Oracle® Identity Management

概要および配置プランニング・ガイド

10*g*（9.0.4）

部品番号 : B12379-02

2004 年 6月

ORACLE®

Oracle Identity Management 概要および配置プランニング・ガイド , 10*g*（9.0.4）

部品番号 : B12379-02

原本名 : Oracle Identity Management Concepts and Deployment Planning Guide 10*g* (9.0.4)

原本部品番号 : B10660-01

原本著者 : Richard Strohm

原本協力者 : Cynthia Kibbe, Ganesh Kirti, Ashish Kolli, Michael Mesaros, Valarie Moore, Richard Smith, Uppili Srinivasan, Arun Swaminathan

目次

4 Oracle Identity Management の管理と使用

5 他の識別情報管理ソリューションとの統合

6 エンタープライズ・アプリケーションの統合

A Oracle Internet Directory のデフォルト設定

索引

図リスト

はじめに

『Oracle Identity Management 概要および配置プランニング・ガイド』では、管理者およびアプリケーション開発者向けに、識別情報管理の概念を説明し、配置プランニングの情報を示します。

「はじめに」の項目は次のとおりです。

対象読者

このマニュアルの対象読者は次のとおりです。

- 識別情報の管理責任者
- Oracle アプリケーションの管理者
- エンタープライズ・アプリケーションの開発者

構成

この『Oracle Identity Management 概要および配置プランニング・ガイド』で説明する概念のフレームワークは、Oracle Identity Management インフラストラクチャの理解、および社内への配置に必要です。Oracle Identity Management インフラストラクチャの具体的なコンポーネントの配置方法や管理方法の詳細は、対応する管理者ガイドで説明しています。

このマニュアルは、次の章から構成されています。

第 1 章「識別情報管理の概要」
この章では、識別情報管理の概要を示し、企業で必要な理由について説明します。

第 2 章「Oracle Identity Management の概念とアーキテクチャ」
この章では、Oracle Identity Management の概念およびアーキテクチャについて説明します。

第 3 章「Oracle Identity Management の配置プランニング」
この章では、Oracle Identity Management の配置について説明します。

第 4 章「Oracle Identity Management の管理と使用」
この章では、Oracle Identity Management の管理および使用法について説明します。

第 5 章「他の識別情報管理ソリューションとの統合」
この章では、Oracle Identity Management と他の識別情報管理ソリューションとの統合について説明します。

第 6 章「エンタープライズ・アプリケーションの統合」
この章では、エンタープライズ・アプリケーションと Oracle Identity Management の統合について説明します。

付録 A「Oracle Internet Directory のデフォルト設定」
この付録では、Oracle Internet Directory のインストール時に使用できるデフォルト設定について説明します。

関連ドキュメント

詳細は、次の Oracle ドキュメントを参照してください。

- 『Oracle Application Server 10*g* 管理者ガイド』
- 『Oracle Application Server 10*g* セキュリティ・ガイド』
- 『Oracle Application Server 10*g* 高可用性ガイド』
- Oracle Application Server 10*g* のインストレーション・ガイド
- 『Oracle Application Server Certificate Authority 管理者ガイド』
- 『Oracle Application Server Single Sign-On 管理者ガイド』
- 『Oracle Internet Directory 管理者ガイド』

表記規則

この項では、このマニュアルで使用される表記規則について説明します。

規則	意味	例
太字	太字は、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。	この句を指定すると、**索引構成表**が作成されます。
固定幅フォントの大文字	固定幅フォントの大文字は、システム指定の要素を示します。このような要素には、パラメータ、権限、データ型、Recovery Manager キーワード、SQL キーワード、SQL*Plus またはユーティリティ・コマンド、パッケージおよびメソッドがあります。また、システム指定の列名、データベース・オブジェクト、データベース構造、ユーザー名およびロールも含まれます。	NUMBER 列に対してのみ、この句を指定できます。 BACKUP コマンドを使用して、データベースのバックアップを作成できます。 USER_TABLES データ・ディクショナリ・ビュー内の TABLE_NAME 列を問い合せます。 DBMS_STATS.GENERATE_STATS プロシージャを使用します。

規則	意味	例
固定幅フォントの小文字	固定幅フォントの小文字は、実行可能ファイル、ファイル名、ディレクトリ名およびユーザーが指定する要素のサンプルを示します。このような要素には、コンピュータ名およびデータベース名、ネット・サービス名および接続識別子があります。また、ユーザーが指定するデータベース・オブジェクトとデータベース構造、列名、パッケージとクラス、ユーザー名とロール、プログラム・ユニットおよびパラメータ値も含まれます。	`sqlplus` と入力して、SQL*Plus をオープンします。 パスワードは、`orapwd` ファイルで指定します。 `/disk1/oracle/dbs` ディレクトリ内のデータ・ファイルおよび制御ファイルのバックアップを作成します。 `hr.departments` 表には、`department_id`、`department_name` および `location_id` 列があります。 `QUERY_REWRITE_ENABLED` 初期化パラメータを `true` に設定します。 `oe` ユーザーとして接続します。
	注意 : プログラム要素には、大文字と小文字を組み合せて使用するものもあります。これらの要素は、記載されているとおりに入力してください。	`JRepUtil` クラスが次のメソッドを実装します。
固定幅フォントの小文字のイタリック	固定幅フォントの小文字のイタリックは、プレースホルダまたは変数を示します。	*`parallel_clause`* を指定できます。 `U`*`old_release`*`.SQL` を実行します。ここで、*`old_release`* とはアップグレード前にインストールしたリリースを示します。

1

識別情報管理の概要

この章では、識別情報管理の概要を示し、識別情報管理システムのコンポーネントを解説し、Oracle Identity Management の概要および目的について説明します。

この章では、次のトピックについて説明します。

識別情報管理とは

識別情報管理は、識別情報管理システムの様々なコンポーネントにより、組織内のネットワーク・エンティティのセキュリティ・ライフサイクルを管理するプロセスです。最も一般的には、組織のアプリケーション・ユーザーの管理を指します。セキュリティ・ライフサイクルの手順には、アカウントの作成、停止、権限の変更およびアカウントの削除が含まれます。

管理されるネットワーク・エンティティには、デバイス、プロセス、アプリケーションなど、ネットワーク環境で対話を行うものがすべて含まれます。また、識別情報管理作業で管理されるエンティティには、顧客、取引先パートナ、Web サービスなど、組織外のユーザーも含まれます。

識別情報管理システムを使用することで、企業には次の利点が得られます。

- アカウント管理の一元化とタスクの自動化により、管理コストが削減される。
- 新しいアプリケーションで既存インフラストラクチャを利用して、ユーザー・アカウントとユーザー権限をプロビジョニングできるため、アプリケーションの配置が迅速化する。
- 新規ユーザーがアプリケーションに素早くアクセスできるため、ユーザーの経験が高まる。
- ユーザー・パスワードとセキュリティ資格証明を集中管理し、一元化された認可情報およびポリシー情報を利用できるようにアプリケーションをカスタマイズすることで、セキュリティと使い勝手が改善される。

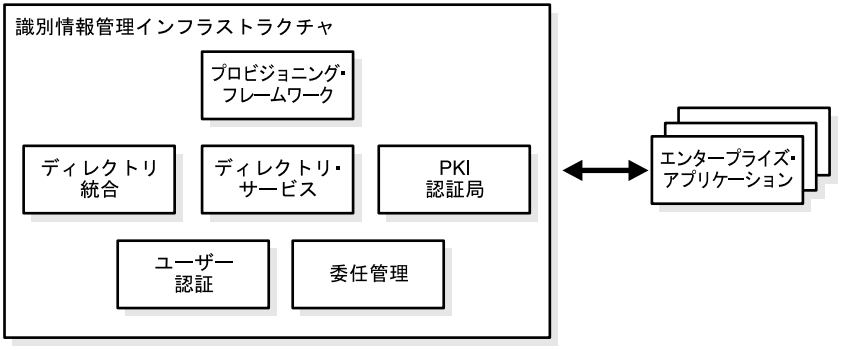
識別情報管理システムのコンポーネント

完全な識別情報管理システムには、次のコンポーネントが含まれます。

- スケーラブルでセキュアな、ユーザー情報を格納および管理するための業界標準に準拠したディレクトリ・サービス。
- （人事管理アプリケーションなどの）エンタープライズ・プロビジョニング・システムにリンクさせた、またはスタンドアロンで操作可能なプロビジョニング・フレームワーク。
- 識別情報管理ディレクトリを従来の、またはアプリケーション固有のディレクトリに企業が接続できるディレクトリ統合プラットフォーム。
- 公開鍵インフラストラクチャ（PKI）証明書を作成および管理するシステム。
- ユーザー認証のためのランタイム・モデル。
- 識別情報管理システムの管理者が、個別のアプリケーションの管理者を選択して、またはユーザーに直接、アクセス権限を委任できる委任管理モデルおよびアプリケーション。非常に重要な様々な要件をサポートできるセキュリティ・モデルおよびユーザー・インタフェース・モデル。

図 1-1 に、識別情報管理システムの概要を示します。

図 1-1 識別情報管理システムの概要



Oracle Identity Management の概要

Oracle Identity Management は、Oracle 製品で分散セキュリティを実現する統合インフラストラクチャです。Oracle Identity Management は、Oracle Application Server、Oracle9*i* Database Server および Oracle Collaboration Suite に付属しています。

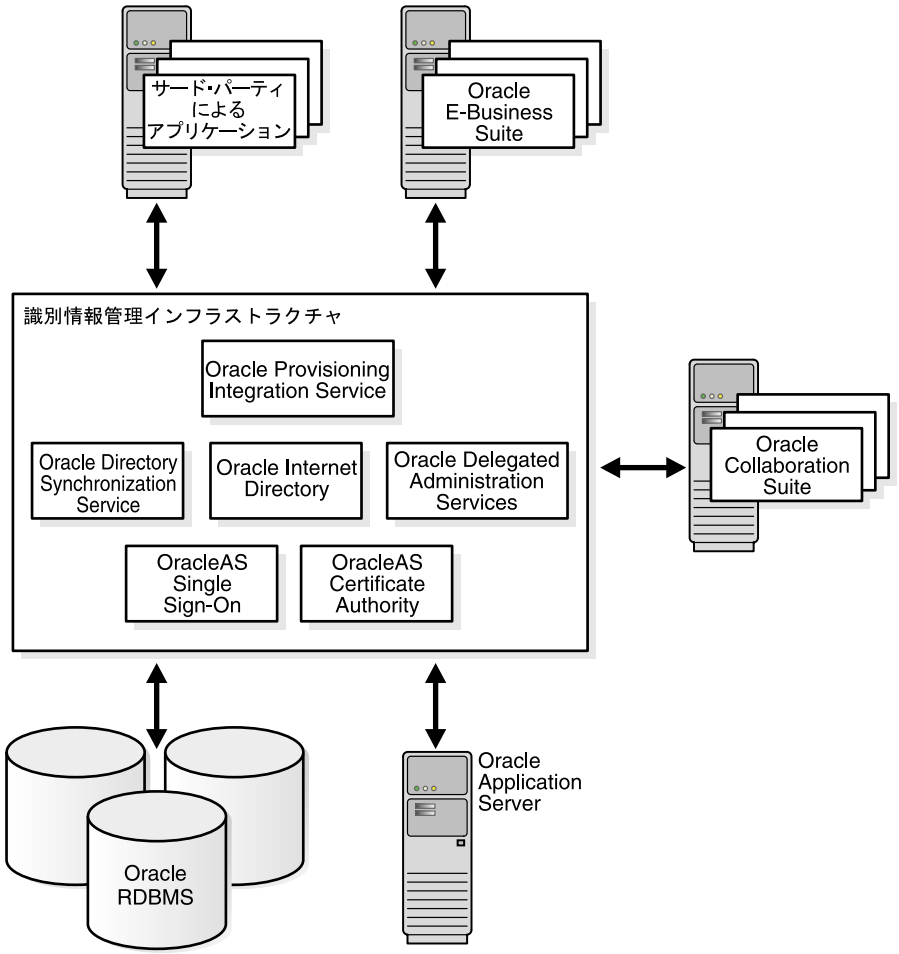
Oracle Identity Management インフラストラクチャには、次のコンポーネントが含まれます。

- **Oracle Internet Directory**: Oracle9*i* Database Server に実装される、スケーラブルで堅牢な LDAP V3 準拠のディレクトリ・サービスです。
- **Oracle Provisioning Integration Service**: Oracle Directory Integration and Provisioning のコンポーネントで、ターゲット・アプリケーションに通知を送信し、ユーザーのステータスと情報に対する変更を反映します。
- **Oracle Directory Synchronization Service**: Oracle Directory Integration and Provisioning のコンポーネントで、次のことを実行できます。
  - Oracle Internet Directory と他に接続されているディレクトリとの間で、データを同期化する。
  - 独自の接続エージェントを開発および配置する。
- **Oracle Delegated Administration Services**: Oracle Internet Directory のコンポーネントで、これによってユーザーおよびアプリケーション管理者は、信頼できるプロキシ・ベースでディレクトリ情報を管理できます。
- **Oracle Application Server Single Sign-On**（OracleAS Single Sign-On）: 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・アクセスを実現します。

- **Oracle Application Server Certificate Authority**（OCA）: X.509v3 証明書の発行、取消し、更新および公開を行い、PKI ベースの厳密認証方法をサポートします。

Oracle Identity Management インフラストラクチャは、図 1-2 に示すように、Oracle E-Business Suite や Oracle Collaboration Suite など、多種多様なアプリケーションで使用できます。

図 1-2 Oracle Identity Management



Oracle Identity Management は、Oracle 製品に対するエンタープライズ・インフラストラクチャを構築する目的で設計されていますが、ユーザーやサード・パーティが作成したエンタープライズ・アプリケーションに対して、汎用目的の識別情報管理ソリューションとしても機能します。

また、サード・パーティのアプリケーション・ベンダーは、Oracle Identity Management インフラストラクチャを検証し、適切に動作することを保証しています。

Oracle Identity Management の目的

Oracle Identity Management は、アーキテクチャに関する次の 3 つの重要な目的を達成するために設計されています。

- Oracle Identity Management は、Oracle Application Server、Oracle9*i* Database Server、Oracle E-Business Suite、Oracle Collaboration Suite など、あらゆる Oracle 製品およびテクノロジ・スタックに対する共通インフラストラクチャという役割を果たします。したがって、Oracle Identity Management は、セキュリティ、信頼性、スケーラビリティに優れたものであると同時に、Oracle 製品およびテクノロジのコアな機能と整合性がとられています。

  Oracle Identity Management は、あらゆる Oracle 製品とテクノロジ・スタックに対して一貫したセキュリティ・モデルを提供します。Oracle Identity Management のインフラストラクチャは、プランニングおよび配置を 1 度行うだけで、現在および将来にわたる Oracle 製品の配置をサポートします。

- サード・パーティによる既存の識別情報管理インフラストラクチャへの投資を有効活用し拡張するうえで、Oracle Identity Management は、セキュリティ、効率性、信頼性に優れた手段となります。

  – Oracle Identity Management は、サード・パーティの識別管理環境内で、Oracle テクノロジ・スタック全体に対する単一の一貫した統合点となります。そのため、様々な Oracle 製品をサード・パーティ環境に対して個別に構成および管理する必要がなくなります。

  – Oracle Identity Management では、Oracle Directory Integration and Provisioning を使用することで、サード・パーティのエンタープライズ・ディレクトリのプランニングと配置へのこれまでの投資を活用できます。これにより、ディレクトリのネーミング、ディレクトリのツリー構造、スキーマ拡張、アクセス制御、セキュリティ・ポリシーなど、主要な要件をマッピングおよび継承する手段が提供されます。既存のフレームワークに構築されたユーザー登録、識別情報、およびアカウント・プロビジョニング用の各プロシージャは、Oracle Identity Management の対応する操作にシームレスに組み込むことができます。

  - サード・パーティの認証サービスが使用されている場合は、現行の認証サービスを OracleAS Single Sign-On と統合することで、Oracle 環境にアクセスするユーザーもシームレスなシングル・サインオンができるようになります。主要なサード・パーティ認証プラットフォームに対して、検証済の相互運用ソリューションが構築されており、新製品に対しても、十分に定義されたインタフェースを使用して同様のソリューションを実装できます。

- Oracle Identity Management インフラストラクチャが全社的な識別情報管理の基盤となって、Oracle 製品だけでなく、企業環境に配置されたサード・パーティ・ベンダー製品もサポートできます。

  Oracle Identity Management を導入すると、Oracle およびサード・パーティのあらゆる製品に対するユーザー・プロビジョニングおよびアカウント・プロビジョニングの両プロセスが効率化されて、所有コストが下がります。また、Oracle Identity Management には、高度なセキュリティ、スケーラビリティおよび豊富な機能が備わっています。Oracle Identity Management では、関連するインタフェースすべてで業界標準がサポートされているため、様々なアプリケーション環境で使用できるように、カスタマイズと拡張ができます。

2

Oracle Identity Management の概念とアーキテクチャ

この章では、識別情報管理を効率的に配置するために、配置プランナが理解しておく必要のある概念について説明します。また、Oracle Identity Management アーキテクチャの概要と、Oracle 環境におけるアプリケーションおよびユーザーのプロビジョニング・ライフサイクルについて説明し、識別情報管理の説明でよく使用される用語を解説します。

この章には、次の項があります。

識別情報管理の用語

ここでは、識別情報管理における重要な用語および概念の一部を紹介し、その定義について解説します。

- **アカウント・プロビジョニング**: 特定のアプリケーションおよびネットワーク認証用にアカウントを作成し、そのアカウントが持つ資格を管理することで、アプリケーションが管理するリソースに対して、アカウントのアクセスを許可および制御するプロセス。
- **認証**: エンティティにより要求された認証を、その資格証明に基づいて検証するプロセス。
- **認可**: 認可ポリシーと整合性のある特定の資格を構築するプロセス。
- **認可ポリシー**: セキュリティ・プリンシパルの資格とその資格に関連付ける制約を定義する宣言。
- **一元化されたアサーション・サービス**: 認証アサーションを生成する識別情報管理インフラストラクチャの構成要素。OracleAS Single Sign-On は、認証アサーションを生成するアサーション・サービスの一例です。OCA も、生成する X.509v3 証明書が、ネットワーク・エンティティの識別情報とその資格に関するアサーションなので、アサーション・サービスの一種です。
- **資格**: ネットワークのエンティティが実行できるアクション、およびそのエンティティがアクセスできるリソース。
- **識別情報**: ネットワーク・エンティティを一意に識別する属性のセット。1 つのネットワーク・エンティティには、ネットワーク内の様々なアプリケーションへのアクセスに使用するアカウントを複数設定できます。各アプリケーションは、このエンティティに設定された複数の属性を使用することで、複数のアカウントを区別できます。たとえば、1 人のユーザーは、電子メール・サービスでは電子メール ID により、人事管理アプリケーションでは従業員番号により識別されます。こうした属性のグローバルなセットにより、エンティティの識別情報が構成されます。
- **識別情報の管理**: ネットワーク・エンティティの識別情報に関連付けられた情報を管理する行為。この情報は、識別情報管理インフラストラクチャ自体に使用され、管理権限が決められます。
- **識別情報データベース**: 識別情報を保持および管理するために設計された専用データベース・サービス。
- **識別情報管理ポリシー**: 社内の識別情報の管理に影響を与えるポリシーで、ネーミング・ポリシーやセキュリティ・ポリシーなどがあります。
- **識別情報管理レルム**: 識別情報とそれに関連するポリシーの集合で、ユーザーを集団に分割し、集団ごとに別々の識別情報管理ポリシーを適用するときなどに使用します。
- **認証ポリシー・アサーション・サービス**: エンティティの認証または認可に関する検証可能なアサーションを生成するプロセス。ネットワーク・エンティティは、エンティティがアクセスする他のサービスに、生成されたアサーションを提示します。

- **識別情報のプロビジョニング**: 識別情報の認証を容易にするために、ネットワーク・エンティティの識別情報と必要な資格証明を構築する行為。
- **ポリシー決定サービス**: アプリケーションにより保護され、アクセスが制御されるリソースに関連付けられた適用可能な資格ポリシーを解析するプロセス。アプリケーション自体に組み込まれた決定サービスに依存するアプリケーションと、一元化された決定サービスに依存するアプリケーションがあります。
- **セキュリティ・プリンシパル**: ユーザー、ユーザー・グループ、ロールなど、認可ポリシーの対象となるもの。セキュリティ・プリンシパルは、ネットワーク内での識別情報とその識別情報を証明する資格証明を持つエンティティで、それは人間でもアプリケーションでも構いません。

