

Oracle Access Manager

Oracle ホワイト・ペーパー
2006 年6 月

ご注意

本書は、オラクルの一般的な製品の方向性を示すことが目的です。情報を提供することだけが目的であり、契約とは一切関係がありません。商品、コード、または機能を提供するものではなく、購入の判断にご利用いただくためのものではありません。オラクル製品の機能に関する開発、発表、時期については、オラクルの判断に従うものとします。

はじめに

インターネットが情報配信の主要な手段となったため、企業や政府機関は、顧客やパートナーが製品サポート・データなどのリソースにアクセスできるように、IT インフラストラクチャを開放しなければならないという課題に直面しています。また、各種企業データへの社員によるアクセスを規制し、だれが何にアクセスしたかを追跡し、記録する必要もあります。先進的な組織は、規制に準拠し、運用コストを削減し、アプリケーションの安全性と可用性を改善するために、ID 管理ソリューションへの依存性を高めています。強力な ID 管理戦略には、ユーザー・ライフサイクルを管理し、ユーザー・プロフィール・データを安全に保存、管理し、これらのプロフィールに基づいてアプリケーション・アクセスを制御するための統合されたテクノロジーが必要です。

Oracle Access Manager は、業界唯一のポリシーベースのアクセス管理ソリューションです。異機種プラットフォームのサポートを提供するだけでなく、Oracle Fusion Applications および Oracle Fusion Middleware と統合されています。

Oracle Access Manager は、The Global 1000（世界の企業 1,000 社）の多くの大企業に配置され、世界最大級のアクセス数を誇る数多くのポータルを支えています。企業は、Oracle Access Manager を使用して、複数のベンダー製品やプラットフォームに配置されたポータル、エクストラネット、およびイントラネットに、セキュリティ、管理制御、ユーザーのセルフサービス、委任管理、および認知度の向上を実現しています。本書では、異機種アプリケーションにエンドツーエンドのセキュリティ・インフラストラクチャを提供する ID 管理、認証、認可、および監査などの Oracle Access Manager の主要コンポーネントと機能について説明します。

Oracle Access Manager の概要

Oracle Access Manager は、Web アクセス管理とユーザー ID 管理用のための Oracle Identity Management ソリューションです。Oracle Access Manager は、複雑な異種企業環境に対応するように設計されています。Oracle Fusion Middleware の主要コンポーネントとして、Oracle の現在と将来の ERP、CRM、および Collaboration Suite アプリケーションに迅速に対応することを保証します。

Oracle Access Manager は、強力なアクセス管理システムとクラス最高の ID 管理システムを組み合わせ、市場で唯一の製品です。

Oracle Access Manager は、アクセス・システムと ID システムから構成されています。アクセス・システムは、集中管理された認証、認可、および監査を提供してアプリケーションの安全性を確保し、企業リソース全体にわたるシングル・サインオンとアクセス制御を実現します。ID システムは、個人、グループ、および組織に関する情報を管理します。ユーザーの委任管理だけでなく、承認作業との自己登録インタフェースも実現します。これらのシステムはシームレスに統合され、同時に配置することも、個別に配置することも可能です。

Oracle Access Manager 用のバックエンド・リポジトリは、複数のディレクトリ・サーバーを組み合わせることができる LDAP に基づくディレクトリ・サービスです。このディレクトリ・サービスは、主に 2 つの目的で利用できます。

- アクセス・システムと ID システムが使用、管理するポリシー、構成、およびワークフローに関連するデータを保存する。
- ID システムが管理し、アクセス・ポリシーを評価するためにアクセス・システムが使用する、ユーザー、グループ、および組織データを含む ID を保存する。

アクセス管理

Oracle Access Manager のアクセス・システムは、集中管理された認証、認可、および監査を提供し、Web リソースや J2EE リソース（JSP、サーブレット、EJB など）および従来のシステムなどの企業リソース全体にわたるシングル・サインオンとセキュアなアクセスを実現します。アクセス・システムは、ポリシーを通じてあらゆる種類のリソースを保護できる拡張可能なソリューションです。従来のアプリケーションやカスタム・アプリケーションは、アクセス・システムの広範な API を利用することによって、認証、認可、および監査をアプリケーション外部に移行し、分散アプリケーションまたは分散システムで、集中管理されたアクセス・ポリシーを実施できます。

認証

アクセス・システムは、Oracle Access Manager が保護するリソースにアクセスしようとするユーザーとシステムを認証する集中的な手段を提供します。アクセス・システムは、以下の認証方法をサポートしています。

- 基本的なユーザー名/パスワード
- X.509 証明書
- スマート・カード
- 2 要素トークン
- フォームベース
- 認証 API によるカスタム認証

Oracle Access Manager は、Web リソースや J2EE リソースに対する集中管理されたポリシーベースの認証、認可、および監査サービスを提供します。

