

Novell Identity Manager

3.0

2005年12月8日

IDENTITY MANAGER ユーザアプリケーション：管理ガイド

www.novell.com



Novell®

保証と著作権

米国 Novell, Inc. およびノベル株式会社は、本書の内容または本書に起因する結果に関して、いかなる表示も行いません。また、本書の商品性、および特定用途への適合性について、いかなる黙示の保証も行いません。米国 Novell, Inc. およびノベル株式会社は、本書の内容を改訂または変更する権利を常に留保します。米国 Novell, Inc. およびノベル株式会社は、このような改訂または変更を個人または事業体に通知する義務を負いません。

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使用に起因する結果に関して、いかなる表示も行いません。また、商品性、および特定目的への適合性について、いかなる黙示の保証も行いません。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。米国 Novell, Inc. およびノベル株式会社は、このような変更を個人または事業体に通知する義務を負いません。

本契約の締結に基づいて提供されるすべての製品または技術情報には、米国の輸出管理規定およびその他の国の貿易関連法規が適用されます。お客様は、取引対象製品の輸出、再輸出または輸入に関し、国内外の輸出管理規定に従うこと、および必要な許可、または分類に従うものとします。お客様は、現在の米国の輸出除外リストに記載されている企業、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。本ソフトウェアの輸出については、www.novell.co.jp/info/exports/expmtx.html または www.novell.com/ja-jp/company/exports/ もあわせてご参照ください。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對し如何なる責任も負わないものとします。

Copyright © 1997, 1998, 1999, 2000, 2001, 2002, 2003, 2004-2005 Novell, Inc. All rights reserved. 本書の一部または全体を無断で複製、写真複写、検索システムへの登録、転載することは、その形態を問わず禁止します。

米国 Novell, Inc. は、本ドキュメントで説明されている製品に組み込まれた技術に関する知的財産権を有します。これらの知的財産権は、<http://www.novell.com/company/legal/patents/> に記載されている 1 つ以上の米国特許、および米国ならびにその他の国における 1 つ以上の特許または出願中の特許を含む場合があります。

本ソフトウェアとそのドキュメントに対する権利、特許、著作権、およびそれに対して適用可能なその他すべての財産権は、あらゆる場合において、単独でおよび独占的に Novell とそのライセンス許諾者に留まるものであり、ユーザはこのような権利に矛盾する行為を一切取らないものとします。本ソフトウェアは著作権法および国際条約の条項によって保護されています。ユーザは、本ソフトウェアまたはそのドキュメントから著作権表示またはその他の登録商標権の表示を取り除かないものとし、本ソフトウェアまたはそのドキュメントのコピーあるいは抽出物すべての当該の表示を複製する必要があります。ユーザは本ソフトウェアの所有権を取得することにはなりません。

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 製品のオンラインマニュアル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/ja-jp/documentation をご覧ください。

Novell の商標

Novell は、米国 Novell, Inc. の米国およびその他の国々における登録商標です。

SUSE は、米国 Novell, Inc. の米国およびその他の国々における登録商標です。

第三者の商標

第三者の商標は、それぞれの所有者に属します。

第三者の保証と著作権

Apache ソフトウェアライセンス バージョン 1.1

Copyright © 2000 The Apache Software Foundation. All rights reserved.

ソースおよびバイナリの形式における再配布および使用は、変更の有無にかかわらず、次の条件を満たした場合に許可されます。

1. ソースコードの再配布では、上記の著作権表示、本諸条件リスト、および次の免責事項を保持する必要があります。
2. バイナリ形式での再配布では、そのドキュメントまたは配布に付属する他の資料、あるいはその両方に、上記の著作権表示、本諸条件リスト、および次の免責事項を複製する必要があります。
3. 配布に付属するエンドユーザードキュメントがある場合は、次の謝辞を含める必要があります。「本製品には Apache Software Foundation (<http://www.apache.org/>) によって開発されたソフトウェアが含まれています。」

本謝辞はソフトウェア自身に表示することもでき、通常サードパーティの謝辞が表示される場所であればどこにでも表示できます。

4. 書面による事前の許可なしに、「Apache」および「Apache Software Foundation」という名称を、本ソフトウェアから派生した製品の保証または販売促進のために使用してはなりません。書面による許可については、apache@apache.org までお問い合わせください。
5. Apache Software Foundation の書面による事前の許可なしに、本製品から派生した製品を「Apache」と呼んだり、製品名に「Apache」と記載したりすることはできません。

本ソフトウェアは「現状のまま」提供されるものであり、販売可能性に関する保証の黙示的保証を含む明示的または黙示的保証、および特定の用途に対する適合性はすべて放棄されます。いかなる場合においても、APACHE SOFTWARE FOUNDATION またはその貢献者は、直接的、間接的、付随的、特殊、例示的、または結果的な損害（代替商品またはサービスの調達、使用不能、データの紛失、または利益の逸失、あるいは事業の中断を含むが、これらに限定されない）に対して、契約行為、厳格責任、不法行為（不注意または別の方法を含む）を含め、責任の理論にかかわらず、たとえかかる損害の発生の可能性を知らされていた場合であっても、一切責任を負いません。

Autonomy

Copyright ©1996-2000 Autonomy, Inc.

Bouncy Castle

License Copyright © 2000 - 2004 The Legion Of The Bouncy Castle (<http://www.bouncycastle.org>)

本ソフトウェアのコピーおよび関連ドキュメントファイル（「本ソフトウェア」）を入手した任意の人物に対し、本ソフトウェアの使用、コピー、変更、マージ、公開、配布、サブライセンス、または販売、あるいはこれらすべてを行う権利を制限することなく、ここに、制限なしに本ソフトウェアを扱う許可を無償で与え、当該目的で本ソフトウェアが提供された人物に対し、次の条件に従って、許可を与えます。

本ソフトウェアのすべてのコピーまたは大部分に上記の著作権表示と本許可の表示を含める必要があります。

本ソフトウェアは、明示的または黙示的を問わず、販売可能性に関する保証、特定の用途に対する適合性、および権利侵害を含むがこれらに限定されないいかなる保証もなしに、「現状のまま」提供されるものです。いかなる場合においても、著者または著作権保持者は、主張、損害、またはその他の責任に対し、本ソフトウェアの使用または本ソフトウェアとの関連、あるいは本ソフトウェアを他の方法で扱ったことから生じる契約の訴訟、不法行為、またはその他においても、一切責任を負いません。

Castor Library

オリジナルのライセンスは、<http://www.castor.org/license.html> に掲載されています。

本プロジェクトのコードは、BSD と同様のライセンス「license.txt」に従ってリリースされています。

Copyright 1999-2004 © Intalio Inc., and others. All rights reserved.

このソフトウェアおよび関連ドキュメント（「本ソフトウェア」）の再配布および使用は、変更の有無にかかわらず、次の条件を満たした場合に許可されます。

1. ソフトウェアコードの再配布では、著作権の記述および表示を保持する必要があります。再配布においても、本ドキュメントのコピーを含める必要があります。
2. バイナリ形式での再配布では、そのドキュメントまたは配布に付属する他の資料、あるいはその両方に、上記の著作権表示、本諸条件リスト、および次の免責事項を複製する必要があります。
3. Intalio Inc. の書面による事前の許可なしに、「ExoLab」という名称を、本ソフトウェアから派生した製品の保証または販売促進のために使用してはなりません。書面による許可については、info@exolab.org までお問い合わせください。
4. Intalio Inc. の書面による事前の許可なしに、本ソフトウェアから派生した製品を「Castor」と呼んだり、ソフトウェアの名称に「Castor」と記載したりすることはできません。Exolab、Castor、および Intalio は Intalio Inc. の商標です。
5. ExoLab に対する当然の賞賛は、プロジェクト (<http://www.exolab.org/>) に与えてください。

本ソフトウェアは INTALIO および貢献者によって「現状のまま」提供されるものであり、販売可能性に関する保証の黙示的保証を含む明示的または黙示的保証、および特定の用途に対する適合性はすべて放棄されます。いかなる場合においても、INTALIO またはその貢献者は、直接的、間接的、付随的、特殊的、例示的、または結果的な損害（代替商品またはサービスの調達、使用不能、データの紛失、または利益の逸失、あるいは事業の中断を含むが、これらに限定されない）に対して、契約行為、厳格責任、不法行為（不注意または別の方法を含む）を含め、責任の理論にかかわらず、たとえかかる損害の発生の可能性を知らされていた場合であっても、一切責任を負いません。

Indiana University Extreme!Lab ソフトウェアライセンス

Version 1.1.1

Copyright © 2002 Extreme!Lab, Indiana University. All rights reserved.

ソースおよびバイナリの形式における再配布および使用は、変更の有無にかかわらず、次の条件を満たした場合に許可されます。

1. ソースコードの再配布では、上記の著作権表示、本諸条件リスト、および次の免責事項を保持する必要があります。
2. バイナリ形式での再配布では、そのドキュメントまたは配布に付属する他の資料、あるいはその両方に、上記の著作権表示、本諸条件リスト、および次の免責事項を複製する必要があります。
3. 配布に付属するエンドユーザドキュメントがある場合は、次の謝辞を含める必要があります。「本製品には Indiana University Extreme!Lab (<http://www.extreme.indiana.edu/>) によって開発された製品が含まれています。」

本謝辞はソフトウェア自身に表示することもでき、通常サードパーティの謝辞が表示される場所であればどこにでも表示できます。

4. 書面による事前の許可なしに、「Indiana University」および「Indiana University Extreme!Lab」という名称を、本ソフトウェアから派生した製品の保証または販売促進のために使用してはなりません。書面による許可については、<http://www.extreme.indiana.edu/> までお問い合わせください。
5. Indiana University の書面による事前の許可なしに、本製品から派生した製品で「Indiana University」という名称を使用したり、製品名に「Indiana University」と記載したりすることはできません。

本ソフトウェアは「現状のまま」提供されるものであり、販売可能性に関する保証の黙示的保証を含む明示的または黙示的保証、および特定の用途に対する適合性はすべて放棄されます。いかなる場合においても、作者またはその貢献者は、直接的、間接的、付随的、特殊的、例示的、または結果的な損害（代替商品またはサービスの調達、使用不能、データの紛失、または利益の逸失、あるいは事業の中断を含むが、これらに限定されない）に対して、契約行為、厳格責任、不法行為（不注意または別の方法を含む）を含め、責任の理論にかかわらず、たとえかかる損害の発生の可能性を知らされていた場合であっても、一切責任を負いません。

JDOM.JAR

Copyright © 2000-2002 Brett McLaughlin & Jason Hunter. All rights reserved.

ソースおよびバイナリの形式における再配布および使用は、変更の有無にかかわらず、次の条件を満たした場合に許可されます。

1. ソースコードの再配布は、上記の著作権表示、本諸条件リスト、および次の免責事項を保持する必要があります。
2. バイナリ形式での再配布では、そのドキュメントまたは配布に付属する他の資料、あるいはその両方に、上記の著作権表示、本諸条件リスト、およびこれらの条件に従った免責事項を複製する必要があります。
3. 「JDOM」という名称を、本ソフトウェアから派生した製品の保証または販売促進のために使用してはなりません。書面による許可については、license@jdom.org までお問い合わせください。
4. JDOM Project Management (pm@jdom.org) の書面による事前の許可なしに、本製品から派生した製品を「JDOM」と呼んだり、製品名に「JDOM」と記載したりすることはできません。

さらに、再配布に付属するエンドユーザドキュメント、またはソフトウェア自体の中、あるいはその両方に、次と同等の謝辞を含めることも要求します(ただし必須ではありません)。「本製品には JDOM Project (<http://www.jdom.org/>) によって開発されたソフトウェアが含まれています。」

または、<http://www.jdom.org/images/logos> で入手可能なロゴを使用して、この謝辞に図を使用することもできます。

本ソフトウェアは「現状のまま」提供されるものであり、販売可能性に関する保証の黙示的保証を含む明示的または黙示的保証、および特定の用途に対する適合性はすべて放棄されます。いかなる場合においても、JDOM の作者またはプロジェクトへの貢献者は、直接的、間接的、付随的、特殊的、例示的、または結果的な損害(代替商品またはサービスの調達、使用不能、データの紛失、または利益の逸失、あるいは事業の中断を含むが、これらに限定されない)に対して、契約行為、厳格責任、不法行為(不注意または別の方法を含む)を含め、責任の理論にかかわらず、たとえかかる損害の発生の可能性を知らされていた場合であっても、一切責任を負いません。

Phaos

本ソフトウェアは、部分的に SSLava™ Toolkit (Copyright ©1996-1998 by Phaos Technology Corporation) から派生しています。All rights reserved. 顧客が Phaos ソフトウェアの機能にアクセスすることは禁じられています。

W3C

W3C® ソフトウェア表示およびライセンス

本作業物(および含まれるソフトウェア、README などのドキュメント、または他の関連する品目)は、次のライセンスに従って著作権保持者によって提供されています。本作業物の入手、使用またはコピー、あるいはその両方を行うことにより、ユーザ(使用者)は、次の条件を読んで理解し、それらに従うことに同意します。

このソフトウェアとそのドキュメントのコピー、変更、および配布の許可は、変更の有無にかかわらず、いかなる目的でも無償で与えられます。この場合、ソフトウェアおよびドキュメント、あるいはその一部(変更を含む)のすべてのコピーに、以下の内容を記載するものとします。

1. この通知の全文。再配布された作業物または派生作業物のユーザに見える場所に記載します。
2. 既存の知的財産権の免責事項、通知、または条件すべて。これらがまったく存在しない場合、再配布または派生したコードの本文内に、W3C の Software Short Notice を含める必要があります(ハイパーテキストを推奨、テキストも可)。
3. 変更が行われた日付を含む、ファイルに対する変更または改変内容の表示(コードが派生している場所への URI を提供することをお勧めします)。

本ソフトウェアおよびドキュメントは「現状のまま」提供されるもので、著作権保持者は、販売可能性に関する保証または特定の用途に対する適合性、あるいは本ソフトウェアまたはドキュメントの使用によって、サードパーティの特許、著作権、商標などの権利を侵害しないことを含むが、これらに限定されない表示または保証を、明示的または黙示的を問わず、一切行いません。

著作権保持者は、本ソフトウェアまたはドキュメントの使用から生じる直接的、間接的、特殊、または結果的な損害に対して一切責任を負いません。

具体的な書面による事前の許可なしに、著作権保持者の名称および商標を、本ソフトウェアに関する広告または広報に使用することはできません。本ソフトウェアおよび関連ドキュメントの著作権に対する権利は、常に著作権保持者に帰します。

目次

本書について	9
ページのパート I 概要	11
1 概要	13
1.1 サポートされている役割のタイプ	15
1.1.1 LDAP 管理者	16
1.1.2 ユーザアプリケーション管理者	16
1.1.3 エンドユーザ	17
1.1.4 委任ユーザ	18
1.1.5 プロキシユーザ	19
1.2 データの抽象化：柔軟な識別情報管理のための重要な概念	20
1.3 高レベルアーキテクチャ概要	21
1.3.1 アイデンティティポータル	22
1.3.2 JBoss	23
1.3.3 データベース	23
1.3.4 Identity Manager エンジン	24
1.3.5 ユーザアプリケーションドライバ	24
1.3.6 ディレクトリ抽象化レイヤ	26
1.3.7 ワークフローエンジン	26
1.3.8 ユーザインタフェース	27
1.4 設計および設定用ツール	27
1.5 ユーザアプリケーション使用シナリオ	28
1.5.1 シナリオ A: ユーザが同じ組織内の別の人物の情報を検索する	29
1.5.2 シナリオ B: マネージャが新しいユーザを作成する	30
1.5.3 シナリオ C: ユーザのプロビジョニング	33
1.6 次のステップ	35
2 運用環境の設計	37
2.1 トポロジ	37
2.1.1 最小設計	37
2.1.2 高可用性の設計	38
2.1.3 設計上の制約	39
2.2 セキュリティ	40
2.2.1 相互認証	42
2.3 パフォーマンスの調整	42
2.3.1 ログ	42
2.3.2 アイデンティティポータル	43
2.3.3 JVM	44
2.3.4 セッションタイムアウト値	44
2.4 クラスタリング	45
2.4.1 JBoss のクラスタリング	45
2.4.2 JBoss クラスタへのユーザアプリケーションのインストール	48
2.4.3 ユーザアプリケーションクラスタグループのキャッシング設定	51
2.4.4 クラスタリング用のワークフローの設定	51

ページのパート II ユーザアプリケーション環境の設定	53
-----------------------------	----

3 ユーザアプリケーションドライバの設定	55
-----------------------------	-----------

3.1 ユーザアプリケーションドライバについて	55
3.2 ユーザアプリケーションドライバの作成	56
3.3 ユーザアプリケーションドライバの起動	62
3.4 ワークフローの自動起動の設定	63
3.4.1 ポリシーについて	63
3.4.2 アイデンティティポータル内のイベントに基づいて起動されるワークフローの設定	64

4 ディレクトリ抽出化レイヤの設定	75
--------------------------	-----------

4.1 ディレクトリ抽出化レイヤ定義について	75
4.2 はじめに	76
4.2.1 ユーザアプリケーションドライバの設定	77
4.2.2 プロビジョニングビューへのアクセス	81
4.2.3 ディレクトリ抽出化レイヤエディタの起動	82
4.3 エンティティおよび属性の操作	87
4.3.1 エンティティを追加する手順	87
4.3.2 データに必要な内容の分析	87
4.3.3 エンティティの定義	88
4.4 リストの操作	104
4.4.1 優先ロケールリストについて	106
4.4.2 プロビジョニングカテゴリリストについて	106
4.5 組織図の関係の操作	106
4.5.1 関係のプロパティのリファレンス	108
4.6 環境設定の操作	109
4.7 表示テキストのローカライズ	110
4.7.1 サポートされている言語	110
4.7.2 テキストのローカライズ	111
4.8 ディレクトリ抽出化レイヤ定義のインポート、検証、および展開	111
4.8.1 インポートについて	111
4.8.2 検証について	114
4.8.3 展開について	114

5 ログの設定	119
----------------	------------

5.1 イベントログについて	119
5.1.1 ログレベル設定について	119
5.2 Novell Audit サーバへのログ	119
5.2.1 ログアプリケーションとしての Identity Manager アプリケーションスキーマの Novell Audit サーバへの追加	120
5.2.2 Novell Audit のログの有効化	121
5.2.3 ログ対象イベントの種類	122
5.2.4 ログレポート	124

ページのパート III ユーザアプリケーションの管理	129
----------------------------	-----

6 [管理] タブの使用	131
---------------------	------------

6.1 [管理] タブについて	131
6.2 [管理] タブを使用できるユーザ	131
6.3 [管理] タブへのアクセス	132

6.4	実行できる管理アクション	135
7	ページの管理	137
7.1	ページの管理について	137
7.1.1	コンテナページについて	137
7.1.2	共有ページについて	143
7.1.3	ページの使用に関する例外	144
7.2	コンテナページの作成とメンテナンス	144
7.2.1	コンテナページの作成	145
7.2.2	コンテナページへのコンテンツの追加	148
7.2.3	コンテナページからコンテンツを削除する	149
7.2.4	コンテナページのレイアウトを変更する	150
7.2.5	コンテナページにコンテンツを配置する	151
7.2.6	コンテナページの表示	153
7.3	共有ページの作成とメンテナンス	153
7.3.1	共有ページの作成	154
7.3.2	共有ページにコンテンツを追加する	158
7.3.3	共有ページからコンテンツを削除する	159
7.3.4	共有ページのレイアウトを変更する	160
7.3.5	共有ページにコンテンツを配置する	161
7.3.6	共有ページの表示	163
7.4	ページの許可を割り当てる	163
7.4.1	ページに表示許可を割り当てる	164
7.4.2	共有ページに所有者を割り当てる	167
7.4.3	[ユーザまたはグループの作成] ページへのユーザアクセスを有効にする	168
7.4.4	個々の [管理] ページへのユーザアクセスを有効にする	169
7.5	グループのデフォルトページを設定する	170
7.6	コンテナページのデフォルト共有ページを選択する	172
8	テーマの環境設定	175
8.1	テーマの環境設定について	175
8.2	テーマのプレビュー	176
8.3	テーマの選択	177
8.4	テーマのブランディングのカスタマイズ	178
9	ポートレットの管理	181
9.1	ポートレットの管理について	181
9.2	ポートレットアプリケーションの管理	182
9.2.1	サーバ上のポートレットアプリケーションにアクセスする	182
9.2.2	ポートレットアプリケーションの情報を表示する	183
9.2.3	ポートレットアプリケーションの登録を取り消す	184
9.3	ポートレット定義を管理する	185
9.3.1	展開されたポートレットアプリケーションのポートレット定義にアクセスする	185
9.3.2	ポートレット定義を登録する	186
9.3.3	ポートレット定義の情報を表示する	187
9.4	登録されたポートレットを管理する	190
9.4.1	展開されたポートレットアプリケーションでポートレット登録にアクセスする	190
9.4.2	ポートレット登録の情報を表示するには	191
9.4.3	ポートレット登録にカテゴリを割り当てる	192
9.4.4	ポートレット登録の設定を変更する	193
9.4.5	ポートレット登録の初期設定を変更する	196
9.4.6	ポートレット登録のセキュリティ許可を割り当てる	197
9.4.7	ポートレットの登録を取り消す	200

10	ポータル環境設定	201
10.1	ポータル環境設定について	201
10.2	一般設定	201
10.2.1	変更可能な設定	202
10.2.2	読み込み専用の設定	204
10.3	LDAP 接続パラメータ	204
10.3.1	変更可能な設定	205
10.3.2	読み込み専用の設定	206
11	セキュリティ環境設定	209
11.1	セキュリティ環境設定について	209
11.2	ユーザアプリケーション管理者を割り当てる	210
12	ログ環境設定	213
12.1	ログ環境設定について	213
12.2	ログについて	213
12.3	ログレベルの変更	216
12.4	Novell Audit へのログメッセージの送信	217
12.5	ログ設定の持続	217
13	キャッシング環境設定	219
13.1	キャッシング環境設定について	219
13.2	キャッシュのフラッシュ	219
13.2.1	ディレクトリ抽象化レイヤキャッシュのフラッシュ	221
13.2.2	クラスタ内のキャッシュのフラッシュ	221
13.3	キャッシュを設定する	221
13.3.1	キャッシングの実装について	222
13.3.2	キャッシュ設定の保存について	222
13.3.3	キャッシュ設定の表示について	224
13.3.4	基本キャッシュ設定	224
13.3.5	クラスタのキャッシュ設定	226
14	ポータルデータのエクスポートおよびインポートのためのツール	229
14.1	ポータルデータのエクスポートおよびインポートについて	229
14.1.1	用途	229
14.1.2	要件	230
14.1.3	制限	230
14.1.4	手順	230
14.2	ポータルデータのエクスポート	231
14.3	ポータルデータのインポート	232
	ページのパート IV ポートレット参照	237
15	ポートレットについて	239
15.1	アクセサリポートレット	239
15.2	管理ポートレット	239
15.2.1	共有ページナビゲーションポートレット	240
15.3	識別ポートレット	240
15.4	パスワードポートレット	241

15.5	システムポートレット	241
16	作成ポートレットの参照先	243
16.1	作成ポートレットについて	243
16.2	作成ポートレットの設定	245
16.2.1	ディレクトリ抽象化レイヤの設定	246
16.3	作成の初期設定の設定	247
17	詳細ポートレットの参照	251
17.1	詳細ポートレットについて	251
17.1.1	エンティティデータの表示	252
17.1.2	エンティティデータの編集	255
17.1.3	エンティティデータの電子メール送信	258
17.1.4	組織図へのリンク	258
17.1.5	他のエンティティの詳細情報へのリンク	258
17.1.6	エンティティデータの印刷	259
17.2	前提条件	259
17.2.1	ディレクトリ抽出化レイヤの設定	260
17.2.2	エンティティに権利を割り当てる	260
17.3	他のポートレットからの詳細ポートレットの起動	260
17.3.1	リスト検索ポートレットからの起動	261
17.3.2	組織図ポートレットからの起動	261
17.4	ページからの詳細ポートレットの使用	262
17.5	初期設定	262
17.5.1	初期設定について	263
18	組織図ポートレットの参照	265
18.1	組織図について	265
18.1.1	組織図の関係について	266
18.1.2	組織図の表示について	267
18.2	組織図ポートレットの設定	267
18.2.1	ディレクトリ抽象化レイヤの設定	268
18.2.2	組織図の初期設定	268
18.2.3	イメージの動的なロード	278
19	パスワード管理ポートレットの参照	281
19.1	パスワードを管理するための準備作業	281
19.1.1	パスワード管理機能について	281
19.1.2	eDirectory で必要な設定	281
19.2	パスワードポートレットについて	284
19.2.1	パスワードセルフサービスポートレットのモード	284
19.3	「IDM ログイン」ポートレット	285
19.3.1	要件	285
19.3.2	用途	286
19.4	「IDM 本人確認の回答」ポートレット	286
19.4.1	要件	287
19.4.2	用途	287
19.5	「IDM ヒントの設定」ポートレット	288
19.5.1	要件	288
19.5.2	用途	288
19.6	「IDM パスワードの変更」ポートレット	289

19.6.1	要件	289
19.6.2	用途	290
19.7	「IDM パスワードを忘れた場合」ポートレット	291
19.7.1	要件	291
19.7.2	用途	292
20	リスト検索ポートレットの参照	295
20.1	リスト検索ポートレットについて	295
20.1.1	結果リストの表示形式について	298
20.2	リスト検索ポートレットの設定	300
20.2.1	ディレクトリ抽象化レイヤの設定	301
20.2.2	リスト検索の初期設定	302
	ページのパート V プロビジョニング要求の設計と管理	309
21	ワークフローベースプロビジョニングの概要	311
21.1	ワークフローベースのプロビジョニングについて	311
21.1.1	上位レベルのアーキテクチャ	312
21.1.2	プロビジョニングおよびワークフローの例	315
21.2	プロビジョニングの設定および管理	321
21.3	プロビジョニングのセキュリティ	321
22	プロビジョニング要求定義の設定	325
22.1	プロビジョニング要求の環境設定プラグインについて	325
22.2	インストールされているテンプレートでの作業	326
22.3	プロビジョニング要求定義の設定	329
22.3.1	ドライバの選択	329
22.3.2	プロビジョニング要求の作成または編集	330
22.3.3	プロビジョニング要求の削除	343
22.3.4	既存のプロビジョニング要求のステータスの変更	344
22.3.5	既存のプロビジョニング要求の権利の定義	345
23	プロビジョニングワークフローの管理	347
23.1	ワークフロー管理プラグインについて	347
23.2	ワークフローの管理	348
23.2.1	ワークフローサーバへの接続	348
23.2.2	検索条件に合致するワークフローの検索	351
23.2.3	アクティブなワークフローの表示の制御	353
23.2.4	ワークフローインスタンスの終了	354
23.2.5	ワークフローインスタンスの詳細の表示	354
23.2.6	ワークフローインスタンスの再割り当て	355
23.3	電子メールサーバの設定	356
23.4	インストールされている電子メールテンプレートでの作業	357
23.4.1	デフォルトのコンテンツおよび形式	358
23.4.2	テンプレートの編集	358
23.4.3	テンプレートのデフォルト値の変更	360

ページのパート VI 付録	363
A スキーマ拡張	365
A.1 属性のスキーマ拡張	365
A.2 Objectclass のスキーマ拡張	367
A.3 LDIF の表現	369
B アプリケーションアーカイブの設定	379
B.1 ユーザアプリケーション WAR について	379
B.2 セッションタイムアウトの設定	379

本書について

目的

本書では、次の機能を含む、Novell Identity Manager ユーザアプリケーションの管理方法について説明します。

- ◆ Identity Manager の識別セルフサービス機能
- ◆ ワークフローベースのプロビジョニング機能 (Identity Manager のプロビジョニングモジュールを追加した場合)

Identity Manager に含まれる他の機能の管理 (すべてのパッケージに共通) については、『Novell Identity Manager: 管理ガイド』を参照してください。

対象読者

本書は、Identity Manager ユーザアプリケーションの識別セルフサービス機能、またはワークフローベースのプロビジョニング機能の設定、展開、および管理を担当するシステム管理者、設計者、およびコンサルタントを対象としています。

これらの機能についてのエンドユーザ用のドキュメントは、『Identity Manager ユーザアプリケーション: ユーザーズガイド』として提供されています。

前提条件

本書では次のことが前提となっています。

- ◆ Identity Manager (および、必要に応じて Identity Manager のプロビジョニングモジュール) をインストールしていること

これらの製品のインストール方法については、『Novell Identity Manager: インストールガイド』を参照してください。

- ◆ Identity Manager の他の機能が適宜設定済みであること

『Novell Identity Manager: 管理ガイド』を参照してください。

このマニュアルの内容

次に、本書に記載されている内容の概要を示します。

パート	説明
11 ページのパート I 「概要」	Identity Manager ユーザアプリケーションについて説明し、組織におけるユーザアプリケーションの利用についてその計画立案を支援します。

パート	説明
53 ページのパート II 「ユーザアプリケーション環境の設定」	組織のニーズに合うように、Identity Manager ユーザアプリケーション環境のさまざまな側面 (ユーザアプリケーションドライバ、ディレクトリ抽象化レイヤ、およびログなど) を設定する方法について説明します。
129 ページのパート III 「ユーザアプリケーションの管理」	ユーザインタフェースの [管理] タブを使用して、Identity Manager ユーザアプリケーションを設定および管理する方法について説明します。
237 ページのパート IV 「ポートレット参照」	Identity Manager ユーザインタフェースで使用される識別情報およびシステムポートレットを設定する方法について説明します。
309 ページのパート V 「プロビジョニング要求の設計と管理」	Identity Manager のプロビジョニングモジュールを使ったプロビジョニングに必要なリソース、ワークフロー、および要求定義を設定、展開、および管理する方法について説明します。
	注：このパートの内容は、Identity Manager のプロビジョニングモジュールをインストールしている場合にのみ当てはまります。
363 ページのパート VI 「付録」	Identity Manager ユーザアプリケーションに関する追加の参照情報 (スキーマ拡張) とその他高度なトピック (アプリケーションアーカイブの設定) について説明します。

参照

その他の関連マニュアルおよび readme 情報については、Novell ドキュメントサイトの [Identity Manager のページ \(http://www.novell.com/idm/\)](http://www.novell.com/idm/) を参照してください。

概要

次の章では、Identity Manager ユーザアプリケーションについて説明し、組織におけるユーザアプリケーションの利用法についてその計画立案を支援します。

- ◆ 13 ページの第 1 章「概要」
- ◆ 37 ページの第 2 章「運用環境の設計」

概要

1

Novell Identity Manager ユーザアプリケーションは、洗練された識別サービスフレームワークに基づき、直感的で高度な設定や管理が行える、多機能で強力な Web アプリケーションです。Identity Manager のプロビジョニングモジュールと Novell Audit を併用することにより、Identity Manager ユーザアプリケーションは、安全でスケーラブル、そして管理が容易な総合的なエンドツーエンドのプロビジョニングソリューションになります。

このユーザアプリケーションには Web ベースの次のエンドユーザ機能が備わっています。

- ◆ 個人別電話帳
- ◆ 組織図
- ◆ ユーザの検索 (カスタム検索設定を保存可能)
- ◆ セルフサービスのパスワード管理
- ◆ 簡易なユーザ管理ツール
- ◆ ワークフローの開始と監視 (プロビジョニングモジュールがインストールされている場合)
- ◆ 個人およびチームのタスク管理 (プロビジョニングモジュールがインストールされている場合)
- ◆ 委任機能とプロキシ機能

システム管理者用の機能としては、ユーザアプリケーションには、次の設定機能および管理機能が備わっています。

- ◆ プロキシおよび委任の権利を設定し管理するためのインタフェース
- ◆ ログツールおよびカスタマイズした Crystal Report へのアクセス
- ◆ ウィザードベースのワークフロー設定 (プロビジョニングモジュールがインストールされている場合)
- ◆ 進行中のワークフローを再割り当てしたり終了したりできるワークフロー管理 (プロビジョニングモジュールがインストールされている場合)
- ◆ カスタムディレクトリの抽象化定義や関係を作成できる Eclipse ベースの Designer アプリケーション

次の表で、各機能についてさらに詳しく説明します。

機能	説明
標準ベース、ブラウザに依存しない、拡張可能な Web UI ユーザ環境	管理者は、ページレイアウトやデフォルト (ホーム) ページの変更、新しいページの追加、全体的な外観 (テーマ) の変更などを行えます。 JSR-168 準拠のポートレットを追加することで、ユーザアプリケーションを拡張できます。

機能	説明
プロビジョニングワークフロー (プロビジョニングモジュールがインストールされている場合)	管理者は、プロビジョニング要求を処理する独自のワークフローを作成できます。 作成したワークフローは、適切な権利を持つエンドユーザによって開始できます。
イベント駆動型ワークフロー (プロビジョニングモジュールがインストールされている場合)	ユーザが開始するワークフローに加えて、管理者は指定したイベントがアイデンティティポータルで発生した場合に、ワークフローが自動起動されるように設定できます。
拡張個人別電話帳	ユーザ情報をアルファベット順、地域別、スキルセット別などで表示できます。
組織図	ユーザアプリケーションには AJAX を利用した高度な組織図作成ポートレットが含まれており、豊富な機能をインタラクティブに利用できます。
ユーザの検索	ユーザは識別情報を検索したり、後で再利用できるようカスタム検索定義を保存したりできます。
パスワードセルフサービス	ユーザアプリケーションでは、エンドユーザがパスワード管理機能にアクセスでき、ヘルプデスクへの問い合わせ回数を軽減できます。
軽量なユーザ管理	ユーザアプリケーションでは、IT 管理者ではないエンドユーザでも、識別情報を制限内で管理できます。
Eclipse ベースの Designer	Designer アプリケーションを使用することにより、システム管理者、開発者、コンサルタント、および他の IT 専門家は、さまざまな設定やその他の操作をすばやく簡単に実行できます。たとえば、 Designer では、エンティティの定義や関係、ドライバポリシーやフィルタ、およびさまざまなドライバやドライバセットの設定作業をオフラインで実行できます。変更はプロジェクトに保存することも、アイデンティティポータルにアップロードすることもできます。
プロキシ役割 (プロビジョニングモジュールがインストールされている場合)	ユーザアプリケーションのユーザインタフェースから、適切な権利を持つユーザは特定のユーザのプロキシ役割を定義できます (プロキシとは、あるユーザの代理として、そのユーザが持つすべての権利を持ち、タスクを実行できるユーザのことです)。
タスクの委任 (プロビジョニングモジュールがインストールされている場合)	ユーザアプリケーションのユーザインタフェースから、マネージャ (または適切な権利を持つユーザ) は、特定の従業員が不在 (稼働不可) かどうかに応じて、他の従業員にそのタスクを自動委任するよう設定できます。委任は細分化されており、特定のタスクを異なる担当者に委任できます。
ディレクトリ抽象化レイヤ	ランタイムフレームワークが、アイデンティティポータルへのアクセスやワークフローという低レベルのメカニズムから Web アプリケーションロジックを分離し、安全で堅牢なディレクトリ抽象化アーキテクチャを実現します。この分離は、ディレクトリ抽象化レイヤ (または単に抽象化レイヤ) という仲介レイヤを通して実現されます。

機能	説明
ユーザに直接表示される全データのアクセス制御	抽象化レイヤ (eDirectory の洗練された「有効な権利」モデルを利用) により、識別データとワークフローの表示、およびデータ変更に対するユーザの権利が自動的に制限されます。これはユーザ、およびポートレットに対しても透過的に行われます。
エンドユーザによる識別データ検証	ユーザアプリケーションでは、ユーザがアイデンティティポータル内部の自分の識別情報を表示、検証、および更新することができます。
柔軟なログ	さまざまなイベントをサーバログ (log4j を使用) または Novell Audit、あるいはその両方に簡単に記録できます。
Novell Audit レポート	本製品には、プロビジョニング関連の一般的なレポート生成タスクを反映する Crystal Report のテンプレートが付属しています。
高可用性	本製品のユーザアプリケーションおよび承認フロー要素は、スケーラビリティを高めるためにクラスタ化できます。 重要: このバージョンのプロビジョニングモジュールでは、処理中のワークフローインスタンスの自動フェールオーバーはサポートされていません。ただし、処理中のフローが中断された場合には、残りのサーバノードで手動による介入処置を施して処理を続行し、完了することができます。
電子メールテンプレート管理 UI	iManager を使用して、ワークフローの電子メールテンプレートを関連付けたり、カスタマイズしたりできます。
アクセサリポートレット	ユーザアプリケーションには、GroupWise、Exchange、Lotus Notes、Web メール、ネットワークファイル、NetStorage、HTML、ショートカット、RSS、およびメッセージ用のポートレットなど、すぐに使えるさまざまなポートレットが付属しています。

これらは、Identity Manager の標準機能ではありません。本製品の標準機能については、『Identity Manager 管理ガイド』を参照してください。

1.1 サポートされている役割のタイプ

Identity Manager ユーザアプリケーションには、さまざまな識別情報管理機能が含まれています。これらすべての機能タイプがすべてのユーザにとって必要なわけではなく、ユーザの役割によって、使用できる (または表示できる) 機能は異なります。

ユーザは次のカテゴリの 1 つ以上に当てはまることを前提としています。各カテゴリではそれぞれ使用できるツールと機能が異なります。次の用語は本マニュアル全体を通して使用されます。

1.1.1 LDAP 管理者

LDAP 管理者には、アイデンティティポータル (eDirectory 8.7.x または 8.8) に対する最大限の設定権限とシステム管理権限があります。これはユーザアプリケーション管理者 (次の節で説明) とともに共有される論理的な役割で、アプリケーションサーバ (JBoss)、データベース (MySQL など)、およびポータルベースの Web UI 自体に対するシステム権限を持つユーザまたはエンティティです。

LDAP 管理者は、次の 2 種類のツールを選んで作業できます。頻度の低い (通常は一度きりの) タスクには Eclipse ベースの Designer for Identity Manager、日常の管理タスクには iManager ツールを使用します。

通常、Designer for Identity Manager を使用して実行する頻度の低いタスクには次のようなものがあります。

- ◆ Identity Manager ユーザアプリケーションで使用できる抽象化レイヤの定義、属性、および関係の設定 (詳細については [75 ページの第 4 章「ディレクトリ抽出化レイヤの設定」](#) を参照してください)。
- ◆ ディレクトリ抽出化レイヤ定義の検証 ([75 ページの第 4 章「ディレクトリ抽出化レイヤの設定」](#) を参照してください)。
- ◆ ユーザアプリケーションドライバの設定の変更 ([55 ページの第 3 章「ユーザアプリケーションドライバの設定」](#) を参照してください)。
- ◆ エンティティおよび属性の表示ラベル、組織図の関係名、およびグローバルリスト項目とローカルリスト項目の表示テキストのローカライズ ([75 ページの第 4 章「ディレクトリ抽出化レイヤの設定」](#) を参照してください)。
- ◆ ユーザアプリケーションドライバおよびその設定のインポートとエクスポート。
- ◆ その他のオフラインタスク。

管理者 (LDAP 管理者、または次の節で説明するユーザアプリケーション管理者) が稼働中のシステムで通常実行する日常のタスクは iManager で行います。これには次のようなタスクが含まれます。

- ◆ 電子メールテンプレートの管理。
- ◆ プロビジョニングされたリソースまたはプロビジョニング要求の定義や指定。
- ◆ ワークフロー定義の有効/無効の切り替え。これによりワークフロー定義のアクティブと非アクティブを切り替えます。
- ◆ 処理中のワークフローの終了。
- ◆ Novell Audit のログデータに対するレポートの実行。

これらのタスクの一部 (ワークフロー関連) は、プロビジョニングモジュールがインストールされている場合にのみ該当します。こうしたタスクの多くは、LDAP 管理者ではなくユーザアプリケーション管理者 (次の節で説明) によって実行される場合もあります。

1.1.2 ユーザアプリケーション管理者

ユーザアプリケーション管理者は、Web アプリケーション (JBoss で実行されるブラウザベースのアプリケーション) の管理に関連したタスクを実行します。この役割の管理ツールには、Identity Manager ユーザインタフェースの [管理] タブからアクセスします。

ユーザアプリケーションでは次のアクションを実行できます。

- ◆ アイデンティティボールド (LDAP プロバイダ) への接続方法の指定など、さまざまなユーザアプリケーションの設定。詳細については、[201 ページの第 10 章「ポータル環境設定」](#)を参照してください。
- ◆ Identity Manager ユーザインタフェースに表示されるページ、およびそれにアクセスできるユーザの決定。[137 ページの第 7 章「ページの管理」](#)を参照してください。
- ◆ Identity Manager ユーザインタフェースで使用できるポートレット、およびそれにアクセスできるユーザの決定。[181 ページの第 9 章「ポートレットの管理」](#)を参照してください。
- ◆ Identity Manager ユーザインタフェースの外観や操作方法の設定。[175 ページの第 8 章「テーマの環境設定」](#)を参照してください。
- ◆ Identity Manager ユーザアプリケーションが生成するログメッセージのレベル、および Novell Audit に送信するメッセージの制御。[213 ページの第 12 章「ログの環境設定」](#)を参照してください。
- ◆ Identity Manager ユーザアプリケーションが使用するさまざまなキャッシュの管理。[219 ページの第 13 章「キャッシングの環境設定」](#)を参照してください。
- ◆ Identity Manager ユーザアプリケーションで使用される Web コンテンツ (ページおよびポートレット) のエクスポートとインポート。[229 ページの第 14 章「ポータルデータのエクスポートおよびインポートのためのツール」](#)を参照してください。
- ◆ 特定のユーザに対するプロキシ権利の設定。
- ◆ エンドユーザに表示されるユーザインタフェース関連のその他多くのタスク。

iManager では次のタスクを実行できます。

- ◆ 電子メールテンプレートの管理。
- ◆ プロビジョニングされたリソースやプロビジョニング要求定義の定義または指定。
- ◆ ワークフロー定義の有効 / 無効の切り替え。これによりワークフロー定義のアクティブと非アクティブを切り替えます。
- ◆ 処理中のワークフローの終了。
- ◆ Novell Audit のログデータに対するレポートの実行。

これらのタスクの一部 (ワークフロー関連) は、プロビジョニングモジュールがインストールされている場合にのみ該当します。

1.1.3 エンドユーザ

エンドユーザとは、ユーザアプリケーションのユーザインタフェースを構成するさまざまなポートレットや Web ページを表示したり、使用したりするユーザのことです。ここでは、エンドユーザとは、従業員、マネージャ、または従業員とマネージャのプロキシまたは委任ユーザを意味します。

エンドユーザは潜在的に多くの機能を使用できますが、これは管理者が有効にした機能の数に依存します。エンドユーザは、Identity Manager ユーザアプリケーションを使用して最低限、次の機能を実行できます。

- ◆ 組織図ポートレットを使用した、ユーザオブジェクトの階層関係の表示。
- ◆ 適切な権利を持つユーザ情報の表示と編集。

- ◆ 詳細な検索条件を使用したユーザまたはリソースの検索 (保存して再利用可能)。
- ◆ 忘れてしまったパスワードの回復。
- ◆ チームメンバーへの電子メールの送信 (個別または一括)。

さらに、プロビジョニングモジュールがインストールされている場合は、ユーザアプリケーションの Web インタフェースから次のタスクも実行できます。

- ◆ リソースの要求 (事前定義されたワークフローを 1 つ開始する)。
- ◆ これまでになされた要求のステータスの表示。
- ◆ タスクの要求およびタスクリストの表示 (リソース、受信者、または他の特性を指定)。
- ◆ プロキシ割り当ての表示。
- ◆ 委任割り当ての表示。
- ◆ 不在 (稼働不可) または在席 (稼働可) の指定。
- ◆ 他のユーザに代わってタスクを要求するためにプロキシモードに入る。
- ◆ チームタスクの表示、チームリソースの要求など (マネージャのみ)。



1.1.4 委任ユーザ

委任ユーザとは、そのユーザの権利に合った 1 つ以上の特定のタスクを委任され、別のユーザに代わって、委任されたタスクを実行できるエンドユーザのことです。たとえば、John は休暇を取るため、その間自分のタスクを Mary に割り当てることにします。John が委任するタスクに必要な権利を Mary が持っていることを前提とし、Mary を John の委任ユーザにします。ユーザアプリケーション上で John が自分を不在 (稼働不可) としてマークすると、通常は John のタスクリストに表示されるタスクがすべて Mary のタスクリストに表示されます。そして、Mary は委任ユーザの役割を果たします。Mary は John のタスクを完全に自分のタスクとして処理できます (John のタスクではなくなります)。この委任ユーザの定義を、次に説明するプロキシユーザの定義と比べてみてください。

委任はタスクベースで行われます。つまり、責任をすべて委任するか、まったく委任しないかの二者択一的な決定になるとは限りません(ただし実際には、要求があった場合、ユーザインタフェース上で、あるユーザの全タスクを1人の委任ユーザにすべて委ねることも可能です)。1人のユーザは複数の委任ユーザを指定できます。委任ユーザはそれぞれ、与えられたタスクだけに責任を持ちます(たとえば、Johnは新しいビジネスカードの要求タスクだけをMaryに割り当て、新しいSiebelアカウントの要求はBillに割り当てることもできます)。そして、あるタスクを割り当てられた元の所有者が特定のタスクに対して自分が不在(稼働不可)であることを示すと、責任の移譲(新しいタスクの再割り当て)が自動的に行われます。不在(稼働不可)を示したタスク所有者は、委任の期限を指定できます。これもタスク別に指定できます。この移譲はルール準拠のためログに記録されます。

委任ユーザについてのユーザインタフェース機能の詳細については、『Identity Manager ユーザアプリケーション: ユーザーズガイド』を参照してください。さらに、このガイドの [321 ページのセクション 21.3 「プロビジョニングのセキュリティ」](#) も参照してください。

1.1.5 プロキシユーザ

プロキシユーザとは、他のユーザの識別情報を一時的に引き継ぐことによって、そのユーザの役割を果たすエンドユーザのことです。元のユーザの権利はすべてプロキシユーザに適用されます。その作業の元の担当者は、引き続きその作業の担当ユーザのままです。たとえば、Johnは、中国への出張中、自分の管理アシスタントであるCliveに、自分の全タスクへのアクセス権を割り当て、その処理を依頼するとします。Johnに適切な権限があれば、CliveをJohnのプロキシとして指定できます (Johnに適切な権限がない場合、ユーザアプリケーション管理者が権利を設定します)。いったん、プロキシ関係が確立されると、Cliveは、2つの役割を果たすことになります。CliveとJohnの2つの役割です。Johnの役割で作業する場合、CliveはJohnができることをすべて実行できます。Cliveがある作業を完了すると、それはJohn自身が行ったものとみなされます。

前の節で説明した委任メカニズムとは対照的に、プロキシ関係では元のユーザのタスクや設定すべてがプロキシユーザに表示されます(およびそれら进行处理する権限が与えられます)。また、プロキシユーザは、プロキシの役割を担当している間、Johnがアクセスできる属性、関係、またはシステム設定すべてにアクセスできます。

委任とプロキシのもう1つの違いとして、委任メカニズムの場合は、タスクごとに複数の委任ユーザに委任を行えるのに対し、プロキシメカニズムでは、プロキシユーザが常に、元のユーザのタスクすべてを担当します。つまり、ユーザが誰かをプロキシとして指名すると、そのプロキシユーザはあたかもそのユーザになったかのように、すべてのタスクを表示し、処理できるということです。

プロキシとして他のユーザの代わりに処理した内容は、Novell Auditに記録されます(ルールに準拠していることを示すため)。

他のプロキシシナリオについては、『Identity Manager ユーザアプリケーション: ユーザーズガイド』の「[プロビジョニング情報の設定](#)」を参照してください。

1.2 データの抽象化：柔軟な識別情報管理のための重要な概念

Identity Manager ユーザアプリケーションを理解するために重要な概念は、データの抽象化、つまり、ディレクトリ抽象化レイヤ定義のインスタンスを定義、表示、および操作できるということです。

従来のストレージ技術では、リレーショナルデータベース、X.500 ディレクトリなど、どのリポジトリを使用する場合でも、通常、データエントリ（データベースの行、X.500 ディレクトリのオブジェクトなど）は、詳細に定義されたスキーマに厳密に従う必要がありました。保存されているデータのクエリは、（理論上は）いくらでも複雑にすることができ、またデータはインデックスやバックリンクを含んでいてもかまいませんが、実際のデータエントリ自体は固定された定義に従うことが求められます。さらに、適用されるスキーマは、時間が経っても著しく変更されることはないことが前提になっています。

これは、異なるデータソース上の異なるスキーマに依存する情報を統合して、新しい（場合によっては一時的な）スキーマに準拠するデータオブジェクトを作成するような場合、問題になります。識別情報は複合的で変化する傾向があることから、識別データはその典型的な例といえます。識別情報の基になる各データはさまざまなソースから取得されており、各データには（当然ながら）それを保護しようとする管理者がいる場合があります。

スキーマ定義が厳格な（または規則で制限されている）場合、識別データの分散は識別情報管理の上で難題となります。この問題に取り組む1つの方法としては、識別データを1つの論理ボールドに集約し（1つのディレクトリとして実装し）、必要に応じてソースデータから論理識別情報を集めるという方法があります。これは、たとえば、従来のLDAP オブジェクトと属性を任意の抽象化レイヤの定義と属性にマップする1つ以上の論理スキーマに従って行います。これにより、識別データは高度に複合的で動的になります。識別情報の定義を変更してもLDAP スキーマを変更する必要はありません。特定のアプリケーション、または特定のアプリケーションを使用する特定のユーザに合わせて、識別情報オブジェクトを自由に再定義できます。

この総合的なアプローチはデータ抽象化と呼ばれます。つまり、識別情報は必要に応じて必要な形式で表現されます。

識別データの抽象化には、次のような多くの利点があります。

- ◆ 潜在的にLDAP ディレクトリスキーマの混乱につながる恐れのある変更を避けることができます。
- ◆ 抽象化テクノロジーは他のシステムに介入しないため、接続システムへの変更は必要ありません。
- ◆ データ間の新しい関係を構築できます。
- ◆ 抽象化レイヤの定義はいつでも変更または拡張できます。
- ◆ オブジェクトの属性は必要な数だけ設定できます。
- ◆ 関連のない複数のLDAP オブジェクトクラスの属性は、抽象化レイヤ定義でマージできます。
- ◆ 属性名には任意の名前を使用できます（LDAP 名を使用する必要はありません）。
- ◆ 詳細なアクセス制御ポリシーはそのまま使用できます（ユーザには表示権限のあるデータのみが表示されます）。
- ◆ 新しいオブジェクトタイプ（または属性の組み合わせ）に対し、純粋なLDAP 環境では不可能な、複雑な検索ができます。

Identity Manager では、抽象化を利用して、これらすべての目標を (およびその他の目標も) 達成できます。

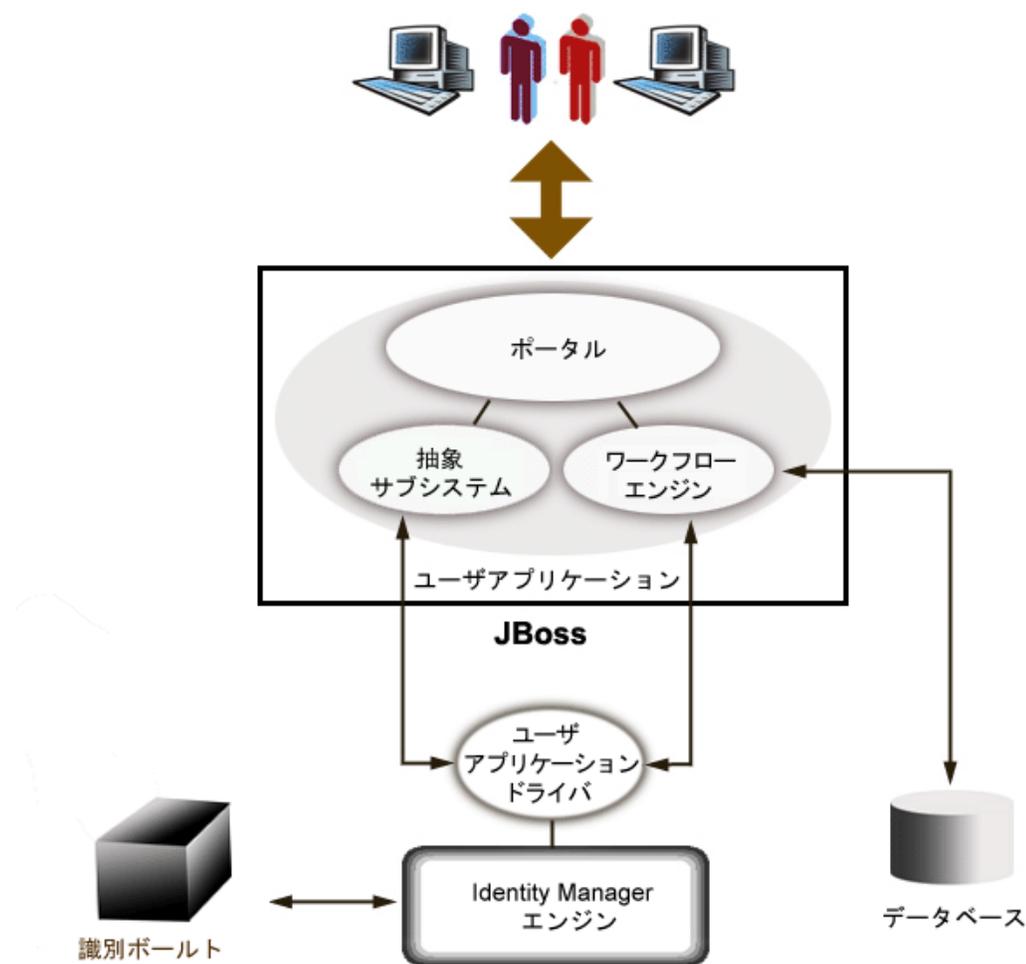
1.3 高レベルアーキテクチャ概要

Identity Manager ユーザアプリケーションは、独立したコンポーネントの連携によって成り立っています。次の表では、コアコンポーネントとその基本的な役割について説明します。

コンポーネント	説明
アイデンティティポータル (eDirectory 8.7.3 または 8.8)	ユーザデータ (および他の識別データ)、IDM ドライバセットとドライバ、さまざまな抽象化レイヤの生成物、およびワークフローの生成物 (プロビジョニングモジュールがインストールされている場合) のリポジトリ。
Identity Manager エンジン	eDirectory (および接続システム) でイベントを監視する Identity Manager ランタイムフレームワーク。ポリシーを適用し、アイデンティティポータルとの間で送受信されるデータをルーティングします。
ユーザアプリケーションドライバ	ユーザアプリケーションドライバは、ユーザアプリケーションと通信し、抽象化レイヤの定義が変更されるとユーザアプリケーションがそのキャッシュを更新できるようにします。プロビジョニングモジュールがインストールされている場合、アイデンティティポータル内のイベントがワークフローをトリガするよう、ユーザアプリケーションドライバを設定することもできます。また、エンタイトルメント情報をアイデンティティポータルに返し、ワークフローの完了時にエンタイトルメントが付与されたかどうかに関する記録を残します。
ユーザアプリケーション: Web UI	ユーザアプリケーションの Web UI は、JSR 168 準拠のポートレットが接続するブラウザベースの Java アプリケーションです。
ユーザアプリケーション: 抽象化レイヤ	抽象化レイヤはアイデンティティポータルからプレゼンテーション層ロジックを分離し、識別データに対する要求がすべて抽象化レイヤを経由するようにします。ポートレットコードでは識別情報に直接アクセスできません。すべての要求は抽象化レイヤを経由し、その制約 (アクセス制御など) に従います。
ユーザアプリケーション: ワークフローエンジン (プロビジョニングモジュールがインストールされている場合のみ)	ワークフローエンジンとは、管理者が定義したワークフローに含まれる手順を管理および実行する一連の Java 実行可能ファイルです。
JBoss アプリケーションサーバ	オープンソースの JBoss アプリケーションサーバは、ユーザアプリケーション、抽象化レイヤ、およびワークフローエンジンが実行されるランタイムフレームワークを提供します。
データベース (デフォルトでは MySQL)	データベース (サポートされているデータベースについては『インストールガイド』を参照) には、ユーザアプリケーションのための設定情報、およびワークフローの状態が保存されます (プロビジョニングモジュールがインストールされている場合)。
Composer サービスドライバ	Composer サービスドライバはユーザアプリケーションドライバの一部で、ワークフローを起動してアイデンティティポータルのイベントに応答するようカスタム設定できます。

コンポーネント	説明
Novell Audit	Novell Audit は、さまざまな種類のデータ (ワークフローで生成されたデータなど) を永続保存できる独立したログサーバです。詳細については、このマニュアル後半のログの設定に関する章を参照してください。

これらのコンポーネントは、情報の流れという観点から考えると、次の図のように論理的にリンクしています。物理的には、各コンポーネントは、ほとんどの場合、複数のコンピュータに存在します。たとえば、アイデンティティポータル (およびその主な管理ツールである iManager) は Identity Manager エンジンを実行するコンピュータ上に共に配置されますが、JBoss (およびユーザアプリケーション) は通常、別のコンピュータ (クラスター化されている場合はコンピュータのグループ) 上にホストされます。同じように、データベース (MySQL) は通常、パフォーマンスだけでなくセキュリティと障害復旧の観点から、専用のコンピュータに配置されます。



1.3.1 アイデンティティポータル

アイデンティティポータルは、さまざまな種類の識別データおよび抽象化レイヤ定義を保存するために使用されます。eDirectory (Windows、Solaris、または Linux で実行) のイン

スタンスの1つがこの目的用に使用されます。Identity Manager は、eDirectory を使用することにより、信頼性およびスケーラビリティが非常に高く、パーティション機能とレプリケーション機能を備えたエンタープライズクラスの LDAPv3 ディレクトリを利用できます。さらに、Identity Manager と eDirectory を結ぶ一元的な管理統合ポイントとして、柔軟的な Web ベースの管理設定ツール (iManager) を使用します。

1.3.2 JBoss

ユーザアプリケーションは、Java Web アプリケーションアーカイブ、つまり WAR ファイルとしてパッケージ化されています。WAR は、広く使用されているオープンソースの Java アプリケーションサーバである JBoss に展開されます (図には示されていませんが、JBoss はサーブレットエンジンとして Tomcat を使用します)。実行環境として JBoss を使用すると、次のような多くの利点をもたらされます。

- ◆ ソースコードを自由に入手できます。
- ◆ JBoss はバージョン 4.0.3 からクラスタ化が可能になりました。
- ◆ JBoss は J2EE に完全準拠しているため、どのような J2EE アプリケーションでも実行できます。ユーザアプリケーションが実行されるのと同じ JBoss のインスタンスで、追加のアプリケーション (Web サービスなど) をホストできます。
- ◆ JBoss は、標準の JAAS および JACC の Java セキュリティサービスと認証サービスをサポートしています (ユーザアプリケーションはアイデンティティボールドにアクセスするために、これらに依存します)。
- ◆ JBoss は一般的なバージョンの Windows や Linux を含め、さまざまなプラットフォームで実行できます。

ユーザアプリケーションの WAR には、ユーザアプリケーション用の実行可能コードが含まれます。また、この実行可能コードは、機能を分離する MVC (Model-View-Controller) アーキテクチャを使用して構築されます。ユーザ側のインタフェースは、ユーザアプリケーション内のモジュラーポートレットとして実行されます。組織図の表示、検索の実行、ユーザ詳細の表示、パスワードのリセットなどに応じて別個のポートレットが存在します。

JBoss への Web アプリケーションの展開の詳細については、<http://www.jboss.org/products/jbossas/docs> (<http://www.jboss.org/products/jbossas/docs>) にある JBoss のドキュメントを参照してください。

1.3.3 データベース

ユーザアプリケーションは、データベースを使用して、次の情報を格納します (デフォルトでは MySQL。サポートされているデータベースについては、『インストールガイド』を参照してください)。

- ◆ ユーザアプリケーション環境設定データ : Web ページの定義、ポートレットインスタンスの登録、および初期設定値など。
- ◆ プロビジョニングモジュールがインストールされている場合、ワークフローの状態情報はデータベースに保持されます (実際のワークフロー定義はアイデンティティボールドに保存されます)。
- ◆ Novell Audit のログ

1.3.4 Identity Manager エンジン

Identity Manager 製品は、ランタイムエンジン、ドライバ、およびポリシーで構成されています。Identity Manager エンジンはアイデンティティボールド内のイベントに応答し、アイデンティティボールドとの間で送受信されるデータのフローと変換を管理します。ドライバオブジェクトは、特定の接続システムに特有のデータ処理動作を指定するために設計された実行可能コードと生成物 (ポリシードキュメントなど) をカプセル化します。Identity Manager ユーザアプリケーションは接続システムの 1 つです。アイデンティティボールド、ユーザアプリケーションの抽象化レイヤ、およびワークフローエンジン間の通信は、ユーザアプリケーションドライバを経由して行われます (次の節を参照)。

ユーザアプリケーションは、抽象化レイヤの生成物を保存する目的でさまざまなディレクトリオブジェクトに依存するため、ユーザアプリケーションで要求されるカスタム LDAP オブジェクトとその属性に対応するように、eDirectory スキーマを拡張する必要があります。スキーマの拡張は、Identity Manager のインストールプロセスの一部として自動的に実行されます。ただし、ユーザアプリケーションドライバがインストールされてアクティブになるまで、カスタムオブジェクトと属性にデフォルト値は入力されません。

1.3.5 ユーザアプリケーションドライバ

ユーザアプリケーションドライバは、ユーザアプリケーションが動作する上で重要な要素です。ユーザアプリケーションドライバの役割の一つは、アイデンティティボールドで重要なデータ値が変更されたときに抽象化レイヤに通知し、抽象化レイヤがそのキャッシュを更新できるようにすることです。

プロビジョニングモジュールがインストールされている場合は、アイデンティティボールドの属性値の変化に応答してワークフローを自動的に起動するよう、ユーザアプリケーションドライバを設定できます。

ユーザアプリケーションドライバはランタイムコンポーネントであるだけでなく、ディレクトリオブジェクト (ユーザアプリケーションのランタイムの生成物で構成される) のストレージラッパーでもあります。ユーザアプリケーションドライバに関連付けられるディレクトリ生成物の典型例を次に示します。



注: 表示されている名前は、LDAP 共通名 (cn) 値です。さまざまなオブジェクトクラスのスキーマを命名する方法については、別の箇所で説明します。

次では生成物のカテゴリについて詳細に説明します。

ドライバセットオブジェクト

Identity Manager のインストールでは、ドライバをドライバセットとしてグループ化する必要があります。1つのディレクトリサーバで、1度にアクティブ化できるドライバセットの数は1つに限られます。セット内のドライバは、ドライバセット全体に影響を与えることなく個別にオンとオフを切り替えることができます。ユーザアプリケーションドライバも、他の IDM ドライバと同じように、ドライバセット内に存在していなければなりません。ドライバセットはユーザアプリケーションによって自動作成されるわけではありません。ユーザがドライバセットをあらかじめ作成し、その中にユーザアプリケーションドライバを作成する必要があります。

ユーザアプリケーションドライバ

ユーザアプリケーションドライバオブジェクト (任意の名前を命名可) は、さまざまな生成物のコンテナです。すべての Identity Manager のドライバと同じように、ユーザアプリケーションドライバも、発行者チャンネルと購読者チャンネルのオブジェクトとポリシーを実装します。発行者チャンネルがユーザアプリケーションによって使用されることはありませんが、カスタムでは利用可能です。

AppConfig オブジェクト

AppConfig オブジェクトは、さまざまなユーザアプリケーション設定オブジェクトのコンテナです。

RequestDefs

これはプロビジョニング要求定義のコンテナで、ユーザアプリケーションランタイムが使用できる、管理者によって設定された要求定義です (プロビジョニングモジュールが存在している場合)。ここに保存される定義 (XML 形式) は、適切な権利を持つエンドユーザがユーザアプリケーションを使用してインスタンス化できる要求のクラスを表します。RequestDef は、WorkflowDef (次の節で説明) を ResourceDef に関連付けます。

WorkflowDefs

ワークフローオブジェクトのコンテナで、デザイン時の説明に加え、テンプレートや未使用のフローも含まれます。

ResourceDefs

プロビジョニングリソース定義のコンテナで、デザイン時の説明に加え、テンプレートや未使用のターゲットも含まれます。

ServiceDefs

サービス定義オブジェクトのコンテナで、ワークフローによって呼び出される Web サービスをラップします。

DirectoryModel

抽象化レイヤのメタレベルオブジェクト (ChoiceDefs、EntityDefs、RelationshipDefs) で、識別ポートレットで公開できるさまざまな種類のディレクトリのコンテンツ (一部はユーザ定義可能、他は管理者による設定) を表します。

AppDefs

キャッシュ設定情報や電子メール通知プロパティなど、ランタイム環境の初期化に使用される設定オブジェクトのコンテナです。

ProxyDefs

プロキシ定義のコンテナです。

DelegateeDefs

委任定義のコンテナです。

1.3.6 ディレクトリ抽象化レイヤ

ポートレットは、ディレクトリ抽象化レイヤへのクエリによって識別データを取得します。ディレクトリ抽象化レイヤは、クライアントプロセスから識別データアクセスを分離するコード層です。たとえば、ポートレットが識別データを検索する必要がある場合、抽象化レイヤはポートレットに代わり、アイデンティティポールのターゲットコンテナに対し適切な LDAP クエリを実行します。どのような場合でも、ポートレットがアイデンティティポールの直接クエリを実行することはありません。

抽象化レイヤは、システムの管理者や適切な権利を持つ他のユーザが指定したとおりに、抽象化レイヤ定義を作成したり変更したりできるコードレイヤでもあります。こうした変更を行う場合、システムエキスパートは Designer アプリケーションのディレクトリ抽象化レイヤエディタを使用します。詳細については、このガイド後半の **75 ページの第 4 章「ディレクトリ抽出レイヤの設定」** を参照してください。

実行時、抽象化レイヤは、アイデンティティポールの取得したさまざまな設定データやエンティティ定義データをキャッシュします。ユーザアプリケーションで使用されるさまざまなキャッシュは、管理者がより細かく管理できます。キャッシュおよびキャッシュ管理の詳細については、**219 ページの第 13 章「キャッシングの環境設定」** を参照してください。

1.3.7 ワークフローエンジン

ワークフローエンジン (プロビジョニングモジュールで使用可能) は、ランタイムクラスのセットで、プロセス定義 (ワークフローがインスタンス化されたときに作成されるランタイム生成物) の指定に従ってワークフローの手順を実行します。また、状態情報を記録し、MySQL や Oracle などのデータベースに保持します。詳細については、**23 ページのセクション 1.3.3「データベース」** を参照してください。

ワークフローの作成方法など、ワークフローシステムの詳細については、このガイド後半の **311 ページの第 21 章「ワークフローベースプロビジョニングの概要」** を参照してください。

1.3.8 ユーザインタフェース

Identity Manager のユーザインタフェースは、JSR168 準拠ポータル (プロビジョニングモジュールの場合は Java Server Pages) の集まりで構成されます。これらは JBoss の Java Web アプリケーション内で実行されます。ポータルアーキテクチャにより、高度なモジュール性が確保され、コンテンツをカスタマイズしたり、ユーザによるページ表示を制御できます。ユーザアプリケーションのフレームワークは、さまざまな種類のコンテナサービスを提供し、ウィンドウの状態、ポータルの初期設定、永続保存、キャッシング、テーマ、ログなどを管理し、セキュリティのゲートキーパとしての役割を果たします。これに対し、ユーザアプリケーションが実行されるアプリケーションサーバは、クラスタ化によるスケーラビリティ、JDBC を経由したデータベースへのアクセス、および証明書ベースのセキュリティサポートなど、アプリケーション全体に対するさまざまなサービスを提供します。

このアーキテクチャでもたらされる高度なカプセル化は、Identity Manager ユーザアプリケーションに堅牢で安全なプレゼンテーション層環境を提供します。また、ユーザインタフェースのすべての面で高度な管理制御を実現します。

ユーザインタフェースの各部分の管理の詳細については、このガイドの [129 ページのパート III 「ユーザアプリケーションの管理」](#) 内の各章を参照してください。

1.4 設計および設定用ツール

Identity Manager ユーザアプリケーションのさまざまな機能は、Identity Manager Designer ツール (Eclipse Rich Client Platform ベース) や iManager プラグインを使用することで、カスタマイズできます。

次の表では、使用可能なツールとその使用目的について説明します。

ツール	目的
Designer for Identity Manager	Identity Manager の一般的な設定ツールで、このツールを使用して開発者、コンサルタント、またはシステム管理者はドライバセット、ドライバ、ポリシー定義、およびその他の生成物を詳細に設定および変更できます。
Designer 用ディレクトリ抽象化レイヤエディタプラグイン	カスタムオブジェクトおよびその関係を定義し、抽象化レイヤのさまざまな設定を変更できます。このガイド後半の 75 ページの第 4 章「ディレクトリ抽出レイヤの設定」 を参照してください。
プロビジョニング要求設定プラグイン	使用可能なプロビジョニング要求の種類を定義および設定できます (iManager)。
プロビジョニングされたリソースエディタ (近日中にリリース)	Designer のプラグインで、リソース (ワークフローに応答して付与されるリソースを表すオブジェクト) を作成および設定できます。
ワークフロー定義エディタ (近日中にリリース)	Designer 用のグラフィカルワークフロー定義プラグインです。

ツール	目的
ワークフロー電子メールテンプレートエディタ	iManager のプラグインで、管理者が電子メールテンプレートを追加、削除、および編集できます。これらのテンプレートは、ユーザにワークフローイベントを通知する目的でワークフローシステムが使用します。
Ireport.exe (ログレポートツール) および iManager の監査およびログ機能	事前定義された数多くのログレポート (Identity Manager 付属) を Crystal Reports (.rpt) 形式で出力し、Novell Audit データベースに記録されたデータをフィルタリングできます。Ireport.exe ログレポートツール (Windows のみ) は、レポートを生成する方法の 1 つです。他の方法を使用してレポートを作成することもできます。詳細については、119 ページの第 5 章「ログの設定」を参照してください。

ユーザアプリケーションのカスタム抽象化レイヤ定義を設定するにあたり、システム設計エキスパートは、通常、最初に Designer for Identity Manager でディレクトリ抽象化レイヤエディタを使用することから始めます。これらのオブジェクトは、抽象化レイヤで使用できるようになります (したがって、ユーザインタフェースのユーザも使用できます)。これらのオブジェクトの定義や使用に対してアクセス制御を細かく設定できます。これにより、管理者やエンドユーザは自分が適切な権利を持つオブジェクト (とその属性) だけを表示および操作できるようになります。

プロビジョニングモジュールがインストールされている場合、システム設計エキスパートや管理者は、iManager のプロビジョニング要求設定ウィザードを使用して、ユーザアプリケーションでユーザが使用できるプロビジョニングリソースやワークフローを定義できます。同時に、管理者は、iManager の電子メールテンプレートエディタ機能を使用して、ワークフローによって送信される電子メール通知の内容を定義することもできます。この詳細については、347 ページの第 23 章「プロビジョニングワークフローの管理」を参照してください。

管理者は通常、抽象化レイヤ、プロビジョニング要求定義、監査要件、および電子メールテンプレートを設定した後に、201 ページの第 10 章「ポータル環境設定」で説明されている管理機能を使用して、ユーザアプリケーション (セキュリティ、キャッシング、およびその他の機能を含む) に影響するさまざまな設定操作を実行します。最後に管理者は、このガイドのパート IV にある各章で説明されているインタフェースを使用して、必要に応じてポートレットを個別に設定します。

注: 次の章では、これらタスクのいくつかについて詳しく解説します。次のシナリオに目を通してから、運用環境を実装するようにしてください。

1.5 ユーザアプリケーション使用シナリオ

Identity Manager ユーザアプリケーションには、数多くの機能があります。ここでは、いくつかの例を挙げて、ユーザアプリケーションを使用して実際の問題を解決する方法について説明します。

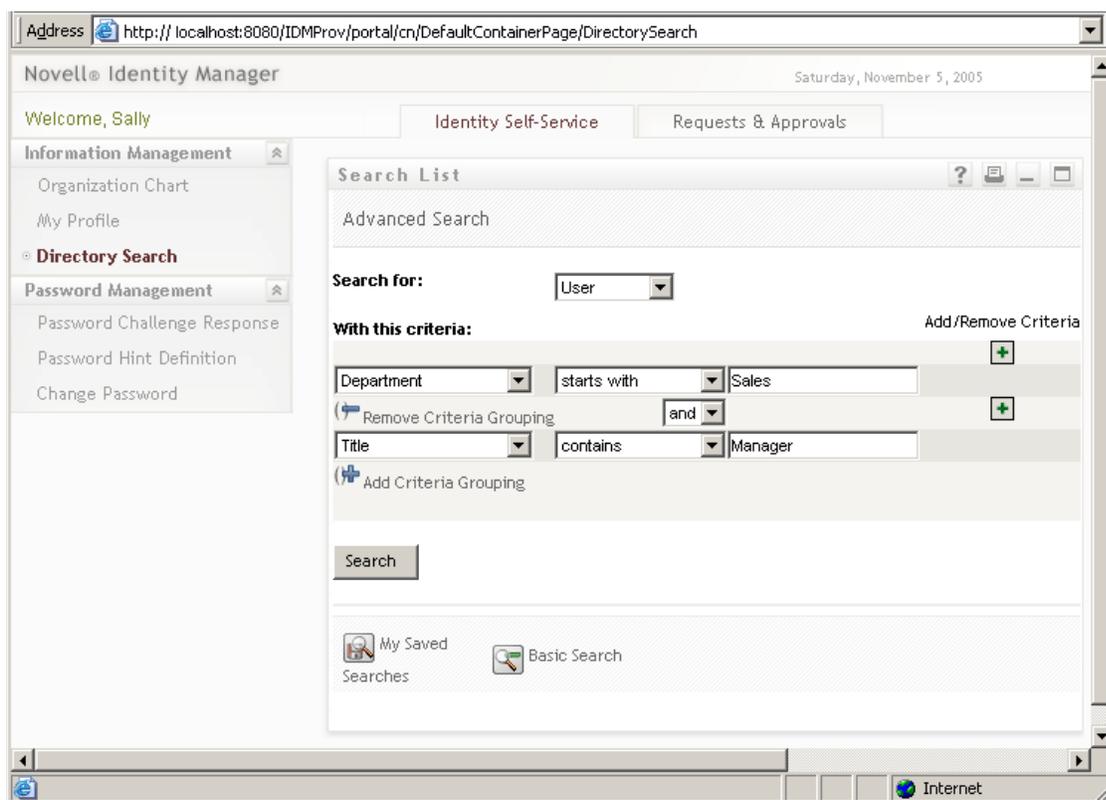
1.5.1 シナリオ A: ユーザが同じ組織内の別の人物の情報を検索する

一般的な使用例の1つとして、従業員が同じ組織内の別の人物の情報を必要とする場合があります。次に例を示します。

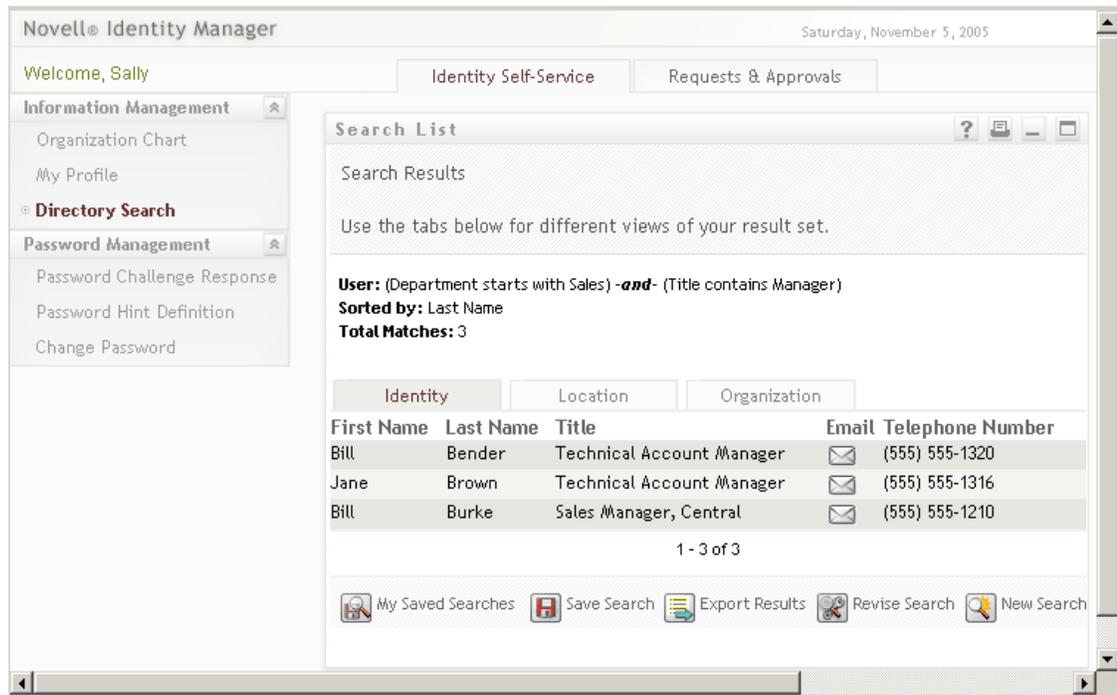
- ◆ 同僚のフルネームや連絡先情報を確認する
- ◆ ある地域内の特定のスキルセットを持つ人をすべて検索する
- ◆ 特定の人物のマネージャを確認する

このような操作(複雑なクエリに基づいた高度な検索を含む)は、ディレクトリ検索インタフェースを使用すれば簡単に実行できます。通常、エンドユーザはユーザアプリケーションにログインしてから [識別セルフサービス] タブを前面に表示させます(まだ前面に表示されていない場合)。続いて、左側のナビゲーションリンクの列にある [ディレクトリ検索] リンクをクリックします。

次の画面は、ログインユーザが、[部署] が「Sales」で始まり、[Title] に「マネージャ」が含まれるユーザを検索する高度な検索を設定している画面です。



検索が完了すると、次のような検索結果の画面が表示されます。



画面の下側にはボタンが並んでおり、この検索に使用した高度なクエリの保存、クエリの変更、および新規検索などを実行できます。また、検索された人物の上にはタブが並んでいる点にも注目してください。この画面では識別情報順に人物が並んでいますが、これらのタブを使用して場所順や組織順に表示することもできます。

1.5.2 シナリオ B: マネージャが新しいユーザを作成する

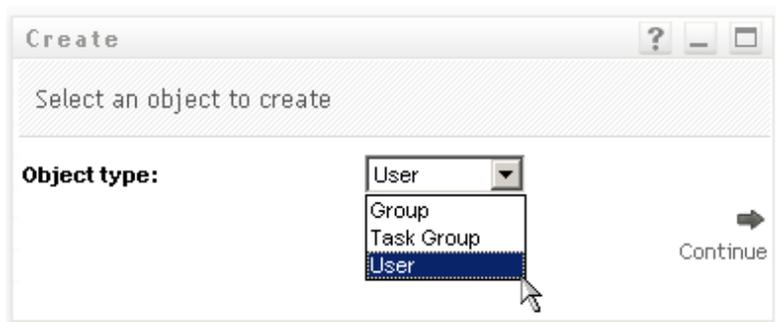
ある会社のある部門が新しいインターン、契約社員、またはその他の外部委託作業員などの非従業員（決められた期間だけその会社で働く人）を雇うことになった場合を考えます。この新しい人物をシステムに入力して、適切に限定されたリソースのセットがプロビジョニングされるよう（前述したユーザ検索で検索されるよう）にする必要があります。この人物は正社員ではないため、社内の正式な人事システムには入力しません。しかし、この人物の識別情報（およびリソースへのアクセス権）を安全な方法で管理する必要があります。

この部門のマネージャとして、ユーザをシステムに入力する権限があるとします。これを行うには、ログインしてから、ページの左側にあるナビゲーションリンクの列に [ユーザまたはグループの作成] リンクがあることを確認します (次の図を参照してください)。



注 : ログインユーザに適切な権利がなければ、このリンクは表示されません。

このリンクをクリックすると、新しいユーザとしてグループを作成するのか、タスクグループを作成するのか、ユーザを作成するのかを尋ねる画面が表示されます (次の図を参照)。



[ユーザ] を選択して [続行] をクリックすると、次のウィザードパネルでこのユーザの個人情報を入力できます。

The screenshot shows a window titled "Create" with a subtitle "Set attributes for this User" and a note "* - indicates required." The window is divided into two main sections: "Base Parameters" and "Object Attributes".

Base Parameters:

- Object ID:*** Input field containing "ckravitz".
- Container:*** Input field containing "ou=users,ou=MyUnit,o=MyOrg" with search and refresh icons to its right.

Object Attributes:

A "Hide" checkbox is located to the left of the first attribute. The attributes are:

- First Name:*** Input field containing "Carter".
- Last Name:*** Input field containing "Kravitz".
- Title:** Input field containing "Intern".
- Department:** Input field containing "Sales".
- Region:** Input field containing "Southwest".
- Email:** Input field containing "ck@blueskyu.edu".
- Manager:** Input field containing "Kip Keller" with search, refresh, and edit icons to its right.
- Telephone Number:** Input field containing "(000) 555-1239" with add (+) and delete (x) icons to its right.

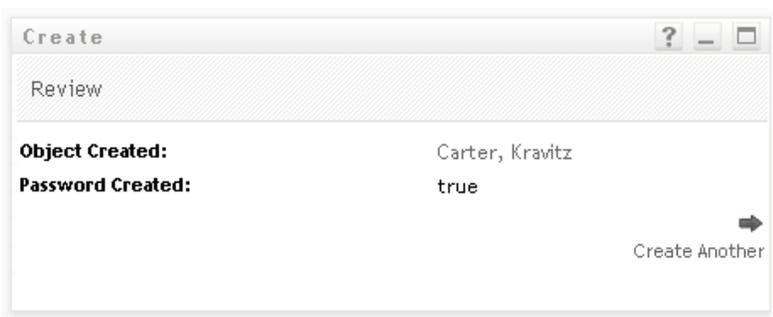
次の画面では新しいユーザのパスワードを設定できます。

The screenshot shows a window titled "Create" with a subtitle "Create Password". It contains two input fields for password creation:

- Password:** Input field containing "*****".
- Confirm Password:** Input field containing "*****".

At the bottom of the window, there are two buttons: "Back" with a left-pointing arrow and "Continue" with a right-pointing arrow. A mouse cursor is pointing at the "Continue" button.

最後の画面ではこれまでの処理の最終的な結果が表示されます。



この例では、新しく入力された人物は通常のユーザの権利をすべて備えたユーザになります。ただし、たとえばディレクトリ抽象化レイヤエディタを使用して「インターン」オブジェクトなどを定義し、そのタイプのオブジェクトだけに当てはまる固有の属性や権利を設定することもできます。この場合、前に説明した画面の選択肢に [グループ]、[タスクグループ]、および [ユーザ] に加えて [Intern] が表示されます。

1.5.3 シナリオ C: ユーザのプロビジョニング

従業員が、他人の承認が必要なリソース (オフィス機器、会社のクレジットカード、またはデータベースへのアクセスなど) を取得しなければならないことがあります。これはプロビジョニング要求と呼ばれます。Identity Manager では、プロビジョニングモジュールがインストールおよび設定されている場合、プロビジョニング要求はワークフローによって処理されます。

注: これまでの例とは異なり、この例ではプロビジョニングモジュールがインストールおよび設定されていることが必要になります。

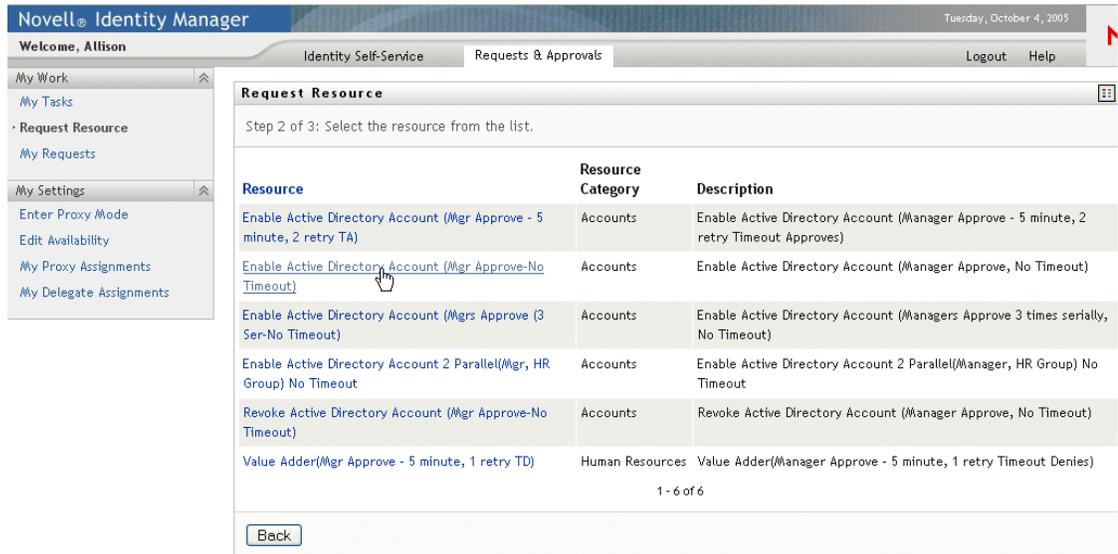
ユーザは最初にユーザアプリケーションにログインし、その最初のページを表示します。ページの上で [要求と承認] タブをクリックし、それからナビゲーションフレームの左

側にある [リソースのリクエスト] リンクを確認します。[リソースのリクエスト] リンクをクリックすると、最初の要求フォームがユーザアプリケーションに表示されます。



[リソースカテゴリ] ドロップダウンメニューには、任意の名前のエンタイトルメントを含む、任意の数のリソースタイプが含まれています (エンタイトルメントとその作成方法の詳細については、『Identity Manager 管理ガイド』を参照してください)。使用可能なプロビジョニングリソース (つまり、このユーザが現在持つ権利で要求できるリソース) をすべて表示するには、図のように [All] を選択します。

ユーザが [続行] をクリックすると、次の画面に、このユーザがアクセスできるすべてのプロビジョニング要求タイプが表示されます。



この例でユーザは、Active Directory アカウントを要求しようと考えています。これにはマネージャの承認が必要です。該当するリンクをクリックし、簡単なフォームに入力するだけで、関連付けられたワークフローが起動し、このユーザのマネージャに、実行する必要があるタスクに関する電子メール通知を送信できます。そして、マネージャは、自分の

[要求と承認] ページにログインします。このページにあるマネージャのタスクリストにはこの従業員の要求が含まれており、承認または拒否の決定を待機している状態になっています (マネージャが休暇中の場合、マネージャが指定したプロキシに通知が送信されず。プロキシはログインしてマネージャが通常行うのと同じ処理を実行できます)。この間、ブラウザ画面はワークフロー要求が正常に送信されたことを示す要約のページに切り替わります。

この社内ディレクトリのアカウントの付与は、エンタイトルメント要求の一例です。Identity Manager ユーザアプリケーションではさまざまな種類のエンタイトルメント要求を設定できます。さらに、さまざまな種類のワークフロー (1 人または複数のマネージャによる承認、順次フロー、並行フロー、タイムアウトの有無など) を作成できます。いずれの場合でも、細かいアクセス制御により、ワークフローやその他の情報の表示を管理することができます。

これらの機能の詳細については、このガイド後半の章を参照してください (これらの章は主に管理者向けです。この機能の使用方法の詳細については、『Identity Manager ユーザアプリケーション: ユーザーズガイド』を参照してください)。

1.6 次のステップ

運用環境の設計について、さらに詳しく確認する場合は、次の章に進んでください ([37 ページの第 2 章「運用環境の設計」](#))。そうでない場合には、それぞれ次の情報に関する章に直接進むことができます。

ユーザアプリケーションのログおよび監査機能については、[119 ページの第 5 章「ログの設定」](#)を参照してください。

ユーザインタフェースの外観や操作方法のカスタマイズについては、[175 ページの第 8 章「テーマの環境設定」](#)を参照してください。

iManager 以外のユーザアプリケーションの管理インタフェースから管理されるセキュリティについては、[209 ページの第 11 章「セキュリティの環境設定」](#)を参照してください。

ユーザアプリケーションのキャッシュ管理機能については、[219 ページの第 13 章「キャッシングの環境設定」](#)を参照してください。

パスワード管理機能については、[281 ページの第 19 章「パスワード管理ポートレットの参照」](#)を参照してください。

ポートレット管理については、[181 ページの第 9 章「ポートレットの管理」](#)を参照してください。

ポータルデータのインポートとエクスポートについては、[229 ページの第 14 章「ポータルデータのエクスポートおよびインポートのためのツール」](#)を参照してください。

組織図の機能については、[265 ページの第 18 章「組織図ポートレットの参照」](#)を参照してください。

ディレクトリ検索機能については、[295 ページの第 20 章「リスト検索ポートレットの参照」](#)を参照してください。

新しいオブジェクトの作成 (ポートレットの作成) に関するオプションとその管理方法については、[243 ページの第 16 章「作成ポートレットの参照先」](#)を参照してください。

ワークフローの設定と管理については、311 ページの第 21 章「ワークフローベースプロビジョニングの概要」、325 ページの第 22 章「プロビジョニング要求定義の設定」、および 347 ページの第 23 章「プロビジョニングワークフローの管理」を参照してください。

運用環境の設計

この章では、運用環境のセットアップに関する事項について解説します。サンドボックス環境やテスト環境(または他の運用前環境)から運用環境へ移行する際の考慮事項について説明します。

この章は次の節で構成されています。

- ◆ 37 ページのセクション 2.1 「トポロジ」
- ◆ 40 ページのセクション 2.2 「セキュリティ」
- ◆ 42 ページのセクション 2.3 「パフォーマンスの調整」
- ◆ 45 ページのセクション 2.4 「クラスタリング」

2.1 トポロジ

各主要サブシステムのインスタンス数が非常に多く、それらを接続する方法も多数あるという場合でも、可能なレイアウトがすべてサポートされるわけではありません。何が可能かということだけではなく、どういった理由でどの構成を優先するのかといったことを理解することが重要です。

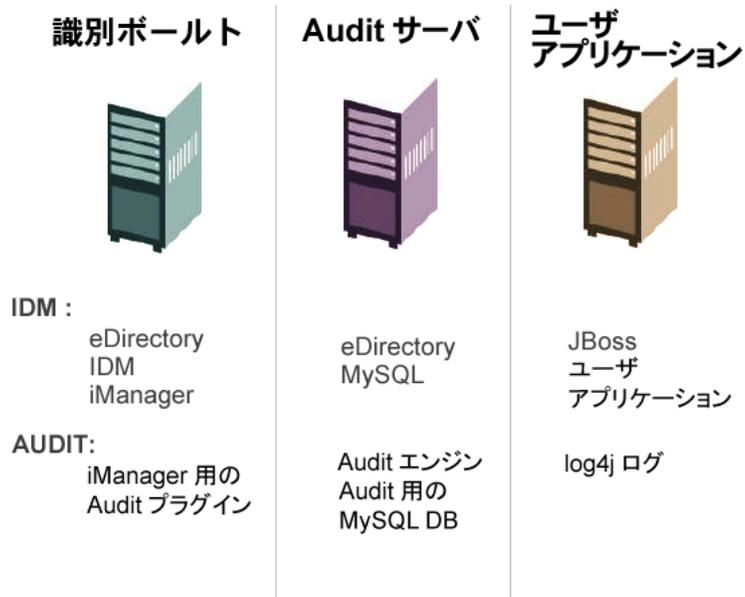
2.1.1 最小設計

ユーザアプリケーションの最も簡単な論理構成は「すべてを1つずつ」インストールする方法です。1つのアイデンティティポータルツリー、Identity Manager エンジンとドライバに1インスタンス、ユーザアプリケーションの1インスタンスを実行する JBoss に1インスタンスで構成されます。物理的な実装の観点から考えると、論理的にはこのすべてを1台のコンピュータで実行できます。しかし実際にはさまざまな理由(セキュリティ、メンテナンス性、特にパフォーマンス)から、この実装はお勧めできません。実用的な実際のインストールに必要なコンピュータの台数を決めるときには、最低限次の点を考慮してください。

- ◆ **Novell Audit** サーバ: 実行時、ユーザアプリケーション環境からのイベント情報(他の情報が含まれている場合も多い)の取得を担当します。社内の他のアプリケーションの永続ストアとして二重の役割を果たす場合もあります。さまざまな理由から、Identity Manager システムの他の主要部分(JBoss やアイデンティティポータルなど)を、Novell Audit サーバと同じコンピュータに置くことはお勧めできません。
- ◆ **アイデンティティポータル**: アイデンティティポータルは、非常に大量のトラフィックが発生するコンポーネントのため、高いパフォーマンスとスケーラビリティが求められます。アイデンティティポータルは専用のコンピュータで実行することもできます。つまり、ユーザアプリケーションが展開される JBoss など、トラフィックの多い他のシステムが、アイデンティティポータルと同じコンピュータ上で同時に実行されないようにすることができます。
- ◆ **データベース**: MySQL (またはサポートされている他のデータベース)のこのインスタンスが Novell Audit データベースでもある場合、このインスタンスを専用のコンピュータで実行することもできます。データベースは、ユーザアプリケーションによって次のように使用されます。
- ◆ **ポータル設定データの永続ストア**

- ◆ 処理中のワークフローに関する状態情報の永続ストア (プロビジョニングモジュールがインストールされている場合)
- ◆ Novell Audit のログストア (オプション)
- ◆ *JBoss*: パフォーマンスおよび容量上の理由から、このシステムを専用のコンピュータで実行することもできます。

以上を考慮した結果、最小設計として次の 3 台のコンピュータから成る構成が考えられます。



2.1.2 高可用性の設計

クラスタリングにより可用性を高めたり容量を大きくしたりする方法については、この章後半の節で詳しく説明しています。ここでは、次の点について理解してください。

- ◆ **Identity Manager** はマルチノードインストールおよび共有ストレージメカニズムを使用してアイデンティティポータル、エンジン、およびドライバの高可用性をサポートしています。詳細については、『**Identity Manager 管理ガイド**』の「高可用性」を参照してください。SUSE Linux を使用してシステムをセットアップする場合の詳細については、次の URL の記事を参照してください。

<http://support.novell.com/cgi-bin/search/searchtid.cgi?/10093317.htm> (<http://support.novell.com/cgi-bin/search/searchtid.cgi?/10093317.htm>)

- ◆ ユーザアプリケーションの高可用性は、JBoss クラスタリングにより実現できます。各ノードが 1 つのユーザアプリケーションインスタンスを実行するように JBoss クラスタを設定できます。インスタンス間の関係はすべて同等 (ピア) です。ただし、インスタンス間でのセッションレプリケーションは行われません。各インスタンスはそれ自体の作業を担当し、同等の別のノードによって開始されたセッションを終了させることはありません。
- ◆ 自動フェールオーバーはサポートされていません (直前に説明した理由により)。ただし、クラスタノードが失われた後でも、ダウンしたノードと同じワークフローエンジン ID で新しいノードがオンラインになると、中断したワークフローを再開できます

(この場合、新しいワークフローエンジンが開始されると、中断したワークフローは自動的に再開されます)。

詳細については、[45 ページのセクション 2.4 「クラスタリング」](#)を参照してください。

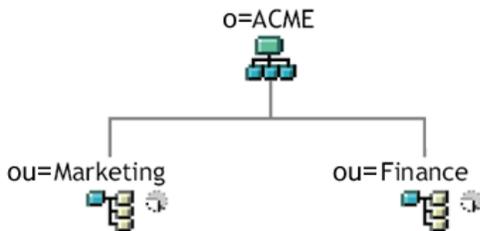
2.1.3 設計上の制約

一般に、アーキテクチャ上の最も重要な制約は次の 2 つです。

- ◆ ユーザアプリケーションインスタンスは、複数のユーザコンテナに対して、処理 (検索、クエリ、およびユーザの追加など) を行うことはできません。また、あるユーザコンテナがいったんアプリケーションに関連付けられると、その関連付けが変更されることはありません。
- ◆ ユーザアプリケーションドライバを複数のユーザアプリケーションに関連付けることはできません。ただし、複数のユーザアプリケーションが同じ JBoss クラスタにある同等の複数のノードにインストールされている場合は例外です。つまり、ドライバとユーザアプリケーション間において 1 対多のマッピングはサポートされていません。

1 番目の制約により、ユーザアプリケーションの設計には高度なカプセル化が求められます。

たとえば、次のような組織構造があるとします。



ユーザアプリケーションのインストール時、アイデンティティボールド内でユーザアプリケーションの検索対象となる最上位のユーザコンテナを指定するよう求められます。この場合、`ou=Marketing,o=ACME`、または `ou=Finance,o=ACME` のように指定できます。両方を指定することはできません。ユーザアプリケーションの検索とクエリ (および管理者ログイン) はすべて、指定したコンテナのいずれかを検索範囲にして実行されます。

注: 理論上は、`o=ACME` を検索範囲に指定すれば `Marketing` と `Finance` の両方を網羅できます。しかし大規模な組織では、(`Marketing` と `Finance` に関係する 2 つのコンテナだけではなく) 多数の `ou` コンテナが存在する可能性があるため、実用的ではありません。

もちろん、(リソースを共有しない) 2 つの独立したユーザアプリケーションのインストールを作成し、1 つをマーケティング用、もう 1 つを財務用として使用することもできます。各インストールは、それぞれ独自のデータベース、および適切に設定されたユーザアプリケーションドライバを持ちます。各ユーザアプリケーションは別々に管理され、独自のテーマを持つこともあります。

どうしても、1 つのユーザアプリケーションインストールの同じ検索範囲にマーケティングと財務を設定する必要がある場合には、2 つの方法が考えられます。1 つの方法としては、2 つの同等ノードの上位に新しいコンテナオブジェクト (`ou=MarketingAndFinance` など) を挿入し、その新しいコンテナを検索範囲のルートとしてポイントする方法がありま

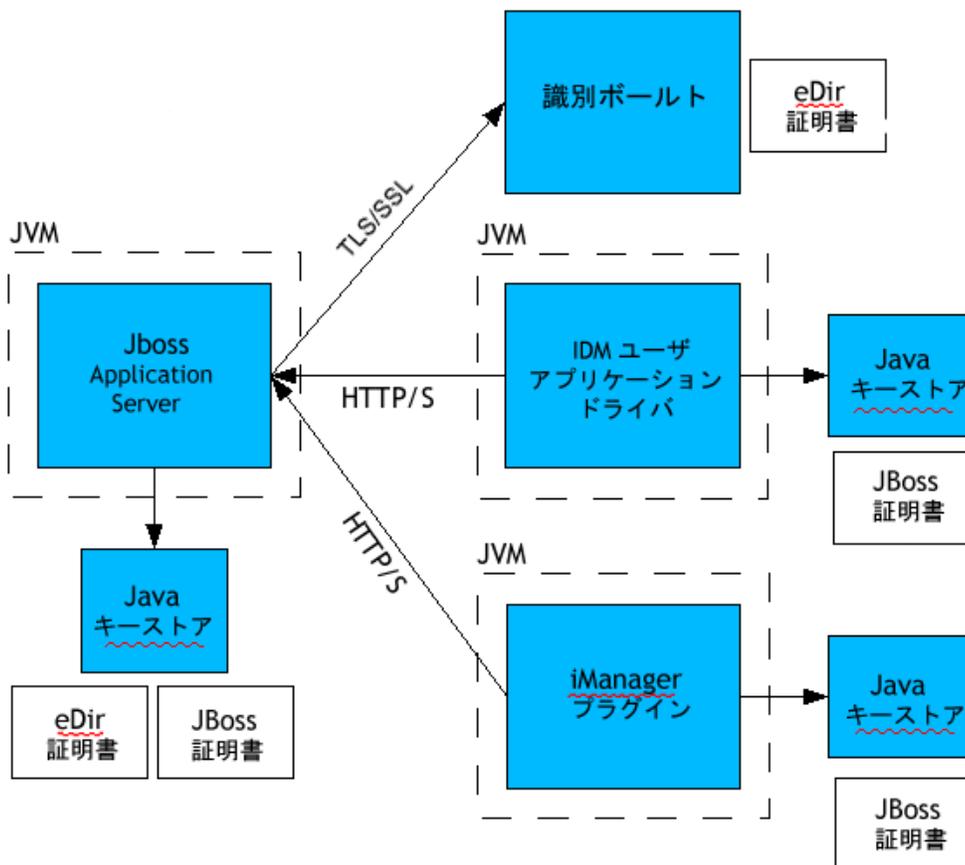
す。もう1つの方法は、元の ACME ツリー上の必要な部分を組み合わせた、フィルタリングされたレプリカ (特殊なタイプの eDirectory ツリー) を作成し、そのレプリカのルートコンテナをポイントするという方法です (フィルタリングされたレプリカの詳細については、『Novell eDirectory 管理ガイド』を参照してください)。

