概要ガイド

Novell® Identity Manager

4.0.1

2011 年 04 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、米国の輸出管理規定およびその他の国の輸出関連法規の制限を受けます。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。

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 マニュアルの 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

このガイドでは、WorkloadIQ 製品の 1 つである Novell Identity Manager について紹介します。この製品は、物理、仮想、およびクラウド環境にわたって識別情報とアクセスを管理します。このガイドでは、コストを削減し、規制を確実に遵守しつつお客様がビジネス上の問題を解決するのに、Identity Manager がどのように役立つかについて説明します。また、Identity Manager ソリューションを作成するのに使用できる Identity Manager のコンポーネントおよびツールに関する技術的な概要も含まれています。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/idm401/index.html) を参照してください。

追加のマニュアル

Identity Manager のドライバに関するマニュアルについては、Identity Manager ドライバの Web サイト (http://www.novell.com/documentation/idm401drivers/index.html) を参照してください。

Identity Manager およびビジネスプロセスの自動化

1

この項に含まれる情報は、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特定します。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、27 ページの第 4 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。これらの機能 (ワークフロー、役割、検証、セルフサービス、監査、およびレポーティング) は、ビジネスポリシーが主導するマルチシステムのデータ同期を使用してユーザのプロビジョニングやパスワードの管理という、IT 組織において最も困難かつ時間のかかる 2 つの職務に関わるプロセスを自動化させます。

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。

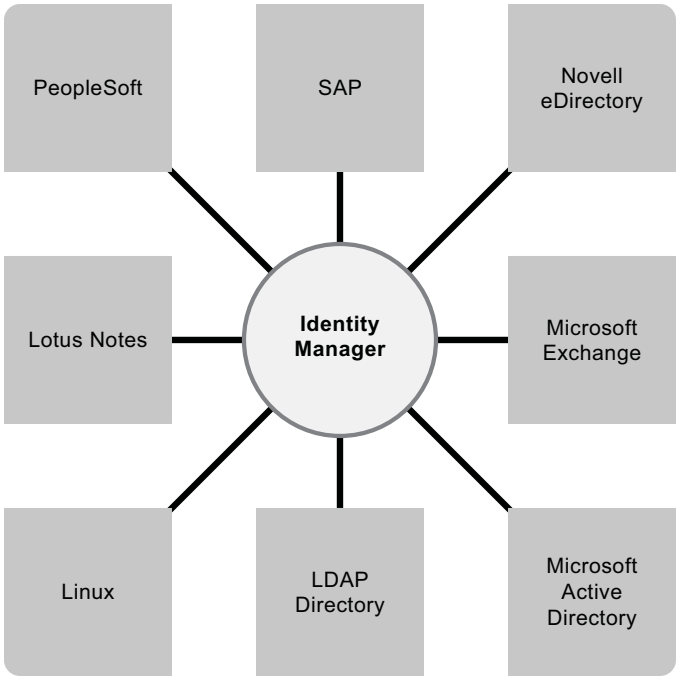
- 8 ページのセクション 1.1「データ同期」
- 11 ページのセクション 1.2「ワークフロー」
- 12 ページのセクション 1.3「役割および検証」
- 13 ページのセクション 1.4「セルフサービス」
- 14 ページのセクション 1.5「監査、レポーティング、および規制の遵守」

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、Salesforce、Microsoft SharePoint、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。

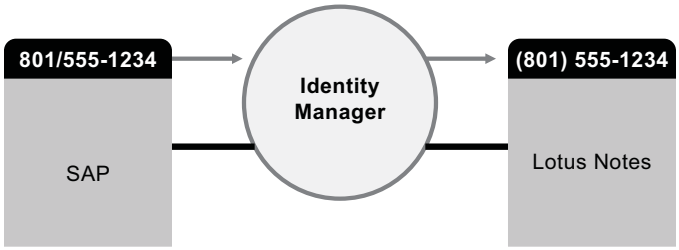
図 1-2 *複数のシステムを接続する Identity Manager*



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。

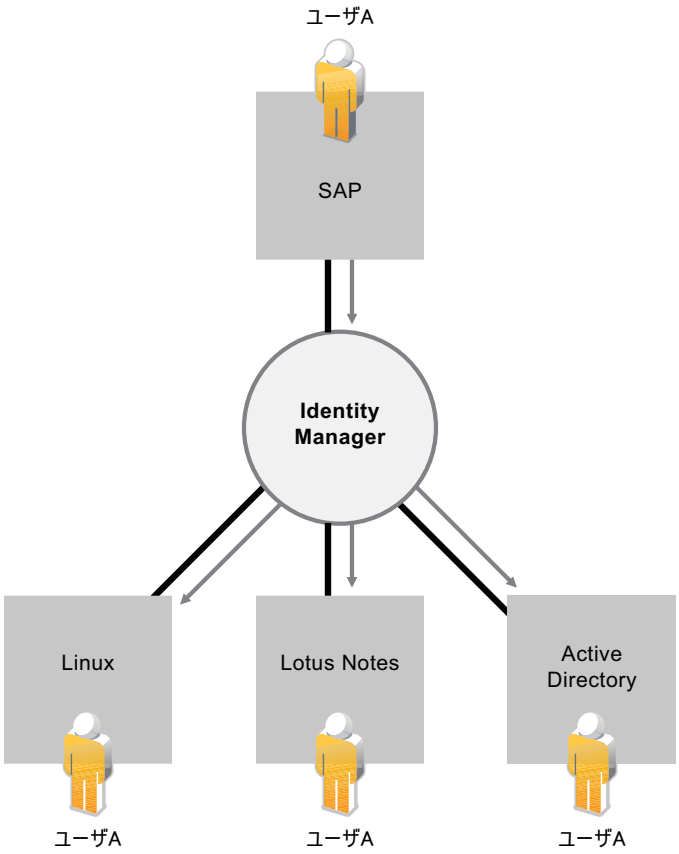
次の図では、ユーザの電話番号に関して権限のあるソースは SAP HR データベースです。Lotus Notes システムでは電話番号を使用するので、Identity Manager で番号を必要な形式に変換し、Lotus Notes システムと共有します。電話番号は SAP HR システムで変更されるたびに、Lotus Notes システムに同期されます。

図 1-3 *接続システム間で同期されるデータ*



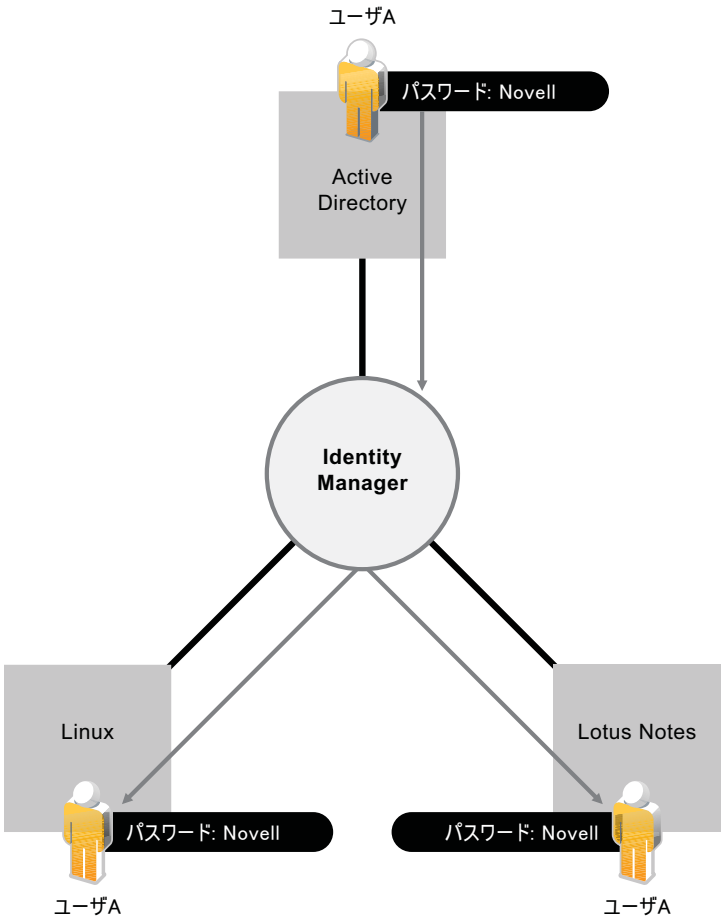
既存のユーザのデータを管理することは、Identity Manager のデータ同期機能の始まりにすぎません。さらに、Identity Manager では、Active Directory などのディレクトリ、PeopleSoft や Lotus Notes などのシステム、および UNIX や Linux などのオペレーティングシステムで、ユーザアカウントを新規作成したり、既存のアカウントを削除したりすることもできます。たとえば、新しい従業員を SAP HR システムに追加する場合、Identity Manager システムでは、Active Directory 内に新しいユーザアカウント、Lotus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