アクセス・システムを使用すると、認証レベル階層を決定するポリシーを定義し、ビジネス要件に適合するために組み合わせて使用することができます。たとえば、ユーザー名とパスワードで社員ポータル・システムを保護できますが、機密データを扱う機密性の高い HR セルフサービス・アプリケーションの場合、RSA SecurID トークンを使用してユーザーを認証する必要がある場合があり、より機密性の高いリソースやアプリケーションに対して、より高度なセキュリティを提供できます。

さらに、ポリシーベースの認証モデルにより、各種のユーザー・タイプやバックエンド認証リポジトリを扱える認証のフローや手順を定義できます。たとえば、認証のフローで、ユーザー名とパスワードを要求し、この認証情報を LDAP ディレクトリと比較してユーザーを認証します。ただし、この認証が失敗しても、ア

アクセス・システムは、Windows ドメインと比較して認証を試みることができます。エンド・ユーザーは、この認証のフローを意識しません。認証の柔軟性により、この複雑さをエンド・ユーザーから隠したまま、各種のバックエンド認証システムをシームレスに移行し、統合することができます。

Access Manager は、各種の認証方法と機器を統合するための認証 API を提供します。SecurID などのスマート・カードのサポートが同梱されています。認証 API を使用すると、生体認証や 2 つの要素による認証を含む、ほとんどすべての認証形態をサポートするように、Access Manager を拡張できます。

ユーザーが認証されると、アクセス・システムは、一度サインオンするだけで、そのポリシー・ドメイン内の他のリソースにもアクセスできるユーザー用のシングル・サインオン・セッションを作成します。

認可

デフォルトで、アクセス・システムは、Web リソースや J2EE リソースへのアクセスの安全性を確保するために、集中管理されたポリシーベースの認可サービスを提供します。認可は、このドメイン用のリソースを保護する方法を指定する 1 組のデフォルト・ルールにある認可式を含むポリシー・ドメインによって制御されます。管理者は、ブラウザベースの管理システムである Policy Manager コンソールを使用して、ユーザー、ロール、グループの帰属関係（静的、ネスト、または動的）、時刻、曜日、および IP アドレスによって特定のリソースへのアクセスを制限するポリシーを定義します。

さらに、アクセス・システムは、カスタム認可プラグインを作成することによりアクセス管理ポリシーにカスタム認可ロジックを組み込んで、付属の認可オプションの利用可能範囲を拡大できる Authorization API を提供しています。多くの場合、認可プラグインを使用して、アクセス・システムを配置するときに継続使用または移行が望まれる既存の認可ロジックまたは認可システムを組み込みます。

集中的に認可を行うことで、開発者はセキュリティ・ポリシーの実施でなく、アプリケーションのビジネス・ロジックに集中できるので、開発費用が大幅に削減されます。

監査

監査サービスは、Oracle Access Manager が監視するイベントの詳細で柔軟なログ機能を提供します。これらのイベントには、認証の成功または失敗、認可の成功または失敗などがあります。監査証跡には、アクター（たとえばユーザー）からの設定可能な ID 情報や文脈情報（たとえば、時刻、発信元 IP アドレス、Web サーバーまたは Web サーバー・ファーム用のホスト識別子）などが記録されます。

Access Manager は、管理者がすべての監視対象イベントに適用されるデフォルトまたは「包括的」監査ポリシーを定義できる、ポリシーベースの監査モデルを提供します。ただし、必要に応じて、アプリケーション・レベルやリソース・レベル（たとえば、URL リソースや J2EE リソース）といった、より細かいレベルでこのポリシーの例外を設定できます。そのため、管理者は、特定のアプリケーションやリソースの機密性や重要性に応じて、必要な監査情報の量を管理することもできます。たとえば、デフォルトのポリシーが、操作とリソースに加えて、ユー

ザーのログイン名だけを取得するのに対し、HRセルフサービス・アプリケーションについては、この監査ポリシーは、ユーザーがアプリケーションにアクセスした IP アドレス、トランザクションを処理した特定の Web サーバーの識別子とともに、社員番号とコスト・センターも取得することができます。

監査プロセスにより、管理者は、他社製品と統合することによって、脅威や侵入の検出、セキュリティ監視、およびビジネスレベルの報告を実行できます。監査ログは、フラット・ファイルまたはデータベース (Oracle RDBMS 10g, SQL Server) に記録し、Oracle Reports や Business Objects などの他社製報告ツールを使用して取り出し、ある期間、あるアプリケーションでの認証の失敗、ユーザー別のアクセス履歴、ユーザー別またはアプリケーション別の認可の失敗など、総合的な監査報告書を作成することができます。

アクセス・システムのコンポーネント

アクセス・システムには、WebGate または Web サーバー・クライアント、AccessGate または API ベースのクライアント、Access Server、および Policy Manager が含まれています。ポリシー・データ、構成データ、および ID データ用のバックエンド・ストアは、LDAP ベースのディレクトリ・サーバーです。以下に、各コンポーネントの機能について説明します。

