Oracle Advanced Security による暗号化とリダクション

保管データの暗号化と機密情報のリダクションのための予防措置

2025年6月、バージョン[1.0]

公開

はじめに

セキュリティ脅威の高まりと、コンプライアンス要件、統合、クラウド・コンピューティングの拡大は、データ・セキュリティの重要性が高まっている理由の一部に過ぎません。最初の米国侵害通知法から約20年経過し、データへのアクセスが増えるに従い、強力な予防措置のニーズが高まり続けています。欧州連合の一般データ保護規則（GDPR）などのイニシアチブにより、データ・セキュリティは引き続き、組織にとって最優先事項です。ユーザーがラップトップから移行した、タブレットやスマートフォンなどのクライアント・デバイスには、盗難によって機密情報が簡単に漏えいしてしまう可能性があります。アウトソーシング、オフショアリング、企業合併、絶えまない組織変更によって、さらにリスクが高まります。悪意のある内部関係者が機密データを取得したり、外部のハッカーがソーシャル・エンジニアリング攻撃によってサーバーにアクセスしたりすることが簡単になるためです。このような傾向の高まりによって、使用するアプリケーションに関係なく、機密データの一元的かつ効率的な保護がかつてないほど重要になっています。機密データをソースで一貫して保護するセキュリティ対策を講じることは、保存データが増え続け、データへのアクセスが従来の境界を超えて拡大するに伴い、重要な制御手段になっています。データの保護には、データ駆動型セキュリティを介したセキュリティ体制の評価、データ損失の防止、疑わしいアクティビティの検出、ソースでのデータ・アクセス制御の適用を実施するための制御手段を含む多層防御マルチレイヤー・アプローチが必要です。Oracle Database 19cでは、これらの領域ごとに重要な新しいセキュリティ対策を提供することで、オラクルの業界有数のデータベース・セキュリティ・ソリューションを強化しています。

Oracle DatabaseのOracle Advanced Securityオプションには、保管データの暗号化と機密データのリダクションを包含する2つの基本的な予防措置機能があります。これらの予防措置によって、ストレージやアプリケーションから機密データが直接公開されないよう保護できます。Oracle Advanced Securityの透過的データ暗号化（TDE）によって、データベースを迂回したり、オペレーティング・システム・レベルのデータファイル、データベース・バックアップ、データベース・エクスポートなどから機密情報を読み取ろうとしたりする攻撃を防ぐことができます。Oracle Advanced SecurityのData Redactionは、問合せ結果の機密データがデータベースを離れる前にそのデータを改訂して、アプリケーションに未承認データが表示されるリスクを軽減することで、TDEを補完します。このホワイト・ペーパーでは、TDEとData Redaction、およびこれらの重要な予防措置がどのように連携して機密データを保護するかについて説明します。

「EU GDPR準拠に向け、弊社では、Oracle Advanced Security、Oracle Key Vault、Oracle Database Vault、Oracle Audit Vault、Oracle Database Firewallを含むOracle Database Securityソリューションを選択して、弊社のOracleデプロイメントを合理化および簡素化しました。Oracleにより、リスクを最小限に抑え、全体的なセキュリティをさらに強化しています。」

NOS社、CIO、
Henrique Zacarias氏

暗号化によるデータベース迂回の防止

保管データの暗号化は、データベースの迂回による機密データへの未承認アクセスを防ぐための重要な制御です。オペレーティング・システムの特権アカウントは、攻撃者や悪意のある内部関係者が物理ストレージ内の機密情報に直接アクセスするための手段の1つにすぎません。

Oracle Advanced Securityの透過的データ暗号化は、データベース・レイヤーのデータを暗号化することで、攻撃者によるデータベースの迂回や、ストレージからの機密情報の読取りを防ぎます。データベースの認証を受けたアプリケーションやユーザーは、引き続き透過的にアプリケーション・データにアクセスできますが、データベースを迂回しようとする未認証のユーザーは、クリア・テキスト・データへのアクセスが拒否されます。より分かりやすくするため、オペレーティング・システムの特権ユーザーが、簡単なシェル・コマンドを使用して、データベースの表領域ファイルにアクセスして機密情報を抽出できると考えてみましょう。また、紛失、盗難、不適切に廃棄されたディスクやバックアップから機密データを読み取る攻撃の可能性を考えてみましょう。図1は、Linuxの一般的な"strings"コマンドと検索パターンを使用して、顧客のクレジット・カード番号をストレージから直接抽出する例です。

