Oracle® Identity and Access Management

概要

10*g*（10.1.4.0.1）

部品番号 : B31466-01

2006 年 9 月

ORACLE®

Oracle Identity and Access Management 概要 , 10*g*（10.1.4.0.1）

部品番号 : B31466-01

原本名 : Oracle Identity and Access Management Introduction 10*g* (10.1.4.0.1)

原本部品番号 : B31291-01

原本著者 : Ellen Desmond

原本協力者 : Francisco Abedrabbo, Pradeep Bhoj, Sidharth Choudhury, Rohit M. Gupta, Hasan Rizvi, Ashish Koli, Michael Mesaros, Sanjay Rallapalli, Olaf Stullich, Frank Villavicencio

目次

はじめに ix

対象読者 x
ドキュメントのアクセシビリティについて x
関連ドキュメント x
表記規則 xi
サポートおよびサービス xi

1 Oracle Identity and Access Management の概要

Oracle Identity and Access Management 製品 1-2
ディレクトリ・サービス 1-2
Oracle Internet Directory 1-2
Oracle Virtual Directory 1-3
Oracle Directory Integration Platform 1-3
アクセス管理 1-4
Oracle Access Manager 1-4
アクセス・システム 1-4
ID システム 1-4
Oracle Identity Federation 1-4
Oracle Application Server Single Sign-On 1-5
Oracle Enterprise Single Sign-On Suite 1-5
ID 管理 1-5
Oracle Identity Manager 1-5
Oracle Delegated Administration Services 1-6
Oracle Identity and Access Management 製品のパッケージング 1-6
Oracle Identity and Access Management Suite 1-6
Oracle Application Server インフラストラクチャ・コンポーネント 1-7

2 ドキュメント・ロードマップ

Oracle Identity and Access Management 管理者 2-2
Oracle Identity and Access Management 製品のインストールおよびアップグレード 2-2
Oracle Identity and Access Management 製品の管理 2-3
Oracle アプリケーション開発者 2-4
エンタープライズ・セキュリティ・アーキテクト 2-5

3 Oracle Internet Directory

Oracle Internet Directory の利点 3-2
Oracle Internet Directory の機能 3-2
Identity Management Grid Control プラグインでの管理 3-3
参照整合性 3-3
サーバー・チェーン 3-3
他の Oracle 製品との統合 3-3
セキュリティ 3-4
グローバリゼーション・サポート 3-5
分散ディレクトリ 3-5
Oracle Internet Directory の動作 3-5
Oracle Internet Directory のコンポーネント 3-5
Oracle Internet Directory の接続 3-6
Oracle ディレクトリ・サーバー・インスタンス 3-9

4 Oracle Virtual Directory

Oracle Virtual Directory の利点 4-2
Oracle Virtual Directory の機能 4-3
データ・フェデレーション 4-3
データの所有権 4-4
複数のデータ・アダプタ 4-4
柔軟性の高いセキュリティ・ドメイン 4-5
セキュア・データ公開 4-5
高可用性サポート 4-6
アプリケーション統合 4-6
柔軟性の高いデプロイ 4-7
カスタム・アプリケーション・プログラミング・インタフェース 4-7
低コスト、高価値のソリューション 4-7
Oracle Virtual Directory の動作 4-8
イントラネット ID の例 4-8
エクストラネット ID の例 4-9
シナリオ・レビュー 4-9

5 Oracle Directory Integration Platform

Oracle Directory Integration Platform の利点 5-2
Oracle Directory Integration Platform の機能 5-2
Oracle Directory Integration Platform の動作 5-3
同期 5-3
統合 5-5
Oracle Directory Integration Platform の例 5-6

6 Oracle Access Manager

Oracle Access Manager の利点 6-2
Oracle Access Manager アクセス・システムの機能 6-2
Oracle Access Manager アクセス・システムの動作 6-4
Oracle Access Manager アクセス・システムのコンポーネント 6-4

Policy Manager とアクセス・システム・コンソール 6-5
Access Server 6-6
WebGates および AccessGates 6-7
アクセス・システムの操作 6-7
Oracle Access Manager ID システムの機能 6-8
Oracle Access Manager ID システムの動作 6-10
Oracle Access Manager ID システムのコンポーネント 6-10
Identity Server および ID アプリケーション 6-11
WebPass 6-12

7 Oracle Identity Federation

Oracle Identity Federation の利点 7-2
Oracle Identity Federation の機能 7-2
Oracle Identity Federation の動作 7-3
フェデレーション・ユースケース 7-3
フェデレーション・イベント・フロー 7-5
フェデレーション・プロトコル・プロファイル 7-5
フェデレーション・アーキテクチャ 7-6

8 OracleAS Single Sign-On

Oracle Application Server Single Sign-On の利点 8-2
Oracle Application Server Single Sign-On の機能 8-2
OracleAS Single Sign-On の動作 8-3
シングル・サインオン・システムのコンポーネント 8-3
Single Sign-On Server へのアクセス 8-4
パートナ・アプリケーションへのアクセス 8-4
2 回目以降のパートナ・アプリケーションの認証 8-5
パートナ・アプリケーションからのログアウト 8-5
外部アプリケーションへのアクセス 8-5
OracleAS Portal の外部アプリケーション・ポートレットへのアクセス 8-5
外部アプリケーションの最初の認証 8-5
外部アプリケーションの 2 回目以降の認証 8-6
外部アプリケーションからのログアウト 8-6

9 Oracle Identity Manager

Oracle Identity Manager の利点 9-2
Oracle Identity Manager プロビジョニングの機能 9-2
Oracle Identity Manager の動作 9-3
層 1: クライアント 9-4
層 2: アプリケーション・サーバー 9-5
層 3: データベース 9-5
Oracle Identity Manager のアテステーションおよびレポート作成 9-6
機能の概略 9-6
レポートのタイプ 9-6
Oracle Identity Manager のアテステーションおよびレポート作成の動作 9-8

10 Oracle Delegated Administration Services

Oracle Delegated Administration Services の利点 10-2
Oracle Delegated Administration Services の機能 10-2
Identity Management Grid Control プラグインでの管理 10-2
Oracle Internet Directory セルフ・サービス・コンソール 10-2
権限委任レベル 10-3
プロキシ・ユーザーの集中化 10-3
Oracle Delegated Administration Services の動作 10-4

索引

図一覧

3-1 Oracle Internet Directory の概要 3-6
3-2 標準的な Oracle Internet Directory ノード 3-7
3-3 Oracle ディレクトリ・サーバー・インスタンス・アーキテクチャ 3-9
4-1 Oracle Virtual Directory サーバー・アーキテクチャ 4-2
4-2 ディレクトリ・サービスの仮想化と分散 4-2
4-3 イントラネットおよびエクストラネット・アプリケーションの環境 4-8
5-1 Oracle Directory Integration Platform Service: ディレクトリの同期 5-4
5-2 Oracle Directory Integration Platform Service: アプリケーションの統合 5-5
5-3 Oracle Directory Integration Platform 環境の例 5-6
6-1 基本アクセス・システムのインストール 6-4
6-2 基本的なアクセス・システム構成 6-8
6-3 単純な環境におけるコンポーネント 6-10
7-1 従業員ポータルからパートナへのシングル・サインオン 7-3
7-2 フェデレーテッド・アカウントの作成 7-4
7-3 Oracle Identity Federation 7-6
7-4 Oracle Identity Federation のサード・パーティ統合 7-7
8-1 mod_osso でのシングル・サインオン 8-4
9-1 Oracle Identity Manager の 3 層のアーキテクチャ 9-4
10-1 ホスト環境における管理レベル 10-3
10-2 Oracle Delegated Administration Services におけるプロキシ・ユーザー機能 10-4
10-3 Oracle Delegated Administration Services 環境における情報フロー 10-5

表一覧

2-1 インストールまたはアップグレード前にお読みください 2-2
2-2 管理の前にお読みください 2-3
2-3 アプリケーション開発の前にお読みください 2-4
2-4 使用する製品を決定するためにお読みください 2-5
3-1 Oracle Internet Directory ノードのコンポーネント 3-7

はじめに

このマニュアルは、Oracle Identity and Access Management の概要です。

対象読者

このマニュアルは、次の読者を対象にしています。

- ID 管理者およびアクセス管理者
- Oracle アプリケーション開発者
- エンタープライズ・セキュリティ・アーキテクト

ドキュメントのアクセシビリティについて

オラクル社は、障害のあるお客様にもオラクル社の製品、サービスおよびサポート・ドキュメントを簡単にご利用いただけることを目標としています。オラクル社のドキュメントには、ユーザーが障害支援技術を使用して情報を利用できる機能が組み込まれています。HTML 形式のドキュメントで用意されており、障害のあるお客様が簡単にアクセスできるようにマークアップされています。標準規格は改善されつつあります。オラクル社はドキュメントをすべてのお客様がご利用できるように、市場をリードする他の技術ベンダーと積極的に連携して技術的な問題に対応しています。オラクル社のアクセシビリティについての詳細情報は、Oracle Accessibility Program の Web サイト `http://www.oracle.com/accessibility/` を参照してください。

ドキュメント内のサンプル・コードのアクセシビリティについて

スクリーン・リーダーは、ドキュメント内のサンプル・コードを正確に読めない場合があります。コード表記規則では閉じ括弧だけを行に記述する必要があります。しかし JAWS は括弧だけの行を読まない場合があります。

外部 Web サイトのドキュメントのアクセシビリティについて

このドキュメントにはオラクル社およびその関連会社が所有または管理しない Web サイトへのリンクが含まれている場合があります。オラクル社およびその関連会社は、それらの Web サイトのアクセシビリティに関しての評価や言及は行っておりません。

Oracle サポート・サービスへの TTY アクセス

アメリカ国内では、Oracle サポート・サービスへ 24 時間年中無休でテキスト電話（TTY）アクセスが提供されています。TTY サポートについては、(800)446-2398 にお電話ください。

関連ドキュメント

関連ドキュメントの詳細は、第 2 章を参照してください。

表記規則

このマニュアルでは次の表記規則を使用します。

表記規則	意味
太字	太字は、操作に関連する Graphical User Interface 要素、または本文中で定義されている用語および用語集に記載されている用語を示します。
イタリック	イタリックは、ユーザーが特定の値を指定するプレースホルダ変数を示します。
固定幅フォント	固定幅フォントは、段落内のコマンド、URL、サンプル内のコード、画面に表示されるテキスト、または入力するテキストを示します。

サポートおよびサービス

次の各項に、各サービスに接続するための URL を記載します。

Oracle サポート・サービス

オラクル製品サポートの購入方法、および Oracle サポート・サービスへの連絡方法の詳細は、次の URL を参照してください。

```
http://www.oracle.co.jp/support/
```

製品マニュアル

製品のマニュアルは、次の URL にあります。

```
http://otn.oracle.co.jp/document/
```

研修およびトレーニング

研修に関する情報とスケジュールは、次の URL で入手できます。

```
http://www.oracle.co.jp/education/
```

その他の情報

オラクル製品やサービスに関するその他の情報については、次の URL から参照してください。

```
http://www.oracle.co.jp
http://otn.oracle.co.jp
```

注意： ドキュメント内に記載されている URL や参照ドキュメントには、Oracle Corporation が提供する英語の情報も含まれています。日本語版の情報については、前述の URL を参照してください。

1

Oracle Identity and Access Management の概要

Oracle Identity and Access Management は、企業がユーザー ID を全ライフサイクルにわたって自動的に管理することを可能にし、ユーザーに企業内のリソースと資産へ安全にアクセスする手段を提供する製品群です。オラクル社は、この製品群の最初の製品である Oracle Internet Directory を 1999 年に発表しました。それ以降、ディレクトリの同期、ディレクトリのセキュアな管理、Web シングル・サインオン・サービスなど多数の ID およびアクセス管理機能を開発し発表しています。そのすべては Oracle 製品群に統合されました。2005 年と 2006 年に、オラクル社は戦略的買収を通じて、ID およびアクセス管理の機能をさらに強化しました。オラクル社は、ID フェデレーション、Web アクセス管理、委任 ID 管理、ユーザー ID プロビジョニングおよび仮想ディレクトリのテクノロジの最善のソリューションに大幅な投資を行っています。

この章の内容は次のとおりです。

- Oracle Identity and Access Management 製品
- Oracle Identity and Access Management 製品のパッケージング

Oracle Identity and Access Management 製品

この項では、Oracle Identity and Access Management を構成する個別の製品を紹介します。製品は機能別に 3 つの大きなカテゴリに分けることができます。

- ディレクトリ・サービス
- アクセス管理
- ID 管理

ディレクトリ・サービス

Lightweight Directory Access Protocol（LDAP）に基づくディレクトリ・サービスは、ID およびアクセス管理の戦略の中心です。オラクル社は、一般的な企業におけるデプロイでの要件を満たし、その他の Oracle 製品での活用も可能な、スケーラブルなディレクトリおよび統合テクノロジを提供します。Oracle Directory Services には、次のコンポーネントが含まれます。

- Oracle Internet Directory
- Oracle Virtual Directory
- Oracle Directory Integration Platform

Oracle Internet Directory

Oracle Internet Directory は、Oracle Database のスケーラビリティ、高可用性およびセキュリティ機能を利用した、スケーラブルで堅固な LDAP V3 準拠ディレクトリ・サービスです。Oracle Internet Directory は、ID およびアクセス管理デプロイの集中化されたユーザー・リポジトリとして機能し、Oracle アプリケーション環境におけるユーザー管理を簡略化します。異機種エンタープライズ向けの非常にスケーラブルな規格ベースのディレクトリとしても機能します。

パフォーマンス、高可用性およびセキュリティは、Oracle Internet Directory の際立った特徴です。Oracle Internet Directory サーバーは、SMP プラットフォームにデプロイされているか、ハードウェア・クラスタ内のノードとしてデプロイされているかにかかわらず、CPU 数によるスケーラビリティを可能にする、マルチ・プロセス、マルチ・インスタンスのアーキテクチャを採用しています。これは業界でも独自のものであり、シングル・プロセスを採用しているディレクトリとは明らかに異なる点です。他にも、Oracle Internet Directory が抜きん出ている領域として、データ管理があります。ユーザー数が増えるにつれて、パイロット・インストールの構成、新しいディレクトリ・ノードの迅速なデプロイ、ディレクトリ・データのバックアップ、オンライン・バルク・プロビジョニングの実行に関する課題も増えます。Oracle Internet Directory は、Oracle Database のデータ管理機能を活用して、ホット・バックアップおよびパラレル・ロード操作をサポートします。さらに、Oracle Internet Directory は、オンライン・バルク・ユーザー・プロビジョニングを促進する高速のマルチスレッド・クライアント・ツールなどの特殊なディレクトリ管理ツールを提供します。また、Oracle Internet Directory は Oracle Database のセキュリティ機能を引き出して、セキュア・ディレクトリ・プロセスおよびデータ・ストアを提供します。

Oracle Internet Directory は、ユーザーおよび資格証明管理、電子メール・アドレス・ストレージ、および名前解決などのサービスについて、OracleAS Portal、Oracle E-Business Suite、Oracle Collaboration Suite および Oracle Database などのアプリケーションに使用される Oracle 製品群の主要なコンポーネントです。さらに、Oracle Internet Directory は PeopleSoft アプリケーションのディレクトリ・ストアとしてサポートされています。

Oracle Virtual Directory

セキュアなアプリケーション環境を作成するには、複数の場所やサービスに散在している既存のユーザー ID 情報を統合する必要がしばしばあります。Oracle Virtual Directory（以前の OctetString Virtual Directory Engine）は、LDAP または XML プロトコルを通して、これらのデータ・ソースへ単一で動的なアクセス・ポイントを提供します。これは、データを格納場所から移動したりコピーすることなく、リアルタイムに結合して単一の論理的なディレクトリとして表出することにより実現します。Oracle Virtual Directory は、Oracle Internet Directory、Microsoft Active Directory および Sun Java Systems Directory のインスタンスなどに格納された ID データについて、複数のアプリケーション固有のビューを提供できます。また、アプリケーション固有のソースへのデータ・アクセスを確保し、既存のデータ・ソースへの可用性を向上するためにも使用できます。これらの機能を使用すると、アプリケーションをデプロイする前にユーザーの情報を統合する必要がなくなり、アプリケーションのデプロイを促進し、コストを削減します。Oracle Virtual Directory は、ユーザー・リポジトリが追加、変更または削除されるにつれて変化する ID の状況に、それらのアプリケーションを常に適応させることができます。

Oracle Virtual Directory は、アプリケーションの既存 ID インフラストラクチャへの統合を促進します。Oracle Virtual Directory は、既存のディレクトリやユーザー・リポジトリを変更することなくこの統合を行うので、企業がデータの「所有権および表示の問題」に関して政治的な調整をする必要をなくし、迅速にこれらのサービスをデプロイすることを可能にします。Oracle Virtual Directory は、個別のアプリケーションの特定のニーズについて最適化されたディレクトリ情報の、複数のアプリケーションの中心となるビューを提供するためにデプロイすることもできます。

Oracle Directory Integration Platform

Oracle Directory Integration Platform は、ディレクトリ同期およびアプリケーション統合を様々なディレクトリおよび互換性のある Oracle 製品全体で実行するために設計された Oracle Internet Directory のコンポーネントです。Oracle Directory Integration Platform により、Oracle Internet Directory に依存するアプリケーションでは、他のディレクトリおよびエンタープライズ・ユーザー・リポジトリで管理されているユーザー・データを活用できます。同期機能により、顧客は様々なディレクトリと Oracle Internet Directory 間でデータを同期化できます。アプリケーション統合機能では、ユーザーの状態または情報に対する変更を、対象のアプリケーションに通知します。Oracle Directory Integration Platform は、複数の部門やアプリケーションに関連したディレクトリ情報を一括して格納および管理する企業レベルのメタ・ディレクトリを実装するためにも使用できます。Oracle Internet Directory には、Oracle Human Resources、Oracle Database、および Sun Java System Directory Server、Microsoft Active Directory、Novell eDirectory、OpenLDAP などのサード・パーティの LDAP サーバーと、購入直後に同期するためのエージェントが含まれます。

アクセス管理

アクセス管理は、エンタープライズ・リソースへのユーザー・アクセスを制御する手段です。アクセス管理製品により、異機種アプリケーション環境でファイングレインなアクセスの集中管理ができるだけでなく、購入直後から Oracle Portal、Oracle Collaboration Suite および Oracle E-Business Suite などの Oracle 製品との統合ができます。

Oracle アクセス管理製品には次のものがあります。

- Oracle Access Manager
- Oracle Identity Federation
- Oracle Application Server Single Sign-On
- Oracle Enterprise Single Sign-On Suite

Oracle Access Manager

以前は Oracle COREid Access and Identity として知られていた Oracle Access Manager は、異機種環境で実行中の Web アプリケーションおよびリソースへのアクセス制御だけでなく、Web ベースの ID 管理も提供します。複雑なディレクトリ中心の環境で多くのユーザーを管理するために必要な、ユーザーおよびグループ管理、委任管理、パスワード管理およびセルフサービス機能を提供します。Access Manager は、ブラウザ・フォーム、デジタル証明およびスマートカードなどの一般的な認証方式をすべてサポートし、OracleAS 10*g*、BEA WebLogic、IBM WebSphere、Vignette などを含む、ほとんどのアプリケーション・サーバーおよびポータルとシームレスに統合します。ユーザー ID および資格証明には、Oracle Internet Directory、Microsoft Active Directory および Sun Java System Directory を含む、多数のリポジトリからアクセスできます。Access Manager では、ユーザー・アクセス・ポリシーは集中管理を通じて高度な粒度で定義および強制できます。

アクセス・システム アクセス・システムでは、URL やレガシーな非 HTTP のアプリケーションなどのリソースを保護することができます。ID システムによって格納された情報を使用して、リソースにアクセスできるユーザー、グループおよび組織を制御します。リソースへのアクセスを制御する設定情報とセキュリティ・ポリシーをディレクトリ・サーバーへ格納します（Oracle Access Manager 固有のオブジェクト・クラスを使用します）。アクセス・システムの構成設定、アクセス・ポリシー・データおよびユーザー・データの格納に同じディレクトリを使用できます。または、このデータを別のディレクトリ・サーバーに格納できます。

ID システム ID システムは、委任管理、ユーザー・セルフサービスおよびリアルタイムの変更管理を提供する一連のアプリケーションです。ID システムは、ユーザー、グループおよび組織についての情報を格納します。たとえば、ディレクトリ・サーバーでグループを作成、管理および削除できます。承認が必要ないセルフサービス、承認付きのサブスクリプション、ルールベースのサブスクリプション、サブスクリプションの非許可などの、グループのサブスクリプション・ポリシーを定義できます。

Oracle Identity Federation

ビジネス・プロセスを Web に移行する企業が増えるにつれて、より多くの組織でパートナ・アプリケーションを含めるためにエンタープライズの境界を拡張する必要性が増しています。フェデレーテッド ID 管理を使用すると、クロスドメインのシングル・サインオンを可能にすることと、企業がユーザー ID を管理し、他のドメインで管理されているリソースへのアクセス時にそれらを保証できるようにすることによって、企業は独立して活動することも、ビジネス目的で協力することもできます。

以前は COREid Federation として知られていた Oracle Identity Federation は、スタンドアロン・アプリケーションの使いやすさと移植性を、スケーラブルで規格ベースの実績ある相互操作アーキテクチャと組み合せた、自己完結型のフェデレーション・ソリューションを提供します。企業がプライバシおよびセキュリティの規制へのコンプライアンスを高めつつ、ポータルまたはエクストラネット内にビジネス・パートナを安全にリンクする際に役立ちます。ID フェデレーションにより、企業は業界標準のプロトコルを選択しながら複数のパートナーを管理することができます。ID フェデレーションは、顧客の ID 管理インフラストラクチャ（Oracle および Oracle 以外）との組込み統合を提供して包括的なユーザー・エクスペリエンスを実現し、自動登録、ID マッピング、シームレスなアクセス制御ナビゲーションなどの例に対応します。

Oracle Application Server Single Sign-On

Oracle Application Server Single Sign-On（OracleAS Single Sign-On）は、Oracle およびサード・パーティの Web アプリケーションへのシングル・サインオン・アクセスを提供します。OracleAS Single Sign-On は、Oracle Portal、Oracle Collaboration Suite および Oracle E-Business Suite などの Oracle アプリケーションに対するシングル・サインオンを可能にします。Oracle のみの環境に軽量の認証ソリューションを提供し、基本的なユーザー名とパスワードによる認証および X.509 証明書ベースの認証をサポートします。OracleAS Single Sign-On では、Oracle Internet Directory に格納されたユーザー ID および資格証明に対する認証を、Oracle Directory Integration Platform を介した Microsoft Active Directory および Sun Java System Directory などその他のリポジトリへの統合とともにサポートします。

Oracle Enterprise Single Sign-On Suite

Oracle Enterprise Single Sign-On Suite（eSSO Suite）は発売予定の製品です。この製品は、既存アプリケーションへの変更を必要とせず、エンタープライズ内のすべてのアプリケーションおよびリソースへの真のシングル・サインオンを提供します。これにより、デスクトップおよびすべてのレガシー・アプリケーションへの強力な複数ファクタの認証を、シームレスに改良できます。eSSO Suite では、ユーザーは複数のパスワードやユーザー名を記憶して管理する必要がありません。また、忘れてしまったパスワードのリセットを求めるユーザーに応対するヘルプデスクの時間と費用を節約します。Oracle eSSO Suite では、ユーザーが一度ログオンすると、eSSO が残りを行い、ログオン、パスワード選択、パスワード変更とリセットを含む、すべてのパスワード管理を自動化します。

ID 管理

Oracle Identity Management は、ファイアウォールの内側と外側の両方のエンタープライズ・リソース全体で、エンタープライズがユーザー ID のエンドツーエンド・ライフサイクルを管理できるようにする製品セットです。

ユーザー ID のプロビジョニングの自動化によって IT 管理コストが削減でき、セキュリティが向上します。プロビジョニングは法規制のコンプライアンスにおいても重要な役割を果します。コンプライアンス・イニシアティブでは、これらの規格へのコンプライアンスの実証だけではなく、企業ポリシーの施行にも焦点が置かれています。エンタープライズ ID 管理ソリューションは、ユーザーおよびそのアクセス権限を監査する手段だけでなく、企業ポリシーのユーザー管理面を実装するメカニズムも提供することができます。

Oracle Identity and Access Management Suite には、次の ID 管理製品が含まれます。

- Oracle Identity Manager
- Oracle Delegated Administration Services

Oracle Identity Manager

Oracle Identity Manager プラットフォームは、ユーザー ID のプロビジョニングおよびプロビジョニング解除を自動化し、ファイアウォールの内側と外側の両方のエンタープライズ・リソース全体での、企業によるユーザー ID の全ライフサイクルにわたる管理を可能にします。包括的なワークフロー・エンジンに内包された、ユーザー・プロビジョニング、ID 管理およびパスワード管理を自動化する ID 管理プラットフォームを提供します。

ユーザー ID のプロビジョニングの自動化によって IT 管理コストが削減でき、セキュリティが向上します。プロビジョニングは法規制のコンプライアンスにおいても重要な役割を果します。Oracle Identity Manager の主な機能には、パスワード管理、ワークフローおよびポリシー管理、ID リコンシリエーション、レポート作成および監査、アダプタを介した拡張性が含まれます。

Oracle Identity Manager は、アテステーション・サポートも提供します。アテステーションは、ユーザーまたはシステム・マネージャに人々のアクセス権限を定期的に確認させるプロセスです。既存のサーベンス・オクスリー要件では、企業が財政上重要なすべてのシステムについて 3 ～ 6 か月ごとにアテステーションを実施することが要求されています。Identity Manager には、エンタープライズ顧客が費用効果が高くタイムリな方法でこれらの法的要件を満たすために役立つ、非常にフレキシブルなアテステーション・ソリューションが含まれています。アテステーション・プロセスを Identity Manager で設定することにより、エンタープライズ顧客

は、レビューア用のユーザー・アクセス権限レポートの生成、配信、確認、サインオフ、委任、トラッキングおよびアーカイブのプロセスを、定期的または不定期ベースで自動化できます。

Oracle Delegated Administration Services

Oracle Delegated Administration Services は Oracle Internet Directory の一部で、ユーザーおよびアプリケーション管理者ごとのディレクトリ情報の信頼できるプロキシ・ベース管理を提供します。Oracle Delegated Administration Services は、OracleAS Portal、Oracle Collaboration Suite、Oracle Database Security Manager および Oracle E-Business Suite などの Oracle 製品用の管理インタフェースに埋め込まれた、一連の事前定義済の Web ベース・ユニットとして実装されます。Oracle Internet Directory に組み込まれているのは、DAS セルフサービス・コンソールです。これは、Oracle Delegated Administration Services フレームワーク上に構築された使いやすい Web ベースのツールです。DAS セルフサービス・コンソールは、エンド・ユーザーおよびアプリケーション管理者がディレクトリ内でデータを検索および管理できるようにし、Oracle Application Server 管理者に Oracle 環境におけるエンド・ユーザー管理の手段を提供します。

Oracle Identity and Access Management 製品のパッケージング

Oracle Identity and Access Management ソリューションには、次の 2 つのパッケージがあります。

- 異機種環境エンタープライズの ID およびアクセス管理要件に対応することを目的とした最善のコンポーネントの包括セットである Oracle Identity and Access Management Suite
- Oracle Application Server インフラストラクチャ・インストールの一部として含まれるコンポーネントのセット

この項では、これらの 2 つのパッケージについて説明します。この項の内容は次のとおりです。

- Oracle Identity and Access Management Suite
- Oracle Application Server インフラストラクチャ・コンポーネント

Oracle Identity and Access Management Suite

Oracle Identity and Access Management Suite には次の製品が含まれています。これらの製品は、このマニュアルで説明されています。

- Oracle Internet Directory
- Oracle Virtual Directory
- Oracle Access Manager
- Oracle Identity Federation
- Oracle Identity Manager

さらに、Oracle Identity and Access Management Suite には、フェデレーションおよびセキュア Web サービス・アプリケーションの開発のための API を提供する Oracle Security Developer Tools が含まれます。

