Oracle Direct Seminar

ORACLE®

本当は遅くない! オラクルの監査と暗号の実際

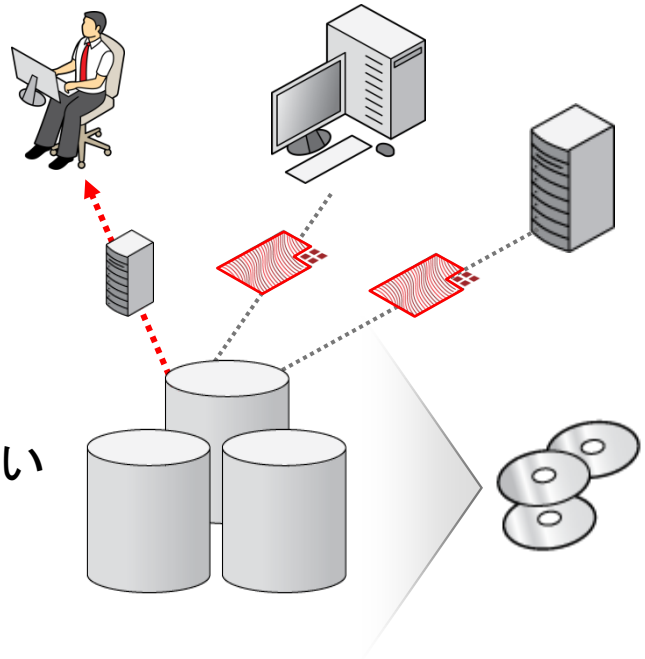
日本オラクル株式会社　テクノロジー製品事業統括本部
シニアエンジニア ,CISSP　西村克也

Oracle Direct

Oracle Direct Seminar

データベースの暗号化って何？

- どういった脅威があるのか？
  - データベースとの通信の盗聴
  - データベースに関連するファイルの盗難
  - バックアップメディアの盗難・紛失

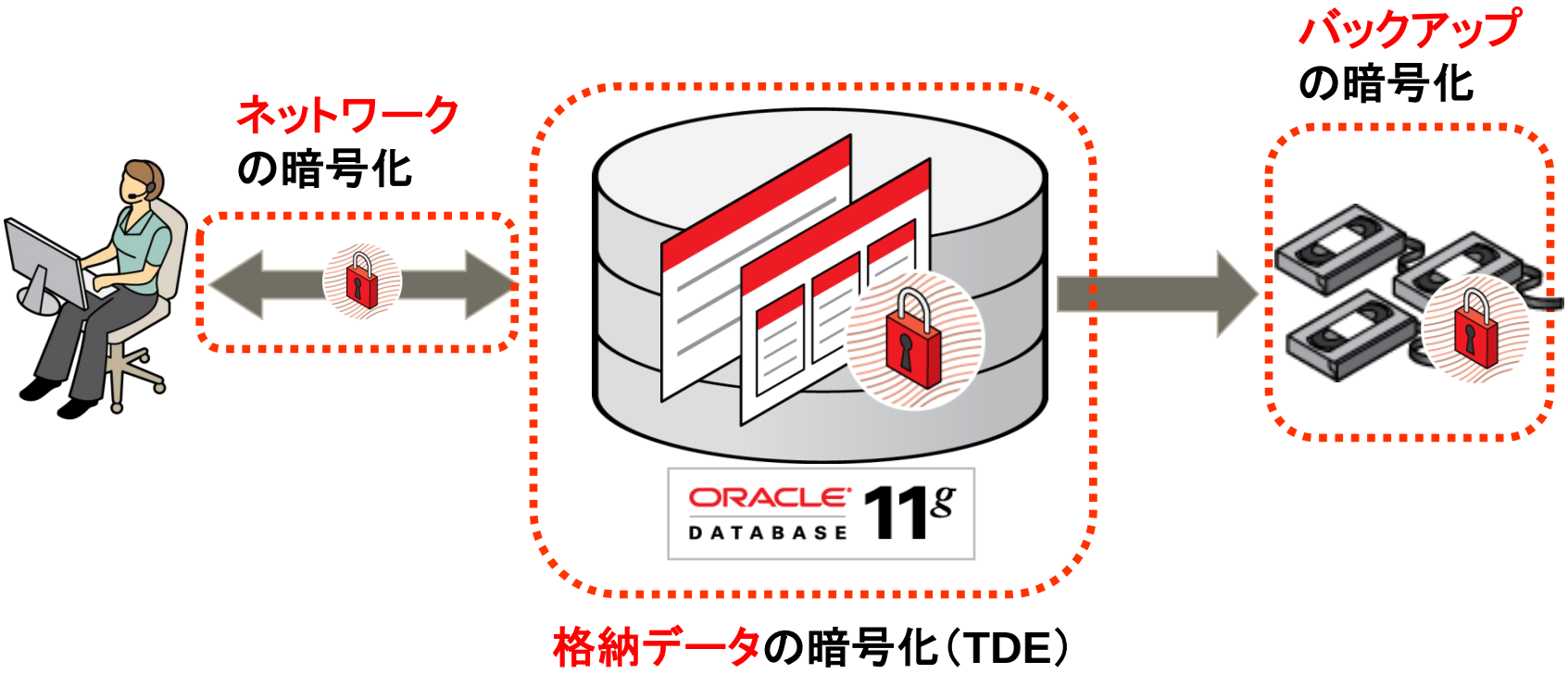


- 暗号化するとどうなるのか？
  - パケットキャプチャしても通信内容は分からない
  - Oracleのファイルをバイナリレベルで読み取れない

- ただし・・
  - 暗号化はデータベース・セキュリティの一部
  - 認証、アクセス制御と組み合わせることで効果倍増

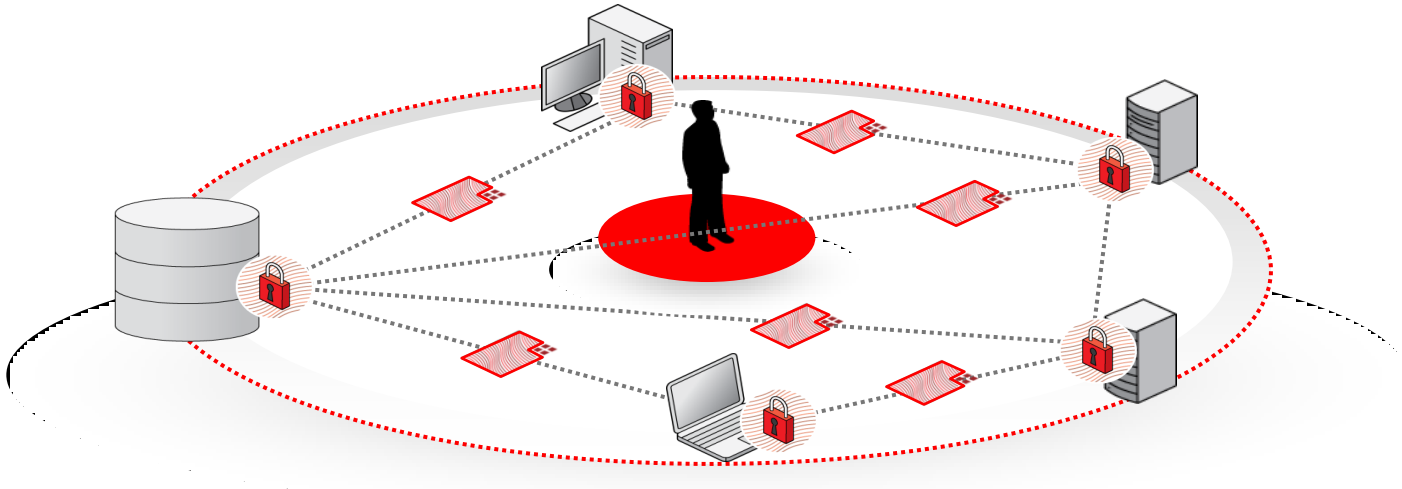
Oracle Advanced Security

- 可用性と機密性を両立したOracleデータベース暗号化機能
- 暗号化が求められるセキュリティ要件への対応を支援



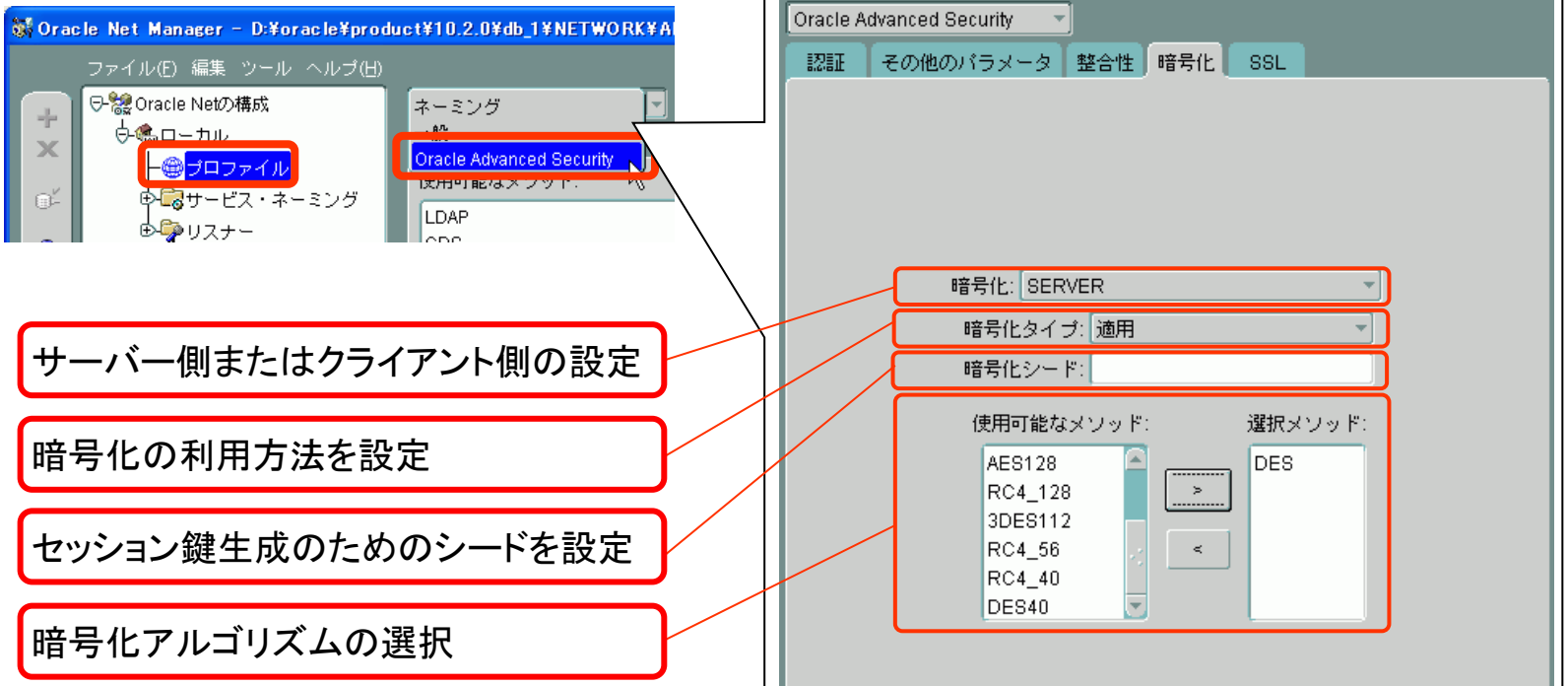
ネットワークの暗号化

- データベース・サーバーのすべての通信データを暗号化
  - クライアント～データベース間
  - アプリケーションサーバ～データベース間
  - データベース・リンク、DataGuardによるデータベース間のミラーリング
- AES 暗号アルゴリズム、鍵管理の必要なし
- JDBC Thin/OCIクライアントにも対応