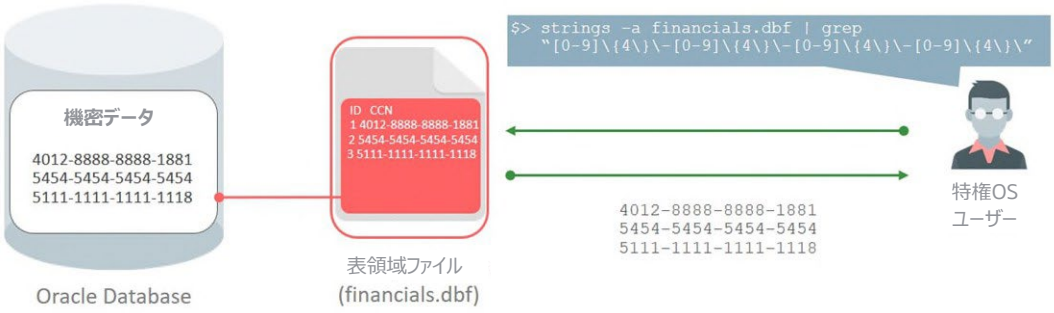

図1：Oracleデータベースの表領域ファイルからの顧客のクレジット・カード番号抽出

Oracle Advanced Securityの透過的データ暗号化

透過的データ暗号化は、アプリケーションの透過性を維持しつつ、データベース内の最適なレイヤーに常駐してデータベースの迂回を防止します。TDEは素早くデプロイでき、アプリケーションの表領域、またはSYSTEM、SYSAUX、TEMP、UNDO表領域を含むデータベース全体を暗号化します。これはアプリケーションに対して透過的です。暗号化と復号化のプロセスでアプリケーションの変更は不要であり、アプリケーション・ユーザーが暗号化データを直接処理する必要はないためです。もっとも重要な点として、TDEの組込み2層鍵アーキテクチャにより、停止時間なしでの鍵のローテーションを実現するとともに、鍵のライフサイクル全体を管理し、メタデータ属性を利用してライフタイム全体で鍵を追跡することができます。図2は、TDEを使ったOracleデータベースの暗号化によってデータベースの迂回を防ぐ方法を示しています。

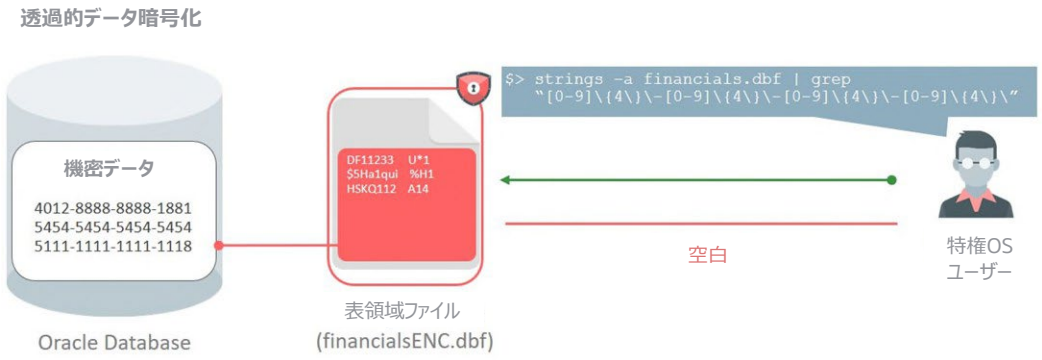

図2：透過的データ暗号化を使った暗号化によるデータベース迂回の防止

TDEは、ストレージ・ボリューム全体を暗号化したり、新しいツールキットやプログラミングAPIを必要としたりする他のアプローチとは異なる独自のものです。これらのアプローチでは、多くの迂回攻撃から保護されず、アプリケーションを大幅に変更する必要があり、鍵管理が複雑です（または鍵管理が行われません）。また、Oracle Advanced Compression、Oracle Real Application Clusters（Oracle RAC）、Oracle Recovery Manager（Oracle RMAN）、Oracle Multitenant、Oracle GoldenGate、Oracle Data Guardなどの補完的なテクノロジーと統合されていません。

TDEによる高レベルな保護は、以下の図に示すとおり、強力な暗号化の共通の標準に従っています。Oracle Database 19cのTDEは、認定暗号化スイートのみを使用して、FIPS 140-2レベル1暗号化モジュールを利用した操作をサポートします。

