Oracle Direct Seminar

ORACLE

今さら聞けない!?セキュリティ対策

日本オラクル株式会社
Oracle Direct

Oracle Direct Seminar

Agenda

- はじめに
- 基本機能で実現できるセキュリティ対策
  - Oracle Databaseインストール時の設定事項
  - 認証：ユーザの管理
  - 認証：パスワードポリシーの設定とOS認証
  - アクセス制御：オブジェクトレベル制御
  - 格納データの暗号化
  - 監査
  - まとめ
- Appendix
  - Enterprise Editionの機能

無償技術サービスOracle Direct Concierge

・SQL Serverからの移行アセスメント
・MySQLからの移行相談
・PostgreSQLからの移行相談
・Accessからの移行アセスメント
・Oracle Database バージョンアップ支援
・Oracle Developer/2000 Webアップグレード相談
・パフォーマンス・クリニック
・Oracle 構成相談
・Oracle Database 高可用性診断
・システム連携アセスメント
・システムセキュリティ診断
・簡易業務診断
・メインフレーム資産活用

http://www.oracle.com/lang/jp/direct/services.html

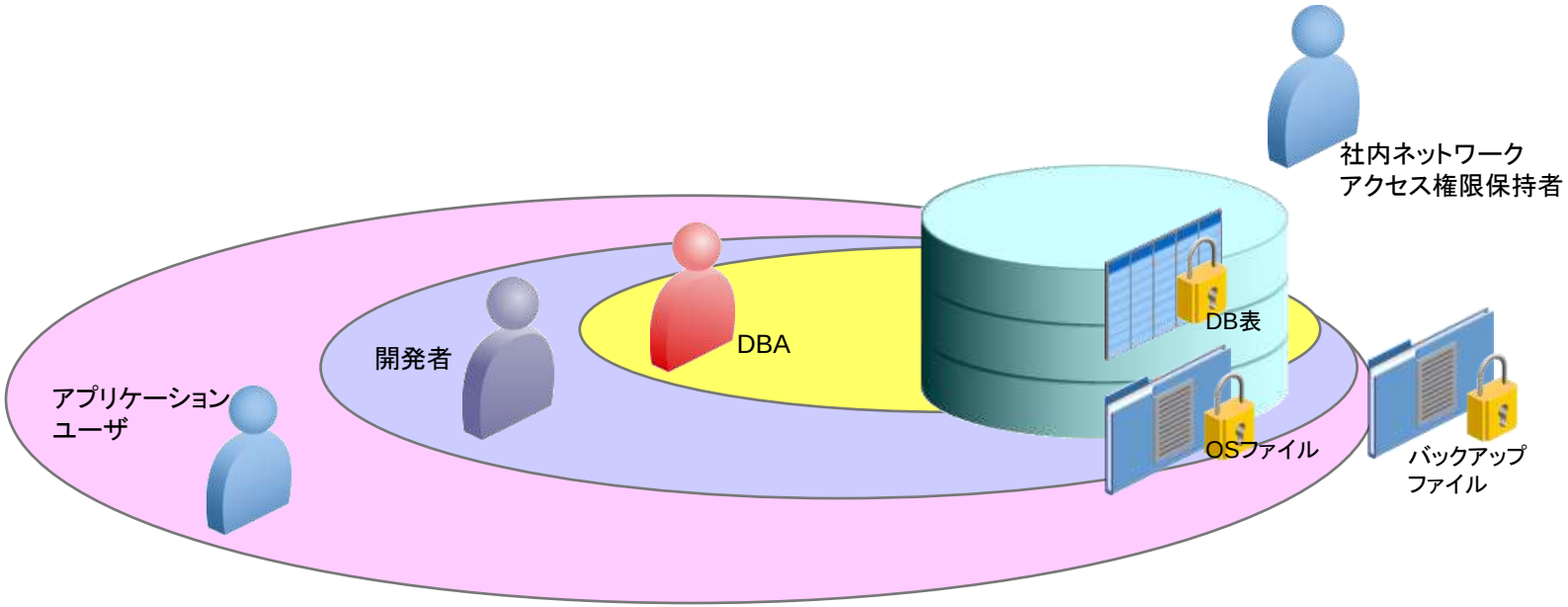
データベース環境において起こりうる脅威

アプリケーションユーザによる不正行為
- 不正な閲覧、データ改竄
- 不正なログイン

開発者による不正行為
- データの破壊行為
- 不正な権限付与
- 不正なユーザ作成などの構成変更

DBAによる不正行為
- データベースの破壊行為
- 監査証跡の改竄

社内アクセスによる不正行為
- サーバー内のOSファイルの取得
- バックアップファイル（ディスクやテープ）の取得



Oracleで実現するセキュアなデータベース環境

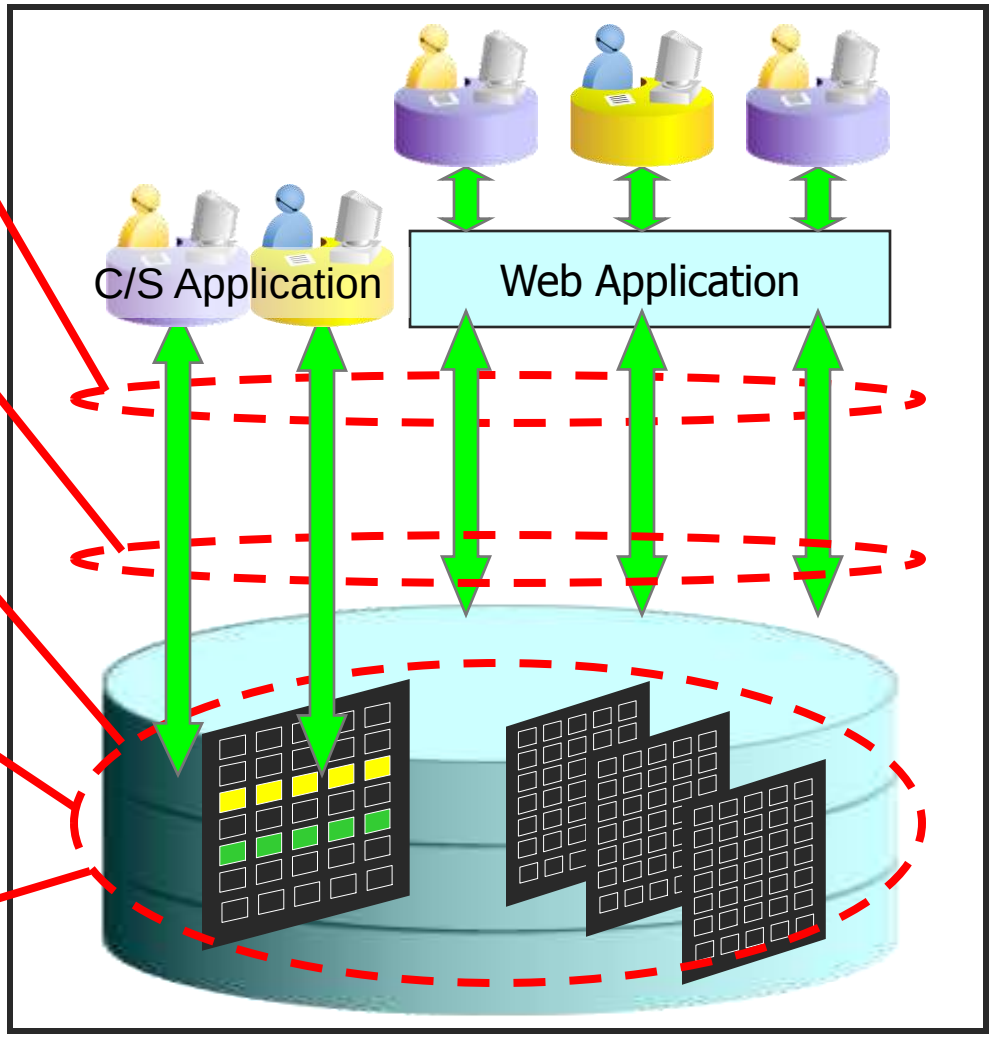
1.通信データの暗号化
- Oracle Net Serviceの暗号化、符号化

2. 認証の強化
- パスワード・ポリシー
- 他社製認証デバイスの利用(外部認証)
- PKIによる認証(グローバル認証)
- 3階層アプリの認証強化(プロキシ認証,EUS)

3.データへのアクセス制御
- オブジェクトレベル制御(View,Grant)
- 値レベル制御(VPD)
- デュアルロックによる制御強化

4.格納データの暗号化
- 透過的データ暗号化(TDE)
- バックアップデータの暗号化

5. 監査
- 必須監査
- 標準監査
- DBA監査
- 特定データアクセス監査



Agenda

- はじめに
- 基本機能で実現できるセキュリティ対策
  - Oracle Databaseインストール時の設定事項
  - 認証：ユーザの管理
  - 認証：パスワードポリシーの設定とOS認証
  - アクセス制御：オブジェクトレベル制御
  - 格納データの暗号化
  - 監査
  - まとめ
- Appendix
  - Enterprise Editionの機能

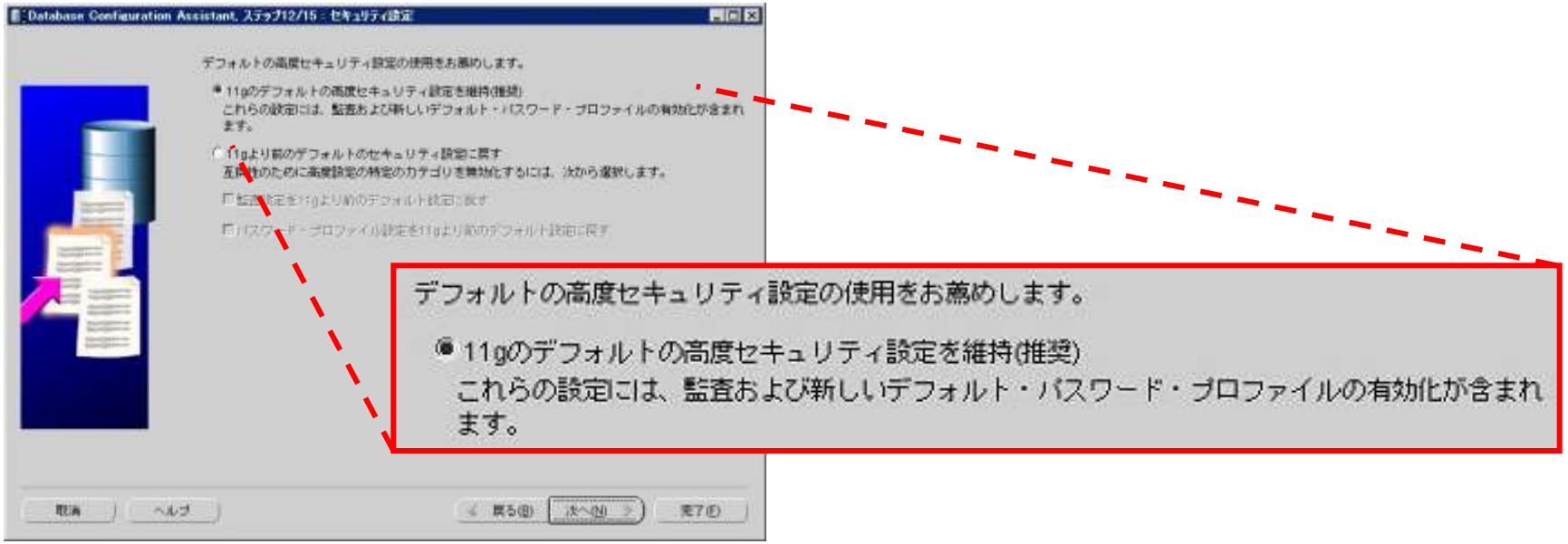
無償技術サービスOracle Direct Concierge

・SQL Serverからの移行アセスメント
・MySQLからの移行相談
・PostgreSQLからの移行相談
・Accessからの移行アセスメント
・Oracle Database バージョンアップ支援
・Oracle Developer/2000 Webアップグレード相談
・パフォーマンス・クリニック
・Oracle 構成相談
・Oracle Database 高可用性診断
・システム連携アセスメント
・システムセキュリティ診断
・簡易業務診断
・メインフレーム資産活用

http://www.oracle.com/lang/jp/direct/services.html

初期状態からセキュアなデータベース

- Database Configuration Assistant(DBCA)にて
  データベースの構成を行う際のセキュリティ設定画面



具体的に初期設定される内容

- 標準監査の有効化
- デフォルト・プロファイルのパスワード制限の強化
- PUBLICロールからのCREATE EXTERNAL JOB権限の削除

※Oracle Database 11gR2よりデフォルトで高度なセキュリティ設定が有効化されているため、
DBCAではセキュリティ設定画面が廃止されています

インストールおよび構成のチェックリスト

初期状態からセキュアなデータベース

認証の管理

外部からのアクセス

権限の管理

その他のセキュリティトピックス

- マニュアル 『Oracle Database 2日でセキュリティ・ガイド』
  http://download.oracle.com/docs/cd/E16338_01/server.112/b56296/toc.htm
- ホワイト・ペーパー 『Oracle Databaseのセキュリティ・チェックリスト』
  http://www.oracle.com/technology/global/jp/products/security/db_security/doc/twp_security_checklist_database.pdf
- Oracle Direct Seminar 『意外と簡単!? Oracle Database 11g – セキュリティ編 – 』
  http://otndnld.oracle.co.jp/easy/oracle11gr1/windows/3rd/index.html#b01

Agenda

- はじめに
- 基本機能で実現できるセキュリティ対策
  - Oracle Databaseインストール時の設定事項
  - 認証：ユーザの管理
  - 認証：パスワードポリシーの設定とOS認証
  - アクセス制御：オブジェクトレベル制御
  - 格納データの暗号化
  - 監査
  - まとめ
- Appendix
  - Enterprise Editionの機能

