

アイデンティティマネージメント



16 April 2007

株式会社アルデイト

ID管理の必要性

何故ID管理が求められているのか

■ 求められるコンプライアンスへの対応

● 法整備状況

- J-SOX法関連の整備・・・2008年3月
- 個人情報保護法・・・2005年4月
- 情報基盤強化税制・・・2006年4月～二年間 など

コンプライアンスにおいては、組織がどんな法令、規則に従わなければならないかは関係なく、下記の質問に回答できる必要がある

- ・誰が、何に、いつ、アクセスしたか？
- ・誰が、そのアクセスを認めたか？
- ・アクセスを付与し、削除する管理ポリシーは何か？
- ・これらのポリシーの適用/実施方法は文書化されているか？
- ・マネージメントの主張をサポートするどんな証拠が存在するか？

US-SOX法関連で
指摘される
ITインフラ欠陥

- ◆ 特定できない、もしくは解決できない職務分掌
- ◆ 過度のアクセス特権が本番システムに存在する
- ◆ 非保護OS上で会計APLやポータルが稼動
- ◆ アカウント付与、確認、削除プロセスが不完全
- ◆ 非保護DB上での会計APL稼動
- ◆ プログラム、テーブル、インターフェースがセキュアでない
- ◆ 開発者による本番システムへのアクセス

★ID管理を導入した上で留意すべきポイント【例】

- ◆ ID、パスワードは適切に管理
- ◆ 業務上不要な権限を付与しない
- ◆ ID、権限の付与ワークフローの可視化
- ◆ 退職者などの不要IDの削除
- ◆ 職務分掌に従って相互に権限を限定
- ◆ ID、権限の付与のログ取得

■ 続出する情報漏洩事件を防ぐ

- ◆ 簡単に「なりすまし」ができる環境、「誰か良くわからない」環境では、セキュリティ対策が実効性を失う可能性がある
- ◆ 職務分掌、個人情報保護ポリシー、集約された監査が必要

ID管理と認証基盤の確立はセキュリティのベースとなる

■ 肥大化するID管理コストの削減

- ◆ SSO、パスワードリセット、管理委譲、ユーザ・セルフサービスプロビジョニングが人による運用がなされており、コストが膨大

● 簡略化されたID管理の効果

- ◆ IDの作成: 5day → 20minutes
- ◆ IDの削除: 1week → 1minutes

大規模、運用期間が長いほど、コスト削減効果がUP

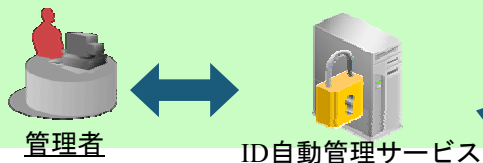
Oracle社のアイデンティティマネージメント製品群

必要な要素を網羅的に

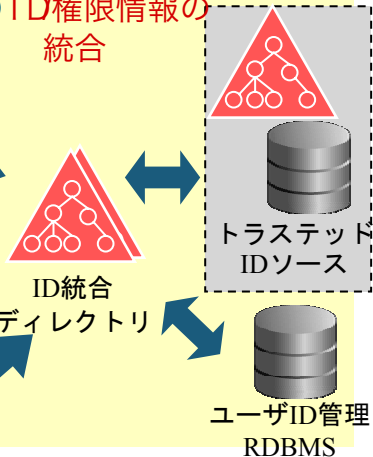
■ Oracle Identity And Access Management Suites

Oracle社のID管理ソリューション「Oracle Identity And Access Management Suites」は、ID管理に必要な要素を網羅的に備えています。

