Oracle® Identity Management

インフラストラクチャ管理者ガイド

10*g*（10.1.4.0.1）

部品番号 : B31508-01

2006 年 9 月

ORACLE®

Oracle Identity Management インフラストラクチャ管理者ガイド , 10*g*（10.1.4.0.1）

部品番号 : B31508-01

原本名 : Oracle Identity Management Infrastructure Administrator's Guide, 10*g* (10.1.4.0.1)

原本部品番号 : B15994-01

原本著者 : Ellen Desmond

原本協力者 : Darren Calman, Ed King, Ashish Kolli, Daniel Shih, Saurabh Shirvastava, Olaf Stullich, Uppili Srinivasan

目次

A　ファンアウト・レプリケーションによる ID 管理のデプロイ

B　Oracle Internet Directory のデフォルトの設定

図一覧

表一覧

はじめに

『Oracle Identity Management インフラストラクチャ管理者ガイド』では、ID 管理に関連する概念を説明し、管理者およびアプリケーション開発者にデプロイ計画情報を提供します。

「はじめに」の内容は次のとおりです。

対象読者

このドキュメントは、次の読者を対象としています。

- ID 管理の管理者
- Oracle アプリケーション管理者
- エンタープライズ・アプリケーション開発者

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

詳細は、次のガイドを参照してください。

- 『Oracle Application Server 管理者ガイド』
- 『Oracle Application Server セキュリティ・ガイド』
- 『Oracle Application Server 高可用性ガイド』
- Oracle Application Server 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 高可用性ガイド』
- 『Oracle Application Server Single Sign-On 管理者ガイド』
- 『Oracle Internet Directory 管理者ガイド』
- 『Oracle Identity Management 委任管理ガイド』
- 『Oracle Identity Management 統合ガイド』
- 『Oracle Identity Management ユーザー・リファレンス』

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。

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

ID 管理インフラストラクチャの概要

Oracle の ID およびアクセス管理ソリューションは、次の 2 つのパッケージから構成されています。

- Oracle Identity and Access Management Suite。異種エンタープライズの ID およびアクセス管理要件に対処することを目的とした、ベスト・オブ・ブリード・コンポーネントの包括的なセットです。
- ID 管理インフラストラクチャ。Oracle Application Server インフラストラクチャ・インストール環境の一部として含まれるコンポーネントのセットです。

この章では、この 2 つのパッケージについて説明します。この章の内容は次のとおりです。

Oracle Identity and Access Management Suite

Oracle Identity and Access Management Suite には、次のものが含まれます。

- Oracle Internet Directory。これは ID 管理インフラストラクチャにも含まれます。これについては、次の項で説明します。
- Oracle Identity Federation。規格に基づくマルチプロトコルのドメイン間シングル・サインオンを提供します。
- Oracle Security Developer Tools。フェデレーションおよびセキュア Web サービス・アプリケーションを開発するための API を提供します。
- Oracle Access Manager。Web ベースの ID 管理と、異種環境で稼働する Web アプリケーションおよびリソースへのアクセス制御を提供します。
- Oracle Identity Manager。異種性の高いテクノロジがある複合環境を管理するために設計されたエンタープライズ・プロビジョニング・プラットフォームです。
- Oracle Virtual Directory。複数の場所およびサービスに分散するユーザー ID 情報への単一アクセス・ポイントを提供します。

ID 管理インフラストラクチャ

ID 管理インフラストラクチャは、Oracle Application Server Infrastructure インストール環境に含まれる ID 管理コンポーネントのセットです。インフラストラクチャは、Oracle 製品に対して分散セキュリティを提供し、Oracle Application Server、Oracle Database および Oracle Collaboration Suite に含まれています。

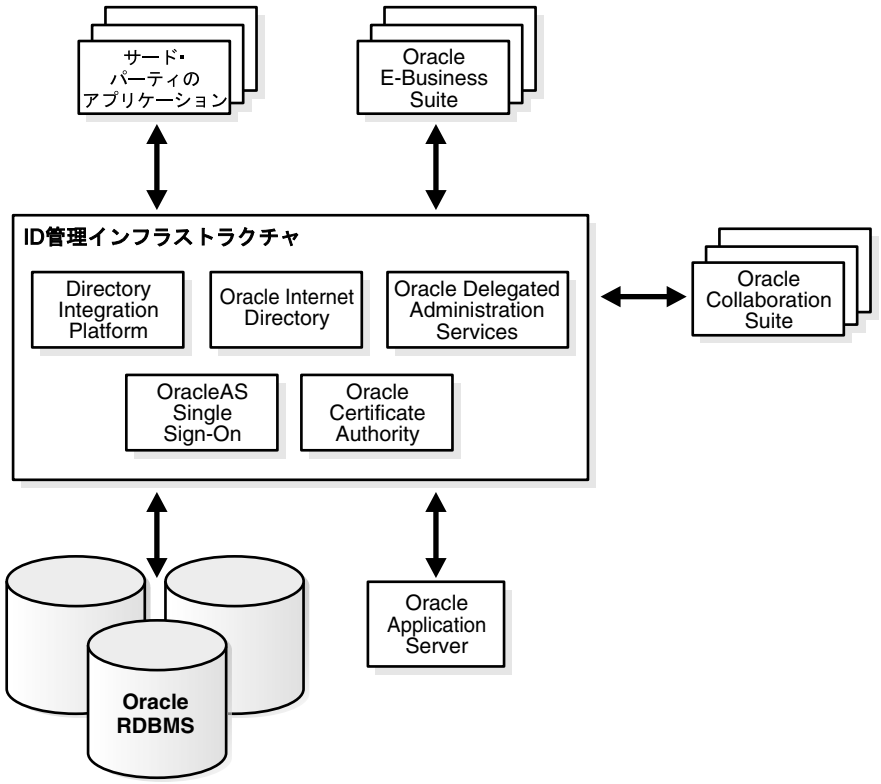
> **関連資料：** Oracle Application Server のインストレーション・ガイドの OracleAS Infrastructure のインストールに関する章

ID 管理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: Oracle Database に実装された、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 Directory Integration Platform: ディレクトリ中心の環境でディレクトリ同期およびプロビジョニング・タスクを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 Identity Manager とは異なり、Oracle Directory Integration Platform は、ディレクトリおよび互換 Oracle 製品から構成される同種環境を管理するように設計されています。Oracle Directory Integration Platform は、データ同期を使用してプロビジョニング・タスクを実行します。Oracle Directory Integration Platform では、ワークフローおよびフル機能ポリシー・エンジンが不要な場合にデプロイ・フットプリントが小さくなります。ユーザーのステータスまたは情報に対する変更がターゲット・アプリケーションに通知されます。
- Oracle Application Server Certificate Authority: X.509v3 証明書を発行、取消し、更新および公開して PKI ベースの厳密認証方式をサポートするコンポーネントです。
- 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・アクセスを提供するコンポーネントです。
- Oracle Delegated Administration Services: Oracle Internet Directory のコンポーネントであり、ユーザーおよびアプリケーション管理者による信頼できるプロキシベースのディレクトリ情報管理を提供します。

図 1-1 に示すように、サード・パーティのアプリケーション、Oracle E-Business Suite、Oracle Application Server、Oracle Database および Oracle Collaboration Suite を含む多くの異なるアプリケーションが、ID 管理インフラストラクチャを使用できます。

図 1-1 ID 管理インフラストラクチャ・アプリケーション・サポート



ID 管理インフラストラクチャは、Oracle 製品のエンタープライズ・インフラストラクチャを提供しますが、カスタム・アプリケーションおよびサード・パーティのエンタープライズ・アプリケーション用の汎用 ID 管理ソリューションとすることもできます。

また、サード・パーティ・アプリケーション・ベンダーは、ID 管理インフラストラクチャを認定して適切な動作を保証します。

ID 管理インフラストラクチャの目標

ID 管理インフラストラクチャは、3 つの主要アーキテクチャ目標を満たすように設計されています。

- ID 管理インフラストラクチャは、Oracle Application Server、Oracle Database、Oracle E-Business Suite および Oracle Collaboration Suite を含むすべての Oracle 製品およびテクノロジ・スタックの共有インフラストラクチャです。

  ID 管理インフラストラクチャは、すべての Oracle 製品およびテクノロジ・スタック間に一貫性のあるセキュリティ・モデルを提供します。ID 管理インフラストラクチャは、現在または将来の Oracle 製品のデプロイをサポートするために、計画および 1 回デプロイされます。

- ID 管理インフラストラクチャは、セキュアで効率が高く信頼性のある使用方法を提供し、既存のサード・パーティ ID 管理インフラストラクチャへの投資効果を拡大します。

  – サード・パーティの ID 管理環境では、ID 管理インフラストラクチャは Oracle テクノロジ・スタック全体との一貫性のある単一統合ポイントを提供し、様々な Oracle 製品とサード・パーティ環境の統合を構成および管理する必要をなくします。

  – Oracle Directory Integration Platform を使用することにより、ID 管理インフラストラクチャは、サード・パーティのエンタープライズ・ディレクトリの計画およびデプロイに対する投資を利用します。これにより、ディレクトリ・ネーミング、ディレクトリ・ツリー構造、スキーマ拡張、アクセス制御、セキュリティ・ポリシーなどの主要な考慮事項をマッピングおよび継承する方法が提供されます。既存のフレームワークでユーザー登録について確立された手順は、ID 管理インフラストラクチャ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を使用している場合、OracleAS Single Sign-On は、サービスとの統合方法を提供し、Oracle 環境にアクセスするユーザーにシームレスなシングル・サインオン操作性を提供します。主要なサード・パーティ認証プラットフォームには認定済の相互運用ソリューションがあり、詳細に定義されたインタフェースを利用して新製品の類似ソリューションを実装できます。

- ID 管理インフラストラクチャは、企業にデプロイされている他の Oracle 製品およびサード・パーティ製品をサポートするために、ID 管理の企業全体の基盤となることができます。

  ID 管理インフラストラクチャは、すべての Oracle 製品およびサード・パーティ製品のアカウント情報のメンテナンスを効率化することで、所有コストを削減できます。高水準のセキュリティおよびスケーラビリティも提供し、多数の機能も用意しています。すべての関連インタフェースで業界標準をサポートすることにより、ID 管理インフラストラクチャは、多くの異なるアプリケーション環境でカスタマイズして使用できます。

2

ID 管理インフラストラクチャの概念およびアーキテクチャ

この章では、デプロイ計画者が ID 管理を効率よくデプロイするために理解する必要のある概念を紹介します。ID 管理インフラストラクチャのアーキテクチャの概要、Oracle 環境の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、および ID 管理の説明によく使用される用語を示します。

この章の内容は次のとおりです。

ID 管理の概念

この項では、ID 管理の基本的な概念を説明します。内容は次のとおりです。

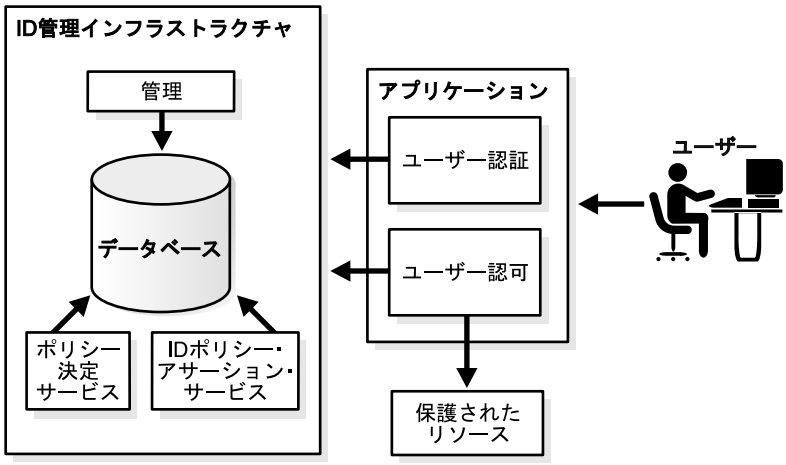
- アプリケーション・セキュリティと ID 管理の統合
- ID およびアプリケーションのプロビジョニングのライフサイクル
- 管理委任

アプリケーション・セキュリティと ID 管理の統合

この項では、様々な ID 管理インフラストラクチャ・コンポーネントおよび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、エンタープライズ環境でセキュアなアプリケーション・デプロイを作成する方法を理解するための基本情報を示します。

アプリケーション統合モデルを図 2-1 に示します。

図 2-1 アプリケーション統合モデル



このモデルでは、次の主要サービスが ID 管理インフラストラクチャによって実行されます。

- **管理およびプロビジョニング :** ID 管理インフラストラクチャにより管理される ID の管理およびプロビジョニング・サービスを提供します。ID 管理インフラストラクチャでは、これらのサービスは Oracle Delegated Administration Services や Oracle Directory Integration Platform などのツールを使用して実行されます。
- **ポリシー決定サービス :** ポリシー決定サービスは、アプリケーションがアクセスを保全および制御するリソースに関連付けられた権限ポリシーを解析します。Oracle Internet Directory は、ID 管理インフラストラクチャ自体に対してポリシー決定サービスを実行します。
- **ID ポリシー・アサーション・サービス :** ID 管理インフラストラクチャでは、これらのサービスは OracleAS Single Sign-On および OracleAS Certificate Authority によって実行されます。

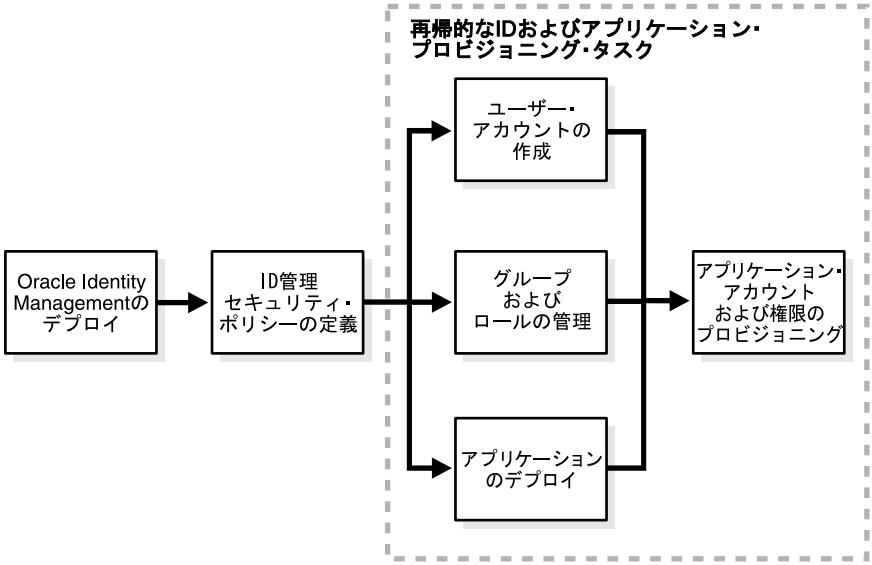
ID 管理インフラストラクチャに対してデプロイされるアプリケーションは、次の方法でインフラストラクチャと対話します。

- **ユーザー認証 :** ユーザーは、アプリケーションにアクセスするときに、ID 管理インフラストラクチャによって提供されているサービスを使用してユーザー資格証明を検証します。認証およびアプリケーションとの関連通信は、ID ポリシー・アサーション・サービスで実行されます。たとえば、ID 管理インフラストラクチャの場合、これは OracleAS Single Sign-On による暗号化されたブラウザ Cookie の形式での資格証明の検証になります。
- **ユーザー認可 :** 認証後、アプリケーションは、アプリケーションで保護されているリソースに対してユーザーが十分な権限を持っているかどうかもチェックする必要があります。このチェックは、ID 管理インフラストラクチャで管理されている ID 情報に基づいてアプリケーションが実行します。たとえば、Java2 Enterprise Edition アプリケーションは、認証後に Oracle Application Server Java Authentication and Authorization Service（JAAS）Provider（OracleAS JAAS Provider）を使用して、ID 管理インフラストラクチャ内のユーザーおよびロール情報にアクセスします。

ID および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 環境でのユーザー ID およびアプリケーションのプロビジョニング・フローの概要を示します。

図 2-2 ID およびアプリケーションのプロビジョニング・フロー



次に、図 2-2 に示したプロビジョニング・フローを説明します。

1. 製品のインストールおよび構成ツールを使用して ID 管理インフラストラクチャをデプロイします。
2. ID 管理セキュリティ・ポリシーを定義します。これらのポリシーは、ユーザーおよびアプリケーションがどのデータにアクセスできるかを決定します。これらのポリシーは、Oracle Internet Directory 内のアクセス制御リスト（ACL）に格納され、通常は Oracle Directory Manager を使用して管理されます。
3. 次のアクティビティは、通常は実行中に発生します。各アクティビティはパラレルに発生する場合があり、特定の順序はありません。
   - ユーザー ID が Oracle Internet Directory でプロビジョニングされます。これらの ID は、人事管理アプリケーション、ユーザー管理ツール（Oracle Internet Directory セルフサービス・コンソールなど）、他のディレクトリとの同期、またはバルク・ロード・ツールといった複数のソースから取得できます。

- グループおよびロールが Oracle Internet Directory で管理されます。グループおよびグループ・メンバーシップは、Oracle Internet Directory セルフサービス・コンソールや別のディレクトリ・サービスとの同期など、多数の方法で定義できます。
- アプリケーション・インスタンスが ID 管理インフラストラクチャに対してデプロイされます。通常、このときに、ID 管理インフラストラクチャ管理者が Oracle Internet Directory 管理ツールを使用して最初にアプリケーション管理者にアクセス権を付与します。アプリケーション管理者は、アプリケーションのインストールおよび構成ツールを使用して、アプリケーションをサポートするために必要なディレクトリ・オブジェクトおよびエントリを作成します。

4. ユーザー ID、グループおよびロールとアプリケーションが、アプリケーション・プロビジョニングのプロセスを通じて関連付けられます。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を通じて自動的に実行することもできます。

管理委任

ID 管理インフラストラクチャには、エンタープライズ・ユーザー、グループおよびサービスの集中リポジトリが必要です。ただし、ビジネス要件により、集中化された一連の管理者が集中リポジトリを管理するのは難しくなります。

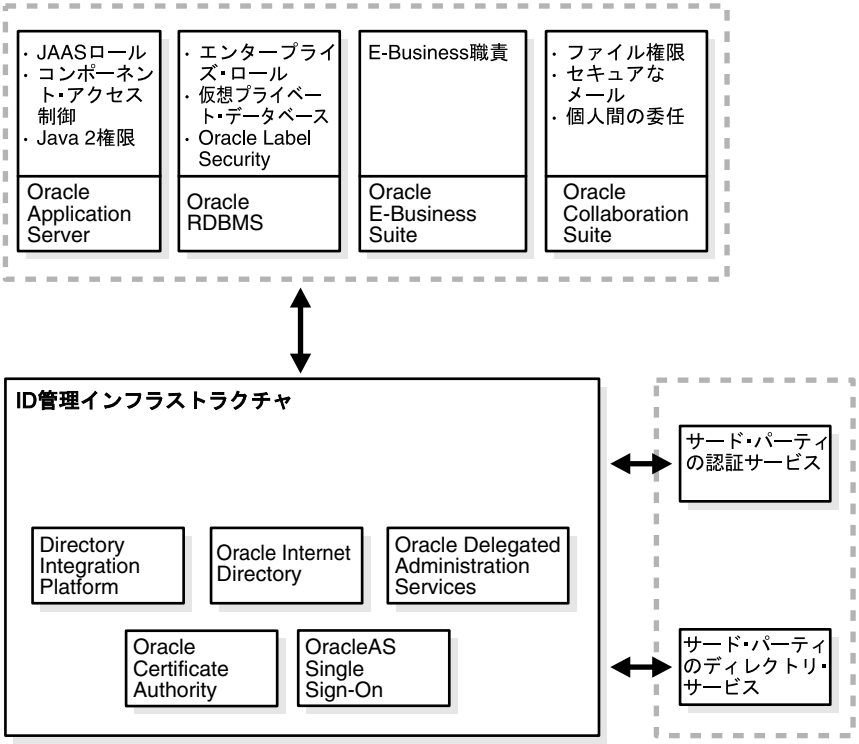
たとえば、ビジネスでは、エンタープライズ・ユーザー管理の管理者は、電子メール・サービスの管理者と異なる場合があります。財務の管理者はユーザーの権限を完全に制御することが必要な場合があり、OracleAS Portal 管理者は特定のユーザーまたは特定のグループの Web ページを完全に制御することが必要な場合があります。これらの管理者のニーズを満たし、異なるセキュリティ要件を満たすために、ID 管理システムは委任管理を必要とします。

委任管理では、セキュリティ要件に応じて、ID 管理システム内のデータの管理を多くの異なる管理者に分散できます。このように集中リポジトリと委任された権限を組み合せると、ID 管理インフラストラクチャにセキュアでスケーラブルな管理が実現されます。

Oracle 製品との ID 管理統合

各 Oracle テクノロジ・スタック（Oracle Application Server、Oracle Database、Oracle E-Business Suite および Oracle Collaboration Suite）は、設計に適したセキュリティ・モデルをサポートします。それにもかかわらず、図 2-3 に示すように、これらはすべて ID 管理インフラストラクチャを使用して、それぞれのセキュリティ・モデルおよび機能を実装します。

図 2-3 Oracle 製品との ID 管理統合



Oracle Application Server は、Java Authentication and Authorization Service（JAAS）と呼ばれる 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 で定義されたユーザーおよびロールを使用するように構成できます。