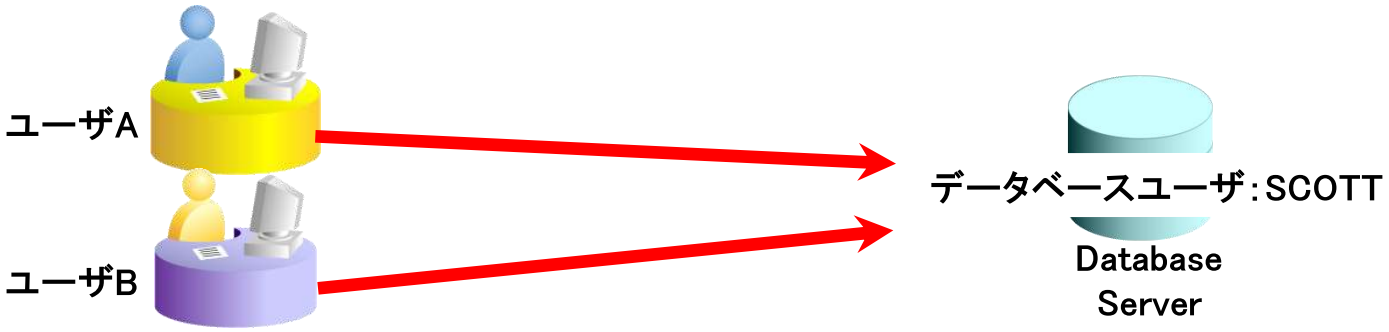
無償技術サービスOracle Direct Concierge

・SQL Serverからの移行アセスメント
・MySQLからの移行相談
・PostgreSQLからの移行相談
・Accessからの移行アセスメント
・Oracle Database バージョンアップ支援
・Oracle Developer/2000 Webアップグレード相談
・パフォーマンス・クリニック
・Oracle 構成相談
・Oracle Database 高可用性診断
・システム連携アセスメント
・システムセキュリティ診断
・簡易業務診断
・メインフレーム資産活用

http://www.oracle.com/lang/jp/direct/services.html

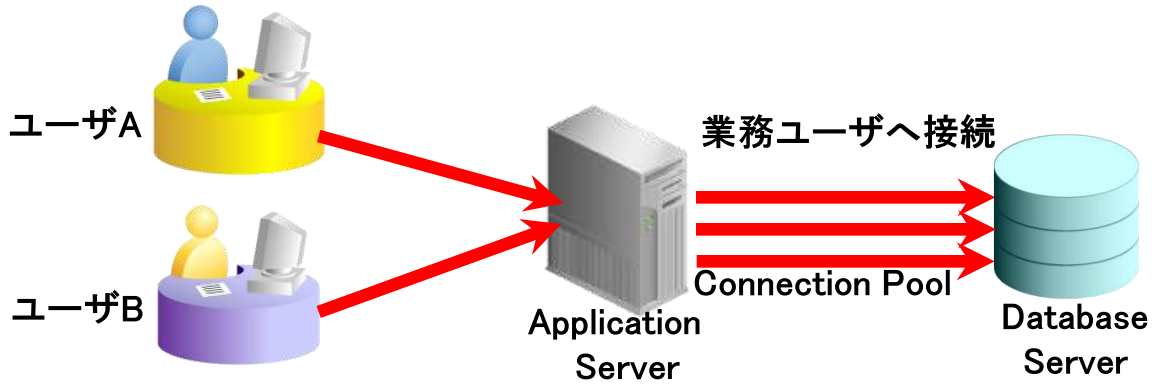
データベース・セキュリティの前提として・・・

- Oracleデータベースにアクセスするユーザを個別に作成していないと？

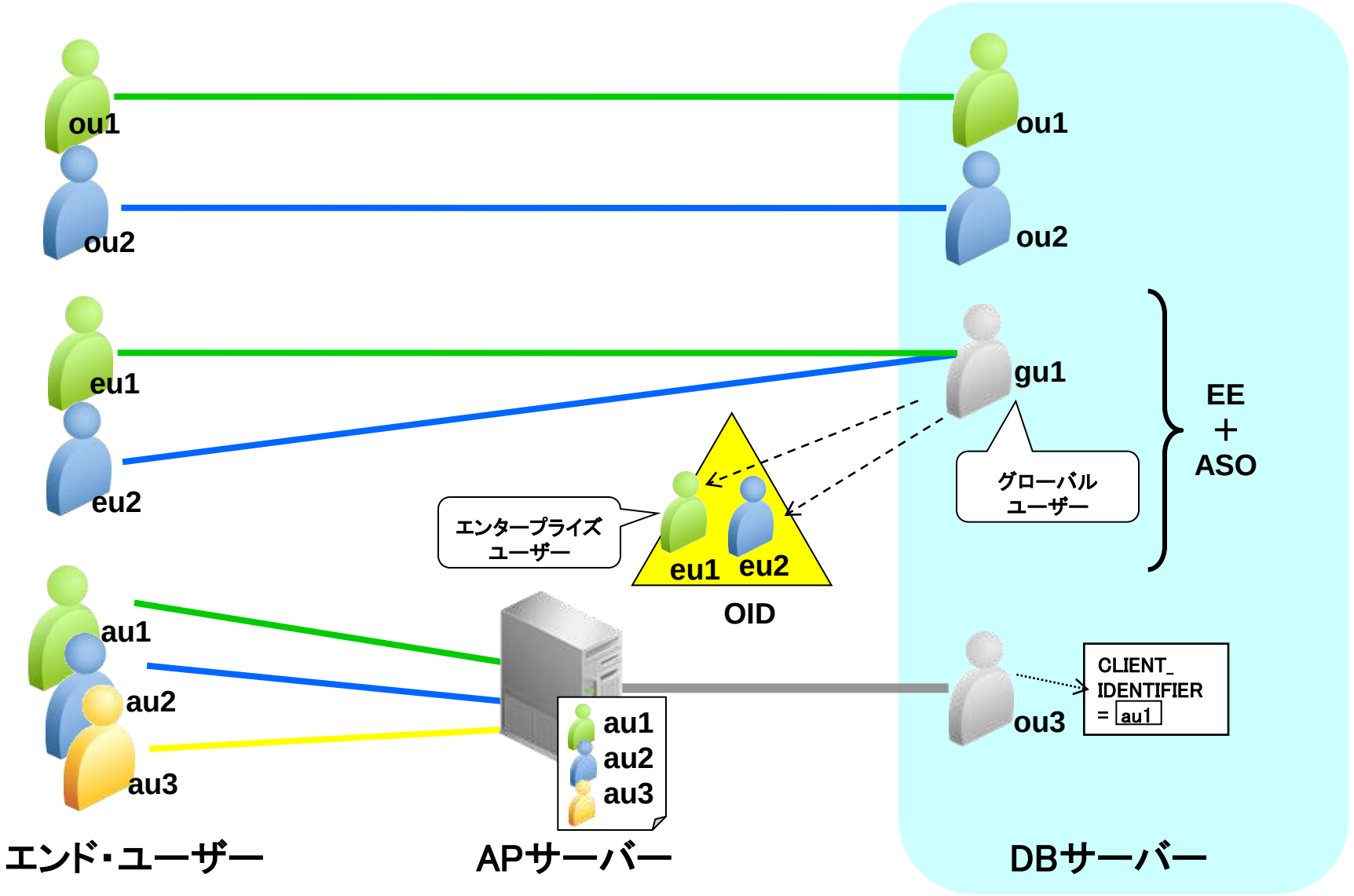


業務データにアクセスしたのは誰？全員同じ権限でよい？

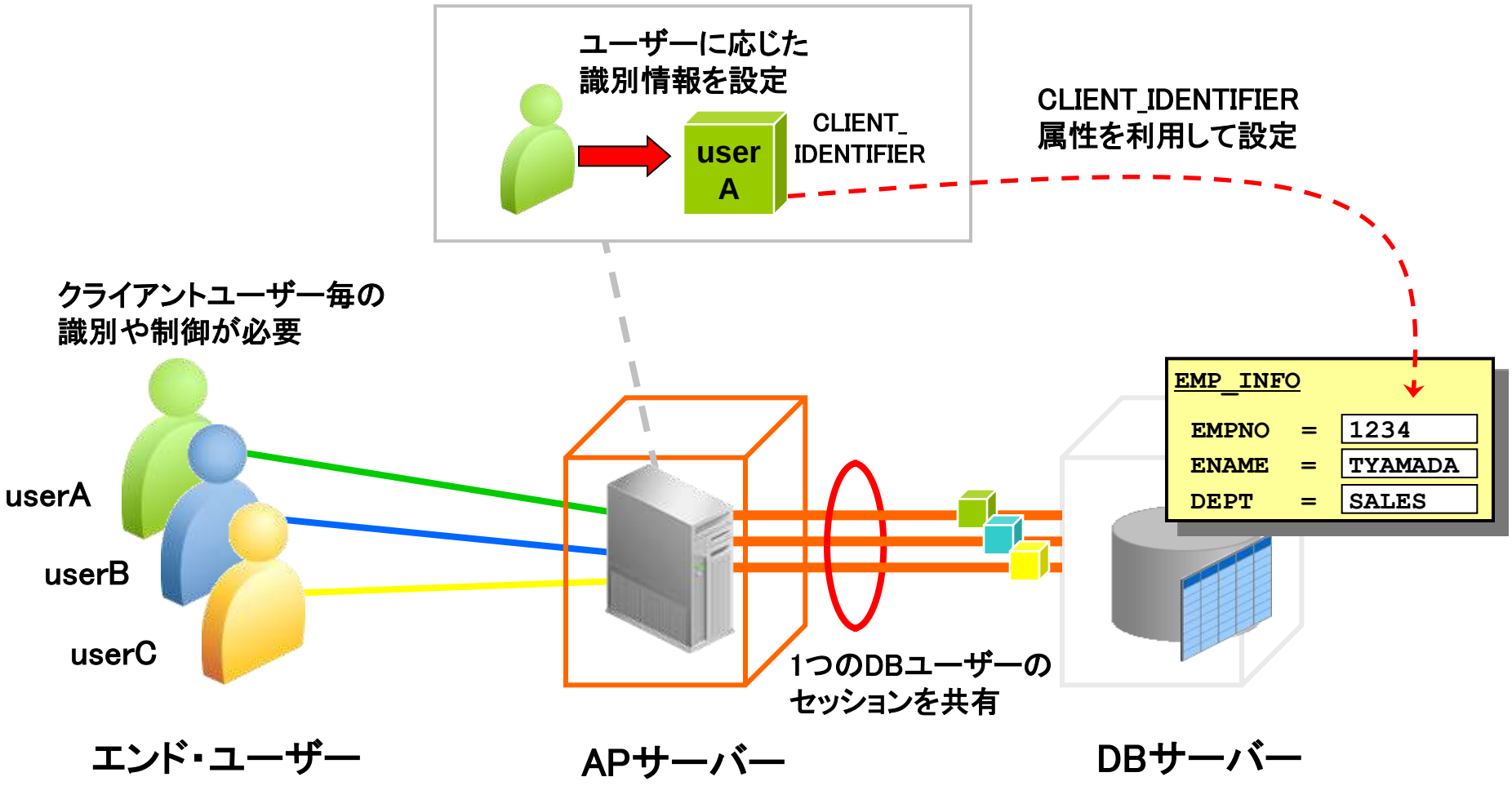
- N階層構造のアプリケーションで、監査およびアクセス制御には別の仕組みが必要



アプリケーション・ユーザーとDBユーザー



クライアント・ユーザーの識別（APユーザー）



OCI／Java（JDBC）／.NET(ODP.NET)を使うアプリケーションで可能

クライアント識別子

- エンドユーザがアプリ経由でデータをアクセスする際に、接続しているエンドユーザを特定する仕組み
  - (アプリケーションで利用するユーザ情報 != Oracleユーザ)

アプリケーション処理内でDBセッションを利用する毎にクライアント識別子としてユーザ情報を設定すると、後続の処理でユーザ情報を認識できる。

- 設定方法(PL/SQL)

※ PL/SQLの他、OCIとJDBCより利用可能

```
EXECUTE DBMS_SESSION.SET_IDENTIFIER('USER01');
```

- クライアント識別子の取得例:

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

クライアント識別子を設定することでできること

- V$SESSIONのclient_identifier列に値が設定
  - Oracle Databaseにアクセスしているアプリケーションユーザを識別可能
- DBA_AUDIT_TRAILの client_idに値が設定される
  - 監査ログにアプリケーションユーザが記録される。
- アプリケーションユーザ単位で、業務データを絞り込むことができる。
  - アプリケーションユーザの所属する部課でデータを絞り込んだ例

```
SELECT ....
  FROM B
 WHERE (B.部CD, B.課CD) in (
          SELECT 部CD, 課CD
            FROM 部課_ユーザT
           WHERE ユーザID = SYS_CONTEXT('USERENV','CLIENT_IDENTIFIER')
   );
```

Agenda

- はじめに
- 基本機能で実現できるセキュリティ対策
  - Oracle Databaseインストール時の設定事項
  - 認証：ユーザの管理
  - 認証：パスワードポリシーの設定とOS認証
  - アクセス制御：オブジェクトレベル制御
  - 格納データの暗号化
  - 監査
  - まとめ
- Appendix
  - Enterprise Editionの機能

パスワード・ポリシーの強化

- プロファイル（データベース・リソースの制限）を作成し、USERに割り当てる。
  - CREATE USER時にPROFILE指定を省略すると「DEFAULT」プロファイルが割り当てられる

- パスワード・ポリシー関連の制限（抜粋）

制限名	内容
FAILED_LOGIN_ATTEMPTS	ログイン試行回数の制限
PASSWORD_LIFE_TIME	パスワード有効期間
PASSWORD_REUSE_TIME	パスワードが再利用できるようにまでの期間
PASSWORD_REUSE_MAX	現行のパスワードを再利用する前に必要なパスワードの変更回数
PASSWORD_LOCK_TIME	ログインが指定された回数連続して失敗した場合、アカウントがロックされる日数
PASSWORD_GRACE_TIME	ログインが許可される猶予期間の日数
PASSWORD_VERIFY_FUNCTION	パスワード検証用のファンクションを指定（＊1）

（＊1）ファンクションのサンプル：$ORACLE_HOME/rdbms/admin/utlpwdmg.sql

パスワード・ポリシー設定例

- Oracle上のユーザ tanaka にプロファイル prof を設定した例：

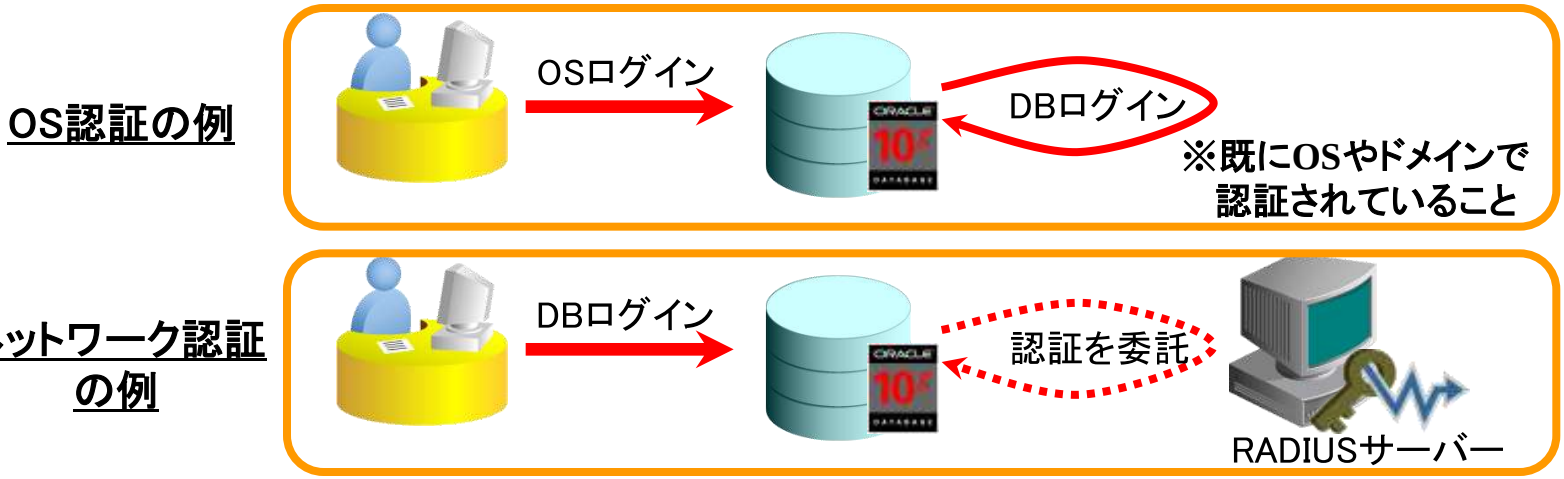
```
SQL> CREATE PROFILE prof LIMIT
SQL>   FAILED_LOGIN_ATTEMPTS 4
SQL>   PASSWORD_LOCK_TIME   30
SQL>   PASSWORD_LIFE_TIME   90
SQL>   PASSWORD_GRACE_TIME   3;

SQL> ALTER USER tanaka PROFILE prof;
```

- サンプル、$ORACLE_HOME/rdbms/admin/utlpwdmg.sql の内容
  - ユーザー名と同じかどうかのチェック
  - パスワード長のチェック
  - 簡単な用語でないかのチェック
  - 英文字、数字、記号が入っているかのチェック
  - 過去に使ったパスワードかどうかのチェック

外部認証（OS認証）

- 外部認証
  - Oracle上のユーザのパスワード管理とユーザ認証を外部サービスにて実施する認証形態

- 外部サービス
  - オペレーティング・システム … Standard Editionでも利用可能
  - ネットワーク・サービス … Enterprise Edition ＋ Advanced Security
    - RADIUS認証、Kerberos認証など



外部認証（OS認証）- 設定

- 初期化パラメータ
  - OS_AUTHENT_PREFIX　OS認証ユーザの接頭辞（デフォルト：OPS$）
- SQLNET.ora（Windowsのみ）
  - sqlnet.authentication_services =(NTS)
- ユーザ作成
  - UNIX

```
SQL> CREATE USER OPS$SCOTT IDENTIFIED EXTERNALLY;
```

