

ORACLE DATABASE VAULT

主な利点



- 特権ユーザーによる機密アプリケーション・データへのアクセスの防止
- 柔軟なセキュリティ制御による、アプリケーション、データベース、およびデータへのアクセス制御
- 職務の分離における有効化
- Oracle Database 10g Release 2、Oracle Database 11g Release 1 で使用可能
- Oracle - PeopleSoft アプリケーションによる検証



Oracle Database Vault は、規制順守およびインサイダーの脅威に対する保護のための強力な内部制御を提供します。Oracle Database Vault は、特権ユーザーが機密アプリケーション・データを参照するのを防止するだけでなく、アプリケーション、データベース、データにアクセスできる人物、時間、場所、および方法にポリシーを適用します。Oracle Database Vault は、既存のアプリケーションを変更することなく、データベース・アプリケーションを透過的に保護します。

Oracle Database Vault

サーベンス・オクスリー (SOX) 法、クレジットカード業界 (PCI) のデータ・セキュリティ・スタンダード、医療保険の相互運用性と責任に関する法律 (HIPAA) などの規制において、財務、医療、クレジットカード記録などの機密情報を不正なアクセスや変更から保護するために、厳密な内部制御が求められています。

Oracle Database Vault は、強力で使いやすいセキュリティ・ソリューションを Oracle Database 内で提供します。これにより、企業は新規および既存のアプリケーションを使用しながら、現行および今後の規制を順守できます。また、世界中でインサイダーの脅威に対する懸念が増加しています。CSI/FBI 2005 Computer Crime and Security の調査によると、情報システムに関するデータの損失や攻撃の 70% 以上は、インサイ

ダーによって実行されています。インサイダーとは、システムやデータに対して、少なくともある程度のアクセスを認可された人物です。

規制の順守およびインサイダーの脅威に対する保護に

おいて、既存の環境に対する次の 2 つの主要な拡張機能が求められています。

- 特権ユーザーによる機密データへの不正なアクセスを制限するための予防的制御
- アプリケーション、データベース、データにアクセスできる人物、時間、場所および方法における、柔軟で適応性のある制御

Oracle Database Vault のレルム、ファクタ、およびルール (以下に説明) は、データベース内で連携し、日常のデータベース管理を妨げることなく、最も強力なユーザーからもアクセスを制限します。これらの機能の使用方法は柔軟性と適応性に富んでおり、既存のアプリケーションを変更することなくセキュリティ要件を適用できます。

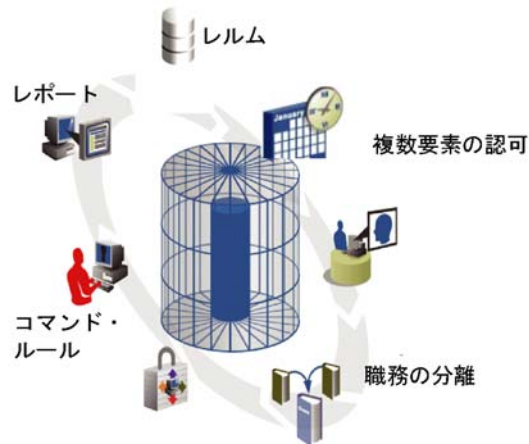


図 1 : Oracle Database Vault の概要

Oracle Audit Vault

関連製品：

- Oracle Audit Vault
 - 複数のデータベースからの監査データの透過的な統合
 - 組み込みレポートによるコンプライアンス・レポートの簡素化
 - アラートによる脅威の早期検出
 - データベース上の監査ポリシーの管理
 - 堅牢な Oracle Database テクノロジーによる拡張
 - オープンなウェアハウス・スキーマに対するカスタム・レポートの構築
- Oracle Advanced Security
 - アプリケーションの SQL コードに変更を加えることなく、透過的にデータを暗号化
 - AES 256 のサポート
 - 厳密認証
 - ネットワークの暗号化
- Oracle Label Security
 - ラベル・ベースのアクセス制御
 - マルチレベルのセキュリティ
 - 機密データの保護
 - ラベル要素による Oracle Database Vault との統合
 - 情報セキュリティにおける国際評価基準 (Common Criteria) EAL4 の評価
- Oracle Secure Backup
 - テープのバックアップ時のデータベースおよびファイル・システム・データの暗号化
- Oracle Recovery Manager (RMAN) との統合および 256 ビット AES までのサポート

特権ユーザーの制御

IT 管理者、データベース管理者、およびアプリケーション管理者は、企業内で非常に信頼されるポジションにあります。ただし、規制順守、アウトソーシング、アプリケーションの統合、およびインサイダーの脅威に対する懸念の増加により、機密性の高いアプリケーション・データへのアクセスに対して、強力な制御が必要になっています。

既存のアプリケーション・コードを修正してアクセス制御を改良するのは、時間やコストがかかり、ほとんどの企業にとって現実的な方法とは言えません。Oracle Database Vault のレールを使用すると、企業は DBA を含む強力な特権ユーザーのアプリケーション・データへの

アクセスを制限できます。レールは簡単に定義でき、アプリケーション全体または一連の表の周囲に容易かつ迅速に設置できます。

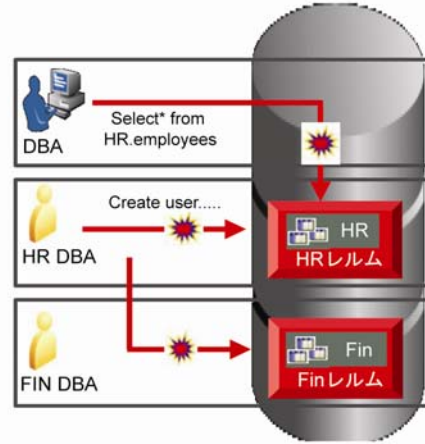


図 2：Oracle Database Vault のレール、ルール、およびファクタ

柔軟性および適応性

Oracle Database Vault のルールおよびファクタを使用すると、いつ、どこで、誰が、どのようにデータベース、データ、およびアプリケーションにアクセスできるかを制限し、アプリケーション・セキュリティを大幅に強化できます。IP アドレスや認証方式などの複数のファクタの使用方法は柔軟性と適応性に富んでおり、既存のアプリケーションを変更することなく認可要件を適用できます。たとえば、データベースへのアクセスを特定の中間層へ限定できます。また、すべての SQL コマンドにコマンド・ルールを定義し、追加の制御を提供できます。

職務の分離

Oracle Database Vault は、職務の分散を制御する強力な機能を提供し、データベースが不正に変更されることを防止します。Oracle Database Vault は、セキュリティ管理、アカウント管理、およびリソース管理に対し、3つの異なる役割を標準で提供します。たとえば、Oracle Database Vault を利用すると、*create user* 権限を持つ DBA であっても適切な役割を持たない場合は、新しいユーザーを作成することはできません。さらに、リソース管理の役割を、バックアップ、パフォーマンス、およびパッチ適用の役割に分類できます。また、任意で役割を統合できます。

アプリケーションの検証

オラクルでは、PeopleSoft アプリケーションを用いて Oracle Database Vault を検証しています。使いやすいセットアップ・スクリプトと手順は、Oracle Technology Network (英語) からダウンロードできます。Oracle E-Business Suite および Siebel による検証は現在進行中であり、年内に完了する予定です。

Copyright 2007, Oracle. All Rights Reserved.

本文書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。本文書は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。オラクル社は本文書に関するいかなる法的責任も明確に否認し、本文書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。本文書はオラクル社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。

Oracle は米国 Oracle Corporation およびその子会社、関連会社の登録商標です。その他の名称はそれぞれの会社の商標です。