Oracle ホワイト・ペーパー

2009 年 9 月

Oracle Database 11g Release 2 の Oracle Database Vault

はじめに

規制遵守、産業スパイ活動、インサイダーの脅威。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。また、組織の競争力を維持するためには、統合やオフショアリングを利用し、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が必要とされます。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。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莫大なものです。その一方で、米国サーベンス・オクスリー（SOX）法、EU データ保護指令、医療保険の相互運用性と説明責任に関する法律（HIPAA）、クレジットカード業界のデータ・セキュリティ基準（PCI-DSS）などの規制や、多数のデータ侵害通知法を遵守するには、機密データへのアクセスを厳密に制御する必要があります。Oracle Database Vault が提供する強力かつ透過的なセキュリティ・ソリューションを利用することで、組織は、規制を遵守し、コスト効率に優れた方法でシステムを配置し、機密データへの不正アクセスを防止できます。

Oracle Database Vault

従来、IT に関する意思決定に影響を与える 2 大要因は、パフォーマンスと可用性でした。しかしこの 10 年で、セキュリティも不可欠な要素としてリストアップされるようになりました。Oracle Database のセキュリティ・オプションである Oracle Database Vault は、既存のアプリケーション環境に透過的に適用できる、柔軟性と適応性に優れたセキュリティ制御機能を提供します。Oracle Database Vault のセキュリティ制御機能には、レルム、コマンド・ルール、ファクタ、職務の分離、およびレポートが含まれます。これらの制御機能により、アプリケーション・コードを変更しなくても、既存アプリケーションのセキュリティが透過的に強化されます。レルムは、Oracle データベース内部のファイアウォールのように機能することで、特権ユーザーによるアプリケーション・データ・アクセスを予防的に制御します。コマンド・ルールおよびファクタは、いつ、どこで、誰が、どのように、データベースやデータ、そしてアプリケーションにアクセスできるかを制御します。コマンド・ルールは、IP アドレス、認証方式、プログラム名などのファクタを使用して、一般的なデータベース・コマンドにルールを適用することで、既存アプリケーションのセキュリティを強化します。Oracle Database Vault の職務の分離機能は、既存データベースに最小権限モデルを適用することで、従来のデータベース管理活動と Oracle Database Vault のセキュリティ管理から、アカウント管理を分離します。

表1 Oracle Database Vaultの機能

機能	説明
レルム	Oracleデータベース内の境界であり、ファイアウォールのような役割を果たすことで、特権ユーザーがその特殊権限を使用してもアプリケーション・データにアクセスできないようにします。
コマンド・ルール	データベース・コマンドの実行を制御するセキュリティ・ルールです。
ファクタ	Database Vaultのコマンド・ルールおよびレルムと組み合わせて使用する環境パラメータ（IPアドレス、認証方式）です。データへの信頼パスを作成し、いつ、どこで、誰が、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できるかを定義します。
職務の分離	標準で提供される、データベース内の最小権限の制御機能であり、主要な管理アクション（アカウント管理、セキュリティ管理、データベース管理）を分離します。
レポート	標準で提供されるセキュリティ関連レポートであり、試行されたレルム違反とその他のDatabase Vaultが実施する制御に関する詳細情報が含まれます。

Oracle Database Vault は、Oracle9i Database Release 2、Oracle Database 10g Release 2、および Oracle Database 11g で利用できます。

Oracle Database Vault と規制

多くの規制に共通するのは、機密データへのアクセスと職務の分離に関して、厳密かつ実証可能な制御を求めている点です。実際、規制要件の多くは手続きに関したものですが、未承認のアクセスやデータ変更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。