  - Windows（以下のいずれか）

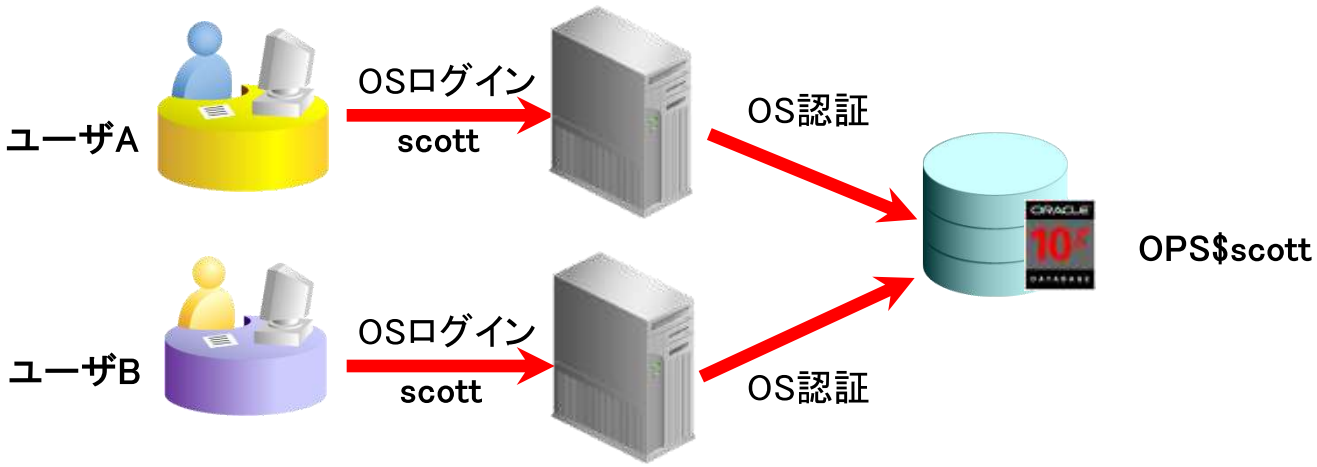
```
SQL> CREATE USER "OPS$ホスト名¥SCOTT"  IDENTIFIED EXTERNALLY;
SQL> CREATE USER "OPS$ドメイン名¥SCOTT" IDENTIFIED EXTERNALLY;
```

外部認証（OS認証） - 接続

1. OSもしくはドメインにて認証（ログイン）する
2. 認証済みのOS上より、Oracleのユーザ ID、パスワードを省略して接続

```
$ whoami
scott
$ sqlplus /@接続先
```

UNIX系OSの例



Agenda

- はじめに
- 基本機能で実現できるセキュリティ対策
  - Oracle Databaseインストール時の設定事項
  - 認証：ユーザの管理
  - 認証：パスワードポリシーの設定とOS認証
  - アクセス制御：オブジェクトレベル制御
  - 格納データの暗号化
  - 監査
  - まとめ
- Appendix
  - Enterprise Editionの機能

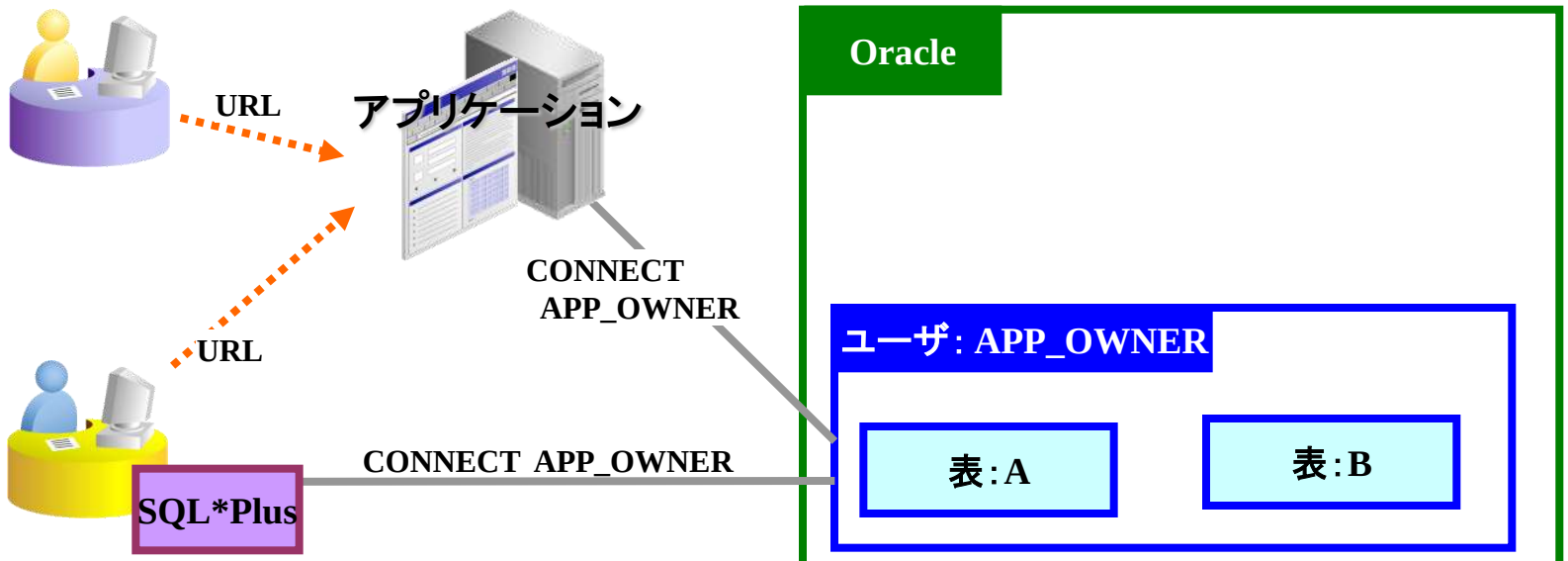
無償技術サービスOracle Direct Concierge

・SQL Serverからの移行アセスメント
・MySQLからの移行相談
・PostgreSQLからの移行相談
・Accessからの移行アセスメント
・Oracle Database バージョンアップ支援
・Oracle Developer/2000 Webアップグレード相談
・パフォーマンス・クリニック
・Oracle 構成相談
・Oracle Database 高可用性診断
・システム連携アセスメント
・システムセキュリティ診断
・簡易業務診断
・メインフレーム資産活用

http://www.oracle.com/lang/jp/direct/services.html

いろんな人が本番データに直接アクセスしていませんか？

- 検索ツール（MS-Access）やSQL*Plusでエンドユーザがアクセスできると。。

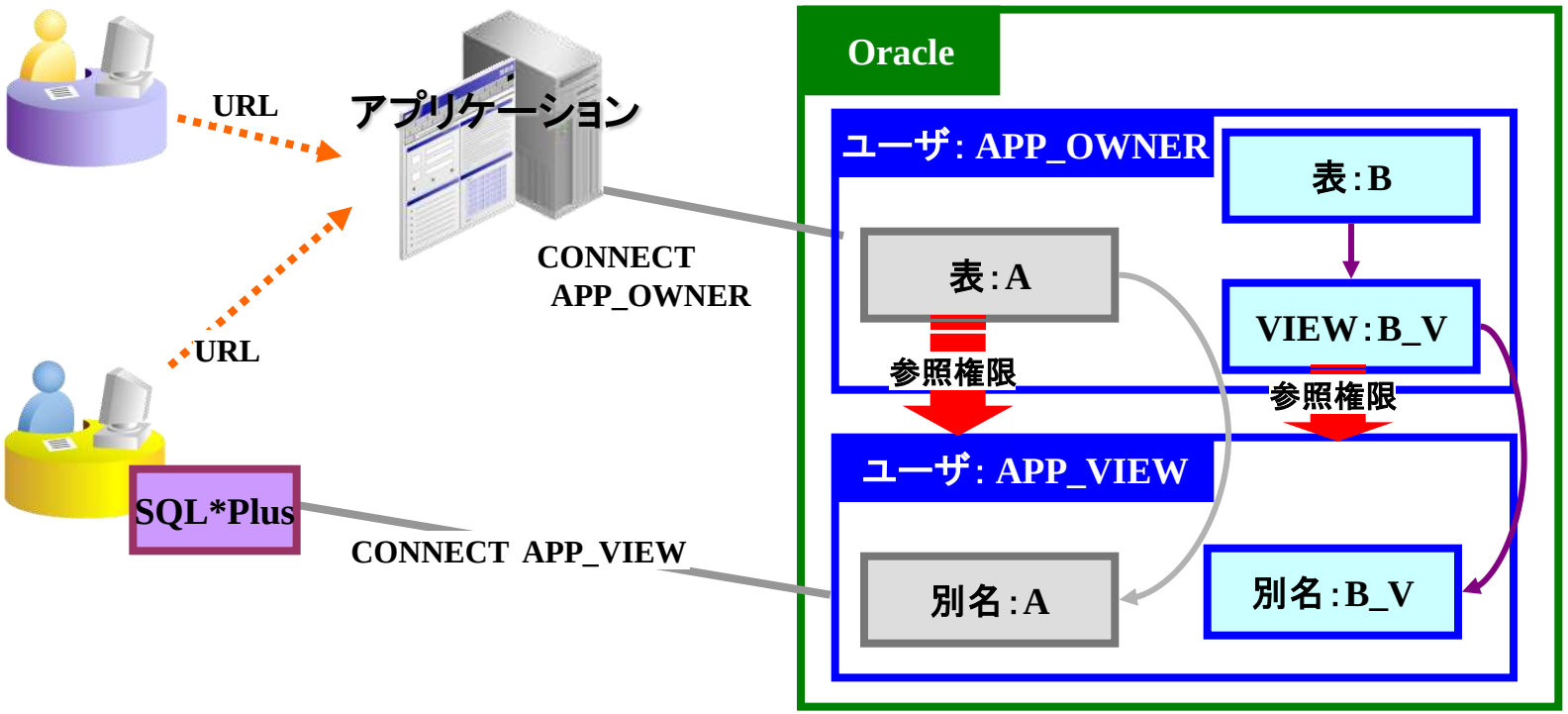


課題1）みえてはいけないデータが見えてしまう

課題2）誤ってデータを更新・削除をしてしまう可能性がある

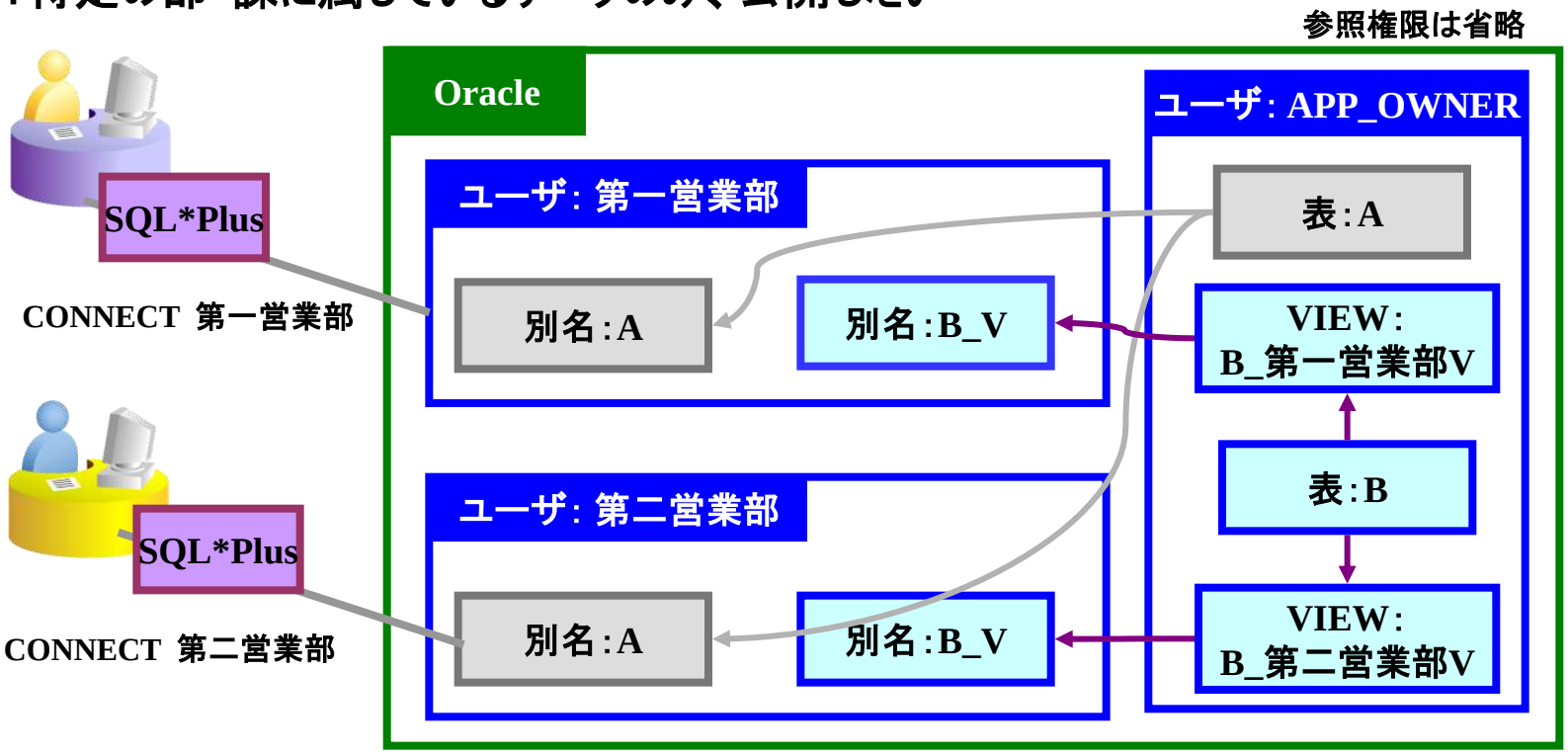
VIEWとオブジェクト権限によるアクセス制限

- VIEWでみせてはいけない列を見せないようにする
- 参照用のOracleユーザを作成し、オブジェクトの別名（SYNONYM）を作成
- 参照用Oracleユーザへの、本番データのオブジェクト権限は参照のみとし、不用意な更新をさせない



ユーザ毎に見てよいデータ(行)を変えたい

- VIEWでは見せてはいけない列のみでなく、ユーザ毎に行も絞り込みたい
  例:特定の部・課に属しているデータのみ、公開したい



課題1) 似たようなVIEWをユーザ毎に作成すると管理が大変

課題2) ユーザ毎に別名(SYNONYM)を作成するのも大変

応用例）ユーザ毎に見てよいデータ（行）を変えたい

課題1）似たようなVIEWをユーザ毎に作成すると管理が大変

「Oracleユーザが参照してもよい部・課」テーブルがあるならば、
USER関数を利用したVIEWを作成可能

```
CREATE OR REPLACE VIEW B_V AS
   SELECT ....
     FROM B
    WHERE (B.部CD, B.課CD) in (
     SELECT 部CD, 課CD FROM 部課_ユーザT WHERE ユーザID = USER
    );
```