Oracle Application Server インフラストラクチャ・コンポーネント

このマニュアルに記載されている 4 つの ID およびアクセス管理製品は Oracle Application Server インフラストラクチャのコンポーネントであり、Oracle Application Server、Oracle Database および Oracle Collaboration Suite に含まれています。これらの 4 つの製品には次のものがあります。

- Oracle Internet Directory
- Oracle Directory Integration Platform
- Oracle Application Server Single Sign-On
- Oracle Delegated Administration Services

Oracle Application Server インフラストラクチャをインストールする際に、これらのコンポーネントを同じサーバーまたは異なるサーバーにインストールするように選択できます。

> **関連資料：** Oracle Application Server のインストレーション・ガイドの OracleAS インフラストラクチャのインストールに関する章

注意： Oracle Internet Directory は、Oracle Identity and Access Management Suite と Oracle Application Server インフラストラクチャの両方に含まれています。

Oracle Application Server 10*g*（10.1.4.0.1）の時点で、これらの 4 つの製品は Identity Management Grid Control プラグインで管理できます。これは Oracle Enterprise Manager 10*g* Grid Control の機能を使用します。

> **関連資料：**『Oracle Identity Management インフラストラクチャ管理者ガイド』の Identity Management Grid Control プラグインに関する章

Oracle Application Server インフラストラクチャには、Oracle Application Server Certificate Authority も含まれます。これは、X.509v3 証明書を発行、取消および公開して、PKI ベースの強力な認証方式をサポートします。

2

ドキュメント・ロードマップ

この章では、他のドキュメントへのポインタを提供します。この章は、次の異なるカテゴリのユーザーのための項から構成されます。

- Oracle Identity and Access Management 管理者
- Oracle アプリケーション開発者
- エンタープライズ・セキュリティ・アーキテクト

Oracle Identity and Access Management 管理者

この項では、Oracle Identity and Access Management の管理者が読む必要のあるドキュメントをリスト表示します。Oracle Identity and Access Management の管理者のタスクは、次の 2 つの大きな項目に分類されます。

- Oracle Identity and Access Management 製品のインストールおよびアップグレード
- Oracle Identity and Access Management 製品の管理

Oracle Identity and Access Management 製品のインストールおよびアップグレード

この項では、Oracle Identity and Access Management の管理者が特定の製品をインストールまたはアップグレードする前に読む必要のあるドキュメントをリスト表示します。

表 2-1 インストールまたはアップグレード前にお読みください

タスク	ドキュメント
Oracle Internet Directory、Oracle Directory Integration Platform、Oracle Delegated Administration Services または Oracle Application Server Single Sign-On のインストール	『Oracle Application Server エンタープライズ・デプロイメント・ガイド』 Oracle Application Server のリリース・ノート Oracle Application Server のクイック・インストレーション・ガイド Oracle Application Server のインストレーション・ガイド
Oracle Internet Directory、Oracle Directory Integration Platform、Oracle Delegated Administration Services または Oracle Application Server Single Sign-On のアップグレード	Oracle Application Server のリリース・ノート 『Oracle Application Server アップグレードおよび互換性ガイド』
Oracle Virtual Directory のインストールまたはアップグレード	『Oracle Virtual Directory Server Installation Guide』
Oracle Access Manager のインストールまたはアップグレード	『Oracle Access Manager アップグレード・ガイド』 『Oracle Access Manager インストレーション・ガイド』
Oracle Identity Federation のインストールまたはアップグレード	『Oracle Identity Federation 管理者ガイド』のインストールに関する章
Oracle Identity Manager のインストールまたはアップグレード	『Oracle Identity Manager Installation and Upgrade Guide for JBoss』 『Oracle Identity Manager Installation and Upgrade Guide for WebLogic』 『Oracle Identity Manager Installation and Upgrade Guide for WebSphere』

Oracle Identity and Access Management 製品の管理

この項では、Oracle Identity and Access Management の管理者が特定の製品を管理する前に読む必要のあるドキュメントをリスト表示します。Oracle Internet Directory、Oracle Directory Integration Platform、Oracle Delegated Administration Services または Oracle Application Server Single Sign-On を管理する前に、各製品用の特定のドキュメントだけでなく、最初の行にリスト表示されているドキュメントも参照してください。

表 2-2 管理の前にお読みください

タスク	入門ドキュメント	上級ドキュメント
Oracle Internet Directory、Oracle Directory Integration Platform、Oracle Delegated Administration Services または Oracle Application Server Single Sign-On の管理	『Oracle Identity Management インフラストラクチャ管理者ガイド』 『Oracle Application Server クイック管理者ガイド』	『Oracle Application Server 管理者ガイド』 『Oracle Application Server エンタープライズ・デプロイメント・ガイド』 『Oracle Application Server パフォーマンス・ガイド』 『Oracle Application Server 高可用性ガイド』
Oracle Internet Directory の管理	『Oracle Internet Directory 管理者ガイド』の第 1 章および第 2 章	『Oracle Internet Directory 管理者ガイド』のその他の章
Oracle Directory Integration Platform の管理	『Oracle Identity Management 統合ガイド』の第 1 章	『Oracle Identity Management 統合ガイド』のその他の章
Oracle Delegated Administration Services の管理	『Oracle Identity Management 委任管理ガイド』の第 1 章	『Oracle Identity Management 委任管理ガイド』のその他の章
Oracle Application Server Single Sign-On	『Oracle Application Server Single Sign-On 管理者ガイド』の第 1 章	『Oracle Application Server Single Sign-On 管理者ガイド』のその他の章
Oracle Virtual Directory の管理	『Oracle Virtual Directory Server Product Manual』の第 1 章	『Oracle Virtual Directory Server Product Manual』のその他の章
Oracle Access Manager の管理	『Oracle Access Manager 概要』の第 1 章	『Oracle Access Manager 概要』のその他の章 『Oracle Access Manager ID および共通管理ガイド』 『Oracle Access Manager アクセス管理ガイド』 『Oracle Access Manager デプロイメント・ガイド』 『Oracle Access Manager カスタマイズ・ガイド』 『Oracle Access Manager 統合ガイド』 『Oracle Access Manager スキーマ詳細』
Oracle Identity Federation の管理	『Oracle Identity Federation 管理者ガイド』の第 1 章	『Oracle Identity Federation 管理者ガイド』のその他の章

表 2-2 管理の前にお読みください（続き）

タスク	入門ドキュメント	上級ドキュメント
Oracle Identity Manager の管理	『Oracle Identity Manager Design Console Guide』の第 1 章 『Oracle Identity Manager Administrative and User Console Guide』の第 1 章	『Oracle Identity Manager Administrative and User Console Guide』のその他の章 『Oracle Identity Manager Design Console Guide』のその他の章 『Oracle Identity Manager Administrative and User Console Customization Guide』 『Oracle Identity Manager Tools Reference Guide』 『Oracle Identity Manager Audit Report Developer Guide』 『Oracle Identity Manager Best Practices Guide』

Oracle アプリケーション開発者

この項では、Oracle アプリケーションの管理者が読む必要のあるドキュメントをリスト表示します。

表 2-3 アプリケーション開発の前にお読みください

タスク	ドキュメント
Oracle Internet Directory、Oracle Directory Integration Platform、Oracle Delegated Administration Services または Oracle Application Server Single Sign-On 用のアプリケーションの開発	『Oracle Identity Management インフラストラクチャ管理者ガイド』 『Oracle Application Server アプリケーション開発者ガイド』 『Oracle Containers for J2EE セキュリティ・ガイド』 Sun Developer Network（`http://java.sun.com/products/jndi`）にある Java Naming and Directory Interface（JNDI）ドキュメント 『Oracle Containers for J2EE サービス・ガイド』 『Oracle Identity Management アプリケーション開発者ガイド』 『Oracle Internet Directory API Reference』 Oracle Application Server のリリース・ノートの API 固有の注意のすべて
Oracle Virtual Directory 用のアプリケーションの開発	『Oracle Virtual Directory Server Product Manual』の第 8 章、第 9 章および第 10 章
Oracle Access Manager 用のアプリケーションの開発	『Oracle Access Manager 開発者ガイド』 『Oracle Access Manager カスタマイズ・ガイド』
Oracle Identity Federation 用のアプリケーションの開発	『Oracle セキュリティ開発ツール・リファレンス』の第 9 章および第 11 章 『Oracle Security Developer Tools Liberty SDK 1.1 Java API Reference』 『Oracle Security Developer Tools Liberty SDK 1.2 Java API Reference』 『Oracle Security Developer Tools SAML 1.0/1.1 Java API Reference』 『Oracle Security Developer Tools SAML 2.0 Java API Reference』

表 2-3 アプリケーション開発の前にお読みください（続き）

タスク	ドキュメント
Oracle Identity Manager 用のアプリケーションの開発	『Oracle Identity Manager Audit Report Developer's Guide』
	『Oracle Identity Manager Application Development API Usage Guide』
	『Oracle Identity Manager Tools Reference』
	『Oracle Identity Manager Design Console Guide』

エンタープライズ・セキュリティ・アーキテクト

この項には、エンタープライズ・セキュリティ・アーキテクトがどの ID およびアクセス管理製品を使用するか判断するために読む必要のあるドキュメントをリスト表示しています。

表 2-4 使用する製品を決定するためにお読みください

ドキュメント
『Oracle Application Server 高可用性ガイド』
『Oracle Application Server エンタープライズ・デプロイメント・ガイド』
『Oracle Identity Management インフラストラクチャ管理者ガイド』
『Oracle Internet Directory 管理者ガイド』の第 1 章および第 2 章
『Oracle Identity Management 統合ガイド』の第 1 章
『Oracle Identity Management 委任管理ガイド』の第 1 章
『Oracle Virtual Directory Server Product Manual』の第 1 章、第 2 章および第 3 章
『Oracle Access Manager 概要』の第 1 章
『Oracle Access Manager デプロイメント・ガイド』
『Oracle Access Manager 統合ガイド』
『Oracle Access Manager アクセス管理ガイド』
『Oracle Application Server Single Sign-On 管理者ガイド』の第 1 章
『Oracle Identity Federation 管理者ガイド』の第 1 章
『Oracle Identity Manager Design Console Guide』の第 1 章
『Oracle Identity Manager Administrative and User Console Guide』の第 1 章
『Oracle Identity Manager Best Practices Guide』

3

Oracle Internet Directory

Oracle Internet Directory は、分散したユーザーおよびネットワーク・リソースに関する情報の迅速な取得と集中管理を可能にする、汎用ディレクトリ・サービスです。Lightweight Directory Access Protocol（LDAP）バージョン 3 に、Oracle Database の高いパフォーマンス、スケーラビリティ、堅牢性および可用性を組み合せています。

この章の内容は次のとおりです。

- Oracle Internet Directory の利点
- Oracle Internet Directory の機能
- Oracle Internet Directory の動作

Oracle Internet Directory の利点

Oracle Internet Directory には様々な利点がありますが、その中でも、スケーラビリティ、高可用性、セキュリティおよび Oracle 環境との密な統合があります。

- **スケーラビリティ :** Oracle Internet Directory は Oracle Database の長所を引き出し、数テラバイトのディレクトリ情報のサポートを可能にします。さらに、共有 LDAP サーバーやデータベース接続プーリングなどのテクノロジにより、秒単位未満の検索レスポンス時間で数千のクライアントを同時にサポートします。

  Oracle Internet Directory は、Oracle Directory Manager や様々なコマンドライン・ツールなど、大量のデータを操作するためのデータ管理ツールも提供します。

- **高可用性 :** Oracle Internet Directory は、様々な重要アプリケーションのニーズを満たすように設計されています。たとえば、ディレクトリ・サーバー間の完全なマルチマスター・レプリケーションをサポートします。レプリケーション・コミュニティ内のあるサーバーが使用できなくなった場合、ユーザーは別のサーバーからデータにアクセスできます。サーバー上のディレクトリ・データへの変更に関する情報は、Oracle Database 上の特殊な表に格納されます。これらは、堅固なレプリケーション・メカニズムである Oracle Database Advanced Replication によって、ディレクトリ環境全体にレプリケートされます。

  Oracle Internet Directory は、Oracle Database の可用性機能もすべて活用します。ディレクトリ情報は Oracle Database に安全に格納されているため、Oracle のバックアップ機能によって保護されます。また、大規模なデータ・ストアと重い負荷で実行されている Oracle Database も、システム障害からすばやくリカバリできます。

- **セキュリティ :** Oracle Internet Directory は包括的で柔軟性の高いアクセス制御を提供します。管理者は、特定のディレクトリ・オブジェクトまたはディレクトリ・サブツリー全体へのアクセス権を付与または制限できます。また、Oracle Internet Directory は 3 つのユーザー認証レベルを実装しています。匿名、パスワード・ベースおよび証明書ベース（認証済アクセスとデータ・プライバシのための Secure Socket Layer（SSL）バージョン 3 を使用）の 3 つです。

- **Oracle 環境との統合 :** Oracle Internet Directory は、Oracle Directory Integration Platform を通じて、Oracle 環境と他のディレクトリ（NOS ディレクトリ、サード・パーティ・エンタープライズ・ディレクトリおよびアプリケーション固有のユーザー・リポジトリなど）との間に単一の統合ポイントを提供します。

Oracle Internet Directory の機能

Oracle コンポーネントでは、管理を簡単にし、セキュリティを厳重にし、複数ディレクトリ間の統合を簡単にするために Oracle Internet Directory を使用します。

Oracle Internet Directory には、次の機能があります。

- Identity Management Grid Control プラグインでの管理
- 参照整合性
- サーバー・チェーン
- 他の Oracle 製品との統合
- セキュリティ
- グローバリゼーション・サポート
- 分散ディレクトリ

Identity Management Grid Control プラグインでの管理

Oracle Application Server 10*g*（10.1.4.0.1）の時点で、Oracle Internet Directory を Identity Management Grid Control プラグインで管理できます。これは Oracle Enterprise Manager 10*g* Grid Control の機能を使用します。

関連資料：『Oracle Identity Management インフラストラクチャ管理者ガイド』の Identity Management Grid Control プラグインに関する章

参照整合性

参照整合性を有効にすると、ディレクトリ内のエントリを更新するたびに、サーバーはそのエントリを参照する他のエントリも更新します。

サーバー・チェーン

この機能により、同期やデータの移行をせずに、サード・パーティの LDAP ディレクトリにあるエントリをディレクトリ・ツリーの一部にマップし、Oracle Internet Directory を介してそれらにアクセスできます。

他の Oracle 製品との統合

Oracle Internet Directory は次のような複数の Oracle 製品と統合されています。

- **Oracle Virtual Directory** では、ターゲット・リポジトリの 1 つとして Oracle Internet Directory を使用できます。
- **Oracle Access Manager** では、Oracle Internet Directory を使用してスケーラブルで可用性の高いバック・エンド ID ストレージを提供します。
- **Oracle Identity Federation** では Oracle Internet Directory を ID リポジトリとして使用できます。Oracle Internet Directory を使用して、ID プロバイダとして実行時に SAML アサーションを作成します。
- **Oracle Identity Manager** では、ID のプロビジョニング先および ID 変更のリコンサイル元の LDAP ターゲット・システムとして Oracle Internet Directory を使用します。
- **Oracle Web Services Manager** では、Oracle Internet Directory を認証および認可に使用できる ID 情報のリポジトリとして使用します。
- **OracleAS Portal** では、セルフ・サービスの統合エンタープライズ・ポータルが、共通ユーザーおよびグループ属性を Oracle Internet Directory に格納できます。Oracle Portal 管理ツールでも、特定のタスクについて Oracle Delegated Administration Services を活用します。
- **Oracle Collaboration Suite** では、次の用途に Oracle Internet Directory を使用します。
  - ユーザーおよびグループについての情報の集中管理
  - Oracle Collaboration Suite コンポーネントのプロビジョニング（Oracle Internet Directory 内のデータに関連性のある変更が加えられるたびに、コンポーネントに通知する）
  - Oracle Collaboration Suite コンポーネントを使用して他のディレクトリに接続するエンタープライズのための、集中的な統合

  Oracle Internet Directory と Oracle Collaboration Suite を統合して、Oracle 製品全体でのユーザー管理およびプロビジョニングの共通のフレームワークを提供します。
- **Oracle Net Services** では、Oracle Internet Directory を使用して、データベース・サービスおよびサービスを表すために使用する単純名（ネット・サービス名）を格納および解決します。

- **データベース・エンタープライズ・ユーザー・セキュリティ**では、顧客は数千のエンタープライズ・ユーザーのデータベース・アクセスを簡単に管理できます。データベース・エンタープライズ・ユーザーは、データベース・ロールや権限などの認証および認可情報とともにディレクトリに格納されます。ユーザーが Oracle データベースにアクセスすると、データベースはユーザーの情報を Oracle Internet Directory から取得し、それを使用してサーバー上のユーザー・セッションのセキュリティ・コンテキストを設定します。このようなデータベース・アクセスの集中管理によって、管理者はすべてのアクセスを簡単に制御できます。
- **Oracle E-Business Suite** は Oracle Internet Directory と統合され、Oracle 製品全体でのユーザー管理およびプロビジョニングの共通のフレームワークを提供します。
- **Oracle Secure Enterprise Search**（SES）は複数のリポジトリに対する均一検索機能を提供します。Oracle Internet Directory は SES ユーザー認証および認可のための基本インフラストラクチャを提供します。SES によって使用されるアクセス制御リストに定義されたすべてのユーザーおよびロールは、Oracle Internet Directory に格納されます。

セキュリティ

Oracle Internet Directory は Oracle Identity Management インフラストラクチャの主な要素です。これにより、Oracle Internet Directory の共有インスタンスおよび関連付けられたインフラストラクチャ・ピースに対して動作する複数の Oracle コンポーネントをデプロイできます。この共有によって、エンタープライズはすべてのアプリケーションのセキュリティ管理を単純化することができます。

Oracle Internet Directory は、Oracle Identity Management インフラストラクチャにおける役割の他にも、情報保護のための多数の強力な機能を提供します。

Oracle Internet Directory のセキュリティ機能には次のものがあります。

- データの整合性 : データが転送中に改ざんされないことを保証します。
- データのプライバシ : データが Oracle Internet Directory とネットワーク内の他のコンポーネント間での転送中に不適切に観察されていないことを保証します。
- 認証 : ユーザー、ホストおよびクライアントの ID が正しく検証されることを保証します。
- 認可 : ユーザーが権限を持つ情報のみを読取りまたは更新することを保証します。
- パスワード・ポリシー : パスワードの定義方法および使用方法のルールを作成および強制します。
- パスワードの保護 : パスワードが容易に他人に検出されないことを保証します。

これらすべての機能を、Oracle Internet Directory で有効化されている複数のアプリケーションに対して均一なセキュリティ・ポリシーを施行するために使用できます。また、これはエンタープライズ環境とホスト環境のいずれでも実行できます。これは管理委任用のディレクトリをデプロイすることにより行います。このデプロイにより、グローバル管理者が部門のアプリケーションのメタデータへのアクセスを部門管理者に委任することなどが可能になります。これらの部門管理者は、自分の部門のアプリケーションへのアクセスを制御できます。

グローバリゼーション・サポート

Oracle Internet Directory は LDAP バージョン 3 の国際化（I18N）規格に従っています。これらの規格では、ディレクトリ・データを格納するデータベースで Unicode Transformation Format 8-bit（UTF-8）キャラクタ・セットを使用することが求められています。Oracle9*i* で、AL32UTF8 と呼ばれる新しい UTF-8 キャラクタ・セットが追加されました。このデータベース・キャラクタ・セットは、最新の追加文字を含む最新バージョンの Unicode（3.2）をサポートしています。これにより、Oracle Internet Directory では、Oracle グローバリゼーション・サポートでサポートされているほぼすべての言語の文字データを格納できます。また、Oracle Internet Directory 実装には複数の異なるアプリケーション・プログラム・インタフェースが含まれていますが、Oracle Internet Directory では各 API で正しい文字コードが使用されます。

分散ディレクトリ

オンライン・ディレクトリは論理的に集中化されていますが、物理的に複数のサーバーに分散させることができます。この分散によって単一のサーバーで行う必要のある作業が減り、ディレクトリが多数のエントリに対応できます。

分散ディレクトリは、レプリケートもパーティション化も可能です。情報がレプリケートされると、同じネーミング・コンテキストが複数のサーバーに格納されます。情報がパーティション化されると、一意で重複しない 1 つ以上のネーミング・コンテキストが各ディレクトリ・サーバーに格納されます。分散ディレクトリ内では、一部の情報はパーティション化され、一部の情報はレプリケートされます。

Oracle Internet Directory の動作

この項の内容は次のとおりです。

- Oracle Internet Directory のコンポーネント
- Oracle Internet Directory の接続
- Oracle ディレクトリ・サーバー・インスタンス

Oracle Internet Directory のコンポーネント

Oracle Internet Directory には次のものが含まれます。

- 直接に TCP/IP 上で多層アーキテクチャを使用して、人々やリソースの情報についてのクライアント・リクエストおよびその情報の更新に応答する、Oracle ディレクトリ・サーバー
- Oracle ディレクトリ・サーバー間で LDAP データをレプリケートする、Oracle ディレクトリ・レプリケーション・サーバー
- 次のようなディレクトリ管理ツール
  - Java ベースのグラフィカル・ユーザー・インタフェースを通じてディレクトリ管理を単純化する Oracle Directory Manager
  - LDAP クライアントから起動する多様なコマンドライン管理およびデータ管理ツール
  - Oracle Enterprise Manager 10*g* Application Server Control コンソールのディレクトリ・サーバー管理ツール。これらのツールでは次の内容を実行できます。
    * リアルタイムのイベントおよび統計を通常のブラウザから監視
    * データを新しいリポジトリに収集するプロセスの開始
- Oracle Internet Directory ソフトウェア開発者キット

  関連資料： Oracle Internet Directory ソフトウェア開発者キットの情報については、『Oracle Identity Management アプリケーション開発者ガイド』を参照してください。

Oracle Internet Directory の接続

Oracle Internet Directory ノードは、同じディレクトリ・ストアに接続された 1 つ以上のディレクトリ・サーバー・インスタンスで構成されます。ディレクトリ・ストア（すなわち、ディレクトリ・データのリポジトリ）は、Oracle Database です。

Oracle ディレクトリ・サーバーは、Oracle Database 上のアプリケーションとして稼働します。データベースとの通信には Oracle Net Services を使用します。これは、オペレーティング・システムに依存しない Oracle のデータベース接続ソリューションです。データベースは、同じホスト上にある場合もそうでない場合もあります。図 3-1 はこれらの関係を示しています。これはサーバー・アプリケーションとして稼働中の Oracle Internet Directory を示します。LDAP クライアントとディレクトリ管理クライアントは、LDAP を使用して Oracle ディレクトリ・サーバーに接続します。Oracle ディレクトリ・サーバーは Oracle データベースに Oracle Net Services を使用して接続します。

図 3-1 Oracle Internet Directory の概要

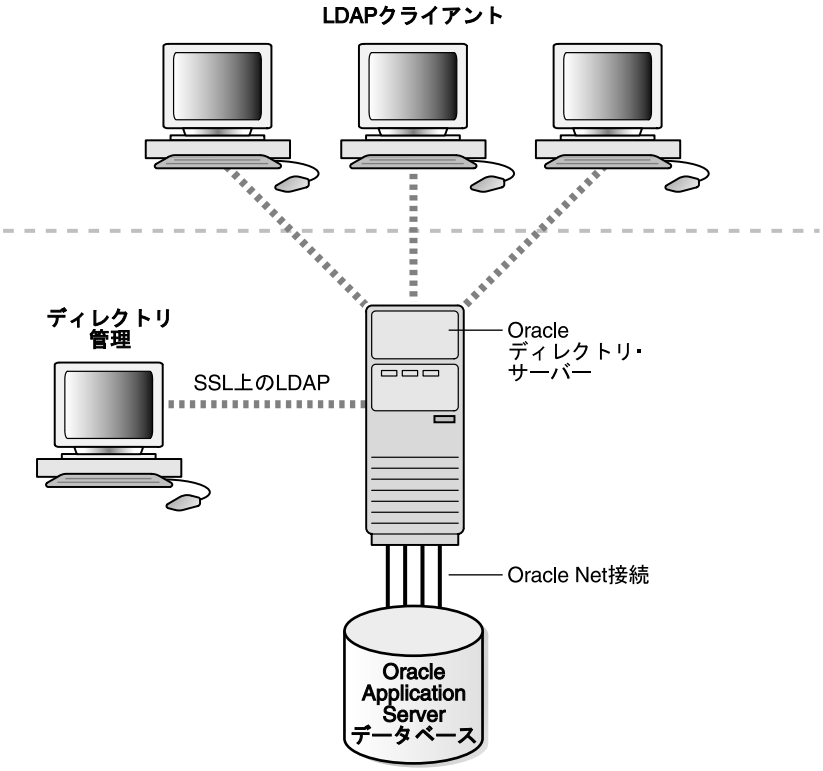


図 3-2 は、単一ノード上で実行中の様々なディレクトリ・サーバー・コンポーネントとその関連性を示しています。

Oracle Net Services は、Oracle データベース・サーバーと次との接続のすべてに使用されます。

- オブジェクト・クラス
- 非 SSL ポート 389 上の Oracle ディレクトリ・サーバー・インスタンス 1
- SSL 有効ポート 636 上の Oracle ディレクトリ・サーバー・インスタンス 2
- OID モニター

LDAP は、非 SSL ポート 389 上のディレクトリ・サーバー・インスタンス 1 と次との間の接続に使用されます。

- Oracle Directory Manager
- Oracle ディレクトリ・レプリケーション・サーバー

2 つのディレクトリ・サーバー・インスタンスとディレクトリ・レプリケーション・サーバーは、オペレーティング・システムを介して OID モニターに接続します。

図 3-2 標準的な Oracle Internet Directory ノード

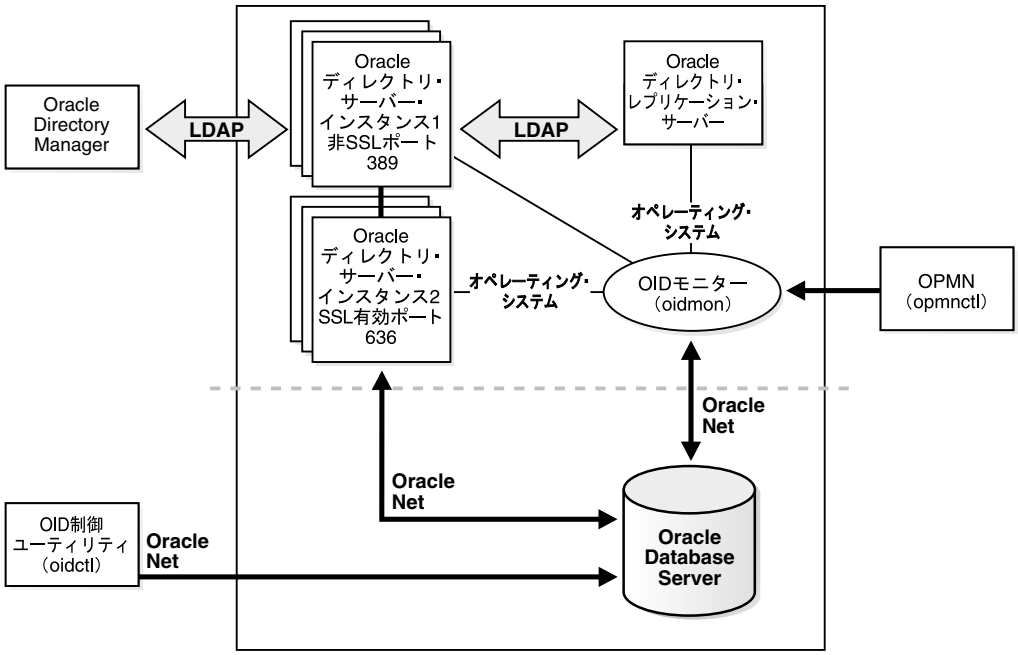


図 3-2 に示すように、Oracle Internet Directory ノードには次の主要コンポーネントが含まれます。

表 3-1 Oracle Internet Directory ノードのコンポーネント

コンポーネント	説明
Oracle ディレクトリ・サーバー・インスタンス	LDAP サーバー・インスタンスまたはディレクトリ・サーバー・インスタンスとも呼ばれ、特定の TCP/IP をリスニングしている単一の Oracle Internet Directory ディスパッチャ・プロセスを通じてディレクトリ・リクエストを提供します。1 つのノードに、それぞれ別のポートをリスニングしている複数のディレクトリ・サーバー・インスタンスがある場合があります。
Oracle ディレクトリ・レプリケーション・サーバー	レプリケーション・サーバーとも呼ばれ、変更を追跡して別の Oracle Internet Directory システムのレプリケーション・サーバーに送信します。1 つのノードにレプリケーション・サーバーは 1 つのみです。レプリケーション・サーバーを構成するかどうかは選択できます。
Oracle Database Server	ディレクトリ・データを格納します。ディレクトリ専用のデータベースを使用することを強くお薦めします。データベースは、ディレクトリ・サーバー・インスタンスと同じノードに置くことができます。
Oracle Process Manager and Notification Server（OPMN）	Oracle Internet Directory を Oracle Application Server コンポーネントとして管理します。OPMN は `$ORACLE_HOME/opmn/conf/opmn.xml` の OID コンポーネント・スニペット内のディレクティブを使用し、OIDMON および OIDCTL を必要に応じて起動します。Oracle Internet Directory サーバー・インスタンスは認識されません。

