19c ORACLE Database

Oracle Advanced Security

Oracle Database 19c ReleaseのOracle Advanced Securityには、アプリケーションの機密データの保護に不可欠な、業界をリードする暗号化およびデータ改訂機能が搭載されています。透過的データ暗号化とData Redactionによって、アプリケーション・レイヤー、オペレーティング・システム、バックアップ・メディア、およびデータベース・エクスポートでの機密情報への不正アクセスを防ぎます。Oracle Advanced Securityは、Oracle Multitenantを完全にサポートしており、Oracleエンジニアド・システムと統合されているため、パフォーマンスが非常に優れています。

プライバシとコンプライアンスのための暗号化とデータ改訂

データの保護には、予防的、発見的、管理的制御を含む多層防御手段が必要です。Oracle Advanced Securityは予防的制御を行って、多くの規制要件に対応し、データ侵害を防ぎ、プライバシ関連の情報を保護できます。たとえば、クレジット・カードのデータはストレージで自動的に暗号化され、取得時には、問合せ結果でデータベースから抽出される前に、その場で復号化および改訂されます。これら2つの機能は、プライバシ規制やクレジット・カード業界のデータ・セキュリティ標準（PCI-DSS）などの標準に準拠する上で重要です。

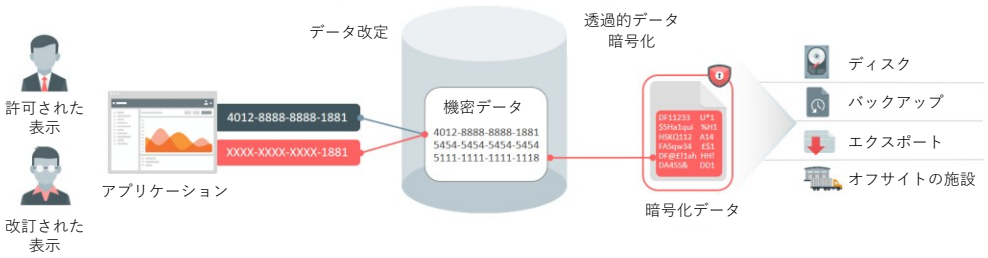

図1：Oracle Advanced Securityの概要

ビジネス上のおもなメリット

- 機密データを保護し、PCI-DSS、HIPAA、EU GDPR、その他の規制のデータ暗号化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
- 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
- データ管理ライフサイクル全体を通じて、暗号化データを常に保護し、その可用性を維持
- アプリケーションとデータベースに必要な変更を最小限に抑えて、導入コストと運用コストを削減
- 複数のアプリケーションとユーザーにまたがったデータ改訂の一元管理により、ガバナンスを改善
- Oracle Multitenantオプションを完全にサポートして、安全なデータ隔離を実現

ORACLE

透過的データ暗号化

透過的データ暗号化では、保管データを暗号化することにより、データベース環境外からの不正アクセスから機密データを保護します。これにより、オペレーティング・システムの特権ユーザーが制御をバイパスして、データベース・ファイルの内容を直接調べて機密情報に直接アクセスすることを防げます。また、データベース・ストレージのメディアやバックアップの盗難、紛失、不適切な廃棄も防ぐことができます。

このソリューションは、アプリケーションに対して透過的です。データがストレージへの書込み時に自動的に暗号化され、ストレージからの読取り時に復号化されるためです。データベース・レイヤーとアプリケーション・レイヤーで実施されるアクセス制御は、引き続き有効です。SQL問合せを変更することはなく、アプリケーションのコードや構成の変更は不要です。

透過的データ暗号化ではOracle Databaseのキャッシング最適化が使用されるため、暗号化と復号化のプロセスが非常に高速です。また、インテル® AES-NIおよびOracle SPARCのプラットフォーム（Oracle ExadataやSPARC SuperClusterなど）で提供されているCPUベースのハードウェア・アクセラレーションを利用します。さらに、Exadata Smart Scanによって、複数のストレージ・セルでデータを同時に高速で復号化したり、Exadata Hybrid Columnar Compressionによって暗号化操作の実行総数を減らしたりすることができます。

透過的データ暗号化には、データ暗号化鍵とマスター暗号化鍵で構成される2層の暗号化鍵管理アーキテクチャがあります。マスター鍵は、Oracle WalletまたはOracle Key Vaultではデータベースの外部に格納されます。組込みの機能により、ライフサイクル全体を通じて鍵が管理され、補助鍵ローテーションが提供されます。全データを再暗号化するオーバーヘッドが発生しません。

透過的データ暗号化は、導入が容易で、データベース・インストールの一部としてデフォルトでインストールされます。本番システム上で無停止のまま、既存の表領域をオンラインで暗号化できます。または、メンテナンス期間中、ストレージのオーバーヘッドを生じさせずに、オフラインで暗号化することもできます。さらに、透過的データ暗号化は、標準でOracle Automatic Storage Management（Oracle ASM）と連携して、ASMファイル・ストアのデータを保護します。