次の項で説明する識別情報管理の概念には、これらの用語が使用されています。

識別情報管理の概念

この項では、次の各トピックで、識別情報管理の基本的な概念について説明します。

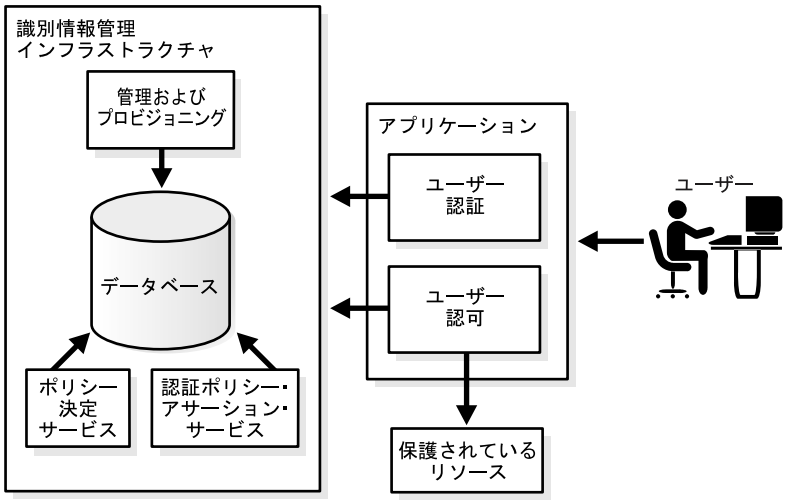
- アプリケーション・セキュリティと識別情報管理の統合
- 識別情報とアプリケーションのプロビジョニングのライフサイクル
- 管理の委任

アプリケーション・セキュリティと識別情報管理の統合

この項では、Oracle Identity Management と統合される代表的アプリケーションの管理者に対して、青写真を提供します。また、Oracle Identity Management の様々なコンポーネントとサービスの役割を理解するためのフレームワークを提供し、企業環境でアプリケーションのセキュアな配置を図る方法を理解するための基本を説明します。

図 2-1 に、アプリケーション統合モデルを示します。

図 2-1 アプリケーション統合モデル



このモデルでは、識別情報管理インフラストラクチャによって、次の重要なサービスが実行されます。

- **管理およびプロビジョニング** : 識別情報管理インフラストラクチャによって管理される識別情報に対して、管理サービスとプロビジョニング・サービスを実行します。Oracle Identity Management では、Oracle Delegated Administration Services および Oracle Directory Integration and Provisioning などのツールを使用して、これらのサービスを実行します。
- **ポリシー決定サービス** : OracleAS Portal などのアプリケーションで実行するのが一般的ですが、Oracle Identity Management では、Oracle Internet Directory によって、識別情報管理インフラストラクチャ自体にポリシー決定サービスを実行します。
- **認証ポリシー・アサーション・サービス** : Oracle Identity Management では、OracleAS Single Sign-On および Oracle Application Server Certificate Authority で実行します。

識別情報管理インフラストラクチャに配置されたアプリケーションは、次の方法でインフラストラクチャとやり取りします。

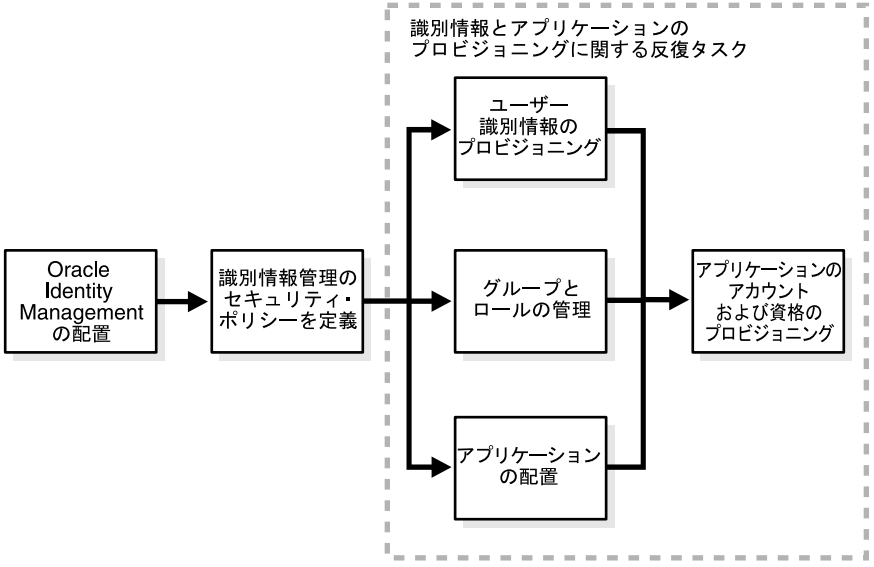
- **ユーザー認証** : ユーザーがアプリケーションにアクセスすると、識別情報管理インフラストラクチャにより提供されるサービスを使用して、ユーザーの資格証明が検証されます。アプリケーションに対する認証およびそれに関連する通信は、認証ポリシー・アサーション・サービスを使用して実行されます。たとえば、Oracle Identity Management インフラストラクチャの場合、ユーザー認証は暗号化されたブラウザ Cookie 形式での資格証明の検証になり、OracleAS Single Sign-On により実行されます。

- **ユーザー認可**: 認証が終わると、アプリケーションは、アプリケーションが保護するリソースに対してユーザーが十分な権限を持つかどうかをチェックする必要があります。アプリケーションは、識別情報管理インフラストラクチャで管理されている認証情報に基づいてユーザー認可を実行します。たとえば、J2EE アプリケーションでは、認証が終わると、Oracle Application Server Java Authentication and Authorization Service（OracleAS JAAS Provider）を使用して、Oracle Identity Management インフラストラクチャ内のユーザー情報およびロール情報にアクセスします。

識別情報とアプリケーションのプロビジョニングのライフサイクル

この項では、Oracle 環境におけるユーザー識別情報とアプリケーションのプロビジョニングの流れについて、概要を説明します。

図 2-2 識別情報とアプリケーションのプロビジョニングのライフサイクル



次に、図 2-2 に示したプロビジョニングの流れについて説明します。

1. 最初のステップでは、製品のインストール・ツールと構成ツールを使用して、Oracle Identity Management インフラストラクチャを配置します。
2. 次のステップでは、識別情報管理のセキュリティ・ポリシーを定義します。このポリシーにより、ユーザーとアプリケーションがアクセスできるデータが決まります。セキュリティ・ポリシーは Oracle Internet Directory のアクセス制御リスト（ACL）として編成され、通常は Oracle Directory Manager を使用して管理します。

3. 次の 3 つのアクティビティは、継続的に発生するものです。これらの各アクティビティは同時に実行できます。また、実行順序に制限はありません。

   - ユーザー識別情報は Oracle Internet Directory でプロビジョニングします。ユーザー識別情報は、他のディレクトリとの同期化またはディレクトリ・バルク・ロード・ツールにより、人事管理アプリケーションやユーザー管理ツール（たとえば Oracle Internet Directory Self-Service Console）など、複数のソースから取得できます。
   - グループとロールは Oracle Internet Directory で管理します。グループおよびグループ・メンバーシップは、Oracle Internet Directory Self-Service Console や他のディレクトリ・サービスとの同期化など、いくつかの方法で定義できます。
   - アプリケーション・インスタンスは Oracle Identity Management インフラストラクチャに配置します。このアクティビティでは、最初に識別情報管理インフラストラクチャの管理者が、Oracle Internet Directory の管理ツールを使用して、アプリケーション管理者にアクセス権を付与するのが一般的です。次に、アプリケーション管理者が、アプリケーションのインストール・ツールと構成ツールを使用して、アプリケーションのサポートに必要なディレクトリ・オブジェクトとエントリを作成します。

4. ユーザー識別情報、グループとロール、アプリケーションは、アプリケーションのアカウント・プロビジョニング・プロセスを通じて関連付けます。これは、アプリケーション管理ツールを使用して手動で実行することも、プロビジョニング統合によって自動的に実行することもできます。

管理の委任

Oracle Identity Management では、エンタープライズのユーザー、グループおよびサービスを管理するリポジトリを一元化する必要があります。ただし、ビジネス要件によっては、特定の管理者グループが、すべての管理情報を一元化して管理するのが困難になる場合があります。

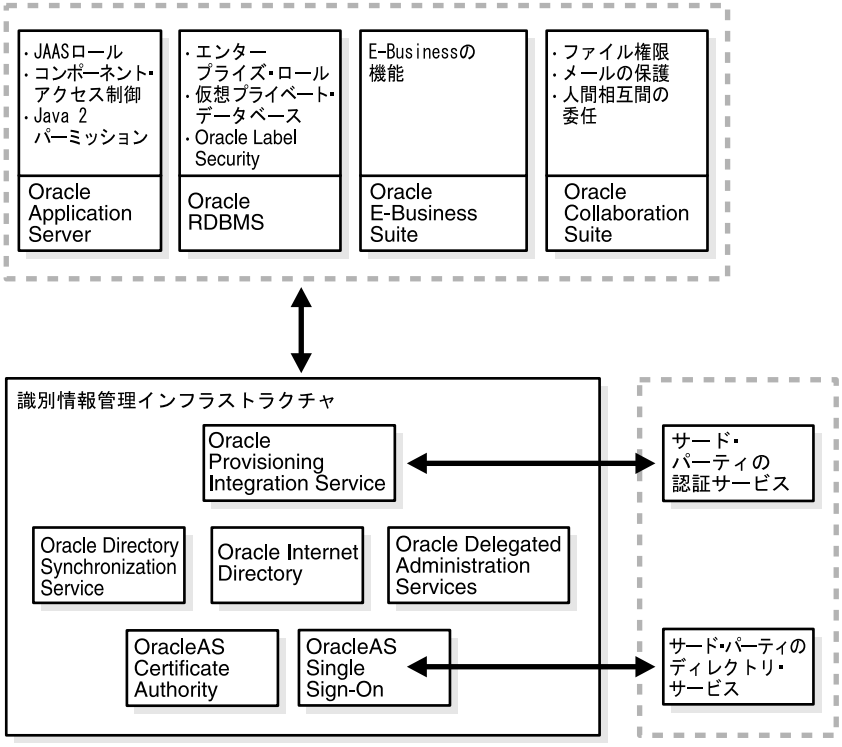
たとえば、ある業務では、エンタープライズ・ユーザー管理と電子メール・サービスで、管理者が異なる場合があります。また、財務の管理者は対象ユーザーの権限を完全に制御できる必要があり、OracleAS Portal の管理者は特定のユーザーまたはグループに対して、Web ページを完全に制御できる必要があります。このような目的の異なる管理者の必要性を満たし、異なるセキュリティ要件に対応するには、識別情報管理システムに委任管理機能が必要になります。

委任管理機能があると、識別情報管理システム内のデータの管理作業を、セキュリティ要件に応じて、多数の管理者に分散できます。一元化されたリポジトリと委任権限を組み合せることで、識別情報管理インフラストラクチャにおける管理が、セキュリティとスケーラビリティの優れたものとなります。

識別情報管理と Oracle 製品の統合

Oracle Application Server、Oracle9*i* Database Server、Oracle E-Business Suite および Oracle Collaboration Suite の各 Oracle テクノロジ・スタックは、その設計に適切なセキュリティ・モデルをサポートしています。それにもかかわらず、これらすべての製品は、図 2-3 に示すように、個々のセキュリティ・モデルとセキュリティ機能の実装に Oracle Identity Management インフラストラクチャを採用しています。

図 2-3 識別情報管理と Oracle 製品の統合



Oracle Application Server は、Java Authentication and Authorization Service（JAAS）という J2EE 準拠のセキュリティ・サービスをサポートします。JAAS は、Oracle Internet Directory に定義されているユーザーとロールを使用するように構成できます。

同様に、Enterprise User Security と Oracle Label Security のデータベース・セキュリティ機能は、Oracle Internet Directory に定義されているユーザーとロールを利用する手段を提供します。これらの両プラットフォームにより、プラットフォーム個々のネイティブなセキュリティ機能を使用して開発されたアプリケーションで、基盤となる識別情報管理インフラストラクチャを透過的に利用できるようになります。

Oracle E-Business Suite と Oracle Collaboration Suite のアプリケーション・スタックは、Oracle9*i* Database Server プラットフォームおよび Oracle Application Server プラットフォームの上の層に位置し、Oracle Identity Management インフラストラクチャと間接レベルで統合されます。また、これらの製品には、Oracle Identity Management に依存する製品固有の機能もあります。たとえば、Oracle Email や Oracle Voicemail & Fax などの Oracle Collaboration Suite コンポーネントは、コンポーネント固有のユーザー環境、個人情報、アドレス帳などの管理に、Oracle Internet Directory を使用します。

これらの Oracle テクノロジ・スタックでは、Oracle Directory Integration and Provisioning を利用して、ユーザーのアカウントおよび権限のプロビジョニングとプロビジョニング解除を自動化できます。ユーザー環境と個人情報の管理をセルフサービスで行えるように、Oracle Delegated Administration Services が幅広く使用されています。また、これらの製品のセキュリティ管理インタフェースでは、ユーザーとグループ管理に、サービス・ユニットと呼ばれる基本単位を利用します。

3

Oracle Identity Management の配置プランニング

この章では、Oracle Identity Management サービスの配置プランニングの方法論について説明します。

この章には、次の項があります。

識別情報管理の配置プランニング・プロセス

製品の配置と使用を成功させるには、識別情報管理インフラストラクチャを十分にプランニングする必要があります。

ここでは、Oracle Identity Management インフラストラクチャの配置プランニング・プロセスを、次のように説明します。

- 要件分析と、配置に関する高度な検討事項を最初に説明し、次にそれぞれの検討事項に焦点を当てた論理的な配置プランを紹介します。
- 配置プランニングの検討事項を詳しく説明します。

図 3-1 に、識別情報管理の配置をプランニングする際のプロセスの流れを示します。

図 3-1 配置プランニング・プロセス

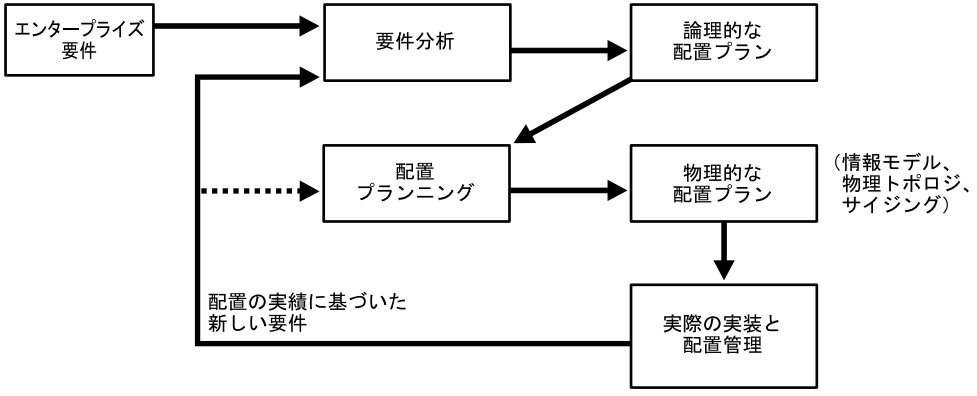


図 3-1 に示すように、配置プランニングは繰り返し行うプロセスです。最初の要件に応じて、高度なプランニングを行い論理的な配置プランを作成します。次に、その論理配置プランを使用して詳細な配置プランニングを行い、実際の実装に使用する物理的な配置プランを作成します。実装後に新しい要件が生じた場合は、分析、プランニングおよび配置の各プロセスを繰り返します。

要件分析

この項では、Oracle Identity Management の配置プランニング時に分析が必要になる代表的なエンタープライズ要件について説明します。これらの要件には、プロセスの問題、機能要件、および可用性を高めるために検討すべき事項が含まれます。この分析フェーズが終了するときには、Oracle Identity Management インフラストラクチャの高度な論理配置プランが決定します。

この項では、次のトピックについて説明します。

- 高度なエンタープライズ要件
- 要件の論理配置プランへの変換
- 要件分析のまとめ

高度なエンタープライズ要件

この項では、高度な要件について説明します。トピックの構成は次のとおりです。

- Oracle Identity Management インフラストラクチャのプランニングおよび配置担当者の決定
- 配置する Oracle Identity Management コンポーネントの決定
- 情報モデル要件の検討
- セキュリティ管理の一元化要件の検討
- エンタープライズ・アプリケーション要件の検討
- 自治的な管理要件の検討
- セキュリティ分離要件の検討
- サード・パーティの識別情報管理との統合要件の検討
- 高可用性、スケーラビリティおよびパフォーマンスの要件の検討

Oracle Identity Management インフラストラクチャのプランニングおよび配置担当者の決定

小規模な配置では、アプリケーション管理者が Oracle Identity Management のプランニング、配置および管理を担当するのが一般的です。

大規模な配置では、Oracle およびサード・パーティの各種アプリケーション間でサービスを共有するなど、識別情報管理インフラストラクチャが実現する一元サービスを利用できます。この場合は、アプリケーション、ネットワークおよびセキュリティの各管理者で構成されるグループを中央に作成して、これらのサービスを担当させるのが一般的です。このグループは、一般的に次のようなタスクを実行します。

- 識別情報管理システムの配置の設計
- 共有インフラストラクチャのセキュリティ・ポリシーの定義
- 配置の管理
- プロセスおよびログ・ファイルの監視
- パフォーマンスとマシンの負荷の監視
- 障害の発生に備えた、データのバックアップ戦略の実装とデータのリストア

配置する Oracle Identity Management コンポーネントの決定

Oracle Identity Management を構成する各コンポーネントにより、多くの管理タスクが一元化されます。

Oracle Internet Directory と OracleAS Single Sign-On は基本的な識別情報管理サービスを実現し、Oracle Delegated Administration Services は、ユーザーがパスワードをセルフサービスで管理するための中心的な手段です。これらの検討事項をふまえて、Oracle Internet Directory、OracleAS Single Sign-On および Oracle Delegated Administration Services の実装をプランニングします。

他のサード・パーティ・ディレクトリと統合する場合は、Oracle Directory Integration and Provisioning を配置します。ディレクトリ統合プラットフォームの構成には、特定のディレクトリ同期化プロファイルが使用されています。このプロファイルによって、サポートされているサード・パーティ・ディレクトリと同期化できます。

Oracle Directory Integration and Provisioning のプロビジョニング統合機能は、OracleAS Portal や Oracle Collaboration Suite など、多くの Oracle 製品で利用できるため、サード・パーティ・ディレクトリを使用しない場合でも、Oracle Directory Integration and Provisioning サービスの配置の検討は必要です。

公開鍵インフラストラクチャ（PKI）を配置する場合は、Oracle Application Server Certificate Authority を使用して証明書を発行および管理できます。サード・パーティの PKI がすでに配置されている場合は、Oracle Identity Management インフラストラクチャの他のコンポーネントと Oracle 製品を構成すると、既存の認証局を利用できます。

さらに、一部の Oracle 製品では、ユーザー認証のサポートに、Oracle Identity Management インフラストラクチャの一部コンポーネントの配置が必要になります。

注意： Oracle Identity Management の各種コンポーネントに対する個々の Oracle 製品の依存関係の詳細は、各製品の管理者ガイドを参照してください。

より小規模な Oracle インストールおよび本番前環境では、アプリケーション管理者は Oracle Identity Management インフラストラクチャの最小インスタンスをインストールして、Oracle アプリケーションをサポートできます。

関連項目： このインストールのガイドラインは、『Oracle Application Server 10*g* 管理者ガイド』を参照してください。

最後に、他の識別情報管理コンポーネントがすでに配置されている組織や、配置予定の組織もあるでしょう。Oracle Identity Management は、他のエンタープライズ向け識別情報管理ソリューションや、企業環境のプロビジョニングと管理用に配置済のアプリケーションを利用できるように設計されています。

識別情報管理が必要な Oracle コンポーネントはいずれも、Oracle Identity Management インスタンスによりサポートされます。このインスタンスと配置済のインフラストラクチャ・コンポーネントが連携することで、どちらの環境でも、透過的なユーザー管理と Web のシングル・サインオンが実現されます。

情報モデル要件の検討

Oracle Identity Management インフラストラクチャでは、ユーザーの識別情報をすべて格納するリポジトリとして、Oracle Internet Directory が使用されます。エンタープライズ・ユーザーは、社内の複数のアプリケーションにアクセスできます。ただし通常は、同一ユーザーの識別情報を表すエントリは、Oracle Internet Directory 内に 1 つのみにします。ディレクトリ情報ツリー（DIT）全体におけるユーザー・エントリの位置とその内容は、Oracle Internet Directory などの識別情報管理インフラストラクチャのコンポーネントを配置する前にプランニングする必要があります。

アプリケーション・サービス・プロバイダ（ASP）を、識別情報管理の一元化が必須となるように配置した場合、ASP 管理者や ASP の各顧客（契約者）のユーザーに対して、別々の識別情報管理レルムを作成する必要があります。

セキュリティ管理の一元化要件の検討

E-Business とエンタープライズ・アプリケーションが増大してくると、IT 部門はユーザー・プロファイル情報を再利用する方法を検討する必要があります。また、セキュリティを犠牲にしたり機密情報を漏らすことなく、社内と社外で増加するユーザーがアクセスできるようにする必要もあります。ユーザー識別情報は複数のアプリケーションに複数のバージョンがあるため、その管理はますます厄介な作業になっています。そのため、集約型の識別情報管理インフラストラクチャを検討して、アカウントの一元的な作成と管理、単一のパスワードと資格証明の管理、Web アプリケーションへのシングル・サインオンなどの機能を実現できるようにする必要があります。

エンタープライズ・アプリケーション要件の検討

通常、識別情報管理インフラストラクチャは、Oracle や他社による様々なエンタープライズ・アプリケーションで共有されます。したがって、エンタープライズ・アプリケーションの配置については、次の要件を検討することが重要です。