表 3-1 Oracle Internet Directory ノードのコンポーネント（続き）

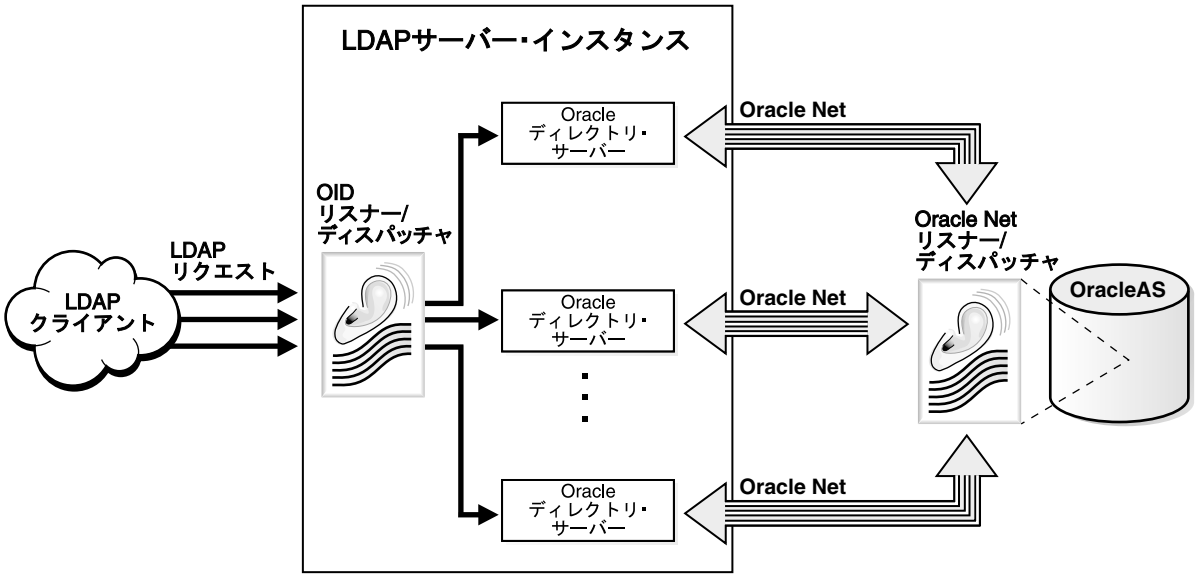
コンポーネント	説明
OID モニター（OIDMON）	LDAP サーバー・プロセスを開始、監視および終了します。レプリケーション・サーバーをインストールするように選択する場合、OID モニターがこれを制御します。OID 制御ユーティリティ（OIDCTL）を通じてコマンドを発行してディレクトリ・サーバー・インスタンスを起動または停止すると、コマンドはこのプロセスで解析されます。 OID モニターは、ユーザーが OID 制御ユーティリティから起動した LDAP サーバー・インスタンスの起動および停止リクエストを実行します。OID モニターはサーバーの監視も行い、サーバーが異常な理由で停止した場合には再起動します。 サーバー・インスタンスを起動すると、OID モニターはディレクトリ・インスタンス・レジストリにエントリを追加し、プロセス表でデータを更新します。また、プロセス表で検出したすべてのサーバーを再起動します。ディレクトリ・サーバー・インスタンスを停止すると、プロセス表が更新されます。OID モニターが異常停止したサーバーを再起動する場合、レジストリ・エントリをサーバーの起動時間で更新します。 OID モニターのすべてのアクティビティは、`$ORACLE_HOME/ldap/log/oidmon.log` ファイルに記録されます。このファイルは、Oracle Internet Directory サーバー・ファイル・システム上にあります。 OID モニターは、オペレーティング・システムから提供されるメカニズムを通じてサーバーの状態をチェックします。
OID 制御ユーティリティ（OIDCTL）	Oracle Internet Directory サーバー表にメッセージ・データを置いて OID モニターと通信します。このメッセージ・データには、各 Oracle ディレクトリ・サーバー・インスタンスの実行に必要な構成パラメータが含まれます。

Oracle ディレクトリ・レプリケーション・サーバーは、LDAP を使用して Oracle ディレクトリ（LDAP）サーバー・インスタンスと通信します。データベースと通信するために、すべてのコンポーネントは OCI/Oracle Net Services を使用します。Oracle Directory Manager およびコマンドライン・ツールは、LDAP 上の Oracle ディレクトリ・サーバーと通信します。

Oracle ディレクトリ・サーバー・インスタンス

各 Oracle ディレクトリ・サーバー・インスタンスは、LDAP サーバー・インスタンスとも呼ばれ、図 3-3 のようになります。

図 3-3 Oracle ディレクトリ・サーバー・インスタンス・アーキテクチャ



1 つのインスタンスは 1 つのディスパッチャ・プロセスと 1 つ以上のサーバー・プロセスで構成されています。デフォルトでは、各インスタンスに 1 つのサーバー・プロセスがありますが、この数は増やすことができます。Oracle Internet Directory ディスパッチャおよびサーバー・プロセスでは、複数スレッドを使用して負荷を分散できます。LDAP クライアントは、ポートの LDAP コマンドをリスニングする Oracle Internet Directory リスナー / ディスパッチャ・プロセスに LDAP リクエストを送信します。

Oracle Internet Directory リスナー / ディスパッチャは Oracle ディレクトリ・サーバーにリクエストを送信し、次にこのサーバーがサーバー・プロセスを作成します。サーバー・プロセスは LDAP 操作リクエストを処理し、Oracle データベース・インスタンスに接続してディレクトリ・ストアにアクセスします。ディレクトリ・サーバーは、各操作に対して 1 つのサーバー・プロセスを生成して、クライアント・リクエストを処理します。

マルチ・サーバー・プロセスは、Oracle Internet Directory による複数のプロセッサ・システムの利用を可能にします。作成されるサーバー・プロセス数は、構成パラメータ ORCLSERVERPROCS によって決まります。デフォルトは 1 です。

各サーバー・プロセスからのデータベース接続は、構成パラメータ ORCLMAXCC の値セットに応じて、必要な場合に生成されます。各サーバー・プロセスによって生成されるデータベース接続の数は、ORCLMAXCC + (ORCLMAXCC/2) + 1 に等しくなります。configset0 の ORCLMAXCC のデフォルト値は 2 です。サーバー・プロセスは、Oracle Net Services を介してデータ・サーバーと通信します。Oracle Net Services リスナー / ディスパッチャは、リクエストを Oracle Database にリレーします。

4

Oracle Virtual Directory

Oracle Virtual Directory は LDAPv3 が有効なサービスであり、1 つ以上のエンタープライズ・データ・ソースを単一のディレクトリ・ビューに仮想的に抽象化します。Oracle Virtual Directory は、インフラストラクチャやアプリケーションをわずかな変更で、または変更することなく、LDAP を認識するアプリケーションを多様なディレクトリ環境に統合する機能を提供します。

この章の内容は次のとおりです。

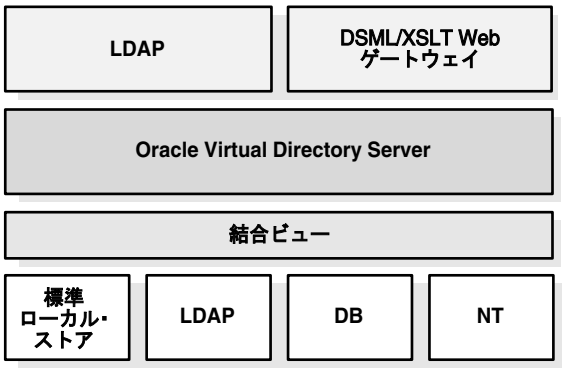
- Oracle Virtual Directory の利点
- Oracle Virtual Directory の機能
- Oracle Virtual Directory の動作

Oracle Virtual Directory の利点

Oracle Virtual Directory には次の利点があります。

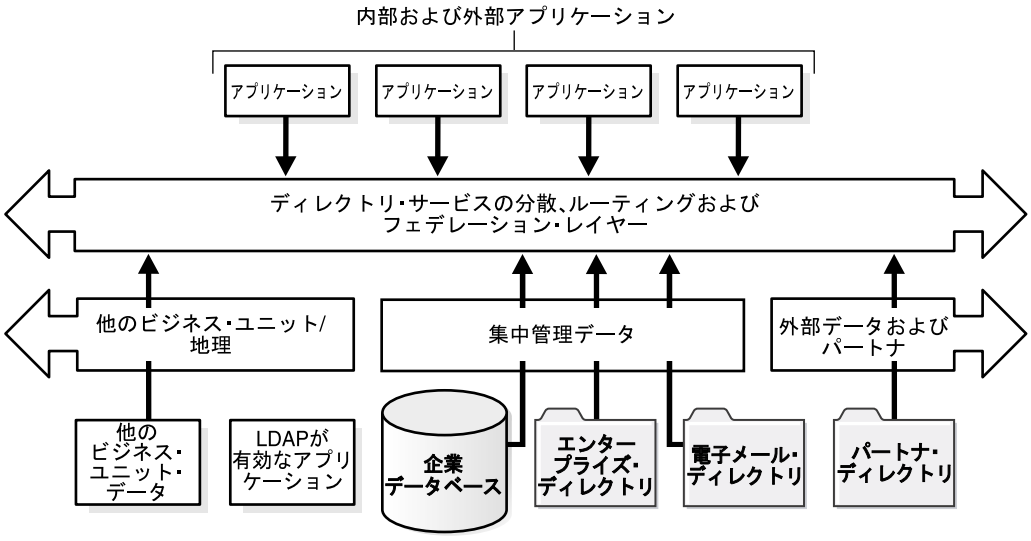
- **複数のディレクトリの統合 :** 図 4-1 に示すように、Oracle Virtual Directory は、アプリケーション・ディレクトリの要件に一致するように既存のディレクトリ・データを変換することができます。Oracle Virtual Directory は、アダプタ・アーキテクチャを介して複数のディレクトリ・ソースと通信します。完全なスキーマおよびネームスペース変換サービスを提供し、プロキシ設定された複数のソースからアプリケーションに提供されたデータに、共通の一貫したフォーマットがあることを保証します。

図 4-1 Oracle Virtual Directory サーバー・アーキテクチャ



- **ディレクトリ・サービスの仮想化および分散の提供 :** 図 4-2 に示すように、エンタープライズには、フォーマット、地理および所有者が異なる多数のディレクトリ・ソースが存在する場合があります。これらの従来のエンタープライズ・ディレクトリには、LDAP が有効なアプリケーション、リレーショナル・データベースおよび電子メールシステムが追加されます。Oracle Virtual Directory は、分散セキュリティ、ルーティング、統合およびデータレベルのフェデレーションなど、実際的な問題を扱うためのディレクトリ・サービス統合レイヤーを提供します。

図 4-2 ディレクトリ・サービスの仮想化と分散



- **管理コストの削減とセキュリティの向上 :** Oracle Virtual Directory は、重複、同期およびレプリケーションによる更新の問題をなくします。データは常に最新であり、一貫しています。

- **エンタープライズ・アプリケーションの迅速な拡張 :** Oracle Virtual Directory では、エンタープライズ・ディレクトリ・アプリケーションおよびレガシー・データをサポートしています。企業リソース、サプライヤおよび顧客は、安全で正確なデータ・アクセスを利用できます。
- **情報へのユビキタス・アクセスの提供 :** ソフトウェアは LDAPv3 に完全に準拠しています。ほとんどのアプリケーションと連携し、多数のディレクトリ製品、ツールおよびアプリケーションとの互換性があります。
- **実装コストの低減 :** Oracle Virtual Directory の入手または実装は、カスタムまたは同期ベースのソリューションよりも費用がかかりません。Oracle Virtual Directory Server は、特定のアプリケーション統合問題を解決するために戦術的にデプロイするか、または全体のディレクトリ・インフラストラクチャ・アーキテクチャに戦略的にデプロイできます。

Oracle Virtual Directory の機能

Oracle Virtual Directory Server には次の機能があります。

- データ・フェデレーション
- データの所有権
- 複数のデータ・アダプタ
- 柔軟性の高いセキュリティ・ドメイン
- セキュア・データ公開
- 高可用性サポート
- アプリケーション統合
- 柔軟性の高いデプロイ
- カスタム・アプリケーション・プログラミング・インタフェース
- 低コスト、高価値のソリューション

データ・フェデレーション

Oracle Virtual Directory Server は、クライアント・リクエストを処理し、それらを 1 つ以上の既存ディレクトリにフォーマット（LDAP、RDBMS など）を問わずに動的に再ルーティングするディレクトリ・ゲートウェイとして機能します。Oracle Virtual Directory Server は、仮想ディレクトリ階層をクライアントに示し、次にそのツリーの階層ブランチを指定した LDAP または RDBMS サーバーに割り当てることで、これを行います。Oracle Virtual Directory Server がディレクトリ間のセキュリティ、プロトコルおよびデータ変換の問題を処理するため、LDAP クライアントは、すべての情報が単一の信頼できるディレクトリ（Oracle Virtual Directory Server）に由来するものとみなします。

データの所有権

非常に見えにくいけれども、最も重要な仮想化の利点の 1 つが、データの所有権です。多くの場合、ディレクトリは特定の目的や目標を持った組織によって設定されます。別の組織が最初の組織の所有するデータにアクセスする場合、データの所有者および管理者に関する疑問が生じます。異なる当事者が情報を共有および使用する場合、問題が生じることがあります。既存データの再使用の価値は誰もが認識していますが、データの再使用は多くの注意点と制御の問題を提起します。データを所有する組織の多くが、データのコピーが別の組織または外部の第三者に渡る際には非常に懸念を抱きます。誰が責任を持つのでしょうか。誰が正確性を保証するのでしょうか。誰がセキュリティと秘匿性を保証するのでしょうか。情報がコピーされた場合、情報を所有する組織は、どのようにして他者による情報の使用方法および管理方法を確認するのでしょうか。

プロキシ・テクノロジを介した仮想化では、データの帰属先（つまり所有者）がデータを保管することで、これらの政治的な問題の多くを解消します。所有者はいつでも、このデータへのアクセスを制限または切断できます。さらに、所有者はこの情報を自由に改訂でき、パートナが常に最新の関連情報を利用していることを確認できます。最も重要な点は、所有者が情報を保管し、その情報の使用を継続的に監視および制御できることです。Oracle Virtual Directory Server は、情報をコピーしないことで、このタイプのソリューションをサポートします。Oracle Virtual Directory Server がアクセスする情報は、リアルタイムに生起します。これにより、コンシューマとプロバイダには、情報が最新であり、正確であり、認可されていることが保証されます。

複数のデータ・アダプタ

Oracle Virtual Directory Server は、アダプタと呼ばれる、無制限の数のディレクトリ・データ接続コンポーネントをサポートします。各アダプタは、特定の親の識別名（DN）で表される特定のネームスペースを管理します。複数のアダプタを組み合せて重複させることにより、カスタマイズされたディレクトリ・ツリーにすることができます。

Oracle Virtual Directory Server は、次のアダプタのタイプをサポートします。

- **LDAP アダプタ :** Microsoft Active Directory、Novell® eDirectory™、Sun™ONE Directory または IBM/Tivoli SecureWay® Directory などの LDAPv2/LDAPv3 ディレクトリ・サーバーにも、Oracle Virtual Directory Server と同様に、プロキシ・アクセスを提供します。LDAP プロキシは、接続プーリングおよび操作レベルのロード・バランシングだけでなく、ネームスペース変換も提供します。
- **データベース・アダプタ :** リレーショナル・データベース・データの LDAP 仮想化を提供します。ほぼすべてのデータ構造を LDAP オブジェクトの階層にマップできます。DB アダプタも、自動スキーマ・マッピングおよび属性値変換を提供します。
- **ローカル・ストア・アダプタ :** Oracle Virtual Directory Server がスタンドアロン・ディレクトリ・サーバーとして稼働できるようにするローカル・ディレクトリ・ストアを提供します。標準アダプタは、シングル・マスター・レプリケーションをサポートし、SLURPD レプリケーションをサポートする他のディレクトリ・サーバー（IBM/Tivoli SecureWay® や Netscape Directory など）と互換性があります。
- **Windows NTLM アダプタ :** Microsoft Windows ドメインの LDAP 仮想化を提供します（注意 : Win32 プラットフォームでのみ可能）。
- **JoinView アダプタ :** 他の Oracle Virtual Directory Server アダプタにあるエントリ間のリアルタイム結合機能を提供します。JoinView アダプタは、顧客固有の Joiner を開発できる拡張可能な API を提供します。JoinView アダプタには、Simple、OneToMany および Shadow という購入直後から使用可能な 3 つの Joiner が付属しています。これらの Joiner は、Oracle Virtual Directory Server Joiner の幅広い機能、および実行可能な異なる結合機能を示します。これらの Joiner の詳細は、このガイドで後述します。

リストされたアダプタ以外に、Oracle Virtual Directory Server は、定義済の API を使用してほぼすべてのデータ・ソースに接続可能なプラグインを使用するカスタム・アダプタの作成機能もサポートしています。たとえば、カスタム・アダプタは、Web サービスを介して使用可能な情報の抽象化に使用できます。

柔軟性の高いセキュリティ・ドメイン

新しいビジネス・アプリケーションを複数のビジネス組織全体に配置する際には、複数のディレクトリ・セキュリティ・インフラストラクチャが存在することから、ID とセキュリティが複雑になる場合があります。Microsoft Active Directory 管理者には周知のとおり、複数の Windows インフラストラクチャ（フォレスト）を持つことは管理およびパフォーマンスの面で利点がありますが、フォレスト間に自動の信頼性がなく、フォレスト内のグローバル・カタログもないという短所があります。

> **関連資料：**『Microsoft TechNet Paper: Design Considerations for Delegation of Administration in Active Directory』（`http://www.microsoft.com/technet/prodtechnol/windows2000serv/technologies/activedirectory/plan/addeladm.mspx`）

Oracle Virtual Directory Server は、アクセス制御のための IETF 標準をすべてサポートするために構築されたファイングレインなアクセス制御を伴う新しい推移的なセキュリティ・コンテキストを作成できます。その一方で、実装のための IETF ドラフト・モデルもサポートしています。Oracle Virtual Directory Server は、プロキシするソース・ディレクトリからのセキュリティ制限と適切に統合するようにも設計されています。これは、管理者に最大限のセキュリティ制御を与えるマルチレイヤーまたはマルチドメイン・セキュリティ概念に帰結します。

Oracle Virtual Directory Server は、多様な認証モデルをサポートします。SSL/TLS（StartTLS を含む）および証明書ベースの認証に加えて、Oracle Virtual Directory Server は、プロキシしたサーバーでサーバー / サーバー認証を使用（それ自体を認証）することができます。または、ユーザー・コンテキストをソース・ディレクトリに渡すことができます。Oracle Virtual Directory Server およびソース・ディレクトリでユーザーコンテキストを提供することで、両方のディレクトリがエンドユーザー・コンテキストのセキュリティ制御を提供できます。

セキュア・データ公開

Oracle Virtual Directory Server には、次のような標準機能があります。

- **SSL/TLS:** Oracle Virtual Directory Server には、セキュアな通信セッションを LDAP クライアントに提供する SSL/TLS 機能があります。これにより、Oracle Virtual Directory Server を信頼できるトランスポート・メカニズムとすることで、セキュリティがより高くなります。
- **トランザクション・クレンジング :** Oracle Virtual Directory Server はプロトコル変換エンジンに基づいています。これは、信頼できるプロキシ設定されたディレクトリ・ソースに転送する前に、すべての問合せの構成を解除し、再コンパイルして妥当性を評価するということを意味します。これにより、ソース LDAP サーバーが不正または未認可の問合せから保護されます。Oracle Virtual Directory Server は次のような項目に制限を設定する機能を提供することで、ガベージ・リクエストのクリーン後に、限られたリソースを不正な攻撃による大量の負荷にさらすことのないように保護できます。
  - 接続当たりの最大操作数
  - 最大同時接続数
  - 特定のサブジェクトに対する指定期間内の最大合計接続数
  - 特定のアドレスに対する指定期間内の最大合計接続数

Oracle Virtual Directory Server は、独自のアクセス制御を実装し、プロキシされた内部ディレクトリ・データへのアクセスをフィルタ処理します。

高可用性サポート

Oracle Virtual Directory は次の高可用性サポートを提供します。

- **フォルト・トレランスおよびフェイルオーバー :** Oracle Virtual Directory Server は 2 つの形式のフォルト・トレランスを提供します。
  - フォルト・トレランス構成内で構成可能
  - フォルト・トレラント・プロキシ・ソースへのフローを管理可能

  単純なコピーまたは構成ファイルの共有でも、複数の Oracle Virtual Directory Server を迅速にデプロイできます。ラウンド・ロビン DNS、リダイレクタまたはクラスタ・テクノロジと組み合せることで、Oracle Virtual Directory Server は完全なフォルト・トレラント・ソリューションを提供します。

  プロキシ設定された各ディレクトリ・ソースについて、特定のソースの複数ホスト（レプリカ）にアクセスするように Oracle Virtual Directory Server を構成できます。ホスト間でインテリジェントにフェイルオーバーし、負荷をホスト間で分散します。フレキシブル構成オプションによって、管理者は特定のレプリカ・ノードにダイレクトされる負荷の割合を制御し、特定のホストが読取り専用レプリカであるか読取り / 書込みサーバー（マスター）であるかを示すことができます。これにより、読取り専用レプリカに書き込もうとすることから生じる不要な参照が避けられます。

- **ロード・バランシング :** Oracle Virtual Directory Server には、負荷を分散し、プロキシ設定された LDAP ディレクトリ・ソース間での障害を管理することのできる強力なロード・バランシング機能が備わっています。

  Oracle Virtual Directory Server の仮想ディレクトリ・ツリー機能では、多くのディレクトリ情報セットを複数の個別ディレクトリ・サーバーに分割することができます。Oracle Virtual Directory Server は、分離したディレクトリ・ツリーのブランチを単純に「接着」することで、分離したデータ・セットを再結合して 1 つの仮想ツリーに戻せます。アプリケーションまたはデータがこれをサポートしていない場合や、個々のディレクトリのディレクトリ・ツリーを重複させる必要がある場合、Oracle Virtual Directory Server はルーティングをサポートします。

  ルーティングとは、最適化された検索ターゲットを決定するため、検索ベースに追加できる検索フィルタを意味します。このモードでは、Oracle Virtual Directory Server は自動的に問合せを適切な仮想ディレクトリ・ソースにルーティングし、数百万のディレクトリ・エンティティに対応することができます。

アプリケーション統合

ディレクトリは、必要とするデータに、アプリケーションが一貫性のあるフォーマットまたはスキーマを持つ形式でアクセスできる場合にのみ役立ちます。しかし、エンタープライズ環境には一般に、異なるスキーマ、ネームスペースおよびデータ設計のディレクトリ・リポジトリが無数に含まれています。既存ディレクトリ情報にセキュアなブリッジを提供することに加えて、Oracle Virtual Directory Server はメタディレクトリに似た、オンザフライでデータを変換する機能も提供します。この機能によって、管理者は異なる組織とディレクトリ・インフラストラクチャ間で検出されるデータの相違を容易に正規化することができます。

結果として仮想化されたディレクトリ・ビューには、アプリケーションが実行する必要のあるディレクトリ情報がすべて含まれ、根本的な変更または統合テクノロジをアプリケーションに構築する必要がありません。

柔軟性の高いデプロイ

Oracle Virtual Directory Server の管理コンソールである Oracle Virtual Directory Manager は、オープン・ソースの Eclipse プラットフォームに基づく、拡張可能な充実した管理環境です。単一の Oracle Virtual Directory Server を単一の環境で使用するか、複数のデータ・センターと複数のデプロイ段階に数十のサーバーが存在する環境で使用するかにかかわらず、デプロイおよび管理を単純化します。

管理は、公開された WSDL 仕様の Web サービス API を介して実行することもできます。これにより、管理者は GUI を順に実行することなく、スクリプトを作成して、またはプログラム的に Oracle Virtual Directory Server にアクセスできます。

カスタム・アプリケーション・プログラミング・インタフェース

Oracle Virtual Directory Server では、3 つの主な領域で製品を拡張できます。これにより、顧客とコンサルタントは Oracle Virtual Directory Server の機能を強化し、特定のビジネス上または技術的な統合ニーズを満たすことができます。

- **Oracle Virtual Directory Server プラグイン :** Oracle Virtual Directory Server は、Java サーブレット・フィルタをモデルとする柔軟性のあるプラグイン・フレームワークを提供します。プラグインは、カスタム・ロジックをトランザクションの一部として提供するため、または単にカスタム・データ・ソースに接続するために使用できます。プラグインはグローバルに、または特定のアダプタのみに挿入できます。プラグインの順序は変更できます。また、プラグインは特定のタイプのトランザクションに分離できます。Oracle Virtual Directory Server の管理ツールには、新しいプラグインの作成ウィザードおよびすぐに開始するために使用できる例が備わっています。
- **カスタムの Joiner:** Oracle Virtual Directory Server JoinView Adapter は、Joiner と呼ばれる拡張可能なモデルに基づいています。異なる動作をするカスタムの Joiner を作成できます。Joiner は、マッピング、結合および前処理 / 後処理 / ハンドラ・イベント処理などの機能を提供します。Joiner は、単純なエントリ・レベルの結合のために作成することも、複雑な結合ロジックまたはトランザクション処理およびロールバック機能のために拡張することもできます。
- **Web ゲートウェイ :** Oracle Virtual Directory Server には、カスタマイズ可能な DSML/XSLT ベースのゲートウェイが含まれます。このゲートウェイは、静的 HTML および XSLT の表示コンテンツをサポートする Apache Web サーバー・モデルに基づく基本的な Web サーバーを提供します。ゲートウェイには、変更操作だけでなく問合せも可能な、ディレクトリが使用可能なインタフェースが含まれます。Web サーバー・セキュリティによって、カスタム委任管理アプリケーションをこのインタフェースに基づいて開発することが可能になります。

低コスト、高価値のソリューション

従来のディレクトリ統合ソリューションでは、稼働するために複雑な LDAP プロビジョニングおよびレプリケーション・スキーム、さらに同期化が必要です。これらの新しいディレクトリは、維持および管理する必要のある、もう 1 つのディレクトリ・ソースとなります。

軽量なリアルタイムのサービスとして、Oracle Virtual Directory Server は、同期および複製ではなく既存のディレクトリ・インフラストラクチャを再使用することで効率を高めます。Oracle Virtual Directory Server は既存のエンタープライズ・ディレクトリの範囲を拡大し、その価値を活用します。

