Oracle Direct Seminar

ORACLE®

実践!! Oracleデータベースの監査

日本オラクル株式会社

Oracle Direct

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

Agenda

- Oracle Database監査機能
- ユーザ特定のポイント
- Oracleのセキュリティ・ソリューション
- Appendix
  - ログ監査の実践例
  - Oracle Audit Vault

Oracle Databaseの監査機能の種類

	必須監査	DBA監査	標準監査	ファイングレイン監査
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	
対象バージョン	-			
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） ・10g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
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)

Agenda

- Oracle Database監査機能
  - 必須監査
  - 標準監査
  - FGA監査
  - DBA監査
  - Log Miner
- ユーザ特定のポイント
- Oracleのセキュリティ・ソリューション
- Appendix
  - ログ監査の実践例
  - Oracle Audit Vault

必須監査とは

デフォルトで行われる、必要最低限の監査:

データベース管理者(DBA)による基本操作、およびリスナーを介したOracle Net Servicesによるインスタンスへの接続は、デフォルトで必ず監査される

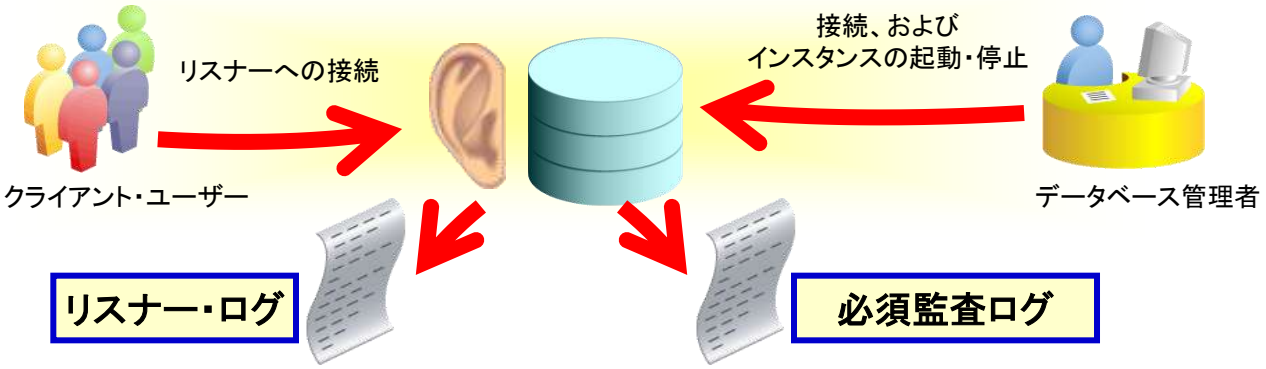
監査対象

OS監査 (必須監査)

- インスタンスの起動と停止
- 管理者ユーザー(SYSDBA/SYSOPER)によるインスタンスへの接続

リスナー・ログ

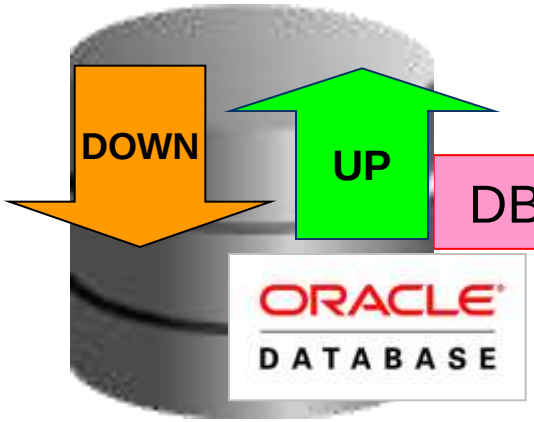
- リスナーに対する接続、および接続エラー
- インスタンスに接続後に発生するエラーは対象外(例:ログイン・エラー)
  ※"lsnrctl set log_status off" によってログが吐かれないようにすることも可能