TDEが使用する標準の暗号化とハッシング・アルゴリズム

暗号化アルゴリズム	鍵の長さ
Advanced Encryption Standard（AES）	128ビット、192ビット、256ビット
トリプル・データ暗号化規格（TDES）	168ビット

TDE表領域暗号化によるアプリケーション全体の保護

Oracle Advanced SecurityのTDE表領域暗号化では、基盤となる表領域と索引を暗号化することによってアプリケーション表全体を保護します。この方式では、データの機密性やそのデータ型に関係なく、アプリケーションの表領域が暗号化されます。表領域暗号化では、特定のデータベース列の識別が不要であるため、暗号化プロセスが簡素化されます。表領域暗号化は、暗号化が必要な大量の機密データがデータベースに含まれており、その列がさまざまな場所に存在する場合に便利です。これらすべての理由により、TDE表領域暗号化はオラクルのお客様に選ばれる暗号化方式となっています。

TDE列暗号化による機密データの保護

Oracle Advanced Securityには、TDE列暗号化も用意されています。TDE列暗号化は、アプリケーション表の特定のデータ（クレジット・カード番号や米国の社会保障番号など）の暗号化に使用できます。ユーザーは機密データや規制データが含まれるアプリケーション・スキーマ内の列を識別し、その列だけを暗号化します。この方法は、データベース表が大きく、暗号化が必要な列が少数で、その列を特定できている場合に便利です。

TDE列暗号化は、各問合せによって返されるデータセットが大きく異なるウェアハウス・アプリケーションで一般に有効です。TDE列暗号化によって暗号化されたデータは、バックアップ・メディアや破棄されたディスク・ドライブにも暗号化された状態で残るため、未承認のアクセスや、データベースを迂回する潜在的なデータ侵害を防ぐことができます。

パフォーマンス特性

TDEの暗号化操作は非常に高速で、関連するOracle Database機能との統合性に優れています。TDEでは、インテル® AES-NIやOracle SPARC T4以降のプラットフォームで使用可能なCPUベースのハードウェア暗号化アクセラレーションを利用して、パフォーマンスを著しく向上させています。TDE表領域暗号化のブロック・レベル操作の場合、データベースのバッファとキャッシュによって、パフォーマンスがさらに上がります。表領域暗号化は、Oracle Advanced Compressionとシームレスに統合されているため、暗号化の前に圧縮が行われます。また、表領域暗号化は、Oracle Exadataの高度なテクノロジー（Exadata Hybrid Columnar Compression（EHCC）やSmart Scanなど）と統合されているため、特定の暗号化処理をストレージ・セルにオフロードして、高速にパラレル実行できます。

組込みの鍵管理

鍵管理は、暗号化ソリューションのセキュリティに不可欠です。Oracle Advanced SecurityのTDEには、データ暗号化鍵とマスター暗号化鍵で構成される、標準の2層の鍵管理アーキテクチャがあります。データ暗号化鍵はデータベースによって自動的に管理され、次に、マスター暗号化鍵によって暗号化されます。マスター暗号化鍵は、Oracle Wallet（鍵を保護する標準ベースのPKCS12ファイル）内、またはOracle Key Vault（業界標準OASIS Key Management Interoperability Protocol（KMIP）準拠の一元管理鍵管理プラットフォーム）内のデータベースの外部で保存および管理されます。マスター鍵と暗号化データを別々に保管することで、攻撃を軽減できます。クリア・データにアクセスするには、鍵と暗号化データの両方を個別に攻撃することが必要になるためです。

また、2層の鍵アーキテクチャによって、すべての機密データを再度暗号化しなくても、マスター鍵をローテーションできます。

Oracle Database 18cでは、ユーザーが規制要件に対応し、社内ポリシーに準拠できるようにするため、Bring Your Own Key（BYOK）のサポートが開始されました。この機能により、自分のユーザー生成鍵をAdvanced Securityオプションの透過的データ暗号化のマスター暗号化鍵として使用できます。それらの外部鍵は、TDEによって直接取り込まれるようにするか、TDE有効データベースで、後で使用できるようOKVにバッチアップロードすることができます。

Oracle Databaseには専用のSYSKM権限があり、TDEの初期化、マスター・キーのローテーション、キーストア・パスワードの変更などのすべての鍵管理操作を実行可能です。このロールは、指定のユーザー・アカウントに任意で委任して、これらの機能の役割を分離できます。