Oracle Virtual Directory の動作

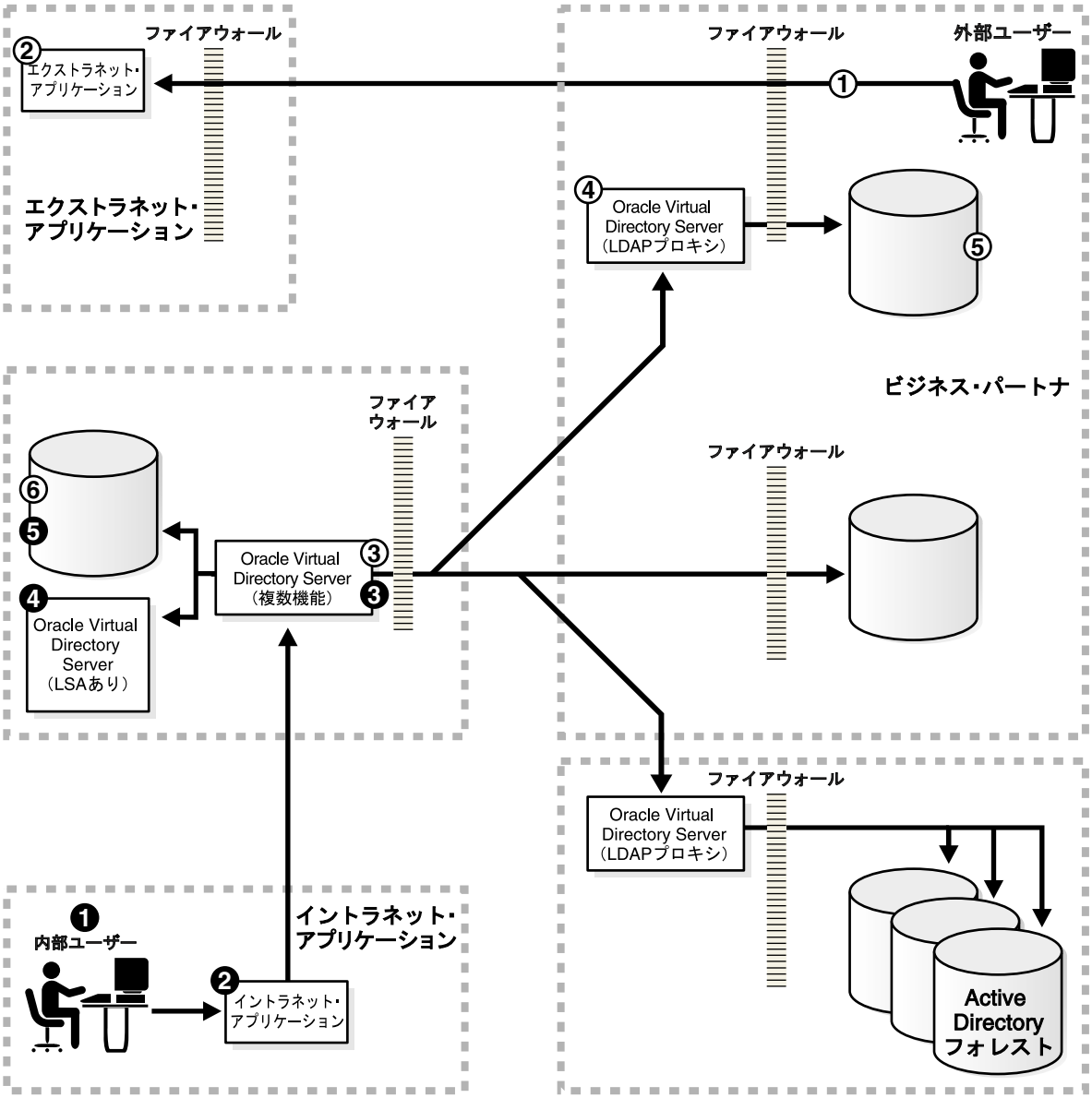
この項の内容は次のとおりです。

- イントラネット ID の例
- エクストラネット ID の例
- シナリオ・レビュー

イントラネット ID の例

図 4-3 では、Oracle Virtual Directory Server が様々な方法で使用されています。左下隅では、内部エンドユーザー（1）がイントラネット・ベースの Web アプリケーション（2）にアクセスしています。

図 4-3 イントラネットおよびエクストラネット・アプリケーションの環境



アクセス中に、アプリケーション（またはポリシー・サービス）はユーザーの ID およびパスワードをリクエストします。次に、アプリケーションまたはポリシー・サービスが Oracle Virtual Directory Server（3）に LDAPv3 を使用してアクセスし、LDAP バインド・リクエストを使用して資格証明を検証します。Oracle Virtual Directory Server が次にこのリクエストをローカル・ディレクトリ・サーバー・ストア（4）にルーティングし、資格証明を検証します。検証時に、Oracle Virtual Directory Server が検証結果をアプリケーション（2）に返します。

この先のリクエストでは、アプリケーションがユーザーのディレクトリ・エントリを Oracle Virtual Directory Server からリクエストし、アプリケーション・プロファイルおよび権限が取得できるようにします。これを行うため、Oracle Virtual Directory Server は透過的な結合を実行し、ローカル・ディレクトリ・サーバー（4）および RDBMS からの情報（5）の両方の属性を結合します。結果が収集されると、Oracle Virtual Directory Server は結果を 1 つの仮想エントリにマージし、イントラネット・アプリケーションに返します。

注意： アプリケーションは、インフラストラクチャの一部としてポリシー・サーバーを含む場合と含まない場合があります。

エクストラネット ID の例

図 4-3 に示す外部 ID の例では、外部組織またはビジネス・パートナ・ユーザー（1）がエクストラネット・ベースの Web アプリケーション（2）にアクセスしています。アプリケーションは LDAPv3 を使用して Oracle Virtual Directory Server（3）に接続し、LDAP バインドを使用してユーザーの資格証明を検証します。

この段階で、Oracle Virtual Directory Server は資格証明が外部ディレクトリにマップされていることを認識します。Oracle Virtual Directory Server は、ビジネス・パートナの外部 Oracle Virtual Directory Server ディレクトリ（4）に SSL 暗号化リンクを使用して接続し、自分の資格証明を使用してビジネス・ユニット間の問合せを検証します。ビジネス・パートナの Oracle Virtual Directory Server が Oracle Virtual Directory Server（3）を検証すると、リクエストが認識され、内部 LDAPv3 ディレクトリ（5）に渡されます。Oracle Virtual Directory Server は適切なビジネス間のアクセス制御を適用し、フィルタされた結果をディレクトリから Oracle Virtual Directory Server に返します。これにより、Oracle Virtual Directory Server はビジネス・パートナ・ユーザーのパスワードを検証してアプリケーション（2）に成功または失敗を返すことができます。

最後に、イントラネット・アプリケーションの例のように、アプリケーションが Oracle Virtual Directory Server にユーザーの追加属性を問い合せることがあります。Oracle Virtual Directory Server は、クライアントが提供するビジネス・パートナ・ディレクトリ（5）からの情報と、企業データベース（6）にローカルに格納されている情報をリンクする結合を実行します。

シナリオ・レビュー

このシナリオは、非常に複雑なシナリオ全体での機能を示しています。Oracle Virtual Directory Server は情報ルーターおよび Joiner として機能し、複数のセキュア・ソースからの情報を仲介して、アプリケーションまたはセキュリティ・インフラストラクチャのニーズを満たします。Oracle Virtual Directory Server は、単一のイントラネット内の情報を結合するだけでなく、ビジネス・パートナからの情報を活用することもできます。これによって、ホスト・ビジネスのディレクトリにおけるプロビジョニングや管理の必要なしにビジネス・パートナがエクストラネット・アプリケーションを使用できるようになるため、これは特に重要です。ビジネス・パートナ・ユーザーは自分のローカル・ディレクトリでリアルタイムに認証されます。

Oracle Virtual Directory Server は、LDAP プロキシ・サーバーとしても重要な役割を果すことができます。Oracle Virtual Directory Server はオプションで、ビジネス・パートナによりディレクトリ・ファイアウォールとして機能するように使用される場合があります。Oracle Virtual Directory Server は、外部からの内部ディレクトリ情報へのアクセスを、適切に認証および認可します。図の右下では、Oracle Virtual Directory Server の独自のルーティング機能が、この情報をクライアントから分離したまま、どのように複数の内部ディレクトリまたは Windows の Active Directory フォレストにルーティング許可するかがわかります。Oracle Virtual Directory Server はファイアウォールとして、認可された外部パーティに表示される情報へのアクセスを制御および制限します。Oracle Virtual Directory Server は仮想ディレクトリ・コンポーネントとして、ビジネス・パートナが使用するデータを公開するため、データを単純化および再構築します。

5

Oracle Directory Integration Platform

この章では、Oracle Directory Integration Platform と、そのコンポーネント、構造および管理ツールを紹介します。この章の内容は次のとおりです。

- Oracle Directory Integration Platform の利点
- Oracle Directory Integration Platform の機能
- Oracle Directory Integration Platform の動作

Oracle Directory Integration Platform の利点

Oracle Directory Integration Platform は、アプリケーションおよびサード・パーティの LDAP ディレクトリを含めたディレクトリを Oracle Internet Directory と統合することで、管理の時間とコストを軽減します。Oracle Directory Integration Platform の利点は次のとおりです。

- **ディレクトリの同期 :** Oracle Human Resources 内の従業員レコードと Oracle Internet Directory 内の従業員レコードとの一貫性を保つことができます。
- **アプリケーションの統合 :** Oracle Directory Integration Platform では、Oracle Internet Directory 内のデータのサブセットに増分変更が適用されるたびに、LDAP が有効な特定のアプリケーション（OracleAS Portal など）に通知できます。
- **サード・パーティの LDAP ディレクトリとの統合 :** Microsoft Active Directory、Sun Java System Directory、Novell eDirectory および OpenLDAP などの様々なディレクトリと統合できます。たとえば、Oracle コンポーネントへのアクセスが Oracle Internet Directory に格納されたデータに依存している Oracle Application Server 環境でも、Microsoft Active Directory を中央のエンタープライズ・ディレクトリとして使用できます。Directory Integration Platform では Microsoft Active Directory のデータと Oracle Internet Directory のデータを同期できるため、このディレクトリのユーザーは Oracle コンポーネントにアクセスできます。

Oracle Directory Integration Platform の機能

Oracle Directory Integration Platform には、次の機能があります。

- **Identity Management Grid Control プラグイン :** Oracle Application Server 10*g*（10.1.4.0.1）の時点で、Oracle Directory Integration Platform を Identity Management Grid Control プラグインで管理することができます。Identity Management Grid Control プラグインは、Oracle Enterprise Manager 10*g* Grid Control の機能を使用します。

  関連資料 :『Oracle Identity Management インフラストラクチャ管理者ガイド』の Identity Management Grid Control プラグインに関する章

- **インストール・オプション :** デフォルトでは、Oracle Directory Integration Platform は Oracle Internet Directory のコンポーネントとしてインストールされます。ただし、スタンドアロンのインストールとして Oracle Directory Integration Platform をインストールすることもできます。次の状況では、Oracle Directory Integration Platform のスタンドアロン・インスタンスをインストールする必要があります。
  - パフォーマンス上の理由から、Oracle Internet Directory を別のホストで実行する必要がある場合
  - 統合および同期する必要のあるアプリケーションが集中的な処理を必要とする場合
  - 高可用性のため、Oracle Directory Integration Platform の複数のインスタンスを実行する必要がある場合
- **ディレクトリの同期 :** ディレクトリの同期には、Oracle Internet Directory と別の LDAP 有効ディレクトリ間でのデータの移動および変換が含まれます。Oracle Internet Directory と他の接続ディレクトリの両方に存在するエントリおよび属性の一貫性が保たれます。

  関連資料 :
  - 『Oracle Identity Management 統合ガイド』
  - ディレクトリ統合アシスタント（`dipassistant`）の情報については、『Oracle Identity Management ユーザー・リファレンス』の Oracle Directory Integration Platform ツールに関する章

- **アプリケーションの統合 :** アプリケーションの統合には、Oracle Internet Directory で発生するエントリへの変更を、それらの変更の追跡に関与するアプリケーションに通知することが含まれます。アプリケーションの統合により、ユーザーまたはグループ情報などのディレクトリ変更を、アプリケーションに通知できます。こうした変更は、アプリケーション・プロセスへのユーザー・アクセスが許可されるかどうか、および使用可能なリソースに影響することがあります。

  関連資料 :

  - 『Oracle Identity Management 統合ガイド』
  - プロビジョニング・サブスクリプション・ツールの情報については、『Oracle Identity Management ユーザー・リファレンス』の Oracle Directory Integration Platform ツールに関する章

- **スケジューリング :** 事前定義済スケジュールに基づく同期または統合プロファイルを処理します。
- **マッピング :** 接続ディレクトリと Oracle Internet Directory 間でデータを変換するためのルールを実行します。
- **データ伝播 :** コネクタを使用して接続ディレクトリとデータを交換します。
- **イベント通知 :** Oracle Internet Directory に格納されたユーザーまたはグループ・データへの関連性のある変更をアプリケーションに通知します。

Oracle Directory Integration Platform の動作

Oracle Directory Integration Platform サーバーは、同期および統合機能を提供する共有サーバー・プロセスです。

この項の内容は次のとおりです。

- 同期
- 統合
- Oracle Directory Integration Platform の例

同期

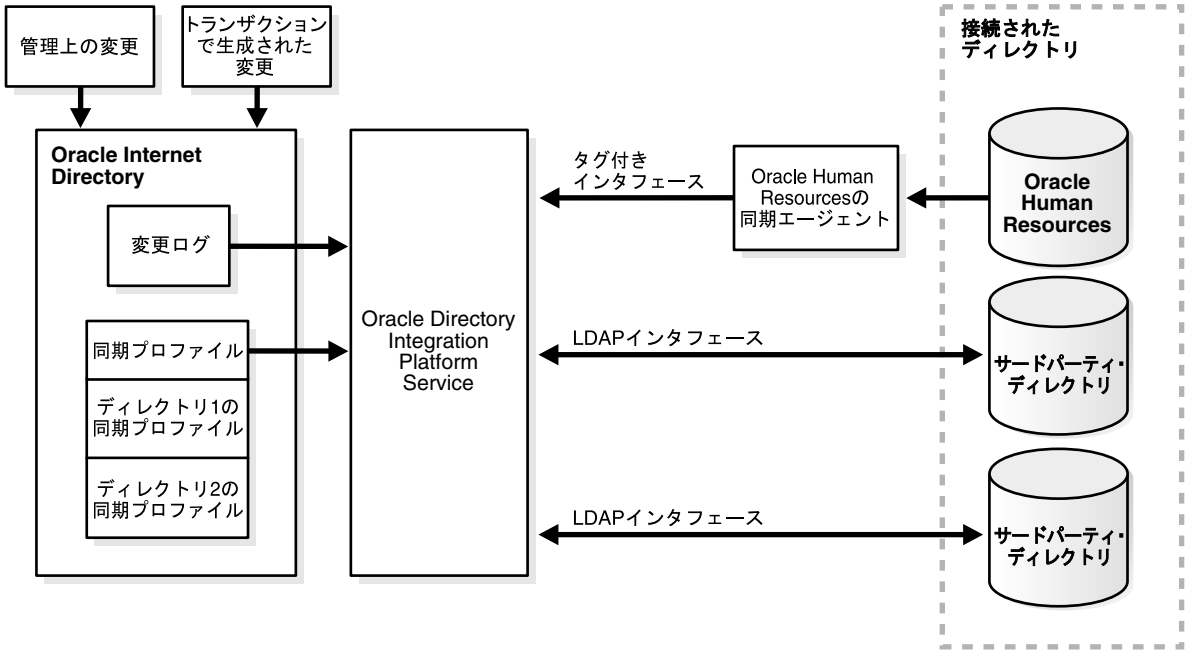
Oracle Application Server コンポーネントでは、Oracle Internet Directory がすべての情報の中央ディレクトリであり、その他のすべてのディレクトリはこれと同期化されます。この同期では、次のことが可能です。

- 一方向 : 一部の接続ディレクトリでは、Oracle Internet Directory に変更を伝えるのみで、変更の受信は行いません。たとえば、従業員情報のプライマリ・リポジトリとしての Oracle Human Resources もこれに該当します。
- 双方向 : Oracle Internet Directory における変更を接続ディレクトリにエクスポートし、接続ディレクトリにおける変更を Oracle Internet Directory にインポートできます。

特定の属性が Oracle Directory Integration Platform Service により対象になる場合と無視される場合があります。たとえば、Oracle Human Resources の従業員バッジ番号の属性が、Oracle Internet Directory の接続ディレクトリまたはクライアント・アプリケーションとは関連性がないことがあります。その同期化は実行しない場合があります。一方で、従業員 ID 番号にはそれらのコンポーネントとの関連性があるため、同期する場合があります。

図 5-1 は、ディレクトリ同期という状況でのサンプル・デプロイにおける、Oracle Directory Integration Platform Service 内のコンポーネント間の相互作用を示しています。

図 5-1 Oracle Directory Integration Platform Service: ディレクトリの同期



すべてのこのような同期アクティビティのトリガーを実行する中心的メカニズムは、Oracle Internet Directory 変更ログです。Oracle Internet Directory を含めた接続ディレクトリへのすべての変更に対して、1 つ以上のエントリを追加します。Oracle Directory Integration Platform Service は次を実行します。

- 変更ログを監視します。
- 1 つ以上の同期プロファイルに対応する変更が発生するたびにアクションをとります。
- 記録された変更に対応する個別プロファイルを持つその他すべての接続ディレクトリに、適切な変更を伝えます。このようなディレクトリには、リレーショナル・データベース、Oracle Human Resources、Microsoft Active Directory、Sun Java System Directory、Novell eDirectory または OpenLDAP などがあります。これらの変更を、接続ディレクトリが必要とするインタフェースおよびフォーマットを使用して伝えます。Directory Integration Platform コネクタを介した同期によって、Oracle Internet Directory では Oracle Internet Directory クライアントが必要とするすべての情報が最新の状態に保たれます。

さらに、Oracle Directory Integration Platform Service により、各統合アプリケーションには、ユーザーまたはグループ情報などの変更が通知されます。これを実行するために、任意の統合プロファイルに含まれる情報に依存します。各プロファイルは次を実行します。

- 適用先のアプリケーションおよび組織を一意に識別
- アプリケーションへの通知が必要なユーザー、グループおよび操作などを指定

プロファイルは、アプリケーションのインストール時にプロビジョニング・サブスクリプション・ツールを使用して作成する必要があります。

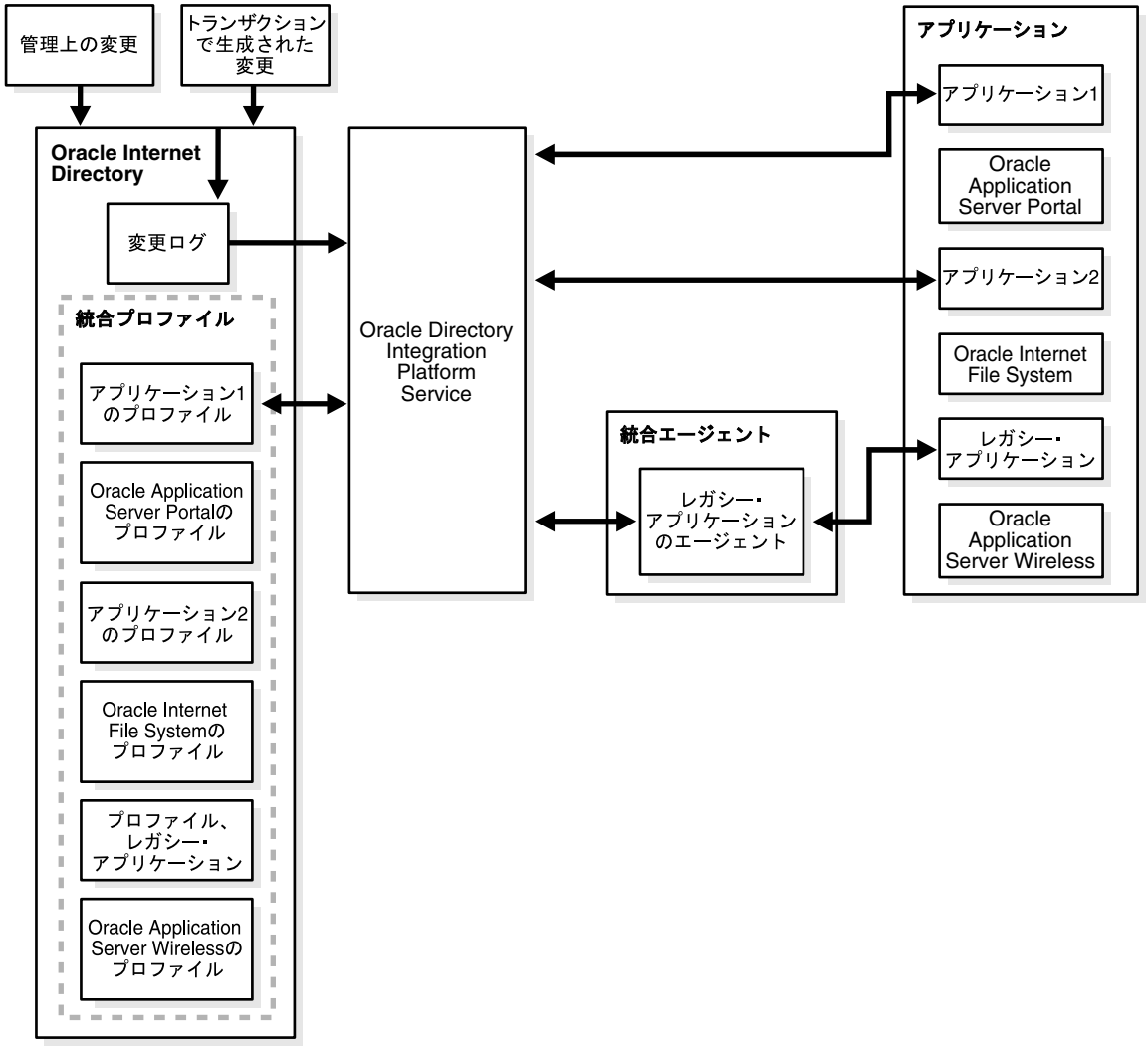
> **関連資料：** プロビジョニング・サブスクリプション・ツールの情報については、『Oracle Identity Management ユーザー・リファレンス』の Oracle Directory Integration Platform ツールに関する章

Oracle Internet Directory 内の変更がアプリケーションの統合プロファイルで指定されているものと一致する場合、Oracle Directory Integration Platform Service は関連データをアプリケーションに送信します。

統合

図 5-2 は、レガシー・アプリケーション用の統合エージェントの特殊例を含めた Oracle Directory Integration Platform Service 環境のコンポーネント間の相互作用を示しています。この図は、Oracle Internet Directory、Oracle Directory Integration Platform Service、統合エージェントおよびアプリケーション間の相互作用を示します。Oracle Internet Directory は、OracleAS Portal、Oracle Internet File System および Oracle9*i*AS Wireless を含む複数のアプリケーションの変更ログと統合プロファイルを含んでいるものとして表示されています。管理およびトランザクション生成の変更は、Oracle Internet Directory に入力されます。Oracle Internet Directory 内の変更ログ・データおよび統合プロファイル・データは、Oracle Directory Integration Platform Service に送信されます。Oracle Directory Integration Platform Service は、データを統合エージェント（特にレガシー・アプリケーションの統合エージェント）に送信します。次に、その情報はレガシー・アプリケーション自体に送信されます。Oracle Directory Integration Platform Service は、様々な他の統合アプリケーションにもデータを送信します。

図 5-2 Oracle Directory Integration Platform Service: アプリケーションの統合



Oracle Directory Integration Platform の例

図 5-3 は、Oracle Directory Integration Platform のサンプル・デプロイを示しています。この図は、Oracle Directory Integration Platform 内のコンポーネント間の関係を示します。左側は Oracle Internet Directory で、構成管理情報およびステータス情報が格納されます。双方向の矢印は、Oracle Internet Directory と管理ツール間の相互の関係を示します。双方向の矢印は、Oracle Internet Directory と Oracle Directory Integration Platform Service 間の関係も示します。矢印が後者から接続ディレクトリの例（Oracle Human Resources、Sun iPlanet および Microsoft Active Directory）を指しています。別の双方向の矢印が、Oracle Directory Integration Platform Service から統合アプリケーションの例（統合アプリケーション 1、OracleAS Portal、統合アプリケーション 2、Oracle Files、レガシー・アプリケーションおよび Oracle Application Server Wireless）を指しています。

図 5-3 Oracle Directory Integration Platform 環境の例

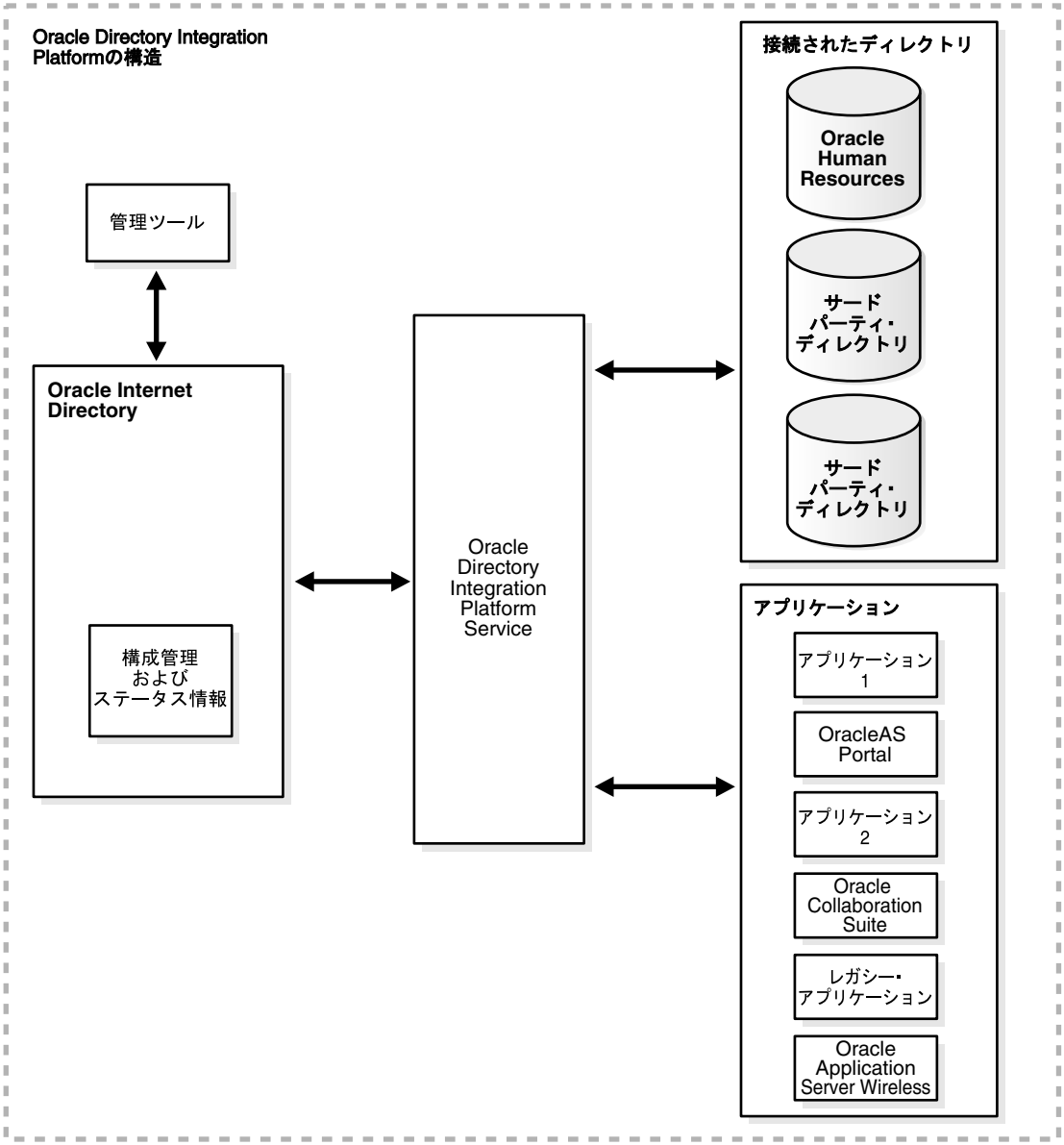


図 5-3 の例では、Oracle Internet Directory は Oracle Directory Integration Platform Service を介して接続ディレクトリと同期化されます。この例では、接続ディレクトリは Oracle Human Resources、Sun Java System Directory および Microsoft Active Directory です。同様に、Oracle Internet Directory 内の変更は、様々なアプリケーションに同じサービスを使用して送信されます。この例では、統合アプリケーションには OracleAS Portal、Oracle Files、Oracle Application Server Wireless、2 つの未指定の統合アプリケーション、およびレガシー・アプリケーションが含まれます。

