概要

Novell®
Identity Manager

3.6.1

2009 年 5 月 15 日

www.novell.com

保証と著作権

米国 Novell, Inc. およびノベル株式会社は、この文書の内容または使用について、いかなる保証、表明または約束も行っていません。また文書の商品性、および特定の目的への適合性については、明示と黙示を問わず一切保証しないものとします。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、すべてのノベル製ソフトウェアについて、いかなる保証、表明または約束も行っていません。またノベル製ソフトウェアの商品性、および特定の目的への適合性については、明示と黙示を問わず一切保証しないものとします。米国 Novell, Inc. およびノベル株式会社は、ノベル製ソフトウェアの内容を変更する権利を常に留保します。

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

米国 Novell, Inc. は、本文書に記載されている製品に実装されている技術に関する知的所有権を保有します。これらの知的所有権は、「Novell Legal Patents (http://www.novell.com/company/legal/patents/)」の Web ページに記載されている 1 つ以上の米国特許、および米国ならびにその他の国における 1 つ以上の特許または出願中の特許を含む場合があります。

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

オンラインマニュアル: 本製品とその他の Novell 製品の最新のオンラインマニュアルにアクセスするには、Novell Documentation の Web ページ (http://www.novell.com/documentation) を参照してください。

Novell の商標

Novell の商標一覧については、「商標とサービスの一覧 (http://www.novell.com/company/legal/trademarks/tmlist.html)」を参照してください。

サードパーティ資料

サードパーティの商標は、それぞれの所有者に帰属します。

目次

このガイドについて

このガイドは、Novell® Identity Manager が解決に役立つビジネス問題を紹介しています。さらに、ソリューションで使用できる Identity Manager ソフトウェアコンポーネントおよびツールの技術的な概要についても説明しています。このガイドは、以下で構成されています。

対象読者

このガイドは、Identity Manager ビジネスソリューション、テクノロジ、およびツールについて高度なレベルの説明を必要とする管理者、コンサルタント、およびネットワークエンジニアを対象としています。

マニュアルの更新

このマニュアルの最新のバージョンについては、Identity Manager のマニュアルの Web サイト (http://www.novell.com/documentation/idm36/index.html) を参照してください。

追加のマニュアル

Identity Manager の他のドライバに関するマニュアルついては、Identity Manager ドライバの Web サイト (http://www.novell.com/documentation/idm36drivers/index.html) を参照してください。

マニュアルの表記規則

Novell のマニュアルでは、「より大きい」記号 (>) を使用して手順内の操作と相互参照パス内の項目の順序を示します。

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

プラットフォームによっては、シングルパス名に円記号 (\) を使用できる場合とスラッシュ (/) を使用できる場合がありますが、パス名は円記号で表記されます。Linux*、UNIX* など、スラッシュを使う必要があるプラットフォームを使用しているユーザは、必要に応じてスラッシュを使用してください。

1 Identity Manager および ビジネスプロセスの自動化

次の情報で、Novell® Identity Manager システムの実装により自動化できる一部のビジネスプロセスを識別します。Identity Manager が提供しているビジネス自動化ソリューションについてすでに知っている場合は、19 ページの第 2 章「Identity Manager アーキテクチャ」に示されている技術紹介に進んでください。

ID のニーズの管理は、大部分のビジネスの中枢となる機能です。たとえば、月曜の朝を想像してください。キュー内の要求リストを下方向にスクロールします。

- Jim Taylor の携帯電話番号が変更されています。HR データベースおよび他の 4 つの独立したシステムでその情報を更新する必要があります。
- 長い休暇から戻ってきたばかりの Karen Hansen が自分の電子メールのパスワードを忘れてしまっています。彼女がパスワードを取得するか、リセットするのを手伝う必要があります。
- Jose Altimira は先ほど新しい従業員として雇われました。従業員にネットワークアクセスおよび電子メールアカウントを付与する必要があります。
- Ida McNamee が Oracle* 財務データベースにアクセスしたいと考えています。3 名の異なるマネージャから承認を得る必要があります。
- John Harris は買掛金部門から法務部門に異動したところです。法務チームの他のメンバーと同じリソースへのアクセス権を付与し、買掛金リソースへのアクセス権を削除する必要があります。
- 上司の Karl Jones が、Oracle 財務データベースへのアクセス権を求める Ida McNamee による要求を見て、アクセス権を持つユーザの数が増えることを心配しています。上司のためにデータベースへのアクセス権を持つすべてのユーザを表示するレポートを生成する必要があります。

意気込んで最初の要求に着手しますが、すべての要求に対応すること、まして自分に割り当てられた他のプロジェクトを完了するための時間を確保することが難しいことは分かっています。

このような状況が繰り返される職場においては、Identity Manager が役立つ可能性があります。実際に、次の説明で紹介する Identity Manager の主な機能は、以上のすべての業務を含めたさまざまな業務を自動化するのに役立つ可能性があります。お客様のビジネスポリシーに基づいた複数システムのデータ同期に重点を置き、ワークフロー、役割、検証、セルフサービス、監査、およびレポートの機能を組み合わせることにより、IT 組織にとって最も難しく時間のかかる 2 つの業務、ユーザのプロビジョニングおよびパスワードの管理に関与するプロセスを自動化できます。

図 1-1 Identity Manager の主な機能

次のセクションでは、Identity Manager の機能と、これらの機能を組織の識別ニーズをうまく満たすように役立てる方法について紹介します。

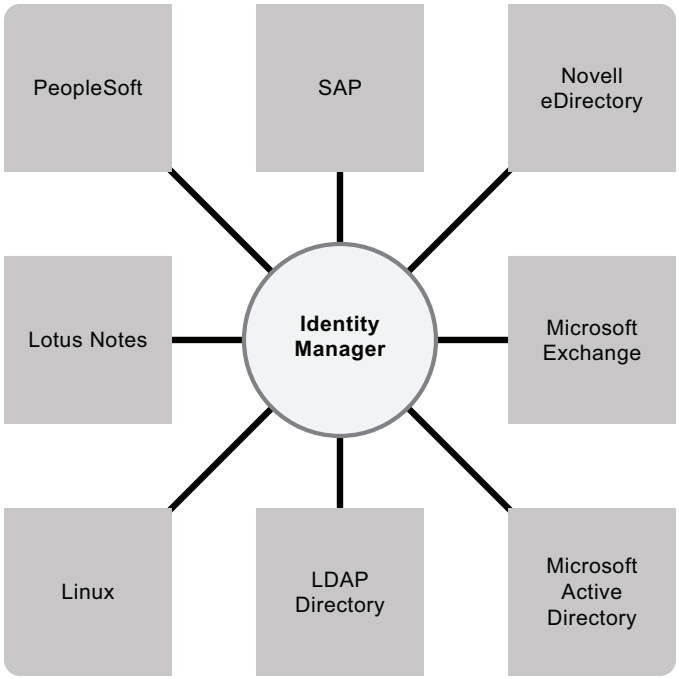
- 10 ページのセクション 1.1「データ同期」
- 13 ページのセクション 1.2「ワークフロー」
- 14 ページのセクション 1.3「役割および検証」
- 15 ページのセクション 1.4「セルフサービス」
- 16 ページのセクション 1.5「監査とレポート」

1.1 データ同期

お客様の組織が特殊なケースでないのであれば、識別データは複数のシステムに格納されています。そうでなければ、1 つのシステムに識別データを格納し、別のシステムでうまく使用できるようにしています。いずれにしても、システム間でデータの共有および同期を容易に実行する必要があります。

