
ORACLE®

#odddtky

Oracle DBA & Developer Days 2014

データベース・セキュリティの実装をすべて解説

西村克也
プリンシパルエンジニア, CISSP

日本オラクル株式会社
製品戦略統括本部
データベースエンジニアリング本部

for your **Skill**

使える実践的なノウハウがここにある

Oracle
DBA & Developer Days
2014

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

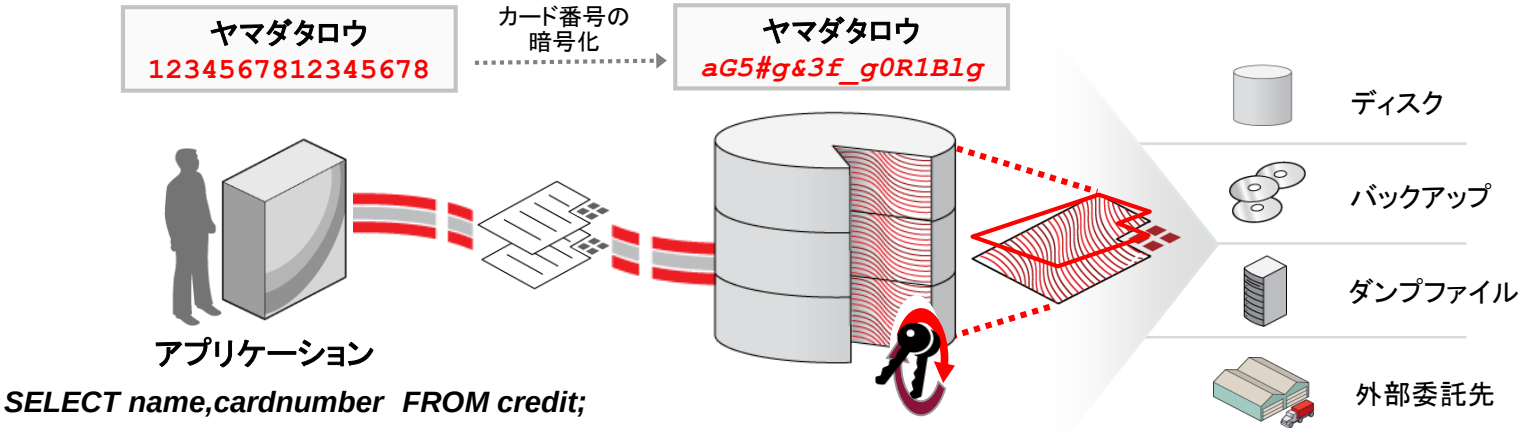
Oracle Advanced Securityが実現するセキュリティ対策

データの暗号化
Transparent Data Encryption

リアルタイムアクセス制御
Data Redaction

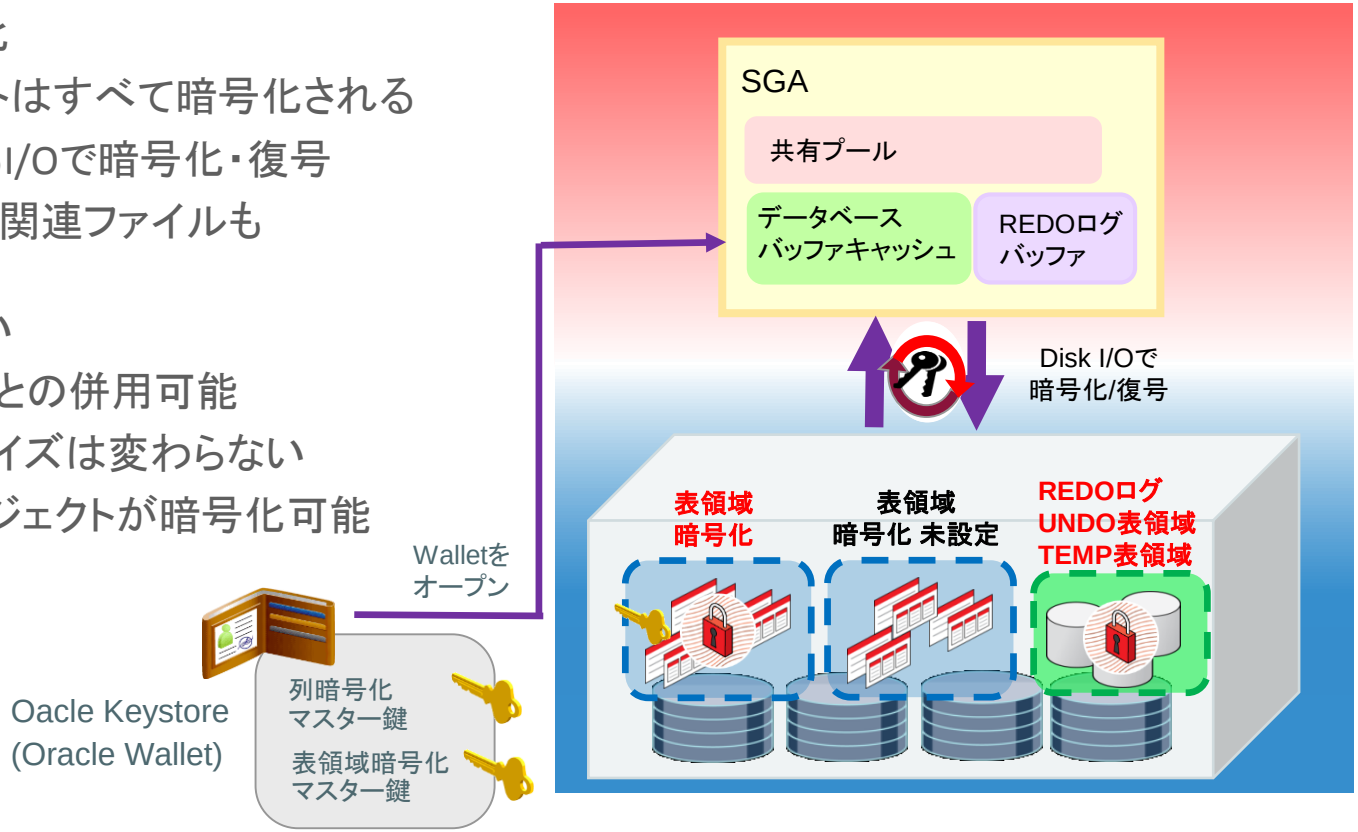
Transparent Data Encryption（TDE）

- 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



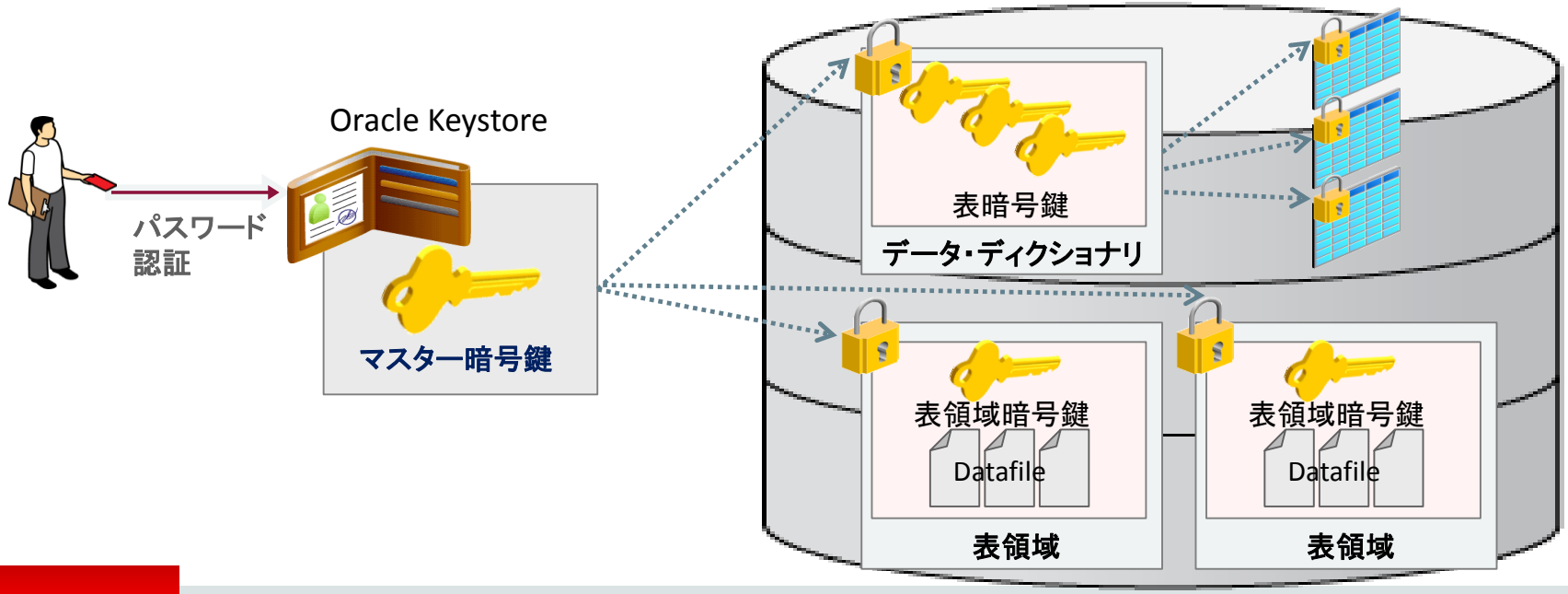
TDE 表領域暗号化

- 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)



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
------------------------------------------------------------------------------- ---------------------------
AfrZm0w5EE9kv2NNme6cpwIAAAAAAAAAAAAAAAAAAAAAAAAAAAAA  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

