Novell Identity Manager

3.5.1

www.novell.com

ADMINISTRATION GUIDE (管理ガイド)

September 28, 2007

Novell®

保証と著作権

米国 Novell, Inc. およびノベル株式会社は、この文書の内容または使用について、いかなる保証、表明または約束も行っていません。また文書の商品性、および特定の目的への適合性について、いかなる黙示の保証も否認し、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いません。またノベル製ソフトウェアの商品性、および特定の目的への適合性について、いかなる黙示の保証も否認し、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。

本契約の下で提供される製品または技術情報はすべて、米国の輸出規制および他国の商法の制限を受けます。お客様は、すべての輸出規制を遵守し、製品の輸出、再輸出、または輸入に必要なすべての許可または等級を取得するものとします。お客様は、現在の米国の輸出除外リストに掲載されている企業、および米国の輸出管理規定で指定された輸出禁止国またはテロリスト国に本製品を輸出または再輸出しないものとします。お客様は、取引対象製品を、禁止されている核兵器、ミサイル、または生物化学兵器を最終目的として使用しないものとします。ノベル製ソフトウェアの輸出に関する詳細については、www.novell.com/info/exports/ を参照してください。弊社は、お客様が必要な輸出承認を取得しなかったことに対し如何なる責任も負わないものとします。

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

オンラインマニュアル: 本製品とその他の Novell 製品のオンラインヘルプにアクセスする場合や、アップデート版を入手する場合は、www.novell.com&documentation をご覧ください。

目次

このガイドについて

Novell® Identity Manager は、アプリケーション、ディレクトリ、およびデータベース間で情報を共有するためのデータ共有および同期サービスです。このサービスでは、分散された情報をリンクし、ユーザは識別情報の変更時に指定システムを自動的に更新するポリシーを設定できます。Identify Manager は、アカウントプロビジョニング、セキュリティ、ユーザセルフサービス、認証、認可、自動化されたワークフロー、および Web サービスの基盤となります。Identify Manager を使用すると、分散された識別情報を統合、管理、および制御できるため、適切なユーザに適切なリソースを安全に提供できます。

このガイドでは、Identity Manager の技術の概要と、管理、および設定の機 \'94\'5c について説明します。

フィードバック

本マニュアルおよびこの製品に含まれているその他のマニュアルについて、皆様のご意見やご要望をお寄せください。オンラインヘルプの各ページの下部にある［ユーザコメント］機能を使用するか、http://www.novell.com/documentation/feedback.html にアクセスし、コメントを入力してください。

マニュアルの更新

このマニュアルの最新のバージョンについては、Identity Manager のマニュアルの Web サイト (http://www.novell.com/documentation/idm35) を参照してください。

追加のマニュアル

Identity Manager のインストールおよびアップグレードに関するマニュアルについては、『*インストールガイド* (http://www.novell.com/documentation/idm35)』を参照してください。

Identity Manager のポリシーとフィルタのマニュアルについては、『ポリシーガイド (http://www.novell.com/documentation/idm35)』を参照してください。

設計と実装の実践に関するマニュアルについては、『*Designer 2.1 for Identity Manager: Administration Guide* (http://www.novell.com/documentation/designer21/)』を参照してください。

パスワードポリシー、パスワードセルフサービス、およびパスワードの管理に関するマニュアルについては、『*パスワード管理ガイド* (http://www.novell.com/documentation/password_management/index.html)』を参照してください。

Identity Manager ドライバの使用に関するマニュアルについては、Identity Manager Driver のマニュアルの Web サイト (http://www.novell.com/documentation/idm35drivers/index.html) を参照してください。

マニュアルの表記規則

\'96\'7b\'83\'7d ニュアルでは、手順に含まれる複数の操作および相互参照パス内の項目を分けるために、左向きの不等号 (>) を使用しています。

商標記号 (®、™ など) 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。

Identity Manager アーキテクチャの概要

1

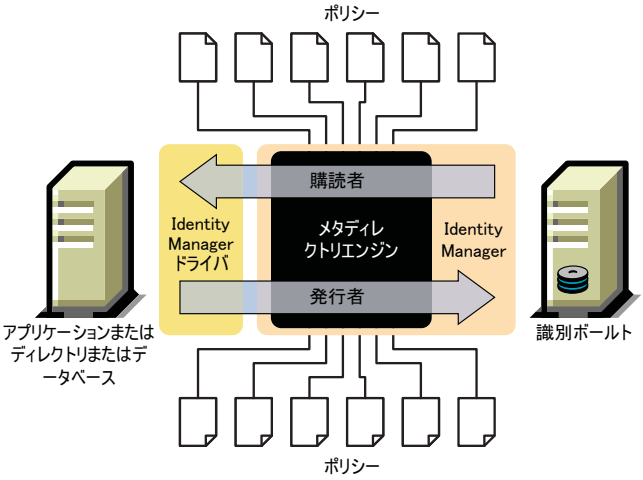
Identity Manager には、次の 3 つの主なコンポーネントがあります。

1.1 Identity Manager

Identity Manager は、識別ボールトと接続システム間におけるデータの同期機能を提供します。接続システムは、アプリケーション、ディレクトリ、データベース、またはファイルで \'8d\'5c 成されます。

Identity Manager には、いくつかのコンポーネントが含まれています。次の \'90\'7d は、基 \'96\'7b コンポーネントとそれらの関係を示します。

図 1-1 *Identity Manager のコンポーネント*



Metadirectory エンジンは Identity Manager アーキテクチャの重要なモジュールです。このエンジンは、Identity Manager ドライバが識別 \'83\'7bールトと情報を同期化できるインタフェースを提供し、異なるデータシステムでも接続してデータを共有できるようにします。

メタディレクトリエンジンは、XML 形式を使用して識別ボールトデータおよび識別ボールトイベントを処理します。Metadirectory エンジンはルールプロセッサとデータ変換エンジンを採用し、2 つのシステム間のデータフローを操作しています。

1. すべての Identity Manager ドライバのフィルタを読み込みます。
2. 適切な識別 \'83\'7bールトイベントのドライバを登録します。
3. 各ドライバの指定に従ってデータをフィルタ処理します。

4. 各ドライバに渡される識別 \'83\'7bールトイベントのキャッシュを設定します。

識別 \'83\'7bールトは、初期化時に次の処理を実行します。

- イベントがキャッシュされると、そのキャッシュを所有するドライバがイベントを読み込みます。
- ドライバは識別ボールトデータを eDirectory のネイティブ形式で受信し、これを XDS 形式 (Identity Manager で使用される XML ボキャブラリで、ポリシーによって変換できます) に変換した後、イベントをメタディレクトリエンジンに送信します。このエンジンが接続システムドライバ内のすべてのポリシーを読み込み、ポリシーに従って XML 形式のデータが作成されて、接続システムドライバに送信されます。次に、接続システムにデータが送信されます。ポリシーの詳細については、「*Identity Manager 3.5.1 のポリシーの理解*」を参照してください。
- ドライバの発行者部分は、接続システムからの更新情報の収集と、それらの情報の識別ボールトへの送信を担当します。2 つのシステム間で共有している情報の変更が接続システムドライバに通知されると、接続システムドライバはそれらの情報を収集し、フィルタに適合したデータ群かどうかを確認した後 XDS 形式に変換してエンジンに送信します。

1.1.1 Metadirectory エンジン

メタディレクトリエンジンは、eDirectory インタフェースと同期エンジンの 2 つのコンポーネントに分けられます。

eDirectory インタフェース

メタディレクトリエンジンに組み込まれた eDirectory インタフェースは、eDirectory で発生するイベントを検出するために使用されます。このインタフェースは、イベントキャッシュを使用することで、Identity Manager に確実にイベントを送信できるようにしています。eDirectory インタフェースは複数のドライバをロードできます。つまり、その eDirectory サーバ用に実行されている Identity Manager のインスタンスは 1 つだけですが、複数の接続システムと通信できます。識別ボールトと接続システムの間でイベントループが発生しないように、このインタフェースにはループバック検出機能が組み込まれています。このインタフェースにはループバック保護機 \'94\'5c が含まれていますが、個々の接続システムドライバにループバック検出機 \'94\'5c を組み込むことをお勧めします。

同期エンジン

同期エンジンは、Identity Manager ポリシーを各イベントに適用します。ポリシーは、DirXML スクリプトを使用してポリシービルダで作成します。ポリシービルダを使用すると、XML ドキュメントまたは XSLT で記述されたスタイルシートを使用する代わりに、GUI インタフェースを使ってポリシーを作成できます。スタイルシートも使用できますが、使いやすさではポリシービルダの方が優れています。ポリシービルダーまたは DirXML スクリプトの詳細については、「*Identity Manager 3.5.1 のポリシーの理解*」を参照してください。

同期エンジンは各タイプのポリシーをソースドキュメントに適用します。これらの変換を完了する機能は、Identity Manager の最も強力な機能の 1 つです。識別 \'83\'7bールトと接続システムとの間で共有されるときに、データはリアルタイムで変換されます。

1.1.2 ドライバ設定ファイル

ドライバ設定は、Identity Manager に含まれる事前設定済みの XML ファイルです。これらの設定ファイルは iManager および Designer のウィザードを使用してインポートできます。

これらのドライバ設定にはサンプルポリシーが含まれます。これらは運用環境での使用を目的としたものではなく、ユーザが変更するテンプレートとして提供されています。

1.1.3 Identity Manager のイベントキャッシュ

eDirectory から生成されるすべてのイベントは、正常に処理されるまでイベントキャッシュに格納されています。これによって、接続不良、システムリ \'83\'5cースの損失、ドライバの入手不 \'94\'5c、またはその他のネットワーク障害によってデータが失われないようにしています。

1.1.4 ドライバシム

ドライバシムは、接続システムと識別ボールト間における情報のルートとして機能します。シムは Java*、C、または C++ で記述されます。

メタディレクトリエンジンとドライバシムの間の通信は、イベント、クエリ、および結果を記述する XML ドキュメントの形式で行われます。ドライバシムは一般的にはドライバと呼ばれます。これは、識別 \'83\'7bールトと接続システムとの間で情報が転送されるルートです。

シムでサポートされているオブジェクトイベントは次のとおりです。

- 追加 (作成)
- 変更
- 削除
- ÿ»×—
- 移動
- クエリ

また、Identity Manager が接続システムを照会できるように、シムは定義済みクエリの機 \'94\'5c をサポートしている必要があります。

識別 \'83\'7bールトで、接続システムでアクションを引き起こすイベントが発生すると、Identity Manager は、その識別 \'83\'7bールトイベントを記述する XML ドキュメントを作成し、加入者チャネルを介してドライバシムに送信します。

接続システムでイベントが発生すると、接続システムイベントを記述する XML ドキュメントがドライバシムによって生成されます。続いて、ドライバシムが発行者チャネルを使用してその XML ドキュメントを Identity Manager に送信します。Identity Manager は、発行者ポリシーを使用してイベントを処理した後、適切なアクションを実行するよう識別 \'83\'7bールトに指示します。

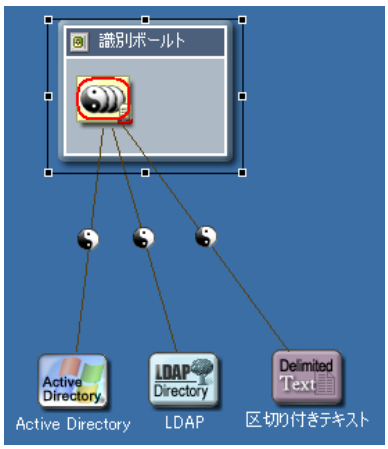
1.1.5 ドライバセット

ドライバセットは複数の Identity Manager ドライバを格納するコンテナオブジェクトです。一度に 1 つのドライバセットを 1 つのサーバに関連付けることができます。このため、実行中のドライバはすべて同じドライバセットにグループ化する必要があります。

ドライバセットオブジェクトは、そのオブジェクトを使用しているいずれかのサーバ上にある完全な読み書き可能レプリカに存在しなければならないため、ドライバセットをパーティションに分割することをお勧めします。これは、ユーザのレプリカが別のサーバに移動された場合に、ドライバオブジェクトが移動されないようにするためです。

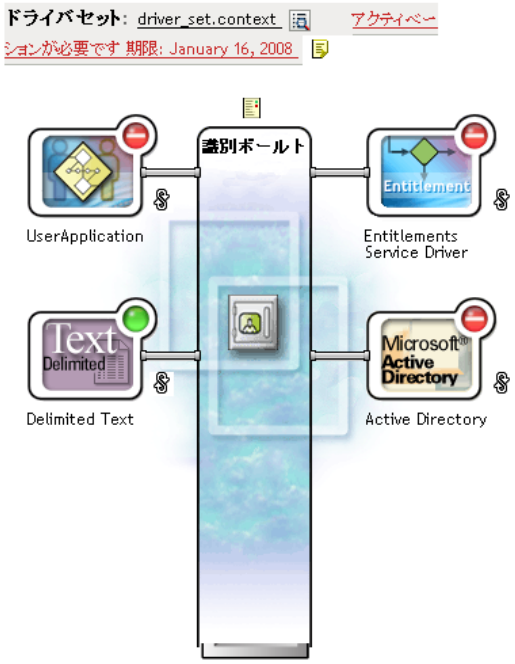
次の \'90\'7d は、Designer でドライバセットがどのように \'95\'5c 示されるのかを示します。

図 1-2 *Designer でのドライバセット*



次の \'90\'7d は、iManager でドライバセットがどのように \'95\'5c 示されるのかを示します。

図 1-3 iManager でのドライバセット



Designer の Modeler (前の図 1-2) または iManager の概要ページ (前の図 1-3) から、以下を実行できます。

- ドライバセットとそのプロパティを \'95\'5c 示および変更する
- ドライバセット内のドライバを \'95\'5c 示する
- ドライバのステータスを変更する
- ドライバセットをサーバに関連付ける
- ドライバを追加または削除する
- ドライバセットの起動情報を \'95\'5c 示する
- ドライバセットのステータスログを \'95\'5c 示する

1.1.6 ドライバオブジェクト

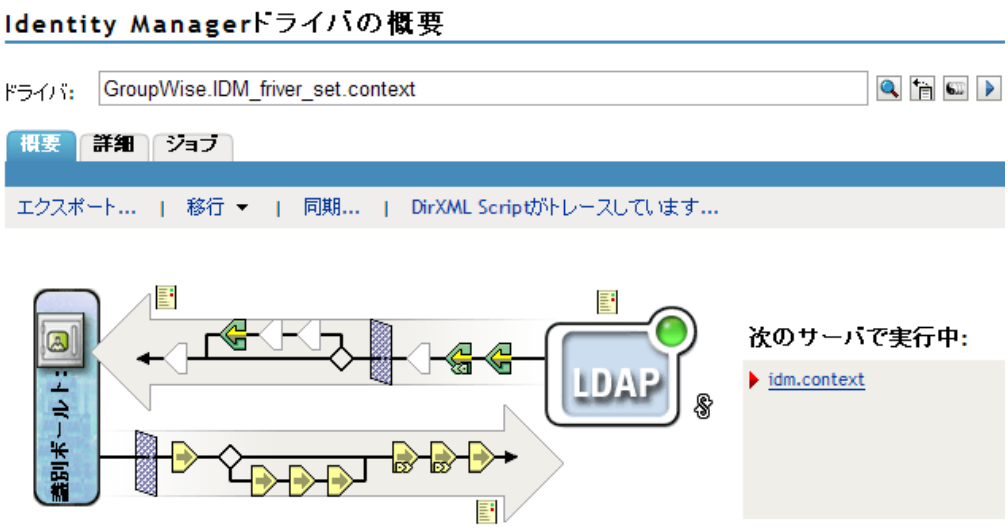
ドライバオブジェクトは、識別ボールトと統合されている接続システムに接続されているドライバを表します。次のコンポーネントは、ドライバオブジェクトとその設定パラメータを \'8d\'5c 成しています。

- ドライバセットオブジェクトに含まれる eDirectory ツリーのドライバオブジェクト。
- ドライバオブジェクトに含まれる加入者チャネルオブジェクト。
- ドライバオブジェクトに含まれる発行者オブジェクト。
- ドライバオブジェクト、加入者オブジェクト、および発行者オブジェクトによって参照される複数のポリシーオブジェクト。
- ドライバオブジェクトによって参照される実行可 \'94\'5c ドライバシム。
- 管理者によって設定されるシム固有のパラメータ。

- ドライバオブジェクトの eDirectory パスワード。このパスワードをシムで使用して、シムのリモート部分を認証できます。
- 接続システムに接続し、認証するために使用する認証パラメータ。
- エンタイトルメント。すべてのドライバに必要なものではありません。エンタイトルメントは、ドライバの作成時に有効にしたり、または後で追加したりできます。
- 次を含む、ドライバの起動オプション。
  - 無効 : ドライバは実行されません。
  - 手動 : ドライバは iManager を介して手動で起動する必要があります。
  - 自動起動 : 識別ボールトが起動すると、ドライバが自動的に起動します。
- Schema Mapping Policy の参照。
- 接続システムのスキーマを XML 表現。これは通常、シムを介して接続システムから自動的に取得されます。

iManager では、［Identity Manager ドライバの概要］ページにアクセスして、既存のドライバのパラメータ、ポリシー、スタイルシート、およびエンタイトルメントを変更できます。Identity Manager ドライバの概要を次に示します。

図 1-4 *Identity Manager ドライバの概要*



ドライバオブジェクトは、eDirectory の権利の確認にも使用されます。ドライバオブジェクトには、読み込みまたは書き込みを行うオブジェクトに対して、必要な eDirectory 権利を付与する必要があります。このためには、ドライバオブジェクトを、ドライバが同期化する eDirectory オブジェクトのトラスティにするか、ドライバオブジェクトに同等セキュリティを付与します。

権利の割り当ての詳細については、『*Novell eDirectory 8.8 管理ガイド*』の「eDirectory での権利 (http://www.novell.com/documentation/edir88/index.html?page=/documentation/edir88/edir88/data/fbachifb.html)」を参照してください。

1.1.7 発行者チャネルと加入者チャネル

Identity Manager ドライバには、データを処理するための発行者チャネルと購読者チャネルの 2 つのチャネルが含まれています。発行者チャネルは、接続システムから識別ボールトにイベントを送信します。購読者チャネルは、識別ボールトから接続システムにイベントを送信します。各チャネルには、データの処理と変換の方法を定義する独自のポリシーが含まれています。

図 1-5 *Designer の発行者チャネルおよび加入者チャネル*

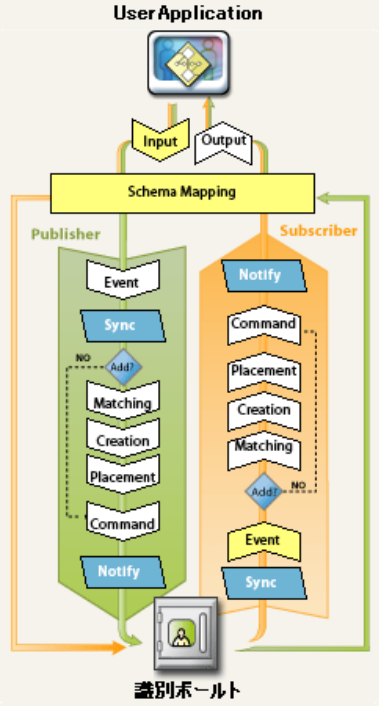
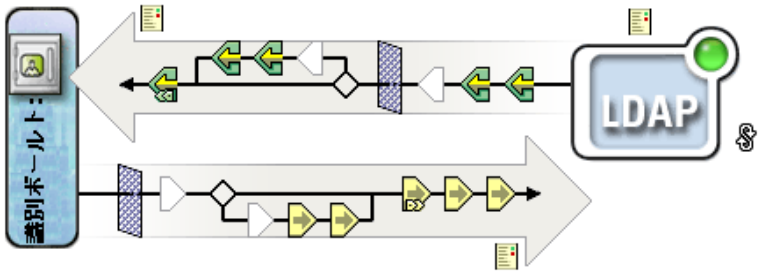


図 1-6 *iManager の発行者チャネルおよび加入者チャネル*



1.1.8 イベントとコ \'83\'7d ンド

Identity Manager のイベントとコマンドの違いは重要です。イベントがドライバに送信される場合、そのイベントはコマンドです。イベントが Identity Manager に送信される場合、そのイベントは通知です。ドライバは、Identity Manager にイベント通知を送信する際に、接続システムで発生した変更を Identity Manager に通知します。Metadirectory エンジンは、設定可 \'94\'5c なルールに基づいて、どのコ \'83\'7d ンドを識別 \'83\'7bールトに送信する必要があるかを決定します (コ \'83\'7d ンドが必要な場合)。

Identity Manager は、ドライバにコ \'83\'7d ンドを送信する場合、すでに識別 \'83\'7bールトイベントを入力として受け付けて適切なポリシーを適用し、コ \'83\'7d ンドが \'95\'5c す接続システム内の変更が必要であると判断しています。

1.1.9 ポリシーとフィルタ

ポリシーとフィルタによって、システム間のデータフローを制御できます。ポリシー内のルールを使用して、接続システムまたは接続元で使用するために、管理側の識別ボールトのクラス、属性、およびイベントをどのように変換するのかを定義します。ポリシーとフィルタの詳細については、「*Identity Manager 3.5.1 のポリシーの理解*」を参照してください。

1.1.10 関連付け

大部分の識別情報管理製品では、接続システムからディレクトリにオブジェクトをマップするために、接続システムに何らかの識別子を格納する必要があります。Identity Manager では、接続システムを変更する必要はありません。識別ボールトの各オブジェクトには、識別ボールトブジェクトを接続システム内の一意の識別子にマップする関連付けテーブルが含まれています。このテーブルはリバースインデックス形式なので、接続システムは、識別 \'83\'7bールトの更新時に識別 \'83\'7bールト識別子 (識別名など) をドライバに提供する必要がありません。

2 つのオブジェクト間の関連付けは、識別ボールト内の別のオブジェクトとまだ関連付けられていないオブジェクトでイベントが発生したときに作成されます。関連付けを作成するためには、定義可能な条件の最低限のセットが各オブジェクトで一致している必要があります。たとえば、4 つの属性のうち 2 つ (フルネーム、電話番号、従業員 ID、電子メールアドレス) が 90% 以上一致する場合にオブジェクトを関連付けるルールを作成できます。

2 つのオブジェクトが同じかどうかを判断するための条件は、一致ポリシーで定義します。変更されたオブジェクトに対して一致するオブジェクトが見つからない場合は、新しいオブジェクトが作成されます。このためには、最低限の作成条件すべてに一致していなければなりません。これらの条件はポリシーの作成によって定義されます。最後に、新しいオブジェクトをネーミング階層の中のどの位置に作成するかが Placement Policy (配置ポリシー) によって定義されます。

関連付けは次の 2 つの方法で作成できます。

- オブジェクト間の一致として
- 特定場所内のオブジェクトの新しい作成として

形成されたオブジェクト間の関連付けは、管理者がオブジェクトを作成するか、または関連付けを削除するまで有効です。

関連付けテーブル

Identity Manager では、関連付けとは、eDirectory 内のオブジェクトを、接続システムに存在するオブジェクトと一致させることを指します。Identity Manager を初めてインストールしたときに、eDirectory スキーマが拡張されます。この拡張には、すべての eDirectory オブジェクトのベースクラスに結び付けられた新しい属性が含まれます。この属性が関連付けテーブルです。関連付けテーブルは、eDirectory オブジェクトがリンクされているす

べての接続システムオブジェクトを追跡します。このテーブルは自動的に作成および維持されるため、この情報を手動で編集する必要はほとんどありません。

オブジェクト上の関連付け属性は iManager で \'95\'5c 示できます。

1 iManager で、ツールバーの［*View Objects*］アイコンを選択します。

2 オブジェクトを参照して選択し、［*Modify Object*］を選択します。

3 ［Identity Manager］タブを選択します。

［Identity Manager］タブに関連付け属性が \'95\'5c 示されます。

1.2 ユーザアプリケーション

ユーザアプリケーションはプロビジョニングソリューションです。これは Identity Manager のアドオン製品です。ユーザアプリケーションにより、強力な承認ワークフローが Identity Manager に統合されます。これにより組織は、手動介入が必要ない自動ルールのほかに、人的入力に基づいてもプロビジョニングを決定できます。詳細については、ユーザアプリケーションのドキュメント (http://www.novell.com/documentation/idm35) を参照してください。

1.3 Designer

Designer は、スタンドアロンのクライアントアプリケーションです。Modeler スペース、Palette、ビュー、ポリシービルダ、ドキュメントジェネレータなどの機能で構成されており、生産性の高い環境で Identity Manager ベースのソリューションを設計、テスト、ドキュメント化、および展開できます。Designer の詳細については、『*Designer 2.1 for Identity Manager: Administration Guide (http://www.novell.com/documentation/designer21)* 』を参照してください。

Identity Manager ドライバの管理 2

このセクションでは、Identity Manager ドライバの作成と管理に役立つ情報について説明します。主なトピックは次のとおりです。

2.1 ドライバの作成と設定

使用する各 Identity Manager ドライバに対して、ドライバオブジェクトを作成し、ドライバ設定をインポートする必要があります。ドライバオブジェクトには、設定パラメータとそのドライバのポリシーが含まれます。ドライバオブジェクトの作成時に、ドライバ固有の設定ファイルをインポートします。ドライバ設定には、デフォルトのポリシーセットが含まれています。これらのポリシーは、データ共有モデルを簡単に実装できるようにすることを目的としています。ほとんどの場合は、出荷時のデフォルト設定を使用してドライバを設定してから、環境の要件に応じてドライバの設定を変更します。

ドライバオブジェクトを作成するには、次の 2 つの方法があります。

- ［ドライバの作成］タスク - 1 つのドライバを作成して、ドライバ設定をインポートできます。詳細については、22 ページのセクション 2.1.1「ドライバオブジェクトの作成」を参照してください。
- ［ドライバのインポート］タスク - 複数のドライバを同時に作成して、それらの設定をインポートできます。詳細については、22 ページのセクション 2.1.2「複数のドライバの作成」を参照してください。

2.1.1 ドライバオブジェクトの作成

ドライバ設定 (XML) ファイルを使用して、ドライバが適切に動作するために必要なオブジェクトを作成および設定します。また、ドライバ設定ファイルには、実装に合わせて変更できるポリシーの例も含まれています。

1. iManager で、［*Identity Manager ユーティリティ*］>［*新規ドライバ*］の順に選択します。
2. ドライバを作成するドライバセットを選択し、［*次へ*］をクリックします。

   このドライバを新しいドライバセットに配置する場合は、ドライバセット名、コンテキスト、および関連サーバを指定する必要があります。
3. ［*サーバから環境設定をインポートします (.XML ファイル)*］を選択し、.xml ファイルを選択し、［*次へ*］をクリックします。

   ドライバ設定ファイルは、Identity Manager のインストール時にサーバにインストールされます。
4. プロンプトに従ってドライバ設定のインポートを完了します。

必要な Identity Manager オブジェクトが作成されます。インポート中に同等セキュリティを定義しなかったり、管理ユーザを除外したりした場合、これらの作業は、ドライバオブジェクトのプロパティを変更することによって完了できます。

注 : インポート処理中にエンタイトルメントを有効にしない場合、エンタイトルメントポリシーは作成されません。後でエンタイトルメントを使用する場合は、エンタイトルメントが有効な新しいドライバを作成する必要があります。

2.1.2 複数のドライバの作成

Identity Manager には、複数のドライバを一度に作成する機能が備わっています。このプロセスは、ドライバ設定 (XML) ファイルでは、ドライバを適切に動作させるために必要なオブジェクトが作成および設定され続けるという点で、単一のドライバを作成するプロセスとほぼ同じです。

複数のドライバを同時にインポートする

1. iManager で、［*Identity Manager ユーティリティ*］>［*インポート環境設定*］の順に選択します。
2. 新しいドライバを作成するドライバセットを選択し、［*次へ*］をクリックします。

   これらのドライバを新しいドライバセットに配置する場合は、ドライバセット名、コンテキスト、および関連サーバを指定する必要があります。
3. ドライバセットに追加するアプリケーション設定を選択し、［*次へ*］をクリックします。
4. プロンプトに従って要求されたデータを指定し、［*Next*］*をクリックします。*

   同時にインポートする設定を複数選択した場合、ドライバの設定ページが 1 つずつ表示されます。

ドライバごとに必要な Identity Manager オブジェクトが作成されます。インポート中に同等セキュリティを定義しなかったり、管理ユーザを除外したりした場合、これらの作業は、ドライバオブジェクトのプロパティを変更することによって完了できます。

2.2 Identity Manager 環境での DirXML 1.1a ドライバの管理

DirXML® 1.1a 用に作成された既存のドライバは、Identity Manager でも引き続き動作します。

Identity Manager 3.5.1 に付属のメタディレクトリエンジンは、古いドライバとの後方互換性を備えています (古いドライバシムと環境設定が最新の製品アップデートとパッチで更新されている必要があります)。このエンジンは後方互換性を備えているため、必要に応じて、変更を加えずに Identity Manager サーバ上で DirXML 1.1a ドライバを実行できます。

ただし、iManager プラグインの後方互換性には制限があります。旧ドライバは［ドライバセットの概要］に表示できますが、ドライバを変換しなければドライバ設定は表示または編集できません。［ドライバセットの概要］で DirXML 1.1a ドライバをクリックすると、ドライバが DirXML 1.1a 形式であることが Identity Manager プラグインによって検出され、ウィザードを使用してドライバを 3.5 形式に変換するように要求されます。

既存のドライバセットを変更しない場合は、ウィザードをキャンセルできます。

1.1a 形式の 1.1a ドライバを編集するには、DirXML 1.1a プラグインを使用する必要があります。これを実行するには、1.1a プラグインがインストールされた別の iManager Web サーバを使用する必要があります。Identity Manager に付属している Identity Manager プラグインを使用する場合は、ドライバを Identity Manager 3.5.1 形式に変換してからドライバ設定を編集します。

2.3 ドライバ設定を DirXML 1.1a から Identity Manager3.5.1 形式にアップグレードする

DirXML 1.1a からアップグレードするには、Identity Manager 3.5.1 をインストールする必要があります。Identity Manager 3.5.1 のインストールによって新しいドライバシムがインストールされますが、既存のドライバオブジェクトまたはドライバ設定は変更されません。

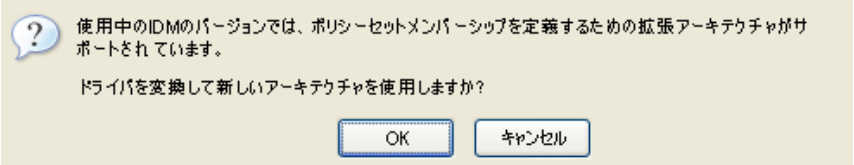
DirXML 1.1a 用に作成された既存のドライバ設定は、Identity Manager で引き続き動作します。ただし、Identity Manager プラグインで編集できるのは、Identity Manager3.5.1 形式のドライバのみです。

重要 : Identity Manager ドライバシムまたはドライバ設定を DirXML 1.1a エンジンで実行することはできません。

DirXML 1.1a ドライバを Identity Manager 形式に変換する場合に役立つウィザードが用意されています。

ウィザードを起動する

1. iManager で、［*Identity Manager*］>［*Identity Manager Overview*］*の順にクリックします。*
2. 変換するドライバを含むドライバセットを選択して、［*検索*］をクリックします。
3. 変換するドライバのアイコンをクリックします。
4. 表示されているメッセージを読み、［*OK*］をクリックします。

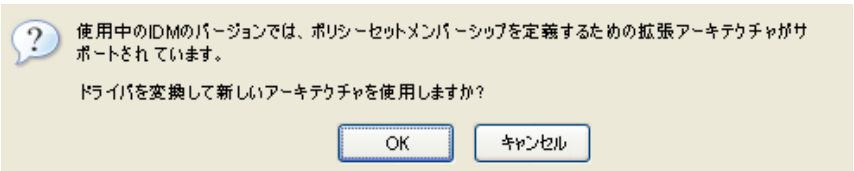


5 複数のドライバをアップグレードする場合は、ステップ 2 からステップ 4 を繰り返します。

2.4 ドライバを Identity Manager 3.5.1 形式にアップグレードする

Identity Manager 3.5.1 には、ポリシーが互いに参照しあう方法についての新しいアーキテクチャが含まれています。この新しいアーキテクチャを利用して、ドライバ設定をアップグレードする必要があります。ドライバをアップグレードしないことも選択できますが、iManager プラグインの後方互換性には制限があります。旧ドライバは［ドライバセットの概要］に表示できますが、ドライバをアップグレードしなければドライバ設定は表示または編集できません。

1 iManager で、［*Identity Manager*］>［*Identity Manager Overview*］*の順にクリックします。*
2 変換するドライバを含むドライバセットを選択して、［*検索*］をクリックします。
3 変換するドライバのアイコンをクリックします。
4 表示されているメッセージを読み、［*OK*］をクリックします。



5 複数のドライバをアップグレードする場合は、ステップ 2 からステップ 4 を繰り返します。

2.5 ドライバの起動、停止、または再起動

1 iManager で、［*Identity Manager*］>［*Identity Manager Overview*］*の順にクリックします。*
2 ドライバが存在するドライバセットを参照し、［*検索*］をクリックします。
3 ステータスを変更するドライバアイコンの右上隅をクリックし、ドライバが停止している場合は［*Start driver*］*をクリックし、ドライバが実行中の場合は［*Stop driver］をクリックします。

2.6 ドライバパラメータ

各ドライバのプロパティには、ドライバパラメータがあります。パラメータには、ドライバ固有の情報が保存されます。SSL の使用有無、ドライバのハートビート設定、ポーリング間隔、認証方法などの情報がパラメータに保存されます。

2.7 インスペクタツールを使用する

iManager には、Identity Manager および Identity Manager オブジェクトと関連付けられたオブジェクトを点検できるツールのセットが含まれています。

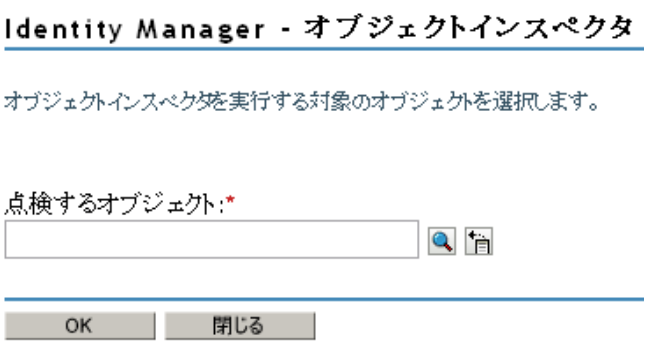
- 25 ページのセクション 2.7.1「オブジェクトを点検する」
- 27 ページのセクション 2.7.2「ドライバを点検する」
- 29 ページのセクション 2.7.3「ドライバのキャッシュファイルを点検する」

2.7.1 オブジェクトを点検する

Identity Manager オブジェクトインスペクタは、オブジェクトが Identity Manager 関係にどのように関わっているかについての詳細情報を確認するために管理者が使用できるツールです。これらの関係には、選択したオブジェクトに関連付けられている接続システム、識別ボールトと接続システム間のデータフローの方法、現在識別ボールトに格納されていて接続システムにある属性値、接続システムドライバ環境設定などが含まれます。

1 ［*Identity Manager*］の役割で［*オブジェクトインスペクタ*］をクリックして、［*Identity Manager インスペクタ*］ページを表示します。

このページで、Identity Manager インスペクタを実行するオブジェクトを選択できます。



2 点検するオブジェクトの完全識別名を指定するか、［*オブジェクトセレクタ*］アイコンをクリックして、希望するオブジェクトを選択します。

iManager には以前選択したオブジェクトのレコード保持されているので、［*オブジェクト履歴*］アイコンをクリックして、以前選択したオブジェクトの一覧から選択することもできます。

3 オブジェクトの選択が終わったら、［*OK*］をクリックします。

［オブジェクトインスペクタ］ページには、接続システムに関する情報が表に表示されます。

図 2-1 オブジェクトインスペクタ

- **削除 :** 接続システムとの関連付けを削除するには、関連付けの左側にあるチェックボックスをオンにして、［*削除*］をクリックします。すべての関連付けを削除するには、［削除］カラムの下にあるチェックボックスをオンにしてから、［*削除*］をクリックします。
- **［更新］:** 接続システムの関連付けを再読み込みし、テーブルを更新するには、［*更新*］を選択します。
- **アクション :** 関連付け参照の左側にあるチェックボックスをオンにして、接続システムを選択します (［新しい関連付けの追加］アクション項目のボックスを選択する必要はありません)。［*アクション*］をクリックして、メニューを展開します。メニューには次のものが含まれます。
  - **ドライバの概要を実行 :** 接続システムのドライバの概要ページがポップアップウィンドウで表示されます。
  - **ドライバセットの概要を実行 :** 接続システムのドライバセットの概要ページがポップアップウィンドウで表示されます。
  - **ドライバの設定 :** 接続システムのドライバのプロパティページがポップアップウィンドウで表示されます。
  - **ドライバセットの設定 :** 接続システムのドライバセットのプロパティページがポップアップウィンドウで表示されます。
  - **新しい関連付けの追加 :** オブジェクトの DirXML 関連付け属性に新しい属性値を追加するのに必要なパラメータがプロンプトされます。
  - **関連付けの編集 :** 接続システムの DirXML 関連付け属性値のパラメータを編集するようにプロンプトされます。
- **コネクタ :** 接続システムの DirXML 関連付け属性値のパラメータを編集するようにプロンプトされます。

  サーバエントリには、ドライバのドライバセットに関連付けられているサーバが表示されます。サーバの右側にある［*編集*］アイコンをクリックすると、サーバのプロパティページがポップアップウィンドウで表示されます。［*クエリ*］アイコンをクリックすると、ドライバフィルタ内のすべてのクラスの属性値がクエリされます。フィルタが大きければ大きいほど、クエリにかかる時間が長くなります。インスペクタが接続システムと通信できない場合、「属性をアプリケーションからクエリできない」というメッセージが表示されます。

  ドライバフィルタの関連付けクラス (グループなど) とそれらの属性 (説明やメンバー) は、サーバエントリの下に一覧表示されます。クラスをクリックして、そのクラス内の定義済み属性のすべての値を確認します。属性をクリックしてその値を確認

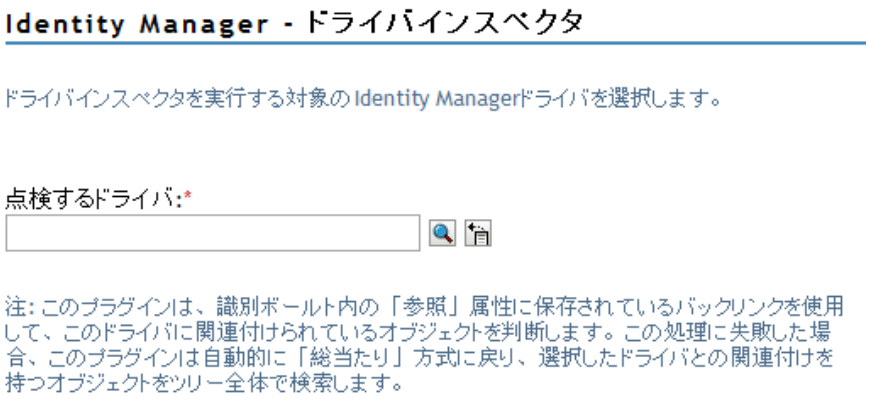
する、または属性の右側にあるエントリをクリックして、識別ボールトの値またはアプリケーションの値を確認することもできます。定義されている値がない場合は、エントリに「値なし」と表示されます。インスペクタが接続システムと通信できない場合、「属性をアプリケーションからクエリできない」というメッセージが表示されます。

- **状態 :** 接続システムの状態に「有効」、「無効」、「処理済み」、「保留中」、「手動」、および「移行」と表示されます。
- **オブジェクト ID:** 接続システムに関連付けられたオブジェクトの ID 値です。接続システムドライバに ID がない場合、このカラムには「*なし*」と表示されます。

2.7.2 ドライバを点検する

Identity Manager ドライバインスペクタは、選択したドライバに関連付けられているオブジェクトに関する詳しい情報を表示できる管理者用のツールです。ドライバインスペクタにアクセスする

1. iManager で、［*Identity Manager*］>［*ドライバインスペクタ*］の順に選択します。
2. 点検するドライバを参照して選択し、［*OK*］をクリックします。



Identity Manager ドライバインスペクタの表には、選択したドライバに関連付けられているオブジェクトに関する情報が表示されます。

図 2-2 Identity Manager ドライバインスペクタの表

- **ドライバ :** 点検されているドライバの［ドライバの概要］を実行するためのリンクです。
- **ドライバセット :** ドライバが格納されているドライバセットの［ドライバセットの概要］を実行するためのリンクです。
- **削除 :** 選択したオブジェクトの関連付けを削除します。
- **［更新］ :** このオプションは、ドライバに関連付けられているすべてのオブジェクトを再読み込みして、表示されている情報を更新する場合に選択します。
- **アクション :** ドライバに関連付けられたオブジェクトに対してアクションを実行します。［アクション］をクリックして、メニューを展開します。メニューには次のものが含まれます。
  - **すべての関連付けを表示 :** ドライバに関連付けられているオブジェクトをすべて表示します。
  - **「使用不可」関連付け用フィルタ :**「使用不可」状態のドライバに関連付けられているオブジェクトをすべて表示します。
  - **「手動」関連付け用フィルタ :**「手動」状態のドライバに関連付けられているオブジェクトをすべて表示します。
  - **「移行」関連付け用フィルタ :**「移行」状態のドライバに関連付けられているオブジェクトをすべて表示します。
  - **「保留中」関連付け用フィルタ :**「保留中」状態のドライバに関連付けられているオブジェクトをすべて表示します。
  - **「処理済み」関連付け用フィルタ :**「処理済み」状態のドライバに関連付けられているオブジェクトをすべて表示します。
  - **「未定義」関連付け用フィルタ :**「未定義」状態のドライバに関連付けられているオブジェクトをすべて表示します。
  - **関連付けの概要 :** ドライバに関連付けられているすべてのオブジェクトの状態を表示します。
- **オブジェクト DN:** 関連付けられているオブジェクトの DN を表示します。

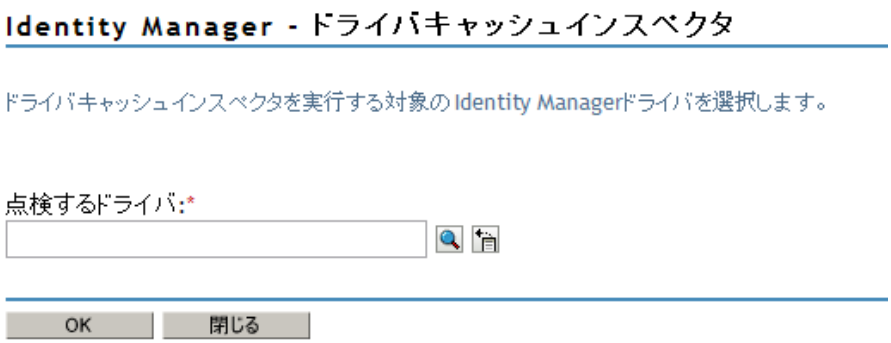
- **ステータス :** オブジェクトの関連付けの状態を表示します。
- **オブジェクト ID:** 関連付けの値を表示します。

2.7.3 ドライバのキャッシュファイルを点検する

Identity Manager ドライバキャッシュインスペクタは、ドライバの停止中に、イベントが保存されているキャッシュファイルに関する情報を表示します。

1 iManager で、［*Identity Manager*］>［*ドライバキャッシュインスペクタ*］の順に選択します。

2 Identity Manager ドライバキャッシュインスペクタを実行するドライバを参照して選択します。



［Identity Manager ドライバキャッシュインスペクタ］ページでは、表形式を使用して、ドライバの停止中に、イベントを保存するキャッシュファイルに関する情報が表示できます。

図 2-3 *Identity Manager ドライバキャッシュインスペクタ*

- **ドライバ :** キャッシュファイルに関連付けられているドライバに対して［ドライバの概要］を実行するためのリンクです。
- **ドライバセット :** ドライバが格納されているドライバセットに対して［ドライバセットの概要］を実行するためのリンクです。
- **ドライバのキャッシュ :** キャッシュファイルのこのインスタンスが含まれるサーバオブジェクトを一覧表示します。

- **［ドライバの起動］/［ドライバの停止］アイコン :** ドライバの現在の状態が表示され、ドライバを起動または停止できます。
- **［編集］アイコン :** 現在選択されているサーバオブジェクトのプロパティを編集できます。
- **削除 :** キャッシュファイル内にある選択した項目を削除します。
- **［更新］:** このオプションは、キャッシュファイルを再読み込みして、表示されている情報を更新する場合に選択します。
- **表示 :** 表示する項目数を制限します。オプションは次のとおりです。
  - 1 ページに 25
  - 1 ページに 50
  - 1 ページに 100
  - その他 : 目的の数を指定できます。
- **アクション :** キャッシュファイル内にあるエントリに対してアクションを実行できます。［アクション］をクリックするとメニューが展開され、次の項目が表示されます。
  - **すべて展開 :** キャッシュファイルに表示されているエントリをすべて展開します。
  - **すべて縮小 :** キャッシュファイルに表示されているエントリをすべて縮小します。
  - **Go To:** キャッシュファイル内にある指定したエントリにアクセスできます。エントリ番号を指定して、［*OK*］をクリックします。
  - **キャッシュの概要 :** キャッシュファイルに保存されているイベントすべての概要を表示します。

2.8 グローバル設定値の使用

グローバル構成値 (GCV) は、ドライバパラメータに似た設定です。グローバル設定値は、ドライバセットに対しても、個々のドライバに対しても指定できます。ドライバに GCV 値がない場合、ドライバはドライバセットからその GCV の値を継承します。

GCV によって、パスワード同期やドライバハートビートなどの Identity Manager 機能の設定、および個々のドライバ環境設定の機能に固有の設定を指定できます。一部の GCV はドライバに付属していますが、ユーザが独自の GCV を追加することもできます。ポリシーでこれらの値を参照すると、ドライバ設定を容易にカスタ \'83\'7d イズできます。

重要 : パスワード同期の設定は GCV ですが、これらを編集する場合は、［GCV］ページではなく、ドライバの［サーバ変数］ページで利用できるグラフィカルインタフェースを使用することをお勧めします。パスワード同期の設定が表示される［サーバ変数］ページには、その他のドライバパラメータと同様のタブとしてアクセスできます。または、［*パスワードの管理*］>［*パスワード同期*］の順にクリックしてドライバを検索し、ドライバ名をクリックすることでアクセスできます。このページは、パスワード同期の各設定のオンラインヘルプを含みます。

Identity Manager のパスワード同期に関連しない GCV を追加、削除、または編集する

1 iManager で、［*Identity Manager*］>［*Identity Manager Overview*］*の順にクリックします。*

2 ドライバセットまたはドライバオブジェクトを参照してクリックし、［*検索*］をクリックします。
3 ドライバの右上隅をクリックし、［*Edit properties*］をクリックします。
4 ［*Global Config Values*］を選択します。
5 ドライバ作成時に設定されたデフォルト値を変更します。
6 追加的な情報を追加するには、［*Edit XML*］をクリックします。
7 ［*Enable XML editing*］をクリックします。
8 XML を追加、削除、または編集し、［*OK*］をクリックして変更を適用します。

2.9 DirXML コ \'83\'7d ンドラインユーティリティの使用

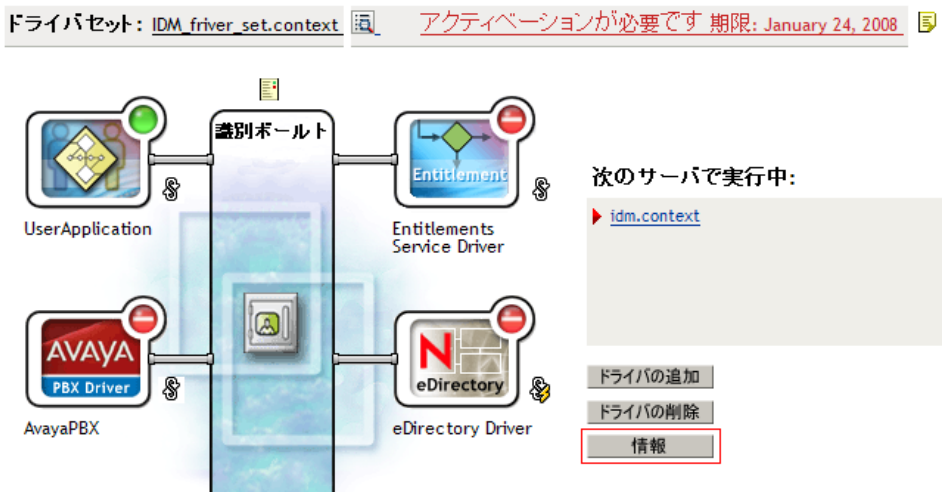
DirXML コマンドラインユーティリティを使用すると、Identity Manager 固有の eDirectory の verb にアクセスできます。このユーティリティは、iManager または Designer の代わりにはなりません。このユーティリティは、主にスクリプトを作成するために使用します。DirXML コマンドラインユーティリティの詳細については、303 ページの付録 A「DirXML コ \'83\'7d ンドラインユーティリティ」を参照してください。日常のタスクには、iManager または Designer を使用します。

2.10 バージョン情報を表示する

バージョン検出ツールでは、次のことができます。

2.10.1 階層構造でバージョン情報を表示する

1 iManager で、［*Identity Manager*］>［*Identity Manager の概要*］の順にクリックし、［*検索*］をクリックしてドライバセットを検索します。
2 ［Identity Manager Overview］画面で［*Information*］をクリックします。



［*Identity Manager ユーティリティ*］>［*バージョン検出*］の順に選択し、ドライバセットを参照して選択して［*OK*］をクリックすることもできます。

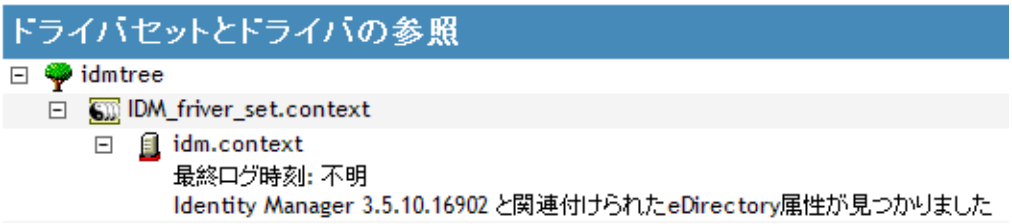
3 トップレベル、または展開していない状態でバージョン情報を \'95\'5c 示します。

展開していない階層 \'95\'5c 示では、次が \'95\'5c 示されます。

- 認証されている eDirectory ツリー
- 選択したドライバセット
- ドライバセットに関連付けられているサーバ

  ドライバセットが 2 つ以上のサーバに関連付けられている場合、各サーバの Identity Manager 情報を表示できます。
- ドライバ

4 サーバアイコンを展開して、サーバに関連するバージョン情報を表示します。



トップレベルのサーバアイコンの展開ビューでは、次が \'95\'5c 示されます。

- 前回のログ時間
- サーバ上で実行中の Identity Manager のバージョン

5 ドライバアイコンを展開して、ドライバに関連するバージョン情報を表示します。

トップレベルのドライバアイコンの展開ビューには、次が \'95\'5c 示されます。

- ドライバ名
- ドライバモジュール (com.novell.nds.dirxml.driver.nds.DriverShimImpl など)

ドライバアイコンの下位にあるサーバの展開ビューには、次が \'95\'5c 示されます。

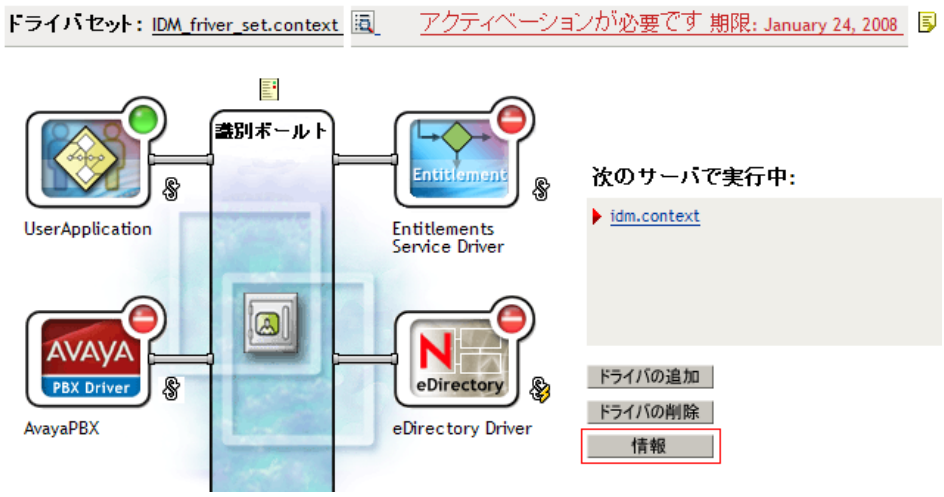
- ドライバ ID
- サーバ上で実行されているドライバのインスタンスのバージョン

2.10.2 バージョン情報をテキストファイルとして表示

Identity Manager では、バージョン情報をファイルに発行できます。この情報はテキスト形式で表示できます。テキスト形式に含まれる情報は、階層ビューと同じです。

1 iManager で、［*Identity Manager*］>［*Identity Manager の概要*］の順にクリックし、［*検索*］をクリックしてドライバセットを検索します。

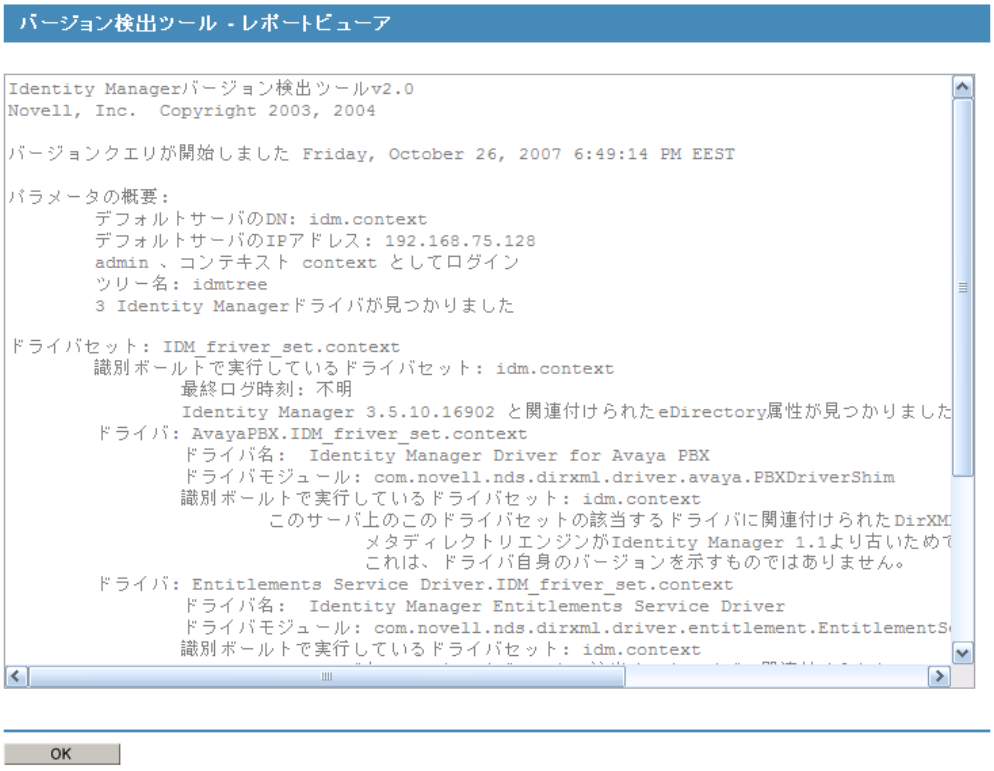
2 ［Identity Manager Overview］画面で［*Information*］をクリックします。



［*Identity Manager ユーティリティ*］>［*バージョン検出*］の順に選択し、ドライバセットを参照して選択して［*情報*］をクリックすることもできます。

3 ［Versioning Discovery Tool］ダイアログ \'83\'7bックスで、［*View*］をクリックします。

情報が［Report Viewer］ウィンドウにテキストファイルとして \'95\'5c 示されます。



2.10.3 バージョン情報を保存する

バージョン情報は、ローカルドライブまたはネットワークドライブにテキストファイルとして保存できます。

1 iManager で、［*Identity Manager*］>［*Identity Manager の概要*］の順にクリックし、［*検索*］をクリックしてドライバセットを検索します。

2 ［Identity Manager Overview］画面で［*Information*］をクリックします。

［*Identity Manager ユーティリティ*］>［*バージョン検出*］の順に選択し、ドライバセットを参照して選択して［*情報*］をクリックすることもできます。

3 ［Versioning Discovery Tool］ダイアログ \'83\'7bックスで、［*Save As*］をクリックします。

4 ［File Download］ダイアログ \'83\'7bックスで、［*Save*］をクリックします。

5 目的のディレクトリに移動し、ファイル名を入力して［*Save*］をクリックします。

Identity Manager によってデータがテキストファイルに保存されます。

2.11 名前付きパスワードの使用

Identity Manager では、特定のドライバで使用される複数のパスワードを安全に保存できます。この機能は、名前付きパスワードと呼ばれます。それぞれのパスワードはキー、または名前でアクセスできます。

また、名前付きパスワード機 \'94\'5c を使用して、ユーザ名などの情報を安全に保存することもできます。

ドライバポリシーで名前付きパスワードを使用するには、実際のパスワードではなくパスワードの名前を使用してパスワードを参照します。その後、メタディレクトリエンジンからドライバにパスワードが送信されます。この節で説明する名前付きパスワードの保存と復元の方法は、ドライバシムを変更することなく、どのドライバでも使用できます。

注 : Lotus Notes 用 Identity Manager ドライバで提供されているサンプル設定には、この方法で名前付きパスワードを使用する例が含まれています。Notes ドライバシムは、名前付きパスワードを使用する他の方法をサポートするようにカスタマイズされており、それらの方法の例も含まれています。詳細については、『*Identity Manager Driver for Lotus Notes*』を参照してください。

この節では、次の項目について説明します。

- 37 ページのセクション 2.11.1「Designer を使用して名前付きパスワードを設定する」
- 37 ページのセクション 2.11.2「iManager を使用して名前付きパスワードを設定する」
- 39 ページのセクション 2.11.3「ドライバポリシーでの名前付きパスワードの使用」
- 39 ページのセクション 2.11.4「DirXML コ\'83\'7dンドラインユーティリティを使用した名前付きパスワードの設定」

2.11.1 Designer を使用して名前付きパスワードを設定する

1 ドライバを選択し、右クリックして［*プロパティ*］を選択します。

2 ［*Named Password*］*を選択し、*［New］をクリックします。

3 ［Named Password］で［*Name*］*を指定します。*

4 ［Named Password］で［*Display name*］*を指定します。*

5 名前付きパスワードを指定し、パスワードを再入力します。

6 ［*OK*］*を 2 回クリックします。*

2.11.2 iManager を使用して名前付きパスワードを設定する

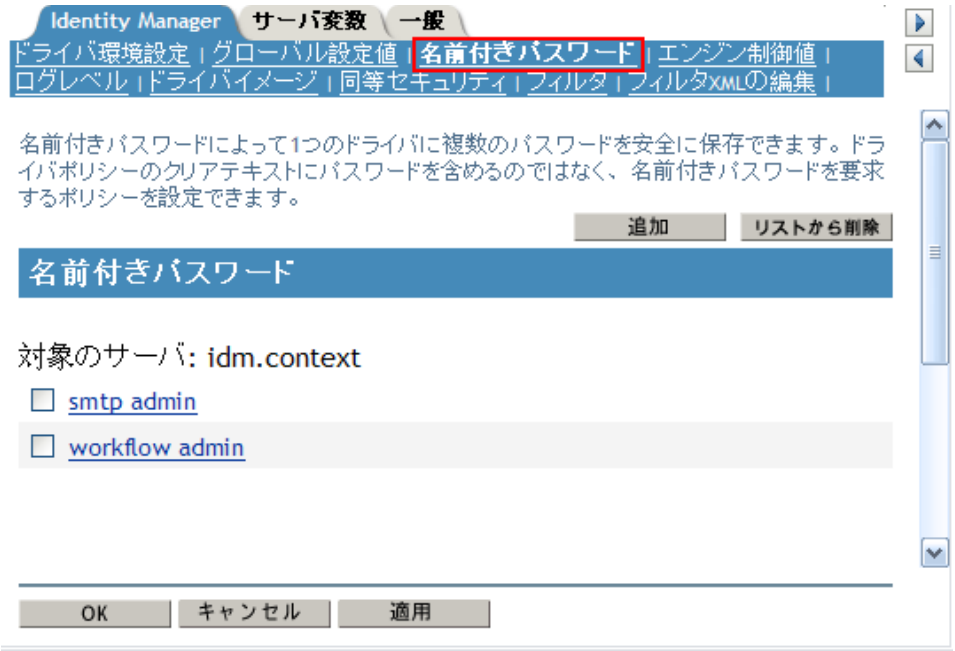
1 iManager で、［*Identity Manager*］> ［*Identity Manager Overview*］*の順にクリックします。*

2 ドライバセットを検索するか、対象のドライバセットを含むコンテナを参照して選択します。ドライバセットのグラフィック画面が \'95\'5c 示されます。

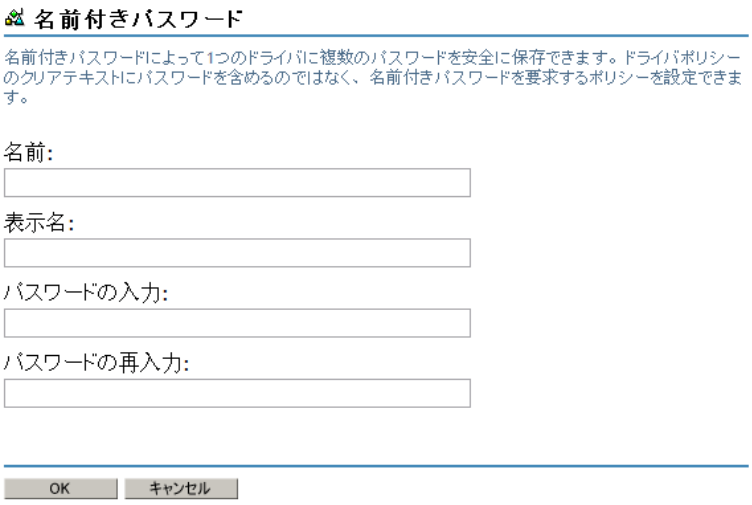
3 ［Identity Manager Overview］画面で、ドライバアイコンの右上隅をクリックし、［*Edit properties*］*をクリックします。*

4 ［Identity Manager］タブの［Modify Object］ページで、［*Named Passwords*］*をクリックします。*

このドライバの現在の名前付きパスワードが一覧表示されている［名前付きパスワード］ページが表示されます。名前付きパスワードを設定していない場合、このリストは空です。



5 名前付きパスワードを追加するには、［*Add*］*をクリックしてフィールドに入力し、*［OK］をクリックします。



6 名前、\'95\'5c 示名、およびパスワードを指定し、［*OK*］*を 2 回クリックします。*

この機 \'94\'5c を使用して、ユーザ名などの情報を安全に保存することもできます。

7 「ドライバを再起動して変更を有効にしますか ?(OK= はい、キャンセル = いいえ)」というメッセージが表示されたら、［*OK*］をクリックします。

8 名前付きパスワードを削除するには、［*削除*］をクリックします。パスワードが削除されます。削除の確認を求めるメッセージは \'95\'5c 示されません。

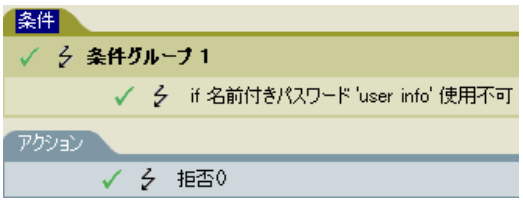
2.11.3 ドライバポリシーでの名前付きパスワードの使用

- 39 ページの 「Policy Builder の使用」
- 39 ページの 「XSLT の使用」

Policy Builder の使用

ポリシービルダを使用すると、名前付きパスワードを呼び出すことができます。新しいルールを作成し、条件として名前付きパスワードを選択します。名前付きパスワードが使用可能か、使用不可かに応じてアクションを設定します。次に、名前付きパスワードのユーザ情報が使用不可である場合に、イベントが拒否される例を示しています。

図 2-4 *名前付きパスワードを使用したポリシー*



XSLT の使用

次の例は、XSLT 内の購読者チャネルのドライバポリシーで、名前付きパスワードを参照する方法を示しています。

```
<xsl:value-of select="
query:getNamedPassword($srcQueryProcessor,mynamedpassword)"
xmlns:query=" http://www.novell.com/nxsl/java/
com.novell.nds.dirxml.driver.XdsQueryProcessor/>
```

2.11.4 DirXML コ \'83\'7d ンドラインユーティリティを使用した名前付きパスワードの設定

- 39 ページの「DirXML コ \'83\'7d ンドラインユーティリティでの名前付きパスワードの作成」
- 41 ページの「DirXML コ \'83\'7d ンドラインユーティリティでの名前付きパスワードの削除」

DirXML コ \'83\'7d ンドラインユーティリティでの名前付きパスワードの作成

1 DirXML コ \'83\'7d ンドラインユーティリティを実行します。

詳細については、303 ページの付録 A「DirXML コ \'83\'7d ンドラインユーティリティ」を参照してください。

2 ユーザ名とパスワードを入力します。

次のオプションリストが \'95\'5c 示されます。

```
DirXML commands
 1: Start driver
 2: Stop driver
 3: Driver operations...
```

```
 4: Driver set operations...
 5: Log events operations...
 6: Get DirXML version
 7: Job operations...
99: Quit
Enter choice:
```

3「3」を入力して、ドライバの操作を選択します。

ドライバの番号付きリストが \'95\'5c 示されます。

4 名前付きパスワードを追加するドライバの番号を入力します。

次のオプションリストが \'95\'5c 示されます。

```
Select a driver operation for:
driver_name
 1: Start driver
 2: Stop driver
 3: Get driver state
 4: Get driver start option
 5: Set driver start option
 6: Resync driver
 7: Migrate from application into DirXML
 8: Submit XDS command document to driver
 9: Submit XDS event document to driver
10: Queue event for driver
11: Check object password
12: Initialize new driver object
13: Passwords operations
14: Cache operations
99: Exit
Enter choice:
```

5「13」を入力して、パスワードの操作を選択します。

次のオプションリストが \'95\'5c 示されます。

```
Select a password operation
 1: Set shim password
 2: Reset shim password
 3: Set Remote Loader password
 4: Clear Remote Loader password
 5: Set named password
 6: Clear named password(s)
 7: List named passwords
 8: Get passwords state
99: Exit
Enter choice:
```

6「5」を入力して、新しい名前付きパスワードを設定します。

次のプロンプトが \'95\'5c 示されます。

```
Enter password name:
```

7 名前付きパスワードの参照に使用する名前を入力します。

8 次のプロンプトが \'95\'5c 示されたら、セキュリティで保護する実際のパスワードを入力します。

```
Enter password:
```

パスワードに入力する文字は \'95\'5c 示されません。

9 次のプロンプトが \'95\'5c 示されたら、パスワードをもう一度入力して確認します。

```
Confirm password:
```

10 パスワードを入力して確認すると、パスワードの操作メニューに戻ります。

このステップが終わったら、オプション 99 を 2 回使用してメニューを終了し、DirXML コ \'83\'7d ンドラインユーティリティを終了します。

DirXML コ \'83\'7d ンドラインユーティリティでの名前付きパスワードの削除

このオプションは、以前に作成した名前付きパスワードが必要なくなった場合に便利です。

1 DirXML コ \'83\'7d ンドラインユーティリティを実行します。

詳細については、303 ページの付録 A「DirXML コ \'83\'7d ンドラインユーティリティ」を参照してください。

2 ユーザ名とパスワードを入力します。

次のオプションリストが \'95\'5c 示されます。

```
DirXML commands
 1: Start driver
 2: Stop driver
 3: Driver operations...
 4: Driver set operations...
 5: Log events operations...
 6: Get DirXML version
 7: Job operations...
99: Quit
Enter choice:
```

3 「3」を入力して、ドライバの操作を選択します。

ドライバの番号付きリストが \'95\'5c 示されます。

4 名前付きパスワードを削除するドライバの番号を入力します。

次のオプションリストが \'95\'5c 示されます。

```
Select a driver operation for:
driver_name
 1: Start driver
 2: Stop driver
 3: Get driver state
 4: Get driver start option
 5: Set driver start option
 6: Resync driver
 7: Migrate from application into DirXML
 8: Submit XDS command document to driver
 9: Submit XDS event document to driver
10: Queue event for driver
11: Check object password
12: Initialize new driver object
13: Passwords operations
```

```
14: Cache operations
99: Exit
Enter choice:
```

5「13」を入力して、パスワードの操作を選択します。

次のオプションリストが \'95\'5c 示されます。

```
Select a password operation
 1: Set shim password
 2: Reset shim password
 3: Set Remote Loader password
 4: Clear Remote Loader password
 5: Set named password
 6: Clear named password(s)
 7: List named passwords
 8: Get passwords state
99: Exit
Enter choice:
```

6 (オプション)「7」を入力して、既存の名前付きパスワードのリストを参照します。

既存の名前付きパスワードのリストが \'95\'5c 示されます。

この手順によって、削除するパスワードが正しいことを確認できます。

7「6」を入力して、1 つまたは複数の名前付きパスワードを削除します。

8 次のプロンプトが \'95\'5c 示されたら、「No」を入力して、1 つの名前付きパスワードを削除します。

```
Do you want to clear all named passwords? (yes/no):
```

9 次のプロンプトが \'95\'5c 示されたら、削除する名前付きパスワードの名前を入力します。

```
Enter password name:
```

削除する名前付きパスワードの名前を入力すると、次のパスワード操作メニューに戻ります。

```
Select a password operation
 1: Set shim password
 2: Reset shim password
 3: Set Remote Loader password
 4: Clear Remote Loader password
 5: Set named password
 6: Clear named password(s)
 7: List named passwords
 8: Get passwords state
99: Exit
Enter choice:
```

10 (オプション)「7」を入力して、既存の名前付きパスワードのリストを参照します。

既存の名前付きパスワードのリストが \'95\'5c 示されます。

このステップによって、削除したパスワードが正しいことを確認できます。

このステップが終わったら、オプション 99 を 2 回使用してメニューを終了し、DirXML コ \'83\'7d ンドラインユーティリティを終了します。

2.12 ドライバオブジェクトとサーバの再関連付け

ドライバオブジェクトはサーバに関連付けられています。

何らかの理由で関連付けが無効になった場合、次のいずれかで示されます。

- Identity Manager サーバ上の eDirectory をアップグレードしたときに、「UniqueSPIException error -783.」というエラーメッセージが \'95\'5c 示される。
- ［Identity Manager Overview］画面のドライバの横にサーバのリストが \'95\'5c 示されない。
- ［Identity Manager Overview］画面のドライバの横にサーバのリストが \'95\'5c 示されるが、名前が文字化けしている。

この問題を解決するには、ドライバオブジェクトとサーバの関連付けを解除したうえで、再度関連付ける必要があります。

iManager にログインし、［Identity Manager の概要］画面のドライバに移動します。アイコンを使用してサーバを削除し、ドライバアイコンの横にあるサーバ名リストにサーバを追加します。削除してから追加することで、サーバがドライバに再度関連付けられます。

2.13 ドライバハートビートの追加

ドライバハートビートは、Identity Manager 2 以降に付属している Identity Manager ドライバの機能です。この使用は必須ではありません。ドライバハートビートは、ドライバパラメータと指定した間隔を使用して設定します。ハートビートパラメータが存在し、間隔値が 0 以外の場合、指定された間隔内に発行者チャネル上で通信が行われていなければ、ドライバはハートビートドキュメントを Metadirectory エンジンに送信します。

ドライバハートビートの目的は、ドライバによる発行者チャネルでの通信が、望ましい頻度で発生していない場合に、一定間隔でアクションを開始できるトリガを提供することです。ハートビートを利用する場合は、ドライバ設定などのツールをカスタマイズする必要があります。Metadirectory エンジンは、ハートビートドキュメントを受け付けますが、それによってアクションを実行することはありません。

ほとんどのドライバでは、ハートビートのドライバパラメータはサンプル設定では使用されていませんが、このパラメータを追加できます。

Identity Manager に付属しないカスタムドライバであっても、ドライバの開発者がハートビートドキュメントをサポートするようドライバを作成していれば、ハートビートドキュメントを提供できます。

ハートビートを設定するには、次の手順を実行します。

1. iManager で、［*Identity Manager*］>［*Identity Manager Overview*］*の順にクリックします。*
2. ドライバセットを参照して選択し、［*検索*］をクリックします。
3. ［Identity Manager Overview］画面で、ドライバアイコンの右上隅をクリックし、［*Edit properties*］*をクリックします。*
4. ［Identity Manager］*タブで、*［*Driver Configuration*］*をクリックし、*［*Drive Paramter*］*までスクロールし、*［*Heart Beat*］*または同様の \'95\'5c 示名を探します。*

   ハートビートのドライバパラメータがすでに存在する場合は、その間隔を変更して変更を保存すると、設定は完了です。

間隔の値は 1 未満には設定できません。値 0 は、この機 \'94\'5c がオフになっていることを意味します。

通常、時間の単位は分ですが、ドライバの中には秒を使用するなど、分以外を実装しているものもあります。

5 ハートビートのドライバパラメータが存在しない場合は、［Edit XML］をクリックします。

6 次の例のようなドライバパラメータのエントリを、<publisher-options> の子として追加します。(AD ドライバでは、これを <driver-options> の子にします)。

```
<pub-heartbeat-interval display-name="Heart Beat">10</pub-
heartbeat-interval>
```

ヒント：ドライバを再起動してもハートビートドキュメントが生成されない場合は、XML 内のドライバパラメータの場所を確認してください。

7 変更を保存し、ドライバが停止および再起動されることを確認します。

ドライバパラメータを追加した後で、グラフィカルビューを使用して間隔を編集できます。もう 1 つの方法は、間隔のグローバル構成値 (GCV) への参照を作成する方法です。他のグローバル設定値と同様に、ドライバハードビートは、各ドライバオブジェクトのレベルではなくドライバセットレベルで設定できます。ドライバに特定のグローバル設定値がなく、ドライバセットにグローバル設定値がある場合、ドライバはドライバセットの値を継承します。

次に、Notes ドライバによって送信されたハートビートのステータスドキュメントの例を示します。

```
<nds dtdversion="2.0" ndsversion="8.x">
  <source>
    <product build="20031112_1037" instance="blackcap"
version="2.0">DirXML Driver for Lotus Notes</product>
    <contact>Novell, Inc.</contact>
  </source>
  <input>
    <status level="success" type="heartbeat"/>
  </input>
</nds>
```

2.14 Identity Manager のプロセスの \'95\'5c 示

Identity Manage のプロセスイベントを表示するには、DSTRACE を使用します。これは、Identity Manager をテストおよびトラブルシューティングする場合にのみ使用してください。ドライバの運用中に DSTRACE を実行すると、Identity Manager サーバ上の使用率が増え、イベントの処理が非常に低速になる場合があります。

Identity Manager のプロセスを DSTRACE で確認するには、値をドライバセットおよびドライバに追加します。これは、Designer および iManager で実行できます。

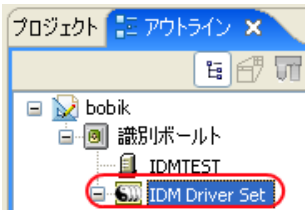
- 45 ページのセクション 2.14.1「Designer でのトレースレベルの追加」
- 47 ページのセクション 2.14.2「iManager でのトレースレベルの追加」
- 48 ページのセクション 2.14.3「ファイルへの Identity Manager のプロセスのキャプチャ」

2.14.1 Designer でのトレースレベルの追加

トレースレベルは、ドライバセットまたは各ドライバに追加できます。

ドライバセット

1 Designer 内で開いているプロジェクトの［*アウトライン*］ビューで、ドライバセットを選択します。



2 右クリックして［*Properties*］*を選択し*、［5. Trace］をクリックします。

3 トレースパラメータを設定し、［*OK*］をクリックします。ドライバセットのトレースパラメータの詳細については、45 ページの 表 2-1 を参照してください。

ドライバセットトのトレースレベルを設定すると、すべてのドライバが DSTRACE ログに記述されます。

表 2-1 *ドライバセットのトレースパラメータ*

パラメータ	説明
ドライバのトレースレベル	ドライバのトレースレベルを上げると、DSTRACE に表示される情報量が増えます。 トレースレベル 1 はエラーを示しますが、エラーの原因にはなりません。パスワード同期の情報を \'95\'5c 示するには、トレースレベルを 5 に設定します。
XSL のトレースレベル	DSTRACE では、XSL イベントが表示されます。このトレースレベルは、XSL スタイルシートのトラブルシューティング時にのみ設定します。XSL 情報を \'95\'5c 示しない場合は、レベルをゼロに設定します。
Java デバッグポート	開発者は Java デバッガをアタッチできます。
Java トレースファイル	このフィールドの値が設定されている場合、ドライバセットのすべての Java 情報がファイルに書き込まれます。このフィールドの値は、そのファイルのパッチです。 ファイルを指定すると、Java 情報がこのファイルに書き込まれます。Java をデバッグする必要がない場合、このフィールドを空白のままにします。

パラメータ	説明
トレースファイルのサイズ制限	Java トレースファイルの制限を設定できます。ファイルサイズを無制限に設定した場合、ディスクスペースがなくなるまでファイルサイズが増加します。 **注 :** トレースファイルは複数のファイルに作成されます。Identity Manager により自動的に最大のファイルサイズが 10 で割られ、10 個のファイルが作成されます。これらのファイルを組み合わせたサイズが、トレースファイルの最大サイズと等しくなります。

ドライバ

1. Designer 内の開いているプロジェクトの［アウトライン］ビューで、ドライバを選択します。
2. 右クリックして［*プロパティ*］を選択し、［*8. Trace (8. トレース)*］をクリックします。
3. トレースパラメータを設定し、［*OK*］をクリックします。これらのパラメータの詳細については、46 ページの 表 2-2 を参照してください。

   ドライバにのみパラメータを設定した場合、そのドライバの情報のみが DSTRACE ログに記述されます。

表 2-2 *ドライバのトレースパラメータ*

パラメータ	説明
トレースレベル	ドライバのトレースレベルを上げると、DSTRACE に表示される情報量が増えます。 トレースレベル 1 はエラーを示しますが、エラーの原因にはなりません。パスワード同期の情報を \'95\'5c 示するには、トレースレベルを 5 に設定します。 ［*ドライバセットの設定を使用する*］を選択した場合、値はドライバセットから取得されます。
トレースファイル	選択したドライバに対して、ファイル名および Identity Manager 情報を書き込む場所を指定します。 ［*ドライバセットの設定を使用する*］を選択した場合、値はドライバセットから取得されます。

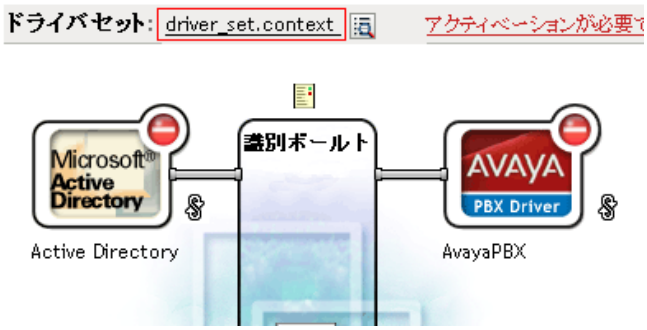
パラメータ	説明
トレースファイルのサイズ制限	Java トレースファイルの制限を設定できます。ファイルサイズを無制限に設定した場合、ディスクスペースがなくなるまでファイルサイズが増加します。 **注 :** トレースファイルは複数のファイルに作成されます。Identity Manager により自動的に最大のファイルサイズが 10 で割られ、10 個のファイルが作成されます。これらのファイルを組み合わせたサイズが、トレースファイルの最大サイズと等しくなります。 ［*ドライバセットの設定を使用する*］を選択した場合、値はドライバセットから取得されます。
トレース名	ドライバトレースメッセージの前に、ドライバ名の代わりに入力した値が付きます。ドライバ名が長い場合に使用します。

2.14.2 iManager でのトレースレベルの追加

トレースレベルは、ドライバセットまたは各ドライバに追加できます。

ドライバセット

1. iManager で、［*Identity Manager*］>［*Identity Manager Overview*］*の順に選択します。*
2. ドライバセットを参照し、［*検索*］をクリックします。
3. ドライバセット名をクリックします。



4. ドライバセットの［*その他*］タブを選択します。
5. トレースパラメータを設定し、［*OK*］をクリックします。これらのパラメータの詳細については、45 ページの 表 2-1 を参照してください。

ドライバ

1. iManager で、［*Identity Manager*］>［*Identity Manager の概要*］の順に選択します。
2. ドライバがある場所でドライバセットを参照し、［*検索*］をクリックします。
3. ドライバの右上隅をクリックし、［*Edit properties*］*をクリックします。*

4 ドライバの［*その他*］タブを選択します。

5 トレースパラメータを設定し、［*OK*］をクリックします。詳細については、46 ページの 表 2-2 を参照してください。

注 : ［*Use setting from Driver Set*］*のオプションは、iManager には存在しません。*

2.14.3 ファイルへの Identity Manager のプロセスのキャプチャ

Identity Manager のプロセスは、ドライバのパラメータを使用して、または DSTRACE を介してファイルに保存されます。ドライバのパラメータは、トレースファイルパラメータです。

DSTRACE を介してキャプチャされたドライバプロセスは、Identity Manager エンジンで発生するプロセスです。リモートローダを使用する場合は、Identiry Manager エンジンのトレースをキャプチャするとの同時にリモートローダのトレースをキャプチャする必要があります。

次の方法は、異なる OS プラットフォーム上で DSTRACE を使用して、Identity Manager のプロセスをキャプチャおよび保存する場合に役立ちます。

NetWare

DSTRACE.NLM を使用して、トレースメッセージをシステムコンソールに表示する、またはファイル (SYS:\SYSTEM\DSTRACE.LOG) に書き込みます。DSTRACE.NLM により、［DSTRACE Console］という名前の画面にトレースメッセージが表示されます。

1 サーバコン \'83\'5cールで「DSTRACE.NLM」と入力します。

これにより、メモリに DSTRACE.NLM がロードされます。

2 サーバコン \'83\'5cールで「DSTRACE SCREEN ON」と入力します。

［DSTRACE Console］画面にトレースメッセージが \'95\'5c 示されます。

3 サーバコンソールで「DSTRACE FILE ON」と入力します。

これにより、DSTRACE Console に送信されたトレースメッセージが DSTRACE.LOG にキャプチャされます。

4 サーバコン \'83\'5cールで「DSTRACE -ALL」と入力します。

すべてのトレースのフラグをオフにします。

5 サーバコンソールで「DSTRACE +DXML DSTRACE +DVRS」と入力します。

Identity Manager イベントが \'95\'5c 示されます。

6 サーバコンソールで「DSTRACE +TAGS DSTRACE +TIME」と入力します。

メッセージタグおよびタイムスタンプが \'95\'5c 示されます。

7 ［DSTRACE Console］画面に切り替え、渡されるイベントを確認します。

8 サーバコン \'83\'5cールに再度切り替えます。

9 サーバコン \'83\'5cールで「DSTRACE FILE OFF」と入力します。

ログファイルへのトレースメッセージのキャプチャが停止されます。ファイルへの情報のログも停止されます。

10 テキストエディタで DSTRACE.LOG を開き、変更したイベントまたはオブジェクトを検索します。

Windows

1. ［コントロールパネル］>［NDS Services］>［dstrace.dlm］の順に開き、［*Start*］*をクリックします。*

   ［NDS Server Trace Utility］という名前のウィンドウが開きます。
2. ［*Edit*］>［Options］の順に選択し、［*Clear All*］*をクリックします。*>

   これにより、すべてのデフォルトのフラグがクリアされます。
3. ［*DirXML*］>［*DirXML ドライバ*］の順に選択します。
4. ［OK］をクリックします。
5. ［*ファイル*］>［*新規*］の順に選択します。
6. ファイル名および DSTRACE 情報を保存する場所を指定し、［Open］をクリックします。
7. イベントが発生するのを待機します。
8. ［*File*］>［*Close*］*の順に選択します。*

   これにより、ログファイルへの情報の書き込みが停止されます。
9. テキストエディタでファイルを開き、変更したイベントまたはオブジェクトを検索します。

UNIX

1. 「ndstrace」と入力し、ndstrace ユーティリティを起動します。
2. 「set ndstrace=nodebug」と入力します。

   現在設定してあるすべてのトレースのフラグをオフにします。
3. 「set ndstrace on」と入力します。

   トレースメッセージがコン \'83\'5cールに \'95\'5c 示されます。
4. 「set ndstrace file on」と入力します。

   eDirectory がインストールされたディレクトリにある ndstrace.log ファイルに、トレースメッセージがキャプチャされます。デフォルトでは、/var/nds です。
5. 「set ndstrace=+dxml」と入力します。

   Identity Manager イベントが \'95\'5c 示されます。
6. 「set ndstrace=+dvrs」と入力します。

   Identity Manager ドライバイベントが \'95\'5c 示されます。
7. イベントが発生するのを待機します。
8. 「set ndstrace file off」と入力します。

   これにより、ファイルへの情報のログが停止されます。
9. 「exit」と入力し、ndstrace ユーティリティを終了します。
10. テキストエディタでファイルを開きます。変更されたイベントまたはオブジェクトを検索します。

iMonitor

iMonitor を使用すると、Web ブラウザから DSTRACE 情報を参照できます。Identity Manager が実行されている場所は関係ありません。iMonitor を実行するファイルは、次のとおりです。

- NDSIMON.NLM - NetWare で動作します。
- NDSIMON.DLM - Windows で動作します。
- ndsimonitor - UNIX で動作します。

1. http://*server_ip*:8008&/nds から iMonitor にアクセスします。

   ポート 8008 はデフォルトのポートです。
2. 管理者権限を使用してユーザ名およびパスワードを入力し、［*Login*］*をクリックします。*
3. 左側の［*Trace Configuration*］*を選択します。*
4. ［*Clear All*］*をクリックします。*
5. ［DirXML］>［DirXML Drivers］の順に選択します。
6. ［*Trace On*］*をクリックします。*
7. 左側の［*Trace History*］*を選択します。*
8. ドキュメントの［Modification Time of Current］をクリックし、ライブトレースを \'95\'5c 示します。
9. より頻繁に情報を \'95\'5c 示するには、［*Refresh Interval*］*を変更します。*
10. 左側の［*Trace Configuration*］*を選択し、*［Trace Off］をクリックしてトレースをオフにします。
11. ［トレース履歴］を選択すると、トレースの履歴を表示できます。ファイルはタイムスタンプで区別されます。

HTML ファイルのコピーが必要な場合、デフォルトの場所は次のとおりです。

- NetWare: SYS:\SYSTEM\ndsimon\DSTRACE*.htm
- Windows: *Drive_letter*:\Novell\NDS\ndsimon\dstrace*.htm
- UNIX: /var/nds/dstrace/*.htm

リモートローダ

リモートローダサービスを実行しているマシンで発生するイベントをキャプチャできます。

1. アイコンをクリックして、リモートローダコンソールを起動します。
2. ドライバインスタンスを選択して、［*編集*］をクリックします。
3. ［*トレースレベル*］を 3 以上に設定します。
4. トレースファイルの場所とファイルを指定します。
5. そのファイルで使用できるディスク容量を指定します。
6. ［*OK*］を 2 回クリックして、変更を保存します。

以下のスイッチを使用して、コマンドラインからトレースを有効にすることもできます。詳細については、66 ページのセクション 3.4「リモートローダを設定する」を参照してください。

表 2-3 *コマンドライントレーススイッチ*

オプション	2 次名	パラメータ	説明
-trace	-t	整数	トレースレベルを指定します。これはアプリケーションシムをホストする場合にのみ使用できます。トレースレベルは Identity Manager サーバで使用されているレベルと同じです。 例 : -trace 3 or -t3
-tracefile	-tf	ファイル名	トレースメッセージを書き込むファイルを指定します。トレースメッセージは、トレースレベルがゼロよりも大きい場合にファイルに書き込まれます。トレースメッセージは、トレースウィンドウが開いていなくてもファイルに書き込まれます。 例 : -tracefile c:\temp\trace.txt または -tf c:\temp\trace.txt
-tracefilemax	-tfm	サイズ	トレースファイルがディスク上で使用できる最大サイズを指定します。このオプションを指定すると、tracefile オプションを使用して指定した名前の付いたトレースファイルと、最大 9 個の追加ロールオーバーファイルが生成されます。ロールオーバーファイルには、メインのトレースファイル名と「_n」に基づいた名前が付けられます。「n」は 1 ～ 9 の値になります。 サイズのパラメータはバイト数です。K (キロバイト)、M (メガバイト)、または G (ギガバイト) のサフィックスを使用してサイズを指定します。 リモートローダの起動時にトレースファイルのデータが指定した最大サイズよりも大きい場合、10 ファイルすべてのロールオーバーが完了するまで、トレースファイルのデータは指定した最大値よりも大きいままとなります。 例 : -tracefilemax 1000M または -tfm 1000M

3 リモートローダを使用するかしないかを判断する

Identity Manager には、Identity Manager の機能をアプリケーション間に拡張できる追加機能があります。この機能はリモートローダと呼ばれています。リモートローダを使用すると、アプリケーションと同じサーバに識別ボールトおよびメタディレクトリエンジンがインストールされていなくても、ドライバがアプリケーションにアクセスできるようになります。Identity Manager をインストールする際の計画プロセスの一部として、リモートローダを使用するかしないかを決める必要があります。このセクションでは、リモートローダとは何か、およびリモートローダをインストールおよび設定する方法について説明します。

3.1 概要

メタディレクトリエンジンのインストールを設定する方法には、2 つあります。図 3-1 には、最初の方法が示されています。これには、同じサーバにインストールされ、稼動している識別ボールト、メタディレクトリエンジン、およびドライバシムが表示されています。ドライバシムは、アプリケーションおよびメタディレクトリエンジンと通信するように設定されています。

図 3-1 *同じサーバにインストールされているすべてのコンポーネント*

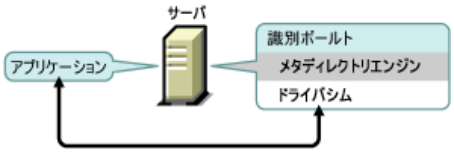
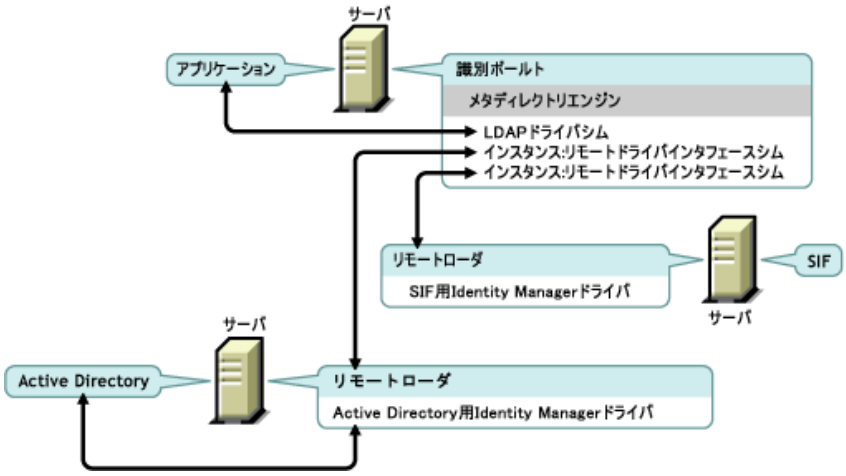


図 3-2 には、両方の設定が示されています。LDAP ドライバは、メタディレクトリエンジンや識別ボールトと同じサーバにインストールされています。SIF ドライバおよび Active Directory ドライバは、リモートローダとは違うサーバにインストールされています。リモートローダを使用すると、同じサーバに識別ボールトおよびメタディレクトリエンジンがインストールされていなくても、ドライバがアプリケーションにアクセスできるようになります。

図 3-2 リモートローダを使用するシステム



リモートローダを使用すると、別の場所の異なるプロセスで、メタディレクトリエンジンが識別ボールトとデータを交換できるようになります。以下の場合が含まれます。

- **メタディレクトリエンジンを実行しているサーバ上の別のプロセスとして実行する：**

  メタディレクトリエンジンは、eDirectory™ プロセスの一部として実行されます。Identity Manager ドライバは、メタディレクトリエンジンを実行しているサーバで実行できます。実際に、これらは Metadirectory エンジンと同じプロセスの一部として実行できます。

  ただし、戦略的な理由やトラブルシューティングを簡素化するために、Identity Manager ドライバをサーバ上の別のプロセスとして実行することができます。

  ドライバが別のプロセスとして実行されている場合、リモートローダにより、Metadirectory エンジンとドライバ間の通信チャネルが提供されます。

- **メタディレクトリエンジンを実行していないサーバで実行する：**

  一部の Identity Manager ドライバは、メタディレクトリエンジンを実行している場所では実行できません。リモートローダを使用すると、メタディレクトリエンジンを特定の環境で実行しつつ、Identity Manager ドライバを別の環境のサーバで実行できます。たとえば、NetWare® サーバ上では Active Directory ドライバは実行できません。メタディレクトリエンジンを NetWare サーバで実行している間に、リモートローダを Active Directory サーバで実行できます。

  - **シナリオ：別々のサーバ。**メタディレクトリエンジンが NewWare サーバ上で実行している場合。Active Directory 用の Identity Manager ドライバを実行する必要があります。このドライバは、Active Directory 環境で実行する必要があるため、NetWare サーバ上では実行できません。Windows 2003 サーバにリモートローダをインストールして実行します。リモートローダは、Active Directory ドライバと Metadirectory エンジンの間の通信チャネルになります。
  - **シナリオ：ホスト以外。**メタディレクトリエンジンが Solaris* で実行している場合。ユーザアカウントのプロビジョニングを行う NIS システムと通信する必要があります。通常、NIS システムはメタディレクトリエンジンをホストしません。NIS システム上にリモートローダと NIS 用の Identity Manager ドライバをインストールします。NIS システム上のリモートロードが NIS ドライバを実行し、Metadirectory エンジンと NIS ドライバがデータを交換できるようにします。

Novell® では、可能な場合、ドライバで使用する際にはリモートローダの設定を使用することをお勧めします。接続システムがメタディレクトリエンジンと同じサーバにある場合でも、リモートローダを使用してください。リモートローダの設定でドライバを実行することで、以下の利点が得られます。

- eDirectory がドライバシムが遭遇する例外から保護されます。
- ドライバコマンドをリモートアプリケーションまたはデータベースにオフロードすることで、メタディレクトリエンジンを実行しているサーバのパフォーマンスが向上します。
- メタディレクトリエンジンがインストールされていないサーバで追加のドライバを実行できます。

3.2 安全なデータ転送の提供

リモートローダを使用する予定の場合、まず、リモートローダとメタディレクトリエンジンの間で安全なデータ転送を確立します。これには、SSL (セキュアソケットレイヤ) を使用して、リモートローダとメタディレクトリエンジンの間で接続を確立する必要があります。

この設定を行うには、以下のタスクを実行します。

- 55 ページのセクション 3.2.1「サーバ証明書の作成」
- 56 ページのセクション 3.2.2「自己署名証明書のエクスポート」

証明書のある場所がわからない場合は、簡単に新しい証明書を作成できます。

ただし、SSL サーバ証明書がすでに存在し、SSL 証明書を使用した経験がある場合は、新しい証明書を作成して使用するのではなく、既存の証明書を使用できます。

サーバがツリーに参加すると、eDirectory によって次のデフォルトの証明書が作成されます。

- SSL CertificateIP
- SSL CertificateDNS

3.2.1 サーバ証明書の作成

1 Novell iManager で、［*Novell Certificate Server*］>［*Create Server Certificate*］*の順にクリックします。*

2 証明書を所有するサーバを選択し、証明書にニックネーム (remotecert など) を付けます。

重要 : 証明書のニックネームにはスペースを使用しないことをお勧めします。たとえば、「remote cert」ではなく、「remotecert」を使用します。

また、証明書のニックネームは書き留めておいてください。このニックネームは、ドライバのリモート接続パラメータの KMO 名に使用します。

---

3 ［Creation method］は［*Standard*］*のままにし、*［Next］をクリックします。

4 ［Summary］の画面を確認し、［*Finish*］*をクリックして*［Close］をクリックします。

これでサーバ証明書が作成されました。56 ページのセクション 3.2.2「自己署名証明書のエクスポート」に進みます。

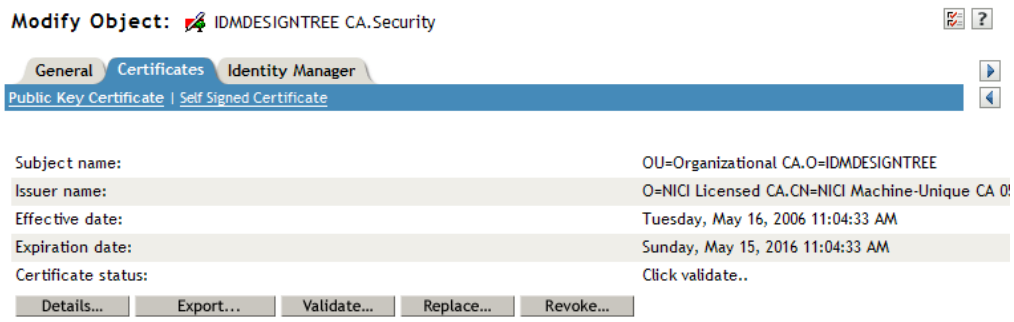
3.2.2 自己署名証明書のエクスポート

1 iManager で、［*eDirectory Administration*］> ［*Modify Object*］*の順にクリックします。*

2 ［Security］コンテナの［Certificate Authority］を参照して選択し、［*OK*］*をクリックします。*

認証局 (CA) にはツリー名に基づいた名前 (Treename-CA.Security) が付けられます。

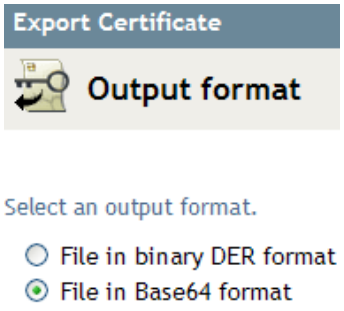
3 ［*Certificates*］*タブをクリックして*［Self-Signed Certificate］、［*Export*］*の順にクリックします。*>



4 Export Certificate Wizard で、［*No*］*を選択して*［Next］をクリックします。

秘密鍵は証明書と一緒にエクスポートしません。

5 ［*Base64 形式のファイル*］(IDMDESIGNTREE CA.b64 など) を選択し、［*次へ*］をクリックします。



重要 : Windows 2003 R2 SP1 32 ビットサーバでリモートローダを実行していいる場合、証明書は Base64 形式にする必要があります。DER 形式を使用すると、リモートローダが Identity Manager エンジンに接続できません。

6 ［*Save the exported certificate to a file*］*へのリンクをクリックし、ファイル名を指定して、場所を指定してから*［Save］をクリックします。

7 ［Save As］ダイアログ \'83\'7bックスで、このファイルをローカルディレクトリにコピーします。

8 ［*閉じる*］をクリックします。

3.3 リモートローダをインストールする

この章では、以下について説明します。

- 65 ページのセクション 3.3.7「HR-UX、AS/400、OS/390、または z/OS へのリモートローダのインストール」

3.3.1 要件

各ドライバに対して、接続されたシステムが使用可能であり、関連する API が提供されている必要があります。各システムに固有のオペレーティングシステムおよび接続システムの要件については、Identity Manager ドライバのマニュアル (http://www.novell.com/documentation/idm35drivers) を参照してください。

3.3.2 サポートされているドライバ

リモートローダがサポートされているドライバを以下に示します。

- Active Directory*
- Avaya* PBX
- 区切りテキスト
- Exchange 5.5
- GroupWise®
- JDBC*
- JMS
- LDAP
- Linux* および UNIX* 用ドライバ
- Lotus Notes*
- NT ドメイン
- PeopleSoft* 3.7
- PeopleSoft 5.2
- Remedy* ARS
- SAP* HR
- SAP User Management
- スクリプティング
- SIF*
- SOAP
- WorkOrder
- 手動タスクサービス
- Null サービス
- LoopBack

各ドライバの詳細については、Identity Manager 3.5 ドライバマニュアルの Web サイト (http://www.novell.com/documentation/idm35drivers/) を参照してください。

リモート機能が備わっていないドライバでは、リモートローダは使用できません。例

- eDirectory

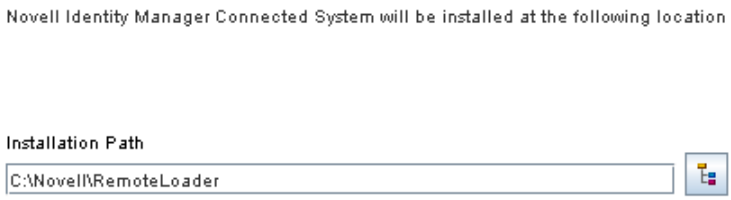
- 役割ベースエンタイトルメント
- ユーザアプリケーション

3.3.3 リモートローダの Windows サーバへのインストール

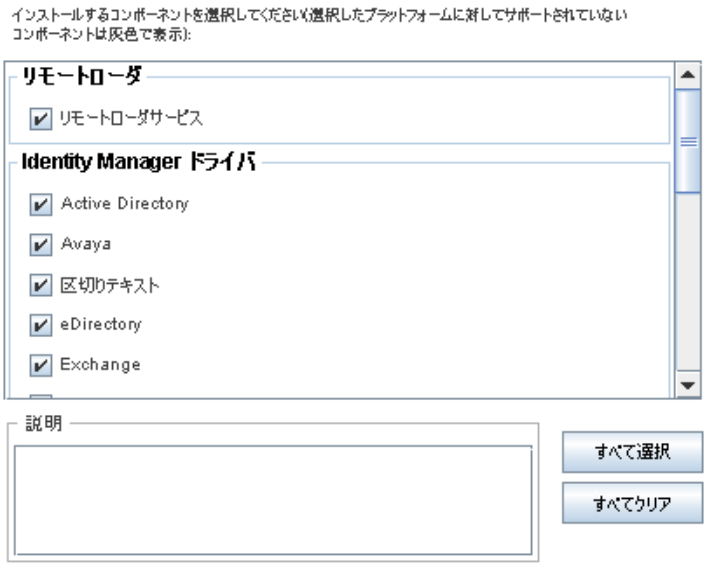
リモートローダのコンソールでは、rlconsole.exe を使用して、dirxml_remote.exe とインタフェースが確立されます。dirxml_remote.exe は、Windows 上で実行している Identity Manager ドライバとメタディレクトリエンジンを通信できるようにする実行可能ファイルです。