特定のシステムレイアウトについてご質問がある場合には、Novell の担当者までお問い合わせください。

2.2 セキュリティ

運用前段階から運用段階に移行するときは、通常、システムのセキュリティ面を強化する必要があります。サンドボックステストで、通常の HTTP を使用してユーザアプリケーションドライバを JBoss に接続したり、ドライバとアプリケーションサーバの通信に (一時的な手段として) 自己署名付き証明書を使用したりしていた場合でも、運用環境では、会社の Verisign (または他の信頼できるプロバイダ) の証明書に基づいたサーバ認証による安全な接続を使用する必要があります。

Identity Manager のユーザアプリケーション環境では、次の図のようにさまざまな部分で X.509 証明書が使用されます。



デフォルトでは、ユーザアプリケーションとアイデンティティポータル間の通信はすべて、TLS (Transport Layer Security) により保護されます。アイデンティティポータル (eDirectory) 証明書は、インストール時に JBoss キーストアへ自動的にインストールされ

まず、特に指定しない限り、ユーザアプリケーションのインストーラは、eDirectory 証明書のコピーを JRE のデフォルト *cacerts* ストアに保存します。

安全に通信するには、図のようにサーバ証明書を複数の場所に配置する必要があります。図中の *JBoss cert* ボックスが表示されている場所で、自己署名付き証明書を使用するか、Verisign などの認証局 (CA) によって発行された証明書を使用するかに応じて、異なる設定手順が必要です。

自己署名付き証明書

有名な信頼できる認証局 (Verisign など) が発行した証明書を使用する場合には、特別な設定手順は必要ありません。しかし、自己署名付き証明書を作成して使用する場合には、次の手順が必要です。

- 1 次のようなコマンドライン構文を使用して、自己署名付き証明書のキーストアを作成します。

```
keytool -genkey -alias tomcat -keyalg RSA -storepass changeit -
keystore jboss.jks -dname
"cn=JBoss,ou=exteNd,o=Novell,l=Waltham,s=MA,c=US" -keypass
changeit
```

証明書のほかに「jboss.jks」というファイルも作成します。

- 2 キーストアファイル (jboss.jks) を次の例のような JBoss ユーザアプリケーションディレクトリにコピーします。

```
cp jboss.jks ~/jboss-4.0.2/server/spitfire/conf
```

JBoss での SSL の有効化

JBoss で SSL を有効にするには、*[IDM]/jboss/server/IDM/deploy/* から *jbossweb-tomcat55.sar* ファイルを探し、このファイルから *server.xml* を見つけ、テキストエディタでファイルを開きます。次のセクションをアンコメントするか追加して、SSL を有効にします。

```
<Connector port="8443" address="${jboss.bind.address}"
maxThreads="100" strategy="ms" maxHttpHeaderSize="8192"
emptySessionPath="true" scheme="https" secure="true"
clientAuth="false" keystoreFile="${jboss.server.home.dir}/spitfire/
conf/jboss.jks" keystorePass="changeit" sslProtocol = "TLS" />
```

SOAP セキュリティの有効化

IDM.war で *web.xml* ファイルを見つければ、テキストエディタで開きます。ファイルの最後の方にある次のセクションをアンコメントします。

```
<security-constraint> <web-resource-collection> <web-resource-
name>IDMProv</web-resource-name> <url-pattern>/*</url-pattern> <http-
method>POST</http-method> <http-method>GET</http-method>
<description>IDM Provisioning Edition</description> </web-resource-
collection> <user-data-constraint> <transport-guarantee>CONFIDENTIAL</
```

```
transport guarantee> </user-data-constraint> </security-constraint>
```

ファイルとアーカイブを保存してから JBoss を再起動します。

2.2.1 相互認証

Identity Manager のユーザアプリケーションは、従来のサーバ認証シナリオをサポートしていますが (Web 上のセキュア Web ページを用いた https セッションで一般的に使用されています)、双方向の証明書ベース認証は、初期状態ではサポートしていません。ただし、Novell iChain を使用することにより、この機能を入手できます。このため、たとえば組織でパスワードではなくユーザ証明書でユーザがログインできるようにする必要がある場合、iChain を環境に追加することでこの機能を実現できます。

詳細については、Novell の担当者までお問い合わせください。

2.3 パフォーマンスの調整

パフォーマンスの調整は複雑な課題です。Identity Manager ユーザアプリケーションは、さまざまな対話を行う幅広いテクノロジーに依存しています。パフォーマンスの低下を招くような設定シナリオやユーザ対話シナリオをすべて予測することは不可能です。それでもなお、サブシステムの中にはパフォーマンスを飛躍的に向上できるベストプラクティスとなり得るものもあります。詳細については、次を参照してください。

2.3.1 ログ

ユーザアプリケーションでは、Novell Audit によるログと、オープンソースの Apache *log4j* フレームワークによるログが可能です。デフォルトでは Novell Audit によるログは無効になっています。これに対し、*log4j* によるファイルとコンソールのログはデフォルトで有効になっています。

注：ログが可能なイベントの種類、およびログの有効/無効の切り替えについては、このガイド後半の [119 ページの第 5 章「ログの設定」](#) と [213 ページの第 12 章「ログの環境設定」](#) を参照してください。

log4j の設定は `$IDMINSTALL/jboss/server/IDMProv/conf/` の中にある `log4j.xml` というファイルに含まれています。このファイルの下部に、次のエントリがあります。

```
<root>      <priority value="INFO" />      <appender-ref ref="CONSOLE" />
>      <appender-ref ref="FILE" /> </root>
```

root 内に値を割り当てると、レベルが明示的に割り当てられていないログアペンダはすべて root に指定されたログレベル (この場合は INFO) を継承します。たとえば、デフォルトでは FILE アペンダにはしきい値レベルが割り当てられていないため、ルートのしきい値レベルを引き継ぎます。

log4j で使用されるログレベルは DEBUG、INFO、WARN、ERROR、および FATAL で、これは `org.apache.log4j.Level` クラスで定義されています。これらの設定を適切に使用しないと、パフォーマンスの面で問題が発生する可能性があります。

概して、INFO や DEBUG は特定の問題をデバッグするときだけに使用すべきです。

ルートに含まれるアペンダに特定のしきい値レベルが設定されていない場合、デバッグを行うとき以外(すでに説明したように)、しきい値を ERROR、WARN、または FATAL に設定する必要があります。

ログレベルが高いときのパフォーマンスは、メッセージの冗長性とはほとんど関係なく、*log4j* ではコンソールとファイルのログが同時書き込みに関与しているという単純な事実に影響されます。AsyncAppender クラスを使用できますが、このクラスを使用してもパフォーマンスの向上が保証されるわけではありません。この問題 (Apache *log4j* の既知の問題で、Identity Manager の問題ではありません) については、「<http://logging.apache.org/log4j/docs/api-1.2.8/org/apache/log4j/performance/Logging.html>」を参照してください。

ユーザアプリケーションのログ設定ファイルのデフォルトのレベルである INFO(前述) は、多くの環境で問題になりませんが、パフォーマンスが重要な環境では先ほどの *log4j.xml* のエントリを次のように変更する必要があります。

```
<root> <priority value="ERROR"/> <appender-ref ref="FILE"/> </root>
```

つまり、CONSOLE を削除し、ログレベルを ERROR に設定します。完全にテストおよびデバッグされた運用環境では、INFO レベルでのログは必要ありません。また、CONSOLE のログを有効にする必要もありません。これらのログを無効にするとパフォーマンスが大きく向上します。

log4j の詳細については、<http://logging.apache.org/log4j/docs> のドキュメントを参照してください。

Identity Manager で Novell Audit を使用する際の詳細については、『Novell Identity Manager 管理ガイド』を参照してください。

2.3.2 アイデンティティポールド

利用頻度の高いディレクトリサーバ環境では、LDAP クエリがボトルネックになる可能性があります。Novell eDirectory (Identity Manager のアイデンティティポールドのベース) は、オブジェクトが多数でも高いレベルのパフォーマンスを維持するために、頻繁に要求される情報を記録し、インデックスに保存します。複雑なクエリでも、インデックス化された属性を持つオブジェクトに対して実行した場合には、応答は高速になります。

eDirectory では、初期状態で、次の属性がインデックス化されています。

```
Aliased Object Name cn dc Equivalent to Me extensionInfo Given Name  
GUID ldapAttributeList ldapClassList Member NLS:Common Certificate  
Obituary Reference Revision Surname uniqueID uniqueID_SS
```

Identity Manager をインストールすると、デフォルトのディレクトリスキーマが、ユーザアプリケーションに関する新しい *objectclass* タイプと新しい属性で拡張されます。ユーザアプリケーション固有の属性は(デフォルトでは)インデックス化されません。パフォーマンスを向上させるため、特に 5,000 以上のオブジェクトがユーザコンテナに含まれる場合には、こうした属性の一部(また必要に応じて従来の LDAP 属性のいくつか)をインデックス化できます。

考え方としては、定期的にクエリされることが分かっている属性だけをインデックス化します(定期的にクエリされる属性は運用環境によって大きく異なります)。どの属性が頻繁に使用されるかを見極める唯一の方法は、ランタイム時に述語統計を収集することです(ただし、収集プロセス自体はパフォーマンスを低下させます)。

述語統計の収集プロセスの詳細については、『eDirectory 管理ガイド』を参照してください。このガイドではインデックス化についても詳しく解説しています。一般的には、次の作業が必要です。

- ◆ Console One を使用して、該当する属性の述語統計の収集を開始する
- ◆ システムに負荷をかける
- ◆ 統計の収集を無効にして結果を分析する
- ◆ インデックス化しておくると便利な各属性のインデックスを作成する

インデックス化する属性がわかっている場合は、Console One を使用する必要はありません。インデックスを作成し管理するには、iManager で [eDirectory の保守] > [Indexes (インデックス)] の順にクリックします。たとえば、組織図のユーザが *isManager* 属性に基づいて検索することがわかっている場合は、その属性をインデックス化し、パフォーマンスが向上するかどうかを確かめることができます。

注: ベストプラクティスとして、最低限 *manager* 属性および *isManager* 属性をインデックス化することをお勧めします。

属性のインデックス化とパフォーマンスの詳細については、Peter Kuo と Jim Henderson 共著の『Novell's Guide to Troubleshooting eDirectory』(QUE Books, ISBN 0-7897-3146-0)の「Tuning eDirectory」を参照してください。

『eDirectory 管理ガイド』の「Novell eDirectory のメンテナンス」の章に記載されているパフォーマンス調整に関する記述も参照してください。

2.3.3 JVM

Java 仮想マシンに割り当てられるヒープメモリの量はパフォーマンスに影響することがあります。最小メモリ値や最大メモリ値の設定値が低すぎたり高すぎたりすると(「高すぎる」とはコンピュータの物理メモリより多いことを意味します)、ページファイルのスワッピングが過剰に発生する可能性があります。

JBoss サーバの最大 JVM サイズを設定するには、[IDM]/jboss/bin/にある `run.conf` ファイルまたは `run.bat` ファイル(前者は Linux 用、後者は Windows 用)をテキストエディタで編集します。「-Xmx」を `128m` から `512m` またはそれ以上に増やします。ご使用の環境に最適な設定が見つかるまで、調整を繰り返さなければならない場合があります。

注: JBoss および Tomcat のパフォーマンス調整のヒントについては、<http://wiki.jboss.org/wiki/Wiki.jsp?page=JBossASTuningSliming> (<http://wiki.jboss.org/wiki/Wiki.jsp?page=JBossASTuningSliming>) を参照してください。

2.3.4 セッションタイムアウト値

セッションタイムアウト(ユーザが Web ブラウザのページを表示したままにしてから、サーバによってセッションタイムアウトの警告ダイアログが表示されるまでの時間)は、`IDM.war` アーカイブの `web.xml` ファイルで変更できます。この値は、アプリケーションが

実行されるサーバおよび使用環境に合わせて調整する必要があります。一般に、セッションタイムアウト値は実用上差し支えのない限り小さくすることをお勧めします。業務の要件から5分のセッションタイムアウトが可能であれば、サーバはタイムアウト値が10分だった場合よりも2倍早く未使用のリソースを開放できます。これにより Web アプリケーションのパフォーマンスとスケーラビリティが向上します。

セッションタイムアウト値を調整するときは次の点を考慮してください。

- ◆ セッションタイムアウトの時間が長いと、短時間に大勢のユーザがログインした場合、JBoss サーバのメモリが不足する可能性があります。これは、開かれたセッションが多すぎれば、どのアプリケーションサーバでも起こり得ます。
- ◆ ユーザがユーザアプリケーションにログインすると、そのユーザの LDAP 接続が作成されてセッションにバインドされます。このため、開かれたセッションが多いほど、保持される LDAP 接続の数が多くなります。セッションタイムアウトまでの時間が長いほど、こうした接続が開いたままになっている時間が長くなります。LDAP サーバに対して開いている接続が多すぎると、(接続がアイドル状態であっても)システムのパフォーマンスが低下する可能性があります。
- ◆ サーバおよび使用環境のJVMヒープおよびガーベージコレクション調整パラメータが最適化されているにもかかわらず、サーバで `OutOfMemoryErrors` が発生するようになったら、セッションタイムアウト値を低くしてみてください。

セッションタイムアウト値を調整するには、`IDM.war` アーカイブを開いて `web.xml` ファイルを見つけ、ファイルの次の部分を編集する必要があります(デフォルト値である数値の20は、20分を表します)。

```
<session-config>           <session-timeout>20</session-timeout> </session-config>
```

ファイルとアーカイブを保存し、サーバを再起動します。

注: Web アーカイブファイルの手動編集は、Java Web アプリケーションの開発と展開に熟練したユーザが行ってください。

2.4 クラスタリング

クラスタ環境でユーザアプリケーションを使用する場合、次の3つの点を考慮してください。

- ◆ JBoss クラスタの設定 (45 ページのセクション 2.4.1「JBoss のクラスタリング」を参照)
- ◆ ユーザアプリケーションのキャッシングの設定 (51 ページのセクション 2.4.3「ユーザアプリケーションクラスタグループのキャッシング設定」を参照)
- ◆ ワークフローエンジンの設定 (51 ページのセクション 2.4.4「クラスタリング用のワークフローの設定」を参照)

2.4.1 JBoss のクラスタリング

クラスタとは、一連のサービスを提供するアプリケーションサーバノードの集まりです。クラスタの目的は、アプリケーションのパフォーマンスと信頼性を高めることにありま

す。一般的に、クラスタはエンタープライズアプリケーションに次の3つの利点をもたらします。

- ◆ 高可用性
- ◆ スケーラビリティ (容量の増加)
- ◆ 負荷分散

高可用性とは、アプリケーションの信頼性が高く、展開されている間高い割合で使用できることを意味します。クラスタでは同じアプリケーションがすべてのノードで実行されるため、高可用性が実現します。1つのノードでエラーが発生しても、他のノードではアプリケーションが引き続き実行されています。Identity Manager ユーザアプリケーションをクラスタで実行すると、高可用性の利点を享受できます。ただし、Identity Manager のユーザアプリケーションは、HTTPセッションのレプリケーションはサポートしていません。つまり、あるノードに処理中のセッションがあり、そのノードでエラーが発生すると、セッション情報は失われます。

負荷分散はクラスタのメンバー間で作業負荷を分散する方法です。負荷分散の目的は、パフォーマンスを向上させることです。負荷分散はさまざまな方法で実現できます (DNS ラウンドロビン、ハードウェア負荷分散など)。負荷分散の各方法の詳細については、<http://www.onjava.com/pub/a/onjava/2001/09/26/load.html> (<http://www.onjava.com/pub/a/onjava/2001/09/26/load.html>) を参照してください。どのような方法を取るにせよ、クラスタ設定には負荷分散機能を含めることをお勧めします。

JBoss クラスタグループ

JBoss クラスタは JGroups という通信モジュールをベースにしています。JGroups は JBoss と同時にインストールされます (JBoss がなくても使用できます)。JGroups はグループ間の通信を提供し、これによって共通の名前、マルチキャストアドレス、およびマルチキャストポートを共有します。

クラスタ化された JBoss サーバをインストールすると、クラスタを管理するための JGroups グループが JBoss によって2つ定義されます。1つは *DefaultPartition* と呼ばれ、`/deploy/cluster-service.xml` で定義されます。このクラスタグループは JBoss によって使用され、核となるクラスタリングサービスを提供します。また、JBoss は2つ目のクラスタグループとして *Tomcat-Cluster* を定義します。このクラスタグループは `/deploy/tc-cluster-service.xml` で定義され、JBoss の内部で実行される Tomcat サーバにセッションレプリケーションを提供します。

Identity Manager ユーザアプリケーションは3番目のクラスタグループを使用します。このクラスタグループは UUID 名を使用することで、ユーザがサーバに追加する他のクラスタグループとの衝突リスクを最小限に抑えます。デフォルトでは、クラスタグループは `c373e901aba5e8ee9966444553544200` という名前が付けられています。このクラスタは JBoss サービスファイルを使用して設定されていません。その代わりに、設定はディレクトリに存在し、ユーザアプリケーションの管理機能で設定できます。JGroups および JBoss のクラスタリングに精通しているユーザは、このインタフェースを使用してユーザアプリケーションのクラスタ設定を調整できます。クラスタ設定の変更をサーバノードに適用するには、そのサーバノードを再起動する必要があります。

ユーザアプリケーションのクラスタグループは、クラスタ環境でユーザアプリケーションのキャッシュを調整する目的でのみ使用されます。ユーザアプリケーションのクラスタグループは2つの JBoss クラスタグループとは無関係で、それらのグループとは全く連携しません。ユーザアプリケーションのクラスタグループと2つの JBoss グループは、異なる

グループ名、マルチキャストアドレス、およびマルチキャストポートをデフォルトで使用するため、設定し直す必要はありません。

ユーザアプリケーションのクラスタグループの設定は、ディレクトリ設定を共有する Identity Manager 3 アプリケーションすべてと共有されます。ユーザアプリケーションの管理インタフェースにあるローカル設定オプションは、管理者がクラスタからノードを削除したり、クラスタ内のサーバのメンバーシップを変更したりできるようにする目的で用意されています。たとえば、クラスタリングを全体で無効にしてから、ディレクトリ設定を共有するサーバのサブセットに対してローカルでクラスタリングを有効にすることができます。

アプリケーションのファームिंग

JBoss ではクラスタ全体にホットデプロイが可能です。これを行うには、クラスタ化された JBoss インスタンスのファームディレクトリにアプリケーション EAR、WAR、または JAR をコピーします。1 台のコンピュータでホットデプロイを実行すると、そのコンポーネントはクラスタ内の全インスタンスに自動的に展開されます。その間、クラスタは実行を続けます。

JBoss アプリケーションサーバのバージョン 4.0.2 (このマニュアルの執筆時点でユーザアプリケーションのインストールプログラムに付属) には、使用法に関して未解決の問題があるため、このバージョンを使用したホットデプロイによるアプリケーション展開はお勧めできません。ただし、このマニュアルの発行後にこの技術が改善される可能性があるため、JBoss ファームング技術を使用してユーザアプリケーションを正常に展開するために必要な手順について説明しています (50 ページの「JBoss ファームングを使用したクラスタへのユーザアプリケーションの展開」を参照)。

MySQL データベース

ユーザアプリケーションのインストールプログラムは、ユーザアプリケーションで使用できるように MySQL データベースマネージャをインストールしてデータベースを作成するか、既存の Oracle、Microsoft SQL Server、または MySQL を使用します。データベースはデータの永続性を維持する役割を果たします。JBoss クラスタのノードはすべて、同じデータベースインスタンスにアクセスする必要があります。ユーザアプリケーションは標準の JDBC コールを使用してデータベースのアクセスや更新を行います。ユーザアプリケーションは、JNDI ツリーにバインドされた JDBC データソースを使用してデータベースへの接続を開きます。ユーザアプリケーションのインストールプログラムを使用して JBoss クラスタを作成した場合、データソースは自動的にインストールされます。JBoss クラスタを手動で設定する場合は、クラスタ内の全ノードで展開ディレクトリにデータソースファイル (IDM-ds.xml) をコピーする必要があります。また、MySQL を使用している場合は、JBoss /server/IDM/lib ディレクトリにある MySQL JDBC ドライバ (*mysql-connector-java-3.1.10-utf8-clob-fix-bin.jar*) を JBoss の server/IDM/lib ディレクトリにコピーする必要があります。

ログ

クラスタのログを有効にするには、JBoss サーバ設定の \conf ディレクトリ (例: \server\IDM\conf) にある log4j.xml 設定ファイルを編集し、ファイルの最後の方にある次のようなセクションをアンコメントする必要があります。

```
<!-- Clustering logging --> - <!-- Uncomment the following to redirect
the org.jgroups and org.jboss.ha categories to a cluster.log
file.<appender name="CLUSTER"
```

```

class="org.jboss.logging.appender.RollingFileAppender"> <errorHandler
class="org.jboss.logging.util.OnlyOnceErrorHandler"/> <param
name="File" value="{jboss.server.home.dir}/log cluster.log"/> <param
name="Append" value="false"/> <param name="MaxFileSize" value="500KB"/
> <param name="MaxBackupIndex" value="1"/> <layout
class="org.apache.log4j.PatternLayout"> <param
name="ConversionPattern" value="%d %-5p [%c] %m%n"/> </layout> </
appender> <category name="org.jgroups"> <priority value="DEBUG" />
<appender-ref ref="CLUSTER"/> </category> <category
name="org.jboss.ha"> <priority value="DEBUG" /> <appender-ref
ref="CLUSTER"/> </category> -->

```

cluster.log ファイルは、JBoss サーバ設定の *log* ディレクトリ (例: *\server\IDM\log*) にあります。

2.4.2 JBoss クラスタへのユーザアプリケーションのインストール

クラスタにユーザアプリケーションをインストールする場合は、ユーザアプリケーションのインストールプログラムを使用してクラスタ内の各ノードにユーザアプリケーションをインストールすることをお勧めします。JBoss フェーリングを使用してクラスタにユーザアプリケーションを展開することはお勧めしませんが、代替手段としてその手順を説明しておきます。

クラスタ内の各ノードでのユーザアプリケーションのインストールプログラムの使用

JBoss には、*minimal*、*default*、および *all* という 3 種類の既製のサーバ設定が付属しています。クラスタリングは *all* の設定でのみ有効になります。*/deploy* フォルダにある *cluster-service.xml* ファイルには、デフォルトのクラスタパーティションの設定が記述されています。ユーザアプリケーションのインストール時に、インストールプログラムでクラスタにインストールするよう指定すると、インストールプログラムはすべての設定のコピーを作成し、そのコピーに *IDM* という名前を付けます (これはデフォルト設定です。インストールプログラムを使用して名前を変更できます)。それからこの設定にユーザアプリケーションをインストールします。

ユーザアプリケーションのインストールプログラムを使用して、クラスタ内の各ノードにユーザアプリケーションをインストールするには：

- 1 番目の JBoss ノードでユーザアプリケーションの完全インストール (MySQL、JBoss、およびユーザアプリケーション) を実行します。ユーザアプリケーションのインストールプログラムを使用する際の詳細については、『Identity Manager 3 インストールガイド』を参照してください。
 - ユーザアプリケーションのデータベースとして MySQL を使用すると、ユーザアプリケーションのインストールプログラムによって、MySQL が新しくインストールされます。指定した MySQL の root ユーザのパスワードを記録しておきます。この情報は、クラスタ内の残りのノードにユーザアプリケーションをインストールするときに必要になります。
 - インストールプログラムの [IDM Configuration (IDM 構成)] 画面で、[clustering (all) (クラスタリング (すべて))] オプションを選択します。
 - 環境に合わせて、他のインストールオプションを選択します。

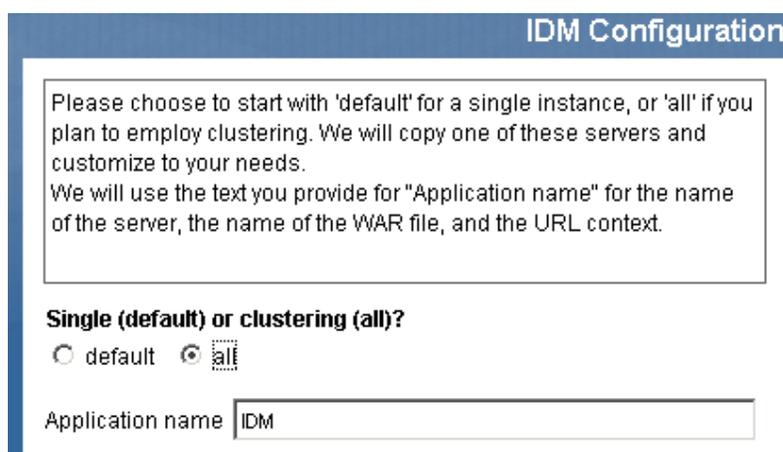
- 2 MySQL がまだ実行されていない場合は、/IDM/mysql ディレクトリにある *start-mysql.bat* ファイルを使用して MySQL を起動します。

注: Linux では、次のシェルコマンドを使用して MySQL デーモンが実行されているかどうかを判断できます。

```
ps -A | grep mysqld
```

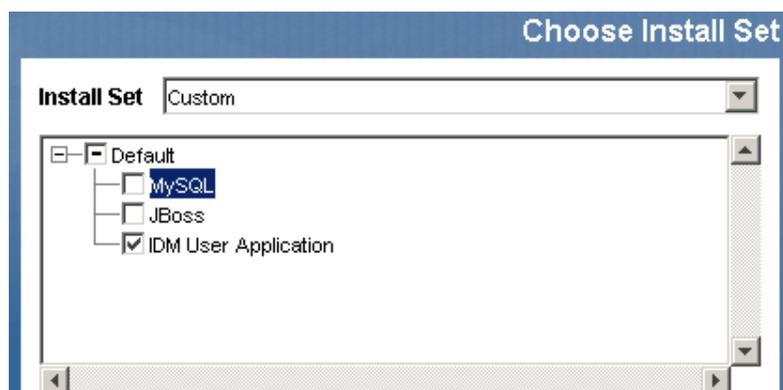
このコマンドにより `mysqld` で終わる複数の行が返されれば、このデーモンは実行されています。

- 3 IDM ディレクトリにある *start-jboss.bat* (Windows) ファイルまたは *start-jboss.sh* (Linux) ファイルを使用して JBoss とユーザアプリケーションを起動します。



- 4 JBoss クラスタ内に追加された各ノードに対して、ユーザアプリケーションのカスタムインストールを実行します。

- ユーザアプリケーションだけを選択してインストールします。



- ユーザアプリケーションのデータベースをインストールするサーバのIPアドレスまたはホスト名を指定します。
- ユーザアプリケーションデータベースのデータベースユーザ名とパスワードを指定します。MySQL を使用している場合は、ユーザ名は `root`、パスワードはインストール処理中に **ステップ 1** で指定したパスワードになります。

- ◆ インストールプログラムの [IDM Configuration (IDM 構成)] 画面で、[clustering (all) (クラスタリング (すべて))] オプションを選択します。
 - ◆ 環境に合わせて、他のインストールオプションを選択します。
- 5 IDM ディレクトリにある *start-jboss.bat* (Windows) または *start-jboss.sh* (Linux) を使用して JBoss クラスタの各ノードを起動します。

JBoss ファーミングを使用したクラスタへのユーザアプリケーションの展開

問題が発生するおそれがあるため、JBoss バージョン 4.0.2 以前では JBoss ファーミングを使用しないでください (詳細については、<http://jira.jboss.com/jira/browse/JBAS-1899> (<http://jira.jboss.com/jira/browse/JBAS-1899>) を参照してください)。ユーザアプリケーションのインストールプログラムを使用して、クラスタ内の各ノードにユーザアプリケーションをインストールすることをお勧めします (詳細については、この章の 48 ページの「**クラスタ内の各ノードでのユーザアプリケーションのインストールプログラムの使用**」を参照してください)。ただし、JBoss 4.0.3 以降でファーミングを使用して JBoss クラスタにユーザアプリケーションを展開する場合は、次の手順に従います。

注：次の内容は、自己責任で試験的に JBoss 4.0.3 を使用することを望むユーザのための手順です。公式にサポートされているバージョンは 4.0.2 です。

JBoss ファーミングを使用してクラスタにユーザアプリケーションを展開するには：

- 1 JBoss クラスタノードの 1 つに対してユーザアプリケーションのカスタムインストールを実行します。ユーザアプリケーションと MySQL (MySQL を使用している場合。それ以外の場合はユーザアプリケーションのみ) をインストールするよう選択します。インストールはノード内のクラスタがすべて実行されている状態で実行できますが、ユーザアプリケーションはクラスタで最初に開始されるノードにインストールしてください。
- 2 /server/IDM/lib ディレクトリにある JDBC ドライバファイル (たとえば、MySQL を使用している場合、JDBC ドライバファイルは *mysql-connector-java-3.1.10-utf8-clob-fix-bin.jar*) をクラスタの各ノードにある対応するディレクトリにコピーします。
- 3 ユーザアプリケーションと同時にインストールされた *cacerts* ファイルを JRE の /lib/security ディレクトリから、クラスタの各ノードにある JRE の /lib/security ディレクトリにコピーします。
- 4 IDM.war ファイルと IDM-ds.xml データソースファイルを、サーバ設定ディレクトリの /deploy ディレクトリから、サーバ設定ディレクトリの /farm ディレクトリに移動します。ファイルは実際に移動してください。元のファイルを /deploy ディレクトリに残さないでください。
- 5 ユーザアプリケーションのデータベースを起動します (付属の MySQL を使用する場合は、/IDM/mysql ディレクトリにある *start-mysql.bat* ファイルを使用して MySQL を起動します)。
- 6 ユーザアプリケーションとユーザアプリケーションのデータベースをインストールしたノードの IDM ディレクトリにある *start-jboss.bat* (Windows) または *start-jboss.sh* (Linux) を使用して JBoss とユーザアプリケーションを起動します。
- 7 クラスタ内の他のノードを起動します。

2.4.3 ユーザアプリケーションクラスタグループのキャッシング設定

JGroups および JBoss クラスタリングに精通しているユーザは、ユーザアプリケーションの管理ユーザインタフェースを使用してクラスタグループのキャッシング設定を変更できます (226 ページのセクション 13.3.5 「クラスタのキャッシュ設定」を参照してください)。クラスタ設定の変更をサーバノードに適用するには、そのサーバノードを再起動する必要があります。

2.4.4 クラスタリング用のワークフローの設定

ワークフローエンジンのクラスタリングは、ユーザアプリケーションのキャッシュフレームワークとは無関係に動作します。クラスタ環境でワークフローエンジンを正常に動作させるには、いくつかの手順を実行する必要があります。

- ◆ クラスタ内のサーバはすべて同じデータベースをポイントしている必要があります。これには、推奨された方法を使用してクラスタにユーザアプリケーションをインストールした場合 (48 ページの 「クラスタ内の各ノードでのユーザアプリケーションのインストールプログラムの使用」を参照)、インストールプロセス中に、そのユーザアプリケーション用のデータベースをインストールしたサーバの IP アドレスとホスト名を指定します。ファームリングを使用してクラスタノードにユーザアプリケーションを展開した場合 (50 ページの 「JBoss ファームリングを使用したクラスタへのユーザアプリケーションの展開」を参照) は、/deploy ディレクトリのデータソースファイル (IDM-ds.xml) を、ユーザアプリケーションを最初にインストールしたノードにある /farm ディレクトリに移動します。これにより、クラスタ内のすべてのノードにデータソースが展開されます。
- ◆ クラスタ内の各サーバは固有のエンジン ID で起動する必要があります。このために、サーバの起動時に `com.novell.afw.wf.engine-id` のシステムプロパティを設定します。たとえば、JBoss を起動して、サーバのワークフローエンジンにエンジン ID として ENGINE1 を割り当てる場合は、次のコマンドを使用します。

```
run.sh -Dcom.novell.afw.wf.engine-id=ENGINE1 (Linux)
```

```
run.bat -Dcom.novell.afw.wf.engine-id=ENGINE1 (Windows)
```

特定のサーバで実行されているワークフローエンジンによりワークフロープロセスのインスタンスが起動されると、ワークフロープロセスはそのサーバでのみ実行および完了できます。これにより、ワークフロープロセスが安全に実行されます。ただし、プロセスインスタンスのフェールオーバーはサポートされていません。クラスタ内のサーバがクラッシュした場合、同じ ID を持つエンジンが再起動されるまでプロセスインスタンスは再起動されません。

ハードウェアやソフトウェアに深刻な問題が発生したためにサーバコンピュータが再起動できない場合は、別のコンピュータでアプリケーションサーバを起動できます。この場合は復旧できないコンピュータで使用されていたのと同じワークフローエンジン ID を使用します。エンジン ID は論理名であり、エンジンが実行されていた物理コンピュータに対する直接マッピングではないため、中断されたプロセスインスタンスは代替りのコンピュータで正常に完了します。

プロセスインスタンスは、プロセスを起動したエンジンが所有しています。ただし、ユーザがクラスタ内の任意のユーザアプリケーションにログオンして、プロセスの詳細を表示したり、プロセスを一時停止したり、またはプロセスに割り当てられたタスクを完了したりできます。プロセスを所有しないエンジン上で一時停止されたプロセスや完了されたタ

スクは保留状態になり、それらを所有するエンジンによって検出されると実行が再開されます。

ユーザアプリケーション環境の設定



次の章では、Identity Manager ユーザアプリケーション環境のさまざまな要素を組織のニーズに合わせて設定する方法について説明します。

- ◆ 55 ページの第 3 章「ユーザアプリケーションドライバの設定」
- ◆ 75 ページの第 4 章「ディレクトリ抽出化レイヤの設定」
- ◆ 119 ページの第 5 章「ログの設定」

ユーザアプリケーションドライバの設定

3.1 ユーザアプリケーションドライバについて

ユーザアプリケーションドライバは、プロビジョニングワークフローを開始する役割と、アイデンティティポールの変更 (たとえば、Designer for Identity Manager を使用してディレクトリ抽象化レイヤを変更した場合) をユーザアプリケーションに通知する役割を果たします。このドライバでは購読者チャンネルだけが使用されます。このドライバは、アイデンティティプールからユーザアプリケーション (アプリケーションサーバで実行) へのメッセージを処理します。ユーザアプリケーションで発生するイベントで、アイデンティティプールに返されるイベントもありますが、こうしたイベントはユーザアプリケーションドライバの発行者チャンネルを使用しません。

アプリケーションサーバが起動すると、ドライバはアプリケーションサーバとのセッションを確立します。ドライバは、アプリケーションサーバで実行されているユーザアプリケーションにメッセージを送信します (たとえば「仮想ディレクトリ定義の新しいセットを取得する」など)。

ドライバのソースコンポーネントは次のとおりです。

- ◆ **ComposerDriverShim.jar** – Composer ドライバシムです。Windows では lib ディレクトリ (`\Novell\NDS\lib`) に、Linux では classes ディレクトリ (`/usr/lib/dirxml/classes`) にインストールされます。
- ◆ **srvprvUAD.jar** – アプリケーションドライバシムです。Windows では lib ディレクトリ (`\Novell\NDS\lib`) に、Linux では classes ディレクトリ (`/usr/lib/dirxml/classes`) にインストールされます。
- ◆ **UserApplicationDriver.xml** - 新しいドライバをセットアップするための事前設定データが含まれたファイルです。このファイルは DirXML.Drivers ディレクトリ (Windows では `\Tomcat\webapps\nps\DirXML.Drivers`、Linux では `/usr/lib/dirxml/rules/DirXML.Drivers`) にインストールされます。

ユーザアプリケーションドライバコンポーネントは、Identity Manager 3 のインストール時にインストールされます。Identity Manager 3 のユーザアプリケーションを実行するには、新規または既存のドライバセットにユーザアプリケーションドライバを追加し、ドライバのアクティブ化を行う必要があります。

ユーザの作業環境によっては、ユーザアプリケーションドライバの設定がほとんど必要ない場合も、ドライバポリシーに複雑な業務ルールのセットを実装することが必要になる場合もあります。ユーザアプリケーションドライバは Identity Manager の他のドライバと同じく、柔軟なデータ同期メカニズムを備えています。

この章では、ユーザアプリケーションドライバの作成、設定、および起動方法、またアイデンティティプール内のイベントに基づいてワークフローが自動的に開始されるようドライバを設定する方法について説明します。この章は次の節で構成されています。

- ◆ [56 ページのセクション 3.2 「ユーザアプリケーションドライバの作成」](#)

- 62 ページのセクション 3.3 「ユーザアプリケーションドライバの起動」
- 63 ページのセクション 3.4 「ワークフローの自動起動の設定」

3.2 ユーザアプリケーションドライバの作成

ドライバを作成するには：

- 1 アイデンティティポータルを管理する iManager のインスタンスにログインします。
- 2 iManager のナビゲーションフレームにある [Identity Manager ユーティリティ] ノードを開きます。



- 3 [新規ドライバ] をクリックします。ドライバ作成ウィザードが表示されます。

Create Driver ?

Welcome to the Create Driver Wizard

The Identity Manager product includes all product components. The drivers you are authorized to deploy are determined by the drivers you have purchased.

Application drivers are contained in a driver set. When you create a driver, make sure that the server associated with the driver set contains a non-filtered writable replica of the partition that contains the driver set. If it does not, then a read/write replica will be added or the existing replica will be converted to read/write.

Where do you want to place the new driver?

In an existing driver set
driverset.novell

In a new driver set

<< Back Next >> Cancel Finish

次の手順では、新しいドライバを作成する場所を選択します。既存のドライバセットにドライバを作成することもできますし、新しいドライバセットを作成することもできます。

- 4 [既存のドライバの中] を選択すると、アイデンティティポルトを参照してドライバセットを見つけるためのウィザードが表示されます。既存のドライバセットを選択して、[次へ] をクリックします。

[新しいドライバセットの中] を選択した場合は、新しいドライバセットのプロパティを定義する画面が表示されます。ドライバセットの名前、ツリーコンテキスト、およびサーバを指定して、[次へ] をクリックします。

ドライバ作成ウィザードの次の画面が表示されます。

Import or create a new Application Driver for this driver set.

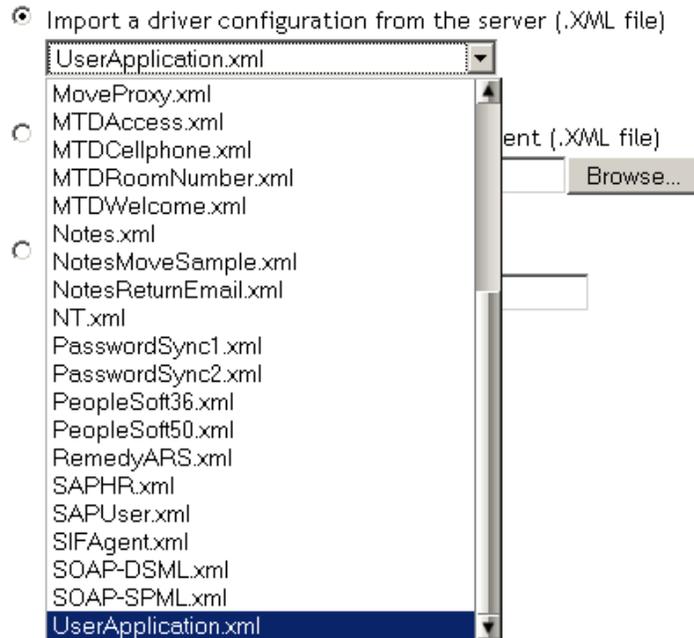
Import a driver configuration from the server (.XML file)

Import a driver configuration from the client (.XML file)
File: Browse...

Create a new driver
Name:

- 5 [サーバからのドライバ環境設定のインポート] をクリックし、XML ファイルのリストから [UserApplication.xml] を選択します。

Import or create a new Application Driver for this driver set.



- 6 [次へ] をクリックします。ドライバ名など、ドライバを設定するためのページが表示されます。

UserApplication (Driver)

The driver writer requested that the following information be supplied in order to import this driver configuration file. An * indicates required information.

The name of the driver contained in the driver configuration file is "UserApplication". Enter the actual name you want to use for the driver.

Driver name: *	Existing drivers:
<input type="text" value="UserApplication"/>	<input type="text" value="<Select an existing driver to update>"/>

ドライバのデフォルト名は UserApplication です。デフォルト名を使用することもできますが、プロジェクトに適した名前を付けることもできます。

- 7 ドライバ名を変更する場合は、[ドライバ名] フィールドに新しい名前を入力します。
- 8 [認証 ID] フィールドに、ドット形式 (admin.orgunit.novell など) でユーザアプリケーション管理者の DN を指定します (ユーザアプリケーション管理者の詳細については [16 ページのセクション 1.1.2 「ユーザアプリケーション管理者」](#) を参照)。
- 9 [アプリケーションパスワード] フィールドおよび [パスワードを再入力] フィールドに、[認証 ID] フィールドで示されるユーザアプリケーション管理者のパスワードを指定します。
- 10 [アプリケーションコンテキスト] フィールドに、ユーザアプリケーションのインストール時に指定したアプリケーション名を入力します。デフォルト名は IDM です。
- 11 [ホスト] フィールドに、ユーザアプリケーションが実行されるアプリケーションサーバのホスト名または IP アドレスを指定します。
- 12 [ポート] フィールドに、アプリケーションサーバで実行されるユーザアプリケーションと通信するためにドライバが使用するポートを指定します (8080 など)。
- 13 [次へ] をクリックします。ドライバ環境設定のインポート中であることを示すメッセージが表示されます。それから、ドライバ作成ウィザードの次のページが表示されます。

UserApplication2 ドライバ:

新しく作成したドライバについて次の作業を行うことをお勧めします:

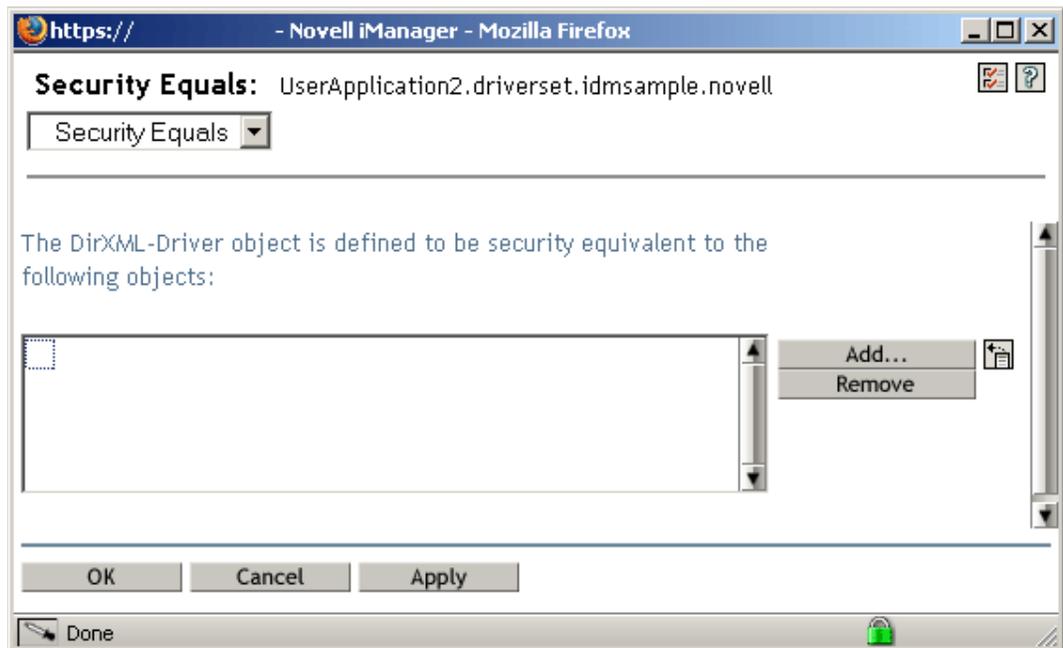
- ドライバの「同等セキュリティ」を定義します。
- 「管理の役割」を表すすべてのオブジェクトを指定して、レプリケーションから除外します。

「同等セキュリティ」の定義

「管理者の役割」の除外

ドライバオブジェクトには、読み書きするオブジェクトに対する適切なアイデンティティボールド権利を付与する必要があります。これを行うには、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。ドライバにはユーザ、ポストオフィス、リソース、および配布リストに対する読み書きの権利、またポストオフィスコンテナに対する作成と読み書きの権利が必要です。通常、ドライバには管理者と同等のセキュリティを付与する必要があります。

- 14 [Define Security Equivalences (同等セキュリティの定義)] をクリックします。新しいウィンドウが表示されます。



- 15 [追加] をクリックします。表示されるウィンドウで、このドライバに割り当てるのに適した権利レベルを持つオブジェクトをツリーから選択します (admin など)。



- 16 適切なレベルのアイデンティティゴールト権利を持つオブジェクトをツリーから選択し、[OK] をクリックします。前のウィンドウに戻ります。
- 17 [OK] をクリックします。ドライバ作成ウィザードに戻ります。

- 18 「管理の役割」の除外 をクリックします。[除外されたユーザ] ウィンドウが表示されます。この機能を使用すると、他のアイデンティティポータルで管理者パスワードが変更され、ユーザアプリケーションドライバが属しているツリーに複製された場合、管理者がそのユーザアプリケーションドライバにログインできなくなることを防ぎます。
- 19 [追加] をクリックします。表示されるウィンドウのディレクトリツリーを参照して、データをドライバに渡さないユーザを探します。ドライバ接続経由で管理者データを複製することは推奨されていないため、通常は管理者オブジェクトを除外します。
- 20 除外する管理者の役割を選択し、[OK] をクリックします。前のウィンドウに戻ります。
- 21 [OK] をクリックします。ドライバ作成ウィザードに戻ります。
- 22 [次へ] をクリックします。ドライバの概要のページが表示されます。
- 23 [概要の終了] をクリックします。アイデンティティポータルにあるドライバがグラフィカル表示されます。



注：この画面は、iManager ナビゲーションツリーの [Identity Manager] にある [Identity Manager の概要] リンクを使用すればいつでも表示できます。

新しいドライバが、アイデンティティポータルトランクに接続された大きいアイコンで表示されます。

3.3 ユーザアプリケーションドライバの起動

ユーザアプリケーションドライバを起動するには：

- 1 iManager ナビゲーションツリーで [Identity Manager] リンクをクリックし、Identity Manager カテゴリで使用できるコマンドを表示します。

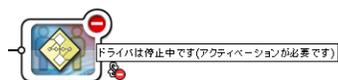


- 2 iManager ナビゲーションツリーにある [Identity Manager] リンクの下に [Identity Manager の概要] リンクをクリックします。

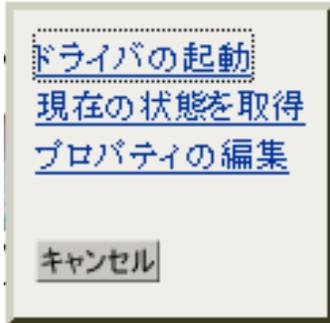


表示されるウィザードでシステムを参照し、起動するドライバが含まれるドライバセットを見つけます。

- 3 ドライバセットを選択し、[次へ] をクリックします。[Identity Manager の概要] ページが表示されます。
- 4 ドライバアイコンの右上隅にある円形のステータスインジケータをクリックします。



ドライバの起動と停止、およびドライバのプロパティの編集に関するコマンドが含まれたメニューが表示されます。



5 [ドライバの起動] をクリックします。

3.4 ワークフローの自動起動の設定

プロビジョニングモジュールがインストールされている場合、ユーザがリソースを要求してプロビジョニング要求を開始したときに、ワークフローが自動的に起動されます。また、Identity Manager のユーザアプリケーションドライバはアイデンティティポータル内のイベントをリッスンし、イベントにตอบสนองして適切なプロビジョニングワークフローを起動します (設定されている場合)。たとえば、アイデンティティポータルに新しいユーザが追加されるとプロビジョニングワークフローが自動起動されるよう、ユーザアプリケーションドライバを設定できます。ユーザアプリケーションドライバがワークフローを自動起動するよう設定するには、Identity Manager のポリシーとルールを使用します。

3.4.1 ポリシーについて

ユーザアプリケーションドライバでも、Identity Manager の他のドライバと同じ方法でフィルタとポリシーを使用できます。アイデンティティポータルでイベントが発生すると、そのイベントを説明する XML ドキュメントが Identity Manager によって作成されます。XML ドキュメントは、チャンネルを通して接続システムに渡されます (この場合、接続システムはユーザアプリケーションです)。ドライバに関連付けられたフィルタやポリシーで、イベントにตอบสนองする方法を定義できます。また、その応答処理中に接続システムが使用できる形式に XML ドキュメントを変換する方法も定義できます。Identity Manager はいくつかのカテゴリのポリシーを提供しています (イベント変換、コマンド変換、スキーママッピング、出力変換など)。これらのポリシーを決められた手順で適用することにより、XML ドキュメントを変換できます。ここでは、アイデンティティポータルのイベントに基づいてワークフローを起動する例を示します。どのポリシーを使用してもワークフローを起動できますが、この例では最も簡単で便利な方法を示します。

ユーザアプリケーションドライバを作成すると、ドライバが使用するためのイベント変換ポリシーが作成されます。イベント変換ポリシーは、残りの購読者チャンネルポリシーで処理される XML ドキュメントを作成する役割を果たします。

注: ユーザアプリケーションドライバの作成時に作成されたイベント変換ポリシーは変更しないでください。このポリシーの DN は Manage.Modify.Subscriber で始まります。このポリシーを変更するとワークフロープロセスが失敗するおそれがあります。

空のスキーママッピングポリシーも作成されます。このポリシーは、アイデンティティボールド内のイベントに基づいてワークフローを起動する際の開始点として使用できます。

3.4.2 アイデンティティボールド内のイベントに基づいて起動されるワークフローの設定

ワークフローを自動起動する最も簡単な方法は、スキーママッピングポリシーエディタを使用する方法です。ユーザアプリケーションドライバでは、この目的のためにユーザが編集できる空のポリシーが用意されています。

スキーママッピングポリシーエディタを使用して、アイデンティティボールドの属性 (eDirectory の `trigger` 属性を含む。この属性が変化するとワークフローが起動します) をターゲットワークフローのランタイムデータにマップします。ランタイムデータは、ワークフロー定義テンプレート (詳細については [325 ページの第 22 章「プロビジョニング要求定義の設定」](#) を参照) によって決定されます。ワークフローが正常に完了するには、ランタイムデータが必要です。アイデンティティボールドを使用するとユーザアプリケーションドライバの動作をカスタマイズできますが、ワークフローが作成されると、そこに多数のグローバル属性が作成されます。グローバル属性は、アイデンティティボールドのどのオブジェクトクラスにも属さない属性です。これらの属性は、`<workflowName>_StartWorkflow`、`<workflowName>_recipient`、および `<workflowName>_reason` という名前になります。常に存在する他の 2 つの属性もあり、これらは `AllWorkflows:reason` および `AllWorkflows:recipient` という名前になります。`_StartWorkflow` 属性はワークフローの起動に使用されます。`_recipient` 属性および `_reason` 属性は、ワークフローに必要なランタイムデータをアイデンティティボールドから受け入れるのに使用されます。

この手順を実行する前に、ワークフローのトリガとして使用するアイデンティティボールド属性の名前を確認しておく必要があります。また、起動するワークフローの名前も確認する必要があります。ワークフローにはすべて、`<workflowName>_StartApprovalFlow` という特別な属性が含まれています。適切な eDirectory 属性をワークフローの `<workflowName>_StartApprovalFlow` 属性にマッピングすることにより、アイデンティティボールド内のイベントに基づいてワークフローが自動起動するよう設定できます。

アイデンティティボールド内のイベントに基づいてワークフローが起動されるように設定するには：

- 1 iManager で、iManager ナビゲーションツリーにある [Identity Manager] の下の [Identity Manager の概要] リンクをクリックします。



[Identity Manager の概要] ページが表示されます。このページでは、ドライバセットを選択するよう求めるメッセージが表示されます。

- 2 [ツリー全体を検索する]、[検索] の順にクリックします。[Identity Manager の概要] ページに、現在選択されているドライバセットのドライバを表すグラフィックが表示されます。

3 ユーザアプリケーションドライバを表す大型のドライバアイコンをクリックします。



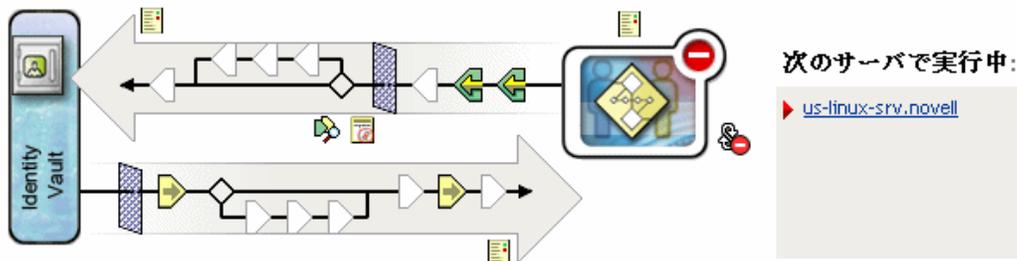
UserApplication

[Identity Manager ドライバの概要] が表示されます。

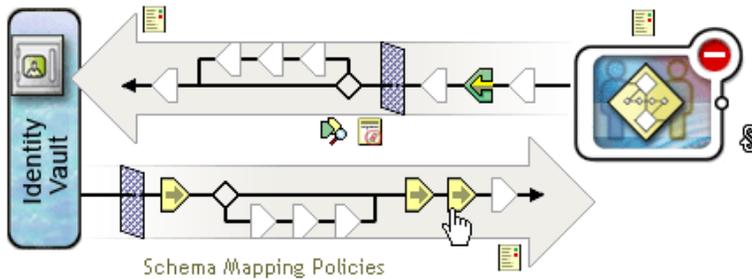
▶ [Identity Managerの概要の選択](#) ▶ [Identity Managerの概要](#)

Identity Managerドライバの概要

ドライバ: UserApplication.drivset.novell アクティベーションが必要です 期限: September 25, 2006



上の左向きの矢印は発行者チャンネル (ユーザアプリケーションドライバでは使用されません) を表し、下の右向きの矢印は購読者チャンネルを表します。グラフィック内のオブジェクトにマウスポインタを置くと、そのオブジェクトの説明が表示されます。

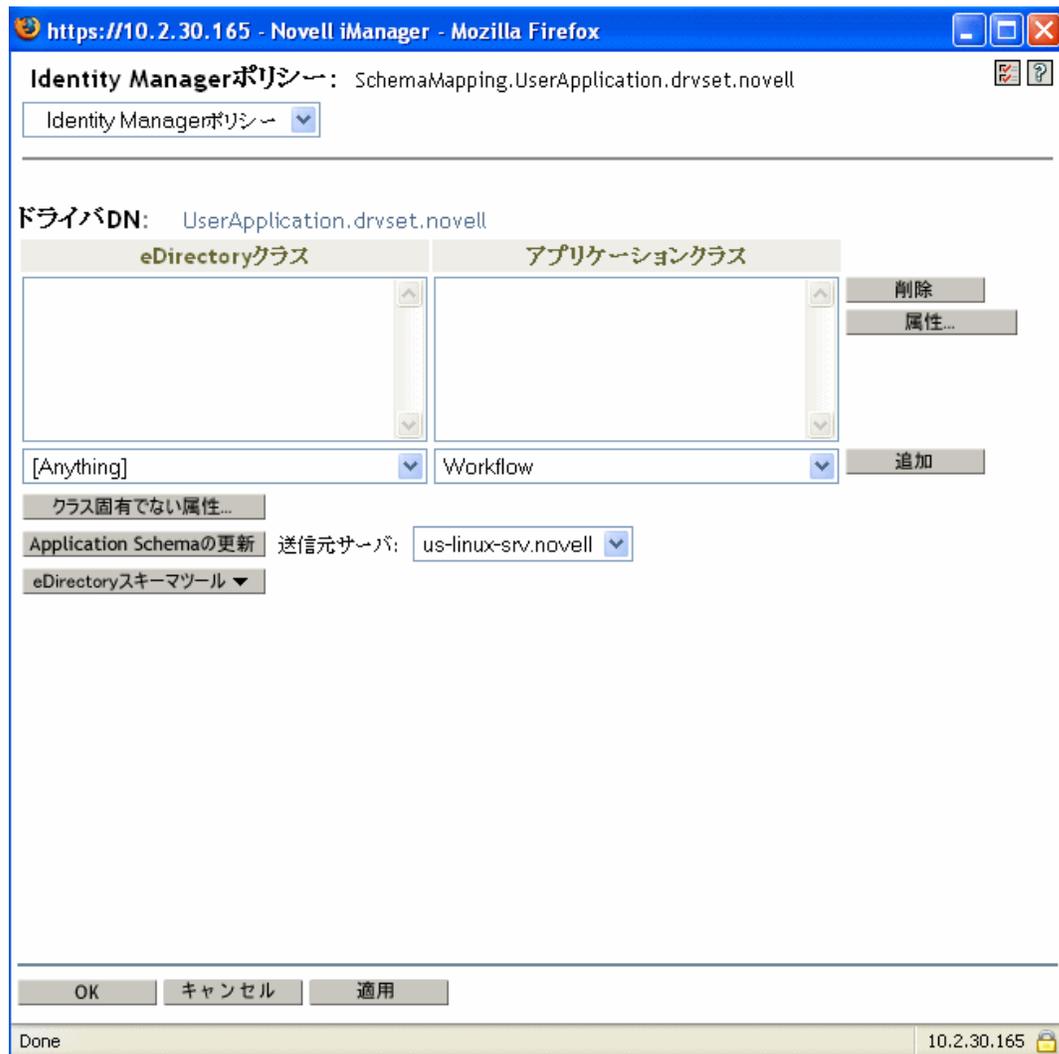


- 4 購読者チャンネルの [スキーママッピングポリシー] アイコンをクリックします。[スキーママッピングポリシー] ダイアログボックスが表示され、デフォルトのスキーママッピングポリシー名が強調表示されます。



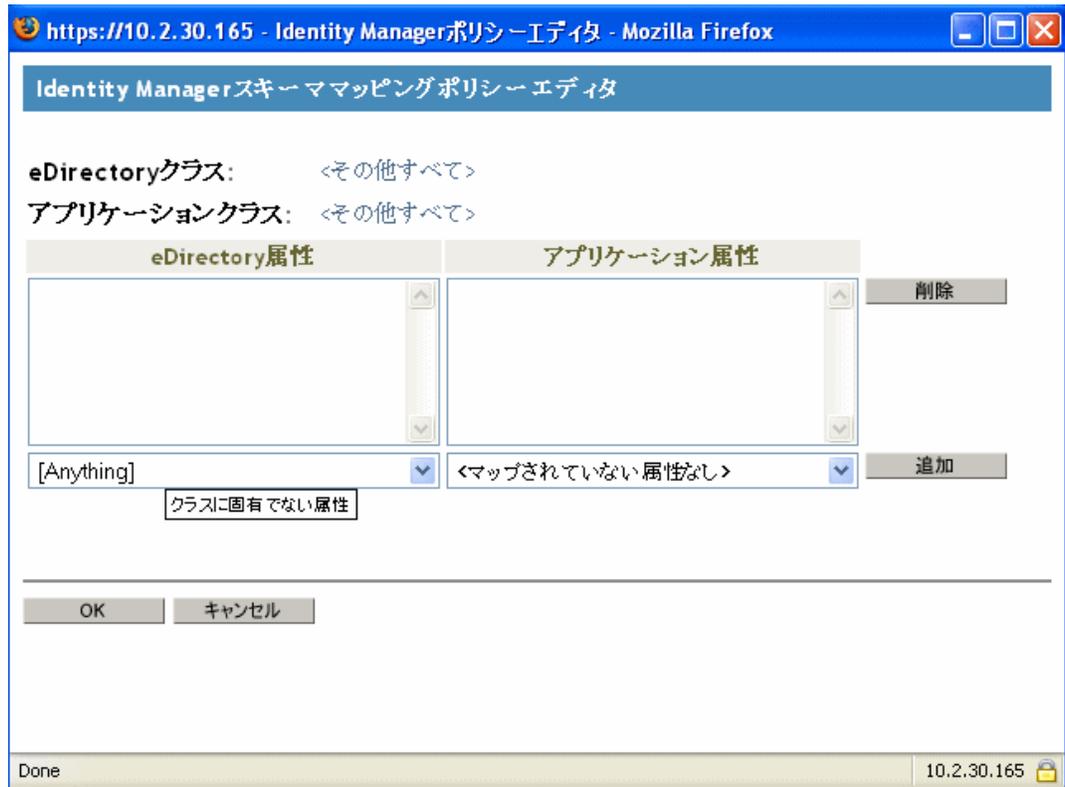
- 5 [編集] をクリックします。[Identity Manager ポリシー] ダイアログボックスが表示されます。このダイアログボックスは、アイデンティティポールのクラスをアプリケーションのクラスにマップするために使用します。この手順ではこの機能を使用し

ません。その代わりに、eDirectory 属性をグローバルユーザアプリケーション属性にマッピングします。



- 6 [アプリケーションスキーマのリフレッシュ] をクリックします。スキーマを読み込むためにドライバを停止し、再起動するよう促すメッセージが表示されます。スキーマのリフレッシュには約 60 秒かかります。ここでは、次の手順の準備として最新のワークフロー情報のセットが読み込まれます。この情報により、アイデンティティポルトから、起動されるワークフローに配信される情報が指定されます。
- 7 [OK] をクリックして、スキーマをリフレッシュします。スキーマリフレッシュが完了するとメッセージが表示されます。
- 8 [OK] をクリックして、スキーマリフレッシュのメッセージを閉じます。[Identity Manager ポリシー] ダイアログボックスに戻ります。

- 9 [クラスに固有でない属性] をクリックします。Identity Manager スキーママッピングポリシーエディタが表示されます。



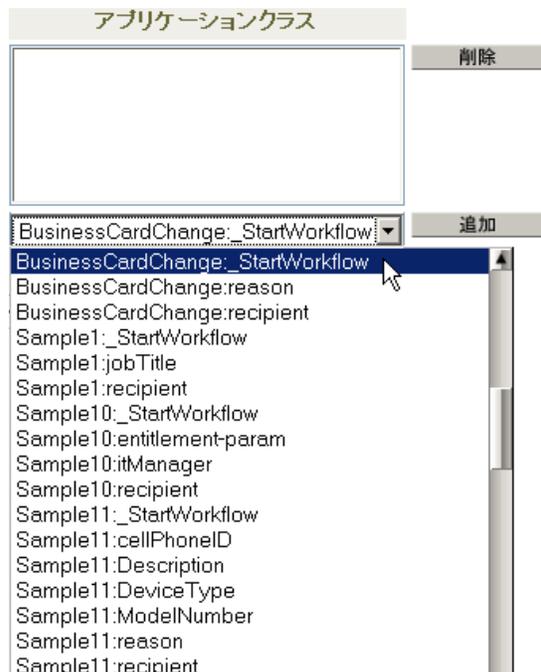
[eDirectory 属性] ドロップダウンリストには、eDirectory のすべての属性が含まれています。

[アプリケーション属性] ドロップダウンリストには、アクティブなすべてのワークフローの属性が含まれています。リスト内の属性には、AllWorkflows (属性がすべてのワークフローに適用されることを示します)、または特定のワークフロー名が先頭に付いています。同じ eDirectory 属性 (manager など) を、すべてのワークフローの manager 属性にマップする場合は、manager を Allworkflows:manager にマップします。異なる eDirectory 属性 (HRmanager など) を特定のワークフローで使用するには、eDirectory 属性を特定のワークフロー属性 (BusinessCardChange:manager など) にマップします。

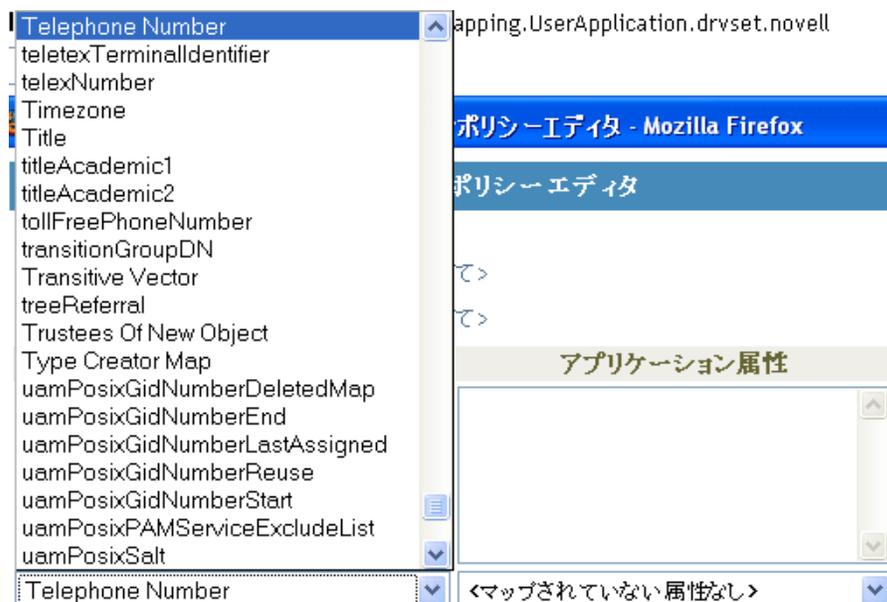
マップされた属性は、[eDirectory 属性] 列と [アプリケーション属性] 列に並んで表示されます。

次の手順では、ワークフローの起動に使用する eDirectory 属性をそのワークフローの StartWorkflow 属性にマップします。ワークフローで他の eDirectory 属性も使用される可能性がある場合は、その属性もマップしてください。たとえば、eDirectory の Address 属性がワークフローのトリガである場合、ワークフローでは City や State などの属性も必要になります。代わりに、これらの属性をポリシーでマップすることもできます。

- 10 [アプリケーション属性] リストで、設定するワークフローの `_StartWorkflow` 属性を選択します。次の例では、`BusinessCardChange` ワークフローの `_StartWorkflow` 属性が表示されています (`BusinessCardChange_StartWorkflow`)。



- 11 [eDirectory 属性] リストで eDirectory 属性を選び、その属性が変更された場合にワークフローを起動するようにします。次の例では、`Telephone` 属性が選択されています。この場合、従業員の電話番号が変更されると、`BusinessCardChange` ワークフローが必ず起動します。



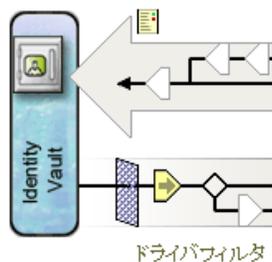
- 12 [追加] をクリックします。eDirectory 属性がアプリケーション属性にマップされます。

eDirectory属性	アプリケーション属性
Telephone Number	BusinessCardChange._StartWorkflow
[Anything]	AllWorkflows:approver

- 13 ワークフローで必要となる eDirectory 属性がまだある場合、**ステップ 10** から **ステップ 12** までを繰り返して、マップが必要な属性をすべてマップします。

アプリケーションの `_StartApprovalFlow` 属性にマップされた eDirectory 属性で変化が起きると、ワークフローが自動起動されます。ただし、eDirectory 属性が購読者チャンネルのドライバフィルタに含まれている場合は、eDirectory 属性がスキーママッピングポリシーに到達するだけです。次の手順では、eDirectory 属性を購読者チャンネルのドライバフィルタに追加します。

- 14 [OK] をクリックして、Identity Manager スキーママッピングポリシーエディタを閉じます。
- 15 [OK] をクリックして、[Identity Manager ポリシー] ダイアログボックスを閉じます。
- 16 [閉じる] をクリックして、[スキーママッピングポリシー] ダイアログボックスを閉じます。
- 17 購読者チャンネルの [ドライバフィルタ] アイコンをクリックします。



フィルタウィンドウが表示されます。



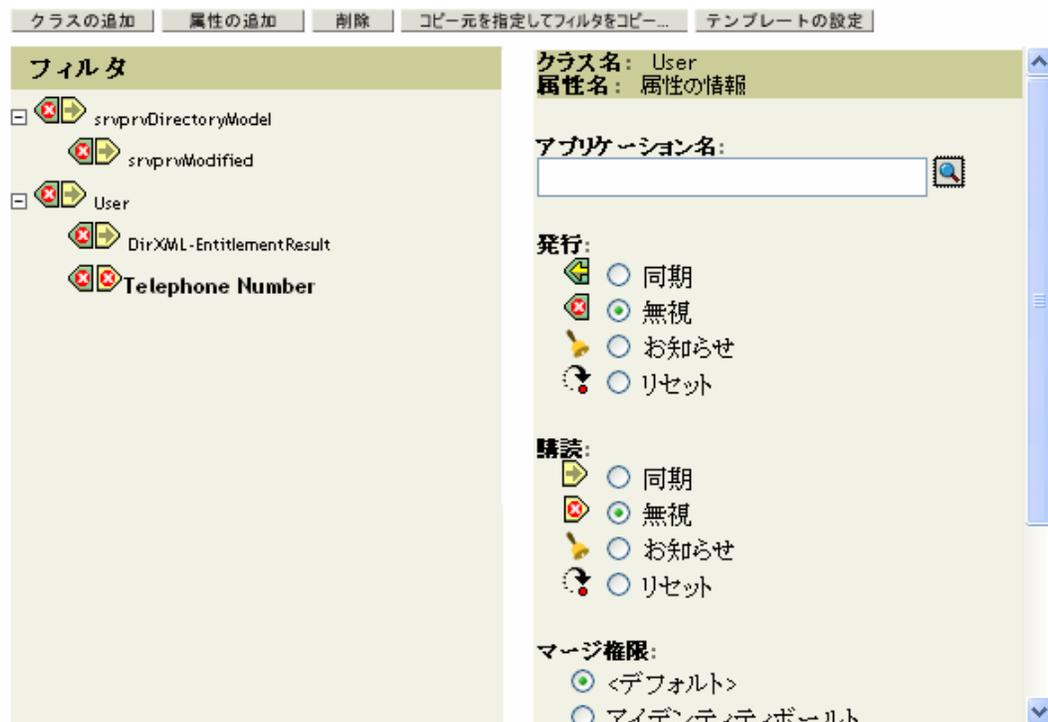
イベントフィルタでは、Identity Manager エンジンがイベントを処理するオブジェクトクラスや属性を指定します。左側にある読み込み専用の [フィルタ] リストでは、クラスの属性が表示されます。右側の [クラス名] リストでは、ターゲットオブジェクトに関連付けられたオプションが表示されます。

- 18 フィルタに追加する属性が属しているクラスの名前をクリックします (User など)。
- 19 [属性の追加] をクリックします。属性のリストが表示されます。

- 20 属性を選択して、[OK] をクリックします。[フィルタ] リストに属性が追加されます。



- 21 属性名をクリックします。右側のパネルに、その属性の同期オプションが表示されます。



- 22 [購読者] で、[同期] をクリックします。



- 23 フィルタに対して他の属性を指定します。属性値への変更がレポートおよび同期されるためには、その属性で [同期] を選択します。属性値への変更がレポートおよび同期されないようにするには、[無視] を選択します。

- 24** [OK] をクリックします。変更を有効にするためにドライバを再起動するかどうか尋ねるメッセージが表示されます。
- 25** [OK] をクリックします。[Identity Manager ドライバの概要] ページに戻ります。

ディレクトリ抽出化レイヤの設定

この章では、ディレクトリ抽出化レイヤエディタを使用して、Identity Manager ユーザアプリケーションで使用されるディレクトリ抽出化レイヤデータを定義する方法について説明します。ここで取り扱う内容は次のとおりです。

- ◆ 75 ページのセクション 4.1 「ディレクトリ抽出化レイヤ定義について」
- ◆ 76 ページのセクション 4.2 「はじめに」
- ◆ 87 ページのセクション 4.3 「エンティティおよび属性の操作」
- ◆ 104 ページのセクション 4.4 「リストの操作」
- ◆ 106 ページのセクション 4.5 「組織図の関係の操作」
- ◆ 109 ページのセクション 4.6 「環境設定の操作」
- ◆ 110 ページのセクション 4.7 「表示テキストのローカライズ」

4.1 ディレクトリ抽出化レイヤ定義について

ディレクトリ抽出化レイヤとは、アイデンティティポールの論理ビューを提供するデータ定義のセットです。ディレクトリ抽出化レイヤは次の内容を定義します。

- ◆ Identity Manager ユーザアプリケーションで使用できるアイデンティティポールのオブジェクトと属性。
- ◆ アイデンティティポールのデータをユーザインタフェースで表示する方法。
- ◆ 組織図ポートレットで使用可能な関係。

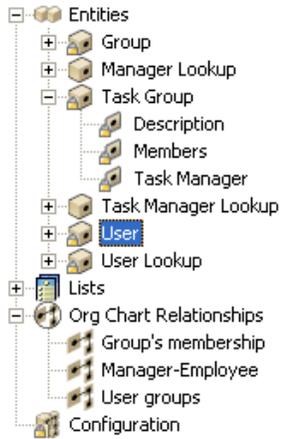
ユーザアプリケーションの外観や機能を変更する場合は、ディレクトリ抽出化レイヤエディタを使用してこうしたデータ定義を変更します。次の方法で変更できます。

- ◆ 他のアイデンティティポールのオブジェクトを追加する
- ◆ アイデンティティポールのオブジェクトで使用できる属性のセットを変更する
- ◆ リストのコンテンツを変更する
- ◆ アイデンティティポールのオブジェクト間の異なる関係を表示する

Identity Manager ユーザアプリケーションのインストール手順では、ユーザアプリケーションが正常に機能するのに必要となる、抽出化レイヤ定義の基本セットがインストールおよび展開されます。このインストールではまた、ユーザアプリケーションドライバやユーザアプリケーションによって使用される eDirectory スキーマ拡張も作成されます。スキーマ拡張の詳細については、365 ページの付録 A 「スキーマ拡張」を参照してください。Designer for Identity Manager を使用して新しいユーザアプリケーションドライバインスタンスを作成した場合、ローカルファイルシステムにも同じファイルの基本セットが作成されます。

データ抽出化レイヤデータの必須定義 自分の Identity Manager ユーザアプリケーションのカスタマイズを始めると、ディレクトリ抽出化レイヤのオブジェクトに変更を加える必要が出てくる場合もありますが、特定のアイデンティティポールのオブジェクト (エンティティ)、属性、関係、およびリストは削除や変更ができません。削除や変更を行うと、ユーザアプリケーションは正常に機能しなくなります。削除できない定義は南京錠型のア

アイコンで識別できます。この例では、「タスクグループ」エンティティとその属性がすべてロックされていることが分かります。



ディレクトリ抽出化レイヤ定義の保存場所 ディレクトリ抽出化レイヤ定義は XML ファイルで、次のように保存、展開およびキャッシュされます。

- ◆ **Designer** コンピュータのローカルファイルシステムにある、プロビジョニングプロジェクトの `Provisioning\AppConfig\DirectoryModel` サブディレクトリに保存されます。プロジェクトに複数のユーザアプリケーションがある場合は、ディレクトリ名に番号が付きます (`AppConfig1`、`AppConfig2` など)。
- ◆ ユーザアプリケーションドライバの `AppConfig.DirectoryModel` コンテナに展開されません。XML ファイルは、対応するディレクトリ抽出化レイヤ定義オブジェクトの `XMLData` 属性に保存されます。各エンティティ、関係、およびリストは、ユーザアプリケーションドライバの `AppConfig.DirectoryModel` コンテナに含まれる固有のオブジェクトインスタンスです。
- ◆ ユーザアプリケーションが展開されるアプリケーションサーバにキャッシュされません。

4.2 はじめに

Designer for Identity Manager のプロビジョニングビューおよびディレクトリ抽出化レイヤエディタの機能を使用して、ディレクトリ抽出化レイヤのコンテンツを定義します。次の手順を使って開始します。

手順	タスク	説明
1	Identity Manager プロジェクトを作成する	次のものが含まれています。 <ul style="list-style-type: none"> ◆ アイデンティティボルトの設定 ◆ ドライバセットのプロパティの指定 Identity Manager のマニュアルを参照してください。

手順	タスク	説明
2	モデラにユーザアプリケーションドライバを追加する	Identity Manager ユーザアプリケーションドライバは、モデラパレットの [Provisioning] フォルダにあります。
		
3	ユーザアプリケーションドライバを設定する	77 ページのセクション 4.2.1 「ユーザアプリケーションドライバの設定」の手順を参照してください。
4	[プロビジョニング] ビューにアクセスする	81 ページのセクション 4.2.2 「プロビジョニングビューへのアクセス」を参照してください。
5	ディレクトリ抽出化レイヤエディタを起動する	82 ページの 「ディレクトリ抽出化レイヤエディタを起動するには :」 を参照してください。

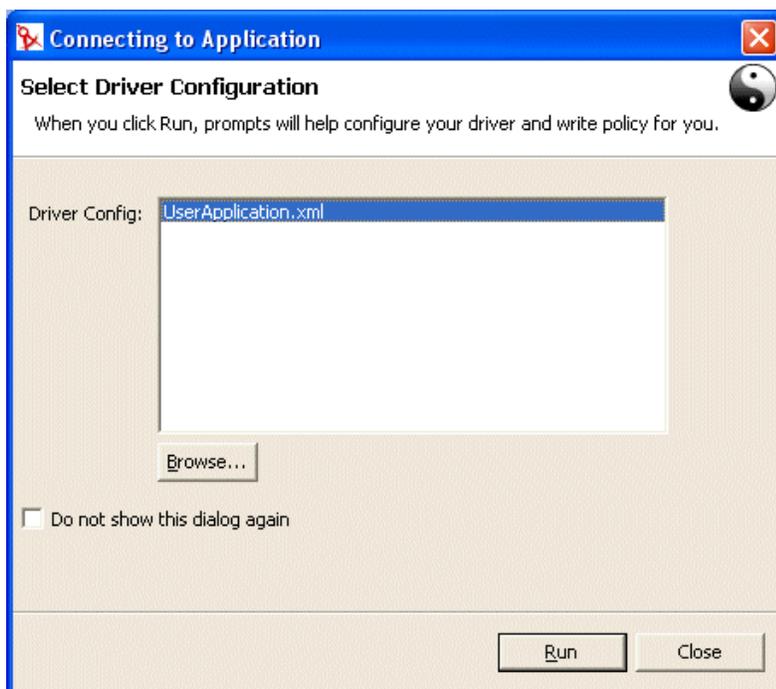
4.2.1 ユーザアプリケーションドライバの設定

Identity Manager プロジェクトを作成したら、次の手順に従ってください。

ユーザアプリケーションドライバを設定するには：

- 1 キャンバスに [User Application (ユーザアプリケーション)] ドライバのアイコンをドロップします。

ドライバを設定するよう求めるメッセージが表示されます。



- 2 [UserApplication.xml] (デフォルト) を選択してから [実行] をクリックします。

- 3 [はい] または [いいえ] をクリックして、ウィザードがエントリの検証を処理する方法を指定します。

Import Information Requested

The driver writer requested that the following information be supplied in order to import this driver configuration file.

Information requested: * Required

Enter the driver name. Entering the name of or selecting an existing driver will overwrite its configuration. The Driver name 'UserApplication' was provided as a default value by the Configuration File.

Driver name: *

UserApplication

Enter the DN of the User Application Administrator. This value should match the user entered during the User Application installation. Use the DOT format i.e., admin.orgunit.novell or use browse. This is a required field.

Authentication ID: *

Application Password:

Reenter the password:

Enter the User Application Context. This is the context portion of the URL for the User Application WAR file. The default is: IDM.

Application Context:

IDM

OK Cancel

Enter the Host Name or IP address of the application server where the User Application is running. For example, 'http://ServerName' or 'https://123.456.78.99'. This is a required field.

Host: *

Enter the host port on the application server specified above. This is the port where the User Application is accessible e.g. 80, 8080, 8090.

Port:

OK Cancel

4 各フィールドに、次のとおり値を指定します。

プロパティ	指定する内容
ドライバ名	<ul style="list-style-type: none">◆ 既存のドライバの名前 (ユーザアプリケーションのインストール中に指定された、ドライバセット内のドライバ)。◆ 新しいドライバの名前。
認証 ID	ユーザアプリケーションの管理者の DN。
アプリケーションパスワードとパスワードの再入力	ユーザアプリケーション管理者 (前の項目) のパスワード。
アプリケーションコンテキスト	ユーザアプリケーションのコンテキストの名前 (インストール時に指定。たとえば、IDM など)。
ホスト	Identity Manager ユーザアプリケーションが展開されたアプリケーションサーバのホスト名または IP アドレス。この情報は次のように使用されます。 <ul style="list-style-type: none">◆ アプリケーションサーバでワークフローを起動し、ワークフローに接続してアクセスする (および、終了、撤回など)。◆ キャッシュされたデータ定義を更新する。
ポート	ホスト (前の項目) のポート。

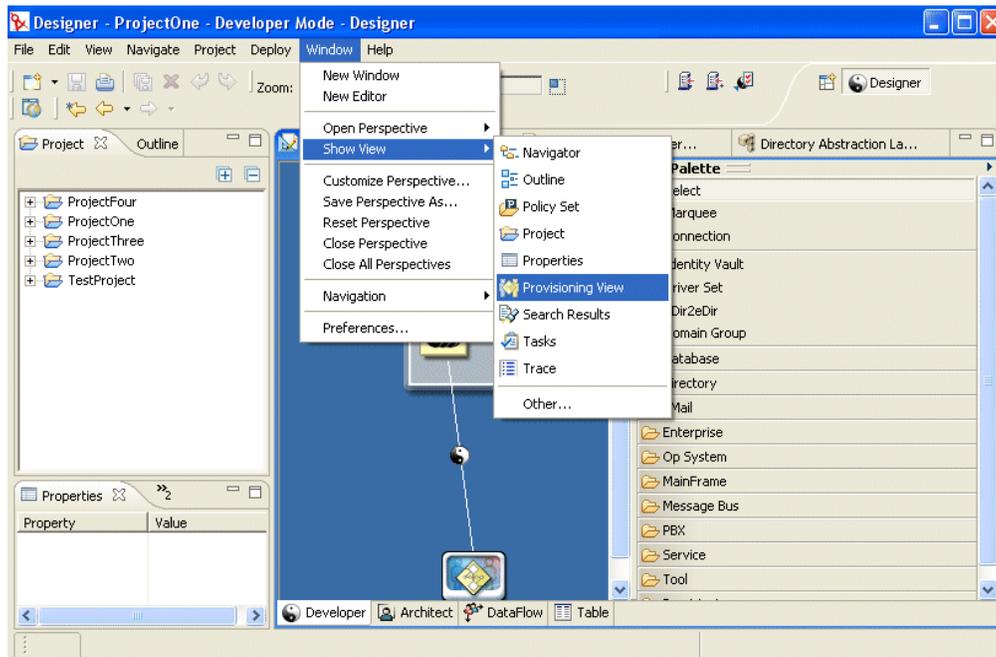
5 [OK] をクリックします。

4.2.2 プロビジョニングビューへのアクセス

プロビジョニングビューにアクセスするには：

1 次の方法のいずれかの方法を選択します。

- ◆ [Window (ウィンドウ)] > [Show View (ビューの表示)] > [Provisioning View (プロビジョニングビュー)] の順にクリックします。



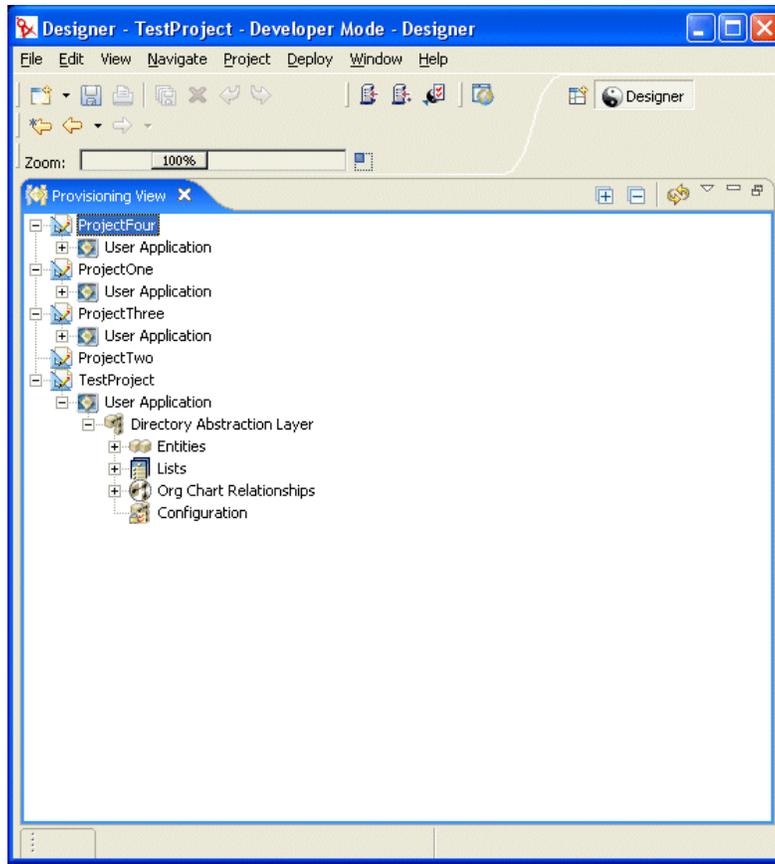
- ◆ [Provisioning (プロビジョニング)] フォルダを開き、[Provisioning View (プロビジョニングビュー)] をクリックする。
- ◆ [OK] をクリックします。

または

- ◆ [User Application (ユーザアプリケーション)] アイコンを選択して右クリックし、[アプリケーション] > [Show Provisioning View (プロビジョニングビューの表示)] の順にクリックします。

プロビジョニングビューに、今作成したプロジェクトが、同じワークスペースにある他のプロビジョニングプロジェクトと共に表示されます。

ヒント：ビューに表示されるはずのアプリケーションが表示されない場合、プロジェクトが壊れている可能性があります。プロジェクトが壊れている場合は、作成し直す必要があります。



プロビジョニングビューについて

プロビジョニングビューでは、常にプロビジョニング機能にアクセスできます。プロビジョニングビューの項目をダブルクリックすると、その項目用のエディタが開きます。プロビジョニングビューを使用して、ディレクトリ抽出化レイヤ定義に関する次のアクションを実行します。

- ◆ アイデンティティポータルから1つ以上のオブジェクト定義をインポートします。
- ◆ データ定義の構造を検証します。
- ◆ プロジェクトで指定した定義をアイデンティティポータルに展開します。
- ◆ ディレクトリ抽出化レイヤ定義を作成および削除します。

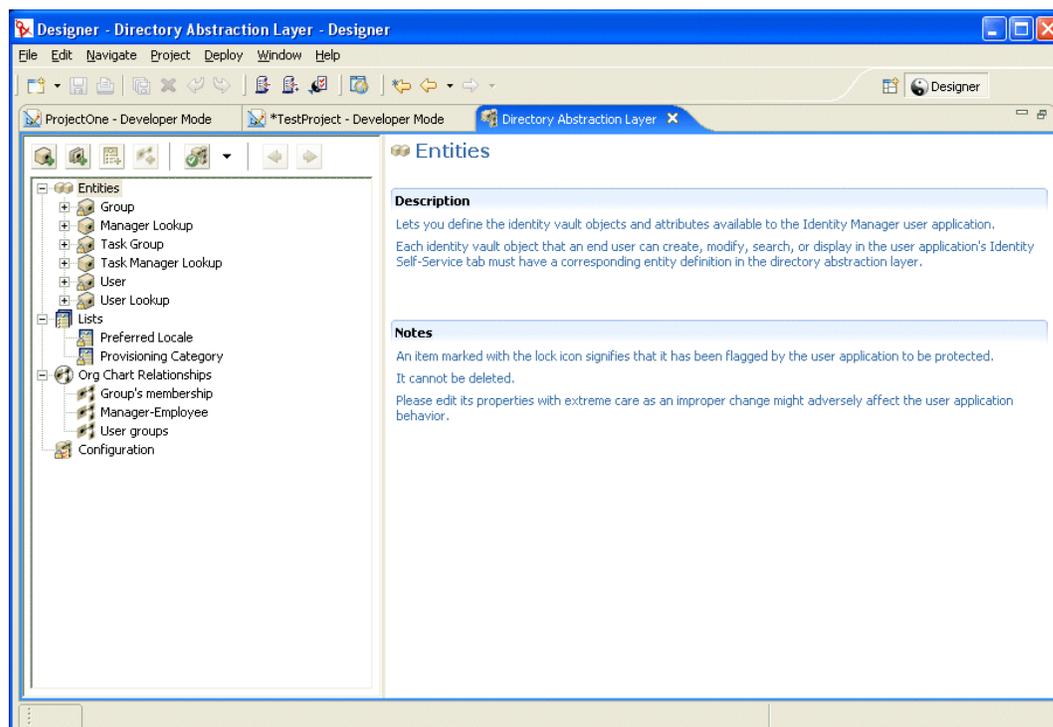
詳細については、[111 ページのセクション 4.8「ディレクトリ抽出化レイヤ定義のインポート、検証、および展開」](#)を参照してください。

4.2.3 ディレクトリ抽出化レイヤエディタの起動

ディレクトリ抽出化レイヤエディタを起動するには：

- 1 プロビジョニングビューが開いた状態で、[Directory Abstraction Layer (ディレクトリ抽象化レイヤ)] ノードに移動します。
- 2 [Directory Abstraction Layer (ディレクトリ抽象化レイヤ)] ノードをダブルクリックします。

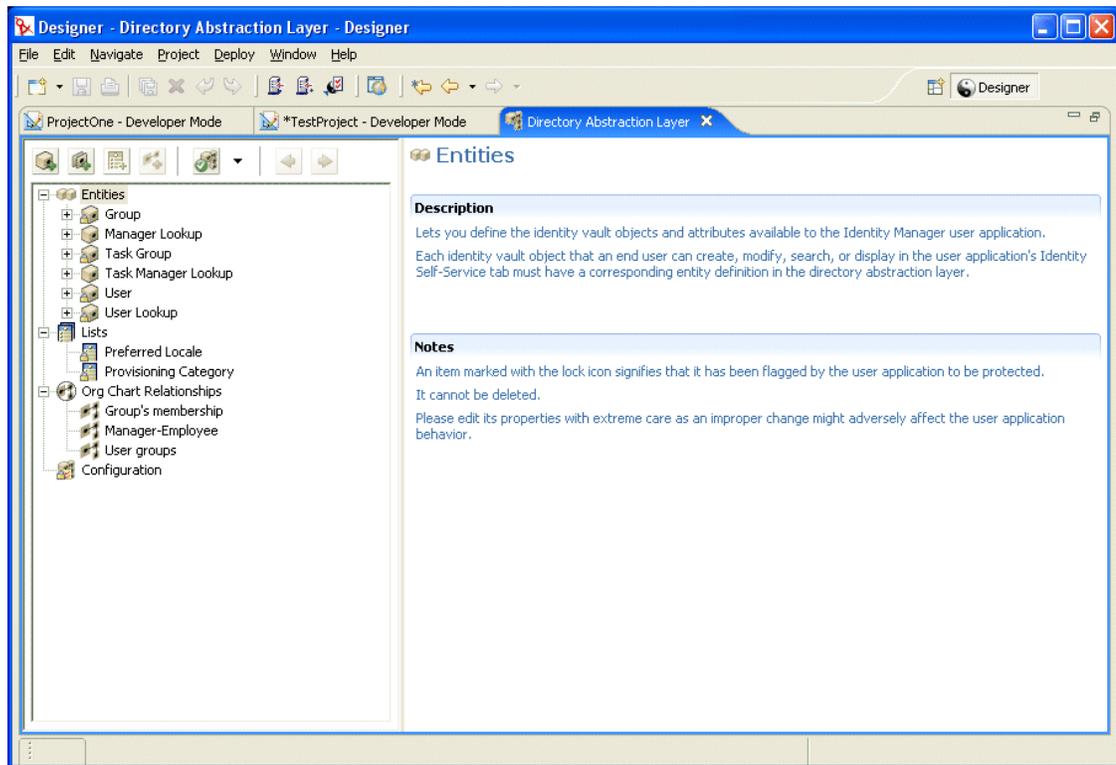
[Entities (エンティティ)], [Lists (リスト)], [Org Chart Relationships (組織図の関係)], および [Configuration (環境設定)] が含まれたツリーが表示されます。



ディレクトリ抽出化レイヤエディタについて

ディレクトリ抽出化レイヤエディタでは、ディレクトリ抽出化レイヤを構成する XML ファイルのセットをグラフィカルに定義できます。ディレクトリ抽出化レイヤエディタは Eclipse ベースのツールで、Identity Manager プロジェクトのプロビジョニングビューからアクセスできます。

ディレクトリ抽出化レイヤエディタを最初に開くと、抽出化レイヤオブジェクトの基本セットが表示されます。これは新しいプロビジョニングプロジェクトを作成するたびに自動生成されます。



ディレクトリ抽出化レイヤエディタのノードには次の内容が含まれます。

要素	説明
エンティティ	<p>エンティティは、このプロジェクトに設定され、ユーザアプリケーションが使用できるアイデンティティポータルプロジェクトを表します。エンティティには2つの種類があります。</p> <ul style="list-style-type: none"> ◆ スキーマからマップされるエンティティ。これらのエンティティは、アイデンティティポータルに存在し、ユーザアプリケーションを通して直接ユーザに公開されるオブジェクトを表します。ユーザは通常、このようなタイプのオブジェクトの属性を作成、検索、および変更できます。 ◆ LDAP 関係を表すエンティティ。これは DNLookups と呼ばれます。これらのエンティティはインデックス検索を表し、公開する特定タイプの属性をサポートするために使用されます。DNLookup エンティティは、LDAP オブジェクト間の関係についての情報を提供します。DNLookup エンティティは次のポートレットによって使用されます。 ◆ 組織図ポートレットが関係の判断に使用します。 ◆ 検索リスト、作成、および詳細のポートレットが、ポップアップ選択リストや DN コンテキストを提供するために使用します。
Lists (リスト)	<p>グローバルリストのコンテンツを定義できます。グローバルリストは、</p> <ul style="list-style-type: none"> ◆ 1つの属性に関連付けられています。その属性がユーザアプリケーションで表示される場合、属性はドロップダウンリストに表示されます。 ◆ iManager のプロビジョニング要求の環境設定プラグインで使用されるカテゴリの表示に使用されます。
組織図の関係	<p>ユーザアプリケーションの [識別セルフサービス] タブにある組織図アクションで使用されます。ユーザは、スキーマベースのエンティティ間の階層関係をマップできます。</p> <p>詳細については、106 ページのセクション 4.5 「組織図の関係の操作」を参照してください。</p>
環境設定	<p>一般的な環境設定パラメータです。</p> <p>詳細については、109 ページのセクション 4.6 「環境設定の操作」を参照してください。</p>

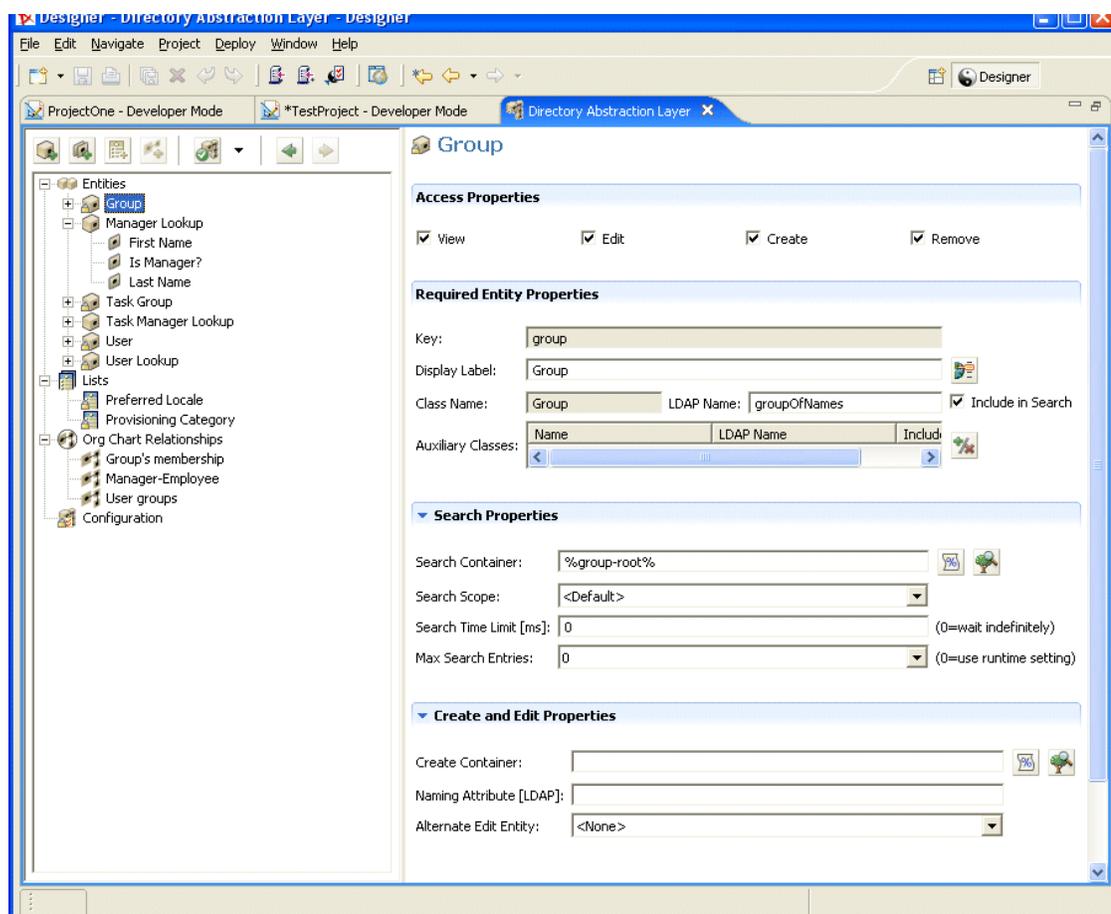
XML ファイルがローカルで保存される場合 ディレクトリ抽出化レイヤエディタは、エンティティ、リスト、または関係のそれぞれに対して XML ファイルを1つずつ生成します。ファイルはプロジェクトの Provisioning\AppConfig\DirectoryModel フォルダに保存されます。オブジェクトのキーに基づいてファイル名が付けられます。次のディレクトリで構成されます。

ディレクトリ	説明
ChoiceDefs	グローバルリストを定義するファイルが含まれます。ファイルには拡張子 .choice が付きます。
EntityDefs	エンティティおよび属性を定義するファイルが含まれます。ファイルには拡張子 .entity が付きます。
RelationshipDefs	組織図ポートレットで使用可能な関係を定義するファイルが含まれます。ファイルには拡張子 .relation が付きます。

ディレクトリ抽出化レイヤエディタの機能を使用して、ユーザ独自のアイデンティティボールドスキーマをモデル化した新しい定義を追加できます。プロビジョニングビューの機能を使用して、アイデンティティボールドに新しい定義を展開できます。

ディレクトリ抽出化レイヤエディタの使用

ディレクトリ抽出化レイヤエディタは2つのペインに分かれています。左側のペインには、ディレクトリ抽出化レイヤのコンテンツが表示されます。左側のペインで項目を選択すると、右側のペインには選択された項目の属性や設定が表示されます。



4.3 エンティティおよび属性の操作

Identity Manager ユーザアプリケーションでユーザが検索、表示、編集できるようにするアイデンティティボールドブジェクトはすべて、ディレクトリ抽出化レイヤのエンティティとして定義する必要があります。たとえば、ユーザアプリケーションで inetOrgPerson アイデンティティボールドブジェクトを使用するには、そのためのエンティティ定義を作成する必要があります。

4.3.1 エンティティを追加する手順

次の手順に従って、ディレクトリ抽出化レイヤにエンティティを追加します。

手順	タスク	参照先
1	ユーザアプリケーションで使用するアイデンティティボールドブジェクトを決定します。	87 ページのセクション 4.3.2 「データに必要な内容の分析」
2	ディレクトリ抽出化レイヤエディタを使用して、ディレクトリ抽出化レイヤのアイデンティティボールドブジェクトを定義します。	88 ページのセクション 4.3.3 「エンティティの定義」
3	プロビジョニングビューを使用して、データ定義を検証します。	111 ページのセクション 4.8 「ディレクトリ抽出化レイヤ定義のインポート、検証、および展開」
4	アイデンティティボールドに定義を展開します。	114 ページのセクション 4.8.3 「展開について」
5	アプリケーションサーバのキャッシュを更新して、新しい抽出化レイヤ定義を組み込みます。	219 ページの第 13 章 「キャッシングの環境設定」
6	Identity Manager ユーザアプリケーションをテストして、変更が正常に表示されることを確認します。	

4.3.2 データに必要な内容の分析

ディレクトリ抽出化レイヤでアイデンティティボールドデータをモデル化する場合、次の点を確認する必要があります。

- ◆ Identity Manager ユーザアプリケーションで使用可能にするディレクトリの各種パーツ
たとえば、ユーザが検索したり表示したりできるオブジェクトのリストの場合、このリストを抽出化レイヤ定義の基本セットと比較し、何を追加する必要があるか判断します。
- ◆ カスタム拡張や補助クラスを含むスキーマの構造
- ◆ 次を含むデータの構造：
 - ◆ 必須データとオプションデータ
 - ◆ 検証ルール
 - ◆ オブジェクト間の関係 (DN 参照)
 - ◆ 属性の定義方法 (たとえば、電話番号を表す属性には自宅、オフィス、および携帯電話の電話番号など複数の値が含まれることがあります)
- ◆ データを表示できるユーザ