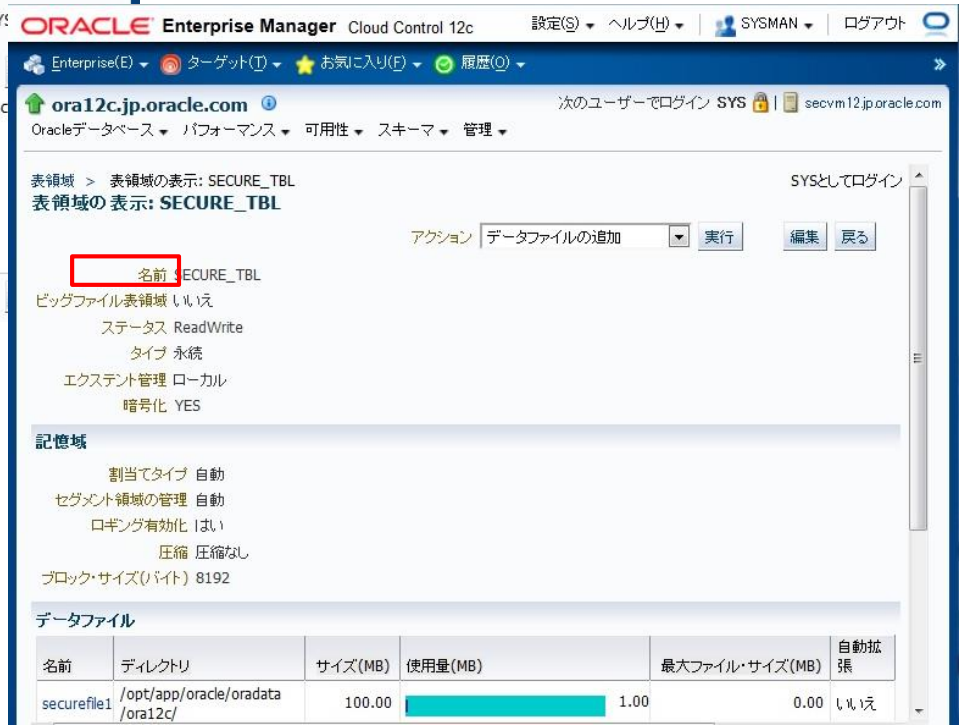
```
CREATE TABLESPACE securespace
DATAFILE '/opt/app/oracle/oradata/ora12c/enc.dbf' SIZE 100M ENCRYPTION USING 'AES256'
DEFAULT STORAGE (ENCRYPT);
```

- 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

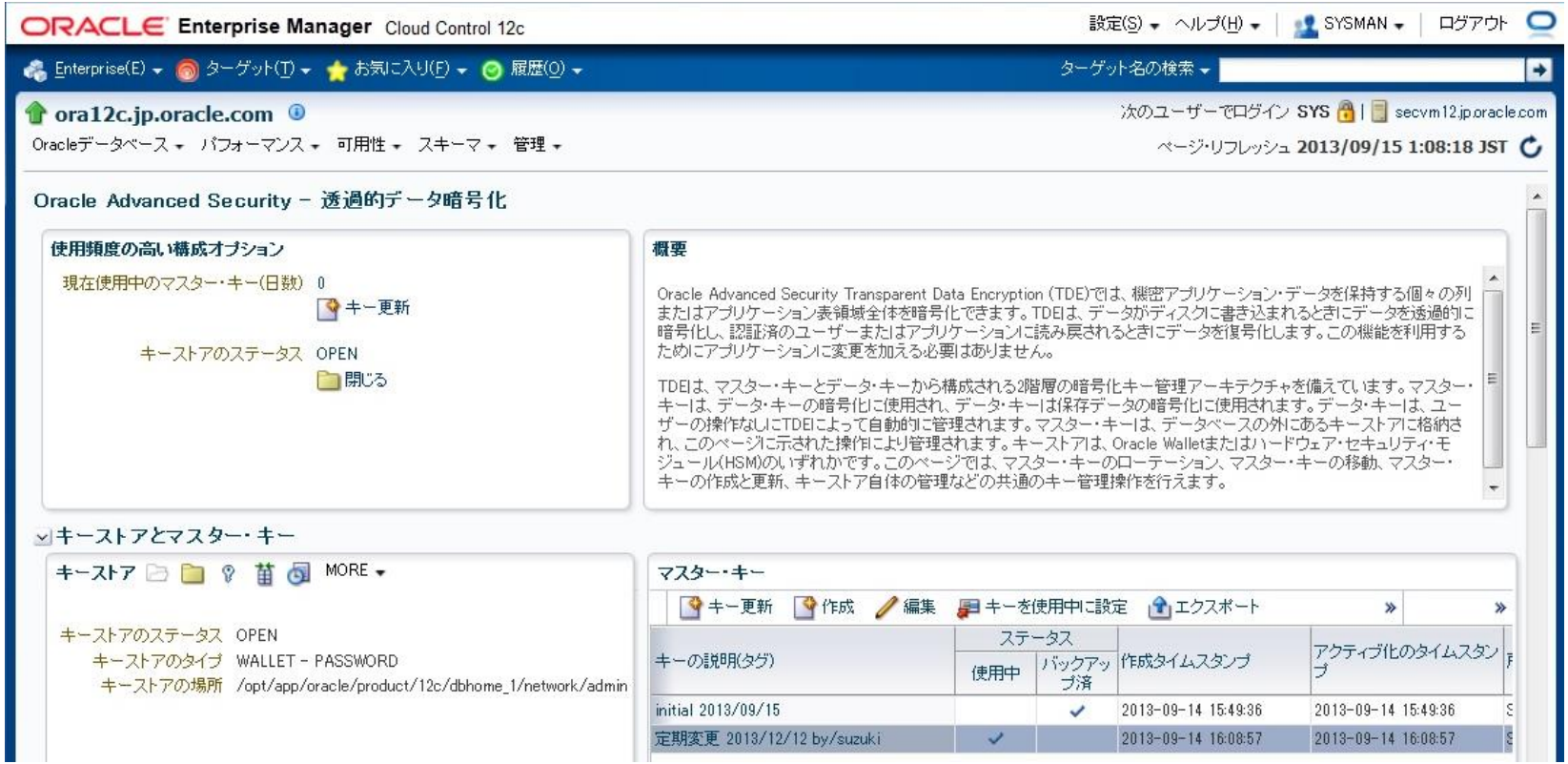
※ 既存の表を暗号化された表領域に移動する場合
- 表のオンライン再定義 (DBMS_REDEFINITION)
- ALTER TABLE MOVE ～
- Oracle DataPump Export/Import