1. Novell のダウンロード Web サイト (http://download.novell.com) から、Identity_Manager_3_5_1_NW_Win.iso をダウンロードします。
2. IDM3.5.1_NW_Win:\nt\install.exe にある Windows 用の Identity Manager インストールプログラムを実行します。
3. インストールプログラムを実行する言語を選択して、［*OK*］をクリックします。
4. ［ようこそ］ページが表示されたら、［*次へ*］をクリックします。
5. 使用許諾書に同意して、［概要］ページを表示します。
6. ［Identity Manager のインストール］ダイアログボックスで、［*Novell Identity Manager 接続システム*］以外のすべてのコンポーネントを選択解除して、［*次へ*］をクリックします。

7. 接続システム (リモートローダとリモートドライバシム) の場所を選択し、［*Next*］をクリックします。



8 ［*Remote Loader Service*］とリモートドライバシム (ドライバ) を選択し、［Next］をクリックします。



9 実行要件を確認して、インストールする製品を \'95\'5c 示し、［*Finish*］をクリックします。

10 デスクトップに［Remote Loader Console］アイコンを作成するかどうかを選択します。

11 ［*完了*］をクリックして、インストールを実行します。

3.3.4 Linux にリモートローダをインストールする

リモートローダは、GUI インタフェースまたはコマンドラインを使用してインストールできます。

- 60 ページの 「GUI を使用して Linux にリモートローダをインストールする」
- 61 ページの 「コマンドラインを使用して Linux にリモートローダをインストールする」

GUI を使用して Linux にリモートローダをインストールする

1 Novell のダウンロード Web サイト (http://download.novell.com) から、Identity_Manager_3_5_1_Linux.iso をダウンロードします。

2 ホストコンピュータで、root としてログインします。

3 Linux に GUI をインストールするには、ルートディレクトリにある install.bin ファイルをクリックします。インストールファイルをターミナルモードで実行するか、それとも表示モードで実行するかを尋ねるメッセージが表示されます。［*ターミナル*］を選択します。

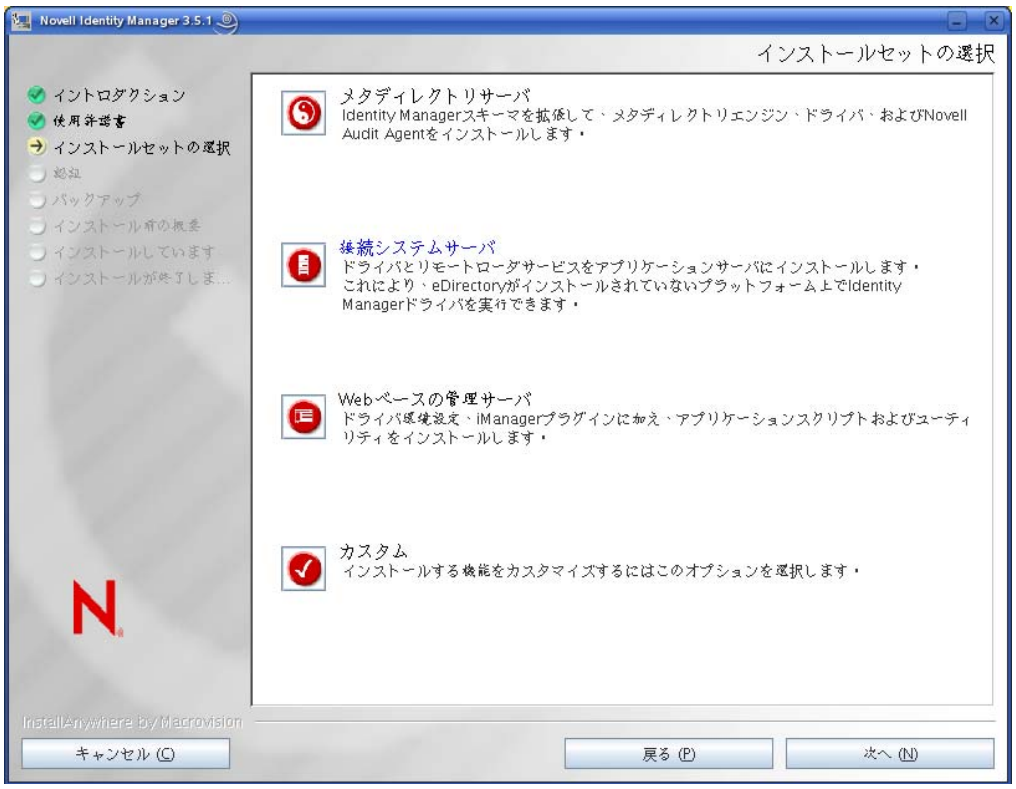
install.bin ファイルにより X ウィンドウが存在するかどうかがチェックされ、存在する場合は、Identity Manager の Linux 用 GUI インストールプログラムが起動されます。

4 インストールプログラムを実行する言語を選択して、［*OK*］をクリックします。

5 ［ようこそ］ページが表示されたら、［*次へ*］をクリックします。

6 使用許諾書に同意して、［次へ］をクリックします。

7 ［*接続システムサーバ*］をクリックして、［*次へ*］をクリックします。



8 アクティベーション要件を確認して、インストールする製品を表示し、［*インストール*］をクリックします。

9 ［概要］画面の内容を確認し、［*完了*］をクリックします。

コマンドラインを使用して Linux にリモートローダをインストールする

1 Novell のダウンロード Web サイト (http://download.novell.com) から、Identity_Manager_3_5_1_Linux.iso をダウンロードします。

2 ホストコンピュータで、root としてログインします。

3 IDM3.5.1_Lin:\linux\setup\idm_linux.bin にあるインストールファイルを実行します。

4 使用許諾契約に同意した後で、<Enter> キーを押し、次の［Choose Install Set］ページを \'95\'5c 示します。

```
================================================================================
インストールセットの選択
------------

このインストーラでインストールするインストール セットを選択してください。

  ->1- メタディレクトリサーバ
    2- 接続システムサーバ
    3- Webベースの管理サーバ

    4- カスタマイズ...

インストール セットの番号を入力するか、デフォルトを使用する場合は <ENTER> キーを押してください。
     :
```

5 「2」と入力して［接続システムサーバ］を選択し、<Enter> キーを押します。

6 ［インストール前の概要］画面で、インストールすることを選択したコンポーネントを確認して、<Enter> キーを押します。

```
================================================================================
インストール前の概要
----------

続行する前に次を確認してください:

インストール セット
    接続システムサーバ

製品コンポーネント:
    LDAPドライバ,
    SAPドライバ,
    JDBCドライバ,
    区切りテキストドライバ,
    Lotus Notesドライバ,
    リモートローダ,
    Groupwiseドライバ,
    Avayaドライバ,
    SOAPドライバ,
    Remedyドライバ,
    PeopleSoftドライバ,
    JMSドライバ,
    Linux/Unix双方向ドライバ,
    Linux/Unix設定ドライバ,
    RACFドライバ,
    トップシークレットドライバ


続行するには <ENTER> キーを押します。:
```

3.3.5 UNIX にリモートローダをインストールする

rdxml は、Solaris、Linux、または AIX* 環境で実行されている Identity Manager ドライバと Metadirectory エンジンが通信できるようにする実行ファイルです。

リモートローダは、GUI インタフェースまたはコマンドラインを使用してインストールできます。

- 63 ページの 「GUI を使用して UNIX にリモートローダをインストールする」
- 63 ページの 「コマンドラインを使用して UNIX にリモートローダをインストールする」

GUI を使用して UNIX にリモートローダをインストールする

1 Novell のダウンロード Web サイト (http://download.novell.com) から、Identity_Manager_3_5_1_Unix.iso をダウンロードします。

2 プラットフォームに合わせて次のインストールファイルの 1 つを実行します。

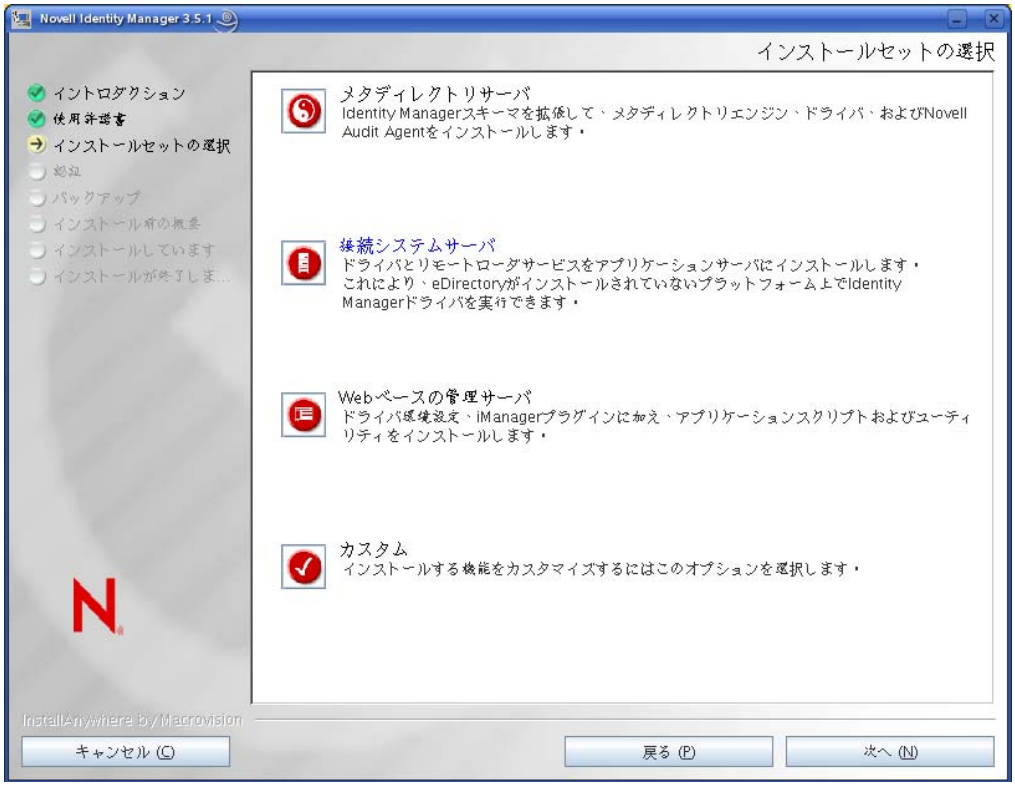
- IDM3.5.1_Unix:\aix\setup\idm_aix.bin -i gui
- IDM3.5.1_Unix:\solaris\setup\idm_solaris.bin -i gui

3 インストールプログラムを実行する言語を選択して、［*OK*］をクリックします。

4 ［ようこそ］ページが表示されたら、［*次へ*］をクリックします。

5 使用許諾書に同意して、［次へ］をクリックします。

6 ［*接続システムサーバ*］をクリックして、［*次へ*］をクリックします。



7 アクティベーション要件を確認して、インストールする製品を表示し、［*インストール*］をクリックします。

8 ［概要］画面の内容を確認し、［*完了*］をクリックします。

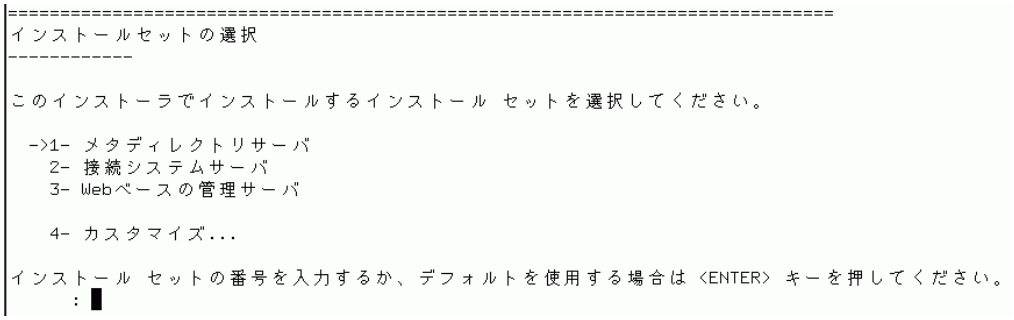
コマンドラインを使用して UNIX にリモートローダをインストールする

1 Novell のダウンロード Web サイト (http://download.novell.com) から、Identity_Manager_3_5_1_Unix.iso をダウンロードします。

2 プラットフォームに合わせて次のインストールファイルの 1 つを実行します。

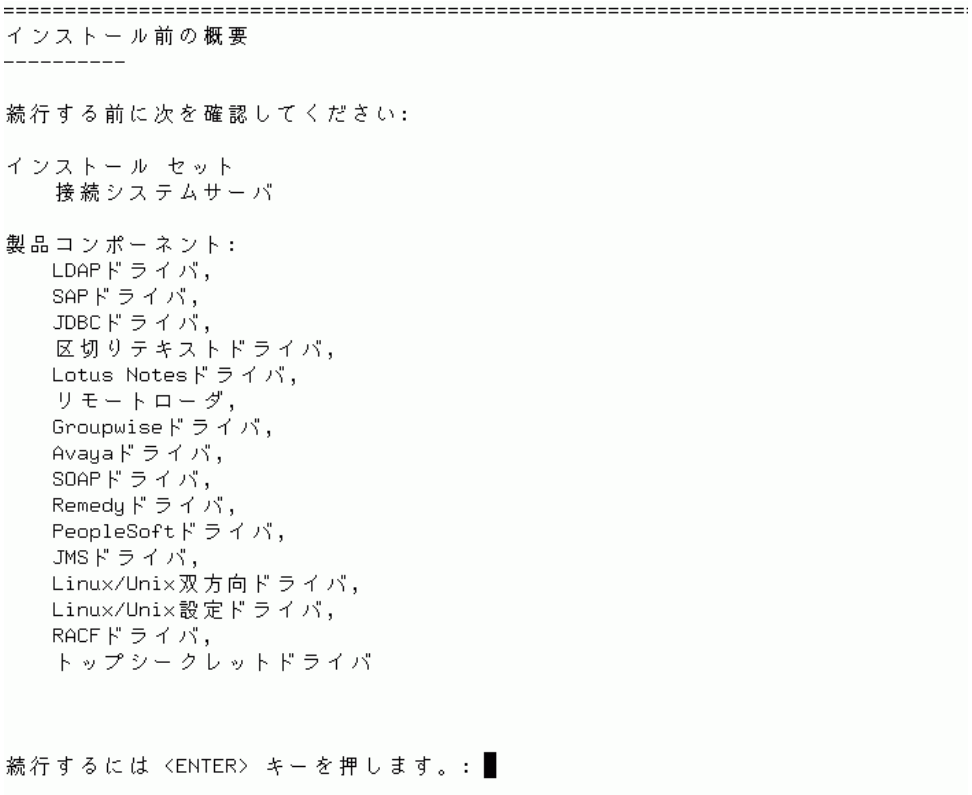
- IDM3.5.1_Unix:\aix\setup\idm_aix.bin
- IDM3.5.1_Unix:\solaris\setup\idm_solaris.bin

3 使用許諾契約に同意した後で、<Enter> キーを押し、次の［Choose Install Set］ページを \'95\'5c 示します。



4「2」と入力して［*接続システムサーバ*］を選択し、<Enter> キーを押します。

5［インストール前の概要］画面で、インストールすることを選択したコンポーネントを確認して、<Enter> キーを押します。



3.3.6 Java リモートローダを UNIX、Linux、または AIX にインストールする

dirxml_jremote は、純粋な Java リモートローダです。これは、1 つのサーバで実行しているメタディレクトリエンジンと、rdxml または dirxml_jremote を実行していない場所で実行している Identity Manager ドライバとの間で、データを交換するために使用されます。

互換性がある JRE*(最低 1.4.0、1.4.2 以降を推奨) および Java Sockets がインストールされていればどのシステムでも動作しますが、正式にサポートされているのは次のものです。

- HP-UX*
- AS/400*
- OS/390
- z/OS
- および、すべてのサポートされているメタディレクトリエンジンプラットフォーム

このセクションの説明は、Identity Manager がダウンロードされていると仮定しています。Identity Manager をダウンロードする必要がある場合は、Novell のダウンロード Web サイト (http://download.novell.com) にアクセスしてください。

1. ホストシステムで、Java 1.4.x JDK*/JRE が使用可能なことを確認します。
2. dirxml_jremote.tar.gz ファイルを、リモートローダを実行しているサーバ上の希望する場所にコピーします。このファイルは、IDM_3.5.1_Linux:\java_remoteloader\dirxml_jremote.tar.gz にあります。

   例、/usr/dirxml
3. dirxml_jremote.tar.gz を解凍して展開します。

   例、gunzip dirxml_jremote.tar.gz または tar xvf dirxml_jremote.tar
4. アプリケーションシム .jar ファイルを、dirxml_jremote.tar が抽出されたときに作成された lib サブディレクトリにコピーします。
5. 以下のいずれかを実行して、dirxml_jremote スクリプトをカスタマイズします。
   - Java 実行可能ファイルに、PATH 環境変数を使用してアクセスできることを確認します。詳細については、75 ページのセクション 3.5「Solaris、Linux、または AIX での環境変数の設定」を参照してください。
   - dirxml_jremote スクリプトを編集して、Java 実行可能ファイルへのパスを Java を実行するスクリプトラインに追加します。
6. アプリケーションシムで使用するサンプルの config8000.txt ファイルを設定します。詳細については、69 ページのセクション 3.4.2「設定ファイルを作成して、リモートローダを設定する」を参照してください。

3.3.7 HR-UX、AS/400、OS/390、または z/OS へのリモートローダのインストール

HP-UX、AS/400、OS/390、および z/OS のプラットフォームには、Java リモートローダが必要です。

1. Java リモートローダを実行するターゲットシステムにディレクトリを作成します。
2. ステップ 1 で作成したディレクトリに、Identity Manager CD またはダウンロードイメージから /java_remoteloader ディレクトリ内の適切なファイルをコピーします。

プラットフォーム	ファイル
HP-UX AS/400 z/OS OS/390	dirxml_jremote.tar.gz dirxml_jremote.tar.gz dirxml_jremote_mvs.tar dirxml_jremote_mvs.tar

3 HP-UX、AS/400、または z/OS の場合は、dirxml_jremote ファイルを解凍します。

4 コピーした tar 形式ファイルを解凍 (untar) します。

これで Java リモートローダを設定する準備ができました。tar ファイルにはドライバが含まれないため、ドライバを手動で lib ディレクトリにコピーする必要があります。lib ディレクトリは、解凍を行ったディレクトリの下にあります。

MVS の詳細については、dirxml_jremote_mvs.tar ファイルを解凍し、usage.html ドキュメントを参照してください。

3.4 リモートローダを設定する

リモートローダは、.dll、.so、または .jar ファイルに含まれる Identity Manager アプリケーションシムをホストできます。Java リモートローダは Java ドライバシムのみをホストします。ネイティブ (C++) ドライバシムはロードまたはホストしません。

リモートローダコンソールユーティリティというグラフィカルユーティリティを使用して、またはコマンドラインから Windows 上にドライバを設定できます。

- 66 ページのセクション 3.4.1「Windows でのリモートローダの設定」
- 69 ページのセクション 3.4.2「設定ファイルを作成して、リモートローダを設定する」

3.4.1 Windows でのリモートローダの設定

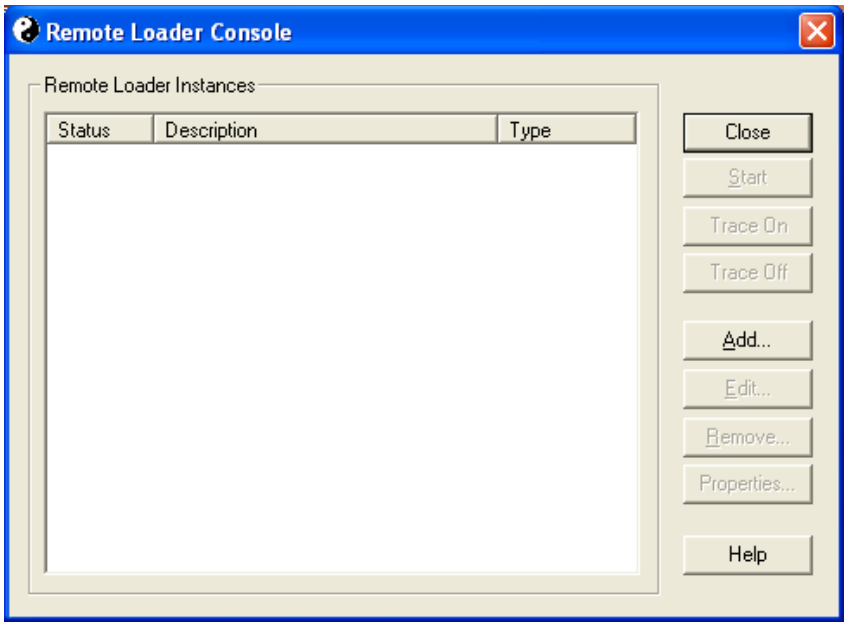
リモートローダコンソールユーティリティを使用すると、Windows サーバでリモートローダを実行しているすべての Identity Manager を管理できます。このユーティリティは Identity Manager のインストール時にインストールされます。

Identity Manager にアップグレードすると、コンソールによりリモートローダの既存のインスタンスが検出され、インポートされます。(自動的にインポートするには、ドライバ設定をリモートローダのディレクトリ (通常は c:\novell\remoteloader) に保存する必要があります)。これでコン \'83\'5cールを使用してリモートドライバを管理できます。

1 デスクトップにある［*リモートローダコンソール*］アイコンをダブルクリックして、リモートローダコンソールを起動します。

リモートローダコンソールを使用すると、リモートローダの各インスタンスを起動、停止、追加、削除、および編集できます。

2 このサーバ上の自分のドライバにリモートローダのインスタンスを追加するには、［*追加*］をクリックします。



3 *リモートドライバの設定*パラメータを指定します。

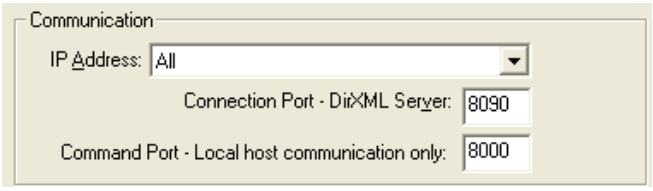
3a リモートローダのインスタンスを識別する説明を指定します。

3b ドライバに適したシムを参照して選択します。

3c 設定ファイルの名前を指定します。

リモートローダのコン \'83\'5cールは設定パラメータをこのテキストファイルに保存し、実行時にこれらのパラメータを使用します。

4 *通信*パラメータを指定します。



4a リモートローダがメタディレクトリサーバからの接続をリッスンする IP アドレスを指定します。

4b リモートローダがメタディレクトリサーバからの接続をリッスンする TCP ポートを指定します。

この接続におけるデフォルトの TCP/IP ポートは 8090 になります。新しいインスタンスを作成するたびに、デフォルトポート番号が自動的に 1 ずつ増えます。

4c リモートローダが Stop や Change Trace Level などのコマンドをリッスンする TCP ポート番号を指定します。

特定のコンピュータ上で実行されるリモートローダの各インスタンスには、異なるコマンドポート番号を設定する必要があります。デフォルトのコマンドポートは 8000 です。新しいインスタンスを作成するたびに、デフォルトポート番号が自動的に 1 ずつ増えます。

注 : 異なる接続ポートとコ \'83\'7d ンドポートを指定することによって、複数のドライバインスタンスをホストする同じサーバ上で、リモートローダの複数のインスタンスを実行できます。

---

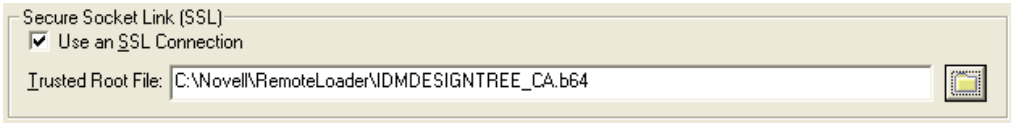
5 *リモートローダパスワード*を指定します。

このパスワードは、ドライバのリモートローダインスタンスへのアクセスを制御するために使用します。このパスワードは、［Identity Manager ドライバ設定］ページの［*リモートローダパスワードの入力*］フィールドで指定したパスワードと同じ大文字と小文字の組み合わせで指定する必要があります。

6 *ドライバオブジェクトパスワード*を指定します。

リモートローダでは、このパスワードを使用してメタディレクトリサーバに対する認証が行われます。このパスワードは、［Identity Manager ドライバ設定］ページの［*ドライバオブジェクトパスワード*］フィールドで指定したパスワードと同じ大文字と小文字の組み合わせで指定する必要があります。

7 *Secure Socket Link* パラメータを指定します。

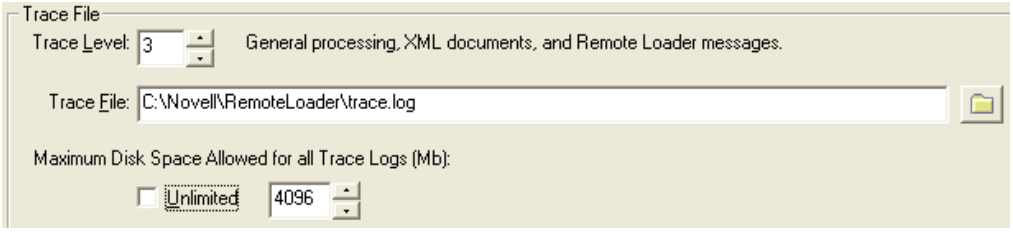


7a リモートローダとメタディレクトリサーバ間の転送データを暗号化している場合は、［*SSL 接続を使用*］を選択します。

7b ルート認証局ファイルを参照して選択します。

これは、eDirectory ツリーの組織認証局からエクスポートされた自己署名証明書です。詳細については、56 ページのセクション 3.2.2「自己署名証明書のエクスポート」を参照してください。

8 *トレースファイル*パラメータを指定します。



8a リモートローダおよびドライバからの情報メッセージを含むトレースウィンドウを表示するために、1 以上のトレースレベルを指定します。

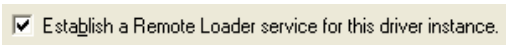
最も一般的な設定は、トレースレベル 3 です。トレースレベルを 0 に設定すると、トレースウィンドウは表示されません。

8b トレースメッセージを書き込むトレースファイル名を指定します。

特定のマシンで実行しているリモートローダの各インスタンスには、個別のトレースファイルを使用する必要があります。トレースメッセージは、トレースレベルがゼロよりも大きい場合にだけトレースファイルに書き込まれます。

8c このインスタンスのトレースファイルに使用できる最大のディスク容量を指定します。

9 リモートローダをサービスとして設定する場合は、［*Establish a Remote Loader service for this driver instance (このドライバインスタンスのリモートローダサービスを設定する)*］を選択します。



このオプションを有効にすると、コンピュータの起動時にオペレーティングシステムにより自動的にリモートローダが起動されます。

10 ［*OK*］をクリックして、設定情報を保存します。

パラメータを変更する必要がある場合は、以下の手順を実行します。

1 リモートローダコンソールの［*説明*］カラムから、リモートローダインスタンスを選択します。

2 ［*Stop*］*をクリックしてリモートローダのパスワードを入力し、*［OK］をクリックします。

3 ［*編集*］をクリックして、設定情報を変更します。これらはリモートローダインスタンスを追加するときに入力するのと同じフィールドです。

4 ［*OK*］をクリックして、変更を保存します。

3.4.2 設定ファイルを作成して、リモートローダを設定する

リモートローダを実行するには、設定ファイル (LDAPShim.txt など) が必要です。このファイルを作成するための GUI インタフェースがあるのは、Windows だけです。設定ファイルは、コマンドラインのオプションを使用して作成または編集できます。以下のステップに従って、設定ファイルの基本的なパラメータを設定します。追加的なパラメータの詳細については、317 ページの付録 B「リモートローダの設定のオプション」を参照してください。

1 設定ファイルを作成するには、テキストエディタを開きます。

2 (オプション)-description オプションを使用して、説明を指定します。

オプション	2 次名	パラメータ	説明

-description	-desc	短い説明	トレースウィンドウのタイトルと Novell Audit のログに使用される短い説明の文字列 (SAP など) を指定します。
			例 :
			`-description SAP`
			`-desc SAP`
			設定ファイルには、リモートローダコンソールによって長い形式が配置されます。長い形式 (たとえば -description) または短い形式 (たとえば -desc) のいずれかを使用できます。

3 -commandport オプションを使用して、リモートローダインスタンスによって使用される TCP/IP ポートを指定します。

オプション	2 次名	パラメータ	説明

-commandport	-cp	ポート番号	リモートローダのインスタンスにより制御目的で使用される TCP/IP ポートを指定します。リモートローダインスタンスがアプリケーションシムをホストしている場合、コマンドポートは、別のリモートローダインスタンスが、シムをホストしているインスタンスと通信するポートになります。リモートローダインスタンスが、アプリケーションシムをホストしているインスタンスにコマンドを送信する場合、コマンドポートは管理インスタンスがリッスンしているポートになります。コ \'83\'7d ンドポートが指定されていない場合のデフォルトポートは 8000 です。複数の接続ポートとコ \'83\'7d ンドポートを指定することで、異なるドライバインスタンスをホストしている同じサーバ上でリモートローダの複数のインスタンスを実行できます。
			例 :
			`-commandport 8001`
			`-cp 8001`

4 -connection オプションを使用して、Identity Manager のリモートインタフェースシムで実行されているメタディレクトリサーバに接続するためのパラメータを指定します。

「-connection “ *パラメータ* [パラメータ] [パラメータ]” 」と入力します。

たとえば、次のいずれかを入力します。

```
-connection "port=8091 rootfile=server1.pem"
-conn "port=8091 rootfile=server1.pem"
```

パラメータはすべて二重引用符で囲む必要があります。パラメータには、次のようなものがあります。

オプション	2 次名	パラメータ	説明

-connection	-conn	接続設定文字列	Identity Manager リモートインタフェースシムを実行しているメタディレクトリサーバに接続するための接続パラメータを指定します。リモートローダのデフォルトの接続方法は、SSL を使用した TCP/IP です。この接続におけるデフォルトの TCP/IP ポートは 8090 になります。同じサーバで、リモートローダの複数のインスタンスを実行できます。リモートローダの各インスタンスは別々の Identity Manager アプリケーションシムインスタンスをホストします。リモートローダの各インスタンスに別々の接続ポートとコ \'83\'7d ンドポートを指定することによって、リモートローダーの複数のインスタンスを区別します。
			
			例 :
			`-connection Ågport=8091 rootfile=server1.pemÅh`
			`-conn Ågport=8091 rootfile=server1.pemÅh`

port		10 進数のポート番号	必須パラメータです。リモートローダがリモートインタフェースシムからの接続をリッスンする TCP/IP ポートを指定します。 例 : `port=8090`

address		IP アドレス	オプションのパラメータです。リモートローダが特定のローカル IP アドレスをリッスンするよう指定します。これは、リモートローダをホストするサーバが複数の IP アドレスを持ち、リモートローダが 1 つのアドレスのみをリッスンしなければならない場合に便利です。
			
			次の 3 つの操作を選択してください。
			`address=address numberaddress=ÅflocalhostÅfDonÅft use this parameter`
			
			アドレスを使用しない場合、リモートローダはすべてのローカル IP アドレスをリッスンします。
			
			例 :
			`address=137.65.134.83`

rootfile			条件付きパラメータです。SSL を実行していて、リモートローダがネイティブドライバと通信する必要がある場合、次を入力します。 rootfile=’*trusted certname*’

オプション	2 次名	パラメータ	説明
keystore			条件付きパラメータです。.jar ファイルに含まれる Identity Manager アプリケーションシムにのみ使用します。 リモートインタフェースシムによって使用される証明書の発行者のルート認証局証明書を含む Java キーストアのファイル名を指定します。通常、これはリモートインタフェースシムをホストしている eDirectory ツリーの認証局です。 SSL を実行していて、リモートローダが Java ドライバと通信する必要がある場合、次の key-value ペアを入力します。 keystore='*keystorename*' storepass='*password*'
-storepass		storepass	.jar ファイルに含まれる Identity Manager アプリケーションシムにのみ使用します。keystore パラメータで指定した Java キーストアのパスワードを指定します。 例 : `storepass=mypassword` このオプションは Java リモートローダにのみ適用されます。

5 (オプション) -trace オプションを使用して、トレースパラメータを指定します。

オプション	2 次名	パラメータ	説明

-trace	-t	整数	トレースレベルを指定します。これはアプリケーションシムをホストする場合にのみ使用できます。トレースレベルはメタディレクトリサーバで使用されているレベルと同じです。
			
			例 :
			`-trace 3`
			`-t 3`

6 (オプション) -tracefile オプションを使用して、トレースファイルを指定します。

オプション	2 次名	パラメータ	説明

-tracefile	-tf	ファイル名	トレースメッセージを書き込むファイルを指定します。トレースメッセージは、トレースレベルがゼロよりも大きい場合にファイルに書き込まれます。トレースメッセージは、トレースウィンドウが開いていなくてもファイルに書き込まれます。
			
			例 :
			`-tracefile c:\temp\trace.txt`
			`-tf c:\temp\trace.txt`

7 (オプション) -tracefilemax オプションを使用して、トレースファイルのサイズを制限します。

オプション	2 次名	パラメータ	説明

-tracefilemax	-tfm	サイズ	トレースファイルがディスク上で使用できる最大サイズを指定します。このオプションを指定すると、tracefile オプションを使用して指定した名前の付いたトレースファイルと、最大 9 個の追加「ロールオーバ」ファイルが生成されます。ロールオーバファイルには、メインのトレースファイル名と「*_n*」に基づいた名前が付けられます。「n」は 1 ～ 9 の値になります。
			
			サイズのパラメータはバイト数です。K (キロバイト)、M (メガバイト)、または G (ギガバイト) のサフィックスを使用してサイズを指定します。
			
			リモートローダの起動時にトレースファイルのデータが指定した最大サイズよりも大きい場合、10 ファイルすべてのロールオーバーが完了するまで、トレースファイルのデータは指定した最大値よりも大きいままとなります。
			
			例 :
			`-tracefilemax 1000M`
			`-tfm 1000M`
			
			この例では、トレースファイルは 1GB までです。

8 -class オプションを使用してクラスを指定するか、-module オプションを使用してモジュールを指定します。

オプション	2 次名	パラメータ	説明

-class	-cl	Java クラス名	管理する Identity Manager アプリケーションシムの Java クラス名を指定します。
			
			たとえば、Java ドライバに対しては次のいずれかを入力します。
			`-class com.novell.nds.dirxml.driver.ldap.LDAPDriverShim`
			`-cl com.novell.nds.dirxml.driver.ldap.LDAPDriverShim`
			
			Java では、キーストアを使用して証明書を読み取ります。-class **オプションと** -module オプションは互いに排他的で、どちらか一方のみ使用できます。
			
			Java クラス名のリストを参照するには、317 ページの付録 B「リモートローダの設定のオプション」の 324 ページの 表 B-2 を参照してください。

オプション	2 次名	パラメータ	説明

-module	-m	モジュール名	ホストされる Identity Manager アプリケーションシムを含むモジュールを指定します。
			
			たとえば、ネイティブドライバに対しては次のいずれかを入力します。
			`-module "c:\Novell\RemoteLoader\Exchange5Shim.dll"`
			`-m "c:\Novell\RemoteLoader\Exchange5Shim.dll"`
			
			または
			`-module "usr/lib/dirxml/NISDriverShim.so"`
			`-m "usr/lib/dirxml/NISDriverShim.so"`
			
			-module オプションでは、ルートファイル証明書が使用されます。-module **オプションと** -class オプションは互いに排他的で、どちらか一方のみ使用できます。

9 ファイルに名前を付けて保存します。

リモートローダの実行中に一部の設定を変更することができます。それらの設定の一部のリストについては、表 3-1 を参照してください。それらの設定の完全なリストについては、317 ページの付録 B「リモートローダの設定のオプション」を参照してください。

表 3-1 *選択済みリモートローダパラメータ*

パラメータ	説明
-commandport	リモートローダのインスタンスを指定します。
-config	環境設定ファイルを指定します。
-javadebugport	指定されたポートでリモートローダのインスタンスがデバッグを有効にするよう指定します。
-password	認証用のパスワードを指定します。
-service	インスタンスをサービスとしてインストールします。(Windows のみ)。
-tracechange	トレースレベルを変更します。
-tracefilechange	書き込み先のトレースファイルの名前を変更します。
-unload	リモートローダのインスタンスをアンロードします。
-window	リモートローダインスタンスでトレースウィンドウのオン / オフを切り替えます。(Windows のみ)。

3.5 Solaris、Linux、または AIX での環境変数の設定

リモートローダをインストールした後で、rdxml の現在のディレクトリを変更する環境変数 RDXML_PATH を設定できます。設定後、このディレクトリは、以降に作成するファイルの基本パスになります。RDXML_PATH 変数の値を設定するには、次のコマンドを入力します。

- set RDXML_PATH=path
- export RDXML_PATH

3.6 リモートローダを起動する

リモートローダを起動する方法は、各プラットフォームによって異なります。

- 75 ページのセクション 3.6.1「Windows でリモートローダを起動する」
- 77 ページのセクション 3.6.2「Solaris、Linux、または AIX でリモートローダを起動する」

3.6.1 Windows でリモートローダを起動する

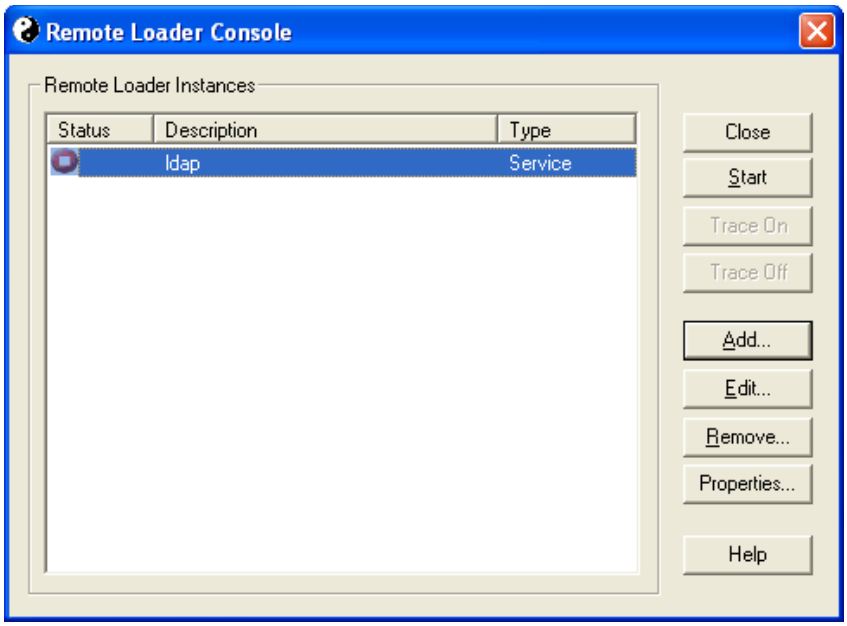
リモートローダは、［リモートローダコンソール］アイコンまたはコマンドラインから起動できます。

- 75 ページの 「リモートローダコンソールから起動する」
- 76 ページの 「Windows のコマンドラインから起動する」

リモートローダコンソールから起動する

1 デスクトップ上の［*リモートローダコンソール*］アイコンをクリックします。

2 ドライバインスタンスを選択し、［*Start*］*をクリックします。*



Windows のコマンドラインから起動する

コマンドライン機能は、dirxml_remote.exe を実行することで使用できます。デフォルトでは、このファイルは c:\novell\RemoteLoader\dirxml_remote.exe にあります。コマンドプロンプトで、次の操作を行います。

1. リモートローダのパスワードを設定します。パスワードコマンドのオプションについては、77 ページの 表 3-2 を参照してください。

   dirxml_remote -config *path_to_config_file* -sp *password password*

2. リモートローダを起動します。

   dirxml_remote -config *path_to_config_file*

3. iManager を使用して、ドライバを起動します。
4. リモートローダが正常に動作していることを確認します。

   リモートローダがメタディレクトリサーバ上のリモートインタフェースシムと通信している場合にのみ、リモートローダにより Identity Manager アプリケーションシムがロードされます。つまり、たとえば、リモートローダがメタディレクトリサーバとの通信を失うと、アプリケーションシムはシャットダウンされます。

表 3-2 パスワードコマンドラインのオプション

オプション	2 次名	パラメータ	説明

-password	-p	パスワード	コマンド認証のパスワードを指定します。このパスワードは、コマンドの発行先のローダインスタンスの setpasswords で指定した最初のパスワードと同じにする必要があります。コ \'83\'7d ンドオプション (unload や tracechange など) を指定した場合に password オプションを指定しないと、コ \'83\'7d ンドの対象となるローダのパスワードを入力するよう要求するメッセージが \'95\'5c 示されます。
			
			例 :
			`-password novell4`
			`-p novell4`

-setpasswords	-sp	パスワード パスワード	リモートローダインスタンスのパスワード、およびリモートローダが通信するリモートインタフェースシムの Identity Manager ドライバオブジェクトのパスワードを指定します。引数の最初のパスワードは、リモートローダのパスワードです。オプション引数の 2 番目のパスワードは、メタディレクトリサーバのリモートインタフェースシムに関連付けられた Identity Manage ドライバオブジェクトのパスワードです。どちらのパスワードも指定しないか、または両方のパスワードを指定する必要があります。パスワードを指定しない場合、リモートローダよりパスワードを要求するメッセージが表示されます。これは環境設定オプションです。このオプションを使用すると、指定したパスワードがリモートローダのインスタンスに設定されます。ただし、このオプションを指定しても、Identity Manager アプリケーションシムはロードされず、ローダの別のインスタンスとも通信しません。
			
			例 :
			`-setpasswords novell4 staccato3`
			`-sp novell4 staccato3`

3.6.2 Solaris、Linux、または AIX でリモートローダを起動する

Solaris、Linux、または AIX では、バイナリコンポーネント rdxml によってリモートローダの機能が提供されます。デフォルトでは、このコンポーネントは /usr/bin/ ディレクトリにあります。

1 リモートローダのパスワードを設定します。コマンドパスワードのオプションについては、77 ページの 表 3-2 を参照してください、

プラットフォーム	コマンド
Solaris LInux AIX	rdxml -config *path_to_config_file* -sp *password password*
HP-UX AS/400 OS/390 z/OS	dirxml_jremote -config *path_to_config_file* -sp *password password*

2 リモートローダを起動します。

プラットフォーム	コマンド
Solaris LInux AIX	rdxml -config *path_to_config_file*
HP-UX AS/400 OS/390 z/OS	dirxml_jremote -config *path_to_config_file*

3 iManager を使用して、ドライバを起動します。

4 リモートローダが適切に動作していることを確認します。

リモートローダがメタディレクトリサーバ上のリモートインタフェースシムと通信している場合にのみ、リモートローダにより Identity Manager アプリケーションシムがロードされます。つまり、たとえば、リモートローダがメタディレクトリサーバとの通信を失うと、アプリケーションシムはシャットダウンされます。

Linux、Solaris、または AIX では、ps コマンドまたはトレースファイルを使用して、コマンドおよび接続ポートがリッスンしているかどうかを調べます。

HP-UX などのプラットフォームでは、トレースファイル上で tail コマンドを使用して Java リモートローダを監視します。

```
tail -f trace filename
```

ログの最終行に次の情報が \'95\'5c 示される場合、ローダは正常に実行されていて、Identity Manager リモートインタフェースシムからの接続を待機しています。

```
TRACE: Remote Loader: Entering listener accept()
```

UNIX で自動的に起動するようにリモートローダ (rdxml) を設定するには、TID 10097249 (http://support.novell.com/cgi-bin/search/searchtid.cgi?/10097249.htm) を参照してください。

3.7 リモートローダを停止する

リモートローダを停止する方法は、各プラットフォームによって異なります。表 3-3 に各プラットフォームの説明があります。

表 3-3 *リモートローダを停止する方法*

プラットフォーム	コマンド
Windows	リモートローダのコン \'83\'5cールを使用して、ドライバインスタンスを停止します。
Solaris LInux AIX	rdxml -config *path_to_config_file* -u
HP-UX AS/400 OS/390 z/OS	dirxml_jremote -config *path_to_config_file* -u

コンピュータ上でリモートローダの複数のインスタンスが実行されている場合は、リモートローダが適切なインスタンスを停止できるように -cp *コマンドポートオプション*を渡します。

リモートローダを停止する場合、十分な権利を持っているか、リモートローダのパスワードを入力する必要があります。たとえば、リモートローダを Windows サービスとして実

行している場合。リモートローダを停止するための十分な権限を持っています。パスワードを入力しますが、パスワードが正しくないことに気付きます。リモートローダが停止します。

リモートローダはパスワードを受け入れません。この場合パスワードが冗長であるため、パスワードは無視されます。サービスではなくアプリケーションとしてリモートローダを実行している場合、パスワードが使用されます。

3.8 リモートローダを使用するための、Identity Manager ドライバを設定する

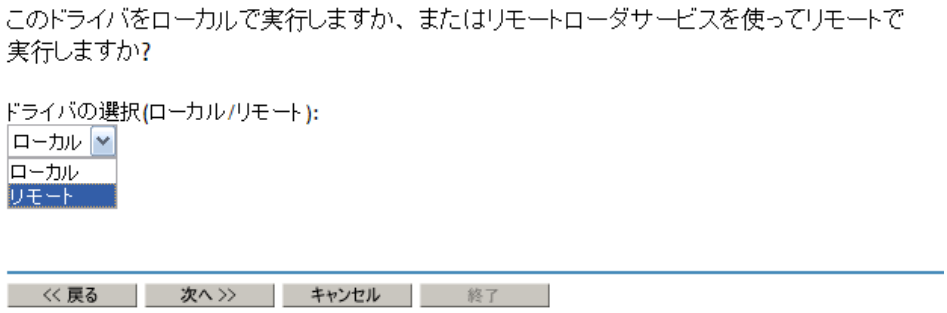
新しいドライバを設定するか、または既存のドライバを有効にして、リモートローダと通信できます。このセクションでは、リモートローダと通信できるようにするためのドライバの設定に関する一般的な情報について説明します。ドライバ固有の情報については、適切なドライバの実装ガイドを参照してください。

- 79 ページのセクション 3.8.1「新しいドライバのインポートおよび設定」
- 80 ページのセクション 3.8.2「既存のドライバの設定」
- 82 ページのセクション 3.8.3「キーストアの作成」

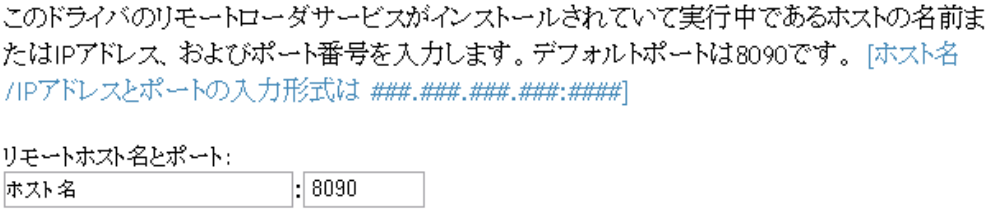
3.8.1 新しいドライバのインポートおよび設定

1 iManager で、新しいドライバをインポートまたは作成して設定します。

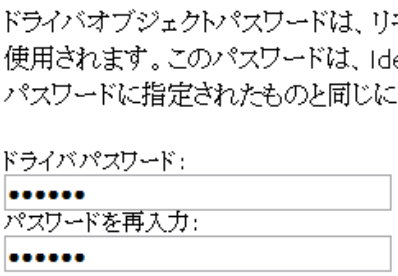
2 設定オプションの下部までスクロールし、ドロップダウンリストから［Remote］を選択し、［*Next*］*をクリックします。*



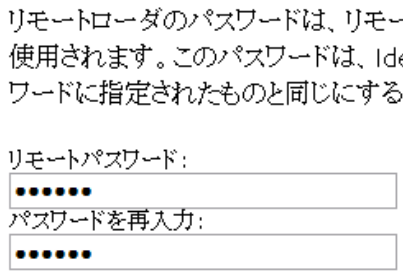
3 リモートのホスト名とポートを指定します。



4 ドライバパスワードのパスワードを入力して再入力します。



5 リモートローダのパスワードを入力して再入力し、［*次へ*］をクリックします。



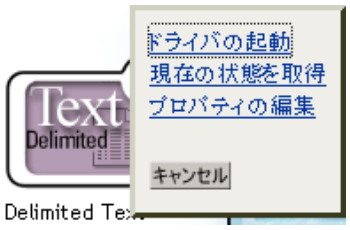
6 セキュリティが同等なユーザを定義し、［*Next*］をクリックし、［Finish］をクリックします。

3.8.2 既存のドライバの設定

リモートローダに接続するための、ドライバオブジェクトのパラメータを指定します。

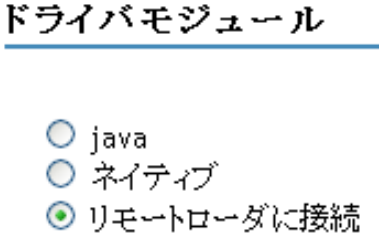
1 iManager で、［*Identity Manager*］>［*Identity Manager Overview*］の順にクリックします。

2 変更するドライバオブジェクトを参照して選択します。



3 ドライバのステータスアイコンをクリックし、［*Edit Properties*］をクリックします。

4 ［*ドライバモジュール*］セクションで、［*リモートローダに接続*］を選択します。



5［*認証*］セクションで、リモートローダのパラメータを指定します。

- ［Remote Loader Connection Parameters］

  以前は、自己署名証明書をエクスポートしていました。(参照先 56 ページのセクション 3.2.2「自己署名証明書のエクスポート」.) SSL では、自己署名証明書のニックネームが必要です。

  *［リモートローダ接続パラメータ］*編集ボックスで、キーと値のペアのパラメータを入力します。たとえば、次のように入力します。

  ```
  hostname=192.168.0.1 port=8090 kmo=remotecert
  hostname=192.168.0.1 port=8090 kmo=’remote cert’
  ```

  - **ホスト名 :** ホスト名または IP アドレス (190.162.0.1 など)。リモートローダを実行するコンピュータのアドレスまたは名前を指定します。IP アドレスまたはサーバ名を指定しない場合、この値がローカルホストのデフォルトになります。
  - **port:** リモートローダが、リモートインタフェースシムからの接続を受け入れる場所です。この通信パラメータを指定しないと、値はデフォルトで 8090 に設定されます。
  - **kmo:** SSL に使用するキーと証明書を含む暗号化キーオブジェクト (KMO) のキー名 (kmo=remotecert など) を指定します。

    証明書の名前にスペースを使用した場合は、KMO オブジェクトのニックネームを一重引用符で囲む必要があります。

    KMO オブジェクト名は、55 ページのセクション 3.2.1「サーバ証明書の作成」のステップ 2 で指定したニックネーム値です。

- **アプリケーションのパスワードの入力 :** アプリケーションユーザ ID のパスワードを指定します。通常、ドライバがアプリケーションと接続するために、ドライバシムはこのパスワードを必要とします。
- **リモートローダのパスワードの入力 :** リモートローダのパスワードを指定します。リモートインタフェースは、このパスワードを使用してリモートローダで自身を認証します。

  アプリケーションのパスワードとリモートローダのパスワードは、両方を同時に設定するか、または両方を同時にリセットしてください。

6 *[OK]* をクリックします。

3.8.3 キーストアの作成

キーストアは、暗号化キーおよび証明書 (オプション) を含む Java ファイルです。リモートローダと Metadirectory エンジンの間で SSL を使用する必要があり、Java シムを使用する場合は、キーストアファイルを作成する必要があります。

- 82 ページの 「Windows でのキーストア」
- 82 ページの 「Solaris、Linux、または AIX でのキーストア」
- 82 ページの 「すべてのプラットフォームでのキーストア」

Windows でのキーストア

Windows で Keytool ユーティリティを実行します。このユーティリティは通常、c:\novel\lremoteloader\jre\bin ディレクトリにあります。

Solaris、Linux、または AIX でのキーストア

Solaris、Linux、または AIX の環境では、create_keystore ファイルを使用します。Create_keystore は rdxml とともにインストールされます。また、\dirxml\Java_remoteloader ディレクトリにある dirxml_jremote.tar.gz ファイルにも含まれています。create_keystore ファイルは、Keytool ユーティリティを呼び出すシェルスクリプトです。

UNIX では、自己署名証明書を使用してキーストアが作成されると、Base64 またはバイナリの DER 形式で証明書をエクスポートできます。

コ \'83\'7d ンドラインで次を入力します。

create_keystore self-signed_certificate_name keystorename

たとえば、次のいずれかを入力します。

```
create_keystore tree-root.b64 mystore
create_keystore tree-root.der mystore
```

create_keystore スクリプトにより、キーストアパスワード用にハードコードされている “dirxml” のパスワードが指定されます。キーストアに保存されるのはパブリック証明書とパブリックキーのみなので、セキュリティリスクはありません。

すべてのプラットフォームでのキーストア

任意のプラットフォームでキーストアを作成するには、コ \'83\'7d ンドラインで次を入力します。

keytool -import -alias trustedroot -file self-signed_certificate_name -keystore filename -storepass

filename には任意の名前を指定できます (rdev_keystore など)。

ポリシーの作成

4

ポリシーにより、識別 \'83\'7bールトに対する情報フローを特定の環境に合わせてカスタ \'83\'7d イズできます。

たとえば、ある会社ではメインのユーザクラスとして inetorgperson を使用していて、別の会社では User を使用しているとします。これを処理するために、各システムで呼び出すユーザをメタディレクトリエンジンに指示するポリシーが作成されています。接続システム間でユーザに影響する操作をやり取りする場合、Identity Manager は、この変更を行うポリシーを適用します。

また、ポリシーは、新しいオブジェクトの作成、属性値の更新、スキー \'83\'7d 変換の実行、一致条件の定義、Identity Manager の関連付けの維持など、多くのタスクを実行します。

ポリシーの詳細なガイドについては、「*Identity Manager 3.5.1 のポリシーの理解*」を参照してください。このガイドの内容は次のとおりです。

- 使用可 \'94\'5c な各ポリシーの詳細な説明
- XSLT スタイルシートを使用したポリシー作成の説明

『*Identity Manager 3.5.1 用 iManager のポリシー*』の「*Designer 2.1 のポリシー*」に各条件、アクション、名詞、および動詞の例や構文を含む、詳細なポリシービルダのユーザガイドとリファレンスがあります。

接続システム間のパスワード同期 5

5.1 概要

Identity Manager では、パスワードの発行と加入に対するユニバーサルパスワードと接続システムのサポートを利用することによって、双方向パスワード同期が提供されています。

ユーザアカウントのその他の属性と同様に、承認されたデータ \'83\'5cースを選択できます。

5.1.1 パスワードの概要

NDS® パスワード、単純パスワード、配布パスワード、およびユニバーサルパスワードは、異なる目的のために使用されます。eDirectory と Identity Manager の以前のバージョンでは、接続システムで更新できるのは NDS パスワードのみで、これは一方向の同期でした。

Identity Manager ではユニバーサルパスワードが使用されています。これは、他の識別ボールトのパスワードと同期できる、逆方向の同期が可能なパスワードです。ユニバーサ

ルパスワードは eDirectory 8.7.1 で導入され、3 つの層の暗号化によって保護されています。

NMAS™ は、ユニバーサルパスワードと他の識別ボールトのパスワードの関係を制御します。たとえば、NMAS は、ユニバーサルパスワードと NDS パスワード、単純パスワード、または配布パスワードの同期を保つかどうかを制御します。NMAS は、パスワードを変更しようとする着信要求を受信し、NMAS のパスワードポリシーの設定に従って処理します。

Identity Manager では、配布パスワードを使用して識別ボールトと接続システム間のパスワード同期が制御されます。Identity Manager では、識別ボールトと接続システム間の双方向パスワード同期ポリシー、パスワードトンネル、および接続システムのパスワード確認ステータスを含む、配布パスワードを使用する特定のパスワード同期機能が実装されます。

ユニバーサルパスワードのように、配布パスワードも 3 つの暗号化層で保護されていて、逆方向で同期化できます。

NMAS のパスワードポリシーでは、配布パスワードをユニバーサルパスワードと同じにするかどうかを指定できます。(設定は、［*ユニバーサルパスワードの設定時に配布パスワードを同期する*］です)。配布パスワードがユニバーサルパスワードと同じで、接続システムの双方向パスワード同期を使用するよう選択する場合は、Identity Manager を使用して eDirectory からユニバーサルパスワードを抽出して、その他の接続システムに送信できます。パスワードの転送、およびパスワードを保存する接続システムをセキュリティで保護する必要があります。(253 ページの第 9 章「セキュリティ : ベストプラクティス」を参照してください。)

配布パスワードがユニバーサルパスワードと同じではない場合 (NMAS パスワードポリシーで設定を無効にしているため)、ユニバーサルパスワードまたは NDS パスワードを使用せずに、またはこれらに影響せずに、配布パスワードを使用した接続システム間でパスワードを「トンネル」することができます。トンネルは、接続システム間のみでパスワードを同期します。有効になっている場合、トンネルでは識別ボールト / ユニバーサルパスワードは設定されません。

さまざまな eDirectory パスワードの詳細については、『*Novell Modular Authentication Services (NMAS) 2.3 Administration Guide* (http://www.novell.com/documentation/nmas23/index.html)』を参照してください。Identity Manager でパスワード同期を使用する方法については、120 ページのセクション 5.8「パスワード同期の実装」を参照してください。

5.1.2 双方向パスワード同期とは？

双方向パスワード同期は、指定した接続システムからパスワードを受け取る Identity Manager と、指定した接続にパスワードを配布する Identity Manager の組み合わせです。

特定の接続システムと双方向でパスワードを同期できるかどうかは、接続システムが何をサポートしているかによって決まります。

接続システムの中には、Identity Manager から修正された新しいパスワードを受け入れ、ユーザの実際のパスワードを Identity Manager に提供できるものもあります。これらの接続システムは、Identity Manager との双方向パスワード同期をサポートしているシステムです。

- Active Directory
- Novell® eDirectory™

- Network Information Services (NIS)
- NT ドメイン

これらの接続システムでは、ユーザは、いずれかのシステムでパスワードを変更して、Identity Manager を介してそのパスワードを他のシステムと同期化できます。ただし、NMAS パスワードポリシーで高度なパスワードルールを使用している場合、ユーザがユーザアプリケーション r セルフサービスコンソールでパスワードを変更できるようにすることをお勧めします。このコン \'83\'5cールにはユーザのパスワードが準拠しなければならないすべてのルールが \'95\'5c 示されるため、パスワード変更には最適な場所です。

その他の接続システムはユーザの実際のパスワードを提供できないため、完全な双方向パスワード同期をサポートできません。ただし、ドライバ設定内にポリシーを定義することによって、これらのシステムは、パスワードを作成するために使用できるデータを提供し、Identity Manager に送信できます。

他のシステムの中には、新しいユーザの初期パスワードの設定またはパスワードの変更、あるいはその両方を含め、Identity Manager からパスワードを受け入れることができるものもあります。詳細については、94 ページのセクション 5.2「パスワード同期をサポートする接続システム」を参照してください。

5.1.3 Password Synchronization 1.0 と Identity Manager パスワード同期の比較

表 5-1 *Password Synchronization 1.0 と Identity Manager パスワード同期*

	Password Synchronization 1.0	Identity Manager 2 および 3 のパスワード同期
製品の提供	Identity Manager とは別の製品です。	Identity Manager に含まれており、別個には販売されていません。
プラットフォーム	◆ Active Directory ◆ NT ドメイン ◆ eDirectory	次のプラットフォームでは完全な双方向パスワード同期がサポートされています。 ◆ Active Directory ◆ eDirectory ◆ NIS ◆ NT ドメイン これらの接続システムは、Identity Manager へのユーザパスワードの発行をサポートしています。ユニバーサルパスワード (および配布パスワード) は逆方向に同期できるため、Identity Manager はパスワードを接続システムに配布できます。 加入者パスワード要素をサポートする接続システムは、パスワードを Identity Manager から受信できます。 詳細については、94 ページのセクション 5.2「パスワード同期をサポートする接続システム」を参照してください。

	Password Synchronization 1.0	Identity Manager 2 および 3 のパスワード同期
識別 \'83\'7bールトで使用されているパスワード	NDS パスワード (逆方向は不可 \'94\'5c)	ユニバーサルパスワード (逆方向の同期が可能)、または配布パスワード (同様に逆方向の同期が可能)。また、必要に応じて NDS パスワードの同期を維持することもできます。シナリオの例については、120 ページのセクション 5.8「パスワード同期の実装」を参照してください。
Windows 接続システムの主な機 \'94\'5c	識別ボールトパスワードが Windows パスワードと同期されるようにパスワードを Identity Manager に送信する場合。NDS パスワードは逆方向に同期化できないため、パスワードは NT または AD に戻されていませんでした。	双方向パスワード同期を提供する場合。ユニバーサルパスワード (および配布パスワード) は逆方向に同期化できるため、パスワードは両方のディレクトリで同期化できます。
LDAP 変更	サポートされていません。	サポートあり
Novell Client™	必須。	不要
nadLoginName 属性	パスワードの更新を保つために使用されます。	未使用。
パスワード同期機 \'94\'5c を含むコンポーネント	nadLoginName を更新するための機 \'94\'5c は Identity Manager ドライバに含まれていました。	ドライバ環境設定の Identity Manager ポリシーがパスワード同期機能を提供します。ドライバは単に、ポリシー内のロジックから発生する、メタディレクトリエンジンによって与えられるタスクを実行します。ドライバマニフェスト、グローバル構成値、およびドライバフィルタ設定もパスワード同期をサポートする必要があります。これは、サンプルドライバ環境設定に含まれており、既存のドライバに追加できます。詳細については、111 ページのセクション 5.7「パスワード同期をサポートするための、既存のドライバ設定のアップグレード」を参照してください。
エージェント	別個の \'83\'5c フトウェア。	エージェントはインストールされます。この機 \'94\'5c はドライバの一部になりました。

5.1.4 Identity Manager パスワード同期の機 \'94\'5c

Identity Manager パスワード同期は双方向です。パスワードは、接続システムから送信されて Identity Manager で受信したり、Identity Manager から配布されて接続システムで受信したりできます。

接続システムからのパスワードの受信

DirXML® および Identity Manager の以前のバージョンと同様に、接続システムは識別 \'83\'7bールトにパスワードを発行できます。

Identity Manager がパスワードを受け入れる元の接続システムアプリケーションを指定できます。さらに、Identity Manager が実行されている同じ識別ボールト内でユーザのパスワードを更新するか、または Identity Manager が接続システム間のみでパスワードを同期する単なるルートまたは「トンネル」として動作するかどうかも選択できます。つまり、識別 \'83\'7bールトパスワードを、Identity Manager が接続システムに配布するパスワードと別にすることができます。

一部の接続システム (AD、その他の識別 \'83\'7bールト、NT、および NIS) は、ユーザの実際のパスワードを提供できます。つまり、ユーザが接続システムでパスワードを変更した場合に、その変更を Identity Manager と同期化して、その他の接続システムに戻すことができます。

その他の接続システムはユーザの実際のパスワードの提供をサポートしていませんが、名字または従業員 ID に基づいた初期パスワードなど、スタイルシートで生成したパスワードを Identity Manager に提供するように設定できます。

接続システムへのパスワードの配布

Identity Manager のパスワード同期は、共通のパスワードを各接続システムに配布できます。

Identity Manager の以前のバージョンでは、ドライバは接続システム上のユーザアカウントから Identity Manager にパスワードを送信でき、パスワードを使用して eDirectory 内の対応するユーザを更新できました。しかし、eDirectory 内の NDS パスワードは、逆方向に同期化できないため、中央の Identity Manager 識別ボールトから複数の接続システムにパスワードを送ることはできませんでした。eDirectory パスワードを取得するには、パスワードが eDirectory に保存される前に、Novell Client などを介して取得する以外にありませんでした。

eDirectory 8.7.3 によって提供されるユニバーサルパスワードは、逆方向の同期が可能です。このため、Identity Manager では接続システムからのパスワードを受け入れ、識別ボールトから新しいアカウントの初期パスワードの設定およびパスワードの変更をサポートする接続システムにそのパスワードを配布できます。

パスワードの発行元に関係なく、Identity Manager は、接続システムにパスワードを配布する場所であるリポジトリとして配布パスワードを使用します。ユニバーサルパスワードと同様に、配布パスワードでも、パスワードポリシーを適用できます。

パスワードの同期時にユニバーサルパスワードと配布パスワードを使用する方法については、120 ページの 「パスワード同期の実装」を参照してください。

ユーザの他の属性と同様に、どのシステムが信頼されたパスワードのソースなのかを決定できます。Identity Manager は、認証された \'83\'5c ースから他の接続システムにパスワードを配布します。

双方向パスワード同期は、これをサポートする接続システム間に設定できます。

データストアおよび接続システムでのパスワードポリシーの適用

Identity Manager では、NMAS を呼び出すことによって、着信パスワードにパスワードポリシーを適用できます。接続システムから Identity Manager に発行されるパスワードがポリシーに準拠していない場合は、Identity Manager がその識別ボールトへのパスワードを受け入れないように指定できます。つまり、ポリシーに準拠しないパスワードはその他の接続システムに配布されません。

さらに、Identity Manager では、接続システムにパスワードポリシーを適用することもできます。Identity Manager に対して発行されたパスワードがポリシーのルールに準拠していない場合、Identity Manager はパスワードを受け入れて配布しないだけでなく、識別\'83\'7bールト名の現在の配布パスワードを使用して接続システム上の準拠しないパスワードをリセットするように指定できます。

たとえば、パスワードに少なくとも 1 つの数字を含める必要があるとします。しかし、接続システム自体にはそのようなポリシーを適用する機能がありません。接続システムから送られてきて、ポリシーのルールに準拠していないパスワードを Identity Manager でリセットするように指定します。

高度なパスワードルールと Identity Manager のパスワード同期を使用している場合、すべての接続システムのパスワードポリシーを調査して、eDirectory パスワードポリシーの高度なパスワードルールと互換性があることを確認することをお勧めします。この調査は、パスワードを正常に同期するために役立ちます。

NMAS パスワードポリシーが割り当てられているユーザが、接続システムのパスワード同期に参加させるユーザと一致していることを確認する必要があります。

NMAS パスワードポリシーはツリー中心で割り当てられます。一方、パスワード同期はドライバごとに設定されます。また、ドライバは各サーバにインストールされ、マスタレプリカまたは読み書き可能レプリカ内のユーザのみが管理できます。パスワード同期により期待される結果を取得するには、パスワード同期のドライバを実行するサーバにあるマスタレプリカまたは読み書き可能レプリカのコンテナが、ユニバーサルパスワードが有効なパスワードポリシーを割り当てたコンテナと一致するようにします。パーティションルートコンテナにパスワードポリシーを割り当てることによって、そのコンテナとサブコンテナ内のすべてのユーザに確実にパスワードポリシーが割り当てられます。

NMAS のパスワードポリシーをユーザに割り当てる方法の詳細については、『*パスワード管理ガイド* (http://www.novell.com/documentation/password_management/index.html)』の「Assigning Password Policies to Users」を参照してください。

パスワードの同期のシナリオ

Identity Manager を使用すると、どのシステムが信頼されたパスワードのソースであるかを指定できます。また、管理者はパスワード受諾の流れも決定します。

Identity Manager のパスワード同期機能のほとんどは、識別ボールトが提供する、逆方向に同期できるパスワード機能であるユニバーサルパスワードに依存します。しかし、いくつかのシナリオでは、ユニバーサルパスワードを展開する必要はありません。

Identity Manager のパスワード同期は、配布パスワードにも依存します。ユニバーサルパスワードと同様に、ポリシーを配布パスワードに適用できます。

パスワード同期を実装する基本的な方法については、120 ページの 「パスワード同期の実装」を参照してください。これらのシナリオを組み合わせて、各環境のニーズを満たすことができます。

Novell Client を使用しない Windows でのパスワードの同期

Active Directory と NT ドメインとのパスワード同期に、Novell Client は必要なくなりました。

パスワード同期の失敗のユーザへの通知

90 ページの 「データストアおよび接続システムでのパスワードポリシーの適用」では、Identity Manager は準拠しないパスワードを (接続システムから) 受諾しないことによってパスワードポリシーを適用できることを説明しています。

電子メール通知機 \'94\'5c を使用すると、ユーザが行ったパスワード変更が成功しなかった場合に、Identity Manager から通知するように指定できます。

シナリオ。NT ドメインからの着信パスワードがパスワードポリシーに準拠しない場合、受け入れないように Identity Manager を設定しました。電子メール通知機能を有効にしました。NMAS のパスワードポリシーの 1 つのルールで、会社名をパスワードとして使用できないよう指定されています。ユーザは、NT ドメインの接続システム上でパスワードを会社名に変更します。NMAS はパスワードを受け入れず、Identity Manager からユーザに、パスワードの変更が同期化されなかったことを知らせる電子メールメッセージが送信されます。

この機能を使用するには、電子メールサーバとテンプレートを設定する必要があります。次をカスタ \'83\'7d イズできます。

- Identity Manager が送信するメッセージのテキスト
- コピーを管理者に送信する通知

詳細については、158 ページの 「電子メール通知の設定」を参照してください。

ユーザのパスワード同期ステータスのチェック

Identity Manager を使用すると、接続システムに問い合わせて、ユーザのパスワード同期のステータスを確認できます。接続システムがパスワードの確認機 \'94\'5c をサポートしている場合、パスワードが正常に同期化されているかどうかを確認できます。

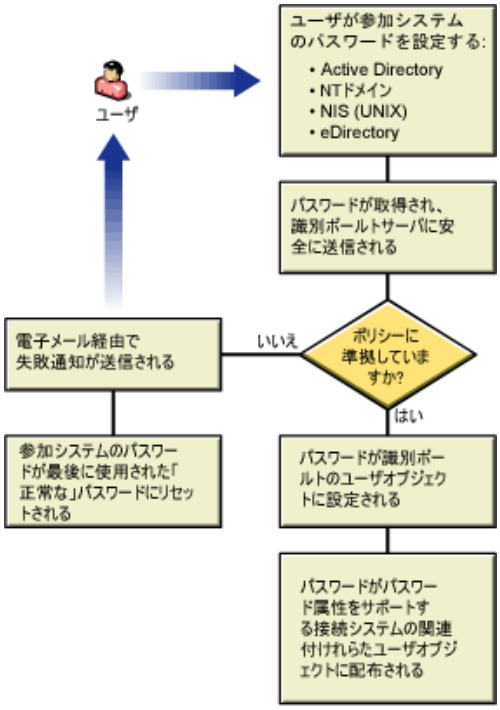
パスワードを確認する方法の詳細については、157 ページの 「ユーザのパスワード同期ステータスの確認」を参照してください。

パスワードの確認をサポートしているシステムのリストについては、94 ページの 「パスワード同期をサポートする接続システム」を参照してください。

5.1.5 パスワード同期のフローの概要

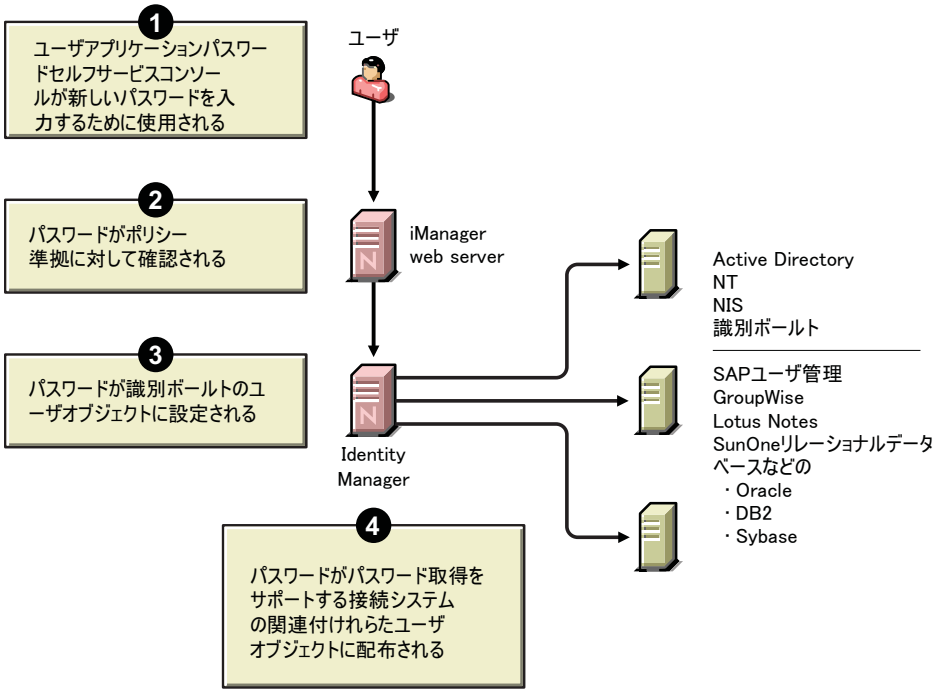
次の \'90\'7d は、接続システムが Identity Manager にパスワードを発行する方法を示しています。

図 5-1 *接続システムが Identity Manager にパスワードを発行する方法*



次の \'90\'7d は、Identity Manager が接続システムにパスワードを配布する方法を示しています。

図 5-2 *Identity Manager が接続システムにパスワードを配布する方法*

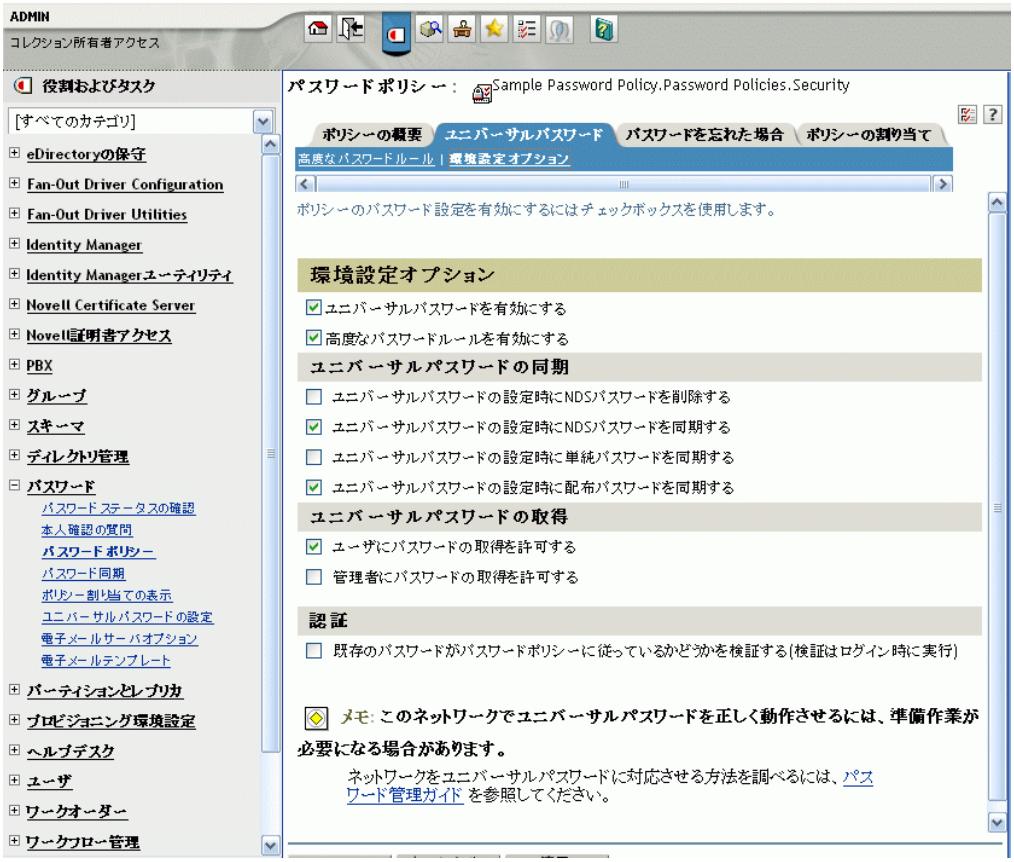


5.1.6 ブラウザ表示の差異

このドキュメントでは、iManager でのオプションを説明するために、手順で頻繁に図を使用します。オプションが実際にデスクトップ上にどのように \'95\'5c 示されるかは、ブラウザに依存します。

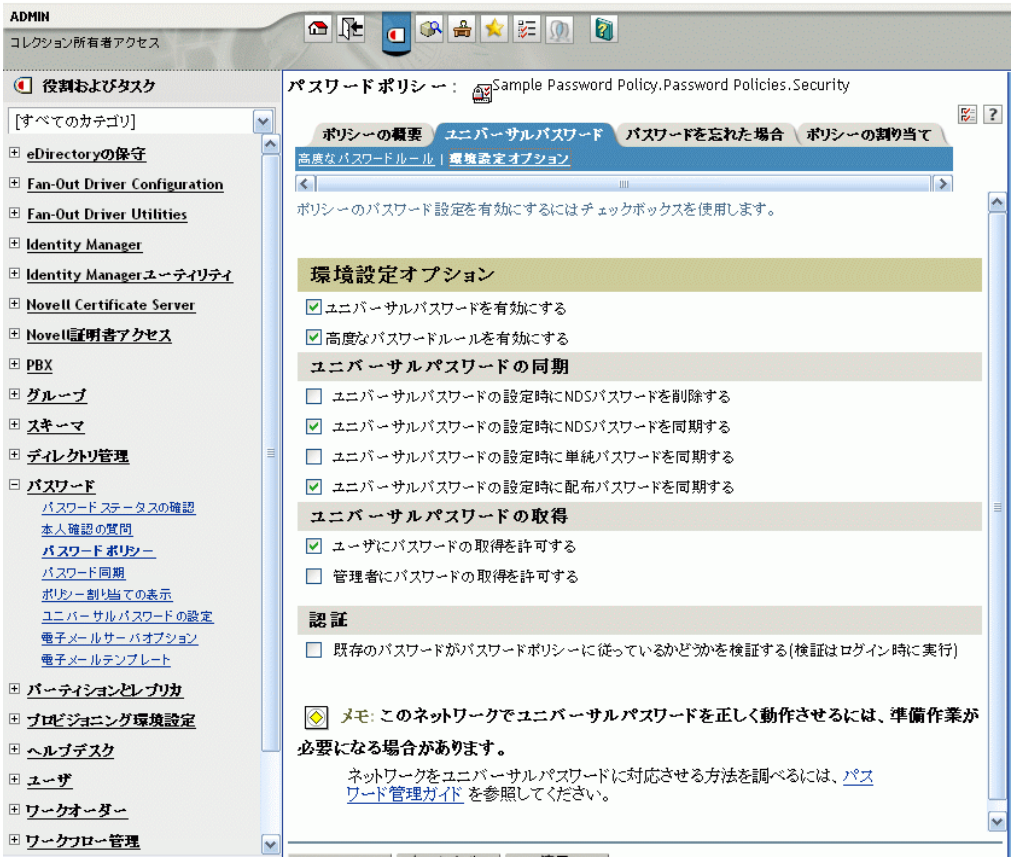
たとえば、Internet Explorer では、タブを使用した iManager のオプションが \'95\'5c 示されます。

図 5-3 *iManager のタブ*



しかし、Firefox ブラウザでは、iManager のオプションはドロップダウンリストを使用して \'95\'5c 示されます。

図 5-4 iManager のドロップダウンリスト



このドキュメントでは、Firefox ブラウザでの \'95\'5c 示に従って \'90\'7d を \'95\'5c 示しています。

5.2 パスワード同期をサポートする接続システム

ユーザオブジェクトが作成されると、Identity Manager は常に接続システムからパスワードを受信できます。これは、接続システムがユーザの実際のパスワードをそのシステムから提供できない場合でも同じです。

AD、NT、eDirectory、および NIS は Identity Manager からパスワードを受け入れて、ユーザの実際のパスワードを Identity Manager に送信することもできます。つまり、これらのシステムは双方向パスワード同期を完全にサポートしています。

発行者チャネルのドライバ設定内でポリシーを定義すると、パスワードを作成するために使用できるデータを他のシステムが提供できます。大部分のドライバのドライバ設定例には、名字に基づいてデフォルトのパスワードを提供するポリシー例が含まれています。

接続システムは、Identity Manager からのパスワードを受け入れる各種機能を備えています。一部の接続システムは、新しいアカウントの初期パスワードの設定をサポートしますが、パスワード変更イベントはサポートしません。

サンプルドライバ環境設定の機能は、ドライバマニフェストに記載されています。以下の表は、ドライバマニフェストにない追加情報を示しています。表は、新しいアカウントに設定されている初期パスワードをアプリケーションが受け入れるかどうか、既存のパス

ワードへの変更を受け入れるかどうかを示しています。\'83\'7d ニフェストでは、接続システムがパスワードを受け取ることができることだけが示されており、この違いについては示されていません。

類似した機 \'94\'5c を持つサンプルドライバ設定を参照できるように、ドライバはグループ化されています。

5.2.1 双方向のパスワード同期をサポートするシステム

次の接続システムでは、双方向のパスワード同期がサポートされています。これらは、接続システム上のユーザの実際のパスワードを提供し、Identity Manager からパスワードを受諾できます。

表 5-2 *双方向のパスワード同期をサポートするシステム*

接続システムのドライバ	加入者チャネル	加入者チャネル	加入者チャネル	発行者チャネル
	アプリケーションが初期パスワードの設定を受け取ることができる	アプリケーションがパスワードの変更を受け取ることができる	アプリケーションがパスワードの確認をサポートしている	Identity Manager がパスワードを提供 (同期化) できる
Active Directory	はい	はい	はい	はい
eDirectory [1]	はい	はい	はい	はい
NT ドメイン	はい	はい	いいえ	はい
NIS	はい	はい	はい	はい
SIF	はい	はい	いいえ	はい

[1] 識別ボールトツリー間では、ユニバーサルパスワードがユーザに対して有効化されていない場合でも、ユーザに双方向パスワード同期を提供できます。詳細については、122 ページのセクション 5.8.2「シナリオ 1: NDS パスワードを使用した、2 つの識別ボールト間の同期」を参照してください。

5.2.2 Identity Manager のパスワードを受け入れるシステム

次の接続システムは、Identity Manager からある程度までパスワードを受け入れることができます。これらは、接続システム上のユーザの実際のパスワードを Identity Manager に提供できません。

ユーザの実際のパスワードは提供できませんが、接続システム上の他のユーザデータに基づいて、発行者チャネル上のポリシーを使用してパスワードを作成するように設定できます。(サンプルドライバ設定には、名字に基づいたデフォルトのパスワードが示されています)。

表 5-3 Identity Manager のパスワードを受け入れるシステム

接続システムのドライバ	加入者チャネル アプリケーションが初期パスワードの設定を受け取ることができる	加入者チャネル アプリケーションがパスワードの変更を受け取ることができる	加入者チャネル アプリケーションがパスワードの確認をサポートしている	発行者チャネル Identity Manager がパスワードを提供 (同期化) できる
Groupwise®	はい	はい	いいえ	いいえ [2]
JDBC	はい [3]	×4	いいえ	No [5]
LDAP	はい [6]	はい [6]	はい	いいえ
メモ	はい	はい [7]	はい [7]	いいえ
SAP User Management	はい	はい	いいえ	いいえ

[2]GroupWise は 2 つの認証方法をサポートします。

- GroupWise は独自の認証を提供し、ユーザパスワードを維持します。
- GroupWise は LDAP を使用して eDirectory に対して認証し、パスワードは維持しません。

  このオプションを使用する場合、GroupWise はドライバによって同期されたパスワードを無視します。

[3] 初期パスワードを設定する機能は、OS ユーザアカウントが Oracle*、MS SQL、MySQL*、Sybase* などのデータベースのユーザアカウントと異なるすべてのデータベースで利用できます。

[4]JDBC の Identity Manager ドライバを使用して接続システムのパスワードを変更できますが、サンプルドライバ設定にはその機能は示されていません。

[5] パスワードはテーブルに格納する際にデータとして同期化できます。

[6] 対象となる LDAP サーバで userpassword 属性を設定できる場合。

[7]Notes ドライバはパスワードの変更を受け入れ、Lotus Notes の HTTPPassword フィールドのパスワードのみを確認できます。

5.2.3 パスワードを受け入れたり、提供したりしないシステム

次の接続システムはパスワードを受諾できません。また、接続システムサンプルドライバ設定を使用して、ユーザのパスワードを提供することもできません。

ユーザのパスワードを Identity Manager に提供することはできませんが、接続システム上の他のユーザデータに基づいて、発行者チャネル上のポリシーを使用してパスワードを作成するように設定できます。(サンプルドライバ設定には、名字に基づいたデフォルトのパスワードが示されています)。

表 5-4 パスワードを受け入れたり、提供したりしないシステム

接続システムのドライバ	加入者チャネル アプリケーションが初期パスワードの設定を受け取ることができる	加入者チャネル アプリケーションがパスワードの変更を受け取ることができる	加入者チャネル アプリケーションがパスワードの確認をサポートしている	発行者チャネル Identity Manager がパスワードを提供 (同期化) できる
区切りテキスト	No [8]	No [8]	No [8]	No [8]
Exchange 5.5	いいえ	いいえ	いいえ	いいえ
PeopleSoft 3.6	いいえ	いいえ	いいえ	いいえ
PeopleSoft 4.0	いいえ	いいえ	いいえ	いいえ
SAP HR	いいえ	いいえ	いいえ	いいえ

[8] 区切りテキスト用の Identity Manager ドライバには、パスワード同期を直接サポートするドライバシムの機能がありません。ただし、このドライバは、同期先の接続システムによってはパスワードを処理するように設定できます。

5.2.4 パスワード同期をサポートしないシステム

次の接続システムは、パスワード同期での使用向けではありません。

表 5-5 パスワード同期をサポートしないシステム

接続システムのドライバ	加入者チャネル アプリケーションが初期パスワードの設定を受け取ることができる	加入者チャネル アプリケーションがパスワードの変更を受け取ることができる	加入者チャネル アプリケーションがパスワードの確認をサポートしている	発行者チャネル Identity Manager がパスワードを提供 (同期化) できる
Avaya* PBX	いいえ	いいえ	いいえ	いいえ
エンタイトルメントサービスドライバ	いいえ	いいえ	いいえ	いいえ
LoopBack サービスドライバ	いいえ	いいえ	いいえ	いいえ
手動タスクサービスドライバ	いいえ	いいえ	いいえ	いいえ

5.3 パスワード同期の前提条件

パスワード同期は、次の要素に依存します。

- 98 ページの 「ユニバーサルパスワードのサポート」
- 98 ページの 「ドライバマニフェストのパスワード同期機能」
- 98 ページの 「グローバル構成値を使用してパスワード同期を制御する」
- 101 ページの 「ドライバ設定で必要なポリシー」

- 105 ページの 「パスワード取得のために接続システムにインストールするフィルタ」
- 105 ページの 「ユーザ用に作成した NMAS のパスワードポリシー」
- 105 ページの 「NMAS ログインメソッド」

5.3.1 ユニバーサルパスワードのサポート

接続システム間でのパスワード同期に対応するには、Identity Manager でユニバーサルパスワードを使用する必要があります。次を参照してください。

- 『*パスワード管理ガイド*(http://www.novell.com/documentation/password_management/index.html)』の「Deploying Universal Password」
- 107 ページのセクション 5.4.3「ユニバーサルパスワードを使用するための準備作業」

5.3.2 ドライバマニフェストのパスワード同期機能

ドライバ \'83\'7d ニフェストは、接続システムが次のパスワード同期機 \'94\'5c をサポートするかどうかを宣言します。

- ユーザの実際のパスワードを Identity Manager に発行する
- Identity Manager のパスワードを受諾する

  \'83\'7d ニフェストでは、初期パスワードの作成の受諾とパスワード変更の受諾は区別されません。
- Identity Manager で接続システム上のパスワードを確認し、ユーザのパスワード同期ステータスを決定できる

注 : ドライバマニフェストは、ドライバの開発者、またはドライバ環境設定を作成する Identity Manager のエキスパートによって記述されます。ネットワーク管理者が編集するためのものではありません。ドライバマニフェストは、ドライバシムおよび環境設定の実際の機能を表します。マニフェストのみを変更しても機能は変更されません。機能を追加するには、ドライバシム、接続システム、またはドライバ環境設定を拡張する必要があります。

Identity Manager に付属するサンプルのドライバ環境設定はドライバマニフェストエントリを含みます。既存のドライバにこれらを追加するには、111 ページのセクション 5.7「パスワード同期をサポートするための、既存のドライバ設定のアップグレード」を参照してください。

5.3.3 グローバル構成値を使用してパスワード同期を制御する

グローバル構成値を使用すると、ポリシーで参照できる定数値を設定できます。グローバル設定値はレプリカごとの属性に保持されるため、サーバ変数と呼ばれることもあります。

パスワード同期では、グローバル構成値を使用して Identity Manager に対するパスワードフローの設定を作成できます。ドライバ設定内の Identity Manager パスワード同期ポリシーはグローバル設定値の設定に基づいて動作するように記述されるため、ポリシーを編集せずにパスワードのフローを簡単に変更できます。

グローバル構成値を使用して、各接続システムの次の設定を制御できます。

表 5-6 *接続システムの設定*

設定	説明
接続システムから Identity Manager がパスワードを受け取るかどうか	この設定は、接続システムによって提供されるパスワード、および発行者チャネルのドライバ設定内の Identity Manager ポリシーによって作成できるパスワードに適用できます。この設定を無効にすると、両方のタイプのパスワードが除去されるため、パスワードは Identity Manager に到達しません。
Identity Manager がユニバーサルポリシーを直接更新するか、配布パスワードを直接更新するかの指定	Identity Manager はエントリポイント (Identity Manager が更新するパスワード) を制御します。NMAS は、NMAS パスワードポリシーで設定した内容に基づいて各種パスワード間のパスワードのフローを制御します。NMAS のパスワードポリシーを \'95\'5c 示するには、次のように操作します。 1. iManager で、［*Passwords*］> ［Password Policies］の順に選択します。 2. ［*Password Policy List*］でポリシーを選択します。 3. ［*編集*］をクリックします。 4. ドロップダウンリストまたはタブからオプションを選択します (使用している iManager のバージョンによります)。 これらの方法を使用するシナリオについては、5.8「パスワード同期の実装」のセクションを参照してください。
接続システムから Identity Manager への着信パスワードに NMAS パスワードポリシーを適用するかどうか	これらのポリシーが適用された場合、準拠しない着信パスワードは Identity Manager のデータストアに書き込まれません。
接続システム上の NMAS のパスワードポリシーを適用するために、ポリシー ルールに準拠しないパスワードをリセットして、Identity Manager が Identity Manager のパスワードを使用するかどうか	このオプションは、接続システムでサポートされていない場合は NMAS インタフェース内で淡色表示されます (サポートされているかどうかはドライバマニフェストで宣言されています)。発行者チャネル上でパスワード操作が失敗した後にのみ、パスワードがリセットされます。
接続システムがパスワードを受け取るかどうか	この設定は Identity Manager によって配布されるパスワードと、購読者チャネルのドライバ環境設定内の Identity Manager ポリシーによって作成できるパスワードの両方に適用されます。この設定を無効にすると、両方のタイプのパスワードが除去されるため、パスワードは接続システムに到達しません。 このオプションは、接続システムがサポートしない場合はインタフェース内で淡色 \'95\'5c 示されます (サポートしているかどうかはドライバ \'83\'7d ニフェストで宣言されています)。
パスワードが同期化されなかった場合に、ユーザに電子メールで通知するかどうか	影響を受けるユーザに電子メールを自動的に送信します。

Identity Manager に付属するドライバ環境設定はドライバマニフェストエントリを含みます。既存のドライバにこれらを追加するには、111 ページのセクション 5.7「パスワード同期をサポートするための、既存のドライバ設定のアップグレード」を参照してください。

グローバル設定値を編集する

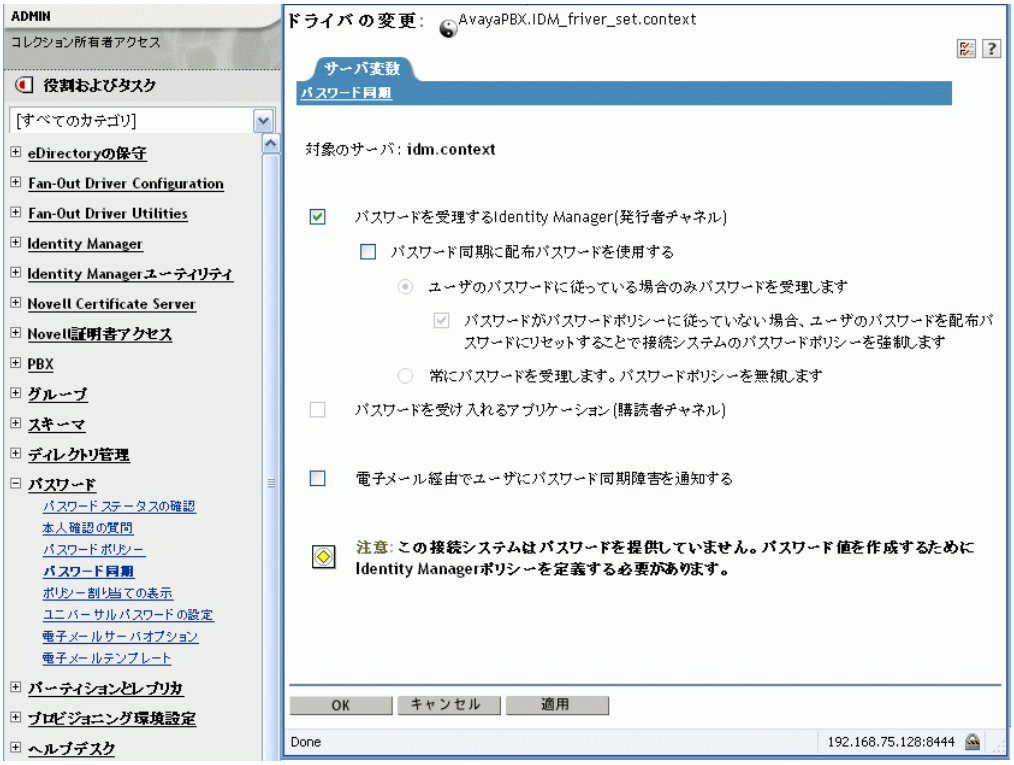
1 iManager で、［*Passwords*］> ［Password Synchronization］の順に選択します。

2 ドライバを検索します。

接続システムドライバを検索する場所を指定すると、iManager によって検索されたすべての接続システムに対するパスワードフロー設定の概要が \'95\'5c 示されます。

3 設定を \'95\'5c 示するために、ドライバ名をクリックします。

［Modify Driver］ページに、パスワード同期のグローバル設定値が \'95\'5c 示されます。



このページのオプションが淡色 \'95\'5c 示されている場合は、接続システムがそのオプションをサポートしていないことをドライバ \'83\'7d ニフェストが示しています。

4 変更を加え、［*OK*］*をクリックします。*

注 : 各ドライバに個別にグローバル構成値を設定できます。ドライバに対するグローバル構成値が、ドライバセット上のグローバル構成値を上書きします。特定のドライバに値を設定すると、より細かく制御できます。このページには、個々のドライバに存在するグローバル設定値だけを \'95\'5c 示できます。

ドライバセットオブジェクトにグローバル構成値を設定すると、ドライバが自身の値がない場合に、そのグローバル構成値がそのドライバセット内のドライバによって継承されます。ドライバに自身の設定がなく、ドライバセットからのグローバル構成値を継承する場合、iManager には値が表示されません。iManager には継承されているグローバル設定値は \'95\'5c 示されませんが、グローバル設定値はパスワード同期ポリシーによって適用されます。

5.3.4 ドライバ設定で必要なポリシー

各ドライバの発行者チャネルおよび購読者チャネルの Identity Manager ポリシーにより、上述のグローバル構成値に基づき、パスワードのフローが制御されます。これらのポリシーは、Identity Manager のドライバ設定に含まれています。

既存のドライバ設定を置き換えるのではなく更新する場合は、特定のポリシーを設定に追加する必要があります。(参照先 111 ページのセクション 5.7「パスワード同期をサポートするための、既存のドライバ設定のアップグレード」.) パスワード同期を機 \'94\'5c させるには、これらのポリシーをドライバ設定の正しい場所に指定する必要があります。

- 101 ページの 「発行者コ \'83\'7d ンド変換設定で必要なポリシー」
- 103 ページの 「発行者入力変換ポリシーセットで必要なポリシー」
- 103 ページの 「加入者コ \'83\'7d ンド変換ポリシーセットで必要なポリシー」
- 104 ページの 「加入者出力変換ポリシーセットで必要なポリシー」

発行者コ \'83\'7d ンド変換設定で必要なポリシー

［パスワード同期ポリシー名］カラムに一覧表示されているポリシーは、表示されている順に存在する必要があります。また、これらは発行者コ \'83\'7d ンド変換ポリシーセットの最後のポリシーでもある必要があります。

表 5-7 *発行者コ\'83\'7d ンド変換設定で必要なポリシー*

ドライバ設定内の場所	パスワード同期ポリシー名	ポリシーの実行内容
Publisher Command Transformation (発行者コ\'83\'7d ンド変換)	Password(Pub)-Default Password Policy (パスワード (発行者)- デフォルトパスワードポリシー)	Add オブジェクトにまだパスワードが含まれていない場合は、デフォルトのパスワードを Add オブジェクトに追加します。 このポリシーと Password(Sub)-Default Password Policy (パスワード (購読者)- デフォルトパスワードポリシー) は、変更または削除できる唯一のポリシーです。パスワード同期機 \'94\'5c が適切に機 \'94\'5c するためには、他のポリシーを変更せずに使用する必要があります。
	Password(Pub)-Check Password GCV (パスワード (発行者)- パスワード GCV の確認)	GCV を確認し、Identity Manager がこの接続システムからパスワードを受け入れるよう指定しているかどうかを判断します。指定していない場合は、すべてのパスワード要素を除去します。 GCV の名前は enable-password-publish で、表示名は［*Identity Manager はアプリケーションからのパスワードを受け入れる*］です。
	Password(Pub)-Publish Distribution Password (パスワード (発行者)- 配布パスワードの発行)	<password> 要素を、ユニバーサルパスワードを更新できる形式に変換します。 このポリシーが参照する GCV は、次のとおりです。 ◆ publish-password-to-dp ◆ enforce-password-policy
	Password(Pub)-Publish NDS Password (パスワード (発行者)-NDS パスワードの発行)	NDS パスワードを更新するように指定している場合に、<password> 要素が通過できるようにします。指定していない場合は、<password> 要素を除去します。 このポリシーは、publish-password-to-nds という GCV を参照します。
	Password(Pub)-Add Password Payload (パスワード (発行者)- パスワードペイロードの追加)	電子メール通知のために、エンジン内で回覧されるペイロードデータを \'91\'7d 入します。
	Password(Sub)-Add Password Payload (パスワード (加入者)- パスワードペイロードの追加)	電子メール通知のために、エンジン内で回覧されるペイロードデータを \'91\'7d 入します。

発行者入力変換ポリシーセットで必要なポリシー

入力変換に複数のポリシーがある場合、パスワード (発行者)- 加入者の電子メール通知ポリシーは最後に記述することをお勧めします。

表 5-8 *発行者入力変換ポリシーセットで必要なポリシー*

ドライバ設定内の場所	パスワード同期ポリシー名	ポリシーの実行内容
Publisher Input Transformation (発行者入力変換)	Password(Pub)-Sub Email Notifications (パスワード (発行者)- 加入者の電子メール通知)	パスワードペイロード情報が送られてきて、ステータスが問題を示す場合、ユーザに電子メールを送信します。送信には、eDirectory のインターネット電子メールアドレス属性に示されている電子メールアドレスが使用されます。 このポリシーは、notify-user-on-password-dist-failure という GCV を参照して、通知電子メールを送信するかどうかを決定します。

加入者コ \'83\'7d ンド変換ポリシーセットで必要なポリシー

［パスワード同期ポリシー名］カラムに一覧表示されているポリシーは、表示されている順に存在する必要があります。また、これらは加入者コ \'83\'7d ンド変換ポリシーセットの最後のポリシーでもある必要があります。

表 5-9 加入者コ\'83\'7d ンド変換ポリシーセットで必要なポリシー

ドライバ設定内の場所	パスワード同期ポリシー名	ポリシーの実行内容
Subscriber Command Transformation (加入者コ\'83\'7d ンド変換)	Password(Sub)-Transform Distribution Password (パスワード (加入者)- 配布パスワードの変換)	ユニバーサルパスワードを <password> 要素に変換します。
	Password(Sub)-Default Password Policy (パスワード (加入者)- デフォルトパスワードポリシー)	Add オブジェクトにまだパスワードが含まれていない場合は、デフォルトのパスワードを Add オブジェクトに追加します。 このポリシーと Password(Pub)-Default Password Policy (パスワード (発行者)- デフォルトパスワード) は、変更または削除できる唯一のポリシーです。パスワード同期機 \'94\'5c が適切に機 \'94\'5c するためには、他のポリシーを変更せずに使用する必要があります。
	Password(Sub)-Check Password GCV (パスワード (加入者)- パスワード GCV の確認)	GCV を確認し、接続システムがパスワードを受け入れるよう指定しているかどうかを判断します。指定していない場合は、すべてのパスワード要素を除去します。 GCV の名前は enable-password-subscribe で、\'95\'5c 示名は *[Application accepts passwords from Identity Manager data store]* です。
	Password(Sub)-Add Password Payload (パスワード (加入者)- パスワードペイロードの追加)	電子メール通知のために、エンジン内で回覧されるパスワードペイロードデータを \'91\'7d 入します。

