ORACLE

ORACLE 23ai Database

Oracle Advanced Security

Oracle Database 23ai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によって、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ぐことができます。Data Redactionは、アプリケーション・インタフェースのデータに動的マスキングを提供します。オラクルの透過的データ暗号化は、Recovery Manager、Real Application Clusters、Advanced Compression、Oracle Sharding、Data Guard、GoldenGate、MultitenantなどのOracle Databaseテクノロジーと連携して動作し、オラクルが設計したシステムで高パフォーマンスを実現します。

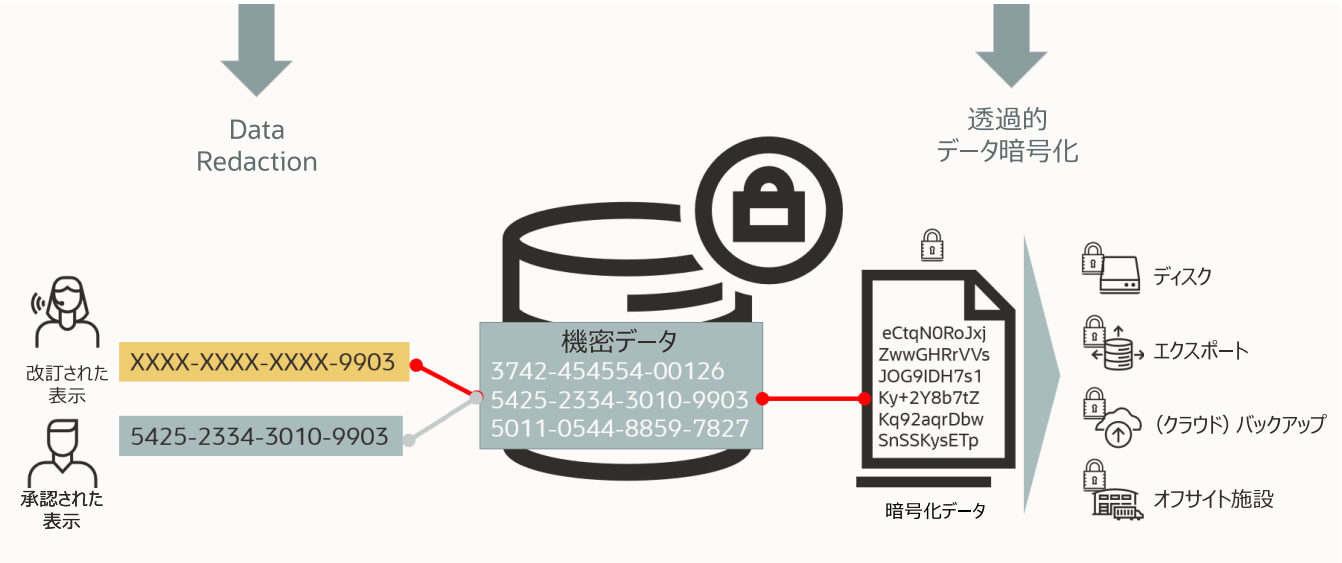
ビジネス上のおもなメリット

- 機密データを保護し、PCI-DSS、HIPAA、EU GDPRのデータ暗号化規定、その他の規制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

プライバシとコンプライアンスのための暗号化およびData Redaction

Oracle Advanced Securityは、2つの重要なデータ・セキュリティ・ソリューションを組み合わせて、多くの規制要件に対応し、データ侵害を防止し、プライバシ関連の情報を保護します。Oracle Advanced Securityを使用すると、アプリケーションの機密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



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、オンライン・ストレージ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アクセス制御をバイパスしてデータベース・ファイルの内容を調べ、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、不適切な廃棄を防ぐこともできます。

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も透過的です。アプリケーション・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は高速です。また、インテル®、AMD、およびOracle SPARCのCPU（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。暗号化されたデータのExadata Smart Scanは、複数のストレージ・セル上でデータを並行して復号化することで高速化されます。Exadata Hybrid Columnar Compressionは、必要な暗号化操作の数を減らすことで効率的に実行されます。

透過的データ暗号化は、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を実装します。管理者はマスター鍵を、Oracle Walletでローカルに、またはOracle Key Vaultで一元的に管理できます。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、簡易な鍵のローテーションが実施されます。これにより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短時間で導入でき、デフォルトではデータベース・インストールの一部に含まれています。ユーザーは既存の表領域を、オンラインで、本番システムの停止時間ゼロで暗号化するか、またはオフラインで、メンテナンス期間中にストレージ・オーバーヘッドを発生させることなく暗号化することができます。透過的データ暗号化は、Oracle Data Guard、Oracle Real Application Clusters（RAC）、およびマルチテナント・データベースですぐに使用できます。Oracle Database Configuration Assistant（DBCA）は、既存のデータベースを自動的に暗号化したり、暗号化されたデータベースを作成したりできます。

