

Oracle Advanced Securityによる Oracle Database 12cでの暗号化とリダクション

Oracle ホワイト・ペーパー | 2017年3月



目次

はじめに	1
暗号化によるデータベース迂回の防止	2
Oracle Advanced Security 透過的データ暗号化	2
TDE 列暗号化による機密データの保護	3
TDE 表領域暗号化によるアプリケーション全体の保護	4
TDE データベース暗号化を使ったデータベースの保護	4
パフォーマンス特性	4
組込みの鍵管理	4
暗号化による一般的な運用アクティビティへの影響	6
Data Redaction による機密データの公開制限	6
Oracle Advanced Security の Data Redaction	7
ポリシーと変換	8
パフォーマンス特性	8
セキュリティに関する考慮事項	9
Data Redaction の簡単なデプロイ	9
他の方法との比較	10
Oracle マルチテナント・アーキテクチャでの暗号化とリダクションの適用	11
結論	11

はじめに

セキュリティ脅威の高まり、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。最初の米国漏洩通知法から10年余りが経過し、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もあり、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・デバイスに移行し、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り隙が生じ、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されかねません。このような危機の高まりによって、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。機密データを情報源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、情報源でのデータ・アクセス管理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 12c Release 2 では、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、こうした脅威に対応する新たなセキュリティ対策を提供します。

Oracle Database 12c の Oracle Advanced Security オプションには、保管データの暗号化と、アプリケーションで表示される機密データのリダクション(マスク)という、2つの必須の予防措置があります。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 Transparent Data Encryption (TDE, 透過的データ暗号化) によって、データベースを迂回し、オペレーティング・システム・レベルのデータファイル、バックアップやエクスポート・ファイルなどから直接機密情報を読み取ろうとした攻撃を防ぎます。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リダクションして、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。

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まさに、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手段の1つです。

Oracle Advanced Security の Transparent Data Encryption (TDE, 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。

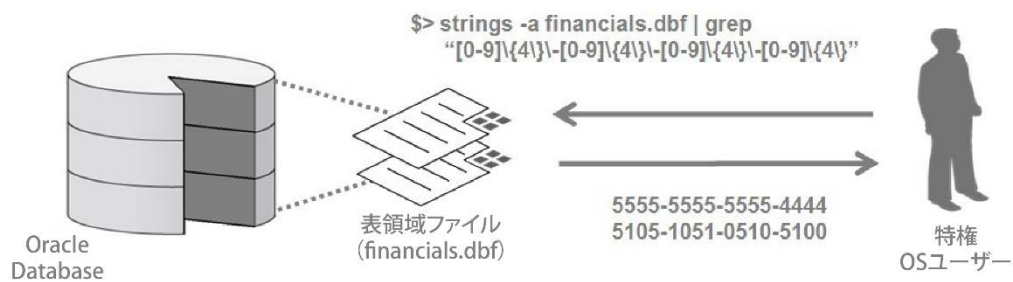


図1：Oracleデータベースの表領域ファイルからの顧客のクレジット・カード番号抽出

Oracle Advanced Security Transparent Data Encryption

透過的データ暗号化はデータベース内の最適なレイヤーに存在してデータベースの迂回を防ぎながら、アプリケーションの透過性を維持します。TDE は迅速にデプロイされ、個々のアプリケーション表の列、アプリケーションの表領域、または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。暗号化と復号化のためにアプリケーションの追加・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。もっとも重要なのは、TDE の組込みの 2 層暗号化鍵管理によって、鍵のライフ・サイクル全体の管理、便利なメタデータ属性を使ったライフタイム全体にわたる鍵の追跡、補助暗号化鍵のローテーション、停止時間なしの新しいマスター鍵への切り替えを実行できることです。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。

