Oracleホワイト・ペーパー
2012年7月

ファイングレイン認可：Oracle Entitlements Serverの使用に関する技術的洞察

免責事項

以下の事項は、弊社の一般的な製品の方向性に関する概要を説明するものです。また、情報提供を唯一の目的とするものであり、いかなる契約にも組み込むことはできません。以下の事項は、マテリアルやコード、機能を提供することをコミットメント（確約）するものではないため、購買決定を行う際の判断材料になさらないで下さい。オラクルの製品に関して記載されている機能の開発、リリース、および時期については、弊社の裁量により決定されます。

概要

ID管理は、IDストアやプロビジョニング、認証などの個別のIDセキュリティ・サービスを外部化することで、徐々に発展を遂げてきました。COTS（Commercially available Off-The-Shelf/商用既製品）ソリューションを利用する企業には、セキュリティ機能を構築するための専用チームや専門知識が必要ないという利点があります。しかし、認可に関して言えば、セキュリティ製品が外部化してきたのはURLアクセスに対する境界（コースグレイン）認可のみであり、複雑でファイングレインなアクセス・ロジックの大半は、引き続きアプリケーション内にハードコードされているのが現状です。オラクルの戦略的な認可ソリューションであるOracle Entitlements Serverは、アプリケーションの認可を外部化し、複雑な認可要件を表す高度なポリシー・モデルを提供します。また、複数の標準に基づく認可モデルをサポートすることで柔軟性を提供するとともに、Java SE、Java EE、.NET、SOAといった関連するシステムと事前に統合されています。

はじめに

ID管理は、簡素なものから始まり、大きな飛躍を遂げてきました。当初、すべてのユーザー名とパスワードはフラットなテキスト・ファイルに保管されており、プロビジョニングはこれらのファイルをテキスト・エディタで変更するに過ぎず、認証はユーザー・パスワードを文字列比較しただけのものでした。現在、ほとんどの企業では、ヒューマン・ワークフローや高度なシングル・サインオン（SSO）メカニズムが統合された専用のプロビジョニング・ソリューションを使用して、ユーザーを企業LDAPに保管しています。しかし、アプリケーションによって直接処理されているID管理領域も依然として存在します。ファイングレイン認可は、その最たる例です。URLベースの境界認可が外部化されたとしても、コア・アプリケーション側の認可は多くの場合、カスタム・アプリケーション・コードによって処理されています。コードを使用してセキュリティ要件を実装することは、次のような意味合いを持ちます。

a） セキュリティ・ポリシーが脆弱になる上に、すべての変更に対して冗長な開発サイクルとテスト・サイクルを実行する必要があります。

b） 脅威やセキュリティ侵害に対して迅速に対応する能力が欠如します。

c） セキュリティ・ポリシーと認可に関する実行時の決定を分析し、監査することは困難です。

d） アプリケーション開発者はしなくても良い作業を何度も繰り返し実行せざるを得ないため、開発サイクルが長期化し、コストが上昇するだけでなく、多くの場合、柔軟性に欠け、セキュリティが不十分な実装がもたらされます。

e） 開発コストと保守コストが上昇します。

これらの問題の根底にある原因は、セキュリティが通常のアプリケーションとは別に処理するべき特殊領域である事実です。アプリケーション開発チームは、たいてい、最善の製品やサービスを届けるという企業の構想に向けて取組みを行います。多くの場合、セキュリティは、収益創出のビジネス目標とはかけ離れています。アプリケーション・コードにセキュリティを融合させることは、互いに相容れない2つの目標を結合することになります。この問題に対処するための最善の方法は、分割攻略方式に従って、個別に解決できる、より*小さな項目に問題を分割することです。*アプリケーションにこれを当てはめると、セキュリティを外部サービスとして取り扱う必要が生じます。アプリケーション内部で計算を行って決定するのではなく、外部サービスを利用して認可に関する決定を行う必要があります。

外部の認可サービスを使用することで、アプリケーション側で複雑なセキュリティ管理を理解する必要はなくなります。アプリケーション開発者はセキュリティやコンプライアンスを気にすることなく、ビジネス上の問題を解決するベスト・オブ・ブリード・ソリューションの提供に集中できます。また、専用の認可サービスであれば、政府や業界による高水準のコンプライアンス要件から低水準の適用まで、複雑なセキュリティをあらゆる側面からサポートできるでしょう。

Oracle Entitlements Serverの概要

Oracle Entitlements Serverは、企業全体で、アプリケーションとサービスをエンド・ツー・エンドで保護するファイングレイン認可ソリューションです。Java EE、Java SE、.NET、SOA、コンテンツ管理などのシステムやデータベースを含む豊富なシステムに認可機能を提供します。Oracle Entitlements Serverには複数の統合機能が標準提供されており、影響を最小限に抑えたまま特定の実装に*組み込むことができます。*また、開発サイクルと導入サイクルを切り離せるため、アプリケーション開発者が導入の問題に煩わされることはありません。すべてのアプリケーション・テクノロジーに向けたオラクルの戦略的認可ソリューションであるOracle Entitlements Serverは、オラクルの顧客の中でももっとも複雑かつ大規模な実装のパフォーマンス要件とスケーラビリティ要件にも対応できるように設計されています。認証とは異なり、認可リクエストにはマイクロ秒単位でレスポンスが求められることもあり、1つのWebページ・アクセスが50以上の個別認可リクエストを生成する場合もあります。Oracle Entitlements Serverは、*ロール・ベースのアクセス制御（RBAC）*標準と*属性ベースのアクセス制御（ABAC）*標準に基づく、高度な階層型のポリシー・モデルを提供します。また、*マルチレベルの委任管理*をサポートしているため、セキュリティ・ポリシーの作成と管理を厳密に制御できます。Oracle Entitlements Serverは、市場でもっとも成熟したファイングレイン認可製品であり、10年以上前から使用されています。

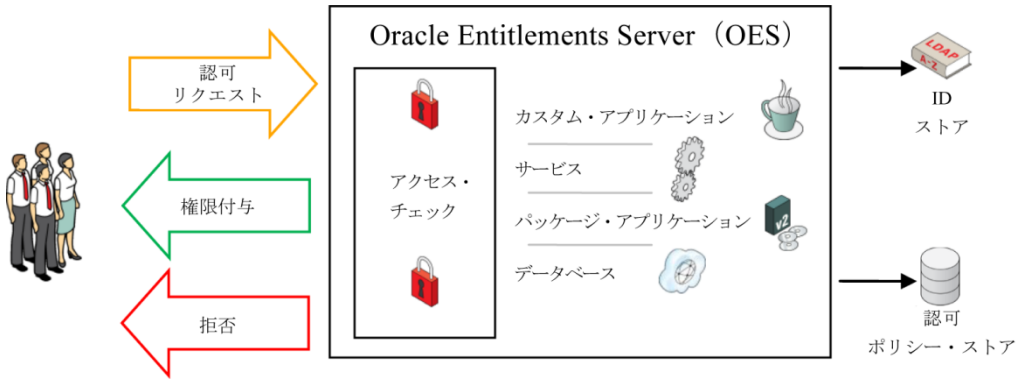


図1：Oracle Entitlements Serverの概要

上の図は、Oracle Entitlements Serverの概要を示したものです。ユーザーは、Webページへのアクセスなどの通常活動の一環として、アクセス・リクエストを生成します。Oracle Entitlements Serverは、これらのリクエストを正規化した形式へとマッピングし、認可ポリシーに対するチェックを実行します。ポリシー評価の実行中、Oracle Entitlements Serverは、LDAPシステムやデータベース、またWebサービスなどの外部データソースから取得した情報を利用できます。最後に、Oracle Entitlements Serverは、認可レスポンスを*認可決定とオブリゲーション*（オブリゲーションについては、*ポリシー設計*の項で説明）の形で要求元に送り返します。

Oracle Entitlements Serverのアーキテクチャ

Oracle Entitlements Serverは、次のコンポーネントで構成されています。

コンポーネント・アーキテクチャ

管理コンソール

管理コンソールは、ポリシーの作成と管理向けにWebベースの高機能なUIを提供し、ポリシーの更新情報をアプリケーションに配信します。さらに、ポリシー・ライフ・サイクルを管理するため、インポート・ツール、エクスポート・ツール、移行ツールを提供します。

ポリシー・ストア

ポリシー・ストアは、認可ポリシーの集中型永続ストアとしての役割を果たします。このポリシー・ストアを利用することで、セキュリティの一元管理が可能になります。アプリケーションは、必要に応じてポリシー配信サービスをバイパスし、中央のポリシー・ストアから直接ポリシーを取得することもできます。

セキュリティ・モジュール（SM）

セキュリティ・モジュールは、コアの認可エンジンを含むランタイム・コンポーネントです（別名ポリシー決定ポイント（PDP））。ユーザーまたはアプリケーションから認可リクエストを受け取ると、SMは、関連するすべてのポリシーに対してこのリクエストを評価し、最終的な認可結果を返します。ポリシー評価の一環として、SMは、LDAPシステムやデータベース、Webサービスやその他のデータソースなどの外部データソースから情報を検索できます。SMは、必要に応じてポリシーを直接管理するように構成することもできます。こうすることで、1つのアプリケーションでポリシー管理、ポリシー決定、ポリシー実施を実行できるようになります。

ポリシー配信サービス

ポリシー配信サービスは、Oracle Entitlements Server*管理サーバー*と各種の*セキュリティ・モジュール*間の橋渡しをします。一連のポリシー変更の配信準備が整ったと管理者が判断すると、ポリシー配信プロセスが開始されます。次に、*ポリシー配信サービス*によって自動的にプロビジョニング・ライフ・サイクルが処理され、配信ペイロードを最小化するため、SMに含まれるポリシーと最新のポリシーとの差分が計算されます。*ポリシー配信サービス*は、転送レベルのセキュリティを確保するだけでなく、必要な認可ポリシーのみがSMまたはアプリケーションに送信されるようにします。SMが起動されると、保留中のポリシー更新情報がすべて*ポリシー配信サービス*から取得されます。また、顧客は任意で、Oracle Entitlements Serverポリシー配信サービスの代わりに独自のプロビジョニング・ソリューションを使用できます。

ポリシー・シミュレータとポリシー・ライフ・サイクル管理ツール

Oracle Entitlements Serverは、管理コンソールからポリシーをシミュレートする機能を提供しています。*ポリシー・シミュレーション*を使用することで、ポリシー変更の影響をテスト、分析、トラブルシューティングし、特定のアプリケーションに対するポリシーの適用方法を理解できます。