同様に、メタデータ・リポジトリ・セキュリティ機能（エンタープライズ・ユーザーおよび Oracle Label Security）は、Oracle Internet Directory で定義されたユーザーおよびロールを利用する方法を提供します。これらのプラットフォームはどちらも、プラットフォームのそれぞれのネイティブ・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が基礎となる ID 管理インフラストラクチャを透過的に利用することを促進します。

Oracle E-Business Suite および Oracle Collaboration Suite アプリケーション・スタックは、Oracle Database および Oracle Application Server の上に階層化され、ID 管理インフラストラクチャとの間接的な統合を提供します。また、これらの製品には、ID 管理インフラストラクチャに依存する独立した機能があります。たとえば、Oracle Mail や Oracle Voicemail & Fax などの Oracle Collaboration Suite コンポーネントは、Oracle Internet Directory を使用してコンポーネント固有のユーザー・プリファレンス、個人連絡先およびアドレス帳を管理します。

また、これらの Oracle テクノロジ・スタックは、Oracle Directory Integration Platform を使用して、ユーザー・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的に行います。Oracle Delegated Administration Services は、ユーザー・プリファレンスおよび個人連絡先のセルフサービス管理にのみ使用されます。また、これらの製品のセキュリティ管理インタフェースは、サービス・ユニットと呼ばれるユーザーおよびグループ管理ビルディング・ブロックを使用します。

3

ID 管理インフラストラクチャのデプロイ計画

この章では、ID 管理インフラストラクチャ・サービスをデプロイするための計画方法について説明します。

この章の内容は次のとおりです。

ID 管理デプロイ計画プロセス

製品のデプロイと使用が成功するかどうかは、よく計画された ID 管理インフラストラクチャにかかっています。

この項では、次のような ID 管理インフラストラクチャのデプロイ計画プロセスを概説します。

- 要件分析と上位レベルのデプロイ考慮事項を、これらの考慮事項を強調する論理的なデプロイ・プランとともに示します。
- デプロイ計画の詳細な考慮事項を示します。

図 3-1 に、ID 管理デプロイを計画する際に従うプロセスを示します。

図 3-1 デプロイ計画プロセス

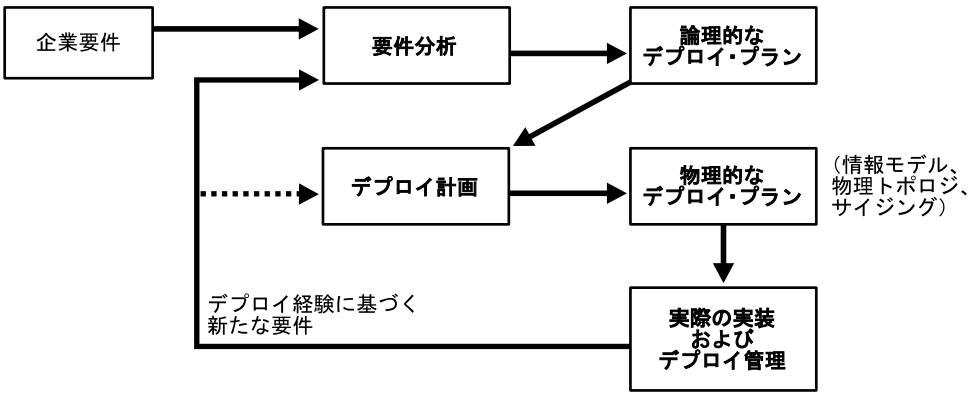


図 3-1 に示すように、デプロイ計画プロセスは反復的です。初期要件に基づいて、上位レベルの計画を実行して論理的なデプロイ・プランを作成し、論理的なデプロイ・プランを使用して詳細なデプロイ計画を実行し、実際の実装の物理的なデプロイ・プランを作成します。実装後に新たな要件が発生した場合は、分析、計画およびデプロイ・プロセスを繰り返します。

ID 管理インフラストラクチャのデプロイの要件分析

この項では、ID 管理インフラストラクチャのデプロイを計画する際に分析する必要のある一般的な企業要件をいくつか説明します。要件には、プロセスの問題、機能要件および高可用性の考慮が含まれます。ID 管理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のに役立つ様々な論理デプロイ・プランについても説明します。論理的なデプロイの決定を推進する主要件の一部として、エンタープライズ統合、管理制御およびアプリケーション・デプロイ要件があります。

要件分析プロセスの最後に、1 つ以上の論理 ID 管理インフラストラクチャから構成される ID 管理インフラストラクチャ・デプロイの上位レベルの論理アーキテクチャを選択します。これは、次の項で概説する詳細なデプロイ計画の基礎です。

この項の内容は次のとおりです。

- 上位レベルの企業要件
- 論理的なデプロイ・プランへの要件の変換

上位レベルの企業要件

この項では、上位レベル要件を説明します。内容は次のとおりです。

ID 管理インフラストラクチャを計画およびデプロイする人物の決定

小規模なデプロイでは、アプリケーション管理者が一般に ID 管理インフラストラクチャの計画、デプロイおよび管理を担当します。

大規模なデプロイでは、様々な Oracle アプリケーションとサード・パーティ・アプリケーション間でのサービスの共有など、ID 管理インフラストラクチャに用意されている集中サービスを利用できます。また、アプリケーション、ネットワーク、およびこれらのサービスを担当するセキュリティ管理者から構成されるセントラル・グループを作成できます。通常、このグループは次のタスクを実行します。

- ID 管理システムのデプロイの設計
- 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
- デプロイの管理
- プロセスおよびログ・ファイルの監視
- パフォーマンスおよびマシンの負荷の監視
- データ・バックアップ計画の実装および障害時のデータのリストア

デプロイする ID 管理インフラストラクチャのコンポーネントの決定

ID 管理インフラストラクチャを構成するコンポーネントは、多くの管理タスクを集中化します。

Oracle Internet Directory、OracleAS Single Sign-On および Oracle Delegated Administration Services の実装を計画します。Oracle Internet Directory および OracleAS Single Sign-On は、基本的な ID 管理サービスを提供し、Oracle Delegated Administration Services はユーザー・パスワードの自己メンテナンスの主要手段です。

他のサード・パーティ・ディレクトリと統合している場合は、Oracle Directory Integration Platform をデプロイします。ディレクトリ統合プラットフォームは、サポートされるサード・パーティ・ディレクトリとの同期を可能にする特定のディレクトリ同期プロファイルで構成されます。

サード・パーティ・ディレクトリを使用していない場合は、Oracle Application Server Portal や Oracle Collaboration Suite などの多くの Oracle 製品がプロビジョニング統合機能を使用するため、Oracle Directory Integration Platform サービスのデプロイを検討する必要があります。

公開鍵インフラストラクチャ（PKI）をデプロイしている場合は、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 をすでにデプロイしている場合は、既存の認証局を使用するように残りの ID 管理インフラストラクチャおよび他の Oracle 製品を構成できます。

また、Oracle 製品には、ユーザー管理をサポートするために ID 管理インフラストラクチャ・コンポーネントのデプロイを必要とするものがあります。

注意： 様々な ID 管理インフラストラクチャ・コンポーネントに対する個々の Oracle 製品の依存性の詳細は、それぞれの管理者ガイドに説明されています。

Oracle 製品の小規模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 ID 管理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。

関連資料： インストールのガイドラインは、『Oracle Application Server 管理者ガイド』を参照してください。

多くの企業には、他の ID 管理コンポーネントがあるか、それをデプロイする計画があります。ID 管理インフラストラクチャは、エンタープライズ環境をプロビジョニングおよび管理するためにすでに存在する他のエンタープライズ ID 管理ソリューションおよびアプリケーションを使用するように設計されています。

Oracle Application Server、Oracle Database、Oracle Collaboration Suite など、ID 管理を使用する Oracle コンポーネントは、ID 管理インフラストラクチャ・インスタンスによってサポートされています。このインスタンスは、両方の環境に透過的なユーザー管理および Web シングル・サインオンを提供するためにデプロイ済インフラストラクチャ・コンポーネントと連動します。

情報モデル要件の検討

Oracle Identity Management インフラストラクチャは、すべてのユーザー ID を格納するためのリポジトリとして Oracle Internet Directory を使用します。ユーザーは、企業内の複数のアプリケーションに対するアクセス権を持つことができます。ただし通常は、Oracle Internet Directory には特定のユーザーの ID を表す 1 つのエントリのみ存在する必要があります。Oracle Internet Directory およびその他の ID 管理インフラストラクチャ・コンポーネントをデプロイする前に、ディレクトリ情報ツリー（DIT）内のユーザー・エントリの場所と内容を計画する必要があります。

集中 ID 管理が必要なアプリケーション・サービス・プロバイダ（ASP）のデプロイでは、ASP 管理者および各 ASP 顧客（サブスクライバ）のユーザーに対して異なる ID 管理レルムを作成する必要があります。

集中セキュリティ管理要件の検討

E-Business およびエンタープライズ・アプリケーションが拡大すると、ID 部門は、セキュリティを低下させたり機密情報を外部にさらしたりすることなく、企業の内部と外部両方で、ユーザー・プロファイル情報を再利用する方法および増加するユーザーにアクセス権を付与する方法を検討する必要があります。複数のアプリケーション間で複数バージョンのユーザー ID を管理すると、作業が困難になります。集中化されたアカウントの作成および管理、単一パスワードと資格情報の管理、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ために集中 ID 管理インフラストラクチャのデプロイを検討します。

エンタープライズ・アプリケーション要件の検討

通常、ID 管理インフラストラクチャは、Oracle とその他のエンタープライズ・アプリケーションの寄せ集め間で共有されます。したがって、次のデプロイ要件を検討することが重要です。

- **ユーザーのタイプ :** OracleAS Portal などのエンタープライズ・アプリケーションを、内部（イントラネット）ユーザーに加えてビジネス・パートナーなどの外部（インターネット）ユーザーに対して使用可能にすることが必要な場合があります。その結果、すべての ID に対して 1 つの Oracle Internet Directory が適切か、ID のグループごとに別々の Oracle Internet Directory が適切かを判断する必要があります。
- **アプリケーション負荷要件 :** アプリケーションの負荷および可用性要件によって、ID 管理インフラストラクチャの可用性がどの程度必要かが決まります。アプリケーションの可用性が高い必要がある場合は、そのアプリケーションが依存する ID 管理インフラストラクチャの可用性が高い必要があります。
- **ASP 要件 :** ID 管理デプロイとは別に、アプリケーションが必要とする要件を検討します。たとえば、ASP デプロイでは、管理委任が必要な場合があります。

管理自律性要件の検討

- **新規アプリケーションのデプロイの部門自律性 :** 大規模企業では、独立した部門単位内でのアプリケーションの管理自律性が必要な場合があります。このような場合は、集中 ID 管理インフラストラクチャをメンテナンスする一方で、アプリケーション固有のデータとともに、一部のエンタープライズ・データを含む独立した部門別アプリケーション・リポジトリが必要な場合があります。
- **共通 ID 情報を管理するための管理自律性 :** セキュリティ・ポリシーは、ID 管理を計画する際の重要な考慮事項です。企業要件を満たすために、ID、ロール、ポリシーおよびグループを管理するための管理モデルを検討します。企業のセキュリティ・ポリシーで定義されている共通権限に従って、ユーザーの ID を管理できる必要があります。
- **ID 管理インフラストラクチャに対してデプロイされた個々のアプリケーションに対する管理自律性 :** 企業では、各エンタープライズ・アプリケーションを異なる管理者が担当する場合があります。たとえば、エンタープライズ・ユーザー管理の管理者は、電子メール・サービスの管理者と異なる場合があります。財務の管理者はユーザーの権限を完全に制御することが必要な場合があり、OracleAS Portal 管理者は特定のユーザーまたは特定のグループの Web ページを完全に制御することが必要な場合があります。また、どのユーザーがどのリソースにどのセキュリティ・レベルでアクセスする必要があるかを定義する必要があります。管理者のニーズを満たし、異なるセキュリティ要件を満たすために、管理制御要件を検討する必要があります。

セキュリティ分離要件の検討

OracleAS Portal など、内部ユーザーと外部ユーザーの両方に対して使用可能にする必要のあるエンタープライズ・アプリケーションをデプロイする場合があります。企業イントラネット・リソースが外部ユーザーから分離され、またイントラネット・アプリケーションが外部ポータルを対象とした DoS 攻撃から保護されるようにする必要があります。このようなデプロイでは、内部と外部の ID 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な場合があります。

組織の制約と高水準の経営陣の要求により、異なる環境に別々の ID 管理インフラストラクチャをデプロイして、環境間を明確に分離し、ある環境から別の環境に保護を提供することが必要な場合があります。場合によっては、ある環境に対するデータ変更を分離したり、それらの伝播を遅延させたりすることが必要な場合もあります。

注意 : これらは主に高水準の考慮事項であり、実際のスループット計算やキャパシティ計算からは派生せず、通常は次の計画段階でチューニングおよびサイジングによって対処されます。

サード・パーティ ID 管理統合要件の検討

企業にサード・パーティの ID 管理インフラストラクチャがすでにある場合は、次の統合機能を検討します。

- **Windows 統合 :** 企業が Active Directory や Kerberos 認証などの Microsoft Windows コンポーネントを使用している場合は、ID 管理コンポーネントに必要な統合を検証します。統合機能の例として、Oracle Internet Directory とのユーザー情報の同期や OracleAS Single Sign-On 認証の統合があります。
- **ユーザー・アカウント管理 :** ユーザー・アカウント管理は、エンタープライズ・システムでの新規ユーザーの追加および削除に使用されるプロセスを意味します。新規ユーザー・アカウントは、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多くの異なるソースから作成される可能性があります。1 つのシステムに新規ユーザーが作成されると、自動化されたプロビジョニングにより、必要なユーザー・アカウント・プロファイルが他のエンタープライズ・アプリケーションに作成されます。

  企業に HR や CRM などのエンタープライズ・アプリケーションがデプロイされている場合は、ID 管理システムでユーザー・プロビジョニング統合機能を使用することを検討します。ユーザー・プロビジョニングは、異なるソースから実行することもできます。
- **ディレクトリ・サービス :** 企業に iPlanet などの LDAP ディレクトリがデプロイされている場合は、LDAP サーバーを Oracle Internet Directory と同期して、ユーザー管理を集中化することを検討します。
- **ランタイム・セキュリティ・サービス統合 :** ユーザーが、Oracle Internet Directory と統合されたアプリケーションおよびサード・パーティまたは Web 認証アプリケーションにアクセスする必要がある場合は、単一のデジタル ID で Web アプリケーションに OracleAS Single Sign-On アクセスを行えるようにする統合要件を検討します。

高可用性、スケーラビリティおよびパフォーマンス要件の検討

ID 管理インフラストラクチャには複数のコンポーネントが含まれ、それぞれに可用性の考慮事項があります。高可用性ソリューションは、ID 管理に関連付けられているプロセスのソフトウェア障害を検出し、リカバリできる必要があります。コンポーネントは、アプリケーション全体の可用性要件を満たすようにデプロイする必要があります。

アプリケーションの使用状況とユーザー・トラフィックに基づいて、パフォーマンス要件を検討する必要があります。アプリケーションのデプロイ時に増加するユーザー・トラフィックに対してデプロイを拡張できるように、デプロイの考慮事項を計画する必要があります。

3-22 ページの「物理ネットワーク・トポロジの計画」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、許容される物理トポロジをリストします。

論理的なデプロイ・プランへの要件の変換

この項では、論理的なデプロイ・プランを選択するのに役立つ、一般に使用される論理デプロイ・モデルについて説明します。要件をこれらのモデルの 1 つ以上と対応させることで、論理的なデプロイ・プランを導出できます。

この項の内容は次のとおりです。

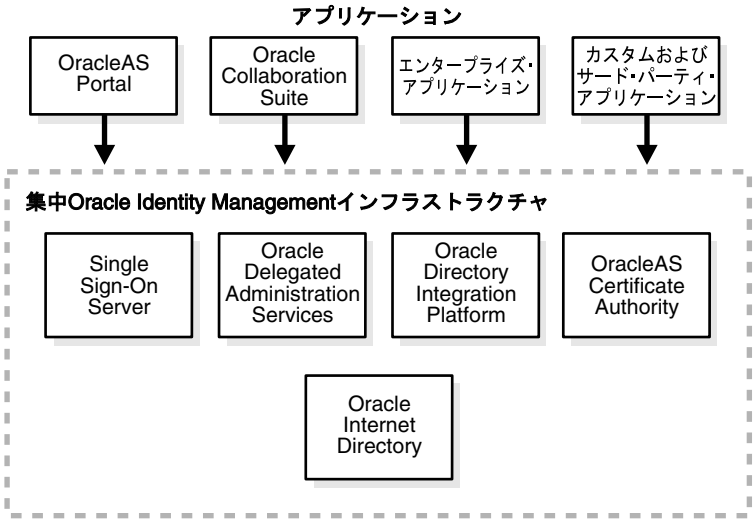
集中 ID 管理システムのデプロイのモデル : 標準エンタープライズ・モデル

図 3-2 に示すような標準エンタープライズ・モデルでは、組織内のグループは単一の集中化された ID 管理インフラストラクチャを管理およびデプロイします。エンタープライズ・アプリケーションのインスタンスがデプロイされると、それらのインスタンスは集中化されたインフラストラクチャを使用します。集中化セキュリティ・モデルにより、アプリケーションを集中インフラストラクチャに対してインストールできますが、権限が制御されます。このモデルにより、新規アプリケーションのデプロイと管理がはるかに簡単になり、集中化されたアカウント作成および管理、単一パスワードおよび資格証明管理、Web アプリケーションへのシングル・サインオンなどの特定の機能を有効にすることでアプリケーションのユーザビリティが向上します。情報モデルは、このデプロイのすべてのユーザーに対して同じです。

このタイプのデプロイでは、次の機能が実装されます。

- 企業全体で単一のコンソールを通じてエンタープライズ ID の作成および共有プロパティの管理を行う集中管理
- Oracle およびその他のエンタープライズ・アプリケーションの共有 ID 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 集中 ID 管理インフラストラクチャ



内部および外部ユーザーのモデル

OracleAS Portal などのエンタープライズ・アプリケーションを内部ユーザーと外部ユーザーに対して使用可能にする必要があります。その結果、エンタープライズ・アプリケーションは、内部 ID と外部 ID のプロファイルおよび権限情報をメンテナンスする必要があります。この統合は最適ですが、イントラネット・リソースが外部ユーザーから分離され、またイントラネット・アプリケーションが外部ポータルを対象とした DoS 攻撃から保護されるようにすることも重要です。

次の例に、内部ユーザーと外部ユーザーへのアクセスを示します。それぞれ、エクストラネット環境とイントラネット環境など、分離が必要なアプリケーション・グループ間でセキュリティ環境の分離を行います。

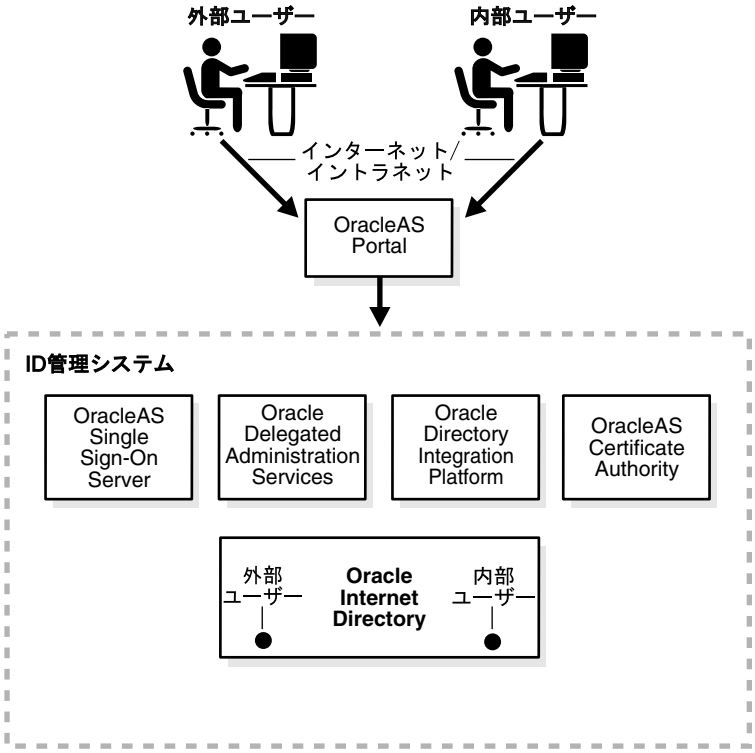
例 A: 1 つの ID 管理インフラストラクチャの使用

図 3-3 に示すような単一の論理 Oracle Internet Directory を使用して、内部および外部ユーザー・プロファイルを格納し、ユーザー情報が内部ユーザーと外部ユーザーの両方に対して同一に構成されます。同じ論理 Oracle Internet Directory 内の両方のタイプのユーザーのユーザー・プロファイルの格納には、別のサブツリーを使用します。パスワード・ポリシーは、両方のタイプのユーザーに対して同じにすることができます。

このタイプのデプロイでは、次の機能が実装されます。

- 内部ユーザーと外部ユーザーにアクセス権を付与するアプリケーション・デプロイ
- 集中サービスおよび管理

図 3-3 1 つの ID 管理インフラストラクチャの使用



例 B: 2 つの ID 管理インフラストラクチャの使用 : セキュリティ分離

この例では、2 つの ID 管理インフラストラクチャを使用します。図 3-4 に示すように、エンタープライズ・ネットワークの内部と外部からアプリケーションにアクセスするユーザー用にそれぞれ 1 つずつ使用します。このタイプのデプロイでは、内部と外部のユーザー・リポジトリ間に明確な境界があります。外部ユーザーが制限されている場合は、内部ユーザーがより多くのリソースを使用できます。