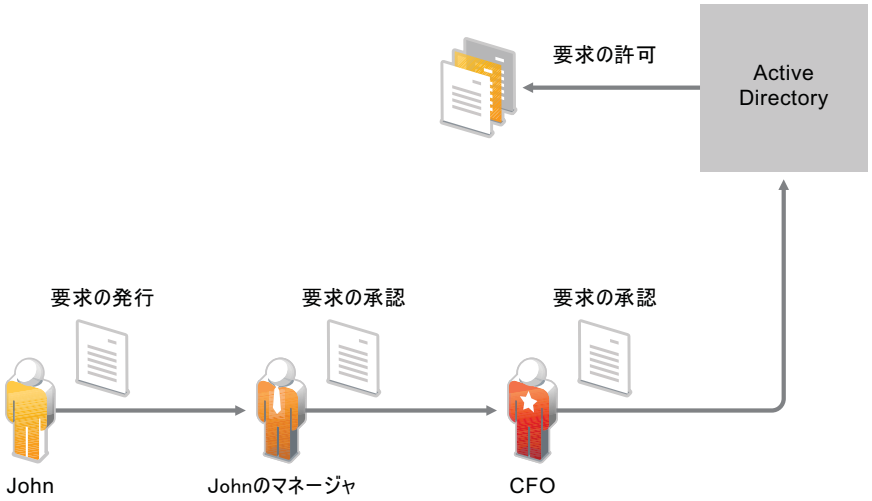


1.2 ワークフロー

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



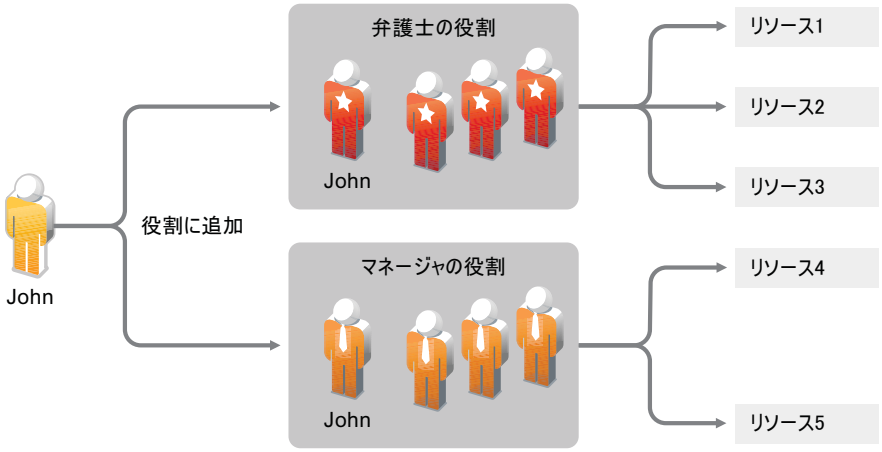
特定のイベントが発生するか (新規ユーザが HR システムに追加される場合など)、ユーザの要求によって手動で開始されるたびにワークフローを自動的に開始することができます。承認がタイミングよく行われるように、プロキシ承認者および承認チームをセットアップすることができます。

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を要求することがよくあります。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 役割ベースのリソースのプロビジョニング



組織内で発生する出来事の結果、ユーザを自動的に役割に追加することができます (たとえば、弁護士という役職名を持つ新規ユーザは、SAP HR データベースに追加されます)。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特定の役割があります。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。」

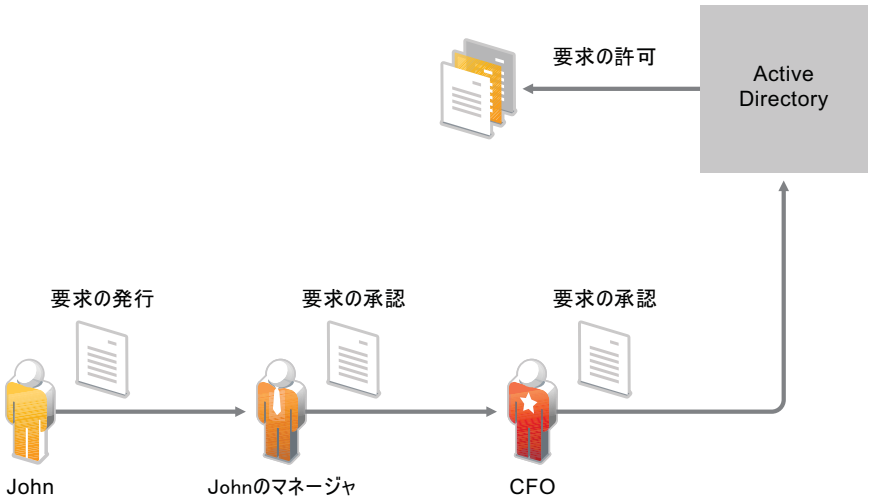
Identity Manager では、責任を負う必要のあるユーザに管理業務を委任できます。たとえば、各ユーザが、

- 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、11 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、レポーティング、および規制の遵守

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、過去または現在を問わずユーザのプロビジョニングアクティビティが監査のためにすべて追跡され、ログが記録されることが分かっているので、作業が楽になります。Identity Manager には、お客様の組織内部の識別ボールトと管理対象システムの現状と望ましい状態に関する情報のインテリジェントリポジトリが含まれています。ウェアハウスに問い合わせることで、お客様の組織に関連するビジネスの法律および規則を完全に遵守するのに必要なあらゆる情報を取得できます。

ウェアハウスでは、お客様のビジネスエンタイトルメントに関する 360° のビューが提供され、組織内で識別情報に対して付与された権限や許可の過去および現在の状況を確認するのに必要な知識が得られます。この知識をもとに、最も高度な GRC (Governance Risk and Compliance) に関する問い合わせであっても答えることができます。

Identity Manager には事前定義されたレポートが含まれています。このレポートを使用すると、識別情報ウェアハウスに対して問い合わせを実行し、ビジネス、IT、および会社の方針を遵守していることを明らかにできます。事前定義されたレポートがニーズを満たさない場合は、カスタムレポートを作成することもできます。

Identity Manager 4.0.1 の機能

2

Novell Identity Manger 4.0.1 は、コストを削減し、物理、仮想、およびクラウド環境にわたってコンプライアンスを確実に実行することで、お客様の既存の IT 資産と SaaS (Software As a Service) などの新しいコンピューティングモデルを活用するインテリジェントな識別情報フレームワークを提供します。Novell Identity Manager ソリューションによって、お客様のビジネスにおいて最新の識別情報が確実に使用されるようになります。お客様は、ファイアウォール内部およびクラウドへと拡張された環境で識別情報を管理、プロビジョニング、プロビジョニング解除することで、企業レベルでの管理を維持できます。Identity Manager は、コンプライアンス管理をクラウドまで拡張するのにも役立ちます。

Identity Manager 4.0.1 は、Identity Manager ドライバポリシーを事前設定したり、カスタマイズしたりするための統合された識別情報管理、役割管理、レポーティング、およびパッケージ管理機能を提供します。さまざまなシステムドメインにわたってセキュリティポリシーを適用することもできます。Identity Manager により、ますます強化される法的な要求事項の中でもユーザライフサイクルを管理し、ファイアウォール内部またはクラウド環境においてますます深刻さを増しているセキュリティ上の問題に十分対処するために、より戦略的なユーザプロビジョニングを使用したよりきめ細やかな保護を適用できます。インテリジェント識別情報のフレームワークは、既存のインフラストラクチャを SaaS などの新しいコンピューティングモデルとともに使用するのに役立ちます。

- 17 ページのセクション 2.1「Identity Manager 4.0.1 の新機能」
- 18 ページのセクション 2.2「Identity Manager 4.0 の機能」

2.1 Identity Manager 4.0.1 の新機能

- **リソース要求アクティビティ：**リソース要求アクティビティによって、ユーザに対するリソースの付与または取り消しを自動化できます。たとえば、新しい従業員が出社初日に必要となるすべてのリソースをプロビジョニングするプロビジョニング要求定義を書いたりすることが考えられます。リソース要求アクティビティを使用すると、その従業員に対する所定のリソースの承認を自動化できます。リソース要求アクティビティの詳細については、『*User Application: Design Guide*』の「*Resource Request Activity*」を参照してください。
- **Telemetry:** Identity Manager Telemetry は、Identity Manager 4.0.1 で採用された新しいジョブです。このジョブは、使用量計算ツールまたはライセンス監視ツールとして機能します。これらのツールでは、ライセンスを追加したり、使用されていないライセンスをリタイアさせたりできるので、Identity Manager のお客様に価値をもたらします。また、お客様は、不活動ユーザ向け価格設定のメリットも活用できます。

  Telemetry のジョブは、お客様の環境にインストールされている Identity Manager ソフトウェアおよびハードウェアや Identity Manager ドライバの使用状況に関する詳細情報を収集します。お客様が Novell Customer Center に登録すると、情報が Novell に送信されます。Novell では、この情報を利用することで、お客様のサポートを向上させ、より効率的かつ効果的に Identity Manager の開発およびテストを実施し、将来において重要な意思決定が可能になります。詳細については、『*Identity Manager 4.0.1 Jobs Guide*』を参照してください。

- **レポート :** 次のレポートが Identity Reporting Module に追加されました。
  - **識別ボールト内のユーザステータスの変更 :** 識別ボールトのユーザに関する重要なイベントを表示します。
  - **識別ボールト内のユーザパスワードの変更 :** 識別ボールト内のユーザパスワードの変更をすべて表示します。
  - **受信者別のアクセス要求 :** 受信者別にグループ化されたリソース割り当てワークフロープロセスが表示されます。
  - **リクエスタ別のアクセス要求 :** リクエスタ別にグループ化されたリソース割り当てワークフロープロセスが表示されます。
  - **リソース別のアクセス要求 :** リソース別にグループ化されたリソース割り当てワークフロープロセスが表示されます。

2.2 Identity Manager 4.0 の機能

このセクションで前述した、新しく追加された機能に加えて、Identity Manager 4.0.1 は、Identity Manager 4.0 で導入された次の機能を備えています。

- **そのまま使える包括的なレポーティング :** Novell Identity Manager 4.x 製品スイートの統合レポーティングモジュールは、社内およびクラウド環境にわたって、コンプライアンスの可視性を強化します。レポーティング機能は、ユーザの識別情報の状態およびアクセス権、またはユーザのアクションおよびプロビジョニング履歴に関するレポートを表示できます。詳細については、『*Identity Reporting Module Guide*』を参照してください。
- **強化された統合 :** すべてのコンポーネントが同じサーバ上に存在するような新しい Identity Manager ソリューションを構築するために、Novell Identity Manager 4.x には、インストールプロセスを簡素化し、より迅速にシステムを設定できる統合インストーラが含まれています。Identity Manager のコンポーネントを個別にインストールする代わりに、統合インストーラを使用して 1 回の操作ですべてのコンポーネントをインストールできます。詳細については、『*Identity Manager 4.0.1 統合インストールガイド*』を参照してください。
- **パッケージ管理 :** Identity Manager 4.x にはパッケージ管理という新しい概念が導入されました。これは、Identity Manager のポリシーコンテンツの高品質な構成要素を作成、配布、および利用するためのシステムです。Identity Manager パッケージの詳細については、『*Designer 4.0.1 for Identity Manager 4.0.1 管理ガイド*』の「*Configuring Packages*」を参照してください。
- **クラウドタイプのドライバ :** Identity Manager 4.x で提供されているいくつかのドライバは、SaaS と直ちに統合できます。このドライバは、プロビジョニング、プロビジョニング解除、要求 / 承認プロセス、パスワードの変更、識別情報プロファイルの更新、およびレポーティングなどの機能を提供することで、SaaS およびホスト型ソリューションとのシームレスな統合を可能にします。新しい SharePoint および Salesforce.com ドライバにより、お客様の企業識別情報をクラウドアプリケーションアイコンと統合できます。クラウドタイプのドライバの詳細については、『*Identity Manager 4.0.1 Driver for Salesforce.com Implementation Guide*』および『*Identity Manager 4.0.1 Driver for SharePoint Implementation Guide*』を参照してください。
- **組み込まれた識別ボールト :** Novell Identity Manager 4.x 製品のアーキテクチャには、オプションの組み込み識別ボールトが含まれているので、識別情報を管理する目的で別途ディレクトリ構造を作成する必要がありません。さらに、Novell Identity Manager 4.x 製品ファミリには、識別ボールトを Active Directory またはさまざまなデータベー

