

Oracle Advanced Security

ORACLE
DATABASE **12^c**

Oracle Database 12c Release 2 (12.2) の Oracle Advanced Security には、機密性の高いアプリケーション・データの保護に不可欠な、業界をリードする暗号化機能とデータ改訂機能が搭載されています。Transparent Data Encryption 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。

ビジネス上のおもな利点

- 機密データを保護し、PCI-DSS、HIPAA、EU GDPR などの規制のデータ暗号化規定に簡単かつコスト効率の高い方法で準拠
- 機密データの開示による、データ侵害のビジネス・リスクに対処
- 暗号化されたデータは保護され、データ管理ライフサイクル全体にわたって使用可能
- 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ることで、導入コストと運用コストを削減
- すべてのアプリケーションおよびユーザーにわたってデータ改訂を一元管理することで、ガバナンスを向上
- Oracle Multitenant オプションの完全サポートにより、セキュアなデータ分離が可能

プライバシー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 が提供する予防的制御によって、多くの規制要件に対応し、データ侵害を防ぎ、プライバシー関連の情報を保護することができます。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、問合せ結果でデータベースから抽出される際にその場で取得、復号化、改訂されます。これら 2 つの機能は、プライバシー規制や、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ために重要です。

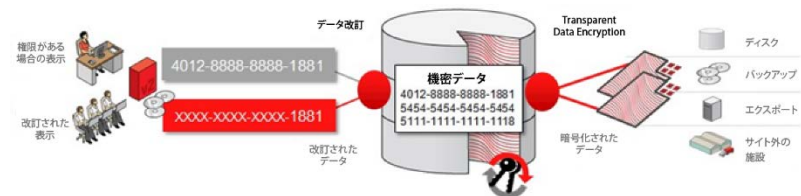


図1：Oracle Advanced Securityの概要

Transparent Data Encryption

Transparent Data Encryption (TDE) では、保管中の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迂回してデータベース・ファイルの内容を直接調べ、機密情報に直接アクセスすることを防ぎます。また、Transparent Data Encryption は、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、不適切な廃棄からも保護します。

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き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。

おもな機能

Transparent Data Encryption

- アプリケーションを変更することなく、データベース列、表領域、またはデータベース全体のアプリケーション・データを暗号化
- 既存の表領域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
- AES (128、192、および 256 ビット鍵) などの業界標準の暗号化アルゴリズム、および ARIA、SEED、GOST などの各国の暗号化アルゴリズムを使用
- Oracle Key Vault と連携し、数百もの暗号化データベースに効率的な鍵管理を提供
- インテル® AES-NI および Oracle SPARC T シリーズのハードウェア・アクセラレーション機能を利用
- データベース・テクノロジー (Oracle RMAN、Oracle ASM、Oracle RAC、Advanced Compression、Active Data Guard、GoldenGate など) と直接統合

データ改訂

- 実行中の改訂により、アプリケーションでの機密情報の開示を制限
- 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
- 正規表現を使用して 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 との直接統合

Transparent Data Encryption では Oracle Database のキャッシュ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、Transparent Data Encryption では、インテル® AES-NI および Oracle SPARC プラットフォーム (Oracle Exadata や SuperCluster など) の 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、実行が必要な暗号化操作の総数を減らしたりすることができます。

Transparent Data Encryption 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 ウォレットまたは Oracle Key Vault ではデータベースの外部に格納されます。鍵のライフサイクル全体にわたる、組込みの鍵管理機能には補助鍵ローテーションがあり、すべてのデータを再暗号化することによるオーバーヘッドはありません。

Transparent Data Encryption は簡単に導入でき、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。本番システムで既存の表領域を停止時間なしにオンラインで暗号化でき、メンテナンス期間中にストレージでのオーバーヘッドなしにオフラインで暗号化することもできます。また、Transparent Data Encryption は標準で Oracle Automatic Storage Management と連携し、AMS 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の改訂

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 によって、アプリケーションの変更が最小限で済みます。内部データベース・バッファ、キャッシュ、ストレージ内の実データは変更されず、変換されたデータがアプリケーションに戻される際に、元のデータ型と形式が維持されているためです。Data Redaction がデータベース操作アクティビティ (バックアップ、リストア、アップグレード、パッチなど) や高可用性クラスタに影響す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した方法とは異なり、Data Redaction の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。改訂形式ライブラリには、一般的なタイプの機密情報 (クレジット・カード番号、国民識別番号など) に適用できる事前構成済みの列テンプレートが用意されています。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。

オンプレミスとクラウドの企業データの保護

Transparent Data Encryption と Data Redaction は、多層防御手段のセキュリティ戦略の一部として簡単に導入および管理できます。Oracle Enterprise Manager の便利で包括的な管理コンソールを使用してポリシーを定義および適用できます。コマンドライン API も使用できます。

関連製品

Oracle Database 12c 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

Transparent Data Encryption 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、Transparent Data Encryption の表領域暗号化と Oracle Recovery Manager 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 を完全サポートしており、データベース・テナント間のセキュアなデータ分離を実現します。Transparent Data Encryption と Data Redaction の両方は、プラグブル・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、転送中のプラグブル・データベースを保護します。





Oracle Advanced Security は、データのライフサイクル全体にわたってアプリケーションの透過性を提供する、Oracle Database 向けの唯一のデータベース保護ソリューションです。パフォーマンスが低下したり、コンピューティング・リソースの拡張が必要になったりすることはありません。クラウドへの移行を準備している組織では、このソリューションにより、オンプレミスとクラウドの両方の資産に同じデータ保護ソリューションを利用できます。

お問い合わせ

Oracle Advanced Security について詳しくは、oracle.com を参照するか、+1.800.ORACLE1 でオラクルの担当者にお問い合わせください。



CONNECT WITH US

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

Integrated Cloud Applications & Platform Services

Copyright © 2016, 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、記載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。0116



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