

ORACLE®



# データベースを強化する3つのポイント

## ◎ 監査

データへのアクセスを漏れなく記録と保全  
不正なアクセスの兆候を監視し見逃さずに通知  
インシデントの原因究明の重要な手掛かり  
データベースへの不正なアクセスを未然に遮断

Audit Vault and  
Database Firewall

## ◎ アクセス制御

特権ユーザに適切な権限とルールを付与

Database Vault

## ◎ 暗号化

ユーザの接続情報やアプリの情報によって  
アクセスできる情報を制限

機密データの漏洩、持ち出し対策  
安全なテストデータの作成、個人情報の匿名化

Advanced Security  
Data Masking and  
Subsetting

# Oracle Advanced Securityが実現するセキュリティ対策

データの暗号化

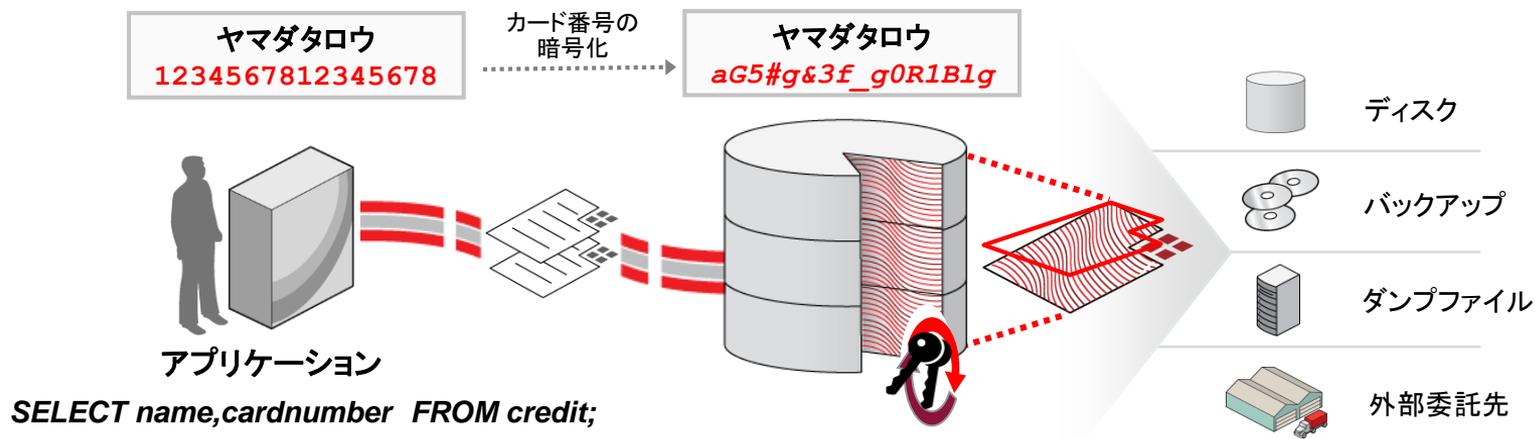
Transparent Data Encryption

リアルタイムアクセス制御

Data Redaction

# Transparent Data Encryption (TDE)

- 強力な暗号アルゴリズムを利用した暗号化を実施
  - NISTの標準共通鍵暗号方式 AES(128/192/256bit) に対応
- Oracle Wallet やHardware Security Moduleを利用した暗号鍵管理メカニズム
- アプリケーションからは透過的にデータの暗号化/復号
  - 既存のアプリケーション(SQL)を改修する必要はなし



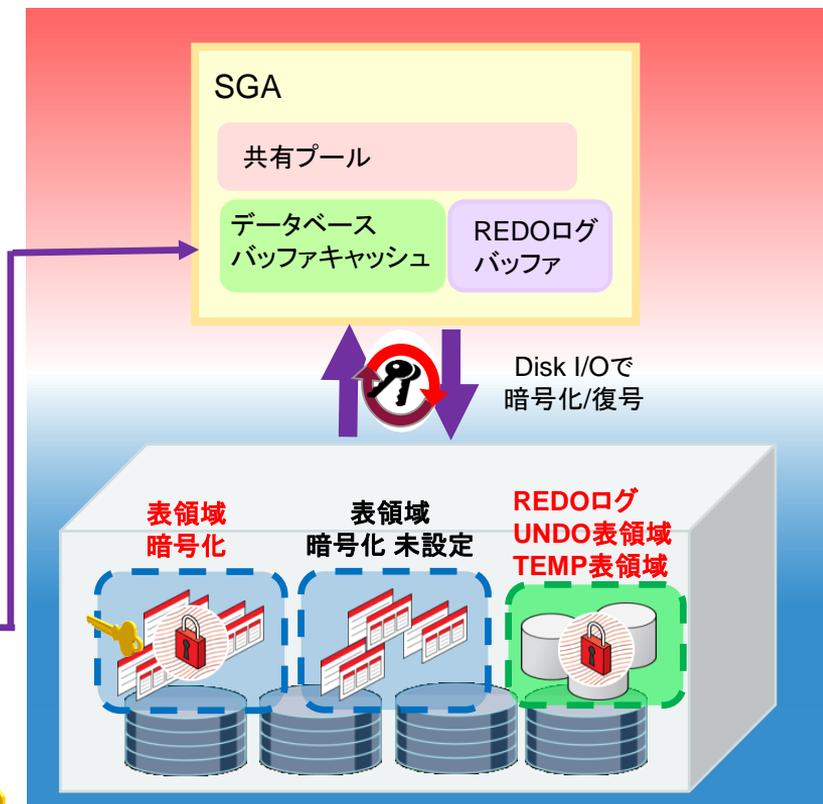
# TDE 表領域暗号化

- 表領域単位での暗号化
- 表領域内のオブジェクトはすべて暗号化される
- データブロックに対するI/Oで暗号化・復号
- 表領域以外のOracleの関連ファイルも暗号化される
- メモリ上は暗号化しない
- Advanced Compressionとの併用可能
- 暗号化してもデータサイズは変わらない
- ほとんどすべてのオブジェクトが暗号化可能 (BFILEのみ不可)

Oacle Keystore  
(Oracle Wallet)

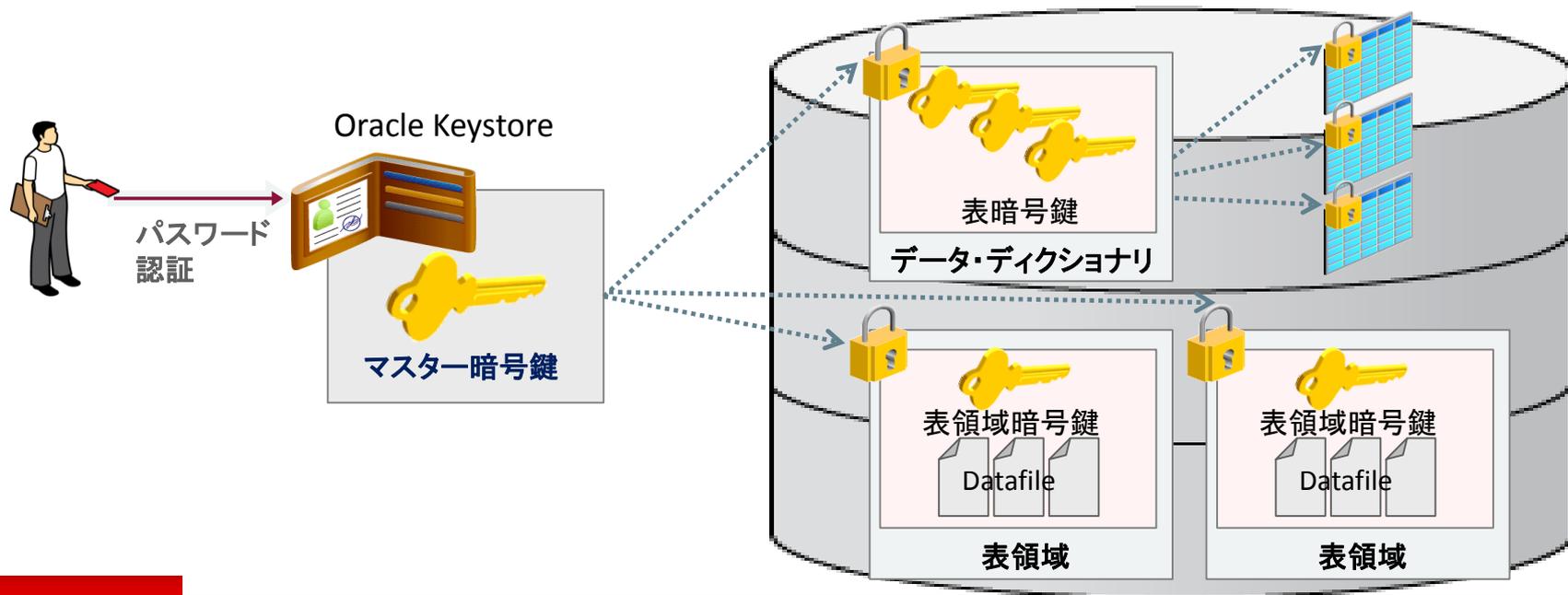
列暗号化  
マスター鍵  
表領域暗号化  
マスター鍵

Walletを  
オープン



# TDEの暗号鍵の仕組み

- Oracle Keystore に、マスター暗号鍵が格納される (※11gR2まではOracle Wallet)
- マスター暗号鍵は、それぞれの列暗号鍵と表領域暗号鍵を暗号化する
- 表ごとの暗号鍵、表領域ごとの暗号鍵でそれぞれの実データを暗号化する