スなど、企業内の識別情報の他のリポジトリと容易に統合できるようにするドライバが含まれています。詳細については、『*Identity Manager 4.0.1 統合インストールガイド*』を参照してください。

- **簡素化された識別情報および役割の管理 :** Novell Identity Manager 4.x 製品ファミリでは、異なる役割リポジトリを簡単に 1 つの場所に集めて統合できるようになりました。つまり、識別情報の別々のソースを管理する必要がなくなったのです。新しい直感的なインタフェースで役割マッピング管理者を使用することで、Novell Identity Manager 4.x にサードパーティの役割およびプロファイルを割り当てることもできます。詳細については、『*Novell Identity Manager Role Mapping Administrator 4.0.1 User Guide*』を参照してください。
- **強化されたツール :** Designer は、お客様のニーズを満たす Identity Manager ソリューションを構築するのに必要なビジネス情報および技術情報が含まれる重要なツールです。Designer 4.x ではいくつか機能が拡張されました。「*新機能* (http://www.novell.com/documentation/designer401/resources/whatsnew/index.html)」から Designer の拡張機能リストを参照してください。Designer の機能および管理については、『*Designer 4.0.1 for Identity Manager 4.0.1 Administration Guide*』を参照してください。さらに、Identity Manager には、データの分析およびクリーニングのプロセスを簡素化するためのツールが含まれています。詳細については、『*Analyzer 4.0.1 for Identity Manager Administration Guide*』を参照してください。

Identity Manager ファミリ

3

お客様のさまざまなニーズを満たすために、Identity Manager ファミリは、次の 3 つの異なる製品グループに分かれています。

- Identity Manager Advanced Edition
- Identity Manager Standard Edition
- コンプライアンス管理プラットフォーム

Identity Manager Advanced Edition には、Identity Manager Standard Edition で利用できる Identity Manager の機能に加えて追加機能が含まれています。コンプライアンス管理プラットフォームには、Identity Manager Advanced Edition と Standard Edition の機能に加えて追加機能が含まれています。

図 3-1 *Identity Manager の製品グループ*

Advanced Edition と Standard Edition で利用できる Identity Manager の機能を比較するには、「Identity Manager Version Comparison (http://www.novell.com/products/identitymanager/features/identitymanager-version-comparison.html)」を参照してください。

- 22 ページのセクション 3.1「Identity Manager Advanced Edition」
- 22 ページのセクション 3.2「Identity Manager Standard Edition」
- 24 ページのセクション 3.3「コンプライアンス管理プラットフォーム」
- 25 ページのセクション 3.4「Identity Manager Standard Edition と Advanced Edition のアクティベート」

3.1 Identity Manager Advanced Edition

The Identity Manager 4.0.1 Advanced Edition には、さまざまな機能一式が含まれており、主にエンタープライズクラスのユーザプロビジョニングを対象としています。このグループには、Standard Edition の識別セルフサービス機能だけでなく、ワークフローベースのプロビジョニングのあらゆる機能が含まれています。Advanced Edition では、ワークフロー承認プロセスを開始したり、役割とリソースをプロビジョニングしたり、コンプライアンス機能を活用したりできます。また、Advanced Edition には、Work Dashboard が含まれています。

Identity Manager 4.0.1 Advanced Edition は個別の ISO イメージとして入手可能です。

注 : Identity Manager 4.0.1 Advanced Edition では 90 日間の評価パッケージが利用できます。

3.2 Identity Manager Standard Edition

お客様のさまざまな要件を満たすために、Novell では Identity Manager 4.0.1 Standard Edition を導入いたしました。Standard Edition には、Identity Manager Advanced Edition で利用可能な機能のサブセットが含まれます。

Standard Edition では、Identity Manager の以前のバージョンに存在した次のような機能がすべてそのまま提供されます。

- 識別情報の同期
- ルールベースの自動化されたプロビジョニング
- パスワード管理とパスワードセルフサービス
- 既存のホワイトページと組織のチャート作成機能を持つ識別セルフサービス

注 : 統合モジュールは、Identity Manager Advanced Edition と Standard Edition のどちらでも変更はありません。

上記のリストに加えて、Standard Edition には、Advanced Edition が提供する次の機能が含まれています。

- ユーザインタフェースの外観
- レポーティングモジュール
- コンテンツパッケージのフレームワーク
- REST API および Single Sign-on (SSO) のサポート
- 更新用のアナライザツール

Identity Manager 4.0.1 Standard Edition は個別にダウンロードできる ISO イメージとして入手可能です。Standard Edition から Advanced Edition にアップグレードするには、Identity Manager Advanced Edition の ISO イメージを使用します。Advanced Edition にアップグレードするには、正しいアクティベーションを適用する必要があります。Standard Edition から Advanced Edition へのアップグレードに関する詳細については、『*Identity Manager 4.0.1 Upgrade and Migration Guide*』を参照してください。

Identity Manager Standard Edition の ISO イメージを使用して、既存の Identity Manager Advanced Edition から移行することはできません。Identity Manager Advanced Edition から Standard Edition に移行するには、Advanced Edition をサーバからアンインストールしてから、Standard Edition の ISO イメージを Identity Manager のメディアからインストールします。

次の機能は、Identity Manager Standard Edition では利用できません。

- 役割マッピング管理者 (RMA) は、利用できません。
- ユーザアプリケーションには次のような制限が適用されます。
  - **ビジネスユーザは［Identity Self-Service］タブのみを利用できます :** Standard Edition では、ユーザアプリケーションにビジネスユーザでログインすると、［*Identity Self-Service*］タブのみ表示されます。ユーザアプリケーション管理者でログインすると、［*Administration*］タブも表示されます。
  - **役割とリソースはサポートされていません :** 役割とリソースを使用するには、Advanced Edition が必要です。Standard Edition では、［*Roles and Resources*］タブは利用できません。
  - **［Compliance］タブがサポートされていません :**［*Compliance*］タブを利用するには Identity Manager 4.0.1 Advanced Edition が必要です。Standard Edition では、［*Compliance*］タブは利用できません。
  - **Work Dashboard は利用できません :** Standard Edition では、［*Work Dashboard*］タブは利用できません。
  - **カスタムの役割はサポートされていません :** カスタムの役割を定義する機能は利用できません。Standard Edition ではシステムの役割のみサポートしています。
  - **ワークフローはサポートされていません :** 承認ワークフローを開始する機能はサポートされていません。
  - **REST API:** 役割、リソース、ワークフローなどに関連する REST API は利用できません。
  - **セキュリティモデルが簡略化されています :** Standard Edition では、Advanced Edition に含まれる機能を何気なく使用してしまうような状況を避けるために、きめ細かいレベルでセキュリティモデルが提供されています。次の管理者の役割のみを割り当てる必要があります。
    - **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。
    - **レポート管理者 :** このユーザにはセキュリティドメイン内のすべての機能が付与されています。レポート管理者は、レポーティングドメイン内のすべてのオブジェクトで利用可能なあらゆるアクションを実行できます。
    - **セキュリティ管理者 :** この役割によって、セキュリティドメイン内のすべての機能がメンバーに付与されます。セキュリティ管理者は、セキュリティドメイン内のすべてのオブジェクトで利用可能なあらゆるアクションを実行できます。この役割は、Identity Manager Advanced Edition のすべて機能を委任したり、それに対するユーザアクセスを許可したりできます。そのため、ユーザアプリケーションの役割とレポート管理の役割からは分離されています。

注 : Standard Edition では、テストの目的の場合はセキュリティモデルがロックダウンされていません。したがって、セキュリティ管理者は、ドメイン管理者、委任された管理者、さらにはセキュリティ管理者などを割り当てることができます。ただし、これらの高度な機能の使用は、エンドユーザ使用許諾契約で規定されているように、本番環境ではサポートされません。運用環境では、すべての管理者の割り当てがライセンスによって制限されます。Novell は、本番環境が契約内容に必ず準拠するように、監査データベース内に監視データを収集できます。また、1 人のユーザのみにセキュリティ管理者としての許可を与えることを推奨します。

ユーザアプリケーションの機能の詳細については、『*Identity Manager Roles Based Provisioning Module 4.0 User Application: Administration Guide*』を参照してください。

- Identity Reporting Module には次のような制限が適用されます。
  - **管理対象システムのゲートウェイドライバが無効になっている :** 管理対象システムのゲートウェイドライバは、エンタイトルメントがサポートされる限り、Identity Manager 4.0.1 内でデータ収集が有効になっているすべての管理対象システムから情報を取得できます。

    Identity Manager Standard Edition では管理対象システムのゲートウェイドライバは無効になっています。
  - **レポートに識別ボールトのデータのみが表示される :** Identity Manager Standard Edition で生成されたレポートには識別ボールトのデータのみが表示され、管理対象 (接続) システムに関するデータは表示されません。
  - **レポートに履歴データが表示されない :** Standard Edition では、過去の状態に関するデータをレポート作成用に収集する機能が付属していません。Standard Edition を使用する場合、現在の状態に関するデータのみを確認できます。
  - **一部のレポートが利用できない :** Identity Manager 4.0 および 4.0.1 では、いくつかの新しいレポートが追加されています。Standard Edition には、接続システムおよび履歴データに当てはまるレポートは含まれていません。
  - **一部のレポートにデータが含まれていない :** 役割、リソース、およびワークフロープロセスなど、Standard Edition では利用できないデータをレポートで使用しているため、Identity Manager Advanced Edition を購入した場合のみ有意義なレポートが一部存在します。

