

# Oracle DBA & Developer Days 2011

日本オラクル、今年最大の技術トレーニングイベント

2011年11月9日(水)～11月11日(金) シェラトン都ホテル東京



## ORACLE®

### 不正アクセスからデータを守れ！！

### ～Oracle Databaseの特権ユーザ管理、機密情報の安全な管理、暗号化

日本オラクル株式会社 製品戦略統括本部 戦略製品ソリューション本部  
シニアセールスコンサルタント 福田 知彦

以下の事項は、弊社の一般的な製品の方向性に関する概要を説明するものです。また、情報提供を唯一の目的とするものであり、いかなる契約にも組み込むことはできません。以下の事項は、マテリアルやコード、機能を提供することをコミットメント(確約)するものではないため、購買決定を行う際の判断材料になさらないで下さい。オラクル製品に関して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されます。

OracleとJavaは、Oracle Corporation 及びその子会社、関連会社の米国及びその他の国における登録商標です。文中の社名、商品名等は各社の商標または登録商標である場合があります。

# 昨今の不正アクセス事件のトレンド

## なりすまし

ID盗難(フィッシング)

## 脆弱性攻撃

SQLインジェクション  
OS脆弱性  
ミドルウェア脆弱性

## 境界防御を迂回する攻撃

標的型メール  
USBメモリ

## 内部不正

社員  
運用委託業者  
開発ベンダー

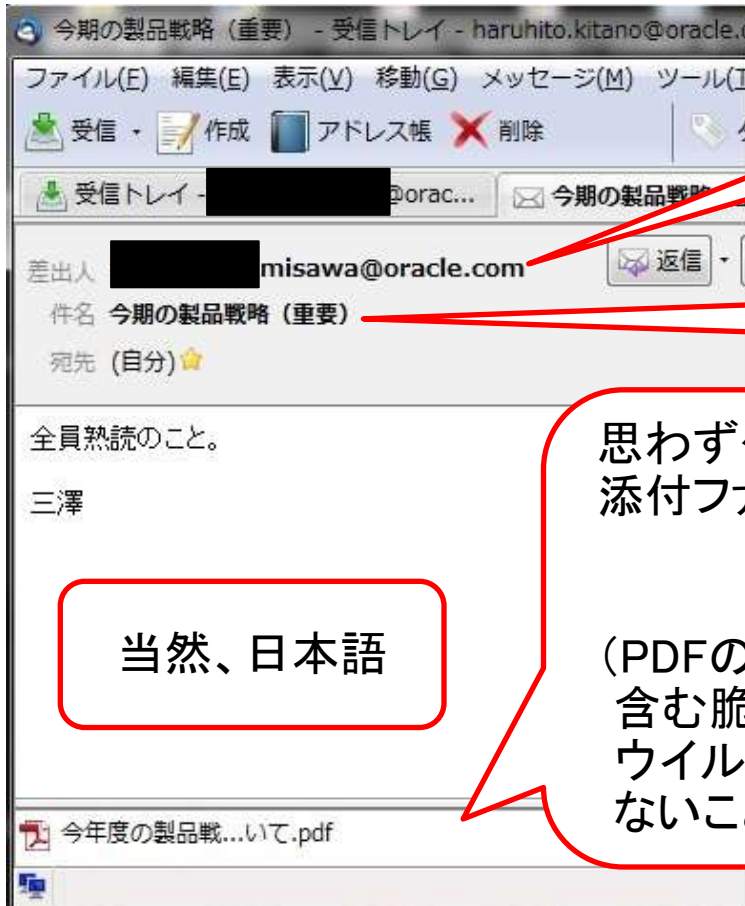
組織的  
標的型

個人情報  
技術情報  
知的財産

# 境界防御を迂回する攻撃

## Advanced Persistent Threats (APT)

たとえば、こんなメールがきても開かない自信はありますか？



実在の人物  
(特に上司・役員など...)

いかにも業務に関係が  
ありそうなタイトル

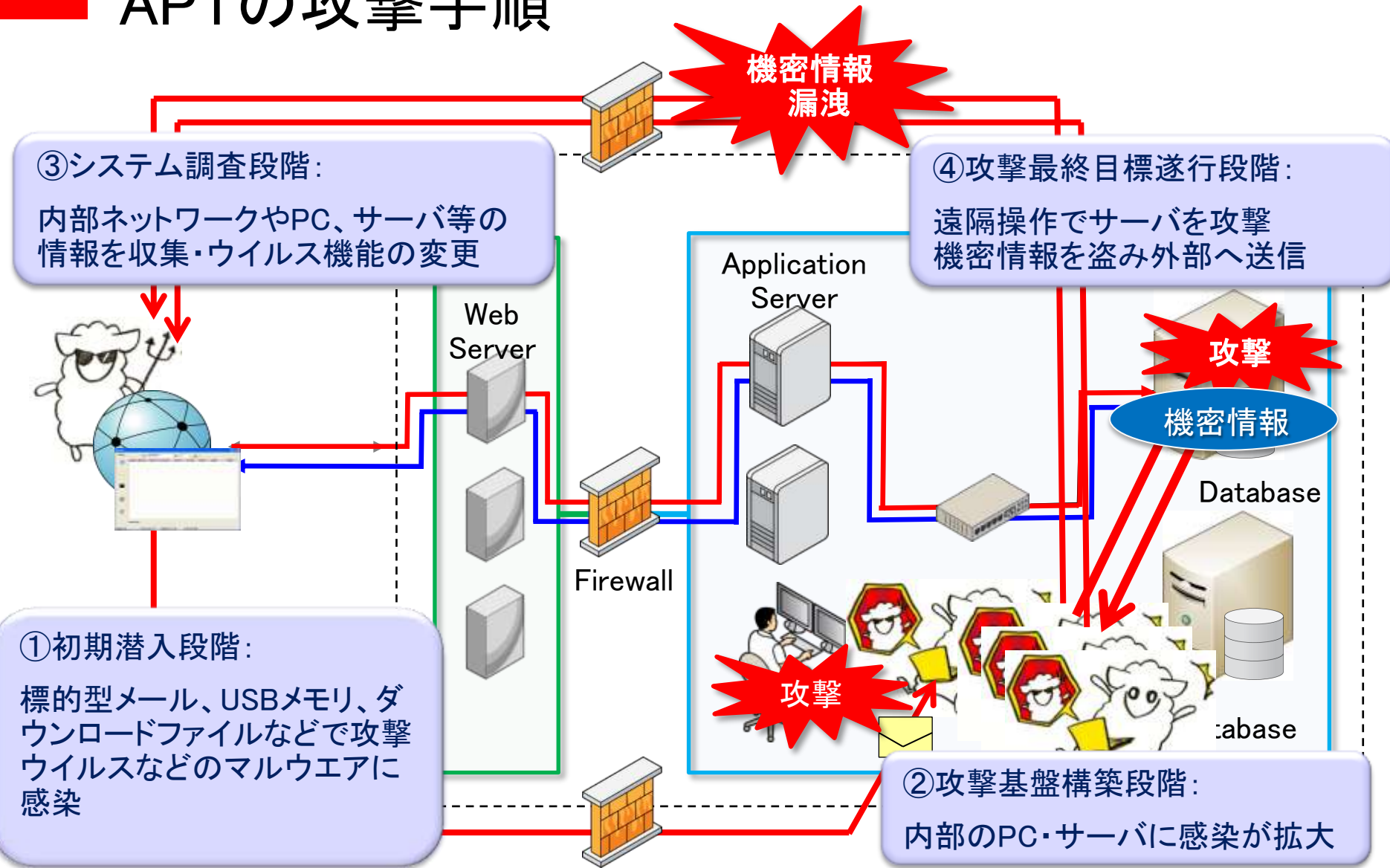
思わずクリックしたくなる  
添付ファイル...

