpd
```

または

```
/usr/sbin/snmpdm
```

注: HP-UX SNMP マスタエージェントを停止するには、`/etc/snmpd -k` というコマンドを実行します。



## ネイティブエージェントアダプタ (NAA) の起動と設定

NAA エージェント (naaagt) の起動に先立ち、次の環境変数をエクスポートしておく必要があります。

- ◆ HP\_NAA\_CNF - NAA 設定ファイル名
- ◆ HP\_NAA\_PORT - NET-SNMP マスタエージェントが監視する非標準UDPポート番号
- ◆ HP\_NAA\_GET\_COMMUNITY - NAA から NET-SNMP マスタエージェントへの SNMP 要求で使うコミュニティ名。

例：

```
export HP_NAA_CNF=/etc/ndssnmp/ndssnmpNAA.cfg
export HP_NAA_PORT=8161 ## 非標準UDPポートを指定
export HP_NAA_GET_COMMUNITY=public
```

NAA エージェントについて詳しくは、naaagt のマニュアルページを参照してください。

次のコマンドを実行すると、NAA エージェントが起動されます。

**/usr/sbin/naaagt**

**注：**NAA エージェントを起動するには root としてのアクセス権が必要です。

## NET-SNMP マスタエージェントの起動 / 設定

NET-SNMP マスタエージェントを設定する前に、まずこれをダウンロードし、インストールしておく必要があります。

- 1 NET-SNMP バージョン 5.0.8 tar ファイル (net-snmpp-5.0.8-HP-UX\_B.11.00\_9000\_712.tar.gz) を、[SourceForge.net \(http://sourceforge.net/project/showfiles.php?group\\_id=12694\)](http://sourceforge.net/project/showfiles.php?group_id=12694) からダウンロードします。
- 2 上記 tar ファイルを展開すると NET-SNMP バージョン 5.0.8 のバイナリが得られます。これをカレントディレクトリ /usr/local 以下にインストールしてください。

NET-SNMP マスタエージェントを、次の手順で設定します。

- ◆ ファイル /etc/ndssnmp/snmpd-net-snmpp.conf でホスト名を設定します。  
trapsink サーバ public  
ここで「サーバ」は、トラップの送り先ホスト名を表します。
- ◆ /etc/ndssnmp/snmpd-net-snmpp.conf に次のような記述がなければ追加してください。  
master agentx

**注：**NET-SNMP 5.0.8 にはマスタエージェント設定ファイルのサンプルが付属していません。eDirectory SNMP コンポーネントに付属しているサンプルを使ってください。eDirectory をインストールすると、/etc/ndssnmp 以下にサンプルファイル snmpd-net-snmpp.conf があるはずです。

NET-SNMP 5.0.8 マスタエージェントは次のようなコマンドで起動します。

```
NET-SNMP がインストールされたディレクトリ /usr/local/sbin/snmpd -C -c /etc/ndssnmp/
snmpd-net-snmpp.conf 8161
```

**重要：**設定ファイルを書き替えた場合、マスタエージェントとサブエージェントを再起動する必要があります。

## サブエージェントの起動

サブエージェントを起動するには、次のコマンドを実行してください。

```
/sbin/init.d/ndssnmpsa start
```

ユーザ名とパスワードを求められるので入力してください。正常に認証されれば、`/etc/ndssnmp/ndssnmp.cfg` で `INTERACTION = on` という設定になっている場合、次のようなメッセージが現れます。

```
Do you want to remember password?(Y/N)
```

ここで「**Y**」と入力すると、パスワードが保存されます。次回からは、パスワードを入力することなくサブエージェントを起動できます。

「**N**」と入力した場合は、次回からもパスワードを求められます。

## サブエージェントの停止

サブエージェントを停止するには、次のコマンドを実行してください。

```
/sbin/init.d/ndssnmpsa stop
```

# SNMP による eDirectory の監視

eDirectory の動作を監視するために、SNMP の機能であるトラップや統計を使うことができます。

ただし、そのためには、NCP サーバ、LDAP グループ、LDAP サーバオブジェクトに対して、次のような権利が必要です。

- ◆ NCP サーバオブジェクトに対するスーパーバイザ権
- ◆ LDAP グループオブジェクトの「LDAP クリアテキストパスワードを許可する」属性に対する読み出し権利
- ◆ LDAP サーバオブジェクトの LDAP TCP Port 属性、LDAP SSL Port 属性に対する読み出し権利

通常、管理者としてログインしたユーザならば、SNMP により eDirectory サーバを監視する上で問題が生じることはありません。

## トラップ

ndsServerStart (2001) および ndsServerStop (2002) を設定できなかったトラップの中から、119 個のトラップが SNMP コンポーネントによって生成されます。これらのトラップはデフォルトで有効です。

トラップの生成状況は MIB ブラウザで確認できます。

注: なお、42 番、92 番、100 番のトラップは、NetWare の場合しか生成されません。

| トラップ<br>番号 | トラップ名              | 生成される条件   |
|------------|--------------------|---|
| 1          | ndsCreateEntry     | 新規オブジェクトがディレクトリに追加されたとき。<br><br>例：<br><br>LDAP ツール、ICE、ConsoleOne <sup>®</sup> 、iManager などを使ってオブジェクトを生成したとき。   |
| 2          | ndsDeleteEntry     | オブジェクトが削除されたとき。<br><br>例：<br><br>LDAP ツール、ICE、ConsoleOne、iManager などを使ってオブジェクトを削除したとき。  |
| 3          | ndsRenameEntry     | オブジェクト名が変更されたとき。<br><br>例：<br><br>LDAP ツール、ICE、ConsoleOne、iManager などを使ってオブジェクト名を変更したとき。  |
| 4          | ndsMoveSourceEntry | オブジェクトのコンテキストが変わったとき。このトラップにより、変更前のコンテキストが通知されます。<br><br>例：<br><br>ldapmodrdrn や ldapsdk でオブジェクトを移動したとき。  |
| 5          | ndsAddValue        | オブジェクトの属性値が追加されたとき。<br><br>例：<br><br>LDAP ツール、ICE、ConsoleOne、iManager などを使って、属性に新しい値を追加したとき。<br><br>注: 返される値が NULL の場合は、セキュリティ保護されたチャネルを経由してディレクトリにアクセスする必要があります。詳細については、 <a href="#">494 ページの「暗号化属性にアクセスする」</a> を参照してください。 |

| トラップ<br>番号 | トラップ名                  | 生成される条件  |
|------------|------------------------|--|
| 6          | ndsDeleteValue         | <p>オブジェクトの属性値が削除されたとき。</p> <p>例：</p> <p>LDAP ツール、ICE、ConsoleOne、iManager などを使って、属性値を削除したとき。</p> <p>注：返される値が NULL の場合は、セキュリティ保護されたチャネルを経由してディレクトリにアクセスする必要があります。詳細については、<a href="#">494 ページの「暗号化属性にアクセスする」</a>を参照してください。</p>                    |
| 7          | ndsCloseStream         | <p>ストリーム属性が変更されたとき。</p>  |
| 8          | ndsDeleteAttribute     | <p>オブジェクトの属性値 ( 単一値と定義されているもの ) が削除されたとき。</p> <p>例：</p> <p>LDAP ツール、ICE、ConsoleOne、iManager などを使って、属性値を削除したとき。</p> <p>注：返される値が NULL の場合は、セキュリティ保護されたチャネルを経由してディレクトリにアクセスする必要があります。詳細については、<a href="#">494 ページの「暗号化属性にアクセスする」</a>を参照してください。</p> |
| 9          | ndsCheckSecurityEquiv  | <p>あるエントリの同等セキュリティベクトルが検査されたとき。</p> <p>例：</p> <p>LDAP ツール、ICE、ConsoleOne、iManager などを使って、同等セキュリティ属性を変更したとき。</p>  |
| 10         | ndsUpdateSecurityEquiv | <p>あるエントリの同等セキュリティベクトルが変更されたとき。</p> <p>例：</p> <p>LDAP ツール、ICE、ConsoleOne、iManager などを使って、同等セキュリティ属性を変更したとき。</p>  |
| 11         | ndsMoveDestEntry       | <p>オブジェクトのコンテキストが変わったとき。このトラップにより、変更後のコンテキストが通知されます。</p> <p>例：</p> <p>ldapmodrdn や ldapsdk でオブジェクトを移動したとき。</p>   |
| 12         | ndsDeleteUnusedExtref  | <p>バックリンクオブジェクトが削除されたとき。</p>   |
| 13         | ndsAgentOpenLocal      | <p>ローカルディレクトリエージェントがオープンされたとき。</p> <p>例：</p> <p>標準修復を実行したとき。</p>   |

| トラップ<br>番号 | トラップ名                  | 生成される条件   |
|------------|------------------------|---|
| 14         | ndsAgentCloseLocal     | ローカルディレクトリエージェントがクローズされたとき。<br>例：<br>標準修復を実行したとき。   |
| 15         | ndsDSABadVerb          | DSAgent 要求に関連づけられたバード番号が正しくないとき。<br>例：<br>DClient 呼び出しを使って、eDirectory に不正なバード要求を送ったとき。                          |
| 16         | ndsMoveSubtree         | コンテナオブジェクトがそれに含まれるオブジェクトと共に移動されたとき。<br>例：LDAP ツール、ICE、ConsoleOne、iManager などを使って、パーティションを他のコンテキストに移動したとき。       |
| 17         | ndsNoReplicaPointer    | レプリカにレプリカポインタが関連づけられていないとき。   |
| 18         | ndsSynclnEnd           | インバウンド同期が終了したとき。  |
| 19         | ndsBacklinkSecurEquiv  | バックリンク操作により、オブジェクトの同等セキュリティベクトルが更新されたとき。<br>例：<br>LDAP ツール、ICE、ConsoleOne、iManager などを使って、同等セキュリティ属性を変更したとき。    |
| 20         | ndsBacklinkOperPrivChg | バックリンク操作により、オブジェクトのコンソールオペレータ権利が変更されたとき。  |
| 21         | ndsDeleteSubtree       | コンテナオブジェクトがそれに含まれるオブジェクトと共に削除されたとき。   |
| 22         | ndsReferral            | 参照が作成されたとき。   |
| 23         | ndsUpdateClassDef      | スキーマクラス定義が更新されたとき。<br>例：<br>新規クラスまたは属性をプライマリサーバに追加し、セカンダリサーバ側で、LDAP ツール、ICE、ConsoleOne、iManager などを使って同期を取ったとき。 |
| 24         | ndsUpdateAttributeDef  | スキーマ属性定義が更新されたとき。<br>例：<br>新規属性をプライマリサーバに追加し、セカンダリサーバ側で、LDAP ツール、ICE、ConsoleOne、iManager などを使って同期を取ったとき。        |
| 25         | ndsLostEntry           | eDirectory のローカルサーバには存在しないはずのエントリに対する更新要求があったとき。  |
| 26         | ndsPurgeEntryFail      | ページ処理に失敗したとき。   |

| トラップ<br>番号 | トラップ名                 | 生成される条件   |
|------------|-----------------------|---|
| 27         | ndsPurgeStart         | ページ処理を開始したとき。<br><br>例：<br><br>dstrace を実行し、ndstrace=*j と設定したとき。                                  |
| 28         | ndsPurgeEnd           | ページ処理が終了したとき。<br><br>例：<br><br>dstrace を実行し、ndstrace=*j と設定したとき。                                  |
| 29         | ndsLimberDone         | limber 処理が終了したとき。<br><br>例：<br><br>dstrace の設定により、所定の時間間隔で limber (レプリカの同期更新) 処理が起動され、終了したとき。     |
| 30         | ndsPartitionSplitDone | パーティション分割処理が終了したとき。<br><br>例：<br><br>ConsoleOne、iManager などを使って、パーティションを作成したとき。                   |
| 31         | ndsSyncServerOutStart | ある特定のサーバに同期するアウトバウンド同期処理が起動されたとき。<br><br>例：<br><br>dstrace の設定により、所定の時間間隔でアウトバウンド同期処理が起動されたとき。    |
| 32         | ndsSyncServerOutEnd   | ある特定のサーバに同期するアウトバウンド同期処理が終了したとき。<br><br>例：<br><br>dstrace の設定により、所定の時間間隔でアウトバウンド同期処理が起動され、終了したとき。 |
| 33         | ndsSyncPartitionStart | パーティション同期処理が起動されたとき。<br><br>例：<br><br>あるコンテナをパーティション分割したとき。                                       |
| 34         | ndsSyncPartitionEnd   | パーティション同期処理が終了したとき。<br><br>例：<br><br>あるコンテナをパーティション分割したとき。  |

| トラップ<br>番号 | トラップ名                | 生成される条件  |
|------------|----------------------|--|
| 35         | ndsMoveTreeStart     | サブツリーの移動処理が起動されたとき。<br><br>パーティションの移動に伴い、サブツリーも移動します。<br><br>例：<br><br>ConsoleOne、iManager などを使って、パーティションを作成し、他のコンテナに移動したとき。   |
| 36         | ndsMoveTreeEnd       | サブツリーの移動処理が終了したとき。<br><br>パーティションの結合処理に伴い、サブツリーも移動します。<br><br>例：<br><br>ConsoleOne、iManager などを使って、パーティションを作成し、他のコンテナに移動したとき。  |
| 37         | ndsJoinPartitionDone | パーティションの結合処理が終了したとき。<br><br>例：<br><br>ConsoleOne、iManager などを使って、パーティションを作成し、他のパーティションと結合したとき。   |
| 38         | ndsPartitionLocked   | パーティションがロックされたとき ( 結合処理の際など )。<br><br>例：<br><br>ConsoleOne、iManager などを使って、パーティションを作成したとき。   |
| 39         | ndsPartitionUnlocked | パーティションのロックが解除されたとき ( 結合処理が終了したときなど )。<br><br>例：<br><br>ConsoleOne、iManager などを使って、パーティションを作成したとき。   |
| 40         | ndsSchemaSync        | スキーマの同期処理が起こったとき。<br><br>例：<br><br>Idapsdk schsync のスケジュール設定により、スキーマの同期処理が始まったとき。  |
| 41         | ndsNameCollision     | 他のサーバにある別のオブジェクトと名前が重複 ( 衝突 ) したとき。<br><br>例：<br><br>iMonitor を使い、プライマリサーバとセカンダリサーバのアウトバウンド同期処理を無効にした状態で、LDAP ツールを使って両サーバにユーザオブジェクトを作成したとします。こうしておいて、iMonitor でアウトバウンド同期処理を実行すると、衝突が起こります。 |

| トラップ<br>番号 | トラップ名                  | 生成される条件   |
|------------|------------------------|---|
| 42         | ndsNLMLoaded           | NetWare で、NLM™ プログラムがロードされたとき。<br>このトラップは NetWare でのみ発生します。<br>例：<br>nldap.nlm をロードまたはアンロードしたとき。                    |
| 43         | ndsChangeModuleState   | eDirectory モジュール (NLM / DLM) がロードまたはアンロードされたとき。<br>例：<br>nldap モジュールをロードまたはアンロードしたとき。                               |
| 44         | ndsLumberDone          | バックグラウンドでの limber 処理が始まったとき。  |
| 45         | ndsBacklinkProcDone    | バックリンク処理が終了したとき。<br>例：<br>dstrace の設定により、所定の時間間隔でバックリンク処理が起動され、終了したとき。  |
| 46         | ndsServerRename        | サーバ名が変更されたとき。<br>例：<br>ldapmodrdn または ldapsdk を使って、サーバ名を変更したとき。   |
| 47         | ndsSyntheticTime       | 将来のタイムスタンプを付与したオブジェクトが作成されたとき。eDirectory サーバの同期に際しては、合成時刻として扱うこととなります。<br>例：<br>ndsconfig を使って、セカンダリサーバをツリーに追加したとき。 |
| 48         | ndsServerAddressChange | limber 処理によりサーバ参照が変更されたとき。<br>例：<br>サーバの IP アドレスを変更して ndsd を再起動したとき。  |
| 49         | ndsDSARead             | エントリが読み出されたとき。<br>eDirectory を対象とする操作があれば、必ずこのトラップが生成されます。<br>例：<br>ldapsearch を実行したとき。                             |
| 50         | ndsLogin               | eDirectory へのログインがあったとき。<br>例：<br>ndslogin を使ってツリーにログインしたとき。  |



| トラップ<br>番号 | トラップ名                | 生成される条件  |
|------------|----------------------|--|
| 51         | ndsChangePassword    | パスワードが変更されたとき。<br>例：<br>ldapmodify を使ってユーザオブジェクトのパスワードを変更したとき。                               |
| 52         | ndsLogout            | eDirectory からログアウトされたとき。<br>例：<br>Novell クライアントからツリーへの接続を切ったとき。                              |
| 53         | ndsAddReplica        | サーバパーティションにレプリカが追加されたとき。<br>例：<br>ndsconfig を使ってツリーに新規レプリカを追加したとき。                           |
| 54         | ndsRemoveReplica     | レプリカが削除されたとき。<br>例：<br>ConsoleOne、iManager などを使って、あるサーバからレプリカを削除したとき。                        |
| 55         | ndsSplitPartition    | パーティションが分割されたとき。<br>例：<br>ConsoleOne、iManager などを使って、パーティションを作成したとき。                         |
| 56         | ndsJoinPartition     | ペアレントパーティションにチャイルドパーティションが結合されたとき。<br>例：<br>パーティションを作成しておき、ConsoleOne、iManager などを使って結合したとき。 |
| 57         | ndsChangeReplicaType | パーティションのレプリカタイプが変更されたとき。<br>例：<br>レプリカタイプをマスタから読み書き用に変更したとき。                                 |
| 58         | ndsAddEntry          | 新規オブジェクトが追加されたとき。<br>例：<br>ConsoleOne、iManager などを使って、新規オブジェクトを追加したとき。                       |
| 59         | ndsAbortPartitionOp  | パーティションに関する処理が中断されたとき。<br>例：<br>コンテナのパーティション分割処理を実行し、途中で中断したとき。                              |

| トラップ<br>番号 | トラップ名                 | 生成される条件   |
|------------|-----------------------|---|
| 60         | ndsRecvReplicaUpdates | 同期処理中に、レプリカ側で更新通知を受け取ったとき。<br><br>例：<br><br>複数のサーバツリーから成る構成の eDirectory サーバで、レプリカを保持しているサーバに対して更新要求を送った場合。この操作は ConsoleOne や iManager で実行できます。  |
| 61         | ndsRepairTimeStamps   | レプリカのタイムスタンプが修復されたとき。<br><br>例：<br><br>dsrepair (Linux および UNIX の場合は ndsrepair、Windows の場合は NDSCons) を使って、タイムスタンプの DIB 修復処理を実行したとき。   |
| 62         | ndsSendReplicaUpdates | 同期処理中にレプリカが更新されたとき。<br><br>例：<br><br>複数のサーバツリーから成る構成の eDirectory サーバで、レプリカを保持しているサーバに対して更新要求を送った場合。この操作は ConsoleOne や iManager で実行できます。   |
| 63         | ndsVerifyPass         | パスワードが正しいと確認されたとき。<br><br>例：<br><br>無効になったパスワードを変更する際、確認のために入力させた旧パスワードが正しいと確認されたとき。  |
| 64         | ndsBackupEntry        | エントリがバックアップされたとき。<br><br>例：<br><br>dsbackup ユーティリティ (Linux および UNIX の場合は ndsbackup、Windows の場合は NDSCons) を使って、eDirectory オブジェクトをバックアップしたとき。   |
| 65         | ndsRestoreEntry       | エントリが復元されたとき。<br><br>例：<br><br>dsbackup ユーティリティ (Linux および UNIX の場合は ndsbackup、Windows の場合は NDSCons) を使って、バックアップされていた eDirectory オブジェクトを復元したとき。   |
| 66         | ndsDefineAttributeDef | スキーマに属性定義が追加されたとき。<br><br>例：<br><br>eDirectory ツリースキーマに属性定義を追加して拡張したとき。ZENWorks <sup>®</sup> 、NMAST <sup>™</sup> などといった eDirectory 用アプリケーションをインストールすると、スキーマは拡張されず。また、ConsoleOne や iManager、Linux および UNIX 用スキーマ拡張ユーティリティ ndssch でも拡張できます。 |

| トラップ<br>番号 | トラップ名                 | 生成される条件   |
|------------|-----------------------|---|
| 67         | ndsRemoveAttributeDef | スキーマから属性定義が削除されたとき。<br><br>例：<br><br>eDirectory ツリースキーマから属性定義を削除したとき。属性は、ConsoleOne や iManager、Linux および UNIX 用スキーマ拡張ユーティリティ ndssch を使って削除できます。   |
| 68         | ndsRemoveClassDef     | スキーマからクラス定義が削除されたとき。<br><br>例：<br><br>eDirectory ツリースキーマからオブジェクトクラス定義を削除したとき。オブジェクトクラスは、ConsoleOne や iManager、Linux および UNIX 用スキーマ拡張ユーティリティ ndssch を使って削除できます。  |
| 69         | ndsDefineClassDef     | スキーマにクラス定義が追加されたとき。<br><br>例：<br><br>eDirectory ツリースキーマにクラス定義を追加して拡張したとき。ZENWorks、NMAS などといった eDirectory 用アプリケーションをインストールすると、スキーマは拡張されず。また、ConsoleOne や iManager、Linux および UNIX 用スキーマ拡張ユーティリティ ndssch でも拡張できます。 |
| 70         | ndsModifyClassDef     | クラス定義が変更されたとき。<br><br>例：<br><br>既存のオブジェクトクラスや属性定義を変更したとき。   |
| 71         | ndsResetDSCounters    | eDirectory に内蔵されたカウンタがリセットされたとき。  |
| 72         | ndsRemoveEntryDir     | エントリーに関連づけられたディレクトリが削除されたとき。  |
| 73         | ndsCompAttributeValue | 属性値が比較されたとき。<br><br>例：<br><br>属性値を他のオブジェクトの属性値と比較したとき。<br><br>ユーザオブジェクトを対象とする LDAP 検索により、入力された値と電話番号が一致するかどうか検査するような場合。   |
| 74         | ndsOpenStream         | ストリーム属性がオープンまたはクローズされたとき。<br><br>例：<br><br>読み込み用または書き出し用としてストリームを生成した、あるいはオープンしたとき。<br><br>ユーザオブジェクトのログインスクリプトを作成したとき。DIB ディレクトリ以下にファイルが生成される結果、このトラップが発生します。   |

| トラップ<br>番号 | トラップ名                   | 生成される条件  |
|------------|-------------------------|--|
| 75         | ndsListSubordinates     | <p>コンテナオブジェクトに対して、それに含まれるエントリのリストを取得する処理が実行されたとき。この処理では、コンテナオブジェクトの直下にあるエントリのみが検索の対象となります。</p> <p>例：</p> <p>ConsoleOne、iManager などを使って、コンテナオブジェクトをクリックすることにより、これに含まれるオブジェクトを一覧表示しようとしたとき。</p>  |
| 76         | ndsListContainerClasses | <p>エントリに対して、これを含めることができるクラスのリストを取得する処理が実行されたとき。</p> <p>例：</p> <p>あるオブジェクトについて、これを含めることができるクラス (コンテナクラス) を一覧表示しようとしたとき。</p> <p>ユーザオブジェクトを含めることができるコンテナクラスを検索すれば、Organization (組織)、Organization Unit (部署)、Domain (ドメイン) などといったクラスが表示されるはずです。</p> |
| 77         | ndsInspectEntry         | <p>エントリの検査処理が実行されたとき。</p> <p>例：</p> <p>あるエントリについて、これまでにエラーが発生したことがあるかどうかを検査しようとしたとき。</p> <p>バックグラウンドで eDirectory のフラットクリーナ処理を実行する際にこのイベントが発生する結果、トラップが送られることとなります。</p>   |
| 78         | ndsResendEntry          | <p>エントリの再送信処理が実行されたとき。</p> <p>例：</p> <p>レプリカの作成処理中に、エントリの再送信が起こったとき。サーバ間の接続に問題があり、オブジェクトの送信に失敗したような場合に起こります。</p>   |
| 79         | ndsMutateEntry          | <p>エントリの変換処理が実行されたとき。</p> <p>例：</p> <p>バイナリオブジェクトクラスからユーザオブジェクトクラスに変換したとき。</p>   |
| 80         | ndsMergeEntries         | <p>2つのエントリがマージされたとき。</p> <p>例：</p> <p>2つのユーザオブジェクトをマージしたとき。Entry2 (ndsEntryName2) を Entry (ndsEntryName) にマージしたような場合。</p>  |

| トラップ<br>番号 | トラップ名                 | 生成される条件   |
|------------|-----------------------|---|
| 81         | ndsMergeTree          | 2つの eDirectory ツリーがマージされたとき。<br><br>例：<br><br>dsmerge (Linux および UNIX の場合は ndsmerge、Windows の場合は NDSCons) を使って、2つの eDirectory ツリーをマージしたとき。      |
| 82         | ndsCreateSubref       | サブオーディネートリファレンスが生成されたとき。<br><br>例：<br><br>チャイルドパーティションのレプリカをサーバから削除したとき。自動的にサブオーディネートリファレンスのレプリカが生成され、その結果トラップが発生します。                           |
| 83         | ndsListPartitions     | パーティションのリスト取得処理が実行されたとき。<br><br>例：<br><br>ConsoleOne や iManager を使い、パーティションビューやスキーマビューで eDirectory サーバオブジェクトをクリックすることにより、サーバ上のパーティションを一覧表示したとき。 |
| 84         | ndsReadAttribute      | 属性値が読み出されたとき。<br><br>例：<br><br>ツリーの検索処理を実行したとき。   |
| 85         | ndsReadReferences     | エントリの参照が読み出されたとき。   |
| 86         | ndsUpdateReplica      | パーティションレプリカに対して、レプリカの更新処理が実行されたとき。<br><br>例：<br><br>あるサーバからユーザを削除したとき。他のサーバ上のレプリカでもこれを削除しようとするため、更新処理が起こります。                                    |
| 87         | ndsStartUpdateReplica | パーティションレプリカに対して、レプリカの更新開始処理が開始されたとき。<br><br>例：<br><br>あるサーバからユーザを削除したとき。他のサーバ上のレプリカでもこれを削除しようとするため、更新処理が起こります。                                  |
| 88         | ndsEndUpdateReplica   | パーティションレプリカに対して、レプリカの更新処理が実行され、終了したとき。<br><br>例：<br><br>あるサーバからユーザを削除したとき。他のサーバ上のレプリカでもこれを削除しようとするため、更新処理が起こります。                                |

| トラップ<br>番号 | トラップ名                   | 生成される条件   |
|------------|-------------------------|---|
| 89         | ndsSyncPartition        | パーティションレプリカに対して、パーティションの同期処理が実行されたとき。<br><br>例：<br><br>あるパーティションからユーザを削除したとき。ndstrace を使うと同期処理の状況を見ることができます。  |
| 90         | ndsSyncSchema           | ルートのマスタレプリカが、そのスキーマをサーバと同期させる要求を受け取ったとき。<br><br>例：<br><br>ConsoleOne から [ウィザード] > [スキーマ] と操作するか、LDAP ツール、ndssch ユーティリティなどを使って、新規クラスを追加したとき。   |
| 91         | ndsCreateBackLink       | バックリンクが生成されたとき。ローカルには存在しないオブジェクトが参照されると、バックリンクが生成されます。<br><br>例：<br><br>複数のサーバから成る構成で、いくつかのユーザを含むパーティションを生成したとします。サーバの1つからこのパーティションを削除すると、サブオーディネートリファレンスが生成されます。このとき、削除されたパーティションに存在していたユーザを参照するバックリンクが生成されます。 |
| 92         | ndsCheckConsoleOperator | バックリンクにより、コンソールオペレータの権利が検査されたとき。<br><br>このトラップは NetWare でのみ発生します。   |
| 93         | ndsChangeTreeName       | ツリー名が変更されたとき。<br><br>例：<br><br>マージユーティリティ dsmerge/ndsmerge を使ってツリー名を変更したとき。   |
| 94         | ndsStartJoinPartition   | パーティションの結合処理が始まったとき。<br><br>例：<br><br>ConsoleOne、LDAP ツールなどを使って、パーティションを結合したとき。   |
| 95         | ndsAbortJoinPartition   | パーティションの結合処理が中断されたとき。<br><br>例：<br><br>ConsoleOne、LDAP ツールなどを使って、パーティションを結合したとき。  |

| トラップ番号 | トラップ名                   | 生成される条件  |
|--------|-------------------------|--|
| 96     | ndsUpdateSchema         | スキーマ更新処理が実行されたとき。<br>例：<br>ConsoleOne から [ウィザード] > [スキーマ] と操作するか、LDAP ツール、ndssch ユーティリティなどを使って、新規クラスを追加したとき。 |
| 97     | ndsStartUpdateSchema    | スキーマ更新処理が開始されたとき。<br>例：<br>ConsoleOne から [ウィザード] > [スキーマ] と操作するか、LDAP ツール、ndssch ユーティリティなどを使って、新規クラスを追加したとき。 |
| 98     | ndsEndUpdateSchema      | スキーマ更新処理が終了したとき。<br>例：<br>ConsoleOne から [ウィザード] > [スキーマ] と操作するか、LDAP ツール、ndssch ユーティリティなどを使って、新規クラスを追加したとき。  |
| 99     | ndsMoveTree             | ツリー移動処理が実行されたとき。<br>例：<br>パーティションをあるコンテナから別のコンテナに移動したとき。   |
| 100    | ndsReloadDS             | DS が再ロードされたとき。<br>このトラップは NetWare でのみ発生します。<br>例：<br>dstrace=*R と設定したとき。                                     |
| 101    | ndsConnectToAddress     | 特定のアドレスとの間で接続が確立されたとき。<br>例：<br>ConsoleOne、iManager などを使ってツリーをブラウズしたとき。                                      |
| 102    | ndsSearch               | 検索処理が実行されたとき。<br>例：<br>LDAP ツールを使ってツリーに対する ldapsearch を実行したとき。   |
| 103    | ndsPartitionStateChange | パーティションが作成または削除されたとき。<br>例：<br>新規パーティションを作成したとき。   |

| トラップ<br>番号 | トラップ名                     | 生成される条件   |
|------------|---------------------------|---|
| 104        | ndsRemoveBacklink         | 使われていない外部参照が削除され、該当するオブジェクトを保持しているサーバに対して、バックリンク削除要求が送られたとき。  |
| 105        | ndsLowLevelJoinPartition  | パーティションの結合処理中に、低レベルの結合処理が実行されたとき。<br><br>例：<br><br>ConsoleOne、iManager、LDAP ツールなどを使って、パーティションを結合したとき。 |
| 106        | ndsCreateNameBase         | eDirectory ネームベースが作成されたとき。  |
| 107        | ndsChangeSecurityEquals   | 同等セキュリティ属性が変更されたとき。<br><br>例：<br><br>ConsoleOne、iManager などを使って、あるユーザの同等セキュリティを変更し、管理者と同等にしたとき。       |
| 108        | ndsRemoveEntry            | eDirectory からエントリが削除されたとき。<br><br>例：<br><br>ConsoleOne、iManager などを使って、ユーザを削除したとき。                    |
| 109        | ndsCRCFailure             | 断片化した NCP 要求を構成し直す際に、CRC ( 冗長巡回検査 ) エラーが発生したとき。   |
| 110        | ndsModifyEntry            | eDirectory エントリが変更されたとき。<br><br>例：<br><br>ConsoleOne、iManager などを使って、ユーザの属性を変更したとき。                   |
| 111        | ndsNewSchemaEpoch         | スキーマが DSRepair でリセットされたとき。<br><br>例：<br><br>Linux および UNIX 上で、ndsrepair -S-Ad を使って新規スキーマエポックを作成したとき。  |
| 112        | ndsLowLevelSplitPartition | パーティションを作成する際に、低レベル分割処理が実行されたとき。<br><br>例：<br><br>ConsoleOne、iManager、LDAP ツールなどを使って、パーティションを作成したとき。  |
| 113        | ndsReplicaInTransition    | レプリカが追加または削除されたとき。  |



| トラップ<br>番号 | トラップ名             | 生成される条件   |
|------------|-------------------|---|
| 114        | ndsAclModify      | <p>オブジェクトのトラスティが変更された、すなわち ACL (アクセス制御リスト) オブジェクトが変更されたとき。</p> <p>例 :</p> <p>LDAP ツール、ICE、ConsoleOne、iManager などを使って、オブジェクトのトラスティを追加、変更、削除したとき。</p>   |
| 115        | ndsLoginEnable    | <p>ユーザアカウントを有効にする要求をサーバから受け取ったとき。</p> <p>例 :</p> <p>LDAP ツール、ICE、ConsoleOne、iManager などを使って、アカウント属性を無効から有効に変更したとき。</p>  |
| 116        | ndsLoginDisable   | <p>ユーザアカウントを無効にする要求をサーバから受け取ったとき。</p> <p>例 :</p> <p>LDAP ツール、ICE、ConsoleOne、iManager などを使って、アカウント属性を有効から無効に変更したとき。</p>  |
| 117        | ndsDetectIntruder | <p>不正侵入を検出したため、ユーザアカウントがロックされたとき。</p> <p>例 :</p> <p>LDAP ツール、ICE、ConsoleOne、iManager などを使って不正侵入 (Intruder) 属性を設定することにより、ユーザアカウントをロックしたとき。</p>   |
| 2001       | ndsServerStart    | <p>サブエージェントが eDirectory サーバに、正常に再接続できたとき。このトラップには 2 つの変数が含まれています。</p> <ul style="list-style-type: none"> <li>◆ ndsTrapTime : サブエージェントが eDirectory サーバに再接続した時刻を、1970 年 1 月 1 日午前 0 時 (万国標準時) からの経過秒数で表します。</li> <li>◆ ndsServerName : サブエージェントが再接続した eDirectory サーバを表します。</li> </ul> <p>例 :</p> <p>サブエージェントが稼働したままの状態であった eDirectory サーバを停止し、再び起動したとき。</p> |

| トラップ<br>番号 | トラップ名         | 生成される条件  |
|------------|---------------|--|
| 2002       | ndsServerStop | <p>サブエージェントと eDirectory サーバとの接続が失われたとき。このトラップには 2 つの変数が含まれています。</p> <ul style="list-style-type: none"> <li>◆ ndsTrapTime : サブエージェントが eDirectory サーバと切断された時刻を、1970 年 1 月 1 日午前 0 時 (万国標準時) からの経過秒数で表します。</li> <li>◆ ndsServerName : サブエージェントがそれまで接続されていた eDirectory サーバを表します。</li> </ul> <p>例 :</p> <p>サブエージェントが稼動中に eDirectory サーバを停止したとき。</p> |

## 暗号化属性にアクセスする

eDirectory 8.8 以降では、特定の重要データをディスクに保存したり、ネットワーク上からそのデータにアクセスする場合に、データを暗号化して保護できます。暗号化属性へのアクセスにセキュリティ保護されたチャネルを使用する場合は、事前にそれを指定できます。詳細については、[247 ページの「暗号化属性にアクセスする」](#)を参照してください。

暗号化属性へのアクセスにセキュリティ保護されたチャネルのみを使用すると指定している場合は、NDS 値イベントがブロックされます。値イベントに関連するトラップの値データは NULL になり、暗号化属性の値を取得するにはセキュリティ保護されたチャネルが必要であるということを示すエラー「-6089」が返されます。値データが NULL になるトラップは次のとおりです。

- ◆ ndsAddValue
- ◆ ndsDeleteValue
- ◆ ndsDeleteAttribute

## トラップに関する設定

トラップに関する設定の手順はプラットフォームによって異なります。

| プラットフォーム       | ユーティリティ       |
|----------------|---------------|
| NetWare        | dssnmpsa      |
| Windows        | ndssnmpcfg    |
| Linux および UNIX | ndssnmpconfig |

## NetWare の場合

NetWare では、`dssnmpsa` を使ってトラップに関する設定を行います。これは `sys:\etc\` ディレクトリにあります。このユーティリティの機能としては、トラップの有効 / 無効の切り替え、各トラップ間の時間間隔の設定、デフォルトの時間間隔の設定、操作に失敗した場合のトラップの有効化、すべてのトラップのリスト表示などがあります。

`dssnmpsa` の使い方が分からなくなったときは、コマンドラインから「`help dssnmpsa`」と入力してください。

使用法 :

`dssnmpsa` *トラップコマンド*

NetWare で使えるトラップコマンドについては、[495 ページの「NetWare のトラップコマンド」](#)を参照してください。

### NetWare のトラップコマンド

| トラップコマンド | 説明  | 使用法   |
|----------|---|---|
| DISABLE  | トラップを無効にするコマンド。NMS は、トラップが送られてきても受け取らないようになります。 | <code>dssnmpsa "DISABLE <i>トラップ指定</i>"</code><br><br>「 <i>トラップ指定</i> 」は次のいずれかの形式で指定してください。<br><br>特定のトラップ ( 次の例では 10 番、11 番、100 番 ) を無効にしたい場合 :<br><br><code>dssnmpsa "DISABLE 10, 11, 100"</code><br><br>特定のトラップ ( 次の例では 10 番、11 番、100 番 ) 以外をすべて無効にしたい場合 :<br><br><code>dssnmpsa "DISABLE ID != 10, 11, 100"</code><br><br>ある範囲の番号のトラップ ( 次の例では 20 ~ 29 番 ) を無効にしたい場合 :<br><br><code>dssnmpsa "DISABLE 20-29"</code><br><br>トラップをすべて無効にしたい場合 :<br><br><code>dssnmpsa "DISABLE ALL"</code> |

| トラップコマンド | 説明  | 使用法  |
|----------|---|--|
| ENABLE   | <p>トラップを有効にするコマンド。NMSは、送られてきたトラップを受け取るようになります。</p>  | <p>dssnmpsa "ENABLE <i>トラップ指定</i>"</p> <p>「<i>トラップ指定</i>」は次のいずれかの形式で指定してください。</p> <p>特定のトラップ ( 次の例では 10 番、11 番、100 番 ) を有効にしたい場合 :</p> <p>dssnmpsa "ENABLE 10, 11, 100"</p> <p>特定のトラップ ( 次の例では 10 番、11 番、100 番 ) 以外をすべて有効にしたい場合 :</p> <p>dssnmpsa "ENABLE ID != 10, 11, 100"</p> <p>ある範囲の番号のトラップ ( 次の例では 20 ~ 29 番 ) を有効にしたい場合 :</p> <p>dssnmpsa "ENABLE 20-29"</p> <p>トラップをすべて有効にしたい場合 :</p> <p>dssnmpsa "ENABLE ALL"</p> |
| INTERVAL | <p>時間間隔を設定する、または表示するためのコマンド。</p> <p>ここでいう時間間隔とは、同じトラップを繰り返し送る場合に、何秒間の間隔をおくかを表すものです。</p> <p>0 ~ 2,592,000 の範囲 ( 秒単位 ) で設定してください。</p> <p>この範囲外の値を指定した場合、デフォルトの時間間隔が指定されたものとみなします。</p> <p>設定値を 0 とすれば、トラップがすべて送られるようになります。</p> | <p>時間間隔の設定値を表示する場合 :</p> <p>dssnmpsa "213,240,79 INTERVAL"</p> <p>複数のトラップについて時間間隔を設定する場合 ( 次の例では 12 番、17 番、101 番トラップについて 5 秒と設定 ) :</p> <p>dssnmpsa "12 17 101 INTERVAL 5"</p> <p>デフォルトの時間間隔を表示する場合 :</p> <p>dssnmpsa "DEFAULT INTERVAL"</p> <p>デフォルトの時間間隔を設定する場合 :</p> <p>dssnmpsa "DEFAULT INTERVAL = 10"</p>  |

| トラップコマンド | 説明                         | 使用法   |
|----------|----------------------------|---|
| LIST     | ある条件を満たすトラップ番号を一覧表示するコマンド。 | <p>dssnmpsa LIST <i>トラップ指定</i></p> <p>「<i>トラップ指定</i>」には、トラップ番号のほか、以下に述べるキーワードで条件を指定できます。</p> <p>ALL、ENABLED、DISABLED、FAILED、またはこれらを論理演算子でつないだもの。</p> <p>例：</p> <p>有効なトラップをすべて、名称を添えて表示：</p> <p>dssnmpsa LIST ENABLED</p> <p>無効なトラップをすべて、名称を添えて表示：</p> <p>dssnmpsa LIST DISABLED</p> <p>117 種類すべてのトラップについて、名称を添えて表示：</p> <p>dssnmpsa LIST ALL</p> <p>特定の番号 ( 次の例では 12 番、224 番、300 番 ) のトラップについて、名称を添えて表示：</p> <p>dssnmpsa LIST ID = 12,224,300</p> <p>特定の番号 ( 次の例では 12 番、224 番、300 番 ) 以外のトラップをすべて、名称を添えて表示：</p> <p>dssnmpsa LIST ID != 12,224,300</p> <p>有効なエラートラップをすべて、名称を添えて表示：</p> <p>dssnmpsa LIST FAILED</p> |

| トラップコマンド | 説明  | 使用法  |
|----------|---|--|
| READ_CFG | <p>設定ファイル ndstrap.cfg を参照して、ディレクトリ構成を再設定するコマンド。</p> <p>環境設定ファイルの設定に加えられた変更はすべて有効になります。いくつかのコマンドを ndstrap.cfg に記述しておき、ひとまとめにして実行する、という使い方を主として想定したユーティリティです。</p> <p>ndstrap.cfg は sys:%etc% 以下にあります。</p> <p>ndstrap.cfg ファイルでは、トラップの環境設定に使用されるオペレーショナルパラメータを設定し、SNMP トラップの操作を設定する方法を指定します。このファイルは、READ_CFG コマンドにより起動される、トラップの環境設定ユーティリティ ndssnmpconfig が参照します。</p> | dssnmppsa "READ_CFG"   |
| FAILURE  | <p>エラートラップをすべて表示するコマンド。</p> <p>エラートラップとは、イベントの失敗時に生成されるトラップのことです。</p> <p>注：エラートラップをいったん無効にし、「enable trapid」コマンドで再び有効にすると、エラートラップではなく、正常に処理されたことを表すトラップとして扱われるようになります。</p>   | <p>dssnmppsa "FAILURE トラップ指定"</p> <p>「トラップ指定」には、トラップ番号をコンマまたはスペースで区切って指定するほか、キーワード「ALL」や論理式を指定できます。</p> <p>例：</p> <p>複数のトラップをエラートラップと設定：</p> <p>dssnmppsa "FAILURE 10,11,100"</p> <p>指定した番号以外のすべてのトラップをエラートラップと設定：</p> <p>dssnmppsa "FAILURE ID != 24,30"</p> <p>すべてのトラップをエラートラップと設定：</p> <p>dssnmppsa "FAILURE ALL"</p> |

## Windows の場合

Windows では、`ndssnmpcfg` を使ってトラップに関する設定を行います。このユーティリティはインストールパス `%snmp%` ディレクトリにあります。このユーティリティの機能としては、トラップの有効 / 無効の切り替え、各トラップ間の時間間隔の設定、デフォルトの時間間隔の設定、操作に失敗した場合のトラップの有効化、すべてのトラップのリスト表示などがあります。

使用法 :