課題2）ユーザ毎に別名（SYNONYM）を作成するのも大変

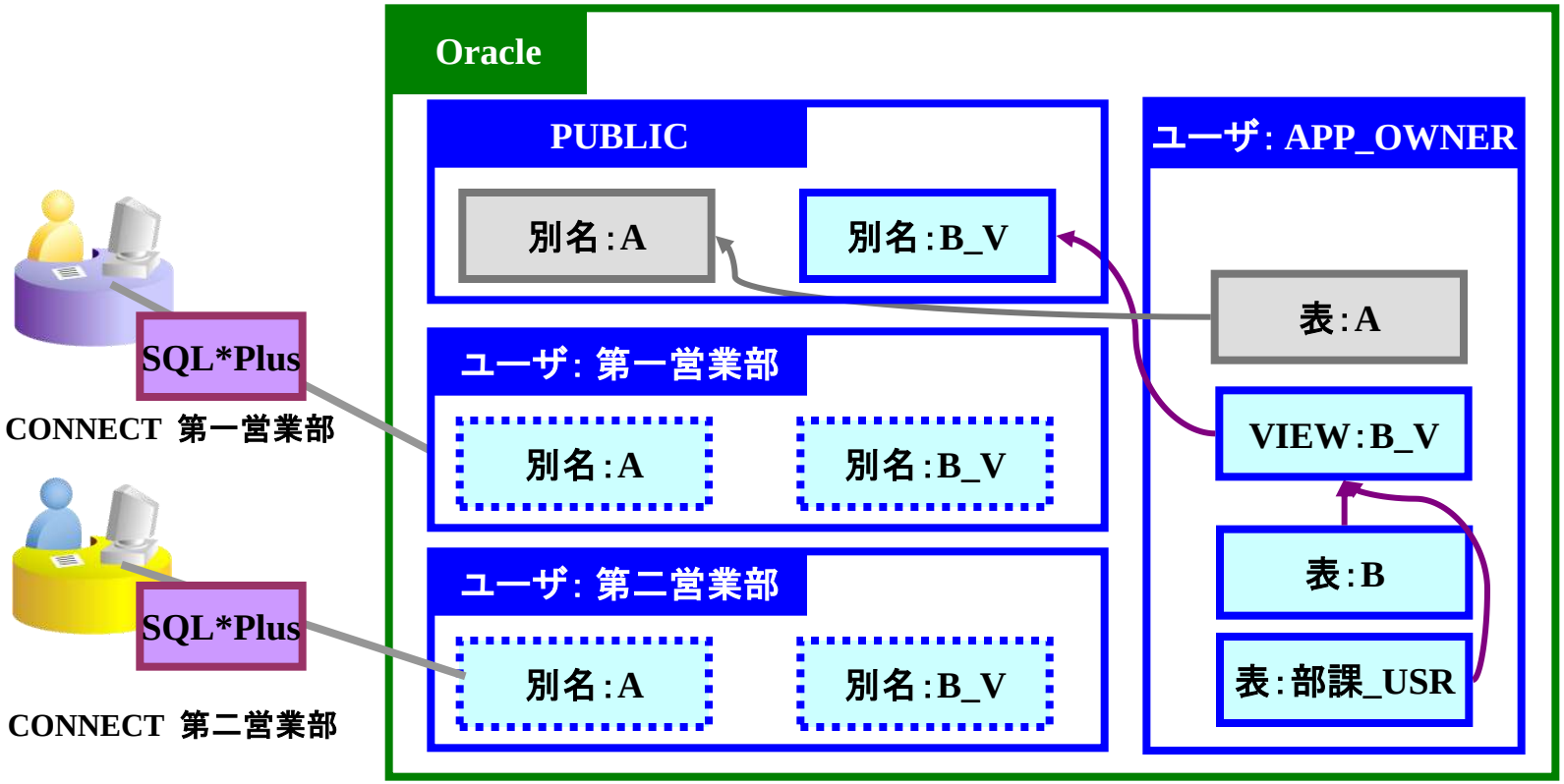
PUBLIC SYNONYM を作成し、PUBLICに参照権限を付与することで対応

```
CREATE PUBLIC SYNONYM B_V FOR B_V;
GRANT SELECT ON B_V TO PUBLIC;
```

応用例）ユーザ毎に見てよいデータ（行）を変えたい

- USER関数を用いたVIEW、PUBLIC SYNONYMとの組み合わせ

参照権限は省略



ユーザーの異動などがあっても表：部課_USR のメンテナンスで対応できる

Agenda

暗号化についての詳細は8/24実施の
実践!!セキュリティ
～OracleDatabaseの暗号化～
セミナーにご参加ください

- はじめに
- 基本機能で実現できるセキュリティ対策
  - Oracle Databaseインストール時の設定事項
  - 認証:ユーザの管理
  - 認証:パスワードポリシーの設定とOS認証
  - アクセス制御:オブジェクトレベル制御
  - 格納データの暗号化
  - 監査
  - まとめ
- Appendix
  - Enterprise Editionの機能

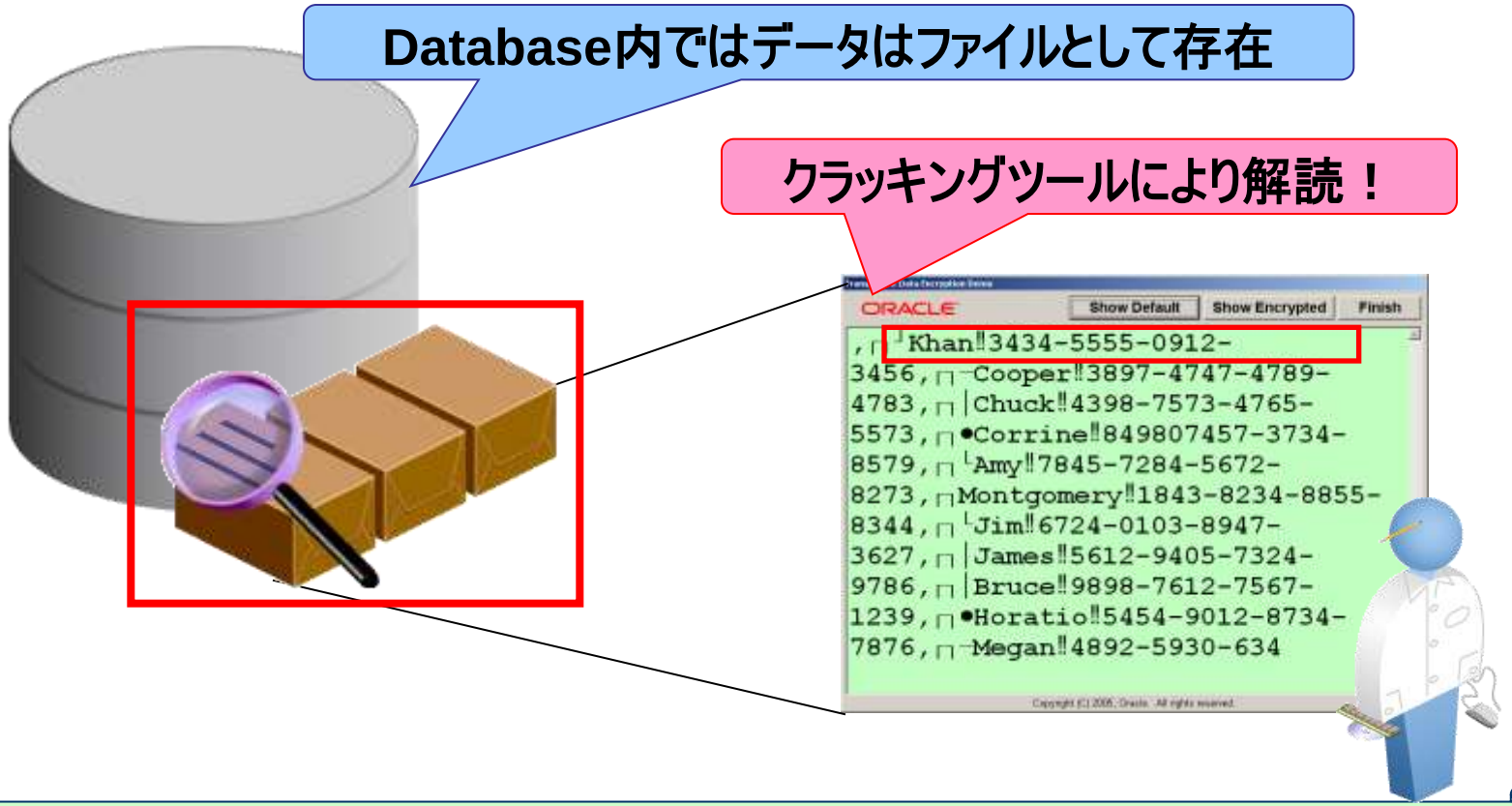
無償技術サービスOracle Direct Concierge

・SQL Serverからの移行アセスメント
・MySQLからの移行相談
・PostgreSQLからの移行相談
・Accessからの移行アセスメント
・Oracle Database バージョンアップ支援
・Oracle Developer/2000 Webアップグレード相談
・パフォーマンス・クリニック
・Oracle 構成相談
・Oracle Database 高可用性診断
・システム連携アセスメント
・システムセキュリティ診断
・簡易業務診断
・メインフレーム資産活用

http://www.oracle.com/lang/jp/direct/services.html

データの暗号化 – データファイルの暗号化

- データファイルの盗難の危険性の認識



悪意を持つユーザからは格好の対象となる

標準のPL/SQLパッケージの使用

予め、各パッケージのプロシージャを使用して、暗号化用/復号化用のファンクションを作成しておきます。

暗号化してデータを挿入
SQL> INSERT INTO customers(cust_id)
VALUES (encrypt_function('xxxxxx'));

復号してデータを取得
SQL> SELECT decrypt_function(cust_id)
FROM customers;

USER_ID	NAME	ADDRESS	CARD_ID
001	KING	TOKYO	3351-xxxx-xx
002	SCOTT	FUKUOKA	3352-xxxx-xx
003	CLARK	SAPPORO	3353-xxxx-xx

復号されたデータ

USER_ID	NAME	ADDRESS	CARD_ID
001	KING	TOKYO	mCJs8Aakm
002	SCOTT	FUKUOKA	p$hv/WiMnhf
003	CLARK	SAPPORO	V%Jsa6aUm

暗号化されて格納

パッケージによる暗号化・復号化の問題点

従来の暗号化方法

パッケージによる暗号化・複合化

- DBMS_OBFUSCATION_TOOLKIT(R8.1～)
- DBMS_CRYPTO(R10.1～)

– 暗号化/復号化 のたびにパッケージを呼び出してデータを処理
→ TDEに比べ追加のコストがかかる

■ パッケージを使用した場合

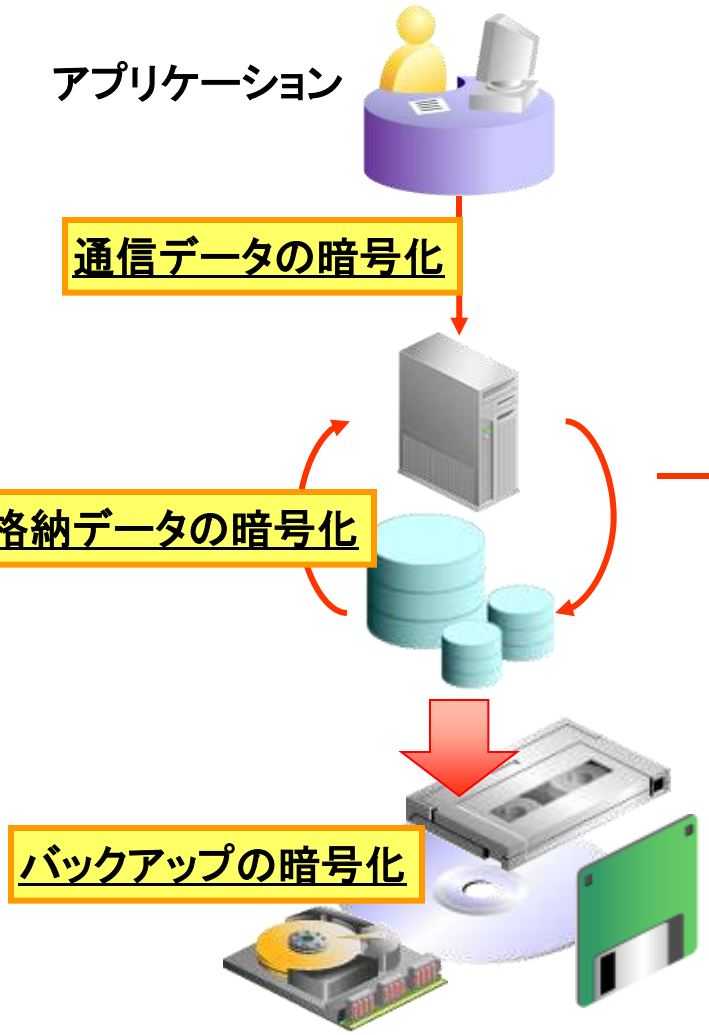
事前のパッケージ呼び出しによる暗号化オーバヘッドがかかりパフォーマンス面で不利

SQL文中に挿入するため、状況により改変も必要

暗号化してデータを挿入
SQL> INSERT INTO customers(cust_id)
VALUES (encrypt_function('xxxxxx'));

復号化してデータを取得
SQL> SELECT decrypt_function(cust_id)
FROM customers;

EE + Advanced Security Optionで可能となる暗号化



- 透過的なデータ暗号化
  （TDE: Transparent Data Encryption）
  - アプリケーションの修正が不要
  - 暗号化キーの管理を自動化
  - 索引が使用可能
  - 従来の方式と比較して高速に
  - ディスクやメディアを問わない暗号化の実現

- RMAN バックアップの暗号化
  - RMANで取得したバックアップセットの暗号化

暗号化処理に伴うオーバーヘッド

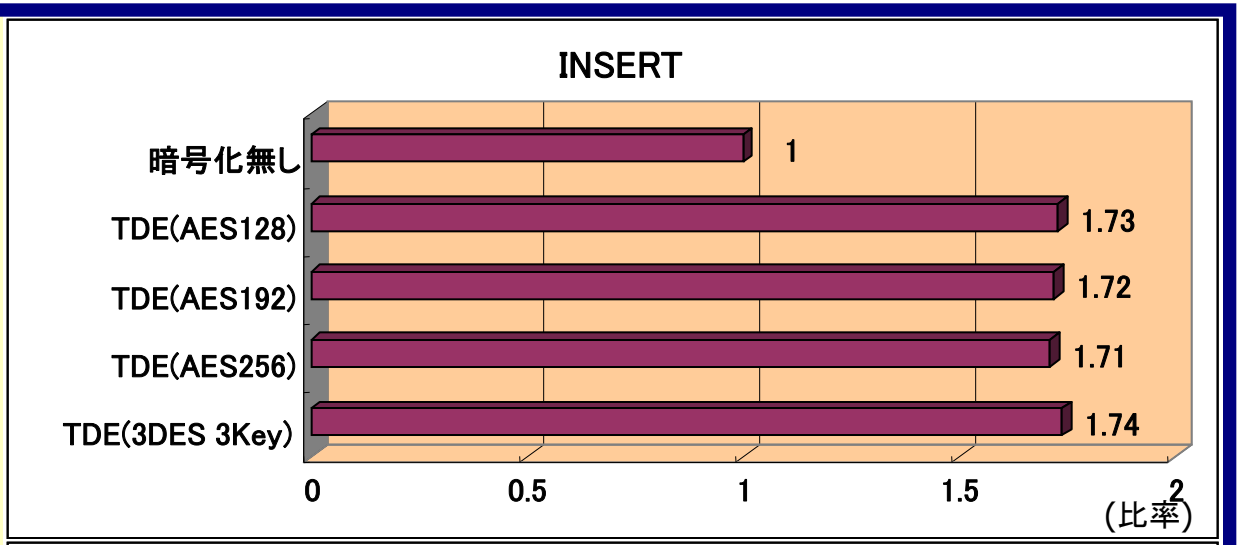
- 使用する暗号化アルゴリズムの違いによる、INSERT/SELECT処理性能の比較結果

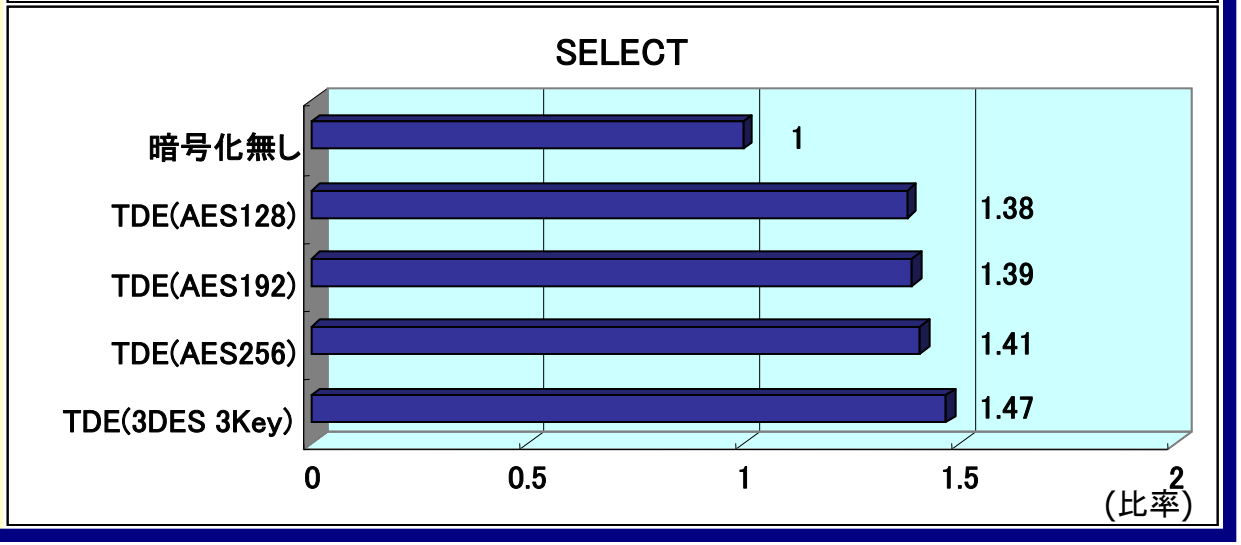
- どのアルゴリズムを使用しても、暗号化処理によって性能処理は劣化
  - INSERT：約1.7倍
  - SELECT：約1.4倍
- 鍵長を考慮すると、AESは3DESに比べて高速
- AESの鍵長の差異は、処理性能にほとんど影響を与えない