# マスタ暗号鍵の構成手順(12c)

- SQLNET.ORAにKeystoreを作成するロケーションを記述する

```
ENCRYPTION_WALLET_LOCATION=  
  (SOURCE=  
    (METHOD=FILE)  
    (METHOD_DATA=  
      (DIRECTORY=/opt/app/oracle/product/12c/dbhome_1/network/admin)))
```

- SYSKM権限(またはSYSユーザ)でSQL\*PLUSにログインする

```
SQLPLUS / AS SYSKM  
Enter password: password  
Connected.
```

- Keystoreを作成する。成功すると指定のロケーションにewallet.p12ファイルが作成される

```
ADMINISTER KEY MANAGEMENT CREATE KEYSTORE  
'/opt/app/oracle/product/12c/dbhome_1/network/admin' IDENTIFIED BY password;
```

# マスタ暗号鍵の構成手順(12c)

- Keystoreをオープンする

```
ADMINISTER KEY MANAGEMENT SET KEYSTORE OPEN IDENTIFIED BY password;
```

- マスター暗号鍵を作成する。※変更・再作成の場合も同様

```
ADMINISTER KEY MANAGEMENT SET KEY USING TAG 'tag名' IDENTIFIED BY password  
WITH BACKUP;
```

- Keystoreにマスター暗号鍵が生成され、Keystoreのあるロケーションにバックアップが作成される以降は、通常通りの暗号表、暗号化表領域の作成手順へ

```
SELECT KEY_ID,ACTIVATION_TIME FROM V$ENCRYPTION_KEYS;
```

KEY_ID	CREATION_TIME
AfrZm0w5EE9kv2NNme6cpwIAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA	13-02-07 06:59:41

# 暗号化表領域の作成

- 表領域の作成時に列暗号化を指定

```
CREATE TABLESPACE securespace  
DATAFILE '/opt/app/oracle/oradata/ora12c/enc.dbf' SIZE 100M ENCRYPTION USING 'AES256'  
DEFAULT STORAGE (ENCRYPT);
```

- 以降は、従来通り表を作成を作成する際の表領域として指定する

- ※ 既存の表を暗号化された表領域に移動する場合
  - 表のオンライン再定義 (DBMS\_REDEFINITION)
  - ALTER TABLE MOVE ~
  - Oracle DataPump Export/Import

# DEMONSTRATION

Oracle Security Solutions



# Oracle Enterprise Managerによる暗号化表領域の設定例

The screenshot displays the Oracle Enterprise Manager Cloud Control 12c interface. The top navigation bar includes the Oracle logo, 'Enterprise Manager Cloud Control 12c', and user information for 'SYSMAN'. The breadcrumb trail shows 'ora12c.jp.oracle.com' and '表領域の作成'. The main content area is titled '表領域の作成' (Tablespace Creation) and shows the name 'enc\_tbl' in the '\*名前' field. Under the 'タイプ' (Type) section, the '永続' (Permanent) radio button is selected, and the '暗号化' (Encryption) checkbox is checked, with a red box highlighting the '暗号化 オプション' (Encryption Option) button. The 'ステータス' (Status) section has '読取り/書込み' (Read/Write) selected. The 'UNDO保存保証' (UNDO Retention Guarantee) is set to 'いいえ' (No).

ORACLE Enterprise Manager Cloud Control 12c 設定(S) ヘルプ(H) SYSMAN ログアウト

Enterprise(E) ターゲット(T) お気に入り(F) 履歴(O)

ora12c.jp.oracle.com 次のユーザーでログイン SYS | secvm12.jp.oracle.com

Oracleデータベース パフォーマンス 可用性 スキーマ 管理

表領域 > 表領域の作成 SYSとしてログイン

表領域の作成

複数のデータベースに対して実行 SQL表示 取消 OK

一般 記憶域

\*名前 enc\_tbl

エクステンツ管理

- ローカル管理
- ディクショナリ管理

タイプ

- 永続
  - デフォルト永続表領域として設定
  - 暗号化 暗号化オプション
- 一時
  - デフォルト一時表領域として設定
- UNDO

UNDO保存保証  はい  いいえ

ステータス

- 読取り/書込み
- 読取り専用
- オフライン

Enterprise(E) ターゲット(T) お気に入り(F) 履歴(O)

ora12c.jp.oracle.com 次のユーザーでログイン SYS | secvm12.jp.oracle.com

Oracleデータベース パフォーマンス 可用性 スキーマ 管理

表領域 > 表領域の作成

表領域の暗号化オプション : SECURE\_TBL

表領域を暗号化すると、データが暗号化形式でディスクに格納されるので、表領域のすべてのオブジェクトが保護されます。Oracleが存在し、オープン状態である必要があります。

ウォレット・ステータス オープン

暗号化アルゴリズム AES256

Enterprise(E) ターゲット(T) お気に入り(F) 履歴(O)

ora12c.jp.oracle.com 次のユーザーでログイン SYS | secvm12.jp.oracle.com

Oracleデータベース パフォーマンス 可用性 スキーマ 管理

表領域 > 表領域の表示: SECURE\_TBL

表領域の表示: SECURE\_TBL

SYSとしてログイン

アクション データファイルの追加 実行 編集 戻る

名前 SECURE\_TBL

ビッグファイル表領域 いいえ

ステータス ReadWrite

タイプ 永続

エクステン管理 ローカル

暗号化 YES

記憶域

割当てタイプ 自動

セグメント領域の管理 自動

ロギング有効化 いいえ

圧縮 圧縮なし

ブロック・サイズ(バイト) 8192

データファイル

名前	ディレクトリ	サイズ(MB)	使用量(MB)	最大ファイル・サイズ(MB)	自動拡張
securefile1	/opt/app/oracle/oradata/ora12c/	100.00	<div style="width: 100%; height: 10px; background-color: #00b0f0;"></div>	1.00	0.00

# 暗号鍵の管理

ORACLE Enterprise Manager Cloud Control 12c

Enterprise(E) ターゲット(T) お気に入り(F) 履歴(O) ターゲット名の検索

ora12c.jp.oracle.com 次のユーザーでログイン SYS secvm12.jp.oracle.com ページリフレッシュ 2013/09/15 1:08:18 JST

### Oracle Advanced Security - 透過的データ暗号化

**使用頻度の高い構成オプション**

現在使用中のマスター・キー(日数) 0

キー更新

キーストアのステータス OPEN

開じる

**概要**

Oracle Advanced Security Transparent Data Encryption (TDE)では、機密アプリケーション・データを保持する個々の列またはアプリケーション表領域全体を暗号化できます。TDEは、データがディスクに書き込まれるときにデータを透過的に暗号化し、認証済のユーザーまたはアプリケーションに読み戻されるときにデータを復号化します。この機能を利用するためにアプリケーションに変更を加える必要はありません。

TDEは、マスター・キーとデータ・キーから構成される2階層の暗号化キー管理アーキテクチャを備えています。マスター・キーは、データ・キーの暗号化に使用され、データ・キーは保存データの暗号化に使用されます。データ・キーは、ユーザーの操作なしにTDEによって自動的に管理されます。マスター・キーは、データベースの外にあるキーストアに格納され、このページに示された操作により管理されます。キーストアは、Oracle Walletまたはハードウェア・セキュリティ・モジュール(HSM)のいずれかです。このページでは、マスター・キーのローテーション、マスター・キーの移動、マスター・キーの作成と更新、キーストア自体の管理などの共通のキー管理操作を行えます。

**キーストアとマスター・キー**

キーストア MORE

キーストアのステータス OPEN

キーストアのタイプ WALLET - PASSWORD

キーストアの場所 /opt/app/oracle/product/12c/dbhome\_1/network/admin

**マスター・キー**

キー更新 作成 編集 キーを使用中に設定 エクスポート

キーの説明(タグ)	ステータス		作成タイムスタンプ	アクティブ化のタイムスタンプ
	使用中	バックアップ済		
initial 2013/09/15		✓	2013-09-14 15:49:36	2013-09-14 15:49:36
定期変更 2013/12/12 by/suzuki	✓		2013-09-14 16:08:57	2013-09-14 16:08:57