Identity Manager を使用すると、SAP*、PeopleSoft*、Lotus Notes*、Microsoft* Exchange、Microsoft Active Directory*、Novell eDirectory™、Linux および UNIX、LDAP ディレクトリなど、広範なアプリケーション、データベース、オペレーティングシステム、およびディレクトリにわたって情報を同期、変換、および配信することができます。

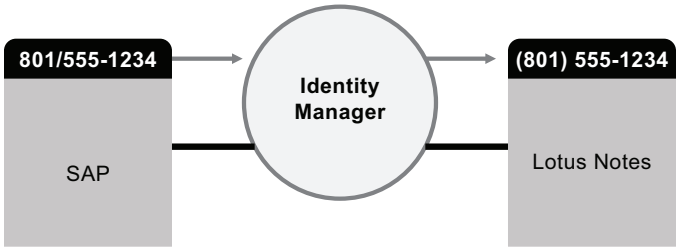
図 1-2 *複数のシステムを接続する Identity Manager*



接続システム間でデータフローを制御します。他のシステム間で、どのデータを共有するか、あるデータに関してどのシステムが権限のあるソースであるか、どのようにしてデータを解釈および変換して他のシステムの要件を満たすのかを決定します。

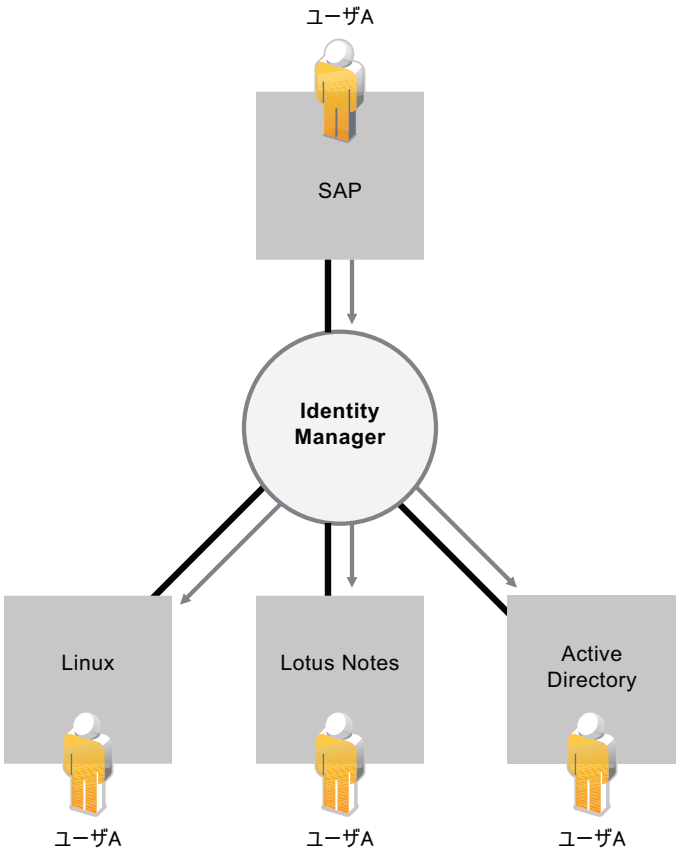
次の図では、ユーザの電話番号に関して権限のあるソースは SAP HR データベースです。Lotus Notes システムでは電話番号を使用するので、Identity Manager で番号を必要な形式に変換し、Lotus Notes システムと共有します。電話番号は SAP HR システムで変更されるたびに、Lotus Notes システムに同期されます。

図 1-3 *接続システム間で同期されるデータ*



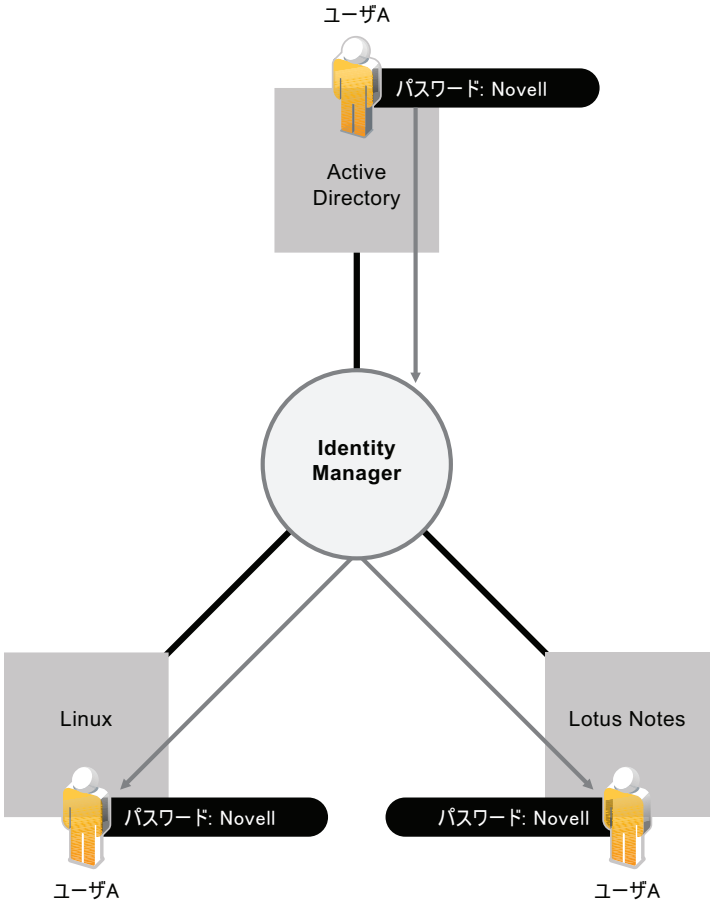
既存のユーザのデータを管理することは、Identity Manager のデータ同期機能の始まりにすぎません。さらに、Identity Manager では、Active Directory などのディレクトリ、PeopleSoft や Lotus Notes などのシステム、および UNIX や Linux などのオペレーティングシステムで、ユーザアカウントを新規作成したり、既存のアカウントを削除したりすることもできます。たとえば、新しい従業員を SAP HR システムに追加する場合、Identity Manager システムでは、Active Directory 内に新しいユーザアカウント、Lotus Notes 内に新しいアカウント、Linux NIS アカウント管理システム内に新しいアカウントを自動的に作成できます。

図 1-4 接続システムでのユーザアカウントの作成



データ同期機能の一環として、Identity Manager をシステム間のパスワードの同期に役立てることもできます。たとえば、ユーザが Active Directory 内の自分のパスワードを変更する場合、Identity Manager によってパスワードを Lotus Notes および Linux に同期することができます。

図 1-5 接続システム間でのパスワードの同期

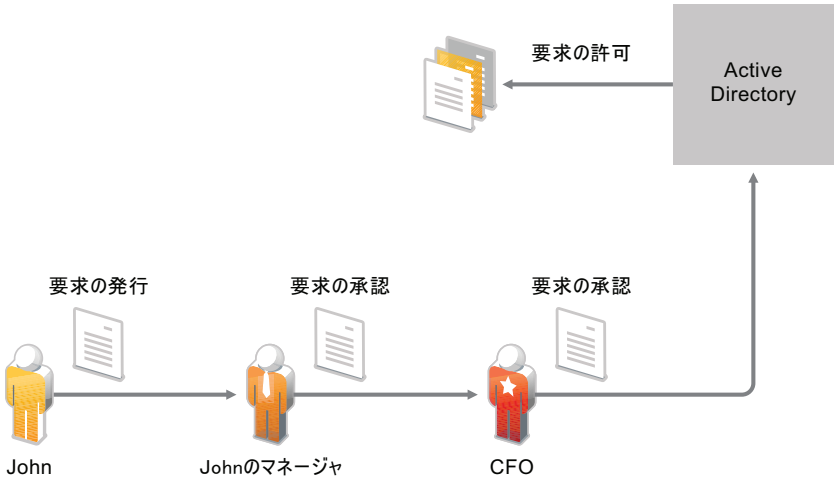


1.2 ワークフロー

ユーザが承認を必要としない組織内の多くのリソースにアクセスすることがあります。ただし、他のリソースへのアクセスは制限されており、1 名以上のユーザからの承認を必要とする可能性があります。