最大限のセキュリティの強固さと性能を両立するなら AES 256bit

おすすめ

※100万行の暗号化データの挿入、検索を行った際の処理時間を比較（シリアル処理）





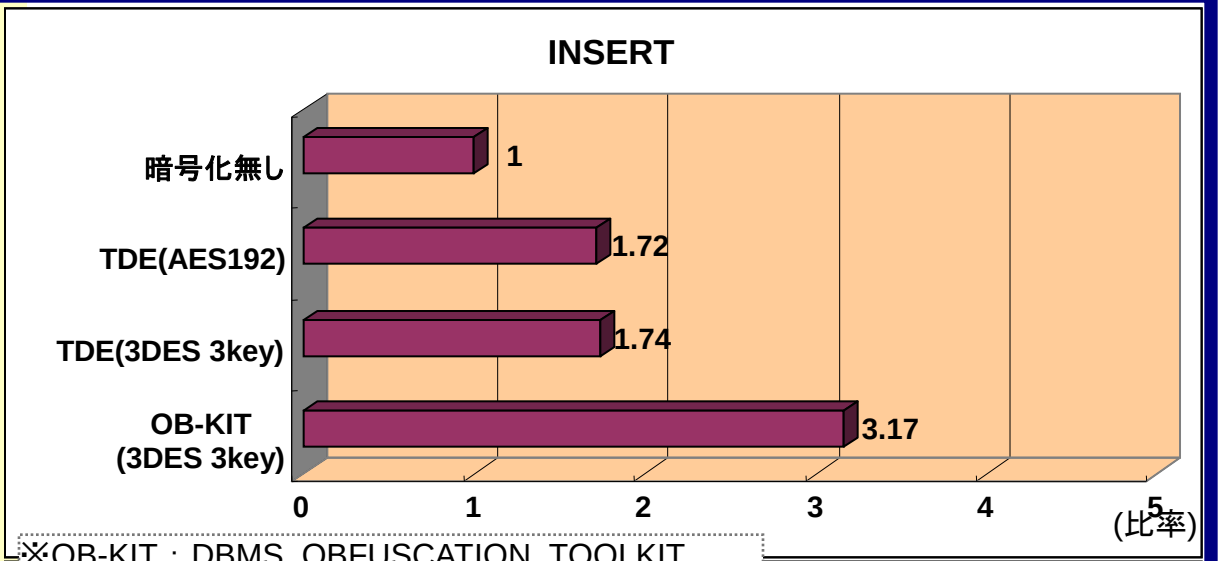
従来の暗号化方法との性能比較

- TDE vs DBMS_OBFUSCATION_TOOLKIT 性能比較結果

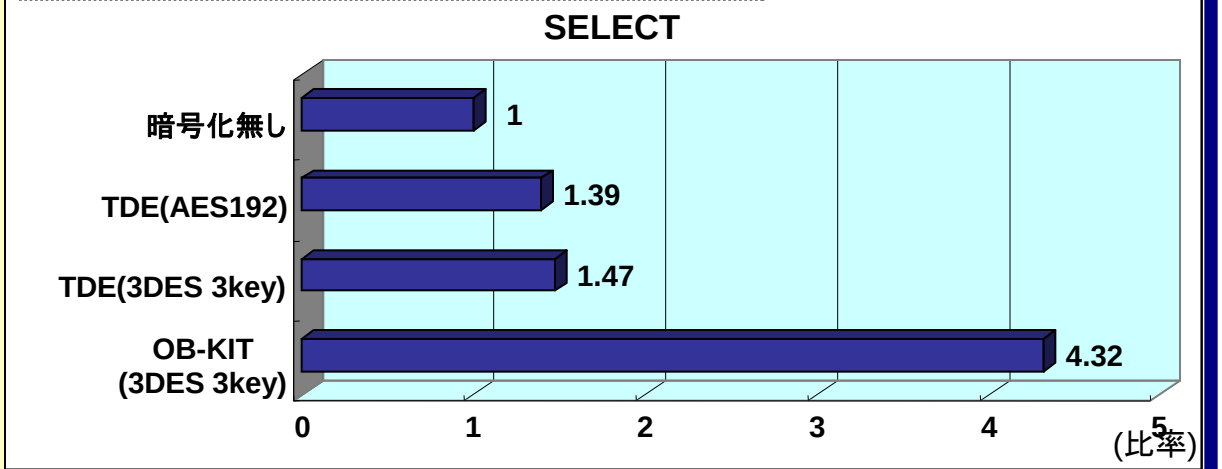
- 暗号化処理を行うことにより、処理性能が劣化する
  <TDE>
  - INSERT：約1.7倍
  - SELECT：約1.4倍

  <DBMS_OBFUSCATION_TOOLKIT>
  - INSERT：約3.2倍
  - SELECT：約4.3倍
- TDEのほうが、DBMS_OBFUSCATION_TOOLKITよりも明らかに処理性能が高い
  - INSERT：約2倍
  - SELECT：約3倍

※100万行の暗号化データの挿入、検索を行った際の処理時間を比較（シリアル処理）



※OB-KIT：DBMS_OBFUSCATION_TOOLKIT



Agenda

監査についての詳細は8/31実施の
実践!!セキュリティ
実践!!セキュリティ～Oracle Databaseの監査～
セミナーにご参加ください

- はじめに
- 基本機能で実現できるセキュリティ対策
  - Oracle Databaseインストール時の設定事項
  - 認証:ユーザの管理
  - 認証:パスワードポリシーの設定とOS認証
  - アクセス制御:オブジェクトレベル制御
  - 格納データの暗号化
  - 監査
  - まとめ
- Appendix
  - Enterprise Editionの機能

無償技術サービスOracle Direct Concierge

・SQL Serverからの移行アセスメント
・MySQLからの移行相談
・PostgreSQLからの移行相談
・Accessからの移行アセスメント
・Oracle Database バージョンアップ支援
・Oracle Developer/2000 Webアップグレード相談
・パフォーマンス・クリニック
・Oracle 構成相談
・Oracle Database 高可用性診断
・システム連携アセスメント
・システムセキュリティ診断
・簡易業務診断
・メインフレーム資産活用