以下の図のように、Oracle Enterprise Managerには、TDEマスター鍵の作成、ローテーション、管理を行うための便利なグラフィカル・ユーザー・インタフェースがあります。

Oracle Key Vaultは、地理的に散在するデータセンター全体にわたって最大16のアクティブなOKVインスタンスをクラスタ化することによって鍵の可用性を維持する、エンタープライズ・グレードの唯一の鍵管理プラットフォームです。フルスタックのセキュリティ強化ソフトウェア・アプライアンスであり、暗号化鍵、Oracle Wallets、Javaキーストア、ACFSボリューム暗号化鍵、Solaris暗号化鍵、資格署名ファイルを一元管理することができます。Oracle Key Vaultは、Oracle DatabaseおよびMySQL TDEと連携して、作成、ローテーション、有効期限などのTDEマスター鍵の管理を自動化します。Oracle Key Vaultは、直接ネットワーク接続上のTDEマスター鍵を一元管理して、ローカル・ウォレット・ファイルを不要にし、定期的なパスワード・ローテーション、ウォレット・ファイルのバックアップ、ウォレット・ファイルのリカバリなどのウォレット・ファイルの管理に関する運用およびセキュリティ上の難問を軽減します。Oracle Key VaultとTDEを併用することにより、サイトでは、運用効率を改善し、TCOを削減し、一貫した鍵管理ポリシーを適用しながら、TDEデプロイメントをさまざまな拠点における数百数千の規模のデータベースに拡張することができます。RESTful APIでは、OKV管理者によるそれ以上の介入なしに、現在または将来の任意の数のTDE有効データベースのセキュアな自動化オンボードが許容されます。

Oracle Key Vaultは、nCipherおよびSafenet（現在のThales）製の使用者の多いハードウェア・セキュリティ・モジュール（HSM）とも統合して、OKVをロック解除する秘密鍵が耐改ざん性のある特殊なFIPS 140-2レベル3認定ハードウェア・モジュールに保存される信頼の起点（RoT）関係を確立します。

Oracle Key Vaultはハイブリッド・クラウド・デプロイメントをサポートするので、Oracle Cloudに移行する組織は、Oracle Key Vaultを使って、クラウドとオンプレミス双方のデータベースでTDEデプロイメントをサポートできます。

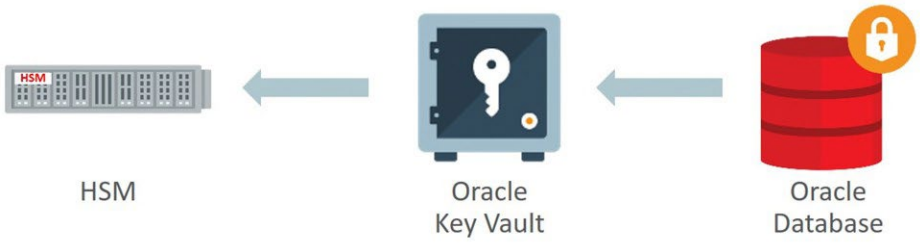

図3：TDEの信頼の起点としてのOracle Key VaultとHSM

暗号化による一般的な運用アクティビティへの影響

日常的な必須のデータベース運用アクティビティが適切に実行されていないと、迂回が簡単になり、機密データが漏えいしてしまう可能性があります。このようなアクティビティの例としては、データベースのバックアップとリストア、データの移動、高可用性クラスタリング、レプリケーションなどがあります。

Oracle Advanced SecurityのTDEとの統合例

データベース・テクノロジー	統合ポイントの例	TDEのサポート
高可用性クラスタ	Oracle Real Application Clusters（Oracle RAC）、Oracle Data Guard	✓
バックアップとリストア	Oracle Recovery Manager、Oracle Secure Backup	✓
エクスポートとインポート	Oracle Data PumpのExportとImport	✓
データベース・レプリケーション	Oracle GoldenGate	✓
プラガブル・データベース	Oracle Multitenant	✓
エンジニアド・システム	Oracle Exadata Smart Scan	✓
ストレージ管理	Oracle Automatic Storage Management（ASM）およびASM Cluster File System（ACFS）	✓
データ圧縮	Oracle Standard/Advanced/Hybrid Columnar Compression	✓