Identity Manager には、プロビジョニングプロセスで適切なリソース承認者を要求するワークフロー機能が備わっています。たとえば、Active Directory アカウントですでに設定されている John が Active Directory を使用して一部の財務レポートにアクセスする必要があるとします。ここでは、John の直接のマネージャと CFO の両方からの承認が必要です。幸いにも、John の要求をマネージャに転送し、マネージャからの承認後に CFO に転送する承認ワークフローがセットアップされています。CFO による承認で、John が経理ドキュメントのアクセスおよび表示を行うのに必要な Active Directory 権限の自動プロビジョニングがトリガされます。

図 1-6 ユーザのプロビジョニングのための承認ワークフロー



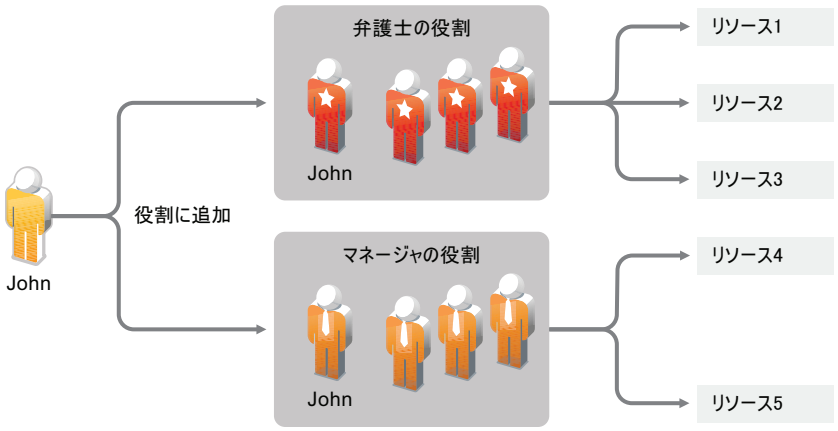
特定のイベントが発生するか (新規ユーザが HR システムに追加される場合など)、ユーザの要求によって手動で開始されるたびにワークフローを自動的に開始することができます。承認がタイミングよく行われるように、プロキシ承認者および承認チームをセットアップすることができます。

1.3 役割および検証

ユーザが組織内の役割に基づいてリソースにアクセスする必要があることがあります。たとえば、法律事務所の弁護士は事務所の弁護士補助員とは異なるリソースのセットにアクセスする必要がある場合があります。

Identity Manager を使用すると、組織の役割に基づいてユーザをプロビジョニングすることができます。役割を定義し、組織のニーズに従って割り当てを行います。ユーザに役割を割り当てると、Identity Manager はその役割に関連付けられているリソースへのアクセス権を持つユーザをプロビジョニングします。ユーザに複数の役割を割り当てる場合、次の図に示すように、そのすべての役割に割り当てられているリソースへのアクセス権を受信します。

図 1-7 役割に基づくリソースのプロビジョニング



組織で発生するイベントの結果としてユーザを役割に自動的に追加することができます (弁護士のジョブタイトルで SAP HR データベースに追加する新規ユーザなど)。役割に追加されるユーザに承認が必要な場合、ワークフローを構築して、役割の要求を適切な承認者にルーティングすることができます。手動でユーザを役割に割り当てることもできます。

場合によっては、役割が競合するため、同じユーザに割り当ててはいけない役割を持っていることがあります。Identity Manager には義務の分離機能があります。この機能を使用すると、組織のユーザが競合を例外にしない限り、競合する役割にユーザが割り当てられることがなくなります。

役割の割り当てによって組織内のリソースに対するユーザのアクセスが決定されるので、適切な割り当てを行う必要があります。不適切な割り当てを行うと、会社および組織の規制の遵守が脅かされる可能性があります。Identity Manager を使用すると、検証プロセスを通じて役割の割り当てが適切であるかどうかを検証することができます。このプロセスで、組織内の担当ユーザが次の役割に関連付けられているデータを認証します。

- **ユーザプロファイルの検証 :** 選択されたユーザは自分のプロファイル情報が正しいかどうかを検証し、間違った情報を変更します。役割の割り当てを変更するには、正しいプロファイル情報が必要です。
- **義務の分離違反検証 :** 担当ユーザが義務の分離違反に関するレポートをレビューし、レポートの正確さを検証します。レポートには、ユーザを競合する役割に割り当てることができる例外のリストが示されています。
- **役割の割り当ての検証 :** 担当ユーザがレポートリストで選択された役割、および各役割に割り当てられたユーザ、グループ、および役割をレビューします。さらに、担当ユーザは情報の正確さを検証する必要があります。
- **ユーザの割り当ての検証 :** 担当ユーザはレポートリストで選択されたユーザ、およびユーザに割り当てられた役割をレビューします。さらに、担当ユーザは情報の正確さを検証する必要があります。

検証レポートは元来、役割の割り当てが正確であること、および競合する役割の例外を許可するのに有効な理由が存在することを保証するのに役立つように設計されています。

1.4 セルフサービス

ビジネスマネージャおよび部門が、スタッフを信頼しないで、自分のユーザの情報およびアクセスのニーズの管理を要求することはよくあります。次の言葉を何度も聞いたことがあるでしょう。「どうして会社のディレクトリにある自分の電話番号を変更できないのか。」または、「私はマーケティング部門にいる。どうしてマーケティング情報のデータベースにアクセスするためにヘルプディスクに電話する必要があるのか。」

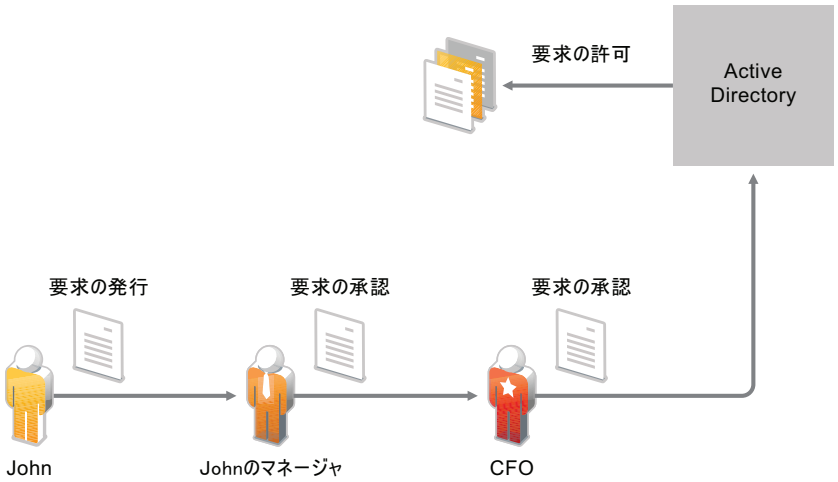
Identity Manager では、責任を負う必要のあるユーザに管理業務を委任できます。たとえば、各ユーザが、

