

Oracle Database Vault

Oracle ホワイト・ペーパー
2007 年6 月

はじめに

規制順守のための内部統制の強化、業界のベスト・プラクティスの適用、インサイダーの脅威からの保護、これらは今日のグローバル経済において組織が直面する課題のほんの一部にすぎません。インサイダーの脅威などの問題は目新しいものではありませんが、機密情報に対する不正アクセスへの懸念はかつてないほどに高まっています。『CSI/FBI 2005 Computer Crime and Security』によると、70%以上の情報システム・データの損失および攻撃は、インサイダー（つまり、システムとそのデータへの一定レベルのアクセスを認可された内部関係者）により実行されています。インサイダーによるセキュリティ違反は、企業の外部からの攻撃よりも多額の損失を招く場合があります。データの盗難によるコストは、財務的観点から見ても、広報的観点から見ても膨大なものになります。同時に、グローバル経済で競争力を維持するため、コスト効率に優れた方法で IT システムを配置する柔軟性を確保しながら、PCI、サーベンス・オクスリー（SOX）法、Basel II などの業界のベスト・プラクティスおよび規制を順守しなければなりません。

既存のアプリケーションや IT 運用を、既存の規制や新たな規制と業界のベスト・プラクティスに準拠させるには、透過的なセキュリティ制御が不可欠です。しかし、既存アプリケーションの変更は時間とコストのかかる作業です。したがって、既存アプリケーションを変更せずに透過的な保護を実現する新しいセキュリティ製品が必要になります。

Oracle Database Vault

データベース、アプリケーション、およびデータへのアクセスを制御するには、データベース内で適用される高度なアクセス制御機能が必要になります。Oracle Database Vault は、ビジネス・データを保護するための業界有数のソリューションです。従来のクライアント・サーバー・アプリケーションから Web ベースのアプリケーションまで、Oracle Database Vault は、アプリケーションを変更することなく、柔軟性と透過性に優れ、高度な適応性を備えたセキュリティ制御機能を提供します。Oracle Database Vault は、先ごろ、Info Security Products Guide 誌の 2007 Global Excellence in Database Security Award を受賞しました。

過去数十年間にわたって、何千ものアプリケーションが開発されてきました。これらのアプリケーションには、HR や財務処理の分野で幅広く使用されているものもありますが、ほとんどは業界固有のビジネス課題に対応するように設計されたカスタム・アプリケーションです。現在、多くのアプリケーション環境には高い権限を持つユーザー（特権ユーザー）がいます。今日の規制やベスト・プラクティスでは、特権ユーザーが、市販のレポート作成ツールを使用してデータにアクセスすることを防止する強力な制御機能が求められています。Oracle Database Vault

は、特権ユーザーの制御機能とカスタム・セキュリティ・ポリシーを使用して、これらの課題に対応するよう設計されています。Oracle Database Vault は、Oracle Database 10g Release 2、および Oracle Database 11g Release 1 で使用できます。また、Oracle PeopleSoft アプリケーションで検証済みです。Oracle E-Business Suite および Siebel を含むその他のアプリケーションでの検証は、現在実施中です。



特権ユーザーの制御

レールム

- 特権ユーザーによるアプリケーション・データへのアクセスの防止

職務の分離

- データベース内の管理アクションの制御による、規制やベスト・プラクティスに違反する行為の防止

レポート

- レールムやその他の Oracle Database Vault の実施アクションに関するセキュリティ・レポートの実行

柔軟性と適応性に優れたカスタム・セキュリティ・ポリシー

複数ファクタ認可

- 信頼パスの作成により、誰が、いつ、どこで、どのように、アプリケーション、データおよびデータベースにアクセスするかを定義

コマンド・ルール

- IT セキュリティと内部または外部の監査者による推奨に基づいた運用ポリシーの実施

図1. Oracle Database Vault 概要

Oracle Database Vault と規制

Oracle Database Vault のレールム、職務の分離、コマンド・ルール、およびファクタを利用すると、各国の規制における特定の条項に関連するリスクを全体的に軽減できます。SOX 法、医療保険の相互運用性と説明責任に関する法律 (HIPAA)、Basel II、PCI などの規制に含まれるテーマは共通しており、内部統制、職務の分離、機密情報に対する強力なアクセス制御が含まれます。実際、SOX 法や HIPAA などの規制に見られる要件の多くは手続き上の要件ですが、未承認のデータ変更やアクセスなどに付随するリスクを軽減するには、技術的なソリューションが必要になります。