アクセス・システムの中で、WebGate と AccessGate は、ポリシー実施ポイント (PEP) です。Access Server は、ポリシー決定ポイント (PDP) です。また、Policy Manager は、ポリシー管理機関です。

WebGate

WebGate は、HTTP ベースのリソースでアクセス・ポリシーを実施するための付属アクセス・クライアントであるため、アクセス・システムの Web ポリシー実施ポイント (PEP) です。WebGate クライアントは、ほとんどの代表的な Web サーバーでプラグインまたはモジュールとして動作し、Web リソースに対する HTTP 要求を傍受して、アクセス制御ポリシーが適用される Access Server へ転送します。WebGate は、HTTP プロトコルに対応し、URL、セッション Cookie、HTTP リダイレクト、セキュアなセッション (HTTPS) を理解し、さらに WebGate の性能改善と、アクセス数が多いサイトでスケーラビリティを可能にするポリシー・キャッシュを実装しているため、Web サーバー環境で動作するように最適化されています。

AccessGate

AccessGate とは、WebGate 以外の任意のアクセス・システム・クライアント、つまりアクセス・システムの非 Web PEP のことを指します。通常は、Access API を使用するクライアントの実装です。AccessGate を使用して、BEA WebLogic、IBM WebSphere、Oracle Containers for J2EE などのアクセス・システムで使用できる J2EE アプリケーション・サーバーやポータル・コネクタを作成します。さらに、お客様独自のアクセス・システム・クライアントを実装し、カスタム・アプリケーションやカスタム・システムへの実施ポイントを開発することができます。

Access Server

Oracle Access Manager の Access Server は、Web リソースと Web 以外のリソースにアクセス・ポリシーを実施するスタンドアロン・ソフトウェア・サーバー、つまりアクセス・システムのポリシー決定ポイント（PDP）です。Access Server は、負荷分散とフェイルオーバーをサポートするために、単一インスタンスに、またはクラスタ化された実装の一部として配置できます。Access Server には負荷分散とフェイルオーバーが組み込まれているため、外部の負荷分散機能を配置する必要はありません。Access Server は、認証、認可、および監査サービスに加え、ユーザーがリソースにアクセスするときに動的ポリシー評価機能を提供します。アクセス・システムは、ユーザー情報とポリシー情報両方の設定可能なキャッシュ機能を提供して、アクセス・ポリシー評価の性能を大幅に改善する拡張可能なサーバーです。

Policy Manager およびアクセス・システム・コンソール

Oracle Access Manager の Policy Manager は、保護対象のリソースを設定し、アクセス・ポリシーを作成し、管理するためのブラウザベースのグラフィック・ツール、つまりアクセス・システムのポリシー管理機関（PMA）です。Policy Manager は、アクセス・システム用のログイン・インタフェースを提供し、ポリシー・データを管理するためにディレクトリ・サーバーと通信し、ポリシーが変更されたときに Access Server キャッシュを更新するために Oracle Access Protocol 経由で Access Server と通信します。図 1 に、Policy Manager のポリシー管理インタフェースの画面例を示します。マスター・アクセス管理者と委任アクセス管理者は、Policy Manager を使用して以下を実行します。

- 以下で構成されるポリシー・ドメインを作成し、管理する。
 - 保護するリソースの種類
 - 認証、認可、および監査ルール
 - ポリシー（例外）
 - 管理権限
- ポリシー・ドメインにリソースを追加する。
- アクセス・ポリシーの実施をテストする。

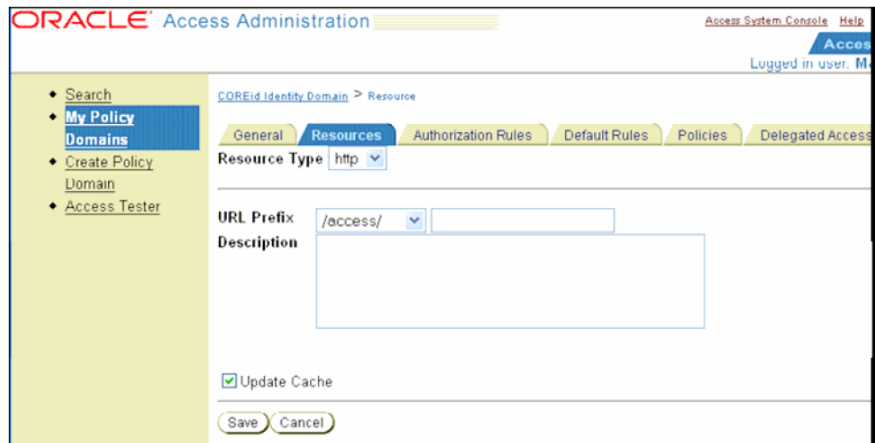


図 1. Policy Manager によるポリシーとリソースの定義

Policy Manager は、ポリシー管理用の Web ベースの中央コンソールを提供します。アクセス・システム・コンソールは、アクセス・システム・コンポーネントの管理と設定に使用する Web ベースの管理インターフェースです。