- 会社のディレクトリ内にある各自のデータを管理できるようにすることができます。あなたが電話番号を変更するのではなく、各自が 1 つの場所で電話番号を変更し、Identity Manager によって同期されたすべてのシステムでその番号を変更することもできます。

- パスワードを変更し、忘れたパスワードのヒントを設定し、忘れたパスワードの問題と答えを設定します。ユーザがパスワードを忘れているので、あなたがパスワードをリセットするのではなく、ヒントまたは問題に対する答えを受信した後に、ユーザが自分でパスワードをリセットすることができます。
- データベース、システム、ディレクトリなどのリソースに対するアクセスを要求します。あなたにアプリケーションに対するアクセスを要求するように呼びかけるのではなく、ユーザが使用可能なリソースのリストからアプリケーションを選択することができます。

各ユーザのセルフサービスだけでなく、Identity Manager にはユーザの要求のサポート、監視、および承認を担当する機能についてセルフサービス管理が用意されています。たとえば、13 ページのセクション 1.2「ワークフロー」で使用されている、以下に示すシナリオについて説明します。

図 1-8 *セルフサービスによるプロビジョニングワークフロー*



John が必要とするドキュメントへのアクセスを要求するために Identity Manager セルフサービス機能を使用するだけでなく、John のマネージャと CFO が要求を承認するためにセルフサービス機能を使用します。承認ワークフローを確立すると、John は自分の要求の進行状況を開始および監視でき、John のマネージャと CFO は John の要求に応答することができます。John のマネージャと CFO の承認によって、John が必要とする Active Directory 権限のプロビジョニングがトリガされ、財務ドキュメントの表示およびアクセスが行われます。

1.5 監査とレポート

Identity Manager を使用しないと、ユーザのプロビジョニングは冗長で時間と費用のかかる作業になる可能性があります。ただし、その作業は、プロビジョニングアクティビティが組織のポリシー、要件、および規制を遵守してきたかどうかを検証することよりも不適切である可能性があります。適切なユーザが適切なリソースへのアクセス権を持っていますか。同じリソースから不適切なユーザが削除されていますか。昨日働き始めた従業員は仕事に必要なネットワーク、電子メール、および 6 つの他のシステムに対するアクセス権を持っていますか。先週退職した従業員については、アクセス権をキャンセルしましたか。

Identity Manager を使用すると、監査のためにユーザのプロビジョニングアクティビティをすべて追跡し、ログを記録する作業が軽減することがあります。Identity Manager は発生するすべてのアクティビティに対してイベントメッセージを発行します。Novell Sentinel™ を使用することによって、以下のタイプのレポートを生成するために、これらのメッセージを収集できます。

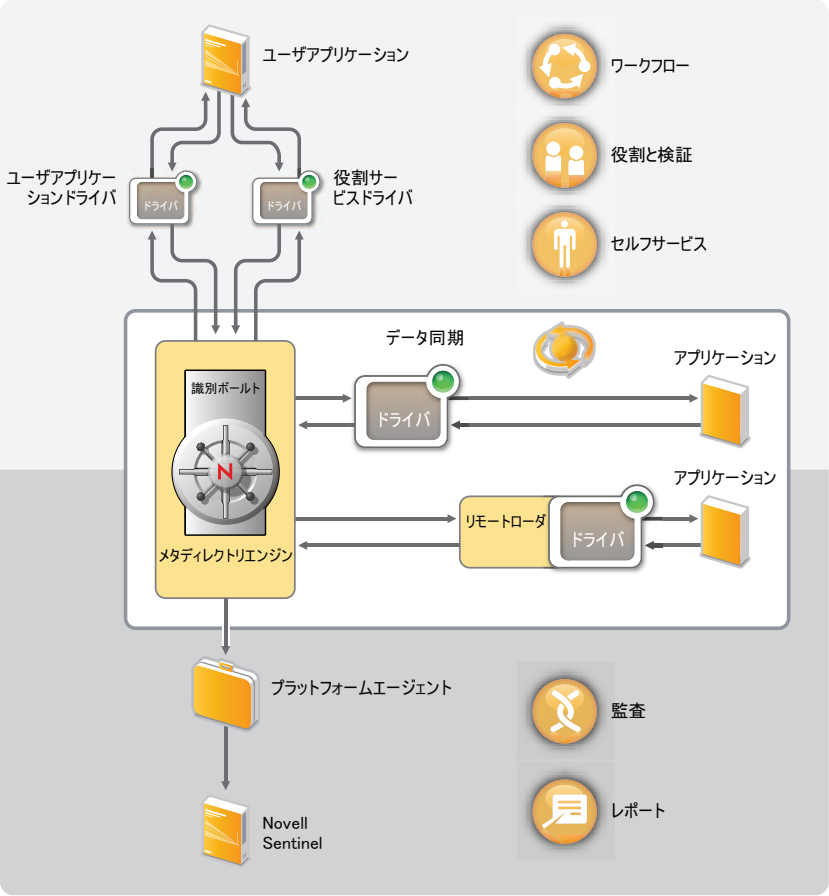
- 特定の期間にわたるすべての承認ワークフロー。各ワークフロー用に記録された操作 (開始、転送、拒否、承認など) があります。
- 特定の期間にわたるプロビジョニングされたワークフロー。各リソース用に記録された操作 (送信、権限の付与、取り消し、成功など) があります。
- 特定の期間にわたる 1 名のユーザに関するすべてのワークフローのステータス、パスワードの変更、および管理についての変更。
- 特定の期間にわたる 1 名のユーザに関するすべてのリソースプロビジョニング。
- 特定の期間にわたるすべてのユーザに関するすべてのリソースプロビジョニング。

Novell Sentinel は、Identity Manager とは個別に販売されています。

Identity Manager アーキテクチャ 2

次の図は、データ同期、ワークフロー、役割、検証、セルフサービス、監査 / レポートなど、9 ページの第 1 章「Identity Manager および ビジネスプロセスの自動化」で紹介されている Novell® Identity Manager の機能を提供する高レベルなアーキテクチャコンポーネントを示しています。

図 2-1 *Identity Manager の高レベルのアーキテクチャ*



各コンポーネントは次のセクションで紹介されています。

- 20 ページのセクション 2.1「データ同期」
- 24 ページのセクション 2.2「ワークフロー、役割、検証、およびセルフサービス」
- 26 ページのセクション 2.3「監査とレポート」