当然、日本語

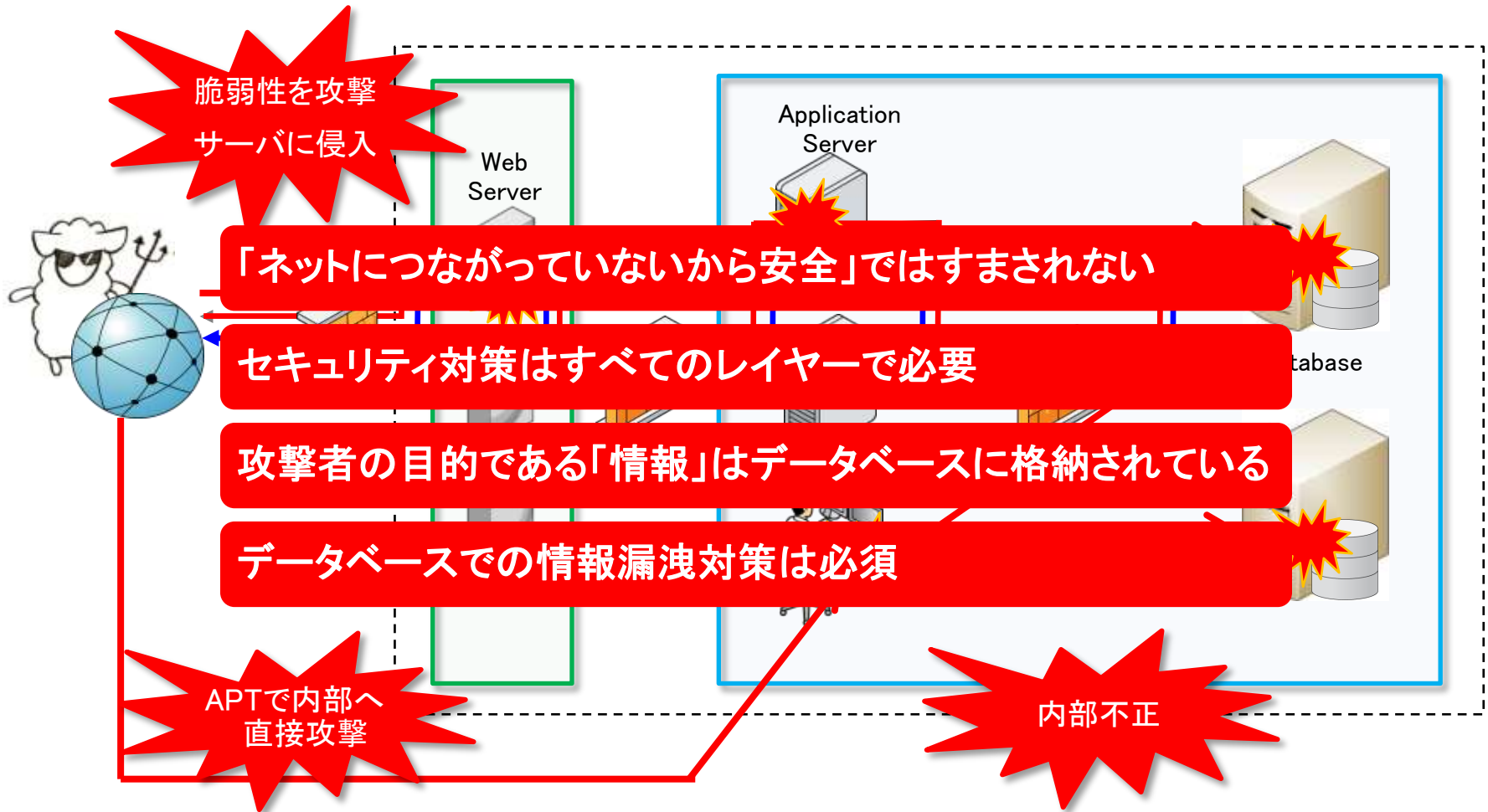
(PDFの割合が多く、ゼロデイを  
含む脆弱性を攻撃する。  
ウイルス対策ソフトで検出でき  
ないこともある)



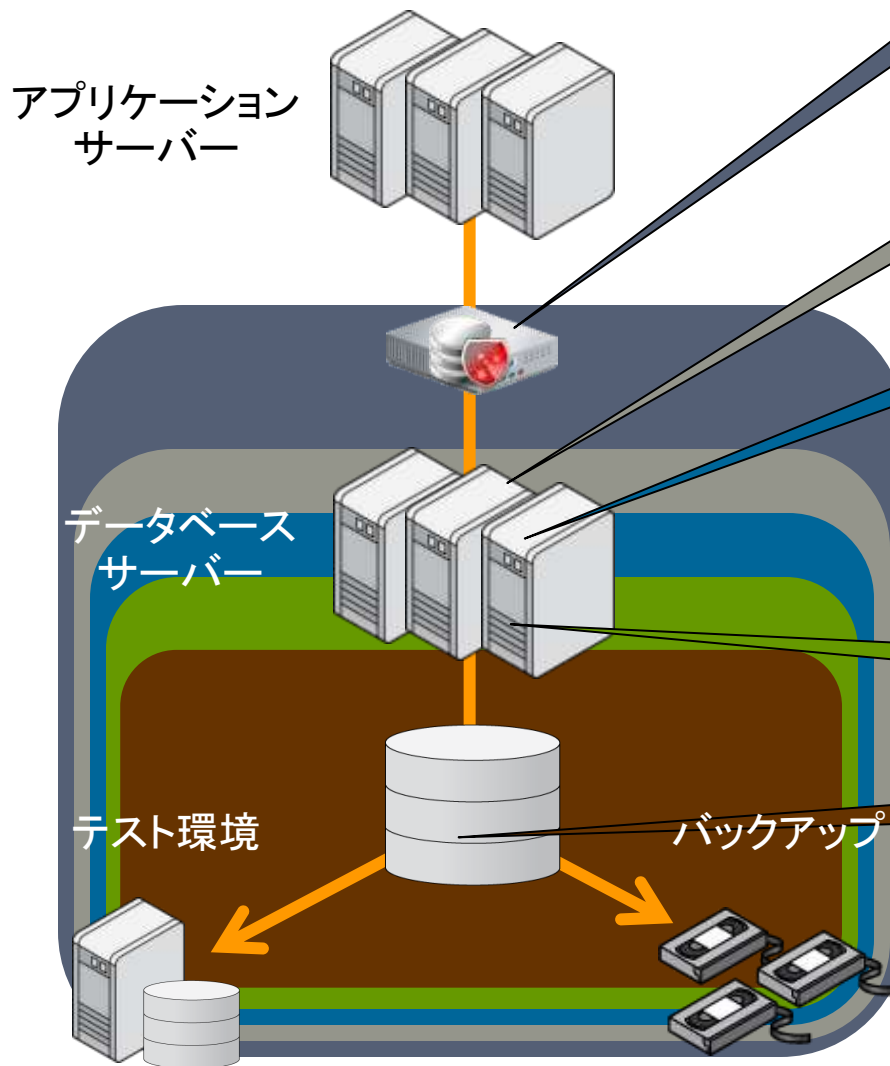
# APTの攻撃手順



# 境界防御の限界 ～ 狙われるデータベース



# Oracle Databaseのセキュリティソリューション



## モニタリング・ブロッキング

- 不正アクセス検知・防御・監査レポート自動化 (Oracle Database Firewall)
- 接続元サーバーの制限 (Listener)

## 認証

- ユーザー認証

## アクセス制御

- 権限 (システム権限・オブジェクト権限)
- 行や列レベルでのアクセス制御 (仮想プライベートデータベース)
- 特権ユーザー管理・職務分掌 (Oracle Database Vault)

## 監査

- データベース監査機能 (標準監査・ファイングレイン監査・DBA監査)

## 暗号化・マスキング

- 格納データ暗号化 (Oracle Advanced Security)
- ネットワーク通信暗号化 (Oracle Advanced Security)
- バックアップデータ暗号化 (Oracle Advanced Security)
- 安全なテストデータの作成 (Oracle Data Masking)

# セキュリティ担保の考え方

- ✗ リスクをゼロにする
- 許容できるレベルにリスクを軽減する

多層防御

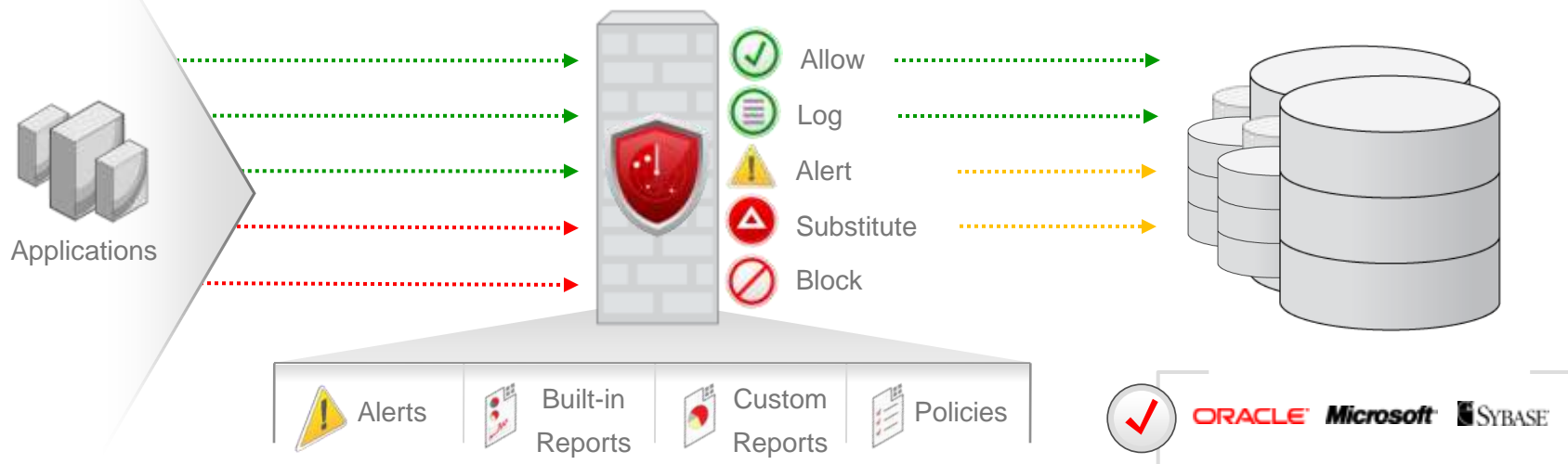
検知(Detection)と予防(Prevention)