必須監査（詳細）

監査対象	インスタンス起動/停止、管理者権限による接続 -- リスナー経由での接続
初期化パラメータの設定	不要
監査証跡出力先	監査証跡： ■AUDIT_TRAIL=os、db、db,extended、設定なし の場合 UNIX: ＜AUDIT_FILE_DEST 初期化パラメータで定めた出力先＞/ora_<pid>.aud Windows: イベント・ビューアのログファイル ■AUDIT_TRAIL=xml、xml,extended　のいずれかの場合 ＜AUDIT_FILE_DEST 初期化パラメータで定めた出力先＞/ora_<pid>.xml ※XMLでの出力は Oracle 10gR2 以降で可能 ※Windowsの場合、イベント・ビューアのログファイルにも出力される -- Listenerログ： $ORACLE_HOME/network/log/listener_<*リスナー名*>.log（デフォルト） もしくは listener.ora の LOG_DIRECTORY_<*リスナー名*> で定めた出力先
取得可能監査ログ	時刻、OS情報、DBインスタンス、アクション、行使したシステム権限、終了コード -- 時刻、プログラム、接続先ホスト名、終了コード
Audit 文の実施	不要
解除方法	必須なので解除はできない

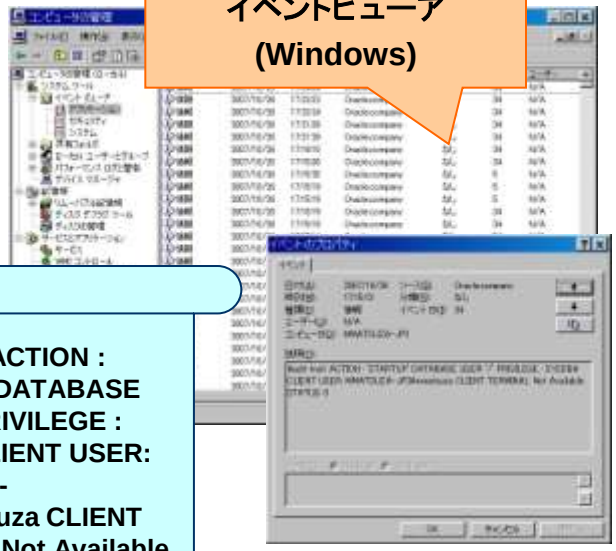
必須監査のログ出力



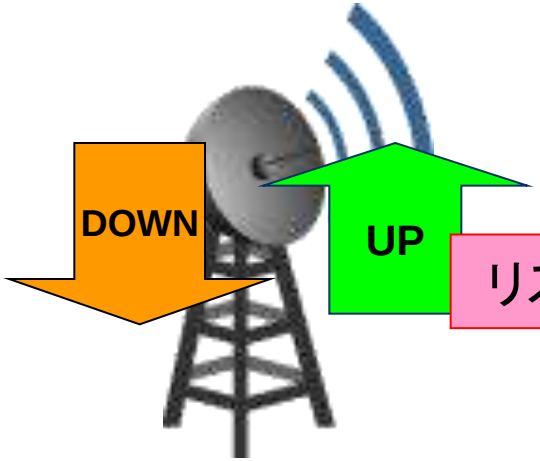
DBの起動停止

OS上のログファイル

イベントビューア
(Windows)



Audit trail: ACTION : 'STARTUP' DATABASE USER: '/' PRIVILEGE : SYSDBA CLIENT USER: MMATSUZA-JP2¥mmatsuza CLIENT TERMINAL: Not Available STATUS: 0 .