サイトはパブリックかプライベートか

これらの情報が揃ったら、この情報を使用してアイデンティティポルトプロジェクトを抽出化レイヤエンティティにマップします。

注：eDirectory ACL はすべての抽出化レイヤオブジェクトに適用されます。オブジェクトおよび属性に対する有効な権利は、アプリケーションのログイン時に確立された認証ユーザに基づきます。

4.3.3 エンティティの定義

ユーザアプリケーションで公開する内容に応じて、次の2種類のエンティティを定義できます。

- ◆ スキーマからマップされるエンティティ。これらのエンティティは、アイデンティティポルトに存在し、ユーザアプリケーションを通して直接ユーザに公開されるオブジェクトを表します。この種類のエンティティを定義する場合、ユーザに利用してもらうすべての属性を公開します。このエンティティタイプの例としては、「ユーザ」、「グループ」、および「タスクグループ」があります。異なる種類のユーザに異なる属性のセットを公開する場合は、同じオブジェクトに対し複数のエンティティ定義を作成することもできます。詳細については、[88 ページの「1つのオブジェクトへの複数のエンティティ定義の作成」](#)を参照してください。
- ◆ LDAP 関係を表すエンティティ。この種類のエンティティは DNLookup と呼ばれ、次の目的でユーザアプリケーションに使用されます。

- ◆ 関連するエンティティ間での DN 検索の結果をリストに入力する
- ◆ 更新や削除が行われた場合、複数の DN 参照属性間の参照整合性を維持する

DNLookup をサポートするエンティティは、関係を判断するために組織図ポートレットによって使用されます。また、検索ポートレット、作成ポートレット、および詳細ポートレットによっても、ポップアップ選択リストや DN コンテキストを表示する目的で使用されます。この種類のエンティティには、「マネージャのルックアップ」、「タスクマネージャのルックアップ」、「ユーザのルックアップ」などがあります。詳細については、[100 ページの「DNLookup 制御タイプの使用」](#)を参照してください。

1つのオブジェクトへの複数のエンティティ定義の作成

同じアイデンティティポルトプロジェクトを表しながら異なる方法でデータを表示する、複数のエンティティ定義を作成できます。エンティティ定義内で、次のことを行うことができます。

- ◆ エンティティ定義ごとに異なる属性を定義する

または

- ◆ 同じ属性を定義するが、異なるアクセスプロパティ（属性の検索、表示、編集、および非表示の方法を制御）を指定する

注：エンティティ定義にフィルタを含め、結果セットで特定のエンティティを非表示にする方法もあります。

これで、ユーザインタフェースの異なる部分に異なるエンティティ定義を使用できるようになります。たとえば、1つは公開サイト用、もう1つは社内サイト用に従業員のディレ

クトリを作成する場合を考えてみましょう。公開サイトでは従業員の姓名、および電話番号を記載し、社内サイトでは役職、マネージャなど追加の情報も含めることにします。その方法を次に示します。

1 2つのエンティティ定義を作成します(異なるキーを使用します)。

どちらのエンティティ定義も同じアイデンティティポータルプロジェクトを公開しますが、1つのエンティティ定義キーは公開従業員情報、別のエンティティ定義キーは社内従業員情報です。

2 各エンティティ定義で、異なるセットの属性を定義します。1つは公開従業員情報、もう1つは社内従業員情報です。

3 Identity Manager ユーザアプリケーションの [ポータル管理] タブで、公開ページ用と社内ページ用のポートレットインスタンスをそれぞれ作成します。

ポートレットインスタンスの作成の詳細については、[181 ページの第9章「ポートレットの管理」](#)を参照してください。

エンティティ定義を作成する手順

公開するエンティティおよび属性を決めたら、エディタを使用してディレクトリ抽出化レイヤに追加できます。次のような一連の手順を実行します。

手順	操作	参照先
1.	開始するファイルのセットを決めます。 <ul style="list-style-type: none">◆ 定義の基本セットに追加する◆ すでに展開された定義から開始する	87 ページのセクション 4.3.1「エンティティを追加する手順」 111 ページのセクション 4.8.1「インポートについて」
1a.	使用するエンティティの一部は eDirectory の基本スキーマに含まれていません。eDirectory スキーマを拡張しても、エディタの選択可能なオブジェクトおよび属性のリストに自動的に反映されるわけではありません。このため、Designer のローカルスキーマファイルを更新して、拡張したカスタムオブジェクトおよびカスタム属性を反映させる必要があります。	89 ページの「使用可能なスキーマ要素のリストを更新するには」
2.	ディレクトリ抽出化レイヤにエンティティを1つ以上追加します。	90 ページの「エンティティの追加」
3.	エンティティに属性を追加します。	93 ページの「属性の追加」

使用可能なスキーマ要素のリストの更新

使用可能なスキーマ要素のリストを更新するには：

- 1 Identity Manager** プロジェクトが開いた状態でアイデンティティポータルを選択し、右クリックしてから [Live Operations (ライブ操作)] > [Import Schema (スキーマのインポート)] の順にクリックします。
- [Import from eDirectory (eDirectory からのインポート)] を選択し、eDirectory ホストの仕様を入力します。
- [次へ] をクリックします。

- 4 インポートするクラスおよび属性を選択し、[完了] をクリックします。

エンティティの追加

エンティティを追加する場合は、エンティティの追加ウィザードを使用するか (次の節で説明)、エディタのツールバーで [Add Entity (エンティティの追加)] ボタンをクリックします。

注: [Add Entity (エンティティの追加)] ボタンを使用するときは、作成するエンティティのオブジェクトクラスを選択するよう促すメッセージが表示されます。必要な属性はエディタによって自動的にエンティティに追加されます。続いて [属性の追加] ダイアログボックスを使用してエンティティ定義を完了できます。

エンティティの追加ウィザードを使用してエンティティを追加するには:

- 1 次のいずれかの方法でエンティティの追加ウィザードを起動します。

プロビジョニングビューから起動する場合

- ◆ [Entities (エンティティ)] ノードを選択し、右クリックしてから [New (新規)] をクリックします。
- ◆ [File (ファイル)] > [New (新規)] > [Provisioning (プロビジョニング)] の順にクリックします。[Directory Abstraction Layer Entity (ディレクトリ抽象化レイヤエンティティ)] をクリックします。[Next (次へ)] をクリックします。

ディレクトリ抽出化レイヤエディタから起動する場合

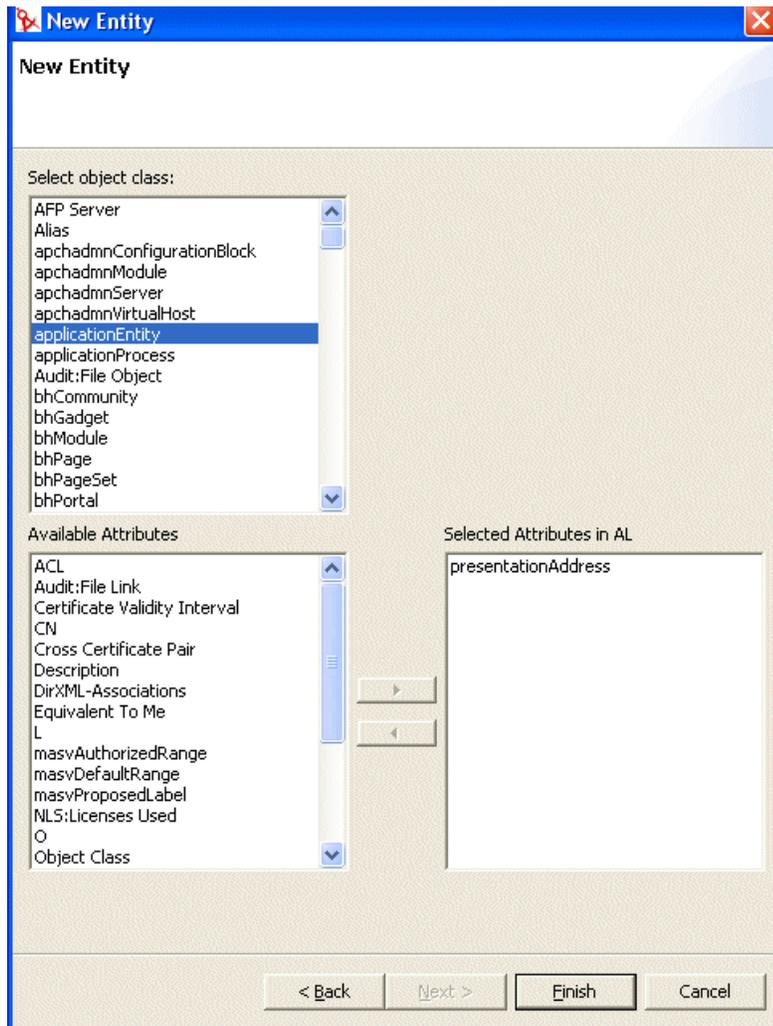
- ◆ [Entities (エンティティ)] ノードを選択し、右クリックしてから [New Entity-Attributes Wizard (新規エンティティ属性ウィザード)] をクリックします。
[New Entity (新規エンティティ)] ダイアログボックスが表示されます。

注: [ファイル] メニューから起動した場合、他の方法で起動した場合には表示されないフィールドがダイアログボックスに表示されます。次に示します。

2 各フィールドに、次のとおり値を指定します。

フィールド	説明
[Identity Manager Project (Identity Manager プロジェクト)] と [Provisioning Application (プロビジョニングアプリケーション)]	エンティティおよび属性を追加する Identity Manager プロジェクトおよびプロビジョニングアプリケーションを選択します。 注： これらのフィールドは、[ファイル] メニューからウィザードを起動したときに表示されます。
[Entity Key (エンティティキー)]	エンティティの固有識別子です。
[Display label (表示ラベル)]	ユーザインタフェースでこのエンティティが参照されるときに表示される文字列です。

- 3 [Next (次へ)] をクリックします。[New Entity (新規エンティティ)] ダイアログボックスが表示されます。



- 4 作成するエンティティのオブジェクトクラスを選択し、[Available Attributes (使用可能な属性)] リストから使用する属性を選択します。

ヒント：作成するエンティティのオブジェクトクラスが [Available Object Classes (使用可能なオブジェクトクラス)] のリストにないときは、Designer のローカルスキーマファイルの更新が必要な場合があります。89 ページの「使用可能なスキーマ要素のリストを更新するには:」の手順に従ってください。

- 5 [Finish (完了)] をクリックします。

編集用のプロパティシートが表示されます。

詳細については、94 ページの「エンティティのプロパティの参照」を参照してください。

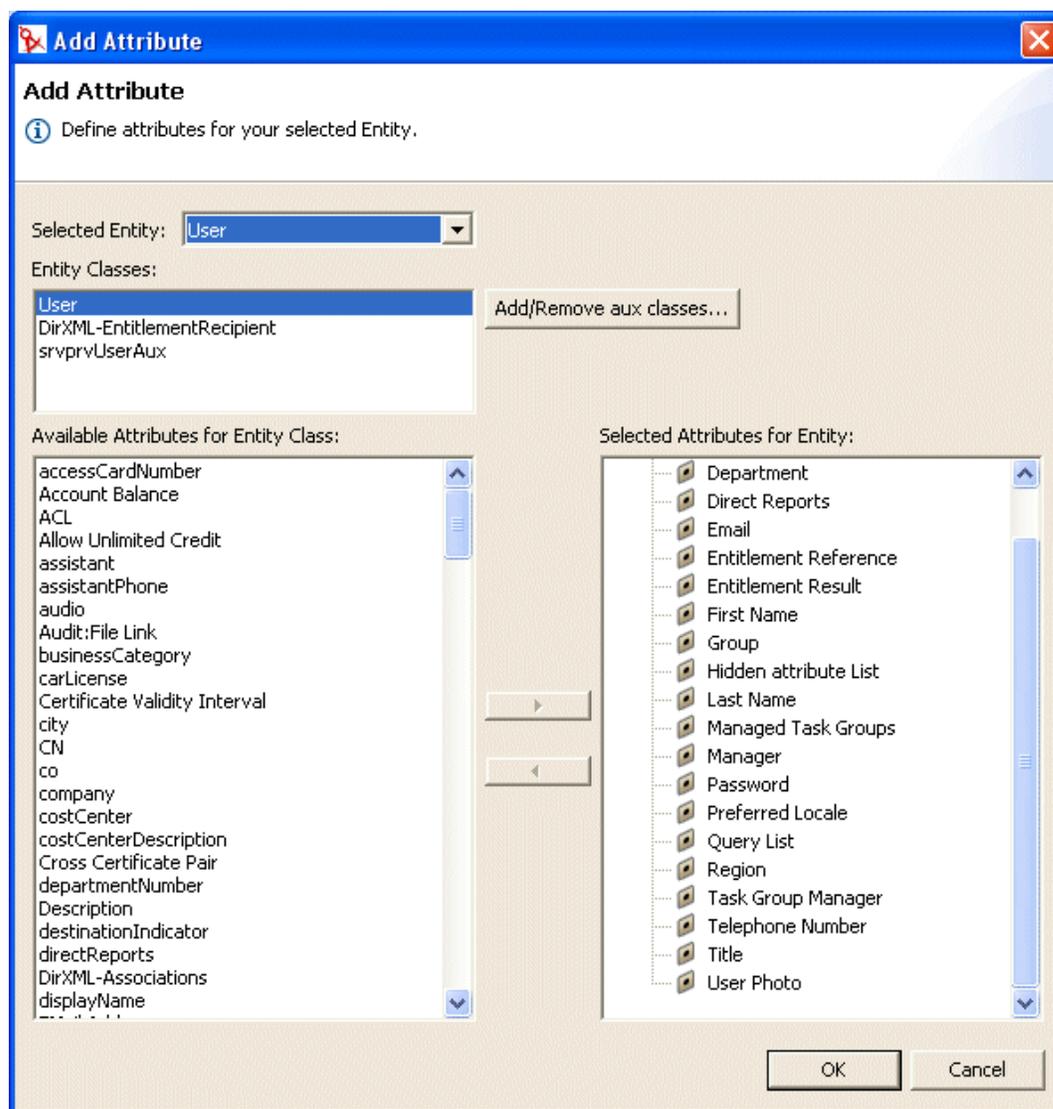
注：ユーザアプリケーションで属性を使用可能にするには、属性を含むエンティティを展開する必要があります。

属性の追加

属性を追加するには：

- 1 エンティティを選択します。
- 2 次のいずれかの方法で属性を追加します。
 - ◆ 右クリックしてから [Add Attribute (属性の追加)] をクリックする。または
 - ◆ [Add Attribute (属性の追加)] アイコンをクリックする。

次の選択画面が表示されます。



- 3 [Available Attributes for Entity Class (エンティティクラスの使用可能な属性)] リストから属性を選択し、[Selected Attributes for Entity (エンティティの選択された属性)] リストに追加します。

ヒント：作成する属性が [Available Attributes for Entity Class (エンティティクラスの
使用可能な属性)] リストにないときは、Designer のローカルスキーマファイルの更
新が必要な場合があります。89 ページの「使用可能なスキーマ要素のリストを更新
するには:」の手順に従ってください。

4 [OK] をクリックします。

編集用のプロパティシートが表示されます。

詳細については、97 ページの「属性のプロパティの参照」を参照してください。

注：ユーザアプリケーションで属性を使用可能にするには、展開が必要です。

エンティティのプロパティの参照

エンティティには次の種類のプロパティを設定できます。

- ◆ 94 ページの「エンティティのアクセスプロパティ」
- ◆ 94 ページの「エンティティの必須プロパティ」
- ◆ 95 ページの「エンティティの検索プロパティ」
- ◆ 96 ページの「エンティティの作成と編集のプロパティ」
- ◆ 96 ページの「パスワード管理プロパティ」

エンティティのアクセスプロパティ

アクセスプロパティは、ユーザアプリケーションがエンティティと対話する方法を制御し
ます。次のプロパティがあります。

プロパティ	説明
作成	選択 — ユーザアプリケーションでこのオブジェクトを作成できます。
編集	非選択 — 基になる ACL に関係なく、このオブジェクトをユーザアプリケー ションで変更できません。 選択 — このオブジェクトは場合によって変更可能ですが、その判別にはア イデンティティボルトの ACL が使用されます。
表示	選択 — ユーザアプリケーションでこのオブジェクトを表示できます。
削除	選択 — ユーザアプリケーションでこのオブジェクトを削除できます。

エンティティの必須プロパティ

エンティティの必須プロパティは次のとおりです。

プロパティ名	説明
キー	このエンティティの固有識別子です。このオブジェクトをユーザアプリケー ションが参照する方法を定義します。
表示ラベル	ユーザインタフェースでオブジェクトを表示する方法を定義します。
クラス名	Novell Directory Service (NDS) のクラス名です。

プロパティ名	説明
LDAP name (LDAP 名)	LDAP オブジェクトクラスの名前です。
検索	選択 — このエンティティを検索できます。識別ポートレット (エンティティ検索リストやエンティティ組織図など) のクエリで使用されるエンティティは選択 (true に設定) する必要があります。
補助クラス	このエンティティの補助クラスのリストです。補助クラスは存在しない場合もあります。 補助クラスを追加する場合、補助クラスの LDAP 名、NDS 名、およびその補助クラスが検索可能かどうかを指定する必要があります。

エンティティの検索プロパティ

エンティティの検索プロパティは次のとおりです。

プロパティ名	説明
検索コンテナ	検索が開始される LDAP ノードまたはコンテナの識別名 (検索ルート)。次に例を示します。 ou=sample, o=ourOrg アイデンティティポータルを参照してコンテナを選択できます。または、 96 ページの「事前定義パラメータの使用」 で説明されている事前定義パラメータの 1 つを使用できます。
検索スコープ	検索ルートから検索対象になる範囲を指定します。 次の値があります。 <デフォルト>— この検索スコープは、[コンテナとサブコンテナ] を選択した場合と同じです。 コンテナ — 検索ルートの DN と検索ルートレベルのすべてのエントリを検索対象とします。 コンテナとサブコンテナ — 検索ルートの DN とすべてのサブコンテナが検索されます。これは <Default> を選択した場合と同じです。 オブジェクト — 指定したオブジェクトに検索スコープを限定します。この検索は、指定したオブジェクトが存在するかどうか確認するために使用されます。
検索制限時間 (ミリ秒)	値をミリ秒単位で指定します。制限時間を指定しない場合は 0 を指定します。
最大検索数	検索で返される検索結果エントリの最大数を指定します。 ランタイム設定を使用する場合は 0 を指定します。 推奨値： 100 ~ 200 の範囲が最も効率的です。 1000 より高い値は設定しないでください。

エンティティの作成と編集のプロパティ

エンティティの作成と編集のプロパティは次のとおりです。

プロパティ名	定義
コンテナの作成	<p>このタイプの新しいエンティティが作成されるコンテナの名前。</p> <p>アイデンティティポータルを参照してコンテナを選択できます。または、96 ページの「事前定義パラメータの使用」で説明されている事前定義パラメータの1つを使用できます。</p> <p>この値が指定されていない場合は、新しいオブジェクトのコンテナを指定するよう促すメッセージが作成ポータルによって表示されます。ポータルではエンティティ定義で指定した検索ルートがベースとして使用され、ユーザは検索ルートからドリルダウンできます。エンティティ定義で検索ルートが指定されていない場合は、ユーザアプリケーションのインストール時に指定したルート DN が使用されます。</p>
名前付け属性	<p>エンティティの名前付け属性 (RDN:Relative Distinguished Name (相対識別名)) です。エンティティでアクセスパラメータの「作成」が選択されている場合だけ、この値が必要です。</p>
代替編集エンティティ	<p>編集エンティティの属性は、詳細ポータルの編集モードで表示されます。</p> <p>ドロップダウンリストからエンティティを選択します。選択しようとしているエンティティが詳細ポータルに表示されない場合は [<なし>] を選択します。</p>

パスワード管理プロパティ

パスワード管理プロパティは次のとおりです。

プロパティ名	定義
パスワード属性	<p>このエンティティのパスワードが保存される属性を選択します。</p>
属性の作成時にパスワードを必要とする	<p>選択 — このエンティティの作成時にパスワードを要求します。</p>

事前定義パラメータの使用

ディレクトリ抽出化レイヤエディタでは、特定の値に対して事前定義パラメータを使用できます。使用できるパラメータは次のとおりです。

事前定義パラメータ	説明
%driver-root%	<p>プロビジョニングドライバの DN を表します。この値はインストール時、あるいはその後の設定時にユーザアプリケーションの設定の中で指定されます。これはユーザアプリケーションのレルム設定に保存されます。</p>
%user-root%	<p>ユーザコンテナ DN を表します。この値はインストール時、あるいはその後の設定時にユーザアプリケーションの設定の中で指定されません。これはユーザアプリケーションのレルム設定に保存されます。</p>

事前定義パラメータ	説明
%group-root%	グループコンテナの DN を表します。この値は、インストール時、あるいはその後の設定時にユーザアプリケーションの設定の中で指定されます。これはユーザアプリケーションのレルム設定に保存されます。

属性のプロパティの参照

属性には次の種類のプロパティを設定できます。

- ◆ 97 ページの「属性のアクセスプロパティ」
- ◆ 98 ページの「属性の必須プロパティ」
- ◆ 98 ページの「属性のフィルタとフォーマットのプロパティ」
- ◆ 98 ページの「属性の UI 制御プロパティ」

属性のアクセスプロパティ

属性のアクセスプロパティは次のとおりです。

名前	説明
編集	選択 — この属性をユーザアプリケーションで編集および変更できます。このプロパティを選択 (true に設定) しても、基となるアイデンティティボールドの ACL や有効な権利で編集が禁止されている場合は、この属性を編集できない場合があります。
有効	非選択 — ユーザアプリケーションでこの属性を使用できなくなります。ファイルからエントリを削除するのと同じです。
非表示	<p>ユーザアプリケーションの [非表示] チェックボックスを有効にするか無効にするかを制御します。ユーザは [非表示] チェックボックスを使用して、属性 (ユーザの写真など) をアプリケーションで表示するかどうかを制御できます。</p> <p>非選択 — この属性に対して [非表示] チェックボックスが無効になるため、ユーザはこの属性を非表示にすることができなくなります。</p> <p>選択 — ユーザアプリケーションで [非表示] チェックボックスが有効になります。ただし、ログインユーザは次の条件を満たしている必要があります。</p> <ul style="list-style-type: none"> ◆ 属性の所有者、またはユーザアプリケーション管理者であること。 ◆ アイデンティティボールドの <code>srvprvHideAttributes</code> 属性を更新するトラスティ権を持っていること。 <p>これらの条件が満たされていなければ、この設定が選択 (true に設定) されていても [非表示] チェックボックスはユーザインタフェースで無効になります。</p>
	<p>ヒント: 画像を含む属性を非表示にした場合でも、前に表示した属性についてはブラウザのキャッシュが更新されるまで画像が表示されることがあります。</p>
複数値	<p>この属性で複数の値を扱えるかどうかを指定します (電話番号など)。</p> <p>選択 — 属性は複数の値を持つことができます。</p>

名前	説明
読み込み	選択 — ユーザアプリケーションはこの属性をクエリできます。大部分の属性でこのプロパティを選択 (true に設定) する必要がありますが、パスワードなど一部の属性では非選択にする必要があります。
必須	選択 — 必ず指定しなければならない属性を示します。
検索	選択 — ユーザアプリケーションはこの属性を検索できます。エンティティ検索リストまたはエンティティ組織図などの識別ポートレットで、クエリに使用される属性は選択する必要があります。
	ヒント: 検索で使用される属性も eDirectory でインデックス化すると、検索が速くなります。
表示	選択 — ユーザアプリケーションはこの属性を表示できます。ほとんどの場合このプロパティを true に設定する必要がありますが、パスワードなど一部の属性では非選択にする必要があります。

属性の必須プロパティ

名前	説明
キー	属性の固有識別子です。
表示ラベル	ユーザアプリケーションで表示されるラベル。
属性名	この属性の NDS 名。
LDAP 名	この属性の LDAP 名。

属性のフィルタとフォーマットのプロパティ

名前	説明
フィルタ: WHERE 属性	この属性でアイデンティティボールドの検索を実行するための LDAP フィルタを指定できます。
有効	選択 — フィルタを有効にします。

属性の UI 制御プロパティ

名前	説明
データタイプ	次のリストからデータタイプを選択します。 <ul style="list-style-type: none"> ◆ バイナリ ◆ ブール ◆ DN ◆ 整数 ◆ LocalizedString ◆ 文字列 ◆ 時間

名前	説明
----	----

フォーマットタイプ	ユーザアプリケーションでデータをフォーマットするために使用されます。次のフォーマットがあります。
-----------	--------------------------------------------------

- ◆ なし
- ◆ AOL IM
- ◆ 電子メール
- ◆ Groupwise IM
- ◆ イメージ
- ◆ 電話番号
- ◆ Yahoo IM
- ◆ イメージ URL
- ◆ 日付
- ◆ DateTime

フォーマットタイプはデータタイプに依存しています。たとえば、時間データタイプは、「日付」と「DateTime」のフォーマットにのみ関連付けられます。

名前	説明
----	----

制御タイプ

制御タイプは次のとおりです。

DNLookup— この属性が DN 参照を含むことを定義します。次の場合に使用します。

- ◆ 関連するエンティティ間での DN 検索の結果をリストに入力する
- ◆ 更新や削除が行われた場合、複数の DN 参照属性間の参照整合性を維持する

ユーザアプリケーションはこの情報を使用して特別なユーザインタフェース要素を生成し、DNLookup 定義に基づいて最適化された検索を実行します。

詳細については、100 ページの「**DNLookup 制御タイプの使用**」を参照してください。

グローバルリスト — この属性をドロップダウンリストで表示します。リストのコンテンツはこの属性定義以外のファイルで定義されます。

詳細については、104 ページの**セクション 4.4 「リストの操作」**を参照してください。

ローカルリスト — この属性をドロップダウンリストで表示します。リストのコンテンツはこの属性で定義されます。ローカルリストを定義するには、次の手順に従います。

1. 属性が選択された状態で、「制御タイプ」を「ローカルリスト」に設定します。



2. [追加] ボタンをクリックしてさらに値を追加します。リスト内の項目の位置を変更するには、上下の矢印ボタンを使用します。

[値] 列で、アイデンティティボールドに書き込む値を入力します。ここで使用できるのは小文字、数字、およびアンダースコア (_) のみです。

3. [ラベル] 列で、ユーザインタフェースに表示するテキストを入力します。

範囲 — 「範囲」制御タイプ (整数データタイプ) を使用してユーザが入力できる値を連続した一定の範囲内に限定します。範囲の開始値と終了値を指定します。

DNLookup 制御タイプの使用

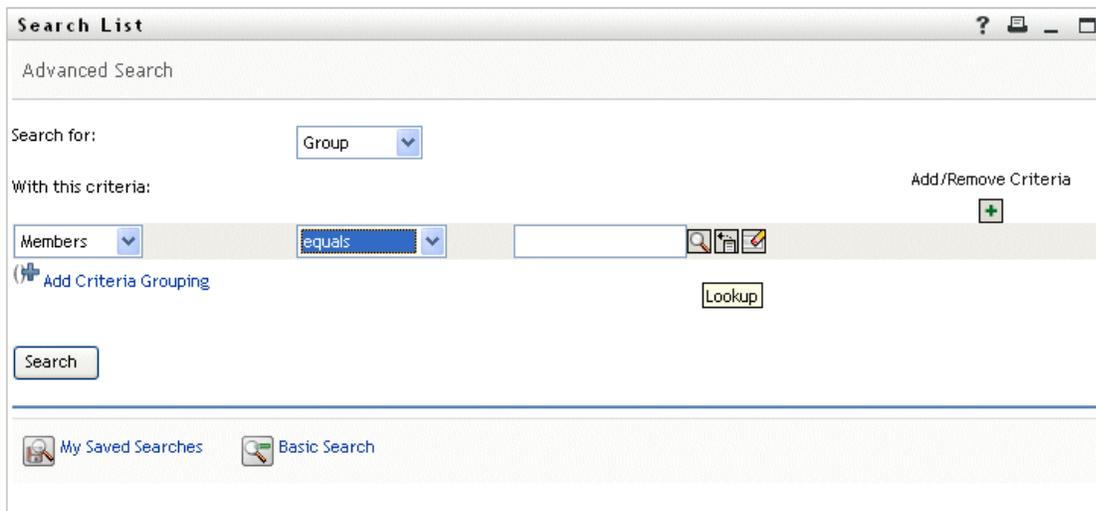
制御タイプを DNLookup として定義した場合、

- ◆ この属性をユーザが検索すると、ユーザは可能な値のリストから選択できます。

- ◆ この属性が作成、入力、または削除されると、ユーザの操作（作成、削除、更新）に基づいて関連するエンティティの属性が適切に更新され、参照整合性が維持されます。

選択リストの DNLookup

インストールされたユーザアプリケーションには「ユーザ」と「グループ」のエンティティ定義が含まれています。「ユーザ」のエンティティ定義には「グループ」とばれる属性があり、DNLookup 制御タイプとして定義されています。これにより、どの識別ポートレットでも、特定ユーザのグループの選択リストを表示できます。たとえば、ユーザがディレクトリ検索を実行するとします。あるグループに属すユーザを検索しようとしたときに、そのグループ名が不明でした。この場合、検索オブジェクトとして「ユーザ」を選択し、検索条件には次のように [グループ] を含めます。



[グループ] は「ユーザ」エンティティの DNLookup 制御タイプとして定義されているため、[ルックアップ] アイコンが表示されます。ユーザがこのアイコンを選択すると、グループの候補リストが表示されます。

First Name	Last Name
Abby	Spencer
Admin	idmsample
Allison	Blake
Angie	Chung
Anthony	Palani
April	Smith

ユーザはリストからグループを選択できます。

参照整合性のための DNLookup

LDAP ではグループ関係を両方向にマップできるため、更新や同期のための DNLookup は重要です。たとえば、次のように設定されているデータがあるとします。

- ◆ ユーザオブジェクトに次のようなグループ属性のいずれかが含まれる。
- ◆ 複数の値。
- ◆ ユーザが属すグループのすべてを一覧表示する。
- ◆ グループオブジェクトに次のようなユーザ属性のいずれかが含まれる。
- ◆ 複数の値。
- ◆ ユーザ属性はグループに属すユーザのすべてを一覧表示する。

この場合、ユーザオブジェクトではユーザが属しているすべてのグループを示す属性を持つことができます。また、グループオブジェクトでは、グループ内のすべてのメンバーを含む DN 属性を持つことができます。

ユーザが更新を要求した場合、ユーザアプリケーションは関係を遵守し、ターゲット属性とソース属性を同期させる必要があります。DNLookup では、同期させる必要がある両方の属性を指定します。この手法を使用して、グループ構造のオブジェクトだけでなく、関連性のあるすべてのオブジェクトを同期させることができます。このタイプの

DNLookup 制御タイプを作成するときは、DNLookup の関係整合性プロパティで説明されている DNLookup の詳細プロパティを指定します。

DNLookup プロパティの参照

DNLookup の表示プロパティは次のとおりです。

フィールド	定義
ルックアップエンティティ	検索するエンティティの名前。たとえば、「タスクグループ」エンティティには「タスクマネージャ」用の属性が含まれます。このフィールドに入力するには、「タスクマネージャ」のユーザを知っている必要があります。
詳細エンティティ	ユーザがユーザアプリケーションのハイパーテキストリンクをクリックして詳しい情報を要求した場合に、詳細を表示するエンティティのキー。DNLookup を定義すると、識別ポートレットでハイパーテキストリンクを表示できるようになります。ユーザはこれを使用してリンク先のオブジェクトの詳細を表示できます。
表示する属性	検索の完了時に表示する属性を 1 つ以上選択します。
自動クエリの実行	表示属性の表示方法を定義します。 <ul style="list-style-type: none">◆ 選択 — エンティティの自動クエリを実行し、結果を選択可能リストに表示します。大量のデータが返される場合は、ユーザが長い結果セットをスクロールしなければならないため、このオプションを選択することはお勧めしません。◆ 非選択 — ユーザがエンティティのクエリの検索条件を指定できるようにします。結果は選択可能リストに表示されます。

DNLookup 関係整合性のプロパティ— このプロパティはグループまたはグループメンバーなど、2 つのオブジェクト間のデータを同期させるために使用されます。

プロパティ	定義
更新するソース属性	更新する属性の名前。属性には「更新するターゲット属性」への DN 参照が含まれている必要があります。これは 2 つの異なるオブジェクトの属性を同期させる場合に必要です。
更新するターゲット属性	「更新するソース属性」と同時に更新が必要な属性の名前。これは LDAP 属性名です。これは、2 つの異なるオブジェクトの属性を同期させる場合に必要です。属性に DN 参照が含まれている必要があります。
ターゲット補助クラス (必要な場合)	「更新するターゲット属性」を含む補助クラスの名前。

4.4 リストの操作

リストノードでは、グローバルリストのコンテンツを定義できます。グローバルリストは、次の目的で Identity Manager ユーザアプリケーションによって使用されます。

- ◆ 属性値のリストを使用できます。属性が編集用としてユーザインタフェースに表示される場合、候補値がドロップダウンリストに表示されます。
- ◆ iManager のプロビジョニング要求の環境設定プラグインで使用可能なカテゴリの定義に使用されます。これは特殊なリストです。詳細については、[106 ページのセクション 4.4.2 「プロビジョニングカテゴリリストについて」](#) を参照してください。

新しいグローバルリストを作成するには：

- 1 次のいずれかの方法で新規リストウィザードを起動します。

プロビジョニングビューから起動する場合

- ◆ [ファイル] > [新規] > [Provisioning (プロビジョニング)] の順にクリックします。[Directory Abstraction Layer List (ディレクトリ抽象化レイヤリスト)] をクリックします。[次へ] をクリックします。
- ◆ [Lists (リスト)] ノードを選択し、右クリックしてから [新規] をクリックします。

ディレクトリ抽出化レイヤエディタから起動する場合

- ◆ [New List (新規リスト)] ボタンをクリックします。
- ◆ [Lists (リスト)] ノードを選択し、右クリックしてから [Add List (リストの追加)] をクリックします。

[New List (新規リスト)] ダイアログボックスが表示されます。

注：[ファイル] メニューから起動した場合、他の方法で起動した場合には表示されないフィールドがダイアログボックスに表示されます。

New List

Specify project and application for the new list as well as the key for the new list.

Identity Manager Project: TestProject

Provisioning Application: User Application

List Key:

Display Label:

< Back Next > Finish Cancel

2 各フィールドに、次のとおり値を指定します。

フィールド	説明
[Identity Manager Project (Identity Manager プロジェクト)] と [Provisioning Application (プロビジョニングアプリケーション)]	エンティティおよび属性を追加する Identity Manager プロジェクトおよびプロビジョニングアプリケーションを選択します。
リストキー	リストの固有識別子です。
表示ラベル	ユーザインタフェースでこのリストが参照されるときに使用される文字列です。

注：これらのフィールドは、[ファイル] メニューからウィザードを起動したときに表示されます。

3 [完了] をクリックします。[Global Lists (グローバルリスト)] プロパティシートが表示されます。

4 次のフィールドに入力します。

フィールド	説明
表示ラベル	Designer で表示されるこのリストの名前。
ラベル	ユーザインタフェースに表示する一覧項目のテキストです。
値	アイデンティティポルトに保存するリスト項目の値です。ここで使用できるのは小文字、数字、およびアンダースコア (_) のみです。

設計環境でリストを使用できるようになりました。

5 プロジェクトを保存します。

注：ランタイム環境でリストを使用可能にするには、展開が必要です。

4.4.1 優先ロケールリストについて

優先ロケールリストは、ブラウザの言語がサポートされている言語ではない場合に使用されるデフォルトの言語を示します。このリストのコンテンツは、ユーザアプリケーションに組み込まれているユーザの編集アクションのデフォルト設定で表示されます。

4.4.2 プロビジョニングカテゴリリストについて

プロビジョニングカテゴリのリストは、プロビジョニングされたリソース (エンタイトルメント) およびプロビジョニング要求の整理に役立つカテゴリのセットを定義します。このリストのカテゴリは次のアプリケーションで表示されます。

- ◆ iManager— プロビジョニング要求の環境設定プラグイン
- ◆ ユーザアプリケーション— [要求と承認] タブ

プロビジョニング要求のリストキーは変更できませんが、リストへの項目追加、既存のカテゴリの値またはラベルの変更は可能です。

プロビジョニングカテゴリのリストのコンテンツを変更するには：

- 1 エディタ上に正しいプロジェクトが開いていることを確認します。
- 2 [Lists (リスト)] ノードをクリックします。
- 3 [プロビジョニングカテゴリ] を選択します。
- 4 グローバルリストのプロパティペインを使用して変更します。

注：カテゴリキーの入力には [値] フィールドを使用します。小文字、数字、およびアンダースコア () 以外は、カテゴリキーとして無効なため [値] フィールドで使用できるのはこれらの文字に限られます。カテゴリキーはカテゴリの識別子としてシステム内部で使用されます。

- 5 変更を保存して、展開します。アプリケーションサーバのキャッシュを更新してください。

変更が展開されると、ユーザアプリケーションおよび iManager プラグインに変更が反映されます。

4.5 組織図の関係の操作

[Org Chart Relationships (組織図の関係)] ノードでは、ディレクトリ抽出化レイヤで定義されたエンティティ間の階層関係を定義できます。関係には、類似したエンティティ間 (ユーザとユーザなど) の関係と、類似していないエンティティ間 (ユーザとデバイスなど) の関係があります。

ユーザアプリケーションでは次の関係が定義されています。

- ◆ グループのメンバーシップ
- ◆ マネージャと従業員
- ◆ ユーザグループ

関係を正常に展開するには、関係のコンポーネントすべて(エンティティと属性)があらかじめ展開されている必要があります。

新しい関係を作成するには：

- 1 次のいずれかの方法で新しい関係を作成できます。

プロビジョニングビューから起動する場合

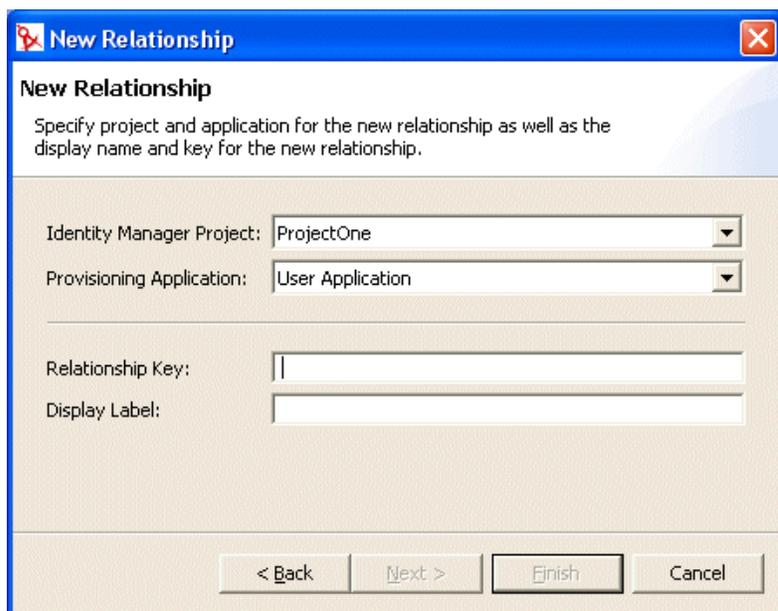
- ◆ [ファイル] > [新規] > [Provisioning (プロビジョニング)] の順にクリックします。[Directory Abstraction Layer Relationship (ディレクトリ抽象化レイヤの関係)] を選択してから、[次へ] をクリックします。
- ◆ [Org Chart Relationships (組織図の関係)] ノードを選択し、右クリックしてから [追加] をクリックします。

ディレクトリ抽出化レイヤエディタから起動する場合

- ◆ [Add Relationship (関係の追加)] ボタンをクリックします。
- ◆ [Org Chart Relationships (ディレクトリ抽象化レイヤの関係)] ノードを選択し、右クリックしてから [Add Relationship (関係の追加)] をクリックします。

[New Relationship (新しい関係)] ダイアログボックスが表示されます。

注：[ファイル] メニューから起動した場合、他の方法で起動した場合には表示されないフィールドがダイアログボックスに表示されます。

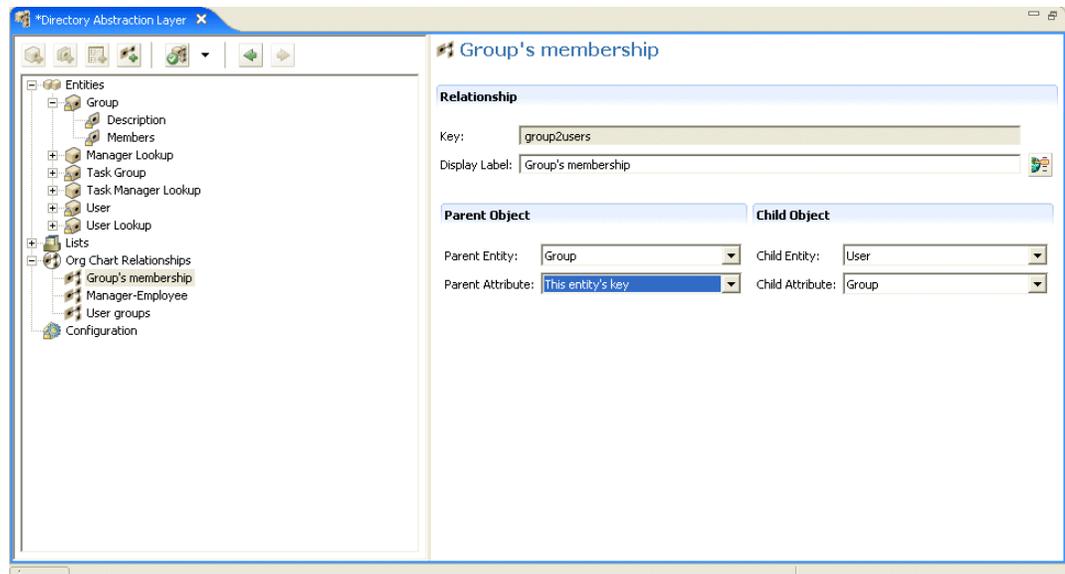


- 2 各フィールドに、次のとおり値を指定します。

フィールド	操作
[Identity Manager Project (Identity Manager プロジェクト)] と [Provisioning Application (プロビジョニングアプリケーション)]	適切な Identity Manager プロジェクトとプロビジョニングアプリケーションが選択されていることを確認してください。 注: このフィールドは、[ファイル] メニューから関係を作成したときに表示されます。
[関係キー]	関係キーの固有値を入力します。
[表示ラベル]	Identity Manager のユーザインタフェースに関係が示されるときに表示させる文字列を入力します。

3 [完了] をクリックします。

関係が作成され、そのプロパティシートが編集用を開きます。



4.5.1 関係のプロパティのリファレンス

フィールド	説明
キー	関係の固有識別子で、読み込み専用です。 ヒント: この値は組織図ポートレットの初期設定シートで指定します。
表示ラベル	この関係が他の識別ポートレットで参照されたときに表示される名前を指定します。たとえば、詳細ポートレットで [Choose Org Chart (組織図の選択)] アイコンをクリックすると、この値が表示されます。 表示ラベルの翻訳テキストを入力するには、[ローカライズ] をクリックします。

フィールド	説明
親エンティティ	<p>ドロップダウンリストからエンティティを選択します。</p> <p>選択したエンティティは、組織図の階層で親オブジェクトになります。たとえば、マネージャと従業員の関係では、親エンティティはユーザになります。グループとメンバーの関係では、親エンティティはグループになります。</p> <p>ディレクトリ抽出化レイヤ要件—このリストのエンティティはディレクトリ抽出化レイヤで定義されたエンティティのサブセットです。親エンティティでは、表示アクセスプロパティが選択 (true に設定) されている必要があります。</p>
親属性	<p>ドロップダウンリストから属性を選択します。</p> <p>この属性は、対応する子エンティティの検索に使用されます。この属性値が子エンティティの属性に含まれる対応した値と一致する場合 (次の「子属性」を参照)、関係を確立できます。</p> <p>ディレクトリ抽出化レイヤ要件—この属性リストの値には、選択した親エンティティの属性が使用されます。DNLookup 制御タイプとして定義された属性だけが含まれます。</p>
子エンティティ	<p>階層で子オブジェクトになるエンティティを選択します。たとえば、マネージャと従業員の関係では、子エンティティはユーザになります。従業員とリソースの関係では、子エンティティはデバイスになります。</p> <p>このエンティティには、親属性に関係した属性が含まれている必要があります。</p>
子属性	<p>親属性に一致する属性を選択します。</p> <p>これは、対応する親エンティティを検索するときに使用される子エンティティの属性を指定します。この属性値が親エンティティの属性に含まれる対応した値と一致する場合 (前の「親属性」を参照)、関係を確立できます。</p>

注：組織図ポートレットでは、ダイナミックグループが完全にはサポートされていません。ダイナミックグループは、関係の親エンティティとしては定義できませんが、子エンティティとしては定義できます。

関係を削除するには：

- 1 削除する関係を選択します。
- 2 右クリックして、[削除] を選択します。

4.6 環境設定の操作

[Configuration (環境設定)] ノードでは、ユーザアプリケーションの一般的な環境設定プロパティを設定できます。次のプロパティがあります。

プロパティ	説明
デフォルト「マイプロファイル」エンティティ	<p>ユーザが、ユーザインタフェースの [マイプロファイル] をクリックしたときに表示されるエンティティを定義します。</p> <p>このフィールドは、オブジェクトクラスがユーザ (または LDAP inetOrgPerson) のエンティティだけを表示するよう制限されています。</p>
デフォルトロケール	<p>ユーザアプリケーションの表示ラベルで使用するデフォルトの言語を定義します。ブラウザに設定されている言語がサポートされていない場合、代わりにこのロケールが使用されます。</p> <hr/> <p>注: ブラウザのロケールは、サポートされている言語のデフォルトロケールよりも優先されます。</p>
コンテナクラス	<p>ユーザの作成アクションまたはグループの作成アクションに、コンテナクラスの選択リストのコンテンツを提供します。ユーザは選択リストから、新しく作成したオブジェクトを保存するコンテナを選択します。</p>

4.7 表示テキストのローカライズ

ディレクトリ抽出化レイヤエディタでは、次の表示テキストを簡単にローカライズできます。

- ◆ エンティティおよび属性の表示ラベル
- ◆ 組織図の関係名
- ◆ グローバルリストおよびローカルリストの項目

4.7.1 サポートされている言語

表示テキストは、次の1つ以上の言語にローカライズできます。

- ◆ 英語
- ◆ フランス語
- ◆ ドイツ語
- ◆ イタリア語
- ◆ 日本語
- ◆ 韓国語
- ◆ ポルトガル語
- ◆ ロシア語
- ◆ 中国語 (簡体字)
- ◆ スペイン語
- ◆ 中国語 (繁体字)

4.7.2 テキストのローカライズ

ディレクトリ抽出化レイヤエディタでは、いくつかの方法で抽出化レイヤ定義をローカライズできます。ローカライズ用のダイアログボックスには次の方法でアクセスできます。

ローカライズするテキストの定義	アクション
ディレクトリ抽出化レイヤでローカライズ可能なすべての項目	<ul style="list-style-type: none">◆ [Set Global Localization (グローバルローカライズの設定)] をクリックします (ディレクトリ抽出化レイヤエディタのツールバーにあります)。 ターゲットフィールドにローカライズしたテキストを入力する前に、ターゲット言語を選択してください。
特定のエンティティ、関係、またはリスト	<ul style="list-style-type: none">◆ ディレクトリ抽出化レイヤエディタのツリービューで、ローカライズするオブジェクトを選択します。◆ 右クリックして、[ローカライズ] を選択します。 ターゲットフィールドにローカライズしたテキストを入力する前に、ターゲット言語を選択してください。
単一の表示ラベル	<ul style="list-style-type: none">◆ 特定のエンティティまたは属性を選択します。◆ [Localize Display Label (表示ラベルのローカライズ)] をクリックします (プロパティペインの [表示ラベル] フィールドの横にあります)。

各ダイアログボックスの外観は少しずつ異なりますが、次のフィールドが含まれています。

- ◆ 元 — 通常はオブジェクトタイプ (エンティティ、リスト、または関係など) とキーです。
- ◆ ソース — 翻訳対象のテキスト (表示ラベル)。
- ◆ ターゲット言語 — サポートされている言語の 1 つ。
- ◆ ターゲット — 翻訳テキスト。

4.8 ディレクトリ抽出化レイヤ定義のインポート、検証、および展開

ディレクトリ抽出化レイヤ定義のインポート、検証、および展開は、Designer のプロビジョニングビューで実行するアクションです。

- ◆ [111 ページのセクション 4.8.1 「インポートについて」](#)
- ◆ [114 ページのセクション 4.8.2 「検証について」](#)
- ◆ [114 ページのセクション 4.8.3 「展開について」](#)

4.8.1 インポートについて

インポート機能では、既存の定義のセットをインポートできます。次の場合にインポートを使用できます。

- ◆ 展開されたプロジェクトを基にして新しいプロジェクトを開始する場合。

- ◆ 同じプロジェクトに携わっている他の開発者と定義を共有する場合。たとえば、他の開発者がユーザエンティティに属性を追加したり、新しいグローバルリストを追加したりすることがあります。この開発者がアイデンティティボールドに新しい定義を展開した場合、ユーザはそれをインポートして、両者が確実に同一の定義を使用するようになります。

既存の定義をインポートするには：

- 1 プロビジョニングビューを開きます。
- 2 インポートするオブジェクトを決定します。
 - ◆ 定義の全セット
 - ◆ 1つの定義タイプのセット (すべてのエンティティやすべての関係など)
 - ◆ 特定のオブジェクト (「ユーザ」エンティティなど)
- 3 次の操作を実行してインポートします。
 - ◆ 特定のオブジェクトをインポートする場合はリストからオブジェクトを選択し、右クリックして [Import Object (オブジェクトのインポート)] を選択します。
 - ◆ 定義の完全なセットをインポートする場合は [Directory Abstraction Layer (ディレクトリ抽象化レイヤ)] ノードを選択し、右クリックして [Import All (すべてインポート)] または [Import Object (オブジェクトのインポート)] をクリックします。
- 4 [eDirectory Browse (eDirectory の参照)] アイコンをクリックして [DirectoryModel] ノードに移動します。インポートするオブジェクトを選択してから [OK] をクリックします。
 - ◆ オブジェクトが一致する場合は、違いがないためインポートは実行されないことを知らせるメッセージが表示されます。
 - ◆ オブジェクトが一致しない場合は、インポートするオブジェクトを確認できます。インポート項目として選択した項目を確認し、必要に応じて変更した後、[OK] をクリックします。

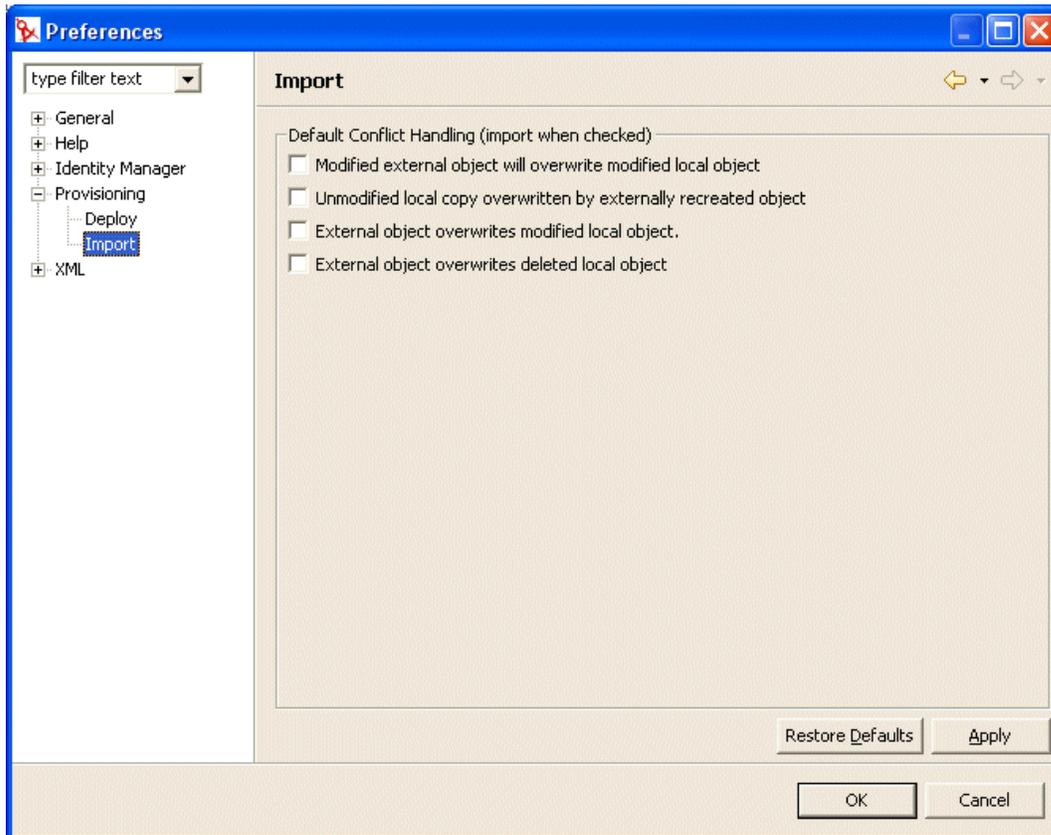
インポートの初期設定

インポートの初期設定では、アイデンティティボールドのデータとローカルのディレクトリ抽出化レイヤファイル間の衝突を Designer が解決する方法を指定できます。別々のユーザやツールがアイデンティティボールドのディレクトリ抽出化レイヤ定義にアクセスするため、こうした衝突が発生することがあります。他の管理者や開発者が、iManager ツールや独自のローカルの Designer ベースプロジェクトを使用して定義を変更することもあります。ローカルファイルシステムとアイデンティティボールドの定義の間で衝突が発生した場合の処理方法を初期設定で指定できます。

インポートの初期設定を行うには：

- 1 [Window (ウィンドウ)] > [初期設定] の順にクリックします。

- 2 ツリーの [Provisioning (プロビジョニング)] ノードを開き、[Import (インポート)] をクリックします。



- 3 初期設定を選択します。

初期設定	説明
Modified external object will overwrite modified local object (変更されている外部のオブジェクトで変更されているローカルオブジェクトを上書きする)	ローカルファイルとアイデンティティボルトの両方の定義に変更が含まれています。ローカルでの変更は、この時点では展開されていません。 アイデンティティボルトオブジェクトがローカルファイルへの変更を上書きするよう設定する場合は、このオプションを選択します。
Unmodified local copy overwritten by externally recreated object (外部で再作成されたオブジェクトで変更されていないローカルコピーを上書きする)	アイデンティティボルトオブジェクトは1度削除されてから再作成されました。ローカルファイルのセットには、変更されていない元の定義が含まれています。 インポート時にローカルコピーを上書きする場合は、このオプションを選択します。
External object overwrites modified local object (変更されているローカルオブジェクトを外部オブジェクトで上書きする)	ローカルファイルには、アイデンティティボルトに展開されていない変更が含まれています。インポート時にローカルファイルを上書きする場合は、このオプションを選択します。

初期設定	説明
External object overwrites deleted local object (削除されているローカルオブジェクトを外部オブジェクトで上書きする)	<p>定義をローカルで削除しましたが、変更が展開されていません。このため、オブジェクトはまだアイデンティティボールドに存在しています。</p> <p>アイデンティティボールドのオブジェクトをローカルファイルシステムにコピーする場合は、このオプションを選択します。このオプションを選択すると、展開されていない変更は失われます。</p>

4.8.2 検証について

ローカルファイルシステムにあるディレクトリ抽出化レイヤのデータ定義は、展開する前に検証できます。検証では次のことが実行されます。

- ◆ XML の形式が正しく、エンティティ、属性、リスト、関係などに必要な要素を定義するスキーマに準拠しているか検証します。
- ◆ すべてのエンティティを確認し、他のエンティティやグローバルリストへの参照が有効であることを確認します。

たとえば、エンティティとその属性を検証する場合、[Edit Entity (編集エンティティ)] フィールド、[DN Lookup (DN ルックアップ)] フィールド、および [Detail Entity (詳細エンティティ)] フィールドを経由する他のエンティティへの参照がすべて、実際に存在するエンティティを参照しているかどうかを検証プログラムが確認します。

- ◆ 各エンティティに属性が少なくとも 1 つ定義されていることを確認します。
- ◆ 各ローカルリストおよびグローバルリストに項目が少なくとも 1 つ含まれていることを確認します。

プロビジョニングビューでは、定義を選択的に検証できます。次の方法で検証を実行できます。

- ◆ ノード内のすべての項目を検証する場合は、ノードを選択し、右クリックしてから [Validate (検証)] をクリックします。
- ◆ ノード内の 1 つのオブジェクトを検証する場合は、オブジェクトを選択し、右クリックしてから [Validate (検証)] をクリックします。

ディレクトリ抽出化レイヤのツールバーにある [Validate Abstraction Layer (抽出化レイヤの検証)] ボタンをクリックすると、すべての定義を検証できます。

注：検証では、アイデンティティボールドにオブジェクトが存在するかどうかの確認は行われません。

4.8.3 展開について

Identity Manager ユーザアプリケーションで変更を反映させるには、アイデンティティボールドに定義を展開する必要があります。

アイデンティティボールドに定義のセットを展開するには：

- 1 ディレクトリ抽出化レイヤエディタを使用して行ったすべての変更を保存します。

展開しようとしたときに変更が未保存の場合、保存されていない定義を示すダイアログボックスが表示されます。このダイアログボックスは最新の変更を保存するよう促します。変更を保存しない場合でもオブジェクトはサーバに展開されますが、未保存の変更は展開されません。変更を保存しないよう選択した場合でも、展開はキャンセルされません。

- 2 プロビジョニングビューを開きます。
- 3 ディレクトリ抽出化レイヤエディタまたはサブセットを使用して定義したオブジェクトをすべて展開するかどうか決定します。

- ◆ 全部を展開する場合：

ルートノードを選択し、右クリックしてから [Deploy All (すべて展開)] をクリックします。

- ◆ 特定のエンティティ、関係、リスト、または環境設定を展開する場合：

展開する対象を選択し、右クリックしてから [Deploy object (オブジェクトの展開)] をクリックします。

アイデンティティボールの資格情報を求めるメッセージが表示される場合があります。エディタにより検証が実行され、検証に関するメッセージがダイアログボックスに表示されます。展開する項目を選択または選択解除して検証メッセージに応答します。展開に必要な選択をした後、展開を実行したら、展開の成功または失敗したことを示すメッセージが表示されます。

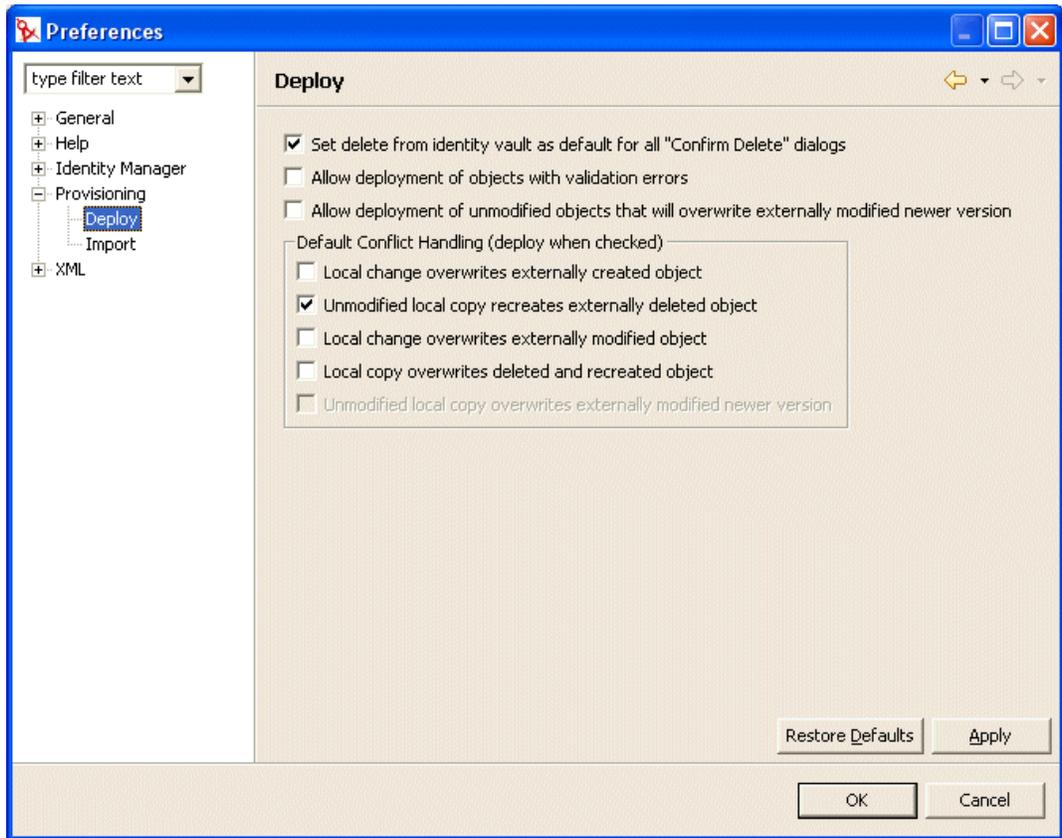
展開の初期設定の選択

展開の初期設定では、アイデンティティボールのデータとローカルのディレクトリ抽出化レイヤファイル間の衝突を Designer が解決する方法を指定できます。他のユーザがアイデンティティボールに変更を展開したにもかかわらず、こうした変更がローカルファイルシステムの定義に反映されていない場合、衝突が発生することがあります。こうした衝突の処理方法を指定するには、初期設定で衝突の解決方法を指定します。

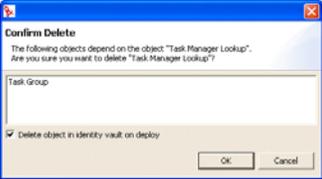
展開の初期設定を行うには：

- 1 [Window (ウィンドウ)] > [初期設定] の順にクリックします。

- ツリーの [Provisioning (プロビジョニング)] ノードを開き、[Deploy (展開)] をクリックします。



- 展開の全般的な初期設定を指定します。

初期設定	説明
Set delete from identity vault as default for all “Confirm Delete” dialogs (すべての「削除の確認」ダイアログボックスで、アイデンティティポータルからの削除をデフォルト設定する)	<p>プロビジョニングビューまたはディレクトリ抽出化レイヤエディタでオブジェクトを削除しようとする、削除の確認を求める次のようなダイアログボックスが表示されます。</p>  <p>この初期設定では、削除の確認ダイアログボックスにある 「Delete object in identity vault on deploy (展開時アイデンティティポールのオブジェクトを削除する)」 のチェックボックスをデフォルトでオンにするかどうかが決まります。この初期設定を選択すると、デフォルトでアイデンティティポールのオブジェクトを常に削除するよう設定されます。</p> <p>ローカルオブジェクトは常に削除されます。</p>
Allow deployment of objects with validation errors (検証エラーのあるオブジェクトの展開を許可する)	<p>選択 — 検証時に問題のあったオブジェクトでも展開する場合はこのオプションを選択します。展開時に、Designer は 111 ページのセクション 4.8「ディレクトリ抽出化レイヤ定義のインポート、検証、および展開」 で説明されている検証ルールに従って、展開中の定義を検証します。</p> <p>非選択 — 検証時に問題のあった定義は展開されません。</p>
Allow deployment of unmodified objects that will overwrite externally modified newer version (変更されていないオブジェクトの展開により、変更されている外部の新しいバージョンが上書きされることを許可する)	<p>選択 — ローカルファイルは変更されていないが、アイデンティティポールのオブジェクトが変更されている場合、ローカルファイルがアイデンティティポールのファイルを上書きするようにするにはこの初期設定を選択します。</p> <p>非選択 — アイデンティティポールの新しいバージョンを維持する場合は、こちらを選択します。</p> <p>このオプションを選択した場合、衝突解決の初期設定で 「Unmodified local copy overwrites externally modified newer version (変更されていないローカルコピーで、変更されている外部の新しいバージョンを上書きする)」 も選択すると、このオプションをデフォルトの動作として設定できます。</p>

4 衝突解決の初期設定を指定します。

初期設定	説明
Local change overwrites externally created object (外部で作成されたオブジェクトをローカルコピーで上書きする)	<p>選択 — 展開中のオブジェクトがアイデンティティポールのオブジェクトを上書きします。</p> <p>非選択 — この衝突が起きた場合、展開は実行されません。</p>

初期設定	説明
Unmodified local copy recreates externally deleted object (変更されていないローカルコピーが外部で削除されたオブジェクトを再生成する)	<p>選択 — 展開中のローカルオブジェクトが、アイデンティティボールドですでに削除されたオブジェクトを作成します。</p> <p>非選択 — この衝突が起きた場合、展開は実行されません。</p>
Local change overwrites externally modified object (外部で変更されたオブジェクトをローカルコピーで上書きする)	<p>選択 — アイデンティティボールドが他のユーザによって変更された場合でも、ローカル定義が常に展開されます。</p> <p>非選択 — この衝突が起きた場合、展開は実行されません。</p>
Local copy overwrites deleted and recreated object (削除および再作成されたオブジェクトをローカルコピーで上書きする)	<p>選択 — アイデンティティボールドのオブジェクトが削除された場合、または削除してから再作成された場合でも、ローカルオブジェクトが常に展開されます。</p> <p>非選択 — この衝突が起きた場合、展開は実行されません。</p>
Unmodified local copy overwrites externally modified newer version (変更されていないローカルコピーで、変更されている外部の新しいバージョンを上書きする)	<p>展開の一般初期設定で [Allow deployment of unmodified objects that will overwrite externally modified newer version (変更されていないオブジェクトの展開により、変更されている外部の新しいバージョンが上書きされることを許可する)] が選択されている場合のみ、この初期設定を使用できます。</p> <p>選択 — ローカルファイルは未変更で、アイデンティティボールドのオブジェクトが変更されている場合、ローカルファイルは常にデフォルトの動作としてアイデンティティボールドのファイルを上書きします。</p> <p>非選択 — アイデンティティボールドの新しいバージョンを維持する場合は、こちらを選択します。</p>

ログの設定

この章では次の内容を説明します。

- ◆ 119 ページのセクション 5.1 「イベントログについて」
- ◆ 119 ページのセクション 5.2 「Novell Audit サーバへのログ」

5.1 イベントログについて

Identity Manager ユーザアプリケーションは、Apache Software Foundation より配布されるオープンソースログパッケージである *log4j* を使用してログを行います。デフォルトでは、イベントメッセージは、システムコンソールおよびアプリケーションサーバのログファイルに、「情報」以上のログレベルで記録されます。Novell Audit でログするように、ユーザアプリケーションを設定することもできます。イベントは、アクティブ化されたすべてのロガー（ログの記録先）に記録されます。

重要 : Novell Audit にログする場合は、[Novell Audit のドキュメント \(http://www.novell.com/documentation/nsureaudit\)](http://www.novell.com/documentation/nsureaudit) を参照することをお勧めします。

5.1.1 ログレベル設定について

コンソールのログでは、同期書き込みが行われます。このため、ログの書き込み作業によってプロセッサ使用率の問題や同時並行のインピーダンスの問題が起こる可能性があります。<installdir>/jboss/server/IDMProv/conf/log4j.xml の設定を変更することにより、優先度のデフォルト値を ERROR に変更できます。次のような root ノードを見つけます。

```
<root> <appender-ref ref="CONSOLE"/> <appender-ref ref="FILE"/> </root>
```

優先度の値を次のように変更します。

```
<root> <priority value="ERROR"/> <appender-ref ref="FILE"/> </root>
```

root に値を割り当てると、レベルが明示的に割り当てられていないアペンダはすべて root のレベルを継承するようになります。デフォルトでは、ファイルアペンダにはしきい値レベルが割り当てられていないため、root のしきい値レベルを引き継ぎます。しきい値レベルが割り当てられている root 内のアペンダは、ERROR または WARN のいずれにするのが妥当です。エラーレベルを WARN より高く設定すると、パフォーマンスに影響が出ます。

5.2 Novell Audit サーバへのログ

Novell Audit サーバにログするには、次の手順に従います。

ステップ	操作	参照先
1	Identity Manager アプリケーションスキーマをログアプリケーションとして Novell Audit サーバに追加します。	120 ページのセクション 5.2.1 「ログアプリケーションとしての Identity Manager アプリケーションスキーマの Novell Audit サーバへの追加」
2	アプリケーションサーバ上で Novell Audit のプラットフォームエージェントを設定します。	<p>Novell Audit にイベントをレポートするクライアントはすべて、プラットフォームエージェントを必要とします。プラットフォームエージェントは、logevent 環境設定ファイルで設定できます。このファイルには、プラットフォームエージェントが Novell Audit サーバと通信するために必要な構成情報が含まれています。このファイルは、デフォルトで、アプリケーションサーバ上の次の場所にあります。</p> <ul style="list-style-type: none"> ◆ Linux—/etc/logevent.conf ◆ Windows—<WindowsDir>/logevent.cfg (通常は c:¥windows) <p>「LogHost」設定で、Novell Audit サーバの IP アドレスまたは DNS 名を指定します。次に例を示します。</p> <pre>LogHost=xxx.xxx.xxx.xxx</pre> <p>環境に応じて他の設定を指定します。</p> <hr/> <p>重要 : logevent 環境設定ファイルを作成または変更した後は、JBoss アプリケーションサーバを再起動して変更を有効にする必要があります。</p> <hr/> <p>logevent 環境設定ファイル構造の詳細については、『Novell Audit Administration Guide』のログシステムに関する章の「Configuring the Platform Agent」(http://www.novell.com/documentation/nsureaudit) の節を参照してください。</p>
3	Novell Audit のログを有効にします。	121 ページのセクション 5.2.2 「Novell Audit のログの有効化」

5.2.1 ログアプリケーションとしての Identity Manager アプリケーションスキーマの Novell Audit サーバへの追加

ログアプリケーションとして Identity Manager ユーザアプリケーションを使用するよう Novell Audit を設定するには、次の手順に従います。

- 1 次のファイルを見つけます。

```
DirXML.lsc
```

プラットフォーム	場所
Linux	インストール後： /opt/novell/naudit/logschema/dirxml.lsc
Windows	インストールメディア上： /nt/dirxml/nsure_audit/nauditextensions/lsc/ dirxml.lsc

- 2 Web ブラウザを使用して iManager にアクセスし、管理者としてログインします。
- 3 [Roles and Tasks (役割とタスク)] > [Auditing and Logging (監査とログ)] の順にクリックし、[Logging Server Options (ログサーバオプション)] を選択します。
- 4 ツリー内の [Logging Services container (ログサービスコンテナ)] を参照し、適切な [Audit Secure Logging Server (監査セキュアログサーバ)] を選択します。[OK] をクリックします。
- 5 [Log Applications (ログアプリケーション)] タブを表示し、適切なコンテナ名を選択してから [New Log Application (新規ログアプリケーション)] リンクをクリックします。
- 6 [New Log Application (新規ログアプリケーション)] ダイアログボックスが表示されたら、次のように指定します。

設定項目	操作
Log Application Name (ログアプリケーション名)	ユーザの環境に応じた適切な名前を入力します。
Import LSC File (LSC ファイルのインポート)	[参照] ボタンを使って、DirXML.lsc ファイルを選択します。

- [OK] をクリックします。追加されたアプリケーションの名前が [Log Applications (ログアプリケーション)] タブに表示されます。
- 7 [OK] をクリックして Novell Audit サーバの設定を完了します。
 - 8 ログアプリケーションのステータスがオンになっていることを確認してください。オンの場合、ステータスの下の円が緑色になっています。赤の場合は、クリックしてオンにしてください。
 - 9 Novell Audit サーバを再起動して、新しいログアプリケーション設定を有効にします。

5.2.2 Novell Audit のログの有効化

Identity Manager ユーザアプリケーションで Novell Audit のログを有効にするには：

- 1 管理者としてユーザアプリケーションにログインします。

- 2 [管理] タブを選択します。
- 3 [ログ] タブを選択します。
- 4 [ログメッセージを Audit にも送信する] チェックボックス (タブの下部) をオンにします。
- 5 後でアプリケーションサーバが再起動されてもこの変更が維持されるように、[ログ変更を保持する] が選択されていることを確認します。

5.2.3 ログ対象イベントの種類

Identity Manager ユーザアプリケーションは、ワークフロー要求、検索要求、詳細要求、およびパスワード要求から自動的にイベントセットをログします。デフォルトでは、Identity Manager ユーザアプリケーションはアクティブなログチャンネルすべてに次のイベントを自動的にログします。

イベント ID	プロセス	イベント	重大度
31400	詳細ポートレット	Delete_Entity	情報
31401		Update_Entity	情報
31410	パスワード変更ポートレット	Change_Password_Failure	エラー
31411		Change_Password_Success	情報
31420	パスワードを忘れた場合のポートレット	Forgot_Password_Change_Failure	エラー
31421		Forgot_Password_Change_Success	情報
31430	検索ポートレット	Search_Request	情報
31431		Search_Saved	情報
31440	作成ポートレット	Create_Entity	情報

イベント ID	プロセス	イベント	重大度
31520	ワークフロー	Workflow_Error	エラー
31521		Workflow_Started	情報
31522		Workflow_Forwarded	情報
31523		Workflow_Reassigned	情報
31524		Workflow_Approved	情報
31525		Workflow_Refused	情報
31526		Workflow_Ended	情報
31527		Workflow_Claimed	情報
31528		Workflow_Unclaimed	情報
31529		Workflow_Denied	情報
3152A		Workflow_Completed	情報
3152B		Workflow_Timedout	情報
3152C		User_Message	情報
31533		Workflow_Retracted	情報
3152D	プロビジョニング	Provision_Error	エラー
3152E		Provision_Submitted	情報
3152F		Provision_Success	情報
31530		Provision_Failure	エラー
31531		Provision_Granted	情報
31532		Provision_Revoked	情報

イベント ID	プロセス	イベント	重大度
31450	セキュリティコンテキスト	Create_Proxy_Definition_Success	情報
31451		Create_Proxy_Definition_Failure	エラー
31452		Update_Proxy_Definition_Success	情報
31453		Update_Proxy_Definition_Failure	エラー
31454		Delete_Proxy_Definition_Success	情報
31455		Delete_Proxy_Definition_Failure	エラー
31456		Create_Delegatee_Definition_Success	情報
31457		Create_Delegatee_Definition_Failure	エラー
31458		Update_Delegatee_Definition_Success	情報
31459		Update_Delegatee_Definition_Failure	エラー
3145A		Delete_Delegatee_Definition_Success	情報
3145B		Delete_Delegatee_Definition_Failure	エラー
3145C		Create_Availability_Success	情報
3145D		Create_Availability_Failure	エラー
3145E		Delete_Availability_Success	情報
3145F		Delete_Availability_Failure	エラー

5.2.4 ログレポート

Novell Audit のデータベースチャネルにイベントのログを記録する場合、そのデータに関するレポートを生成することができます。Novell Audit のデータベースにログされるデータに対し、次のような方法でレポートを生成できます。

- ◆ Novell Audit のレポートアプリケーションを使用して、独自のレポートを実行する。または、次の [124 ページの「事前定義されたログレポート」](#) で説明されている事前定義レポートを実行する。
- ◆ iManager の [Auditing and Logging (監査とログ)] > [Queries (クエリ)] を使用して、ログデータに対するクエリを記述する。
- ◆ ログデータに対する SQL クエリを独自に記述する。

デフォルトの Novell Audit のテーブルは NAUDITLOG です。

事前定義されたログレポート

次の事前定義されたログレポートが Crystal Reports (.rpt) 形式で作成され、Novell Audit データベースにログされたデータをフィルタリングできます。

レポート名	説明
Administrative Action Report (管理アクションレポート)	Identity Manager のユーザアプリケーションポータルで開始された管理アクションがすべて表示されます。このレポートには、アクションを開始した管理者名が含まれます。 iManager または Designer for IDM を使用して実行された管理上の変更は除外されます。
Historical Approval Flow Report (認証フロー履歴レポート)	指定した期間内での認証フローのアクティビティが表示されます。
Resource Provisioning report (リソースプロビジョニングレポート)	すべてのプロビジョニングアクティビティがリソース別に表示されます。
Specific User Audit Trail (特定ユーザの監査記録)	あるユーザに関するアクティビティがすべて表示されます。アクティビティには、プロビジョニングとセルフサービスの両方のアクティビティが含まれます。
Specific User Provisioning report (特定ユーザのプロビジョニングレポート)	特定ユーザのプロビジョニングアクティビティがすべて表示されます。
User Provisioning report (ユーザプロビジョニングレポート)	すべてのプロビジョニングアクティビティがユーザ別に表示されます。

サンプルレポート 次に、「Specific User Audit Trail (特定ユーザの監査記録)」 レポートのサンプルを示します。

Novell® Audit Report for Identity Manager

Specific User Audit Trail

Report Period: - 10/13/2005 8:51:32AM

User ID: ablake

Report Last Modified: 10/13/2005

Report Generated On: 10/13/2005

Total pages: 8

Approval Flow

Workflow Event: fecedbe80a3d4abd83c9476a1b576ea2

Date / Time	Action	Initiator ID
9/12/2005 3:20:42PM	Workflow Started	cn=ablake,ou=users,ou=idm sample-Jeff,o=novell
9/12/2005 3:20:43PM	Workflow Forwarded	Workflow Administrator
9/12/2005 3:25:43PM	Workflow Reassigned	Unclaimed
9/12/2005 3:30:44PM	Workflow Forwarded	Workflow Administrator
9/12/2005 3:30:44PM	Workflow Ended	Workflow Administrator
9/12/2005 3:30:44PM	Workflow Denied	System

Workflow Event: fc6d74b1268243b3beac52261439dea0

Date / Time	Action	Initiator ID
9/28/2005 1:12:19PM	Workflow Started	cn=ablake,ou=users,ou=idm sample-Jeff,o=novell
9/28/2005 1:12:22PM	Workflow Forwarded	Workflow Administrator
9/28/2005 2:12:23PM	Workflow Forwarded	Workflow Administrator
9/28/2005 2:12:23PM	Workflow Forwarded	Workflow Administrator
9/28/2005 2:12:23PM	Workflow Forwarded	Workflow Administrator
9/28/2005 2:12:23PM	Workflow Forwarded	Workflow Administrator
9/28/2005 2:12:23PM	Workflow Approved	System
9/28/2005 2:12:23PM	Workflow Approved	System
9/28/2005 2:12:23PM	Workflow Completed	Workflow Administrator
9/28/2005 2:12:27PM	Workflow Forwarded	Workflow Administrator
9/28/2005 2:12:27PM	Workflow Ended	Workflow Administrator
9/28/2005 2:12:27PM	Provision Submitted	Workflow Administrator
9/28/2005 2:12:27PM	Provision Granted	Workflow Administrator

Workflow Event: efaa8304e07641edb9e6375a1a36e396

Date / Time	Action	Initiator ID
10/12/2005 11:58:13AM	Workflow Started	cn=ablake,ou=users,ou=idm sample-qatest,o=novell
10/12/2005 11:58:13AM	Workflow Forwarded	Workflow Administrator

Workflow Event: ea341eb11a824e669e356837745fe264

Date / Time	Action	Initiator ID
9/27/2005 4:24:44PM	Workflow Started	cn=m m ackenzie,ou=users,ou=idm sample-Jeff,o=novell
9/27/2005 4:24:44PM	Workflow Forwarded	Workflow Administrator

レポートファイルの場所 レポートファイルは次の場所に保存されます。

プラットフォーム

場所

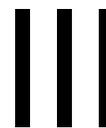
Windows

/nt/dirxml/reports

これらのレポートをテンプレートとして使用して、Crystal Reports Designer でカスタムレポートを作成できます。また、Novell Audit 付属の Windows プログラムである Audit Report (lreport.exe) を使用してレポートを実行することもできます。事前定義されたレポートは、Novell Audit のデフォルトログデータベース *naudit* とデータベーステーブル *nauditlog* に対してデータの問い合わせを行います。ご使用の Novell Audit ログデータベースの名前が異なる場合は、Crystal Reports Designer の [Set Datasource Location (データソースの場所の設定)] メニュー項目を使用して、データベース名 *naudit* を実際のデータベース名に変えてください。

詳細については、Novell Audit のマニュアル (<http://www.novell.com/documentation/nsureaudit>) のレポート操作に関する節を参照してください。

ユーザアプリケーションの管理



次の章では、ユーザインタフェースの [管理] タブを使用して、Identity Manager ユーザアプリケーションを設定および管理する方法について説明します。

- ◆ 131 ページの第 6 章「[管理] タブの使用」
- ◆ 137 ページの第 7 章「ページの管理」
- ◆ 175 ページの第 8 章「テーマの環境設定」
- ◆ 181 ページの第 9 章「ポートレットの管理」
- ◆ 201 ページの第 10 章「ポータル環境設定」
- ◆ 209 ページの第 11 章「セキュリティの環境設定」
- ◆ 213 ページの第 12 章「ログの環境設定」
- ◆ 219 ページの第 13 章「キャッシングの環境設定」
- ◆ 229 ページの第 14 章「ポータルデータのエクスポートおよびインポートのためのツール」

[管理] タブの使用

この章では Identity Manager ユーザインタフェースの [管理] タブを使用する方法を解説します。[管理] タブを使用して Identity Manager ユーザアプリケーションを設定および管理する方法について説明します。ここで取り扱う内容は次のとおりです。

- ◆ 131 ページのセクション 6.1 「[管理] タブについて」
- ◆ 131 ページのセクション 6.2 「[管理] タブを使用できるユーザ」
- ◆ 132 ページのセクション 6.3 「[管理] タブへのアクセス」
- ◆ 135 ページのセクション 6.4 「実行できる管理アクション」

6.1 [管理] タブについて

Identity Manager のユーザインタフェースには、主にエンドユーザがアクセスし、タブから、識別セルフサービスやワークフローベースのプロビジョニング (Provisioning Module for Identity Manager を使用) を行うことができます。このブラウザベースのユーザインタフェースには、[管理] タブも用意されており、管理者がアクセスして、基本的な Identity Manager ユーザアプリケーションのさまざまな特性を設定できます。

たとえば、次の場合に [管理] タブを使用できます。

- ◆ ユーザインタフェースの外観と操作方法のテーマの変更。
- ◆ エンドユーザが使用する識別セルフサービス機能のカスタマイズ。
- ◆ 管理アクションを実行できるユーザの指定。
- ◆ ユーザアプリケーションおよびその実行方法に関する他の詳細情報の管理。

6.2 [管理] タブを使用できるユーザ

[管理] タブは、Identity Manager ユーザインタフェースの通常のエンドユーザには表示されません。このタブの表示およびアクセスが可能なユーザは次の 2 つのタイプに限定されます。

- ◆ ユーザアプリケーション管理者

ユーザアプリケーション管理者は、Identity Manager ユーザアプリケーションに関連するすべての管理機能を実行できます。この中には、Identity Manager ユーザインタフェースの [管理] タブにアクセスし、そこでサポートされているすべての管理アクションを実行する操作も含まれます。

インストール中、任意のユーザを 1 人、ユーザアプリケーション管理者として指定します。インストール後、そのユーザは [管理] タブにある [セキュリティ] ページを使用して、必要に応じてその他のユーザアプリケーション管理者を指定できます。

詳細については、209 ページの第 11 章「セキュリティの環境設定」を参照してください。

- ◆ ユーザアプリケーション管理者によって許可されたユーザ

必要に応じて、ユーザアプリケーション管理者は、1人または複数のエンドユーザに対し、[管理] タブの特定のページへのアクセス許可を割り当てることができます。これらの許可の割り当てには、[管理] タブの [ページ管理] ページを使用します。詳細については、[137 ページの第7章「ページの管理」](#)を参照してください。

6.3 [管理] タブへのアクセス

ユーザアプリケーション管理者(または許可された他のユーザ)になると、Identity Manager ユーザアプリケーションを管理する必要がある場合に、Identity Manager ユーザインタフェースの [管理] タブにアクセスできます。アクセスに必要なのはサポートされた Web ブラウザのみです。

サポートされている Web ブラウザの詳細については、『Novell Identity Manager: インストールガイド』を参照してください。

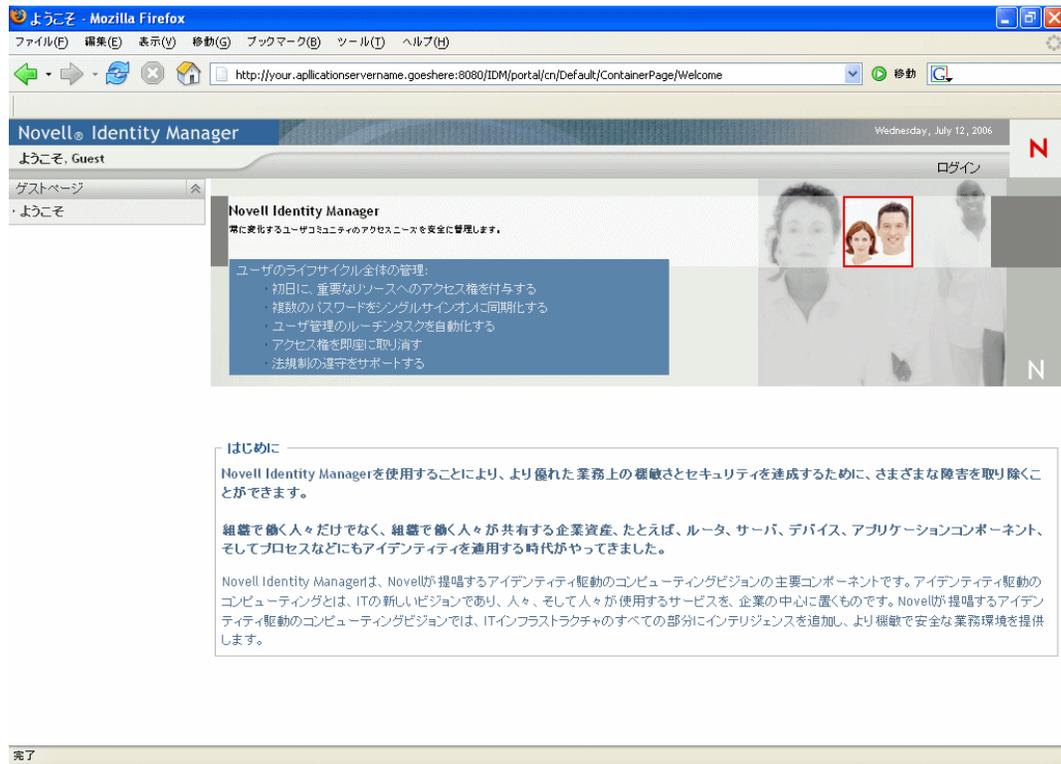
注: Identity Manager ユーザインタフェースを使用する場合、Web ブラウザで「JavaScript が有効になっている」ことを確認してください。

[管理] タブにアクセスするには:

- 1 Web ブラウザで、Identity Manager ユーザインタフェースの URL へ移動します(サイトの設定により異なります)。次に例を示します。

`http://myappserver:8080/IDM`

ユーザインタフェースの初期画面が開きます。

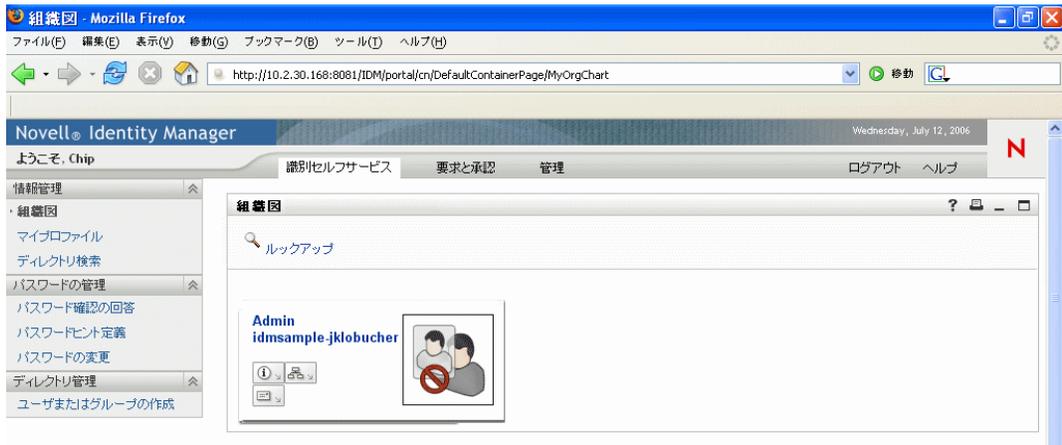


- 2 ページヘッダの [ログイン] リンクをクリックします。
ユーザ名とパスワードの入力を促すメッセージが表示されます。



- 3 ユーザアプリケーション管理者 (または [管理] タブにアクセスできるユーザ) のユーザ名とパスワードを入力し、[ログイン] をクリックします。

ログインすると、そのユーザに指定されたユーザインタフェースのコンテンツが表示されます。次に例を示します。



デフォルトでは、[識別セルフサービス] タブが表示されます。

4 [管理] タブをクリックします。

[管理] タブには、実行できる管理者アクションのメニューが表示されます。メニューの各項目から、対応する設定や制御のページが表示されます。デフォルトでは、[ページ管理] ページが表示されます。



Identity Manager ユーザインタフェースのアクセスや操作に関する一般的な情報については、『Identity Manager ユーザアプリケーション：ユーザズガイド』を参照してください。

6.4 実行できる管理アクション

[管理] タブが表示されたら、使用可能なアクションを使用して Identity Manager ユーザーアプリケーションを設定および管理できます。次に各アクションの要約を示します。

アクション	説明
ページ管理	<p>Identity Manager ユーザインタフェースに表示されるページ、およびそのページにアクセスできるユーザを制御します。</p> <p>詳細については、137 ページの第 7 章「ページの管理」を参照してください。</p>
テーマ	<p>Identity Managery ユーザインタフェースの外観と操作方法を決定します。</p> <p>詳細については、175 ページの第 8 章「テーマの環境設定」を参照してください。</p>
ポートレット管理	<p>Identity Manager ユーザインタフェースで使用できるポートレット、およびそれらにアクセスできるユーザを制御します。</p> <p>詳細については、181 ページの第 9 章「ポートレットの管理」を参照してください。</p>
ポータル	<p>Identity Manager ユーザーアプリケーションのポータル特性を制御し、ユーザーアプリケーションがアイデンティティボールド (LDAP プロバイダ) に接続する方法を指定します。</p> <p>詳細については、201 ページの第 10 章「ポータルの環境設定」を参照してください。</p>
セキュリティ	<p>Identity Manager ユーザーアプリケーションのユーザーアプリケーション管理者を指定します。</p> <p>詳細については、209 ページの第 11 章「セキュリティの環境設定」を参照してください。</p>
ログ	<p>Identity Manager ユーザーアプリケーションが生成するログメッセージのレベルを制御し、これらのメッセージを Novell Audit に送信するかどうかを指定します。</p> <p>詳細については、213 ページの第 12 章「ログの環境設定」を参照してください。</p>
キャッシング	<p>Identity Manager ユーザーアプリケーションが使用するさまざまなキャッシュを管理します。</p> <p>詳細については、219 ページの第 13 章「キャッシングの環境設定」を参照してください。</p>
ツール	<p>Identity Manager ユーザーアプリケーションによって使用されるポータルコンテンツ (ページとポートレット) をエクスポートおよびインポートできます。</p> <p>詳細については、229 ページの第 14 章「ポータルデータのエクスポートおよびインポートのためのツール」を参照してください。</p>

ページの管理

この章では、Identity Manager ユーザインタフェースの [管理] タブの [ページ管理] ページを使用する方法について説明します。ここで取り扱う内容は次のとおりです。

- ◆ 137 ページのセクション 7.1 「ページの管理について」
- ◆ 144 ページのセクション 7.2 「コンテナページの作成とメンテナンス」
- ◆ 153 ページのセクション 7.3 「共有ページの作成とメンテナンス」
- ◆ 163 ページのセクション 7.4 「ページの許可を割り当てる」
- ◆ 170 ページのセクション 7.5 「グループのデフォルトページを設定する」
- ◆ 172 ページのセクション 7.6 「コンテナページのデフォルト共有ページを選択する」

[管理] タブにアクセスして操作する一般的な情報については、131 ページの第 6 章「[管理] タブの使用」を参照してください。

7.1 ページの管理について

[ページ管理] のページを使用して、Identity Manager ユーザインタフェースに表示されるページを制御したり、それに対するアクセス権をユーザに割り当てたりすることができます。ユーザインタフェースは次の 2 種類のページで構成されます。

ページの種類	説明
コンテナ	コンテナページは、共有ページの外観と操作方法、企業ブランドマーク、およびナビゲーション方法の一貫性を保つ役目を果たします。
共有	共有ページは特定の目的 (ユーザのプロファイルの更新など) に使用される、整合性のとれたコンテンツのセットを提供します。これは複数のユーザが使用するサービスを提供することから共有ページと呼ばれます。

どちらのページタイプでも、コンテンツの形式は、ポートレット (Java 標準プラグ可能ユーザインタフェースエレメント) 形式になります。

ポートレットの詳細については、181 ページの第 9 章「ポートレットの管理」および 237 ページのパート IV 「ポートレット参照」を参照してください。

7.1.1 コンテナページについて

この節では、Identity Manager ユーザインタフェースで重要な役割を果たすいくつかのコンテナページについて説明します。

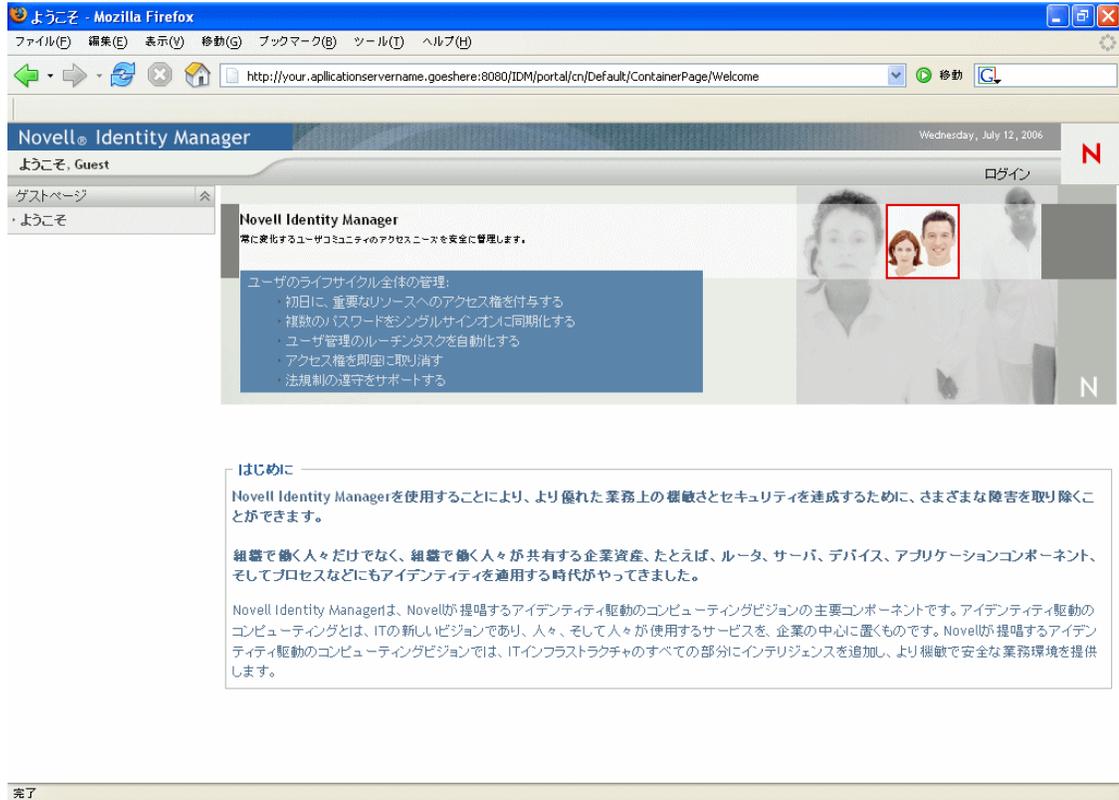
- ◆ 138 ページの「GuestContainerPage」
- ◆ 140 ページの「DefaultContainerPage」
- ◆ 141 ページの「管理コンテナページ」

これらのコンテナページは、必要に応じて変更できます。また、独自のコンテナページを追加することもできます。

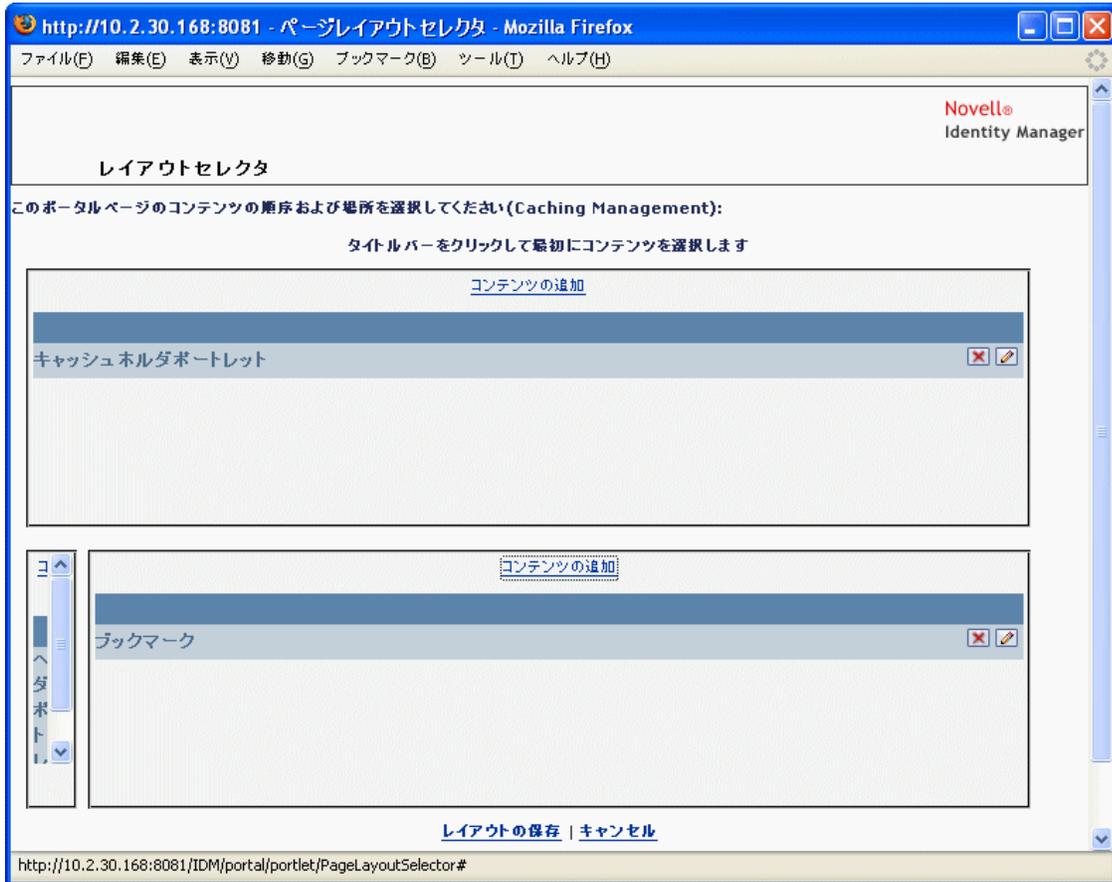
コンテナページの操作については、144 ページのセクション 7.2 「コンテナページの作成とメンテナンス」を参照してください。

GuestContainerPage

デフォルトでは、ユーザが Identity Manager ユーザインタフェースにアクセスすると、ログインの前に GuestContainerPage と呼ばれるコンテナページが表示されます。このコンテナページは次のような外観をしています。



GuestContainerPage の内部は、次のようなレイアウトになっています。



GuestContainerPage のレイアウトは3つの領域に分けられており、それぞれに次のポートレットが表示されます。

ポートレット	説明
HeaderPortlet	ユーザインタフェースのヘッダ情報およびトップレベルのタブコントロールが表示されます。
共有ページナビゲーション	メニューが縦に表示され、ユーザはこのメニューから共有ページを選択して表示できます。
ポータルページコントローラ	ユーザが共有ページナビゲーションポートレットで現在選択している共有ページが表示されます。

デフォルトでは、ユーザがログインする前は、これらのポートレットに次のコンテンツのみ表示されます。

- ◆ ヘッダ内に1つのリンク: ログイン
- ◆ 1つの共有ページ: ようこそ

ユーザがまだログインしていないため、共有ページナビゲーションポートレットは、[Guest ページ] カテゴリにある共有ページのみを表示し、他のカテゴリはすべて除外し