簡単なポリシー・シミュレーションのケースでは、*ユーザー*と*リソース・アクション*のペアを指定すると、パラメータに基づいて次の情報が取得されます。

a) *プリンシパル*に付与される*外部ロール*と、*静的ロール付与*と*ロール・マッピング・ポリシー*のリスト

b) 関連するロールまたは認可ポリシーの評価に必要な*属性*

c) 関連するロールまたは認可ポリシーの一部として実行された評価機能の値

d) 関連するロール、*認可ポリシー*、または*オブリゲーション*の一部である*動的属性*の値。動的属性の値が未知の場合、ユーザーが明示的に設定できるように空白が返されます。

e) 最終的に返された認可決定（*付与または拒否*）、*オブリゲーション*、関連する*認可ポリシー*

認可決定の一環として属性値が評価される場合、その他の値を使用して追加のシミュレーションを実行できます。

Oracle Entitlements Serverは、*開発からテスト*、また*テストから本番*へとポリシーを移行するための自動化ツールを提供しています。また、顧客は、ソース・コードとともにポリシー・ファイルをバージョン管理システムに保存できます。移行ツールは、ポリシーのバックアップやリストア、および障害時リカバリ用に使用できます。

認可決定の計算の一部として、セキュリティ・モジュールは、外部のIDストアやデータベース、およびWebサービス（ポリシー情報ポイント（PIP））から取得した情報を使用します。

監査とレポーティング

あらゆるセキュリティ・システムにとって、*監査*は重要な部分です。分析、コンプライアンス、レポーティングは、監査データに大きく依存しています。Oracle Entitlements Serverの監査機能は、追跡のアカウンタビリティを考慮して設計されています。イベントは、どのように開始されたかに関係なく、監査レコード内で追跡されます。これには、アプリケーションによって開始された認可リクエストだけでなく、Oracle Entitlements Server認可ポリシーに対する変更の追跡が含まれます。認可ポリシーに対するすべての変更は、バックエンドの管理APIレイヤーで追跡されるため、イベントがどのような方法で開始された場合でも、監視の対象になります。同様に、認可決定リクエストもバックエンドAPIで記録されるため、Java SE、Java EE、SOA、.NETといった各種環境にわたってアクセスが一様に追跡されます。

高い負荷にさらされているアプリケーションの場合、フル監査を有効化すると、ディスク領域がいっぱいになり、CPUやディスクのIO帯域幅を大量に使用します。Oracle Entitlements Serverの監査機能は、階層型の柔軟な監査構成をサポートしているため、永続化する情報に適切な量を選択することで、その他のオーバーヘッドを最小化できます。

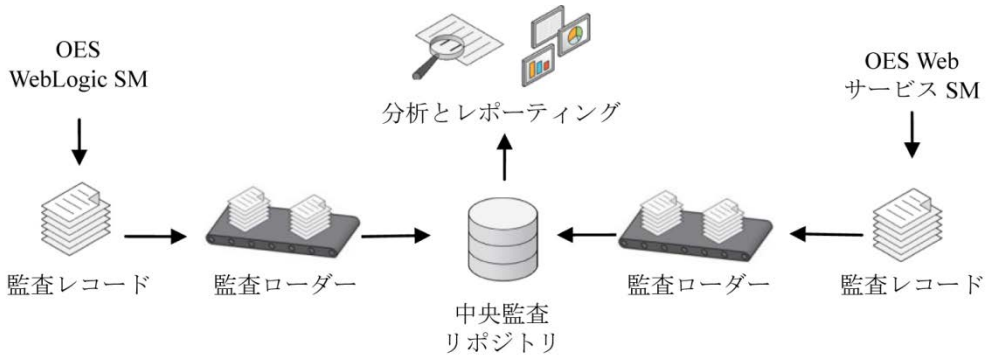


図3：（監査とレポーティング）

上の図は、Oracle Entitlements Serverの監査アーキテクチャを示したものです。このアーキテクチャは、Oracle Platform Security Servicesの一元化監査フレームワークに基づいています。監査レコードはローカルのファイル・システム上にスプールされ、定期的に中央ストアに送信されます。Oracle Entitlements Serverの監査レコードは、分析ツールやレポーティング・ツールで処理できる形式になっています。たとえば、Oracle Business Intelligence Publisher（Oracle BI Publisher）を使用して、Oracle Entitlements Server監査データに対するレポートを生成し、分析を実行できます。

スケーラビリティ

キャッシング

Oracle Entitlements Serverのキャッシング・アーキテクチャは、柔軟性を維持しながら、パフォーマンスを最大化するよう設計されています。次の図は、Oracle Entitlements Serverのキャッシング・アーキテクチャを示したものです。Oracle Entitlements Serverのキャッシングは、マルチレベルに分かれています。認可APIに組み込まれたキャッシュは、要求された決定が最近計算されたかどうかを特定します。これにより、中央のOracle Entitlements ServerのSMに対する高コストのラウンドトリップが最小化されます。決定キャッシングはSM内に実装されており、ポリシー配信サービスと緊密に統合されています。ポリシーが変更されると、決定キャッシュは自動的に無効化されます。次の層にあるPIP（属性）キャッシングには、LDAPシステムやデータベース、Webサービスなどの外部データソースからフェッチした情報が保存されます。ユーザーは、これらのキャッシュ以外にカスタム・キャッシングを追加したり、エンタープライズ・グリッドからデータをフェッチしたりすることができます。この多層キャッシング・アーキテクチャを利用することで、アプリケーションは、ネットワーク・ラウンドトリップやコストのかかるポリシー計算を回避できます。

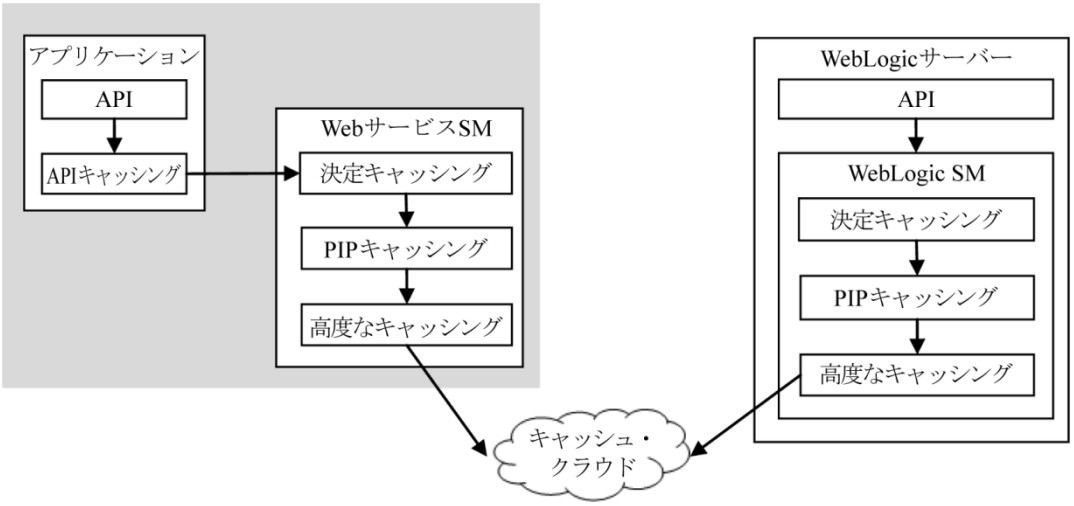


図4：キャッシング・アーキテクチャ

SMPとマルチコア・アーキテクチャ

Oracle Entitlements Serverの認可エンジンは、本質的にマルチスレッド化されています。このエンジンは、アプリケーションの要件や使用可能なコアとCPUの数に基づいてスケールアップするよう設計されています。認可エンジン内の競合とロッキングは、最小限に抑えられています。このため、アプリケーションは複数のスレッドやCPUにわたる拡張を実現できます。また、リソース使用を制限するため、スレッド・サイズや接続プール・サイズの最大値を指定できます。

クラスタ化、ロードバランシング、フェイルオーバー、高可用性

Oracle Entitlements Serverの構成および実装アーキテクチャでは、レプリケーションを容易に実行できます。Oracle Entitlements Serverでは、インストールと構成のメカニズムが簡素化されているため、実装のスケールアップとスケールダウンが簡単になりました。Oracle Entitlements Serverは、エンド・ツー・エンドのフル冗長性をサポートしており、シングル・ポイント障害はありません。すべてのコンポーネントを完全冗長モードで実装できるだけでなく、あらゆるOracle Entitlements Serverコンポーネントに複数のエンド・ポイントを構成できるため、これらのエンド・ポイント間での透過的なフェイルオーバーがサポートされます。Oracle Entitlements Server管理サーバーには、複数のポリシー・ストア、IDストア、シングル・サインオン（SSO）プロバイダに対するサポートが組み込まれています。複数のOracle Entitlements Server管理サーバーをプライマリ/ホット・スタンバイ・モードで実装できます。Oracle Entitlements ServerランタイムAPIに対して、冗長なSMを構成できます。プライマリSMへの接続に問題が発生すると、アプリケーションに影響を与えることなく、APIによって透過的にバックアップへのフェイルオーバーが実行されます。同様に、Oracle Entitlements ServerのSMも冗長エンド・ポイントをサポートしており、複数のポリシー・ストア・インスタンス（Oracle Real Application Clusters（Oracle RAC）テクノロジーを使用）や管理サーバー、属性リポジトリ（PIP）を構成できます。SMによってエラーが検出されると、スタンバイ・インスタンスへのフェイルオーバーが透過的に実行されます。すべてのOracle Entitlements Serverコンポーネントに対して、コマンドラインを使用した非対話型モードのインストールと構成がサポートされています。これを使用すると、障害時リカバリの目的で、システム全体を自動的に再作成できます。