# マスター暗号鍵の変更

Oracle Enterprise Manager Cloud Control 12c

Enterprise(E) ターゲット(T) お気に入り(F) 履歴(O) ターゲット名の検索

ora12c.jp.oracle.com 下のユーザーでログイン SYS | secvm12.jp.oracle.com

Oracle データベース パフォーマンス 可用性 スキーマ 管理

Oracle Advanced Security - 透過的データ保護

使用頻度の高い構成オプション

現在使用中のマスター・キー(日数) 0

キー更新

キーストアのステータス OPEN

閉じる

キーストアとマスター・キー

キーストア MORE

キーストアのステータス OPEN

キーストアのタイプ WALLET - PASSWORD

キーストアの場所 /opt/app/oracle/product/12c/dbhome\_1/network/admin

**キー更新**

**警告**  
これは注意を要する操作です。新しいマスター・キーが作成され、「使用中」として設定されます。

キーストアの場所 /opt/app/oracle/product/12c/dbhome\_1/network/admin

\* ウォレット・パスワード ●●●●●●●●

\* キーの説明(タグ) 定期変更 2013/12/12 by Tanaka

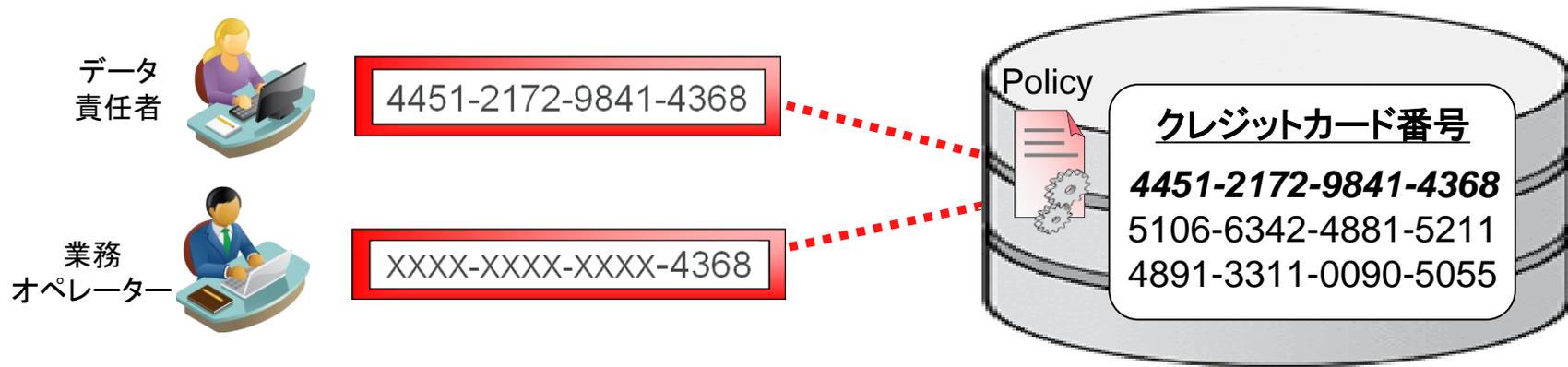
キーストア自動バックアップの識別子

識別子の自動生成

OK 取消

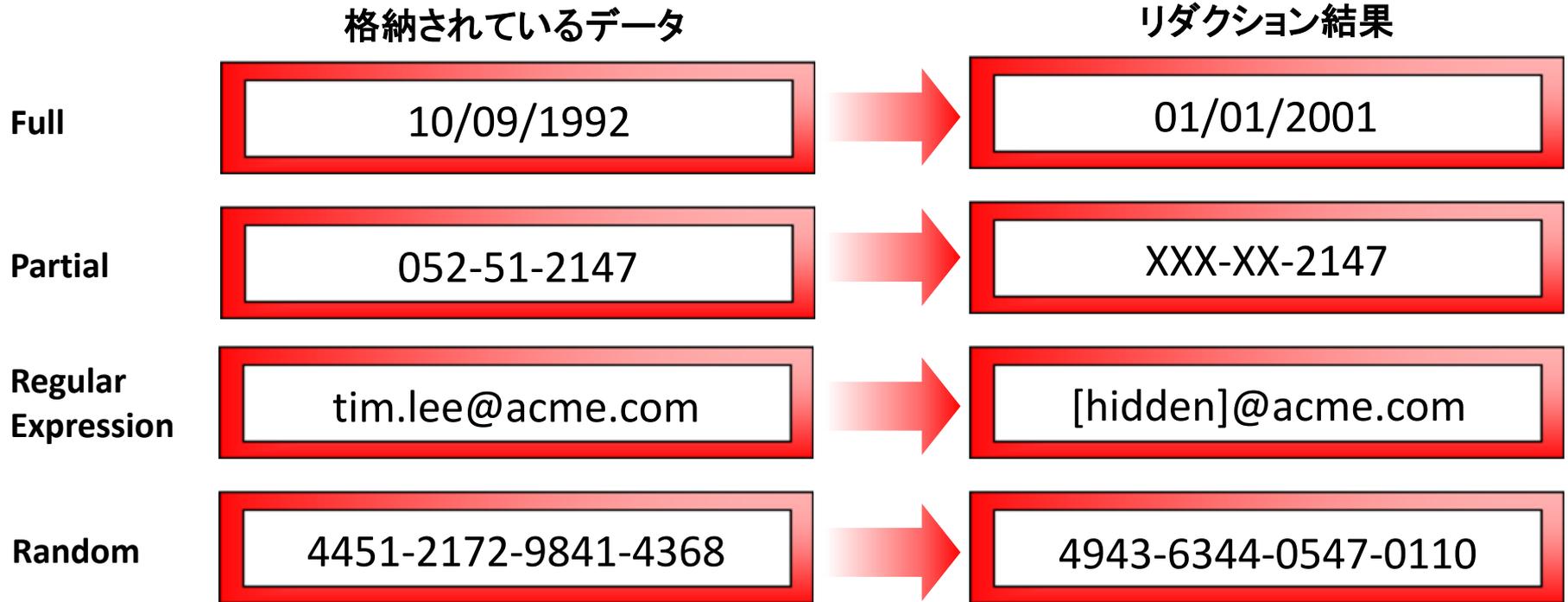
キーの説明(タグ)	ステータス		作成タイムスタンプ	アクティブ化のタイムスタンプ
	使用中	バックアップ済		
initial 2013/09/15		✓	2013-09-14 15:49:36	2013-09-14 15:49:36
定期変更 2013/12/12 by/suzuki	✓		2013-09-14 16:08:57	2013-09-14 16:08:57

# Oracle Data Redaction



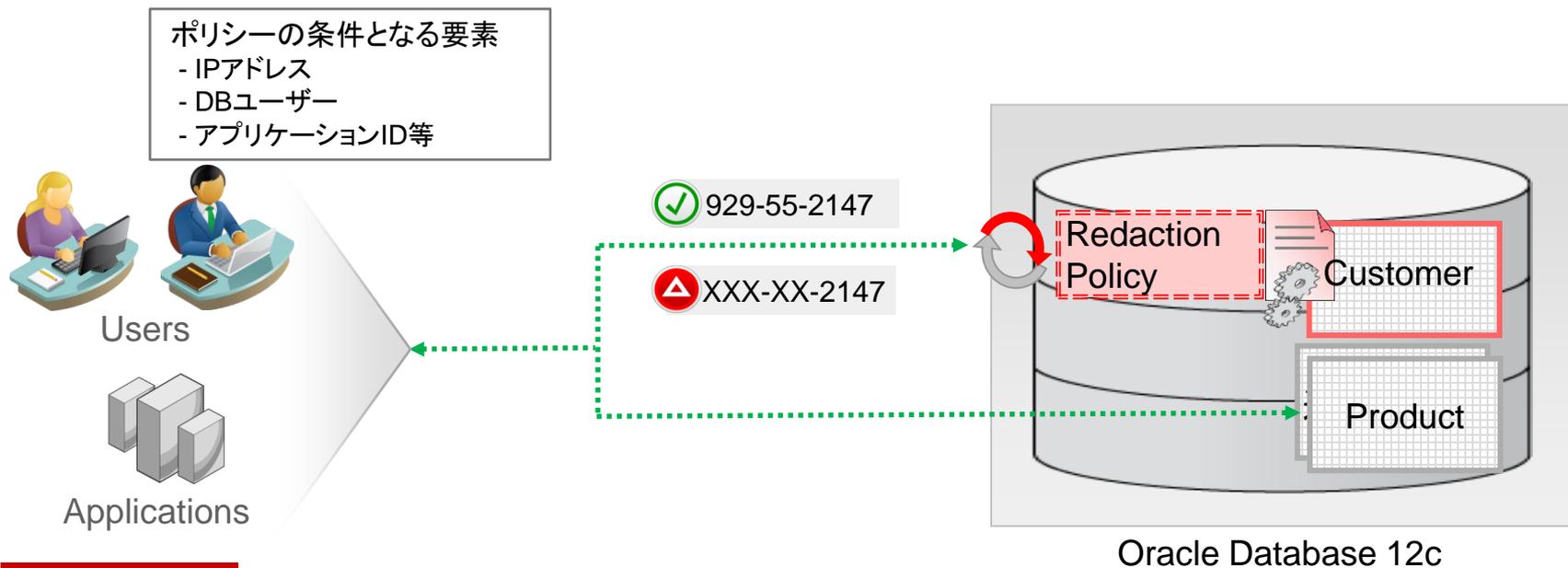
- ユーザーの権限やクライアント情報に応じてリアルタイムにデータをリダクション
- アプリケーションのコード修正は必要のないデータベース内で完結する列アクセス制御
- コールセンターやサポート業務などの職責に応じた顧客情報へのアクセス制御の実現や PCIDSS に対応したクレジットカード番号の表示、アプリ開発者の直接アクセスも制御

# サポートされるリダクションの種類



# Oracle Data Redactionのアーキテクチャ

- リダクション・ポリシーを表やビューに対してDBMS\_REDACTプロシージャで定義
- 対象にできる列は、CHAR/VARCHAR2、NUMBER、DATE、BLOB/CLOB型
- リダクション・ポリシーの条件に応じて、列の値を任意にリダクションする



# リダクション・ポリシーの作成

## DBMS\_REDACT.ADD\_POLICYプロシージャ

DBMS_REDACT.ADD_POLICY	
object_schema	リダクション・ポリシーを適用するスキーマ名
object_name	リダクション・ポリシーを適用する表、またはビュー名
policy_name	作成するリダクション・ポリシー名
column_name	リダクション・ポリシーを適用する列名 ※複数指定したい場合は、DBMS_REDACT.ADD_POLICYで別途追加する
function_type	DBMS_REDACT.FULL DBMS_REDACT.RANDOM DBMS_REDACT.PARTIAL DBMS_REDACT.REGEXP
expression	SYS_CONTEXTの値に基づく、Boolean型の条件式を定義。 条件の結果値が“True”である場合のみ、リダクションが実行される
function_parameters	DBMS_REDACT.PARTIALを使用する場合のデータのINとOUTの定義
regexp.....	function_typeがDBMS_REDACT.REGEXPの場合のオプション群

# Expression(条件式)の作成方法

- SYS\_CONTEXTでセッション情報を取り出し、比較する条件の値を取得する
- 結果がTRUE or FALSEで評価できるように作成し、TRUEの場合にリダクションが行われる