ネットワークの暗号化 - 設定例-

Oracle Net Managerを利用して通信暗号化方式を設定 (または、sqlnet.oraを直接編集)



編集内容は、sqlnet.oraに自動的に追記

```
SQLNET.ENCRYPTION_SERVER = required
SQLNET.ENCRYPTION_TYPES_SERVER= (AES256)
```

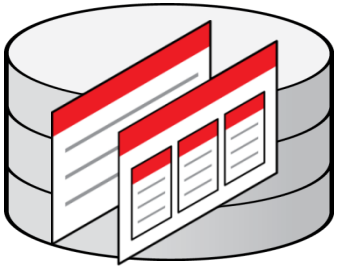
従来の格納データ暗号化機能の問題点

暗号化ツールキット（PL/SQLパッケージ）
を利用したデータの暗号化はOracle 9i以前からも可能

しかし

```
SQL> declare
  2    input_data varchar2(256) := '暗号化したい文字列';
  3    key_data raw(8) := dbms_obfuscation_toolkit.desgetkey(
  4        seed => utl_raw.cast_to_raw(rpad('abcd', 80, 'abcd')));
  5    output_data raw(256);
  6    output_data2 raw(256);
  7  begin
  8    dbms_output.put_line(input_data);
  9   dbms_obfuscation_toolkit.desencrypt(
 10      input => utl_raw.cast_to_raw(rpad(input_data, ((floor(lengthb(input_data)/8 + .9)) * 8))),
 11      key => key_data,
 12      encrypted_data => output_data);
 13    dbms_output.put_line(output_data);
 14    dbms_obfuscation_toolkit.desdecrypt(
 15      input => output_data,
 16      key => key_data,
 17      decrypted_data => output_data2);
 18    dbms_output.put_line(utl_raw.cast_to_varchar2(rtrim(output_data2)));
 19  end;
 20  /
```

暗号化ツールキットの利用

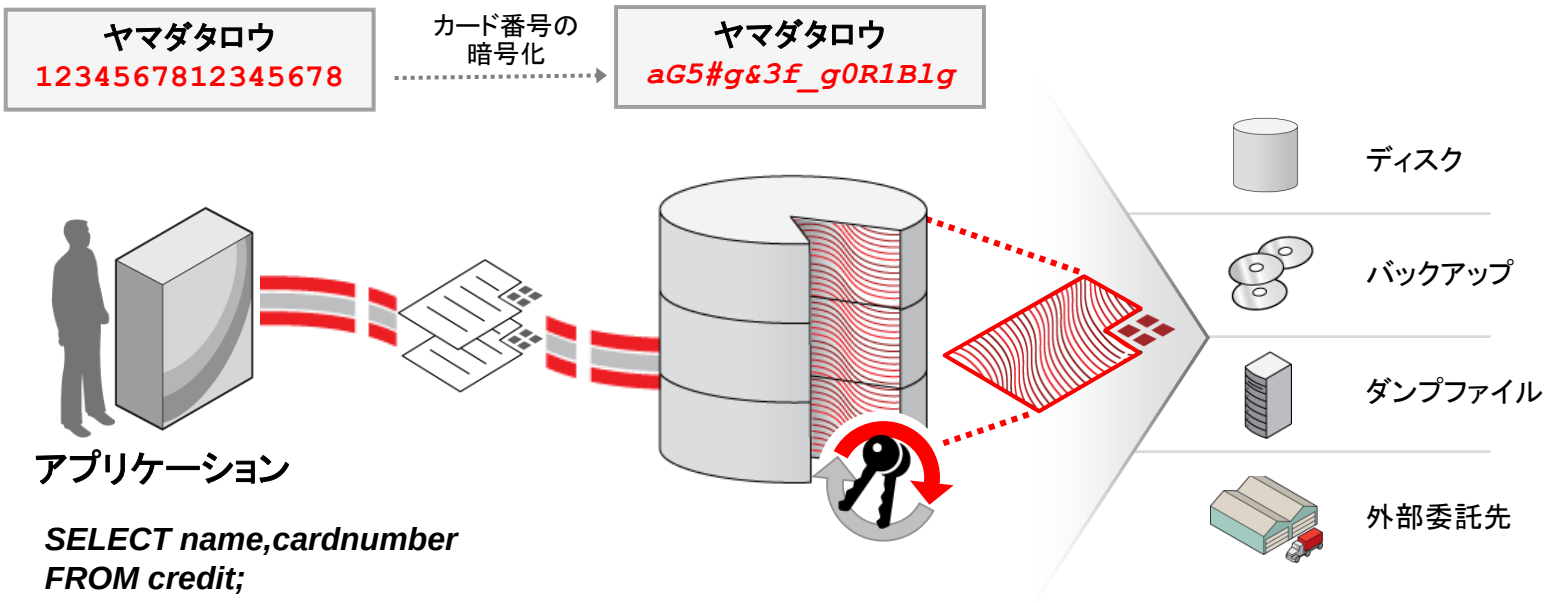


- アプリケーションの変更が必要
- パフォーマンスの劣化が大きい
- 暗号鍵管理の問題

セキュリティ要件上は求められていても、
データ暗号化の実装は困難・・

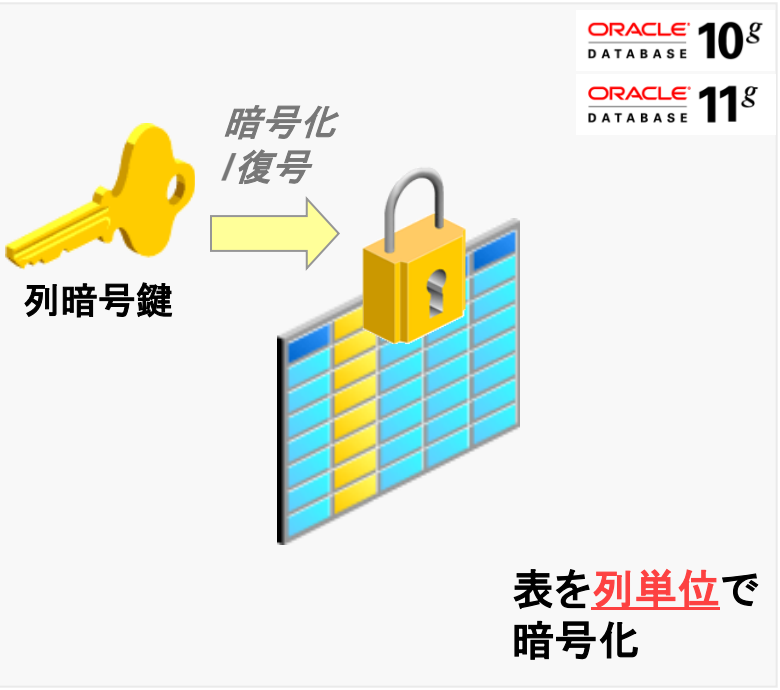
Transparent Data Encryption（TDE）

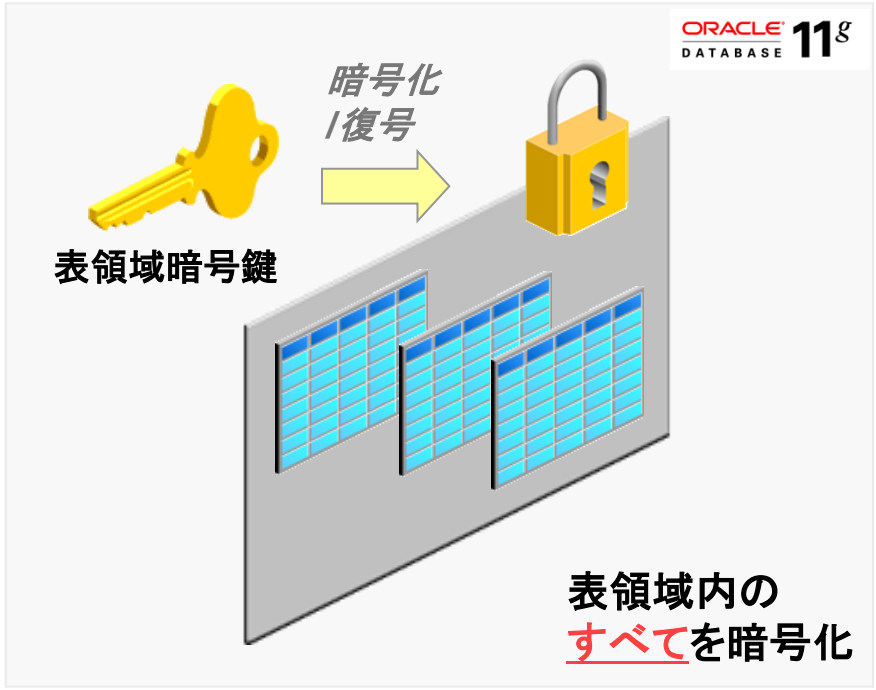
- アプリケーションからは透過的にデータの暗号化、復号を実行
  - 既存のアプリケーション（SQL）を改修する必要はない
- Oracle Wallet やHardware Security Moduleを利用した暗号鍵管理
- 強力な暗号アルゴリズムを利用した暗号化を実施
  - NISTの標準共通鍵暗号方式 AES(128/192/256bit) に対応