http://www.oracle.com/lang/jp/direct/services.html

データベース環境において起こりうる脅威と監査機能

一般ユーザによる不正行為

- 不正なログイン
- 不正な閲覧、データ改竄、破壊行為
- 不正な権限付与
- 不正なユーザ作成などの構成変更

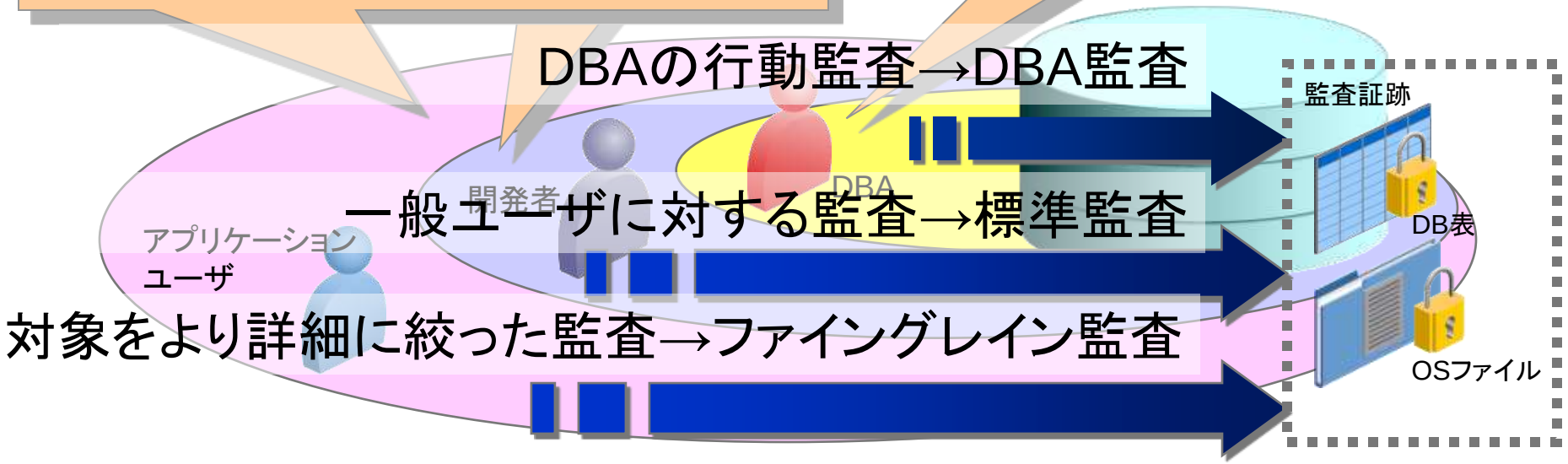
DBAによる不正行為

- 不正な閲覧、データ改竄、破壊行為
- 不正なユーザ作成などの構成変更
- 不正な権限付与
- 監査証跡の改竄

一般ユーザによる不正行為

Webアプリケーションユーザによる不正行為

- 不正な閲覧、データ改竄



その他の監査機能

DBの起動停止・リスナーへの接続

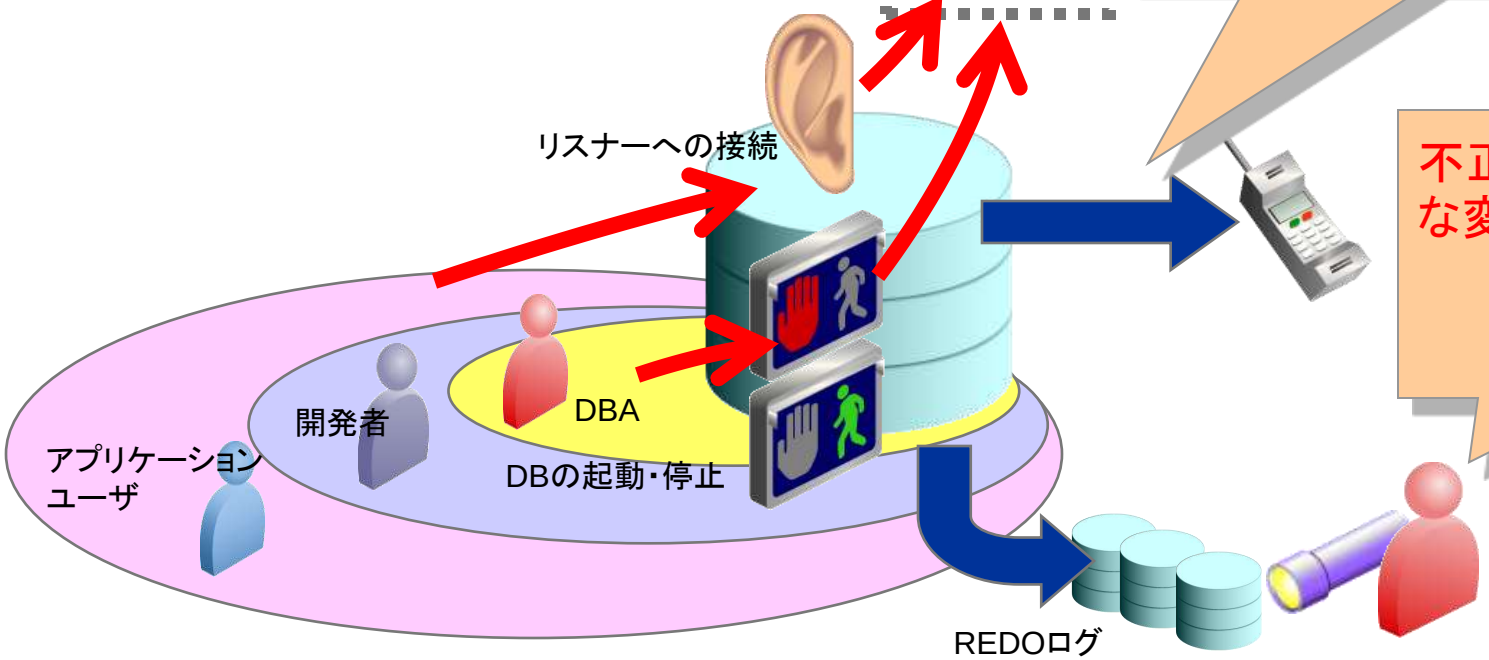
必ず行なわれる監査

監査証跡

OSファイル

監査証跡の記録以外のアクション

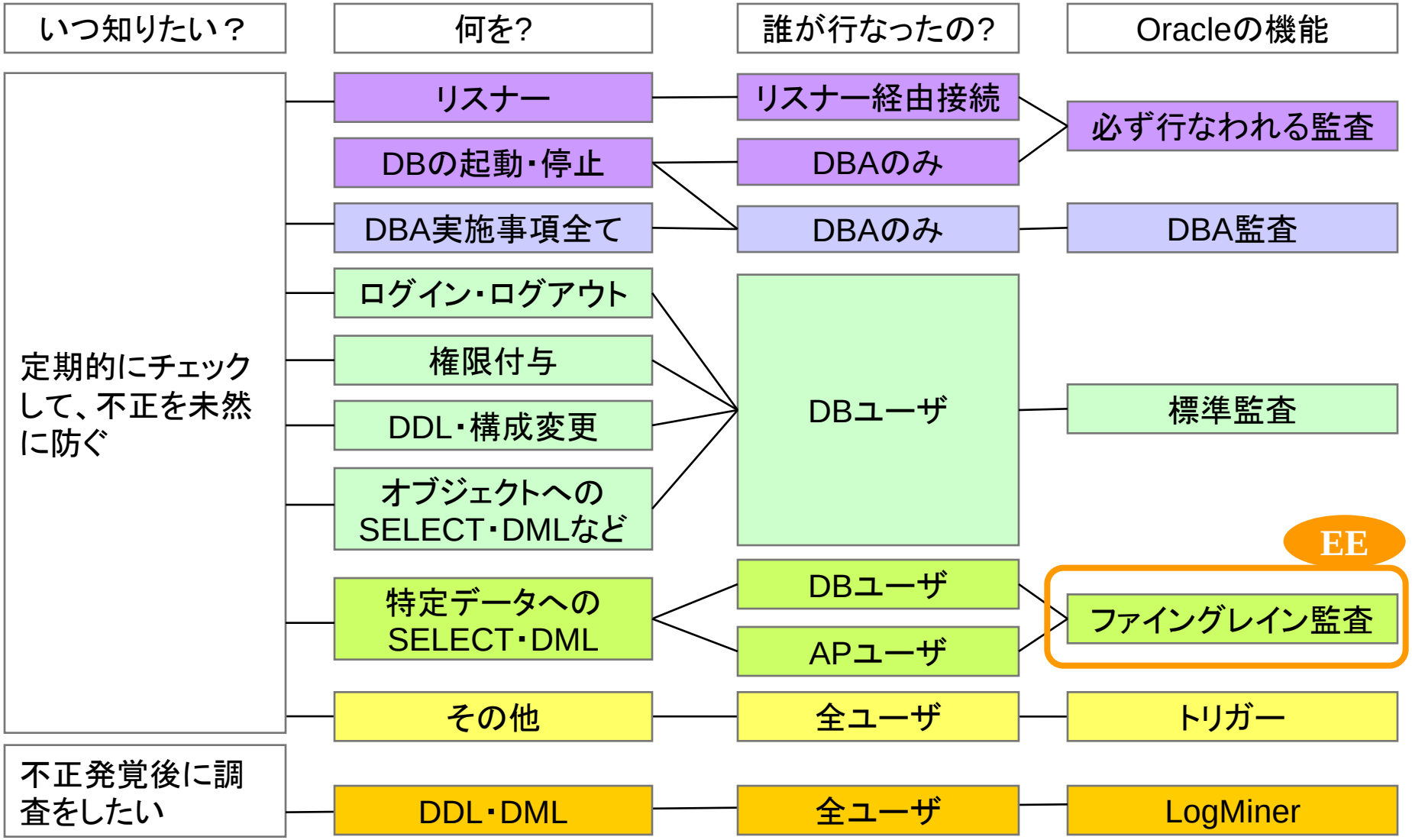
トリガーによる処理



不正発覚後の、詳細な変更履歴の参照

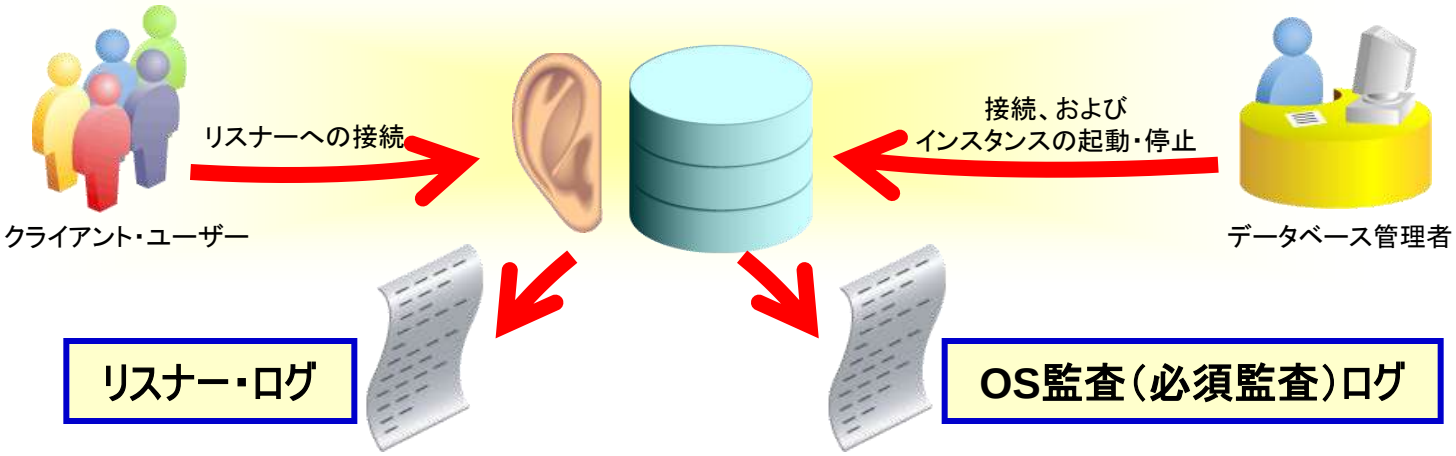
LogMiner

オラクルで実現できる監査の種類



必須監査

- 必須監査：デフォルトでおこなわれる、必要最低限の監査
  - 特権ユーザ（DBA）による基本操作（起動・停止）
  - リスナーを介したOracle Net Servicesによるインスタンスへの接続

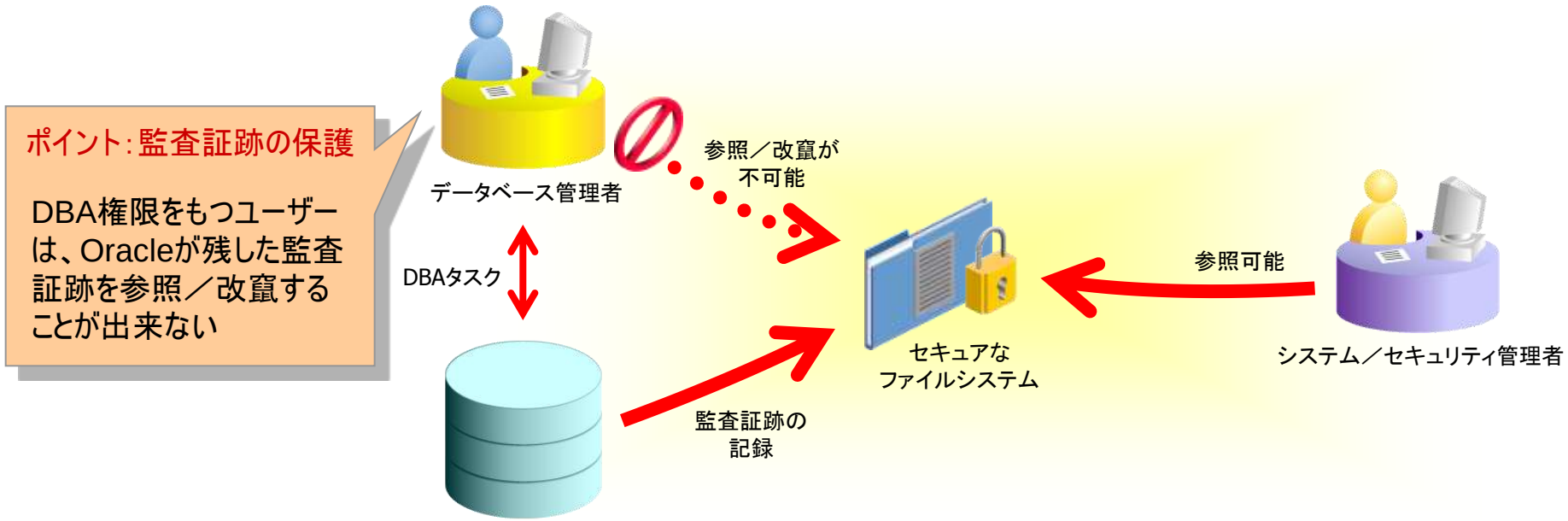


必須監査で取得できる監査証跡

- SYSOPER/SYSDBAでの接続、DBの起動・停止
  - 出力先:
    - Windows: イベントログ
    - Windows以外:$ORACLE_HOME/rdbms/audit/ora_xxxxx.aud
      (xxxx はプロセス番号)
  - 出力を停止することはできない。
- Listenerへの接続
  - 出力先:
    - Windows: %ORACLE_HOME%¥network¥log¥<リスナー名>.log
    - Windows以外:$ORACLE_HOME/¥network/log/<リスナー名>.log
  - リスナーを経由しない接続は当然記録されない
  - Oracle Net Servicesのエラーも記録される(TNS-xxxxx)
  - ログインエラー(パスワード違い等)はNetのエラーではないので記録されない
  - デフォルトでは出力、停止は可能。(停止:lsnrctl set log_status off)

DBA監査（9iR2以降）

- 正当なDBA権限を持ったユーザーによる不正アクセスへの対策
  - DBAユーザーが行う全ての操作をOS上に監査証跡として残すことにより、システム／セキュリティ管理者によるDBAユーザーの監査を可能にする



DBA監査の取得方法

- 初期化パラメータ

·AUDIT_SYS_OPERATIONS DBA監査をおこなうかどうか（デフォルトFALSE）
·AUDIT_FILE_DEST 監査証跡の出力場所（デフォルト$ORACLE_HOME/rdbms/audit）
·AUDIT_TRAIL 監査取得有無および出力形式を指定
（none | os | db | db,extended | xml | xml,extended）

- 出力先
  - Windows: ｲﾍﾞﾝﾄﾛｸﾞ
  - Windows以外: AUDIT_FILE_DEST で指定されたディレクトリ

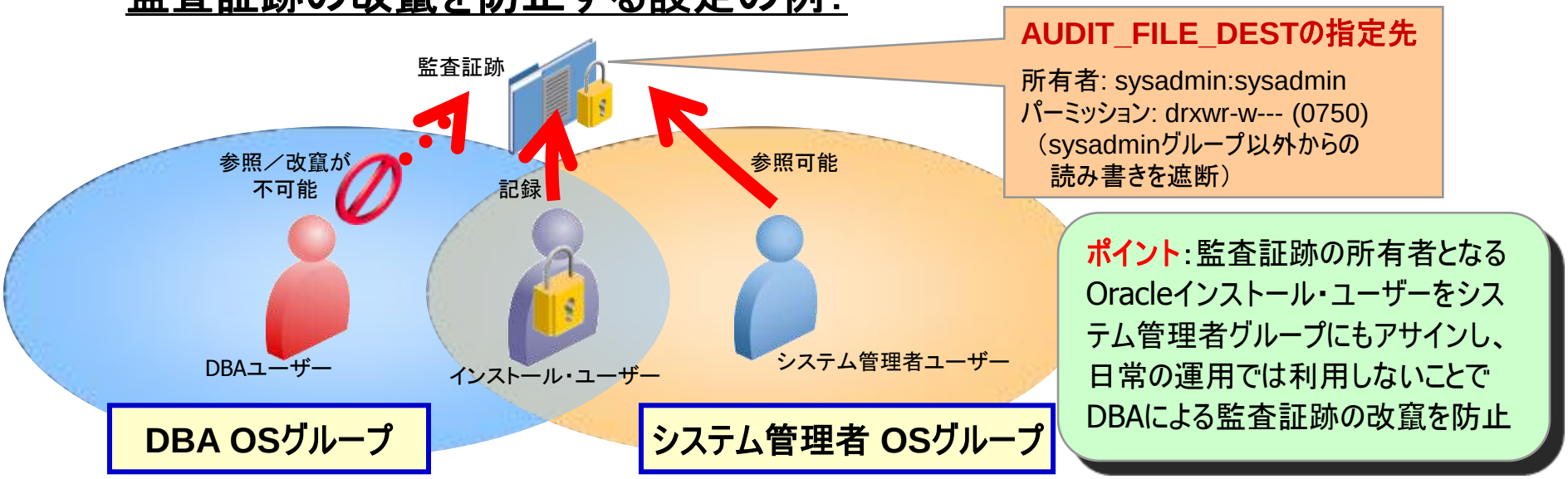
- 出力形式
  - 通常のログファイル
  - XML形式（audit_trail=xml もしくは xml,extended）

```
Thu Jan 24 12:58:00 2002
ACTION: 'CONNECT'
DATABASE USER: '/'
OSPRIV: SYSDBA
CLIENT USER: jeff
CLIENT TERMINAL: pts/2
STATUS: 0

Thu Jan 24 12:58:00 2002
ACTION: 'update salary set base=1000
 where name='myname''
DATABASE USER: ''
OSPRIV: SYSDBA
CLIENT USER: jeff
CLIENT TERMINAL: pts/2
STATUS: 0
```

DBA監査 - 運用上のポイント

- OS管理者とDBAのそれぞれを別々のユーザー / グループとして管理し、相互の行動を監視できる形で運用を行う
- システム／セキュリティ管理者によるDBAの監視を実現するためには、DBAによる監査証跡の改竄を防止する必要がある
- 監査証跡は、Oracleのインストール・ユーザーのUIDで記録される

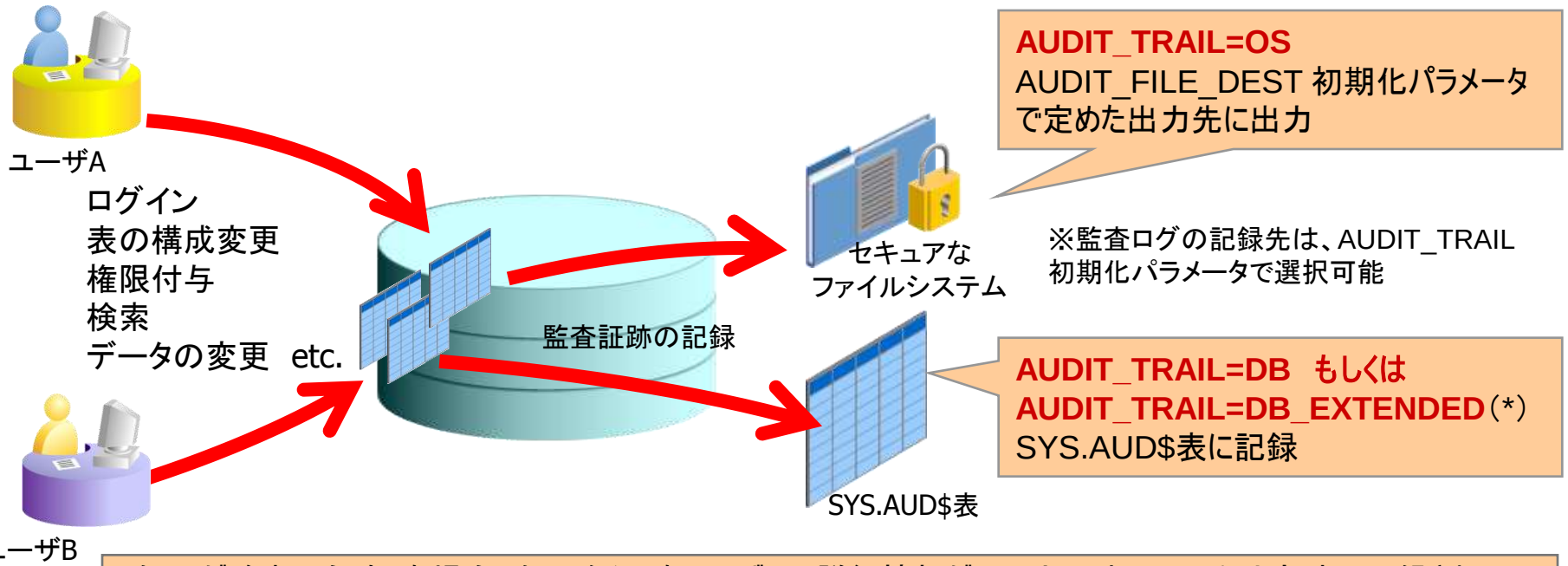
監査証跡の改竄を防止する設定の例：



標準監査

- システムに即した不正行為への対策：

  一般ユーザの特定オブジェクトに対する操作、権限付与、およびデータベース構成変更に対し、監査証跡を取得する



・処理が監査に合致した場合、処理を行ったユーザーの詳細情報がSQL文とともに aud$ 内部表に記録される

・aud$ の内容は、DBA_AUDIT_TRAIL ビューを利用して確認する

（*）AUDIT_TRAIL=DB_EXTENDEDはOracle10gからの機能です

標準監査の取得方法

- 初期化パラメータ

```
・AUDIT_FILE_DEST      監査証跡の出力場所（デフォルト$ORACLE_HOME/rdbms/audit）
・AUDIT_TRAIL          監査取得有無および出力形式を指定
                       (none | os | db | db,extended | xml | xml,extended)
```

- 標準監査の機能
  1. **セッション監査**
     - ログオン・ログアウトを監査することで、**不審なログオン行為を早期発見**する
  2. **オブジェクト監査**
     - 特定オブジェクトに対する検索や更新処理などの操作を監査することで、**不審なデータアクセス行為**を早期発見する
  3. **権限監査**
     - 特定スキーマからの権限付与を監査し把握することで、**不審な権限付与**を早期発見する
  4. **SQL文監査（DDL文監査など）**
     - 特定スキーマからのDDLなどの発行されたSQL文を監査することで、**不審な構成変更**を早期発見する

監査証跡の記録先の違いによる監査証跡の違い

- 監査証跡の記録先をOSにすると、取得される監査証跡項目が限定される

監査ログ情報	AUDIT_TRAIL		
	OS	DB	DB_EXTEND
SQL文に使用されたバインド値（ある場合）	ー	ー	○
SQLテキスト（監査をトリガーしたSQLテキスト）	ー	ー	○
操作の完了コード	○	○	○
データベース・ユーザー名 （DATABASE USER）（OS）	○	○	○
UTC（協定世界時）書式による日時のタイムスタンプ	ー	○	○
識別名	○	○	○
グローバル・ユーザーの一意ID	ー	○	○
インスタンス番号	ー	○	○
アクセスされたスキーマ・オブジェクトの名前	○	○	○
オペレーティング・システムのログイン・ユーザ名 （CLIENT USER）	○	○	○
実行または試行された操作 （ACTION）	○	○	○
処理番号（UNIX: ProcessId、Windows: ProcessId:ThreadId）	○	○	○
プロキシ・セッションの監査ID	ー	○	○
SQL文のSCN（システム変更番号）	ー	○	○
セッション識別子	○	○	○
使用されたシステム権限（PRIVILEGE）	○	○	○
端末識別子	○	○	○
トランザクションID	ー	○	○