表2 Oracle Database Vaultと規制（サンプル・リスト）

規制	要件	Database Vault で適用可能か？
米国サーベンス・オクスリー法 第302条	未承認のデータ変更の防止	可能
米国サーベンス・オクスリー法 第404条	データ変更と未承認のアクセスの防止	可能
米国サーベンス・オクスリー法 第409条	DoSおよび未承認のアクセスの防止	可能
グラム・リーチ・ブライリー法	未承認のアクセスおよび変更の防止	可能
HIPAA 164.306、164.312	未承認のデータ・アクセスの防止	可能
Basel II - 内部リスク管理	未承認のデータ・アクセスの防止	可能
CFR Part 11（FDA）	未承認のデータ・アクセスの防止	可能
日本の個人情報保護法	未承認のデータ・アクセスの防止	可能
PCI - 要件7	カード会員データへのアクセスを、業務上の必要範囲内に制限	可能
PCI - 要件8.5.6	ベンダーがリモート保守に使用するカウントは、必要なときのみ有効	可能
PCI - 要件3.4の補助制御	以下の基準に基づいて、カード会員データまたはデータベースへのアクセスを制限 • 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	可能
PCI - 要件A.1：ホスティング･プロバイダによるカード会員データ環境の保護	各事業体が、その事業体のカード会員データ環境にのみアクセス	可能

Oracle Database Vault のレルム

データベース管理者やその他の特権ユーザーは、データベース保守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、特権ユーザーが実行する日常的なタスクの一部にすぎません。しかし、データベースの特権ユーザーによる機密アプリケーション・データの参照を防止することが、ますます重要になっています。アプリケーションの統合や適切なソーシング、オフショアリングを実行するには、財務、人事、医療、小売、およびその他のアプリケーション内の機密データに対するアクセスを厳密に制御する必要があります。

Oracle Database Vault のレルムは、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 のレルムを使用すると、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を実現できます。

Oracle Database Vault のコマンド・ルールとファクタ

Oracle Database Vault のコマンド・ルールは、従来のデータベースの役割をはるかに上回る、複数ファクタ認可による制御を可能にします。コマンド・ルールと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・アクセスの信頼パスを作成できます。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ファクタと組み合わせて使用することで、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。また、独自のビジネス要件に合わせた、カスタム・ファクタも定義できます。

Oracle Database Vault のコマンド・ルールを利用すると、よく使用するデータベース・コマンド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。さらに、重要なビジネス・データが強力に保護されます。たとえば、コマンド・ルールを使用することで、DBA やアプリケーション所有者であっても、本番環境からアプリケーション表を削除できないように設定できます。コマンド・ルールは、Oracle Database Vault 管理コンソールまたは Oracle Database Vault コマンドライン・インタフェースを使用して、容易に管理できます。

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、データベース内の制御を強化し、多くの規制に見られる要件を満たします。Oracle Database Vault では、次の 3 種類の権限が標準でデータベース内に作成されます。

表3 Oracle Database Vaultの職務の分離

権限	説明
アカウント管理	アカウント管理の権限を持つユーザーは、データベース・ユーザーを作成、削除、および変更できます。既存の特権ユーザーは、アカウント管理アクティビティを実行できません。
セキュリティ管理	セキュリティ管理の権限を持つユーザーは、データベースのセキュリティ管理者（Database Vaultの所有者）になります。セキュリティ管理者は、レルム、コマンド・ルール、ファクタ、およびDatabase Vault固有の各種セキュリティ・レポートを管理できます。セキュリティ管理者は、保護されたビジネス・データに対して自身のアクセスを認可することはできません。
データベース管理	データベース管理の権限を付与されると、DBA権限を持つユーザーは、保護されたビジネス・データにアクセスすることなく、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、データベースに関連する通常の管理作業と保守作業を引き続き実行できます。

Oracle Database Vault の拡張性を利用すると、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、データベース管理権限をさらに分割して、バックアップ、パフォーマンス、パッチ適用という権限を作成できます。小規模の企業では、権限を統合したり、各権限に異なるログイン・アカウントを割り当てたりすることで、よりきめ細かいアカウンタビリティと監査を実現できます。