加入者出力変換ポリシーセットで必要なポリシー

出力変換に複数のポリシーがある場合、パスワード (加入者)- 発行者の電子メール通知ポリシーは最後に記述することをお勧めします。

表 5-10 加入者出力変換ポリシーセットで必要なポリシー

ドライバ設定内の場所	パスワード同期ポリシー名	ポリシーの実行内容
Subscriber Output Transformation (加入者出力変換)	Password(Sub)-Pub Email Notifications (パスワード (加入者)- 発行者の電子メール通知)	パスワードペイロード情報が送られてきて、ステータスが問題を示す場合、ユーザに電子メールを送信します。 このポリシーは、notify-user-on-password-dist-failure という GCV を参照して、通知電子メールを送信するかどうかを決定します。

5.3.5 パスワード取得のために接続システムにインストールするフィルタ

AD、NT ドメイン、および NIS では、ユーザのパスワードを取得するためにフィルタをインストールする必要があります。

詳細については、154 ページのセクション 5.9「パスワードフィルタの設定」を参照してください。

5.3.6 ユーザ用に作成した NMAS のパスワードポリシー

ユニバーサルパスワードを使用しなくてもパスワード同期の一部の機能は使用できますが、ユーザ用にユニバーサルパスワードを有効にするには NMAS パスワードポリシーを使用する必要があります。また、パスワードポリシーによって、高度なパスワードルールを指定し、ユーザの既存のパスワードがルールに準拠しているかどうか確認するように指定できます。

Identity Manager のパスワード同期を使用するには、パスワードポリシーを理解する必要があります。パスワードポリシーについては、『*パスワード管理ガイド* (http://www.novell.com/documentation/password_management/index.html)』の「Managing Passwords by Using Password Policies」を参照してください。

5.3.7 NMAS ログインメソッド

状況によっては、NMAS 単純パスワードログインメソッドを用意して、パスワード機能を実行できるようにする必要があります。たとえば、LDAP ではこのメ \'83\'5cッドが必要です。

ログインメソッドの詳細については、『*Novell Modular Authentication Services (NMAS) 3.0 Administration Guide* (http://www.novell.com/documentation/nmas30/index.html)』を参照してください。

5.4 Identity Manager パスワード同期およびユニバーサルパスワードを使用するための準備作業

- 106 ページの 「NDS パスワードからユニバーサルパスワードへの切り替え」

5.4.1 NDS パスワードからユニバーサルパスワードへの切り替え

パスワードポリシーを使用してユーザのグループに対してユニバーサルパスワードをオンにする場合、ユニバーサルパスワードに値を設定する必要があります。

NDS パスワードを更新するためにこれまでパスワード同期を使用していた場合は、ユーザのパスワードの移行準備をする必要があります。ユニバーサルパスワードを使用するように切り替えるには、次のいずれかを実行し、ユーザがユニバーサルパスワードを作成するようにします。

- Novell Client を使用している場合、ユニバーサルパスワードをサポートする Novell Client を導入します。

  Identity Manager のパスワード同期には、Novell Client は必要ありません。

  Novell Client を導入した後、ユーザが次回 Novell Client を使用してログインすると、ハッシュ前に NDS パスワードがキャプチャされ、ユニバーサルパスワードを追加するために使用されます。(『Password Management Guide』の「Planning Login and Change Password Methods for your Users」を参照してください)。
- Novell Client を使用していない場合は、ユーザに iManager セルフサービスコンソールにログインさせます。このログインメソッドにより、ユニバーサルパスワードに値が入力されます。iManager セルフサービスコンソールにアクセスするには、iManager サーバの /nps に移動します。たとえば、https://www.myiManager.com/nps です。
- ユニバーサルパスワードが有効な LDAP サーバを使用して認証するサービスを通じて、ユーザにログインさせます。たとえば、会社のポータルを介してログインします。

5.4.2 ユーザによるパスワードの変更

ユーザが iManager、iManager セルフサービスコンソール、または Novell Client でパスワードを変更する場合、NMAS パスワードポリシーの高度なパスワードルールが表示されます。ルールを \'95\'5c 示すると、ユーザはルールを推測しなくても、ルールに準拠したパスワードを作成できます。

パスワードフローの設定方法によっては、ユーザが接続システムでパスワードを変更すると、パスワードが Identity Manager および他の接続システムと同期されます。ただし、ユーザがパスワードを変更する際、接続システムには、高度なパスワードルールが \'95\'5c 示されません。

高度なパスワードルールを必ず適用してルールに準拠しないパスワードの作成を回避したい場合、iManager のセルフサービスコン \'83\'5cールまたは Novell Client のみでパスワードを変更するようユーザに要求するか、高度なパスワードルールをユーザに周知徹底させます。

接続システムでは、パスワードポリシーのルールを表示しなくてもユーザはパスワードを変更できます。したがって、ユーザはルールを正しく覚えていない場合があります。ユー

ザが最初にパスワードを変更する場合、接続システム自体のポリシーのみに適用されます。接続システムでルールに準拠しないパスワードをユーザが作成すると、Identity Manager の設定によっては、次の問題が発生することがあります。

- 接続システムからIdentity Managerに渡されるパスワードにポリシーを適用する設定を有効にしている場合、ユーザの新しいパスワードは識別ボールトに同期されません。ユーザにエラーを通知するよう Identity Manager を設定している場合、電子メールによりパスワードが同期化されなかったことがわかります。
- 接続システムの準拠しないパスワードを置き換えるようIdentity Managerを設定している場合、ユーザは、選択した新しいパスワードで接続システムにログインできなくなります。

  Identity Manager は接続システムのパスワードを、ユーザが最後に作成したルールに準拠したパスワードである可 \'94\'5c 性の高い、配布パスワードにリセットします。

5.4.3 ユニバーサルパスワードを使用するための準備作業

ユニバーサルパスワードを使用する準備をするには、『*パスワード管理ガイド* (http://www.novell.com/documentation/password_management/index.html)』の「Deploying Universal Password」を参照してください。必要な多くの情報がその章にあります。

次のことも考慮してください。

- ユニバーサルパスワードを使用するには、eDirectory 8.7.1 以降が必要です。NetWare® 6.5 は必要ありません。
- Identity Manager のパスワード同期は、ユニバーサルパスワードと配布パスワードの両方に依存しています。配布パスワードは、Identity Manager が接続システムにパスワードを配布する元になるリポジトリです。ユニバーサルパスワードと同様に、NMAS ポリシーも配布パスワードに適用できます。
- Identity Manager に付属の Identity Manager iManager プラグインには、パスワード管理プラグインが含まれています。これらのプラグインを使用すると、パスワードポリシーを作成したり、ユニバーサルパスワードを NDS パスワード、通常パスワード、および配布パスワードと同期させる方法を決定したりできます。

  これらのプラグインは、NetWare 6.5 に付属のユニバーサルパスワードのプラグインを置き換えます。これらについては、『*パスワード管理ガイド* (http://www.novell.com/documentation/password_management/index.html)』の「Managing Passwords by Using Password Policies」を参照してください。
- eDirectory 8.6.2 は、Identity Manager が使用するツリーとしては使用できません。しかし、eDirectory 8.6.2 では、パスワード同期機能のサブセットにはサポートされています。したがって、環境全体をアップグレードする準備ができていない場合、他のツリーに対して eDirectory 8.6.2 を使用できます。
- ユニバーサルパスワードを展開するためにソフトウェアをアップグレードする場合の影響を最小限に抑える 1 つの方法は、Identity Manager のための別のツリーを識別ボールトとして作成することです。多くの環境では、Identity Manager およびドライバ用に識別 \'83\'7bールトがすでに使用されています。
- ユニバーサルパスワードは、パスワードポリシーの適用や特殊文字の使用など、従来のパスワード管理ツールではサポートされていない機 \'94\'5c を提供します。
- NDS パスワードとユニバーサルパスワードとの同期がずれる状態 (「パスワードドリフト」とも呼ばれます) を回避するには、Novell Client および他のユーティリティを更新する必要があります。『*パスワード管理ガイド* (http://www.novell.com/

documentation/password_management/index.html)』の「Planning Login and Change Password Methods for Your Users」を参照してください。

- Novell Client の最新バージョンはユニバーサルパスワードをサポートしているので、ユーザに対して初めてユニバーサルパスワードを有効にする際に値を入力し、ユーザがパスワードを変更する場合に NMAS のパスワードポリシーを \'95\'5c 示および適用できます。
- 接続システムでは、パスワードポリシーで作成した高度なパスワードルールは表示されません。現時点では、Novell Client でも高度なパスワードルールは \'95\'5c 示されませんが、Novell Client では高度なパスワードルールは適用されます。

  パスワードの変更は iManager のセルフサービスコン \'83\'5cールのみで行うようユーザに徹底してください。

  接続システムで、または Novell Client の最新バージョンを使用してパスワードをユーザが変更することを許可する場合には、パスワードポリシーをユーザに周知徹底し、ルールに準拠した正しいパスワードをユーザが作成するよう、サポートします。
- ConsoleOne® でユニバーサルパスワードがサポートされるのは、NetWare 6.5 以降のサーバ、または最新の Novell Client がインストールされているコンピュータで使用される場合のみであることを、管理者およびヘルプデスクに理解させてください。
- 管理者およびヘルプデスクのユーザが、NDS パスワードのみをサポートするユーティリティを使用する意味を理解するようにしてください。これらのユーティリティはログインには使用できますが、パスワードの変更には使用できません。この方法により、パスワードドリフトを回避できます。

  『*Novell Modular Authentication Services (NMAS) 3.0 Administration Guide* (http://www.novell.com/documentation/nmas30/index.html)』では、ユニバーサルパスワードのユーティリティおよびサポートが一覧表示してある TID を参照しています。

5.4.4 コンテナの一致

NMAS パスワードポリシーはツリー中心で割り当てられます。一方、パスワード同期はドライバごとに設定されます。ドライバはサーバごとにインストールされ、マスタレプリカまたは読み書き可能レプリカのユーザのみ管理できます。

パスワード同期により期待される結果を取得するには、パスワード同期を実行するサーバにあるマスタレプリカまたは読み書き可能レプリカのコンテナが、ユニバーサルパスワードが有効なパスワードポリシーを割り当てたコンテナと一致するようにします。パーティションルートコンテナにパスワードポリシーを割り当てることによって、そのコンテナとサブコンテナ内のすべてのユーザに確実にパスワードポリシーが割り当てられます。

5.4.5 電子メール通知の設定

電子メール通知機 \'94\'5c を使用するには、次のことが必要です。

- iManager の［Notification Configuration］タスク作業を使用し、電子メールサーバを設定する。
- 必要に応じて、iManager の［Notification Configuration］タスクを使用し、電子メールのテンプレートをカスタ \'83\'7d イズする。
- 識別 \'83\'7bールトユーザが Internet EMail Address 属性に入力済みであることを確認します。

158 ページのセクション 5.12「電子メール通知の設定」の指示に従います。

5.5 新しいドライバの設定と同期

現在の環境で Password Synchronization 1.0 を使用しておらず、ドライバを作成するか、または既存の環境設定を新しい Identity Manager の環境設定に置き換える場合は、Identity Manager のパスワード同期機能を設定します。

1. 現在の環境でユニバーサルパスワードを使用する準備ができていることを確認します。

   詳細については、105 ページのセクション 5.4「Identity Manager パスワード同期およびユニバーサルパスワードを使用するための準備作業」を参照してください。

2. ドライバを作成するか、既存のドライバの設定を Identity Manager の設定で置き換えます。

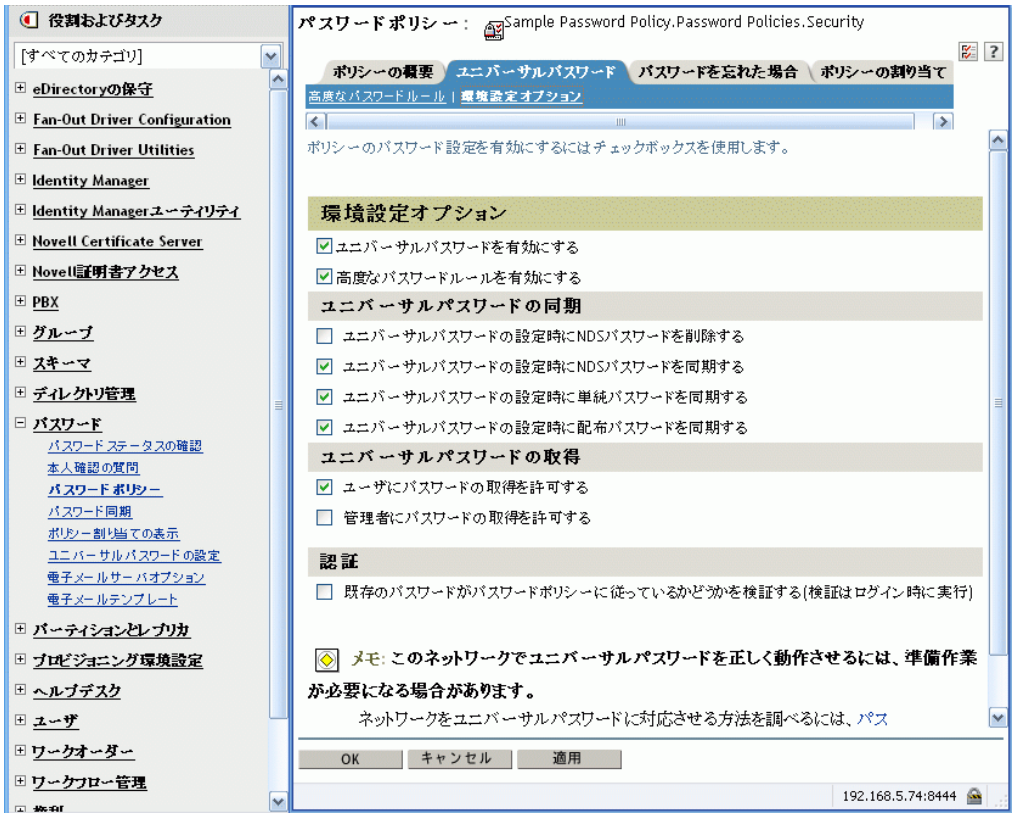
   Identity Manager の設定には、Identity Manager ポリシーおよび Identity Manager のパスワード同期に必要なその他の項目が含まれています。新しいドライバ設定のサンプルのインポートについては、個々の『Identity Manager Driver Guides (http://www.novell.com/documentation/idm35drivers/)』を参照してください。

3. ユニバーサルパスワードが有効な NMAS パスワードポリシーを作成し、ユニバーサルパスワードをオンにします。

   『*パスワード管理ガイド*(http://www.novell.com/documentation/password_management/index.html)』の「Creating Password Policies」を参照してください。NetWare 6.5 でユニバーサルパスワードを以前使用したことがある場合、『*Password Management Administration Guide*』の「(NetWare 6.5 Only) Re-Creating Universal Password Assignments」で、いくつかの追加的なステップについて説明しています。

   パスワードポリシーは、ツリーのできるだけ上位のレベルに割り当てることをお勧めします。

   ［Configuration Options］ページを使用すると、NMAS が同期された異なる種類のパスワードをどのように保持するのかを選択できます。



パスワード同期の使用のシナリオ、および Identity Manager のパスワードポリシーの適用方法については、120 ページのセクション 5.8「パスワード同期の実装」を参照してください。オンラインヘルプも参照してください。

4 (Active Directory、NIS、または NT ドメインのみ) 接続システムで Identity Manager のパスワードをユーザに割り当てる場合は、新しいパスワード同期のフィルタをインストールし、設定します。

ステップについては、「Identity Manager Drivers (http://www.novell.com/documentation/idm35drivers/)」にある各ドライバのドライバ実装ガイドを参照してください。

5 各接続システムで、パスワードフローが正しく設定されていることを確認してください。

5a iManager で、［*Passwords*］> ［Password Synchronization］の順にクリックし、管理する接続システムのドライバを検索します。

5b パスワードフローの現在の設定を \'95\'5c 示します。

これは、グローバル構成値 (GCV) のグラフィカルインタフェースです。ドライバの名前をクリックして、これらを編集します。次の設定を編集できます。

- Identity Manager がシステムからパスワードを受諾するかどうか。
- Identity Manager でどのパスワードを更新するか : ユニバーサルパスワードポリシーを直接、または配布ポリシーを直接。

  Identity Manager はエントリポイント、つまり Identity Manager で更新するパスワードを制御します。NMAS は、パスワードポリシーの環境設定オプションで設定した内容に基づいて、各種パスワード間のパスワードのフローを制御します。の \'90\'7d を参照してください。109 ページのステップ 3

- Identity Manager に入力されるパスワードの変更に、ユーザのパスワードポリシーを適用するかどうか。
- 接続システムにユーザのパスワードポリシーを適用し、準拠しないパスワードをリセットするかどうか。
- この接続システムがパスワードを受諾するかどうか。
- パスワード同期に失敗した場合、電子メール通知を送信するかどうか。

6 パスワード同期をテストします。

- Identity Manager のパスワードが指定したシステムに配布されることを確認します。
- 指定した接続システムがIdentity Managerにパスワードを公開しているかを確認します。

トラブルシューティングのヒントについては、120 ページのセクション 5.8「パスワード同期の実装」を参照してください。

5.6 Password Synchronization 1.0 のアップグレード

この作業は、Password Synchronization 1.0 で使用されている Active Directory および NT ドメインの既存の Identity Manager ドライバのみに適用されます。

Password Synchronization 1.0 からアップグレードする場合には、正しいステップに従うことが重要です。

手順については、Identity Manager Drivers (http://www.novell.com/documentation/dirxmldrivers/index.html) にある Active Directory および NT ドメイン用 Identity Manager ドライバのドライバ実装ガイドを参照してください。

5.7 パスワード同期をサポートするための、既存のドライバ設定のアップグレード

ここでは、既存のドライバ設定を Identity Manager のサンプル設定に置き換えるのではなく、Identity Manager パスワード同期のサポートを既存のドライバ設定に追加する方法について説明します。

パスワード同期に使用する各ドライバにサポートを追加します。これを行うには、「オーバーレイ」設定ファイルをインポートし、ポリシー、ドライバ \'83\'7d ニフェスト、および GCV を一度に追加します。

ポリシー、ドライバ \'83\'7d ニフェスト、および GCV を追加した後、ドライバ フィルタに nspmDistributionPassword 属性も追加する必要があります。

重要 : Password Synchronization 1.0 で使用されている Active Directory または NT ドメイン用 Identity Manager ドライバをアップグレードする場合は、「Identity Manager Drivers (http://www.novell.com/documentation/dirxmldrivers/index.html)」にある、Active Directory および NT ドメイン用 Identity Manager ドライバのドライバ実装ガイドのアップグレード手順に従います。

この手順で追加されるポリシーは、ユニバーサルパスワードおよび配布パスワードを使用し、パスワード同期をサポートするためのものです。NDS パスワードのみを同期するために Identity Manager ドライバを使用している場合には、このポリシーは Identity Manager ドライバの環境設定に使用できません。で説明するように、NDS パスワードは、これらのポリシーではなく、Public Key および Private Key の属性を使用して、同期化されます。122 ページのセクション 5.8.2「シナリオ 1: NDS パスワードを使用した、2 つの識別ボールト間の同期」

- 112 ページの 「ステップ 1: ドライバを Identity Manager 3.5 形式に変換する」
- 115 ページの 「ステップ 2: ドライバ環境設定に追加する」
- 116 ページの 「ステップ 3: フィルタ設定を変更する」
- 119 ページの 「ステップ 4: パスワード同期のフローを設定する」

前提条件

- ❑ Export Drivers Wizard を使用し、既存のドライバのバックアップを作成します。
- ❑ 新しいドライバシムがインストール済みであることを確認します。

  ［Check Password Status］など、パスワード同期の機 \'94\'5c の中には、Identity Manager のドライバシムがないと機 \'94\'5c しないものもあります。

重要 : Password Synchronization 1.0 で使用されている AD または NT ドメイン用 Identity Manager ドライバをアップグレードする場合は、アップグレード手順を確認してから、ドライバシムをインストールしてください。手順については、「Identity Manager Drivers (http://www.novell.com/documentation/dirxmldrivers/index.html)」にある Active Directory および NT ドメイン用 Identity Manager ドライバのドライバ実装ガイドのアップグレードの説明に従います。

5.7.1 ステップ 1: ドライバを Identity Manager 3.5 形式に変換する

1 現在の環境でユニバーサルパスワードを使用する準備ができていることを確認します。

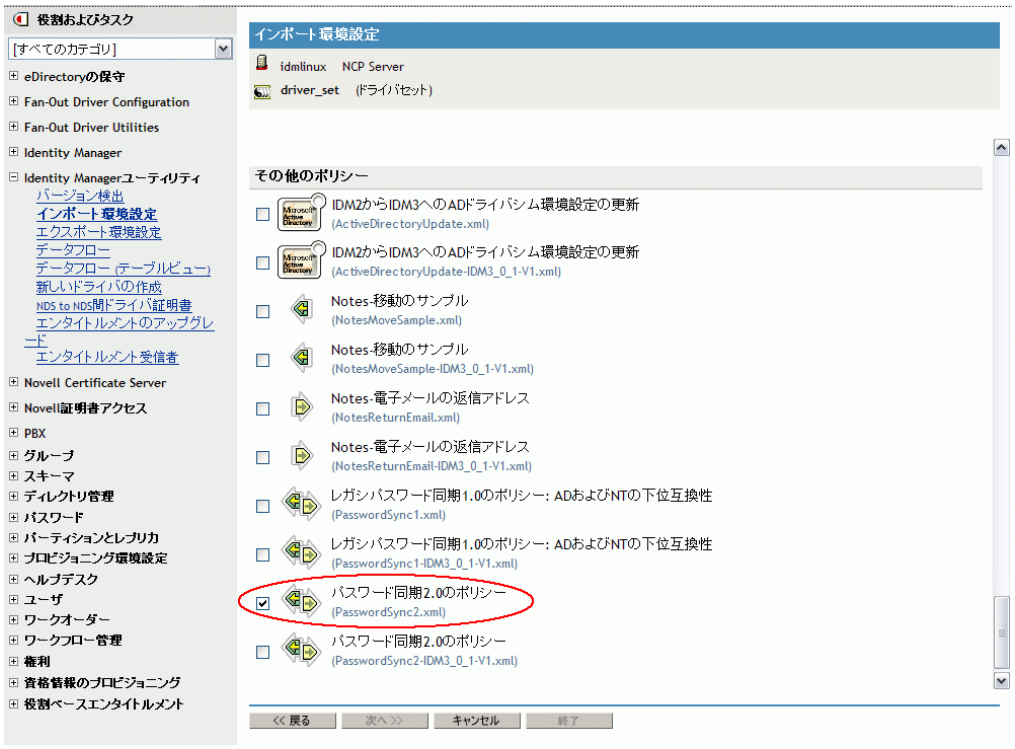
  詳細については、105 ページのセクション 5.4「Identity Manager パスワード同期およびユニバーサルパスワードを使用するための準備作業」を参照してください。

  DirXML® 1.1a を使用している場合、23 ページのセクション 2.3「ドライバ設定を DirXML 1.1a から Identity Manager3.5.1 形式にアップグレードする」を参照してください。

2 iManager で、［Identity Manager ユーティリティ］>［*ドライバのインポート*］の順にクリックします。

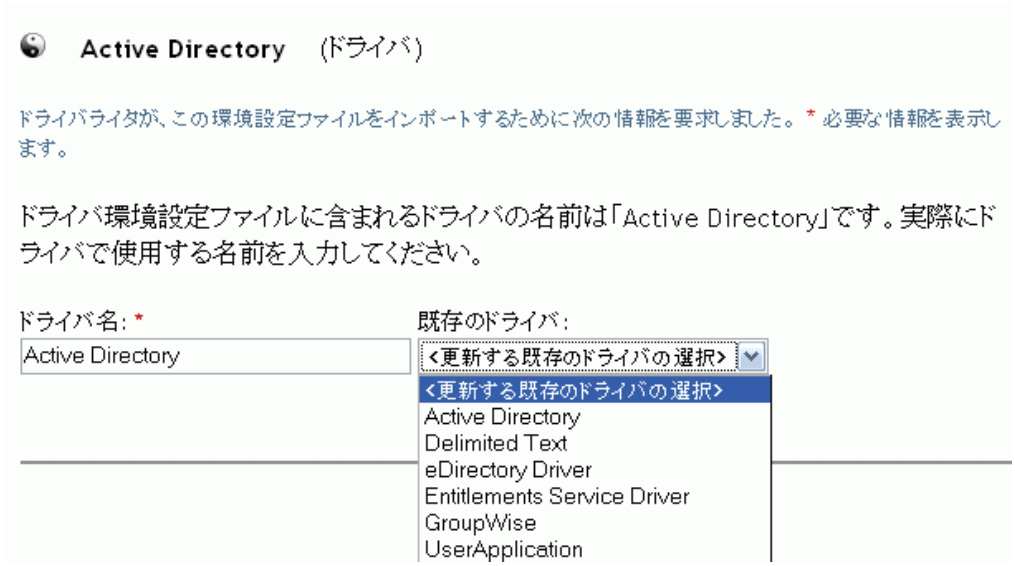
3 既存のドライバの存在するドライバセットを選択し、［*Next*］*をクリックします。*

4 表示されるドライバ環境設定のリストで、［*その他のポリシー*］までスクロールし、［*パスワード同期 2.0 のポリシー*］のみを選択します。



5 ［*次へ*］をクリックします。

6 ［*Existing drivers*］ドロップダウンリストで、*更新する既存のドライバを選択します。*



7 ［*Connected System*］ドロップダウンリストで、*接続システムのタイプを選択します。*

ドロップダウンリストにドライバ名が \'95\'5c 示されない場合、［*Other Systems*］*を選択します。*

ドライバのタイプに基づき、Import Driver Wizard は、ドライバ設定の機 \'94\'5c と接続システムを示すドライバ \'83\'7d ニフェストのエントリを作成します。

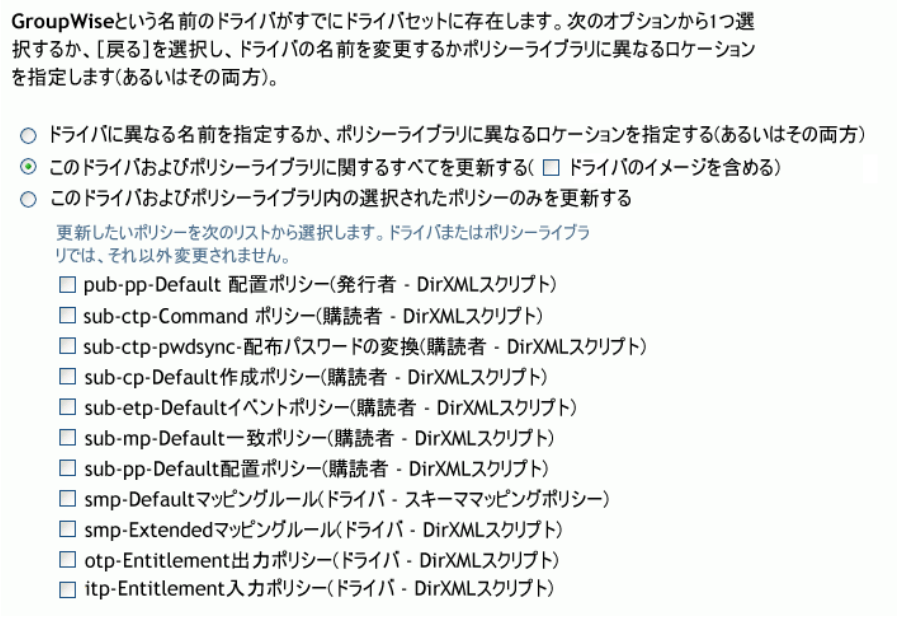
- 接続システムが Identity Manager にパスワードを提供できるかどうか。

これは、スタイルシートを使用して作成できるパスワードではなく、接続システム上のユーザの実際のパスワードを参照します。これが可 \'94\'5c なのは、Active Directory、eDirectory、および NIS のみです。

- 接続システムがIdentity Managerからのパスワードを受け入れることができるかどうか。
- パスワードが Identity Manager のパスワードに一致しているかを、接続システムが確認できるかどうか。

パスワード同期のポリシーが機能するには、正しいドライバマニフェストのエントリが必要です。ドライバマニフェストは、接続システム、Identity Manager のドライバシム、およびドライバ環境設定ポリシーを結合した機能を示し、通常はネットワーク管理者が編集することはできません。

8 ［*次へ*］をクリックします。



9 保存するドライバ \'83\'7d ニフェストまたは GCV 値がない場合、［*Update everything about that driver*］*を選択します。*

このオプションでは、パスワード同期に必要なドライバ \'83\'7d ニフェスト、GCV、および Identity Manager ポリシーを指定します。

ドライバマニフェストおよび GCV によって、すでに存在する値が上書きされます。Identity Manager 2 ではこれらの種類のドライバパラメータは新しいため、DirXML 1.*x* ドライバには上書きされる既存の値はありません。

パスワード同期のポリシーは、既存のポリシーオブジェクトを上書きしません。単にドライバオブジェクトに追加されます。

注 : 保存するドライバマニフェストまたは GCV 値がない場合、［*該当ドライバで選択したポリシーのみを更新*］を選択し、すべてのポリシーのチェックボックスをオンにします。このオプションでは、パスワードポリシーがインポートされますが、ドライバマニフェストまたは GCV は変更されません。追加する値がある場合には、手動で \'93\'5c り付ける必要があります。

---

10 ［*Next*］*をクリックし、*［Finish］をクリックしてウィザードを完了します。

この時点で、新しいポリシーはドライバオブジェクトの下のポリシーオブジェクトとして作成されていますが、ドライバ設定の一部にはなっていません。設定にリンクさせるには、発行者および加入者チャネルのドライバ設定右側のポイントに、各ポリシーを手動で \'91\'7d 入する必要があります。

5.7.2 ステップ 2: ドライバ環境設定に追加する

追加するポリシーのリスト、およびその \'91\'7d 入場所については、101 ページのセクション 5.3.4「ドライバ設定で必要なポリシー」を参照してください。

新しい各ポリシーを既存のドライバ設定の正しい場所に \'91\'7d 入します。

ポリシーセットに複数のポリシーがある場合、これらの Identity Manager のパスワード同期のポリシーが最後に \'95\'5c 示されているようにしてください。

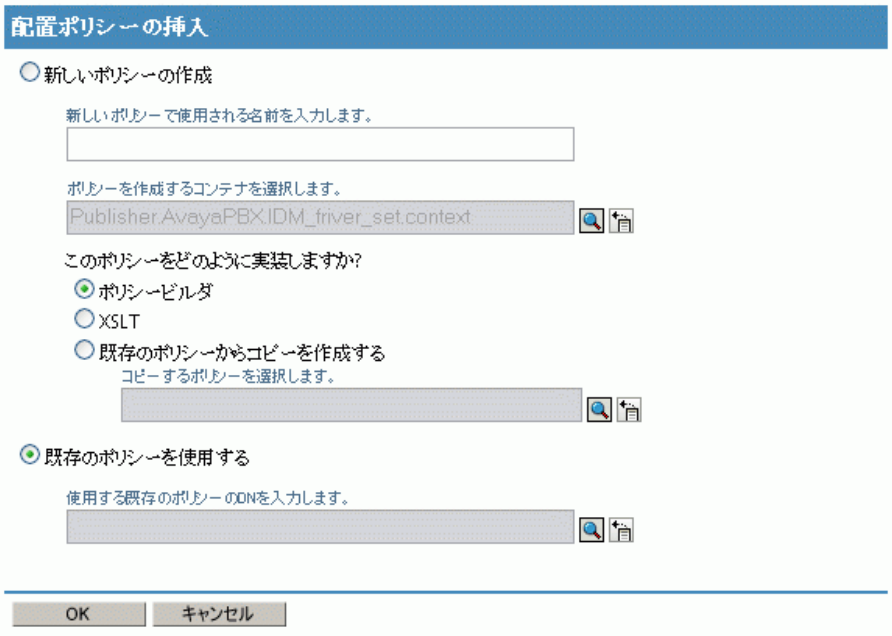
ポリシーごとに、次のステップを繰り返します。

1 ［*Identity Manager*］>［*Identity Manager の概要*］*の順に選択し、更新するドライバが含まれているドライバセットを検索します。*

2 (AvayaPBX などの) 更新したドライバをクリックします。

3 新しいポリシーを追加する必要がある場所のアイコン (発行者チャネルの［Command Transformation Policies］など) をクリックします。

4 ［挿入］*をクリックし、新しいポリシーを追加します。*



5 ［*Use an existing policy*］をクリックし、*新しいポリシーオブジェクトを参照して*［OK］をクリックします。

6 新しいポリシーでリストに複数のポリシーがある場合、矢印ボタンを使用して、新しいポリシーをリスト内の正しい場所に移動します。

にリスト \'95\'5c 示されている順序にポリシーが \'95\'5c 示されていることを確認します。101 ページのセクション 5.3.4「ドライバ設定で必要なポリシー」

5.7.3 ステップ 3: フィルタ設定を変更する

1 パスワードを同期化するオブジェクトクラス (ユーザなど) については、フィルタに nspmDistributionPassword 属性があり、次の設定になっていることを確認します。

- 発行者チャネルについては、フィルタが *nspmDistributionPassword 属性*を無視するよう設定します。
- 加入者チャネルについては、フィルタが *nspmDistributionPassword 属性*を通知するよう設定します。

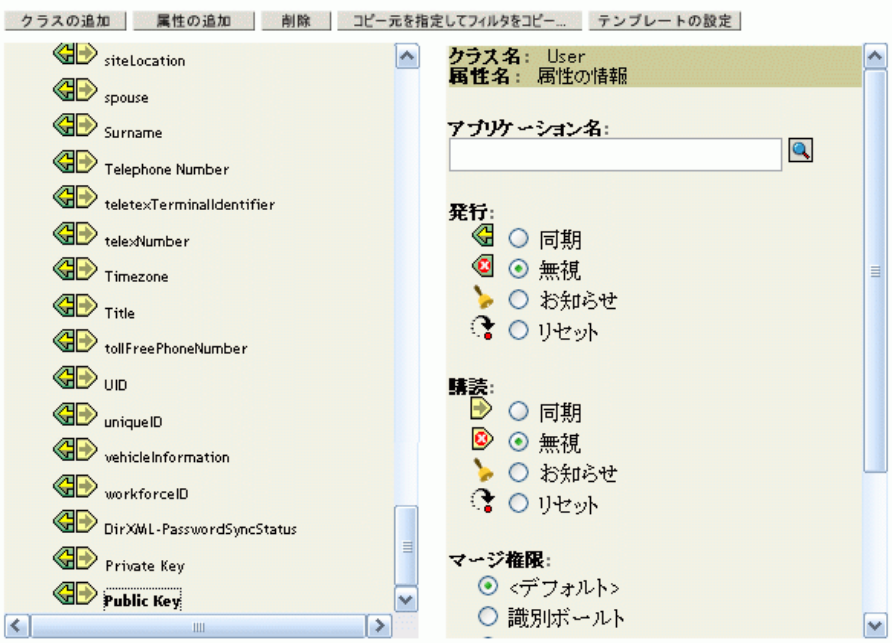
属性を表示するには、スクロールしてクラス (ユーザなど) を選択し、属性をスクロールする必要があります。

nspmDistributionPassword が一覧 \'95\'5c 示されない場合は、

1a クラスが選択されていることを確認し、［*Add Attribute*］*をクリックします。*

1b nspmDistributionPassword までスクロールして選択し、［OK］をクリックします。

2 ［*nspmDistributionPassword*］*属性が*［Notify］に設定されているすべてのオブジェクトでは、Public Key および Private Key 属性の両方を［Ignore］に設定します。



3 パスワード同期に使用するためにアップグレードする各ドライバで、(「Identity Manager 3.5 の形式に、ドライバを変換する」の)112 ページのステップ 2 から、この節 (「フィルタ設定の変更」) のステップ 2 までを繰り返します。

この時点で、ドライバには、新しいドライバシム、Identity Manager 形式、およびその他のパスワード同期をサポートするために必要なドライバ設定の要素が設定されます。これらの要素は、ドライバ \'83\'7d ニフェスト、GCV、パスワード同期化ポリシー、およびフィルタ設定です。

4 個々のドライバの導入ガイドで、Identity Manager のパスワード同期の設定に関する追加的なステップまたは情報について確認してください。「Identity Manager Drivers (http://www.novell.com/documentation/lg/dirxmldrivers/index.html)」を参照してください。

5 ユニバーサルパスワードが有効なパスワードポリシーを作成し、ユニバーサルパスワードをオンにします。

『*パスワード管理ガイド*(http://www.novell.com/documentation/password_management/index.html)』の「Creating Password Policies」を参照してください。NetWare 6.5 でユニバーサルパスワードを以前使用したことがある場合、『*Password Management Administration Guide*』の「(NetWare 6.5 Only) Re-Creating Universal Password Assignments」で、いくつかの追加的なステップについて説明しています。

パスワードポリシーは、ツリーのできるだけ上位のレベルに割り当てることをお勧めします。

[環境設定オプション] ページには、NMAS で同期された異なる種類のパスワードを保持する方法を選択するオプションがあります。ほとんどの実装では、デフォルト設定で動作します。詳細については、そのページのオンラインヘルプを参照してください。

パスワード同期の使用のシナリオ、およびパスワードポリシーの適用方法については、120 ページのセクション 5.8「パスワード同期の実装」を参照してください。

NMAS パスワードポリシーはツリー中心で割り当てられます。一方、パスワード同期はドライバごとに設定されます。ドライバはサーバごとにインストールされ、マスタレプリカまたは読み書き可能レプリカのユーザのみ管理できます。

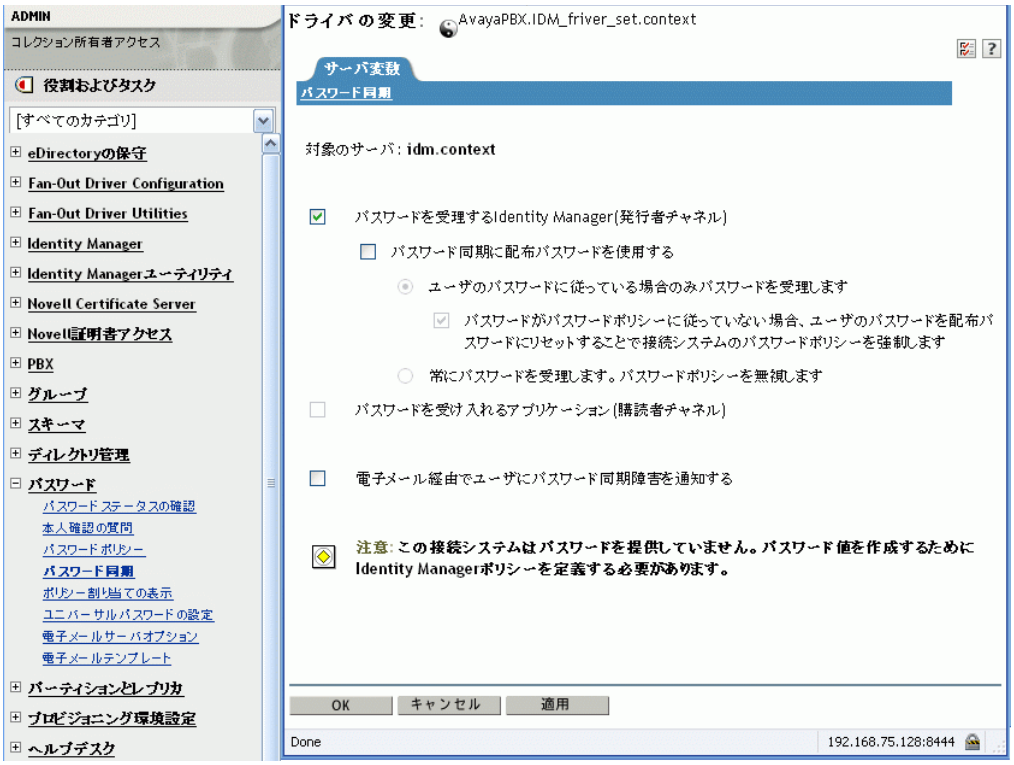
パスワード同期により期待される結果を取得するには、パスワード同期を実行するサーバにあるマスタレプリカまたは読み書き可能レプリカのコンテナが、ユニバーサルパスワードが有効なパスワードポリシーを割り当てたコンテナと一致するようにします。パーティションルートコンテナにパスワードポリシーを割り当てることによって、そのコンテナとサブコンテナ内のすべてのユーザに確実にパスワードポリシーが割り当てられます。

5.7.4 ステップ 4: パスワード同期のフローを設定する

パスワードフローが各接続システムに対して希望する方法で設定されていることを確認します。

1. iManager で、［*Passwords*］> ［Password Synchronization］の順に選択します。
2. 管理する接続システム用のドライバのツリーまたはコンテナを検索します。

3. ドライバを選択し、パスワードフローの現在の設定を \'95\'5c 示します。



このページに、グローバル構成値 (GCV) が一覧表示されます。オプションを選択して変更します。

Identity Manager はエントリポイント、つまりどのパスワードを Identity Manager が更新するかを制御します。NMAS では、［環境設定オプション］で設定したオプションに基づいて、異なる種類のパスワード間のパスワードフローが制御されます。(100 ページのステップ 3 に［環境設定オプション］ページが示されています)。［*パスワード同期に配布パスワードを使用する*］を選択した場合、Identity Manager では配布パスワードが直接使用されます。このオプションをオフにした場合、Identity Manager ではユニバーサルパスワードが直接使用されます。

(図を含む) これらのオプションの詳細については、120 ページのセクション 5.8「パスワード同期の実装」を参照してください。オンラインヘルプも参照してください。

4 パスワード同期をテストします。

Identity Manager のパスワードが指定したシステムに配布されることを確認します。

指定した接続システムが Identity Manager にパスワードを公開しているかを確認します。

トラブルシューティングのヒントについては、120 ページのセクション 5.8「パスワード同期の実装」を参照してください。

5.8 パスワード同期の実装

Identity Manager で提供されているパスワード同期の機能により、いくつかの異なるシナリオを実装できます。このセクションでは、基本シナリオについて説明し、Identity Manager のパスワード同期と NMAS パスワードポリシーの設定がパスワード同期の方法

にどのように影響を与えるかについて理解するために役立つ情報を提供します。現在の環境のニーズに合わせて、1 つまたは複数のシナリオ使用できます。

- 121 ページのセクション 5.8.1「Identity Manager と NMAS の関係の概要」
- 122 ページのセクション 5.8.2「シナリオ 1: NDS パスワードを使用した、2 つの識別ボールト間の同期」
- 125 ページのセクション 5.8.3「シナリオ 2: ユニバーサルパスワードを使用したパスワードの同期」
- 136 ページのセクション 5.8.4「シナリオ 3: Identity Manager で配布パスワードを更新することで、識別ボールトと接続システムを同期する」
- 145 ページのセクション 5.8.5「シナリオ 4: トンネル」
- 150 ページの 「シナリオ 5: アプリケーションパスワードを単純パスワードに同期する」

5.8.1 Identity Manager と NMAS の関係の概要

- 121 ページの 「ユーティリティと NMAS」
- 122 ページの 「Identity Manager と NMAS」

ユーティリティと NMAS

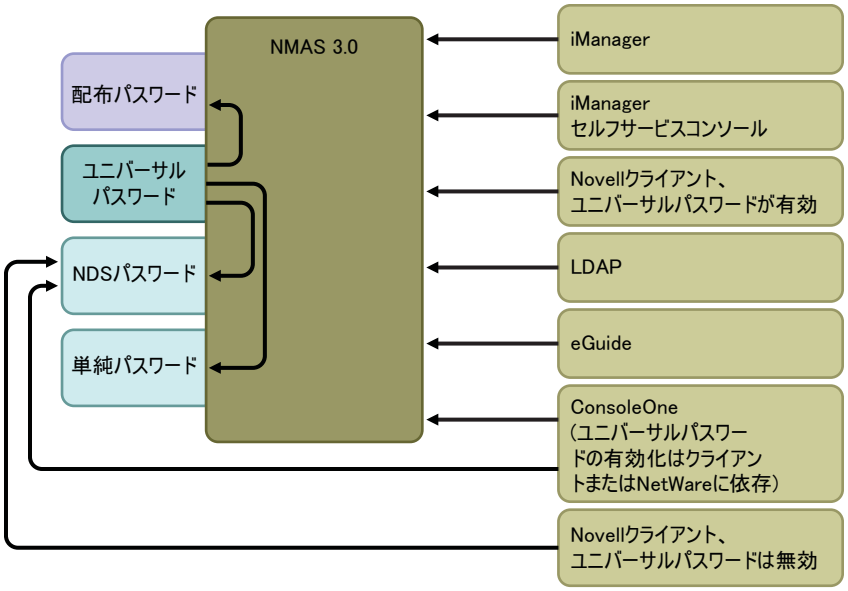
iManager などのユーティリティと Novell Client は、特定のパスワードを直接更新せずに、NMAS と通信します。NMAS は、どのパスワードが更新されるのかを決定するエンティティです。

NMAS パスワードポリシーの設定に基づいて、NMAS が識別 \'83\'7bールト内でパスワードを同期します。

ユニバーサルパスワードが有効でないレガシーユーティリティは、NDS パスワードを直接更新します。NMAS と通信し、NMAS がどのパスワードを更新するかを決定するのではありません。ユーザおよびヘルプデスクの管理者が環境内でレガシーユーティリティをどのように使用するかに留意してください。レガシーユーティリティは、NDS パスワードを NMAS と通信せずに直接更新するため、ユニバーサルパスワードと NMAS 2.3 を使用している場合、パスワードドリフト (ユニバーサルパスワードと NDS パスワードとの同期がずれる状態) が発生する場合があります。

たとえば、ユニバーサルパスワードのサポートを確認するには、ユーザが Novell Client をアップグレードしていることを確認し、ヘルプデスクのユーザが ConsoleOne を最新の Novell Client または NetWare リリースのみで使用していることを確認します。

図 5-5 NMAS を使用したパスワードの同期



Identity Manager と NMAS

Identity Manager は、「エントリポイント」を制御します (ユニバーサルパスワードまたは配布パスワードを直接更新します)。NMAS は、識別 \'83\'7bールト内のパスワード同期のフローを制御します。

シナリオ 1 では、eDirectory の Identity Manager ドライバを使用して、NDS パスワードを直接更新できます。このシナリオは基本的に、DirXML 1.*x* で提供されるものと同じです。

シナリオ 2、シナリオ 3、およびシナリオ 4 では、Identity Manager を使用して、ユニバーサルパスワードまたは配布パスワードを更新します。Identity Manager は NMAS と通信して、パスワードを変更します。これにより、NMAS は NMAS パスワードポリシーの設定の決定に基づき他の識別ボールトパスワードを更新し、パスワードを接続システムと同期できるように、NMAS パスワードポリシーから高度なパスワードルールを適用できます。これらのシナリオでは、接続システムに Identity Manager が配布するパスワードは、必ず配布パスワードとなります。

シナリオ 2、シナリオ 3、およびシナリオ 4 の間での違いは、NMAS パスワードポリシーセットとそれぞれの接続システムドライバ用の Identity Manager のパスワード同期の設定の異なる組み合わせにあります。

5.8.2 シナリオ 1: NDS パスワードを使用した、2 つの識別ボールト間の同期

Password Synchronization 1.0 と同様に、eDirectory ドライバを使用して 2 つの識別ボールト間で NDS パスワードを同期できます。このシナリオでは、ユニバーサルパスワードの実装は必要なく、eDirectory 8.6.2 以降で使用できます。この種類のパスワード同期は、公開鍵と秘密鍵のペアの同期化とも呼ばれます。

この方法は、識別ボールト間でパスワードを同期する場合のみ使用します。この方法は NMAS を使用しないので、接続アプリケーションとパスワードを同期する目的では使用できません。

- 123 ページの 「シナリオ 1 の長所と短所」
- 124 ページの 「シナリオ 1 の設定」
- 125 ページの 「シナリオ 1 のトラブルシューティング」

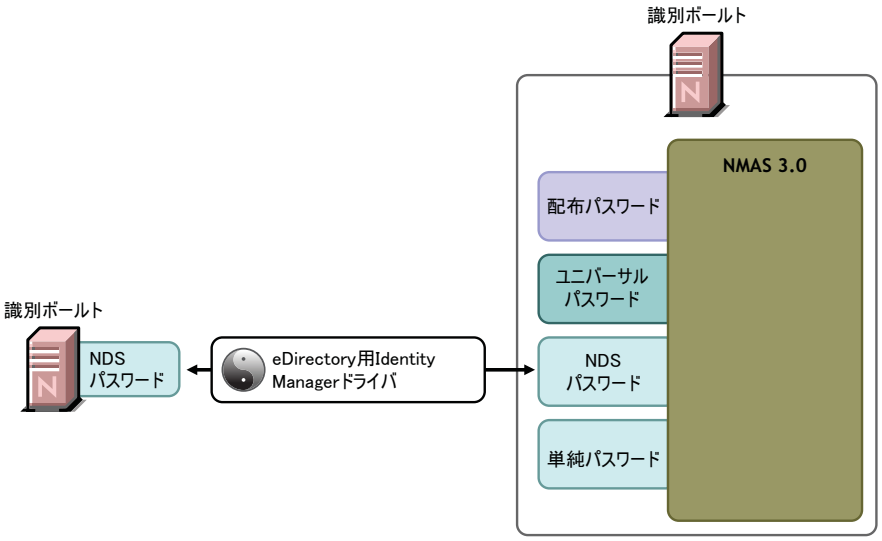
シナリオ 1 の長所と短所

表 5-11 *長所 : NDS パスワードを使用した eDirectory 間でのパスワード同期*

長所	短所
設定が簡単です。ドライバフィルタに正しい属性を含めるだけです。 各ステージで Identity Manager および eDirectory 8.7.3 を実装する場合、この方法により段階的に実装できます。 • 新しいパスワード同期のポリシーをドライバ設定に追加する必要がない。 • ユニバーサルパスワードを識別 \'83\'7b一ルトに実装する必要がない。 • eDirectory 8.6.2 以降を実行している接続された \'83\'7b一ルトで使用できる。 • NMAS 2.3 は必要ない。 NDS パスワードに設定した基 \'96\'7b 的なパスワード制限を適用します。	この方法は、識別ボールト間でパスワードを同期します。他の接続システムとパスワードを同期化することはできません。 ユニバーサルパスワードまたは配布パスワードはアップデートされません。 NMAS を使用しないので、別の識別 \'83\'7b一ルトからのパスワードに対して設定したパスワードポリシーの高度なパスワードルールとの照合によってパスワードを検証できません。 NMAS を使用しないので、パスワードが NMAS パスワードポリシーに準拠していない場合でも、接続された識別 \'83\'7b一ルトでパスワードをリセットできません。 パスワード同期化に失敗したパスワードについては、電子メール通知は使用できません。 iManager のタスクの［パスワードステータスの確認］操作はサポートされていません。(この機 \'94\'5c では配布パスワードが必要です。)

次の図は、DirXML 1.*x* と同様、eDirectory の Identity Manager ドライバを使用して 2 つの識別ボールト間で NDS パスワードを同期できることを示しています。このシナリオでは、NMAS と通信しません。

図 5-6 NDS パスワードを使用した、2 つの識別\'83\'7bールト間の同期



シナリオ 1 の設定

この種類のパスワード同期を設定するには、ドライバを設定します。

ユニバーサルパスワードの展開

必要ありません。

Password Policy (パスワードポリシー) の設定

なし。

パスワード同期の設定

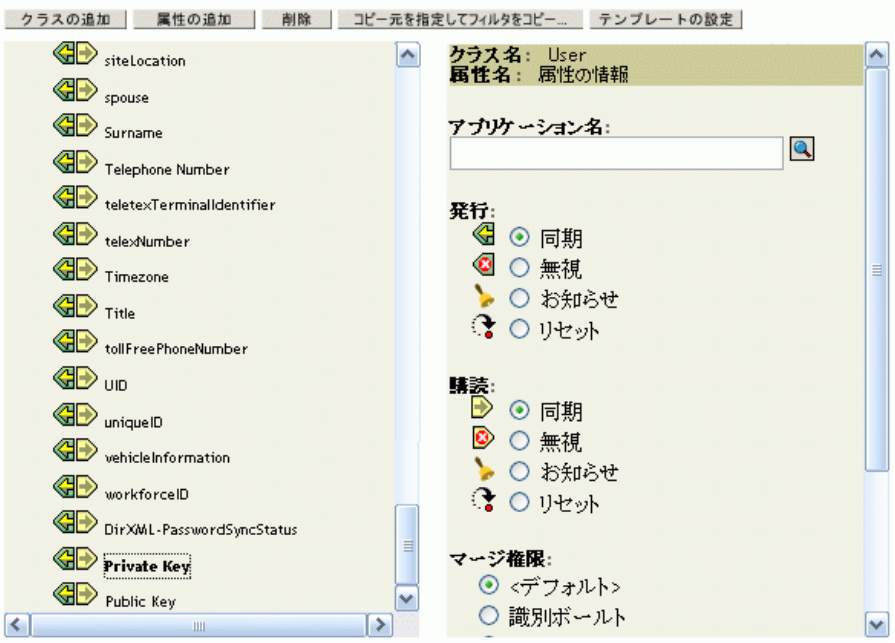
なし。ドライバの［Password Synchronization］ページの設定は、この方法の NDS パスワード同期には影響しません。

ドライバ設定

101 ページのセクション 5.3.4「ドライバ設定で必要なポリシー」に一覧表示されているパスワード同期のポリシーを削除します。これらのポリシーは、ユニバーサルパスワードおよび配布パスワードをサポートするためのものです。NDS パスワードは、これらのポリシーではなく、Public Key および Private Key の属性を使用して、同期化されます。

両方の識別ボールトドライバのドライバフィルタによって、パスワードを同期するすべてのオブジェクトクラスの公開鍵および秘密鍵の属性が同期されていることを確認します。次の \'90\'7d は、例を示します。

図 5-7 Private 属性と Public Key 属性の同期



シナリオ 1 のトラブルシューティング

- ［DStrace］オプションをオンにします。
- ドライバフィルタについて、Public Key と Private Key の属性が同期化されており、無視されていないことを確認します。
- のヒントも参照してください。169 ページのセクション 5.13「パスワード同期のトラブルシューティング」

5.8.3 シナリオ 2: ユニバーサルパスワードを使用したパスワードの同期

Identity Manager では、接続システムのパスワードを識別 \'83\'7bールトのユニバーサルパスワードに同期化できます。

ユニバーサルパスワードがアップデートされると、NMAS パスワードポリシーの設定により、NDS パスワード、配布パスワード、または通常パスワードもアップデートできます。

接続システムはパスワードを Identity Manager に発行できますが、すべての接続システムがユーザの実際のパスワードを提供できるわけではありません。たとえば、Active Directory はユーザの実際のパスワードを Identity Manager に発行できます。PeopleSoft は PeopleSoft システム自体からパスワードを提供することはできませんが、ユーザの従業員 ID または名字に基づくパスワードなど、ドライバ設定のポリシーで作成された初期パスワードは提供できます。すべてのドライバが Identity Manager からのパスワードの変更を購読できるわけではありません。詳細については、94 ページのセクション 5.2「パスワード同期をサポートする接続システム」を参照してください。

- 126 ページの 「シナリオ 2 の長所と短所」

- 127 ページの 「シナリオ 2 の設定」
- 132 ページの 「シナリオ 2 のトラブルシューティング」

シナリオ 2 の長所と短所

表 5-12 *長所 : ユニバーサルパスワードを使用した同期*

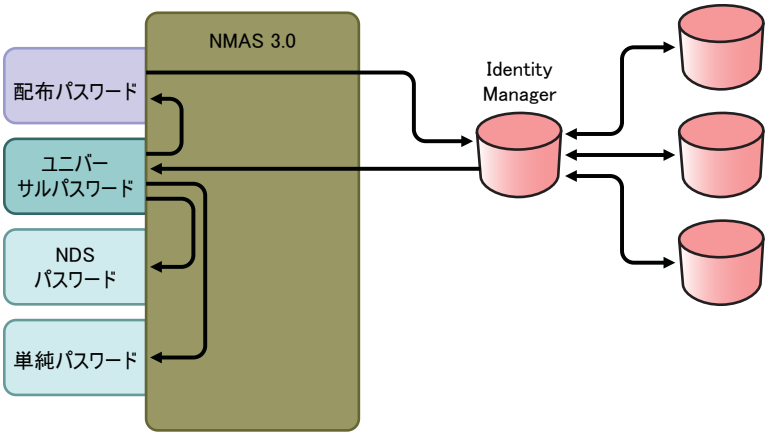
長所	短所
識別 \'83\'7bールトおよび接続システムとのパスワードの同期が可 \'94\'5c です。 パスワードを NMAS パスワードポリシーと照合して検証できます。 接続システムから受信したパスワードがパスワードポリシーに準拠していない場合など、失敗したパスワード操作を電子メールで通知できます。 ユニバーサルパスワードが配布パスワードと同期化され、接続システムがパスワードの確認をサポートする場合、iManager の［Check Password Status］タスクをサポートします。 NMAS は、ルールが有効にされている場合、パスワードポリシーの高度なパスワードルールを適用します。接続システムから受信したパスワードがルールに準拠していない場合、エラーが生成され、オプションで指定しているときは電子メール通知が送信されます。 パスワードポリシーのルールを適用しない場合は、NMAS パスワードポリシーの［*高度なパスワードルールを有効にする*］チェックボックスをオフにできます。	設計上、接続システムのパスワードのリセットはこの方法ではサポートされません。パスワードポリシーの設定によっては、配布パスワードとユニバーサルパスワードが同一でないことがあるためです。

図 5-8 は、このシナリオの以下のフローを示しています。

1. パスワードが、Identity Manager を通って来る。
2. Identity Manager が NMAS と通信して、ユニバーサルパスワードを直接アップデートする。
3. NMAS が、ユニバーサルパスワードを、配布パスワードおよび NMAS パスワードポリシー設定に従って、その他のパスワードに同期化する。
4. Identity Manager が配布パスワードを取得し、パスワードを受諾するよう設定されている接続システムに配布する。

この \'90\'7d では複数の接続システムが Identity Manager に接続しているように示されていますが、接続システムのドライバごとに設定を作成することに注意してください。

図 5-8 ユニバーサルパスワードを使用したパスワードの同期



シナリオ 2 の設定

この種類のパスワード同期を設定する

- 127 ページの 「ユニバーサルパスワードの展開」
- 127 ページの 「Password Policy (パスワードポリシー) の設定」
- 129 ページの 「パスワード同期の設定」
- 131 ページの 「ドライバ設定」

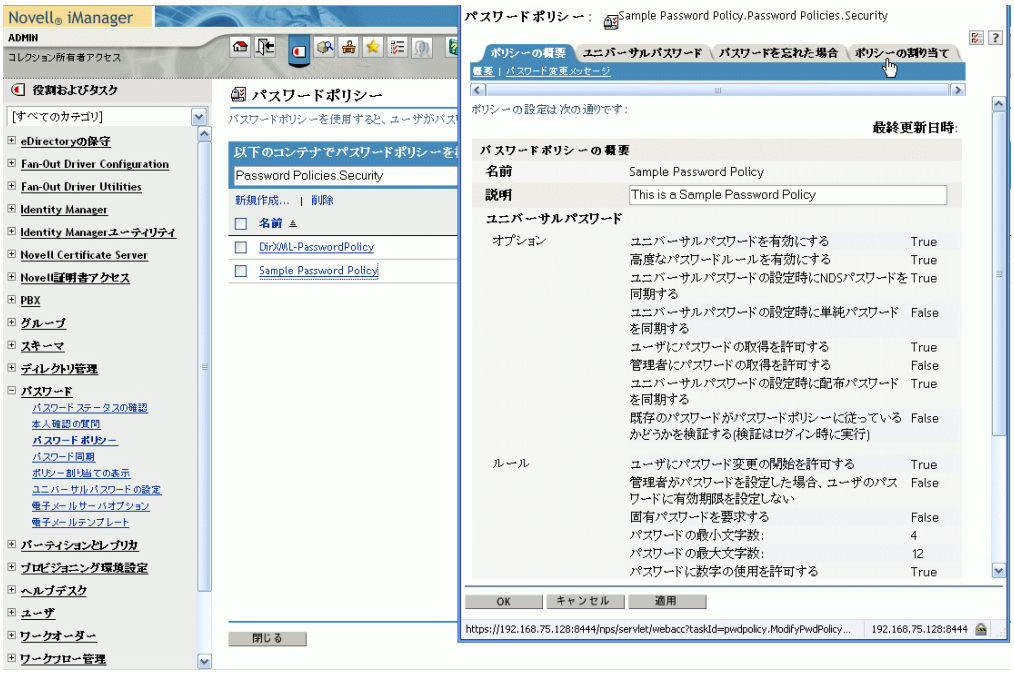
ユニバーサルパスワードの展開

現在の環境でユニバーサルパスワードを使用する準備ができていることを確認します。詳細については、105 ページのセクション 5.4「Identity Manager パスワード同期およびユニバーサルパスワードを使用するための準備作業」を参照してください。

Password Policy (パスワードポリシー) の設定

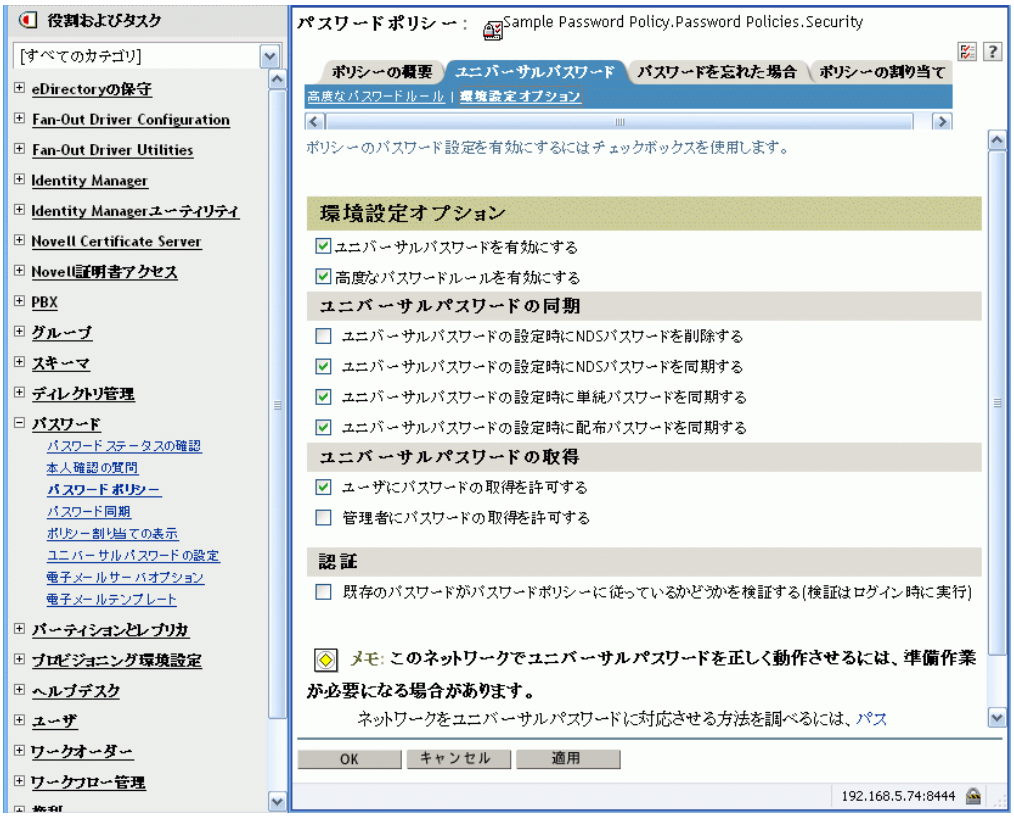
NMAS パスワードポリシーが、この種類のパスワード同期を実行したい識別 \'83\'7bールトの一部に割り当てられていることを確認してください。

1. iManager で、［*Passwords*］> ［Password Policies］の順に選択します。
2. ポリシーを選択し、［*Edit*］をクリックします。
3. パスワード同期を実行するオブジェクトを参照して選択します。



ツリー構造全体 (セキュリティコンテナのログインポリシーオブジェクトを参照して選択する)、パーティションルートコンテナ、コンテナ、または特定のユーザに、ポリシーを割り当てることができます。管理を簡易化するには、ツリー内のできるだけ高い位置にパスワードポリシーを割り当てることをお勧めします。

4 ［Password Policy］で、次のオプションが選択されていることを確認します。



- *ユニバーサルパスワードを有効にする*
- *ユニバーサルパスワードの設定時に NDS パスワードを同期する*
- *ユニバーサルパスワードの設定時に配布パスワードを同期する*

  Identity Manager は配布パスワードを取得して接続システムに配布するので、双方向のパスワード同期を可 \'94\'5c にするためにこのオプションをオンにすることが重要です。

5 必要に応じ、［Password Policy］の他の設定を完了します。

NMAS では、ルールが有効にされている場合、パスワードポリシーの高度なパスワードルールが適用されます。パスワードポリシーのルールを適用しない場合は、［*高度なパスワードルールを有効にする*］チェックボックスをオフにします。

高度なパスワードルールを使用している場合、パスワードを受信している接続システムのパスワードポリシーと競合しないことを確認します。

パスワード同期の設定

1 iManager で、［*Passwords*］> ［Password Synchronization］の順に選択します。

2 接続システムのドライバを検索し、ドライバを選択します。

3 接続システムのドライバの設定を作成します。

次のオプションが選択されていることを確認します。

- *パスワードを受理する Identity Manager(発行者チャネル)*

  ドライバマニフェストに「password-publish」機能が含まれていない場合、メッセージがページに表示されます。これは、パスワードがアプリケーションから取得できず、パスワードを発行するには、ポリシーを使用してドライバ設定にパスワードを作成するしかないことをユーザに通知するものです。

- *パスワードを受け入れるアプリケーション (購読者チャネル)*

  接続システム j がパスワードの受け入れをサポートしない場合、このオプションは淡色 \'95\'5c 示になります。

これらの設定により、接続システムでサポートされている場合には、双方向のパスワード同期が可 \'94\'5c になります。

パスワードの信頼されたソースについては、ビジネスポリシーに合わせて設定を調整できます。たとえば、接続システムがパスワードを購読するが発行しないようにする場合は、[*Application accepts passwords (Subscriber Channel)*] のみを選択します。

4 [*パスワード同期に配布パスワードを使用する*] がオフになっていることを確認します。

このシナリオでは、Identity Manager がユニバーサルパスワードを直接更新します。接続システムへのパスワードの配布には引き続き配布パスワードが使用されますが、配布パスワードは、Identity Manager ではなく NMAS により、ユニバーサルパスワードからアップデートされます。

5 (オプション) 必要に応じ、次のオプションを選択します。

- *電子メール経由でユーザにパスワード同期障害を通知する*

  電子メール通知には、eDirectory ユーザオブジェクトの Internet EMail Address 属性の入力が必要です。

電子メール通知は、他に影響を与えません。これらは、電子メールをトリガしたXML ドキュメントの処理には影響しません。失敗した場合、操作自体が再試行されない限り、電子メール通知は再試行されません。ただし、電子メール通知のデバッグメッセージはトレースファイルに書き込まれます。

ドライバ設定

1 必要な Identity Manager スクリプトパスワード同期化ポリシーが、パスワード同期に使用する各ドライバのドライバ設定に含まれていることを確認します。

ポリシーは、ドライバ設定の正しい位置に正しい順序で記述されている必要があります。ポリシーのリストについては、101 ページのセクション 5.3.4「ドライバ設定で必要なポリシー」を参照してください。

Identity Manage のサンプル設定には、すでにポリシーが含まれています。既存のドライバをアップデートする場合は、111 ページのセクション 5.7「パスワード同期をサポートするための、既存のドライバ設定のアップグレード」のステップを使用してポリシーを追加できます。

2 nspmDistributionPassword 属性のために、フィルタを正しく設定します。

- 発行者チャネルについては、ドライバフィルタがすべてのオブジェクトクラスの *nspmDistributionPassword 属性を無視するよう設定します。*
- 加入者チャネルについては、ドライバフィルタがすべてのオブジェクトクラスの *nspmDistributionPassword 属性を通知するよう設定します。*

3 ［nspmDistributionPassword］属性が［*Notify*］*に設定されているすべてのオブジェクトでは、Public Key および Private Key 属性の両方を*［Ignore］に設定します。

4 パスワードのセキュリティを確保するには、Identity Manager のオブジェクトへの権利を持つユーザを制御していることを確認します。

シナリオ 2 のトラブルシューティング

- 133 ページの 「シナリオ 2 のフローチャート」
- 133 ページの 「識別 \'83\'7bールトへのログインの問題」
- 134 ページの 「パスワードを購読する別の接続システムへのログインのトラブルシューティング」
- 135 ページの 「パスワードのエラーについての電子メールが生成されない」
- 135 ページの 「[Check the Object Password] を使用した場合のエラー」
- 135 ページの 「DSTrace の便利なコ \'83\'7d ンド」

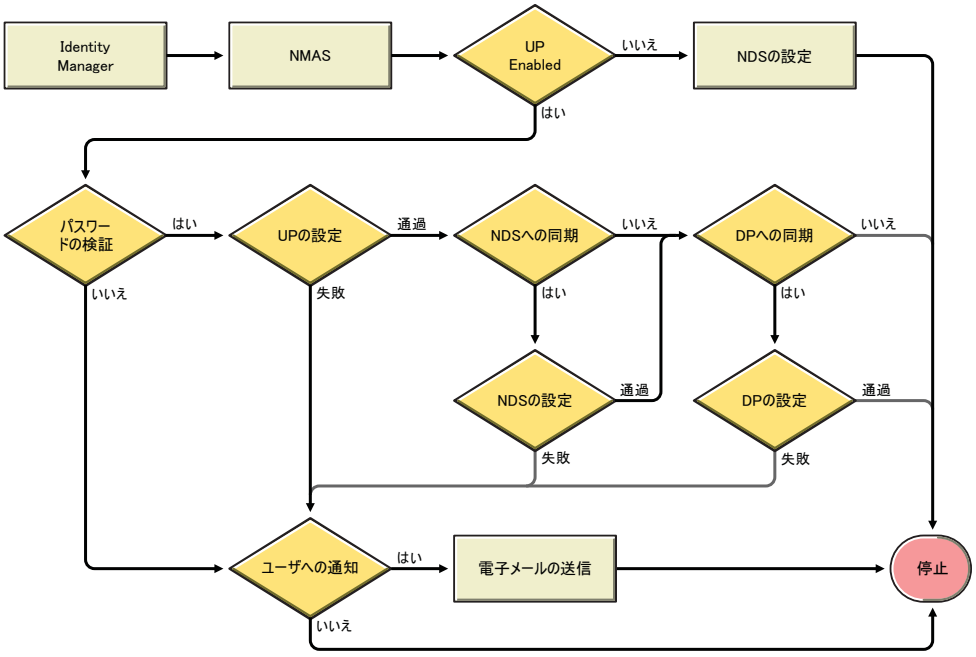
のヒントも参照してください。169 ページのセクション 5.13「パスワード同期のトラブルシューティング」

シナリオ 2 のフローチャート

図 5-9 は、NMAS が Identity Manager から受信するパスワードの処理の方法を示しています。このシナリオでは、パスワードがユニバーサルパスワードに同期されます。NMAS では、次に基づいてパスワードを処理する方法が決定されます。

- NMAS パスワードポリシーで、ユニバーサルパスワードが有効になっているかどうか。
- 着信パスワードが準拠する必要がある高度なパスワードルールが有効になっているかどうか。
- ユニバーサルパスワードとその他のパスワードとを同期するためのパスワードポリシーに、どのようなその他の設定があるのか。

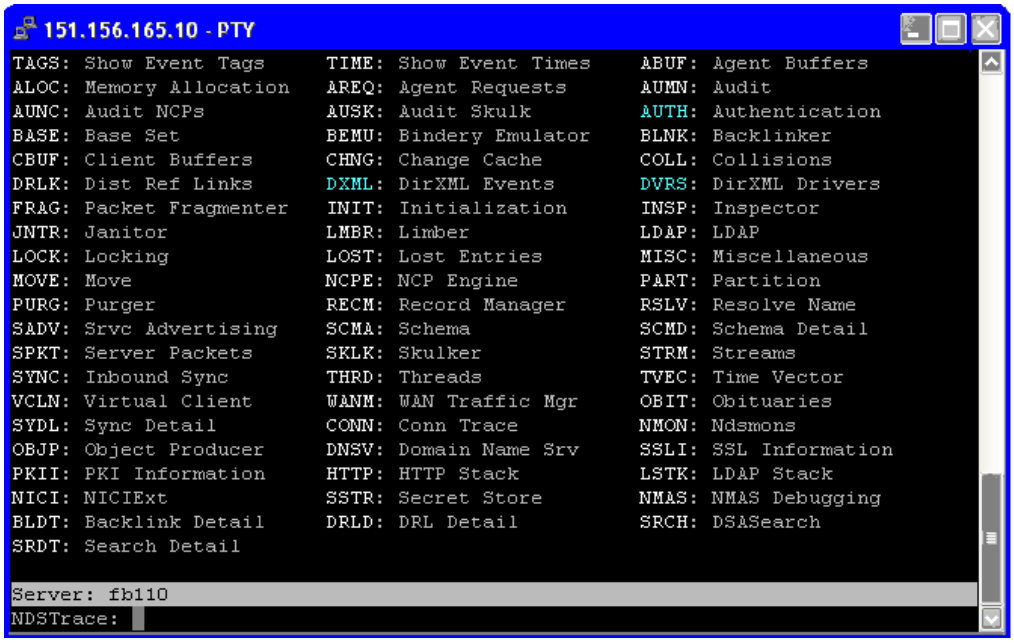
図 5-9 *NMAS が Identity Manager から受信するパスワードの処理の方法*



識別 \'83\'7bールトへのログインの問題

- DSTrace で、［*+AUTH*］、［*+DXML*］、および［*+DVRS*］の設定をオンにします。

図 5-10 DSTrace コ\'83\'7d ンド



- <password>または<modify-password>の要素がIdentity Managerに渡されていることを確認します。渡されていることを確認するには、トレース画面のオプションがオンになっていることを確かめます。
- パスワードポリシーのルールに従い、パスワードが有効であることを確認します。
- NMAS パスワードポリシーの設定と割り当てを確認します。ポリシーをユーザに直接割り当て、正しいポリシーが使用されるようにします。
- ドライバの［Password Synchronization］ページで、［*DirXML accepts passwords*］*が選択されていることを確認します。*
- ［Password Policy］で、［*Synchronize Distribution Password when setting Universal Password*］*が選択されていることを確認します。*

パスワードを購読する別の接続システムへのログインのトラブルシューティング

このセクションでは、この接続システムが Identity Manager にパスワードを発行しているが、そのパスワードを購読するもう 1 つの接続システムがこのシステムからの変更を受信していないように思える場合の、トラブルシューティングについて説明します。この関係は、第 2 の接続システムとも呼ばれ、第 1 の接続システムから Identity Manager を通じてパスワードを受信することを意味します。

- DSTrace の［*+DXML*］および［*+DVRS*］の設定をオンにし、Identity Manager のルール処理を確認します。
- ドライバの Identity Manager のトレースレベルを［*3*］*に設定します。*
- ［Password Synchronization］の［*Identity Manager Accepts Passwords*］*オプションが選択されていることを確認します。*
- ドライバフィルタの nspmDistributionPassword 属性が、131 ページのステップ 2 に説明されているとおりに正しく設定されていることを確認します。

- <*password*> (Addの場合)または<modify-password>の要素が接続システムに送信されていることを確認します。確認するには、［DSTrace］画面またはファイルのトレースオプションが、最初の項目で説明したとおり、オンになっていることを確かめます。
- Identity Manager スクリプトパスワードポリシーが、101 ページのセクション 5.3.4「ドライバ設定で必要なポリシー」で説明されているとおり、ドライバ設定の正しい位置と順序にあることを確認します。
- 識別 \'83\'7bールトの NMAS パスワードポリシーと、接続システムにより適用されるパスワードポリシーと比較し、互換性があることを確認します。

パスワードのエラーについての電子メールが生成されない

- DSTrace の［*+DXML*］の設定をオンにし、Identity Manager のルール処理を確認します。
- ドライバの Identity Manager のトレースレベルを［*3*］*に設定します。*
- 電子メールを生成するルールが選択されていることを確認します。
- 識別 \'83\'7bールトオブジェクトを検証し、ユーザの正しい電子メールアドレスが Internet EMail Address 属性に含まれていることを確認します。
- 通知設定タスクで、SMTP サーバと電子メールテンプレート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、158 ページのセクション 5.12「電子メール通知の設定」を参照してください。

［Check the Object Password］を使用した場合のエラー

iManager のパスワードステータスの確認タスクにより、ドライバでオブジェクトパスワードの確認アクションが発生します。問題が発生した場合は、次を確認します。

- ［オブジェクトパスワードの確認］から -603 が返される場合、識別ボールトブジェクトに nspmDistributionPassword 属性が含まれていません。nspmDistributionPassword 属性に対してドライバフィルタが正しい設定になっていることを確認します。また、パスワードポリシーで［*Synchronize Distribution Password when Setting Universal Password*］*が選択されていることを確認してください。*
- ［Check Object Password］が「Not Synchronized」を返す場合、ドライバ設定に適切なパスワード同期のポリシーが含まれていることを確認します。
- 識別 \'83\'7bールトの NMAS のパスワードポリシーと、接続システムにより適用されるパスワードポリシーと比較し、互換性があることを確認します。
- ［オブジェクトパスワードの確認］は、配布パスワードから起動します。配布パスワードがアップデートされていない場合、［Check Object Password］によって、パスワードが同期化されていることがレポートされないことがあります。
- Identity Manager ドライバのみについては、［Check Password Status］は、配布パスワードではなく NDS パスワードを確認することに注意してください。

DSTrace の便利なコ \'83\'7d ンド

+DXML: Identity Manager ルール処理および可能性のあるエラーメッセージを表示する

+DVRS: Identity Manager ドライバのメッセージを表示する

+AUTH: NDS パスワードの変更を表示する

5.8.4 シナリオ 3: Identity Manager で配布パスワードを更新することで、識別ボールトと接続システムを同期する

このシナリオでは、Identity Manager は配布パスワードを直接アップデートし、他の識別\'83\'7bールトパスワードをどのように同期化するかは NMAS が決定します。

接続システムはパスワードを Identity Manager に発行できますが、すべての接続システムがユーザの実際のパスワードを提供できるわけではありません。たとえば、Active Directory はユーザの実際のパスワードを Identity Manager に発行できます。PeopleSoft は PeopleSoft システム自体からパスワードを提供することはできませんが、ユーザの従業員 ID または名字に基づくパスワードなど、ドライバ設定のポリシーで作成された初期パスワードは提供できます。すべてのドライバが Identity Manager からのパスワードの変更を購読できるわけではありません。詳細については、94 ページのセクション 5.2「パスワード同期をサポートする接続システム」を参照してください。

- 136 ページの 「シナリオ 3 の長所と短所」
- 137 ページの 「シナリオ 3 の設定」
- 141 ページの 「シナリオ 3 のトラブルシューティング」

シナリオ 3 の長所と短所

表 5-13 *長所 : 配布パスワードの更新による、識別ボールトと接続システムの同期*

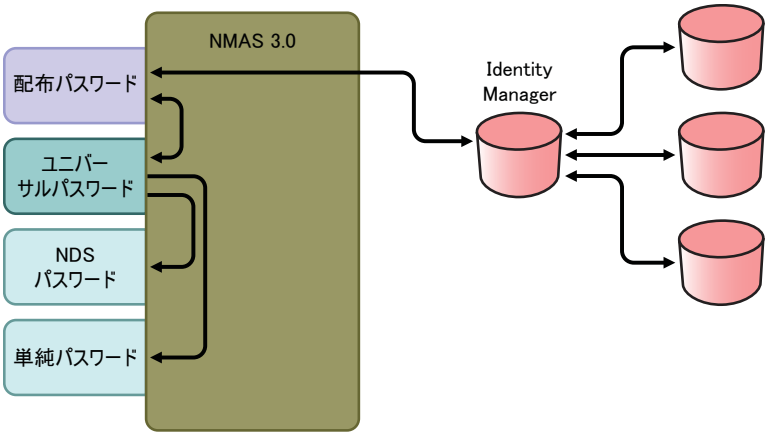
長所	短所
識別 \'83\'7bールトと接続システム間でパスワードを同期化できます。 接続システムから受信したパスワードに対して、パスワードポリシーを適用するかどうかを選択できます。 パスワード同期が失敗した場合に通知を送信するよう指定できます。 パスワードポリシーを適用する場合、接続システムのパスワードがパスワードポリシーに準拠しないときに配布パスワードにリセットするよう選択できます。	

このシナリオの \'90\'7d は、次のフローを示します。

1. パスワードが、Identity Manager を通って来る。
2. Identity Manager が NMAS と通信して、配布パスワードを直接アップデートする。
3. Identity Manager は配布パスワードを使用し、パスワードを受け入れるよう指定した接続システムに配布します。
4. NMAS は、ユニバーサルパスワードを、配布パスワード、およびパスワードポリシー設定に基づいてその他のパスワードに同期化します。

図 5-11 では複数の接続システムが Identity Manager に接続しているように示されていますが、接続システムのドライバごとに設定を作成する点に注意してください。

図 5-11 配布パスワードのアップデートによる、識別\'83\'7bールトおよび接続システムの同期化



シナリオ 3 の設定

この種類のパスワード同期を設定する

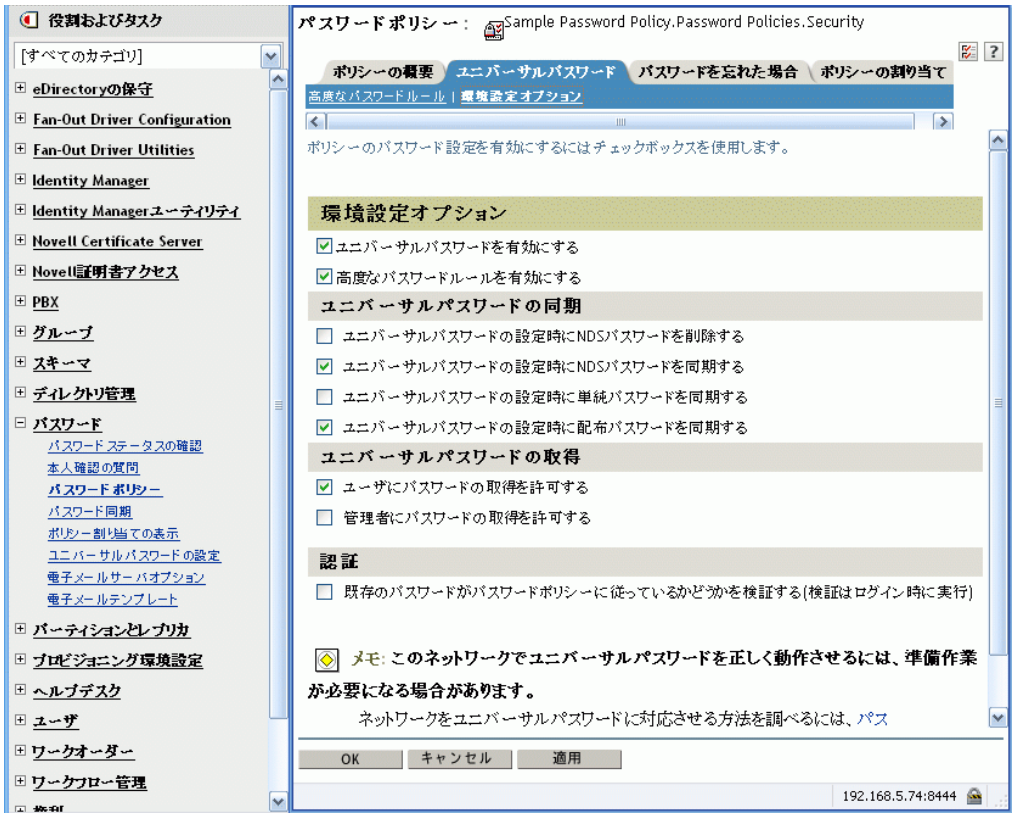
- 137 ページの 「ユニバーサルパスワードの展開」
- 137 ページの 「Password Policy (パスワードポリシー) の設定」
- 138 ページの 「パスワード同期の設定」
- 140 ページの 「ドライバ設定」

ユニバーサルパスワードの展開

現在の環境でユニバーサルパスワードを使用する準備ができていることを確認します。詳細については、105 ページのセクション 5.4「Identity Manager パスワード同期およびユニバーサルパスワードを使用するための準備作業」を参照してください。

Password Policy (パスワードポリシー) の設定

1. iManager で、［*Passwords*］> ［Password Policies］の順に選択します。
2. パスワードポリシーが、この種類のパスワード同期を実行する識別ボールトツリーの一部に割り当てられていることを確認します。パスワードポリシーは、ツリー構造全体、パーティションルートコンテナ、コンテナ、または特定のユーザに割り当てることができます。管理を簡易化するには、ツリー内のできるだけ高い位置にパスワードポリシーを割り当てることをお勧めします。
3. ［Password Policy］で、次のオプションが選択されていることを確認します。



- *ユニバーサルパスワードを有効にする*
- *ユニバーサルパスワードの設定時に NDS パスワードを同期する*
- *ユニバーサルパスワードの設定時に配布パスワードを同期する*

  Identity Manager は配布パスワードを取得して接続システムに配布するので、双方向のパスワード同期を可 \'94\'5c にするためにこのオプションをオンにすることが重要です。

4 高度なパスワードルールを使用している場合、パスワードを受信している接続システムのパスワードポリシーと競合しないことを確認します。

パスワード同期の設定

1 iManager で、［*Passwords*］> ［Password Synchronization］の順に選択します。
2 接続システムのドライバを検索し、ドライバを選択します。
3 接続システムのドライバの設定を作成します。

次のオプションが選択されていることを確認します。

- *パスワードを受理する Identity Manager (発行者チャネル)*
- *パスワード同期に配布パスワードを使用する*

  ドライバマニフェストに「password-publish」機能が含まれていない場合、メッセージがページに表示されます。これは、パスワードがアプリケーションから取得できず、パスワードを発行するには、ポリシーを使用してドライバ設定にパスワードを作成するしかないことをユーザに通知するものです。
- *パスワードを受け入れるアプリケーション (購読者チャネル)*

これらの設定により、接続システムでサポートされている場合には、双方向のパスワード同期が可 \'94\'5c になります。

パスワードの信頼されたソースについては、ビジネスポリシーに合わせて設定を調整できます。たとえば、接続システムがパスワードを購読するが発行しないようにする場合は、[*Application accepts passwords (Subscriber Channel)*] のみを選択します。

4 [*Use Distribution Password for password synchronization*] のオプションを使用し、パスワード同期の NMAS パスワードポリシーを適用させるか無視するかを指定します。

5 (オプション) パスワードポリシーを適用させるように指定した場合、パスワードがポリシーに準拠しない場合に接続システムのパスワードを Identity Manager がリセットするかどうかも指定します。

6 (オプション) 必要に応じ、次のオプションを選択します。

- *電子メール経由でユーザにパスワード同期障害を通知する*

  電子メール通知には、eDirectory ユーザオブジェクトの Internet EMail Address 属性の入力が必要です。

  電子メール通知は、他に影響を与えません。これらは、電子メールをトリガした XML ドキュメントの処理には影響しません。失敗した場合、操作自体が再試行

されない限り、電子メール通知は再試行されません。ただし、電子メール通知のデバッグメッセージはトレースファイルに書き込まれます。

ドライバ設定

1 必要な Identity Manager スクリプトパスワード同期化ポリシーが、パスワード同期に使用する各ドライバのドライバ設定に含まれていることを確認します。

ポリシーは、ドライバ設定の正しい位置に正しい順序で記述されている必要があります。ポリシーのリストについては、101 ページのセクション 5.3.4「ドライバ設定で必要なポリシー」を参照してください。

Identity Manage のサンプル設定には、すでにポリシーが含まれています。既存のドライバをアップデートする場合は、111 ページのセクション 5.7「パスワード同期をサポートするための、既存のドライバ設定のアップグレード」の手順を使用してポリシーを追加できます。

2 nspmDistributionPassword 属性のために、フィルタを正しく設定します。

- 発行者チャネルについては、ドライバフィルタがすべてのオブジェクトクラスの *nspmDistributionPassword 属性を無視するよう設定します。*
- 加入者チャネルについては、ドライバフィルタがすべてのオブジェクトクラスの *nspmDistributionPassword 属性を通知するよう設定します。*

3 ［nspmDistributionPassword］属性が［*Notify*］*に設定されているすべてのオブジェクトでは、ドライバフィルタの Public Key および Private Key 属性の両方を*［Ignore］に設定します。

4 パスワードのセキュリティを確保するには、Identity Manager のオブジェクトへの権利を持つユーザを制御していることを確認します。

シナリオ 3 のトラブルシューティング

- 141 ページの 「シナリオ 3 のフローチャート」
- 142 ページの 「eDirectory へのログインのトラブルシューティング」
- 143 ページの 「パスワードを購読する別の接続システムへのログインのトラブルシューティング」
- 144 ページの 「パスワードのエラーについての電子メールが生成されない」
- 144 ページの 「[Check Password Status] を使用した場合のエラー」
- 145 ページの 「DSTrace の便利なコ \'83\'7d ンド」

のヒントも参照してください。169 ページのセクション 5.13「パスワード同期のトラブルシューティング」

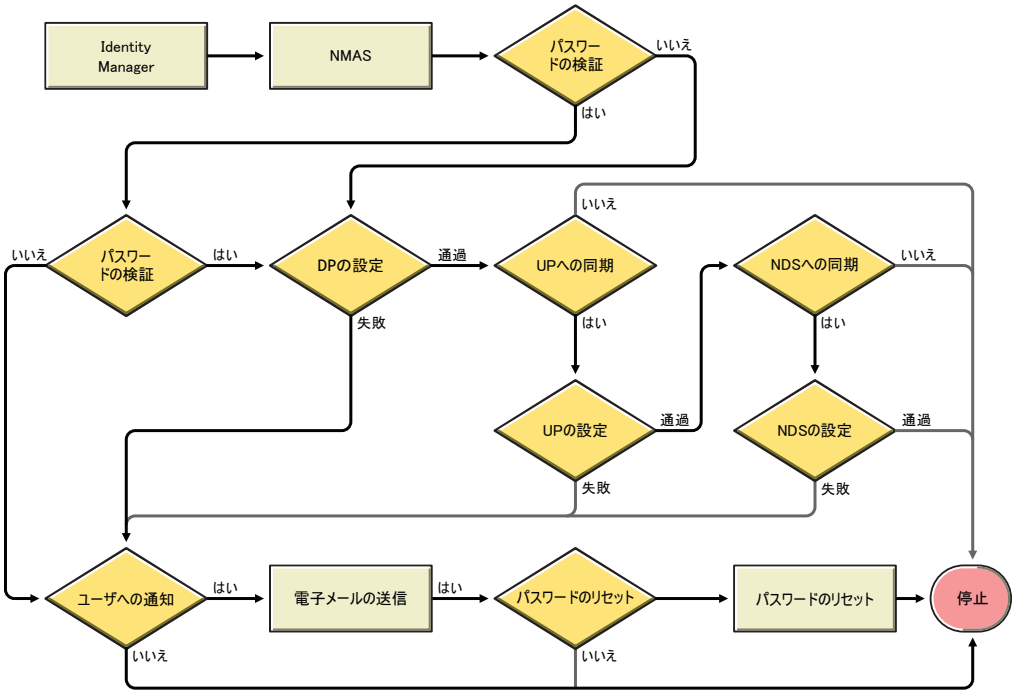
シナリオ 3 のフローチャート

図 5-12 は、NMAS が Identity Manager から受信するパスワードの処理の方法を示しています。このシナリオではパスワードが配布パスワードに同期され、NMAS では次が決定されます。

- パスワードポリシーのルールに対して着信パスワードを検証する必要があることを指定したかどうかに基づいた、パスワードの処理方法 (ユニバーサルパスワードおよび高度なパスワードルールが有効になっている場合)。

- ユニバーサルパスワードとその他のパスワードとを同期するためのパスワードポリシーに、どのようなその他の設定があるのか。

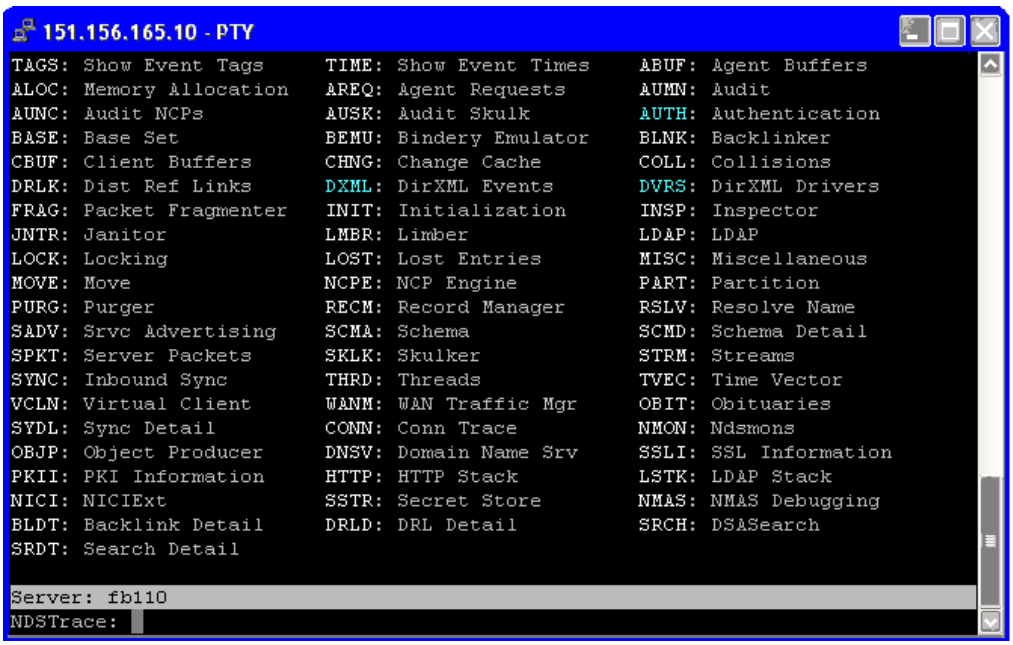
図 5-12 *配布パスワードに同期される Identity Manager のパスワード*



eDirectory へのログインのトラブルシューティング

- DSTrace で、［*+AUTH*］、［*+DXML*］、および［*+DVRS*］の設定をオンにします。

図 5-13 *DSTrace コ\'83\'7d ンド*



- <password>または<modify-password>の要素がIdentity Managerに渡されていることを確認します。確認するには、［DSTtrace］画面またはファイルのトレースオプションが、最初の項目で説明したとおり、オンになっていることを確かめます。
- NMAS パスワードポリシーのルールに従い、パスワードが有効であることを確認します。
- NMAS パスワードポリシーの設定と割り当てを確認します。ポリシーをユーザに直接割り当て、正しいポリシーが使用されるようにします。
- ドライバの［Password Synchronization］ページで、［*Identity Manager accepts passwords (Publisher Channel)*］*が選択されていることを確認します。*
- ［NMAS Password Policy］で、［*Synchronize Distribution Password when setting Universal Password*］*が選択されていることを確認します。*
- ［NMAS Password Policy］で、必要に応じて［*Synchronize NDS Password when setting Universal Password*］*が選択されていることを確認します。*
- ユーザが Novell Client または ConsoleOne を通じてログインしている場合は、バージョンを確認します。ユニバーサルパスワードが NDS パスワードに同期化されていない場合、レガシーな Novell Clients および ConsoleOne からは、識別 \'83\'7bールトにログインできないことがあります。

  ユニバーサルパスワードを認識する Novell Client および ConsoleOne のバージョンが利用できます。『*NMAS 3.0 Administration Guide* (http://www.novell.com/documentation/nmas30/index.html)』を参照してください。
- 一部のレガシーユーティリティは NDS パスワードを使用して認証され、ユニバーサルパスワードが NDS パスワードと同期されていない場合には、識別ボールトにログインできません。ほとんどのユーザは NDS パスワードを使用せず、管理者またはヘルプデスクのユーザがレガシーユーティリティへの認証を必要とする場合は、ヘルプデスクのユーザには異なるパスワードポリシーを使用し、異なるユニバーサルパスワード同期化のオプションを指定できるようにします。

パスワードを購読する別の接続システムへのログインのトラブルシューティング

このセクションでは、この接続システムが Identity Manager にパスワードを発行しているが、そのパスワードを購読するもう 1 つの接続システムがこのシステムからの変更を受信していないように思える場合の、トラブルシューティングについて説明します。この関係は、第 2 の接続システムとも呼ばれ、第 1 の接続システムから Identity Manager を通じてパスワードを受信することを意味します。

- DSTrace の［*+DXML*］および［*+DVRS*］の設定をオンにし、Identity Manager のルール処理および可能性のあるエラーを確認します。
- ドライバの Identity Manager のトレースレベルを［*3*］*に設定します。*
- ［Password Synchronization］ページの［*Identity Manager accepts passwords (Publisher Channel)*］*オプションが選択されていることを確認します。*
- ［Password Policy］で、［*Synchronize Distribution Password when Setting Universal Password*］*が選択されていないことを確認します。*

  Identity Manager は、配布パスワードを使用して、パスワードを接続システムに同期します。ユニバーサルパスワードは、この同期化方法の配布パスワードに同期化させる必要があります。
- ドライバフィルタの nspmDistributionPassword 属性を確認します。

- <password> 要素 (Add の場合) または <modify-password> 要素が、nspmDistributionPassword 属性の Add 属性および Modify 属性の操作に変換されていることを確認します。確認するには、［DSTrace］画面またはファイルのオプションが、最初の項目で説明したとおり、オンになっていることを確かめます。
- Identity Manager スクリプトパスワードポリシーが、101 ページのセクション 5.3.4「ドライバ設定で必要なポリシー」で説明されているとおり、ドライバ設定の正しい位置と順序にあることを確認します。
- 識別 \'83\'7bールトのパスワードポリシーと、接続システムにより適用されるパスワードポリシーと比較し、互換性があることを確認します。

パスワードのエラーについての電子メールが生成されない

- DSTrace の［*+DXML*］の設定をオンにし、Identity Manager のルール処理を確認します。
- ドライバの Identity Manager のトレースレベルを［*3*］*に設定します。*
- 電子メールを生成するルールが選択されていることを確認します。
- 識別 \'83\'7bールトオブジェクトを検証し、Internet EMail Address 属性に正しい値が含まれていることを確認します。
- 通知設定タスクで、SMTP サーバと電子メールテンプレート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、158 ページのセクション 5.12「電子メール通知の設定」を参照してください。

電子メール通知は、他に影響を与えません。これらは、電子メールをトリガした XML ドキュメントの処理には影響しません。失敗した場合、操作自体が再試行されない限り、電子メール通知は再試行されません。電子メール通知のデバッグメッセージはトレースファイルに書き込まれます。

［Check Password Status］を使用した場合のエラー

iManager の［Check Password Status］タスクにより、ドライバで［Check Object Password］アクションが実行されます。

- 接続システムでパスワードのチェックがサポートされていることを確認してください。詳細については、94 ページのセクション 5.2「パスワード同期をサポートする接続システム」を参照してください。

  接続システムがパスワードチェック機 \'94\'5c をサポートするようドライバ \'83\'7d ニフェストに示されてない場合は、iManager からこの機 \'94\'5c を使用することはできません。
- ［オブジェクトパスワードの確認］から -603 が返される場合、識別ボールトブジェクトに nspmDistributionPassword 属性が含まれていません。ドライバフィルタ、および［Password Policy］の［*Synchronize Universal to Distribution*］*オプションを確認します。*
- ［Check Object Password］が「Not Synchronized」を返す場合、ドライバ設定に Identity Manager パスワード同期の適切なポリシーが含まれていることを確認します。
- 識別 \'83\'7bールトのパスワードポリシーと、接続システムにより適用されるパスワードポリシーと比較し、互換性があることを確認します。
- ［*オブジェクトパスワードの確認*］は、配布パスワードを確認します。配布パスワードがアップデートされていない場合、［*Check Object Password*］*によって、パスワードが同期化されていることがレポートされないことがあります。*

- 識別ボールトでは、［*パスワードステータスの確認*］は、ユニバーサルパスワードではなく NDS パスワードを確認することに注意してください。つまり、ユーザのパスワードポリシーで NDS パスワードをユニバーサルパスワードに同期化するよう指定されていない場合は、常に、パスワードが同期化されていないとレポートされます。配布パスワードおよび接続システムのパスワードは同期化されないことがありますが、NDS パスワードおよび配布パスワードの両方がユニバーサルパスワードに同期化されない限り、［Check Password Status］は正確とは限りません。

DSTrace の便利なコ \'83\'7d ンド

+*DXML*: Identity Manager ルール処理および可能性のあるエラーメッセージを表示する。

+*DVRS*: Identity Manager ドライバのメッセージを表示する。

+*AUTH*: NDS パスワードの変更を表示する。

5.8.5 シナリオ 4: トンネル

Identity Manager では、識別ボールトのパスワードはそのままにしながら、接続システム間でパスワードを同期できます。これは「トンネリング」と呼ばれます。

このシナリオでは、Identity Manager が配布パスワードを直接更新します。このシナリオは 136 ページのセクション 5.8.4「シナリオ 3: Identity Manager で配布パスワードを更新することで、識別ボールトと接続システムを同期する」とほとんど同じです。異なる点は、ユニバーサルパスワードおよび配布パスワードは同期されないことです。これは、NMAS のパスワードポリシーを使用しないか、または［*Synchronize Distribution Password when setting Universal Password*］*のオプションを無効にしたパスワードポリシーを使用して実行します。*

- 146 ページの 「シナリオ 4 の長所と短所」
- 147 ページの 「シナリオ 4 の設定」
- 148 ページの 「シナリオ 4 のトラブルシューティング」

シナリオ 4 の長所と短所

表 5-14 *トンネリングの長所*

長所	短所
識別 \'83\'7bールトのパスワードはそのままにしながら、接続システム間でパスワードを同期化できます。 パスワードポリシーでは、ユニバーサルパスワードを有効にしておく必要はありませんが、使用している環境ではユニバーサルパスワードがサポートされている必要があります。 接続システムが iManager の［Check Password Status］タスクをサポートする場合、このシナリオも［Check Password Status］タスクをサポートします。 パスワード同期が失敗した場合に通知を送信するよう指定できます。 接続システムのパスワードがパスワードポリシーに準拠しない場合、それをリセットできます。 ユニバーサルパスワードおよび高度なパスワードルールが有効になっている場合、パスワードポリシーを適用するよう指定した際はパスワードポリシーが適用され、接続システムのパスワードをリセットできます。	ユニバーサルパスワードおよび高度なパスワードルールが無効になっている場合、パスワードポリシーは適用されず、接続システムのパスワードはリセットできません。