3.3 コンプライアンス管理プラットフォーム

Novell Compliance Management Platform は、アイデンティティ、アクセス、およびセキュリティを管理するための Novell 製品を組み合わせた製品で、ソリューションの導入と管理を簡単にする実績のある一連のツールが付属しています。このプラットフォームは、アイデンティティおよびアクセスに関する情報を、セキュリティ情報およびイベント管理技術と統合し、社内全体のネットワークイベントを総合的にリアルタイム表示します。この緊密な統合によって強力なリスク管理機能が実現し、経営方針が自動化された IT プラクティスへと移行されます。詳細については、Compliance Management Platform の Web サイト (http://www.novell.com/documentation/ncmp10/) を参照してください。

3.4 Identity Manager Standard Edition と Advanced Edition のアクティベート

Identity Manager Standard Edition および Advanced Edition は、インストール後 90 日以内にアクティベートする必要があります。そうしないと、90 日後にシャットダウンします。Identity Manager Standard Edition および Advanced Edition は、90 日間はすべての機能が動作します。90 日以内のいつでも、またはその後でも、Identity Manager 製品をアクティベートするよう選択できます。詳細については、『*Identity Manager 4.0.1 Framework Installation Guide*』の「Activating Novell Identity Manager Products」を参照してください。

アクティベーションされていない既存の Advanced Edition システムに Standard Edition のアクティベーションを適用すると、Identity Manager メタディレクトリサーバとドライバが機能しなくなります。

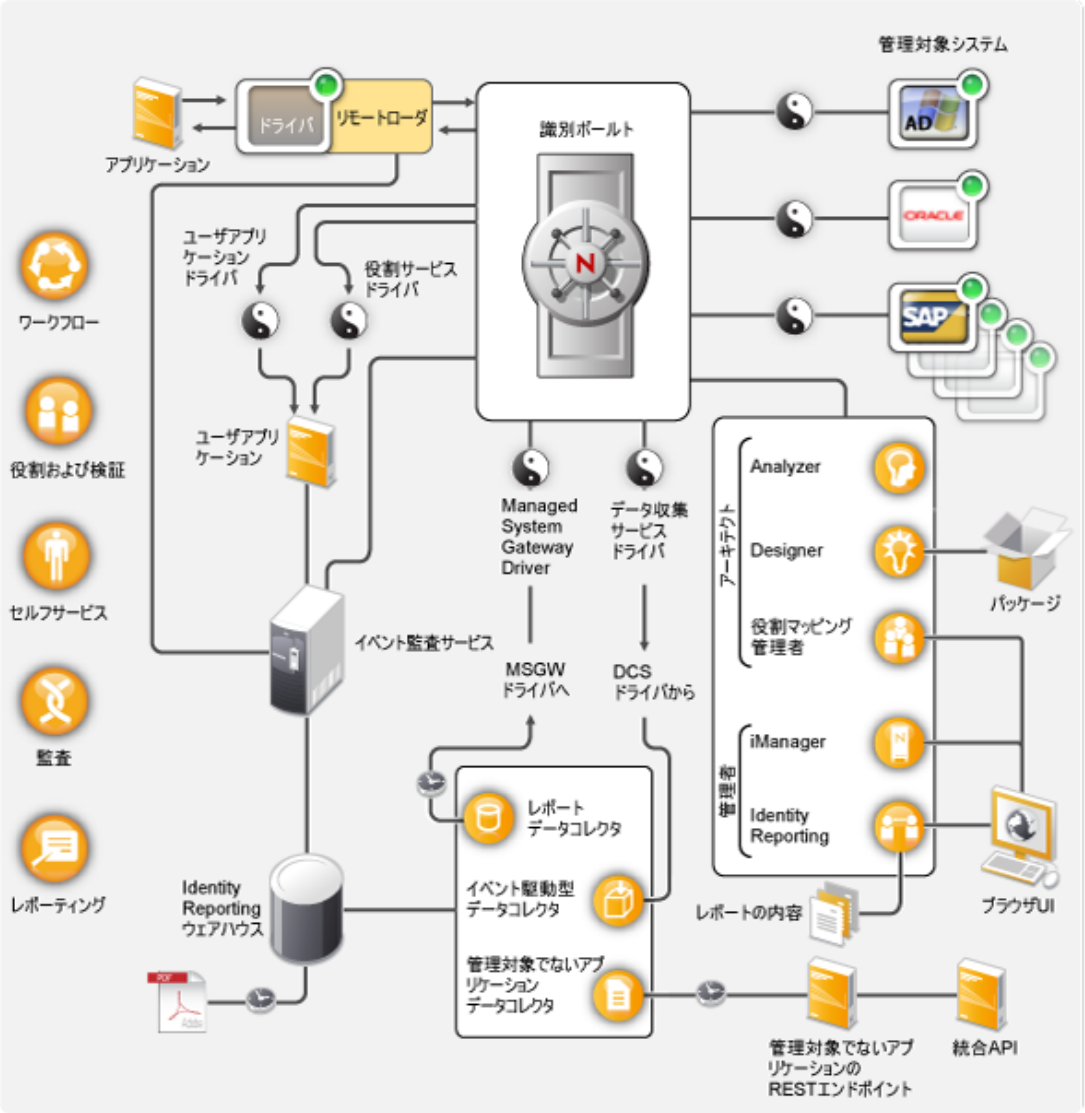
注 : Identity Manager Advanced Edition および Identity Manager Standard Edition の両方をご使用の場合は、正しいアクティベーションを正しいサーバで使用するようにしてください。

Identity Manager アーキテクチャ

4

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、7 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 4-1 *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。

- 28 ページのセクション 4.1「データ同期」
- 32 ページのセクション 4.2「ワークフロー、役割、検証、およびセルフサービス」
- 35 ページのセクション 4.3「監査とレポート」

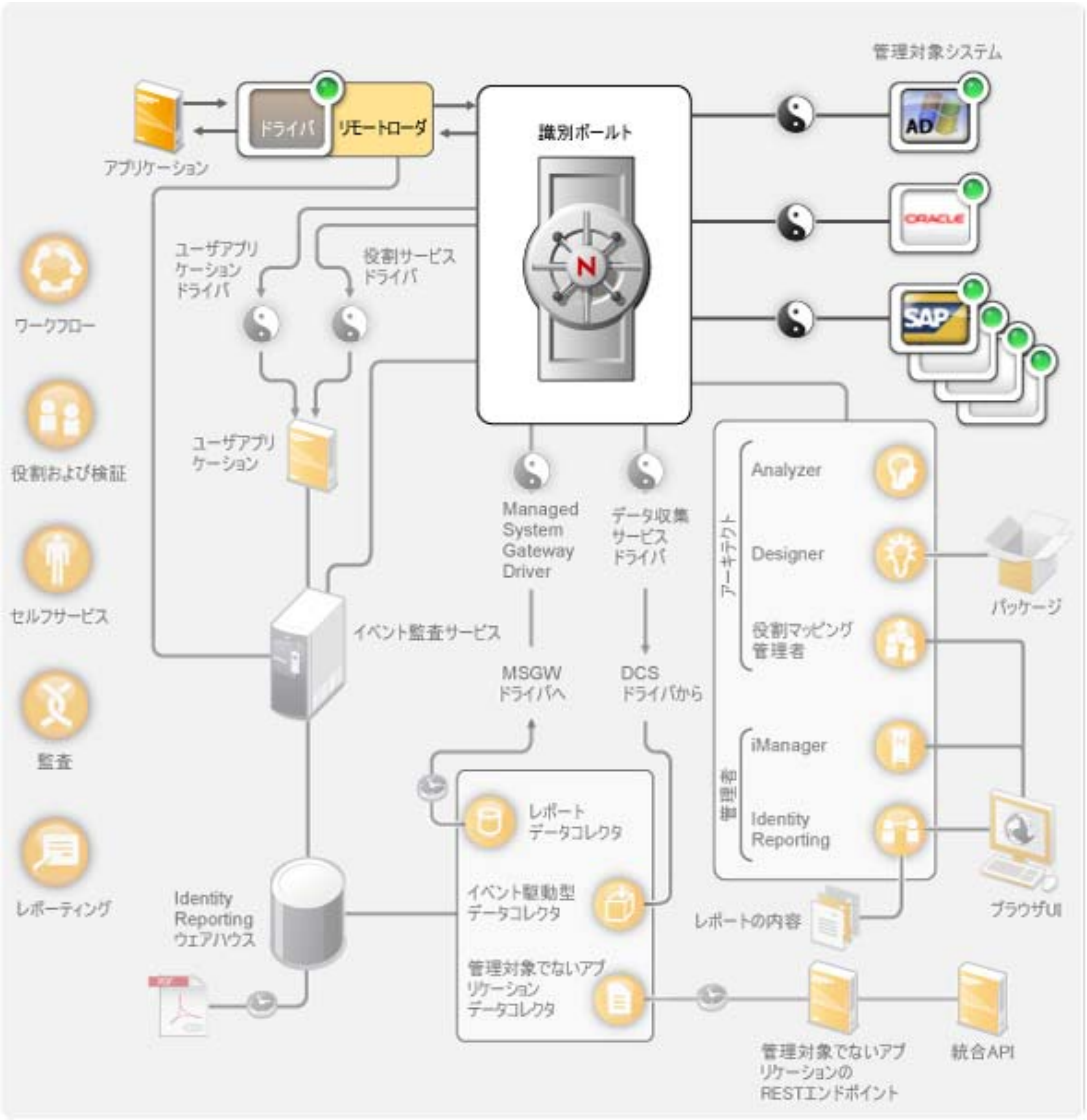
4.1 データ同期

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、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、Identity Manager 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 4-2 *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。

4.1.1 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。

Identity Manager 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、Identity Manager 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。Identity Manager エンジンは、メタディレクトリエンジンとも呼ばれます。