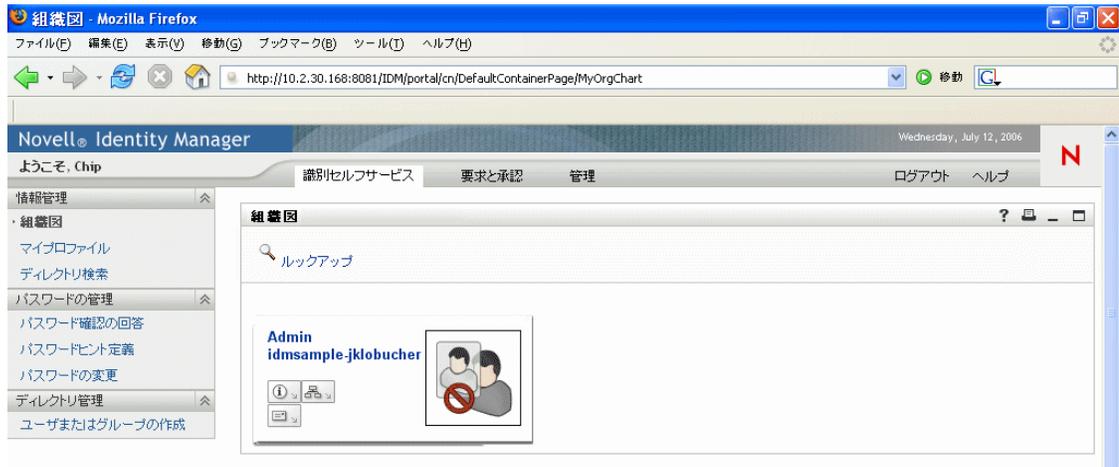
ます。デフォルトでは [ようこそ] ページだけが [Guest ページ] カテゴリに表示されます。

ログイン後、共有ページナビゲーションポートレットは [Guest ページ] カテゴリを除外します。代わって共有ページの他のカテゴリが表示されます (初期設定に従います)。

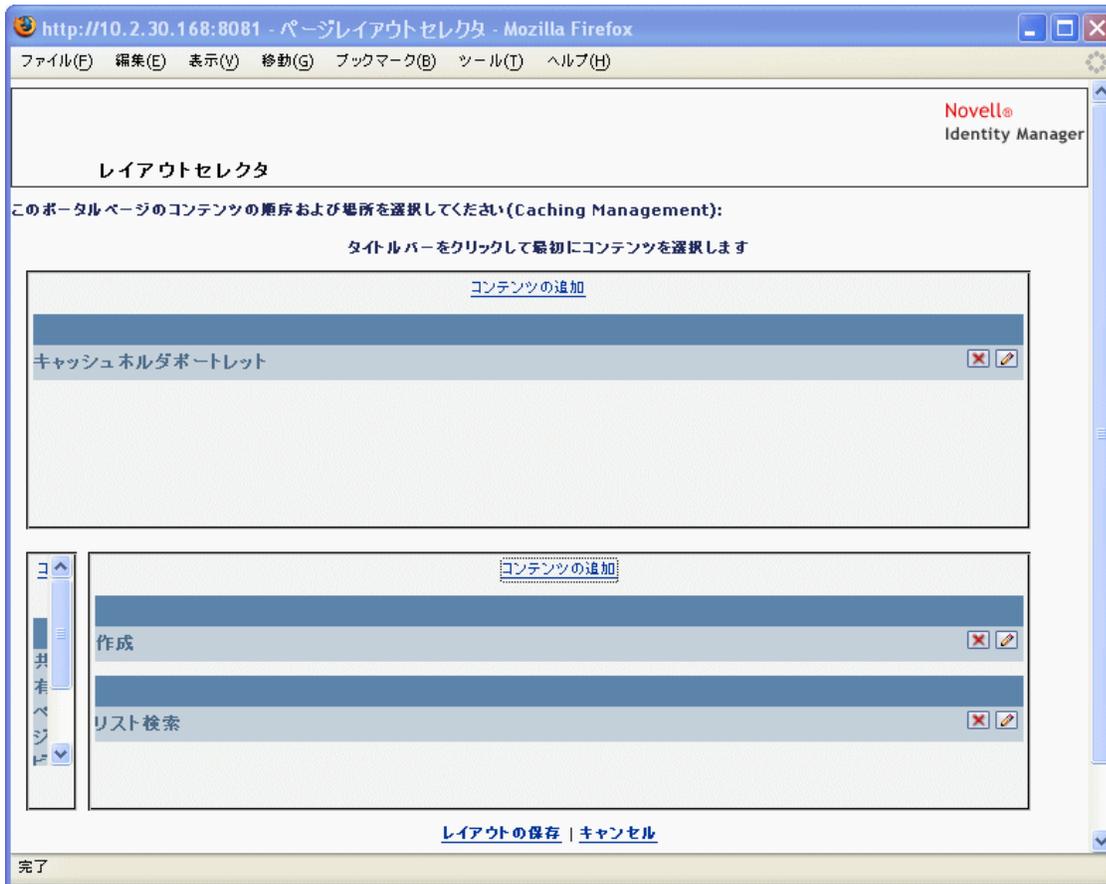
共有ページナビゲーションポートレットの詳細については、[239 ページの第 15 章「ポートレットについて」](#)を参照してください。

DefaultContainerPage

デフォルトでは、ユーザが Identity Manager ユーザインタフェースにログインすると、DefaultContainerPage と呼ばれるコンテナページに移動します。このコンテナページは次のような外観をしています。



DefaultContainerPage の内部は、次のようなレイアウトになっています。



DefaultContainerPage のレイアウトは3つの領域に分けられており、それぞれに次のポートレットが表示されます。

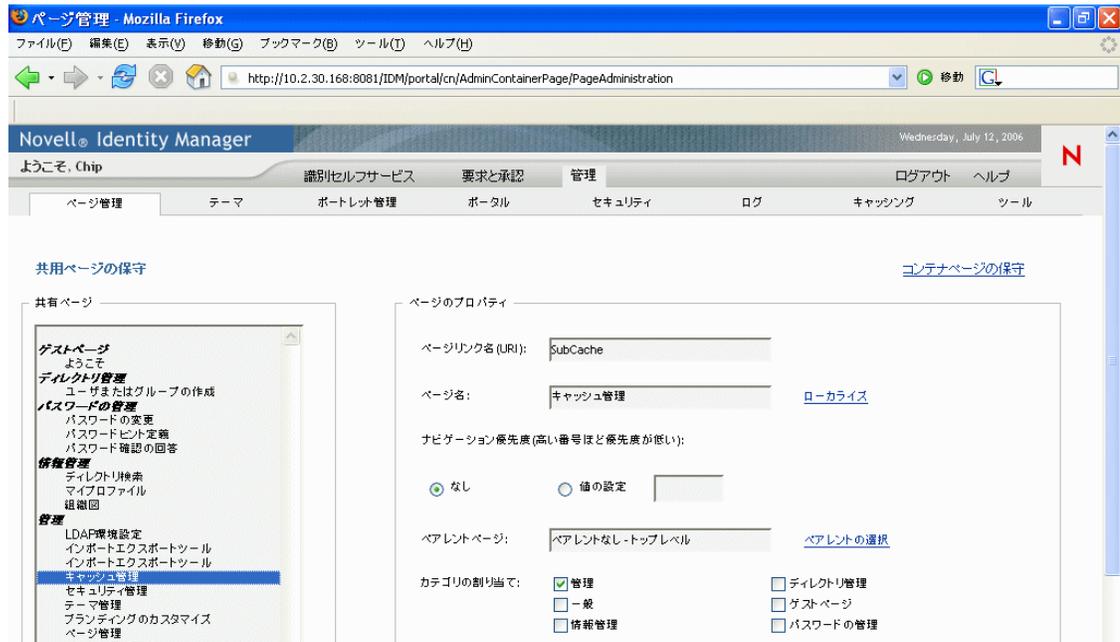
ポートレット	説明
HeaderPortlet	ユーザインタフェースのヘッダ情報およびトップレベルのタブコントロールが表示されます。
共有ページナビゲーション	縦のメニューが表示され、ユーザはこのメニューから共有ページを選択して表示できます。
ポータルページコントローラ	ユーザが共有ページナビゲーションポートレットで現在選択している共有ページが表示されます。
セッションタイムアウト警告	ユーザセッションのタイムアウトが近づくと警告メッセージが表示されます。

ユーザがログインすると、DefaultContainerPage の HeaderPortlet に [識別セルフサービス] タブが自動的に表示されます。

管理コンテナページ

デフォルトでは、ユーザアプリケーション管理者 (および許可された他のユーザ) が Identity Manager ユーザインタフェースの [管理] タブをクリックすると、管理コンテナ

ページと呼ばれるコンテナページが表示されます。このコンテナページは次のような外観をしています。



管理コンテナページの内部は、次のようなレイアウトになっています。



管理コンテナページのレイアウトは2つの領域に分けられており、それぞれに次のポートレットが表示されます。

ポートレット	説明
HeaderPortlet	ユーザインタフェースのヘッダ情報およびトップレベルのタブコントロールが表示されます。
管理リスト表示	2番目のレベルのタブが表示され、ユーザはこの中から管理アクションを選択して実行できます。
ポータルページコントローラ	管理リスト表示ポートレットでユーザが現在選択しているタブに対応する共有ページが表示されます。
セッションタイムアウト警告	ユーザセッションのタイムアウトが近づくと警告メッセージが表示されます。

7.1.2 共有ページについて

Identity Manager ユーザインタフェースには、コンテナページの主なコンテンツを構成する数多くの共有ページがあります。これらの共有ページは、必要に応じて変更できます。また、独自の共有ページを追加することもできます。

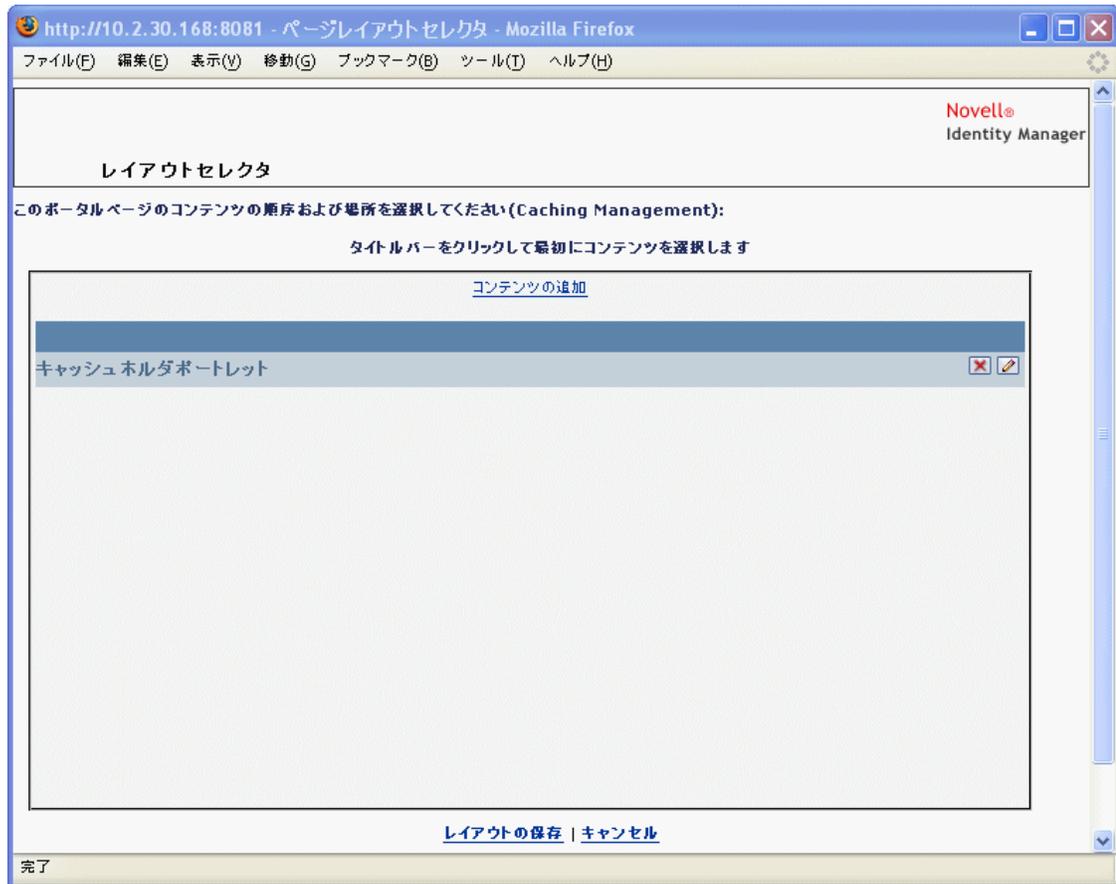
共有ページの操作の詳細については、[153 ページのセクション 7.3 「共有ページの作成とメンテナンス」](#)を参照してください。

標準の共有ページ

共有ページの一例を示します。ユーザが Identity Manager ユーザインタフェースにログインすると、DefaultContainerPage によってデフォルトの共有ページである組織図が表示されます。



組織図の内部は、次のようなレイアウトになっています。



組織図のレイアウトは1つの領域だけで構成されており、ポートレットが1つだけ表示されます (組織図ポートレット)。

7.1.3 ページの使用に関する例外

この章では、Identity Manager ユーザインタフェースのトップレベルのタブが、次に示す各ページを基にしてどのように構成されているかを説明しました。

- [識別セルフサービス] タブは DefaultContainerPage を使用します。
- [管理] タブは管理コンテナページを使用します。

ただし、[要求と承認] タブは別のアーキテクチャを基にしているため、[ページ管理]からは操作できません。

7.2 コンテナページの作成とメンテナンス

コンテナページを作成またはメンテナンスするには次の手順に従います。

- 1 新しいコンテナページを作成するか、既存のコンテナページを選択します (145 ページのセクション 7.2.1 「コンテナページの作成」を参照してください)。

- 2 コンテンツをポートレット形式でページに追加します (148 ページのセクション 7.2.2 「[コンテナページへのコンテンツの追加](#)」を参照してください)。
ページからコンテンツを削除することもできます (149 ページのセクション 7.2.3 「[コンテナページからコンテンツを削除する](#)」を参照してください)。
- 3 ポータルレイアウトを選択します (150 ページのセクション 7.2.4 「[コンテナページのレイアウトを変更する](#)」を参照してください)。
- 4 選択したレイアウトのコンテンツの順序と位置を決めます (151 ページのセクション 7.2.5 「[コンテナページにコンテンツを配置する](#)」を参照してください)。
- 5 コンテナページの URL をブラウザに入力して、新しいページを表示します (153 ページのセクション 7.2.6 「[コンテナページの表示](#)」を参照してください)。

コンテナページとレイアウト コンテナページは、完全にポータルレイアウトにバインドされているわけではありません。このため、コンテナページのレイアウトを切り替えてもページのコンテンツは失われません。コンテナページに新しいレイアウトを適用すると、ページに追加されたポートレットは自動的に新しいレイアウトで表示されます。新しいレイアウトではコンテンツの位置調整が必要なこともあります。

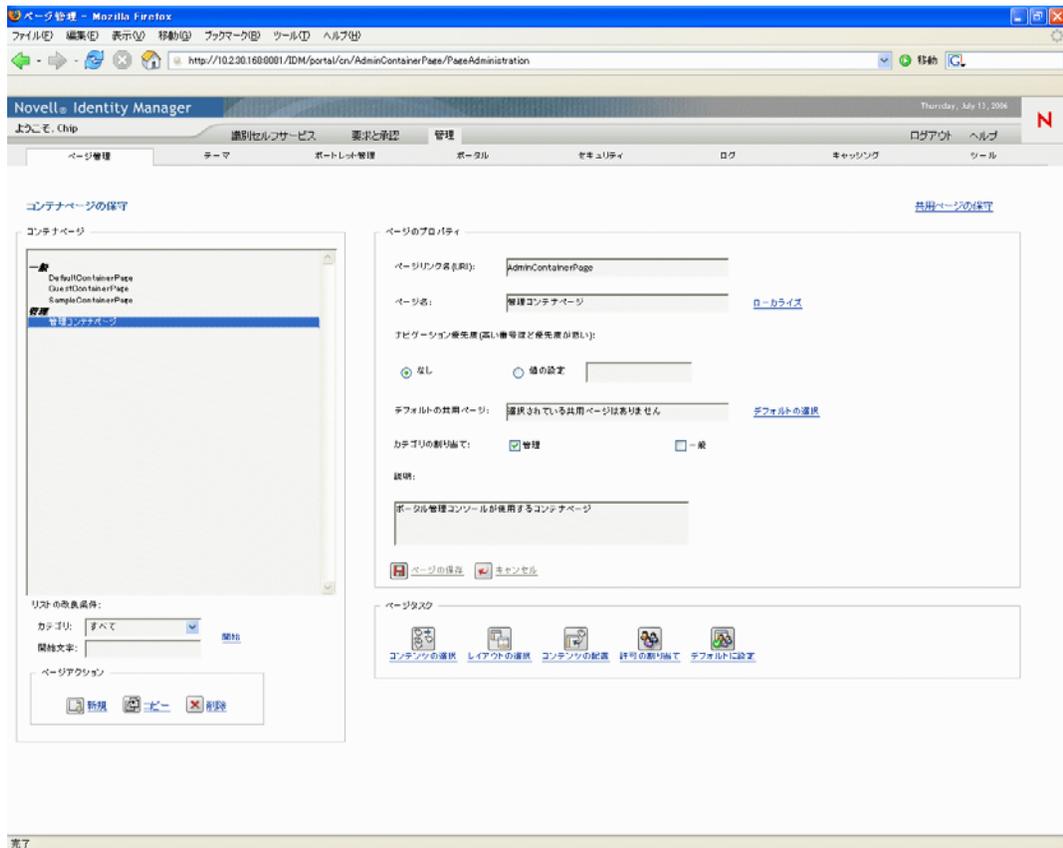
7.2.1 コンテナページの作成

コンテナページは初めから作成することも、既存のページをコピーして作成することもできます。この節では、両方の手順を説明します。

コンテナページを初めから作成するには：

- 1 [ページ管理] ページで [コンテナページの維持] を選択します。

[コンテナページの維持] パネルが表示されます。



- 2 [新規] ページアクションを選択します (パネルの左下にあります)。タイトルとカテゴリが未設定のコンテナページが作成されます。
- 3 コンテナページのページプロパティを指定します。

プロパティ	操作
ページリンク名 (URI)	ページの URI 名を指定します (ユーザインタフェースの URL 内に表示されます)。URI を指定した例を次に示します。 MyContainerPage 実際の URL は次のようになります。 <code>http://myappserver:8080/IDM/portal/cn/MyContainerPage</code>

プロパティ	操作
ページ名	ページの表示名を指定します。次に例を示します。 My Container Page この名前を他の言語にローカライズする場合は、[ローカライズ] をクリックします。
ナビゲーション優先度	次のいずれかを指定します。 <ul style="list-style-type: none"> ◆ なし — このコンテナページに優先度を割り当てる必要がない場合に指定します。 ◆ 値の設定 — このコンテナページに、他のコンテナページに対する優先度を割り当てます。優先度は、-1 ~ 9999 の間の整数を指定します。-1 は優先度が最高で、9999 は優先度が最低を意味します。 優先度順にページがリストされるときに特定の順序で表示する場合や、(ユーザが複数のグループに属しているため) デフォルトページが複数存在するときに特定のページを選択する場合、優先値を設定しておく と 便利 です。
デフォルトの共有ページ	172 ページのセクション 7.6 「コンテナページのデフォルト共有ページを選択する」 を参照してください。
カテゴリの割り当て	ページに適したカテゴリを次から選択します。適当なものがない場合は選択せず、複数ある場合は複数選択します。 <ul style="list-style-type: none"> ◆ 管理 ◆ 一般 カテゴリ順にページが一覧表示されるときに適切に整理されるようにする、またはページがカテゴリ順にフィルタされるときに適切なサブセットが選択されるようにする場合は、カテゴリを割り当てておく と 便利 です。
説明	ページを説明するテキストを入力します。

- 4 [ページの保存] をクリックします ([ページのプロパティ] セクションの下部にあります)。

既存のページをコピーしてコンテナページを作成するには :

- 1 [ページ管理] ページで [コンテナページの維持] を選択します。
[Maintain Container Pages] パネルが表示されます (前の手順と同じです)。
- 2 コンテナページのリストから、コピーするページを選択します。

ヒント : リストが長い場合は、リストを (カテゴリ順や開始テキスト順に) 並べ替えると、目的のページを見つけやすくなります。

- 3 [コピー] のページアクションを選択します (パネルの左下にあります)。
新しいコンテナページが作成され、[Copy of OriginalPageName (OriginalPageName のコピー)] という名前が付けられます。
- 4 コンテナページのページプロパティを指定します (前の手順と同じです)。

- 5 [ページの保存] をクリックします ([ページのプロパティ] セクションの下部に表示されます)。

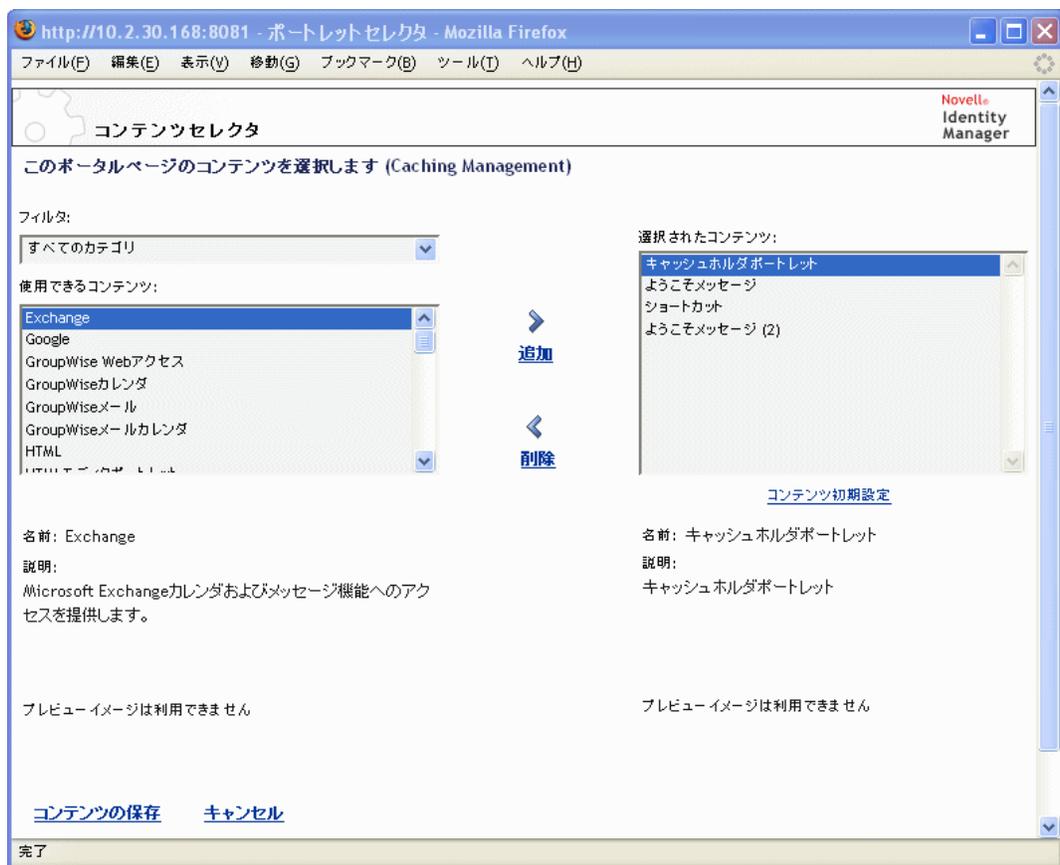
7.2.2 コンテナページへのコンテンツの追加

コンテナページを作成したら、次の手順として、ページに設定するポートレットを選択してコンテンツを追加します。Identity Manager ユーザアプリケーションに付属の作成済みポートレットを使用することも、登録した他のポートレットを使用することもできます。

コンテナページにコンテンツを追加するには：

- 1 [コンテナページの維持] パネルで新規または既存のページを開き、[コンテンツの選択] ページタスクをクリックします (パネルの下部にあります)。

新しいブラウザウィンドウに [コンテンツセレクタ] が表示されます。



- 2 使用可能なコンテンツの中から特定のカテゴリのコンテンツを表示する場合は、[フィルタ] ドロップダウンメニューからカテゴリを選択します。
- 3 [使用できるコンテンツ] のリストからポートレットを1つまたは複数選択します。

ヒント：リストから隣接していないポートレットを複数選択する場合は <Ctrl> キーを押しながら選択します。連続したポートレットを複数選択する場合は <Shift> キーを押しながら選択します。

- 4 [追加] をクリックして、選択したポートレットを [選択されたコンテンツ] リストに移動します。
- 5 [コンテンツ初期設定] をクリックすると、コンテナページのために選択したポートレットの初期設定を編集できます。指定した初期設定値は、ページに表示されるポートレットのインスタンスに反映されます。
- 6 [コンテンツの保存] をクリックします。

これでコンテナページのコンテンツを選択しました。続いて [150 ページのセクション 7.2.4 「コンテナページのレイアウトを変更する」](#) の説明に従って新しいレイアウトを選択するか、[151 ページのセクション 7.2.5 「コンテナページにコンテンツを配置する」](#) の説明に従って現在のレイアウトにコンテンツを配置できます。

7.2.3 コンテナページからコンテンツを削除する

コンテナページの作成中、あるページからポートレットを削除してコンテンツを削除することも可能です。このような場合、次の手順に従って [コンテンツセレクト] または [レイアウトセレクト] を使用します。

[コンテンツセレクト] を使ってコンテナページからコンテンツを削除するには：

- 1 [コンテナページの維持] パネルでページを開き、[コンテンツの選択] ページタスクをクリックします (パネルの下部にあります)。

新しいブラウザウィンドウに [コンテンツセレクト] が表示されます (前の手順と同じです)。

- 2 削除するポートレットを [選択されたコンテンツ] リストから選択し、[削除] をクリックします。

ポートレットがページから削除されます。

- 3 [コンテンツの保存] をクリックします。

[レイアウトセレクト] を使ってコンテナページからコンテンツを削除するには：

- 1 [コンテンツページの維持] パネルでページを開き、[コンテンツの配置] ページタスクをクリックします (パネルの下部にあります)。

新しいブラウザウィンドウに [レイアウトセレクタ] が表示され、そのページのポートレットが表示されます。



- 2 削除するポートレットの X ボタンをクリックします。
- 3 確認のメッセージが表示されたら、[OK] をクリックします。
ポートレットがページから削除されます。
- 4 [レイアウトの保存] をクリックします。

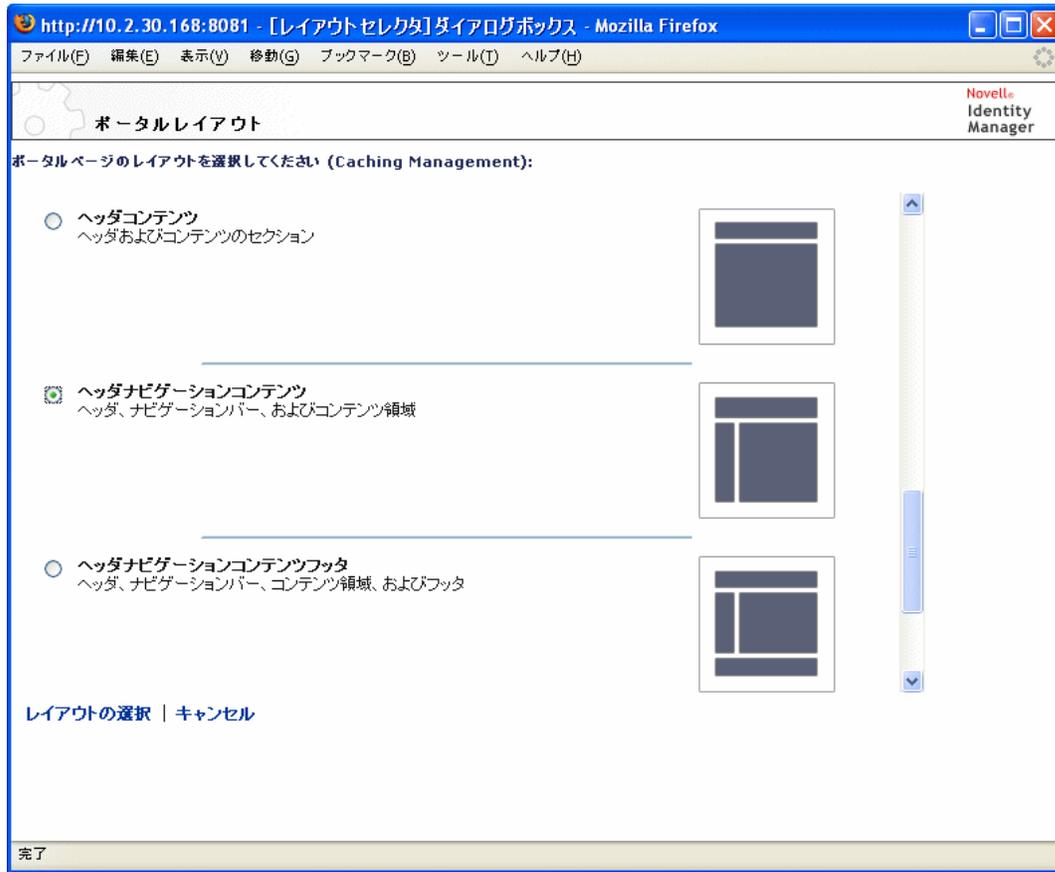
7.2.4 コンテナページのレイアウトを変更する

コンテナページのレイアウトを変更すると、新しいレイアウトに合わせて既存のコンテンツが移動します。場合によっては、最終的なそれぞれの位置を調整する必要があります。

コンテナページのレイアウトを変更するには：

- 1 [コンテンツページの維持] パネルでページを開き、[レイアウトの選択] ページタスクをクリックします (パネルの下部にあります)。

新しいブラウザウィンドウに [ポータルレイアウト] のリストが表示されます。



- 2 選択項目をスクロールし、使用するレイアウトを選択します。
- 3 [レイアウトの選択] をクリックします。

7.2.5 コンテナページにコンテンツを配置する

コンテナページのコンテンツやレイアウトを指定した後、選択したレイアウトにコンテンツを配置できます。また、特定の場所に他のポートレットを追加したり、ポートレットを削除したりできます。

コンテナページにコンテンツを配置するには：

- 1 [コンテンツページの維持] パネルでページを開き、[コンテンツの配置] ページタスクをクリックします (パネルの下部にあります)。

新しいブラウザウィンドウに [レイアウトセレクタ] が表示され、そのページのポートレットが表示されます。



- 2 ページにポートレットを追加する場合は、次の手順に従います。
 - 2a 目的のレイアウトフレーム内で [コンテンツの追加] をクリックします。
新しいブラウザウィンドウに [ポートレットセレクタ] が表示されます。
 - 2b 使用可能なコンテンツの中から特定のカテゴリのコンテンツを表示する場合は、[フィルタ] ドロップダウンメニューからカテゴリを選択します。
 - 2c [使用できるコンテンツ] リストから追加するポートレットを選択します。
 - 2d [コンテンツの選択] をクリックします。
[ポートレットセレクタ] が閉じ、選択したポートレットが [レイアウトセレクタ] の目的のレイアウトフレームに表示されます。
- 3 レイアウト内の別の場所にポートレットを移動する場合は、次のブラウザ別の手順に従います。

ブラウザ	操作
Internet Explorer	<ol style="list-style-type: none"> 1. ポートレットのタイトルバーにカーソルを移動し、カーソルが手の形になるようにします。 2. マウスの左ボタンを押し、レイアウト内の目的の場所にポートレットをドラッグします。

ブラウザ	操作
Mozilla	<ol style="list-style-type: none"> 1. 移動するポートレットをクリックします。 2. 移動先のレイアウトフレームの内側をクリックします。 ポートレットが指定した位置に移動します。

- 4 レイアウトからポートレットを削除する場合は、次の手順に従います。
 - 4a 削除するポートレットの X ボタンをクリックします。
 - 4b 確認のメッセージが表示されたら、[OK] をクリックします。
ポートレットがレイアウトから削除されます。
- 5 ポートレットの初期設定を編集する場合は、次の手順に従います。
 - 5a 編集するポートレットの鉛筆型のボタンをクリックします。
ポートレットのコンテンツ初期設定がブラウザに表示されます。
 - 5b 必要に応じて初期設定値を変更します。
指定した初期設定値は、ページに表示されるポートレットのインスタンスに反映されます。
 - 5c [設定の保存] をクリックします。
- 6 [レイアウトの保存] をクリックして変更を保存し、[レイアウトセクタ] を閉じます。

7.2.6 コンテナページの表示

コンテナページを表示するには、ブラウザでコンテナページの URL に移動します。

コンテナページを表示するには：

- ◆ Web ブラウザで、次の URL に移動します。

```
http://server:port/IDM-war-context/portal/cn/container-page-name
```

たとえば、MyContainerPage というコンテナページを表示するには、次のページに移動します。

```
http://myappserver:8080/IDM/portal/cn/MyContainerPage
```

7.3 共有ページの作成とメンテナンス

共有ページの作成とメンテナンスは次の手順で行います。

- 1 新しい共有ページを作成するか、既存の共有ページを選択します (154 ページのセクション 7.3.1 「共有ページの作成」を参照してください)。
- 2 ページにコンテンツをポートレット形式で追加します (158 ページのセクション 7.3.2 「共有ページにコンテンツを追加する」を参照してください)。

ページからコンテンツを削除することもできます (159 ページのセクション 7.3.3 「共有ページからコンテンツを削除する」を参照してください)。

- 3 ポータルレイアウトを選択します (160 ページのセクション 7.3.4 「共有ページのレイアウトを変更する」を参照してください)。
- 4 選択したレイアウトのコンテンツの順序と位置を決めます (161 ページのセクション 7.3.5 「共有ページにコンテンツを配置する」を参照してください)。
- 5 共有ページの URL をブラウザに入力して、新しいページを表示します (163 ページのセクション 7.3.6 「共有ページの表示」を参照してください)。

共有ページとレイアウト 共有ページはポータルレイアウトに完全にバインドされているわけではありません。このため、共有ページのレイアウトを切り替えてもページのコンテンツは失われません。新しいレイアウトが適用されると、ページに追加されたポートレットは自動的に新しいレイアウトで表示されます。新しいレイアウトではコンテンツの位置調整が必要なこともあります。

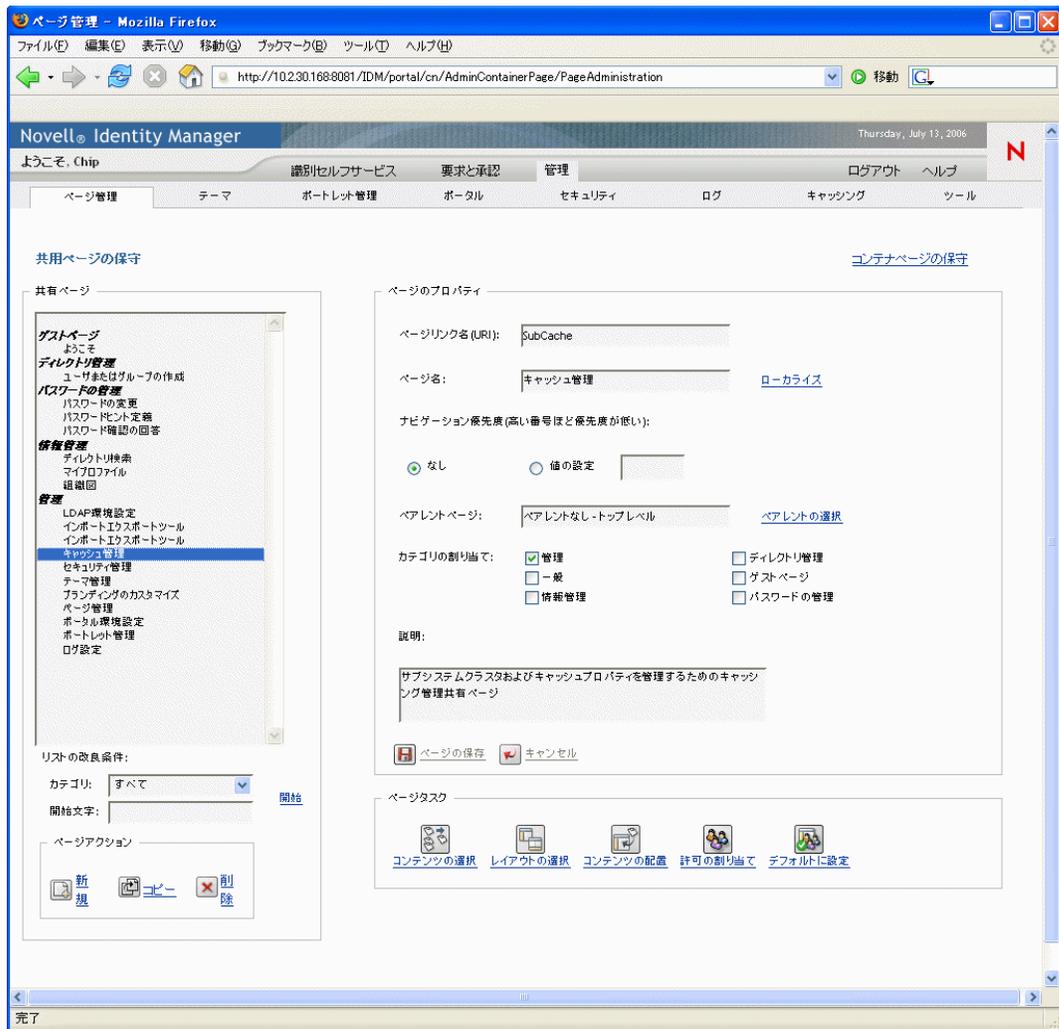
7.3.1 共有ページの作成

共有ページは初めから作成することも、既存のページをコピーして作成することもできます。この節では、両方の手順を説明します。

共有ページを初めから作成するには：

- 1 [ページ管理] ページで [共有ページの維持] を選択します。

[共有ページの維持] パネルが表示されます。



- 2 [新規] ページアクションを選択します (パネルの左下にあります)。
タイトルとカテゴリが未設定の共有ページが作成されます。
- 3 共有ページのページプロパティを指定します。

プロパティ	操作
ページリンク名 (URI)	<p>ページの URI 名を指定します (ユーザインタフェースの URL 内に表示されます)。URI を指定した例を次に示します。</p> <p>MySharedPage</p> <p>実際の URL は次のようになります。</p> <p>http://myappserver:8080/IDM/portal/cn/MyContainerPage/MySharedPage</p>
ページ名	<p>ページの表示名を指定します。次に例を示します。</p> <p>My Shared Page</p> <p>この名前を他の言語にローカライズする場合は、[ローカライズ] をクリックします。</p>
ナビゲーション優先度	<p>次のいずれかを指定します。</p> <ul style="list-style-type: none"> ◆ なし — この共有ページに優先度を割り当てる必要がない場合に指定します。 ◆ 値の設定 — この共有ページに、他の共有ページに対する優先度を割り当てます。優先度は、-1 ~ 9999 の間の整数を指定します。-1 は優先度が最高で、9999 は優先度が最低を意味します。 <p>優先度順にページがリストされるときに特定の順序で表示する場合や、(ユーザが複数のグループに属しているため) デフォルトページが複数存在するときに特定のページを選択する場合、優先値を設定しておく便利です。</p>
親ページ	<p>この共有ページを他の共有ページの子として設定する場合は、[親の選択] をクリックします。表示の問題を避けるために、親ページと子ページが両方とも同じカテゴリに属していることを確認してください。</p> <p>エンドユーザがランタイム時に共有ページナビゲーションポートレットを使用すると、この関係が表示されます。共有ページのリストを表示すると、親ページの下に子ページがインデント表示されます。</p> <p>子ページは親ページのコンテンツ、初期設定、および設定を継承しません。逆に言えば、親ページがそれ自体のコンテンツと同時に子ページのコンテンツを自動的に表示することはありません。</p>

プロパティ	操作
カテゴリの割り当て	<p>ページに適したカテゴリを次から選択します。適当なものがない場合は選択せず、複数ある場合は複数選択します。</p> <ul style="list-style-type: none"> ◆ 管理 ◆ ディレクトリ管理 ◆ 一般 ◆ Guest ページ ◆ 情報管理 ◆ パスワードの管理 <p>カテゴリ順にページが一覧表示されるときに適切に整理されるようにする、またはページがカテゴリ順にフィルタされるときに適切なサブセットが選択されるようにする場合は、カテゴリを割り当てておくが便利です。</p> <hr/> <p>注：「Guest ページ」は特別なカテゴリで、ユーザのログイン前に表示される（ログイン後には非表示の）共有ページの識別に使用されます。詳細については、239 ページの第 15 章「ポートレットについて」の共有ページナビゲーションポートレットの節を参照してください。</p> <hr/>
説明	ページを説明するテキストを入力します。

- 4 [ページの保存] をクリックします（[ページのプロパティ] セクションの下部にあります）。

既存のページをコピーして共有ページを作成するには：

- 1 [ページ管理] ページで [共有ページの維持] を選択します。
[共有ページの維持] パネルが表示されます（前の手順と同じです）。
- 2 共有ページのリストから、コピーするページを選択します。

ヒント：リストが長い場合は、リストを（カテゴリ順や開始テキスト順に）並べ替えると、目的のページを見つけやすくなります。

- 3 [コピー] のページアクションを選択します（パネルの左下にあります）。
新しい共有ページが作成され、[Copy of OriginalPageName (<OriginalPageName> のコピー)] という名前が付けられます。
- 4 共有ページのページプロパティを指定します（前の手順と同じです）。
- 5 [ページの保存] をクリックします（[ページのプロパティ] セクションの下部にあります）。

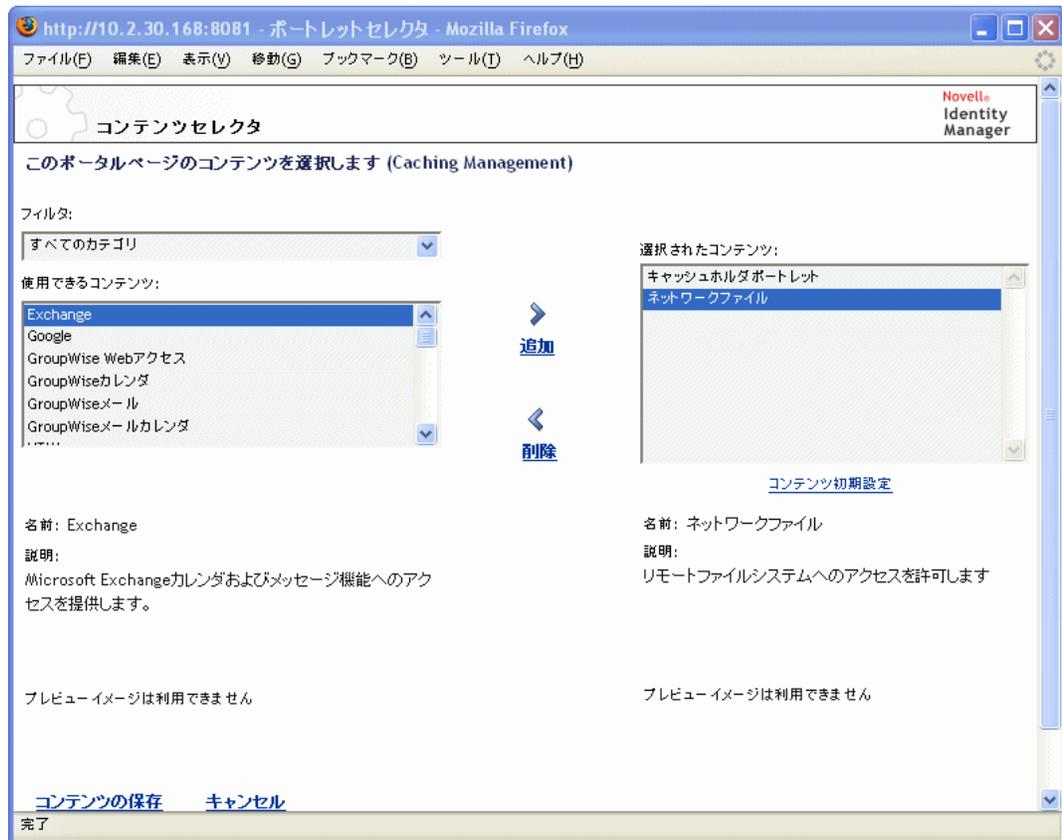
7.3.2 共有ページにコンテンツを追加する

共有ページを作成したら、次の手順として、ページに設定するポートレットを選択してコンテンツを追加します。Identity Manager ユーザアプリケーションに付属の作成済みポートレットを使用することも、登録した他のポートレットを使用することもできます。

共有ページにコンテンツを追加するには：

- 1 [共有ページの維持] パネルで新規または既存のページを開き、[コンテンツの選択] ページタスクをクリックします (パネルの下部にあります)。

新しいブラウザウィンドウに [コンテンツセレクタ] が表示されます。



- 2 使用可能なコンテンツの中から特定のカテゴリのコンテンツを表示する場合は、[フィルタ] ドロップダウンメニューからカテゴリを選択します。
- 3 [使用できるコンテンツ] リストからポートレットを1つまたは複数選択します。

ヒント：リストから隣接していないポートレットを複数選択する場合は <Ctrl> キーを押しながら選択します。連続したポートレットを複数選択する場合は <Shift> キーを押しながら選択します。

- 4 [追加] をクリックして、選択したポートレットを [選択されたコンテンツ] リストに移動します。

- 5 [コンテンツ初期設定] をクリックすると、共有ページのために選択したポートレットの初期設定を編集できます。指定した初期設定値は、ページに表示されるポートレットのインスタンスに反映されます。
- 6 [コンテンツの保存] をクリックします。

これで共有ページのコンテンツを選択しました。続いて **160 ページのセクション 7.3.4 「共有ページのレイアウトを変更する」** の説明に従って新しいレイアウトを選択するか、**161 ページのセクション 7.3.5 「共有ページにコンテンツを配置する」** の説明に従って現在のレイアウトのコンテンツを配置できます。

7.3.3 共有ページからコンテンツを削除する

共有ページの作成中、あるページからポートレットを削除してコンテンツを削除する必要が出てくる場合もあります。このような場合、次の手順に従って [コンテンツセクタ] または [レイアウトセクタ] を使用します。

[コンテンツセクタ] を使って共有ページからコンテンツを削除するには：

- 1 [共有ページの維持] パネルでページを開き、[コンテンツの選択] ページタスクをクリックします (パネルの下部にあります)。
新しいブラウザウィンドウに [コンテンツセクタ] が表示されます (前の手順と同じです)。
- 2 削除するポートレットを [選択されたコンテンツ] リストから選択し、[削除] をクリックします。
ポートレットがページから削除されます。
- 3 [コンテンツの保存] をクリックします。

[レイアウトセクタ] を使って共有ページからコンテンツを削除するには：

- 1 [共有ページの維持] パネルでページを開き、[コンテンツの配置] ページタスクをクリックします (パネルの下部にあります)。

新しいブラウザウィンドウに [レイアウトセクタ] が表示され、そのページのポートレットが表示されます。



- 2 削除するポートレットの X ボタンをクリックします。
- 3 確認のメッセージが表示されたら、[OK] をクリックします。
ポートレットがページから削除されます。
- 4 [レイアウトの保存] をクリックします。

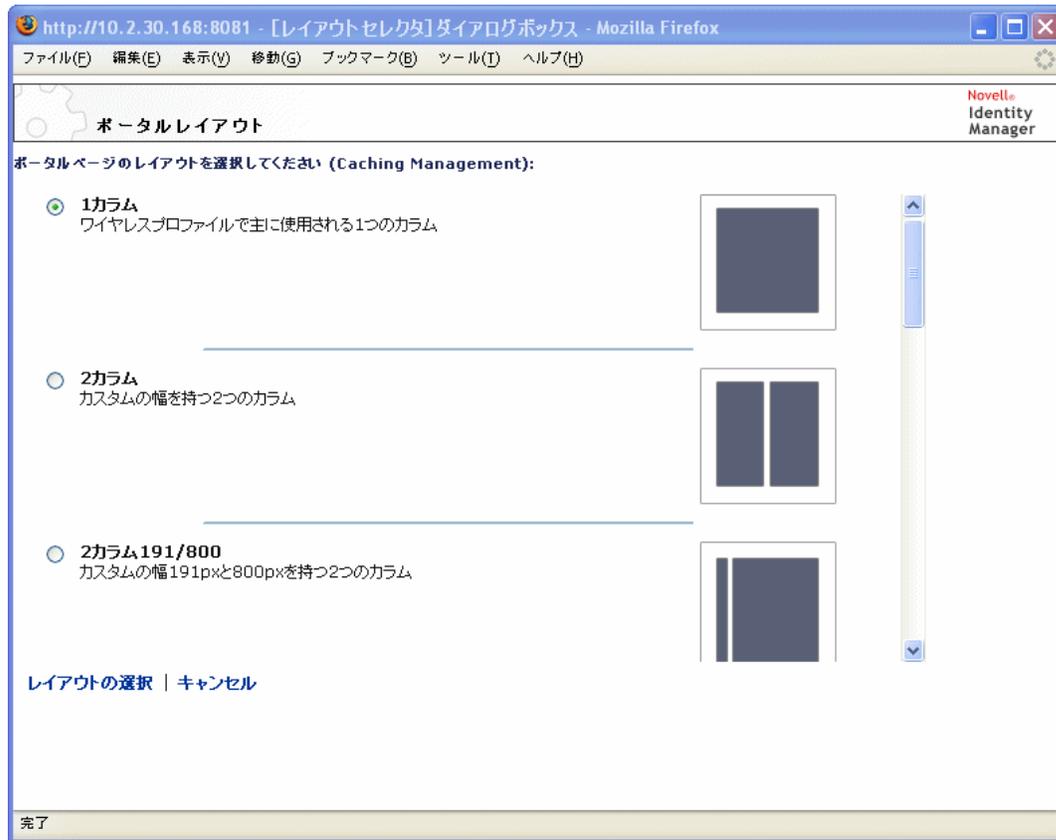
7.3.4 共有ページのレイアウトを変更する

共有ページのレイアウトを変更すると、新しいレイアウトに合わせて既存のコンテンツが移動します。場合によっては、最終的なそれぞれの位置を調整する必要があります。

共有ページのレイアウトを変更するには：

- 1 [共有ページの維持] パネルでページを開き、[レイアウトの選択] ページタスクをクリックします (パネルの下部にあります)。

新しいブラウザウィンドウに [ポータルレイアウト] リストが表示されます。



- 2 選択項目をスクロールし、使用するレイアウトを選択します。
- 3 [レイアウトの選択] をクリックします。

7.3.5 共有ページにコンテンツを配置する

共有ページのコンテンツやレイアウトを指定した後、選択したレイアウトにコンテンツを配置できます。また、特定の場所に他のポートレットを追加したり、ポートレットを削除したりできます。

共有ページにコンテンツを配置するには：

- 1 [共有ページの維持] パネルでページを開き、[コンテンツの配置] ページタスクをクリックします (パネルの下部にあります)。

新しいブラウザウィンドウに [レイアウトセクタ] が表示され、そのページのポートレットが表示されます。



- 2 ページにポートレットを追加する場合は、次の手順に従います。
 - 2a 目的のレイアウトフレーム内で [コンテンツの追加] をクリックします。
新しいブラウザウィンドウに [ポートレットセクタ] が表示されます。
 - 2b 使用可能なコンテンツの中から特定のカテゴリのコンテンツを表示する場合は、[フィルタ] ドロップダウンメニューからカテゴリを選択します。
 - 2c [使用できるコンテンツ] リストから追加するポートレットを選択します。
 - 2d [コンテンツの選択] をクリックします。
[ポートレットセクタ] が閉じ、選択したポートレットが [レイアウトセクタ] の目的のレイアウトフレームに表示されます。
- 3 レイアウト内の別の場所にポートレットを移動する場合は、次のブラウザ別の手順に従います。

ブラウザ	操作
Internet Explorer	<ol style="list-style-type: none"> 1. ポートレットのタイトルバーにカーソルを移動し、カーソルが手の形になるようにします。 2. マウスの左ボタンを押し、レイアウト内の目的の場所にポートレットをドラッグします。

ブラウザ	操作
Mozilla	<ol style="list-style-type: none"> 1. 移動するポートレットをクリックします。 2. 移動先のレイアウトフレームの内側をクリックします。 ポートレットが指定した位置に移動します。

- 4 レイアウトからポートレットを削除する場合は、次の手順に従います。
 - 4a 削除するポートレットの X ボタンをクリックします。
 - 4b 確認のメッセージが表示されたら、[OK] をクリックします。
ポートレットがレイアウトから削除されます。
- 5 ポートレットの初期設定を編集する場合は、次の手順に従います。
 - 5a 編集するポートレットの鉛筆型のボタンをクリックします。
ポートレットのコンテンツ初期設定がブラウザに表示されます。
 - 5b 必要に応じて初期設定値を変更します。
指定した初期設定値は、ページに表示されるポートレットのインスタンスに反映されます。
 - 5c [設定の保存] をクリックします。
- 6 [レイアウトの保存] をクリックして変更を保存し、[レイアウトセクタ] を閉じます。

7.3.6 共有ページの表示

共有ページを表示するには、ブラウザで共有ページの URL に移動します。

共有ページを表示するには：

- ◆ Web ブラウザで、次の URL に移動します。

```
http://server:port/IDM-war-context/portal/pg/shared-page-name
```

たとえば、MyContainerPage という共有ページを表示するには、次のページに移動します。

```
http://myappserver:8080/IDM/portal/pg/MySharedPage
```

7.4 ページの許可を割り当てる

他のユーザ、グループ、およびコンテナに対して、特定のコンテナページや共有ページを操作できる許可を割り当てることができます。次に示す 2 種類のセキュリティレベルの許可を割り当てることができます。

許可	説明	許可の対象
表示	ユーザ、グループ、またはコンテナにページへのアクセスを許可します。また、使用可能なページリストにそのページが表示されます。	コンテナページと共有ページ
所有権	ユーザ、グループ、またはコンテナにページのコンテンツやレイアウトの変更を許可します。また、そのユーザ、グループ、またはコンテナが、他のユーザ、グループ、およびコンテナに表示許可および所有権許可を割り当てることを許可します。	共有ページ

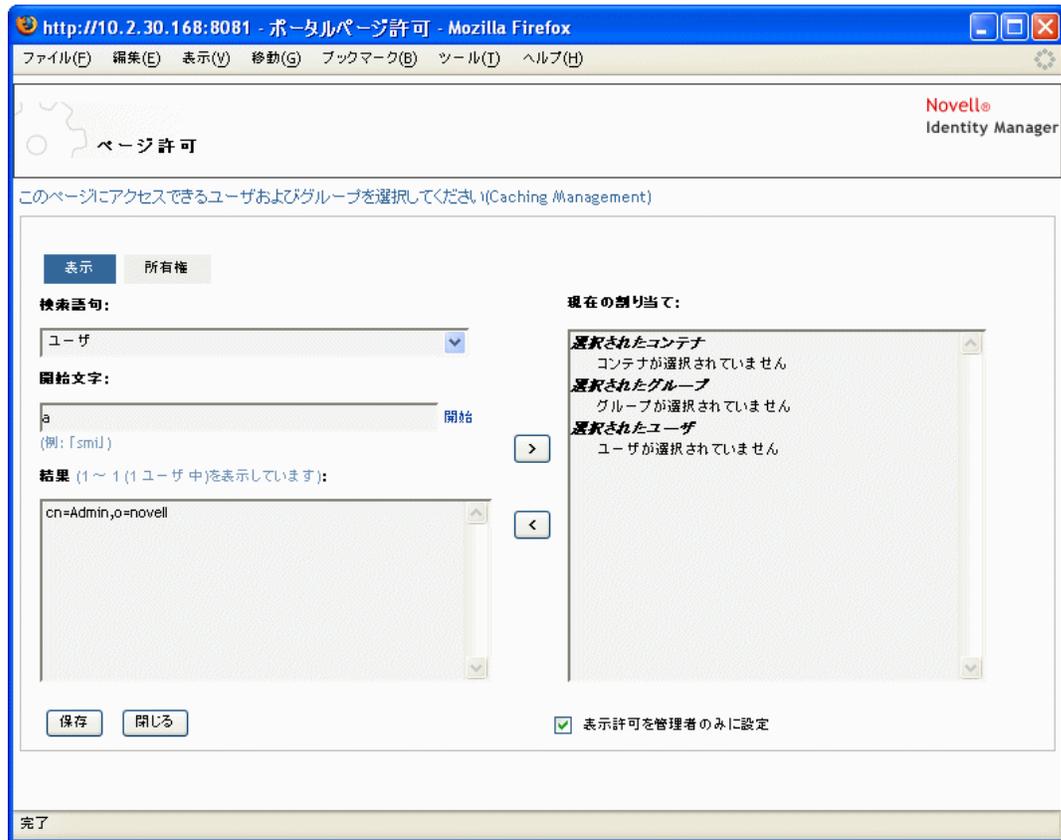
7.4.1 ページに表示許可を割り当てる

ユーザにコンテナページや共有ページを表示許可を割り当てると、ユーザはそのページにアクセスできるようになります。また、そのユーザの使用可能なページリストにそのページが表示されるようになります。

コンテナページや共有ページを表示許可を割り当てるには：

- 1 [コンテナページの維持] パネルまたは [共有ページの維持] パネルでページを開き、[許可の割り当て] ページタスクをクリックします (パネルの下部)。

新しいブラウザウィンドウに [ページ許可] ダイアログボックスが表示されます。



2 [表示] タブに移動します。

3 次の検索設定値を指定します。

設定	操作
検索対象	次のいずれかをドロップダウンメニューから選択します。 <ul style="list-style-type: none">◆ ユーザ◆ グループ◆ コンテナ

設定	操作
開始文字	<p>可能な操作</p> <ul style="list-style-type: none"> ◆ 指定したタイプ (ユーザ、グループ、またはコンテナ) で使用できるオブジェクトをすべて検索する場合は、この設定を空白にします。 ◆ これらのオブジェクトのサブセットを検索する場合は、目的の CN 値の開始文字を入力します。大文字小文字は区別されません。また、ワイルドカードはサポートされていません。 <p>たとえば、S で開始するグループを検索することにより、検索結果は次のように絞り込まれます。</p> <p>cn=Sales, ou=groups, o=MyOrg</p> <p>cn=Service, ou=groups, o=MyOrg</p> <p>cn=Shipping, ou=groups, o=MyOrg</p> <p>Se で開始するグループを検索すると、次のような結果が返ります。</p> <p>cn=Service, ou=groups, o=MyOrg</p>

- 4 [開始] をクリックします。
検索結果は、[結果] リストに表示されます。
 - 5 ページを割り当てるユーザ、グループ、またはコンテナを選択して、[追加 (>)] ボタンをクリックします。
- ヒント : 複数項目を選択する場合には、<Ctrl> キーを押しながら選択します。
- 6 次のようにページロックの有効または無効を設定します。

可能な操作	操作手順
ページをロックし、ユーザアプリケーション管理者だけが表示できるようにする	[表示許可を管理者のみに設定] をオンにします。
割り当てられたすべてのユーザ、グループ、およびコンテナがページを表示できるようにする	[表示許可を管理者のみに設定] をオフにします。

注 : この設定をオフにした状態でユーザ、グループ、またはコンテナがページに対して明示的に割り当てられていない場合、全員にこのページへの表示許可が割り当てられることになります。

7 [保存]、[閉じる] の順にクリックします。

7.4.2 共有ページに所有者を割り当てる

共有ページの所有者ユーザは、所有するページのコンテンツを変更でき、そのページのポートレットの初期設定を変更できます。

共有ページに所有権許可を割り当てるには：

- 1 [共有ページの維持] パネルでページを開き、[許可の割り当て] ページタスクをクリックします (パネルの下部にあります)。

新しいブラウザウィンドウに [ページ許可] ダイアログボックスが表示されます (前の手順と同じです)。

- 2 [所有権] タブに移動します。
- 3 次の検索設定値を指定します。

設定	操作
検索対象	次のいずれかをドロップダウンメニューから選択します。 <ul style="list-style-type: none">◆ ユーザ◆ グループ◆ コンテナ
開始文字	可能な操作 <ul style="list-style-type: none">◆ 指定したタイプ (ユーザ、グループ、またはコンテナ) で使用できるオブジェクトをすべて検索する場合は、この設定を空白にします。◆ これらのオブジェクトのサブセットを検索する場合は、目的の CN 値の開始文字を入力します。大文字小文字は区別されません。また、ワイルドカードはサポートされていません。 たとえば、S で開始するグループを検索することにより、検索結果は次のように絞り込まれます。 <pre>cn=Sales,ou=groups,o=MyOrg</pre> <pre>cn=Service,ou=groups,o=MyOrg</pre> <pre>cn=Shipping,ou=groups,o=MyOrg</pre> <p>Se で開始するグループを検索すると、次のような結果が返ります。</p> <pre>cn=Service,ou=groups,o=MyOrg</pre>

4 [開始] をクリックします。

検索結果は、[結果] リストに表示されます。

5 ページを割り当てるユーザ、グループ、またはコンテナを選択して、[追加 (>)] ボタンをクリックします。

ヒント：複数項目を選択する場合には、<Ctrl> キーを押しながら選択します。

6 次のようにページロックの有効または無効を設定します。

可能な操作	操作手順
ページをロックし、ユーザアプリケーション管理者だけが操作できるようにする	[所有権許可を管理者のみに設定] をオンにします。
割り当てられたすべてのユーザ、グループ、およびコンテナがページを操作できるようにする	[所有権許可を管理者のみに設定] をオフにします。

注：この設定をオフにした状態で、ページに対して明示的に割り当てられたユーザ、グループ、またはコンテナがない場合、**全員**がこのページへの所有権許可が割り当てられることになります。

7 [保存]、[閉じる] の順にクリックします。

7.4.3 [ユーザまたはグループの作成] ページへのユーザアクセスを有効にする

デフォルトでは、ユーザアプリケーション管理者だけが [ユーザまたはグループの作成] ページを表示および使用できます。このページは、Identity Manager ユーザインタフェースの [識別セルフサービス] タブの共有ページです。ただし、ユーザアプリケーション管理者は状況に応じて、このページにアクセスするための許可を 1 人または複数のエンドユーザに割り当てることができます。たとえば、管理職にある、あるユーザが、ユーザ、グループ、またはタスクグループを自分自身で作成する機能を必要とすることがあります。

[ユーザまたはグループの作成] ページへのアクセスをユーザに許可するには：

- 1 [共有ページの維持] パネルで、[ユーザまたはグループの作成] という名前のページを開きます。
- 2 [許可の割り当て] ページタスクを使用して、適切なユーザ、グループ、またはコンテナに、[ユーザまたはグループの作成] 共有ページの表示許可を与えます。
- 3 [ページ管理] から [ポートレット管理] に切り替え、CreatePortlet というポートレット登録を開きます (これは [ユーザまたはグループの作成] ページで使用されます)。
- 4 [セキュリティ] パネルを使用して、適切なユーザ、グループ、またはコンテナに、CreatePortlet ポートレット登録に対するリスト許可と実行許可を与えます。
ポートレットの許可の割り当ての詳細については、[181 ページの第 9 章「ポートレットの管理」](#)を参照してください。
- 5 iManager に移動し、管理者アカウントを使用してアイデンティティボルトのツリーにログインします。

- 6 [ユーザまたはグループの作成] を使用するユーザが、オブジェクト (ユーザ、グループ、およびタスクグループ) が作成されるコンテナの「Entry Rights」プロパティを作成する権利を持っていることを確認します。

たとえば、選択したコンテナのトラスティを変更し、適切なユーザ、グループ、またはコンテナをトラスティとして追加できます。それから各トラスティに対し次の権利を割り当てます。

プロパティ名	割り当てられる権利	継承
「All Attributes Rights」	<ul style="list-style-type: none"> ◆ 比較 ◆ 読み込み ◆ 書き込み 	継承する (このチェックボックスをオンにします)
「Entry Rights」	<ul style="list-style-type: none"> ◆ 参照 ◆ 作成 	継承する (このチェックボックスをオンにします)

必要な権利をアイデンティティボールドで割り当てなかった場合 (または何らかの理由でこうした権利が生成されなかった場合)、[ユーザまたはグループの作成] によってエンドユーザに対し次のようなエラーメッセージが表示されます。

```
User 'cn=mmackenzie,ou=users,ou=idmsample,o=novell' does not have
permission to create
'cn=MyNewGroup,ou=groups,ou=idmsample,o=novell' or modify related
objects.
```

[ユーザまたはグループの作成] ページの使用方法 (このページにアクセスできる場合) については、『Identity Manager ユーザアプリケーション: ユーザーズガイド』を参照してください。

7.4.4 個々の [管理] ページへのユーザアクセスを有効にする

デフォルトでは、ユーザアプリケーション管理者だけが Identity Manager ユーザインタフェースの [管理] タブ、およびそのタブに含まれるページ ([ページ管理]、[テーマ]、[ポートレット管理]、[ポータル]、[セキュリティ]、[ログ]、[キャッシング]、[ツール]) にアクセスできます。ただし必要であれば、ユーザアプリケーション管理者は 1 人または複数のエンドユーザに、[管理] タブの特定のページを表示および使用する許可を割り当てることができます。たとえば、ユーザアプリケーション管理者ではないユーザが、定期的にテーマを変更する必要がある場合があります。

[管理] ページへのユーザアクセスを有効にするには:

- 1 [コンテナページの維持] パネルで [管理コンテナページ] を開きます。
これは、Identity Manager ユーザインタフェースの [管理] タブに移動したときに使用されるコンテナページです。
- 2 [許可の割り当て] ページタスクを使用して、適切なユーザ、グループ、またはコンテナに、[管理コンテナページ] の表示許可を与えます。
- 3 [共有ページの維持] パネルで、適切な [管理] ページ ([管理] カテゴリ内にある共有ページの 1 つ) を開きます。

- 4 [許可の割り当て] ページタスクを使用して、適切なユーザ、グループ、またはコンテナに、その共有ページの表示許可および所有権許可を与えます。
- 5 指定したユーザ、グループ、またはコンテナに、指定したページで使用される各ポートレットの実行許可があることを確認します(これらのポートレットに制限が設定されている場合)。

ポートレットの許可の割り当ての詳細については、[181 ページの第9章「ポートレットの管理」](#)を参照してください。

7.5 グループのデフォルトページを設定する

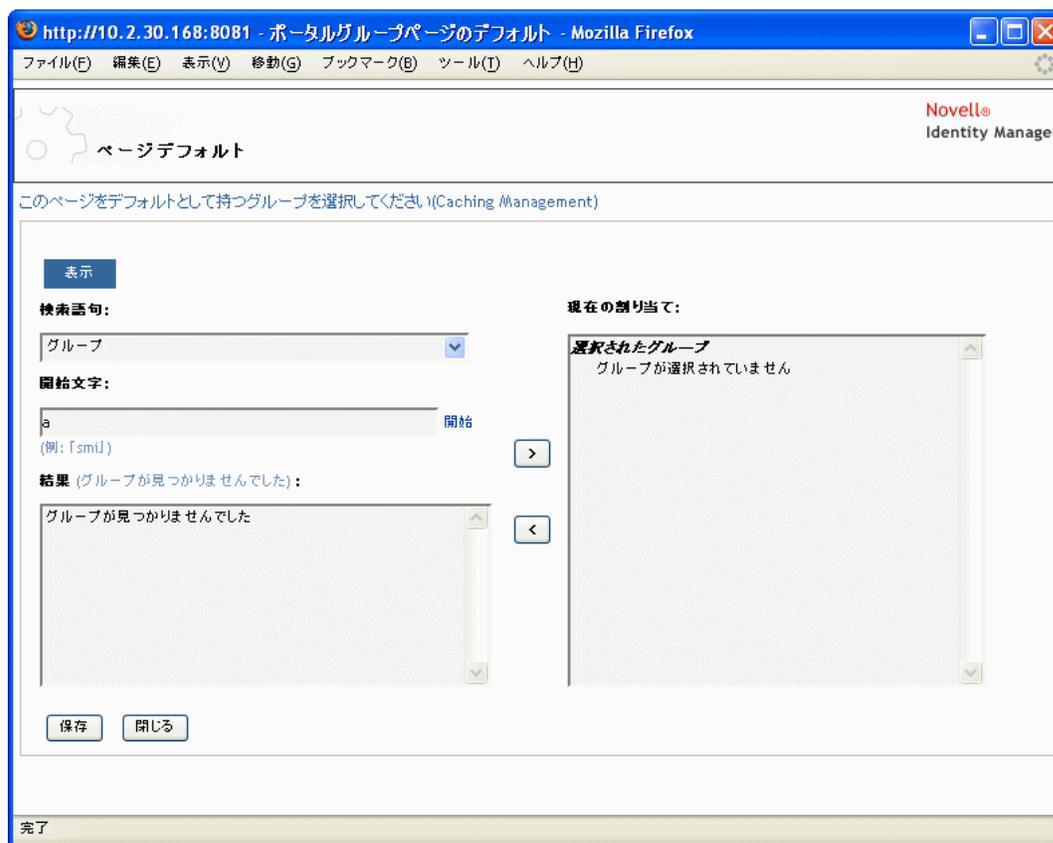
認可したユーザグループに対し、デフォルトのコンテナページおよびデフォルトの共有ページを割り当てることができます。ユーザがログインしたときに表示されるコンテナページ、およびコンテナページ上に表示される共有ページは、これらの設定によって決まります。

ユーザが複数のグループに属しており、デフォルトのページが複数割り当てられている場合、表示されるコンテナページと共有ページは [ナビゲーション優先度] を使用して決定されます。

グループにデフォルトのコンテナページまたはデフォルトの共有ページを割り当てるには :

- 1 [コンテナページの維持] パネルまたは [共有ページの維持] パネルでページを開き、[デフォルトに設定] ページタスクをクリックします(パネルの下部にあります)。

ブラウザの新しいウィンドウに [ページデフォルト] のダイアログボックスが表示されます。



2 次の検索設定値を指定します。

設定	操作
検索対象	[グループ] が自動的に選択されます。

設定	操作
開始文字	<p>可能な操作</p> <ul style="list-style-type: none"> ◆ 使用できるすべてのグループを検索する場合には、この設定を空白にします。 ◆ これらのグループのサブセットを検索する場合には、目的の CN 値の開始文字を入力します。大文字小文字は区別されません。また、ワイルドカードはサポートされていません。 <p>たとえば、S で開始するグループを検索することにより、検索結果は次のように絞り込まれます。</p> <pre>cn=Sales,ou=groups,o=MyOrg</pre> <pre>cn=Service,ou=groups,o=MyOrg</pre> <pre>cn=Shipping,ou=groups,o=MyOrg</pre> <p>Se で開始するグループを検索すると、次のような結果が返ります。</p> <pre>cn=Service,ou=groups,o=MyOrg</pre>

- 3 [開始] をクリックします。
検索結果は、[結果] リストに表示されます。
- 4 このページをデフォルトとして設定するグループを選択して、[追加 (>)] ボタンをクリックします。
ヒント: 複数項目を選択する場合には、<Ctrl> キーを押しながら選択します。
- 5 [保存]、[閉じる] の順にクリックします。

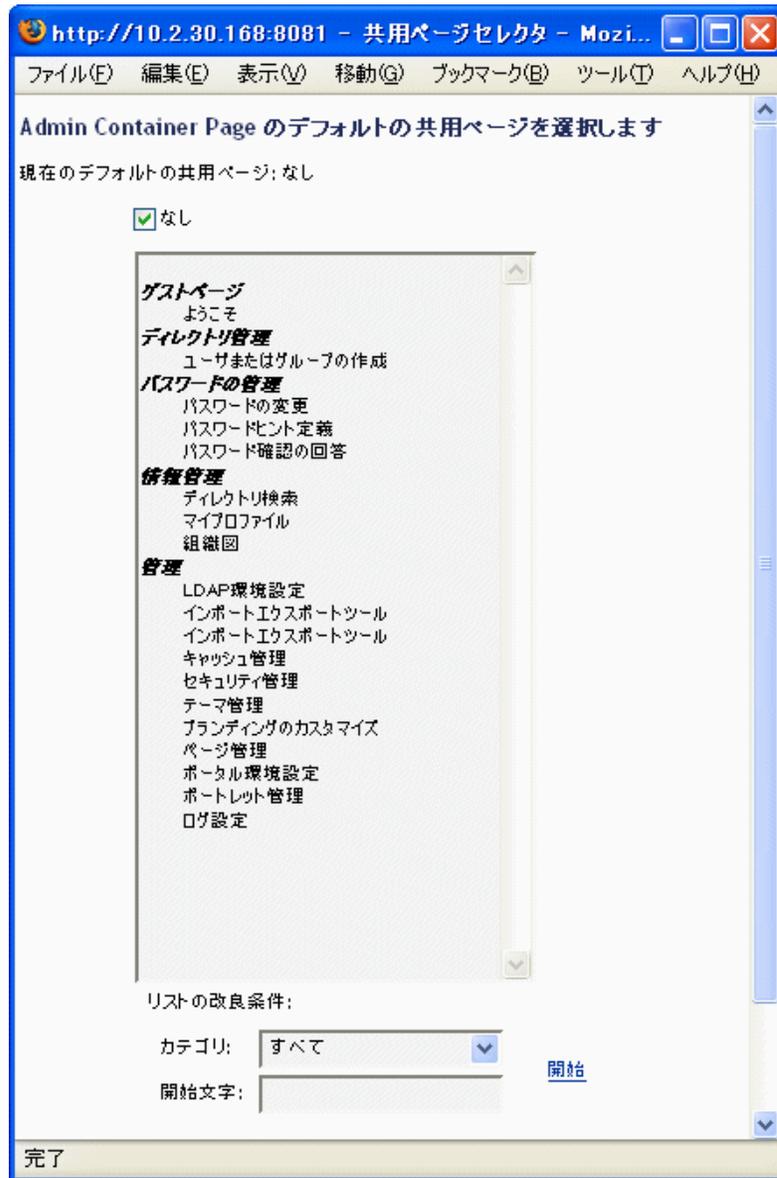
7.6 コンテナページのデフォルト共有ページを選択する

使用する各コンテナページに対してデフォルトの共有ページを割り当てられます。ユーザーインターフェースは、表示内容を決定するときはこのページ割り当てを参照します。

コンテナページのデフォルト共有ページを割り当てるには：

- 1 [コンテナページの維持] パネルでコンテナページを開きます。
- 2 [ページのプロパティ] セクションで [デフォルトの共有ページ] を確認し、[デフォルトの選択] をクリックします。

ブラウザの新しいウィンドウにデフォルトの共有ページを選択するためのダイアログボックスが表示されます。



- 共有ページのリストが長い場合は、リストを(カテゴリ順や開始テキスト順に)並べ替えると、目的のページを見つけやすくなります。
- コンテナページのデフォルトとして使用する共有ページを選択します(デフォルトを設定しない場合は [なし] をオンにします)。
- [保存] をクリックして選択を適用し、ダイアログボックスを閉じます。
- [ページの保存] をクリックします([ページのプロパティ] セクションの下部にあります)。

テーマの環境設定

この章では、Identity Manager ユーザインタフェースの [管理] タブの [テーマ] ページを使用する方法について説明します。ここで取り扱う内容は次のとおりです。

- ◆ 175 ページのセクション 8.1 「テーマの環境設定について」
- ◆ 176 ページのセクション 8.2 「テーマのプレビュー」
- ◆ 177 ページのセクション 8.3 「テーマの選択」
- ◆ 178 ページのセクション 8.4 「テーマのブランディングのカスタマイズ」

[管理] タブにアクセスして操作する一般的な情報については、131 ページの第 6 章「[管理] タブの使用」を参照してください。

8.1 テーマの環境設定について

[テーマ] ページを使用して、Identity Managery ユーザインタフェースの外観や操作方法を制御できます。

「テーマ」とは外観上の特徴のセットで、ユーザインタフェース全体 (Guest ページ、ログインページ、[識別セルフサービス] タブ、[要求と承認] タブ、および [管理] タブ) に適用されます。ユーザインタフェースでは常に 1 つのテーマだけが有効になっています。[テーマ] ページでは、切り替えることができるよういくつかのテーマが用意されています。

[テーマ] ページでは、次の操作も実行できます。

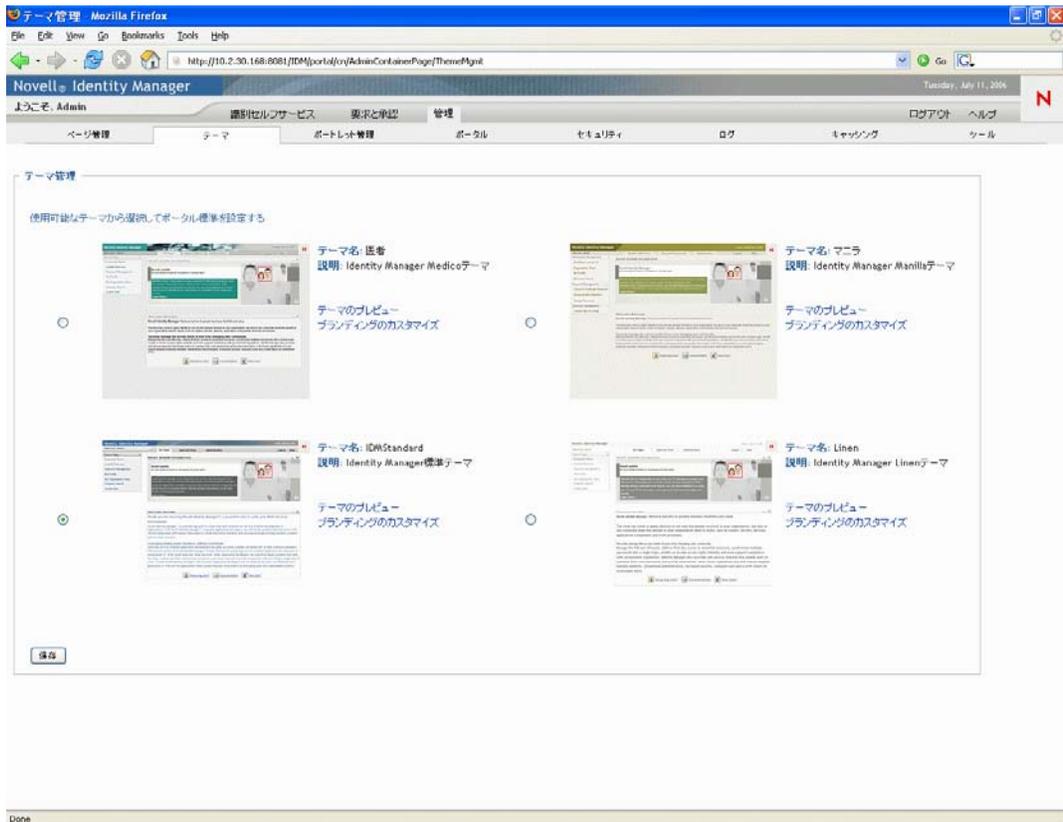
- ◆ 各テーマをプレビューして、どのように表示されるか確認できます。
- ◆ いずれかのテーマをカスタマイズして、ユーザ独自のブランディング (ロゴなど) を反映させることができます。

8.2 テーマのプレビュー

テーマを選択する前に、テーマによって Identity Manager ユーザインタフェースの外観がどのように変わるかプレビューできます。

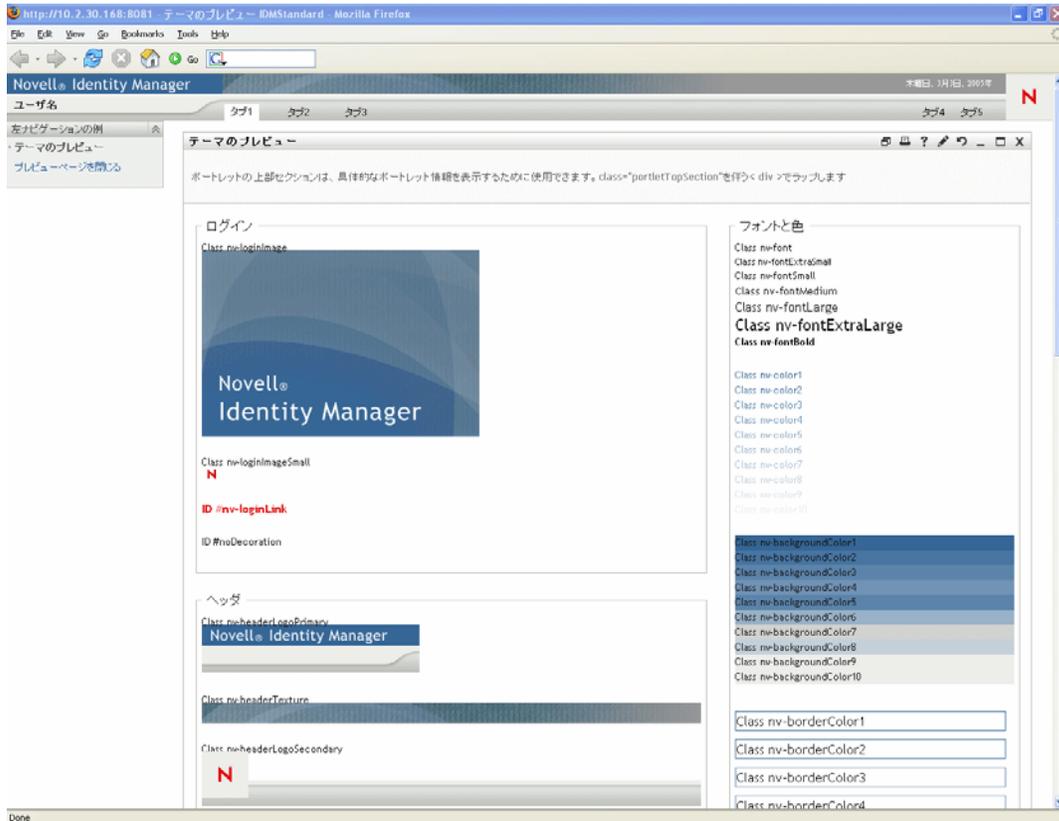
テーマをプレビューするには：

- 1 [テーマ] ページに移動します。



- 2 プレビューするテーマを選び、そのテーマの [テーマのプレビュー] リンクをクリックします。

ブラウザの新しいウィンドウにそのテーマのプレビューが表示されます。



- 3 プレビューをスクロールして、テーマの特徴を確認します。
- 4 確認できたら、[プレビューページを閉じる] (左上隅にあります) をクリックするか、手動でプレビューウィンドウを閉じます。

8.3 テーマの選択

気に入ったテーマが見つかったら、そのテーマを Identity Manager ユーザインタフェースの現在のテーマとして選択できます。

テーマを選択するには：

- 1 [テーマ] ページに移動します。
 - 2 使用するテーマのラジオボタンをクリックします。
 - 3 [保存] ボタンをクリックします。
- 選択したテーマが反映され、ユーザインタフェースの外観が変わります。

8.4 テーマのブランディングのカスタマイズ

どのテーマも、ユーザ独自の画像に入れ替えたり、色設定を変更したりしてカスタマイズできます。これにより、会社や組織のブランディングに合わせて Identity Manager ユーザインタフェースをカスタム表示できます。

テーマのブランド設定をカスタマイズするには：

- 1 [テーマ] ページに移動します。
- 2 カスタマイズするテーマを見つけ、そのテーマの [ブランディングのカスタマイズ] リンクをクリックします。

[テーマ] ページにそのテーマの [ブランディングのカスタマイズ] 設定が表示されます。





3 必要に応じて、次の設定をカスタマイズします。

- ◆ ヘッダ画像
- ◆ ナビゲーション領域の色
- ◆ ログイン画像

それぞれの設定を指定する際には、画面の指示に従ってください。

4 [保存] ボタンをクリックします。

現在のテーマを編集した場合は、カスタマイズした内容が反映され、ユーザインタフェースの外観が変わります。テーマに対するカスタマイズをすべて取り消す場合は、[リセット] ボタンをクリックします。

注: カスタマイズ中にも [テーマのプレビュー] ボタンを使用できますが、この場合、元のテーマが表示されます。変更した内容は反映されません。

5 このテーマの作業が完了したら、[テーマセレクトに戻る] ボタンをクリックします。

ポートレットの管理

この章では、Identity Manager ユーザインタフェースの [管理] タブの [ポートレット管理] ページを使用する方法について説明します。ここで取り扱う内容は次のとおりです。

- ◆ 181 ページのセクション 9.1 「ポートレットの管理について」
- ◆ 182 ページのセクション 9.2 「ポートレットアプリケーションの管理」
- ◆ 185 ページのセクション 9.3 「ポートレット定義を管理する」
- ◆ 190 ページのセクション 9.4 「登録されたポートレットを管理する」

[管理] タブにアクセスして操作する一般的な情報については、131 ページの第 6 章「[管理] タブの使用」を参照してください。

9.1 ポートレットの管理について

[ポートレット管理] ページを使用すると、Identity Manager のユーザインタフェースで使用できるポートレット、およびそれらのポートレットへのアクセス許可を持つユーザを制御できます。ポートレットは、プラグ可能なユーザインタフェースエレメント (Java 標準に基づく) で、ユーザインタフェース内のページのコンテンツ (コンテナページや共有ページなど) を提供します。

ポートレットの管理については、次の項目を操作します。

操作対象	説明
ポートレットアプリケーション	<p>Java Portlet 1.0 準拠の WAR で、ポートレット展開記述子 <code>portlet.xml</code>、およびオプションで他のポートレットランタイムアーティファクトが含まれます。</p> <p>182 ページのセクション 9.2 「ポートレットアプリケーションの管理」 を参照してください。</p>
ポートレット定義	<p>ポートレット環境設定パラメータを指定する記述子です (<code>portlet.xml</code> から読み込まれます)。アプリケーション内の各ポートレットに対し 1 つの定義があります。</p> <p>185 ページのセクション 9.3 「ポートレット定義を管理する」 を参照してください。</p>
ポートレット登録	<p>ポートレット定義に基づくポートレットの登録です。1 つのポートレットアプリケーションに、同じポートレットを複数登録できます。</p> <p>190 ページのセクション 9.4 「登録されたポートレットを管理する」 を参照してください。</p>

Identity Manager ユーザインタフェースに付属するポートレットの詳細については、237 ページのパート IV 「ポートレット参照」を参照してください。コンテナページおよび共有ページでのポートレットの使用については、137 ページの第 7 章「ページの管理」を参照してください。

9.2 ポートレットアプリケーションの管理

Identity Manager ユーザアプリケーションがインストールされると、アプリケーションサーバに IDM.war が展開され、これが自動的にポートレットアプリケーションとして登録されます。IDM.war (インストール時に名前の変更が可能)には、Identity Manager ユーザインタフェースのデフォルトの環境設定で使用されるすべてのポートレットが含まれています。また、デフォルトで使用されないポートレットも含まれています。IDM.war のポートレットの詳細については、[237 ページのパート IV 「ポートレット参照」](#)を参照してください。

ただし、IDM.war のポートレットしか使用できないというわけではありません。他の標準ポートレットアプリケーション (Java Portlet 1.0 準拠 WAR) をアプリケーションサーバに展開すれば、Identity Manager ユーザインタフェースでこれらのポートレットアプリケーションおよびそのポートレットを操作できます。たとえば、[ポートレット管理] ページには、IDM.war と共に、このようなポートレットアプリケーションも表示されます。

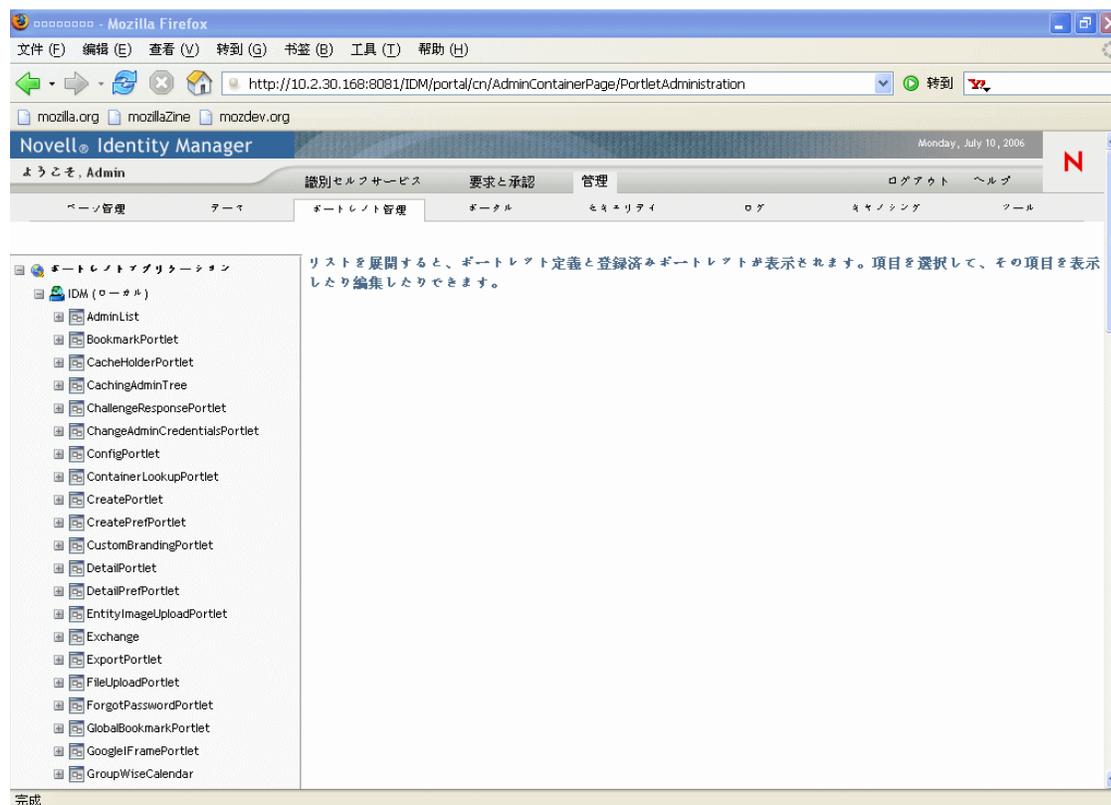
[ポートレット管理] のページでは、IDM.war および他のポートレットアプリケーションを、次の方法により管理できます。

- [182 ページのセクション 9.2.1 「サーバ上のポートレットアプリケーションにアクセスする」](#)
- [183 ページのセクション 9.2.2 「ポートレットアプリケーションの情報を表示する」](#)
- [184 ページのセクション 9.2.3 「ポートレットアプリケーションの登録を取り消す」](#)

9.2.1 サーバ上のポートレットアプリケーションにアクセスする

[ポートレット管理] のページに移動すると、アプリケーションサーバ上に展開されている (IDM.war およびその他の) ポートレットアプリケーションのリストが自動的に表示さ

れます。このリストは左側にツリー形式で表示され、ツリーから展開と移動ができ、選択したポートレットアプリケーションとそのコンテンツを管理できます。



9.2.2 ポートレットアプリケーションの情報を表示する

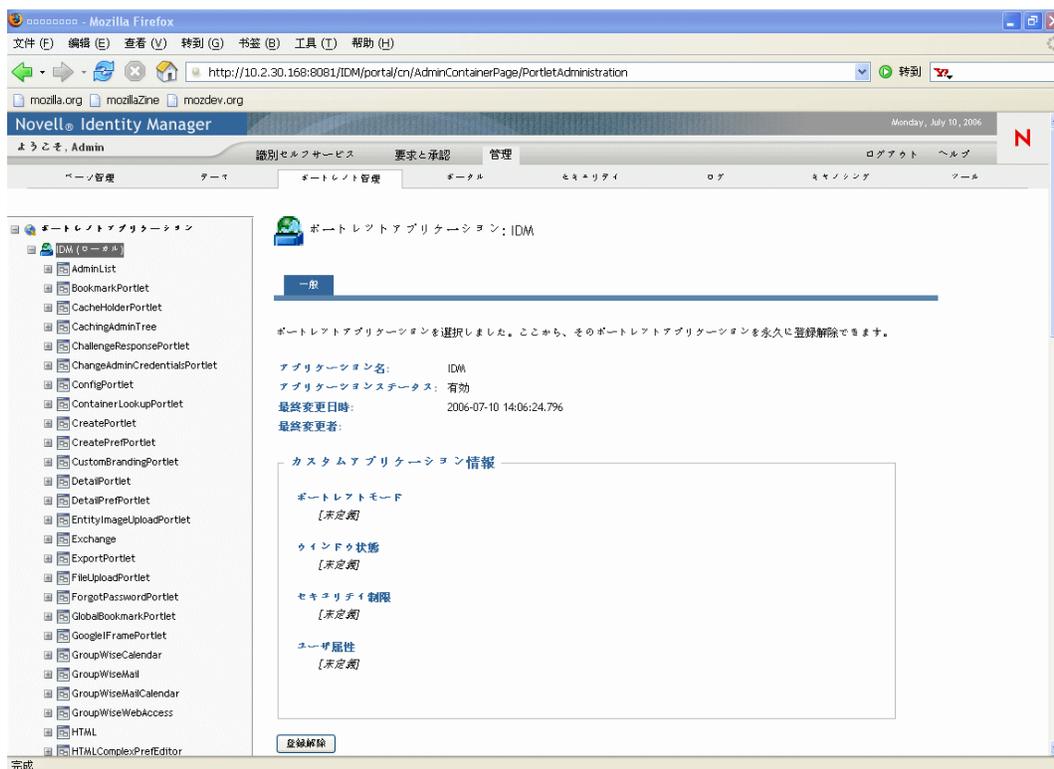
リストされたポートレットアプリケーションに関する次の情報を表示できます (読み込み専用)。

- ◆ 名前
- ◆ ステータス (有効または無効)
- ◆ 最後に変更された日付
- ◆ アプリケーションを最後に変更したユーザ
- ◆ カスタムアプリケーション情報 (該当する場合): ポートレットモード、ウィンドウ状態、セキュリティの制約、およびユーザ属性

ポートレットアプリケーションに関する情報を表示するには:

- ◆ [ポートレットアプリケーション] リストで、情報を表示するポートレットアプリケーションを選択します。

[一般] パネルが右側に表示され、選択したポートレットアプリケーションの情報が表示されます。



9.2.3 ポートレットアプリケーションの登録を取り消す

アプリケーションサーバからポートレットアプリケーションを削除するときは、展開を解除する前にポートレットアプリケーションの登録を取り消す必要があります。登録を取り消さないと、サーバが再起動したときにポートレットアプリケーションが自動的に再展開されます。

ポートレットアプリケーションの登録を取り消すと、アプリケーションデータを保存するデータベースから、関係する初期設定やその他設定がすべて削除されます。

注：ローカルのポートレットコンテナの登録を取り消すことはできません（これはポータルにとってローカルのポートレットアプリケーションになります）。ローカルのポートレットコンテナは、ポータル（Identity Manager ユーザアプリケーション）内に含まれるポートレットを管理します。

ポートレットアプリケーションの登録を取り消すには：

- 1 [ポートレットアプリケーション] リストで、登録を取り消すポートレットアプリケーションを選択します。

[一般] パネルが右側に表示されます（前の手順と同じです）。

- 2 [登録解除] をクリックします。
確認のウィンドウが表示されます。

3 [OK] をクリックして、アクションを確認します。

処理が完了すると、登録を取り消したポートレットアプリケーションは [ポートレットアプリケーション] リストから削除されます。

4 アプリケーションサーバからポートレットアプリケーションを削除するには、サーバのツールを使用し、ポートレットアプリケーションが含まれるアーカイブの展開を解除します。

注：登録を解除したポートレットアプリケーションを再登録するには、再展開する必要があります。

9.3 ポートレット定義を管理する

[ポートレット管理] ページでは、ポートレットアプリケーションのポートレット定義に関連した次のタスクを実行できます。

- ◆ [185 ページのセクション 9.3.1 「展開されたポートレットアプリケーションのポートレット定義にアクセスする」](#)
- ◆ [186 ページのセクション 9.3.2 「ポートレット定義を登録する」](#)
- ◆ [187 ページのセクション 9.3.3 「ポートレット定義の情報を表示する」](#)

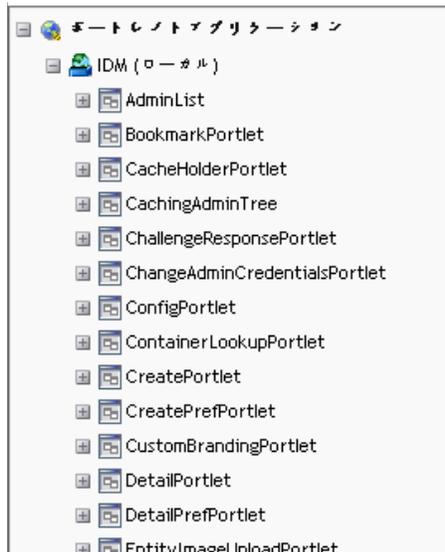
9.3.1 展開されたポートレットアプリケーションのポートレット定義にアクセスする

[ポートレットアプリケーション] リストには、選択したポートレットアプリケーションのポートレット定義が表示されます。

展開されたポートレットアプリケーションのポートレット定義にアクセスするには：

- ◆ [ポートレットアプリケーション] リストで、アクセスするポートレット定義のポートレットアプリケーションを展開します。

ツリーのポートレットアプリケーションの下にポートレット定義がすべて表示されます。



9.3.2 ポートレット定義を登録する

ポートレットを使用する前に、ポータル (Identity Manager ユーザアプリケーション) にポートレット定義を登録する必要があります。登録されたポートレット定義は「ポートレット登録」と呼ばれます。1つのポートレットに対し複数の登録を作成できるため、同じページにそのポートレットのインスタンスを複数設定できます。

ポートレット登録はポートレットクラスの初期設定とその他設定をすべて継承しますが、これらの値は次の方法で変更できます。

- ◆ ポートレット定義を登録する場合 — [190 ページのセクション 9.4 「登録されたポートレットを管理する」](#) を参照してください。
- ◆ ポートレットのインスタンスをページに追加する場合 — [137 ページの第 7 章 「ページの管理」](#) を参照してください。

Identity Manager ユーザアプリケーションに付属するポートレットはすべて、自動的に登録されます。

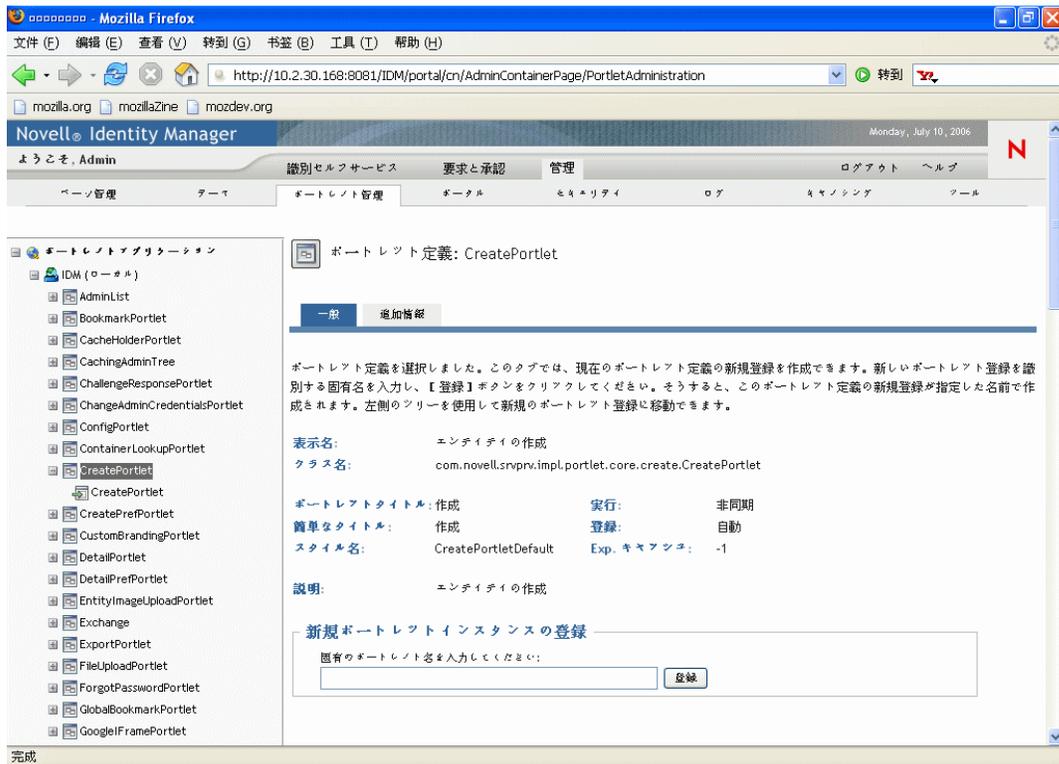
編集モード ポートレット定義が編集モードを提供する場合、エンドユーザはランタイム時にポートレット登録の特定の初期設定を変更できます。この場合、ポートレットの `doEdit()` メソッドのロジックに従います。

Identity Manager ユーザアプリケーションでは、デフォルトの編集モードも実装していません。`doEdit()` メソッドが明示的に実装されていない場合は、デフォルトの初期設定シートが表示されます。