- DBユーザー名がSCOTTの場合

```
SYS_CONTEXT('USERENV','SESSION_USER') = 'SCOTT'
```

- IPアドレスがNULLの場合

```
SYS_CONTEXT('USERENV','IP_ADRESS') IS NULL
```

- クライアント情報にMGRのユーザー名が含まれていなかった場合

```
SYS_CONTEXT('USERENV', CLIENT_IDENTIFIER) not like 'MGR%'
```

- ユーザーがMGRロールを持っていなかった場合

```
SYS_CONTEXT('SYS_SESSION_ROLES','MGR') = FALSE
```

# ユーザ識別子(Client\_identifier)の設定方法

- データベースが知りうるできないアプリケーションの情報は、(シングルサインオンのユーザ名や、使用されているアプリケーションの名前等) Client\_identifierを経由することでデータベースセッションの情報に格納し取り出せる

## SQL\*PLUSの場合

SQL\*PLUSの場合、接続後に以下を実行

```
execute dbms_session.set_identifier('任意の値')
```

Ex)

```
execute dbms_session.set_identifier('user=tanaka id=001234')
```

## JDBCの場合

DBへ接続オープン後、以下を追加

```
String metrics[] =
```

```
new String[OracleConnection.END_TO_END_STATE_INDEX_MAX];
```

```
metrics[OracleConnection.END_TO_END_CLIENTID_INDEX] = "任意の値";
```

```
conn.setEndToEndMetrics(metrics, (short) 0);
```

## ユーザ識別子を取得

```
EXECUTE DBMS_SESSION.SET_IDENTIFIER('APP001');
```

PL/SQLプロシージャが正常に完了しました。

```
SELECT SYS_CONTEXT('USERENV',  
'CLIENT_IDENTIFIER') FROM DUAL;
```

```
SYS_CONTEXT('USERENV','CLIENT_IDENTIFIER')
```

```
-----  
APP001
```

## .NETの場合

DBへ接続オープン後、以下を追加

```
conn.ClientId = "任意の値" ;
```

# DEMONSTRATION

Oracle Security Solutions



# Data Redactionの設定例

ORACLE Enterprise Manager Cloud Control 12c

設定(S) ヘルプ(H) SYSMAN ログアウト

Enterprise(E) ターゲット(T) お気に入り(F) 履歴(O)

ターゲット名の検索

ora12c.jp.oracle.com

次のユーザーでログイン SYSTEM secvm12.jp.oracle.com

Oracleデータベース パフォーマンス 可用性 スキーマ 管理

ページ・リフレッシュ 2013/10/11 12:29:47 JST

### データ・リダクション

Oracle Data Redactionでは、ディスクまたはキャッシュの基礎となるデータベース・ブロックを変更せずに、アプリケーションに表示される機密情報を迅速にリダクションする簡易な方法が用意されています。データはフレキシブルで多角的なポリシーに従ってリアルタイムでリダクションされます。

#### データ・リダクション・ポリシーの検索

スキーマ %  
表/ビュー %  
ポリシー名 %

実行

#### データ・リダクション・ポリシー

作成 編集 表示 有効化 無効化 削除

+	表/ビュー	ポリシー名	有効	リダクションされる列
+	作成			

Enterprise(E) ターゲット(T) お気に入り(F) 履歴(O) ターゲット名の検索

ora12c.jp.oracle.com 次のユーザーでログイン SYSTEM secvm12.jp.oracle.com

Oracleデータベース パフォーマンス 可用性 スキーマ 管理 ページリフレッシュ 2013/10/11 12:30:06 JST

### データ・リダクション・ポリシーの作成:

取消 SQL表示 OK

\* スキーマ  **リダクション対象**

\* 表/ビュー  **・SCOTTユーザー**

\* ポリシー名  **・CUSTOMER表**

\* ポリシー式

リダクションするデータベース・スキーマと表またはビューを選択してData Redactionポリシーを作成し、ポリシー名を割り当てます。

このリストを使用してリダクションする特定の列を選択し、リダクション後のフォーマットを指定します。

3. リダクション・ポリシー式を確認して更新します。ポリシー式のデフォルトは1=1 (TRUE)で、常にリダクションすることを意味します。

鉛筆アイコンをクリックして「ポリシー式ビルダー」ダイアログを表示すると、ポリシー式を簡単に記述できます。論理演算子を使用して複数の条件を結合することもできます。機密データをデフォルトでリダクションし、指定した例外条件が満たされる場合にのみ実データを表示するホワイトリストを作成するときに便利です。

### オブジェクト列

**+** 追加 変更 削除

列名	列のデータ型	リダクション機能	機能属性

## データ・リダクション・ポリシーの編集: app\_policy

取消 SQL表示 OK

\* スキーマ SCOTT  
\* 表/ビュー CUSTOMER  
\* ポリシー名 app\_policy

1=1

\* ポリシー式

手順

追加

\* 列 FIRSTNAME

\* 列のデータ型 VARCHAR2

リダクション・テンプレート カスタム

\* リダクション機能 RANDOM

リダクション対象

- ・FIRSTNAME列
- ・ランダムリダクション

ランダム・リダクション。問い合わせを行ったユーザーに示されるリダクション済のデータは、列のデータ型に応じて、表示されるたびにランダムに生成された値として表示されます。

OK 取消

オブジェクト列

Enterprise(E) ターゲット(T) お気に入り(F) 履歴(O) ターゲット名の検索

ora12c.jp.oracle.com 次ユーザーでログイン SYSTEM secvm12.jp.oracle.com

Oracleデータベース パフォーマンス 可用性 スキーマ 管理 ページ・リフレッシュ 2013/10/11 12:53:17 JST

### データ・リダクション・ポリシーの編集: app\_policy

取消 SQL表示 OK

\* スキーマ SCOTT  
 \* 表/ビュー CUSTOMER  
 \* ポリシー名 app\_policy

1=1 

\* ポリシー式

**手順**

1. リダクションするデータベース・スキーマと表またはビューを選択してData Redactionポリシーを作成し、ポリシーに名前を割り当てます。
2. 下の列リストを使用してリダクションする特定の列を選択し、リダクション後のフォーマットを指定します。
3. リダクション・ポリシー式を確認して更新します。ポリシー式のデフォルトは1=1 (TRUE)で、常にリダクションすることを意味します。

鉛筆アイコンをクリックして「ポリシー式ビルダー」ダイアログを表示すると、ポリシー式を簡単に記述できます。論理演算子を使用して複数の条件を結合することもできます。機密データをデフォルトでリダクションし、指定した例外条件が満たされる場合にのみ表データを表示するホワイトリストを作成するときに便利です。

**オブジェクト列**

+ 追加 変更 削除

列	列のデータ型	リダクション機能	機能属性
CUSTID	VARCHAR2	PARTIAL	WWWFWWWFVWWWVWWWVWWW-VWWW-VWWW-VWWW-VWWW*,1,12
FIRSTNAME	VARCHAR2	RANDOM	
LASTNAME	VARCHAR2	RANDOM	
VALIDDATE	VARCHAR2	FULL	

- リダクション対象**
- CARDNO列 (部分リダクション)
  - FISRTNAME列 (ランダムリダクション)
  - LASTNAME列 (ランダムリダクション)
  - VALIDATE列 (フルリダクション)

Enterprise(E) ターゲット(T) お気に入り(F) 履歴(O) ターゲット名の検索

ora12c.jp.oracle.com 次のユーザーでログイン SYSTEM secvm12.jp.oracle.com

Oracleデータベース パフォーマンス 可用性 スキーマ 管理 ページリフレッシュ 2013/10/11 12:37:25 JST

### データリダクションポリシーの編集: app\_policy

ポリシー式ビルダー

Oracleデータベース環境

- ポリシーの適用時 セッション・ユーザー 次一致しない SCOTT

Oracle APEXアプリケーション

- ポリシーの適用時 アプリケーション・ユーザー 次一致しない BLAKE

Oracleラベル・セキュリティ (OLS)

- ポリシーはユーザーが次の場合に有効 所有しない ラベル C:PCI ポリシー PII\_DATA
- ポリシーはユーザーが次の場合に有効 不可能 ラベルにアクセス C:PCI ポリシー PII\_DATA

ポリシー式

```
SYS_CONTEXT('USERENV', 'SESSION_USER') != 'SCOTT' OR  
SYS_CONTEXT('USERENV', 'SESSION_USER') IS NULL
```

リダクション条件  
・SCOTTユーザ以外は  
リダクションさせる

オブジェクト列

+ 追加 変更 削除

Enterprise(E) ターゲット(T) お気に入り(F) 履歴(O) ターゲット名の検索

ora12c.jp.oracle.com 次ユーザーでログイン SYSTEM | secvm12.jp.oracle.com

Oracleデータベース パフォーマンス 可用性 スキーマ 管理 ページリフレッシュ 2013/10/11 13:13:27 JST

### データ・リダクション・ポリシーの編集: app\_policy

取消 SQL表示 **OK**

\* スキーマ SCOTT

\* 表/ビュー CUSTOMER

\* ポリシー名 app\_policy

\* ポリシー式

```
SYS_CONTEXT('USERENV', 'SESSION_USER')
!= 'SCOTT' OR SYS_CONTEXT('USERENV',
'SESSION_USER') IS NULL
```

**手順**

1. リダクションするデータベース・スキーマと表/ビューを選択してData Redactionポリシーをポリシーに名前を割り当てます。
2. 下のリストを使用してリダクションを選択し、リダクション後のフォーマットを指定します。
3. リダクション・ポリシー式を確認して更新します。ポリシー式のデフォルトはI=1 (TRUE)で、常にリダクションすることを意味します。

鉛筆アイコンをクリックして「ポリシー式」ダイアログを表示すると、ポリシー式を簡単に記述することもできます。AND演算子を使用して複数の条件を結合することもできます。特定の列に指定された機密レベルが満たされる場合にのみデータをリダクションするポリシーを作成するときに便利です。