DEMONSTRATION

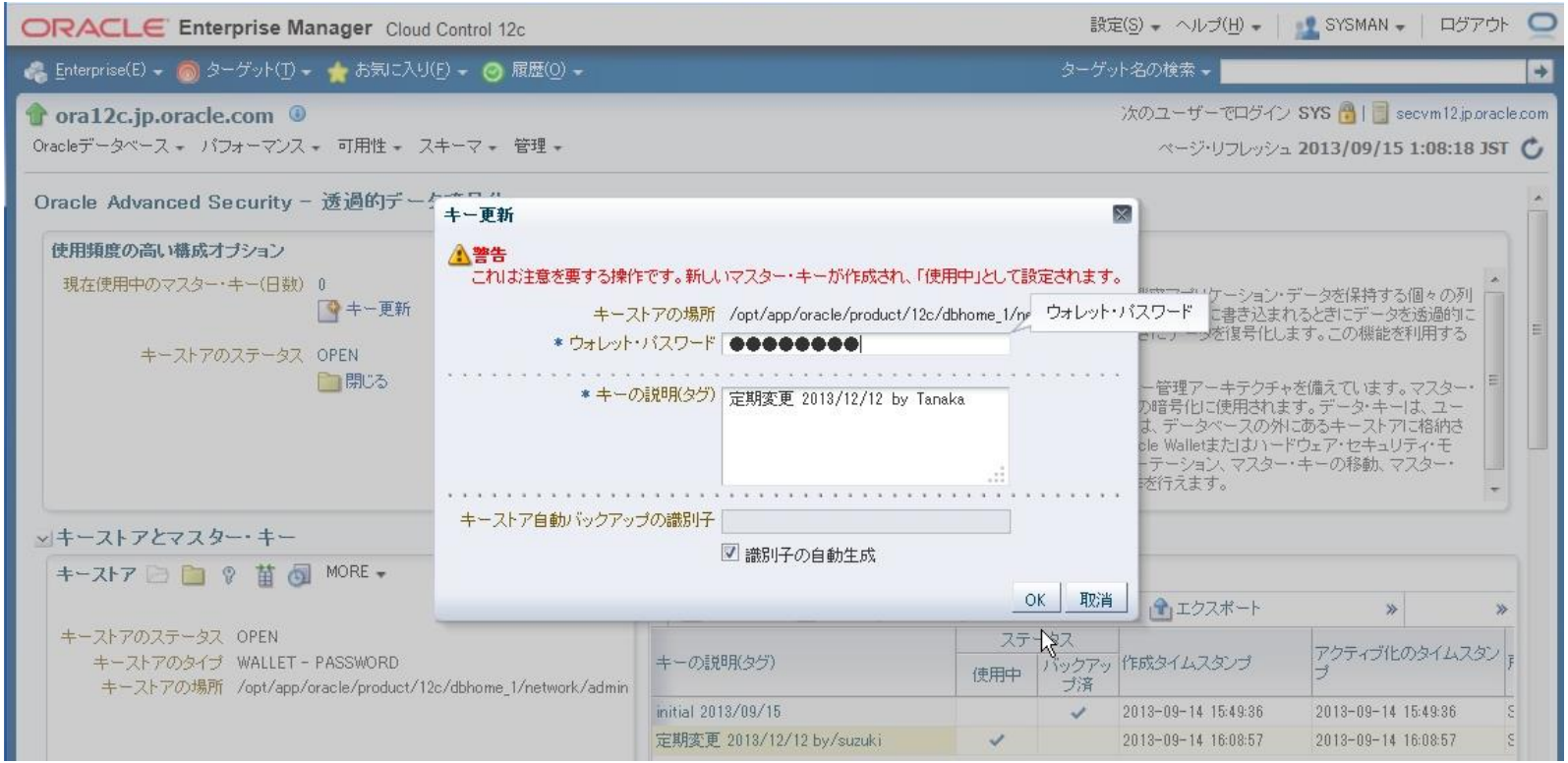
Oracle Enterprise Managerによる暗号化表領域の設定例



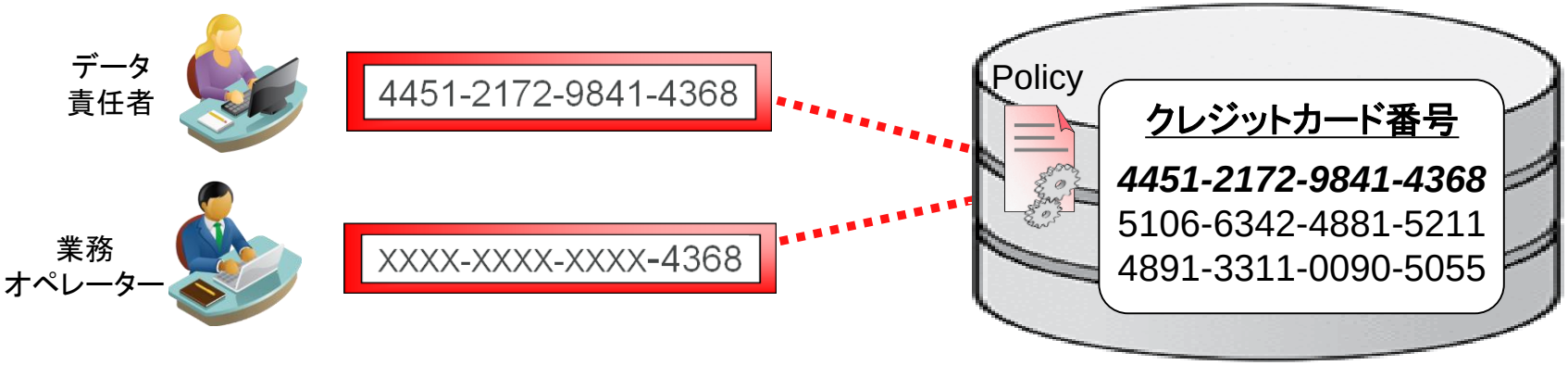
暗号鍵の管理



マスター暗号鍵の変更

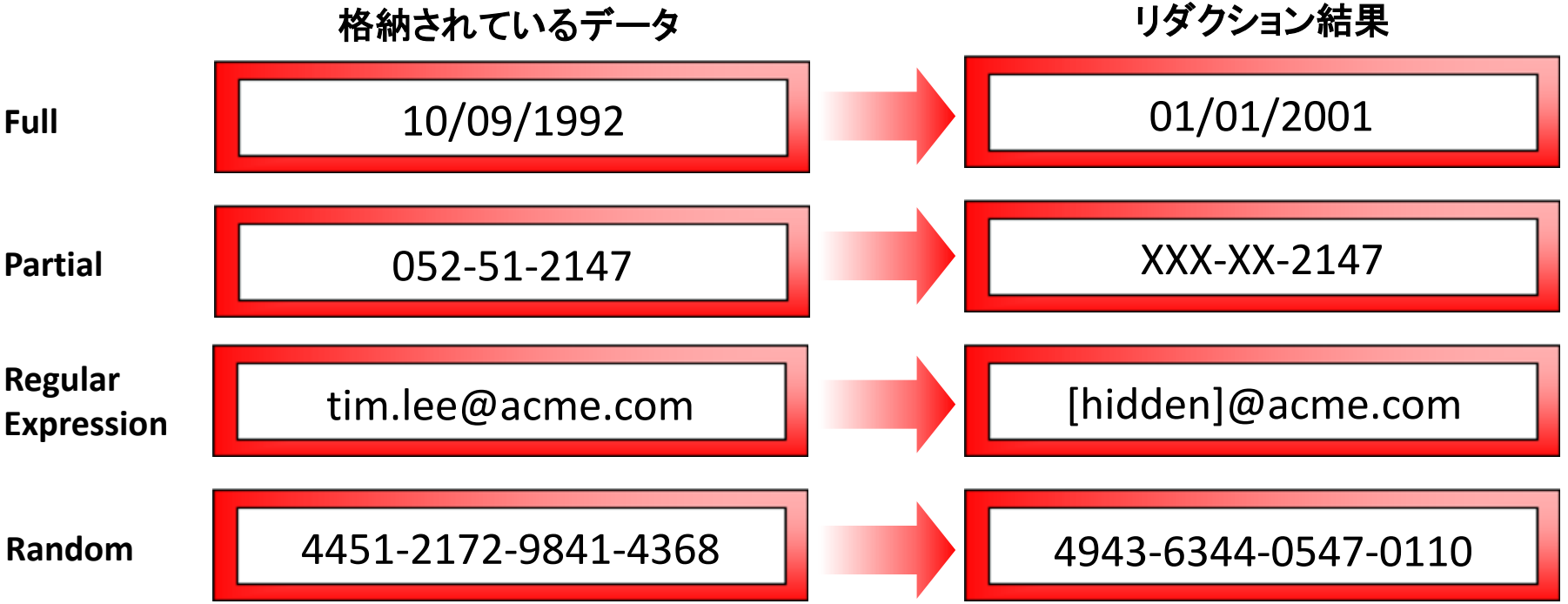


Oracle Data Redaction



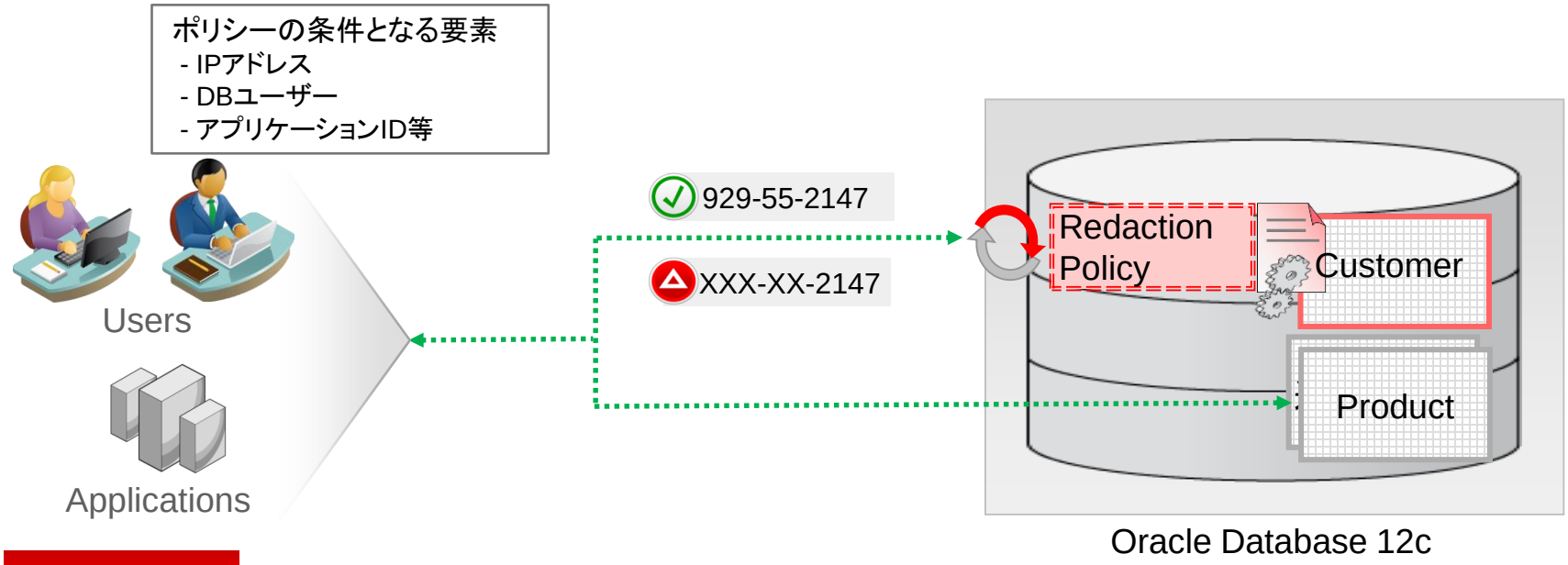
- ユーザーの権限やクライアント情報に応じてリアルタイムにデータをリダクション
- アプリケーションのコード修正は必要のないデータベース内で完結する列アクセス制御
- コールセンターやサポート業務などの職責に応じた顧客情報へのアクセス制御の実現やPCIDSSに対応したクレジットカード番号の表示、アプリ開発者の直接アクセスも制御