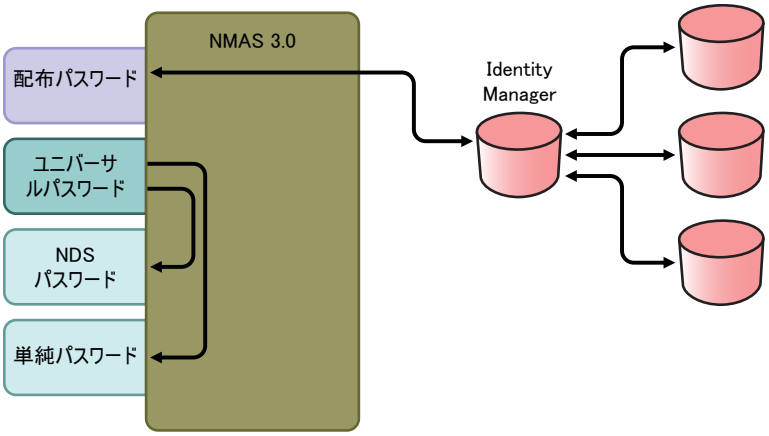
図 5-14 は、次のフローを示しています。

1. パスワードが、Identity Manager を通って来る。
2. Identity Manager が NMAS と通信して、配布パスワードを直接アップデートする。
3. Identity Manager は配布パスワードを使用し、パスワードを受諾するよう指定した接続システムに配布します。

このシナリオの重要な点は、NMAS パスワードポリシーで、［*ユニバーサルパスワードの設定時に配布パスワードを同期する*］が無効になっている点です。配布パスワードとユニバーサルパスワードは同期化されないので、Identity Manager は、識別 \'83\'7bールトのパスワードはそのままにしながら、接続システム間でパスワードを同期化します。

この \'90\'7d では複数の接続システムが Identity Manager に接続しているように示されていますが、接続システムのドライバごとに設定を作成することに注意してください。

図 5-14 Identity Manager での配布パスワードのアップデートによるトンネリング



シナリオ 4 の設定

この種類のパスワード同期を設定するには、次を設定します。

- 147 ページの 「ユニバーサルパスワードの展開」
- 147 ページの 「Password Policy (パスワードポリシー) の設定」
- 148 ページの 「パスワード同期の設定」
- 148 ページの 「ドライバ設定」

ユニバーサルパスワードの展開

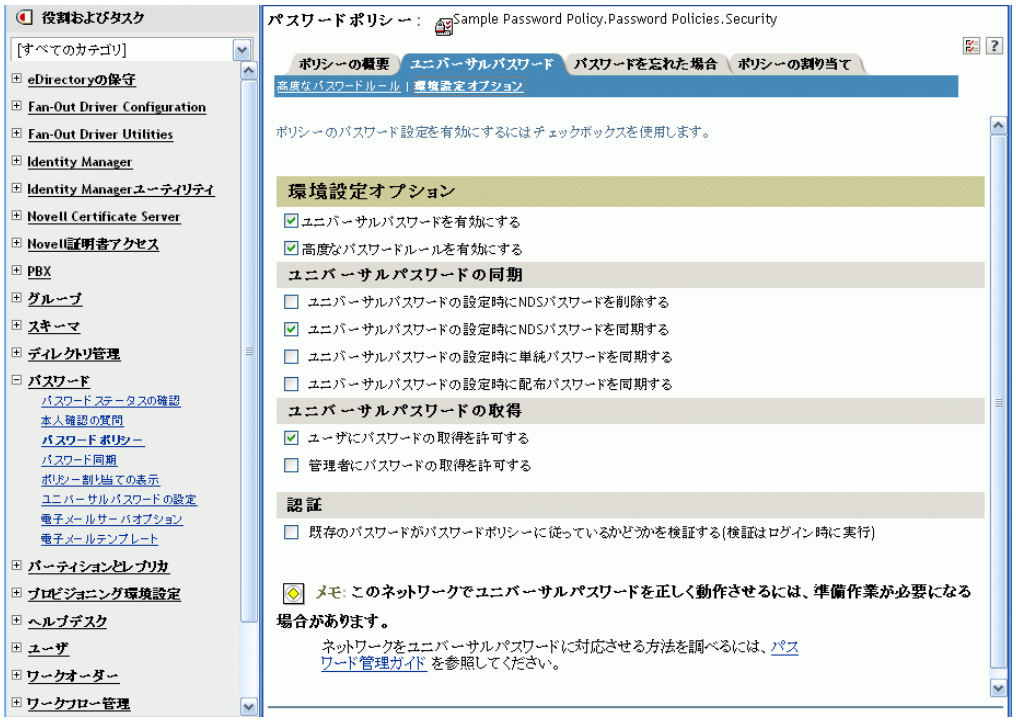
パスワードポリシーでユニバーサルパスワードを有効にする必要はありませんが、使用している環境では、ユニバーサルパスワードをサポートする eDirectory 8.7.3 を使用している必要があります。詳細については、105 ページのセクション 5.4「Identity Manager パスワード同期およびユニバーサルパスワードを使用するための準備作業」を参照してください。

Password Policy (パスワードポリシー) の設定

パスワードポリシーを確認して、以下の内容を確認します。

- ［*ユニバーサルパスワードの設定時に配布パスワードを同期する*］が選択されていないことを確認します。

  識別ボールトのパスワードに影響を与えずにパスワードのトンネリングを実行するには、これが重要です。ユニバーサルパスワードを配布パスワードと同期しないことによって、配布パスワードをそのままにして、接続システムに対する Identity Manager でのみ使用できます。Identity Manager は、識別 \'83\'7bールトのパスワードには影響を与えずに接続システム間でパスワードを配布するルートとして機 \'94\'5c します。



- 必要に応じてパスワードポリシーのその他の設定を行います。

  パスワードポリシー内のその他のパスワード設定はオプションです。

パスワード同期の設定

の「パスワード同期の設定」と同じ設定を使用します。136 ページのセクション 5.8.4「シナリオ 3: Identity Manager で配布パスワードを更新することで、識別ボールトと接続システムを同期する」

ドライバ設定

の「ドライバ設定」と同じ設定を使用します。136 ページのセクション 5.8.4「シナリオ 3: Identity Manager で配布パスワードを更新することで、識別ボールトと接続システムを同期する」

シナリオ 4 のトラブルシューティング

パスワード同期がトンネリングのための設定になっている場合、配布パスワードは、ユニバーサルパスワードおよび NDS パスワードと異なるものになります。

- 149 ページの 「パスワードを購読する別の接続システムへのログインのトラブルシューティング」
- 149 ページの 「パスワードのエラーについての電子メールが生成されない」
- 150 ページの 「[Check Password Status] を使用した場合のエラー」
- 150 ページの 「DSTrace の便利なコ \'83\'7d ンド」

のヒントも参照してください。169 ページのセクション 5.13「パスワード同期のトラブルシューティング」

パスワードを購読する別の接続システムへのログインのトラブルシューティング

このセクションでは、この接続システムが Identity Manager にパスワードを発行しているが、そのパスワードを購読するもう 1 つの接続システムがこのシステムからの変更を受信していないように思える場合の、トラブルシューティングについて説明します。この関係は、第 2 の接続システムとも呼ばれ、第 1 の接続システムから Identity Manager を通じてパスワードを受信することを意味します。

- DSTrace の［*+DXML*］および［*+DVRS*］の設定をオンにし、Identity Manager のルール処理および可能性のあるエラーを確認します。
- ドライバの Identity Manager のトレースレベルを［*3*］*に設定します。*
- ［Password Synchronization］ページの［*Identity Manager accepts passwords (Publisher Channel)*］*オプションが選択されていることを確認します。*
- ［Password Policy］で、［*Synchronize Distribution Password when Setting Universal Password*］*が選択されていないことを確認します。*

  Identity Manager は、配布パスワードを使用して、パスワードを接続システムに同期します。ユニバーサルパスワードは、この同期化方法の配布パスワードに同期化させる必要があります。
- ドライバフィルタのnspmDistributionPassword属性が正しく設定されていることを確認します。
- <password> 要素 (Add の場合) または <modify-password> 要素が、nspmDistributionPassword 属性の Add 属性および Modify 属性の操作に変換されていることを確認します。確認するには、［DSTrace］画面またはファイルのトレースオプションが、最初の項目で説明したとおり、オンになっていることを確かめます。
- Identity Manager スクリプトパスワードポリシーが、101 ページのセクション 5.3.4「ドライバ設定で必要なポリシー」で説明されているとおり、ドライバ設定の正しい位置と順序にあることを確認します。
- 識別 \'83\'7bールトのパスワードポリシーと、接続システムにより適用されるパスワードポリシーと比較し、互換性があることを確認します。

パスワードのエラーについての電子メールが生成されない

- DSTrace の［*+DXML*］の設定をオンにし、Identity Manager のルール処理を確認します。
- ドライバの Identity Manager のトレースレベルを［*3*］*に設定します。*
- 電子メールを生成するルールが選択されていることを確認します。
- 識別 \'83\'7bールトオブジェクトを検証し、Internet EMail Address 属性に正しい値が含まれていることを確認します。
- 通知設定タスクで、SMTP サーバと電子メールテンプレートを確認します。詳細については、158 ページのセクション 5.12「電子メール通知の設定」を参照してください。

電子メール通知は、他に影響を与えません。これらは、電子メールをトリガした XML ドキュメントの処理には影響しません。失敗した場合、操作自体が再試行されない限り、電子メール通知は再試行されません。電子メール通知のデバッグメッセージはトレースファイルに書き込まれます。

［Check Password Status］を使用した場合のエラー

iManager の［Check Password Status］タスクにより、ドライバで［Check Object Password］アクションが実行されます。

- 接続システムでパスワードのチェックがサポートされていることを確認してください。詳細については、94 ページのセクション 5.2「パスワード同期をサポートする接続システム」を参照してください。

  接続システムがパスワードチェック機 \'94\'5c をサポートするようドライバ \'83\'7d ニフェストに示されてない場合は、iManager からこの機 \'94\'5c を使用することはできません。
- ［オブジェクトパスワードの確認］アクションから -603 が返される場合、識別ボールトブジェクトに nspmDistributionPassword 属性が含まれていません。Identity Manager 属性フィルタ、および［Password Policy］の［*Synchronize Universal to Distribution*］*オプションを確認します。*
- ［Check Object Password］アクションが「Not Synchronized」を返す場合、ドライバ設定に Identity Manager パスワード同期の適切なポリシーが含まれていることを確認します。
- 識別 \'83\'7bールトのパスワードポリシーと、接続システムにより適用されるパスワードポリシーと比較し、互換性があることを確認します。
- ［オブジェクトパスワードの確認］アクションは、配布パスワードを確認します。配布パスワードがアップデートされていない場合、［Check Object Password］によって、パスワードが同期化されていることがレポートされないことがあります。

DSTrace の便利なコ \'83\'7d ンド

+*DXML*: Identity Manager ルール処理および可能性のあるエラーメッセージを表示する。

+*DVRS*: Identity Manager ドライバのメッセージを表示する。

+*AUTH*: NDS パスワードの変更を表示する。

+*DCLN*: NDS DClient メッセージを表示する。

5.8.6 シナリオ 5: アプリケーションパスワードを単純パスワードに同期する

このシナリオは、パスワード同期機能の特別な使用方法です。Identity Manager および NMAS を使用し、接続システムからパスワードを取得して、識別ボールトの単純パスワードに直接同期できます。接続システムがハッシュされたパスワードのみを提供する場合、ハッシュを元に戻さずに、単純パスワードに同期できます。他のアプリケーションは、同じクリアテキスト、あるいは LDAP または Novell Client によりハッシュされたパスワードを使用し、識別 \'83\'7bールトに対して認証できます。NMAS コンポーネントは、通常パスワードをログインメ \'83\'5cッドとして使用するよう設定されます。

接続システムのパスワードがクリアテキストである場合、そのまま接続システムから 識別 \'83\'7bールトの通常パスワードの場所に発行できます。

接続システムがハッシュされたパスワード (MD5、SHA、SHA1、または UNIX Crypt がサポートされています) のみを提供する場合、それらのパスワードは、{MD5} のようにハッシュの種類を指定して単純パスワードに発行する必要があります。

同じパスワードで認証する別のアプリケーションについては、ユーザのパスワードを取得し LDAP を使用して通常パスワードに対して認証するよう、アプリケーションをカスタ\'83\'7d イズする必要があります。

NMAS は、アプリケーションから取得したパスワードの値と、単純パスワードの値を比較します。単純パスワードとして保存されているパスワードがハッシュ値である場合、NMAS は、アプリケーションのパスワードの値を使用して正しいタイプのハッシュ値を生成してから比較します。アプリケーションから取得したパスワードと通常パスワードが同一である場合、NMAS はユーザを認証します。

このシナリオでは、ユニバーサルパスワードは使用できません。

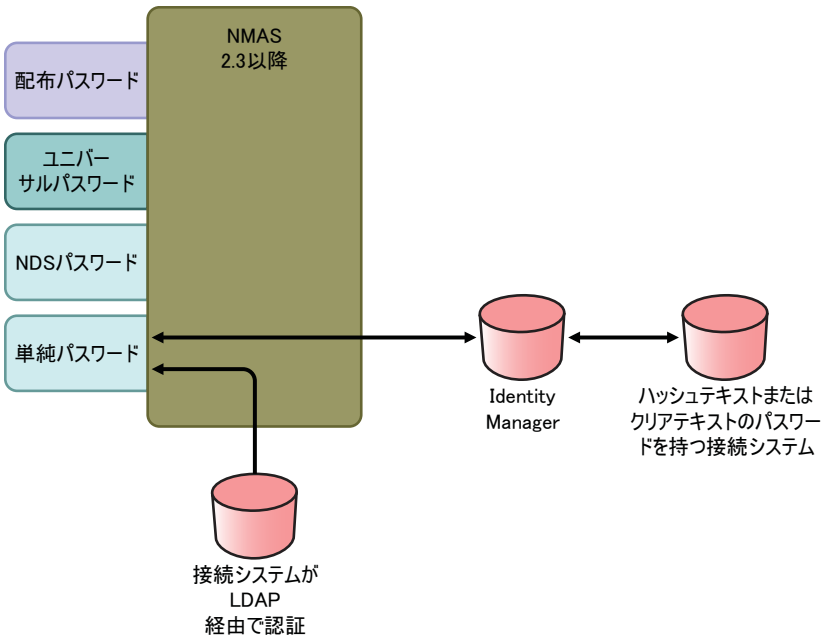
- 151 ページの 「NDS パスワードへの同期の長所」
- 152 ページの 「シナリオ 5 の設定」

NDS パスワードへの同期の長所

表 5-15 *NDS パスワードへの同期の長所*

長所	短所
◆ 通常パスワードを直接アップデートできます。 ◆ ハッシュされたパスワードを同期化し、ハッシュを戻さずに、複数のアプリケーションでの認証に使用できます。	◆ ユニバーサルパスワードは使用できません。 ◆ パスワードを忘れた場合の機\'94\'5cおよびパスワードセルフサービス機 \'94\'5c は、NDS パスワードをサポートする程度では使用できますが、通常パスワードについては使用できません。 ◆ Set Universal Password タスクはユニバーサルパスワードに依存しているため、管理者はそのタスクを使用して識別 \'83\'7bールトのユーザのパスワードを設定することはできません。

図 5-15 NDS パスワードへの同期



シナリオ 5 の設定

- 152 ページの 「Password Policy (パスワードポリシー) の設定」
- 152 ページの 「パスワード同期の設定」
- 152 ページの 「ドライバ設定」

Password Policy (パスワードポリシー) の設定

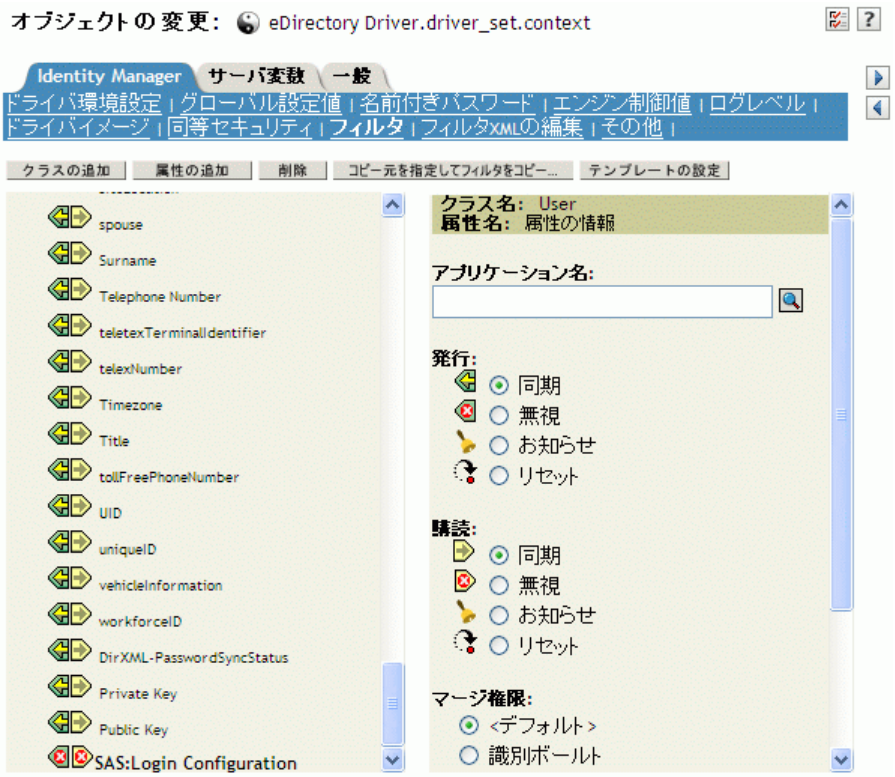
このシナリオでは、ユーザに対するパスワードポリシーは必要ありません。ユニバーサルパスワードは使用できません。

パスワード同期の設定

このシナリオでは、Identity Manager スクリプトを使用して、SAS:Login Configuration 属性を直接変更します。つまり、iManager の［Password Synchronization］ページを使用して設定される、パスワード同期のグローバル設定値 (GCV) に効果はありません。

ドライバ設定

1 フィルタの SAS:Login Configuration 属性が、発行者チャネルおよび加入者チャネルの両方に対して［*Synchronize*］*に設定されていることを確認してください。*



2 ドライバポリシーで、接続システムからのパスワードを発行するよう設定します。

3 ハッシュされたパスワードについては、ドライバポリシーで、(ハッシュのタイプがアプリケーションからまだ提供されていないいる場合は) ハッシュのタイプを末尾に付けるよう設定します。

- {MD5} *hashed_password*

  このパスワードは Base64 でエンコードされています。

- {SHA} *hashed_password*

  このパスワードは Base64 でエンコードされています。

- {CRYPT} *hashed_password*

クリアテキストパスワードおよび Unix Crypt パスワードハッシュは、Base 64 でエンコードされていません。

4 パスワードを通常パスワードに設定するには、SAS:Login Configuration 属性を変更するようドライバポリシーを設定します。

次の例では、変更操作内で modify-attr 要素を使用して、通常パスワードを MD5 でハッシュされたパスワードに変更する方法を示しています。

```
<modify-attr attr-name="SAS:Login Configuration>
    <add-value>
        <value>{MD5}2tEgXrIHtAnGHOzH3ENslg==</value>
    </add-value>
</modify-attr>
```

クリアテキストパスワードについては、次の例に従います。

```
<modify-attr attr-name="SAS:Login Configuration>
    <add-value>
```

```
            <value>clearpwd</value>
        </add-value>
    </modify-attr>
```

追加操作については、add-attr 要素に次のどちらかを含めます。

```
<add-attr attr-name="SAS:Login Configuration>
    <value>{MD5}2tEgXrIHtAnGHOzH3ENslg==</value>
</add-attr>
```

または

```
<add-attr attr-name="SAS:Login Configuration>
    <value>clearpwd</value>
</add-attr>
```

5.9 パスワードフィルタの設定

接続システムの中には、ユーザの実際のパスワードを Identity Manager に提供できるものもあります。

Active Directory、NIS、および NT ドメインでパスワードをキャプチャするには、接続システムにパスワードフィルタをインストールするための設定を行う必要があります。

- 154 ページのセクション 5.9.1「Active Directory および NT ドメインのためのパスワード同期のフィルタの設定」
- 154 ページのセクション 5.9.2「NIS のためのパスワード同期のフィルタの設定」

5.9.1 Active Directory および NT ドメインのためのパスワード同期のフィルタの設定

この情報は、Identity Manager Drivers (http://www.novell.com/documentation/dirxmldrivers/index.html) にある Active Directory および NT ドメイン用 Identity Manager ドライバのドライバ実装ガイドの「Password Synchronization」のセクションにあります。

Active Directory および NT ドメイン用 Identity Manager ドライバは、1 台の Windows コンピュータにのみインストールする必要があります。他のドメインコントローラにはドライバのインストールは必要ありませんが、Identity Manager に送信するパスワードをキャプチャするために、pwfilter.dll ファイルをドメインコントローラごとにインストールする必要があります。

設定と管理を簡素化するために、ドライバがインストールされている Windows コンピュータからすべてのドメインコントローラに対してこの作業を実 \'8e\'7b するためのユーティリティが用意されています。

5.9.2 NIS のためのパスワード同期のフィルタの設定

NIS 3.0 用の Identity Manager ドライバは、ファイル、NIS、および NIS+ の 3 つの UNIX 認証データストアで動作します。パスワードをキャプチャし NIS 対応の Identity Manager ドライバに送信するために、PAM モジュールが用意されています。

NIS ドライバのための PAM モジュールの展開については、Identity Manager Drivers (http://www.novell.com/documentation/lg/dirxmldrivers/index.html) にある『*Identity Manager Driver for NIS Implementation Guide*』で説明しています。

5.10 パスワード同期の管理

- 155 ページの 「システム間のパスワードフローの設定」
- 157 ページの 「接続システムへのパスワードポリシーの適用」
- 157 ページの 「eDirectory パスワードを同期化されたパスワードとは別にそのままにしておく方法」

5.10.1 システム間のパスワードフローの設定

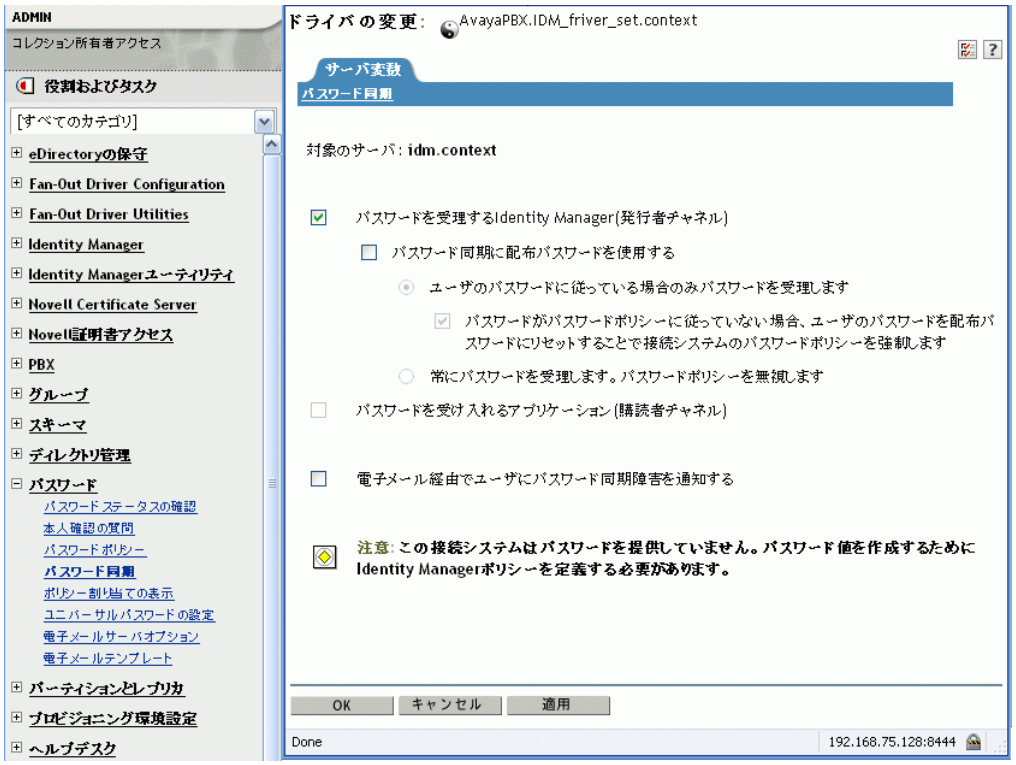
パスワードを受諾または発行するためにシステムがどのように設定されているのかを \'95\'5c 示するには、次のように操作します

1 iManager で、［*Passwords*］> ［Password Synchronization］の順に選択します。

2 接続システムのドライバを検索します。

検索結果には、Identity Manager および接続システム間のパスワードフローについての設定が \'95\'5c 示されます。

設定を変更するには、接続システムのドライバ名をクリックします。



［Modify Driver］ページでは、Identity Manager が受信するパスワードにパスワードポリシーを適用するかどうかと、接続システムにパスワードポリシーを適用して接続システムのパスワードをリセットするかどうかを設定できます。

このページの設定は、サーバごとに保存される GCV (グローバル構成値) です。詳細については、98 ページのセクション 5.3.3「グローバル構成値を使用してパスワード同期を制御する」を参照してください。

5.10.2 接続システムへのパスワードポリシーの適用

高度なパスワードルールおよび Identity Manager のパスワード同期を使用している場合、次を実行することをお勧めします。

1 すべての接続システムのパスワードポリシーを調査する。
2 高度なパスワードルールが接続システム上のパスワードポリシーと互換性があることを確認する。

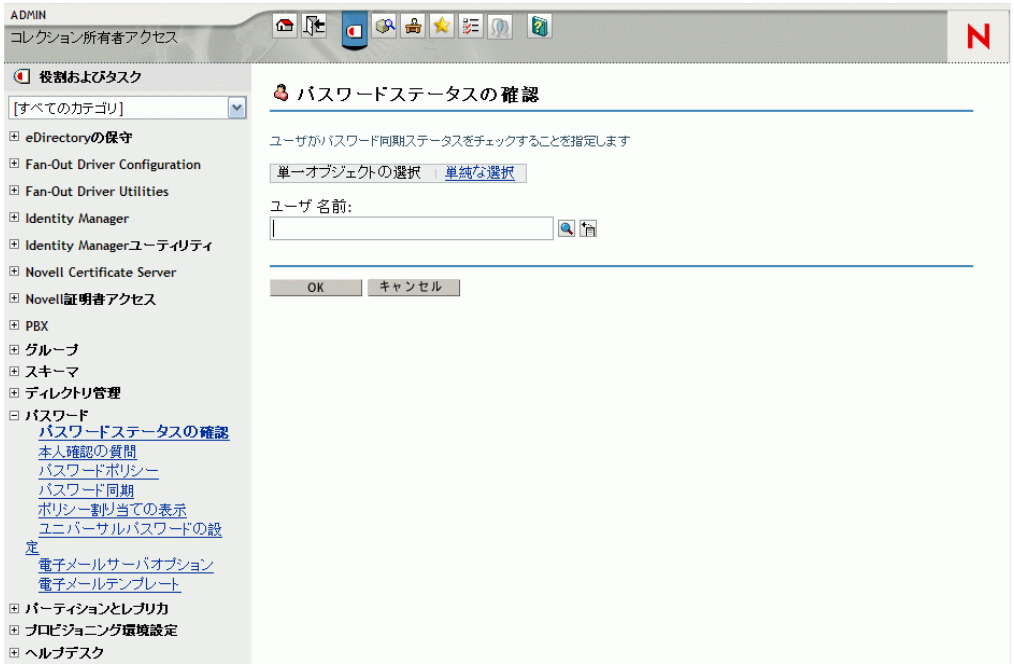
5.10.3 eDirectory パスワードを同期化されたパスワードとは別にそのままにしておく方法

このシナリオについては、145 ページのセクション 5.8.5「シナリオ 4: トンネル」で説明しています。

5.11 ユーザのパスワード同期ステータスの確認

特定のユーザの配布パスワードが接続システムのパスワードと同じかどうかを判断できます。

1 iManager で、［*Passwords*］> ［Check Password Status］の順に選択します。



2 ユーザを参照して選択します。

［Check Password Status］タスクにより、ドライバで［Check Object Password］アクションが実行されます。

すべてのドライバでパスワードチェックがサポートされているわけではありません。パスワードチェックをサポートするドライバには、ドライバの \'83\'7d ニフェストにパスワードチェック機 \'94\'5c が含まれている必要があります。iManager では、\'83\'7d ニフェスト

にこの機 \'94\'5c が含まれていないドライバにパスワードチェックの操作を送信できません。

［オブジェクトパスワードの確認］アクションは、配布パスワードを確認します。配布パスワードがアップデートされていない場合、［Check Object Password］によって、パスワードが同期化されていないとレポートされることがあります。

次のいずれかが発生した場合、配布パスワードは更新されません。

- で説明する同期化方法を使用している場合。122 ページのセクション 5.8.2「シナリオ 1: NDS パスワードを使用した、2 つの識別ボールト間の同期」
- ユニバーサルパスワードを同期化している (125 ページのセクション 5.8.3「シナリオ 2: ユニバーサルパスワードを使用したパスワードの同期」を参照) が、ユニバーサルパスワードを配布パスワードに同期化するパスワードポリシーの設定オプションを有効にしていない場合。

注 : 識別ボールトでは、［パスワードステータスの確認］アクションは、ユニバーサルパスワードではなく NDS パスワードを確認することに注意してください。したがって、ユーザのパスワードポリシーで NDS パスワードをユニバーサルパスワードに同期するよう指定されていない場合は、常に、パスワードが同期されていないとレポートされます。配布パスワードおよび接続システムのパスワードは同期化されないことがありますが、NDS パスワードおよび配布パスワードの両方がユニバーサルパスワードに同期化されない限り、［Check Password Status］は正確とは限りません。

5.12 電子メール通知の設定

iManager のタスクを使用すると、電子メールサーバを指定したり、電子メール通知機 \'94\'5c のテンプレートをカスタ \'83\'7d イズしたりできます。

パスワード同期およびパスワードセルフサービスから自動化された電子メールをユーザに送信するために、電子メールのテンプレートが提供されています。

テンプレートは、テンプレートを使用するアプリケーションによって提供されるので、ユーザが作成する必要はありません。電子メールテンプレートは、識別ボールトのテンプレートオブジェクトで、通常は、ツリーのルートにあるセキュリティコンテナに配置されています。これは識別 \'83\'7bールトオブジェクトですが、iManager を介してのみ編集する必要があります。

これはモジュラフレームワークです。電子メールテンプレートを使用する新しいアプリケーションが追加された場合、テンプレートは、それを使用するアプリケーションとともにインストールできます。

iManager での選択に基づき、電子メールを送信するかどうかが制御されます。パスワードを忘れた場合、［パスワードを忘れた場合］アクションの［ユーザにパスワードを電子メールで送信する］、または［ユーザにヒントを送信する］を選択した場合のみ、電子メール通知が送信されます。『*パスワード管理ガイド* (http://www.novell.com/documentation/password_management/index.html)』の「Providing Users with Forgotten Password Self-Service」を参照してください。

［*Notify the user of password synchronization failure via e-mail*］*を選択した場合、失敗したパスワード同期の操作のみ、および指定したドライバに対してのみ電子メールを送信するためにパスワード同期が設定されます。*

図 5-16 パスワード同期の設定

SMTP 認証情報がドライバポリシーに含まれていることも確認する必要があります。

- 159 ページのセクション 5.12.1「前提条件」
- 160 ページのセクション 5.12.2「電子メール通知を送信するための SMTP サーバの設定」
- 161 ページの 「通知のための電子メールテンプレートの設定」
- 161 ページのセクション 5.12.4「ドライバポリシーでの SMTP 認証情報の提供」
- 163 ページのセクション 5.12.5「電子メール通知テンプレートへの独自の置換タグの追加」
- 169 ページのセクション 5.12.6「電子メール通知の管理者への送信」
- 169 ページのセクション 5.12.7「電子メール通知テンプレートのローカライズ」

5.12.1 前提条件

- ❑ eDirectory ユーザが Internet EMail Address 属性に入力済みであることを確認します。
- ❑ パスワード同期の電子メール通知を使用する場合は、パスワード同期のドライバポリシーに SMTP サーバのパスワードが含まれていることを確認します。詳細については、161 ページのセクション 5.12.4「ドライバポリシーでの SMTP 認証情報の提供」を参照してください。
- ❑ 電子メールアドレスを入力していないユーザがいる可能性がある場合や、すべての失敗操作の通知の電子メールレコードが必要な場合は、ユーザだけではなく、パスワード管理者アカウントにも電子メール通知を送信するよう選択することを検討します。

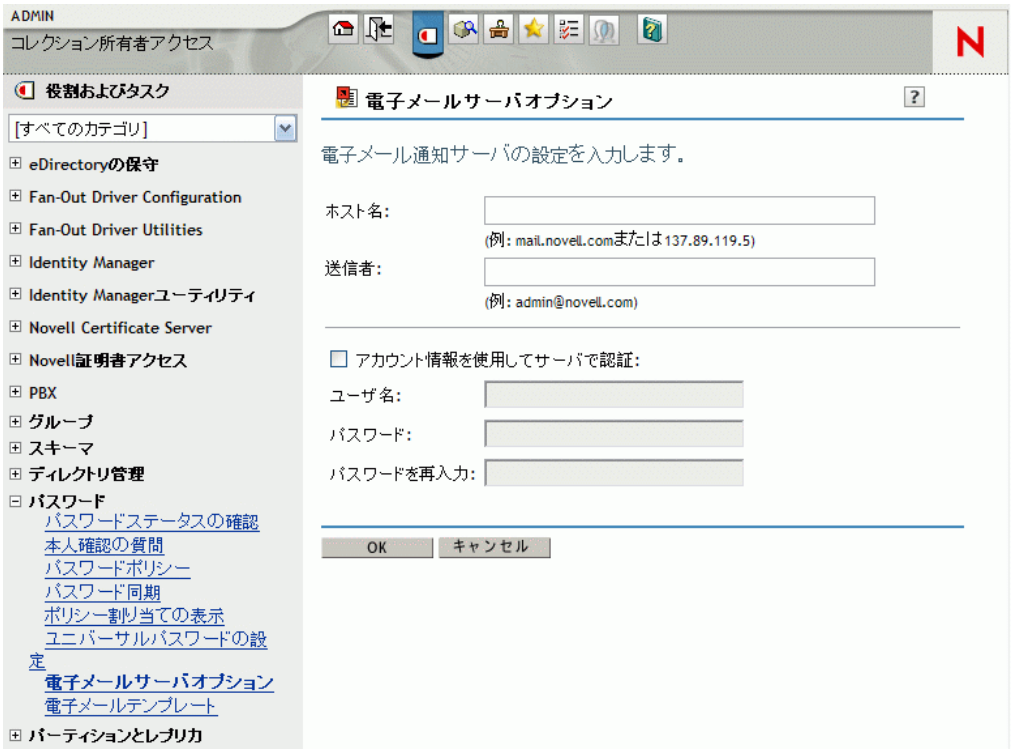
  この電子メールアドレスは、Identity Manager のスクリプトポリシーの［*宛先*］フィールドに入力されている必要があります。詳細については、169 ページのセクション 5.12.6「電子メール通知の管理者への送信」を参照してください。

- ❑ eDirectory および Identity Manager が UNIX サーバ上にある場合は、サーバは電子メールテンプレートオブジェクトのレプリカを保存する必要があります。

  これらのオブジェクトは、ルートのセキュリティコンテナにあります。つまり、サーバにはルートパーティションのレプリカが必要です。

5.12.2 電子メール通知を送信するための SMTP サーバの設定

1 iManager で、［*Passwords*］> ［Email Server Options］の順に選択します。



2 次の情報を入力します。

- ホスト名。
- 電子メールメッセージの［*送信者*］フィールドに表示する名前 (Administrator など)。
- 必要に応じ、サーバに対して認証するためのユーザ名およびパスワード

3 ［*OK*］をクリックします。

4 Identity Manager ドライバでパスワード同期を使用しており、電子メール通知機 \'94\'5c を使用する場合は、次の作業も必要です。

4a 電子メールを送信する前に SMTP サーバで認証が必要な場合、ドライバポリシーにパスワードが含まれていることを確認します。ステップについては、161 ページのセクション 5.12.4「ドライバポリシーでの SMTP 認証情報の提供」を参照してください。

にある［Email Server Options］ページで指定する認証情報は、パスワードを忘れた場合の通知には \'8f\'5c 分ですが、パスワード同期の通知には不 \'8f\'5c 分です。ステップ 2

4b 変更に伴いアップデートする必要のある Identity Manager ドライバを再起動します。

ドライバはテンプレートおよび SMTP サーバ情報を、起動時のみ読み込みます。

5 の説明に従い、電子メールテンプレートをカスタ \'83\'7d イズします。161 ページの「通知のための電子メールテンプレートの設定」

メッセージを送信する機 \'94\'5c を使用する場合は、電子メールサーバの設定後、電子メールテンプレートを使用するアプリケーションから電子メールメッセージを送信できます。

5.12.3 通知のための電子メールテンプレートの設定

これらのテンプレートは、独自のテキストでカスタマイズできます。テンプレートの名前は、使用目的を示します。

1 iManager で、［*Passwords*］> ［Edit Email Templates］の順に選択します。

2 必要に応じてテンプレートを編集します。

置換タグを追加する場合は、追加の作業が必要となることがあります。163 ページのセクション 5.12.5「電子メール通知テンプレートへの独自の置換タグの追加」の指示に従います。

3 変更に伴いアップデートする必要のある Identity Manager ドライバを再起動します。

ドライバはテンプレートおよび SMTP サーバ情報を、起動時のみ読み込みます。

5.12.4 ドライバポリシーでの SMTP 認証情報の提供

160 ページのセクション 5.12.2「電子メール通知を送信するための SMTP サーバの設定」に、SMTP サーバのユーザ名およびパスワードを指定します。パスワードを忘れた場合の電子メール通知については、これで \'8f\'5c 分です。

ただし、パスワード同期の電子メール通知については、ドライバポリシーにもパスワードを含める必要があります。メタディレクトリエンジンは、ユーザ名にアクセスできますが、パスワードにはアクセスできません。ドライバポリシーでパスワードを提供する必要があります。

次の条件に該当する場合は、この手順を実行する必要があります。

- SMTP サーバがセキュリティ保護されており、電子メールを送信する前に認証が必要な場合。
- Identity Manager パスワード同期を Identity Manager ドライバで使用している場合。
- ドライバのパスワード同期の設定で、［*Notify the user of password synchronization failure via e-mail*］を選択した場合。

ドライバポリシーに SMTP サーバのパスワードを追加する

1. パスワード同期を使用するために必要なポリシーがドライバに含まれていることを確認します。

   必要なポリシーは、サンプルドライバ設定で提供されています。また、111 ページのセクション 5.7「パスワード同期をサポートするための、既存のドライバ設定のアップグレード」に従い、追加することもできます。
2. iManager で、［*Identity Manager*］>［*Identity Manager の概要*］の順に選択します。
3. ドライバセットを検索するか、対象のドライバセットを含むコンテナを参照して選択します。
4. ［Identity Manager Driver Overview］で、ドライバのアイコンをクリックします。
5. ［Input Transformation］アイコンまたは［Output Transformation］アイコンを選択します。

6. ポリシーを選択し、［*Edit*］をクリックします。
7. ルールをクリックします。
8. ［Do Send E-mail from Template］アクションを含むルールで、SMTP サーバのパスワードを指定します。

たとえば、サンプルドライバ設定を使用している場合、次のパスワード同期ポリシーを変更する必要があります。

ポリシーセット	ポリシー名	ルール名
Input Transformation (入力変換)	Password(Pub)-Sub Email Notifications (パスワード (発行者)- 加入者の電子メール通知)	◆ パスワード購読時のエラーを電子メールで送信する ◆ Identity Manager データストアのパスワードを使用して接続システムのパスワードをリセットする際のエラーを電子メールで送信する
Output Transformation (出力変換)	Password(Sub)-Pub Email Notifications (パスワード (加入者)- 発行者の電子メール通知)	◆ パスワード発行操作のエラーを電子メールで送信する

次の \'90\'7d は、パスワードを必要とする［Do Send E-mail from Template］アクションの例を示します。

識別 \'83\'7bールトに保存されている場合、パスワードは不明です。

9 ルールを選択し (確認マークを付け)、［*OK*］をクリックします。

5.12.5 電子メール通知テンプレートへの独自の置換タグの追加

電子メール通知テンプレートには、デフォルトで定義されているタグがいくつかあり、これらを使用すると、ユーザへのメッセージを簡単にパーソナライズできます。また、独自のタグを追加することもできます。

タグを追加できるかどうかは、電子メールテンプレートを使用するアプリケーションによって異なります。

- 164 ページの 「パスワード同期の電子メール通知テンプレートへの置換タグの追加」
- 168 ページの 「パスワードを忘れた場合の電子メール通知テンプレートに対する、置換タグの追加」

パスワード同期の電子メール通知テンプレートへの置換タグの追加

パスワード同期の電子メール通知テンプレートには置換タグを追加できます。ただし、追加されたタグは、電子メール通知テンプレートを参照するすべてのパスワード同期化ポリシールールに定義しないと使用できません。［Do Send Email From Template］アクションを使用する場合、テンプレート内で宣言される置換タグはすべて、アクションの子 arg-strings 要素で定義する必要があります。

たとえば、Identity Manager には、電子メール通知テンプレートに含まれるデフォルトの置換タグが容易されています。Identity Manager では、デフォルトのパスワード同期ポリシーも、ドライバ環境設定で提供されています。電子メールテンプレートで提供されるデフォルトのタグもそれぞれ、電子メールテンプレートが使用するパスワード同期のポリシーの各ルールで定義されています。

たとえば、UserGivenName タグは、Password Set Fail という名前の電子メールテンプレートで定義されているデフォルトのタグの 1 つです。［*パスワードを取得できなかった場合に電子メールを送信する*］という名前のポリシールールは、［テンプレートから電子メールを送信］アクションの電子メールテンプレートを参照します。このルールは、パスワードの同期に失敗したときにユーザに通知する場合にポリシーで使用されます。同じ UserGivenName タグは、そのルールで arg-string 要素として定義されます。

この例のように、追加する新しい各タグは、電子メールテンプレートと、その電子メールテンプレートを参照するポリシールールの両方で定義する必要があります。これは、ユーザに電子メールを送信する場合に、Metadirectory エンジンが置換タグの代わりに正しいデータを \'91\'7d 入する方法を認識できるようにするためです。

例として、Identity Manager に付属の Identity Manager ドライバ設定にあるタグを参照できます。

次のガイドラインに注意してください。

- 電子メールテンプレートで置換タグと呼ばれる項目は、Policy Builder のコンテキストではトークンと呼ばれます。
- この節の手順で説明するように、置換タグの引数文字列の定義を簡略化するには、Policy Builder を使用します。
- 追加するタグは、次のどれかに定義できます。
  - ユーザの送信元または送信先の属性

    パスワードを忘れた場合のために電子メールテンプレートにタグを追加する場合とは異なり、識別ボールトのユーザオブジェクトにある属性と同じ名前を持つタグを追加しただけでは、そのタグを使用できません。パスワード同期化の電子メール通知テンプレートと使用するすべてのタグと同様に、電子メールテンプレートを参照するポリシーでも、タグを定義する必要があります。
  - グローバル設定値 (GCV)
  - XPATH 式

  eDirectory ユーザ属性に限定されている、パスワードを忘れた場合のための電子メールテンプレートにあるタグとは対照的です。
- パスワードを忘れた場合の電子メールテンプレートにタグを追加する場合は、eDirectory のユーザ属性の正確な名前を使用する必要がありますが、置換タグには任意の名前を付けることができます。ただし、電子メールテンプレートを参照するポリシーのタグの定義に使用される名前と一致することが必要です。

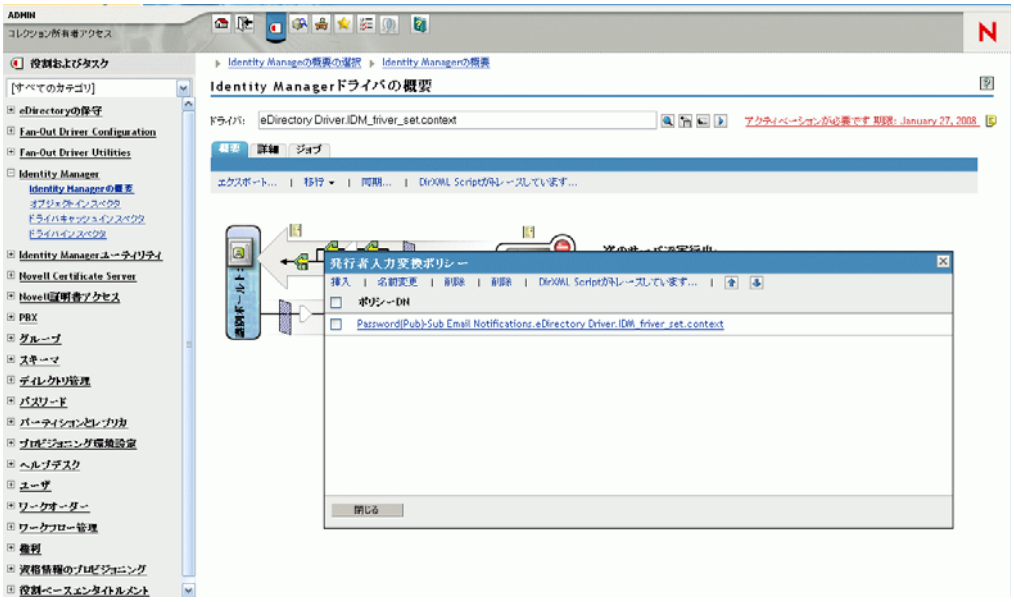
ポリシーにタグを定義するには、電子メール通知テンプレートを参照するポリシーをすべて検索し、ポリシービルダを使用してそれらのポリシーにタグを追加します。各ポリシーで、テンプレートを参照する各ルールを編集します。

電子メール通知テンプレートを参照するポリシーをすべて確実に検索する 1 つの方法は、ドライバ設定をエクスポートし、XML で、電子メール通知テンプレートと同じ名前のテンプレートを持つ do-send-e-mail アクションを検索することです。

1. iManager で、［*Identity Manager*］> ［Identity Manager Overview］の順に選択します。
2. 編集するポリシーのあるドライバを含むドライバセットを選択します。
3. 編集するポリシーが設定されているドライバのアイコンをクリックします。
4. 発行者チャネルまたは加入者チャネルで、編集するポリシーが含まれている一連のポリシーをクリックします。

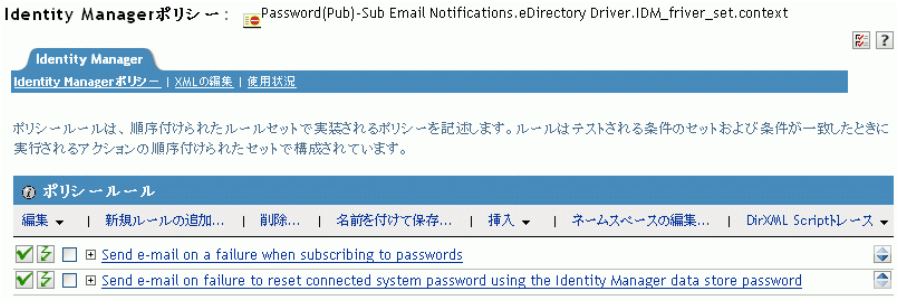
   たとえば、Identity Manager に付属している eDirectory ドライバ用のドライバ設定には、パスワード同期化の両方の電子メール通知テンプレートを参照する Input Transformation (入力変換) ポリシーセットのポリシーが含まれます。
5. ポリシーをクリックした後、［*Edit*］*をクリックします。*

   次の \'90\'7d は、eDirectory ドライバの Password(Pub)-Sub Email Notifications (パスワード (発行者)- 加入者の電子メール通知) ポリシーを編集する方法を示しています。

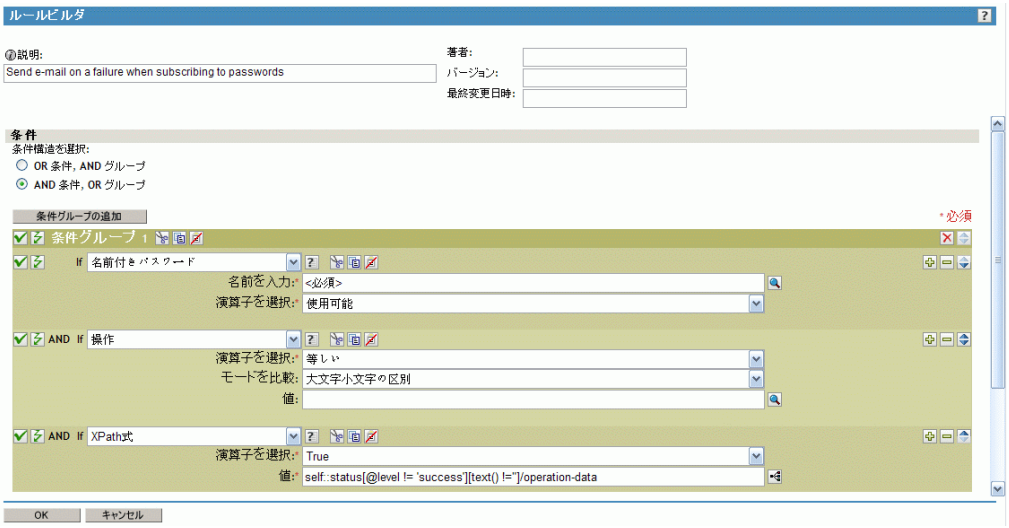


6. 開かれたルールのリストから、電子メール通知テンプレートを参照するルールをクリックします。

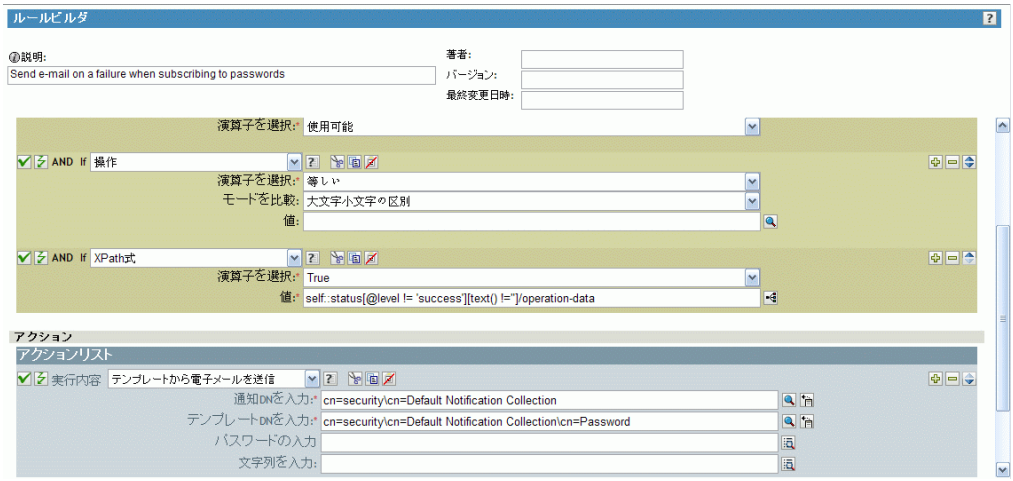
   たとえば、Password(Pub)-Sub Email Notifications (パスワード (発行者)- 購読者の電子メール通知) ポリシーでは、このようなルールのリストが表示されます。これらのルールは両方とも、パスワード同期の電子メールテンプレートの 1 つを参照します。両方のテンプレートにタグを追加する場合は、両方のルールを編集する必要があります。



最初のルールをクリックすると、次のページが \'95\'5c 示されます。



7 ［*Actions*］セクションまでスクロールします。



8 ［*テンプレートから電子メールを送信*］ルールを使用する場合は、 をクリックします。

文字列ビルダが開きます。この例のルールでは、次の図のような文字列のリストが表示されます。電子メール通知テンプレートに使用されるデフォルトのタグは、このよ

うに、Identity Manager ドライバ環境設定の一部であるパスワード同期ポリシーですでに定義されています。デフォルトのタグは、例として使用できます。

9 電子メール通知機 \'94\'5c テンプレートで使用するタグを定義するには、[*Append New String*] *をクリックし、タグの名前を入力します。*

電子メール通知機 \'94\'5c テンプレートで使用する名前と正確に一致する名前であることを確認してください。

10 [*文字列の値*] フィールドの [参照] ボタン

11 [引数ビルダ] ページでは、電子メール通知テンプレートでこのタグを使用する場合にどの値を引用するかを指定します。

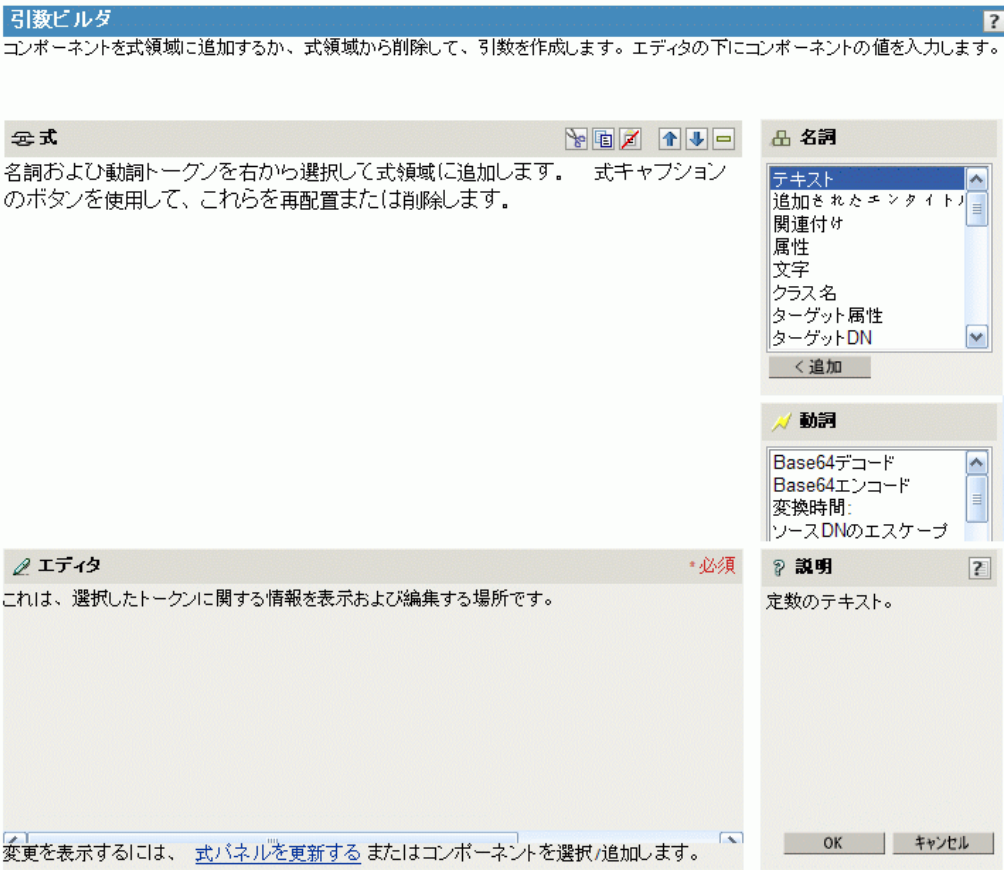
以下のタグを定義できます。

- ユーザの送信元または送信先の属性

  パスワードを忘れた場合のために電子メールテンプレートにタグを追加する場合とは異なり、識別ボールトのユーザオブジェクトにある属性と同じ名前を持つタグを追加しただけでは、そのタグを使用できません。パスワード同期化の電子メール通知テンプレートと使用するすべてのタグと同様に、電子メールテンプレートを参照するポリシーでも、タグを定義する必要があります。

- グローバル設定値 (GCV)
- XPATH 式

次の \'90\'7d は、タグを定義する方法を示しています。



タグの定義が終了したら［OK］をクリックします。タグが［String Builder］ページに文字列の 1 つとして\'95\'5c 示されます。

12 *［OK］をクリックしてすべてのページを終了し、ポリシーの変更を保存します。*

13 電子メール通知テンプレートを参照するすべてのポリシーのルールを編集するには、このステップを繰り返します。

14 ポリシーで定義したタグを電子メール通知テンプレートに追加します。ポリシーで使用した名前と完全に同じ名前を使用します。

これにより、電子メール通知テンプレートの \'96\'7b 文で、タグの名前を使用できるようになります。

15 変更内容を保存して、ドライバを再起動します。

パスワードを忘れた場合の電子メール通知テンプレートに対する、置換タグの追加

次のガイドラインに従い、パスワードを忘れた場合の電子メール通知テンプレートにタグを追加できます。

- 追加できるタグは、メッセージの送信先のユーザオブジェクトの LDAP 属性に対応するタグのみです。
- 追加するタグの名前は、ユーザオブジェクトの LDAP 属性の名前と完全に同じであることが必要です。

  LDAP 属性と eDirectory 属性の名前の対応については、LDAP の Identity Manager ドライバのスキー \'83\'7d\'83\'7dッピングルールを参照してください。

- その他の設定は必要ありません。

5.12.6 電子メール通知の管理者への送信

デフォルトの設定では、電子メール通知はユーザに対してのみ送信されます。Identity Manager に付属のポリシーでは、影響するユーザの識別 \'83\'7bールトオブジェクトの電子メールアドレスを使用します。

ただし、パスワード同期のポリシーでは、電子メール通知を管理者に対しても送信できるよう設定できます。設定するには、ポリシーの 1 つの Identity Manager スクリプトを変更する必要があります。

管理者の電子メールアドレスとトークンを定義し、管理者にブラインドコピーを送信します。

管理者にコピーを送信するには、電子メールを作成するポリシー (通知を送信するためにポリシーが電子メールアドレスを検索する PublishPasswordEmails.xml など) を変更し、追加の <arg-string> 要素と管理者の電子メールアドレスを追加します。

次の例では、追加的な arg-string 要素を示しています。

```
<arg-string name="to">
<token-text>Admin@company.com</token-text>
</arg-string>
```

変更後、必ずドライバを再起動するようにしてください。

5.12.7 電子メール通知テンプレートのローカライズ

次のことに注意してください。

- デフォルトのテンプレートは英語で \'95\'5c 記されていますが、他の言語を使用するようテキストを編集できます。
- ポリシーの arg-string トークン定義と置換タグの名前が一致するよう、置換タグの名前と定義は英語のままでなければなりません。
- パスワードを忘れた場合の電子メール通知についてのみ、電子メールのエンコード方法を指定するために、portalservlet.properties ファイルに設定を追加する必要があります。例 :

  ```
  ForgottenPassword.MailEncoding=EUC-JP
  ```

  この設定が存在しない場合、電子メール変換にエンコードは使用されません。
- パスワード同期の電子メールメッセージについては、<mail、<message、および < ‘> 要素に charset という名前の XML 属性を指定できます。

  これらの要素の使用方法の詳細については、電子メールテンプレートの詳細が記述されている『*DirXML Driver for Manual Task Service Implementation Guide* (http://www.novell.com/documentation/dirxmldrivers/index.html)』を参照してください。

5.13 パスワード同期のトラブルシューティング

- のヒントを参照してください。120 ページのセクション 5.8「パスワード同期の実装」
- NMAS に通常パスワードログインメ \'83\'5cッドがインストールされていることを確認します。

- eDirectory ログインメ \'83\'5cッド、または Identity Manager により同期化する接続システムのパスワードに NMAS でパスワードポリシーを適用するサーバに、ツリーのルートのコピーがあることを確認します。
- パスワード同期を必要とするユーザが、パスワードを同期するドライバのある同じサーバに複製されていることを確認します。他のドライバの機 \'94\'5c と同様に、ドライバは、同じサーバの、\'83\'7d スタレプリカまたは読み書き可 \'94\'5c レプリカに存在するユーザのみを管理できます。
- Web サーバと識別 \'83\'7bールトとの間で SSL が適切に設定されていることを確認します。
- ユーザを最初に作成したときにパスワードが準拠していないというエラーが\'95\'5c示されたにもかかわらず、パスワードが識別 \'83\'7bールトに正しく設定されている場合は、ドライバポリシーのデフォルトのパスワードが、ユーザに適用されるパスワードポリシーに準拠していない可 \'94\'5c 性があります。

  次のシナリオでは、Active Directory ドライバが使用されています。しかし、他のドライバでも同じ問題が発生する場合があります。

  初期パスワードの提供。Active Directory 内のユーザに一致させるために、ドライバにより識別ボールトに新しいユーザオブジェクトが作成されるときに、Active Directory ドライバにユーザの初期パスワードを提供させたいとします。Active Directory ドライバのサンプル環境設定は、初期パスワードをユーザの追加とは別の操作として送信します。さらに、Active Directory からパスワードが提供されない場合はユーザのデフォルトパスワードを提供するポリシーも含んでいます。

  ユーザの追加とパスワードの設定は別々に実行されるため、一時的ではあっても、新しいユーザはデフォルトのパスワードを常に受信します。ユーザを追加後すぐに Active Directory ドライバがパスワードを送信するため、デフォルトのパスワードはすぐに更新されます。デフォルトパスワードがユーザの識別 \'83\'7bールトのパスワードポリシーに準拠しない場合、エラーが \'95\'5c 示されます。

  たとえば、ユーザの名字を使用して作成されたパスワードがパスワードポリシーに対して短すぎる場合は、パスワードが短すぎることを示す -216 エラーが表示されます。ただし、その後 Active Directory がポリシーに準拠する初期パスワードを送信した場合には、状況はすぐに解決されます。

  使用しているドライバにかかわらず、ユーザオブジェクトを作成する接続システムが初期パスワードを提供するようにするには、次のいずれかのアクションを実行することを検討します。これらの方法は、初期パスワードが Add イベントに付属しないけれども、それ以降のイベントとして提供される場合には、特に重要です。

  - 組織のために識別ボールトで定義されたパスワードポリシーにデフォルトのパスワードが準拠するように、デフォルトのパスワードを作成する発行者チャネルのポリシーを変更します。(［*Passwords*］*を選択し*、［Password Policies］を選択します。)

    初期パスワードが認証されたアプリケーションから提供されると、デフォルトパスワードを上書きします。

    このオプションを使用することをお勧めします。これは、システム内で高レベルのセキュリティを維持するために、デフォルトのパスワードポリシーを用意することが推奨されているためです。

  - 発行者チャネルで、デフォルトのパスワードを作成するポリシーを削除します。サンプルの環境設定では、このポリシーはコマンド変換ポリシーセットにより提供されます。識別ボールトでは、パスワードのないユーザも追加できます。このオプションは、新しく作成されたユーザオブジェクトについてのパスワードが最

終的に加入者チャネルから提供されることを想定しており、ユーザオブジェクトは一時的にはパスワードなしで存在できます。

- パスワードポリシーはツリー中心で割り当てられます。一方、パスワード同期はドライバごとに設定されます。ドライバはサーバごとにインストールされ、マスタレプリカまたは読み書き可能レプリカのユーザのみ管理できます。

  パスワード同期により期待される結果を取得するには、パスワード同期を実行するサーバにあるマスタレプリカまたは読み書き可能レプリカのコンテナが、ユニバーサルパスワードが有効なパスワードポリシーを割り当てたコンテナと一致するようにします。パーティションルートコンテナにパスワードポリシーを割り当てることによって、そのコンテナとサブコンテナ内のすべてのユーザに確実にパスワードポリシーが割り当てられます。

- DSTrace の便利なコ \'83\'7d ンド

  +*DXML*: Identity Manager ルール処理および可能性のあるエラーメッセージを表示する。

  +*DVRS*: Identity Manager ドライバのメッセージを表示する。

  +*AUTH*: NDS パスワードの変更を表示する。

  +*DCLN*: NDS DClient メッセージを表示する。

エンタイトルメントの作成と使用

6

Identity Manager を使用すると、接続されたシステム間でデータを同期できます。エンタイトルメントにより、ユーザまたはグループに対する条件を設定できます。条件が一致すると、接続されたシステム内のビジネスリソースへのアクセス権を付与したり、取り消したりするイベントが開始されます。これにより、もう 1 つのレベルの制御を取得し、リ\'83\'5c ースの付与および取り消しを自動化できます。

エンタイトルメントを機能させるには、エンタイトルメントの作成とエンタイトルメントの管理という 2 つの局面があります。エンタイトルメントは、iManager または Designer を使用して作成します。iManager を使用してエンタイトルメントを作成するには、iManager の Identity Manager ユーティリティのヘッダで［*エンタイトルメントの作成*］オプションを選択します。詳細については、179 ページのセクション 6.4「iManager を介した XML でのエンタイトルメントの記述」を参照してください。

Designer を使用してエンタイトルメントを作成し、既存の Identity Manager ドライバに展開することもできます。Designer を使用すると、エンタイトルメントウィザードを使用してエンタイトルメントを作成できます。エンタイトルメントウィザードには、グラフィカルインタフェースが示され、ステップに従うことでエンタイトルメントを作成できます。iManager では、シンプルなインタフェースを介してエンタイトルメントを作成しますが、XML エディタを使用して追加のプロパティを追加する必要があります。これはグラフィカルインタフェースであるため、エンタイトルメントの作成および編集には Designer を使用することをお勧めします。

エンタイトルメントを作成した後 (または特定の Identity Manager ドライバで事前に設定されたエンタイトルメントを使用して)、エンタイトルメントを管理する必要があります。エンタイトルメントは、2 つのパッケージまたはエージェントによって (役割ベースエンタイトルメントポリシーとしての iManager を介して、またはワークフローベースのプロビジョニングのユーザアプリケーションを介して) 管理されます。ワークフローベースのプロビジョニングで使用されるエンタイトルメントについては、『*Identity Manager 3.5.1 User Application: Administration Guide*』の「“ プロビジョニング要求定義の設定 ”」を参照してください。

条件が一致した場合、役割ベースエンタイトルメントポリシーによりビジネスリソースを付与できます。たとえば、ユーザが条件 1、2、および 3 を満たしている場合、Role-Based Entitlement (役割ベースのエンタイトルメント) ポリシーを介して、ユーザはグループ H のメンバーになりますが、ユーザが条件 4 および 5 を満たしている場合、グループ I のメンバーになります。このエンタイトルメントがワークフローベースのプロビジョニングを介して機 \'94\'5c するには、最初に承認が必要です。

- 198 ページのセクション 6.7「Entitlement Policy (エンタイトルメントポリシー) の作成」
- 206 ページのセクション 6.8「Role-Based Entitlement (役割ベースのエンタイトルメント) ポリシー間での衝突解決」
- 210 ページのセクション 6.9「Role-Based Entitlement (役割ベースのエンタイトルメント) のトラブルシューティング」
- 211 ページのセクション 6.10「Role-Based Entitlement (役割ベースのエンタイトルメント) およびワークフローベースのプロビジョニングのエンタイトルメントに適用されるエンタイトルメント要素」

6.1 用語集

この章で使用される用語を次に示します。

表 6-1 *用語集*

用語	説明
エンタイトルメント	接続システム内のビジネスリ \'83\'5c ースを \'95\'5c す識別 \'83\'7bールトオブジェクト。
エンタイトルメントエージェント	エンタイトルメントを付与したり、取り消したりします。Role-Based Entitlement (役割ベースのエンタイトルメント) では、エージェントはエンタイトルメントサービスドライバです。
付与または取り消し	エンタイトルメントの付与または取り消しの解釈は、Identity Manager ドライバのグローバル設定の変数 (GCV) によって制御されます。
エンタイトルメントコンシュー \'83\'7d	エンタイトルメント関連の情報を使用するものすべて。エンタイトルメントコンシュー \'83\'7d には、iManager、ユーザアプリケーション、および Identity Manager ポリシーが含まれています。

6.2 エンタイトルメントを作成する : 概要

- 175 ページのセクション 6.2.1「エンタイトルメントをサポートする、設定済みの Identity Manager ドライバ」
- 176 ページのセクション 6.2.2「他の Identity Manager ドライバでのエンタイトルメントの有効化」

エンタイトルメントで実行する内容を事前に理解しておく必要があります。エンタイトルメントは、ポリシーを介して Identity Manager ドライバに組み込んだ機能から動作します。これらのドライバポリシーによってルールが実装され、識別ボールトと接続システムとの間でイベントが処理されます。Identity Manager ドライバのポリシーで実行する内容を指定しないと、エンタイトルメントは機能しません。たとえば、コ \'83\'7d ンドポリシーの［Check User Modify for Group Membership］ルールの［action］セクションを指定しない場合、グループメンバーシップエンタイトルメントの付与または取り消しの試行は無視されます。

すべての接続システムのリソースに対する付与および取り消しの機能を正しく設計するためには、Identity Manager で実行する内容を正確に理解しておく必要があります。次の 4 つのステップの手順は、エンタイトルメントの作成および使用の計画に役立ちます。

1. ビジネスの場で実現したいことを理解します。Identity Manager を介してほとんど何でも設計および実装できますが、定義されていないことを実装する前に、実現したい内容を理解しておく必要があります。何をしたいのかの番号付きリストを作成します。
2. 番号付きリストの 1 つのポイントを表すエンタイトルメントを定義します。値のないエンタイトルメントと値のあるエンタイトルメントを作成できます。値のあるエンタイトルメントは、外部クエリから値を取得できます。エンタイトルメントは、管理者が定義した形式にすることも、自由形式にすることもできます。に例を示しています。189 ページのセクション 6.4.6「独自のエンタイトルメントを作成するためのエンタイトルメントの例」
3. Identity Manager ドライバにポリシーを追加し、設計されたエンタイトルメントを実装します。Identity Manager ドライバ用のポリシーを作成するには、接続システムで情報が処理および受信される方法、および Novell® eDirectory™ に情報が保存される方法の点で、XSLT または DirXML スクリプトに精通している必要があります。優れた DirXML* のプログラマでない限り、これはコンサルタントの仕事です。
4. エンタイトルメントを付与または取り消すための管理エージェントを設定します。自動処理にする場合、Role-Based Entitlement (役割ベースのエンタイトルメント) を使用します。手動処理にする場合、ワークフローベースのプロビジョニングを使用します。

6.2.1 エンタイトルメントをサポートする、設定済みの Identity Manager ドライバ

Identity Manager には、エンタイトルメント、エンタイトルメントを実装するためのポリシー、およびエンタイトルメントアクティビティのリッスンが有効になっているドライバがすでに含まれている、設定ファイル付きの多くのドライバが付属しています。ドライバを初めてインストールする際、事前設定済みの要素をドライバの一部にするために、エンタイトルメントを有効にする必要があります。以下のドライバには、エンタイトルメントをサポートする設定ファイルが付属しています。

- Active Directory
- 交換
- GroupWise
- LDAP
- NIS
- Lotus Notes
- NT ドメイン
- RACF

これらの事前設定済みのドライバでは、上記の 4 つのステップの最初の 3 つが実行されます。ドライバに含まれているエンタイトルメントのタイプの例は、最も一般的なシナリオ

(ユーザアカウント、グループ、および電子メール配布リストの付与および取り消し) で使用できます。具体的には、次のようなメカニズムがあります。

- Active Directory: アカウント、グループメンバーシップ、Exchange メールボックスの付与および取り消し
- Exchange 5.5: メールボックスとグループメンバーシップの付与および取り消し
- GroupWise: アカウントおよび配布リストのメンバーの付与および取り消し
- LDAP: ユーザアカウントの付与および取り消し
- Linux and UNIX: アカウントの付与および取り消し
- Lotus Notes: ユーザアカウントおよびグループメンバーシップ付与および取り消し
- NT Domain: ユーザアカウントおよびグループメンバーシップ付与および取り消し
- RACF: グループアカウントおよびグループメンバーシップの付与および取り消し

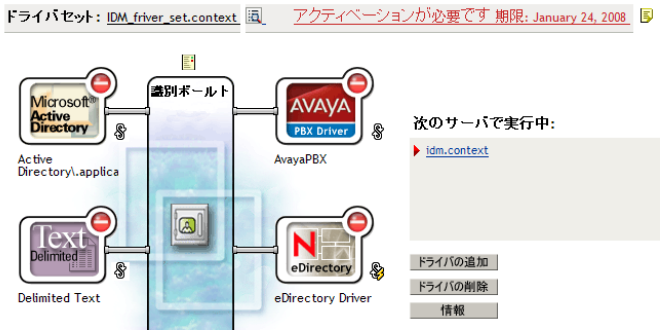
これらのエンタイトルメントおよびポリシーの例は、自分のニーズを満たしていればそのまま使用できます。ニーズを満たすように変更する、または例として使用して、iManager または Designer を介して独自のエンタイトルメントおよびポリシーを作成することもできます。繰り返しますが、事前設定済みのドライバのエンタイトルメントを使用するには、事前設定済みのドライバを Designer または iManager で初めて作成するときにエンタイトルメントを有効にする必要があります。事前設定済みのエンタイトルメントは、ドライバを再作成しない限り、後で追加することはできません。

Identity Manager 2.x でエンタイトルメントを使用していて、これらのエンタイトルメントを Identity Manager 3.5.1 で使用するには、［*Identity Manager ユーティリティ*］の［*エンタイトルメントのアップグレード*］オプションを実行します。

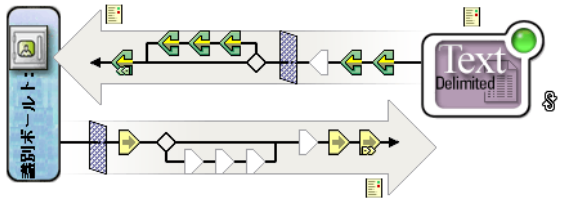
6.2.2 他の Identity Manager ドライバでのエンタイトルメントの有効化

事前設定済みのエンタイトルメントが含まれていない Identity Manager ドライバで、エンタイトルメントを使用することもできます。ドライバでエンタイトルメントのサポートを有効にするには、DirXML-EntitlementRef 属性をドライバフィルタに追加します。これには次の操作を行います。

1. ［*Identity Manager*］> ［Identity Manager Overview］の順に選択します。
2. ドライバがある場所でドライバセットを参照し、［*検索*］をクリックします。
3. ［Identity Manager の概要］ページで、ドライバオブジェクトをクリックします。

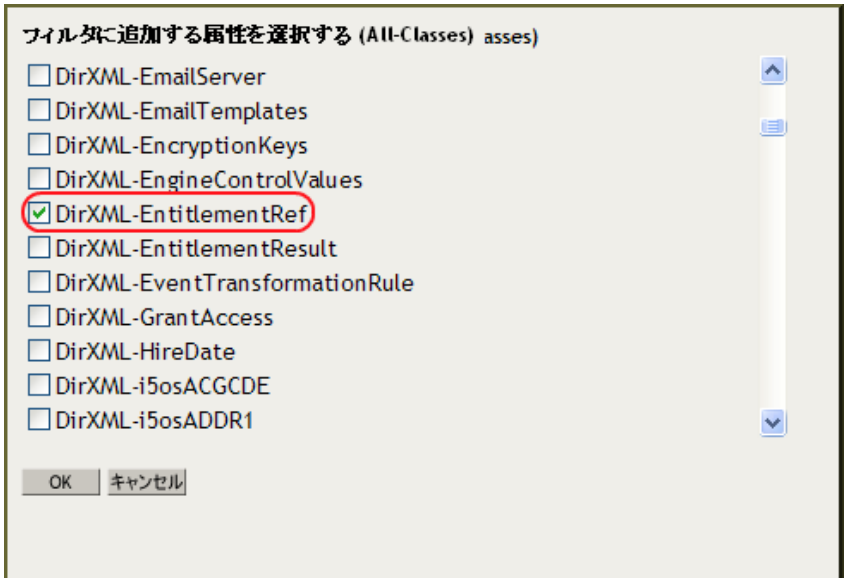


4 「ドライバの概要」ページで識別ボールトの右側にある［*ドライバフィルタ*］アイコン (赤い円で囲まれています) をクリックします。



5 *属性の追加*］を選択し、下部までスクロールして［*すべての属性を表示*］を選択します。

6 ［*DirXML-EntitlementRef*］属性を選択して、［*OK*］をクリックします。



7 ［フィルタ］ページで［*DirXML-EntitlementRef*］を選択し、購読ヘッダで［*通知*］を選択します。

8 ［*OK*］をクリックし、変更を保存します。

ドライバ上で Designer を介してエンタイトルメントを作成すると、この処理は自動的に実行されます。

6.3 エンタイトルメントの必要条件

- ❑ eDirectory 8.7.3 以降
- ❑ Identity Manager 2.x または 3.x
- ❑ エンタイトルメントサービスドライバ

  エンタイトルメントを使用する場所の各ドライバセットに、エンタイトルメントサービスドライバが必要です。エンタイトルメントサービスドライバを使用するには、各ドライバセットについて、簡単な設定が一度だけ必要です。
- ❑ エンタイトルメントをサポートするドライバ設定

  接続システムでエンタイトルメントを使用する前に、次のいずれかを実行します。

  - ドライバの Identity Manager ドライバ設定をインポートし、そのドライバのエンタイトルメントが有効になっていることを指定する。
  - ドライバがエンタイトルメントをサポートするようにする。これには次の操作を行います。

    a. iManager または Designer を使用してエンタイトルメントを作成します (Designer をお勧めします)。

    b. で説明したように、DirXML-EntitlementRef 属性をドライバフィルタに追加します。176 ページのセクション 6.2.2「他の Identity Manager ドライバでのエンタイトルメントの有効化」

    c. ステップ 1 で作成したエンタイトルメントを実装するよう、ポリシーを記述します。

6.4 iManager を介した XML でのエンタイトルメントの記述

エンタイトルメントで何が必要なのかを理解するために、有効化されたエンタイトルメントがある、事前設定済みのドライバのひとつである Active Directory のエンタイトルメントおよびポリシーを確認できます。これには、Novell のエンタイトルメント DTD (Document Type Definition) の調査が含まれています。また、DTD に基づいてエンタイトルメントを記述する XML の例も見てみます。

この節では、次の項目について説明します。

6.4.1 エンタイトルメントが有効になっている場合に、Active Directory ドライバによって何が追加されるか

エンタイトルメントが有効な Active Directory ドライバには、構造に次の変更が含まれています。

- ドライバフィルタに DirXML-EntitlementRef 属性を追加します。DirXML-EntitlementRef 属性により、ドライバフィルタはエンタイトルメントアクティビティをリッスンできます。
- ユーザアカウントのエンタイトルメントを作成します。ユーザアカウントのエンタイトルメントにより、ユーザの Active Directory のアカウントが付与または取り消されます。アカウントが付与されると、ユーザは有効なログオンアカウントを取得できます。アカウントが取り消されると、ドライバがどのように設定されているのかに応じて、ログオンアカウントは無効になるか、削除されます。
- グループメンバーシップのエンタイトルメントを作成します。グループのエンタイトルメントにより、Active Directory のグループのメンバーシップが付与または取り消されます。グループは識別ボールト内のグループと関連付けられている必要があります。メンバーシップが取り消されると、グループからユーザが削除されます。外部ツールによって Active Directory 内の制御されているグループにユーザが追加され、ユーザがドライバによって削除されない場合、グループメンバーシップエンタイトルメントは発行者チャネルには適用されません。また、エンタイトルメントが取り消されるのではなく、ユーザオブジェクトから削除された場合、Active Directory ドライバではアクションは実行されません。

- Exchange メールボックスエンタイトルメントを作成します。グループのエンタイトルメントにより、Microsoft Exchange のユーザの Exchange メール \'83\'7bックスが付与または取り消されます。
- エンタイトルメント情報を多くのポリシーに追加します。

次のポリシーには、エンタイトルメントが適切に機 \'94\'5c するように追加的なルールが含まれています。

- InputTransform (ドライバレベル)。このポリシーの［Check Target Of Add Association For Group Membership Entitlements (グループメンバーシップエンタイトルメントに対する add-association の対象を確認する)］ルールでは、グループメンバーシップエンタイトルメントの「add-association」の対象が確認されます。Active Directory で作成されるユーザに割り当てられたグループメンバーシップのエンタイトルメントは、ユーザが正常に作成されるまでは処理できません。Add-association は、Active Directory でドライバによってオブジェクトが作成されたことを示します。オブジェクトもグループエンタイトルメント処理に対してタグ付きである場合、すぐに実行されます。
- イベント変換 (発行者チャネル)。このポリシーの［ユーザアカウントの削除を許可しない］ルールでは、識別ボールトのユーザアカウントの削除は拒否されます。ユーザアカウントのエンタイトルメントを使用する場合、管理対象のユーザアカウントは識別ボールト内のエンタイトルメントで制御されます。Active Directory で削除しても、識別ボールト内の制御オブジェクトは削除されません。識別 \'83\'7bールト内のオブジェクトを今後変更したり、\'83\'7dージ操作を実行すると、Active Directory でアカウントが再作成される場合があります。
- コマンド (購読者チャネル)。コ \'83\'7d ンドポリシーには、エンタイトルメントに関する次のルールが含まれています。
  - ユーザアカウントのエンタイトルメント変更 (削除オプション) ルール。ユーザアカウントのエンタイトルメントによって、Active Directory の有効なアカウントがユーザに付与されます。エンタイトルメントを取り消すと、［*アカウントのエンタイトルメントが取り消された場合*］グローバル変数で選択した値に応じて、Active Directory アカウントが無効になるか、削除されます。エンタイトルメントが変更され、［Delete］オプションを選択した場合、このルールが実行されます。
  - ユーザアカウントエンタイトルメントの変更 (無効オプション) ルール。ユーザアカウントのエンタイトルメントによって、Active Directory の有効なアカウントがユーザに付与されます。エンタイトルメントを取り消すと、［*アカウントのエンタイトルメントが取り消された場合*］グローバル変数で選択した値に応じて、Active Directory アカウントが無効になるか、削除されます。エンタイトルメントが変更され、［Disable］オプションを選択した場合、このルールが実行されます。
  - ［Check User Modify for Group Membership Being Granted or Revoked］ルール。
  - ［Check User Modify for Exchange Mailbox Being Granted or Revoked］ルール。
- 一致 (購読者チャネル)。これはアカウントのエンタイトルメントです。このポリシーの既存のアカウントルールとは一致しません。Identity Manager ユーザアプリケーションまたは役割ベースエンタイトルメントでユーザアカウントのエンタイトルメントを使用する場合、エンタイトルメントを付与または取り消すことにより、アカウントが作成または削除されます (または無効になります)。ユーザが Active Directory のアカウントに対する権利を与えられていない場合、デフォルトポリシーは Active Directory の既存のアカウントとは一致しません。る Active Directory の一致していアカウントにエンタイトルメントポリシーを適用する場合は、このルールを変更または

削除します。これにより、Active Directory アカウントが削除されるか、または無効になります。

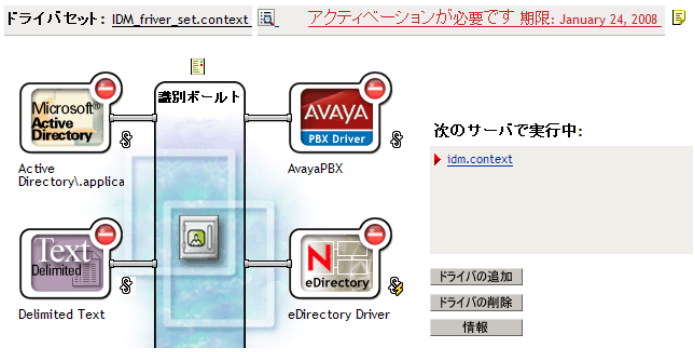
- 作成 (購読者チャネル)。Create Policy (作成ポリシー) には、エンタイトルメントに関する次のルールが含まれています。
  - アカウントエンタイトルメント : エンタイトルメントが付与されない場合にアカウント作成をブロックします。Identity Manager ユーザアプリケーションまたは役割ベースエンタイトルメントでユーザアカウントのエンタイトルメントを使用する場合、アカウントのエンタイトルメントを明確に付与されたユーザに対してのみアカウントが作成されます。エンタイトルメントが付与されない場合、このルールによりユーザアカウント作成が拒否されます。
  - 無効なログインが存在しない場合、識別 \'83\'7bールトのアカウントが有効になります。
  - 追加後にグループエンタイトルメントのチェックの準備をします。追加されたオブジェクトはグループに追加するために終了する必要があるので、グループエンタイトルメントは追加処理が完了した後で処理されます。追加処理が完了したときに入力変換で確認された運用プロパティとともに、追加がフラグ \'95\'5c 示されます。
  - 追加後にエンタイトルメントの交換を確認する必要があることを示します。
  - ユーザ名を Windows ログオン名にマップします。eDirectory ユーザ名の後に userPrincipalName が設定されている場合、eDirectory オブジェクト名と Active Directory ドメインの名前に userPrincipalName を設定します。

iManager で次のステップを実行すると、各ポリシーの実際の XML コードを \'95\'5c 示できます。

1 ［*Identity Manager*］> ［Identity Manager Overview］の順に選択します。

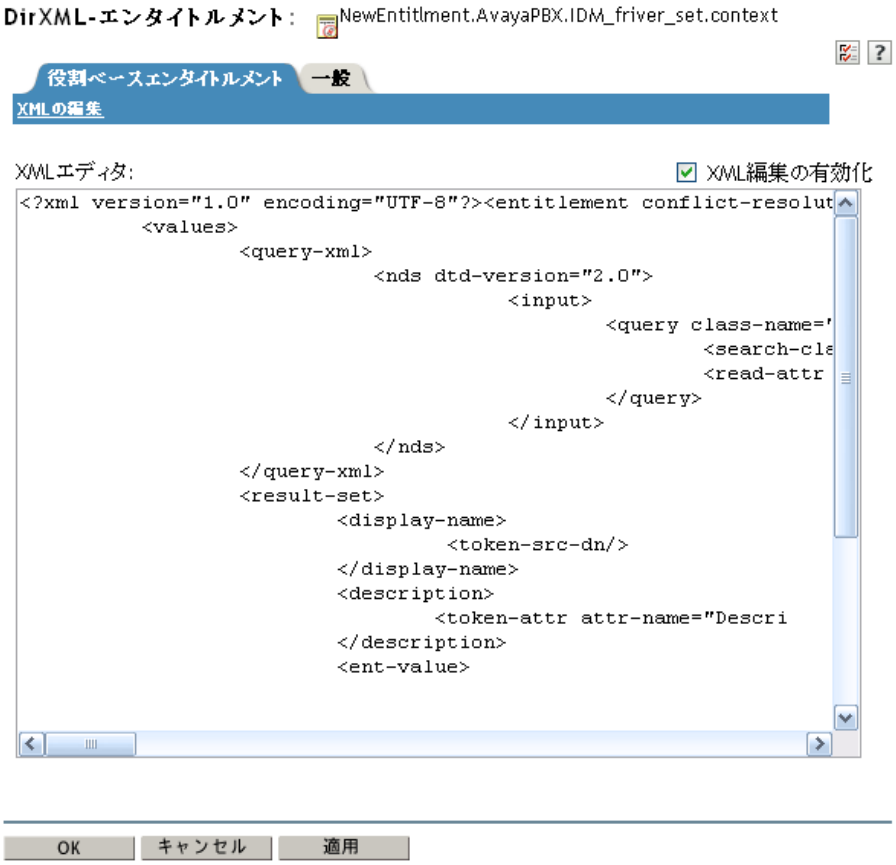
2 ドライバがある場所でドライバセットを参照し、［*検索*］をクリックします。

3 ［Identity Manager の概要］ページで、ドライバオブジェクトをクリックします。



4 ［ドライバの概要］ページで、［*詳細*］をクリックし、［*エンタイトルメント*］をクリックします。

5 エンタイトルメント名をクリックして、ポリシーを XML で表示します。



ポリシーの作成および編集の詳細については、「*Identity Manager 3.5.1 のポリシーの理解*」を参照してください。また、そのドライバ固有のポリシーを作成するには、選択した『Identity Manager ドライバガイド (http://www.novell.com/documentation/idm35drivers/index.html)』を参照してください。

有効化されたエンタイトルメントを持つ Active Directory ドライバには、3 つのエンタイトルメント (ユーザアカウント、グループ、および Exchange メール) が付属しています。

図 6-1 Active Driver ドライバに付属しているエンタイトルメント

の記述サンプルの一部として、これらのエンタイトルメントの XML コードを \'95\'5c 示できます。189 ページのセクション 6.4.6「独自のエンタイトルメントを作成するためのエンタイトルメントの例」

6.4.2 Novell のエンタイトルメントのドキュメントタイプ定義 (DTD) の使用

一部のエンタイトルメントは、エンタイトルメントが有効になっているドライバで事前定義されています。これらのエンタイトルメントを使用するか、iManager または Designer で独自のエンタイトルメントを作成できます。独自のエンタイトルメントを作成するには、エンタイトルメントを作成する例として、次の Novell エンタイトルメント DTD を使用します。

この DTD の説明では、iManager を介してこの XML 形式でエンタイトルメントを記述する方法の 4 つの例を示します。XML 形式について詳しくない場合は、より簡単にエンタイトルメントを作成できる Designer の Entitlement Wizard を使用してください。

Novell のエンタイトルメント DTD

```
<!-************************************************************->
<!-- DirXML Entitlements DTD  <!-- Novell Inc. <!-- 1800 South Novell
Place <!-- Provo, UT 84606-6194 <!-- Version=1.0.0 <!-- Copyright 2005
Novell, Inc. All rights reserved --> <!--
********************************************************** --> <!--
Entitlement definition stored in the XmlData attribute of a
DirXML-Entitlement object. --> <!ELEMENT entitlement (values?)>
<!ATTLIST entitlement conflict-resolution (priority | union)
"priority" display-name CDATA #REQUIRED description CDATA #REQUIRED >
<!ELEMENT values (query-app | value+)?> <!ATTLIST values multi-valued
(true | false) "true" > <!ELEMENT value (#PCDATA)> <!ELEMENT query-app
(query-xml, result-set)> <!ELEMENT query-xml ANY> <!ELEMENT result-set
(display-name, description, ent-value)> <!ELEMENT display-name(token-
```

```
attr | token-src-dn | token-association)> <!ELEMENT ent-value (token-
association | token-src-dn | token-attr)> <!ELEMENT description
(token-association | token-src-dn | token-attr)> <!ELEMENT token-
association EMPTY> <!ELEMENT token-attr EMPTY> <!ATTLIST token-attr
attr-name CDATA #REQUIRED > <!ELEMENT token-src-dn EMPTY> <!--
Entitlement reference stored in the DirXML-EntitlementRef attribute of
a DirXML-EntitlementRecipient or a DirXML-SharedProfile object. -->
<!ELEMENT ref (src?, id?, param?)> <!ELEMENT param (#PCDATA)>
<!ELEMENT id (#PCDATA)> <!ELEMENT src (#PCDATA)> <!--     Entitlement
result stored in the DirXML-EntitlementResult attribute of a DirXML-
EntitlementRecipient object. --> <!ELEMENT result(dn, src, id?,
param?, state, status, msg?,timestamp)> <!ELEMENT dn (#PCDATA)>
<!ELEMENT state (#PCDATA)> <!ELEMENT status (#PCDATA)> <!ELEMENT msg
ANY> <!ELEMENT timestamp (#PCDATA)> <!--    Cached query results stored
in the DirXML-SPCachedQuery attribute of a DirXML-Entitlement object.
--> <!ELEMENT items (item*)> <!ELEMENT item (item-display-name?, item-
description?, item-value)> <!ELEMENT item-display-name (#PCDATA)>
<!ELEMENT item-description (#PCDATA)> <!ELEMENT item-value (#PCDATA)>
<!--    Representation of a DirXML-EntitlementRef within the DirXML
Script and within the operation-data of an operation in an XDS
document. --> <!ELEMENT entitlement-impl (#PCDATA)> <!ATTLIST
entitlement-impl name CDATA #REQUIRED src CDATA #REQUIRED id CDATA
#IMPLIED state (0 | 1) #REQUIRED src-dn CDATA #REQUIRED src-entry-id
CDATA #IMPLIED >
```

6.4.3 エンタイトルメント DTD の説明

エンタイトルメント DTD は、定義、参照、結果、キャッシュされたクエリ、および内部の参照情報の 5 つの部分に分けられます。ヘッダは単なるコメントであり、必須ではありません。DTD では、エンタイトルメント定義のヘッダは次のようになります。

<!-- DirXML-Entitlement オブジェクトの XmlData 属性に格納されているエレメント定義 -->

ヘッダの次に要素 (ELEMENT) および属性リスト (ATTLIST) が続きます。以下は、エンタイトルメント定義ヘッダの下にある要素および属性の詳しい説明です。これは、エンタイトルメントを作成するときに重点を置く必要があるメインヘッダです。

<!ELEMENT entitlement (values?)>

ルートレベルの要素は、<entitlement> です。これには、単一、オプション、子の <values> 要素を含めることができます。この後には属性リストが続きます。属性リストには、conflict-resolution、display-name、および description が含まれています。衝突解決では、Priority 属性または Union 属性の値を使用します。

conflict-resolution (priority | union) "priority"

役割ベースエンタイトルメントでは、衝突の解決を使用して、値のあるエンタイトルメントが同じオブジェクトに複数回適用された場合に行うアクションを決定します。たとえば、ユーザ U がエンタイトルメントポリシー A およびエンタイトルメントポリシー B のメンバーであるとします。それぞれが同じ値のあるエンタイトルメント E を参照していますが、異なる値を持っています。エンタイトルメントポリシー A のエンタイトルメント E には、値 (a、b、c) が設定されています。Entitlement Policy (エンタイトルメントポリシー) B のエンタイトルメント E は、一連の値を持っています (c、d、e)。

衝突の解決の属性により、どの値がユーザ U に適用されるかが決まります。union に設定されている場合、ユーザ U には両方の値のセット (a、b、c、d、e) が割り当てられます。priority に設定されている場合、どの Entitlement Policy (エンタイトルメントポリシー) がより高い優先度を持っているのかに応じて、ユーザ U は 1 つの値のみを取得します。

エンタイトルメントが単一の値である場合、優先度によって衝突を解決する必要があります。値を結合すると複数の値が適用されるからです。現在では、Role-Based Entitlement (役割ベースのエンタイトルメント) がこの属性を使用していますが、今後はワークフローのエンタイトルメントも使用する場合があります。

display-name CDATA #REQUIRED description CDATA #REQUIRED

リテラルのエンタイトルメント名は、エンタイトルメントで表示される文字である必要はありません。Display-name および Description の属性は、エンドユーザの表示用のものです。(Designer では、実際のエンタイトルメント名を使用する代わりに、エンタイトルメントの \'95\'5c 示名を選択するオプションがあります。)

<!ELEMENT values (query-app | value+)?> <!ATTLIST values multi-valued (true | false) "true"

<values> 要素は必須ではありません。これは、エンタイトルメントに値があることを示します。この要素を使用しない場合、エンタイトルメントには値がないことを意味します。値のあるエンタイトルメントの例としては、配布リストを付与するエンタイトルメントがあります。値のないエンタイトルメントの例としては、Active Directory ドライバに付属しているユーザアカウントのエンタイトルメントなど、アプリケーションでアカウントを付与するエンタイトルメントがあります。

値のあるエンタイトルメントは、値を 3 つのソースから受け取ります。1 つのソースは、(<query-app> 要素によって設計された) 外部アプリケーションです。もう 1 つは、値が列挙されている事前定義されたリストからです (1 つ以上の <value> 要素)。3 番目のソースは、エンタイトルメントのクライアントからです (<value> 子を持たない <values> 要素)。例を使用して、値が機 \'94\'5c する様子を説明します。

値のあるエンタイトルメントは single-valued または multi-valued の場合があり、デフォルトは multi-valued です。この制限を適用するのは、エンタイトルメントのクライアントの作業です。

<!ELEMENT value (#PCDATA)>

エンタイトルメント値は、入力されない文字列です。

<!ELEMENT query-app (query-xml, result-set)>

値が (電子メール配布リストなどの) 外部アプリケーションから生成された場合、<query-xml> 要素を介してアプリケーションクエリを指定する必要があります。<result-set> 要素を介してクエリから結果を抽出します。では、この 2 つの例を示しています。190 ページの 「例 2: アプリケーションクエリエンタイトルメント : 外部クエリ」

<!ELEMENT query-xml ANY>

XML クエリは XDS 形式です。<query-xml> コマンドは、接続されたアプリケーションからオブジェクトを検索したり読み取るために使用されます。DirXML ルール、オブジェクトの移行などの機能は、ドライバのクエリコマンドの実装内容に依存します。XML クエリの詳細については、Novell のクエリに関する開発者用ドキュメント (http://developer.novell.com/ndk/doc/dirxml/dirxmlbk/ref/ndsdtd/query.html) を参照してください。

<!ELEMENT result-set (display-name, description, ent-value)> <!ELEMENT display-name(token-attr | token-src-dn | token-association)> <!ELEMENT ent-value (token-association | token-src-dn | token-attr)> <!ELEMENT description (token-association | token-src-dn | token-attr)> <!ELEMENT token-association EMPTY> <!ELEMENT token-attr EMPTY> <!ATTLIST token-attr attr-name CDATA #REQUIRED

外部アプリケーションクエリの結果を解釈するには、結果セットの要素を使用します。対象となるデータは、値の表示名 (display-name 子要素)、値の説明 (description 子要素)、および文字列のエンタイトルメント値 (ent-value 子要素。これは表示されません) の 3 つです。

token 要素の <token-src-dn>、<token-association>、<token-attr> は、実際は、src-dn 属性値、関連付けの値、または任意の属性値を、XDS 形式の XML ドキュメントからそれぞれ抽出する、XPATH 式のプレースホルダです。DTD では、クエリ結果が XDS であることが想定されています。

DTD の他のヘッダ

エンタイトルメント DTD の残りのエンタイトルメントのヘッダは異なる機 \'94\'5c を持っていますが、エンタイトルメントを作成するときに注目する必要がある項目ではありません。

<!-- DirXML-EntitlementRecipient または DirXML-SharedProfile オブジェクトの DirXML-EntitlementRef 属性に格納されているエンタイトルメント参照。-->

DTD のエンタイトルメント参照の部分に保存された情報は、エンタイトルメントオブジェクトを指します。この情報は、(役割ベースエンタイトルメントドライバ、Entitlement.xml、または認証フロードライバ、UserApplication.xml などの) 管理エージェントによって配置されます。これは、接続システムで発生するアクションのトリガイベントです。このヘッダの DTD では何もする必要はありませんが、エンタイトルメントオブジェクトが参照されることを確認するためにこの情報を使用できます。

<!-- DirXML-EntitlementRecipient オブジェクトの DirXML-EntitlementResult 属性に格納されているエンタイトルメントの結果。-->

エンタイトルメントの結果部分は、エンタイトルメントが付与されたかまたは取り消されたかに関する結果をレポートします。情報には、イベントの状態またはステータス、およびいつイベントが付与または取り消されたのか (タイムスタンプで表示) が含まれています。このヘッダの要素および属性では、何もする必要はありません。

<!-- DirXML-Entitlement オブジェクトの DirXML-SPCachedQuery 属性に格納されているキャッシュされたクエリの結果。-->

エンタイトルメントのクエリ部分には、外部アプリケーションから収集されたエンタイトルメント値が含まれています。エンタイトルメントのクライアントでこの情報を表示する必要がある場合、この情報は再度使用できます。これらの値は、エンタイトルメントオブジェクトの DirXML-SPCachedQuery 属性に保存されています。このヘッダの要素および属性では、何もする必要はありません。

<!-- DirXML スクリプト内、および XDS ドキュメントの操作の operation-data 内の DirXML-EntitlementRef 表現。-->

DTD では複数のドキュメントの値が定義されるため、この EntitlementRef 部分は、実際にはエンタイトルメント定義の一部ではありません。このヘッダの要素および属性では、何もする必要はありません。

6.4.4 Designer を介したエンタイトルメントの作成

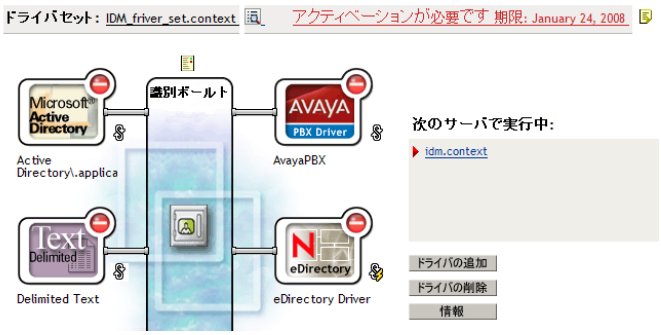
187 ページのセクション 6.4.5「iManager でのエンタイトルメントの作成および編集」の例ではエンタイトルメントを記述するための実際の XML コードを示していますが、Identity Manager に付属している Designer ユーティリティを使用すると、エンタイトルメントをより簡単に記述できます。Designer モデラで Identity Manager ドライバを識別ボールトに追加した後、アウトラインビューでドライバを右クリックし、［エンタイトルメントの追加］を選択します。Entitlement Wizard でエンタイトルメントのタイプを指定するように \'95\'5c 示され、ウィザードによりステップごとに作成できます。

エンタイトルメントウィザードの使用の詳細については、『Designer for Identity Manager: Administration Guide』を参照してください。

6.4.5 iManager でのエンタイトルメントの作成および編集

エンタイトルメントの作成には Designer の Entitlement Wizard を使用することをお勧めしますが、iManager を介してエンタイトルメントを作成できます。

1 ［*Identity Manager*］ > ［Identity Manager Overview］の順に選択します。
2 ドライバがある場所でドライバセットを参照し、［*検索*］をクリックします。
3 ［Identity Manager の概要］ページで、ドライバオブジェクトをクリックします。