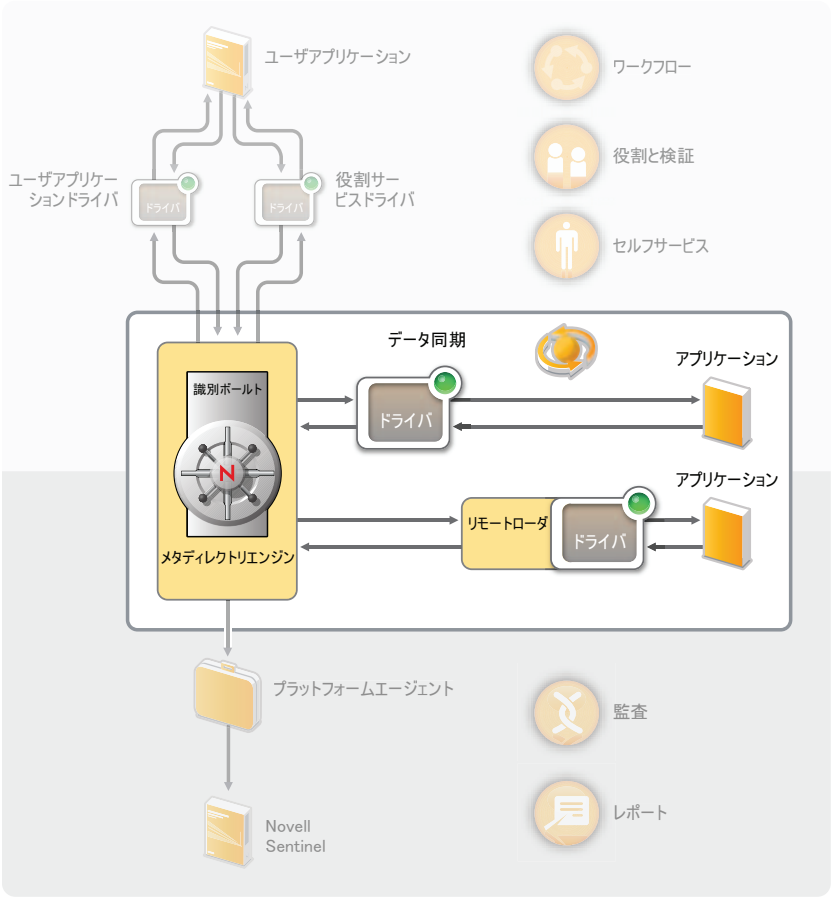
2.1 データ同期

データ同期によって、ビジネスプロセスの自動化のための基礎が提供されます。最も簡単な形式で、データ同期では、データ項目を変更する場所からそのデータ項目を必要とする別の場所にデータを移動します。たとえば、従業員の電話番号が会社の人材システムで変更される場合、その変更は理想的に、従業員の電話番号を格納している他のすべてのシステムで自動的に表示されます。

Identity Manager は識別データの同期だけではありません。Identity Manager を使用すると、接続アプリケーションまたは識別ボールト内に格納されているすべての種類のデータを同期できます。

パスワードの同期を含むデータ同期は、Identity Manager ソリューションの 5 つの基本的なコンポーネント、識別ボールト、メタディレクトリエンジン、ドライバ、リモートローダ、および接続アプリケーションによって実現しています。これらのコンポーネントは次の図に示します。

図 2-2 *Identity Manager アーキテクチャコンポーネント*



次のセクションでは、これらの各コンポーネント、および組織のシステム間でデータを効率的に同期するために理解する必要のある概念について説明します。

- 21 ページのセクション 2.1.1「コンポーネント」
- 21 ページのセクション 2.1.2「主な提案」

2.1.1 コンポーネント

識別ボールト : 識別ボールトは、アプリケーション間で同期するデータのメタディレクトリの役割を果たしています。たとえば、PeopleSoft システムから Lotus Notes に同期されたデータが最初に識別ボールトに追加され、Lotus Notes システムに送信されます。さらに、識別ボールトには、ドライバ構成、パラメータ、およびポリシーなどの Identity Manager に固有の情報が格納されます。Novell eDirectory™ は識別ボールトに使用されます。

メタディレクトリエンジン : 識別ボールトまたは接続アプリケーション内でデータが変更されると、メタディレクトリエンジンによってその変更が処理されます。識別ボールトで発生するイベントでは、エンジンによって変更が処理され、ドライバを通じてアプリケーションにコマンドが発行されます。アプリケーションで発生するイベントでは、エンジンによってドライバからの変更が受信され、その変更が処理され、識別ボールトにコマンドが発行されます。メタディレクトリエンジンは *Identity Manager エンジン*と呼ばれることもあります。

ドライバ : ドライバは、識別情報を管理するアプリケーションに接続します。ドライバには次の 2 つの役割があります。1) アプリケーション内のデータ変更 (イベント) をメタディレクトリエンジンにレポートする。2) メタディレクトリエンジンによって送信されたデータ変更 (コマンド) をアプリケーションに対して実行する。

リモートローダ : ドライバをインストールして、接続しているアプリケーションと同じサーバで実行する必要があります。アプリケーションがメタディレクトリエンジンと同じサーバにある場合、必要なのは、そのサーバにドライバをインストールすることだけです。ただし、アプリケーションがメタディレクトリエンジンと同じサーバにない場合 (つまり、ローカルではなく、エンジンのサーバに対してリモートである場合)、ドライバおよびリモートローダをアプリケーションサーバにインストールする必要があります。リモートローダはドライバをロードし、ドライバの代わりにメタディレクトリエンジンと通信します。

アプリケーション : ドライバの接続先のシステム、ディレクトリ、データベース、またはオペレーティングシステム。アプリケーションはドライバが使用できる API を提供することによって、アプリケーションデータの変更を特定し、アプリケーションデータの変更を行う必要があります。アプリケーションは*接続システム*と呼ばれることもあります。

2.1.2 主な提案

チャネル : 2 つの別の *チャンネル*を伝わる識別ボールトと接続システムの間のデータフロー。*購読者チャンネル*によって、識別ボールトから接続システムへのデータフローが実現します。つまり、接続システムが識別ボールトからデータを購読します。*発行者チャンネル*によって、接続システムから識別ボールトへのデータフローが実現します。つまり、接続システムが識別ボールトにデータを発行します。

データ表示 : *XML ドキュメント*でチャンネルを通過するデータフロー。XML ドキュメントは、識別ボールトまたは接続システムで変更が行われると、作成されます。XML ドキュメントは、ドライバのチャンネルに関連付けられているフィルタおよびポリシーのセットを通ってドキュメントを転送するメタディレクトリエンジンを通過します。すべての処理が XML ドキュメントに適用されている場合、メタディレクトリエンジンがドキュメントを使用して識別ボールトに対して適切な変更を開始するか (発行者チャンネル)、ドライバがドキュメントを使用して接続システムで適切な変更を開始します (購読者チャンネル)。

データ操作 : XML ドキュメントがドライバチャンネルを通過するので、ドキュメントのデータはチャンネルに関連付けられている*ポリシー*の影響を受けます。

ポリシーは、データ形式の変更、識別ボールトと接続システムとの間での属性マッピング、データフローの条件付きブロック、電子メール通知の生成、データの種類の変更など、多くの場合に使用します。

データフロー制御 : *フィルタ*、すなわち*フィルタポリシー*はデータフローを制御します。フィルタは、識別ボールトと接続システムとの間で同期するデータ項目を指定します。たとえば、ユーザデータは一般的にシステム間で同期されます。したがって、ユーザデータは大部分の接続システムのフィルタにリストされています。ただし、プリンタは通常、大部分のアプリケーションにとって興味の対象ではないので、プリンタデータは大部分の接続システムのフィルタには表示されません。

識別ボールトと接続システムの間にはすべて 2 つのフィルタがあります。識別ボールトから接続システムへのデータフローを制御する購読者チャンネルのフィルタと、接続システムから識別ボールトへのデータフローを制御する発行者チャンネルのフィルタです。

信頼されたソース : 識別に関連付けられている大部分のデータ項目には、概念上の所有者がいます。データ項目の所有者はその項目の*信頼されたソース*とみなされます。通常、データ項目の信頼されたソースのみが、データ項目を変更することができます。

たとえば、会社の電子メールシステムは通常、従業員の電子メールアドレスの信頼されたソースとみなされます。会社のホワイトページディレクトリの管理者がそのシステムで従業員の電子メールアドレスを変更する場合、電子メールシステムに対する変更を有効にする必要があるので、その変更は、従業員が実際に電子メールを受信するかどうかには影響を与えません。