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ことが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
```

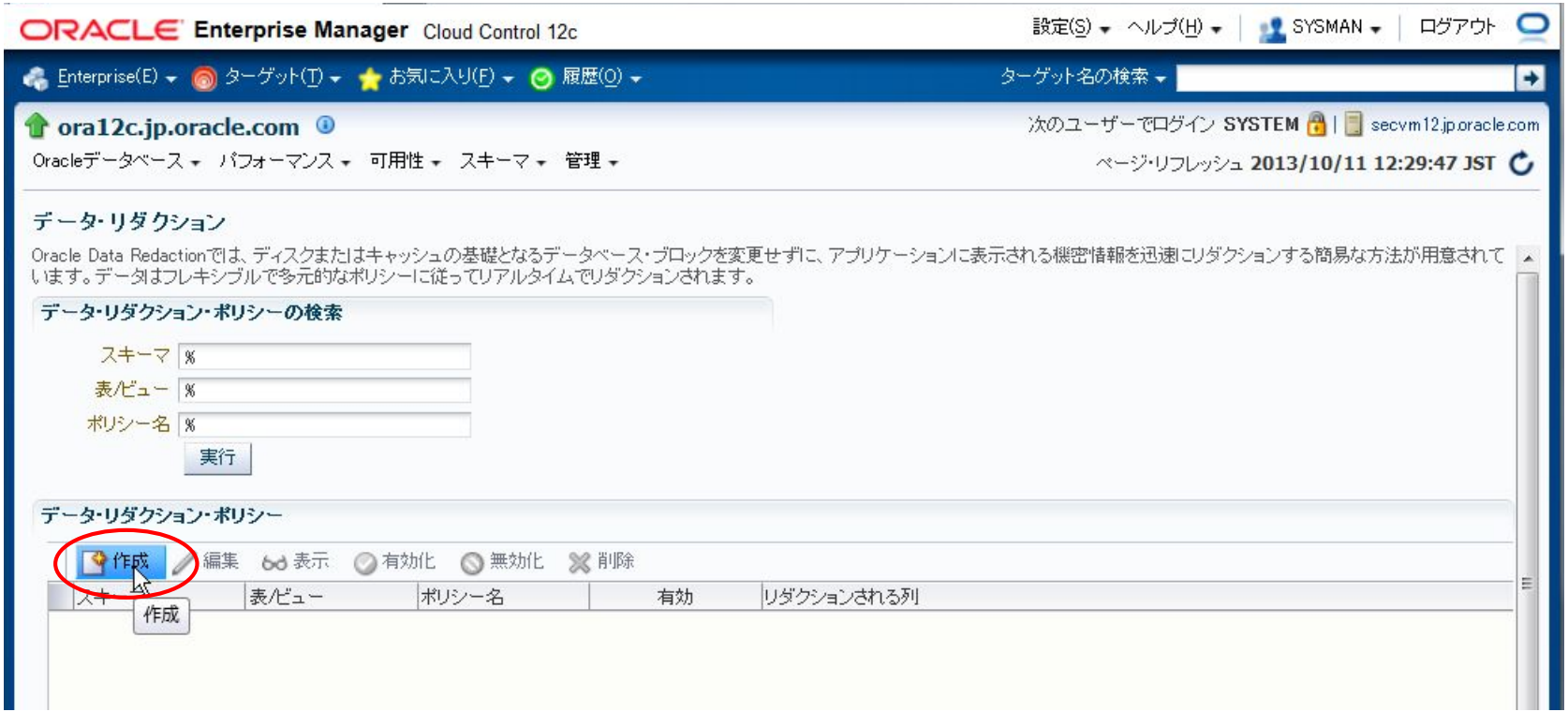
.NETの場合

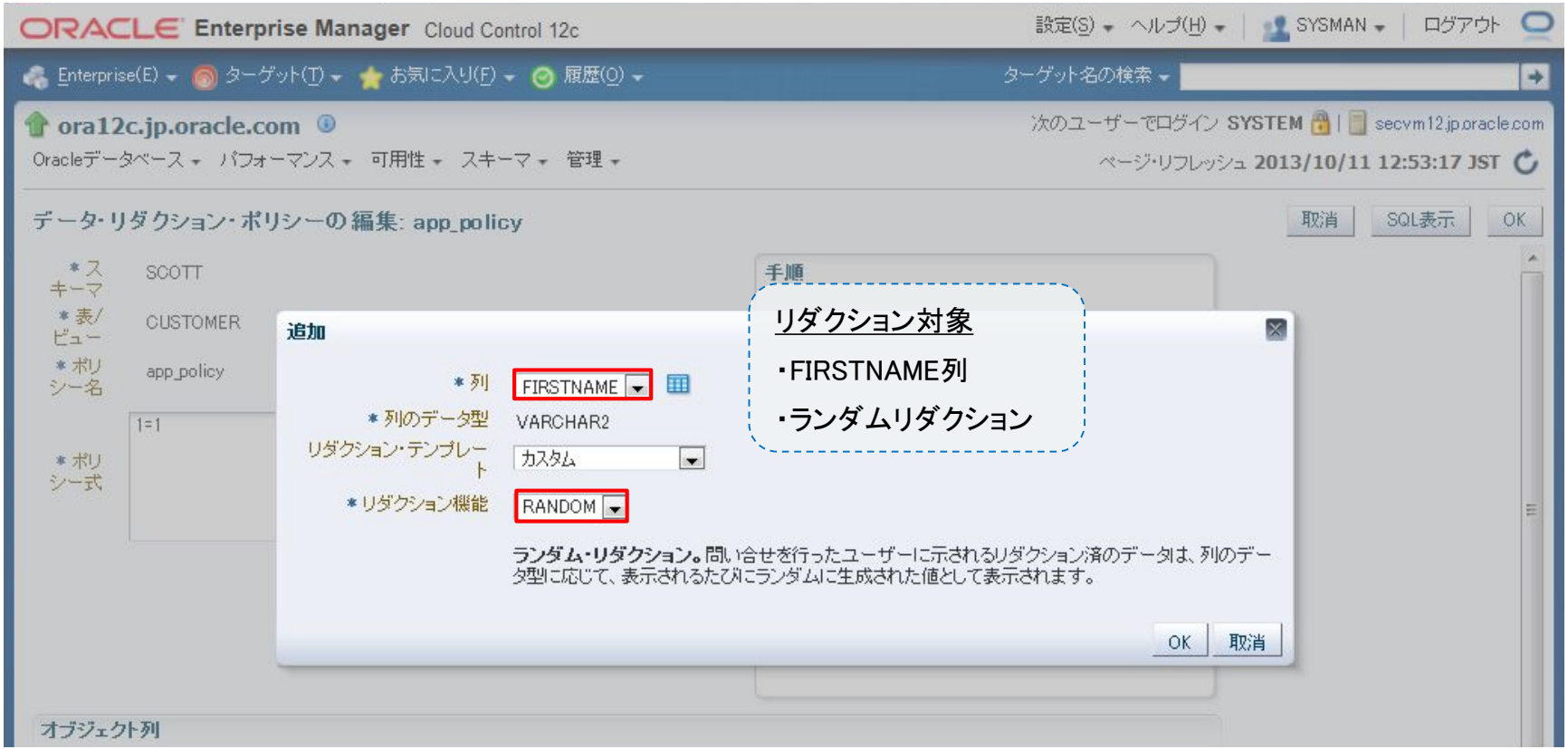
DBへ接続オープン後、以下を追加

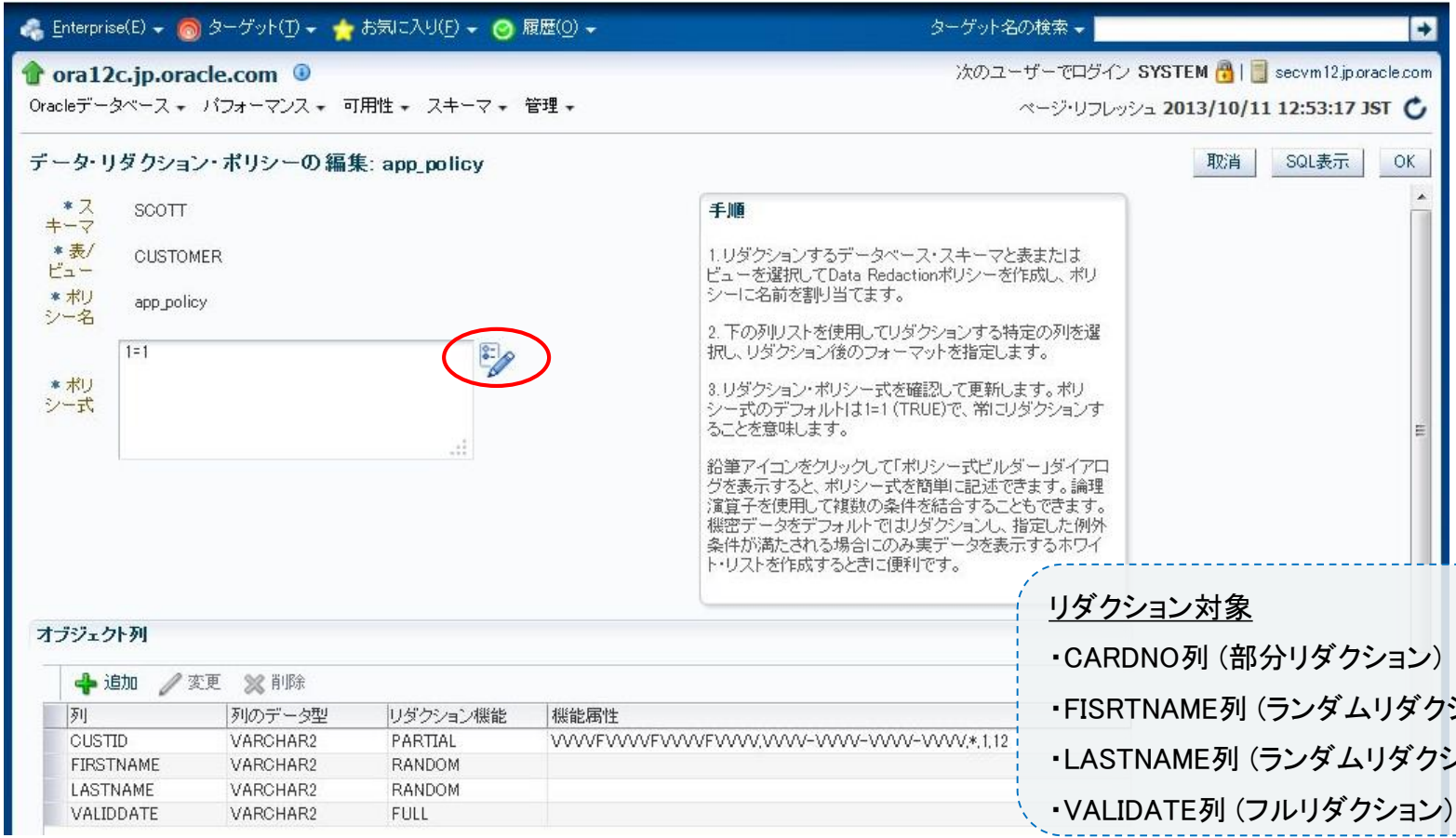
conn.ClientId = “任意の値” ‘

DEMONSTRATION

Data Redactionの設定例

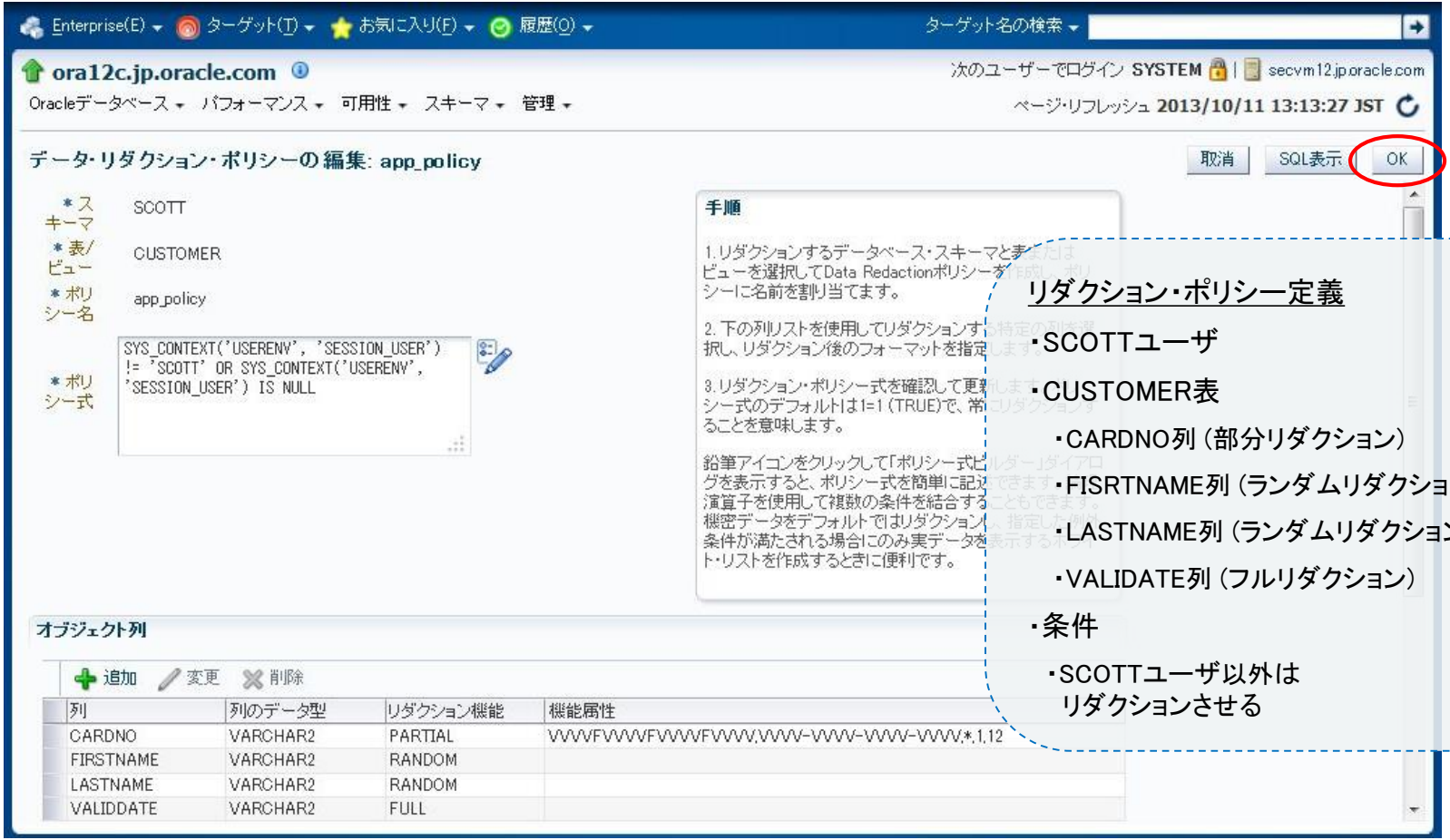






リダクション対象

- 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）



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）
  - 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）