# Oracle Databaseのセキュリティソリューション

- モニタリング・ブロッキング
- 認証
- アクセス制御
- 監査
- 暗号化・マスキング
- Oracle Database Firewall
- Listener

# Oracle Database Firewallによる データベース直前での防御



- ・ アプリケーションとデータベースの間に位置し、ネットワークトラフィックからSQL文を収集・文法解析
  - ・ **ブロッキング**: SQLを解析し、危険と判断されるものはブロックや警告を行うことで内部不正・外部攻撃からデータベースを保護
  - ・ **モニタリング**: 収集したSQLをログとして記録・管理・レポートイング

# Listenerを利用した接続元サーバー制限

- リスナーへの接続を、ホワイトリストまたはブラックリスト形式でアクセス制御可能

sqlnet.oraに以下のパラメータを設定

接続制限の有効化 (デフォルト値はNO)

TCP.VALIDNODE\_CHECKING=YES

ホワイトリスト形式での接続許可リストの指定

TCP.INVITED\_NODES=(apsrv1.jp.oracle.com, apsrv2.jp.oracle.com, 192.168.56.2)

ブラックリスト形式での接続拒否リストの指定 (INVITED\_NODEの設定が優先)

TCP.EXCLUDED\_NODES=(192.168.54.\*, apserv3.jp.oracle.com)

TCP.INVITED\_NODESを指定する場合、リスナーを起動するサーバーを必ず追加する必要があります。  
設定後に設定の再読み込み(lsnrctl reload)が必要です。

「Net Servicesリファレンス」マニュアルの「sqlnet.oraファイルのパラメータ」も併せて参照してください。  
[http://download.oracle.com/docs/cd/E16338\\_01/network.112/b56287/sqlnet.htm#i500318](http://download.oracle.com/docs/cd/E16338_01/network.112/b56287/sqlnet.htm#i500318)



# Oracle Databaseのセキュリティソリューション

- モニタリング・ブロッキング
- **認証**
- アクセス制御
- 監査
- 暗号化・マスキング
- 外部パスワードストア
- DBAの認証

# 外部パスワードストア

- Oracle Walletにユーザー名・パスワードを安全に格納

```
$ sqlplus /@<接続文字列>
```

- バッチや運用スクリプトにユーザー名・パスワードを記載不要

sqlnet.oraに以下のパラメータを設定

## Walletの場所の指定

```
WALLET_LOCATION =  
  (SOURCE=(METHOD=FILE)(METHOD_DATA=  
    (DIRECTORY=<Wallet格納ディレクトリ>)))
```

## Walletの優先利用の設定

```
SQLNET.WALLET_OVERRIDE=TRUE
```

Wallet格納ディレクトリのアクセス権限は「700」とする必要があります。

# 外部パスワードストア（続き）

## Walletの作成と設定

### Walletの作成

```
$ mkstore -wrl <Wallet格納ディレクトリ> -create
```

（ここでWalletのパスワードを設定します）

### Walletへの資格証明の追加

```
$ mkstore -wrl <Wallet格納ディレクトリ> -createCredential <接続文字列> <ユーザー名>
```

（ここで対象データベースへのログインパスワードとWalletのパスワードの入力を求められます）

「セキュリティガイド」マニュアルの「パスワード資格証明用の安全性の高い外部パスワード・ストアの管理」も併せて参照してください。

[http://download.oracle.com/docs/cd/E16338\\_01/network.112/b56285/authentication.htm#CHDHGAIJ](http://download.oracle.com/docs/cd/E16338_01/network.112/b56285/authentication.htm#CHDHGAIJ)

# DBAのOS認証の禁止

- OSのDBAグループに所属するユーザーはパスワードを指定せずにSYSDBAとして接続可能

```
$ sqlplus / as sysdba
```

- 以下の方法でこの認証方式でのログインを禁止可能
  - SQLNET.AUTHENTICATION\_SERVICES

sqlnet.oraに以下のパラメータを設定

## OS認証禁止設定

```
SQLNET.AUTHENTICATION_SERVICES=NONE
```

「Net Servicesリファレンス」マニュアルの「sqlnet.oraファイルのパラメータ」も併せて参照してください。  
[http://download.oracle.com/docs/cd/E16338\\_01/network.112/b56287/sqlnet.htm#i500318](http://download.oracle.com/docs/cd/E16338_01/network.112/b56287/sqlnet.htm#i500318)

- Oracle Database Vaultの利用



## Oracle Databaseのセキュリティソリューション

- モニタリング・ブロッキング
- 認証
- **アクセス制御**
- 監査
- 暗号化・マスキング
- システム権限
- オブジェクト権限
- 仮想プライベートデータベース
- Oracle Database Vault

# 権限

## システム権限

- ・ ユーザーに対してデータベースの特定の操作を実行可能かどうかを設定

例) CREATE SESSION、CREATE TABLE、SELECT ANY TABLE

- ・ 一般的に特権と呼ばれるもの
  - ・ DB管理者用のDBAロールは多数のシステム権限の集合

## オブジェクト権限

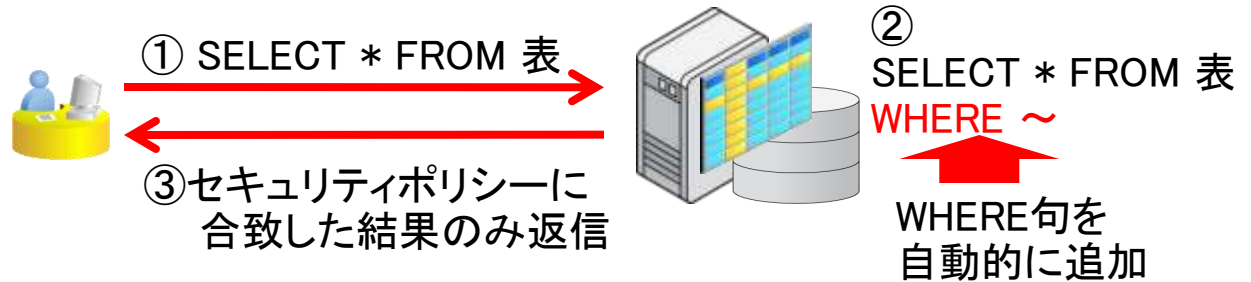
- ・ ユーザーに対して特定のオブジェクトに対してアクセス可能かどうかを設定

システム権限、オブジェクト権限と許可される操作の一覧は、「SQL言語リファレンス」マニュアルの「GRANT」の説明にあります。

[http://download.oracle.com/docs/cd/E16338\\_01/server.112/b56299/statements\\_9013.htm#i2077938](http://download.oracle.com/docs/cd/E16338_01/server.112/b56299/statements_9013.htm#i2077938)

# 仮想プライベートデータベースによる 行・列レベルのアクセス制御

セッションの属性情報  
DBユーザー名  
クライアントホスト  
プログラム名  
時間  
APPユーザー (\*)



- ・ データベース内部で自動的にWHERE句を付加することにより、SQL文の実行結果を制御可能
- ・ WHERE句の内容はPL/SQLで記述するため、動的に設定可能
- ・ DBMS\_RLSパッケージプロシージャで設定

(\*) アプリケーションユーザー名をDBに伝播する仕組みと組み合わせてアプリケーションユーザーごとのアクセス制御も可能です。

DBMS\_RLSパッケージプロシージャの詳細は、「PL/SQLパッケージプロシージャおよびタイプリファレンス」マニュアルの「DBMS\_RLS」の説明にあります。

[http://download.oracle.com/docs/cd/E16338\\_01/appdev.112/b56262/d\\_rls.htm#i1000830](http://download.oracle.com/docs/cd/E16338_01/appdev.112/b56262/d_rls.htm#i1000830)

