19c ORACLE Database

# Oracle Database Vault

Oracle Database Vaultは強力なコントロールと職務分離により、未許可の特権ユーザーによる機密データへのアクセス、およびデータベースへの不正な変更を阻止し、追加のコントロールとして信頼パスを使って、不正アクセスからデータベースを保護します。強力で透過的なセキュリティ・ソリューションで、規制遵守、コスト効率に優れたシステムの展開、機密データへの不正アクセス防止を支援します。

## 製品の概要

### Oracle Database Vaultとは何ですか。

Oracle Database Vaultは強力なセキュリティ・コントロールを実施して、特権ユーザーによる機密情報への不正アクセスを防止し、意図しない誤った変更からデータベースを保護します。これらの機能を使えば、悪意のあるユーザーが特権アカウントを使ってデータベースを攻撃するリスクが軽減されます。

### すでにデータベースが暗号化されていてもOracle Database Vaultが必要な理由は何ですか。

ほとんどのサイバー攻撃では、特権ユーザー・アカウント情報を盗み出すために、さまざまな手段を講じています。サイバー攻撃者は特権ユーザー・アカウントから機密情報の宝庫への鍵を得て、パラレル・システムに飛び込んだり、システムのデータをこっそり盗んだりすることができます。

暗号化は、OSレベルのデータベース・ファイル、ストレージ・デバイス、バックアップ・デバイス、エクスポート・ファイルから機密データを盗み出せるデータベース・バイパス攻撃を防止します。

適切に暗号化すれば、サイバー攻撃者がデータベースから機密データを盗むにはデータベース特権ユーザー・アカウントから攻撃せざるを得なくなります。Oracle Database Vaultで強力なコントロールを実施すれば、特権アカウント悪用によるデータ漏えいのリスクを最小限に抑えられます。



ORACLE

Oracle Database Vaultは信頼パス機能を提供して、IPアドレス、プログラム名、時刻、ユーザー名などのシステム要因を使って機密データへのアクセスをさらに制限します。

強力な保護制御とアクセス制御に加えて、職務分離の原則も実施しサポートします。

**Oracle Database Vaultはセキュリティとコンプライアンスをどのように改善するのですか。**

Oracle Database Vaultは、もっともよくあるサイバー攻撃方法である特権ユーザー攻撃のリスクを最小限にすることで、セキュリティを向上させます。ほとんどのコンプライアンス要件には、職務分離の管理、および機密データへの管理アクセスの防止が含まれます。Oracle Database Vaultはデータベース・エンジンにセキュリティを実装するので、サイバー攻撃の発生元がどのネットワークまたはサーバーでも、これらのセキュリティ管理は準備万端に対処します。

**Oracle Database Vaultはセキュリティ標準を基に評価されているのですか。**

Oracle Database Vaultは、コモン・クライテリアの認可を受けています。Oracle DatabaseとOracle Database Vault認可の最新情報については、Oracle Technology NetworkのWebサイトでご確認ください。ITセキュリティ評価のコモン・クライテリアは、IT製品のセキュリティを評価する、国際的に認められた標準（ISO 15408）です。

**Oracle Database Vaultは、クラウドに対してどのようなセキュリティを提供していますか。**

Oracle Database Vaultは、データベースへの特権ユーザー・アクセス権限のあるクラウド管理者または社内管理者による攻撃からクラウド内の機密データを保護します。データベースは、クラウド管理者または社内管理者による不正な変更からも保護されます。

**Oracle Database Vaultを使用することで、サーベンス・オクスリー法、PCI、HIPAA、ITAR、EU GDPRにおけるコンプライアンス要件に対応できますか。**

Oracle Database Vaultは、サーベンス・オクスリー法、PCI、HIPAA、ITAR、EU GDPRなどの各種規制にある技術的なセキュリティ要件への対処を支援するように設計されています。ユーザーは、これらの規制が要求するプロセスと手順にも従う必要があります。Oracle Database Vaultは、データベース内に強力な内部管理機能を実装することで、誰がいつ、どこから、どのようにしてアプリケーション・データにアクセスできるのかをコントロールします。さらに、データベースに行える変更を制御することで、データベースの可用性とセキュリティを維持します。

## コンポーネントと機能

**Oracle Database Vaultには、どのようなセキュリティ管理機能が搭載されていますか。**

レルム - レルムはデータベース内部の"保護ゾーン"であり、DBAなどの特権ユーザーがレルム内のデータにアクセスすることを防止します。Oracle Database Vaultのセキュリティ管理者は、レルムを作成して、保護対象の機密データベース・オブジェクトをレルム内に追加し、レルムにアクセスする必要のあるユーザーまたはロールに権限を付与できます。レルムは、単一の表、複数の表、アプリケーション・スキーマ全体、または複数のアプリケーション・スキーマを保護できます。レルムには、必須レルムという2つ目のタイプのものがあり、保護を拡張して、オブジェクト所有者による不正アクセスもブロックします。Oracle Database Vaultのセキュリティ管理者しか機密データへのアクセスを許可できません。