- **アプリケーションがサービスを提供するユーザーのタイプ**: OracleAS Portal などのエンタープライズ・アプリケーションは、内部（イントラネット）ユーザーに加えて、ビジネス・パートナなどの外部（インターネット）ユーザーが、インターネット経由でアクセスできるようにすることが必要になる場合もあります。結果として、1 つの Oracle Internet Directory にすべてのユーザー識別情報を保持するか、別々の Oracle Internet Directory にグループごとのユーザー識別情報を保持するかを検討します。
- **アプリケーションの負荷要件**: アプリケーションの負荷要件と可用性要件は、高可用性を実現できるように識別情報管理インフラストラクチャを配置することの必要性を示しています。
- **ASP 要件**: 識別情報管理の配置とは別に、ASP の配置では、アプリケーション必須の要件を検討する必要があります。

自治的な管理要件の検討

- **新規アプリケーションの配置における部門の自治性**: 多くの大企業では、独立した部門単位で、アプリケーションを自治的に管理できるようにする必要があります。こうしたケースでは、一元化された識別情報管理インフラストラクチャを維持しながら、それとは別に、アプリケーション固有のデータとともに、エンタープライズ・データの一部を格納したアプリケーション・リポジトリを部門別に作成する必要性が考えられます。
- **共通の認証情報に対する管理の自治性**: 識別情報管理をプランニングする際の重要な検討事項として、特定の業務に従事する全従業員に適用するセキュリティ・ポリシーがあります。ユーザーの識別情報は、企業のセキュリティ・ポリシーで定義する共通権限に基づいて管理できるようにする必要があります。識別情報、ロール、ポリシーおよびグループの管理には、その企業の要件に適合した管理モデルを検討します。
- **識別情報管理インフラストラクチャに配置された個々のアプリケーションに対する管理の自治性**: ある業務では、エンタープライズ・ユーザー管理と電子メール・サービスで、管理者が異なる場合があります。また、財務の管理者は対象ユーザーの権限を完全に制御できる必要があり、OracleAS Portal の管理者は特定のユーザーまたはグループに対して、Web ページを完全に制御できる必要があります。さらに、管理者は、どのユーザーがどのリソースにどのセキュリティ・レベルでアクセスできるかを定義する必要があります。こうした様々な管理者の求める必要性とそれぞれのセキュリティ要件を満たすには、管理に対する制御要件を検討します。

セキュリティ分離要件の検討

OracleAS Portal のようなエンタープライズ・アプリケーションを配置した場合、従業員と非従業員の両方がアクセスできるようにする必要があります。こうしたアプリケーションを社内と社外両方のユーザーが共有する場合でも、企業のイントラネット・リソースを非従業員から完全に分離し、エクストラネット・ポータルをターゲットとした DoS 攻撃から、イントラネット・アプリケーションを保護することが重要です。こうした場合の配置では、エンタープライズと非エンタープライズの識別情報管理インフラストラクチャ間で、セキュリティの分離が必要になります。

組織上の制約と高度な管理要件によっては、環境間に明確な境界を設け、環境を別の環境から保護するために、環境ごとに別々の識別情報管理インフラストラクチャを配置することを検討する必要性が考えられます。また、データ変更を特定の環境に限定したり、その伝播を遅延させることが必要になる場合もあります。[1]

サード・パーティの識別情報管理との統合要件の検討

サード・パーティの識別情報管理インフラストラクチャがすでに配置されている企業では、次の統合機能について検討します。

- **Windows との統合** : Active Directory や Kerberos 認証など、Microsoft Windows インフラストラクチャのコンポーネントが使用されている場合は、それらの識別情報管理コンポーネントに必要な統合について検討します。Oracle Internet Directory とのユーザー情報の同期化、OracleAS Single Sign-On 認証の統合などが、統合機能の例です。
- **ユーザー・プロビジョニング** : ユーザー・プロビジョニングとは、各種エンタープライズ・システムに新規ユーザーを追加したり、そこからユーザーを削除するプロセスです。新規ユーザーのプロビジョニングは、人事管理（HR）システム、カスタマ・リレーションシップ・マネジメント（CRM）・システム、ネットワーク管理環境など、数種類のソースから実行される可能性があります。あるシステムで新規ユーザーが作成されたときは、ユーザーの自動プロビジョニング機能により、他のエンタープライズ・アプリケーションにも必要なユーザー・アカウント・プロファイルが作成されます。

  HR や CRM などのエンタープライズ・アプリケーションが配置されている場合は、その識別情報管理システムとのユーザー・プロビジョニングの統合機能を検討します。統合後も、ユーザー・プロビジョニングは異なるソースから実行できます。
- **ディレクトリ・サービス** : iPlanet などの LDAP ディレクトリが配置されている場合は、LDAP サーバーと Oracle Internet Directory を同期化してユーザー管理を一元化することを検討します。
- **ランタイム・セキュリティ・サービスの統合** : アプリケーション・ユーザーが、サード・パーティ・ディレクトリおよび Web 認証アプリケーションに統合されているアプリケーションと、Oracle Identity Management に統合されているアプリケーションの両方にアクセスする必要がある配置の場合は、統合要件を検討し、単一のデジタル認証で Web アプリケーションに OracleAS Single Sign-On アクセスできるようにします。

[1] これらは主として高度な検討事項であり、実際のスループットや容量を計算して求めたものではありません。スループットと容量の計算は、プランニングの次の段階のチューニングとサイジングで検討するのが一般的です。

高可用性、スケーラビリティおよびパフォーマンスの要件の検討

識別情報管理インフラストラクチャでは、複数のコンポーネントが連動してサービスを提供します。識別情報管理インフラストラクチャが、重要なサービスをすべて提供するには、必要なコンポーネントがすべて使用可能である必要があります。高可用性ソリューションでは、識別情報管理のコンポーネントに関連するプロセスのあらゆるソフトウェア障害を検出し、その障害からリカバリできることが必要になります。高可用性要件は配置構成と関係するため、これらの要件は配置プランニングの一部として検討します。

パフォーマンス要件は、アプリケーションの使用方法とユーザーのトラフィックに基づいて検討する必要があります。ユーザーのトラフィックの増加に対応してアプリケーションを追加配置するときに、配置を容易に拡張できるように、配置構成をプランニングします。

3-27 ページの「ネットワークの物理トポロジのプランニング」に、高可用性、スケーラビリティ、パフォーマンスなどの要件を実装する物理トポロジを示します。

要件の論理配置プランへの変換

この項では、一般的な論理配置モデルを紹介しますので、論理配置プランを選択する際に参考にしてください。これらのモデルのいくつかに各自の要件を当てはめることで、論理配置プランを作成できます。

この項では、次のトピックについて説明します。

- 集約型の識別情報管理システムを配置するモデルー標準的なエンタープライズ・モデル
- 社内と社外のユーザーにサービスを提供するモデル
- 部門別アプリケーションの管理に自治性を与えるモデル
- Windows 環境に Oracle Identity Management を統合するモデル

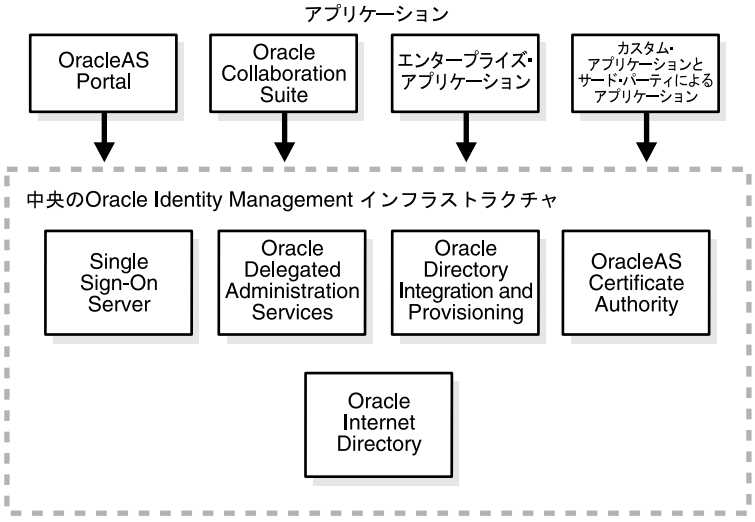
集約型の識別情報管理システムを配置するモデルー標準的なエンタープライズ・モデル

図 3-2 に示すような標準的なエンタープライズ・モデルでは、1 つの識別情報管理インフラストラクチャを一元的に配置して、組織中央のグループが管理を担当します。配置されるエンタープライズ・アプリケーションのインスタンスは、この一元化されたインフラストラクチャを使用します。一元化されたセキュリティ・モデルでは、中央のインフラストラクチャに対してアプリケーションをインストールしますが、権限は制御できます。このモデルでは、新規アプリケーションの配置と管理がずっと簡単になると同時に、アカウントの一元的な作成と管理、単一のパスワードと資格証明の管理、Web アプリケーションへのシングル・サインオンなどの機能を有効にすることで、アプリケーションの使い勝手が向上します。この配置では、すべてのユーザーに対して同じ情報モデルが使用されます。

このタイプの配置では次の実装が必要になります。

- 全社を対象とした単一コンソールによる中央管理。これによって、企業の識別情報を作成し共有プロパティを管理します。
- Oracle や他社による様々なエンタープライズ・アプリケーションで共有される識別情報管理インフラストラクチャ。
- アプリケーションの管理を委任するための管理制御。

図 3-2 中央の識別情報管理インフラストラクチャ



社内と社外のユーザーにサービスを提供するモデル

OracleAS Portal のようなエンタープライズ・アプリケーションには、社内と社外両方のユーザーがアクセスできる必要があります。その結果、エンタープライズ・アプリケーションでは、従業員と非従業員両方のプロファイルと権限情報の保持が必要になります。このような統合は効果的ですが、企業のイントラネット・リソースを非従業員から完全に分離し、エクストラネット・ポータルをターゲットとした DoS 攻撃から、イントラネット・アプリケーションを保護することも重要です。

ここでは、社内と社外のユーザーに対してアクセスを提供する 2 つの例を紹介します。どちらの例でも、エクストラネット環境やイントラネット環境などの環境間で分離が必要となるアプリケーション・グループに対して、セキュリティ環境を分離します。

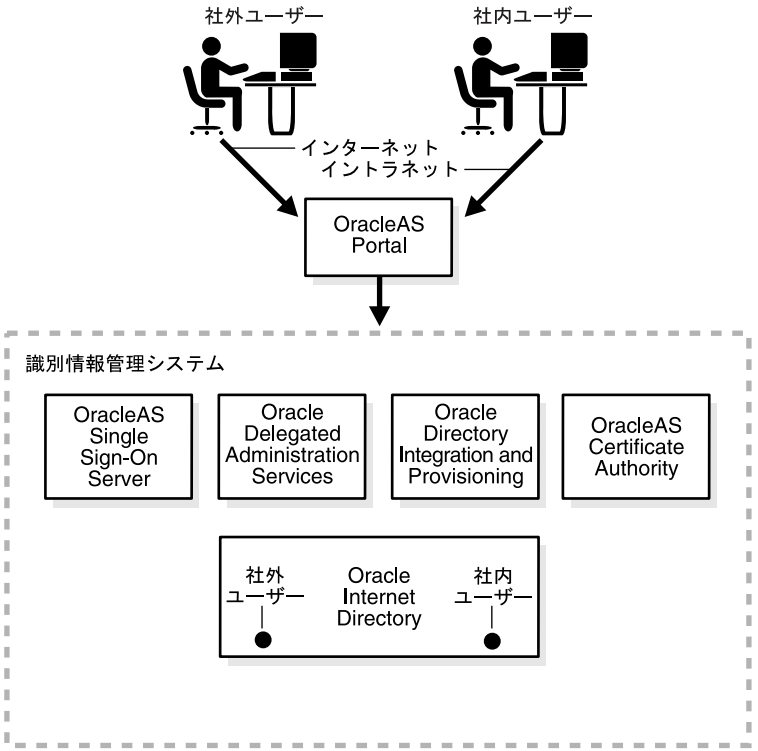
例 A: 1 つの識別情報管理インフラストラクチャの使用

図 3-3 に示すような 1 つの論理的な Oracle Internet Directory を使用して、社内と社外のユーザーのプロファイルを格納します。ユーザー情報は、社内と社外両方のユーザーで、同じモデル化が行われます。1 つの論理的な Oracle Internet Directory に両方のタイプのユーザー・プロファイルを格納するには、別々のサブツリーを使用します。パスワード・ポリシーは、両タイプのユーザーに同じものを設定できます。

このタイプの配置では次の実装が必要になります。

- 社内と社外のユーザーに対してアクセスを提供するアプリケーション配置。
- 中央でのサービスと管理。

図 3-3 1 つの識別情報管理インフラストラクチャの使用



例 B: 2 つの識別情報管理インフラストラクチャの使用 - セキュリティの分離

この例では、エンタープライズ・ネットワークの内外からアプリケーションにアクセスするユーザーに対して、それぞれ異なる 2 つの識別情報管理インフラストラクチャを使用します。図 3-4 に、このモデルを示します。このタイプの配置では、社内と社外のユーザー・リポジトリ間に明確な境界があります。社内のリソースを社外のトラフィックに公開しない場合は、可用性が向上します。

この例で説明されている分離を実現するには、多くの配置手段が必要になります。エクストラネット・ポータル用のディレクトリ・サービスの分離が主要な手段になります。エンタープライズ・ディレクトリと同期化させるのは、従業員の識別情報と機密でないプロファイル情報のみですが、イントラネット・アプリケーションの識別情報とそれに関連するメタデータはレプリケートしません。非従業員の識別情報（自己登録されたものなど）、エクストラネット・ポータル固有のユーザー・プロファイルと作業環境、エクストラネット・ポータルに配置されたアプリケーションの識別情報とロールは、専用のディレクトリに保持し、エンタープライズ・ディレクトリにはレプリケートしません。この情報モデルは、どちらの論理的な Oracle Internet Directory インスタンスでも同じです。

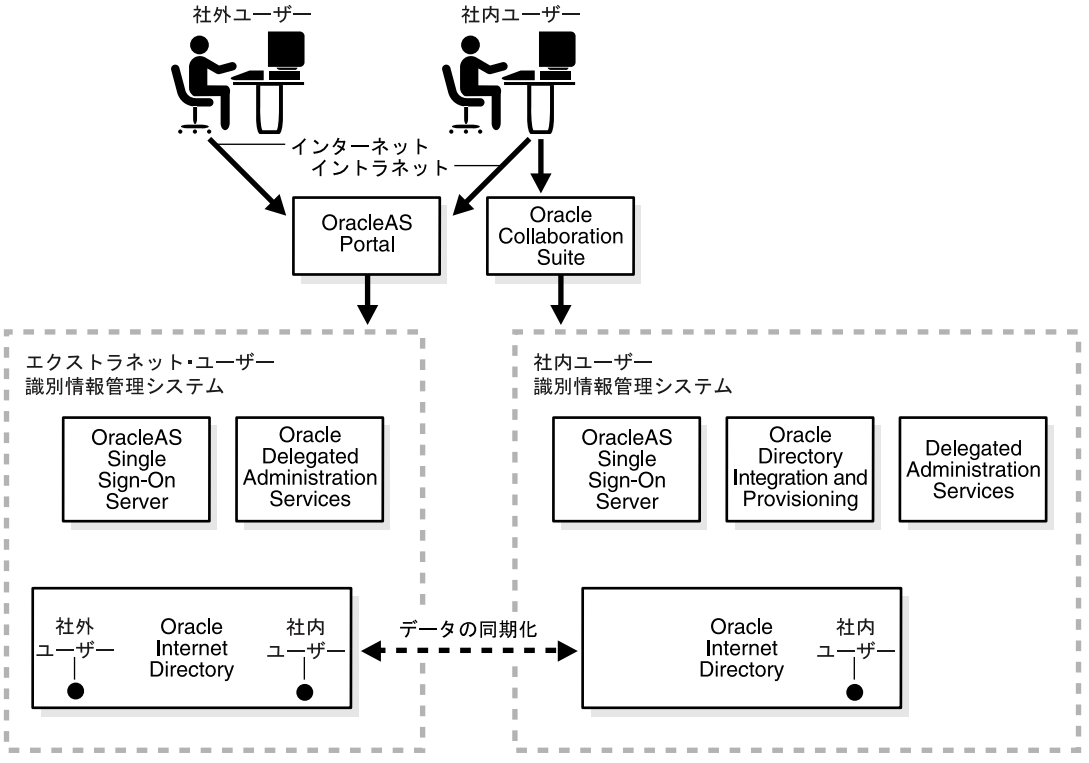
シングル・サインオン認証に対しては、DNS ベースのルーティングを使用して、別々の識別情報管理インフラストラクチャにユーザーをルーティングできます。

注意： イントラネット内のアプリケーションにアクセスする従業員は、エクストラネット・ポータルおよび、Oracle Collaboration Suite などの社内に配置された他のアプリケーションに対して、シングル・サインオンでアクセスできます。

このタイプの配置では次の実装が必要になります。

- セキュリティの分離 : エクストラネット環境やイントラネット環境などの環境間で分離が必要となるアプリケーション・グループに対して、セキュリティ環境を分離します。
- アクセス可能性 : アプリケーションには社内と社外両方のユーザーがアクセスでき、2 つの識別情報管理インフラストラクチャによりサービスが提供されます。
- データの同期化 : アプリケーション必須のデータは、2 つの識別情報管理インフラストラクチャ間で同期化されます。
- 可用性 : 社内のユーザーと社外のユーザーが、別々の識別情報管理インフラストラクチャを使用できるようにします。

図 3-4 2 つの識別情報管理インフラストラクチャの使用



部門別アプリケーションの管理に自治性を与えるモデル

多くの大企業では、独立した部門単位で、アプリケーションを自治的に管理できるようにする必要があります。このタイプの配置では、部門ネットワークおよび組織単位内で独立して管理されるアプリケーションを、自治的に管理できます。

このタイプの配置では、ファンアウト・レプリカが、自治的に管理されるアプリケーションに対するローカルなインフラストラクチャとして機能します。ファンアウト・レプリカは、レプリケートされた Oracle Internet Directory です。その構成には、中央レプリカからの一方向レプリケーションが使用されていますが、ローカル・インフラストラクチャに対しては、ローカル・アプリケーションを編集して、直接的に配置、プロビジョニングおよび管理できるように構成されています。編集したローカル情報が、中央レプリカに対して逆方向にレプリケートされることはありません。

例 A: アプリケーションに対する、中央でのシングル・サインオンと部門の自治性

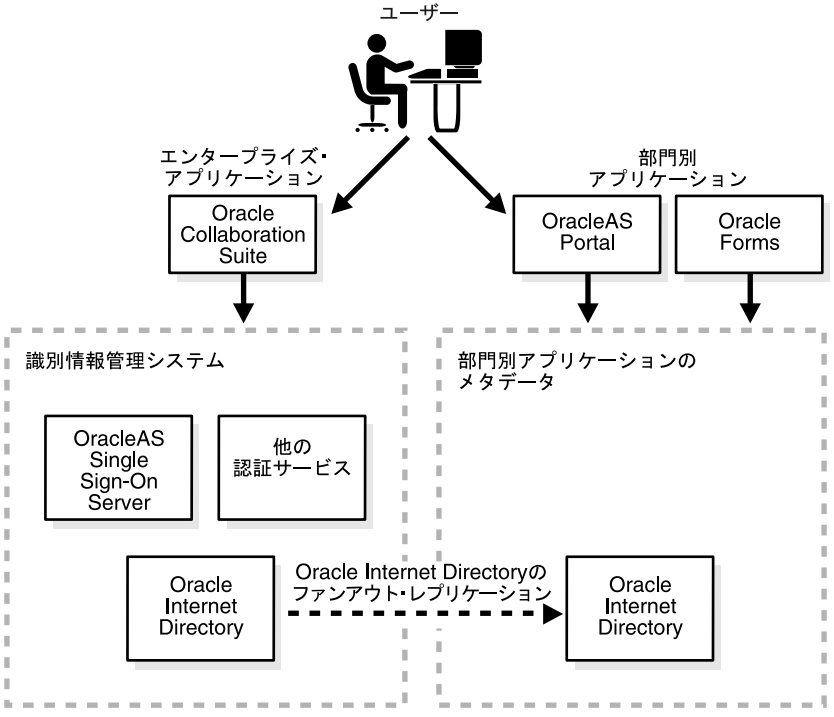
この例では、シングル・サインオンとユーザー・パスワード管理サービスを全社で一元化すると同時に、アプリケーション・データの保持には部門の自治性を導入します。図 3-5 に、このモデルを示します。一元化されたシングル・サインオンはユーザー認証に使用されます。一方、アプリケーションは、中央の Oracle Internet Directory と部門別の Oracle Internet Directory のどちらを使用するかに応じて、異なる Oracle Internet Directory インスタンスにリンクできます。

OracleAS Portal などのアプリケーションは、部門別の Oracle Internet Directory Server に対してインストールされますが、認証には中央の識別情報管理サービスを使用します。部門別アプリケーションは、各部門のローカル管理者が管理します。

このタイプの配置では次の実装が必要になります。

- 部門内のアプリケーションに対する管理上の自治性。
- 一元化された識別情報管理インフラストラクチャ。
- あらゆるアプリケーションに対する統一されたログインおよびログアウト操作。

図 3-5 中央でのシングル・サインオンと部門の自治性



例 B: 部門別の識別情報管理システム

この例では、部門ごとに別々の認証サービスを導入しますが、エンタープライズ・アプリケーションには中央の識別情報管理サービスをそのまま使用します。図 3-6 に、このモデルを示します。