# Oracle Database Vaultによる 特権ユーザー管理・職務分掌の実現

～ 今までの Oracle Database ～  
DBAに管理権限が集中



データベース  
管理者

データベース管理

ユーザー・アカウント管理

セキュリティ・ポリシー管理

アプリケーション・データの管理

データベースの起動/停止、全ユーザー・データの操作や、セキュリティ設定の変更などあらゆる操作が実行可能



データベース管理者による  
不正なデータ操作や情報漏えいのリスク！

～ Oracle Database Vault ～  
複数の管理者が管理権限を分担

データベース管理

データベースの起動/停止 など  
※実データへのアクセスは不可！



データベース  
管理者

ユーザー・アカウント管理

ユーザーの作成/削除  
※実データへのアクセスは不可！



アカウント  
管理者

セキュリティ・ポリシー管理

セキュリティの設定/監視  
※実データへのアクセスは不可！



セキュリティ  
管理者

アプリケーション・データの管理

ユーザー・データの管理、  
アクセス権の設定



アプリケーション  
管理者

## ■ DBAの特権を制御

- ✓ 管理権限を分割し、SYS/SYSTEMへの権限集中によるリスクを回避

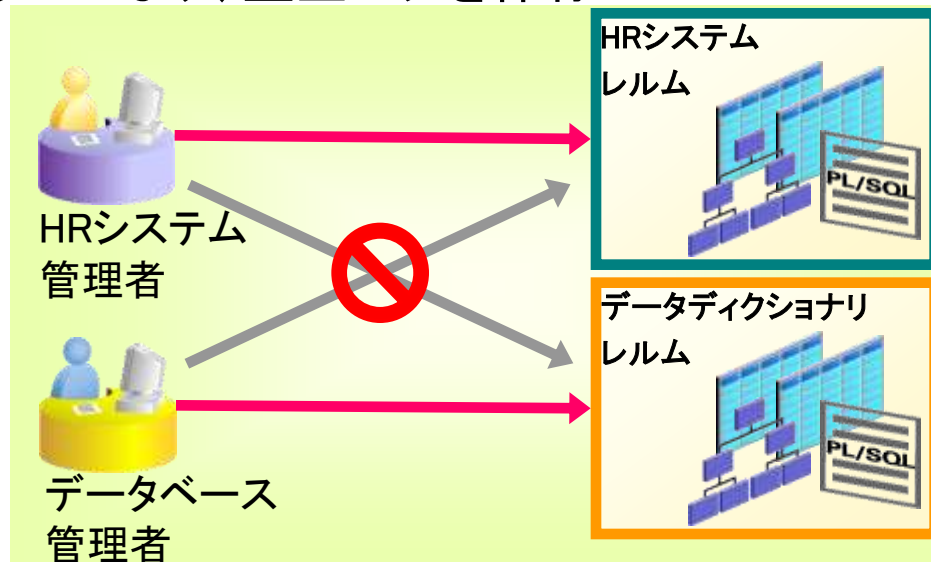
# Oracle Database Vaultの機能①

## レルム(保護領域)

- 任意のスキーマ・オブジェクトのセットを保護・管理するための論理的な領域
  - レルムごとにレルムの管理者を作成することが可能
  - レルム管理者以外の特権(システム権限)でアクセス不可
  - 認可を受けていないレルムに対する、システム権限でのアクセスや DDL はレルム違反エラーとなり、監査ログを保存

### ポイント:

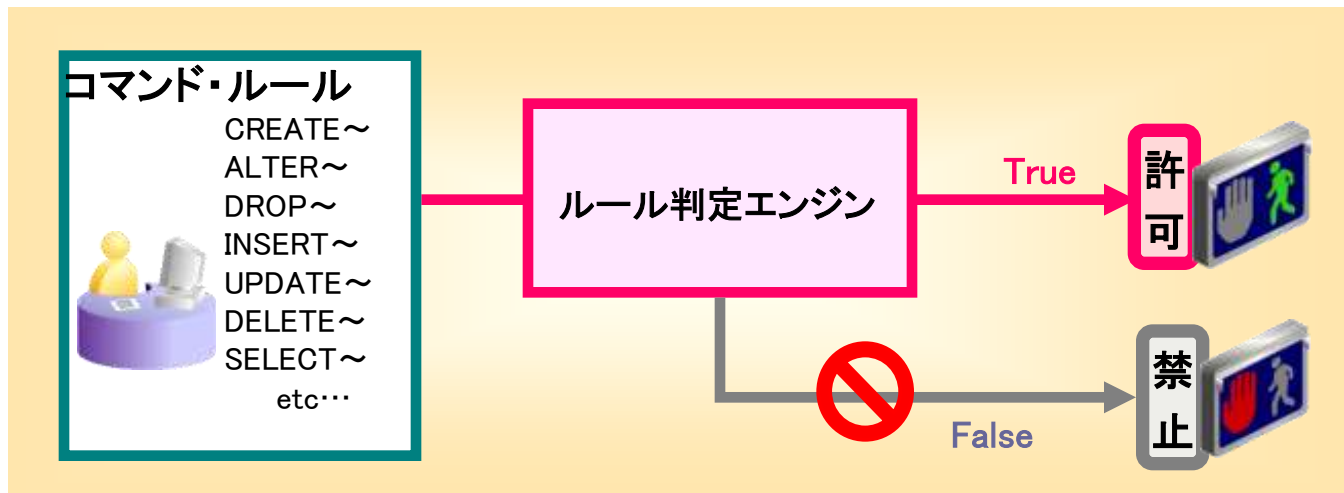
- 例えば、HRユーザーの持っているオブジェクトをすべてHRレルムで保護すれば、データベース管理者であったとしても、HRオブジェクトへのアクセスは許可されない。  
(特権ユーザーの排除)



# Oracle Database Vaultの機能②

## コマンドルール

- SQLコマンド毎に、実行可能な条件を設定
  - SQLコマンドの実行権限を持っていても、セキュリティポリシー(ルール)に合致しない場合はエラーとなり、監査ログを保存





## Oracle Databaseのセキュリティソリューション

- モニタリング・ブロッキング
- 認証
- アクセス制御
- **監査**
- 暗号化・マスキング
- **必須監査**
- **DBA監査**
- **標準監査**
- **ファイングレイン監査**

# Oracle Databaseの監査機能

- 必須監査 **SE** **EE**
  - 必ず出力されるとめることのできないログ
- DBA監査 **SE** **EE**
  - SYSDBA権限で接続したユーザーの全データベース操作に対する監査
  - AUDIT\_SYS\_OPERATIONS初期化パラメータで設定
- 標準監査 **SE** **EE**
  - 設定したSQLコマンドが発行されたことに対する監査
  - AUDITコマンドで設定
  - AUDIT\_TRAIL初期化パラメータで監査証跡出力先設定
- ファイングレイン監査 **EE**
  - 特定のデータ(列、条件)にアクセスがあったことに対する監査
  - DBMS\_FGAパッケージプロシージャで設定

# Oracle Databaseの監査機能比較

	必須監査	DBA監査	標準監査	ファイングレイン監査
監査対象	<ul style="list-style-type: none"> <li>• インスタンス起動</li> <li>• インスタンス停止</li> <li>• SYSDBA権限でのデータベース接続</li> </ul>	<ul style="list-style-type: none"> <li>• すべての操作</li> </ul>	<ul style="list-style-type: none"> <li>• ログイン</li> <li>• CREATE、ALTERなどのデータベース操作</li> <li>• SELECT、UPDATEなどのデータ操作</li> </ul>	<ul style="list-style-type: none"> <li>• 特定のデータ(列、条件指定可能)へのSELECT、INSERT、UPDATE、DELETE</li> </ul>
監査証跡出力先	<ul style="list-style-type: none"> <li>• OSファイル</li> </ul>	<ul style="list-style-type: none"> <li>• OSファイル</li> <li>• SYSLOG</li> <li>• XMLファイル</li> </ul>	<ul style="list-style-type: none"> <li>• データベース表</li> <li>• OSファイル</li> <li>• SYSLOG</li> <li>• XMLファイル</li> </ul>	<ul style="list-style-type: none"> <li>• データベース表</li> <li>• XMLファイル</li> <li>• ユーザー定義アクション</li> </ul>

各初期化パラメータの詳細は「リファレンス」マニュアルの初期化パラメータを参照してください。

[http://download.oracle.com/docs/cd/E16338\\_01/server.112/b56311/toc.htm](http://download.oracle.com/docs/cd/E16338_01/server.112/b56311/toc.htm) (目次)