Identity Manager では、項目の信頼されたソースを指定するフィルタを使用します。たとえば、PBX システムと識別ボールトの間のフィルタが従業員の電話番号を PBX システムから識別ボールトに転送するだけでなく、識別ボールトから PBX システムにも転送する場合、PBX システムは電話番号の信頼されたソースです。他のすべての接続システムの関係により、識別ボールトから PBX システムだけでなく、PBX システムから識別ボールトに電話番号を転送できる場合、最終的な効果は、PBX システムが企業内の従業員の電話番号の信頼されたソースのみであることです。

自動プロビジョニング : 自動プロビジョニングは Identity Manager の機能を参照し、単純なデータ項目の同期ではなく、ユーザのプロビジョニングアクションを生成します。

たとえば、人材データベースが大部分の従業員データの信頼されたソースである通常の Identity Manager システムでは、HR データベースに従業員を追加すると、識別ボールト内の対応するアカウントの自動作成がトリガされます。識別ボールトアカウントが自動作成されると、その次に、電子メールシステムで従業員の電子メールアカウントの自動作成がトリガされます。電子メールシステムのアカウントのプロビジョニングに使用するデータは、識別ボールトから取得されます。このデータには、従業員名、場所、電話番号などが含まれている場合があります。

アカウント、アクセス、およびデータの自動プロビジョニングは、次のさまざまな方法で制御することができます。

- *データ項目値*: たとえば、さまざまな構成要素のためのアクセスデータベース内のアカウントの自動作成は、従業者の場所の属性における値によって制御できます。

- *承認ワークフロー*: たとえば、財務部門の従業員を作成すると、財務システムでの新しい従業員のアカウントの承認を要求する財務部長に対する自動電子メールをトリガすることができます。財務部長は、部長が要求を承認または拒否する Web ページに対する電子メールの指示を受けます。次に、承認によって、財務システムの従業員に対してアカウントの自動作成がトリガされます。
- *役割の割り当て*: 従業員にはアカウンタントの役割が与えられます。Identity Manager では、システムワークフロー (人が介入しない)、人による承認フロー、またはその両方を組み合わせることによって、すべてのアカウント、アクセス、およびアカウンタントの役割に割り当てられるデータを持つ従業員をプロビジョニングします。

エンタイトルメント : エンタイトルメントには、アカウントやグループメンバーシップなどの、接続システムのリソースが表示されます。接続システム内のエンタイトルメント用に確立された基準にユーザが適合する場合、Identity Manager は、リソースへのアクセス権が付与されているユーザになるユーザのイベントを処理します。もちろん、リソースに対するアクセスを有効にするため、すべてのポリシーが所定の位置にある必要があります。たとえば、ユーザが Active Directory の Exchange アカウント用の基準に適合する場合、メタディレクトリエンジンは、Exchange アカウントを提供する Active Directory ドライバポリシーのセットを介してユーザを処理します。

エンタイトルメントの主な利点は、複数のドラバポリシーではなく、1 つのエンタイトルメントでリソースへのアクセスに対してビジネスロジックを定義できることです。たとえば、4 つの接続システムでユーザにアカウントを付与するアカウントエンタイトルメントを定義できます。ユーザにアカウントを付与するかどうかは、エンタイトルメントによって決定されます。これは、4 つのドライバのそれぞれのポリシーにビジネスロジックを含める必要がないことを意味しています。代わりに、ポリシーがアカウントを付与するためのメカニズムを提供する必要があります。ビジネスロジックを変更する必要がある場合、各ドライバではなく、エンタイトルメントで変更します。

ジョブ : ほとんどの場合、Identity Manager はデータ変更またはユーザ要求に応じて動作します。たとえば、1 つのシステムで一部のデータが変更されると、Identity Manager は別のシステム内の対応するデータを変更します。または、ユーザがシステムへのアクセスを要求すると、Identity Manager は適切なプロセス (ワークフロー、リソースプロビジョニングなど) を開始し、アクセスを提供します。

ジョブを使用すると、データ変更またはユーザ要求では開始されないアクションを Identity Manager が実行できるようになります。ジョブは、識別ボールトおよび対応する一部の実装コードに格納されている設定データで構成されています。Identity Manager には、ドライバの開始または停止、期限切れが近づいているパスワードに関する電子メール通知の送信、およびドライバのヘルスステータスの確認などのアクションを実行する事前定義されたジョブが含まれています。また、カスタムジョブを実装して、目的のアクションの実行に必要なコードを作成することを要求するカスタムジョブなど、他のアクションを実行することもできます。

ワークオーダー : 通常、識別ボールトまたは接続アプリケーション内のデータ変更は、瞬時に処理されます。ワークオーダーを使用すると、特定の日時で実行するタスクをスケジュールすることができます。たとえば、新しい従業員を雇いましたが、ある月で開始するようにスケジュールされていないとします。その従業員を HR データベースに追加する必要がありますが、開始日までは会社のリソース (電子メール、サーバなど) に対するアクセス権を付与してはいけません。ワークオーダーを使用しない場合、ユーザにはすぐにアクセス権が付与されます。ワークオーダーが実装されていると、開始日のみにアカウントのプロビジョニングが開始されるワークオーダーが作成されます。

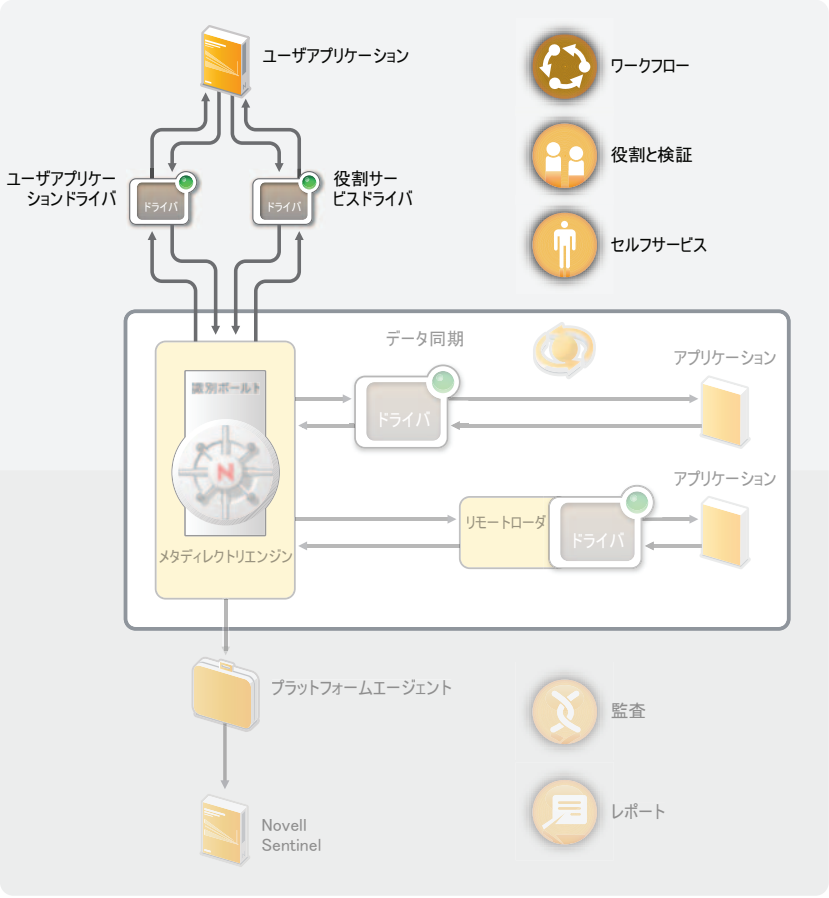
2.2 ワークフロー、役割、検証、およびセルフサービス

Identity Manager には、専用のアプリケーションであるユーザアプリケーションがあり、承認ワークフロー、役割の割り当て、検証、および識別セルフサービスが提供されています。