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。アプリケーション内のデータ変更 (イベント) を Identity Manager エンジンにレポートする。Identity Manager 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 Identity Manager 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 Identity Manager 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 Identity Manager 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。

4.1.2 主な提案

チャネル : 2 つの別の*チャネル*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 Identity Manager 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、Identity Manager 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 (購読者チャネル)。

データ操作 : XML ドキュメントがドライバチャネルを通過するので、ドキュメントのデータはチャ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、さまざまな建物用のアクセスデータベース内にアカウントを自動作成する操作は、従業員の場所の属性の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 :** たとえば、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、Identity Manager 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、複数のドライ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。

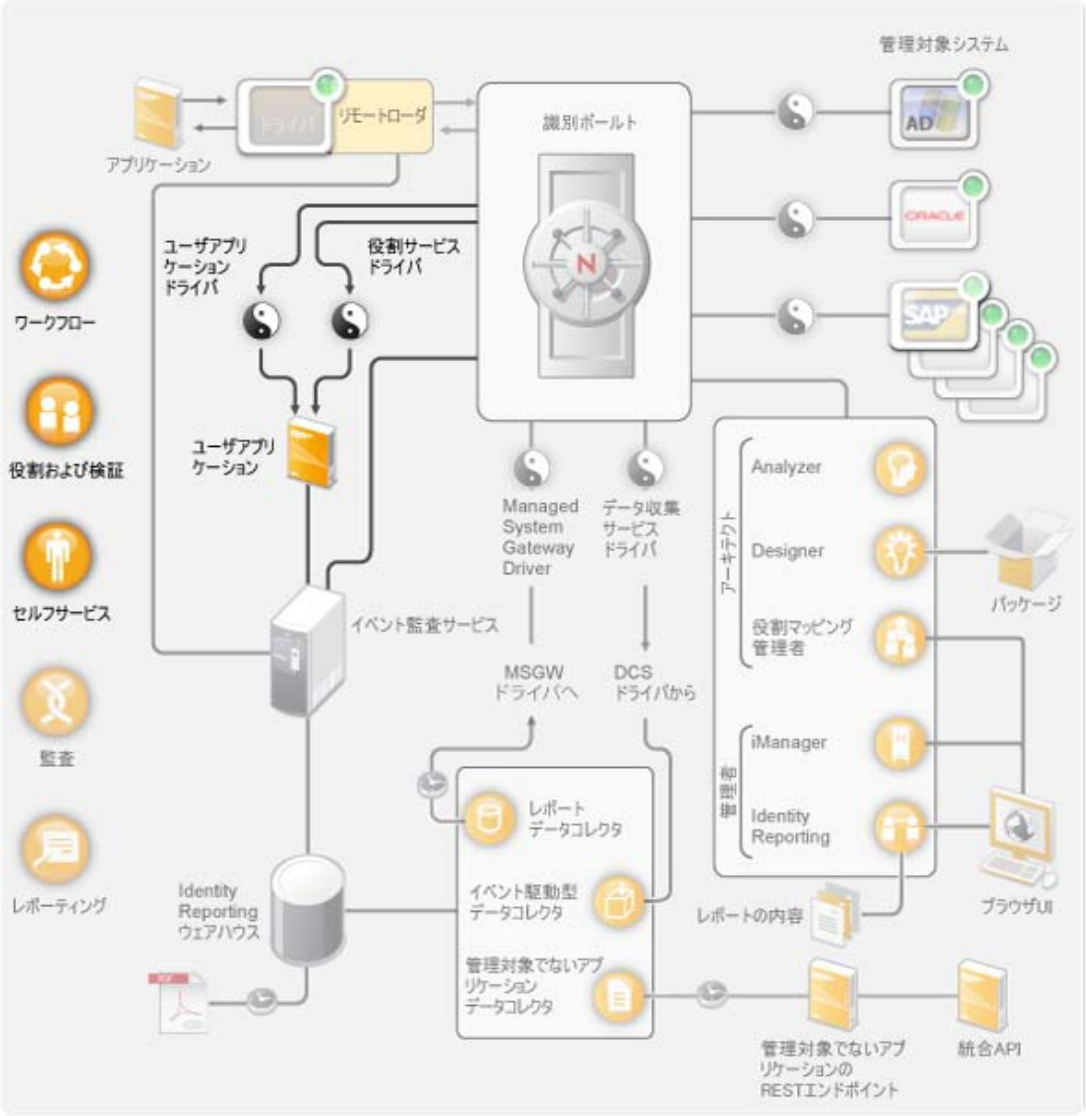
4.2 ワークフロー、役割、検証、およびセルフサービス

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。

User Application Roles Based Provisioning Module は、Identity Manager 4.0.1 Advanced Edition の一部です。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、役割分担制約、および認証機能を備えた標準的なユーザアプリケーションが含まれています。Identity Manager 4.0.1 Advanced Edition には、標準および役割ベースのプロビジョニングモジュール機能が含まれています。

図 4-3 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。

- 33 ページのセクション 4.2.1「コンポーネント」
- 34 ページのセクション 4.2.2「主なコンセプト」

4.2.1 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。

役割とリソースのサービスドライバ : 役割とリソースのサービスドライバは、すべての役割とリソースの割り当てを管理し、承認を必要とする役割とリソース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ー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。

4.2.2 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。どの役割が競合すると考えられるかを規定する義務の分離制約を構築できます。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、義務の分離違反として記録されるので、次に説明する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。

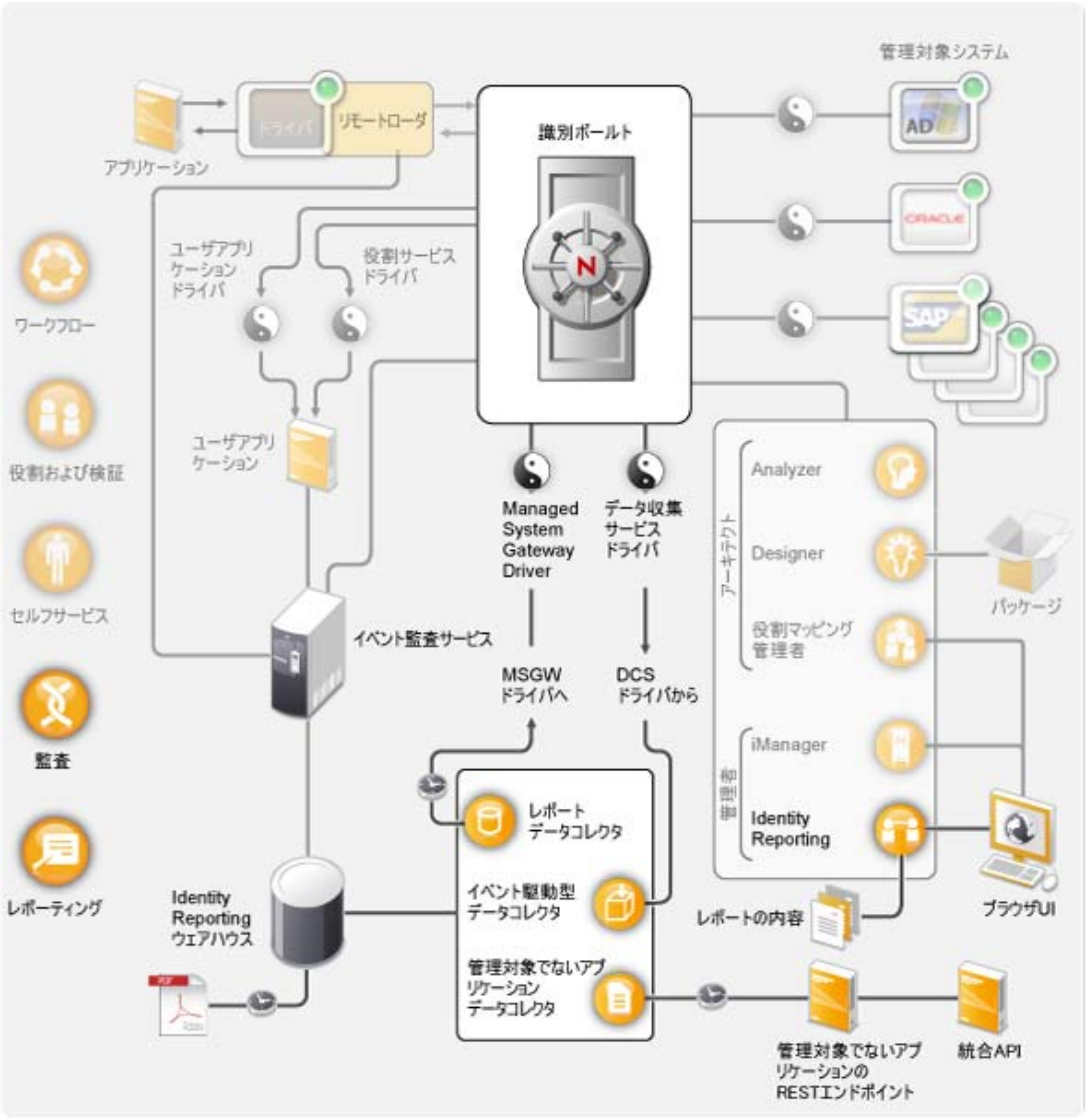
Roles Manager は、義務の分離制約の管理、役割システムの設定、およびすべてのレポートの実行に関する例外を持つ Roles Module Administrator と同じことができます。Roles Module Administrator には役割システム内で無制限のスコープがありますが、Roles Manager のスコープは特別設計のユーザ、グループ、および役割に限定されています。

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。

4.3 監査とレポート

監査およびレポーティングは、次の図が示すように、Identity Manager 4.0.1 の新機能である Identity Reporting モジュールによって提供されます。

図 4-4 *Identity Manager の監査とレポート*



Identity Reporting モジュールは、Identity Manager の 設定のさまざまな側面に関する重要なビジネス情報を表示するレポートを生成します。これには、識別ボールトおよび Active Directory または SAP などの管理対象システムから収集された情報も含まれます。Identity Reporting モジュールでは、次のコンポーネントを使用してデータを管理します。