暗号化方式の種類

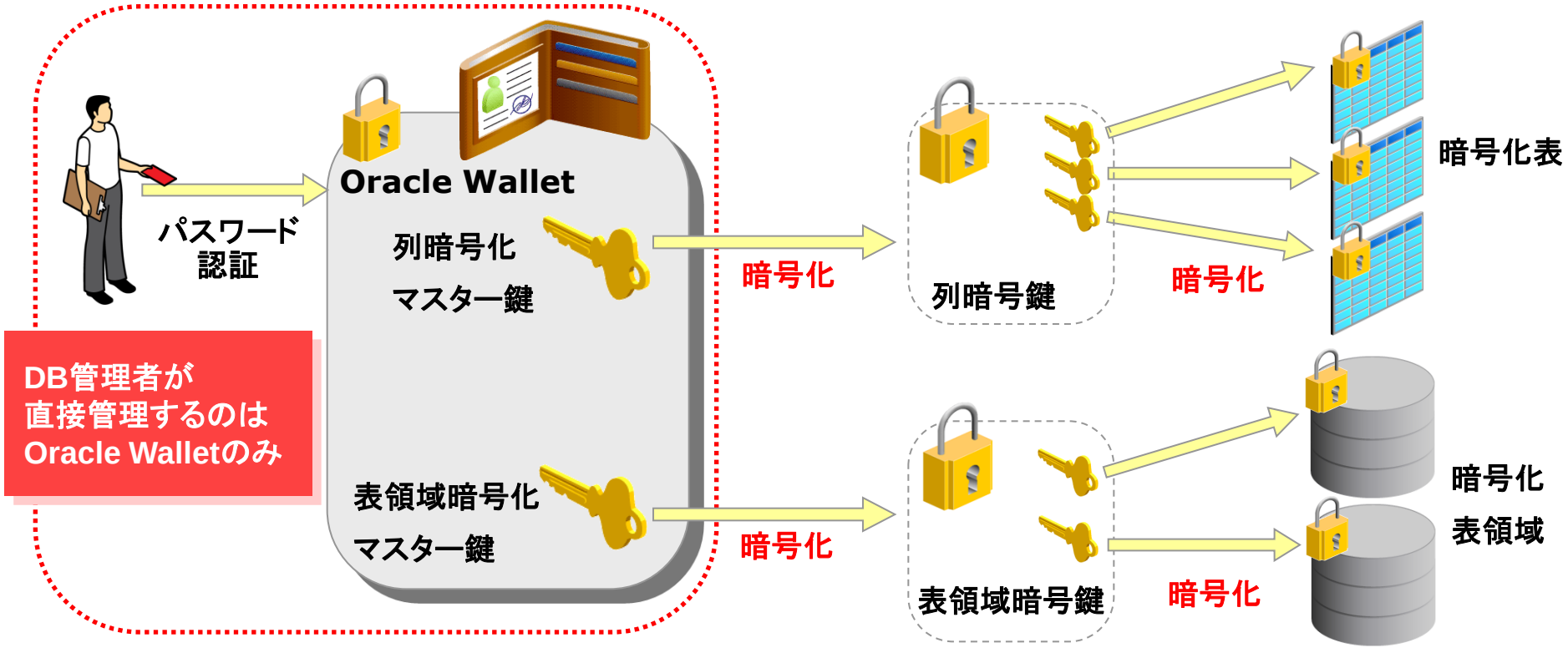
- 2種類の暗号化粒度
  - 列暗号化: 表の列ごとに暗号化を指定（10gR2～）
  - 表領域暗号化: 表領域内のすべてのデータを暗号化（11g～）





暗号鍵管理メカニズム

- TDEで利用される暗号鍵関連コンポーネント
  - Oracle Walletパスワード(1つ)
  - 列暗号化マスター鍵(1つ)、表領域暗号化マスター鍵(1つ)
  - 列暗号鍵(暗号化表ごとに1つ)、表領域暗号鍵(暗号化表領域ごとに1つ)



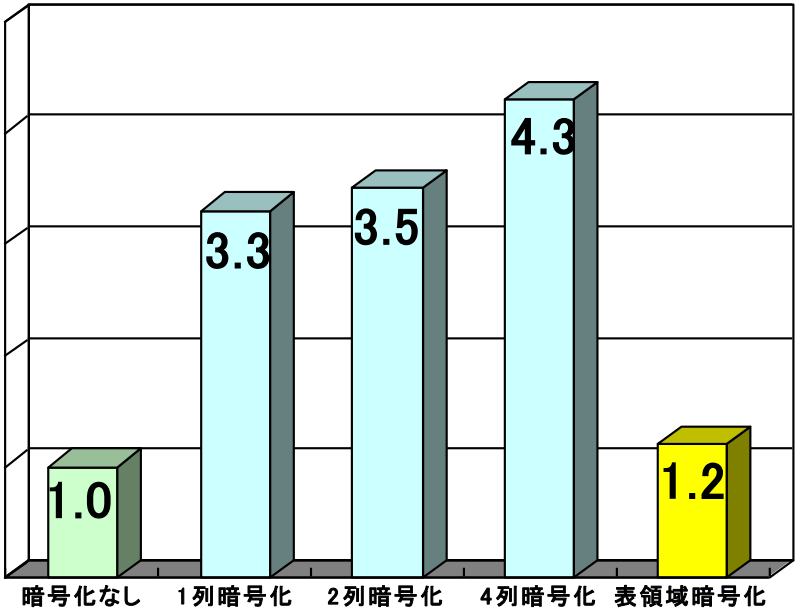
列暗号化、表領域暗号化の特徴

	列暗号化	表領域暗号化
暗号化のタイミング	行アクセス時	データ・ブロックに対するI/O発生時
暗号化アルゴリズム	3DES168, AES128 ,AES192 ,AES256	
暗号化により保護される場所	メモリ、ディスク	ディスク
データサイズ	暗号化対象データの量に比例して増加	暗号化前と変わらない
性能への影響	暗号化列へのアクセス頻度に応じて劣化	暗号化表領域のディスクI/O頻度に応じて劣化
対象オブジェクト	列のみ 暗号化列に対する索引は、B-Tree索引の一意検索のみ可能	表領域内のすべてのオブジェクト BITMAP索引の作成やB-Tree索引の範囲検索も利用可能

許容できるセキュリティ・レベルと可用性のバランスに応じて選択

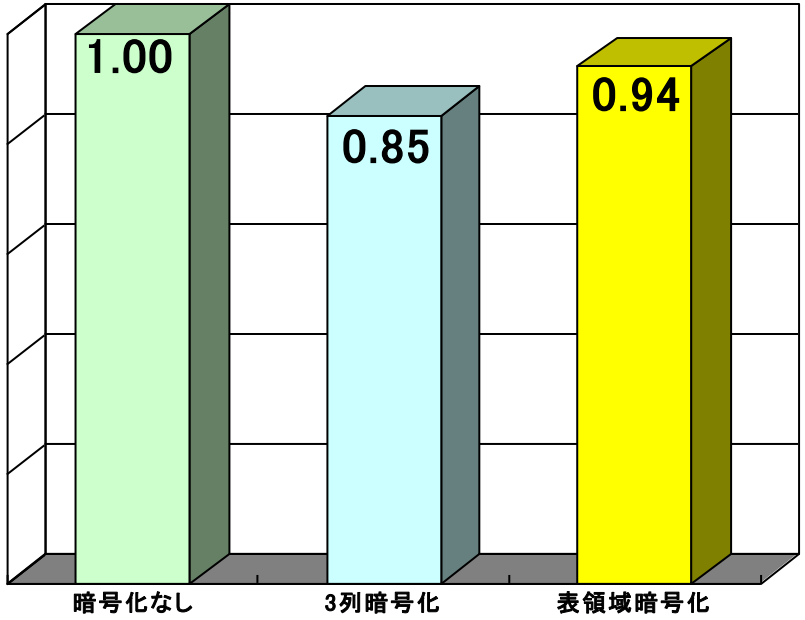
性能面への影響

- 列暗号化は暗号列数が増えるごとに処理時間に影響
- 列暗号化と比較して、表領域暗号化はバッチ処理、OLTP処理ともに性能への影響が小さい



バッチ処理に関する処理時間の比較

INSERT文を数十万回実行する処理を実行し、暗号化なしの場合を1としたときの相対処理時間を、列暗号化（1,2,4列）、表領域暗号化の場合でそれぞれ記載



OLTP処理に関するスループットの比較

TPC-Cベンチマークを実行し、暗号化なしの場合を1としたときの相対スループットを、列暗号化、表領域暗号化の場合でそれぞれ記載

さらに高速な暗号化を実現

- AES-NI（Advanced Encryption Standard New Instructions）
  - Intel® Xeon® プロセッサー 5600 番台から搭載された新しい命令セット
  - 暗号化/復号処理をプロセッサー側で高速処理するアクセラレーション機能
  - Oracle Databaseと組み合わせた高速な暗号処理を実現