Oracle Advanced SecurityのTDEは、このような必須のデータベース運用アクティビティをサポートしており、データを暗号化された状態にしておくことができます。表領域暗号化は、Oracle Recovery Manager（バックアップとリストア）、Oracle Data Pump（データの移動）、Oracle Data Guard（冗長性とフェイルオーバー）、およびOracle GoldenGate（レプリケーション）に統合されています。また、TDEは、データベースの内部機能（REDOなど）に統合されており、ログでのデータ漏えいの危険性を防止します。このようにデータベース暗号化を完全統合することで、複雑な実際の環境で、運用プロセスのギャップを利用した迂回攻撃に対して保護しながら、ソリューションを簡単にデプロイできます。

Oracle Database 19cのTDEには、クリア・テキストから暗号化された表領域への表領域変換を実行する場合のオプションが2つあります。停止時間を作らずに変換を実行しなければならないデプロイメントの場合、オンライン表領域暗号化をバックグラウンドで実行して、システム操作を維持しながら、表領域をクリア・テキストから暗号化テキストに変換します。また、TDEでは、ストレージ・オーバーヘッドを生じさせずに表領域を効率的に変換するオフライン表領域変換モードも利用できます。

Data Redactionによる機密データの公開制限

プライバシやコンプライアンスには、アプリケーションでのデータ公開を管理するためのコスト効率の高い方法が必要です。スマートフォン・デバイスやタブレット・デバイスの保有により、機密データ公開の問題の緊急性が増しています。従来のオフィス環境以外でのデータ・アクセスが一般的になっているためです。従来のアプリケーションでも、機密データの漏えいを軽減するには包括的なソリューションが必要です。たとえば、コール・センターのアプリケーションの場合、顧客のクレジット・カード情報と個人識別情報がコール・センターのオペレーター用に画面表示されます。このような情報の公開は、正規のアプリケーション・ユーザーに対する場合であっても、個人情報保護違反となり、データを不要なリスクにさらす可能性があります。

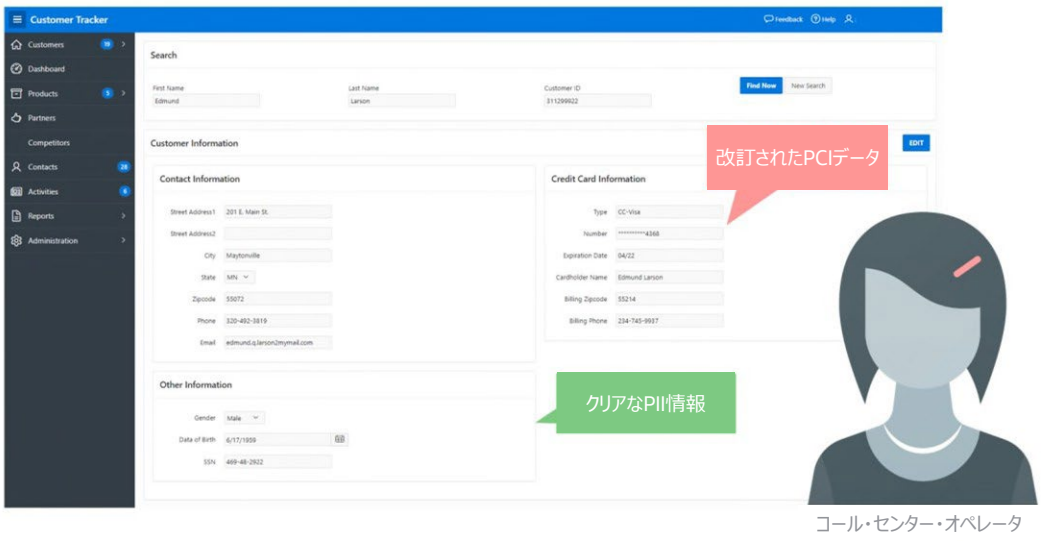

図4：コール・センター・アプリケーションに表示されるクリアな情報と改訂された情報

Oracle Advanced SecurityのData Redaction

Oracle Advanced SecurityのData Redactionでは、データベースの問合せ結果内の機密データがアプリケーションで表示される前に、選択的にその場で改訂できます。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。保存データは変更されないままですが、表示データはデータベースの外に出る前に、その場で変換、改訂されます。Data Redactionによって機密情報の公開を減らし、機密情報がアプリケーション・ページに公開されてしまう可能性があるアプリケーションの欠陥の悪用を防ぐことができます。これは、アプリケーションの大幅な変更なしで機密データの公開を制限する必要がある、新規と従来の両方のアプリケーションに非常に適しています。Oracle Data Redactionは、レポート・アプリケーションと読み取り専用の他のアプリケーションに特に適しています。