```
ndssnmpcfg -h [ ホスト名[: ポート] ] -p パスワード -a ユーザ FDN -c コマンド
```

| パラメータ | 説明  |
|-------|---|
| -h    | DNS ホスト名または IP アドレス                       |
| -p    | 認証に使う「ユーザ FDN」パスワード                       |
| -a    | 管理者権限を持つユーザの完全識別名                         |
| -c    | トラップコマンド (499 ページの「Windows のトラップコマンド」を参照) |

## Windows のトラップコマンド

| トラップコマンド | 説明  | 使用法   |
|----------|---|---|
| DISABLE  | トラップを無効にするコマンド。NMS は、トラップが送られてきても受け取らないようになります。 | 特定のトラップ ( 次の例では 10 番、11 番、100 番 ) を無効にしたい場合 :<br><code>ndssnmpcfg "DISABLE 10, 11, 100"</code><br><br>特定のトラップ ( 次の例では 10 番、11 番、100 番 ) 以外をすべて無効にしたい場合 :<br><code>ndssnmpcfg "DISABLE ID != 10, 11, 100"</code><br><br>ある範囲の番号のトラップ ( 次の例では 20 ~ 29 番 ) を無効にしたい場合 :<br><code>ndssnmpcfg "DISABLE 20-29"</code><br><br>トラップをすべて無効にしたい場合 :<br><code>ndssnmpcfg "DISABLE ALL"</code> |

| トラップコマンド | 説明  | 使用法  |
|----------|---|--|
| ENABLE   | <p>トラップを有効にするコマンド。NMSは、送られてきたトラップを受け取るようになります。</p>  | <p>ndssnmpcfg "ENABLE <i>トラップ指定</i>"</p> <p>「<i>トラップ指定</i>」は次のいずれかの形式で指定してください。</p> <p>特定のトラップ ( 次の例では 10 番、11 番、100 番 ) を有効にしたい場合 :</p> <p>ndssnmpcfg "ENABLE 10, 11, 100"</p> <p>特定のトラップ ( 次の例では 10 番、11 番、100 番 ) 以外をすべて有効にしたい場合 :</p> <p>ndssnmpcfg "ENABLE ID != 10, 11, 100"</p> <p>ある範囲の番号のトラップ ( 次の例では 20 ~ 29 番 ) を有効にしたい場合 :</p> <p>ndssnmpcfg "ENABLE 20-29"</p> <p>トラップをすべて有効にしたい場合 :</p> <p>ndssnmpcfg "ENABLE ALL"</p> |
| INTERVAL | <p>時間間隔を設定する、または表示するためのコマンド。</p> <p>ここでいう時間間隔とは、同じトラップを繰り返し送る場合に、何秒間の間隔をおくかを表すものです。</p> <p>0 ~ 2,592,000 の範囲 ( 秒単位 ) で設定してください。</p> <p>この範囲外の値を指定した場合、デフォルトの時間間隔が指定されたものとみなします。</p> <p>設定値を 0 とすれば、トラップがすべて送られるようになります。</p> | <p>時間間隔の設定値を表示する場合 :</p> <p>ndssnmpcfg "213,240,79 INTERVAL"</p> <p>複数のトラップについて時間間隔を設定する場合 ( 次の例では 12 番、17 番、101 番トラップについて 5 秒と設定 ) :</p> <p>ndssnmpcfg "12 17 101 INTERVAL 5"</p> <p>デフォルトの時間間隔を表示する場合 :</p> <p>ndssnmpcfg "DEFAULT INTERVAL"</p> <p>デフォルトの時間間隔を設定する場合 :</p> <p>ndssnmpcfg "DEFAULT INTERVAL=10"</p>  |



| トラップコマンド | 説明                         | 使用法   |
|----------|----------------------------|---|
| LIST     | ある条件を満たすトラップ番号を一覧表示するコマンド。 | <p>ndssnmpcfg LIST <i>トラップ指定</i></p> <p>「<i>トラップ指定</i>」には、トラップ番号のほか、以下に述べるキーワードで条件を指定できます。</p> <p>ALL、ENABLED、DISABLED、FAILED、またはこれらを論理演算子でつないだもの。</p> <p>例：</p> <p>有効なトラップをすべて、名称を添えて表示：</p> <pre>ndssnmpcfg LIST ENABLED</pre> <p>無効なトラップをすべて、名称を添えて表示：</p> <pre>ndssnmpcfg LIST DISABLED</pre> <p>117 種類すべてのトラップについて、名称を添えて表示：</p> <pre>ndssnmpcfg LIST ALL</pre> <p>特定の番号 ( 次の例では 12 番、224 番、300 番 ) のトラップについて、名称を添えて表示：</p> <pre>ndssnmpcfg LIST ID = 12,224,300</pre> <p>特定の番号 ( 次の例では 12 番、224 番、300 番 ) 以外のトラップをすべて、名称を添えて表示：</p> <pre>ndssnmpcfg LIST ID != 12,224,300</pre> <p>有効なエラートラップをすべて、名称を添えて表示：</p> <pre>ndssnmpcfg LIST FAILED</pre> |

| トラップコマンド | 説明  | 使用法  |
|----------|---|--|
| READ_CFG | <p>設定ファイル ndstrap.cfg を参照して、ディレクトリ構成を再設定するコマンド。</p> <p>環境設定ファイルの設定に加えられた変更はすべて有効になります。いくつかのコマンドを ndstrap.cfg に記述しておき、ひとまとめにして実行する、という使い方を主として想定したユーティリティです。</p> <p>ファイル ndstrap.cfg はディレクトリインストールディレクトリ¥SNMP にあります。</p> <p>ndstrap.cfg ファイルでは、トラップの環境設定に使用されるオペレーショナルパラメータを設定し、SNMPトラップの操作を設定する方法を指定します。このファイルは、READ_CFG コマンドにより起動される、トラップの環境設定ユーティリティ ndssnmpcfg が参照します。</p> | ndssnmpcfg "READ_CFG"  |
| FAILURE  | <p>エラートラップをすべて表示するコマンド。</p> <p>エラートラップとは、イベントの失敗時に生成されるトラップのことです。</p> <p>注：エラートラップをいったん無効にし、「enable trapid」コマンドで再び有効にすると、エラートラップではなく、正常に処理されたことを表すトラップとして扱われるようになります。</p>   | <p>ndssnmpcfg "FAILURE <i>トラップ指定</i>"</p> <p>「<i>トラップ指定</i>」には、トラップ番号をコンマまたはスペースで区切って指定するほか、キーワード「ALL」や論理式を指定できます。</p> <p>例：</p> <p>複数のトラップをエラートラップと設定：</p> <p>ndssnmpcfg "FAILURE 10,11,100"</p> <p>指定した番号以外のすべてのトラップをエラートラップと設定：</p> <p>ndssnmpcfg "FAILURE ID != 24,30"</p> <p>すべてのトラップをエラートラップと設定：</p> <p>ndssnmpcfg "FAILURE ALL"</p> |

## Linux、UNIX の場合 :

Linux および UNIX では、`ndssnmpconfig` を使ってトラップに関する設定を行います。これは `/etc/ndssnmp/` ディレクトリにあります。このユーティリティの機能としては、トラップの有効/無効の切り替え、各トラップ間の時間間隔の設定、デフォルトの時間間隔の設定、操作に失敗した場合のトラップの有効化、すべてのトラップのリスト表示などがあります。

使用法 :

```
ndssnmpconfig -h [ ホスト名[: ポート] ] -p パスワード -a ユーザFDN -c コマンド
```

| パラメータ | 説明   |
|-------|--|
| -h    | DNS ホスト名または IP アドレス                              |
| -p    | 認証に使う「ユーザFDN」パスワード                               |
| -a    | 管理者権利を持つユーザの完全識別名                                |
| -c    | トラップコマンド (503 ページの「Linux および UNIX のトラップコマンド」を参照) |

## Linux および UNIX のトラップコマンド

| トラップコマンド | 説明  | 使用法   |
|----------|---|---|
| DISABLE  | トラップを無効にするコマンド。NMS は、トラップが送られてきても受け取らないようになります。 | 特定のトラップ ( 次の例では 10 番、11 番、100 番 ) を無効にしたい場合 :<br><code>ndssnmpconfig "DISABLE 10, 11, 100"</code><br><br>特定のトラップ ( 次の例では 10 番、11 番、100 番 ) 以外をすべて無効にしたい場合 :<br><code>ndssnmpconfig "DISABLE ID != 10, 11, 100"</code><br><br>ある範囲の番号のトラップ ( 次の例では 20 ~ 29 番 ) を無効にしたい場合 :<br><code>ndssnmpconfig "DISABLE 20-29"</code><br><br>トラップをすべて無効にしたい場合 :<br><code>ndssnmpconfig "DISABLE ALL"</code> |

| トラップコマンド | 説明  | 使用法  |
|----------|---|--|
| ENABLE   | <p>トラップを有効にするコマンド。NMS は、送られてきたトラップを受け取るようになります。</p>   | <p><code>ndssnmpconfig "ENABLE <i>トラップ指定</i>"</code></p> <p>「<i>トラップ指定</i>」は次のいずれかの形式で指定してください。</p> <p>特定のトラップ ( 次の例では 10 番、11 番、100 番 ) を有効にしたい場合 :</p> <p><code>ndssnmpconfig "ENABLE 10, 11, 100"</code></p> <p>特定のトラップ ( 次の例では 10 番、11 番、100 番 ) 以外をすべて有効にしたい場合 :</p> <p><code>ndssnmpconfig "ENABLE ID != 10, 11, 100"</code></p> <p>ある範囲の番号のトラップ ( 次の例では 20 ~ 29 番 ) を有効にしたい場合 :</p> <p><code>ndssnmpconfig "ENABLE 20-29"</code></p> <p>トラップをすべて有効にしたい場合 :</p> <p><code>ndssnmpconfig "ENABLE ALL"</code></p> |
| INTERVAL | <p>時間間隔を設定する、または表示するためのコマンド。</p> <p>ここでいう時間間隔とは、同じトラップを繰り返し送る場合に、何秒間の間隔をおくかを表すものです。</p> <p>0 ~ 2,592,000 の範囲 ( 秒単位 ) で設定してください。</p> <p>この範囲外の値を指定した場合、デフォルトの時間間隔が指定されたものとみなします。</p> <p>設定値を 0 とすれば、トラップがすべて送られるようになります。</p> | <p>時間間隔の設定値を表示する場合 :</p> <p><code>ndssnmpconfig "213,240,79 INTERVAL"</code></p> <p>複数のトラップについて時間間隔を設定する場合 ( 次の例では 12 番、17 番、101 番トラップについて 5 秒と設定 ) :</p> <p><code>ndssnmpconfig "12 17 101 INTERVAL 5"</code></p> <p>デフォルトの時間間隔を表示する場合 :</p> <p><code>ndssnmpconfig "DEFAULT INTERVAL"</code></p> <p>デフォルトの時間間隔を設定する場合 :</p> <p><code>ndssnmpconfig "DEFAULT INTERVAL=10"</code></p>  |

| トラップコマンド | 説明                         | 使用法  |
|----------|----------------------------|--|
| LIST     | ある条件を満たすトラップ番号を一覧表示するコマンド。 | <p>ndssnmpconfig LIST &lt; トラップ指定 &gt;</p> <p>「トラップ指定」には、トラップ番号のほか、以下に述べるキーワードで条件を指定できます。</p> <p>ALL、ENABLED、DISABLED、FAILED、またはこれらを論理演算子でつないだもの。</p> <p>例：</p> <p>有効なトラップをすべて、名称を添えて表示：</p> <pre>ndssnmpconfig LIST ENABLED</pre> <p>無効なトラップをすべて、名称を添えて表示：</p> <pre>ndssnmpconfig LIST DISABLED</pre> <p>117 種類すべてのトラップについて、名称を添えて表示：</p> <pre>ndssnmpconfig LIST ALL</pre> <p>特定の番号 ( 次の例では 12 番、224 番、300 番 ) のトラップについて、名称を添えて表示：</p> <pre>ndssnmpconfig LIST ID = 12,224,300</pre> <p>特定の番号 ( 次の例では 12 番、224 番、300 番 ) 以外のトラップをすべて、名称を添えて表示：</p> <pre>ndssnmpconfig LIST ID != 12,224,300</pre> <p>有効なエラートラップをすべて、名称を添えて表示：</p> <pre>ndssnmpconfig LIST FAILED</pre> |

| トラップコマンド | 説明   | 使用法  |
|----------|--|--|
| READ_CFG | <p>設定ファイル ndstrap.cfg を参照して、ディレクトリ構成を再設定するコマンド。</p> <p>環境設定ファイルの設定に加えられた変更はすべて有効になります。いくつものコマンドを ndstrap.cfg に記述しておき、ひとまとめにして実行する、という使い方を主として想定したユーティリティです。</p> <p>ファイル ndstrap.cfg はディレクトリ /etc/ndssnmp/ にあります。</p> <p>ndstrap.cfg ファイルでは、トラップの環境設定に使用されるオペレーショナルパラメータを設定し、SNMPトラップの操作を設定する方法を指定します。このファイルは、READ_CFG コマンドにより起動される、トラップの環境設定ユーティリティ ndssnmpcfg が参照します。</p> | ndssnmpconfig "READ_CFG"   |
| FAILURE  | <p>エラートラップをすべて表示するコマンド。</p> <p>エラートラップとは、イベントの失敗時に生成されるトラップのことです。</p> <p>注：エラートラップをいったん無効にし、「enable trapid」コマンドで再び有効にすると、エラートラップではなく、正常に処理されたことを表すトラップとして扱われるようになります。</p>  | <p>ndssnmpconfig "FAILURE <i>トラップ指定</i>"</p> <p>「<i>トラップ指定</i>」には、トラップ番号をコンマまたはスペースで区切って指定するほか、キーワード「ALL」や論理式を指定できます。</p> <p>例：</p> <p>複数のトラップをエラートラップと設定：</p> <pre>ndssnmpconfig "FAILURE 10,11,100"</pre> <p>指定した番号以外のすべてのトラップをエラートラップと設定：</p> <pre>ndssnmpconfig "FAILURE ID != 24,30"</pre> <p>すべてのトラップをエラートラップと設定：</p> <pre>ndssnmpconfig "FAILURE ALL"</pre> |

## 統計情報

- ◆ [507 ページの「ndsDbCache」](#)
- ◆ [508 ページの「ndsDbConfig」](#)
- ◆ [508 ページの「ndsProtolIfOps」](#)
- ◆ [510 ページの「ndsServerInt」](#)

## ndsDbCache

| ディレクトリ以下にある管理対象オブジェクト      | 説明                                    |
|----------------------------|---------------------------------------|
| ndsDbSrvApplIndex          | eDirectory サーバアプリケーションを固有に識別するインデックス。 |
| ndsDbDibSize               | eDirectory データベースの容量 (KB 単位)。         |
| ndsDbBlockSize             | eDirectory データベースのブロック容量 (KB 単位)。     |
| ndsDbEntryCacheMaxSize     | エントリキャッシュの最大容量 (KB 単位)。               |
| ndsDbBlockCacheMaxSize     | ブロックキャッシュの最大容量 (KB 単位)。               |
| ndsDbEntryCacheCurrentSize | 現在のエントリキャッシュ容量。                       |
| ndsDbBlockCacheCurrentSize | 現在のブロックキャッシュ容量。                       |
| ndsDbEntryCacheCount       | キャッシュ内のエントリ数。                         |
| ndsDbBlockCacheCount       | キャッシュ内のブロック数。                         |
| ndsDbEntryCacheOldVerCount | キャッシュ内に残っている旧バージョンのエントリ数。             |
| ndsDbBlockCacheOldVerCount | キャッシュ内に残っている旧バージョンのブロック数。             |
| ndsDbEntryCacheOldVerSize  | 旧バージョンのエントリキャッシュ容量。                   |
| ndsDbBlockCacheOldVerSize  | 旧バージョンのブロックキャッシュ容量。                   |
| ndsDbEntryCacheHits        | キャッシュ内のエントリがヒットした回数。                  |
| ndsDbBlockCacheHits        | キャッシュ内のブロックがヒットした回数。                  |
| ndsDbEntryCacheHitLooks    | キャッシュ内のエントリがヒットするかどうか試みられた回数。         |
| ndsDbBlockCacheHitLooks    | キャッシュ内のブロックがヒットするかどうか試みられた回数。         |
| ndsDbEntryCacheFaults      | キャッシュ内のエントリがヒットしなかった回数。               |
| ndsDbBlockCacheFaults      | キャッシュ内のブロックがヒットしなかった回数。               |
| ndsDbEntryCacheFaultLooks  | キャッシュ内のエントリがヒットしないかどうか試みられた回数。        |
| ndsDbBlockCacheFaultLooks  | キャッシュ内のブロックがヒットしないかどうか試みられた回数。        |

## ndsDbConfig

| ディレクトリ以下にある管理対象オブジェクト                | 説明   |
|--------------------------------------|--|
| ndsDbCfgSrvApplIndex                 | eDirectory サーバアプリケーションを固有に識別するインデックス。                  |
| ndsDbCfgDynamicCacheAdjust           | 動的キャッシュ調整が有効かどうか。<br>0 = 無効<br>1 = 有効                  |
| ndsDbCfgDynamicCacheAdjustPercent    | 動的キャッシュ調整に、空きメモリの何 % を割り当てるか。                          |
| ndsDbCfgDynamicCacheAdjustMin        | 動的キャッシュ調整に使う最小容量。キャッシュ容量制限を KB 単位で表したもの。               |
| ndsDbCfgDynamicCacheAdjustMinToLeave | 動的キャッシュ調整に使う最小容量のうち、利用可能なメモリから差し引く容量 (KB 単位)。          |
| ndsDbCfgHardLimitCacheAdjust         | キャッシュ調整に割り当てるメモリ容量にハード制限を設定するかどうか。<br>0 = 無効<br>1 = 有効 |
| ndsDbCfgHardLimitCacheAdjustMax      | キャッシュの最大容量 (KB 単位)。これはハードメモリ制限を表します。                   |
| ndsDbCfgBlockCachePercent            | ブロックキャッシュに割り当てる比率。                                     |
| ndsDbCfgCacheAdjustInterval          | キャッシュ調整を行う時間間隔 (秒単位)。                                  |
| ndsDbCfgCacheCleanupInterval         | キャッシュのクリーンアップを行う時間間隔 (秒単位)。                            |
| ndsDbCfgPermanentSettings            | 常時接続の設定が有効かどうか。<br>0 = 無効<br>1 = 有効                    |

## ndsProtolfOps

| ディレクトリ以下にある管理対象オブジェクト  | 説明  |
|------------------------|---|
| ndsProtolfSrvApplIndex | eDirectory サーバアプリケーションを固有に識別するインデックス。               |
| ndsProtolfIndex        | eDirectory サーバのプロトコルインタフェースに対応するエントリを固有に識別するインデックス。 |
| ndsProtolfDescription  | DS プロトコルインタフェースに使うポート番号。                            |
| ndsProtolfUnauthBinds  | 認証を省略した匿名バインド要求を受け取った回数。                            |



| ディレクトリ以下にある管理対象オブジェクト           | 説明  |
|---------------------------------|---|
| ndsProtolfSimpleAuthBinds       | バインド要求のうち、簡易認証手続きにより認証に成功したものの回数。簡易認証手続きとは、パスワードを暗号化して、またはクリアテキストのまま送ることにより行うものです。                            |
| ndsProtolfStrongAuthBinds       | バインド要求のうち、強度の高い認証手続きである SASL および X.500 の認証に成功したものの回数。外部認証手続きによるものも数に含まれます。                                    |
| ndsProtolfBindSecurityErrors    | バインド要求のうち、認証手続きが適切でない、あるいは認証情報が無効であるために拒否したものの回数。   |
| ndsProtolfInOps                 | DUA (ディレクトリユーザエージェント) または他の eDirectory サーバから受け取った要求の回数。   |
| ndsProtolfReadOps               | 受け取った読み出し要求の数。  |
| ndsProtolfCompareOps            | 受け取った比較要求の数。  |
| ndsProtolfAddEntryOps           | 受け取ったエントリ追加要求の数。  |
| ndsProtolfRemoveEntryOps        | 受け取ったエントリ削除要求の数。  |
| ndsProtolfModifyEntryOps        | 受け取ったエントリ変更要求の数。  |
| ndsProtolfModifyRDNops          | 受け取った RDN (相対識別名) 変更要求の数。   |
| ndsProtolfListOps               | 受け取ったリスト要求の数。   |
| ndsProtolfSearchOps             | 受け取った検索要求 (ベースオブジェクト検索、1 レベル検索、サブツリー全体の検索) の数。  |
| ndsProtolfOneLevelSearchOps     | 受け取った 1 レベル検索要求の数。  |
| ndsProtolfWholeSubtreeSearchOps | 受け取ったサブツリー全体の検索要求の数。  |
| ndsProtolfExtendedOps           | 拡張処理の回数。  |
| ndsProtolfReferrals             | 処理要求に応じて返した参照の個数。   |
| ndsProtolfChainings             | この eDirectory サーバから他の eDirectory サーバに転送した処理の数。  |
| ndsProtolfSecurityErrors        | 受け取った要求のうち、セキュリティ保護方針に合致しなかったものの数。  |
| ndsProtolfErrors                | 受け取った要求のうち、エラーのため応じなかったものの数。ただしセキュリティ保護エラー、参照エラーを除きます。一部でも処理ができたものは数に含めません。たとえば、名前づけや更新、属性、サービスに関連するエラーがあります。 |
| ndsProtolfReplicationUpdatesIn  | eDirectory サーバから取得した、または受け取ったレプリカ作成更新の数。  |
| ndsProtolfReplicationUpdatesOut | eDirectory サーバに送った、または検知されたレプリカ作成更新の数。  |

| ディレクトリ以下にある管理対象オブジェクト | 説明   |
|-----------------------|--|
| ndsProtolflnBytes     | インタフェース上の受信トラフィック (バイト単位)。DUA(ディレクトリユーザエージェント)からの要求、他の eDirectory サーバからの応答などといったトラフィックがこれに当たります。 |
| ndsProtolfOutBytes    | インタフェース上の送信トラフィック (バイト単位)。DUA や eDirectory サーバへの応答、他の eDirectory サーバへの要求などといったトラフィックがこれに当たります。   |

## ndsServerInt

| ディレクトリ以下にある管理対象オブジェクト             | 説明  |
|-----------------------------------|---|
| ndsSrvIntSrvApplIndex             | eDirectory サーバアプリケーションを固有に識別するインデックス。   |
| ndsSrvIntProtolfIndex             | eDirectory サーバのプロトコルインタフェースに対応するエントリを固有に識別するインデックス。   |
| ndsSrvIntIndex                    | このオブジェクトは ndsSrvIntSrvApplIndex および ndsSrvIntProtolfIndex と組み合わせて使います。ndsSrvIntSrvApplIndex で示される eDirectory サーバと、特別なプロトコルを使うピア eDirectory サーバとの間でやり取りされる情報を格納した、仮想的な行を固有に識別するためのキーとなります。 |
| ndsSrvIntURL                      | ピア eDirectory サーバの URL。   |
| ndsSrvIntTimeOfCreation           | この行が作成された時刻。1970 年 1 月 1 日午前 0 時 (万国標準時) からの経過秒数で表します。  |
| ndsSrvIntTimeOfLastAttempt        | ピア eDirectory サーバとの接続を試みた直近の時刻。1970 年 1 月 1 日午前 0 時 (万国標準時) からの経過秒数で表します。   |
| ndsSrvIntTimeOfLastSuccess        | ピア eDirectory サーバと正常に接続できた直近の時刻。1970 年 1 月 1 日午前 0 時 (万国標準時) からの経過秒数で表します。  |
| ndsSrvIntFailuresSinceLastSuccess | ピア eDirectory サーバと正常に接続した直近の時刻以降に発生したエラーの数。まだ一度も正常に接続できていない場合は、このエントリが作成されて以来のエラー数。   |
| ndsSrvIntFailures                 | このエントリが作成されて以来、ピア eDirectory サーバとの接続に失敗した回数。  |
| ndsSrvIntSuccesses                | このエントリが作成されて以来、ピア eDirectory サーバとの接続に成功した回数。  |

## トラブルシューティング

問題を迅速に解決できるよう、実際に発生したエラー状況、その解決に役立つ情報が、ログファイルに記録されています。

詳しくは「[Troubleshooting SNMP](#)」を参照してください。

| プラットフォーム          | サブエージェント   | サーバ   | マスタ  |
|-------------------|--|---|--|
| Windows NT / 2000 | インストールディレクトリ<br>¥nds¥dssnmpsa.log                    | インストールディレクトリ<br>¥nds¥dssnmpsrv.log          | 該当なし   |
| Solaris           | /var/opt/novell/<br>eDirectory/log/<br>ndssnmpsa.log | /var/opt/novell/<br>eDirectory/log/ndsd.log | /var/adm/messages  |
| Linux             | /var/opt/novell/<br>eDirectory/log/<br>ndssnmpsa.log | /var/opt/novell/<br>eDirectory/log/ndsd.log | /var/log/messages  |
| AIX               | /var/opt/novell/<br>eDirectory/log/<br>ndssnmpsa.log | /var/opt/novell/<br>eDirectory/log/ndsd.log | /var/adm/messages  |
| HP-UX             | /var/opt/novell/<br>eDirectory/log/<br>ndssnmpsa.log | /var/opt/novell/<br>eDirectory/log/ndsd.log | net-snmp-5.0.8 マスタエー<br>ジェント : /usr/adm/<br>snmpd.log<br><br>NAA エージェント : /var/<br>adm/snmpd.log |



# 16

## Novell eDirectory のメンテナンス

Novell® eDirectory™ のパフォーマンスを最適にするには、定期的なヘルスチェック手順を実行し、必要に応じてハードウェアのアップグレードや交換を行ってディレクトリをメンテナンスする必要があります。

この章では、次のメンテナンスに関するトピックについて説明します。

### パフォーマンス

- ◆ 513 ページの「eDirectory のパフォーマンスの改善」
- ◆ 522 ページの「Linux、Solaris、AIX、および HP-UX システムでの eDirectory パフォーマンスの改善」
- ◆ 528 ページの「eDirectory のパフォーマンスの改善」

### ヘルスチェック

- ◆ 533 ページの「eDirectory の正常な動作の維持」
- ◆ 536 ページの「監視のためのリソース」

### ハードウェアの交換

- ◆ 536 ページの「ハードウェアのアップグレードやサーバの交換」

### eDirectory の回復

- ◆ 543 ページの「ハードウェア障害後の eDirectory の復元」

## eDirectory のパフォーマンスの改善

eDirectory のパフォーマンスに最も大きく影響するのは、キャッシュの設定です。NDS® の以前のバージョンでは、ブロックキャッシュ制限を指定することにより、eDirectory がキャッシュに使用するメモリ量を制御できました。デフォルトでは、8 MB の RAM がキャッシュに使用されていました。

eDirectory 8.5 以降では、ブロックキャッシュ制限およびエン트리キャッシュ制限を指定できます。ブロックキャッシュは NDS の前のバージョンでも使用可能で、データベースの物理ブロックのみをキャッシュします。エン트리キャッシュは eDirectory 8.5 に導入された機能で、データベースの論理エントリをキャッシュします。エントリをキャッシュすることで、ブロックキャッシュからメモリ内にエントリをインスタンス化するために要する処理時間を削減できます。

この2つのキャッシュにはいくらか重複する部分がありますが、各キャッシュはそれぞれ異なる操作でのパフォーマンスを向上させるために設計されています。ブロックキャッシュは、更新操作で最も効果的です。エン트리キャッシュは、名前解決など、エントリを読み込んで eDirectory ツリーをブラウズする操作で最も効果的です。

ブロックキャッシュとエントリキャッシュのいずれも、クエリのパフォーマンスを向上させます。ブロックキャッシュは、インデックス検索を高速化します。エントリキャッシュは、インデックスから参照されるエントリの取得を高速化します。

eDirectory 8.8 のデフォルト値を次に示します。

- ◆ eDirectory をインストールするサーバにレプリカがない場合、デフォルトでは 16 MB のハードメモリ制限が設定され、ブロックキャッシュ用に 8 MB、エントリキャッシュ用に 8 MB が使用されます。  
詳細については、[515 ページの「ハードメモリ制限について」](#)を参照してください。
- ◆ サーバにレプリカがある場合、デフォルトでは使用可能メモリの 51% という動的調整制限が設定され、最小しきい値は 8 MB、最大しきい値は 24 MB になります。  
詳細については、[514 ページの「動的調整制限について」](#)を参照してください。

## エントリキャッシュとブロックキャッシュでメモリを配分する

キャッシュ用に使用可能な全メモリが、エントリキャッシュとブロックキャッシュとで共有されます。デフォルトでは、均等に配分されます。NDS 8 の以前のバージョンで使用できたブロックキャッシュ量を維持するには、eDirectory の合計キャッシュサイズを 2 倍にする必要があります。LDIF インポートのパフォーマンス向上のためにキャッシュを使用する場合、合計キャッシュサイズを 2 倍にするか、デフォルトのキャッシュ設定を変更します。デフォルトのキャッシュ設定を変更するには、[516 ページの「動的調整制限およびハードメモリ制限を設定する」](#)を参照してください。

キャッシュ可能なブロック数およびエントリ数が多いほど、全体のパフォーマンスは向上します。大きなデータベースの場合には不可能ですが、データベース全体をエントリキャッシュおよびブロックキャッシュにキャッシュできれば理想的です。一般的に、ブロックキャッシュと DIB セットの比率ができるだけ 1:1 になるように設定します。エントリキャッシュについては、1:2 または 1:4 の比率になるようにします。最適なパフォーマンスを得るためには、これらの比率を上回るようにしてください。

## デフォルトのキャッシュ設定を使用する

eDirectory には、キャッシュメモリの使用量を制御する方法として、動的調整制限とハードメモリ制限の 2 つの方法があります。どちらの方法も使用できますが、この 2 つは互いに排他的であるため同時に両方を使用することはできません。最後に使用した方法により、常に以前の設定が置き換えられます。

### 動的調整制限について

動的調整制限では、eDirectory は他のプロセスによるメモリ消費量の増減に応じて、定期的にメモリ使用量を調整します。制限は、使用可能な物理メモリの割合として指定します。eDirectory はこの割合を使用し、一定の間隔で新しいメモリ制限を再計算します。新しいメモリ制限は、その時点で使用可能な物理メモリの割合として算出されます。

割合とともに、しきい値として最大値および最小値も設定できます。しきい値はバイト数で指定し、eDirectory がその値に調整します。しきい値には、使用するバイト数、または使用可能量として残すバイト数のいずれかが指定できます。デフォルトの最小しきい値は 16 MB です。デフォルトの最大しきい値は 4 GB です。

最小しきい値と最大しきい値による制限が矛盾する場合は、最小しきい値が優先されます。たとえば、次のような設定を指定したとします。

|                   |                     |
|-------------------|---------------------|
| 最小しきい値            | 8 MB                |
| 使用する利用可能な物理メモリの割合 | 75                  |
| 最大しきい値            | 10 MB を使用可能量として維持する |

eDirectory がキャッシュ制限を調整するとき、使用可能な物理メモリが 16 MB あるとします。eDirectory は、新しい制限値を 12 MB として算出します。eDirectory は、算出した新しい制限値が最小しきい値と最大しきい値の範囲内にあるかをチェックします。この例では、最大しきい値の設定により 10 MB を使用可能量として残しておく必要があるため、eDirectory は制限値を 6 MB に設定します。しかし、最小しきい値は 8 MB であるため、eDirectory は最終的に制限値を 8 MB に設定します。

動的調整制限では、間隔の長さも指定します。デフォルトの間隔は 15 秒です。間隔が短いほど、より最新の状態に基づいてメモリが使用されます。ただし、割合の再計算によりメモリの割り当てと解放が発生するため、必ずしも間隔が短いほど良いわけではありません。

## ハードメモリ制限について

ハードメモリ制限は、eDirectory の以前のバージョンで、メモリ消費を制御するために使用されている方法です。次のいずれかの方法でハードメモリ制限を設定します。

- ◆ 固定バイト数
- ◆ 物理メモリの割合  
その期間の物理メモリの割合が、固定バイト数になります。
- ◆ 使用可能な物理メモリの割合  
その期間の使用可能な物理メモリの割合が、固定バイト数になります。

## キャッシュをクリーンアップする


NDS 8 はトランザクションの整合性を維持するために、キャッシュ内に複数のバージョンのブロックとエントリを作成します。NDS 8 の以前のバージョンでは、これらのブロックやエントリは不要になっても削除されませんでした。eDirectory 8.8 では、バックグラウンドプロセスにより定期的にキャッシュがブラウザされ、古いバージョンが消去されます。これにより、キャッシュメモリの消費量が最小限に抑えられます。デフォルトのブラウザ間隔は 15 秒です。

## 動的調整制限およびハードメモリ制限を設定する

動的調整制限およびハードメモリ制限は、次のいずれかの方法で設定できます。

- ◆ 516 ページの「Novell iMonitor を使用する」
- ◆ 517 ページの「\_ndsdb.ini ファイルの使用」

### Novell iMonitor を使用する

- 1 [エージェント環境設定]  をクリックします。
- 2 [データベースキャッシュ] をクリックし、次の情報を確認します。

| データベースキャッシュ情報   | 説明  |
|-----------------|---|
| 最大サイズ           | 指定したキャッシュが拡張できる最大サイズ (KB) です。   |
| 現在のサイズ          | 指定したキャッシュの現在のサイズ (KB) です。   |
| キャッシュされたアイテム    | 指定したキャッシュ内のアイテム数です。   |
| キャッシュされた古いバージョン | 指定したキャッシュ内の古いバージョンの数です。古いバージョンのキャッシュアイテムは、データベースの読み込みトランザクションの整合性を維持するために保持されます。つまり、あるスレッドが読み込みトランザクションを実行しており、別のスレッドが書き込みトランザクションを実行している場合、書き込みによって変更されるブロックの古いバージョンが読み込み操作のために保持されます。これは、読み込みのトランザクションを実行している間に変更処理が発生したとしても、読み込みの表示結果に整合性があるようにするためです。 |
| 古いバージョンのサイズ     | キャッシュされる古いバージョンのアイテムサイズ (KB) です。  |
| ヒット             | 指定したキャッシュ内のアイテムに正常にアクセスできた回数です。   |
| ヒット表示           | 指定したキャッシュ内で、アイテムに正常にアクセスする前に参照されたアイテム数です。ヒット表示とヒットの比率が、キャッシュ検索効率の目安となります。通常、この比率はほぼ 1:1 になるようにします。  |
| 失敗              | アイテムが指定したキャッシュ内に見つからず、低いレベルのキャッシュまたはディスクから取得されなければならなかった回数です。   |
| 失敗表示            | 必要なアイテムが指定したキャッシュ内にはないと判断されるまでに、キャッシュ内で参照されたアイテムの数です。失敗表示と失敗の比率が、キャッシュ検索効率の目安となります。通常、この比率はほぼ 1:1 になるようにします。  |



3 次のオプションから選択します。

| オプション            | 説明   |
|------------------|--|
| ダイナミック調整         | eDirectory データベースのキャッシュに使用するシステムメモリの大きさを、必要と判断される大きさと、次に示すパラメータに基づいて動的に調整します。                |
| キャッシュ調整パーセンテージ   | レコードキャッシュおよびブロックキャッシュに使用可能なメモリの割合です。   |
| キャッシュサイズの制約条件    | ダイナミック調整で、指定した制約条件に従います。つまり、キャッシュのメモリの大きさを指定した大きさより小さくせず、使用可能なメモリの合計から指定した大きさを引いた値より大きくしません。 |
| ハードメモリ制限         | キャッシュに使用するシステムメモリの正確な大きさです。  |
| キャッシュ最大サイズ       | レコードキャッシュとブロックキャッシュを合わせたサイズ (KB) です。   |
| ブロックキャッシュパーセンテージ | ブロックキャッシュに割り当てられる使用可能なシステムメモリの割合です。残りの割合が、レコードキャッシュに割り当てられます。                                |
| キャッシュ調整間隔        | この間隔は、ダイナミック調整を設定している場合のみ使用されます。調整間隔は、指定したパーセンテージと制約条件に基づき、どれくらいの頻度でキャッシュサイズを調整するかを制御します。    |
| キャッシュクリーンアップ間隔   | どれくらいの頻度で古い未使用のバージョンをキャッシュから削除するかを制御します。   |
| 永続的なキャッシュ設定      | このオプションを選択すると、iMonitor を使用して送信した変更は、前に保存した設定やデフォルトのシステム設定に上書きされ、永続的な変更になります。                 |

4 [送信] をクリックします。

### \_ndsdb.ini ファイルの使用

1 \_ndsdb.ini をテキストエディタで開きます。

NetWare® では、このファイルは sys:\netware にあります。通常、Windows NT および Windows 2000 では、このファイルは ¥Novell¥NDS¥DIBfiles にあります。

2 ファイルに該当する構文を追加します。

| コマンド                | 変数の説明      | 定義   |
|---------------------|------------|--|
| cache= キャッシュバ<br>イト | 使用する固定バイト数 | ハードメモリ制限を設定します。<br><br>たとえば、8 MB のハードメモリ制限を設定するには、次のように入力します。<br><br>cache=8000000 |

| コマンド              | 変数の説明  | 定義   |
|-------------------|--|--|
| cache= キャッシュオプション | <p>複数のオプションをコンマで区切り、任意の順序で指定できます。</p> <ul style="list-style-type: none"> <li>◆ DYN<br/>動的調整制限を設定します。</li> <li>◆ HARD<br/>ハードメモリ制限を設定します。</li> <li>◆ %: パーセンテージ<br/>使用する利用可能なメモリまたは物理メモリの割合を設定します。</li> <li>◆ AVAIL または TOTAL<br/>使用可能な物理メモリまたは合計物理メモリの割合を指定します。ハードメモリ制限においてのみ、使用できます。</li> <li>◆ MIN: バイト数<br/>最小バイト数。</li> <li>◆ MAX: バイト数<br/>最大バイト数。</li> <li>◆ LEAVE: バイト数<br/>使用可能量として残しておく最小バイト数。</li> </ul> | <p>ハードメモリ制限または動的調整制限を設定します。</p> <p>たとえば、動的調整制限で使用可能メモリを 75% に設定し、最小バイト数を 16 MB に設定するには、次のように入力します。</p> <p>cache=DYN,<br/>%:75,MIN:16000000</p> <p>また、ハードメモリ制限で合計物理メモリの 75% を設定し、最小バイト数を 16 MB に設定するには、次のように入力します。</p> <p>cache=HARD,%:75,MIN:<br/>16000000</p> |

**3** (オプション) 動的調整制限の間隔を指定するには、次の行を追加します。

cacheadjustinterval= 秒数

**4** (オプション) エントリとブロックの古いバージョンをクリーンアップする間隔を指定するには、次の行を追加します。

cachecleanupinterval= 秒数

**5** (オプション) ブロックキャッシュとエントリキャッシュでのメモリ配分の割合を変更するには、次の行を追加します。

blockcachepersent= パーセント

変数「パーセント」は、0 ~ 100 の範囲で指定する必要があります。ここで指定する割合は、ブロックキャッシュに使用するキャッシュメモリのパーセンテージです。残りの割合がエントリキャッシュ用に使用されます。割合を 0 に設定することはお勧めできません。

**6** 変更は、eDirectory サーバの再起動後に有効になります。

## DSTrace を使用して制限を設定する

eDirectory for NetWare を使用している場合、DSTrace で動的調整制限やハードメモリ制限を設定できます。変更を有効にするために、サーバを再起動する必要はありません。

- 1 (オプション) 固定バイト数のハードメモリ制限を設定するには、サーバコンソールで次のように入力します。

**SET DSTTRACE=! MB バイト単位でのRAMの使用量**

たとえば、8 MB のハードメモリ制限を設定するには、次のように入力します。