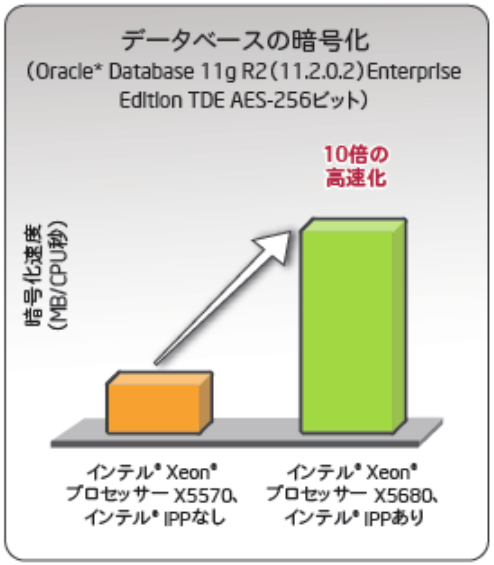
インテル® Xeon® プロセッサー X5680

- Oracle Database 11g R2 (11.2.0.2) Enterprise Edition
- TDE AES-256ビット 表領域暗号化

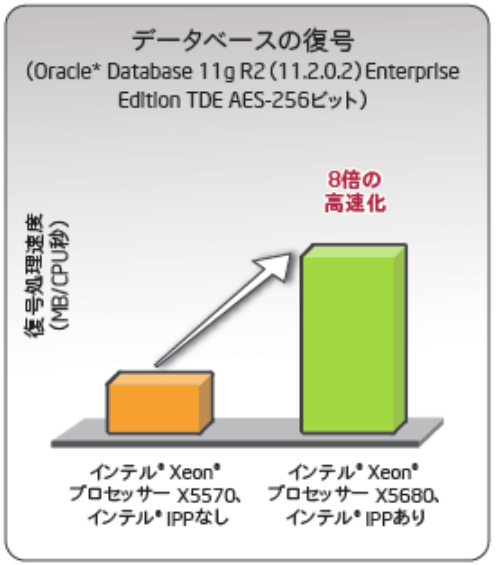
テストケース

- 100万行を空のテーブルにINSERT処理(30回)
- 510万行をテーブルからSELECT処理

暗号化 10倍高速



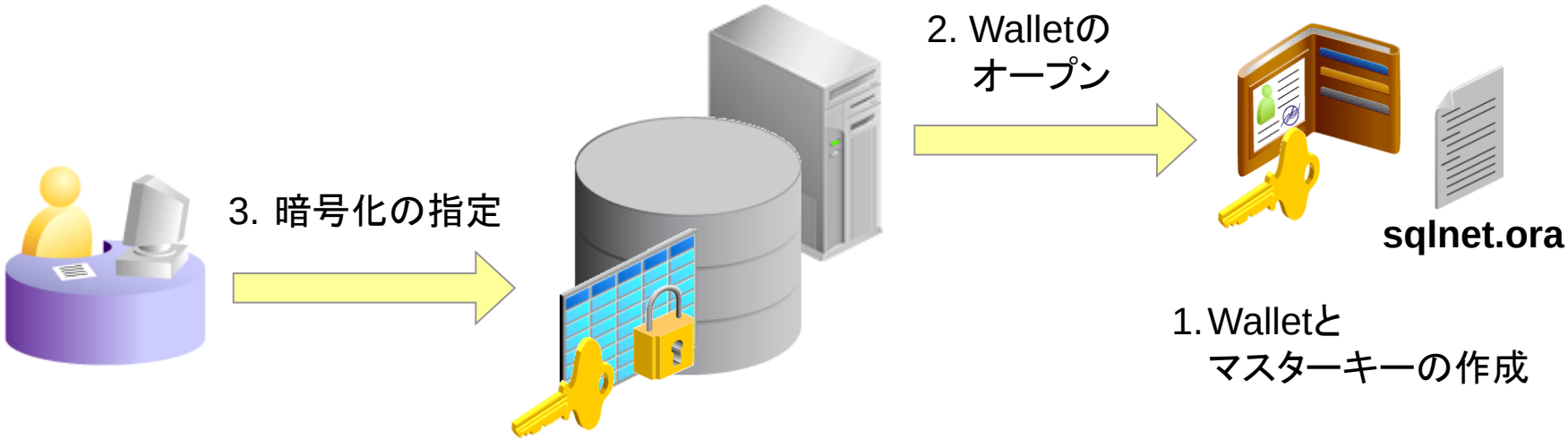
復号 8倍高速



Intel White papersより引用: http://download.intel.com/jp/business/japan/pdf/323587-001JA.pdf

格納データの暗号化 - 設定例 -

1. Oracle Walletを作成し、マスターキーを格納
   - sqlnet.ora にWalletのロケーションを記述
   - SQL*Plusから、SYSユーザーでマスターキーを作成
2. Walletをオープン（インスタンス起動毎に一度）
3. データベースで列暗号化または表領域暗号化を指定



格納データの暗号化 - 設定例 -

1. Oracle Walletを作成し、マスターキーを格納
   - sqlnet.oraにWallet のロケーションを記述

```
ENCRYPTION_WALLET_LOCATION =
 (SOURCE = (METHOD = FILE)
           (METHOD_DATA = (DIRECTORY = D:¥oracle¥WALLET)))
```

   - SQL*Plusから、SYSユーザーでマスターキーを作成

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

Wallet パスワードを定義

2. Oracle Walletをオープン

```
SQL> ALTER SYSTEM SET ENCRYPTION WALLET OPEN
     IDENTIFIED BY "password";
```

格納データの暗号化 - 設定例 -

3-a. 表の作成時に列暗号化を指定

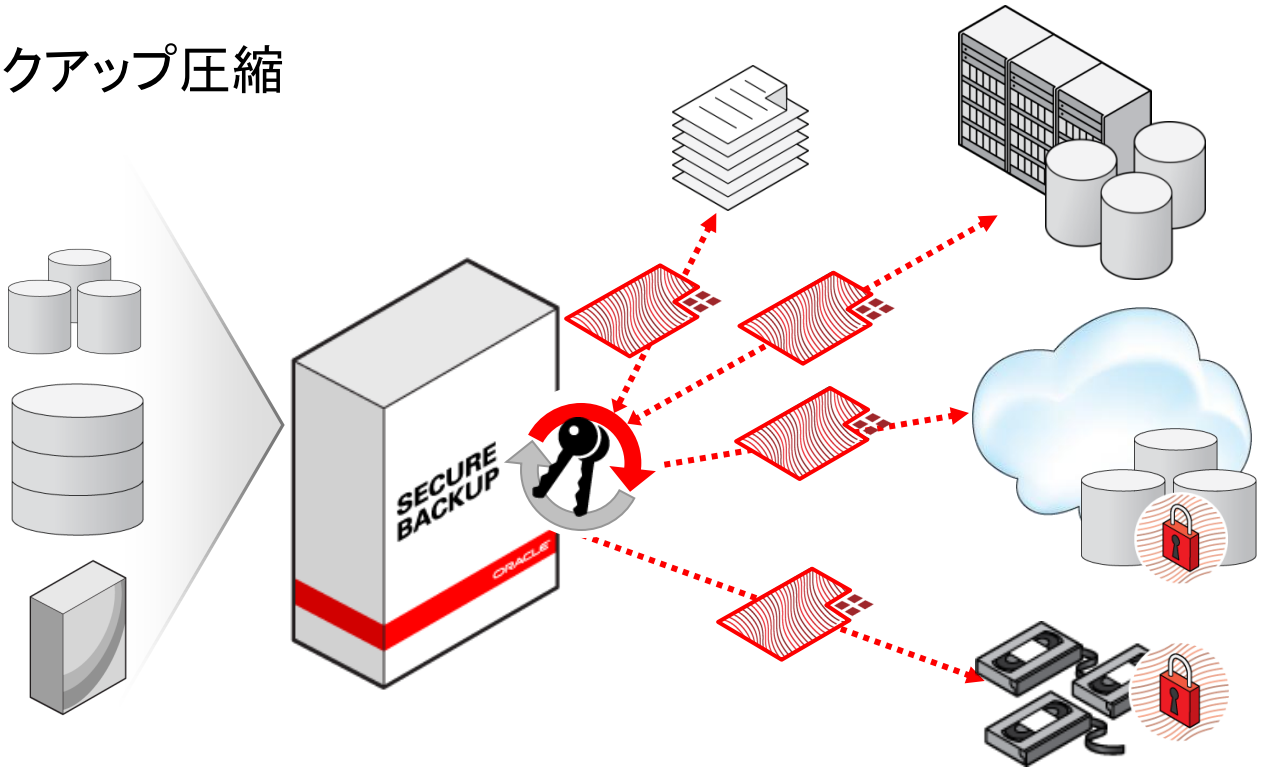
```
CREATE TABLE credit (
  name       VARCHAR2(20),
  cardnumber VARCHAR2(16) ENCRYPT
                          USING 'AES256' SALT );
```

3-b. 表領域の作成時に暗号化を指定

```
CREATE TABLESPACE securespace
DATAFILE '/u02/oradata/orcl/secure01.dbf' SIZE 100M
ENCRYPTION USING 'AES256'
DEFAULT STORAGE (ENCRYPT);
```

バックアップデータの暗号化

- 暗号化対象となるバックアップデータ
  - ダンプファイル (Data Pump)
  - ディスク (Recover Manager)
  - テープ
- 高速なバックアップ圧縮



Oracle Databaseの監査機能

	①必須監査(オペレーティング・システム監査)	②DBA監査	③標準監査（任意監査）	④ファイングレイン監査（任意監査）
対象となるEdition	全エディション	全エディション	全エディション	ORACLE DATABASE ENTERPRISE EDITION
対象バージョン	-	9i CLUSTER / ORACLE DATABASE 10g / ORACLE DATABASE 11g	9i CLUSTER / ORACLE DATABASE 10g / ORACLE DATABASE 11g	9i CLUSTER / ORACLE DATABASE 10g / ORACLE DATABASE 11g
監査対象	・インスタンス起動 ・インスタンス停止 ・管理者権限によるデータベース接続	・データベース管理者としてログインしたユーザーのデータベース操作	・データベースへの操作（ログイン、CREATE/ALTER/DROPなどのアクション、UPDATE、DELETEなどのオブジェクトへの操作）	・特定のデータ（列名、条件指定可能）へのアクセス（SELECT） ・Oracle10gからはUPDATE、DELETE、INSERTへも可能
監査証跡出力先	・OSファイル	・OSﾌｧｲﾙ / ｼｽﾃﾑﾋﾞｭｰｱ(Win) ・Syslog(10gR2～) ・XMLファイル(10gR2～)	・DBA_AUDIT_TRAILビュー ・OSﾌｧｲﾙ / ｼｽﾃﾑﾋﾞｭｰｱ(Win) ・Syslog(10gR2～) ・XMLファイル(10gR2～)	・DBA_FGA_AUDIT_TRAILビュー ・ユーザー定義表 ・メール送信も可能 ・XMLファイル(10gR2～)
取得可能な監査証跡	・OSによって生成された監査レコード ・データベース監査証跡レコード ・常に監査されるデータベース関連のアクション ・管理ユーザー（SYS）用の監査レコード	・時刻 ・操作(SQL文全体) ・データベースユーザー名/権限 ・OSユーザー名/端末 ・終了コード	・時刻 ・操作(SQL文の種類) ・データベースユーザー名/権限 ・OSユーザー名/端末 ・終了コード	・時刻 ・データベースユーザー ・OSユーザー名/端末 ・アクセスしたオブジェクト名 ・ファイングレイン監査ポリシー名 ・操作(SQL文全体) ・ユーザー定義アクション(オプション)

データベースにおけるログの種類

- 特権ユーザ、管理者用ユーザのログ
  - 特権ユーザ(SYSDBA, SYSOPER)での操作履歴
  - 管理者用ユーザ(DBAロールなどの高い権限を付与されているユーザ)の操作履歴

基本的にはすべてのログを取得する必要がある

- 一般ユーザのログ
  - アプリケーション(WEB,C/S等のシステム)内で使用されている自動化された(構文化された)操作履歴
  - 開発者・運用者が、SQL*PLUSや開発ツールなどから使用する自動化されていない(自由にSQLを作成できる)操作履歴