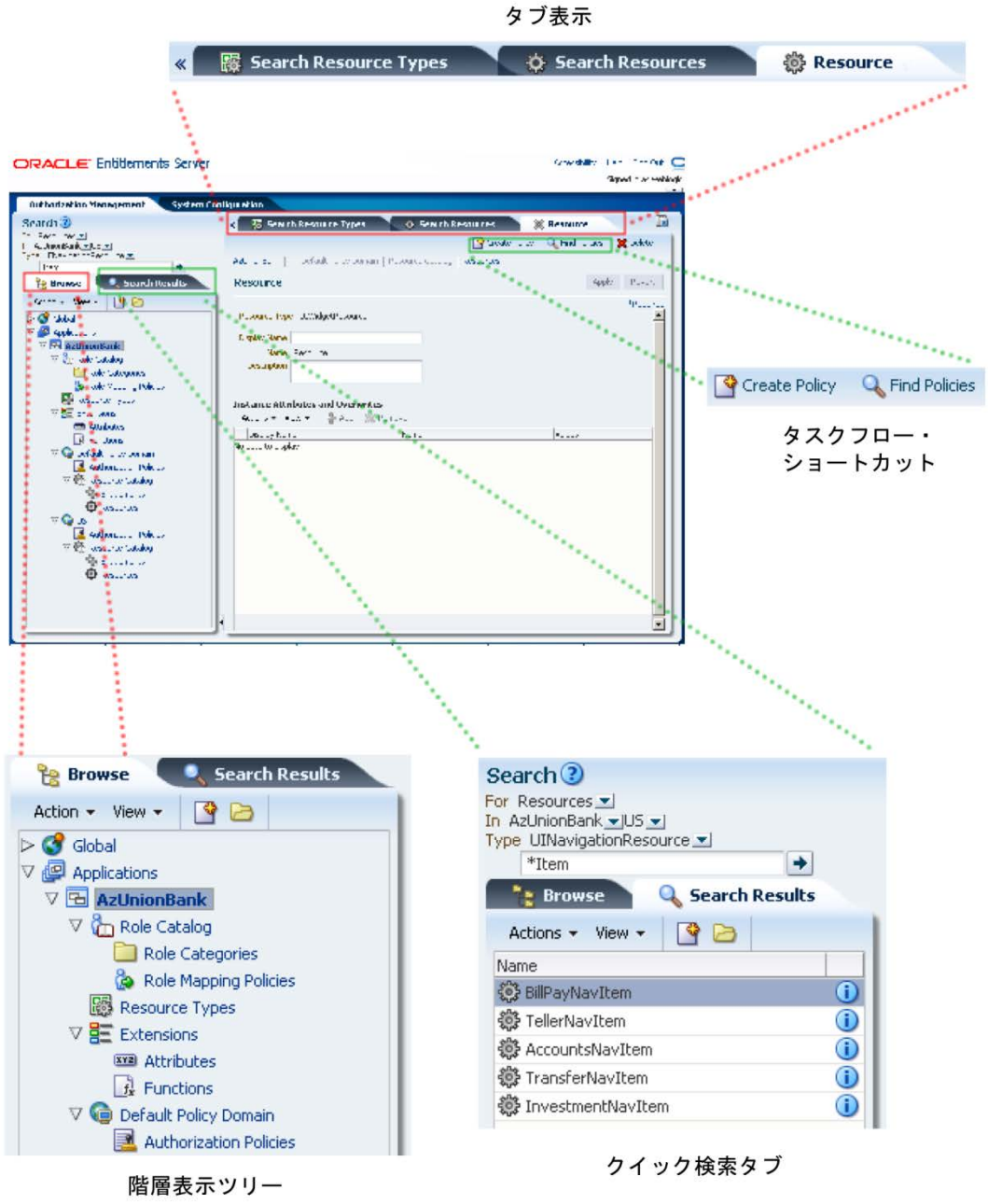


図5：（Oracle Entitlements Server管理コンソール）

Oracle Entitlements Server*管理コンソール*（UI）は、階層的な概念と検索の概念を考慮して構成されています。ナビゲーションするには、階層表示ツリーを順にたどることも、クイック検索を使用してオブジェクトを直接探すこともできます。階層を順にたどることでポリシー・オブジェクトの場所を見つけることができるため、経験の浅いユーザーにとって、構造化された構成は有用です。その一方で、経験豊かなユーザーは検索対象を明確に把握しており、各種のポリシー要素へ直接アクセスする必要があるため、検索の使用を好みます。

Oracle Entitlements Server*管理コンソール*は、一般的なタスク・フローを簡素化するためのショートカットを提供しています。たとえば、*リソース*画面には*Policy Search*画面と*Policy Creation*画面のショートカットが用意されています。*管理コンソール*では、一般的なタスク・フローの実行に必要なクリック数やコンテキストの切替え数を最小化するために、タブ付きのUIレイアウトを提供しています。このレイアウトを使用すると、ユーザーは複数のタスクを並行して実行できます。管理コンソールはWeb 2.0テクノロジーを使用して構築されており、*ドラッグ・アンド・ドロップ*などの機能を提供しています。また、UIのルック・アンド・フィールをカスタマイズすることもできます。

Oracle Entitlements Serverの認可ポリシー・モデル

概要

Oracle Entitlements Serverが提供するポリシー・モデルは、一般的なビジネス・フロー、アプリケーション・フロー、そしてサービス・フローを厳密に表現することを目指しています。その目標は、企業のコンプライアンス要件や規制要件を表すモデルをユーザーが簡単に構築できるような*ポリシー・モデリング・ツール・キット*を提供することにあります。個別のビジネス・ロールと権限に対する単純な1対1マッピングは、ポリシーの肥大化を招きがちであるだけでなく、さらに重要なことに、基盤となるプロセスとオブジェクトの関係を捉えてはいません。さらに、属性と権限を継承できます。Oracle Entitlements Serverの階層構造を利用すると、ポリシーのサイズと複雑さを大幅に軽減できます。

Oracle Entitlements Serverは、ABAC（XACML（eXtensible Access Control Markup Language））、RBAC（NIST RBAC）、ERBAC（Enterprise RBAC）、JAASのポリシー・モデルをサポートしています。ビジネス要件に応じて、これらのポリシー・モデルのうちの1つまたは複数を使用できます。

ポリシー設計

多くの場合、ビジネス・プロトコルとオブジェクトは階層型になる傾向があります。たとえば、ローン承認プロセスは複数のサブプロセスで構成されており、これらのサブプロセスの一部はさらにきめ細かいプロセスで構成されている場合があります。同様に、Webアプリケーションは複数のWebページで構成される場合が多く、各ページにはさまざまなセクションが含まれ、各セクションには各種の情報が含まれます。次の図に、Webページを階層型に分解した様子を示します。左側は標準的なWebページの構造を、右側は同じ構造に対するリソース階層を示しています。Webページ要素とリソースは、それぞれ1対1で対応しています。ユーザーがメイン・ページ（下図を参照）へのアクセス権を持たない場合、そこに含まれるサブ要素へのアクセスも自動的に拒否されます。したがって、ユーザーが通常のチェックをバイパスして下層コンテンツに直接アクセスしようとした場合、リクエストは拒否されます。

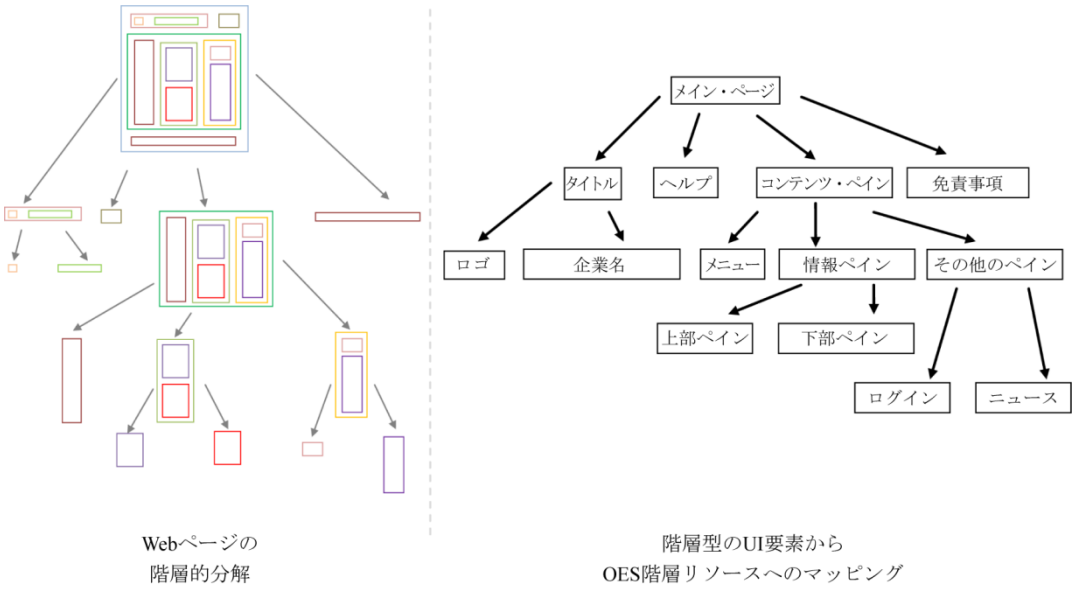


図6：WebページからOracle Entitlements Serverリソース・ツリーへのマッピング

*ロール・ベースのアクセス制御（RBAC）*は、よく理解されている単純なテクノロジーです。すでに30年以上にわたって、積極的に使用されています。現在、RBACは、業界全体でもっとも広く使用されているセキュリティ・モデルの1つであり、RBACを使用したセキュリティ・モデルは、多くのセキュリティ専門家によって理解されていますRBACの基礎となるのはロールであり、*エンタープライズ・ロール*（またはグループ）は、コースグレイン認可の基盤を形成しています。エンタープライズ・ロールは認証時に静的に割り当てられ、ログイン・セッションが続く限り持続されます。この種のロール割当ては、過剰な権限を招きます。反対に、*アプリケーション・ロール*（ファイングレイン・ロール）は動的な性質を持ち、認可リクエストの開始時に生成されて、認可決定が計算されると削除されます。*アプリケーション・ロール*は、*コンテキスト*に基づいて割り当てられます。たとえば、企業全体に対して マネージャー・ロールを付与する場合と、認可リクエストがその直属のコンテキスト内にある場合のみ マネージャー・ロールを付与する場合について考えてみましょう。

Oracle Entitlements Serverでは、*ポリシー*に基づいて*アプリケーション・ロール*を動的に割り当てることができます。次のサンプル・ユースケースについて考えてみましょう。*多くの大学では、課程（クラス）の管理方法に関して、各教授に相当な柔軟性が与えられています。*教授は、場所や試験スケジュール、登録方法、成績などを変更することが認められており、これらの権限は、その課程を担当するメインの指導者のみに制限されています。この制限は、次の認可ポリシーとして要約できます。*"大学の課程を管理できるのは、その課程を指導している教員のみである。"*