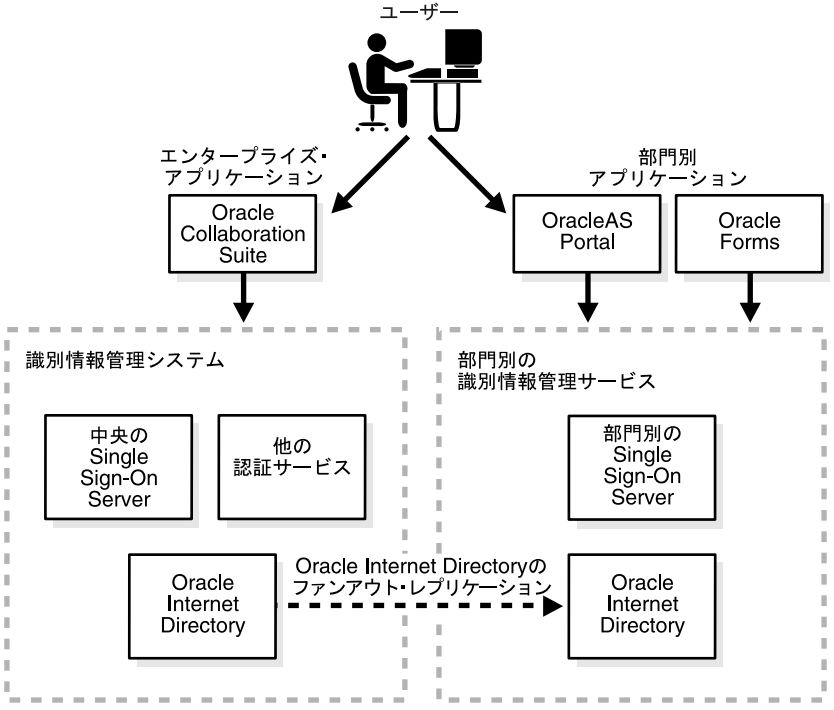
OracleAS Portal などのアプリケーションは、部門別の Oracle Internet Directory サービスおよび OracleAS Single Sign-On サービスに対してインストールされます。部門別アプリケーションは、各部門のローカル管理者が管理します。

このモデルでは、各部門内のアプリケーションでのみ、統一されたログインおよびログアウト操作が可能になります。一方、このモデルは、中央サービスに大きな障害が発生した場合に有用なフェイルオーバー・プランとなります。中央の Oracle Internet Directory から部門の Oracle Internet Directory に、エンタープライズ・ユーザーとパスワード・ポリシーの情報をレプリケートする場合は、Oracle Internet Directory のファンアウト・レプリケーションが使用されます。

このタイプの配置では次の実装が必要になります。

- 部門内のアプリケーションに対する管理上の自治性。
- 部門の自治性を図るための、複数の識別情報管理インフラストラクチャ。
- 中央の識別情報管理インフラストラクチャに障害が発生しても、部門別アプリケーションの可用性を持続する。

図 3-6 部門別の識別情報管理インフラストラクチャ



Windows 環境に Oracle Identity Management を統合するモデル

この配置では、Oracle Identity Management システムおよび、Oracle Human Resources など既存のエンタープライズ・アプリケーションと、Microsoft Active Directory などサード・パーティの LDAP サーバーを統合する方法について説明します。

例 A: エンタープライズ・プロビジョニングとの統合

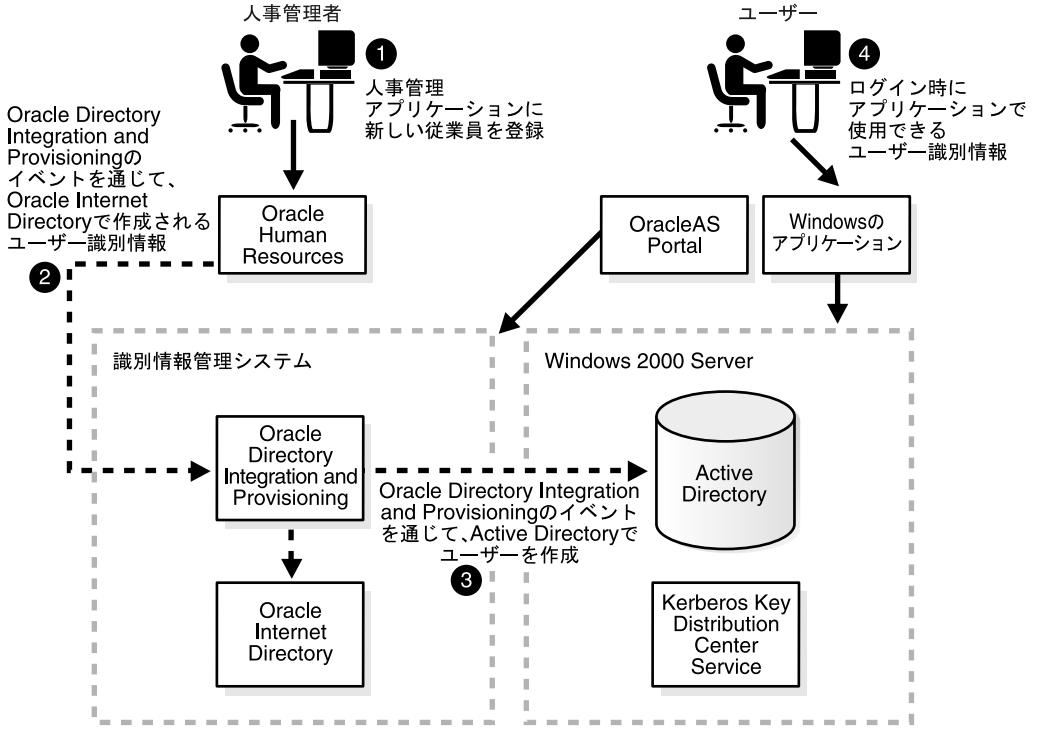
この例では、エンタープライズ・アプリケーションが、ユーザー・プロビジョニングの起点になります。次に、Oracle Directory Synchronization Service により、ユーザー・アカウント情報が Oracle Internet Directory と Active Directory に作成されます。図 3-7 に、このモデルを示します。

ユーザー識別情報が Oracle Internet Directory に作成された後は、ユーザーは OracleAS Single Sign-On により認証され、Oracle Internet Directory 対応のアプリケーションがユーザー・データにアクセスできるようになります。同様に、Windows アプリケーションは Active Directory に作成されたユーザー・データにアクセスできるようになります。

このタイプの配置では次の実装が必要になります。

- 識別情報管理システムとエンタープライズ・ユーザー・プロビジョニング・システムの統合。この場合、ユーザー・プロビジョニングはエンタープライズ・アプリケーションが起点となり、ユーザー・プロファイル・データは、アプリケーションから Oracle Internet Directory に同期化されます。
- サード・パーティのディレクトリとの統合（この例では、Active Directory との同期化）。
- ユーザー・アカウントは Oracle Internet Directory と Active Directory の両方で同期化されるため、ユーザーは Oracle Internet Directory と Active Directory のどちらかに対応するアプリケーションにアクセスできます。

図 3-7 識別情報管理インフラストラクチャとエンタープライズ・プロビジョニングの統合



例 B: Windows ユーザー・プロビジョニングとの統合

ユーザーおよびネットワーク・リソースを管理する企業ディレクトリとして Windows Active Directory が配置されている場合は、図 3-8 に示すように、Oracle Identity Management インフラストラクチャと既存の Active Directory を統合できます。

この例では、Windows 環境が、ユーザー・プロビジョニングの起点になります。Windows 管理者は、Windows ツールを使用して、ユーザー・アカウントをシステムにプロビジョニングできます。Active Directory に新しく作成されたデータと Oracle Internet Directory の同期化は、Oracle Directory Synchronization Service により実行されます。Active Directory のドメイン・ユーザー・データは、Oracle Internet Directory のデフォルト・レルムに同期化されます。社内に複数の Active Directory ドメインが配置されている場合は、1 つのレルムに複数のサブツリーを作成することで、Oracle Application Server に対する Oracle Internet Directory のエンタープライズ向きの使用形態としてモデル化できます。

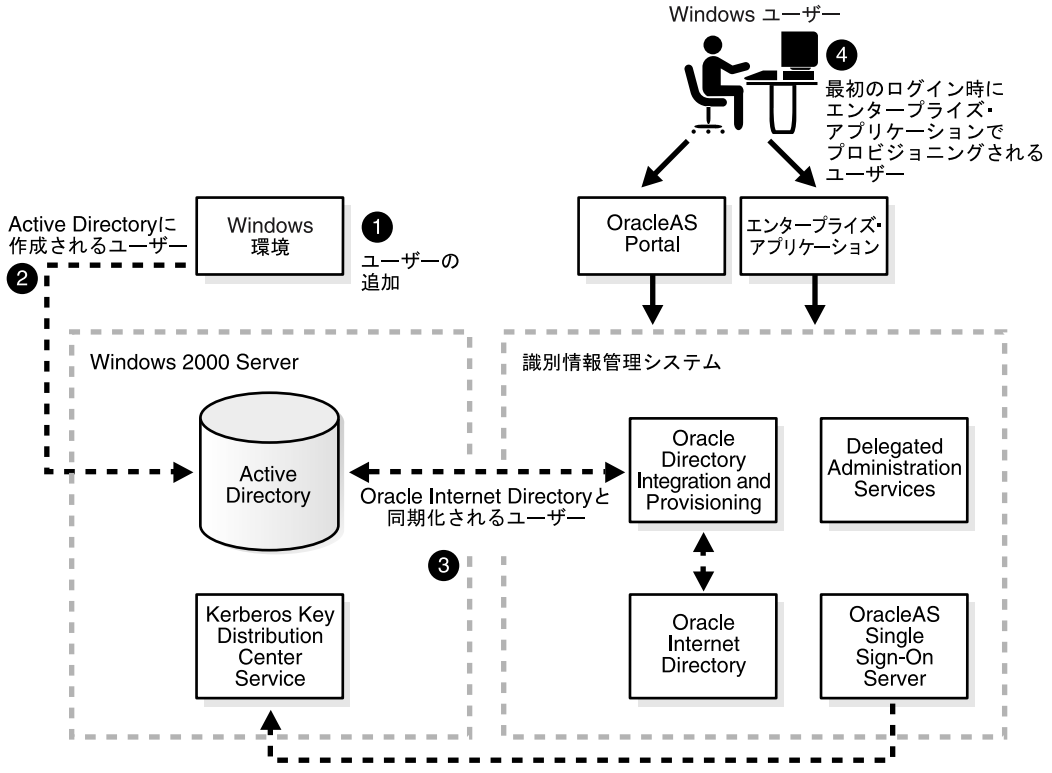
ユーザー・アカウントが Oracle Internet Directory と同期化された後は、エンタープライズ・アプリケーションはユーザー・プロファイルにアクセスでき、ユーザーは中央の OracleAS Single Sign-On を介してアプリケーションにログインできるようになります。

また、OracleAS Single Sign-On では、Windows Kerberos ベースのプロトコルを使用する Windows のネイティブ認証がサポートされます。Windows のネイティブ認証機能を使用すると、Windows 環境で有効な Kerberos チケットを発行されたユーザーは、ユーザー名とパスワードを入力しなくても Web アプリケーションにログインできます。この機能のサポートにより、Windows ユーザーは、Kerberos 対応の Windows デスクトップへのログインに成功すると、ポータル・アプリケーションにも自動的にログインできます。Windows Kerberos 認証がサポートされない場合は、Oracle Internet Directory の外部認証プラグインにより、Active Directory に対してユーザーが認証されます。

このタイプの配置では次の実装が必要になります。

- Oracle Identity Management システムと既存の Windows システムのシームレスな統合。
- サード・パーティのディレクトリとの統合。
- パートナのアプリケーションにシングル・サインオンするための Windows Kerberos 認証との統合。
- Oracle Identity Management インフラストラクチャ対応のエンタープライズ・アプリケーションへの、Windows ユーザーのシームレスなアクセス。

図 3-8 識別情報管理インフラストラクチャと Windows ユーザー・プロビジョニングとの統合



アプリケーション・サービス・プロバイダ・ホスティング環境での一元的な識別情報管理インフラストラクチャの配置

ASP の配置では、ネームスペースの異なるユーザー・グループに対して、別々の識別情報管理レルムを作成する必要があります。ASP 管理者は、自社の顧客または契約者、あるいはその両方に対してホスティングするアプリケーションを管理します。各契約者は特定の識別情報管理レルムと関連付けられ、そのユーザー、グループおよび関連するポリシーが ASP により管理されます。この配置では、ASP 契約者ごとに異なるレルムを使用することで、ASP のすべての識別情報管理サービスには、識別情報管理インフラストラクチャを 1 つしか使用しない点に注意してください。

Oracle Internet Directory で複数のレルムを使用することとは別に、OracleAS Single Sign-On、および OracleAS Portal や Oracle Collaboration Suite などのアプリケーションで、マルチ・レルム機能を有効にする必要があります。

図 3-9 に、Acme と XY Corporation という 2 つの企業に対してホスティングする配置を示します。

図 3-9 ホスティングされた配置での複数の識別情報管理レルム

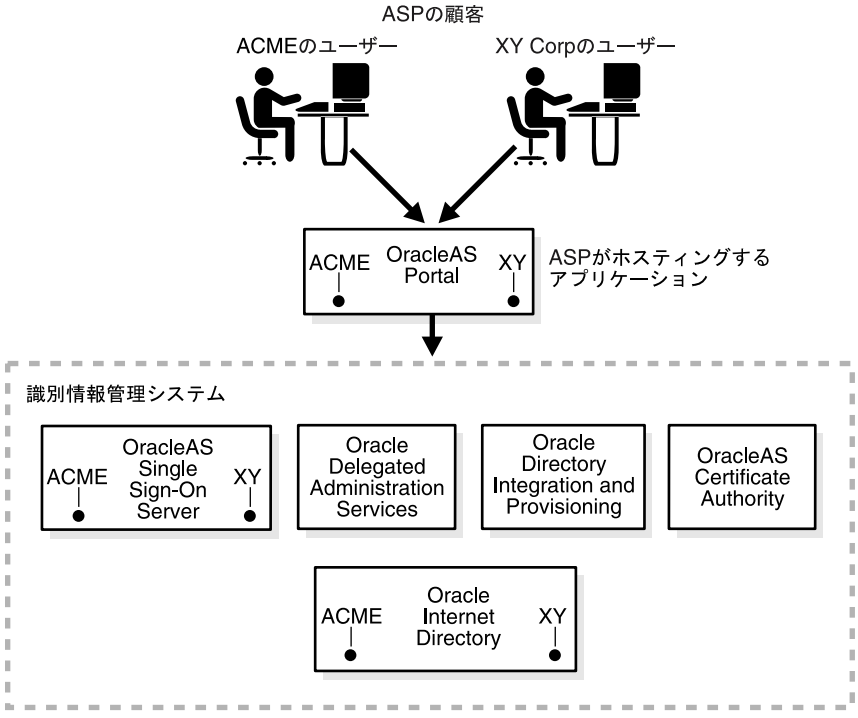


図 3-9 に示すように、デフォルトの識別情報管理レルムに定義されている ASP ユーザーが、契約者に対してホスティングする各種アプリケーションを管理します。各契約者は特定の識別情報管理レルムと関連付けられ、そのユーザー、グループおよび関連するポリシーが ASP により管理されます。

要件分析のまとめ

この項では、高度なプランニングの実践プロセスとして、エンタープライズの一般的な配置において検討すべきいくつかの要件と検討事項について説明しました。また、様々な論理配置プランについて説明しましたので、Oracle Identity Management インフラストラクチャの最適な論理アーキテクチャを選択する際に参考にしてください。論理的な配置を決定する主な要件として、エンタープライズの統合、管理制御要件、アプリケーションの配置などの要件を説明しました。

要件分析プロセスの最後に、1 つまたは複数の論理的な識別情報管理インフラストラクチャで構成される Oracle Identity Management の配置に、高度な論理アーキテクチャを選択します。これは、詳細な配置プランニングの基礎となるもので、次の項で説明します。

詳細な配置プランニング

Oracle Identity Management 配置の論理アーキテクチャが決定されたら、次のステップとして、配置に関する詳細な追加事項を決定します。これらの事項には、ディレクトリ情報モデルの編成や物理トポロジの詳細などがあります。

この項では、次のトピックについて説明します。

- ディレクトリ情報の論理編成のプランニング
- ネットワークの物理トポロジのプランニング
- 詳細な配置プランニングのまとめ

ディレクトリ情報の論理編成のプランニング

ディレクトリ情報はディレクトリ情報ツリー（DIT）で編成されます。ここでは、DIT の定義の詳細について説明します。配置プランナは、企業の目的をレビューすると同時に、企業のニーズに最適な構成を特定し、配置プランニングの指針として使用します。

図 3-10 Oracle Internet Directory の情報ツリー

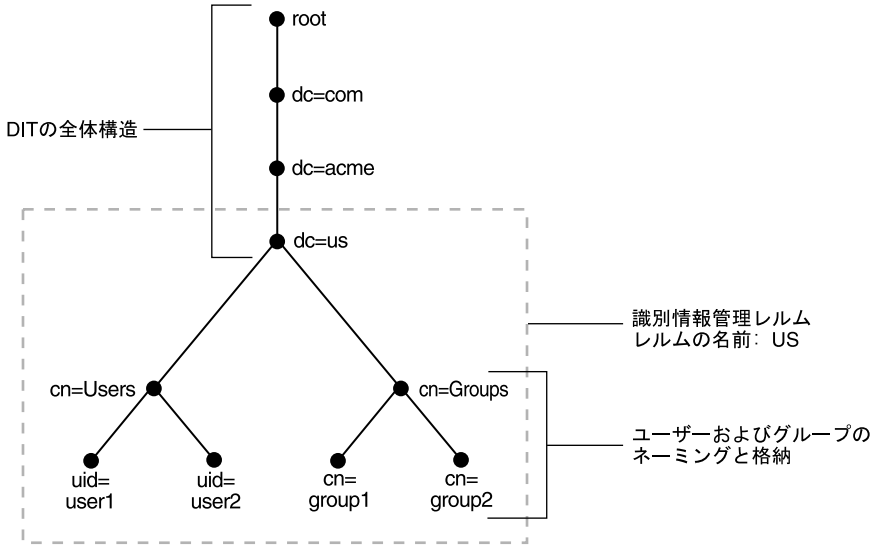


図 3-10 に、Acme という名前の仮想企業の DIT を示します。この例では、米国に配置するという前提で、ディレクトリ情報の論理編成が次のように決められています。

- DIT の階層全体を表すには、ドメイン名ベースのスキーマを使用します。識別情報管理インフラストラクチャの配置先が米国のため、全情報を表す DIT に dc=us,dc=acme,dc=com が使用されています。
- すべてのユーザーは、cn=users というコンテナ内に表されます。このコンテナ内では、すべてのユーザーが同じレベルで表されます（これよりも下に階層はありません）。また、全ユーザーに対する一意の識別子として、uid 属性が選択されています。
- エンタープライズ・グループはすべて、cn=groups というコンテナ内に表されます。このコンテナ内では、すべてのエンタープライズ・グループが同じレベルで表され、全グループ・エントリに対するネーミング属性は cn です。
- 識別情報管理レルムのルートにはコンテナ dc=us が選択されており、これは US を表しています。この配置では、US レルム内のすべてのユーザーに、同種のセキュリティ・ポリシーを適用することを前提としています。

Oracle Internet Directory は識別情報管理インフラストラクチャ全体の共有リポジトリとなるため、DIT を適切にプランニングすると、次のような利点がもたらされます。

- Oracle Identity Management インフラストラクチャでは、配置要件を反映したセキュリティ・ポリシーを適用できます。
- ディレクトリ・サービスのより効果的な物理配置の実装が容易になります。
- ディレクトリ・サービスに投資済の企業の場合は、Oracle Internet Directory との同期化を迅速にセットアップできます。

この項では、次のトピックについて説明します。

- ディレクトリ情報ツリーの全体構造のプランニング
- ユーザーおよびグループのネーミングと格納のプランニング
- 識別情報管理レルムのプランニング

ディレクトリ情報ツリーの全体構造のプランニング

このタスクの目的は、基本的な DIT 階層を設計することです。この階層は、識別情報管理に統合する社内のすべてのアプリケーションで使用します。これには、次の点を考慮します。

- ディレクトリの編成により、効果的なアクセス制御が可能になります。完全レプリケーションと部分レプリケーションのいずれかの実装をプランニングする場合、ディレクトリ・レプリケーションに正しい境界とポリシーを適用できるのは、DIT 設計にそうした分離が反映されている場合のみです。