Oracle Database Vault のレポート

Oracle Database Vault は、多数のレポートを標準で提供しており、レルムにより阻止されたデータ・アクセスなどに関するレポートを作成できます。たとえば、レルムで保護されたアプリケーション表内のデータに DBA がアクセスしようとすると、Oracle Database Vault によってアクセスが阻止されるとともに、監査レコードが作成されます。この監査レコードは、レルム違反レポートから容易に参照できます。

Oracle Database Vault の管理性

Oracle Database Vault では、レルム、コマンド・ルール、およびルール・セットを管理するための管理コンソールが提供されています。このコンソールでは、Oracle Database Vault のレポートも表示できます。全社レベルの管理を実現するため、Oracle Database Vault は Oracle Enterprise Manager Grid Control と統合されています。Oracle Enterprise Manager Grid Control は、Oracle Database Vault を監視し、データベース間で Oracle Database Vault のセキュリティ設定をコピーする機能を提供します。たとえば、Oracle Database Vault のレルムおよびコマンド・ルール定義は、データベースを有効にする事前に設定およびテストされた中央データベースから別の Oracle Database Vault へと、コーディングなしで簡単に複製できます。

Oracle Database Vault とアプリケーション

Oracle Database Vault は、多数の Oracle アプリケーションおよびパートナー・アプリケーションで認定されています。この認定には、すぐに使用できる各アプリケーション固有のセキュリティ・ポリシーが含まれています。ここには、それぞれのアプリケーションで機能するレルムとコマンド・ルールが定義されています。

表4 Oracle Database Vaultの各アプリケーションに対する認定

アプリケーション	認定について	アプリケーション固有の保護ポリシーは有効か？
Oracle E-Business Suite（リリース11iおよび12）	認定済み	有効
Oracle PeopleSoft	認定済み	有効
Oracle JD Edwards EnterpriseOne	認定済み	有効
Oracle Siebel	認定済み	有効
Oracle Internet Directory	認定済み	有効
SAP	認定済み	有効

顧客事例

アクセス制御の対象が知的財産、個人情報、クレジットカード情報、または財務データのどれであるかに関係なく、Oracle Database Vault はあらゆる業種にメリットをもたらします。Oracle Database Vault の強力な予防制御機能により、規制を遵守し、巧妙さを増す脅威から身を守ることができます。

表5 顧客事例

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へのアクセスを制限すること	顧客アプリケーション・データの周囲にレルムを定義し、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。
アプリケーション・アクセスは、中間層プロセスと中間層サーバーを経由させること	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で実行され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データベース構造を保護すること	追加のコマンド・ルールを定義することで、ビジネス・データ構造の削除や消去など、故意または過失による危険な操作から保護。
パッチ適用とバックアップを特定の保守期間に実施し、パッチ適用プロセスを監視すること	保守期間を限定するコマンド・ルールを定義することで、データベース保守用の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保守期間中の2名ルールを適用。

この顧客は上記要件を満たすことで、機密データの保護と規制遵守を維持しながら、バックエンド処理をアウトソーシングすることに成功しました。

結論

Oracle Database Vault は、規制要件に対応し、インサイダーの脅威によるリスクを軽減するための、業界有数のアクセス制御ソリューションです。Oracle Database Vault の透過的なセキュリティ制御機能は、SOX、HIPAA、PCI-DSS などの一般的な規制要件に対応します。Oracle Database Vault は、Oracle9i Database Release 2、Oracle Database 10g Release 2、および Oracle Database 11g で利用できます。Oracle Database Vault は、Oracle E-Business Suite、Oracle PeopleSoft、Oracle Siebel、Oracle JD Edwards EnterpriseOne、および SAP の各アプリケーションで認定されています。Oracle Database Vault を使用すると、既存アプリケーションで容易かつ透過的に予防制御を実現できます。これにより、規制要件を遵守し、未承認のデータ・アクセスによるリスクを軽減しながら、データ統合やアウトソーシングなどのコスト削減戦略を推進できます。

Oracle Database 11g Release 2 の
Oracle Database Vault
2009 年 9 月
著者：Kamal Tbeileh
共著者：Paul Needham

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

0109