この例で説明する分離を実現するために必要な多くのデプロイ手段があります。エクストラネット・ポータルのディレクトリ・サービスの分離は重要な手段です。従業員の ID および機密性のないプロファイル情報のみがエンタープライズ・ディレクトリと同期されますが、イントラネット・アプリケーションの ID および関連メタデータはレプリケートされません。外部ユーザー ID（自己登録またはそれ以外）、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、プリファレンス、および外部ポータルに接続されているアプリケーションの ID とロールは専用のディレクトリ内で表現されますが、エンタープライズ・ディレクトリにはレプリケートされません。情報モデルが両方の論理 Oracle Internet Directory インスタンス内で同じであることが最適です。

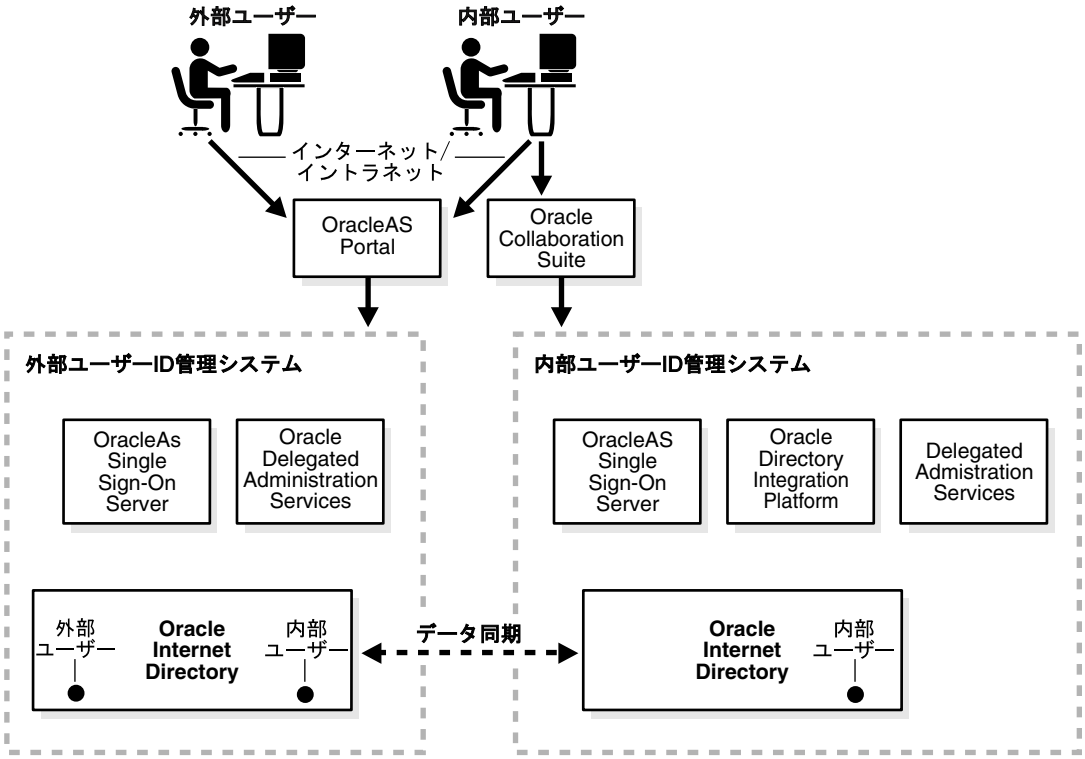
DNS ベースのルーティングを使用して、ユーザーを異なる ID 管理インフラストラクチャにルーティングして、シングル・サインオン認証を実現できます。

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外部ユーザーは、外部ポータル、および Oracle Collaboration Suite などの内部的にデプロイ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・アクセスを行うことができます。

このタイプのデプロイでは、次の機能が実装されます。

- セキュリティ分離 : エクストラネット環境とイントラネット環境など、分離が必要なアプリケーション・グループ間に境界が提供されます。
- アクセス : 内部ユーザーと外部ユーザーは 2 つの ID 管理インフラストラクチャを使用してアプリケーションにアクセスできます。
- データ同期 : アプリケーションの必須データが 2 つの ID 管理インフラストラクチャ間で同期されます。
- 可用性 : 内部ユーザーと外部ユーザーに対して別々の ID 管理インフラストラクチャを使用できます。

図 3-4 2 つの ID 管理インフラストラクチャの使用



部門アプリケーションに管理自律性を提供するモデル

多くの大規模企業では、独立した部門単位内にアプリケーションの管理自律性が必要な場合があります。このタイプのデプロイは、部門ネットワークと組織単位内で独立して管理されるアプリケーションに管理自律性を提供します。

このタイプのデプロイでは、ファンアウト・レプリカが自律管理アプリケーションのローカル・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、集中レプリカからの 1 方向または双方向レプリケーションで構成されたレプリケート済 Oracle Internet Directory です。ローカル・アプリケーションをローカル・インフラストラクチャに対して直接デプロイおよび管理するために、編集可能なものとして構成されています（レプリケーションの方向が集中レプリカからローカル・レプリカへの 1 方向の場合、結果として生成されるローカル情報は集中レプリカにレプリケートされません）。

例 A: アプリケーションの集中シングル・サインオンおよび部門自律性

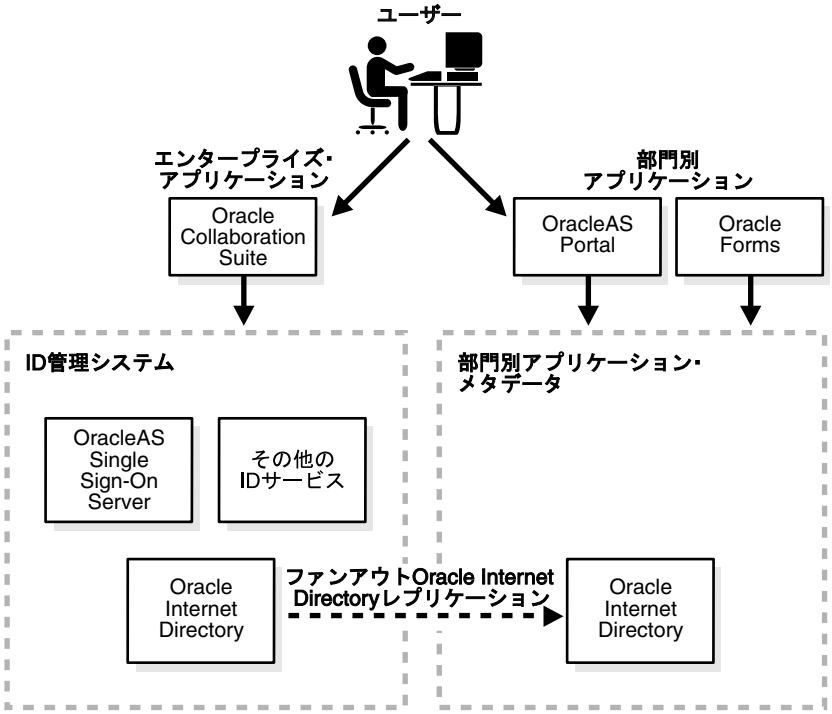
この例では、図 3-5 に示すように、アプリケーション・データをメンテナンスするための部門自律性を提供する一方で、企業全体に集中シングル・サインオンおよびユーザー・パスワード管理サービスを提供します。ユーザー認証には集中シングル・サインオンが使用されるため、アプリケーションは、集中 Oracle Internet Directory と部門の Oracle Internet Directory のどちらを使用するかに応じて、異なる Oracle Internet Directory インスタンスにリンクできます。

OracleAS Portal などのアプリケーションは、独立した部門別 Oracle Internet Directory サーバーを使用するようにインストールされますが、認証には集中 ID 管理サービスを使用します。ローカル管理者が部門アプリケーションを管理します。

このタイプのデプロイでは、次の機能が実装されます。

- 部門内のアプリケーションの管理自律性
- 集中 ID 管理インフラストラクチャ
- すべてのアプリケーション間での統一ログインおよびログアウト

図 3-5 集中シングル・サインオンおよび部門自律性



例 B: 部門別 ID 管理システム

図 3-6 に示すように、この例でもエンタープライズ・アプリケーションの集中 ID 管理サービスを使用しますが、部門ごとに別々の認証サービスを提供します。

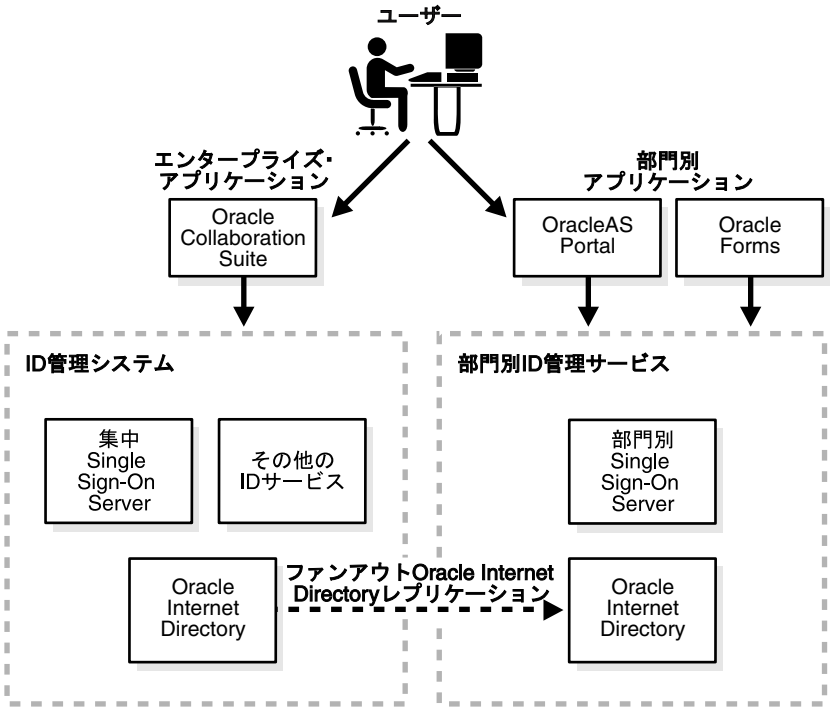
OracleAS Portal などのアプリケーションは、部門ごとの Oracle Internet Directory および OracleAS Single Sign-On サービスを使用するようにインストールされます。ローカル管理者が部門アプリケーションを管理します。

このモデルでは、各部門内のアプリケーションについてのみ、ユーザーのログインおよびログアウト操作性が統一されています。このモデルは、集中サービスで破滅的な停止が発生した場合のフェイルオーバー・プランとして役立ちます。ファンアウト Oracle Internet Directory レプリケーションを使用して、集中 Oracle Internet Directory から部門の Oracle Internet Directory にエンタープライズ・ユーザーおよびパスワード・ポリシー情報をレプリケートします。

このタイプのデプロイでは、次の機能が実装されます。

- 部門内のアプリケーションの管理自律性
- 部門自律性のための独立した ID 管理インフラストラクチャ
- 集中 ID 管理インフラストラクチャでの障害に影響されない部門アプリケーションの可用性の継続

図 3-6 部門別 ID 管理インフラストラクチャ



Windows 環境での ID 管理インフラストラクチャの統合のモデル

このデプロイでは、ID 管理インフラストラクチャと、Oracle Human Resources などの既存のエンタープライズ・アプリケーションおよび Microsoft Active Directory などのサード・パーティ LDAP サーバーの間のエンタープライズ・アプリケーション統合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

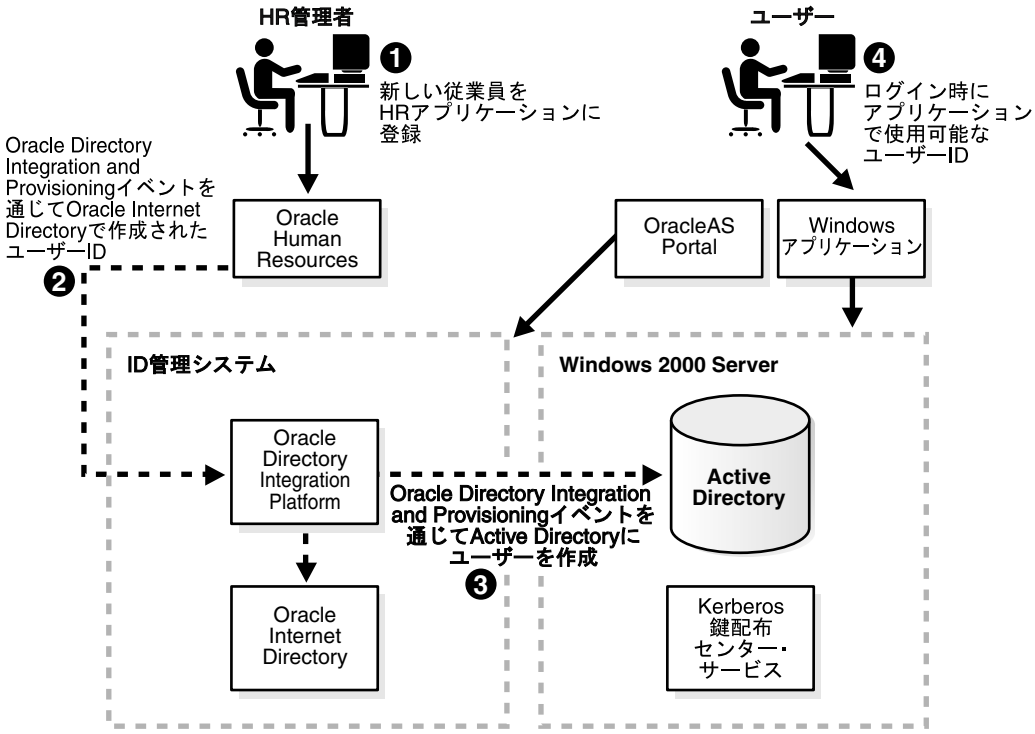
この例では、ユーザー・プロビジョニングは最初にエンタープライズ・アプリケーションにより起動されます。図 3-7 に示すように、Oracle Directory Synchronization Service を使用して、ユーザー ID が Oracle Internet Directory および Active Directory に作成されます。

ユーザー ID が Oracle Internet Directory に作成されると、OracleAS Single Sign-On はユーザーを認証し、Oracle Internet Directory 対応のアプリケーションがユーザー・データへのアクセス権を取得します。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・データへのアクセス権を取得します。

このタイプのデプロイでは、次の機能が実装されます。

- エンタープライズ・アプリケーションによってユーザー・プロビジョニングが起動され、ユーザー・プロファイル・データがアプリケーションから Oracle Internet Directory に同期される、エンタープライズ・ユーザー・プロビジョニング・システムとの ID 管理システム統合
- サード・パーティ・ディレクトリとの統合（この例では Active Directory 同期）
- ユーザー・アカウントが Oracle Internet Directory と Active Directory の両方で同期されると、ユーザーが Oracle Internet Directory と Active Directory の両方に対して有効になっているアプリケーションにアクセスできるようになる機能

図 3-7 エンタープライズ・プロビジョニングとの ID 管理インフラストラクチャ統合



例 B: Windows ユーザー・プロビジョニングとの統合

企業がユーザーおよびネットワーク・リソースを管理するための企業ディレクトリとして Active Directory をデプロイしている場合は、図 3-8 に示すように、ID 管理インフラストラクチャを既存の Active Directory と統合できます。

この例では、ユーザー・プロビジョニングは最初に Windows 環境で行われます。Windows 管理者は、Windows ツールを使用してシステム内のユーザー・アカウントをプロビジョニングできます。Active Directory 内の新規に作成されたユーザー・アカウント・データと Oracle Internet Directory の同期は、Oracle Directory Synchronization Service を使用して行われます。Active Directory ドメイン・ユーザー・データは、Oracle Internet Directory のデフォルト・レルム内で同期されます。エンタープライズ・デプロイに複数の Active Directory ドメインがある場合、それらのドメインは、1 つのレルム内の複数のサブツリーを使用して Oracle Application Server の Oracle Internet Directory を企業全体で使用するように構成されます。

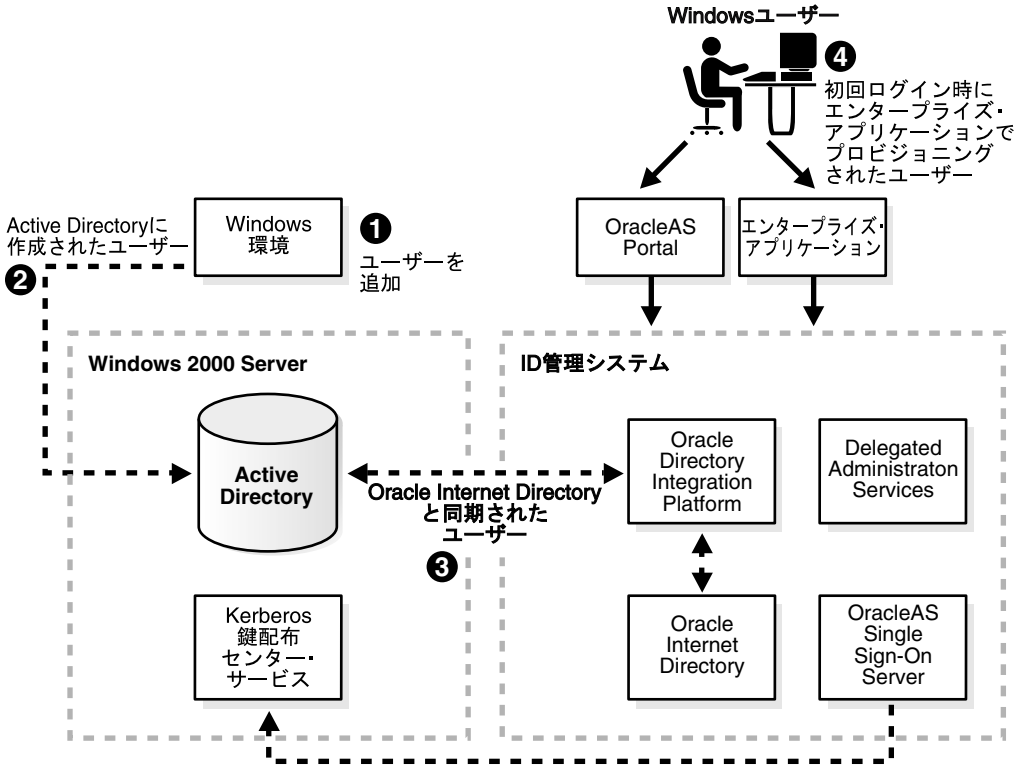
ユーザー・アカウントが Oracle Internet Directory と同期された後、エンタープライズ・アプリケーションはユーザー・プロファイルにアクセスでき、ユーザーは集中 OracleAS Single Sign-On を通じてアプリケーションにログインできます。

また、OracleAS Single Sign-On は、Windows Kerberos ベースのプロトコルを使用して Windows システム固有の認証をサポートします。この機能により、有効な Kerberos チケットを Windows 環境で発行したユーザーは、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。このサポートにより、Windows ユーザーは、ユーザーが Kerberos 対応の Windows デスクトップに正常にログインした後でポータル・アプリケーションに自動的にログインできます。Windows Kerberos 認証が可能でない場合は、Oracle Internet Directory 外部認証プラグインが Active Directory に対してユーザーを認証します。

このタイプのデプロイでは、次の機能が実装されます。

- 既存の Windows システムとの ID 管理インフラストラクチャのシームレスな統合
- サード・パーティ・ディレクトリとの統合
- パートナ・アプリケーションでのシングル・サインオンのための Windows Kerberos 認証との統合
- ID 管理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 Windows ユーザー・プロビジョニングとの ID 管理インフラストラクチャ統合



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集中 ID 管理インフラストラクチャのデプロイ

ASP デプロイでは、様々な ID 管理レルムをユーザーの様々なネームスペースに対して作成する必要があります。ASP 管理者は、顧客、サブスクライバ、またはその両方に対してホスティングされているアプリケーションを管理します。各サブスクライバには、ASP がユーザー、グループおよび関連ポリシーを管理する ID 管理レルムが関連付けられています。このデプロイでは、ASP サブスクライバごとに異なるレルムを使用して、すべての ASP ID 管理サービスに対して ID 管理インフラストラクチャを 1 つのみ使用します。

Oracle Internet Directory 内の複数のレルムを使用するのとは別に、複数のレルム機能を 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有効にする必要があります。