- サード・パーティのディレクトリ・サーバーと統合する場合は、既存の DIT に合せて Oracle Internet Directory の DIT を設計し、必要となる同期化プロセスを簡略化します。この点は、他のベンダーが提供するソフトウェアを動作させるのに、Active Directory など、他のディレクトリを将来的に配置するプランが必要となる場合、Oracle Internet Directory の現行の配置に対しても利点があります。こうしたケースでは、サード・パーティのディレクトリの配置プランで定義済の DIT 設計と整合性のある DIT 設計を Oracle Internet Directory に選択することで、同期化タスクが大幅に管理しやすくなります。
- 一企業における設計では、その企業の DNS ドメイン名に合せた DIT 設計を選ぶだけで十分です。たとえば、`acme.com` というドメイン名を持つ企業に Oracle Internet Directory をセットアップする場合は、`dc=acme,dc=com` のようなディレクトリ構造をお薦めします。`engineering.acme.com` の `engineering` のような、部門または組織レベルのドメイン構成要素の使用は避けます。
- X.500 ディレクトリ・サービスが配置されていて、他のサード・パーティの LDAP ディレクトリが本番環境にない場合は、国ベースの DIT 設計を選択することをお薦めします。たとえば、X.500 ディレクトリ・サービスを配置済の企業では、ルートを `o=acme,c=US` にした DIT 設計がより適しています。

ディレクトリは Oracle とサード・パーティ両方の複数アプリケーションで使用される可能性があるため、DIT の全体構造を構築する相対識別名に使用するネーミング属性は、定式の属性に限定します。次の属性は、通常、大半のディレクトリ対応アプリケーションで定式化されています。

- **`c`**: 国の名前
- **`dc`**: DNS ドメイン名の構成要素
- **`l`**: 市区町村や郡など、地域を表す名前
- **`o`**: 組織の名前
- **`ou`**: 組織単位の名前
- **`st`**: 州（都道府県）の名前

DIT 設計でよくある間違いの 1 つは、企業の部門構造や組織構造を反映させた DIT を設計することです。通常、部門構造や組織構造は頻繁に変更されるため、こうした設計はお薦めできません。企業ディレクトリは組織変更からできるかぎり独立させることが重要です。

ユーザーおよびグループのネーミングと格納のプランニング

DIT の設計全体に適用される設計上の検討事項の大半は、ユーザーおよびグループのネーミングと格納にも適用できます。ただし、Oracle Internet Directory でユーザーとグループをモデル化する際には、このほかにも注意が必要となる事項があります。

ユーザー識別情報に関する検討事項

Oracle Identity Management インフラストラクチャでは、すべてのユーザー識別情報のリポジトリとして Oracle Internet Directory が使用されます。1 人のユーザーが社内の複数のアプリケーションにアクセスできるアカウントを持つ場合でも、同一ユーザーの識別情報を表すエントリは、Oracle Internet Directory には 1 つしかありません。DIT 全体におけるユーザー・エントリの位置とその内容は、Oracle Internet Directory などのインフラストラクチャ・コンポーネントを配置する前にプランニングする必要があります。

ユーザー識別情報をプランニングするときは、次の点を検討します。

- ディレクトリの全体構造のプランニングと同様に、現行の所属部門と部門階層に基づいたユーザーの編成は避けます。そのかわりに、ユーザーの所属部門情報は、ユーザーのディレクトリ・エントリの属性として記録します。
- ユーザーを所属部門や管理階層に基づいて階層編成しても、パフォーマンス上の利点はありません。そのため、ユーザー識別情報を記録する DIT はできるだけフラットにします。
- 異なる編成による維持と管理が必要な複数のユーザー・グループを配置する場合は、管理上の境界に基づいてコンテナにユーザーを分割編成し、アクセス制御の設定を簡略化することをお薦めします。これは、レプリケーションが必要となる場合にも効果的です。
- ユーザーの一意な識別に使用するデフォルト属性は、`CN` または `CommonName` です。通常、`CommonName` の値は個人のフルネームになるため、この値の一意性は必ずしも保証されません。かわりに、ユーザーを一意に識別する属性には、`uid` 属性や `mail` 属性を使用します。
- 通常、大半の企業では、人事部門が、従業員に一意の名前と番号を割り当てるルールを策定します。ディレクトリ・エントリにおいて一意のネーミング構成要素を選択するときは、この管理ルールを活用して、そのポリシーに従います。
- ディレクトリに作成されるユーザー・エントリはすべて、オブジェクト・クラスの `inetOrgPerson` と `orclUserV2` に所属する必要があります。
- サード・パーティのディレクトリを使用している場合または将来的に配置するプランがある場合は、分散ディレクトリ間での同期化およびそのために必要となる管理を簡略化できるように、ユーザーのネーミングとディレクトリの格納は、サード・パーティのディレクトリで一般的に使用されているものに合せてプランニングします。

グループ識別情報に関する検討事項

Oracle Identity Management インフラストラクチャに統合されるアプリケーションでは、Oracle Internet Directory の配置で作成される全社的なグループに基づいて認可を実行することもできます。ユーザー識別情報と同様に、グループ識別情報の位置とその内容も、注意深くプランニングする必要があります。

グループ識別情報をプランニングするときは、次の点を検討します。

- エンタープライズ・グループを所属部門や所有権に基づいて階層編成しても、パフォーマンス上の利点はありません。グループ識別情報を記録する DIT はできるだけフラットにして、すべてのアプリケーションが容易にグループを発見できるようにし、アプリケーション間でグループの共有を促進します。
- DIT 内ではユーザーとグループを分離して、エントリの集合ごとに異なる管理ポリシーを適用できるようにします。
- グループを一意に識別する属性には、cn または CommonName を使用します。
- ディレクトリ内のすべてのグループ・エントリを、オブジェクト・クラスの groupOfUniqueNames と orclGroup に所属させることをお薦めします。groupOfUniqueNames は、グループを表すインターネット標準です。orclGroup を使用すると、グループの管理にセルフサービス・コンソールを利用できます。
- 全社的なグループごとに新しいディレクトリ・アクセス制御を作成するのではなく、グループの所有者属性を使用して、このグループを所有する 1 人または複数のユーザーをリストし、次に、所有者属性にリストされているすべてのユーザーに対して、変更や削除などの特定の権限を付与する高レベルのアクセス制御ポリシーを作成することを検討します。
- description 属性に、テキストによる説明を移入し、ユーザーがグループの目的を容易に理解できるようにすることを検討します。
- Oracle Delegated Administration Services ユニットおよびセルフサービス・コンソールに、よりわかりやすいグループ名を表示できるように、orclGroup オブジェクト・クラスから displayName 属性を移入することを検討します。
- 管理ポリシーの異なる複数の編成による維持と管理が必要な複数のグループを配置する場合は、管理上の境界に基づいてコンテナにグループを分割編成し、アクセス制御の設定を簡略化することをお薦めします。これは、レプリケーションが必要となる場合にも効果的です。
- サード・パーティのディレクトリを使用している場合または将来的に配置するプランがある場合は、分散ディレクトリ間での同期化およびそのために必要となる管理を簡略化できるように、グループのネーミングとディレクトリの格納は、サード・パーティのディレクトリで一般的に使用されているものに合せてプランニングします。

識別情報管理レルムのプランニング

ここまでの項では、DIT の全体構造を構築し、ユーザーとグループを配置するためのガイドラインについて説明しました。こうしたガイドラインに合せた実装では配置構成が過多になる場合があるため、ディレクトリ自体のメタデータにある配置指針を取得します。このメタデータを使用することで、Oracle Identity Management インフラストラクチャに依存する Oracle ソフトウェアおよび他のサード・パーティ・ソフトウェアは、配置指針を把握し、カスタマイズされた環境で問題なく動作できます。

Oracle Internet Directory の識別情報管理レルムでは、この配置指針を取得して、エンタープライズのユーザーおよびグループに関連する識別情報管理ポリシーを配置に対して設定できます。

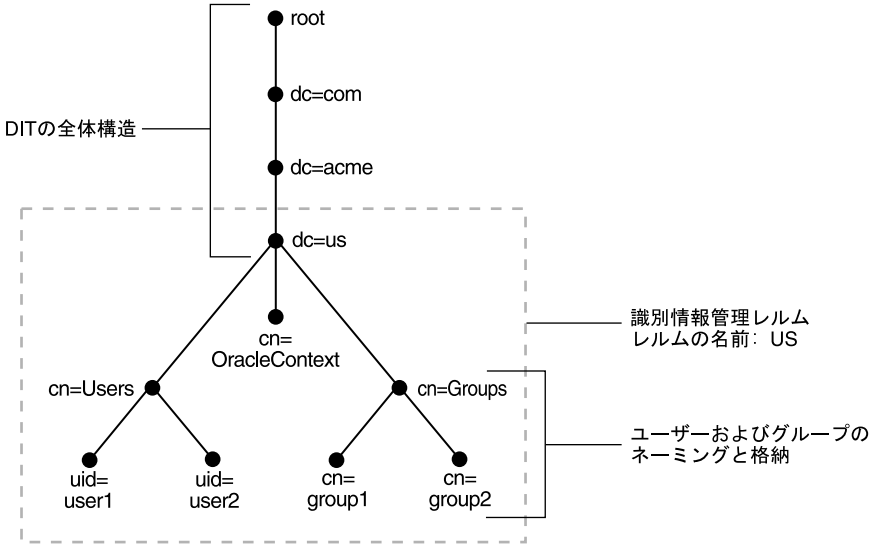
> **関連項目：** 識別情報管理レルムの詳細は、2-2 ページの「識別情報管理の用語」を参照してください。

DIT の全体構造とユーザーとグループの配置場所を選択したら、Oracle Internet Directory で識別情報管理レルムのルートになるディレクトリ・エントリを特定します。このエントリは、識別情報管理レルムで定義される識別情報管理ポリシーの有効範囲を決める役割を持ちます（デフォルトでは、識別情報管理レルムのルートの下にあるすべてのディレクトリ・サブツリーが有効範囲になります）。このエントリの下には、`OracleContext` という名前の特別なエントリが作成されます。そこに格納される内容は次のとおりです。

- 配置に固有の DIT 設計（ユーザーおよびグループのネーミングや配置場所など）
- このレルムに関連付けられた識別情報管理ポリシー
- Oracle アプリケーションには公開されないレルム固有の追加情報

図 3-11 に、ドメイン名ベースの DIT 構造を使用する、Acme という仮想企業での配置を示します。

図 3-11 識別情報管理レルム



このケースでは、コンテナ dc=us,dc=acme,dc=com が、識別情報管理レルムのルートとして選択されたディレクトリ・エントリになります。cn=OracleContext コンテナには、ユーザーおよびグループのネーミング・ポリシーや格納ポリシーなど、レルム固有のポリシーが保持されます。

新しい識別情報管理レルムは、dc=us をルートにして作成されます。この識別情報管理レルムの有効範囲は、デフォルトでは、このルートの下にあるすべてのサブツリーに限定され、その名前は US となります。

Oracle Internet Directory で識別情報管理レルムをプランニングするときは、次の点を検討します。

- 社内のセキュリティ要件に応じて、識別情報管理レルムのルートを選択する必要があります。通常、大半の企業では、Oracle Internet Directory で必要となる識別情報管理レルムは 1 つのみです。
- サード・パーティのディレクトリを使用している場合または将来的に配置するプランがある場合は、分散ディレクトリ間での同期化およびそのために必要となる管理を簡略化できるように、サード・パーティのディレクトリの DIT 設計に合せて、識別情報管理レルムのルートを選択します。
- Oracle Internet Directory での識別情報管理レルムのセットアップと管理には、Oracle Internet Directory の管理インタフェースを使用します。そのインタフェースには、Oracle Internet Directory Configuration Assistant、Oracle Internet Directory Self-Service Console、および他のいくつかのコマンドライン・ツールがあります。
- 識別情報管理レルムをセットアップした後は、新しい配置によるカスタマイズを反映させるために、ディレクトリのネーミング・ポリシーと格納ポリシーの更新をプランニングします。この更新は、Oracle Identity Management インフラストラクチャを使用する他の Oracle アプリケーションをインストールして使用する前に実行する必要があります。

関連項目：

- 識別情報管理レルムのカスタマイズの詳細は、『Oracle Internet Directory 管理者ガイド』を参照してください。
- デフォルト・モデルの詳細は、付録 A「Oracle Internet Directory のデフォルト設定」を参照してください。

ネットワークの物理トポロジのプランニング

識別情報管理インフラストラクチャの物理トポロジの選択は多くの要件に影響されますが、その中で最も一般的なものは高可用性とスケーラビリティです。個々の識別情報管理インフラストラクチャで高可用性とスケーラビリティを実現するには、Oracle Application Server Active Failover Cluster などのオプションを使用できます。

高可用性とは、システムが処理と機能を継続できる時間が、稼動時間のうち相当高い割合を占めることをいいます。高可用性は、単一の障害箇所がシステム全体の障害になるのを防ぎ、冗長な構成を使用することで実装できます。同様に、複数の識別情報管理コンポーネント・インスタンスとロード・バランサを連結すると、可用性の高い環境を実現できます。

ここでは、高可用性とスケーラビリティを実現する物理トポロジをわかりやすく図式化して紹介し、それぞれの配置例の利点について説明します。各自の企業目標をレビューし、要件に最も適合する構成を選択する必要があります。

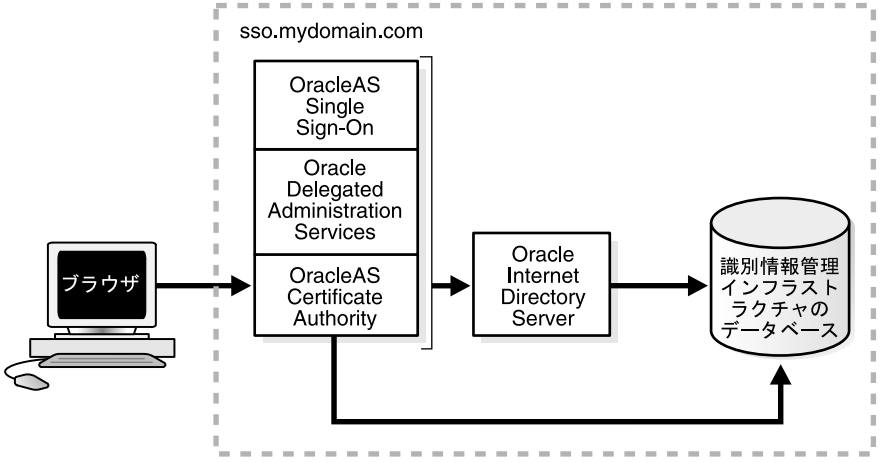
この項では、次のトピックについて説明します。

- 識別情報管理インフラストラクチャのデフォルトの配置
- DMZ ネットワークへの識別情報管理インフラストラクチャの配置
- 複数の中間層を使用する識別情報管理インフラストラクチャの配置
- コールド・フェイルオーバー・クラスタ・ソリューションを 使用する識別情報管理インフラストラクチャの配置
- Active Failover Cluster への識別情報管理インフラストラクチャの配置
- 識別情報管理インフラストラクチャのレプリケーション
- レプリケートされたディレクトリ環境でのアプリケーションの配置
- 地理的に分散された識別情報管理インフラストラクチャの配置
- 識別情報管理インフラストラクチャの、障害時リカバリを考慮した配置
- Oracle Application Server Certificate Authority の推奨される配置

識別情報管理インフラストラクチャのデフォルトの配置

Oracle Application Server Infrastructure のデフォルトのインストール構成では、図 3-12 に示すように、OracleAS Single Sign-On、Oracle Application Server Certificate Authority、Oracle Delegated Administration Services など、すべてのインフラストラクチャ・コンポーネントが同一のシステムにインストールされます。

図 3-12 OracleAS Single Sign-On と Oracle Delegated Administration Services のデフォルトの配置



この配置は簡単で、リポジトリと Oracle Internet Directory の一部として、OracleAS Single Sign-On、Oracle Application Server Certificate Authority および Oracle Delegated Administration Services が、自動的に構成されます。この配置は、開発環境またはテスト環境を迅速にセットアップする場合に適しています。

DMZ ネットワークへの識別情報管理インフラストラクチャの配置

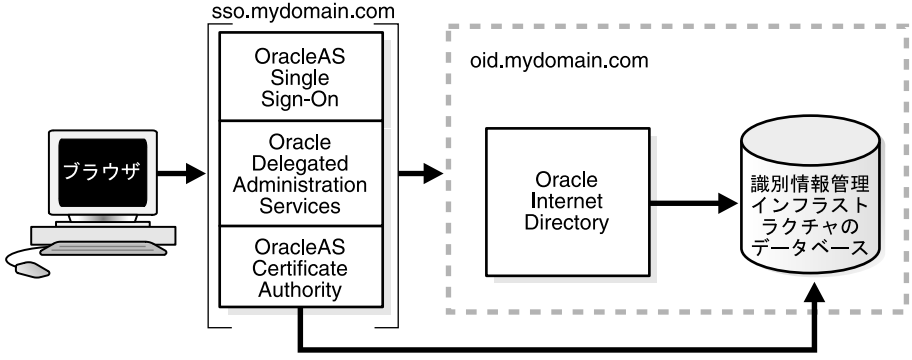
本番環境の配置では、セキュリティ・ポリシーの指定により、OracleAS Single Sign-On Server 全体をパブリック・ネットワークに公開しない場合があります。こうしたケースでは、図 3-13 に示すように、配置を分割し、Oracle Application Server Infrastructure の中間層を DMZ に配置し、Oracle Internet Directory とその基盤となるデータベースを、イントラネット・ファイアウォールの内側に配置します。

Oracle Delegated Administration Services と Oracle Application Server Certificate Authority は中間層のコンポーネントとなるため、これらに関する検討事項は OracleAS Single Sign-On の中間層に関する検討事項と同じです。

この配置では、インフラストラクチャの中間層と、Oracle Internet Directory およびその基盤データベースとの間で、セキュリティが分離されます。

Oracle Application Server Certificate Authority の中間層とリポジトリ間でセキュリティを分離するには、その両者間にネットワーク・レベルの暗号化が必要になります。

図 3-13 OracleAS Single Sign-On、Oracle Delegated Administration Services、Oracle Application Server Certificate Authority を DMZ に配置するモデル

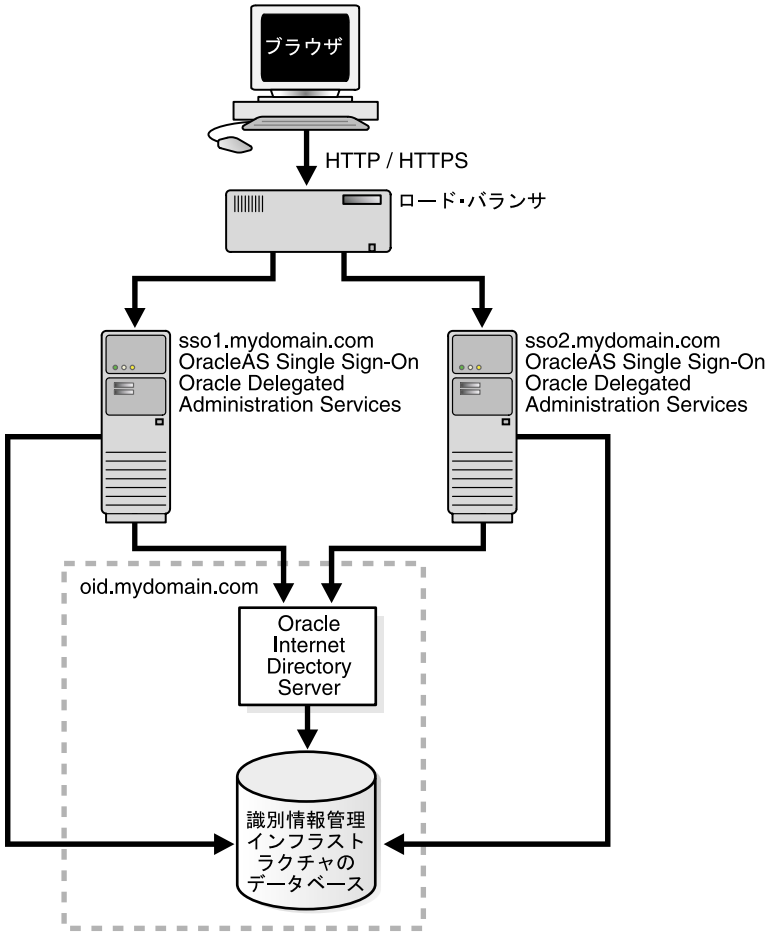


複数の中間層を使用する識別情報管理インフラストラクチャの配置

高可用性が要求される配置では、OracleAS Single Sign-On および Oracle Delegated Administration Services の中間層を複数配置することで、負荷を調整すると同時にフェイルオーバー処理をサポートできます。OracleAS Single Sign-On の中間層を複数配置しても、同じ Oracle Internet Directory Server が使用されます。