- 条件
  - SCOTTユーザ以外は リダクションさせる

Data Redactionの設定完了

各バージョンで使用できるASOの機能

	Oracle Database 10*g* Release 2	Oracle Database 11*g* Release 1	Oracle Database 11*g* 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)	✓

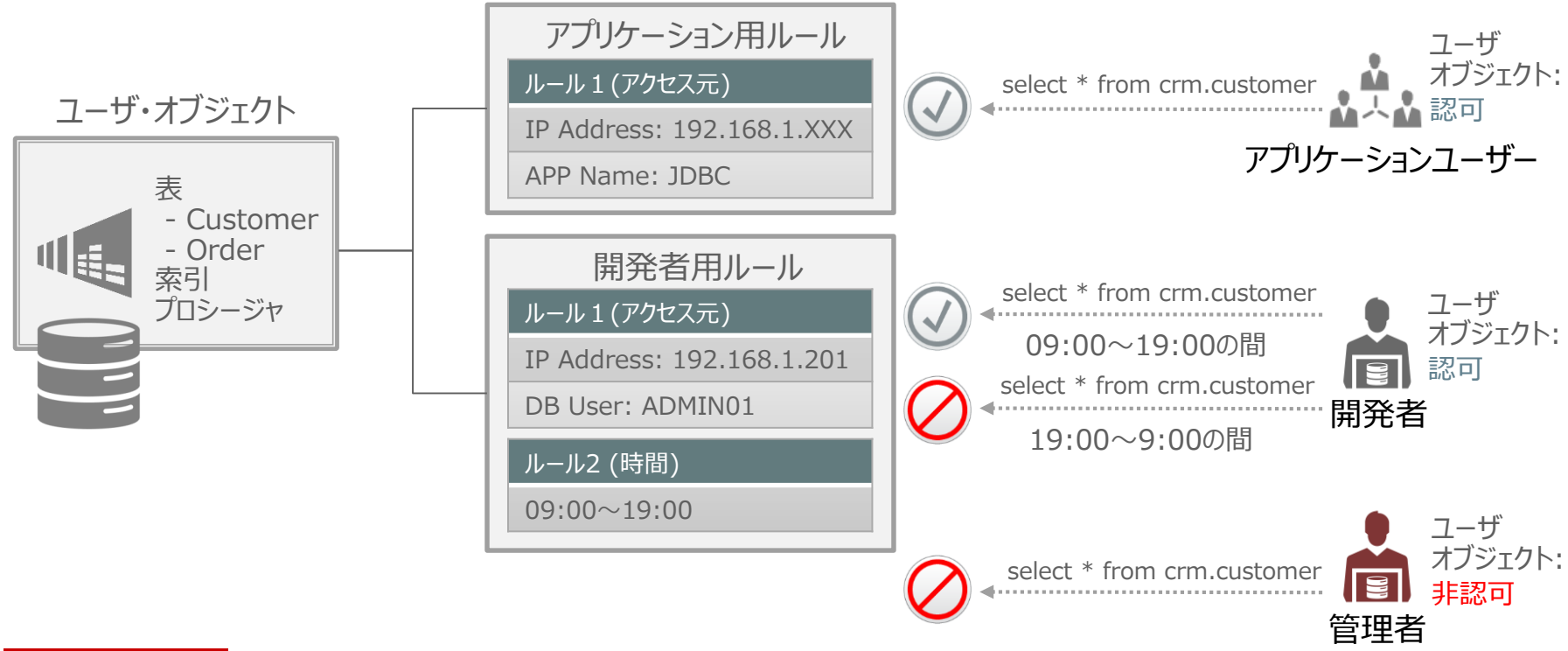
※1 対応プラットフォームは、Oracle Linux / Redhat (64bit), 11.2.0.2～　注)Windows OSは、11.2.0.4～(対応予定)
※2 対応プラットフォームは、Solaris 11.1 (64bit), SPARC T4/5, 11.2.0.3～
※3 11.2.0.4のみ

Oracle Database Vault

特権ユーザのための強制アクセス・コントロール

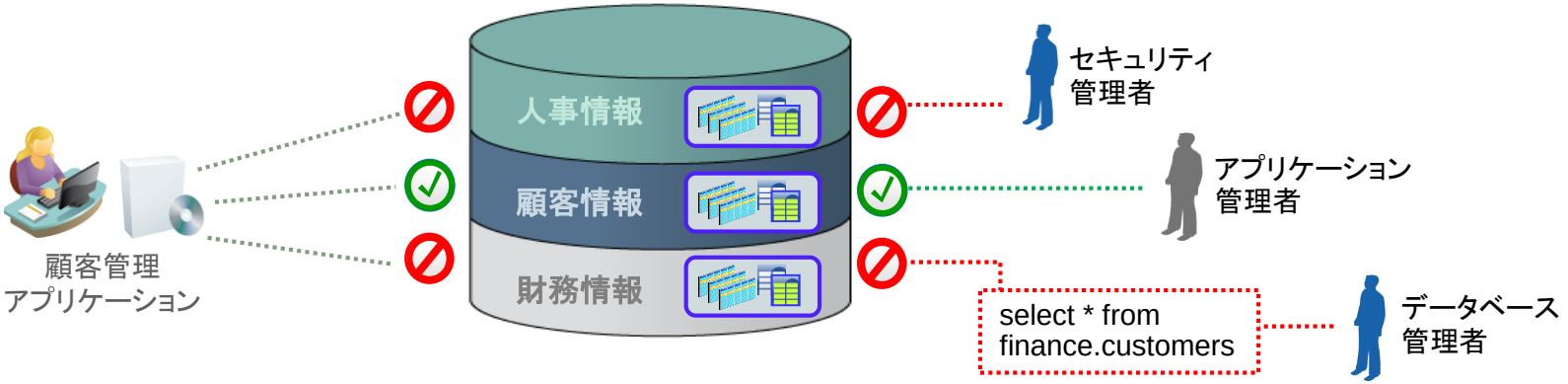
職務分掌	特権ユーザ（SYS, DBA権限）であっても情報にはアクセスさせない