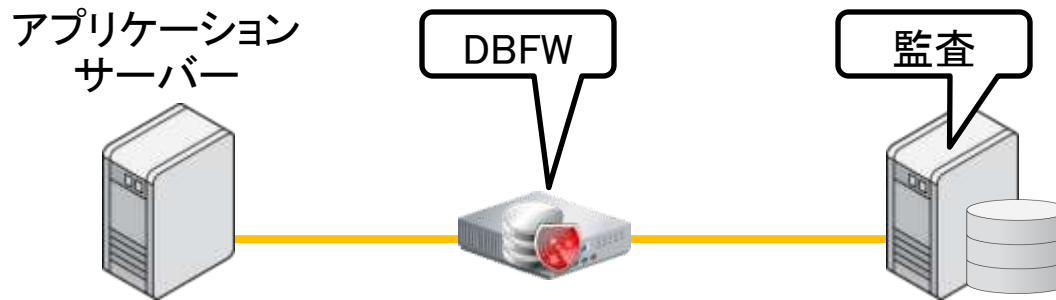
AUDITコマンドと標準監査可能なアクションの一覧は「SQL言語リファレンス」マニュアルの「AUDIT」を参照してください

[http://download.oracle.com/docs/cd/E16338\\_01/server.112/b56299/statements\\_4007.htm#i2059073](http://download.oracle.com/docs/cd/E16338_01/server.112/b56299/statements_4007.htm#i2059073)

DBMS\_FGAパッケージプロシージャの詳細は、「PL/SQLパッケージプロシージャおよびタイプリファレンス」マニュアルの「DBMS\_FGA」の説明にあります。

[http://download.oracle.com/docs/cd/E16338\\_01/appdev.112/b56262/d\\_fga.htm#i1001938](http://download.oracle.com/docs/cd/E16338_01/appdev.112/b56262/d_fga.htm#i1001938)

# 監査とOracle Database Firewall



	Oracle Database Firewall	監査
メリット	<ul style="list-style-type: none"><li>• 簡単な設定ですべてのSQLをモニタリング可能</li><li>• 性能への影響が小さい</li><li>• データベースサーバーの外部で監査証跡を保存可能</li><li>• アラート・レポート機能</li></ul>	<ul style="list-style-type: none"><li>• すべてのSQL文を監査可能</li><li>• 監査条件を詳細に設定可能</li></ul>
デメリット	<ul style="list-style-type: none"><li>• データベースサーバーで発行されたSQL文は取得できない</li></ul>	<ul style="list-style-type: none"><li>• 性能に影響がでる場合がある</li><li>• 取得した監査証跡の解析手法を考える必要がある</li><li>• 設定が複雑になりがち</li></ul>



## Oracle Databaseのセキュリティソリューション

- モニタリング・ブロッキング
- 認証
- アクセス制御
- 監査
- 暗号化・マスキング
- Oracle Advanced Security
- Oracle Data Masking

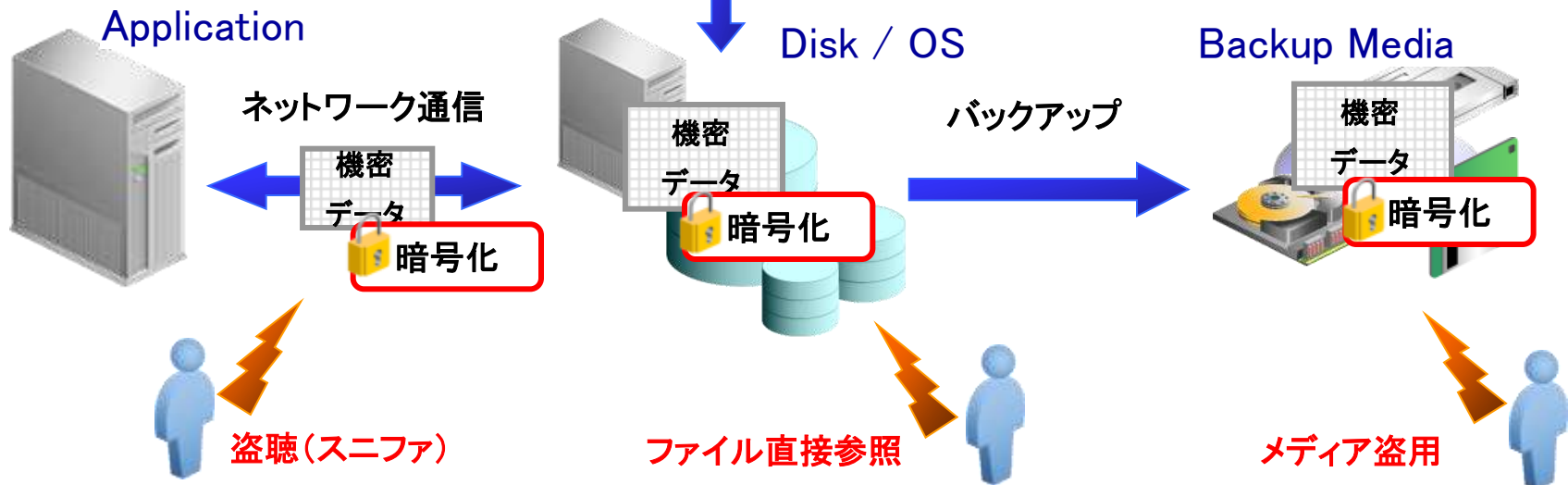
# 暗号化が必要な領域

Oracle

Oracle Database



OS / Hardware



データベースのアクセス・コントロールが施行できない部分では  
暗号化は不正アクセスに対する有効な解決策

ORACLE

# Oracle Net通信の暗号化

- 設定のみで暗号化可能

サーバー側sqlnet.oraに以下のパラメータを設定

## 暗号の有効化

```
SQLNET.ENCRYPTION_SERVER=  
[REQUIRED | REQUESTED | ACCEPTED | REJECTED]
```

## 暗号アルゴリズムの選択

```
SQLNET.ENCRYPTION_TYPES_SERVER=RC4_256 (例)
```

クライアント側sqlnet.oraに以下のパラメータを設定

## 暗号の有効化

```
SQLNET.ENCRYPTION_CLIENT=  
[REQUIRED | REQUESTED | ACCEPTED | REJECTED]
```

## 暗号アルゴリズムの選択

```
SQLNET.ENCRYPTION_TYPES_CLIENT=RC4_256 (例)
```

# Oracle Net通信の暗号化設定

- サーバーとクライアントの設定により暗号化通信をおこなうかどうかを決定

クライアント側の設定値

サーバー側の設定値

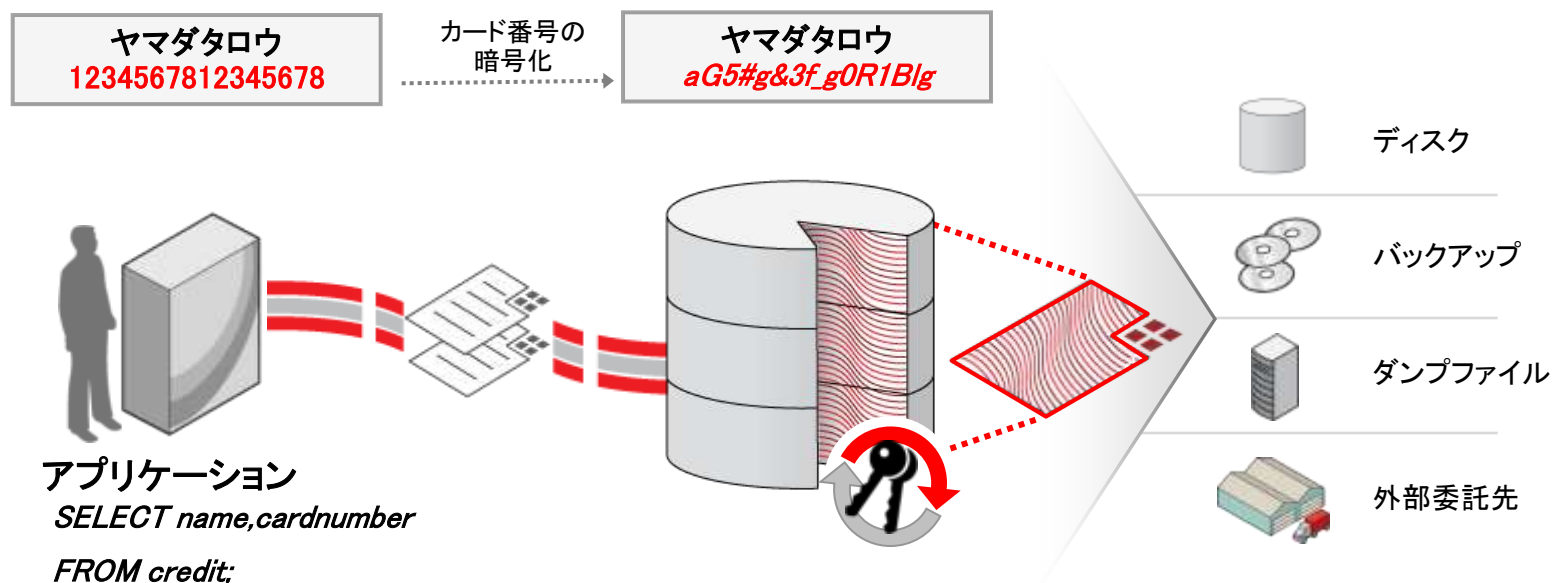
	REQUIRED	REQUESTED	<u>ACCEPTED</u>	REJECTED
REQUIRED	暗号化	暗号化	暗号化	接続失敗
REQUESTED	暗号化	暗号化	暗号化	非暗号化
<u>ACCEPTED</u>	暗号化	暗号化	非暗号化	非暗号化
REJECTED	接続失敗	非暗号化	非暗号化	非暗号化