図 3-14 に示すこの配置では、インフラストラクチャ中間層をさらに追加でき、スケーラビリティも向上します。

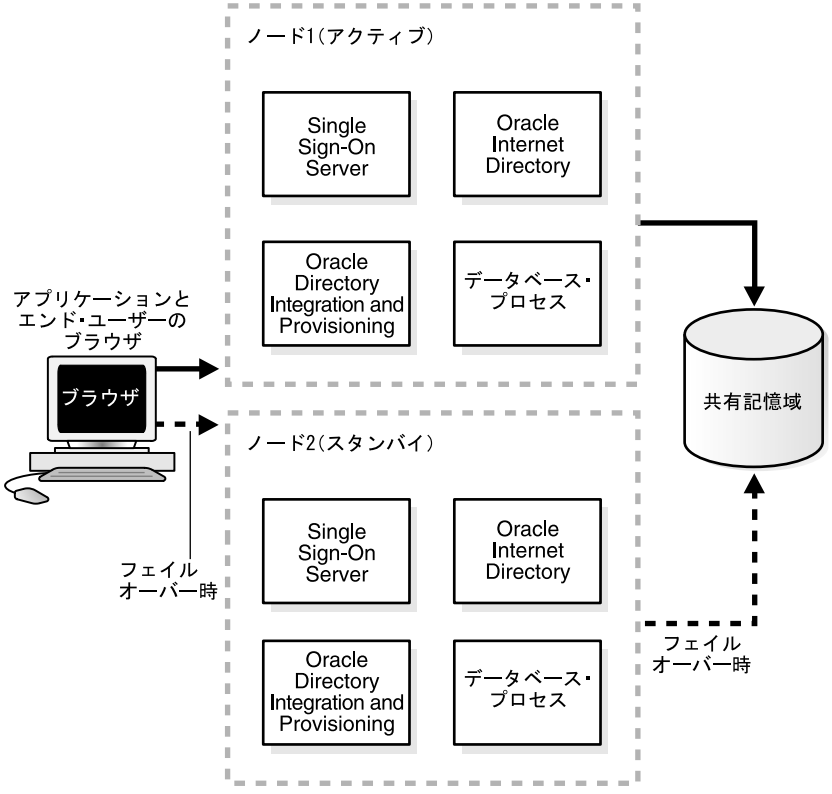
図 3-14 OracleAS Single Sign-On と Oracle Delegated Administration Services の複数の中間層で、Oracle Internet Directory Server を 1 台使用するモデル



コールド・フェイルオーバー・クラスタ・ソリューションを使用する識別情報管理インフラストラクチャの配置

コールド・フェイルオーバーは、ローカルなハードウェアおよびソフトウェアの障害からサイトを保護する、高可用性ソリューションです。こうした障害の例には、システム・パニックやノード・クラッシュなどがあります。

図 3-15 コールド・フェイルオーバーを使用する Oracle Internet Directory の配置



2 つのノード・ハードウェアによるクラスタを使用して高可用性を実現します。図 3-15 に示すように、2 つのノードが共有記憶域に接続され、仮想的な論理 IP アドレスが物理ノードの一方（ノード 1）でアクティブになります。したがって、ノード 1 が 1 次ノードまたはアクティブ・ノードになります。両方の物理ノードからアクセスできる共有記憶域ディスクには、Oracle Identity Management インフラストラクチャを 1 つだけインストールします。

1 次ノードに障害が発生した場合は、論理的な IP アドレスが 2 次ノードに引き継がれます。次に、インフラストラクチャのすべての処理が 2 次ノードで開始されます。識別情報管理インフラストラクチャにアクセスするアプリケーション・プロセスでは、論理 IP と共有記憶域が引き継がれ、データベースやデータベース・リスナーなどのすべてのプロセスが起動するまでの間、一時的にサービスが停止します。

コールド・フェイルオーバー・ソリューションは、フェイルオーバー時に一時的なサービスの停止を伴う高可用性ソリューションです。

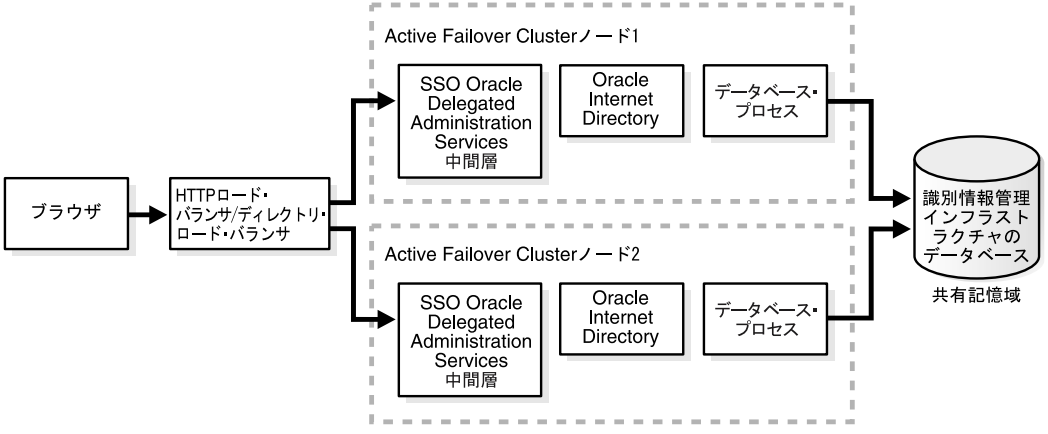
Active Failover Cluster への識別情報管理インフラストラクチャの配置

Oracle Application Server では、Active Failover Cluster への Oracle Application Server Infrastructure のインストールがサポートされます。Oracle Application Server Infrastructure のデフォルト・インストールでは、図 3-16 に示すように、OracleAS Single Sign-On（Oracle Application Server Containers for J2EE と Apache を含む）、Oracle Delegated Administration Services、Oracle Internet Directory、データベースなど、すべてのインフラストラクチャ・コンポーネントが 1 つの Active Failover Cluster ノードにインストールされます。

フェイルオーバー・アクセスには、HTTP および Oracle Internet Directory のロード・バランサが使用されます。OracleAS Single Sign-On では、JDBC のフェイルオーバー・サポートを使用するデータベース・フェイルオーバーが可能です。Oracle Internet Directory を構成する際には、接続時フェイルオーバーと透過的アプリケーション・フェイルオーバーという、2 種類のデータベース・フェイルオーバー方式を使用できます。

Active Failover Cluster の配置では、OracleAS Single Sign-On 中間層、Oracle Internet Directory Server およびデータベースに、高可用性とフェイルオーバー・アクセスが実現されます。

図 3-16 Active Failover Cluster への OracleAS Single Sign-On および Oracle Delegated Administration Services の配置



識別情報管理インフラストラクチャのレプリケーション

高可用性が要求される配置では、OracleAS Single Sign-On の中間層を複数配置することで、負荷を分散すると同時にフェイルオーバー・アクセスをサポートできます。また、Oracle Internet Directory はレプリケーション環境にセットアップでき、それにより中間層からのアクセスに対して、Oracle Internet Directory Server の高可用性を実現できます。図 3-17 に、この配置を示します。

この配置は、Oracle Application Server Infrastructure をインストールする前にプランニングする必要があります。このプランニングには、OracleAS Single Sign-On Server および Oracle Internet Directory Server への URL の指定、インフラストラクチャ中間層と Oracle Internet Directory の両方に対するロード・バランサのセットアップが含まれます。

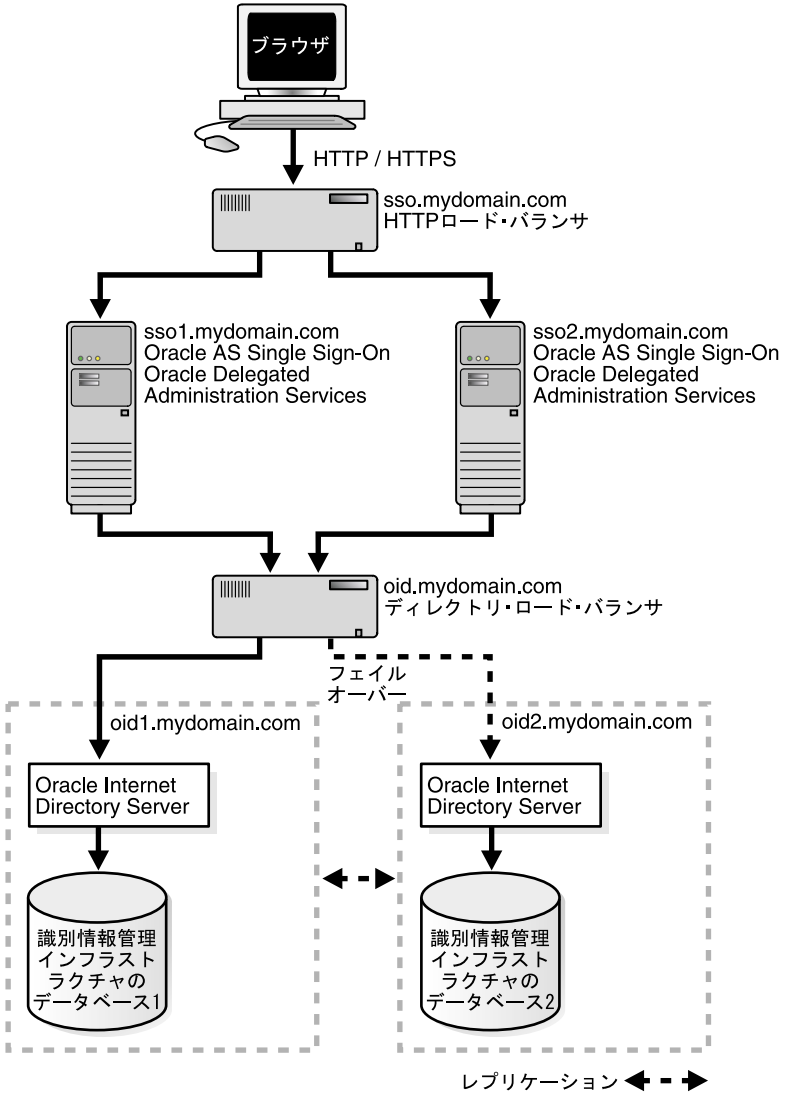
Oracle Internet Directory へのロード・バランサの構成には、永続的（ステートフル）なルーティングとフェイルオーバーを使用します。ロード・バランサは、ロード・バランス要求に対して構成しないでください。

この配置では、Oracle Internet Directory Server と OracleAS Single Sign-On 中間層のそれぞれに対して、高可用性とフェイルオーバーが組み込まれます。

Oracle Internet Directory のマルチマスター・レプリケーション・ネットワークには、次のような利点があります。

- **単一の障害箇所にならない**: 識別情報のレプリカを複数持つことで、ネットワーク上のアプリケーションに対して、ディレクトリ・サービスが単一の障害箇所になるのを防止します。
- **透過的なフェイルオーバー**: ネットワーク・レプリカのフロントエンドに適切なロード・バランサや構成可能なルーティング要素を配置することで、Oracle Internet Directory のノードが使用不能になった場合に、ネットワークの代替ノードに対して、アプリケーションが透過的にフェイルオーバーされます。
- **ロード・バランス**: ロード・バランサを導入して、レプリケーション・ネットワークの Oracle Internet Directory ノード間にアプリケーションとユーザーのアクセス要求を分散することで、1 つのノードがオーバーロードしてパフォーマンスが低下することがなくなります。

図 3-17 レプリケートされた Oracle Internet Directory ネットワーク。OracleAS Single Sign-On および Oracle Delegated Administration Services の中間層を複数使用。



レプリケートされたディレクトリ環境でのアプリケーションの配置

ディレクトリのレプリケーションは非同期方式のため、ネットワーク内のディレクトリ・ノードは常に整合性がとられているわけではありません。このディレクトリ・レプリケーション方式で保証されるのは、ネットワーク内の特定のノードで実行された変更が、最終的には他のすべてのノードに適用され、許容可能な時間内に同期化されることです。ただし、この方式では、すべてのノードがリアルタイムでいつも同じであることは保証されません。

レプリカ間の緩やかな結合の結果として、レプリケーション・ネットワークにおいて、異なる物理ディレクトリ・サーバーに接続された異なるアプリケーション間では、参照するディレクトリに一時的な不一致が生じる場合があります。こうした一時的な不一致は多くの場合許容範囲内で、アプリケーション・ユーザーの操作に悪影響を与えることはありません。ただし、状況によっては、ユーザーに影響する場合もあります。たとえば、パスワードのリセット時に、その変更内容が OracleAS Single Sign-On に接続されているディレクトリ・サーバーに即座に反映されないと、ユーザーを混乱させたり、利便性が損なわれます。

非同期レプリケーションによる一時的な不一致に加えて、マルチマスター・ネットワークでは、異なるディレクトリ・ノードにある同じ情報に対して異なる変更が同時に行われるというように、変更の競合が発生する可能性があります。競合が発生した場合、Oracle Internet Directory レプリケーションでは、競合解消と呼ばれる調停プロセスを使用して、複数のノード間で情報を収束することができます。

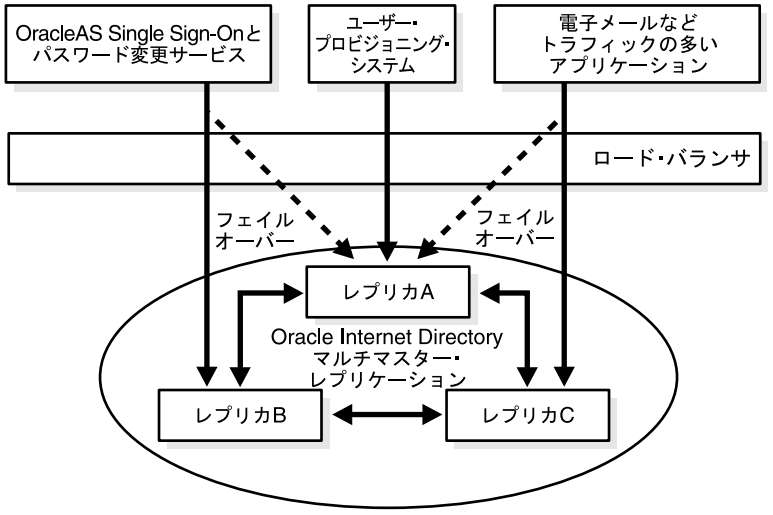
この問題を回避するには、レプリケートされたディレクトリ・ネットワークにアプリケーションを配置するときに、適切な実践方法に従うことが重要です。レプリケートされたネットワーク環境にディレクトリ対応アプリケーションを配置するときに、管理者が考慮すべきガイドラインを次に示します。

1. 企業のディレクトリ・データの主要カテゴリごとに、1 次レプリカを指定します。
   a. 1 次レプリカに適用する典型的なカテゴリはユーザー・エントリおよび一般的なユーザー属性で、それにはユーザー・パスワードなどの認証資格証明、ユーザー・グループと配置一覧、ユーザーのプロファイル、作業環境および主要なアプリケーション・スイートに関連付けられたロールなどが含まれます。
   b. 1 次レプリカを指定することが単一のマスター環境を意味するわけではありません。実際は、マスター・ノードは複数あり、その中で、ディレクトリ・データの異なるカテゴリのプロビジョニングごとに異なるノードが指定されます。ディレクトリまたはネットワークに障害が発生すると、プロビジョニング・アプリケーションは他のアプリケーションと同じように、代替マスターに一時的にフェイルオーバーすることができます。
   c. この配置方法では、マルチマスター・ネットワークが持つ柔軟性と、単一マスター構成が持つ緊密なデータ整合性が組み合されています。
      – 特定のカテゴリに属すデータのリカバリは、複数マスター間での調停が不要になるため、管理が容易になります。
      – パスワード認証サービスなど特定の属性の変更が重要となるサービスでは、最新の値について、関連付けられた 1 次レプリカに左右される場合があります。

2. アプリケーションの中間層とバックエンド・サーバー・コンポーネントは、レプリケーション・ネットワーク内の特定のディレクトリ・サーバー・インスタンスを使用するように配置します。
   - アプリケーションの中間層とバックエンド・サーバー・コンポーネントでは、均一的なロード・バランシングと配置は不適切であるため、お薦めできません。たとえば、OracleAS Single Sign-On Server での一続きのログイン操作が、異なる Oracle Internet Directory Server にルーティングされた場合、ログインの再試行制限などの認証ポリシーを効果的に適用できなくなります。
   - 均一的な負荷分散は、エンド・ユーザーによるアドレス帳の参照など、重要でない操作にのみ適しています。
3. 関連するアプリケーションの中間層とバックエンド・サーバー・コンポーネントは、ディレクトリ・サーバー・インスタンスを共有するように配置します。異なるアプリケーション・グループは、異なるディレクトリ・インスタンスを共有できます。
   - この方法は、関連するアプリケーションが、それらが依存する異なるディレクトリ・サーバー間での一時的な不一致に影響されないことを保証します。たとえば、パスワードのリセットに使用する OracleAS Single Sign-On とヘルプデスク・アプリケーションは、同じ Oracle Internet Directory インスタンスを共有する必要があります。そうでない場合、OracleAS Single Sign-On Server が、パスワードの変更がされていない別の Oracle Internet Directory Server に接続されるため、ユーザーがパスワードをリセットした後にサインオンできなくなります。
4. ディレクトリへのデータの大量プロビジョニングは、ディレクトリ・ネットワークとディレクトリ・ネットワーク内のすべてのノードが正常な状態のときに実行します。
   - ディレクトリ・ネットワークのどこかに機能不全があるとき、レプリケートや調停を必要とする変更のバックログが過度にあるときなどは、大量プロビジョニングを続行すると、問題が悪化したりデータとサービスが全面的に損なわれるおそれがあります。
   - レプリケーション環境の稼動状況の監視と診断は、定期的に実行する必要があります。Oracle Internet Directory には、これらの操作をサポートするツールが用意されています。

これらのガイドラインを考慮に入れた、レプリケートされたディレクトリ環境でのエンタープライズ・アプリケーションの構成例を図 3-18 に示します。この配置では、OracleAS Single Sign-On と、Oracle Delegated Administration Services などのパスワード変更サービスが、1 次サーバーとしてレプリカ B を使用し、一時的なフェイルオーバー・サーバーとしてレプリカ A を使用するように構成されています。同様に、電子メールなどトラフィックの多いアプリケーションは、1 次サーバーとしてレプリカ C を使用し、フェイルオーバー・サーバーとしてレプリカ A を使用するように構成されています。

図 3-18 レプリケートされた環境でのエンタープライズ・アプリケーションの構成



地理的に分散された識別情報管理インフラストラクチャの配置

支店が地理的に分散されている企業では、複数の OracleAS Single Sign-On インスタンスを地理的に異なるロケーションに分散配置して、ローカルにユーザーを認証できれば便利です。図 3-19 に示すようなこの配置では、認証に関連するネットワークのラウンドトリップが減り、アプリケーションへのアクセスがより速くなります。OracleAS Single Sign-On Server データはすべての支店間でグローバルにレプリケートされるため、従業員が他の支店に出張する場合にも、認証はローカルに実行できます。

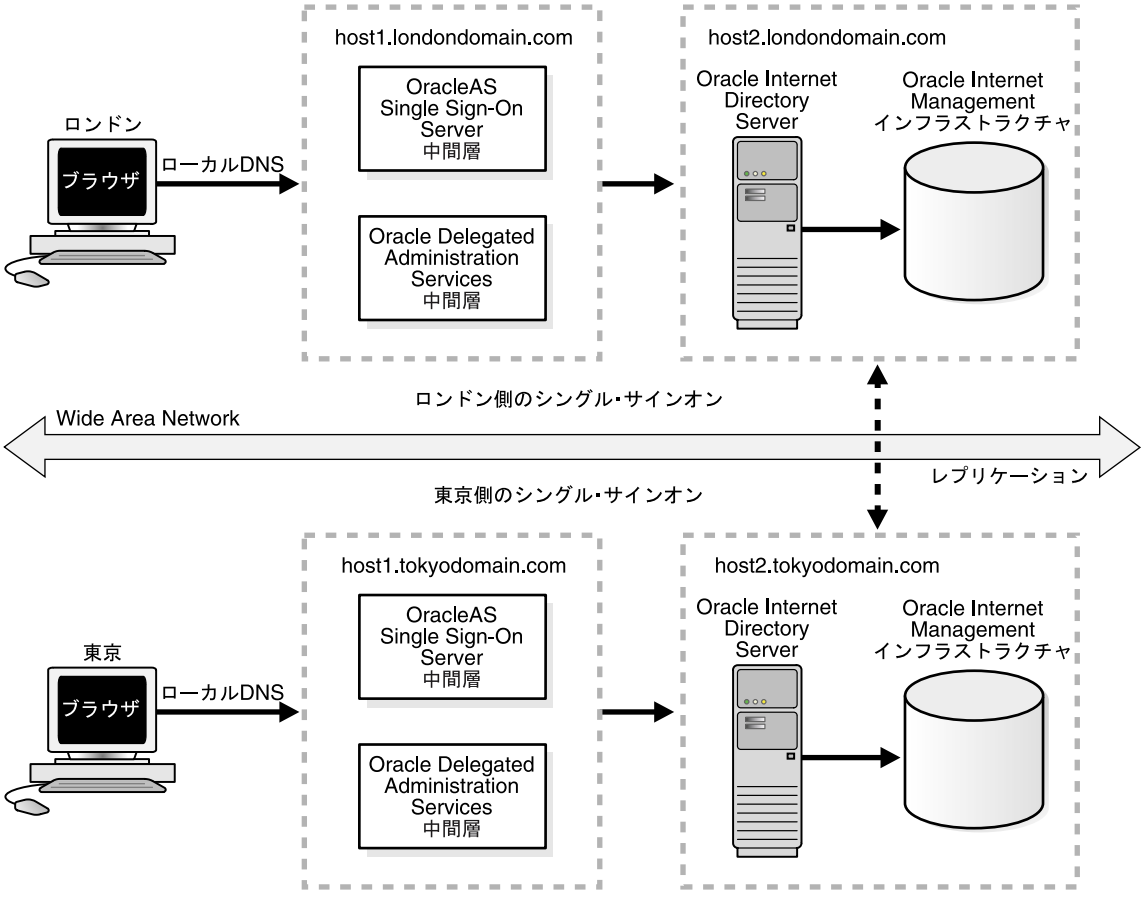
複数の地理的なロケーションにアプリケーションが配置されている企業では、少なくとも 2 つの地域に対して、Oracle Internet Directory レプリカを物理的に配置することが重要です。この構成により、（ネットワークの障害や自然災害などによる）地域的な可用性の問題が、従属アプリケーションのグローバルなサービス停止につながるのを防止できます。