コマンド・コントロール - コマンド・コントロール（コマンド・ルール）は、SELECT文、ALTER SYSTEM文、データベース定義言語（DDL）文、データ操作言語（DML）文などのSQL文に対してユーザーが実行できる条件を制御します。コマンド・ルールはセキュリティ・ポリシー（ルール・セット）を評価することで、文がどの条件で許可されるかどうかを決定します。

信頼パス – 信頼パス・ルール・セットは、自身の決定プロセスで複数の要因を利用し、レルム・アクセスおよびコマンド・コントロールと関連付けることができます。セキュリティ管理者は、個々のコンプライアンス要件またはセキュリティ要件に基づいてルールを定義できます。ルール・セットは、時刻、IPアドレス、ホスト名、プログラム名、または任意の数の識別可能なユーザー関連属性などのファクタを使用します。たとえば、アプリケーション・アクセスの制限事項として、就業時間内や、内部IPアドレスまたは内部IPアドレス範囲からのアクセスに制限される場合、ユーザーは特定のデータにだけアクセスできます。このような制限は、DBAを含むすべてのデータベース・ユーザーに適用できます。

オペレーション制御 – 広く普及しているデータベース統合テクノロジーであるOracle Multitenantのセキュリティを強化します。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

### Oracle Database Vaultで作成される新しいロールは何ですか。

Oracle Database Vaultの作成時に、2つの主要ロールが作成され、ユーザーに付与されます。DV_OWNERロールとDV_ACCTMGRロールです。DV_OWNERロールでは、セキュリティ・オブジェクト（レルム、コマンド・ルールなど）を作成し、認可ユーザーを追加し、コントロールやOracle Database Vaultセキュリティ・オブジェクトに関わる他の管理タスクを有効/無効にすることができます。DV_ACCTMGRロールはユーザーとプロファイルの作成と管理に使用します。これら2つのロールのサブセットである他のロールも複数作成されます。SYSDBA権限では、これら2つのロールのアカウントで失われたパスワードを回復することができないため、これらのロールのアカウントのバックアップを取っておくことが重要です。言い換えると、少なくとも2つのデータベース・アカウントにDV_OWNERロールを付与しておく必要があります。このロールを付与したデータベース・アカウントは、Database Vaultの日々の構成と管理に使用するものの他に、1つは組織の特権アカウント管理ソリューションに格納する緊急アカウントとして使用します。

### 新しいOracle Database Vaultのロールで、現在のデータベース管理者の作業はどのように変わりますか。

ほとんどのDBAのタスクは変わりません。これまでと変わる点は、ユーザーとプロファイルを作成し、管理することです。このセキュリティ関連のタスクは、DV_ACCTMGRロールのユーザーしか実行できません。また、Data PumpやJob Schedulingのような機密データが漏洩しかねないタスクには、DV_OWNERロールのアカウントからさらに認可を得る必要があります。

### Oracle Database Vaultの職務分離の管理は小規模の組織ではどのように機能しますか。

オラクルでは、Oracle Database Vaultが提供するその他のロール（Oracle Database Vault所有者 – セキュリティ管理を担当するセキュリティ管理者、およびOracle Database Account Manager – 新しいユーザーとプロファイルの作成と管理を担当するセキュリティ管理者）には別々の管理者を指定することをお勧めしています。これらの管理者はデータベース管理者とは別で異なります。ただし、小規模の組織では、管理者を分けられない場合があります。そのような場合は、1人にこれらのロールを１つ以上割り当てることができます。ただし、同じ人が複数のデータベース・セキュリティ・ロールを担う場合でも、各ロールをその人の個別のユーザー・アカウントに割り当てることをお勧めします。そうすると、これらのアカウントの1つを盗んだ悪意のあるユーザーによる攻撃の影響を最小限に抑えることができます。

### Oracle Database Vault所有者は、レルムで保護されたデータを表示できますか。

いいえ。Oracle Database Vault所有者は、レルムやコマンド・コントロールなどのセキュリティ・ポリシーの設定だけを行うことができ、レルムやコマンド・コントロールで保護されたデータを見ることはできません。このアクセス権を自分に付与することはできません。

**Oracle Database Vault所有者のセキュリティの責務を委任することはできますか。**

Database Vaultポリシーを使用すると、関連するレルムとコマンド・ルールをグループ化し、ポリシー所有者に委任できます。ポリシー所有者は、Oracle Database Vault管理者の完全なロールと権限がなくても、ポリシーに変更を加えることができます。ポリシー所有者が、委任されたポリシーに変更を加えるには、DV_POLICY_OWNERロールが必要です。

**Oracle Database Vault所有者がセキュリティ・オブジェクトに対して行った変更はどのように監査されるのですか。**

セキュリティ・オブジェクトへの変更（有効化、無効化、オブジェクトの追加、認可の追加など）はすべて監査されます。この機能は無効化できません。

**Oracle Database Vaultは、プラガブル・データベースの機密データに対する共通ユーザーからのアクセスをブロックできますか。**

Oracle Database 19cリリース以降、Oracle Database Vault Operations Controlは、自律型、通常のクラウド、またはオンプレミスの環境のプラガブル・データベース（PDB）に格納されているローカル・データへの、共通ユーザー（インフラストラクチャDBAなど）からのアクセスをブロックできるようになりました。PDBのローカル・データにアクセスしなければならない共通ユーザーやアプリケーションは、例外リストに追加することができます。