アプリケーションの機密データを改訂

Data Redactionでは、問合せ結果内の機密データがカスタム・アプリケーションで表示される前に、選択的に実行中に改訂できます。このため、未承認ユーザーが機密データを見ることはできません。また、同じデータにアクセスするアプリケーション・モジュール間で、データベース列を一貫して改訂できます。Data Redactionは、内部データベース・バッファ、キャッシュ、またはストレージにある実際のデータは変更せず、さらに、変換されたデータをアプリケーションに戻すときに元のデータ型およびデータ書式設定を維持するので、アプリケーションに対する変更の必要性は最小限に抑えられます。バックアップ、リストア、アップグレード、パッチ適用、高可用性クラスタなどのデータベース操作アクティビティに、影響を与えることはありません。

アプリケーション・コーディングや追加のソフトウェア・コンポーネントに依存する方法とは異なり、Data Redactionポリシーはデータベース・カーネルで直接実施されます。宣言的ポリシーは、部分/ランダム/全改訂など、さまざまなデータ変換に適用できます。改訂は、データベースによって追跡されたり、アプリケーションからデータベースに渡されたりする各種要素（ユーザーID、アプリケーションID、クライアントIPアドレスなど）に基づく条件によって変わる場合があります。改訂書式ライブラリが提供する事前構成済みの列テンプレートは、クレジット・カード番号や社会保障番号といった一般的な種類の機密データに対応できます。ポリシーを有効にすると、アクティブなセッションでもすぐに実施されます。

おもな機能

透過的データ暗号化

- アプリケーションを変更することなく、データベースの列、表領域、またはデータベース全体に格納されたアプリケーション・データを暗号化
- 既存の表領域のオンライン暗号化をサポート
- 補助鍵のローテーションによる、組込み暗号鍵のライフサイクル管理
- AES（128、192、256ビット鍵）などの業界標準暗号化アルゴリズム、およびARIA、SEED、GOSTなどの地域の暗号化アルゴリズムを使用
- Oracle Key Vaultと連携して、暗号化された数百のデータベースの鍵を効率的に管理
- インテル® AES-NIおよびOracle SPARC Tシリーズでハードウェア・アクセラレーションを利用
- データベース・テクノロジー（Oracle RMAN、Oracle ASM、Oracle RAC、Oracle Advanced Compression、Oracle Data Guard、Oracle GoldenGateなど）との直接統合
- プラガブル・データベース間でキーストアを分離した方が望ましい場合は、各プラガブル・データベースのキーストアの作成をサポート
- ユーザー定義によるマスター暗号化鍵の作成をサポート

Data Redaction

- 実行中の改訂により、アプリケーションでの機密情報の公開を制限
- 宣言的な改訂ポリシーをデータベースで一元的に管理
- さまざまなアプリケーション・シナリオに適した複数の改訂変換
- 正規表現を使って、LOB（CLOB/NCLOB）の非構造化データを改訂

オンプレミスおよびクラウドの企業データを保護

透過的データ暗号化とData Redactionは、導入が簡単で、多層防御手段のセキュリティ戦略の一部として簡単に管理できます。Oracle CloudのOracle Databaseにあるデータは、透過的データ暗号化を使って、常に暗号化されています。Oracle Enterprise Managerには、ポリシーを定義および適用するための便利で包括的な管理コンソールがあります。コマンドラインAPIも使用できます。

透過的データ暗号化とData Redactionによって、使用頻度の高いOracle Databaseツールが統合され、他のデータベース機能が補完されます。たとえば、透過的データ暗号化の表領域暗号化とOracle Recovery Manager（Oracle RMAN）が連携してシームレスに機能することで、バックアップの暗号化と圧縮が実行されます。

Oracle Advanced Securityは、Oracle Multitenantを完全にサポートして、データベース・テナント間のデータ・セキュリティの分離を実現します。透過的データ暗号化とData Redactionは、プラガブル・データベースが新しいマルチテナント・コンテナ・データベースに移動する際も引き続き機能し、転送中のプラガブル・データベースを保護します。

Oracle Advanced Securityは、パフォーマンスのペナルティやコンピューティング・リソース拡張の要件を生じさせずに、データ・ライフサイクル全体を通じて、アプリケーションの透過性とカバレッジを実現する、Oracle Database唯一のデータ保護ソリューションです。クラウドへの移行準備を進めている企業がこのソリューションを採用すると、オンプレミスとクラウド双方の資産に対して同じデータ保護ソリューションを利用できます。

- Oracle Enterprise Managerを使用したポリシー管理、およびOracle SQL Developerとの直接統合

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

19c ORACLE Database

オラクルの情報を発信しています

+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