Oracle Internet Directory とデータベースがレプリケーション環境にセットアップされている場合でも、OracleAS Single Sign-On の各サイトでは、そのローカル・サイトに配置されている専用の Oracle Internet Directory とデータベースが使用されます。

レプリケートされた OracleAS Single Sign-On サイトが Wide Area Network（WAN）を超えて分散する場合は、ユーザー・リクエストが地理的に最も近いサイトにルーティングされるようにローカル DNS サーバーを構成する必要があります。

あるサイトでデータベースの障害が検出された場合は、別のサイトにあるデータベースを指すように、Oracle Internet Directory Server および OracleAS Single Sign-On Server が再構成されます。OracleAS Single Sign-On 中間層の障害が検出された場合は、リモートの中間層にトラフィックをルーティングするように、ネットワークが再構成されます。

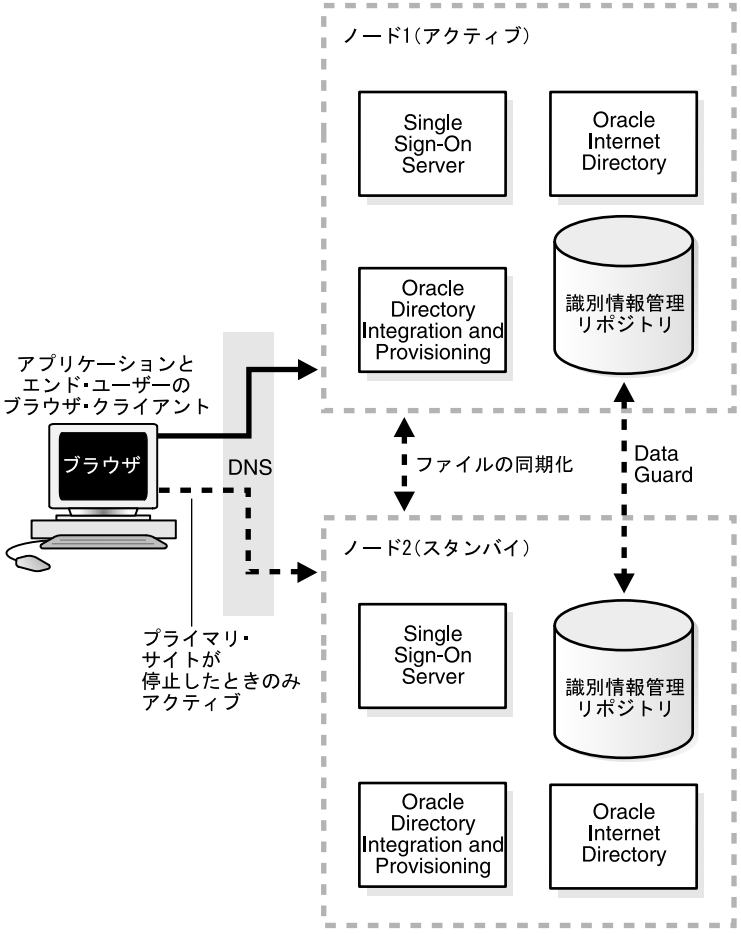
図 3-19 地理的に分散された配置



識別情報管理インフラストラクチャの、障害時リカバリを考慮した配置

障害時リカバリとは、自然災害によるサイトの障害からシステムをリカバリする方法を指します。自然災害による障害には、地震、台風、洪水、火災などがあります。単純な定義では、障害時リカバリは、データベースおよび構成ファイルを含むサイト全体のレプリケートと、ハードウェアまたはサブコンポーネントの置換を意味します。最も厳重な意味での要件には、災害時にサービスの実行が継続されることが含まれます。この配置なら、識別情報管理インフラストラクチャは、データの損傷や損失につながるサイトの障害やメディアの障害からも保護されます。

図 3-20　Oracle Data Guard を使用した Oracle Internet Directory の配置



識別情報管理インフラストラクチャの単一インスタンスなどの認証ソフトウェアは、Oracle Data Guard を装備した複数のデータ・センターで実行できるため、データ・センターの障害から保護されます。Oracle Data Guard では、単一インスタンス・ディレクトリのデータ・リカバリと透過的なフェイルオーバーもサポートされます。

図 3-20 に示すように、Oracle Data Guard は、スタンバイ用の識別情報管理インフラストラクチャを物理的に維持し、Oracle Identity Management の 1 次インフラストラクチャと同期化するように構成されます。Oracle Internet Directory と他の Oracle Internet Directory コンポーネントは、識別情報管理の 1 次インフラストラクチャのデータベース・ノードで起動します。

障害時リカバリ中は、スタンバイ・ノードが 1 次ノードに切り替わり、仮想ホスト名がスタンバイ・ノードに引き継がれ、識別情報管理プロセスがスタンバイ・ノードで開始されます。

Oracle Application Server Certificate Authority の推奨される配置

本番環境の配置では、Oracle Application Server Certificate Authority は別のホストにその固有のリポジトリとともに配置することをお薦めします。Oracle Identity Management インフラストラクチャの他のコンポーネントには、このドキュメントで説明されている任意の構成方法を採用できます。

Oracle Application Server Certificate Authority ホスト・システムは、次のガイドラインに加えて、可能なかぎりのあらゆる方式を使用して安全にする必要があります。

- Oracle Application Server Certificate Authority システムへの物理的なアクセスは厳しく制御します。
- オペレーティング・システムは強固に保護し、システムに対するユーザー・アカウントは制限します。
- Oracle Application Server Certificate Authority のリポジトリは、データベースのセキュリティ・ガイドラインに従って保護します。
- Oracle Application Server を保護します。
- リポジトリ・データベースの監査を有効にします。

物理セキュリティやネットワーク・セキュリティなどのガイドラインに従って、システム全体のセキュリティを強化します。

詳細な配置プランニングのまとめ

ここまでの項では、ディレクトリ情報ツリーのプランニングの詳細について説明し、高可用性とパフォーマンス要件を満たす物理トポロジの例をいくつか紹介しました。

詳細な配置プランニングの最終段階では、各企業の要件に最適な DIT と物理トポロジを選択する必要があります。最終的な物理ネットワーク・トポロジでは、これまでの項で説明した 1 つ以上の物理トポロジを組み合せて使用することもできます。

物理トポロジを選択した後は、インストールと詳細な構成情報について、Oracle Identity Management のインストール・ドキュメントおよびコンポーネント固有の管理者ガイドを参照してください。

配置プランニングは、循環的なプロセスとして、企業の変化するニーズに常に柔軟に対応する必要があります。実際の実装以外にも、識別情報管理の配置では、識別情報管理インフラストラクチャの稼動状況とパフォーマンスを監視し、必要に応じて修正アクションを実行できるように、十分に定義されたプロセスを構築する必要があります。

関連項目：

- 「はじめに」の「関連ドキュメント」

4

Oracle Identity Management の管理と使用

この章では、Oracle Identity Management インフラストラクチャの管理方法と使用方法について、Oracle Delegated Administration Services によるユーザー管理と、インフラストラクチャ自体の管理に関する検討事項を中心に説明します。

また、Oracle Identity Management インフラストラクチャでの Oracle およびサード・パーティ・アプリケーションの配置サポートに関する検討事項についても説明します。

この章では、次のトピックについて説明します。

Oracle Identity Management インフラストラクチャの管理

配置が順調に完了した後は、ルーチン監視、Oracle Identity Management インフラストラクチャ内の個別コンポーネントやエンタープライズ・データの管理など、Oracle Identity Management インフラストラクチャの管理に関連するタスクをいくつか行います。

この項では、次のトピックについて説明します。

- Oracle Identity Management インフラストラクチャのルーチン監視
- 個々の Oracle Identity Management コンポーネントの管理
- Oracle Identity Management インフラストラクチャ内のエンタープライズ・データの管理

Oracle Identity Management インフラストラクチャのルーチン監視

表 4-1 に、Oracle Identity Management インフラストラクチャのルーチン監視の実行に必要な各種タスク、ツールおよび関連ドキュメントを示します。

表 4-1 ルーチン監視タスク

タスク	ツール	関連ドキュメント
Oracle Internet Directory Server の稼動状況とパフォーマンスの監視	■ Oracle Enterprise Manager Application Server Control ■ LDAP コマンドライン・ツール	『Oracle Internet Directory 管理者ガイド』
Oracle Directory Integration and Provisioning の稼動状況の監視	Application Server Control	『Oracle Internet Directory 管理者ガイド』
Oracle Delegated Administration Services の稼動状況の監視	Application Server Control	『Oracle Internet Directory 管理者ガイド』
OracleAS Single Sign-On の稼動状況の監視	Application Server Control	『Oracle Application Server Single Sign-On 管理者ガイド』

個々の Oracle Identity Management コンポーネントの管理

表 4-2 は、Oracle Identity Management の個々のコンポーネントの管理に必要な各種タスク、ツールおよび関連ドキュメントについて説明しています。

表 4-2 Oracle Identity Management コンポーネントの管理

タスク	ツール	関連ドキュメント
ディレクトリ・サービスの開始と停止	■ Application Server Control ■ `oidctl` コマンドライン・ツール	『Oracle Internet Directory 管理者ガイド』
ディレクトリ・サービスの構成	Oracle Directory Manager	『Oracle Internet Directory 管理者ガイド』
Oracle Directory Integration and Provisioning サービスの開始と停止	■ Application Server Control ■ `oidctl` コマンドライン・ツール	『Oracle Internet Directory 管理者ガイド』
Oracle Directory Integration and Provisioning の構成	■ Oracle Directory Manager ■ Directory Integration Platform Assistant	『Oracle Internet Directory 管理者ガイド』
Oracle Delegated Administration Services の開始と停止	■ Application Server Control ■ `opmctl` コマンドライン・ツール	■ 『Oracle Internet Directory 管理者ガイド』 ■ 『Oracle Application Server 10*g* 管理者ガイド』
Oracle Delegated Administration Services の構成	Oracle Delegated Administration Services の「構成」タブ	『Oracle Internet Directory 管理者ガイド』
OracleAS Single Sign-On の開始と停止	■ Application Server Control ■ `opmctl` コマンドライン・ツール	■ 『Oracle Application Server Single Sign-On 管理者ガイド』 ■ 『Oracle Application Server 10*g* 管理者ガイド』
OracleAS Single Sign-On へのパートナ・アプリケーションの登録	`ossoreg.jar` 登録ツール	『Oracle Application Server Single Sign-On 管理者ガイド』

Oracle Identity Management インフラストラクチャ内のエンタープライズ・データの管理

個々のコンポーネントの監視と管理に加えて、表 4-3 は、Oracle Identity Management インフラストラクチャ内のエンタープライズ・データ（ユーザー、グループ、アプリケーションおよびポリシー）の管理に必要な各種タスク、ツールおよび関連ドキュメントについて説明しています。

表 4-3 エンタープライズ・データの管理

タスク	ツール	関連ドキュメント
ユーザー管理（ユーザーの追加、削除、変更）	■ Oracle Delegated Administration Services ■ LDAP コマンドライン・ツール ■ Oracle Directory Manager	『Oracle Internet Directory 管理者ガイド』
グループ管理（グループの追加、削除、変更）	■ Oracle Delegated Administration Services ■ LDAP コマンドライン・ツール ■ Oracle Directory Manager	『Oracle Internet Directory 管理者ガイド』
アプリケーション配置のセキュリティの管理	■ Oracle Delegated Administration Services ■ LDAP コマンドライン・ツール ■ Oracle Directory Manager	■ 『Oracle Internet Directory 管理者ガイド』 ■ 『Oracle Application Server 10*g* 管理者ガイド』
権限の委任	■ Oracle Delegated Administration Services ■ LDAP コマンドライン・ツール ■ Oracle Directory Manager	『Oracle Internet Directory 管理者ガイド』
OracleAS Single Sign-On パートナと外部アプリケーションの管理	OracleAS Single Sign-On 管理アプリケーション	『Oracle Application Server Single Sign-On 管理者ガイド』

Oracle Identity Management での管理の委任

Oracle Identity Management によりサポートされる委任モデルは、各企業のセキュリティ要件に合せてカスタマイズ可能です。この配置では、Oracle Identity Management インフラストラクチャを使用して、エンタープライズの識別情報、エンタープライズのグループとロール、およびエンタープライズの識別情報やとグループに依存するアプリケーションを管理します。

この項では、次のトピックについて説明します。

ユーザー管理の委任

図 4-1 に示すように、ユーザー管理権限の最終的な委任先は、Identity Management インフラストラクチャを使用する Oracle コンポーネント、またはエンド・ユーザーのいずれかです。権限は、ユーザーやアプリケーションなどの識別情報、またはロールやグループに委任できます。

一般的な配置では、Oracle Internet Directory のスーパー・ユーザーが、識別情報管理レルムを作成し、そのレルム内の特定のユーザーを識別情報管理レルムの管理者に決めます。スーパー・ユーザーは、識別情報管理レルムの新しい管理者にすべての権限を委任します。委任された管理者は、Oracle Application Server の管理者などの Oracle 定義ロールに、Oracle コンポーネントで必要とされる特定の権限を委任します。これらの定義ロールは、Oracle コンポーネントの配置時に、コンポーネントに付与されます。

レルム管理者は、必要な権限を Oracle 定義ロールに委任するだけでなく、ヘルプ・デスク管理者などの配置固有のロールを定義して、特定の権限をそのロールに委任することもできます。次に、それぞれの管理者が、それらのロールをユーザーに付与します。

Oracle Internet Directory に格納されている電話番号の変更や、言語環境、アプリケーション固有の作業環境の変更など、ユーザー管理タスクの大半はセルフサービスに向いているため、これらの権限はレルム管理者および Oracle アプリケーション・コンポーネントの両方からユーザーに委任することが可能です。

グループ管理の委任

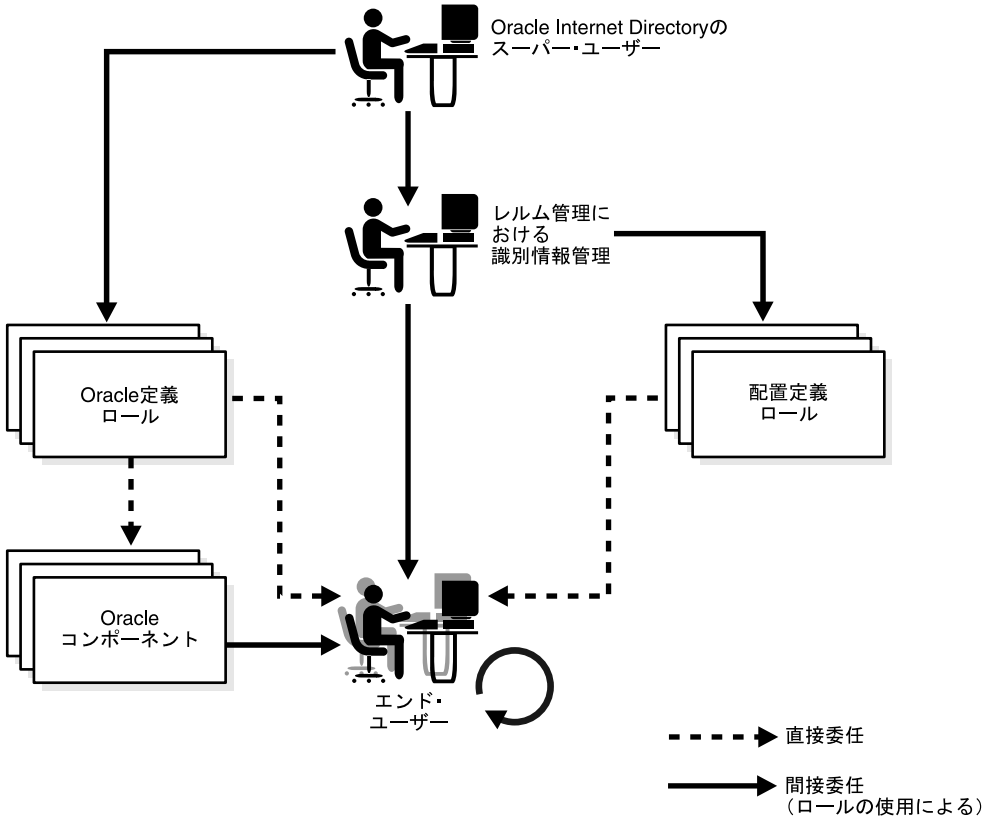
図 4-1 に示すように、ユーザー管理の委任と同様、グループ管理権限の最終的な委任先は、Identity Management インフラストラクチャを使用する Oracle コンポーネント、またはエンド・ユーザーのいずれかです。

Oracle Internet Directory のスーパー・ユーザーは、識別情報管理レルムの管理者に、レルム内のグループに関連するすべての権限を委任します。委任された管理者は、Oracle 定義ロールに、Oracle コンポーネントで必要とされる特定のグループ管理権限を委任します。これらの定義ロールは、Oracle コンポーネントの配置時に、コンポーネントに付与されます。

レルム管理者は、必要な権限を Oracle 定義ロールに委任するだけでなく、ヘルプ・デスク管理者などの配置固有のロールを定義して、そのロールに特定の権限を委任することもできます。次に、それぞれの管理者が、それらのロールをユーザーに付与します。

グループが作成されたら、1 人以上のグループ所有者をエンド・ユーザーの中から決めて、その所有者に以降のすべてのグループ管理を委任できます。これらの所有者はセルフサービス・コンソールを使用することで、付与された権限に基づいてグループを管理できます。

図 4-1 ユーザーおよびグループ管理権限の委任



コンポーネント配置と管理の委任

Oracle コンポーネントの配置と管理に必要な権限は、配置時権限とランタイム権限の 2 つに大別できます。

配置時権限とは、ディレクトリ内に適切なエントリを作成したり、共有リポジトリにメタ情報を格納するときに必要となる権限です。一元化されたリポジトリを構築することにより、それ以上の管理手順を必要とすることなく、複数のノードからコンポーネントを実行できます。

ランタイム権限とは、Identity Management インフラストラクチャ内にある Oracle コンポーネントを、実行中にやり取りできるように設定するために必要とされる権限です。具体的な権限としては、ユーザー属性の表示、新規ユーザーの追加、グループ・メンバーシップの変更などがあります。すべての Oracle コンポーネントで、コンポーネント固有の管理ツールが、Oracle Internet Directory にアクセスし適切なエントリを作成するための特定の権限セットを必要とします。

図 4-2 に、Oracle Identity Management インフラストラクチャにおけるランタイム権限と配置時権限の委任を示します。

図 4-2 ランタイム権限と配置時権限の委任

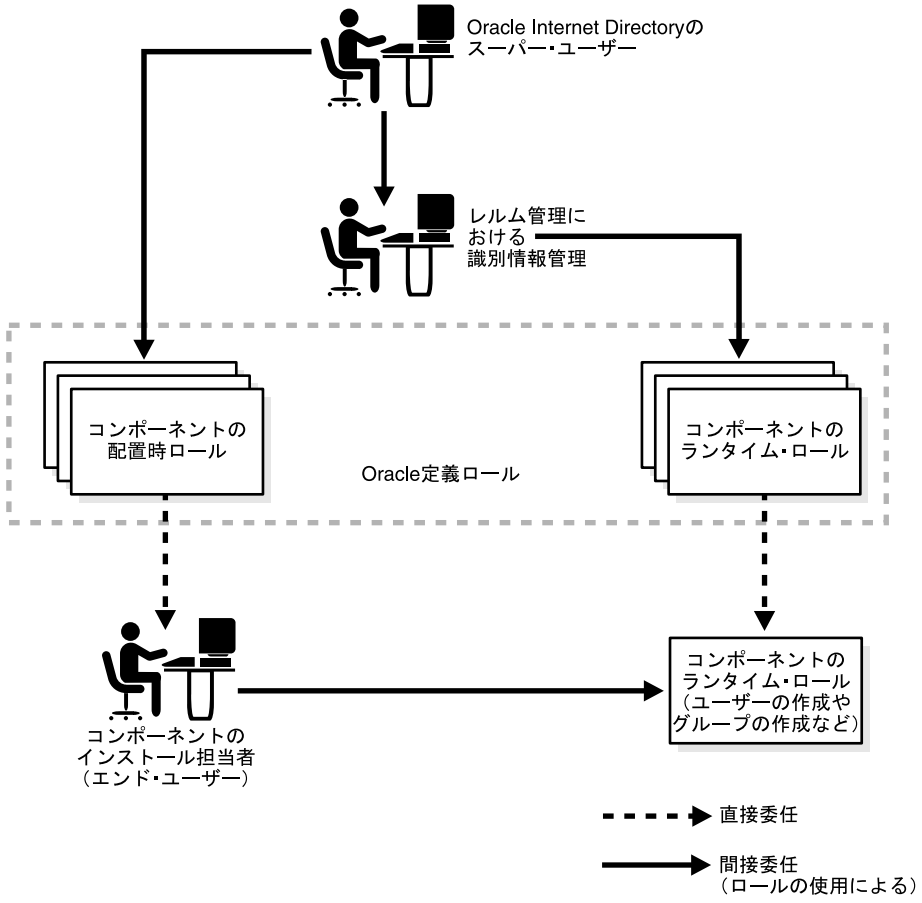


図 4-2 では、スーパー・ユーザーが特定の配置権限をグループに付与し、配置プロセスで特定のユーザーをそのグループのメンバーとすることで、特定の Oracle コンポーネントをインストールするユーザーに、その権限が付与されている点に注意してください。次に、インストール・プロセスの一部として、コンポーネントのインストール担当者が、コンポーネントに対して特定のランタイム権限を付与します。