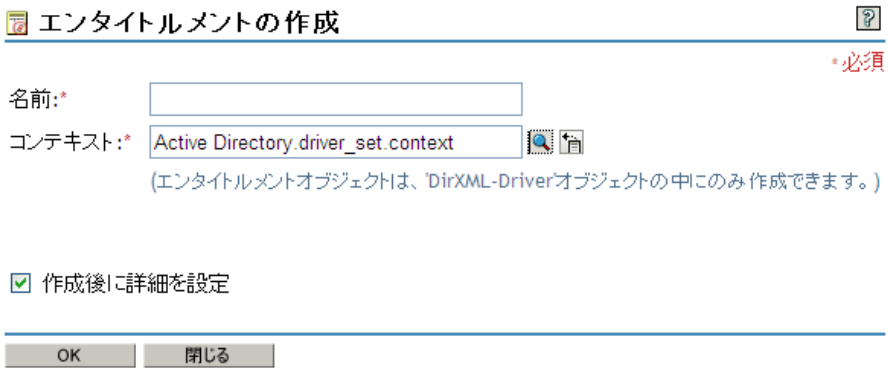


4 ［ドライバの概要］ページで、［*詳細*］をクリックし、［*エンタイトルメント*］をクリックします。

5 ［*挿入*］をクリックして、エンタイトルメントを作成します。
6 エンタイトルメントの名前を指定します。

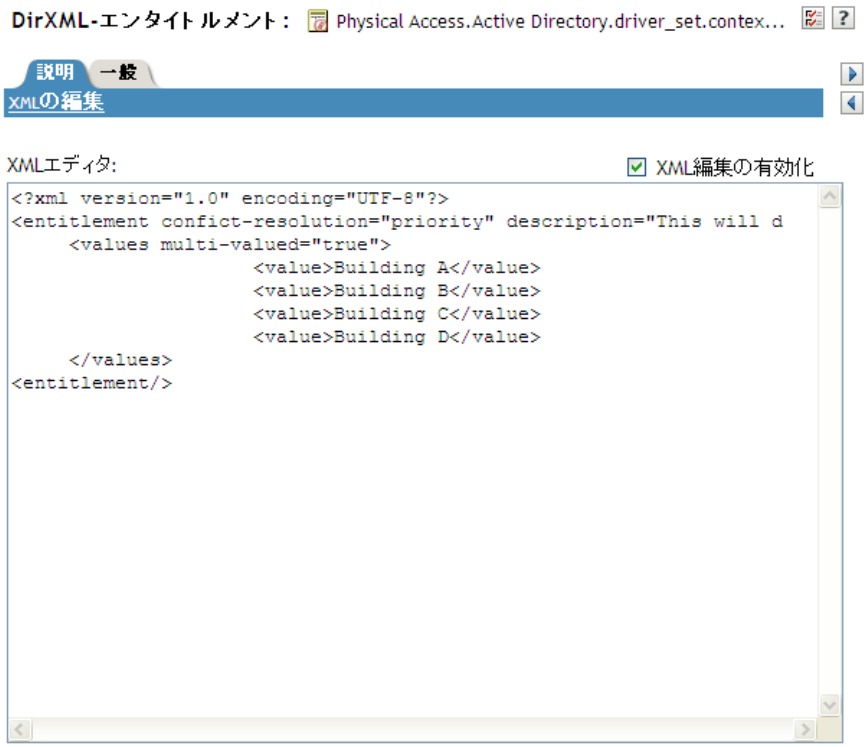
注 : エンタイトルメントの名前は変更しないでください。エンタイトルメント名を後で変更する場合、そのエンタイトルメントを実装しているポリシー内のすべての参照も変更する必要があります。エンタイトルメント名は、ポリシー内の Ref 属性および Result 属性に保存されます。

ドライバオブジェクトが選択されているため、エンタイトルメントのコンテキストはすでに取り込まれています。



7 [*作成後に詳細を設定*] がオンになっていることを確認し、[*OK*] をクリックします。

8 [*XML 編集の有効化*] をオンにして、エンタイトルメントを作成します。



9 エンタイトルメントの作成に関する情報メッセージを読み、[*閉じる*] をクリックします。

6.4.6 独自のエンタイトルメントを作成するためのエンタイトルメントの例

値なしと値ありの 2 種類のエンタイトルメントを作成できます。値のあるエンタイトルメントは、外部クエリ、管理者が定義したリストから、または自由形式で値を取得できます。作成できる 4 つのタイプのエンタイトルメントの例を以下に示します。

注 : 右向きの不等号 (<) の付いていない行がある場合、行はラップされており、情報が 2 行 (または 3 行) ではなく、通常は 1 行に表示されていることを意味します。これらは、アカウントのエンタイトルメント以外は、それぞれのタイプの値のあるエンタイトルメント用に作成できる単なる例です。

例 1: アカウントのエンタイトルメント : 値なし

```
<?xml version="1.0" encoding="UTF-8"?>
<entitlement conflict-resolution="priority"
    description="This is an Account Entitlement"
    display-name="Account Entitlement"/>
```

この例では、値のないエンタイトルメントの名前は「Account」です。この後ろには、デフォルト設定の優先度を持つ conflict-resolution 行があります。これはたいていの場合、エンタイトルメントが役割ベースエンタイトルメントに使用されている場合、優先度を持つ RBE によって値が設定されることを意味します。(しかし、これは値のないエンタイトルメントの例であるため、値のある設定には適用されません)。エンタイトルメントの説明は「This is an Account Entitlement」であり、表示名は「Account Entitlement」です。これが、アカウントのエンタイトルメントを作成するために必要なすべての情報です。これは、アプリケーションでアカウントを付与するために使用できます。

有効化されたエンタイトルメントを持つ Active Directory ドライバには、ユーザアカウントの付与または取り消しのために Active Directory によって使用される UserAccount エンタイトルメントがあります。

```
<?xml version="1.0" encoding="UTF-8"?>
<entitlement conflict-resolution="union"
      description="The User Account entitlement grants or denies an
      account in ActiveDirectory for the user. When granted, the user
      is given an enabled logon account.When revoked, the logon
      account is either disabled or deleted depending on how the drive
      is configured."display-name="User Account Entitlement"
name="UserAccount">
</entitlement>
```

この例では、衝突の解決は Union です。これにより、エンタイトルメントで割り当てられた値をマージできます。(繰り返しますが、値のある設定は値のないエンタイトルメント

には適用されません)。［Description］フィールドでは、このエンタイトルメントの使用目的、および作成理由を説明します。これは、エンタイトルメントを今後変更するユーザにとっては役立つ情報です。管理エージェントには、ユーザアカウントのエンタイトルメントとして <display-name> が \'95\'5c 示されますが、エンタイトルメントの実際の名前は UserAccount です。

例 2: アプリケーションクエリエンタイトルメント : 外部クエリ

有効なエンタイトルメントが設定されている Active Directory ドライバが付属している Group および Exchange メールボックスのエンタイトルメントでは、アプリケーションクエリの例が提供されています。イベントを実行するために接続システムからの外部情報が必要な場合、このエンタイトルメントのタイプを使用します。

```
<?xml version="1.0" encoding="UTF-8"?>
<entitlement conflict-resolution="union"
   description="The Group Entitlement grants or denies membership in
   a group in Active Directory. The group must be associated with a
   group in the Identity Vault. When revoked, the user is removed from
   the group. The group membership entitlement is not enforced on the
   publisher channel: If a user is added to a controlled group in
   Active Directory by some external tool, the user is not removed by
   the driver. Further, if the entitlement is removed from the user
  object instead of being simply revoked, the driver takes no action."
display-name="Group Membership Entitlement" name="Group">
   <values>
      <query-app>
         <query-xml>
            <nds dtd-version="2.0">
               <input>
                  <query class-name="Group"
                     scope="subtree">
                     <search-class class-name="Group"/>
                     <read-attr attr-name="Description"/>
                  </query>
               </input>
            </nds>
         </query-xml>
         <result-set>
            <display-name>
                <token-src-dn/>
            </display-name>
            <description>
               <token-attr attr-name="Description"/>
            </description>
            <ent-value>
               <token-association/>
            </ent-value>
         </result-set>
      </query-app>
   </values>
</entitlement>
```

この例では、エンタイトルメントが複数回同じオブジェクトに適用された場合、グループのエンタイトルメントでは Union を使用して衝突が解決されます。Union 属性により、関

連するすべての Role-Based Entitlement (役割ベースのエンタイトルメント) ポリシーのエンタイトルメントが \'83\'7dージされます。したがって、1 つのポリシーがエンタイトルメントを取り消し、その他のポリシーがエンタイトルメントを付与した場合、最終的にはエンタイトルメントが付与されます。

グループの説明は、ドライバのポリシーのルールを介して何が設定されたかが詳細に説明されているため役立ちます。この説明は、最初にエンタイトルメントを定義するときに、どの程度詳しく説明するのかを知るための良い例です。

<display-name> はグループメンバーシップのエンタイトルメントです。これは役割ベースのエンタイトルメントの iManager などの管理エージェントに表示されます。名前はエンタイトルメントの相対識別名 (RDN) です。\'95\'5c 示名を定義しない場合、エンタイトルメントの名前はその RDN です。

初期のクエリ値により、ツリーのトップでグループのクラス名が検索され、サブツリーも検索されます。これらの値は接続されている Active Directory サーバから取得したものであり、<nds> タグでアプリケーションクエリが開始されます。<query-xml> タグで、次に類似した情報をこのクエリが受信します。

```
<instance class-name="Group" src-dn="o=Blanston,cn=group1">
   <association>o=Blanston,cn=group1</association>
   <attr attr-name="Description"> the description for group1</attr>
</instance>
<instance class-name="Group" src-dn="o=Blanston,cn=group2">
   <association>o=Blanston,cn=group2</association>
   <attr attr-name="Description"> the description for group2</attr>
</instance>
<instance class-name="Group" src-dn="o=Blanston,cn=group3">
   <association>o=Blanston, cn=group3</association>
   <attr attr-name="Description"> the description for group3</attr>
</instance>
<!-- ... ->
```

次に、<result-set> タグで、クエリから受け取った情報が、さまざまなフィールドに入力されます。たとえば、<display-name> フィールドは o=Blanston,cn=group1 を受け取ります。<description> フィールドは the description for group1 を受け取り、<ent-value> フィールドは o=Blanston,cn=group1 を受け取ります。複数のグループが存在し、クエリの条件を満たしたため、この情報も収集され、他のインスタンスとして \'95\'5c 示されました。

注 : 関連付け形式の値はすべての外部システムで一意であるため、問い合わせが行われた各外部システムで形式および \'8d\'5c 文は異なります。

その他の例としては Exchange Mailbox エンタイトルメントがあります。

```
<?xml version="1.0" encoding="UTF-8"?>
<entitlement conflict-resolution="union"
  description="The Exchange Mailbox Entitlement grants or denies an
  Exchange mailbox for the user in Microsoft Exchange."
  display-name="Exchange Mailbox Entitlement" name="ExchangeMailbox">
  <values>
      <query-app>
         <query-xml>
            <nds dtd-version="2.0">
               <input>
                  <query class-name="msExchPrivateMDB"
```

```
                     dest-dn="CN=Configuration," scope="subtree">
                     <search-class class-name="msExchPrivateMDB"/>
                     <read-attr attr-name="Description"/>
                     <read-attr attr-name="CN"/>
                  </query>
               </input>
            </nds>
         </query-xml>
         <result-set>
            <display-name>
               <token-attr attr-name="CN"/>
            </display-name>
            <description>
               <token-attr attr-name="Description"/>
            </description>
            <ent-value>
              <token-src-dn/>
            </ent-value>
         </result-set>
      </query-app>
   </values>
</entitlement>
```

この例では、エンタイトルメントが複数回同じオブジェクトに適用された場合、Exchange メールボックスのエンタイトルメントでは Union を使用して衝突が解決されます。Union 属性により、関連するすべての Role-Based Entitlement (役割ベースのエンタイトルメント) ポリシーのエンタイトルメントが \'83\'7dージされます。したがって、1 つのポリシーがエンタイトルメントを取り消し、その他のポリシーがエンタイトルメントを付与した場合、最終的にはエンタイトルメントが付与されます。

説明には、エンタイトルメントが Microsoft Exchange のユーザの Exchange メールボックスを付与または取り消すことが示されています。エンタイトルメントの詳細としてはこれで十分です。display-name は Exchange メールボックスのエンタイトルメントです。これは役割ベースエンタイトルメントの iManager などの管理エージェントに表示されます。名前はエンタイトルメントの相対識別名 (RDN) です。\'95\'5c 示名を定義しない場合、エンタイトルメントの名前はその RDN です。

初期のクエリ値によって msExchPrivateMDB のクラス名が検索されます。これは、Configuration のコンテナを検索し始め、サブツリーを検索し続ける Microsoft Exchange の機能呼び出しです。これらの値は接続されている Active Directory データベースから取得したものであり、アプリケーションクエリは <nds> タグで開始されます。eDirectory には msExchPrivateMDB のクラスと同等のものがありません。したがって、そのようなクエリを実行する Microsoft Exchange の機能呼び出しに精通している必要があります。しかし、Active Directory ドライバで見つかったルールおよびポリシーがあるため、クエリは完了します。

エンタイトルメントコンシューマでは、クエリによって取得された情報が使用されます。たとえば、エンタイトルメント値 (ent-value) は、DirXML-EntitlementRef 属性を介して Identity Manager ポリシーに渡されます。iManager またはユーザアプリケーションによって \'95\'5c 示名および説明情報が \'95\'5c 示され、DirXML-SPCachedQuery 属性に保存されます。

例 3: 管理者定義のエンタイトルメント : リスト付き

3 番目の例は、リストエントリを選択した後に付与または取り消しのイベントを作成する管理者定義のエンタイトルメントです。

```
<?xml version="1.0" encoding="UTF-8"?>
<entitlement conflict-resolution="union"
    description="This will show Administrator-defined Values">
         <display-name="Admin-defined Entitlement"/>
         <values multi-valued="true">
            <value>Building A</value>
            <value>Building B</value>
            <value>Building C</value>
            <value>Building D</value>
            <value>Building E</value>
            <value>Building F</value>
      </values>
</entitlement>
```

この例では、エンタイトルメント名は、管理者が定義しエンタイトルメントの定義済み表示名を持つ管理者定義です。(エンタイトルメントの RDN とは異なる表示名にする場合のみ、表示名を設定する必要があります)。conflict-resolution の行は Union の設定を表します。これにより、エンタイトルメントは割り当てられた値をマージできます。

エンタイトルメントの説明は「*This will show Administrator-defined Values*」です。multi-value 属性は true に設定されます。これにより、エンタイトルメントで値を複数回割り当てられるようになります。この例では、値は会社のビルの文字「Building A」から「Building F」です。次に、iManager RBE タスクなどのエンタイトルメントのクライアント、またはユーザアプリケーションを介して、ユーザまたは定義されたタスクマネージャはビルの情報を指定できます。これは、Novell eDirectory などの外部アプリケーションに含まれます。

例 4: 管理者定義のエンタイトルメント : リストなし

4 番目の例は、エンタイトルメントでイベントを付与または取り消す前に、値の入力を管理者に強制する管理者定義のエンタイトルメントです。初期の設定ですべての情報を持っていないためにタスクリストを作成できない場合、この種類のエンタイトルメントを使用できます。

```
<?xml version="1.0" encoding="UTF-8"?>
<entitlement conflict-resolution="priority"
    description="There will be no pre-defined list">
    <values multi-valued="false"/>
</entitlement>
```

この例では、エンタイトルメント名は管理者定義 (リストなし) であり、表示名のエントリがないため、表示名としてエンタイトルメント名が使用されます。衝突の解決がデフォルトである優先度に再度設定されます。つまり、役割ベースのエンタイトルメントによってエンタイトルメントが使用された場合、優先度がある RBE によって値が設定されます。iManager RBE タスクなどのエンタイトルメントのクライアントを介して、またはユーザアプリケーションを介して、ビルの情報を指定します。これは、eDirectory などの外部アプリケーションに含まれます。

6.4.7 エンタイトルメントの作成のステップの完了

174 ページのセクション 6.2「エンタイトルメントを作成する : 概要」で説明されているように、エンタイトルメントの作成例には、エンタイトルメントの作成および使用方法についての最初の 2 つのステップが紹介してあります。これには、ステップ 1 であるエンタイトルメントで実行することのチェックリストの作成と、ステップ 2 であるチェックリスト内の項目に対するエンタイトルメントの記述が含まれています。ステップ 3 である、Identity Manager ドライバのポリシーの作成はこの章の範囲外です。ポリシーの作成および編集の詳細については、「*Identity Manager 3.5.1 のポリシーの理解*」、および適切な『Identity Manager ドライバガイド (http://www.novell.com/documentation/idm35drivers/index.html)』を参照してください。

エンタイトルメントを作成した後、または、特定の Identity Manager ドライバで事前設定済みのエンタイトルメントを使用した後は、それらを管理する必要があります。これはステップ 4 です。エンタイトルメントは、2 つのパッケージまたはエージェントによって、つまり役割ベースエンタイトルメントポリシーとしての iManager を介して、またはワークフローベースのプロビジョニングのユーザアプリケーションを介して管理されます。ワークフローベースのプロビジョニングで使用されるエンタイトルメントについては、『*Identity Manager 3.5.1User Application: Administration Guide* 』の「“ プロビジョニング要求定義の設定 ”」を参照してください。この章の残りの部分では、Role-Based Entitlement (役割ベースのエンタイトルメント) に重点を置きます。

6.5 Role-Based Entitlement (役割ベースのエンタイトルメント) の管理の概要

- 195 ページのセクション 6.5.1「エンタイトルメントサービスドライバの機 \'94\'5c 方法」

従来、接続システムのエンタイトルメントはドライバごとに管理され、その方法はポリシービルダで作成するポリシーのようなドライバ設定ポリシーの作成と編集に限られていました。この従来型の分散モデルでは、別の管理者が各 Identity Manager ドライバと接続システムを管理することがほとんどで、システムのリ \'83\'5c ースをユーザが利用できるかどうかを決定するビジネスポリシーは、各接続システムドライバのドライバ設定ポリシーで別々に「ハードコード」されます。

役割ベースエンタイトルメントモデルは、1 人または少数の管理者がエンタイトルメントポリシーを制御する権利を持つ環境に適しています。このような管理者は、Identity Manager 全体を理解している必要がありますが、Role-Based Entitlement インタフェースを使用するために Identity Manager または XSLT または DirXML スクリプトに関する \'8f\'5c 分な専門知識はなくてもかまいません。

条件が一致した場合、役割ベースエンタイトルメントポリシーによりビジネスリソースを自動的に付与または取り消すことができます。エンタイトルメントとは、リソースにアクセスするための許可書のようなものです。許可書があると指定したリソースにアクセスでき、そのような許可書がないとアクセスできません。作業例としては、ユーザが条件 1、2、および 3 を満たさない場合、Role-Based Entitlement (役割ベースのエンタイトルメント) ポリシーを介して、ユーザはグループ H のメンバーになるけれども、ユーザが条件 4 および 5 を満たす場合、ユーザはグループ I のメンバーになることを指定できます。

Role-Based Entitlement (役割ベースのエンタイトルメント) の管理を設定するには、次の 3 つのステップを行います。

1. まだに実行していない場合は、176 ページのセクション 6.2.2「他の Identity Manager ドライバでのエンタイトルメントの有効化」で説明したとおりに、Identity Manager ドライバオブジェクトの DirXML-EntitlementRef 属性を有効にします。
2. 196 ページのセクション 6.6「エンタイトルメントサービスドライバオブジェクトの作成」の説明に従い、エンタイトルメントサービスドライバ (Entitlement.xml) をインストールします。
3. で説明したとおりに、iManager で Role-Based Entitlement (役割ベースのエンタイトルメント) ポリシーを作成します。198 ページのセクション 6.7「Entitlement Policy (エンタイトルメントポリシー) の作成」

6.5.1 エンタイトルメントサービスドライバの機 \'94\'5c 方法

役割ベースエンタイトルメントは、エンタイトルメントサービスドライバ (Entitlement.xml) に依存しています。このドライバは、エンタイトルメントポリシーにユーザがメンバーシップを持っているかどうかを監視するエンジンサービスです。ユーザが Entitlement Policy (エンタイトルメントポリシー) のダイナミックグループのダイナミックメンバーシップ条件に合致するか、またはスタティックに含まれる場合、エンタイトルメントサービスドライバは、ユーザオブジェクトの DirXML-EntitlementRef 属性の情報を更新します。

175 ページのセクション 6.2.1「エンタイトルメントをサポートする、設定済みの Identity Manager ドライバ」に一覧表示してあるシステムについては、Identity Manager ドライバ設定をインポートするときにエンタイトルメントを有効にできます。Identity Manager には、エンタイトルメント、エンタイトルメントを実装するためのポリシー、およびエンタイトルメントアクティビティのリッスンが有効になっているドライバがすでに設定に含まれている、多くのドライバが付属しています。提供されたポリシーをレビューすることができます。これらのポリシーでは、DirXML-EntitlementRef 属性を監視し、エンタイトルメントを付与または取り消すことにより、エンタイトルメントがサポートされています。

次のいずれかが発生した場合のみ、エンタイトルメントサービスドライバによって DirXML-EntitlementRef 属性が更新されます。

- ［Reevaluate Membership］タスクを使用した場合
- ツリーのどの部分でユーザを再評価するかを指定した場合
- ユーザが移動した場合
- ユーザが名前変更された場合
- Entitlement Policy (エンタイトルメントポリシー) のメンバーシップに使用される属性が変更された場合

エンタイトルメントポリシーを使用すると、接続システム上のエンタイトルメントおよび識別ボールトでの権限を付与できます。接続システムのエンタイトルメントは、次のとおりです。

- アカウント
- 電子メール配布リストのメンバーシップ
- グループメンバーシップ
- 指定した値が入力された、接続システムで対応するオブジェクトの属性

- Placement (配置)
- その他のカスタ \'83\'7d イズ可 \'94\'5c なエンタイトルメント

エンタイトルメントで作成できるいくつかのオプションについて、有効化されたエンタイトルメントを持つドライバ設定で示しています。

各ドライバセットで使用するエンタイトルメントサービスドライバは 1 つであるため、エンタイトルメントポリシーが管理できるのは、ドライバセットに関連付けられているサーバ上の読み書き可能レプリカまたはマスタレプリカに含まれるユーザだけです。

役割ベースエンタイトルメントポリシーの機能は、Identity Manager に基づいています。したがって、接続システムを管理するには、Identity Manager ドライバをインストールして適切に設定し、Identity Manager プラグインをインストールする必要があります。

Entitlement Policy の割り当てと Identity Manager ドライバ設定との間に衝突が発生するのを回避するため、ビジネスポリシーと、それが Identity Manager でどのように管理されているかに注意してください。Identity Manager の Entitlement Policy (エンタイトルメントポリシー) およびドライバ設定のポリシーは、属性を管理している間は重複または衝突することはできません。

6.6 エンタイトルメントサービスドライバオブジェクトの作成

エンタイトルメントポリシーを作成するには、エンタイトルメントサービスドライバオブジェクトが必要です。ドライバセットごとに 1 つ作成する必要があります。

オブジェクトがない場合は、［Role-Based Entitlement］の役割およびタスクをクリックした際に、エンタイトルメントサービスドライバオブジェクトを作成するようプロンプトが \'95\'5c 示されます。

1 エンタイトルメントサービスドライバがすでにあるかどうかを調べます。

  iManager で［*役割ベースエンタイトルメント*］>［*役割ベースエンタイトルメント*］の順にクリックし、ドライバセットを選択して［*OK*］をクリックします。

  - ［No Entitlements Service Driver］ページが \'95\'5c 示された場合は、ステップ 2 に進み、エンタイトルメントサービスオブジェクトを作成します。
  - エンタイトルメントポリシーのリストがある［役割ベースエンタイトルメント］ページが表示された場合、エンタイトルメントサービスドライバオブジェクトはすでに存在しています。このプロシージャを実行する必要はありません。198 ページのセクション 6.7「Entitlement Policy (エンタイトルメントポリシー) の作成」に進みます。

2 ［No Entitlements Service Drive］ページで、［*Yes*］をクリックします。

  Create Driver Wizard が開きます。

  [*Identity Manager ユーティリティ*］>［*インポート環境設定*］の順にクリックすることもできます。

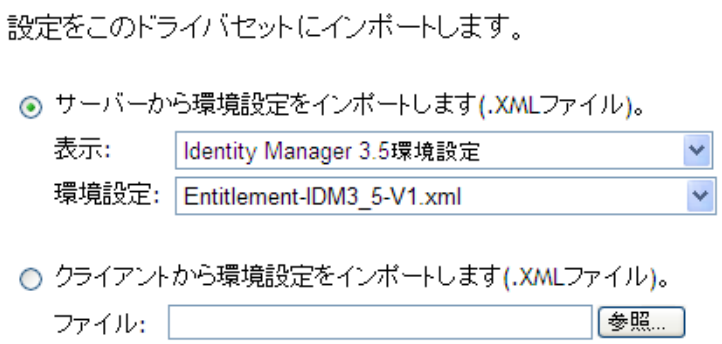
3 ［ドライバの作成ウィザード］ページで、［*既存のドライバセットの中*］を選択し、［*次へ*］をクリックします。

4 ［*サーバから環境設定をインポートします (.XML ファイル)*］ドロップダウンリストで、ドライバ環境設定のソート方法を選択します。

  - すべての環境設定

- Identity Manager 3.5 環境設定
- Identity Manager 3.0 環境設定
- IDM バージョンに関連付けられていない環境設定

5 *Entitlement-IDM3_5-V1.xml* を選択し、［*次へ*］をクリックします。



6 エンタイトルメントサービスドライバオブジェクトの名前を指定し (またはデフォルトの名前を受け入れ)、［*次へ*］をクリックします。

正しいドライバ設定ファイルは、自動的に選択されます。

7 同等セキュリティを定義するか、管理の役割を除外することをお勧めします。これらの両方に対して Admin ユーザを追加し、［*Next*］*をクリックします。*

8 サ \'83\'7d リをレビューし、［*Finish*］*をクリックします。*

エンタイトルメントドライバのドライバシムは、Identity Manager をインストールしたときにデフォルトでインストールされます。エンタイトルメントドライバ設定ファイルは、iManager サーバに Identity Manager プラグインをインストールする際にデフォルトでインストールされます。

ウィザード完了後、エンタイトルメントのプラグインにアクセスし、このドライバセットに対して Role-Based Entitlement (役割ベースのエンタイトルメント) ポリシーの作成を開始できます。

重要 : エンタイトルメントサービスドライバをホストするドライバセットが、複数のサーバに割り当てられている場合、エンタイトルメントサービスドライバは、それらのサーバの 1 つでのみ有効にする必要があり、一度に複数のサーバで有効にすることはできません。その他の設定はサポートされていません。

iManager 内のエンタイトルメントサービスドライバを含むドライバセットに複数のサーバを追加することができますが、iManager の役割ベースエンタイトルメントのプラグインにより、ドライバセットが複数のサーバに割り当てられているかどうかがチェックされ、割り当てられている場合は設定エラーメッセージが表示されます。他の方法 (LDAP 呼び出しなど) ではそのような設定エラーメッセージは表示されませんが、サポートされ

ている唯一の設定は、エンタイトルメントサービスドライバを 1 つのサーバに関連付ける設定です。

6.7 Entitlement Policy (エンタイトルメントポリシー) の作成

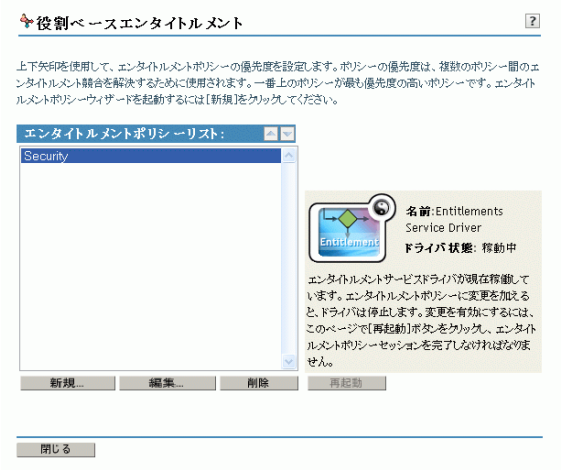
- 202 ページのセクション 6.7.1「Entitlement Policy (エンタイトルメントポリシー) のためのメンバーシップの定義」
- 203 ページのセクション 6.7.2「Entitlement Policy (エンタイトルメントポリシー) のためのエンタイトルメントの選択」

Entitlement Policy (エンタイトルメントポリシー) を作成するには、提供されるウィザードを使用します。

1. エンタイトルメントサービスドライバが設定されていること、および必要なドライバ設定が作成されていることを確認します。
2. iManager で、［*Role-Based Entitlements*］>［*Role-Based Entitlements*］*の順にクリックします。*
3. ドライバセットを選択します。

   Entitlement Policy (エンタイトルメントポリシー) は、ドライバセットごとに設定します。

   既存のエンタイトルメントポリシーのリストが、次の図に示されているページのように開きます。初めて Role-Based Entitlement (役割ベースのエンタイトルメント) を使用する場合は、リストに \'95\'5c 示されるポリシーはありません。



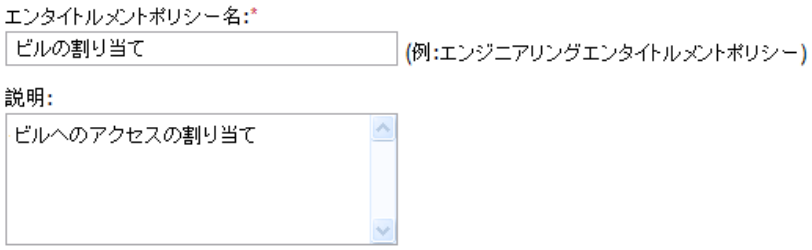
4. *［新規］*をクリックします。

   *エンタイトルメントポリシー*ウィザードが開きます。

   注 : 新しいエンタイトルメントポリシーを作成すると、エンタイトルメントサービスドライバが停止します。ポリシーの作成が完了したら、［*再起動*］をクリックする必要があります。

5. ウィザードのステップ 5a からステップ 5f に従い、新しいポリシーを作成します。ウィザードの各ステップについては、オンラインヘルプを参照してください。

5a ポリシーの名前と説明を指定して、［*次へ*］をクリックします。



5b 検索パラメータを定義して、ダイナミックメンバーシップフィルタを定義します。

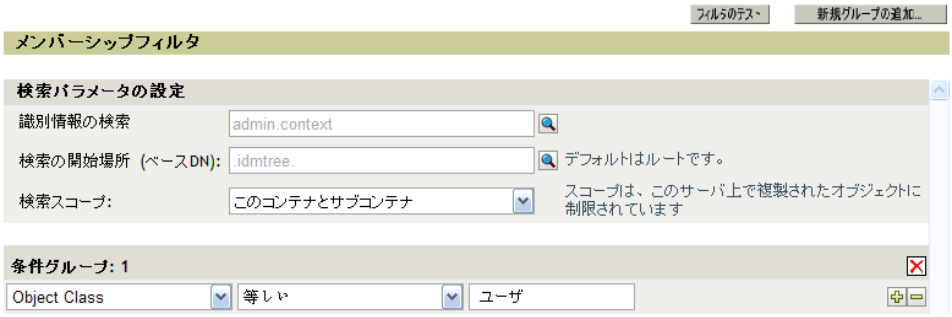
5b1 検索を実行する権限があるユーザを指定します。

5b2 検索を開始する場所を指定します。

5b3 検索のスコープを指定します。

5b4 フィルタ条件を定義して、［*次へ*］をクリックします。

条件により、エンタイトルメントポリシーのメンバーであるユーザが判断されます。



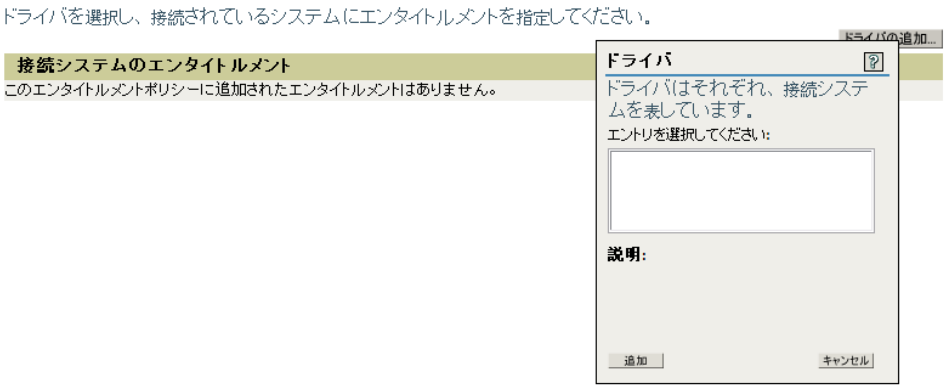
5c 検索条件にメンバーを含めるまたは条件からメンバーを除外して、スタティックメンバーを定義して、［*次へ*］をクリックします。

5d ポリシーのエンタイトルメントと値を定義します。

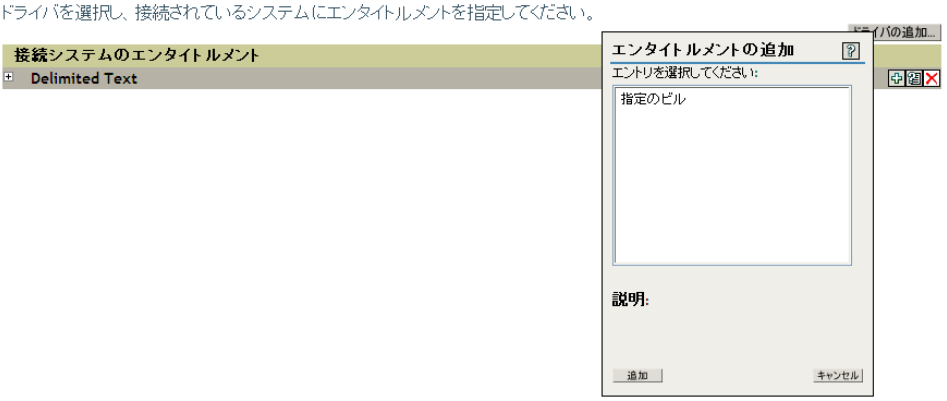
5d1 [*ドライバの追加*] をクリックして、含める Identity Manager ドライバと要素を選択します。

エンタイトルメントは 179 ページのセクション 6.4「iManager を介した XML でのエンタイトルメントの記述」で作成しました。

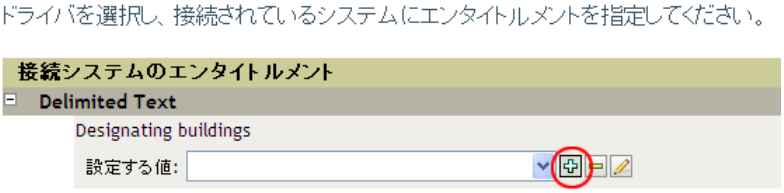
5d2 エンタイトルメントが設定されているドライバを参照して選択し、[*追加*] をクリックします。



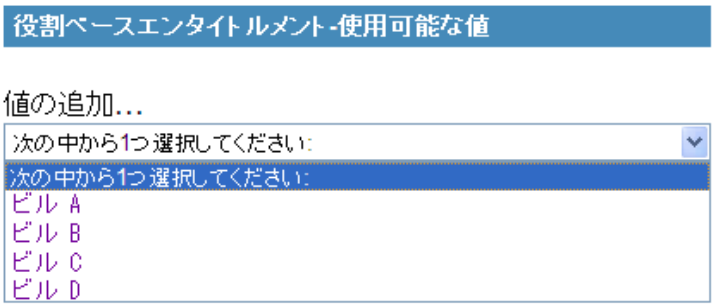
5d3 エンタイトルメントを選択して、[*追加*] をクリックします。



5d4 プラス [+] アイコンをクリックして、エンタイトルメントの値を定義します。



5d5 希望する値を選択して、[*OK*] をクリックします。

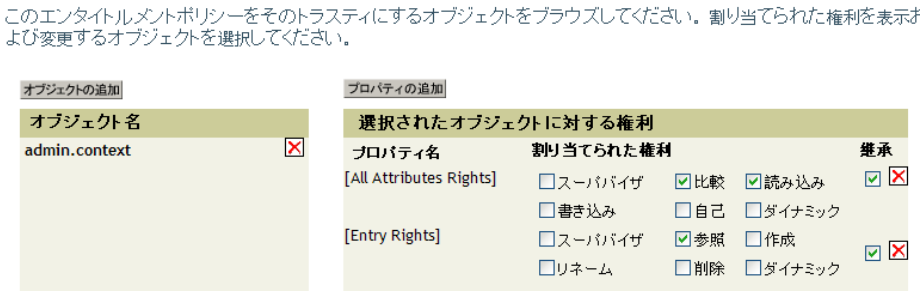


5d6 ［*次へ*］をクリックします。

5e このエンタイトルメントポリシーをトラスティにするオブジェクトを参照します。

5e1 ［*オブジェクトの追加*］をクリックしてオブジェクトを参照して、［*OK*］をクリックします。

5e2 オブジェクトを選択して、［*プロパティの追加*］をクリックします。



5e3 希望するプロパティを定義して、［*次へ*］をクリックします。

5f サマリを読み、実行したい内容がエンタイトルメントポリシーで行われることを確認します。確認後問題なければ［*Finish*］*をクリックし、問題があれば*［Back］をクリックします。

6 ［*Restart*］*をクリックしてセッションを完了します。*

Entitlement Policy (エンタイトルメントポリシー) の作成により、エンタイトルメントサービスドライバがオフになります。

6.7.1 Entitlement Policy (エンタイトルメントポリシー) のためのメンバーシップの定義

Identity Manager ドライバと同様、各エンタイトルメントポリシーが管理できるのは、割り当てられたサーバ上のマスタレプリカまたは読み書き可能レプリカに存在するオブジェクトだけです。各 Entitlement Policy (エンタイトルメントポリシー) は、特定のサーバに割り当てられている 1 つのドライバセットオブジェクトに関連付けられます。

エンタイトルメントポリシーのメンバーになることができるのは、ユーザオブジェクト、およびユーザのクラスに基づく他のオブジェクトタイプだけです。エンタイトルメントポリシーの［メンバーシップ］ページを表示するには、［*役割ベースエンタイトルメント*］>［*役割ベースエンタイトルメント*］の順に選択し、エンタイトルメントポリシーリストから編集するエンタイトルメントポリシーを強調表示し、［*編集*］を選択します。Internet Explorer ブラウザでは［*Membership*］*タブを選択します。Firefox ブラウザではプルダウンメニューから［Edit Dynamic Members］を選択します。*

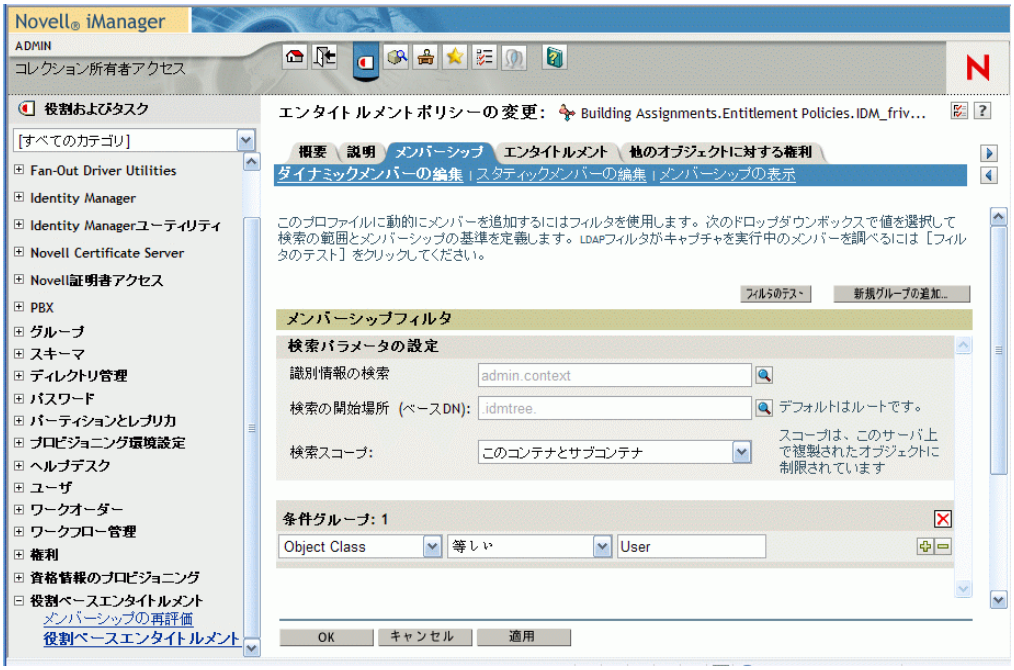
エンタイトルメントポリシーは、ダイナミックグループオブジェクトです。エンタイトルメントポリシーのメンバーシップは、ダイナミックおよびスタティックの 2 つの方法で定義できます。同じエンタイトルメントポリシーで、この両方の方法を使用できます。

- **ダイナミック：** 役職名に「マネージャ」という語が含まれるかなど、オブジェクトの属性値に基づき、メンバーシップの条件を定義できます。指定する条件は、LDAP フィルタに変換されます。

  条件に一致するユーザは自動的にエンタイトルメントポリシーの一部になります。各ユーザを個別にポリシーに追加する必要はありません。ダイナミックメンバーシップは、ダイナミックグループオブジェクトと同様です。

  オブジェクトが変更されダイナミックメンバーシップの条件に合致しなくなった場合は、エンタイトルメントは自動的に取り消されます。

図 6-2 *ダイナミックメンバーおよびスタティックメンバーの編集*



- **スタティック** - ダイナミックメンバーシップの条件 (LDAP フィルタ) の作成に加え、特定のユーザを含めたり、除外したりすることができます。

  フィルタの条件に一致しないメンバーは、スタティックに追加できます。フィルタの条件に合致していても、Entitlement Policy (エンタイトルメントポリシー) に含める必要がないメンバーは除外できます。

注 : [*役割ベースエンタイトルメント*] > [*メンバーシップの再評価*] オプションの順にクリックして再評価を実行し、エンタイトルメントサービスドライバを停止した場合、ドライバを再起動後に、再評価処理を開始できます。

6.7.2 Entitlement Policy (エンタイトルメントポリシー) のためのエンタイトルメントの選択

- 203 ページの 「接続システムのアカウント」
- 204 ページの 「電子メール配布リストおよび NOS リストのメンバーシップ」
- 205 ページの 「接続システムの属性値」

エンタイトルメントを使用すると、接続システム上のサービスおよび識別 \'83\'7bールトの権利へのアクセスを付与または取り消すことができます。

インストールするエンタイトルメントが有効なドライバには、エンタイトルメントポリシーを使用して割り当てることができるエンタイトルメントのリストが付属しています。エンタイトルメントポリシーで使用できる、独自のエンタイトルメントを作成できます。ドライバが提供できるエンタイトルメントは、ドライバの子オブジェクトです。これは、ドライバおよび接続システムの機 \'94\'5c を示すためにドライバ開発者が作成するものです

識別ボールト内のオブジェクトに対するトラスティ権は、エンタイトルメントポリシーのメンバーにただちに付与されます。デフォルトでは、次に Entitlement Policy (エンタイトルメントポリシー) メンバーシップに使用される属性が変更されたとき、またはユーザが別のコンテナに移動されたり名前変更されたりしたときに、接続システムのエンタイトルメントが Entitlement Policy (エンタイトルメントポリシー) の各メンバーに付与されます。

接続システムのエンタイトルメントは、次のとおりです。

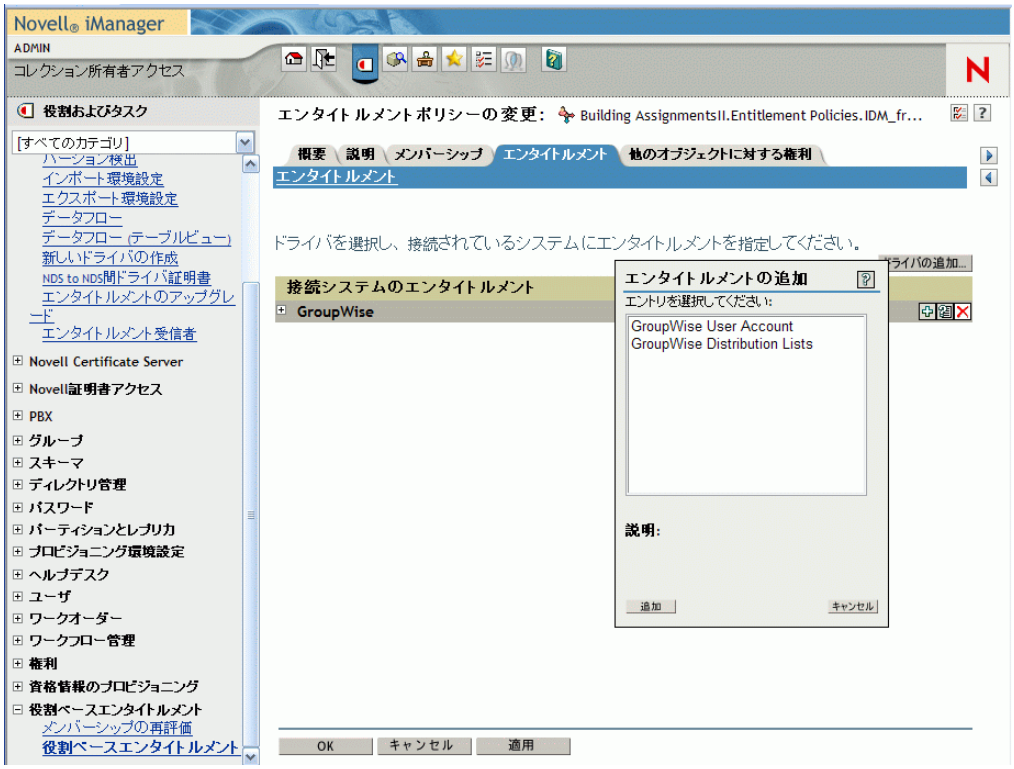
- アカウント
- 電子メール配布リストのメンバーシップ
- NOS リストのグループメンバーシップ
- 指定した値が入力された、接続システムで対応するオブジェクトの属性
- その他のカスタ \'83\'7d イズ可 \'94\'5c なエンタイトルメント

接続システムのアカウント

エンタイトルメントポリシーにエンタイトルメントを追加するには、[エンタイトルメント] ページに移動してドライバを選択します。ドライバが提供するエンタイトルメントを示すポップアップウィンドウが \'95\'5c 示されます。

たとえば、次の \'90\'7d は、GroupWise ドライバにより 2 種類のエンタイトルメントが提供され、リストの先頭に [GroupWise User Account] が \'95\'5c 示されていることを示します。

図 6-3 エンタイトルメントを定義するインタフェース



電子メール配布リストおよび NOS リストのメンバーシップ

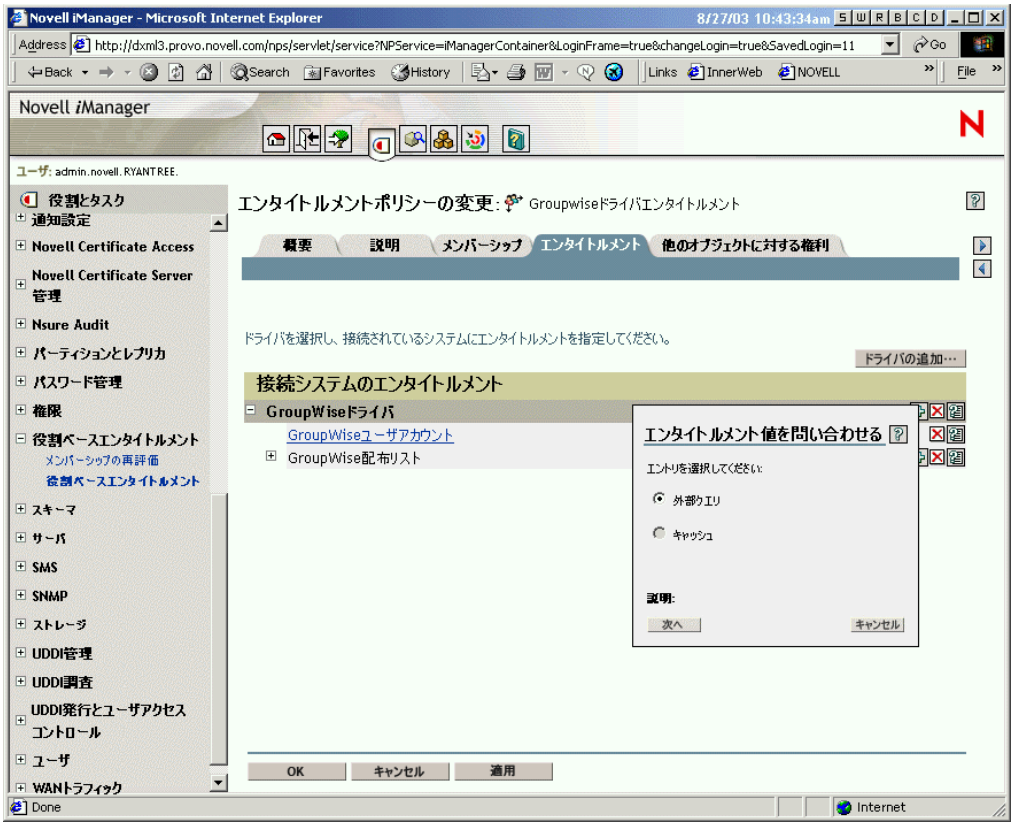
接続システム上のグループにメンバーシップを割り当てるには、ドライバが提供するエンタイトルメントのリストからメンバーシップエンタイトルメントを選択します。

次の \'90\'7d は、［GroupWise Distribution Lists］がリストの 2 番目に \'95\'5c 示されている例を示します。

図 6-4 GroupWise 配布リストの選択

この例で［GroupWise Distribution Lists］を選択した場合、次の \'90\'7d の例のようなクエリポップアップが \'95\'5c 示されます。

図 6-5 エンタイトルメントのクエリ



エンタイトルメントポリシーインタフェースを使用すると、電子メール配布リストまたは NOS リストを問い合わせることができます。クエリが実行された後、キャッシュされたリストを \'95\'5c 示するよう選択できます。

ドライバは完全なリストを返すように設定されているので、接続システムに存在するリストから選択できます。

注 : 完全なリストを返すクエリではなく、指定したグループ名にリストを制限するようドライバをカスタ \'83\'7d イズできます。

接続システムの属性値

接続システムのユーザアカウントには、属性値を割り当てられます。このインタフェースにより、ユーザアカウントに割り当てる値を入力できます。

次の \'90\'7d は、Notes の属性 Department に属性値を追加する例を示します。

図 6-6 属性値の追加

6.8 Role-Based Entitlement (役割ベースのエンタイトルメント) ポリシー間での衝突解決

- 206 ページのセクション 6.8.1「衝突の概要」
- 208 ページのセクション 6.8.2「各エンタイトルメントの衝突の解決方法の変更」
- 209 ページのセクション 6.8.3「Entitlement Policy (エンタイトルメントポリシー) の優先度の設定」

6.8.1 衝突の概要

Entitlement Policy (エンタイトルメントポリシー) を作成する場合、特定のユーザに影響を与えるポリシーがそのユーザへのエンタイトルメントの割り当てと衝突する可 \'94\'5c性があります。

このような衝突の解決方法を、次に説明します。一部のエンタイトルメントについては、衝突の解決を変更できます。

- **値のないエンタイトルメントが付加された場合。**多くの場合、アカウントのエンタイトルメントには値がありません。ユーザがエンタイトルメントポリシーによって接続システムのアカウントを付与される場合、ユーザはその接続システムのアカウントを受け取ります。別の Entitlement Policy (エンタイトルメントポリシー) が衝突するかどうかは関係なく、結果が付加されます。

  これは常に正しく、アカウント付与についての衝突の解決方法は変更できません。

  値のないエンタイトルメントは、照明のスイッチに例えることができます。「オン」または「オフ」、付与されたか付与されないかです。

  たとえば、「\'83\'7d ネージャ Entitlement Policy (エンタイトルメントポリシー)」によって Jean Chandler 氏に Exchange アカウントが付与されるにもかかわらず、Jean Chandler 氏が、同様に Exchange アカウントを付与する「メールルーム従業員 Entitlement Policy (エンタイトルメントポリシー)」からは除外されている場合、Jean 氏は Exchange アカウントを取得できます。

- **値のあるエンタイトルメントがデフォルトで付加されるが、優先度に従って解決するよう選択できる場合 -** グループメンバーシップなどのエンタイトルメントには、値、または値のある属性のグループ名のリストがあります。デフォルトでは、この種類のエンタイトルメントも付加できます。

  必要に応じて、この種類のエンタイトルメントの衝突の解決を変更できます。

  - **conflict-resolution=“union”—**「union」という値は、エンタイトルメントが付加可能であることを意味します。ユーザには、ポリシーのメンバーシップにより割り当てられているすべてのエンタイトルメントが付与されます。異なるエンタイトルメント値は単に追加され、ユーザはそれらすべてを取得します。

    たとえば、Jameel 氏が、「トレードショーメーリングリスト」という GroupWise の電子メール配布リストのメンバーシップを付与する「トレードショーコントラクタポリシー」のメンバーであり、「トレードショーメーリングリスト」という電子メール配布リストも割り当てる「トレードショー \'83\'7d ネージャポリシー」のメンバーシップから除外されている場合でも、電子メール配布リストのメンバーシップが引き続き付与されます。

    別の例を挙げると、メールルームポリシーにより、「メールルームスタッフ」という Active Directory グループのメンバーシップが Consuela 氏に付与され、緊急ボランティアポリシーによる「緊急対応」という Active Directory グループのメンバーシップも付与されている場合、Consuela 氏には Active Directory 内の両グループのメンバーシップが付与されます。

    この設定では、ポリシーのリスト内の Entitlement Policy (エンタイトルメントポリシー) の順序は、エンタイトルメントについては重要ではありません。

  - **conflict-resolution=“priority”—**「priority」という値は、2 つの異なるポリシー間の値が衝突した場合、または 1 つのポリシーに含まれるユーザが別のポリシーでは除外されている場合、そのユーザに付与されるエンタイトルメントは、Entitlement Policy (エンタイトルメントポリシー) のリストでより上位に記述されている Entitlement Policy (エンタイトルメントポリシー) のエンタイトルメントのみになることを意味します。

    前の例は、この設定では別の結果となります。

    前の Jameel 氏の例では、GroupWise の電子メール配布リストのエンタイトルメントが「priority」という値を持ち、「トレードショー \'83\'7d ネージャポリシー」

が「トレードショーコントラクタポリシー」より上位にリスト \'95\'5c 示される場合、「トレードショーメーリングリスト」のメンバーシップは、Jameel 氏に付与されません。

前の Consuela 氏の例では、Active Directory NOS グループメンバーシップのエンタイトルメントが「priority」という値を持ち、メールルームポリシーが緊急ボランティアポリシーよりリスト内で上位にある場合、Consuela 氏にはメールルームスタッフグループのメンバーシップのみが付与されます。衝突の解決が付加ではなく優先度によって設定されているため、緊 \'8b\'7d 対応グループのメンバーシップは付与されません。

たとえば、役割ベースエンタイトルメントを使用して別のシステムの階層構造にユーザを配置するように環境を設定する場合には、この機能が役立ちます。ユーザは任意の 1ヶ所に配置でき、同時に 2ヶ所に配置することはできません。

設定は、ドライバごとに提供される各エンタイトルメントとは関係ありません。

原則として、「priority」の設定を使用する場合、管理者またはマネージャのポリシーは、エンドユーザや個々の貢献者のポリシーよりリスト内で上位に配置する必要があります。広いメンバーシップを持つグループは、狭いメンバーシップを持つグループより上位に配置することをお勧めします。

6.8.2 各エンタイトルメントの衝突の解決方法の変更

1. iManager で、［*Identity Manager*］>［*Identity Manager Overview*］*の順にクリックし、ドライバセットを選択します。*
2. ［ドライバ］状態ボタンをクリックし、［*ドライバの停止*］を選択します。
3. 変更するエンタイトルメントを提供するドライバのドライバアイコンをクリックします。
4. ［ドライバの概要］ページで、［*詳細*］をクリックし、［*エンタイトルメント*］をクリックします。

5. エンタイトルメント名をクリックして、XML ビューアでエンタイトルメントを編集します。
6. ［*Enable XML editing*］*チェック \'83\'7b ックスをオンにします。*
7. XML で、変更するエンタイトルメントの定義を検索します。

   たとえば、次の行を検索します。

```
<entitlement conflict-resolution="union" description="Grants
membership to GroupWise Distribution lists" display-name="GroupWise
Distribution Lists" name="gwDistLists">
```

8 conflict-resolution の値を変更します。次の 2 つの値を指定できます。

```
conflict-resolution="union"
conflict-resolution="priority"
```

これらの値の詳細については、206 ページの 「Role-Based Entitlement (役割ベースのエンタイトルメント) ポリシー間での衝突解決」を参照してください。

9 ［*OK*］をクリックし、変更を保存します。

10 ［*概要*］タブをクリックして、ドライバアイコンにアクセスします。

11 ［*再起動*］をクリックしてドライバを再起動します。

12 ［*Identity Manager の概要*］をクリックして、エンタイトルメントサービスドライバを参照して再起動します。

6.8.3 Entitlement Policy (エンタイトルメントポリシー) の優先度の設定

デフォルトでは、エンタイトルメントポリシーのリスト内の順序に意味はありません。これは、Identity Manager に付属のドライバには、各エンタイトルメントの衝突の解決方法として conflict-resolution="union" が設定されているためです。

任意のエンタイトルメントを conflict-resolution="priority" に変更した場合、エンタイトルメントポリシーのリスト内の順序は意味を持ちますが、対象となるのは変更したエンタイトルメントのみです。これらの値の詳細については、206 ページの 「Role-Based Entitlement (役割ベースのエンタイトルメント) ポリシー間での衝突解決」を参照してください。

エンタイトルメントポリシーの順序を変更するには、エンタイトルメントポリシーのリストの横にある矢印ボタンを使用します。リスト内の最初のポリシーは、優先度が最も高いことを示します。

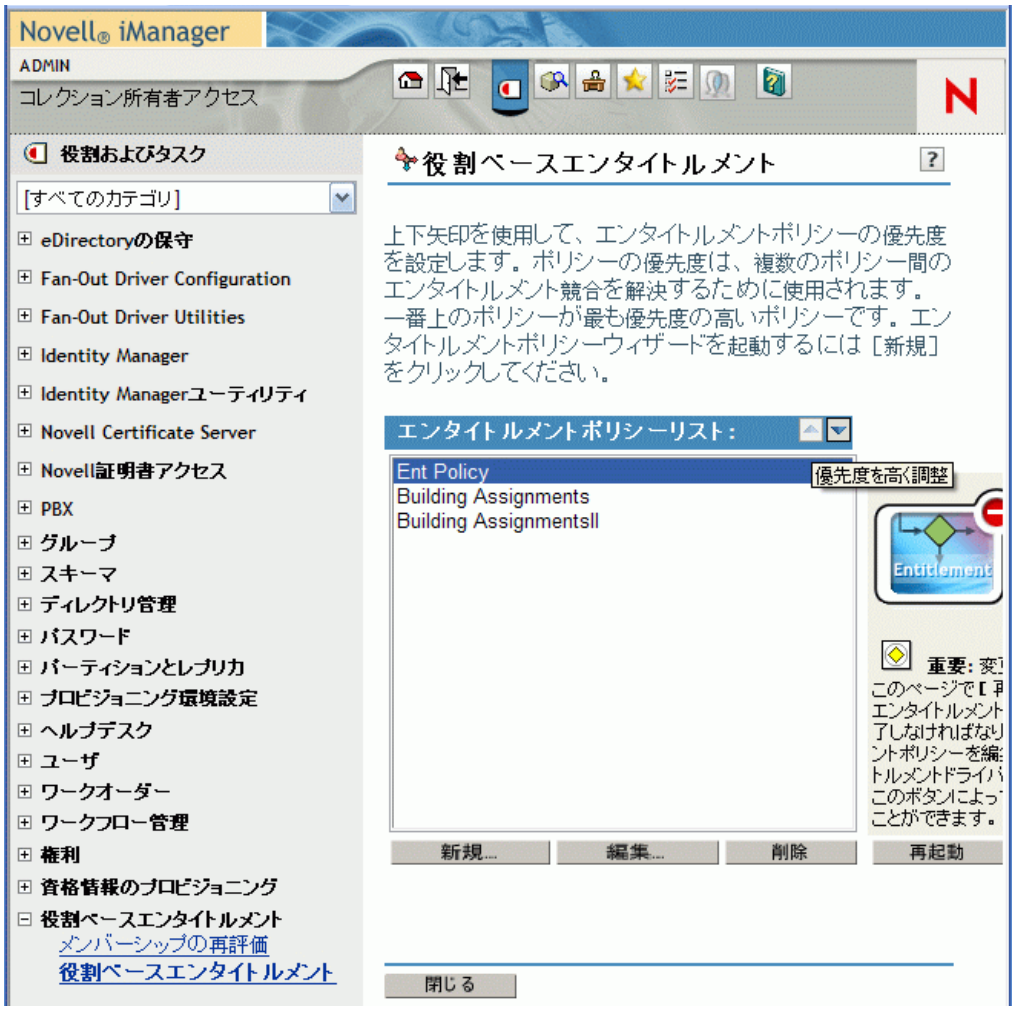
1 iManager で、［*Role-Based Entitlements*］> ［*Role-Based Entitlements*］*の順にクリックします。*

2 ドライバセットを検索して選択します。

Entitlement Policy (エンタイトルメントポリシー) のリストを示すページが \'95\'5c 示されます。

3 矢印 \'83\'7b タンを使用してポリシーをリスト内で上下に移動し、Entitlement Policy (エンタイトルメントポリシー) の優先度を変更します。

Entitlement Policy (エンタイトルメントポリシー) をリストの最上位に移動すると、最も高い優先度が与えられます。



4 ［*Close*］*をクリックしてドライバを再起動します。*

優先度の変更は、ドライバを再起動するまでは有効になりません。

6.9 Role-Based Entitlement (役割ベースのエンタイトルメント) のトラブルシューティング

トラブルシューティングに際しては、次のことに注意してください。

- ポリシーがリストされているページで［*新規*］、［*編集*］、または［*削除*］をクリックしてポリシーを変更すると、*エンタイトルメントサービスドライバ*は停止します。同じページで［*Restart*］*をクリックするまで、ドライバは再起動しません。*

  この機 \'94\'5c は、ポリシーに対する変更が完了していない間は、ドライバが運用環境でエンタイトルメントを付与または取り消しするのを回避するためです。
- 同様に、エンタイトルメントサービスドライバは、同時に複数のユーザが Entitlement Policy (エンタイトルメントポリシー) を編集している可 \'94\'5c 性がある場合は、起動しません。
- 各ドライバセットで使用されるエンタイトルメントサービスドライバは 1 つであるため、エンタイトルメントポリシーが管理できるのは、ドライバセットに関連付けられ

ているサーバ上の読み書き可能レプリカまたはマスタレプリカに含まれるユーザだけです。

6.10 Role-Based Entitlement (役割ベースのエンタイトルメント) およびワークフローベースのプロビジョニングのエンタイトルメントに適用されるエンタイトルメント要素

以下の情報は、特定の実装だけでなく、すべてのエンタイトルメントに適用されます。

- 211 ページのセクション 6.10.1「エンタイトルメントの付与または取り消しのの意味の制御」
- 211 ページのセクション 6.10.2「データの損失の回避」
- 212 ページのセクション 6.10.3「パスワード同期およびエンタイトルメント」

6.10.1 エンタイトルメントの付与または取り消しのの意味の制御

エンタイトルメントの付与または取り消しの結果は、制御できます。各ドライバには、「付与」または「取り消し」の意味を制御するサポートオプションのリストが提供されています。

たとえば、GroupWise アカウントを追加する場合、付与によって実際には無効な状態のアカウントがユーザに付与されるという意味になるよう指定できます。これにより、ユーザがアカウントにアクセスするには、管理者による作業が必要になります。または、アカウントを有効にするように選択でき、これがデフォルトです。

デフォルトでは、ドライバ設定では、データを最も確実に保存できるオプションが使用されます。たとえば、管理者がポリシーを変更する際に誤りがあった場合に、意図せずアカウントが失われることがないよう、GroupWise アカウントの削除のデフォルトの意味は「無効」に設定されています。別の例を挙げると、Identity Manager ドライバ設定では、別のシステムのユーザアカウントからの値があるエンタイトルメントは取り消されません。ユーザに電子メール配布リストのメンバーシップが付与され、後にユーザがエンタイトルメントポリシーの条件に一致しなくなった場合、そのユーザは単にポリシーメンバーシップを取り消されます。アカウントは無効になりますが、グループメンバーシップおよび属性値は削除されません。別の結果が必要な場合は、Identity Manager のベテランユーザがドライバ設定をカスタ \'83\'7d イズできます。

エンタイトルメントの取り消しの解釈は特に重要です。Role-Based Entitlement (役割ベースのエンタイトルメント) 機 \'94\'5c を使用すると、研究室環境で結果をテストせずに、運用環境で組織のエンタイトルメントを一括して変更できるためです。

事前設定済みのドライバのグローバル設定の変数を編集すると、付与または取り消しの解釈の設定を変更できます。独自のカスタム設定を作成している場合、エンタイトルメントの付与および取り消しを解釈する GCV を追加できます。

6.10.2 データの損失の回避

役割ベースエンタイトルメントは、ポリシーのメンバーシップに基づき、アカウントなどのエンタイトルメントを一括して変更できるように設計されています。ただし、これは、ポリシーの変更時に誤りがあると問題になる可能性があることを意味します。Identity

Manager に付属のドライバ設定では、影響の最も少ない設定が使用されています。GCV を使用して、意 \'90\'7d しないデータの損失を回避する方法を理解する必要があります。

たとえば、削除は、アカウントのエンタイトルメントの取り消しを解釈する GCV の値として使用しないことをお勧めします。

新しいエンタイトルメントポリシーを作成または編集する際にデータを保護するもう 1 つの方法は、ポリシーの編集が終了しないうちは、ドライバをオフにして変更できないようにする方法です。編集が完了したら、エンタイトルメントポリシーインタフェースの［*再起動*］ボタンを使用して、ドライバを手動で再起動できます。同様に、別のユーザが Entitlement Policy (エンタイトルメントポリシー) を編集している可 \'94\'5c 性がある場合に、［*Restart*］*\'83\'7b タンを使用してエンタイトルメントサービスドライバを再起動しようとすると、他のユーザの変更作業が完了するまではドライバを再起動しないようにプロンプトが \'95\'5c 示されます。*

6.10.3 パスワード同期およびエンタイトルメント

で説明するとおり、パスワード同期は、役割ベースエンタイトルメントを使用するドライバに対しては、他のドライバと同じ方法で管理されます。85 ページの 「接続システム間のパスワード同期」

ジョブをスケジュールする 7

Designer および iManager には、イベントをスケジュールするためのジョブスケジュールユーティリティがあります。このユーティリティを使用して、特定の日にアカウントを無効にしたり、企業リソースへの個人のアクセス権の拡張を要求するワークフローを開始したりするようにシステムを設定できます。

- インストールされているジョブ定義からジョブオブジェクトを作成します。
- ジョブを実行するタイミング、ジョブを実行するサーバ、eDirectory オブジェクトに関するジョブのスコープ、およびジョブの中間結果と最終結果のレポートなどを定義します。
- ジョブのパラメータの値、ジョブの説明、および表示名を設定します。
- ジョブを有効 / 無効にする、ジョブを手動で起動する、実行中のジョブを停止する、および実行中のジョブの一覧を表示します。

- 213 ページのセクション 7.1「Designer でジョブをスケジュールする」
- 225 ページのセクション 7.2「iManager 内でジョブをスケジュールする」

7.1 Designer でジョブをスケジュールする

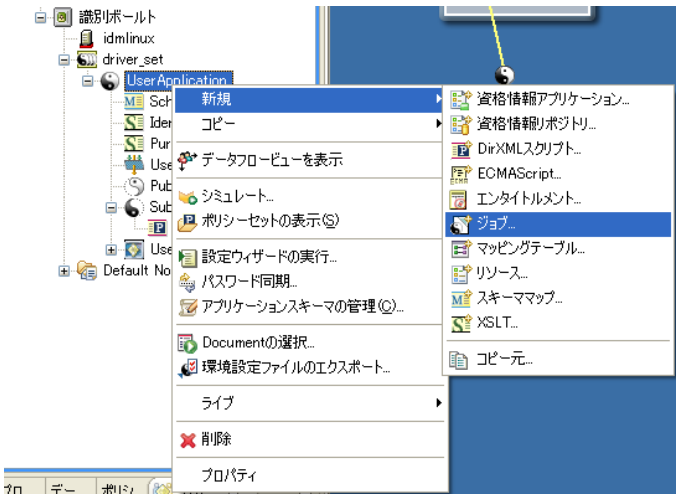
Designer のジョブスケジューラには、iManager のジョブスケジューラの機能とほぼ同じ機能が含まれています。

- 213 ページのセクション 7.1.1「ジョブを作成する」
- 215 ページのセクション 7.1.2「ジョブを編集する」

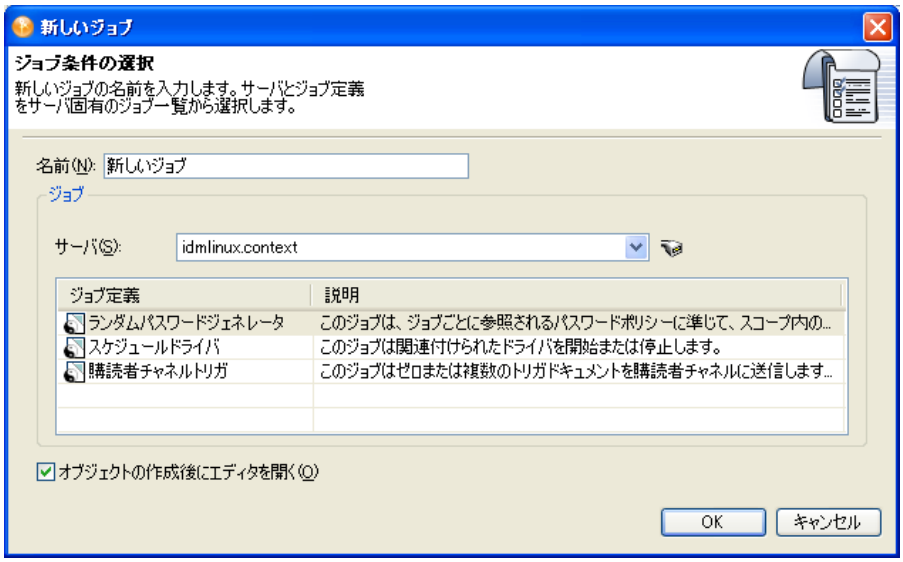
7.1.1 ジョブを作成する

Designer で新しいジョブを作成する

1 概要ビューでドライバを右クリックして、[*新規作成*] > [*ジョブ*] の順に選択します。



2 新しいジョブウィンドウで、ジョブに内容がわかる名前を付けるか、表示されている名前を使用します。



3 [サーバ] フィールドで、ジョブを実行するサーバを選択します。ドロップダウン項目をクリックして、リストされている以外のサーバを選択することができます。

4 管理者がカスタムジョブの定義を作成し、選択したサーバにインストールしている場合、サーバエントリの右側にある [*サーバからジョブ定義を更新する*] アイコンをクリックして、サーバから使用可能なジョブのライブリストを読み込みます。Designer は、オフラインモデリングツールであるため、サーバの*ジョブ定義*リストには、デフォルトでは、Identity Manager 3.5 のジョブ定義のみ表示されます。

5 ジョブの定義を選択します。新規ジョブウィザードには、3 つのジョブ定義が表示されます。追加のカスタムジョブが表示されている場合もあります。

- **ランダムパスワードジェネレータ :** ジョブのスコープ内にある各ジョブに対して、ランダムなパスワードが生成されます。パスワードは、ジョブが参照するパスワードポリシーオブジェクトと一致するように、NMAS™ によって生成されます。これらのパスワードポリシーオブジェクトは、通常は eDirectory™ ユーザパスワードポリシーで使用されるオブジェクトとは異なります。

  ジョブからは、生成されたパスワードが一度に 1 つずつドライバの購読者チャネルに送信されます。購読者チャネルポリシーは、パスワードに対してアクションを実行する必要があります。

- **スケジュールドライバ :** 関連付けられているドライバを起動または停止します。停止しているドライバを起動するため、または稼動中のドライバを停止するために、ドライバを切り替えることもできます。

- **購読者チャネルトリガ :** ゼロまたは複数のトリガドキュメントを購読者チャネルに送信します。この送信は、スコープが定義されている場合はオブジェクトごとに 1 つのドキュメント、スコープが定義されていない場合はシングルのトリガイベントとなります。

  トリガイベントドキュメントにより、ジョブスコープオブジェクトが識別されます。トリガイベントは必要に応じて、キャッシュをバイパスして、「キューの先頭に移動」できます。トリガジョブにより、個人的な要件を満たすためにカスタマイズできるドライバポリシーを使用できます。

6 ジョブを編集するかどうかを決めます。［*オブジェクトの作成後にエディタを開く*］オプションを選択すると、新たに作成したジョブにより最初のジョブオブジェクトが保存された後で、そのジョブが IDM ジョブエディタウィンドウで開きます。この時点でエディタを開きたくない場合は、エディタの選択を解除します。

7 *［OK］*をクリックします。

8 ファイルの矛盾ウィンドウには、ジョブオブジェクトを保存して続行するためのオプションがあります。ジョブオブジェクトを作成して、IDM ジョブエディタの使用を継続する場合は、［*はい*］をクリックします。レガシーシステム要件を配布ルールのベースとして使用しない場合は、*［いいえ］*をクリックします。

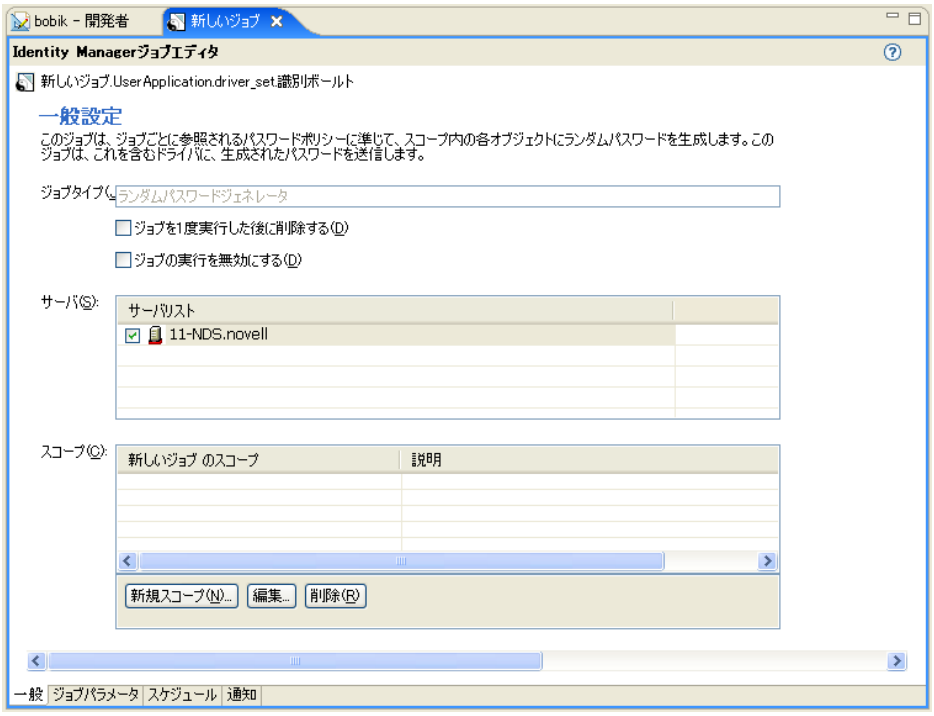
9 216 ページの 「［一般］タブでジョブエディタを選択する」に進みます。

7.1.2 ジョブを編集する

- 216 ページの 「［一般］タブでジョブエディタを選択する」
- 218 ページの 「［ジョブパラメータ］タブでジョブエディタを選択する」
- 221 ページの 「［スケジューラ］タブでジョブエディタを選択する」
- 223 ページの 「［通知］タブでジョブエディタを選択する」
- 224 ページの 「スコープオブジェクトがあるジョブを展開する」

ジョブを作成した後は、そのジョブを便利なものにするために必要な情報を追加する必要があります。ジョブを編集するには、概要ビューで新たに作成したジョブをダブルクリックして、そのジョブを IDM ジョブエディタビューに表示します。

図 7-1 *IDM ジョブエディタビュー*

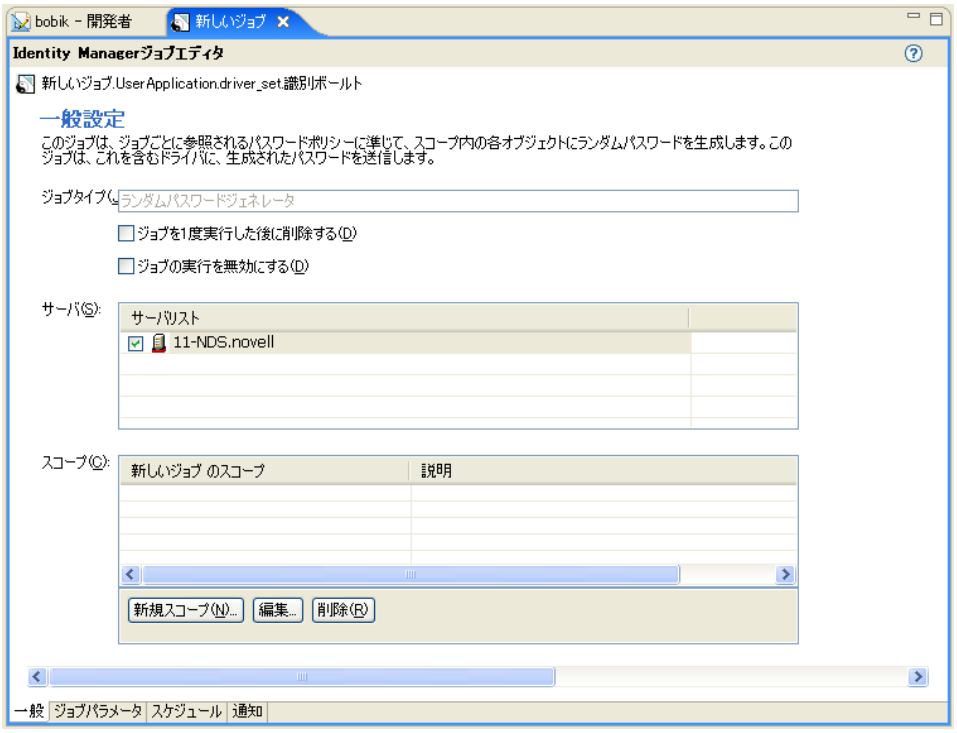


IDM ジョブエディタのビューの一番下には、4 つのタブがあります。

［一般］タブでジョブエディタを選択する

［一般］タブの一番上の行には、ジョブの Java クラス名が表示されます。その後には、選択したジョブのタイプを示すジョブタイプが表示されます。ジョブタイプヘッダで、ジョブを有効または無効にする、またはジョブを実行後に削除することを指定できます。

図 7-2 *［一般］タブの項目*



1 ジョブを実行後に削除するには、［*一度実行後にジョブを削除する*］を選択します。

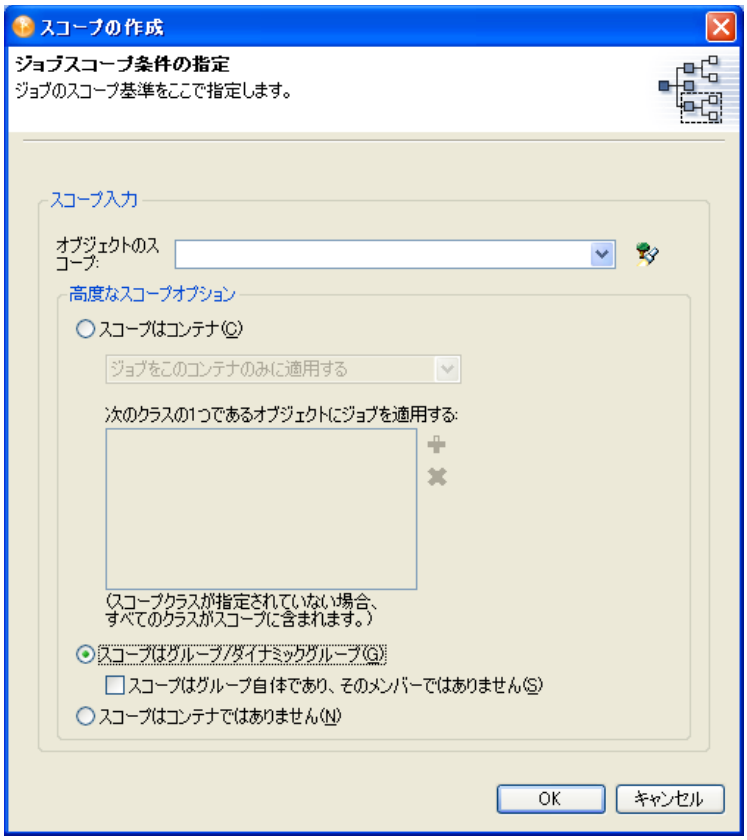
2 ジョブを実行できなくするには、［*ジョブを実行できなくする*］を選択します。

3 ［*サーバリスト*］カラムで、このジョブを実行する 1 つまたは複数のサーバを選択します。

   このジョブを割り当てるのに役立つ、サーバのフィルタ済みのリストを使用できます。カスタムジョブは 1 つのサーバにインストールできますが、他のサーバにもインストールすることはできません。この場合、このカスタムジョブが割り当てられていないサーバは、サーバリストから除外されます。

   ジョブは、それぞれのサーバにインストールされてさえいれば、複数のサーバに割り当てることができます。Designer では、ジョブが正常にインストールおよびパッケージされていて、メタディレクトリエンジンがそれらのジョブを認識できる場合のみ、この関連付けが認められます。

4 スコープを［スコープ］カラムに追加するには、［*新規スコープ*］をクリックします。



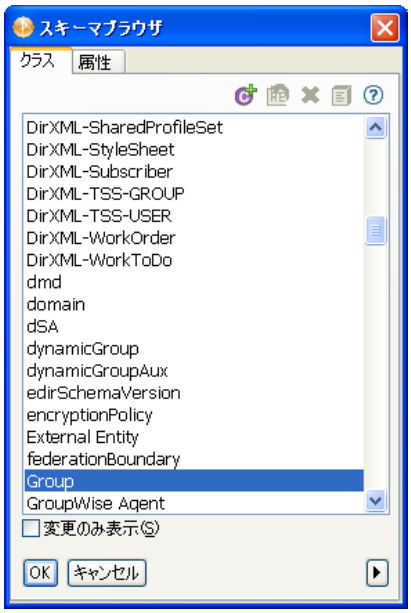
5 スコープオブジェクトを選択するには、オブジェクトの識別名を入力するか、［*参照*］アイコンを使用して、オブジェクトを参照して選択します。［*OK*］をクリックして、スコープオブジェクトを追加します。

スコープを使用すると、このジョブを適用するオブジェクトを定義できます。eDirectory 内のオブジェクトはコンテナ、ダイナミックグループ、グループ、またはリーフオブジェクトです。グループオブジェクトを選択する場合、ジョブはグループのメンバー、またはグループにのみ適用できます。コンテナオブジェクトを選択する場合、ジョブはそのコンテナのすべての子孫、そのコンテナのすべての子、またはそのコンテナにのみ適用できます。

6 オブジェクトがコンテナの場合は、［*スコープはコンテナ*］を選択します。次に、ジョブを適用する方法を選択します。

- ジョブをこのコンテナのみに適用する
- ジョブをこのコンテナの子に適用する
- このコンテナのすべての子孫にジョブを適用する

7 (オプション) ［*ジョブをこのコンテナの子に適用する*］または［*このコンテナのすべての子孫にジョブを適用する*］を選択する場合は、スコープするクラスを指定できます。プラス［+］アイコンをクリックして、スキーマブラウザウィンドウを表示して、スコープするクラスを選択します。クラススキーマを選択して、［*OK*］をクリックします。



クラスは［*クラス*］ボックスに追加されます。クラスを削除するには、クラスを選択して、マイナス［-］アイコンをクリックします。

8 オブジェクトがグループまたはダイナミックグループの場合は、［*スコープはグループ/ダイナミックグループ*］を選択します。次に、スコープがグループ用の場合は、［*スコープはグループ自体であり、そのメンバーではありません*］オプションを選択できます。

9 オブジェクトがコンテナ以外の場合は、［*スコープはコンテナではありません*］を選択します。

10 スコープの条件を選択したら、［*OK*］をクリックして［一般設定］ページに戻ります。

11 スコープを編集する必要がある場合は、スコープ名を選択して、［*編集*］をクリックします。

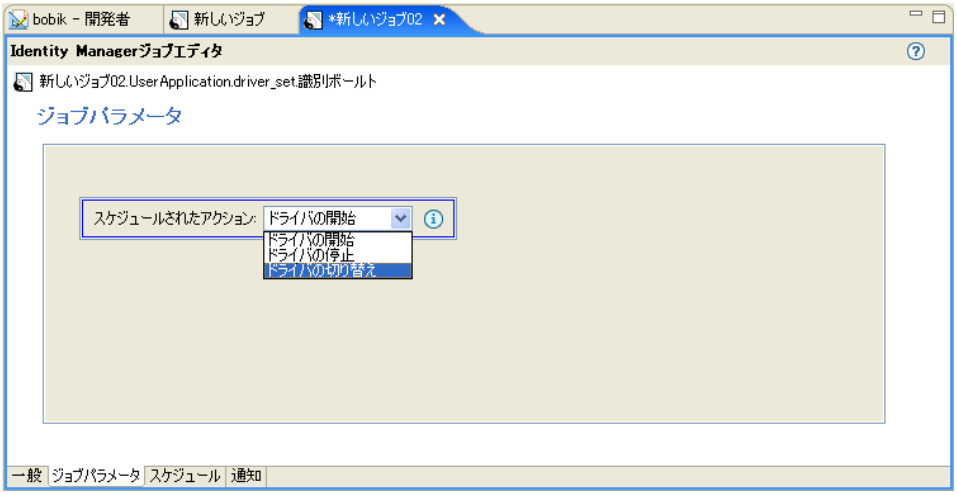
12 スコープを削除するには、スコープ名を選択して［*削除*］をクリックします。

［ジョブパラメータ］タブでジョブエディタを選択する

［ジョブパラメータ］ページでは、追加パラメータをジョブに追加して、パラメータの現在の設定内容を確認できます。実行できる内容は、選択したジョブのタイプによって異なります。

スケジュールドライバジョブのパラメータ

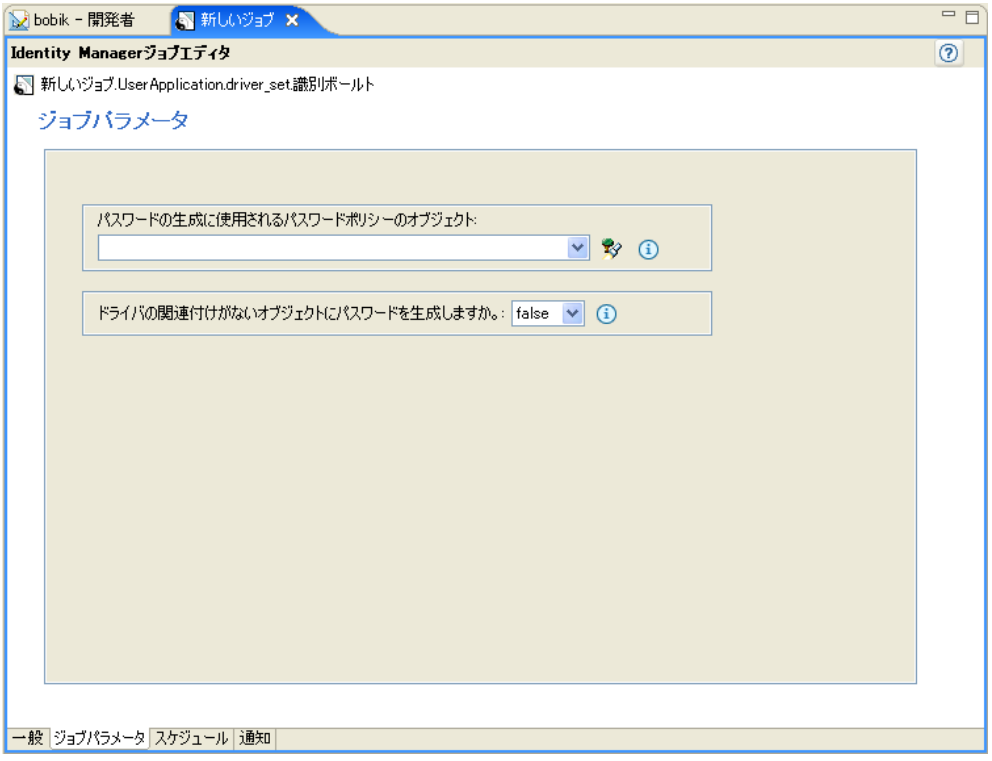
図 7-3 スケジュールドライバジョブの［ジョブパラメータ］ページ



1. ジョブでドライバを開始する場合は、［*ドライバの開始*］を選択します。
2. ジョブでドライバを停止する場合は、［*ドライバの停止*］を選択します。
3. ジョブでドライバが開始している場合は停止し、ドライバが停止している場合は開始する場合は、［*ドライバの切り替え*］を選択します。

ランダムパスワードの生成ジョブのパラメータ

図 7-4 ランダムパスワードの生成ジョブの［ジョブパラメータ］ページ

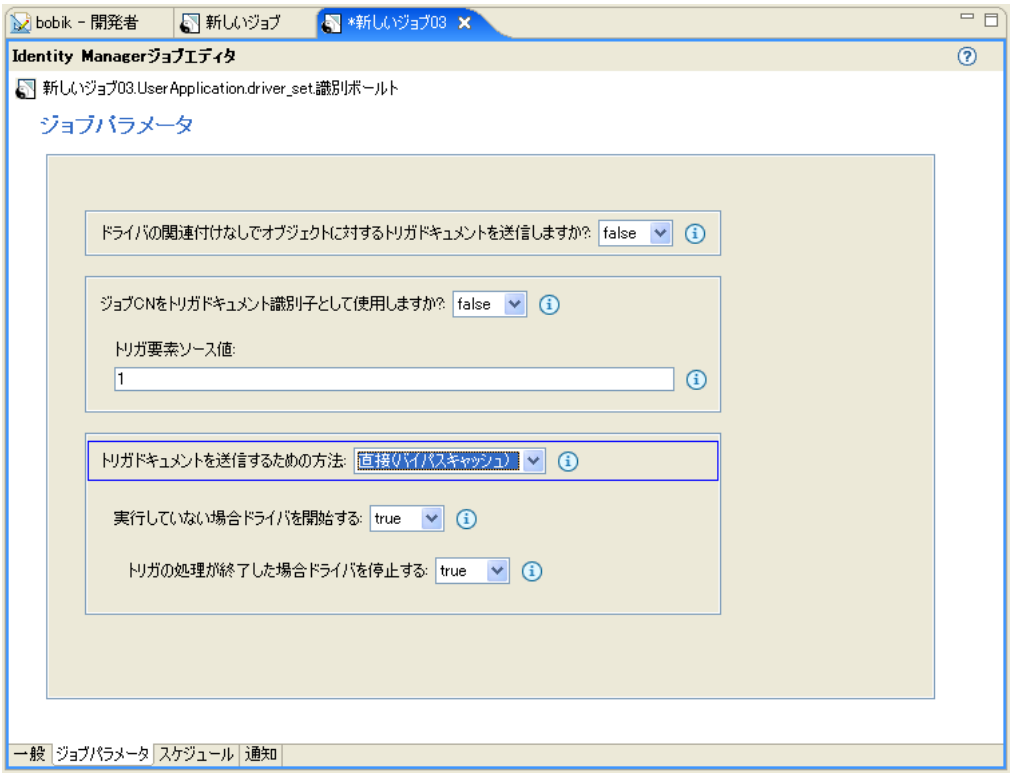


1 パスワードポリシーオブジェクトの識別名を入力するか、［*参照*］アイコンを使用して、パスワードの生成に使用するパスワードポリシーを選択します。

2 ドライバが関連付けられていないスコープオブジェクトのパスワードを生成する場合は、［*True*］を選択します。それ以外は、［*False*］を選択します。

購読者チャネルトリガジョブのパラメータ

図 7-5 *購読者チャネルトリガジョブの［ジョブパラメータ］ページ*



1 ドライバが関連付けられていないスコープオブジェクトのトリガドキュメントを送信する場合は、［*True*］を選択します。それ以外は、デフォルトの［*False*］のままにします。

2 ジョブの CN(共通名) をドキュメント識別子のトリガとして使用する場合は、デフォルトの［*True*］のままにします。それ以外は、［*False*］を選択します。

3 (オプション)［*False*］を選択した場合は、トリガ要素のソース属性の値としてジョブが使用できる文字列を指定します。

4 トリガドキュメントを送信する方法を選択します。トリガ元のジョブをキューに入れる場合は、デフォルトの［*キュー (キャッシュの使用)*］のままにします。それ以外は、［*直接 (バイパスキャッシュ)*］を選択します。

5 (オプション)［*直接 (バイパスキャッシュ)*］を選択した場合、［*実行していない場合ドライバを開始する*］オプションが表示されます。実行していないドライバを開始する場合は、デフォルトの［*True*］のままにします。それ以外は、［*False*］を選択します。

6 (オプション)［*実行していない場合ドライバを開始する*］オプションで［*True*］を選択した場合、デフォルトの［*True*］が設定された状態で［*トリガの処理が終了した*

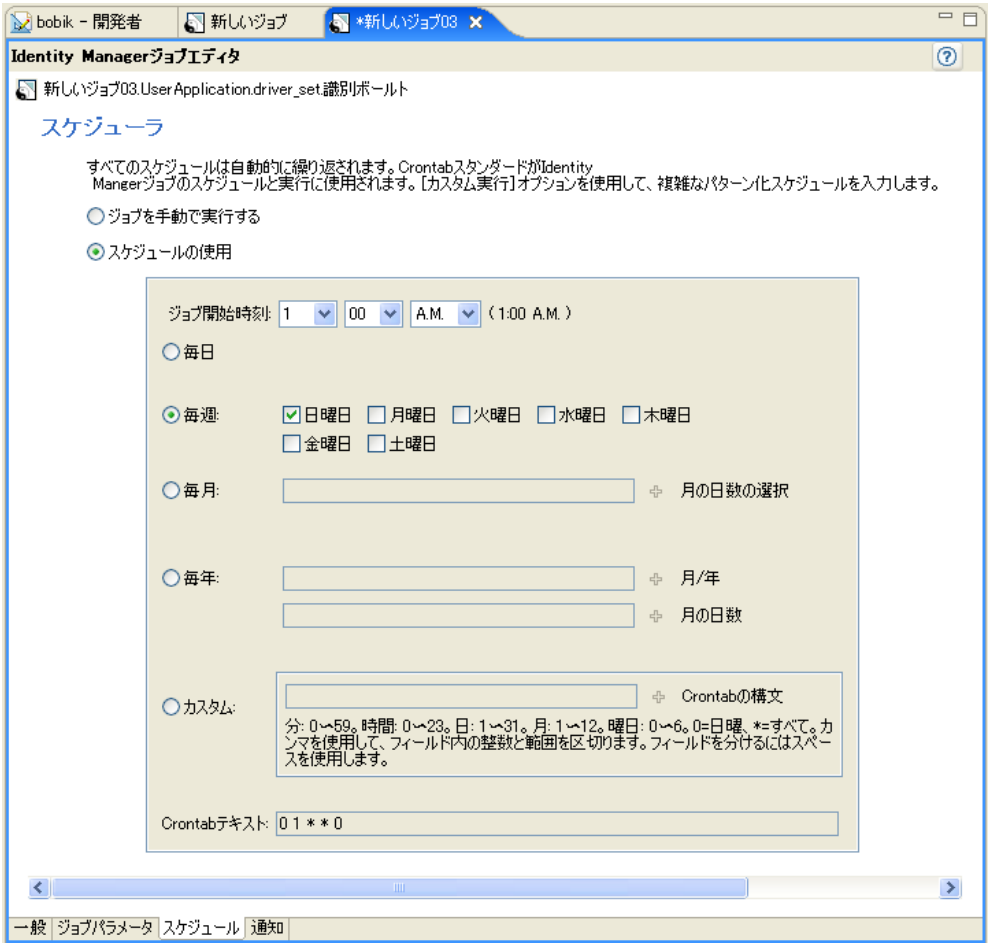
場合ドライバを停止する］オプションが表示されます。デフォルトの設定を使用して、トリガジョブの処理が終了したらドライバを停止するか、［*False*］を選択してドライバを稼動し続けます。

カスタマイズされたジョブ定義には、それぞれ独自のパラメータのセットがあります。

［スケジューラ］タブでジョブエディタを選択する

［スケジューラ］タブを使用すると、ジョブを実行するタイミングを設定できます。

図 7-6 *［スケジューラ］タブのジョブオプション*



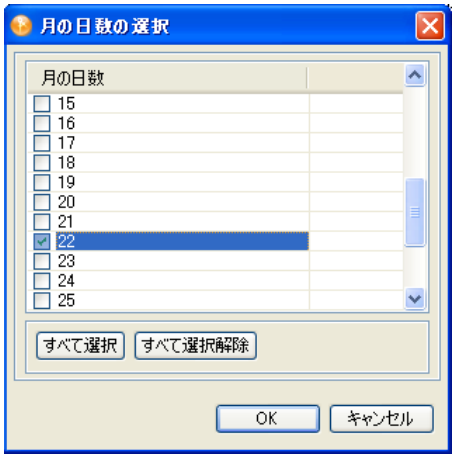
1 ［*スケジュールの使用*］オプションを選択して、ジョブの実行日時、および周期 (毎日、毎週、毎月、毎年) を設定します。

   選択したときにジョブを実行するには、［*ジョブを手動で実行する*］オプションを選択します。

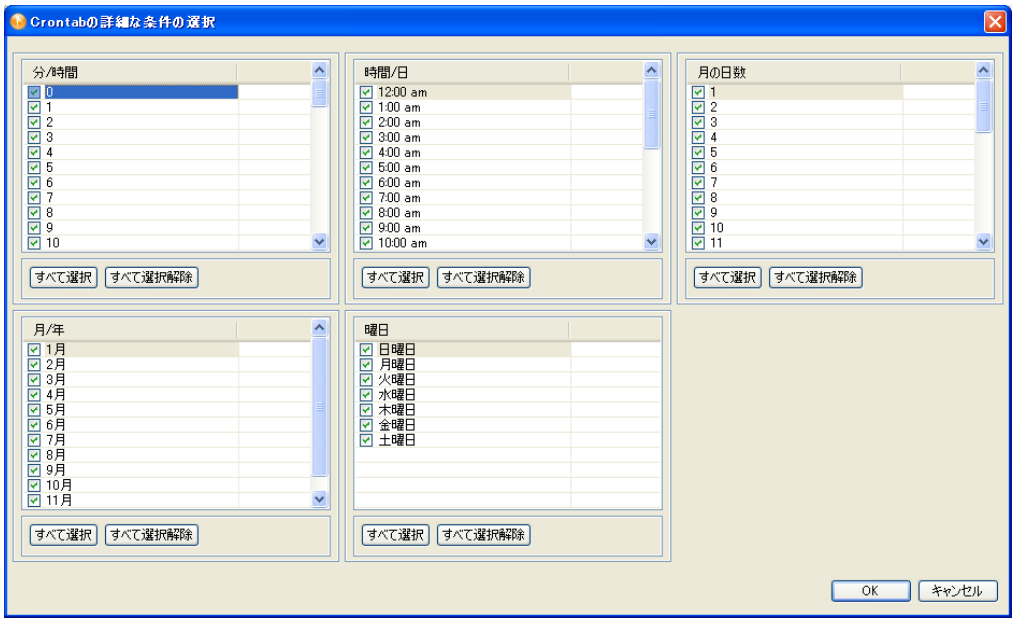
2 ［*スケジュールの使用*］を選択した場合は、ジョブを開始する時刻を設定します。ドロップダウンメニューを使用して、時間、分、および［*午前*］または［*午後*］を選択します。デフォルトは午前 1 時です。

3 ジョブを繰り返し実行する場合は、［*毎日*］、［*毎週*］、［*毎月*］、［*毎年*］、または［*カスタム*］の各フィールドを使用して、実行するタイミングを選択します。

たとえば、ジョブを毎週実行する場合は、［*毎週*］を選択して、実行する曜日を選択します。ジョブを月に一度実行する場合は、［*毎月*］を選択しし、［*Plus (+)*］アイコンをクリックして、日を選択します。



4 (オプション) ［*カスタム*］を選択して、［Crontab の詳細な条件の選択］ページから分、時間、日、月、および曜日を選択します。



5 ［Crontab の詳細な条件の選択］ページでは、デフォルトですべてが選択されています。［*すべて選択解除*］をクリックして、ジョブを実行するに日時を選択し、［*OK*］をクリックして［スケジューラ］ページに戻ります。

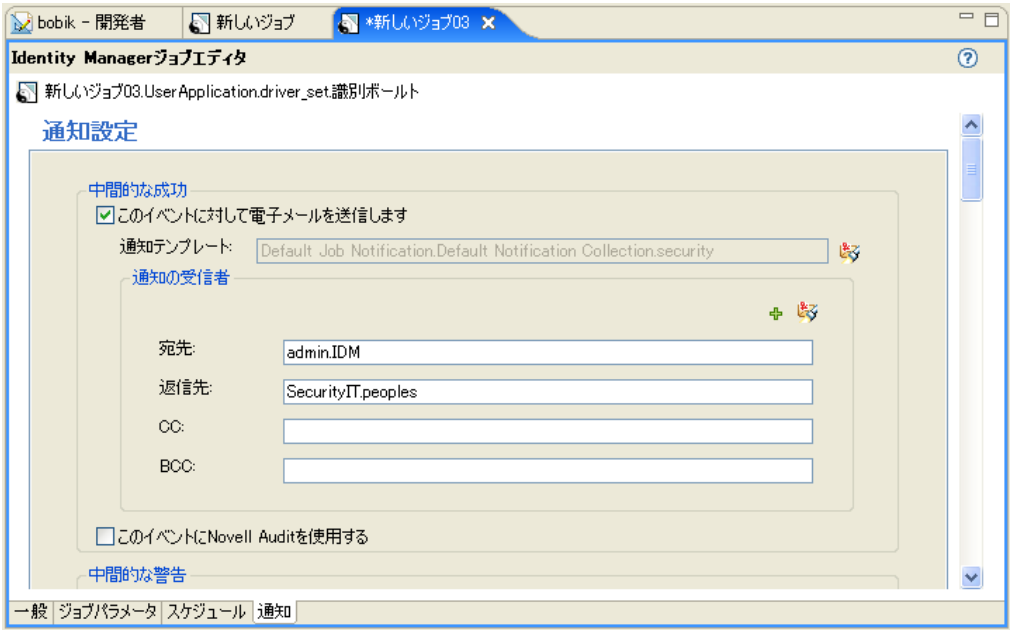
［*Crontab テキスト*］フィールドに表示される情報には、［スケジューラ］ページで設定した内容が表示されます。たとえば、［*毎月*］をクリックして 2 つの日を選択した場合、それら 2 つの日が［*Crontab テキスト*］フィールドに表示されます。