Oracle Database Vault (DBV) と規制		
規制	要件	DBV により リスクが 軽減される
SOX 法第 302 条	未承認のデータ変更	はい
SOX 法第 404 条	データの改ざん、 未承認アクセス	はい
SOX 法第 409 条	DoS、 未承認アクセス	はい
グラム・リーチ・プライリー法	未承認のアクセス、 改ざん、開示	はい
HIPAA 164.306	未承認のデータ・アクセス	はい
HIPAA 164.312	未承認のデータ・アクセス	はい
Basel II - 内部リスク 管理	未承認のデータ・アクセス	はい
CFR Part 11	未承認のデータ・アクセス	はい
日本の個人情報保護法	未承認のデータ・アクセス	はい
PCI - 要件 7	ビジネス上の必要性に応じた、カード 所持者データへのアクセス制限	はい
PCI - 要件 8.5.6	ベンダーが使用するリモート・メン テナンス用アカウントに対する必要 時のみの有効化	はい
PCI - 要件 3.4 の 補助制御	以下の条件に基づいて、カード所持 者データまたはデータベースへのア クセスを制限する機能の提供 ・ IP アドレス/MAC アドレス ・ アプリケーション/サービス ・ ユーザー・アカウント/グループ	はい
PCI - 要件 A.1 : ホスティング・ プロバイダによるカード所持者 データ環境の保護	カード所持者が自身の データ環境にのみアクセス するような制御	はい

表 1. Oracle Database Vault と規制の概要

特権ユーザーの制御

データベース管理者やその他の特権ユーザーは、データベース・メンテナンスにおいて重要な役割を果たします。バックアップとリカバリ、パフォーマンス・チューニング、そして高可用性の実現は、すべて DBA の職務の一環です。しかし、特権ユーザーがデータベースからアプリケーションの機密データを参照できないようにすることが、ますます重要な要件になってきています。さらに、アプリケーション統合により、財務アプリケーションや人事アプリケーションなどに含まれる機密性の高いビジネス・データ間での明確な境界が必要とされています。

Oracle Database Vault のレールム

Oracle Database Vault のレールムは、DBA、アプリケーション所有者、およびその他の特権ユーザーによる、高い権限を利用したアプリケーション・データの参照を防止します。Oracle Database Vault のレールムは予防制御機能を導入することにより、データ侵害が発生した場合の潜在的な影響を緩和するとともに、DBA がより効率

的に作業を実行できるようにします。Oracle Database Vault のレلمを使用すると、アプリケーション全体を保護することも、アプリケーション内の特定の表を保護することもできるため、柔軟性と適応性に富んだセキュリティが実現できます。

Oracle Database Vault の職務の分離

Oracle Database Vault の職務の分離機能は、体系的なセキュリティ・アプローチを使用して、データベースの内部統制を強化します。Oracle Database Vault では、標準で3つの異なるレスポンスビリティがデータベース内に作成されています。

レスポンスビリティ	説明
アカウント管理	アカウント管理のレスポンスビリティを持つユーザーは、データベース・ユーザーの作成、削除、変更を行えます。既存の特権ユーザーは、アカウント管理活動を実行することはできません。
セキュリティ管理	セキュリティ管理のレスポンスビリティを持つユーザーは、データベースのセキュリティ管理者（Oracle Database Vault の所有者）になります。セキュリティ管理者は、Oracle Database Vault のレلمやコマンド・ルールの設定、これらを使用するユーザーの認可、および Oracle Database Vault 固有の各種セキュリティ・レポートの実行を行えます。セキュリティ管理者は、保護されたビジネス・データに対する自身のアクセスを認可することはできません。
リソース管理	リソース管理のレスポンスビリティを付与されると、DBA 権限を持つユーザーは、バックアップとリカバリ、パッチ適用、パフォーマンス・チューニングなどの、データベースに関連する通常の管理作業とメンテナンス作業を引き続き実行できます。

表2. Oracle Database Vault の職務の分離

Oracle Database Vault の拡張性を利用することで、独自のビジネス要件に合わせて職務の分離機能をカスタマイズできます。たとえば、リソース管理レスポンスビリティをさらに分割し、バックアップ、パフォーマンス、パッチ適用というレスポンスビリティを作成できます。小規模の企業でレスポンスビリティを統合することや、各レスポンスビリティに別々のログイン・アカウントを割り当てることで、よりきめ細かいアカウントビリティと監査を実現します。

Oracle Database Vault は、標準で多数のレポートを提供しており、レلمにより阻止されたデータ・アクセス・リクエストなどに関するレポートを作成できます。

たとえば、レールムによって保護されたアプリケーション表のデータに DBA がアクセスしようとした場合、Oracle Database Vault 内部の特別に保護された表に監査レコードが作成されます。Oracle Database Vault に含まれるレールム違反レポートを使用すると、これらの監査レコードを簡単に表示できます。

柔軟性と拡張性に優れたアクセス制御

規制とプライバシー法が世界中で急増するにしたがって、既存のアクセス制御要件や新たに生じるアクセス制御要件に合わせて容易に変更できる、柔軟性と適応性に富んだセキュリティ・ポリシーが必要になってきました。アクセス制御要件をさらに複雑にするのは、アプリケーションのアウトソーシングやホスティング、またはオンデマンド・アプリケーションです。Oracle Database Vault は、これらのアクセス制御要件や将来発生する要件への対応にこの上なく適した強力な機能を導入しました。