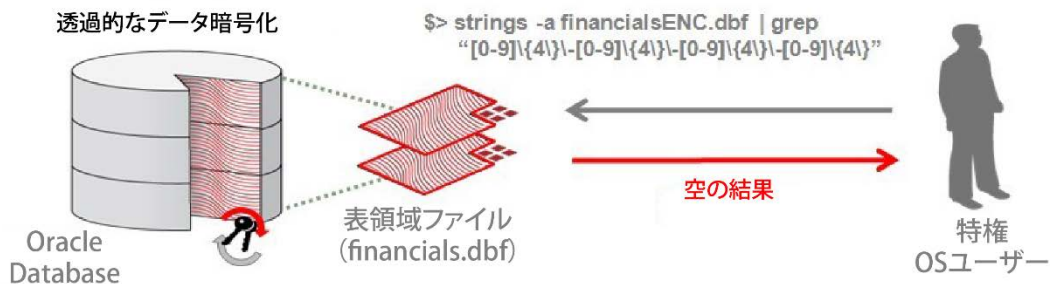


図2：透過的なデータ暗号化を使った暗号化によるデータベース迂回の防止

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、Oracle Advanced Compression、Oracle Real Application Clusters (Oracle RAC)、Oracle Recovery Manager (Oracle RMAN)、Oracle Multitenant、Oracle GoldenGate、Oracle Active 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 12c Release 2 の TDE は、SSL/TLS の認定暗号化スイートと TDE 暗号化を使用することで、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。

暗号化アルゴリズム	ハッシュ・アルゴリズム (オプション)
Advanced Encryption Standard (AES) の鍵の長さ： 128ビット、192ビット、256ビット	Secure Hash Algorithm 1 (SHA-1) ダイジェストの長さ： 160ビット
トリプル・データ暗号化規格 (TDES) の鍵の長さ： 168ビット	
地域的な暗号化アルゴリズム ARIAおよびSEED GOST	

図3：TDEが使用する標準の暗号化とハッシング・アルゴリズム

TDE列暗号化による機密データの保護

Oracle Advanced Security の TDE 列暗号化を使用して、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）を暗号化できます。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も便利です。Oracle Enterprise Manager の Sensitive Data Discovery によって、機密列が迅速に検索、識別されます。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。

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、基盤の表領域の暗号化により、アプリケーション表全体が保護されます。この方法では、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。同じデータベース内で、TDE 表領域暗号化と TDE 列暗号化を互いに独立して、または一緒に使用できます。TDE 列暗号化と TDE 表領域暗号化の両方の場合と同様に、潜在的な迂回攻撃への対策として、データはバックアップ・メディア上で保護され続けます。

TDEデータベース暗号化を使ったデータベースの保護

Oracle Advanced Security TDE のデータベース暗号化は、オラクルが提供する表領域 SYS、SYSAUX、TEMP、UNDO を含めたデータベース全体を保護します。Oracle Database 12c Release 2 の新機能であるこのアプローチにより、システムとメタデータの機密情報は暗号化とアプリケーション・データを介してずっと保護されます。

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 プラットフォームや Oracle SPARC T4/T5 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により、パフォーマンスが 5 倍以上に向上しています。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おり、圧縮後に確実に暗号化します。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) と統合されており、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。

組み込みの鍵管理

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データベースの外部、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 (一元的な鍵管理プラットフォーム) 内に保存され、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 Advanced Security は、マスター鍵のローテーションやキーストア・パスワードの変更など、すべての鍵管理操作を実行できる専用の SYSKM ロールを定義します。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・インターフェースがあります。

Oracle Key Vault は、セキュリティが強化されたフルスタックのソフトウェア・アプライアンスで、暗号化鍵、Oracle Wallet、Java キーストア、資格証明ファイルを一元管理します。Oracle Key Vault は TDE と連携して、作成、ローテーション、有効期限など TDE マスター鍵の管理を自動化します。

Oracle Key Vault は、マスター・リポジトリ内の Oracle Wallet の内容を項目化して保存します。ローカル・コピーを誤って削除した場合、またはパスワードを忘れてしまった場合に、マスター・リポジトリ内のこれらの項目をサーバーに復元することができます。また、Oracle Key Vault は、ローカル・ウォレット・ファイルを使う代わりに、直接ネットワーク接続を介して TDE マスター鍵を一元的に管理できるため、定期的なパスワードのローテーション、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、ウォレット・ファイルを個別に管理する面倒な手間がなくなります。Oracle Key Vault と TDE を併用すると、運用効率の改善、TCO の削減、一貫した鍵管理ポリシーの実現を達成しながら、サイトで TDE デプロイメントを数百または数千ものデータベースにスケーリングできます。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。