［通知］タブでジョブエディタを選択する

［通知設定］ページでは、ジョブの結果で行うことを定義できます。このページには、「*中間*」と「*最終*」の 2 つの部分があり、それぞれに「*成功*」、「*警告*」、「エラー」、および「*中止*」という結果が表示されます。

［通知設定］ページでは、各結果の通知方法を設定できます。アクションには、「監査結果を送信する」、または「結果が確定したときに電子メールを送信する」が含まれます。

図 7-7 *［通知］タブのジョブオプション*



1. ［*このイベントに対して電子メールを送信します*］を選択すると、Designer により、［*通知テンプレート*］フィールドに *Default Job Notification.Default Notification.security* テンプレートが配置されます。テンプレートを変更するには、［*モデルブラウザ*］アイコンをクリックして、別のテンプレートを選択します。
2. ［通知の受信者］で、ユーザまたはグループの完全な識別名を入力して、結果を送信する相手を選択します。［*Plus (+)*］アイコンを使用して、メールプロファイルを作成できます。

［*宛先*］と［*返信先*］フィールドは、プロファイルの必須フィールドです。

3 情報を入力し終えたら、［*OK*］をクリックします。

4 結果を Novell® Audit に送信する場合は、［*このイベントに Novell Audit を使用する*］を選択します。

5 各オプションに対して、ステップ 1 からステップ 4 を繰り返します。

- *中間的な > 成功*
- *中間的な警告*
- *中間的なエラー*
- *中間的な中止*
- *最終的な成功*
- *最終的な警告*
- *最終的なエラー*
- *最終的な中止*

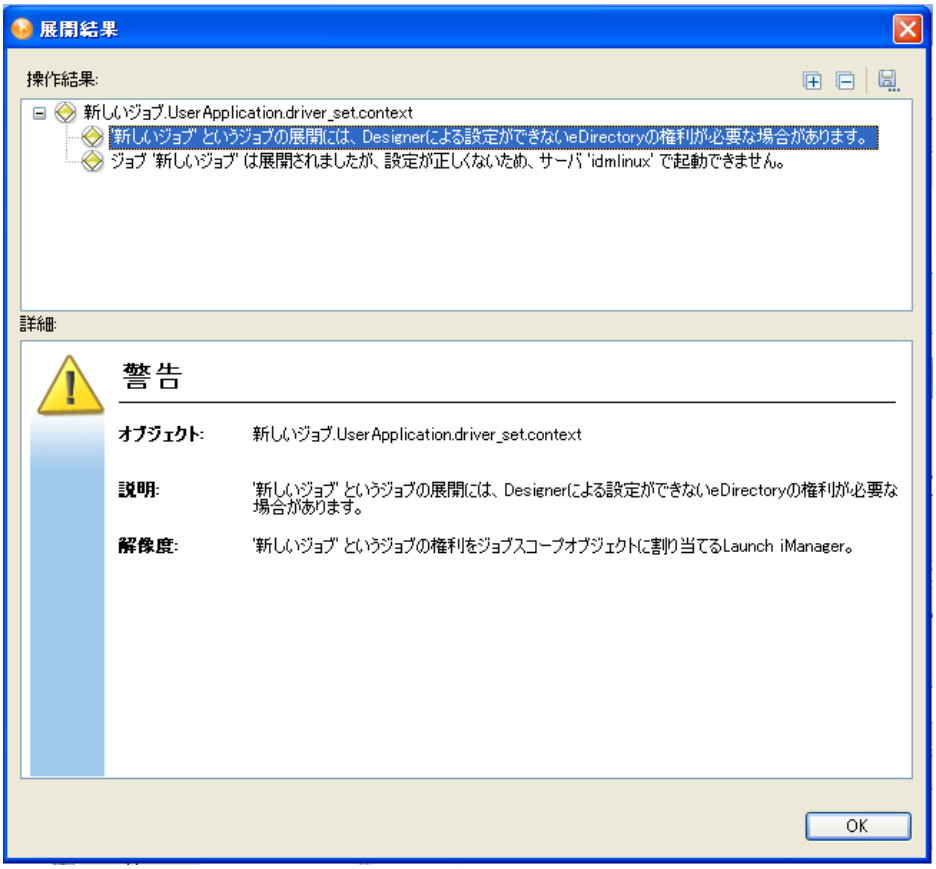
オプションを選択しないと、結果に対するアクションは行われません。

スコープオブジェクトがあるジョブを展開する

ジョブによっては、eDirectory データや特定の Identity Manager のアクション (ドライバの起動および停止など) にアクセスする必要があります。このようなアクセスは、eDirectory の権利の割り当て対象となり、DirXMLJob オブジェクトに付与された権利で制御されます。Identity Manager のアクションは、特別な属性で制御されますが、データの読み書きには eDirectory の通常の権利が必要になります。

スコープオブジェクトがあるジョブオブジェクトを展開する際、それらのジョブオブジェクトには Designer で正常にセットアップできない eDirectory の権利が割り当てられている場合があります。タスクを完了するのに必要な権利は、ジョブオブジェクトに割り当てられているスコープオブジェクトによって異なります。

図 7-8 スコープオブジェクトがあるジョブを展開するときの警告メッセージ



ジョブオブジェクトを展開するときにこの警告が表示される場合は、iManager ユーティリティを使用して eDirectory の権利をジョブオブジェクトに割り当て、ジョブオブジェクトがジョブスコープオブジェクトに正常にアクセスして、タスクを完了できるようにします。

7.2 iManager 内でジョブをスケジュールする

iManager のジョブスケジューラには、Designer にあるジョブスケジューラと同様の機能が含まれています。ただし、iManager のジョブスケジューラでは、ジョブの起動と停止、およびジョブのステータスの取得が行えます。

［Identity Manager ドライバの概要］ページからアクセスする［ジョブ］ページには、選択したドライバの既存のジョブオブジェクトが表示される表が含まれており、ジョブオブジェクトの名前が一覧表示されています。次はジョブドライバ用に作成されたスケジュールジョブの例です。

図 7-9 ［Identity Manager ドライバの概要］ページのジョブのタブ

7.2.1 ジョブ列ヘッダ

ヘッダにはジョブの名前、ジョブが有効か無効か、実行スケジュール、ジョブの説明があります。ジョブ名をクリックして、［ジョブプロパティ］ページを表示します。ジョブを有効または無効にするには、［有効］列の下で［有効 / 無効］アイコンをクリックします。［次回スケジュールされた実行］ヘッダには、ジョブの実行がスケジュールされているかどうか、およびスケジュールされている場合のスケジュール日が表示されます。ジョブの完全な説明が一覧表示されてポップアップウィンドウを確認するには、ジョブの説明をクリックします。

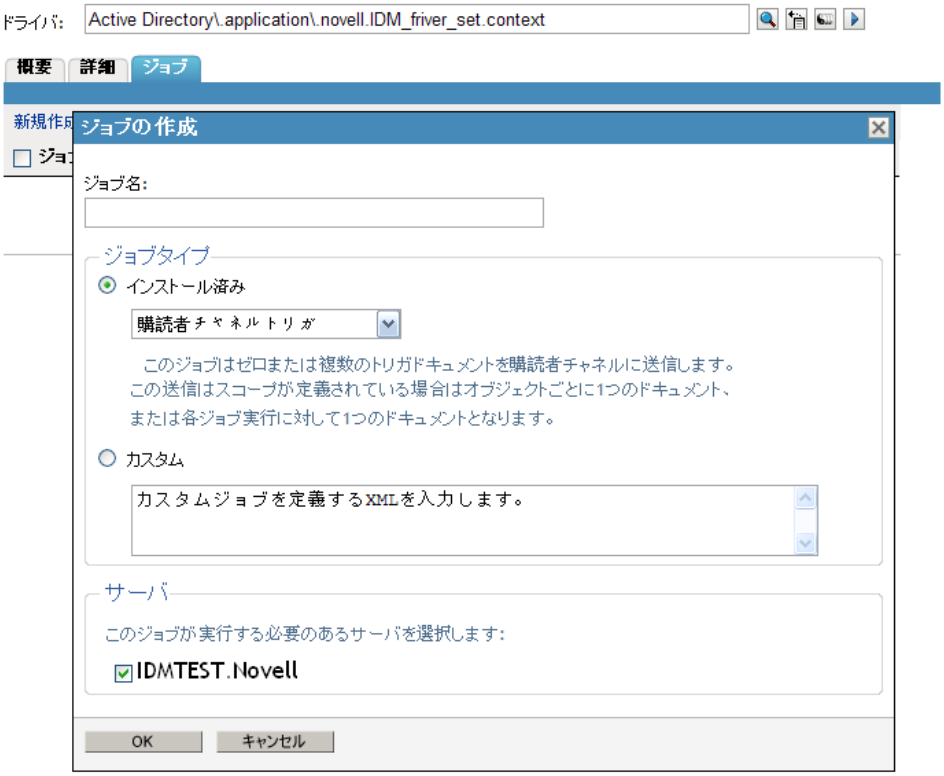
メニューバーのコマンドを使用して次の操作を実行します。

- 226 ページの 「新規」
- 228 ページの 「即時実行」
- 228 ページの 「停止」
- 228 ページの 「有効にする」
- 228 ページの 「無効」
- 228 ページの 「ステータスの取得」
- 228 ページの 「削除」

新規

iManager で新しいジョブを作成する

1 ［新規作成］をクリックして、［ジョブの作成］ページを表示します。



2 ジョブ名エントリで、ジョブにわかりやすい名前を設定します。

3 ［*ジョブタイプ*］で、［*インストール済み*］ジョブまたは［*カスタム*］ジョブを選択します。デフォルトは［*インストール済み*］です。

3a ［*インストール済み*］で、ジョブの定義を選択します。［ジョブの作成］ページに、サーバにインストールされているすべてのジョブが表示されます。Identity Manager 3.5 には、3 つのジョブ定義が付属しています。

- **ランダムパスワードジェネレータ :** ジョブのスコープ内にある各ジョブに対して、ランダムなパスワードが生成されます。パスワードは、ジョブが参照するパスワードポリシーオブジェクトと一致するように、NMAS によって生成されます。これらのパスワードポリシーオブジェクトは、通常は eDirectory ユーザパスワードポリシーで使用されるオブジェクトとは異なります。

  ジョブからは、生成されたパスワードが一度に 1 つずつドライバの購読者チャネルに送信されます。購読者チャネルポリシーは、パスワードに対してアクションを実行する必要があります。

- **スケジュールドライバ :** 関連付けられているドライバを起動または停止します。停止しているドライバを起動するため、または稼動中のドライバを停止するために、ドライバを切り替えることもできます。

- **購読者チャネルトリガ :** ゼロまたは複数のトリガドキュメントを購読者チャネルに送信します。この送信は、スコープが定義されている場合はオブジェクトごとに 1 つのドキュメント、スコープが定義されていない場合はシングルのトリガイベントとなります。

  トリガイベントドキュメントにより、ジョブスコープオブジェクトが識別されます。トリガイベントは必要に応じて、キャッシュをバイパスして、

「キューの先頭に移動」できます。トリガジョブにより、個人的な要件を満たすためにカスタマイズできるドライバポリシーを使用できます。

3b ［カスタム］を選択した場合は、カスタムジョブを定義する XML コードを入力します。

4 ［*サーバ*］フィールドで、ジョブを実行する 1 つまたは複数のサーバを選択します。

5 *［OK］*をクリックします。新しいジョブにより、［ジョブプロパティ］ページが開きます。

6 228 ページのセクション 7.2.2「ジョブのパラメータを設定する」に進みます。

即時実行

ジョブの左側にあるボックスをオンにしてジョブを選択して、［即時実行］をクリックします。

停止

ジョブの左側にあるボックスをオンにしてジョブを選択して、［停止］をクリックします。

有効にする

ジョブの左側にあるボックスをオンにしてジョブを選択して、［*有効*］をクリックします。ジョブが有効になると、［*有効*)］カラムの［*無効*］アイコンがチェックマークに変わります。

無効

ジョブの左側にあるボックスをオンにしてジョブを選択して、［*無効*］をクリックします。［*有効*］カラムの［*有効*］アイコンが［*無効*］アイコンに変わります。

ステータスの取得

ジョブの左側にあるボックスをオンにしてジョブを選択して、［*ステータスの取得*］をクリックします。

削除

ジョブを削除するには、ジョブ名の左側にあるボックスをオンにして、［*削除*］をクリックします。選択したジョブがディレクトリから削除されるというメッセージが表示されます。ジョブを削除する場合は［*OK*］をクリックし、操作を中断する場合は［*キャンセル*］をクリックします。複数のジョブを削除するには、複数のボックスをクリックします。すべてのジョブを削除するには、左上のボックスをクリックします。

7.2.2 ジョブのパラメータを設定する

ジョブをクリックして［ジョブプロパティ］ページを表示し、ジョブの実行方法を設定します。

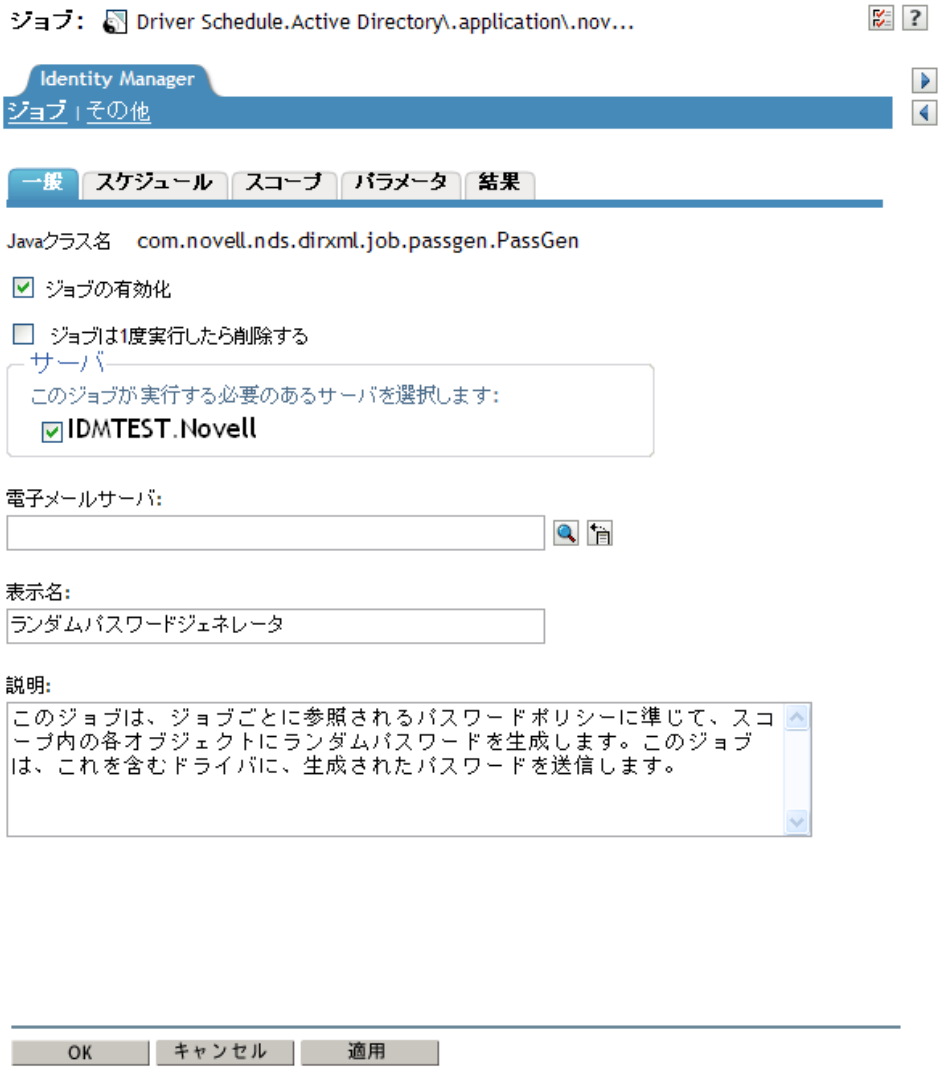
- 229 ページの 「［一般］タブで選択する」
- 230 ページの 「［スケジュール］タブで選択する」
- 231 ページの 「［スコープ］タブで選択する」

- 233 ページの 「[パラメータ] タブで選択する」
- 235 ページの 「[結果] タブで選択する」

[一般] タブで選択する

[一般] タブの一番上の行には、ジョブの Java クラス名が表示されます。

図 7-10 *[一般] タブの項目*



1 ジョブを有効にするには、[*ジョブの有効化*] を選択します。

2 ジョブを実行後に削除するには、[*ジョブを 1 度実行した後に削除する*] を選択します。

3 [*サーバ*] カラムで、このジョブを実行する 1 つまたは複数のサーバを選択します。

このジョブを割り当てるのに役立つ、サーバのフィルタ済みのリストを使用できます。カスタムジョブは 1 つのサーバにインストールできますが、他のサーバにもインストールすることはできません。この場合、このカスタムジョブが割り当てられていないサーバは、サーバリストから除外されます。

ジョブは、それぞれのサーバにインストールされてさえいれば、複数のサーバに割り当てることができます。iManager では、ジョブが正常にインストールおよびパッケージされていて、メタディレクトリエンジンがそれらのジョブを認識できる場合のみ、この関連付けが認められます。

4 *電子メールサーバ*エントリの場合は、デフォルトの通知コレクションテンプレートを参照します。［参照］ボタン、［セキュリティコンテナ］の順に選択して、デフォルト通知コレクションオブジェクトを選択します。完全な識別パスは、Default Notification Collection.Security です。または、［履歴］アイコンを使用して、以前選択した項目から選択することができます。

5 他のジョブ設定を確認します。

- *表示名*エントリには、選択されたジョブのタイプが表示されます。
- ［*説明*］フィールドには、該当ジョブタイプに対して記述されている説明が表示されます。

［スケジュール］タブで選択する

［スケジューラ］タブを使用すると、ジョブを実行するタイミングを設定できます。

図 7-11 *［スケジューラ］タブのジョブオプション*

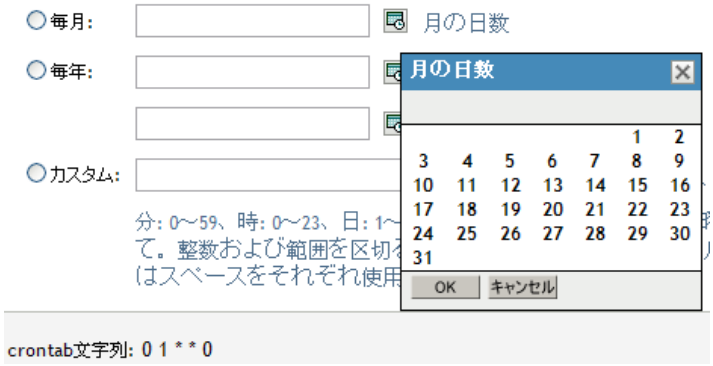
1 ［*スケジュールどおりの実行*］オプションを選択して、日付と時間、およびジョブを日次、週次、月次、または年次で実行するかを設定します。

または、選択したときにジョブを実行するには、［*手動の実行*］オプションを選択します。

2 ［*スケジュールどおりの実行*］を選択した場合、ジョブを開始する時刻（時間と分）を入力します。ドロップダウンメニューを使用して、［*午前*］または［*午後*］を選択します。デフォルトは午前 1 時です。

3 ジョブを繰り返し実行する場合は、［*毎日*］、［*毎週*］、［*毎月*］、［*毎年*］、または［*カスタム*］の各フィールドを使用して、実行するタイミングを選択します。

たとえば、ジョブを毎週実行する場合は、［*毎週*］を選択して、実行する曜日を選択します。ジョブを月に一度実行する場合は、［*毎月*］を選択しし、［*カレンダ*］アイコンをクリックして、日を選択します。



4 ［*カスタム*］を選択した場合は、分、時間、日、月、および曜日を次の crontab 構文で指定します。

- 分 : 0-59、時間 : 0-23、日 : 1-31、月 : 1-12、曜日 : 0-6、0 は日曜日、* はすべて。
- カンマ (,) を使用して整数と範囲を区切り、スペースを使用して各フィールドを区切ります。

［*crontab 文字列*］フィールドに表示される情報には、［カスタム］エントリで設定した内容が表示されます。たとえば、「30,2,1,12,5」と入力して、<*Enter*> キーを押すと、これらの数字が［*crontab 文字列*］フィールドに表示されます。

5 ジョブをスケジュールする日 (複数可) を選択したら、［*OK*］をクリックします。

［スコープ］タブで選択する

スコープを使用すると、このジョブを適用するオブジェクトを定義できます。eDirectory 内のオブジェクトはコンテナ、ダイナミックグループ、グループ、またはリーフオブジェクトです。グループオブジェクトを選択する場合、ジョブはグループのメンバー、またはグループにのみ適用できます。コンテナオブジェクトを選択する場合、ジョブはそのコンテナのすべての子孫、そのコンテナのすべての子、またはそのコンテナにのみ適用できます。

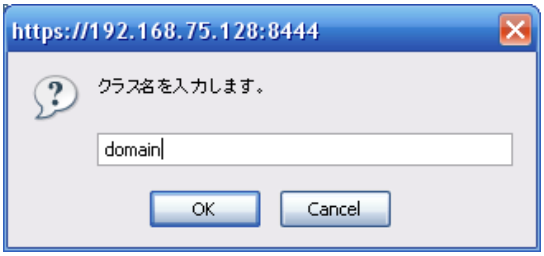
1 ［*追加*］をクリックして、スコープをジョブオブジェクトに追加します。

2 ［ジョブスコープ］ページで、［*参照*］アイコンを使用してオブジェクトを参照します。［*OK*］をクリックして、スコープオブジェクトを追加します。

3 オブジェクトがコンテナの場合は、ジョブを適用する方法を選択します。

- *ジョブをこのコンテナの子孫に適用する*
- *ジョブをこのコンテナの子に適用する*
- *ジョブをこのコンテナのみに適用する*

4 (オプション) [*ジョブをこのコンテナの子に適用する*] または [*このコンテナのすべての子孫にジョブを適用する*] を選択する場合は、スコープするクラスを指定できます。[*Plus (+)*] アイコンをクリックして、[クラス名を入力してください] ページを表示して、スコープするクラスを指定します。[*OK*] をクリックします。



クラスは、［*以下のクラスの 1 つであるオブジェクトにのみジョブを適用します*］ボックスに追加されます。クラスを削除するには、クラスを選択して、［*Minus (-)*］アイコンをクリックします。

5 オブジェクトがグループまたはダイナミックグループの場合、［*ジョブをこのグループのメンバに適用する*］、またはスコープがこのグループ用の場合は［*ジョブをこのグループのみに適用する*］を選択します。

6 スコープの条件を選択したら、［*OK*］をクリックして、スコープジョブを［ジョブスコープ］ページに追加します。

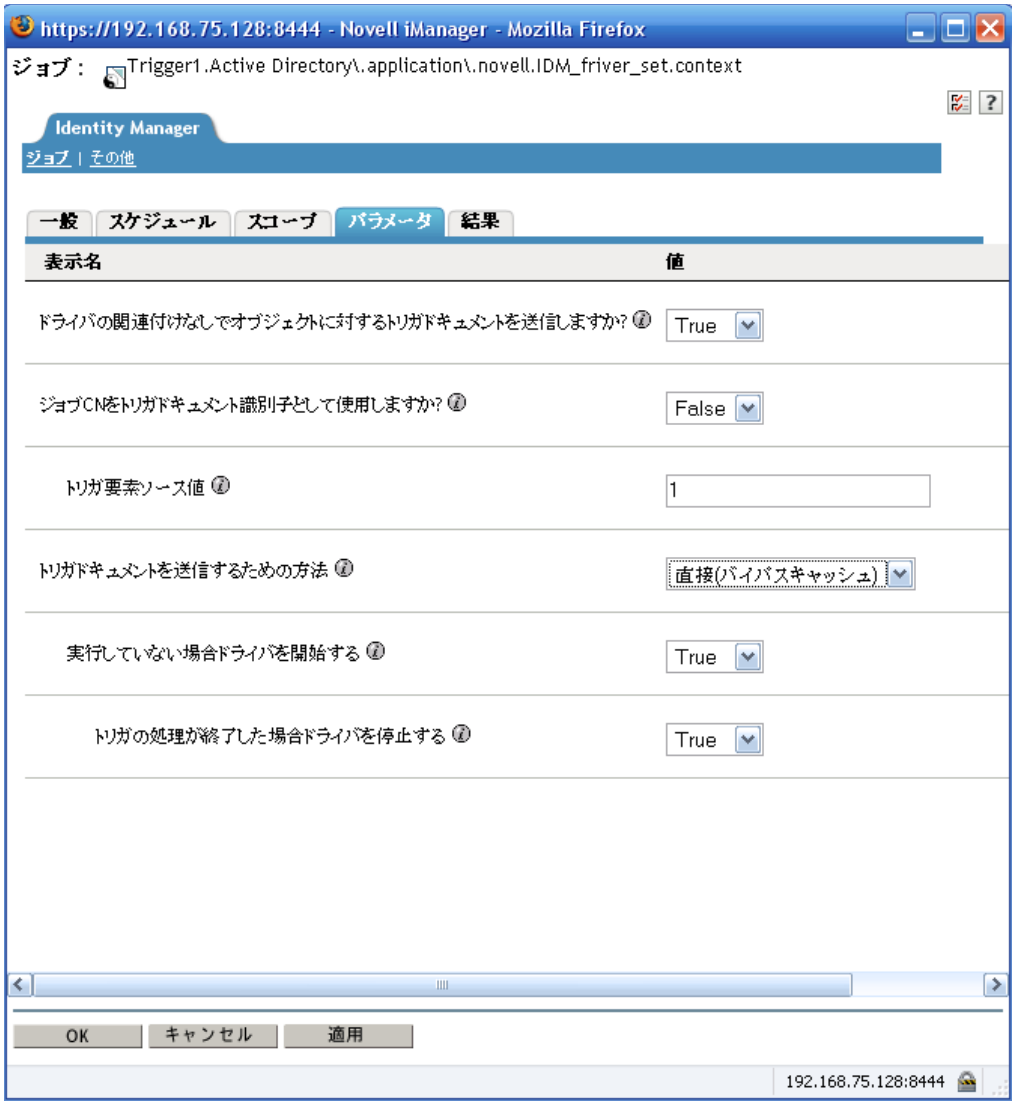
7 スコープを編集する必要がある場合は、スコープ名をクリックします。

8 スコープを削除するには、スコープ名を選択して［*削除*］をクリックします。

［パラメータ］タブで選択する

［パラメータ］ページでは、ジョブがその仕事を実行しているときにそのジョブによって使用されるパラメータを設定できます。実行できる内容は、選択したジョブのタイプによって異なります。次のプロシージャでは、例に購読者チャネルトリガが使用されています。

図 7-12 購読者チャネルトリガジョブの［ジョブパラメータ］ページ



1 ドライバが関連付けられていないスコープオブジェクトのトリガドキュメントを送信する場合は、［*True*］を選択します。それ以外は、デフォルトの［*False*］のままにします。

2 ジョブの CN(共通名) をドキュメント識別子のトリガとして使用する場合は、デフォルトの［*True*］のままにします。それ以外は、［*False*］を選択します。

3 (オプション)［*False*］を選択した場合は、トリガ要素のソース属性の値としてジョブが使用できる文字列を指定します。

4 トリガドキュメントを送信する方法を選択します。トリガ元のジョブをキューに入れる場合は、デフォルトの［*キュー (キャッシュの使用)*］のままにします。それ以外は、［*直接 (バイパスキャッシュ)*］を選択します。

5 (オプション)［*直接 (バイパスキャッシュ)*］を選択した場合、［*実行していない場合ドライバを開始する*］オプションが表示されます。実行していないドライバを開始する場合は、デフォルトの［*True*］のままにします。それ以外は、［*False*］を選択します。

6 (オプション) ［*実行していない場合ドライバを開始する*］オプションで［*True*］を選択した場合、デフォルトの［*True*］が設定された状態で［*トリガの処理が終了した場合ドライバを停止する*］オプションが表示されます。デフォルトの設定を使用して、トリガジョブの処理が終了したらドライバを停止するか、［*False*］を選択してドライバを稼動し続けます。

すべてのジョブ定義には、それぞれ独自のパラメータのセットがあります。

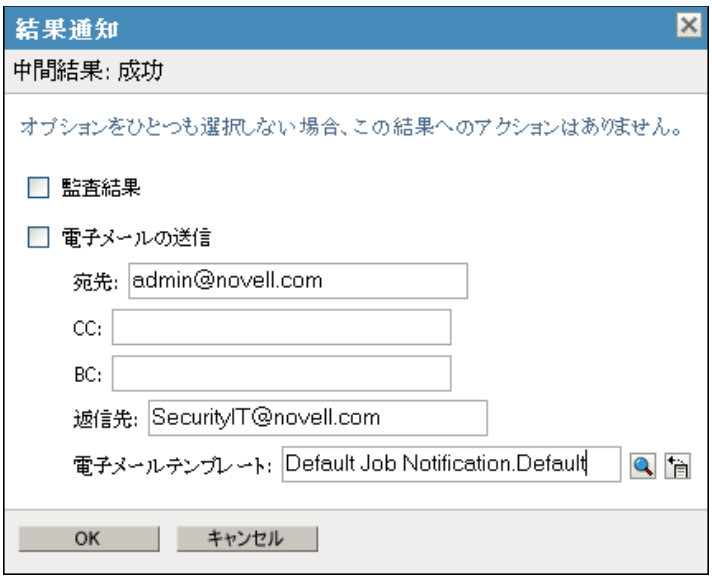
［結果］タブで選択する

［*結果*］タブでは、ジョブの結果で行うことを定義できます。［結果］ページは「*中間結果*」と「*最終結果*」の 2 つの部分で構成されています。それぞれ、次の結果が表示されます。「*成功*」、［*警告*］、「エラー」、および「*中止*」。

［結果］カラムの右側は、［*アクション*］カラムです。［*アクション*］カラムをクリックすると、各結果の通知方法を設定できます。アクションには、「監査結果の送信」、または「結果が出た際に電信メールで送信する」が含まれます。オプションを選択しないと、結果に対するアクションは行われません。

図 7-13 *［結果］タブから通知を受け取るユーザを設定する*

1 ［*アクション*］エントリをクリックして、［結果通知］ページを表示します。



2 ［*電子メールの送信*］で、ユーザまたはグループの電子メール名を入力して、結果を送信する相手を選択します。

［*宛先*］、［*返信先*］、および［*電子メールテンプレート*］フィールドは、プロファイルの必須フィールドです。電子メールテンプレートの完全な識別名は、*Default Job Notification.Default Notification Collection.Security* です。

3 情報を入力し終えたら、［*OK*］をクリックします。

4 結果を Novell Audit に送信する場合は、［*監査結果*］を選択します。

5 ステップ 1 からステップ 4 を各オプションに対して繰り返します。

- *中間的な成功*
- *中間的な警告*
- *中間的なエラー*
- *中間的な中止*
- *最終的な成功*
- *最終的な警告*
- *最終的なエラー*
- *最終的な中止*

オプションを選択しないと、結果に対するアクションは行われません。

Novell Identity Manager 3.5.1 用 Client Login Extension

8

Novell® Identity Manager 3.5.1 用 Client Login Extension を使用すると、Novell および Microsoft* GINA のログインクライアントにリンクを追加することで、パスワードセルフサービスを容易に利用できます。ユーザがログインクライアントで［*パスワードを忘れた場合*］リンクをクリックすると、Client Login Extension によりブラウザが制限付きで起動され、ユーザは Identity Manager ユーザアプリケーションのパスワードセルフサービス機能にアクセスできます。この機能は、パスワードを忘れたユーザがヘルプデスクに問い合わせる件数を削減するのに役立ちます。

Novell Identity Manager 3.5 用の Client Login Extension 設定ユーティリティを実行して、Client Login Extension MSI ファイルを設定します。次にこのファイルを、Novell Client™ ソフトウェアまたは Microsoft GINA を実行しているクライアントワークステーションにインストールします。Client Login Extension は、Windows* XP ワークステーションおよび Windows 2000 ワークステーションで動作します。

Client Login Extension MSI ファイルは、多くの言語で提供されています。英語を含め、各言語の Client Login Extension ファイルは、使用する前に設定する必要があります。

システム管理者は、Client Login Extension 設定ユーティリティを使用して、Client Login Extension MSI ファイルの以下の設定情報を指定できます。

- パスワードセルフサービスの URL を設定できます。
- Microsoft GINA クライアントの場合、「パスワード忘れた場合」などのテキストをパスワードセルフサービスへのリンクに含めることができます。

注 : Novell Identity Manager 3.5 用 Client Login Extension ネイティブの Microsoft GINA および Novell Client 4.91 SP3 以降で動作します。Novell Client 4.91 SP3 以降を除き、Microsoft GINA を変更するアプリケーションでは動作しません。Client Login Extension は、ライセンスされた Novell Identity Manager 3.5 システムでテストおよび使用されています。

以下のステップを順に実行して、Client Login Extension 設定ユーティリティをインストールし、このユーティリティを使用して、Client Login Extension MSI ファイルを設定できます。Client Login Extension MSI ファイルを使用するための説明も含まれています。

- 238 ページのセクション 8.1「Novell Identity Manager 3.5 用 Client Login Extension を実行する準備をする」
- 238 ページのセクション 8.2「Novell Identity Manager 3.5 用 Client Login Extension 設定ユーティリティをインストールする」
- 243 ページのセクション 8.3「Client Login Extension 設定ユーティリティを使用して、Client Login Extension MSI ファイルを設定する」
- 247 ページのセクション 8.4「Client Login Extension MSI ファイルをインストールする」
- 249 ページのセクション 8.5「パスワードを忘れた場合機能を使用する」

8.1 Novell Identity Manager 3.5 用 Client Login Extension を実行する準備をする

Client Login Extension を実行する前には、Identity Manager 3.5 システムを稼動し、パスワードセルフサービス機能を有効にするユーザアプリケーションを正しく設定している必要があります。(Identity Manager 3.5 およびユーザアプリケーションをインストールする方法の詳細については、『*Identity Manager 3.5.1 Installation Guide*』を参照してください。)

パスワードセルフサービス機能を有効にするためには、以下を実行する必要があります。

- ユニバーサルパスワードを有効にする
- パスワードポリシーを作成する、または既存のパスワードポリシーを選択する
- ［パスワードを忘れた場合］オプションを有効にして、設定する
- 適切なユーザ、グループ、またはコンテナにパスワードポリシーを割り当てる
- SSL を有効にする

まず、［*パスワード*］>［*パスワードポリシー*］>［*パスワードを忘れた場合*］オプションの順に選択し、［*ポリシーの割り当て*］オプションを選択して、iManager を介してパスワードセルフサービス機能を設定します。パスワードセルフサービス機能の詳細については、『Novell Password Management Administration Guide (http://www.novell.com/documentation/password_management31/index.html)』の第 3 章「パスワードポリシーを使用したパスワードの管理」および第 4 章の「パスワードセルフサービス」を参照していください。

Identity Manager ユーザアプリケーションを使用して、パスワード設定を完了します。Identity Manager ユーザアプリケーションを使用した、パスワードセルフサービスの設定の詳細については、『Identity Manager 3.5 User Application: Administration Guide (http://www.novell.com/documentation/idm35/index.html)』の項 5.3「パスワード管理の設定」を参照してください。

JBoss* で SSL をオンにする必要もあります。『Identity Manager 3.5 User Application: Administration Guide (http://www.novell.com/documentation/idm35/index.html)』の項 2.2.2「自己署名証明書」および 2.2.3「JBoss で SSL をオンにする」を参照してください。Client Login Extension は、SSL をオンにしないと機能しません。

［パスワードを忘れた場合］機能を有効にし、パスワードポリシーを割り当てると、使用する制限付きブラウザへの有効な HTML リンクが確立されます。このリンクは、https://hostname:8443/IDM/jsps/pwdmgt/ForgotPassword.jsf 次のような HTTPS に対して設定する必要があります。Client Login Extension 設定ユーティリティを使用するときは、この URL を使用します。

8.2 Novell Identity Manager 3.5 用 Client Login Extension 設定ユーティリティをインストールする

Novell のダウンロードページ (http://download.novell.com/index.jsp) から idmcle.exe ファイルをダウンロードする必要があります。［製品］または［テクノロジ］で［*Identity Manager*］を選択し、［*検索*］をクリックするか、［キーワード］で「*Client Login Extensiton*」と入力して［*検索*］をクリックします。［*Novell Identity Manager 3.5 用 Client Login Extension*］を選択してダウンロードし、ステップに従い idmcle.exe ファイルをダウンロードします。

ファイルがダウンロードされたら、idmcle.exe ファイルをダブルクリックして、Client Login Extension 設定ユーティリティのファイルおよび Client Login Extension MSI ファイルのファイルをインストールします。このプロセスでは ,NET プラットフォームもインストールされます (すでにインストールされていない場合)。

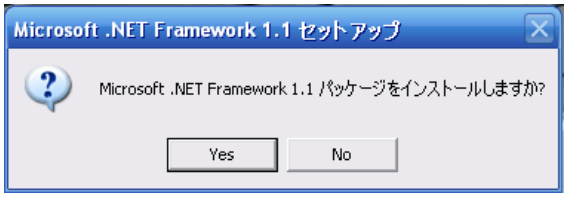
idmcle.exe ファイルから、以下のファイルを含む idmcle フォルダが作成されます。

- ClientLoginExtensionConfigurationUtilitySetup.msi
- Config.ini
- dotnetfx.exe
- Settings.ini
- Setup.exe

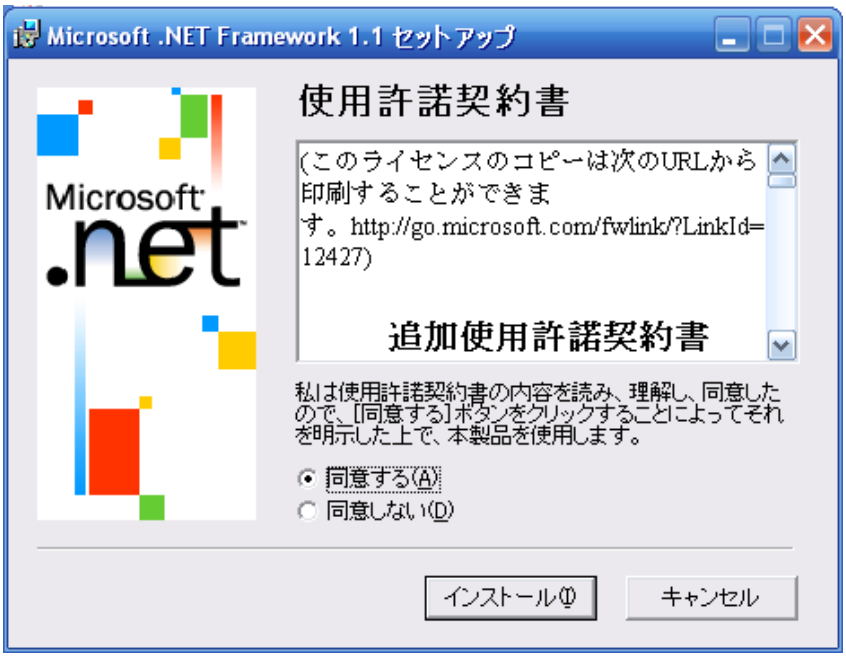
Client Login Extension をインストールする

1 idmcle フォルダから Setup.exe を実行して、Client Login Extension 設定ユーティリティインストーラを起動します。

2 ［*OK*］をクリックして、インストールを続行します。インストーラにより、このマシンに .NET プラットフォームがインストールされているかどうかがチェックされます。.NET がインストールされている場合、ステップ 5 に進みます。インストールされていない場合、次のダイアログボックスが表示されます。

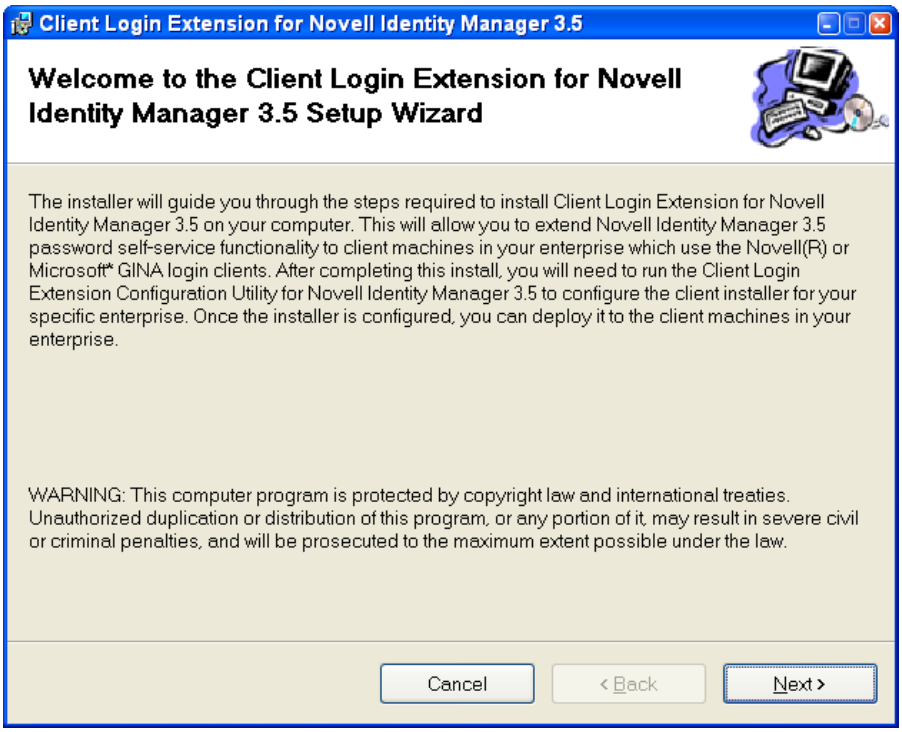


3 ［*はい*］をクリックして、Microsoft .NET Framework をインストールします。



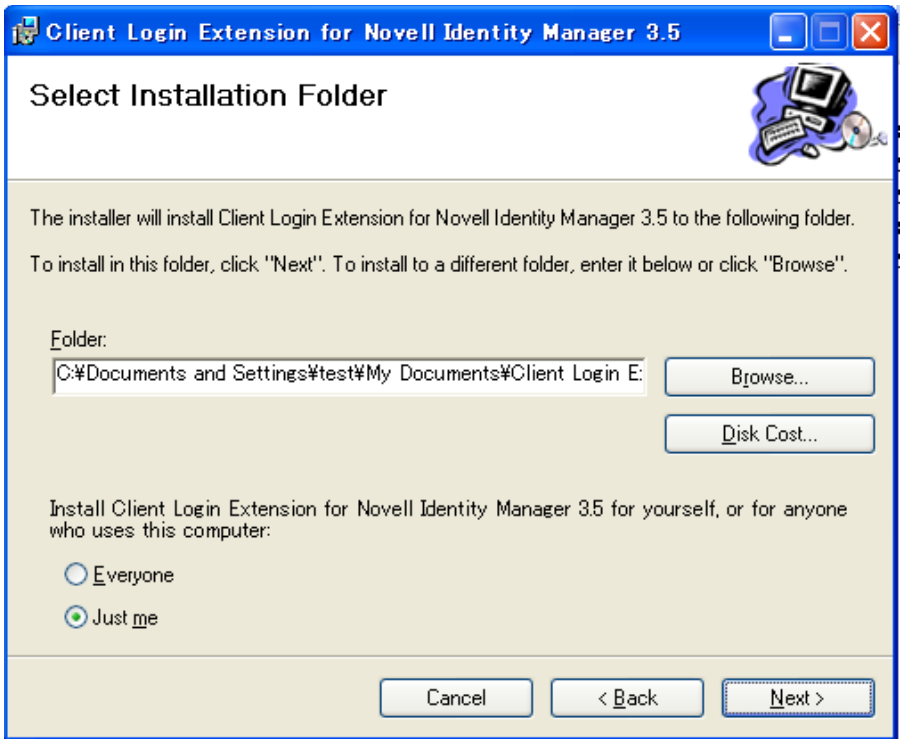
4 ［*同意する*］をクリックして、［*インストール*］をクリックします。

.NET Framework がインストールされると、Novell Identity Manager 3.5 用 Client Login Extension のセットアップウィザードが起動します。



5 ウィザードの先頭ページの情報を読み、［*次へ*］をクリックします。

6 ［使用許諾書］ページで、使用許諾書を読みます。同意する場合は、［*同意する*］をクリックして、［*次へ*］をクリックします。



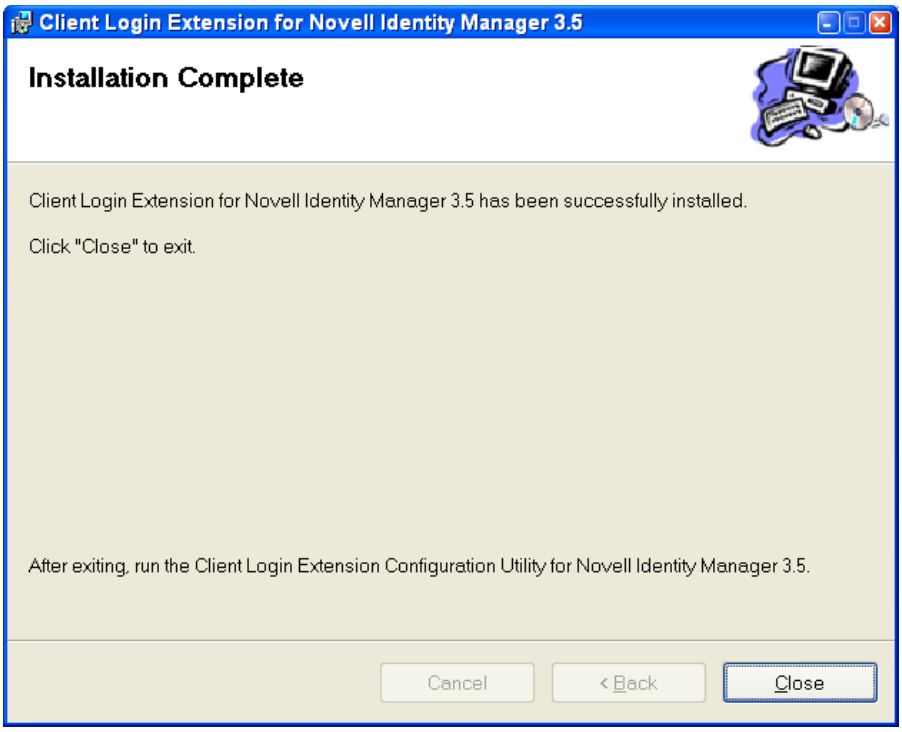
7 ［インストールフォルダの選択］ページで、デフォルトのディレクトリを使用するか、［*参照*］をクリックして別のディレクトリを選択します。

デフォルトのディレクトリは、C:\Documents and Settings\Username\My Documents\Client Login Extension Configuration Utility for Novell Identity Manager 3.5 です。

現在ログインしているユーザ、またはこのマシンを使用する他のユーザのショートカットを作成することを選択することもできます。デフォルトは、［*Just me*］です。

8 ［*次へ*］をクリックします。

9 ［インストールの確認］ページで、［*次へ*］をクリックして、Client Login Extension 設定ユーティリティおよび Client Login Extension ファイルをインストールします。



10 インストールが完了したら、［*閉じる*］をクリックして、［*OK*］をクリックします。

インストール処理により、ClientLoginExtensionConfigurationUtility.exe への 2 つのショートカットが作成されます。1 つはデスクトップ用で、もう 1 つは［*すべてのプログラム*］メニュー用です。インストール処理により、インストールフォルダに以下のフォルダとファイルがインストールされます。

- ClientLoginExtensionConfigurationUtility.exe
- Interop.WindowsInstaller.dll
- license.rtf
- Installer/
  - IdentityManagerClientLoginExtension_en.msi (英語 (デフォルト))
  - IdentityManagerClientLoginExtension_de.msi (ドイツ語)
  - IdentityManagerClientLoginExtension_es.msi (スペイン語)
  - IdentityManagerClientLoginExtension_fr.msi (フランス語)
  - IdentityManagerClientLoginExtension_it.msi (イタリア語)
  - IdentityManagerClientLoginExtension_ja.msi (日本語)
  - IdentityManagerClientLoginExtension_zh_CN.msi (中国語マンダリン)
  - IdentityManagerClientLoginExtension_zh_TW.msi (繁体字中国語)

11 243 ページのセクション 8.3「Client Login Extension 設定ユーティリティを使用して、Client Login Extension MSI ファイルを設定する」に進みます。

8.2.1 Novell Identity Manager 3.5 用 Client Login Extension 設定ユーティリティをアンインストールする

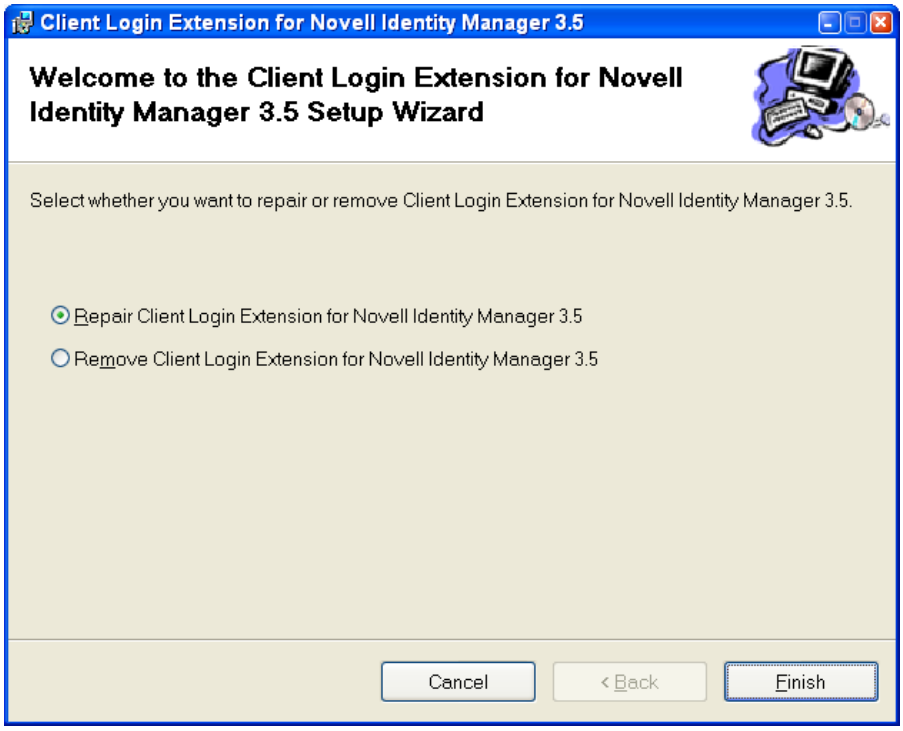
設定ユーティリティをアンインストールする

［プログラムの追加と削除］を使用して、設定ユーティリティをアンインストールする

1 コントロールパネルで［プログラムの追加と削除］ダイアログボックスを開き、［*Novell Identity Manager 3.5 用 Client Login Extension 設定ユーティリティ*］を選択します。次に［*削除*］をクリックします。

セットアップウィザードを使用して、設定ユーティリティをアンインストールする

1 Novell Identity Manager 3.5 用 Client Login Extension セットアップウィザードを再起動するには、Setup.exe を再度実行します。

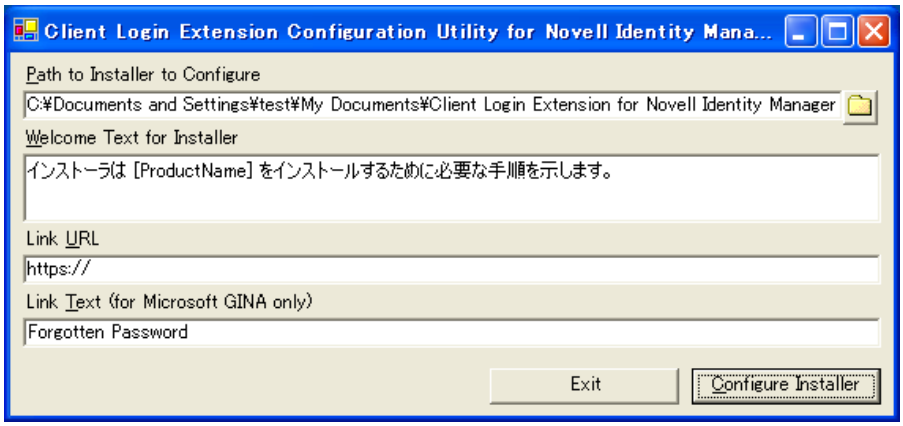


2 *Novell Identity Manager 3.5 用 Client Login Extension の削除*］オプションを選択して、［*完了*］をクリックします。

8.3 Client Login Extension 設定ユーティリティを使用して、Client Login Extension MSI ファイルを設定する

1 ［*Novell Identity Manager 3.5 用 Client Login Extension 設定ユーティリティ*］ショートカットをクリックして、Client Login Extension 設定ユーティリティを起動します。

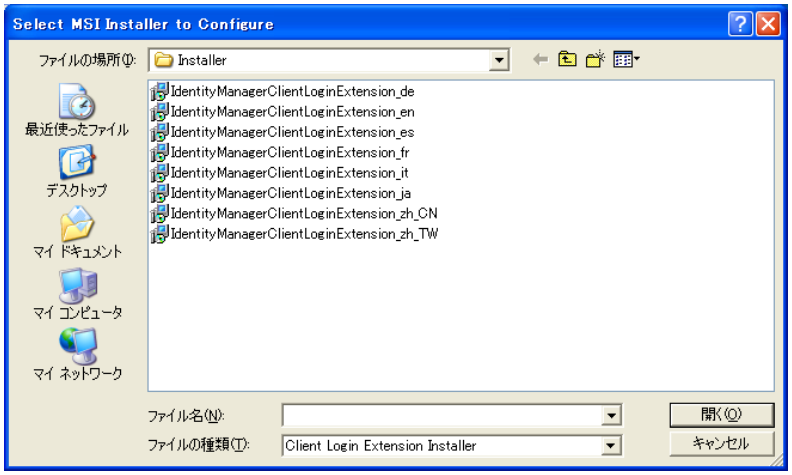
または、ClientLoginExtensionConfigurationUtility.exe ファイルをダブルクリックして、ユーティリティを起動します。



［*設定するインストーラへのパス*］オプションに、設定されている Client Login Extension インストーラの英語バージョンへのパスが表示されます。このテキストボックスに有効な MSI ファイルへのパスが含まれている場合は常に、ユーティリティにより自動的にファイルが開かれ、ファイルに含まれる情報とともに他のコントロールが表示され、［*インストーラの設定*］ボタンが有効になります。

2 (オプション) 他の言語を選択する場合は、［*参照*］ボタンをクリックして、別の言語の Client Login Extension インストーラファイルを選択します。

デフォルトでは、［*参照*］ボタンをクリックすると、インストールフォルダ内のインストーラサブフォルダが開き、Client Login Extension インストーラのパターンに一致するすべてのファイルが表示されます。



3 「ようこそ」テキストの情報を変更するか、そのままの状態で保存します。

このテキストボックスの情報は、Client Login Extension のようこそ画面に表示されます。文字列 *[ProductName]* には、「*Novell Identity Manager 3.5 用 Client Login Extension*」と表示されます。

4 Client Login Extension の制限付きブラウザで、ユーザアプリケーションの［パスワードを忘れた場合］ページに接続するための URL を指定します。DNS 名または IP ア

ドレスを使用できます。［パスワードを忘れた場合］ページにリンクする DNS 名を使用している URL の例を次に示します。

https://hostname:8443/IDM/jsps/pwdmgt/ForgotPassword.jsf

これは、外部パスワード WAR にアクセスするためにも設定できます。この設定を行うには、『Identity Manager 3.5 Installation Guide (http://www.novell.com/documentation/idm35/index.html)』の項 5.8.4「外部パスワード WAR にアクセスする」を参照してください。

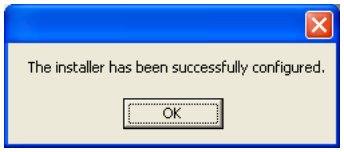
重要 : ユーザアプリケーションの［パスワードを忘れた場合］ページをポイントしている有効な URL が必要です。URL がない場合、クライアントの接続が失敗し、ワークステーションからログインできないことがあります。詳細については、251 ページのセクション 8.5.1「トラブルシューティング」を参照してください。

---

5 Microsoft GINA を使用しているワークステーションがある場合は、Client Login Extension で使用される制限付きブラウザへのリンクに表示されるテキストを指定します。

デフォルトのテキストは「*パスワードを忘れた場合*」です。Novell クライアント内のボタンのテキストは、Novell クライアントより表示されているものなので、ここでは変更できません。

6 すべての情報を入力したら、［*インストーラの設定*］をクリックして、新しい設定の設定を選択した Client Login Extension ファイルに書き込みます。



7 ［*OK*］をクリックして確認メッセージを閉じます。

8 Client Login Extension 設定ユーティリティは開いたままなので、別の Client Login Extension MSI ファイルを他の言語で設定できます。この設定を行うには、*設定するインストーラへのパス*］オプションの右側にある［*参照*］ボタンをクリックして、別の言語を選択して、他のファイルを設定します。244 ページのステップ 2 から 245 ページのステップ 7 の手順に従い、msi ファイルを設定します。

一般的な言語用のローカライズされた Client Login Extension MSI ファイルが、設定ユーティリティによりインストーラフォルダに配置されます。ローカライズされた各インストーラは個別に設定する必要があります。

Client Login Extension で提供される言語以外の Client Login Extension MSI ファイルをローカライズする方法については、246 ページのセクション 8.3.1「他の言語の Client Login Extension ファイルをローカライズする」を参照してください。.

9 Novell Identity Manager 3.5 用 Client Login Extension 設定ユーティリティウィンドウを閉じるには、［*終了*］をクリックします。

注 : Client Login Extension MSI ファイルは、Client Login Extension 設定ユーティリティで開いている間は実行できません。

8.3.1 他の言語の Client Login Extension ファイルをローカライズする

Client Login Extension 設定ユーティリティで提供される以外の言語の Client Login Extension をローカライズするには、Orca を使用して、MSI データベースのコンテンツを直接編集できます (IdentityManagerClientLoginExtension.msi)。

Orca (Orca.exe) (http://msdn2.microsoft.com/en-us/library/aa370557.aspx) は、Windows インストーラパッケージを作成および編集するためのデータベーステーブルエディタです、Orca は、Windows SDK Components for Windows Installer Developers (http://msdn2.microsoft.com/en-us/library/aa370834.aspx) から利用できます。

IdentityManagerClientLoginExtension.msi 用にローカライズするテキストは、以下の表にあります。

表 8-1 *ローカライズする必要があるテキスト*

テーブル	列	コメント
コントロール	テキスト	
Dialog	役職	
ディレクトリ	DefaultDir	“|” の後にテキストを入力します。
起動条件	説明	
プロパティ	値	ProductName、Manufacturer、ARPCONTACT、および VSDVERSIONMSG のみ。
RadioButton	テキスト	
レジストリ	値	set LogFile、LinkURL、LinkText、PasswordComplexityText、および LoginExtDesc が設定ユーティリティのデフォルトです。
Shortcut	名前	“|” の後にテキストを入力します。
Shortcut	説明	Null でない場合。
UIText	テキスト	

警告 : ユーザインタフェーステキストのみ翻訳します。たとえば、角括弧で囲まれているテキスト ([xxxx]) や大文字と小文字が混ざっているテキスト (XxxXxxXxx) は翻訳しないでください。インストーラを中断するプロパティ名と識別子を変更します。

以下のプロシージャを使用して、Client Login Extension MSI ファイルを新しい言語にローカライズします。

1 IdentityManagerClientLoginExtension.msi を IdentityManagerClientLoginExtension_ *xx*.msi にコピーします。ここで、*xx* は新しい言語 (ロケール) の識別子です。

2 IdentityManagerClientLoginExtension_ *xx*.msi を Orca.exe で開き、246 ページの 表 8-1 に表示されているテーブルとカラムを編集してローカライズしたテキストを挿入し、ファイルを保存して閉じます。

3 IdentityManagerClientLoginExtension_ *xx*.msi を、Client Login Extension 設定ユーティリティ (ClientLoginExtensionConfigurationUtility.exe) で開き、デフォルト値を確認し、必要に応じて変更を加えて、*インストーラの設定*］をクリックします。

注 : レジストリテーブルに設定したデフォルト値を編集する必要がない場合でも、ステップ 3 は必須です。Client Login Extension 設定ユーティリティを使用して、Client Login Extension MSI ファイルを有効にする変更を加えます。

8.4 Client Login Extension MSI ファイルをインストールする

Client Login Extension MSI ファイルを設定すると、IdentityManagerClientLoginExtension_xx.msi ファイル (またはその配布名) をユーザまたは配布メカニズムに配布できます。*xx* は言語 (ロケール) の識別子です。IdentityManagerClientLoginExtension_xx.msi ファイルは、インストーラフォルダにあります。

Client Login Extension MSI ファイルを実行する予定のすべてのワークステーションに、Microsoft .NET Framework をインストールする必要もあります。バージョンの一致を保つには、Client Login Extension 機能に付属している dotnetfx.exe ファイルを使用します。このファイルは idmcle フォルダにあります。

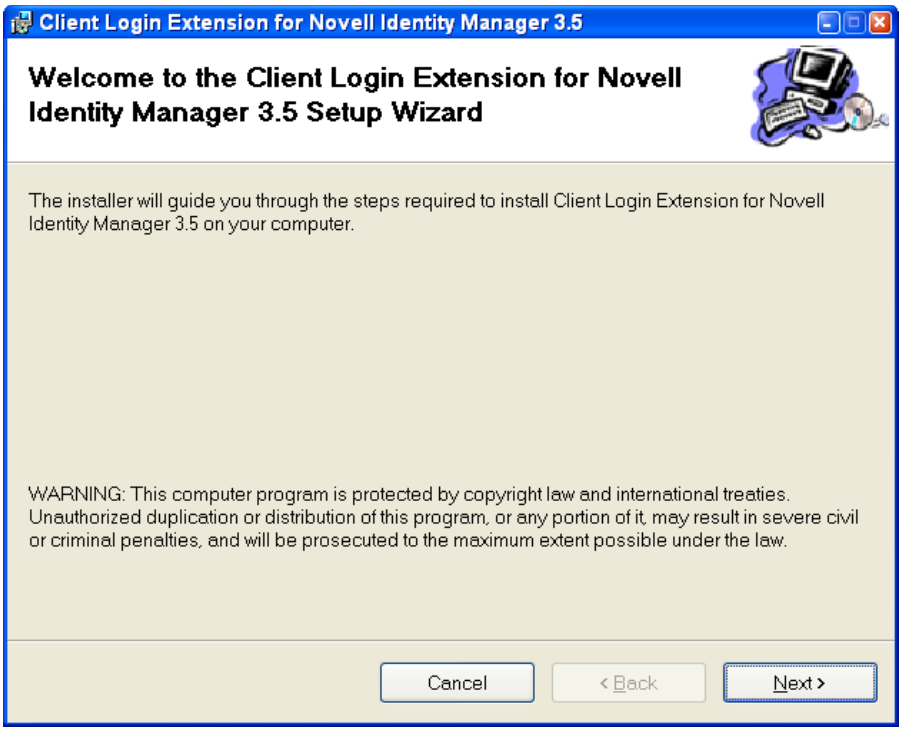
注 : Client Login Extension は、ネイティブの Microsoft GINA および Novell Client 4.91 SP3 でのみ動作します。Novell Client 4.91 SP3 を除き、Microsoft GINA を変更するアプリケーションでは動作しません。Client Login Extension は、Windows XP ワークステーションおよび Windows 2000 ワークステーションで動作します。

---

1 Client Login Extension MSI ファイルを実行する予定の各ワークステーションで、dotnetfx.exe ファイルを実行して Microsoft .NET Framework をインストールします。238 ページのセクション 8.2「Novell Identity Manager 3.5 用 Client Login Extension 設定ユーティリティをインストールする」のステップ 2 を参照してください。

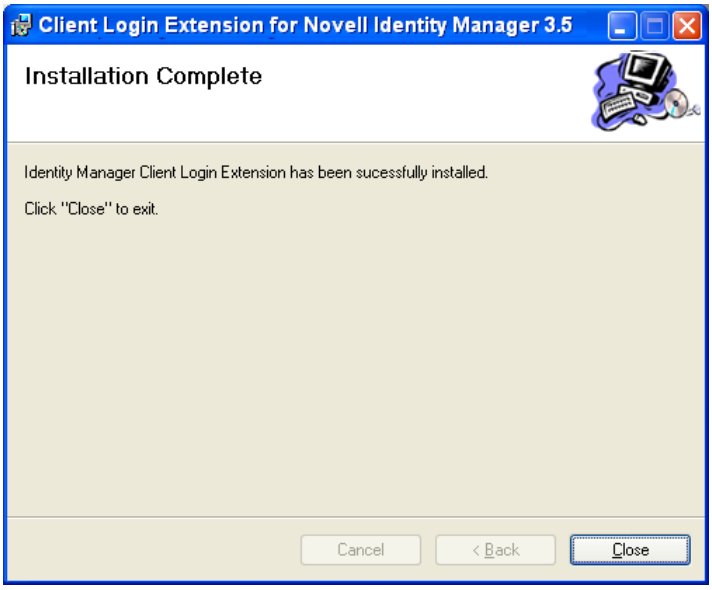
2 Microsoft .NET Framework をインストール後、IdentityManagerClientLoginExtension_xx.msi ファイルをダブルクリックして、Client Login Extension のようこそページを開きます。

ようこそメッセージは、Client Login Extension 設定ユーティリティで入力したテキストです。



3 ［*次へ*］をクリックして、インストールをスタートします。

4 Client Login Extension がインストールされたら、［*閉じる*］をクリックします。



5 (オプション)Client Login Extension をアンインストールするには、コントロールパネルの［プログラムの追加と削除］ダイアログボックスを開き、［*Novell Identity Manager 3.5 用 Client Login Extension*］をクリックして［*削除*］をクリックします。

8.4.1 Client Login Extension インストーラのコマンドラインオプションを使用する

Client Login Extension MSI ファイルは、標準の MSI インストーラです。これは、msdn (http://msdn2.microsoft.com/en-us/library/aa367988.aspx) にある標準の Msiexec.exe コマンドラインオプションのいずれとでも使用できます。いくつかの例を以下に示します。

Client Login Extension MSI ファイル (ユーザインタフェースなし) をインストールするには、コマンドラインに以下のコマンドを入力します。

msiexec /i IdentityManagerClientLoginExtension_en.msi /q

または

IdentityManagerClientLoginExtension_en.msi /q

最後に表示されるモーダルダイアログボックスを除き、ユーザインタフェースのないファイルをインストールするには、次のコマンドを入力します。

msiexec /i IdentityManagerClientLoginExtension_en.msi /qn+

または

IdentityManagerClientLoginExtension_en.msi /qn+

ユーザインタフェースのないファイルをアンインストールするには、次のコマンドを入力します。

msiexec /x IdentityManagerClientLoginExtension_en.msi /q

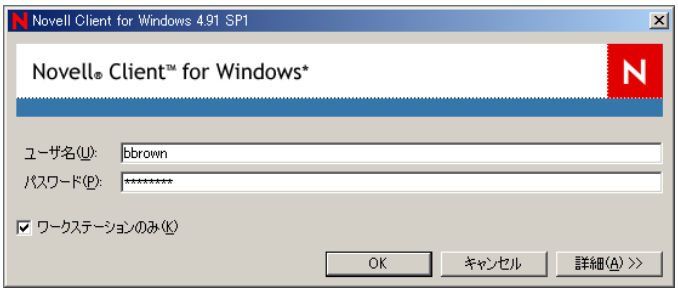
最後に表示されるモーダルダイアログボックスを除き、ユーザインタフェースのないファイルをアンインストールするには、次のコマンドを入力します。

msiexec /x IdentityManagerClientLoginExtension_en.msi /qn+

8.5 パスワードを忘れた場合機能を使用する

Novell Client 4.91 SP3 または Microsoft GINA を実行しているワークステーションで Client Login Extension MSI ファイルを実行し、有効な HTTPS リンクを指定すると、パスワードセルフサービス機能が使用できるようになります。(238 ページのセクション 8.1「Novell Identity Manager 3.5 用 Client Login Extension を実行する準備をする」を参照して、パスワードセルフサービスを機能させるためのすべての情報を設定していることを確認してください)。

1 パスワードを忘れた場合は、Novell クライアントで［*パスワードを忘れましたか ?*］リンクをクリックしてください。

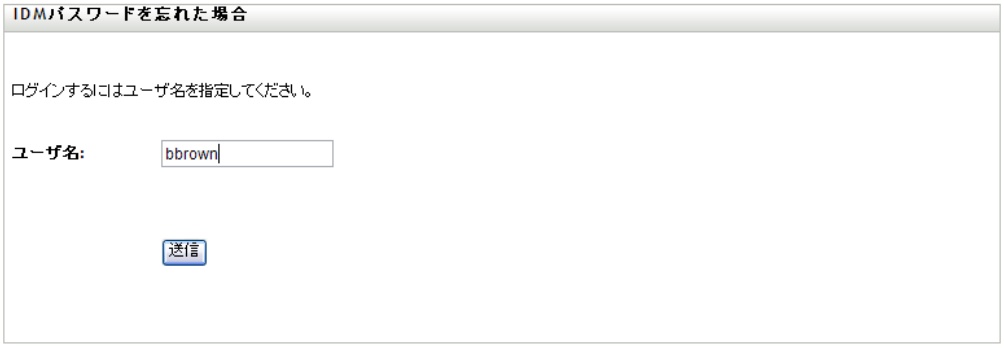


Client Login Extension を設定すると、Microsoft GINA のリンクに「*パスワードを忘れた場合*」、またはユーザが入力したテキストが表示されます。

［*パスワードを忘れましたか*］リンクをクリックして、制限付きブラウザを起動します。このブラウザからは、Client Login Extension 設定ユーティリティで指定した URL にのみアクセスできます。制限付きブラウザでは以下のことを実行できます。

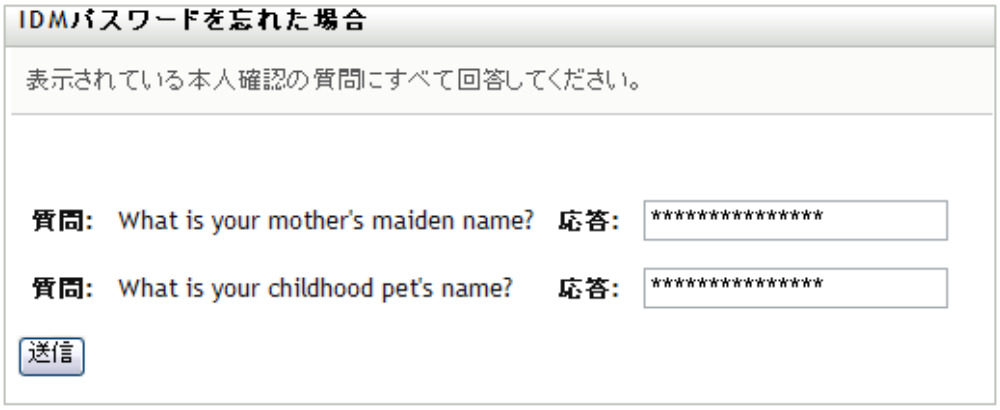
- プロトコルが HTTPS であることを確認する
- ホスト名を検証する
- ターゲット Web サイトが Internet Explorer の制限付きサイトゾーンで運営されていることを確認する
- ホットキーを無効にする
- タブを無効にする
- 右クリックを無効にする
- ActiveX* を無効にする
- スクリプトを無効にする
- Winlogon プロセスとは切り離されている独自のプロセスを実行する

2 制限付きブラウザで［パスワードを忘れた場合］ページを開くと、［IDM パスワードを忘れた場合］ダイアログボックスが表示されます。ログイン名を入力して、［*送信*］をクリックします。



［IDM パスワードを忘れた場合］ダイアログボックスが表示されるタイミングは、システム管理者による［パスワードを忘れた場合］オプションの設定方法によって異なります。ヒントが表示される、ヒントが電子メールで送信される、パスワードが電子メールで送信される、またはパスワードの変更が許可されます。本人確認の質問が与えられることもあります。

この例では、ユーザには本人確認の質問とヒントが与えられています。

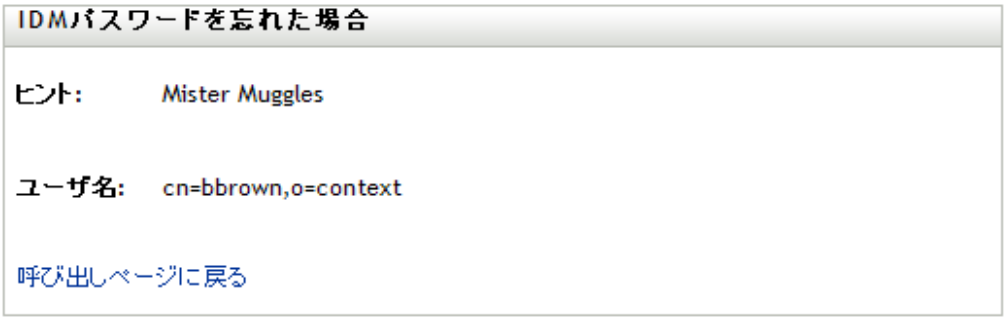


3 質問に対する回答を入力して、[*送信*] をクリックします。

質問の数と質問の内容は、システム管理者が設定できます。

質問に正確に回答しない場合、「*本人確認の回答に失敗しました*」というメッセージが表示され、もう一度質問が表示されます。

4 質問に正確に回答すると、システム管理者がパスワードセルフサービスを設定した方法に応じてパスワードのヒントが表示されます。



5 ブラウザを閉じます (ブラウザは制限付きのため、*呼び出しページに戻る* リンクが機能しないためです)。ヒントを使用して、パスワードを思い出します。それでもパスワードを思い出せない場合は、システム管理者に連絡してください。

8.5.1 トラブルシューティング

[パスワードを忘れた場合] 機能を使用する際には、以下の情報を覚えておいてください。

- システム管理者により、このプロセスを介したパスワードの変更が許可されている場合、すべての変更がネットワーク全体に行き渡るには 15 分以上かかります。すぐにシステム管理者に連絡せずに待機してください。
- Novell クライアントを使用していて、すでにネットワークにログインしている場合は、タスクバーにある赤い [N] を右クリックして、[*NetWare ログイン*] を選択し、[*パスワードを忘れましたか ?*] リンクを選択します。制限付きブラウザは起動しません。Client Login Extension は、ログインしていないときのみ適用されます。
- Identity Manager のユーザアプリケーションを実行しているサーバがダウンしているときに、*パスワードを忘れましたか ?*] リンクを選択すると、制限付きブラウザの最初

のページに赤字で「*エラーが発生しました*」というメッセージが表示されます。システム管理者に問い合わせてください。

- Identity Manager の外部 WAR を実行しているサーバがダウンしているときに、*パスワードを忘れましたか?*］リンクを選択すると、制限付きブラウザの最初のページに「*ページが見つかりません*」というメッセージが表示されます。システム管理者に問い合わせてください。
- ［IDM パスワードを忘れた場合］ページの URL の設定が間違っている場合に、［*パスワードを忘れましたか?*］リンクを選択すると、制限付きブラウザの最初のページに「*ページが見つかりません*」というメッセージが表示されます。システム管理者に問い合わせてください。

セキュリティ：ベストプラクティス 9

9.1 SSL の使用

SSL が使用できる場合は、すべての転送に対して有効する必要があります。SSL は、メタディレクトリエンジンとリモートローダ (55 ページのセクション 3.2「安全なデータ転送の提供」を参照) の間、メタディレクトリエンジンまたはリモートローダと接続システムの間で有効にする必要があります。

SSL を有効にしないと、パスワードなどの情報をクリアテキスト形式で送信することになります。

9.2 アクセスのセキュリティ保護

識別 \'83\'7bールトおよび Identity Manager のオブジェクトに対するアクセスについては、セキュリティ保護を実行します。

物理的なセキュリティ - 識別 \'83\'7bールトがインストールされた物理的なサーバがある場所へのアクセスを保護します。

アクセス権 - Identity Manager には、Identity Manager のオブジェクトを作成し、ドライバを設定するための管理権が必要です。次を作成または変更する権限を持つユーザを監視および制御します。

- Identity Manager ドライバセット
- Identity Manager ドライバ
- ドライバ設定オブジェクト (フィルタ、スタイルシート、ポリシー)。特に、パスワードの取得または同期に使用するポリシー。
- パスワードポリシーオブジェクト (およびこれらを編集するための iManager タスク)。これらのオブジェクトは、相互に同期するパスワードと、使用するパスワードセルフサービスオプションを制御しているためです。

9.2.1 タスクベースのアクセスをドライバとドライバセットに付与する

eDirectory の標準のオブジェクトベースのアクセスコントロールに加え、Identity Manager では、完全なスーパバイザ権をドライバオブジェクトに与えるのではなく、Identity

Manager ドライバで特定のタスクのみ実行するためのトラスティ権利を割り当てることができます。たとえば、あるユーザはドライバオブジェクトの設定 (オブジェクトプロパティの作成および変更) のみでき、他のユーザはドライバの開始と停止のみできるというようなトラスティ権利を割り当てることができます。

Identity Manager には、役割ベースのアクセスを可能にする以下のドライバオブジェクト属性が用意されています。

属性	説明
DirXML-AccessRun	Identity Manager ドライバとジョブを開始および停止します
DirXML-AccessMigrate	識別ボールトへの移行操作を管理します
DirXML-AccessSubmitCommand	ドライバのパススルーコマンドを管理します
DirXML-AccessCheckObjectPassword	ドライバの「オブジェクトパスワードの確認」コマンドを管理します
DirXML-AccessConfigure	ドライバおよびジョブの設定を管理します
DirXML-AccessManage	ドライバのキャッシュファイルの内容を表示および変更します

これらの属性にトラスティ権利を設定すると、Identity Manager の verb および sub-verb へのアクセスが付与されます。読み込みアクセス権では状態の表示 (verb 状態の取得)、書き込みアクセス権では状態の変更 (verb 状態の設定) ができます。たとえば、読み込みアクセス権をドライバオブジェクトの DirXML-AccessRun 属性に付与すると、ユーザはドライバの状態 (開始または停止) を取得できます。書き込みアクセス権を付与すると、ユーザはドライバ状態を設定できます (開始を停止に変更する、または停止を開始に変更する)。

属性ベースのアクセスをドライバのタスクに割り当てる目的は、明確な管理者の役割を作成し、場合によっては eDirectory の管理者の役割オブジェクトを使用して、すべての管理機能を公開することなく、ユーザが特定の管理タスクを実行できるようにすることにあります。これらの役割を作成することは、上述の DirXML-Access 属性にアクセス権を提供する以上の権利を付与することになり、他の属性へのアクセス権、および他の Identity Manager オブジェクトへのアクセス権を含めることができます。以下の例は、管理者の役割の作成における柔軟性を示しています。

ドライバの開始 / 停止管理者 この管理者の役割を割り当てられたユーザは、特定のドライバセットにあるすべてのドライバを開始および停止できます。この役割には、以下のアクセス権が必要です。

- ドライバセットオブジェクトの参照権
- ドライバセットオブジェクトの DirXML-AccessRun への読み書き権 (継承あり)

ドライバ管理者 この管理者の役割を割り当てられたユーザは、単一のドライバオブジェクトを管理できます。この役割には、以下のアクセス権が必要です。

- ドライバオブジェクトの参照および作成権
- ドライバオブジェクトの [すべての属性の権利] への読み書き権

注 : これらの権利が継承されていることを確認し、ドライバ管理者がドライバのポリシーオブジェクトも管理できるようにします。

iManager を使用して、eDirectory のアクセス権を付与する方法の詳細については、『iManager Administration Guide (http://www.novell.com/documentation/imanager26/imanager_admin_26/data/bu0906q.html)』を参照してください。

9.3 パスワードを管理する

接続システム間で情報を交換する場合は、交換のセキュリティを確保するために、予防措置をとる必要があります。特にパスワードにはセキュリティが必要です。

- パスワードヒント属性 (nsimHint) もパブリックに読み込み可能で、これによって、パスワードを忘れた認証を受けていないユーザが自分のヒントにアクセスできます。パスワードヒントを使用すると、ヘルプデスクへの問い合わせの手間を削減できます。

  セキュリティのため、パスワードヒントは、ユーザの実際のパスワードが含まれていないかどうかチェックされます。ただし、パスワードについて多くの情報を与えるパスワードヒントを作成することはできます。

  パスワードヒントの使用時にセキュリティを強化するには、次の点に注意してください。

  - パスワードセルフサービスに使用されている LDAP サーバ上の nsimHint 属性にのみアクセスを許可する。
  - パスワードヒントを受け取る前にユーザがチャレンジ質問に答えることを要求する。
  - 自分だけが理解できるパスワードヒントを作成するようユーザに注意する。パスワードポリシーの［パスワード変更メッセージ］は、これを実行する 1 つの方法です。『パスワード管理ガイド (http://www.novell.com/documentation/password_management/index.html)』の「Adding a Password Change Message」を参照してください。

  パスワードヒントをまったく使用しないよう選択した場合は、どのパスワードポリシーでもパスワードヒントを使用していないことを確認します。パスワードヒントの設定をしないようにするには、先に進んでから、『パスワードの管理ガイド (http://www.novell.com/documentation/password_management/index.html)』の「Disabling Password Hint by Removing the Hint Gadget」の説明に従い、パスワードヒントガジェットを完全に削除します。

- 本人確認の質問はパブリックに読み込み可能です。これは、パスワードを忘れた認証されていないユーザが別の方法で認証を受けることができるようにするためです。チャレンジ質問を要求することで、パスワードを忘れた場合のセルフサービスのセキュリティが向上します。これは、忘れたパスワードまたはパスワードヒントを受け取る前、またはパスワードをリセットする前に、正しく回答することによってユーザが自らの識別情報を証明する必要があるためです。

  チャレンジ質問には不正侵入者ロックアウト設定が適用されるため、不正侵入者による不正な試行回数は制限されています。

  ただし、ユーザはパスワードの手がかりを含む本人確認の質問を作成できます。本人だけが理解できる本人確認の質問と回答を作成するように徹底してください。パスワードポリシーの［パスワード変更メッセージ］は、これを実行する 1 つの方法です。『Password Management Administration Guide (http://www.novell.com/documentation/

password_management/index.html)』の「Adding a Password Change Message」を参照してください。

- セキュリティのため、［Forgotten Password］のアクション［*E-mail password to user*］および［Allow user to reset password］は、チャレンジ質問に答えるようにユーザに要求している場合にのみ実行できます。
- NMAS™ 2.3.4 では、管理者によって変更されたユニバーサルパスワードに関するセキュリティが強化されました。これは基 \'96\'7b 的に、以前に NDS パスワードで提供されていた機 \'94\'5c と同じように動作します。

  新しいユーザを作成する場合やヘルプデスクへの問い合わせに応答する場合などに、管理者がユーザのパスワードを変更する場合、パスワードポリシーでパスワードを期限切れにする設定が有効になっていると、パスワードは自動的に期限切れになります。パスワードポリシーのこの設定は、高度なパスワードルールに［*パスワードが期限切れになるまでの日数 (0-365)*］という名前で存在します。この特定の機 \'94\'5c については、日数は重要ではありませんが、設定を有効にする必要があります。

9.4 強力なパスワードポリシーの作成

パスワードポリシーオブジェクトは、パスワードが準拠しているかどうかをアプリケーションで確認できるようにするために、パブリックに読み込み可能です。つまり、認証されていないユーザでも、識別ボールトに問い合わせて、どのパスワードポリシーが設定されているかを確認できます。パスワードポリシーにより強力なパスワードの作成が要求される場合、『*パスワード管理ガイド* (http://www.novell.com/documentation/password_management/index.html)』の「Create Strong Password Policies」に説明されているように、これによりリスクが発生することはありません。

Identity Manager パスワード同期を使用すると、ユーザパスワードを簡略化し、ヘルプデスクのコストを削減できます。双方向パスワード同期は、120 ページのセクション 5.8「パスワード同期の実装」で説明されているように、eDirectory と接続システム間との間でパスワードを複数の方法で共有できるように提供されています。

ユニバーサルパスワードとパスワードポリシーを使用することで、ユーザに対して強力なパスワード構文要件を適用できます。パスワードポリシーの［高度なパスワードルール］を使用して、パスワードに関する組織のベストプラクティスを定義できます。［高度なパスワードルール］機能を使用すると、Novell 構文または Microsoft Complexity Policy を使用するパスワード構文を管理できます。詳細については、『*Novell Password Management 3.1 Administration Guide* (http://www.novell.com/documentation/password_management31/pwm_administration/data/ampxjj0.html)』の「Managing Passwords by Using Password Policies」を参照してください。

たとえば、Novell パスワード構文のオプションを使用すると、ユーザパスワードが次のようなルールに準拠するように要求できます。

- 固有のパスワードの要求 -

  ユーザがパスワードを再利用できないようにし、システムが比較のために履歴リストに保存するパスワードの数を制限できます。
- パスワードに使用する文字の最小数の要求 -

  長いパスワードの要求は、パスワードを強化する最適な方法の 1 つです。
- パスワードに使用する数字の最小数の要求 -

パスワードに 1 つ以上の数値を含めるよう要求することは、不正侵入者が辞書の単語を使用してログインしようとする「辞書攻撃」の防止に役立ちます。

- 特定のパスワードの除外 -

  会社名や地名、または test や admin という単語など、セキュリティリスクになると思われる単語を除外できます。除外リストは辞書全体をインポートするためのものではありませんが、除外単語リストは長くてもかまいません。ただし、長い除外リストを使用すると、ユーザのログインに時間がかかります。「辞書攻撃」を防ぐ方法としては、数字または特殊文字を要求する方が適切です。

ツリーの場所によってパスワード要件が異なる場合は、複数のパスワードポリシーを作成できます。パスワードポリシーは、ツリー全体、パーティションルートコンテナ、コンテナ、または個々のユーザに割り当てることができます。(管理を簡素化するために、パスワードポリシーは、ツリーのできるだけ上位のレベルに割り当てることをお勧めします)。

さらに、不正侵入者ロックアウトも選択できます。通常どおり、eDirectory のこの機能では、ログインに何回失敗したらアカウントをロックするかを指定できます。これは、パスワードポリシーの設定ではなく、親コンテナの設定です。詳細については、『*Novell eDirectory 管理ガイド*(http://www.novell.com/documentation/edir88/index.html?page=/documentation/edir88/edir88/data/afxkmdi.html)』の「Managing User Accounts」を参照してください。

9.5 接続システムのセキュリティ保護

データを同期する先の接続システムは、そのデータを危険な方法で保存または転送することがあります。

パスワードを交換するシステムは、セキュリティで保護してください。たとえば、LDAP、NIS、および Winsows には、それぞれセキュリティの問題があり、これらのシステムとのパスワード同期を有効にする前に、これらの問題を考慮する必要があります。

多くの \'83\'5c フトウェアベンダは、製品について従う必要のある具体的なセキュリティガイドラインを提供しています。

9.5.1 パスワード生成

Identity Manager 3.5 には、ジョブスケジューラ用の事前に設定されたパスワード生成ジョブがあります。パスワード生成ジョブにより、eDirectory のユーザオブジェクトのグループ用のランダムなパスワードが、定期的にまたは要求に応じて生成されます。この機能は主に、Novell 証明書ログインなどの製品をサポートするために設計されていますが、他の状況でも使用できます。

パスワード生成ジョブを呼び出すと、NMAS がパスワードポリシーで初期化され、指定したジョブスコープの各オブジェクトに対して以下が発生します。

1. NMAS では、ジョブで指定したパスワードポリシーと一致するランダムなパスワードが生成されます。パスワードポリシーは、nspmPasswordPolicy オブジェクトに保存されます。一般的に、各接続システムには独自のポリシーオブジェクトがあります。これらのポリシーオブジェクトは、DirXML-Driver および DirXML-DriverSet オブジェクトに保存できます。
2. 生成された各パスワードは一度に 1 つずつ含まれるドライバの購読者チャネルに送信されます。

オブジェクトにドライバの無効でない関連付けがある場合、<generated-password> イベントがドライバの購読者チャネルイベントキュー (キャッシュ) に送信されます。

オブジェクトにドライバの関連付けがなく、関連付けのないオブジェクトのイベントを送信するオプションが選択されている場合、<generated-password> イベントがドライバの購読者チャネルイベントキュー (キャッシュ) に送信されます。

3. 生成されたパスワードを処理する方法は、購読者チャネルのポリシーによって決まります。ジョブスケジューラの役割は、パスワードを生成して、購読者チャネルに渡すだけです。

9.6 Designer for Identity Manager

Identity Manager の Designer を使用する場合は、次の問題を考慮します。

- Identity Manager ドライバを作成または変更する権限を持つユーザを監視および制御します。

  Identity Manager オブジェクトの作成およびドライバの設定には、管理者権限が必要です。

- 識別 \'83\'7bールトの管理者パスワードをコンサルタントに付与する前に、管理者に割り当てられる権利を、コンサルタントがアクセスするツリーのエリア内に制限します。
- プロジェクトファイル (.proj) を削除するか、会社のディレクトリに保存します。

  Designer .proj ファイルは、会社のプロジェクトサイトに存続します。コンサルタントは、プロジェクトの完了後にファイルを取得することはできません。

- プロジェクトファイル、ログファイル、およびトレースファイルが必要なくなったら、それらを削除します。
- ラップトップの廃棄または売却を行う前に、プロジェクトファイルが削除されていることを確認します。
- Designer から識別 \'83\'7bールトへの接続は、物理的にセキュアな状態を保ちます。

  そうでない場合、何者かがネットワークを監視し、機密情報を引き出す可 \'94\'5c 性があります。

- Document Generator を使用してドキュメントを作成する場合、ドキュメントの取り扱いには注意します。

  これらのドキュメントには、パスワードおよび機密データがクリアテキストで含まれている場合があります。

- Designer が eDirectory 属性の読み書きを実行する必要がある場合、属性を暗号化属性として \'83\'7dークしないでください。

  Designer は、暗号化属性の読み書きができません。

- 機密に属するパスワードを保存しないでください。

  現在、Designer プロジェクトは暗号化されていません。パスワードのみがエンコードされています。このため、保存されたパスワードを持つ Designer プロジェクトを共有しないでください。

  セッションのパスワードを保存するが、プロジェクトにパスワードを保存しない

  a. ［Outline］の展開ビューで、［Identity Vault］を右クリックします。

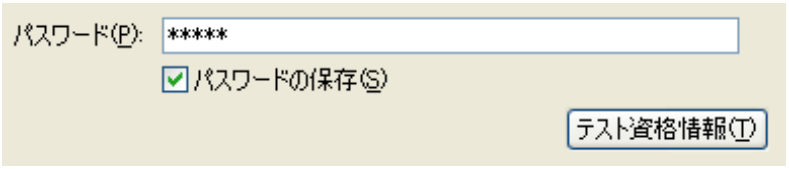
  b. ［Properties］を選択します。

c. ［Configuration］ページでパスワードを入力し、［OK］*をクリックします。*

パスワードは、1 セッションにつき一度入力できます。プロジェクトを閉じると、パスワードは消失します。

パスワードをハードドライブに保存するには、手順 1 ～ 3 を実行し、［Save Password］*を選択してから*［OK］をクリックします。

図 9-1 *Save Password*



9.7 セキュリティの業界ベストプラクティス

サーバ上の未使用ポートをブロックするなど、セキュリティ対策に関する業界ベストプラクティスに従います。

9.8 機密情報に対する変更のトラッキング

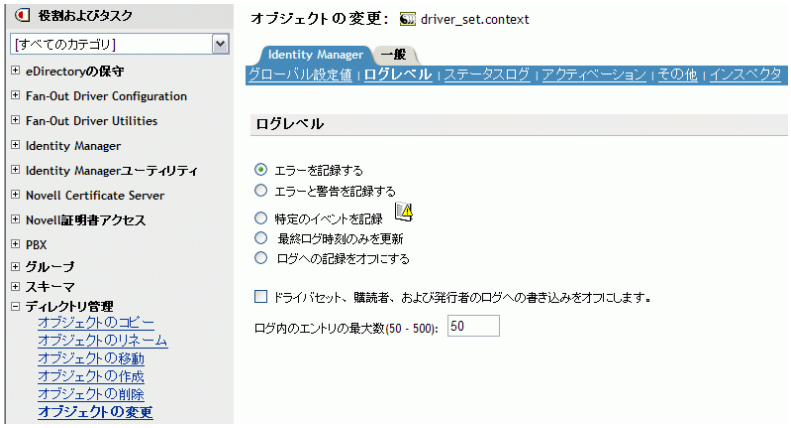
- 259 ページのセクション 9.8.1「iManager を使用したイベントのログ」
- 260 ページのセクション 9.8.2「Designer を使用したイベントのログ」

9.8.1 iManager を使用したイベントのログ

Novell Audit を使用すると、セキュリティにとって重要と思われるイベントのログを記録できます。

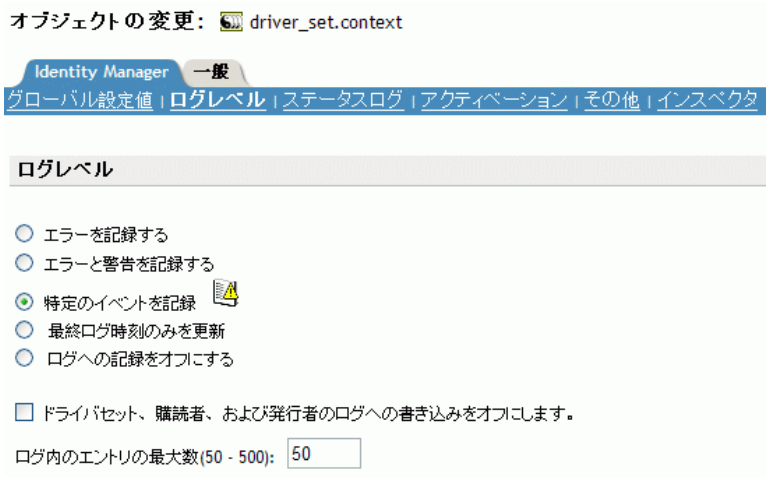
たとえば、特定の識別 \'83\'7bールトのドライバ (またはドライバセット) のパスワードの変更のログを記録するには、次の手順を実行します。

1 ［*eDirectory 管理*］>［*オブジェクトの変更*］>［*ログレベル*］の順に選択します。



iManage のバージョンにより、ドロップダウンリストまたはタブから選択します。

2 ［Log Specific Events］*を選択します。*



3 特定のイベントを選択するには、ログイベントアイコン をクリックします。

4 ［Events］ページで、次を選択します。

- ［Operation Events］で、［*Change Password*］チェックボックスをオンにします。

  この項目は、NDS のパスワードの直接の変更を監視します。

- 変換イベントで、［*パスワード設定*］および［*パスワード同期*］の両方を選択します。これら 2 つの項目は、ユニバーサルパスワードおよび配布パスワードのイベントを監視します。

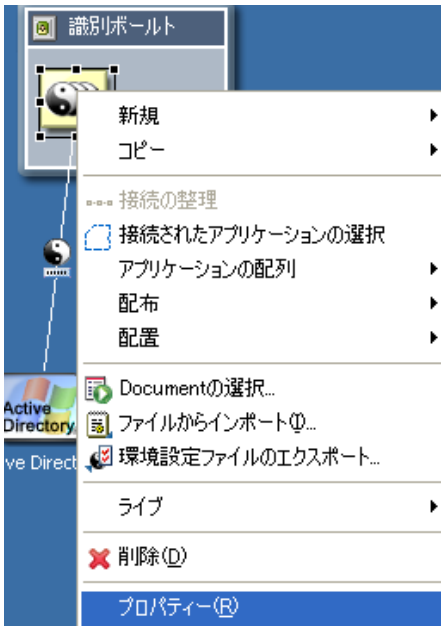
5 ［*OK*］を 2 回クリックします。

9.8.2 Designer を使用したイベントのログ

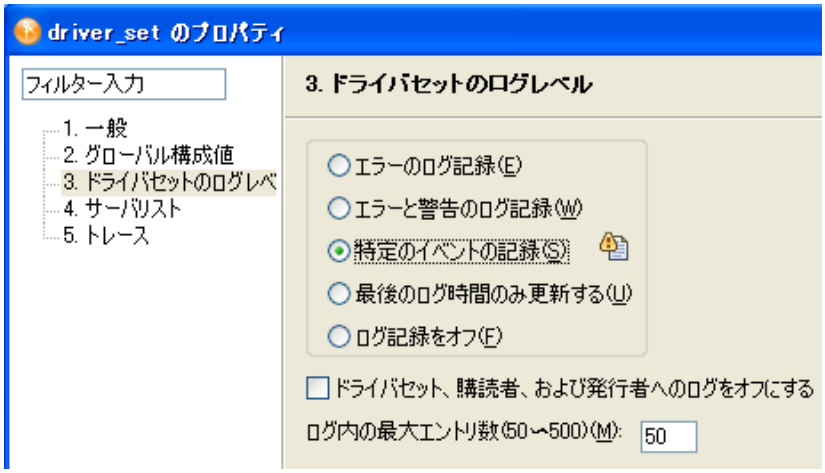
ドライバセットまたはドライバに適用されるイベントは、ログを記録できます。

ドライバセットのイベントのログ

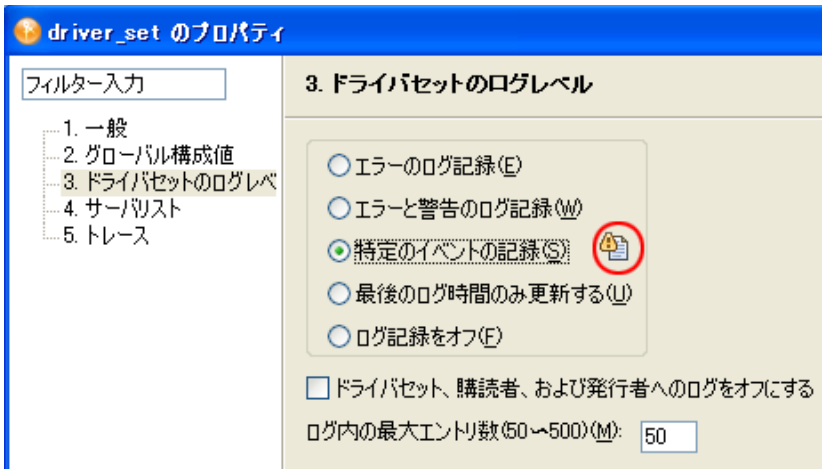
1 Designer で、ドライバセットを右クリックしてから［Properties］*を選択します。*



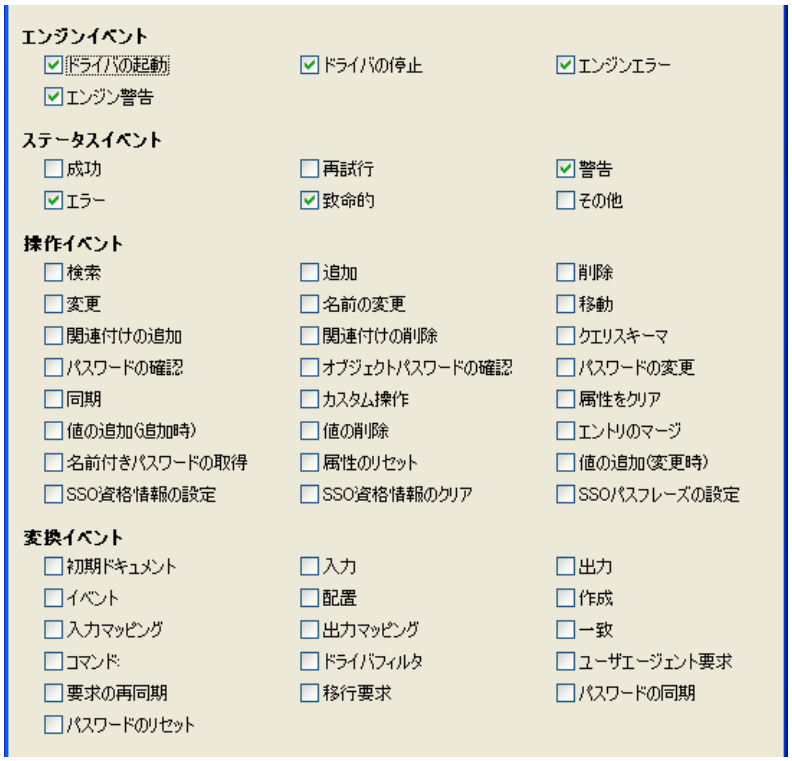
2 ［Driver Set Log Level］、［*Log Specific Events*］の順に選択します。