```
SET DSTTRACE=! MB8388608
```

- 2 (オプション) パーセンテージによって算出されるハードメモリ制限を設定するには、サーバコンソールで次のように入力します。オプションは、指定するものだけを入力します。

**SET DSTTRACE=!MHARD,AVAIL OR TOTAL,% : パーセント ,MIN : バイト数,  
MAX : バイト数 ,LEAVE : 残すバイト数 ,NOSAVE**

たとえば、ハードメモリ制限で合計物理メモリの 75% を設定し、最小バイト数を 16 MB に設定して、これらのオプションをスタートアップファイルに保存しないように指定するには、次のように入力します。

```
SET DSTTRACE=!MHARD,%:75,MIN:16777216,NOSAVE
```

- 3 (オプション) 動的調整制限を設定するには、サーバコンソールで次のように入力します。

**SET DSTTRACE=!MDYN,% : パーセント ,MIN : バイト数,MAX :  
バイト数,LEAVE : 残すバイト数,  
NOSAVE**

たとえば、動的調整制限で使用可能メモリの 75% を設定し、最小値を 8 MB に設定するには、次のように入力します。

```
SET DSTTRACE=!MDYN,%:75,MIN:8388608
```

## LDAP for eDirectory をチューニングする

基本的な LDAP サーバのハードウェアとソフトウェア設定、チューニングパラメータ、およびディレクトリ編成のヒントについての詳細は、[How to Configure and Optimize eDirectory LDAP Servers \(LDAP サーバを環境設定および最適化する方法\)](http://developer.novell.com/research/appnotes/2000/sepembe/04/a000904.htm) (<http://developer.novell.com/research/appnotes/2000/sepembe/04/a000904.htm>) を参照してください。

## メモリを管理する

eDirectory は、データベースキャッシュとディレクトリのためにメモリを使用します。これらはメモリプールとしてそれぞれに割り当てられます。ディレクトリエンジンは、オペレーティングシステムで利用できるメモリプールから必要なメモリを取り込んで使用します。データベースは、次に詳しく説明するパラメータにより定義されたキャッシュプールを使用します。一般に、eDirectory に割り当てるデータベースキャッシュの量が多いほどパフォーマンスはよくなります。ただし、eDirectory はバッファにシステムメモリを使用するため、クライアントがクエリを実行し、そのクエリが大量のデータを戻す場合には、ディレクトリで大量のクエリ応答を行えるように、データベースキャッシュのサイズを小さくして、システムメモリを確保しなければならない場合もあります。

データベースエンジンは、データベースキャッシュを使用して、最近アクセスしたブロックを保持します。このキャッシュの初期定義サイズは固定値で 16 MB です。このキャッシュのサイズは、出荷バージョンの eDirectory でコマンドラインから変更できます。次の例は、eDirectory データベースキャッシュのサイズを 80 MB に設定するコマンドです。

```
set dstrace=!mb 80000000
```

あるいは、NetWare サーバ上の SYS:¥\_netware ディレクトリまたは Windows や UNIX の環境における eDirectory データベースファイルが格納されたディレクトリ (Windows では通常、インストールディレクトリ \nds\dbfiles、Linux および UNIX では通常、\var\nds\dib) に \_ndsdb.ini という名前のファイルを定義することもできます。このテキストファイルに、次のような行を設定するだけです。

```
cache=80000000
```

等号 (=) の前後にスペースは入れないでください。

eDirectory 8.8 のキャッシュは、以前のバージョンと同様に、ハード制限値に基づいて初期化できます。さらに、上限と下限はハード値で設定できるほか、使用可能なメモリの割合でも設定できます。動的割り当て用の制御パラメータを使用すれば、キャッシュサイズを使用状態に応じて増減させることができます。適切なパラメータを設定すれば、データベースキャッシュは他のシステムリソースからの要求に応じて、そのサイズを増減させます。

\_ndsdb.ini ファイルを変更することにより、データベースメモリの使用を手動で制御できます。INI ファイルコマンドの形式は次のとおりです。

```
cache= キャッシュのバイト数 # Set a hard memory limit
```

他の形式を次の表に示します。

| コマンド                       | 説明   |
|----------------------------|--|
| cache= キャッシュオプション          | ハードメモリ制限または動的調整制限を設定します。複数のキャッシュオプションをコマンドで区切り、任意の順序で指定できます。これらはいずれも必須ではありません。キャッシュオプションを次に示します。 |
| DYN または HARD               | 動的制限またはハードメモリ制限。   |
| AVAIL または TOTAL            | ハードメモリ制限が選択された場合にのみ有効です。動的調整制限の場合は、これらのオプションは省略します。  |
| %: パーセンテージ                 | 使用可能な物理メモリまたは合計物理メモリの割合。   |
| MIN: バイト数                  | 最小バイト数。  |
| MAX: バイト数                  | 最大バイト数。  |
| LEAVE: バイト数                | OS 用として残す最小バイト数。   |
| blockcachepersent= パーセンテージ | キャッシュをブロックキャッシュおよびレコードキャッシュに分離します。   |

ハードメモリ制限が指定された状態で、メモリの割合としてデータベースキャッシュを定義する場合、管理者は、合計メモリの割合または使用可能なメモリの割合のいずれかを選択できます。動的制限の場合には、必ず利用可能なメモリが基準になります。次に示すコマンド例はすべて、\_ndsdb.ini ファイルで使用できます。

次の例では、動的制限を使用可能なメモリの 75%、最小バイト数を 16 MB、OS 用に残すバイト数を 32 MB と設定しています。

```
cache=DYN,%,75,MIN:16000000, LEAVE 32000000
```

次の例では、ハードメモリ制限を合計物理メモリの 75%、最小バイト数を 18 MB、最大バイト数を 512 MB と設定しています。

```
cache=HARD, TOTAL,%,75,MIN:18000000, MAX 512000000
```

次の例は古いスタイルのコマンドで、ハードメモリ制限を 8 MB に設定しています。

```
cache=8000000
```

データベースキャッシュは、ブロックキャッシュとレコードキャッシュに配分されます。ブロックキャッシュには、ディスクに格納されたデータのミラーとして、データブロックとインデックスブロックが保持されます。レコードキャッシュには、メモリに展開された形でのディレクトリオブジェクトと属性が保持されます。ディレクトリへの追加や更新では、ブロックキャッシュの設定が使用されます。大半の処理が読み込みの場合には、レコードキャッシュが使用されます。適切なサイズのキャッシュを割り当てないで多数の順次更新処理を実行すると、両方のキャッシュにスラッシュ状態を招くことがあります。指定によって変更しない場合、キャッシュの 50% がブロックキャッシュに、50% がレコードキャッシュに割り当てられます。blockcachepersent オプションを \_ndsdb.ini ファイルに追加することにより、データブロックとインデックスブロックに割り当てるキャッシュの比率を指定できます (デフォルトは 50% です)。残りのキャッシュ領域はエントリに使用されます。

たとえば、60% をブロックキャッシュに、40% をレコードキャッシュにするには、次のように入力します。

```
blockcachepersent=60
```

どちらかのキャッシュを 100% に設定して、他方のキャッシュが使用できないようにすることは避けてください。通常、一方のキャッシュに 75% 以上は設定しないようにしてください。

データベースキャッシュの設定は Novell iMonitor を使用して制御することもできます。

キャッシュサイズは使用できるメモリの量により動的に変動しますが、カスタム環境用に DSTRACE コマンドを使用することは可能です。

# Linux、Solaris、AIX、および HP-UX システムでの eDirectory パフォーマンスの改善

次のセクションでは、Linux および UNIX システム上で eDirectory のパフォーマンスを改善する方法について説明します。

- ◆ 522 ページの「eDirectory サーバを微調整する」
- ◆ 523 ページの「eDirectory のキャッシュを最適化する」
- ◆ 526 ページの「Novell eDirectory 用に Solaris OS をチューニングする」

## eDirectory サーバを微調整する

Linux および Solaris 上の Novell eDirectory は、動的に調整されるスレッドプールを使用して、クライアントの要求を処理します。スレッドプールは自動的に調整され、多くの場合は最適なパフォーマンスが提供されます。ただし、次のパラメータを `/etc/opt/novell/eDirectory/conf/nds.conf` ファイルに設定することによって、サーバへの負荷が急激に高くなった場合にスレッドの起動により発生する遅延を回避できます。

| パラメータ                                 | 説明および推奨される設定  |
|---------------------------------------|---|
| <code>n4u.server.idle-threads</code>  | 最小スレッド数 (アクティビティとは無関係)。<br><br>このパラメータ値は、クライアントアクティビティが通常の場合に、新しいスレッドの生成に必要とされる時間を最小にするように、平均クライアント負荷に基づいて決める必要があります。   |
| <code>n4u.server.max-threads</code>   | 最大スレッド数。<br><br>このパラメータ値は、同時にサービスを提供する必要があるクライアントの最大数に基づいて決める必要があり、次のスレッドを考慮することが推奨されます。 <ul style="list-style-type: none"><li>◆ eDirectory は、最低でも 16 のスレッドを必要とします。</li><li>◆ 255 の LDAP 接続それぞれに、1 つのスレッドが必要です (Monitor Thread : 監視スレッド)。</li><li>◆ 現在のクライアントのそれぞれに、1 つのスレッドが必要です (Worker Thread : 動作スレッド)。</li></ul> |
| <code>n4u.server.start-threads</code> | eDirectory の起動時に起動するスレッド数。<br><br>このパラメータ値は、クライアントアクティビティが通常の場合に、新しいスレッドの生成に必要とされる時間を最小にするように、平均クライアント負荷に基づいて決める必要があります。  |

## eDirectory のキャッシュを最適化する

Novell eDirectory では永続キャッシュを使用しているため、サーバに対して行われた変更はベクトルに保持されます。変更の途中でサーバがクラッシュした場合、サーバが稼働状態に戻ると、eDirectory はより高速でロードして数秒間で変更を同期させます。Novell eDirectory は、システムエラーが発生した場合、ロールバックモデルとログファイルを使用してトランザクションをロールフォワードします。

eDirectory のキャッシュは最初 16 MB に設定され、その 50% がブロックキャッシュに、残りの 50% がレコードキャッシュに割り当てられます。15 分後、eDirectory はキャッシュのしきい値を変更し、キャッシュに使用可能な空きメモリの 51% まで初期化できるようにしますが、少なくとも 24 MB は OS 用に残します。このアルゴリズムは、使用可能な空きメモリ量を判別できるようにするコールをホスト OS がサポートしている場合のみ使用されます。

eDirectory キャッシュの最適化は、次の方法で行えます。

- ◆ [523 ページの「Linux システムおよび UNIX システムにおける固定量の RAM 使用」](#)
- ◆ [525 ページの「キャッシュパラメータの設定」](#)

eDirectory キャッシュの最適化の詳細については、[528 ページの「eDirectory のパフォーマンスの改善」](#)を参照してください。

### Linux システムおよび UNIX システムにおける固定量の RAM 使用

上記のアルゴリズムは Windows および NetWare では有効ですが、Linux システムおよび UNIX システムでは機能しません。Linux システムおよび UNIX システムでは、OS によって報告される使用可能な空きメモリは、他のオペレーティングシステムよりも少なくなります。これは、Linux OS および UNIX OS がファイルシステムブロック、頻繁に実行するプログラム、ライブラリなどの内部キャッシング用に空きメモリを使用するためです。このメモリ割り当てに加え、通常、Linux および UNIX 上のライブラリは解放されたメモリを OS に戻しません。

このような理由で、キャッシュには固定量の RAM を割り当てることをお勧めします。

Linux システムおよび UNIX システムで固定量の RAM を割り当てるには、次のいずれかの操作を行います。

- ◆ [523 ページの「手動で .ini ファイルを作成する」](#)
- ◆ [524 ページの「Novell iMonitor を使用する」](#)


#### 手動で .ini ファイルを作成する

- 1 eDirectory データベースファイル (DIB セット) が格納されたディレクトリ (通常、`/var/opt/novell/eDirectory/data/dib`) と同じディレクトリに、`_ndsdb.ini` という名前のファイルを作成します。
- 2 次に示すパラメータを、`_ndsdb.ini` ファイルに追加します。

| パラメータ                               | 説明  |
|-------------------------------------|---|
| <code>blockcachepersent=50</code>   | データベースブロックのキャッシングに割り当てるキャッシュの割合を設定します。                    |
| <code>cacheadjustinterval=15</code> | eDirectory が空きメモリの利用状況を評価し、全体のキャッシュサイズを調整する時間 (秒) を設定します。 |

| パラメータ                   | 説明  |
|-------------------------|---|
| cachecleanupinterval=15 | eDirectory がダーティキャッシュブロックをディスクに書き込む時間 ( 秒 ) を設定します。 |
| cache=16777216          | ハードメモリ制限 ( バイト数 ) を設定します。                           |

## Novell iMonitor を使用する

- 1 [エージェント環境設定]  をクリックします。
- 2 [データベースキャッシュ] をクリックし、次の情報を確認します。

| データベースキャッシュ情報   | 説明  |
|-----------------|---|
| 最大サイズ           | 指定したキャッシュが拡張できる最大サイズ (KB) です。   |
| 現在のサイズ          | 指定したキャッシュの現在のサイズ (KB) です。   |
| キャッシュされたアイテム    | 指定したキャッシュ内のアイテム数です。   |
| キャッシュされた古いバージョン | 指定したキャッシュ内の古いバージョンの数です。古いバージョンのキャッシュアイテムは、データベースの読み込みトランザクションの整合性を維持するために保持されます。つまり、あるスレッドが読み込みトランザクションを実行しており、別のスレッドが書き込みトランザクションを実行している場合、書き込みによって変更されるブロックの古いバージョンが読み込み操作のために保持されます。これは、読み込みのトランザクションを実行している間に変更処理が発生したとしても、読み込みの表示結果に整合性があるようにするためです。 |
| 古いバージョンのサイズ     | キャッシュされる古いバージョンのアイテムサイズ (KB) です。  |
| ヒット             | 指定したキャッシュ内のアイテムに正常にアクセスできた回数です。   |
| ヒット表示           | 指定したキャッシュ内で、アイテムに正常にアクセスする前に参照されたアイテム数です。ヒット表示とヒットの比率が、キャッシュ検索効率の目安となります。通常、この比率はほぼ 1:1 になるようにします。  |
| 失敗              | アイテムが指定したキャッシュ内に見つからず、低いレベルのキャッシュまたはディスクから取得されなければならなかった回数です。   |
| 失敗表示            | 必要なアイテムが指定したキャッシュ内ないと判断されるまでに、キャッシュ内で参照されたアイテムの数です。失敗表示と失敗の比率が、キャッシュ検索効率の目安となります。通常、この比率はほぼ 1:1 になるようにします。  |



3 次のオプションから選択します。

| オプション            | 説明   |
|------------------|--|
| ダイナミック調整         | eDirectory データベースのキャッシュに使用するシステムメモリの大きさを、必要と判断される大きさと、次に示すパラメータに基づいて動的に調整します。                |
| キャッシュ調整パーセンテージ   | レコードキャッシュおよびブロックキャッシュに使用可能なメモリの割合です。   |
| キャッシュサイズの制約条件    | ダイナミック調整で、指定した制約条件に従います。つまり、キャッシュのメモリの大きさを指定した大きさより小さくせず、使用可能なメモリの合計から指定した大きさを引いた値より大きくしません。 |
| ハードメモリ制限         | キャッシュに使用するシステムメモリの正確な大きさです。  |
| キャッシュ最大サイズ       | レコードキャッシュとブロックキャッシュを合わせたサイズ (KB) です。   |
| ブロックキャッシュパーセンテージ | ブロックキャッシュに割り当てられる使用可能なシステムメモリの割合です。残りの割合が、レコードキャッシュに割り当てられます。                                |
| キャッシュ調整間隔        | この間隔は、ダイナミック調整を設定している場合のみ使用されます。調整間隔は、指定したパーセンテージと制約条件に基づき、どれくらいの頻度でキャッシュサイズを調整するかを制御します。    |
| キャッシュクリーンアップ間隔   | どれくらいの頻度で古い未使用のバージョンをキャッシュから削除するかを制御します。   |
| 永続的なキャッシュ設定      | このオプションを選択すると、iMonitor を使用して送信した変更は、前に保存した設定やデフォルトのシステム設定に上書きされ、永続的な変更になります。                 |

4 [送信] をクリックします。

## キャッシュパラメータの設定

デフォルトでは、eDirectory は動的キャッシュを使用します。eDirectory のキャッシュサイズの増加に使用できる十分な RAM がある場合は、eDirectory キャッシュへの RAM の割り当てを増加することによって、大容量データベースを使用する場合の eDirectory のパフォーマンスを大幅に向上できます。

次の表に示すパラメータを調整すれば、eDirectory のパフォーマンスを向上できます。

| eDirectory キャッシュパラメータ   | 説明   |
|-------------------------|--|
| blockcachepercent= 値    | データベースブロックのキャッシングに割り当てるキャッシュの割合を設定します。デフォルトのポート番号は 50 です。            |
| cachecleanupinterval= 値 | eDirectory がダーティキャッシュブロックをディスクに書き込む時間 (秒) を設定します。デフォルトのポート番号は 15 です。 |

| eDirectory キャッシュパラメータ  | 説明  |
|------------------------|---|
| cacheadjustinterval= 値 | eDirectory が空きメモリの利用状況进行评估し、全体のキャッシュサイズを調整する時間 (秒) を設定します。デフォルトのポート番号は 15 です。 |
| cache= 値               | eDirectory がキャッシングに使用できるメモリのハード制限 (バイト数) を設定します。                              |
| cache=leave: 値         | 使用可能量として残しておく最小バイト数を指定します。  |
| min: 値                 | 最小キャッシュサイズをバイト数で指定します。  |
| max: 値                 | 最大キャッシュサイズをバイト数で指定します。  |

このアルゴリズムに従うと、Novell eDirectory のデフォルト設定は次のようになります。

```
cache=dyn,%:51,min:16777216,max:0,leave:0
```

この設定は、次のことを示しています。

- ◆ 最小キャッシュサイズは 16 MB である。
- ◆ 最大キャッシュサイズの限度はない。
- ◆ 動的なキャッシュ調整が行われ、使用可能なメモリの 51% まで使用される。
- ◆ OS 用に 24 MB が残される。

eDirectory は、すべてのアプリケーションが開始され、システムが安定するように、16 MB のハードメモリ制限で動作します。

eDirectory が合計メモリの割合を使用するように設定することもできます。これを行うには、次のようにキャッシュを指定します。

```
cache=hard,total,%: バイト単位での合計メモリのパーセンテージ
```

## Novell eDirectory 用に Solaris OS をチューニングする

次のセクションでは、Solaris のカーネル、ネットワーク、およびファイルシステムのチューニング方法について説明します。

**重要:** 最初に、推奨されているパッチを Solaris OS に適用済みであることを確認します。詳細については、『Novell eDirectory 8.8 インストールガイド』の [Novell eDirectory の Solaris へのインストールまたはアップグレード](#) を参照してください。

- ◆ [527 ページの「Solaris カーネルをチューニングする」](#)
- ◆ [527 ページの「Solaris ネットワークをチューニングする」](#)
- ◆ [527 ページの「Solaris ファイルシステムを微調整する」](#)

## Solaris カーネルをチューニングする

Solaris 上の eDirectory パフォーマンスを最適化するには、/etc/system ファイルで次のカーネル変数を設定します。

| パラメータ                           | 説明   |
|---------------------------------|--|
| set maxphys=1048576             | 1 回の SCSI 転送で転送できる最大バイト数です。  |
| set md_maxphys=1048576          | DiskSuite、vol_maxio、または VxVM を使用している場合の、1 回の SCSI 転送で転送できる最大バイト数です。                            |
| set ufs:ufs_LW= 使用可能なメモリの 1/128 | 1 つのファイルに対する未処理バイト数の境界値です。これを下回ると、他の処理が休眠状態となっている原因の条件変数が切り替えられます。                             |
| set ufs:ufs_HW= 使用可能なメモリの 1/64  | 1 つのファイルの書き込み失敗境界値に対する未処理バイト数です。   |
| ctcp:TCP 接続ハッシュサイズ=8192         | カーネルのデータ構造を検索するために割り当てられた、TCP 接続に関連する接続ハッシュエントリの数です。(この数は、LDAP クライアントの数に応じて 262144 まで大きくできます。) |

## Solaris ネットワークをチューニングする

LDAP の検索パフォーマンスは、Solaris の ndd コマンドを使用して改善できます。次に示すコマンド構文を使用すれば、ネットワークの操作や動作に影響する、チューニング可能なパラメータを分析し、変更できます。