The screenshot shows the 'Master Keys' management interface in Oracle Enterprise Manager. It includes a toolbar with actions like Rekey, Create, Edit, Put Key In Use, Export, Import, and Detach. Below is a table listing keys with their status and timestamps. A 'Use Key' dialog box is overlaid, warning that this is a sensitive operation that will change the current Master Key 'in use'. The dialog shows the Keystore Location as '/etc/oracle/wallets/orcl', the Key Description as 'Q2 Key', and a masked password field.

Key Description (i.e. Tag)	Status		Creation Timestamp	Activation Timestamp
	In Use	Backed Up		
Q1 Key	✓		2012-12-28 04:20:34	2013-01-02 08:35:22
Q2 Key		✓	2012-12-28 04:21:20	
Q3 Key		✓	2012-12-28 04:22:05	
Q4 Key		✓	2012-12-28 04:23:01	

Use Key

Warning
This is a sensitive operation. It will change the current Master Key "in use".

Keystore Location: /etc/oracle/wallets/orcl

* Wallet Password: [Masked]

Key Description (i.e. Tag): Q2 Key

OK Cancel

図4 : Oracle Enterprise ManagerによるTDEマスター鍵の管理とローテーション

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。

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、Oracle Active Data Guard	✓
バックアップとリストア	Oracle Recovery Manager (Oracle RMAN) 、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	✓
プラグابل・データベース	Oracle Multitenantオプション	✓
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 (Oracle ASM)	✓
データ圧縮	Oracle Standard/Advanced/Hybrid Columnar Compression	✓

図5：Oracle Advanced SecurityのTDEとの統合例

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 Active 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 12c Release 2 の TDE 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ための 2 つのオプションを提供します。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、システム操作を止めることなく、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

プライバシー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。

コール・センター

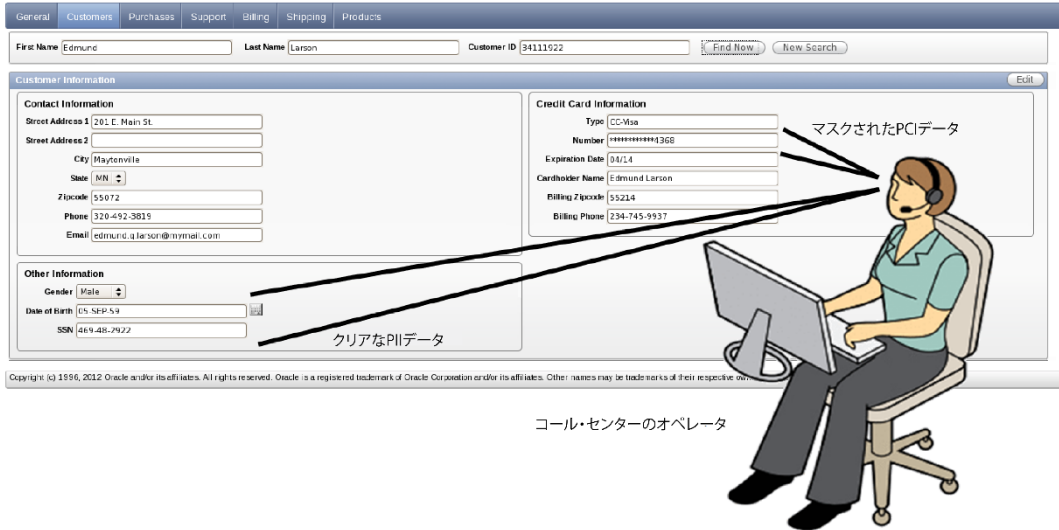


図6：コール・センター・アプリケーションに表示されるクリアな情報とリダクションされた情報 (PII: 個人特定情報、PCI: カード支払情報)

