

注：本書は情報提供のみを目的としています。下記の事項は、マテリアルやコード、機能の提供を確約するものではなく、また、購買を決定する際の判断材料とはなりません。本書に記載されている機能の開発、リリースおよび時期については、弊社の裁量により決定いたします。

ORACLE ADVANCED SECURITY

主な機能と利点



- SSN、クレジットカード番号、およびその他のプライバシー・データの透過的な暗号化
- 表領域の暗号化によるアプリケーション表全体の透過的な暗号化
- RMAN および TDE によるデータベース・バックアップ全体の暗号化
- SQL*Net ネットワーク・トラフィックの透過的な暗号化
- 厳密認証 (Kerberos、PKI、RADIUS) の有効化
- 規制順守 - PCI、SOX、HIPAA
- 標準準拠 (3DES 168、AES 256、SHA-1、x.509v3、PKCS #7/10/11/12、TLS 1.0)

Oracle Advanced Security は、ネットワーク上、バックアップ・メディア上、またはデータベース内の機密データを不正な開示から保護することにより、顧客の規制順守要件への対応を支援します。Oracle Advanced Security の Transparent Data Encryption は、既存のアプリケーションを変更する必要なく、業界で最も高度な暗号化機能を機密情報保護のために提供します。

Transparent Data Encryption

Oracle Advanced Security の Transparent Data Encryption (TDE) は、堅牢な暗号化ソリューションにより、オペレーティング・システム・レベルでの不正なアクセスや、ハードウェアまたはバックアップ・メディアの盗難による不正なアクセスから、機密データを保護します。TDE は、社会保障番号やクレジットカード番号などの個人情報を守ることに、プライバシーおよびペイメント・カード産業 (PCI) 要件に対処します。次のシンプルな `alter table` コマンドを使用することにより、管理者は既存のアプリケーション表内で機密データを暗号化できます。

```
SQL> alter table customers modify (credit_card_number encrypt)
```

ほとんどのデータベース暗号化ソリューションと異なり、TDE は既存のアプリケーションに対して完全に透過的で、トリガー、ビュー、または他のアプリケーションの変更は必要ありません。

データは、透過的に暗号化され、アプリケーション・ユーザーが認証に成功し、すべての認可チェックを通過した後に透過的に復号化されます。認可チェックには、ユーザーがアプリケーション表上で必要な `select` およ

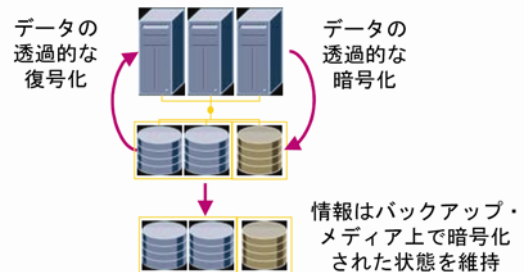


図 1 Transparent Data Encryption の概要

び `update` 権限の確認や、Oracle Database Vault、Oracle Label Security、および Oracle Virtual Private Database の適用ポリシーのチェックがあります。また、既存のデータベース・バックアップ手順を引き続き適用できます。この際、データはバックアップでも暗号化された状態が維持されます。データベースのバックアップ全体の暗号化では、TDE を Oracle RMAN と組み合わせて使用できます。

表領域の暗号化

Oracle Database 11g Release 1 の Oracle Advanced Security は、表領域の暗号化をサポートします。Oracle Enterprise Manager によって、またはコマンド・ライン上で表領域が作成されると、ファイルがファイル・システム上で暗号化されることを指定するオプションができます。新規のデータが `insert` コマンドまたは Oracle Data Pump を使用して新規の表領域に追加されると、表全体が透過的に暗号化されます。データベースが、暗号化された表領域からデータ・ブロックを読み取ると、データベースはデータ・ブロックを透過的に復号化します。

注：本書は情報提供のみを目的としています。下記の事項は、マテリアルやコード、機能の提供を確約するものではなく、また、購買を決定する際の判断材料とはなりません。本書に記載されている機能の開発、リリースおよび時期については、弊社の裁量により決定いたします。