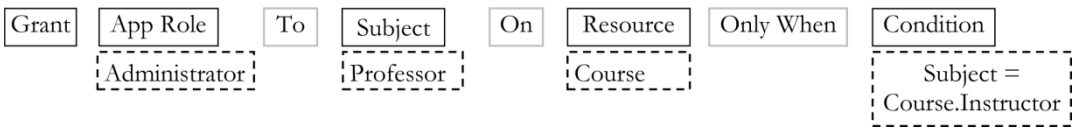


図7a：ロール・マッピング・ポリシーの構成

ロール・マッピング・ポリシーには拒否（または否定的付与）を指定することもできます。次のポリシーでは、*"銀行終業後1時間経過すると、どの従業員に対しても窓口（出納係）ロールを割り当てることはできない"*、と規定されています。

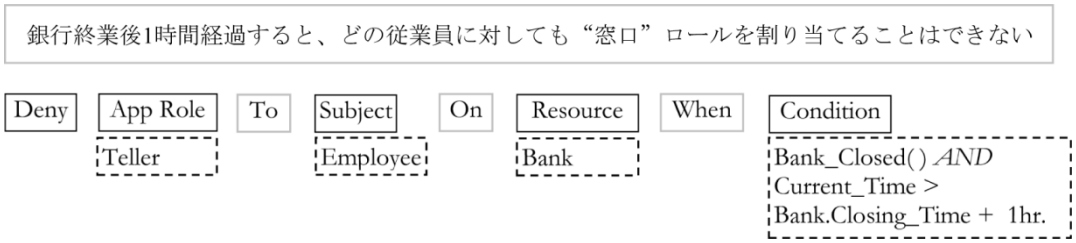


図7b：拒否を含むロール・マッピング・ポリシーの構成

多くの場合、*ビジネス・ロール*は階層型の構造を持ちます。高い職位にある従業員には、その直属の階層にある要員の権限が自動的に付与されます。このような実際の関係をモデル化するため、Oracle Entitlements Serverは階層ロールをサポートしています。次の図に示したとおり、研究開発ディレクターには開発者、構築エンジニア、開発マネージャー、テスト・エンジニア、テスト・マネージャーのロールが暗黙的に割り当てられます。このような組織では、バイス・プレジデントは組織全体を管理下に置くことができます。

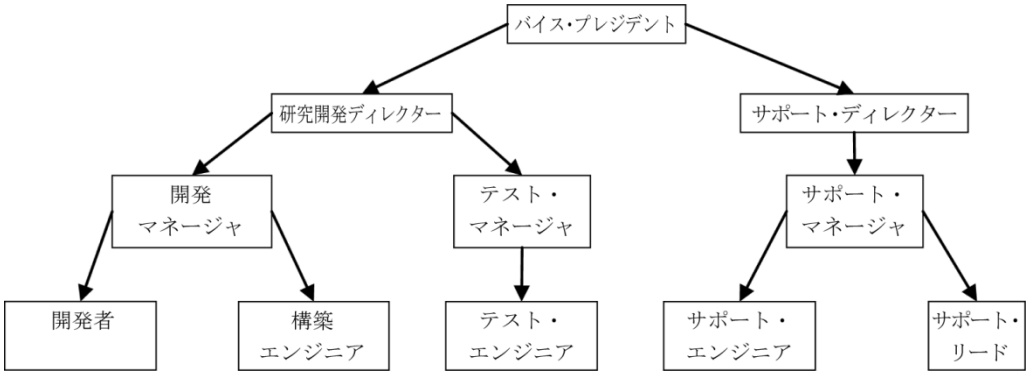


図8：ビジネス・ロールの階層特性

Oracle Entitlements Serverポリシーの条件文を使用すると、いつロールを付与または拒否するかに関して、追加の制御を行うことができます。この文には、ユーザー、エンタープライズ・ロール（グループ）、リソース、環境、およびカスタムの属性に基づく式が指定されます。たとえば、次の図は、"*下級の株取引担当者は1日に100万ドル未満の取引しか実行できない*"というポリシー条件の作成方法を示しています。Oracle Entitlements Serverを使用すると、LDAPシステムやデータベース、Webサービスなどから取得した情報に対してポリシー属性を直接マッピングできます。また、Oracle Entitlements Serverファンクションを使用して、条件内でカスタム・プラグインを起動することもできます。ユーザーは、ロード可能なモジュールとしてコードをパッケージ化し、そのファンクション定義をOracle Entitlements Serverファンクションにマッピングできます。

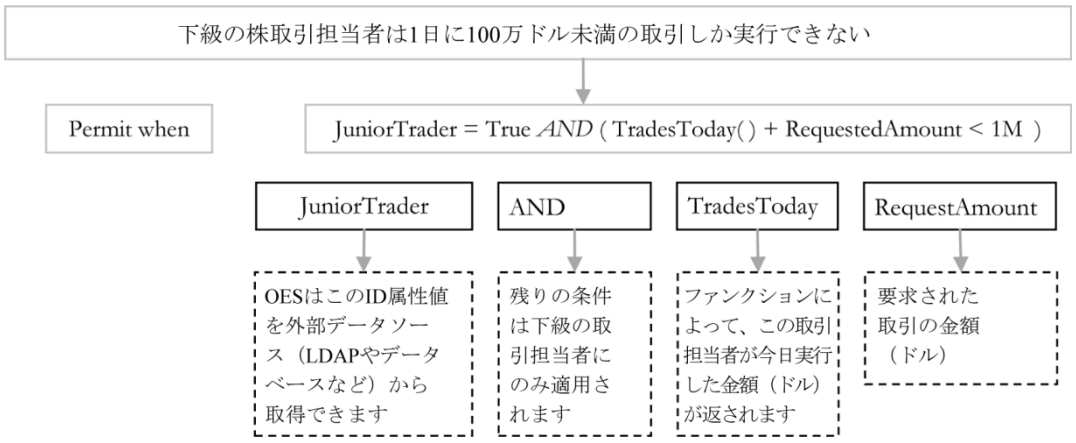


図9：サンプルのポリシー条件

多くの場合、実際のプロセスは複数のリソースにまたがります。Oracle Entitlements Serverでは、*エンタイトルメント*を使用することで、ビジネス・フローとUIタスク・フローを厳密にモデル化できます。エンタイトルメントは、特定のビジネス・タスクを実行するために必要なリソースとアクションを組み合わせたものです。たとえば、銀行口座の開設処理は、複数フォームの入力、各口座名義人に対する項目の作成、最終的な口座の作成など、いくつかの個別ステップで構成されています。銀行従業員が新規口座の開設を許可されている場合、いくつかのWebフォームへのアクセスと顧客の経済的な経歴をチェックする機能が必要になります。エンタイトルメントを使用すると、口座開設などのタスク・フローをエンド・ツー・エンドで表すことができます。ビジネス・タスク・フローに必要なすべての権限（リソースとアクション）は、1つのエンタイトルメントとしてグループ化できます。このようにエンタイトルメントを使用することで、セキュリティ管理者は細かい権限に悩まされることなく、大局的なビジネス・タスク・フローに取り組むことができます。エンタイトルメントがもたらすもう1つの利点は、正規表現を使用してリソースを特定できる点です。自動生成されたリソース名は特定のテキスト・パターンに従うことが多いため、正規表現パターン（すべてのスプレッドシート・ドキュメントを参照する"*.xls"など）を使用すると、このようなリソース・コレクションの特定が容易になります。

動的なロールの割当てによって解決されるのは、認可問題の最初の半分のみです。最終的に、これらのロールは実際の権限にマッピングする必要があります。Oracle Entitlements Serverの認可ポリシーを使用すると、権限に対して、ユーザー、エンタープライズ・ロール、アプリケーション・ロールを動的にマッピングできます。Oracle Entitlements Server認可ポリシーは、条件式が一致した場合のみ、認証対象（Subject）が特定のリソース（Resource）に対して、特定のアクション（Action）を実行する権限を付与（Permit）または拒否（Deny）します。たとえば、従業員が物理的にオフィス内にいる場合のみ、顧客のクレジットカード情報を参照できるポリシーがコールセンターに設定されているとします。このポリシーは、"*イントラネットIPアドレスから接続している場合のみ、従業員に顧客クレジットカード番号の参照を許可する*"、と表現できます。

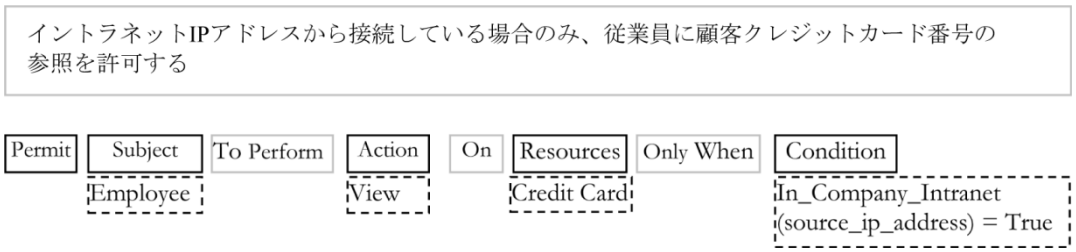


図10：ビジネス・ロールの階層特性

Oracle Entitlements Serverは、XACMLのオブリゲーション概念もサポートしています。一部のユースケースでは、認可エンジンを使用した単純な*許可/拒否*では十分でない場合があります。これは、条件の一部が認可エンジンでは評価できない場合に発生します。たとえば、データ・セキュリティのユースケースでは単純な*YES/NO*回答は十分ではなく、データベース内で検索フィルタ（SQLのWhere句など）を適用する必要があります。このような場合は、認可要求を評価する際、Oracle Entitlements Serverの認可ポリシーから*オブリゲーション*としてSQLフィルタを返すことができます。

Oracle Entitlements Serverを使用したRBACモジュールの構築

RBACモジュールでは、エンタープライズ・セキュリティのモデル化にロールが使用されます。RBACにとって、権限はロールをわずかに拡張したものに過ぎません。ロールは、次の3つのカテゴリに分けられます。

a) *全社的な静的ロール：*ユーザーが何を実行しようとするかに関係なく、これらのロールは付与されます。たとえば、従業員ロールは会社全体で共通しているため、静的な割当てになります。このようなロールの最適な保管先は、LDAPなどの全社的なIDストアです。通常、これらのロールは認証時に割り当てられ、一般に、セッションが無効になるまで維持されます。

b) *アプリケーション固有の静的ロール*: これらは、一部のエンタープライズ・アプリケーションに固有の静的ロール割当てになります。ユーザーには、アクセスしようとするアプリケーションによって異なるロールが付与されます。通常、これらのロールがユーザーのセッション中に変更されることはありません。Oracle Entitlements Serverでは、これらのロール割当てを直接管理する機能を提供しています。

c) *アプリケーション固有の動的ロール：*これらは、動的に、または条件に応じて、割り当てられるアプリケーション・ロールです。これらのロールは、ユーザーが開始したアクションによって必要に応じて割り当てられます。たとえば、ファンド・マネージャーというロールが一人のユーザーに割り当てられる場合、特定のファンドについての権限のみが付与されるべきです。これらのロールは認可リクエストが出される際に生成され、認可決定が計算されると破棄されます。前述のとおり、Oracle Entitlements Serverは、コンテキストに基づいてロール割当てを正確に制御する、高度な機能を提供しています。