```
ndd -set /dev/tcp 変数名 変数の値
```

変数の推奨値を次の表に示します。

| パラメータ                         | 説明  |
|-------------------------------|---|
| tcp_conn_req_max_q: 1024      | 「q」はキューを表します。これは完成されたソケットで、ペンを保持し、アプリケーションが受諾を発行するまでソケットは存続します。 |
| tcp_time_wait_interval: 60000 | 待機間隔(ここでは小さな値)を設定します。   |
| tcp_xmit_hiwat: 64000         | TCP の最大および最小送信ウィンドウサイズを調整します。                                   |
| tcp_xmit_lowat: 64000         |   |
| tcp_slow_start_initial: 2     | 最初の転送パケット数を 1 から 2 に調整します。                                      |

## Solaris ファイルシステムを微調整する

Solaris ファイルシステムが適切にチューニングされると、Solaris 上の Novell eDirectory のパフォーマンスが改善されます。特に、ディレクトリヘデータをバルクロードする場合のパフォーマンスが非常に向上します。eDirectory のファイルシステムチューニングは、データベースのチューニングと類似しています。Solaris ファイルシステムの詳細については、Sunworld\* の Web サイト (<http://www.sunworld.com/sunworldonline>) を参照してください。

## eDirectory のパフォーマンスの改善

eDirectory 8.8 では、バルクロードのパフォーマンスを向上させるための新しいオプションが用意されています。

バルクロードのパフォーマンスを向上させるために Novell インポート / エクスポート変換ユーティリティを使用して調整可能なパラメータは次のとおりです。

- ◆ 528 ページの「eDirectory キャッシュの設定」
- ◆ 529 ページの「LBURP トランザクションサイズの設定」
- ◆ 529 ページの「ICE の非同期要求の数を増やす」
- ◆ 530 ページの「LDAP 書き込みスレッド数の増加」
- ◆ 530 ページの「ICE のスキーマ検証を無効にする」
- ◆ 531 ページの「ACL テンプレートを無効にする」
- ◆ 532 ページの「バックリンカ」
- ◆ 532 ページの「インラインキャッシュを有効 / 無効にする」
- ◆ 533 ページの「LBURP のタイムアウト周期の拡大」

各オペレーティングシステムの調整可能パラメータも参照してください。

### eDirectory キャッシュの設定

パフォーマンス低下の最も一般的な原因には、ディスク I/O の管理不良や eDirectory キャッシュのメモリ割り当て不足があります。eDirectory が実質的に唯一のアプリケーションである場合は、eDirectory のキャッシュを最大で 2.5 GB に設定できます。割り当てられたキャッシュは、最終的にはすべてが使用されます。高揮発性のデータを処理している場合、eDirectory のパフォーマンスはキャッシュ量を増やすことで向上します。

キャッシュは 100 MB ~ 2.5 GB の範囲で設定できます。通常、DIB の 3 倍から 4 倍以上のサイズが必要になることはありません。DIB のサイズが大きい場合でも、キャッシュは 2 GB までにしてください。

テスト済みの最小キャッシュサイズは 0 で、最大キャッシュサイズは 2.5 GB です。適切なキャッシュサイズは、同じサーバで実行される他の処理が必要とするメモリ量、および必要とするディスクキャッシュ量を基に決める必要があります。色々なキャッシュサイズを試してみて、最適なキャッシュサイズを決めてください。

バルクロードのパフォーマンスを最適にするには、eDirectory キャッシュの割り当てで、ブロックキャッシュにより高い割り当て率を設定します。90% に設定することをお勧めします。この設定は、処理が完了した後でリセットできます。

iMonitor を使用すれば、最も迅速に `blockcachepcentage` パラメータを変更できます。この作業を行う方法については、197 ページの「Novell iMonitor 2.1 の使用」を参照してください。

詳細については、『Novell® eDirectory 8.7.1:Linux\* および UNIX\* のパフォーマンスチューニング』(<http://www.novell.com/collateral/4621373/4621373.pdf>) の「キャッシュサブシステムのチューニング」を参照してください。

## LBURP トランザクションサイズの設定

LBURP トランザクションサイズによって、1つのトランザクションにおいて ICE から LDAP サーバに送信されるレコード数が設定されます。十分なメモリがあり、この値を大きくしても I/O 競合が発生しない場合、この値を大きくすることでバルクロードのパフォーマンスを向上できます。

デフォルトの LBURP トランザクションサイズは 25 です。この値は LDIF ファイルが少ない (操作数が 100,000 より少ない) 場合には適切ですが、レコード数が多い場合には不適切です。LBURP トランザクションサイズは、1 ~ 350 の範囲で設定できます。

### トランザクションサイズの変更

トランザクションサイズを変更するには、`/etc/opt/novell/eDirectory/conf/nds.conf` ファイルで `n4u.ldap.lburp.transize` パラメータの値を変更します。理想的なシナリオでは、トランザクションサイズが大きいほど、パフォーマンスはより高くなります。ただし、次の理由のため、トランザクションサイズには必要以上に大きな値を設定しないようにします。

- トランザクションサイズが大きいほど、サーバはトランザクションを処理するためにより多くのメモリを割り当てる必要があります。システムが少ないメモリで稼働している場合、スワッピングのために処理が遅くなることがあります。
- LDIF ファイルにエラーがなく、eDirectory にある既存のエントリがコメント化されていることが必要です。トランザクションに 1 つでもエラーがあると (追加しようとしたオブジェクトがすでにディレクトリに存在するという場合も含めて)、eDirectory は LBURP トランザクション設定を無視し、操作ごとにコミットを実行してデータの整合性を確認します。

詳細については、「[LDIF ファイルのデバッグ](#)」を参照してください。

- LBURP の最適化は、リーフオブジェクトに対してのみ有効です。トランザクションにコンテナオブジェクトとそのサブオーディネートオブジェクトが含まれている場合、eDirectory はこれをエラーと見なします。これを回避するには、最初に別の LDIF ファイルを使用してコンテナオブジェクトをロードするか、前方参照の使用を有効にします。

詳細については、『*Novell eDirectory 8.8 Troubleshooting Guide*』の「[前方向参照の有効化](#)」を参照してください。

## ICE の非同期要求の数を増やす

これは、LDAP サーバから結果が返されるまでに ICE クライアントからサーバに非同期で送信できるエントリ数を意味します。

非同期要求の数は、10 ~ 200 の範囲で設定できます。デフォルト値は 100 です。最小値 (10) よりも小さい値はデフォルトに戻されます。小さな LDIF ファイルには最小値が適切です。

理想的なシナリオでは、ウィンドウサイズが大きいほど、パフォーマンスはより高くなります。ただし、ウィンドウサイズが大きくなるほど、クライアントが LDIF ファイルのエントリを処理するために割り当てるメモリの量が多くなるため、ウィンドウサイズを必要以上に大きく設定しないでください。システムが少ないメモリで稼働している場合、スワッピングのために処理が遅くなることがあります。

ICE の非同期要求の数を変更するには、ICE コマンドラインオプションまたは iManager を使用します。

## ICE コマンドラインオプションを使用する場合


非同期要求の数は、ICE コマンドラインオプション **-Z** を使って指定できます。これは、LDAP ターゲットハンドラの一部として使用できます。

ICE クライアントによって送信される非同期要求の数を 50 に設定するには、次のコマンドを入力します。

```
ice -SLDIF -f LDIF ファイル -a -c -DLDAP -d cn=admin,o=novell -Z50 -w パスワード
```

## iManager の ICE ウィザードを使用する場合

ICE クライアントによって送信される非同期要求の数を iManager で設定する方法は次のとおりです。

- 1 [役割およびタスク] ボタン  をクリックします。
- 2 [eDirectory の保守] > [インポート / エクスポート変換ウィザード] の順にクリックします。
- 3 **データをファイルからインポートするタスクと LDAP サーバ間でデータを移行するタスクの両方で、LDAP ターゲットハンドラ画面の [LBURP ウィンドウサイズ] フィールドに値を入力します。**
- 4 [次へ] をクリックします。

詳細については、ウィザードのヘルプを参照してください。

## LDAP 書き込みスレッド数の増加

LDAP サーバで複数の書き込みスレッドを使えるようになりました。同時処理によって発生するエラーを避けるために前方参照を有効にするには、次のように ICE コマンドラインオプション **-F** を使用します。

```
ice -SLDIF -f LDIF ファイル -a -c -DLDAP -d cn=admin,o=novell -w パスワード -F
```

## ICE のスキーマ検証を無効にする

ICE クライアントのスキーマ検証を無効にするには、次のように ICE コマンドラインオプション **-C** と **-n** を使用します。

```
ice -C -n -SLDIF -f LDIF ファイル -a -c -DLDAP -d cn=admin,o=novell -w パスワード
```

## ACL テンプレートを無効にする

バルクロードのパフォーマンスを向上させるために、ACL (アクセス制御リスト) テンプレートを無効にすることができます。これによりいくつかの ACL が見つからなくなりますが、必要な ACL を LDIF ファイルに追加するか、それらの ACL を後から適用することで、この問題は解決できます。

- 1 次のコマンドを実行します。

```
ldapsearch -D 管理者のCN -w パスワード -b cn=schema -s base
objectclasses=inetorgperson
```

このコマンドの出力は次のようになります。

```
dn: cn=schema
```

```
objectClasses: ( 2.16.840.1.113730.3.2.2 NAME 'inetOrgPerson' SUP
organizationalPerson STRUCTURAL MAY ( groupMembership $ ndsHomeDirectory
$ loginAllowedTimeMap $ loginDisabled $ loginExpirationTime $
loginGraceLimit $ loginGraceRemaining $ loginIntruderAddress $
loginIntruderAttempts $ loginIntruderResetTime $
loginMaximumSimultaneous $ loginScript $ loginTime $
networkAddressRestriction $ networkAddress $ passwordsUsed $
passwordAllowChange $ passwordExpirationInterval $
passwordExpirationTime $passwordMinimumLength $ passwordRequired $
passwordUniqueRequired $ printJobConfiguration $ privateKey $ Profile $
publicKey $ securityEquals $ accountBalance $ allowUnlimitedCredit $
minimumAccountBalance $ messageServer $ Language $ UID $
lockedByIntruder $ serverHolds $ lastLoginTime $ typeCreatorMap $
higherPrivileges $ printerControl $ securityFlags $ profileMembership $
Timezone $ sASServiceDN $ sASSecretStore $ sASSecretStoreKey $
sASSecretStoreData $ sASPKIStoreKeys $ userCertificate
$nDSPKIUserCertificateInfo $ nDSPKIKeystore $ rADIUSActiveConnections $
rADIUSAttributeLists $ rADIUSConcurrentLimit $ rADIUSConnectionHistory
$ rADIUSDefaultProfile $ rADIUSDialAccessGroup $ rADIUSEnableDialAccess
$ rADIUSPassword $ rADIUSServiceList $ audio $ businessCategory $
carLicense $ departmentNumber $ employeeNumber $ employeeType $
givenName $ homePhone $ homePostalAddress $ initials $ jpegPhoto $
labeledUri $ mail $ manager $ mobile $ pager $ ldapPhoto $
preferredLanguage $ roomNumber $ secretary $ uid $ userSMIMECertificate
$ x500UniqueIdentifier $ displayName $ userPKCS12 ) X-NDS_NAME 'User' X
-NDS_NOT_CONTAINER '1' X-NDS_NONREMOVABLE '1' X-NDS_ACL_TEMPLATES (
'2#subtree#[Self]#[All Attributes Rights]' '6#entry#[Self]#loginScript'
'1#subtree#[Root Template]#[Entry Rights]'
'2#entry#[Public]#messageServer' '2#entry#[Root
Template]#groupMembership' '6#entry#[Self]#printJobConfiguration'
'2#entry#[Root Template]#networkAddress' )
```

- 2 この出力から、太字で示されている情報を削除します。
- 3 変更を加えた出力を LDIF ファイルとして保存します。
- 4 新しく保存した LDIF ファイルに次の情報を追加します。

```
dn: cn=schema
changetype: modify
delete: objectclasses
objectclasses: ( 2.16.840.1.113730.3.2.2 )
-
add:objectclasses
```

これにより、新しい LDIF は次のようになります。

```
dn: cn=schema
changetype: modify
delete: objectclasses
objectclasses: ( 2.16.840.1.113730.3.2.2 )
-
add:objectclasses
objectClasses: ( 2.16.840.1.113730.3.2.2 NAME 'inetOrgPerson' SUP
organization alPerson STRUCTURAL MAY ( groupMembership $ ndsHomeDirectory
$ loginAllowedTimeMap $ loginDisabled $ loginExpirationTime $
loginGraceLimit $ loginGraceRem aining $ loginIntruderAddress $
loginIntruderAttempts $ loginIntruderResetTime $
loginMaximumSimultaneous $ loginScript $ loginTime $
networkAddressRestri ction $ networkAddress $ passwordsUsed $
passwordAllowChange $ passwordExpirationInterval $
passwordExpirationTime $ passwordMinimumLength $ passwordRequired
$passwordUniqueRequired $ printJobConfiguration $ privateKey $ Profile $
publicKey $ securityEquals $ accountBalance $ allowUnlimitedCredit $
minimum AccountBalance $ messageServer $ Language $ UID $
lockedByIntruder $ serverHolds $ lastLoginTime $ typeCreatorMap $
higherPrivileges $ printerControl $ securityFlags $ profileMembership $
Timezone $ sASServiceDN $ sASSecretStore $ sASSecretStoreKey $
sASSecretStoreData $ sASPKIStoreKeys $ userCertificate $
nDSPKIUserCertificateInfo $ nDSPKIKeystore $ rADIUSActiveConnections $
rADIUSAttributeLists $ rADIUSConcurrentLimit $ rADIUSConnectionHistory $
rADIUSDefa ultProfile $ rADIUSDialAccessGroup $ rADIUSEnableDialAccess
$rADIUSPassword $ rADIUSServiceList $ audio $ businessCategory $
carLicense
$ departmentNumbe r $ employeeNumber $ employeeType $ givenName $
homePhone $ homePostalAddress $ initials $ jpegPhoto $ labeledUri $ mail
$ manager $ mobile $ pager $ ldap Photo $ preferredLanguage $ roomNumber
$ secretary $ uid $ userSMIMECertifica te $ x500UniqueIdentifier $
displayName $ userPKCS12 ) X-NDS_NAME 'User' X-ND S_NOT_CONTAINER '1' X
-NDS_NONREMOVABLE '1' )
```

**5** 次のコマンドを入力します。

```
ldapmodify -D 管理者の CN -w パスワード -f LDIF ファイル名
```

## バックリンカ

バックリンカは、特に参照整合性をチェックするバックグラウンドプロセスであり、eDirectory サーバが起動してから 50 分後に実行されます。その後は 13 時間後に実行されます。バルクロードの処理中にバックリンカが実行されないように注意してください。ロードされるオブジェクトの数やオブジェクトがロードされる回数によっては、バックリンカが実行されると、バルクロードの処理速度が低下することがあります。

## インラインキャッシュを有効 / 無効にする

サーバのインラインキャッシュ変更を有効または無効にできます。インラインキャッシュ変更は、アウトバウンド同期が無効になっている場合のみ、無効にできます。アウトバウンド同期を有効にすると、インラインキャッシュ変更も有効になります。

インラインキャッシュ変更を無効にすると、このレプリカの変更キャッシュが無効としてマークされ、[エージェント環境設定] > [パーティション] に無効なフラグが付けられます。インラインキャッシュ変更を有効にすると、変更キャッシュの再構築時に、無効な変更キャッシュのフラグが削除されます。



## LBURP のタイムアウト周期の拡大

デフォルトでは、クライアントのタイムアウト周期は 20 分 (1200 秒) です。ただし、バルクロードの処理の際、LBURP トランザクションサイズが 250 であり、非常に大きな値を持つ多数の属性が対象であり、しかも、サーバで同時 LBURP 処理が有効になっている場合、サーバは ICE クライアントによって送信されるデータを処理するために使用中になり、クライアントへの応答は規定の時間内に行われません。この場合、ICE クライアントはタイムアウトになります。

このため、タイムアウト周期を拡大することをお勧めします。タイムアウト周期を拡大するには、環境変数 LBURP\_TIMEOUT に大きな値 (秒) を設定してエクスポートします。

たとえば、LBURP\_TIMEOUT 変数に 1200 秒を設定してエクスポートするには次のように入力します。

```
export ICE_LBURP_TIMEOUT=1200
```

## eDirectory の正常な動作の維持

ディレクトリサービスの動作を正常に維持することは、あらゆる組織にとって重要です。Novell iMonitor を使用して定期的にヘルスチェックを行うことで、ディレクトリは適切に機能し、アップグレードやトラブルシューティングを容易に実行できます。

## ヘルスチェックを実行する時期

一般に、ネットワークを頻繁に変更しない場合 (サーバとパーティションの追加は 2 ~ 3ヶ月おきで、頻繁に行われるのは単純な変更だけの場合)、ヘルスチェックは月に 1 度実行します。

ネットワークの変更が頻繁に発生する場合 (パーティションやサーバが毎週追加される、あるいは組織の再編成を行っている場合)、ヘルスチェックは週に 1 度実行します。

環境の変更に応じて、ヘルスチェックの頻度を調整します。ヘルスチェックの実行頻度に影響する要素を次に示します。

- ◆ パーティションとレプリカの数
- ◆ サーバを保持しているレプリカの安定度
- ◆ eDirectory パーティション内の情報量
- ◆ オブジェクトのサイズと複雑さ
- ◆ 以前の DSRepairs 内のエラー数

ヘルスチェックを実行すると、所有する権利に基づき、iMonitor がすべてのサーバから情報を集めます。なお、ヘルスチェックレポートを実行すると、ネットワークトラフィックが発生し、ディスク容量を消費する場合がありますことに注意してください。

## ヘルスチェックの概要

完全なヘルスチェックでは、次の情報がチェックされます。

- ◆ eDirectory のバージョン

同一バージョンの NetWare 上で異なるバージョンの NDS や eDirectory を実行していると、同期に問題が発生する場合があります。NDS または eDirectory のバージョンが古い場合は、最新のソフトウェアパッチを [Novell Directory Services Patches and Files \(http://support.novell.com/filefinder/5069/index.html\)](http://support.novell.com/filefinder/5069/index.html) からダウンロードしてください。

- ◆ 時刻の同期

すべての eDirectory サーバは、正確な時刻を維持する必要があります。タイムスタンプが各オブジェクトおよびプロパティに割り当てられ、これによりオブジェクトおよびプロパティの更新が正しい順序で行われます。eDirectory では、タイムスタンプを使用して、同期が必要なレプリカを判別します。

- ◆ 同期の許容範囲

インバウンドやアウトバウンドのデータ変更により同期を行ってから経過した期間で、どれだけのデータが未処理となっているかなどをチェックします。

- ◆ バックグラウンド処理

プロセスはさまざまなタスクを実行しますが、その中には変更の複製およびシステム情報の保守があります。

- ◆ 外部参照
- ◆ 破損通知
- ◆ eDirectory スキーマ

これらのチェックを実行するための詳細な手順については、次のセクション「[iMonitor を使用した eDirectory のヘルスチェック](#)」を参照してください。

## iMonitor を使用した eDirectory のヘルスチェック


環境設定によっては、eDirectory サーバのヘルスチェックを iMonitor の次の 2 つの方法のいずれかを使用して実行できます。

- ◆ [ナビゲータフレームを使用する](#)
- ◆ [アシスタントフレームを使用する](#)

### ナビゲータフレームを使用する


- 1 iMonitor へアクセスする

[199 ページの「iMonitor へアクセスする」](#)を参照してください。

- 2 ナビゲータフレームで、レポートアイコン  をクリックします。

- 3 アシスタントフレームで、[レポート設定] リンクをクリックします。

データフレームに、実行可能レポートリストが表示されます。

- 4 レポートの設定アイコン  をクリックして、必要なサーバ情報を表示させます。

データフレームに、サーバ情報レポートが表示されます。このレポートを使用して、レポートに必要なオプションを選択します。

- 5 [ヘルスのサブレポート] チェックボックスをオンにします。
- 6 指定した間隔でレポートを実行するには、データフレームの [レポートのスケジュール] セクションで、必要なオプションを選択します。  
**重要:** スケジュールされたレポートを実行した場合、Public ユーザとして実行されるため、認証されたユーザとして実行するより少ない情報しか得られない場合があります。
- 7 [レポートの実行] をクリックして、レポートを開始します。

## アシスタントフレームを使用する


- 1 iMonitor へアクセスする  
199 ページの「**iMonitor へアクセスする**」を参照してください。
- 2 アシスタントフレームで、[エージェントヘルス] をクリックします。  
iMonitor が情報を取得するサーバ ( 接続先のサーバとは限りません ) のヘルスチェック情報が、データフレームに表示されます。

## レポート情報の検討

レポートが生成されたら、データフレームにレポート結果が表示されます。ツリー内に正常に動作していないサーバがある場合、レポートは次の 3 つのカテゴリに分けられます ( グループ化では最も正常に動作していないサーバが最初になります )。

- ◆ 警告のあるサーバ
- ◆ 疑わしいサーバ
- ◆ 正常なサーバ

警告のあるサーバや疑わしいサーバがない場合は、これらのカテゴリは表示されません。

正常に動作していないサーバがある場合は、そのサーバの横の [エージェントヘルスのサブレポート] リンク  をクリックします。オンラインのコンテキストヘルプを使用して、問題を解決します。このヘルプは、個々のオプションの意味、それが重要である理由、問題の解決方法、範囲の調整方法、およびヘルスチェックに追加するオプションがあるかどうかを確認するのに役立ちます。

**重要:** 警告のあるサーバがある場合、その問題を解決することを強くお勧めします。疑わしいサーバについても、評価することをお勧めします。

## 詳細情報

eDirectory の正常な動作を維持するために使用するツールおよび技術については、『Novell Certified Directory Engineer Course 991: Advanced eDirectory Tools and Diagnostics』に記載されています。このコースでは、次の方法について学習します。

- ◆ eDirectory ヘルスチェックの実行方法
- ◆ eDirectory の正しい操作方法
- ◆ eDirectory の問題の適切な診断、トラブルシューティング、および解決の方法
- ◆ eDirectory トラブルシューティングのツールおよびユーティリティの使用法

このコースの詳細については、[Novell Training Services Web サイト \(http://www.novell.com/training/index.html\)](http://www.novell.com/training/index.html) を参照してください。

## 監視のためのリソース

Novell DSTrace ユーティリティは、NetWare、Windows NT、Linux、Solaris、AIX および HP-UX 上で動作します。このツールは、eDirectory の膨大なリソースを監視するのに役立ちます。DSTrace の詳細については、次を参照してください。

- ◆ [210 ページの「トレースを環境設定する」](#)
- ◆ [Looking Into the Directory Services Trace \(DSTrace\) Options \(http://developer.novell.com/research/sections/netmanage/dirprimer/2001/august/spv.htm\)](http://developer.novell.com/research/sections/netmanage/dirprimer/2001/august/spv.htm)
- ◆ [More on Using the DSTrace Command \(http://developer.novell.com/research/sections/netmanage/dirprimer/2001/septembe/p010901.htm\)](http://developer.novell.com/research/sections/netmanage/dirprimer/2001/septembe/p010901.htm)

また、eDirectory 環境用の他の管理ソリューションを提供するサードパーティの製品も使用できます。詳細については、次の Web サイトを参照してください。

- ◆ [BindView \(http://www.bindview.com\)](http://www.bindview.com)
- ◆ [Blue Lance \(http://www.bluelance.com\)](http://www.bluelance.com)
- ◆ [NetPro\\* \(http://www.netpro.com\)](http://www.netpro.com)

弊社のパートナーが提供していない eDirectory の特性をモニタしたり、監視する必要がある場合、Novell Consulting Services が Novell Event System を使用した評価と監視のカスタマイズをお手伝いいたします。

## ハードウェアのアップグレードやサーバの交換

このセクションでは、ハードウェアをアップグレードまたは交換する際に、特定のサーバ上の eDirectory を移す、または保護するための情報について説明します。ここでの説明は、[389 ページの「Novell eDirectory のバックアップと復元」](#)の情報に基づいています。

Backup eDirectory Management Tool を使用すれば、次の操作を行うための eDirectory 情報を作成できます。

- ◆ [536 ページの「サーバを交換しないでハードウェアまたは記憶デバイスを計画的にアップグレードする」](#)
- ◆ [540 ページの「サーバの計画的な交換」](#)

## サーバを交換しないでハードウェアまたは記憶デバイスを計画的にアップグレードする

記憶デバイスや RAM などのハードウェアのアップグレードを計画している場合、Backup eMtool を使用して eDirectory およびファイルシステムのコールドバックアップを行います。これにより、サーバの eDirectory 識別情報とファイルシステムデータが保護されます。このバックアップには、次の利点があります。

- ◆ 記憶デバイスを交換する場合、バックアップによって古い記憶デバイスから新しい記憶デバイスに情報を移すことができます。
- ◆ eDirectory が格納されたディスクパーティションまたはディスクボリュームを含む記憶デバイスを交換する場合、このバックアップ情報を用いれば、復元プロセスを使用して eDirectory データベースを新しい記憶デバイス上に再構築できます。
- ◆ eDirectory のコールドバックアップを実行し、その後でデータベースをクローズしておけば、バックアップ後のデータベースの変更を心配することなくハードウェアをアップグレードし、データベースを移すことができます。
- ◆ 何か問題が発生した場合、バックアップを使用して復元できます。

eDirectory のコールドバックアップを実行する場合、オプションを使用してサーバ上の eDirectory をロックし、使用不可にする必要があります。これにより、バックアップ後のデータ変更を防げます。このサーバと通信している他のサーバからは、このサーバは停止しているように見えます。通常サーバに送信される eDirectory 情報は、そのサーバと再び通信できるようになるまで、ツリー内の別のサーバに保存されます。保存された情報は、サーバがオンライン状態に戻ったときに、サーバを同期するために使用されます。

**注:** eDirectory ツリー内の他のサーバは、このサーバがすぐにオンライン状態に戻ると期待しているため、アップグレードをすばやく完了させ、できるだけ早くサーバ上の eDirectory データベースをオープンする必要があります。

ハードウェアのアップグレードを計画的に実行するには、次の手順に従います。

- 1 アップグレードによりサーバに問題が発生するかもしれないと心配なら、必要に応じて、使用する別のコンピュータを準備するとよいでしょう。

540 ページの「1. サーバ交換の準備」を参照してください。

- 2 eDirectory データベースのコールドバックアップを実行し、その後でデータベースをクローズし、ロックしたままにしておくには、eMBox クライアントコマンドを次のように使用します。NICI を使用する場合は、`-e` オプションを使用してセキュリティファイルもバックアップします。

```
backup -f バックアップファイルの名前とパス  
-l ログファイルの名前とパス -e -t -c -o -d
```

NICI を使用する場合は、`-e` スイッチを使用して NICI ファイルをバックアップします。(eMBox クライアントとスイッチの使用についての詳細は、420 ページの「eMBox クライアントによる手動バックアップ」および 420 ページの「eMBox クライアントによる手動バックアップ」を参照してください。)

これで、eDirectory データベースはロックされました。手順を完了するまでは、サーバ上で新たなデータ変更が実行されないように、データベースをロックしたままにしておく必要があります。

サーバが使用できない時間を最小限に抑えるために、以降の手順をすばやく完了させます。

- 3 お好みのバックアップツールを使用して、ファイルシステムをバックアップします。(NetWare の場合、SMS™ が使用できます。)

データベースをバックアップした後で、ファイルシステムのバックアップを行うのは重要です。これにより、eDirectory バックアップファイルが、他のファイルシステムと一緒にテープに保存されます。

- 4 サーバを停止させ、ハードウェアを交換します。

- 5 ハードウェアを交換した後で、ハードウェア変更の種類に応じた以下の手順を実行します。

| ハードウェア変更の種類 ...   | 実行する手順  |
|---|---|
| 記憶デバイスに変更がない場合  | サーバを起動し、データベースのロック解除を行います。  |
| 記憶デバイスの交換を行ったが、eDirectory が格納されたディスクパーティション/ボリュームに変更はない場合 | <ol style="list-style-type: none"> <li>1. サーバと eDirectory を起動します。</li> <li>2. 交換した記憶デバイス上にあったディスクパーティション/ボリュームのファイルシステムだけを復元します。</li> <li>3. eDirectory データベースのロックを解除します。</li> </ol>  |
| NetWare 以外のオペレーティングシステム環境の eDirectory が格納された記憶デバイスを交換した   | <ol style="list-style-type: none"> <li>1. 必要に応じてオペレーティングシステムをインストールします。</li> <li>2. 記憶デバイスの変更により影響を受けたディスクパーティション上に、ファイルシステムを復元します。</li> <li>3. 新しい記憶デバイス上の、新しい一時的なツリー内に、eDirectory をインストールします。</li> <li>4. バックアップから eDirectory を復元します (元のツリー内に配置されます)。このとき、復元した後で eDirectory がクローズされ、ロックされたままになるようにオプションを指定します。次のようなコマンドを使用します。<br/> <code>restore -r -f バックアップファイルの名前とパス -l ログファイルの名前とパス -e</code><br/><br/> NICI ファイルをバックアップしてあった場合は、-e オプションを使用します。インクルードファイルに列挙されたファイルをバックアップしてあった場合は、-u オプションを追加します。 </li> <li>5. eDirectory データベースのロックを解除します。</li> <li>6. NICI セキュリティファイルを復元した場合は、復元を完了した後で、サーバを再起動してセキュリティシステムを再初期化します。</li> <li>7. サーバが通常どおりに応答するか、チェックします。<br/><br/> ConsoleOne<sup>®</sup> を使用して、サーバとその同期をチェックします。ログインスクリプトと印刷が正しく動作することを確認します。 </li> <li>8. このサーバでロールフォワードログを使用していた場合、復元を完了した後で、ロールフォワードログ設定を再作成します。ロールフォワードログを有効にしてから、改めてフルバックアップも取る必要があります。<br/><br/> 復元した後は、設定がデフォルトの状態にリセットされます。つまり、ロールフォワードログがオフになっています。フルバックアップが改めて必要となるのは、スケジュールに従って次に無人でのフルバックアップが取られるまでに、再び障害が起こる可能性があるためです。 </li> </ol> |

| ハードウェア変更の種類 ...  | 実行する手順   |
|--|--|
| <p>NetWare 上の eDirectory と SYS: ポリリュームが含まれた記憶デバイスを交換した</p> | <p>NetWare 上のファイルシステムデータを復元する場合、ファイルシステム権の保持に関わる問題があることを認識しておく必要があります。eDirectory を復元した後で、ファイルシステムを復元する必要があります。また、<a href="#">404 ページの「NetWare のファイルシステムデータを復元する際のアクセス権の保存」</a>で説明している追加の手順も必要になる場合があります。</p> <ol style="list-style-type: none"> <li>新しい記憶デバイスに NetWare と eDirectory をインストールし、一時的な新しいツリー内に新しい SYS: ポリリュームを作成します。</li> <li>新しい SYS: ポリリューム上に、バックアップテープからコピーした eDirectory バックアップファイルを配置します。</li> <li>バックアップから eDirectory を復元します (元のツリー内に配置されます)。このとき、復元した後で eDirectory がクローズされ、ロックされたままになるようにオプションを指定します。次のようなコマンドを使用します。<br/> <pre>restore -r -f バックアップファイルの名前とパス -i ログファイルの名前とパス -e</pre> <p>NICI ファイルをバックアップしてあった場合は、-e オプションを使用します。インクルードファイルに列挙されたファイルをバックアップしてあった場合は、-u オプションを追加します。</p> </li> <li>記憶デバイスの交換によって影響を受けたすべてのポリリュームのファイルシステムを復元します。</li> <li>eDirectory データベースのロックを解除します。</li> <li>NICI セキュリティファイルを復元した場合は、復元を完了した後で、サーバを再起動してセキュリティシステムを再初期化します。</li> <li>サーバが通常どおりに応答するか、チェックます。<br/><br/>iMonitor を使用して、サーバとその同期をチェックします。ログインスクリプトと印刷が正しく動作することを確認します。</li> <li>このサーバでロールフォワードログを使用していた場合、復元を完了した後で、ロールフォワードログ設定を再作成します。ロールフォワードログを有効にしてから、改めてフルバックアップも取る必要があります。<br/><br/>復元した後は、設定がデフォルトの状態にリセットされます。つまり、ロールフォワードログがオフになっています。フルバックアップが改めて必要となるのは、スケジュールに従って次に無人でのフルバックアップが取られるまでに、再び障害が起こる可能性があるためです。</li> </ol> |



サーバが通常どおりに応答しない場合、次にいずれかの方法によって回復する必要があります。

- ◆ 変更前のハードウェア環境設定が機能していたことから、これを再作成します。
- ◆ 作成した eDirectory バックアップとファイルシステムを使用して、このサーバの識別情報を別のコンピュータに移します。540 ページの「サーバの計画的な交換」を参照してください。

## サーバの計画的な交換

次に示す手順で、サーバの eDirectory アイデンティティとファイルシステムデータを別のコンピュータ上に移すことで、実際にサーバを置き換えます。ここでは、古いサーバをサーバ A とし、それに置き換わるサーバをサーバ B としています。

Backup eMTool を使用して eDirectory のコールドバックアップ ( データベースをクローズした状態でのバックアップ ) を実行し、さらにお好みのツールを使用してファイルシステムのバックアップをして、サーバの交換に備えます。このバックアップ情報を用いれば、復元プロセスを使用して、新しいコンピュータ上にサーバを再構築できます。

eDirectory のコールドバックアップを実行する場合、オプションを使用してサーバ A 上の eDirectory をロックし、使用不可にする必要があります。これにより、バックアップ後のデータ変更を防げます。このサーバと通信している他のサーバからは、このサーバは停止しているように見えます。通常サーバに送信される eDirectory 情報は、そのサーバと再び通信できるようになるまで、ツリー内の別のサーバに保存されます。保存された情報は、新しいコンピュータであるサーバ B 上で、サーバがオンライン状態に戻ったときに同期するために使用されます。

**注:** eDirectory ツリー内の他のサーバは、このサーバがすぐにオンライン状態に戻ることを期待しているため、できるだけ早く交換してサーバに eDirectory 情報を復元する必要があります。

サーバを置き換えるための手順の概要を次に示します。

1. 交換する際のサーバ A の停止時間を短くするには、540 ページの「1. サーバ交換の準備」で説明しているようにサーバ B にオペレーティングシステムをインストールするなどして、交換前にできるだけサーバ B の準備を整えておきます。
2. 541 ページの「2. eDirectory のバックアップを作成する」の説明に従って、サーバ A の eDirectory とシステムファイルをバックアップします。
3. 542 ページの「3. サーバ交換における eDirectory 情報の復元」の説明に従って、サーバ B に情報を移します。

### 1. サーバ交換の準備

次に示すサーバ A とサーバ B のチェックリストを使用して、サーバ A を交換する準備ができているかを確認します。開始する前にサーバ B の準備をしておけば、あるコンピュータから別のコンピュータへ転送する間のサーバの停止時間を減らすことができます。

#### サーバ A の準備

- サーバ A に最新のバージョンのオペレーティングシステムがインストールされていることを確認します。
- Tree パーティションのマスタを保持しているサーバで DSRepair を実行し、さらに時刻同期を実行して、サーバ A のツリーが正常に機能していることを確認します。
- サーバ A のデータベースで DSRepair を実行します。サーバ A が完全に同期されていることを確認します。



## サーバ B の準備

- 最新バージョンのオペレーティングシステムをインストールします。このオペレーティングシステムは、サーバ A のものと同じである必要があります。
- サーバ B を新しい一時的なツリーに配置し、eDirectory をインストールします。  
(542 ページの「3. サーバ交換における eDirectory 情報の復元」の過程で eDirectory を復元するには、サーバ B をサーバ A が配置されていた元のツリー内に配置します。)
- (NetWare の場合のみ) サーバの交換でファイルシステムデータを復元する場合、ファイルシステム権の保持に関わる問題があることを認識しておく必要があります。ファイルシステムの復元の前に、eDirectory の復元を計画する必要があります。また、404 ページの「NetWare のファイルシステムデータを復元する際のアクセス権の保存」で説明している追加の手順も必要になる場合があります。

続いて、次のセクション 541 ページの「2. eDirectory のバックアップを作成する」の手順を実行します。

## 2. eDirectory のバックアップを作成する

サーバ交換の前に、eDirectory のバックアップを作成する必要があります。540 ページの「1. サーバ交換の準備」が完了した後は eMBox Client を使用し、バックアップの後でデータベースを使用不可にしてロックする詳細オプションを設定して、サーバ A 上の eDirectory データベースのコールドバックアップを実行します。

eDirectory のコールドバックアップ (データベースがクローズ中のバックアップ) を作成し、その後でデータベースをクローズのままにしておくには、次の手順に従います。

- 1 540 ページの「1. サーバ交換の準備」が完了していることを確認します。
- 2 次に示すような eMBox クライアントのコマンドで、`-c`、`-o`、および `-d` スイッチを使用して、サーバ A 上の eDirectory データベースのコールドバックアップを実行し、完了した後はデータベースをクローズしてロックしたままにします。

`backup -f` バックアップファイルの名前とパス  
`-l` ログファイルの名前とパス `-e -t -c -o -d`

NICI を使用する場合、`-e` スイッチを使用して NICI ファイルをバックアップします。(eMBox クライアントとスイッチの使用についての詳細は、420 ページの「eMBox クライアントによる手動バックアップ」および 420 ページの「eMBox クライアントによる手動バックアップ」を参照してください。)

サーバ A の eDirectory データベースがロックされます。データベースをサーバ B 上に復元しツリー内に戻すまでは、サーバ上で新たなデータ変更が実行されないように、データベースをロックしたままにしておく必要があります。

サーバアップグレードまたはサーバ交換の残りの手順を迅速に完了させ、サーバが使用できない時間を最小限に抑えます。

- 3 サーバ A のファイルシステムのフルバックアップを作成します。(NetWare では、SMS が使用できます。)

データベースをバックアップした後で、ファイルシステムのバックアップを行うのは重要です。これにより、eDirectory バックアップファイルが、残りのファイルシステムと一緒にテープに保存されます。

SMS の使用方法の詳細については、『*Management Services 管理ガイド*』 (<http://www.novell.com/documentation/lg/nw65/smsadmin/data/hjc2z4tu.html>) を参照してください。

- 4 サーバ A 上の eDirectory データベースをロックし、サーバ A をネットワークから外します。

続いて 542 ページの「3. サーバ交換における eDirectory 情報の復元」の手順を実行します。

### 3. サーバ交換における eDirectory 情報の復元

サーバ A の eDirectory 識別情報およびファイルシステムをサーバ B に移すには、次の手順に従います。

- 1 540 ページの「1. サーバ交換の準備」および 541 ページの「2. eDirectory のバックアップを作成する」が完了していることを確認します。
- 2 サーバ B が起動し、eDirectory が実行されていることを確認します。
- 3 復元により、サーバ A の eDirectory 識別情報およびファイルシステムを次の手順でサーバ B に移します。

- 3a サーバ A の eDirectory コールドバックアップファイルをサーバ B にコピーします。

サードパーティのファイル圧縮ツールは圧縮性能が良いので、そのようなツールを使用した場合、バックアップファイルはとても小さくなる場合があります。これにより、ファイルのコピーを早くできる場合があります。

- 3b 複製した eDirectory のバックアップファイルを使用して、サーバ A の eDirectory データベースをサーバ B 上に復元します。それには、eMBox コマンドラインクライアントで、次のようなコマンドを使用します。