ログの95%以上は、アプリケーションからのログ!!
本当に意味のあるのは、残り5%のアプリケーションを経由しないログ

特権ユーザのログ

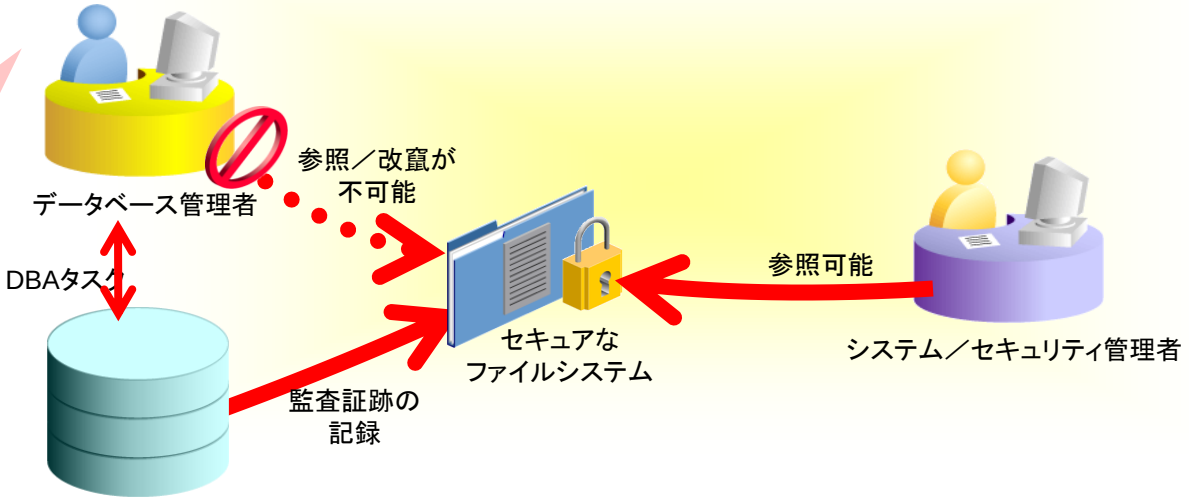
特権ユーザ = DBA(データベース管理者)

Oracle DatabaseのDBA監査は、特権ユーザであるSYSやSYSDBAで行われた全ての操作を記録
設定方法は、初期化パラメータファイル「AUDIT_SYS_OPERATIONS」をTRUEに

監査対象	DBA監査
	• SYS/SYSDBA/SYSOPER権限で行われた全ての操作 • 監査証跡は必ずOS上に記録され、データベース内には記録されない • Unixの場合は、AUDIT_FILE_DEST の示すファイル・システム上のディレクトリ • Windowsの場合はイベントビューアに記録

ポイント:監査証跡の保護

DBA権限をもつユーザーは、Oracleが残した監査証跡を参照／改竄することが出来ない



特権ユーザログの例

■行った操作

```
SQL> CONNECT / AS SYSDBA
接続されました。
SQL>
SQL> -- 行の挿入
SQL> INSERT INTO scott.testtab
  2  VALUES ( 1 );

1行が作成されました。
SQL> COMMIT;
コミットが完了しました。

SQL> -- データの参照
SQL> SELECT COUNT(*)
  2  FROM scott.testtab;

  COUNT(*)
----------
         5
SQL>
```

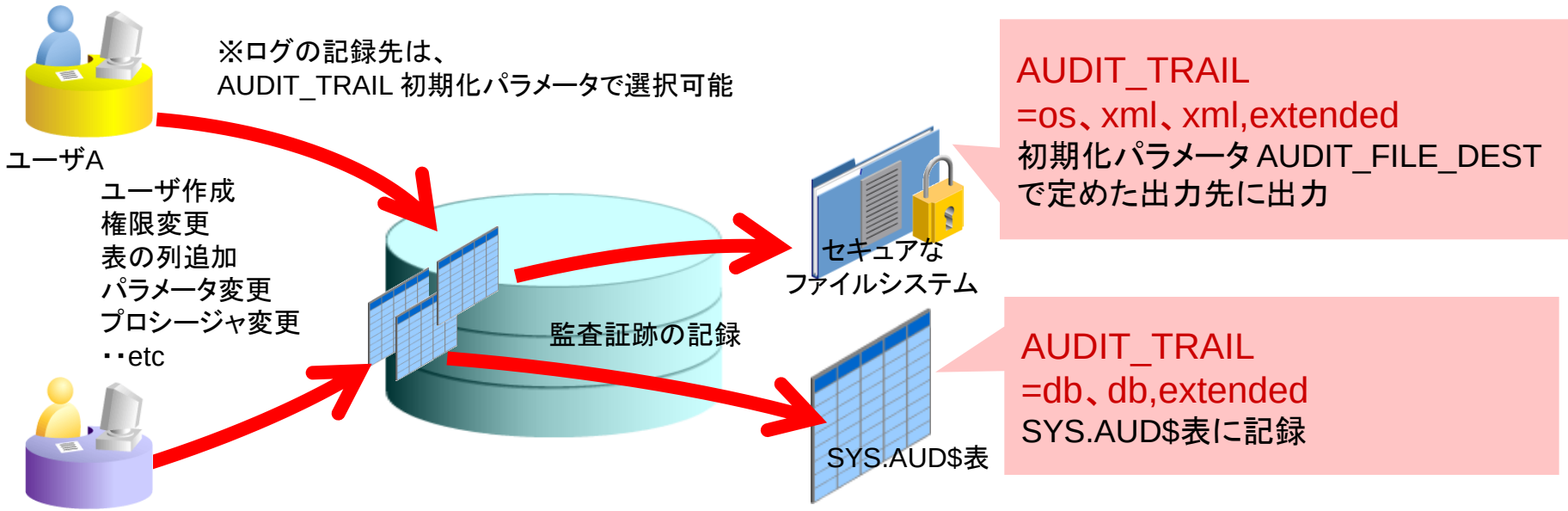
■記録された監査証跡

```
Fri Mar 25 23:08:20 2005
ACTION : 'CONNECT'
DATABASE USER: '/'
PRIVILEGE : SYSDBA
CLIENT USER: oracle
CLIENT TERMINAL: pts/3
STATUS: 0

Fri Mar 25 23:08:20 2005
ACTION : 'insert into scott.testtab values ( 1 )'
DATABASE USER: '/'
PRIVILEGE : SYSDBA
CLIENT USER: oracle
CLIENT TERMINAL: pts/3
STATUS: 0

Fri Mar 25 23:08:20 2005
ACTION : 'commit'
DATABASE USER: '/'
PRIVILEGE : SYSDBA
CLIENT USER: oracle
CLIENT TERMINAL: pts/3
STATUS: 0

Fri Mar 25 23:08:20 2005
ACTION : 'select count(*) from scott.testtab'
DATABASE USER: '/'
PRIVILEGE : SYSDBA
CLIENT USER: oracle
CLIENT TERMINAL: pts/3
STATUS: 0
```

管理者用ユーザのログ

管理者用ログ = データベースの構成に関わるログ

Oracle Databaseの標準監査(文・権限監査)は、ユーザ作成や権限付与、表やプロシージャ等のオブジェクトの変更など、運用や保守で行われた全ての操作が記録される



- 処理が監査条件に合致した場合、処理を行ったユーザーの詳細情報やタイムスタンプ、SQL文などがAUDIT_TRAILパラメータに応じて、OS形式、XML形式、SYS.AUD$表で記録される
- AUD$表 とXMLファイルの内容は、DBA_COMMON_AUDIT_TRAIL ビューにより一括で確認可能

管理者用ユーザ ログの対象項目

- 権限監査(34種類)

ALTER ANY PROCEDURE ALTER PROCEDURE	CREATE ANY LIBRARY CREATE LIBRARY	DROP ANY TABLE DROP TABLE
ALTER ANY TABLE ALTER TABLE	CREATE ANY PROCEDURE CREATE PROCEDURE	DROP PROFILE
ALTER DATABASE	CREATE ANY TABLE CREATE TABLE	DROP USER
ALTER PROFILE	CREATE EXTERNAL JOB	EXEMPT ACCESS POLICY
ALTER SYSTEM	CREATE PUBLIC DATABASE LINK	GRANT ANY OBJECT PRIVILEGE GRANT OBJECT PRIVILEGE
ALTER USER	CREATE SESSION	GRANT ANY PRIVILEGE GRANT PRIVILEGE
AUDIT SYSTEM	CREATE USER	GRANT ANY ROLE GRANT ROLE
CREATE ANY JOB CREATE JOB	DROP ANY PROCEDURE DROP PROCEDURE	

- 文監査(6種類)

ROLE	SYSTEM AUDIT	PUBLIC SYNONYM
DATABASE LINK	PROFILE	SYSTEM GRANT

- 追加

EXECUTE ON SYS.DBMS_DATAPUMP	EXECUTE ON SYS. DBMS_SCHEDULER	(必要に応じて左記以外のパッケージも 監査対象に追加)

管理者用ユーザ ログの取得例

■ 基本形

```
AUDIT  対象とする権限/文 BY ACCESS;
```

■ 権限監査

AUDIT GRANT ANY PRIVILEGE BY ACCESS;　← 権限付与に関しての操作をすべて記録

```
OS_USERNAME     USERNAME        USERHOST        TERMINAL    TIMESTAMP          OWNER
--------------- --------------- --------------- ----------- ------------------ ----------
security        SAKURA          jpsun1444       pts/2       20050502 15:40:52  SAKURA

OBJ_NAME        ACTION_NAME           GRANTEE         OS_PROCESS
--------------- --------------------- --------------- ------------
EMP             GRANT OBJECT           IZUMI           6712
```

■ 文監査

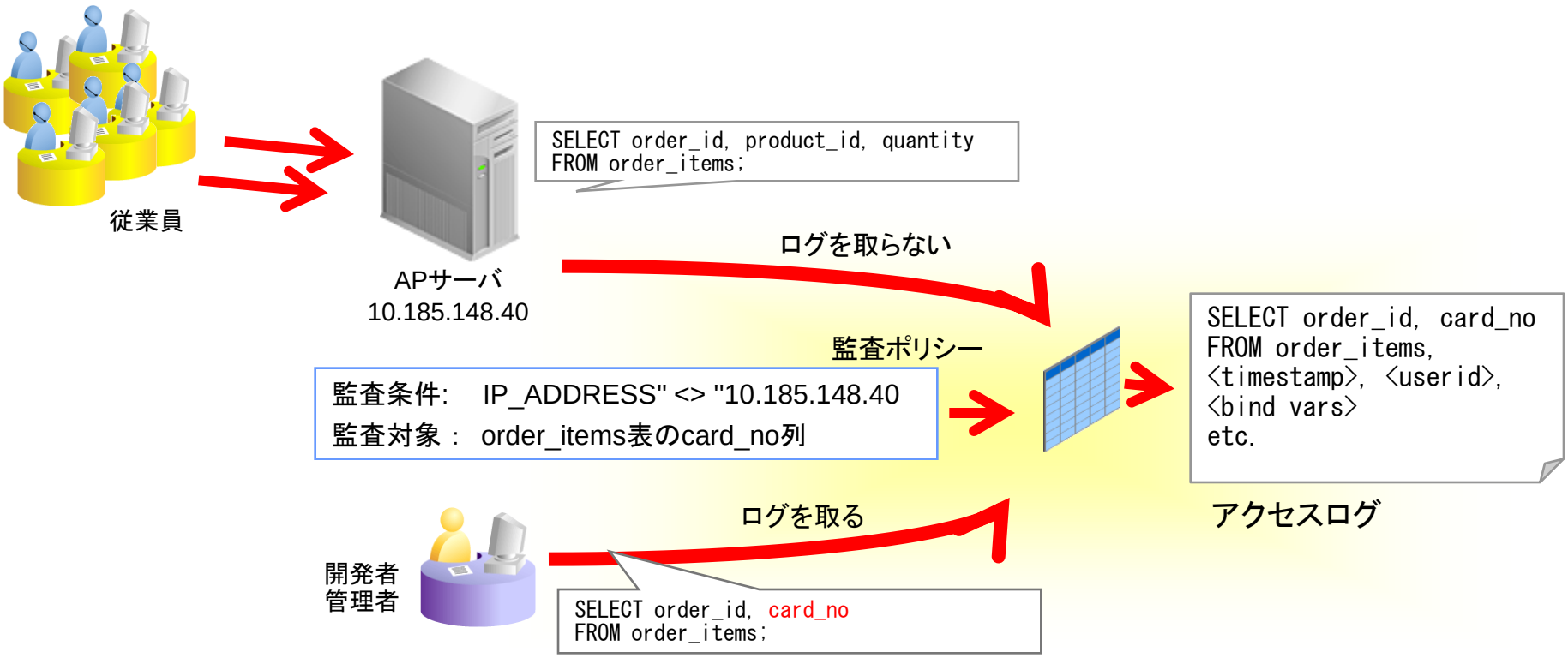
AUDIT GRANT ROLE BY ACCESS;　← SQL文でROLEが含まれている場合はすべて記録

```
OS_USERNAME     USERNAME        USERHOST        TERMINAL    TIMESTAMP          OWNER
--------------- --------------- --------------- ----------- ------------------ ----------
security        HR              jpsun1444       pts/2       20070702 21:22:52

OBJ_NAME        ACTION_NAME           GRANTEE         OS_PROCESS
--------------- --------------------- --------------- ------------
APP_ROLE        CREATE ROLE                            32586
```