**Oracle Database Vault Operations Controlを有効にするのはどれくらい複雑ですか。**

有効化は簡単で、PDBユーザーにとって透過的に行われます。Database Vault Operations Controlを有効にするには、DBMS_MACADM.ENABLE_APP_PROTECTION PL/SQLプロシージャを使用します。

**Oracle Database VaultはOracle Enterprise Managerで管理できますか。**

はい。Oracle Enterprise Manger Cloud Controlには、レルム、ルール、ルール・セット、コマンド・ルールなど、ほとんどのOracle Database Vault機能に対応する管理インタフェースが備わっています。

**Oracle Database VaultでOracle DBAのタスクはどのように変わりますか。**

Oracle Database Vaultでは、ほとんどのDBAタスクは変わりません。これまでと変わる点は、ユーザーとプロファイルを作成し、管理することです。このセキュリティ関連のタスクは、DV_ACCTMGRロールのユーザーしか実行できません。また、Data PumpやJob Schedulingのような機密データが漏洩しかねないタスクには、DV_OWNERロールのアカウントからさらに認可を得る必要があります。詳しくは、Oracle Technology Network（OTN）に掲載されているホワイト・ペーパー『Oracle Database VaultによるDBA管理のベスト・プラクティス』を参照してください。

## デプロイメント

**Oracle Database Vaultのレルムとコマンド・ルールによるデータベースへのパフォーマンス・オーバーヘッドは何ですか。**

Oracle E-Business Suiteでのテストでは、Oracle Database Vaultのレルムとコマンド・コントロールによるオーバーヘッドは2 %未満という最小限のものでした。Oracle Database Vaultが有効化される場合でも、通常のデータベース・チューニングが引き続き適用されます。

**開発システムから本番システムにOracle Database Vaultセキュリティ・ポリシーを移行する方法を教えてください。**

以下の2つの方法で移行できます。

Oracle Enterprise Managerを使用すると、1つのOracleデータベースから他の複数データベースに対して、Oracle Database Vaultセキュリティ・ポリシーを移行できます。

Oracle Enterprise Managerでは、既存のセキュリティ・ポリシーからOracle Database Vault APIスクリプトを生成することもできます。このAPIスクリプトを編集し、任意の数のターゲットOracle Databaseに対して実行し、それらのデータベースでセキュリティ・ポリシーを作成できます。

**Oracle Database Vaultでは、アプリケーションはどのように認可されデプロイされるのですか。**

Oracle Database 12c Release 2以降、Oracle Database Vaultにはシミュレーション・モードが導入されています。このモードでは、Oracle Database Vaultセキュリティ・コントロールがチェックされますが、アクセスを防止する代わりに、ポリシー違反をシミュレーション・ログに記録します。そのため、ユーザーはOracle Database Vaultから邪魔されずに、リグレッション・テストを最初から最後まで実行できます。Oracle Database Vaultセキュリティ・コントロールで調整が必要かどうかを確認するために、リグレッション・テストの終了時にシミュレーション・ログが分析されます。Oracle Database Vaultの保護を有効にする前に本番環境で最終チェックを行うため、アプリケーションが本番環境に入ると、シミュレーション・モードが再び使用されます。

**Oracle Database Vaultで保護されたデータベースにパッチを適用する方法を教えてください。**

Oracle Database Vaultでは、データベース・パッチ適用モードを開始して、Oracle Database Vaultを無効にせずに、データベースにパッチを適用できます。その場合、セキュリティ管理者（DV_OWNERロールのユーザー）がDBAにDV_PATCH_ADMINロールを付与することで、DBAがデータベースにパッチを適用できるようになります。パッチを適用したら、セキュリティ管理者は、DBAに対するDV_PATCH_ADMINロールを取り消します。DV_PATCH_ADMINロールを使用すると、DBAは保護されたアプリケーション・データにアクセスすることなく、データベースにパッチを適用できます。

**データベースのシステムとセッションにDBAが不正な変更を行うのをどのように防ぐのですか。**

コマンド・ルールを使用すると、データベースで実行できるコマンドを制限できます。ALTER SYSTEMとALTER SESSIONは強力なコマンドであり、その粒度の細かい使用は、コマンド・ルールと信頼パスの使用で制限することができます。

## 詳細情報

**Oracle Database Vaultに関する詳細情報の入手先を教えてください。**

詳しくは、Oracle Technology Network（OTN）に掲載のOracle Database Vaultのページを参照してください。データ・シート、ホワイト・ペーパー、顧客事例、エンドユーザー向け文書、ディスカッション・フォーラムなど、有益な各種情報をオンラインで入手できます。Oracle Universityでは、Oracle Database Vaultのトレーニング・コースを提供しています。

https://www.oracle.com/jp/database/technologies/security/db-vault.html

19c ORACLE Database

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