ポートレット定義を登録するには：

- 1 [ポートレット管理] リストで、ポートレット登録を作成するポートレット定義を展開します。

[一般] パネルが右側に表示されます。



選択したポートレットの既存の登録が、[ポートレットアプリケーション] ツリー(左側)の対応するポートレット定義名の下にリストされます。

- 2 [新規ポートレットインスタンスの登録] テキストボックスでポートレット登録の固有の名前を入力し、[登録] をクリックします。

新しいポートレット登録が作成され、[ポートレットアプリケーション] ツリーにリストされます。

- 3 新しいポートレット登録の初期設定およびその他設定を変更する場合は、[190 ページのセクション 9.4 「登録されたポートレットを管理する」](#) を参照してください。

9.3.3 ポートレット定義の情報を表示する

リストされたポートレット定義に関する次の情報を表示できます(読み込み専用です)。

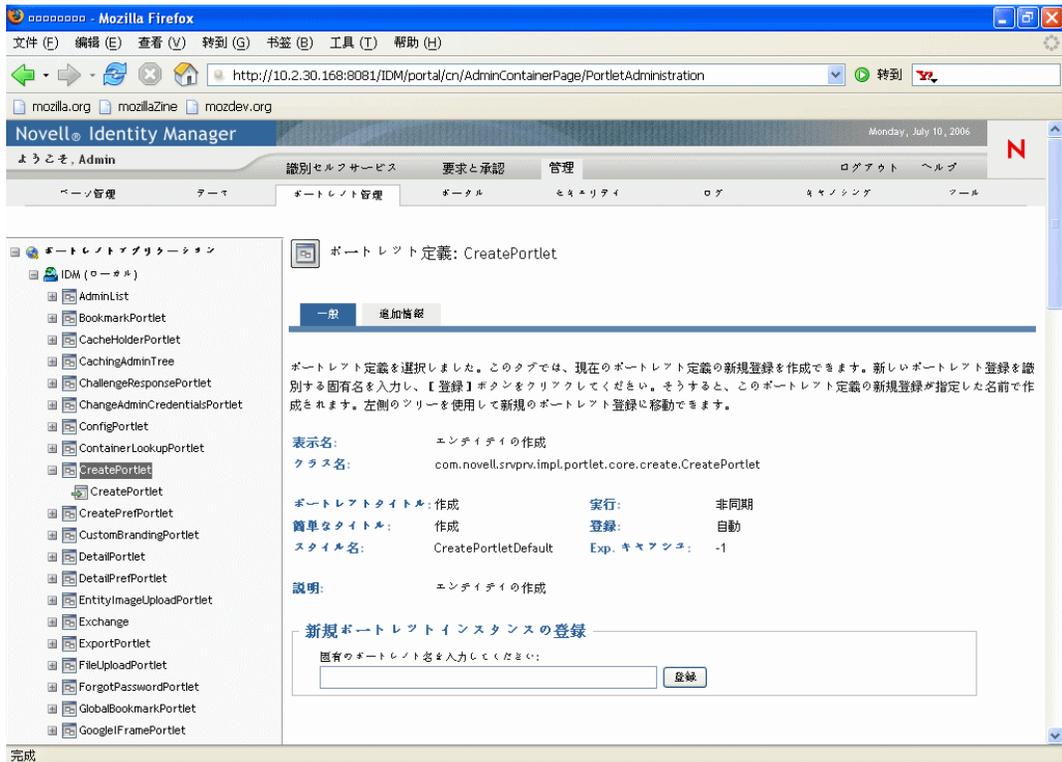
- ◆ 表示名
- ◆ クラス名
- ◆ ポートレットのタイトル
- ◆ 実行タイプ(同期または非同期)
- ◆ 短いタイトル
- ◆ 登録のタイプ
- ◆ スタイル名
- ◆ キャッシュの有効期限

- ◆ 説明
- ◆ 初期化パラメータ
- ◆ キーワード
- ◆ サポートされている MIME タイプ
- ◆ ポートレットによってサポートされているモード
- ◆ サポートされているロケール
- ◆ サポートされているデバイス
- ◆ セキュリティの役割

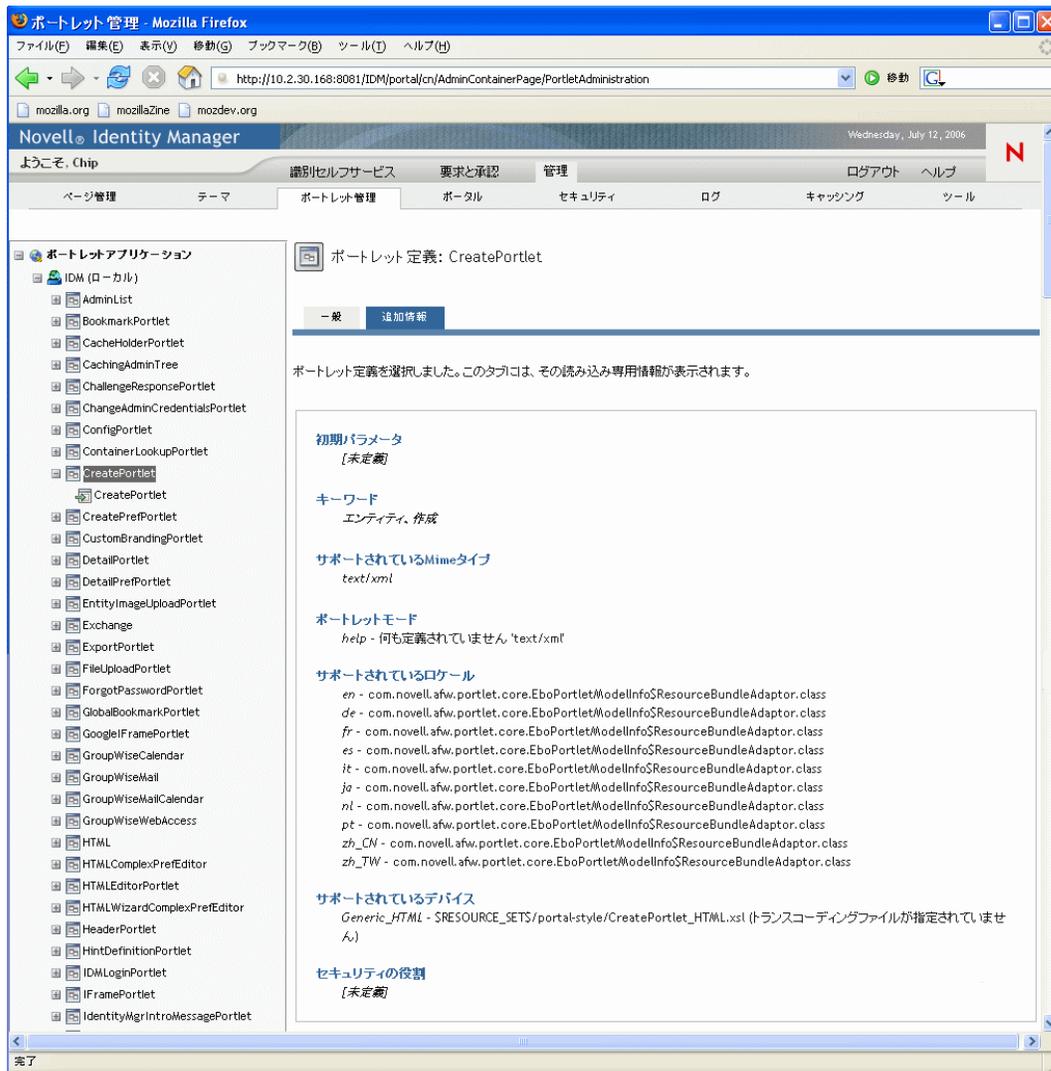
ポートレット定義の情報を表示するには：

- 1 [ポートレットアプリケーション] リストで、情報を表示するポートレット定義を選択します。

[一般] パネルが右側に表示され、選択したポートレット定義の情報が表示されます。



2 [追加情報] パネルに移動し、選択したポートレットの詳細を表示します。



9.4 登録されたポートレットを管理する

[ポートレット管理] ページでは、ポートレットアプリケーションのポートレット登録に関連した次のタスクを実行できます。

- ◆ 190 ページのセクション 9.4.1 「展開されたポートレットアプリケーションでポートレット登録にアクセスする」
- ◆ 191 ページのセクション 9.4.2 「ポートレット登録の情報を表示するには」
- ◆ 192 ページのセクション 9.4.3 「ポートレット登録にカテゴリを割り当てる」
- ◆ 193 ページのセクション 9.4.4 「ポートレット登録の設定を変更する」
- ◆ 196 ページのセクション 9.4.5 「ポートレット登録の初期設定を変更する」
- ◆ 197 ページのセクション 9.4.6 「ポートレット登録のセキュリティ許可を割り当てる」
- ◆ 200 ページのセクション 9.4.7 「ポートレットの登録を取り消す」

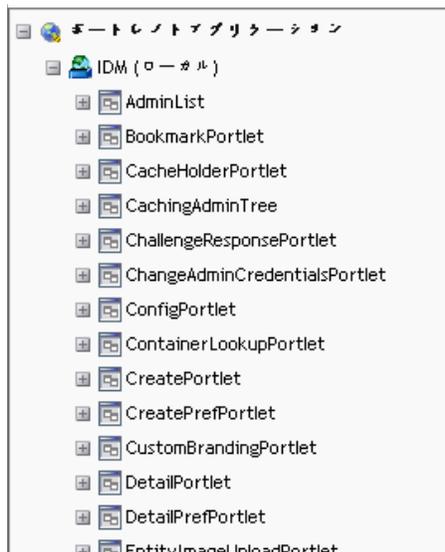
9.4.1 展開されたポートレットアプリケーションでポートレット登録にアクセスする

[ポートレットアプリケーション] リストには、選択したポートレットアプリケーション内の各ポートレット定義のポートレット登録が表示されます。

展開されたポートレットアプリケーション内のポートレット登録にアクセスするには：

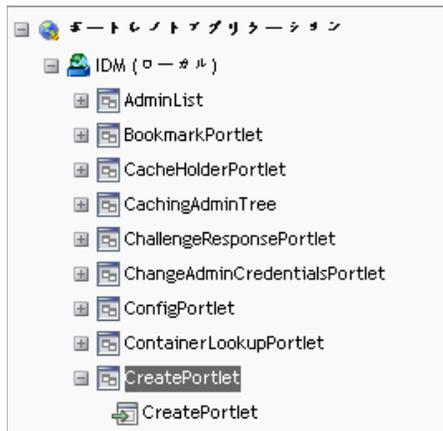
- 1 [ポートレットアプリケーション] リストで、アクセスするポートレット定義と登録が含まれるポートレットアプリケーションを展開します。

ツリーのポートレットアプリケーションの下にポートレット定義がすべて表示されます。



- 2 アクセスするポートレット登録のポートレット定義を展開します。

ツリーのポートレット定義の下に該当するポートレット登録がすべて表示されます。



9.4.2 ポートレット登録の情報を表示するには：

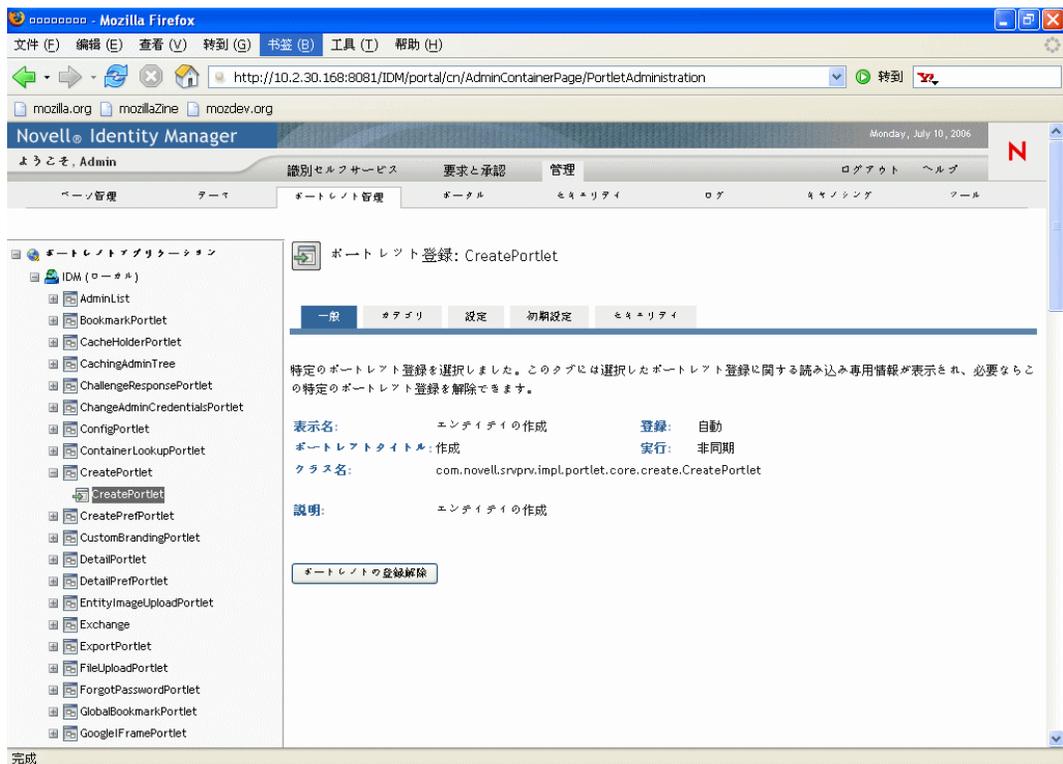
リストされたポートレット登録に関する次の情報を表示できます (読み込み専用です)。

- ◆ 表示名
- ◆ 登録のタイプ
- ◆ ポートレットのタイトル
- ◆ 実行タイプ (同期または非同期)
- ◆ クラス名
- ◆ 説明

ポートレット登録の情報を表示するには：

- ◆ [ポートレットアプリケーション] リストで、情報を表示するポートレット登録を選択します。

[一般] パネルが右側に表示され、選択したポートレット登録の情報が表示されます。



9.4.3 ポートレット登録にカテゴリを割り当てる

ポートレット登録をカテゴリ別に整理すると、ポートレットアプリケーションで特定のポートレットを容易に検索できます。

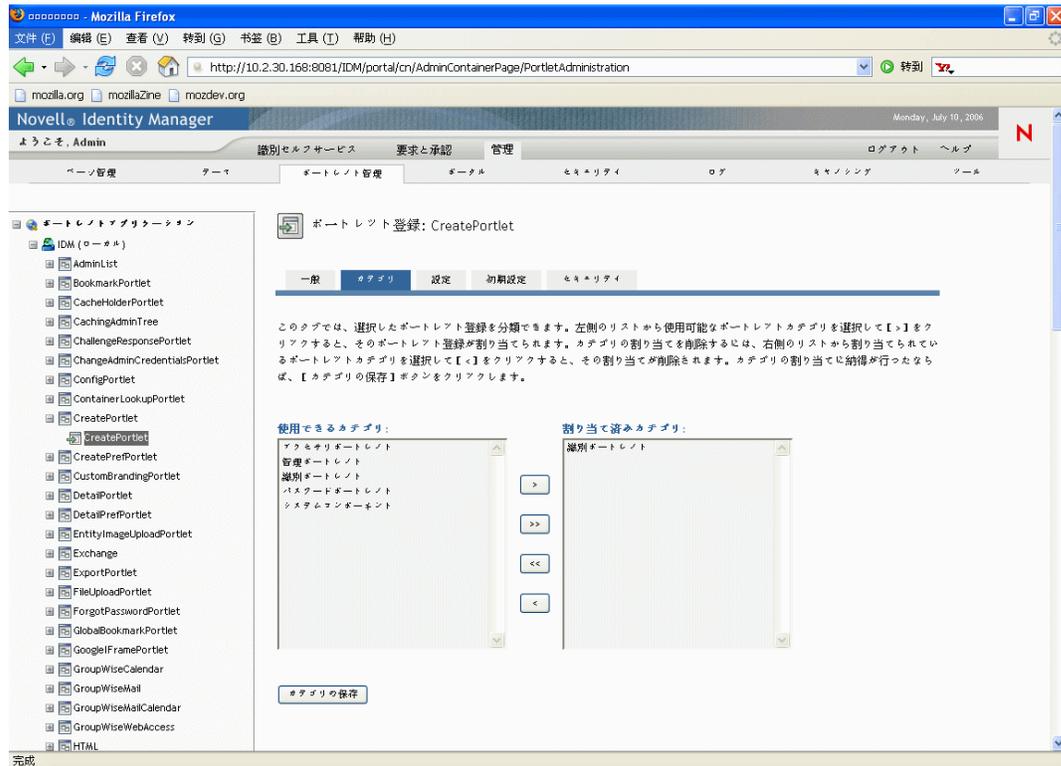
ポートレット登録にカテゴリを割り当てるには：

- 1 [ポートレットアプリケーション] リストで、カテゴリを設定するポートレット登録を選択します。

[一般] パネルが右側に表示されます。

- 2 [カテゴリ] パネルに移動します。

このパネルには、選択したポートレット登録で利用できるカテゴリのリスト、および割り当てられたカテゴリのリストが表示されます。



3 [割り当て済みカテゴリ] リストを適宜更新します。

可能な操作	操作手順
ポートレット登録に1つまたは複数のカテゴリを割り当てる	割り当てる各カテゴリを選択し、[>] をクリックします。
ポートレット登録にすべてのカテゴリを割り当てる	[>>] をクリックします。
1つまたは複数のカテゴリの割り当てを削除する	削除する各カテゴリを選択し、[<] をクリックします。
すべてのカテゴリの割り当てを削除する	[<<] をクリックします。

4 [カテゴリの保存] をクリックします。

9.4.4 ポートレット登録の設定を変更する

ポートレット設定では、ポータル (Identity Manager ユーザアプリケーション) が個別のポートレットと対話的にやり取りする方法が定義されます。各ポートレットは次の設定で構成されます。

- ◆ タイトル

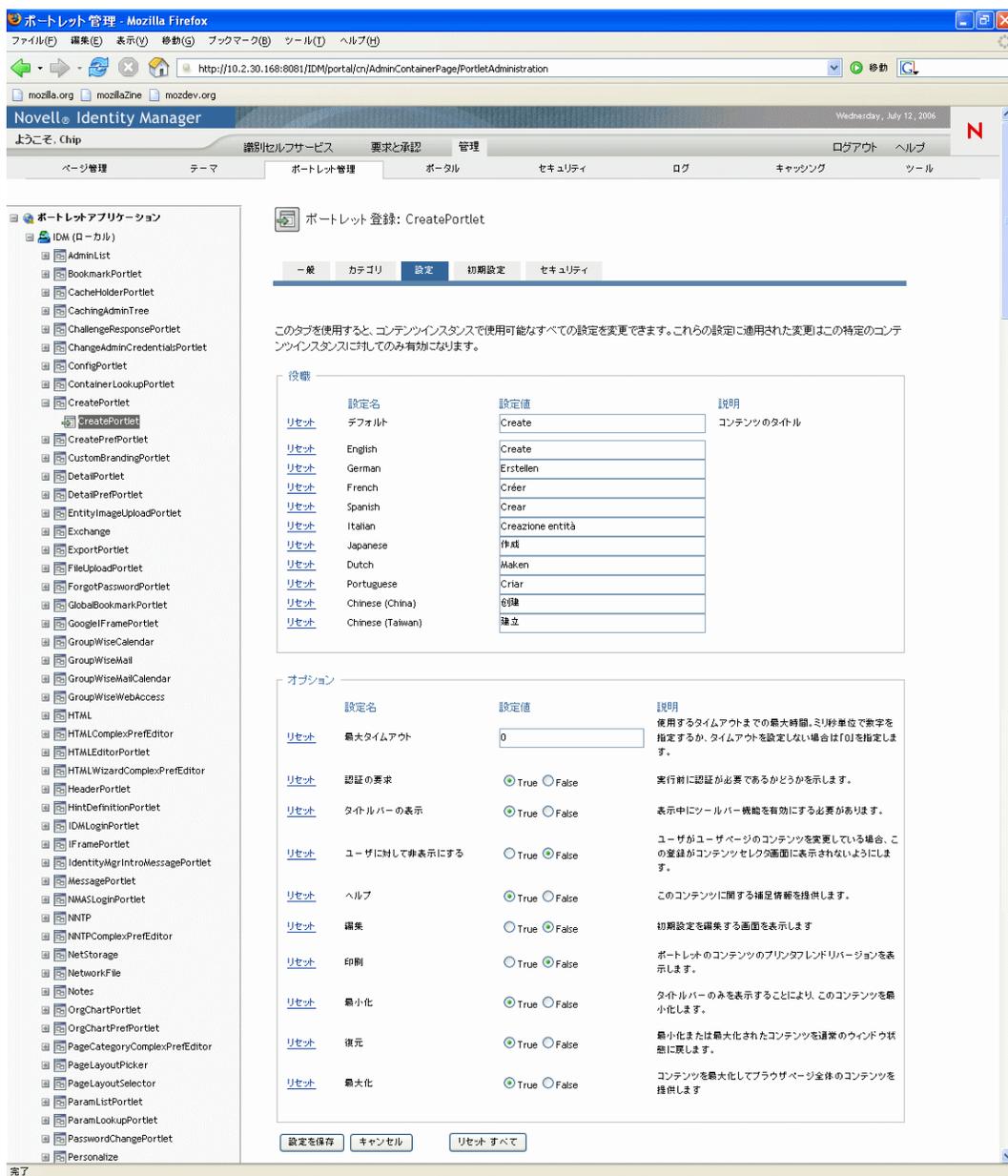
- ◆ タイムアウトの最大時間
- ◆ 認証の必要性
- ◆ タイトルバーの表示 / 非表示
- ◆ ユーザに対して非表示にする
- ◆ ポートレットアプリケーションで定義されたオプション

標準 Java Portlet 1.0 の設定が、ポートレットアプリケーション WAR のポートレット展開記述子 (portlet.xml) 内に定義されています。これらの設定値は [ポートレット管理] ページを使用して登録別に変更できます。この場合、新しい値は選択したポートレット登録にのみ適用されます。

ポートレット登録の設定を変更するには：

- 1 [ポートレットアプリケーション] リストで、設定を変更するポートレット登録を選択します。
[一般] パネルが右側に表示されます。
- 2 [設定] パネルに移動します。

このパネルには、選択したポートレット登録の現在の設定が表示されます。



3 必要に応じて設定を変更します。

このパネルでの作業中、次のアクションも実行できます。

可能な操作

未保存の変更を破棄する

このポートレット登録の設定をすべてデフォルト値に戻す (対応するポートレット定義がベースになります)。

操作手順

[キャンセル] をクリックします。

[すべてリセット] をクリックします。

可能な操作	操作手順
個々の設定をデフォルト値に戻す	各設定の横にある [リセット] リンクをクリックします。

4 [設定を保存] をクリックします。

9.4.5 ポートレット登録の初期設定を変更する

ポートレットの初期設定は、ポートレットの設計時に開発者がポートレット展開記述子で定義します。初期設定は、ポートレットの開発者の実装に基づきポートレットごとに異なります。

[ポートレット管理] ページを使用して、これらの初期設定値を登録ごとに変更できます。この場合、新しい値は選択したポートレット登録にのみ適用されます。

ポートレット登録の初期設定を変更するには：

- 1 [ポートレットアプリケーション] リストで、初期設定を変更するポートレット登録を選択します。

[一般] パネルが右側に表示されます。

- 2 [初期設定] パネルに移動します。

このパネルには、選択したポートレット登録の現在の初期設定が表示されます。

The screenshot shows the 'Novell Identity Manager' web interface. The main content area is titled 'ポートレット登録: CreatePortlet'. Below the title, there are tabs for '一般', 'カテゴリ', '設定', '初期設定', and 'セキュリティ'. The '初期設定' tab is active. A message states: 'このタブを使用すると、このコンテンツインスタンスに定義されたすべてのデフォルトの初期設定を変更できます。初期設定に適用された変更はこの特定のコンテンツインスタンスに対してのみ有効になります。' Below this is a table with the following data:

初期設定	選択値	要求	読み込み専用	非表示
リセット 初回ログイン時にパスワードを有効期限切れにしますか?	true	詳細	<input type="checkbox"/>	<input type="checkbox"/>
リセット Virtual Entity マネジメント優先設定の作成	カスタム初期設定の表示/編集	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

At the bottom of the table, there are buttons for '設定の保存', 'キャンセル', 'すべてリセット', and '説明'. The page footer shows '完成'.

- 3 必要に応じて初期設定を変更します。

このパネルでの作業中、次のアクションも実行できます。

可能な操作	操作手順
初期設定の詳細情報を表示する	[説明] をクリックします。
未保存の変更を破棄する	[キャンセル] をクリックします。
このポートレット登録の初期設定をすべてデフォルト値に戻す(対応するポートレット定義がベースになります)。	[すべてリセット] をクリックします。
個々の初期設定をデフォルト値に戻す	各初期設定の横にある [リセット] リンクをクリックします。

4 ポートレット定義で指定された、各ロケールの初期設定のローカライズバージョンを変更する場合は、次の手順に従います。

4a その初期設定の横にある [詳細] リンクをクリックします(リンクが表示されている場合)。

各ロケールの初期設定値がパネルに表示されます。

4b 必要に応じて値を変更します。

4c [OK] をクリックして変更を適用し、初期設定のメインリストに戻ります。

5 [設定の保存] をクリックします。

9.4.6 ポートレット登録のセキュリティ許可を割り当てる

ユーザ、グループ、およびコンテナに、ポートレット登録に対する次のセキュリティ許可を割り当てられます。

許可	説明
リスト	ユーザは、選択したリストからポートレット登録を表示できます。
実行	ユーザは、ポータルページでポートレット登録を実行できます。

セキュリティ許可を変更した場合、新しい値は選択したポートレット登録にのみ適用されます。

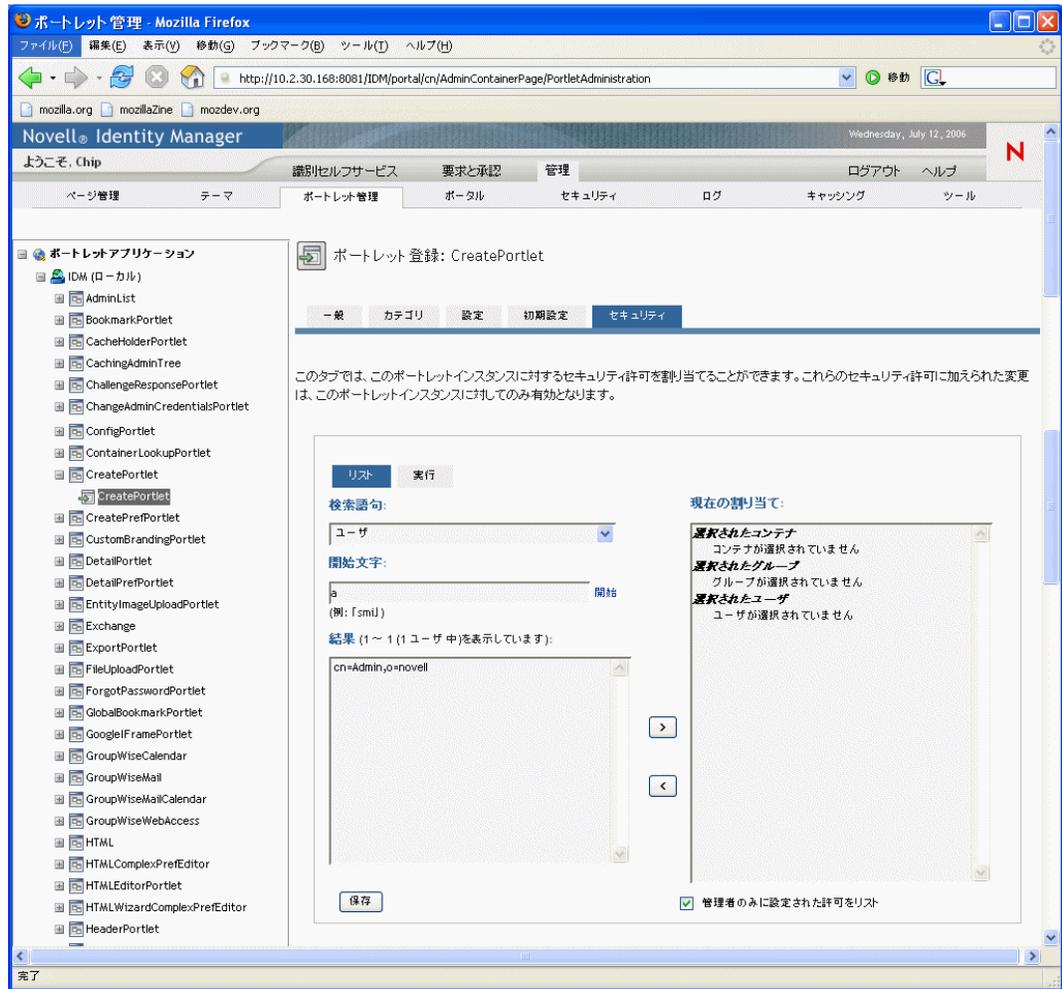
ポートレット登録のセキュリティ許可を割り当てるには：

1 [ポートレットアプリケーション] リストで、セキュリティ許可を変更するポートレット登録を選択します。

[一般] パネルが右側に表示されます。

2 [セキュリティ] パネルに移動します。

このパネルには、選択したポートレット登録の現在のセキュリティ許可が表示されます。



- 3 割り当てる許可のタイプに応じて、[リスト] タブまたは [実行] タブに移動します。
- 4 次の検索設定値を指定します。

設定	操作
検索対象	次のいずれかをドロップダウンメニューから選択します。 <ul style="list-style-type: none"> ◆ ユーザ ◆ グループ ◆ コンテナ

設定	操作
開始文字	<p>可能な操作</p> <ul style="list-style-type: none"> ◆ 指定したタイプ (ユーザ、グループ、またはコンテナ) で使用できるオブジェクトをすべて検索する場合は、この設定を空白にします。 ◆ これらのオブジェクトのサブセットを検索する場合は、目的の CN 値の開始文字を入力します。大文字小文字は区別されません。また、ワイルドカードはサポートされていません。 <p>たとえば、S で開始するグループを検索することにより、検索結果は次のように絞り込まれます。</p> <pre>cn=Sales,ou=groups,o=MyOrg</pre> <pre>cn=Service,ou=groups,o=MyOrg</pre> <pre>cn=Shipping,ou=groups,o=MyOrg</pre> <p>Se で開始するグループを検索すると、次のような結果が返ります。</p> <pre>cn=Service,ou=groups,o=MyOrg</pre>

5 [開始] をクリックします。

検索結果は、[結果] リストに表示されます。

6 ポートレット登録に割り当てるユーザ、グループ、またはコンテナを選択して、[追加 (>)] ボタンをクリックします。

ヒント : 複数項目を選択する場合には、<Ctrl> キーを押しながら選択します。

7 ポートレット登録のロックの有効または無効を次のように設定します。

可能な操作	操作手順
ポートレット登録をロックして、ユーザアプリケーション管理者だけがそのポートレット登録を一覧表示したり実行したりできるようにする	[リスト許可を管理者のみに設定] および [実行許可を管理者のみに設定] をオンにします。
割り当てられたすべてのユーザ、グループ、およびコンテナがポートレット登録を表示および実行できるようにする	[リスト許可を管理者のみに設定] および [実行許可を管理者のみに設定] をオフにします。

注 : この設定をオフにした状態でポートレット登録に対して明示的に割り当てられたユーザ、グループ、またはコンテナがない場合、ユーザ全員がこのポートレット登録に対しリスト許可と実行許可を持つこととなります。

8 [保存] をクリックします。

9.4.7 ポートレットの登録を取り消す

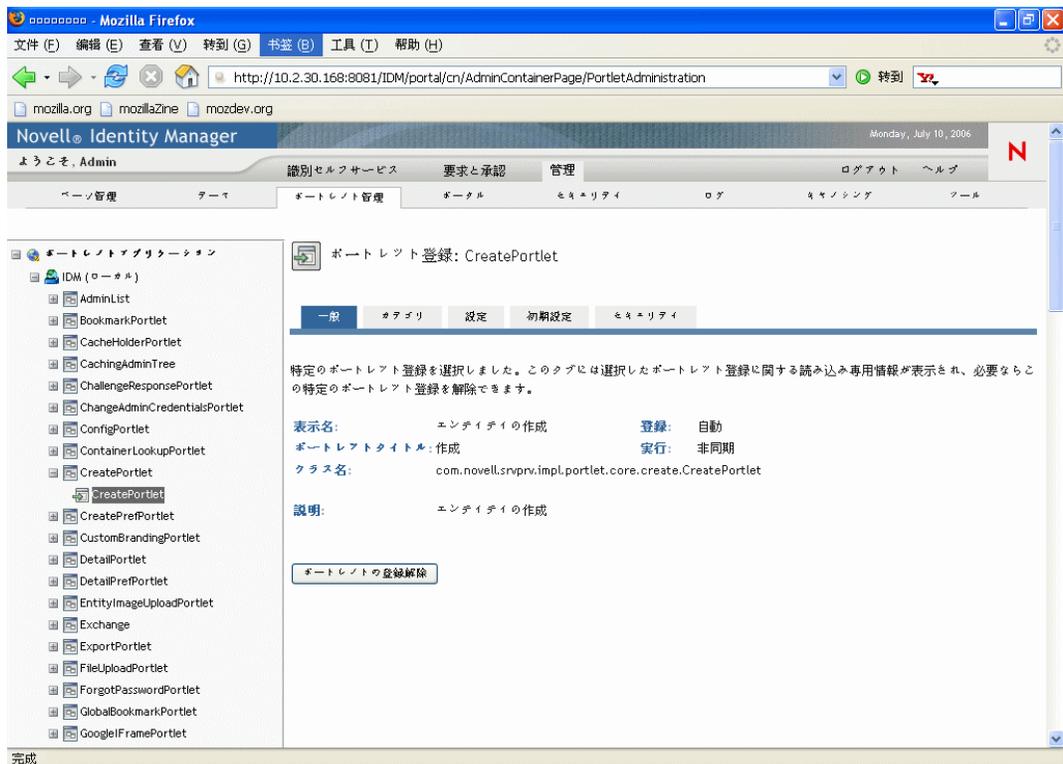
必要に応じて、[ポートレット管理] ページを使用してポートレットの登録を取り消すことができます。

注：自動登録で定義されたポートレットは、登録を取り消してもアプリケーションサーバーの再起動時に自動的に再登録されます。

ポートレットの登録を取り消すには：

- 1 [ポートレットアプリケーション] リストで、登録を取り消すポートレット登録を選択します。

[一般] パネルが右側に表示され、選択したポートレット登録の情報が表示されます。



- 2 [ポートレットの登録解除] をクリックします。
- 3 登録取り消しの操作を確認するメッセージが表示されたら、[OK] をクリックします。

この章では、Identity Manager ユーザインタフェースの [管理] タブの [ポータル] ページを使用する方法について説明します。ここで取り扱う内容は次のとおりです。

- ◆ 201 ページのセクション 10.1 「ポータル環境設定について」
- ◆ 201 ページのセクション 10.2 「一般設定」
- ◆ 204 ページのセクション 10.3 「LDAP 接続パラメータ」

[管理] タブにアクセスして操作する一般的な情報については、131 ページの第 6 章「[管理] タブの使用」を参照してください。

10.1 ポータル環境設定について

[ポータル] ページを使用すると、Identity Manager ユーザアプリケーションのポータル特性を制御したり、ユーザアプリケーションのアイデンティティボールド (LDAP プロバイダ) への接続方法を指定したりできます。

10.2 一般設定

[ポータル] ページには [一般設定] パネルが用意されており、次の操作に使用できます。

- ◆ 一時的に (次のアプリケーションサーバの再起動またはユーザアプリケーションの再展開まで)、Identity Manager ユーザアプリケーションのポータル特性の一部を変更する
- ◆ Identity Manager ユーザアプリケーションのその他のポータル特性を表示する

一般設定を管理するには：

- 1 [ポータル] のページで、左側のナビゲーションメニューから [一般設定] を選択します。

[一般設定] パネルが表示されます。



- 複数の [ウォーコンテキスト] がある場合は、アクセスしようとしている設定に含まれるものを選択します。
パネルが更新され、選択したコンテキストの現在の設定が表示されます。
- 必要に応じて設定の確認、あるいは変更を行います。詳細については、次を参照してください。
 - 202 ページのセクション 10.2.1 「変更可能な設定」
 - 204 ページのセクション 10.2.2 「読み込み専用の設定」
- 変更を適用する場合には、[保存] をクリックします。

10.2.1 変更可能な設定

[一般設定] パネルでは、複数のポータル設定を変更できます。変更した値は、次のアプリケーションサーバの再起動またはユーザアプリケーションの再展開まで有効です。再起動または再展開が発生すると、これらの設定はユーザアプリケーション WAR のデフォルト値に戻ります。

設定	操作
リクエストタイムアウト (デフォルト)	<p>タイムアウトが発生するまでに要求が待機するデフォルト時間 (ミリ秒) を指定します。</p> <p>タイムアウトを定義する非同期ポートレットがない場合、またはこの値より大きいタイムアウトを定義するポートレットがない場合、このデフォルト値が使用されます。レンダリングする 1 つまたは複数のポートレットがこのデフォルト値より大きいタイムアウトを定義する場合、デフォルトではなくその値が使用されます。</p> <p>ポートレットに定義されたタイムアウト値が小さすぎる場合に発生する多くのタイムアウト発生通知メッセージを抑える目的で、この設定を使用できます。</p> <hr/> <p>注: このデフォルトのタイムアウトが発生する前にすべてのポートレットがレンダリングできれば、要求はただちにクライアントに返されます。</p>
リクエストタイムアウト (最大)	<p>要求が取り消されるまでの最大時間 (ミリ秒) を指定します。この時間の経過後、この値より大きいタイムアウト値を定義するポートレットがあるかどうかにかかわらず、すべての要求がクライアントに返されます。</p> <p>この設定は、1 つまたは複数のポートレットが大きいタイムアウト値を定義している場合でも、ポータルが適宜応答するように、使用されます。</p>
パラレルポートレットの表示	<p>ポータルの非同期ポートレットレンダリングを有効または無効にします。</p> <p>これは拡張機能であり、デフォルトでは無効になっています。この機能を有効にすると、ポータルは非同期レンダリング要求を個別スレッドに割り当てます (ポートレットはパラレルのコンテンツをレンダリングできるようになります)。</p> <p>この機能が無効になっていると、すべてのポートレットはメイン要求スレッドのコンテンツを同期的にレンダリングします。</p>
強制的にポートレットのレンダタイムアウトを実行	<p>スレッドプールに十分な個別スレッドがない場合、非同期ポートレットがメイン要求スレッドにコンテンツのレンダリングを委任できるかどうかを指定します。</p> <p>[いいえ] を選択すると、個別スレッドが使用できない場合、非同期ポートレットはメイン要求スレッドで実行できます。</p> <p>[はい] を選択すると、非同期ポートレットは個別スレッドが使用可能になるまで待機し、それから、コンテンツのレンダリングを再開します。レンダリング要求を実行する前にポートレットにタイムアウトが発生した場合、ポートレット固有のエラーメッセージがポートレットウィンドウに表示されます。</p>

設定	操作
強制的にポートレットのシリアルレンダリングを同期する	<p>同期ポートレットの実行方法を指定します。</p> <p>[はい] を選択すると、同期ポートレットはすべてメイン要求スレッドで実行されます。</p> <p>[いいえ] を選択すると、ポータルは、同期レンダリング要求を処理するための別々のスレッドを割り当てることができます (これにより、メイン要求スレッドのボトルネックを回避できます)。</p>

10.2.2 読み込み専用の設定

次の設定は情報表示のためのものであり、[一般設定] パネルでは変更できません。

ポータルのホームページのパス	デフォルトのレイアウト
ポータルのコントローラサブレットのパス	デフォルトのスタイル
ポータルのポートレットのパス	デフォルトのテーマ
ポータルのログインページのパス	ポータルのリソースパス
デフォルトのコンテナページ	

これらの設定の値は、ユーザアプリケーション WAR で設定されます ([デフォルトのテーマ] には [テーマ] ページの現在のテーマで選択した結果が反映されます)。

10.3 LDAP 接続パラメータ

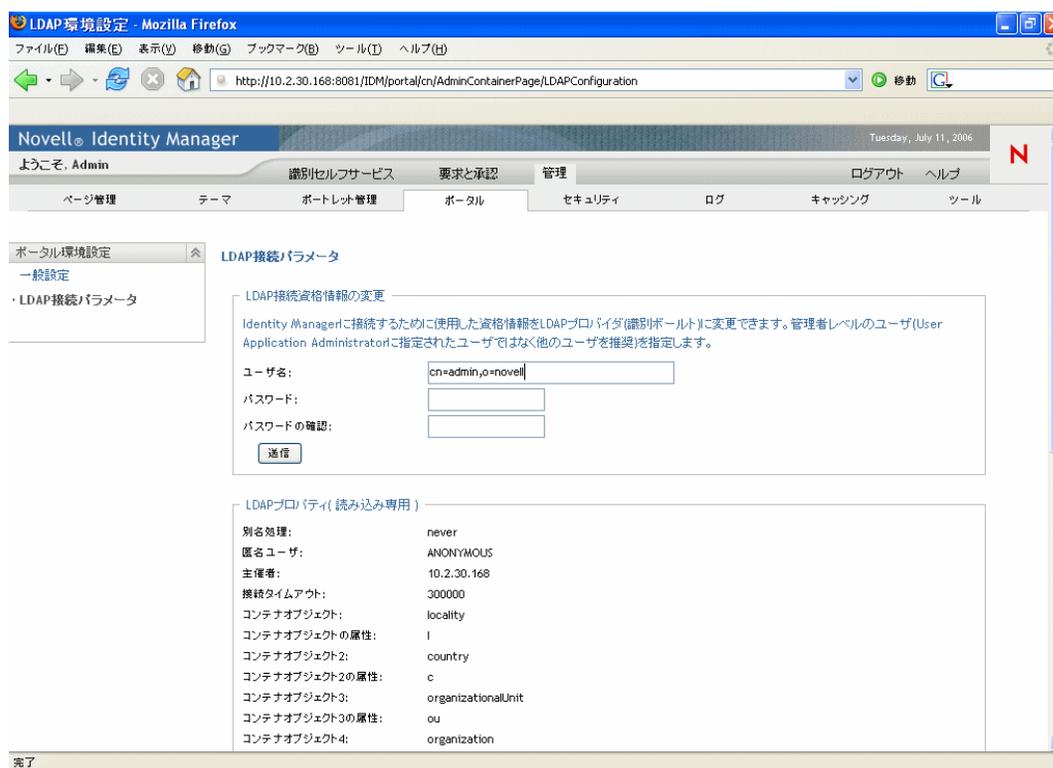
[ポータル] ページには [LDAP 接続パラメータ] パネルが用意されており、次の操作に使用できます。

- ◆ Identity Manager ユーザアプリケーションがアイデンティティボールド(LDAPプロバイダ)に接続するときに使用する資格情報を変更する
- ◆ Identity Manager ユーザアプリケーションの他の LDAP プロパティを表示する

LDAP 接続パラメータを管理するには：

- 1 [ポータル] ページで、左側のナビゲーションメニューから [LDAP 接続パラメータ] を選択します。

[LDAP 接続パラメータ] パネルが表示されます。



2 必要に応じて設定の確認、あるいは変更を行います。詳細については、次を参照してください。

- ◆ 202 ページのセクション 10.2.1 「変更可能な設定」
- ◆ 206 ページのセクション 10.3.2 「読み込み専用の設定」

3 変更を適用する場合は、[送信] をクリックします。

10.3.1 変更可能な設定

[LDAP 接続パラメータ] パネルでは、Identity Manager ユーザアプリケーションがアイデンティティポルト (LDAP プロバイダ) に接続するとき使用する資格情報の設定を変更できます。このパネルで行った変更は、ランタイム時にユーザアプリケーションのデータベースに保存され、アイデンティティポルトに対して検証されます (このパネルからの変更により、インストール時にユーザアプリケーション WAR に記録されている元の資格情報の値は更新されません)。

設定	操作
ユーザ名	<p>アイデンティティポータルでフルの管理者権利を持つユーザの名前を入力します。Identity Manager ユーザアプリケーションは、管理者としてアイデンティティポータルにアクセスする必要があります。</p> <p>通常、アイデンティティポールのルート管理者を LDAP 接続ユーザ名として指定します。ルート管理者はツリーを完全制御できるため、トラスティ権を特に割り当てる必要はありません。</p> <p>次に例を示します。</p> <pre>cn=admin,o=myorg</pre> <p>その他のユーザを指定した場合、ユーザアプリケーションドライバのプロパティ「All Attributes Rights」および「Entry Rights」に継承可能なトラスティ権を割り当てる必要があります。</p> <hr/> <p>注：混乱を避けるため、ユーザアプリケーションのユーザアプリケーション管理者を LDAP 接続ユーザ名として指定しないことをお勧めします。これら 2 つの目的には、別々のアカウントを使用するのが妥当です。</p>
パスワード および パスワードの確認	<p>アイデンティティポールのユーザ名に現在設定されているパスワードを入力します。</p>

10.3.2 読み込み専用の設定

次の設定は情報表示のためのものであり、[LDAP 接続パラメータ] パネルでは変更できません。

ALIAS_HANDLING	GROUP_USER_MEMBER_ATTRIB
ANONYMOUS_USER	KEYSTORE_PATH
AUTHORITY	LOGIN_ATTRIBUTE
CONNECTION_TIMEOUT	NAME
CONTAINER_OBJECT	OBJECT_ATTRIB
CONTAINER_OBJECT_ATTRIB	PROVISION_ROOT
CONTAINER_OBJECT2	REFERRAL
CONTAINER_OBJECT2_ATTRIB	ROOT_NAME
CONTAINER_OBJECT3	USE_DYNAMIC_GROUPS
CONTAINER_OBJECT3_ATTRIB	USE_REGISTERED_DYNAMIC_GROUPS
CONTAINER_OBJECT4	USE_SSL

CONTAINER_OBJECT4_ATTRIB	USER_GROUP_MEMBER_ATTRIB
CONTEXT_FACTORY	USER_OBJECT
DYNAMIC_GROUP_OBJECT	USER_ROOT_CONTAINER
GROUP_OBJECT	USER_SEARCH_SCOPE
GROUP_ROOT_CONTAINER	UUID_ATTRIB
GROUP_SEARCH_SCOPE	UUID_AUX_CLASS

これらの設定の値は、ユーザアプリケーションのインストール時に指定されます。

セキュリティの環境設定

11

この章では、Identity Manager ユーザインタフェースの [管理] タブの [セキュリティ] ページを使用する方法について説明します。ここで取り扱う内容は次のとおりです。

- 209 ページのセクション 11.1 「セキュリティの環境設定について」
- 210 ページのセクション 11.2 「ユーザアプリケーション管理者を割り当てる」

[管理] タブにアクセスして操作する一般的な情報については、131 ページの第 6 章「[管理] タブの使用」を参照してください。

11.1 セキュリティの環境設定について

[セキュリティ] ページを使用すると、Identity Manager ユーザアプリケーションのユーザアプリケーション管理者を指定できます。

ユーザアプリケーション管理者は、Identity Manager ユーザアプリケーションに関連するすべての管理機能を実行できます。この中には、Identity Manager ユーザインタフェースの [管理] タブにアクセスし、そこでサポートされているすべての管理アクションを実行する操作も含まれます。

インストール中、任意のユーザを 1 人、ユーザアプリケーション管理者として指定します。インストール後、そのユーザは [セキュリティ] ページを使用して、必要に応じてその他のユーザアプリケーション管理者を指定できます。

ユーザアプリケーション管理者となるユーザは、通常、ユーザアプリケーションの LDAP 設定で指定されるユーザルートコンテナに格納されます。これによってそのユーザは、毎回完全な識別名を求められることなくユーザ名だけでログインできます。また、このユーザは通常、ツリー内のオブジェクトを管理および作成する権利を持ちますが、これは必須ではありません。

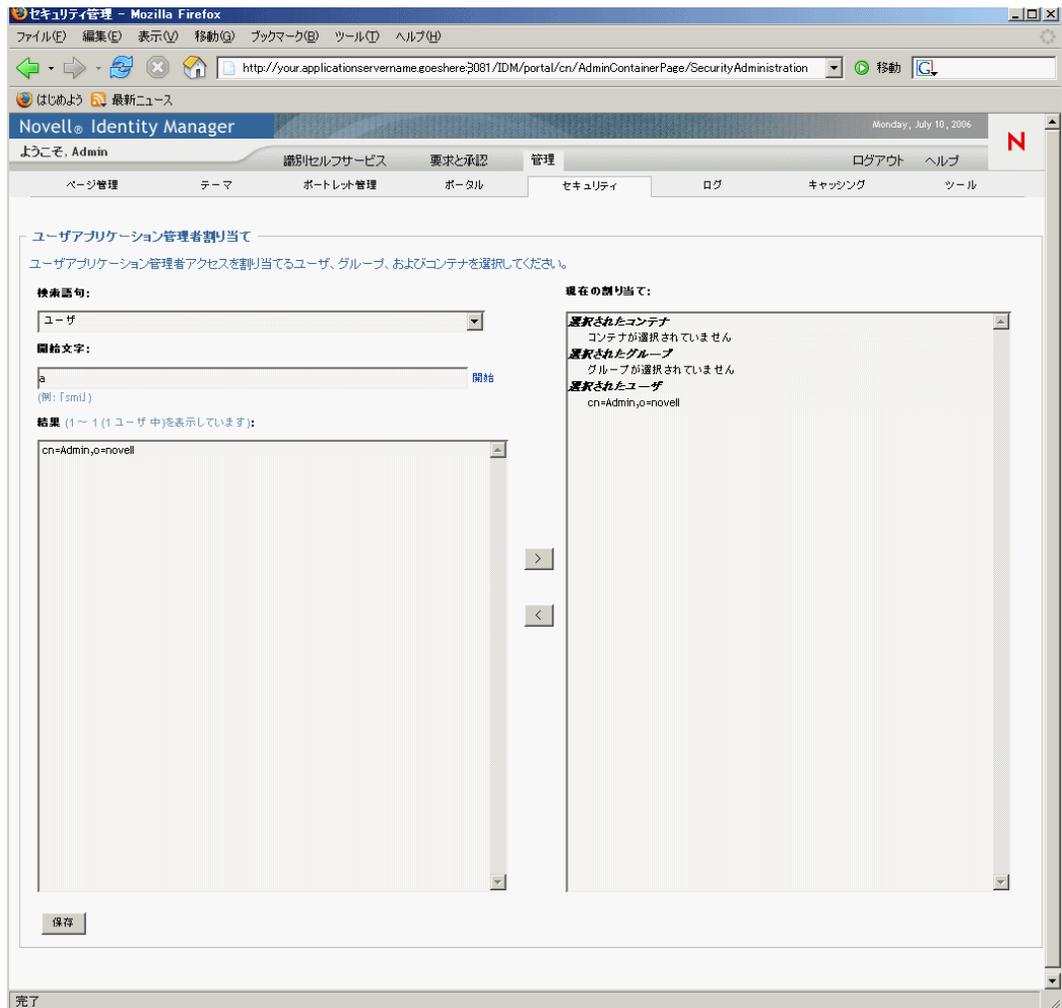
注：必要に応じて、ユーザアプリケーション管理者は、1 人または複数のエンドユーザに対し、[管理] タブの特定のページへのアクセス許可を割り当てることができます。これらの許可の割り当てには、[管理] タブの [ページ管理] ページを使用します。詳細については、137 ページの第 7 章「ページの管理」を参照してください。

11.2 ユーザアプリケーション管理者を割り当てる

ユーザアプリケーション管理者を割り当てる際には、ユーザ、グループ、またはコンテナを指定できます。

ユーザアプリケーション管理者を割り当てるには：

- 1 [セキュリティ] ページに移動します。



- 2 次の検索設定値を指定します。

設定	操作
検索対象	次のいずれかをドロップダウンメニューから選択します。 <ul style="list-style-type: none">◆ ユーザ◆ グループ◆ コンテナ

設定	操作
開始文字	<p>可能な操作</p> <ul style="list-style-type: none"> ◆ 指定したタイプ (ユーザ、グループ、またはコンテナ) で使用できるオブジェクトをすべて検索する場合は、この設定を空白にします。 ◆ これらのオブジェクトのサブセットを検索する場合は、目的の CN 値の開始文字を入力します。大文字小文字は区別されません。また、ワイルドカードはサポートされていません。 <p>たとえば、S で開始するグループを検索することにより、検索結果は次のように絞り込まれます。</p> <pre>cn=Sales,ou=groups,o=MyOrg</pre> <pre>cn=Service,ou=groups,o=MyOrg</pre> <pre>cn=Shipping,ou=groups,o=MyOrg</pre> <p>Se で開始するグループを検索すると、次のような結果が返ります。</p> <pre>cn=Service,ou=groups,o=MyOrg</pre>

3 [開始] をクリックします。

検索結果は、[結果] リストに表示されます。

4 ユーザアプリケーション管理者を割り当てるユーザ、グループ、またはコンテナを選択して、[追加 (>)] ボタンをクリックします。

ヒント : 複数項目を選択する場合には、<Ctrl> キーを押しながら選択します。

5 [保存] をクリックします。

ユーザアプリケーション管理者の割り当てを解除するには :

1 [現在の割り当て] のリストで、ユーザアプリケーション管理者としての割り当てを解除するユーザ、グループ、またはコンテナを選択して、[削除 (<)] ボタンをクリックします。

ヒント : 複数項目を選択する場合には、<Ctrl> キーを押しながら選択します。

2 [保存] をクリックします。

ログの環境設定

この章では、Identity Manager ユーザインタフェースの [管理] タブの [ログ] ページを使用する方法について説明します。ここで取り扱う内容は次のとおりです。

- ◆ 213 ページのセクション 12.1 「ログの環境設定について」
- ◆ 213 ページのセクション 12.2 「ログについて」
- ◆ 216 ページのセクション 12.3 「ログレベルの変更」
- ◆ 217 ページのセクション 12.4 「Novell Audit へのログメッセージの送信」
- ◆ 217 ページのセクション 12.5 「ログ設定の持続」

[管理] タブにアクセスして操作する一般的な情報については、131 ページの第 6 章「[管理] タブの使用」を参照してください。

12.1 ログの環境設定について

[ログ] ページを使用すると、Identity Manager ユーザアプリケーションが生成するログメッセージのレベルを制御したり、これらのメッセージを Novell Audit に送信するかどうかを指定したりすることができます。

Identity Manager ユーザアプリケーションは、Apache Software Foundation より配布されるオープンソースログパッケージである *log4j* を使用してログを行います。デフォルトでは、イベントメッセージは次の両方にログされます。

- ◆ Identity Manager ユーザアプリケーションが展開されるアプリケーションサーバのシステムコンソール。
- ◆ Identity Manager ユーザアプリケーションが展開されるアプリケーションサーバのログファイル。次に例を示します。

```
jboss/server/IDM/log/server.log
```

これはローリングログファイルです。特定のサイズに達すると、別のファイル(など)にロールオーバーします。

Novell Audit を使用している場合には、イベントメッセージを Novell Audit にログするように設定することもできます。

ログ環境および Novell Audit の設定の詳細については、119 ページの第 5 章「ログの設定」を参照してください。

12.2 ログについて

[ログ] ページには、さまざまなログが一覧表示されます。各ログは、Identity Manager ユーザアプリケーションの異なる部分からのイベントメッセージを出力します。出力レベルはログごとに異なります。

ログ名は *log4j* 規則に基づきます。これらのログ名はメッセージ出力のコンテキストを示し、生成されるイベントメッセージ内で確認できます。

ログ名	説明
com.novell	他の Identity Manager ユーザアプリケーションログの親
com.novell.afw.portal.aggregation	ポータルページの処理に関連するメッセージ
com.novell.afw.portal.persist	ポータルデータ (ポータルページおよびポートレット登録を含む) の維持に関連するメッセージ
com.novell.afw.portal.portlet	ポータルコアポートレットおよびアクセサリポートレットからのメッセージ
com.novell.afw.portal.util	ポータルインポートポートレットまたはポータルエクスポートポートレットおよびナビゲーションポートレットからのメッセージ
com.novell.afw.portlet.consumer	ポートレットレンダリングに関連するメッセージ
com.novell.afw.portlet.core	コアポートレット API に関連するメッセージ
com.novell.afw.portlet.persist	ポートレットデータ (ポートレット環境設定およびその他設定値を含む) の維持に関連するメッセージ
com.novell.afw.portlet.producer	ポータル内のポートレットの登録および設定に関連するメッセージ
com.novell.afw.portlet.util	ポートレットにより使用されるユーティリティコードに関連するメッセージ
com.novell.afw.theme	テーマサブシステムからのメッセージ
com.novell.afw.util	ポータルユーティリティクラスに関連するメッセージ
com.novell.soa.af.impl	承認フロー (プロビジョニングワークフロー) サブシステムからのメッセージ
com.novell.srvprv.apwa	「要求と承認」 Web アプリケーション (アクションおよびタグ) からのメッセージ
com.novell.srvprv.impl.portlet.core	コア識別ポートレットおよびパスワードポートレットからのメッセージ
com.novell.srvprv.impl.portlet.util	識別関連ユーティリティポートレットからのメッセージ
com.novell.srvprv.impl.servlet	UI 制御フレームワークの Ajax サブレットおよび Ajax サービスからのメッセージ
com.novell.srvprv.impl.uictrl	UI 制御レジストリ API および承認形式レンダリングからのメッセージ
com.novell.srvprv.impl.vdata	ディレクトリ抽象化レイヤからのメッセージ
com.novell.srvprv.spi	UI 制御レジストリ API からのメッセージ
com.sssw.fw.cachemgr	フレームワークキャッシュサブシステムに関連するメッセージ
com.sssw.fw.core	フレームワークコアサブシステムに関連するメッセージ
com.sssw.fw.directory	フレームワークディレクトリサブシステムに関連するメッセージ

ログ名	説明
com.sssw.fw.event	フレームワークイベントサブシステムに関連するメッセージ
com.sssw.fw.factory	フレームワークファクトリサブシステムに関連するメッセージ
com.sssw.fw.persist	フレームワーク持続サブシステムに関連するメッセージ
com.sssw.fw.resource	フレームワークリソースサブシステムに関連するメッセージ
com.sssw.fw.security	フレームワークセキュリティサブシステムに関連するメッセージ
com.sssw.fw.server	フレームワークサーバサブシステムに関連するメッセージ
com.sssw.fw.servlet	フレームワークサーブレットサブシステムに関連するメッセージ
com.sssw.fw.session	フレームワークセッションサブシステムに関連するメッセージ
com.sssw.fw.usermgr	フレームワークユーザサブシステムに関連するメッセージ
com.sssw.fw.util	フレームワークユーティリティサブシステムに関連するメッセージ
com.sssw.portal.manager	Portal Manager に関連するメッセージ
com.sssw.portal.persist	ポータル <small>の</small> 維持に関連するメッセージ

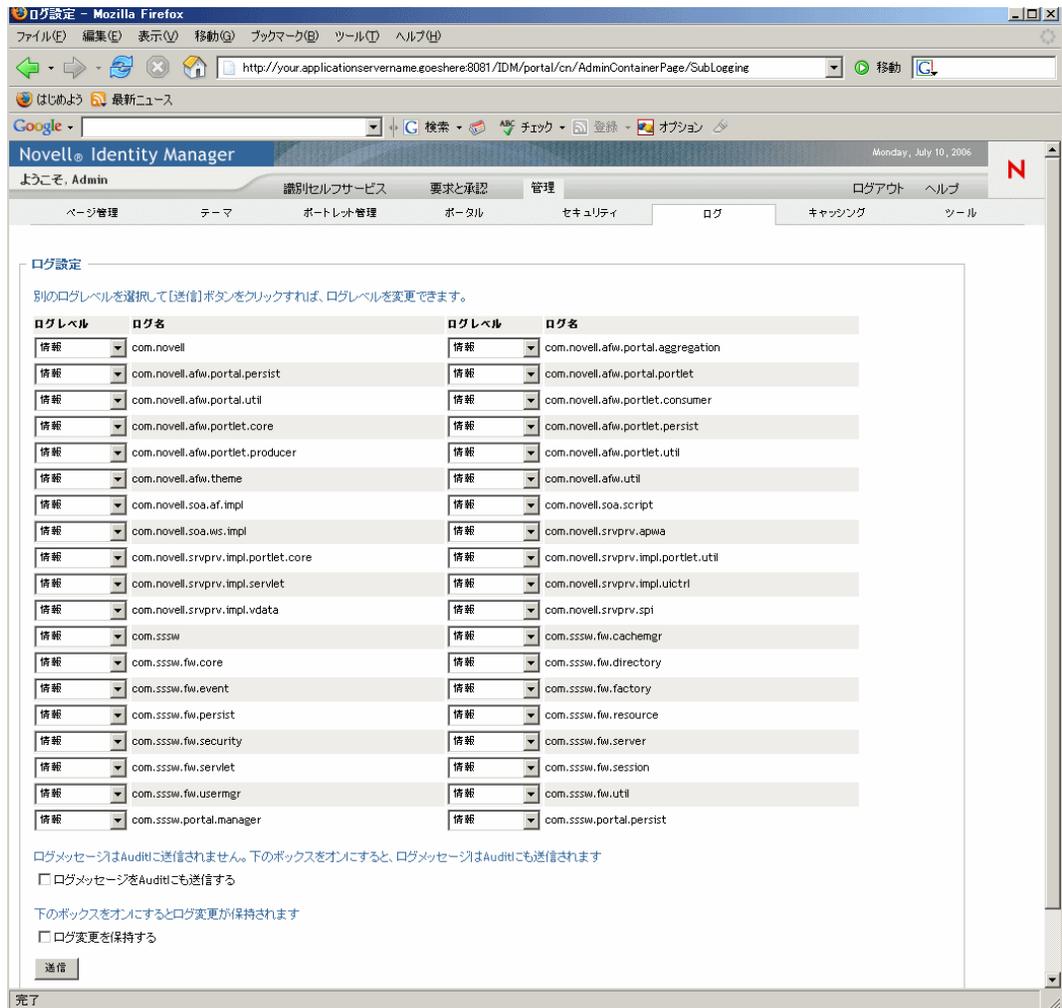
ユーザアプリケーションのログは階層的で、たとえば、**com.novell** はその下にある他のログの親となります。ログが追加された場合は、そのプロパティを継承します。

12.3 ログレベルの変更

特定のログに設定されているレベルを変更することにより、そのログに書き込まれる情報量を制御できます。デフォルトでは、すべてログは「情報」に設定されています。これは中間のレベルです。

ログレベルを変更するには：

- 1 [ログ] ページに移動します。



- 2 ページ上で、レベルを変更するログを見つけます。
- 3 ドロップダウンメニューから次のいずれかのレベルを選択します。

レベル	説明
致命的	詳細度は最小： 致命的エラーをログに書き込みます。

レベル	説明
エラー	エラー (および上記すべて) をログに書き込みます。
警告	警告 (および上記すべて) をログに書き込みます。
情報	情報メッセージ (および上記すべて) をログに書き込みます。
DEBUG	デバッグ情報 (および上記すべて) をログに書き込みます。
トレース	詳細度は最大: トレース情報 (および上記すべて) をログに書き込みます。

- 4 必要に応じて、他のログに対して、**ステップ 2** および **ステップ 3** を繰り返します。
- 5 [送信] をクリックします。

12.4 Novell Audit へのログメッセージの送信

[ログ] ページから、Identity Manager ユーザアプリケーションがイベントメッセージ出力を Novell Audit に送信するかどうかを制御できます。デフォルトでは、ユーザアプリケーションのインストール時に有効にしない限り、Novell Audit へのログは無効になっています。

Novell Audit へのログを有効または無効にするには：

- 1 [ログ] ページに移動します。
- 2 次のチェックボックスをオンまたはオフにします。

Also send logging messages to Audit

- 3 [送信] をクリックします。

12.5 ログ設定の持続

デフォルトでは、[ログ] ページで加えられた変更は、次にアプリケーションサーバが再起動されるか、ユーザアプリケーションが再展開されるまで有効です。その後は、ログ設定はデフォルト値に戻ります。

ただし、[ログ] ページには、設定に対する変更を持続できるオプションがあります。この機能を有効にすると、ログ設定値は、Identity Manager ユーザアプリケーションが展開されたアプリケーションサーバのログ環境設定ファイルに保存されます。次に例を示します。

```
jboss/server/IDM/conf/extendlogging.xml
```

設定の持続を有効または無効にするには：

- 1 [ログ] ページに移動します。
- 2 次のチェックボックスをオンまたはオフにします。

Persist the logging changes

- 3 [送信] をクリックします。

この章では、Identity Manager ユーザインタフェースの [管理] タブの [キャッシング] ページを使用する方法について説明します。ここで取り扱う内容は次のとおりです。

- ◆ 219 ページのセクション 13.1 「キャッシングの環境設定について」
- ◆ 219 ページのセクション 13.2 「キャッシュのフラッシュ」
- ◆ 221 ページのセクション 13.3 「キャッシュを設定する」

[管理] タブにアクセスして操作する一般的な情報については、131 ページの第 6 章「[管理] タブの使用」を参照してください。

13.1 キャッシングの環境設定について

[キャッシング] ページを使用して、Identity Manager ユーザアプリケーションが使用するさまざまなキャッシュを管理できます。再利用可能な一時データをアプリケーションサーバに格納してパフォーマンスを最適化するために、ユーザアプリケーションではキャッシュが使用されます。

必要に応じてコンテンツをフラッシュしたり、キャッシュの環境設定を変更したりすることで、キャッシュを制御できます。

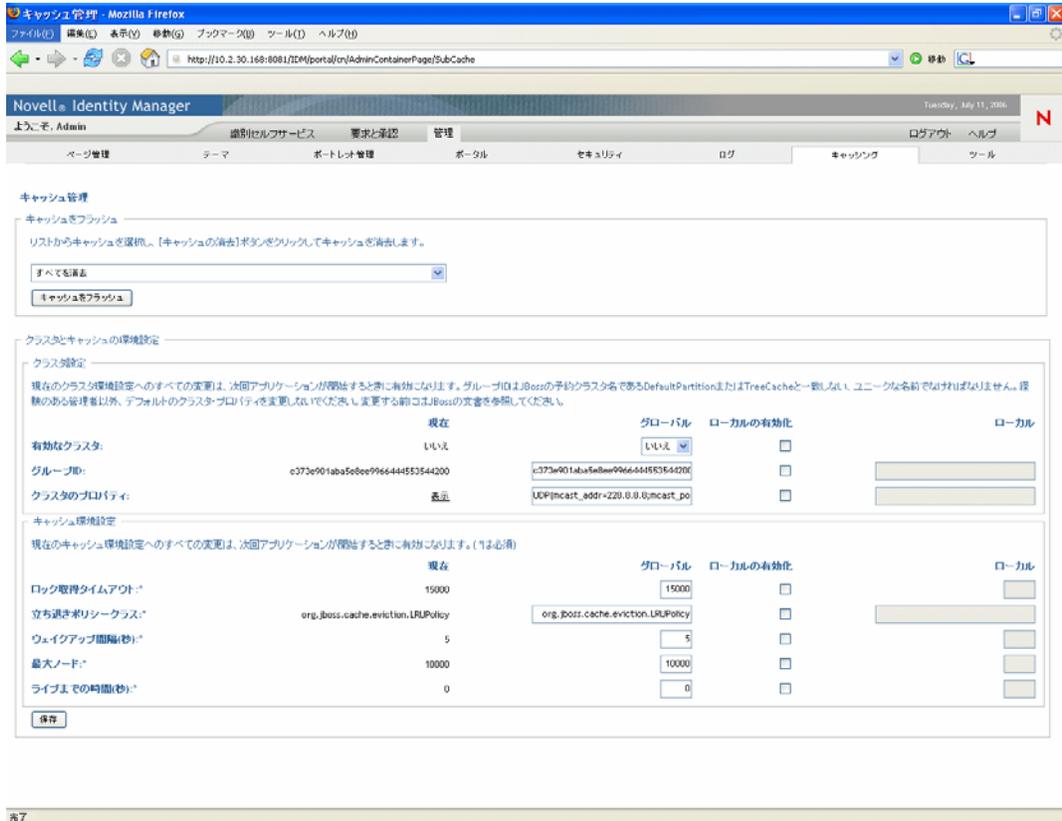
13.2 キャッシュのフラッシュ

キャッシュは Identity Manager ユーザアプリケーションでそのキャッシュを使用するサブシステムに基づいて名前が付けられます。通常は、データの使用頻度またはソースデータの変更頻度に基づいてユーザアプリケーションが自動的にキャッシュをフラッシュするた

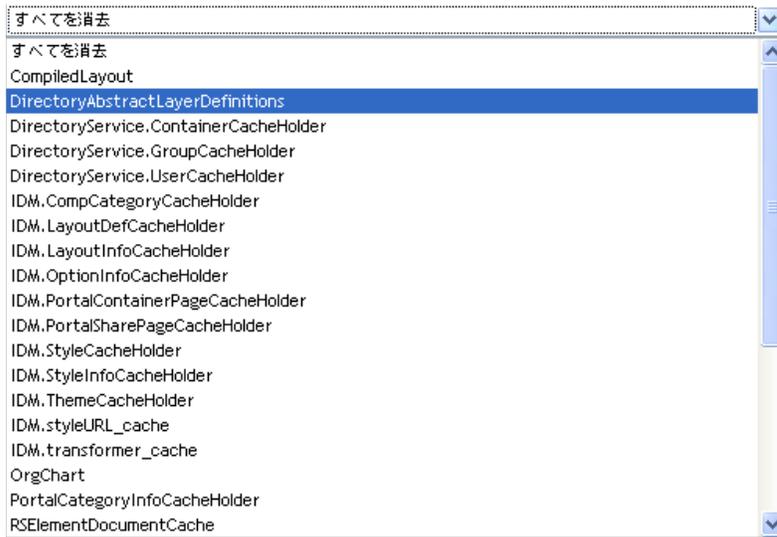
め、ユーザが自らキャッシュをフラッシュする必要はありません。ただし、特別に必要な場合は、選択したキャッシュまたはすべてのキャッシュを手動でフラッシュできます。

キャッシュをフラッシュするには：

- 1 [キャッシュ] ページに移動します。



- ページの [キャッシュをフラッシュ] セクションで、ドロップダウンメニューからフラッシュ対象のキャッシュを選択します (または [すべてを消去] を選択します)。



使用可能なキャッシュのリストは、動的なリストです。その時点でキャッシングされているデータに従って動的に変わる点に注意してください。

- [キャッシュをフラッシュ] ボタンをクリックします。

13.2.1 ディレクトリ抽象化レイヤキャッシュのフラッシュ

ユーザアプリケーションのディレクトリ抽象化レイヤにもキャッシュが存在します。すべてのデータモデル操作でパフォーマンスを最適化するため、`DirectoryAbstractLayerDefinitions` キャッシュではアプリケーションサーバ上に抽象化レイヤ定義を格納します。

通常、ユーザアプリケーションは、`DirectoryAbstractLayerDefinitions` キャッシュと、アイデンティティポータルに格納されている抽象化レイヤ定義との同期を自動的に行います。ただし、必要に応じて、最新定義を強制的にアイデンティティポータルからロードさせるために、(上述した方法で)`DirectoryAbstractLayerDefinitions` キャッシュを手動でフラッシュすることもできます。

ユーザアプリケーションのディレクトリ抽象化レイヤの詳細については、[75 ページの第 4 章「ディレクトリ抽出化レイヤの設定」](#)を参照してください。

13.2.2 クラスタ内のキャッシュのフラッシュ

クラスタアプリケーションサーバ環境および非クラスタアプリケーションサーバ環境のいずれでも、キャッシュのフラッシュはサポートされています。アプリケーションサーバがクラスタの一部である場合に手動でキャッシュをフラッシュすると、クラスタ内にあるすべてのサーバのキャッシュも自動的にフラッシュされます。

13.3 キャッシュを設定する

[キャッシング] ページを使用して、クラスタアプリケーションサーバ環境または非クラスタアプリケーションサーバ環境のキャッシュ環境設定を表示または変更できます。変更

はただちに保存されますが、次回ユーザアプリケーションが再起動されるまで有効になりません。

ヒント：ユーザアプリケーションを再起動するには、アプリケーションサーバの再起動、アプリケーションの再展開 (WAR が変更されている場合)、アプリケーションの強制的な再起動 (アプリケーションサーバのマニュアルに記載されている方法による) のいずれかを行います。

キャッシュを設定するには、次について理解する必要があります。

- ◆ 222 ページのセクション 13.3.1 「キャッシングの実装について」
- ◆ 222 ページのセクション 13.3.2 「キャッシュ設定の保存について」
- ◆ 224 ページのセクション 13.3.3 「キャッシュ設定の表示について」
- ◆ 224 ページのセクション 13.3.4 「基本キャッシュ設定」
- ◆ 226 ページのセクション 13.3.5 「クラスタのキャッシュ設定」

13.3.1 キャッシングの実装について

Identity Manager ユーザアプリケーションでは、キャッシングは JBoss Cache により実装されます。JBoss Cache は、JBoss Application Server に含まれているオープンソースのキャッシングアーキテクチャであり、他のアプリケーションサーバでも実行できます。

JBoss Cache の詳細については、www.jboss.org/products/jboss-cache (<http://www.jboss.org/products/jboss-cache>) を参照してください。

13.3.2 キャッシュ設定の保存について

キャッシュ環境設定を制御するための設定には 2 つのレベルがあります。これら 2 つのレベルの設定を使用して、Identity Manager ユーザアプリケーションのキャッシング動作をカスタマイズできます。

レベル	説明
グローバル設定	<p>グローバル設定は、複数のアプリケーションサーバが同じ設定値を使用できるように、まとめてアイデンティティポルトに格納されます。たとえば、アプリケーションサーバがクラスタになっている場合、通常、クラスタ環境設定のグローバル設定値が使用されます。</p> <p>アイデンティティポルトからグローバル設定を見つけるには、Identity Manager ユーザアプリケーションドライバの下にある次のオブジェクトを探します。</p> <pre data-bbox="516 583 1008 611">configuration.AppDefs.AppConfig</pre> <p>例：</p> <pre data-bbox="516 768 1279 825">configuration.AppDefs.AppConfig.MyUserApplicationDriver.MyDriverSet.MyOrg</pre> <p>環境設定オブジェクトの XmlData 属性には、グローバル設定データが含まれています。</p>
ローカル設定	<p>ローカル設定は、各サーバが 1 つまたは複数のグローバル設定の値を上書きできるように、各アプリケーションサーバに個別に保存されます。たとえば、アプリケーションサーバをグローバル設定で指定したクラスタから削除したり、サーバを別のクラスタに再割り当てしたりする場合に、ローカル設定を指定できます。</p> <p>アプリケーションサーバからローカル設定を見つけるには、JBoss サーバ環境設定の conf ディレクトリの下にある次のファイルを探します。</p> <pre data-bbox="516 1262 976 1289">sys-configuration-xmldata.xml</pre> <p>例：</p> <pre data-bbox="516 1440 1149 1497">jboss/server/IDM/conf/sys-configuration-xmldata.xml</pre> <p>サーバがローカル設定になっている場合、そのデータはこのファイルに含まれます (ローカル設定が指定されていない場合、このファイルは存在しません)。</p>

グローバル設定は、ユーザアプリケーションドライバの特定のインスタンスを使用する各アプリケーションサーバのデフォルト値と考えます。グローバル設定の変更は、サーバが個別にローカル上書きを指定している場合を除き、次回ユーザアプリケーションの再起動時に、各サーバに反映されます。

13.3.3 キャッシュ設定の表示について

[キャッシング] ページでは、現在の (最後にユーザアプリケーションを再起動してからの) キャッシュ設定が表示されます。また、これらの設定に対応するグローバル値およびローカル値も表示され、設定を変更することもできます (変更された設定は、次回ユーザアプリケーションの再起動時から有効になります)。

クラスとキャッシュの環境設定				
クラス別設定				
現在のクラス環境設定へのすべての変更は、次回アプリケーションが開始するときに有効になります。グループIDはJBossの予約クラス名であるDefaultPartitionまたはTreeCacheと一致しない、ユニークな名前であればなりません。経験のある管理者以外、デフォルトのクラスプロパティを変更しないでください。変更する前にはJBossの文書を参照してください。				
	現在	グローバル	ローカルの有効化	ローカル
有効なクラス:	いいえ	<input type="text" value="いいえ"/>	<input type="checkbox"/>	<input type="text"/>
グループID:	c373e901aba5e8ee9966444553544200	<input type="text" value="c373e901aba5e8ee9966444553544200"/>	<input type="checkbox"/>	<input type="text"/>
クラスのプロパティ:	表示	<input type="text" value="UDP(mcast_addr=228.8.8;mcast_po"/>	<input type="checkbox"/>	<input type="text"/>

キャッシュ環境設定				
現在のキャッシュ環境設定へのすべての変更は、次回アプリケーションが開始するときに有効になります。(*は必須)				
	現在	グローバル	ローカルの有効化	ローカル
ロック取得タイムアウト:*	15000	<input type="text" value="15000"/>	<input type="checkbox"/>	<input type="text"/>
立ち退きポリシークラス:*	org.jboss.cache.eviction.LRUPolicy	<input type="text" value="org.jboss.cache.eviction.LRUPolicy"/>	<input type="checkbox"/>	<input type="text"/>
ウェイクアップ間隔(秒):*	5	<input type="text" value="5"/>	<input type="checkbox"/>	<input type="text"/>
最大ノード:*	10000	<input type="text" value="10000"/>	<input type="checkbox"/>	<input type="text"/>
ライブまでの時間(秒):*	0	<input type="text" value="0"/>	<input type="checkbox"/>	<input type="text"/>

グローバル設定では、値の設定が必須です。ローカル設定はオプションです。

13.3.4 基本キャッシュ設定

次のキャッシュ設定は、クラスタアプリケーションサーバ環境および非クラスタアプリケーションサーバ環境の両方に適用されます。

基本キャッシュ設定を設定するには：

- 1 [キャッシング] ページに移動します。
- 2 [キャッシュ環境設定] セクションで、必要に応じて、次の設定のグローバル値またはローカル値を指定します。

設定	操作
ロック取得タイムアウト	オブジェクトでロックが取得されるまでキャッシュが待機する間隔 (ミリ秒) を指定します。ユーザアプリケーションのアプリケーションログに大量のロックタイムアウト例外が書き込まれる場合に、この設定値を増やすことができます。デフォルトは 15000 ミリ秒です。

設定	操作
立ち退きポリシークラス	<p>使用するキャッシュ立ち退きポリシーのクラス名を指定します。デフォルトは、JBoss Cache が提供する LRU 立ち退きポリシーです。</p> <pre>org.jboss.cache.eviction.LRUPolicy</pre> <p>この設定は、必要に応じて、JBoss Cache がサポートする別の立ち退きポリシーに変更できます。</p> <p>サポート対象の立ち退きポリシーについては、www.jboss.org/products/jboss-cache (http://www.jboss.org/products/jboss-cache) を参照してください。</p>
ウェイクアップ間隔 (秒)	<p>次の動作を実行するためにキャッシュ立ち退きポリシーがウェイクアップするまでの待機間隔 (秒) を指定します。</p> <ul style="list-style-type: none"> 立ち退きノードイベントの処理 サイズ制限および期限切れノードのクリーンアップ
最大ノード	<p>キャッシュで許容される最大ノード数を指定します。無制限の場合は、次の値を指定します。</p> <p>0</p>
ライブまでの時間 (秒)	<p>ノードが一扫されるまでのアイドル時間 (秒) を指定します。無制限の場合は、次の値を指定します。</p> <p>0</p>

これらの設定は必須です。各設定にはグローバル値を指定する必要があり、ローカル値もオプションで使用される場合があります。

設定のグローバル値をローカル値で上書きする場合は、その設定の [ローカルの有効化] チェックボックスをオンにしてから、ローカル値を指定します。ローカル値がすべて有効であることを確認してください。有効な値でない場合、変更を保存できません。

注: [ローカルの有効化] チェックボックスがオフになっている設定は、保存時、既存のローカル値が削除されます。

- [保存] をクリックします。
- 保存した設定を反映できる状態になったら、該当アプリケーションサーバ上でユーザーアプリケーションを再起動します。

13.3.5 クラスタのキャッシュ設定

この節では、Identity Manager ユーザアプリケーションをクラスタアプリケーションサーバ間で実行する場合のキャッシングの設定方法について説明します。次について理解する必要があります。

- ◆ 226 ページのセクション「クラスタリングの実装について」
- ◆ 226 ページの「クラスタでのキャッシングの動作について」
- ◆ 226 ページの「クラスタを使用するための準備作業」
- ◆ 227 ページの「クラスタのキャッシュを設定する」

クラスタリングの実装について

Identity Manager ユーザアプリケーションでは、キャッシングのクラスタサポートは JGroups により実装されます。JGroup は、JBoss Application Server に含まれているオープンソースのクラスタリングアーキテクチャであり、他のアプリケーションサーバでも実行できます。

ユーザアプリケーションのクラスタは、JGroups を実行し、共通のグループ ID を使用するネットワーク上のノードから構成されます。デフォルトでは、ユーザアプリケーションのクラスタに用意されているグループ ID は、次のような UUID となります。

```
c373e901aba5e8ee9966444553544200
```

UUID により一意性が保たれるため、ユーザアプリケーションのクラスタのグループ ID が環境内にある他のクラスタのグループ ID と競合することはありません。たとえば、JBoss Application Server では、2 つの JGroups クラスタが使用され、それぞれ対応するグループ ID である DefaultPartition と TreeCache は予約されています。

JGroups の詳細については、www.jboss.org/products/jgroups (<http://www.jboss.org/products/jgroups>) を参照してください。

クラスタでのキャッシングの動作について

ユーザアプリケーションを起動すると、アプリケーションのキャッシュ設定により、クラスタに参加してキャッシュ変更をクラスタ内の他のノードに複製するかどうか判断されます。クラスタリングが有効になっている場合、ユーザアプリケーションは、変更発生時にキャッシュエントリ無効メッセージを各ノードに送信することにより、この複製を実行します。

クラスタを使用するための準備作業

クラスタでキャッシングを使用するには、2 つの主な手順を実行する必要があります。

1 JGroups クラスタの設定

ここでは、すべての環境設定を使用するための JBoss Application Server をインストールし、それからクラスタ内の各サーバに Identity Manager ユーザアプリケーション (IDM.war) を配布します。Identity Manager ユーザアプリケーション (IDM.war) は通常、farm ディレクトリに配置されます。

2 ユーザアプリケーションのキャッシュ環境設定におけるクラスタ使用の有効化

次に示す 227 ページの「クラスタのキャッシュを設定する」を参照してください。

クラスタのキャッシュを設定する

クラスタを使用できる状況になったら、クラスタのキャッシング設定を指定します。

クラスタのキャッシュを設定するには：

- 1 [キャッシング] ページに移動します。
- 2 [クラスタ設定] セクションで、必要に応じて、次の設定のグローバル値またはローカル値を指定します。

設定	操作
有効なクラスタ	グループ ID により指定されたクラスタ内の別のノードにキャッシュの変更を複製する場合は、[True] を選択します。クラスタに参加しない場合は、[False] を選択します。
グループ ID	参加対象の JGroups クラスタのグループ ID を指定します。通常は、ユーザアプリケーションクラスタ用に用意されているグループ ID のデフォルト値を変更する必要はありません。ただし、別のクラスタを使用する場合は変更します。 DefaultPartition および TreeCache というグループ ID は、JBoss Application Server が使用するために予約されています。 ヒント：グループ ID をログメッセージに表示する場合は、キャッシングログ (com.sssw.fw.cachemgr) のレベルが「情報」以上になっていることを確認します。
クラスタのプロパティ	グループ ID により指定されたクラスタの JGroups プロトコルスタックを指定します。この設定は、クラスタのプロパティ調整の必要が想定される経験のある管理者のためのものです。経験のある管理者以外は、デフォルトのプロトコルスタックを変更しないでください。 現在のクラスタのプロパティを表示するには、[表示] をクリックします。 JGroups プロトコルスタックの詳細については、 www.jboss.org/wiki/Wiki.jsp?page=JGroups (http://www.jboss.org/wiki/Wiki.jsp?page=JGroups) を参照してください。

設定のグローバル値をローカル値で上書きする場合は、その設定の [ローカルの有効化] チェックボックスをオンにしてから、ローカル値を指定します。

注：[ローカルの有効化] チェックボックスがオフになっている設定は、保存時、既存のローカル値が削除されます。

クラスタ内のすべてのノードの [グループ ID] および [クラスタのプロパティ] が同じ設定になっていることを確認します。特定のノードについてこれらの設定を確認する場合には、そのサーバ上のユーザインタフェースの URL を参照することにより、そのノードを実行している Identity Manager ユーザインタフェースにアクセスし、それから [キャッシング] ページを表示する必要があります。

- 3 [保存] をクリックします。

- 4 保存した設定を反映できる状態になったら、該当アプリケーションサーバ上でユーザアプリケーションを再起動します。

ポータルデータのエクスポートおよびインポートのためのツール

この章では、Identity Manager ユーザインタフェースの [管理] タブの [ツール] ページを使用する方法について説明します。ここで取り扱う内容は次のとおりです。

- ◆ 229 ページのセクション 14.1 「ポータルデータのエクスポートおよびインポートについて」
- ◆ 231 ページのセクション 14.2 「ポータルデータのエクスポート」
- ◆ 232 ページのセクション 14.3 「ポータルデータのインポート」

[管理] タブにアクセスして操作する一般的な情報については、131 ページの第 6 章「[管理] タブの使用」を参照してください。

14.1 ポータルデータのエクスポートおよびインポートについて

[ツール] ページを使用して、Identity Manager ユーザアプリケーションが使用するポータルコンテンツ (ページおよびポートレット) のエクスポートまたはインポートを実行できます。このコンテンツは「ポータル環境設定状態」とも呼ばれ、次の内容が含まれます。

- ◆ コンテナページおよび共有ページ (各ページの割り当て済みポートレット、各ポートレットの初期設定およびその他設定など)
- ◆ ポートレット登録

エクスポートおよびインポートのためのツールを使用すると、必要に応じて、1 つのポータル (ユーザアプリケーション) から別のポータルにポータル環境設定状態を移動できます。各ツールの機能は次のとおりです。

ツール	機能
ポータルデータエクスポート	選択したコンテナページ、共有ページ、およびポートレットの XML 記述を生成します。XML ファイルは、ポータルデータエクスポートの ZIP ファイル内に格納され、ポータルデータインポートツールへの入力データとして使用できます。
ポータルデータインポート	ポータルデータエクスポートの ZIP ファイルを入力データとして受け取ります。ポータルデータエクスポートの ZIP ファイルを使用して、ポータル (ユーザアプリケーション) 内にコンテナページ、共有ページ、およびポートレットを生成します。

14.1.1 用途

ポータルデータエクスポートツールとポータルデータインポートツールは、次の用途に使用できます。

- ◆ テスト (ソース) 環境から運用 (ターゲット) 環境に、ポータル環境設定状態を移行する
- ◆ ポータル環境設定状態の変更部分を更新する

- ◆ ポータルをクローン複製する
- ◆ (オプション) ターゲットポータルの環境設定状態を上書きする

14.1.2 要件

ポータルデータエクスポートツールおよびポータルデータインポートツールを使用するには、ソースおよびターゲットのアプリケーションサーバ上で、Identity Manager ユーザアプリケーション (ポータル) が展開および実行されている必要があります。

ソースサーバとターゲットサーバが同じアイデンティティポータルにアクセスしている必要はありません。適切であれば、異なるアイデンティティポータルにアクセスしていても問題ありません。アイデンティティポータル内のユーザ、グループおよびコンテナが同じである必要もありません。

14.1.3 制限

ポータルデータエクスポートツールおよびポータルデータインポートツールは、次の用途には使用できません。

- ◆ サーバがユーザ要求の処理中にポータル環境設定状態のエクスポートまたはインポートを行う
- ◆ ポータルのクラスおよびリソースをエクスポートまたはインポートする
- ◆ ポートレットのクラスおよびリソースをエクスポートまたはインポートする
- ◆ ポータルで使用されている識別データおよびプロビジョニングデータをエクスポートおよびインポートする
- ◆ ページおよびポートレット以外の管理設定をエクスポートおよびインポートする
- ◆ 古いバージョンのポータルから新しいバージョンのポータルへの環境設定状態を移行する (ポータルは同じバージョンで行う必要があります)

14.1.4 手順

ポータルデータをエクスポートおよびインポートするには：

- 1 増分更新を行う場合には、ターゲットポータルのバックアップを作成します。
- 2 ソースポータルから、ポータルデータエクスポートツールを使用して、ポータルデータをエクスポートします。
231 ページのセクション 14.2 「ポータルデータのエクスポート」 を参照してください。
- 3 ターゲットポータルから、ポータルデータインポートツールを使用して、ターゲットポータルにポータルデータをインポートします。
232 ページのセクション 14.3 「ポータルデータのインポート」 を参照してください。
- 4 ターゲットポータルに目的のデータがインポートされていることを確認します。

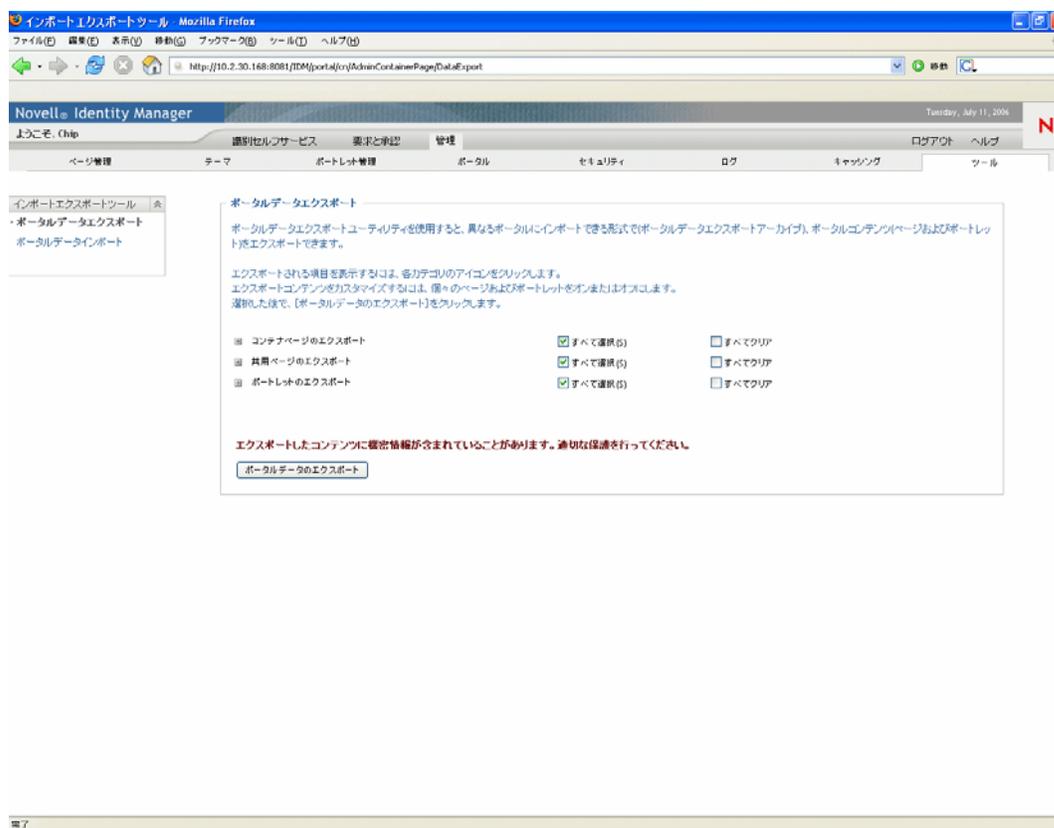
14.2 ポータルデータのエクスポート

この節では、ポータル環境設定状態をポータルデータエクスポートの ZIP ファイルにエクスポートする方法について説明します。

ポータルデータをエクスポートするには：

- 1 [ツール] ページで、左側のナビゲーションメニューから [ポータルデータエクスポート] を選択します。

[ポータルデータエクスポート] パネルが表示されます。



- 2 画面の指示に従い、エクスポートするポータルページおよびポートレットを選択します。

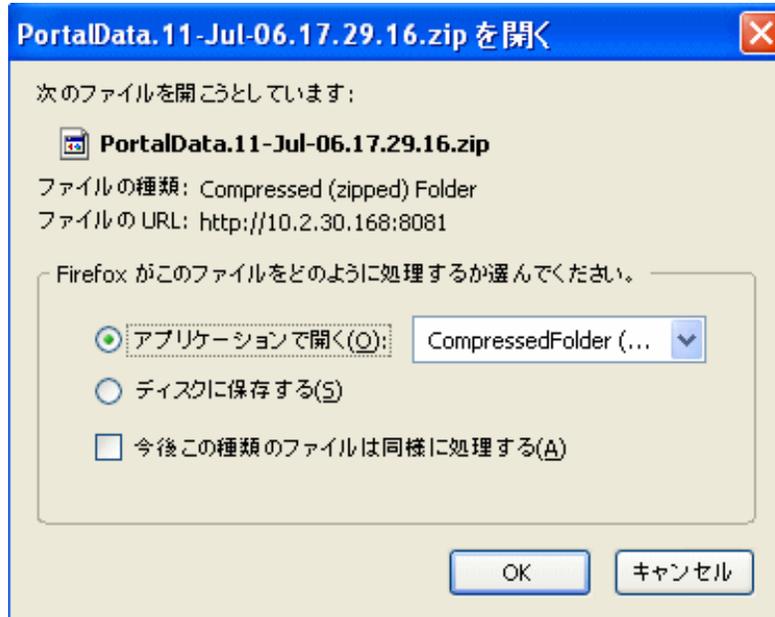
注：エクスポート対象として選択しなかったポートレットがエクスポートされる場合があります。ポートレットを含むページをエクスポートする場合、そのポートレットをエクスポート対象として含めない場合も、エクスポートされたページについてランタイムエラーが発生しないことを確認するためポートレットがエクスポートされます。

- 3 選択が完了したら、[ポータルデータのエクスポート] ボタンをクリックします。

新しいポータルデータエクスポートの ZIP ファイルが作成され、現在の日付および時刻を含むデフォルトの名前が付けられます。次に例を示します。

PortalData.21-Oct-05.09.12.16.zip

この ZIP ファイルをローカルに保存する (または適切なアーカイブユーティリティで開く) ように要求するメッセージが表示されます。次に例を示します。



- 4 ポータルデータエクスポートの ZIP ファイルを適切な場所に保存します。

14.3 ポータルデータのインポート

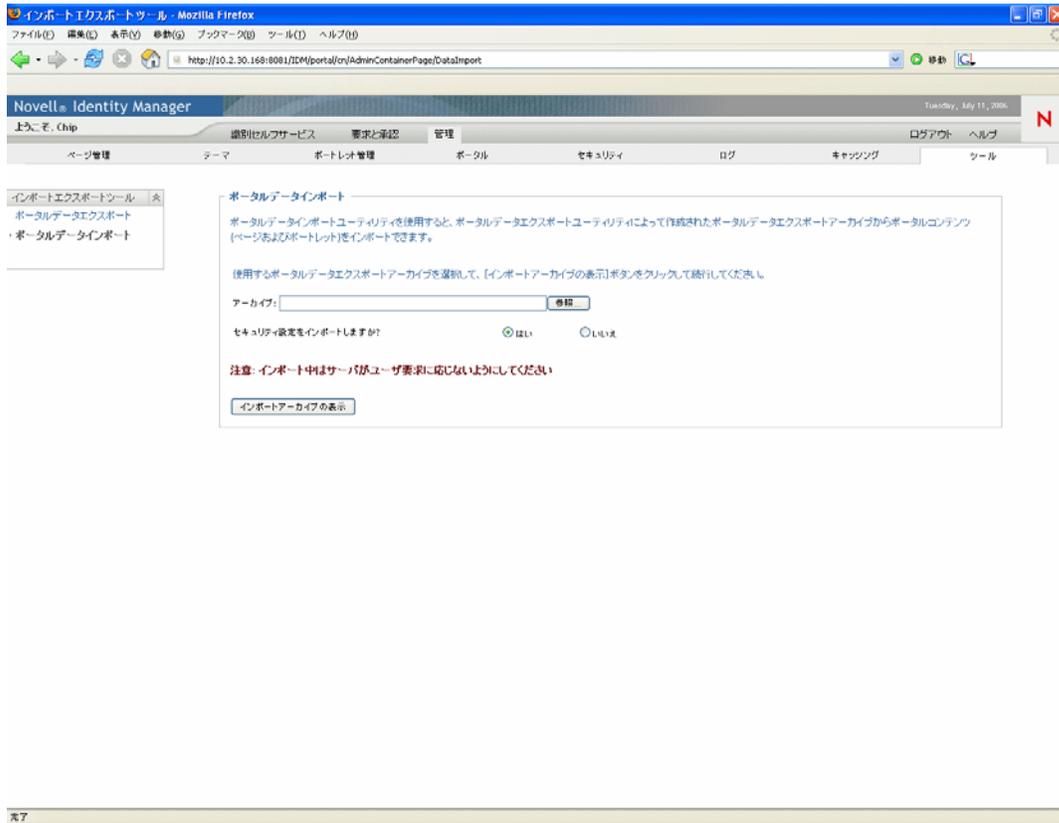
この節では、ポータルデータエクスポートの ZIP ファイルをポータルにインポートする方法について説明します。

注: インポート中は、ターゲットアプリケーションサーバが実行していて、ユーザ要求を処理していないことが必要です。

ポータルデータをインポートするには:

- 1 [ツール] のページで、左側のナビゲーションメニューから [ポータルデータインポート] を選択します。

[ポータルデータインポート] パネルが表示されます。



2 次の基本インポート設定を指定します。

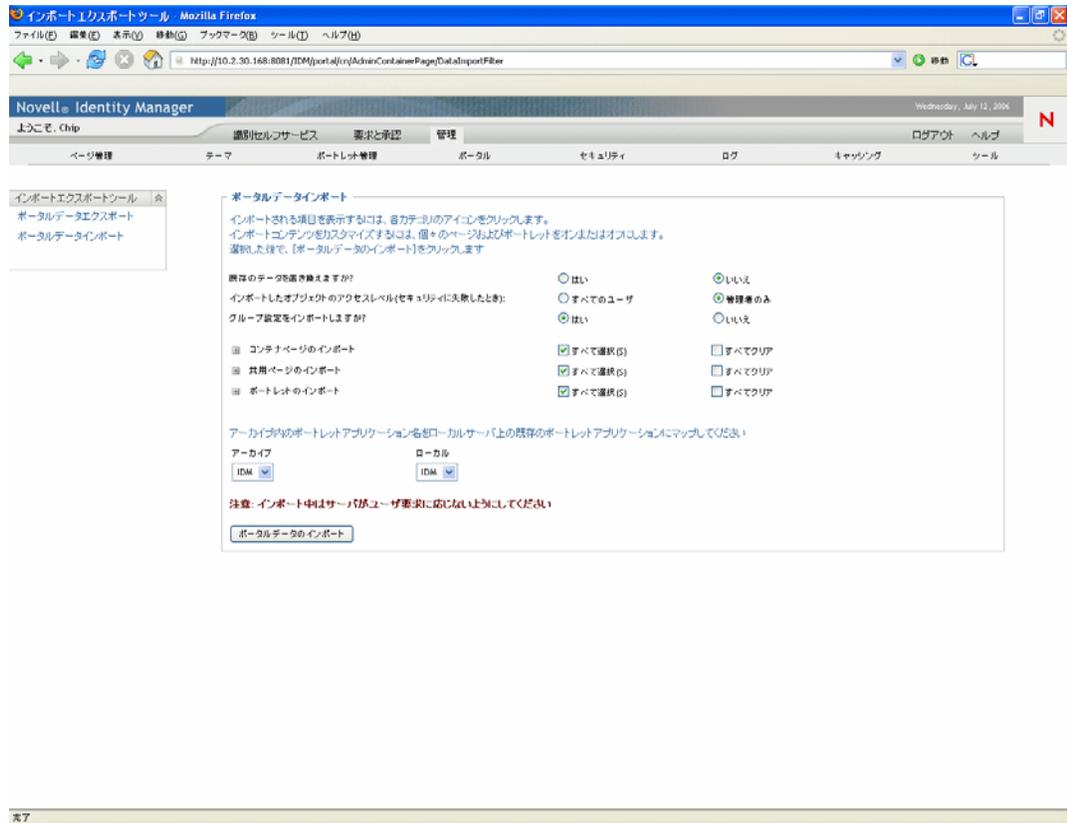
設定	操作
アーカイブ	[参照] ボタンをクリックし、インポートするポータルデータエクスポートの ZIP ファイルを選択します。次に例を示します。 PortalData.21-Oct-05.09.12.16.zip

セキュリティ設定をインポートしますか? 次のいずれかを選択します。

- ◆ はい — ポータルデータエクスポートの ZIP ファイルで指定されている、ページおよびポートレットに対するユーザ、グループ、およびコンテナのアクセス権をインポートする場合。関連するユーザ、グループ、およびコンテナがターゲットポータルアイデンティティポータルに存在することを確認してください。存在しないエンティティの許可はインポートできません。
- ◆ いいえ — ポータルデータエクスポートの ZIP ファイルが指定する許可を無視する場合。