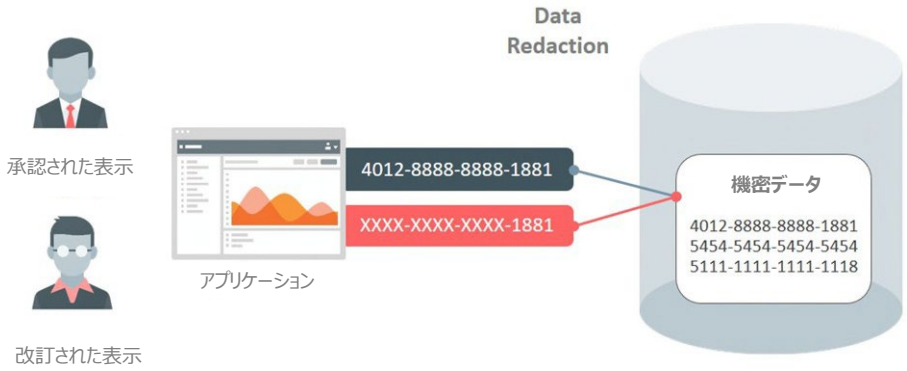

図5：Data Redactionを使用した、アプリケーションで表示される機密データの改訂

ポリシーと変換

Oracle Advanced SecurityのData Redactionは、指定した列のすべてのデータを改訂したり、特定のデータ箇所を保持したり、交換データをランダムに生成したりする、さまざまな変換をサポートします。サポートされるデータ変換の例は、次のとおりです。

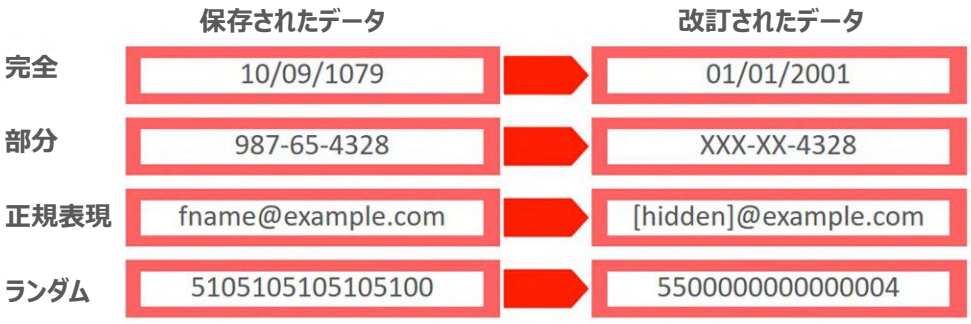

図6：Data Redactionによる変換の例

Data Redactionでは、データベースやアプリケーション自体から入手可能な豊富なランタイム・コンテキストを利用して、宣言的なポリシー条件に基づき、業務上必要な決定を行います。

たとえば、ユーザー識別子、ユーザー・ロール、クライアントIPアドレスなどです。

Oracle Application Express（Oracle APEX）、Oracle Real Application Security、およびOracle Label Securityから入手可能なコンテキスト情報も利用して、リダクション・ポリシーを定義できます。ポリシー条件では、Oracle APEXが自動的に追跡するアプリケーション・ユーザーとアプリケーション識別子を利用できるため、Oracle APEXアプリケーションのリダクションは簡単です。

Data Redactionポリシー内で複数のランタイム条件を組み合わせ、改訂の実行時期について細かく制御できます。このポリシーはデータベース内で保存および管理され、有効になるとすぐに実施されます。

パフォーマンス特性

高速パフォーマンスは、Data Redactionにとって非常に重要です。通常は、ターゲット・データベースが本番システムであるためです。ディスク、キャッシュ、バッファに保存されているデータを変更することなく、データを実行時にその場で変換する必要があります。この変換は本番環境で実行され、頻繁に繰り返されるため、パフォーマンス・オーバーヘッドは小さくなるはずです。

Data Redactionの重要なパフォーマンス特性の1つは、実証済みの高パフォーマンスでのデータ変換のみをサポートする点です。これは、本番以外の環境でのデータ変換に使用できる、実行可能なすべての操作のサブセットです。この特定のサブセットによって、長期間の実行やプロセッサに負荷がかかる操作を回避できます。

