19c ORACLE Database

Oracle Database Vault

Oracle Database Vaultは強力なセキュリティ制御機能を提供することで、機密データを不正アクセスから保護し、データベース管理者とデータ所有者間の職務を分離してプライバシ要件や規制要件に対応します。制御機能によって特権アカウントによるアプリケーション・データへのアクセスをブロックするとともに、認可された信頼パスでデータベース内部での機密情報の操作を制御できます。さらに、Oracle Database Vaultによって既存のデータベース環境を透過的に保護することで、コストと時間のかかるアプリケーション変更が不要になります。

特権アカウントの制御

侵害された特権データベース・アカウントは、機密データにアクセスするためにもっとも一般に使用されるルートの1つです。この広範な無制限のアクセスは、データベースのメンテナンスを容易にしますが、侵害された特権アカウントは大量のデータに不適切にアクセスする攻撃の糸口にもなります。アプリケーション・スキーマ、テーブル、およびストアド・プロシジャについて定義されたOracle Database Vaultのレルムの制御機能により、悪意のあるユーザーが特権アカウントを利用して機密データにアクセスするのを防止できます。さまざまな標準ファクタ（IPアドレス、認証方式、プログラム名など）を使用して、盗まれたパスワードによる攻撃を防止する信頼パス認可を簡単に実装できます。

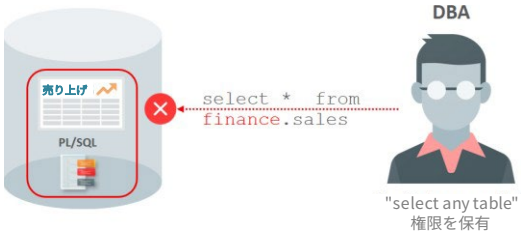

図1：Oracle Database Vaultのレルムによる特権アカウントでのアクセスの防止

ビジネス上のおもなメリット

- 機密データを保護し、GDPR、PCI-DSS、HIPAA、SOX、その他の規制にともなう内部統制、職務分掌およびアクセス制御の規定に準拠するための容易で費用対効果に優れた手段を提供します。
- 機密データ漏洩によるデータ漏洩のビジネス・リスク管理を支援します。
- 特権ユーザーとDBAによる機密データへのアクセスをブロックするための予防的制御を実装しています。
- データベース内部での操作を制御することで、潜在的な脅威による構成の不正な変更を防止して、監査不適合を回避できます。
- エンタープライズ・アプリケーション（Fusion Applications、E-Business Suite、PeopleSoft、Siebel、SAPなど）に関するアプリケーションごとの保護ポリシーにより、時間を節約し環境を保護します。

ORACLE

データベース構成の制御

監査で指摘されることがもっとも多いものとして、データベース権限の不正変更（DBAロールや新しいアカウントおよびデータベース・オブジェクトの付与など）が挙げられます。本番環境の不正な変更により、セキュリティが弱まり、ハッカーの侵入経路が開かれ、プライバシおよびコンプライアンス規制に違反する可能性があるため、そのような変更を防止することはセキュリティだけでなくコンプライアンスの点からも重要です。Oracle Database Vaultのコマンド・ルールにより、データベース内部での操作（データベース変更、システム設定変更、表切捨て、ユーザー作成などのコマンドを含む）を制御できます。これらの制御機能により、不正な構成変更を防止するとともに、ハッカーや悪意のある内部関係者によるアプリケーションの改ざんや変更も防止できます。

職務の分離

Oracle Database Vaultは、セキュリティ管理、アカウント管理、および日常的なデータベース管理アクティビティの3つの職務を明確に分離する制御機能を標準で提供します。Oracle Database Vaultが提供する職務分離の制御機能はカスタマイズが可能で、リソースが限られている企業では、Oracle Database Vaultによって分離される複数の職務を同じ管理者に割り当てることもできます。

エンタープライズ・アプリケーション保護ポリシー

主要なエンタープライズ・アプリケーション（Oracle Fusion Applications、Oracle E-Business Suit、Oracle PeopleSoft、Oracle Siebel、Oracle Financial Services（i-Flex）、Oracle Primavera、SAP、Finacle from Infosysなど）に関しては、Oracle Database Vaultのアプリケーション別の保護ポリシーとガイドラインを使用できます。

Database Vaultのセキュリティ制御とシミュレーション・モードを使用して、顧客のアプリケーションを迅速に検証することができます。シミュレーション・モードではセキュリティ違反をブロッキングするのではなくキャプチャするので、リグレッション・テストにより、本番環境の正当なアクティビティを妨げることなく、必要なセキュリティの変更をキャプチャできます。シミュレーション・モードでは、オペレーションに悪影響を及ぼすことなく、新しいセキュリティ制御を本番環境に素早く導入できます。

オペレーション制御

Oracle Multitenantにおけるデータベース統合は、Database Vaultのオペレーション制御によるセキュリティ強化の恩恵を受けています。Oracle Database Vault Operations Controlは、PDBユーザーが他のPDBやデータベースに影響を与えないようにするPDBロックダウン・プロファイルを使用するのとは別に、プラガブル・データベース内のアプリケーションの機密データに対するMultitenantコンテナ管理者のアクセスを透過的に防止します。

管理性

Oracle Database Vaultは、現在サポートされているすべてのデータベース・バージョンに組み込まれており、容易に有効にすることができます。Oracle Database Vaultの管理はOracle Enterprise Manager Cloud Controlと完全に統合されるため、セキュリティ管理者は、一元化された効率的なインタフェースによってOracle Database Vaultを管理できます。セキュリティの責務をドメイン・セキュリティのエキスパートに任せることができます。

おもな機能

- オブジェクト所有者も含め、オブジェクトへの直接アクセスを許可されているユーザーによるものであっても、Oracle Database Vaultの**レルム**により権限の悪用および機密データへのアクセスを予防します。
- Oracle Database Vaultの**コマンド・ルール**および**ファクタ**を使用して、本番環境での不正な変更と人為的エラーを予防します。
- アプリケーションやクライアントとデータベースとの間に**信頼パス**を定義することにより、盗まれた資格証明の使用を防止します。
- Oracle Database Vault **オペレーション制御**により、インフラストラクチャDBAやMultitenantコンテナ管理者がプラガブル・データベースの機密データにアクセスするのを予防します。
- シミュレーション・モードを使ってカスタム・アプリケーションとパッケージ・アプリケーションをテストすることで、セキュリティ制御を迅速に検証します。

関連製品

Oracle Database 19cの多層防御セキュリティ・ソリューション：

- Oracle Advanced Security
- Oracle Key Vault
- Oracle Data Masking and Subsetting Pack
- Oracle Label Security
- Oracle Audit Vault and Database Firewall
- Oracle Database Security Assessment Tool

CONNECT WITH US

+1.800.ORACLE1までご連絡いただくか、oracle.comをご覧ください。
北米以外の地域では、oracle.com/contactで最寄りの営業所をご確認いただけます。

blogs.oracle.com/cloudsecurity/db-sec facebook.com/oracle twitter.com/oracle

Integrated Cloud Applications & Platform Services

ORACLE

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