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、選択的にその場でリダクション(マスク)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、リダクションされます。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。

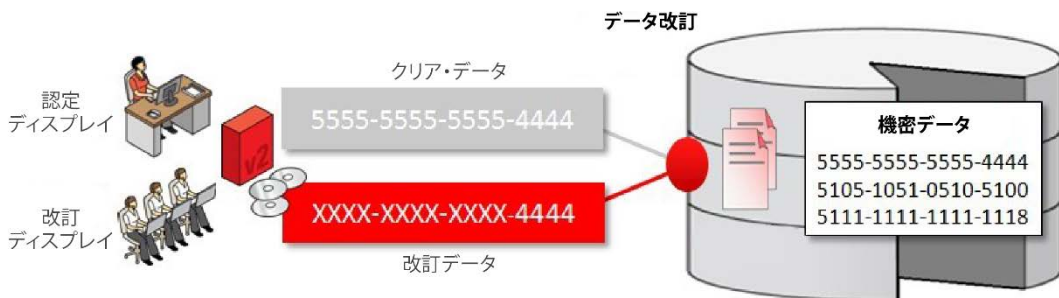


図7：Data Redactionを使用した、アプリケーションで表示される機密データのリダクション

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リダクションしたり、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。

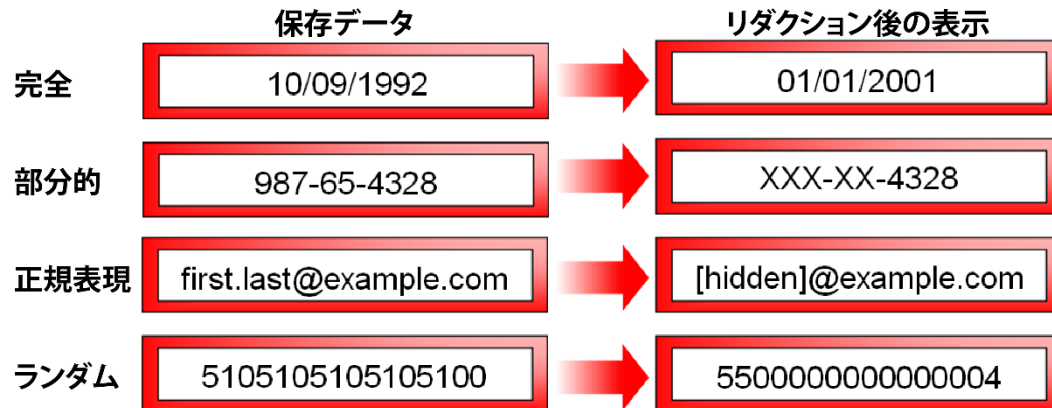


図8 : Data Redactionによる変換の例

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。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ポリシー条件で利用できるため、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て、リダクション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・オーバーヘッドを抑える必要が有ります。

Data Redaction の重要なパフォーマンス特性の 1 つは、実証済みの高性能なデータ変換のみを採用している点です。データ変換のなかには本番以外の環境でなら実行可能なものもありますが、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るサブセットを採用しています。

Data Redaction はまた、データベース・カーネルの一部として実装されているため、Oracle Database のパフォーマンス最適化を利用できます。この実装によって、データ変換が高速なインメモリで処理されます。ポリシー情報はメモリ内にキャッシュされ、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。アプリケーションなどの他の方法で個別に実装したリダクション(マスキング)によって発生しうる、潜在的な脆弱性を回避することができます。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く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リダクションすることで、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・コピーによってリダクション・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。リダクション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せん。ただし Data Redaction の本来の目的は、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、機密データの一部を返す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）も含めたアクセスを制御、監視する、他の Oracle Database セキュリティ・ソリューションと相互に連携します。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リダクション・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。