これらから分かるとおり、*全社的な静的ロール*は簡単に計算できますが、柔軟性に欠けます。動的ロールは認可リクエストごとに計算する必要がありますが、柔軟で動的な性質を持ちます。また、多くの場合、参照局所性によって、これらのロールがキャッシュからフェッチされるため、完全な計算は必要ありません。静的または動的な特性とロール範囲が、適切なロール・タイプを選択する際の決め手となります。変更要件によっては、*全社的なロール*から*アプリケーション固有の動的ロール*に変換したり、その逆を実行したりすることもできます。この種の相互運用性が実現されるのは、Oracle Entitlements Serverが*NIST RBAC*標準と*ABAC*標準に基づいているためです。

Oracle Entitlements Serverを使用したABACモデルの構築

属性は、ABAC（Attribute Based Access Control）モデルの基盤です。Oracle Entitlements Serverでは各種の属性（ユーザー、エンタープライズ・ロール、リソース、アプリケーション・ロール、要求アクションなど）がサポートされていますが、特殊な要件がある場合は、カスタム属性を定義することもできます。ABACは条件に大きく依存しているため、基本的にこれらの属性に基づいて式を評価することで、すべての認可決定が行われます。ABACは動的な計算を多く利用しているため、認可モデルとしては、RBACよりも高い柔軟性を実現しています。ただし、これには静的なポリシー・データに基づく監査実行能力を犠牲にする必要があります。また、複雑さが増しているため、ABACモデルは、相当するRBACモデルよりも計算集約型になります。

Oracle Entitlements Serverのポリシー構造は、ビジネスのセキュリティ要件をそのままABACモデルにマッピングできるように配置されています。サブジェクト（ユーザー、エンタープライズ・ロール、アプリケーション・ロール）、リソース、アクション、および属性は、ABACポリシーでもっともよく使用される要素です。Oracle Entitlements ServerのUIでは、ポリシーの構築を簡素化するため、これらのオブジェクトに関する使いやすい抽象化が作成されています。また、Oracle Entitlements Serverは、リソースや属性、およびポリシーの継承をサポートしているため、ポリシーを戦略的に配置することで、多数のユーザーやリソースを制御できるようになります。

クレームと連携認可のサポート

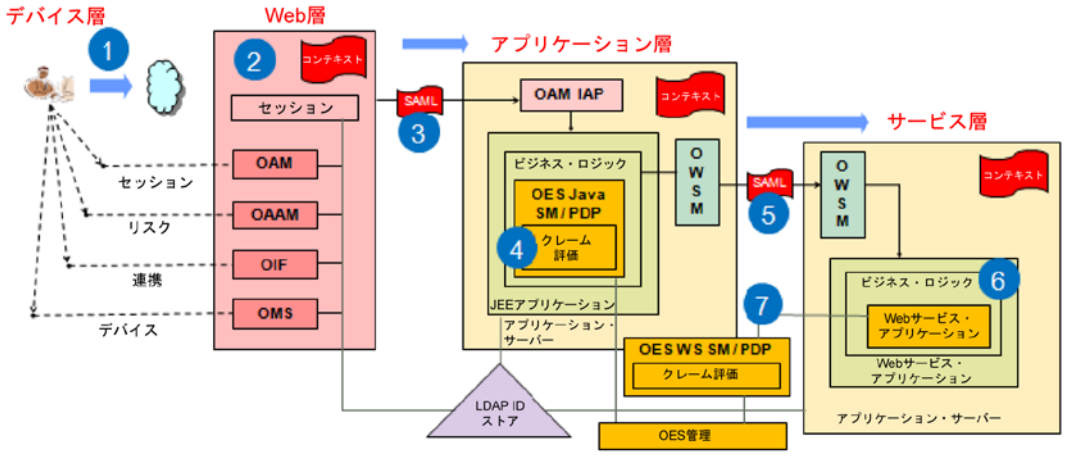
.NETおよびMicrosoftのシステムは、クレーム・ベースのモデルに大きく依存しています。Oracle Entitlements Serverの観点から見ると、クレームは、署名付きの属性と値の組み合わせであり、オンデマンドで検証できます。クレーム（SAMLアサーションとX-509証明書を含む）を環境属性にマッピングし、認可要求の一部として直接渡すことができます。また、Oracle Entitlements Serverは、ポリシーの実行中にCustom Attribute RetrieversやCustom Functionを使用して、適切なクレーム発行元から要求されたクレーム情報を取得できます。クレームは分散モデルに基づいているため、容易に連携できます。しかし、過剰な連携は集中制御の低下を招くため、必要な場合のみに留める必要があります。

リスクとコンテキストに基づくアクセス

Oracle Entitlements ServerとOracle Access Managementは、コンテキスト認識型コンピューティングを実現する独自のエンド・ツー・エンド・ソリューションを提供します。

IDコンテキストは、Oracle Entitlements Serverによる認可決定向けに自動的に提供されるため、組織はユーザーやデバイス、ランタイム・コンテキストに基づいて、ユーザーに許可される実行内容やアクセスできる情報を制御できます。ランタイム・コンテキストの例を次に挙げます（以下に限定されるわけではありません）。

- ユーザーの属性、ロール、リソース、動的属性と環境条件
- システムに対してユーザーが認証された方法
- システム・アクセスに使用されているデバイス・タイプ（例：PC、モバイル機器）
- デバイスに関する情報 - 登録済みデバイスまたは信頼できるデバイスであるか、物理ロケーション、IPアドレス、オペレーティング・システム、ジェイルブレイクされているか、ウイルス・スキャンとファイアウォールは有効か、VPNは有効か、など
- 連携パートナーからのアサーション
- リスク・レベル - アクセス・パターンやトランザクションにおける異常のリアルタイム分析に基づく



上の図は機能の使用例を示しています。

1） ユーザーがデバイスからアプリケーションにアクセスします。

2） Oracle Access ManagerがIDをアサートし、IDコンテキストを作成します。

3） 作成されたIDコンテキストは、SAMLアサーション・トークンを介してJavaEE層に自動伝播されます。

4） アプリケーションは、ローカルのOracle Entitlements Server認可PDPを呼び出して、ポリシーを評価します。

5） Oracle Web Services Manager（Oracle WSM）によって、SAMLを介してコンテキストがWebサービス層に自動伝播されます。

6） アプリケーションによる意思決定向けにコンテキストが提供されます。

7） コンテキストはリモートのOracle Entitlements Server PDPに自動伝播され、コンテキスト内の情報を認可決定で利用できます。

委任管理

ポリシー管理は、エンド・ツー・エンドのセキュリティにとって決定的な要素です。権限付与されたユーザーのみが変更を実施できるようにするためには、管理に関する正しいチェックとバランスが不可欠です。Oracle Entitlements Serverは、システム、アプリケーション、カスタム・サブアプリケーションの各レベルで、多層の委任管理を実現します。監査者ロールにはすべてのアプリケーション・ポリシーに対する参照権限のみを付与し、QAエンジニアには一部のアプリケーションに対する参照権限のみを付与し、開発者には特定のアプリケーション・サブコンポーネントに対してリソースを作成し、ポリシーを管理する権限のみを付与できます。

次の図では、以下の権限が設定されています。

a） Aliceには、アプリケーション1のポリシーにのみ参照権限が付与されています。

b） Bobには、*アプリケーション2のコンポーネントXとアプリケーション1*のポリシーに対する管理権限が付与されています。

c） Charlieには、すべてのアプリケーションに対する参照権限が付与されています。

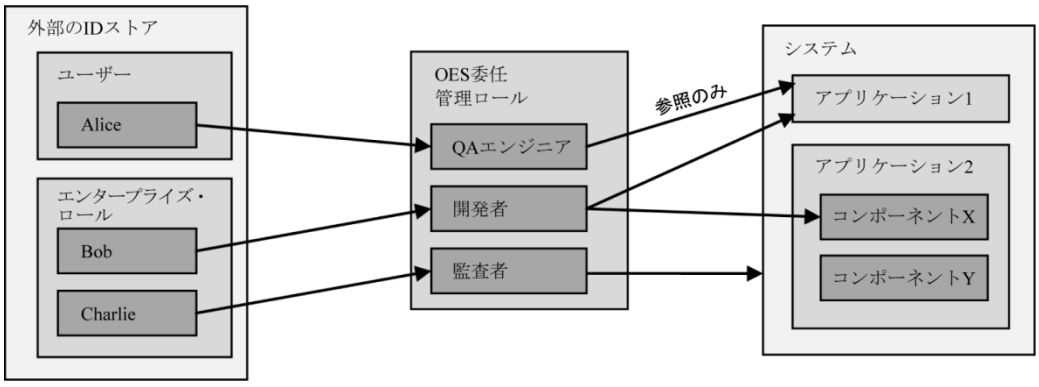


図11：委任管理

Oracle Entitlements Serverの統合

Oracle Entitlements Serverはエンタープライズ認可サービスであり、Java SE、Java EE、SOA、および.NETのエコシステムを含むエンド・ツー・エンドのソリューションを提供します。Oracle Entitlements Serverでは複数の統合機能が標準で提供されているだけでなく、多数の環境に対して簡単にゼロから統合を作成できるように設計されています。

Java EE

Java EEは成熟したJavaシステムであり、エンタープライズ・アプリケーションを構築およびデプロイするためのサービスを提供します。Java EEアプリケーションは、EJBやWebサービス、Webアプリケーション、RMIなどのサービスを公開します。コンテナは限定された形での境界認可のみを提供しており、たとえば、ユーザーのSAMLアサーション内に定義されたID属性に基づいて、Webサービス・メソッドへのアクセスを制限するようなことはできません。また、コンテナにはドメイン間で認可ポリシーを共有する機能が備わっていないため、大規模企業にとっては重大な制約事項になります。