3 ［*記録するイベントの選択*］アイコンをクリックします。



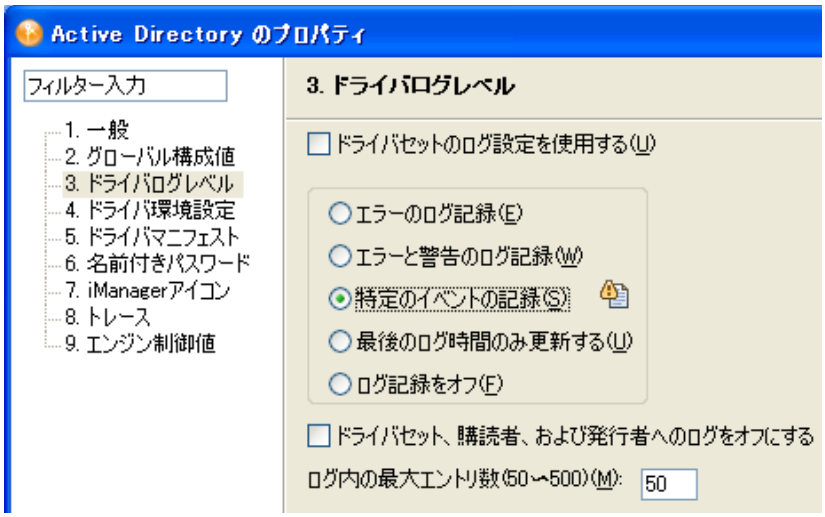
4 ログを記録するイベントを選択してから、［OK］をクリックします。



ドライバのイベントのログ

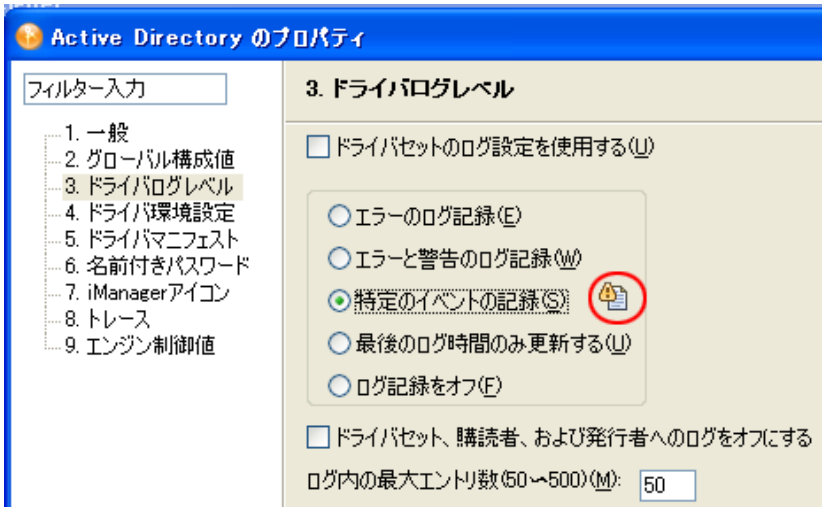
1 Designer で、ドライバを右クリックして［*プロパティ*］を選択します。

2 ［Driver Log Level］、［*Log Specific Events*］の順に選択します。



ドライバセットの設定をそのまま使用する場合は、［*OK*］をクリックします。そうでない場合は、［Use log settings from the Driver Set］*チェック\'83\'7bックスをオフにしてから［Log specific events*］を選択し、［OK］*をクリックします。>*

3 ［*Select Events to Log*］*アイコンをクリックします。*



4 ログを記録するイベントを選択してから、［OK］*をクリックします。*


エンジンイベント
ドライバの起動
ドライバの停止
エンジンエラー
エンジン警告
ステータスイベント
成功
再試行
警告
エラー
致命的
その他
操作イベント
検索
追加
削除
変更
名前の変更
移動
関連付けの追加
関連付けの削除
クエリスキーマ
パスワードの確認
オブジェクトパスワードの確認
パスワードの変更
同期
カスタム操作
属性をクリア
値の追加(追加時)
値の削除
エントリのマージ
名前付きパスワードの取得
属性のリセット
値の追加(変更時)
SSO資格情報の設定
SSO資格情報のクリア
SSOパスフレーズの設定
変換イベント
初期ドキュメント
入力
出力
イベント
配置
作成
入力マッピング
出力マッピング
一致
コマンド:
ドライバフィルタ
ユーザエージェント要求
要求の再同期
移行要求
パスワードの同期
パスワードのリセット

エンジンサービスの管理

10

次のドライバは、外部接続システムではなく、メタディレクトリエンジンサービスに対してのみ使用されます。これらは、Identity Manager をインストールするときに自動的にインストールされます。

- 265 ページのセクション 10.1「エンタイトルメントサービスドライバ」
- 265 ページのセクション 10.2「手動タスクサービスドライバ」
- 282 ページのセクション 10.3「ループバックサービスドライバ」
- 283 ページのセクション 10.4「Null サービスドライバ」

エンジンサービスは、エンジン制御値でも管理できます。詳細については、284 ページのセクション 10.5「エンジン制御値」を参照してください。

10.1 エンタイトルメントサービスドライバ

Identity Manager を使用すると、接続システム間でデータを同期できます。エンタイトルメントにより、ユーザまたはグループに対する条件を設定できます。条件が一致すると、接続されたシステム内のビジネスリソースへのアクセス権を付与したり、取り消したりするイベントが開始されます。これにより、1 レベル上の制御が可能になり、リソースの付与および取り消しを自動化できます。エンタイトルメントの詳細については、173 ページの第 6 章「エンタイトルメントの作成と使用」を参照してください。

10.2 手動タスクサービスドライバ

手動タスクサービスドライバは、データイベントが発生したこと、およびユーザ側でアクションが必要かどうかを 1 人または複数のユーザに通知するために開発されました。従業員のプロビジョニングシナリオでは、データイベントが新しいユーザオブジェクトの作成で、ユーザアクションには、eDirectory™ またはアプリケーションにデータを入力してオフィス番号を割り当てる作業が含まれます。他のシナリオとしては、新しいユーザオブジェクトが作成されたことの管理者への通知、ユーザがオブジェクト上のデータを変更したことの管理者への通知などがあります。

手動タスクサービスドライバの設定は、通常、購読者チャネルポリシーと電子メールテンプレート、発行者チャネル Web サーバテンプレートとポリシーという 2 つの独立した関連のあるサブシステムの設定を伴います。

SMTP サーバ名、Web サーバポート番号などのドライバパラメータも設定する必要があります。

この節では、次の項目について説明します。

- 266 ページのセクション 10.2.1「インストール」
- 266 ページのセクション 10.2.2「概要」
- 273 ページのセクション 10.2.3「パラメータおよびテンプレートを設定する」
- 282 ページのセクション 10.2.4「補足情報」

10.2.1 インストール

- **インストール :** 手動タスクサービスドライバは、Identity Manager インストールプログラムを使用して［*メタディレクトリサーバ*］オプションをインストールするときに自動的にインストールされます。
- **プラットフォーム :** ドライバは、Identity Manager およびリモートローダによってサポートされているプラットフォームで実行されます。
- **アクティベーション :** ドライバには、個別のアクティベーションは必要ありません。Metadirectory エンジンをアクティブにすると、このドライバもアクティブになります。

10.2.2 概要

このセクションには、ドライバの機能が動作する方法に関する情報が含まれています。

- 266 ページの 「動作モード」
- 267 ページの 「手動タスクサービスドライバによって、電子メールメッセージおよび Web ページがどのように作成されるのか」
- 268 ページの 「テンプレート」
- 271 ページの 「置換トークン」
- 271 ページの 「置換データ」
- 271 ページの 「テンプレートのアクション要素」
- 271 ページの 「加入者チャネルの電子メール」
- 273 ページの 「発行者チャネルの Web サーバ」

動作モード

次の 2 つの主な操作モードがサポートされています。

- **データの直接要求 :** ユーザが eDirectory にデータを入力することを要求する電子メールメッセージが送信されます (他のアプリケーションによって使用される可能性があります)。電子メールの受信者は、メッセージ内の URL をクリックすることによりメッセージに応答します。URL は、手動タスクサービスドライバの発行者チャネルで実行されている Web サーバを指しています。ユーザは、Web サーバによって生成された動的な Web ページと情報をやりとりし、eDirectory を認証して要求されたデータを入力します。
- **イベント通知 :** 発行者チャネルを使用せずに、電子メールメッセージがユーザに送信されます。電子メールメッセージは、単に eDirectory で何かが発生したことを通知したり、または Novell iManager、その他のアプリケーション、またはカスタムインタフェースなどの発行者チャネルの Web サーバ以外の方法を介してデータを要求したりするだけの場合があります。

例 : 購読者チャネルの電子メール、発行者チャネルの Web サーバレスポンス

次は、新しい従業員の \'83\'7d ネージャが従業員に部屋番号を割り当てるという、従業員のプロビジョニング例のシナリオです。

1. eDirectory で新しいユーザオブジェクトが作成されます (会社の人事システム用の Identity Manager ドライバなど)。

2. 手動タスクサービスドライバの購読者チャネルから、ユーザのマネージャおよびマネージャのアシスタントに SMTP メッセージが送信されます。SMTP メッセージには、発行者チャネルの Web サーバを参照する URL が含まれています。URL には、ユーザを識別し、要求されたデータを送信することを承認されたユーザを識別するデータ項目も含まれています。
3. マネージャまたはマネージャのアシスタントは、電子メールメッセージ内の URL をクリックして、Web ブラウザで HTML 形式でメッセージを表示します。次に、\'83\'7d ネージャまたはアシスタントは次を実行します。
   - 誰が電子メールメッセージに応答するのかを識別する方法として、eDirectory ユーザオブジェクトの DN を選択します。
   - eDirectory パスワードを入力します。
   - 新しい従業員の部屋番号を入力します。
   - ［Submit］\'83\'7b タンをクリックします。
4. 手動タスクサービスドライバの発行者チャネルを経由して、新しい従業員の部屋番号が eDirectory に送信されます。

例 : 購読者チャネルの電子メール、発行者チャネルのレスポンスがない場合

次に、資産管理システムで、新しい従業員の \'83\'7d ネージャが従業員にコンピュータを割り当てるというシナリオの例を示します。

1. 会社の人事システム用の Identity Manager ドライバにより、eDirectory で新しいユーザオブジェクトが作成されます。
2. 手動タスクサービスドライバの購読者チャネルから、ユーザのマネージャおよびマネージャのアシスタントに SMTP メッセージが送信されます。SMTP メッセージには、資産管理システムへのデータの入力に関する説明が含まれています。
3. \'83\'7d ネージャまたはアシスタントが、資産管理システムにデータを入力します。
4. (オプション) 資産管理システムの Identity Manager ドライバを経由して、コンピュータの識別データが eDirectory に送信されます。

手動タスクサービスドライバによって、電子メールメッセージおよび Web ページがどのように作成されるのか

電子メールメッセージ、HTML Web ページ、および XDS ドキュメントは、すべてドキュメントと見なすことができます。手動タスクサービスドライバによって、ドライバに提供された情報に基づいてドキュメントが動的に作成されます。

テンプレートは、動的な部分または置換部分の、\'8d\'5c 成された最終のドキュメントが \'95\'5c 示される場所を示す置換トークンとともに、\'83\'7b イラープレートまたはドキュメントの固定部分が含まれている XML ドキュメントです。

手動タスクサービスドライバの購読者チャネルおよび発行者チャネルの両方で、ドキュメントを作成するためのテンプレートが使用されます。加入者チャネルにより電子メールメッセージが作成され、発行者チャネルにより Web ページおよび XDS ドキュメントが作成されます。

ドキュメントの動的な部分は置換データから提供されます。購読者チャネルの置換データは、(コマンド変換ポリシーなどの) 購読者チャネルポリシーによって提供されます。発行者チャネルの置換データは、Web サーバに送信される HTTP データによって提供されます (URL データと HTTP POST データの両方)。手動タスクサービスドライバは、(Web

サーバのアドレスなどの) 手動タスクサービスドライバにとって既知の特定のデータを自動的に提供します。

テンプレートは、XSLT スタイルシートによって処理されます。これらのテンプレート処理のスタイルシートは、購読者チャネルまたは発行者チャネルでポリシーとして使用されるスタイルシートとは別のものです。

置換データはパラメータとして XSLT スタイルシートに提供されます。スタイルシート処理の出力は、電子メールメッセージの本文、Web ページ、または発行者チャネル上の Identity Manager への送信に使用されている XML、HTML、またはテキストドキュメントです。

置換データは、電子メールメッセージの URL を経由して購読者チャネルから発行者チャネルに渡されます。URL には、置換データ項目が含まれているクエリ部分が含まれています。

手動タスクサービスドライバには、電子メールドキュメント、HTML ドキュメント、および XDS ドキュメントを作成するためにテンプレートを処理するのに十分な事前定義されたスタイルシートが付属しています。他のカスタムのスタイルシートは、追加の処理オプションを提供するために記述することができます。

XSLT スタイルシートおよび置換データのみを使用する、高度なドキュメントの作成方法も使用できます。テンプレートは使用しません。しかし、このガイドではテンプレートによる方法を使用することを想定しています。これは、XSLT のプログラミング知識なしで設定および管理するには、テンプレートによる方法がより簡単であるためです。

テンプレート

テンプレートは、出力ドキュメントを生成するために、スタイルシートによって処理される XML ドキュメントです。出力ドキュメントは、XML、HTML、またはプレーンテキストです (または、XSLT を使用して生成されるその他のドキュメントです)。

テンプレートは、購読者チャネルで電子メールメッセージテキストを生成したり、発行者チャネルで動的な Web ページや XDS ドキュメントを生成するために、手動タスクサービスドライバで使用されます。

テンプレートには、テキスト、要素、および置換トークンが含まれています。置換トークンは、テンプレートを処理するスタイルシートに提供されたデータによって出力ドキュメントで置換されます。

さまざまな目的のテンプレートの例をいくつか以下に示します。例では、置換トークンは 2 つの $ 記号の間にある文字列です。

テンプレートには、アクション要素を含めることもできます。アクション要素は、テンプレート処理のスタイルシートによって解釈された制御要素です。アクション要素については、339 ページの付録 F「手動タスクサービスドライバ : テンプレートアクション要素の参照」で説明しています。

次のテンプレートの例は、HTML の電子メールメッセージ \'96\'7b 文を生成するために使用されます。

```
<html xmlns:form="http://www.novell.com/dirxml/manualtask/form">
<head></head>
<body>
Dear $manager$,<p/>
<p>
```

```
This message is to inform you that your new employee <b>$given-name$
$surname$</b> has been hired.
<p>
You need to assign a room number for this individual. Click <a
href="$url$">Here</a> to do this.
</p>
<p>
Thank you,<br/>
HR Department
</p>
</body>
</html>
```

次のテンプレートの例は、プレーンテキストの電子メールメッセージ \'96\'7b 文を生成するために使用されます。

```
<form:text xmlns:form="http://www.novell.com/dirxml/manualtask/form">
Dear $manager$,

This message is to inform you that your new employee $given-name$
$surname$ has been hired.

You need to assign a room number for this individual. Use the following
link to do this:

$url$

Thank you,

The HR Department

</form:text>
```

テンプレートは XML ドキュメントである必要があるため、<form:text> 要素は必須です。<form:text> 要素はテンプレート処理の一部としてストリップされます。

データの入力用に Web ページとして使用される HTML 形式を生成するには、次のテンプレートが使用されます。

```
<html  xmlns:form="http://www.novell.com/dirxml/manualtask/form">
<head>
<title>Enter room number for $subject-name$</title>
</head>
<body>
    <link href="novdocmain.css" rel="style sheet" type="text/css"/>
    <br/><br/><br/><br/>
    <form class="myform" METHOD="POST" ACTION="$url-base$/
process_template.xsl">
        <table cellpadding="5" cellspacing="10" border="1"
align="center">
          <tr><td>
          <input TYPE="hidden" name="template" value="post_form.xml"/>
          <input TYPE="hidden" name="subject-name" value="$subject-
name$"/>
          <input TYPE="hidden" name="association"
value="$association$"/>
```

```
          <input TYPE="hidden" name="response-style sheet"
value="process_template.xsl"/>
          <input TYPE="hidden" name="response-template"
value="post_response.xml"/>
          <input TYPE="hidden" name="auth-style sheet"
value="process_template.xsl"/>
          <input TYPE="hidden" name="auth-template"
value="auth_response.xml"/>
        <input TYPE="hidden" name="protected-data" value="$protected-
data$"/>
          You are:<br/>
          <form:if-single-item name="responder-dn">
           <input TYPE="hidden" name="responder-dn" value="$responder-
dn$"/>
            $responder-dn$
          </form:if-single-item>          <form:if-multiple-items
name="responder-dn">          <form:menu name="responder-dn"/>
</form:if-multiple-items>
        </td></tr>
        <tr><td>
          Enter your password: <br/>
<input name="password" TYPE="password" SIZE="20" MAXLENGTH="40"/>
        </td></tr>
        <tr><td>
          Enter room number for $subject-name$:<br/>
          <input TYPE="text" NAME="room-number" SIZE="20"
MAXLENGTH="20" value="$query:roomNumber$"/>
        </td></tr>
        <tr><td>
          <input TYPE="submit" value="Submit"/> <input TYPE="reset"
value="Clear"/>
        </td></tr>
      </table>
    </form>
  </body>
</html>
```

XDS ドキュメントを生成するには、次のテンプレートを使用します。

```
<nds>
  <input>
    <modify class-name="User" src-dn="not-applicable">
      <association>$association$</association>
      <modify-attr attr-name="roomNumber">
        <remove-all-values/>
        <add-value>
          <value>$room-number$</value>
        </add-value>
      </modify-attr>
    </modify>
  </input>
</nds>
```

置換トークン

上記のテンプレートの例では、$ で区切られた項目が置換トークンです。たとえば、$manager$ は、マネージャの実際の名前に置換されます。

置換トークンは、テキストまたは XML 属性値のいずれかで \'95\'5c 示できます (上記の最初の例の <a> 要素の href 値に注目してください)。

置換データ

置換データは、テンプレートから生成された出力ドキュメントの置換トークンの場所を占める文字列で構成されます。置換データは、購読者チャネルのデータ、発行者チャネルの HTTP データによって提供されるか、またはドライバによって自動的に提供されます。置換データの追加のタイプとしては、Identity Manager を経由して eDirectory から取得されたデータがあります (クエリデータ)。置換データについては、331 ページの付録 D「手動タスクサービスドライバ : 置換データ」でより詳しく説明しています。

加入者チャネルのデータ : 購読者チャネルの置換データには、2 つのタイプがあります。最初のタイプは、電子メールメッセージを作成するための、テンプレートでの置換トークンの置換の値として使用されます。2 番目のタイプは、URL が発行者の Web サーバに送信されたときに、発行者チャネルでデータが使用可 \'94\'5c であるように、URL のクエリ部分にあります。

HTTP データ : URL クエリ文字列データ、HTTP POST データ、またはその両方として、発行者チャネルの Web サーバに置換データが提供されます。

自動データ : 手動タスクサービスドライバによって、自動データが提供されます。自動データ項目については、337 ページの付録 E「手動タスクサービスドライバ : 自動置換データ項目」で詳しく説明しています。

クエリデータ : クエリで始まる置換トークンは、eDirectory から現在のデータを取得するための要求であると見なされます。クエリの後のトークン部分は、eDirectory オブジェクト属性の名前です。問い合わせるオブジェクトは、置換データ項目のひとつである association、src-dn、または src-entry-id によって指定されます。項目は、前のセンテンスで \'95\'5c 示されている順に考慮されます。

テンプレートのアクション要素

アクション要素は、シンプルなロジック制御、または HTML 形式の HTML 要素を作成するために使用されるテンプレートの namespace-qualified 要素です。要素を修飾するために使用されているネームスペースは、http://www.novell.com/dirxml/manualtask/form にあります。このドキュメントおよび手動タスクサービスドライバで提供されているサンプル テンプレートでは、使用されているプレフィクスは form です。

アクション要素については、339 ページの付録 F「手動タスクサービスドライバ : テンプレートアクション要素の参照」で詳しく説明しています。

加入者チャネルの電子メール

手動タスクサービスドライバの購読者チャネルは、電子メールメッセージを送信するように設計されています。これを実行するために、ドライバでは <mail> という名前のカスタム XML 要素がサポートされています。購読者チャネルのポリシーによって、ユーザの作成などの eDirectory イベントに応じて <mail> 要素が構成されます。<mail> 要素が表示される例を以下に示します。

```
<mail src-dn="\PERIN-TAO\novell\Provo\Joe">
  <to>JStanley@novell.com</to>
  <cc>carol@novell.com</cc>
  <reply-to>HR@novell.com</reply-to>
  <subject>Room Assignment Needed for: Joe the Intern</subject>
  <message mime-type="text/html">
    <stylesheet>process_template.xsl</stylesheet>
    <template>html_msg_template.xml</template>
    <replacement-data>
      <item name="manager">JStanley</item>
      <item name="given-name">Joe</item>
      <item name="surname">The Intern</item>
      <url-data>
        <item name="file">process_template.xsl</item>
        <url-query>
          <item name="template">form_template.xml</item>
          <item name="responder-dn" protect="yes">\PERIN-TAO\big-
org\phb</item>
          <item name="responder-dn" protect="yes">\PERIN-TAO\big-
org\carol</item>
          <item name="subject-name">Joe The Intern</item>
        </url-query>
      </url-data>
    </replacement-data>
    <resource cid="css-1">novdocmain.css</resource>
  </message>
  <message mime-type="text/plain">
    <stylesheet>process_text_template.xsl</stylesheet>
    <template>txt_msg_template.xml</template>
    <replacement-data>
      <item name="manager">JStanley</item>
      <item name="given-name">Joe</item>
      <item name="surname">The Intern</item>
      <url-data>
          <item name="file">process_template.xsl</item>
          <url-query>
            <item name="template">form_template.xml</item>
            <item name="responder-dn" protect="yes">\PERIN-TAO\big-
org\phb</item>
            <item name="responder-dn" protect="yes">\PERIN-TAO\big-
org\carol</item>
            <item name="subject-name">Joe The Intern</item>
          </url-query>
        </url-data>
      </replacement-data>
    </message>
  <attachment>HR.gif</attachment>
</mail>
```

手動タスクサービスドライバの購読者チャネルでは、<mail> 要素に含まれている情報を使用して、SMTP 電子メールメッセージが構成されます。URL を構成して電子メールメッセージに挿入できます。その URL を介して、電子メールの受信者はその電子メールメッセージに応答できます。URL は、発行者チャネルの Web サーバを指したり、またはいくつかの他の Web サーバを指すこともできます。

<mail> 要素およびそのコンテンツの詳細については、343 ページの付録 G「手動タスクサービスドライバ : <mail> 要素参照」を参照してください。

発行者チャネルの Web サーバ

手動タスクサービスドライバの発行者チャネルでは、ユーザが Web ブラウザを介して eDirectory にデータを入力できるように設定されている Web サーバが実行されています。Web サーバは、手動タスクサービスドライバの加入者チャネルから送信された電子メールメッセージと組み合わせて機 \'94\'5c するように設計されています。

発行者チャネルの Web サーバは、スタティックファイルおよびダイナミックコンテンツを提供できます。スタティックファイルの例としては、.css スタイルシート、イメージなどがあります。ダイナミックコンテンツの例としては、URL または HTTP POST データに含まれている置換データに基づいて変更される Web ページがあります。

発行者チャネルの Web サーバは、通常、購読者チャネルによって送信された電子メールに対して、ユーザが eDirectory にデータを入力できるように設定されます。一般的なユーザの Web サーバとの情報のやりとりは、次のとおりです。

1. ユーザは Web ブラウザを使用して、電子メールメッセージの URL を Web ブラウザに送信します。URL では、動的な Web ページを作成するために使用されたスタイルシート、テンプレート、および置換データが指定されています (通常 HTML 形式が含まれています)。
2. Web サーバによってスタイルシートおよび置換データを使用してテンプレートが処理されることによって、HTML ページが作成されます。URL によって参照されるリ \'83\'5c ースとして、HTML ページがユーザの Web ブラウザに返されます。
3. ブラウザに HTML ページが \'95\'5c 示され、要求された情報をユーザが入力します。
4. ブラウザによって、入力された情報が含まれている HTTP POST 要求、および電子メールの URL からのその他の情報が送信されます。電子メールに応答しているユーザの DN およびユーザのパスワードは、POST データにある必要があります。
5. Web サーバでは、ユーザの DN とパスワードを使用して認証が行われます。認証が失敗した場合、POST 要求の結果として、失敗のメッセージが含まれている Web ページが返されます。失敗のメッセージは、POST データで指定したスタイルシートおよびテンプレートを使用して構成できます。認証が成功した場合、処理が続行されます。
6. POST データで指定したスタイルシートおよびテンプレートを使用して、Web サーバで XDS ドキュメントが構成されます。XDS ドキュメントが、発行者チャネル上の Identity Manager に送信されます。
7. XDS ドキュメントの送信の結果は、POST データで指定したスタイルシートおよびテンプレートとともに、データ送信の結果をユーザに示す Web ページを構成するために使用されます。POST 要求の結果として、この Web ページがブラウザに送信されます。

10.2.3 パラメータおよびテンプレートを設定する

- 274 ページの 「ドライバの設定」
- 276 ページの 「加入者の設定」
- 277 ページの 「発行者の設定」
- 277 ページの 「加入者チャネルのポリシー」

- 279 ページの 「加入者チャネルの電子メールテンプレート」
- 279 ページの 「発行者チャネルのポリシー」
- 280 ページの 「発行者チャネルの Web ページテンプレート」
- 280 ページの 「発行者チャネルの XDS テンプレート」
- 281 ページの 「トレースの設定」

ドライバの設定

このセクションでは、ドライバオブジェクトのユーザインタフェースの［ドライバ設定］セクションに表示されているパラメータについて説明します。

これらのパラメータの多くは、実際の発行者チャネルの Web サーバ用です。手動タスクサービスドライバの加入者もこれらにアクセスする必要があるため、これらは［Driver Settings］エリアに \'95\'5c 示されます。

- 274 ページの 「ドキュメントベースの DN」
- 275 ページの 「ドキュメントのディレクトリ」
- 275 ページの 「HTTP サーバを使用する (true|false)」
- 275 ページの 「HTTP IP アドレスまたはホスト名」
- 275 ページの 「HTTP ポート」
- 276 ページの 「KMO の名前」
- 276 ページの 「キーストアファイルの名前」
- 276 ページの 「キーストアパスワード」
- 276 ページの 「証明書の名前 (キーエイリアス)」
- 276 ページの 「証明書のパスワード (キーパスワード)」

ドキュメントベースの DN

このパラメータは、コンテナオブジェクトの eDirectory DN です。手動タスクサービスドライバでは、eDirectory またはディスクから (XSLT スタイルシートを含む)XML ドキュメントをロードできます。XML ドキュメントを eDirectory からロードする必要がある場合、ドキュメントがロードされるルートコンテナがこのパラメータによって識別されます。

eDirectory からロードされたドキュメントは、eDirectory オブジェクトの属性値に常駐します。指定しない場合、属性は XmlData です。ドキュメントが含まれているオブジェクトの名前の # 文字の後ろに属性名を追加することにより、属性を指定できます。

たとえば、ドキュメントベースの DN が「*novell\Manual Task Documents*」に指定されたとします。また、「*templates*」という名前の「*Manual Task Documents*」の下にコンテナがあるとします。

e-mail _template という名前の DirXML-Style スタイルシートオブジェクトが *templates* ディレクトリに常駐している場合、次のリソース識別子を XML ドキュメントを参照するために使用できます。*templates/e-mail _template* または *templates/e-mail _template#XmlData*。

リソースの識別子は、置換データ、URL データ、または HTTP POST データとして提供できます。たとえば、次の要素は購読者チャネルの <message> 要素の下に表示されます。

```
<template>templates/e-mail _template#XmlData</template>
```

ドキュメントのディレクトリ

このパラメータにより、テンプレート、XSLT スタイルシートなどのリソース、および発行者チャネルの Web サーバより提供されるその他のファイルのリソースを検索するための基本ディレクトリとして使用されるファイルシステムディレクトリが識別されます。値の例は次のとおりです。

Windows	c:\Novell\Nds\mt_files
NetWare®	SYS:\SYSTEM\mt_files
UNIX	/usr/lib/dirxml/rules/manualtask/mt_files

HTTP サーバを使用する (true|false)

このパラメータは、発行者チャネルを介して Web サーバを実行するかどうかを示します。Web サーバを実行する必要がある場合は、パラメータを True に設定し、Web サーバを実行する必要がない場合、False に設定します。

レスポンス URL を持たない電子メール、またはその他のアプリケーションを指す URL を持つ電子メールの送信に、手動タスクサービスドライバのみが使用される場合、システムリ \'83\'5c ースを節約するために HTTP サーバを実行しないでください。

HTTP IP アドレスまたはホスト名

このパラメータを使用すると、発行者チャネルの Web サーバが HTTP 要求をリッスンする複数のローカル IP アドレスを指定できます。

HTTP IP アドレスまたはホスト名のパラメータ値を空白のままにしておくと、発行者チャネルの Web サーバはデフォルトの IP アドレスをリッスンします。単一の IP アドレスが設定されているサーバの場合は、これで十分です。dot-notation の IP アドレスをパラメータ値として配置すると、発行者チャネルの Web サーバは指定されたアドレスの HTTP 要求をリッスンします。

メールコマンド要素でホスト名またはアドレスが指定されていない場合、HTTP IP アドレスまたはホスト名で指定した値は、URL を構成するために購読者チャネルのメールハンドラによって使用されます。［HTTP サーバを使用する (true|false)］のパラメータが False に設定されている場合、メールメッセージの URL の構成で使用するために、HTTP IP アドレスまたはホスト名を使用して Web サーバのアドレスまたは名前を指定できます。

HTTP ポート

このパラメータは、発行者チャネルの Web サーバが着信要求リッスンする TCP ポートを示す整数値です。この値が指定されていない場合、Web サーバ接続で SSL が使用されるかどうかに応じて、ポート番号のデフォルトが 80 または 443 になります。

手動タスクサービスドライバが Identity Manager サーバで実行されている場合 (つまり、リモート \'83\'7d シン上のリモートローダの下で実行されない場合)、HTTP ポートを 80 または 443 以外に設定する必要があります。これは、iMonitor またはその他のプロセスは通常、ポート 80 および 443 を使用しているためです。

KMO の名前

これが空白でない場合、このパラメータは、発行者チャネルの Web サーバによって SSL に使用されるサーバ証明書およびキーが含まれている Directory の暗号化キーオブジェクトの名前になります。

このパラメータを設定すると、発行者チャネルの Web サーバで HTTP 要求の実行に SSL が使用されます。

このパラメータは、すべての Java キーストアパラメータに優先します (276 ページの「キーストアファイルの名前」を参照)。

eDirectory パスワードは発行者チャネル Web サーバを使用して HTTP POST データに渡されるので、セキュリティ上の理由のため SSL の使用をお勧めします。

キーストアファイルの名前

このパラメータは、キーストアパスワード、証明書の名前 (キーエイリアス)、および証明書パスワード (キーパスワード) と組み合わせて、発行者チャネルの Web サーバによって SSL で使用される証明書およびキーが含まれている Java キーストアファイルを指定するために使用します。

このパラメータを設定すると、発行者チャネルの Web サーバで HTTP 要求の実行に SSL が使用されます。

KMO の名前のパラメータが設定されている場合、このパラメータおよび関連付けられているパラメータは無視されます。

eDirectory パスワードは発行者チャネル Web サーバを使用して HTTP POST データに渡されるので、セキュリティ上の理由のため SSL の使用をお勧めします。

キーストアパスワード

このパラメータでは、キーストアファイルの名前のパラメータで指定した Java キーストアファイルのパスワードを指定します。

証明書の名前 (キーエイリアス)

このパラメータでは、キーストアファイルの名前のパラメータで指定した Java キーストアファイルで使用するための証明書の名前を指定します。

証明書のパスワード (キーパスワード)

このパラメータでは、証明書の名前 (キーエイリアス) のパラメータを使用して指定した証明書のパスワードを指定します。

加入者の設定

- 277 ページの 「SMTP サーバ」
- 277 ページの 「SMTP のアカウント名」
- 277 ページの 「デフォルトの「From」アドレス」
- 277 ページの 「追加的なハンドラ」

SMTP サーバ

このパラメータでは、電子メールメッセージを送信するために購読者チャネルで使用される SMTP サーバの名前を指定します。

SMTP のアカウント名

SMTP サーバのパラメータを使用して指定した SMTP サーバで認証が必要とされる場合、このパラメータで、認証に使用するアカウント名を指定します。使用されるパスワードは、ドライバの認証パラメータに関連付けられているアプリケーションのパスワードです。

デフォルトの「From」アドレス

指定されている場合、、購読者チャネルによって送信される電子メールメッセージの SMTP from フィールドで使用される電子メールアドレスです。指定されていない場合、購読者に送信された <mail> 要素には <from> 要素が含まれている必要があります。

購読者に送信された <mail> 要素の <from> 要素で、このパラメータは上書きされます。

追加的なハンドラ

指定されている場合、これはスペースで区切られた Java クラス名のリストです。各クラス名は、com.novell.nds.dirxml.driver.manualtask.CommandHandler インタフェースを実装し、カスタム XDS 要素を処理するカスタムクラスです。<mail> のハンドラは組み込みハンドラです。

カスタムハンドラに関する追加的な情報については、359 ページの付録 I「手動タスクサービスドライバ : 購読者チャネル用のカスタム要素ハンドラ」を参照してください。

発行者の設定

このセクションでは、発行者チャネルの設定について説明します。

追加的なサーブレット

空白でない場合、これはスペースで区切られた Java クラス名のリストです。各クラス名は、javax.servlet.http.HttpServer を拡張するカスタムクラスです。カスタムサーブレットを使用して発行者チャネルの Web サーバの機 \'94\'5c を拡張できます。

カスタムサーブレットに関する追加的な情報については、361 ページの付録 J「手動タスクサービスドライバ : 発行者チャネル用のカスタムサーブレット」を参照してください。

加入者チャネルのポリシー

購読者チャネルポリシーの設定は、手動タスクサービスドライバを使用して特定のインストールで実行する内容に依存します。しかし、特定のガイドラインが役立ちます。

一般的には、購読者に送信するために <mail> 要素を構成するのに最適な場所は、コマンド変換ポリシー内です。その理由は、コマンドがコマンド変換ポリシーに到達するまでに、大部分のメタディレクトリエンジン処理が完了しているためです。つまり、追加イベントに対してポリシーの作成が処理されます (たとえば電子メールの構成に必要なすべての属性を持たないオブジェクトに対する追加イベントの拒否の許可)。これは、関連付けのないオブジェクトの変更イベントが、すでに追加イベントに変換されていることも意味します。

電子メールメッセージを \'8d\'5c 成する XSLT スタイルシートは、追加的な情報の eDirectory を問い合わせる必要がある場合と、ない場合があります。

たとえば、電子メールメッセージが新しい従業員の歓迎メッセージである場合、追加コマンドには、名、名字、およびインターネットの電子メールアドレスなどの必要な情報をすべて含めることができます。これは、作成ポリシーで、名前、名字、およびインターネットの電子メールアドレスが必要な属性であることを指定して行います。これにより、必要な情報が含まれている追加コ \'83\'7d ンドのみが Command Transformation(コ \'83\'7d ンド変換) に到達できます。

しかし、電子メールメッセージが従業員のマネージャに対するメッセージである場合は、スタイルシートを使用して eDirectory に問い合わせをする必要があります。マネージャ DN は、従業員のユーザオブジェクトの追加イベントから取得できますが、その情報はマネージャのユーザオブジェクトの属性であるため、マネージャの電子メールアドレスを取得するためにクエリを行う必要があります。

また、ドライバに関連付けられているオブジェクトの変更コマンドの結果として電子メール通知が生成される場合、変更コマンドに含まれていない情報を取得するためにクエリを実行する必要があります。

コマンドをブロックして、購読者チャンネルに到達しないようにする

電子メールメッセージが追加イベント以外のイベントから生成される場合、監視されるオブジェクトに対する、追加イベントが購読者チャネルに到達させる必要があります。追加イベントが購読者チャネルに到達するのを許可すると、生成された関連付けの値が購読者チャネルから Identity Manager に返されます。

手動タスクサービスドライバポリシーによって監視される eDirectory オブジェクトが、手動タスクサービスドライバに関連付けられていることが重要です。関連付けられたオブジェクトのみ、削除イベント、名前変更イベント、および移動イベントがドライバにレポートされます。また、関連付けられていないオブジェクトの変更イベントは、購読者チャネルのイベント変換後に追加イベントに変換されます。

その他のすべてのコマンド (変更、移動、名前変更、および削除) は、コマンド変換ポリシーによってブロックされ、購読者チャネルに到達しないようにする必要があります。購読者チャネルでは、<Add> コマンドおよび <Mail> コマンドのみ処理されます。その他のコマンドは、購読者チャネルによりエラーが返されます。

電子メールメッセージの生成

電子メールメッセージは、送信される電子メールメッセージを説明する <mail> 要素の受信に対する返信として、購読者によって送信されます。<mail> 要素およびそのコンテンツの説明については、343 ページの付録 G「手動タスクサービスドライバ : <mail> 要素参照」を参照してください。

電子メールメッセージは、任意の Identity Manager イベント (追加、変更、名前変更、移動、削除) に対して生成できます。

<mail> 要素の <message> 要素の子で提供された置換データは、次の 2 つの主な要因によって決まります。

- メッセージ本文の生成に使用されたテンプレート。電子メールテンプレートによって使用される置換項目は、<replacement-data> 要素の子として表示されます。
- 電子メールによって発行者チャネル上のレスポンスが発生する場合に、発行者チャネルの Web ページテンプレートに必要な情報。Web ページテンプレートによって使用

される置換項目は、<url-query> 要素の子として表示されます。これは、<url-data> の子であり、<replacement-data> の子でもあります。

電子メールメッセージに発行者チャネルの Web サーバを指す URL が含まれており、ユーザから情報を取得するために使用される場合、置換データに少なくとも 1 つの responder-dn 項目が含まれている必要があります。responder-dn 項目の値は、メッセージが送信されるユーザのユーザオブジェクトの DN である必要があります。

テンプレートでクエリの置換トークン (271 ページのセクション「置換データ」を参照) が使用されている場合、<message> 要素の置換データには、src-dn、src-entry-id という名前の項目、または適切な値の関連付けが含まれている必要があります。問い合わせが実行される eDirectory オブジェクトがすでに手動タスクサービスドライバに関連付けられている場合のみ、関連項目を使用できます。関連付けられていないオブジェクトに対して加入者によって生成された関連付けは、クエリが発生したときに eDirectory オブジェクトに記述されていないため使用できません。

<message> 要素で、MIME タイプのメッセージ本文を指定できます。MIME タイプが指定され、スタイルシートが指定されていない場合 (つまり、<message> の <stylesheet> 要素の子がない場合)、2 つあるデフォルトのスタイルシート名のいずれかが使用されます。MIME タイプが text/plain の場合、デフォルトのスタイルシート名は process_text_template.xsl です。MIME タイプが text/plain 以外の場合、デフォルトのスタイルシート名は process_template.xsl です。

加入者チャネルの電子メールテンプレート

電子メールテンプレートは、ボイラープレートトークンおよび置換トークンが含まれている XML ドキュメントです。電子メールメッセージ本文のテキストを生成するために、電子メールテンプレートが使用されます。テンプレートに関する一般的な情報については、268 ページの 「テンプレート」を参照してください。

電子メールテンプレートで使用されている置換トークンによって、<mail> 要素を構成する購読者チャネルポリシーによって構成された、<replacement-data> 要素の子として提供される必要がある <item> 要素が指定されます。たとえば、電子メールテンプレートに置換トークン $employee-name$ がある場合、<message> 要素の置換データに <item name= “employee-name” > 要素がある必要があります。従業員名の項目がない場合、テンプレート内の置換トークンによって占められている場所には、電子メールメッセージ \'96\'7b 文のテキストはありません。

プレーンテキスト、HTML、または XML であるメッセージ \'96\'7b 文を生成するために、電子メールテンプレートを使用できます。

電子メールテンプレートによってプレーンテキストのメッセージが生成される場合、そのメッツセージは、出力タイプとしてプレーンテキストを指定するスタイルシートによって処理される必要があります。スタイルシートで出力タイプとしてプレーンテキストが指定されていない場合、望ましくない XML エスケーピングが発生します。デフォルトの手動タスクサービスドライバのスタイルシートである、process_text_template.xsl は、通常、プレーンテキストのテンプレートの処理に使用されます。

発行者チャネルのポリシー

手動タスクサービスドライバのほとんどの実装では、発行者チャネルのポリシーは必要ありません。これは、Web ページおよび XDS テンプレートを構成することができるので、XDS で必要とする結果を得ることができ、XDS がポリシーによってさらに処理される必要がないためです。

ポリシーが必要な場合は、インストールに固有のポリシーになります。

発行者チャネルの Web ページテンプレート

Web ページテンプレートは、ボイラープレートトークンおよび置換トークンが含まれている XML ドキュメントです。Web ページテンプレートは、Web ページのドキュメント (通常は HTML ドキュメント) を生成するために使用されます。テンプレートに関する一般的な情報については、268 ページの 「テンプレート」を参照してください。

Web ページテンプレートの置換トークンにより、購読者チャネルの URL クエリデータとして提供される置換データが指定されます。発行者チャネルの置換データは、HTTP GET 要求の URL クエリ文字列、および HTTP POST 要求の URL クエリ文字列と POST データから取得されます。

購読者チャネルから、電子メールメッセージへ、次に発行者チャネルの Web サーバへの置換データのフローの例として、次のシナリオを考えてみます。

手動タスクサービスドライバは、新しい従業員に部屋番号を割り当てることを新しい従業員のマネージャに依頼するように設定されています。マネージャに対する電子メールのトリガは、購読者チャネルのコマンド変換ポリシーによって処理される、新しいユーザオブジェクトの <add> コマンドです。

マネージャが電子メールメッセージの URL をクリックすると、マネージャの Web ブラウザに Web ページが表示されます。Web ページでは、誰のために \'83\'7d ネージャが部屋番号を入力しているのかを示す必要があります。

これを実行するには、名前で新しいユーザを識別する置換データ項目が購読者チャネルの <url-query> 要素に含まれています。

```
<item name=”subject-name”>Joe the Intern</item>
```

これにより、URL クエリ文字列には (他の文字列の間に)「subject-name=Joe%20the%20Intern」が含まれます「%20」は URL エンコードスペースです。

マネージャが電子メールメッセージの URL をクリックすると、マネージャの Web ブラウザから発行者チャネルの Web サーバに URL が送信されます。Web サーバによって、「subject-name」という名前の置換データ項目が「Joe the Intern」という値とともに \'8d\'5c 成されます。

URL によっても指定されている Web ページテンプレートには、置換トークン $subject-name$ が含まれます。Web ページを \'8d\'5c 成するために Web ページテンプレートがスタイルシートによって処理されると、置換トークンが「Joe the Intern」に置換されます。これにより、ユーザオブジェクトの作成によって電子メールが送信された従業員の Web ページがカスタ \'83\'7d イズされます。

加入者チャネルから発行者チャネルへのトランザクションの追加的な情報については、347 ページの付録 H「手動タスクサービスドライバ : 新しい従業員のデータフローシナリオ」を参照してください。

発行者チャネルの XDS テンプレート

XDS テンプレートは、ボイラープレートトークンおよび置換トークンが含まれている XML ドキュメントです。XDS テンプレートは、手動タスクサービスドライバの発行者チャネルの Identity Manager に送信された XDS ドキュメントを生成するために使用されま

す。テンプレートに関する一般的な情報については、268 ページの 「テンプレート」を参照してください。

XDS テンプレートの置換トークンによって、HTTP POST 要求のデータとして Web サーバに提供されたいくつか置換データが指定されます。

たとえば、次の XDS テンプレートについて考えてみます。

```
<nds>
  <input>
    <modify class-name="User" src-dn="not-applicable">
      <association>$association$</association>
      <modify-attr attr-name="roomNumber">
        <remove-all-values/>
        <add-value>
          <value>$room-number$</value>
        </add-value>
      </modify-attr>
    </modify>
  </input>
</nds>
```

HTTP POST データが関連付けの値および room-number の値を提供する必要があることが、テンプレートの置換トークンによって指定されます。

通常、関連付けの値は購読者チャネルで生成されます。購読者チャネルの電子メールには、電子メールメッセージに配置される URL のクエリ文字列内の association=value が配置されます。URL が Web サーバに送信されたときに Web ページを生成するために使用される Web ページテンプレートでは、通常、非 \'95\'5c 示の INPUT 要素に関連付けの値が配置されます。

```
<INPUT TYPE="hidden" NAME="association" VALUE="$association$"/>
```

非表示の INPUT 要素として関連付けの値を配置すると、「association=value」のペアが HTTP POST データの一部として送信されます。

次に似た INPUT 要素を使用して、Web ページに room-number の値が入力されます。

```
<input TYPE="text" NAME="room-number" SIZE="20" MAXLENGTH="20"/>
```

マネージャが「1234」と入力して［送信］をクリックした場合、Web ブラウザによって「room-number=1234」が HTTP POST データの一部として送信されます。

次に、Web サーバによって <item name=“association”> 置換データ項目、および XDS テンプレートを処理するときに使用された <item name=“room-number”> 置換データ項目が生成されます。

XDS ドキュメントが、POST データで指定されたスタイルシート付きの XDS テンプレートを処理することにより生成され、その XDS ドキュメントが手動タスクサービスドライバの発行者チャネル上の Identity Manager に送信されます。

トレースの設定

手動タスクサービスドライバでは、さまざまなトレースレベルのメッセージが出力されます。

レベル	トレースメッセージの説明
0	トレースメッセージはありません
1	トレースの基 \'96\'7b 的な操作の単一行のメッセージ
2	追加のメッセージはありません (メタディレクトリエンジンは、このレベル以上で XML ドキュメントがトレースされます)
3	追加的なメッセージはありません
4	テンプレートおよびスタイルシートからの、ドキュメントの \'8d\'5c 成に関連するメッセージ
5	置換データのドキュメントがトレースされています

10.2.4 補足情報

手動タスクサービスドライバの設定の詳細については、以下のセクションを参照してください。

- 331 ページの付録 D「手動タスクサービスドライバ : 置換データ」
- 337 ページの付録 E「手動タスクサービスドライバ : 自動置換データ項目」
- 339 ページの付録 F「手動タスクサービスドライバ : テンプレートアクション要素の参照」
- 343 ページの付録 G「手動タスクサービスドライバ : <mail> 要素参照」
- 347 ページの付録 H「手動タスクサービスドライバ : 新しい従業員のデータフローシナリオ」
- 359 ページの付録 I「手動タスクサービスドライバ : 購読者チャネル用のカスタム要素ハンドラ」
- 361 ページの付録 J「手動タスクサービスドライバ : 発行者チャネル用のカスタムサーブレット」

10.3 ループバックサービスドライバ

ループバックサービスドライバは、購読者チャネルから同じドライバの発行者チャネルに送信されたすべての操作を転送するユーティリティドライバです。ループバックサービスドライバは、ポリシーに実装できるさまざまなカスタム動作を実装するために使用できます。

このドライバは、外部アプリケーションとは通信しません。購読者チャネルから同じドライバの発行者チャネルに操作が転送されます。

ループバックサービスドライバは、Identity Manager インストールプログラムを使用して［メタディレクトリサーバ］オプションをインストールするときに自動的にインストールされます。このドライバは、Identity Manager およびリモートローダサービスによってサポートされているプラットフォームで稼動します。このドライバは、個別に起動する必要はありません。メタディレクトリエンジンをアクティブにすると、このドライバもアクティブになります。

このドライバの基本設定には、多くの情報は含まれていません。

- ポリシーはありません。
- 空のフィルタがあります。
- 発行者ハートビートの設定オプションがありますが、「無効」に設定されています。
- ドライバをインポートするときに、プロンプト情報は表示されません。

ループバックドライバを設定する

1. iManager で、［*Identity Manager ユーティリティ*］>［*インポート環境設定*］の順に選択します。
2. ドライバセットを選択し、［*次へ*］*をクリックします。*

   このドライバを新しいドライバセットに配置する場合は、ドライバセット名、コンテキスト、および関連サーバを指定する必要があります。
3. ドライバの環境設定をソートする方法を選択します。
   - すべての環境設定
   - Identity Manager 3.5 環境設定
   - Identity Manager 3.0 環境設定
   - IDM バージョンに関連付けられていない環境設定
4. ［*ループバックサービスドライバ*］を選択して、［*次へ*］をクリックします。
5. ドライバの名前を指定して、［*次へ*］をクリックします。
6. ドライバの同等セキュリティを定義して、管理者の役割から複製を除外し、［*次へ*］をクリックします。
7. サマリを読んで、［*完了*］をクリックします。

10.4 Null サービスドライバ

Null サービスドライバでは、ポリシーに完全に実装されているタスクを実行するためにドライバシムを設定できる最小限のドライバが提供されます。これは、機能面ではループバックドライバと似ています。1 つ重要な違いがあり、Null サービスドライバでは購読者チャネルから発行者チャネルへの接続は行われず、大部分の操作のシンクとして動作し、操作がシミュレートされて「成功」が返されます。発行者チャネルから Identity Manager エンジンに送信される唯一の情報は、ドライバのハートビートです。

Null サービスドライバは、Identity Manager インストールプログラムを使用して［メタディレクトリサーバ］オプションをインストールするときに自動的にインストールされます。このドライバは、Identity Manager およびリモートローダサービスによってサポートされているプラットフォームで稼動します。このドライバは、個別に起動する必要はありません。メタディレクトリエンジンをアクティブにすると、このドライバもアクティブになります。

このドライバの基本設定には、多くの情報は含まれていません。

- ポリシーはありません。
- 空のフィルタがあります。
- 発行者ハートビートの設定オプションがありますが、「無効」に設定されています。
- ドライバをインポートするときに、プロンプト情報は表示されません。

Null サービスドライバの一般的な使用法には、以下のものが含まれます。

- 購読者フィルタでの変更、クラスの*同期*および属性の*通知*を監視するクラスと属性を追加する。
- 特定のオブジェクトまたは属性の変更に反応して、以下のようなアクションを実行する購読者イベント変換ポリシーを追加する。
  - 識別ボールトに変更内容を戻す (ソース属性およびオブジェクトを操作するアクションを使用)。
  - 電子メールを送信する。
  - カスタム監査イベントを生成する。
  - Identity Manager の外部で発生する変更を伝えるために拡張機能を呼び出す。
- すべてのイベントを拒否する最終的な購読者イベント変換ポリシーを追加する。

Null サービスドライバを設定する

1. iManager で、［*Identity Manager ユーティリティ*］>［*インポート環境設定*］の順に選択します。
2. ドライバセットを選択し、［次へ］*をクリックします。*

   このドライバを新しいドライバセットに配置する場合は、ドライバセット名、コンテキスト、および関連サーバを指定する必要があります。
3. ドライバの環境設定をソートする方法を選択します。
   - すべての環境設定
   - Identity Manager 3.5 環境設定
   - Identity Manager 3.0 環境設定
   - IDM バージョンに関連付けられていない環境設定
4. ［*Null サービスドライバ*］を選択して、［*次へ*］をクリックします。
5. ドライバの名前を指定して、［*次へ*］をクリックします。
6. ドライバの同等セキュリティを定義して、管理者の役割から複製を除外し、［*次へ*］をクリックします。
7. サマリを読んで、［*完了*］をクリックします。

10.5 エンジン制御値

エンジン制御値は、メタディレクトリエンジンのデフォルトの特定動作を変更するために使用できる手段です。これらの値には、サーバがドライバセットオブジェクトと関連付けられている場合のみアクセスできます。

iManager で :

1. ［*Identity Manager*］>［*Identity Manager の概要*］の順にクリックし、［*検索*］をクリックして、そのドライバに関連付けられているドライバセットを検索します。
2. ドライバを参照して、ドライバアイコンの右上隅をクリックします。
3. ［*プロパティの編集*］>［*エンジン制御値*］の順にクリックします。

   エンジン制御値の一覧については、表 10-1 を参照してください、

Designer で :

1. モデラーで、ドライバ行を右クリックします。
2. ［*プロパティ*］>［*エンジン制御値*］の順に選択します。
3. ［*サーバのエンジンコントロール*］フィールドの右側にあるツールヒントアイコンをクリックします。サーバが識別ボールトと関連付けられており、ユーザが認証されている場合、エンジン制御値が大きなペインで表示されます。

   エンジン制御値の一覧については、表 10-1 を参照してください、

表 10-1 *エンジン制御値*

オプション	説明
購読者チャネル再試行間隔 (秒単位)	購読者チャネル再試行間隔では、アプリケーションシムの購読者オブジェクトから再試行ステータスが戻された後で、メタディレクトリエンジンがキャッシュ済みトランザクションの処理を再試行する頻度を制御します。
DN 構文属性値の完全修飾フォーム	DN 構文属性値の修飾指定では、DN 構文属性値を非修飾スラッシュ形式で表すか、完全修飾スラッシュ形式で表すかを制御します。True の設定は、値が修飾形式で表わされていることを意味します。
名前変更イベント用の修飾形式	名前変更イベント用の修飾形式では、名前変更イベントの識別ボールトから取得する新しい名前の部分をタイプ識別子とともに購読者チャネルに表示するかどうかを制御します。たとえば、「CN=」というようになります。True の設定は、名前が修飾形式で表わされていることを意味します。
最大 eDirectory 複製待機時間 (秒単位):	最大 eDirectory™ 複製待機時間では、特定の変更をローカルレプリカとリモートレプリカ間で複製するまでにメタディレクトリエンジンが待機する最大時間を制御します。これは、操作を実行するために同じツリーにあるリモート eDirectory 得サーバに、メタディレクトリエンジンが接続する必要があり、操作 (Identity Manager サーバが移動オブジェクトのマスタレプリカを保持していないときのオブジェクト移動、テンプレートから作成されたユーザのファイルシステムの権利操作など) が完了する前にリモートサーバとの間で変更が複製されるのを待機する必要がある場合にのみ作用します。
XSLT 未準拠バックワード互換モードの使用	このコントロールでは、メタディレクトリエンジンが使用する XSLT プロセッサをバックワード互換モードに設定します。バックワード互換モードにより、XPath 1.0 および XSLT 1.0 標準に準拠しない 1 つまたは複数の動作が XSLT プロセッサで使用されます。これは、標準でない動作に依存する既存の DirXML® スタイルシートがあるバックワード互換性が関与することで行われます。 たとえば、1 つのオペランドがノードセットであり、もう一方のオペランドがノードセット以外であるときの XPath "!=" 演算子の動作は Identity Manager 2.0 までの DirXML リリースでは不正です。この動作は修正されましたが、修正された動作は、既存の DirXML スタイルシートとのバックワード互換性を確保するために、この制御により無効に設定されています。

オプション	説明
一度に移行するアプリケーションオブジェクトの最大数	このコントロールは、アプリケーションからのオブジェクトの移行操作の一部として実行される 1 回のクエリの間に、メタディレクトリエンジンがアプリケーションから要求するアプリケーションオブジェクトの数を制限するために使用します。 アプリケーションからの移行操作中に、java.lang.OutOfMemoryError エラーが発生する場合、この数はデフォルト値より少なくする必要があります。デフォルトは 50 です。 **注 :** このコントロールによって移行できるアプリケーションオブジェクト数は制限されません。バッチサイズが制限されるだけです。
識別ボールトに作成されたオブジェクトに creatorsName を設定する	このコントロールは、このドライバにより識別ボールトに作成されたすべてのオブジェクトのこのドライバの DN に creatorsName 属性を設定するかどうかを決定するために、Identity Manager エンジンによって使用されます。 creatorsName 属性を設定すると、このドライバによってされたオブジェクトを容易に識別できるようになりますが、パフォーマンス上のペナルティも発生します。この属性を設定しない場合、creatorsName 属性は、デフォルトで、ドライバをホストする NCP™ サーバオブジェクトの DN に設定されます。
保留中の関連付けの書き込み	このコントロールは、購読者チャネルでの処理中に Identity Manager で保留中の関連付けをオブジェクトに書き込むかどうかを判断します。 保留中の関連付けを書き込むメリットはほとんど (またはまったく) ないにもかかわらず、パフォーマンスには悪影響を与えてしまいます。それにもかかわらず、後方互換性のためにこれをオンにするオプションが存在しています。
パスワードイベント値の使用	このコントロールは、購読者チャネルの追加および変更イベント用に nspmDistributionPassword 属性に対して報告された値のソースを判断します。 このコントロールを False に設定すると、nspmDistributionPassword の現在の値が取得され、属性イベントの値として報告されます。つまり、現在のパスワード値のみが利用可能です。これはデフォルトの動作です。 このコントロールを True に設定すると、eDirectory イベントとともに記録された値が復号化され、属性イベントの値として報告されます。つまり、イベントの際に、古いパスワード値 (存在する場合) と置換用パスワード値の両方が利用可能です。これは、新しいパスワードを設定できるようにするために古いパスワードが必要な特定のアプリケーションとパスワードを同期する場合に便利です。
パスワード同期ステータス報告の有効化	このコントロールは、購読者チャネルパスワードの変更イベントのステータスを Identity Manager エンジンが報告するか動かを判断します。 購読者チャネルのパスワード変更イベントのステータスを報告すると、Identity Manager ユーザアプリケーションなどのアプリケーションは、接続アプリケーションと同期する必要があるパスワード変更の同期の進行状況を監視することができます。

高可用性

11

Identity Manager を共有ストレージで使用し、高可用性を実現できます。クラスタリング環境で Novell® eDirectory™ および Identity Manager を使用するには、いくつかのステップを実行する必要があります。

この節では、次の項目について説明します。

11.1 Linux および UNIX で共有ストレージを使用するための、eDirectory および Identity Manager の設定

このセクションでは、共有ストレージを使用して高可用性クラスタのフェールオーバーを実現できるように、eDirectory および Identity Manager を設定する方法について説明します。この節の説明は、特定のクラスタ \'83\'7d ネージャに固有のものではなく、Linux または UNIX プラットフォーム上の高可用性クラスタの共有ストレージ一般に当てはまります。

基本的な概念は、eDirectory および Identity Manager の状態データを共有ストレージに配置し、サービスを現在実行しているクラスタノードから利用できるようにするということです。つまり、通常は /var/nds/dib にある eDirectory データストアをクラスタ共有ストレージに再配置する必要があります。Identity Manager の状態データも /var/nds/dib にあります。クラスタノード上の各 eDirectory インスタンスは、共有ストレージのデータストアを使用するように設定する必要があります。その他の eDirectory の設定データも、共有ストレージに常駐する必要があります。

eDirectory データストアの他に、サーバ固有のキーをクラスタノード間で複製するために、NICI (Novell International Cryptographic Infrastructure) のデータも共有する必要があります。一般的には、NICI のデータを共有ストレージに移動するのではなく、NICI のデータを各クラスタノードのローカルストレージにコピーする方が適切です。クラスタノードがセカンダリ状態になっていて共有ストレージをホストしていない場合でも、クライアントの NICI 機 \'94\'5c をクラスタノード上で使用できるようにするために、この方法をお勧めします。

以降の節では、次の前提に基づいて、eDirectory および NICI のデータの共有について説明します。

- NICI、eDirectory、および Identity Manager のデータと設定には、デフォルトのインストール先を使用している。

  Identity Manager のデータについて、eDirectory のデータとは別に説明することはしません。関連する Identity Manager のデータは eDirectory のデータと同じ場所に配置されているためです。
- eDirectory および Identity Manager のインストール手順を熟知している。

- 2 ノードクラスタを使用している。

  2 ノードクラスタは、高可用性を実現するために最も一般的に使用されている設定です。ただし、この節で説明する概念は、*n* ノードクラスタにも容易に拡張できます。

この節では、次の項目について説明します。

11.1.1 eDirectory をインストールする

注 : NICI は、eDirectory インストール手順の一部としてインストールされます。

1. プライ \'83\'7d リクラスタノードに eDirectory をインストールします。
2. プライマリクラスタノードで eDirectory を設定します。プライマリクラスタノードに新しいツリーを作成するか、既存のツリーにサーバをインストールします。
   eDirectory サーバの名前には、UNIX サーバの名前に使用していないものを使用します。クラスタノードの 1 つに固有の名前を使用するのではなく、クラスタに共通の名前を使用してください。
3. セカンダリクラスタノードに、同じバージョンの eDirectory をインストールします。セカンダリクラスタノードでは eDirectory を設定しないでください。

   セカンダリノードには個別のツリーはありません。

11.1.2 Identity Manager のインストール

1. *［Metadirectory Server］オプションを使用して、プライ \'83\'7d リクラスタノードに Identity Manager をインストールします。*

   インストールプロセスにより、Identity Manager ファイルがインストールされ、Identity Manager で使用する eDirectory ツリーが設定されます。
2. セカンダリクラスタスイッチを使用し、セカンダリクラスタに同じバージョンの Identity Manager をインストールします。次を入力します。
   `dirxml_platform.bin -DCLUSTER_INSTALL="true"`

   インストールでは、*［Metadirectory Server］オプションを選択します。*

   セカンダリクラスタスイッチを使用すると、Identity Manager ファイルがインストールされますが、追加の eDirectory 設定は実行されません。セカンダリノードには個別のツリーがないので、設定は必要ありません。

11.1.3 NICI データの共有

NICI は、eDirectory、Identity Manager、および Novell クライアントアプリケーションで使用される暗号化サービスを提供します。eDirectory とともに使用する場合、NICI はサーバ

固有のキーを提供します。これらのサーバ固有のキーは、eDirectory がクラスタサービスとして実行されるすべてのクラスタノードで同じでなければなりません。

NICI データの共有には、2 つの方法があります。

- NICI データをクラスタ共有ストレージに配置する

  この方法の短所は、クラスタノードが共有ストレージをホストしていない場合、NICI に依存するアプリケーションはそのクラスタノード上でエラーを引き起こす点です。
- プライ \'83\'7d リサーバからセカンダリサーバのローカル保存領域に NICI データをコピーする。

NICI データをコピーする

1. セカンダリクラスタノードの /var/novell/nici を、(/var/novell/nici.sav などの) 別の名前に変更します。
2. プライ \'83\'7d リクラスタノードからセカンダリクラスタノードに /var/novell/nici ディレクトリをコピーします。

   このためには、scp を使用するか、またはプライ \'83\'7d リノードの /var/novell/nici ディレクトリのファイルを作成してセカンダリノードに転送し、セカンダリノードのディレクトリで解凍 (untar) します。

11.1.4 eDirectory および Identity Manager のデータの共有

デフォルトでは、eDirectory では、/var/nds/dib にデータストアが格納されます。設定および状態のその他の項目も、/var/nds とそのサブディレクトリに格納されます。eDirectory のデフォルトの設定ディレクトリは、/etc です。以下は、高可用性クラスタの共有ストレージとともに使用するために eDirectory および Identity Manager を設定するために必要なステップです。これらの手順は、共有ストレージが /shared に \'83\'7d ウントされていることを前提としています。

- 289 ページの 「プライ \'83\'7d リノード上の手順」
- 290 ページの 「セカンダリノード上の手順」

プライ \'83\'7d リノード上の手順

1. /var/nds ディレクトリのサブツリーを /shared/var/nds にコピーします。
2. /var/nds ディレクトリを別の名前 (たとえば /var/nds.sav) に名前変更します。

   必ずしも必要ではありませんが、この時点でバックアップを作成すると、必要に応じて eDirectory を再インストールすることなく作業をやり直すことができます。
3. /var/nds to /shared/var/nds からのシン \'83\'7b リックリンク (たとえば ln -s /shared/var/nds /var/nds) を作成します。
4. 次のシン \'83\'7b リックリンクを作成します。

リンク元	リンク先
/shared/var/nds/class16.conf	/etc/class16.conf
/shared/var/nds/class32.conf	/etc/class32.conf

リンク元	リンク先
/shared/var/nds/help.conf	/etc/help.conf
/shared/var/nds/ndsimonhealth.conf	/etc/ndsimonhealth.conf
/shared/var/nds/miscicon.conf	/etc/miscicon.conf
/shared/var/nds/ndsimon.conf	/etc/ndsimon.conf
/shared/var/nds/macaddr	/etc/macaddr

5 /etc/nds.conf のバックアップコピーを作成します。

6 /etc/nds.conf を /shared/var/nds に移動します。

7 /shared/var/nds/nds.conf を編集し、次のエントリをファイルに \'91\'7d 入します (現在のエントリを同じ名前で上書きします)。

- n4u.nds.dibdir=/shared/var/nds/dib
- n4u.server.configdir=/shared/var/nds
- n4u.server.vardir=/shared/var/nds
- n4u.nds.preferred-server=localhost

次のエントリについては、eth0:0 をクラスタ共有 Ethernet インタフェースのインタフェース名に置き換えます。lo も、ローカルホスト Ethernet インタフェースのインタフェース名に置き換えます。

- n4u.nds.server.interfaces=eth0:0@524,lo@524
- http.server.interfaces=eth0:0@8008,lo@8008
- https.server.interfaces=eth0:0@8009,lo@8009

8 /etc/nds.conf から /shared/var/nds/nds.conf にシンボリックリンクを作成します。

9 ndsd を起動し、ndsd が共有ストレージで動作することを確認します。

10 ndsd を停止します。

11 ndsd を、ホストするリ \'83\'5cースのクラスタ \'83\'7d ネージャのリストに配置します。

12 ndsd をデーモンのリストから削除し、起動時に初期化プロセスによって起動されるようにします。

セカンダリノード上の手順

1 /var/nds ディレクトリを別の名前 (たとえば /var/nds.sav) に変更します。厳密には必要ありませんが、バックアップを作成すると、必要に応じて eDirectory を再インストールすることなく作業をやり直すことができます。

2 /var/nds から /shared/var/nds にシンボリックリンクを作成します。

3 /etc/nds.conf のバックアップコピーを作成します。

4 /etc/nds.conf を削除します。

5 /etc/nds.conf から /shared/var/nds/nds.conf にシンボリックリンクを作成します。

6 ndsd を、ホストするリ \'83\'5cースのクラスタ \'83\'7d ネージャのリストに配置します。

7 ndsd をデーモンのリストから削除し、起動時に初期化プロセスによって起動されるようにします。

プライ \'83\'7d リノードおよびセカンダリノードの手順が完了した後、クラスタサービスを起動します。プライ \'83\'7d リノードで、eDirectory および Identity Manager が起動します。

11.1.5 Identity Manager ドライバの考慮事項

Identity Manager ドライバのほとんどは、クラスタ設定で実行できます。ただし、次のことを考慮する必要があります。

- 実行可 \'94\'5c ドライバ (.jar ファイルまたは共有オブジェクト、あるいはその両方) は、各クラスタノードにインストールする必要があります。
- ドライバがサポートするアプリケーションと同じサーバでドライバを実行する必要がある場合、アプリケーションもクラスタサービスの一部として実行されるよう設定する必要があります。
- ドライバで、ドライバ固有の状態データを保存する場所が設定可 \'94\'5c な場合、その場所はクラスタ共有ストレージ上に存在する必要があります。

  たとえば、変更ログなしで使用する LDAP ドライバ、トリガレスモードで使用する JDBC ドライバなどです。
- ドライバが設定データを eDirectory の外部に格納する場合、その設定データは共有ストレージに配置するか、各クラスタノードに複製する必要があります。たとえば、Manual Task Driver のテンプレートディレクトリなどです。

11.2 SuSE Linux についてのケーススタディ

SUSE LINUX Enterprise Server 8 とともに共有ストレージで実行されている Identity Manager の詳細については、TID10093317 (http://support.novell.com/cgi-bin/search/searchtid.cgi?/10093317.htm) を参照してください。

Identity Manager ライセンスの監査 12

Novell® Identity Manager ライセンス監査ツールを使用すると、次のライセンス使用数を判定できます。

- 特定のツリー内の Identity Manager ライセンス
- 特定の追加料金ドライバのライセンス
- Novell SecretStore® ライセンス
- Protocom* SecureLogin ライセンス

Identity Manager ライセンスは、次の条件を満たす各オブジェクトに対してカウントされます。

- オブジェクトが、Identity Manager ドライバ内で関連付けられている。
- Identity Manager ドライバの関連付けに有効な関連付けキーがある。
- 関連付けキーが「無効」とマークされていない。

追加のドライバライセンスは、追加料金ドライバに対して無効ではない有効な関連付けが 1 つ以上あるオブジェクトに対してカウントされます。この概念は、298 ページのセクション 12.3「監査結果の理解」でより詳細に説明されています。

ライセンス監査ツールは、要求に応じてレポートを生成します。監査を後で実行するようにスケジュールすることもできます。監査をスケジュールすると、ライセンス監査ツールのグラフィカルインタフェースは変更できないようにロックされます。グラフィカルインタフェースは、パスワードを入力してロックを解除しない限り、監査が完了するまでロックされたままになります。

この項では、次のトピックについて説明します。

12.1 ライセンス監査ツールのインストール

ライセンス監査ツールは、Windows マシンまたは Linux マシンにインストールできます。インストール後、ライセンス監査ツールを使用して、指定した eDirectory サーバの関連付けを監査できます。

12.1.1 Windows でのインストール

Identity Manager のインストールルーチンにより、Windows にはデフォルトでライセンス監査ツールがインストールされます。Identity Manager のインストール時に［ユーティリ

ティ］チェックボックスをオフにした場合は、ライセンス監査ツールを別途インストールする必要があります。

1 Identity Manager インストール (install.exe) ユーティリティを起動します。

［*Please Select Components to Install (インストールするコンポーネントを選択してください)*］ページが表示されるまで、通常どおりインストールルーチンを実行します。

2 ［*ユーティリティ*］を選択して、［*次へ*］をクリックします。

3 インストールパスを指定して、［*次へ*］をクリックします。

デフォルトの場所は、C:\Novell\NDS\DirXMLUtilities です。

4 インストールするユーティリティを選択し、［*次へ*］をクリックします。

［*ライセンス監査ツール*］が選択されていることを確認してください。

5 ［Installation Summary (インストールの概要)］ページで、［*完了*］をクリックして、選択したユーティリティをインストールします。

6 ［インストールが完了しました］ページで、［*閉じる*］をクリックします。

これでライセンス監査ツールがインストールされました。

ライセンス監査ツールは、4 つの .jar ファイル (AuditMain.jar、forms_rt.jar、ldap.jar、および ObjDisabler.jar) と、2 つの .bat ファイル (idmadt.bat および idmlat.bat) で構成されています。これらのファイルは、Identity Manager CD-ROM またはイメージファイルの \nt\dirxml\utilities\idm_lat にあります。

12.1.2 Linux でのインストール

ライセンス監査ツールは、Linux/UNIX プラットフォームでも使用できますが、インストールルーチンの一部としてはインストールされません。ライセンス監査ツールをインストールするには、次のステップを完了します。

1 Identity Manager CD-ROM またはイメージファイルで、ライセンス監査ツールのファイルを検索します。

ライセンス監査ツールのファイルは、/linux/setup/utilities/idm_lat にあります。

2 次のファイルを Linux/UNIX ファイルシステムにコピーします。

- AuditMain.jar
- forms_rt.jar
- ldap.jar
- ObjDisabler.jar
- idmadt
- idmlat

12.2 システムの監査

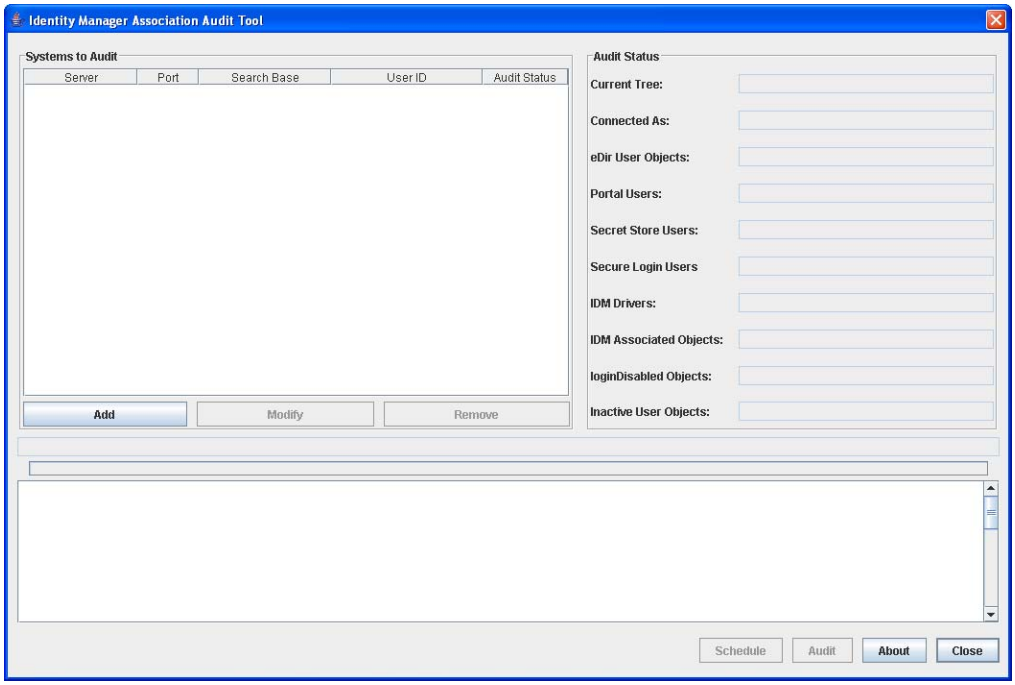
ライセンス監査ツールを使用してシステムを監査する際には、次のステップを実行します。各ステップについては、該当する項で説明されています。ツールがロードされた後の

プロセスは、ライセンス監査ツールがサポートされているすべてのプラットフォームで同一です。

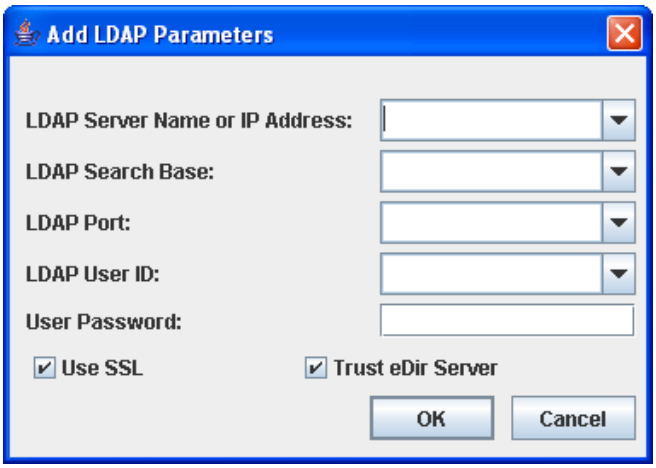
- 295 ページのセクション 12.2.1「監査パラメータの設定」
- 297 ページのセクション 12.2.2「監査のスケジュール」
- 298 ページのセクション 12.2.3「ライセンス監査ツールのロック解除」
- 298 ページのセクション 12.2.4「監査結果の保存」

12.2.1 監査パラメータの設定

1 Windows では .bat ファイル、Linux/UNIX ではスクリプトファイルである idmlat を起動して、ライセンス監査ツールを開きます。次の図は、ライセンス監査ツールのユーザインタフェースを示しています。



2 ［*追加*］をクリックして、監査するサーバを選択します。



3 ターゲットの LDAP サーバに関する必要な情報を入力して、［*OK*］をクリックします。

LDAP Server Name or IP Address (LDAP サーバ名または IP アドレス): ディレクトリツリーを監査するために、ライセンス監査ツールが接続する LDAP サーバを指定します。

LDAP Search Base (LDAP 検索ベース): ライセンス監査ツールが監査を実行するディレクトリコンテナを指定します。

有効な LDAP DN (例 : ou=dirxml,o=provo) を使用します。ツリーのルートから監査を開始するには、< なし > を指定するか、このフィールドを空白のままにします。

LDAP ポート : 指定したサーバの LDAP サービスを検索するためにライセンス監査ツールが使用するポートを指定します。

ポート 389 はデフォルトの LDAP ポートで、ポート 636 はセキュアな LDAP アクセス (SSL 経由) のためのデフォルトのポートです。ただし、識別ボールトの LDAP ポートは設定可能なため、指定したサーバに対して有効なポートを使用していることを確認してください。

LDAP User ID (LDAP ユーザ ID): LDAP サーバに接続するためにライセンス監査ツールが使用するユーザ ID を指定します。

SSL 経由で接続している場合は、このパラメータを指定する必要があります。

指定したユーザ ID に、ツリー内のすべてのオブジェクトへのアクセス権があることを確認してください。この値には anonymous を指定できますが、anonymous には十分な権利がないため、監査するオブジェクトをすべて表示できない場合があります。

ユーザパスワード : LDAP サーバに接続するためにライセンス監査ツールが使用するユーザパスワードを指定します。

これは、［LDAP User ID (LDAP ユーザ ID)］フィールドで指定したユーザのパスワードです。［LDAP User ID (LDAP ユーザ ID)］で anonymous を指定した場合は、値を入力しないでください。

SSL の使用 : LDAP サーバに接続するときにライセンス監査ツールが SSL を使用するように指定するには、このオプションを選択します。選択すると、ライセンス監査ツールは、［*LDAP ポート*］フィールドで指定したポートに対する SSL バインドを試みます。

Trust eDir Server (eDir サーバを信頼する): ライセンス監査ツールが指定した eDirectory サーバを信頼できるように指定するには、このオプションを選択します。

ライセンス監査ツールは、Novell LDAP SDK の特別な機能を使用して、ライセンス監査ツールがすでに LDAP サーバを信頼していることを LDAP SSL クライアントに通知します。つまり、SSL を使用する際に、ライセンス監査ツールにはサーバの証明書のコピーが必要なくなります。

ライセンス監査ツールが使用されるコンテキストを考慮すると、これは有効な方法です。これにより、ユーザはサーバの証明書のコピーを取得しなくても、ライセンス監査ツールで SSL を使用できます。サーバの証明書を信頼するようにライセンス監査ツールを設定することもできます。

4 (オプション) 必要に応じて、ステップ 2 とステップ 3 を繰り返して、監査を実行する他の LDAP サーバを追加します。

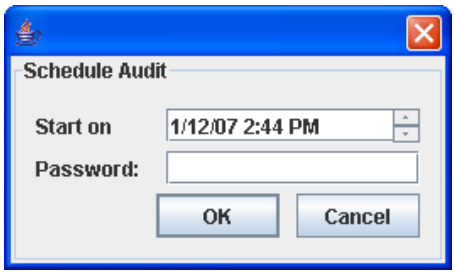
12.2.2 監査のスケジュール

必要な LDAP パラメータを指定したら、［*監査*］ボタンをクリックしてただちに監査を実行できます。または、［*スケジュール*］をクリックして、特定の日時に監査を実行するよう設定します。ツリーの監査はツリーのサイズによっては時間がかかることがあるので、可能であれば、ピーク時間を避けて監査を実行するようにスケジュールしてください。

監査をスケジュールするには、次のステップを完了します。監査をスケジュールすると、ライセンス監査ツールのインタフェースはロックされます。

1 ライセンス監査ツールで、［*スケジュール*］をクリックします。

監査をスケジュールするには、最低 1 つの LDAP サーバを設定しておく必要があります。



2 必要なスケジュール情報を指定して、［*OK*］をクリックします。

Start on (開始日時): 監査を開始する日時を指定します。

表示されるフォーマットで日時を指定します。または、フィールドに表示されている数値のいずれかを選択し、フィールドの右側にある矢印を使用して、値を増減します。

パスワード : この監査のパスワードを指定します。

ここに入力するパスワードが監査ツールのロックを解除するキーになります。

監査をスケジュールすると、ライセンス監査ツールのインタフェースがロックされ、他のユーザは監査パラメータや結果を変更できなくなります。監査スケジュールまたはパラメータを変更するためにインタフェースのロックを解除する必要がある場合は、298 ページの 「ライセンス監査ツールのロック解除」を参照してください。

12.2.3 ライセンス監査ツールのロック解除

監査をスケジュールすると、ライセンス監査ツールのインタフェースがロックされ、他のユーザは監査パラメータや結果を変更できなくなります。監査スケジュールまたはパラメータを変更するためにインタフェースのロックを解除するには、監査をスケジュールしたときに指定したパスワードを使用する必要があります。

監査スケジュールより前にライセンス監査ツールのインタフェースをロック解除すると、現在スケジュールされている監査は終了します。

1 ライセンス監査ツールで、［*Unlock (ロック解除)*］をクリックします。

2 監査パスワードを入力して、［*OK*］をクリックします。

12.2.4 監査結果の保存

ライセンス監査ツールで監査が実行されると、［Audit Status (監査ステータス)］ウィンドウに結果が表示されます。さらに、ライセンス監査ツールインタフェースの一番下にあるテキストウィンドウに完全な監査レポートが表示されます。これら 2 つのウィンドウを使用して、監査結果を確認できます。レポートは長くなる可能性があるため、監査データは一連のテキストファイルにも保存されます。

treename-summary.log: 完全な監査レポートが含まれています。

treename-logindisabled.log: (オプション) ログインが無効になっている DNS オブジェクト名のリストが含まれています。

treename-inactiveusers.log: 1 年以上認証されていない DNS オブジェクト名のリストが含まれています。

12.3 監査結果の理解

監査レポートの主要なコンポーネントには、次のものが含まれます。

パラメータの概要 : 監査のパラメータが表示されます。LDAP サーバの情報および監査しているディレクトリツリーが含まれます。

Audit Results Summary (監査結果の概要): Identity Manager の監査で検出された結果の概要が表示されます。これには関連付けられているオブジェクトの数が含まれ、これはツリーで使用されている Identity Manager ベースライセンスの数に対応します。

Object Class Summary (オブジェクトクラスの概要): オブジェクトクラス別にオブジェクトの関連付けが表示されます。

Driver Association Summary (ドライバ関連付けの概要): Identity Manager ドライバ別にオブジェクト関連付けが表示されます。ライセンス監査ツールがドライバを認識した場合は、そのドライバ名が表示されます。認識できない場合、ドライバは < カスタム > としてのみ識別されます。

Driver Summary (ドライバの概要): 監査で識別された各 Identity Manager ドライバの概要が表示されます。ドライバ名とコンテキスト、ドライバモジュール、そのドライバに対して処理されたオブジェクト関連付けの数、および無効になっているオブジェクト関連付けの数が含まれます。

監査レポートの外観は次のようなものになります。

```
Identity Manager License Auditing Tool v1.4Novell, Inc. Copyright 2001
- 2007Audit started Wednesday, November 13, 2007 at 10:49 AMParameter
Summary: LDAP Server Name: 10.1.1.222LDAP Server Port: 636Search Base:
(null)Connected as: cn=admin,o=lab1Tree Name: LABTESTAudit Results
Summary: DLAT found 7061 user objectsDLAT found 0 SecretStore users
DLAT found 0 SecureLogin usersDLAT found 26 DirXML DriversDLAT found
12664 associated objectsObject Class Summary7060 associations to
Object Class inetOrgPerson5604 associations to Object Class
costCenterDriver Association Summary7058 associations to DirXML Driver
for eDirectory drivers4408 associations to DirXML Driver for
Peoplesoft (Consulting Release) drivers12473 associations to <Custom>
drivers12626 associations to DirXML Driver for JDBC drivers12643
associations to DirXML Driver for Peoplesoft driversDriver:
CN=NDSTONDS - PRV-NDS4,CN=NDS DRIVERS,O=SERVICESDriver Name: DirXML
Driver for eDirectoryDriver Module:
com.novell.nds.dirxml.driver.nds.drivershimimplProcessed Associations:
1162  Disabled Associations: 2Driver: CN=WSE - SECURITY,CN=TELECOM
DRIVER SET,O=SERVICESDriver Name: <Custom>Driver
Module:com.novell.nds.dirxml.driver.wsejdbc.wsedrivershimProcessed
Associations: 7033Disabled Associations: 1Driver: CN=PS8
DRIVER,CN=PEOPLESOFT DRIVER,O=SERVICESDriver Name: DirXML Driver for
PeoplesoftDriver Module: npsshim.dllProcessed Associations: 7039
Disabled Associations: 2Driver: CN=BIG USERS DRIVER,CN=BIG EWORKS
PSCOSTCENTER,O=SERVICESDriver Name: DirXML Driver for JDBCDriver
Module: com.novell.nds.dirxml.driver.jdbc.jdbcdrivershimProcessed
Associations: 6978Disabled Associations: 1Driver: CN=PS8 COSTCENTER
DRIVER,CN=BIG EWORKS PSCOSTCENTER,O=SERVICESDriver Name: DirXML Driver
for PeoplesoftDriver Module: npsshim.dllProcessed Associations: 5604
Disabled Associations: 0Audit completed Wednesday, November 13, 2007
at 12:16 PM
```

12.4 ライセンス関連付けの無効化

IDMADT (Identity Manager 関連付け無効ツール) を使用して、Identity Manager を機能させたくないオブジェクトに対する関連付けを無効にできます。IDMADT は、ライセンス監査ツールの出力ファイルを使用して、それらのログファイルからオブジェクトのリストを特定し、オブジェクトの関連付けステータスを ASSOCIATION_DISABLED に変更します。これにより、Identity Manager に対し、それらのオブジェクトの情報の同期化を停止するよう指示します。一度ステータスを変更すると、それらのオブジェクトはライセンス監査ツールでカウントされなくなるので、それらのオブジェクトのライセンスは必要なくなります。

この項では、次のトピックについて説明します。

- 300 ページのセクション 12.4.1「IDMADT のインストール」
- 300 ページのセクション 12.4.2「IDMADT の使用」

12.4.1 IDMADT のインストール

IDMADT は Java v1.4.2 以降と互換性がある Java アプリケーションです。IDMADT をインストールするには、次のファイルを好みのディレクトリにコピーします。

ObjDisabler.jar: IDMADT Java クラス

Ldap.jar: LDAP Java クラス

Forms_rt.jar: ユーザインタフェース Java クラス

Idmadt.bat: IDMADT を実行するための Windows バッチファイル

Idmadt: IDMADT を実行するための Linux スクリプトファイル

12.4.2 IDMADT の使用

IDMADT を使用するには、次の手順で IDMADT を起動します。

1 IDMADT を起動します。

使用しているオペレーティングシステムに応じて、Windows バッチファイル (Idmadt.bat)、または Linux スクリプトファイル (Idmadt) を実行します。

2 必要なパラメータを入力します。

IDMADT には、次のパラメータが必要です。

LDAP Server Nname or IP Address (LDAP サーバ名または IP アドレス): ツリーを監査するために IDMADT が接続する LDAP サーバを指定します。

LDAP ポート : LDAP サービスを検索するために IDMADT が使用するポートを指定します。指定した LDAP サーバで有効な SSL ポートを指定してください。ポート 636 がデフォルトの SSL ポートです。

ユーザ ID: 指定した LDAP サーバに接続するために IDMADT が使用するユーザ ID を指定します。指定したユーザ ID は、ツリー内のすべてのオブジェクトにアクセスできる必要があります。この値に <anonymous> を指定することもできますが、多くの場合、<anonymous> には十分な権利がありません。

LDAP 内のユーザ ID をカンマ区切り形式でタイプフルに指定します。例 : cn=admin,ou=IST,o=MyCompany。

ユーザパスワード : 指定したユーザ ID に対する有効なパスワードを指定します。

入力ファイル : 処理するオブジェクトのリストが含まれているライセンス監査ツールファイルの名前を指定します。<*treename*>-logindisabled.log と <*treename*>-inactiveusers.log という 2 つの関連ファイルがあります。［*開く*］をクリックして、目的のファイルを参照します。

処理するファイルごとに一度、IDMADT を実行する必要があります。

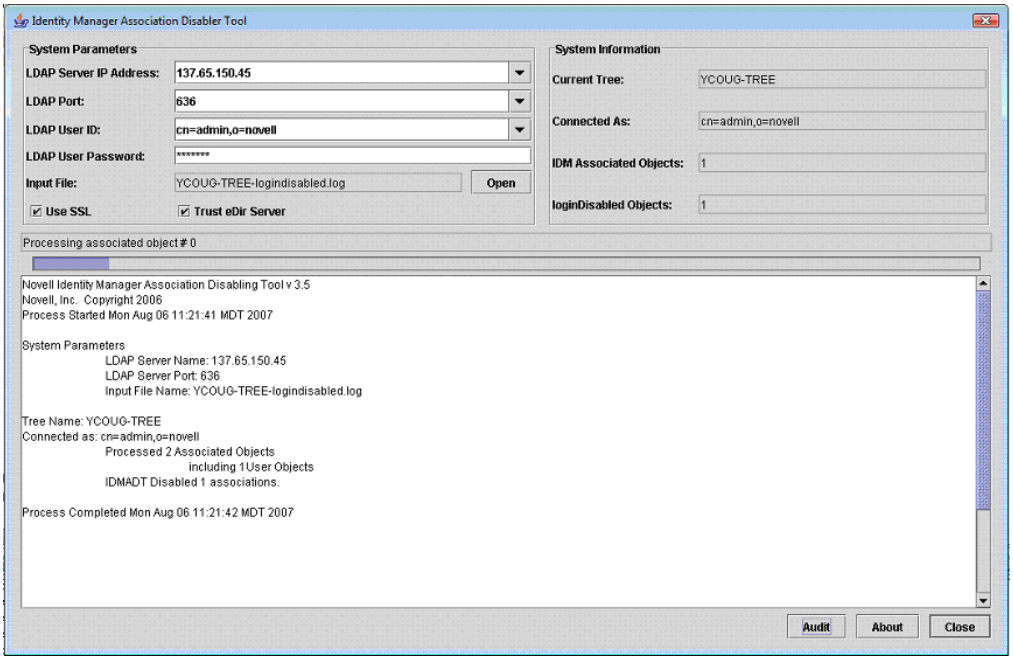
Use SSL (SSL を使用する) および Trust eDir Server (eDir サーバを信頼する):

IDMADT はオブジェクトを変更するため、信頼関係とともに SSL 認証をオンにしてください。

3 ［開始］*をクリックします。*

IDMADT ユーザインタフェースの［システム情報］セクションに LDAP サーバに関する情報が表示されます。現在の操作の進行状況は IDMADT ユーザインタフェースの一番下にあるログペインに表示されます。

現在の処理を中止するには、［*Abort (中止)*］をクリックします。



DirXML コ \'83\'7d ンドラインユーティリティ

A

DirXML® コマンドラインユーティリティを使用すると、ドライバを管理するためにコマンドラインインタフェースを使用できます。コマンドでドライバを管理するためのスクリプトを作成できます。

このユーティリティとスクリプトは、Identity Manager のインストール中にすべてのプラットフォームにインストールされます。ユーティリティは次の場所にインストールされます。

- Windows: \Novell\Nds\dxcmd.bat
- NetWare®: sys:\system\dxcmd.ncf
- UNIX: /usr/bin/dxcmd

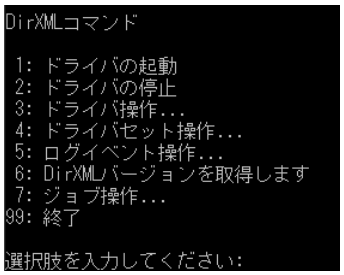
DirXML コマンドラインユーティリティの使用方法には、次の 2 つがあります。

- 303 ページのセクション A.1「インタラクティブモード」
- 312 ページのセクション A.2「コ \'83\'7d ンド ラインモード」

A.1 インタラクティブモード

対話モードには、DirXML コマンドラインユーティリティを制御および使用するためのテキストインタフェースが用意されています。

1. コンソールで、「dxcmd」と入力します。
2. Identity Manager オブジェクトに対する十分な権利を持つユーザの名前 (admin.novell など) を入力します。
3. ユーザのパスワードを入力します。



4. 実行するコマンドの数を入力します。

   304 ページの 表 A-1 はオプションの一覧で、使用できる機能を示しています。
5. ユーティリティを終了するには、「99」と入力します。

注 : UNIX または Linux で eDirectory™ 8.8 を実行している場合、-host および -port パラメータを指定する必要があります。たとえば、「dxcmd -host 10.0.0.1 -port 524」。パラメータを指定しない場合、jclient エラーが発生します。

```
novell.jclient.JCException: connect (to address) 111 UNKNOWN ERROR
```

デフォルトでは、eDirectory 8.8 はローカルホストをリッスンしません。DirXML コマンドラインユーティリティでは、サーバの IP アドレスやホスト名、および認証可能なポートを解決する必要があります。

表 A-1 *インタラクティブモードのオプション*

オプション	説明
1: *ドライバの起動*	ドライバを起動します。複数のドライバがある場合、各ドライバは番号付きで一覧表示されます。ドライバを起動するドライバの番号を入力します。
2: *ドライバの停止*	ドライバを停止します。複数のドライバがある場合、各ドライバは番号付きで一覧表示されます。ドライバを停止するドライバの番号を入力します。
3: *ドライバ操作*	ドライバに対して実行可能な操作が一覧表示されます。複数のドライバがある場合、各ドライバは番号付きで一覧表示されます。実行可能な操作を表示するドライバの番号を入力します。操作の一覧については、305 ページの 表 A-2 を参照してください。
4: *ドライバセット操作*	ドライバセットに対して実行可 \'94\'5c な操作が一覧 \'95\'5c 示されます。 ◆ 1: ドライバセットをサーバと関連付けます ◆ 2: ドライバセットのサーバとの関連付けを解除します ◆ 99: 終了
5: *ログイベント操作*	Novell® Audit を介したイベントのログに対して実行可能な操作を一覧表示します。これらのオプションの詳細については、310 ページの 表 A-5 を参照してください。
6: *DirXML バージョンの取得*	インストールされた Identity Manager のバージョンを一覧 \'95\'5c 示します。
7: *ジョブ操作*	Identity Manager 用に作成されたジョブを管理します。
99: *終了*	DirXML コマンドラインユーティリティを終了します。

図 A-1 *［ドライバオプション］*

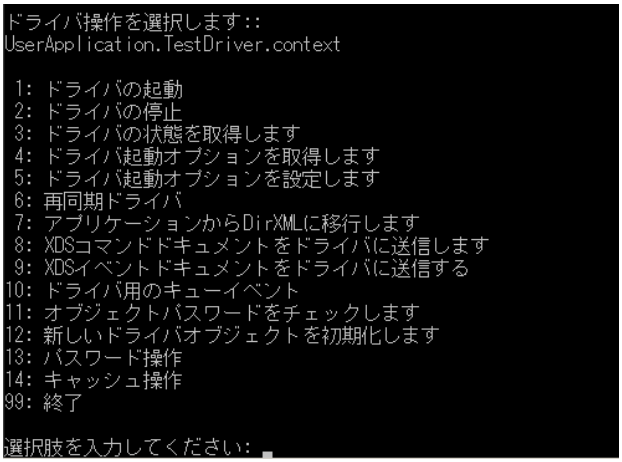


表 A-2 *f⁄ Þðþ⁄ µÃ⁄ °Æ›*

オプション	説明
1: *ドライバの起動*	ドライバを起動します。
2: *ドライバの停止*	ドライバを停止します。
3: *ドライバステータスの取得*	ドライバの状態を一覧 \'95\'5c 示します。 ◆ 0 - ドライバは停止中です ◆ 1 - ドライバを起動しています ◆ 2 - ドライバは実行中です ◆ 3 – ドライバを停止しています
4: *ドライバ起動オプションの取得*	現在のドライバの起動オプションを一覧 \'95\'5c 示します。 ◆ 1 - ［Disabled］ ◆ 2 - ［Manual］ ◆ 3 - ［Auto］
5: *ドライバ起動オプションの設定*	ドライバの起動オプションを変更します。 ◆ 1 - ［Disabled］ ◆ 2 - ［Manual］ ◆ 3 - ［Auto］ ◆ 99 - ［Exit］

オプション	説明
6: *再同期 ドライバ*	ドライバの再同期を強制します。遅延時間の入力を求められます。*再同期の最小時間を指定しますか ?(はい / いいえ)*。 「はい」と入力した場合、再同期を行う日時を指定します。*日付 / 時刻を入力します (形式 0/27/05 3:27 PM)*。 「いいえ」と入力した場合、再同期がすぐに実行されます。
7: *アプリケーションから DirXML に移行*	クエリコマンドを含む XML ドキュメントを処理します : *XDS クエリドキュメントのファイル名を入力します:* Novell nds.dtd (http://developer.novell.com/ndk/doc/dirxml/dirxmlbk/ref/ndsdtd/query.html) を使用して、クエリコマンドが含まれている XML ドキュメントを作成します。 例 : NetWare: sys:\files\query.xml Windows: c:\files\query.xml Linux: /files/query.xml
8: *XDS コマンドドキュメントをドライバに送信*	XDS コマンドドキュメントを処理します : *XDS コマンドドキュメントのファイル名を入力します:* 例 : NetWare: sys:\files\user.xml Windows: c:\files\user.xml Linux: /files/user.xml *応答のファイル名を入力します:* 例 : NetWare: sys:\files\user.log Windows: c:\files\user.log Linux: /files/user.log
9: *XDS イベントドキュメントをドライバに送信*	プロセスおよび XDS イベントドキュメント : *XDS イベントドキュメントのファイル名を入力します:* 例 : NetWare: sys:\files\add.xml Windows: c:\files\add.xml Linux: /files/add.xml

オプション	説明
10: *ドライバ用のキューイベント*	イベントをドライバキューに追加します : *XDS イベントドキュメントのファイル名を入力します:* 例 : NetWare: sys:\files\add.xml Windows: c:\files\add.xml Linux: /files/add.xml
11: *オブジェクトパスワードの確認*	ドライバに関連付けられた接続システム内のオブジェクトのパスワードを検証します。これは、オブジェクトの eDirectory パスワード (ユニバーサルパスワードとともに使用される配布パスワード) に一致します。 *ユーザ名を入力します*:
12: *新しいドライバオブジェクトの初期化*	新しいドライバオブジェクト上のデータを内部的に初期化します。これは、テスト目的のみです。
13: *パスワード操作*	パスワードオプションは 9 種類あります。これらのオプションの詳細については、307 ページの 表 A-3 を参照してください。
14: *キャッシュ操作*	キャッシュ操作は 5 種類あります。これらのオプションの詳細については、309 ページの 表 A-4 を参照してください。
99: *終了*	ドライバオプションを終了します。

図 A-2 *パスワード操作*

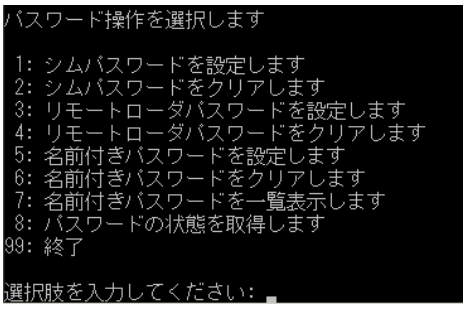


表 A-3 *パスワード操作*

説明	説明
1: *シムパスワードの設定*	アプリケーションのパスワードを設定します。これは、接続システムを認証するために使用しているユーザアカウントのパスワードです。
2: *シムパスワードのクリア*	アプリケーションパスワードをクリアします。

説明	説明
3: *リモートローダパスワードの設定*	リモートローダインスタンスへのアクセスを制御するために、リモートローダのパスワードが使用されます。 リモートローダのパスワードを入力し、パスワードを再度入力して確認します。
4: *リモートローダパスワードのクリア*	リモートローダのパスワードをクリアし、ドライバオブジェクトでリモートローダのパスワードが設定されていない状態にします。
5: *名前付きパスワードの設定*	パスワードまたはその他のセキュリティ情報をドライバに保存できます。詳細については、36 ページのセクション 2.11「名前付きパスワードの使用」を参照してください。 次の 4 つのプロンプトが \'95\'5c 示されます。 ◆ *パスワード名を入力します:* ◆ *パスワードの説明を入力します:* ◆ *パスワードを入力します:* ◆ *パスワードを確認します:*
6: *名前付きパスワードのクリア*	指定した名前付きパスワード、またはドライバオブジェクトに保存されているすべての名前付きパスワードをクリアします : *すべての名前付きパスワードをクリアしますか ?(はい / いいえ)*。 「はい」と入力した場合、すべての名前付きパスワードがクリアされます。「いいえ」と入力した場合、クリアするパスワード名を指定するよう要求されます。
7: *名前付きパスワードの一覧表示*	ドライバオブジェクトに保存されているすべての名前付きパスワードを一覧表示します。パスワード名およびパスワードの説明が一覧 \'95\'5c 示されます。
8: *パスワード状態の取得*	次に対してパスワードが設定されている場合、一覧 \'95\'5c 示します。 ◆ ドライバオブジェクトのパスワード : ◆ アプリケーションのパスワード : ◆ リモートローダのパスワード : dxcmd ユーティリティを使用すると、アプリケーションのパスワードおよびリモートローダのパスワードを設定できます。このユーティリティでは、ドライバオブジェクトのパスワードは設定できません。ユーティリティには、パスワードが設定されているかいないかが表示されます。
99: *終了*	現在のメニューを終了し、ドライバオプションに戻ります。

図 A-3 *キャッシュ操作*

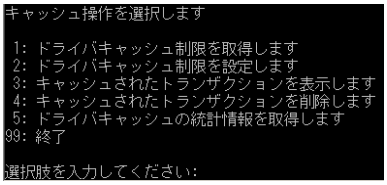


表 A-4 *キャッシュ操作*

説明	説明
1: *ドライバキャッシュ制限の取得*	ドライバに設定されている現在のキャッシュの制限を \'95\'5c 示します。
2: *ドライバキャッシュ制限の設定*	ドライバのキャッシュの制限をキロバイトで設定します。値 0 は無制限です。
3: *キャッシュされたトランザクションの表示*	キャッシュに保存されたイベントを使用してテキストファイルが作成されます。\'95\'5c 示するトランザクションの数を選択できます。 ◆ *オプショントークンを入力します*(デフォルト=0)。 ◆ *返されるトランザクションレコードの最大数を入力します* (デフォルト =1): ◆ *応答のファイル名を入力します:*
4: *キャッシュされたトランザクションの削除*	キャッシュに保存されているトランザクションを削除します。 ◆ *位置トークンを入力します* (デフォルト =0): ◆ *削除する最初のトランザクションのイベント ID 値を入力します (オプション):* ◆ *削除するトランザクションレコード数を入力します (デフォルト =1)*。
99: *終了*	現在のメニューを終了し、ドライバオプションに戻ります。

図 A-4 *ログイベントの操作*

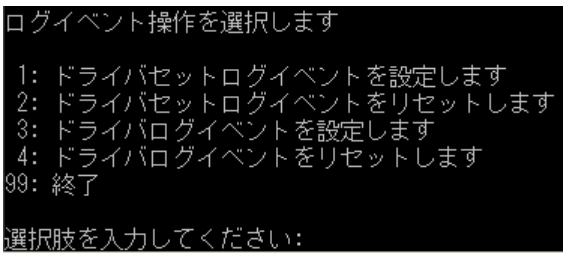


表 A-5 ログイベントの操作

説明	説明
1: *ドライバセットログイベントの設定*	Novell Audit を介してドライバセットイベントをログに記録できるようにします。ログの対象は 49 項目から選択できます。これらのオプションのリストについては、310 ページの 表 A-6 を参照してください。 ログに記録する項目の番号を入力します。項目を選択したら、「99」と入力して選択を受諾します。
2: *ドライバセットログイベントのリセット*	すべてのログイベントのオプションをリセットします。
3: *ドライバログイベントの設定*	Novell Audit を介してドライバイベントをログに記録できるようにします。ログ記録の対象は 49 項目から選択できます。これらのオプションのリストについては、310 ページの 表 A-6 を参照してください。 ログに記録する項目の番号を入力します。項目を選択したら、「99」と入力して選択を受諾します。
4: *ドライバログイベントのリセット*	すべてのログイベントのオプションをリセットします。
99: *終了*	ログイベント操作のメニューを終了します。