イベント監査サービス：レポートのインポート、変更、削除、またはスケジューリングなどのレポーティングモジュール内で実行されたアクションに関するログイベントを取得するサービスです。イベント監査サービス (EAS) は、RBPM (Roles Based Provisioning Module) および役割マッピング管理者 (RMA) 内で実行されるアクションに関連するログイベントを取得します。

アイデンティティ情報ウェアハウス : 次の種類の情報のためのリポジトリです。

- レポートの管理情報 (レポート定義、レポートスケジュール、完了したレポートなど)、レポーティングに使用されるデータベースビュー、および設定情報。
- 識別情報データ (レポートデータコレクタ、イベント駆動型データコレクタ、および非管理対象データコレクタによって収集される)。
- 監査データ (イベント監査サービスによって収集されたイベントが含まれる)。

アイデンティティ情報ウェアハウスには、SIEM (Security Information and Event Management、セキュリティ情報およびイベント管理) データベースに含まれる自身のデータが保存されます。

データ収集サービス : 組織のさまざまなソースから情報を集めるサービスです。データ収集サービスには、次の 3 つのサブサービスが含まれます。

- **レポートデータコレクタ :** プルデザインモデルを使用して、1 つ以上の識別ボールトデータソースからデータを取得します。収集は、一連の環境設定パラメータによって決定され、定期的に実行されます。データを収集するために、コレクタが Managed System Gateway Driver を呼び出します。
- **イベント駆動型データコレクタ :** プッシュデザインモデルを使用して、データ収集サービスドライバが取得したイベントデータを収集します。
- **非管理対象アプリケーションデータコレクタ :** それぞれのアプリケーション専用に記述された REST エンドポイントを呼び出すことによって、1 つ以上の非管理対象アプリケーションからデータを取得します。非管理対象アプリケーションとは、識別ボールトに接続されていない企業内のアプリケーションのことです。詳細については、『*Identity Reporting Module Guide*』の「REST Services for Reporting」を参照してください。

データ収集サービスドライバ : アカウント、役割、リソース、グループ、およびチームメンバーシップなど、識別ボールトに保存されているオブジェクトに対する変更を取得するドライバです。データ収集サービスドライバは、自身をデータ収集サービスに登録し、変更イベント (データの同期、追加、変更、および削除イベント) をデータ収集サービスにプッシュします。

取得された情報は、次のオブジェクトに対する変更を記録します。

- ユーザアカウントおよび識別情報
- 役割および役割レベル
- グループ

注 : Identity Reporting Module は動的グループをサポートせず、静的グループデータに関するレポートのみを生成します。

- グループメンバーシップ
- プロビジョニング要求の定義
- 義務の分離の定義および違反
- ユーザエンタイトルメント関連付け
- リソース定義およびリソースパラメータ
- 役割およびリソースの割り当て
- 識別ボールトのエンタイトルメント、エンタイトルメントタイプ、およびドライバ

Managed System Gateway Driver: 管理対象システムから情報を収集するドライバです。ドライバは識別ボールトに問い合わせて管理対象システムのデータを取得します。取得されたデータには、次のものが含まれます。

- すべての管理対象システムのリスト
- 管理対象システムのすべてのアカウントのリスト
- エンタイトルメントの種類、値、割り当て、および管理対象システムのユーザアカウントプロファイル

Identity Reporting: レポーティングモジュール用のユーザインタフェースを使用すると、パフォーマンスを最適化するために、レポートを混雑していない時間帯に実行するようスケジュールするのが楽になります。Identity Reporting モジュールの詳細については、『*Identity Reporting Module Guide*』を参照してください。

レポート : Identity Manager には、識別情報ウェアハウス内の情報を実用的かつ利用可能な方法で表示するための事前定義されたレポートが含まれています。カスタムレポートを作成することもできます。レポートの詳細については、「*Using Identity Manager 4.0 Reports*」を参照してください。カスタムレポートの詳細については、『*Identity Reporting Module Guide*』の「Creating Custom Report Definitions」を参照してください。

非管理対象アプリケーションの REST エンドポイント : 非管理対象アプリケーションとは、識別ボールトに接続されていないにもかかわらず、レポートの対象となるデータを含むアプリケーションのことです。アプリケーションに REST エンドポイントを定義することで、レポーティングモジュールがこのアプリケーションからデータを収集できます。

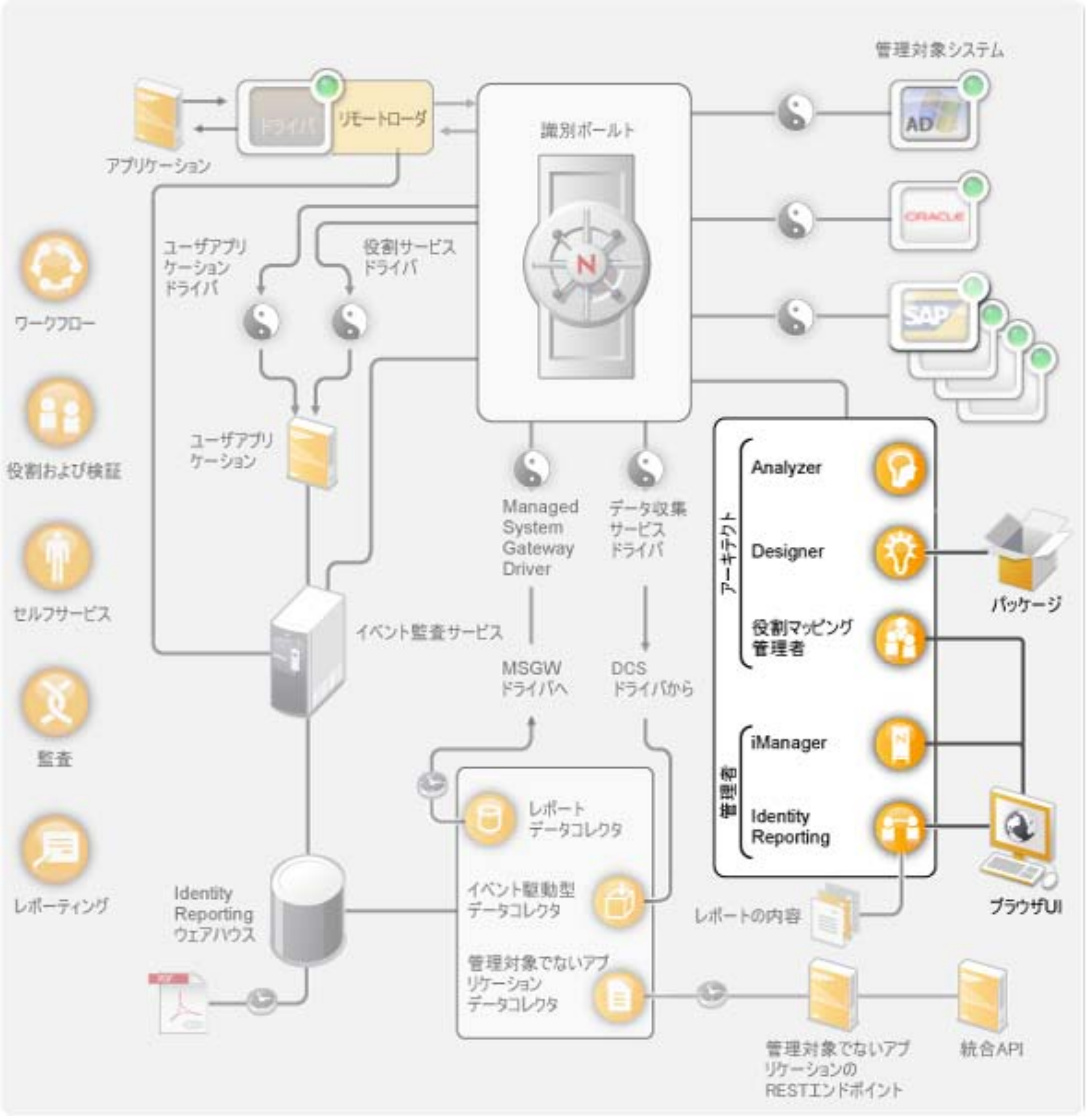
統合 API: Identity Reporting Module は、管理対象でないアプリケーション用の REST エンドポイントを実装したり、カスタムレポーティングアプリケーションを作成したりできる一連の REST API を提供します。

Identity Manager ツール

5

Identity Manager では、お客様が Identity Manager によるソリューションを構築し、維持するのに役立つツールを提供しています。それぞれにツールには特定の機能があります。

図 5-1 *Identity Manager ツール*



Designer を使用して、Identity Manager システムをオフライン環境でデザイン、作成、および設定し、ライブシステムに変更を展開します。また、Designer は、Identity Manager のドライバポリシーを事前設定したり、カスタマイズしたりするためのパッケージ管理機能を提供します。データを分析、クリーンアップ、および同期用に準備するための Identity Manager ソリューションを構築する場合には、Analyzer が使用されます。

役割マッピング管理者を使用して、Identity Manager のソリューション全体を通じて役割を作成および管理します。

iManager を使用して Designer と同様のタスクを実行したり、システムの健全性を監視したりすることもできます。ただし、iManager ではパッケージ管理がサポートされていません。iManager は管理タスクに使用し、Designer はパッケージへの変更、モデリング、および展開前のテストを必要とする設定タスクに使用することを推奨します。