Oracle Entitlements Serverは、*WebLogic*、*WebSphere*、*Apache Tomcat*、*JBoss*を含む標準Java EEコンテナをサポートしています。また、Oracle Entitlements Serverのネーミング・メカニズムでは、クラスタ・アーキテクチャがサポートされています。クラスタ内のすべてのノードには、自動的に同じ構成とポリシーが適用されます。これにより、大規模クラスタの構成と認可ポリシーの管理が簡単になります。Oracle Entitlements Serverは、JSP、サーブレット、URL、Web、サービス、EJB、JDBC、JMS、JNDI、RMIなどのJava EEコンポーネントに対する保護をサポートしています。

Java EEデプロイメントに対して、Oracle Entitlements Serverは、JSPタグ・バージョンの認可APIを提供しています。これらは、宣言型のセキュリティ向けにWebアプリケーションで使用できます。

WebSphere、Apache Tomcat、JBossに対して、Oracle Entitlements Serverは、コンテナ全体の認可サービスを提供しています。これらは、コンテナにデプロイされたすべてのアプリケーションから使用できます。アプリケーションは認可リクエストを出すだけでなく、適切な権限があれば、認可ポリシー自体を参照したり変更したりすることもできます。

WebLogicの場合、APIと管理APIのサポートに加えて、Oracle Entitlements Serverはコンテナ自体に対するプライマリ・セキュリティ・プロバイダとしての役割を果たすため、アプリケーションがOracle Entitlements Serverを意識する必要はありません。アプリケーションがコンテナのサービスを使用する際、根底にあるセキュリティ・フレームワークから自動的にOracle Entitlements Serverが呼び出され、認可決定が適用されます。つまり、Oracle Entitlements Serverは、WebLogicに対してPEPの役割を果たします。次に、アーキテクチャ図を示します。

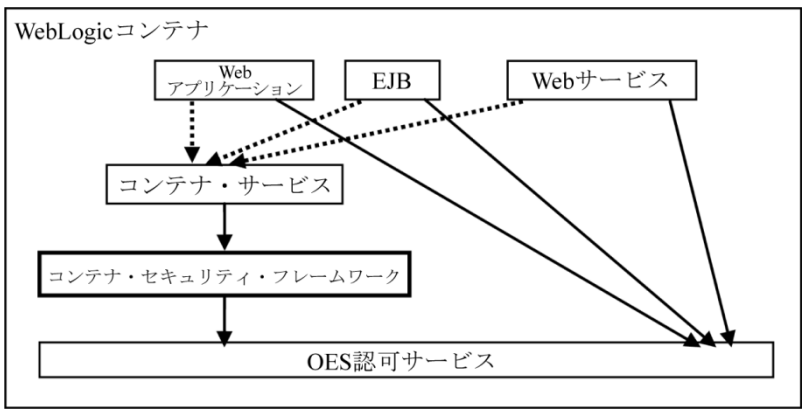


図13：コンテナ・セキュリティの認可プロバイダとしてのOracle Entitlements Server

Java SE

この数年の間に、SpringやHibernate、Apache Tomcatなどの軽量Javaテクノロジーの普及が進んできました。フットプリントが小さく柔軟性に優れたこれらのテクノロジーは、特定の種類のプロジェクトに適しています。これらのテクノロジーはそれぞれ特殊な問題領域に焦点を合わせており、たとえば、Springは制御の反転やアスペクト指向プログラミングに対応しています。しばしば、セキュリティは、その主要サービスとはまったく異なる役割を果たします。Oracle Entitlements Serverは、ABACポリシーとRBACポリシーに対する手厚いサポートを提供することで、これらのフレームワークでエンタープライズ・クラスの認可機能を実現します。

Oracle Entitlements ServerのJava SMは、Java SE環境向けに事前統合されたフォーム・ファクタです。管理APIと実行時認可APIを含むOracle Entitlements Server機能のフル・セットが含まれています。セキュリティと、特に認可は、各アプリケーションだけでなく、アプリケーションに含まれる各モジュールやオブジェクトに共通する分野横断的な課題の典型的な例です。Springアノテーションを使用することで、Oracle Entitlements Serverは、パッケージから個々のメソッドまでのすべてを保護できます。この方法では、Springメソッドを呼び出すと、自動的にOracle Entitlements Serverが呼び出されて認可が実行されます。また、Oracle Entitlements ServerをSpringの*AccessDecisionManager*プロバイダとしてネイティブ統合し、"*authz:authorize*"タグを使用してUI要素を保護することもできます。

*Hibernate*はJAASを使用して、宣言型のセキュリティを実現しています。*Hibernate*を使用しているアプリケーションは、JAASの認可プロバイダとしてOracle Entitlements Serverを使用できます。また、Oracle Entitlements ServerをHibernateのインターセプタとして使用すると、データベース内のオブジェクトに対する読取り、作成、更新、削除といった処理を制御することもできます。

サービス指向アーキテクチャ

多くの企業が、そのサービス・バックプレーンとしてサービス指向アーキテクチャ（SOA）を利用しています。SOAは、Javaや.NET、そしてレガシー・メインフレームのアプリケーション間でサービスを相互接続するために使用されています。Oracle Entitlements Serverは、個々のSOA要素やサービスを保護するだけでなく、サービスとしての認可機能を提供します。Oracle Entitlements Serverは、スケーラブルな高可用性環境の構築を支援するため、SOAデプロイメント・モデルに対する明示的なサポートを提供しています。

Oracle Enterprise Gateway、Vordel、DataPower、Layer 7などのXMLゲートウェイは、Oracle Entitlements Serverを使用して、Webサービスの認可機能を管理できます。Oracle Entitlements Serverポリシーは、ユーザーや起動したメソッド、またはメッセージ本体の情報（要求された顧客IDとSAMLアサーション、またはSOAPヘッダーとボディから取得したその他の属性など）に基づいて、個別APIの起動を認可できます。また、Oracle Entitlements Serverを使用すると、Webサービス・コードを変更することなく、Webサービス・リクエストのレスポンスに含まれる特定の情報を修正するか、または暗号化するかを決定することもできます。待機時間を短縮するために、*Oracle API Gateway*や*Vordel*などのWebサービス・ゲートウェイにOracle Entitlements Serverを直接埋め込むこともできます。サービス・バス（例：Oracle Service Bus）とともにOracle Entitlements Serverを使用すると、Webサービスを保護できます。Oracle Entitlements Serverは、SOA環境での*Oracle Service Bus*実装向けに、すぐに使用できるセキュリティ・モジュールを提供しています。Oracle Entitlements Serverは、*Oracle Web Services Manager*を使用することで、OracleのSOAおよびWebLogicインフラストラクチャに埋め込まれた*Webサービス・セキュリティ・エージェント*にABACとRBACに対する豊富な

サポートを提供します。

Oracle CoherenceやMemcachedなどのエンタープライズ・グリッドは、おもに、データのキャッシングと配信を効率的かつ確実に行う方法の提供に焦点を合わせているため、セキュリティが主要課題に含まれないことも多くあります。この場合、個別のオブジェクト・アクセスに対する認可機能が存在しないため、機密性の高い環境では問題が発生します。Oracle Entitlements Serverをセキュリティ層として使用すると、キャッシュ・リクエストをインターセプトして認可を適用できます。Oracle Entitlements Serverはそれぞれのネイティブ実装を拡張することで、Coherenceのキャッシング・サービス、名前付きキャッシュ、オブジェクト検索に対するアクセスを保護します。

Oracle Entitlements Serverは、XACML標準ベースのリクエスト/レスポンス・メカニズムを使用することで、.NETシステム（*とその他のアプリケーション*）をサポートします。これにより、任意の.NETアプリケーションからOracle Entitlements Serverに対して、認可リクエストを直接送信できます（*注：.NET環境では、ネイティブのOpenAZ APIとローカル決定キャッシング機能も提供されています*）。Oracle Entitlements Serverはコアの認可サービスを提供しており、このサービスは、アプリケーションの固有要件を満たすためにカスタマイズできます。

コンテンツ・ポータルとコンテンツ管理サーバー

Microsoft SharePointやOracle WebCenterなどのコンテンツ管理サーバーは、ドキュメントの保存、取得、共有に関して優れた機能を提供します。これらのサーバーには、多くの場合、標準でドキュメントの保護機能が含まれています。Oracle Entitlements Serverは、RBACとABACに基づく高度なモデルを使用して、これらの単純なセキュリティ・モデルを拡張します。たとえば、Oracle Entitlements Serverのポリシー制約を使用すると、"*認可レベル4を持つ従業員のみが機密ドキュメントを表示できる*"というポリシーを簡単に実装できます。Oracle Entitlements Serverは、Oracle UCMのイベント・フィルタを使用して、ドキュメント操作（読取り、更新、削除、検索など）をインターセプトします。ドキュメントのメタデータをOracle Entitlements Server属性に直接マッピングし、認可ポリシーやロール・マッピング・ポリシーで使用できます。

*Microsoft SharePoint*は、ポータルとドキュメント・リポジトリの両方の役割を果たします。Oracle Entitlements Serverは、SharePointのサイト、URL、ページ、ポートレット、Webパーツ、ページ・コンテンツ、およびドキュメントを保護するためのポリシー適用ポイント（PEP）を標準で提供しています。Oracle Entitlements ServerのHTTPモジュールはWebページを保護し、Oracle Entitlements ServerのWeb ControlはWebパーツを保護します。

さらに、Oracle Entitlements Serverは、コードの条件付き実行とカスタムUIレンダリングを可能にする、認可タグ・ライブラリ（AuthrorizationTagLib）を提供しています。

データ・セキュリティ

企業において、ほとんどのデータはデータベースから生じ、各種のサービス層を通過し、最終的にUIによってレンダリングされます。データの発生箇所でデータを保護することは、情報の漏えいを防ぐための確実な方法です。Oracle Entitlements Serverは、データ層でのOracle Virtual Private Database（Oracle VPD）ベース・フィルタの作成と、DAO（データ・アクセス・オブジェクト）層でのアクセス保護をサポートしています。

アプリケーション内のDAO層は、オブジェクトの永続性を処理する層です。オブジェクト検索からSQLへのマッピングの一部として、SQLフィルタの形でOracle Entitlements Serverポリシーを適用できます。たとえば、マネージャーが全従業員の給与を表示する問合せを実行した場合、Oracle Entitlements Serverによって、employee.manager_id = $current_userといったSQLの*Where句*が生成されます。DAO層では*アプリケーション・コンテキスト*が提供されているため、利用できるすべてのコンテキスト情報を使用して、高度な認可ポリシーを作成できます。また、特定の従業員に対して、ユーザーが実行できる処理（採用、昇進、手当ての表示など）の種類を決定するポリシーを作成することもできます。