管理者は、アクセス・システム・コンソールを使用して、アクセス・システムを管理および運用できます。管理者は、Access Client と Access Server の追加、変更、および削除、認証と認可方式の設定、マスター監査の設定、ホスト識別子の設定、特定のユーザーの取り消し、暗号用の共有秘密鍵の管理、システム・ステータスの監視、および Policy Manager で管理しているポリシーによって保護する新しい種類のリソースの定義を行うことができます。図 2 に、アクセス・システム・コンソールを示します。

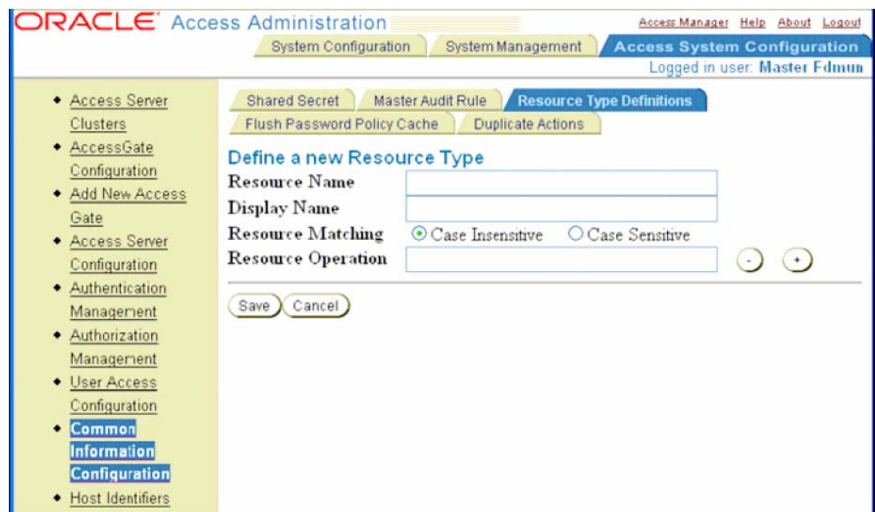


図 2. アクセス・システム・コンソールによるシステム管理

アクセス・システム・アーキテクチャ

図3に、アクセス・システム・アーキテクチャの概要を示します。3つの主要コンポーネント（WebGate、Access Server、およびPolicy Manager）、およびポリシー・ストアとIDリポジトリとして使用されるバックエンド・ディレクトリ・サーバーが配置されたアクセス・システムを示しています。Oracle Access Protocol（旧称NetPointまたはCOREid Access Protocol）は、ユーザー認証および認可中のアクセス・システム・コンポーネント間のセキュアな通信を可能にします。