図 3-9 に、Acme および XY Corporation という 2 つの企業でのホスティング・デプロイを示します。

図 3-9 ホスティング・デプロイでの複数の ID 管理レルム

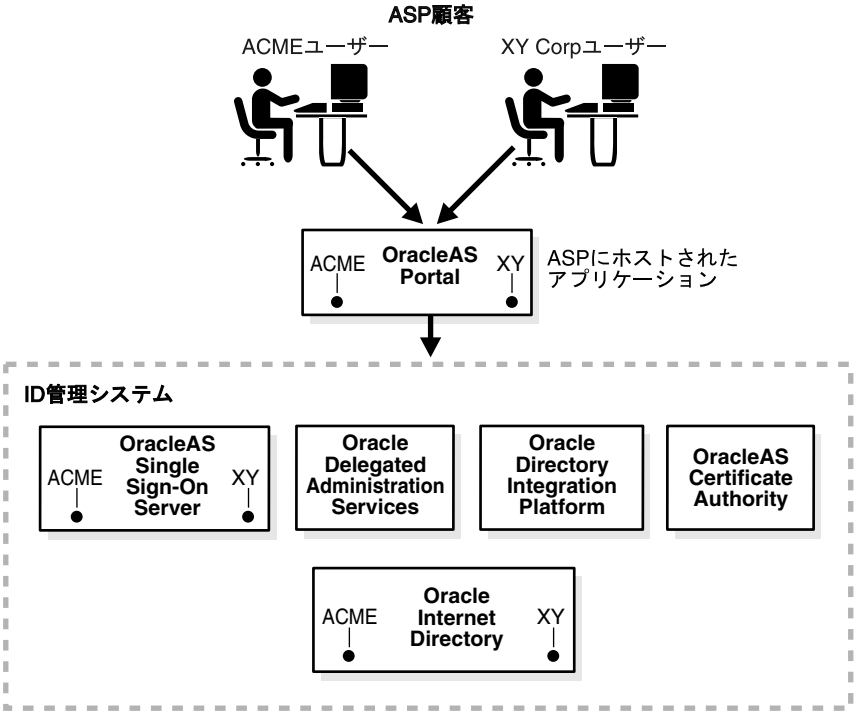


図 3-9 に示すように、デフォルトの ID 管理レルムに定義されている ASP ユーザーは、サブスクライバに対してホスティングされている各種アプリケーションを管理します。各サブスクライバには、ASP がユーザー、グループおよび関連ポリシーを管理する ID 管理レルムが関連付けられています。

ID 管理インフラストラクチャの詳細なデプロイ計画

ID 管理インフラストラクチャ・デプロイの論理アーキテクチャが決定された後、次の手順はデプロイのその他の詳細の決定です。これらには、ディレクトリ情報モデルの仕様と物理トポロジの詳細が含まれます。

この項では、ディレクトリ情報ツリー（DIT）の計画の詳細を説明し、高可用性およびパフォーマンス要件を満たすいくつかの物理トポロジをリストします。

詳細なデプロイ計画の最後に、要件を最もよく満たす DIT および物理トポロジが選択されている必要があります。最終的な物理ネットワーク・トポロジには、この項でリストする 1 つ以上の物理トポロジの組合せが含まれている場合があります。

物理トポロジを選択した後で、ID 管理インフラストラクチャのインストール・ドキュメントとコンポーネント固有の管理者ガイドで、インストールおよび詳細構成情報を参照してください。

デプロイ計画は、変化する企業ニーズを満たすのに十分な柔軟性を持つ必要のある反復プロセスです。実際の実装に加えて、ID 管理デプロイは、詳細に定義されたプロセスを設定して、ID 管理インフラストラクチャの状態およびパフォーマンスを監視し、必要に応じて修正処理を行う必要があります。

関連項目：「はじめに」の「関連ドキュメント」

この項の内容は次のとおりです。

ディレクトリ情報の論理編成の計画

ディレクトリ情報は、ディレクトリ情報ツリー（DIT）に編成されます。この項では、DIT の定義の詳細について説明します。デプロイ計画者は、目的を確認し、ニーズを最もよく満たす構成を識別し、その構成をデプロイ計画ガイドとして使用する必要があります。

この項の内容は次のとおりです。

サンプルのディレクトリ情報ツリー

ディレクトリは、Oracle とサード・パーティ両方の複数のアプリケーションによって使用される可能性があるため、DIT 構造全体を構成する相対識別名で使用されるネーミング属性は定式属性に制限される必要があります。次の属性は、ほとんどのディレクトリ対応アプリケーションで一般に定式になっている属性です。

- **c:** 国の名前
- **cn:** 共通名
- **dc:** DNS ドメイン名のコンポーネント
- **l:** 都市、国、その他の地域などの場所の名前
- **o:** 組織の名前
- **ou:** 組織単位の名前
- **st:** 州などの行政区画の名前

図 3-10 Oracle Internet Directory 情報ツリー

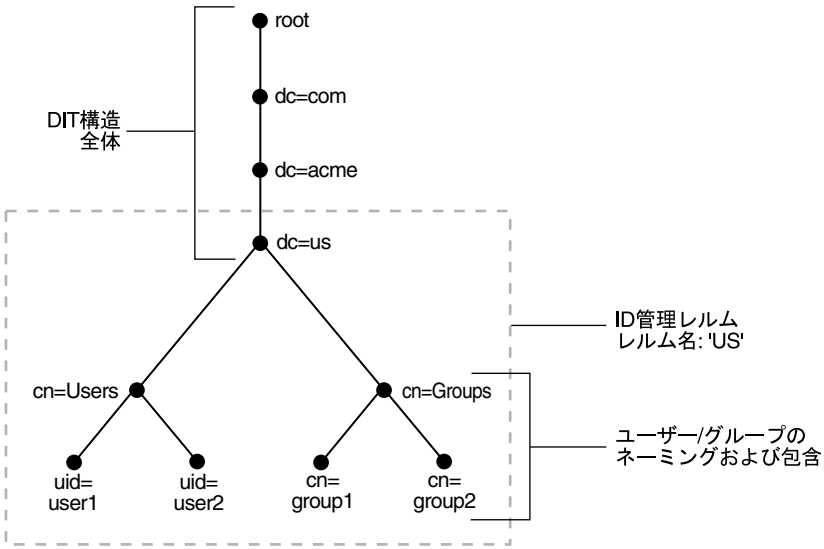


図 3-10 は、米国デプロイでのディレクトリ情報の論理編成について次の決定を行う Acme という架空の会社の DIT を示しています。

- ドメイン名ベースのスキーマを使用して DIT 階層全体を表します。ID 管理インフラストラクチャは米国にデプロイされるため、すべての情報を表すために選択された DIT は `dc=us,dc=acme,dc=com` です。
- コンテナ内で表されているすべてのユーザーは `cn=users` と呼ばれます。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（組織ベースの階層はありません）。また、すべてのユーザーの一意識別子として `uid` 属性が選択されています。
- コンテナ内で表されているすべてのエンタープライズ・グループは `cn=groups` と呼ばれます。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、すべてのグループ・エントリのネーミング属性は `cn` です。
- `US` という名前の ID 管理レルムのルートとして、コンテナ `dc=us` が選択されています。デプロイでは、`US` レルム内のすべてのユーザーに対して類似のセキュリティ・ポリシーを施行することが期待されます。

Oracle Internet Directory は ID 管理インフラストラクチャ全体の共有リポジトリであるため、適切に計画された DIT は、企業に次のような利益をもたらします。

- ID 管理インフラストラクチャが、デプロイ要件に即したセキュリティ・ポリシーを施行できます。
- より効率のよいディレクトリ・サービスの物理デプロイを実装できます。
- 企業がディレクトリ・サービスにすでに投資している場合でも、企業は Oracle Internet Directory との同期を迅速設定できます。

> **関連資料：** LDAP 属性の詳細は、『Oracle Internet Directory 管理者ガイド』を参照してください。

ディレクトリ情報ツリー構造全体の計画

このタスクの目的は、企業内のすべての ID 管理統合アプリケーションが次の目的に使用する基本的な DIT 階層を設計することです。

- ディレクトリ編成で効果的なアクセス制御を促進します。完全レプリケーションまたは部分レプリケーションの実装を計画している場合は、DIT 設計が分離を反映している場合にのみ、ディレクトリ・レプリケーションの適切な境界およびポリシーを施行できます。
- エンタープライズがサード・パーティ・ディレクトリ・サーバーと統合される場合は、Oracle Internet Directory の DIT 設計を既存の DIT に合せて、必要な同期プロセスの簡略化を試みます。この考慮事項は、他のベンダーのソフトウェアを操作するために Active Directory などの他のディレクトリのデプロイを将来的に計画することが必要な Oracle Internet Directory の現在のデプロイにも利益があります。この場合は、サード・パーティ・ディレクトリの計画済デプロイの優先 DIT 設計と一貫性のある Oracle Internet Directory の DIT 設計を選択すると、同期タスクがより管理しやすくなります。
- 単一企業シナリオでは、企業のドメイン名に合せた DIT 設計を選択するだけで十分です。たとえば、ドメイン名 `acme.com` を所有する企業で Oracle Internet Directory が設定される場合は、`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` 内の `engineering` のような部門レベルまたは組織レベルのドメイン・コンポーネントの使用はお薦めしません。ほとんどの企業では、頻繁な部門再構成と再編成が行われます。企業ディレクトリを組織変更からできるだけ分離することが重要です。
- 企業が X.500 ディレクトリ・サービスをデプロイし、他のサード・パーティ LDAP ディレクトリが本番環境にない場合、企業は国ベースの DIT 設計を選択すると利益がある場合があります。たとえば、`o=acme,c=US` というルートのある DIT 設計は、X.500 ディレクトリ・サービスがすでに存在する企業により適している場合があります。

ユーザーとグループのネーミングおよび包含の計画

DIT 設計全体に適用される設計考慮事項のほとんどは、ユーザーおよびグループのネーミングと包含にも適用されます。ただし、Oracle Internet Directory でユーザーおよびグループを構成する際には注意する必要のある追加の考慮事項があります。

ユーザー ID に関する考慮事項

ID 管理インフラストラクチャは、すべてのユーザー ID のリポジトリとして Oracle Internet Directory を使用します。ユーザーが企業内の複数のアプリケーションにアクセスするアカウントを持っている場合でも、Oracle Internet Directory には特定のユーザーの ID を表すエントリが 1 つのみあります。Oracle Internet Directory およびその他のインフラストラクチャ・コンポーネントをデプロイする前に、DIT 全体でのこれらのエントリの場所と内容を企業で計画する必要があります。

ユーザー ID を計画する際には、次のことを考慮します。

- ディレクトリ構造全体の計画と同様に、現在の部門アフィリエーションおよび階層に基づいてユーザーを編成するのは避けます。かわりに、ユーザーの組織情報を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。
- 組織アフィリエーションや管理チェーンに基づいてユーザーを階層に編成するパフォーマンス上の利点はないため、ユーザーを含む DIT はできるだけフラットに保つ必要があります。
- デプロイのユーザー数が異なり、それぞれが異なる組織によってメンテナンスおよび管理されている場合は、これらの管理境界に基づいてユーザーをコンテナに分割して、アクセス制御の設定を簡略化し、レプリケーションが必要な場合に役立つようにすることをお薦めします。
- ユーザーを一意に識別するデフォルト属性は、cn または `CommonName` です。`CommonName` の典型的な値はその人物のフルネームです。ただし、人物の名前は変更される場合や一意でない場合があります。できれば、`uid` 属性など、変更されず、ユーザーを一意に識別する代替属性を選択してください。
- 通常、ほとんどの企業には、従業員の一意の名前と番号の割当てルールを設定する人事管理部門があります。ディレクトリ・エントリの一意ネーミング・コンポーネントを選択する場合は、この管理インフラストラクチャを利用し、そのポリシーを使用する必要があります。
- ディレクトリに作成されたすべてのユーザー・エントリは、オブジェクト・クラス `inetOrgPerson` および `orclUserV2` に属する必要があります。
- 企業がサード・パーティ・ディレクトリを使用している場合、または将来サード・パーティ・ディレクトリをデプロイすることを計画している場合は、ユーザー・ネーミングとディレクトリ包含を、サード・パーティ・ディレクトリで一般に使用されるものに合せて、分散ディレクトリの同期およびその後の管理を簡略化します。

グループ ID に関する考慮事項

ID 管理インフラストラクチャと統合される一部のアプリケーションは、その認証を、デプロイで作成された Oracle Internet Directory 内の企業全体のグループに基づいて行うこともできます。ユーザー ID と同様に、グループ ID の場所と内容は慎重に計画する必要があります。

グループ ID の計画の考慮事項は次のとおりです。

- 階層内のエンタープライズ・グループの編成を組織のアフィリエーションや所有権に基づいて行うパフォーマンス上の利点はありません。グループを含む DIT はできるだけフラットに保ち、すべてのアプリケーションによってグループが簡単に検出されるようにし、アプリケーション間でのこれらのグループの共有を促進します。
- DIT 内のユーザーとグループを分離し、エントリ・セット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ために使用される属性は、`cn` または `CommonName` である必要があります。
- ディレクトリ内のすべてのグループ・エントリがオブジェクト・クラス `groupOfUniqueNames` および `orclGroup` に属するようにすることをお薦めします。groupOfUniqueNames オブジェクト・クラスは、グループを表すためのインターネット標準です。orclGroup オブジェクト・クラスは、セルフサービス・コンソールを利用してグループを管理するために使用できます。
- 企業全体の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かわりに、グループの所有者属性を使用して、どのユーザーがこのグループを所有するかをリストし、所有者属性にリストされているすべてのユーザーに変更や削除などの特殊な権限を付与する上位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` 属性に説明テキストを移入して、ユーザーがグループの目的を簡単に理解できるようにすることを検討します。
- `orclGroup` オブジェクト・クラスの `displayName` 属性を設定して、Oracle Delegated Administration Services 単位およびセルフサービス・コンソールにより判読しやすいグループ名を表示できるようにすることを検討します。
- デプロイに異なるグループ・セットがあり、それぞれが異なる管理ポリシーを持つ異なる組織によってメンテナンスおよび管理されている場合は、これらの管理境界に基づいてグループをコンテナに分割して、アクセス制御の設定を簡略化し、レプリケーションが必要な場合に役立つようにすることをお薦めします。
- 企業がサード・パーティ・ディレクトリを使用している場合、または将来サード・パーティ・ディレクトリをデプロイすることを計画している場合は、グループ・ネーミングとディレクトリ包含を、サード・パーティ・ディレクトリで一般に使用されるものに合せて、分散ディレクトリの同期およびその後の管理を簡略化します。

ID 管理レルムの計画

前の項では、DIT 全体の構成とユーザーおよびグループの配置のガイドラインを説明しました。これらのガイドラインの実装によりデプロイ構成が多様になる可能性があるため、ディレクトリ自体のメタデータ内にデプロイの意図を取り込む必要があります。このメタデータにより、Oracle ソフトウェア、および ID 管理インフラストラクチャに依存する他のサード・パーティ・ソフトウェアは、デプロイの意図を理解し、カスタマイズされた環境で正常に機能できます。

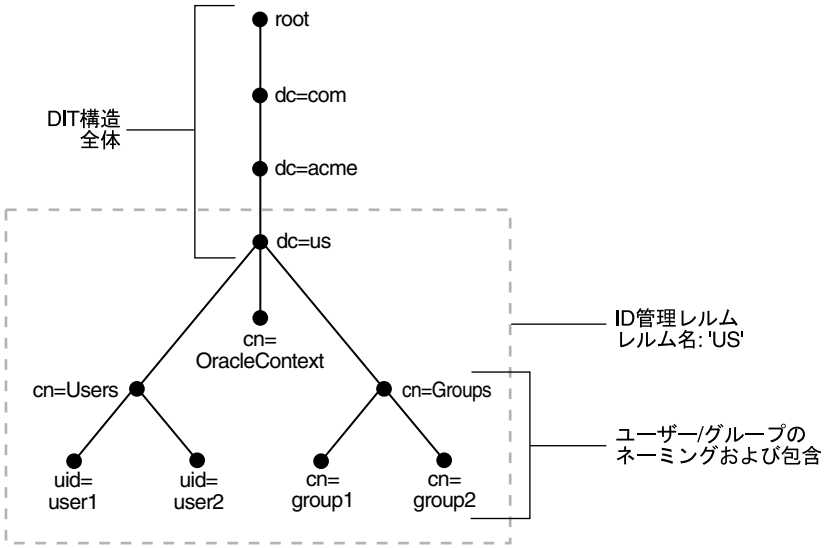
Oracle Internet Directory 内の ID 管理レルムは、このデプロイの意図を取得し、デプロイでエンタープライズ・ユーザーおよびグループに関連する ID 管理ポリシーを設定できるようにします。

DIT 全体と、ユーザーおよびグループの配置を選択した後で、Oracle Internet Directory で ID 管理レルムのルートとして機能するディレクトリ・エントリを識別します。このエントリは、ID 管理レルムに定義されている ID 管理ポリシーの有効範囲を決定するのに役立ちます（デフォルトでは、有効範囲は ID 管理レルムのルートの下のディレクトリ・サブツリー全体です）。このエントリの下に、次の内容を含む `OracleContext` という特殊エントリが作成されます。

- デプロイ固有の DIT 設計（ユーザーおよびグループのネーミングと配置を含む）
- このレルムに関連付けられている ID 管理ポリシー
- Oracle アプリケーションにプライベートな追加のレルム固有情報

図 3-11 に、ドメイン名ベースの DIT 構造を使用する Acme 社のデプロイを示します。

図 3-11 ID 管理レルム



この場合、コンテナ `dc=us,dc=acme,dc=com` は ID 管理レルムのルートとして選択されたディレクトリ・エントリです。`cn=OracleContext` コンテナは、ユーザーおよびグループのネーミングおよび包含ポリシーを含む、レルム固有のポリシーを格納します。

ルートが `dc=us` である新しい ID 管理レルムが作成されます。デフォルトでは、ID 管理レルムの有効範囲は、ルートの下のディレクトリ・サブツリー全体に制限され、その名前は `us` です。

Oracle Internet Directory で ID 管理レルムを計画する際には、次のことを考慮します。

- 企業のセキュリティ・ニーズにより、ID 管理レルムのルートの選択が指示されます。通常は、ほとんどの企業は Oracle Internet Directory に 1 つの ID 管理レルムのみ必要とします。
- 企業がサード・パーティ・ディレクトリを使用している場合、または将来サード・パーティ・ディレクトリをデプロイすることを計画している場合は、ID 管理レルム・ルートの選択を、サード・パーティ・ディレクトリの DIT 設計に合せて、分散ディレクトリの同期およびその後の管理を簡略化します。

- Oracle Internet Directory コンフィギュレーション・アシスタント、Oracle Internet Directory セルフサービス・コンソール、その他のコマンドライン・ツールなどの Oracle Internet Directory 管理インタフェースを使用して、Oracle Internet Directory で ID 管理レルムを設定および管理します。
- ID 管理レルムが設定された後で、ディレクトリのネーミングおよび包含ポリシーを計画して、デプロイで行われたカスタマイズを反映します。この更新は、ID 管理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および使用する前に行う必要があります。

関連資料：

- ID 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。
- 情報モデルのデフォルトについては、付録 B「Oracle Internet Directory のデフォルトの設定」を参照してください。

物理ネットワーク・トポロジの計画

ID 管理インフラストラクチャに対する物理トポロジの選択は、多くの要件の影響を受けます。最も一般的な要件は、高可用性とスケーラビリティです。

高可用性は、システムが非常に高い時間割合で処理および機能を継続する能力です。高可用性は、シングル・ポイント障害を削減し、冗長コンポーネントを使用することで実装できます。同様に、複数の ID 管理コンポーネント・インスタンスをロード・バランサと組み合せると、高可用性環境を提供できます。

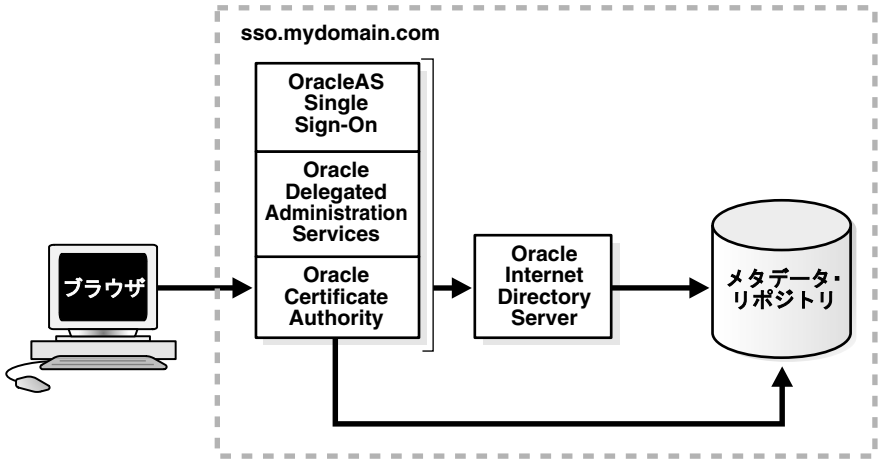
この項では、高可用性およびスケーラビリティのために使用できるいくつかの物理トポロジについて説明し、各デプロイ例の利点を強調します。目的を確認し、企業の要件に最もよく合致する構成を識別する必要があります。

この項の内容は次のとおりです。

ID 管理インフラストラクチャのデフォルト・デプロイ

Oracle Application Server インフラストラクチャのデフォルト・インストールでは、図 3-12 に示すように、OracleAS Single Sign-On、Oracle Application Server Certificate Authority および Oracle Delegated Administration Services を含むすべてのインフラストラクチャ・コンポーネントを同じシステムにインストールします。

図 3-12 OracleAS Single Sign-On および Oracle Delegated Administration Services のデフォルト・デプロイ



このデプロイは単純であり、OracleAS Single Sign-On、Oracle Application Server Certificate Authority および Oracle Delegated Administration Services をリポジトリおよび Oracle Internet Directory の一部として自動的に構成します。このデプロイは、迅速なデプロイの設定または環境のテストには十分です。