チェックサムを利用した通信の完全性の確認も可能

「Net Servicesリファレンス」マニュアルの「sqlnet.oraファイルのパラメータ」も併せて参照してください。  
[http://download.oracle.com/docs/cd/E16338\\_01/network.112/b56287/sqlnet.htm#i500318](http://download.oracle.com/docs/cd/E16338_01/network.112/b56287/sqlnet.htm#i500318)

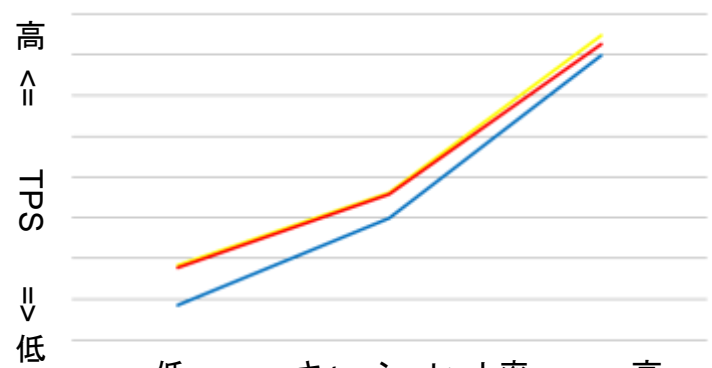
# 格納データの暗号化

- 透過的データ暗号化
  - NIST標準の強力な暗号アルゴリズムを利用  
(AES 128/192/256bitに対応)
  - Oracle WalletやHardware Security Moduleを利用した鍵管理メカニズム
  - アプリケーションから透過的(書き換えもチューニングも不要)
  - 表領域単位で格納データを暗号化



# 最新Intelチップ機能を利用した性能影響の最小化

- AES-NI (Advanced Encryption Standard New Instructions)を利用することで高速な暗号処理を実現

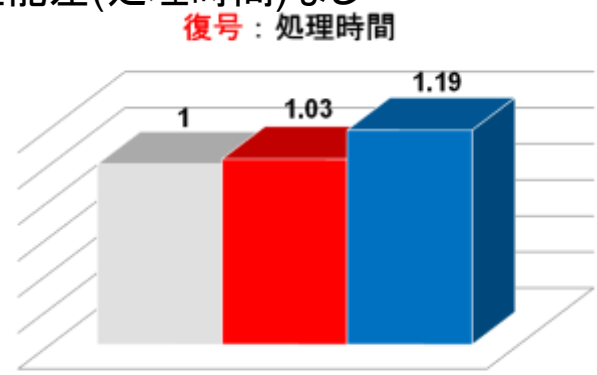
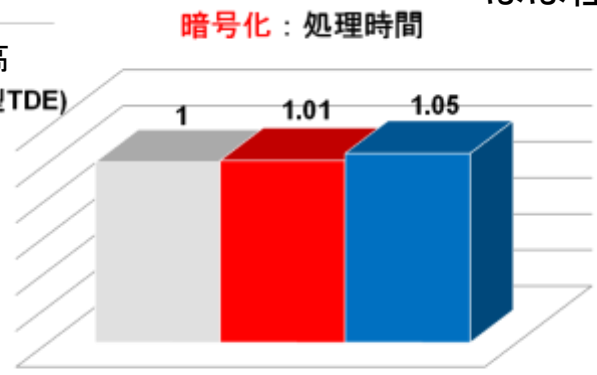


暗号化なし — AES-NI有り — AES-NIなし(従来型TDE)

- 検索:更新の割合=8:2
- 40 threadで実行

← OLTP処理の処理性能  
 キャッシュヒット率にかかわらず  
 AES-NIがあれば暗号化なしの時と  
 性能差(TPS)なし

↓ バッチ処理の処理性能  
 AES-NIがあれば暗号化なしの時と  
 ほぼ性能差(処理時間)なし



■ 暗号化なし ■ TDE(AES-NI) ■ TDE(AES-NIなし) ■ 暗号化なし ■ TDE(AES-NI) ■ TDE(AES-NIなし)

- Direct Pathを利用し、バッファキャッシュをバイパス (TDEの動作仕様として一番負荷が高いケース)

# 透過的データ暗号化利用手順

sqlnet.oraに以下のパラメータを設定

## Walletの場所の指定

```
ENCRYPTION_WALLET_LOCATION =  
  (SOURCE=(METHOD=FILE)(METHOD_DATA=  
  (DIRECTORY=<Wallet格納ディレクトリ>)))
```

Wallet格納ディレクトリのアクセス権限は「700」とする必要があります。

ENCRYPTION\_WALLET\_LOCATIONの代わりにWALLET\_LOCATIONを利用することもできます。

## 暗号鍵(マスターキー)の作成

```
SQL> ALTER SYSTEM SET ENCRYPTION KEY  
  2 IDENTIFIED BY "welcome1";
```

## 暗号化表領域の作成

```
SQL> CREATE TABLESPACE ENC_TBS  
  2 DATAFILE ~  
  3 ENCRYPTION USING 'AES192'  
  4 DEFAULT STORAGE (ENCRYPT);
```

# 設定の注意点

透過的データ暗号化には、今回紹介した表領域単位の暗号化の他に、列単位の暗号化もあります。列単位の暗号化も含めた透過的データ暗号化の詳細は「Advanced Security管理者ガイド」マニュアルの「透過的データ暗号化を使用した格納済みデータの保護」を参照してください。

[http://download.oracle.com/docs/cd/E16338\\_01/network.112/b56286/asotrans.htm#g1011122](http://download.oracle.com/docs/cd/E16338_01/network.112/b56286/asotrans.htm#g1011122)

Walletはデータベース起動ごとに有効化(オープン)する必要があるため、以下の手順で自動オープン  
の設定をしておくと便利です。

```
mkstore -wrl <Wallet格納ディレクトリ> -createSSO
```

「Net Servicesリファレンス」マニュアルの「sqlnet.oraファイルのパラメータ」も併せて参照してください。

[http://download.oracle.com/docs/cd/E16338\\_01/network.112/b56287/sqlnet.htm#i500318](http://download.oracle.com/docs/cd/E16338_01/network.112/b56287/sqlnet.htm#i500318)

表領域の作成の詳細は、「SQL言語リファレンス」マニュアルの「CREATE TABLESPACE」も併せて  
参照してください。

[http://download.oracle.com/docs/cd/E16338\\_01/server.112/b56299/statements\\_7003.htm#i2231734](http://download.oracle.com/docs/cd/E16338_01/server.112/b56299/statements_7003.htm#i2231734)

# バックアップの暗号化

- RMANと統合されたバックアップ暗号化
  - パスワードもしくはWalletを利用した暗号化/復号が可能
  - Enterprise Managerの画面から設定可能

The screenshot shows the Oracle Enterprise Manager 11g Database Control interface. The breadcrumb trail is: ホーム > フォルダツリー > ユーザー > ログアウト > データベース. The main navigation bar includes: オプション, 設定, スケジュール, 確認. The current page title is "カスタマイズ・バックアップのスケジュール: オプション". The breadcrumb for the current page is: データベース > 設定 > バックアップ計画 > カスタマイズ・バックアップ > オブジェクト・タイプ > データベース全体. The "バックアップ・タイプ" section has "全体バックアップ" selected. The "暗号化" section is expanded, showing "Recovery Manager暗号化を使用" selected, "暗号化アルゴリズム" set to "AES256", and "暗号化モード" set to "Oracle Encryption Wallet". There are password input fields for "パスワード" and "パスワードの確認".