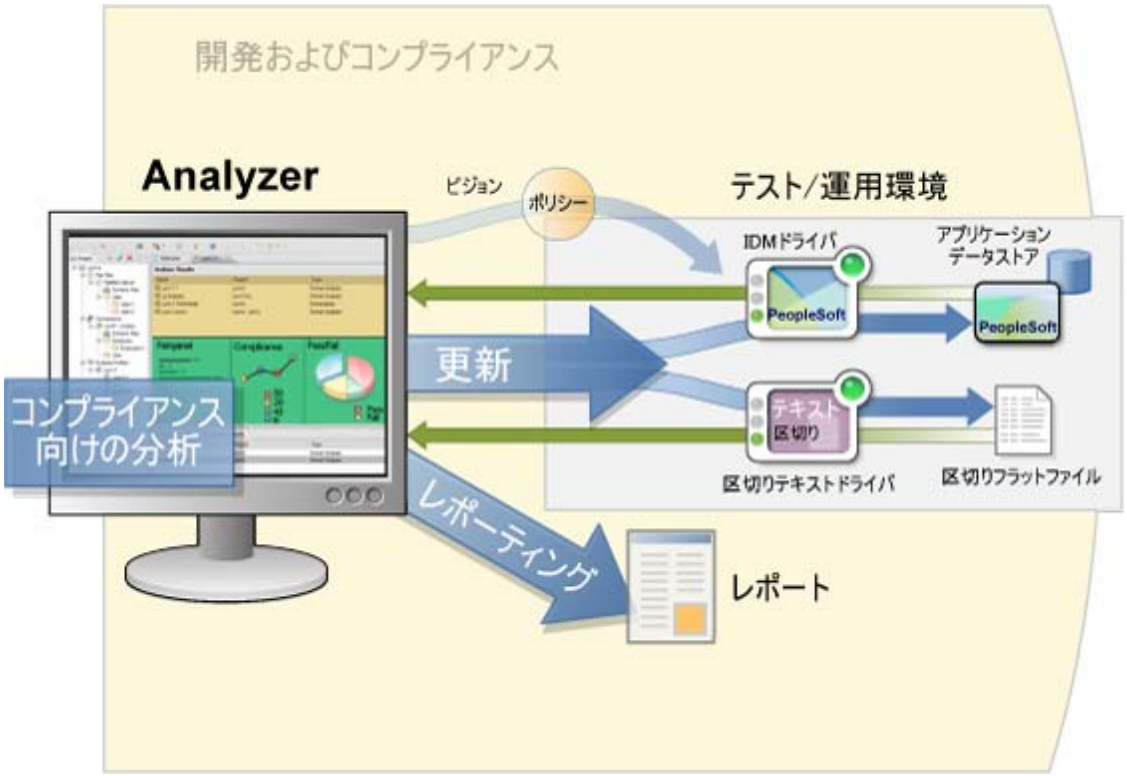
これらの各ツールの詳細情報については、次の項を参照してください。

- 40 ページのセクション 5.1「Analyzer」
- 41 ページのセクション 5.2「Designer」
- 42 ページのセクション 5.3「iManager」
- 42 ページのセクション 5.4「役割マッピング管理者」
- 43 ページのセクション 5.5「Identity Reporting」

5.1 Analyzer

Analyzer とは、Eclipse ベースの識別情報管理ツールセットで、プロビジョニングデータ分析、データクレンジング、データ更新、およびデータ監視とレポーティングが、内部データの品質方針を確実に遵守するようにします。Analyzer を使用すると、企業内に保存されているすべてのデータを分析、拡張、および制御できます。

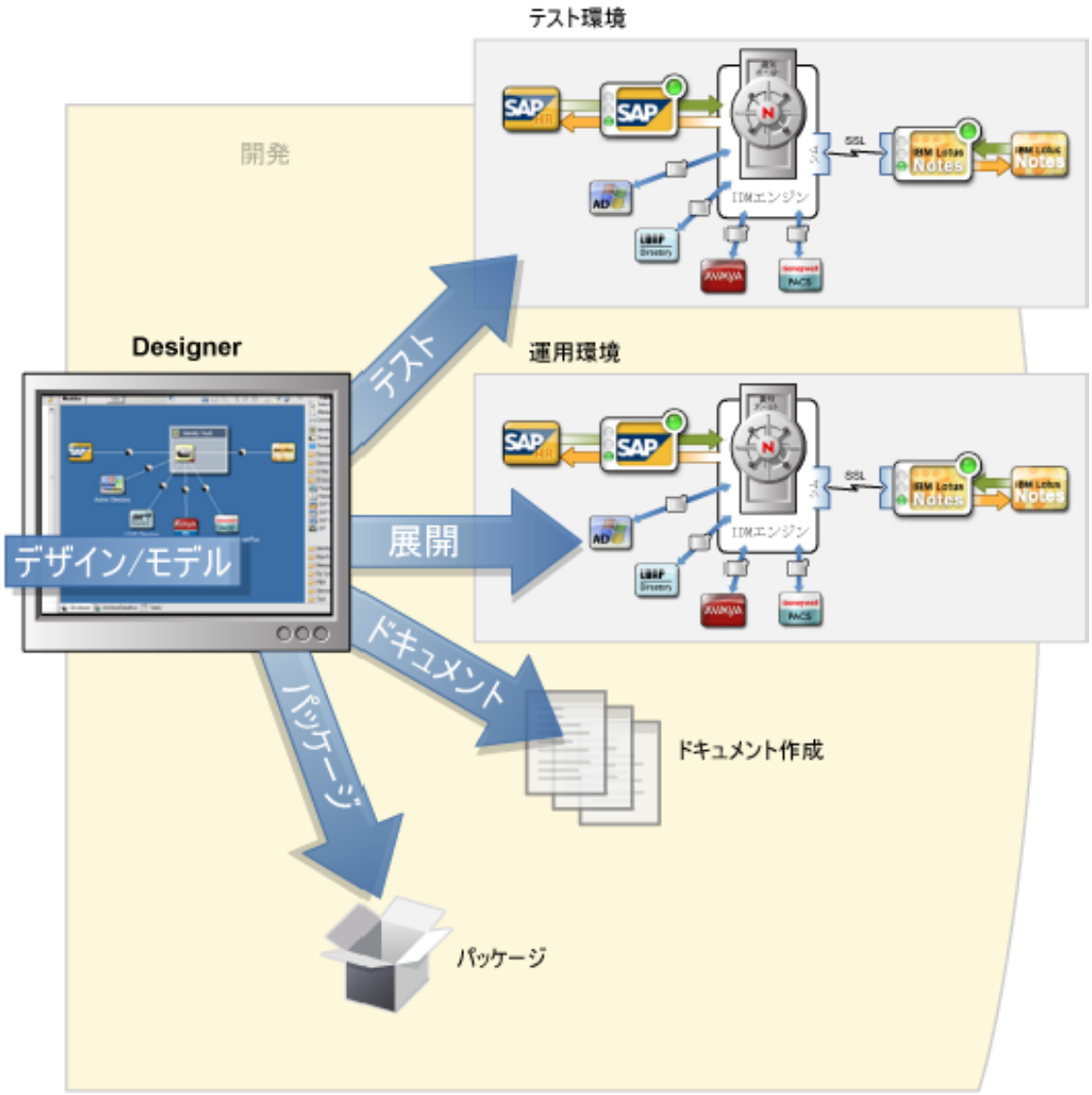
図 5-2 *Identity Manager 用の Analyzer*



5.2 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されます。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 5-3 Designer for Identity Manager



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。

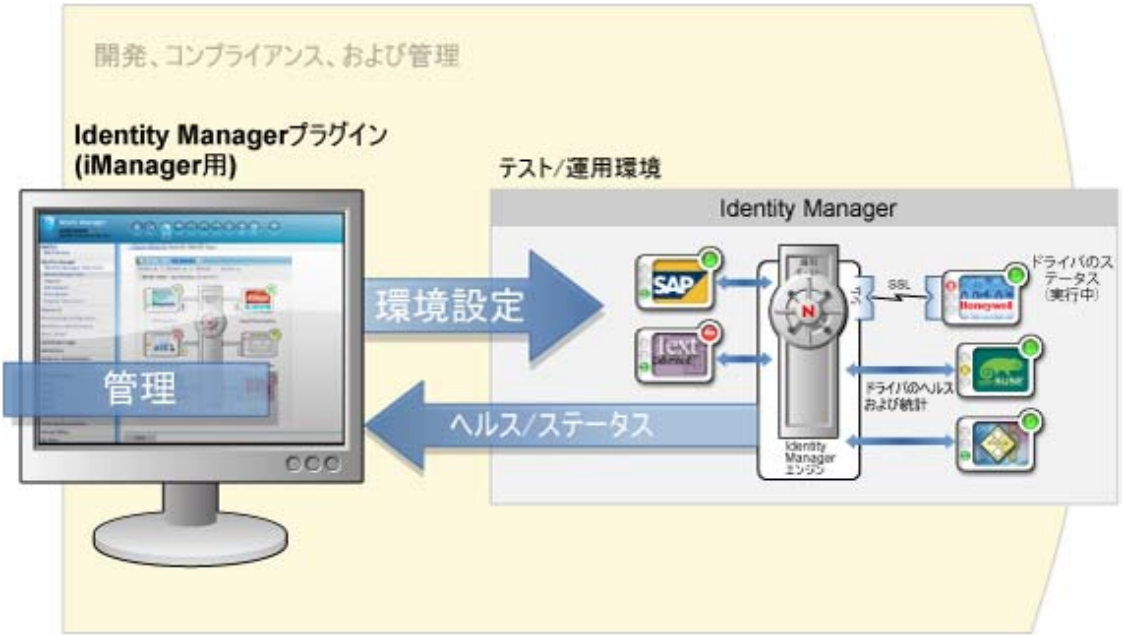
展開 : Designer での操作は、展開の開始時に運用環境に展開されます。これにより、運用環境でライブにする前に、ユーザが実験、結果のテスト、および問題の解決を行えます。