注意： 大半の Oracle コンポーネントは権限セットが事前に定義された状態で出荷されますが、特定のビジネス要件に合せて権限を変更することは常に可能です。

Oracle Internet Directory の委任管理サービス

Oracle Delegated Administration Services では、ビジネス要件に従って、管理責任を割り当てることができます。また、エンタープライズのコンポーネント別に、大まかなセキュリティ・ポリシーと綿密なセキュリティ・ポリシーが用意されているので、特定の管理者や管理者グループが、リソースへのアクセスを個別に管理できます。ただし、異なるセキュリティ情報は作成できないようになっています。

Oracle Internet Directory ベースの中間層委任アーキテクチャでは、複数のレルム、管理ドメイン、アプリケーション、ビジネス・ユニットおよび地理ロケーションに属する数百万のユーザーがサポートされます。一元化されたリポジトリとの結合により、Oracle Identity Management では分割管理が可能となり、所有コストが削減されます。

アプリケーション設計者が直面する課題の 1 つは、ユーザー管理とリソース管理を、アプリケーション間で一貫性のあるセキュリティと使用セマンティクスにより実行できることです。たとえば、複数のアプリケーションがグループを管理する必要がある場合、各アプリケーションが、グループ管理の実装に必要となる様々な手順とディレクトリの ACL セマンティクスを理解する必要がなくなります。

Oracle Identity Management システム権限のユーザー・インタフェースは様々な委任管理サービス・ユニット（DAS サービス・ユニット）に分割でき、それらはアプリケーション・コンソールにより組み合せることができます。たとえば、アプリケーション・コンソールを使用してユーザー属性を変更する必要がある場合は、適切な DAS サービス・ユニットへのリンクをそのコンソールまたはポータル・ページに統合することで、ユーザー・インタフェースを作成する必要がなくなります。

また、様々な DAS サービス・ユニットを使用して、言語環境や自宅住所などの属性の更新に使用するセルフサービス・アプリケーションを構築できます。こうした DAS サービス・ユニットベースの統合アプローチにより、一貫性のあるセキュリティ・セマンティクスに加えて、一貫性のある使用モデルとコンポーネントの再利用が可能になります。

5

他の識別情報管理ソリューションとの統合

この章では、Oracle コンポーネントと他のエンタープライズ向け識別情報管理ソリューションとの統合について説明します。

この章では、次のトピックについて説明します。

統合の目的

Oracle の一般的な製品配置において、Oracle Identity Management インフラストラクチャは不可欠のコンポーネントですが、他の識別情報管理ソリューションとも統合できるように設計されています。共通インフラストラクチャの周辺に Oracle 製品を統合すると、次のような他のエンタープライズ向け識別情報管理ソリューションとも単一点で統合できます。

- ディレクトリ・サービス
- ユーザー認証サービス
- ユーザー・プロビジョニング・アプリケーション
- サード・パーティの PKI ソリューション

識別情報管理の統合により、Oracle ユーザーは既存のエンタープライズ・インフラストラクチャ・コンポーネントを Oracle 環境で使用できるようになります。これには、次のような利点があります。

- **統合化されたユーザー・プロビジョニング**: ユーザー・プロビジョニングとは、各種エンタープライズ・システムに新規ユーザーを追加したり、そこからユーザーを削除するプロセスです。新規ユーザーのプロビジョニングは、人事管理（HR）システム、カスタマ・リレーションシップ・マネジメント（CRM）・システム、ネットワーク管理環境などの複数の異なるソースから実行される可能性があります。あるシステムで新規ユーザーが作成されたときは、自動化されたユーザー・プロビジョニングにより、他のエンタープライズ・アプリケーションにも必要なユーザー・アカウント・プロファイルが作成されます。
- **一元化されたユーザー管理**: 作成されたユーザー・アカウントは維持および管理する必要があります。ユーザー管理の一元化により、パスワード、ロール、アプリケーションの作業環境など、ユーザーに割り当てられたすべてのアプリケーション関連情報が 1 箇所で管理されます。
- **ランタイム・セキュリティ・サービスの統合**: 多くの組織は、ユーザーの実行時の操作を透過的にしたいと考えています。これは、企業環境内の様々なアプリケーションが、認証とデータのプライバシに関して共通のセキュリティ・セットを使用できる必要があることを意味します。

これらの利点を享受するには、Oracle Identity Management、サード・パーティ・ディレクトリ、セキュリティおよびユーザー認証環境を統合するためのツールと戦略が必要になります。

> **関連項目：** これらの統合ソリューションの配置の詳細は、『Oracle Internet Directory 管理者ガイド』および『Oracle Application Server Single Sign-On 管理者ガイド』を参照してください。

統合ツールと戦略

Oracle Identity Management には、各種のサービスおよび API、事前定義済ディレクトリ接続ソリューション、標準のサポートなど、他の識別情報管理環境との統合に使用するツールがいくつか用意されています。この項では、それらのツールについて簡単に説明します。これらの使用方法の詳細は、各コンポーネントのドキュメントを参照してください。

Oracle Directory Integration and Provisioning

Oracle Directory Integration and Provisioning は Oracle Internet Directory に組み込まれる 1 組のサービスとインタフェースで構成され、Oracle Internet Directory と他のリポジトリ間の同期化およびプロビジョニング・ソリューションの開発を支援します。対象となるリポジトリには、サード・パーティ・ディレクトリ（SunONE Directory や Microsoft Active Directory Services など）、アプリケーション・ユーザー・リポジトリ（フラット・ファイルに格納されるものなど）、HR 情報が記録されたデータベース表などが含まれます。

Oracle Directory Integration and Provisioning には公開 API が付属しており、使用可能な業界標準がそのまま組み込まれています。オラクル社、顧客およびサード・パーティは、そうした標準を使用することによって、カスタマイズした同期化ソリューションおよびプロビジョニング・ソリューションの開発と配置ができます。また、Oracle Directory Integration and Provisioning は、Oracle Internet Directory と、サード・パーティのメタディレクトリおよびプロビジョニング・ソリューション間での相互運用性を高めます。

Oracle Internet Directory のプラグイン・アーキテクチャ

Oracle Internet Directory では PL/SQL ベースのプラグイン・フレームワークがサポートされるため、ディレクトリ操作の前後またはディレクトリ操作時に実行可能なカスタム・ルーチンを組み込むことができます。たとえば、このフレームワークを使用して、次のようなルーチンを作成できます。

- ディレクトリ・サーバーでディレクトリを操作する前に、データを検証します。
- ディレクトリの操作後に、特定のアクションを実行します。
- カスタムなパスワード・ポリシーを定義します。
- NOS ディレクトリなどの外部の資格証明ストアにより、ユーザーを認証します。

> **関連項目：** 詳細は、『Oracle Internet Directory 管理者ガイド』を参照してください。

事前定義済ディレクトリ接続ソリューション

Oracle Internet Directory には、Oracle Directory Integration and Provisioning および Oracle Internet Directory プラグイン・アーキテクチャに基づいて構築された事前定義済接続ソリューションが用意されています。これにより、他のシステムから Oracle Identity Management 領域へのユーザーの自動プロビジョニングおよび Oracle Identity Management 領域のユーザーの他のシステムからの管理が可能になります。事前定義済接続ソリューションには、次のものが含まれます。

- Oracle E-Business Suite リリース 11*i* Human Resources
- Oracle データベース表
- SunONE および iPlanet Directory Services
- Microsoft Active Directory Services

> **関連項目：** 事前定義済ディレクトリ接続ソリューションの詳細は、『Oracle Internet Directory 管理者ガイド』を参照してください。

OracleAS Single Sign-On パートナ API

OracleAS Single Sign-On ではサード・パーティの認証用 API がサポートされるため、サード・パーティの信頼性の高い認証方式からユーザー識別情報を取得できます。アプリケーション・ユーザーは、この機能を使用することで、2 つの環境にある Web アプリケーションに 1 度のログインでアクセスできます。

> **関連項目：** 詳細は、『Oracle Application Server Single Sign-On 管理者ガイド』を参照してください。

Oracle Application Server Java Authentication and Authorization Service の開発者用 API

Oracle Application Server Java Authentication and Authorization Service を使用することで、Oracle J2EE 環境で動作するユーザー記述の Java アプリケーションで、認証サービスに OracleAS Single Sign-On および Oracle Internet Directory が使用可能になります。

> **関連項目：** 詳細は、『JAAS Provider API Reference』を参照してください。

LDAP 標準のサポート

Oracle Internet Directory では、IETF RFC 2251 に従って、LDAPv3 標準がサポートされます。

> **関連項目：** 事前定義済ディレクトリ接続ソリューションの詳細は、『Oracle Internet Directory 管理者ガイド』を参照してください。

認証標準のサポート

OracleAS Single Sign-On では、Kerberos 鍵配布センターが発行する Kerberos チケットを使用するユーザー認証がサポートされます。この認証では、（Windows 環境などで）有効な Kerberos チケットを発行されたユーザーが、ユーザー名とパスワードを入力することなく、Web アプリケーションにログインできるようになります。

> **関連項目：** 詳細は、『Oracle Application Server Single Sign-On 管理者ガイド』を参照してください。

X.509v3 証明書標準のサポート

Oracle Identity Management では、X.509v3 標準の PKI 証明書の発行と使用がサポートされており、強固な認証サービスを構築できます。既存の X.509v3 認証局を使用する顧客は、Oracle 環境でもその証明書を使用できます。

6

エンタープライズ・アプリケーションの統合

Oracle Identity Management には、あらゆる Oracle 製品に対する共有インフラストラクチャとしてのサービスに加えて、サード・パーティのエンタープライズ・アプリケーションの配置を支援するサービスとプログラム・インタフェースが用意されています。自作のアプリケーションに識別情報管理を組み込む必要があるアプリケーション開発者にとって、これらのインタフェースは有益です。

この章では、これらのインタフェースについて説明し、Oracle Identity Management 環境での適切なアプリケーション開発方法を紹介します。

次の 2 タイプのアプリケーションを Oracle Identity Management に統合できます。

- 社内に配置済の既存アプリケーション。これまでにそのようなアプリケーションに投資していれば、Oracle Identity Management インフラストラクチャと統合することで、その利点を享受できます。
- 今後、企業の IT 部門または ISV が、Oracle テクノロジ・スタックに基づいて開発する新規アプリケーション。

この章では、次のトピックについて説明します。

Oracle Identity Management との統合の利点

エンタープライズ・アプリケーションと Oracle Identity Management インフラストラクチャとの統合には、次のような利点があります。

- **アプリケーション配置の効率化と低コスト化**: 新規アプリケーションの配置に既存の Oracle Identity Management インフラストラクチャを使用すると、配置が大幅に簡略化されます（主にオラクル社の顧客の場合）。Oracle Delegated Administration Services のセルフサービス・コンソールを使用することで、アプリケーション管理の特定のタスクをユーザーに委任でき、アプリケーションの配置コストが削減されます。
- **Oracle アプリケーションとのシームレスな統合**: すべての Oracle アプリケーションが Oracle Identity Management インフラストラクチャに依存するため、エンタープライズ・アプリケーションは Oracle Identity Management インフラストラクチャとのネイティブな統合により、これまで以上に使いやすくなります。
- **サード・パーティの識別情報管理ソリューションとのシームレスな統合**: Oracle Identity Management インフラストラクチャには、サード・パーティの識別情報管理インフラストラクチャと統合する機能が組み込まれているため、アプリケーション開発者は各自のアプリケーションにこの機能を利用できます。

アプリケーションの統合に使用できる Oracle Identity Management のサービス

カスタム・アプリケーションで Oracle Identity Management を使用できるようにするために、一連のサービスと API が公開およびサポートされています。これには、次のようなものがあります。

- Oracle Internet Directory には C、Java および PL/SQL 用の LDAP API が付属し、他の LDAP SDK と互換性があります。
- Oracle Delegated Administration Services では、コアとなるセルフサービス・コンソールが提供され、サード・パーティ・アプリケーションのサポート用にカスタマイズできます。また、ディレクトリ・データの操作に使用するカスタマイズされた管理インタフェースを構築するためのサービスも用意されています。
- Oracle Directory Synchronization Services では、Oracle Internet Directory と、サード・パーティ・ディレクトリおよび他のユーザー・リポジトリを同期化するカスタム・ソリューションの開発と配置が支援されます。
- Oracle Provisioning Integration Services では、サード・パーティ・アプリケーションをプロビジョニングするメカニズムと、Oracle 環境と他のプロビジョニング・システムを統合する手段が提供されます。
- OracleAS Single Sign-On には、他の Oracle Web アプリケーションとシングル・サインオンを共有するパートナ・アプリケーションの開発と配置に使用する API が用意されています。

- JAZN は Oracle Application Server Java Authentication and Authorization Service 標準の Oracle 実装です。この標準があることで、Oracle J2EE 環境を使用して Web 用に開発されたアプリケーションが、認証および認可に識別情報管理インフラストラクチャを利用できます。

既存のアプリケーションと Oracle Identity Management の統合

特定のビジネス機能を実行するいくつかのアプリケーションが、企業環境にすでに配置されている場合があります。Oracle Identity Management インフラストラクチャには、次のようなサービスが用意されているので、これを利用して既存アプリケーションの動作を変更できます。

- **自動化されたユーザー・プロビジョニング** : Oracle Identity Management インフラストラクチャで実行されたプロビジョニング・イベントに合せて、既存アプリケーションでのユーザー・プロビジョニングを自動化するカスタム・プロビジョニング・エージェントを開発できます。このエージェントは、Oracle Provisioning Integration Service のインタフェースを使用して開発する必要があります。

  関連項目： 自動化されたユーザー・プロビジョニングの配置の詳細は、『Oracle Internet Directory 管理者ガイド』を参照してください。

- **ユーザー認証サービス** : 既存アプリケーションのユーザー・インタフェースが HTTP ベースの場合は、Oracle HTTP Server に統合し、`mod_osso` を使用してその URL を保護すると、すべての受信ユーザー・リクエストが OracleAS Single Sign-On サービスを使用して認証されます。
- **一元化されたユーザー・プロファイル管理** : 既存アプリケーションのユーザー・インタフェースが HTTP ベースで、OracleAS Single Sign-On の認証と統合されている場合は、アプリケーションに Oracle Delegated Administration Services のセルフサービス・コンソールを使用して、ユーザー・プロファイル管理を一元化できます。セルフサービス・コンソールは、アプリケーション固有の必要性を満たすようにカスタマイズできます。

新規アプリケーションと Oracle Identity Management の統合

新規アプリケーションを開発する場合または既存アプリケーションの新しいリリースをプランニングする場合、アプリケーション開発者は、Oracle Identity Management インフラストラクチャにより提供されるサービスをより幅広く使用できます。アプリケーション開発者は、次の統合ポイントについて検討する必要があります。

- **ユーザー認証サービス** : アプリケーション開発者には、次のオプションがあります。
  - アプリケーションが J2EE ベースの場合は、Oracle Application Server Java Authentication and Authorization Service インタフェースにより提供されるサービスを使用できます。

  - アプリケーションが Oracle Application Server Containers for J2EE に依存する場合は、mod_osso により提供されるサービスを使用して、ユーザーを認証し、HTTP ヘッダーにあるユーザーに関する重要情報を取得できます。
  - アプリケーションがスタンドアロンの Web ベースのアプリケーションの場合は、OracleAS Single Sign-On API を使用するパートナ・アプリケーションとして OracleAS Single Sign-On を使用できます。
  - アプリケーションのアクセス・インタフェースが非 Web ベースの場合は、Oracle Internet Directory LDAP API（C、PL/SQL および Java で使用可能）を使用してユーザーを認証できます。

- **一元化されたプロファイル管理**: アプリケーション開発者には、次の使用可能なオプションがあります。
  - アプリケーション開発者は、アプリケーション固有のプロファイルとユーザーの作業環境を、Oracle Internet Directory の属性としてモデル化できます。
  - アプリケーションのユーザー・インタフェースが HTTP ベースで、OracleAS Single Sign-On の認証と統合されている場合は、アプリケーションに Oracle Delegated Administration Services のセルフサービス・コンソールを使用して、ユーザー・プロファイル管理を一元化できます。セルフサービス・コンソールは、アプリケーション固有の必要性を満たすようにカスタマイズできます。
  - アプリケーションは、Oracle Internet Directory LDAP API（C、PL/SQL および Java で使用可能）を使用して、実行時にユーザー・プロファイルを取得することもできます。
- **自動化されたユーザー・プロビジョニング**: アプリケーション開発者は、次のオプションについて検討する必要があります。
  - アプリケーションのユーザー・インタフェースが HTTP ベースで、OracleAS Single Sign-On の認証と統合されている場合、アプリケーション開発者は、ユーザーが初めてアプリケーションにアクセスしたときにユーザー・プロビジョニングが自動的に実行されるように実装できます。
  - アプリケーションは Oracle Provisioning Integration Service とも統合できます。それにより、Oracle Identity Management インフラストラクチャで、識別情報の追加、既存の識別情報のプロパティの変更、既存の識別情報の削除などの管理アクションが実行された場合に、それに対応して、ユーザー・アカウントのプロビジョニングとプロビジョニング解除を自動実行できます。

A

Oracle Internet Directory のデフォルト設定

この付録では、Oracle Internet Directory のインストール時に使用できるデフォルト設定について説明します。

Oracle Internet Directory をインストールすると、デフォルトの DIT が作成され、配置に関するいくつかの前提に基づいて、デフォルトの識別情報管理レルムがセットアップされます。

この後の説明は、Oracle Internet Directory のインストール時に実行されるすべての操作をまとめたものです。

- Oracle Internet Directory がインストールされるマシンのドメイン名に基づいて、デフォルトの DIT が作成されます。たとえば、Oracle Internet Directory が `oidhost.us.acme.com` という名前のマシンにインストールされる場合は、デフォルトの DIT は `dc=us,dc=acme,dc=com` になります。
- デフォルトの識別情報管理レルムが作成されます。そのベースは、マシンのドメイン名に対応します。前の例をそのまま使用すると、デフォルトの識別情報管理レルムのルートは `dc=us,dc=acme,dc=com` になります。

  レルム固有のすべてのポリシーとメタデータが格納される Oracle Context という名前のエンティティが、このレルムに関連付けられます。この例では、Oracle Context は `cn=OracleContext,dc=us,dc=acme,dc=com` という識別名で作成されます。Oracle Context のエントリとその下にあるノードは、Oracle ソフトウェアがレルム固有のポリシーと設定を検出する際の基盤としての役割を持ちます。
- ディレクトリ構造とネーミング・ポリシーがデフォルトの識別情報管理レルムに作成され、Oracle コンポーネントが様々な識別情報を検索できるようになります。次に、これらのポリシーのデフォルト値について説明します。
  - すべてのユーザーは、識別情報管理レルムのベースの下にある `cn=users` コンテナに配置されます。このシナリオでは、識別名は `cn=users,dc=us,dc=acme,dc=com` になります。

- Oracle Identity Management インフラストラクチャを使用して、識別情報管理レルムに新規ユーザーを作成する場合も、同じように cn=users コンテナの下に作成されます。
- Oracle Identity Management インフラストラクチャを使用して、識別情報管理レルムに作成した新規ユーザーはすべて、オブジェクト・クラスの orclUserV2 と inetOrgPerson に属します。
- すべてのグループは、識別情報管理レルムのベースの下にある cn=groups コンテナに配置されます。このシナリオでは、識別名は cn=groups,dc=us,dc=acme,dc=com になります。
- cn=orcladmin という名前のブートストラップ・ユーザーが、cn=users コンテナの下に作成されます。このシナリオでは、ブートストラップ・ユーザーの完全修飾された識別名は、cn=orcladmin,cn=users,dc=us,dc=acme,dc=com になります。
- デフォルトの認証ポリシーが作成され、認証サービスが適切なアクションを実行できるようになります。このポリシーには、デフォルトのディレクトリ・パスワード・ポリシー（パスワードの長さ、ロックアウト、有効期間など）や、ユーザーのプロビジョニング時に自動的に生成される必要がある追加のパスワード検証機能などが含まれます。
- 識別情報の管理権限が作成され、ブートストラップ・ユーザーに付与されます。ブートストラップ・ユーザーは、Oracle Delegated Administration Services のセルフサービス・コンソールにより、これらの認可をさらに委任できます。これらの権限には、次のものが含まれます。
  * ユーザーの作成、ユーザー・プロファイルの変更、グループの作成など、識別情報管理での一般的な操作権限。
  * Identity Management インフラストラクチャを使用する新規 Oracle アプリケーションをインストールする権限。
  * Oracle Delegated Administration Services の管理権限。

索引

X

あ

か

さ

た

な

は

や

ら