標準ユーザアプリケーションは Identity Manager に付属しています。標準バージョンには、ユーザが忘れたパスワードを思い出したり、リセットしたりするのに使用するパスワードセルフサービス、ユーザのディレクトリ情報を管理する組織チャート、および識別ボールトでのユーザ作成を可能にするユーザ管理機能があります。

ユーザアプリケーションの役割ベースのプロビジョニングモジュールは、Identity Manager のアドオンとして別売されています。役割ベースのプロビジョニングモジュールを追加すると、標準ユーザアプリケーションの機能は、高度なセルフサービス、承認ワークフロー、役割ベースのプロビジョニング、義務の分離の制約、および検証を含むように拡張されます。

図 2-3 *Identity Manager ユーザアプリケーション*



次のセクションでは、これらの各コンポーネントについて説明し、コンポーネントを効率的に実装および管理するために理解する必要のあるコンセプトについても説明します。

- 25 ページのセクション 2.2.1「コンポーネント」
- 25 ページのセクション 2.2.2「主なコンセプト」

2.2.1 コンポーネント

ユーザアプリケーション : ユーザアプリケーションはブラウザベースの Web アプリケーションで、ユーザおよびビジネス管理者に、さまざまな識別セルフサービスおよび役割のプロビジョニングのタスクを実行する機能を提供しています。このタスクには、パスワードおよび識別データの管理、プロビジョニングおよび役割の割り当て要求の開始および監視、プロビジョニング要求の承認プロセスの管理、検証レポートの確認などがあります。これには、アプリケーションの承認プロセスを通じて要求のルーティングを制御するワークフローエンジンがあります。

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は、設定情報が格納しており、識別ボールトで変更が行われたかどうかをユーザアプリケーションに通知します。また、識別ボールト内のイベントがワークフローをトリガして、ユーザアプリケーションに対するワークフローのプロビジョニングアクティブティの成功または失敗をレポートし、ユーザが要求の最終ステータスを表示できるように設定することもできます。

役割サービスドライバ : 役割サービスドライバは、すべての役割の割り当てを管理し、承認を必要とする役割の割り当て要求のワークフローを開始し、グループまたはコンテナメンバシップに従って間接的な役割の割り当てを維持します。このドライバは、役割のメンバーシップに基づいてユーザのエンタイトルメントを付与および取消し、完了した要求のクリーンアップ手順を実行します。

2.2.2 主なコンセプト

ワークフローベースのプロビジョニング ワークフローベースのプロビジョニングは、ユーザがリソースに対するアクセス権を要求する方法を提供しています。プレゼンテーション要求は、1 名以上のユーザからの承認を含んでいる可能性のある、事前定義されたワークフローによってルーティングされます。すべての承認が付与されると、ユーザがリソースに対するアクセス権を受信します。また、識別ボールトで発生するイベントに応じてプロビジョニング要求を間接的に開始することもできます。たとえば、ユーザをグループに追加すると、特定のリソースに対するアクセス権をユーザに付与する要求が開始されることがあります。

役割ベースのプロビジョニング 役割ベースのプロビジョニングは、割り当てられる役割に基づいてユーザが特定のリソースに対するアクセス権を受信する方法を提供しています。ユーザには 1 つ以上の役割を割り当てることができます。役割の割り当てに承認が必要な場合、割り当て要求によってワークフローが開始されます。

義務の分離 : 競合する役割にユーザが割り当てられないように、ユーザアプリケーションの役割ベースのプロビジョニングモジュールには義務の分離機能が用意されています。競合すると考えられる役割を定義する義務の分離*制約*を確立できます。役割が競合する場合、義務の分離*承認者*が制約に対するすべての*例外*を承認または拒否できます。承認された例外は、美無の分離*違反*として記録されるので、以下に示す承認プロセスによってレビューすることができます。

役割の管理 : *Roles Module Administrator* および *Roles Manager* のシステムの役割に割り当てられているユーザが、役割を管理する必要があります。

Roles Module Administrator は、新しい役割の作成、既存の役割の変更、役割の削除、役割間の関係の変更、ユーザに対する役割の割り当ての許可および取り消し、義務の分離制約の作成、変更、および削除を行います。

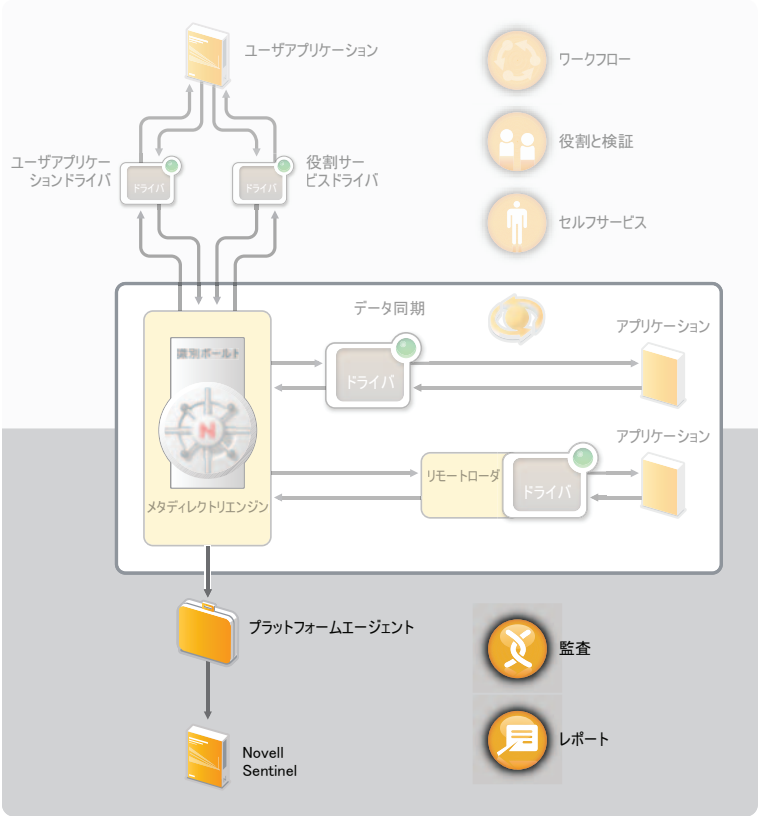
Roles Manager は、義務の分離制約の管理、役割システムの設定、およびすべてのレポートの実行に関する例外を持つ Roles Module Administrator と同じことができます。また、Roles Module Administrator には役割システム内に限定されたスコープがありますが、Roles Manager のスコープは特別設計のユーザ、グループ、および役割に限定されています。

検証 : 役割の割り当てによって、組織内のリソースに対するユーザのアクセスが決定されるので、不正確な割り当てによって会社と政府の両方の規制に準拠することが妨げられることがあります。Identity Manager は、検証プロセスによる役割の割り当ての正確さの検証に使用できます。このプロセスを使用して、各ユーザは各自のプロファイル情報を検証し、Roles Manager は役割の割り当ておよび義務の分離違反を検証することができます。