# 安全なテストデータの作成

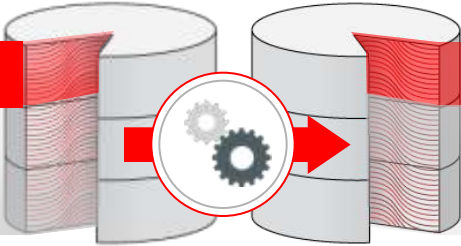
効率的なテストのために、  
本番環境に近いデータが必要

機密情報を含んだデータをテストに  
利用するには情報漏洩のリスクがある

- **機密性の高い情報を不可逆な形式でマスキング**
  - 個人情報
  - 医療情報、患者情報
  - 支払用カード情報など
- Enterprise ManagerのGUI画面で簡単にマスキングの設定、実行

本番データベース

LAST_NAME	CREDIT_ID	SALARY
AGUILAR	203-33-3234	40,000
BENSON	323-22-2943	60,000



テストデータベース

LAST_NAME	CREDIT_ID	SALARY
ANSKEKSL	111-23-1111	60,000
BKJHHEIEDK	222-34-1345	40,000

# データのマスクングを簡単に定義、実行

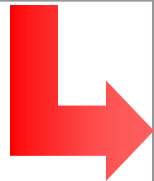
フォーマット・ライブラリ

フォーマット・ライブラリには、すぐに使用できるマスクング・フォーマットの集合が含まれて

検索

選択	フォーマット	データ型	サンプル
<input checked="" type="radio"/>	電話番号	文字	003-2000-3710
<input type="radio"/>	苗字のリスト	ソース・タイプ	上田
<input type="radio"/>	名前のリスト	ソース・タイプ	博
<input type="radio"/>	メールアドレス	文字	haiaaaw@gaaaaaif.com
<input type="radio"/>	Visa Credit Card Number	文字	
<input type="radio"/>	USA Phone Number Formatted	文字	
<input type="radio"/>	USA Phone Number	文字	

- マスクング定義はすべてGUIで作成
- 一度作成したマスクング定義は再利用可能



列マスクの定義

所有者 HOBATA  
表 USERS  
列 NAME  
データ型 VARCHAR2(30)

デフォルトでは、表内のすべてのレコードは、指定したフォーマットを使用してマスクングされます。オプションで、条件を使用して複数のレコードのサブセットを識別できます。各サブセットは、対応するマスクング・フォーマットを使用してマスクングできます。これらのサブセットは、指定した順序でマスクングされます。サブセットが後続の条件と一致しても、このサブセットが再度マスクングされることはありません。

すべて開く | すべて閉じる

選択	条件	フォーマット・エントリのプロパティ				サンプル	削除
		プロパティ	値	プロパティ	値		
<input checked="" type="radio"/>	▼ デフォルト条件						
	固定数値	固定数値	0				
	ランダム桁数	開始の長さ	1	終了の長さ	2		
	固定文字列	固定文字列	-				
	ランダム桁数	開始の長さ	2	終了の長さ	4		
	固定文字列	固定文字列	-				
	ランダム数値	開始値	0	終了値	9999		

# 多様なマスキングをサポート

- 固定数値
- 固定文字列
- ランダム桁数
- ランダム数値
- ランダム文字列
- ランダム日付
- 配列リスト
- シャッフル
- 置換
- 表の列の値・・・など

固定文字列への  
変換

ID	NAME
1	SMITH
2	ALLEN
3	JONES
4	CLARK
5	ADAMS
:	:



ID	NAME
1	XXXXXX
2	XXXXXX
3	XXXXXX
4	XXXXXX
5	XXXXXX
:	:

ランダム数値+固定文字列  
への変換

ID	CARDNUMBER
1	7488-2984-1736-7400
2	4033-6177-0089-6401
3	6141-5126-0475-8802
4	1139-4145-6222-3703
5	8337-6263-1608-0104
:	:



ID	CARDNUMBER
1	5870-2967-9149-5700
2	9634-7334-4874-2301
3	8430-8214-6445-1102
4	1573-9537-1503-5503
5	0606-3321-6271-8304
:	:

シャッフル

ID	COUNTRY
1	US
2	JP
3	US
4	UK
5	FR
:	:



ID	COUNTRY
1	US
2	FR
3	UK
4	FR
5	JP
:	:

# 論理的に関連のある列へのマスキング

依存性を維持したマスキング

(ランダム文字列)

ID	COMPANY	SALES_REP
1	ABC Material	SMITH
2	ZZZ Manufacture	CLARK
3	B&C Inc	JONES
4	OPQ World	CLARK
5	YYY Corp	ADAMS
:		:



NAME	COUNTRY
CLARK	UNITED_KINGDOM
JONES	UNITED_STATES
SMITH	AUSTRALIA
KEITH	IRELAND
ADAMS	CANADA
:	:

外部キー制約はないが、  
アプリで関連付けて使用



ID	COMPANY	SALES_REP
1	ABC Material	cccchfk
2	ZZZ Manufacture	aaaafdk
3	B&C Inc	bbbeoh
4	OPQ World	aaaafdk
5	YYY Corp	99999k
:		:

NAME	COUNTRY
aaaafdk	UNITED_KINGDOM
bbbeoh	UNITED_STATES
cccchfk	AUSTRALIA
1234akf	IRELAND
99999k	CANADA
:	:

手動で列を指定することにより、  
関連付けてマスク

# カーディナリティを維持したマスキング

マスク前

都道府県
東京都
東京都
東京都
大阪府
大分県

where 都道府県='東京都'

3件

全ての行を単純に置き換えると、要素の数や各要素の割合が変化し、where句、group by句などを含むクエリの結果が変化してしまう

元のデータが同一である(異なる)場合、マスク先も同一になる(異なる)ようにマスクを行う

マスク後

都道府県
AAAAAA
AAAAAA
AAAAAA
AAAAAA
AAAAAA

where 都道府県='AAAAAA'

3件

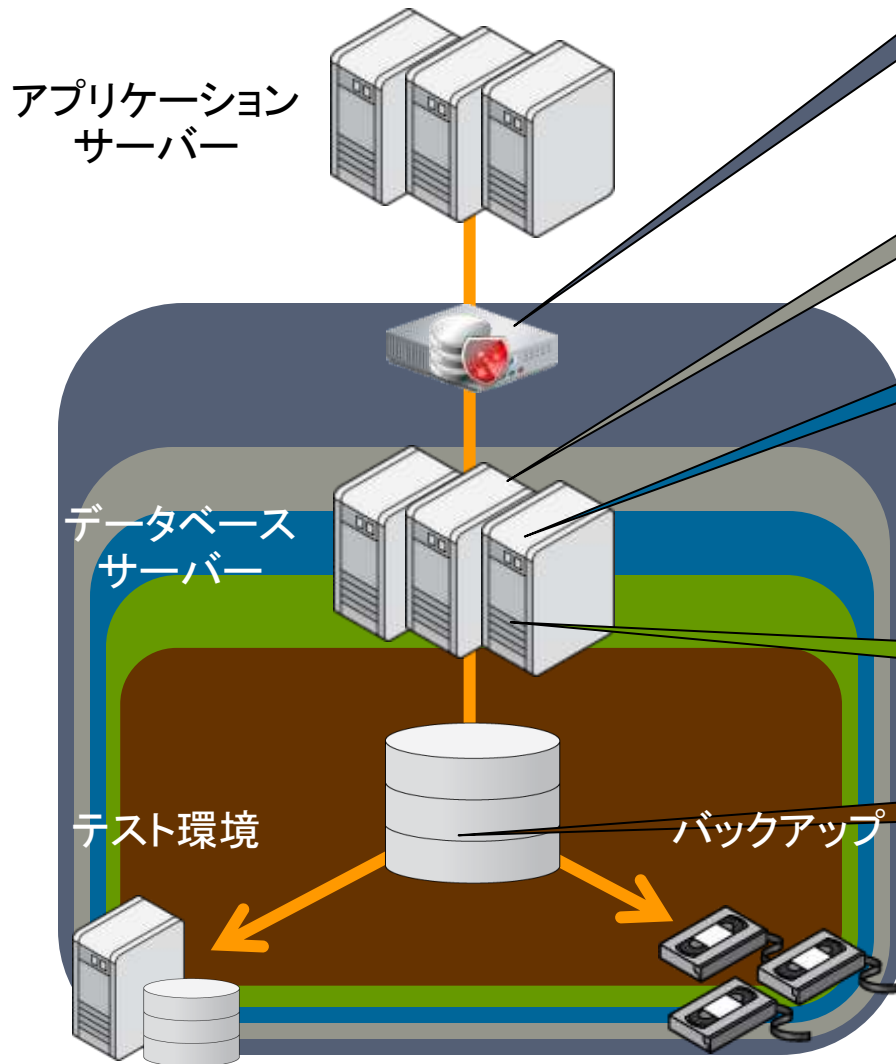
都道府県
AAAAAA
AAAAAA
AAAAAA
BBBBBB
CCCCCC

where 都道府県='AAAAAA'

5件

# まとめ:

## Oracle Databaseのセキュリティソリューション



### モニタリング・ブロッキング

- 不正アクセス検知・防御・監査レポート自動化 (Oracle Database Firewall)
- 接続元サーバーの制限 (Listener)