6

Oracle Access Manager

Oracle Access Manager（以前の Oblix NetPoint および Oracle COREid）は、あらゆる ID 管理およびセキュリティ機能を提供します。これらの機能には、Web シングル・サインオン、ユーザーのセルフサービスおよび自己登録、ワークフロー、監査およびアクセスのレポート作成、ポリシー管理、動的グループ管理および委任管理があります。

Oracle Access Manager は次の 2 つのシステムで構成されます。

- **アクセス・システム :** これを使用して、Web ベースと非 Web ベースのアプリケーション、Web ページおよびその他のリソースへの、シングルおよびマルチドメインのシングル・サインオンを構成します。ユーザー名およびパスワード、証明書を要求するユーザー認証スキームを構成できます。あるいは、カスタム・ログイン・フォームを設計できます。ユーザーは定義されたスキームに基づいて認証されます。認証スキームは、ヘッダー変数、時間または外部ソースから取得したデータなどの条件に基づいています。認証スキームには外部認証プラグインを使用できます。認証および認可アクティビティの監査およびレポートを構成できます。サード・パーティ統合により、スマート・カードおよび他のテクノロジの使用が可能になります。
- **ID システム :** これを使用すると、ユーザーは自分のプロファイルを管理し、自己登録を実行し、グループ・メンバーシップへのサブスクライブと管理を行い、他の組織の資産を管理できます。ID システムには、ロスト・パスワードの取得のためのセルフサービスなど、パスワード・ポリシーの作成および管理のための機能が含まれます。多数のユーザーを管理できるように委任管理を構成することができます。ワークフロー機能により、追加情報および承認のために ID システム機能をルーティングできます。また、ワークフロー・ステップは、外部アプリケーションにコールを送信できます。

この章では、Oracle Access Manager 10*g*（10.1.4.0.1）の概要を説明します。この章の内容は次のとおりです。

- Oracle Access Manager の利点
- Oracle Access Manager アクセス・システムの機能
- Oracle Access Manager アクセス・システムの動作
- Oracle Access Manager ID システムの機能
- Oracle Access Manager ID システムの動作

Oracle Access Manager の利点

Oracle Access Manager では、リソースへの外部アクセスを一方的にブロックできる境界防御モデルから、ビジネス・ルールに基づくセキュリティ・モデルに変更できます。ビジネス・システムおよびデータを、従業員、顧客およびサプライヤに安全に提供できます。

Oracle Access Manager は、企業の機能を従業員、顧客、パートナおよびサプライヤの拡張グループに配信すること、アプリケーション全体で高いレベルのセキュリティを維持すること、ユーザーおよびビジネス・パートナが必要な情報にアクセスできるようにすることを、エンタープライズが容易に行えるようにします。

たとえば、内部ユーザー、サプライヤおよび顧客が一意のデータ・セットへのアクセスを必要とするとします。さらに、全員が見る必要のある共通データもあるとします。Oracle Access Manager を使用すると、ID ベースのポリシーによって正しいレベルのアクセス権を各グループに提供でき、同時に、全員が必要なデータおよびアクセス権を持つデータのみに安全にアクセスできるようにすることができます。

Oracle Access Manager を使用して、外部ビジネス・パートナーに対してオープンな会社ポータルを管理できます。たとえば、顧客が製造原料および機器をオーダーすることのできるポータルでは、ポータルを通じて公開されるすべてのアプリケーションは、アクセス権を付与する 1 つのプラットフォーム（Oracle Access Manager）で保護されます。これらのリソースを保護するアクセス・ポリシーの管理を完全に企業に委任し、IT 部門ではなくビジネス・ユニットがアクセス権を与える顧客、サプライヤおよびパートナを決定するようにできます。これは、顧客、従業員およびサプライヤを含めた多数の人間を管理する必要がある場合でも可能です。

Oracle Access Manager を使用して、異なるタイプの権限を異なるクラスのユーザーに付与することもできます。たとえば医療組織では、次のように、異なるグループが異なる種類のデータを表示できるようにデータを管理できます。

- 医療計画のメンバーは医療情報を表示できます。
- 従業員に医療サービスを提供する企業は医療計画を管理できます。
- 医師と病院は患者の情報を表示できます。

組織は Oracle Access Manager を使用してアプリケーション・アカウントを集約できます。たとえば、金融機関がセルフサービス・ポータルを構成して、顧客がシングル・ログインでオンライン・バンキング、住宅ローン情報および保険などの異なるアカウントにアクセスできるようにできます。

Oracle Access Manager アクセス・システムの機能

アクセス・システムは、アクセス・ポリシーの作成を集中化する一方で、ポリシーの管理および強制の分散化を可能にします。次のタイプのリソースは、アクセス・システムを使用して保護できます。

- ディレクトリ、ページ、Web ベース・アプリケーション、問合せ文字列などの HTTP リソース
- Java Server Pages（JSP）、サーブレット、Enterprise Java Beans（EJB）などの J2EE アプリケーション・サーバー・リソース
- スタンドアロン・プログラム（Java、C、C++）、ERP アプリケーション、CRM アプリケーションなどその他のリソース

この項では、主要なアクセス制御機能の概要を説明します。

- **認証サービス :** Oracle Access Manager で保護されたリソースへのアクセスを試行するユーザーおよびシステムを認証する一般的な手段を提供します。認証サービスでは、基本的なユーザー名とパスワードの認証方式とデジタル証明や SecurID カードなどのより強力な認証方式の両方をサポートします。

  標準認証プラグインを使用することも、認証プラグイン API を使用して独自のカスタム・プラグインを作成することもできます。各カスタム・プラグインは、関連情報を Access Server とプラグイン間で受け渡すための認証インタフェースを実装しています。インタフェース内のメソッドでデータを解析します。

一度ユーザーが認証されると、Oracle Access Manager によってクライアント用のシングル・サインオン（SSO）セッションが作成されます。これにより、ユーザーは他のリソースまたはアプリケーションにアクセスする際に、再度サインオンする必要がなくなります。

- **認可サービス :** 集中化された、一貫性のあるポリシー管理をアプリケーション全体で行う一方で、Web ベースのコンテンツおよびリソースへの粒度の細かいアクセスをユーザーに提供します。機密情報を保護する一方で、ユーザーおよびシステムが必要とする簡単なアクセスを確保できます。

  認可は、ポリシー・ドメインのリソースの保護方法を指定するデフォルト・ルール・セットの一部である認可条件式を含むポリシー・ドメインによって規定されます。アクセス・システムから提供される認可スキームを使用するか、認可プラグイン API を使用して作成されたカスタム・プラグインを含むカスタム・スキームを 1 つ以上構成することができます。『Oracle Access Manager 開発者ガイド』も参照してください。

  認可されると、ユーザーにはリソースへのアクセス権が付与されます。

- **監査サービス :** Oracle Access Manager のイベントに関する柔軟性のある詳細なレポート作成、監査およびロギングを、Crystal Reports 用の即時利用可能なレポートとともに提供します。監査およびログ・ファイルでは、サード・パーティ製品と統合することにより、脅威および侵入の検出、セキュリティ・モニタリングおよびビジネスレベルのレポート作成を実行できます。

- **パーソナライズ・サービス :** HTTP ヘッダー変数およびリダイレクション URL を通じて、他のアプリケーションのパーソナライズを可能にします。Oracle Access Manager がユーザー・リクエストを認証または認可する際、返す URL に HTTP ヘッダー変数を含めることができます。これにはディレクトリ内で認証されたユーザーの ID の下に格納されている任意のユーザー・データを含めることができます。

  下流のアプリケーションはこの情報をデコードして、ユーザー・エクスペリエンスのパーソナライズに使用できます。Oracle Access Manager から返される URL にリダイレクション URL を含めることができます。これにより、ユーザーの ID に合わせた別の Web ページにユーザーを移動することができます。

- **シングル・サインオン :** ユーザーおよびユーザーのグループが、シングル・ログインおよび認証後に複数のアプリケーションにアクセスできるようにします。これにより、複数ログインをなくしユーザーの操作性が向上します。シングル・ドメイン・サーバーにアクセスする必要があるユーザーは、生成された Cookie を Web サイトへの後続のリクエスト用に格納します。複数ドメイン・サーバーにアクセスする必要があるユーザーは、中央の Web ログイン・サーバーで生成された Cookie を格納します。これは、関連付けられた Web システム内でアクセスされたそれぞれのサーバーに対して透過的に発生します。

- **委任アクセス管理 :** 管理タスクを分散できます。アクセス・システムの管理担当者が少ない場合、業務を分担する人々を他に指名する必要がある場合があります。たとえば、失効ユーザーのリストを変更し、構成の詳細およびスキームを追加、変更および削除する機能を委任できます。

アクセス・システムのインストールのサンプルの詳細は、6-4 ページの「Oracle Access Manager アクセス・システムの動作」を参照してください。

Oracle Access Manager アクセス・システムの動作

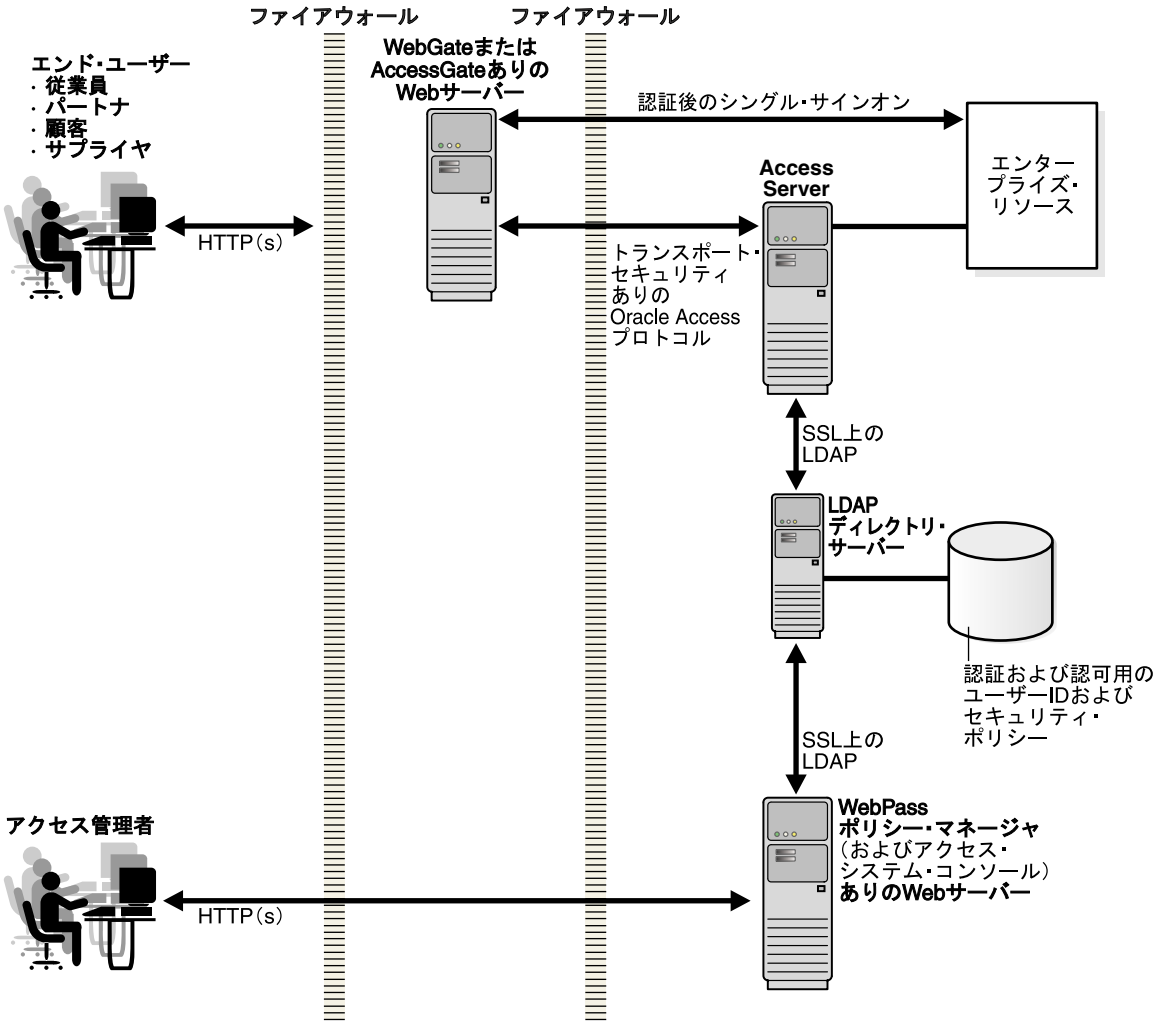
この項の内容は次のとおりです。

- Oracle Access Manager アクセス・システムのコンポーネント
- Policy Manager とアクセス・システム・コンソール
- Access Server
- WebGates および AccessGates
- アクセス・システムの操作

Oracle Access Manager アクセス・システムのコンポーネント

図 6-1 はアクセス・システムの基本コンポーネントを示しています。WebGate は Access Server と通信し、Access Server はディレクトリ・サーバーと通信し、Policy Manager は WebPass を介してディレクトリ・サーバーと通信します。

図 6-1 基本アクセス・システムのインストール



Oracle Access プロトコル（以前の名称は NetPoint または COREid Access プロトコル）は、ユーザー認証および認可中のアクセス・システム・コンポーネント間の通信を可能にします。Web クライアント間（Policy Manager および WebPass、Access Server および WebGate）のトランスポート・セキュリティは、オープン、シンプル（Oracle 提供）および証明書（サード・

パーティ CA）になります。シンプルおよび証明書モードの両方で、Oracle Access Manager コンポーネントは X.509 デジタル証明のみを使用します。

Access Server とディレクトリ・サーバー間（および Policy Manager とディレクトリ・サーバー）のトランスポート・セキュリティは、オープンまたは SSL 有効のいずれかです。すべての Policy Manager とディレクトリ・サーバー間で同じモードを使用する必要があります。

Policy Manager のインストールおよび設定中に、LDAP ディレクトリ・サーバーはポリシー・データ（アクセス・ポリシー・データ）を含めるように更新されます。Policy Manager に定義されたアクセス・ポリシー定義はすべて、ディレクトリ・サーバーに格納されます。

Policy Manager とアクセス・システム・コンソール

ここでは、Policy Manager、アクセス・システム・コンソール、およびそれぞれで使用可能な機能について紹介します。

Policy Manager: Policy Manager はアクセス・システムのログイン・インタフェースを提供し、ディレクトリ・サーバーと通信してポリシー・データを書き込み、OAP 上の Access Server と通信して特定のポリシー変更を行った時に Access Server を更新します。

マスター・アクセス管理者および委任アクセス管理者は、次のことに Policy Manager を使用します。

- 次から構成されるポリシー・ドメインの作成および管理
  - 保護するリソース・タイプ
  - 認証、認可および監査ルール
  - ポリシー（例外）
  - 管理権限
- ポリシー・ドメインへのリソースの追加
- アクセス・ポリシーの強制のテスト

Policy Manager は、（Policy Manager と同じディレクトリ・レベルにインストールされた）WebPass ありの Web サーバー・インスタンスをホストしているマシンにインストールする必要があります。フォルト・トレランスのため、複数の Policy Manager をインストールすることをお薦めします。Policy Manager のインストールの詳細は、『Oracle Access Manager インストレーション・ガイド』を参照してください。

アクセス・システム・コンソール : Policy Manager に含まれています。アクセス・システム・コンソールへのログイン・インタフェースと、任意のマスター管理者、マスター・アクセス管理者および委任アクセス管理者が次の機能オプションを使用できるようにする機能を提供します。

- **システム構成 :** マスター Oracle Access Manager 管理者が、ユーザーをマスター・アクセス管理者にすること、そして委任アクセス管理者およびその権限を追加または削除することを可能にします。マスター・アクセス管理者の職務には、リソース・タイプ、ポリシー・ドメインおよび認証スキームと認可スキームの定義が含まれます。

  管理者は、「システム構成」タブからサーバー設定の表示および変更もできます。たとえば、バグ・レポート用、ユーザー・フィードバック用および企業の Web マスターの電子メールアドレスを指定できます。シングル・サインオンのデフォルトのログアウト URL を変更し、ディレクトリ・サーバーの設定を構成し、キャッシュ設定を表示できます。

- **システム管理 :** マスター管理者は次を管理できます。
  - 診断 : 接続情報を含めた Access Server の詳細を表示します。
  - レポートの管理 : ユーザー・アクセス権限レポートを作成、表示または変更します。
  - 同期レコードの管理 : 指定した日付より前に Policy Manager によって生成された同期レコードをアーカイブまたはパージします。これらのレコードが消費するディレクトリ・サーバー上の領域の管理のため、指定した日付の前に定期的にすべてのレコードをアーカイブまたはパージすることをお薦めします。

- **アクセス・システム構成 :** マスター・アクセス管理者または委任アクセス管理者が次のタスクを完了することを可能にします。
  - AccessGate、Access Server、Access Server クラスタ、ホスト識別子の表示、追加、変更および削除
  - 認証および認可パラメータ、Web リソース・ユーザー権限、共通情報の表示および変更
  - 次を含む共通情報の構成

    共有シークレット : AccessGate または WebGate からブラウザに送信される Cookie を暗号化する暗号化キーを生成します。

    マスター監査ルール : このインストールのデフォルトのマスター監査ルールを作成します。

    リソース・タイプ定義 : リソース・タイプを定義および管理します。

    パスワード・ポリシー・キャッシュのフラッシュ : パスワード・ポリシーを選択し、すべての関連キャッシュをフラッシュするか、ロスト・パスワード管理ポリシーを選択してすべての関連キャッシュをフラッシュします。

    重複アクション : 重複アクション・ヘッダーの処理用のポリシーを選択します。

Access Server

Access Server は、認証および認可で重要な役割を果します。

- 認証には、どの認証方式がリソースに必要かを決定し、ディレクトリ・サーバーから資格証明を収集し、資格証明の検証結果に基づく HTTP レスポンスをアクセス・クライアント（WebGate または AccessGate）に返すことが含まれます。
- 認可には、アクセス情報を収集し、ディレクトリに格納されたポリシー・ドメインおよび認証中に確立された ID に基づくアクセス権を付与することが含まれます。

これらの操作を実行するため、ディレクトリ・サーバーと WebGate の両方と通信する 1 つ以上のスタンドアロン Access Server インスタンスを持つことができます。Access Server インスタンスをインストールする前に、アクセス・システム・コンソールで定義する必要があります。

注意 : フェイルオーバーとロード・バランシングのため、複数の Access Server をインストールすることをお薦めします。

プロセスの概要 : Access Server の機能

1. アクセス・クライアント（WebGate または AccessGate）からリクエストを受信
2. 次を判別するためにディレクトリ・サーバー内の認証、認可および監査ルールを問合せ
   a. リソースが保護されていること（当てはまる場合は、その方法）
   b. ユーザーがすでに認証されていること（ユーザーがまだ認証されていない場合、チャレンジを提供）
   c. ユーザーの資格証明が有効であること
   d. リクエストされたリソースについてユーザーが認可されていること、およびその条件
3. アクセス・クライアントに次のように応答
   a. 認証スキームを送信
   b. 資格証明を検証
   c. ユーザーを認可
   d. 監査

4. セッションを次の方法で管理
   a. WebGate によるユーザー・セッションの終了を支援
   b. タイムアウト発生時の再認証
   c. セッション中のユーザー・アクティビティのトラッキング
   d. ユーザーに対するセッション・タイムアウトの設定

WebGates および AccessGates

Oracle Access Manager のマニュアル全体を通して、AccessGate と WebGate という用語は同義的に使用されます。ただし、次のような注目すべき違いがあります。

- WebGate は、Web リソースへの HTTP リクエストを傍受し、それらを認証および認可のために Access Server に転送する Web サーバー・プラグイン・アクセス・クライアントです。WebGate は、即時使用可能な状態で Oracle Access Manager に同梱されています。
- AccessGate は、ソフトウェア開発者キット（SDK）および Access Manager API を使用して、ユーザーまたはオラクル社が特別に開発するカスタム・アクセス・クライアントです。AccessGate は、ユーザーまたはアプリケーションからの Web および非 Web リソース（非 HTTP）のリクエストを処理するアクセス・クライアントのフォームです。

WebGate はユーザーまたはアプリケーションからリソースへのリクエストを傍受し、認証または認可のために Access Server に転送します。詳細は 6-7 ページの「アクセス・システムの操作」を参照してください。

WebGate をインストールするには、あらかじめアクセス・システム・コンソールで定義し、Access Server または Access Server のクラスタと関連付けておく必要があります。詳細は、『Oracle Access Manager インストレーション・ガイド』を参照してください。

アクセス・システムの操作

次では、アクセス・システムの各コンポーネントが、認証または認可中にどのように連携して動作するかを説明します。図 6-2 も参照してください。

プロセス概要 : ユーザーがアクセスをリクエストする場合

1. WebGate がリクエストを傍受します。

   保護できるサーバーには、特に、Web サーバー、アプリケーション・サーバー、および FTP サーバー（Access Manager SDK を使用）が含まれます。

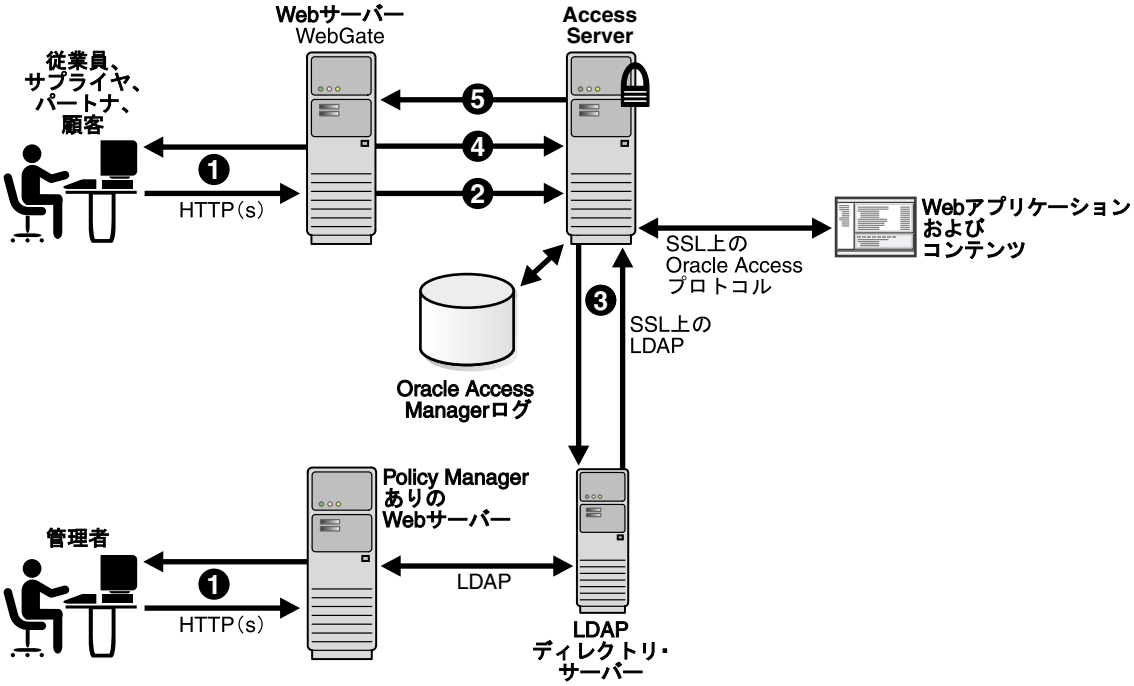
2. WebGate は、リソースが保護されていることおよび保護方法、そしてユーザーが認証されていること（されていない場合、チャレンジがあります）を判別するため、リクエストを Access Server に転送します。

3. Access Server は、ディレクトリ・サーバーでユーザー ID およびパスワードなどの資格証明をチェックし、情報を WebGate に返信し、ユーザーを認証する暗号化された Cookie を生成します。

   Access Server は、ディレクトリ・サーバーに格納された情報を利用し、顧客の指定した ID 識別用の認証方式を使用してユーザーを認証します。Oracle Access Manager の認証では、異なる認証レベルと同様に、任意のサード・パーティ認証方式もサポートします。機密レベルが変化するリソースは、より厳格な認証方式に対応するより高いレベルの認証を要求することで保護できます。

4. 認証に続いて、WebGate は Access Server に適切なセキュリティ・ポリシーを検索し、それらをユーザーの ID と比較し、ユーザーの認可レベルを判断するよう求めます。
   - アクセス・ポリシーが有効な場合、ユーザーは希望するコンテンツまたはアプリケーションへのアクセスを許可されます。
   - ポリシーが正しくない場合、ユーザーはアクセスを拒否され、組織の管理者が定めた別の URL にリダイレクトされます。

図 6-2 基本的なアクセス・システム構成



前述のとおり、Policy Manager はアクセス・システムのログイン・インタフェースを提供し、ディレクトリ・サーバーと通信してポリシー・データを書き込み、特定のポリシー変更を行ったときに OAP 上の Access Server と通信して Access Server を更新します。WebPass は、Policy Manager およびアクセス・システム・コンソールに対する管理者リクエストを傍受および転送します。

Oracle Access Manager ID システムの機能

管理者は、パスワード管理および他の機能を Oracle Access Manager の ID 管理システム上に構築できます。単一の ID 管理システムを使用して、その他のアプリケーションをプライマリ ID システム・コンポーネントに統合できます。これにより、従業員が組織を離れる際に、1 つの ID 変更機能でアクセス・カード、コンピュータ・アカウントおよび給与計算機能をすべて変更できます。カスタマイズおよび XML ベースの統合機能が含まれています。

エンド・ユーザーは、管理者から付与された権限に応じて他のユーザーおよびグループを検索および表示したり、電話番号やパスワードなどの個人情報を変更したり、間取図や資産リストなどの組織情報を表示したりできます。

ID システム管理機能には次のものがあります。

- **ユーザー、グループおよび組織（オブジェクト）の集中管理 :** 様々な人々およびグループに様々なアクセス・ポリシーを提供したり、資産や地図などの組織エンティティを管理したりできます。Oracle Access Manager ID システム内の情報は、ユーザー属性、グループ・メンバーシップまたは組織エンティティとの関連に基づいてアクセス権限を管理するために、Oracle Access Manager Access System で利用できます。
- **動的なロール・ベースの ID 管理 :** ユーザー ID ベースのアクセス権限に基づくキュリティを提供します。たとえば、あるロールには、すべてのユーザー、すべての管理者、または直属の部下のレポートのみを含めることができます。

- **カスタマイズ可能な複数ステップの ID ワークフロー・エンジン :** ID データに関連するビジネス・プロセス、ポリシーおよび承認をマップおよび自動化できます。たとえば、次のワークフローを使用して、ID システム内でビジネス・プロセスをモデル化できます。
  - ユーザー、グループおよび組織の作成、削除および変更
  - ユーザーおよび組織の自己登録の実装
  - グループへのサブスクライブおよびサブスクライブ解除
- **ID 管理のマルチレベル委任 :** ID 管理アクティビティを委任することで、ユーザー数を数百万まで拡大できます。管理者は、付与されている権限のすべてまたは一部を委任できます。また、被委任者が他者に権限を移動できるかどうかを選択できます。委任されたタスクは、権限、ターゲットおよびツリー・パス固有です。
- **セルフ・サービス :** パスワード変更などの組織の機能にセキュアなセルフ・サービス・モデルを実装できます。セルフ・サービス権限を持つユーザーは、自分の情報をワークフローを使用せずに管理できます。
- **自己登録 :** 自己登録ワークフローの開始および処理を通じて、システムに制限付きアクセスを提供します。