透過的	既存アプリケーションの変更不要、どの経路からのアクセスも一律に制御
厳密	ユーザー、クライアント情報（IPアドレス、アプリ名）、時間を組み合わせたポリシー設定

厳密な権限＆ルールの設定により不正アクセスを遮断



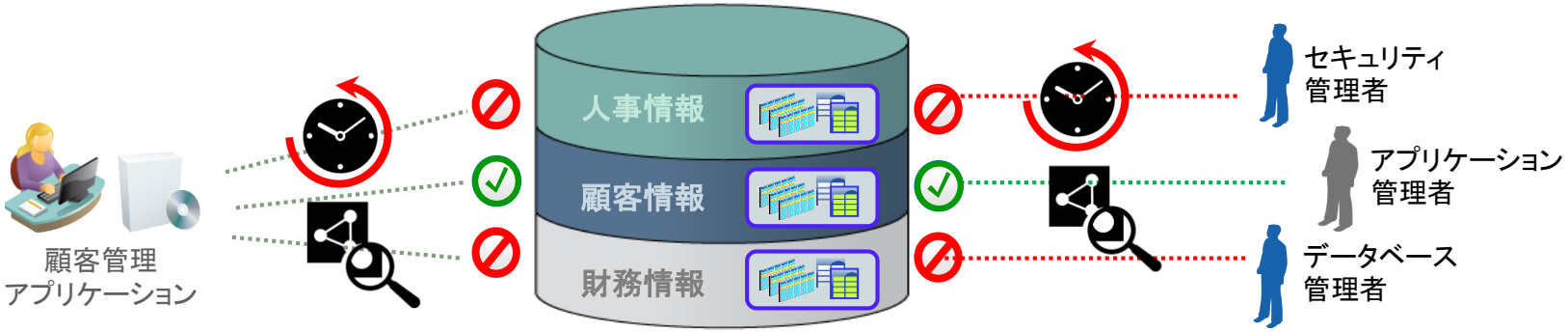
レルム（Realm）

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

- レルム
- 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

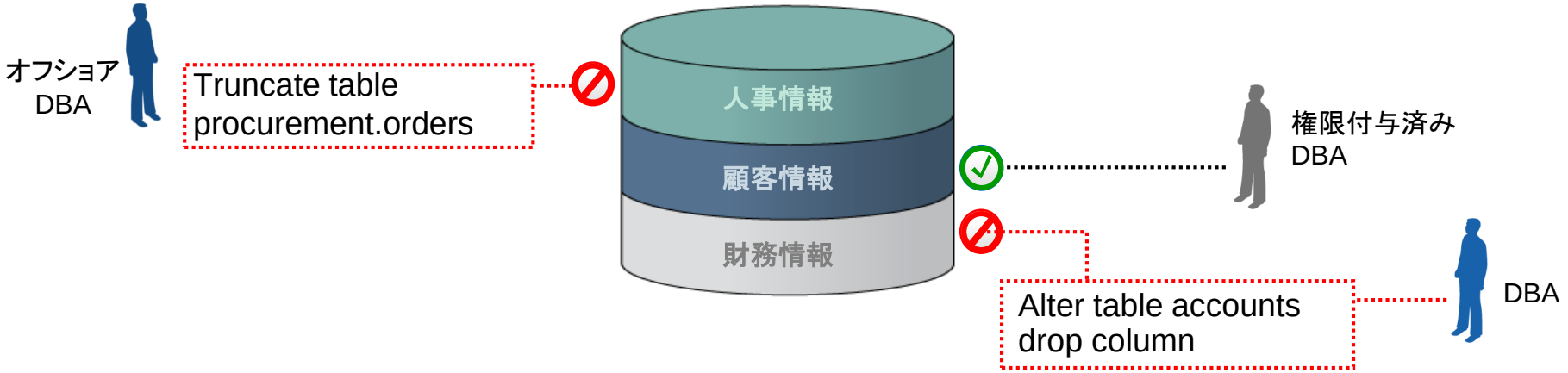
ルール1の条件式：

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

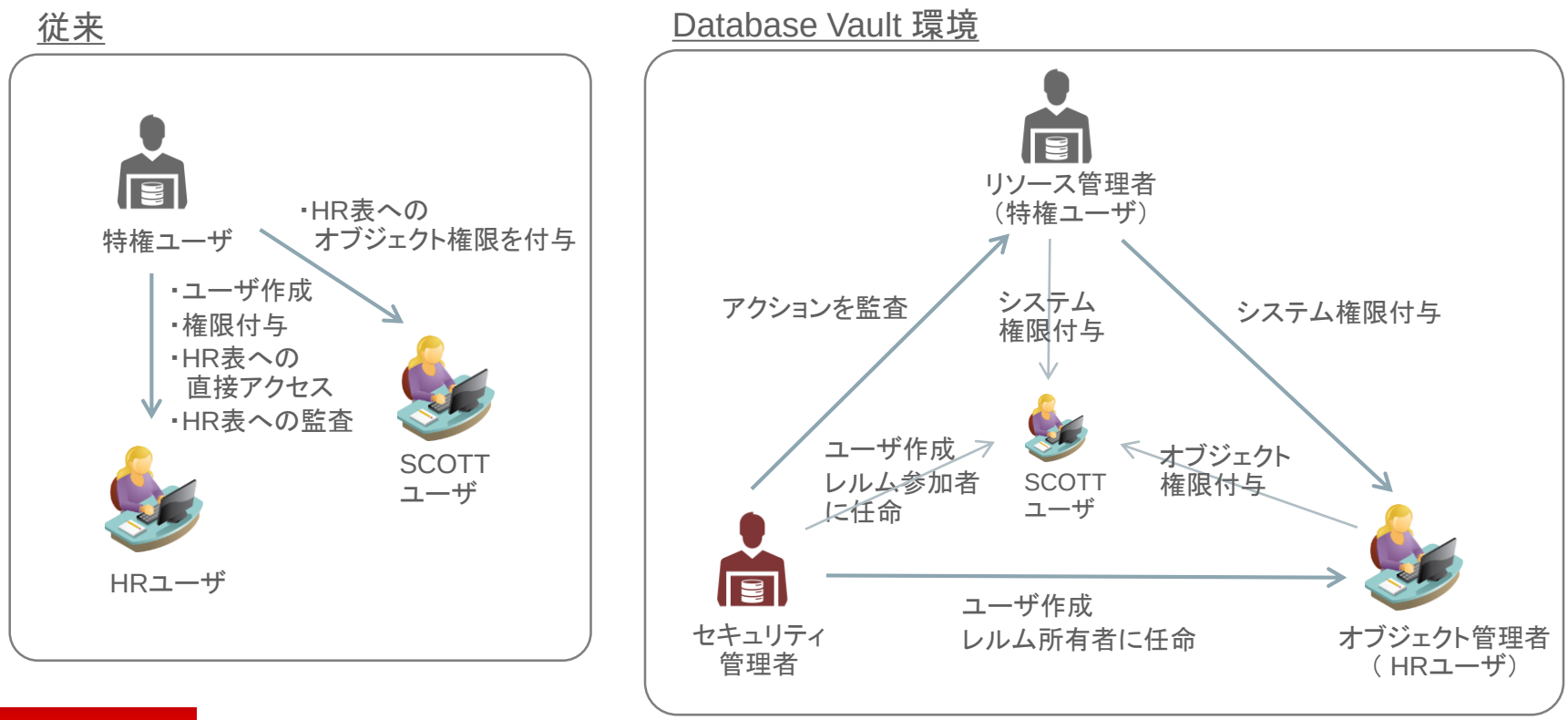
ALTER/CREATE/DROP USER	ALTER/CREATE/DROP FUNCTION	ALTER/CREATE/DROP PROCEDURE
ALTER/CREATE/DROP TABLE	ALTER/CREATE/DROP TABLESPACE	ALTER/CREATE/DROP VIEW