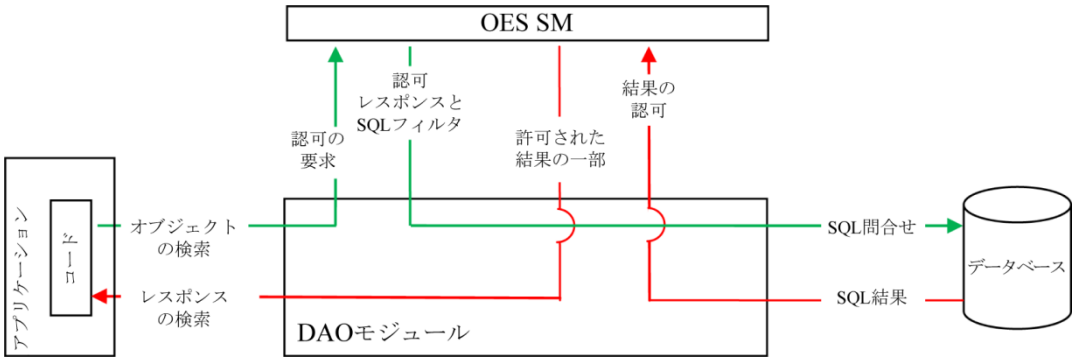


図14：ファイングレイン認可によるデータ・セキュリティ

データベースに保存された情報の機密性が極めて高く、アプリケーションに関係なく徹底的なチェックが必要とされる場合があります。たとえば、クレジットカード番号とパスワードの共有は、必要な範囲内に留める必要があります。このような状況では、データベース自体に制限を適用することが望ましい場合もあります。Oracle Entitlements ServerとともにOracle VPDを使用すると、Oracle Entitlements Server認可ポリシーに基づいて、行レベルや列レベルのフィルタリングを適用できます。このフィルタリングはデータベース内で実行されるため、どのようなアプリケーションに対してもセキュリティ・ポリシーが適用されます。このソリューションは、認可機能を外部化できないレガシー・アプリケーションに対しても有効です。

認可標準

認可標準とモデルには、複数の種類があります。それぞれの標準が、特定の種類の問題を解決するよう特殊化されています。Oracle Entitlements Serverは、幅広い業界標準をサポートすることで、顧客が最適なモデルを選択できるように努めています。これから確認していきますが、すべての標準には長所と短所があります。Oracle Entitlements Serverでは、ユーザーがそれぞれの重要な問題に応じて、好みの標準を選択できます。Oracle Entitlements Serverがサポートしている標準は、NIST RBAC、XACML、Open AZ（PEP決定API）、およびJAASです。

NIST RBAC

RBACはもっとも広く普及しているセキュリティ・モデルの1つであり、30年以上にわたって使用されています。また、各種のオペレーティング・システム、データベース、アプリケーション、ネットワーキング、Webソフトウェアに及ぶ幅広い業界のサポートを得ています。異なる製品間の相互運用性を確保するため、NISTは業界と協力して、ANSI/INCITS 359-2004標準を作成しました。NISTの刊行物である『The NIST Model for Role-Based Access Control: Towards a Unified Standard』に、この標準の概要が示されています。Oracle Entitlements Serverは、NIST RBAC Level 4をネイティブ・サポートしています。これは最高のRBACレベルであり、Flat、Hierarchical、ConstraintのRBACモデルとSymmetricモデルが含まれています。次の表に、Oracle Entitlements Serverポリシー構成メンバーからNIST RBAC仕様へのマッピングを示します。

レベル	Name（名前）	NIST要件	Oracle Entitlements Server機能
1	Flat	ユーザーは、ロールを介して権限を獲得できる	Oracle Entitlements Serverの認可ポリシーを使用すると、ユーザーは付与されたロールに基づいて権限を獲得できます。
		多対多のユーザー対ロール割当て	Oracle Entitlements Serverのロール・マッピング・ポリシーを使用すると、一連のユーザーに対していくつでもロールを割り当てることができます。
		多対多の権限対ロール割当て	Oracle Entitlements Serverの認可ポリシーを使用すると、一連の権限に対して、いくつでもロールを割り当てることができます。
		ユーザー対ロール割当てのレビュー	Oracle Entitlements Server管理コンソールまたは管理APIを使用すると、ユーザー対ロール割当てをレビューできます。
		ユーザーは、複数ロールの権限を同時に使用できる	Oracle Entitlements Serverの認可ポリシーを使用すると、複数のロールを使用して権限を獲得できます。たとえば、権限Xを取得するためには、ロールAとロールBの両方が必要です。
2	Hierarchial	任意階層のサポート	Oracle Entitlements Serverは、ロール階層を標準サポートしており、ロールの継承を実現します。また、汎用階層（標準ツリーと逆引きツリーの両方）をサポートしており、最上位ロールや最下位ロールに対する制限はありません。
3	Constrained	任意階層に対する職務の分離（SOD）のサポート	Oracle Entitlements Serverの動的ロール・マッピング・ポリシーを使用し、矛盾するロールを拒否することで、SODが実現されます。また、付与されたロールを検査する認可ポリシーでもSODがチェックされます。

4	Symmetric	制限付き任意階層に対する権限対ロール・レビューのサポート	Oracle Entitlements Server管理コンソールまたは管理APIを使用すると、ユーザー対ロール割当てをレビューできます。

XACML

XACMLは、ABACをベースにした標準です。最新バージョンの仕様は、Oasis XACML Technical Committeeホームページで確認できます。現在、XACML 3.0が計画の段階にあります。

次の図は、XACML 3.0仕様のセクション3.1、データ・フロー・モデルに基づいたものであり、Oracle Entitlements Serverのメッセージ・フローが、どのようにXACML仕様に準拠しているかを示しています。Oracle Entitlements Serverでは、管理コンソールとSMの両方がポリシー管理ポイント（PAP）の役割を果たしており、使用するプロビジョニング・モデルを決定するのは、ユーザーです。残りのXACMLコンポーネントは、Oracle Entitlements Server SMに含まれます。最初に、PAPを使用してポリシーが作成され、プロビジョニングされます（ステップ1）。クライアントが保護されたリソースにアクセスしようとすると（ステップ2）、ポリシー適用ポイント（PEP）がOracle Entitlements Server APIを使用して認可リクエストを送信します（ステップ3）。必要に応じて、外部リソース名からOracle Entitlements Serverリソースへの形式変換が実行されます（ステップ4）。PDPが決定リクエストを受け取ります（ステップ5）。必要に応じて別の属性に対する問合せを実行します（ステップ6および7）。ステップ8で、関連するポリシー情報ポイントからデータがフェッチされます。ステップ9および10で、ポリシー決定ポイントにレスポンスが送り返されます。PDPは認可決定を計算し、PEPにレスポンスを送信します（ステップ11および12）。必要に応じて、PEPは、返されたオブリゲーションを実行します（ステップ13）。

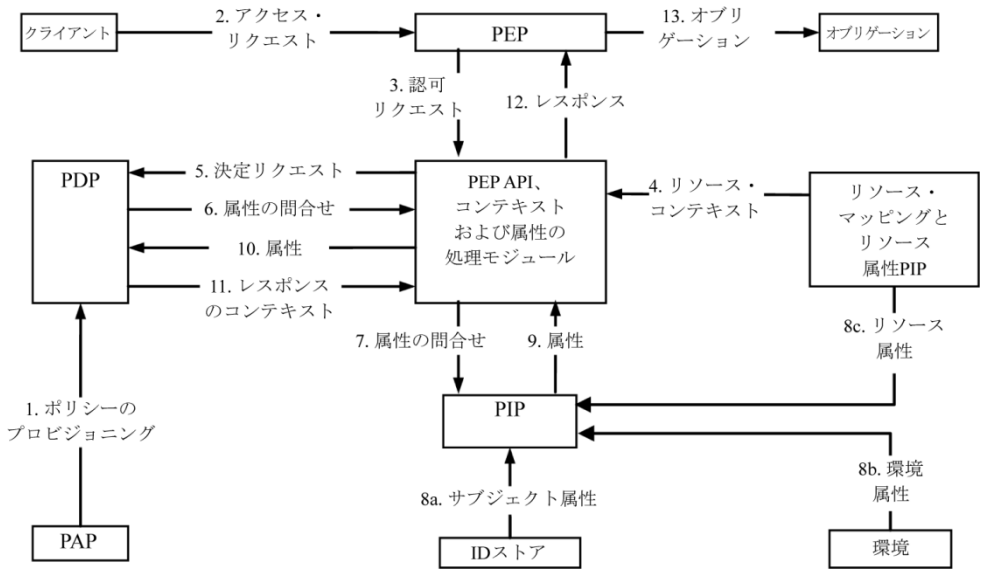


図15：XACMLのフロー・ダイアグラム

XACMLのリクエスト/レスポンス仕様は、SOAPベースのプロトコルに基づいているため、各種の認可サービスとの統合に役立ちます。この仕様によって、PEPとPDP間のメッセージ交換形式が標準化されます。このため、PDPとエンドユーザー・アプリケーションおよびサービスを別々に開発できます。Oracle Entitlements Serverは、XACML 2.0のリクエスト/レスポンス標準とアーキテクチャ・モデルを完全サポートしています。また、XACML 3.0の機能とデータ型をサポートします。Oracle Entitlements Serverは、OASIS XACML 3.0 InterOp（*RSA Conference 2012*）のすべての段階を問題なく完了しています。

注：Oracle Entitlements Server認可エンジン（PDP）は、アプリケーションに組み込むか、またはネットワーク内で一元的にホストできます。多くの場合、組込みアプローチは、従来のXACMLリクエスト/レスポンス・アプローチよりも高いパフォーマンスを提供します。

OpenAZ PEP決定API

XACML仕様では、高水準のプログラミング言語を使用して、アプリケーションやミドルウェアからPEPで認可サービスを起動する方法が定義されていません。このため、OpenAZプロジェクトは、ネイティブ言語バインディングを含む、2つのAPIセットを定義しました。それらは、次のコンポーネントです。AzApiは、XACML認可リクエストとレスポンスの抽象化モデルに基づいており、PEP APIは、Javaオブジェクトに基づいて高水準の抽象化を提供します（*注：Oracle Entitlements Serverは.NETアプリケーション向けに、ネイティブC#ベースのPEP APIも提供します*）。このAPIによって、アプリケーションやミドルウェアの開発者が、認可サービスに要求された低水準の表現への変換を行う必要がなくなります。たとえば、適切なマッパーと適切に設計されたポリシーがあれば、アプリケーションはポリシー決定に対する入力として、Javaビジネス・オブジェクト（カルテなど）を直接提供できます。このオブジェクトは、認可システムによって要求されたネイティブ表現にマッピングされます。