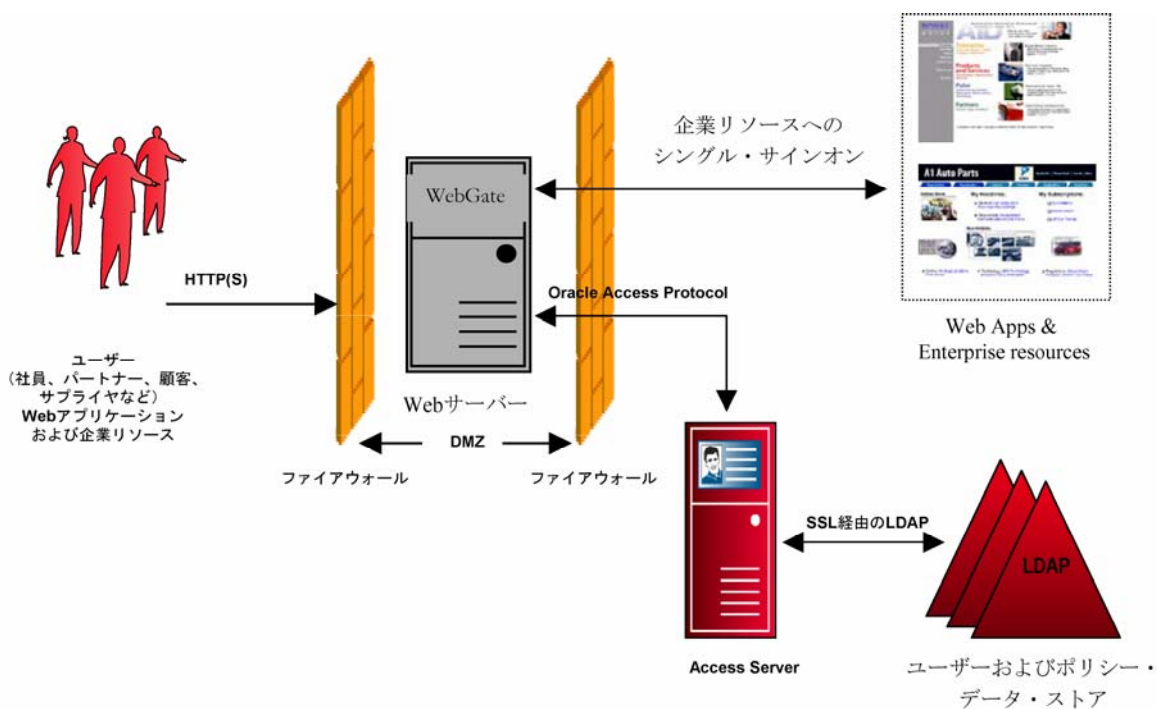


図3. アクセス・システム・アーキテクチャの概要

保護された企業リソースにユーザーがアクセスしようとする時、WebGate と Access Server は以下の手順を実行します。

1. 通常、DMZ に配置される WebGate が、ユーザー要求を傍受し、アクセスされているリソースが保護されているかどうかについて Access Server に確認します。
2. リソースが保護されている場合、WebGate は、ユーザーに資格証明を求め、それを検証するために Access Server へ転送します。
3. Access Server は、提供されたユーザー資格証明をバックエンドのディレクトリ・サーバーと比較して検証します。
4. 検証の結果が WebGate に返送されます。認証が成功すると、WebGate はユーザーのブラウザに Cookie を設定し、保護されているリソースにユーザーがアクセス権を持っているかどうかについて Access Server に確認します。

5. Access Server はディレクトリからポリシーをフェッチし、保護されているリソースにユーザーがアクセスできるかどうかについて評価します。結果が WebGate に返送されます。
6. ユーザーが認可されると、ユーザーは保護されているリソースにアクセスできるようになります。

ID 管理

Oracle Access Manager の ID システムは、管理者とユーザーに、アクセス制御の効果的な管理に必要な主要 ID 管理機能を提供します。実際に使用されると、ID システムは、アクセス・システムが管理するアクセス・ポリシーによってアクセスが制御される ID 用の ID 管理エンティティになります。このアクセス管理と ID 管理の相乗効果は、Oracle Access Manager 固有の差別化要素です。

ID システムのコンポーネントには、Identity Server、WebPass Web サーバー・プラグインがあります。Identity Server は、ユーザー、グループ、組織、および他のオブジェクトに関する ID 情報を管理し、ID 管理フロー専用のワークフロー・エンジンを提供するスタンドアロン・サーバーです。WebPass プラグインは、Web サーバーと 1 つまたは複数の Identity Server インスタンスの間で情報を交換します。このアーキテクチャは高いスケーラビリティを提供するので、管理要件の必要に応じて、より多くの Identity Server を配置できます。

ポータル環境の効果的で費用効率が低い管理には、委任管理、動的グループ管理、およびユーザーのセルフサービスと自動登録といった機能の管理サポートが必要です。Oracle Access Manager の ID システムは、カスタマイズ可能な付属コンソール、ポータル・アプリケーションに埋め込まれたポータル挿入物、または Web サービス経由で統合されたカスタム・インタフェースとしてこれらの機能を提供します。以下で、Oracle Access Manager の ID システムのこれらの機能について説明します。

委任管理

Oracle Access Manager の ID システムは、大規模なユーザーを管理するために不可欠な委任管理を提供します。

ポータル配置が数千、数百万のユーザーをサポートする場合、集中管理チームの課題は、常に変化するユーザー・プロフィールを管理することです。委任管理は、さまざまなユーザー集団の管理責任をグループ管理者に委任することで、このような環境の効率的な管理を可能にします。たとえば、メーカーが 1000 サプライヤー向けのサプライヤー・ポータルを運用する場合、メーカーは各サプライヤー企業のユーザー管理の責任を、各サプライヤーの指定の管理者グループに委任できます。その結果、作業が分散され、データの精度と管理のスケーラビリティが向上します。

Oracle Access Manager は、多くの大規模なポータルで稼働実績があり、今日の市場で最も柔軟で拡張性の高い委任管理機能を提供します。

Oracle Access Manager には、動的グループや属性レベルのアクセス制御などの強力で柔軟な認可機能があります。

動的グループ管理

非常に有用かつ共通した ID 管理を実現するには、アクセス制御を強化し、管理を単純化するために、ユーザーをグループに割り当てる機能が必要です。グループは、ロールを表現する際に最もよく使用される言葉で、ポータル、アプリケーション・サーバー、共同作業システム、およびメッセージング・システムのようなほとんどの主流のアプリケーションがこれを認識できます。