### リダクション・ポリシー定義

- ・SCOTTユーザ
- ・CUSTOMER表
- ・CARDNO列 (部分リダクション)
- ・FIRSTNAME列 (ランダムリダクション)
- ・LASTNAME列 (ランダムリダクション)
- ・VALIDATE列 (フルリダクション)
- ・条件
- ・SCOTTユーザ以外はリダクションさせる

**オブジェクト列**

+ 追加 変更 削除

列	列のデータ型	リダクション機能	機能属性
CARDNO	VARCHAR2	PARTIAL	WWWVFVWWWVFWVFWVWWWVWWW-VWWW-VWWW-VWWW-VWWW*,1,12
FIRSTNAME	VARCHAR2	RANDOM	
LASTNAME	VARCHAR2	RANDOM	
VALIDDATE	VARCHAR2	FULL	

# Data Redactionの設定完了

ORACLE Enterprise Manager Cloud Control 12c

設定(S) ヘルプ(H) | SYSMAN | ログアウト

Enterprise(E) ターゲット(T) お気に入り(F) 履歴(O) | ターゲット名の検索

ora12c.jp.oracle.com | 次のユーザーでログイン SYSTEM | secvm12.jp.oracle.com

Oracleデータベース パフォーマンス 可用性 スキーマ 管理 | ページ・リフレッシュ 2013/10/11 12:31:57 JST

## データ・リダクション

Oracle Data Redactionでは、ディスクまたはキャッシュの基礎となるデータベース・ブロックを変更せずに、アプリケーションに表示される機密情報を迅速にリダクションする簡易な方法が用意されています。データはフレキシブルで多能的なポリシーに従ってリアルタイムでリダクションされます。

### データ・リダクション・ポリシーの検索

スキーマ %  
表/ビュー %  
ポリシー名 %

実行

### データ・リダクション・ポリシー

作成 編集 表示 有効化 無効化 削除

スキーマ	表/ビュー	ポリシー名	有効	リダクションされる列
SCOTT	CUSTOMER	app_policy		4

# 各バージョンで使用できるASOの機能

	Oracle Database 10g Release 2	Oracle Database 11g Release 1	Oracle Database 11g Release 2	Oracle Database 12c Release1
TDE 列暗号化	✓	✓	✓	✓
TDE 表領域暗号化		✓	✓	✓
TDE HSMサポート		✓	✓	✓
TDE w/Intel AES-NI サポート			✓ (※1)	✓
TDE w/SPARC サポート			✓ (※2)	✓
Data Redaction			✓ (※3)	✓

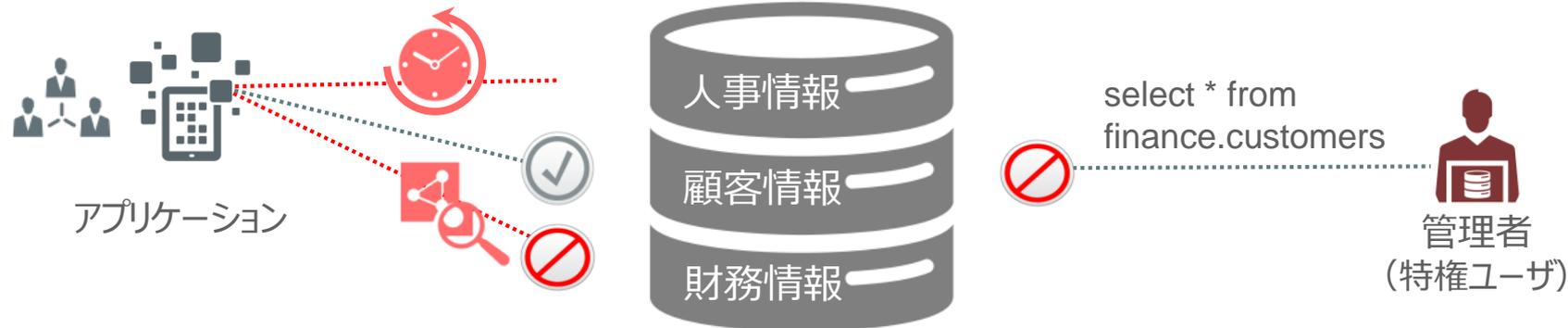
※1 対応プラットフォームは、Oracle Linux / Redhat (64bit), 11.2.0.2～ 注)Windows OSは、11.2.0.4～(対応予定)

※2 対応プラットフォームは、Solaris 11.1 (64bit), SPARC T4/5, 11.2.0.3～

※3 11.2.0.4のみ

# Oracle Database Vault

## 特権ユーザのための強制アクセス・コントロール



### 職務分掌

特権ユーザ（SYS, DBA権限）であっても情報にはアクセスさせない

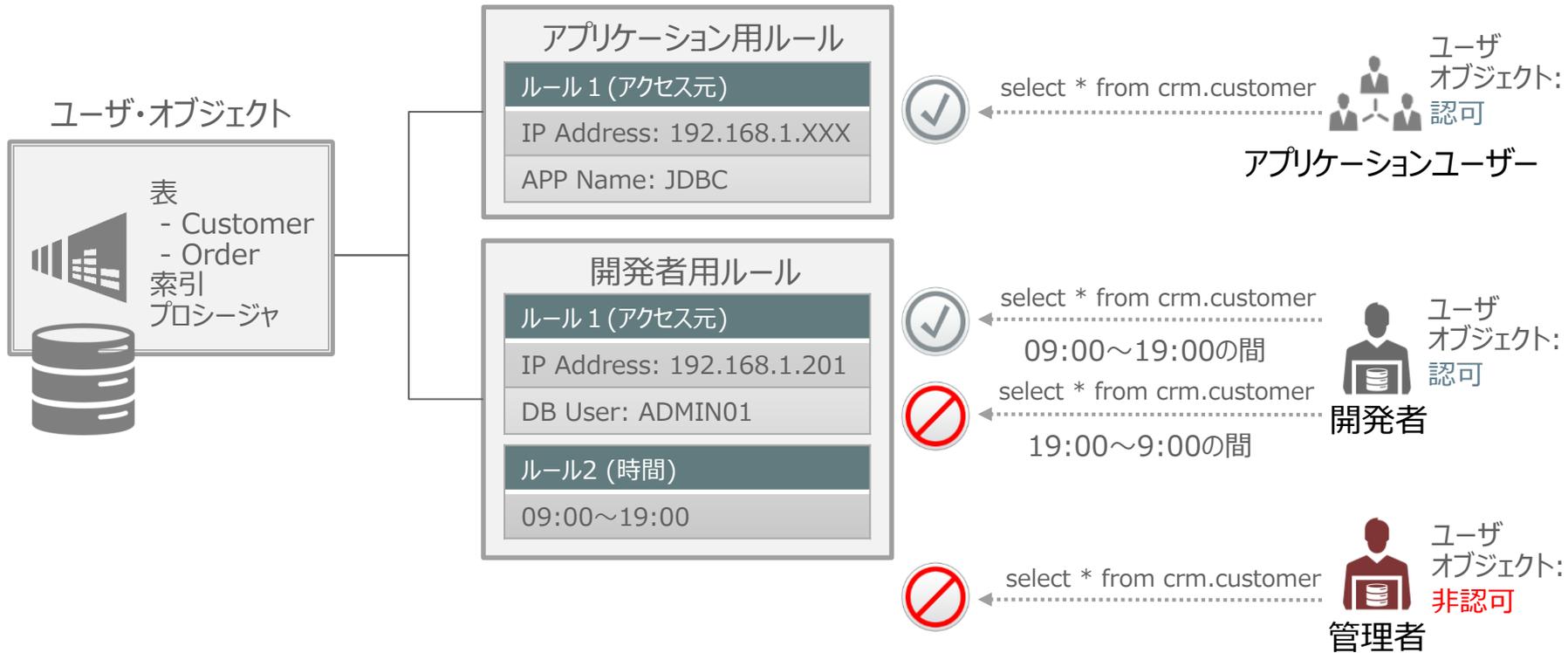
### 透過的

既存アプリケーションの変更不要、どの経路からのアクセスも一律に制御

### 厳密

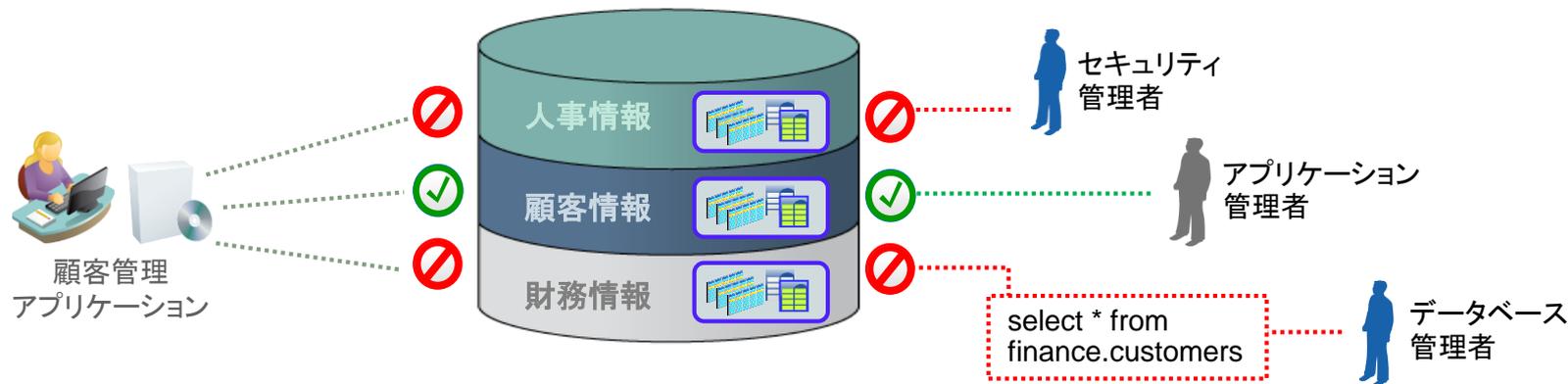
ユーザー、クライアント情報（IPアドレス、アプリ名）、時間を組み合わせたポリシー設定