ORACLE ADVANCED SECURITY

関連製品：

以下の製品は、セキュリティ、プライバシー、および規制要件を満たすための追加のセキュリティを提供します。

- Oracle Database 10g Release 2 - Oracle Database Vault
 - DBA および特権ユーザーからのアプリケーション・データの保護
 - アプリケーションおよびデータベースへのアクセス制御
 - データベースの変更に対する保護
- Oracle Label Security
 - ラベル・ベースのアクセス制御
 - マルチレベルのセキュリティ
 - 機密データの保護
 - ラベル要素による Oracle Database Vault との統合
 - 情報セキュリティにおける国際評価基準 (Common Criteria) EAL4 の評価
- Oracle Secure Backup
 - テープのバックアップ時のデータベースおよびファイル・システムの暗号化
 - Oracle Recovery Manager (RMAN) との統合および256ビットAESまでのサポート

ハードウェア・セキュリティ・モジュール

Oracle Database 11g Release 1 では、TDE は TDE マスター暗号化キーをハードウェア・セキュリティ・モジュール (HSM) デバイス上で外部から格納するように拡張されました。これにより、TDE マスター・キーをより確実に保護できるようになります。Oracle Database 11g Release 1 は、PKCS#11 インタフェースを使用して HSM デバイスと通信を行います。マスター・キーの既存のウォレット・ベースのストレージ・メカニズムに対するサポートは継続されます。

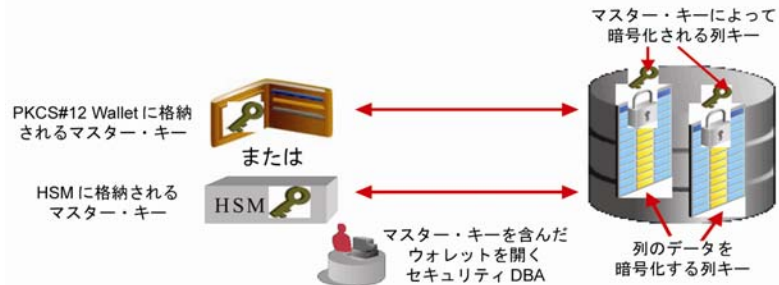


図 2 TDE キー管理アーキテクチャ

転送中のデータに対する強力な保護

Oracle Advanced Security は、Oracle Database とのすべての通信を保護するための配置しやすい包括的なソリューションを提供し、ネイティブのネットワーク暗号化および SSL ベースの暗号化を提供します。公開鍵インフラストラクチャ (PKI) を導入している企業では、SSL ベースの暗号化および認証を使用できます。Oracle Database 10g Release 1 では、TLS 1.0 プロトコル (AES 暗号スイートを含む) に対するサポートが導入されています。Oracle Database では、暗号化を無効にしたクライアントからの接続を拒否するように設定できます。また、柔軟な配置を実現するために、暗号化されていない接続を任意で許可することもできます。Oracle Network Configuration 管理ツールを使用すると、アプリケーションを変更しなくてもネットワーク・セキュリティの設定が簡単に行えるため、企業はネットワーク暗号化を容易に導入できます。

厳密認証によるパスワード・ベース認証の置換え

Oracle Advanced Security は、Kerberos、PKI、RADIUS といった厳密認証サービスのデータベースをサポートします。証明書失効リストは、Oracle Internet Directory または CRL Distribution Points を使用してファイル・システムに格納できます。スマートカードのサポートは、PKCS #11 標準を使用して提供されます。資格証明は、PKCS #12 標準を使用して共有できます。

Copyright 2007, Oracle.All Rights Reserved.

本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。本書は一切間違いがないことを保証するものではなく、さらに、口述による明示または法律による黙示を問わず、特定の目的に対する商品性もしくは適合性についての黙示的な保証を含み、いかなる他の保証や条件も提供するものではありません。オラクル社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。本文書はオラクル社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 は米国 Oracle Corporation 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。