グループは、ユーザーを明示的にメンバーとしてグループに追加して静的に実装することも、メンバーを決定するために実行時に評価されるルールまたはフィルタによって動的に定義することもできます。実際の配置では、大勢のユーザーを静的グループに割り当てると拡張性が低下し、管理者が数千の個別ユーザーからなるグループを手動で管理する必要があります。この場合、ユーザー属性に基づく動的グループを使用する方法が適しています。次の例で、動的グループの価値を示します。

数百万のユーザーを持つ携帯電話会社の顧客ポータルでは、SMS メッセージングを利用するすべての顧客を含む動的グループを「SMS ユーザー」と呼ぶことができます。このグループのユーザーには、追加のサポート Web ページへのアクセスが自動的に許可されます。顧客は SMS メッセージングの利用を中止したり、再開したりすることがあるので、ユーザーを手動でこのグループに割り当てることは現実的でなく、グループを表現する大量のデータが、ストレージ・サイズだけでなく、複製や整合性の維持に関しても、バックエンド・ディレクトリに大きな負担を与えます。この場合、Oracle Access Manager のグループ管理機能を利用する動的グループ方式を採用すると、プロファイル属性に基づいてユーザーを自動的に「SMS 利用者」グループに追加したり、グループから削除したりできます。グループはセットアップ中に適切なフィルタを使用して定義されますが、グループ自体に大きなストレージ容量は必要でなく、ほとんど変化しません。顧客が SMS メッセージの利用を開始すると、ディレクトリ・プロファイルのフラグがアクティブになり、Oracle Access Manager はただちに顧客をグループに追加します。

ユーザーのセルフサービス/自動登録

ユーザー自身がプロファイルを管理できるようにすると、管理のスケラビリティが向上します。ユーザーは、Oracle Access Manager に付属している自動登録画面を使用して、管理者の介入なしにユーザー自身をディレクトリに追加できます。自動登録は、Oracle Access Manager のワークフロー機能を使用して、ユーザーがプロファイルを追加するとき、制御とプロセスがかならず実施されるようにすることができます。また、ユーザーは、許可されているアクセス・レベルの範囲内で自分の属性を変更できます。たとえば、一部のユーザーは、電話番号の更新は許可されているが、職位は変更できません。これらの社員の上司は、職位は変更できるが、部門を変更できない、などです。Oracle Access Manager は、ユーザー属性の限りなく柔軟なアクセス制御をサポートし、ワークフローをこれらの変更に関連させます。その結果、目的とする管理制御レベルの下で、ユーザーの管理能力と柔軟性が向上します。

紛失パスワード管理

ユーザーは、パスワードを忘れたとき、紛失パスワード管理を使用してパスワードをリセットできます。紛失パスワード管理が有効になっている場合、ID システムのログイン・ページまたは管理者が設定した別のページに、リンクが表示されます。リンクを選択すると、事前に設定された 1 つまたは複数の個人的な質問に答えるための Web ページが表示されます。質問に正しく回答すると、ユーザーはオンラインで新しいパスワードをリアルタイムに設定できます。これで、ユーザーは、目的のシステムやアプリケーションを利用できるようになります。

紛失パスワード管理を有効にするには、ディレクトリ管理者が、**Challenge X** と **Response X** (X は、これらが複数のペアになることもあるという意味) といった属性のペアを定義します。管理者は、ID システムコンソールから、これらの属性に対して **Challenge** と **Response** のタイプの意味を割り当て、実行時にユーザーに無作為に提示する質問の数を設定します (通常は、設定した総数のサブセット)。管理者は、ユーザー作成時にこれらの対になった属性を登録しておくことも、自動登録時にユーザー自身にこれらの値を入力するように求めることも可能です。多くの場合、許される質問のリストが事前に定義され、ユーザーは事前に定義された質問のリストから選択します。ID システムは、RSA からライセンスされた強力な暗号方式を使用してこれらの値を暗号化します。

ID システムのコンポーネント

ID システムには、WebPass クライアント、Identity Server、および Policy Manager の ID システムコンソールが含まれます。以下に、各コンポーネントの機能について説明します。

WebPass

WebPass は、ID システムのプレゼンテーション層であり、ブラウザとの HTML インタフェースと SOA 環境での ID 管理機能を提供する SOAP ベースの Web サービス・インタフェースを提供します。

WebPass は、Oracle Identity Protocol (旧称 Netpoint または COREid Identity Protocol) 経由で Web サーバーと Identity Server 間で情報を交換する Web サーバー・プラグインです。したがって、WebPass は、ID システムのプレゼンテーション層です。WebPass は、デフォルトで、ブラウザからアクセスできるようにその内容を HTML で表示します。さらに、SOAP ベースのクライアントが ID システムとプログラム的に対話するために利用できる IdentityXML と呼ぶ Web サービス・インタフェースを提供します。IdentityXML の目的は、ID 管理プロセスを制御するビジネス・ロジックを SOA 環境で利用可能にし、既存のアプリケーションに簡単に統合できるようにすることです。