一般ユーザのログの絞り込み

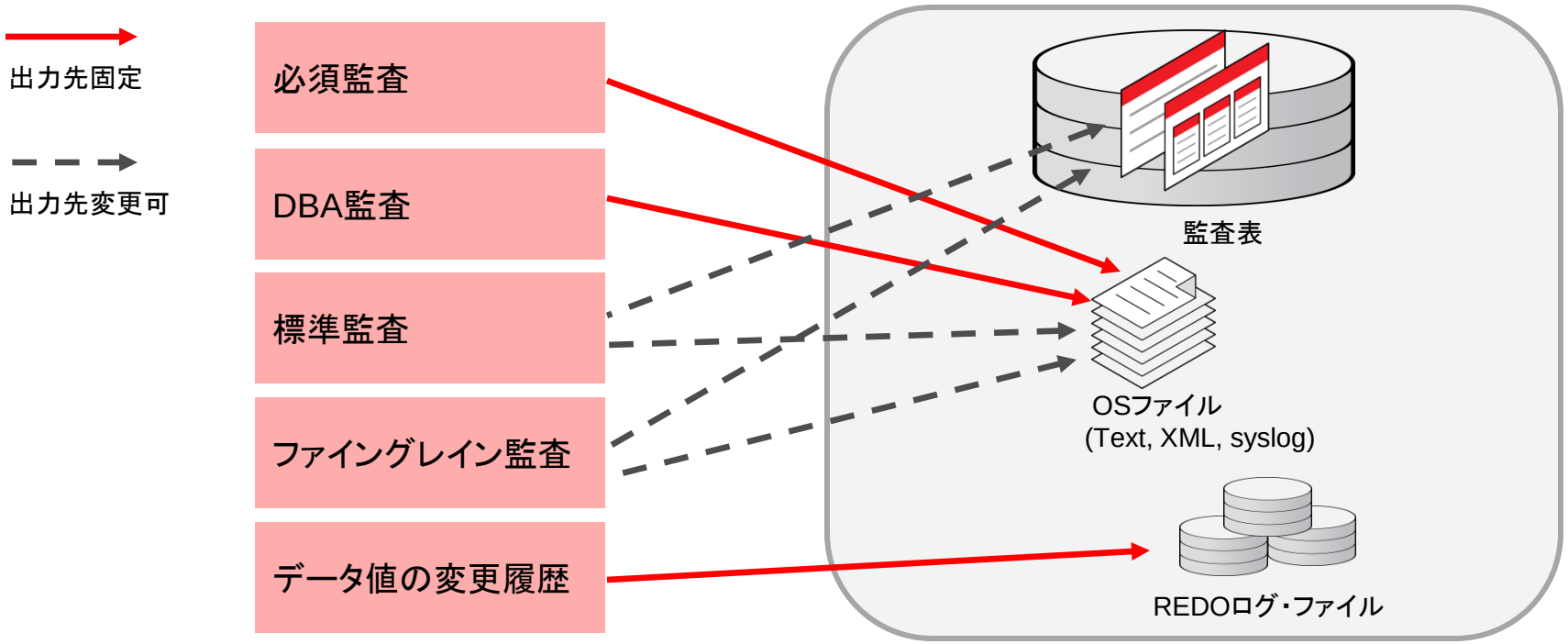
ファイングレイン監査:

・特定の列や行にSELECTやUPDATEなどのDML文を発行された場合や、業務時間外や定められたホスト以外からDML文が発行された場合など、オブジェクトへのアクセスログの取得ルールをきめ細かく指定することができる



監査ログの記録先

- 監査ログ関連のパラメータ
  - DBA監査　audit_sys_operations =　True / False
  - 標準監査　audit_trail = OS /　XML / XML_EXTENDED / DB / DB_EXTENDED
  - 出力先　　audit_file_dest = パス名
- 標準監査とファイングレイン監査ログは、DBA_COMMON_AUDIT_TRAILビューを通じてSQLでアクセスすることが可能（ audit_trail = OSの場合は不可)



取得できるログ項目と出力形式

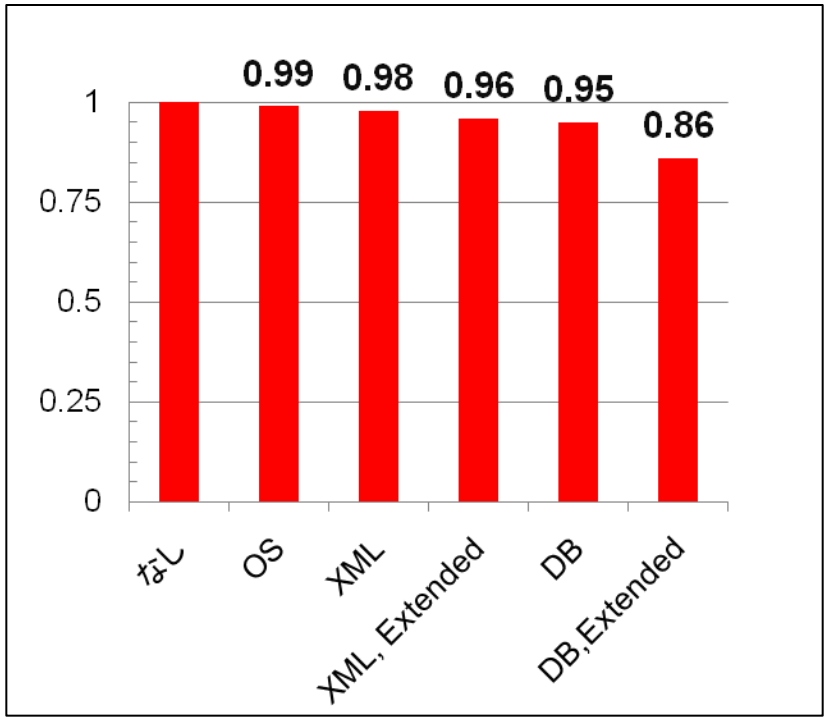
- どの監査設定でもログとして必要な要件は満たしている
- 実行されたSQL文まで特定する必要がある場合には、Extendedを指定

5W1H	項目	出力先				
		OS	XML	XML, Extended	DB	DB, Extended
	出力先	テキスト ファイル	XML ファイル	XML ファイル	DB (AUD$)	DB (AUD$)
いつ	タイムスタンプ	○	○	○	○	○
だれが	DBユーザ名	○	○	○	○	○
どこで	ホスト名 / IPアドレス	○	○	○	○	○
何を	アクセスしたオブジェクト名	○	○	○	○	○
どのように	アクセス種類 (DML)	○	○	○	○	○
どうした	アクセス内容 (SQL TEXT, バインド変数)			○		○

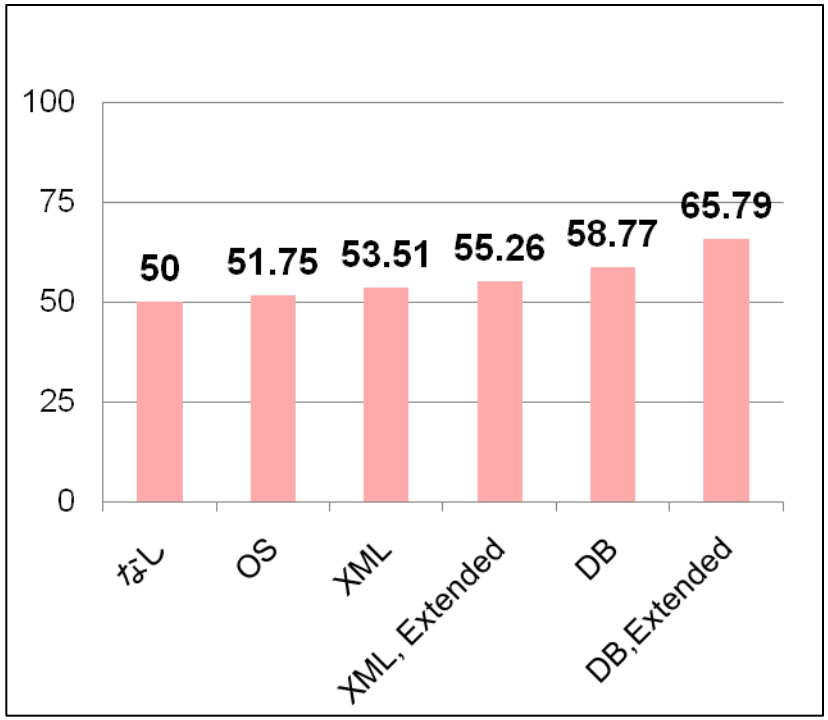
出力形式ごとのオーバーヘッド

- HW: CPU (4x3.40 GHz Xeon), 4GB, X86_64/Linux
- SW: Oracle Database 11.2.0.1
- 上記の環境で、TPC-Cモデルのアプリケーションでトランザクションを発生
  監査レコードは、250レコード/秒で生成