```
restore -r -f バックアップファイルの名前とパス  
-l ログファイルの名前とパス -e
```

NICI を使用する場合、-e スイッチを使用して NICI ファイルを復元します。インクルードファイルに列挙されたファイルをバックアップしてあった場合は、-u オプションを追加します。(eMBox クライアントとスイッチの使用についての詳細は、428 ページの「eMBox クライアントによるバックアップファイルの復元作業」および 420 ページの「eMBox クライアントによる手動バックアップ」を参照してください。)

復元にはロールフォワードログを含める必要はありません。なぜなら、コールドバックアップを実行し、その後でデータベースをクローズしてあるからです。データベースではどのようなトランザクションも実行されていません。データベースはクローズされ、バックアップ以降にはロールフォワードログは作成されていません。

**重要:** NetWare では、ファイルシステムを復元する前に eDirectory を復元することが特に重要です。これにより、トラスティ割り当ておよび権利が、ファイルシステムデータの復元の後で保持されます。詳細については、404 ページの「NetWare のファイルシステムデータを復元する際のアクセス権の保存」を参照してください。

- 3c バックアップされたサーバ A のファイルシステムデータをサーバ B に移します。
- 4 (NetWare の場合のみ) autoexec.ncf で、サーバ B の IP アドレスとサーバ名を、サーバ A のものにリネームします。
- 5 NICI を使用している場合は、サーバを再起動して NICI を再初期化し、復元された NICI セキュリティファイルが使用されるようにします。
- 6 eDirectory データベースのロックを解除します。

- 7** 復元が完了した後は、サーバ B がサーバ A の識別情報を正しく引き継ぎ、通常どおりに応答しているかチェックします。ConsoleOne を使用してサーバとその同期をチェックします。ログインスクリプト、印刷、および NCI セキュリティが正常に機能することを確認します。

サーバの応答が通常どおりなら、サーバの交換は完了です。これで、サーバ A から eDirectory をアンインストールして eDirectory 識別情報を削除し、このコンピュータを別の目的に使用できます。サーバ A をネットワークに戻すのは、eDirectory を削除した後にしてください。そうしないと、eDirectory の同期でネットワークが混乱してしまいます。なぜなら、サーバ A とサーバ B の同じ識別情報により、競合が発生するためです。

- 8** (特定条件における処理) このサーバでロールフォワードログを使用していた場合、復元を完了した後で、ロールフォワードログ設定を作成し直します。ロールフォワードログを有効にしてから、改めてフルバックアップも取る必要があります。

復元した後は、設定がデフォルトの状態にリセットされます。つまり、ロールフォワードログがオフになっています。フルバックアップが改めて必要となるのは、スケジュールに従って次に無人でのフルバックアップが取られるまでに、再び障害が起こる可能性があるためです。

サーバ B が正常に動作せず、サーバ A の識別情報およびファイルシステムを直ちに使用できるようにする必要がある場合は、次を実行します。

- 1** サーバ B のネットワークケーブルを抜くか、またはサーバを停止します。
- 2** サーバ A をネットワークに再接続し、起動してから、eDirectory データベースをオープンします。

DSRepair の実行を要求するシステムメッセージを無視します。

- 3** サーバ B から eDirectory を削除し、再度アップグレードを試みます。

## ハードウェア障害後の eDirectory の復元

eDirectory が配置されたディスクパーティションまたはディスクボリュームを含むハードディスクの障害は、サーバから eDirectory が削除された状態と同じです。(幸いにも複数サーバ環境では、1つのサーバがダウンしても、そのレプリカリング内の残りのサーバが正常に稼働していれば問題はありません。)

eDirectory が格納されたディスクパーティションまたはディスクボリュームの障害の後で eDirectory を復元するには、[409 ページの「復元処理の準備」](#) および [417 ページの「iManager によるバックアップファイルの復元作業」](#) (または、[428 ページの「eMBox クライアントによるバックアップファイルの復元作業」](#)) で説明している手順に従って、バックアップファイルから復元します。

ハードディスクの新規インストールでは、製造元から提供されている指示に従って、サーバのハードディスクが動作することを検証します。新しいハードディスクには、少なくとも置き換えられる元のドライブと同じ記憶容量が必要です。ローカルサーバ情報のファイルを使用して、環境設定情報を確認します。

**注:** サーバのバックアップファイルがない場合は、Xbrowse ツールを使用して eDirectory に照会し、サーバ情報を回復します。この作業は、サーバオブジェクトやその関連オブジェクトをツリーから削除する前に実行する必要があります。XBrowse およびその他の情報は『[Technical Information Document #2960653](#)』 (<http://support.novell.com/servlet/tidfinder/2960653>) にあり、Novell サポートから入手できます。



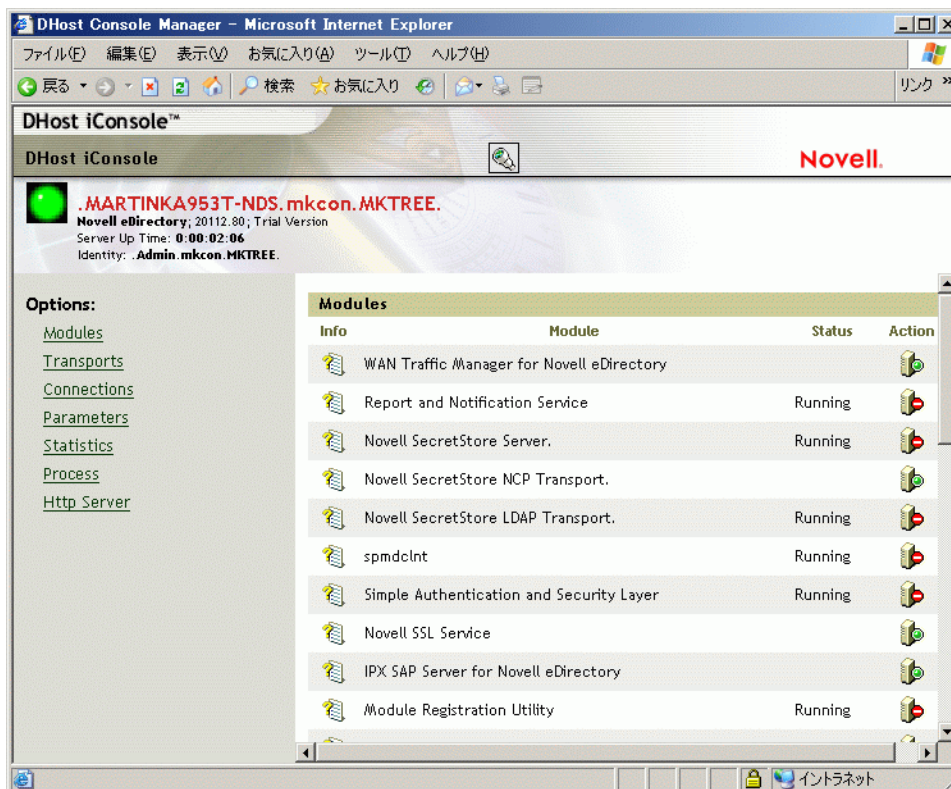
# 17

## DHost iConsole Manager

DHost iConsole Manager は Web ベースのブラウザを使用した管理ツールで、次のことが行えます。

- ◆ DHost モジュールの管理
- ◆ DHost 環境設定パラメータの照会
- ◆ DHost 接続情報の表示
- ◆ スレッドプール統計情報の表示
- ◆ DHost プロトコルスタックマネージャにより登録されたプロトコルに関する詳細情報の表示

図 50 DHost iConsole Manager



DHost iConsole Manager は診断およびデバッグツールとしても使用でき、eDirectory サーバが正常に動作していない場合に HTTP サーバにアクセスできます (詳細については、552 ページの「SAAdmin パスワードを設定する」を参照してください)。

この章では、次の情報について説明します。

- ◆ 546 ページの「DHost について」
- ◆ 547 ページの「DHost iConsole の実行」
- ◆ 548 ページの「eDirectory モジュールの管理」
- ◆ 550 ページの「DHost 情報の照会」
- ◆ 552 ページの「プロセススタック」
- ◆ 552 ページの「SAdmin パスワードを設定する」

## DHost について

Windows、Solaris、Linux、AIX、および HP-UX 用の Novell® eDirectory™ ソフトウェアは、eDirectory for NetWare® と同じコアコードに基づいて作成されています。Windows、Linux および UNIX 版の eDirectory が別のバージョンの eDirectory と適切にやり取りを行うには、NCP™ (NetWare Core Protocol™) サービスのサブセットをサポートする必要があります。このサブセットを操作するプログラムは DHost と呼ばれます。DHost は eDirectory の下で動作し、NetWare オペレーティングシステムがネイティブで提供する機能を NetWare 以外のプラットフォームで提供します。

Dhost は、次の NetWare 指向のサービスを提供します。

| サービス     | 説明   |
|----------|--|
| NCP エンジン | パケットベースのプロトコルで、クライアントが NetWare サーバとの間で要求の送信や応答を受信できるようにします。<br><br>詳細については、 <a href="http://developer.novell.com/ndk/doc/ncp/ncp__enu/data/hc4lztgy.html">NetWare Core Protocols (http://developer.novell.com/ndk/doc/ncp/ncp__enu/data/hc4lztgy.html)</a> を参照してください。    |
| ウォッチドッグ  | ワークステーションが NetWare サーバに接続された状態であることを確認するために使用するパケットです。<br><br>詳細については、 <a href="http://www.novell.com/documentation/lg/nw65/ixp_enu/data/h0cufuir.html">Watchdog Packet Spoofing (http://www.novell.com/documentation/lg/nw65/ixp_enu/data/h0cufuir.html)</a> を参照してください。 |
| 接続テーブル   | NetWare サーバに付随するあらゆるプロセス、プリントサーバ、アプリケーション、ワークステーション、またはその他のエンティティに割り当てられる固有の番号です。この番号は、接続が行われるごとに異なる可能性があります。接続番号は、ネットワークセキュリティの実装やネットワークアカウントに使用されます。この番号は、ファイルサーバ接続テーブル内でのオブジェクトの場所を反映しています。さらにこの番号を使用すると、ネットワークにログインしたオブジェクトに関する情報の識別や取得が容易になります。                     |
| イベントシステム | 個々のサーバのアクティビティを監視する手段をアプリケーションに提供します。  |
| スレッドプール  | 独立したエンティティとして実行され、システムソフトウェアによってスケジュールされる一連の命令です。  |



| サービス    | 説明  |
|---------|---|
| NCP 拡張  | <p>サーバアプリケーション開発者が、NetWare OS に NCP として実装する NLM™ ソフトウェアを作成できるようにします。</p> <p>詳細については、<a href="http://developer.novell.com/ndk/doc/ncp/index.html?page=/ndk/doc/ncp/ncp__enu/data/a1wftl8.html">NCP Extension Concepts (http://developer.novell.com/ndk/doc/ncp/index.html?page=/ndk/doc/ncp/ncp__enu/data/a1wftl8.html)</a> を参照してください。</p> |
| メッセージ処理 | <p>ドキュメントを圧縮または凝縮した形式、またはドキュメントの要約で、大きなドキュメントの電子指紋として機能します。メッセージ処理は、個々のドキュメントに固有のデジタル署名を作成するために使用されます。</p>  |

## DHost iConsole の実行

- ◆ 547 ページの「[NetWare で DHost iConsole を実行する](#)」
- ◆ 547 ページの「[Windows で DHost iConsole を実行する](#)」
- ◆ 548 ページの「[Linux、Solaris、AIX、および HP-UX で DHost iConsole を実行する](#)」

## NetWare で DHost iConsole を実行する

NetWare では、NetWare Remote Manager を使用して DHost iConsole にアクセスできます。SAdmin パスワードの設定や変更を行うには、eDirectory サーバで httpstk.nlm を実行している必要があります。

- 1 Web ブラウザを開きます。
- 2 アドレス (URL) フィールドに、次の形式で入力します。

**http://サーバのTCP/IPアドレス:ポート**

例:

http://137.65.123.11:8028

**注:** デフォルトの代替ポート番号は 8028 です。NetWare リモートマネージャの環境設定ページでこの値を変更した場合は、変更後のポート番号を入力します。

サーバ名と IP アドレスの解決のために DNS (Domain Name Service) をネットワークにインストールしてある場合は、IP アドレスの代わりにサーバの DNS 名を入力することもできます。

- 3 ユーザ名、コンテキスト、パスワードを指定します。

## Windows で DHost iConsole を実行する

- 1 Web ブラウザを開きます。
- 2 アドレス (URL) フィールドに、次の形式で入力します。

**http://サーバ名:ポート/dhost**

たとえば、次のように入力します。

http://MyServer:80/dhost

DHost iConsole へのアクセスに、サーバの IP アドレスを使用することもできます。

例:

http://137.65.135.150:80/dhost

- 3 ユーザ名、コンテキスト、パスワードを指定します。

## Linux、Solaris、AIX、および HP-UX で DHost iConsole を実行する

- 1 Web ブラウザを開きます。
- 2 アドレス (URL) フィールドに、次の形式で入力します。

**http:// サーバ名 : ポート /dhost**

例 :

http://MyServer:80/dhost

DHost iConsole へのアクセスに、サーバの IP アドレスを使用することもできます。

例 :

http://137.65.135.150:80/dhost





- 3 ユーザ名、コンテキスト、パスワードを指定します。

## eDirectory モジュールの管理

DHost iConsole のモジュールページでは、使用可能な eDirectory サービスとその状態についての情報が表示されます。また、このモジュールページからこれらのサービスを開始または停止 (ロードまたはアンロード) できます。

ロードやアンロードができるのは、LDAP、SNMP、HTTPSTK などの非対話型モジュールだけです。

モジュールページには、次に示す属性があります。

| 属性    | 説明  |
|-------|---|
| 情報    |  をクリックして、モジュールの説明、ファイル名、モジュールハンドル、属性、および選択したモジュールの共有オブジェクト名を表示させます。  |
| モジュール | モジュール名を表示します。   |
| ステータス | モジュールが実行されているかどうかを表示します。  |
| アクション | モジュールが実行可能かどうかを示します。モジュールのステータスは、次の 3 つのうちのどれかになります。<br> は、モジュールがシステムモジュールで、アンロードできないことを示します。<br> は、モジュールがロード可能で、ロードの準備ができていることを示します。<br> は、モジュールが実行中であることを示します。 |

- ◆ 549 ページの「NetWare でモジュールをロードまたはアンロードする」
- ◆ 549 ページの「Windows でモジュールをロードまたはアンロードする」
- ◆ 549 ページの「Linux、Solaris、AIX、および HP-UX でモジュールをロードまたはアンロードする」

Novell iManager を使用した eDirectory サービスのロードやアンロードについての詳細は、194 ページの「eDirectory Service Manager」を参照してください。



## NetWare でモジュールをロードまたはアンロードする

- 1 Web ブラウザを開きます。
- 2 アドレス (URL) フィールドに、次の形式で入力します。

**http:// サーバの TCP/IP アドレス : ポート**

例 :

http://137.65.123.11:8028

注 : デフォルトの代替ポート番号は 8028 です。NetWare リモートマネージャの環境設定ページでこの値を変更した場合は、変更後のポート番号を入力します。

サーバ名と IP アドレスの解決のために DNS (Domain Name Service) をネットワークにインストールしてある場合は、IP アドレスの代わりにサーバの DNS 名を入力することもできます。

- 3 ユーザ名、コンテキスト、パスワードを指定します。
- 4 アプリケーションの管理リストで [List Modules (モジュールを一覧)] をクリックします。
- 5 モジュールをロードするには、名前を入力して [Load Module (モジュールをロード)] をクリックします。

モジュールが実際にロードされたかどうかの確認が必要な場合は、[モジュールロード用のシステムコンソールの表示] チェックボックスをオンにします。

## Windows でモジュールをロードまたはアンロードする

- 1 Web ブラウザを開きます。
- 2 アドレス (URL) フィールドに、次の形式で入力します。

**http:// サーバ名 : ポート /dhost**



たとえば、次のように入力します。

http://MyServer:80/dhost

DHost iConsole へのアクセスに、サーバの IP アドレスを使用することもできます。

例 :

http://137.65.135.150:80/dhost

- 3 ユーザ名、コンテキスト、パスワードを指定します。
- 4 [モジュール] をクリックします。
- 5 モジュールをロードするには  をクリックし、アンロードするには  をクリックします。

## Linux、Solaris、AIX、および HP-UX でモジュールをロードまたはアンロードする

- 1 Web ブラウザを開きます。
- 2 アドレス (URL) フィールドに、次の形式で入力します。

**http:// サーバ名 : ポート /dhost**



たとえば、次のように入力します。

http://MyServer:80/dhost

DHost iConsole へのアクセスに、サーバの IP アドレスを使用することもできます。

例 :

http://137.65.135.150:80/dhost

- 3 ユーザ名、コンテキスト、パスワードを指定します。
- 4 [モジュール] をクリックします。
- 5 モジュールをロードするには  をクリックし、アンロードするには  をクリックします。

## DHost 情報の照会

DHost iConsole マネージャを使用すれば、次に示す情報を照会できます。

- ◆ 環境設定パラメータ
- ◆ PSTACK マネージャにより登録されたプロトコル
- ◆ 接続プロパティ
- ◆ スレッドプールの概要

## 環境設定パラメータを表示する

環境設定パラメータは、Linux および UNIX プラットフォームに特有のものです。

DHost iConsole マネージャで、[パラメータ] をクリックします。詳細については、[548 ページの「Linux、Solaris、AIX、および HP-UX で DHost iConsole を実行する」](#)を参照してください。

環境設定パラメータには、次の情報が表示されます。

| オプション  | 説明                      |
|--------|-------------------------|
| パラメータ名 | 環境設定パラメータの名前を表示します。     |
| デフォルト値 | 環境設定パラメータのデフォルト値を表示します。 |
| 設定値    | 現在の設定値を表示します。           |
| 最小値    | パラメータに設定できる最小値を表示します。   |
| 最大値    | パラメータに設定できる最大値を表示します。   |
| タイプ    | パラメータに設定できる値のタイプを表示します。 |

詳細については、『Novell eDirectory 8.8 インストールガイド』の「[環境設定パラメータ](#)」を参照してください。

## プロトコル情報を表示する

DHost iConsole マネージャで、[トランスポート] をクリックします。

次のプロトコル情報が表示されます。

- ◆ ID
- ◆ プロトコル
- ◆ トランスポート

## 接続プロパティを表示する

DHost iConsole マネージャで、[接続] をクリックします。

次の接続プロパティが表示されます。

- ◆ 接続
- ◆ フラグ
- ◆ 識別子
- ◆ 表示名
- ◆ トランスポート
- ◆ 認証名
- ◆ SEV 回数
- ◆ 最終アクセス
- ◆ ロック状態

## スレッドプールの統計情報を表示する

DHost iConsole マネージャで、[統計情報] をクリックします。

次のスレッドプール統計情報が表示されます。

- ◆ Spawned Threads (生成スレッド)
- ◆ Dead Threads (停止スレッド)
- ◆ Idle Threads (アイドルスレッド)
- ◆ Worker Thread (動作スレッド)
- ◆ Peak Worker Thread (ピーク動作スレッド)
- ◆ Ready for Work Thread (動作待機スレッド)
- ◆ Ready Queue Peak Worker Threads (待機キューピーク動作スレッド)
- ◆ Ready Queue Max Wait Time (待機キュー最大待ち時間)
- ◆ Schedule Delay Minimum Time (最小スケジュール遅延時間)
- ◆ Schedule Delay Maximum Time (最大スケジュール遅延時間)
- ◆ Schedule Delay Average Time (平均スケジュール遅延時間)
- ◆ Waiting For Work (動作待ち)
- ◆ Peaking Waiting For Work (ピーク動作待ち)

## プロセススタック

プロセススタックには、DHost のプロセス空間で現在実行されているすべてのスレッドのリストが含まれます。この機能は、主に Novell エンジニアやサポート担当者により、ローレベルのデバッグツールとして使用されます。

このオプションは、Windows でのみ使用できます。

- 1 Web ブラウザを開きます。
- 2 アドレス (URL) フィールドに、次の形式で入力します。

**http://サーバ名:ポート/dhost**

たとえば、次のように入力します。

http://MyServer:80/dhost

DHost iConsole へのアクセスに、サーバの IP アドレスを使用することもできます。

例：

http://137.65.135.150:80/dhost

- 3 ユーザ名、コンテキスト、パスワードを指定します。
- 4 [プロセス] をクリックします。
- 5 スレッドのコールスタックを表示するには、スレッド ID をクリックします。

## SAdmin パスワードを設定する

あらかじめ設定された admin ユーザをセットアップできます。これにより、eDirectory がロードされていない場合に、HTTPSTK (HTTP Protocol Stack) にアクセスできるようになります。事前に設定された管理者ユーザ (SAdmin) には、eDirectory 管理者ユーザオブジェクトと同等の権利があります。サーバが、eDirectory が適切に機能していない状態の場合、このユーザとしてサーバにログインし、eDirectory を使用せずに実行できる必要なすべての診断およびデバッグ作業を実行します。

- ◆ [552 ページの「NetWare で SAdmin パスワードを設定する」](#)
- ◆ [553 ページの「Windows で SAdmin パスワードを設定する」](#)
- ◆ [553 ページの「Linux, Solaris, AIX, および HP-UX で SAdmin パスワードを設定する」](#)

## NetWare で SAdmin パスワードを設定する

NetWare リモートマネージャを使用して SAdmin ユーザオブジェクトを有効にし、このオブジェクトのパスワードを設定または変更します。SAdmin パスワードの設定や変更を行うには、eDirectory サーバで httpstk.nlm を実行している必要があります。

- 1 Web ブラウザを開きます。
- 2 アドレス (URL) フィールドに、次の形式で入力します。


**http://サーバのTCP/IPアドレス:ポート**

例：

http://137.65.123.11:8028

注：デフォルトの代替ポート番号は 8028 です。NetWare リモートマネージャの環境設定ページでこの値を変更した場合は、変更後のポート番号を入力します。

サーバ名と IP アドレスの解決のために DNS (Domain Name Service) をネットワークにインストールしてある場合は、IP アドレスの代わりにサーバの DNS 名を入力することもできます。

- 3 ユーザ名、コンテキスト、パスワードを指定します。
- 4 [環境設定] ボタン  > [Enable Emergency Account (SADMIN User) (緊急アカウントの有効化 (SADMIN ユーザ))] の順にクリックし、[パスワードの設定] をクリックします。
- 5 SAdmin パスワードを指定し、次に指定したパスワードを確認入力します。
- 6 [設定] をクリックします。

## Windows で SAdmin パスワードを設定する

DHOST リモートマネージャページ (/dhost URL またはルートページからアクセス可能) を使用して、SAdmin パスワードを設定します。SAdmin パスワードの設定や変更を行うには、eDirectory サーバで dhost.exe を実行している必要があります。

- 1 Web ブラウザを開きます。
- 2 アドレス (URL) フィールドに、次の形式で入力します。

**http://サーバ名:ポート/dhost**

たとえば、次のように入力します。

http://MyServer:80/dhost

DHost iConsole へのアクセスに、サーバの IP アドレスを使用することもできます。  
例：

http://137.65.135.150:80/dhost

- 3 ユーザ名、コンテキスト、パスワードを指定します。
- 4 HTTP サーバをクリックしてから、SAdmin パスワードを指定します。
- 5 指定したパスワードを確認入力して、[送信] をクリックします。

## Linux、Solaris、AIX、および HP-UX で SAdmin パスワードを設定する

Solaris、Linux、AIX、または HP-UX で SAdmin パスワードを設定するには、次のいずれかの方法を使用できます。

- ◆ [554 ページの「DHOST リモート管理ページ」](#)
- ◆ [554 ページの「Ndsconfig」](#)

## DHOST リモート管理ページ

DHOST リモートマネージャページ (/dhost URL またはルートページからアクセス可能) を使用して、SAdmin パスワードを設定します。SAdmin パスワードの設定や変更を行うには、eDirectory サーバで Novell eDirectory サーバを実行している必要があります。

- 1 Web ブラウザを開きます。
- 2 アドレス (URL) フィールドに、次の形式で入力します。

**http://サーバ名:ポート/dhost**

たとえば、次のように入力します。

http://MyServer:80/dhost

DHost iConsole へのアクセスに、サーバの IP アドレスを使用することもできます。  
例:

http://137.65.135.150:80/dhost

- 3 ユーザ名、コンテキスト、パスワードを指定します。
- 4 HTTP サーバをクリックしてから、SAdmin パスワードを指定します。
- 5 指定したパスワードを確認入力して、[送信] をクリックします。

## Ndsconfig

ndsconfig ユーティリティを使用して、SAdmin パスワードを設定します。SAdmin パスワードの設定や変更を行うには、eDirectory サーバで ndsd を実行している必要があります。

サーバコンソールから、次のように入力します。

**ndsconfig set http.server.sadmin-pwd=パスワード**

ここでパスワードは、新しい SAdmin パスワードです。

ndsconfig ユーティリティの使用に関する詳細については、『Novell eDirectory 8.8 インストールガイド』の「**ndsconfig ユーティリティのパラメータ**」を参照してください。

# 18 eDirectory Management Toolbox

Novell® eDirectory™ Management Toolbox (eMBox) を使用すれば、すべての eDirectory バックエンドユーティリティに、サーバ上だけでなくリモートからもアクセスできます。

eMBox を Novell iManager とあわせて使用すると、DSRepair、DSMerge、バックアップと復元、サービスマネージャなどの eDirectory ユーティリティに Web ベースでアクセスできます。

**重要**：eMBox タスクを実行するには、iManager を使用して、管理するツリーに役割ベースサービスを設定する必要があります。

すべての機能は、ローカルサーバまたはリモートのいずれからでもコマンドラインクライアントを通じて使用できます。eMBox クライアントを使用して、1 つのサーバまたはワークステーションから複数のサーバに対するタスクを実行できます。

バックアップ、DSRepair、DSMerge、スキーマの操作、および eDirectory Service Manager などのすべての eMTool (eDirectory Management Tool) を実行するためには、eDirectory サーバに eMBox がロードされ、実行されている必要があります。

このセクションでは、次のトピックについて説明します。

- ◆ [555 ページの「eMBox コマンドラインクライアントの使用」](#)
- ◆ [566 ページの「eMBox ログの記録の使用」](#)

## eMBox コマンドラインクライアントの使用

eMBox にアクセスする方法の 1 つは、eMBox の Java コマンドラインクライアントを使用することです。このコマンドラインクライアントには、対話式モードとバッチモードの 2 つのモードがあります。対話式モードでは、eMBox コマンドを一度に 1 つずつ実行します。バッチモードでは、コマンドのグループを自動で実行できます。コマンドラインクライアントにはログサービスがあり、いずれのモードでも使用できます。

コマンドラインクライアントは、Java アプリケーションです。これを実行するには、Java Runtime Environment, Sun JVM 1.3.1 が使用できる必要があります。この Java 実行環境は、eDirectory と同時にインストールされます。また、ファイアウォール越しに管理対象のサーバにアクセスできる必要があります。1 つのサーバまたはワークステーションから、複数のサーバに対してタスクを実行できます。

このセクションでは、次のトピックについて説明します。

- ◆ [556 ページの「コマンドラインヘルプを表示する」](#)
- ◆ [556 ページの「eMBox コマンドラインクライアントを対話式モードで実行する」](#)
- ◆ [560 ページの「eMBox コマンドラインクライアントをバッチモードで実行する」](#)
- ◆ [563 ページの「eMBox コマンドラインクライアントのオプション」](#)
- ◆ [564 ページの「eMBox クライアントを使用してセキュア接続を確立する」](#)
- ◆ [564 ページの「eDirectory ポート番号を確認する」](#)

## コマンドラインヘルプを表示する

eMBox クライアントを実行する前に、eMBox の一般的なコマンドラインヘルプを表示するには、次の操作を実行します。

- ◆ Netware<sup>®</sup>、Linux、および UNIX: コマンドラインから「`edirutil -?`」と入力します。
- ◆ Windows : 「`ドライブ¥novell¥nds¥embox¥edirutil.exe -?`」を実行します。

対話式モードで実行中に eMBox の対話型コマンドラインヘルプを表示するには、eMBox クライアントプロンプトで疑問符 (?) を入力します。たとえば、次のように入力します。