# 厳密な権限 & ルールの設定により不正アクセスを遮断



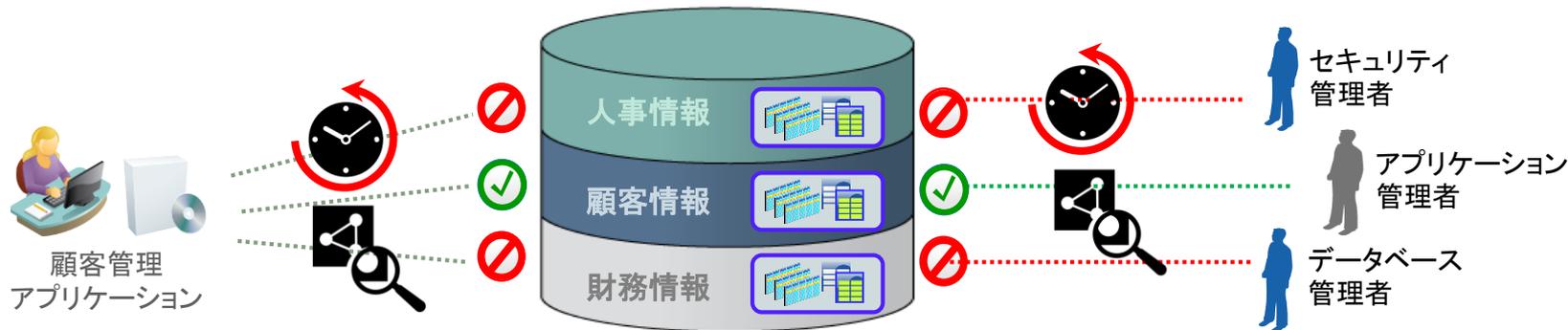
# レルム (Realm)

スキーマ、オブジェクトおよびロールを保護する領域



- ユーザのオブジェクト(表やビュー、パッケージ等)を保護する論理的な領域
- SYSやSYSTEMユーザ、SYSDBAやDBA権限などの特権アクセスはデフォルト拒否される
- 認可されたユーザーのみが、そのレルム内のオブジェクトにアクセス可能
- レルムごとにデータの責任を持つオブジェクト管理者を作成することができる

# ルール・セット (Rule Set)



- レルムやコマンドルールなどに関連づけられる1つ以上のルールの集合体
  - IPアドレスが192.168.1.xxxからのアクセスである
  - 接続ユーザがADMINである
- データベースで取得できる情報を使用して、TRUE またはFALSEで評価される条件
  - Ex) IPアドレスやアプリケーション名などのセッション情報、月日や曜日、時間の情報等が使用可能

# ルール・セットの構成例

## 例) 接続先を限定したルールセット

ルールの紐づけ先

レلم

コマンド  
ルール

セキュア  
アプリケーション  
ロール

ルールセット: 接続先(IPアドレスとユーザ名)で限定する

ルール1:  
IPアドレスが192.168.1.xxxからのアクセスである

ルール2:  
接続ユーザがADMINである



ルールに違反したアクセスはDBの  
監査ログに記録される

ルール1の条件式:

**CLIENT\_IP**

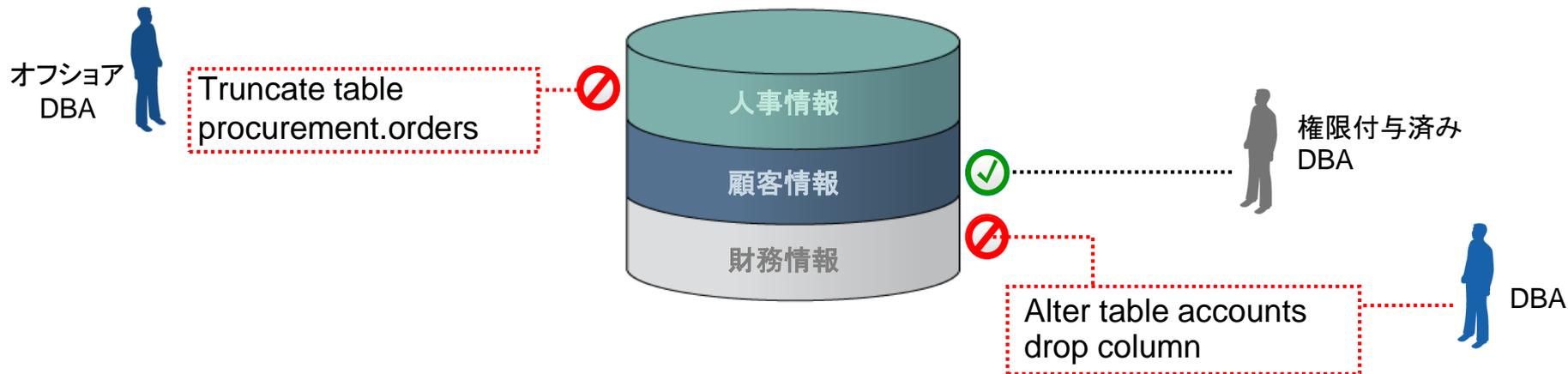
Like '192.168.1.%'

ルール2の条件式:

**SESSION\_USER**

= ADMIN

# コマンドルール (Command Rule)



- SQLコマンドの発行を、ルール・セットに基いて制限する
- ルール・セットがTRUEの場合のみ、SQLコマンドの実行が可能
- SQLコマンドの実行権限(システム権限やオブジェクト権限)は別途必要
- 対象を特定のオブジェクトに対するSELECTやすべてのオブジェクト共通にすることも可能

# コマンドルールで制御できるSQL

ALTER/CREATE/DROP USER	ALTER/CREATE/DROP FUNCTION	ALTER/CREATE/DROP PROCEDURE
ALTER/CREATE/DROP TABLE	ALTER/CREATE/DROP TABLESPACE	ALTER/CREATE/DROP VIEW
ALTER/CREATE/DROP ROLE	ALTER/CREATE/DROP INDEX	ALTER/CREATE/DROP PROFILE
CONNECT	AUDIT	NOAUDIT
CHANGE PASSWORD	GRANT	REVOKE
SELECT	DELETE	INSERT
UPDATE	TRUNCATE TABLE	RENAME

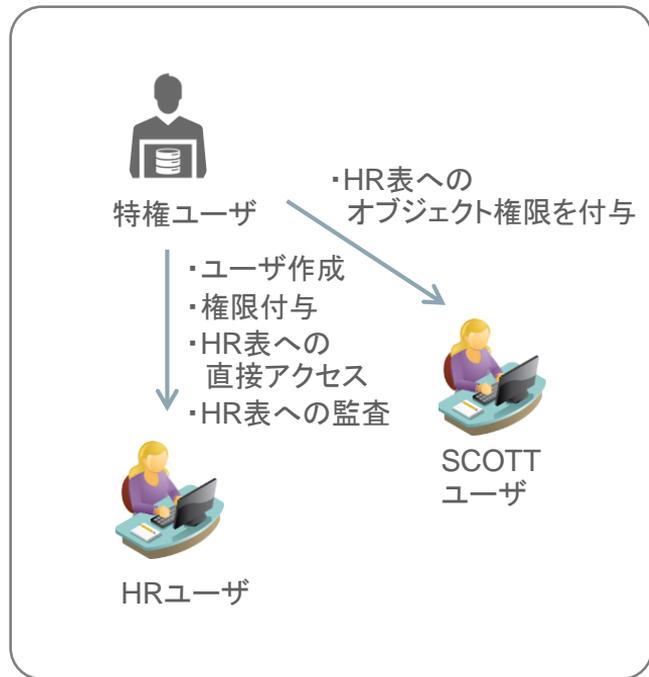
CONNECT ◀ 対象ユーザ: SCOTT + ルール: FALSE SCOTTユーザからの接続を禁止

SELECT ◀ 対象ユーザ: HR + 対象オブジェクト: HR.Employee表 + ルール: SQL\*PLUS

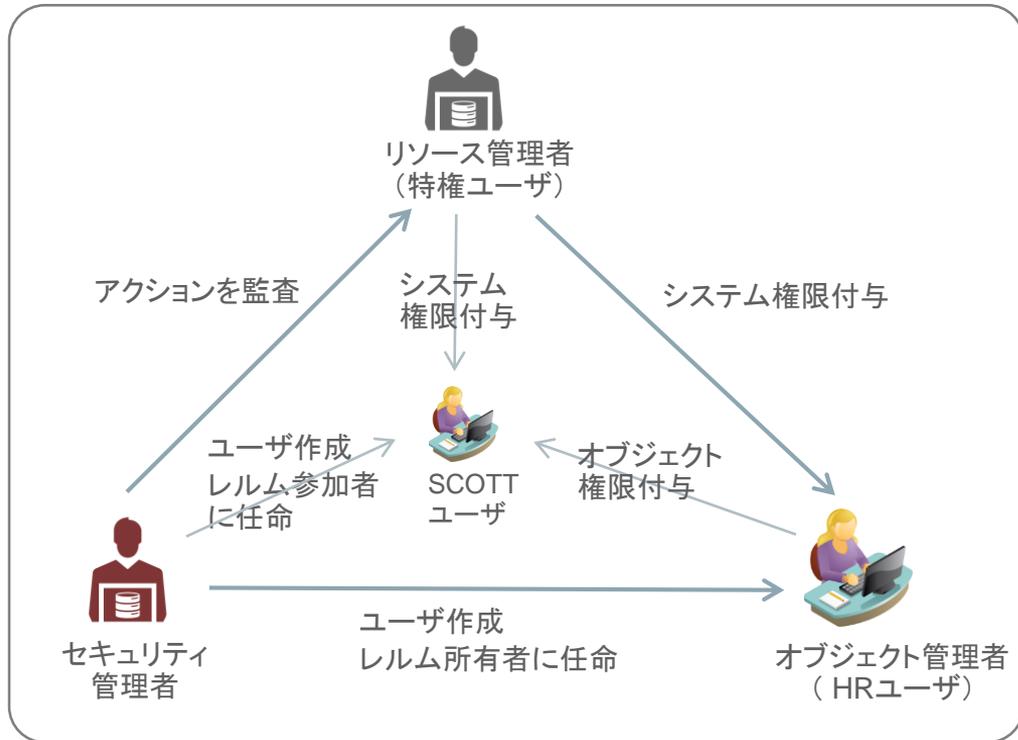
HRユーザがEmployee表をSQL\*PLUSからSELECTすることを禁止