3 [インポートアーカイブの表示] ボタンをクリックします。

このパネルには、選択したポータルデータエクスポートの ZIP ファイルについての詳細情報とインポート方法が表示されます。



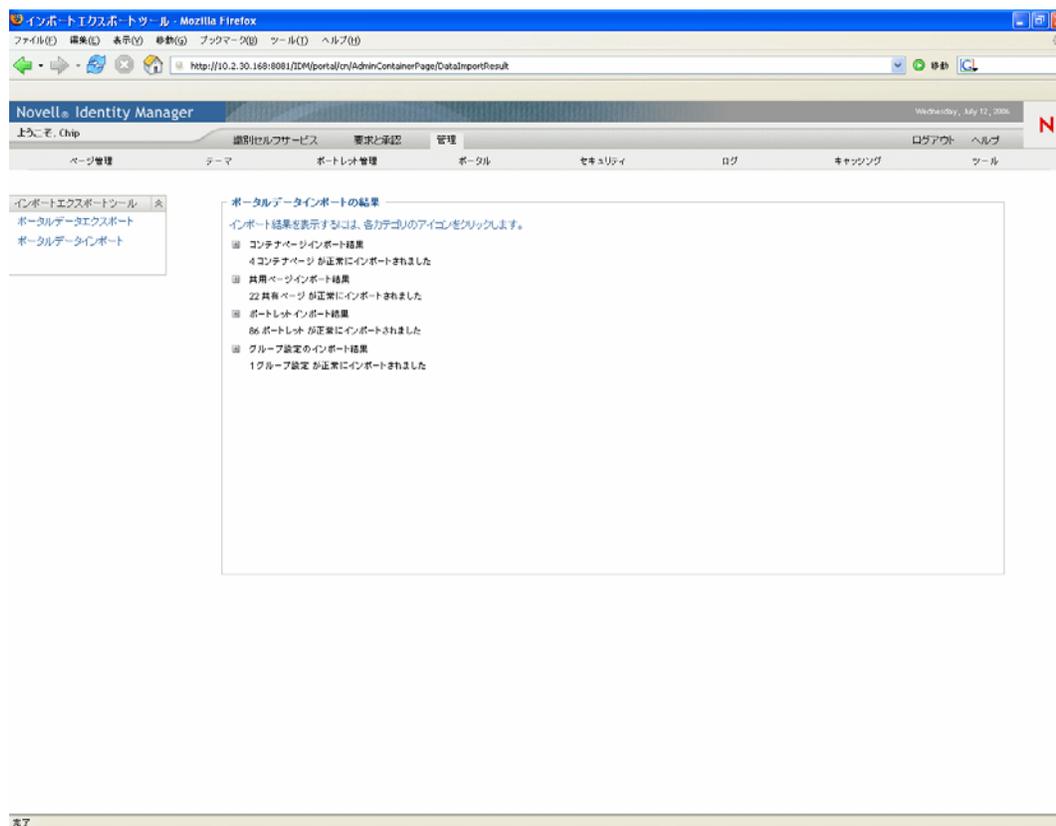
4 次の詳細インポート設定を指定します。

設定	操作
既存のデータを置き換えますか？	次のいずれかを選択します。 <ul style="list-style-type: none">はい — ターゲットポータルにすでに存在するページおよびポートレットの内容を、ポータルデータエクスポートの ZIP ファイル内の対応する内容で上書きする場合。たとえば、ポータルデータエクスポートの ZIP ファイルに MyPage という名前の共有ページがあり、ターゲットポータルにも MyPage という名前の共有ページがある場合、ターゲットポータルの既存のページは上書きされます。いいえ — 既存のページおよびポートレットすべてについて、インポートをスキップする場合。

設定	操作
<p>インポートしたオブジェクトのアクセスレベル</p>	<p>次のいずれかを選択します。</p> <ul style="list-style-type: none"> ◆ すべてのユーザ — インポートされたページおよびポートレットへのアクセスを制限しない場合。 ◆ 管理者のみ — インポートされたページおよびポートレットへのアクセスを制限する場合。 <p>セキュリティ設定のインポートを選択した場合、このアクセスレベルは、セキュリティ設定をインポートできなかった、インポートされたページおよびポートレットについてのみ適用されます (通常、指定したユーザ、グループ、コンテナはターゲットポータルアイデンティティポータルに存在しないため)。</p> <p>セキュリティ設定のインポートを選択しなかった場合、このアクセスレベルは、インポートされたページおよびポートレットすべてに適用されます。</p>
<p>グループ設定をインポートしますか？</p>	<p>セキュリティ設定のインポートを選択した場合、次のいずれかを選択します。</p> <ul style="list-style-type: none"> ◆ はい — ポータルデータエクスポートの ZIP ファイルで指定される、グループのコンテナページと共有ページのデフォルト割り当てをインポートする場合。関連するグループがターゲットポータルアイデンティティポータルに存在することを確認してください。存在しないグループの割り当てはインポートできません。 ◆ いいえ — ポータルデータエクスポートの ZIP ファイルがグループについて指定するデフォルトのページ割り当てを無視する場合。
<p>コンテナページのインポート 共有ページのインポート ポートレットのインポート</p>	<p>画面の指示に従い、ポータルデータエクスポートの ZIP ファイルからターゲットポータルにインポートするページおよびポートレットを選択します。</p> <hr/> <p>注：インポート対象として選択しなかったポートレットがインポートされる場合があります。ポートレットを含むページをインポートする場合、そのポートレットをインポート対象に含めない場合も、インポートされたページについてランタイムエラーが発生しないことを確認するため、ポートレットがインポートされます。</p>
<p>Please map the portlet application names... Archive/Local (アーカイブ内のポートレットアプリケーション名をローカルサーバ上の既存のポートレットアプリケーションにマップしてください アーカイブ / ローカル)</p>	<p>[アーカイブ] ドロップダウンメニューおよび [ローカル] ドロップダウンメニューを使用して、アーカイブ (ポータルデータエクスポートの ZIP ファイル) 内のポートレットアプリケーション名を、ローカル (ターゲット) アプリケーションサーバ上の既存のポートレットアプリケーションにマップします。</p>

- 5 インポートを開始できる準備が整ったら、[ポータルデータのインポート] ボタンをクリックします。

インポートが完了すると、[ポータルデータインポートの結果] パネルが表示されます。



失敗したインポートは赤く表示されます。インポート (またはエクスポート) に関する問題をトラブルシューティングするには、アプリケーションサーバのシステムコンソールまたはログファイル (jboss/server/IDM/log/server.log など) を確認し、次のユーザアプリケーションログからのメッセージを探します。

```
com.novell.afw.portal.util
```

ポートレット参照

IV

次の章では、Identity Manager ユーザインタフェースで使用される識別ポートレットおよびシステムポートレットを設定する方法について説明します。

- ◆ 239 ページの第 15 章「ポートレットについて」
- ◆ 243 ページの第 16 章「作成ポートレットの参照先」
- ◆ 251 ページの第 17 章「詳細ポートレットの参照」
- ◆ 265 ページの第 18 章「組織図ポートレットの参照」
- ◆ 281 ページの第 19 章「パスワード管理ポートレットの参照」
- ◆ 295 ページの第 20 章「リスト検索ポートレットの参照」

ポータルレットについて

この章では、Identity Manager ユーザアプリケーションで使用するポータルレットについて説明します。ここで取り扱う内容は次のとおりです。

- ◆ 239 ページのセクション 15.1 「アクセサリポータルレット」
- ◆ 239 ページのセクション 15.2 「管理ポータルレット」
- ◆ 240 ページのセクション 15.3 「識別ポータルレット」
- ◆ 241 ページのセクション 15.4 「パスワードポータルレット」
- ◆ 241 ページのセクション 15.5 「システムポータルレット」

ポータルレットの管理の詳細については、181 ページの第 9 章「ポータルレットの管理」を参照してください。

15.1 アクセサリポータルレット

アクセサリポータルレットは、Identity Manager ユーザアプリケーションに追加できるさまざまな機能のセットを提供します。アクセサリポータルレットは、電子メール、ファイルシステムなどの機能を提供します。詳細については、次を参照してください。

ポータルレットのカテゴリ	参照先
E-mail (電子メール)	『Identity Manager Accessory Portlet Administration Guide』を参照してください。
File System (ファイルシステム)	
Miscellaneous (その他)	

15.2 管理ポータルレット

管理ポータルレットは、ユーザインタフェースのレイアウトおよびコンテンツの制御に使用します。

注: 管理ポータルレットは使用したり、変更したりしないようにしてください。管理ポータルレットは、ユーザアプリケーションにフレームワークサービスを提供するものです。

次のような管理ポータルレットがあります。

ポータルレット名	説明
ヘッダポータルレット	ユーザインタフェースのヘッダ情報およびトップレベルのタブコントロールが表示されます。 このポータルレットに初期設定はありません。

ポートレット名	説明
共有ページナビゲーション	<p>Identity Manager ユーザアプリケーションの共有ページを含むメニューを表示します。</p> <p>初期設定は、表示内容および表示方法を定義します。</p> <p>240 ページのセクション 15.2.1 「共有ページナビゲーションポートレット」を参照してください。</p>

15.2.1 共有ページナビゲーションポートレット

共有ページナビゲーションポートレットは、Identity Manager ユーザアプリケーションの共有ページへのリンクを生成します。初期設定が、表示する共有ページリンクを定義します。初期設定には、次のものが含まれます。

初期設定	指定する内容
sharedpages-sorting	共有ページがカテゴリ内で表示される順序を指定します。「昇順」または「降順」のいずれかです。
sharedpages-sortmode	共有ページのソート順を指定します。「アルファベット順」または「優先度」のいずれかです。
sharedpages-category	共有ページの 1 つまたは複数のカテゴリを指定します。 カテゴリ名はヘッダとして表示され、そのカテゴリにあるすべての共有ページはリンクとして表示されます。カテゴリに共有ページがない場合は表示されません。カテゴリにない共有ページは、カテゴリ未分類として表示されます。
guest-category	ポータル待ち受けページに表示するポートレットの属するカテゴリを指定します。これは、既存のカテゴリである必要があります。このカテゴリに含まれるページについては、ACL 読み込み制約があってはなりません。

15.3 識別ポートレット

識別ポートレットは、Identity Manager ユーザアプリケーションの [識別セルフサービス] タブで使用されます。次に詳しく示します。

ポートレット名	説明
作成	<p>アイデンティティポータルにオブジェクトを作成するための、ウィザードベースのインタフェースを提供します。</p> <p>243 ページの第 16 章 「作成ポートレットの参照先」を参照してください。</p>
詳細	<p>エンティティの属性データを表示したり、操作したりすることができます。</p> <p>251 ページの第 17 章 「詳細ポートレットの参照」を参照してください。</p>
組織図	<p>アイデンティティポータルとのオブジェクト間の階層リレーションシップを表示したり、参照したりすることができます。</p> <p>265 ページの第 18 章 「組織図ポートレットの参照」を参照してください。</p>

ポートレット名	説明
リスト検索	アイデンティティポータルにあるオブジェクトを検索できます。 295 ページの第 20 章「リスト検索ポートレットの参照」 を参照してください。

15.4 パスワードポートレット

パスワードポートレットは、パスワードセルフサービス機能を Identity Manager ユーザーアプリケーションに提供します。次に詳しく示します。

ポートレット名	参照先
IDM 本人確認の回答	281 ページの第 19 章「パスワード管理ポートレットの参照」 を参照してください。
IDM パスワードの変更	
IDM パスワードを忘れた場合	
IDM ヒントの設定	
IDM ログイン	

15.5 システムポートレット

システムポートレットは、Identity Manager ユーザーアプリケーションにサービスを提供します。

注：システムポートレットの使用または変更は行わないことをお勧めします。

次のようなシステムポートレットがあります。

ポートレット名	説明
ポータルページコントローラ	ユーザが共有ページナビゲーションポートレットで現在選択している共有ページが表示されます。 このポートレットに初期設定はありません。

作成ポートレットの参照先

16

この章では、Identity Manager ユーザアプリケーションで作成ポートレットを使用する方法について説明します。ここで取り扱う内容は次のとおりです。

- ◆ [243 ページのセクション 16.1「作成ポートレットについて」](#)
- ◆ [245 ページのセクション 16.2「作成ポートレットの設定」](#)
- ◆ [247 ページのセクション 16.3「作成の初期設定の設定」](#)

16.1 作成ポートレットについて

作成ポートレットは、さまざまなタイプのアイデンティティポータルオブジェクトを作成するための、使いやすいウィザードを提供します。ポートレットの初期設定で制御できる内容は、次のとおりです。

- ◆ ユーザが作成できるオブジェクトのタイプ
- ◆ ユーザが指定できる属性

詳細については、[247 ページのセクション 16.3「作成の初期設定の設定」](#)を参照してください。

作成ポートレットのデフォルト設定では、ユーザ、グループ、およびタスクグループを作成できるようになっています(作成ポートレットには、Identity Manager ユーザアプリケーションの [ユーザまたはグループの作成] アクションからアクセスできます)。デフォルトでは、このポートレットの操作はユーザアプリケーション管理者に限定されています。

次の例では、デフォルトの作成ポートレットウィザードがユーザに表示するメッセージの内容を示します。

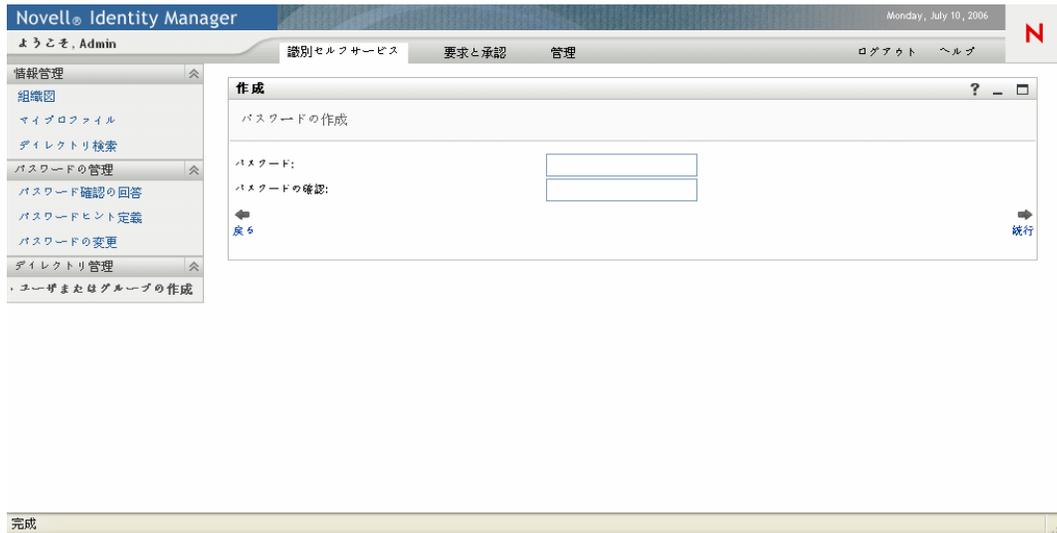
- ◆ 作成するオブジェクトのタイプを選択する：



- ◆ オブジェクトの属性を入力する：



- ◆ 選択したオブジェクトタイプの要求に応じて、パスワードの入力を促すメッセージを表示する：



パスワードポリシーが割り当てられている場合、このポートレットによりカスタムポリシーメッセージが表示されます。

- ◆ オブジェクトの作成に成功すると、情報メッセージが表示され、引き続き編集できるように、そのオブジェクトに対する詳細ポートレットへのリンクも表示されます(詳細ポートレットも同様に設定されている場合)。

16.2 作成ポートレットの設定

作成ポートレットを設定するには、次の手順に従います。

ステップ	タスク	説明
1	デフォルトの「ユーザまたはグループの作成」機能が、要件に一致しているかどうかを判別します	一致する場合は、以降の手順は必要ありません。 一致しない場合は、残りの手順に従う必要があります。
2	ユーザが作成できるオブジェクトのタイプを定義します。	オブジェクトおよび属性をディレクトリ抽象化レイヤに追加します。 詳細については、 75 ページの第 4 章「ディレクトリ抽出化レイヤの設定」 を参照してください。
3	この新しいポートレットにユーザがアクセスできる方法を指定します。	このポートレットを既存ページから起動できるようにするか、新しいページから起動できるようにするか、または、どのユーザをポートレットとページにアクセスできるようにするかについても考慮します。 ページの詳細については、 137 ページの第 7 章「ページの管理」 を参照してください。

ステップ	タスク	説明
4	ページおよびポートレットインスタンスにアクセスできるユーザを指定します。	<p>ページセキュリティを編集し、ユーザをリストに追加します。ページに対するユーザアクセスの制限の詳細については、137 ページの第 7 章「ページの管理」を参照してください。</p> <p>ポートレットインスタンスを編集してセキュリティを変更します。ポートレットに対するユーザアクセスの制限の詳細については、181 ページの第 9 章「ポートレットの管理」を参照してください。</p>
5	ポートレットの初期設定を指定します。	<p>初期設定で定義する内容は次のとおりです。</p> <ul style="list-style-type: none"> ◆ ユーザが作成できるオブジェクト ◆ 作成中に指定する属性 <p>詳細については、247 ページのセクション 16.3「作成の初期設定の設定」を参照してください。</p>
6	テスト	オブジェクトが作成され、属性が適切に指定されていることを確認します。
7	エンドユーザについて、eDirectory における適切な権利を設定します。	オブジェクトを作成するには、ユーザは、オブジェクトが作成される部門および組織のトラスティが割り当て済みである必要があります。

16.2.1 ディレクトリ抽象化レイヤの設定

作成ポートレットのユーザが作成可能なオブジェクト、および指定可能な属性は、ディレクトリ抽象化レイヤで次のように定義する必要があります。

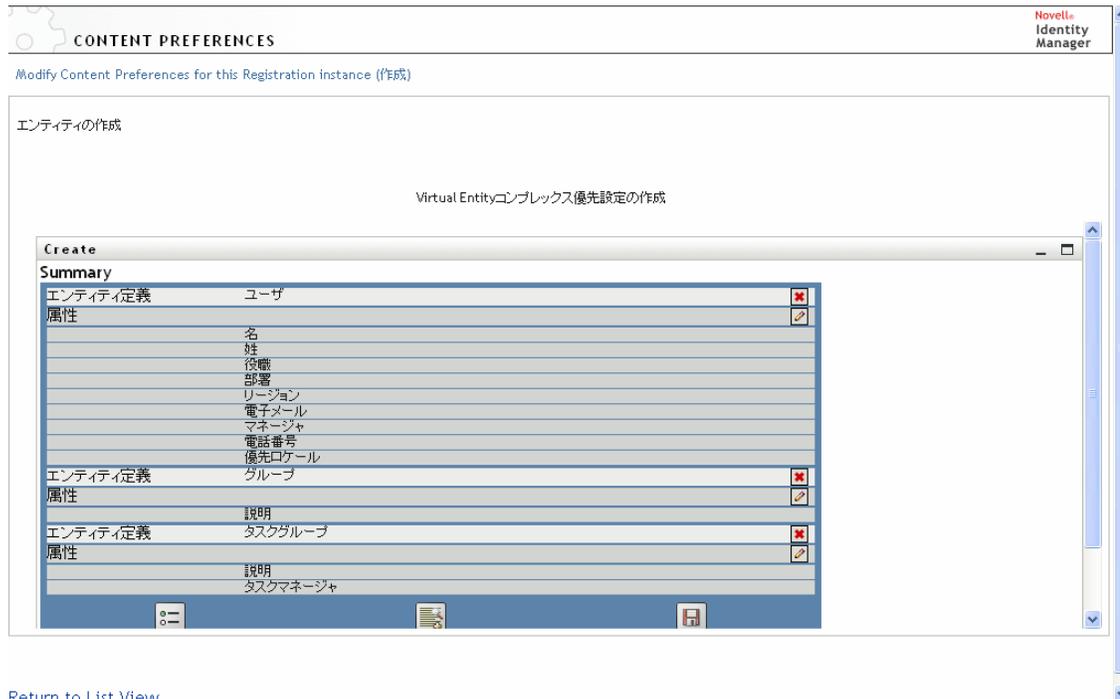
定義タイプ	プロパティ	値
エンティティ	create (作成)	選択
	view (表示)	選択
	Container for Create (作成用コンテナ)	<p>選択しない場合、作成できるエンティティのリストにそのエンティティが表示されません。</p> <p>有効なアイデンティティボールドコンテナを指定します。</p> <p>有効なコンテナが指定されない場合、ユーザアプリケーションのインストール時に指定されたルートコンテナが使用されます。</p>
	password (パスワード)	<p>エンティティタイプが作成時にパスワードを必要とする場合、選択します。</p> <p>作成ポートレットへのアクセス権を持ち、OU のトラスティ権のあるユーザは誰でも、ユーザを作成して初期パスワードを割り当てることができます。新しいユーザの初回ログイン時には、初期パスワードを変更するための IDM パスワードの変更ポートレットにリダイレクトされます。</p> <p>IDM パスワードの変更ポートレットの詳細については、281 ページの第 19 章「パスワード管理ポートレットの参照」を参照してください。</p>
attribute (属性)	enabled (有効)	選択
	表示可	[enabled (有効)] または [viewable (表示可)] を選択しなかった場合、その属性は作成ポートレットで使用できなくなります。

抽象化レイヤの設定の詳細については、[75 ページの第 4 章「ディレクトリ抽出化レイヤの設定」](#)を参照してください。

16.3 作成の初期設定の設定

初期設定を指定することにより、ユーザが作成できるオブジェクトのタイプ、およびユーザが指定可能な、あるいは指定が必要な属性を設定できます。

作成ポートレットの初期設定は、1つのカスタム初期設定ページ内に示されます。このページを開くと、作成ポートレットの初期設定は次のように表示されます。



初期設定は、次のとおりです（「説明」ボタンをクリックすると、このポートレットのオンラインヘルプが表示されます）。

初期設定	説明
エンティティ定義	<p>作成するオブジェクトタイプの名前です。</p> <p>ここから、ポートレットのオブジェクト作成方法を定義するためのエンティティ定義ブロックが開始します。</p> <p>オブジェクトを制限するには：</p> <p>初期設定内のオブジェクトは、ドロップダウンメニューで表示されます。ユーザが作成できるオブジェクトを制限するには、「削除」ボタンを使用して、不要なオブジェクトをこの環境設定シートから削除します。</p> <p>他のエンティティを追加するには：</p> <p>[エンティティ定義の追加] をクリックし、ウィザードの指示に従います。</p>

初期設定	説明
属性	<p>ユーザに入力を促す属性を指定します。オブジェクトに必要な属性はすべて含める必要があります。そうでない場合、実際のオブジェクトの作成が失敗します。また、必須属性が不足している場合は、初期設定を保存できません。</p> <p>属性を追加または削除するには：</p> <ul style="list-style-type: none"> ◆ [Modify Attributes (属性の変更)] ボタンをクリックします。 <div style="text-align: center;">  </div> <ul style="list-style-type: none"> ◆ 属性を追加するには、使用可能な属性のリストから対象の属性を選択します。<Ctrl> キーまたは <Shift> キーを使用すると、複数の属性を選択できます。 ◆ 矢印をクリックして、属性を [選択済み] リストに移動します。属性の削除は、逆の手順になります。 ◆ 属性リストを並べ替えるには、[選択済み] リストの右にある上下の矢印をクリックします。[送信] をクリックします。 <p>属性およびデータタイプ：</p> <p>属性のデータタイプにより属性の表示方法が決まります。たとえば、属性がローカルまたはグローバルのリストサブタイプとして定義されている場合、リストボックスに表示されます。</p> <p>詳細については、87 ページのセクション 4.3 「エンティティおよび属性の操作」を参照してください。</p>

初期設定パネルの設定の完了 有効なエントリが送信されていることを確認するには、[送信] をクリックします。エントリが有効でない場合、初期設定ページの上部にエラーメッセージが表示されます。[送信] をクリックしても、エラーが発生しないようになったら、[リストビューに戻る] をクリックします。リストビューに戻った後は、[設定の保存] をクリックします。

この章では、エンティティの属性データの表示または操作が可能な、詳細ポートレットについて説明します。これは、Identity Manager ユーザアプリケーションの [識別セルフサービス] タブの [マイプロフィール] アクションの基本となります。ここで取り扱う内容は次のとおりです。

- ◆ 251 ページのセクション 17.1 「詳細ポートレットについて」
- ◆ 259 ページのセクション 17.2 「前提条件」
- ◆ 262 ページのセクション 17.5 「初期設定」

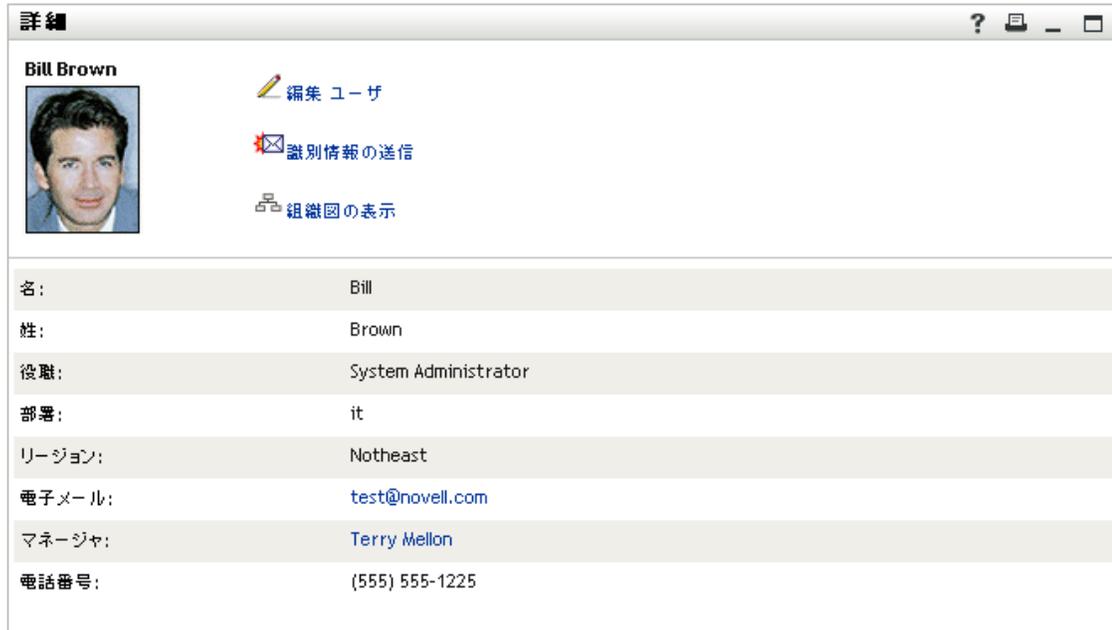
17.1 詳細ポートレットについて

詳細ポートレットはエンティティの属性およびその値を詳細に表示します。このポートレットには、表示、編集という 2 つのモードがあります。詳細ポートレットにアクセスすると、組み込み機能を使用して次のような操作が可能になります。

- ◆ 252 ページのセクション 17.1.1 「エンティティデータの表示」
- ◆ 255 ページのセクション 17.1.2 「エンティティデータの編集」
- ◆ 258 ページのセクション 17.1.3 「エンティティデータの電子メール送信」 (表示モードのみ)
- ◆ 258 ページのセクション 17.1.4 「組織図へのリンク」
- ◆ 258 ページのセクション 17.1.5 「他のエンティティの詳細情報へのリンク」 (表示モードのみ)
- ◆ 259 ページのセクション 17.1.6 「エンティティデータの印刷」 (表示モードのみ)

17.1.1 エンティティデータの表示

詳細ポートレットにアクセスすると、ユーザ、グループなど、選択したエンティティについての属性データが表示されます。たとえば、**Bill Brown** というユーザが自分自身の情報を表示すると、詳細ポートレットには次のような情報が表示されます。



詳細

Bill Brown

 [編集 ユーザ](#)

 [識別情報の送信](#)

 [組織図の表示](#)

名:	Bill
姓:	Brown
役職:	System Administrator
部署:	it
リージョン:	Notheast
電子メール:	test@novell.com
マネージャ:	Terry Mellon
電話番号:	(555) 555-1225

ユーザイメージデフォルトでは、詳細ポートレットには、ユーザの写真属性が含まれるようになっていきます。ただし、アイデンティティポータルにこの属性が含まれていない場合、または含まれてはいるが指定されていない場合、デフォルトイメージが表示されます。ユーザイメージを別の場所に格納する場合は、代わりにそれを表示するようにポートレットを設定できます。

詳細については、[255 ページの「イメージの動的なロード」](#)を参照してください。

表示する属性の決定

詳細ポートレットには次の属性のみ表示されます。

- ◆ ディレクトリ抽象化レイヤデータ定義により表示可能と設定されている属性。

VDD 設定の詳細については、[75 ページの第 4 章「ディレクトリ抽出化レイヤの設定」](#)を参照してください。

- ◆ 詳細ポートレットの初期設定で指定されている属性。

詳細ポートレットに表示される属性の指定については、[262 ページのセクション 17.5「初期設定」](#)を参照してください。

- ◆ 現在のユーザが表示する権利を持っている属性。

たとえば、**salary** 属性を表示する権利を持つマネージャはデータを表示できますが、他のユーザは表示できません。

詳細については、[260 ページのセクション 17.2.2「エンティティに権利を割り当てる」](#)を参照してください。

- ◆ 現在、値が指定されている属性。

属性の表示方法の決定

詳細ポートレットは属性を表示するとき、データをテキスト形式に変換しますが、次の場合は例外になります。

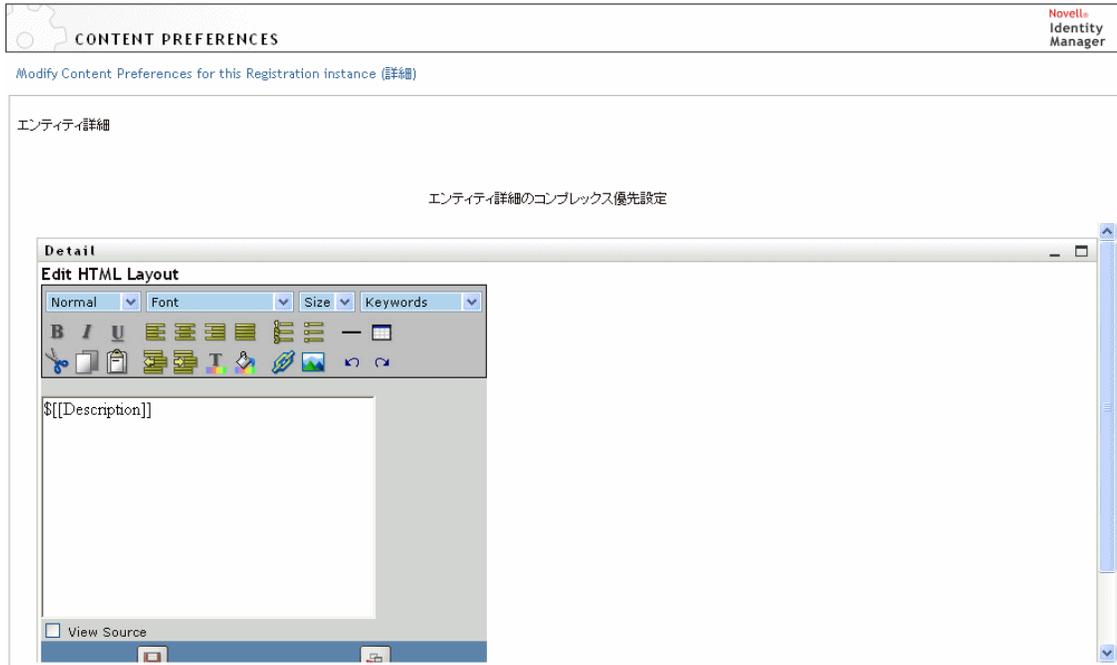
抽象化レイヤ定義内の形式指定	表示方法
Format: email	メールアドレスリンクとして
Format: <ul style="list-style-type: none"> ◆ groupwise-im ◆ aol-im ◆ yahoo-im 	チャットの開始およびユーザの追加を行うアイコンとして
Data type: Binary	イメージを表示するボタンおよびリンクとして
Format: image	
Data type: Boolean	[true] または [false] を示す、無効になっているラジオボタンとして このボタンが表示される時、デフォルト値は示されません。値が指定されるまで属性が実際に作成されないためです。
Multivalue: Selected	各属性値の編集、追加、および削除用コントロールの繰り返しのセットとして (カンマ区切りリスト形式)
Control type: DNLookup	リンクとして 前の例では、Terry Mellon というリンクが、Bill Brown のマネージャの詳細データへのアクセスを示しています。
Control type: <ul style="list-style-type: none"> ◆ ローカルリスト ◆ グローバルリスト 	実際の (キー) 値ではなく表示ラベルとして たとえば、EmployeeType 属性は、実際の値 ft ではなく、Full Time と表示されます。

見出し領域の内容の決定

HTML の標準機能を使用し、詳細ポートレットの見出し領域のレイアウトを編集できます。



詳細ポートレットの初期設定機能には、外観およびコンテンツの作成用に使用できる HTML レイアウトエディタが含まれています。



[Return to List View](#)

HTML レイアウトエディタの使用

HTML レイアウトエディタは、テキスト形式やリストを定義したり、アンカーやイメージなどを指定したりする HTML エディタの標準的な機能を提供します。

キーワードレイアウトの設計時、[キーワード] ドロップダウンメニューから、詳細ポートレットの見出し領域内に変数を挿入し、ランタイム時に特定の属性値で置き換えられるように設定できます。次の構文を使用してキーワードを入力することもできます。

```
$[[keyword]]
```

keyword は、*LastName* などの属性の値を表します。

次の構文を使用すると、属性を連結できます。

```
$[[keyword+keyword]]
```

次に例を示します。

```
$[[FirstName+LastName]]
```

任意の数の属性を連結できます。また次のように、引用符で囲まれた文字列を含めることもできます。

```
${[keyword+"sample text"+keyword]}
```

これにより、キーワードの値と引用符で囲まれたテキストがレンダリングされます。

注：レイアウトでキーワードを誤入力した場合は、それがそのまま (\$[[]] を含む) レンダリングされます。

イメージの動的なロードアイデンティティポータルに格納されているユーザの写真などのイメージを表示するには、HTML レイアウトエディタを使用してその属性名を追加できます。たとえば、ユーザの写真を表示する場合は [ユーザの写真] 属性を追加します。イメージをアイデンティティポータル外に格納している場合は、次のように、HTML エディタのソースの表示モードから **IMG: タグ** を使用する必要があります。

- 1 ポートレットの初期設定に移動し、HTML エディタにアクセスします。
- 2 [ソースの表示] をクリックします。
- 3 次の構文で、**IMG: タグ** を使用して、場所、属性キー、およびファイル拡張子を組み込みます。

```
${[IMG:"URL" + attribute-key-name + "fileextension"]}
```

次の例は、従業員の写真をアプリケーションサーバの /images サブディレクトリに Last Name (姓) ごとに JPG イメージとして格納している場合の構文です。

```
${[IMG:"http://myhost:8080/images/"+LastName+".jpg"]}
```

ランタイム時、ポートレットは URL を LastName 属性およびファイル拡張子 .jpg と連結します。

HTML エディタは柔軟な構文をサポートしています。次の構文のようなテキストおよび属性の組み合わせをサポートしています。

```
${[IMG:"some text" + attribute-key-name + ...]}
```

17.1.2 エンティティデータの編集

詳細ポートレットには、編集リンク ([自分の情報の編集]、[ユーザの編集]、[Edit Device (デバイスの編集)] など) があり、表示モードから編集モードに切り替えられるようになっています。これにより、適切な権利を持つユーザは、現在のエンティティの属性を変更したり、変更を保存したりすることができます。

たとえば、Bill Brown というユーザが自分自身の情報を編集するとき(このユーザが必要な権利を持っている場合)、詳細ポートレットに表示される内容は次のとおりです。

注：ブール属性については、両方のラジオボタンがオフになっている場合、その属性が現在のユーザには存在しないことを示します。[true] または [false] のラジオボタンのいずれかをオンにした場合、そのユーザに対してこの属性が作成され、値が設定されます。

表示する属性の決定

編集モードの場合、詳細ポートレットにより表示される属性は、次のものに限られます。

- ◆ ディレクトリ抽象化レイヤデータ定義により表示可能と設定されている属性。
データ定義の詳細については、75 ページの第 4 章「ディレクトリ抽出化レイヤの設定」を参照してください。
- ◆ 現在のユーザが表示する権利を持っている属性。

たとえば、salary 属性を表示する権利を持つマネージャはデータを表示できますが、他のユーザは表示できません。

詳細については、[260 ページのセクション 17.2.2 「エンティティに権利を割り当てる」](#)を参照してください。

編集モードで表示する属性は、これらの条件すべてを満たしている必要があります。

属性の表示方法の決定

編集モードでは、詳細ポートレットは編集可能な各属性をテキストボックスとして表示します。ただし次の場合を除きます。

属性タイプ仕様 (VDD ファイル内での指定内容)	表示方法
Data type:Binary Format:image	イメージの表示、更新、および追加を行うための Entity Image Upload (エンティティイメージアップロード) ポートレットへのボタンおよびリンクとして
Data type:Boolean	[true] または [false] を示すラジオボタンとして
hide:Selected	[非表示] チェックボックスとして
multivalued=Selected	属性値の編集、追加、および削除用のコントロールのセットとして
Control type:DNLookup	DN の検索および選択のための Param List (パラメータリスト) ポートレットを起動するボタンとして
Control type:	ドロップダウンリストとして (複数選択が可能)
	<ul style="list-style-type: none">◆ ローカルリスト◆ グローバルリスト

定義により、またはユーザの権利が不十分なために編集できない属性は、[無効] または [読み込み専用] と表示されます。

変更の検証

編集時、次の属性タイプ指定についてはデータ検証が自動的に実行されます。

- ◆ Format:email
- ◆ Data type: 整数
- ◆ Control type: 範囲

ローカルリストまたはグローバルリストのコントロールタイプを使用する場合は、指定した属性の範囲外の値を表示リストに含めることができます。そうした値には、範囲外であることを示すフラグが付き、検証の結果、送信対象外となります。

デフォルトの「マイプロパティ」エンティティの定義

ディレクトリ抽象化レイヤにエンティティを定義する場合、ディレクトリ抽象化レイヤエディタの「環境設定」要素内のデフォルトの「マイプロファイル」エンティティに値を指定して、編集用に使用する別のエンティティ定義を指定できます。表示モードから編集

モードに切り替わる際、詳細ポートレットはこの要素が指定されているかどうかをチェックしてから、適切なエンティティ定義を使用して属性を表示します。

たとえば、**Student** のエンティティ定義で、デフォルトの「マイプロフィール」エンティティに「user」という値があるとします。この場合、表示モードは **Student** エンティティ定義を使用しますが、編集モードには **user** エンティティ定義が使用されます。

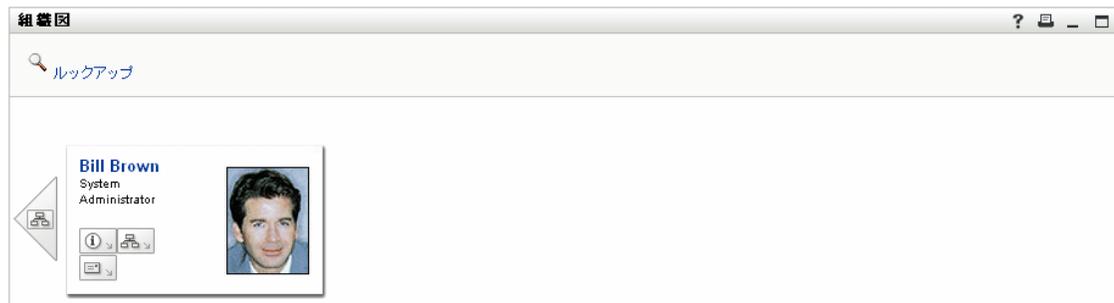
17.1.3 エンティティデータの電子メール送信

詳細ポートレットには、[識別情報の送信] リンクがあります。このリンクをクリックすると、現在のエンティティの [詳細] 画面の URL を、1 人または複数のユーザに電子メールで送信できます。実際の情報ではなく [詳細] 画面の URL を電子メールで送信することにより、セキュリティを確保できます。これは、URL を受信したユーザがその URL を使用するには、適切な権限が必要になるためです。

17.1.4 組織図へのリンク

詳細ポートレットには、[組織図の表示] リンクがあります。このリンクをクリックすると、現在のエンティティの組織図ポートレットを表示できます。

たとえば、**Bill Brown** というユーザの [詳細] 画面が表示されている場合、このリンクをクリックすると、次の画面が表示されます。



組織図ポートレットの詳細については、[265 ページの第 18 章「組織図ポートレットの参照」](#)を参照してください。

17.1.5 他のエンティティの詳細情報へのリンク

詳細ポートレットの設定時、ユーザが現在のエンティティから関連エンティティにリンクできるように設定しなければならない場合があります。これは、コントロールタイプが **DNLookup** に定義されている属性を組み込むことにより可能です。

Manager 属性がユーザの [詳細] 画面に表示される場合、この属性はリンクとして表示されます。このリンクをクリックすると、Manager の [詳細] 画面が表示されます。



ディレクトリ抽象化レイヤの詳細については、[75 ページの第 4 章「ディレクトリ抽出化レイヤの設定」](#)を参照してください。

詳細ポートレットに表示される属性の指定については、[262 ページのセクション 17.5「初期設定」](#)を参照してください。

17.1.6 エンティティデータの印刷

デフォルトの詳細ポートレットの表示設定では、ポートレットのタイトルバー上の [印刷] オプションが有効になっています。[印刷] を有効にした場合、このオプションをクリックすると、詳細コンテンツのプリンタフレンドリバージョンが表示されます。

詳細ポートレットのこれらの設定を変更するには、[管理] タブを使用して、DetailPortlet のポートレット登録を更新します ([ポートレット管理] ページ上で行います)。

詳細については、[181 ページの第 9 章「ポートレットの管理」](#)を参照してください。

17.2 前提条件

詳細ポートレットの使用を開始する前に、次のことを理解しておく必要があります。

- ◆ [260 ページのセクション 17.2.1「ディレクトリ抽出化レイヤの設定」](#)
- ◆ [260 ページのセクション 17.2.2「エンティティに権利を割り当てる」](#)

17.2.1 ディレクトリ抽出化レイヤの設定

詳細ポートレットは、ディレクトリ抽象化レイヤの定義に依存します。特定の詳細ポートレット機能をサポートするための抽象化レイヤデータ定義の設定方法については、この章の次の節を参照してください。

- ◆ [252 ページのセクション 17.1.1 「エンティティデータの表示」](#)
- ◆ [255 ページのセクション 17.1.2 「エンティティデータの編集」](#)
- ◆ [262 ページのセクション 17.4 「ページからの詳細ポートレットの使用」](#)

ディレクトリ抽象化レイヤの設定全般については、[75 ページの第 4 章「ディレクトリ抽出化レイヤの設定」](#)を参照してください。

17.2.2 エンティティに権利を割り当てる

詳細ポートレットのエンティティおよびその属性にアクセスするには、eDirectory の権利が適切に割り当てられている必要があります。

操作	ユーザーに必要な権利
属性の表示	読み込み
属性の編集	書き込み

ユーザーをオブジェクト (エンティティ) のトラスティに指定することで権利を割り当てることができます。続いて、どの属性にどの権利を割り当てるかを指定できます。

17.3 他のポートレットからの詳細ポートレットの起動

詳細ポートレットは、一般的に、他の識別ポートレットからエンティティを選択した後に起動します。詳細ポートレットの起動には、次の方法があります。

- ◆ [261 ページのセクション 17.3.1 「リスト検索ポートレットからの起動」](#)
- ◆ [261 ページのセクション 17.3.2 「組織図ポートレットからの起動」](#)

17.3.1 リスト検索ポータルレットからの起動

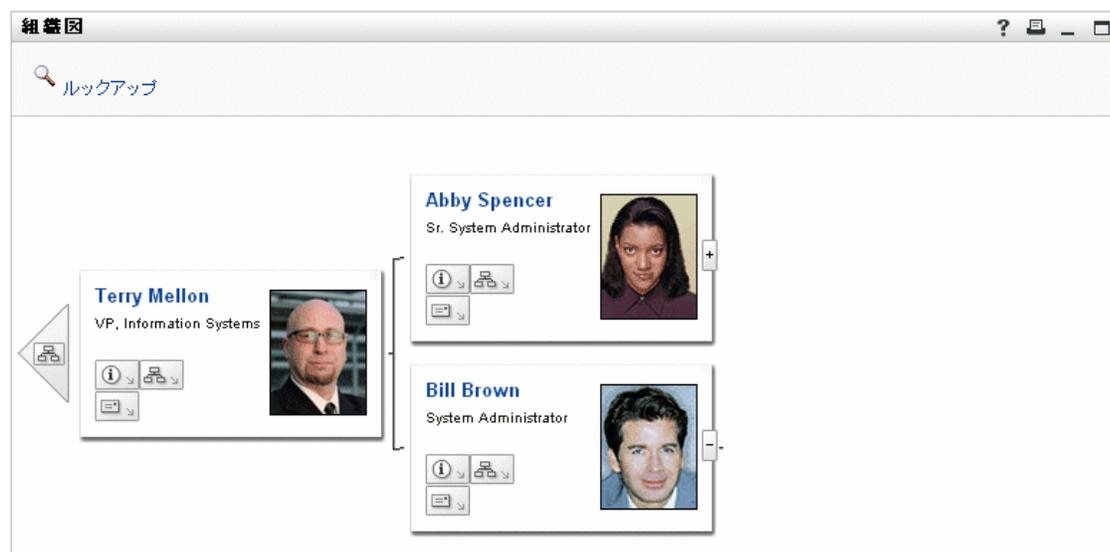
リスト検索ポータルレットで、検索結果内のエンティティ行をクリックすると、そのエンティティの [詳細] 画面が表示されます。たとえば、次のリストの **Bill Brown** 行をクリックすると、詳細ポータルレットが属性データとともに表示されます。



リスト検索ポータルレットの詳細については、295 ページの第 20 章「リスト検索ポータルレットの参照」を参照してください。

17.3.2 組織図ポータルレットからの起動

組織図ポータルレットでは、エンティティの [識別アクション] アイコンをクリックして [情報を表示] を選択すると、そのエンティティの [詳細] 画面が表示されます。たとえば、次の組織図で **Bill Brown** の [情報を表示] をクリックすると、詳細ポータルレットが属性データとともに表示されます。



組織図ポートレットの詳細については、[265 ページの第 18 章「組織図ポートレットの参照」](#)を参照してください。

17.4 ページからの詳細ポートレットの使用

ユーザ自身の属性データを表示したり編集したりするためのセルフサービスをユーザに提供する場合、詳細ポートレットを共有ページに追加します。詳細ポートレットは、共有で使用された場合、自動的に現在のユーザ（または他のデフォルトエンティティ）のデータにアクセスします。

たとえば、**Bill Brown** というユーザは、ログインして次のパーソナルページに移動して、詳細ポートレットを使用して自分の情報を保守できます。



このシナリオ（他のポートレットから起動するのではなく、詳細ポートレットにページからアクセスするシナリオ）で、詳細ポートレットが使用するエンティティ定義を決定するには、ディレクトリ抽象化レイヤの「環境設定」要素で「デフォルトの「マイプロフィール」エンティティ」の設定を指定します。

17.5 初期設定

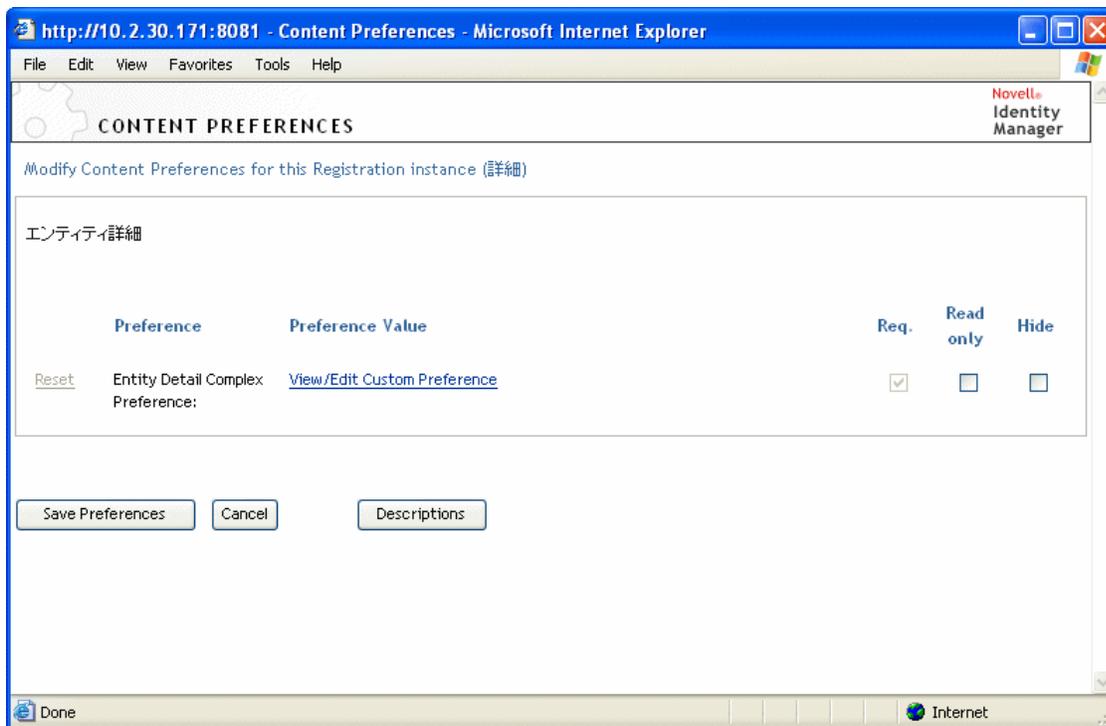
詳細ポートレットのコンテンツおよび外観を定義するには、初期設定を設定します。詳細ポートレットの使用法によって、初期設定を設定する場所が異なります。

共有ページまたはコンテナページからポートレット初期設定にアクセスする場合については、[137 ページの第 7 章「ページの管理」](#)を参照してください。

ポートレット登録のポートレット初期設定にアクセスする場合については、[181 ページの第 9 章「ポートレットの管理」](#)を参照してください。

17.5.1 初期設定について

詳細ポートレットの初期設定はすべて、1つの [エンティティ詳細のコンプレックス優先設定] に含まれています。



この複合初期設定を開くと、詳細ポートレットの各初期設定は次のように表示されます。

コンテンツ 初期設定

Novelle Identity Manager

[この登録インスタンスのコンテンツ初期設定を変更します \(詳細\)](#)

エンティティ詳細

エンティティ詳細のコンプレックス優先設定

詳細

概要

エンティティ定義	ユーザ	✖
リストとして表示する属性		✎
	名	
	姓	
	役職	
	部署	
	リージョン	
	電子メール	
	マネージャ	
	電話番号	
HTMLレイアウト	\${[[FirstName]]} \${[[LastName]]} \${[[UserPhoto]]}	✎
編集エンティティを有効にする	<input checked="" type="radio"/> true <input type="radio"/> False	

[リストビューに戻る](#)

これらの初期設定は、表示モードのみに適用されます (編集モードには適用されません)。次に、各初期設定について説明します。

初期設定	説明
エンティティ定義	<p>ユーザ、デバイス、グループなどの特定のエンティティタイプに対して詳細ポートレットが使用された場合に表示する、属性リストおよび HTML レイアウトを指定します。</p> <p>追加エンティティタイプに対して詳細ポートレットを使用できるようにするには、[エンティティ定義の追加] をクリックします。</p>
リストとして表示する属性	<p>選択したエンティティについて、ポートレットで表示する属性を指定します。これらの属性は、選択した順にリストに表示されます。</p> <p>ボタンを使用すると、必要に応じて属性を追加または削除できます。</p>
HTML レイアウト	<p>HTML レイアウトエディタを開くためのボタンを配置します。このエディタを使用して、選択したエンティティについて、詳細ポートレットによって表示される見出し領域を設計できます。</p> <p>詳細については、253 ページの「見出し領域の内容の決定」を参照してください。</p>

この章では、Identity Manager ユーザアプリケーションの、既存の組織図機能の変更方法および新しい組織図機能の追加方法について説明します。ここで取り扱う内容は次のとおりです。

- ◆ 265 ページのセクション 18.1 「組織図について」
- ◆ 267 ページのセクション 18.2 「組織図ポートレットの設定」
- ◆ 268 ページのセクション 18.2.2 「組織図の初期設定」

18.1 組織図について

組織図ポートレットを使用すると、エンドユーザは、アイデンティティポールのオブジェクト間の階層関係を表示したり、参照したりすることができます。たとえば、次の階層を表示するように組織図ポートレットを定義できます。

- ◆ 組織 (従業員、マネージャなど)
- ◆ グループのメンバーシップ (グループ内のすべての従業員など)
- ◆ ユーザに割り当てられたデバイス (携帯電話、ラップトップなど)

デフォルトでは、Identity Manager ユーザアプリケーションの [識別セルフサービス] タブには [組織図] アクションが含まれています。このアクションは、アイデンティティポールのユーザオブジェクト間の関係を表示する組織図ポートレットです。次の例は、デフォルトの組織図ポートレットで (サンプルデータを使用して) この関係がレンダリングされたときの画面です。



組み込みリンク 組織図ポートレットには、次のリンクが組み込まれています。

リンク	説明
	次の上位レベルに移動できます。これは、親エンティティと子エンティティが同じ関係を表示する場合にのみ使用できます。
	<p>詳細ポートレットを起動します。</p> <p>この組み込みリンクは、273 ページの「組織図のレイアウトの初期設定」で説明されている組織図のレイアウト初期設定で設定できます。</p>
	<p>組織図のリストを表示します。表示する組織図は選択できます。</p> <p>この組織図のリストは動的なリストです。同じ親エンティティタイプを共有する他の組織図が表示されます。たとえば、マネージャの従業員組織図 (親エンティティはユーザ) を表示する場合、このアイコンをクリックすると、表示される組織図のリストには、親エンティティもユーザである関係のみが含まれます。</p> <p>この組み込みリンクは、273 ページの「組織図のレイアウトの初期設定」で説明されている組織図のレイアウト初期設定で設定できます。</p>
	<p>次の目的で電子メールツールを起動します。</p> <ul style="list-style-type: none"> ◆ 現在選択しているユーザの詳細な識別情報を送信する ◆ 電子メールを作成する <p>この組み込みリンクは、273 ページの「組織図のレイアウトの初期設定」で説明されている組織図のレイアウト初期設定で設定できます。</p>
 <u>Lookup</u>	[ルックアップ] リンクでは、エンティティ検索を実行できます。検索の結果、見つかったエンティティは、表示された図のトップノードとなります。
	次のレベルにドリルダウンできます。

組織図の組み込みリンクの追加および制限の詳細については、[273 ページの「組織図のレイアウトの初期設定」](#)を参照してください。

18.1.1 組織図の関係について

組織図ポートレットは、ディレクトリ抽象化レイヤで定義されている関係を表示します。Identity Manager ユーザアプリケーションのインストール後に使用できる関係は、次のとおりです。

- ◆ グループのメンバーシップ
- ◆ マネージャと従業員
- ◆ ユーザグループ

組織図の関係の作成および変更については、[75 ページの第 4 章「ディレクトリ抽出化レイヤの設定」](#)を参照してください。

注:組織図ポートレットでは、ダイナミックグループが完全にはサポートされていません。ダイナミックグループは、関係の親エンティティとしては定義できませんが、子エンティティとしては定義できます。

18.1.2 組織図の表示について

デフォルトでは、組織図は「ポートレットの幅」と「ポートレットの高さ」の初期設定で定義された領域のポートレットフレームに表示されます。定義された領域より大きい領域がコンテンツで必要な場合は、ポートレットの境界が拡張され、ページの高さと幅も拡張されます。ポートレットのタイトルバーにある最大化アイコンをクリックすると、組織図を完全に表示できます(詳細ポートレットから起動する場合は、デフォルトで最大化モードで表示されます)。

ユーザイメージユーザオブジェクトの組織図のレイアウトには、デフォルトで「ユーザの写真」属性が含まれています。ただし、アイデンティティポータルにこの属性が含まれていない場合、または含まれていても指定されていない場合、ランタイム時に組織図で無視されます。写真を別の場所に格納している場合は、それらの写真を表示するよう組織図を設定できます。

詳細については、[278 ページのセクション 18.2.3 「イメージの動的なロード」](#)を参照してください。

18.2 組織図ポートレットの設定

組織図ポートレットを設定するには、次の手順に従います。

ステップ	タスク	説明
1	表示する関係を定義します。	<p>Identity Manager ユーザアプリケーションのインストール時に事前定義された関係のいずれか 1 つを使用するか、独自に作成します。</p> <p>関係の定義の詳細については、75 ページの第 4 章「ディレクトリ抽出化レイヤの設定」を参照してください。</p>
2	関係で使用するエンティティおよび属性が、ディレクトリ抽象化レイヤで使用できることを確認します。	関係の定義の詳細については、 268 ページのセクション 18.2.1 「ディレクトリ抽象化レイヤの設定」 を参照してください。
3	関係を表示する場所を決定します。	<p>組織図を起動するための新しいページを作成するか、詳細ポートレットまたは別の組織図から起動するかを考慮します。</p> <p>ページの作成およびページへのポートレットの追加の詳細については、137 ページの第 7 章「ページの管理」を参照してください。</p>

ス テッ プ	タスク	説明
4	ポートレットの初期設定を指定します。	<p>初期設定で定義する内容は次のとおりです。</p> <ul style="list-style-type: none"> ◆ 表示する属性 ◆ 表示方法 (HTML レイアウト) <p>詳細については、268 ページのセクション 18.2.2 「組織図の初期設定」を参照してください。</p>
5	テスト	関係の定義およびレイアウトをテストします。
6	eDirectory の権利を設定し、パフォーマンス向上にインデックスが有効であれば、インデックスを構築します。	<p>有効な権利—ポートレットにより定義された属性を表示するには、そのポートレットの読み込みの権利が必要です。</p> <p>パフォーマンスの向上—組織図表示のパフォーマンスを向上させるには、eDirectory の値インデックスを関係の子属性に追加します。子属性は LDAP 検索に使用されます。</p>

18.2.1 ディレクトリ抽象化レイヤの設定

組織図で表示するエンティティおよび属性は、ディレクトリ抽象化レイヤで定義する必要があります。次の表では、組織図で表示するそれぞれのエンティティおよび属性について、設定の必要がある属性およびプロパティを示します。

定義タイプ	設定	値
entity	view	選択 (true)
attribute	read	選択 (true)
	search	選択 (true)

[ルックアップ] リンクの要件 [ルックアップ] リンクを使用して、親エンティティキーと同じタイプの他のオブジェクトの検索を実行することにより、組織図を操作できます。[ルックアップ] リンクを使用するには、親エンティティキーに、require アクセスプロパティと search アクセスプロパティが [true] に設定された属性が (ディレクトリ抽象化レイヤエディタで選択) 少なくとも 1 つ必要です。そうでない場合、[ルックアップ] リンクの [オブジェクトルックアップ] ダイアログボックスが、空のダイアログボックスとして表示されます。

エンティティおよび属性の環境設定の詳細については、[75 ページの第 4 章 「ディレクトリ抽出化レイヤの設定」](#)を参照してください。

18.2.2 組織図の初期設定

次に示す 2 つのタイプの初期設定を定義します。

- ◆ [269 ページの 「組織図の関係の初期設定」](#)
- ◆ [273 ページの 「組織図のレイアウトの初期設定」](#)

組織図の関係の初期設定

組織図の関係の初期設定は、1つの初期設定ページに含まれています。

このタブを使用すると、このコンテンツインスタンスに定義されたすべてのデフォルトの初期設定を変更できます。初期設定に適用された変更はこの特定のコンテンツインスタンスに対してのみ有効になります。

初期設定	選択値	要求	読み込み専用	非表示
リセット 表示レイアウト	カスタム初期設定の表示/編集	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
リセット 関係キー	<input type="text" value="user2users"/>	詳細 <input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
リセット 親エンティティキー	<input type="text" value="{[User/id]}"/>	詳細 <input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
リセット デフォルトの深さ	<input type="text" value="1"/>	詳細 <input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
リセット 最大の深さ	<input type="text" value="10"/>	詳細 <input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
リセット ポートレットの幅	<input type="text" value="700"/>	詳細 <input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
リセット ポートレットの高さ	<input type="text" value="400"/>	詳細 <input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
リセット スクロールバーを表示	<input type="radio"/> True <input checked="" type="radio"/> False	詳細 <input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
リセット 組織図のスキン	<input type="text" value="Business Card"/> <input type="button" value="▼"/>	詳細 <input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

選択項目

値	表示
Card	Business Ca

[挿入](#) [削除](#)

NewBleu True Blue 挿入 削除

追加

[リセット](#)

ワイヤを項目に接続 True False

[詳細](#)

[リセット](#)

メニューのタイムアウト

[詳細](#)

[リセット](#)

ツリー表示

挿入 削除

[詳細](#)

追加

[リセット](#)

リープ表示

[詳細](#)

選択項目		
値	表示	
0	Vertical List	挿入 削除
1	Vertical List	挿入 削除
2	Horizontal L	挿入 削除
3	Horizontal L	挿入 削除

追加

[リセット](#)

項目の最大幅

[詳細](#)

[リセット](#)

項目の最小の高さ

[詳細](#)

[リセット](#)

複数値区切り文字

[詳細](#)

設定の保存 キャンセル すべてリセット 説明

初期設定

操作

表示レイアウト

[カスタム初期設定の表示 / 編集] をクリックしてレイアウト初期設定にアクセスします。[273 ページの「組織図のレイアウトの初期設定」](#)を参照してください。

関係キー

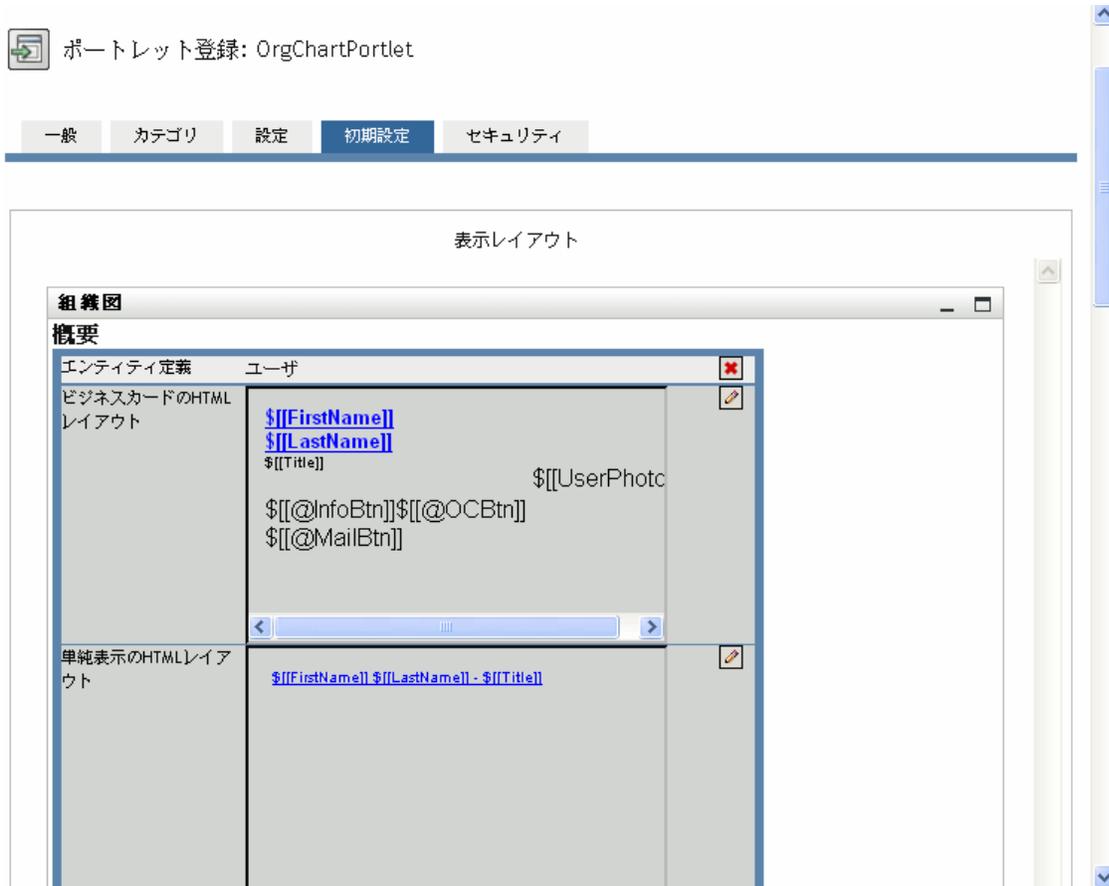
関係キーを指定します。この値は、ディレクトリ抽象化レイヤで指定されている関係キーの1つと対応している必要があります。

初期設定	操作
親エンティティキー	<p>表示する組織図のルートノードを示すエンティティの DN を入力します。現在のユーザの組織図を表示する場合は、「<code>\${User/id}</code>」と入力します (<code>\${User/id}</code> パラメータは現在のユーザの DN を示します)。</p> <p>この値はディレクトリ抽象化レイヤの <code>search-root</code> プロパティで指定したノード内部の値でなければなりません。そうでない場合、LDAP 検索は失敗します。</p> <p>有効な DN の例は次のとおりです (サンプルデータを使用)。</p> <ul style="list-style-type: none"> ◆ Jack Miller という名前の従業員についての、ユーザ対ユーザ関係キーを組織図のルートとして表示する場合は、次のように指定します。 <pre>cn=jmiller,ou=users,ou=sample,o=novell</pre> <ul style="list-style-type: none"> ◆ Accounting グループについてのグループ対ユーザ関係キーをルートノードとして表示する場合は、次のように指定します。 <pre>cn=Accounting,ou=groups,ou=sample,o=novell</pre>
デフォルトの深さ	<p>組織図が最初に表示される時の深さを指定します。</p> <ul style="list-style-type: none"> ◆ 0— ルートのみを表示 ◆ 1— ルートおよび子を表示 ◆ 2— ルート、子、および孫を表示 <p>以下、同様に続きます。この値が [最大の深さ] (次を参照) の値を超えた場合は、[最大の深さ] の値が優先されます。</p>
最大の深さ	<p>組織図でドリルダウンできる最大の深さを定義します。これは、有効な権利によって制限されている組織図内で移動できるかどうかを示すものではありません。</p>
OrgChart のスキン	<p>ビジネスカード</p> <p>eGuide</p> <p>Novell.com</p> <p>接続済み</p> <p>ツールグループ</p>
ワイヤを項目に接続	<p>組織図カードを回線接続するかどうかを指定します。[False] は接続しないことを示します。</p>
メニューのタイムアウト	<p>組み込みリンクに現在表示されているメニューが表示されなくなるまでの時間 (ミリ秒) を指定します。</p>

初期設定	操作
ツリー表示	<p>深さレベルごとの、OrgChart の方向、配置、および外観を定義します。</p> <p>最初の値 n は、$0 \sim n-1$ までのレベルについて、方向、配置、および外観を定義します。最後の値は、$n-1$ より大きい深さレベルについて繰り返し使用されます。値は、$0 \sim 5$ です。</p> <p>次の値があります。</p> <p>0: 項目の垂直リストの上にカードを配置します。</p> <p>1: 項目の垂直リストの上にラインを配置します。</p> <p>2: 項目の水平リストの上にカードを配置します。</p> <p>3: 項目の水平リストの上にラインを配置します。</p> <p>4: 項目の垂直リストの前にカードを配置します。</p> <p>5: 項目の垂直リストの前にラインを配置します。</p>
リーフ表示	<p>1 つの OrgChart ブランチの最高の深さについて、OrgChart の方向、配置、および外観を定義します。</p>
項目の最大幅	<p>この値は丸め (「項目の最小高さ」 * 1.618) と等しくなるようにしてください。</p>
項目の最小の高さ	<p>この値は丸め (「項目の最小幅」 / 1.618) と等しくなるようにしてください。</p>
複数值属性の区切り文字	<p>この文字は複数の値を持つ属性の区切りとして使用します。</p>

組織図のレイアウトの初期設定

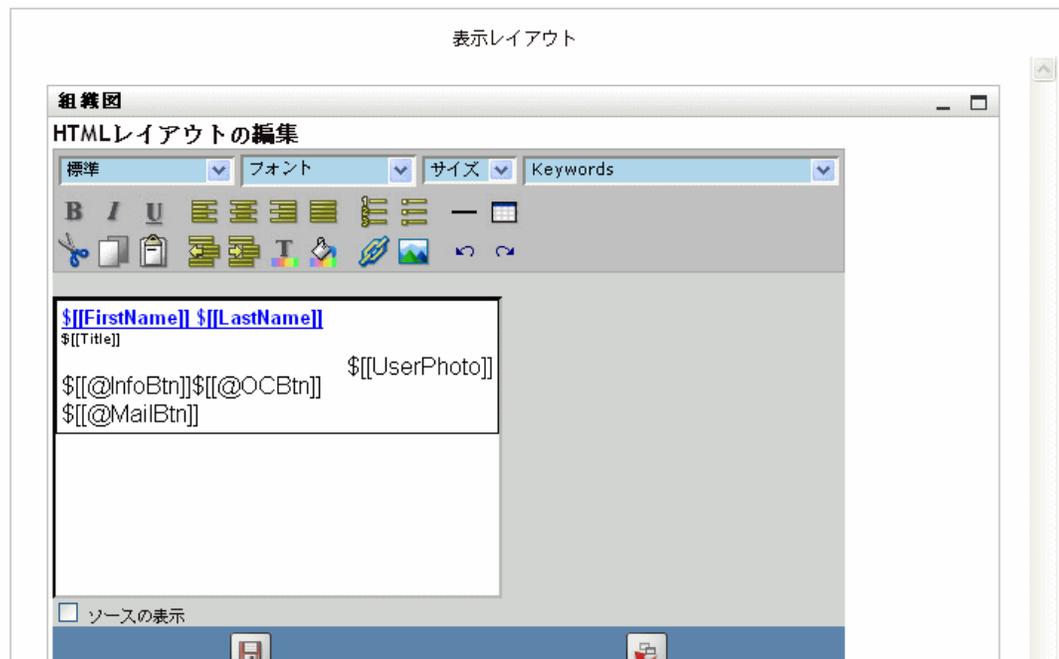
組織図のレイアウト初期設定を使用すると、組織図エントリを表示するときの HTML レイアウトを定義できます。HTML エディタを使用して、より詳細な編集を行うこともできます。278 ページの「外部エディタの使用 -」を参照してください。



ビジネスカードの HTML レイアウト — デフォルトのレイアウトです。

単純表示の HTML レイアウト — 「ツリー表示」初期設定が 1 に設定されている場合に表示されるレイアウトです。

HTML エディタ 編集ボタンをクリックすると、HTML エディタにアクセスできます。HTML エディタの外観を次に示します。



HTML エディタを使用する

HTML エディタは、組織図でリーフレイアウトを定義するための WYSIWYG インタフェースを提供するエディタです。テキスト形式やリストを定義したり、アンカー、イメージなどを指定したりするための標準的な HTML エディタ機能を備えています。属性、コマンド、ナビゲーション URL をレイアウト領域に配置するには、[キーワード] ドロップダウンメニューを使用します。ドロップダウンメニューからキーワードを選択すると、そのキーワードが適切な構文で挿入されます。レイアウト領域内に HTML を追加することもできます。

キーワード レイアウトを設計する際、[キーワード] ドロップダウンメニューを使用して変数を挿入し、ランタイム時に、特定の属性値で置き換えられるようにできます。また、次の構文を使用してキーワードを入力することもできます。

```
${[keyword]}
```

keyword は、LastName などエンティティ属性の値を表します。

次の構文を使用すると、属性を連結できます。

```
${[keyword+keyword]}
```

次に例を示します。

```
$[[FirstName+LastName]]
```

任意の数の属性を連結できます。また次のように、引用符で囲まれた文字列を含めることもできます。

```
$[[keyword+"sample text"+keyword]]
```

これにより、キーワードの値と引用符で囲まれたテキストがレンダリングされます。

注：レイアウトでキーワードを誤入力した場合は、それがそのまま (\$[[]] を含む) レンダリングされます。

HTML エディタの機能とキーワードの使用 **HTML** エディタ機能と [キーワード] ドロップダウンメニューを使用するには：

機能	ヒント
----	-----

[リンクの挿入] ボタン	リンクを挿入するには：
--------------	-------------

Mozilla の場合：

1. ハイパーリンクするテキストを強調表示してから、[リンクの挿入] をクリックします。
2. **URL** を入力し、[リンクの作成] をクリックします。
3. 初期設定を保存します。

IE の場合：

1. [リンクの挿入] をクリックします。
2. ポップアップウィンドウに、**URL** を入力します。
3. ハイパーリンクするテキストを強調表示してから、[リンクの作成] をクリックします (ポップアップウィンドウで行います)。
4. 初期設定を保存します。

注：イメージまたは **URL** が **HTML** エディタの左上方角にある場合、その上にポップアップウィンドウが重なります。ポップアップウィンドウは移動できないため、その場合はエディタの任意の場所でテキストを作成してから正しい場所に切り貼りする必要があります。

機能	ヒント
[イメージの追加] ボタン	<p>Mozilla の場合：</p> <ol style="list-style-type: none"> 1. イメージを挿入する場所にマウスを合わせてから、[イメージの追加] をクリックします。 2. URL およびテキストを入力してから、ポップアップウィンドウの [イメージの作成] をクリックします。 3. 初期設定を保存します。 <p>IE の場合：</p> <ol style="list-style-type: none"> 1. [イメージの追加] をクリックします。 2. ポップアップウィンドウに URL およびテキストを入力し、イメージを挿入する場所にマウスを合わせてから、[イメージの作成] をクリックします。 3. 初期設定を保存します。 <hr/> <p>注： イメージまたは URL が HTML エディタの左上方角にある場合、その上にポップアップウィンドウが重なります。ポップアップウィンドウは移動できないため、その場合はエディタの任意の場所でテキストを作成してから正しい場所に切り貼りする必要があります。</p>
[キーワード] ドロップダウンメニュー：属性	このエンティティに使用できる属性のセットです。
[キーワード] ドロップダウンメニュー：コマンド	<p>他の識別ポートレット、または IM、電子メールツールなどの組み込み機能を、組織図ポートレットから起動するためのコマンドです。</p> <ul style="list-style-type: none"> ◆ IM アクションボタン — IM を送信するためのボタンを作成します。 ◆ 電子メールアクションボタン — 電子メールを送信するためのボタンを作成します。 ◆ OrgChart アクションボタン — 選択したエンティティインスタンスを親とする、別の関係に切り替えるためのボタンを作成します。 ◆ 情報アクションボタン — 詳細ポートレットを起動します。 <p>生成されるボタンの例については、265 ページの「組み込みリンク」を参照してください。</p>

機能	ヒント
----	-----

URL **OrgChart** ナビゲーションの URL リンク — リンクとして表示する URL またはエンティティ属性を指定できます。リンクをクリックすると、クリックしたエンティティをルートノードとする組織図ポートレットが再び表示されます。

制限:

関係の親エンティティと子エンティティが同じオブジェクトタイプである場合にのみ有効です。たとえば、マネージャ - 従業員の関係の場合、両者がユーザです。

使用上のヒント:

キーワードを使用するには、次の操作を行います。

1. [ソースの表示] をクリックします。
2. 次の構文を使用して、「@NavUrl」というキーワードを入力します。

```
<a href="javascript:$[@NavUrl]">someText</a>
```

someText は、ランタイム時に表示されるリンク、またはエンティティ属性を表します。次の例では、「Click here」がクリックできるリンクとなります。

```
<a href="javascript:$[@NavUrl]">Click here</a>
```

次の例では、**FirstName** 属性がクリックできるリンクです。

```
<a href="javascript:$[@NavUrl]">${FirstName}</a>
```

使用上の制限:

Internet Explorer では、次の構文は使用できません。

```
<a href="$[@NavUrl]">someText</a>
```

保存中、**Internet Explorer** により次のコードが追加されます。

```
http://context before $[@NavUrl]
```

これにより、

```
<a href="$[@NavUrl]">someText</a>
```

は、次のようになります。

```
<a href="http://localhost/.../$[@NavUrl]">someText</a>
```

機能**ヒント**

OrgChart ナビゲーションのクリックリンク —onClick イベントで使用するキーワードです (ページ全体ではなく組織図ポートレット領域のみを更新できるようにします)。

使用上のヒント:

キーワードを使用するには、次の操作を行います。

1. [ソースの表示] をクリックします。
2. 次の構文を使用し、「@NavClick」というキーワードを入力します。

```
<A href="javascript:return false;"  
onClick="$[[@NavClick]]">$[[SomeAttribute]]</A>
```

SomeAttribute は、クリック可能なリンクになるエンティティ属性を表します。

「javascript:return false」は必須です。省略すると、エラーが発生します。

定義したレイアウトを保存するには、[送信] をクリックします。

外部エディタの使用 - HTML 外部エディタを使用する場合は、次の手順に従います。

- 1 初期設定で使用できる HTML レイアウトエディタを使用して、エンティティ属性、コマンド、キーワードの HTML ソースを作成します。
- 2 HTML ソースを、選択したエディタにコピーします。
- 3 必要に応じて変更を行います。
- 4 編集が終了したら、HTML ソースを HTML レイアウトエディタの初期設定にコピーします。

18.2.3 イメージの動的なロード

アイデンティティポータルに格納されているユーザの写真などのイメージを表示するには、その属性の名前をビジネスカードに追加します。たとえば、ユーザの写真を表示する場合には、ユーザの写真属性をビジネスカードレイアウトに追加します。

イメージをアイデンティティポールの外部に格納している場合は、次のように、HTML エディタのソースの表示モードから **IMG: タグ**を使用する必要があります。

- 1 組織図ポートレットの初期設定に移動し、HTML エディタにアクセスします。
- 2 [ソースの表示] をクリックします。
- 3 次の構文で、**IMG: タグ**を使用して、場所、属性キー、およびファイル拡張子を組み込みます。

```
$[[IMG:"URL" + attribute-key-name + "fileextension"]]
```

次の例は、従業員の写真をアプリケーションサーバの /images サブディレクトリに Last Name (姓) ごとに JPG イメージとして格納している場合の構文です。

```
$[[IMG:"http://myhost:8080/images/"+LastName+".jpg"]]
```

ランタイム時、組織図ポートレットは URL を LastName 属性とファイル拡張子 .jpg に連結します。

HTML エディタは柔軟な構文をサポートしています。次の構文のようなテキストおよび属性の組み合わせをサポートしています。

```
$[[IMG:"some text" + attribute-key-name + ...]]
```


この章では、パスワードセルフサービスおよびユーザ認証機能を Identity Manager ユーザアプリケーションに追加する方法について説明します。ここで取り扱う内容は次のとおりです。

- ◆ 281 ページのセクション 19.1 「パスワードを管理するための準備作業」
- ◆ 284 ページのセクション 19.2 「パスワードポートレットについて」
- ◆ 285 ページのセクション 19.3 「「IDM ログイン」ポートレット」
- ◆ 286 ページのセクション 19.4 「「IDM 本人確認の回答」ポートレット」
- ◆ 288 ページのセクション 19.5 「「IDM ヒントの設定」ポートレット」
- ◆ 289 ページのセクション 19.6 「「IDM パスワードの変更」ポートレット」
- ◆ 291 ページのセクション 19.7 「「IDM パスワードを忘れた場合」ポートレット」

19.1 パスワードを管理するための準備作業

パスワードセルフサービスおよびユーザ認証を Identity Manager ユーザアプリケーションでサポートするには、次のことを理解しておく必要があります。

- ◆ 281 ページのセクション 19.1.1 「パスワード管理機能について」
- ◆ 281 ページのセクション 19.1.2 「eDirectory で必要な設定」

19.1.1 パスワード管理機能について

Identity Manager ユーザアプリケーションがサポートするパスワード管理機能には、ユーザ認証とパスワードセルフサービスがあります。これらの機能を使用できるようにすると、アプリケーションで次のことが行われます。

- ◆ Novell eDirectory に対する認証のためのログイン情報(ユーザ名およびパスワード)の入力を促すメッセージが表示される
- ◆ パスワードの変更セルフサービスをユーザに提供する
- ◆ パスワードを忘れた場合のセルフサービス (本人確認の回答の入力を促すメッセージの表示、パスワードヒントの表示、パスワード変更の許可など) をユーザが利用できるようにする
- ◆ 本人確認の質問セルフサービスをユーザが利用できるようにする
- ◆ パスワードのヒントセルフサービスをユーザが利用できるようにする

19.1.2 eDirectory で必要な設定

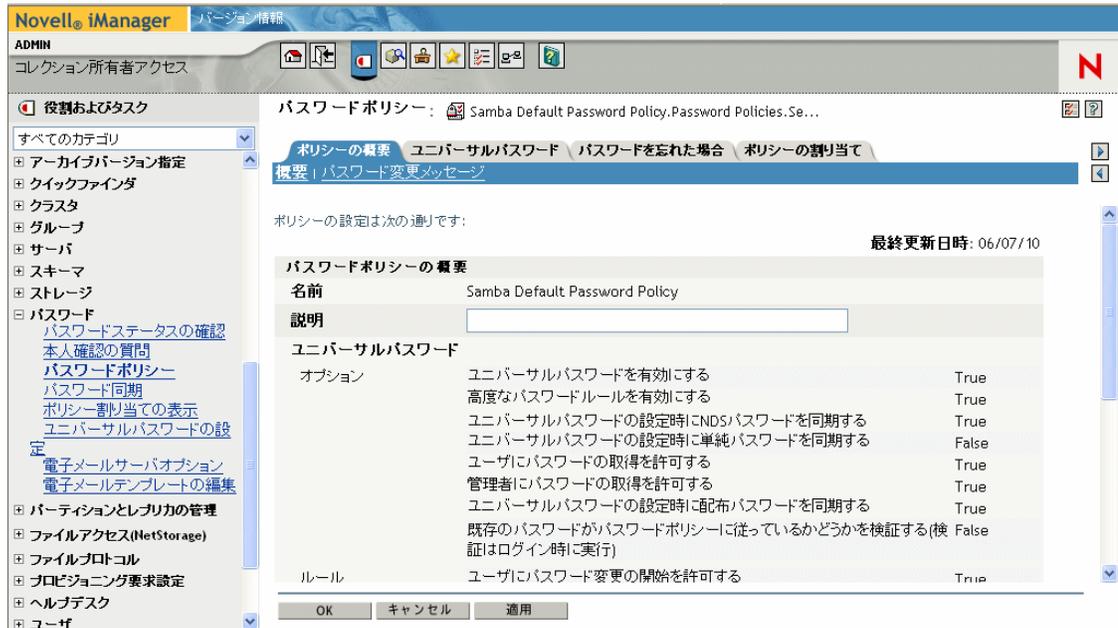
主なパスワードセルフサービスおよびユーザ認証機能を使用する前に、eDirectory で次の操作を実行する必要があります。

- ◆ ユニバーサルパスワードを有効にする
- ◆ 1 つまたは複数のパスワードポリシーを作成する

- ◆ ユーザに適切なパスワードポリシーを割り当てる

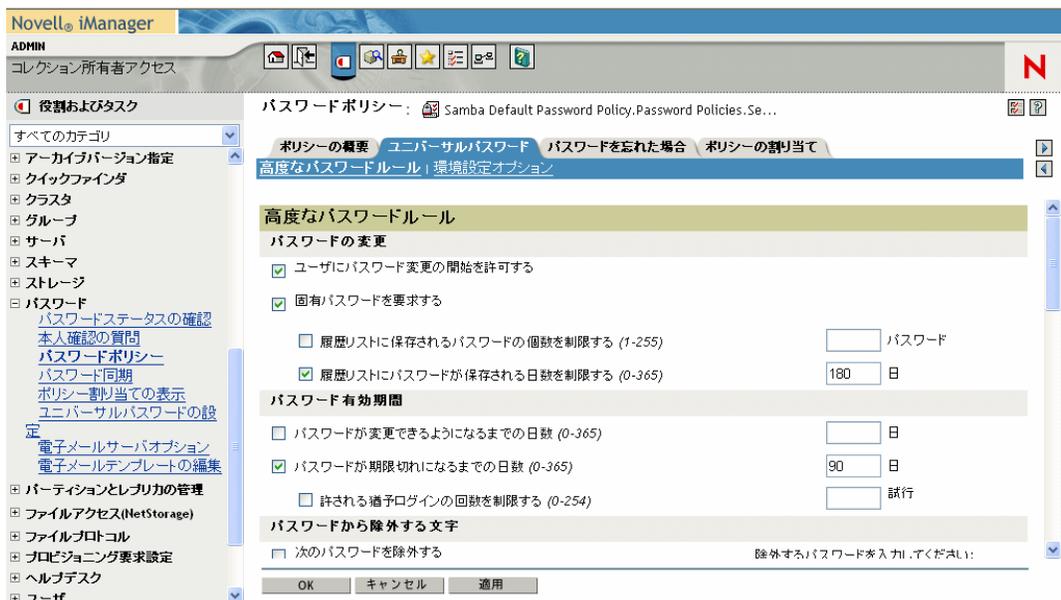
パスワードポリシーは管理者が定義するルールのコレクションで、ユーザパスワードの作成および変更時に基準を指定する目的で使用されます。Novell Identity Manager では、NMAS (Novell Modular Authentication Service) を利用して、管理者が eDirectory のユーザに割り当てるパスワードポリシーを強制します。

必要な設定を行うには、Novell iManager を使用します。次に、iManager を使用した、DocumentationPassword ポリシーの定義例を示します。

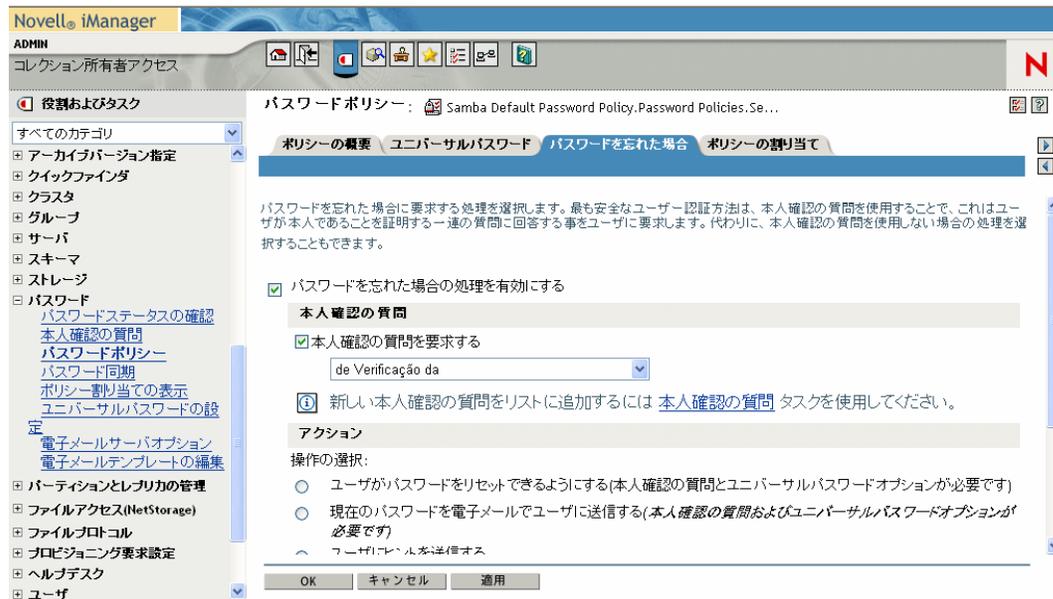


このパスワードポリシーは次の内容を指定します。

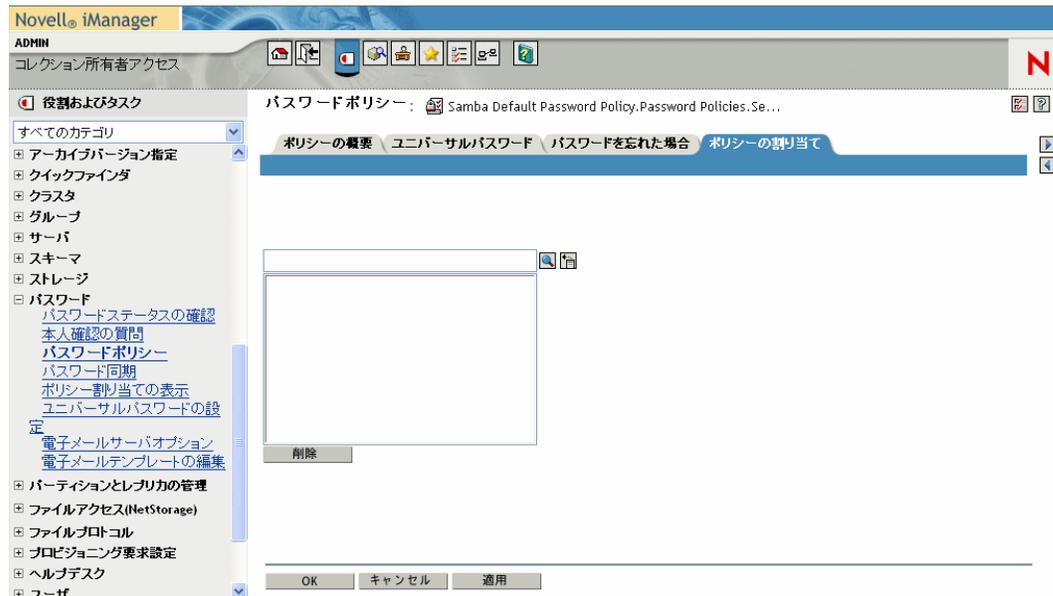
- ◆ ユニバーサルパスワード設定



◆ パスワードを忘れた場合の設定



◆ ポリシーを特定のユーザに適用する割り当て



eDirectory におけるユニバーサルパスワードおよびパスワードポリシーの設定の詳細については、『Novell Identity Manager 管理ガイド (<http://www.novell.com/documentation/dirxml20/index.html>)』を参照してください。

19.2 パスワードポートレットについて

パスワードセルフサービスおよびユーザ認証機能を Identity Manager ユーザアプリケーションに実装するには、次のポートレットを使用します。

ポートレット	説明
285 ページのセクション 19.3 「IDM ログイン」ポートレット	「IDM ログイン」はユニバーサルパスワード、パスワードポリシー、および NMAS を通して Identity Manager でサポートされる堅牢なユーザ認証を提供します。「IDM ログイン」ポートレットはログイン処理中、必要に応じて他のパスワードポートレットにリダイレクトします。
286 ページのセクション 19.4 「IDM 本人確認の回答」ポートレット	このセルフサービスポートレットで次のことを実行できます。 <ul style="list-style-type: none">◆ 管理者が定義する本人確認への有効な回答の設定、およびユーザが定義する本人確認の質問および回答の設定◆ 管理者が定義する本人確認の質問への有効な回答の変更、およびユーザが定義する本人確認の質問および回答の変更
288 ページのセクション 19.5 「IDM ヒントの設定」ポートレット	セルフサービスポートレットでは、パスワードのヒントを設定または変更できます。パスワードのヒントとは、ユーザがパスワードを忘れた場合の手がかりとして表示または電子メール送信されるヒントです。
289 ページのセクション 19.6 「IDM パスワードの変更」ポートレット	このセルフサービスポートレットを使用すると、ユーザは、割り当てられたパスワードポリシーに従って、ユニバーサルパスワードを変更 (リセット) できます。ポリシーを使用して、新しいパスワードが準拠すべきルールが示されます。 ユニバーサルパスワードが有効になっていない場合、このポートレットがユーザの eDirectory(シンプル) パスワードを変更します。このとき、ユーザのパスワード制限が適用されます。
291 ページのセクション 19.7 「IDM パスワードを忘れた場合」ポートレット	このセルフサービスポートレットは、本人確認の回答による認証を使用して、ユーザがパスワードについての情報を (NMAS から) 取得できるようにします。結果は割り当てられたパスワードポリシーにより異なりますが、次にその例を示します。 <ul style="list-style-type: none">◆ 画面上でのユーザのパスワードヒントの表示◆ ユーザへのヒントの電子メール送信◆ ユーザへのパスワードの電子メール送信◆ パスワードのリセット (変更) を促すメッセージの表示

19.2.1 パスワードセルフサービスポートレットのモード

パスワードセルフサービスポートレット (IDM 本人確認の回答、IDM ヒントの設定、および IDM パスワードの変更) は、次の 2 つのモードで動作します。

モード	説明	ランタイム時の動作
スタンドアロンモード	ポートレットは、共有ページ上にスタンドアロンで実行されます。	<ul style="list-style-type: none"> ◆ ポートレットの実行に成功した場合、操作を再実行するためのリンクおよび成功メッセージが表示されます。 ◆ ポートレットの実行に失敗した場合、エラーメッセージが既存のフォームで表示されます。
委任モード	ポートレットはログイン時の検証チェックの結果として、ページに表示されます。	<ul style="list-style-type: none"> ◆ ポートレットの実行に成功した場合、新しいポートレットまたはユーザアプリケーションのメインページにリダイレクトされます。成功メッセージは表示されません。 ◆ ポートレットの実行に失敗した場合、エラーメッセージが既存のフォームで表示されます。

19.3 「IDM ログイン」ポートレット

「IDM ログイン」ポートレットは、ユニバーサルパスワード、パスワードポリシー、およびNMASを通して、Identity Managerでサポートされる堅牢なユーザ認証を実行します。「IDM ログイン」ポートレットはログイン処理中、必要に応じて他のパスワードポートレットにリダイレクトします。

19.3.1 要件

「IDM ログイン」ポートレットの要件は次のとおりです。

トピック	要件
パスワードポリシー	高度なパスワードルールを使用したり、ユーザに [パスワードを忘れた場合] リンクを使用させたりする場合を除き、このポートレットにパスワードポリシーは不要です。

トピック	要件
ユニバーサルパスワード	高度なパスワードルールと共にパスワードポリシーを使用するのでない限り、このポートレットにユニバーサルパスワードは必要ありません。
SSL	このポートレットでは SSL を使用するため、LDAP レルムへの SSL 接続をサポートするようにアプリケーションサーバが適切に設定されていることを確認してください。

19.3.2 用途

「IDM ログイン」ポートレットを使用するには、次のことを理解しておく必要があります。

- ◆ [286 ページの「「IDM ログイン」が他のポートレットにリダイレクトする方法](#)
- ◆ [286 ページの「猶予ログインを使用する」](#)

「IDM ログイン」が他のポートレットにリダイレクトする方法

ランタイム時、「IDM ログイン」ポートレットはログイン処理を完了するのに必要な条件に従って、他のパスワードポートレットにリダイレクトします。次に例を示します。

ユーザの状況	「IDM ログイン」のリダイレクト先
[パスワードを忘れた場合] リンクをクリックする	291 ページのセクション 19.7 「「IDM パスワードを忘れた場合」ポートレット
本人確認の質問と回答を設定する	286 ページのセクション 19.4 「「IDM 本人確認の回答」ポートレット
パスワードヒントを設定する	288 ページのセクション 19.5 「「IDM ヒントの設定」ポートレット
無効なパスワードをリセットする	289 ページのセクション 19.6 「「IDM パスワードの変更」ポートレット

猶予ログインを使用する

猶予ログインを使用すると、「IDM ログイン」ポートレットにより、パスワードの変更を要求する警告メッセージと猶予ログインの残り回数が表示されます。猶予ログインの残り回数がなくなると、「IDM ログイン」ポートレットは、「IDM パスワードの変更」ポートレットにリダイレクトします。

19.4 「IDM 本人確認の回答」ポートレット

このセルフサービスポートレットで次のことを実行できます。

- ◆ 管理者が定義する本人確認への有効な回答の設定、およびユーザが定義する本人確認の質問および回答の設定
- ◆ 管理者が定義する本人確認の質問への有効な回答の変更、およびユーザが定義する本人確認の質問および回答の変更

19.4.1 要件

「IDM 本人確認の回答」 ポートレットの要件を次に示します。

トピック	要件
パスワードポリシー	このポートレットではパスワードを忘れた場合のセルフサービスが有効で、本人確認の質問と回答が設定されているパスワードポリシーを必要とします。
ユニバーサルパスワード	このポートレットでは、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。
eDirectory の設定	<p>このポートレットでは、ログインユーザが属すコンテナのユーザアプリケーション管理者にスーパーバイザ権が付与されている必要があります。これらの特権を持つユーザは、本人確認の回答をシークレットストアに書き込むことができます。</p> <p>たとえば、LDAP レルム管理者が <code>cn=admin, ou=sample, n=novell</code> と設定されており、ユーザが <code>cn=user1, ou=testou, o=novell</code> としてログインする場合を想定します。この場合、<code>cn=admin, ou=sample, n=novell</code> を <code>testou</code> のトラスティとして割り当て、[All attribute rights] にスーパーバイザ権を付与する必要があります。</p>

19.4.2 用途

「IDM 本人確認の回答」 ポートレットを使用するには、次のことを理解しておく必要があります。

- ◆ 288 ページの「ログイン時の「IDM 本人確認の回答」ポートレットの動作」
- ◆ 288 ページの「ユーザアプリケーション上での「IDM 本人確認の回答」ポートレットの動作」

ログイン時の「IDM 本人確認の回答」ポートレットの動作

ログイン中、ユーザが本人確認の質問および回答を設定する必要がある場合には必ず、[\(285 ページ\)](#)「IDM ログイン」ポートレットは自動的に「IDM 本人確認の回答」ポートレットにリダイレクトします。たとえば、管理者が iManager でユーザにパスワードポリシーを割り当てた後に初めてそのユーザがアプリケーションにログインしようとする場合がこれに当たります。このパスワードポリシーでは、[パスワードを忘れた場合] 機能を有効にし、本人確認の質問と回答を設定しておく必要があります。

ユーザアプリケーション上での「IDM 本人確認の回答」ポートレットの動作

ユーザアプリケーションでは、デフォルトで、本人確認の質問と回答を変更するためのセルフサービスが有効になっています。

19.5 「IDM ヒントの設定」ポートレット

セルフサービスポートレットでは、パスワードのヒントを設定または変更できます。パスワードのヒントとは、ユーザがパスワードを忘れた場合の手がかりとして表示または電子メール送信されるヒントです。



19.5.1 要件

「IDM ヒントの設定」ポートレットの要件を次に示します。

トピック	要件
パスワードポリシー	このポートレットではパスワードを忘れた場合のセルフサービスが有効で、本人確認の質問と回答が設定されているパスワードポリシーを必要とします。
ユニバーサルパスワード	このポートレットでは、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。

19.5.2 用途

「IDM ヒントの設定」ポートレットを使用するには、次のことを理解しておく必要があります。

- ◆ [289 ページ](#)の「ログイン時の「IDM ヒントの設定」ポートレットの使用方法」

- ◆ 289 ページの「ユーザアプリケーションページ上で「IDM ヒントの設定」ポータルレットを使用する」

ログイン時の「IDM ヒントの設定」ポータルレットの使用方法

ログイン中、ユーザがパスワードのヒントを設定する必要がある場合には必ず、(285 ページ)「IDM ログイン」ポータルレットは自動的に「IDM ヒントの設定」ポータルレットにリダイレクトします。たとえば、管理者が iManager でユーザにパスワードポリシーを割り当てた後に初めてそのユーザがアプリケーションにログインしようとする場合がこれに当たります。このパスワードポリシーでは、[パスワードを忘れた場合] が有効になり、[ユーザにヒントを送信する] アクションか [ヒントをページに表示] アクションが設定されます。

ユーザアプリケーションページ上で「IDM ヒントの設定」ポータルレットを使用する

デフォルトで、ユーザアプリケーションではパスワードヒントを変更するためのセルフサービスが有効になっています。

19.6 「IDM パスワードの変更」ポータルレット

このセルフサービスポータルレットを使用すると、ユーザは、割り当てられたパスワードポリシーに従って、ユニバーサルパスワードを変更(リセット)できます。ポリシーを使用して、新しいパスワードが準拠すべきルールが示されます。

ユニバーサルパスワードが有効になっていない場合、このポータルレットがユーザの eDirectory(シンプル) パスワードを変更します。このとき、ユーザのパスワード制限が適用されます。

識別セルフサービス 要求と承認 管理 ログアウト ヘルプ

IDMパスワードの変更

パスワードの変更

次に新しいパスワードを入力してください:

パスワードには次のプロパティが必要です:

- パスワードの最小文字数: 4
- パスワードの最大文字数: 12

パスワードには数字を使用できます。

パスワードでは小文字と大文字が区別されます。

パスワードに特殊文字を使用できます。

古いパスワード:

新しいパスワード:

パスワードを再入力してください:

19.6.1 要件

「IDM パスワードの変更」ポータルレットの要件を次に示します。

トピック	要件
ディレクトリ抽象化レイヤの設定	このポートレットでは、ディレクトリ抽象化レイヤの設定は必要ありません。
パスワードポリシー	ユニバーサルパスワードを有効にする高度なパスワードルールを使用するのではない限り、このポートレットでは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	<p>ユニバーサルパスワードにこのポートレットを使用する場合、ユーザに割り当てられたパスワードポリシーの高度なパスワードルールで、[ユーザにパスワード変更の開始を許可する] 設定を有効にする必要があります。</p> <p>このポートレットを eDirectory (シンプル) パスワードに使用する場合、ユーザのパスワード制限で、[Allow user to change password (ユーザにパスワードの変更を許可する)] 設定を有効にする必要があります。</p>

19.6.2 用途

「IDM パスワードの変更」ポートレットを使用するには、次のことを理解しておく必要があります。

- ◆ [290 ページ](#)の「ログイン時の「IDM パスワードの変更」ポートレットの使用方法」
- ◆ [291 ページ](#)の「ユーザアプリケーションページ上で「IDM パスワードの変更」ポートレットを使用する」

ログイン時の「IDM パスワードの変更」ポートレットの使用方法

ログイン処理中、無効なパスワードをリセットする必要がある場合には必ず、[\(285 ページ\)](#)「IDM ログイン」ポートレットは自動的に「パスワードの変更」ポートレットにリダイレクトします。たとえば、管理者により、パスワードのリセットが必要なパスワードポリシーが実装された後に初めてユーザがアプリケーションにログインしようとした場合がこれに当たります。

ユーザに割り当てられたパスワードポリシーで、パスワードを忘れた場合のアクションとしてパスワードのリセットが指定されている場合、[\(291 ページ\)](#)「IDM パスワードを忘れた場合」ポートレットは自動的に「IDM パスワードの変更」ポートレットにリダイレクトします。

ユーザアプリケーションページ上で「IDM パスワードの変更」ポートレットを使用する

デフォルトで、ユーザアプリケーションでは、「IDM パスワードの変更」ポートレットを使用したパスワードの変更セルフサービスが有効になっています。次に例を示します。

19.7 「IDM パスワードを忘れた場合」ポートレット

このセルフサービスポートレットは、本人確認の回答認証を使用し、ユーザがパスワードについての情報を取得できるようにします。結果は割り当てられたパスワードポリシーにより異なりますが、次にその例を示します。

- ◆ 画面上へのユーザのパスワードヒントの表示
- ◆ ユーザへのヒントの電子メール送信
- ◆ ユーザへのパスワードの電子メール送信
- ◆ パスワードのリセット (変更) を促すメッセージの表示

19.7.1 要件

「IDM パスワードを忘れた場合」ポートレットの要件は次のとおりです。

トピック	要件
パスワードポリシー	このポートレットではパスワードを忘れた場合のセルフサービスが有効で、本人確認の質問と回答が設定されているパスワードポリシーを必要とします。

トピック	要件
ユニバーサルパスワード	このポートレットでは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。ただし、パスワードのリセット、またはユーザへのパスワードの電子メール送信というパスワードを忘れた場合のアクションをサポートする場合は、この限りではありません。

19.7.2 用途

「IDM パスワードを忘れた場合」ポートレットを使用するには、次のことを理解しておく必要があります。

- ◆ 292 ページの「ログイン時の「IDM パスワードを忘れた場合」ポートレットの使用方法」
- ◆ 292 ページの「電子メールアクションのための環境設定」
- ◆ 293 ページの「「IDM パスワードを忘れた場合」ポートレットの初期設定」

ログイン時の「IDM パスワードを忘れた場合」ポートレットの使用方法

ログイン処理中に、ユーザが [パスワードを忘れた場合] リンクをクリックすると、(285 ページ) 「IDM ログイン」ポートレットは「IDM パスワードを忘れた場合」ポートレットにリダイレクトします。[IDM パスワードを忘れた場合] が表示されると、次のことが行われます。

- 1 username の入力を促すメッセージが表示されます。
- 2 ユーザについて本人確認の回答認証を実行するために、(285 ページ) 「IDM ログイン」ポートレットにリダイレクトします。
- 3 認証されたユーザに割り当てられているパスワードポリシーで指定された、パスワードを忘れた場合のアクションを実行します。次のいずれかを実行します。
 - ◆ ユーザがパスワードをリセットできるように (289 ページ) 「IDM パスワードの変更」ポートレットにリダイレクトする
 - ◆ パスワードまたはヒントをユーザに電子メールで送信する
 - ◆ ヒントを表示する

注: 「IDM パスワードを忘れた場合」ポートレットは、スタンドアロンで使用するものではありません。ユーザアプリケーションの共有ページには「IDM パスワードを忘れた場合」ポートレットを追加しないでください。このポートレットをページに配置すると、ユーザの認識または許可がないにもかかわらず無人コンピュータで何者かがパスワードを変更するという、セキュリティリスクが発生する可能性があります。

電子メールアクションのための環境設定

パスワードを忘れた場合の電子メールアクションをサポートする場合、電子メール通知サーバを適切に設定する必要があります。

- 1 Web ブラウザを使用して eDirectory サーバの iManager にアクセスし、管理者としてログインします。
- 2 [Roles and Tasks (役割とタスク)] > [パスワード] の順にクリックし、[電子メールサーバオブション] を選択します。

3 適切な設定を指定し、[OK] をクリックします。

「IDM パスワードを忘れた場合」ポータルレットでは、2つの電子メールテンプレートが使用されます。これらのテンプレートには、iManager の [Roles and Tasks (役割とタスク)] > [パスワード] > [電子メールテンプレートの編集] からアクセスできます。次のような名前が付いています。

- ◆ Password hint request (パスワードヒントの要求)
- ◆ Your password request (パスワードの要求)

これらのテンプレートは、必要に応じて編集できます (ただし、構造は変更しないでください)。

「IDM パスワードを忘れた場合」ポータルレットの初期設定

「IDM パスワードを忘れた場合」ポータルレットの初期設定は次のとおりです。

初期設定	説明
login-sequence	使用する NMAS ログインシーケンスです。このバージョンでは、ポータルレットがサポートするのは「本人確認の回答」機能のみです。
ldap-sslport	使用するセキュア LDAP です。デフォルト値は「636」です。
allow-wildcard	ユーザ名にワイルドカードを使用できるかどうかを指定します。デフォルトは「false」です。
encoding	使用する文字のエンコードです。デフォルトは「utf-8」です。

リスト検索ポータルレットの参照

この章では、Identity Manager ユーザアプリケーションで使用するリスト検索ポータルレットの設定およびカスタマイズの方法について説明します。ここで取り扱う内容は次のとおりです。

- 295 ページのセクション 20.1 「リスト検索ポータルレットについて」
- 300 ページのセクション 20.2 「リスト検索ポータルレットの設定」

20.1 リスト検索ポータルレットについて

リスト検索ポータルレットを使用して、アイデンティティポールのコンテンツを検索したり表示したりすることができます。これは、Identity Manager ユーザアプリケーションの [識別セルフサービス] タブのディレクトリ検索アクションの基本となります。ディレクトリ検索アクションは、ユーザ、グループ、およびタスクグループの検索用に設定されます。ディレクトリ検索アクションを変更して、検索可能なオブジェクトおよび属性の範囲を変更することもできます。

次の例では、ディレクトリ検索アクションによる検索条件の定義を示します。



ユーザインタフェース要素	説明
検索対象	検索するオブジェクトのタイプを選択します。
この基準を使用	<p data-bbox="656 340 1393 396">このリストにあるコンテンツの定義の詳細については、302 ページのセクション 20.2.2 「リスト検索の初期設定」を参照してください。</p> <p data-bbox="656 415 1393 472">ドロップダウンメニューから属性および検索演算子を選択することにより、検索条件を定義します。</p> <p data-bbox="656 491 1414 583">[高度な検索] を選択した場合、複数の行と複数のブロックを、包含的 (AND) または排他的 (OR) のいずれかの検索条件グルーピングとして指定できます。</p>
検索	<p data-bbox="656 604 1370 661">検索可能な属性の定義の詳細については、302 ページのセクション 20.2.2 「リスト検索の初期設定」を参照してください。</p> <p data-bbox="656 680 997 714">指定した検索条件を実行します。</p> <p data-bbox="656 732 1370 793">デフォルト検索の定義の詳細については、302 ページのセクション 20.2.2 「リスト検索の初期設定」を参照してください。</p>
マイ保存済み検索	以前に保存した検索の実行、編集、または削除を行うことができます。
 マイ保存済み検索	
高度な検索	<p data-bbox="656 932 1409 1045">[検索] ボタンと同様、行またはブロックを検索条件として追加できます。詳細検索では、複数の行および複数のブロックを、包含的 (AND) または排他的 (OR) のいずれかの検索条件グルーピングとして指定できます。</p> <p data-bbox="656 1064 1370 1121">検索可能な属性の定義の詳細については、302 ページのセクション 20.2.2 「リスト検索の初期設定」を参照してください。</p>
 高度な検索	

次の例は、「A で開始する名」の検索条件を指定した後に表示されたポートレットを示しています (サンプルデータを使用)。

The screenshot shows the Novell Identity Manager web interface. The main content area displays search results for users starting with 'A'. The search criteria are: ユーザ:(名 次で始まる a), ソート基準:姓, 合計一致件数:6. Below the criteria is a table with columns: 識別子, 位置, 組織, 名, 姓, 役職, 電子メール, 電話番号. The table contains 6 rows of user data. At the bottom of the interface, there are several action buttons: マイ保存済み検索, 検索の保存, エクスポートの結果, 検索の訂正, and 新規検索.