Oracle Database Vault の複数ファクタ認可

Oracle Database Vault の複数ファクタ認可により、従来のロール・ベースのアクセス制御の枠を超え、さらに高度なラベル・ベースのアクセス制御が Oracle Database で実現されます。複数ファクタ認可を使用すると、データベースへのアクセスを特定のサブネットまたはアプリケーション・サーバーに制限することで、データ・アクセスの仮想信頼パスを作成できます。承認済みアプリケーションへのデータ・アクセス制限は、Oracle Database Vault のファクタとコマンド・ルールを組み合わせることで実現できます。Oracle Database Vault は、IP アドレスなどの多数の組込みファクタを提供しており、単独またはその他のセキュリティ・ルールと組み合わせることで、既存アプリケーションのセキュリティ・レベルを大幅に向上させます。Oracle Database Vault が提供する組込みファクタに加えて、独自のビジネス要件に合わせて固有のカスタム・ファクタを追加できます。

Oracle Database Vault のコマンド・ルール

Oracle Database Vault のコマンド・ルールを利用すると、ほとんどすべてのデータベース操作に対して簡単にセキュリティ・ポリシーを関連付けることができます。また、内部統制を強化するとともに、業界のベスト・プラクティスとセキュアな構成ポリシーを適用できます。重要なビジネス・データに対して強力な保護機能も実現できます。たとえば、DBA を含むあらゆるユーザーが本番環境からアプリケーション表を削除することを防止できます。コマンド・ルールは、Oracle Database Vault の GUI から、またはコマンドラインから API を使用して容易に管理できます。

Oracle Database Vault とアプリケーション

規制順守とインサイダーの脅威の問題への取り組みを支援するというコミットメントの一部として、オラクルは PeopleSoft アプリケーションを使用して Oracle Database Vault を検証しました。オラクルは、PeopleSoft アプリケーション環境で Oracle Database Vault を使用して、特権ユーザーによるアプリケーション・データ・アクセスを防止する方法を示した、使いやすいガイドを作成しました。また、このガイドには、複数ファクタ認可とコマンド・ルールを使用してより高度なポリシーを適用する方法を示す例も含まれています。使いやすいセットアップ・スクリプト

と段階的な手順は、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 アプリケーションを使用した検証は現在実施中であり、今年中に完了する予定です。また、オラクルはサード・パーティのアプリケーション・プロバイダとも協業しています。

顧客事例

Oracle Database Vault は、ほとんどすべての業界に有効なソリューションです。機密性の高い知的財産から、個人識別情報、クレジット・カード情報、または財務実績まで、ますます巧妙になる脅威に対して機密データを強力に保護する機能が求められています。

金融サービス顧客	
顧客要件	Oracle Database Vault ソリューション
特権ユーザーによる機密データ・アクセスの制限	アプリケーション・データの周囲にレールムを定義し、アプリケーション所有者のみにデータ・アクセスを認可することで、DBA などの特権ユーザーによるアプリケーション・データへのアクセスを防止。
中間層プロセスと中間層サーバーを介したアプリケーション・アクセスの実現	コマンド・ルールを定義することで、データベース・アクセスを特定のサーバー上にある特定の中間層アプリケーションに制限。
故意または過失による有害な変更からのデータベース構造の保護	メンテナンス期間を強制するコマンド・ルールを定義することで、データベース・メンテナンス用の DBA ログインを特定の日時に制限。さらに、複数ファクタ認可を使用してメンテナンス期間中の2名ルールを適用。
バッチ適用とバックアップの特定のメンテナンス期間での実施と、バッチ適用プロセスの監視	コマンド・ルールの定義による、ビジネス・データ構造の削除または消去など、故意または過失による危険な操作からの保護。

表3. Oracle Database Vault の事例

結論

Oracle Database Vault は業界有数のデータベース・セキュリティ・ソリューションであり、規制順守とインサイダーの脅威への懸念に対応します。Oracle Database Vault は、PCI や SOX 法などの規制に付随するアクセス制御要件への対応を支援します。Oracle Database Vault は、Oracle Database 10g Release 2、および Oracle Database 11g Release 1 で使用できます。また、Oracle PeopleSoft アプリケーションで検証済みです。Oracle E-Business Suite および Siebel を含むその他のアプリケーションでの検証は、現在実施中です。Oracle Database Vault を使用すると、特権ユーザーによるアプリケーション・データへのアクセスを防止できます。さらに、時間、IP アドレス、サブネットなどの変数に基づいて、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を厳密に制御できます。要約すると、Oracle Database Vault は、現在のグローバル経済において必要とされる、柔軟性と透過性に優れ、高度な適応性を備えたセキュリティ制御機能を提供します。



Oracle Database Vault

2007年6月

著者: Kamal Tbeileh、Paul Needham

共著者:

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

海外からのお問合せ窓口:

電話: +1.650.506.7000

ファクシミリ: +1.650.506.7200

www.oracle.com

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。