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。

5.3 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。

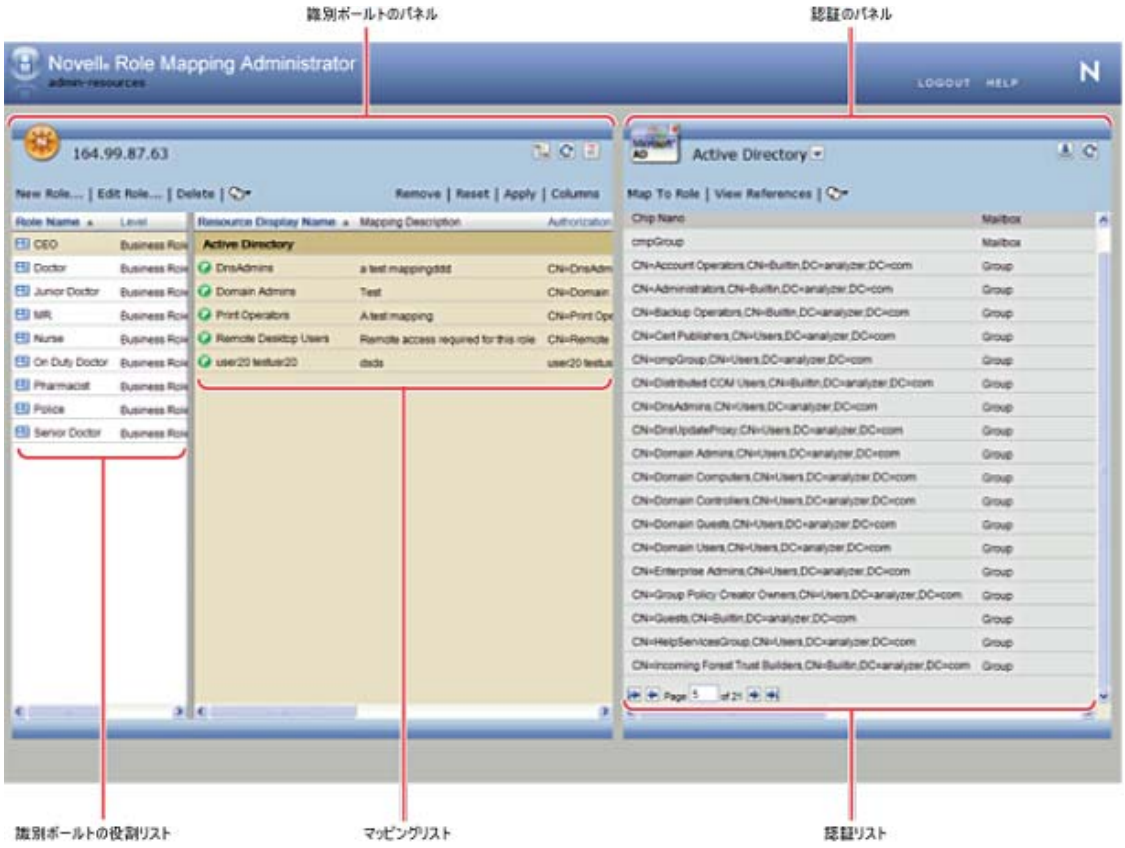
図 5-4 *Novell iManager*



5.4 役割マッピング管理者

役割マッピング管理者とは、主な IT システム内部で付与される権限および許可を検出する Web サービスのことです。このサービスによって、IT 管理者だけでなく、ビジネスアナリストがどの権限がどのビジネス役割に関連付いているかを定義および保守できます。

図 5-5 *役割マッピング管理者*



5.5 Identity Reporting

Identity Reporting モジュールは、Identity Manager の 設定のさまざまな側面に関する重要なビジネス情報を表示するレポートを生成します。これには、識別ボールトおよび Active Directory または SAP などの管理対象システムから収集された情報も含まれます。Identity Reporting Module は、レポートを生成するのに使用できる、一連の事前定義されたレポート定義を提供します。さらに、サードパーティ製ツールで定義されたカスタムレポートをインポートするオプションも使用できます。レポーティングモジュール用のユーザインタフェースを使用すると、パフォーマンスを最適化するために、レポートを混雑していない時間帯に実行するようスケジュールするのが楽になります。

図 5-6 *Identity Reporting モジュール*

Identity Reporting モジュールは、いくつかのオープンな統合ポイントを提供します。たとえば、Identity Manager に接続されていないサードパーティ製のアプリケーションに関するデータを収集する場合、カスタム REST エンドポイントを実装し、これらのアプリケーションアイコンからデータを収集できます。さらに、識別ボールトにプッシュされるデータをカスタマイズできます。このデータが利用可能になったら、カスタムレポートを記述してこの情報を表示できます。

次に行う作業

6

Identity Manager 4.0.1 を構成するコンポーネントを理解したら、次にマニュアルを使用してお客様自身の Identity Manager ソリューションを構築します。次の項では、リストされているタスク向けのマニュアルの入手先を説明します。

6.1 Identity Manager ソリューションの計画

Identity Manager ソリューションをデザインするための最初のステップは、お客様のビジネスにおいてこのソリューションがどのように役立つかを厳密に決定することです。『*Identity Manager 4.0.1 Framework インストールガイド*』の「計画」の項を参考に、Designer を使用して Identity Manager ソリューションの計画を作成します。『*User Application: Design Guide*』を参照し、ユーザアプリケーションソリューションをデザインすることもできます。

Designer を使用すると、プロジェクトの中に情報を取得したり、他のユーザと情報を共有したりできます。変更を開始する前に、Designer を使用してソリューションのモデルを作成することもできます。Designer の詳細については、「*Understanding Designer for Identity Manager*」を参照してください。

6.2 データ同期の準備

計画を作成したら、環境内のデータを同期する準備を行う必要があります。Analyzer は、同期のためにデータを分析、クリーンアップ、および準備するツールです。詳細については、『*Analyzer 4.0.1 for Identity Manager Administration Guide*』を参照してください。

6.3 Identity Manager のインストールまたはアップグレード

計画を作成し、データを準備したら、Identity Manager をインストールできます。お客様の IT 環境が小規模から中規模であり、以前 Identity Manager を使用したことがない場合は、統合インストーラを使用するのが最適です。統合インストーラは、Identity Manager に付属しているすべてのコンポーネントをインストールおよび設定します。詳細については、『*Identity Manager 4.0.1 統合インストールガイド*』を参照してください。

Identity Manager システムをすでに使用していたり、IT 環境 , が大規模だったりする場合は、『*Identity Manager 4.0.1 Framework インストールガイド*』を参照して、Identity Manager の異なるコンポーネントをインストールまたはアップグレードします。Identity Manager の各マネージャコンポーネントは、別々にインストールおよび設定されるので、Identity Manager ソリューションをカスタマイズできます。

- インストール手順については、「Identity Manager 4.0.1 Framework インストールガイド」の「*インストール*」を参照してください。
- アップグレード手順については、『*Identity Manager 4.0.1 Upgrade and Migration Guide*』の「Performing an Upgrade」を参照してください。
- 既存のシステムを新しいハードウェアに移行する場合は、『*Identity Manager 4.0.1 Upgrade and Migration Guide*』の「Performing an Upgrade」を参照してください。
- 役割ベースのプロビジョニングモジュールを移行する必要がある場合は、『*Identity Manager Roles Based Provisioning Module 4.0 User Application: Migration Guide*』を参照してください。

6.4 Identity Manager の設定

Identity Manager をインストールしたら、完全に機能するソリューションになるようにさまざまなコンポーネントを設定する必要があります。

- 46 ページのセクション 6.4.1「データの同期化」
- 46 ページのセクション 6.4.2「役割のマッピング」
- 47 ページのセクション 6.4.3「ユーザアプリケーションの環境設定」
- 47 ページのセクション 6.4.4「設定、監査、レポーティング、およびコンプライアンス」

6.4.1 データの同期化

Identity Manager は、ドライバを使用して異なるアプリケーション、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間でデータを同期します。Identity Manager をインストールしたら、データを同期させるシステムごとに 1 つ以上のドライバを作成し設定する必要があります。

各ドライバには、データ同期に必要な要件および設定手順について説明するマニュアルガイドがあります。ドライバのガイドは、Identity Manager 4.0.1 ドライバのマニュアルの Web サイト (http://www.novell.com/documentation/idm401drivers/index.html) を参照してください。

管理対象システムごとに特有のドライバガイドを参照して、識別情報データを同期するドライバを作成します。

6.4.2 役割のマッピング

異なるシステム間で同期している情報がある場合、役割マッピング管理者 (RMA) を使用して異なるシステム内の役割を管理します。詳細については、『*Novell Identity Manager Role Mapping Administrator 4.0.1 ユーザガイド*』を参照してください。

6.4.3 ユーザアプリケーションの環境設定

次のステップでは、Identity Manager ソリューションにユーザアプリケーションを使用してビジネス的な観点を追加します。ユーザアプリケーションを利用すれば、次のようなビジネスニーズに対処できます。

- 役割ベースのプロビジョニングのアクションを実行する便利な方法を提供します。
- 従業員が完全に組織のポリシーを自覚し、それらのポリシーに準拠する手順を実行することを確認するための方法が組織に確実に存在するようにします。
- ユーザへのセルフサービスの提供、新規ユーザの自己登録、匿名 / ゲストユーザのアクセスを実現します。
- 組織のポリシーに適合した社内リソースへのアクセスと、企業のセキュリティポリシーコンテキスト内でのプロビジョニングが保証されます。
- 社内のすべてのシステムにわたって、ユーザ情報の入力、更新、削除などの管理作業の手間を減らせます。
- 識別情報、サービス、リソース、およびアセットの手動または自動プロビジョニングを管理します。
- 複雑なワークフローをサポートします。

『*Identity Manager Roles Based Provisioning Module 4.0 ユーザアプリケーション : アプリケーションガイド*』には、ユーザアプリケーションのこれらの機能の設定方法に関する情報が含まれています。

6.4.4 設定、監査、レポーティング、およびコンプライアンス

Identity Manager ソリューションを構築する上で最後の最も重要なステップは、ソリューションがビジネスの方針に準拠していることを確認できるように、監査、レポーティング、およびコンプライアンスの機能を設定するステップです。次のガイドを参照し、それぞれの機能をセットアップおよび設定します。

- **監査 :**『*Identity Manager 4.0.1 Reporting Guide for Novell Sentinel*』を参照してください。
- **レポーティング :**『*Identity Reporting Module Guide*』および「*Using Identity Manager 4.0 Reports*」を参照してください。
- **コンプライアンス :**「Identity Manager Roles Based Provisioning Module 4.0 ユーザアプリケーション : 管理ガイド」の「*整合性タブの使用*」を参照してください。

6.5 Identity Manager の管理

Identity Manager ソリューションが完了したら、お客様のビジネスが変化し、成長するに従って Identity Manager ソリューションを管理、維持、および変更するのに役立つさまざまなガイドが存在します。さまざまな管理ガイドが Identity Manager 4.0.1 のマニュアルの Web サイト (http://www.novell.com/documentation/idm401/index.html) の「管理」見出しのところに用意されています。