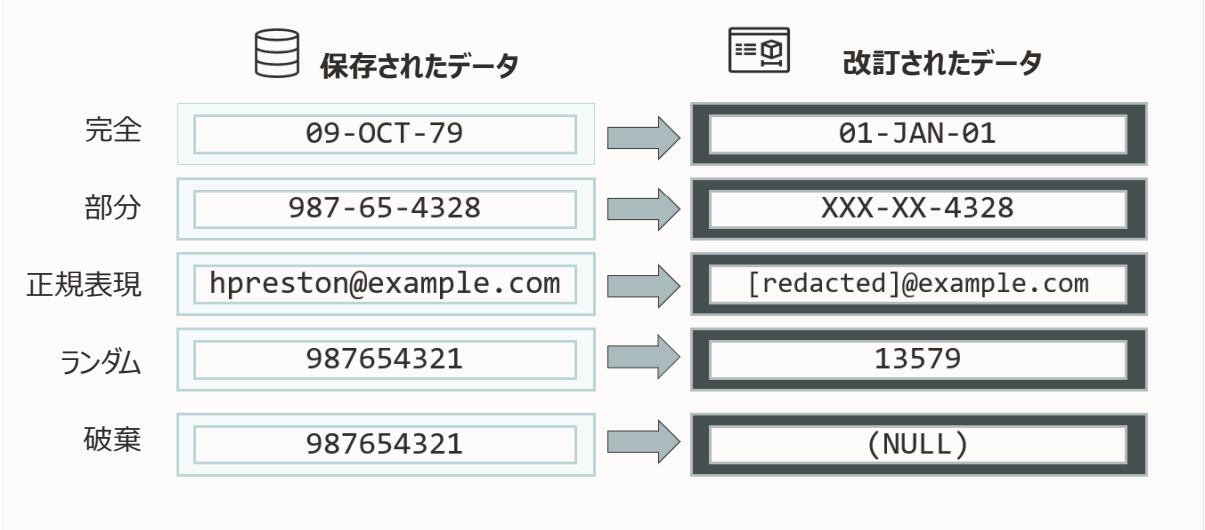
透過的データ暗号化のおもな特徴

- アプリケーションを変更することなくアプリケーション・データを暗号化
- 既存の表領域のオンラインおよびオフラインの暗号化をサポート
- 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
- 業界標準の暗号化アルゴリズムをサポート。XTS暗号モードを使用したAES（128、192、256ビット・キー）、ARIA（128、192、256ビット・キー）、トリプルDES（168ビット）など
- Oracle Key Vaultと連携して、暗号化されたデータベースの鍵をいくつでも効率的に管理
- Oracle SPARC CPU、インテル®、およびAMD®（AES-NI）のハードウェア・アクセラレーションを活用
- Oracle Databaseテクノロジー（Recovery Manager、ACFS、RAC、Advanced Compression、Data Guard、Oracle Sharding、GoldenGateなど）との直接統合
- プラガブル・データベース間でのキーストアの分離をサポート

アプリケーションの機密データの改訂

Data Redactionでは、問合せ結果内の機密データをカスタム・アプリケーションで表示するために、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、アプリケーションに戻す変換データは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。Data Redactionがバックアップ、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。

図2：Data Redactionによる変換



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、部分改訂、ランダム改訂、完全改訂など、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している、事前構成済みの列テンプレートを提供しています。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。

ORACLE

Oracle Data Redactionのおもな特徴

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

オンプレミスとクラウドでの機密データの保護

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データベースは、デフォルトでは透過的データ暗号化を使用して暗号化されており、オンプレミスのデータベースに暗号化をデプロイすると、ハイブリッド企業全体でシームレスなセキュリティを確保できます。Oracle Enterprise Managerには、データベースのフリート全体の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。自動化を促進するコマンドラインAPIも利用できます。

透過的データ暗号化とData Redactionによって、他のデータベース機能が補完され、Oracle Databaseツールと統合されます。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組織は、オンプレミスとクラウド双方のすべてのデータベース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。

関連製品

- Oracle Database 23aiの多層防御ソリューション
- Oracle Key Vault
- Oracle Database Vault
- Oracle Label Security
- Oracle Data Masking and Subsetting Pack
- Oracle Audit Vault and Database Firewall
- Oracle Data Safe

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 facebook.com/oracle twitter.com/oracle