OpenAZのPEP決定APIは、Oracle Entitlements Serverに対するデフォルトの実行時認可APIです。アプリケーションでベンダーの独自仕様のAPIを使用する代わりに、標準のPEP決定APIをもとに構築できます。これにより、新しいアプリケーションやサービスに対する長期的投資が保護されます。

Java Authentication And Authorization Service

Java Authentication and Authorization Service（*JAAS*）標準は、コアJava仕様の一部です。この標準では、Javaアプリケーションが認証サービスと認可サービスを使用する方法が定義されています。JAASの認可では、ポリシーをモデル化するためにリソースとプリンシパルを中心としたビューが使用されます。*JAASポリシー*は、*プリンシパル*、*権限タイプ*、*権限名*、*アクション*で構成されています。このモデルのおもな利点は、Java SEおよびJava EEと事前に統合されている点です。JAAS標準に準拠したアプリケーションは、異なるJDKやJava EEサーバーへの移行時に何ら変更を加える必要はありません。

Oracle Entitlements Serverは、Java SEアプリケーションとJava EEコンテナの両方に対して、*Java2のJAASセキュリティ・プロバイダ*（PDP）として使用できます。つまり、Oracle Entitlements Server認可ポリシーは、EJBなどの高水準サービスからローカル・ハード・ディスク上のファイル読取りといった低水準操作までのすべてを保護します。またOracle Entitlements Serverは、RBACとABACのポリシー・モデルに対するきめ細かいサポートをJAASに提供します。たとえば、Oracle Entitlements Serverでは、"ユーザーの認可レベルがファイルに必要な認可レベルを上回る場合のみ、ユーザーまたは特定のコードはファイルを読み取ることができる"というポリシーをサポートしています。このポリシーを評価するため、Oracle Entitlements Serverは、ID属性である"User Clearance Level"をLDAPから、またファイル属性である"File Clearance Level"を外部データソース（データベースなど）からフェッチし、これら2つの値を比較する必要があります。Java仮想マシン（JVM）によってこれらの決定が透過的に適用されるため、アプリケーション側で基盤となるセキュリティ・メカニズムを意識する必要はありません。

その他のID管理ソフトウェアとの統合

Oracle Entitlements Serverは、オープン標準を利用することで、オラクルやサード・パーティのID管理製品に対する容易な相互運用性を実現しています。オラクルのID管理スタックは、エンド・ツー・エンドのID管理ユースケースのあらゆる領域に対応しています。このため、顧客は、多用なユースケースに対応した事前統合ソリューションをそのまま実装できます。

a) *IDストアと仮想ディレクトリ：*Oracle Entitlements Serverは、LDAP v2/v3標準を使用しています。また、Oracle Internet Directory、Oracle Virtual Directory、Oracle Unified Directory、Oracle Directory Server Enterprise Edition、Sun Java System Directory Server（SJSDS）、Tivoli DS、Active Directory（AD）、Active Directory Application Mode（ADAM）、eDirectory、OpenLDAPに対して認定されています。

b) *IDとロールのプロビジョニング：*Oracle Entitlements Serverは、LDAPディレクトリやデータベースから、ID属性やロールを直接フェッチできます。Oracle Entitlements Server管理APIをその他のプロビジョニング・ソリューションに統合して、エンタイトルメントを自動的に作成することもできます。

c) *認証とSSO：*認可製品であるOracle Entitlements Serverは、その他の認証製品や連携製品、およびSSO製品に対する容易な統合を実現するための機能をいくつか提供しています。認証されたユーザーIDは、次の方法で受け渡されます。

   a. *JAAS Subject*：これは、認証されたサブジェクトを共有するためのJava標準です。ユーザーが認証されると、JAAS SubjectがOracle Entitlements Serverに渡され、認可が実行されます。

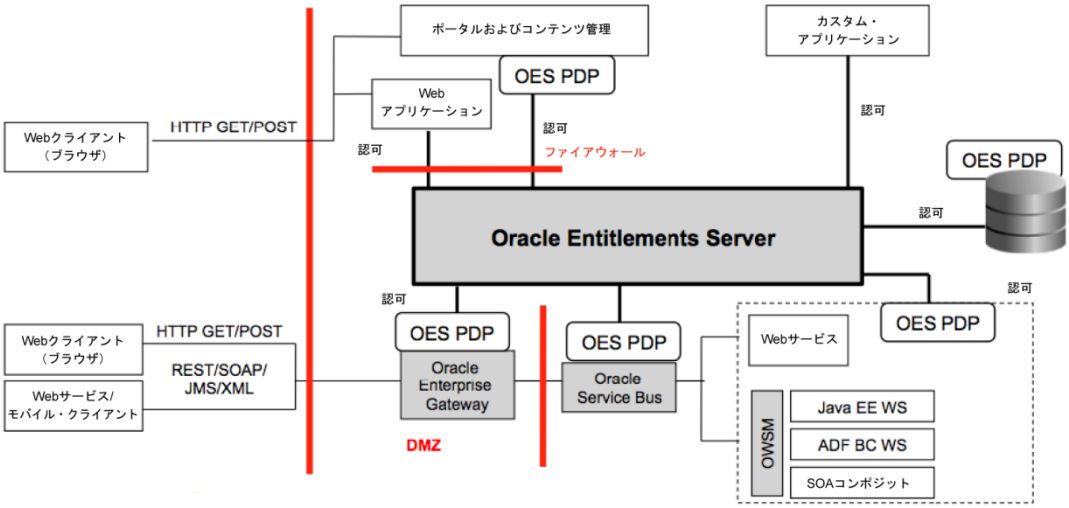
   b. *コンテナ生成のサブジェクト：*Java EEコンテナで実行されている場合、Oracle Entitlements Serverは、対応するコンテナ・ベースのサブジェクト（WebLogicやWebSphereのサブジェクトなど）をサポートします。これによって、コンテナ・セキュリティ・フレームワークとの相互運用性が簡単に実現されます。

   c. *ユーザー名：*必要に応じて、ユーザー名とエンタープライズ・ロールをアプリケーションから直接渡すことができます。

d) *連携、STS、クレーム*：アプリケーションは、コンテキスト属性に適切なクレームを挿入できます。また、Oracle Entitlements Serverは、認可ポリシーの評価中に、必要なクレームをSTSからフェッチできます。

エンタープライズ・アプリケーション向けのリアルタイム認可

Oracle Entitlements Serverは、ミッション・クリティカルなアプリケーションで、極めて短いレスポンスタイムを実現します。また、スケーリングすることで、大量の機密リソース、ユーザー、ロール、認可決定を処理できるように設計されています。Oracle Entitlements Serverは、Oracleベースと非Oracleベースのプラットフォームおよびソリューションを含むミッション・クリティカルな実装で使用されています。Oracle Entitlements Serverはオラクルの戦略的認可エンジンであり、Oracle Fusion Applicationsなどの製品と、Oracle Fusion Middlewareテクノロジー（Oracle SOA Suite、Oracle WebCenter Portal、Oracle WebCenter Spaces、Oracle Application Development Framework、Oracle Identity and Access Management.など）に組み込まれています。



上図に示したとおり、Oracle Entitlements Serverは、Oracle環境だけでなく異種環境での幅広いシナリオにファイングレイン認可を提供します。

結論

アプリケーション・コードに認可決定機能を組み込むと、脆弱で静的なポリシーの原因となり、変わり続けるセキュリティ要件に対応できない結果になります。一元化されたポリシー管理や統一された適用インフラストラクチャが利用できない場合、アプリケーションごとに異なるセキュリティ・メカニズムを使用したセキュリティ・サイロが生まれ、作成された認可ポリシーは組織間で再利用できません。このようなシステムは、時が経つと複雑になって管理が難しくなり、保守の費用もかさみます。先見性に欠け、監査機能が不十分なシステムは、コンプライアンスとセキュリティに関する悪夢をもたらします。標準ベースのCOTS（商用既製品）認可ソリューションを使用すると、異なる組織間でどのようにセキュリティが管理されるかについての制御能力を取り戻すことができます。セキュリティ要件から認可ポリシーへのマッピングは、簡単に実行できます。一元化された

ポリシー管理を自動化されたプロビジョニングと組み合わせると、すべてのアプリケーションとサービスに対して企業全体で一様にセキュリティ・ポリシーを適用できます。

認可サービスとしてのOracle Entitlements Serverは、開発者や管理者がビジネス・ユーザー・フレンドリーな方法でポリシーを管理しながら、実行時のオーバーヘッドを最小限に抑えて、厳格な規制要件やビジネス要件、そしてセキュリティ要件に対応できるように設計されています。この製品は、オラクルの戦略的な認可エンジンであるため、複数のオラクル製品に組み込まれています。Oracle Entitlements Serverは、その基盤として標準を使用することで、可用性とスケーラビリティに優れ、外部化された認可管理ソリューションを、アプリケーションやミドルウェア、およびデータベース向けの高度なポリシー・モデルとともに提供します。エンタイトルメントの一元管理を推進するOracle Entitlements Serverは、企業内のアプリケーションに関するアクセス権を示す中央ビューを提供するとともに、レポーティング・ツールや分析ツールで使用できる監査レコードを生成します。市場やセキュリティ、規制、およびビジネスの要件が変わっても、ポリシーは素早く対応できるため、Oracle Entitlements Serverは、ファイングレイン認可を実現する共有サービスを提供して、迅速なコンプライアンスと優れたビジネス俊敏性を実現します。Oracle Entitlements Serverは、最先端の業界標準や機能をサポートするだけでなく、何十年にもわたって堅牢な認可ソリューションを構築してきた経験を生かして、クリティカルなアプリケーションやサービスの保護に貢献します。

Oracle Entitlements Server
2012年7月
著者：Sid（Oracle Identity Mgt）

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

海外からのお問い合わせ窓口：
電話：+1.650.506.7000
ファクシミリ：+1.650.506.7200
www.oracle.com

Oracle is committed to developing practices and products that help protect the environment

Hardware and Software, Engineered to Work Together