ALTER/CREATE/DROP ROLE	ALTER/CREATE/DROP INDEX	ALTER/CREATE/DROP PROFILE
CONNECT	AUDIT	NOAUDIT
CHANGE PASSWORD	GRANT	REVOKE
SELECT	DELETE	INSERT
UPDATE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

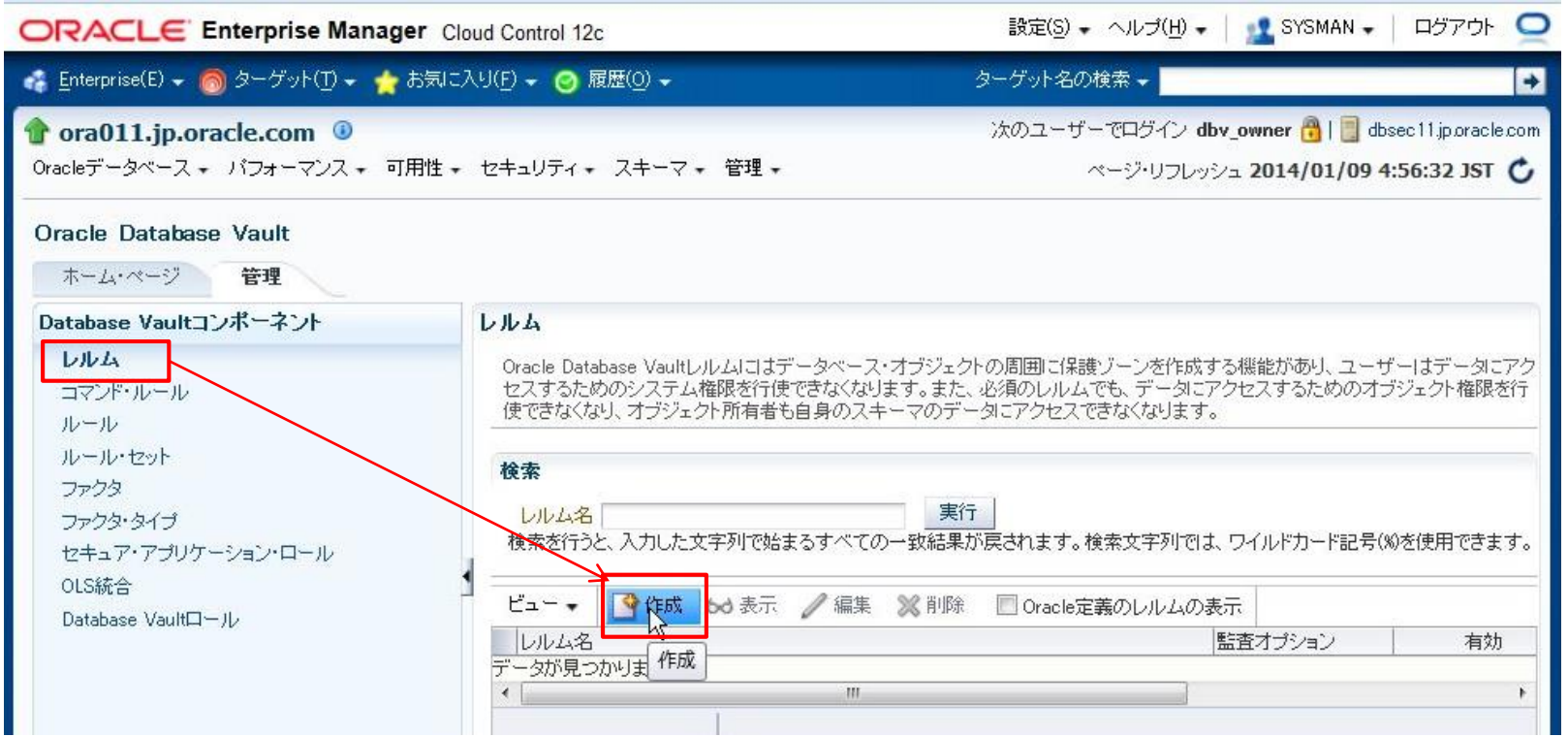
HRユーザがEmployee表をSQL*PLUSからSELECTすることを禁止

Database Vaultによる権限分掌と相互監視



DEMONSTRATION

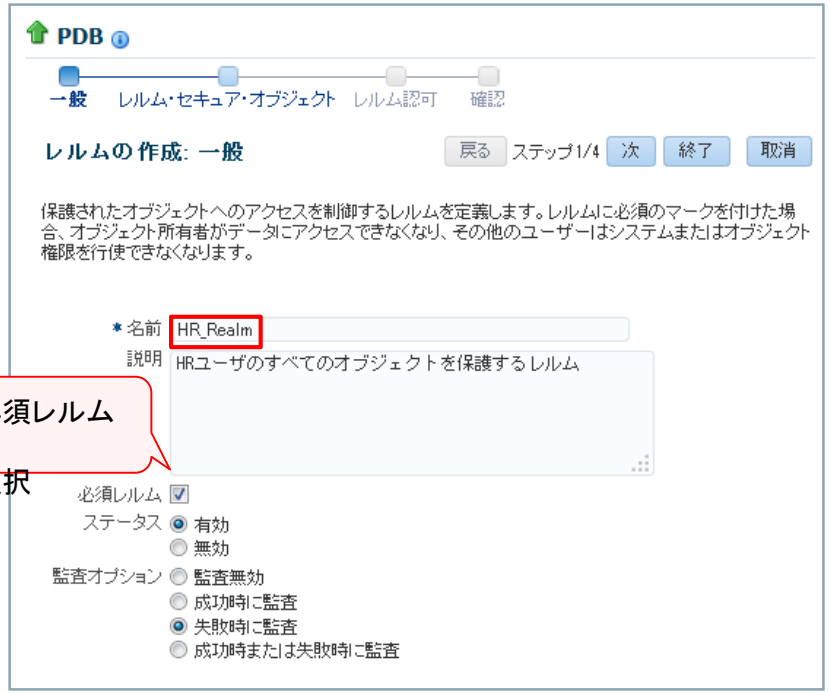
レルム作成の手順

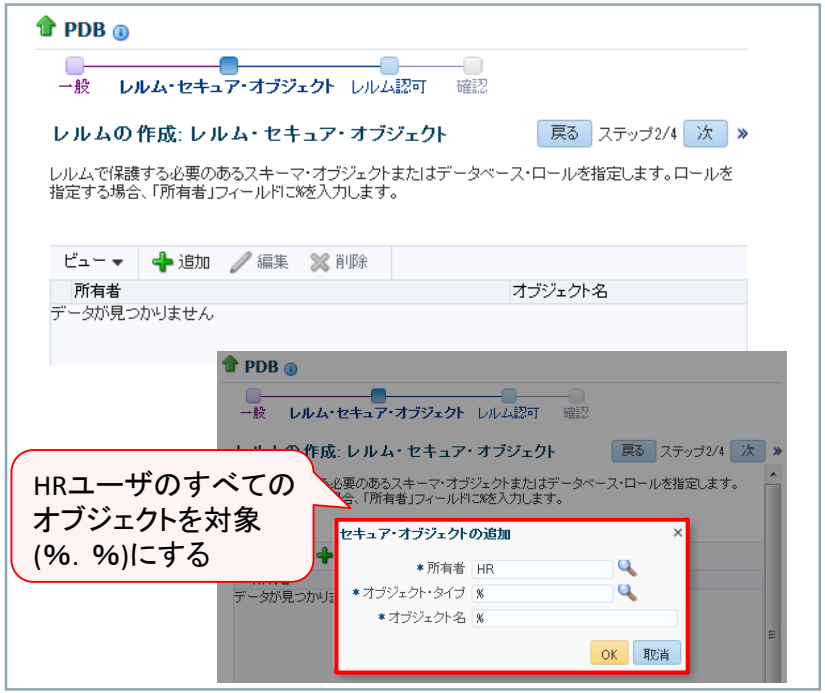


レルム作成の手順

1

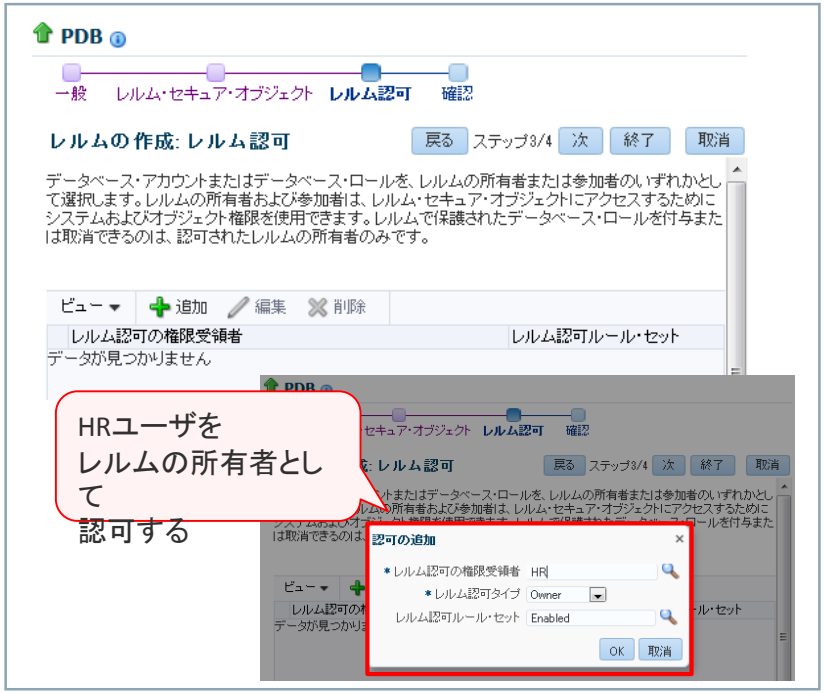
2





レルム作成の手順

3



4

HRレルムが動作しているかの確認