■ 監査なしを1とした場合の相対スループット



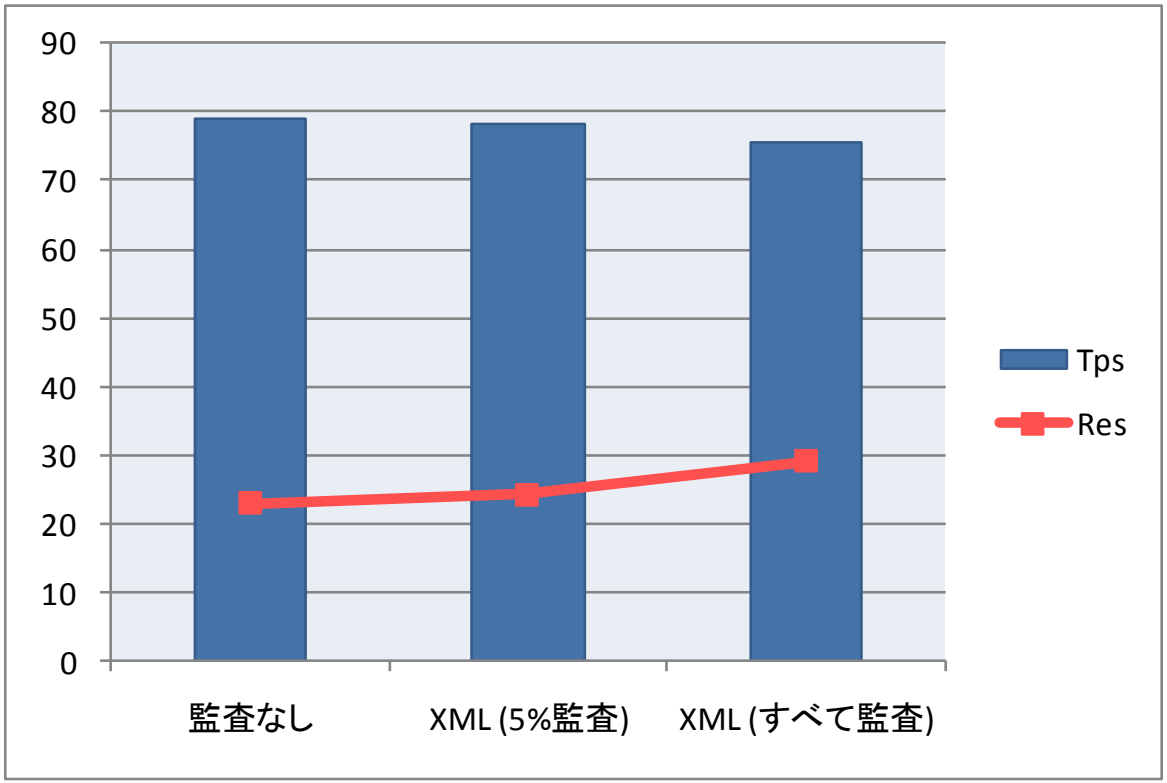
■ 監査なしをCPU 50%とした場合のCPU使用率



http://www-content.oracle.com/technetwork/jp/database/audit-vault/learnmore/twp-security-auditperformance-328826-ja.pdf

ログ絞り込みによる性能への影響

- HW: CPU (2 x 3.16 GHz Xeon quad-core), 8GB, X86_64/Linux
- SW: Oracle Database 11.2.0.2
- オンライン・ショッピング・サイトの処理に類似したアプリケーションを使用し、
  トランザクションをすべて監査と5%のみ監査した場合のTPSとレスポンスタイムを計測



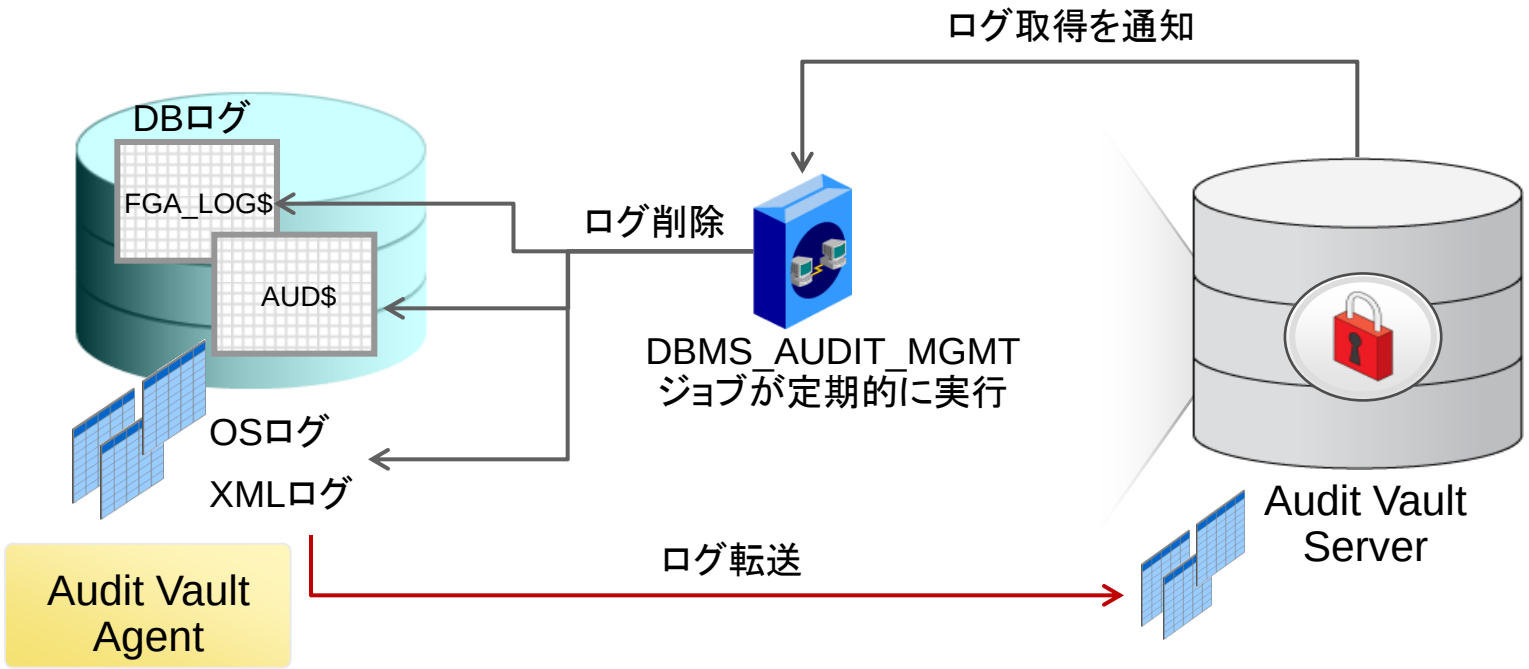
5%監査は、限りなくゼロ

**すべて監査した場合でも
性能への影響は5%以下**

ログメンテナンスの自動化

DBMS_AUDIT_MGMT(ログ管理パッケージ):

・タイムスタンプを使用した定期的なログの削除が可能 (11gR2からは単体で使用可能)
・ Audit Vaultと組み合わせることで、ログをAudit Valtに送信後、送信済を削除するジョブとして使用
・ ログを一元的に集約し保全

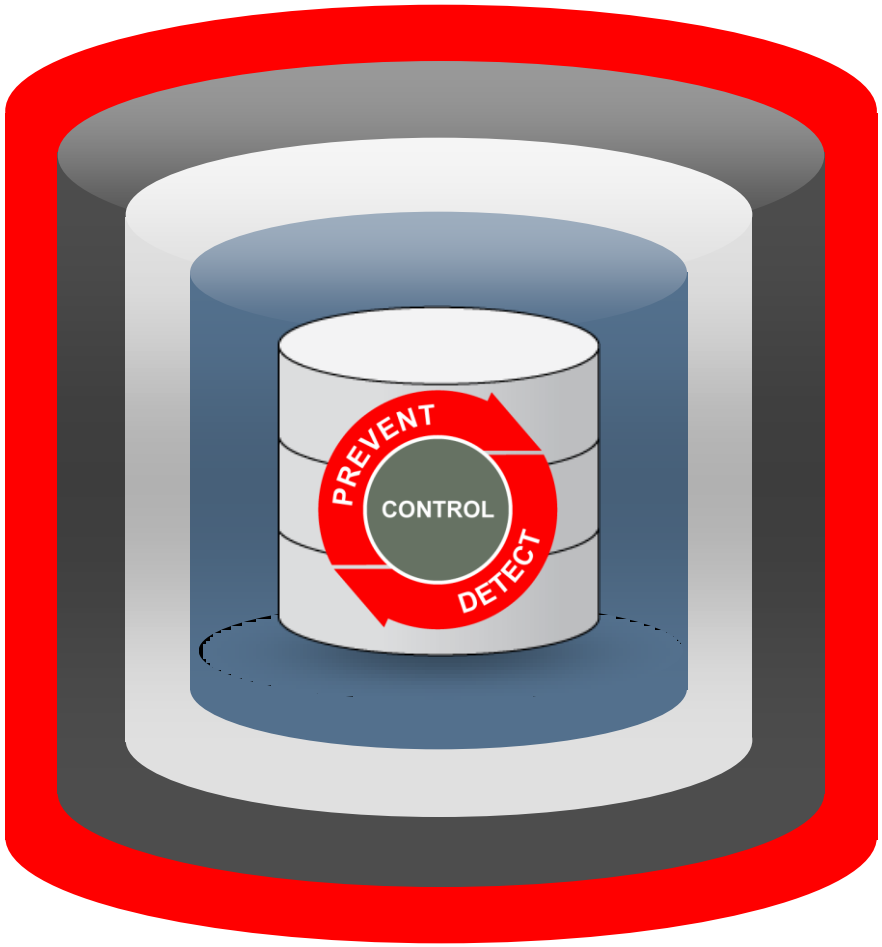


性能への影響を極小化するために

- **ログの出力形式は、OS、XMLのファイル出力にする**
  - ログのファイル出力が性能への影響が最も低い
  - XMLは10gR2以上、OSはすべてのバージョンで使用可能
  - 一般ユーザのログは特権ログや管理者用ユーザログと比較しても総量が多く肥大化する傾向があるため定期的な退避・削除のメンテナンスが必要

- **ログを取得する人・場所・オブジェクトを絞る**
  - すべてのログを取ることに意味はない
  - 自動化(アプリケーションを経由したアクセス等)のログは取らず、非自動化(SQL*PLUSや開発ツール経由でのアクセス等)のログだけを限定して取るなどの取捨選択が必要
  - 個人情報、決済情報、企業秘密情報など、機密性の高い表やビューがアクセスされた場合のみログを取る

Database Layerにおける多層防御



暗号化 & マスキング

- 暗号化 (Advanced Security)
- バックアップの暗号化 (Secure Backup)
- データ・マスキング

アクセス制御

- 行・列レベルアクセス制御
  （Virtual Private Database)
- 特権ユーザ管理、職務分掌
  （Database Vault)