  たとえば、ユーザーが自己登録すると、承認のため適切な人々に登録リクエストが転送されるように、自己登録ワークフローを設定できます。承認されると、ユーザーは即時に、ユーザーの ID 属性に基づくすべての適切なリソースへのアクセス権を自動的に付与されます。
- **データ管理レイヤー :** 複数の LDAP 環境、RDBMS データベースおよび分割ディレクトリ・プロファイルをサポートします。この機能は Data Anywhere とも呼ばれ、Oracle Virtual Directory で使用できます。Data Anywhere は、データを RDBMS および LDAP ディレクトリから仮想 LDAP ツリーに集約および統合します。このツリーは Oracle Access Manager ID システムで管理でき、Oracle Access Manager アクセス・システムでの認証および認可のサポートに使用されます。詳細は、『Oracle Access Manager ID および共通管理ガイド』を参照してください。
- **パスワード管理サービス :** 複数のパスワード・ポリシー、パスワード構成に対する制約、構成可能なパスワードの有効期間と通知、強制的なパスワード変更、ロスト・パスワードの管理設定およびパスワード作成 / 変更ルールを指定できます。
- **ユーザー・インタフェースのカスタマイズ :** Oracle Access Manager アプリケーションの外観を変更して操作を制御し、CGI ファイルまたは JavaScript を Oracle Access Manager 画面に接続するために使用できる複数のメソッドを提供します。詳細は、『Oracle Access Manager カスタマイズ・ガイド』を参照してください。
- **ID 統合のための幅広い API:** ブラウザを使用せずに Oracle Access Manager にアクセスして交信し、Oracle Access Manager 内でイベントにトリガーされる機能と実行可能ファイルを実装できます。詳細は、『Oracle Access Manager カスタマイズ・ガイド』を参照してください。

特に記述がない場合、これらの機能および構成方法は『Oracle Access Manager ID および共通管理ガイド』で参照できます。単純なインストールの図については、次の「Oracle Access Manager ID システムの動作」を参照してください。

Oracle Access Manager ID システムの動作

Oracle Access Manager ID システムは、他のアプリケーションおよびシステムがエンタープライズ全体でユーザー ID およびポリシー情報を活用するために必要なインフラストラクチャを提供します。これにより、各アプリケーション用の個別のユーザー ID リポジトリを作成および管理する必要がなくなります。

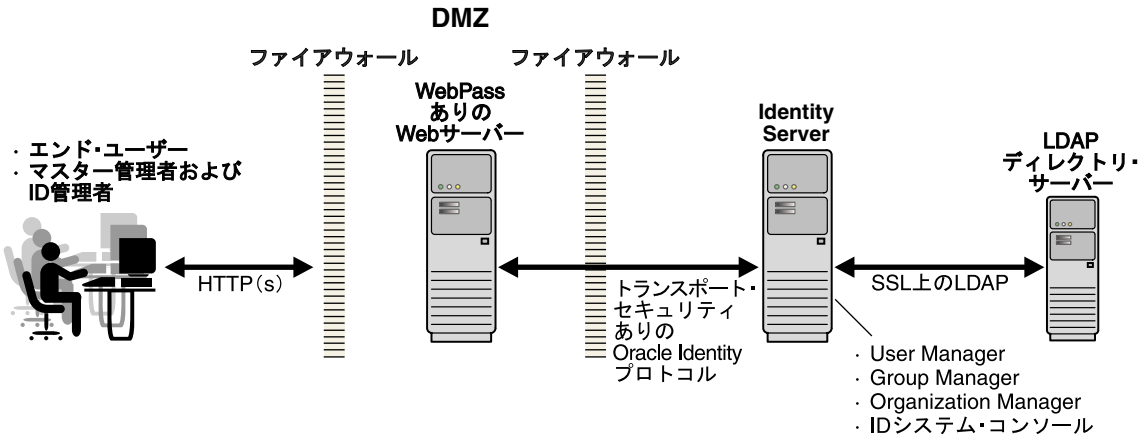
この項の内容は次のとおりです。

- Oracle Access Manager ID システムのコンポーネント
- Identity Server および ID アプリケーション
- WebPass

Oracle Access Manager ID システムのコンポーネント

図 6-3 は、単純な環境における基本の ID システム・コンポーネントと、Oracle Identity Protocol（以前の NetPoint または COREid Identity Protocol）上のコンポーネント間のトランスポート・セキュリティを示しています。エンド・ユーザーと管理者は、ファイアウォールによってコンポーネントから分離されます。WebPass がインストールされた Web サーバーは、DMZ に存在します。Identity Server およびディレクトリ・サーバーは、2 つめのファイアウォールの背後に存在します。

図 6-3 単純な環境におけるコンポーネント



Oracle Identity Protocol は Identity Server と関連 WebPass インスタンスとの通信を簡略化します。Oracle Access Manager Web クライアント（WebPass および Identity Server）間のトランスポート・セキュリティは、オープン、シンプル（Oracle 提供）または証明書（サード・パーティ CA）と指定できます。シンプルおよび証明書モードの両方で、Oracle Access Manager コンポーネントは X.509 デジタル証明のみを使用します。Identity Server とディレクトリ・サーバー間のトランスポート・セキュリティは、オープンまたは SSL 有効のいずれかです。

Oracle Access Manager のインストールおよび設定中に、LDAP ディレクトリ・サーバーが更新され、Oracle Access Manager スキーマとシステム全体のオブジェクト・クラスおよび属性が含まれます。Oracle Access Manager によって、様々なタイプのデータを同じディレクトリ・サーバー・タイプまたは別のディレクトリ・サーバー・タイプに格納できます。次のデータ・タイプがあります。

- **ユーザー・データ :** Oracle Access Manager で管理されるユーザー・ディレクトリ・エントリ
- **構成データ :** ディレクトリに格納され、ID システムで管理される Oracle Access Manager の構成詳細
- **ポリシー・データ :** ディレクトリ・サーバーに格納されている、Policy Manager に定義されたアクセス・ポリシー定義

Oracle Access Manager のインストールおよび設定中に、マスター Oracle Access Manager 管理者（マスター管理者）が割り当てられます。マスター管理者は、デプロイを構成し管理タスクを割り当てる権限を持つスーパーユーザーです。マスター管理者は、システム・コンソールを使用して、マスター ID 管理者およびマスター・アクセス管理者だけではなく追加のマスター管理者も作成できます。たとえば、マスター ID 管理者は他の管理者に認可を委任できます。これにより、数百万のユーザーの管理が可能になります。

ID 情報の管理に加えて、ID システムを使用し、特定のユーザー属性、グループ内のメンバーシップまたは組織との関連に基づいてユーザーのアクセス権限を管理できます。管理者は、権限をワークフローにリンクさせることにより、ユーザーが自己登録した時に、サインオフのため登録リクエストが適切な人々に転送されるようにすることなどができます。

Identity Server および ID アプリケーション

Oracle Access Manager のインストールには、1 つ以上の Identity Server を含める必要があります。Identity Server を使用して、ユーザー、グループ、組織およびその他のオブジェクトに関する ID 情報を管理します。インストールには、1 つ以上の Identity Server インスタンスを含めることができます。Identity Server では、主に次の 3 つの機能を実行します。

- ネットワーク接続全体の LDAP ディレクトリ・サーバーへの読取りおよび書込み
- ユーザー情報をディレクトリ・サーバーへ格納、およびディレクトリを最新状態に維持
- ユーザー、グループおよび組織の ID に関するすべてのリクエストを処理

Identity Server の各インスタンスは、6-12 ページの「WebPass」で述べたように、WebPass プラグインを介して Web サーバーと通信します。

Identity Server は、Web ベースのインタフェースを通じてアクセスできる次の ID アプリケーションを提供します。すべてにレポート作成機能があります。

- **User Manager:** 個別のネットワーク・ユーザーに関連するすべての ID 情報を完全に管理できます。

  User Manager によって、管理者はユーザー ID を追加、変更、非アクティブ化および削除できます。さらに、管理者は User Manager を使用して、ユーザーにディレクトリ・プロファイル（および代替権限）に基づくアクセス権限や、表示および監視のリクエストも提供できます。

  通常、エンド・ユーザーは、他のユーザーを表示し、自分の情報を変更できます。表示可能なユーザーと変更可能な ID 情報は、マスター管理者に付与された権限によって異なります。

- **Group Manager:** 認可された人が静的、動的またはネストされたグループを作成、管理および削除するか、グループ管理を委任できます。

  管理者はグループを作成または削除でき、ユーザーがグループからサブスクライブおよびサブスクライブ解除できるようにします。

  エンド・ユーザーは、グループを表示し、グループ内のメンバーシップにサブスクライブできます。表示可能なグループおよびサブスクリプション権限は、マスター管理者によって付与されます。

- **Organization Manager:** 組織全体で継続中の変更を管理するためのシステム・ルール、アクセス権限およびワークフローの管理に役立ちます。

  管理者は、User Manager または Group Manager に属さない組織および他のオブジェクト（間取図や資産など）を作成および削除できます。

  エンド・ユーザーは、組織のエンティティを表示できます。表示可能な組織のエンティティは、マスター管理者に付与された権限によって異なります。

- **ID システム・コンソール :** 管理者を作成し、管理タスクの委任権限を割り当てるために使用する、Web ベースの管理および構成を提供します。ID システム・コンソールのタブから特定の ID 管理機能にアクセスできます。

WebPass

WebPass は、Web サーバーと Identity Server 間で情報をやりとりする Oracle Access Manager の Web サーバー・プラグインです。Identity Server は、構成に応じて XML ファイルまたは HTML ファイルのいずれかとしてリクエストを処理します。

WebPass は複数の Identity Server と通信できます。Identity Server と通信する各 Web サーバー・インスタンスは、WebPass で構成する必要があります。Oracle Access Manager インストールでは次が必要です。

- 少なくとも 1 つの WebPass を Web サーバーにインストールし、少なくとも 1 つの Identity Server と通信するように構成する必要があります。
- Oracle Access Manager の Policy Manager をホストしている各マシン上に WebPass が必要です。

Identity Server および WebPass のインストール後、Identity Server および WebPass が通信できるように、ID システムの初期設定を完了する必要があります。

プロセスの概要 : WebPass の機能

1. WebPass はユーザー・リクエストを受信し、URL をメッセージの書式にマップします。
2. WebPass はリクエストを Identity Server に転送します。
3. WebPass は情報を Identity Server から受信し、ユーザーのブラウザに返します。

7

Oracle Identity Federation

シングル・サインオン（SSO）は冗長ログインの必要性を減らすことができるため幅広く採用されていますが、フェデレーテッド環境で運営している企業にとっては単なる SSO では不十分です。フェデレーテッド環境とは、サービスをビジネス・パートナと共有する一方で、そうしたサービスを不正なアクセスから保護する環境です。

Oracle Identity Federation は、マルチドメイン ID ネットワークにおけるシングル・サインオンおよび認証を可能にする、スタンドアロンで自己完結型のフェデレーション・サーバーです。Oracle Identity Federation は、Liberty ID-FF および SAML プロトコルなど複数のフェデレーテッド ID プロトコルをサポートします。これにより、他の Oracle Identity Management 製品がソリューション・セットに実装されているかどうかにかかわらず、異機種環境にあるユーザーおよびビジネス上で連携しているユーザーを結びつけることができます。

この章では、フェデレーテッド ID 管理の概要を示し、Oracle Identity Federation の主な機能と利点を説明します。この章の内容は次のとおりです。

- Oracle Identity Federation の利点
- Oracle Identity Federation の機能
- Oracle Identity Federation の動作

Oracle Identity Federation の利点

フェデレーテッド環境では、企業が ID 情報をそれぞれのセキュリティ・ドメイン全体で共有するメカニズムが提供されるため、ビジネス・パートナが ID 管理レルムにおいて統合を実現することができます。

フェデレーテッド ID 管理は、自社の境界を越えた外部にあるコンピューティング・リソースやサービスにアクセスする必要がますます高まるユーザーに応える、SSO パラダイムにおける進化です。フェデレーテッド環境では、そうしたサービスを提供するエンタープライズは、個人またはその他のエンティティの ID 情報をユーザーのホーム組織またはセキュリティ・ドメインから確実に取得できます。これには次の 2 つの利点があります。

1. エンド・ユーザーは、ビジネスが実行されている各エンティティにアクセスするためにログイン資格証明を入力する必要がありません。また、複数のログイン / パスワードを記憶して管理する必要もありません。（ただし、アカウントをリンクできるように、各サイトのアカウントは必要です。）
2. エンタープライズは、パートナ組織での既知のユーザー ID を管理するために追加のアカウントを作成する必要がありません。前述の例では、サービス・プロバイダは、クライアントの医療組織が内部で維持している従業員データを利用できます。

Oracle Identity Federation の機能

Oracle Identity Federation の主な機能は次のとおりです。

- **クロスサイト機能 :** ID プロバイダおよびサービス・プロバイダの両方が含まれる環境に、クロスサイトのアクセスおよび認証機能を実装できます。
- **構成機能 :** 外部サイトを構成、有効化および無効化できます。
- **シングル・サインオン :** ユーザーがシングル・サインオンを使用して、対象サイトのアプリケーションにアクセスできます。
- **フェデレーション・プロトコルのサポート :** Oracle Identity Federation では次の優れたフェデレーション・プロトコルをサポートしています。
  - Liberty ID-FF 1.1
  - Liberty ID-FF 1.2
  - SAML 1.0
  - SAML 2.0（SAML 2.0 レスポンダを含む）
  - WS-Federation
- **その他の製品との統合 :** Oracle Identity Federation は Oracle Internet Directory、Oracle Access Manager および OracleAS Single Sign-On と統合されています。また、次のものもサポートされています。
  - Oracle Access Manager や CA eTrust SiteMinder など、各種の認証エンジン
  - Microsoft Active Directory や Sun Java System Directory Server などの LDAP ストアを含むユーザー・データ・リポジトリ
  - リレーショナル・データベース
- プロトコル間でのシングル・サインオンおよびサインアウトのサポート。
- **アフィリエーション :** Oracle Identity Federation ではアフィリエーションをサポートします。これにより、サービス・プロバイダにフェデレーション情報の共有を許可することで、フェデレーションの数を削減します。
- **証明書の検証 :** Oracle Internet Directory では X.509 証明書の検証をサポートしています。

Oracle Identity Federation の動作

この項の内容は次のとおりです。

- フェデレーション・ユースケース
- フェデレーション・イベント・フロー
- フェデレーション・プロトコル・プロファイル
- フェデレーション・アーキテクチャ

フェデレーション・ユースケース

この項のユースケースでは、複数のアプリケーションに対する 1 回の認証で、フェデレーションがシームレスなエンドユーザー・エクスペリエンスを提供する方法を説明します。

ユースケース 1: パートナ・サイトへのシングル・サインオン

図 7-1 従業員ポータルからパートナへのシングル・サインオン

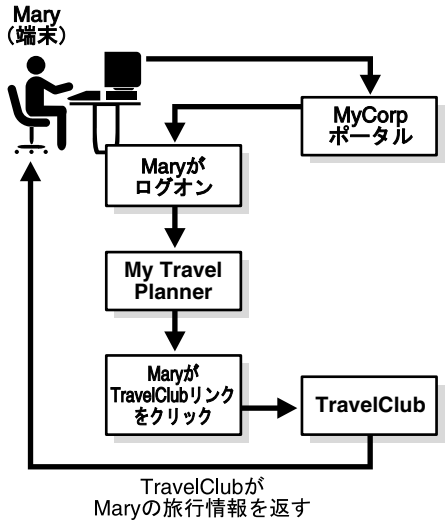


図 7-1 は、MyCorp の従業員である Mary が次の出張の計画を立てようとしている状況を説明しています。彼女はこれを次のステップで、シームレスな単一セッションで実行できます。

1. Mary は自分の端末から、自社の MyCorp 従業員ポータルにアクセスします。
2. ポータルは WS-Federation に対応しており、シングル・サインオン・ダイアログを表示します。
3. Mary がサインオンすると、ポータルは彼女の情報を基にパーソナライズしたページを返します。
4. Mary はポータル内の TravelClub のリンクをクリックし、出張の計画を開始します。TravelClub は、MyCorp の従業員に各種の旅行サービスを提供するパートナ組織です。Mary はすでに TravelClub とのフェデレーテッド・リレーションシップを確立しています。
5. Mary が自分のアカウントにアクセスするには認証が必要であり、TravelClub は MyCorp に認証をリクエストします。MyCorp は必要な ID 情報を旅行サイトに返します。Mary は自動的に TravelClub サイトで認証されます。TravelClub は Mary の旅行アカウント情報のページを返します。
6. 作業の終了後、Mary は MyCorp ホームページのシングル・グローバル・ログアウト機能を使用し、TravelClub と MyCorp の両方のセッションからログアウトできます。

この方法では、Mary は自社の Web サイトで一度認証を受けると、別のサイトに接続して必要なタスクを実行できます。2 つめのサイトでは、追加認証を必要としません。

ユースケース 2: パートナ・サイトでの新規フェデレーテッド・アカウント

図 7-2 フェデレーテッド・アカウントの作成

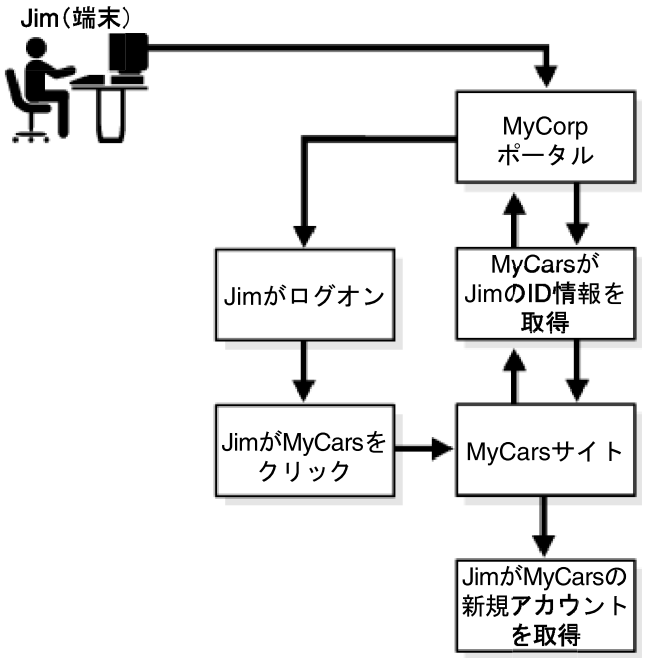


図 7-2 は、MyCorp の別の従業員である Jim が、MyCars で新規アカウントを設定しようとするユースケースを示しています。MyCars は MyCorp の従業員に格安の自動車修理サービスを提供する外部サイトです。手順は次のとおりです。

1. Jim は MyCorp ポータルにサインオンします。
2. ポータル内での作業後に、Jim はポータルの Vendors ページに移動して自動車サービスを探すことにし、MyCars のリンクをクリックします。
3. MyCars に新規アカウントを設定するための情報が要求されます。Jim が同意すると、MyCars は MyCorp と通信して Jim の ID に関連する情報を取得します。
4. これで、MyCars に Jim のアカウントができます。彼は、前述のユースケースで概略を説明したものと同様の方法でここにアクセスできます。

これらのユースケースは、フェデレーテッド・シングル・サインオンとフェデレーテッド ID 管理の典型的な適用例です。次の項では、フェデレーション・テクノロジの主な概念と、Oracle Identity Federation での利用方法をより詳細に説明します。

フェデレーション・イベント・フロー

この項では、フェデレーテッドな相互作用における典型的なメッセージ・フローを説明します。

図 7-1 のユースケースを詳細に説明するため、Mary がすでに mycorp.com で認証されており、彼女がログインしていない travelclub.com に移動するとします。travelclub.com では、Mary がローカル・アカウントにアクセスするために認証を必要とし、SAML 2.0 メッセージとともに Mary を mycorp.com にリダイレクトして、travelclub.com に対するシングル・サインオンをリクエストします。Mary がすでに ID プロバイダにログインしているため、mycorp.com は Mary のアカウントとフェデレーション・データを取得し、彼女を travelclub.com に再度リダイレクトします。travelclub.com はリダイレクトで提供されたプロバイダ識別子 `mycorp.com` とユーザー識別子 `xyz123` を使用して、Mary のフェデレーション・データと彼女のローカル・アカウントを一意に取得できます。

フェデレーション・プロトコル・プロファイル

ID プロバイダおよびサービス・プロバイダは、SAML や Liberty ID-FF などのフェデレーション・プロトコルに定義されたプロファイルおよびサービスを使用してアサーションを交換します。アサーション機能には次のものがあります。

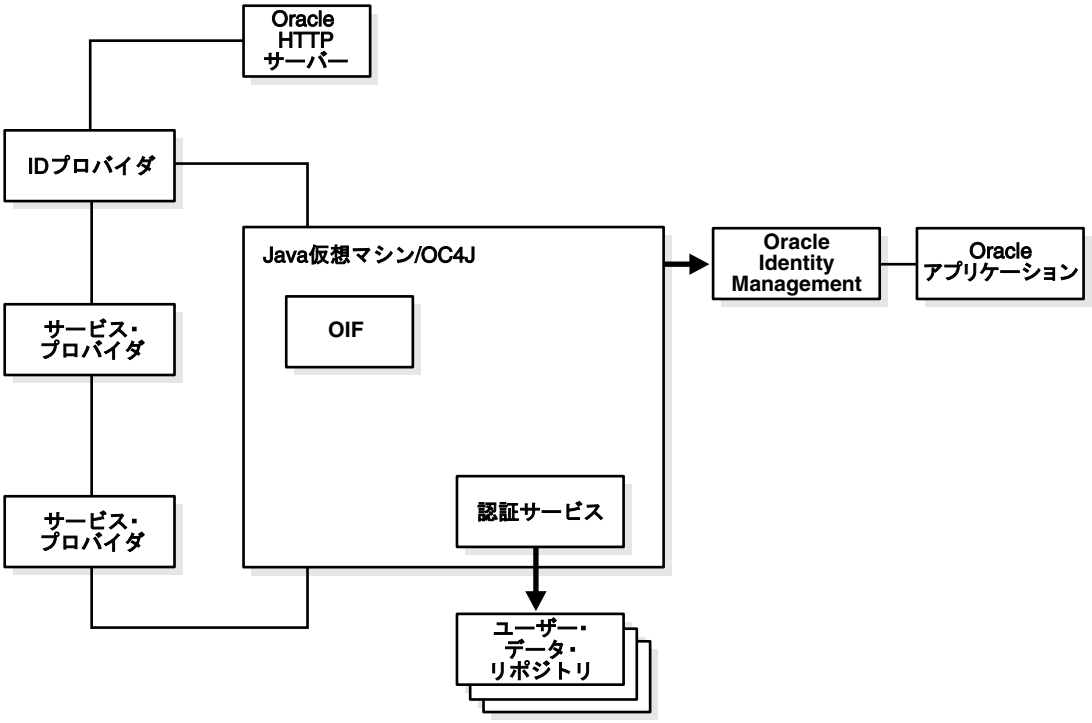
- セキュアな接続の確立
- それらの接続全体に認証データを伝達
- 他の SAML ドメインからアサーションを受信および解析

プロファイルは ID プロバイダ（IdP）とサービス・プロバイダ（SP）間でアサーションを転送するために必要な交換のタイプを示します。この項では、Oracle Identity Federation で使用可能なアサーション・プロファイルを詳しく説明します。

フェデレーション・アーキテクチャ

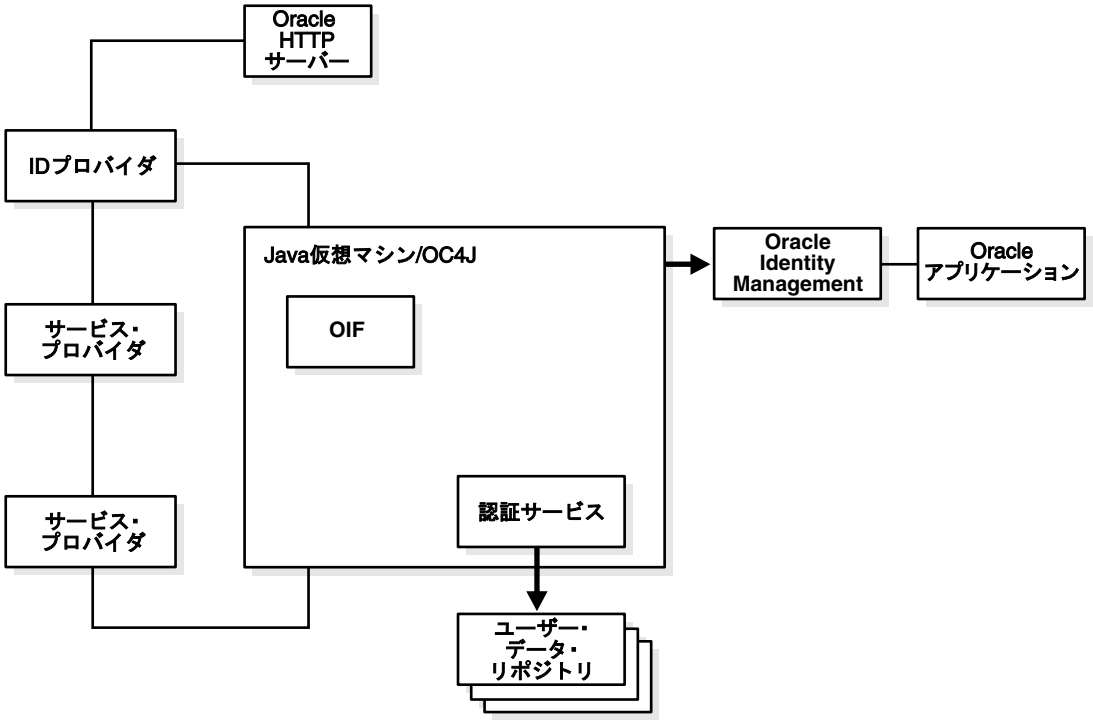
図 7-3 は、Oracle Identity Federation（OIF）のアーキテクチャおよびその他のフェデレーション・コンポーネントへの関係を示します。ここで Oracle Identity Federation は他の ID プロバイダおよびサービス・プロバイダを含むトラスト・サークルのメンバーであり、これらは追加の Oracle Identity Federation インスタンスまたはサード・パーティのプロバイダである場合があります。

図 7-3 Oracle Identity Federation



Oracle Identity Federation には自己完結型で軽量の認証サービスが含まれます。このサービス（図 7-4）は IdMBridge に基づいており、WAR（Web Application aRchive）ファイルに Oracle Identity Federation とともにデプロイされ、サーバーと同じ Java 仮想マシンで稼働します。

図 7-4 Oracle Identity Federation のサード・パーティ統合



Oracle Identity Federation は、各種の認証メカニズムおよびユーザー・データ・リポジトリと通信できます。

1. Oracle Identity Management

   Oracle Identity Federation の認証サービスを構成して、OracleAS Single Sign-On または Oracle Access Manager で保護された次のリソースへのシングル・サインオン・アクセスを有効にすることができます。

   - Oracle Collaboration Suite
   - Oracle E-Business Suite
   - PeopleSoft モジュール
   - その他

   Oracle Application Server Single Sign-On（Oracle Internet Directory ユーザー・リポジトリを使用）または Oracle Access Manager（様々なリポジトリを使用）の他にも、OracleAS Single Sign-On がサード・パーティのアクセス管理ソリューションとの連携のためにデプロイされている場合には、この構成でこれらのソリューションも利用できます。

注意： Oracle Identity Federation と OracleAS Single Sign-On の両方でリソースを保護する環境では、いずれのコンポーネントも、ユーザーが保護されたリソースへのアクセスをリクエストした際に認証メカニズムとなるよう構成できます。たとえば、Oracle Identity Federation から OracleAS Single Sign-On へ認証リクエストを転送できます。また、OracleAS Single Sign-On から Oracle Identity Federation へ、適切な ID プロバイダを検索するようにリクエストできます。詳細は、『Oracle Application Server Single Sign-On 管理者ガイド』を参照してください。