Identity Server

Identity Server は、ユーザー、グループ、組織、および他のオブジェクトに関する ID 情報を管理します。Identity Server は、主に 3 つの機能を実行します。

- ネットワーク接続経由で LDAP ディレクトリ・サーバーから読み取り、LDAP ディレクトリ・サーバーに書き込む。
- ユーザー情報をディレクトリ・サーバーに保存して、ディレクトリの最新状態を維持する。
- ユーザー、グループ、および組織の ID に関係するすべての要求を処理する。

Identity Server は、これらの機能を提供するために、属性値レベルで ID 情報にアクセスするルールを定義し、実施できるように、非常に細分化された属性レベルのアクセス制御機能を実装しています。これは、複雑な委任、プライバシー、およびセルフサービスのビジネス要件に適合する点で、ID システムの最も顕著な長所の 1 つです。さらに、ID システムは、ID 情報の作成、自動登録、要求/承認の変更、非アクティブ化と削除などの ID 管理機能に特化した、特許で保護されたワークフロー・エンジンを提供しています。

また、Identity Server のワークフロー・エンジンは、イベント駆動型であり、カスタム・ログインを起動する API を提供しています。この API は、Identity Server が管理するデータを使用してカスタム・ロジックを評価したり、Identity Server がワークフローの下流手順で使用するために追加データを投入したりできるように、双方向の情報の流れをサポートしています。たとえば、自動登録時に、エンド・ユーザーが最初の手順で顧客 ID 番号を入力すると、Event API を使用して作成されたカスタム・プラグインが、顧客 ID が有効なので登録を許可してもよいことを確認します。さらに、確認プロセスでは、カスタム・プラグインが、ユーザーのメール・アドレスを取得し、ユーザーがワークフローの次の手順でメール・アドレスを確認できるようにワークフローに挿入することができます。

Oracle Access Manager の ID 管理コンソールには、ユーザーのセルフサービス、委任管理、パーソナライズ、および監査機能があります。

ID システムコンソール

ID システムコンソールは、ID システムコンポーネント (WebPass および Identity Server) および ID システムの User Manager、Group Manager、および Organization Manager アプリケーションの Web ベースの設定と管理を提供します。

ID システムアーキテクチャ

ID システムは、WebPass、Identity Server、および ID システムコンソールという 3 つの主要コンポーネントで構成されます。

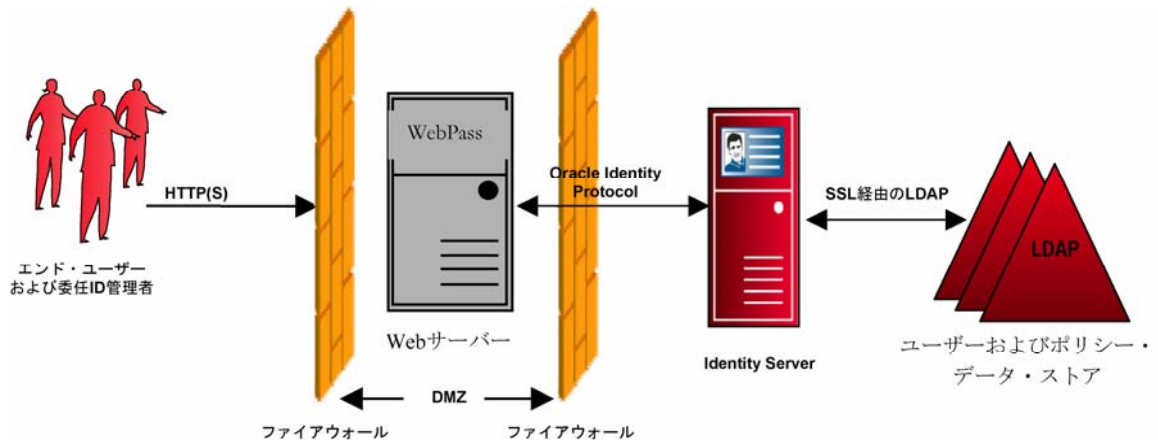


図 4.ID システムアーキテクチャの概要

図 4 に、単純な環境での基本的な ID システムコンポーネントと、Oracle Identity Protocol (旧称 NetPoint または COREid Identity Protocol) 経由のコンポーネント間の転送セキュリティを示します。通常、エンド・ユーザーと管理者は、ファイアウォールによってコンポーネントから分離されます。WebPass をインストールした Web サーバーは、DMZ に存在します。Identity Server とディレクトリ・サーバーは、2 番目のファイアウォールの背後に存在します。Oracle Identity Protocol は、Identity Server とそれに関連する WebPass インスタンス間の通信を容易にします。

監査

Oracle Access Manager は、集中管理された監査データベースにセキュリティおよびプロファイル管理アクティビティを記録することによって、規制順守をサポートできます。