# Database Vaultによる権限分掌と相互監視

## 従来



## Database Vault 環境



# DEMONSTRATION

Oracle Security Solutions



# レلم作成の手順

ORACLE Enterprise Manager Cloud Control 12c

設定(S) ヘルプ(H) SYSMAN ログアウト

Enterprise(E) ターゲット(T) お気に入り(F) 履歴(O) ターゲット名の検索

ora011.jp.oracle.com 次のユーザーでログイン dbv\_owner dbsec11.jp.oracle.com

Oracleデータベース パフォーマンス 可用性 セキュリティ スキーマ 管理 ページリフレッシュ 2014/01/09 4:56:32 JST

### Oracle Database Vault

ホーム・ページ 管理

#### Database Vaultコンポーネント

- レلم**
- コマンド・ルール
- ルール
- ルール・セット
- ファクタ
- ファクタ・タイプ
- セキュア・アプリケーション・ルール
- OLS統合
- Database Vaultロール

#### レلم

Oracle Database Vaultレلمはデータベース・オブジェクトの周囲に保護ゾーンを作成する機能があり、ユーザーはデータにアクセスするためのシステム権限を行使できなくなります。また、必須のレلمでも、データにアクセスするためのオブジェクト権限を行使できなくなり、オブジェクト所有者も自身のスキーマのデータにアクセスできなくなります。

#### 検索

レلم名  実行

検索を行うと、入力した文字列で始まるすべての一致結果が戻されます。検索文字列では、ワイルドカード記号(\*)を使用できます。

ビュー  表示 編集 削除  Oracle定義のレلمの表示

レلم名	監査オプション	有効
データが見つかりま	作成	

# レلم作成の手順

1

レلمの作成: 一般

保護されたオブジェクトへのアクセスを制御するレلمを定義します。レلمに必須のマークを付けた場合、オブジェクト所有者がデータにアクセスできなくなり、その他のユーザーはシステムまたはオブジェクト権限を行使できなくなります。

\*名前

説明 HRユーザのすべてのオブジェクトを保護するレلم

必須レلم

ステータス  有効  
 無効

監査オプション  監査無効  
 成功時に監査  
 失敗時に監査  
 成功時または失敗時に監査

必須レلم  
を  
選択

2

レلمの作成: レلم・セキュア・オブジェクト

レلمで保護する必要があるスキーマ・オブジェクトまたはデータベース・ロールを指定します。ロールを指定する場合、「所有者」フィールドに%を入力します。

所有者	オブジェクト名
HR	%

セキュア・オブジェクトの追加

\*所有者 HR

\*オブジェクト・タイプ %

\*オブジェクト名 %

HRユーザのすべての  
オブジェクトを対象  
(%.%)にする

# レلم作成の手順

3

↑ PDB ⓘ

一般 レلم・セキュア・オブジェクト レلم認可 確認

レلمの作成: レلم認可 戻る ステップ3/4 次 終了 取消

データベース・アカウントまたはデータベース・ロールを、レلمの所有者または参加者のいずれかとして選択します。レلمの所有者および参加者は、レلم・セキュア・オブジェクトにアクセスするためにシステムおよびオブジェクト権限を使用できます。レلمで保護されたデータベース・ロールを付与または取消できるのは、認可されたレلمの所有者のみです。

ビュー ▼ + 追加 ✎ 編集 ✕ 削除

レلم認可の権限受領者	レلم認可ルール・セット
データが見つかりません	

HRユーザをレلمの所有者として認可する

レلم認可の権限受領者: HR

レلم認可タイプ: Owner

レلم認可ルール・セット: Enabled

OK 取消

4

↑ PDB ⓘ

一般 レلم・セキュア・オブジェクト レلم認可 確認

レلمの作成: 確認 戻る ステップ4/4 次 終了 取消

一般

名前: HR\_Realm  
説明: HRユーザのすべてのオブジェクトを保護するレلم  
必須レلم: はい  
ステータス: 有効  
監査オプション: 失敗時に監査

レلم・セキュア・オブジェクト

ビュー ▼

所有者	オブジェクト名
HR	%

レلم認可

ビュー ▼

レلم認可の権限受領者	レلم認可ルール・セット
HR	Enabled

# HRレلمムが動作しているかの確認

```
[oracle@dbsec11 ~]$ sqlplus sys/oracle12c as sysdba@dbsec11.jp.oracle.com:1521/pdb.jp.oracle.com
```

```
SQL*Plus: Release 12.1.0.1.0 Production on 火 8月 12 10:38:48 2014
```

```
Copyright (c) 1982, 2013, Oracle. All rights reserved.
```

```
Oracle Database 12c Enterprise Edition Release 12.1.0.1.0 - 64bit Production  
With the Partitioning, Oracle Label Security, OLAP, Advanced Analytics,  
Oracle Database Vault, Real Application Testing and Unified Auditing options  
に接続されました。
```

```
SQL> show user  
ユーザーは"SYS"です。  
SQL>  
SQL> select * from hr.employees;  
select * from hr.employees  
*  
行1でエラーが発生しました。:  
ORA-01031: 権限が不足しています。
```

SYSユーザからの  
アクセスはできない

## HR\_Realm

- HRのすべてのオブジェクトが対象
- HRがレلمム所有者
- SYSやSYSTEMユーザ、DBAロール、SELECT ANY TABLE等の権限を持っているとしてもレلمム認可されていなければ、左記のようにアクセスはできない
- HRユーザがレلمム所有者なので、オブジェクト権限(DML)の付与などの管理者としての役割を担う
- レلمムに対するアクセス・ルールを含める場合は、後述のルールを設定する

# HRレلمムが動作しているかの確認

```
[oracle@dbsec11 ~]$ sqlplus sys/oracle12c as sysdba@dbsec11.jp.oracle.com:1521/pdb.jp.oracle.com
```

```
SQL*Plus: Release 12.1.0.1.0 Production on 火 8月 12 10:38:48 2014
```

```
Copyright (c) 1982, 2013, Oracle. All rights reserved.
```

```
Oracle Database 12c Enterprise Edition Release 12.1.0.1.0 - 64bit Production  
With the Partitioning, Oracle Label Security, OLAP, Advanced Analytics,  
Oracle Database Vault, Real Application Testing and Unified Auditing options  
に接続されました。
```

```
SQL> show user  
ユーザーは"SYS"です。  
SQL>  
SQL> select * from hr.employees;  
select * from hr.employees  
*  
行1でエラーが発生しました。:  
ORA-01031: 権限が不足しています。
```