識別子	位置	組織	名	姓	役職	電子メール	電話番号
Allison	Chester	Manager					
Admin	Idmsample						
Admin	MacKenzie	Director, Marketing					(555) 555-1220
Allison	Quinn						
Allison	Ryan						
Allison	Sliggins	MIS					

次の機能を使用できるようにリスト検索ポートレットを設定することもできます。

ユーザインタフェース要素

説明

[識別子]、[位置]、[組織] の各タブ

これらのタブのいずれか 1 つをクリックすると、リストがそれぞれ別の方法で表示されます。

形式の詳細な説明については、[298 ページのセクション 20.1.1 「結果リストの表示形式について」](#)を参照してください。

マイ保存済み検索

以前に保存した検索を選択できます。



検索の保存

検索条件を保存し、必要に応じて保存した条件を再実行できます。検索は、現在ログオンしているユーザの `srvsrvQueryList` 属性に保存されます。



エクスポートの結果

検索結果を異なる形式にエクスポートできます。



検索の訂正

検索条件を変更できます。



新規検索

新しい検索を定義できます。



デフォルトでエンドユーザがリスト検索で実行できる操作を次に示します。

- ◆ 検索結果の印刷
- ◆ 結果リストからの電子メールの起動
- ◆ 結果リストからの詳細ポートレットの起動

20.1.1 結果リストの表示形式について

アイデンティティボールドから返されるデータの表示方法を定義できます。データは、次のページタイプに出力できます。

- ◆ 識別ページ — 通常、連絡先情報が記載されます。次に例を示します。



- ◆ 位置ページ — 通常、位置情報が記載されます。次に例を示します。

Novell Identity Manager

ようこそ, Admin

検索結果

下のタブを使用して結果セットのさまざまなビューを表示できます。

ユーザー: (名 次で始まる a)
ソート基準: リージョン
合計一致件数: 6

機別子	姓	組織	リージョン	電子メール	電話番号
Admin	Idmsample				
Admin	MacKenzie				(555) 555 1220
Allison	Quinn				
Allison	Chester				
Allison	Ryan				
Allison	Siggins				

1 - 6 / 6

マイ保存済み検索 | 検索の保存 | エクスポートの結果 | 検索の訂正 | 新規検索

- ◆ 組織ページ — 通常、組織階層情報が記載されます。次に例を示します。

Novell Identity Manager

ようこそ, Admin

検索結果

下のタブを使用して結果セットのさまざまなビューを表示できます。

ユーザー: (名 次で始まる a)
ソート基準: 部署
合計一致件数: 6

機別子	姓	組織	部署	マネージャ	電子メール
Admin	Idmsample				
Admin	MacKenzie		Director, Marketing		
Allison	Quinn				
Allison	Chester		Manager		
Allison	Ryan				
Allison	Siggins		MS		

1 - 6 / 6

マイ保存済み検索 | 検索の保存 | エクスポートの結果 | 検索の訂正 | 新規検索

ポートレットの複合初期設定を使用して、他の結果リスト形式を定義できます。たとえば、アイデンティティボールドスキーマに従業員のスキルまたは資格に関する情報が含まれている場合、結果リストにこの情報を表示するよう設定できます。

ポートレットの設定内容に従って、エンドユーザが実行できる操作を次に示します。

- ◆ 検索するアイデンティティボールドプロジェクトのタイプを選択する (ユーザ、グループなど)
- ◆ 検索する条件を指定する (「名が指定した文字で開始」、 「指定した文字を含む姓」 など)
- ◆ 検索結果を表示する表示形式を選択する
- ◆ ソート順を変更する

20.2 リスト検索ポートレットの設定

リスト検索ポートレットを設定するには、次の手順に従います。

ステップ	タスク	説明
1	次を定義します。 <ul style="list-style-type: none">◆ ユーザが検索できるエンティティおよび属性◆ 結果リストの表示方法	<p>Identity Manager ユーザアプリケーションのインストール時に同時にインストールされる事前定義されたディレクトリ検索アクションをそのまま使用できます。アクションは、変更することも、独自に作成することもできます。</p> <p>詳細については、302 ページのセクション 20.2.2 「リスト検索の初期設定」 を参照してください。</p>
2	検索のためのエンティティおよび属性のセットが、ディレクトリ抽象化レイヤで定義されていることを確認します。	詳細については、 75 ページの第 4 章 「ディレクトリ抽出化レイヤの設定」 を参照してください。
3	ポートレットにユーザがアクセスする方法を決定します。	このポートレットを既存ページから起動できるようにするか、新しいページから起動できるようにするか、
4	ポートレットの初期設定を指定します。	このポートレットを既存ページから起動できるようにするか、新しいページから起動できるようにするか、
5	設定をテストします。	結果リストに、目的の属性が表示されていることを確認します。

ス テッ プ	タスク	説明
6	eDirectory の権利を設定し、パフォーマンス向上にインデックスが有効であれば、インデックスを構築します。	<p>eDirectory の権利： 検索を実行するには：</p> <ul style="list-style-type: none"> ◆ 検索を実行するユーザには、検索対象のユーザまたはオブジェクトに対する参照権が必要です。 <p>検索を保存するには (管理者以外のユーザの場合)：</p> <ul style="list-style-type: none"> ◆ 検索を実行する部門または組織のトラスティである必要があります。 ◆ ユーザには、書き込み権、自己権、およびスーパーバイザ権が必要です。 <p>パフォーマンスの向上—検索のパフォーマンスを向上させるには、eDirectory の値インデックスを、検索で基になる属性に追加します。</p>

さまざまな結果リスト形式の定義の詳細については、[302 ページのセクション 20.2.2 「リスト検索の初期設定」](#)を参照してください。

20.2.1 ディレクトリ抽象化レイヤの設定

検索条件ドロップダウンリストから選択するエンティティおよび属性、およびアイデンティティポルト検索から返されるデータは、ディレクトリ抽象化レイヤで定義されている必要があります。次の表に、リスト検索で使用するエンティティおよび属性について設定の必要があるプロパティを示します。

定義タイプ	設定	ディレクトリ抽象化レイヤの値
entity (エンティティ)	view (表示)	選択 (true)

定義タイプ	設定	ディレクトリ抽象化レイヤの値
attribute (属性)	enable (有効)	選択 (true)
	search (検索)	選択 (true)
	hide (非表示)	非選択 (false)

「false」の場合、この属性の検索を定義できないか、この属性を結果リスト形式に含めることができません。

「search」が選択されている (true の状態) 属性については、「hide」が非選択 (false の状態) でなければなりません。リスト検索ポートレットは、検索時に「hide」プロパティの値を確認しないためです (パフォーマンスの低下を防ぐため)。

たとえば、eDirectory で User1 が HomePhone 属性を、hide=true と設定していると想定します。HomePhone は検索可能であるためリスト検索はレコードを取得しますが、他の属性値は確認しません (確認した場合、パフォーマンスに影響を与える可能性があるため)。結果、他のユーザが HomePhone 属性について完全一致検索を実行した場合、非表示のレコードは結果リストに表示されないこととなります。

ディレクトリ抽象化レイヤのその他の設定 ディレクトリ抽象化レイヤのデータタイプ、形式タイプ、フィルタ、および検索範囲も、リスト検索ポートレットに影響を与えます。データタイプおよび形式タイプは外観に影響を与え、フィルタおよび検索範囲は返されるデータの個数に影響します。

詳細については、[87 ページのセクション 4.3 「エンティティおよび属性の操作」](#) を参照してください。

20.2.2 リスト検索の初期設定

次に示す 2 つのタイプの初期設定を定義します。

- ◆ [303 ページの「検索の初期設定」](#)
- ◆ [305 ページの「結果リスト形式の初期設定」](#)

検索の初期設定

検索の初期設定は、1つの初期設定ページに含まれています。

[この登録インスタンスのコンテンツ初期設定を変更します \(リスト検索\)](#)

リスト検索

初期設定	選択値	要求	読み込み専用	非表示																		
リセット デフォルトモード:	<input type="text" value="My Saved Searches"/>	詳細 <input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>																		
<table border="1"><thead><tr><th colspan="3">選択項目</th></tr><tr><th>値</th><th>表示</th><th></th></tr></thead><tbody><tr><td>MODE_SIMP</td><td>Basic Search</td><td>挿入 削除</td></tr><tr><td>MODE_ADV</td><td>Advanced Se</td><td>挿入 削除</td></tr><tr><td>MODE_SAVE</td><td>My Saved Se</td><td>挿入 削除</td></tr><tr><td colspan="3" style="text-align: center;">追加</td></tr></tbody></table>					選択項目			値	表示		MODE_SIMP	Basic Search	挿入 削除	MODE_ADV	Advanced Se	挿入 削除	MODE_SAVE	My Saved Se	挿入 削除	追加		
選択項目																						
値	表示																					
MODE_SIMP	Basic Search	挿入 削除																				
MODE_ADV	Advanced Se	挿入 削除																				
MODE_SAVE	My Saved Se	挿入 削除																				
追加																						
リセット ページ番号付け:	<input type="text" value="10"/>	詳細 <input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>																		
<table border="1"><thead><tr><th colspan="2">範囲</th></tr><tr><th>最小</th><th>最大</th></tr></thead><tbody><tr><td><input type="text"/></td><td><input type="text"/></td></tr></tbody></table>					範囲		最小	最大	<input type="text"/>	<input type="text"/>												
範囲																						
最小	最大																					
<input type="text"/>	<input type="text"/>																					
リセット 結果制限:	<input type="text" value="0"/>	詳細 <input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>																		
<table border="1"><thead><tr><th colspan="2">範囲</th></tr><tr><th>最小</th><th>最大</th></tr></thead><tbody><tr><td><input type="text"/></td><td><input type="text"/></td></tr></tbody></table>					範囲		最小	最大	<input type="text"/>	<input type="text"/>												
範囲																						
最小	最大																					
<input type="text"/>	<input type="text"/>																					
リセット 複合初期設定の検索とリスト:	カスタム初期設定の表示/編集	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>																		

検索の初期設定を次に示します。

初期設定	操作
デフォルトモード	<p>ユーザが最初にアクセスしたときのポートレットの表示方法を指定します。次の値があります。</p> <p>基本検索 — ユーザは検索条件を1つだけ指定できます。次に例を示します。</p> <p>First Name starts with A</p> <p>高度な検索 — 1つまたは複数の検索ブロックに、複数の検索条件を定義できます。検索条件または検索ブロックで、and と or の論理演算子を使用できます。たとえば、次のような検索を作成できます。</p> <p>(First Name starts with A or First Name starts with B) and (Region = Northeast or Region = Southeast)</p> <p>または</p> <p>(First Name starts with A and Last Name starts with B) or (First Name starts with B and Last Name starts with A)</p> <p>マイ保存済み検索 — 現在ログインしているユーザによって保存された検索のリストを表示します。検索は、ユーザの <code>srvprvQueryList</code> 属性に保存されます。</p> <hr/> <p>注: ランタイム時に検索の実行または編集を行うか、ポートレットの下部にあるボタンをクリックすると、これらのモードのいずれかにアクセスできます。</p>
ページ番号付け	一度に表示できる最大行数を指定します。
結果制限	検索によって返される最大一致件数を指定します。0 に設定している場合は、ディレクトリ抽象化レイヤの設定に従います。
複合初期設定の検索とリスト	<p>次の条件で絞り込む場合にクリックします。</p> <ul style="list-style-type: none"> ◆ 検索するエンティティ ◆ 結果セットタイプ ◆ ページに含める属性および表示する順序 <p>デフォルトでは、ディレクトリ抽象化レイヤに属性 <code>view=true</code> で表示されるオブジェクトは、検索に含まれます。エンティティの属性リストは、ディレクトリ抽象化レイヤに表示され、<code>enable=true</code> と定義されている属性を基にしています。</p>

結果リスト形式の初期設定

複合初期設定ページで、検索に含めるエンティティ、および結果リスト形式を定義できます。デフォルトの初期設定ページ例を次に示します。

コンテンツ 初期設定Identity Manager

この登録インスタンスのコンテンツ初期設定を変更します (リスト検索)

リスト検索

複合初期設定の検索とリスト

リスト検索

概要

エンティティ定義	ユーザ		✖
電子メールをアイコンとして表示	<input checked="" type="radio"/> true <input type="radio"/> False		
結果リストタイプ	デフォルト		+
識別子	<input checked="" type="radio"/>	ソート	✖
属性名	<input type="radio"/>		✎
姓	<input checked="" type="radio"/>		
役職	<input type="radio"/>		
電子メール	<input type="radio"/>		
電話番号	<input type="radio"/>		
位置	<input type="radio"/>	ソート	✖
属性名	<input type="radio"/>		✎
姓	<input type="radio"/>		
リージョン	<input checked="" type="radio"/>		
電子メール	<input type="radio"/>		
電話番号	<input type="radio"/>		
組織	<input type="radio"/>	ソート	✖
属性名	<input type="radio"/>		✎
姓	<input type="radio"/>		
役職	<input type="radio"/>		

[リストビューに戻る](#)

複合初期設定に含まれる設定項目は次のとおりです。

初期設定	操作
エンティティ定義	<p>検索に有効なオブジェクト (view=true) にはそれぞれ、対応する [エンティティ定義] ブロックがあります。これらの初期設定は、次の目的に使用します。</p> <ul style="list-style-type: none"> ◆ 検索に含めるオブジェクトを定義します。 ◆ 結果リスト形式の定義を変更します (表示する属性の追加および削除、およびデフォルトのソート順など)。 ◆ [エンティティ定義] 行の削除ボタンをクリックし、検索に含めないオブジェクトを削除します。これにより、対応する [エンティティ定義] ブロック全体が削除されます。 <p>オブジェクトを後で再び表示するには、[エンティティ定義の追加] (ページ下部) をクリックし、ウィザードの選択パネルの指示に従います。</p> <hr/> <p>ヒント: あるオブジェクトがこのリストに表示されず、ディレクト抽象化レイヤのリストには表示されている場合、そのエンティティオブジェクトの「view」修飾を確認します。「false」に設定されている場合、識別ポートレットはそのエンティティを使用できません。</p>
電子メールをアイコンとして表示	<p>[true] に設定されており、Email 属性が結果リストで指定されている場合、アイコンとして表示されます。[false] に設定されている場合、Email 属性は、完全な電子メールアドレスで表示されます。Email 属性は (テキストの場合もアイコンの場合も)、クリック可能な mailto: リンクです。</p>
結果リストタイプ (デフォルト)	<p>現在のエンティティについて、結果リストのデフォルト形式を指定します。デフォルトは、現在のユーザが別の形式を選択しない場合にのみ使用されます。</p>
結果リストの表示形式ブロック	<p>表示形式 ([識別]、[位置]、[組織] の各ページなど) を指定し、結果リストに含める属性のセットを指定します。</p> <p>結果リストタイプを削除するには：</p> <ul style="list-style-type: none"> ◆ 結果リストタイプの横にある削除ボタンをクリックします。 <p>これにより、そのページタイプおよびすべての関連属性が検索から削除されます。</p> <p>結果セットページを追加するには：</p> <ul style="list-style-type: none"> ◆ 展開ボタンをクリックし、結果セット形式を選択リストから選択します。

初期設定	操作
属性	<p>特定の表示形式で表示する属性のセットを指定します。</p> <p>属性を追加または削除するには：</p> <ul style="list-style-type: none"> ◆ [Modify Attributes (属性の変更)] ボタンをクリックします。 ◆ 属性を追加するには、使用可能な属性のリストから対象の属性を選択します。 ◆ 矢印をクリックして、属性を [選択済み] リストに移動します。属性を結果リストから削除するには、逆の手順を実行します。 ◆ 属性リストを並べ替えるには、[選択済み] リストの右にある上下の矢印をクリックします。 ◆ [送信] をクリックします。 <p>属性とデータタイプ — 属性のデータタイプは、表示方法に影響します。たとえば、ローカルリストまたはグローバルリストのサブタイプとして属性が定義されている場合、指定できる値は、基本検索または高度な検索の条件画面のドロップダウンリストボックスに表示されます。タイプが DN である場合、基本検索または高度な検索の条件画面でユーザが値を選択できるように、[finder and history (検索および履歴)] ボタンが表示され、DN は、結果リストの形式でユーザにわかりやすいように表示されます。データタイプおよびサブタイプは、有効な比較のみが作成されるよう、表示する比較演算子も制限します。</p> <p>詳細については、75 ページの第 4 章「ディレクトリ抽出化レイヤの設定」を参照してください。</p>
結果リスト表示形式ブロックのソート	<p>この属性に基づく結果リストのソート順を指定します。デフォルトのソート順は、結果セットタイプが現在のユーザセッションの表示形式でない場合にのみ有効です。</p> <p>単一値属性および複数値属性 — 結果リストに表示されるレコードの件数は、ソート属性が単一値をとるか、複数値をとるかにより異なります。複数値属性をソートすると、通常、一致件数の合計は同じでもレコード数は多くなります。これは、複数値属性の値がそれぞれ 1 行ずつ表示されるためです。</p>

初期設定パネルの設定の完了

有効なエントリが送信されていることを確認するには、[送信] をクリックします。エントリが有効でない場合、初期設定ページの上部にエラーメッセージが表示されます。エラーが解決できたら、[リストビューに戻る]、[設定の保存] の順にクリックします。

プロビジョニング要求の設計と管理



次の章では、Identity Manager のプロビジョニングモジュールの使い方について説明します。

- ◆ 311 ページの第 21 章「ワークフローベースプロビジョニングの概要」
- ◆ 325 ページの第 22 章「プロビジョニング要求定義の設定」
- ◆ 347 ページの第 23 章「プロビジョニングワークフローの管理」

ワークフローベースプロビジョニングの概要

21

この章では、ワークフローベースのプロビジョニングについて説明します。ここで取り扱う内容は次のとおりです。

- 311 ページのセクション 21.1 「ワークフローベースのプロビジョニングについて」
- 321 ページのセクション 21.2 「プロビジョニングの設定および管理」
- 321 ページのセクション 21.3 「プロビジョニングのセキュリティ」

21.1 ワークフローベースのプロビジョニングについて

ワークフローベースのプロビジョニングは、Identity Manager の主要な機能で、組織のセキュアリソースへのユーザアクセスを管理するプロセスです。このようなリソースには、ユーザアカウント、コンピュータ、データベースなどのデジタルエンティティが含まれます。このリリースでは、プロビジョニングされたリソースは、Identity Manager エンタイトルメントにマップされるようになっています。

Identity Manager は、広範囲のプロビジョニング要求を処理できます。プロビジョニング要求は、組織のリソースへのアクセスを付与するまたは取り消すことを目的とした、ユーザまたはシステムからのアクションです。プロビジョニング要求は、Identity Manager ユーザアプリケーションからエンドユーザが直接開始することもできますし、アイデンティティポールド (eDirectory) で発生するイベントに対応して間接的に開始することもできます。

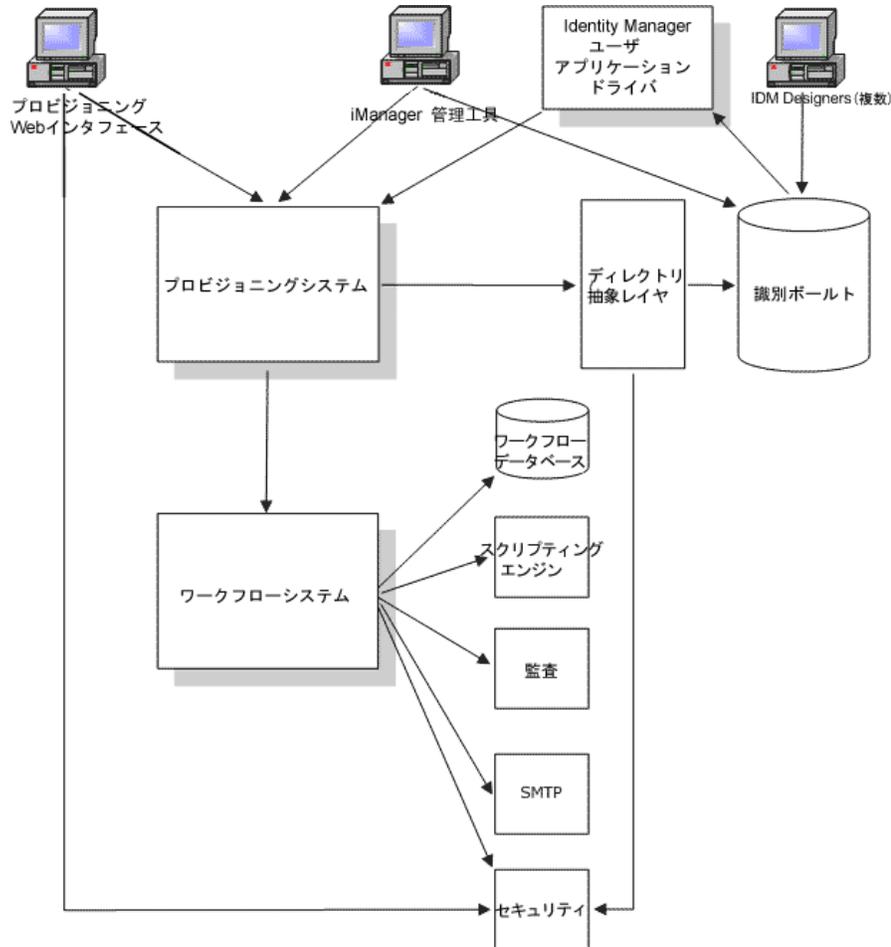
プロビジョニング要求に対して、組織内の 1 人以上の個人による承認が必要な場合、ワークフローが開始されます。このワークフローにより、リクエストの処理に必要な承認が調整されます。1 人の個人からの承認を必要とするプロビジョニング要求もあれば、複数の個人からの承認を必要とするプロビジョニング要求もあります。場合によっては、承認なしに実行できる要求もあります。

承認手順が順次実行されるシーケンシャル方式の処理を必要とするワークフローもあれば、パラレル処理をサポートするワークフローもあります。プロビジョニング要求を定義する際に、ワークフローがサポートする処理方式 (シーケンシャル方式かパラレル方式) を指定します。

Identity Manager には、管理者がユーザアプリケーションにプロビジョニング機能を組み込む際に利用できる Web ベースのツールセットが用意されています。これらのツールを使用して、プロビジョニング要求を設定したり、実行中のワークフローを管理したりできます。プロビジョニング要求を設定するには、管理者が、リソースをワークフローに関連付ける「プロビジョニング要求定義」を作成します。

21.1.1 上位レベルのアーキテクチャ

次の図は、Identity Manager に含まれる、ワークフローベースのプロビジョニングシステムでの上位レベルのアーキテクチャを示します。



次の節では、このアーキテクチャの各コンポーネントについて説明します。

プロビジョニング Web インタフェース

Identity Manager ユーザアプリケーションには、エンドユーザがプロビジョニング要求を送信したり、送信済みのリクエストを管理したりするための Web インタフェースが用意されています。また、ユーザアプリケーション管理者または組織マネージャが、プロビジョニングワークフローにおける委任ユーザとプロキシを割り当てられる機能も備わっています。

ヒント：プロビジョニングおよびワークフローのアクションは、Identity Manager ユーザアプリケーションの [要求と承認] タブで使用できます。

委任ユーザとプロキシの詳細な説明については、[321 ページのセクション 21.3 「プロビジョニングのセキュリティ」](#) を参照してください。ユーザアプリケーションの操作の詳細については、『Identity Manager ユーザアプリケーション：ユーザーズガイド』を参照してください。

iManager 管理ツール

iManager では、プロビジョニング要求およびそれに関連付けられたワークフローの設定および管理に使用するためのプラグインが用意されています。

プロビジョニング要求を設定するには、プロビジョニング要求をプロビジョニングされたリソースに関連付け、関連ワークフローのランタイム特性を指定し、リクエストを有効にします。プロビジョニング要求がいったん開始されると、iManager を使用して、ワークフロープロセスのステータスを表示したり、ワークフロー内のアクティビティを再割り当てしたり、応答のないワークフローを終了したりすることができます。

Identity Manager ユーザアプリケーションドライバ

プロビジョニングリソースへのエンドユーザ要求のサポートに加え、Identity Manager では、eDirectory で発生するイベントに対応してプロビジョニング要求を開始することもできます。Identity Manager のユーザアプリケーションドライバは、イベントをリッスンし、対応するプロビジョニング要求を開始することで応答します。これらのリクエストは、ワークフローを順番に開始して、承認プロセスを処理することができます。たとえば、eDirectory に新しいユーザが追加されると、自動的に事前定義されたプロビジョニング要求とワークフローを開始できます。

プロビジョニングシステム

プロビジョニングシステムは、プロビジョニング要求の開始と実行に必要なすべての処理を実行します。要求に 1 つ以上の承認が必要な場合、プロビジョニングシステムは、ワークフローを順番に呼び出して、ワークフロープロセスを開始します。必要な承認が付与された後、プロビジョニングシステムは、要求どおりにリソースのプロビジョニングを実行します。

プロビジョニングシステムは、アイデンティティポールド (eDirectory) に、使用可能なプロビジョニング要求と未処理のプロビジョニング要求に関する情報を保持します。

要求を開始する場合、またはリクエストの実行に必要な処理を実行する場合、システムはディレクトリ抽象化レイヤを使用してアイデンティティポールドにアクセスします。

ディレクトリ抽象化レイヤの詳細については、75 ページの第 4 章「ディレクトリ抽出化レイヤの設定」を参照してください。

ワークフローシステム

プロビジョニング要求が 1 つ以上の承認を必要とする場合、ワークフローシステムで承認プロセスが調整されます。ワークフローシステムは次のコンポーネントとのやり取りを行います。

- ◆ ワークフローデータベース
- ◆ スクリプトエンジン
- ◆ Audit
- ◆ SMTP
- ◆ セキュリティシステム

ワークフローデータベース

実行中のワークフローの状態を追跡できるように、ワークフローシステムは情報をデータベースに格納します。データベースには、ワークフロープロセスインスタンス、ワークリスト(キュー)、およびワークフロー宛先についての情報が格納されます。ワークフロープロセスの実行中に追加されたコメントも格納されます。

スクリプトエンジン

ワークフローに評価が必要な動的式が含まれている場合には必ず、ワークフローシステムは、スクリプトエンジンを呼び出します。動的式とは、変数、関数、演算子、およびディレクトリ抽象化レイヤのエンティティ参照を含むものを指します。

Novell Audit

ワークフロープロセスの状態をログとして記録する場合、ワークフローシステムは Novell Audit とのやり取りを行います。ワークフローは、実行中、発生するさまざまなイベントについての情報を記録できます。ログデータは、Novell Audit レポートングツールを使用して確認できます。

ログの設定の詳細については、[119 ページの第 5 章「ログの設定」](#)を参照してください。Identity Manager ユーザアプリケーションで生成するログメッセージのレベル制御の詳細については、[213 ページの第 12 章「ログの環境設定」](#)を参照してください。

SMTP

ワークフローシステムは、通常、実行中のさまざまなポイントで電子メール通知を送信します。たとえば、ワークフローアクティビティが新しい宛先に割り当てられる場合に、電子メールが送信されます。

管理者は、iManager で電子メールテンプレートを編集し、このテンプレートをワークフロープロセスで使用することができます。ランタイム時、ワークフローシステムは eDirectory からテンプレートを取得し、タグを通知に適した動的テキストに置き換えます。

電子メール通知は SMTP(Simple Mail Transfer Protocol) で処理されます。

電子メール通知に必要な基本的な設定手順については、[356 ページのセクション 23.3「電子メールサーバの設定」](#)および [357 ページのセクション 23.4「インストールされている電子メールテンプレートでの作業」](#)を参照してください。ワークフローのための電子メール通知の設定の詳細については、[338 ページの「ワークフローアクティビティの設定」](#)を参照してください。

セキュリティ

セキュリティシステムは、ワークフローベースのプロビジョニングアプリケーションのためのセキュリティをすべて処理します。

ワークフローセキュリティの詳細な説明については、[321 ページのセクション 21.3「プロビジョニングのセキュリティ」](#)を参照してください。

21.1.2 プロビジョニングおよびワークフローの例

IT システムのアカウントを必要とするユーザがいる場合を想定します。アカウントを設定するために、ユーザは Identity Manager ユーザアプリケーションを使用して要求を開始します。この要求によりワークフローが開始され、ワークフローにより承認プロセスが調整されます。必要な承認が付与されると、要求が実行されます。このプロセスには 3 つの基本ステップがあります。次にそれぞれについて説明します。

ステップ 1: 要求の開始

Identity Manager ユーザアプリケーションで、ユーザはリソースリストをカテゴリで参照し、プロビジョニングを行うリソースを 1 つ選択します。アイデンティティポータルで、選択したプロビジョニングされたリソースがプロビジョニング要求定義に関連付けられます。プロビジョニング要求定義は、プロビジョニングシステムで最も重要なオブジェクトになります。プロビジョニング要求定義は、リソースをワークフローに関連付け、ワークフロープロセスをエンドユーザに適用する役割を果たします。プロビジョニング要求定義は、ユーザに初期要求フォームを表示したり、初期要求に基づいてワークフローを開始したりするために必要なすべての情報を提供します。

この例では、ユーザは New Account リソースを選択します。ユーザが要求を開始すると、Web アプリケーションは、プロビジョニングシステムから初期要求フォームと、関連する初期要求データを取得します。プロビジョニングシステムは、プロビジョニング要求定義からこれらのオブジェクトを取得します。

プロビジョニング要求が開始されると、プロビジョニングシステムによってイニシエータと受信者が追跡されます。イニシエータとは、要求を作成した人のことです。受信者とは要求の対象になる人のことです。場合によっては、イニシエータと受信者が同じ人物になることもあります。

各プロビジョニング要求には、それぞれに関連付けられた操作があります。ユーザがリソースに対するアクセス権を付与するか取り消すかは操作で決まります。

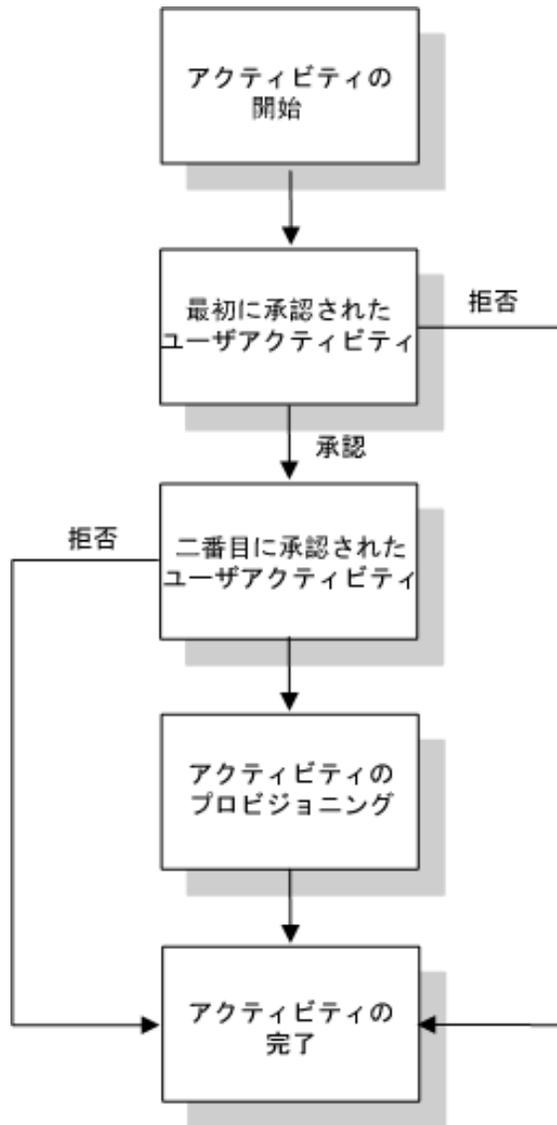
ステップ 2: 要求の承認

ユーザが要求を開始すると、プロビジョニングシステムはワークフロープロセスを開始します。ワークフロープロセスは、承認を調整します。この例では、2 つのレベルの承認が必要です。1 つはユーザのマネージャからの承認で、もう 1 つはマネージャのスーパーバイザからの承認です。承認がワークフロー内のユーザに拒否された場合、フローは終了し、要求は拒否されます。

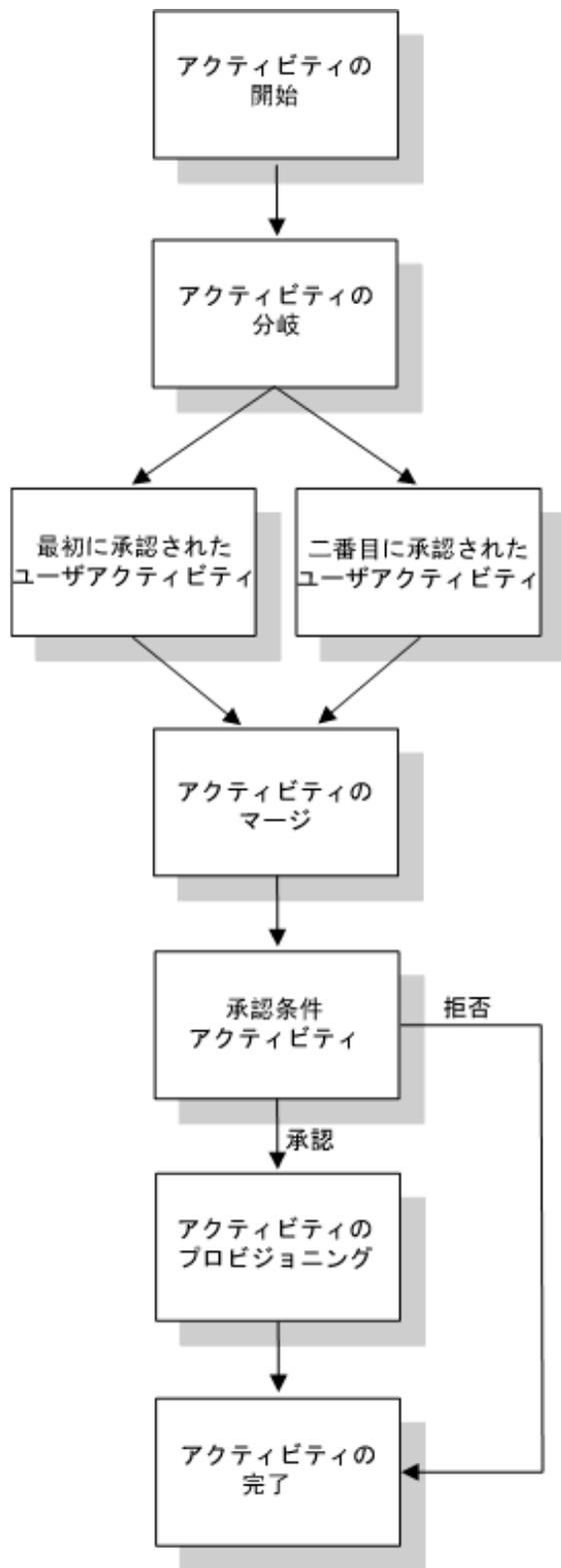
注 : Identity Manager には、最大 5 つまでのレベルのワークフロー承認をサポートするプロビジョニング要求テンプレートが用意されています。Identity Manager の後続リリースでは、Eclipse ベースの設計環境で、独自のカスタムワークフロープロセスを作成できるツールが提供されます。このリリースに付属のテンプレートの詳細については、[326 ページのセクション 22.2 「インストールされているテンプレートでの作業」](#)を参照してください。

ワークフローは、シーケンシャル方式またはパラレル方式のどちらの承認プロセスでも実行できます。シーケンシャルワークフローでは、各承認タスクが次の承認タスクの前に処理される形になります。パラレルワークフローでは、同時に複数の承認タスクを実行できます。

シーケンシャルフロー - 2度の承認で構成されるシーケンシャルワークフローの基本的な設計パターンを次に示します。



パラレルフロー - 2度の承認で構成されるパラレルワークフローの基本的な設計パターンを次に示します。



注：表示ラベル（「1次承認」、「2次承認」など）は、使用しているアプリケーション要件に合わせて簡単に変更できます。パラレルフローの場合、シーケンシャル処理であること

がわかりやすいラベルを指定することもできます。たとえば、「**パラレル承認 1/3**」、「**パラレル承認 2/3**」などのラベルを割り当てる必要があります。

ワークフロー定義は、次のコンポーネントで構成されます。

プロセスコンポーネント	説明
アクティビティ	<p>アクティビティとは、タスクを表すオブジェクトのことです。アクティビティは、ユーザに情報を表示したり、ユーザの応答に対応したり、ユーザには表示されないバックグラウンド機能を実行したりすることができます。</p> <p>先に示した例では、アクティビティはボックスで表示されています。</p> <p>Identity Manager ユーザアプリケーションでは、承認プロセスを処理するユーザアクティビティは、タスクと呼ばれます。[マイ作業] アクショングループの [マイタスク] をクリックすると、エンドユーザは、自分のキューにあるタスクリストを確認できます。特定のタスク用にどのワークフローアクティビティが処理されているかを確認するには、タスクを選択してから、[タスク詳細] フォームの [コメント履歴の表示] ボタンをクリックします。</p> <p>特定のプロビジョニング要求に対してどのワークフローアクティビティが処理されているかを確認するには、[マイリクエスト] をクリックして要求を選択してから、[リクエスト詳細] フォームの [コメントとフロー履歴の参照] ボタンをクリックします。</p> <p>[マイタスク] および [マイリクエスト] の各アクションの詳細については、『Identity Manager ユーザアプリケーション：ユーザーズガイド』を参照してください。</p>
リンク	<p>リンクは、ワークフローのアクティビティを相互に結びつけるものです。リンクは、2つのアクティビティ間でたどられるパスを示します。</p> <p>1つのアクティビティに、複数の着信リンクと複数の送信リンクを設定することができます。1つのアクティビティに複数の送信リンクがある場合、アクティビティの「結果」によって、選択されるリンクが決定されます。結果は、アクティビティにより実行される処理の最終結果です。たとえば、ユーザアクティビティは、ユーザが実行するアクションにより、承認という結果になる場合と、拒否という結果になる場合があります。</p> <p>先に示した例では、リンクは矢印で示されています。</p>

開始アクティビティ - ワークフロープロセスは、開始アクティビティの実行により開始されます。このアクティビティは、初期要求データを使用して、ワークドキュメントを開始します。また、イニシエータ、受信者などの複数のシステム値を関連付け、これらの値をスクリプト式で使用できるようにします。

ユーザアクティビティ - 開始アクティビティの実行が終了すると、ワークフローシステムはフロー内の最初のユーザアクティビティの処理に進みます。ユーザアクティビティは、ユーザのやり取りをサポートするアクティビティです。これらのやり取りを処理するために、ユーザアクティビティは、ユーザが要求を操作するためのフォームを表示します。先に示したワークフローの例では、**First approval** および **Second approval** がユーザアクティビティになります。ユーザアクティビティの表示ラベルはローカライズできます。

1つのユーザアクティビティで、次の1つまたは複数のアクションをサポートできます。

- ◆ 請求

- ◆ 承認
- ◆ 拒否
- ◆ 棄却
- ◆ 再割り当て (組織マネージャおよびユーザアプリケーション管理者のみ使用可能)

注: フォームに表示されるフィールドおよびボタンは、要求されるリソースおよびワークフローの設定方法により異なります。たとえば、「棄却」アクションは、製品付属のテンプレートの多くでサポートされていません。

ユーザアクティビティには、次の5つの結果があります。

- ◆ 承認済み
- ◆ 拒否
- ◆ 棄却
- ◆ エラー
- ◆ タイムアウト

注: 「エラー」と「タイムアウト」の結果は、ユーザがどのアクションも実行しなかった場合にも発生します。

ユーザが要求を承認すると、ワークフローは、フロー内の次のアクティビティに進みます。これ以上承認が必要なければ、リソースがプロビジョニングされます。ユーザが要求を拒否した場合は、作業アイテムがワークフロー内の次のアクティビティに転送され、要求は拒否されます。または、ユーザが組織マネージャまたはユーザアプリケーション管理者である場合には、タスクの再割り当てが可能です。すると、作業アイテムは別のユーザのキューに送られます。

注: 製品付属のプロビジョニング要求テンプレートは、要求が拒否された場合にワークフローを終了するよう設定されています。要求が拒否された場合、フローを終了する完了アクティビティに、作業アイテムが送られます。

ユーザアクティビティが割り当てられる人を「宛先」と呼びます。アクティビティの宛先に、割り当てられたタスクを電子メールで通知することもできます。アクティビティに関連付けられた作業を実行する場合、宛先になっているユーザは電子メールにある URL をクリックし、ワークリスト (キュー) からタスクを見つけ、タスクをリクエストします。

宛先ユーザは指定時間内にユーザアクティビティに応答する必要があります。応答しないとアクティビティでタイムアウトが発生します。通常、タイムアウト間隔は、ユーザが応答できるだけの十分な時間を時間単位または日数単位で指定します。

アクティビティのタイムアウトが発生した場合は、アクティビティに指定された再試行回数に従い、ワークフロープロセスは、アクティビティを再実行しようとします。場合によっては、ワークフロープロセスは、タイムアウトの発生したアクティビティを別のユーザにエスカレートすることもできます。この場合、このアクティビティは新しい宛先 (たとえばユーザのマネージャ) に再度割り当てられ、新しい宛先ユーザがこのアクティビティの作業を実行できるようにします。最後の再試行でタイムアウトが発生した場合、ワークフローの設定内容に従い、そのアクティビティは承認済みまたは拒否としてマークされます。

条件付きアクティビティ - ワークフロープロセスの実行中にテストが実行され、その結果をチェックすることで次の作業が決まる場合があります。条件付きアクティビティがこの機能を提供しています。条件付きアクティビティは、スクリプト式を使用して評価する式を定義します。前に示したワークフローの例では、**Approval Condition** が条件付きアクティビティです。

条件付きアクティビティには、次の3つの結果があります。

- ◆ True
- ◆ False
- ◆ エラー

ブランチアクティビティとマージアクティビティ - パラレル処理をサポートするワークフローでは、ブランチアクティビティにより、2人のユーザが作業アイテムの異なる領域を同時に作業できます。ユーザが作業を完了すると、マージアクティビティにより、フローに合流するブランチが同期化されます。

プロビジョニングアクティビティ - プロビジョニングアクティビティは、プロビジョニング要求を実行します。このアクティビティは、必要な承認がすべて付与された場合にのみ実行されます。

プロビジョニングステップの詳細については、[320 ページの「ステップ 3: 要求の実行」](#)を参照してください。

完了アクティビティ - 完了アクティビティは、ワークフローにおける最後のアクティビティです。フロー内のすべてのアクティビティが完了し、フローの最終結果が有効な場合、完了アクティビティを実行できます。ワークフローシステムは、完了アクティビティへのリンクを調べることにより、プロセスの最終状態を判別できます。承認リンクが完了アクティビティに到達している場合、フロー全体の状態は「承認済み」になります。他の結果 (拒否、タイムアウト、またはエラー) から完了アクティビティに入る場合、フロー全体の状態は「拒否」になります。

ワークフロープロセスが「承認済み」で完了アクティビティに到達している場合、承認プロセスが完了したことを示し、プロビジョニング要求を実行できます。

ステップ 3: 要求の実行

プロビジョニング要求が承認されると、ワークフローシステムはプロビジョニングのステップを開始できます。この時点で、制御はプロビジョニングシステムに戻ります。

プロビジョニングシステムは、プロビジョニング要求を実行する場合、**Identity Manager** エンタイトルメントを実行することも、**eDirectory** のオブジェクトとその属性を直接操作することもできます。プロビジョニングの処理中、プロビジョニングシステムは、プロビジョニングデータ定義に従って、関連オブジェクトを作成し、受信者側のプロビジョニングアクションの結果を記録します。ユーザの要求がある操作の付与か取り消しかによって、このアクションが受信者に対して属性値を設定するか、削除するか、あるいは、受信者の複数値属性に項目を追加するか、複数値属性から項目を削除するかは変わってきます。ここで使用される属性は **eDirectory** 属性です (受信者に補助クラスを追加することにより使用可能になる場合もあります)。属性値は単純タイプの場合と、プロビジョニングシステムが内部サブ属性の値を指定できる複合タイプの場合があります。

21.2 プロビジョニングの設定および管理

プロビジョニング要求定義を設定するには、iManager を使用してプロビジョニングされたリソースへの関連付けを行い、関連ワークフローのランタイム特性を指定し、定義を有効にします。Identity Manager には、事前展開済みのプロビジョニング要求定義とワークフローのセットが同梱されています。これらをテンプレートとして使用して、独自のプロビジョニングシステムを構築することもできます。インストール済みのテンプレートは、使いやすく、かつ広範囲のビジネス環境要件に対応できるようになっています。システムをセットアップするには、インストールされているテンプレートに基づいて新しいオブジェクトを定義してから、これらのオブジェクトを組織のニーズに合うようにカスタマイズします。

プロビジョニング要求定義が設定された後には、iManager を使用して、実行中のワークフロープロセスのステータスを表示したり、ワークフロー内のアクティビティを再割り当てしたり、応答のないワークフローを終了したりすることができます。

iManager を使用したプロビジョニングの設定および管理の詳細については、[325 ページの第 22 章「プロビジョニング要求定義の設定」](#) および [347 ページの第 23 章「プロビジョニングワークフローの管理」](#) を参照してください。

21.3 プロビジョニングのセキュリティ

ユーザが Identity Manager ユーザアプリケーションにログインすると、セキュリティシステムがそのユーザを認証し、プロビジョニングオブジェクトとワークフローオブジェクトにアクセス制御を設定し、これらのオブジェクトを不正使用から保護します。これにより、ユーザはアクセス権を付与されているプロビジョニング要求定義のみを表示することができます。ユーザアプリケーションの認証サービスおよび承認サービスに加え、セキュリティシステムはプロキシ割り当てと委任ユーザ割り当ても管理します。

- 「委任ユーザ」とは、他のユーザの代わりに作業を実行する権限を持つユーザのことです。委任ユーザの割り当ては、特定のプロビジョニング要求定義に適用されます。
- 「プロキシ」とは、1 人または複数のユーザ、グループ、またはコンテナのために任意の作業または全作業を実行できるユーザのことです。プロキシ割り当ては、委任ユーザ割り当てとは異なり、プロビジョニング要求定義に依存しないため、すべての作業および設定に適用されます。

ログが有効になっている場合、プロキシユーザまたは委任ユーザによって実行されたアクションは、他のユーザによって実行されたアクションと併せてすべてログに記録されます。ログメッセージ内では、プロキシユーザまたは委任ユーザによって実行されたアクションは、その旨が明確に示されます。また、プロキシ割り当てまたは委任ユーザ割り当てが新規に定義された場合、このイベントもログに記録されます。

電子メール通知を生成するようプロビジョニング要求定義が設定されている場合、宛先ユーザと同様にプロキシにも電子メール通知が行われます。ただし、委任ユーザには電子メール通知は行われません。

ワークフローのセキュリティの役割 - セキュリティシステムが認識するセキュリティの役割は、次のとおりです。

役割	説明	権利
ユーザアプリケーション管理者	完全な管理権限を持つ <code>locksmith</code> ユーザです。	<p>ユーザアプリケーション管理者が iManager で実行を許可されているタスクを次に示します。</p> <ul style="list-style-type: none"> ◆ プロビジョニング要求の設定 ◆ 実行中のワークフローの管理 <p>ユーザアプリケーション管理者がユーザアプリケーションで実行を許可されているタスクを次に示します。</p> <ul style="list-style-type: none"> ◆ すべてのワークフローキュー内にあるすべてのタスクの表示と編集 ◆ システム内のユーザに対するプロキシ割り当てと委任ユーザ割り当ての定義 ◆ システム内のユーザに対する非表示情報(非表示属性)の表示 ◆ タスクグループマネージャの作成とグループへの割り当て。タスクグループマネージャの作成および割り当てができるのは、ユーザアプリケーション管理者のみです。 <hr/> <p>注 : Identity Manager ユーザアプリケーションの [管理] タブには、ユーザアプリケーションを管理する権利を割り当てるためのツールが含まれています。このタブを使用するには、まず、インストール時にユーザアプリケーション管理者として指定したユーザでログオンする必要があります。</p> <hr/> <p>ユーザアプリケーションのセキュリティ機能の使用については、209 ページの第 11 章「セキュリティの環境設定」を参照してください。</p>

役割	説明	権利
組織マネージャ	<p>従業員の直属のスーパーバイザです。ユーザにはそれぞれ1人の組織マネージャが存在します。</p> <hr/> <p>ヒント: 組織マネージャは、管理マネージャとも考えることができます。</p>	<p>組織マネージャには、次のことが許可されています。</p> <ul style="list-style-type: none"> ◆ 自分のチームのワークフローキューにある全タスクの表示。この機能は管理階層の1つのレベルにのみ有効です。このため、組織マネージャのスーパーバイザはその組織マネージャの直属の部下のタスクを見ることはできません。 ◆ 直属の部下のタスクの編集。直属の部下のタスクが、タスクマネージャと組織マネージャの異なるグループに割り当てられている場合は例外です。この場合、組織マネージャはタスクを表示できますが、編集はできません。このタスクがエスカレーションされると、組織マネージャではなくタスクグループマネージャに移動します。 ◆ タスクの要求、要求の解除、自分のチームメンバーへのタスクの再割り当て。 ◆ 自分自身および自分のチームメンバーに対するプロキシおよび委任ユーザの定義。 ◆ 自分のチームメンバーに対する非表示属性の表示。
タスクグループマネージャ	<p>タスクグループに関連する一連のタスクを担当するユーザです。タスクグループは、LDAP グループオブジェクトの拡張です。タスクグループにはそれぞれ1人のタスクグループマネージャを割り当てることができます。</p> <p>タスクグループマネージャは、ユーザアプリケーション管理者によって割り当てられます。</p> <p>タスクがグループに割り当てられると、グループの <code>srvprvTaskManager</code> 属性には、指定されたタスクグループマネージャであるユーザの DN が指定されます。パフォーマンスを向上させるために、タスクグループマネージャは、ユーザオブジェクトの属性によっても特定されます。タスクグループマネージャに指定されたユーザの <code>srvprvIsTaskManager</code> 属性は「true」に設定されています。</p>	<p>タスクグループマネージャには、次のことが許可されています。</p> <ul style="list-style-type: none"> ◆ 自分がリーダーとして指定されたグループに割り当てられた全タスクの表示と編集。 <p>タスクグループマネージャは、次のことはできません。</p> <ul style="list-style-type: none"> ◆ リソースの作成と要求の撤回。 ◆ プロキシ関係または委任ユーザ関係の定義。 ◆ 自分のチームメンバーに対する非表示属性の表示。

注: ユーザはだれでも、自分の識別情報に関連付けられている非表示属性を表示できません。

プロキシ関係と委任ユーザ関係の定義 - ユーザのプロキシ割り当てを定義するには、**Identity Manager** ユーザアプリケーションの [要求と承認] タブの [チームのプロキシの割り当て] ページを使用します。委任ユーザの割り当てを定義するには、[チームの代理人の割り当て] ページを使用します。このページは、[要求と承認] タブからもアクセスできます。

タスクグループマネージャの作成 - タスクグループのタスクグループマネージャを定義するには、**Identity Manager** ユーザインタフェースの [識別セルフサービス] タブの [ユーザまたはグループの作成] ページを使用します。

タスクグループマネージャ、プロキシ、および委任ユーザの定義の詳細については、『**Identity Manager** ユーザアプリケーション: ユーザーズガイド』を参照してください。

プロビジョニング要求定義の設定

この章では、プロビジョニング要求定義の設定について説明します。ここで取り扱う内容は次のとおりです。

- ◆ 325 ページのセクション 22.1「プロビジョニング要求の環境設定プラグインについて」
- ◆ 326 ページのセクション 22.2「インストールされているテンプレートでの作業」
- ◆ 329 ページのセクション 22.3「プロビジョニング要求定義の設定」

22.1 プロビジョニング要求の環境設定プラグインについて

プロビジョニング要求定義を設定するには、iManager でプロビジョニング要求の環境設定プラグインを使用する必要があります。このプラグインにより、プロビジョニング要求定義をプロビジョニングされたリソースに関連付け、関連ワークフローのランタイム特性を指定し、定義を有効にできます。このリリースでは、プロビジョニングされたリソースは、Identity Manager エンタイトルメントにマップされるようになっています。

注：また、アイデンティティポールの属性に直接マップされているプロビジョニング要求定義を実行することもできます。ただし、インストールされているテンプレートはエンタイトルメントに基づくため、このタイプのリソースには対応していません。

プロビジョニング要求の環境設定プラグインは、iManager の [Identity Manager] カテゴリ内にあります。このプラグインでは、[プロビジョニング要求の環境設定] の役割に [プロビジョニング要求] タスクが含まれています。[プロビジョニング要求] タスクは、次のパネルで構成されます。

パネル	説明
プロビジョニングドライバの選択	Identity Manager ユーザアプリケーションのドライバを選択できます。ドライバには一連の事前展開済みのプロビジョニング要求定義が含まれているため、プロビジョニング要求の設定を開始する前にドライバを選択する必要があります。
プロビジョニング要求の環境設定	次の操作を実行できます。 <ul style="list-style-type: none"> ◆ 使用できるプロビジョニング要求定義を参照し、設定する定義を選択する。 ◆ 既存の定義に基づき、新しいプロビジョニング要求定義を作成する。 ◆ プロビジョニング要求定義のプロパティを設定する。 ◆ プロビジョニング要求定義をプロビジョニングされたリソースに割り当てる。 ◆ 関連ワークフロー内の各アクティビティについて、宛先とタイムアウト設定を編集する。 新しいプロビジョニング要求の作成または既存の要求の編集を選択すると、プラグインによりプロビジョニング要求の環境設定ウィザードが実行されます。

22.2 インストールされているテンプレートでの作業

Identity Manager には、事前展開済みのプロビジョニング要求定義とワークフローのセットが用意されています。これらをテンプレートとして使用し、独自のプロビジョニングシステムを構築できます。システムをセットアップするには、インストールされているテンプレートに基づいて新しいオブジェクトを定義してから、これらのオブジェクトを組織の要件を満たすようにカスタマイズします。

インストールされているテンプレートを使用して、要求を実行するのに必要な承認ステップの数を指定できます。次のステップで構成されるプロビジョニング要求を設定できます。

- ◆ 承認なし
- ◆ 1 次承認ステップ
- ◆ 2 次承認ステップ
- ◆ 3 次承認ステップ
- ◆ 4 次承認ステップ
- ◆ 5 次承認ステップ

シーケンシャル処理またはパラレル処理のどちらをサポートするか、および処理中にワークフローのタイムアウトが発生した場合に要求を承認するか拒否のかも指定できます。

ワークフロー設計パターンの詳細については、[315 ページのセクション 21.1.2 「プロビジョニングおよびワークフローの例」](#) を参照してください。

Identity Manager には次のテンプレートが用意されています。

テンプレート	説明
自己プロビジョニング承認	承認なしにプロビジョニング要求を実行できます。
ワンステップ承認 (タイムアウトと同時に承認する)	プロビジョニング要求の実行に、1 段階の承認を必要とします。アクティビティのタイムアウトが発生した場合、アクティビティは要求を承認し、作業アイテムは次のアクティビティに送られます。
ツーステップ順次承認 (タイムアウトと同時に承認する)	プロビジョニング要求の実行に、2 段階の承認を必要とします。アクティビティのタイムアウトが発生した場合、アクティビティは要求を承認し、作業アイテムは次のアクティビティに送られます。 このテンプレートはシーケンシャル処理をサポートします。
スリーステップ順次承認 (タイムアウトと同時に承認する)	プロビジョニング要求の実行に、3 段階の承認を必要とします。アクティビティのタイムアウトが発生した場合、アクティビティは要求を承認し、作業アイテムは次のアクティビティに送られます。 このテンプレートはシーケンシャル処理をサポートします。

テンプレート	説明
<p>フォーステップ順次承認 (タイムアウトと同時に承認する)</p>	<p>プロビジョニング要求の実行に、4 段階の承認を必要とします。アクティビティのタイムアウトが発生した場合、アクティビティは要求を承認し、作業アイテムは次のアクティビティに送られます。</p> <p>このテンプレートはシーケンシャル処理をサポートします。</p>
<p>ファイブステップ順次承認 (タイムアウトと同時に承認する)</p>	<p>プロビジョニング要求の実行に、5 段階の承認を必要とします。アクティビティのタイムアウトが発生した場合、アクティビティは要求を承認し、作業アイテムは次のアクティビティに送られます。</p> <p>このテンプレートはシーケンシャル処理をサポートします。</p>
<p>ワンステップ承認 (タイムアウトと同時に拒否する)</p>	<p>プロビジョニング要求の実行に、1 段階の承認を必要とします。アクティビティのタイムアウトが発生した場合、ワークフローは要求を拒否します。</p> <p>このテンプレートはシーケンシャル処理をサポートします。</p>
<p>ツーステップ順次承認 (タイムアウトと同時に拒否する)</p>	<p>プロビジョニング要求の実行に、2 段階の承認を必要とします。アクティビティのタイムアウトが発生した場合、ワークフローは要求を拒否します。</p> <p>このテンプレートはシーケンシャル処理をサポートします。</p>
<p>スリーステップ順次承認 (タイムアウトと同時に拒否する)</p>	<p>プロビジョニング要求の実行に、3 段階の承認を必要とします。アクティビティのタイムアウトが発生した場合、ワークフローは要求を拒否します。</p> <p>このテンプレートはシーケンシャル処理をサポートします。</p>
<p>フォーステップ順次承認 (タイムアウトと同時に拒否する)</p>	<p>プロビジョニング要求の実行に、4 段階の承認を必要とします。アクティビティのタイムアウトが発生した場合、ワークフローは要求を拒否します。</p> <p>このテンプレートはシーケンシャル処理をサポートします。</p>
<p>ファイブステップ順次承認 (タイムアウトと同時に拒否する)</p>	<p>プロビジョニング要求の実行に、5 段階の承認を必要とします。アクティビティのタイムアウトが発生した場合、ワークフローは要求を拒否します。</p> <p>このテンプレートはシーケンシャル処理をサポートします。</p>
<p>ツーステップ並行承認 (タイムアウトと同時に承認する)</p>	<p>プロビジョニング要求の実行に、2 段階の承認を必要とします。アクティビティのタイムアウトが発生した場合、アクティビティは要求を承認し、作業アイテムは次のアクティビティに送られます。</p> <p>このテンプレートはパラレル処理をサポートします。</p>

テンプレート	説明
スリーステップ並行承認 (タイムアウトと同時に承認する)	<p>プロビジョニング要求の実行に、3 段階の承認を必要とします。アクティビティのタイムアウトが発生した場合、アクティビティは要求を承認し、作業アイテムは次のアクティビティに送られます。</p> <p>このテンプレートはパラレル処理をサポートします。</p>
フォーステップ並行承認 (タイムアウトと同時に承認する)	<p>プロビジョニング要求の実行に、4 段階の承認を必要とします。アクティビティのタイムアウトが発生した場合、アクティビティは要求を承認し、作業アイテムは次のアクティビティに送られます。</p> <p>このテンプレートはパラレル処理をサポートします。</p>
ファイブステップ並行承認 (タイムアウトと同時に承認する)	<p>プロビジョニング要求の実行に、5 段階の承認を必要とします。アクティビティのタイムアウトが発生した場合、アクティビティは要求を承認し、作業アイテムは次のアクティビティに送られます。</p> <p>このテンプレートはパラレル処理をサポートします。</p>
ツーステップ並行承認 (タイムアウトと同時に拒否する)	<p>プロビジョニング要求の実行に、2 段階の承認を必要とします。アクティビティのタイムアウトが発生した場合、ワークフローは要求を拒否します。</p> <p>このテンプレートはパラレル処理をサポートします。</p>
スリーステップ並行承認 (タイムアウトと同時に拒否する)	<p>プロビジョニング要求の実行に、3 段階の承認を必要とします。アクティビティのタイムアウトが発生した場合、ワークフローは要求を拒否します。</p> <p>このテンプレートはパラレル処理をサポートします。</p>
フォーステップ並行承認 (タイムアウトと同時に拒否する)	<p>プロビジョニング要求の実行に、4 段階の承認を必要とします。アクティビティのタイムアウトが発生した場合、ワークフローは要求を拒否します。</p> <p>このテンプレートはパラレル処理をサポートします。</p>
ファイブステップ並行承認 (タイムアウトと同時に拒否する)	<p>プロビジョニング要求の実行に、5 段階の承認を必要とします。アクティビティのタイムアウトが発生した場合、ワークフローは要求を拒否します。</p> <p>このテンプレートはパラレル処理をサポートします。</p>

ワークフローおよびプロビジョニングされたリソース - これらのプロビジョニング要求定義はそれぞれ、ワークフローおよびプロビジョニングされたリソースに事前に関連付けられています。要求定義に関連付けられているプロビジョニングされたリソースは変更できませんが、ワークフローまたはそのトポロジは変更できません。

プロビジョニング要求のカテゴリ - プロビジョニング要求のテンプレートもそれぞれ、カテゴリに関連付けられています。カテゴリにより、エンドユーザはプロビジョニング要求を整理できます。すべてのプロビジョニング要求テンプレートに含まれるデフォルトのカテゴリは、「エンタイトルメント」です。カテゴリキー、すなわち `srvprvCategoryKey` 属性の値は `entitlements`(小文字) です。

ディレクトリ抽象化レイヤエディタを使用すると、独自のカテゴリを作成できます。新しいカテゴリを作成する際には、カテゴリキー (`srvprvCategoryKey` の値) が小文字になるよ

うに注意してください。これは、Identity Manager ユーザアプリケーションでカテゴリが適切に機能するために必要です。

プロビジョニングカテゴリの作成の詳細については、104 ページのセクション 4.4 「リストの操作」を参照してください。

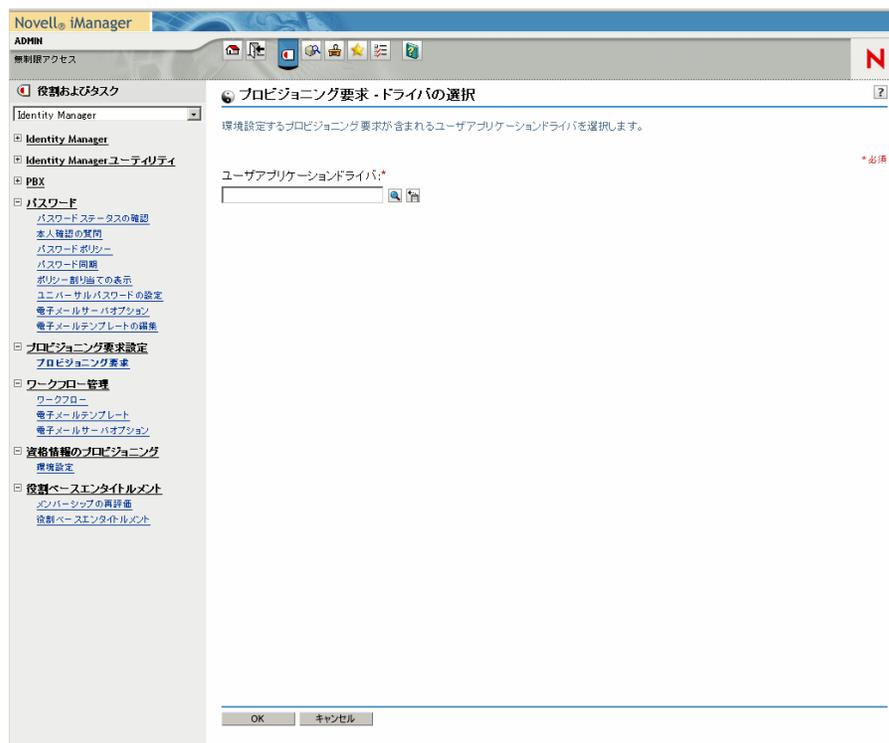
22.3 プロビジョニング要求定義の設定

プロビジョニング要求定義を設定する前に、定義が含まれる Identity Manager ユーザアプリケーションドライバを選択する必要があります。ドライバを選択したら、新しいプロビジョニング要求定義を作成するか、既存の定義を編集できます。また、プロビジョニング要求定義を削除したり、要求定義のステータスを変更したり、要求定義の権利を定義したりすることもできます。

22.3.1 ドライバの選択

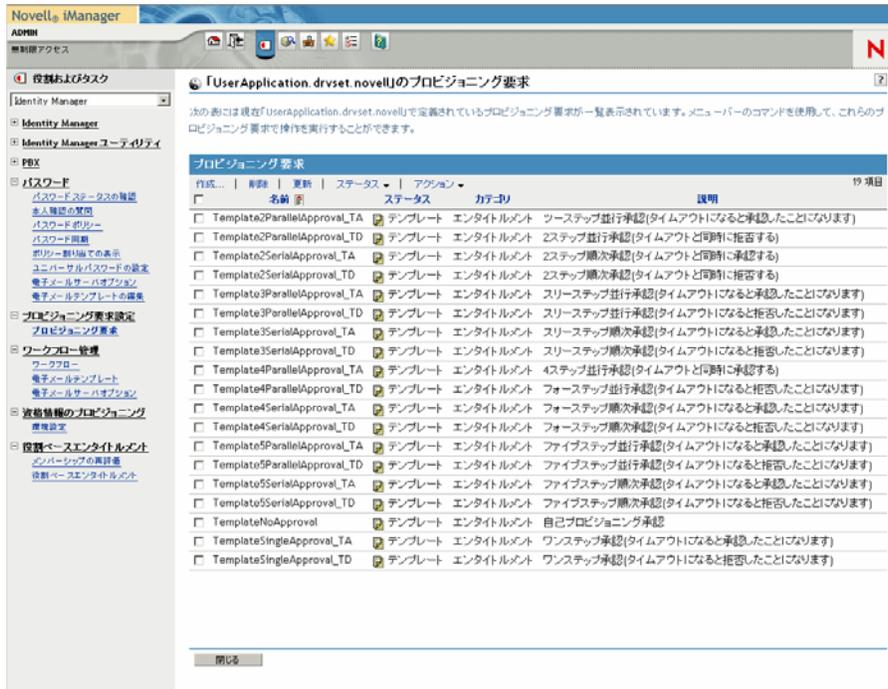
Identity Manager ユーザアプリケーションドライバを選択するには：

- 1 iManager で、[Identity Manager] カテゴリを選択します。
- 2 [プロビジョニング要求の環境設定] 役割を開きます。
- 3 [プロビジョニング要求] タスクをクリックします。
[ユーザアプリケーションドライバ] 画面が表示されます。



- 4 [ユーザアプリケーションドライバ] フィールドでドライバ名を指定し、[OK] をクリックします。

[プロビジョニング要求の環境設定] パネルが表示されます。[プロビジョニング要求の環境設定] パネルには、使用できるプロビジョニング要求定義のリストが表示されます。



インストールされているテンプレートは、[テンプレート] というステータスとともに黒字で表示されます。テンプレートである要求定義には、ハイパーテキストリンクは表示されません。これらは読み込み専用であるためです。

注：要求定義にローカライズされたテキストを使用するよう設定されている場合、これらの定義の名前および説明には、現在のロケールに応じたテキストが表示されます。

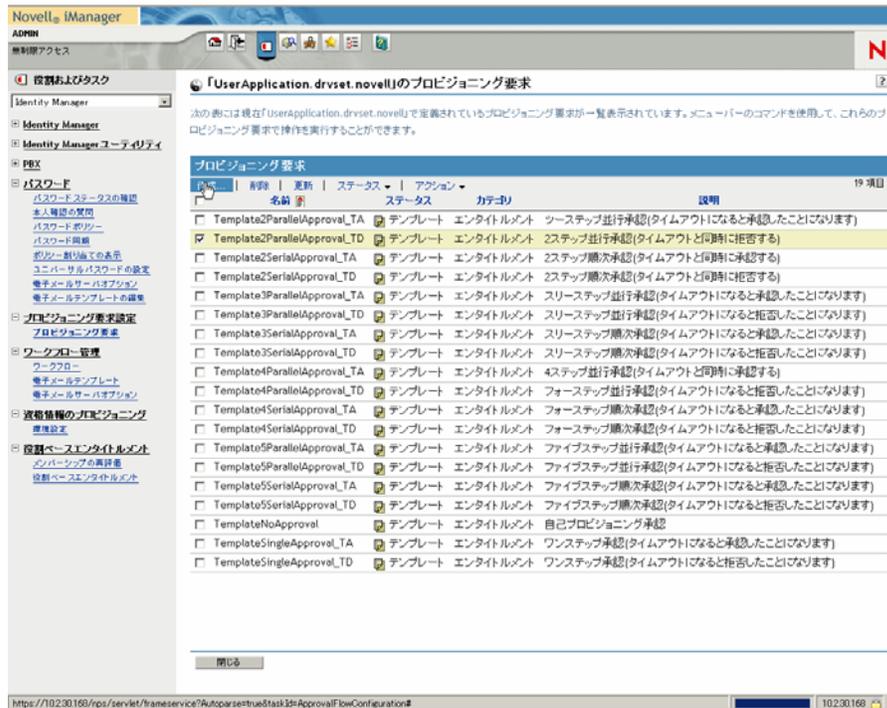
ドライバの変更 - 一度ドライバを選択すると、iManagerセッション中、新しいドライバを選択しない限り選択したドライバが有効になります。新しいドライバを選択するには、[アクション] コマンドをクリックし、[アクション] メニューから [ユーザアプリケーションドライバの選択] を選択します。

22.3.2 プロビジョニング要求の作成または編集

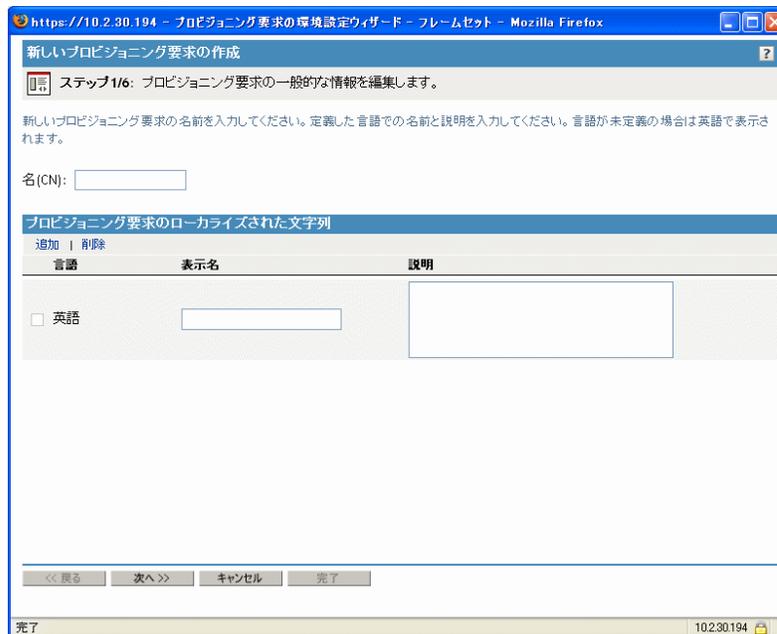
プロビジョニング要求を作成するには：

- 1 [プロビジョニング要求の環境設定] パネルで、テンプレートとして使用するプロビジョニング要求の名前をクリックします。

2 [プロビジョニング要求の環境設定] パネルの [作成元] コマンドをクリックします。



新しいプロビジョニング要求の作成ウィザードの最初のページが表示されます。



3 [名前] フィールドに、新しいオブジェクトの共通名を入力します。

4 アプリケーションでサポートする各言語について、[プロビジョニング要求のローカライズされた文字列] の [表示名] および [説明] の各フィールドにローカライズされたテキストを入力します。このテキストは、ユーザアプリケーションでプロビジョニング要求の識別に使用されます。

- 5 新しい言語をリストに追加するには、[追加] をクリックしてから目的の言語を選択します。

注: デフォルトでは、新しく作成されたプロビジョニング要求では英語だけがサポートされます。

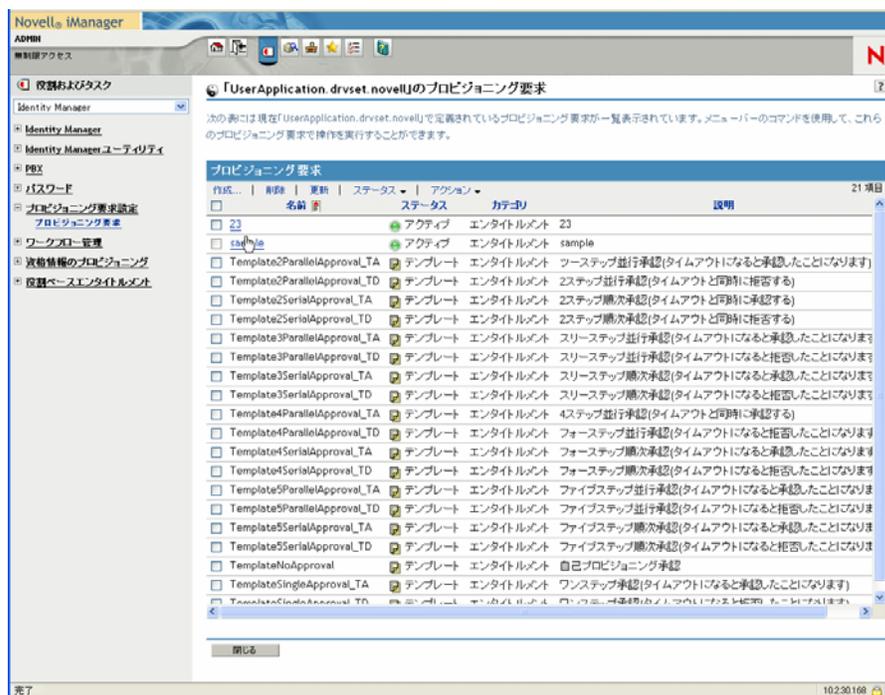
- 6 [次へ] をクリックします。
- 7 334 ページの「**プロビジョニングされたリソースの指定**」の説明に従い、要求定義のプロビジョニングされたリソースを指定します。
- 8 338 ページの「**ワークフローアクティビティの設定**」の説明に従い、要求定義に関連付けるワークフローのアクティビティを設定します。
- 9 342 ページの「**プロビジョニング要求のアクセス権の指定**」の説明に従い、要求定義のアクセス権を指定します。
- 10 342 ページの「**プロビジョニング要求の初期ステータスの指定**」の説明に従い、要求定義の初期ステータスを指定します。

11 設定を確認し、[完了] をクリックします。



既存のプロビジョニング要求を編集するには:

- 1 [プロビジョニング要求の環境設定] パネルで、プロビジョニング要求の名前をクリックします。



テンプレートのプロビジョニング要求を編集することはできません。ステータスが [テンプレート] になっている要求定義には、ハイパーテキストリンクは表示されません。これらは読み込み専用であるためです。

注：要求定義が多数存在すると、[名前]、[説明] など特定の列でソートしなければならない場合があります。列の見出しをクリックするだけで、その列を基にソートできます。

- 2 アプリケーションでサポートする各言語について、[プロビジョニング要求のローカライズされた文字列] の下に一覧表示される言語の横にあるチェックボックスをオンにし、[表示名] と [説明] の各フィールドにローカライズされたテキストを入力します。このテキストは、ユーザアプリケーションでプロビジョニング要求の識別に使用されます。
- 3 新しい言語をリストに追加するには、[追加] をクリックしてから目的の言語を選択します。

注：デフォルトでは、新しく作成されたプロビジョニング要求は英語のみをサポートします。

- 4 [次へ] をクリックします。
- 5 **334 ページの「プロビジョニングされたリソースの指定」**の説明に従い、要求定義のプロビジョニングされたリソースを指定します。
- 6 **338 ページの「ワークフローアクティビティの設定」**の説明に従い、要求定義に関連付けるワークフローのアクティビティを設定します。
- 7 **342 ページの「プロビジョニング要求のアクセス権の指定」**の説明に従い、要求定義のアクセス権を指定します。
- 8 **342 ページの「プロビジョニング要求の初期ステータスの指定」**の説明に従い、要求定義の初期ステータスを指定します。
- 9 設定を確認し、[完了] をクリックします。

プロビジョニングされたリソースの指定

この節では、エンタイトルメントに基づくプロビジョニングされたリソースの指定について詳しく説明します。エンタイトルメントの概念、またはエンタイトルメントの作成および使用については触れません。

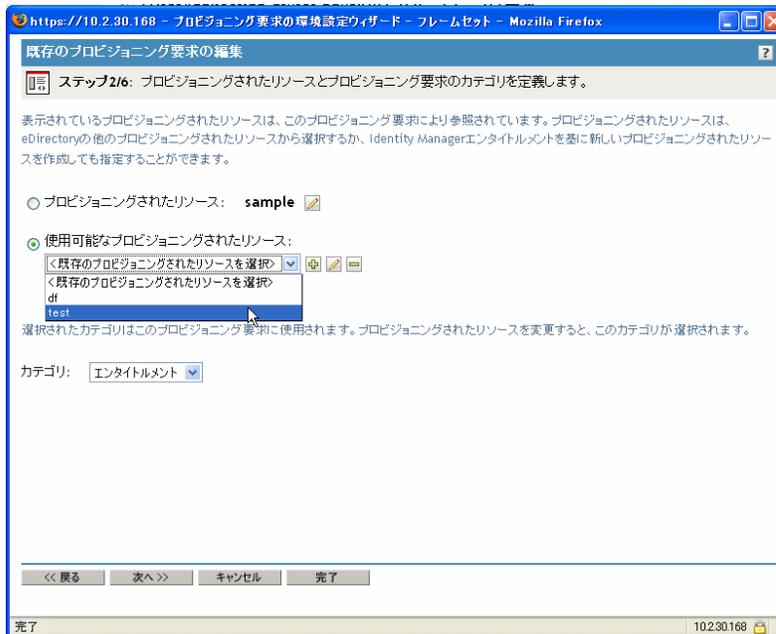
エンタイトルメントの詳細については、『<z-DocTitleInVariable>Novell Identity Manager: 管理ガイド』を参照してください。

プロビジョニングされたリソースを指定するには：

- 1 現在、リクエスト定義に関連付けられているターゲットを使用する場合には、[プロビジョニングされたリソース] ラジオボタンを選択します。

デフォルトでは、有効なリソースを参照するリクエスト定義を編集する場合、[プロビジョニングされたリソース] ラジオボタンが選択されています。新しいプロビジョニング要求を定義している場合には、このラジオボタンは選択されていません。

- 2 現在選択しているドライブ内で以前定義された別のリソースに要求定義を関連付ける場合は、[使用可能なプロビジョニングされたリソース] ラジオボタンを選択し、ドロップダウンリストからターゲットを選択します。



注：エンタイルメントではないリソースに要求定義が関連付けられている場合、リソースを変更することはできません。

- 3 [カテゴリ] ドロップダウンリストから、プロビジョニングされたリソース定義のカテゴリを選択します。
- デフォルトでは、カテゴリは、現在選択しているプロビジョニングされたリソースのカテゴリになっています。プロビジョニングされたリソースを変更すると、リソースのカテゴリに合致するように、リクエスト定義のカテゴリも変わります。リクエスト定義に別のカテゴリを割り当てる場合は、[カテゴリ] ドロップダウンリストからカテゴリを選択します。
- 4 エンタイルメントに基づいて新しいリソースを作成する場合は、[+] ボタンをクリックします。



既存のリソースを編集する場合は、ペンの形をしたボタンをクリックします。



リソースの特性を指定する場合は、次の手順に従います。

- 4a [名 (CN)] フィールドにリソースの名前を入力します。
- 4b [カテゴリ] ドロップダウンリストから、リソースのカテゴリを選択します。
- 4c [エンタイルメント] フィールドで、エンタイルメントを指定します。
- 4d アプリケーションでサポートする各言語について、[プロビジョニングされたリソースのローカライズされた文字列] のに一覧表示されている言語の横にある

チェックボックスをオンにし、[表示名] および [説明] の各フィールドにローカライズされたテキストを入力します。このテキストは、ユーザアプリケーションでのプロビジョニングリソースの識別に使用されます。

- 4e 新しい言語をリストに追加するには、[追加] をクリックしてから目的の言語を選択します。

注：デフォルトでは、新しく作成されたプロビジョニングリソースは英語だけをサポートします。

The screenshot shows a web browser window with the URL `https://10.2.30.168 - プロビジョニングされたリソースウィザード - フレームセット - Mozilla Firefox`. The page title is "新しいプロビジョニングされたリソースの作成" (Create New Provisioned Resource). The current step is "ステップ 1/3: プロビジョニングされたリソースの一般的な情報の編集" (Step 1/3: Edit general information of the provisioned resource).