10gR1～

※ ーは取得不可
※ ○は取得可能
※ AUDIT_TRAILは、初期化パラメータAUDIT_TRAILに設定した値です。

標準監査の運用上の注意点

- BY ACCESS とBY SESSION の違い
  - コマンドオプションによって監査証跡の出力量が異なり、情報も異なるので、監査設定時に注意する

BY ACCESS	監査対象行為毎に1件の監査証跡
BY SESSION	セッション毎に1件の監査証跡

```
SES_ACTIONS
---------------
---------S------
```

※BY SESSIONと指定した場合の
DBA_AUDIT_TRAILのSES_ACTIONS列の例

- 監査証跡の出力先
  - DBAによる監査証跡の改竄を防止する為に、DBA監査との組み合わせる

- クライアント識別子（後述）
  - セッション開始時にクライアント識別子を設定することで、アプリケーション・ユーザの情報も監査ログに格納できる。
    - 前頁のオブジェクト監査例を参照
      - クライアント識別子として 'TANAKA' を設定した例

まとめ: Oracle Databaseが提供しているセキュリティ機能

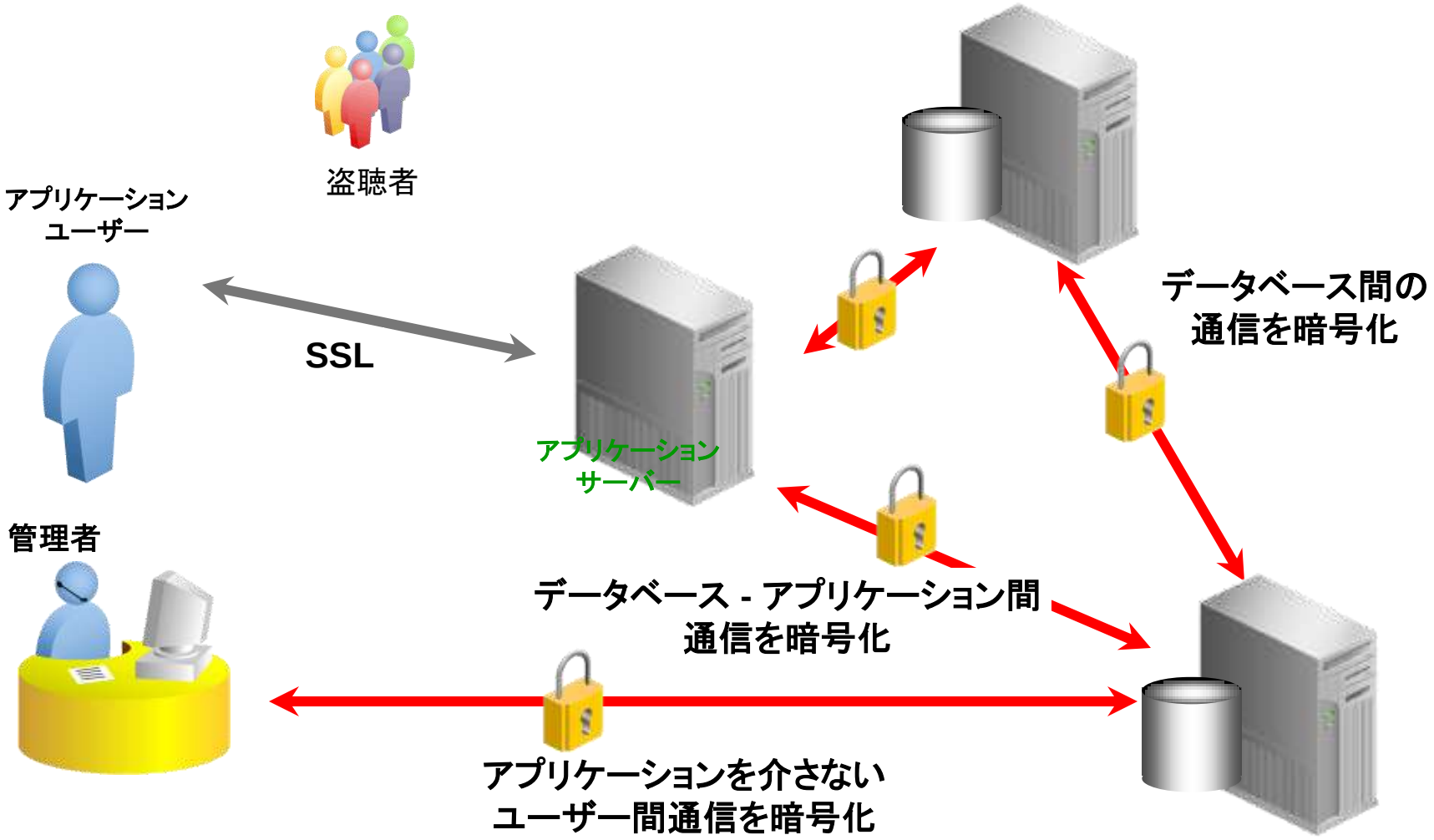
カテゴリ	機能名	利用可能 Edition	必要なOption もしくは製品
通信データの暗号化	Net接続 の暗号化	EE	Advanced Security
認証の強化	**パスワード・ポリシーの強化**	**SE**	
	外部認証(OS認証)	**SE**	
	外部認証(ネットワーク認証)	EE	Advanced Security
	グローバル認証	EE	Advanced Security
	Enterprise User Security (EUS)	EE	Advanced Security
アクセス制御	**オブジェクトレベル制御 (View, GRANT)**	**SE**	
	値レベル制御(Virtual Private Database: VPD)	EE	
	Database Vault を使った職務分掌による デュアルロック機能(＊1)による制御強化	EE	Database Vault
格納データの暗号化	**暗号化ツールキット(DBMS_CRYPTO, DBMS_OBFUSCATION_TOOLKIT)**	**SE**	
	透過的データ暗号化 (Transparent Data Encryption: TDE)	EE	Advanced Security
監査	**必須監査**	**SE**	
	標準監査	**SE**	
	DBA監査	**SE**	
	特定データアクセス監査(ファイングレン監査)	EE	
	Audit Vaultによる監査情報の一元管理		Audit Vault

(＊1):デュアルロック機能とは、行為に対して、少なくとも2名の者が操作しなければその行為を完遂できない方式

Appendix：
Enterprise Editionの機能

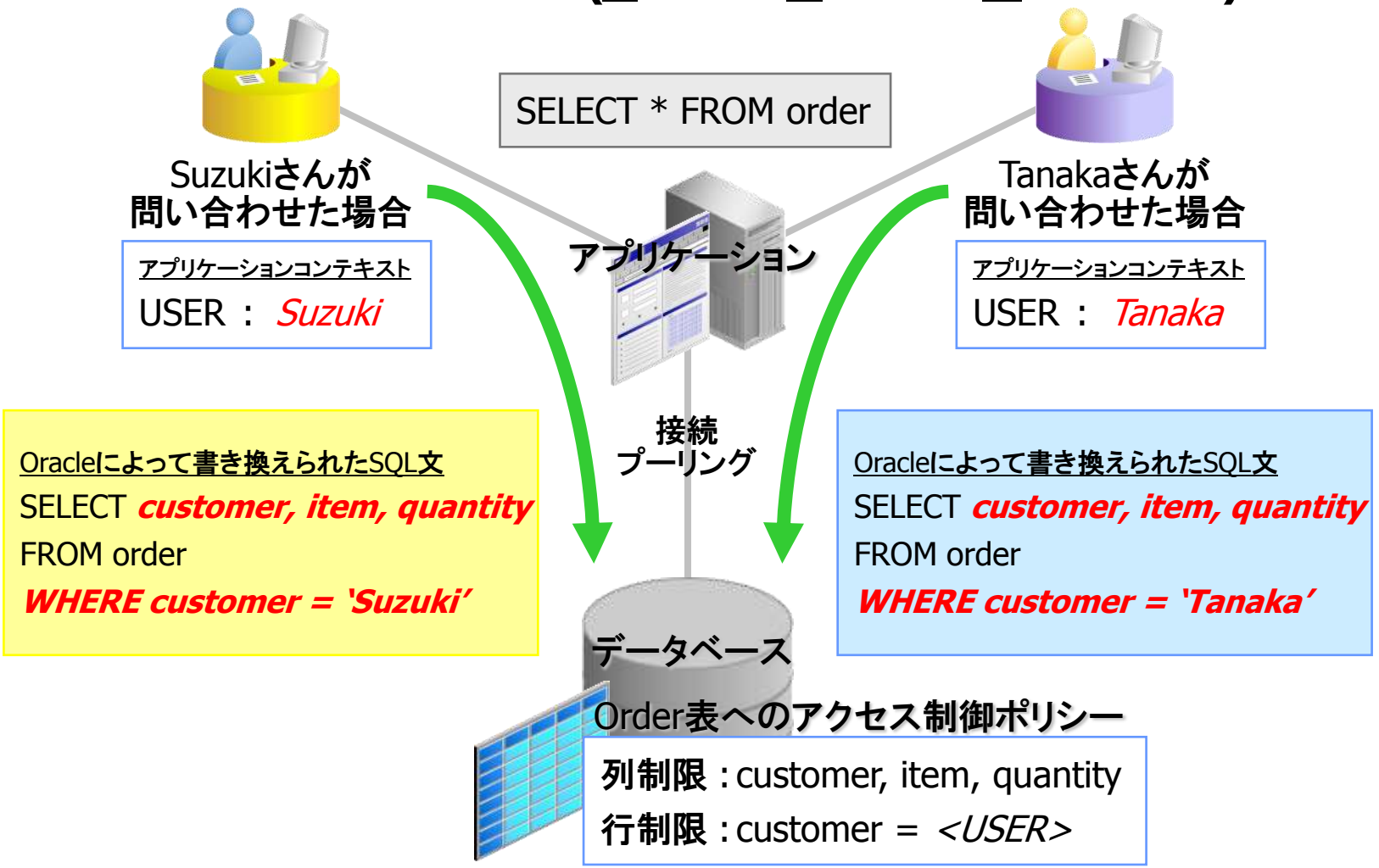
通信データの暗号化

Oracle Advanced Securityによる通信の暗号化



仮想プライベートデータベースによるアクセス制御

仮想プライベートデータベース(Virtual Private Database)



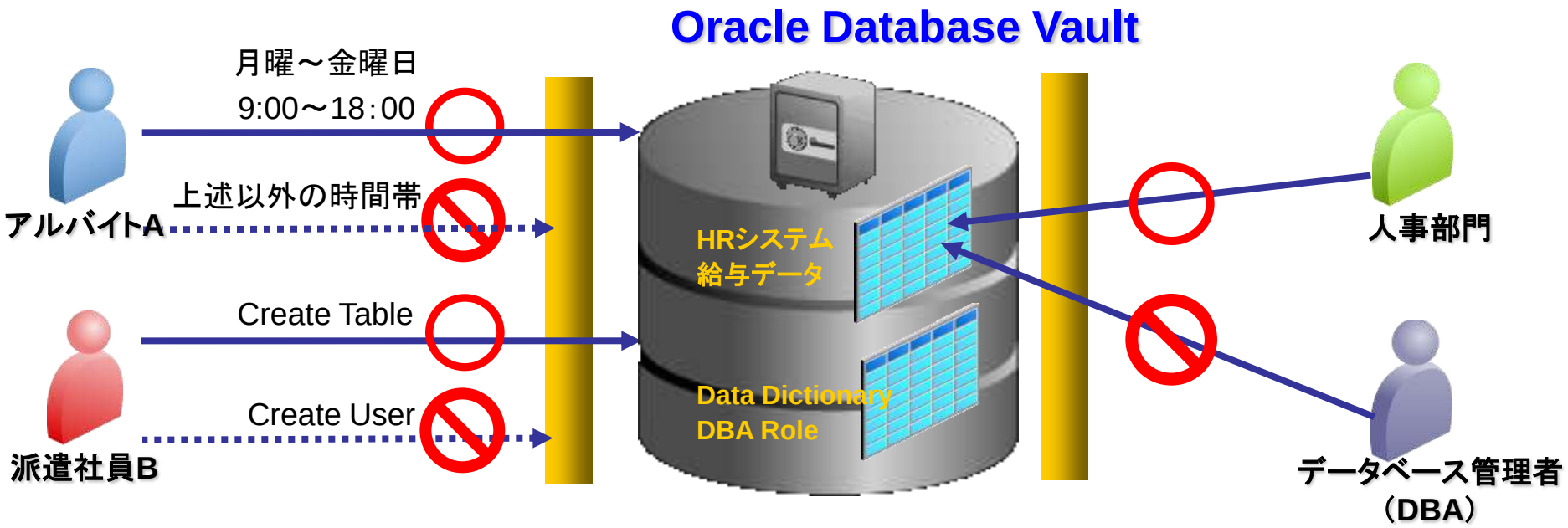
Oracle Database Vault

DBAの権限を制御し、セキュリティ管理者と分離する

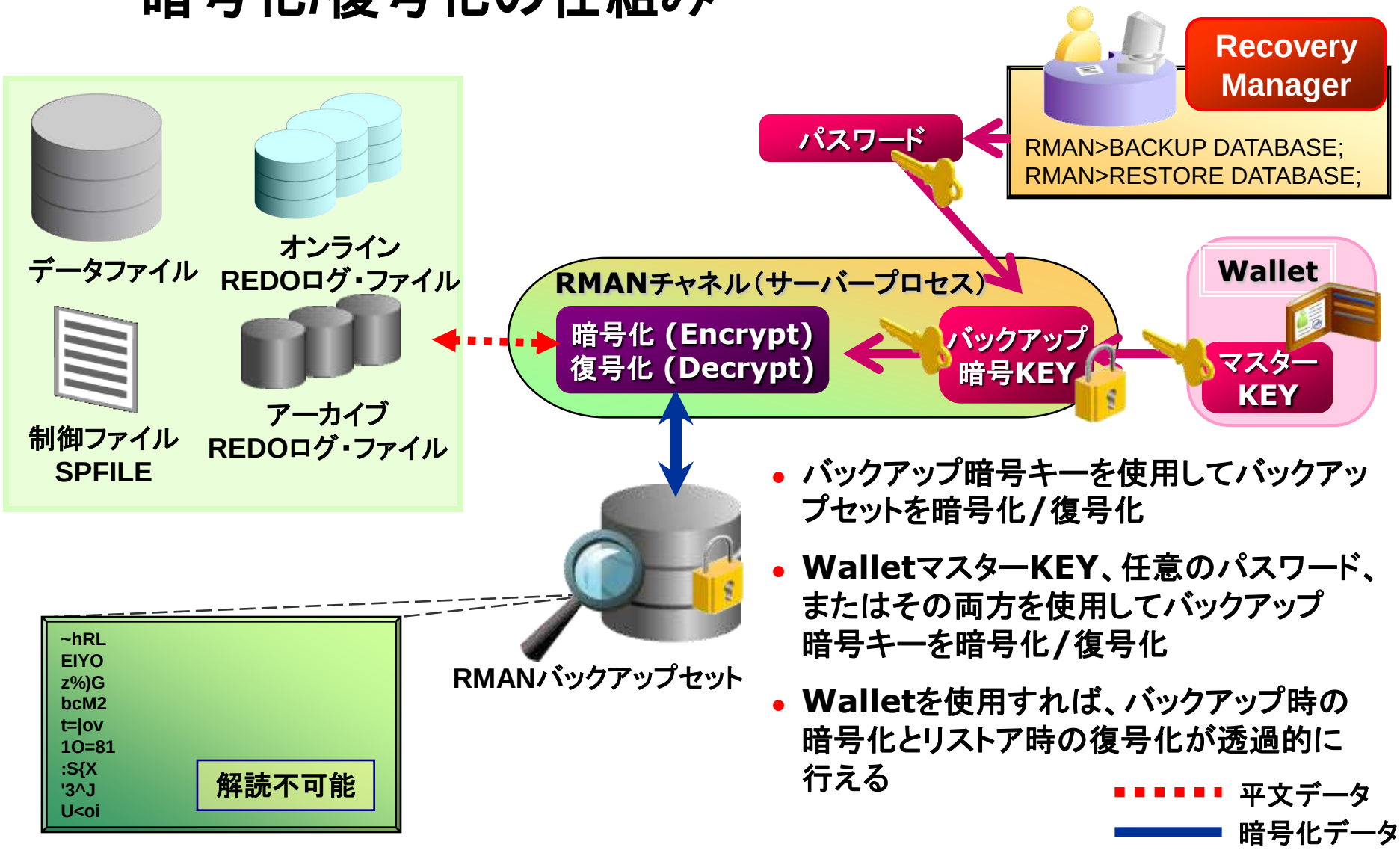
管理者の不正データアクセスを抑制する安全なデータ基盤

- DBAのアクセス権限を制御する
  - ✓ SYS/SYSTEMへの権限集中によるリスクを回避（管理権限の分散）
- ユーザーのコマンド制限、アクティビティの制限
- 複数の要素による認証の強化（時間、IPアドレス、言語 …）