```
[oracle@dbsec11 ~]$ sqlplus sys/oracle12c as sysdba@dbsec11.jp.oracle.com:1521/p
db.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がレルム所有者

・SYSやSYSTEMユーザ、DBAロール、SELECT ANY TABLE等の権限を持っていたとしてもレル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ユーザがレルム所有者なので、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

・レル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レルムが動作しているかの確認

```
[oracle@dbsec11 ~]$ sqlplus sys/oracle12c as sysdba@dbsec11.jp.oracle.com:1521/p
db.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がレルム所有者

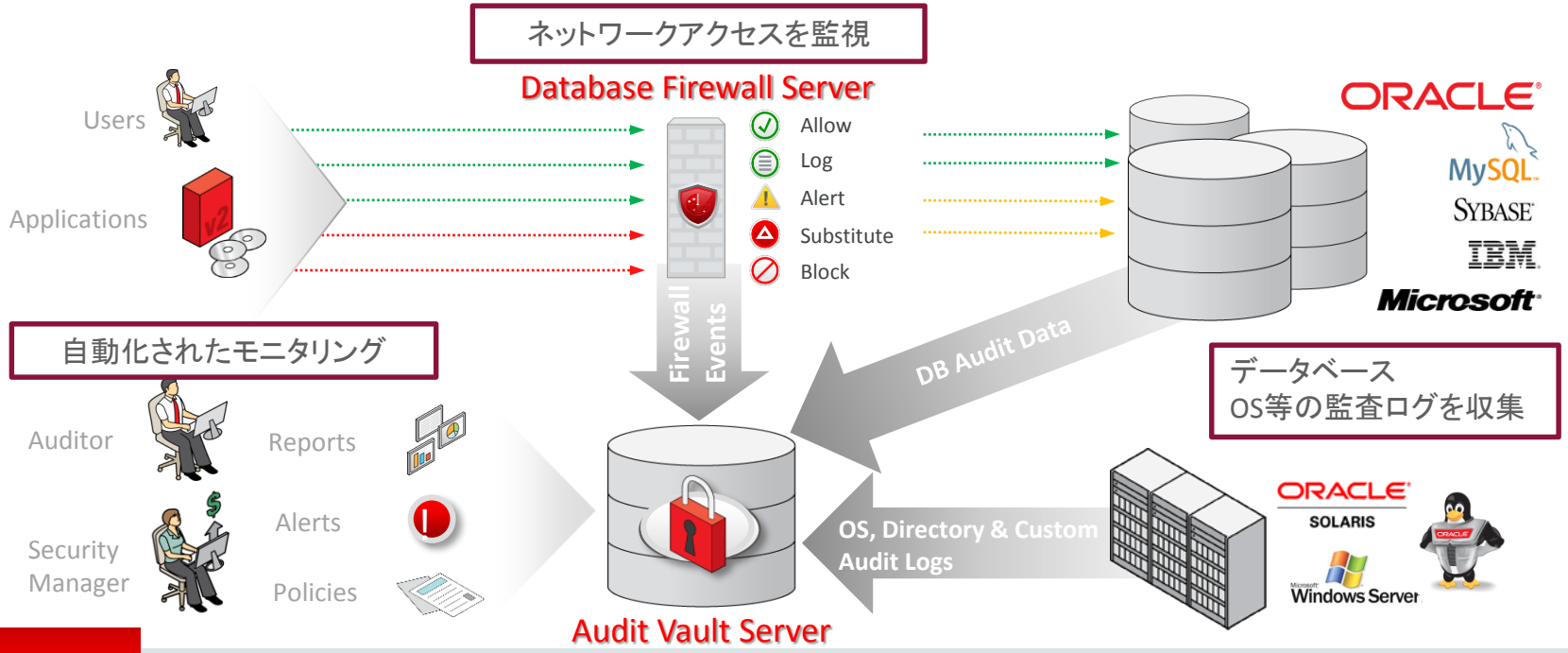
・SYSやSYSTEMユーザ、DBAロール、SELECT ANY TABLE等の権限を持っていたとしてもレルム認可されていなければ、左記のようにアクセスはできない

・HRユーザがレルム所有者なので、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

・レル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

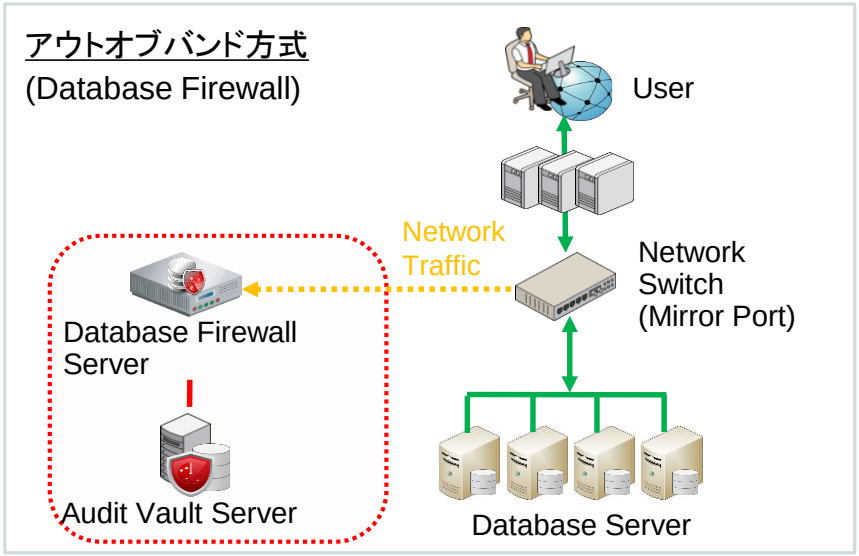
Oracle Audit Vault and Database Firewall

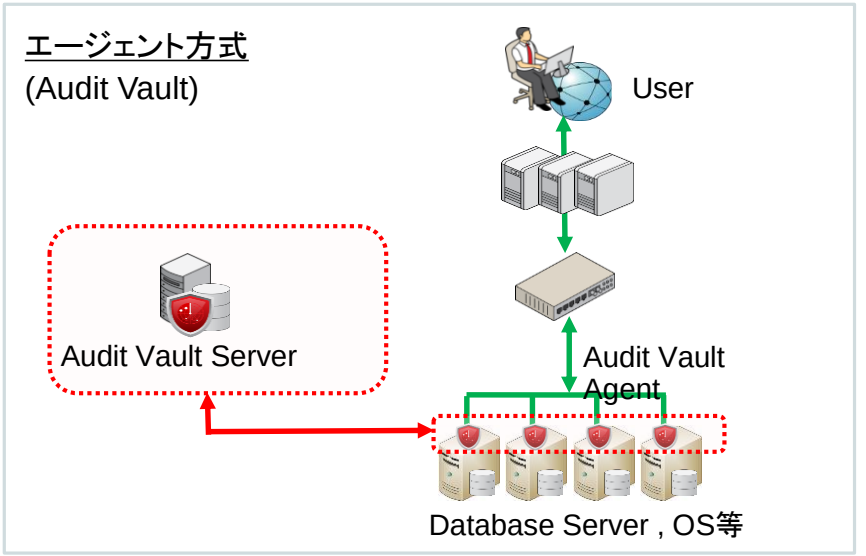
DatabaseやOSの監査ログを一括集約してモニタリング
迅速なセキュリティ対策を可能にするソフトウェア・アプライアンス



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

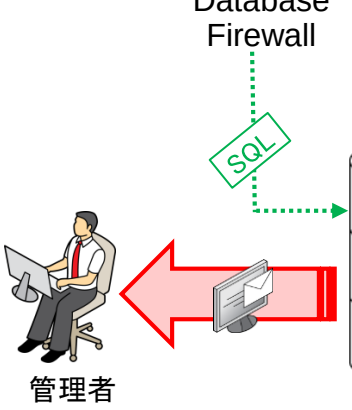


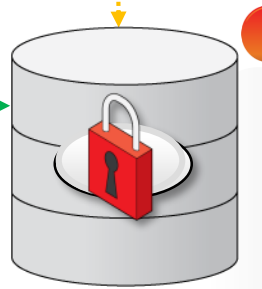


リアルタイムアラート

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





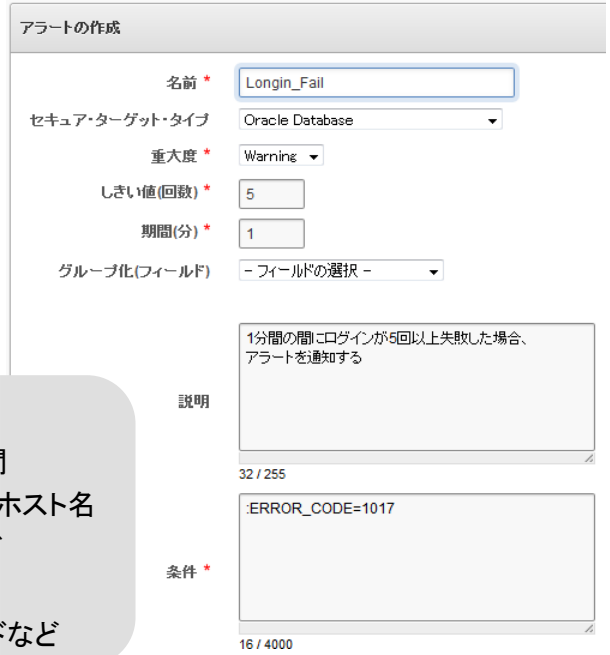
差出人 test <avserver@oracle.com>☆
件名 **Audit Vault Alert: sql_error, 6/18/2013 1:01:50 PM**
宛先 (自分) <test@secvm3.jp.oracle.com>☆

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

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



Oracle Database 12c おすすめ研修コース

ORACLE UNIVERSITY

Oracle Database 12*c*: 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。講義と演習と通じて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	■ Database Vaultの概要 ■ Database Vaultの構成 ■ 権限の分析 (12c 新機能) ■ レルムの構成 ■ ルール・セットの定義 ■ コマンド・ルールの構成 ■ ルール・セットの拡張 ■ セキュア・アプリケーション・ロールの構成 ■ Database Vaultレポートによる監査 ■ ベスト・プラクティスの実装
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 12*c*: 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ン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	■ セキュリティ要件について ■ セキュリティ・ソリューションの選択 ■ 基本的なデータベース・セキュリティ ■ ネットワーク・サービスの保護 ■ ユーザーのBasic認証と厳密認証の使用 ■ グローバル・ユーザー認証の使用 ■ プロキシ認証の使用 ■ 権限とロールの使用 ■ 権限分析の使用 (12c新機能) ■ アプリケーション・コンテキストの使用 ■ 仮想プライベート・データベースの実装 ■ Oracle Label Security の使用 ■ データ・リダクション (12c新機能) ■ データ・マスキングの使用 ■ 透過的機密データ保護の使用 (12c新機能) ■ 暗号化の概念とソリューション ■ DBMS_CRYPTO パッケージを使用した暗号化 ■ 透過的データ暗号化の使用 ■ データベース・ストーレジのセキュリティ ■ 統合監査の使用 (12c新機能) ■ ファイングレイン監査の使用
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。

ORACLE

Hardware and Software
Engineered to Work Together

VISION 2020

#1 CLOUD

ORACLE JAPAN


ORACLE®