Instructions: "新しいプロビジョニングされたリソースの名前を入力し、カテゴリと関連付けるIdentity Managerエンタイトルメントを選択します。定義された言語での表示名と説明を入力します。言語が未定義の場合は、英語で表示されます。"

Form fields:

- 名 (CN):
- カテゴリ:
- エンタイトルメント:

Section: "プロビジョニングされたリソースのローカライズされた文字列" (Localized strings for the provisioned resource)

Buttons: 追加 | 削除

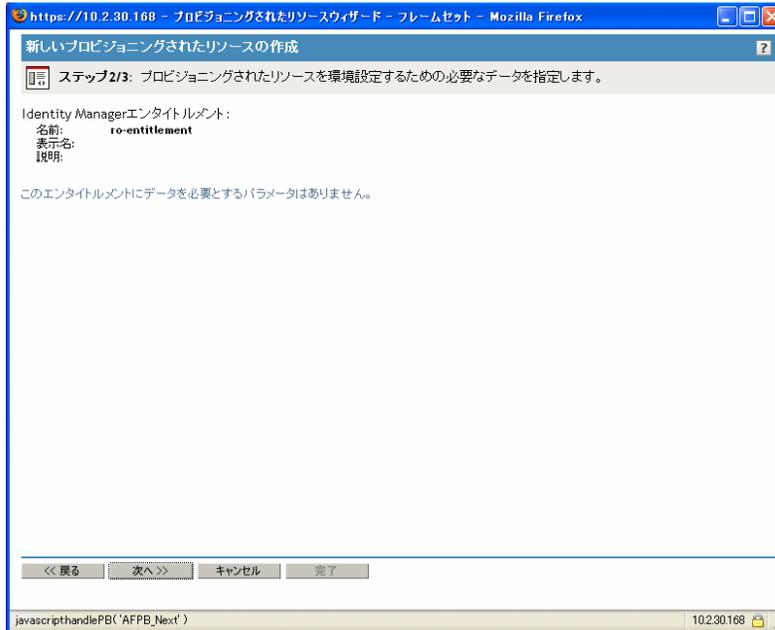
言語	表示名	説明
<input type="checkbox"/> 英語	<input type="text" value="My Resource"/>	<input type="text" value="This is my resource"/>

Navigation buttons: << 戻る | 次へ >> | キャンセル | 完了

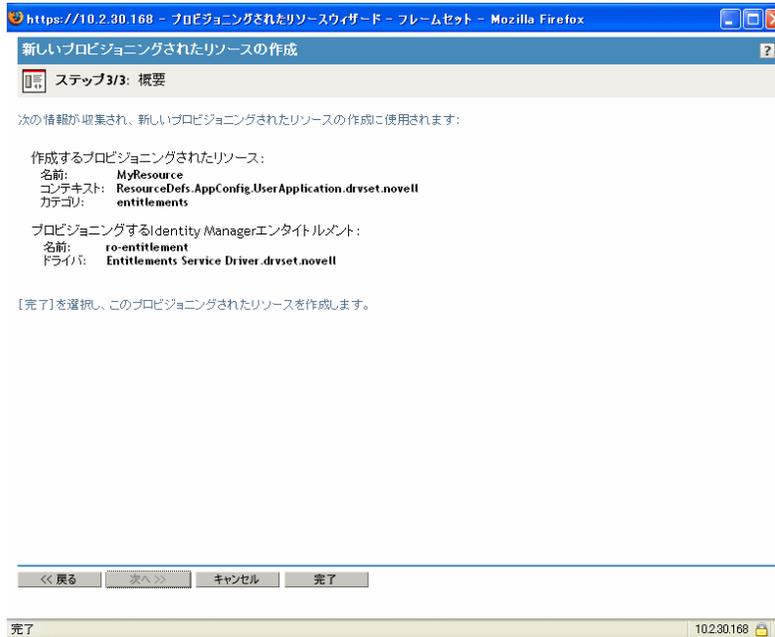
Status bar: 完了 | 10.2.30.168

- 5 [次へ] をクリックします。

プロビジョニングされたリソースウィザードに、エンタイトルメントに必要なパラメータを入力するための画面が表示されます。



- 6 エンタイトルメントにパラメータが必要な場合は、[次へ] をクリックします。
[新しいプロビジョニングされたリソースの作成] ウィザードに [概要] ページが表示され、定義するリソースについての情報が表示されます。



- 7 [完了] をクリックします。

ワークフローアクティビティの設定

関連ワークフローのアクティビティを設定するには：

- 1 [電子メールによる参加者への通知] チェックボックスをオンまたはオフにすることにより、各アクティビティの宛先に電子メールで通知するかどうかを指定します。

新しいプロビジョニング要求の作成

ステップ3/6: プロビジョニング要求を環境設定するために必要なデータを指定します。

電子メールを有効にするか、無効にして、プロビジョニング要求内の各アクティビティの宛先、タイムアウト、再試行情報を定義します。タイムアウトとは宛先がそのアクティビティを実行するために割り当てられた時間を指します。

電子メールによる参加者への通知

1次承認

宛先:

式: 受信者 マネージャ

DN: (例、CN=Admin,O=Novell)

タイムアウト: 48 時間 (値なし: システムデフォルトを使用する)

再試行:

試行回数: 3 (値なし: エントリなし)

宛先:

式: 「1次承認」の宛先 マネージャ

DN: (例、CN=Admin,O=Novell)

<< 戻る 次へ >> キャンセル 完了

完了 10.2.30.168

注：[電子メールによる参加者への通知] チェックボックスをオンにし、宛先にプロキシが指定されている場合、そのプロキシにも電子メールによる通知が行われます。ただし、委任ユーザには電子メール通知は行われません。

- 2 アクティビティの名前の横にあるアイコンをクリックすると、各ワークフローアクティビティに対して表示ラベルをオプションで変更できます(この例では [1 次承認])。

[表示ラベル] フィールドに表示ラベルを入力し、[OK] をクリックします。

言語	表示ラベル
<input checked="" type="checkbox"/> 英語	First approval

注: デフォルトの表示ラベル ([1 次承認]、[2 次承認] など) は、承認がシーケンシャルに処理されることを示しています。パラレルフローの場合、シーケンシャル処理であることがわかりやすいラベルを指定することもできます。たとえば、「パラレル承認 1/3」、「パラレル承認 2/3」などのラベルを割り当てる必要があります。

3 各ワークフローアクティビティについて、次の情報を入力します。

フィールド	説明
宛先の式	<p>アクティビティの宛先を指定する動的な式を指定します。宛先は、式の評価方法に基づいて、ランタイム時に特定されます。</p> <p>宛先式の最初の用語は、次の値のいずれかになります。</p> <ul style="list-style-type: none"> ◆ Initiator ◆ Recipient ◆ Addressee of <i>activity-name</i> <p>ワークフローの各アクティビティの「Addressee of <i>activity-name</i>」が [式] ドロップダウンに表示されます (現在設定中のアクティビティを除きます)。 <i>activity-name</i> は、アクティビティについて指定した表示ラベルです。表示ラベルを指定しなかった場合は、デフォルト名になります。</p> <p>宛先式の 2 番目の用語は、次の値のいずれかになります。</p> <ul style="list-style-type: none"> ◆ Manager ◆ < 属性なし > <p>注: Manager 属性は、抽象化レイヤのユーザエンティティで定義済みの属性であるため、自動的に使用できます。他の属性 (Manager 以外) は、次の条件を充足する場合に、選択可能となります。</p> <ul style="list-style-type: none"> ◆ 抽象化レイヤのユーザエンティティで定義されている ◆ 単一値である ◆ DN データタイプを持つ
宛先の DN	<p>ユーザ、グループ、またはタスクグループの識別名を指定します。</p> <p>注: ユーザアプリケーションの [My Team Tasks (マイチームのタスク)] アクションで、タスクグループマネージャがタスクグループでタスクを検索できるようにする場合は、そのタスクグループを宛先として指定する必要があります。</p>
タイムアウト	<p>宛先がタスクを完了するために割り当てられる時間を指定します。タイムアウト間隔は、アクティビティが宛先により実行されるたびに適用されます。</p> <p>値の単位は、秒、分、時間、または日です。</p>

フィールド	説明
再試行回数	<p>タイムアウト時にアクティビティが再試行する回数を指定します。</p> <p>アクティビティのタイムアウトが発生した場合は、アクティビティに指定された再試行回数に従い、ワークフロープロセスは、アクティビティを再実行しようとします。再試行のたびに、ワークフロープロセスはアクティビティを別のユーザにエスカレートすることができます。この場合、アクティビティは、このユーザにアクティビティの作業を完了する機会を与えるために、別の宛先 (たとえばユーザのマネージャ) に再割り当てされます。最後の再試行でタイムアウトが発生した場合、ワークフローの設定内容に従い、そのアクティビティは承認済みまたは拒否としてマークされます。</p>
再試行宛先の式	<p>タイムアウト制限に到達した場合に、タスクを取得するユーザを特定するためのダイナミックな式を指定します。</p> <p>再試行宛先は、式の評価方法に基づいて、ランタイム時に特定されます。</p> <p>宛先式の最初の用語は、次の値のいずれかになります。</p> <ul style="list-style-type: none"> ◆ approval.getAddressee() ◆ Initiator ◆ Recipient ◆ Addressee of <i>activity-name</i> <p>approval.getAddressee() オプションは、現在の宛先を取得します。</p> <p>ワークフローの各アクティビティの「Addressee of <i>activity-name</i>」が [式] ドロップダウンにリストされます (現在設定中のアクティビティも含まれます)。activity-name は、アクティビティについて指定した表示ラベルです。表示ラベルを指定しなかった場合は、デフォルト名となります。</p> <p>宛先式の 2 番目の用語は、次の値のいずれかになります。</p> <ul style="list-style-type: none"> ◆ Manager ◆ < 属性なし > <p>approval.getAddressee() オプションを選択して Manager を選択する場合、各再試行は、組織内の上位レベルにある新しいマネージャにエスカレートされます。このため、再試行回数は組織に適した数値に設定する必要があります。どのような場合でも、再試行回数は、現在の宛先の上にある管理階層のレベル数を超えることはできません。</p>
再試行宛先の DN	<p>再試行制限に到達した場合に、タスクを取得するユーザまたはグループの識別名を指定します。</p>

4 アクティビティの設定が完了したら、ページをスクロールして、フローの他のアクティビティを確認することが必要になる場合もあります。

5 [次へ] をクリックします。

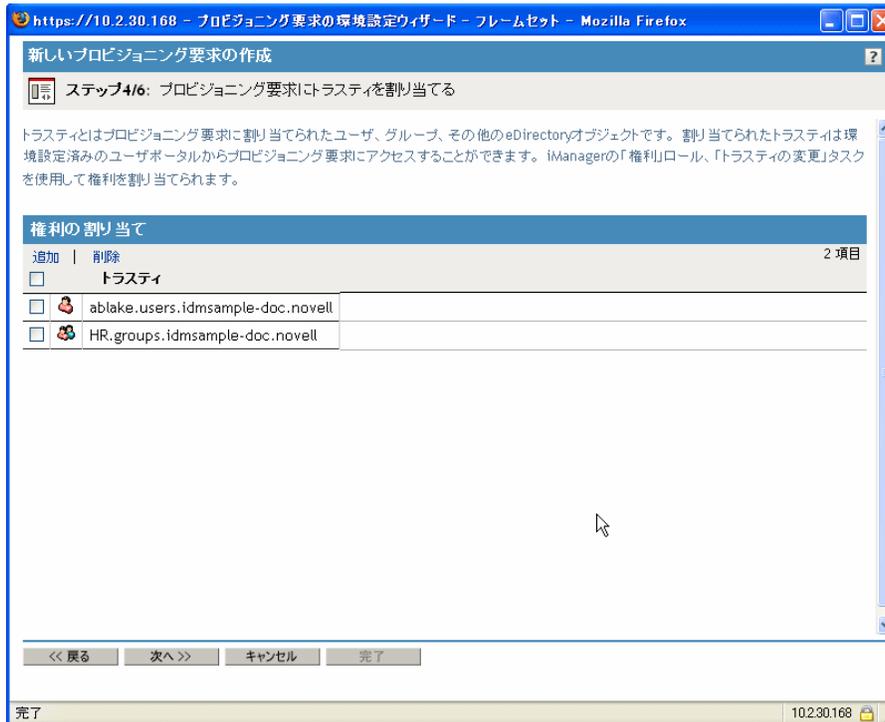
注: 設定できるアクティビティの数は、リクエスト定義に関連付けられているワークフローテンプレートによって異なります。エンタイトルメントパラメータの数およびタイプは、リクエストに関連付けられているプロビジョニングされたリソースによって異なります。

プロビジョニング要求のアクセス権の指定

プロビジョニング要求のアクセス権を指定するには：

- 1 リクエスト定義のトラスティのリストに、ユーザ、グループ、または別の eDirectory オブジェクトを追加するには、[追加] をクリックしてオブジェクトを選択します。

オブジェクトを追加すると、トラスティのリストに表示されます。



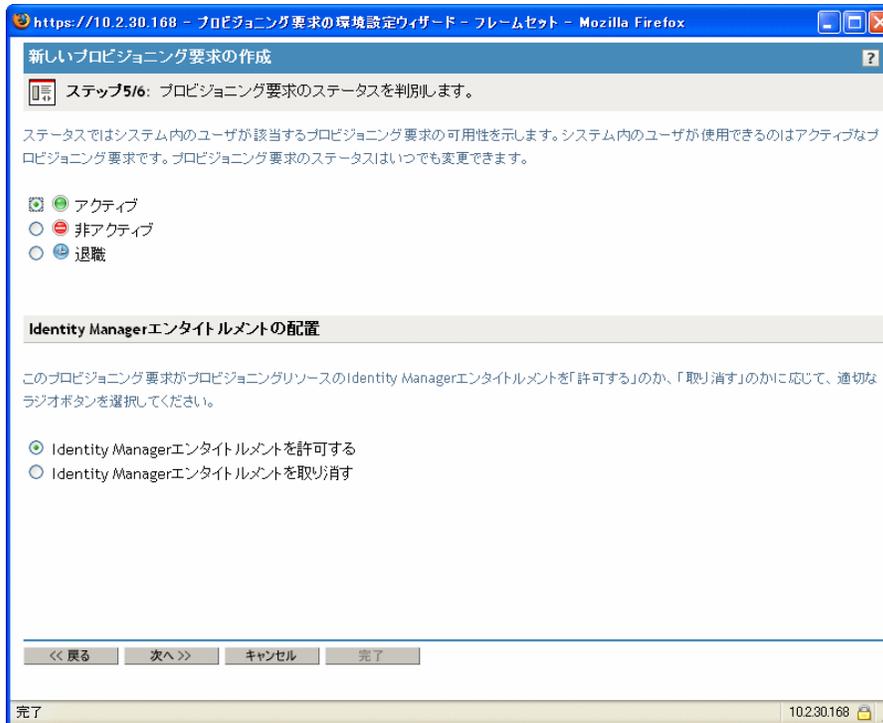
- 2 ユーザ、グループまたは他のオブジェクトを削除するには、[トラスティ] リストから項目を選択し、[削除] をクリックします。
- 3 [次へ] をクリックします。

プロビジョニング要求の初期ステータスの指定

プロビジョニング要求の初期ステータスを設定するには：

- 1 対象のステータスのラジオボタンをクリックします。

ステータス	説明
アクティブ	使用可能。
非アクティブ	一時的な使用不可。デフォルト値。
退職	無効。



- 2 正しいアクションのラジオボタン (付与または取り消し) をクリックします。
- 3 [次へ] をクリックします。

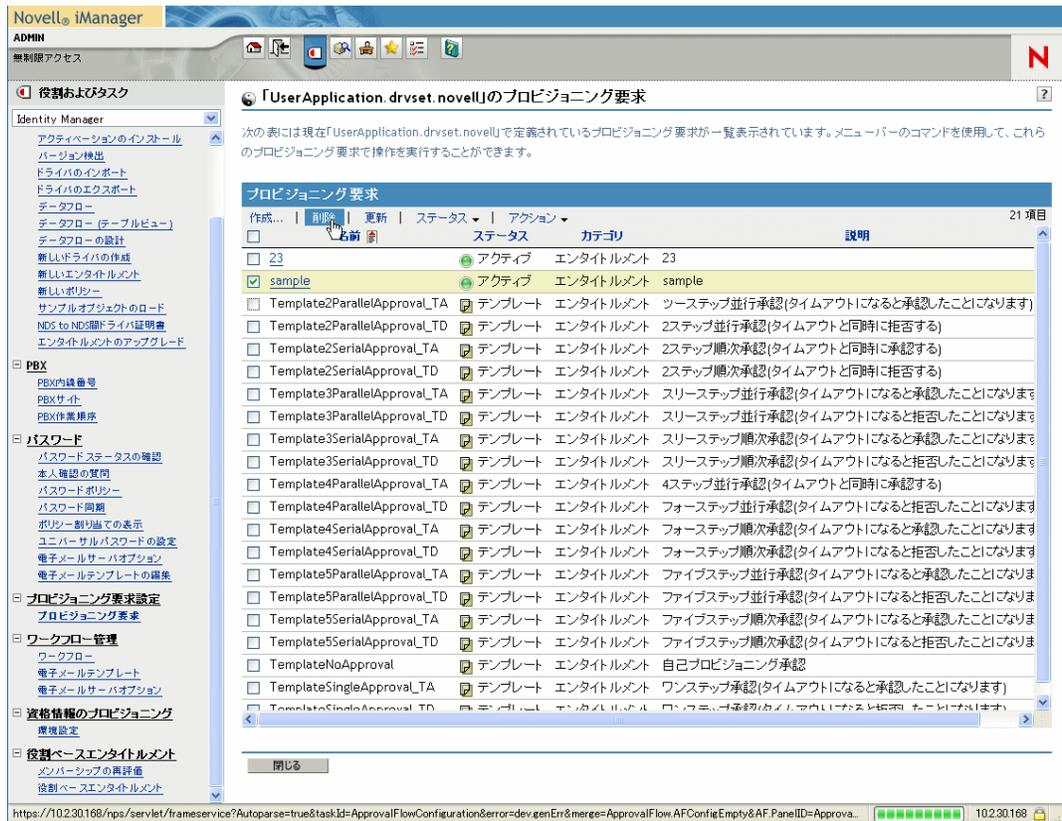
22.3.3 プロビジョニング要求の削除

プロビジョニング要求を削除するには：

- 1 名前の横にあるチェックボックスをオンにし、削除するプロビジョニング要求を選択します。

テンプレートになっているプロビジョニング要求を削除することはできません。

2 [プロビジョニング要求の環境設定] パネルの [削除] コマンドをクリックします。

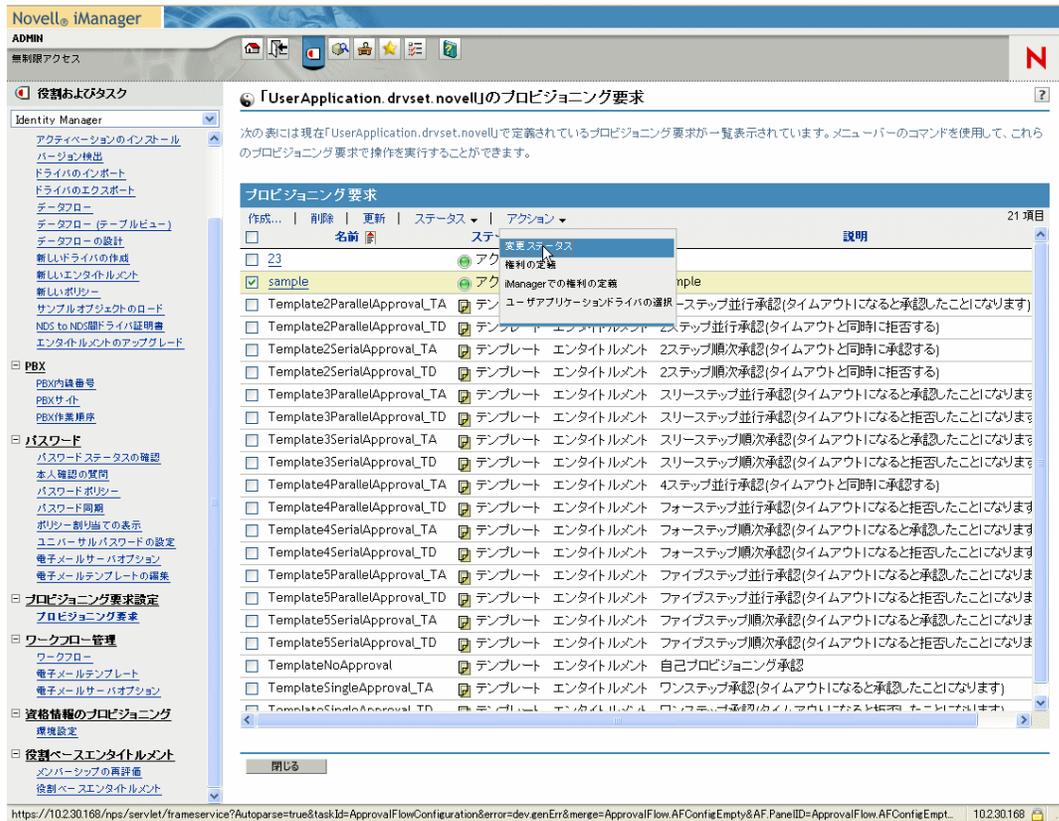


22.3.4 既存のプロビジョニング要求のステータスの変更

既存のプロビジョニング要求のステータスを変更するには：

- 1 名前の横にあるチェックボックスをオンにし、ステータスを変更するプロビジョニング要求を選択します。

- 2 [プロビジョニング要求の環境設定] パネルの [変更ステータス] コマンドをクリックします。



- 3 [ステータス] メニューのステータスをクリックします。

ステータス	説明
アクティブ	使用可能。
非アクティブ	一時的な使用不可。
退職	無効。

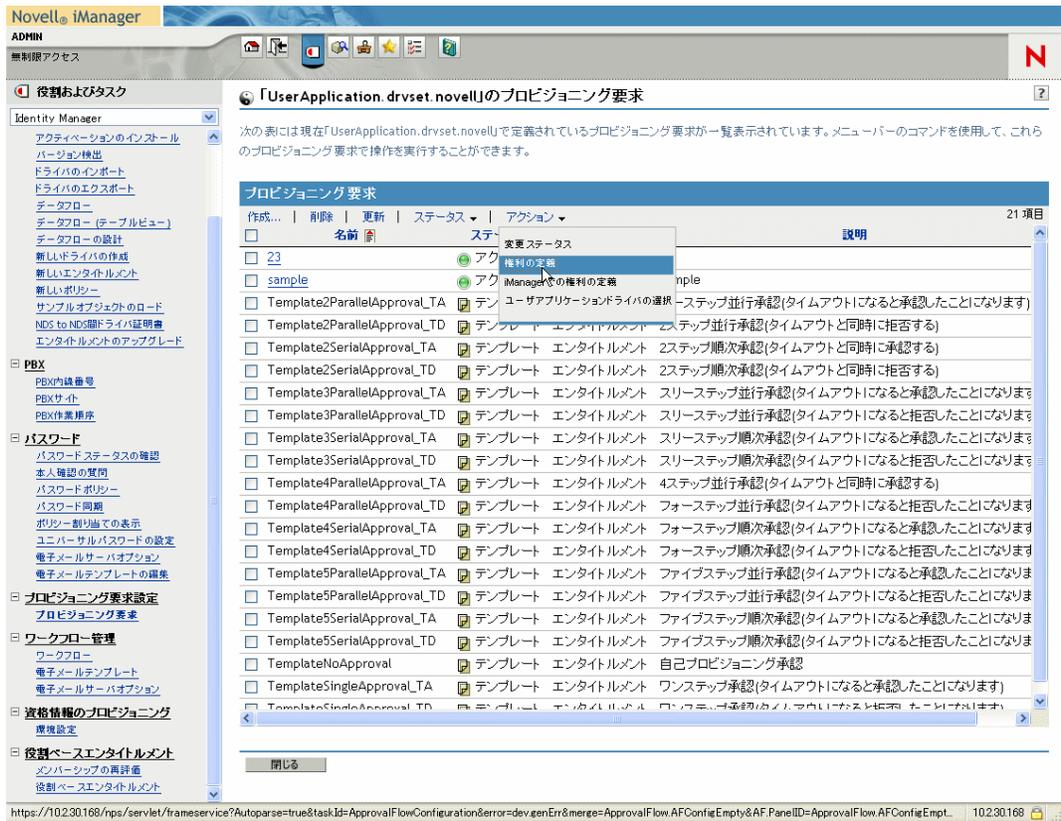
- 4 正しいアクションのラジオボタン (付与または取り消し) をクリックします。
- 5 [完了] をクリックします。

22.3.5 既存のプロビジョニング要求の権利の定義

既存のプロビジョニング要求の権利を定義するには：

- 1 名前の横にあるチェックボックスをオンにし、権利を定義するプロビジョニング要求を選択します。
- 2 [プロビジョニング要求の環境設定] パネルの [アクション] コマンドをクリックします。

3 [アクション] メニューの [権利の定義] コマンドをクリックします。



4 342 ページの「プロビジョニング要求のアクセス権の指定」で説明されている手順に従います。

iManager でプロビジョニング要求の権利を定義するには：

- 1 名前の横にあるチェックボックスをオンにし、権利を定義するプロビジョニング要求を選択します。
- 2 [プロビジョニング要求の環境設定] パネルの [アクション] コマンドをクリックします。
- 3 [アクション] メニューの [iManager での権利の定義] コマンドをクリックします。

プロビジョニングワークフローの管理

23

この章では、ランタイム時のプロビジョニングワークフローの管理について説明します。プロビジョニングワークフローの電子メール通知の設定についても説明します。

ここで取り扱う内容は次のとおりです。

- ◆ 347 ページのセクション 23.1 「ワークフロー管理プラグインについて」
- ◆ 348 ページのセクション 23.2 「ワークフローの管理」
- ◆ 356 ページのセクション 23.3 「電子メールサーバの設定」
- ◆ 357 ページのセクション 23.4 「インストールされている電子メールテンプレートでの作業」

23.1 ワークフロー管理プラグインについて

iManager でワークフロー管理プラグインを使用すると、ブラウザベースのインタフェースを使用して、ワークフロープロセスのステータスを表示したり、ワークフロー内のアクティビティを再割り当てしたり、応答のないワークフローを終了したりすることができます。

ワークフロー管理プラグインは、iManager の [Identity Manager] カテゴリ内にあります。このプラグインでは、[ワークフロー管理] 役割に [ワークフロー] タスクが含まれています。

[ワークフロー管理] 役割には、[電子メールテンプレート] および [電子メールサーバオプション] の各タスクが含まれています。これらのタスクは、[パスワード] 役割の下に一覧表示される他のタスクへのショートカットとなります。

[ワークフロー] タスクについて [ワークフロー] タスクは、次のパネルから構成されます。

パネル	説明
ワークフロー	<p>プロビジョニングワークフローを管理するプライマリユーザインタフェースを提供します。このインタフェースには、現在処理中のワークフローが一覧表示され、これらのワークフローに対してさまざまなアクションを実行できます。</p> <p>[ワークフロー] タスクを開始すると、[ワークフロー] パネルにより、Identity Manager ユーザアプリケーションドライバを選択するよう要求されます。ドライバは、ワークフローサーバを指しています。サーバにログインしてワークフロー管理を開始する前に、ドライバを選択する必要があります。</p> <p>ドライバを選択した後、管理するワークフローを選択するための検索条件を指定できます。</p>
ワークフロー詳細	特定のワークフローに関する詳細情報を表示するための読み込み専用ユーザインタフェースを提供します。

23.2 ワークフローの管理

この節では、ワークフロー管理プラグインを使用したプロビジョニングワークフローの管理手順について説明します。

23.2.1 ワークフローサーバへの接続

ワークフロー管理を開始する前に、ワークフローサーバに接続する必要があります。ユーザアプリケーションドライバが1つのワークフローサーバに関連付けられている場合は、使用するドライバの名前を指定するだけで済みます。ドライバが複数のワークフローサーバに関連付けられている場合は、ターゲットのワークフローサーバを選択する必要があります。

ワークフローサーバに接続するには：

- 1 iManager で、[Identity Manager] カテゴリを選択します。
- 2 [ワークフロー管理] 役割を開きます。
- 3 [ワークフロー] タスクをクリックします。
[ワークフロー] 画面が表示されます。



- 4 以前にターゲットワークフローサーバにアクセスしたことがある場合は、[前にアクセスしたサーバ] ドロップダウンリストからサーバを選択できます。

画面の残りのフィールドにデータが自動的に挿入されます。

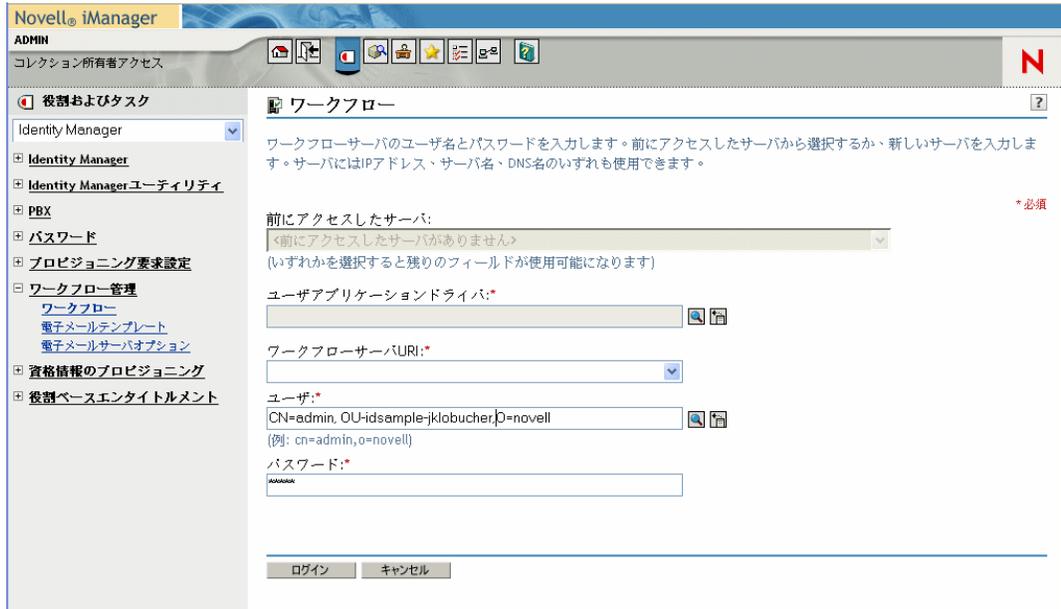
- 5 ワークフローサーバにアクセスしたことがない場合は、[ユーザアプリケーションドライバ] フィールドでドライバ名を指定してから [OK] をクリックします。

画面の残りのフィールドにデータが自動的に挿入されます。

- 6 ドライバが複数のワークフローサーバに関連付けられている場合、[ワークフローサーバ URI] フィールドでターゲットサーバを選択します。
- 7 必要に応じて、[ユーザ] フィールドのユーザ名と [パスワード] フィールドのパスワードを上書きします。

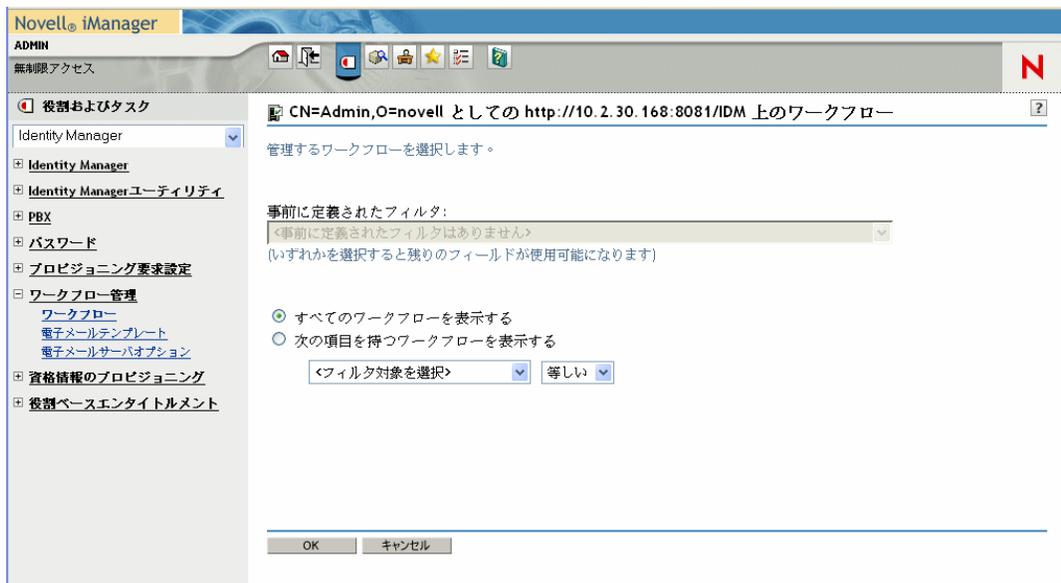
ユーザはユーザアプリケーション管理者である必要があります。デフォルトでは、ユーザ名は、現在 iManager にログインしているユーザに設定されます。このユーザが管理者でない場合は、ユーザ名を変更する必要があります。たとえば、idmsample

test OU のユーザアプリケーション管理者を指すようにユーザを変更する場合は、次のとおりです。



8 [ログイン] をクリックします。

ワークフロー管理プラグインに、ワークフローを検索するためのフィルタを指定するページが表示されます。

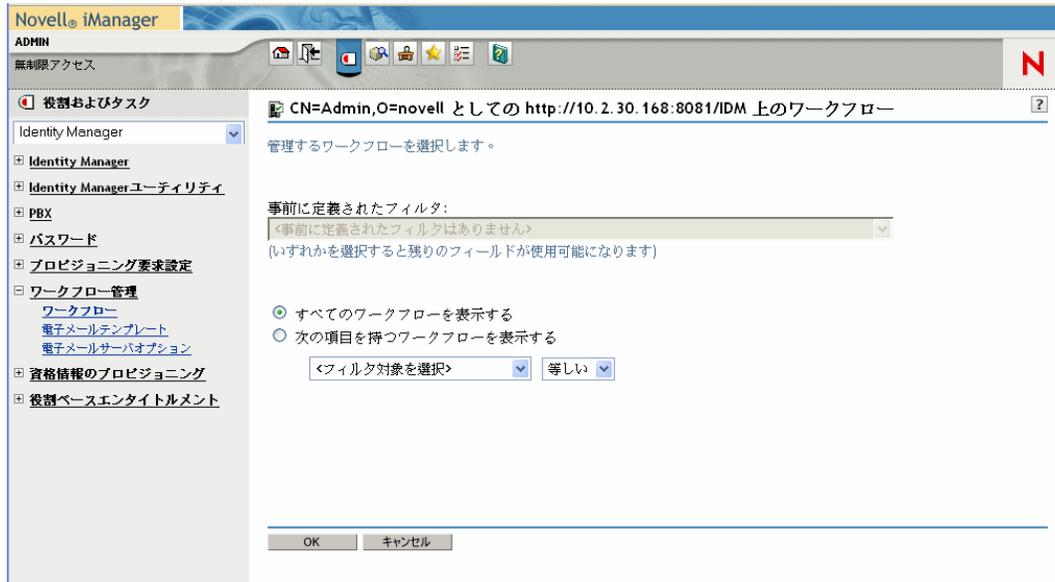


23.2.2 検索条件に合致するワークフローの検索

ターゲットとなるワークフローサーバで多数のワークフロープロセスが実行されている場合、iManagerでワークフローのリストをフィルタリングする必要があります。フィルタリングを行うには、検索条件を指定します。

ワークフローのリストをフィルタリングするための検索条件を指定するには：

- 1 [次の項目を持つワークフローを表示する] ラジオボタンを選択します。



注：デフォルトでは、[すべてのワークフローを表示する] ラジオボタンが選択されています。サーバ上のワークフローの完全なリストを表示する場合は、このデフォルトを変更しないでください。

- 2 条件を指定する属性を選択します。

属性	説明
作成時刻	ワークフローが作成された時刻。
イニシエータ	リクエストを作成したユーザ名。
受信者	受信者のユーザ名。
プロセスステータス	ワークフロープロセス全体のステータス(完了、稼動中、または終了)。
承認ステータス	承認プロセスのステータス(承認済み、拒否、または撤回)。
エンタイトルメントステータス	プロビジョニング要求により開始されるエンタイトルメントのステータス(エラー、致命的エラー、成功、不明、または警告)。

- 3 演算子を選択します。

演算子	コメント
等しい	すべての属性をサポートします。
以前	作成時刻属性のみをサポートします。
以降	作成時刻属性のみをサポートします。
間	作成時刻属性のみをサポートします。

4 属性および演算子の下のフィールドに値を指定します。

[作成時刻] については、日付コントロールと時刻コントロールを使用して値を選択します。[イニシエータ] および [受信者] については、[オブジェクトの履歴] または [オブジェクトセレクタ] を使用して値を指定します。他のすべての属性については、ドロップダウンリストから値を選択します。

5 [OK] をクリックします。

[ワークフロー] パネルで選択したワークフローが表示されます。



ターゲットサーバおよびフィルタの変更 - ワークフローサーバを選択すると、新しいサーバを選択しない限り、iManager セッションの間中、選択したものが有効になります。新しいサーバを選択するには、[アクション] コマンドをクリックし、[アクション] メニューから [サーバの選択] を選択します。



別の検索条件を指定する場合は、[アクション] メニューから [フィルタ定義] を選択します。



23.2.3 アクティブなワークフローの表示の制御

[ワークフロー] パネルには、指定した検索条件に合致するワークフローが一覧表示されます。このリストのフィルタに加え、表示方法を制御することもできます。たとえば、リストを更新する頻度を指定したり、特定の列によってリストをソートしたりできます。

ワークフローのリストを更新する

ワークフローサーバの動作が活発な場合、アクティブワークフローのリストは頻繁に変更されます。このような場合、サーバで実行されるアクティブワークフローのリストの更新が必要になる場合があります。

ワークフローのリストを更新するには：

- 1 [ワークフロー] パネルの [更新] コマンドをクリックします。
- 2 [更新] メニューから次のオプションのいずれかを選択して、更新間隔を指定します。
 - 2a 更新無効
 - 2b 即時更新
 - 2c 10 秒
 - 2d 30 秒
 - 2e 60 秒
 - 2f 5 分

ワークフローのリストのソート

多数のリクエスト定義が存在する場合は、[名前]、[説明] など特定の列でソートしなければならない場合があります。

ワークフローのリストをソートするには：

- 1 ソートする列の見出しをクリックします。

23.2.4 ワークフローインスタンスの終了

ワークフローインスタンスの処理を続行しない場合は、ワークフローを終了できます。

ワークフロープロセスのインスタンスを終了するには：

- 1 ワークフロー名の横にあるチェックボックスをオンにすることにより、[ワークフロー] パネルのワークフローを選択します。
- 2 [ワークフロー] パネルの [停止] コマンドをクリックします。

23.2.5 ワークフローインスタンスの詳細の表示

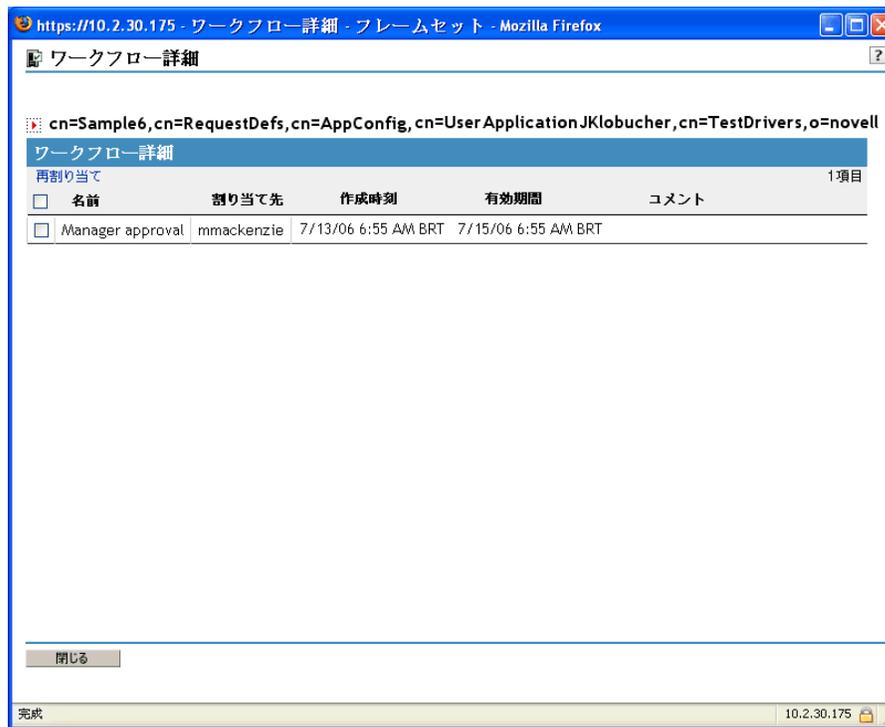
特定のサーバ上で実行中のワークフローのセットが表示された後、ワークフローインスタンスを選択して、実行中のプロセスについての詳細を表示することができます。

注：ワークフローインスタンスがシリアル処理の設計パターンを使用している場合、1つのアクティビティが現在のアクティビティとして表示されます。これは、その作業アイテムを一度に実行できる1人のユーザに限定されるためです。一方、ワークフローがパラレル処理およびブランチ処理に対応している場合、ワークフローインスタンスとして複数の現在のアクティビティが存在することがあります。

特定のワークフローインスタンスについての詳細を表示するには：

- 1 [ワークフロー] パネルのワークフローインスタンスの名前をクリックします。

[ワークフロー詳細] パネルが表示されます。



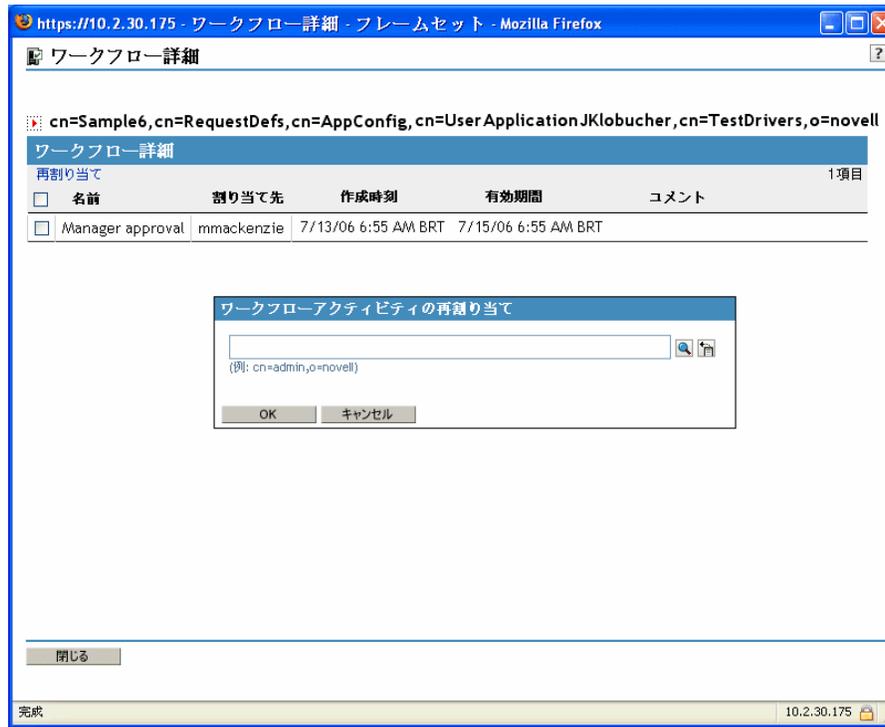
23.2.6 ワークフローインスタンスの再割り当て

ワークフローインスタンスの応答がない場合、作業アイテムを別のユーザまたはグループに再割り当てすることができます。

ワークフローインスタンスの再割り当てを行うには：

- 1 [ワークフロー詳細] パネルの名前の横にあるチェックボックスをオンにし、ワークフローに関連付けられている現在のアクティビティを選択します。

- 2 [ワークフロー詳細] パネルの [再割り当て] コマンドをクリックします。



- 3 作業アイテムの再割り当てを行うユーザまたはグループを選択します。

23.3 電子メールサーバの設定

ワークフローシステムは、通常、実行中のさまざまなポイントで電子メール通知を送信します。たとえば、ワークフローアクティビティが新しい宛先に割り当てられる場合に、電子メールが送信されます。

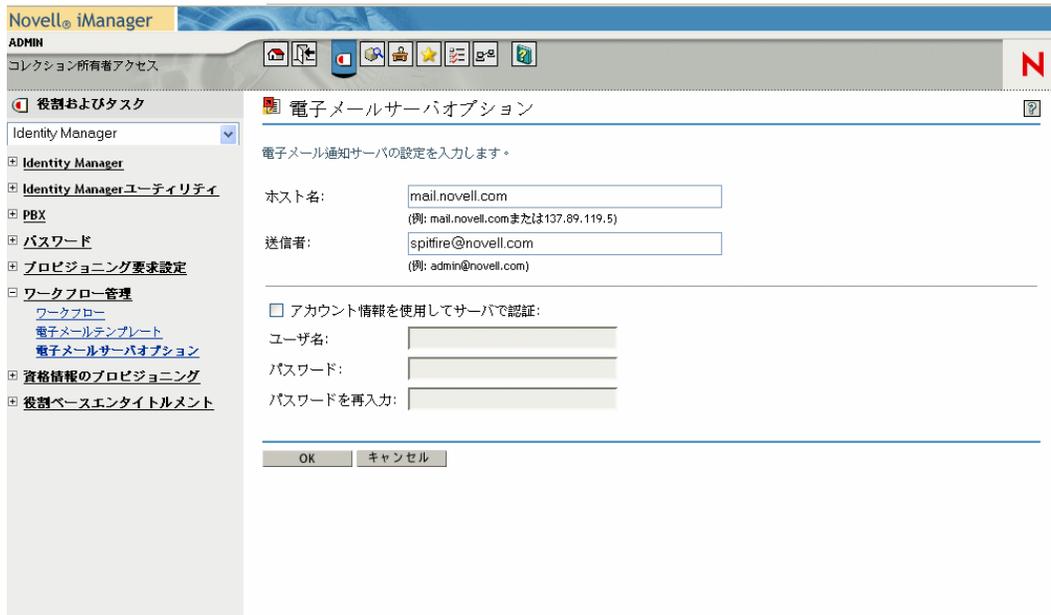
Identity Manager の電子メール通知機能を使用する前に、SMTP 電子メールサーバを設定する必要があります。これには、iManager の [ワークフロー管理] 役割にある [電子メールサーバオプション] のタスクを使用します。

注：このタスクは、[パスワード] 役割の [電子メールサーバオプション] のタスクへのショートカットです。

電子メールサーバを設定するには：

- 1 iManager で、[Identity Manager] カテゴリを選択します。
- 2 [ワークフロー管理] 役割を開きます。
- 3 [電子メールサーバオプション] タスクをクリックします。

[電子メールサーバオプション] 画面が表示されます。



- 4 [ホスト名] フィールドに、ホストサーバの名前 (または IP アドレス) を入力します。
- 5 [送信者] フィールドに、送信者の電子メールアドレスを入力します。
受信者が電子メールを開くと、このテキストが電子メールの見出しの [送信者] フィールドに表示されます。メールサーバの設定によっては、メールサーバがリバースルックアップまたは認証を実行できるように、このフィールド内のテキストはシステム内の有効な送信者でなければならない場合があります。たとえば、「パスワード管理者」などの説明的なテキストではなく、「helpdesk@company.com」と指定します。
- 6 サーバの電子メール送信前に認証を必要とする場合は、[アカウント情報を使用してサーバで認証] チェックボックスをオンにし、ユーザ名およびパスワードを入力します。
- 7 作業が終わったら、[OK] をクリックします。

23.4 インストールされている電子メールテンプレートでの作業

Identity Manager には、ワークフローベースのプロビジョニング専用の電子メールテンプレートが用意されています。これは、「新しいプロビジョニング要求」という電子メールテンプレートです。製品付属のプロビジョニング要求テンプレートはすべて、この電子メールテンプレートに関連付けられています。このため、新しく作成するリクエスト定義もこの電子メールテンプレートを使用します。

「新しいプロビジョニング要求」テンプレートを編集して電子メールメッセージのコンテンツおよび形式を変更することはできますが、新しい電子メールテンプレートを作成することはできません。

「新しいプロビジョニング要求」テンプレートを編集するには、iManager の [ワークフロー管理] 役割にある [電子メールテンプレート] タスクを使用する必要があります。

注：このタスクは、[パスワード] 役割の [電子メールテンプレートの編集] タスクへのショートカットです。

23.4.1 デフォルトのコンテンツおよび形式

製品インストール後の「新しいプロビジョニング要求」テンプレートの外観を次に示します。

```
Dear $userFirstName$, A new provisioning request has been submitted that requires your approval. Request name:$requestTitle$ Submitted by:$initiatorFullName$ Recipient:$recipientFullName$ Please review the details of this request at $PROTOCOL$://$HOST$:$PORT$/$TASK_DETAILS$ to take the appropriate action. You can review a list of all requests pending your approval at $PROTOCOL$://$HOST$:$PORT$/$TASKLIST_CONTEXT$.
```

このテンプレートは、電子メールメッセージをトリガしたプロビジョニング要求定義を識別します。テンプレートには、承認を必要とするタスクに宛先をリダイレクトする URL、そのユーザに属す保留中のタスクの完全なリストを表示する URL も含まれています。

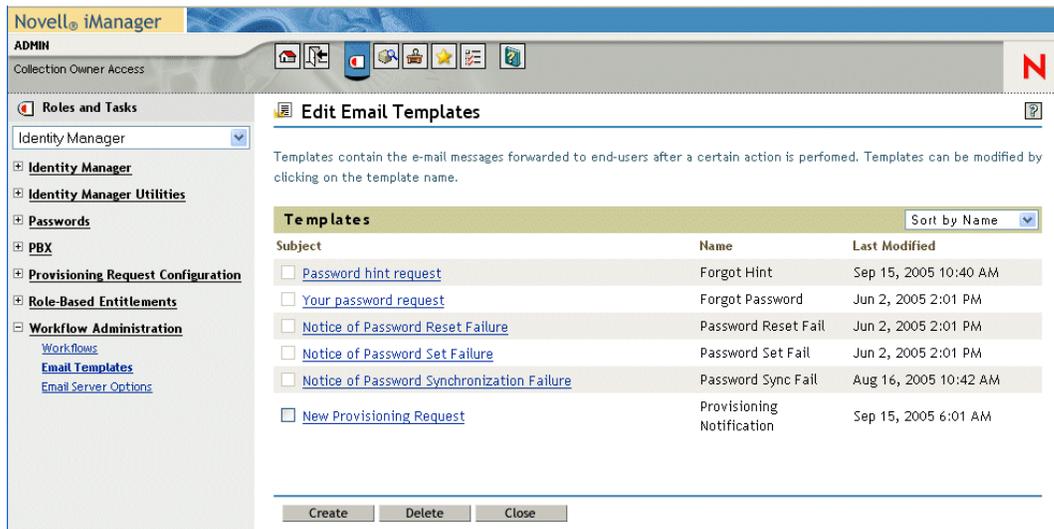
23.4.2 テンプレートの編集

「新しいプロビジョニング要求」テンプレートのコンテンツまたは形式は変更できます。テンプレートは、Identity Manager ユーザアプリケーションのすべてのプロビジョニング要求に適用されます。このため、これから行う編集が、すべてのユーザおよびワークフロータスクについて適切になるよう注意してください。

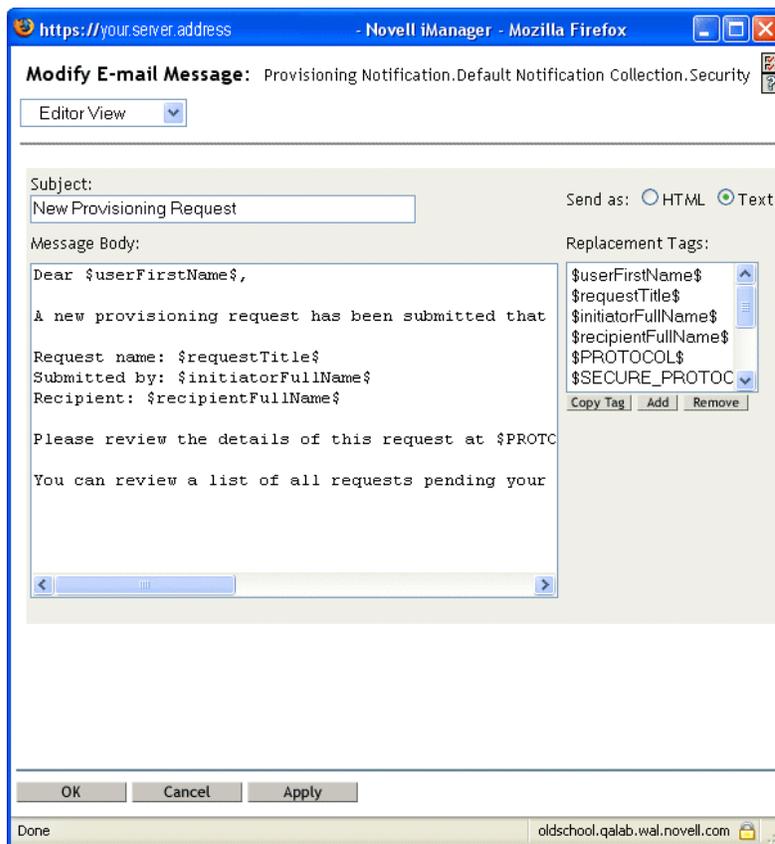
テンプレートを編集するには：

- 1 iManager で、[Identity Manager] カテゴリを選択します。
- 2 [ワークフロー管理] 役割を開きます。
- 3 [電子メールテンプレート] タスクをクリックします。

[電子メールテンプレートの編集] 画面が表示されます。



- 4 テンプレートのリストの [新しいプロビジョニング要求] をクリックします。
[電子メールメッセージの変更] 画面が表示されます。



- 5 [メッセージ本文] ボックスで変更を行います。

- 6 必要に応じて、メッセージ本文に動的テキストが含まれるように、[置換タグ] に表示されている 1 つまたは複数のタグをコピーします。

置換タグについての簡単な説明を次に示します。

タグ	説明
<code>\$userFirstName\$</code>	宛先の名。
<code>\$requestTitle\$</code>	プロビジョニング要求定義の表示名。
<code>\$initiatorFullName\$</code>	イニシエータのフルネーム。
<code>\$recipientFullName\$</code>	受信者のフルネーム。
<code>\$PROTOCOL\$</code>	電子メールメッセージに含まれる URL のプロトコル。
<code>\$SECURE_PROTOCOL\$</code>	電子メールメッセージに含まれる URL のセキュアプロトコル。
<code>\$HOST\$</code>	Identity Manager ユーザアプリケーションを実行する JBoss アプリケーションサーバのホスト。
<code>\$PORT\$</code>	Identity Manager ユーザアプリケーションのポート。
<code>\$SECURE_PORT\$</code>	Identity Manager ユーザアプリケーションのセキュアポート。
<code>\$TASKLIST_CONTEXT\$</code>	宛先について保留となっているすべてのリクエストのリストを表示するページ。
<code>\$TASK_DETAILS\$</code>	この電子メールメッセージが生成されるリクエストの詳細を表示するページ。

- 7 作業が終わったら、[OK] をクリックします。

23.4.3 テンプレートのデフォルト値の変更

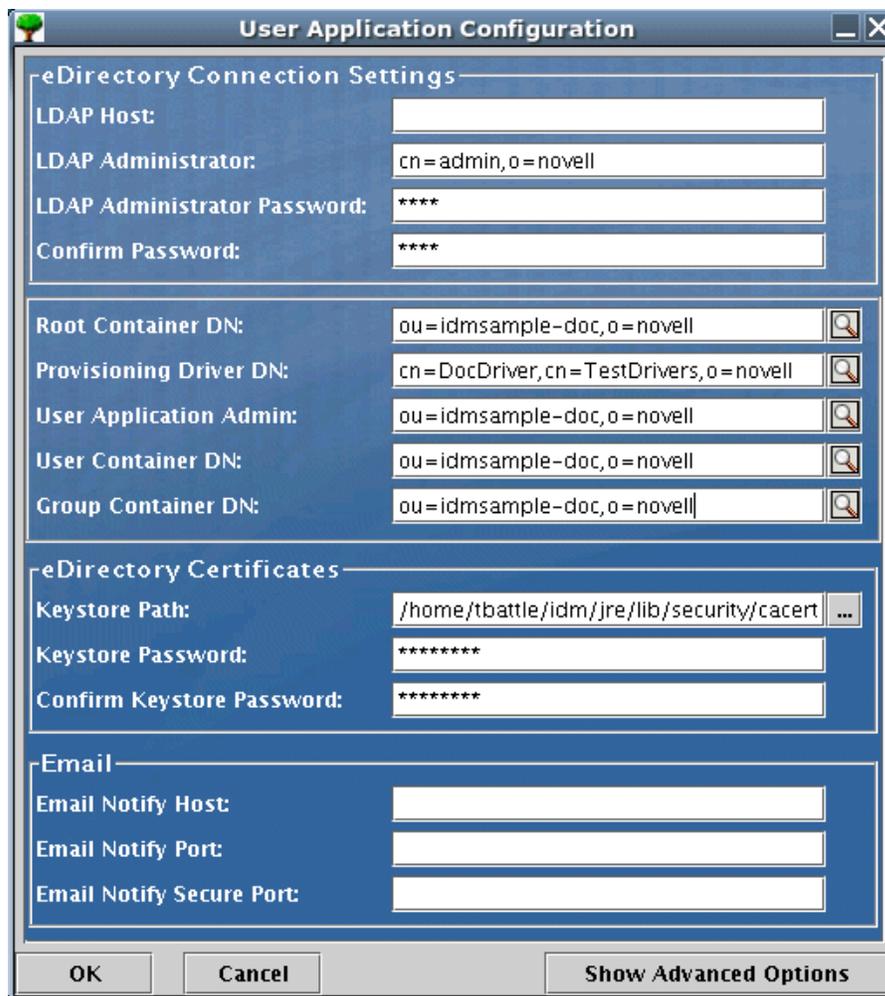
インストール時、電子メールテンプレートで使用する置換タグのいくつかについて、デフォルト値を設定できます。インストール完了後、ユーザアプリケーションの環境設定ツールを使用して、これらの値を変更することもできます。

インストール設定を変更するには：

- 1 `idm` フォルダにある `ldapconfig.sh` スクリプトを実行します。

```
./configupdate.sh
```

注：Windows の場合、実行ファイルは `configupdate.bat` です。



2 必要に応じて、次のフィールドを変更します。

フィールド	説明
Email Notify Host (電子メール通知ホスト)	承認フローで使用される電子メールテンプレート内の \$HOST\$ トークンの置き換えに使用されます。空白のままの場合は、サーバにより計算されます (これは JBoss ホストです)。
Email Notify Port (電子メール通知ポート)	承認フローで使用される電子メールテンプレート内の \$PORT\$ トークンの置き換えに使用されます。
Email Notify Secure Port (電子メール通知のセキュアポート)	承認フローで使用する電子メールテンプレート内の \$SECURE_PORT\$ トークンの置き換えに使用されます。

3 [OK] をクリックして、変更を確認します。

付録

VI

次の付録には、Identity Manager ユーザアプリケーションに関する追加の参照情報と高度なトピックが記載されています。

- ◆ 365 ページの付録 A 「スキーマ拡張」
- ◆ 379 ページの付録 B 「アプリケーションアーカイブの設定」

スキーマ拡張

A

A.1 属性のスキーマ拡張

属性名	説明
srvprvAOLIMAddress	AOL IM アドレス。
srvprvActiveDelegates	ユーザのアクティブな委任ユーザ。
srvprvActiveDelegators	ユーザのアクティブな委任元。
srvprvAssetRef	srvprvAssetRecipientAux クラスによってユーザに関連付けられている名前付き資産に対する集約資産プロパティを表したものの。
srvprvAssignExpiration	プロキシまたは委任ユーザの割り当てが期限切れになる時間。
srvprvAssignFromContainer	プロキシまたは委任ユーザの割り当てのコンテナサブジェクト。
srvprvAssignFromGroup	プロキシまたは委任ユーザの割り当てのグループサブジェクト。
srvprvAssignFromUser	プロキシまたは委任ユーザの割り当てのユーザサブジェクト。
srvprvAssignToRelationship	委任ユーザ割り当てのターゲット関係。
srvprvAssignToUser	プロキシまたは委任ユーザの割り当てのユーザターゲット。
srvprvCategoryKey	特定のプロビジョニング要求定義をプロビジョニングカテゴリのセットに関連付けます。値は srvprvChoice インスタンスのキーです。
srvprvDefaultTheme	デフォルトのテーマ。
srvprvEntitlementRef	DirXML エンタイトルメントへの参照。
srvprvEntityType	ディレクトリ抽象化レイヤエンティティの定義タイプを指定します。
srvprvFlowStrategy	プロビジョニング要求定義に対して使用するフロー起動方法を指定します。
srvprvGrant	true の場合、プロジェクトリクエスト定義が付与処理をサポートするよう指定するフラグ。
srvprvGroupwiseIMAddress	Groupwise IM アドレス。
srvprvHeaderFillerFile	ヘッダフィラーファイル名。
srvprvHeaderFillerImage	ヘッダフィラー画像。
srvprvHeaderFillerLastMod	ヘッダフィラーの最終更新日時。
srvprvHeaderLogo2File	ヘッダロゴのセカンダリイメージのファイル名。

属性名	説明
srvprvAOLIMAddress	AOL IM アドレス。
srvprvHeaderLogo2Image	ヘッダロゴのセカンダリイメージ。
srvprvHeaderLogo2LastMod	ヘッダロゴのセカンダリの最終更新日時。
srvprvHeaderLogoFile	ヘッダロゴのプライマリイメージのファイル名。
srvprvHeaderLogoImage	ヘッダロゴのプライマリイメージ。
srvprvHeaderLogoLastMod	ヘッダロゴのプライマリの最終更新日時。
srvprvHeaderTextureFile	ヘッダテクスチャファイル名。
srvprvHeaderTextureImage	ヘッダテクスチャイメージ。
srvprvHeaderTextureLastMod	ヘッダテクスチャの最終更新日時。
srvprvIsTaskManager	ユーザがタスクグループマネージャかどうかを示します。
srvprvLocalizedDescrs	プロビジョニング Web アプリケーション、 Designer 、および iManager に対し、ローカライズされた説明文字列のセットを提供します。
srvprvLocalizedNames	プロビジョニング Web アプリケーション、 Designer 、および iManager に対し、ローカライズされた表示名文字列のセットを提供します。
srvprvLoginFile	ログインファイル名。
srvprvLoginImage	ログインイメージ。
srvprvLoginLastMod	ログインの最終更新日時。
srvprvLoginSmallFile	ログインスモールファイル名。
srvprvLoginSmallImage	ログインスモールイメージ。
srvprvLoginSmallLastMod	ログインスモールの最終更新日時。
srvprvModified	ディレクトリモデルコンテナ内の定義オブジェクトインスタンスの変更を示すフラグ。
srvprvNavBckgrColor	ナビゲーションの背景色。
srvprvNavBckgrColorLastMod	ナビゲーションの背景色の最終更新日。
srvprvNavColor	ナビゲーションの色。
srvprvNavColorLastMod	ナビゲーションの色の最終更新日時。
srvprvPreferredLocale	保存されたクエリや検索条件のリスト。
srvprvProcessXML	ワークフローおよびプロビジョニングアクションを含むプロビジョニングプロセス定義を表す XML ドキュメント。
srvprvRequestDefName	委任定義に関連付けられているプロビジョニング要求定義名。
srvprvRequestXML	初期の要求フォームとそのデータバインドを表す XML ドキュメント。
srvprvRevoke	true の場合、プロジェクトリクエスト定義が拒否処理をサポートするよう指定するフラグ。

属性名	説明
srvprvAOLIMAddress	AOL IM アドレス。
srvprvStatus	プロビジョニングオブジェクトのステータスを指定します。サポートされている値には次が含まれます。
srvprvTaskGroups	ユーザがタスクマネージャであるグループ。
srvprvUUID	ポートレットの固有の識別子。
srvprvTaskManager	タスクグループのタスクマネージャ。
srvprvYahooIMAddress	Yahoo IM アドレス。

A.2 Objectclass のスキーマ拡張

OBJECTCLASS 名	説明
srvprvAppConfig	DirXML ドライバの親が接続するプロビジョニングシステムのアプリケーション設定オブジェクトのコンテナ。
srvprvAppDefs	プロビジョニングランタイム環境 (Identity ポータルのテーマなど) を初期化するために使用される設定オブジェクトのコンテナ。
srvprvAssetRecipientAux	ユーザに対する非 IT 資産のプロビジョニングを記録します。
srvprvChoice	Identity ポートレットおよび他の Web アプリケーションコンポーネントで使用するため、特定の属性に割り当てたり、クエリで使用したりする値の列挙。
srvprvChoiceDefs	Identity ポートレットおよび Web アプリケーションによって公開されるディレクトリ抽象化レイヤ選択肢の定義のコンテナ。
srvprvDelegateeAssignment	委任ユーザの割り当ての定義。
srvprvDelegateeDefs	委任ユーザの定義のコンテナ。
srvprvDirectoryModel	ディレクトリ抽象化レイヤのメタレベルオブジェクトのコンテナで、Identity ポートレットおよび Web アプリケーションによって公開されるディレクトリの選択内容。
srvprvDirectoryModelConfig	ランタイムディレクトリ抽象化レイヤの環境設定パラメータ。
srvprvEntity	ディレクトリ内にある定義済みクラスの選択属性のビューを定義します。Identity ポートレットおよび他の Web アプリケーションコンポーネントによって使用されます。
srvprvEntityAux	標準の ObjectClass。
srvprvEntityDefs	Identity ポートレットおよび Web アプリケーションによって公開されるディレクトリ抽象化レイヤエンティティの定義のコンテナ。
srvprvProxyAssignment	プロキシの割り当ての定義。
srvprvProxyDefs	プロキシ定義のコンテナ。

OBJECTCLASS 名	説明
srvprvAppConfig	DirXML ドライバの親が接続するプロビジョニングシステムのアプリケーション設定オブジェクトのコンテナ。
srvprvRelationship	Identity ポートレットおよび他の Web アプリケーションコンポーネントで使用できるように、ディレクトリ内のオブジェクトの関係を定義します。
srvprvRelationshipDefs	Identity ポートレットおよび Web アプリケーションによって公開されるディレクトリ抽象化レイヤ関係の定義のコンテナ。
srvprvRequest	許可または拒否するプロビジョニング可能な項目を 1 つ公開します。ワークフローおよびプロビジョニングターゲットのランタイムの側面を定義するワークフロープロセスが含まれます。
srvprvRequestDefs	Web アプリケーションランタイムに対してプロビジョニング可能な項目のセットであるプロビジョニング要求定義のコンテナ。
srvprvResource	プロビジョニング実行操作のために、実行するディレクトリ割り当てのセットを定義します (許可または拒否)。
srvprvResourceDefs	プロビジョニングターゲット定義のコンテナで、デザインタイムの記述の他にテンプレートや未使用ターゲットも含まれます。
srvprvService	特定のワークフローから Web サービスを起動する方法を記述します。これには、入力値および戻り値の指定が含まれます。
srvprvServiceDefs	サービス定義オブジェクトのコンテナで、ワークフローによって呼び出される Web サービスをラップします。
srvprvTaskGroupAux	サービスプロビジョニングのタスクグループ。
srvprvTheme	テーマオブジェクト。
srvprvUserAux	サービスプロビジョニングのユーザエンティティ。
srvprvWebAppConfig	Web アプリケーション設定オブジェクト。
srvprvWorkflow	プロビジョニングアクションの許可を得るために実行される移動条件を含む動作のネットワークを定義します。
srvprvWorkflowDefs	ワークフローオブジェクトのコンテナで、デザイン時の説明に加え、テンプレートや未使用のフローも含まれます。
srvprvServiceDefs	サービス定義オブジェクトのコンテナで、ワークフローによって呼び出される Web サービスをラップします。
srvprvStatus	プロビジョニングオブジェクトのステータスを指定します。サポートされている値には次が含まれます。
srvprvTaskGroupAux	サービスプロビジョニングのタスクグループ。
srvprvTaskGroups	ユーザがタスクマネージャであるグループ。
srvprvTaskManager	タスクグループのタスクマネージャ。
srvprvTheme	テーマオブジェクト。
srvprvUserAux	サービスプロビジョニングのユーザエンティティ。

OBJECTCLASS 名	説明
srvprvAppConfig	DirXML ドライバの親が接続するプロビジョニングシステムのアプリケーション設定オブジェクトのコンテナ。
srvprvWebAppConfig	Web アプリケーション設定オブジェクト。
srvprvWorkflow	プロビジョニングアクションの許可を得るために実行される移動条件を含む動作のネットワークを定義します。
srvprvWorkflowDefs	ワークフローオブジェクトのコンテナで、デザイン時の説明に加え、テンプレートや未使用のフローも含まれます。
srvprvYahooIMAddress	Yahoo IM アドレス。

A.3 LDIF の表現

次に、構文、包含ルール、および上の概要表に記載されていない他の情報を含む完全なスキーマ情報を説明します (LDIF 形式)。この情報は変更される場合があります。

```

version:1 # Copyright (c) 2004-2005 Unpublished Work of Novell, Inc.
All Rights # Reserved.# # THIS WORK IS AN UNPUBLISHED WORK AND CONTAINS
CONFIDENTIAL, # PROPRIETARY AND TRADE SECRET INFORMATION OF NOVELL,
INC. ACCESS TO # THIS WORK IS RESTRICTED TO (I) NOVELL, INC. EMPLOYEES
WHO HAVE A NEED # TO KNOW HOW TO PERFORM TASKS WITHIN THE SCOPE OF
THEIR ASSIGNMENTS AND # (II) ENTITIES OTHER THAN NOVELL, INC. WHO HAVE
ENTERED INTO # APPROPRIATE LICENSE AGREEMENTS.NO PART OF THIS WORK MAY
BE USED, # PRACTICED, PERFORMED, COPIED, DISTRIBUTED, REVISED,
MODIFIED, # TRANSLATED, ABRIDGED, CONDENSED, EXPANDED, COLLECTED,
COMPILED, # LINKED, RECAST, TRANSFORMED OR ADAPTED WITHOUT THE PRIOR
WRITTEN # CONSENT OF NOVELL, INC. ANY USE OR EXPLOITATION OF THIS WORK
WITHOUT # AUTHORIZATION COULD SUBJECT THE PERPETRATOR TO CRIMINAL AND
CIVIL # LIABILITY.# # Base schema extensions for SpitFire # # Last
Modified:6/27/05 (ek) # # See rfc2252 for information on attribute
syntax definitions # String = 1.3.6.1.4.1.1466.115.121.1.15 #
Boolean = 1.3.6.1.4.1.1466.115.121.1.7 # Octet String =
1.3.6.1.4.1.1466.115.121.1.40 # DN = 1.3.6.1.4.1.1466.115.121.1.12 #
Case Exact String = 1.3.6.1.4.1.1466.115.121.1.26 # Case Ignore List
= 2.16.840.1.113719.1.1.5.1.6 # Case Ignore String =
1.3.6.1.4.1.1466.115.121.1.15 # Stream =
1.3.6.1.4.1.1466.115.121.1.5 # Time = 1.3.6.1.4.1.1466.115.121.1.24
# # OID registered for EPM:# subarc "450" registered at:https://
wiki.innerweb.novell.com/wiki.phtml?title=OID_Registration #
attribute prefix:2.16.840.1.113719.1.450.4.{3 digit unique per
attribute} # object class prefix:2.16.840.1.113719.1.450.6.{3 digit
unique number per class} #-----
----- #-- Framework Attributes #-----
-----
----- dn:cn=schema changetype:modify
add:attributeTypes attributeTypes:( 2.16.840.1.113719.1.450.4.127 NAME
'srvprvUUID' DESC 'iWèÀÇÃëÆé´' SYNTAX
1.3.6.1.4.1.1466.115.121.1.26{64512} SINGLE-VALUE X-NDS_PUBLIC_READ

```

```

'1' X-NDS_NOT_SCHED_SYNC_IMMEDIATE '1' ) dn:cn=schema
changetype:modify add:objectClasses objectClasses:(
2.16.840.1.113719.1.450.6.127 NAME 'srvprvEntityAux' DESC 'Standard
ObjectClass' AUXILIARY MAY srvprvUUID X-NDS_NOT_CONTAINER '1' ) #-----
-----
----- #-- User Attributes
#-----
----- dn:cn=schema
changetype:modify add:attributeTypes attributeTypes:(
2.16.840.1.113719.1.450.4.60 NAME 'srvprvHideUser' DESC 'Indicates if
a user is hidden during searches' SYNTAX 1.3.6.1.4.1.1466.115.121.1.7
SINGLE-VALUE ) dn:cn=schema changetype:modify add:attributeTypes
attributeTypes:( 2.16.840.1.113719.1.450.4.61 NAME
'srvprvHideAttributes' DESC 'List of attributes a user is hiding from
other users' SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 ) dn:cn=schema
changetype:modify add:attributeTypes attributeTypes:(
2.16.840.1.113719.1.450.4.62 NAME 'srvprvQueryList' DESC 'List of
saved query/search criteria' SYNTAX 1.3.6.1.4.1.1466.115.121.1.15
SINGLE-VALUE ) dn:cn=schema changetype:modify add:attributeTypes
attributeTypes:( 2.16.840.1.113719.1.450.4.63 NAME
'srvprvCapabilities1' DESC 'Place holder for classifying skills,
knowledge, references, etc. Classifications are defined in the
application.' SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 ) dn:cn=schema
changetype:modify add:attributeTypes attributeTypes:(
2.16.840.1.113719.1.450.4.64 NAME 'srvprvCapabilities2' DESC 'Place
holder for classifying skills, knowledge, references, etc.
Classifications are defined in the application.' SYNTAX
1.3.6.1.4.1.1466.115.121.1.15 ) dn:cn=schema changetype:modify
add:attributeTypes attributeTypes:( 2.16.840.1.113719.1.450.4.65 NAME
'srvprvCapabilities3' DESC 'Place holder for classifying skills,
knowledge, references, etc. Classifications are defined in the
application.' SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 ) dn:cn=schema
changetype:modify add:attributeTypes attributeTypes:(
2.16.840.1.113719.1.450.4.66 NAME 'srvprvCapabilities4' DESC 'Place
holder for classifying skills, knowledge, references, etc.
Classifications are defined in the application.' SYNTAX
1.3.6.1.4.1.1466.115.121.1.15 ) dn:cn=schema changetype:modify
add:attributeTypes attributeTypes:( 2.16.840.1.113719.1.450.4.67 NAME
'srvprvCapabilities5' DESC 'Place holder for classifying skills,
knowledge, references, etc. Classifications are defined in the
application.' SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 ) dn:cn=schema
changetype:modify add:attributeTypes attributeTypes:(
2.16.840.1.113719.1.450.4.68 NAME 'srvprvIMAddress' DESC 'Key-value
pair of Instant messenger Addresses i.e. groupwise~jsmith' SYNTAX
1.3.6.1.4.1.1466.115.121.1.15 ) # This is temporary until we convert
the application to use the multi-value IM address (srvprvIMAddress)
above dn:cn=schema changetype:modify add:attributeTypes
attributeTypes:( 2.16.840.1.113719.1.450.4.69 NAME
'srvprvGroupwiseIMAddress' DESC 'Groupwise IM address' SYNTAX
1.3.6.1.4.1.1466.115.121.1.15 SINGLE-VALUE ) # This is temporary until
we convert the application to use the multi-value IM address
(srvprvIMAddress) above dn:cn=schema changetype:modify
add:attributeTypes attributeTypes:( 2.16.840.1.113719.1.450.4.70 NAME
'srvprvYahooIMAddress' DESC 'Yahoo IM address' SYNTAX

```

```

1.3.6.1.4.1.1466.115.121.1.15 SINGLE-VALUE ) # This is temporary until
we convert the application to use the multi-value IM address
(srvprvIMAddress) above dn:cn=schema changetype:modify
add:attributeTypes attributeTypes:( 2.16.840.1.113719.1.450.4.71 NAME
'srvprvAOLIMAddress' DESC 'AOL IM address' SYNTAX
1.3.6.1.4.1.1466.115.121.1.15 SINGLE-VALUE ) dn:cn=schema
changetype:modify add:attributeTypes attributeTypes:(
2.16.840.1.113719.1.450.4.72 NAME 'srvprvActiveDelegates' DESC 'The
active delegates of a user' SYNTAX 2.16.840.1.113719.1.1.5.1.6 )
dn:cn=schema changetype:modify add:attributeTypes attributeTypes:(
2.16.840.1.113719.1.450.4.73 NAME 'srvprvActiveDelegators' DESC 'The
active delegators of a user' SYNTAX 2.16.840.1.113719.1.1.5.1.6 )
dn:cn=schema changetype:modify add:attributeTypes attributeTypes:(
2.16.840.1.113719.1.450.4.74 NAME 'srvprvIsTaskManager' DESC
'Indicates if user is a task group manager' SYNTAX
1.3.6.1.4.1.1466.115.121.1.7 SINGLE-VALUE ) dn:cn=schema
changetype:modify add:attributeTypes attributeTypes:(
2.16.840.1.113719.1.450.4.75 NAME 'srvprvTaskGroups' DESC 'Groups for
which the user is a task manager' SYNTAX
1.3.6.1.4.1.1466.115.121.1.12 ) dn:cn=schema changetype:modify
add:attributeTypes attributeTypes:( 2.16.840.1.113719.1.450.4.77 NAME
'srvprvPreferredLocale' DESC 'List of saved query/search criteria'
SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 SINGLE-VALUE ) dn:cn=schema
changetype:modify add:objectclasses objectClasses:(
2.16.840.1.113719.1.450.6.128 NAME 'srvprvUserAux' DESC 'Service
provisioning user entity' AUXILIARY MAY ( srvprvHideUser $
srvprvHideAttributes $ srvprvQueryList $ srvprvCapabilities1 $
srvprvCapabilities2 $ srvprvCapabilities3 $ srvprvCapabilities4 $
srvprvCapabilities5 $ srvprvIMAddress $ srvprvGroupwiseIMAddress $
srvprvYahooIMAddress $ srvprvAOLIMAddress $ srvprvIsTaskManager $
srvprvTaskGroups $ srvprvActiveDelegates $ srvprvActiveDelegators $
srvprvPreferredLocale) X-NDS_NOT_CONTAINER '1' ) dn:cn=schema
changetype:modify add:attributeTypes attributeTypes:(
2.16.840.1.113719.1.450.4.129 NAME 'srvprvTaskManager' DESC 'Task
manager of the task group' SYNTAX 1.3.6.1.4.1.1466.115.121.1.12 )
dn:cn=schema changetype:modify add:objectclasses objectClasses:(
2.16.840.1.113719.1.450.6.130 NAME 'srvprvTaskGroupAux' DESC 'Service
provisioning task group' AUXILIARY MAY ( srvprvTaskManager ) X-
NDS_NOT_CONTAINER '1' ) #-----
-----
----- #-- Provisioning Attributes #-----
-----
----- dn:cn=schema changetype:modify
add:attributeTypes attributeTypes:( 2.16.840.1.113719.1.450.4.100 NAME
'srvprvCategoryKey' DESC 'Associates a given Provisioning Request
Definition to a set of provisioning categories.Values are keys to a
srvprvChoice instance.' SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 )
dn:cn=schema changetype:modify add:attributeTypes attributeTypes:(
2.16.840.1.113719.1.450.4.101 NAME 'srvprvGrant' DESC 'Flag which if
true specifies that the Provisioning Request Definition supports a
Grant operation.' SYNTAX 1.3.6.1.4.1.1466.115.121.1.7 SINGLE-VALUE )
dn:cn=schema changetype:modify add:attributeTypes attributeTypes:(
2.16.840.1.113719.1.450.4.102 NAME 'srvprvRevoke' DESC 'Flag which if
true specifies that the Provisioning Request Definition supports a

```

```

Revoke operation.' SYNTAX 1.3.6.1.4.1.1466.115.121.1.7 SINGLE-VALUE )
dn:cn=schema changetype:modify add:attributeTypes attributeTypes:(
2.16.840.1.113719.1.450.4.103 NAME 'srvprvFlowStrategy' DESC
'Specifies the flow invocation strategy to be used for the Provisioning
Request Definition.' SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 SINGLE-VALUE
) dn:cn=schema changetype:modify add:attributeTypes attributeTypes:(
2.16.840.1.113719.1.450.4.104 NAME 'srvprvLocalizedNames' DESC
'Provides set of localized display name strings for the provisioning
web applications, Designers and iManager.' SYNTAX
1.3.6.1.4.1.1466.115.121.1.26 ) dn:cn=schema changetype:modify
add:attributeTypes attributeTypes:( 2.16.840.1.113719.1.450.4.105 NAME
'srvprvLocalizedDescrs' DESC 'Provides set of localized description
strings for the provisioning web applications, Designers and
iManager.' SYNTAX 1.3.6.1.4.1.1466.115.121.1.26 ) dn:cn=schema
changetype:modify add:attributeTypes attributeTypes:(
2.16.840.1.113719.1.450.4.106 NAME 'srvprvStatus' DESC 'Specifies the
status of the Provisioning Object.Supported values will
include:Inactive, Active, Template, and Retired.' SYNTAX
1.3.6.1.4.1.1466.115.121.1.26 SINGLE-VALUE ) dn:cn=schema
changetype:modify add:attributeTypes attributeTypes:(
2.16.840.1.113719.1.450.4.107 NAME 'srvprvProcessXML' DESC 'XML
document representing a Provisioning process definition including
Workflow and Provisioning Action.' SYNTAX
1.3.6.1.4.1.1466.115.121.1.5 SINGLE-VALUE ) dn:cn=schema
changetype:modify add:attributeTypes attributeTypes:(
2.16.840.1.113719.1.450.4.108 NAME 'srvprvEntityType' DESC 'Specifies
Directory Abstraction Layer Entity definition type:P-Public
definitions or S-System definitions.' SYNTAX
1.3.6.1.4.1.1466.115.121.1.15 SINGLE-VALUE ) dn:cn=schema
changetype:modify add:attributeTypes attributeTypes:(
2.16.840.1.113719.1.450.4.109 NAME 'srvprvRequestXML' DESC 'XML
document representing the initial request form and its data bindings'
SYNTAX 1.3.6.1.4.1.1466.115.121.1.5 SINGLE-VALUE ) dn:cn=schema
changetype:modify add:attributeTypes attributeTypes:(
2.16.840.1.113719.1.450.4.110 NAME 'srvprvModified' DESC 'Flag to
indicate changes to definitions object instances in the directory
model container' SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 SINGLE-VALUE )
dn:cn=schema changetype:modify add:attributeTypes attributeTypes:(
2.16.840.1.113719.1.450.4.111 NAME 'srvprvEntitlementRef' DESC
'Reference to a DirXML-Entitlement' SYNTAX
1.3.6.1.4.1.1466.115.121.1.12 SINGLE-VALUE ) #-----
-----
----- #-- Provisioning Configuration
Containers #-----
-----
dn:cn=schema changetype:modify add:objectclasses objectClasses:(
2.16.840.1.113719.1.450.6.100 NAME 'srvprvAppConfig' DESC 'Container
for application configuration objects of the Provisioning System to
which its DirXML-Driver parent connects.' SUP top STRUCTURAL MUST ( cn
$ version ) MAY ( description ) X-NDS_NAMING ( 'cn' ) X-NDS_CONTAINMENT
( 'DirXML-Driver' ) ) dn:cn=schema changetype:modify add:objectclasses
objectClasses:( 2.16.840.1.113719.1.450.6.101 NAME 'srvprvRequestDefs'
DESC 'Container for Provisioning Request Definitions, the set of
provisionable items to the Web Application run-time.' SUP top

```

```

STRUCTURAL MUST ( cn ) MAY ( description ) X-NDS_NAMING ( 'cn' ) X-
NDS_CONTAINMENT ( 'srvprvAppConfig' ) ) dn:cn=schema changetype:modify
add:objectclasses objectClasses:( 2.16.840.1.113719.1.450.6.102 NAME
'srvprvWorkflowDefs' DESC 'Container for Workflow objects, including
design-time descriptions plus any template or unused flows.' SUP top
STRUCTURAL MUST ( cn ) MAY ( description ) X-NDS_NAMING ( 'cn' ) X-
NDS_CONTAINMENT ( 'srvprvAppConfig' ) ) dn:cn=schema changetype:modify
add:objectclasses objectClasses:( 2.16.840.1.113719.1.450.6.103 NAME
'srvprvResourceDefs' DESC 'Container for Provisioning Target
definitions, including design-time descriptions plus any template or
unused targets.' SUP top STRUCTURAL MUST ( cn ) MAY ( description ) X-
NDS_NAMING ( 'cn' ) X-NDS_CONTAINMENT ( 'srvprvAppConfig' ) )
dn:cn=schema changetype:modify add:objectclasses objectClasses:(
2.16.840.1.113719.1.450.6.104 NAME 'srvprvServiceDefs' DESC 'Container
for Service Definition objects, which wrap Web Services called by
Workflows.' SUP top STRUCTURAL MUST ( cn ) MAY ( description ) X-
NDS_NAMING ( 'cn' ) X-NDS_CONTAINMENT ( 'srvprvAppConfig' ) )
dn:cn=schema changetype:modify add:objectclasses objectClasses:(
2.16.840.1.113719.1.450.6.105 NAME 'srvprvDirectoryModel' DESC
'Container for Directory Abstraction Layer meta-level objects,
selected contents of the directory to be exposed by the Identity
Portlets and Web Applications.' SUP top STRUCTURAL MUST ( cn ) MAY (
description $ srvprvModified ) X-NDS_NAMING ( 'cn' ) X-NDS_CONTAINMENT
( 'srvprvAppConfig' ) ) dn:cn=schema changetype:modify
add:objectclasses objectClasses:( 2.16.840.1.113719.1.450.6.106 NAME
'srvprvAppDefs' DESC 'Container for configuration objects used to
initialise the Provisioning run-time environment, such as themes for
the Identity Portal.' SUP top STRUCTURAL MUST ( cn ) MAY ( description
) X-NDS_NAMING ( 'cn' ) X-NDS_CONTAINMENT ( 'srvprvAppConfig' ) )
dn:cn=schema changetype:modify add:objectclasses objectClasses:(
2.16.840.1.113719.1.450.6.111 NAME 'srvprvEntityDefs' DESC 'Container
for Directory Abstraction Layer Entity defintions, to be exposed by the
Identity Portlets and Web Applications.' SUP top STRUCTURAL MUST ( cn )
MAY ( description ) X-NDS_NAMING ( 'cn' ) X-NDS_CONTAINMENT (
'srvprvDirectoryModel' ) ) dn:cn=schema changetype:modify
add:objectclasses objectClasses:( 2.16.840.1.113719.1.450.6.112 NAME
'srvprvRelationshipDefs' DESC 'Container for Directory Abstraction
Layer Relationship definitions, to be exposed by the Identity Portlets
and Web Applications.' SUP top STRUCTURAL MUST ( cn ) MAY ( description
) X-NDS_NAMING ( 'cn' ) X-NDS_CONTAINMENT ( 'srvprvDirectoryModel' ) )
dn:cn=schema changetype:modify add:objectclasses objectClasses:(
2.16.840.1.113719.1.450.6.113 NAME 'srvprvChoiceDefs' DESC 'Container
for Directory Abstraction Layer Choice definitions, to be exposed by
the Identity Portlets and Web Applications.' SUP top STRUCTURAL MUST (
cn ) MAY ( description ) X-NDS_NAMING ( 'cn' ) X-NDS_CONTAINMENT (
'srvprvDirectoryModel' ) ) ##### Provisioning Configuration Object
Classes dn:cn=schema changetype:modify add:objectclasses
objectClasses:( 2.16.840.1.113719.1.450.6.107 NAME 'srvprvRequest'
DESC 'Exposes one provisionable item to be granted or revoked,
including the workflow process which defines the run-time aspects of
the Workflow and Provisioning Target.' SUP top STRUCTURAL MUST ( cn $
srvprvStatus $ srvprvFlowStrategy $ srvprvGrant $ srvprvRevoke $
srvprvCategoryKey $ srvprvLocalizedNames $ srvprvLocalizedDescrs ) MAY
( description $ srvprvEntitlementRef $ XmlData $ srvprvRequestXML $

```

```

srvprvProcessXML ) X-NDS_NOT_CONTAINER '1' X-NDS_NAMING ( 'cn' ) X-
NDS_CONTAINMENT ( 'srvprvRequestDefs' ) ) dn:cn=schema
changetype:modify add:objectclasses objectClasses:(
2.16.840.1.113719.1.450.6.108 NAME 'srvprvWorkflow' DESC 'Defines the
network of activites including traversal conditions to be executed in
order to obtain approval for a provisioning action.' SUP top STRUCTURAL
MUST ( cn $ srvprvLocalizedNames $ srvprvLocalizedDescrs ) MAY (
description $ XmlData ) X-NDS_NOT_CONTAINER '1' X-NDS_NAMING ( 'cn' )
X-NDS_CONTAINMENT ( 'srvprvWorkflowDefs' ) ) dn:cn=schema
changetype:modify add:objectclasses objectClasses:(
2.16.840.1.113719.1.450.6.109 NAME 'srvprvResource' DESC 'Defines the
set of directory assignments to execute for a provisioning fulfillment
operation (either Grant or Revoke).' SUP top STRUCTURAL MUST ( cn $
srvprvLocalizedNames $ srvprvLocalizedDescrs ) MAY ( description $
srvprvEntitlementRef $ XmlData ) X-NDS_NOT_CONTAINER '1' X-NDS_NAMING
( 'cn' ) X-NDS_CONTAINMENT ( 'srvprvResourceDefs' ) ) dn:cn=schema
changetype:modify add:objectclasses objectClasses:(
2.16.840.1.113719.1.450.6.110 NAME 'srvprvService' DESC 'Describes how
to invoke a specific Web Service from an Workflow.This includes
specification of input and return values.' SUP top STRUCTURAL MUST ( cn
) MAY ( description $ XmlData ) X-NDS_NOT_CONTAINER '1' X-NDS_NAMING (
'cn' ) X-NDS_CONTAINMENT ( 'srvprvServiceDefs' ) ) dn:cn=schema
changetype:modify add:objectclasses objectClasses:(
2.16.840.1.113719.1.450.6.114 NAME 'srvprvEntity' DESC 'Defines a view
of selected attributes for defined classes in the directory, used by
the Identity Portlets and other Web Application components.' SUP top
STRUCTURAL MUST ( cn $ srvprvEntityType ) MAY ( description $ XmlData )
X-NDS_NOT_CONTAINER '1' X-NDS_NAMING ( 'cn' ) X-NDS_CONTAINMENT (
'srvprvEntityDefs' ) ) dn:cn=schema changetype:modify
add:objectclasses objectClasses:( 2.16.840.1.113719.1.450.6.115 NAME
'srvprvRelationship' DESC 'Defines relationships between objects in
the directory, for use in the Identity Portlets and other Web
Application components.' SUP top STRUCTURAL MUST ( cn ) MAY (
description $ XmlData ) X-NDS_NOT_CONTAINER '1' X-NDS_NAMING ( 'cn' )
X-NDS_CONTAINMENT ( 'srvprvRelationshipDefs' ) ) dn:cn=schema
changetype:modify add:objectclasses objectClasses:(
2.16.840.1.113719.1.450.6.116 NAME 'srvprvChoice' DESC 'Enumeration of
values which can be assigned to a particular attribute, used in a
query, etc. for use in the Identity Portlets and other Web Application
components.' SUP top STRUCTURAL MUST ( cn ) MAY ( description $ XmlData
) X-NDS_NOT_CONTAINER '1' X-NDS_NAMING ( 'cn' ) X-NDS_CONTAINMENT (
'srvprvChoiceDefs' ) ) dn:cn=schema changetype:modify
add:objectclasses objectClasses:( 2.16.840.113719.1.450.6.117 NAME
'srvprvDirectoryModelConfig' DESC 'Runtime Directory Abstraction Layer
configurariion parameters' SUP top STRUCTURAL MUST ( cn ) MAY (
description $ XmlData ) X-NDS_NOT_CONTAINER '1' X-NDS_NAMING ( 'cn' )
X-NDS_CONTAINMENT ( 'srvprvDirectoryModel' ) ) ##### User Aux Classes
and Attributes dn:cn=schema changetype:modify add:attributeTypes
attributeTypes:( 2.16.840.1.113719.1.450.4.80 NAME 'srvprvAssetRef'
DESC 'Representation of the aggregate asset properties for a named
asset associated to a user via the srvprvAssetRecipientAux class.'
SYNTAX 2.16.840.1.113719.1.1.5.1.6 ) dn:cn=schema changetype:modify
add:objectclasses objectClasses:( 2.16.840.1.113719.1.450.6.80 NAME
'srvprvAssetRecipientAux' DESC 'Records the provisioning of non-IT

```

```

assets on a user' AUXILIARY MAY ( srvprvAssetRef ) ) #-----
-----
----- #-- Web Application Config
Class #-----
-----
dn:cn=schema changetype:modify add:attributeTypes
attributeTypes:(2.16.840.1.113719.1.450.4.20 NAME 'srvprvDefaultTheme'
DESC 'The default theme' SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 SINGLE-
VALUE ) dn:cn=schema changetype:modify add:objectclasses
objectClasses:( 2.16.840.1.113719.1.450.6.21 NAME 'srvprvWebAppConfig'
DESC 'Web Application Config Object' SUP top STRUCTURAL MUST (cn) MAY
(description $ srvprvDefaultTheme $ XmlData ) X-NDS_NOT_CONTAINER '1'
X-NDS_NAMING 'cn' X-NDS_CONTAINMENT ( 'srvprvAppDefs' ) ) #-----
-----
----- #-- Theme Branding
Structural Class #-----
-----
-- dn:cn=schema changetype:modify add:attributeTypes attributeTypes:(
2.16.840.1.113719.1.450.4.21 NAME 'srvprvHeaderLogoImage' DESC 'Header
Logo Primary Image' SYNTAX 1.3.6.1.4.1.1466.115.121.1.5 SINGLE-VALUE )
dn:cn=schema changetype:modify add:attributeTypes attributeTypes:(
2.16.840.1.113719.1.450.4.22 NAME 'srvprvHeaderLogoFile' DESC 'Header
Logo Primary Image File Name' SYNTAX 1.3.6.1.4.1.1466.115.121.1.15
SINGLE-VALUE ) dn:cn=schema changetype:modify add:attributeTypes
attributeTypes:( 2.16.840.1.113719.1.450.4.23 NAME
'srvprvHeaderLogoLastMod' DESC 'Header Logo Primary Last Modified'
SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 SINGLE-VALUE ) dn:cn=schema
changetype:modify add:attributeTypes attributeTypes:(
2.16.840.1.113719.1.450.4.24 NAME 'srvprvHeaderLogo2Image' DESC
'Header Logo Secondary Image' SYNTAX 1.3.6.1.4.1.1466.115.121.1.5
SINGLE-VALUE ) dn:cn=schema changetype:modify add:attributeTypes
attributeTypes:( 2.16.840.1.113719.1.450.4.25 NAME
'srvprvHeaderLogo2File' DESC 'Header Logo Secondary Image File Name'
SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 | SINGLE-VALUE ) dn:cn=schema
changetype:modify add:attributeTypes attributeTypes:(
2.16.840.1.113719.1.450.4.26 NAME 'srvprvHeaderLogo2LastMod' DESC
'Header Logo Secondary Last Modified' SYNTAX
1.3.6.1.4.1.1466.115.121.1.15 SINGLE-VALUE ) dn:cn=schema
changetype:modify add:attributeTypes attributeTypes:(
2.16.840.1.113719.1.450.4.27 NAME 'srvprvHeaderTextureImage' DESC
'Header Texture Image' SYNTAX 1.3.6.1.4.1.1466.115.121.1.5 SINGLE-
VALUE ) dn:cn=schema changetype:modify add:attributeTypes
attributeTypes:( 2.16.840.1.113719.1.450.4.28 NAME
'srvprvHeaderTextureFile' DESC 'Header Texture File Name' SYNTAX
1.3.6.1.4.1.1466.115.121.1.15 SINGLE-VALUE ) dn:cn=schema
changetype:modify add:attributeTypes attributeTypes:(
2.16.840.1.113719.1.450.4.29 NAME 'srvprvHeaderTextureLastMod' DESC
'Header Texture Last Modified' SYNTAX 1.3.6.1.4.1.1466.115.121.1.15
SINGLE-VALUE ) dn:cn=schema changetype:modify add:attributeTypes
attributeTypes:( 2.16.840.1.113719.1.450.4.30 NAME
'srvprvHeaderFillerImage' DESC 'Header Filler Image' SYNTAX
1.3.6.1.4.1.1466.115.121.1.5 SINGLE-VALUE ) dn:cn=schema
changetype:modify add:attributeTypes attributeTypes:(
2.16.840.1.113719.1.450.4.31 NAME 'srvprvHeaderFillerFile' DESC

```

```

'Header Filler File Name' SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 SINGLE-
VALUE ) dn:cn=schema changetype:modify add:attributeTypes
attributeTypes:( 2.16.840.1.113719.1.450.4.32 NAME
'srvprvHeaderFillerLastMod' DESC 'Header Filler Last Modified' SYNTAX
1.3.6.1.4.1.1466.115.121.1.15 SINGLE-VALUE ) dn:cn=schema
changetype:modify add:attributeTypes attributeTypes:(
2.16.840.1.113719.1.450.4.33 NAME 'srvprvLoginImage' DESC 'Login
Image' SYNTAX 1.3.6.1.4.1.1466.115.121.1.5 SINGLE-VALUE ) dn:cn=schema
changetype:modify add:attributeTypes attributeTypes:(
2.16.840.1.113719.1.450.4.34 NAME 'srvprvLoginFile' DESC 'Login File
Name' SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 SINGLE-VALUE ) dn:cn=schema
changetype:modify add:attributeTypes attributeTypes:(
2.16.840.1.113719.1.450.4.35 NAME 'srvprvLoginLastMod' DESC 'Login
Last Modified' SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 SINGLE-VALUE )
dn:cn=schema changetype:modify add:attributeTypes attributeTypes:(
2.16.840.1.113719.1.450.4.36 NAME 'srvprvLoginSmallImage' DESC 'Login
Small Image' SYNTAX 1.3.6.1.4.1.1466.115.121.1.5 SINGLE-VALUE )
dn:cn=schema changetype:modify add:attributeTypes attributeTypes:(
2.16.840.1.113719.1.450.4.37 NAME 'srvprvLoginSmallFile' DESC 'Login
Small File Name' SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 SINGLE-VALUE )
dn:cn=schema changetype:modify add:attributeTypes attributeTypes:(
2.16.840.1.113719.1.450.4.38 NAME 'srvprvLoginSmallLastMod' DESC
'Login Small Last Modified' SYNTAX 1.3.6.1.4.1.1466.115.121.1.15
SINGLE-VALUE ) dn:cn=schema changetype:modify add:attributeTypes
attributeTypes:( 2.16.840.1.113719.1.450.4.39 NAME 'srvprvNavColor'
DESC 'Navigation Color' SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 SINGLE-
VALUE ) dn:cn=schema changetype:modify add:attributeTypes
attributeTypes:( 2.16.840.1.113719.1.450.4.40 NAME
'srvprvNavColorLastMod' DESC 'Navigation Color Last Modified' SYNTAX
1.3.6.1.4.1.1466.115.121.1.15 SINGLE-VALUE ) dn:cn=schema
changetype:modify add:attributeTypes attributeTypes:(
2.16.840.1.113719.1.450.4.41 NAME 'srvprvNavBckgrColor' DESC
'Navigation Background Color' SYNTAX 1.3.6.1.4.1.1466.115.121.1.15
SINGLE-VALUE ) dn:cn=schema changetype:modify add:attributeTypes
attributeTypes:( 2.16.840.1.113719.1.450.4.42 NAME
'srvprvNavBckgrColorLastMod' DESC 'Navigation Background Color Last
Modified' SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 SINGLE-VALUE )
dn:cn=schema changetype:modify add:objectclasses objectClasses:(
2.16.840.1.113719.1.450.6.20 NAME 'srvprvTheme' DESC 'Theme Object'
SUP top STRUCTURAL MUST (cn) MAY (description $ srvprvHeaderLogoImage
$ srvprvHeaderLogoFile $ srvprvHeaderLogoLastMod $
srvprvHeaderLogo2Image $ srvprvHeaderLogo2File $
srvprvHeaderLogo2LastMod $ srvprvHeaderTextureImage $
srvprvHeaderTextureFile $ srvprvHeaderTextureLastMod $
srvprvHeaderFillerImage $ srvprvHeaderFillerFile $
srvprvHeaderFillerLastMod $ srvprvLoginImage $ srvprvLoginFile $
srvprvLoginLastMod $ srvprvLoginSmallImage $ srvprvLoginSmallFile $
srvprvLoginSmallLastMod $ srvprvNavColor $ srvprvNavColorLastMod $
srvprvNavBckgrColor $ srvprvNavBckgrColorLastMod ) X-NDS_NOT_CONTAINER
'1' X-NDS_CONTAINMENT ( 'srvprvAppDefs' ) X-NDS_NAMING 'cn' ) #-----
-----
----- #-- Attributes,
objects, and containers for Proxy, Delegatee and User availability, #-
-----

```

```

----- dn:cn=schema
changetype:modify add:attributeTypes attributeTypes:(
2.16.840.1.113719.1.450.4.120 NAME 'srvprvAssignFromUser' DESC 'User
subjects of a proxy or delegatee assignment' SYNTAX
1.3.6.1.4.1.1466.115.121.1.12 ) dn:cn=schema changetype:modify
add:attributeTypes attributeTypes:( 2.16.840.1.113719.1.450.4.121 NAME
'srvprvAssignFromGroup' DESC 'Group subjects of a proxy or delegatee
assignment' SYNTAX 1.3.6.1.4.1.1466.115.121.1.12 ) dn:cn=schema
changetype:modify add:attributeTypes attributeTypes:(
2.16.840.1.113719.1.450.4.122 NAME 'srvprvAssignFromContainer' DESC
'Container subjects of a proxy or delegatee assignment' SYNTAX
1.3.6.1.4.1.1466.115.121.1.12 ) dn:cn=schema changetype:modify
add:attributeTypes attributeTypes:( 2.16.840.1.113719.1.450.4.123 NAME
'srvprvAssignToUser' DESC 'The User targets of a proxy or delegatee
assignment' SYNTAX 1.3.6.1.4.1.1466.115.121.1.12 ) dn:cn=schema
changetype:modify add:attributeTypes attributeTypes:(
2.16.840.1.113719.1.450.4.124 NAME 'srvprvAssignToRelationship' DESC
'A target relationship of a delegatee assignment' SYNTAX
1.3.6.1.4.1.1466.115.121.1.15 SINGLE-VALUE ) dn:cn=schema
changetype:modify add:attributeTypes attributeTypes:(
2.16.840.1.113719.1.450.4.125 NAME 'srvprvAssignExpiration' DESC 'Time
at which a proxy or delegatee assignment expires' SYNTAX
1.3.6.1.4.1.1466.115.121.1.24 SINGLE-VALUE ) dn:cn=schema
changetype:modify add:attributeTypes attributeTypes:(
2.16.840.1.113719.1.450.4.126 NAME 'srvprvRequestDefName' DESC 'The
provisioning request definition name associated with a delegatee
definition.' SYNTAX 1.3.6.1.4.1.1466.115.121.1.12 ) dn:cn=schema
changetype:modify add:objectclasses objectClasses:(
2.16.840.1.113719.1.450.6.120 NAME 'srvprvProxyDefs' DESC 'Container
for proxy definitions.' SUP top STRUCTURAL MUST ( cn ) MAY (
description ) X-NDS_NAMING ( 'cn' ) X-NDS_CONTAINMENT (
'srvprvAppConfig' ) ) dn:cn=schema changetype:modify add:objectclasses
objectClasses:( 2.16.840.1.113719.1.450.6.121 NAME
'srvprvDelegateeDefs' DESC 'Container for delegatee definitions.' SUP
top STRUCTURAL MUST ( cn ) MAY ( description ) X-NDS_NAMING ( 'cn' ) X-
NDS_CONTAINMENT ( 'srvprvAppConfig' ) ) dn:cn=schema changetype:modify
add:objectclasses objectClasses:( 2.16.840.1.113719.1.450.6.122 NAME
'srvprvProxyAssignment' DESC 'Proxy assignment definition' SUP top
STRUCTURAL MUST ( cn $ srvprvAssignToUser ) MAY ( description $
srvprvAssignFromUser $ srvprvAssignFromGroup $
srvprvAssignFromContainer $ srvprvAssignExpiration ) X-NDS_NAMING (
'cn' ) X-NDS_CONTAINMENT ( 'srvprvProxyDefs' ) ) dn:cn=schema
changetype:modify add:objectclasses objectClasses:(
2.16.840.1.113719.1.450.6.123 NAME 'srvprvDelegateeAssignment' DESC
'Delegatee assignment definition' SUP top STRUCTURAL MUST cn MAY (
srvprvRequestDefName $ description $ srvprvAssignFromUser $
srvprvAssignFromGroup $ srvprvAssignFromContainer $ srvprvAssignToUser
$ srvprvAssignToRelationship $ srvprvAssignExpiration ) X-NDS_NAMING (
'cn' ) X-NDS_CONTAINMENT ( 'srvprvDelegateeDefs' ) ) ##### DO
NOT DELETE THIS LINE #####
#####

```


アプリケーションアーカイブの設定

この付録では、ユーザアプリケーションの WAR ファイルを編集することによってのみ設定可能な高度な設定について説明します。ここで取り扱う内容は次のとおりです。

- 379 ページのセクション B.1 「ユーザアプリケーション WAR について」
- 379 ページのセクション B.2 「セッションタイムアウトの設定」

B.1 ユーザアプリケーション WAR について

Identity Manager ユーザアプリケーションは、J2EE 準拠の Web アプリケーションアーカイブ (WAR) ファイルとしてパッケージ化されています。ユーザアプリケーション WAR ファイルには、アプリケーションの実行時の動作を制御する Java クラスと XML ファイルの集合が含まれています。一般的には、WAR は変更しないでください。ただし、まれに、アプリケーションの動作を制御するために、WAR ファイルを開いて若干の変更を加えなければならない場合があります。

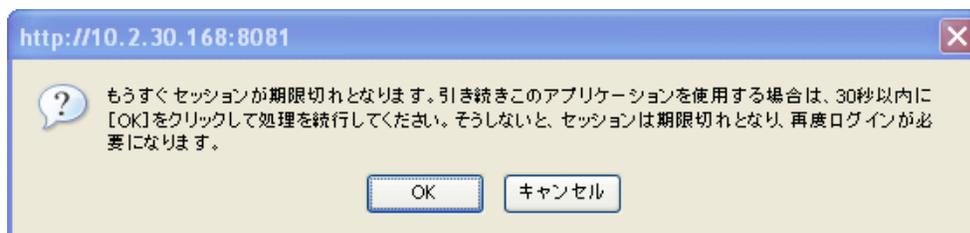
注：この付録の残りの部分では、J2EE の概念と手順に精通していることを想定しています。WAR ファイル内での変更方法がわからない場合は、J2EE のマニュアルを参照してください。

B.2 セッションタイムアウトの設定

サーバが非アクティブなセッションによってオーバーロードするのを防ぐため、Identity Manager ユーザアプリケーションは、長時間非アクティブなままのユーザセッションをタイムアウトさせます。デフォルトのタイムアウト間隔は 10 分です。このデフォルト値を変更するには、ユーザアプリケーション WAR ファイルの WEB-INF フォルダ内にある web.xml ファイルを編集します。

セッションタイムアウト間隔の編集 WAR 内の web.xml ファイルに、<session-timeout> という要素があります (<session-config> 要素の下にあります)。この要素により、セッションがタイムアウトになるまでの非アクティブな時間が指定されます。セッションタイムアウト間隔を設定するには、この要素の値を変更します。値は分単位で指定してください。

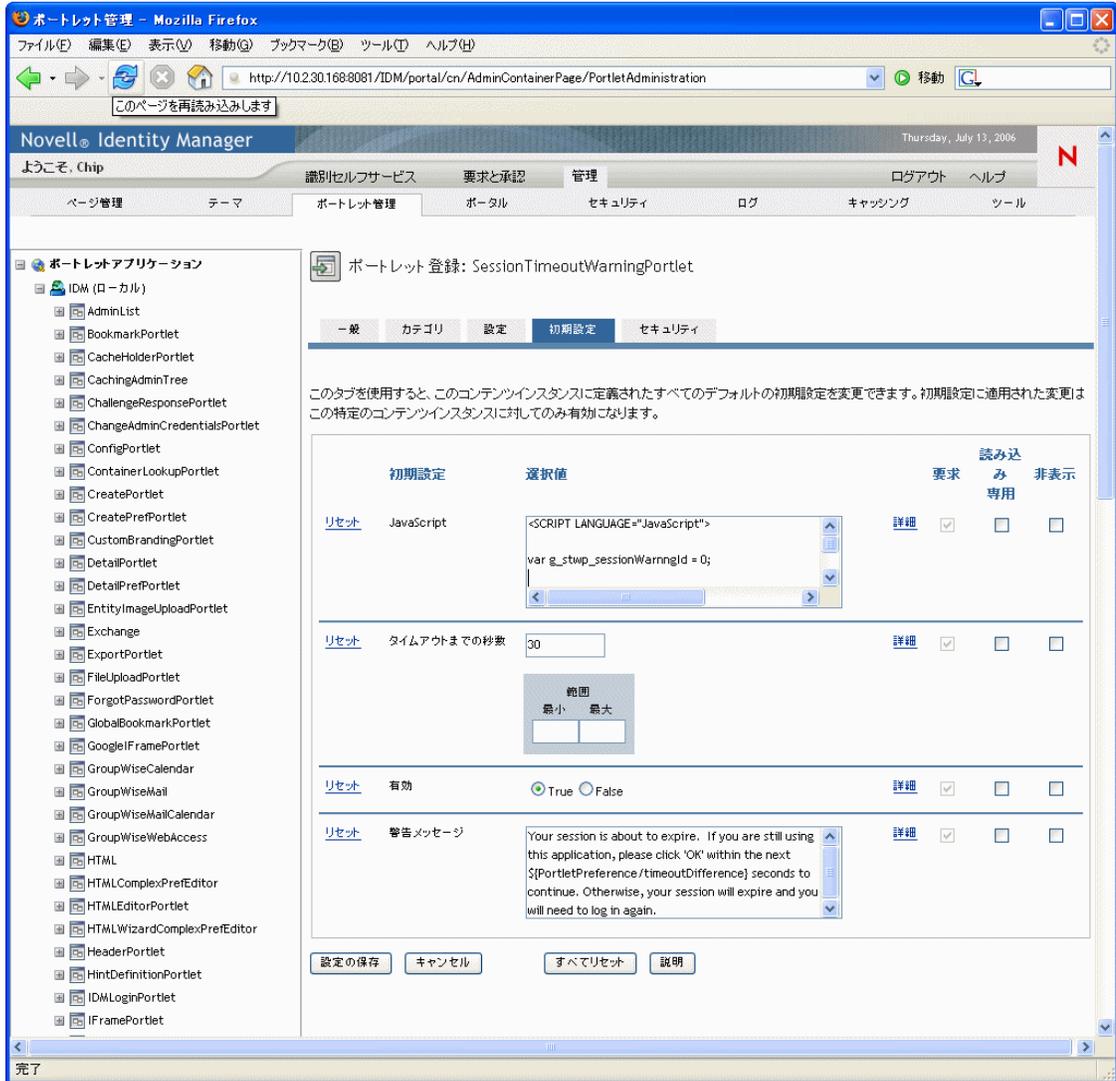
アラートメッセージの動作の制御 デフォルトでは、ユーザのセッションがタイムアウトになる際に、Identity Manager ユーザアプリケーションによってアラートメッセージが表示されます。



ユーザが [OK] をクリックしてメッセージに回答しないと、セッションはタイムアウトになります。アラートメッセージはデフォルトで有効になっています。必要に応じて、こ

れを無効にできます。さらに、ユーザがアラートメッセージに回答するまでの猶予時間を指定することもできます。

アラートメッセージの動作を制御するには、**SessionTimeoutWarningPortlet** を設定する必要があります。このためには、次の図に示すように、ポートレット登録でポートレット初期設定を編集する必要があります。



ユーザがアラートメッセージに回答するまでの猶予時間を指定するには、[タイムアウトまでの秒数] の値を編集します。アラートメッセージを完全に無効にするには、[有効] の横にある [False] をクリックします。変更が終わったら、[設定の保存] をクリックします。