強靭な
アクセス
制御機能



RMANバックアップセットの暗号化
暗号化/復号化の仕組み

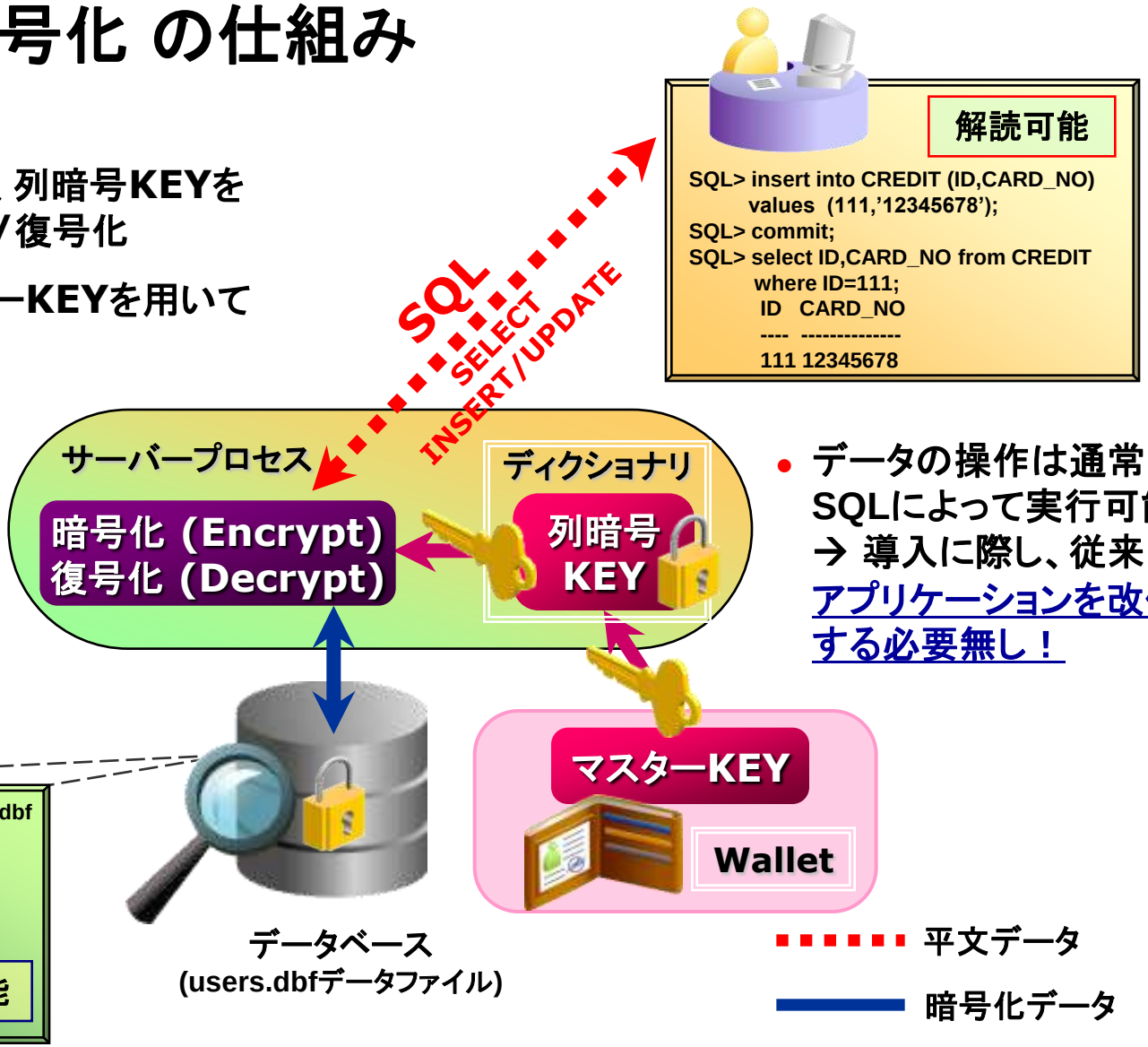


- バックアップ暗号キーを使用してバックアップセットを暗号化/復号化
- **Wallet**マスター**KEY**、任意のパスワード、またはその両方を使用してバックアップ暗号キーを暗号化/復号化
- **Wallet**を使用すれば、バックアップ時の暗号化とリストア時の復号化が透過的に行える

平文データ
暗号化データ

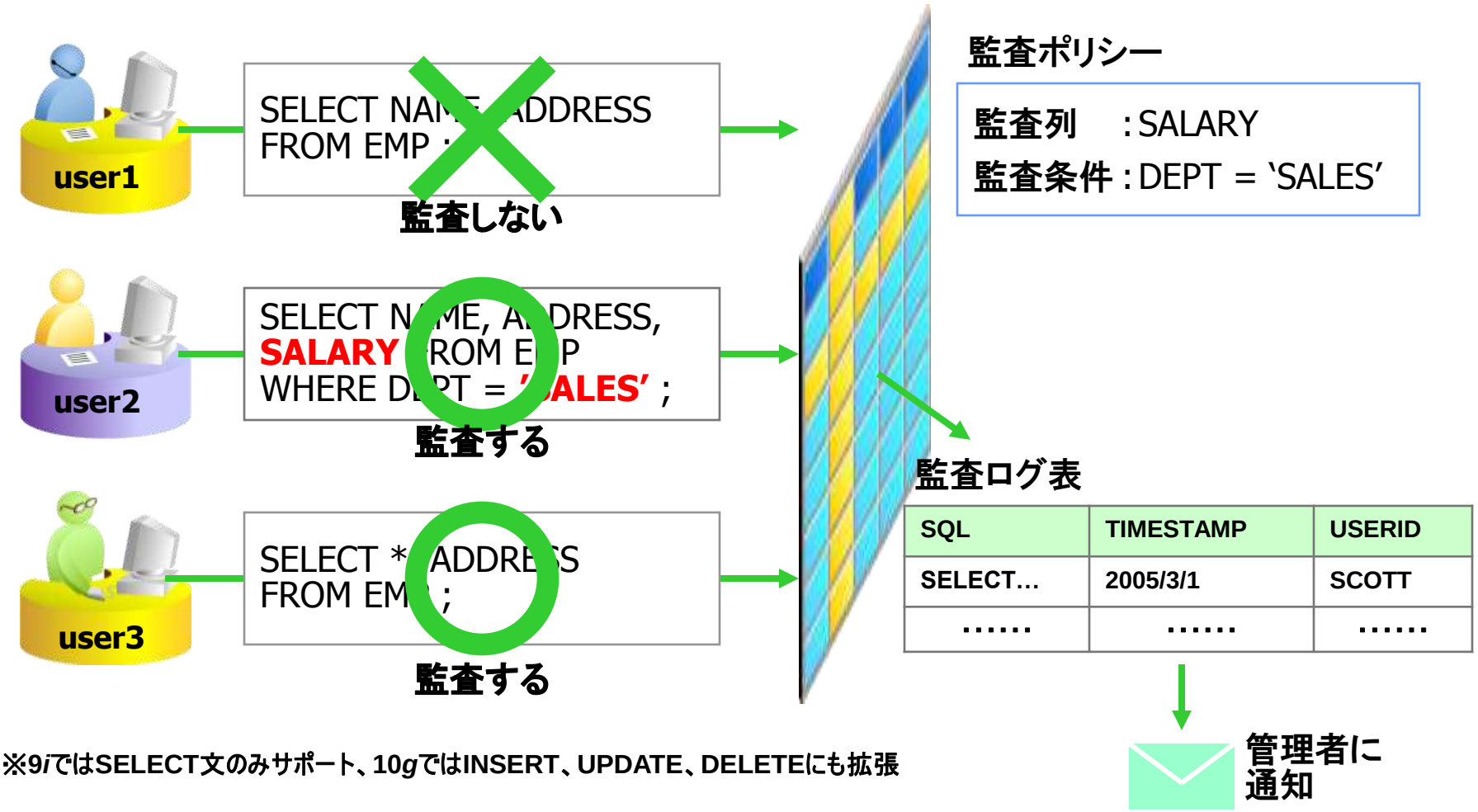
Transparent Data Encryption
暗号化/復号化 の仕組み

- サーバープロセス内で、列暗号KEYを用いてデータを暗号化/復号化
- 列暗号KEYは、マスターKEYを用いて暗号化/復号化
- 暗号化/復号化処理はサーバプロセス内で自動的に実行されるため、クライアント側で運用中に意識する必要は無い



- データの操作は通常のSQLによって実行可能
→ 導入に際し、従来のアプリケーションを改修する必要無し！

ファイングレン監査（9iR1以降）

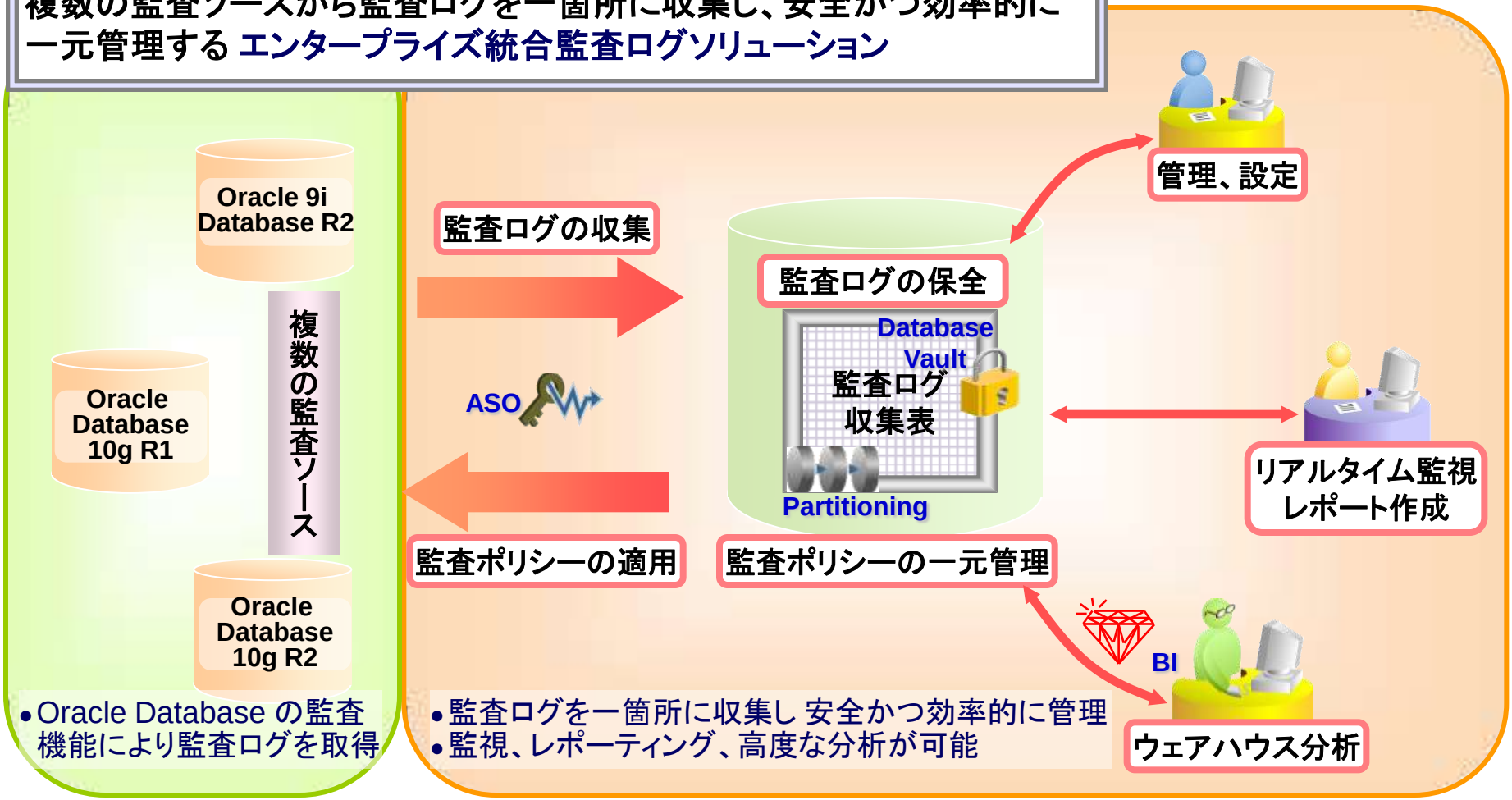


※9*i*ではSELECT文のみサポート、10*g*ではINSERT、UPDATE、DELETEにも拡張

Oracle Audit Vault

監査ログの安全かつ効率的な一元管理

複数の監査ソースから監査ログを一箇所に収集し、安全かつ効率的に一元管理する エンタープライズ統合監査ログソリューション



OTN×ダイセミ　でスキルアップ!!

・一般的な技術問題解決方法などを知りたい！
・セミナ資料など技術コンテンツがほしい！

Oracle Technology Network(OTN)を御活用下さい。

http://otn.oracle.co.jp/forum/index.jspa?categoryID=2

一般的技術問題解決にはOTN掲示版の
「データベース一般」をご活用ください

※OTN掲示版は、基本的にOracleユーザー有志からの回答となるため100%回答があるとは限りません。
ただ、過去の履歴を見ると、質問の大多数に関してなんらかの回答が書き込まれております。

http://www.oracle.com/technology/global/jp/ondemand/otn-seminar/index.html

過去のセミナ資料、動画コンテンツはOTNの
「OTNセミナー　オンデマンド コンテンツ」へ

※ダイセミ事務局にダイセミ資料を請求頂いても、お受けできない可能性がございますので予めご了承ください。
ダイセミ資料はOTNコンテンツ　オン　デマンドか、セミナ実施時間内にダウンロード頂くようお願い致します。

OTNセミナー　オンデマンド　コンテンツ

ダイセミで実施された技術コンテンツを動画で配信中!!

ダイセミのライブ感はそのままに、お好きな時間で受講頂けます。

OTN　オンデマンド　検索

※掲載のコンテンツ内容は予告なく変更になる可能性があります。
　期間限定での配信コンテンツも含まれております。お早めにダウンロード頂くことをお勧めいたします。

オラクル クルクルキャンペーン

あのOracle Database Enterprise Editionが超おトク!!

おトクな買い方
オラクル5年分

- ライセンス使用期間　を5年間に設定
- 初期のライセンスコストがなんと67%OFF　！
- テクニカル・サポート価格も53%OFF　！

Oracle Databaseの
ライセンス価格を大幅に抑えて
ご導入いただけます

多くのお客様でサーバー使用期間とされる
5年間にライセンス期間を限定

- 期間途中で永久ライセンスへ差額移行
- 5年後に新規ライセンスを購入し継続利用
- 5年後に新システムへデータを移行

Enterprise Editionはここが違う!!

- 圧倒的なパフォーマンス!
- データベース管理がカンタン!
- データベースを止めなくていい!
- もちろん障害対策も万全!

この機能でこの価格
ライセンスパック

- Oracle Databaseの機能を存分に使える!
- 2ノードRAC構成も可能!
- サーバー構成によって計4種類のパックから選べる!

詳しくはコチラ
http://www.oracle.co.jp/campaign/kurukuru/index.html

Oracle Direct 0120-155-096

お問い合わせフォーム
http://www.oracle.co.jp/inq_pl/INQUIRY/quest?rid=28

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　検索

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

※フォームの入力には、Oracle Direct Seminar申込時と同じ
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、ご登録されている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）

以上の事項は、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。