DMZ ネットワークでの ID 管理インフラストラクチャのデプロイ

本番デプロイでは、OracleAS Single Sign-On サーバー全体をパブリック・ネットワークに公開しないことをセキュリティ・ポリシーで指定できます。この指定を行う 1 つの方法は、図 3-13 に示すように、Oracle Application Server インフラストラクチャ中間層を DMZ にデプロイし、Oracle Internet Directory およびその基礎となるメタデータ・リポジトリをイントラネット・ファイアウォール内にデプロイすることです。

Oracle Delegated Administration Services および Oracle Application Server Certificate Authority は中間層コンポーネントであるため、考慮事項は OracleAS Single Sign-On 中間層の場合と同じです。

このデプロイは、Oracle Internet Directory からのインフラストラクチャ中間層とその基礎となるメタデータ・リポジトリ間を分離します。

Oracle Application Server Certificate Authority 中間層と Oracle Application Server Certificate Authority リポジトリ間にネットワーク・レベルの暗号化を提供して、Oracle Application Server Certificate Authority 中間層とリポジトリ間でセキュリティ分離が行われるようにする必要があります。

図 3-13 DMZ 内の OracleAS Single Sign-On、Oracle Delegated Administration Services デプロイおよび Oracle Application Server Certificate Authority

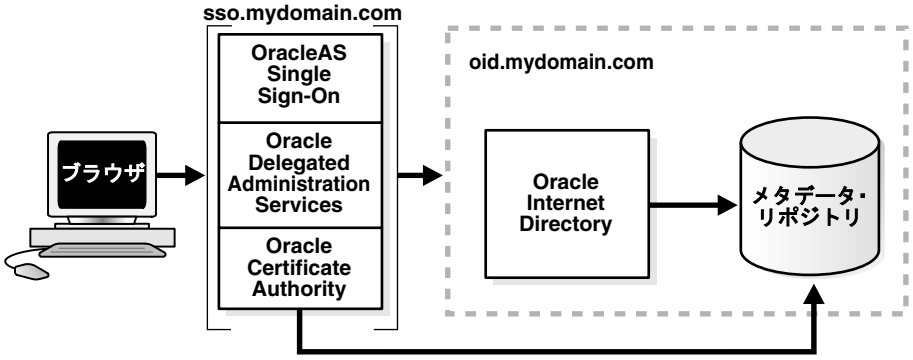
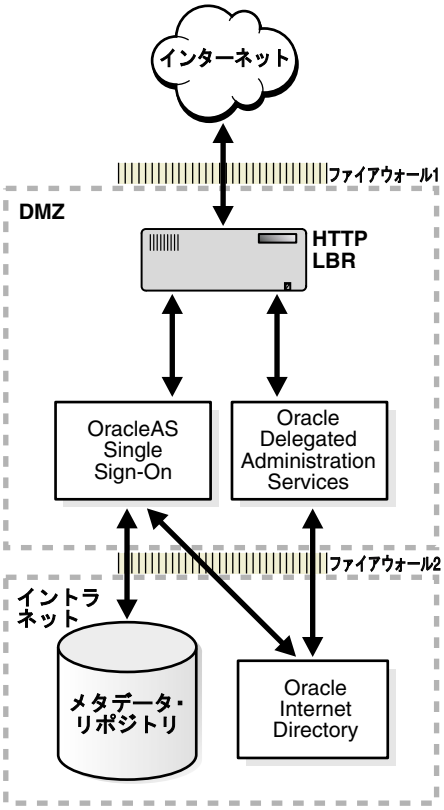


図 3-14 の上位レベル・デプロイ・トポロジは、Web 対応のコンポーネントが DMZ に配置される一方で Oracle Internet Directory およびその基礎となるメタデータ・リポジトリをイントラネット・ゾーンで使用可能にする Oracle Application Server インストール環境を示しています。インターネット Web トラフィックは、トラフィックを Web 対応コンポーネントにルーティングする HTTP ロード・バランサにルーティングされます。このデプロイ構成では、Oracle Internet Directory およびその基礎となるメタデータ・リポジトリがファイアウォールでインターネット・トラフィックから分離されるため、セキュリティが向上します。

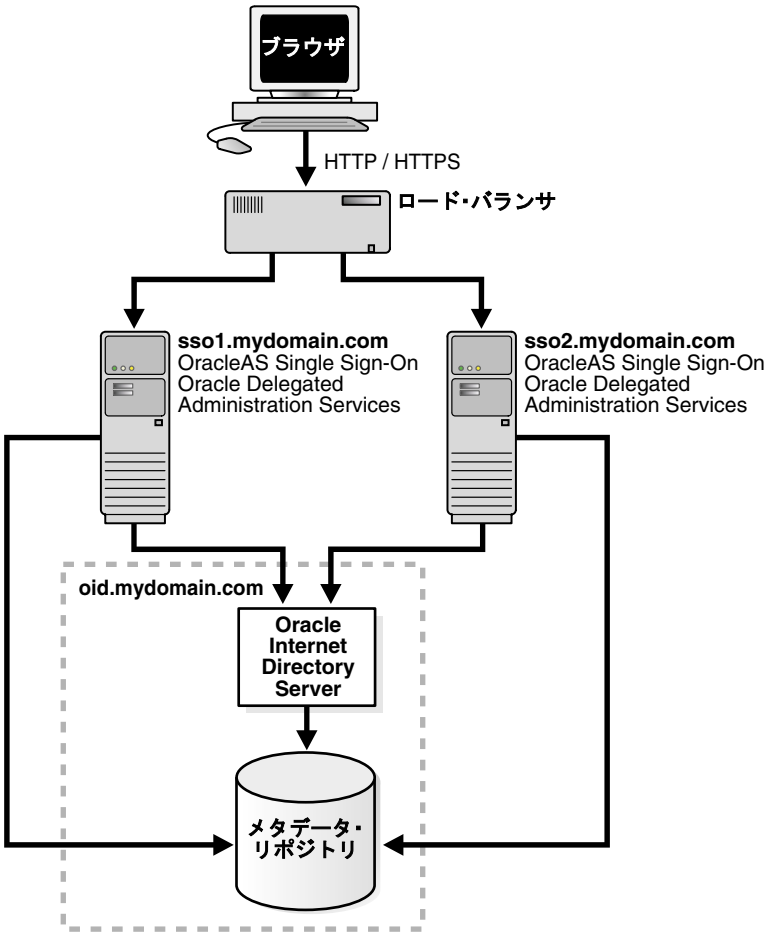
図 3-14 DMZ 内の OracleAS Single Sign-On、Oracle Delegated Administration Services デプロイおよび HTTP ロード・バランサ



複数の中間層を使用した ID 管理インフラストラクチャのデプロイ

可用性の高いデプロイが必要な場合は、負荷を処理しフェイルオーバー・プロセスをサポートするために複数の OracleAS Single Sign-On および Oracle Delegated Administration Services 中間層をデプロイできます。複数の OracleAS Single Sign-On 中間層がデプロイされても、これらは同じ Oracle Internet Directory サーバーを使用します。図 3-15 に示すように、このデプロイは、インフラストラクチャ中間層を追加することでスケーラビリティを向上させます。

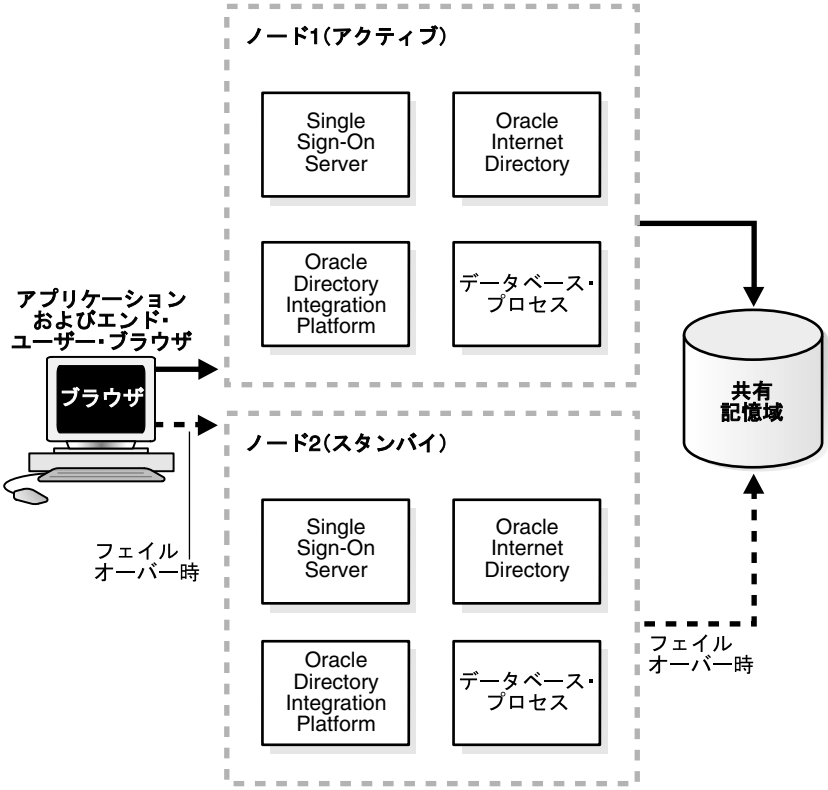
図 3-15 1 つの Oracle Internet Directory Server がある複数の OracleAS Single Sign-On および Oracle Delegated Administration Services 中間層



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した ID 管理インフラストラクチャのデプロイ

コールド・フェイルオーバー・デプロイは、ローカル・ハードウェアおよびソフトウェア障害からの保護を提供するサイト間の高可用性ソリューションです。

図 3-16 コールド・フェイルオーバーを使用した Oracle Internet Directory デプロイ



このデプロイでは、2 ノードのハードウェアベース・クラスタを使用して高可用性を実現します。図 3-16 に示したように、2 つのノードが共有記憶域ディスクに接続されます。ID 管理インフラストラクチャは、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上にあるかぎり、1 つしかインストールする必要はありません。仮想論理 IP アドレスがノード 1 上でアクティブであるため、ノード 1 がプライマリ（アクティブ）ノードで、ノード 2 がセカンダリ（スタンバイ）ノードです。

ノード 1 に障害が発生した場合は、論理 IP アドレスがノード 2 に移ります。その後、すべてのインフラストラクチャ・プロセスはノード 2 で開始されます。論理 IP アドレスと共有記憶域が移動し、メタデータ・リポジトリ、データベース・リスナーおよび他のすべてのプロセスが開始されるときに、ID 管理インフラストラクチャにアクセスしているアプリケーション・プロセスは一時的にサービスを失います。

コールド・フェイルオーバー・ソリューションは、フェイルオーバー中に若干サービスを失いますが、高可用性を提供します。

レプリケートされた ID 管理インフラストラクチャ

レプリケーション対応の Oracle Identity Management は、デプロイ要件に応じて異なる構成でデプロイできます。たとえば、2 つ以上のマルチマスター・レプリケーション・ノードを異なる場所にデプロイすると、分散 ID 管理が可能になります。同じ構成を 1 つの場所にデプロイすると、ローリング・アップグレードがサポートされます。

高可用性デプロイ要件がある場合は、複数の OracleAS Single Sign-On 中間層をデプロイして、負荷に対応し、フェイルオーバー・アクセスをサポートできます。Oracle Internet Directory サーバーは、図 3-17 に示すように、可用性の高い Oracle Internet Directory サーバーを提供するためにレプリカとして設定できます。

このデプロイは、Oracle Application Server インフラストラクチャをインストールする前に計画する必要があります。計画には、OracleAS Single Sign-On および Oracle Internet Directory サーバーの URL の提供と、インフラストラクチャ中間層と Oracle Internet Directory 両方のロード・バランサの設定が含まれます。

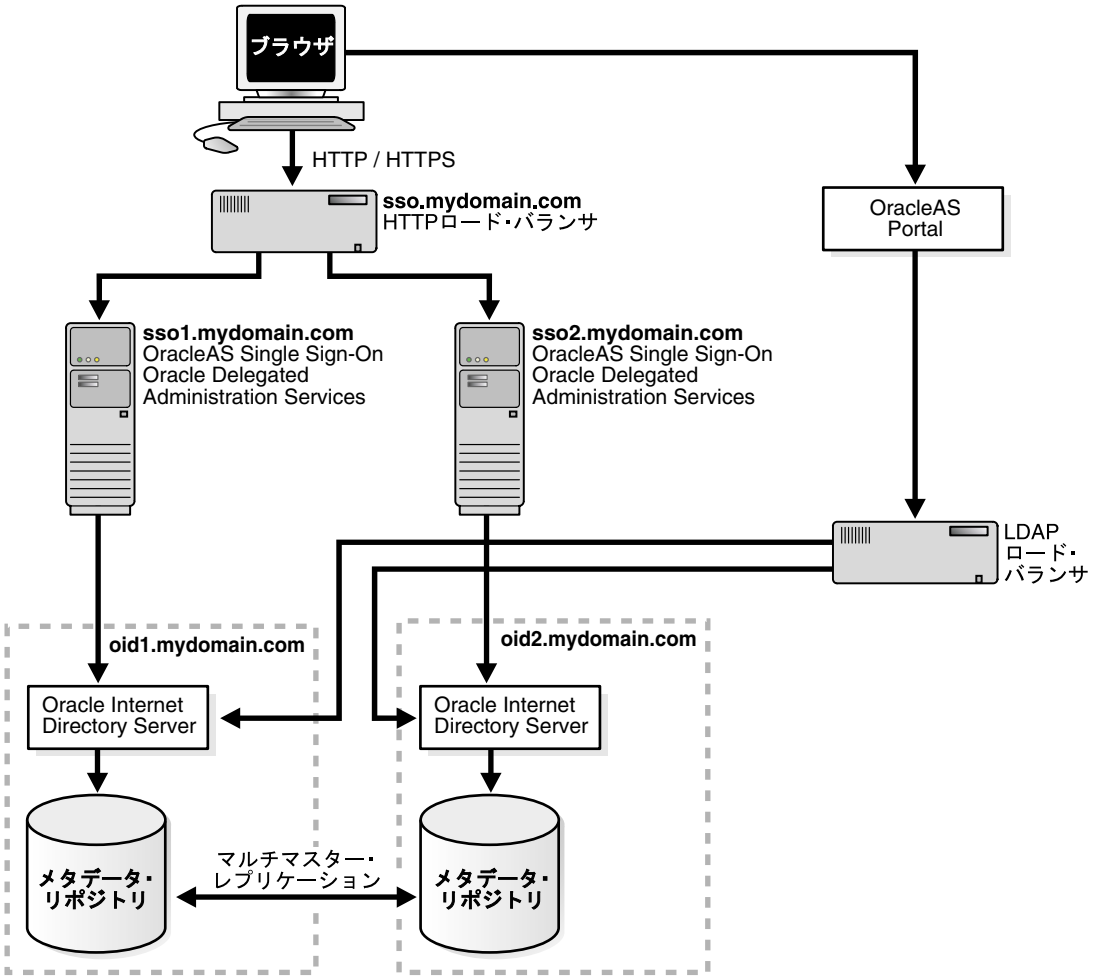
Oracle Internet Directory のロード・バランサは、永続ルーティングを行い、フェイルオーバーを使用するように構成する必要があります。リクエストをロード・バランスするようにロード・バランサを構成する必要はありません。

このデプロイでは、Oracle Internet Directory サーバーと OracleAS Single Sign-On 中間層の両方に高可用性とフェイルオーバーが提供されます。

Oracle Internet Directory 中間層レプリケーションには次の利点があります。

- **シングル・ポイント障害がない :** 複数の同一レプリカにより、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・サービスがシングル・ポイント障害になることが防止されます。
- **透過的フェイルオーバー :** レプリカのネットワークの前にロード・バランサまたはルーティング要素を配置することにより実現されます。これらの要素は、Oracle Internet Directory ノードが使用不能になった場合にアプリケーションがネットワーク内の他のノードに透過的にフェイルオーバーするように構成されます。
- **ロード・バランス :** あるノードが過負荷になってもパフォーマンスが低下しないように、ロード・バランサを使用してレプリケーション・ネットワーク内の Oracle Internet Directory ノード間でアプリケーションおよびユーザー・アクセス・リクエストを分散することにより実現されます。

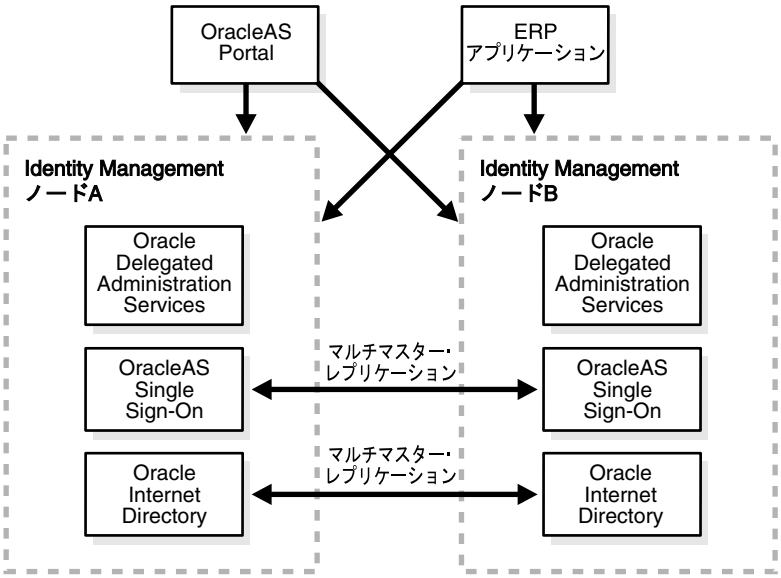
図 3-17 レプリケートされた Oracle Internet Directory ネットワーク内の複数の OracleAS Single Sign-On および Oracle Delegated Administration Services 中間層



- **ローリング・アップグレード・サポート :** エンタープライズ組織では、クリティカルなビジネス・アプリケーションは、ID 管理システムが中断することなくサービスを提供することを必要とします。ただし、パッチ適用やアップグレードなどのメンテナンス作業を実行するためにシステムをしばらく使用不能にすることが必要な場合があります。この問題は、Oracle Identity Management でマルチマスター・レプリケーションをデプロイすることで解決できます。この構成では、メンテナンスのためにレプリケーション・グループからレプリカ・ノード B を除外し、その間に他のノードがビジネス・アプリケーション・リクエストを処理できます。メンテナンス作業が完了した後で、ノード B をオンラインに戻してアプリケーション・リクエストを処理できます。その後ノード B は、ノード B がオフラインのときに発生した変更をノード A から取得します。他のノードは、この手順を繰り返すことでアップグレードまたはパッチ適用できます。

図 3-18 では、Oracle Identity Management ノード A は、ノード B がメンテナンスのためにオフラインになっているときに OracleAS Portal および Oracle Collaboration Suite アプリケーションにサービスを提供します。ノード B のメンテナンス・プロセスが完了すると、ノード A がメンテナンスのためにオフラインになり、その間、アプリケーションはアップグレードされたノード B で動作します。

図 3-18 マルチマスター・レプリケーションでのローリング・アップグレード・サポート



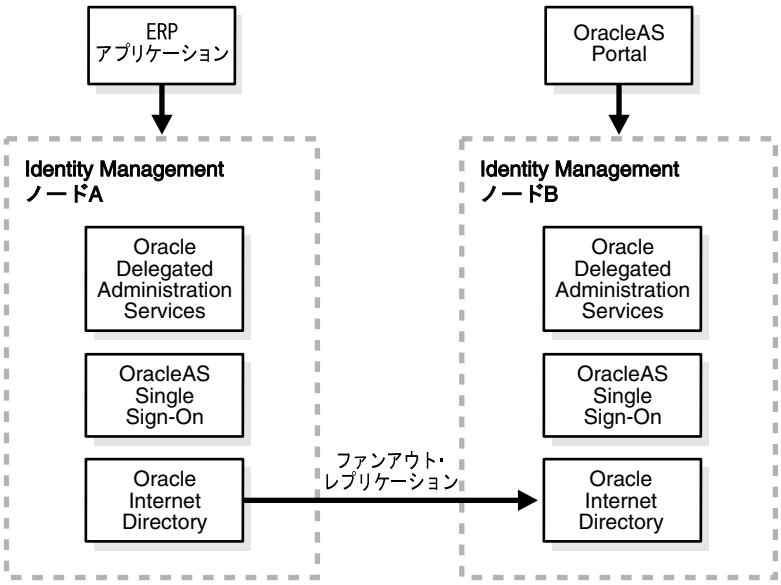
関連資料：『Oracle Application Server 高可用性ガイド』の、マルチマスター・レプリケーションでの Oracle Identity Management のデプロイに関する高水準の説明

ファンアウト・レプリケーション・デプロイ

Oracle Internet Directory は、ファンアウト・レプリケーションをサポートします。この構成では、マスター・レプリカに対する変更がファンアウト・レプリカに伝播されます。伝播は 1 方向または双方向にすることができ、DIT 全体または DIT のサブセットを含むことができます。DIT のサブセットを含む場合は部分レプリカと呼ばれます。

図 3-19 では、ID 管理ノード B がノード A のファンアウト・レプリカです。ノード A のデータがファンアウト・ノードであるノード B に 1 方向にレプリケートされます。ノード A の ID 管理システムは、ERP アプリケーションにサービスを提供します。ファンアウト・ノード B は Oracle Portal にサービスを提供します。