```
eMBox Client> ?
```

ヘルプには、[563 ページの「eMBox コマンドラインクライアントのオプション」](#)で示すようなコマンドラインオプションに関する情報が表示されます。

## eMBox コマンドラインクライアントを対話式モードで実行する

対話式モードでは、eMBox コマンドを一度に 1 つずつ実行します。

このセクションでは、次のトピックについて説明します。

- ◆ [556 ページの「eDirectory サーバで eMBox クライアントを実行する」](#)
- ◆ [557 ページの「ワークステーションで eMBox クライアントを実行する」](#)
- ◆ [558 ページの「サーバにログインする」](#)
- ◆ [559 ページの「使用言語、タイムアウト、およびログファイルを設定する」](#)
- ◆ [559 ページの「eMTool とそのサービスを表示する」](#)
- ◆ [560 ページの「特定のサービスを実行する」](#)
- ◆ [560 ページの「現在のサーバからログアウトする」](#)
- ◆ [560 ページの「eMBox クライアントを終了する」](#)

## eDirectory サーバで eMBox クライアントを実行する

eMBox クライアントおよび Sun JVM 1.3.1 は、eDirectory と同時にインストールされています。eDirectory サーバの対話式モードで eMBox クライアントを開始するには、次の操作を行います。

- ◆ NetWare、Linux、および UNIX : コマンドラインから「`edirutil -i`」と入力します。
- ◆ Windows : 「`ドライブ¥novell¥nds¥edirutil.exe -i`」を実行します。

edirutil ファイルは、eMBox クライアントを実行するためのショートカットです。このファイルには、Java 実行ファイルの場所と eMBox が eDirectory と同時にインストールされたデフォルトの場所が示されています。NetWare の場合、このファイルでは `-ns` オプションが指定されています (これは NetWare の Java オプションで、「新規画面」を意味します)。(Java 実行ファイルの場所は、[557 ページの「eMBox クライアント用にパスおよびクラスパスをセットアップする」](#)で示しているように手動で入力することもできます。)

管理対象のサーバに対して eMBox コマンドラインクライアントを使用するには、ファイアウォール越しにアクセスできる必要があります。そのため、リモートで実行する場合は、VPN アクセスが必要となります。



## ワークステーションで eMBox クライアントを実行する

eDirectory サーバではないコンピュータで eMBox クライアントを使用するには、次の操作を実行します。

- ◆ eMBoxClient.jar ファイルを eDirectory サーバから目的のコンピュータにコピーします。
  - ◆ NetWare: sys:¥system¥embox¥eMBoxClient.jar
  - ◆ Windows: ¥novell¥nds¥embox¥eMBoxClient.jar
  - ◆ Linux および UNIX: /opt/novell/eDirectory/lib/nds-modules/embox/eMBoxClient.jar
- ◆ Sun JVM 1.3.1 がインストールされていることを確認します。
- ◆ 管理するサーバに対して eMBox コマンドラインクライアントを使用するためには、ファイアウォール越しにアクセスできることを確認します。

サーバの場合とは異なり、ワークステーションの場合は、edirutil コマンドをショートカットとして使用して eMBox クライアントを対話式モードで開始することはできません。パスおよびクラスパス内で環境をセットアップするか、パスをその都度手動で入力します。[557 ページの「eMBox クライアント用にパスおよびクラスパスをセットアップする」](#)を参照してください。

## eMBox クライアント用にパスおよびクラスパスをセットアップする

eMBox クライアントが eDirectory サーバで実行され、Java または eMBoxClient.jar ファイルの場所を変更していない場合、edirutil をショートカットとして使用して eMBox クライアントを実行できます。[\(556 ページの「eDirectory サーバで eMBox クライアントを実行する」](#)を参照してください。)

ただし、デフォルトの場所を変更したか、または eMBoxClient.jar ファイルをサーバでないコンピュータ上で実行している場合、あるいはクラスパスを手動で入力したい場合は、eMBox クライアントのパスおよびクラスパスをこのセクションの説明のようにセットアップする必要があります。

次の操作を実行すれば、eMBox クライアントをコンピュータ上のどの場所からでも実行できます。

- ◆ Java 実行ファイル (Java.exe など) があるディレクトリをパスに追加するか、または Java がすでに実行されていることを確認します。

サーバの場合、ほとんどはすでに実行されています。Windows サーバ、Linux サーバ、および UNIX サーバでは、実行ファイルのディレクトリをパスに追加する必要があります。NetWare の場合、ディレクトリをパスに追加するのではなく、Java が実行されている必要があります。

ワークステーションの場合、手動セットアップが必要となる場合があります。たとえば Windows では、[スタート] > [設定] > [コントロールパネル] > [システム] の順にクリックします。[詳細設定] タブで [環境変数] をクリックし、PATH 変数にパスを追加します。

パスを手動で入力するには、次の操作を実行します。Java 実行ファイルへのパスが追加されていない場合、eMBox を実行する前に、最初にコマンドラインで Java 実行ファイルが含まれたディレクトリへ移動する必要があります。たとえば、Windows で次のように入力します。

```
cd c:¥novell¥nds¥embox¥jre¥bin
```

- ◆ eMBoxClient.jar ファイルへのパスを、クラスパスに追加します。

NetWare サーバの場合：

```
set ENVSET= パス¥eMBoxClient.jar
```

Windows サーバまたはワークステーションの場合：

```
set CLASSPATH= パス¥eMBoxClient.jar
```

LINUX サーバおよび UNIX サーバまたはワークステーションの場合：

```
export CLASSPATH= パス /eMBoxClient.jar
```

パスを手動で入力するには、次の操作を実行します。クラスパスを指定するには、次のようにして、eMBox を実行するたびに Java の `-cp` フラグを使用する方法もあります。

```
java -cp パス/eMBoxClient.jar embox -i
```

たとえば、Windows では次のように入力します。

```
java -cp c:¥novell¥nds¥embox¥eMBoxClient.jar embox -i
```

**警告：**NetWare サーバの場合のみ、異常終了を防ぐために `-ns` (「新規画面」を開く NetWare での Java オプション) を追加します。たとえば、次のように入力します。

```
java -ns -cp sys:¥system¥embox¥eMBoxClient.jar embox -i
```

これらの手順を実行した後は、次のコマンドを使用して、コンピュータ上のどの場所からでも対話式モードによる eMBox クライアントを実行できます。

```
java embox -i
```

**警告：**NetWare サーバの場合のみ、異常終了を防ぐために `-ns` (「新規画面」を開く NetWare での Java オプション) を追加します。たとえば、次のように入力します。

```
java -ns embox -i
```

Java コマンドについては、[Sun Web サイト \(http://java.sun.com\)](http://java.sun.com) にある Java のマニュアルを参照してください。

## サーバにログインする

サーバにログインするには、サーバ名または IP アドレス、および特定のサーバへ接続するためのポート番号を指定する必要があります。パブリックログインの場合、ユーザ名およびパスワードは必要ありません。

たとえば、eMBox クライアントを対話式モードでオープンした後で、次のように入力します。

```
login -s 137.65.123.244 -p 8028 -u admin.mycompany  
-w mypassword -n
```

ポート番号についての詳細は、[564 ページの「eDirectory ポート番号を確認する」](#)を参照してください。

## 使用言語、タイムアウト、およびログファイルを設定する

デフォルトの言語は、クライアントシステムの言語です。そのため、ほとんどの場合、特別に言語を設定する必要はありません。同様に、タイムアウトもほとんどの場合、デフォルトの設定で問題ありません。ログファイルを設定するには、ファイル名とファイルを開くモード（追加または上書き）を指定します。

次の表に、コマンド例を示します。

| コマンド                             | 説明   |
|----------------------------------|--|
| <code>set -L en,de</code>        | 使用言語を英語、ドイツ語の優先順で設定します。                                      |
| <code>set -T 100</code>          | タイムアウトを 100 秒に設定します。タイムアウトは、サーバからの応答を待つ時間を設定するものです。          |
| <code>set -l mylog.txt -o</code> | mylog.txt をログファイルとして使用し、開いた後は上書きします。<br><br>デフォルトの設定は「追加」です。 |

## eMTool とそのサービスを表示する

サーバにログインしたら、`list` コマンドを使用して、そのサーバ上で使用できるサービスを表示できます。

`list` コマンドを使用すると、次に示す eMTool とそのサービスが動的に表示されます。

| eMTool   | 説明                                 |
|----------|------------------------------------|
| backup   | Novell eDirectory バックアップ eMTool    |
| dsmerge  | Novell eDirectory マージ eMTool       |
| dsrepair | Novell eDirectory 修復 eMTool        |
| dsschema | Novell eDirectory スキーマ操作 eMTool    |
| service  | Novell eDirectory サービスマネージャ eMTool |

リストを強制的にリフレッシュするには、`-r` を使用します。サービスの詳細を表示するには、`-t` を使用します。コマンド形式だけを表示するには、`-f` を使用します。

次の表に、コマンド例を示します。

| コマンド                            | 説明                           |
|---------------------------------|------------------------------|
| <code>list</code>               | サーバ上で使用できる eMTool を表示します。    |
| <code>list -r</code>            | eMTool リストをリフレッシュします。        |
| <code>list -t backup</code>     | backup サービスの詳細を表示します。        |
| <code>list -t dsrepair</code>   | DSRepair サービスの詳細を表示します。      |
| <code>list -t dsmerge -f</code> | DSMerge サービスのコマンド形式だけを表示します。 |

## 特定のサービスを実行する

サーバにログインした後は、各 eMTool サービスを使用してタスクを実行できます。例：

| コマンド                          | 説明                |
|-------------------------------|-------------------|
| <code>dsrepair.rld</code>     | ローカルデータベースを修復します。 |
| <code>backup.getconfig</code> | バックアップ設定情報を取得します。 |

詳細については、次を参照してください。

- ◆ 420 ページの「eMBox クライアントを使ったバックアップ / 復元作業」
- ◆ 238 ページの「eMBox クライアントを使用したツリーのマージ」
- ◆ 289 ページの「eMBox クライアントを使用したデータベースの修復」
- ◆ 194 ページの「eMBox クライアントのサービスマネージャ eMTool を使用する」

## 現在のサーバからログアウトする

現在のセッションからログアウトするには、次のコマンドを使用します。

**logout**

別のサーバにログインする場合は、自動的に現在のサーバからログアウトされるので、このコマンドは必要ありません。

## eMBox クライアントを終了する

eMBox クライアントを終了するには、次のいずれかのコマンドを使用します。

**exit**

または

**quit**

## eMBox コマンドラインクライアントをバッチモードで実行する

eMBox クライアントをバッチモードで実行するには、次の 3 つの方法があります。

- ◆ 561 ページの「単一タスク」
- ◆ 561 ページの「内部バッチファイル」
- ◆ 562 ページの「システムバッチファイル」

システムバッチファイルと内部バッチファイルを組み合わせて使用することで、コマンドをより自由に実行でき、頻繁に実行するコマンドの編成や再使用が可能です。

## 単一タスク

コマンドラインから単一の eMBox タスクをバッチモードで実行するには、コマンドに `-t` オプションを使用してツールとタスクを指定し、`-i` オプション (対話式モードを指定するオプション) を省くだけです。たとえば、次のように入力します。

```
java embox -s 137.65.123.244 -p 8028 -u admin.mycompany  
-w mypassword -l mylog.txt -t dsrepair.rld -n
```

**警告:** NetWare の場合のみ、異常終了を防ぐために `-ns` (「新規画面」を開く NetWare での Java オプション) を追加します。たとえば、次のように入力します。

```
java -ns embox -s 137.65.123.244 -p 8028 -u admin.mycompany -w mypassword -l mylog.txt  
-t dsrepair.rld -n
```

異なるサーバ上で複数のタスクを実行する場合や、頻繁に実行するタスクの場合は、内部バッチファイルを使用する方が便利です。詳細については、次のセクション「[内部バッチファイル](#)」を参照してください。

## 内部バッチファイル

eMBox クライアントの内部バッチファイルを使用して eMBox クライアントをバッチモードで実行するには、対話式モードで実行するような eMBox コマンドのグループを含むファイルを作成する必要があります。

eMBox クライアントの内部バッチファイルを使用すれば、バッチファイル内のすべてのコマンドを自動で実行できます。複数の eMBox ツールを使用した複数のタスクを、同一のサーバ上でタスクごとにログインとログアウトを繰り返すことなく実行できます。また 1 つのサーバから、複数のサーバに対して複数の eMBox ツールを使用したタスクを実行できます。

内部バッチファイルを使用すれば、頻繁に実行するコマンドの編成や再利用ができます。そのため、これらのコマンドを実行するたびに、コマンドラインから手動で入力する必要はありません。

内部バッチファイルの実行は、コマンドラインから eMBox クライアントコマンドを使用して行います。たとえば、次のコマンドは、サーバにログインし、`mybatch.mbx` ファイル内に列挙されたコマンドを実行します。

```
java embox -s 137.65.123.244 -p 8028 -u admin.mycompany -w mypassword -l  
mylog.txt -o -b mybatch.mbx -n
```

**警告:** NetWare の場合のみ、異常終了を防ぐために `-ns` (「新規画面」を開く NetWare での Java オプション) を追加します。たとえば、次のように入力します。

```
java -ns embox -s 137.65.123.244 -p 8028 -u admin.mycompany -w mypassword -l mylog.txt  
-o -b mybatch.mbx -n
```

もう 1 つの方法は、同様のコマンドをシステムバッチファイル内に記述し、そのファイルがサーバ上で自動実行されるようにスケジューリングすることです。[562 ページの「システムバッチファイル」](#)を参照してください。

次に、eMBox 内部バッチファイルの例を示します。このファイルには、実行するコマンドの例および別のサーバへログインする例が記述されています。この例では、eMBox クライアントを開いたときに、サーバにログインしているものと仮定しています。(それぞれのコマンドは、行を分ける必要があります。# で始まる行はコメントです。)

```
# This file is named mybatch.mbx.  
# This is an example of commands you could use in  
# an eMBox internal command batch file.  
  
# Backup commands
```

```

backup.getconfig
backup.backup -b -f mybackup.bak -l backup.log -t -e -w

# DSRepair commands
dsrepair.rld

# Log in to a different server
login -s 137.65.123.255 -p 8028 -u admin.mycompany -w mypassword -n

# DSMerge commands
dsmerge.pr -u admin.mycompany -p admin.mycompany -n mypassword

# Schema Operations
dsschema.rst
dsschema.dse
dsschema.rls
dsschema.gsu
dsschema.scc
dsschema.irs -n LocalTree

# DSService commands
service.serviceList

# End of example.

```

## システムバッチファイル

他のコマンドラインツールと同様に、eMBox クライアントコマンドが含まれたシステムバッチファイルを作成し、それらをコマンドラインから手動で実行したり、サーバ上で自動で実行されるようにスケジュールしたりできます。たとえば、[423 ページの「バッチファイルと eMBox クライアントによる無人バックアップ」](#)で示す例のように、システムバッチファイルを使用して、自動でバックアップを実行できます。

1つのサーバから複数のサーバに対して、複数の eMBox ツールを使用したタスクを実行できます。

システムバッチファイルでは、eMBox クライアントの単一コマンドと内部バッチファイルを組み合わせて使用できます。これにより、コマンドをより自由に実行でき、頻繁に実行するコマンドの編成や再使用ができます。詳細については、[561 ページの「内部バッチファイル」](#)を参照してください。

バッチファイルを自動で実行する方法については、ご使用のオペレーティングシステムのマニュアルまたはサードパーティ製スケジューリングソフトウェアのマニュアルを参照してください。

**注:** NetWare では、サードパーティのスケジューリングソフトウェアが使用できます。また、サポート対象のツールではありませんが、Novell Technical Support から [CRON.NLM \(http://support.novell.com/servlet/tidfinder/2939440\)](http://support.novell.com/servlet/tidfinder/2939440) をダウンロードしてお使いいただけます。

## eMBox コマンドラインクライアントのオプション

| オプション               | 説明   |
|---------------------|--|
| -? または -h           | ヘルプ情報を表示します。   |
| -i                  | eMBox コマンドを一度に 1 つずつ、対話的に実行します。  |
| -s サーバ              | eMBox サーバの名前または IP アドレスを指定します。<br>デフォルト値は 127.0.0.1 です。  |
| -p ポート              | eMBox サーバのポート番号を指定します。<br>デフォルト値は 80 です。   |
| -u ユーザ              | ユーザ DN を指定します。たとえば、admin.mycompany と指定します。<br>デフォルト値は anonymous です。  |
| -w パスワード            | -u で指定したユーザのパスワードを指定します。   |
| -m モード              | ログインモードを指定します。<br>デフォルト値は dclient です。  |
| -n                  | 安全な SSL 接続を試行しません。保護されていない接続を使用します。<br><br>このオプションを使用しない場合、eMBox クライアントでは SSL 接続を確立しようとします。そのため、クラスパスには JSSE ファイルが必要となり、これがない場合はエラーが返されます。詳細については、 <a href="#">564 ページの「eMBox クライアントを使用してセキュア接続を確立する」</a> を参照してください。 |
| -l ログファイル           | ログファイルの名前を指定します。   |
| -o                  | ログファイルを開いた後は、上書きします。   |
| -T タイムアウト           | サーバから応答を待つ時間 (秒) を指定します。   |
| -L 言語               | 使用できる言語を優先順にコンマ区切りで指定します。たとえば、en-US,de_DE と指定します。このオプションのデフォルトは、クライアントシステムの言語です。   |
| -t [ ツール.] タスクオプション | この接続での単一のサービスを実行します。-t に続く文字列は、有効な eMBox コマンドである必要があります。   |
| -b eMBox バッチファイル    | バッチファイルで指定した一連のサービスを実行します。バッチファイル内の eMBox コマンドは、行を分けて記述する必要があります。# で始まる行はコメントです。   |

## eMBox クライアントを使用してセキュア接続を確立する

非セキュア接続を使用している場合、ユーザ名やパスワードなどの入力したすべての情報は、クリアテキストでネットワーク上に送信されます。

SSL を使用したセキュア接続を確立するには、次の操作を実行します。

- ◆ サーバへログインする際は、コマンドで `-n` オプションを使用しないでください。このオプションは、非セキュア接続を指定するものです。セキュア接続がデフォルトの設定です。
- ◆ クラスパスに、次に示す JSSE (Java Secure Socket Extension) ファイルがあることを確認します。
  - ◆ `jsse.jar`
  - ◆ `jnet.jar`
  - ◆ `jcrt.jar`

これらのファイルがない場合、eMBox クライアントは、セキュア接続が確立できないことを示すエラーを返します。

これらのファイルや JSSE についての情報は、[Sun Web サイト \(http://java.sun.com/products/jsse\)](http://java.sun.com/products/jsse) から入手できます。

## eDirectory ポート番号を確認する

eMBoxクライアントでサーバにログインするには、ポート番号を指定する必要があります。

eDirectoryをインストールする際にポート番号を指定した場合には、その番号を使用します。

デフォルトのポート番号は、次のとおりです。

- ◆ NetWare の場合、デフォルトの非セキュアポートは 8028 で、セキュアポートは 8009 です。
- ◆ その他のプラットフォームの場合、デフォルトの非セキュアポートは 8028 で、セキュアポートは 8010 です。

次に示すセクションには、eDirectory に割り当てられたポートを確認するための、その他のヒントがあります。

- ◆ [564 ページの「Windows の場合」](#)
- ◆ [565 ページの「NetWare の場合」](#)
- ◆ [565 ページの「Linux および UNIX の場合」](#)

### Windows の場合

- 1 [スタート] > [設定] > [コントロールパネル] の順にクリックします。
- 2 Novell eDirectory サービスアイコンをダブルクリックしてから、[トランスポート] タブをクリックします。
- 3 セキュアポート、または非セキュアポートを確認します。
  - ◆ 非セキュアポートを確認するには、HTTP の横のプラス記号をクリックします。
  - ◆ セキュアポートを確認するには、HTTPS の横のプラス記号をクリックします。[Bound Transports ( バインドされたトランスポート )] の横のプラス記号をクリックして、ポート番号を確認します。



## NetWare の場合

サーバオブジェクトのネットワークアドレスプロパティに、ポートが表示されます。

サーバオブジェクトのネットワークアドレスプロパティは、次のツールで確認できます。

- ◆ **iManager** で、[eDirectory 管理] > [オブジェクトの変更] の順にクリックしてサーバオブジェクトを見つけ、[一般] タブのドロップダウンリストでネットワークアドレスを参照します。
- ◆ **ConsoleOne**® で、サーバオブジェクトを右クリックするかまたはサーバオブジェクトを選択した状態で [オブジェクト] > [プロパティ] の順にクリックし、ネットワークアドレスのドロップダウンリストを参照します。

始めが **http:** または **https:** で、終わりが **/portal** のネットワークアドレスを探します。これらのアドレスが、**eMBox** ツールが使用する非セキュアポートおよびセキュアポートです。

ポート番号の確認方法を次に示します。

- ◆ ネットワークアドレス内にポート番号が表示されている場合、その番号が割り当てられたポート番号です。

たとえば、**http://137.65.188.1:8028/portal** の場合、ポート **8028** が **eMBox** ツールで使用されています。

- ◆ サーバの **IP** アドレスだけで、ポート番号が表示されていない場合、デフォルトのポート番号が使用されています。

たとえば、**https://137.65.188.1/portal** の場合、IP アドレスの後にはポート番号が表示されていませんが、これは **eMBox** ツールでデフォルトのポート番号が使用されていることを示しています。デフォルトのポート番号は、**NetWare** では **8009**、それ以外のプラットフォームでは **8010** です。

## Linux および UNIX の場合

次のコマンドを使用して、ポートを表示できます。