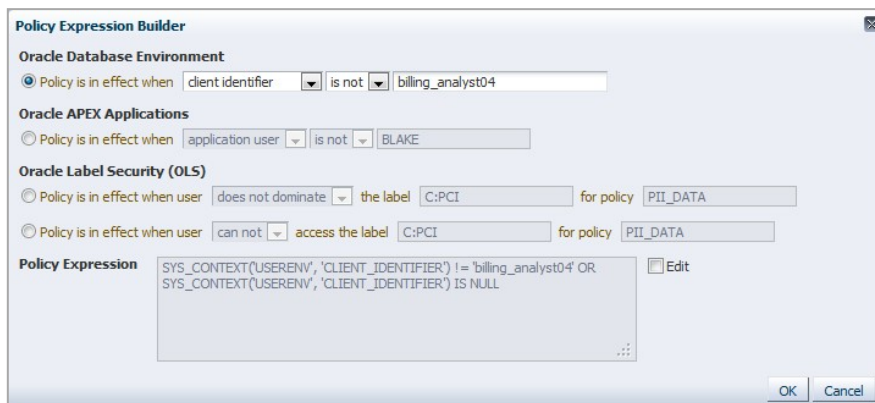



図9：Oracle Enterprise ManagerのPolicy Expression Builderを使用したData Redactionポリシーの作成



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）をリダクションできます。Oracle Enterprise Manager の Sensitive Data Discovery を使い、複雑なアプリケーション・スキーマのなかからリダクション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。リダクションされた値では、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。ランダムなリダクション値は、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 Active 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。また、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

従来、機密データをリダクションするために、多くの場合アプリケーションのコーディングや、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するやり方をしていました。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やり方では、結果的に、企業内で一貫性がなく、ライフタイム期間にわたって保守コストが高くつく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限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ます。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場合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 カーネルで直接リダクションすると、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マルチテナント・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 12c のマルチテナント・アーキテクチャを完全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。リダクション・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と一緒に移動します。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の独立性を維持するため、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。暗号化とリダクションは、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。




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おり、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、データ保護にむけ強力な統制が求められています。Oracle Database 12c Release 2 はクラウドとオンプレミスで利用可能になり、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、データベースのデータ・セキュリティを強固にする手段を提供します。

Oracle Database 12c Release 2 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リダクション(マスク)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。これが、Oracle Database 12c が世界でもっとも高度なデータベース・ソリューションである理由です。



CONNECT WITH US

-  blogs.oracle.com/oracle
-  facebook.com/oracle
-  twitter.com/oracle
-  oracle.com

Oracle Corporation, World Headquarters
500 Oracle Parkway
Redwood Shores, CA 94065, USA

海外からのお問い合わせ窓口
電話：+1.650.506.7000
ファクシミリ：+1.650.506.7200

Integrated Cloud Applications & Platform Services

Copyright © 2017, Oracle and/or its affiliates. All rights reserved. 本文書は情報提供のみを目的として提供されており、ここに記載される内容は予告なく変更されることがあります。本文書は、その内容に誤りがないことを保証するものではなく、また、口頭による明示的保証や法律による黙示的保証を含め、商品性ないし特定目的適合性に関する黙示的保証および条件などのいかなる保証および条件も提供するものではありません。オラクルは本文書に関するいかなる法的責任も明確に否認し、本文書によって直接的または間接的に確立される契約義務はないものとします。本文書はオラクルの書面による許可を前もって得ることなく、いかなる目的のためにも、電子または印刷を含むいかなる形式や手段によっても再作成または送信することはできません。

Oracle および Java は Oracle およびその子会社、関連会社の登録商標です。その他の名称はそれぞれの会社の商標です。

Intel および Intel Xeon は Intel Corporation の商標または登録商標です。すべての SPARC 商標はライセンスに基づいて使用される SPARC International, Inc. の商標または登録商標です。AMD、Opteron、AMD ロゴおよび AMD Opteron ロゴは、Advanced Micro Devices の商標または登録商標です。UNIX は、The Open Group の登録商標です。0317

Oracle Advanced Security による Oracle Database 12c での暗号化とリダクション
2017年3月



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