図 3-19 ファンアウト・レプリケーション・デプロイ



Oracle Identity Management のファンアウト・レプリケーションは、エンタープライズ組織の次のビジネス要件に対処します。

- **セキュリティ分離 :** Oracle Portal などのエンタープライズ・アプリケーションは、内部ユーザーと外部ユーザーの両方に対して使用可能になっている必要があります。その結果、エンタープライズ・アプリケーションは、従業員（内部）ID とその他の（外部）ID 両方のプロファイルおよび権限情報をメンテナンスする必要があります。この統合は最適ですが、企業イントラネット・リソースが外部ユーザーから分離され、またイントラネット・アプリケーションが外部ポータルを対象とした DoS 攻撃から完全に保護されるようにすることも重要です。これは、内部ユーザーのセキュリティ情報を提供するマスター管理ノードと、外部ユーザーを担当するファンアウト ID 管理レプリカを設定することで実現できます。同時に、内部ユーザーはファンアウト・レプリカを使用してデプロイ済ポータルにアクセスすることもできます。
- **管理の分離 :** この例では、アプリケーション・データをメンテナンスするための部門自律性を提供する一方で、企業全体に集中シングル・サインオンおよびユーザー・パスワード管理サービスを提供します。アプリケーションは、集中 Oracle Internet Directory と部門の 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が、ユーザー認証には集中シングル・サインオンが使用されます。

  OracleAS Portal などのアプリケーションは、独立した部門別 Oracle Internet Directory サーバーを使用するようにインストールされますが、認証には集中 ID 管理サービスを使用します。ローカル管理者が部門アプリケーションを管理します。

このタイプのデプロイでは、次の機能が実装されます。

- 部門内のアプリケーションの管理自律性
- 集中 ID 管理インフラストラクチャ
- すべてのアプリケーション間での統一ログインおよびログアウト

- **パフォーマンス分離 :** エンタープライズ組織では、ディレクトリ対応のアプリケーションがエンタープライズ・ディレクトリ・データにアクセスする必要があります。すべてのアプリケーションがディレクトリ・データにアクセスする必要がありますが、過負荷のアプリケーションは予想外に高い負荷をディレクトリに課すことがあります。これにより、ディレクトリ・サービスが使用不能なためにすべてのアプリケーションに対してサービスが停止する場合があります。この問題に対処するために、ファンアウト・レプリカをデプロイでき、特定のディレクトリ・インスタンスにアクセスするようにアプリケーションを構成してディレクトリ・サービスの負荷を分離できます。
- **アプリケーションのメンテナンスおよびアップグレードの分離 :** エンタープライズ組織の部門管理者は、部門のファンアウト・レプリカ・ノードを使用して OracleAS Portal などの Oracle アプリケーションをインストールし、ローカルの部門ニーズに対処できます。これらの部門アプリケーションでは、エンタープライズ・ユーザー・セキュリティ情報を使用できる一方、これらのアプリケーションおよび対応するディレクトリ・データを独立して管理できます。また、部門管理者は、ファンアウト・ディレクトリ・ノードに関連付けられているアプリケーションを独立してアップグレードできます。

  ファンアウト・レプリカは、次のような企業の高度なデプロイ要件をサポートするためにさらにカスタマイズできます。

  - マスターからデータのサブセットをレプリケートします。
  - データ変更をマスターに伝播するためにファンアウト・レプリカにプラグインを構成します。

  たとえば、企業では、ファンアウトでのパスワードの変更を許可する一方で、それらをマスター・レプリカに同期することが必要な場合があります。

  関連項目 : 付録 A の、ファンアウト・レプリケーションでの Oracle Identity Management のデプロイに関する高水準の説明

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・デプロイ

ディレクトリ・レプリケーションは非同期メカニズムであるため、ネットワーク内のディレクトリ・ノードは緩やかに一貫しています。ディレクトリ・レプリケーション・メカニズムは、ネットワーク内のノードに対して変更が行われた場合に、他のすべてのノードが最終的に収束し、許容される時間間隔内に一貫することを保証します。ただし、すべてのノードが常に同一であることは保証されません。

レプリカ間の疎結合の結果、レプリケーション・ネットワーク内の異なる物理ディレクトリ・サーバーに接続されている異なるアプリケーションは、ディレクトリ・ビューで一時的に一貫性を失う場合があります。このような一時的な非一貫性は、アプリケーション・ユーザーに悪影響を与えず、一般には許容されます。ただし、これがユーザーに影響を与える可能性のある状況があります。たとえば、パスワードのリセット時に、その結果による変更が OracleAS Single Sign-On の接続先のディレクトリ・サーバーで即時に反映されない場合、ユーザーが混乱したり不便が生じたりします。

非同期レプリケーションによる一時的な非一貫性に加えて、異なるディレクトリ・ノードの同じデータに対して異なる変更が同時に行われるマルチマスター・ネットワークでは、変更の競合が発生する場合があります。この競合が発生した場合、Oracle Internet Directory レプリケーションでは、競合解消というリコンシリエーションのプロセスを使用して各種ノード間を収束できます。

これらの問題を回避するために、レプリケートされたディレクトリ・ネットワークを使用するようにアプリケーションをデプロイする際には、適切なベスト・プラクティスに従うことが重要です。次に、ディレクトリ対応のアプリケーションをレプリケートされたディレクトリ環境にデプロイする際に管理者が考慮する必要のあるガイドラインを示します。

1. プライマリ・レプリカは、企業のディレクトリ・データの主要カテゴリごとに指定する必要があります。

   a. プライマリ・レプリカの典型的なカテゴリは、ユーザー・エントリと共通ユーザー属性、ユーザー・パスワードとその他の認証資格証明、ユーザー・グループと配布リスト、および主要アプリケーション・スイートに関連付けられているユーザー・プロファイル、プリファレンス、ロールです。

   b. プライマリ・レプリカの指定は、シングルマスター環境を意味しません。実際には多くのマスター・ノードがありますが、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には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の障害時には、他のアプリケーションと同様に、プロビジョニング・アプリケーションは別のマスターに一時的にフェイルオーバーできます。

   c. このデプロイ・プラクティスは、マルチマスター・ネットワークの柔軟性と、シングル・マスター構成のより緊密なデータ一貫性を組み合せます。

      – ある特定のデータのカテゴリのデータ・リカバリは、複数のマスター間のリコンシリエーションが関係しないため管理しやすくなります。

      – パスワードに対する認証サービスなど、特定の属性に対する変更に敏感なサービスは、最新の値を関連プライマリ・レプリカに依存できます。

2. アプリケーションの中間層およびバックエンド・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デプロイする必要があります。

   a. 均一ロード・バランシングおよび負荷分散は許容されず、アプリケーション中間層およびバックエンド・コンポーネントにはお薦めしません。たとえば、OracleAS Single Sign-On サーバーの連続的なログオン操作が異なる Oracle Internet Directory サーバーにルーティングされた場合は、ログオン再試行制限などの認証ポリシーを効果的に施行できません。

   b. 均一負荷分散は、アドレス帳検索など、クリティカルでない操作に対してのみ許容されます。

3. 関連アプリケーションの中間層およびバックエンド・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デプロイする必要があります。アプリケーションの様々なグループが様々なディレクトリ・インスタンスを共有できます。

   このプラクティスにより、関連アプリケーションは、依存している異なるディレクトリ・サーバー間の一時的な非一貫性の影響を受けないことが保証されます。たとえば、パスワードのリセットに使用された OracleAS Single Sign-On およびヘルプデスク・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。そうしないと、OracleAS Single Sign-On サーバーはパスワード変更が行われたのとは異なる Oracle Internet Directory サーバーに接続されているため、ユーザーがパスワードをリセットした後、サインオンできなくなる場合があります。

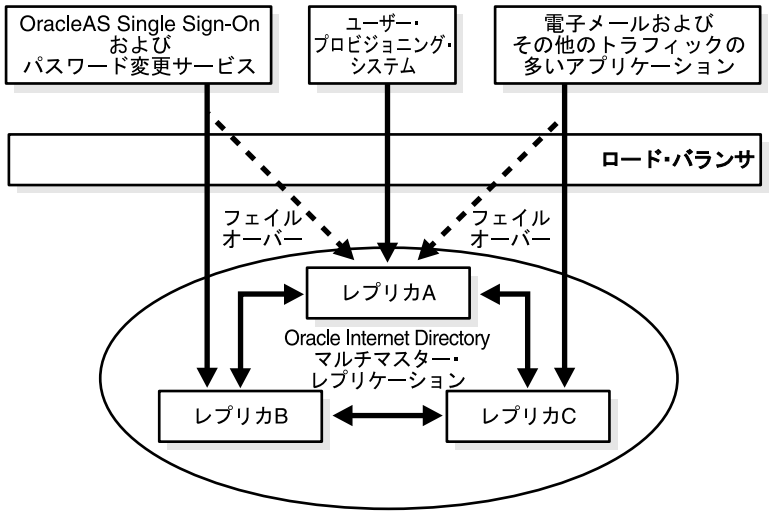
4. ディレクトリ内のデータのバルク・プロビジョニングは、ディレクトリ・ネットワークとディレクトリ・ネットワーク内のすべてのノードが正常な状態にある場合にのみ実行する必要があります。

   a. ディレクトリ・ネットワークのいずれかの部分が停止している場合、またはレプリケートまたは調整されるのを待機している変更のバックログが過剰にある場合は、バルク・プロビジョニングを継続すると、さらに問題が悪化し、データとサービスの消失がさらに広がる可能性があります。

   b. レプリケーション環境の状態監視および診断を定期的に実行する必要があります。Oracle Internet Directory には、このような操作をサポートするツールが含まれています。

前述のガイドラインを考慮して、図 3-20 に、レプリケートされたディレクトリ環境で構成されているエンタープライズ・アプリケーションの例を示します。このデプロイでは、OracleAS Single Sign-On、および Oracle Delegated Administration Services などのその他のパスワード変更サービスは、レプリカ B をプライマリ Oracle Internet Directory サーバーとして使用し、レプリカ A を一時フェイルオーバー・サーバーとして使用するように構成されています。同様に、電子メール・アプリケーションおよびその他の高トラフィック・アプリケーションは、レプリカ C をプライマリ・サーバーとして使用し、レプリカ A を一時フェイルオーバー・サーバーとして使用するように構成されています。

図 3-20 レプリケートされた環境で構成されているエンタープライズ・アプリケーション



地理的に分散した ID 管理インフラストラクチャのデプロイ

地理的に分散した運用ブランチのある企業では、地理的に異なる場所に分散した複数の OracleAS Single Sign-On インスタンスを設定して、ユーザーをローカルに認証する必要があります。このデプロイでは、図 3-21 に示すように、認証のためのネットワークの往復が削減され、アプリケーションへのアクセスが高速になります。OracleAS Single Sign-On サーバー・データはすべての地理的なブランチに対してグローバルにレプリケートされるため、リモートのビジネス・ロケーションに出張する従業員をローカルに認証できます。

地理的に離れた複数の場所にデプロイされたアプリケーションがある企業では、Oracle Internet Directory レプリカを少なくとも 2 つの地域に物理的に分散することが重要です。このような構成により、（ネットワーク障害や自然災害などによる）地域的な可用性の問題から、依存アプリケーションのグローバルなサービス停止が生じることを防止できます。

Oracle Internet Directory およびメタデータ・リポジトリがレプリケーションで設定されている場合でも、OracleAS Single Sign-On サイトはローカル・サイトにある独自の Oracle Internet Directory およびメタデータ・リポジトリを使用します。

レプリケートされた OracleAS Single Sign-On サイトが Wide Area Network（WAN）上に分散している場合、ローカル DNS サーバーは、地理的に最も近いサイトにユーザー・リクエストをルーティングするように構成する必要があります。

あるサイトでデータベース障害が検出された場合、Oracle Internet Directory および OracleAS Single Sign-On サーバーは別のサイトのメタデータ・リポジトリを指すように再構成されます。OracleAS Single Sign-On 中間層の障害が検出された場合、ネットワークはリモート中間層にトラフィックをルーティングするように再構成されます。

図 3-21 地理的に分散したデプロイ

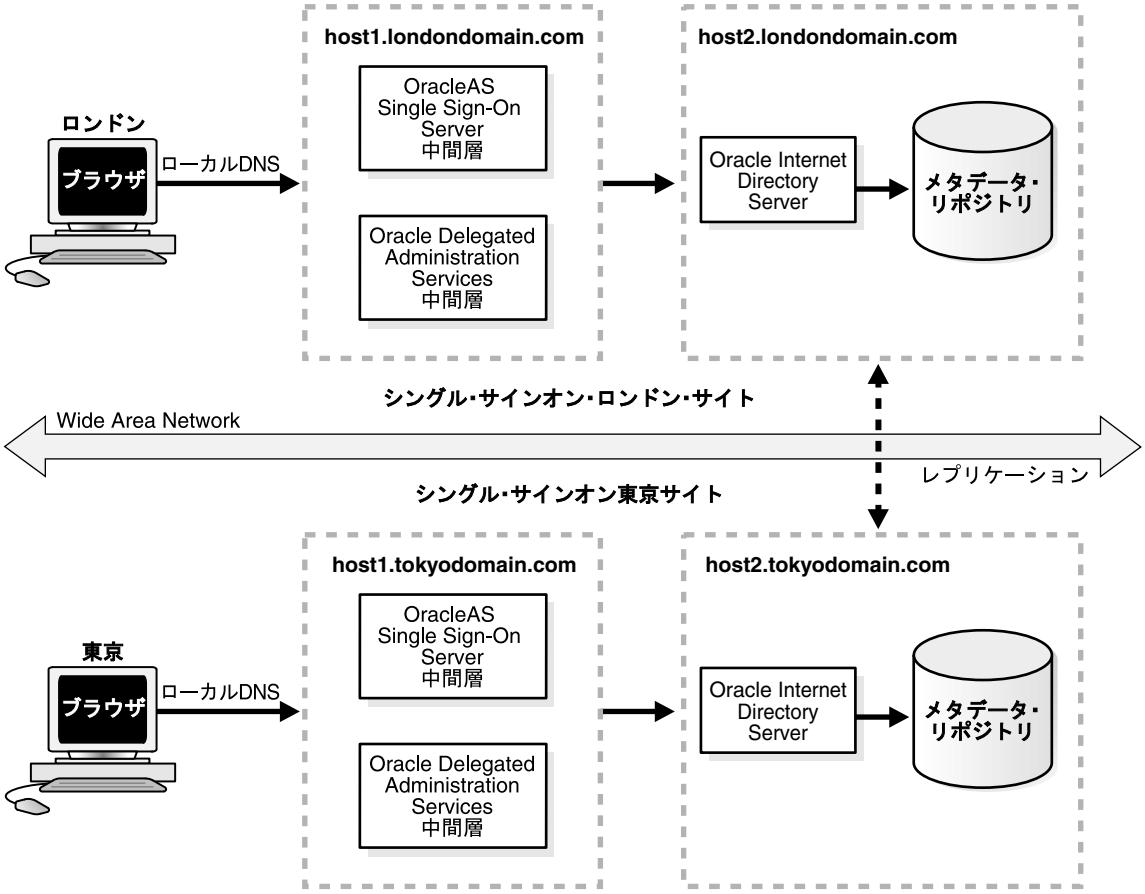
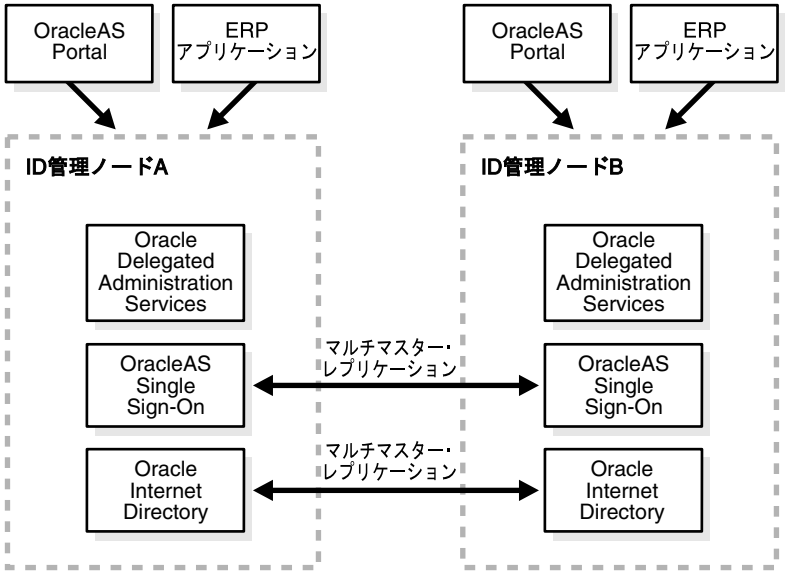


図 3-22 に、地理的に分散したデプロイの別の例を示します。ID 管理ノード A およびノード B は異なる場所にあります。ノード A の近くにある OracleAS Portal や ERP アプリケーションなどのアプリケーションは、ローカル ID 管理システムによって提供されているサービスを使用しています。同様に、ノード B の近くにあるアプリケーションは、ローカル ID 管理システムによって提供されているサービスを使用しています。ノードは Oracle Internet Directory データおよび Oracle Application Server Single Sign-On データをレプリケートします。

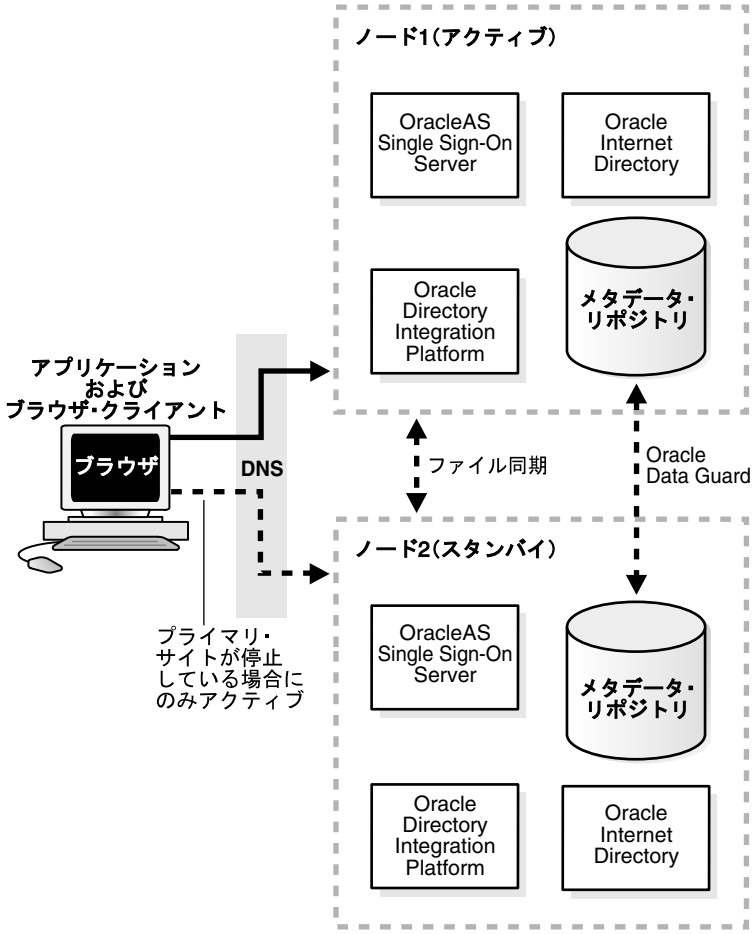
図 3-22 マルチマスター・レプリケーションでの分散デプロイ・サポート



ID 管理インフラストラクチャの障害時リカバリ・デプロイ

障害時リカバリは、破滅的なサイト障害からシステムをリカバリする方法を表します。破滅的な障害の例として、地震、竜巻、洪水、火災などがあります。単純な意味では、障害時リカバリは、ハードウェアまたはサブコンポーネントの置換に加えて、メタデータ・リポジトリと構成ファイルを含むサイト全体のレプリケートを含みます。最も厳しい要件は、災害時にもサービスの実行を継続することです。このデプロイは、ID 管理インフラストラクチャを、データの損傷や消失を引き起こすサイト障害またはメディア障害からも保護します。

図 3-23 Oracle Application Server Guard を使用した Oracle Internet Directory デプロイ



ID 管理インフラストラクチャの単一インスタンスなどの同一ソフトウェアを Oracle Application Server Guard のある複数のデータ・センターで実行して、データ・センター障害から保護できます。Oracle Application Server Guard には、単一インスタンス・ディレクトリ・データ・リカバリおよび透過的フェイルオーバーも用意されています。

図 3-23 に示したように、Oracle Application Server Guard は、プライマリ ID 管理インフラストラクチャと同期されている物理的なスタンバイ ID 管理インフラストラクチャをメンテナンスするように構成されています。Oracle Internet Directory およびその他の Oracle Internet Directory コンポーネントは、プライマリ ID 管理インフラストラクチャのメタデータ・リポジトリ・ノードで開始します。

障害時リカバリ中に、スタンバイがプライマリ・ノードになり、仮想ホスト名はスタンバイに移り、ID 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 の推奨デプロイ

本番デプロイでは、独自のリポジトリのある独立したシステムに Oracle Application Server Certificate Authority をデプロイすることをお薦めします。ID 管理インフラストラクチャのその他のコンポーネントでは、この章で説明したいずれかの構成を使用できます。

Oracle Application Server Certificate Authority システムは、次のガイドラインに加えて、すべての既知のメカニズムで保護する必要があります。

- Oracle Application Server Certificate Authority システムへの物理アクセスは厳密に制御する必要があります。
- オペレーティング・システムを強固にし、システム上のユーザー・アカウントを制限する必要があります。
- Oracle Application Server Certificate Authority のメタデータ・リポジトリは、データベース保護ガイドラインに従って保護する必要があります。
- Oracle Application Server を保護する必要があります。
- メタデータ・リポジトリ・データベース監査をオンにします。