同様に、Oracle Identity Federation と Oracle Access Manager の両方を含む環境でも同様の機能を提供します。

---

2. データ・ストア

次にアクセスするように Oracle Identity Federation を構成できます。

- LDAP ディレクトリ
- RDBMS データベース
- Oracle Access Manager
- eTrust SiteMinder

8

OracleAS Single Sign-On

Oracle Application Server（OracleAS）Single Sign-On を使用すると、1 つのユーザー名、パスワードおよびレルム ID（オプション）を使用して、他の Web アプリケーションと同様に、OracleAS のすべての機能にログインできます。

Oracle コンポーネントは、ログイン機能を OracleAS Single Sign-On サーバーに委任します。ユーザーが最初に Oracle コンポーネントにログインすると、コンポーネントがログインを OracleAS Single Sign-On にリダイレクトします。OracleAS Single Sign-On サーバーは、Oracle Internet Directory に格納された資格証明に照らし、ユーザーが入力した資格証明を検証してユーザーを認証します。ユーザーの認証後および残りのセッションで、OracleAS Single Sign-On サーバーは、ユーザーが使用を求めているコンポーネントおよび使用を認可されているコンポーネントのすべてに対し、アクセス権を付与します。

> **関連資料：** OracleAS Single Sign-On の情報については、『Oracle Application Server Single Sign-On 管理者ガイド』を参照してください。

この章の内容は次のとおりです。

- Oracle Application Server Single Sign-On の利点
- Oracle Application Server Single Sign-On の機能
- OracleAS Single Sign-On の動作

Oracle Application Server Single Sign-On の利点

OracleAS Single Sign-On には次の利点があります。

- **管理コストの削減 :** Single Sign-On Server により、複数のアカウントおよびパスワードをサポートする必要がなくなります。
- **便利なログイン :** ユーザーは、アクセスする各アプリケーションに対し、個別のユーザー名およびパスワードを維持する必要がありません。
- **セキュリティの向上 :** パスワードが一度のみ要求される場合には、ユーザーが単純かつ簡単にわかるパスワードを使用したり、こうしたパスワードを書き留めたりする可能性が低くなります。

Oracle Application Server Single Sign-On の機能

Oracle Application Server Single Sign-On は次の機能を提供します。

- **フェデレーテッド認証 :** Oracle Application Server Single Sign-On を使用してフェデレーテッド認証を実装できます。フェデレーテッド・シングル・サインオンでは、ユーザーに対して異なる会社の Web サイトにある情報へのアクセスを許可しますが、それらのサイトの 1 つのみで認証を行います。Oracle Application Server Single Sign-On を、製品で保護されているリソースにアクセスしようとするユーザーに対する認証メカニズムになるように構成できます。
- **Identity Management Grid Control プラグイン :** Oracle Application Server 10*g*（10.1.4.0.1）の時点で、Oracle Directory Integration Platform を Identity Management Grid Control プラグインで管理することができます。Identity Management Grid Control プラグインは、Oracle Enterprise Manager 10*g* Grid Control の機能を使用します。

  関連資料 :『Oracle Identity Management インフラストラクチャ管理者ガイド』の Identity Management Grid Control プラグインに関する項

- **グローバル・ユーザーの非アクティブのタイムアウト :** グローバル・ユーザーの非アクティブのタイムアウトは、アイドル状態が事前に構成した時間続いた場合に、アプリケーションで強制的な再認証を可能にする機能です。このタイムアウトは、シングル・サインアウトのセッション・タイムアウトよりも短い非アクティブのタイムアウトが必要な、機密事項を扱うアプリケーションに役立つ機能です。
- **ワイヤレス・オプション :** 携帯情報端末、携帯電話および音声認識システムなどのモバイル機器を使用して OracleAS アプリケーションにアクセスできます。OracleAS のインストール時にワイヤレス・オプションを選択すると、モバイル機器用のゲートウェイである Portal-to-Go が自動的に Single Sign-On Server に登録されます。

  関連資料 :

  - 『Oracle Application Server Wireless 管理者ガイド』
  - 『Oracle Application Server Wireless 開発者ガイド』

  Oracle Application Server Wireless の詳細は、前述のマニュアルを参照してください。

- **シングル・サインオフ :** シングル・サインオン・セッションを終了して、すべてのアクティブなパートナ・アプリケーションから同時にログアウトできます。パートナ・アプリケーションで**「ログアウト」**をクリックすると、シングル・サインオフ・ページに移動し、このページでログアウトが発生します。
- **パスワードの変更 :** パスワードの有効期限が近づいた場合に、Oracle Application Server Single Sign-On はパスワードの変更画面を表示します。その他の状況でパスワードを変更またはリセットする場合、管理者以外のユーザーは Oracle Delegated Administration Services を使用できます。

OracleAS Single Sign-On の動作

この項の内容は次のとおりです。

- シングル・サインオン・システムのコンポーネント
- Single Sign-On Server へのアクセス
- パートナ・アプリケーションへのアクセス
- 外部アプリケーションへのアクセス

シングル・サインオン・システムのコンポーネント

OracleAS Single Sign-On は複数のコンポーネントと交信します。次のものが含まれます。

- **Single Sign-On Server:** Single Sign-On Server は、ユーザーが安全に経費報告書、メール、および給付金などのシングル・サインオン・アプリケーションにログインできるようにするプログラム・ロジックで構成されます。Single Sign-On Server のプログラム・ロジックは、Oracle Application Server データベース、Oracle HTTP Server および OC4J サーバーに存在します。
- **パートナ・アプリケーション :** OracleAS Single Sign-On サーバーに認証機能を委任する Oracle Application Server アプリケーションまたは Oracle 以外のアプリケーション。このタイプのアプリケーションでは、mod_osso という認証モジュールからのヘッダーを受け入れることにより、ユーザーの再認証が行われません。パートナ・アプリケーションの例には、OracleAS Portal、OracleAS Discoverer および Oracle Delegated Administration Services が含まれます。
- **外部アプリケーション :** アプリケーションのユーザー名およびパスワードを求める HTML ログイン・フォームを表示する、Oracle 以外のアプリケーション。最初のログイン時に、ユーザーは**「このアプリケーションのログイン情報を保存する」**チェック・ボックスを選択できます。後続のログインで、サーバーはシングル・サインオン・ユーザー名を使用してアプリケーション名およびパスワードを検索および取得し、ユーザーの認証を必要とせずにユーザーをログインさせます。
- **mod_osso:** OracleAS アプリケーションに認証を与える Oracle HTTP Server モジュール。mod_osso は Oracle HTTP リスナーのみで動作します。OracleAS SSO プラグインを使用して、Sun One および IIS などのサード・パーティ・リスナーで動作するアプリケーションを保護することができます。

  関連資料 : mod_osso の情報については、『Oracle Identity Management アプリケーション開発者ガイド』を参照してください。

- **Oracle Internet Directory:** すべてのシングル・サインオン・ユーザーのアカウントおよびパスワード（管理および非管理の両方）のリポジトリ。Single Sign-On Server は、ディレクトリ内のエントリに対してユーザーを認証します。同時に、アプリケーションでのユーザー検証を可能にするユーザー属性をディレクトリから取得します。

Single Sign-On Server へのアクセス

非管理ユーザーは、OracleAS Portal などのパートナ・アプリケーションの URL を入力することにより、Single Sign-On Server に最初にアクセスします。このような URL を入力すると、シングル・サインオンのログイン画面が起動します。正しいユーザー名およびパスワードを入力すると、ユーザーは資格証明を再入力しなくてもその他のパートナ・アプリケーションおよび外部アプリケーションにアクセスできます。

管理ユーザーは、次の形式の URL を入力して、シングル・サインオンの管理ホームページにアクセスできます。

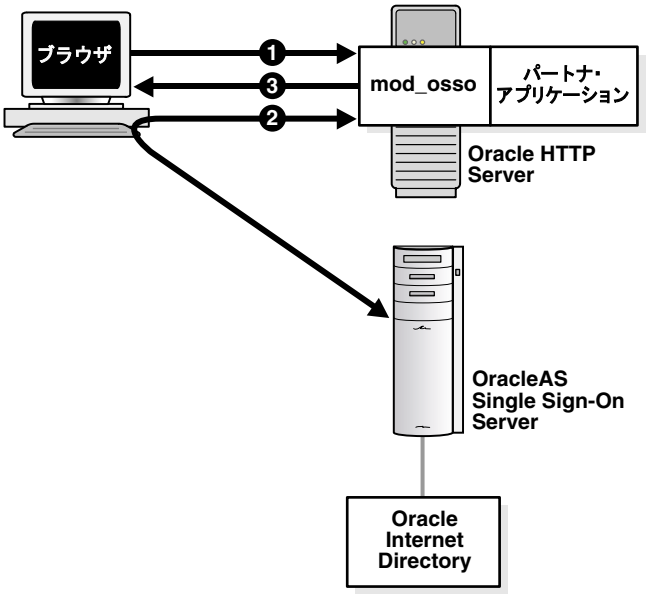
`http://host:port/sso`

host は Single Sign-On Server のあるコンピュータで、*port* はサーバーのポート番号です。サーバーで SSL が有効な場合、`http` を `https` とする必要があります。ポート番号が `80` または `443`（SSL）である場合は、URL から省略できます。これらの番号はデフォルトです。

パートナ・アプリケーションへのアクセス

図 8-1 は、ユーザーが mod_osso で保護されたパートナ・アプリケーションの URL をリクエストすると起きることを示しています。この図は、個別のコンピュータにある Single Sign-On Server およびパートナ・アプリケーション・サーバーを、上下に示しています。パートナ・アプリケーション・サーバーの左はブラウザです。Single Sign-On Server に接続されているのは、Oracle Internet Directory を表すボックスです。矢印は、ブラウザがアプリケーションをリクエストし、Single Sign-On Server にリダイレクトされ、最後にパートナ・アプリケーションに再度リダイレクトされていることを示します。

図 8-1 mod_osso でのシングル・サインオン



1. ユーザーはパートナ・アプリケーションへのアクセスを試行します。
2. ユーザーは Single Sign-On Server にリダイレクトされます。サーバーはユーザーの資格証明を調べます。Oracle Internet Directory で資格証明を検証した後、サーバーは SSO セッションの Cookie を設定し、パートナ・アプリケーションに認証トークンを渡します。
3. アプリケーションはリクエストされたコンテンツを提供します。

2 回目以降のパートナ・アプリケーションの認証

パートナ・アプリケーションにアクセスを要求すると、パートナ・アプリケーション・ログイン・プロセスが開始されます。すでに Single Sign-On Server にログインした後で新しいパートナ・アプリケーションにアクセスしようとしている場合には、次のようになります。

1. ユーザーはパートナ・アプリケーションへのアクセスを試行します。
2. ユーザーは Single Sign-On Server にリダイレクトされます。サーバーはユーザーの認証の資格証明を調べません。SSO セッションの Cookie を使用してユーザー ID を検証します。
3. サーバーは、認証トークンをパートナ・アプリケーションに渡します。
4. アプリケーションはリクエストされたコンテンツを提供します。

パートナ・アプリケーションからのログアウト

外部アプリケーションとは異なり、パートナ・アプリケーションではログアウトの制御を Single Sign-On Server に委譲します。ユーザーがパートナ・アプリケーションの 1 つからログアウトする際に、ユーザーは自動的にその他のパートナ・アプリケーションからログアウトします。

外部アプリケーションへのアクセス

外部アプリケーションは、シングル・サインオン・パートナ・アプリケーションである、OracleAS Portal を介して使用できます。

この項の内容は次のとおりです。

- OracleAS Portal の外部アプリケーション・ポートレットへのアクセス
- 外部アプリケーションの最初の認証
- 外部アプリケーションの 2 回目以降の認証
- 外部アプリケーションからのログアウト

OracleAS Portal の外部アプリケーション・ポートレットへのアクセス

外部アプリケーションにアクセスするには、OracleAS Portal ホームページ上で外部アプリケーション・ポートレットを選択し、表示される外部アプリケーションのリストでアプリケーションを選択します。

外部アプリケーションの最初の認証

外部アプリケーション・ポートレットでアプリケーションを選択すると、外部アプリケーション・ログイン・プロシージャが開始されます。アプリケーションに最初にアクセスしようとしている場合には、次のようになります。

1. 外部アプリケーション・ログイン・プロシージャにより、シングル・サインオンのパスワード・ストアで資格証明がチェックされます。資格証明が見つからない場合には、Single Sign-On Server から入力を求められます。
2. ユーザー名およびパスワードを入力します。アプリケーションのログイン画面上の**ログイン情報を保存する**チェック・ボックスを選択して、パスワード・ストアにこれらの資格証明を保存できます。
3. 資格証明をパスワード・ストアに保存する場合、サーバーはこれらの資格証明を、アプリケーションのログイン処理ルーチンに送信するためのログイン・フォームの構成に使用します。ルーチンは管理者によって事前に構成されており、リクエストされたアプリケーションに関連付けられます。
4. サーバーは、外部アプリケーションに即座に送信するディレクティブとともに、フォームをクライアント・ブラウザに送信します。
5. クライアントはフォームを外部アプリケーションに送信し、ユーザーをログインさせます。

資格証明をパスワード・ストアに保存しない場合、ログインするたびにユーザー名およびパスワードを入力する必要があります。

外部アプリケーションの 2 回目以降の認証

アプリケーションへの最初のアクセス時に資格証明を保存した場合には、後続のログイン中に Single Sign-On Server が資格証明を取得します。プロセスは次のようになります。

1. OracleAS Portal の外部アプリケーション・ポートレット内のリンクの 1 つをクリックします。
2. 外部アプリケーション・ログイン・プロシージャにより、パスワード・ストアで資格証明がチェックされます。
3. Single Sign-On Server が資格証明を検索し、アプリケーションのログイン処理ルーチンに送信するログイン・フォームの構成に使用します。ルーチンは管理者によって事前に構成されており、リクエストされたアプリケーションに関連付けられます。
4. サーバーは、外部アプリケーションに即座に送信するディレクティブとともに、フォームをクライアント・ブラウザに送信します。
5. クライアントはフォームを外部アプリケーションに送信し、ユーザーをログインさせます。

外部アプリケーションからのログアウト

パートナ・アプリケーションとは異なり、外部アプリケーションではログアウトの制御を Single Sign-On Server に委譲しません。これらの各アプリケーションからのログアウトは、ユーザーが実行します。

9

Oracle Identity Manager

Oracle Identity Manager プラットフォームは、アクセス権限管理、セキュリティおよび IT リソースのプロビジョニングを自動化します。Oracle Identity Manager は、生産性を求められるリソースにユーザーを即時に接続し、企業の機密情報を保護するために不正なアクセスを取消しまたは制限します。

Oracle Identity Manager の ID 監査およびコンプライアンス・オートメーション・コンポーネントも、自動認証およびレポート作成を提供します。

この章では、Oracle Identity Manager のアーキテクチャ、利点および主な機能を説明します。この項の内容は次のとおりです。

- Oracle Identity Manager の利点
- Oracle Identity Manager プロビジョニングの機能
- Oracle Identity Manager の動作
- Oracle Identity Manager のアテステーションおよびレポート作成
- Oracle Identity Manager のアテステーションおよびレポート作成の動作

Oracle Identity Manager の利点

ユーザー ID のプロビジョニングの自動化によって IT 管理コストが削減でき、セキュリティが向上します。プロビジョニングは法規制のコンプライアンスにおいても重要な役割を果します。コンプライアンス・イニシアティブでは、これらの規格へのコンプライアンスの実証だけではなく、企業ポリシーの施行にも焦点が置かれています。エンタープライズ ID 管理ソリューションは、ユーザーおよびそのアクセス権限を監査する手段だけでなく、企業ポリシーのユーザー管理面を実装するメカニズムも提供することができます。オラクル社のエンタープライズ・ユーザー・プロビジョニング・ソリューションが、Oracle Identity Manager です。

最近の政府および業界の多数のイニシアティブにより、企業は内部統制および法規制のコンプライアンスを厳密に施行する必要があります。米国市場で取引可能な証券を持つすべての組織は、すべての内部ユーザーおよび外部ユーザーについて、権限も含めたユーザー ID 情報を認可および検証することが要求されています。また、組織内の様々な部門で定義され使用されるアクセス・ポリシーおよびワークフロー・プロセスについても同様です。確立された内部統制、プロセス、ポリシー、プログラムおよびデータを認可するプロセスは、一般にアテステーションと呼ばれます。

ほとんどの企業エンティティでは、アテステーションは手動プロセスおよびスプレッドシートを使用して実行されますが、これには多くの時間とコストがかかる場合があります。こうした手動プロセスには人的ミスが発生しやすく、監査のたびに繰り返す必要があります。これらの定型タスクを自動化することで、組織は時間とコストを大幅に節約できます。オラクル社は、Oracle Identity Manager の ID 監査およびコンプライアンス自動化コンポーネントを使用したアテステーションを提供します。

自動化されたアテステーション機能により、組織は迅速にビジネスおよび IT 環境全体のレポートを生成できます。自動化されたアテステーションは既存の内部統制メカニズムを補完し、コンプライアンスを保証するために導入されたデータ、プラクティスおよびポリシーを検証する手段を提供します。これはユーザー数が多く、動的な場合には特に重要です。自動化されたアテステーション機能を使用することで、組織は標準的プラクティスおよびポリシーを組織内の様々な部門全体で作成して従うことができ、その一方で多様な法規制のコンプライアンス要件を満たすことができます。これは、コストがかかり、時間を消費し、エラーが発生しやすい手動プロセスを使用せずに達成できます。

Oracle Identity Manager プロビジョニングの機能

Oracle Identity Manager プロビジョニングの主な機能には次のものがあります。

スケーラブル・アーキテクチャ : Oracle Identity Manager の J2EE アプリケーション・サーバー・モデルが、スケーラビリティ、フェイルオーバー、ロード・バランシングおよび固有の Web デプロイを提供します。Oracle Identity Manager は、オープンで規格ベースのテクノロジに基づき、3 層アーキテクチャ（クライアント・アプリケーション、Oracle Identity Manager でサポートされている J2EE 準拠のアプリケーション・サーバーおよび ANSI SQL 準拠のデータベース）を採用しており、LDAP 有効アプリケーションと非 LDAP 有効アプリケーションのいずれもプロビジョニングすることができます。

幅広いユーザー管理 : Oracle Identity Manager には、継承、カスタマイズ可能なユーザー ID ポリシー管理、パスワード・ポリシー管理、および顧客の変化するビジネス・ニーズを反映したユーザー・アクセス・ポリシーを備えた、無制限のユーザー組織階層およびユーザー・グループがあります。Oracle Identity Manager には、リソース割当て履歴と、アプリケーションのパラメータおよび権限を管理する機能もあります。委任管理も、包括的な権限設定におけるユーザー管理の主な要素です。

Web ベースのユーザー・セルフサービス : Oracle Identity Manager には、ユーザー情報を管理し、パスワードを変更および同期し、忘れてしまったパスワードをリセットし、使用可能なアプリケーションをリクエストし、使用可能な権限を確認および編集し、ワークフロー・タスクを有効化またはタスクに対応することのできる、カスタマイズ可能な Web ベースのユーザー・セルフサービス・ポータルがあります。

強力で柔軟性の高いプロセス・エンジン : Oracle Identity Manager では、Microsoft Project や Microsoft Visio など使いやすいアプリケーションでビジネスおよびプロビジョニング・プロセス・モデルを作成できます。プロセス・モデルには、承認ワークフローおよびエスカレーションへのサポートが含まれます。イベントおよびエラー・コード・サポートの現在のステータスを含めた、各プロビジョニング・イベントの進捗を追跡できます。Oracle Identity Manager は、複合、分岐、自己回復プロセスおよびデータ交換および依存性のあるネストされたプロセスへのサポートを提供します。プロセス・フローは、完全にカスタマイズ可能であり、プログラミングを必要としません。

Adapter Factory™ を使用した統合 : すべてのシステムをハンドコードしたアダプタでサポートしようとするのは現実的ではありません。そのため、オラクル社ではアダプタ生成のための自動化ツールを開発しました。この Adapter Factory というツールは、幅広いインタフェースとほぼすべてのアプリケーションまたはデバイスをサポートします。これらのアダプタは Oracle Identity Manager サーバー上で実行され、エージェントをターゲット・プラットフォーム上にインストールしたり更新したりする必要がありません。ターゲット・アプリケーション・リソースにネットワークが有効なインタフェースがない状況では、UDDI/SOAP ベース・サポートを使用してリモート統合を作成できます。Adapter Factory を使用すると、実装に数か月かかる統合が数日で完了できます。多数のアダプタを即時に生成できます。Adapter Factory では、既存の統合の更新を維持できるだけでなく、新しい統合のニーズを迅速にサポートすることもできます。Oracle Identity Manager では、外部サード・パーティ・システム上のプログラムをリモート・マネージャを使用して実行することができます。

組込み変更管理 : Oracle Identity Manager では、新しいプロセスをパッケージし、既存のプロセスをインポートおよびエクスポートし、パッケージをあるシステムから別のシステムへ移動することができます。

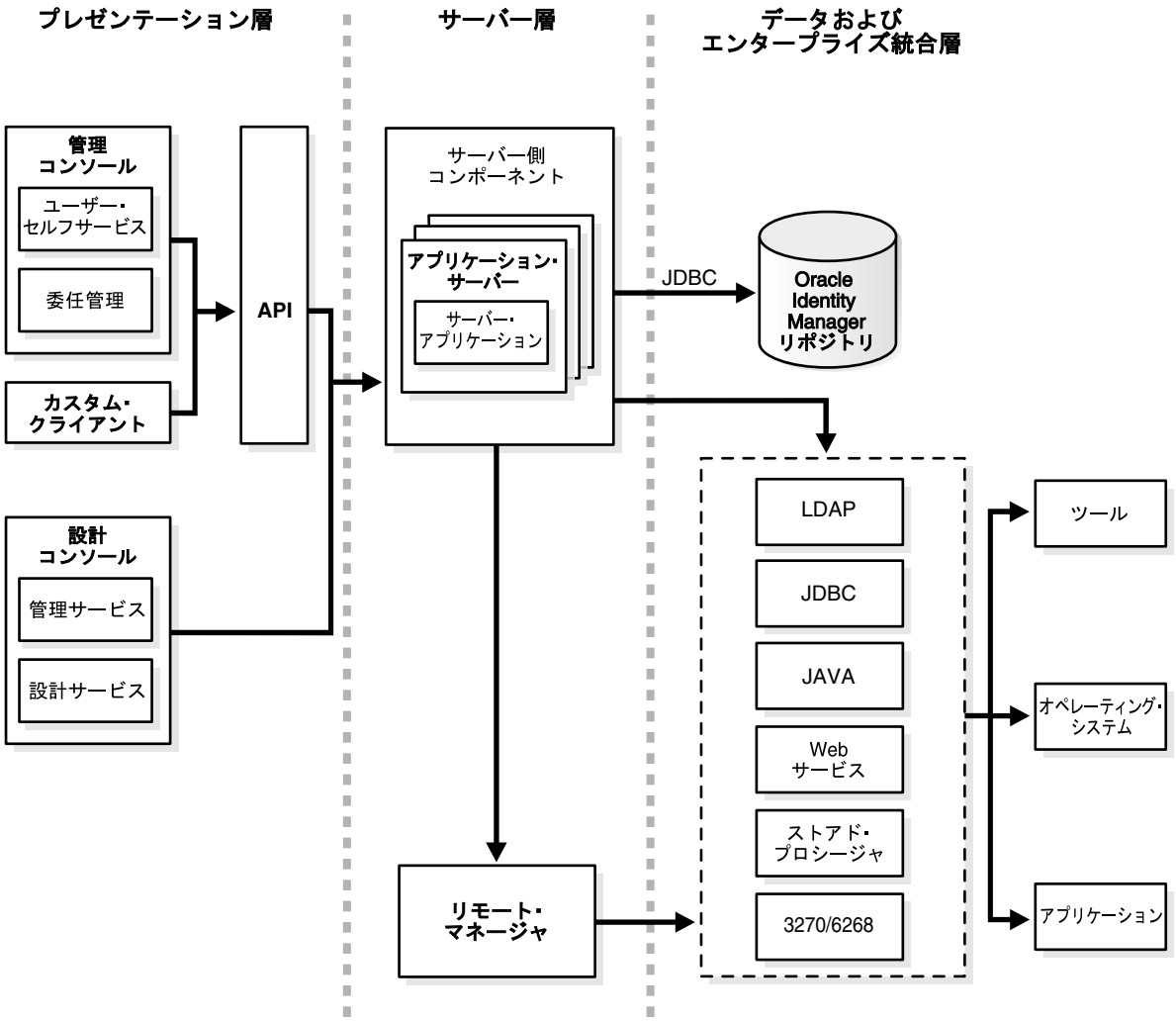
Oracle Identity Manager の動作

Oracle Identity Manager アーキテクチャは、次の 3 層から構成されます。

- 層 1: クライアント
- 層 2: アプリケーション・サーバー
- 層 3: データベース

Oracle Identity Manager の 3 層のアーキテクチャを図 9-1 に示します。

図 9-1 Oracle Identity Manager の 3 層のアーキテクチャ



層 1: クライアント

最初の層は、Java 管理アプリケーションおよびユーザー・コンソール・アプリケーションという 2 つの個別のインタフェースを提供します。

注意： このマニュアルには、Oracle Identity Manager 製品の設計コンソールの動作のみに関連する情報が含まれています。Oracle Identity Manager 管理およびユーザー・コンソールの機能および使用方法の詳細は、『Oracle Identity Manager Administrative and User Console Guide』を参照してください。

Oracle Identity Manager アプリケーションの GUI コンポーネントはこの層に存在します。ユーザーは Oracle Identity Manager クライアントを使用してログインします。これにより、Oracle Identity Manager クライアントは Oracle Identity Manager サーバーと交信し、サーバーにユーザーのログイン資格証明を提供します。Oracle Identity Manager サーバーはこれらの資格証明を検証します。さらに、Oracle Identity Manager クライアントを通じて、データベース内の情報を検索し、またその情報を保存、編集または削除するリクエストを送信できます。

層 2: アプリケーション・サーバー

2 番目の層はビジネス・ロジックを実装します。ビジネス・ロジックは、サポートされている J2EE アプリケーション・サーバー（JBoss アプリケーション・サーバー、BEA WebLogic および IBM WebSphere）により管理される Java Data Objects に存在します。Java Data Objects は Oracle Identity Manager アプリケーションのビジネス・ロジックを実装しますが、外部のどのメソッドにも公開されません。このため、Oracle Identity Manager のビジネス機能にアクセスするために、J2EE インフラストラクチャ内の API レイヤーを使用できます。これは、検索および通信メカニズムを提供します。

Oracle Identity Manager でサポートされている J2EE 準拠のアプリケーション・サーバーは、データベースと通信し、次を担当する唯一のコンポーネントです。

- **Oracle Identity Manager へのログイン :** Oracle Identity Manager でサポートされている J2EE 準拠のアプリケーション・サーバーは、Oracle Identity Manager クライアントをデータベースに接続します。
- **クライアント・リクエストの処理 :** Oracle Identity Manager でサポートされている J2EE 準拠のアプリケーション・サーバーは、Oracle Identity Manager クライアントからのリクエストを処理します。次に、これらのリクエストから適切な情報をデータベースに送信します。サーバーはデータベースからクライアントへのレスポンスも配信します。
- **スケーラビリティ（接続プーリング / 共有）:** Oracle Identity Manager でサポートされている J2EE 準拠のアプリケーション・サーバーは、Oracle Identity Manager クライアントに対して透過的な方法で、単一または複数アプリケーションの使用をサポートします。接続プーリングは、使用のスケーラビリティのリソースを最適化することで、データベース接続性のパフォーマンスを向上させ、動的に**接続プール**のサイズを変更します。
- **システムレベル・データ（メタデータ）の保護 :** Oracle Identity Manager では、**行レベル**のセキュリティを採用して、システムレベルの情報（システム・メタデータ）を誤って削除または変更する可能性のあるユーザーによる不正なアクセスを防ぎます。