2.3 監査とレポート

監査とレポートは、以下の図に示されているように Novell Sentinel™ との統合によって提供されています。

図 2-4 *Identity Manager の監査とレポート*



プラットフォームエージェント：プラットフォームエージェントでは、メタディレクトリエンジンからのイベントを取得し、これらのイベントを Novell Sentinel システムに送信します。

Novell Sentinel: Novell Sentinel は、セキュリティ情報およびイベント管理 (SIEM) ソリューションで、システムネットワーク、アプリケーション、およびセキュリティログのコレクション、分析、およびレポートを自動化します。Novell Sentinel は別売されています。

製品の購入方法など、Novell Sentinel の詳細な紹介については、Novell Sentinel サイト (http://www.novell.com/products/sentinel/) を参照してください。

Identity Manager ツール

3

Identity Manager には、Identity Manager システムのセットアップおよび維持に役立つ 3 つの主要なツール、Designer、iManager、およびユーザアプリケーション管理コンソールがあります。

Designer を使用して、Identity Manager システムをオフライン環境で作成および設定し、ライブシステムに変更を展開します。iManager を使用して、Designer と同じタスクを実行したり、システムのヘルスを監視したりすることができます。ただし、iManager での変更は、すぐに展開されるので、単純な管理には iManager を使用し、展開前にモデリングおよびテストを必要とする複雑な設定タスクには Designer を使用することをお勧めします。

ユーザアプリケーション管理コンソールを使用して、ページおよびポートレットを作成および変更し、アプリケーションの外観を管理します。また、キャッシュやログ設定などのアプリケーション設定を変更し、ユーザアプリケーションのプロビジョニング機能に固有の委任およびプロキシ設定を構成することができます。

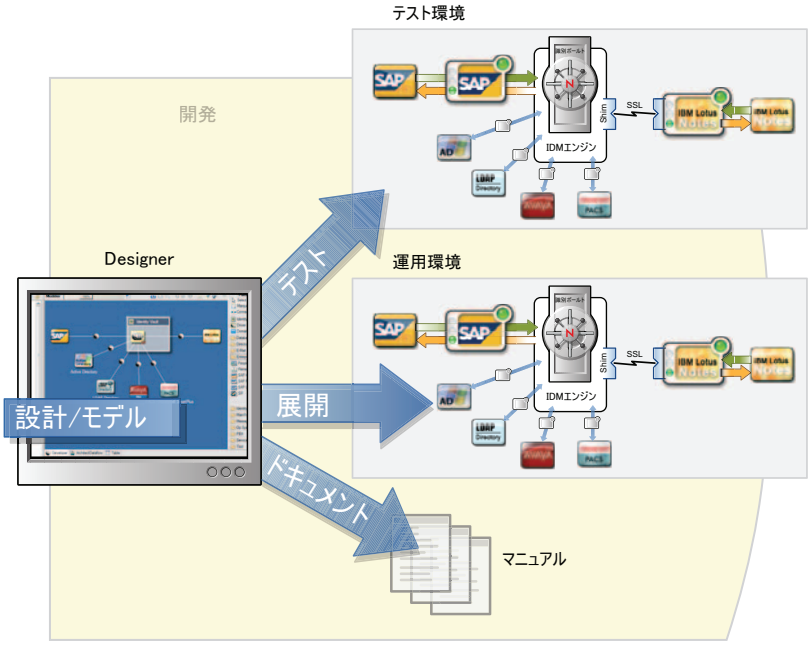
これらの各ツールの詳細情報については、次のセクションを参照してください。

- 29 ページのセクション 3.1「Designer」
- 30 ページのセクション 3.2「iManager」
- 31 ページのセクション 3.3「ユーザアプリケーション管理コンソール」

3.1 Designer

Designer は Eclipse* ベースのツールで、Identity Manager システムの設計、展開、および文書化に使用します。Designer のグラフィカルインタフェースを使用すると、オフライン環境でシステムを設計およびテストしたり、システムを運用環境に展開したり、展開システムの詳細をすべて文書化したりすることができます。

図 3-1 Designer for Identity Manager



Designer を使用しないで Identity Manager システムをセットアップすることは可能ですが、難しいのでお勧めしません。

設計 : Designer には、システムをモデリングできるグラフィカルインタフェースがあります。これには、ユーザが Identity Manager とアプリケーションとの間の接続を作成および制御したり、ポリシーを設定したり、接続アプリケーション間のデータフローを操作したりすることができるビューがあります。

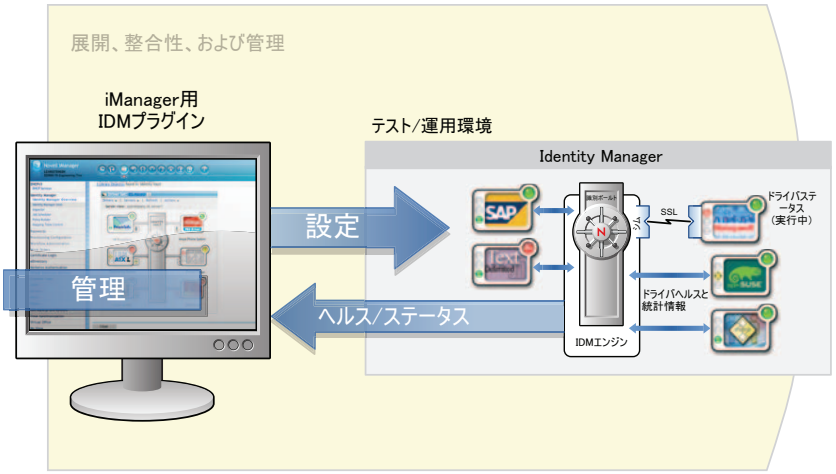
展開 : Designer での操作は、展開の開始時に運用環境に展開されます。これにより、運用環境でライブにする前に、ユーザが実験、結果のテスト、および問題の解決を行えます。

文書化 : システム階層、ドライバ設定、ポリシー設定などを示す詳細なドキュメントを生成することができます。基本的に、システムの技術的な側面を理解するにはすべての情報が必要ですが、ビジネスルールおよびポリシーの遵守の確認に役立ちます。

3.2 iManager

Novell® iManager はブラウザベースのツールで、Identity Manager などの数多くの Novell 製品を単一点で管理できます。iManager 用の Identity Manager プラグインを使用すると、Identity Manager を管理できるだけでなく、Identity Manager システムに関するリアルタイムのヘルスおよびステータス情報を受信できます。

図 3-2 Novell iManager



3.3 ユーザアプリケーション管理コンソール

ユーザアプリケーションは Web ベースの管理コンソールで、ユーザがパスワードセルフサービス、役割、およびプロビジョニングを設定、管理、およびカスタマイズできます。管理コンソールは、管理権限を付与したユーザに対して、ユーザアプリケーションの *管理* タブとして追加されます。

図 3-3 ユーザアプリケーション管理ページ

ユーザアプリケーション管理ページには次のタブがあります。

- **アプリケーション環境設定 :** キャッシュ、LDAP パラメータ、ログ記録、テーマ、およびパスワードモジュールセットアップを設定できます。
- **ページ管理 :** 新しいページを作成したり、既存の識別セルフサービスページをカスタマイズしたりすることができます。
- **ポートレット管理 :** 識別セルフサービスページで使用する新しいポートレットを作成したり、既存のポートレットをカスタマイズしたりすることができます。

- **プロビジョニング :** 委任、プロキシ、タスク、デジタル署名サービス、およびエンジンとクラスタ設定を構成できます。
- **セキュリティ :** プロビジョニング管理者およびユーザアプリケーション管理者権限を持つユーザを定義できます。