その他のガイドラインに従って、物理的なセキュリティやネットワーク・セキュリティなどのシステムのセキュリティを向上させてください。

関連資料 :

- 『Oracle Application Server Certificate Authority 管理者ガイド』の「OracleAS Certificate Authority 配置ガイドライン」
- プラットフォームの Oracle Application Server のインストレーション・ガイド

4

ID 管理インフラストラクチャの管理および使用方法

この章では、ID 管理インフラストラクチャの管理および使用方法について、Oracle Delegated Administration Services でのユーザーの管理やインフラストラクチャ自体の管理に関する考慮事項などを含め説明します。

ID 管理インフラストラクチャでの Oracle アプリケーションおよびサード・パーティ・アプリケーションのデプロイのサポートに関する考慮事項についても説明します。

この章の内容は次のとおりです。

ID 管理インフラストラクチャの管理

正常なデプロイの後、ID 管理インフラストラクチャの管理には、定期的な監視、ID 管理インフラストラクチャの個別のコンポーネントの管理、および ID 管理インフラストラクチャ内の企業データの管理など、多くの管理タスクがあります。

この項の内容は次のとおりです。

ID 管理インフラストラクチャの定期的な監視

表 4-1 では、ID 管理インフラストラクチャの定期的な監視の実行に必要な様々なタスク、ツールおよび参照先を示します。

表 4-1 定期的な監視タスク

タスク	ツール	参照先
Oracle Internet Directory Server のステータスおよびパフォーマンスの監視	■ Identity Management Grid Control Plug-in ■ Application Server Control ■ LDAP コマンドライン・ツール	■ 第 5 章「Identity Management Grid Control Plug-in」 ■ 『Oracle Internet Directory 管理者ガイド』
Oracle Directory Integration Platform のステータスの監視	■ Identity Management Grid Control Plug-in ■ Application Server Control	■ 第 5 章「Identity Management Grid Control Plug-in」 ■ 『Oracle Identity Management 統合ガイド』
Oracle Delegated Administration Services のステータスの監視	■ Identity Management Grid Control Plug-in ■ Application Server Control	■ 第 5 章「Identity Management Grid Control Plug-in」 ■ 『Oracle Identity Management 委任管理ガイド』
OracleAS Single Sign-On のステータスの監視	■ Identity Management Grid Control Plug-in ■ Application Server Control	■ 第 5 章「Identity Management Grid Control Plug-in」 ■ 『Oracle Application Server Single Sign-On 管理者ガイド』

個別の ID 管理インフラストラクチャ・コンポーネントの管理

表 4-2 では、ID 管理インフラストラクチャの個別のコンポーネントの管理に必要な様々なタスク、ツールおよび参照先を示します。

表 4-2 ID 管理インフラストラクチャ・コンポーネントの管理

タスク	ツール	参照先
ディレクトリ・サービスの開始および停止	■ Identity Management Grid Control Plug-in ■ Application Server Control ■ `oidctl` コマンドライン・ツール	■ 第 5 章「Identity Management Grid Control Plug-in」 ■ 『Oracle Internet Directory 管理者ガイド』の「Oracle Internet Directory コンポーネントのプロセス制御」
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 Platform サービスの開始および停止	■ `oidctl` コマンドライン・ツール	『Oracle Identity Management 統合ガイド』
Oracle Directory Integration Platform の構成	■ Oracle Directory Manager ■ Oracle Directory Integration Platform アシスタント	『Oracle Identity Management 統合ガイド』
Oracle Delegated Administration Services の開始および停止	■ Identity Management Grid Control Plug-in ■ Application Server Control ■ `opmctl` コマンドライン・ツール	■ 第 5 章「Identity Management Grid Control Plug-in」 ■ 『Oracle Identity Management 委任管理ガイド』 ■ 『Oracle Application Server 管理者ガイド』
Oracle Delegated Administration Services の構成	Oracle Delegated Administration Services の「構成」タブ	『Oracle Identity Management 委任管理ガイド』
OracleAS Single Sign-On の開始および停止	■ 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 管理者ガイド』
パートナ・アプリケーションの OracleAS Single Sign-On への登録	`ossoreg.jar` 登録ツール	『Oracle Application Server Single Sign-On 管理者ガイド』

ID 管理インフラストラクチャの企業データの管理

個別のコンポーネントの監視および管理に加え、表 4-3 では、ID 管理インフラストラクチャ内でデータ（ユーザー、グループ、アプリケーションおよびポリシー）の管理に企業が利用できるタスク、ツールおよび参照先を示します。

表 4-3 企業データの管理

タスク	ツール	参照先
ユーザー管理（ユーザーの追加、削除および変更）	■ 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、削除および変更）	■ 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・デプロイのセキュリティ管理	■ 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 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 のパートナおよび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』

ID 管理インフラストラクチャの管理の委任

ID 管理インフラストラクチャでサポートされている委任モデルは、企業のセキュリティ要件に対応するようカスタマイズできます。デプロイでは、ID 管理インフラストラクチャを使用して、企業 ID の管理、企業のグループおよびロールの管理、および企業の ID とグループに応じたアプリケーションの管理が行われます。

この項の内容は次のとおりです。

ユーザー管理の委任

図 4-1 で示すとおり、ユーザー管理権限の委任の最終ターゲットは、ID 管理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・ユーザーです。権限はユーザーやアプリケーションなどの ID、またはロールやグループに委任できます。

通常のデプロイでは、Oracle Internet Directory スーパーユーザーは、ID 管理レルムを作成し、そのレルム内の特定のユーザーを ID 管理レルム管理者に指定します。スーパーユーザーはすべての権限を新しい ID 管理レルム管理者に委任し、次にその管理者は Oracle コンポーネントで必要な特定の権限を Oracle Application Server 管理者などの Oracle で定義されたロールに委任します。Oracle コンポーネントには、デプロイ時にロールが付与されます。

必要な権限を Oracle で定義されたロールに委任する以外に、レルム管理者は、ヘルプ・デスク管理者などのデプロイに固有のロールを定義し、特定の権限を委任することができます。それにより、それぞれの管理者はそのロールをユーザーに付与します。

電話番号、言語プリファレンス、Oracle Internet Directory に格納されているアプリケーション固有のプリファレンスの変更などのほとんどのユーザー管理タスクは、セルフサービス指向なので、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がユーザーに委任できます。

グループ管理の委任

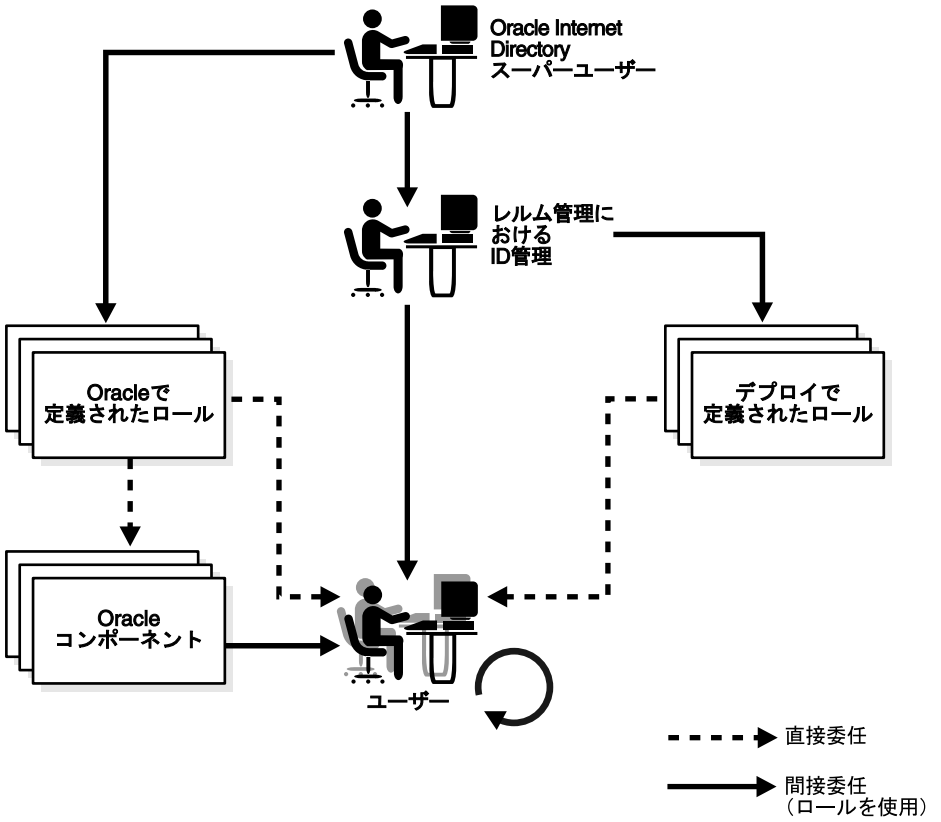
ユーザー管理の委任と同様に、グループ管理権限の委任の最終ターゲットは、図 4-1 に示すとおり、ID 管理インフラストラクチャを使用する Oracle コンポーネントまたはユーザーです。

Oracle Internet Directory スーパーユーザーは、レルム内のすべてのグループ関連権限を ID 管理レルム管理者に委任し、次にその管理者は Oracle コンポーネントで必要な特定のグループ管理権限を Oracle で定義されたロールに委任します。Oracle コンポーネントには、デプロイ時にロールが付与されます。

必要な権限を Oracle で定義されたロールに委任する以外に、レルム管理者は、ヘルプ・デスク管理者などのデプロイに固有のロールを定義し、特定の権限を委任することができます。それにより、それぞれの管理者はそのロールをユーザーに付与します。

グループを作成すると、グループの所有者を 1 人以上指定することができ、その後のグループの管理を所有者（通常はユーザー）に委任することができます。これらの所有者は、セルフサービス・コンソールを使用し、付与される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



コンポーネントのデプロイと管理の委任

Oracle コンポーネントのデプロイと管理に必要な一連の権限は、デプロイ時権限と実行時権限の 2 つのカテゴリに分けられます。

デプロイ時権限は、ディレクトリ内に適切なエントリを作成するのに必要で、共通のリポジトリにメタ情報を格納するための権限です。集中化されたリポジトリを持つことで、コンポーネントを複数のノードから余分な管理手順なしに実行できます。

実行時権限は、ID 管理インフラストラクチャ内で Oracle コンポーネントの実行時の相互作用を容易にするために必要な権限です。これには、ユーザー属性の表示、新規ユーザーの追加およびグループ・メンバーシップの変更を行う権限が含まれます。すべての Oracle コンポーネントにおいて、コンポーネント固有の管理ツールでは、Oracle Internet Directory にアクセス（つまり、適切なエントリを作成）するための特定の権限のセットが必要です。

図 4-2 では、ID 管理インフラストラクチャでのデプロイ時権限および実行時権限の委任を示します。

図 4-2 デプロイ時権限および実行時権限の委任

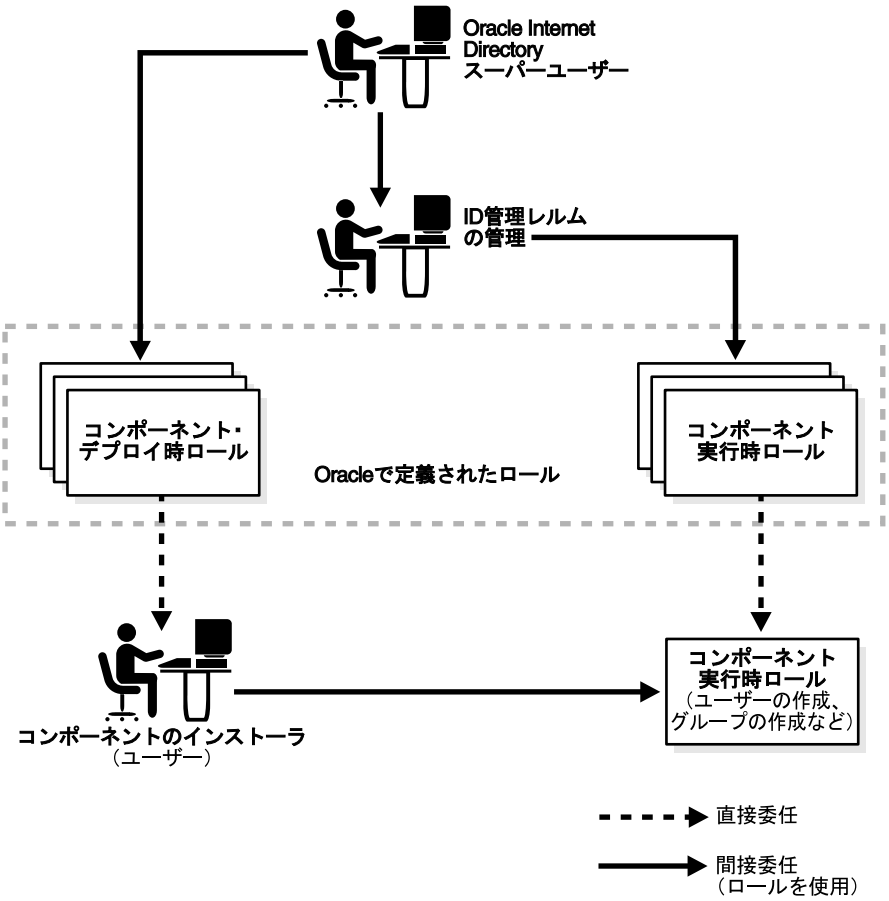


図 4-2 では、スーパーユーザーが特定のデプロイ権限をグループに付与し、その権限をデプロイ・プロセス中に特定の Oracle コンポーネントをインストールする特定のユーザーに、彼らをグループのメンバーにすることで付与しています。次に、インストール・プロセスの一環としてコンポーネント・インストーラは固有の実行時権限をコンポーネントに付与します。

注意： ほとんどの Oracle コンポーネントは一連の権限が事前構成された状態で出荷されますが、固有のビジネス要件を満たすよう権限を変更することができます。

Oracle Internet Directory Delegated Administration Services

Oracle Delegated Administration Services を使用すると、企業はビジネス要件に応じて管理の職責を割り当てることができます。特定の管理者、または複数のセットの管理者がリソースへのアクセスを個別に管理でき、異なるセキュリティ情報を作成する必要がないよう、企業の異なるコンポーネントに異なるレベルのセキュリティ・ポリシーを提供します。

Oracle Internet Directory ベースの複数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、ビジネス単位および地域において数百万のユーザーをサポートします。集中化されたリポジトリと組み合せることで、ID 管理インフラストラクチャでは分散管理が可能になり、総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一貫性のあるセキュリティで行い、アプリケーション全体にセマンティックを使用できるようにすることです。たとえば、複数のアプリケーションでグループの管理が必要な場合、グループ管理の実装に必要な様々なステップやディレクトリ・アクセス制御リスト（ACL）セマンティックを理解することを要求されない必要があります。

ID 管理インフラストラクチャ・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）に分けることができ、このユニットはアプリケーション・コンソールで組み合せることができます。たとえば、アプリケーション・コンソールをユーザー属性のヘンコウニシヨウする必要がある場合、適切な DAS サービス・ユニットのリンクをそのコンソールまたはポータル・ページで統合します。ユーザー・インタフェースを作成する必要はありません。

様々な DAS サービス・ユニットをセルフサービス・アプリケーションの作成に使用することもできます。このアプリケーションは、言語プリファレンスや自宅の住所などの属性の更新に使用できます。したがって、DAS サービス・ユニット・ベースの統合方法は、一貫性のあるセキュリティ・セマンティック、一貫性のある使用モデル、およびコンポーネントの再利用を提供します。

5

Identity Management Grid Control Plug-in

Identity Management Grid Control Plug-in は Oracle Application Server 10*g*（10.1.4.0.1）の新機能です。Identity Management Grid Control Plug-in では、Oracle Enterprise Manager 10*g* Grid Control コンソールの機能を使用して、Oracle Internet Directory、Oracle Application Server Single Sign-On、Oracle Delegated Administration Services および Oracle Directory Integration Platform を監視および管理できます。

関連資料：

- Oracle Application Server のインストレーション・ガイド
- 『Oracle Enterprise Manager 概要』
- 『Oracle Enterprise Manager Grid Control インストレーションおよび基本構成』
- 『Oracle Enterprise Manager アドバンスト構成』

この章の内容は次のとおりです。

Oracle Internet Directory の統計収集の有効化

Identity Management Grid Control Plug-in のインストール後、Oracle Internet Directory の統計収集を有効化する必要があります。これには、`orclStatsFlag` および `orclStatsPeriodicity` を『Oracle Internet Directory 管理者ガイド』で説明されているように設定する必要があります。

注意： Grid Control で統計を収集している場合、`orclStatsPeriodicity` を Enterprise Manager エージェントの収集周期と同じにする必要があります。これはデフォルトで 10 分です。

ユーザー・インタフェースの概要

Identity Management Grid Control Plug-in には、ID 管理インフラストラクチャを監視および管理するページがあります。Identity Management Grid Control Plug-in のページは、次の 5 つのセットにグループ化されています。

- ID 管理スイート
- Oracle Internet Directory
- Oracle Delegated Administration Services
- Oracle Directory Integration Platform
- Oracle Application Server Single Sign-On

「ID 管理スイート」ページでは、スイートに関する情報の管理および表示、コンポーネントに関する高水準の情報を表示できます。他の 4 つのセットはコンポーネント固有のものです。

Identity Management Grid Control Plug-in のページの 4 つのコンポーネント固有のセットそれぞれには次の 2 種類のページがあります。

- コンポーネント・レベル・ページ : コンポーネント全体を監視および管理できます。複数のホストで実行されている複数のサーバーを含めることも可能です。
- サーバー・レベル・ページ : サーバー・レベル・ページは個別のサーバーへのアクセスを提供します。

表 5-1 には、Identity Management Grid Control Plug-in のページを示します。

表 5-1 Identity Management Grid Control Plug-in のページ

名前	タイプ	スイート / コンポーネント
ID 管理スイートの「ホーム」	スイート・レベル	ID 管理スイート
ID 管理スイートの「アラート・サマリー」	スイート・レベル	ID 管理スイート
ID 管理スイートの「デプロイ」	スイート・レベル	ID 管理スイート
ID 管理スイートの「インフラストラクチャ」	スイート・レベル	ID 管理スイート
ID 管理スイートの「パフォーマンス」	スイート・レベル	ID 管理スイート
ID 管理スイートの「トポロジ」	スイート・レベル	ID 管理スイート
Internet Directory コンポーネントの「ホーム」	コンポーネント・レベル	Oracle Internet Directory
Internet Directory コンポーネントの「アラート・サマリー」	コンポーネント・レベル	Oracle Internet Directory
Internet Directory コンポーネントの「パフォーマンス」	コンポーネント・レベル	Oracle Internet Directory

表 5-1 Identity Management Grid Control Plug-in のページ（続き）

名前	タイプ	スイート / コンポーネント
Internet Directory コンポーネントの「トポロジ」	コンポーネント・レベル	Oracle Internet Directory
ディレクトリ・サーバーの「ホーム」	サーバー・レベル	Oracle Internet Directory
ディレクトリ・サーバーの「構成設定」	サーバー・レベル	Oracle Internet Directory
ディレクトリ・サーバーの「パフォーマンス」	サーバー・レベル	Oracle Internet Directory
LDAP レプリケーション・サーバーの構成設定	サーバー・レベル	Oracle Internet Directory
ディレクトリ・サーバーの「レプリケーション・メトリック」	サーバー・レベル	Oracle Internet Directory
ディレクトリ・サーバーの「ユーザー統計」	サーバー・レベル	Oracle Internet Directory
Delegated Administration Services コンポーネントの「ホーム」	コンポーネント・レベル	Oracle Delegated Administration Services
Delegated Administration Services の「アラート・サマリー」	コンポーネント・レベル	Oracle Delegated Administration Services
Delegated Administration Services コンポーネントの「パフォーマンス」	コンポーネント・レベル	Oracle Delegated Administration Services
Delegated Administration Services コンポーネントの「トポロジ」	コンポーネント・レベル	Oracle Delegated Administration Services
委任管理サーバーの「ホーム」	サーバー・レベル	Oracle Delegated Administration Services
委任管理サーバーの「管理」	サーバー・レベル	Oracle Delegated Administration Services
委任管理サーバーの「パフォーマンス」	サーバー・レベル	Oracle Delegated Administration Services
Directory Integration Platform の「ホーム」	コンポーネント・レベル	Oracle Directory Integration Platform
Directory Integration Platform の「アラート・サマリー」	コンポーネント・レベル	Oracle Directory Integration Platform
Directory Integration Platform の「パフォーマンス」	コンポーネント・レベル	Oracle Directory Integration Platform
Directory Integration Platform の「トポロジ」	コンポーネント・レベル	Oracle Directory Integration Platform
Directory Integration Platform サーバーの「ホーム」ページ	サーバー・レベル	Oracle Directory Integration Platform
Directory Integration Platform サーバーの「パフォーマンス」	サーバー・レベル	Oracle Directory Integration Platform
Single Sign-On コンポーネントの「ホーム」	コンポーネント・レベル	Oracle Application Server Single Sign-On
Single Sign-On コンポーネントの「アラート・サマリー」	コンポーネント・レベル	Oracle Application Server Single Sign-On
Single Sign-On コンポーネントの「パフォーマンス」	コンポーネント・レベル	Oracle Application Server Single Sign-On
Single Sign-On コンポーネントの「トポロジ」	コンポーネント・レベル	Oracle Application Server Single Sign-On