```
ndsconfig get | grep http
```

**http.server.interface**、その次にポート番号という表現で記述された行を探します。

また、[565 ページの「NetWare の場合」](#) で説明している方法を使用し、**iManager** または **ConsoleOne** によりポート番号を確認することもできます。

## eMBox ログの記録の使用

eMBox ログの記録はインフラストラクチャモジュールで、DSBackup、DSMerge、DSRepairなどの、すべての eMTool (eDirectory Management Tool) のイベントを記録します。このリリースで提供されているログファイルは1つだけです。このログファイルに、すべての eMTool の操作が記録されます。

eMBox ログの記録は、クライアントログサービスとは異なります。クライアントログサービスは、eMBox クライアントを実行する際に、ログファイルを指定することで提供されるものです(たとえば、eMBox クライアントコマンドで `-l mylogfile.txt` と指定する場合、または iManager でログファイル名として `mylogfile.txt` を入力する場合です)。現在、eMBox ログの記録は eMBox が実行するタスクに対するすべてのサーバメッセージを記録し、その内容は詳細なものです。これに対して、クライアントログサービスではクライアントメッセージおよびクライアントに送信されたメッセージが記録され、進捗状況の概要がレポートされます。

ログの記録は非同期で実行され、デフォルトではすべての操作が記録されます。

このリリースの eMBox ログの記録には、次の機能があります。

- ◆ ログファイルの名前と場所を変更できます。  
デフォルトでは、ログファイルは eDirectory がインストールされたディレクトリ内の `embox¥log` ディレクトリに作成されます。
- ◆ 最大ファイルサイズが変更できます。変更後、ログファイルはリセットされます。  
最大ファイルサイズは 8MB です。
- ◆ ログモードを変更できます。  
すべての新しいメッセージをログファイルに追加するか、または既存のログファイルを上書きするかを選択できます。デフォルトでは、追加のオプションが指定されています。
- ◆ ログの記録を開始または停止できます。  
デフォルトでは、eMBox が起動するとログの記録は開始モードになります。停止モードの間は、メッセージは記録されません。
- ◆ ログファイルの内容をリセットできます。
- ◆ クライアントコンピュータからログファイルを読み込むことができます。

このセクションでは、次のトピックについて説明します。


- ◆ [567 ページの「eMBox ログの記録コマンドラインクライアントを使用する」](#)
- ◆ [567 ページの「Novell iManager で eMBox ログの記録機能を使用する」](#)

## eMBox ログの記録コマンドラインクライアントを使用する

次の表に、eMBox ログの記録コマンドラインクライアントのオプションを示します。

| オプション  | 説明   |
|--|--|
| logstart   | eMBox ログの記録を開始します。   |
| logstop  | eMBox ログの記録を停止します。   |
| readlog  | 現在のログファイルを表示します。   |
| getlogstate  | 現在の eMBox ログの記録の状態 ( 開始または停止 ) を表示します。   |
| getloginfo   | eMBox ログファイルの名前、ログモード ( 追加または上書き )、最大サイズと現在のサイズを表示します。   |
| setloginfo [-f <i>ファイル名</i> ] [-s <i>キロバイト単位のサイズ</i> ] [-a   -o] | 次のパラメータを使用して、eMBox ログファイルの名前、サイズ、ログモード ( 追加または上書き ) を設定します。 <ul style="list-style-type: none"><li>◆ -f <i>ファイル名</i><br/>eMBox ログファイルの名前を設定します。</li><li>◆ -s <i>KB 単位のサイズ</i><br/>ログファイルの最大サイズを設定します。</li><li>◆ -a<br/>新しいログメッセージを現在のログメッセージに追加します。</li><li>◆ -o<br/>ログファイルを上書きします。</li></ul> |
| emptylog   | サーバログファイルの内容をクリアします。   |

## Novell iManager で eMBox ログの記録機能を使用する

- 1 Novell iManager で、[役割およびタスク] ボタン  をクリックします。
- 2 [eDirectory の保守] ユーティリティ > [ログファイル] の順にクリックします。
- 3 ログファイル操作を実行するサーバを指定してから、[次へ] をクリックします。
- 4 サーバへの認証を行ってから、[次へ] をクリックします。
- 5 実行するログファイル操作を選択します。  
詳細については、[ヘルプ] をクリックしてください



# A

## NMAS の注意事項

この付録では、次のトピックについて説明します。

- 569 ページの「独立したパーティションとしてのセキュリティコンテナの設定」
- 569 ページの「複数のセキュリティコンテナを持つツリーのマージ」

### 独立したパーティションとしてのセキュリティコンテナの設定

NMAS™ (Novell® Modular Authentication Services) は、Novell eDirectory™ ツリー全体に適用されるポリシーに依存しています。eDirectory ツリーは、実際にはセキュリティドメインとして機能します。セキュリティポリシーは、ツリー内のすべてのサーバで使用できる必要があります。

NMAS には、NetWare® 5.1 以降の eDirectory ツリーの [Root] から作成された、セキュリティコンテナ内の認証ポリシーとログインメソッドの設定データが格納されています。この情報は、NMAS を使用可能なすべてのサーバで読み込みアクセスできる必要があります。セキュリティコンテナの目的は、ログイン、認証、キー管理などのセキュリティプロパティに関するグローバルポリシーを保持することです。

NMAS により、独立したパーティションとしてセキュリティコンテナを作成し、作成したコンテナを広い範囲で複製することを推奨します。このパーティションは、ツリー内の信頼性の高い複数のサーバでのみ、読み書き可能なパーティションとして複製することをお勧めします。

**注:** セキュリティコンテナはグローバルポリシーを格納しており、サーバでは eDirectory ツリーに指定したセキュリティポリシー全般が変更される可能性があるため、書き込み可能なレプリカを配置するサーバを選択する場合には注意が必要です。NMAS を使用してユーザがログインするには、ユーザオブジェクトのレプリカが NMAS サーバ上に存在する必要があります。

### 複数のセキュリティコンテナを持つツリーのマージ

一方のツリーまたは両方のツリーにセキュリティコンテナがインストールされている eDirectory ツリーをマージする場合、特に注意が必要です。この手順は時間を要する複雑な作業になる可能性があるため、本当に実行する必要があるかどうか確認してください。

**重要:** この説明では、Novell Certificate Server™ 2.21 以前、Novell Single Sign-on 2.x、および NMAS 2.x のツリーを対象としています。

複数のセキュリティコンテナを持つツリーをマージするには次を実行します。

- 1 iManager で、マージするツリーを指定します。
- 2 ソースツリーにするツリーと、ターゲットツリーにするツリーを指定します。  
ソースツリーおよびターゲットツリーについて、次のセキュリティ上の配慮事項に注意してください。
  - ◆ ソースツリーの組織の認証局によって署名された証明書は削除すること。
  - ◆ ソースツリーの組織の認証局は削除すること。
  - ◆ ソースツリー上の Novell SecretStore<sup>®</sup> に保存されたユーザのシークレットは削除すること。
  - ◆ ソースツリー内のすべての NMAS ログインメソッドを削除し、ターゲットツリーに再インストールすること。
  - ◆ ツリーをマージする際に、ソースツリー内に存在したすべての NMAS ユーザを再登録すること。
  - ◆ ソースツリー内に存在したすべてのユーザおよびサーバに、ツリーをマージする際に新しい証明書を作成すること。
  - ◆ ソースツリー内に存在したすべてのユーザのシークレットを SecretStore に再インストールすること。

ソースツリーおよびターゲットツリーの両方が Security というコンテナをツリーのルート直下に保持していない場合、またはツリーのうち一方だけが Security コンテナを保持している場合、これ以上の処置は不要です。その他の場合には、このセクションの残りの手順を続けます。

## ツリーのマージ前に実行する製品固有の操作

このセクションでは、次の情報について説明します。

- ◆ [570 ページの「Novell Certificate Server」](#)
- ◆ [572 ページの「Novell Single Sign-On」](#)
- ◆ [572 ページの「NMAS」](#)
- ◆ [573 ページの「Novell セキュリティドメインインフラストラクチャ」](#)
- ◆ [573 ページの「その他のセキュリティ固有の操作」](#)

### Novell Certificate Server

Novell Certificate Server (PKIS (Public Key Infrastructure Services) の後継バージョン) がソースツリー内のサーバのいずれかにインストールされている場合、次の手順を実行する必要があります。

注：製品の使用状況によっては、指定されたオブジェクトと項目が存在しない可能性があります。次の手順で指定されたオブジェクトや項目がソースツリーに存在しない場合には、手順を省略できます。

- 1 ソースツリー内のルート認証局証明書は、ターゲットツリーにインストールする必要があります。

ルート認証局証明書は、ルート認証局コンテナに含まれる、ルート認証局オブジェクトに格納されています。ルート認証局コンテナはツリー内の任意の場所に作成できます。ただし、セキュリティコンテナ内のルート認証局コンテナに存在するルート認証局証明書は、ソースツリーからターゲットツリーに手動で移動する必要があります。

- 2** ターゲットツリーにルート認証局証明書をインストールします。
  - 2a** ソースツリーのセキュリティコンテナでルート認証局を選択します。
  - 2b** ソースツリーで使用されている正確な名前 (手順 2a) で、ルート認証局コンテナをターゲットツリーのセキュリティコンテナに作成します。
  - 2c** ソースツリーで、選択したルート認証局コンテナのルート認証局オブジェクトを開き、証明書をエクスポートします。

**重要:** 次の手順で使用するため、選択した場所とファイル名を記憶しておきます。
  - 2d** ターゲットツリーで、手順 2b で作成したコンテナのルート認証局オブジェクトを作成します。ソースツリーと同じ名前を指定し、証明書を求められたら、手順 2c で作成したファイルを指定します。
  - 2e** ソースツリーのルート認証局オブジェクトを削除します。
  - 2f** 選択したルート認証局コンテナ内のすべてのルート認証局オブジェクトがターゲットツリーにインストールされるまで、手順 2c から手順 2e を繰り返します。
  - 2g** ソースツリーのルート認証局コンテナを削除します。
  - 2h** すべてのルート認証局コンテナがソースツリー内で削除されるまで、手順 2a から手順 2f を繰り返します。
- 3** ソースツリーの組織の認証局を削除します。

組織の認証局オブジェクトは、セキュリティコンテナ内に存在します。

**重要:** ソースツリーの組織の認証局によって署名された証明書は、この手順以降は使用できません。これには、ソースツリーの組織の認証局によって署名された、サーバ証明書とユーザ証明書も含まれます。
- 4** ソースツリーの組織の認証局によって署名された証明書を持つ、ソースツリー内の暗号化キーオブジェクト (KMO) をすべて削除します。

他の組織の認証局によって署名された証明書を持つ、ソースツリー内の暗号化キーオブジェクトは引き続き有効で、削除する必要はありません。

暗号化オブジェクトに署名している CA の識別情報がわからない場合は、暗号化オブジェクトのプロパティページにある [証明書] タブの [ルート認証局証明書] セクションを参照します。
- 5** ソースツリーの組織の認証局によって署名された、ソースツリー内のユーザ証明書をすべて削除します。

ソースツリー内のユーザがすでに証明書とプライベートキーをエクスポートしている場合、エクスポートされた各証明書とキーは引き続き使用できます。手順 3 を実行した後では、eDirectory 内に残っているプライベートキーと証明書は使用できません。

証明書を持つユーザごとに、ユーザオブジェクトのプロパティを開きます。[セキュリティ] タブの [証明書] セクションの下に、そのユーザのすべての証明書を示すテーブルが表示されます。発行者として組織の認証局が設定されている証明書はすべて削除してください。

ソースツリーの組織の認証局のホストとなっているサーバに、Novell Certificate Server 2.0 以降がインストールされている場合にのみ、ユーザ証明書はソースツリーに存在します。

## Novell Single Sign-On

Novell Single Sign-on がソースツリー内のサーバのいずれかにインストールされている場合、ソースツリーのユーザ用 Novell Single Sign-On シークレットをすべて削除する必要があります。

ソースツリーで Novell Single Sign-on を使用するすべてのユーザについて、ユーザオブジェクトのプロパティを開きます。[セキュリティ] タブの [SecretStore] セクションの下に、そのユーザのすべてのシークレットが表示されます。表示されたシークレットをすべて削除します。

**注:** 製品の使用状況によっては、指定されたオブジェクトと項目が存在しない可能性があります。指定されたオブジェクトや項目が存在しない場合には、この手順を省略できます。

## NMAS

NMAS がソースツリー内のサーバにインストールされている場合、次の手順を実行する必要があります。

**注:** 製品の使用状況によっては、指定されたオブジェクトと項目が存在しない可能性があります。指定されたオブジェクトや項目が存在しない場合には、手順を省略できます。

- 1** ターゲットツリーに、ソースツリーに存在してターゲットツリーには存在しない、NMAS ログインメソッドをインストールします。

必要なすべてのクライアントとサーバのログインコンポーネントをターゲットツリーに適切にインストールするには、Novell のオリジナルソースやベンダー提供のソースを使用して、すべて新しいログインメソッドをインストールすることを推奨します。

メソッドは既存のサーバファイルから再インストールできますが、通常、Novell のパッケージやベンダー提供のパッケージを使用してクリーンインストールを行う方が簡単で確実です。

- 2** ソースツリーで以前に確立されたログインシーケンスをターゲットツリーで使用できるようにするには、対象のログインシーケンスを移行します。
  - 2a** ConsoleOne で、ソースツリーのセキュリティコンテナを選択します。
  - 2b** ログインポリシーオブジェクトを右クリックし、[プロパティ] をクリックします。
  - 2c** [定義済みログインシーケンス] ドロップダウンリストに表示されたログインシーケンスごとに、使用するログインメソッド (右側のウィンドウに表示) をメモします。
  - 2d** ターゲットツリー内のセキュリティコンテナを選択し、手順 2c でメモしたログインメソッドと同じものを使用して、ログインシーケンスを複製します。
  - 2e** 手順が終了したら、[OK] をクリックします。
- 3** ソースツリーの NMAS ログインセキュリティ属性を削除します。
  - 3a** ソースツリーのセキュリティコンテナで、ログインポリシーオブジェクトを削除します。
  - 3b** ソースツリーの許可されたログインメソッドコンテナで、ログインポリシーオブジェクトを削除します。
  - 3c** ソースツリーの許可されたログインメソッドコンテナを削除します。
  - 3d** ソースツリーの許可されたポストログインメソッドコンテナで、ログインポリシーオブジェクトを削除します。
  - 3e** ソースツリーの許可されたポストログインメソッドコンテナを削除します。



## Novell セキュリティドメインインフラストラクチャ

Novell Certificate Server 2.x 以降、Novell Single Sign-on、NMAS、NetWare 5.1 以降、または eDirectory 8.5 以降がソースツリー内のサーバのいずれかにインストールされている場合、Novell セキュリティドメインインフラストラクチャ (SDI) がインストールされます。SDI がインストールされている場合、次の手順を実行します。

**注:** 製品の使用状況によっては、指定されたオブジェクトと項目が存在しない可能性があります。指定されたオブジェクトや項目が存在しない場合には、手順を省略できます。

- 1 W0 オブジェクトとソースツリーの KAP コンテナを削除します。  
KAP コンテナは、セキュリティコンテナ内に存在します。W0 オブジェクトは、KAP コンテナ内に存在します。
- 2 ソースツリー内のすべてのサーバで、`sys:¥system¥nici¥nicisdi.key` ファイルを削除し、セキュリティドメインインフラストラクチャ (SDI) キーを削除します。  
**重要:** ソースツリー内のすべてのサーバで、このファイルを削除したことを確認します。

### その他のセキュリティ固有の操作

ソースツリー内にセキュリティコンテナが残っている場合、ツリーをマージする前に、セキュリティコンテナを削除します。

### ツリーのマージを実行する

ndsmerge ユーティリティを使用して、eDirectory ツリーをマージします。詳細については、[225 ページの第 8 章「Novell eDirectory ツリーのマージ」](#) および [575 ページの付録 B「Novell eDirectory の Linux および UNIX 用コマンドとその使用法」](#) を参照してください。

### ツリーのマージ後に実行する製品固有の操作

このセクションでは、次の情報について説明します。

- ◆ [573 ページの「Novell セキュリティドメインインフラストラクチャ」](#)
- ◆ [574 ページの「Novell Certificate Server」](#)
- ◆ [574 ページの「Novell Single Sign-On」](#)
- ◆ [574 ページの「NMAS」](#)

## Novell セキュリティドメインインフラストラクチャ

W0 オブジェクトがマージ前にターゲットツリーに存在していた場合、ターゲットツリー内に存在していたサーバが使用していたセキュリティドメインインフラストラクチャ (SDI) キーを、ソースツリー内に存在していたサーバにインストールする必要があります。

この手順を実行する一番簡単な方法は、SDI キー (`sys:¥system¥nici¥nicisdi.key` ファイル) を保持していたソースツリー内のすべてのサーバに、Novell Certificate Server 2.52 以降をインストールすることです。Novell Certificate Server がすでにサーバにインストールされている場合でも、この手順を実行する必要があります。

マージ前に、ターゲットツリーに W0 オブジェクトが存在せず、ソースツリー内には存在していた場合は、マージ後のツリーに SDI を再インストールする必要があります。

この手順を実行する一番簡単な方法は、マージ後のツリー内のサーバに Novell Certificate Server 2.52 以降をインストールすることです。Novell Certificate Server は、SDI キー (sys:¥system¥nici¥nicisdi.key ファイル) を保持していたサーバにインストールする必要があります。また、作成されたツリー内の他のサーバにもインストールできます。

Novell Certificate Server のインストールの詳細については、『[Novell Certificate Server 管理ガイド](http://www.novell.com/documentation/beta/crt30/index.html)』(<http://www.novell.com/documentation/beta/crt30/index.html>) を参照してください。

## Novell Certificate Server

Novell Certificate Server を使用している場合、ツリーのマージ後に、ソースツリー内に存在していたサーバとユーザに必要なに応じて証明書を再発行します。

ユーザオブジェクトを含むパーティションのレプリカを保持していたすべてのサーバに、Novell Certificate Server 2.52 以降をインストールすることを推奨します。

サーバに証明書を発行するには、Novell Certificate Server 2.52 がインストールされている必要があります。

Novell Certificate Server 2.52 以降が、組織の認証局のホストとなっているサーバにインストールされている必要があります。詳細については、『[Novell Certificate Server 管理ガイド](http://www.novell.com/documentation/beta/crt30/index.html)』(<http://www.novell.com/documentation/beta/crt30/index.html>) を参照してください。

## Novell Single Sign-On

Novell Single Sign-on を使用している場合、ツリーのマージ後に、ソースツリー内に存在していたユーザの SecretStore シークレットを必要なに応じて再作成する必要があります。

## NMAS

NMAS を使用している場合、ツリーのマージ後に、ソースツリー内に存在していた NMAS ユーザを必要なに応じて再登録する必要があります。

詳細については、『[Novell Modular Authentication Service 管理ガイド](http://www.novell.com/documentation/beta/nmas30/index.html)』(<http://www.novell.com/documentation/beta/nmas30/index.html>) を参照してください。

# B

## Novell eDirectory の Linux および UNIX 用コマンドとその使用方法

この章では、Linux、Solaris、AIX および HP-UX で使用される Novell® eDirectory™ 8.8 のユーティリティおよびその使用方法について説明します。

- ◆ [575 ページの「一般ユーティリティ」](#)
- ◆ [579 ページの「LDAP 固有のコマンド」](#)

### 一般ユーティリティ

このセクションでは、Linux および UNIX での eDirectory ユーティリティとその使用方法について説明します。

注: ユーティリティの使用法の詳細については、ユーティリティのマニュアルページを参照してください。

| コマンド        | 説明  | 使用方法  |
|-------------|---|---|
| nds-install | Novell eDirectory コンポーネントをインストールするユーティリティです | nds-install [-c コンポーネント 1 [-c コンポーネント 2]...] [-h] [--help] [-i] [-j] [-u] |

| コマンド      | 説明                             | 使用法  |
|-----------|--------------------------------|--|
| ndsconfig | Novell eDirectory を環境設定します     | <pre>ndsconfig new [-m &lt;モジュール名&gt;] [-i] [-S &lt;サーバ名&gt;] [-t &lt;ツリー名&gt;] [-n &lt;サーバコンテキ スト&gt;] [-d &lt;DIB のパス&gt;] [-L &lt;LDAP ポート&gt;] [-l &lt;SSL ポート&gt;] [-o HTTP ポート] [-O HTTPS ポート] [-e] -a &lt;管理者 FDN&gt; [-b &lt;バインドする ポート&gt;] [-B &lt;インタフェース 1@ポート 1, インタ フェース 2@ポート 2,..&gt;] [-D &lt;任意の場所&gt;] [--config-file &lt;環境設定ファイル&gt;]  ndsconfig def [-m &lt;モジュール名&gt;] [-i] [-S &lt;サーバ名&gt;] [-t &lt;ツリー名&gt;] [-n &lt;サーバコンテキ スト&gt;] [-d &lt;DIB のパス&gt;] [-L &lt;LDAP ポート&gt;] [-l &lt;SSL ポート&gt;] [-o HTTP ポート] [-O HTTPS ポート] [-e] -a &lt;管理者 FDN&gt; [-D &lt;任意の場所&gt;] [--config-file &lt;環境設定ファイル&gt;]  ndsconfig add [-m &lt;モジュール名&gt;] [-s &lt;サーバ 名&gt;] [-t &lt;ツリー名&gt;] [-p &lt;IP アドレス:ポート&gt;] [-n &lt;サーバコンテキスト&gt;] [-d &lt;DIB のパス&gt;] [-L &lt;LDAP ポート&gt;] [-l &lt;SSL ポート&gt;] [-o HTTP ポート] [-O HTTPS ポート] [-e] -a &lt;管理者 FDN&gt; [-b &lt;バ インドするポート&gt;] [-B &lt;インタフェース 1@ポート 1, インタフェース 2@ポート 2,..&gt;] [-D &lt;任意の場所&gt;] [-E] [--config-file &lt;環境設定ファイル&gt;]  ndsconfig rm [-a &lt;管理者 FDN&gt;] [-b &lt;バインドす るポート&gt;] [--config-file &lt;環境設定ファイル&gt;]  ndsconfig upgrade [-a &lt;管理者 FDN&gt;] [-j] [--config-file &lt;環境設定ファイル&gt;]  ndsconfig {set &lt;値リスト&gt;   get [&lt;パラメータリ スト&gt;]   get help [&lt;パラメータリスト&gt;]}</pre> |
| ndscheck  | ツリーの状態をチェックするユーティリティです         | <pre>ndscheck [-h &lt;ホスト名:ポート&gt;] [-a &lt;管理者 FDN&gt;] [-F &lt;ログファイル名&gt;] [--config-file &lt;環境設定ファイルの名前とパス&gt;] --version</pre>   |
| ndsmanage | eDirectory のインスタンスを表示するユーティリティ | <pre>ndsmanage [-a]  ndsmanage [&lt;ユーザ名&gt;]</pre>  |

| コマンド       | 説明   | 使用法   |
|------------|--|---|
| ndsbackup  | eDirectory オブジェクトのアーカイブを作成し、eDirectory オブジェクトを追加または抽出します | <pre>ndsbackup c [fevwXR] [NDS バックアップファイル] [除外ファイル] [レプリカサーバ名] [-a 管理ユーザ] [-I 包含ファイル] [-E パスワード] [--config-file &lt;環境設定ファイルのパス&gt;]... [eDirectoryobject]  ndsbackup r [fevwXR] [NDS バックアップファイル] [除外ファイル] [レプリカサーバ名] [-a 管理ユーザ] [-I 包含ファイル] [-E パスワード] [--config-file &lt;環境設定ファイルのパス&gt;]... [eDirectoryobject]  ndsbackup t [fevXR] [NDS バックアップファイル] [除外ファイル] [レプリカサーバ名] [-a 管理ユーザ] [-I 包含ファイル] [-E パスワード] [--config-file &lt;環境設定ファイルのパス&gt;]... [eDirectoryobject]  ndsbackup x [fevwXR] [NDS バックアップファイル] [除外ファイル] [レプリカサーバ名] [-a 管理ユーザ] [-I 包含ファイル] [-E パスワード] [--config-file &lt;環境設定ファイルのパス&gt;]... [eDirectoryobject]  ndsbackup s [evXR] [除外ファイル] [レプリカサーバ名] [-a 管理ユーザ] [-I 包含ファイル] [-E パスワード] [--config-file &lt;環境設定ファイルのパス&gt;]... [eDirectoryobject]  ndsbackup --バージョン</pre> |
| ndslogin   | Novell eDirectory の認証を確認するための診断ユーティリティです                 | <pre>ndslogin [-t &lt;ツリー名&gt;] [-h ホスト名[:ポート]] [-p パスワード] [-s] &lt;ユーザ FDN&gt; [--config-file &lt;環境設定ファイルのパス&gt;]</pre>   |
| ndsd       | NDS <sup>®</sup> デーモンです                                  | <pre>/opt/novell/eDirectory/sbin/ndsd [--config-file 環境設定ファイル]</pre> <p><b>注：</b> Solaris を再起動する前に ndsd を停止する必要があります。「<b>/etc/init.d/ndsd stop</b>」と入力します。ルート以外または任意の場所にインストールした場合は、ndsmanage を使用してインスタンスを停止してください。</p>   |
| ndsmonitor | HTTP を使用して、Novell eDirectory ツリー内のサーバの監視および診断を実行します      | <pre>/opt/novell/eDirectory/bin/ndsmonitor [-l [-d &lt;ndsmonitor 環境設定ファイルのパス&gt;]   u] [-h &lt;ローカルインタフェース:ポート&gt;] [--config-file &lt;環境設定ファイルのパス&gt;]</pre>  |
| ndsmerge   | 2 つの Novell eDirectory ツリーをマージするユーティリティです                | <pre>ndsmerge [-m ターゲット管理者 ソース管理者 [ターゲットコンテナ]] [-c] [-t] [-r ターゲットツリー ソース管理者] [-h &lt;ローカルインタフェース:ポート&gt;] [--config-file &lt;環境設定ファイルのパス&gt;]</pre>  |

| コマンド          | 説明  | 使用法  |
|---------------|---|--|
| ndsrepair     | レコード、スキーマ、バインダリオブジェクト、および外部参照など、Novell eDirectory データベースの問題を修復および修正するためのユーティリティです | ndsrepair {-U  -E  -C  -P [Ad]  -S [Ad]  -N  -T  -J <エントリ ID>} [-A <yes/no>] [-O <yes/no>] [-F ファイル名] [-h <ローカルインタフェース:ポート>] [--config-file <環境設定ファイルのパス>]<br><br>ndsrepair -R [-l <yes/no>] [-u <yes/no>] [-m <yes/no>] [-i <yes/no>] [-f <yes/no>] [-d <yes/no>] [-t <yes/no>] [-o <yes/no>] [-r <yes/no>] [-v <yes/no>] [-c <yes/no>] [-A <yes/no>] [-O <yes/no>] [-F ファイル名] [-h <ローカルインタフェース>] [--config-file <環境設定ファイルのパス>] |
| ndssch        | Novell eDirectory スキーマ拡張ユーティリティです   | ndssch [-h <ホスト名>[:<ポート>]] [-t <ツリー名>] <管理者 FDN> <スキーマファイル> ...<br><br>ndssch [-h <ホスト名>[:<ポート>]] [-t <ツリー名>] [-d <管理者 FDN> <スキーマファイル>] [スキーマの説明] ...  |
| ndssnmp       | Novell eDirectory の SNMP サービスモジュールです  | /opt/novell/eDirectory/bin/ndssnmp   |
| ndssnmpconfig | SNMP トラップ環境設定ユーティリティです  | ndssnmpconfig -h [ホスト名[:ポート]] -p <パスワード> -a <ユーザ FDN> -c <コマンド>  |
| ndssnmpsa     | eDirectory SNMP サブエージェントデモンです   | /opt/novell/eDirectory/bin/ndssnmpsa   |
| ndsstat       | サーバ情報を表示するユーティリティです   | ndsstat [-h ホスト名[:ポート]] { -r -s } [--config-file <環境設定ファイルのパス>]  |
| ndstrace      | サーバのデバッグメッセージを表示するユーティリティです   | ndstrace [-l -u -c "コマンド 1;....." - パージョン] [-h <ローカルインタフェース:ポート>] [--config-file <環境設定ファイルのパス>]  |
| nds-uninstall | Novell eDirectory をアンインストールするユーティリティです  | nds-uninstall -c <コンポーネント 1> [[-c <コンポーネント 2>]...] [-h]  |
| nldap         | LDAP Services for eDirectory デーモンです   | /opt/novell/eDirectory/sbin/nldap  |
| nmasinst      | NMAS™ 環境設定ユーティリティです   | nmasinst -i <管理者 FDN> <ツリー名> [-h <ホスト名>[:ポート]]<br><br>nmasinst -addmethod <管理者 FDN> <ツリー名> <config.txt ファイル> [-h <ホスト名>[:ポート]]   |
| npki          | Novell パブリックキーインフラストラクチャサービス  | /opt/novell/eDirectory/sbin/npki   |

# LDAP 固有のコマンド

| コマンド                  | 説明  | 使用法  |
|-----------------------|---|--|
| ldapconfig            | LDAP サーバおよび LDAP グループオブジェクトを設定するユーティリティです | <pre>ldapconfig get [...]   set &lt;属性値リスト&gt; [-t ツリー名   -p ホスト名 [:ポート]]   --config-file &lt;環境設定ファイル&gt;] [-w パスワード] [-a &lt;ユーザ FDN&gt;] [-f]  ldapconfig [-t ツリー名   -p ホスト名 [:ポート]] [-w パスワード   --config-file &lt;環境設定ファイル&gt;] [-a &lt;ユーザ FDN&gt;] [-V] [-R] [-H] [-f] -v &lt;属性&gt;, &lt;属性 2&gt;...</pre> <pre>ldapconfig [-t ツリー名   -p ホスト名 [:ポート]]   --config-file &lt;環境設定ファイル&gt;] [-w パスワード] [-a &lt;管理者 FDN&gt;] [-V] [-R] [-H] [-f] -s &lt;属性&gt;=&lt;値&gt;,&lt;値&gt;,...</pre> |
| ldapadd<br>ldapmodify | LDAP サーバからエントリを追加または変更します                 | <pre>ldapmodify [-a] [-c] [-C] [-M] [-P] [-r] [-n] [-v] [-F] [-l 制限] [-M[M]] [-d デバッグレベル] [-e キーファイル名] [-D バインド DN] [[-W] [-w パスワード]] [-h LDAP ホスト] [-p LDAP ポート] [-P バージョン] [-Z[Z]] [-f ファイル]  ldapadd [-c] [-C] [-l] [-M] [-P] [-r] [-n] [-v] [-F] [-l 制限] [-M[M]] [-d デバッグレベル] [-e キーファイル名] [-D バインド DN] [[-W]  [-w パスワード]] [-h LDAP ホスト] [-p LDAP ポート] [-P バージョン] [-Z[Z]] [-f ファイル]</pre>  |
| ldapdelete            | LDAP サーバからエントリを削除します                      | <pre>ldapdelete [-n] [-v] [-c] [-r] [-l] [-C] [-M] [-d デバッグレベル] [-e キーファイル名] [-f ファイル] [-D バインド DN] [[-W] [-w パスワード]] [-h LDAP ホスト] [-p LDAP ポート] [-Z[Z]] [dn]...</pre>  |
| ldapmodrdn            | LDAP のエントリの相対識別名 (RDN) 変更ツールです            | <pre>ldapmodrdn [-r] [-n] [-v] [-c] [-C] [-l] [-M] [-s 新規スーパーリア] [-d デバッグレベル] [-e キー ファイル名] [-D バインド DN] [[-W] [-w パスワード]] [-h LDAP ホスト] [-p LDAP ポート] [-Z[Z]] [-f ファイル] [dn 新規 RDN]</pre>   |
| ldapsearch            | LDAP の検索ツールです                             | <pre>ldapsearch [-n] [-u] [-v] [-t] [-A] [-T] [-C] [-V] [-M] [-P] [-L] [-d デバッグレベル] [-e キー ファイル名] [-f ファイル] [-D バインド DN] [[-W]  [-w バインドパスワード]] [-h LDAP ホスト] [-p LDAP ポート] [-b 検索基点] [-s スコープ] [-a 逆 参照] [-l 時間制限] [-z サイズ制限] [-Z[Z]] filter [属性....]</pre>   |

| コマンド     | 説明  | 使用法  |
|----------|---|--|
| ndsindex | Novell eDirectory データベースインデックスの作成、リスト表示、一時停止、再開、または削除に使用するユーティリティです | <pre>ndsindex list [-h &lt;ホスト名&gt;] [-p &lt;ポート&gt;] -D &lt;バインド DN&gt; -W [-w &lt;パスワード&gt;] [-l 制限] -s &lt;eDirectory サーバの DN&gt; [-Z[Z]] [&lt;インデックス名 1&gt;, &lt;インデックス名 2&gt;.....]  ndsindex add [-h &lt;ホスト名&gt;] [-p &lt;ポート&gt;] -D &lt;バインド DN&gt; -W [-w &lt;パスワード&gt;] [-l 制限] -s &lt;eDirectory サーバの DN&gt; [-Z[Z]] &lt;インデックス定義 1&gt;  [&lt;インデックス定義 2&gt;.....]  ndsindex delete [-h &lt;ホスト名&gt;] [-p &lt;ポート&gt;] -D &lt;バインド DN&gt; -W [-w &lt;パスワード&gt;] [-l 制限] -s &lt;eDirectory サーバの DN&gt; [-Z[Z]] &lt;インデックス名 1&gt;  [&lt;インデックス名 2&gt;.....]  ndsindex resume [-h &lt;ホスト名&gt;] [-p &lt;ポート&gt;] -D &lt;バインド DN&gt; -W [-w &lt;パスワード&gt;] [-l 制限] -s &lt;eDirectory サーバの DN&gt; [-Z[Z]] &lt;インデックス名 1&gt;  [&lt;インデックス名 2&gt;.....]  ndsindex suspend [-h &lt;ホスト名&gt;] [-p &lt;ポート&gt;] -D &lt;バインド DN&gt; -W [-w &lt;パスワード&gt;] [-l 制限] -s &lt;eDirectory サーバの DN&gt; [-Z[Z]] &lt;インデックス名 1&gt;  [&lt;インデックス名 2&gt;.....]</pre> |



# C

## OpenSLP for eDirectory の設定

この付録では、OpenSLP for Novell® eDirectory™ を Novell Client™ なしでインストールする場合の適切な設定について、ネットワーク管理者向けに説明します。

- ◆ 581 ページの「Service Location Protocol」
- ◆ 581 ページの「SLP の基本」
- ◆ 584 ページの「環境設定パラメータ」

### Service Location Protocol

OpenSLP は、IETF Service Location Protocol バージョン 2.0 標準のオープンソースの実装です。IETF Service Location Protocol バージョン 2.0 標準については、[IETF Request-For-Comments \(RFC\) 2608](http://www.ietf.org/rfc/rfc2608.txt?number=2608) (<http://www.ietf.org/rfc/rfc2608.txt?number=2608>) を参照してください。

OpenSLP ソースコードが提供するインタフェースでは、SLP v2 プロトコルの実装のほかに、プログラムで SLP 機能にアクセスする別の IETF 標準の実装があります。詳細は、[RFC 2614](http://www.ietf.org/rfc/rfc2614.txt?number=2614) (<http://www.ietf.org/rfc/rfc2614.txt?number=2614>) を参照してください。

SLP の動作の詳細を理解するためには、この 2 つのドキュメントを参照し、熟読してください。読みやすい文書ではありませんが、インターネットでの SLP の正しい設定を行うためには重要なドキュメントです。

OpenSLP プロジェクトの詳細については、[OpenSLP](http://www.OpenSLP.org) (<http://www.OpenSLP.org>) Web site and the [SourceForge](http://sourceforge.net/projects/openslp) (<http://sourceforge.net/projects/openslp>) の Web サイトを参照してください。OpenSLP の Web サイトには、環境設定に関する貴重なヒントを含んださまざまな文書があります。ただし、このガイドの作成時点では、これらのドキュメントの多くは未完成です。

### SLP の基本

Service Location Protocol では、次の 3 種類のコンポーネントが定義されています。

- ◆ ユーザエージェント (UA)
- ◆ サービスエージェント (SA)
- ◆ ディレクトリエージェント (DA)

ユーザエージェントは、クライアントがサービスを問い合わせたり、サービスがそれ自体を通知するためのプログラムインタフェースを提供します。ユーザエージェントはディレクトリエージェントに接続し、指定したスコープ内の指定したサービスクラスに登録されたサービスを問い合わせます。

サービスエージェントは、SLP で登録されたローカルサービスを持続的に格納し、維持する場所を提供します。サービスエージェントは主として、登録済みのローカルサービスをメモリ内データベースとして維持します。この場合、サービスはローカル SA がない限り SLP で登録できません。クライアントがサービスを検出するのは UA ライブラリ内のみですが、登録するには SA が必要です。これは主に、ディレクトリエージェントを受信して登録を維持するためには、登録済みサービスの存在を SA が定期的に表明する必要があるためです。

ディレクトリエージェントは、通知されたサービスに対して長期間持続的にキャッシュを提供し、ユーザエージェントがサービスを検索するためのアクセスポイントとなります。キャッシュ機能を提供する DA は、SA が新しいサービスを通知するのを受信し、これらの通知をキャッシュします。DA のキャッシュは短時間で完了します。ディレクトリエージェントは、期限切れのアルゴリズムを使用してエントリキャッシュを有効期限切れにします。ディレクトリエージェントが起動すると、持続的な格納領域 (通常はハードドライブ) からキャッシュを読み込み、アルゴリズムに従ってエントリを有効期限切れにします。新しい DA が起動したり、キャッシュが削除されると、DA はこの条件を検出して受信中のすべての SA に特別な通知を送信します。SA は、DA が直ちにキャッシュを作成できるようにローカルデータベースをダンプします。

ディレクトリエージェントが存在しない場合、UA は SA が応答できる一般的なマルチキャスト方式のクエリを使用し、DA がキャッシュを作成するのとはほぼ同じ方法で、要求されたサービスのリストを作成します。このクエリによって返されるサービスのリストは、DA が提供するリストと比較すると不完全かつ局所的で、特に、多くのネットワーク管理者が使用するマルチキャスト方式でのフィルタ処理では、ブロードキャストおよびマルチキャストの対象がローカルサブネットのみに制限されるためです。

つまり、指定されたスコープに対してユーザエージェントが検索するものは、すべてディレクトリエージェントに依存します。

## Novell Service Location Providers

Novell のバージョンの SLP では、強力なサービスアドバタイズ環境を提供するため、SLP 標準が一部変更されます。しかし、このために一部の拡張性を犠牲にしています。

たとえば、サービスアドバタイズのフレームワークの拡張性を改善するために、サブネット上でのブロードキャストまたはマルチキャストの packets 数が制限されます。SLP の仕様では、これを管理するために、ディレクトリエージェントのクエリに関してサービスエージェントおよびユーザエージェントに制限を加えています。必要なスコープに対応するための最初に検出されたディレクトリエージェントは、サービスエージェント (つまり結果的にローカルユーザエージェント) がそのスコープ上の将来の要求すべてに使用するエージェントとなります。

Novell SLP を実装すると、クエリ情報の検索について既知のディレクトリエージェントをすべてスキャンします。スキャンの所要時間は 300 ミリ秒とかなり長く、したがって、約 3 ~ 5 秒以内で 10 台のサーバしかスキャンできません。SLP がネットワーク上で正しく設定されている場合にはこのような検索の必要はありません。OpenSLP では、ネットワークが実際に SLP トラフィック用に設定されていると見なされます。OpenSLP の応答タイムアウト値は Novell の SLP サービスプロバイダの応答タイムアウト値よりも大きい値です。ディレクトリエージェント数は、エージェントの情報が正確で完全であるかどうかに関係なく、最初に応答するディレクトリエージェントに制限されます。

## ユーザエージェント

ユーザエージェントの物理形式は、アプリケーションにリンクされたスタティックライブラリまたはダイナミックライブラリです。ユーザエージェントにより、アプリケーションは SLP サービスに対して問い合わせることができます。

ユーザエージェントは、アルゴリズムに従って、クエリの送信先になるディレクトリエージェントのアドレスを取得します。指定したスコープの DA アドレスを取得すると、ユーザエージェントはそのスコープから応答がなくなるまで同じアドレスを使用し続けます。応答がなくなると、ユーザエージェントはそのスコープに対する別の DA アドレスを取得します。ユーザエージェントは、指定されたスコープのディレクトリエージェントのアドレスを次の方法で検索します。

1. 現在の要求上のソケットハンドルが、指定したスコープの DA に接続されているかどうかをチェックする ( 要求がマルチパート要求の場合は、要求に対してキャッシュされた接続がすでに存在している可能性があります )。
2. 指定したスコープと一致している DA の、既知のローカル DA キャッシュをチェックする。
3. 指定したスコープでローカル SA に対して DA を確認する ( その後キャッシュに新しいアドレスを追加します )。
4. 指定したスコープに一致する DA のネットワーク設定済みのアドレスを DHCP に問い合わせる ( その後キャッシュに新しいアドレスを追加します )。
5. 既知のポートで DA の検出要求をマルチキャストする ( その後キャッシュに新しいアドレスを追加します )。

スコープを指定しない場合、指定スコープは「デフォルト」になります。つまり、SLP 設定ファイルで静的に定義されたスコープがなく、クエリでスコープを指定していない場合は、使用されるスコープは「デフォルト」という単語になります。また、eDirectory の登録では eDirectory はスコープを指定しないことに注意してください。つまり、eDirectory で使用されるスコープは常に「デフォルト」というわけではありません。スコープが静的に設定されている場合、そのスコープがすべてのローカル UA 要求および SA 登録に対して、指定したスコープがない場合のデフォルトのスコープになります。

## サービスエージェント

サービスエージェントの物理形式は、ホストマシン上での個別のプロセスです。Win32 の場合は、slpd.exe がローカルマシン上のサービスとして実行されます。ユーザエージェントは、既知のポート上のループバックアドレスにメッセージを送信することによって、ローカルサービスエージェントを問い合わせます。

サービスエージェントは、潜在 DA アドレスに DA 検出要求を直接送信することにより、ディレクトリエージェントおよびそれがサポートするスコープリストを検出してキャッシュします。DA 検出要求は、次の方法で送信されます。

1. 静的に設定された DA アドレスをすべてチェックする ( その後 SA の既知の DA キャッシュに新しい DA アドレスを追加します )。
2. DHCP から DA とスコープのリストを要求する ( その後 SA の既知の DA キャッシュに新しいリストを追加します )。

3. 既知のポートで DA の検出要求をマルチキャストする (その後 SA の既知の DA キャッシュに新しいポートを追加します)。
4. DA によって定期的にブロードキャストされた DA のアドバータイズパケットを受信する (その後 SA の既知の DA キャッシュに新しいアドバータイズパケットを追加します)。

ユーザエージェントは常に最初にローカルサービスエージェントに対して問い合わせます。ローカルサービスエージェントの応答によってユーザエージェントが次の検出段階を続行するかどうか決定されるため、このことは重要な点です (DHCP のこのケースについては、[583 ページ](#)の「[ユーザエージェント](#)」の手順 3 および 4 を参照してください)。

## 環境設定パラメータ

%systemroot%/slp.conf ファイル内の各環境設定パラメータも、次のようにして DA の検出を制御します。

```
net.slp.useScopes = <コンマ区切りのスコープリスト>  
net.slp.DAAddresses = <コンマ区切りのアドレスリスト>  
net.slp.passiveDADetection = <"true" または "false">  
net.slp.activeDADetection = <"true" または "false">  
net.slp.DAActiveDiscoveryInterval = <0、1、または秒数>
```

**useScopes** オプションは、SA の通知先のスコープ、および、サービスまたはクライアントアプリケーションで作成された登録またはクエリに指定したスコープが存在しない場合に、クエリが作成されるスコープを示します。**eDirectory** は常にデフォルトのスコープに通知し、問い合わせを行うため、このリストが **eDirectory** の登録およびクエリのデフォルトのスコープのリストになります。

**DAAddresses** はコンマで区切られた IP アドレスのリストで、アドレスは 10 進数とドットで表記されます。このアドレスが他のすべてに対して優先されます。設定された DA のこのリストが登録またはクエリのスコープをサポートしない場合、検出を無効にしている限りは、SA および UA はマルチキャスト方式で DA を検出します。

**passiveDADetection** オプションのデフォルトは「TRUE」です。ディレクトリエージェントは、設定に応じて定期的にそれ自体の存在をサブネットの既知のポート上にブロードキャストします。これらのパケットは **DAAdvert** パケットと名付けられます。このオプションに「FALSE」を設定した場合、ブロードキャスト方式のすべての **DAAdvert** パケットは SA に無視されます。

**activeDADetection** オプションのデフォルトも「TRUE」です。この設定により、SA はすべての DA に対して、指示された **DAAdvert** パケットで応答するように、定期的にブロードキャスト方式で要求できます。指示されたパケットはブロードキャストではありませんが、この要求に対する応答では SA に直接送信されます。このオプションに「FALSE」を設定した場合、SA は定期的な DA の検出要求をブロードキャストしません。

**DAActiveDiscoveryInterval** オプションは **try-state** パラメータです。デフォルト値は 1 です。これは、初期化の際に、SA が DA の検出要求を 1 回送る設定であることを意味する特別な値です。このオプションに 0 を設定すると、**activeDADetection** オプションに「FALSE」を設定した場合と結果は同じです。その他の値は、検出をブロードキャストする間隔を秒数で表します。

このオプションを正しく使用すると、サービスアドバータイズに使用するネットワーク帯域幅を適切に設定できます。ただし、デフォルト設定は平均的なネットワークで拡張性を最適化するように設計されています。

# D

## Novell eDirectory が DNS を使用する際の動作について

クライアントがサーバに Novell® eDirectory™ ツリーに存在しない完全識別名 (admin.novell.novell\_inc など) の解決を要求する場合、または Linux および UNIX 用の Novell iManager や eDirectory のインストールアプリケーションなどのスタンドアロンのアプリケーションを使用している場合で、ツリー内の名前を解決するためのサーバにまだ接続していない場合は、eDirectory はサービスディスカバリプロトコルを使用して名前を解決します。サービスディスカバリプロトコルはネットワークアプリケーションのクラスで、分散コンポーネントを使用してネットワーク内の必要なサービスを検索して使用できます。

eDirectory は、従来 SAP および SLP を使用してネットワークサービスを検索し、通知してきました。DNS はディスカバリプロトコルとして eDirectory 8.7.1 に追加されました。この追加機能では、eDirectory が理解していないツリー名を問い合わせるために、コンピュータは次の順序で検出を試みます。eDirectory がツリー名を理解しない理由は、接続しているサーバがツリーのコピーを保持していないことや、スタンドアロンのアプリケーションを使用していることによります。また、コンピュータは、スタンドアロンのアプリケーションを実行しているか、Novell iManager や ConsoleOne® などの JClient アプリケーションを実行しているか、または eDirectory のディスカバリプロトコルを使用しているサーバの場合があります。

1. ドメインネームシステム (DNS)
2. SLP (Service Location Protocol)
3. SAP (Service Advertising Protocol)

DNS プロトコルを使用すると、eDirectory は、サーバ名「prod\_server4.provo.novell.novell\_inc」など、渡されたままの名前を使用し、その名前で完全な名前の解決を試みます。eDirectory は検出したコンピュータの DNS 検索リストにそれぞれの名前を追加し、そのコンピュータの DNS サーバにその名前のアドレスが存在するかどうかを調べます。たとえば、検出マシンの DNS 検索リストに「dev.novell.com」および「test.novell.com」が含まれている場合、eDirectory は prod\_server4.provo.novell.novell\_inc.dev.novell.com および prod\_server4.provo.novell.novell\_inc.test.novell.com を検索します。

その後、eDirectory は渡された名前からコンポーネントを切り離します。たとえば、「prod\_server4.provo.novell.novell\_inc」を解決する場合、eDirectory は provo.novell.novell\_inc、novell.novell\_inc、novell\_inc の順に試みます。eDirectory は、各々の異なる検索コンテキストに対して検索を行い、最終的にツリーのルート of 単一コンポーネントに検索を試みます。クライアントは接続が成功するまで各アドレスを試行します。アドレスの試行には、DNS サーバから戻されたレコードの順序を使用します。検出を試みるコンピュータが eDirectory 8.7.1 以降を実行している限り、レプリカリング内のサーバがどのコードリビジョンを実行しても問題ありません。

eDirectory ツリー名は、クライアントが名前解決のために使用する DNS ドメインの下の A、AAAA、またはサービス (SRV) リソースレコードを使用する DNS に加えることをお勧めします。A または AAAA レコードを使用する場合、eDirectory サーバはデフォルトの 524 ポートで実行する必要があります。サーバが他のポートを使用する場合は、SRV レコードを使用します。

次のリソースレコードのサンプルでは、ツリー名は「novell\_inc」で DNS 検索コンテキストは「provo.novell.com」です。

| レコード | 例  |
|------|--|
| A    | novell_inc.provo.novell.com.IN A 192.168.1.2   |
| AAAA | novell_inc.provo.novell.com.IN AAAA 4321:0:1:2:3:4:567:89ab  |
| SRV  | _ldap._tcp.novell_inc.provo.novell.com. SRV 0 0 389<br>server1.novell_inc.provo.novell.com SRV 10 0 389<br>server2.novell_inc.provo.novell.com |

冗長性を維持するため、または複数のホスト (レプリカリング内のサーバ) を A レコードに指定するためには、A レコードを 2 つ以上作成します。eDirectory は、それらすべてを検索します。A、AAAA、および SRV レコードの詳細については、[DNS リソースレコード \(http://www.dns.net/dnsrd/rr.html\)](http://www.dns.net/dnsrd/rr.html) を参照してください。

対応するパーティションルートを保持しているものに対して、DNS サーバのレコードエントリを参照する必要はありません。検出するマシンがツリーを認識しているサーバと通信でき次第、ツリー全体を参照して名前を解決できます。たとえば、DNS に「novell\_inc」を設定している場合、「novell\_inc」ルートを保持するサーバには設定する必要がありません。必要なのは「novell\_inc」ツリー内の任意のサーバを参照することだけです。これは、ツリー内でそのサーバに接続できれば、そのサーバがツリー周辺でユーザを参照するためです。

# E

## eDirectory での GSSAPI の設定

Novell® eDirectory™ の SASL-GSSAPI メカニズムを使用すると、LDAP 経由で Kerberos チケットを使用して eDirectory に対する認証を行えます。eDirectory のユーザパスワードを入力する必要はありません。Kerberos チケットは、Kerberos サーバに対する認証を行うことによって取得されます。

SASL-GSSAPI の概要については、『*Novell eDirectory 8.8 What's New Guide*』 (<http://www.novell.com/documentation/beta/edir88/index.html>) を参照してください。

注：SASL-GSSAPI メカニズムは、eDirectory 8.7.1 以降で使用できます。

次のセクションでは、GSSAPI の設定方法と、eDirectory で Kerberos を使用して実行できるさまざまなタスクについて説明し、その他の有用な情報も提供します。

- ◆ [587 ページの「前提条件」](#)
- ◆ [592 ページの「SASL-GSSAPI メソッドの設定」](#)
- ◆ [592 ページの「SASL-GSSAPI メソッドの管理」](#)
- ◆ [599 ページの「ログインシーケンスの作成」](#)
- ◆ [599 ページの「LDAP での SASL-GSSAPI の使用方法」](#)
- ◆ [599 ページの「エラーメッセージ」](#)

## 前提条件

GSSAPI を設定するには、まず次の作業を行う必要があります。

- **SASL-GSSAPI メソッド**：SASL-GSSAPI メソッドをインストールします。『*NMAS 3.0 管理ガイド*』 (<http://www.novell.com/documentation/beta/nmas30/admin/data/a49tuwk.html#a49tuwk>) の「ログインメソッドのインストール」を参照してください。

注：NetWare に SASL-GSSAPI ログインメソッドをインストールする場合は、Windows と同じ手順に従ってください。

SASL-GSSAPI がコンピュータにインストールされているかどうかを確認するには、次のように入力します。