Data Redactionはまた、Oracle Databaseのパフォーマンス最適化を利用できます。これは、データベース・カーネルの一部である場合にのみ可能です。この実装によって、データ変換が高速なインメモリ計算になります。ポリシー情報はメモリ内でキャッシュ化され、ポリシー式は1回の実行で1回だけ評価されるため、行あたりのパフォーマンスに影響はありません。

セキュリティに関する考慮事項

Data Redactionをデータベース・カーネルの一部にすることのもう1つの利点は、セキュリティの強化です。干渉される可能性のあるプロキシに依存していることが原因で、他の改訂技法にとって問題となる潜在的な脆弱性がこの実装によって回避されます。また、カーネル内のData Redactionによって、他のセキュリティ対策が危うくなっても引き続き機密データを保護できます。たとえば、攻撃がアプリケーションやデータベースの他の予防措置を迂回しても、ポリシー内のランタイム条件によって機密データを継続的に改訂することで、SQLインジェクション攻撃の影響を軽減することができます。

また、Data Redactionによって、ポリシーのない新しい表へのデータ・コピーによって改訂ポリシーを迂回するといった、明白な漏えい原因を回避できます。

改訂済みのデータに影響する特定の大量コピー操作は、デフォルトでブロックされます。この動作は、Data Redactionの非適用権限によって、必要に応じてオーバーライドできます。

Data Redactionを使用して、データベースの特権ユーザー（データベース管理者など）が機密データをうっかり見てしまうことを防ぐことはできます。ただしData Redactionの基本的な目的は、ソフトウェア・アプリケーションに表示されるデータをリダクションすることです。Data Redactionによって、特権ユーザーがデータベースに直接接続して、機密データの一部に戻る非定型問合せを実行することを防ぐことはできません（つまり、徹底的な非定型問合せやその他の推論攻撃を止めることはできません）。ただし、Data Redactionは、データベースの特権ユーザー（データベース管理者など）によるアクセスを制御、監視するOracle Databaseセキュリティ・ソリューションと完全に互換性があります。Data Redactionは、Oracle Database VaultやOracle Audit Vault and Database Firewallなどの他のソリューションとともにデプロイして、多層防御セキュリティを実現できます。また、Data Redactionをデータベース暗号化で使用して、TDEを強力に補完することもできます。

Data Redactionの簡単なデプロイ

Data Redactionは、コマンドラインAPIかOracle Enterprise Managerを使用して、既存のアプリケーション用に簡単にデプロイできます。コマンドラインAPIは、保護対象の列、変換の種類、条件を使用するPL/SQLプロシージャです。Oracle Enterprise Managerには便利なPolicy Expression Builderがあり、管理者が既存のアプリケーションに改訂ポリシーを定義して適用できます。以下のように、Policy Expression Builderのダイアログに従って、アプリケーション、データベース、APEXフレームワーク、およびその他のデータベース・セキュリティ・ソリューションから取得したコンテキストを使用するポリシー条件を作成できます。

図7：Oracle Enterprise ManagerのPolicy Expression Builderを使用したData Redactionポリシーの作成

また、Oracle Enterprise Managerでは、事前定義されている列テンプレートを使用して、一般的な機密データ（クレジット・カード番号や米国の社会保障番号など）を改訂できます。Oracle Enterprise ManagerのSensitive Data Discoveryによって、複雑なアプリケーション・スキーマ内で改訂対象の列を特定できます。

Data Redactionがデプロイしやすいもう1つの理由は、アプリケーションとデータベースに対する透過性です。Data Redactionはアプリケーション透過性のために、アプリケーションや各種データベース・オブジェクト（表、ビュー、マテリアライズド・ビューなど）が頻繁に使用する列データ型をサポートしています。改訂された値では、元データの主要特性（データ型やオプションの書式設定文字）が保持されます。

ランダムな改訂値は、既存の列データによって定義されるデータ範囲から引き出されます。Data Redactionは、データベースへの透過性のため、必須のデータベース運用アクティビティには影響しないようになっています。データの移動（Oracle Data Pump）やデータベースのバックアップとリストア（Oracle Recovery Manager）などの管理タスクには影響しません。また、Oracle Real Application Clusters、Oracle Data Guard、Oracle GoldenGateなどのデータベース・クラスタ構成には干渉しません。Data Redactionによって、既存のデータベース・トリガーやOracle Virtual Private Database（Oracle VPD）ポリシーが干渉されることはありません。さらに、Data Redactionはデータベース・カーネルの一部であるため、別途インストールする必要はありません。