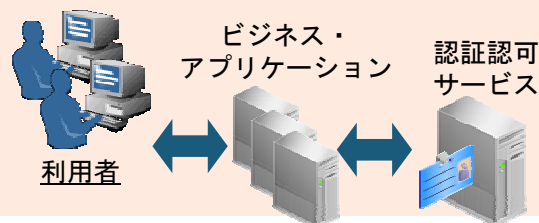
◆ ① ID管理プロセスの統合



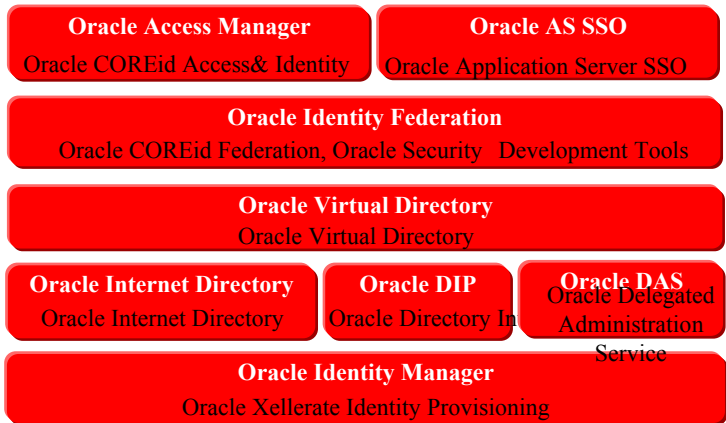
◆ ② ID権限情報の統合



◆ ③ アクセス管理の統合



◆ Oracle Identity And Access Management Suites コンポーネント



■ ID管理プロセスの統合

ディレクトリやユーザID管理RDBMSによって一元的に管理されたIDリポジトリから管理対象のアプリケーションにIDやその属性権限をプロビジョニングします。

■ ID権限情報の統合

分散されて管理されているID情報を統合し、一元管理します。

■ アクセス管理の統合

シングルサインオン環境を提供し、アクセスコントロールの実行、ユーザのグループ管理や権限マッピングなどを実施します。

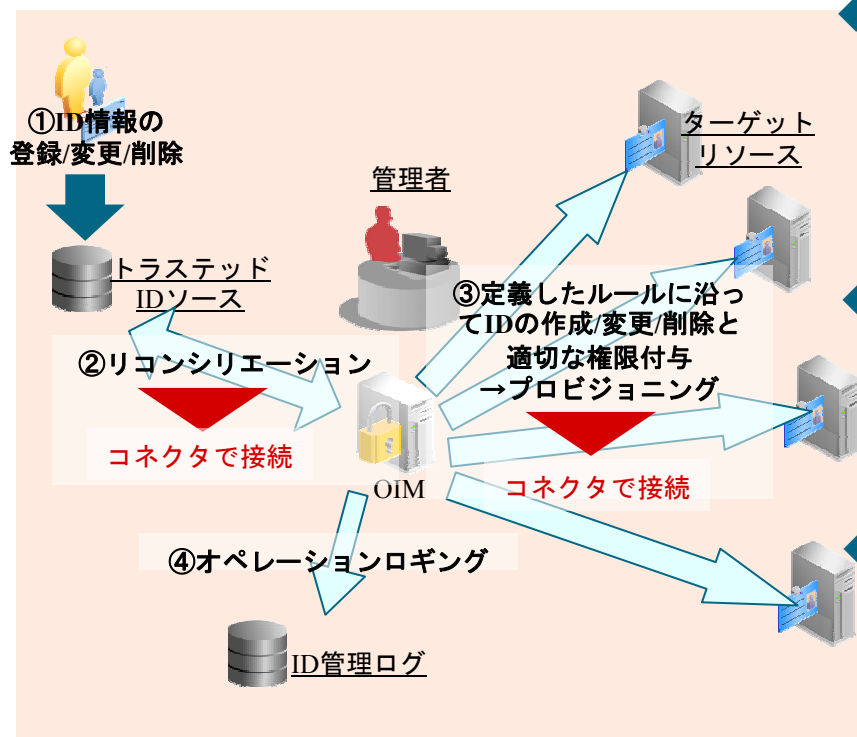
POINT

- ◆ コンプライアンスと個人情報保護を強化します
- ◆ 管理コストを削減します
- ◆ セキュリティを改善します
- ◆ ユーザの使用感を改善します

Oracle Identity Managerで実現できること

ID管理プロセスの統合

■ ID管理業務プロセスの自動化・一元化・可視化



◆ ID情報のライフサイクルを管理

日々追加/変更/削除が行われるターゲットリソースへのID情報をOIMを用いて一元管理することができます。ID管理の業務プロセス（申請・承認 etc.）も合わせて管理できます。OIMは、ユーザーフォーム、アダプター、コネクタ、ルール、・・・といった承認ワークフローの端から端までをコンフィギュレーションで設定することをコンセプトとした、プロビジョニング フレームワークです。

◆ コンプライアンスに対応したレポーティング

OIMではユーザのIDが作成されてから現時点までの全てのイベントを記録しています。ゆえに、「6ヶ月前は誰が何に触ることができたのか」という内部監査にも対応できます。例として、下記のレポーティングが可能です。
リソースアクセスリスト/ポリシーリスト/権限のサマリー etc.

◆ アダプタファクトリでコネクタ開発

Identity Management製品は、予め用意されたアダプタでは接続できない場面に行き当たるはずですが、OIMはこの開発工数を最小化するための Adapter Factoryという仕組みを提供しています。OIMのアダプタは小さな部品の集合体です。これを組み合わせることにより新たなアダプタの雛形をJavaで作成し、コーディングは少量で済むようになっています。

POINT

◆ Oracle Identity Managerには、対象アプリケーションが600を数え、ユーザ数は25000人、管理アカウント数は400,000という超大規模の事例があります。これはOIMのスケールビリティの証明に他なりません。