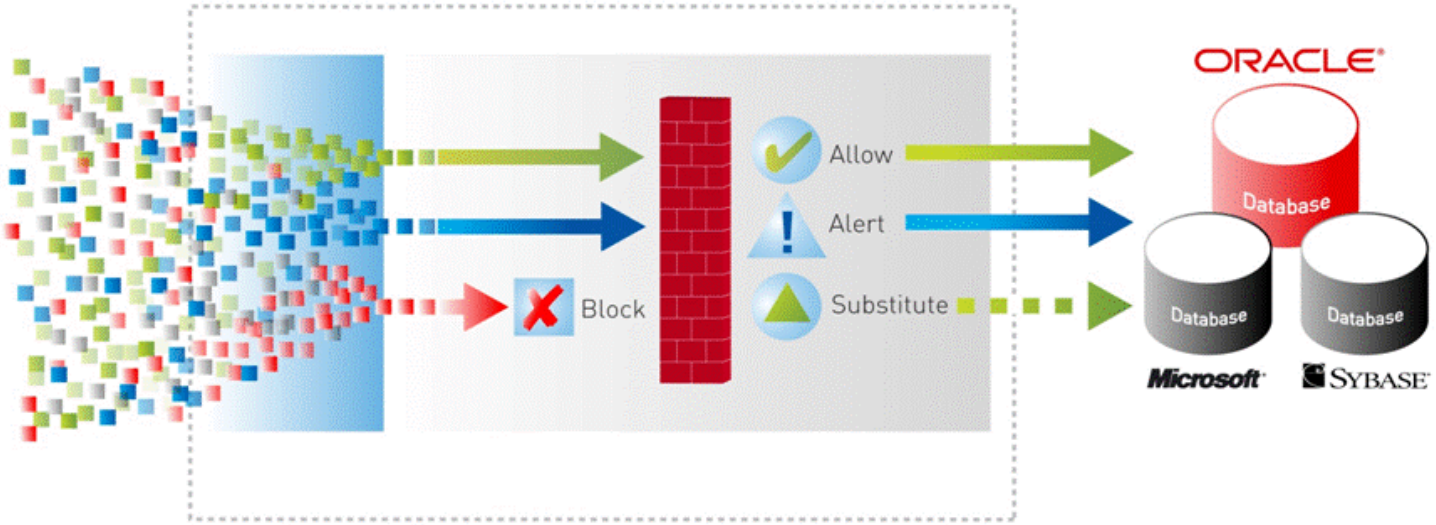
監査

- 標準監査/DBA監査
- ファイングレイン監査
- 構成管理 (Configuration Management)
- 変更管理 (Change Management)
- 監査ログ管理・分析 (Audit Vault)

モニタリング & ブロッキング

- Oracle Database Firewall

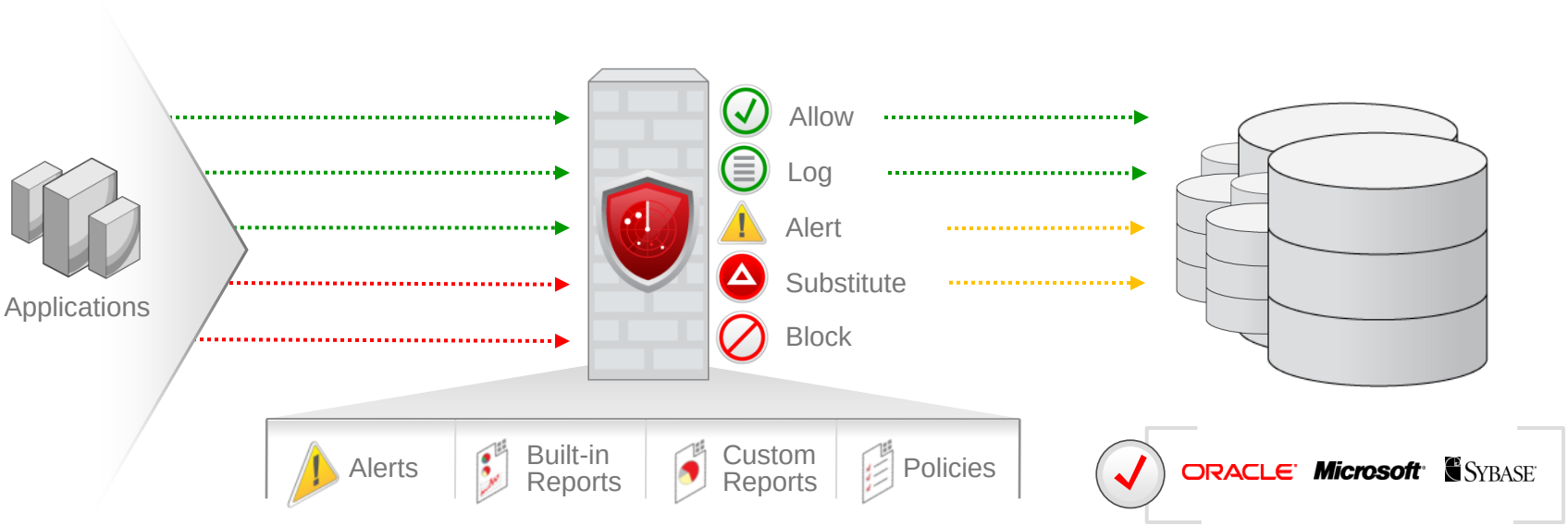
Oracle Database Firewall



- アプリケーションとデータベースの中間に位置し、ネットワーク上からSQL文を収集・解析する。
  - モニタリング：収集したSQL情報をログとして記録・管理・レポーティングを行う（監査ツールの用途として使用）
  - 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または警告することで、内部不正・外部攻撃からデータベースを保護する

Oracle Database Firewall

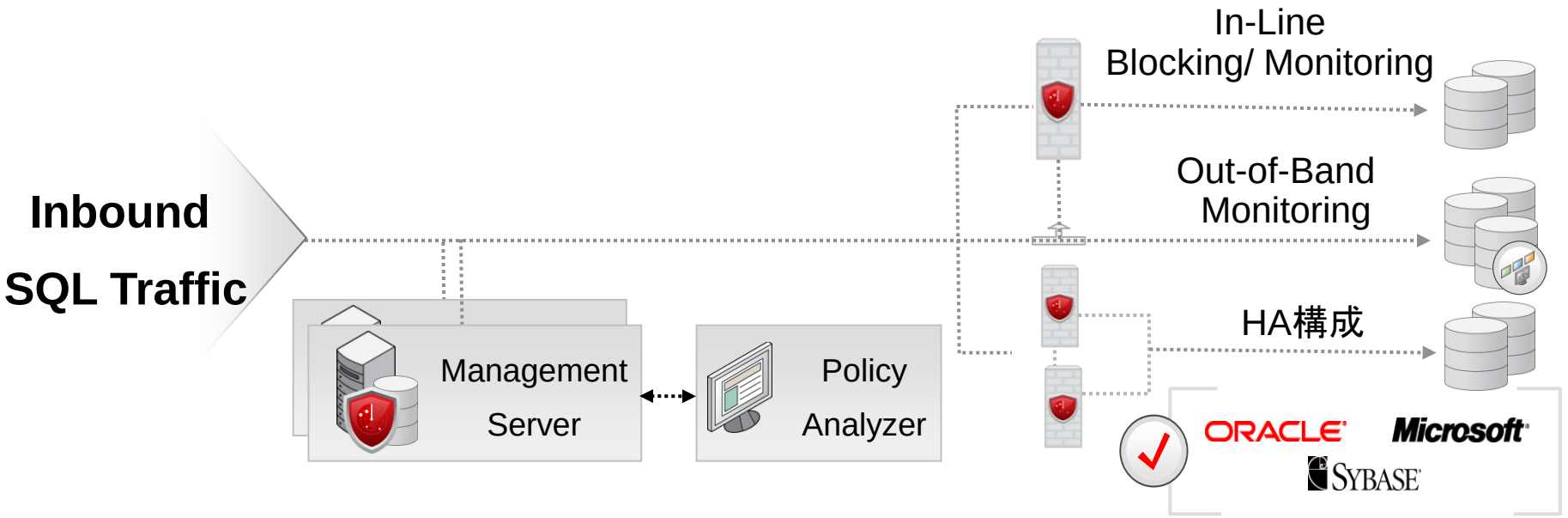
防御のファースト・ライン



- **透過的**
  - 動作しているアプリケーション及びデータベースの変更を必要としない
- **高いパフォーマンス**
  - アプリケーション・データベース間のトランザクション処理への影響はごくわずか
- **正確な検知**
  - 高精度なSQL文法レベルの解析により、誤検知なく不正なSQLのみブロック

Oracle Database Firewall

アーキテクチャ



- モニタリングのみの場合は、スイッチのSPAN Portを使用したOut of Band構成
- ブロッキングの場合は、アプリケーション - データベース間にIn-Lineに配置
- H/A構成に対応
- サポートされるデータベースは、
  Oracle Database 8i～11g、SQL Server 2000・2005・2008、IBM DB2 for LUW 9.x、
  Sybase ASE 、SQL Anywhere

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。

twitter

最新情報つぶやき中

oracletechnetjp

- 人気コンテンツは？
- お勧め情報
- 公開予告　など

OTN トップページ　http://www.oracle.com/technetwork/jp/index.html

ページ左「基本リンク」>「OTN セミナー　オンデマンド」

※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。

ORACLE

Oracle エンジニアのための技術情報サイト

オラクルエンジニア通信

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

twitter

最新情報つぶやき中

oracletechnetjp

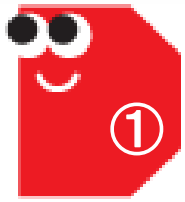
- 技術資料
  - ダイセミの過去資料や製品ホワイトペーパー、スキルアップ資料などを多様な方法で検索できます
  - キーワード検索、レベル別、カテゴリ別、製品・機能別
- コラム
  - オラクル製品に関する技術コラムを毎週お届けします
  - 決してニッチではなく、誰もが明日から使える技術の「あ、そうだったんだ！」をお届けします

こんな資料が人気です

- ✓ 6か月ぶりに資料ダウンロードランキングの首位が交代！ 新王者はOracle Database構築資料でした。
- ✓ データベースの性能管理手法について、Statspack派もEnterprise Manager派も目からウロコの技術特集公開中

オラクルエンジニア通信

Oracle Databaseの価格ご存知ですか？



問題：

Oracle Databaseの最小構成はいくらでしょうか？

ヒント：

Oracle Standard Edition Oneを

5Named User Plus(指名ユーザ) というのが最小構成です。

問題：

Real Applications Clusters(RAC) Optionはいくらでしょうか？

ヒント：

RACはOracle Database Enterprise EditionのOptionです。

答えはこちら↓ ログイン不要の簡単見積もり

ライセンス見積もりヘルプ

検索

見積もり Start!

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.com/jp/direct/inquiry-form-182185-ja.html

※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）

ORACLE