表 5-1 Identity Management Grid Control Plug-in のページ（続き）

名前	タイプ	スイート / コンポーネント
Single Sign-On Server の「ホーム」	サーバー・レベル	Oracle Application Server Single Sign-On
Single Sign-On Server の「管理」	サーバー・レベル	Oracle Application Server Single Sign-On
Single Sign-On Server の「パフォーマンス」	サーバー・レベル	Oracle Application Server Single Sign-On
Single Sign-On Server の「ユーザー統計」	サーバー・レベル	Oracle Application Server Single Sign-On

Identity Management Grid Control Plug-in 内の移動

Grid Control から ID 管理スイートのホームページに移動するには、**「ターゲット」**タブをクリックし、次に **ID 管理**サブタブをクリックします。

ID 管理スイートのホームページから、**「ホーム」**と同じレベルのヘッダーをクリックすると、**ID 管理スイート**の**「インフラストラクチャ」**、**「パフォーマンス」**、**「デプロイ」**および**「トポロジ」**ページに移動できます。

ID 管理スイートの**ホーム**ページからコンポーネントのホームページには、ページの**「コンポーネント」**セクションのコンポーネント名をクリックすると移動できます。アラートが表示された場合、**「スイート・アラートの概要」**セクションの番号をクリックすると、ID 管理スイートの「アラート・サマリー」ページに移動できます。

各コンポーネントのホームページからそのコンポーネントの他のページには、**「ホーム」**と同じレベルのヘッダーをクリックすると移動できます。アラートが表示された場合、**「スイート・アラートの概要」**セクションの番号をクリックすると、そのコンポーネントの**「アラート・サマリー」**ページに移動できます。

各コンポーネントのホームページからそのコンポーネントのサーバー・ページには、ページの**「サーバー」**セクションのサーバー名をクリックすると移動できます。

各サーバーのホームページからそのサーバーの他のページには、**「ホーム」**と同じレベルのヘッダーをクリックすると移動できます。ディレクトリ・サーバーのホームページからディレクトリ・サーバーの「構成設定」ページには、**「LDAP サーバー・インスタンス」**セクションの**「構成設定」**をクリックすると移動できます。「LDAP レプリケーション・サーバーの構成設定」ページには、**「レプリケーション・サーバー・インスタンス」**セクションの**「構成設定」**をクリックすると移動できます。

注意： **Internet Directory コンポーネント**の各ページの**「Internet Directory サーバー」**セクションには、ディレクトリ・サーバーと関連するデータベースの名前がリストされます。名前をクリックすると、データベースのホームページにドリルダウンできます。データベースが「未登録」としてリストされている場合は、Oracle Internet Directory Server を再起動することで使用できるようにすることができます。あるいは、Oracle Internet Directory の別のインスタンスを一時的に起動してから停止することもできます。

注意： 一部の高可用性構成では、Identity Management Grid Control Plug-in に 1 つのメタデータ・リポジトリを共有するすべてのホストについて、同じ情報が表示されます。この動作については今後のリリースで変更する予定です。

Oracle Internet Directory Server の起動、停止および再起動

Oracle Internet Directory Server ターゲットを Internet Directory コンポーネントのホームページ、**「パフォーマンス」**または**「トポロジ」**ページから起動、停止または再起動できます。これを行うには、次の手順を実行します。

1. ページの**「Internet Directory サーバー」**セクションで、**「選択」**列の対応するボックスを選択することでターゲットを選択します。
2. 実行する操作に応じて、**「起動」**、**「停止」**または**「再起動」**をクリックします。
3. **「停止」**または**「再起動」**を実行すると、**「確認」**ページが表示されます。**「はい」**をクリックします。
4. 優先資格証明を設定していない場合は、**「資格証明」**ページが表示されます。Oracle Application Server 管理者の名前とパスワードを入力し、**「続行」**をクリックします。

   操作が進行中の間、**「処理中」**ページが表示されます。最後に**「結果」**ページが表示されます。操作が失敗した場合、**「結果」**ページに理由が表示されます。

委任管理サーバーの起動、停止および再起動

委任管理サーバーを Delegated Administration Services コンポーネントの**ホーム**ページ、**「パフォーマンス」**または**「トポロジ」**ページから起動、停止または再起動できます。これを行うには、次の手順を実行します。

1. ページの**「委任管理サーバー」**セクションで、**「選択」**列の対応するボックスを選択することでターゲットを選択します。
2. 実行する操作に応じて、**「起動」**、**「停止」**または**「再起動」**をクリックします。
3. **「停止」**または**「再起動」**を実行すると、**「確認」**ページが表示されます。**「はい」**をクリックします。
4. 優先資格証明を設定していない場合は、**「資格証明」**ページが表示されます。オペレーティング・システムのユーザーの名前とパスワードを入力し、**「続行」**をクリックします。

   操作が進行中の間、**「処理中」**ページが表示されます。最後に**「結果」**ページが表示されます。操作が失敗した場合、**「結果」**ページに理由が表示されます。

Oracle Identity Management の監視

Identity Management Grid Control Plug-in では、ID 管理スイートの様々な内容について監視できます。

この項の内容は次のとおりです。

- ステータス
- メトリックおよびアラート
- トポロジ
- 事前構成済レポート

ステータス

Identity Management Grid Control Plug-in の多くのページで、コンポーネント、サーバー、またはサーバー内のインスタンスの情報が提供されます。スイート・レベル・ページにはすべてのコンポーネントのステータスがリストされ、コンポーネント・レベル・ページには単一コンポーネントのステータスがリストされます。コンポーネントのステータスは、そのコンポーネントの任意のサーバーが稼働していれば、稼働としてリストされます。サーバー・レベル・ページにはサーバーのステータスがリストされます。サーバーのステータスは、そのサーバーで実行されている任意のインスタンスが稼働していれば、稼働としてリストされます。その他のページには、Identity Management と関連する様々なターゲットのステータスがリストされます。フィールドまたはアイコンをクリックして詳細情報を表示できる場合もあります。

メトリックおよびアラート

Identity Management Grid Control Plug-in の一部のページでは、メトリックが表示され、アラートの情報が示されます。メトリックはシステムの状態の評価に使用される測定の単位です。各コンポーネントには事前定義された一連のメトリックがあります。これらのメトリックの一部には、関連するしきい値があります。しきい値は、監視されているメトリックの値と比較する境界値です。しきい値に達すると、アラートが生成されます。メトリックおよびアラートの詳細は、『Oracle Enterprise Manager 概要』を参照してください。

トポロジ

「トポロジ」ページでは、Enterprise Manager Grid Control のトポロジ・ビューアを使用して ID 管理スイート内のコンポーネント、コンポーネント・サーバー・ターゲット、関連データベースおよびホストがグラフィカルに表示されます。トポロジ・ビューアでは、すべての依存コンポーネントおよびサブサービスがアイコンとして表示され、それらの関係がリンクとして表示されます。Enterprise Manager Grid Control のトポロジ・ビューアを表示するには、Internet Explorer を使用する必要があります。

事前構成済レポート

Identity Management Grid Control Plug-in には、Oracle Internet Directory および Oracle Application Server Single Sign-On 用の事前構成済レポートがいくつか含まれています。アクセスするには、Oracle Internet Directory または Oracle Application Server Single Sign-On のコンポーネント・ページまたはサーバー・ページから**「関連リンク」**の下の**「レポート」**リンクをクリックします。

前のリリースとの互換性

10*g*（10.1.4.0.1）より前のバージョンの Oracle Internet Directory では、Identity Management Grid Control Plug-in のすべての機能はサポートされていません。Identity Management Grid Control Plug-in は、10*g* リリース 2（10.1.2）以下のリリースの Oracle Internet Directory で使用できますが、次のような特定のリンクは適切には解決していません。

- データベース
- レプリケーション・メトリック
- サプライヤ表

6

他の ID 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 ID 管理ソリューションとの統合について説明します。

この章の内容は次のとおりです。

ID 管理統合の理由

ID 管理インフラストラクチャはほとんどの Oracle デプロイで必須のコンポーネントなので、他の ID 管理ソリューションと統合することもできるよう設計されています。共通インフラストラクチャの周りにある Oracle 製品を統合すると、次のようなエンタープライズ ID 管理ソリューションとの統合の核になります。

- 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 PKI ソリューション

ID 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 環境で使用できます。これは次のような利点があります。

- 統合ユーザー・プロビジョニング : ユーザー・プロビジョニングとは、新しいユーザーを様々なエンタープライズ・システムに対して追加および削除するプロセスです。新しいユーザー・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）システムおよびネットワーク管理環境などの様々なソースによって行うことが可能です。新しいユーザーを 1 つのシステムで作成すると、自動化されたユーザー・プロビジョニングにより必要なユーザー・アカウントのフットプリントが他のエンタープライズ・アプリケーションに作成されます。アカウントのフットプリントは、ユーザー・アカウントで必要なアプリケーション・リソースのセットです。
- **ユーザーの集中管理 :** ユーザー・アカウントを一度作成すると、保持および管理する必要があります。ユーザーの集中管理により、パスワード、ロール、アプリケーション・プリファレンスなどのユーザーに関係する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・サービス統合 :** 組織はエンタープライズ環境のアプリケーションで認証およびデータの機密保持に共通のセキュリティ・サービス・セットを使用できることを必要としています。

これらの利点を得るには、ID 管理インフラストラクチャとサード・パーティのディレクトリ、セキュリティおよびユーザー管理環境とを統合するツールと計画が必要です。

> **関連資料 :** 統合ソリューションのデプロイの詳細は、『Oracle Identity Management 統合ガイド』および『Oracle Application Server Single Sign-On 管理者ガイド』を参照してください。

ID 管理統合のツールと計画

ID 管理インフラストラクチャでは、他の ID 管理環境と統合するための多くのツール（様々なサービスおよび API、事前構成済ディレクトリ接続ソリューション、および標準サポート）が提供されます。これらツールについてこの項で概略を説明します。これらの使用方法の詳細は、適切な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 Platform

Oracle Directory Integration Platform は、Oracle Internet Directory と他のリポジトリ（サード・パーティ・ディレクトリ（SunONE Directory や Microsoft Active Directory など）、アプリケーション・ユーザー・リポジトリ（たとえば、フラット・ファイルに格納されている）または HR 情報を含むデータベース表など）の間の同期およびプロビジョニング・ソリューションの開発を容易にする、Oracle Internet Directory に組み込まれているサービスとインタフェースのセットで構成されています。

Oracle Directory Integration Platform には文書化された API が含まれ、存在する場合使用可能な業界標準を組み込みます。これにより、Oracle、ユーザーおよびサード・パーティはカスタマイズされた同期およびプロビジョニング・ソリューションを開発およびデプロイできるようになります。また、Oracle Internet Directory とサード・パーティ・メタディレクトリの相互運用性、およびプロビジョニング・ソリューションが促進されます。

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

Oracle Internet Directory では、ディレクトリ操作前、操作中または捜査後に実行可能なカスタム・ルーチン（Oracle、ユーザー作成またはサード・パーティ）を含められるようにする 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ています。たとえば、フレームワークは次のことに使用できます。

- ディレクトリ・サーバーがデータに対する操作を実行する前にそのデータを検証
- サーバーが操作を実行した後に指定した操作を実行
- カスタム・パスワード・ポリシーを定義
- NOS ディレクトリなどの外部資格証明ストアを介してユーザーを認証

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

事前構成済ディレクトリ接続ソリューション

Oracle Internet Directory には Oracle Directory Integration Platform に作成されている事前構成済接続ソリューション、および Oracle Internet Directory プラグイン・アーキテクチャが含まれており、ID 管理インフラストラクチャのユーザーを他のシステムから自動的にプロビジョニングすることや、ID 管理インフラストラクチャのユーザーをそれらの環境から管理することができます。事前構成済接続ソリューションには、次のものがあります。

- Oracle E-Business Suite
- Oracle Database 表
- SunONE および iPlanet
- Microsoft Active Directory

関連資料： 事前構成済ディレクトリ接続ソリューションの詳細は、『Oracle Identity Management 統合ガイド』を参照してください。

OracleAS Single Sign-On Partner API

OracleAS Single Sign-On では、Oracle Application Server Single Sign-On による信頼できるサード・パーティ認証メカニズムからのユーザー ID の取得を可能にするサード・パーティ認証 API がサポートされています。この機能は、アプリケーション・ユーザーが 2 つの環境にまたがる Web アプリケーションに一度ログインするだけでアクセスできるようにする際に使用できます。

関連資料： 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（JAAS）Provider Developer API

Oracle Application Server Java Authentication and Authorization Service（JAAS）Provider により、認証および ID サービスのために Oracle J2EE 環境で実行されているユーザーが作成した Java アプリケーションで OracleAS Single Sign-On および Oracle Internet Directory を使用できます。

関連資料： 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 に基づき LDAPv3 標準をサポートしています。

> **関連資料：** 事前構成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 鍵配布センターによって発行される 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。これにより、有効な Kerberos チケットを発行されたユーザー（たとえば、Windows 環境内）はユーザー名とパスワードを指定しなくても Web アプリケーションにログインできます。

> **関連資料：** 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

ID 管理インフラストラクチャは、厳密認証サービスのために X.509v3 標準 PKI 証明書を発行し、使用します。既存の X.509v3 認証局を持つユーザーは、Oracle 環境でこれらのその証明書を使用できます。

A

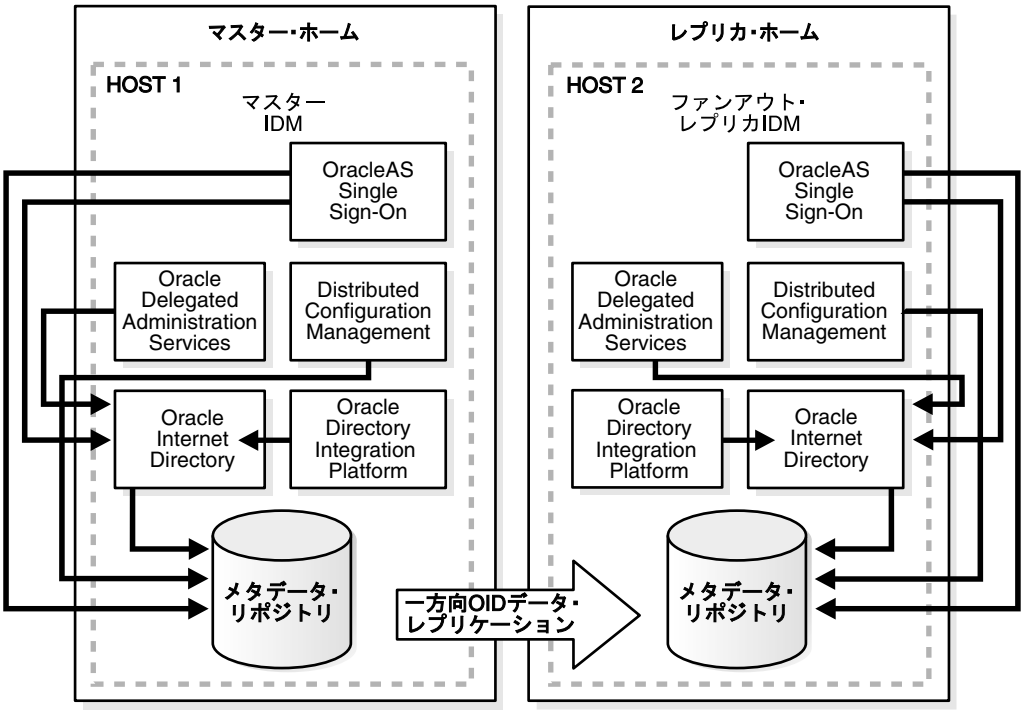
ファンアウト・レプリケーションによるID管理のデプロイ

この付録では、ファンアウト・レプリケーションでID管理インフラストラクチャ・コンポーネントをインストールするための高度な手順を説明します。詳細は、他の箇所で説明します。レプリケーションによるOracle Internet Directoryのインストールの詳細は、『Oracle Internet Directory管理者ガイド』およびOracle Application Serverのインストレーション・ガイドを参照してください。マルチマスター・レプリケーションによるOracle Identity Managementのデプロイの高度な説明は、『Oracle Application Server高可用性ガイド』を参照してください。

図A-1では、MASTER Identity Managementノードが HOST 1にデフォルトのIdentity Managementインストールを使用して、メタデータ・リポジトリ、Oracle Internet Directory、Oracle Directory Integration Platform、Oracle Application Server Single Sign-OnおよびOracle Delegated Administration Servicesとともにインストールされています。

同様に、REPLICA Identity Managementノードが HOST 2にデフォルトのIdentity Managementインストールを使用して、メタデータ・リポジトリ、Oracle Internet Directory、Oracle Directory Integration Platform、Oracle Application Server Single Sign-OnおよびOracle Delegated Administration Servicesとともにインストールされています。

図 A-1 各ホストへの Oracle Internet Directory、Oracle Directory Integration Platform、Oracle Application Server Single Sign-On および Oracle Delegated Administration Services のファンアウト・デプロイ



マスター・ノードのインストール

マスター・ノードには、Oracle Application Server 10*g*（10.1.4.0.1）メタデータ・リポジトリ、Oracle Internet Directory、Oracle Application Server Single Sign-On、Oracle Delegated Administration Services および Oracle Directory Integration Platform を Host 1 に MASTER_HOME を Oracle ホームとして使用してインストールしています。

レプリカ・ノードのインストール

レプリカ・ノードには、Oracle Identity Management およびメタデータ・リポジトリ、Oracle Internet Directory、Oracle Application Server Single Sign-On、Oracle Delegated Administration Services および Oracle Directory Integration Platform を Host 2 に REPLICA_HOME を Oracle ホームとして使用してインストールしています。

注意： レプリカをインストールする場合、Oracle Application Server Single Sign-On、Oracle Delegated Administration Services、Oracle Directory Integration Platform の他に拡張構成画面で **HA** を選択してください。Oracle Universal Installer により、**レプリカ**・インストールを選択するかを尋ねられます。**レプリカ**を選択した場合、Oracle Universal Installer では **ASR レプリカ**または **LDAP レプリカ**を選択できます。**LDAP レプリカ**を選択して続行してください。

ファンアウト・レプリケーション設定

Oracle Universal Installer により、レプリケーションが自動構成されます。インストールが完了したら、すべてが希望どおり機能するかテストしてください。

B

Oracle Internet Directory のデフォルトの設定

この付録では、Oracle Internet Directory のインストール後に可能なデフォルトの設定について説明します。

Oracle Internet Directory のインストールにより、デフォルトの DIT が作成され、デプロイについてのいくつかの仮定を使用してデフォルトの ID 管理レルムが設定されます。

次に示すのは、Oracle Internet Directory のインストール中に実行される操作のサマリーです。

- デフォルトの DIT が、Oracle Internet Directory がインストールされるシステムのドメイン名に基づいて作成されます。たとえば、Oracle Internet Directory が `oidhost.us.acme.com` というマシンにインストールされる場合、デフォルトの DIT は `dc=us,dc=acme,dc=com` です。
- デフォルトの ID 管理レルムが作成されます。そのベースはシステムのドメイン名に対応します。前述の例に従うと、デフォルトの ID 管理レルムのルートは `dc=us,dc=acme,dc=com` です。

  このレルムに関連するエンティティは Oracle コンテキストと呼ばれ、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ます。たとえば、Oracle コンテキストは `cn=OracleContext,dc=us,dc=acme,dc=com` という識別名で作成されます。このエントリ、およびその下のノードは、Oracle ソフトウェアがレルム固有のポリシーおよび設定を検出する際のベースとして機能します。
- デフォルトの ID 管理レルムに作成されたディレクトリ構造とネーミング・ポリシーにより、Oracle コンポーネントは様々な ID を検索できます。次に、これらのポリシーのデフォルト値を示します。
  - すべてのユーザーが ID 管理レルムのベースの下の `cn=users` コンテナに存在します。この場合、識別名は `cn=users,dc=us,dc=acme,dc=com` です。
  - Fusion Middleware Identity Infrastructure を使用して ID 管理レルムに作成された任意の新規ユーザーが、`cn=users` コンテナの下にも作成されます。
  - Fusion Middleware Identity Infrastructure を使用して ID 管理レルムに作成されたすべての新規ユーザーが、オブジェクト・クラス `orclUserV2` および `inetOrgPerson` に属します。
  - すべてのグループが ID 管理レルムのベースの下の `cn=groups` コンテナに存在します。この場合、識別名は `cn=groups,dc=us,dc=acme,dc=com` です。
  - ブートストラップ・ユーザー（レルム管理者）が `cn=users` コンテナの下に作成されます。この場合、ブートストラップ・ユーザーの完全修飾識別名は `cn=orcladmin,cn=users,dc=us,dc=acme,dc=com` です。
  - デフォルトの認証ポリシーが作成され、認証サービスにより適切な操作を実行できます。これらのポリシーには、ユーザーのプロビジョニング時に自動生成される必要がある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、ロックアウトするまでの試行回数、パスワードが失効するまでの日数など）およびその他のパスワード検証機能が含まれます。

- ID 管理権限が作成され、Oracle Delegated Administration Services セルフサービス・コンソールを使用して認可を委任できるブートストラップ・ユーザーに付与されます。権限のいくつかを次に示します。
  - ユーザー作成、ユーザー・プロファイル変更およびグループ作成などの共通 ID 管理操作権限
  - ID 管理インフラストラクチャを使用して新規 Oracle アプリケーションをインストールする権限
  - Oracle Delegated Administration Services を管理する権限