表 A-6 ドライバセットおよびドライバのログイベント

オプション
1: ステータスは成功です
2: ステータスは再試行です
3: ステータスは警告です
4: ステータスがエラーです
5: ステータスは致命的です
6: ステータスはその他です
7: 要素の照会
8: 要素の追加
9: 要素の削除
10: 要素の修正
11: 要素の名前変更
12: 要素の移動
13: 追加 - 関連付け要素
14: 削除 - 関連付け要素

オプション
15: 照会 - スキーマ要素
16: チェック - パスワード要素
17: チェック - オブジェクト - パスワード要素
18: 変更 - パスワード要素
19: 要素の同期
20: シムから事前変換された XDS ドキュメント
21: ポスト入力変換 XDS ドキュメント
22: ポスト出力変換 XDS ドキュメント
23: ポストイベント変換 XDS ドキュメント
24: ポスト配置変換 XDS ドキュメント
25: ポスト作成変換 XDS ドキュメント
26: ポストマッピング変換 (インバウンド)XDS ドキュメン
27: ポストマッピング変換 (アウトバウンド)XDS ドキュメン
28: ポストマッチング変換 XDS ドキュメント
29: ポストコマンド変換 XDS ドキュメント
30: ポストフィルタ済み XDS ドキュメント <Publisher>
31: ユーザエージェント XDS ドキュメント
32: ドライバ再同期要求
33: アプリケーションからのドライバ移行
34: ドライバの起動
35: ドライバの停止
36: パスワードの同期
37: パスワード要求
38: エンジンエラー
39: エンジン警告
40: 属性の追加
41: 属性をクリア
42: 値の追加
43: 値の削除
44: 全体をマージ
45: 名前付きの取得パスワード
46: 属性のリセット

オプション
47: 値の追加 - エントリの追加
48: SSO 資格情報の設定
49: SSO 資格情報のクリア
50: SSO パスフレーズの設定
51: ユーザ定義 ID
99: 確認した項目を受け入れます

表 A-7 *ここに表の題名を入力*

オプション	説明
1: *利用可能なジョブ定義の取得*	既存のジョブを選択できます。 *ジョブ番号を入力します:* *コンテインメントでジョブの定義をフィルタしますか?*「はい」または「いいえ」を入力 *応答のファイル名を入力します:* 例 : NetWare: sys:\files\user.log Windows: c:\files\user.log Linux: /files/user.log
2: *特定のジョブオブジェクトの操作*	特定のジョブに対して操作を実行できます。

A.2 コ \'83\'7d ンド ラインモード

コマンドラインモードを使用すると、スクリプトまたはバッチファイルを使用できます。312 ページの 表 A-8 には、使用可能なさまざまなオプションが含まれています。

コ \'83\'7d ンドラインオプションを使用するには、どの項目を使用してまとめるのかを決定します。

例 : dxcmd -user admin.headquarters -host 10.0.0.1 -password n0vell -start test.driverset.headquarters

このコマンド例は、ドライバを起動します。

表 A-8 *コ \'83\'7d ンドラインオプション*

オプション	説明
設定	

オプション	説明
-user < *ユーザ名* >	テストするドライバに対して管理者権限を持つユーザの名前を指定します。
-host < *名前または IP アドレス* >	ドライバがインストールされているサーバの IP アドレスを指定します。
-password < *ユーザのパスワード*>	上記で指定したユーザのパスワードを入力します。
-port < *ポート番号* >	ポート番号は、デフォルトのポートが使用されていない場合に指定します。
-q < *消音モード*>	コ \'83\'7d ンドが実行されているときに少ない情報を \'95\'5c 示します。
-v < *冗長モード*>	コ \'83\'7d ンドが実行されているときに詳しい情報を \'95\'5c 示します。
-s <*stdout*>	dxcmd コマンドの結果を stdout を書き込みます。
-? < *本メッセージの表示* >	ヘルプメニューを \'95\'5c 示します。
-help < *本メッセージを表示* >	ヘルプメニューを \'95\'5c 示します。
［アクション］	
-start < *ドライバ dn*>	ドライバを起動します。
-stop < *ドライバ dn*>	ドライバを停止します。
-getstate < *ドライバ dn*>	実行されているドライバまたは停止したドライバの状態を \'95\'5c 示します。
-getstartoption < *ドライバ dn*>	ドライバの起動オプションを \'95\'5c 示します。
-setstartoption <*driver dn*> <*disabled*|*manual*|*auto*> <*resync*|*noresync*>	サーバが再起動した場合に、ドライバをどのように起動するのかを設定します。ドライバが再起動したときに、オブジェクトが再同期されるかどうかを設定します。
-getcachelimit < *ドライバ dn*>	ドライバに対して設定されたキャッシュの制限を一覧 \'95\'5c 示します。
-setcachelimit < *ドライバ dn*> <*0 または正の整数* >	ドライバのキャッシュの制限を設定します。
-migrateapp < *ドライバ dn*> < *ファイル名* >	クエリコ \'83\'7d ンドが含まれている XML ドキュメントを処理します。 Novell nds.dtd (http://www.novell.com/documentation/idm35/index.html?page=/documentation/idm35/policy_dtd/data/dtdndsoverview.html#dtdndsoverview) を使用して、クエリコマンドが含まれている XML ドキュメントを作成します。
-setshimpassword < *ドライバ dn*> < *パスワード*>	アプリケーションのパスワードを設定します。これは、接続システムを認証するために使用しているユーザアカウントのパスワードです。
-clearshimpassword < *ドライバ dn*> < *パスワード* >	アプリケーションパスワードをクリアします。

オプション	説明
-setremoteloaderpassword < *ドライバ dn*> < *パスワード*>	リモートローダのパスワードを設定します。 リモートローダインスタンスへのアクセスを制御するために、リモートローダのパスワードが使用されます。
<clearremoteloaderpassword < *ドライバ dn*>	リモートローダのパスワードをクリアします。
-sendcommand < *ドライバ dn*> < *入力ファイル名* > < *出力ファイル名* >	XDS コ \'83\'7d ンドドキュメントを処理します。 入力ファイルとして、XDS コ \'83\'7d ンドドキュメントを指定します。 例 : NetWare: sys:\files\user.xml Windows: c:\files\user.xml Linux: /files/user.log 結果を表示するための出力ファイル名を指定します。 例 : NetWare: sys:\files\user.log Windows: c:\files\user.log Linux: /files/user.log
-sendevent < *ドライバ dn*> < *入力ファイル名* >	ドライバキャッシュをバイパスすることで、ドライバの購読者チャネルにドキュメントを送信します。そのドキュメントは、送信時にキャッシュ内にある他のものより先に処理されます。ドライバが稼動していないときには、送信は失敗します。
-queueevent < *ドライバ dn*> < *入力ファイル名* >	ドライバキャッシュ内のドキュメントをキューイングすることで、ドライバの購読者チャネルにドキュメントを送信します。そのドキュメントは、送信時にキャッシュ内にある他のものの後に処理されます。ドライバが稼動していない場合でも、送信は失敗しません。
-setlogevents <*dn*> < *整数 ...*>	ドライバ上の Novell Audit ログイベントを設定します。整数は、ログに記録する項目のオプションです。入力する整数のリストについては、310 ページの 表 A-6 を参照してください。
-clearlogevents <*dn*>	ドライバ上に設定されているすべての Novell Audit ログイベントをクリアします。
-setdriverset < *ドライバセット dn*>	ドライバセットをサーバに関連付けます。
-cleardriverset	ドライバセットの関連付けをサーバからクリアします。
-getversion	インストールされた Identity Manager のバージョンを表示します。

オプション	説明
-initdriver object <*dn*>	新しいドライバオブジェクト上のデータを内部的に初期化します。これは、テスト目的のみです。
-setnamedpassword < *ドライバ dn*> < *名前*> < *パスワード*> *[説明]*	ドライバオブジェクトの名前付きパスワードを設定します。名前付きパスワードの名前、パスワード、および説明を指定します。
-clearnamedpassword < *ドライバ dn*> < *名前*>	指定した名前付きパスワードをクリアします。
-startjob <*job dn*>	指定したジョブを開始します。
-abortjob <*job dn*>	指定したジョブを中止します。
-getjobrunningstate <*job dn*>	指定したジョブの実行状態を返します。
-getjobenabledstate <*job dn*>	指定したジョブの有効状態を返します。
-getjobnextruntime <*job dn*>	指定したジョブの次の実行時刻を返します。
-updatejob <*job dn*>	指定したジョブを更新します。
-clearallnamedpaswords <*driver dn*>	特定のドライバ上のすべての名前付きパスワード設定をクリアします。

コマンドラインが正常に完了した場合、0 が返されます。0 以外が返された場合は、エラーです。たとえば、0 は「成功」、-641 は「無効な操作」を示します。-641 は、eDirectory のエラーコードです。315 ページの 表 A-9 には、個別のコマンドラインオプションの他の値が含まれています。

表 A-9 *コマンドラインオプションの値*

コマンドラインオプション	値
-getstate	0 - 停止
	1 - 起動
	2 - 実行中
	3 - シャットダウン
	11- スキーマの取得
	上記以外のものはすべてエラーです。
-getstartoption	0 – 使用不可
	1 – 手動
	2 – 自動
	上記以外のものはすべてエラーです。
-getcachelimit	0 - 無制限
	上記以外のものはすべてエラーです。

コマンドラインオプション	値
-getjobrunningstate	0 - 停止 1 - 実行中 上記以外のものはすべてエラーです。
-getjobenabledstate	0 – 使用不可 1 - 使用可能 2 - 設定エラー 上記以外のものはすべてエラーです。
-getjobnextruntime	ジョブの次のスケジュール時間が、eDirectory の時間形式 (00:00:00 Jan 1, 1970UTC からの秒数) で返されます。

リモートローダの設定のオプション

B

次の \'95\'5c のオプションを使用すると、リモートローダを設定できます。

表 B-1 *リモートローダのオプション*

オプション	2 次名	パラメータ	説明
address		IP アドレス	オプションのパラメータです。リモートローダが特定のローカル IP アドレスをリッスンするよう指定します。これは、リモートローダをホストするサーバが複数の IP アドレスを持ち、リモートローダが 1 つのアドレスのみをリッスンしなければならない場合に便利です。 次の 3 つのオプションがあります。アドレス = *アドレス番号*、アドレス =’ローカルホスト’、このパラメータを使用しない。 アドレスを使用しない場合、リモートローダはすべてのローカル IP アドレスをリッスンします。 例 : アドレス =137.65.134.83
-class	-cl	Java クラス名	管理する Identity Manager アプリケーションシムの Java クラス名を指定します。 たとえば、Java ドライバに対しては次のいずれかを入力します。 -class com.novell.nds.dirxml.driver.ldap.LDAPDriverShim -cl com.novell.nds.dirxml.driver.ldap.LDAPDriverShim Java では、キーストアを使用して証明書を読み取ります。-class オプションと -module オプションは排他的で、どちらか一方を使用することができます。 Java クラス名のリストを見るには、324 ページの表 B-2 を参照してください。

オプション	2 次名	パラメータ	説明
-commandport	-cp	ポート番号	リモートローダのインスタンスが制御目的で使用する TCP/IP ポートを指定します。リモートローダインスタンスがアプリケーションシムをホストしている場合、コマンドポートは、別のリモートローダインスタンスが、シムをホストしているインスタンスと通信するポートになります。リモートローダインスタンスが、アプリケーションシムをホストしているインスタンスにコマンドを送信する場合、コマンドポートは管理インスタンスがリッスンしているポートになります。コ \'83\'7d ンドポートが指定されていない場合のデフォルトポートは 8000 です。複数の接続ポートとコ \'83\'7d ンドポートを指定することで、異なるドライバインスタンスをホストしている同じサーバ上でリモートローダの複数のインスタンスを実行できます。 例 : -commandport 8001 -cp 8001
-config	なし	ファイル名	環境設定ファイルを指定します。環境設定ファイルには、config 以外のあらゆるコマンドラインオプションを含めることができます。コマンドラインで指定したオプションは、環境設定ファイル内で指定されたオプションよりも優先されます。 例 : -config config.txt
-connection	-conn	接続設定文字列	Identity Manager リモートインタフェースシムを実行しているメタディレクトリサーバに接続するための接続パラメータを指定します。リモートローダのデフォルトの接続方法は、SSL を使用した TCP/IP です。この接続におけるデフォルトの TCP/IP ポートは 8090 になります。同じサーバで、リモートローダの複数のインスタンスを実行できます。リモートローダの各インスタンスは別々の Identity Manager アプリケーションシムインスタンスをホストします。リモートローダの各インスタンスに別々の接続ポートとコ \'83\'7d ンドポートを指定することによって、リモートローダーの複数のインスタンスを区別します。 例 : -connection "port=8091 rootfile=server1.pem" -conn "port=8091 rootfile=server1.pem"

オプション	2 次名	パラメータ	説明
-description	-desc	短い説明	トレースウィンドウのタイトルと Novell® Audit のログに使用される短い説明の文字列を指定します。 例 : -description SAP -desc SAP 環境設定ファイルには、リモートローダコンソールによって長い形式が配置されます。長い形式 (たとえば -description) または短い形式 (たとえば -desc) のいずれかを使用できます。
-help	-?	なし	ヘルプを \'95\'5c 示します。 例 : -help -?
-java	-j	なし	Java シムインスタンスに設定されるパスワードを指定します。このオプションは、setpasswords オプションとともに使用した場合にのみ有効です。-class を -setpasswords とともに指定した場合、このオプションは不要です。
-javadebugport	-jdp	ポート番号	指定されたポートで、リモートローダインスタンスにより Java デバッグが有効になるように指定します。これは Identity Manager アプリケーションシムの開発者向けです。 例 : -javadebugport 8080 -jdp 8080
keystore			条件付きパラメータです。.jar ファイルに含まれる Identity Manager アプリケーションシムにのみ使用します。 リモートインタフェースシムによって使用される証明書の発行者のルート認証局証明書を含む Java キーストアのファイル名を指定します。通常、これはリモートインタフェースシムをホストしている eDirectory™ ツリーの認証局です。 SSL を実行していて、リモートローダが Java ドライバと通信する必要がある場合、次の key-value ペアを入力します。 keystore=' *keystorename*' storepass=' *password*'

オプション	2 次名	パラメータ	説明
-module	-m	モジュール名	ホストされる Identity Manager アプリケーションシムを含むモジュールを指定します。 たとえば、ネイティブドライバに対しては次のいずれかを入力します。 -module "c:\Novell\RemoteLoader\Exchange5Shim.dll" -m "c:\Novell\RemoteLoader\Exchange5Shim.dll" または -module "usr/lib/dirxml/NISDriverShim.so" -m "usr/lib/dirxml/NISDriverShim.so" -module オプションでは、ルートファイル証明書が使用されます。-module オプションと -module オプションは排他的で、どちらか一方を使用することができます。
-password	-p	パスワード	コマンド認証のパスワードを指定します。このパスワードは、コマンドの発行先のローダインスタンスの setpasswords で指定した最初のパスワードと同じパスワードにする必要があります。コ \'83\'7d ンドオプション (unload や tracechange など) を指定し、password オプションを指定しないと、コ \'83\'7d ンドの対象となるローダのパスワードを入力するよう要求するメッセージが \'95\'5c 示されます。 例 : -password novell4 -p novell4
port		10 進数のポート番号	必須パラメータです。リモートローダがリモートインタフェースシムからの接続をリッスンする TCP/IP ポートを指定します。 例 : port=8090
rootfile			条件付きパラメータです。SSL を実行していて、リモートローダがネイティブドライバと通信する必要がある場合、次を入力します。 rootfile=' *trusted certname*'

オプション	2 次名	パラメータ	説明
-service	-serv	なし、または install/uninstall	インスタンスをサービスとしてインストールするには、アプリケーションシムをホストするために必要なその他の引数とともに引数 install を使用します。たとえば、使用する引数には -module を含める必要がありますが、どの引数にも -connection、-commandport などを含めることができます。 このオプションを指定すると、Wind32 サービスがインストールされますが、サービスは起動されません。 サービスとして実行されているインスタンスをアンインストールするには、アプリケーションシムをホストするために必要なその他の引数とともに引数 uninstall を使用します。 このオプションの引数なしのバージョンは、Win32 サービスとして実行されるインスタンスへのコマンドライン内でのみ使用します。これはインスタンスをサービスとしてインストールする際に自動的に設定されます。 例 : -service install -serv uninstall このオプションは rdxml または Java リモートローダでは使用できません。
-setpasswords	-sp	パスワード パスワード	リモートローダインスタンスのパスワード、およびリモートローダが通信するリモートインタフェースシムの Identity Manager ドライバオブジェクトのパスワードを指定します。引数の最初のパスワードは、リモートローダのパスワードです。オプション引数の 2 番目のパスワードは、メタディレクトリサーバのリモートインタフェースシムに関連付けられた Identity Manage ドライバオブジェクトのパスワードです。どちらのパスワードも指定しないか、または両方のパスワードを指定する必要があります。パスワードを指定しない場合、リモートローダよりパスワードを要求するメッセージが表示されます。これは環境設定オプションです。このオプションを使用すると、指定したパスワードがリモートローダのインスタンスに設定されます。ただし、このオプションを指定しても、Identity Manager アプリケーションシムはロードされず、ローダの別のインスタンスとも通信しません。 例 : -setpasswords novell4 staccato3 -sp novell4 staccato3

オプション	2 次名	パラメータ	説明
-storepass		storepass	.jar ファイルに含まれる Identity Manager アプリケーションシムにのみ使用されます。keystore パラメータで指定した Java キーストアのパスワードを指定します。 例 : storepass=mypassword このオプションは Java リモートローダにのみ適用されます。
-trace	-t	整数	トレースレベルを指定します。これはアプリケーションシムをホストする場合にのみ使用されます。トレースレベルは metadirectory サーバで使用されているレベルと同じです。 例 : -trace 3 -t 3
-tracechange	-tc	整数	アプリケーションシムをホストしているリモートローダのインスタンスに、そのトレースレベルを変更するように命令します。トレースレベルは metadirectory サーバで使用されているレベルと同じです。 例 : -tracechange 1 -tc 1
-tracefile	-tf	ファイル名	トレースメッセージを書き込むファイルを指定します。トレースメッセージは、トレースレベルがゼロよりも大きい場合にファイルに書き込まれます。トレースメッセージは、トレースウィンドウが開いていなくてもファイルに書き込まれます。 例 : -tracefile c:\temp\trace.txt -tf c:\temp\trace.txt
-tracefilechange	-tfc	なし、またはファイル名	アプリケーションシムをホストしているリモートローダのインスタンスに対し、トレースファイルを使用して起動するように命令するか、すでに使用しているファイルを閉じて新しいファイルを使用するように命令します。このオプションを引数なしで使用すると、ホストインスタンスは使用中のすべてのトレースファイルを閉じます。 例 : -tracefilechange c:\temp\newtrace.txt tfc c:\temp\newtrace.txt

オプション	2 次名	パラメータ	説明
-tracefilemax	-tfm	サイズ	トレースファイルがディスク上で使用できる最大サイズを指定します。このオプションを指定すると、tracefile オプションを使用して指定した名前の付いたトレースファイルと、最大 9 個の追加ロールオーバファイルが生成されます。ロールオーバファイルには、メインのトレースファイル名と「*_n*」に基づいた名前が付けられます。「n」は 1 ～ 9 の値になります。 サイズのパラメータはバイト数です。K (キロバイト)、M (メガバイト)、または G (ギガバイト) のサフィックスを使用してサイズを指定します。 リモートローダの起動時にトレースファイルのデータが指定した最大サイズよりも大きい場合、10 ファイルすべてのロールオーバーが完了するまで、トレースファイルのデータは指定した最大値よりも大きいままとなります。 例 : -tracefilemax 1000M -tfm 1000M この例では、トレースファイルは 1GB までです。
-unload	-u	なし	リモートローダのインスタンスをアンロードします。リモートローダが Win32 サービスとして実行されている場合、このコ \'83\'7d ンドはサービスを停止します。 例 : -unload -u
-window	-w	オン / オフ	リモートローダのインスタンスでトレースウィンドウのオン / オフを切り替えます 例 : -window on -w off このオプションは Windows プラットフォームのみで使用可能です。Java リモートローダでは使用できません。

オプション	2 次名	パラメータ	説明
-wizard	-wiz	なし	環境設定ウィザードを起動します。このウィザードは、コマンドラインパラメータなしで dirxml_remote.exe を実行しても起動します。このオプションは、設定ファイルも指定されている場合に便利です。この場合、ウィザードは設定ファイルの値を使用して起動するので、このウィザードを使用して、設定ファイルを直接編集せずに設定を変更できます。 例 : -wizard -wiz このオプションは Windows プラットフォームのみで使用可能です。Java リモートローダでは使用できません。

表 B-2 *Java クラス名*

Java クラス名	ドライバ
com.novell.nds.dirxml.driver.avaya.PBXDriverShim	Avaya PBX Driver
com.novell.nds.dirxml.driver.delimitedtext.DelimitedTextDriver	Delimited Text Driver
com.novell.nds.dirxml.driver.nds.DriverShimImpl	eDirectory Driver
com.novell.nds.dirxml.driver.entitlement.EntitlementServiceDriver	Entitlement Services Driver
com.novell.gw.dirxml.driver.gw.GWdriverShim	GroupWise Driver
com.novell.nds.dirxml.jdbc.JDBCDriverShim	JDBC Driver
com.novell.nds.dirxml.driver.ldap.LDAPDriverShim	LDAP Driver
com.novell.nds.dirxml.driver.loopback.LoopbackDriverShim	Loopback Driver
com.novell.nds.dirxml.driver.manualtask.driver.ManualTaskDriver	Manual Task Driver
com.novell.nds.dirxml.driver.nisdriver.NISDriverShim	NIS Driver
com.novell.nds.dirxml.driver.notes.NotesDriverShim	Notes Driver
com.novell.nds.dirxml.driver.psoftshim.PSOFTDriverShim	PeopleSoft Driver
com.novell.nds.dirxml.driver.SAPShim.SAPDriverShim	SAP HR Driver
com.novell.nds.dirxml.driver.sapusershim.SAPDriverShim	SAP User Management Driver
com.novell.nds.dirxml.driver.sifagent.SIFShim	SIF Driver
com.novell.nds.dirxml.driver.soap.SOAPDriver	Soap Driver
com.novell.idm.driver.ComposerDriverShim	User Appliction
be.opns.dirxml.driver.ars.arsremedydrivershim.ARSDriverShim	Driver for Remedy ARS
com.novell.nds.dirxml.driver.workorder.WorkOrderDriverShim	ワークオーダー

ドライバ設定ファイルを編集する

C

このセクションにある情報を使用するには、XML に精通している必要があります。このセクションの情報を使用すると、作成したドライバにカスタムプロンプトを追加できます。

C.1 ドライバ設定ファイルの変数

iManager プラグインの場合、ドライバ設定ファイルに対して複数のノードタイプが定義されています。以下は、Identity Manager エンジンでサポートされているアクションの一覧です。

- 単一のドライバ設定ファイル全体で繰り返し使用される値の入力が一度求められます。
- ドライバのインポートウィザードの途中で、複数のドライバ設定ファイルで使用される値の入力が一度求められます。
- ユーザが、値のドロップダウンリストから値を選択できます。
- 含まれている XSL スタイルシートに従い、ドライバ設定ファイルがグローバルに変更されます。
- ドライバとその環境に関する情報にアクセスするために宣言しなくても、参照できる組み込み変数。たとえば、ツリー名、ドライバセット名、ドライバセット DN、サーバ名、サーバ DN、ドライバ名、およびドライバ DN。
- プロンプトを階層化する機能。ユーザに複数のセットの質問を尋ね、2 つ目以降のセットをユーザの最初の質問セットに対する応答でコントロールすることができます。詳細については、329 ページのセクション C.2「ドライバ設定ファイルの柔軟なプロンプト」を参照してください。

主な新しいノードタイプは次のものです。

- **variable-decl:** インポート中に入力を求められ、ドライバ設定ファイルに配置されるドライバ設定変数を定義できます。複数の variable-decl ブロックを、プロンプトの階層セットを定義するために使用できます。詳細については、329 ページのセクション C.2「ドライバ設定ファイルの柔軟なプロンプト」を参照してください。
- **variable-ref:** ドライバ設定ファイル内の variable-decl で定義された変数を参照するために使用されます。
- **xsl-modify:** すべての変数およびプロンプトが解決された後で、ドライバ設定ファイルをグローバルに変更するために使用されます。このノードのコンテンツは、パッチ済みのドライバ設定ファイルに適用される XSL スタイルシートとして抽出および使用されます。

ドライバ設定ファイルの XML 拡張子を表示するには、DriverConfigXMLExtension.txt (../samples/DriverConfigXMLExtension.txt) を参照してください。

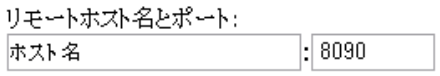
また、以下の点に注意してください。

- 326 ページのセクション C.1.1「一般的な注意」
- 328 ページのセクション C.1.2「ドライバメモのインポート」

C.1.1 一般的な注意

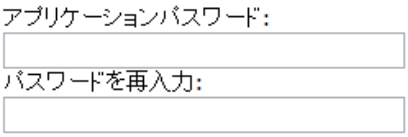
- variable-decls には、text-var は含めることができますが、node-var は含められません。解決される順番が考慮に入れられる場合は、variable-refs を含めることができます。
- variable-decl にオプションの prompt 属性およびオプションの prompt-type 属性が含まれていて、オプションの browse=“yes” 属性設定が含まれていない場合、prompt-type は次のように処理されます。
  - prompt-type"ipa" の結果は、2 つの編集フィールドに格納されます。例については、図 C-1 を参照してください。最初の部分にユーザが指定する値にはコロン (:) が追加され、値の 2 番目の部分にユーザが指定する値は変数でレンダリングされます。

図 C-1 *2 つの編集フィールド*



  - prompt-type" パスワード " の結果は、2 つのパスワード編集フィールドに格納されます。例については、図 C-2 を参照してください。最初のプロンプトは実際のパスワード用で、2 番目のプロンプトは最初のフィールドに指定したパスワードが正しいことを検証するために使用されます。変数参照でレンダリングされた値はパスワードです。

図 C-2 *2 つのパスワードフィールド*



  - フィールド内の prompt-type" 非表示 " の結果は、表示されませんが、次の画面に進む前に以前の条件が満たされていることはチェックされます。
  - その他の prompt-type は無視されます。
- variable-decl に prompt 属性のほかにオプションの description 属性が含まれている場合、description がプロンプトとともに UI 内に表示されます。description 属性の目的は、単純なプロンプトとともに求められている内容を完全に記述することにあります。

  例 :

```
<text-var                var-name="eProv.Company"prompt="Company
name:" description="Please enter the name of your company. This
must be the same name as you entered during the initial
installation."          browse="no">      Novell      </text-var>
```

  prompt と description の違いを説明します。

variable-decl にオプションの description 属性とオプションの highlight 属性が含まれている場合、highlight 属性は次のように処理されます。

- 長さが 2 文字以外の highlight は、無視されます。
- highlight の長さが 2 文字の場合、最初の文字のすべてのオカレンスの前に強調表示をオンにする HTML タグがあり、2 番目の文字のすべてのオカレンスの後に強調表示をオフにする HTML タグがきます。

  例 :

  ```
  <text-var                              var-name="foo"
  prompt="Foo:"                          description="Please enter
  some foo.  Format:  [foo looks like this]">Bar        </text-
  var>
  ```

  description が表示されると、[foo looks like this] が強調表示されます。

- variable-decl に browse=“yes”属性が含まれている場合、DN を提供し、ドライバ設定ファイルに適用されるときに、デフォルトでスラッシュ (/) 形式でフォーマットされると想定されます。

  これは、一般的にドライバライタにはより有用であると想定されており、dn-format=“dot”属性をそれを参照する variable-ref ノードに追加することで、参照ごとに上書きすることができます。

- variable-ref が prompt-type="ipa" 属性が設定された text-var に対するものである場合、part="..." 属性を variable-ref に含めることができます。サポートされている部分は、"ipa" と "port" です。part="ipa" が指定されている場合、変数値の IP アドレス部分のみが返されます。part="port" が指定されている場合、変数値のポート部分のみが返されます。その他の設定は無視され、変数の値全体が返されます。
- variable-declにbrowse="yes"が指定されていないvariable-refのdn-fromatでは、変数がDNを提供するかのように扱われます。DN は指定した dn-format でレンダリングされます。
- dn-format属性でサポートされている値は、"ドット"と"スラッシュ"です。その他の値は " スラッシュ " として扱われ、エラーは生成されません。
- 定義済みの組み込み変数は以下のとおりです。
  - System.TreeName
  - System.DSetDN
  - System.DSetName
  - System.DriverDN
  - System.DriverName
  - System.ServerDN
  - System.ServerName
- 組み込み変数は上書きできます。組み込み変数名のいずれかの名前が付いた変数に variable-decl を含める場合、その定義により同じ名前の組み込み変数が上書きされます。

  これは、すべての変数宣言が処理 (プロンプト、...) された後で実装されます。コードによる値の適用が開始される前に、変数が確認され別の方法で定義されていないすべての組み込み変数が定義されます。

- DN を提供する組み込み変数には、variable-ref に dn-format 属性を含め、DN がレンダリングされる形式を制御できます。デフォルトでは、これらはスラッシュ形式でレンダリングされます。
- node-var と text-var は、同じものとして名前を付けることはできません。これらは同じネームスペースを使用します。
- variable-ref が node-var を参照し、attr-name が含まれる場合、node-var の XSL 文字列値が variable-ref の親ノードの名前付き属性に保存されます。この方法で使用される node-var には、node-name 属性の "#text" を設定できます。これにより、node-var に attr-name 属性を設定する必要がなくなります。

  ノード名 "#text" の node-var は、この方法でのみ参照できます。その他の参照では、ドライバ設定ファイルがインポートされたときにエラーが生じることがあります。
- ユーザがプロンプトに応答し、XML が実際にインポートされる前のパッチ時には、パッチは、以下の順序で行われます。

  a. text-var variable-refs が処理されます。

  b. node-var variable-refs が処理されます。

  c. xsl-modify コマンドが処理されます。

  d. ds-object コマンドが処理されます。

  - パッチは variable-decl で実行されるため、node-var コマンドがパッチされるときには、それらに含まれるすべての text-var コマンドが解決されています。
  - node-var コマンドには、node-var variable-ref を含めることができません。

C.1.2 ドライバメモのインポート

- 選択したドライバ設定ファイルが処理される順序は定義できないので、順序を想定することはできません。
- variable-decl コマンドの場合
  - 選択したドライバからのコマンドは、ドライバからドライバに渡されます。
  - 最初のドライバが優先されます。
    - 変数 foo を定義する最初に遭遇するドライバの変数 foo が、残りすべてのドライバ設定ファイルに使用されます。これらのドライバ間の調整は注意して行ってください。
    - 複数のドライバ設定ファイルで使用される変数 foo は、それを宣言する最初のドライバ設定ファイルで一度だけプロンプトされます。
- 組み込み変数は、ドライバ間に伝達されません。これには、組み込み変数を上書きするために定義するすべての変数が含まれます。各ドライバの組み込み変数は、個別に処理されます。
- その他のプロンプトは、各ドライバ設定ファイルのインポート順の最初に変更なしで処理されます。
- 柔軟なプロンプトでサポートされているプロンプトレイヤの詳細については、329 ページのセクション C.2「ドライバ設定ファイルの柔軟なプロンプト」を参照してください。

C.2 ドライバ設定ファイルの柔軟なプロンプト

variable-decl ブロックは、ユーザの入力に基づき、個別にプロンプトされるようにマークできます。

```
DTD changes:-----------* <!ENTITY % CompareMode "equals | not-equals">
<!--******************************************************** -->  <!--
The variable-decl element contains definitions of variables   -->  <!-
- whose values can be prompted for and referred to throughout  -->  <!-
- the pre-configured driver file.                              -->  <!-
- ******************************************************** -->
<!ELEMENT variable-decl(node-var*,text-var*)>*<!ATTLIST variable-decl*
<!-- The following are used in the support of flexible -->*<!--
prompting.                                              -->*use-when-var
CDATA #IMPLIED*use-when-valueCDATA #IMPLIED*use-when-mode
(%CompareMode) "equals">* Added for flexible prompting.
```

セマンティック

1. use-when-var 属性が設定されていないすべての variable-decl ブロックは、プロンプトセットに追加されます。
2. 変数が定義され、変数値が条件を満たしている、use-when-var 属性が設定されているすべての variable-decl ブロックは、プロンプトセットに追加されます。

   変数の分析には、以前のインポートから渡された組み込み変数と変数が含まれます。
3. ユーザはプロンプトされます。
4. プロンプトセットが空になり、処理するプロンプトがなくなるまで、またはすべての variable-decl ブロックが処理されるまでステップ 2 と 3 が繰り返されます。
5. インポートはこれまでどおり進められます。

注 : use-when-var 変数の比較では、大文字と小文字が区別されます。

例 1

```
     <variable-decl use-when-var="varCheck" use-when-value="Fu" use-
when-mode="equals"><text-var prompt="When Fu?" var-name="fuVar"/></
variable-decl><variable-decl use-when-var="varCheck" use-when-
value="Fu" use-when-mode="not-equals"><text-var prompt="When not Fu?"
var-name="fuVar"/></variable-decl><variable-decl><text-var
prompt="Which other <variable-decl>?" var-name="varCheck"><dropdown>
<value>Fu</value>       <value>Bar</value></dropdown> </text-var></
variable-decl>
```

この例では、ユーザにはドロップダウンリスト付きのプロンプトが表示されます。ドロップダウンの description は、“Which other <variable-decl>?”です。リスト内にあるオプションは、［Fu］と［Bar］です。

ドロップダウンから［Fu］を選択して、［次へ］をクリックすると、ボックス付きのプロンプトが再度表示されます。そのボックスの description は、“When Fu?”です。

ドロップダウンリストから何か他のオプションを選択し、［次へ］をクリックすると、別のボックス付きのプロンプトが表示されます。そのボックスの description は、“When not Fu?”です。

例 2

```
<variable-decl use-when-var="varCheck" use-when-value="Fu"><text-var
prompt="When Fu?" var-name="fuBarVar"/></variable-decl><variable-decl
use-when-var="varCheck" use-when-value="Bar"><text-var prompt="When
when Bar?" var-name="fuBarVar"/></variable-decl><variable-decl><text-
var prompt="Which other <variable-decl>?" var-name="varCheck"/></
variable-decl>
```

この例では、ユーザにボックスが表示されます。そのボックスの description は、“Which other <variable-decl>?”です。ボックス内で "Fu" を指定し、［次へ］をクリックすると、別のボックスが表示されます。2 番目のボックスの description は、“When Fu?" です。

ボックス内で "Bar" を指定し、［次へ］をクリックすると、別のボックスが表示されます。description は、“When Bar?”です。この 2 つ以外のものを指定すると、プロンプトは表示されず、変数 fuBarVar は定義されません。

C.3 非公式の Identity Manager 3.5 ドライバ設定 DTD

非公式の Identity Manager 3.5 ドライバ設定 DTD を確認するには、PCDrivers.txt (../samples/PCDrivers.txt) にアクセスします。DTD は検証用には使用できません。これは有効な XML DTD ではありません。これは、ドライバ設定ファイル内の有効な構成内容をドキュメント化するためのメカニズムです。

手動タスクサービスドライバ : 置換データ

D

置換データは、電子メールメッセージ、Web ページ、および XDS ドキュメントを構成するためのテンプレートとして使用される XML ドキュメントで使用されます。実際の置換は、出力ドキュメントの \'8d\'5c 成の一部として置換を実行する XSLT スタイルシートを持つ、テンプレートドキュメントを処理することにより実行されます。

置換データは、加入者チャネルおよび発行者チャネル上の異なるメカニズムを介して、手動タスクサービスドライバに提供されます。

加入者チャネル

- 置換データは、<mail> 要素の一部として提供されます。
- 提供される置換データの一部は URL データのことがあります。URL データが提供された場合、自動データ項目によって、処理、完了、および置換が実行されます (337 ページの付録 E「手動タスクサービスドライバ : 自動置換データ項目」を参照)。
- 関連付けの値が\'8d\'5c成される必要がある(すなわち<mail>要素がsrc-dn属性を持つ)ことが <mail> 要素によって指定された場合、“association” という名前の自動データ項目が置換データに追加されます。

発行者チャネル

- 置換データは、HTTP URL データと HTTP POST データで提供されます。
- 自動 URL 置換データ項目がテンプレート処理で使用される前に、置換データに追加されます。

XML ドキュメントとしてテンプレート処理されている間は、置換データが存在します。置換データのドキュメントは、replacement-data という名前のパラメータとして、テンプレートを処理するスタイルシートに渡されます。テンプレートが使用されていない場合、スタイルシートによって XML ドキュメントが直接処理されます。

D.1 データのセキュリティ

データ項目は、購読者チャネルによって送信された電子メールに含まれている URL を経由して、購読者チャネルから発行者チャネルに渡されます。URL 内の特定のデータ項目を変更すると、セキュリティ上の問題が生じます。たとえば、URL の加入者チャネルによって提供された URL の responder-dn 値が、発行者チャネルの Web サーバに送信された URL のその他のユーザの DN によって置換された場合、承認されていないユーザが eDirectory 内のデータを変更できる場合があります。

送信された URL 内のデータが、元々購読者チャネルによって提供されたデータと同じであるようにするために、保護されたデータが提供されます。保護されたデータとは、セキュリティ上の理由のため変更できないデータです。このデータは設定によって異なりますが、responder-dn データ項目、および値が変更される eDirectory オブジェクトに対応するデータ項目が常に含まれています。

データ項目は、元の値を暗号化し、暗号化された値を URL クエリ文字列に配置することにより保護されています。発行者の Web サーバが暗号化された値を受信すると、発行者は値の暗号化を解除し、HTTP GET または POST 要求によって提供された暗号化されていないデータ項目との比較に使用します。

データ項目のインスタンスが暗号化されたデータに表示された場合、暗号化されてないデータ項目の値は暗号化されたデータ項目の値の 1 つと一致する必要があります。暗号化されてないデータ項目の値が、暗号化されたデータ項目の値の 1 つに一致しない場合、HTTP 要求は発行者チャネルの Web サーバによって拒否されます。

また、保護されたデータが含まれていないすべての HTTP POST 要求は拒否されます。

例

HTTP POST 要求では、発行者チャネルの Web サーバは、responder-dn という名前の暗号化されてない POST データを使用して、POST データによって提供されたパスワードを確認します。これは、ユーザの eDirectory オブジェクトに対して応答ユーザを認証するために行われます。

加入者チャネルの <url-query> 要素のコンテンツで、次のような 2 つのデータ項目が指定されているとします。

```
<item name="responder-dn" protect="yes">\PERIN-TAO\novell\phb</item>
<item name="responder-dn" protect="yes">\PERIN-TAO\novell\carol</item>
```

加入者チャネルによって生成された URL には、保護されたデータの両方の responder-dn 値が含まれています。

悪意のあるユーザが、生成されて、電子メールメッセージで送信された URL を取得したとします。悪意のあるユーザは、URL を使用して、eDirectory オブジェクトのデータをユーザが変更することができる HTML 形式を取得します。

Web サーバに送信された HTTP POST 要求で、悪意のあるユーザは暗号化されてない responder-dn 値として eDirectory DN (responder-dn=\PERIN-TAO\novell\wally) を使用します。また、悪意のあるユーザは、Web サーバが実行する認証が成功するように、POST データの独自のパスワードを送信します。

しかし、発行者チャネルの Web サーバが HTTP POST データを受信すると、暗号化された保護データ内での“\PERIN-TAO\novell\wally”の検索が失敗し、POST 要求が拒否されます。

D.2 XML 要素

置換データドキュメントを構成する要素について、次に説明します。XML 属性が要素に対して説明されていない場合、使用できません。

D.2.1 <replacement-data>

<replacement-data> 要素は次の場所に \'95\'5c 示できます。

1. 加入者チャネルの <mail> 要素の下の <message> 要素の子として。

手動タスクサービスドライバでは、入力された <replacement-data> 要素がスタンドアロンの <replacement-data> 要素に加工され、テンプレート処理に使用されます。次の処理が発生します。

a. 囲んでいる <mail> 要素に対して関連付けの値が作成された場合、<item name=“association”> 要素が置換データに追加されます。作成された要素の値は、Identity Manager に返された関連付けの値です。

b. <replacement-data> 要素には、<url-data> 要素の子があります。また、構成された URL データが含まれているいくつかの <item> 要素によって <url-data> 要素が置換されます。<url-data> および <url-query> を参照してください。

2. 加入者チャネルまたは発行者チャネルのいずれかで、スタイルシートを使用してドキュメントを \'8d\'5c 成するときに使用される、置換データのドキュメントのスタンドアロンのトップレベルの要素として。

D.2.2 <item>

<item> 要素は、<replacement-data> 要素、<url-data> 要素、または <url-query> 要素の子になることができます。<item> 要素のコンテンツは、テンプレートでの置換トークンの置換で使用されるテキストです。<item> 要素は常に名前属性を使用して名前が付けられます。

<item> 属性

名前 : 名前属性の値によって、置換トークンによってこのデータ項目が参照される名前が指定されます。たとえば、名前属性の値が manager の場合、置換トークン $manager$ は <item name=“manager”> 要素に含まれている値で置換されます。名前属性は必 \'90\'7b です。

protect: <url-query> 要素の子である <item> 要素では、URL クエリ文字列の保護されたデータセクションに項目が追加されるかどうかが保護属性によって指定されます (<url-query> を参照)。保護属性がある場合、「yes」の値を持っている必要があります。

事前定義された <item> 名

特定の <item> 要素には、加入者チャネル、発行者チャネル、または両方のチャネルのいずれかに対して事前定義された意味があります。

template: 発行者チャネルは、HTTP GET 要求に対するレスポンスを生成するときに使用する際に、テンプレート項目の値をテンプレートドキュメントの名前として扱います。

<item name=“template”> が購読者チャネルで <url-query> 要素の子として表示されると、HTTP GET 要求に応答するときに使用されるテンプレートドキュメントの名前を、発行者チャネルの Web サーバに指定するために、値が URL クエリデータに配置されます。

responder-dn: 発行者チャネルでは、eDirectory オブジェクトの DN として HTTP POST データの responder-dn 項目の値が使用されます。これに対して、HTTP POST データで提供されたパスワードが検証されます。

Web サーバでは、responder-dn 値およびパスワード値が含まれていない HTTP POST 要求が拒否されます。また、HTTP POST データに protected-data 項目が含まれていない場合、要求は拒否されます。

購読者チャネルは、<url-query> 要素の下に 1 つ以上の <item name=“responder-dn” protect=“yes” > 要素を提供します。responder-dn 項目はユーザ認証に使用されるため、項目は保護されている必要があります。

password: HTTP POST データを経由して、発行者チャネルの Web サーバに提供されます。この項目のコンテンツは、POST データの responder-dn 項目によって指定された eDirectory オブジェクトに対して検証されるパスワードです。通常パスワード項目は、HTTP POST 要求を生成するために使用される、HTML 形式で入力されます。

例 :

```
<INPUT TYPE= "password" NAME="password" SIZE="20" MAXLENGTH="40"/>
```

response-template: HTTP POST データを経由して、Web サーバに提供されます。POST への応答として使用される Web ページの生成に使用されます。通常 response-template 項目は、HTTP POST 要求を生成するために使用される、HTML 形式の非 \'95\'5c 示の INPUT 要素を使用して指定されます。

例 :

```
<INPUT TYPE="hidden" NAME="response-template" VALUE="post_form.xml"/>
```

response-stylesheet: HTTP POST データを経由して、Web サーバに提供されます。POST への応答として使用される Web ページの生成に使用されます。通常 response-stylesheet 項目は、HTTP POST 要求を生成するために使用される、HTML 形式の非 \'95\'5c 示の INPUT 要素を使用して指定されます。

例 :

```
<INPUT TYPE="hidden" NAME="response-stylesheet"
VALUE="process_template.xsl"/>
```

auth-template: HTTP POST データを経由して、Web サーバに提供されます。ユーザの認証が失敗した場合、POST への応答として使用される Web ページの生成に使用されます。通常 auth-template 項目は、HTTP POST 要求を生成するために使用される、HTML 形式の非 \'95\'5c 示の INPUT 要素を使用して指定されます。

例 :

```
<INPUT TYPE="hidden" NAME="auth-template" VALUE="auth_response.xml"/>
```

auth-stylesheet: HTTP POST データを経由して、Web サーバに提供されます。ユーザの認証が失敗した場合、POST への応答として使用される Web ページの生成に使用されます。通常 auth-template 項目は、HTTP POST 要求を生成するために使用される、HTML 形式の非 \'95\'5c 示の INPUT 要素を使用して指定されます。

例 :

```
<INPUT TYPE="hidden" NAME="auth-stylesheet"
VALUE="process_template.xsl"/>
```

protected-data: protected-data 項目には、購読者チャネルによって構成された暗号化データが含まれています。加入者チャネルでは、保護されたデータ項目は自動的に提供される項目です。

発行者チャネルでは、protected-data 項目は HTTP GET 要求の URL クエリ文字列から取得されます。また、HTTP POST 要求の POST データからも取得されます。

通常保護されたデータ項目は、HTTP GET 要求から Web ページに渡されます。この Web ページは、HTTP GET へのレスポンスを \'8d\'5c 成するために使用されるテンプレート内の置換トークンを経由して HTTP POST を生成するために使用されます。

例 :

```
<INPUT TYPE="hidden" NAME="protected-data" VALUE="$protected-data$"/>
```

D.2.3 <url-data>

<url-data> 要素は、購読者チャネルの <message> 要素の下にある <replacement-data> 要素の子です。この要素には、URL を構成するために使用される <item> 要素、および電子メールメッセージの作成で使用されるテンプレートに入力される関連データ項目が含まれています。また、<url-query> 要素も含まれています。

手動タスクサービスドライバの目的のために、URL は次の 5 個の部分から \'8d\'5c 成されます。

1. http、https、または ftp などのスキーム。
2. www.novell.com または 192.168.0.1 などのホスト。
3. ポート番号。コロンの後に 10 進数の整数を続けます。たとえば、:80 または :8180 です。
4. ファイルまたはリソースの識別子です。通常はファイル名であり、パス情報を含めることができます。たとえば、stylesheets/process_template.xsl です。
5. クエリ文字列。これは、& 文字で区切られた name-value ペアのコレクションです。たとえば、template=form_template.xml&protected-data=AabABJKEL= です。

事前定義された <item> Names Under <url-data>

次のいずれかでない場合、<url-data> 要素の下の <item> 要素は無視されます。すべてがオプション。

file: URL のファイル部分を指定します。発行者チャネルの Web サーバで使用されている場合、URL に対して返される最初の HTML ページを構成するために使用するスタイルシートがファイル項目によって指定されます。発行者チャネルの Web サーバ以外のサーバを使用している場合、ファイル項目によって、URL が参照するリ \'83\'5c ースの名前が指定されます。

ファイル項目が表示されない場合、URl ファイル部分のデフォルトは process_template.xsl になります。

scheme: <url-data> 要素の下にあるオプション項目です。この項目が存在する場合、(http または ftp などの)URL のスキーム部分が指定されます。通常スキーム項目は、URL が発行者の Web サーバ以外のサーバを指す場合のみ使用されます。

スキーム項目が \'95\'5c 示されない場合、発行者チャネルの Web サーバの設定に応じて、URL スキームのデフォルトは http または https いずれかになります。

host: <url-data> 要素の下にあるオプション項目です。この項目が存在する場合、URL のホスト部分が指定されます。通常ホスト項目は、URL が発行者の Web サーバ以外のサーバを指す場合のみ使用されます。

ホスト項目が \'95\'5c 示されない場合、URL ホストのデフォルトは、手動タスクサービスドライバが実行されているサーバの IP アドレス (つまり、発行者チャネルの Web サーバの IP アドレス) になります。

port: <url-data> 要素の下にあるオプション項目です。この項目が存在する場合、URL のポート部分が指定されます。通常ポート項目は、URL が発行者の Web サーバ以外のサーバを指す場合のみ使用されます。

ポート項目が \'95\'5c 示されない場合、URL ポートのデフォルトは発行者チャネルの Web サーバが実行されているポートになります。

D.2.4 <url-query>

<url-query> 要素は、<url-data> 要素の子です。これには、電子メールメッセージで使用される URL のクエリ部分を \'8d\'5c 成するために使用される <item> 要素が含まれています。

<url-query> 要素の子として表示される各項目は、name=“value”という形式名のクエリ文字列に配置されます。ここでは、name は <item> 要素の name 属性の値であり、値は <item> 要素の文字列コンテンツです。

<url-query> の下に表示される Item 要素は、「yes」の値の保護属性を持つことができます。この場合、項目名および値は暗号化され、URL クエリ文字列で生成された name-value ペア内に配置されます。生成された値の名前は protected-data です。値は Base64 でエンコードされており、暗号化されている name-value ペアまたは複数値の属性のペアです。

データを保護すると、発行者チャネルの Web サーバに URL が送信されるときにデータを変更できません。たとえば、電子メールメッセージに応答することを承認されているユーザのみが eDirectory データを変更できるようにするために、responder-dn データ項目を保護する必要があります。

生成された URL が発行者チャネルの Web サーバで使用される場合、<url-query> 要素には、少なくとも 1 つの <item name=“responder-dn”protect=“yes”> 要素が含まれている必要があります。含まれていない場合、Web サーバでは HTTP POST 要求が拒否されます。

手動タスクサービスドライバ : 自動置換データ項目

E

手動タスクサービスドライバは、特定の置換データ項目の要素を自動的に提供します。この節では、これらのデータ項目について説明します。

E.1 加入者チャネルの自動置換データ

加入者チャネルによって処理されているときに、次のデータ項目が replacement-data ドキュメントに自動的に追加されます。

association: <mail> 要素に <association> 要素の子がある場合、または購読者が <add-association> 要素を返した場合、replacement-data ドキュメントに <item name=”association”> 要素が追加されます。<item> 要素のコンテンツは、処理される電子メールメッセージに関連付けられた eDirectory オブジェクトの関連付けの値です。関連付けの値は eDirectory オブジェクトには書き込まれない場合があります。したがって、関連付けの値はクエリには使用できません。

url: <item> 要素のコンテンツは、電子メールメッセージで使用される完全な URL です。購読者チャネルで、<url-data> 要素の下で検出された次の項目から url 項目が作成されます。スキーム、ホスト、ポート、ファイル、および <url-query> 要素の下にある項目。スキーム、ホスト、またはポートが見つからない場合、デフォルト値が使用されます。デフォルト値は、発行者チャネルの Web サーバの設定で決まります。

url-base: <item> 要素のコンテンツは、リ \'83\'5c ースの識別子 (file) およびクエリ文字列を含まない、生成された URL の一部です。

url-query: <item> 要素のコンテンツは、<url-query> 要素の下の <item> 要素から生成された URL クエリ文字列です。

url-file: <item> 要素のコンテンツは、URL のリ \'83\'5c ースの識別子です。

protected-data: <item> 要素のコンテンツは、<url-query> 要素の下の <item> 要素から取得した、暗号化された形式の name-value ペアです。保護属性が「yes」に設定されている <item> 要素のみが保護されたデータ値に追加されます。保護されたデータの詳細については、331 ページの付録 D「手動タスクサービスドライバ : 置換データ」の「データのセキュリティ」を参照してください。

E.2 発行者チャネルの自動置換データ

発行者チャネルの Web サーバによって処理されているときに、次のデータ項目が replacement-data ドキュメントに自動的に追加されます。

post-status: HTTP POST 要求の処理中に、発行者チャネルの Web サーバによって、<item name=“post-status”> 要素が作成され、replacement-data ドキュメントに追加されます。Web サーバへの HTTP POST 要求は、XDS ドキュメントを Identity Manager に送信するための要求です。Identity Manager は、XDS 送信の結果としてステータスドキュメントを返します。<item name=“post-status”> 要素のコンテンツは、Identity Manager への送信の結果として、Identity Manager によって返された <status> 要素のレベル属性の値です。

通常 post-status 項目は、HTTP POST 要求の結果として返される Web ページの \'8d\'5c 成に使用されます。

post-status-message: HTTP POST 要求の処理中に、発行者チャネルの Web サーバによって、<item name=“post-status-message”> 要素が作成され、replacement-data ドキュメントに追加されます。Web サーバへの HTTP POST 要求は、XDS ドキュメントを Identity Manager に送信するための要求です。Identity Manager は、XDS 送信の結果としてステータスドキュメントを返します。<item name=“post-status-message”> 要素のコンテンツは、Identity Manager への送信の結果として、Identity Manager によって返された <status> 要素のコンテンツです。Identity Manager によって返された <status> 要素にコンテンツがある場合のみ、post-status-message 項目が作成されます。

通常 post-status-message 項目は、HTTP POST 要求の結果として返される Web ページの \'8d\'5c 成に使用されます。

url: HTTP GET および HTTP POST 要求の処理中に、発行者チャネルの Web サーバによって、<item name=“url”> 要素が作成され、replacement-data ドキュメントに追加されます。<item> 要素は、replacement-data ドキュメントを使用してドキュメントを作成する前に追加されます。Web サーバの設定によって、URL スキーム、ホスト、およびポートが決定されます。

url-base: HTTP GET および HTTP POST 要求の処理中に、発行者チャネルの Web サーバによって、<item name=“url-base”> が作成され、replacement-data ドキュメントに追加されます。<item> 要素は、replacement-data ドキュメントを使用してドキュメントを作成する前に追加されます。発行者チャネル上の url-base の <item> 要素のコンテンツは、url の <item> 要素と同じです。

手動タスクサービスドライバ : テンプレートアクション要素の参照

F

アクション要素は、シンプルなロジック制御、または HTML 形式の HTML 要素を作成するために使用されるテンプレートドキュメントの namespace-qualified 要素です。要素を修飾するために使用されているネームスペースは、http://www.novell.com/dirxml/manualtask/form にあります。このドキュメントおよび手動タスクサービスドライバで提供されているサンプルテンプレートでは、使用されているプレフィクスがフォームにあります。

このセクションで特に説明されていないアクション要素は、(スタイルシートがカスタマイズされない限り) テンプレート処理のスタイルシートによって出力ドキュメントから除かれます。この動作により、たとえば、プレーンテキストの電子メールメッセージのデータを囲むために form:text 要素を使用できるようになり、テンプレートが有効な XML になります。

F.1 <form:input>

1 つ以上の置換データ項目があるかどうかに基づいて、1 つ以上の HTML INPUT 要素を生成するために <form:input> 要素が使用されます。作成された INPUT 要素の数は、<form:input> 要素の名前属性によって指定された名前を持つ置換データ項目の数に対応しています。

属性

名前 : INPUT 要素を作成するために使用される置換データ項目の名前を指定します。作成された INPUT 要素の名前属性の値として、属性値が使用されます。

type または TYPE: 作成された INPUT 要素のタイプ属性の値を指定します。

値 : 値属性の値が「yes」と同等である場合、値が置換データ項目の文字列値である、作成された INPUT 要素に値属性が追加されます。値属性の値が「yes」以外である場合、作成された INPUT 要素のコンテンツが置換データ項目の文字列値に設定されます。

例

```
<form:input name=“responder-dn” TYPE=“hidden” value=“yes” />
```

以下に類似した、1 つ以上の INPUT 要素を作成します

```
<INPUT name=“responder-dn” TYPE=“hidden” value=“\PERIN-
TAO\novell\phb” />
```

F.2 <form:if-item-exists>

条件付きで出力ドキュメントにデータを挿入するには、<form:if-item-exists> 要素が使用されます。<form:if-item-exists> のコンテンツは、指定した項目が置換データに \'95\'5c 示される場合のみ処理されます。

属性

名前 : 置換データ項目の名前を指定します。1 つ以上の置換データ項目の例が存在する場合、<form:if-item-exists> 要素のコンテンツが処理されます。

例

```
<form:if-item-exists name="post-status-message">
      <tr>
        <td>
          Status message was: $post-status-message$
        </td>
      </tr>
</form:if-item-exists>
```

この例では、post-status-message という名前の置換データ項目がある場合のみ、行が HTML テーブルに \'91\'7d 入されます。

F.3 <form:if-multiple-items>

form:if-multiple-items 要素は、条件付きで出力ドキュメントにデータを挿入するために使用されます。form:if-multiple-items のコンテンツは、指定した項目が置換データに複数回 \'95\'5c 示される場合のみ処理されます。

属性

名前 : 置換データ項目の名前を指定します。置換データ項目の複数の例が存在する場合、form:if-multiple-items のコンテンツが処理されます。

例

```
<form:if-multiple-items name="responder-dn">
    <form:menu name="responder-dn"/>
</form:if-multiple-items>
```

この例では、responder-dn という名前を持つ複数の置換データ項目がある場合、HTML SELECT 要素 (<form:menu> を参照) が作成されます。

F.4 <form:if-single-item>

form:if-single-item 要素は、条件付きで出力ドキュメントにデータを挿入するために使用されます。form:if- single -item のコンテンツは、指定した項目が置換データに 1 回だけ \'95\'5c 示される場合のみ処理されます。

属性

名前 : 置換データ項目の名前を指定します。名前付き項目が置換データに 1 回だけ \'95\'5c 示される場合、form:if-single-item コンテンツが処理されます。

例

```
<form:if-single-item name="responder-dn">
  <input TYPE="hidden" name="responder-dn" value="$responder-dn$"/>
```

```
  $responder-dn$
</form:if-single-item>
```

この例では、「responder-dn」という名前の置換データ項目が置換データに 1 つだけある場合に、HTML INPUT 要素およびいくつかの置換テキストが出力ドキュメントに \'91\'7d 入されます。

F.5 <form:menu>

form:menu 要素は、1 つ以上の OPTION 要素の子を持つ HTML SELECT 要素を生成するために使用されます。最初の OPTION 要素の子には、選択したことを示す確認 \'83\'7d一クが付きます。

属性

名前 : 置換データ項目の名前を指定します。名前付き項目が置換データに表示された場合、HTML SELECT 要素が出力ドキュメントで作成されます。置換データ内の置換データ項目の各インスタンスで、SELECT 要素の子として HTML OPTION 要素が作成されます。

例

```
<form:menu name="responder-dn"/>
```

この例の結果として、次に類似した HTML 要素が作成されます。

```
<SELECT name="responder-dn">
    <OPTION selected>\PERIN-TAO\big-org\php</OPTION>
    <OPTION>\PERIN-TAO\big-org\carol</OPTION>
</SELECT>
```

手動タスクサービスドライバ : <mail> 要素参照

G

<mail> 要素およびそのコンテンツについては、このセクションで詳しく説明しています。要素に対して属性が一覧 \'95\'5c 示されていない場合、要素では属性が定義されていません。

G.1 <mail>

<mail> 要素およびそのコンテンツにより、SMTP メッセージを \'8d\'5c 成するために必要なデータが説明されます。

<mail> 属性

src-dn: 電子メールをトリガする、eDirectory オブジェクトの DN 値が含まれています。電子メールに対して、発行者チャネルの Web サーバを経由してオブジェクトのデータが変更される場合に必要です。

G.2 <to>

<to> 要素は <mail> 要素の子です。1 つ以上の <to> 要素には、SMTP メッセージの主な受信者の電子メールアドレスが含まれています。少なくとも 1 つの <to> 要素が必要です。各 <to> 要素には、単一の電子メールアドレスのみが含まれている必要があります。

G.3 <cc>

<cc> 要素は <mail> 要素の子です。ゼロ以上の <cc> 要素には、SMTP メッセージの CC の受信者の電子メールアドレスが含まれています。<cc> 要素は必須ではありません。各 <cc> 要素には、単一の電子メールアドレスのみが含まれている必要があります。

G.4 <bcc>

<bcc> 要素は <mail> 要素の子です。ゼロ以上の <bcc> 要素には、SMTP メッセージの BCC の受信者の電子メールアドレスが含まれています。<bcc> 要素は必須ではありません。各 <bcc> 要素には、単一の電子メールアドレスのみが含まれている必要があります。

G.5 <from>

<from> 要素は <mail> 要素の子です。<from> 要素には、電子メールの送信者の電子メールアドレスが含まれています。<from> 要素は必須ではありません。<from> 要素がない場合、手動タスクサービスドライバパラメータの一部として提供されたアドレスからのデフォルトが使用されます。

G.6 <reply-to>

<reply-to> 要素は <mail> 要素の子です。<reply-to> 要素には、SMTP メッセージへの返信の送信先となるエンティティの電子メールアドレスが含まれています。<reply-to> 要素は必 \'90\'7b ではありません。

G.7 <subject>

<subject> 要素は <mail> 要素の子です。文字列のコンテンツは、SMTP の件名フィールドを設定するために使用されます。<subject> 要素は必 \'90\'7b ではありませんが、使用することをお勧めします。

G.8 <message>

<message> 要素は <mail> 要素の子です。この要素のコンテンツは、SMTP メッセージのメッセージ本文を作成するために使用されます。少なくとも 1 つの <message> 要素が必要です。メッセージ \'96\'7b 文で代替的な方法 (プレーンテキストと HTML、または英語とその他の言語などの) を持つ SMTP メッセージを \'8d\'5c 成する場合、複数の <message> 要素を提供できます。

<message> 属性

mime-type: オプションで、<message> 要素によって構成されたメッセージ本文の MIME タイプを指定します (テキスト / プレーンまたはテキスト /html など)。mime-type 属性がない場合、ドライバは MIME タイプを自動的に検出しようとします。

電子メールのクライアントは、最も良い \'95\'5c 示方法を選択するために SMTP メッセージが代替的な方法を持っている場合、MIME タイプを使用できます。

言語 : オプションで、<message> 要素によって構成されたメッセージ本文の言語を指定します。値は、SMTP の仕様に従っている必要があります。言語属性がない場合、デフォルトは提供されません。

電子メールのクライアントは、最も良い \'95\'5c 示方法を選択するために SMTP メッセージが代替的な方法を持っている場合、言語仕様を使用できます。

G.9 <stylesheet>

<stylesheet> 要素は、<message> 要素の子です。<stylesheet> 要素のコンテンツは、メッセージ本文の作成に使用される XSLT スタイルシートの名前です。<stylesheet> 要素がない場合、スタイルシートとして process_template.xsl が使用されます。

G.10 <template>

<template> 要素は、<message> 要素の子です。<template> 要素のコンテンツは、メッセージ本文の作成に使用される XML ドキュメントの名前です。<template> 要素がない場合、メッセージ \'96\'7b 文を \'8d\'5c 成するためのメッセージのスタイルシートによって、置換データのドキュメントが処理されます。

G.11 <filename>

<filename> 要素は <attachment> 要素の子です。<filename> 要素のコンテンツはファイル名です。\'8d\'5c 成されたアタッチメントにファイル名を割り当てるために、ファイル名の値が使用されます。

G.12 <replacement-data>

<replacement-data> 要素は、<message> 要素の子です。この要素のコンテンツは、メッセージのテンプレートを処理するスタイルシートに対するパラメータとして使用されます。テンプレートがない場合は、メッセージのスタイルシートによって直接処理されます。<replacement-data> 要素のコンテンツについては、331 ページの付録 D「手動タスクサービスドライバ : 置換データ」および 337 ページの付録 E「手動タスクサービスドライバ : 自動置換データ項目」で説明しています。

G.13 <resource>

<resource> 要素は、<message> 要素の子です。この要素のコンテンツは、メッセージ本文の SMTP メッセージのリソースに組み込まれるファイルの名前として扱われます。たとえば、HTML メッセージ \'96\'7b 文の .css スタイルシートは、リ \'83\'5c ースとして提供できます。

<resource> 属性

cid: メッセージ本文の URL のリソースを参照するために使用されるコンテンツ ID を指定します。たとえば、.css スタイルシートがリ \'83\'5c ースにある場合、cid 値は css-1 になります。HTML メッセージ \'96\'7b 文では、次の要素を使用して .css スタイルシートを参照できます。

```
<link href="cid:css-1" rel="style sheet" type="text/css">
```

G.14 <attachment>

<attachment> 要素は <mail> 要素の子です。これは、<message> と同じコンテンツを持つことができます。または、コンテンツとしてファイル名を持つことができます。ゼロ以上の <attachment> 要素は、<mail> 要素の子として \'95\'5c 示できます。

<attachment> 属性

mime-type: オプションで、添付ファイルの MIME タイプを指定します。mime-type 属性がない場合、ドライバは MIME タイプを自動的に検出しようとします。

言語 : オプションで、添付ファイルの言語を指定します。言語属性がない場合、デフォルトは提供されません。

手動タスクサービスドライバ : 新しい従業員のデータフローシナリオ

H

このセクションでは、新しい従業員を雇用したときに、電子メールメッセージがこの従業員のマネージャに送信されるという場合のデータフローについて、ステップごとに説明していきます。電子メールメッセージで、メッセージ内の URL を使用して従業員の部屋番号の値を入力するよう \'83\'7d ネージャに要求します。

シナリオの例の手動タスクサービスドライバの設定については、次のとおりです。

H.1 加入者チャネルの設定

フィルタ

クラス : User

Attributes: 名前、\'83\'7d ネージャ、名字

ポリシー

Create Policy (作成ポリシー): 名前、\'83\'7d ネージャ、および名字の属性がが必要です。

Command Transformation(コ \'83\'7d ンド変換) ポリシー : <add> を <mail> 要素に変換します。

H.2 発行者チャネルの設定

フィルタ

クラス : User

Attributes: roomNumber

ポリシー

なし。

H.3 データフローの説明

次のリストでは、プロセスを介してフローする最も重要なデータ項目は、responder-dn および association です。responder-dn 項目は、Web サーバを介してデータを入力するユーザを認証するために使用されます。association 項目により、データが変更される eDirectory オブジェクトが識別されます。

1. 会社が新しい従業員を雇用しました。会社の人事 (HR) システムに新しい従業員のデータが入力されます。

2. 人事システムの Identity Manager ドライバにより、eDirectory に新しいユーザオブジェクトが作成されます。ユーザ属性には、名前、名字、および \'83\'7d ネージャが含まれています。
3. 新しいユーザオブジェクトの次の <add> イベントが、手動タスクサービスドライバの加入者チャネルに送信されます。

```
<nds dtdversion="1.1" ndsversion="8.6">
  <input>
    <add class-name="User" src-dn="\PERIN-TAO\novell\Provo\Joe"
src-entry-id="281002" timestamp="1023314433#2">
      <add-attr attr-name="Surname">
        <value type="string">the Intern</value>
      <add-attr>
      <add-attr attr-name="Given Name">
        <value type="string">Joe</value>
      <add-attr>
      <add-attr attr-name="manager">
        <value type="dn">\PERIN-TAO\novell\Provo\phb</value>
      <add-attr>
    </add>
  </input>
</nds>
```

   a. Subscriber Command Transformation (加入者コ \'83\'7d ンド変換) ポリシーでは、\'83\'7d ネージャの電子メールアドレスおよび \'83\'7d ネージャのアシスタントの DN に対して eDirectory にクエリを発行するために、\'83\'7d ネージャ DN 値が使用されます。
   b. \'83\'7d ネージャにアシスタントがいる場合、アシスタントの電子メールアドレスに対して、Subscriber Command Transformation (加入者コ \'83\'7d ンド変換) によって eDirectory にクエリが発行されます。
   c. 購読者コマンド変換によって <mail> 要素が作成され、<add> コマンド要素が <mail> 要素に置換されます。以下の例では、置換データ項目は太字で示しています。

```
<nds dtdversion="1.1" ndsversion="8.6">
  <input>
    <mail src-dn="\PERIN-TAO\novell\Provo\Joe">
      <to>phb@company.com</to>
      <cc>carol@company.com</cc>
      <bcc>HR@company.com</bcc>
      <reply-to>HR@company.com</reply-to>
      <subject>Room Assignment Needed for: Joe the Intern</
subject>
      <message mime-type="text/html">
        <stylesheet>process_template.xsl</stylesheet>
        <template>html_msg_template.xml</template>
        <replacement-data>
          <item name="manager">JStanley</item>          <item
name="given-name">Joe</item>          <item name="surname">the
Intern</item>
          <url-data>
            <item name="file">process_template.xsl</item>
            <url-query>
         <item name="template">form_template.xml</item>
```

```
<item name="responder-dn" protect="yes">\PERIN-
TAO\novell\Provo\phb</item>              <item name="responder-
dn" protect="yes">\PERIN-TAO\novell\Provo\carol</item>
<item name="subject-name">Joe the Intern</item>
            </url-query>
          </url-data>
        </replacement-data>
        <resource cid="css-1">novdocmain.css</resource>
      </message>
    </mail>
  </input>
</nds>
```

d. 手動タスクサービスドライバの加入者は、Nsure™ Identity Manager から <mail> 要素を受信します。

e. <mail> 要素には src-dn 属性があるため、加入者によって関連付けの値が生成されます。

f. 電子メールメッセージの作成に使用するために、購読者によって <mail> 要素のデータから置換データのドキュメントが作成されます。URL のクエリ部分には、さまざまなデータ項目があります (「?」の後に続く太字の URL の部分)。発行者チャネルの Web サーバでは、HTTP GET 要求として URL が Web サーバに送信されるときに、これらのデータ項目が使用されます。

```
<replacement-data>
  <item name="manager">JStanley</item>
  <item name="given-name">Joe</item>
  <item name="surname">the Intern</item>
  <item name="template">form_template.xml</item>
  <item name="responder-dn">\PERIN-TAO\novell\Provo\phb</item>
  <item name="responder-dn">\PERIN-TAO\novell\Provo\carol</
item>
  <item name="subject-name">Joe the Intern</item>
  <item name="association">1671b2:ee4246a561:-
7fff:192.168.0.1</item>
  <item name="url-base">https://192.168.0.1:8180</item>
  <item name="url-file">process_template.xsl</item>
  <item name="protected-data">
rO0ABXNyABlqYXZheC5jcnlwdG8uU2VhbGVkT2JqZWN0PjY9psO3VHACAARbAA
1lbmNvZGVkUGFyYW1zdAACW0JbABBlbmNyeXB0ZWRDb250ZW50cQB+AAFMAAlw
YXJhbXNBbGd0ABJMamF2YS9sYW5nL1N0cmluZztMAAdzZWFsQWxncQB+AAJ4cH
VyAAJbQqzzF/gGCFTgAgAAeHAAAAAPMA0ECEIBRohGPjxEAgEKdXEAfgAEAAAA
uMSFqzHXwtMx8DkRCzkK1O46sEz1u51o3MDvHn+3+fE6SphHr3Hgjli4Jp3rUk
H7y6dXvcu7iq21Vs+9o6iZVzljTIJX/jjRrVZlR5JOuRNhk8JHFZ8FhgsmiIAH
/Fs61k4WmyEcmYfWmfqfBVeThr3Avwcim6ranS5Mm2U5i9Z/DBR13pIAobMpWY
kMaz4+G9e6oovBsiPdp6jSPzbFxcgALI2AMBh4hf9jnx7zOU9Uvd9qXtaE2rR0
AANQQkV0ABBQQkVXaXRoTUQ1QW5kREVT</item>
  <item name="url-
query">template=form_template.xml&amp;responder-dn=%5CPERIN-
TAO%5Cnovell%5Cprovo%5Cphb&amp;responder-dn=%5CPERIN-
TAO%5Cnovell%5Cprovo%5Ccarol&amp;subject-
name=Joe+the+Intern&amp;association=1671b2%3Aee4246a561%3A-
7fff%3A192.168.0.1&amp;protected-
data=rO0ABXNyABlqYXZheC5jcnlwdG8uU2VhbGVkT2JqZWN0PjY9psO3VHACAA
RbAA1lbmNvZGVkUGFyYW1zdAACW0JbABBlbmNyeXB0ZWRDb250ZW50cQB%2BAAF
```

```
MAAlwYXJhbXNBbGd0ABJMamF2YS9sYW5nL1N0cmluZztMAAdzZWFsQWxncQB%2B
AAJ4cHVyAAJbQqzzF%2FgGCFTgAgAAeHAAAAAPMA0ECEIBRohGPjxEAgEKdXEAf
gAEAAAAuMSFqzHXwtMx8DkRCzkK1O46sEz1u51o3MDvHn%2B3%2BfE6SphHr3Hg
jli4Jp3rUkH7y6dXvcu7iq21Vs%2B9o6iZVzljTIJX%2FjjRrVZlR5JouRNhk8J
HFZ8FhgsmiIAH%2FFs61k4WmyEcmYfWmfqfBVeThr3Avwcim6ranS5Mm2U5i9Z%
2FDBR13pIAobMpWYkMaz4%2BG9e6oovBsiPdp6jSPzbFxcgALI2AMBh4hf9jnx7
zOU9Uvd9qXtaE2rR0AANQQkV0ABBQQkVXaXRoTUQ1QW5kREVT</item>
  <item name="url">
https://192.168.0.1:8180/
process_template.xsl?template=form_template.xml&amp;responder-
dn=%5CPERIN-TAO%5Cnovell%5CProvo%5Cphb&amp;responder-
dn=%5CPERIN-TAO%5Cnovell%5Cprovo%5Ccarol&amp;subject-
name=Joe+the+Intern&amp;association=1671b2%3Aee4246a561%3A-
7fff%3A192.168.0.1&amp;protected-
data=rO0ABXNyABlqYXZheC5jcnlwdG8uU2VhbGVkT2JqZWN0PjY9psO3VHACAA
RbAA1lbmNvZGVkUGFyYW1zdAACW0JbABBlbmNyeXB0ZWRDb250ZW50cQB%2BAAF
MAAlwYXJhbXNBbGd0ABJMamF2YS9sYW5nL1N0cmluZztMAAdzZWFsQWxncQB%2B
AAJ4cHVyAAJbQqzzF%2FgGCFTgAgAAeHAAAAAPMA0ECEIBRohGPjxEAgEKdXEAf
gAEAAAAuMSFqzHXwtMx8DkRCzkK1O46sEz1u51o3MDvHn%2B3%2BfE6SphHr3Hg
jli4Jp3rUkH7y6dXvcu7iq21Vs%2B9o6iZVzljTIJX%2FjjRrVZlR5JouRNhk8J
HFZ8FhgsmiIAH%2FFs61k4WmyEcmYfWmfqfBVeThr3Avwcim6ranS5Mm2U5i9Z%
2FDBR13pIAobMpWYkMaz4%2BG9e6oovBsiPdp6jSPzbFxcgALI2AMBh4hf9jnx7
zOU9Uvd9qXtaE2rR0AANQQkV0ABBQQkVXaXRoTUQ1QW5kREV
</item>
</replacement-data>
```

g. 購読者は、html_msg_template.xml with process_template.xsl を処理します。置換データドキュメントはパラメータとしてスタイルシートに渡されます。html_msg_template.xml ドキュメントが続きます。置換トークンは太字で示しています。置換トークンは、置換データのドキュメント内の対応する <item> 要素の値によって置換されます。

```
<html xmlns:form="http://www.novell.com/dirxml/manualtask/
form">
  <head>
  </head>
  <body>
    <link href="cid:css-1" rel="style sheet" type="text/css"/>
    <p>
    Dear $manager$,
    </p>
    <p>
    This message is to inform you that your new employee
<b>$given-name$ $surname$</b> has been hired.
    </p>
    <p>
    Please assign a room number for this individual. Click <a
href="$url$">Here</a> to do this.
    </p>
    <p>
    Thank you,<br/>
    HR<br/>
    HR Department
    </p>
```

```
  </body>
</html>
```

生成された電子メールドキュメントが続きます。置換トークンは、置換データのドキュメント内の対応する <item> 要素の値によって置換されました。

```
<html>
  <head>
<META http-equiv="Content-Type" content="text/html;
charset=UTF-8">
  </head>
  <body>
    <link href="cid:css-1" rel="style sheet" type="text/css">
    <p>
    Dear J Stanley,
    </p>
    <p>
    This message is to inform you that your new employee <b>Joe
the Intern</b> has been hired.
    </p>
    <p>
    Please assign a room number for this individual. Click <a
href="https://192.168.0.1:8180/
process_template.xsl?template=form_template.xml&responder-
dn=%5CPERIN-TAO%5Cnovell%5CProvo%5Cphb&responder-dn=%5CPERIN-
TAO%5Cnovell%5CProvo%5Ccarol&subject-
name=Joe+the+Intern&association=45f0e3%3Aee45e07709%3A-
7fff%3A192.168.0.1&protected-
data=rO0ABXNyABlqYXZheC5jcnlwdG8uU2VhbGVkT2JqZWN0PjY9psO3VHACAA
RbAA1lbmNvZGVkUGFyYW1zdAACW0JbABBlbmNyeXB0ZWRDb250ZW50cQB%2BAAF
MAAlwYXJhbXNBbGd0ABJMamF2YS9sYW5nL1N0cmluZztMAAdzZWFsQWxncQB%2B
AAJ4cHVyAAJbQqzzF%2FgGCFTgAgAAeHAAAAAPMA0ECIr9Z1iG%2BO3BAgEKdXE
AfgAEAAAAuMU%2FSoFRkebvh2d5SqalF91ttjRY5lyyW5%2B%2FFIfOuDdYikYi
DbOJb6607S0dPHjQzeVgu6ptIvGqaEQOEjBjDkY%2Bi4VoVjUSXS3a8fiXB8moM
dPtLJ%2FGyE8QiwbT4xbkQy48i02k99F2vGmlenRpSP6dD31kZl3dpJ0mGgq2yL
%2FeFaynKyqnjkHLMexcqD8WlVooaRl1k2RPk5vDYvC8o2bn22OKKbOnSRM5YlP
S0iWzxo0JVcnVVyt0AANQQkV0ABBQQkVXaXRoTUQ1QW5kREVT">Here</a> to
do this.
    </p>
    <p>
    Thank you,<br>
    HR<br>
    HR Department
    </p>
  </body>
</html>
```

h. SMTP 電子メールメッセージが \'83\'7d ネージャおよび \'83\'7d ネージャのアシスタントに送信されます。

i. 加入者によって、<status> 要素および <add-association> 要素が含まれている XML ドキュメントが Identity Manager に返されます。

4. \'83\'7d ネージャが電子メールメッセージを開き、［Click here］リンクをクリックします。

5. \'83\'7d ネージャの Web ブラウザによって、HTTP GET 要求として発行者チャネルの Web サーバに URL が送信されます。

   a. Web サーバは、次の置換データのドキュメントを作成します。多くのデータ項目は、URL のクエリ部分からのものです。例外は、自動的に生成された項目の url および url-base です。

```
<replacement-data>
  <item name="association">45f0e3:ee45e07709:-
7fff:192.168.0.1</item>
  <item name="protected-
data">rO0ABXNyABlqYXZheC5jcnlwdG8uU2VhbGVkT2JqZWN0PjY9psO3VHACA
ARbAA1lbmNvZGVkUGFyYW1zdAACW0JbABBlbmNyeXB0ZWRDb250ZW50cQB+AAFM
AAlwYXJhbXNBbGd0ABJMamF2YS9sYW5nL1N0cmluZztMAAdzZWFsQWxncQB+AAJ
4cHVyAAJbQqzzF/
gGCFTgAgAAeHAAAAAPMA0ECIr9Z1iG+O3BAgEKdXEAfgAEAAAAuMU/
SoFRkebvh2d5SqalF91ttjRY5lyyW5+/
FifOuDdYikYiDbOJb6607S0dPHjQzeVgu6ptIvGqaEQOEjBjDkY+i4VoVjUSXS3
a8fiXB8moMdPtLJ/
GyE8QiwbT4xbkQy48i02k99F2vGmlenRpSP6dD31kZl3dpJ0mGgq2yL/
eFaynKyqnjkHLMexcqD8WlVooaRl1k2RPk5vDYvC8o2bn22OKKbOnSRM5YlPS0i
Wzxo0JVcnVVyt0AANQQkV0ABBQQkVXaXRoTUQ1QW5kREVT</item>
  <item name="template">form_template.xml</item>
  <item name="responder-dn">\PERIN-TAO\novell\Provo\phb</item>
  <item name="responder-dn">\PERIN-TAO\novell\Provo\carol</
item>
  <item name="subject-name">Joe the Intern</item>
  <item name="url-base">https://192.168.0.1:8180</item>
  <item name="url">https://192.168.0.1:8180</item>
</replacement-data>
```

   Web サーバは、process_template.xsl スタイルシートを使用して form_templates.xml ドキュメントを処理します。置換トークンおよびアクション要素は太字で示しています。データ項目が HTML POST データの一部として Web サーバに渡されるように、さまざまなデータ項目が非 \'95\'5c 示の INPUT 要素に配置されています。

   また、従業員の roomNumber 属性 (存在する場合) の現在値を取得する、$query:roomNumber$ 置換トークンがあります。

```
<html  xmlns:form="http://www.novell.com/dirxml/manualtask/
form">
  <head>
    <title>Enter room number for $subject-name$</title>
  </head>
  <body>
    <link href="novdocmain.css" rel="style sheet" type="text/
css"/>
    <br/><br/><br/><br/>
    <form class="myform" METHOD="POST" ACTION="$url-base$/
process_template.xsl">
        <table cellpadding="5" cellspacing="10" border="1"
align="center">
          <tr><td>
          <input TYPE="hidden" name="template"
value="post_form.xml"/>
          <input TYPE="hidden" name="subject-name"
```

```
value="$subject-name$"/>
          <input TYPE="hidden" name="association"
value="$association$"/>
          <input TYPE="hidden" name="response-style sheet"
value="process_template.xsl"/>
          <input TYPE="hidden" name="response-template"
value="post_response.xml"/>
          <input TYPE="hidden" name="auth-style sheet"
value="process_template.xsl"/>
          <input TYPE="hidden" name="auth-template"
value="auth_response.xml"/>
          <input TYPE="hidden" name="protected-data"
value="$protected-data$"/>
          <form:if-single-item name="responder-dn">
            You are:<br/>
            <input TYPE="hidden" name="responder-dn"
value="$responder-dn$"/>
            $responder-dn$
         </form:if-single-item>         <form:if-multiple-items
name="responder-dn">
            Indicate your identity:<br/>
           <form:menu name="responder-dn"/>          </form:if-
multiple-items>
        </td></tr>
        <tr><td>
          Enter your password: <br/><input name="password"
TYPE="password" SIZE="20" MAXLENGTH="40"/>
        </td></tr>
        <tr><td>
          Enter room number for $subject-name$:<br/>
          <input TYPE="text" NAME="room-number" SIZE="20"
MAXLENGTH="20" value="$query:roomNumber$"/>
        </td></tr>
        <tr><td>
          <input TYPE="submit" value="Submit"/> <input
TYPE="reset" value="Clear"/>
        </td></tr>
      </table>
    </form>
  </body>
</html>
```

結果は次の HTML ページのとおりです。

```
<html>
  <head>
<META http-equiv="Content-Type" content="text/html;
charset=UTF-8">
    <title>Enter room number for Joe the Intern</title>
  </head>
  <body>
    <link href="novdocmain.css" rel="style sheet" type="text/
css">
    <br><br><br><br>
<form class="myform" METHOD="POST" ACTION="https://
```

```
192.168.0.1:8180/process_template.xsl">
<table cellpadding="5" cellspacing="10" border="1"
align="center">
<tr>
<td>
    <input TYPE="hidden" name="template" value="post_form.xml">
    <input TYPE="hidden" name="subject-name" value="Joe the
Intern">
    <input TYPE="hidden" name="association"
value="45f0e3:ee45e07709:-7fff:192.168.0.1">
    <input TYPE="hidden" name="response-style sheet"
value="process_template.xsl">
    <input TYPE="hidden" name="response-template"
value="post_response.xml">
    <input TYPE="hidden" name="auth-style sheet"
value="process_template.xsl">
    <input TYPE="hidden" name="auth-template"
value="auth_response.xml">
    <input TYPE="hidden" name="protected-data"
value="rO0ABXNyABlqYXZheC5jcnlwdG8uU2VhbGVkT2JqZWN0PjY9psO3VHAC
AARbAA1lbmNvZGVkUGFyYW1zdAACW0JbABBlbmNyeXB0ZWRDb250ZW50cQB+AAF
MAAlwYXJhbXNBbGd0ABJMamF2YS9sYW5nL1N0cmluZztMAAdzZWFsQWxncQB+AA
J4cHVyAAJbQqzzF/
gGCFTgAgAAeHAAAAAPMA0ECIr9Z1iG+O3BAgEKdXEAfgAEAAAAuMU/
SoFRkebvh2d5SqalF91ttjRY5lyyW5+/
FIfOuDdYikYiDbOJb6607S0dPHjQzeVgu6ptIvGqaEQOEjBjDkY+i4VoVjUSXS3
a8fiXB8moMdPtLJ/
GyE8QiwbT4xbkQy48i02k99F2vGmlenRpSP6dD31kZl3dpJ0mGgq2yL/
eFaynKyqnjkHLMexcqD8WlVooaRl1k2RPk5vDYvC8o2bn22OKKbOnSRM5YlPS0i
Wzxo0JVcnVVyt0AANQQkV0ABBQQkVXaXRoTUQ1QW5kREVT">
    Indicate your identity:<br>
    <SELECT name="responder-dn">
        <OPTION selected>\PERIN-TAO\novell\Provo\phb</OPTION>
        <OPTION>\PERIN-TAO\novell\Provo\carol</OPTION>
    </SELECT>
</td>
</tr>
<tr>
<td>
    Enter your password: <br>

    <input name="password" TYPE="password" SIZE="20"
MAXLENGTH="40">
</td>
</tr>
<tr>
<td>
    Enter room number for Joe the Intern:<br>
    <input TYPE="text" NAME="room-number" SIZE="20"
MAXLENGTH="20" value="">
</td>
</tr>
<tr>
<td>
```

```
    <input TYPE="submit" value="Submit"> <input TYPE="reset"
value="Clear">
</td>
</tr>
</table>
</form>
</body>
</html>
```

b. \'83\'7d ネージャは Web ページのメニューから eDirectory DN を選択し、パスワードを入力し、新しい従業員の部屋番号を入力し、［Submit］をクリックします。

c. Web ブラウザによって、HTTP POST 要求が Web サーバに送信されます。

d. Web サーバが、POST データから次の置換データのドキュメントを作成します。データはさまざまな非表示の <INPUT> 要素にあることに注意してください。\'83\'7d ネージャによって入力されたデータは太字で示しています。

```
<replacement-data>
  <item name="room-number">cubicle 1234</item>
  <item name="template">post_form.xml</item>
  <item name="response-template">post_response.xml</item>
  <item name="auth-template">auth_response.xml</item>
  <item name="association">45f0e3:ee45e07709:-
7fff:192.168.0.1</item>
  <item name="password" is-sensitive="true"><!-content
suppressed ?</item>
  <item name="protected-
data">rO0ABXNyABlqYXZheC5jcnlwdG8uU2VhbGVkT2JqZWN0PjY9psO3VHACA
ARbAA1lbmNvZGVkUGFyYW1zdAACW0JbABBlbmNyeXB0ZWRDb250ZW50cQB+AAFM
AAlwYXJhbXNBbGd0ABJMamF2YS9sYW5nL1N0cmluZztMAAdzZWFsQWxncQB+AAJ
4cHVyAAJbQqzzF/
gGCFTgAgAAeHAAAAAPMA0ECIr9Z1iG+O3BAgEKdXEAfgAEAAAAuMU/
SoFRkebvh2d5SqalF91ttjRY5lyyW5+/
FifOuDdYikYiDbOJb6607S0dPHjQzeVgu6ptIvGqaEQOEjBjDkY+i4VoVjUSXS3
a8fiXB8moMdPtLJ/
GyE8QiwbT4xbkQy48i02k99F2vGmlenRpSP6dD31kZl3dpJ0mGgq2yL/
eFaynKyqnjkHLMexcqD8WlVooaRl1k2RPk5vDYvC8o2bn22OKKbOnSRM5YlPS0i
Wzxo0JVcnVVyt0AANQQkV0ABBQQkVXaXRoTUQ1QW5kREVT</item>
  <item name="responder-dn">\PERIN-TAO\novell\Provo\phb</item>
  <item name="auth-style sheet">process_template.xsl</item>
  <item name="response-style sheet">process_template.xsl</item>
  <item name="subject-name">Joe the Intern</item>
  <item name="url-base">https://192.168.0.1:8180</item>
  <item name="url">https://192.168.0.1:8180</item>
</replacement-data>
```

e. Web サーバによって、responder-dn の項目の値が、保護されたデータに含まれている responder-dn 値に一致することが確認されます。値が一致しない場合、Web サーバは要求を中止します。値が一致した場合、処理が続行されます。

f. HTTP POST 要求を送信するユーザを認証するために、Web サーバによって、<check-object-password> XDS 要求が発行者チャネル上の Identity Manager に送信されます。

```
<nds dtdversion="1.0" ndsversion="8.6">
  <source>
    <product build="20020606_0824" instance="Manual Task
```

```
Service Driver" version="1.1a">DirXML Manual Task Service
Driver</product>
    <contact>Novell, Inc.</contact>
  </source>
  <input>
    <check-object-password dest-dn="\PERIN-
TAO\novell\Provo\phb" event-id="chkpwd">
      <password><!-- content suppressed --></password>
    </check-object-password>
  </input>
</nds>
```

g. Identity Manager によって、<status level=”success”> が返されます。Identity Manager によって成功以外が返された場合、データ項目 auth_template によって指定されたテンプレート、およびデータ項目 auth_stylesheet によって指定されたスタイルシートを使用して、POST の結果として返された Web ページが作成されます。

h. XDS ドキュメントを生成するために、Web サーバは、process_template.xsl スタイルシートを持つ post_form.xml テンプレートを処理します。置換トークンは太字で示しています。

```
<nds>
  <input>
    <modify class-name="User" src-dn="not-applicable" event-
id=”wfmod”>
      <association>$association$</association>
      <modify-attr attr-name="roomNumber">
        <remove-all-values/>
        <add-value>
          <value>$room-number$</value>
        </add-value>
      </modify-attr>
    </modify>
  </input>
</nds>
```

i. 発行者によって作成された XDS ドキュメントが Identity Manager に送信されます。

```
<nds>
  <input>
    <modify class-name="User" src-dn="not-applicable" event-
id=”wfmod”>
      <association>45f0e3:ee45e07709:-7fff:192.168.0.1</
association>
      <modify-attr attr-name="roomNumber">
        <remove-all-values/>
        <add-value>
          <value>cubicle 1234</value>
        </add-value>
      </modify-attr>
    </modify>
  </input>
</nds>
```

j. Identity Manager によって、結果ドキュメントが返されます。

```
<nds dtdversion="1.1" ndsversion="8.6">
  <source>
    <product version="2.0">Identity Manager</product>
    <contact>Novell, Inc.</contact>
  </source>
  <output>
    <status event-id="wfmod" level="success"></status>
  </output>
</nds>
```

k. Web サーバによって、置換データ項目 post-status (および置換データ項目 post-status-message) が置換データのドキュメントに追加されます。追加されたデータ項目は太字で示しています。

```
<replacement-data>
  <item name="room-number">cubicle 1234</item>
  <item name="template">post_form.xml</item>
  <item name="response-template">post_response.xml</item>
  <item name="auth-template">auth_response.xml</item>
  <item name="association">45f0e3:ee45e07709:-
7fff:192.168.0.1</item>
  <item name="password" is-sensitive=”true”><!-content
suppressed ?</item>
  <item name="protected-
data">rO0ABXNyABlqYXZheC5jcnlwdG8uU2VhbGVkT2JqZWN0PjY9psO3VHACA
ARbAA1lbmNvZGVkUGFyYW1zdAACW0JbABBlbmNyeXB0ZWRDb250ZW50cQB+AAFM
AAlwYXJhbXNBbGd0ABJMamF2YS9sYW5nL1N0cmluZztMAAdzZWFsQWxncQB+AAJ
4cHVyAAJbQqzzF/
gGCFTgAgAAeHAAAAAPMA0ECIr9Z1iG+O3BAgEKdXEAfgAEAAAAuMU/
SoFRkebvh2d5SqalF91ttjRY5lyyW5+/
FifOuDdYikYiDbOJb6607S0dPHjQzeVgu6ptIvGqaEQOEjBjDkY+i4VoVjUSXS3
a8fiXB8moMdPtLJ/
GyE8QiwbT4xbkQy48i02k99F2vGmlenRpSP6dD31kZl3dpJ0mGgq2yL/
eFaynKyqnjkHLMexcqD8WlVooaRl1k2RPk5vDYvC8o2bn22OKKbOnSRM5YlPS0i
Wzxo0JVcnVVyt0AANQQkV0ABBQQkVXaXRoTUQ1QW5kREVT</item>
  <item name="responder-dn">\PERIN-TAO\novell\Provo\phb</item>
  <item name="auth-style sheet">process_template.xsl</item>
  <item name="response-style sheet">process_template.xsl</item>
  <item name="subject-name">Joe the Intern</item>
  <item name="url-base">https://192.168.0.1:8180</item>
  <item name="url">https://192.168.0.1:8180</item>
  <status event-id="" level="success"></status>
  <item name="post-status">success</item>
</replacement-data>
```

l. Web サーバは、process_template.xsl スタイルシートを使用して post_response.xml テンプレートを処理します。置換トークンおよびアクション要素は太字で示しています。

```
<htm xmlns:form="http://www.novell.com/dirxml/manualtask/form">
  <head>
    <title>Result of post for $subject-name$</title>
  </head>
  <body>
    <link href="novdocmain.css" rel="style sheet" type="text/
css"/>
```

```
    <br/><br/><br/><br/>
    <table class="formtable" cellpadding="5" cellspacing="20"
border="1" align="center">
      <tr>
        <td>
          DirXML reported status = $post-status$
        </td>
      </tr>
<form:if-item-exists name="post-status-message">
      <tr>
        <td>
          Status message was: $post-status-message$
        </td>
      </tr>
</form:if-item-exists>
    </table>
  </body>
</html>
```

m. HTTP POST の結果として、結果の Web ページが返されます。置換データのドキュメントに <form:if-item-exists> 要素によって参照されている post-status-message がないため、\'95\'5c の 2 行目はありません。

```
<html>
  <head>
<META http-equiv="Content-Type" content="text/html;
charset=UTF-8">
    <title>Result of post for Joe the Intern</title>
  </head>
  <body>
    <link href="novdocmain.css" rel="style sheet" type="text/
css">
    <br><br><br><br>
    <table class="formtable" cellpadding="5" cellspacing="20"
border="1" align="center">
      <tr>
        <td>
          DirXML reported status = success
        </td>
      </tr>
    </table>
  </body>
</html>
```

手動タスクサービスドライバ : 購読者チャネル用のカスタム要素ハンドラ

ドライバは、SMTP (Simplified Mail Transport Protocol) 以外の方法を使用して、ユーザ通知を送信するための拡張メカニズムを提供します。たとえば、顧客が、SMTP を使用するのではなく、Messaging Application Programming Interface (MAPI) を使用して通知を送信する必要があるとします。

通知の送信に SMTP 以外のメカニズムを使用するには、ドライバの加入者チャネルで送信されるカスタム XML 要素を処理する Java クラスを記述する必要があります。

Java カスタム要素ハンドラは、com.novell.nds.dirxml.driver.manualtask.CommandHandler Java インタフェースを実装する必要があります。カスタム要素クラスの名前は、加入者の設定パラメータの Additional Handlers 項目で指定されます。

購読者チャネルでコマンド要素が発生した場合、ハンドラのテーブルが検索されます。コマンド要素を処理していることをレポートするハンドラが見つかると、コマンド要素がハンドラに渡されます。次にハンドラは必要な処理を実行します。

ドライバには、次の 2 つの組み込みコ \'83\'7d ンド要素のハンドラがあります。<mail> 要素のハンドラ、および <add> 要素のハンドラです。

カスタムコマンド要素は、カスタムハンドラの作成者が定義します。カスタムコ \'83\'7d ンド要素の設計の開始に適しているのは、<mail> 要素の設計です。

<mail> 要素が作成されたのを同じ方法で、加入者チャネルのポリシーによってカスタム要素が作成されます。

com.novell.nds.dirxml.driver.manualtask.CommandHandler のドキュメント、および多くのユーティリティとサポートクラスのドキュメントは、ドライバに付属の javadocs にあります。javadocs は、配布イメージのファイル名 manual_task_docs.zip にあります。

I.1 発行者チャネルの Web サーバと共に使用するための、URL の \'8d\'5c 成

ドライバの発行者チャネルの Web サーバを安全に使用するには、ユーティリティクラスを使用して、通知メッセージに含まれる URL を構成する必要があります。com.novell.nds.dirxml.driver.manualtask.URLData はこのタスクのために設計されています。

サンプルコードは、このプロセスを説明する SampleCommandHandler.java にあります。

I.2 スタイルシートおよびテンプレートドキュメントを使用したメッセージドキュメントの \'8d\'5c 成

SMTP ハンドラが使用するドキュメントを作成する際に、スタイルシート、テンプレートドキュメント、および置換データを組み合わせた、同じ方法を使用すると便利です。これ

を行うには、スタイルシートおよびテンプレートドキュメントを取得し、スタイルシートプロセッサをプログラム的に起動する必要があります。

サンプルコードは、このプロセスを説明する SampleCommandHandler.java にあります。

I.3 SampleCommandHandler.java

サンプルのカスタムコマンドハンドラのソースコードは、ドライバの配布パッケージに付属しています。ソースコードは、配布イメージ内の manual_task_docs.zip ファイルにあります。

ハンドラは、com.novell.nds.dirxml.driver.manualtask.samples.SampleCommandHandler クラスに実装されています。

サンプルのハンドラは、スタイルシートおよびテンプレートを使用してドキュメントを生成し、結果のドキュメントをファイルに書き込むだけです。

I.3.1 SampleCommandHandler クラスのコンパイル

任意の Java 2 コンパイラを使用して、SampleCommandHandler クラスをコンパイルできます。Java コンパイラのクラスパスに、nxsl.jar、dirxml.jar、collections.jar、および ManualTaskServiceBase.jar を配置する必要があります。

I.3.2 SampleCommandHandler クラスの試行

ドライバの部屋番号のサンプル設定のインポートから開始します。

SampleCommandHandler クラスをコンパイルし、結果のクラスファイルを .jar ファイルに配置します。ドライバを実行しているプラットフォームに適した、DirXML の .jar ファイルディレクトリに .jar ファイルを配置します。

ドライバプロパティの Driver Parameters XML セクションにある <subscriber-options> 要素の下に、次の XML 要素を追加します。

```
<output-path display-name="Sample Output Path"></output-path>
```

ドライバパラメータを編集します。Sample Output Path という名前の項目で、SampleCommandHandler により作成されたドキュメントが記述されるディレクトリのパスを指定します。Additional Handlers という名前の項目で、文字列「com.novell.nds.dirxml.driver.manualtask.samples.SampleCommandHandler」を追加します。

加入者チャネルの Command Transformation(コ \'83\'7d ンド変換) ポリシーを、SampleCommandHandler.jav ファイルと同じディレクトリにある CommandXform.xsl に置換します。

ユーザオブジェクトを作成し、マネージャ参照をユーザオブジェクトに追加します。\'83\'7d ネージャが電子メールアドレス値を持っている場合、<sample> コ \'83\'7d ンド要素が加入者に送信され、SampleCommandHandler によって上記で指定した場所のファイルが記述されます。

手動タスクサービスドライバ : 発行者チャネル用のカスタムサーブレット

J

ドライバには拡張メカニズムがあり、その他の機能を発行者チャネルの Web サーバに追加できます。Additional Servlets という名前のドライバ設定項目でサーブレットクラスの名前を指定することにより、発行者はカスタムサーブレットをロードできます。

J.1 発行者チャネルの使用

カスタムサーブレットで Identity Manager にデータを送信する必要がある場合、サーブレットはドライバの発行者チャネルを使用する必要があります。これを行うために、com.novell.nds.dirxml.driver.manualtask.ServletRegistrar および com.novell.nds.dirxml.driver.manualtask.PublisherData クラスが用意されています。サンプルコードは、このプロセスを説明する SampleServlet.java にあります。

J.2 Authentication

カスタムサーブレットは、情報を送信するユーザを認証する必要があります。サンプルコードは、このプロセスを説明する SampleServlet.java にあります。しかし、<check-object-password> 要素を使用して実行される認証のタイプでは、eDirectory™ の権利は確認されません。. ドライバオブジェクトが変更を実行する権利を持っている場合、変更を送信するユーザが権利を持っているかどうかにかかわらず、発行者チャネルで送信された変更は許可されます。

購読者チャネルのコマンドハンドラによって生成された URL を使用している場合、responder-dn データ項目が改ざんされていないことを確認するために、com.novell.nds.dirxml.driver.manualtask.URLData クラスを使用して URL を検証する必要があります。この実行の詳細については、javadocs を参照してください。

J.3 SampleServlet.java

サンプルのサーブレットのソースコードは、ドライバの配布パッケージに含まれています。ソースコードは、配布イメージ内の manualtask_driver_docs.zip ファイルにあります。

サーブレットは、com.novell.nds.dirxml.driver.manualtask.samples.SampleServlet クラスに実装されています。

サンプルのサーブレットは、.sample で終了するすべてのリソースに対する HTTP GET 要求を受諾します。HTTP URL のクエリ文字列には、dest-dn 項目、attr-name 項目、および value 項目が含まれている必要があります。

サーブレットはユーザを認証し、ドライバの発行者チャネルを経由して変更要求を Identity Manager に送信します。

J.3.1 SampleServlet クラスのコンパイル

任意の Java 2 コンパイラを使用して、SampleServlet クラスをコンパイルできます。Java コンパイラのクラスパスに、nxsl.jar、dirxml.jar、collections.jar、および ManualTaskServiceBase.jar を配置する必要があります。

J.3.2 SampleServlet クラスの試行

ドライバの部屋番号のサンプル設定のインポートから開始します。

SampleServlet クラスをコンパイルし、結果のクラスファイルを .jar ファイルに配置します。ドライバを実行しているプラットフォームに適した、DirXML の .jar ファイルディレクトリに .jar ファイルを配置します。

ドライバパラメータを編集します。Additional Servlets という名前の項目で、文字列「com.novell.nds.dirxml.driver.manualtask.samples.SampleServlet」を追加します。

発行者チャネルフィルタへの電話番号の追加

次の URL をブラウザで送信します (ブラウザはドライバと同じ \'83\'7d シンで実行されていると想定します)。

https:localhost:8180/1.sample?dest-dn=username.container&attr-name=Telephone%20Number&value=555-1212

username.container *をツリーのユーザの DN に置換します。*