注意 : 不正なユーザーがシステムレベルの情報を追加、変更または削除しようとする場合、次のようなメッセージが表示されます。

このデータ項目のセキュリティ・レベルは削除不可または更新不可を示しています。

層 3: データベース

3 番目の層は、データベースから構成されます。これは、Oracle Identity Manager 内のデータの記憶域の管理を担当するレイヤーです。

Oracle Identity Manager のアテステーションおよびレポート作成

アテステーションは、ユーザーまたはシステム・マネージャに人々のアクセス権限を定期的に確認させるプロセスです。既存のサーベンス・オクスリー要件では、企業が財政上重要なすべてのシステムについて 3 ～ 6 か月ごとにアテステーションを実施することが要求されています。Identity Manager には、エンタープライズ顧客が費用効果が高くタイムリな方法でこれらの法的要件を満たすために役立つ、非常にフレキシブルなアテステーション・ソリューションが含まれています。アテステーション・プロセスを Identity Manager で設定することにより、エンタープライズ顧客はレビューア用のユーザー・アクセス権限レポートの生成、配信、確認、サインオフ、委任、トラッキングおよびアーカイブのプロセスを、定期的または不定期ベースで自動化できます。

この項の内容は次のとおりです。

- 機能の概略
- レポートのタイプ

機能の概略

現在提供しているアテステーションの主な機能は次のとおりです。

- アテステーション・プロセスの段階的定義
- アテステーション・タスクおよびプロセスのオンデマンドまたは定期的スケジュール
- 複数のリソース全体でのユーザーのファイングレインな権限のアテステーション
- アテステーション・プロセスへの参加のためリソースに財政上重要とタグ付けする機能
- アテステーション・リクエスト内の各アイテムを認証、却下、拒否または委任する機能
- 各リソースの各ユーザーの各権限に対するファイングレインなアテステーション・アクション
- レビューア、ユーザーおよびプロセス所有者へのアテステーション・アクションに関する通知
- レビューア、ユーザーおよびリソース別の処理済、要約済のアテステーション・リクエストのレポート
- 定期監査およびレポート作成用アテステーション・データのアーカイブ
- 定期監査およびレポート作成用に実行されたアテステーション・アクションのアーカイブ

レポートのタイプ

Oracle Identity Manager では、現在 2 種類のアテステーション・レポートを提供しています。

- **操作レポート :** 現在のステータスのスナップショットを示します。次のものが含まれます。
  - **ユーザー権限**（誰が何を持つか）: このレポートで、管理者または監査者は、問合せパラメータに一致するユーザーの権限を問い合せることができます。このレポートは、操作およびコンプライアンスの目的に使用できます。これは操作レポートであり、履歴レポートではありません。
  - **リソース・アクセス・リスト :** このレポートでは、管理者または監査者は、リソースへのすべての既存のプロビジョニング済ユーザーを問い合せることができます。このレポートは、操作およびコンプライアンスの目的に使用できます。これは操作レポートであり、履歴レポートではありません。
  - **グループ・メンバーシップ :** このレポートでは、管理者または監査者は、プロビジョニング環境にあるすべてのリソースで、グループおよびそのメンバーのリストを表示することができます。このレポートは、操作およびコンプライアンスの目的に使用できます。これは、すべてのリソースでのグループ・メンバーシップのスナップショット・レポートであり、履歴レポートではありません。

- **履歴レポート :** 履歴データのビューを提供します。次のものが含まれます。
  - **ユーザー・アクセス履歴**（誰が何を持っていたか）: このレポートでは、管理者または監査者は、ユーザーのライフサイクル全体でのユーザーのリソース・アクセス履歴を表示することができます。このレポートは、コンプライアンスおよびフォレンジック監査の目的に使用できます。これは、ユーザー・アクセス・プロファイルのスナップショット・レポートではありません。これはユーザーの権限の全履歴を示す、存続期間レポートです。
  - **リソース・アクセス・リスト履歴 :** このレポートでは、管理者または監査者は、リソースへのすべての既存のプロビジョニング済ユーザーをライフサイクル全体で問い合せることができます。このレポートは、コンプライアンスおよびフォレンジック監査の目的に使用できます。これは、リソース・アクセス・リストのスナップショット・レポートではありません。これはリソースのアクセス・リスト / 権限の全履歴を示す、存続期間レポートです。
  - **ユーザー・プロファイル履歴 :** このレポートでは、管理者または監査者は、ユーザーのライフサイクル全体でユーザーのプロファイル履歴を表示することができます。このレポートは、コンプライアンスおよびフォレンジック監査の目的に使用できます。これは、ユーザー・プロファイルのスナップショット・レポートではありません。これはユーザーのプロファイルの全履歴を示す、存続期間レポートです。
  - **ユーザー・メンバーシップ履歴 :** このレポートでは、管理者または監査者は、ユーザーのライフサイクル全体でユーザー・グループ内のユーザーのメンバーシップ履歴を表示することができます。このレポートは、コンプライアンスおよびフォレンジック監査の目的に使用できます。これは、メンバーシップのスナップショット・レポートではありません。これはユーザーのグループ・メンバーシップの全履歴を示す、存続期間レポートです。
  - **グループ・メンバーシップ履歴 :** このレポートでは、管理者または監査者は、グループのライフサイクル全体でユーザー・グループの履歴メンバーシップを表示することができます。このレポートは、コンプライアンスおよびフォレンジック監査の目的に使用できます。これは、グループ・メンバーシップのスナップショット・レポートではありません。これはグループ・メンバーシップの全履歴を示す、存続期間レポートです。
  - **ユーザー・ライフサイクル :** このレポートでは、管理者または監査者は、企業環境内の特定のユーザーのアカウント関連データ（ユーザー ID ライフサイクル）の詳細な情報をすべて取得することができます。このレポートは、コンプライアンスおよびフォレンジック監査の目的に使用できます。これは、ユーザー・プロファイルのスナップショット・レポートではありません。これは様々なリソースにおける、ユーザー・プロファイルおよびユーザー権限の全履歴を示す、存続期間レポートです。

Oracle Identity Manager のアテステーションおよびレポート作成の動作

Oracle Identity Manager（OIM）で定義されているように、アテステーション・プロセスには、レビューア、アテストされるデータおよびアテステーション・タスクのスケジュールが含まれます。

自動アテステーション機能は、認定レビューアがデータの正確性を確認する作業を完遂するために必要となるユーザー ID とその詳細な権限情報を表示します。また、レビューアに不正を文書化し修正する手段を提供します。アテステーション・プロセスは、オンデマンドで実行することも、年に一度、6 か月に一度または四半期に一度の一定間隔で定期的に実行するようスケジュールすることもできます。

アテストされるデータは、基本的なユーザー・プロファイル・データから、ユーザーまたはロールに割り当てられたアクセス権または権限に及ぶことがあります。レビューアがアテステーションのために行う特定のアクションには、アテステーション・リクエスト内の各エントリを認証、却下、拒否または委任する機能が含まれます。レビューアは、実行されたアクションの妥当性を示す特定のコメントをリクエスト内の各エントリに入力できます。また、リクエスト内のすべてのエントリに適用する汎用のコメントを入力できます。

各アテステーション・リクエストには、各ユーザーに割り当てられた各権限を含めるなどして、多数のエントリが含まれる場合があります。レビューアは、これらのエントリのそれぞれについて 4 つのアクション（認証、却下、拒否または委任）から 1 つを実行できます。レビューアはリクエスト内のエントリの一部にレスポンスを選択し、選択を保存し、後にリクエストを再度確認して他のエントリのアクションを完了し、最後にアテステーション・リクエスト全体を処理のために送信できます。レビューアおよび影響を受けるユーザーに電子メール通知が送信されるため、データに行われたアクションは認識されます。これらのアテステーションのそれぞれが、後続の監査およびレポート作成用にアーカイブされます。

リソースには、財政上重要とのタグ付けができ、そうしたリソースのユーザー権限はアテステーション・プロセスに参加するように自動的に選択されます。オプションとして、財政上重要とのタグ付けがない特定のリソースもオンデマンドでアテステーション用に選択できます。

アテステーション・リクエストのすべてのデータと実行されたアクションも、後続の監査およびレポート作成の目的でアーカイブされます。

プロセス・フローは次のとおりです。まず、スケジュールされているアテステーション・リクエストまたはオンデマンドのアテステーション・リクエストが生成され、アテステーション・タスクに必要なデータのスナップショットがコンパイルされます。レビューアに、アテステーション・リクエストが通知されます。レビューアはシステムにログインし、自分のアテステーション受信ボックスに表示されるアテステーション・リクエストを表示します。通常、アテステーション・リクエストは多数のエントリから構成されます。エントリは、各ユーザーについてアテストされるユーザー・プロファイル・データまたはユーザー権限データの各項目ごとに 1 つです。レビューアは、各エントリについて次の 4 つから 1 つを選択できます。

- **認証 :** レビューアはデータが正確であるとアテストします。
- **却下 :** レビューアはデータを不正確であるとマークします。
- **拒否 :** レビューアはこのエンティティに対するアテステーションの実行を拒否します。
- **委任 :** レビューアはこのエンティティのアテステーション・タスクを別のレビューアに委任します。

レビューアには、リクエスト内のエントリのサブセットのみについて選択し、行われたアクションを保存し、後に返信してアテステーション・リクエストを完了するためのオプションがあります。レビューアは、各エントリに対する個別のコメント、またはリクエスト内のすべてのエントリに対する汎用のコメントを入力できます。レビューアが各エントリについてアクションを完了すると、今後の処理のためにアテステーション・リクエスト全体を送信できます。この時点で、電子メール通知がこのアテステーション・リクエストに関連するレビューア、ユーザーおよびプロセス所有者に送信されます。

10

Oracle Delegated Administration Services

この章では、管理コンソールおよびセルフサービス・コンソールを作成するための事前定義された Web ベース・ユニットで構成されたフレームワークである、Oracle Delegated Administration Services について説明します。これらのコンソールは、委任管理者およびユーザーが、指定したディレクトリ操作の実行に使用できます。

この章の内容は次のとおりです。

- Oracle Delegated Administration Services の利点
- Oracle Delegated Administration Services の機能
- Oracle Delegated Administration Services の動作

注意： Oracle Delegated Administration Services は、Oracle Internet Directory に格納されている情報の管理のみに使用します。サード・パーティまたは異機種ディレクトリ環境に格納されている情報の管理には、あらゆる ID 管理およびセキュリティ機能を備えた Oracle Access Manager の使用を検討してください。Oracle Access Manager の機能には、Web シングル・サインオン、ユーザーのセルフサービスおよび自己登録、高度なワークフロー機能、レポート作成および監査、ポリシー管理、動的グループ管理、および委任管理があります。

Oracle Delegated Administration Services の利点

委任管理によって、中央ディレクトリにユーザー、グループおよびサービスのすべてのデータを格納でき、その一方でデータの管理を様々な管理者およびユーザーに分散できます。これは、ユーザーの環境における様々なセキュリティの要件を考慮した方法で行われます。

たとえば、エンタープライズがユーザー、グループおよびサービスのすべてのデータを中央ディレクトリに格納し、ユーザー・データに対して 1 人の管理者を必要とし、電子メール・サービスに対してもう 1 人の管理者を必要としているとします。または、ユーザー権限を完全に制御するために Oracle Financial の管理者が必要であり、特定のユーザーまたはグループの Web ページを完全に制御するために OracleAS Portal の管理者が必要であるとします。Oracle Identity Management インフラストラクチャによって提供される委任管理では、多様なセキュリティの要件を持つこれらの管理者のすべてがセキュアかつスケーラブルな方法で集中化されたデータを管理できます。

Oracle Delegated Administration Services の機能

Oracle Delegated Administration Services は、ユーザーのかわりにディレクトリ操作を実行する、一連の事前定義された Web ベースのユニットです。ディレクトリの管理者は、特定の機能を他の管理者やエンド・ユーザーに委任することで、より定型のディレクトリ管理タスクから解放されます。ユーザー・エントリの作成、グループ・エントリの作成、エントリの検索、およびユーザー・パスワードの変更など、ディレクトリが有効なアプリケーションに必要なほとんどの機能が提供されています。

Oracle Delegated Administration Services には、次の機能があります。

- Identity Management Grid Control プラグインでの管理
- Oracle Internet Directory セルフ・サービス・コンソール
- 権限委任レベル
- プロキシ・ユーザーの集中化

Identity Management Grid Control プラグインでの管理

Oracle Application Server 10*g*（10.1.4.0.1）の時点で、Oracle Directory Integration Platform を Identity Management Grid Control プラグインで管理できます。これは Oracle Enterprise Manager 10*g* Grid Control の機能を使用します。

関連資料：『Oracle Identity Management インフラストラクチャ管理者ガイド』の Identity Management Grid Control プラグインに関する項

Oracle Internet Directory セルフ・サービス・コンソール

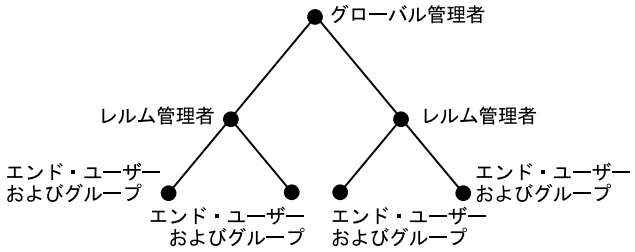
Oracle Delegated Administration Services を使用して、ディレクトリ内のアプリケーション・データを管理する独自のツールを開発できます。または、委任管理サービス・ベースのツールである Oracle Internet Directory セルフ・サービス・コンソールを使用できます。これは、ディレクトリ内で管理されているアプリケーション・データへの管理アクセスが可能になるセルフ・サービス・アプリケーションです。このツールは Oracle Internet Directory で使用できます。

関連資料：『Oracle Identity Management 委任管理ガイド』

権限委任レベル

Oracle Delegated Administration Services を使用して構築されたアプリケーションでは、ユーザーがそれぞれのタイプのユーザーに、特定のレベルのディレクトリへのアクセス権を付与できます。たとえば、ホスティング環境における様々な管理レベルを示す図 10-1 を見てください。この図はディレクトリ情報ツリーを示し、そのルートはグローバル管理者用のエントリです。そのノードからは 2 つの分岐があり、いずれもサブスクライバ管理者ノードに伸びています。各サブスクライバ管理者ノードの下には 2 つのノードがあり、いずれもエンド・ユーザーおよびグループ用です。

図 10-1 ホスト環境における管理レベル



ディレクトリ全体のすべての権限を持つグローバル管理者は、レルム管理者にホスト企業用のレルムを作成し管理する権限を委任することができます。これらの管理者は、エンド・ユーザーおよびグループに、アプリケーション・パスワード、個人データおよびプリファレンスを変更する権限を委任します。このように、各タイプのユーザーに適切なレベルの権限を付与できます。

Oracle Delegated Administration Services で次の権限を委任できます。

- ユーザーおよびグループの作成、編集および削除
- ユーザーおよびグループへの権限の割当て
- サービスおよびアカウントの管理
- Oracle Delegated Administration Services の構成
- Oracle Reports および Oracle Application Server Forms Services のリソース管理

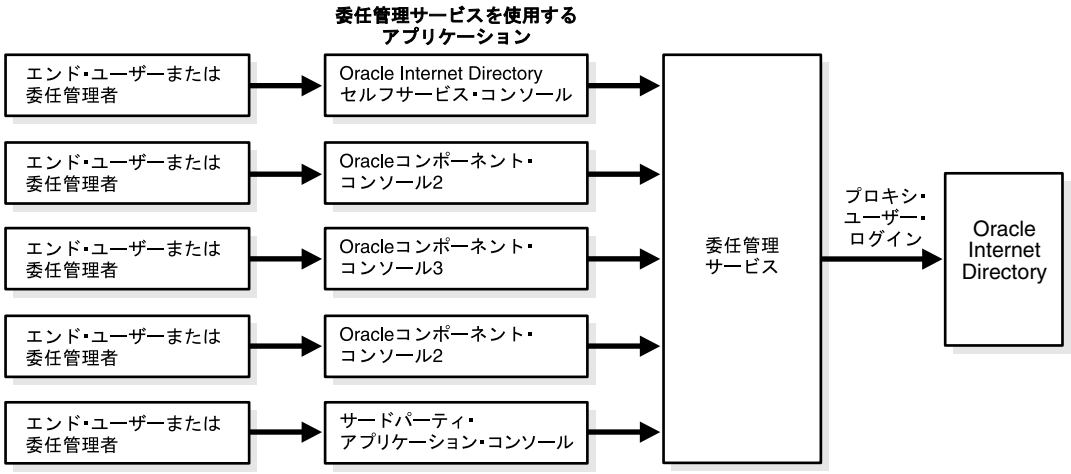
プロキシ・ユーザーの集中化

ユーザーが Oracle コンポーネントにログインする際に、そのコンポーネントがエンド・ユーザーにかわってディレクトリから情報（パスワード検証など）を取得する必要がある場合があります。これを行うため、コンポーネントは通常、プロキシ・ユーザーとしてディレクトリにログインします。これは、ID をエンド・ユーザーの ID に切り替えることができる機能です。

Oracle Delegated Administration Services 環境では、各コンポーネントはプロキシ・ユーザーとしてディレクトリにログインせず、中央の Oracle Delegated Administration Services にログインします。次に、Oracle Delegated Administration Services がプロキシ・ユーザーとしてディレクトリにログインし、ID をエンド・ユーザーの ID に切り替え、そのユーザーのかわりに操作を実行します。ディレクトリにアクセスするすべてのコンポーネントにプロキシ・ユーザーのアクセス権を付与するという安全面で劣る方法のかわりに、このようにしてプロキシ・ユーザーのディレクトリ・アクセスを集中化することができます。

図 10-2 は、任意の Oracle Delegated Administration Services 環境におけるプロキシ・ユーザー機能を示しています。エンド・ユーザーまたは委任された管理者が、中央の Oracle Delegated Administration Services にログインします。Oracle Internet Directory セルフ・サービス・コンソール、他の Oracle コンポーネントのコンソール（OracleAS Portal など）、またはサード・パーティのアプリケーションのコンソールを使用してこれを行います。次に、Oracle Delegated Administration Services がプロキシ・ユーザーとして Oracle Internet Directory にログインします。

図 10-2 Oracle Delegated Administration Services におけるプロキシ・ユーザー機能



Oracle Delegated Administration Services の動作

Oracle Delegated Administration Services は、Oracle Containers for J2EE（OC4J）インスタンス上にデプロイされた J2EE アプリケーションです。Oracle Delegated Administration Services は次の基本タスクを実行します。

1. クライアントからのリクエストの受信
2. （Oracle Internet Directory でデータを取得または更新することによる）それらのリクエストの処理、および LDAP 結果を HTML ページにコンパイル
3. HTML ページをクライアントの Web ブラウザに返信

図 10-3 は、Oracle Delegated Administration Services 環境のコンポーネント間の情報のフローを示しています。

図 10-3 Oracle Delegated Administration Services 環境における情報フロー

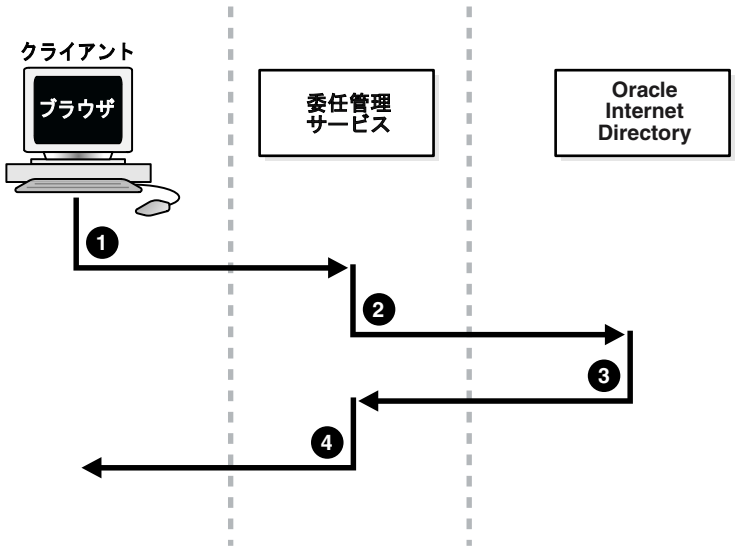


図 10-3 は次を示しています。

1. ユーザーはブラウザから HTTP を使用して、ディレクトリ問合せを含むリクエストを Oracle Delegated Administration Services に送信します。
2. Oracle Delegated Administration Services はリクエストを受信し、適切なサーブレットを起動します。このサーブレットがリクエストを解釈し、LDAP を使用して Oracle Internet Directory に送信します。
3. Oracle Internet Directory は、LDAP 結果を Oracle Delegated Administration Services サーブレットに送信します。
4. Oracle Delegated Administration Services サーブレットは LDAP 結果を HTML ページにコンパイルし、クライアント Web ブラウザに送信します。

索引

A

Access Server
  Oracle Access Manager アクセス・システム，6-4, 6-6
AccessGate
  Oracle Access Manager アクセス・システム，6-7

I

ID 管理
  Oracle Access Manager ID システム，6-8
  フェデレーテッド，7-2
ID システム
  Oracle Access Manager，6-1

L

LDAP
  サーバー，3-9
    マルチスレッド，3-2
  サーバー・インスタンス，3-7，3-8，3-9

O

OC4J
  委任管理サービスによる使用，10-4
OID モニター
  Oracle Internet Directory，3-8
Oracle Application Server Portal, Oracle Internet Directory の使用，3-3
Oracle Collaboration Suite, Oracle Internet Directory の使用，3-3
Oracle Delegated Administration Services
  OracleAS Single Sign-On，8-2
Oracle Directory Integration Platform
  構造，5-6
  説明，5-4
Oracle Directory Integration Platform サーバー
  説明，5-3
Oracle Identity and Access Management Suite
  説明，1-6
Oracle Identity プロトコル
  Oracle Access Manager ID システム，6-10
Oracle Internet Directory
  コンポーネント，3-5
  同期環境における中央ディレクトリ，5-3
  ノード，3-6
Oracle Net Services
  Oracle Internet Directory の使用，3-3
Oracle Secure Federation Services
  アーキテクチャ，7-6
  利点，7-1
OracleAS Single Sign-On
  管理ページ，8-4
  ホームページ，8-4
OracleAS Wireless
  OracleAS Single Sign-On，8-2
Oracle ディレクトリ・サーバー・インスタンス，3-5, 3-7，3-8，3-9
Oracle ディレクトリ・レプリケーション・サーバー
  LDAP を使用してディレクトリ・サーバーと通信，3-8
  Oracle Internet Directory ノードのコンポーネント，3-7
  Oracle Internet Directory のコンポーネント，3-5

P

Policy Manager
  Oracle Access Manager アクセス・システム，6-4, 6-5

S

Single Sign-On Server
  アクセス，8-4

W

WebGate
  Oracle Access Manager アクセス・システム，6-4, 6-7
WebPass
  Oracle Access Manager ID システム，6-12
  Oracle Access Manager アクセス・システム，6-4
Web ベースのユーザー・セルフサービス
  Oracle Identity Manager，9-2

あ

アーキテクチャ
  Oracle Access Manager ID システム，6-10
  Oracle Access Manager アクセス・システム，6-4
  Oracle Application Server Single Sign-On，8-3
  Oracle Directory Integration Platform，5-3

Oracle Identity Federation，7-3
Oracle Identity Manager プロビジョニング，9-3
Oracle Internet Directory，3-5
委任管理サービス，10-5
アクセス・システム・コンソール
Oracle Access Manager アクセス・システム，6-5
アクセス・システムの機能
Oracle Access Manager，6-1
アテステーション・プロセス
Oracle Identity Manager のアテステーションおよびレポート作成，9-8
アプリケーション・サーバー
Oracle Identity Manager，9-5

い

委任管理サービス
OC4J，10-4
アーキテクチャ，10-5
集中プロキシ・ユーザー，10-3
定義，10-2
ディレクトリ・データ管理の委任，10-3
インフラストラクチャ
ID およびアクセス管理コンポーネント，1-7
Oracle Application Server，1-7

か

カスタマイズ
Oracle Access Manager ID システム，6-8
監査サービス
Oracle Access Manager アクセス・システム，6-3
管理ツール
Oracle Internet Directory，3-5

き

機能
Oracle Access Manager ID システム，6-8
Oracle Access Manager アクセス・システム，6-2
Oracle Application Server Single Sign-On，8-2
Oracle Delegated Administration Services，10-2
Oracle Directory Integration Platform，5-2
Oracle Identity Federation，7-2
Oracle Identity Manager のアテステーションおよびレポート作成，9-6
Oracle Identity Manager プロビジョニング，9-2
Oracle Internet Directory，3-2
Oracle Virtual Directory，4-3

く

グローバリゼーション・サポート
Oracle Internet Directory，3-5

こ

高可用性
Oracle Internet Directory，3-2
構成
Oracle Access Manager アクセス・システム，6-6
国際化
Oracle Internet Directory，3-5
コンポーネント
Oracle Internet Directory，3-5
ディレクトリ・サーバー，3-6
コンポーネント , 委任管理サービス，10-5

し

シナリオ
Oracle Virtual Directory，4-8
シングル・サインオン
Oracle Access Manager アクセス・システム，6-3

す

スケーラビリティ , Oracle Internet Directory，3-2
スケーラブル・アーキテクチャ
Oracle Identity Manager，9-2

せ

製品
Oracle Identity and Access Management，1-2
セキュリティ
Oracle Internet Directory，3-2，3-4

て

ディレクトリ
分散，3-5
ディレクトリ・サーバー，3-5，3-9
共有サーバー，3-2
プロセス，3-9
複数，3-9
マルチマスター・レプリケーション，3-2
ディレクトリ・データ管理の委任，10-3
ディレクトリ・レプリケーション・サーバー，3-5，3-7，3-8
ディレクトリ統合プラットフォーム・サーバー
説明，5-3
データ管理レイヤー
Oracle Access Manager ID システム，6-9
データの整合性
Oracle Internet Directory，3-5
データベース
サーバー，3-6
ディレクトリ専用，3-7
データベース接続
Oracle Internet Directory，3-9

と

同期
Oracle Directory Integration Platform，5-2

に

認可
Oracle Access Manager アクセス・システム，6-6
認可サービス
Oracle Access Manager アクセス・システム，6-3
認証
Oracle Access Manager アクセス・システム，6-6

認証サービス
Oracle Access Manager アクセス・システム，6-2

の

ノード , Oracle Internet Directory，3-6

は

パーソナライズ・サービス
Oracle Access Manager アクセス・システム，6-3
パーティション
Oracle Internet Directory，3-5
パスワード管理
Oracle Access Manager ID システム，6-9
パッケージング
Oracle Identity and Access Management 製品，1-6

ふ

フェイルオーバー，3-2
フェデレーション・プロファイル，7-5
フェデレーテッド ID 管理，7-2
イベント・フロー，7-5
ユースケース，7-3
利点，7-2
プロキシ・ユーザー
委任管理サービスにおける集中化，10-3
プロセスの概要
Oracle Access Manager ID システム，6-12
分散ディレクトリ，3-5

ま

マルチ・サーバー・プロセス，3-9
マルチスレッド LDAP サーバー，3-2
マルチマスター・レプリケーション，3-2

ゆ

ユーザー・インタフェースのカスタマイズ
Oracle Access Manager ID システム，6-9
ユーザー管理
Oracle Identity Manager，9-2

り

リカバリ機能 , Oracle，3-2
リクエストの処理
Oracle Delegated Administration Services，10-5
リスナー , ディレクトリ・データベース，3-7，3-9
利点
Oracle Access Manager，6-2
Oracle Application Server Single Sign-On，8-2
Oracle Delegated Administration Services，10-2
Oracle Directory Integration Platform，5-2
Oracle Identity Federation，7-2
Oracle Identity Manager，9-2
Oracle Internet Directory，3-2
Oracle Virtual Directory，4-2

れ

レプリケーション
マルチマスター，3-2