```
ldapsearch -x -h osg-dt-srv9 -b " " -s base | grep -i sasl
```

SASL-GSSAPI がインストールされている場合、コマンドの出力は次のようになります。

```
supportedSASLMechanisms: NMAS_LOGIN
```

- **iManager 用の Kerberos プラグイン**：iManager 用の Kerberos プラグインをインストールします。詳細については、[588 ページの「iManager 用の Kerberos プラグインのインストール」](#)を参照してください。

- ❑ **KDC** : Kerberos KDC (MIT、Microsoft (Active Directory)、または Heimdal) をネットワーク上にインストールします。

Microsoft KDC (Active Directory) を使用する場合は、Kerberos ツールをインストールしておく必要があります。これらのツールは Windows に付属しており、Windows インストール CD の %support%tools%setup.exe からインストールできます。

- ❑ **時刻の同期** : このメソッドを正しく機能させるために、NMASTM クライアントコンピュータ、NMASTM サーバコンピュータ、および KDC コンピュータの時刻を同期します。ネットワーク時刻の同期の詳細については、**91 ページ**の「**ネットワーク時刻の同期**」を参照してください。
- ❑ **LDAP Libraries for C** : 最新の LDAP Libraries for C をデフォルトの場所にインストールします (Windows を除く)。詳細については、次を参照してください。 **LDAP Libraries for C** (<http://developer.novell.com/ndk/cldap.htm>)。
- ❑ **Kerberos LDAP 拡張** : Kerberos LDAP 拡張を追加します。詳細については、**590 ページ**の「**Kerberos の LDAP 拡張の追加**」を参照してください。

**重要** : Kerberos の管理で収集される Kerberos 情報では、大文字と小文字が区別されるため、大文字と小文字を正確に指定する必要があります。

## ネットワークの特性に関する前提

SASL-GSSAPI メカニズムは次の前提に基づいて動作します。

- ◆ ネットワーク上のすべてのコンピュータの時刻がある程度正確に同期されている。言い換えると、システム時刻が 5 分以上異なる 2 台のコンピュータがネットワーク上に存在しない。
- ◆ MAN 環境や WAN 環境では時刻の同期に関するこのような要件を満たすことが難しいため、SASL-GSSAPI メカニズムは主に LAN での使用を想定している。ただし、このメカニズムは LAN のみに限定されていない。
- ◆ Kerberos サーバと Kerberos 管理者を検証なしで無条件に信頼する。
- ◆ DoS (Denial-of-Service) 攻撃に対抗する手段にはならない。詳細については、**RFC 1510** (<http://www.ietf.org/rfc/rfc1510.txt?number=1510>) を参照してください。


## iManager 用の Kerberos プラグインのインストール

- 1 ブラウザを開きます。
- 2 ブラウザウィンドウのアドレスフィールドに、次の URL を入力します。

```
http://ホスト名/nps/iManager.html
```

ホスト名は、SASL-GSSAPI 用の iManager プラグインをインストールする iManager サーバのサーバ名または IP アドレスです。

**注** : 問題が発生した場合は、Tomcat および Web サーバが正しく設定されていることを確認します。詳細については、『**iManager 2.5 管理ガイド**』(<http://www.novell.com/documentation/beta/imanager25/index.html>) を参照してください。

- 3 eDirectory にログインするためのユーザ名とパスワードを指定して、[ログイン] をクリックします。
- 4 iManager ツールバーで、[設定]  をクリックします。
- 5 左側の画面で、[モジュール設定] > [モジュールパッケージのインストール] の順にクリックします。



- 6** kerberosPlugin.npm ファイルの場所を指定するか、[参照] をクリックしてファイルの場所を選択します。

このプラグインパッケージは次の場所にあります。

展開フォルダ<プラットフォーム (Linux、Solaris)>/nmas/NmasMethods/Novell/GSSAPI/plugins/ ( 展開フォルダは、edir88.zip ファイルが展開されたディレクトリです)。kerberosPlugin.npm ファイルを別の場所に移動した場合は、その場所を参照して選択してください。

- 7** [インストール] をクリックします。

このインストールには数分かかります。

**注** : Tomcat がインストールされた Windows IIS Web サーバ上で iManager を実行している場合は、モジュールパッケージのインストール中に「予期しないパーツの終了」というエラーが発生する場合があります。これは、IIS 用の Tomcat リダイレクタを通じてファイルをアップロードする際に発生する既知の問題です。モジュールパッケージのインストールを正しく実行するには、Tomcat から直接 (たとえば、ポート 8080 を使用して) iManager に接続してください。


例 : <http://hostname:8080/nps/iManager.html>

詳細については、『[iManager 2.5 管理ガイド](http://www.novell.com/documentation/beta/imanager25/index.html)』 (<http://www.novell.com/documentation/beta/imanager25/index.html>) を参照してください。

- 8** モジュールが正しく保存されたことを示すメッセージが表示されたら、iManager サーバを再起動します。

iManager を無制限アクセスモードで実行している場合 ( ツリーに RBS コレクションがない場合 ) は、手順 9 ~ 15 を省略してください。

**注** : iManager サーバの再起動の詳細については、『[iManager 2.5 管理ガイド](http://www.novell.com/documentation/beta/imanager25/index.html)』 (<http://www.novell.com/documentation/beta/imanager25/index.html>) を参照してください。

- 9** iManager にログインし、[設定]  をクリックします。
- 10** 左側の画面で、[RBS の設定] > [iManager の設定] の順にクリックします。
- 11** ( 状況によって実行 ) RBS コレクションがすでに作成されている場合は、[コレクションのアップグレード] を選択して、[次へ] > [次へ] の順にクリックします。
- 12** ( 状況によって実行 ) RBS コレクションがない場合は、次の操作を実行します。
- 12a** [新しいコレクションの作成] を選択して、[次へ] をクリックします。
- 12b** 役割ベースサービスを作成するコンテナを選択して、[次へ] をクリックします。
- 13** Novell Kerberos プラグインを選択して、スコープ ( ツリー名または任意のコンテナ ) を割り当ててから、[開始] をクリックして Kerberos 構成用の iManager プラグインのインストールを完了します。

**注** : これにより、Kerberos 管理の役割で選択したスコープにスーパーバイザの権利が割り当てられます。

- 14** 完了メッセージが表示されるのを待って、[閉じる] をクリックします。

- 15** ページをリフレッシュします。

Kerberos 管理の役割が左側の画面に表示されます。

Kerberos 管理の役割が表示されない場合は、上の手順 8 の説明に従って iManager サーバを再起動します。

**注** : iManager サーバが Windows Web サービス (IIS) 上で動作している場合は、NMAS Kerberos 用の iManager プラグインをインストールする前に RBS 収集を作成しておく必要があります。

## Kerberos の LDAP 拡張の追加

Kerberos の LDAP 拡張では、Kerberos キーの管理機能が提供されています。

Kerberos の LDAP 拡張を使用するには、C 言語用の LDAP ライブラリをインストールする必要があります。詳細については、[LDAP Libraries for C \(http://developer.novell.com/ndk/cldap.htm\)](http://developer.novell.com/ndk/cldap.htm) を参照してください。

Kerberos の LDAP 拡張を追加または削除するには、次の場所にある `krbldapconfig` ユーティリティを使用します。

- ◆ **Linux** : 展開フォルダ `/Linux/nmas/NmasMethods/Novell/GSSAPI/Kerberos_ldap_extensions/Linux/krbldapconfig`

例 :

```
/misc/eDir88/Linux/nmas/NmasMethods/Novell/GSSAPI/Kerberos_ldap_extensions/Linux/krbldapconfig
```

- ◆ **Solaris** : 展開フォルダ `/Solaris/nmas/NmasMethods/Novell/GSSAPI/Kerberos_ldap_extensions/Solaris/krbldapconfig`

例 :

```
/misc/eDir88/Linux/nmas/NmasMethods/Novell/GSSAPI/Kerberos_ldap_extensions/Solaris/krbldapconfig
```

- ◆ **NetWare® および Windows** :  
NetWare の場合は、他の任意のプラットフォーム上で `krbldapconfig` を実行できます。  
展開フォルダ `/Windows/nmas/NmasMethods/Novell/GSSAPI/Kerberos_ldap_extensions/Windows/krbldapconfig`

例 :

```
/misc/eDir88/Linux/nmas/NmasMethods/Novell/GSSAPI/Kerberos_ldap_extensions/Windows/krbldapconfig
```

Kerberos LDAP 拡張を追加するには、次の構文を使用します。

```
krbldapconfig {-i | -u} -D バインド DN [-w バインド DN のパスワード] [-h LDAP ホスト] [-p LDAP ポート] [-e ルート認証局証明書]
```

`krbldapconfig` ユーティリティのパラメータについて、次の表で説明します。

| パラメータ              | 説明  |
|--------------------|---|
| -i                 | Kerberos LDAP 拡張を eDirectory に追加します。                                  |
| -u                 | Kerberos LDAP 拡張を eDirectory から削除します。                                 |
| -D バインド FDN        | 管理者または管理者と同等の権利を持つユーザの FDN を指定します。<br>cn=admin,o=org の形式で指定する必要があります。 |
| -w バインド FDN のパスワード | バインド FDN のパスワードを指定します。  |
| -h LDAP サーバ        | Kerberos LDAP 拡張をインストールする必要がある LDAP サーバのホスト名または IP アドレスを指定します。        |

| パラメータ         | 説明   |
|---------------|--|
| -p ポート        | LDAP サーバが動作しているポートを指定します。  |
| -e ルート認証局ファイル | SSL バインド用のルート認証局証明書のファイル名を指定します。<br><br>SSL ポートを使用する場合は、-e オプションを指定してください。<br><br>詳細については、 <a href="#">591 ページの「ルート認証局証明書のエクスポート」</a> を参照してください。 |

**注:** -h オプションを指定しなかった場合は、krbldapconfig を起動したローカルホストの名前がデフォルトとして使用されます。

LDAP サーバポートとルート認証局証明書を指定しなかった場合は、ポート 389 がデフォルトで使用されます。

LDAP サーバポートを指定せずにルート認証局証明書を指定した場合は、ポート 636 がデフォルトで使用されます。

この拡張を追加するには次のように入力します。

```
krbldapconfig -i -D cn=admin,o=org -w password -h ldapserver -p 389
```

削除するには次のように入力します。

```
krbldapconfig -u -D cn=admin,o=org -w password -h ldapserver -p 389
```

**重要:** インストールによる変更を有効にするには、LDAP サーバを手動でリフレッシュする必要があります。詳細については、[363 ページの「LDAP サーバをリフレッシュする」](#)を参照してください。

## ルート認証局証明書のエクスポート

- 1 iManager で、[eDirectory 管理] > [オブジェクトの変更] の順にクリックして、[オブジェクトの変更] ページを開きます。
- 2 [単一オブジェクト] をクリックして、サーバのサーバ証明書オブジェクトを選択します。
- 3 [OK] をクリックします。
- 4 [証明書] タブをクリックし、[ルート認証局証明書] を選択して、証明書の詳細を表示します。
- 5 [エクスポート] をクリックして、証明書エクスポートウィザードを起動します。
- 6 プライベートキーをエクスポートするかどうかを指定して、[次へ] をクリックします。
- 7 [バイナリ DER 形式のファイル] を選択して、[次へ] をクリックします。
- 8 [Save the Exported Certificate to a File (エクスポートされた証明書をファイルに保存)] をクリックします。
- 9 [閉じる] をクリックします。

## SASL-GSSAPI メソッドの設定

- 1 eDirectory への接続に SSL/TLS 接続を使用するように iManager が設定されていない場合、SASL-GSSAPI 用の iManager プラグインは動作しません。レルムのマスターキーとプリンシパルキーを保護するために、安全な接続が必要です。

通常、iManager は eDirectory への接続に SSL/TLS 接続を使用するようにデフォルトで設定されています。Kerberos 管理に使用する LDAP サーバの SSL ルート認証局証明書を iManager に追加する必要があります。

SSL/TLS 接続を使用して eDirectory へ接続するように iManager を設定する方法については、『*iManager 2.0 管理ガイド*』(<http://www.novell.com/documentation/lg/imanager20/index.html?page=/documentation/lg/imanager20/imanager20/data/am4ajce.html#bow4dv4>) を参照してください。

- 2 次の手順を順序どおりに実行します。
  - 2a Kerberos スキーマを拡張する。
  - 2b レルムコンテナを作成する。
  - 2c LDAP サービスプリンシパルを作成する。
  - 2d KDC からサービスプリンシパルキーまたは共有キーを抽出する。
  - 2e eDirectory 内にサービスプリンシパルオブジェクトを作成する。
  - 2f Kerberos のプリンシパル名をユーザオブジェクトに関連付ける。

## SASL-GSSAPI メソッドを使用して設定された eDirectory ツリーをマージする

ツリーのどちらか一方または両方が SASL-GSSAPI メソッドを使用して設定された 2 つのツリーをマージする場合は、ソースツリーにあるすべての Kerberos オブジェクトをターゲットツリー内で手動で作成する必要があります。

## SASL-GSSAPI メソッドの管理

iManager では、Kerberos に関する次の操作を実行できます。

- ◆ 592 ページの「Kerberos スキーマの拡張」
- ◆ 593 ページの「Kerberos レルムオブジェクトの管理」
- ◆ 594 ページの「サービスプリンシパルの管理」
- ◆ 599 ページの「外部プリンシパルの編集」

### Kerberos スキーマの拡張

この作業を行うと、Kerberos のオブジェクトクラスと属性定義を使用して eDirectory を拡張できます。

- 1 スキーマがまだ拡張されていない場合は、[OK] をクリックしてスキーマを拡張します。
- 2 iManager で、[Kerberos Management] > [スキーマの拡張] の順にクリックして、[スキーマの拡張] ページを開きます。

スキーマがすでに拡張されている場合は、そのことを示すメッセージが表示されます。
- 3 [閉じる] をクリックします。

## Kerberos レalmオブジェクトの管理

レalmとは、複数の KDC (Key Distribution Center) によって管理される論理ネットワークです。つまり、レalmとは、複数の KDC によって管理されるドメインまたはプリンシパルのグループです。慣例的に、レalm名はすべて大文字で記述され、インターネットドメインと区別されます。詳細については、[RFC 1510 \(http://www.ietf.org/rfc/rfc1510.txt?number=1510\)](http://www.ietf.org/rfc/rfc1510.txt?number=1510) を参照してください。

このセクションでは次のことについて説明します。

- ◆ [593 ページの「新しいレalmオブジェクトの作成」](#)
- ◆ [593 ページの「レalmオブジェクトの編集」](#)
- ◆ [594 ページの「レalmオブジェクトの削除」](#)

### 新しいレalmオブジェクトの作成

サポートされているデフォルトの暗号化タイプは DES-CBC-CRC です。

- 1 iManager で、[Kerberos Management] > [New Realm] の順にクリックして、[New Realm] ページを開きます。
- 2 作成する Kerberos レalmの名前を指定します。  
レalm名は、このログインメソッドを設定する際に指定するレalm名と一致している必要があります、RFC 1510 の命名規則に準拠している必要があります。
- 3 レalmのマスタパスワードを指定して、パスワードを確認します。  
**注:** マスタパスワードには必ず強力なパスワードを使用してください。
- 4 Kerberos レalmに関連付けるサブツリーを指定するか、オブジェクトセクタアイコンを使用してサブツリーを選択します。  
これは、このレalmの eDirectory サービスプリンシパルを格納するサブツリーまたはコンテナの FDN になります。このサブツリーはユーザプリンシパルには適用できません。  
サブツリーまたはコンテナを選択しない場合は、ツリーのルートがデフォルトで使用されます。
- 5 サブツリー検索の範囲を指定します。
  - ◆ 1レベル: レalmサブツリーの直下にあるエントリのみが検索の対象になります。
  - ◆ サブツリー: レalmサブツリー以下のサブツリー全体が検索の対象になります。
- 6 [OK] をクリックします。

**注:** SASL-GSSAPI では [KDC Services] ボックスは使用しません。

### レalmオブジェクトの編集

- 1 iManager で、[Kerberos Management] > [Edit Realm] の順にクリックして、[Edit Realm] ページを開きます。
- 2 編集する Kerberos レalmの名前を指定するか、オブジェクトセクタアイコンを使用して Kerberos レalmを選択します。
- 3 [OK] をクリックします。

- 4 Kerberos レalmに関連付けるサブツリーを指定するか、オブジェクトセクタアイコンを使用してサブツリーを選択します。

これは、このレalmの eDirectory サービスプリンシパルを格納するサブツリーまたはコンテナの FDN になります。このサブツリーはユーザプリンシパルには適用できません。

サブツリーまたはコンテナを選択しない場合は、ツリーのルートがデフォルトで使用されます。

- 5 サブツリー検索の範囲を指定します。
  - ◆ 1レベル: レalmサブツリーの直下にあるエントリのみが検索の対象になります。
  - ◆ サブツリー: レalmサブツリー以下のサブツリー全体が検索の対象になります。
- 6 [OK] をクリックします。
- 7 (オプション) 別のレalmを編集するには、[タスクの繰り返し] をクリックします。

注: SASL-GSSAPI では [KDC Services] ボックスは使用しません。

## レalmオブジェクトの削除

- 1 iManager で、[Kerberos Management] > [Delete Realm] の順にクリックして、[Delete Realm] ページを開きます。
- 2 削除するレalmを選択します。

複数のレalmを選択するには、<Shift> キーを押しながらかレalmを選択するか、<Shift> キーを押しながらか矢印キーを押します。
- 3 [OK] をクリックします。
- 4 もう一度 [OK] をクリックして削除操作を確定するか、[キャンセル] をクリックして削除操作をキャンセルします。

**重要:** レalmオブジェクトを削除すると、そのレalmにあるすべてのサービスプリンシパルオブジェクトが削除されます。

## サービスプリンシパルの管理

このセクションでは次のことについて説明します。

- ◆ 595 ページの「LDAP サーバ用のサービスプリンシパルの作成」
- ◆ 595 ページの「eDirectory 用のサービスプリンシパルキーの抽出」
- ◆ 596 ページの「eDirectory でのサービスプリンシパルオブジェクトの作成」
- ◆ 597 ページの「Kerberos サービスのプリンシパルキーの表示」
- ◆ 597 ページの「Kerberos サービスのプリンシパルオブジェクトの削除」
- ◆ 598 ページの「Kerberos サービスプリンシパルのパスワードの設定」

## LDAP サーバ用のサービスプリンシパルの作成

KDC に付属する Kerberos 管理ツールを使用して、暗号化タイプとソルトタイプをそれぞれ DES-CBC-CRC と Normal に設定して eDirectory サービスプリンシパルを作成します。

プリンシパルの名前は、`ldap/MYHOST.MYDNSDOMAIN@REALMNAME` の形式にする必要があります。

MIT KDC を使用している場合は、次のようなコマンドを実行します。

```
kadmin:addprinc -randkey -e des-cbc-crc:normal ldap/  
server.novell.com@MITREALM
```

Heimdal KDC を使用している場合は、次のようなコマンドを実行します。

```
kadmin -l  
kadmin> add --random-key ldap/server.novell.com@MITREALM
```

サービスプリンシパルでサポートされていない暗号化タイプを削除するには、次のコマンドを実行します。

```
kadmin> del_enctype ldap/MYHOST.MYDNSDOMAIN@MYREALM des-cbc-md4  
kadmin> del_enctype ldap/MYHOST.MYDNSDOMAIN@MYREALM des-cbc-md5  
kadmin> del_enctype ldap/MYHOST.MYDNSDOMAIN@MYREALM des3-cbc-sha1
```

`MYHOST.MYDNSDOMAIN` はホスト名、`MYREALM` は Kerberos レalm です。

### ベストプラクティス

LDAP サービスプリンシパルキーは定期的に変更することをお勧めします。LDAP サービスプリンシパルキーを変更した場合は、必ず eDirectory 内のプリンシパルオブジェクトを更新してください。

## eDirectory 用のサービスプリンシパルキーの抽出

KDC に付属する Kerberos 管理ツールを使用して、[595 ページの「LDAP サーバ用のサービスプリンシパルの作成」](#)で作成した LDAP サービスプリンシパルのキーを抽出し、ローカルファイルシステムに保存します。この作業を行うには、Kerberos 管理者の協力が必要です。

MIT KDC を使用している場合は、次のようなコマンドを実行します。

```
kadmin: ktadd -k /ディレクトリパス/keytab ファイル名 -e des-cbc-  
crc:normal ldap/server.novell.com@MITREALM
```

Microsoft KDC を使用している場合は、たとえば Active Directory で `ldapMYHOST` というユーザを作成してから、次のコマンドを実行します。

```
ktpass -princ ldap/MYHOST.MYDNSDOMAIN@MYREALM -mapuser ldapMYHOST  
-pass パスワード -out MYHOST.keytab
```

このコマンドを実行すると、プリンシパル (`ldap/MYHOST.MYDNSDOMAIN@MYREALM`) がユーザアカウント (`ldapMYHOST`) にマップされ、ホストプリンシパルのパスワードが `mypassword` に設定され、`MYHOST.keytab` ファイルにキーが抽出されます。



Heimdal KDC を使用している場合は、次のようなコマンドを実行します。

```
kadmin> ext_keytab -k /ディレクトリパス/keytab ファイル名 ldap/  
server.novell.com@MITREALM
```

keytab ファイル名は、抽出されたキーが保存されるファイルの名前です。

## eDirectory でのサービスプリンシパルオブジェクトの作成

595 ページの「LDAP サーバ用のサービスプリンシパルの作成」で指定した名前を使用して Kerberos サービスプリンシパル (ldap/MYHOST.MYDNSDOMAIN@MYREALM) を作成する必要があります。

### ベストプラクティス

eDirectory 用のサービスプリンシパルは、SASL GSSAPI メカニズムを使用できるすべてのサーバからいつでもアクセスできるようになっている必要があります。セキュリティコンテナ内の Kerberos レルムコンテナの下にこれらの eDirectory サービスプリンシパルを作成しない場合は、これらの eDirectory サービスプリンシパルを含むコンテナを独立したパーティションとして作成し、そのコンテナを広範囲で複製することをお勧めします。

- 1 iManager で、[Kerberos Management] > [New Principal] の順にクリックして、[New Principal] ページを開きます。
- 2 作成するプリンシパルの名前を指定します。  
プリンシパルの名前は、ldap/MYDNSDOMAIN@REALMNAME の形式にする必要があります。
- 3 プリンシパルオブジェクトを作成するコンテナの名前を指定するか、オブジェクトセクタアイコンを使用してコンテナを選択します。
- 4 レルムの名前を指定します。  
**手順 2** でレルムの名前を指定した場合は、このフィールドを空白のままにします。
- 5 次のいずれかを実行します。
  - ◆ keytab ファイル名を指定するか、[参照] をクリックして keytab ファイルが保存されている場所を選択します。  
このファイルには、595 ページの「eDirectory 用のサービスプリンシパルキーの抽出」で抽出されたキーが保存されています。
  - ◆ パスワードを指定して確定し、暗号化タイプとソルトタイプの組み合わせを選択します。  
パスワードと暗号化/ソルトタイプの組み合わせは、KDC データベース内のサービスプリンシパルを作成したときに指定した組み合わせと一致させる必要があります。
- 6 [OK] をクリックします。



## Kerberos サービスのプリンシパルキーの表示

- 1 iManager で、[Kerberos Management] > [View Principal Keys] の順にクリックして、[View Principal Keys] ページを開きます。
- 2 表示するプリンシパルキーの名前を指定するか、オブジェクトセクタアイコンを使用してプリンシパルキーを選択します。  
プリンシパルキーに関する次の情報が表示されます。
  - ◆ プリンシパル名
  - ◆ キーテーブル
    - ◆ 番号：キーテーブル内のキーのシリアル番号
    - ◆ バージョン：キーのバージョン
    - ◆ キータイプ：このプリンシパルキーのタイプ
    - ◆ ソルトタイプ：このプリンシパルキーのソルトタイプ
- 3 [OK] をクリックします。

## Kerberos サービスのプリンシパルオブジェクトの削除

1 つまたは複数のオブジェクトを削除できます。また、削除するプリンシパルオブジェクトの高度な選択を行えます。



1 つのオブジェクトを削除するには、次の操作を実行します。

- 1 iManager で、[Kerberos Management] > [Delete Principal] の順にクリックして、[Delete Principal] ページを開きます。
- 2 [単一オブジェクトの選択] をクリックします。
- 3 削除するプリンシパルオブジェクトの名前を指定するか、オブジェクトセクタアイコンを使用してプリンシパルオブジェクトを選択します。
- 4 [OK] をクリックします。
- 5 もう一度 [OK] をクリックして削除操作を確定するか、[キャンセル] をクリックして削除操作をキャンセルします。

複数のオブジェクトを削除するには、次の操作を実行します。

- 1 iManager で、[Kerberos Management] > [Delete Principal] の順にクリックして、[Delete Principal] ページを開きます。
- 2 [複数オブジェクトの選択] をクリックします。
- 3 削除するプリンシパルオブジェクトの名前を指定するか、オブジェクトセクタアイコンを使用してプリンシパルオブジェクトを選択します。
- 4 削除するプリンシパルを選択します。
- 5 [OK] をクリックします。
- 6 もう一度 [OK] をクリックして削除操作を確定するか、[キャンセル] をクリックして削除操作をキャンセルします。

高度な選択方法でプリンシパルオブジェクトを削除するには、次の操作を実行します。

- 1 iManager で、[Kerberos Management] > [Delete Principal] の順にクリックして、[Delete Principal] ページを開きます。
- 2 [高度な選択] をクリックします。
- 3 オブジェクトクラスを選択します。
- 4 プリンシパルオブジェクトが格納されているコンテナを指定するか、オブジェクトセレクトアアイコンを使用してコンテナを選択します。
- 5 **手順 3** で指定したコンテナのサブコンテナも含める場合は、[サブコンテナを含める] をクリックします。
- 6  をクリックして、[高度な選択条件] ウィンドウを開きます。
- 7 ドロップダウンリスト から 属性タイプと 演算子を選択して、対応する値を入力します。
- 8 他の論理グループを選択対象に追加するには、[行の追加]  をクリックします。
- 9 [OK] をクリックしてフィルタを設定します。
- 10 [プレビューの表示] をクリックして、高度な選択のプレビューを表示します。
- 11 [OK] をクリックします。
- 12 もう一度 [OK] をクリックして削除操作を確定するか、[キャンセル] をクリックして削除操作をキャンセルします。

## Kerberos サービスプリンシパルのパスワードの設定

KDC で eDirectory サービスのプリンシパルキーがリセットされた場合は、eDirectory でもそのプリンシパルキーを更新する必要があります。



キーの抽出については、[595 ページの「eDirectory 用のサービスプリンシパルキーの抽出」](#)を参照してください。

- 1 iManager で、[Kerberos Management] > [Set Principal Password] の順にクリックして、[Set Principal Password] ページを開きます。
- 2 個別にパスワードを設定する必要があるプリンシパルオブジェクトの名前を指定するか、オブジェクトセレクトアアイコンを使用してプリンシパルオブジェクトを選択します。
- 3 keytab ファイル名を指定するか、[参照] をクリックして keytab ファイルが保存されている場所を選択します。
- 4 次のいずれかを実行します。
  - ◆ プリンシパルキーが格納されている keytab ファイルの名前を指定するか、[参照] をクリックして keytab ファイルが保存されている場所を選択します。

サービスプリンシパルの作成およびキーの抽出の詳細については、[595 ページの「LDAP サーバ用のサービスプリンシパルの作成」](#)および [595 ページの「eDirectory 用のサービスプリンシパルキーの抽出」](#)を参照してください。
  - ◆ パスワードを指定して確定し、暗号化タイプとソルトタイプの組み合わせを選択します。
- 5 [OK] をクリックしてパスワードを設定します。
- 6 (オプション) 別のプリンシパルのパスワードを設定するには、[タスクの繰り返し] をクリックします。

## 外部プリンシパルの編集

iManager を使用して、Kerberos プリンシパル名を eDirectory に追加できます。

- 1 iManager で、[Kerberos Management] > [Edit Foreign Principals] の順にクリックして、[Edit Foreign Principals] ページを開きます。
- 2 有効なユーザオブジェクトの FDN を指定するか、オブジェクトセクタアイコンを使用してユーザオブジェクトを選択します。
- 3 [OK] をクリックします。
- 4 外部プリンシパル名を指定して、[追加]  をクリックします。  
プリンシパルの名前は、principalname@REALMNAME の形式にする必要があります。  
外部プリンシパル名を削除するには、名前を選択して、[削除]  をクリックします。
- 5 [OK] をクリックします。

## ログインシーケンスの作成

ログインシーケンスの作成については、『[NMAS 3.0 管理ガイド](http://www.novell.com/documentation/beta/nmas30/index.html?page=/documentation/beta/nmas30/admin/data/a49tuwk.html#a4)』(<http://www.novell.com/documentation/beta/nmas30/index.html?page=/documentation/beta/nmas30/admin/data/a49tuwk.html#a4>) の「Managing Login Sequences」を参照してください。

## LDAP での SASL-GSSAPI の使用方法

SASL-GSSAPI をインストールすると、SASL-GSSAPI が他の SASL 方式と共に rootDSE の supportedSASLMechanisms 属性に追加されます。

LDAP サーバは、SASL に問い合わせた環境設定時にインストールしたメカニズムを検索し、インストールされたメカニズムを自動でサポートします。また、supportedSASLMechanisms 属性を使って rootDSE で現在サポートされている SASL メカニズムをレポートします。

そのため、GSSAPI をインストールすると、GSSAPI がデフォルトのメカニズムになります。

ただし、明示的に SASL GSSAPI メカニズムを使用して LDAP の操作を行う場合は、コマンドラインで GSSAPI を指定できます。

たとえば、OpenLDAP で GSSAPI メカニズムを使用して検索を行うには、次のように入力します。

```
ldapsearch -Y GSSAPI -h 164.99.146.48 -b "" -s base
```

## エラーメッセージ

SASL-GSSAPI のエラーメッセージは次の場所に記録されます。

- ◆ Linux および UNIX: ndsd.log
- ◆ NetWare : ログ画面
- ◆ Windows: c:\temp\saslgss.log

詳細については、『[eDirectory 8.8 Troubleshooting Guide](http://www.novell.com/documentation/beta/edir88/index.html)』(<http://www.novell.com/documentation/beta/edir88/index.html>) の **エラーメッセージ** を参照してください。