他の方法との比較

機密データの従来の改訂方法では通常、アプリケーションをコーディングしたり、データベース・サーバーの動作変更のためにサード・パーティ・ソフトウェアをインストールしたりする必要がありました。これらの方法には、Data Redactionと比べて重要な欠点があります。

新しいアプリケーション・ロジックのコーディング、既存のSQL文の変更、カスタム・アプリケーション・スクリプトのオーサリングなどを必要とする方法では、企業内で一貫性のない、ライフタイム期間にわたって保守コストの高い異種ソリューションが生まれる可能性が高くなります。また、カスタム・アプリケーション・コードや新規オブジェクトへのアクセスが適切に行われるよう、新規アプリケーションの開発を厳しく制御する必要があります。

また、コードでは、アプリケーションのパフォーマンスやセマンティックを保守しながら、リダクション・ポリシーが実施される状況下でのさまざまな要素も考慮する必要があります。

Oracle Databaseに新規コンポーネントを追加して、既存のコンポーネントを上書きし、プロキシを確立して、データベースの基本動作を変更する方法では、問題が発生しやすくなります。新規コンポーネントによって攻撃を受けやすくなるだけでなく、パフォーマンス・オーバーヘッドが発生したり、データベースの運用アクティビティに影響したりする可能性があり、アプリケーションが生成する複雑なデータベース問合せを変換しようとすると失敗する場合があります。これに対し、Data Redactionを使用してOracle Databaseカーネルで直接改訂すると、セキュリティとパフォーマンスが向上し、さまざまなデータベース構成、ユースケース、ワークロードとの互換性が上がります。

Oracle Multitenantアーキテクチャでの暗号化とリダクションの適用

Oracle Advanced Securityは、Oracle Databaseのマルチテナント・アーキテクチャを全面的にサポートしています。TDEとData Redactionの属性は、マルチテナント・コンテナ・データベース間の移動時には、自動的にプラガブル・データベース（PDB）に従います。改訂ポリシーを持つPDBを移動する場合、ポリシーはPDBの一部として新しいコンテナに直接送信されます。暗号化されたPDBを移動する場合、転送中は適切なセキュリティ分離を維持するため、そのPDBのTDEマスター鍵は、暗号化データとは別に送信されます。暗号化と改訂は、PDBの組込みと構成の完了直後に通常どおり再開されます。

Oracle Cloudでのデータ暗号化

Oracle Database Cloud Serviceデータベースでは、送信中のデータと保管中のデータをデータ・セキュリティで保護します。 送信中のデータのセキュリティは、ネットワークの暗号化によって確保します。保管中のデータのセキュリティは、Oracle Advanced Securityの透過的データ暗号化を使用して、データベースのデータ・ファイルとバックアップに保存されているデータの暗号化によって実現されます。デフォルトでは、Database Cloud Serviceデータベースでユーザーが作成するすべての新しい表領域が暗号化されます。 Oracle Cloudでのマルチテナント・デプロイメントの場合、TDEでは、プラガブル・データベースあたりキーストアを1つサポートします。 この設計により、テナント間の独立性を大きく高めることができ、独立した鍵管理操作を実現できます。

さらに、お客様が自分のマスター暗号化鍵を管理することができるようにするため、Oracle Key Vaultはハイブリッド・クラウド・デプロイメントをサポートしています。このシナリオでは、Oracle Key Vaultをオンプレミスにデプロイして、クラウドとオンプレミスの両方のデータベースでTDEデプロイメントに対応可能です。

結論

アプリケーションで公開されるデータは急速に増加しているため、企業は使用するデバイスやアプリケーションに関わらず、厳密に制御してデータを保護できるよう準備する必要があります。Oracle Database 19cはクラウドとオンプレミスで利用可能になり、データベースのデータ・セキュリティを実施する重要な制御手段によって、この複雑さを増す環境で機密情報を安全に保持できるように支援します。Oracle Database 19cのOracle Advanced Securityには、2つの重要な予防措置機能があります。透過的データ暗号化によって、保管データを暗号化し、ストレージの機密情報にアクセスするデータベース迂回攻撃を防ぎます。Data Redactionによって、定義済みポリシーに従ってデータベースの問合せ結果をその場で改訂し、アプリケーションでの機密情報の公開を減らします。これら2つの制御を組み合わせることで、マルチレイヤーでの多層防御の基盤が形成されます。これによりOracle Database 19cはさらに確立されます。

ORACLE

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