### 認証

- ユーザー認証

### アクセス制御

- 権限 (システム権限・オブジェクト権限)
- 行や列レベルでのアクセス制御 (仮想プライベートデータベース)
- 特権ユーザー管理・職務分掌 (Oracle Database Vault)

### 監査

- データベース監査機能 (標準監査・ファイングレイン監査・DBA監査)

### 暗号化・マスキング

- 格納データ暗号化 (Oracle Advanced Security)
- ネットワーク通信暗号化 (Oracle Advanced Security)
- バックアップデータ暗号化 (Oracle Advanced Security)
- 安全なテストデータの作成 (Oracle Data Masking)

ORACLE®

参考：

## Oracle Application Express (APEX)

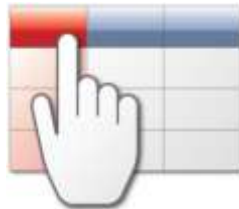
Oracleデータベースを軸としたWebアプリケーション開発ツール  
**簡単かつ迅速に充実したアプリケーションが開発可能**

- ブラウザベースでアプリケーション開発ができる
- コードを書かずにアプリケーションを開発可能
- Oracleデータベース機能とSQL、PL/SQLを生かした開発ができる
- Oracleデータベース標準機能で、サポート体制も充実



### エクセルシートのWeb化

エクセルシートを同時に  
表示、編集できる  
Webアプリケーションに変換



### オンライン・レポート

既存のデータベースに  
SQLベースのレポート・  
アプリケーションを構築



### データ駆動型アプリケーション

暫定的な部門向け  
アプリケーションを開発

# APEXの情報はこちら ～「オラクルエンジニア通信 APEX」で検索

BLOGS HOME PRODUCTS & SERVICES DOWNLOADS SUPPORT PARTNERS COMMUNITIES ABOUT Login

オラクルエンジニア通信 - 技術資料、マニュアル、セミナー **ORACLE**

Oracleエンジニアのための技術情報サイト by Oracle Japan

« [【セミナー資料】おら!オラ!](#) | [Main](#) | [Oracle Data Masking...](#) »

About  
Oracleエンジニアの方がスキルアップ  
していただくために、厳選した情報を

## Oracle Application Express(APEX) - 概要(とは), 資料, マニュアル

By Yusuke.Yamamoto on 12 31, 2009

- [Webカレンダー・アプリケーションを簡単作成～Oracle Application Express 4.1がリリースされました](#)
- [【セミナー動画/資料】Oracleデータベースアプリを簡単作成](#)
- [Oracle Application Express\(Oracle APEX\) 4.0: 日本語チュートリアル](#)
- [ExcelデータのOracle DBへの取り込み\(インポート\)](#)
- [GUIでSQL開発。ドラッグ&ドロップでSELECT文を作成](#)
- [DBオブジェクトのDDL文の簡単\(ブラウザだけで\)生成](#)
- [SQL開発に便利! 実行履歴、実行計画をブラウザで確認](#)
- [データベースからCSVファイルを簡単\(ブラウザだけで\)エクスポート](#)
- [APEX\(Oracle Application Express\)の使い方～インストール無し! 今すぐ使えるAPEX。クラウド上のAPEX](#)
- [【チュートリアル】Oracle Application Express 4.0インストール](#)
- [【セミナー資料】使ってみようOracle Application Express](#)
- [【チュートリアル】Oracle Database 11gのOracle APEX](#)

powered by Feed2JS

**日本語チュートリアル(手順書)**  
インストールの方法、使い方を説明した日本語の手順書を取り揃えました!  
「インストールガイド」  
「データベース・アプリケーションの作り方」  
「グラフ・ガント・チャート、マップの作り方」  
**最新バージョンのダウンロードなど**  
ダウンロード先のご案内や、システム要件など  
ご利用いただくために、必要な情報がまとめられています。

[http://blogs.oracle.com/oracle4engineer/entry/cat\\_apex](http://blogs.oracle.com/oracle4engineer/entry/cat_apex)

ORACLE

# APEXを試したい方は

<http://apex.oracle.com>

ORACLE



Welcome to  
**apex.oracle.com**  
now running Oracle Application Express 4.1

Login

Sign Up

Learn More >

Use [apex.oracle.com](http://apex.oracle.com) to develop database centric web applications with Oracle Application Express. If you have a workspace, click the [login](#) button, otherwise, click the [sign up](#) button to request a new workspace.

Oracle provides [apex.oracle.com](http://apex.oracle.com) as an evaluation service free of charge. Oracle Application Express is a no-cost option of the Oracle database. The latest version of Oracle Application Express can be [downloaded from OTN](#).

※ ログインボタンクリック後は日本語で利用可能です

ORACLE

# OTNセミナーオンデマンド

コンテンツに対する  
ご意見・ご感想を是非お寄せください。

OTNオンデマンド 感想



[http://blogs.oracle.com/oracle4engineer/entry/otn\\_ondemand\\_questionnaire](http://blogs.oracle.com/oracle4engineer/entry/otn_ondemand_questionnaire)

上記に簡単なアンケート入力フォームをご用意しております。

セミナー講師/資料作成者にフィードバックし、  
コンテンツのより一層の改善に役立てさせていただきます。

是非ご協力をよろしくお願いいたします。

# OTNセミナーオンデマンド

日本オラクルのエンジニアが作成したセミナー資料・動画ダウンロードサイト

## 掲載コンテンツカテゴリ(一部抜粋)

Database 基礎

Database 現場テクニック

Database スペシャリストが語る

Java

WebLogic Server/アプリケーション・グリッド

EPM/BI 技術情報

サーバー

ストレージ



超入門! Oracle データベースって何

再生時間: 60分

100以上のコンテンツをログイン不要でダウンロードし放題

データベースからハードウェアまで充実のラインナップ

毎月、旬なトピックの新作コンテンツが続々登場

## 例えばこんな使い方

- 製品概要を効率的につかむ
- 基礎を体系的に学ぶ/学ばせる
- 時間や場所を選ばず(オンデマンド)に受講
- スマートフォンで通勤中にも受講可能



毎月チェック!



コンテンツ一覧 はこちら

<http://www.oracle.com/technetwork/jp/ondemand/index.html>

新作&おすすめコンテンツ情報 はこちら

<http://oracletech.jp/seminar/recommended/000073.html>

OTNオンデマンド



# オラクルエンジニア通信

オラクル製品に関わるエンジニアの方のための技術情報サイト

## オラクルエンジニア通信 - 技術資料、マニュアル、セミナー

Oracleエンジニアのための技術情報サイト by Oracle Japan

新着情報を知りたい

技術資料を探したい

セミナーを受けたい

**About**

Oracleエンジニアの方がスキルアップしていただくために、厳選した情報をお届けしています

技術資料	<p>インストールガイド・設定チュートリアルetc. 欲しい資料への最短ルート</p>	アクセスランキング	<p>他のエンジニアは何を見ているのか？人気資料のランキングは毎月更新</p>
特集テーマ Pick UP	<p>性能管理やチューニングなど月間テーマを掘り下げて詳細にご説明</p>	技術コラム	<p>SQLスクリプト、索引メンテナンスetc. 当たり前運用/機能が見違える!?</p>

<http://blogs.oracle.com/oracle4engineer/>

オラクルエンジニア通信



製品/技術  
情報



Oracle Databaseっていくら？オプション機能も見積れる簡単ツールが大活躍

セミナー



基礎から最新技術までお勧めセミナーで自分にあった学習方法が見つかる

スキルアップ



ORACLE MASTER ! 試験頻出分野の模擬問題と解説を好評連載中

Viva!  
Developer



全国で活躍しているエンジニアにスポットライト。きらりと輝くスキルと視点を盗もう

<http://oracletech.jp/>

oracletech



あなたにいちばん近いオラクル



# Oracle Direct

まずはお問合せください

Oracle Direct



システムの検討・構築から運用まで、ITプロジェクト全般の相談窓口としてご支援いたします。  
システム構成やライセンス/購入方法などお気軽にお問い合わせ下さい。

## Web問い合わせフォーム

専用お問い合わせフォームにてご相談内容を承ります。  
[http://www.oracle.co.jp/inq\\_pl/INQUIRY/quest?rid=28](http://www.oracle.co.jp/inq_pl/INQUIRY/quest?rid=28)

※フォームの入力にはログインが必要となります。  
※こちらから詳細確認のお電話を差し上げる場合がありますので  
ご登録の連絡先が最新のものになっているかご確認下さい。

## フリーダイヤル

0120-155-096

※月曜～金曜  
9:00～12:00、13:00～18:00  
(祝日および年末年始除く)

ORACLE

# **Hardware and Software Engineered to Work Together**

**ORACLE®**