監査レポート作成について、Oracle Access Manager はレポート作成フレームワークをサポートしているので、集中管理されたリレーショナル・データベースにすべてのセキュリティおよびプロファイル管理アクティビティを記録でき、任意の他社製レポート作成ツールを使用してレポートを作成できます。監査担当者は、規制と社内方針に準拠しているという有効な証拠を要求し、管理者もセキュリティと ID 運用の弱点を分析したいと考えています。最も一般的な監査レポートの項目の一部を以下に示します。

- 認証統計 (すべての Access Server にわたる成功/失敗の比率)
- 認可統計 (すべての Access Server にわたる成功/失敗の比率)
- 失敗した認可 (ユーザー別)
- 失敗した認可 (リソース別)
- アクセス・テスト
- グループ履歴 (すべてのグループ・プロファイルに対するすべての変更)
- ID 履歴 (ユーザー別)
- ロックアウトされたユーザー
- パスワードの変更 (特定の期間内)
- 作成/非アクティブ化/再アクティブ化/削除されたユーザー

- ユーザー・プロフィールの変更履歴（全ユーザー対象）
- 非アクティブにされたユーザーのレポート
- ワークフローの実行時間

異機種サポート

Oracle Access Manager は、多くの他社製 Web サーバー、アプリケーション・サーバー、ディレクトリ・サーバー、およびパッケージ・アプリケーションとシームレスに統合されます。

Oracle Access Manager には、さまざまなプラットフォームで動作するアプリケーションを管理し、保護するための統合エージェントが含まれています。これらの統合コンポーネントには、複数のプラットフォームで動作する主要な Web サーバー、アプリケーション・サーバー、およびポータル・サーバー用のエージェントが初めから含まれています。これにより、すでに他社テクノロジーに投資されてきたお客様は、Oracle Access Manager をシームレスに環境に配置できるので、投資収益率（ROI）が上昇します。

Oracle Access Manager の WebGate と AccessGate コンポーネントは、他社製インフラストラクチャやカスタム・インフラストラクチャ製品に接続され、要求を傍受して、アクセス・ポリシーを適用します。現実の本番環境を保護するために、複数のバージョン、製品、およびオペレーティング・システムを網羅するこれほど充実したサポートを提供している ID 管理ベンダーは他にありません。

Oracle Application Server Single Sign-On との相互運用性

Oracle Access Manager は、Oracle Application Server Single Sign-On と完全に相互運用可能なので、Oracle のお客様は、1 回のサインオンですべての企業アプリケーションにアクセスできます。

Oracle Access Manager は、Oracle アプリケーション用の Oracle の組込み認証サービスである Oracle Application Server Single Sign-On と完全に相互運用可能です。そのため、Oracle Portal、Oracle Collaboration Suite、Oracle E-Business Suite Release 11i、または他の Oracle アプリケーションを使用するオラクルのお客様は、Oracle Access Manager を配置して、すべての企業アプリケーションへのアクセスを 1 か所で制御でき、ユーザーは 1 回のサインオンですべての企業アプリケーションにアクセスできます。

まとめ

Oracle Access Manager は、業界で最も総合的なアクセス制御とユーザー ID 管理を提供するソリューションです。Oracle Access Manager のアクセス・システムは、Web シングル・サインオン、複数の認証方法のサポート、および集中管理されたポリシーの評価と実施を提供します。Oracle Access Manager の ID システムは、委任管理、ワークフロー、動的グループ・サポート、およびユーザーのセルフサービス/自動登録などの拡張可能な ID 情報管理を提供します。Oracle Access Manager は、オラクルの企業向け ID 管理ソリューションの主要コンポーネントを提供します。

ORACLE FUSION MIDDLEWARE

Oracle Fusion Middleware
Oracle Access Manager の紹介

2006 年 6 月

Oracle Corporation World Headquarters
500 Oracle Parkway Redwood Shores, CA 94065 U.S.A.

お問い合わせ :
電話 : +1.650.506.7000
ファクシミリ : +1.650.506.7200
oracle.com

Copyright © 2005, Oracle. All rights reserved.

このドキュメントは情報提供のみを目的として提供されており、ここに記載される内容は予告なく変更されることがあります。

Oracle Corporation はこのドキュメントに一切間違いがないことを保証するものではなく、さらに、口述による明示または法律による黙示を問わず、特定の目的に対する商品性もしくは適合性についての黙示的な保証を含み、いかなる他の保証や条件も提供するものではありません。

Oracle Corporation はこのドキュメントに関するいかなる法的責任も明確に否認し、このドキュメントによって直接的または間接的に確立される契約義務はないものとします。

このドキュメントは Oracle Corporation の書面による許可を前もって得ることなく、いかなる目的のためにも、電子または印刷を含むいかなる形式や手段によっても再作成または送信することはできません。このドキュメントで使用しているその他の名称は、各社の商標の場合があります。