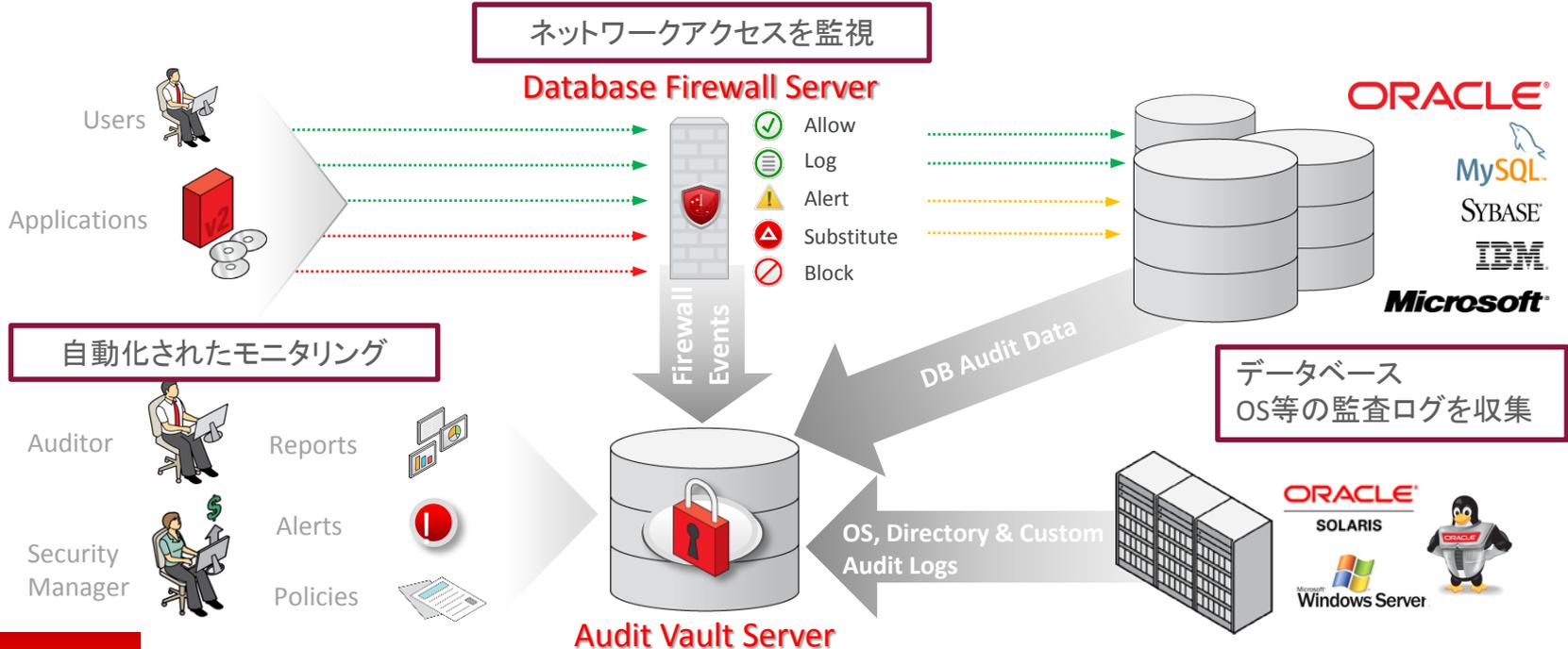
SYSユーザからの  
アクセスはできない

## HR\_Realm

- HRのすべてのオブジェクトが対象
- HRがレلمム所有者
- SYSやSYSTEMユーザ、DBAロール、SELECT ANY TABLE等の権限を持っているとしてもレلمム認可されていなければ、左記のようにアクセスはできない
- HRユーザがレلمム所有者なので、オブジェクト権限(DML)の付与などの管理者としての役割を担う
- レلمムに対するアクセス・ルールを含める場合は、後述のルールを設定する

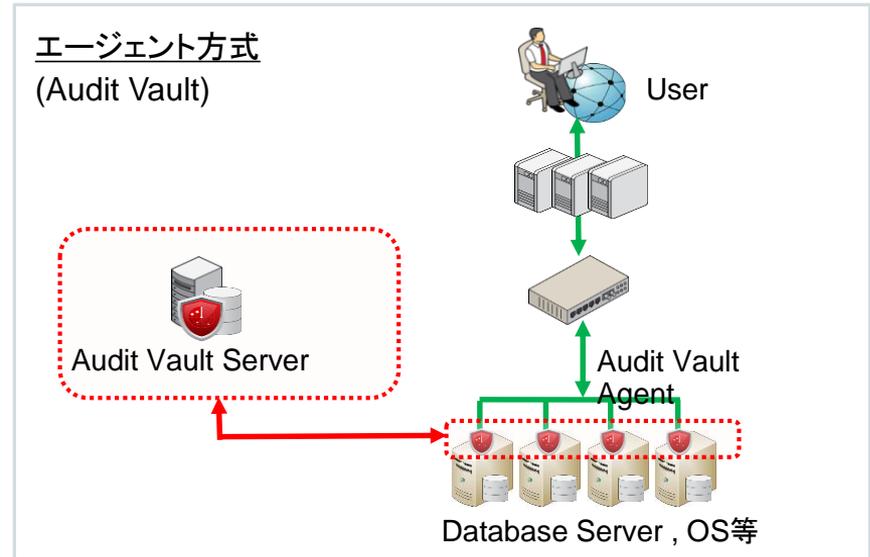
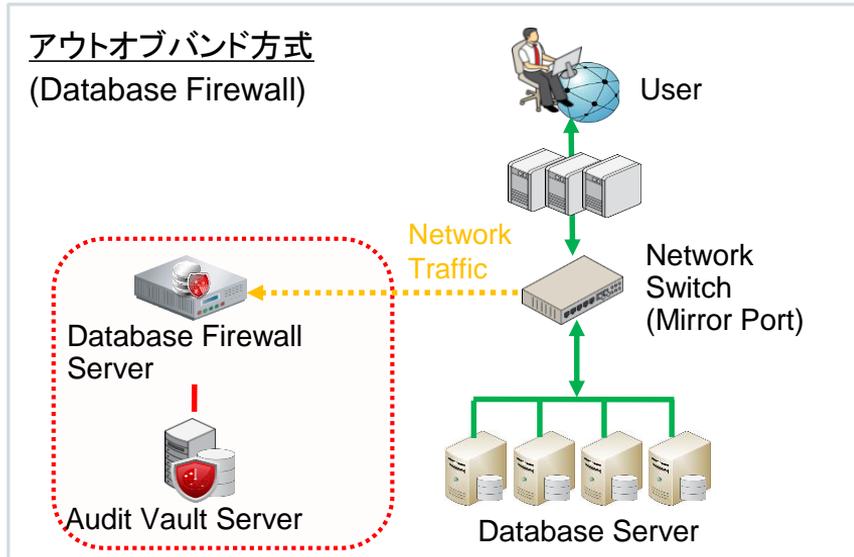
# Oracle Audit Vault and Database Firewall

DatabaseやOSの監査ログを一括集約してモニタリング  
迅速なセキュリティ対策を可能にするソフトウェア・アプライアンス



# 2つのモニタリング方式を提供

- スイッチのミラーポートからSQLパケットをDBFW Serverが受信するオーバヘッドのないアウトオブバンド方式
- Databaseだけでなく、OSやユーザ独自のアプリなど幅広い監査ログの取得を実現するエージェント方式
- お客様のシステムや監査対象に応じて最適な方式を選択、また、組み合わせたハイブリッド方式も可能



# リアルタイムアラート

## アラート条件に基づいて管理者に即座に通知

- Database Firewallがブロッキング、アラート検知した場合
- アラート条件としきい値を超えた場合、指定されたメールアドレスにアラートメール、SYSLOGで送信



差出人 test <avserver@oracle.com>☆  
件名 Audit Vault Alert: sql\_error, 6/18/2013 1:01:50 PM  
宛先 (自分) <test@secvm3.jp.oracle.com>☆

アラートが発生しています。至急確認して下さい。  
Please do not reply to this email. This is an automated message.

Attribute	Value
Alert Name	sql_error
Event Time	6/18/2013 1:04:06 PM
Alert Status	New
Alert Severity	Warning
Description	
URL	https://10.185.151.1/console/f?p=7700:33:::NO::P33_ALERT_ID:244



**Alerts**

条件:  
イベント時間  
IPアドレス, ホスト名  
エラーコード  
ユーザ名  
SQLコマンドなど

アラートの作成

名前 \* Longin\_Fail

セキュア・ターゲット・タイプ Oracle Database

重大度 \* Warning

しきい値(回数) \* 5

期間(分) \* 1

グループ化(フィールド) -フィールドの選択-

説明

1分間の間にログインが5回以上失敗した場合、アラートを送信する

32 / 255

条件 \*

.ERROR\_CODE=1017

16 / 4000



# Oracle Database 12c おすすめ研修コース

## Oracle Database 12c: Database Vault

概要	このコースでは、Oracle Database Vaultを有効化し、レルム、ルール・セット、コマンド・ルール、セキュア・アプリケーション・ロールを用いてデータベース・インスタンスのセキュリティを管理する方法を説明します。また、レポートや監視を使用してセキュリティ違反行為をチェックする方法について説明します。講義と演習を通じてOracle Database Vault が提供する強力なセキュリティ統制のための機能の活用方法を習得できます。	
学習項目	<ul style="list-style-type: none"><li>■ Database Vaultの概要</li><li>■ Database Vaultの構成</li><li>■ 権限の分析 (12c 新機能)</li><li>■ レルムの構成</li><li>■ ルール・セットの定義</li></ul>	<ul style="list-style-type: none"><li>■ コマンド・ルールの構成</li><li>■ ルール・セットの拡張</li><li>■ セキュア・アプリケーション・ロールの構成</li><li>■ Database Vaultレポートによる監査</li><li>■ ベスト・プラクティスの実装</li></ul>
コース日数	2 日間 【トレーニングキャンパス赤坂】2014/12/18-19	

## Oracle Database 12c: セキュリティ

概要	このコースでは、認証、権限とロールの管理に加えて、Oracle Label Security、データベース暗号化、およびOracle Data Reductionなどを使用した機密データの保護する方法を説明します。また統合監査やファイナグレイン監査を構成する方法について説明します。講義と演習を通じてデータベースへのアクセスを保護し機密性を高める方法を習得できます。		
学習項目	<ul style="list-style-type: none"><li>■ セキュリティ要件について</li><li>■ セキュリティ・ソリューションの選択</li><li>■ 基本的なデータベース・セキュリティ</li><li>■ ネットワーク・サービスの保護</li><li>■ ユーザーのBasic認証と厳密認証の使用</li><li>■ グローバル・ユーザー認証の使用</li><li>■ プロキシ認証の使用</li></ul>	<ul style="list-style-type: none"><li>■ 権限とロールの使用</li><li>■ 権限分析の使用 (12c新機能)</li><li>■ アプリケーション・コンテキストの使用</li><li>■ 仮想プライベート・データベースの実装</li><li>■ Oracle Label Security の使用</li><li>■ データ・リダクション (12c新機能)</li><li>■ データ・マスキングの使用</li></ul>	<ul style="list-style-type: none"><li>■ 透過的機密データ保護の使用 (12c新機能)</li><li>■ 暗号化の概念とソリューション</li><li>■ DBMS_CRYPTO パッケージを使用した暗号化</li><li>■ 透過的データ暗号化の使用</li><li>■ データベース・ストレージのセキュリティ</li><li>■ 統合監査の使用 (12c新機能)</li><li>■ ファイングレイン監査の使用</li></ul>
コース日数	5 日間 【トレーニングキャンパス赤坂】2015/1/19-23		

詳細は [Oracle University Webサイト](#)にてご確認ください。

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

**VISION 2020**

**#1 CLOUD**

**ORACLE JAPAN**

ORACLE®