リスナーの起動停止

OS上のログファイル

26-10月-2008 11:00:58 * (CONNECT_DATA=(SID=company)(CID=(PROGRAM=D:¥oracle¥product¥10.2.0¥db_1¥bin¥emagent.exe)(HOST=MMATSUZA-JP2)(USER=SYSTEM))) * (ADDRESS=(PROTOCOL=tcp)(HOST=146.56.34.194)(PORT=3924)) * establish * company * 0

必須監査のログの例

■監査証跡の内容

```
Audit file /opt/oracle/rdbms/audit/ora_10324.aud
Oracle Database 10g Enterprise Edition Release 10.1.0.4.0 - Production
With the Partitioning, Real Application Clusters and Data Mining options
ORACLE_HOME = /opt/oracle
System name:    Linux
Node name:      mylinuxbox
Release:        2.4.21-27.0.2.EL
Version:        #1 Wed Jan 12 23:46:37 EST 2005
Machine:        i686
Instance name: orcl1
Redo thread mounted by this instance: 1
Oracle process number: 20
Unix process pid: 10324, image: oracle@mylinuxb      (TNS V1-V3)

Mon May  2 20:42:17 2005
ACTION : 'CONNECT'
DATABASE USER: '/'
PRIVILEGE : SYSDBA
CLIENT USER: amorimur
CLIENT TERMINAL:
STATUS: 0
```

アクション

試行／実行されたアクション
（AUDIT_ACTIONS表に一覧あり）

システム権限

処理に使われたシステム権限
（SYSTEM_PRIVILEGE_MAP 表に一覧あり）

終了コード

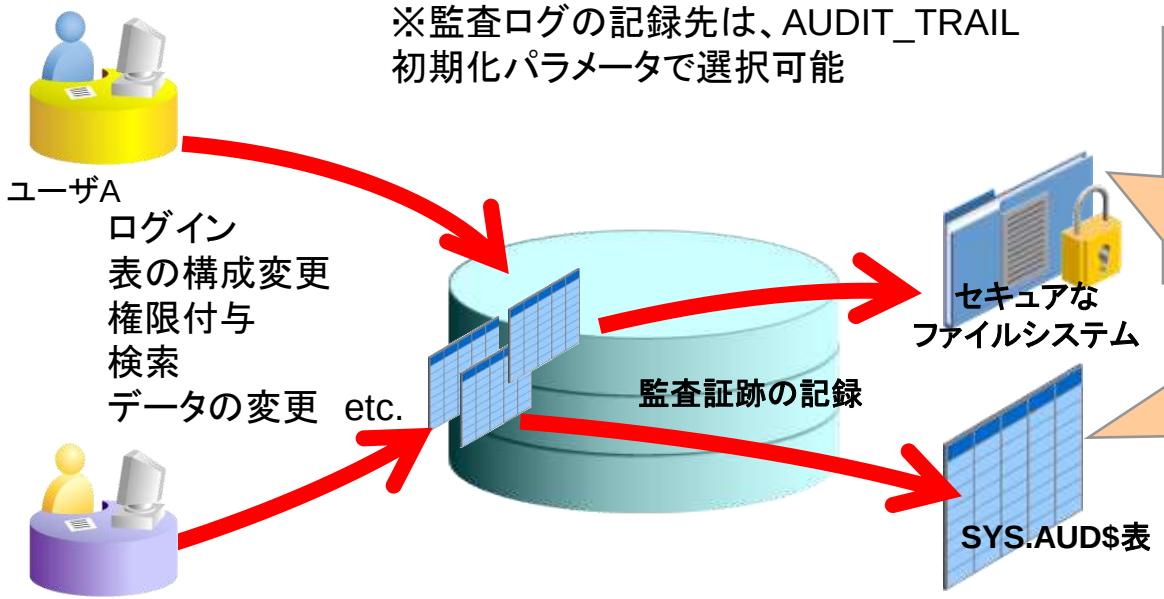
成功時は0、エラー発生時は発生した
Oracleエラー番号（ORA-XX）となる

Agenda

- Oracle Database監査機能
  - 必須監査
  - 標準監査
  - FGA監査
  - DBA監査
  - Log Miner
- ユーザ特定のポイント
- Oracleのセキュリティ・ソリューション
- Appendix
  - ログ監査の実践例
  - Oracle Audit Vault

標準監査とは

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、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SYS.AUD$表（内部表）に記録される
- AUD$表 の内容は、DBA_AUDIT_TRAIL ビューより確認可能

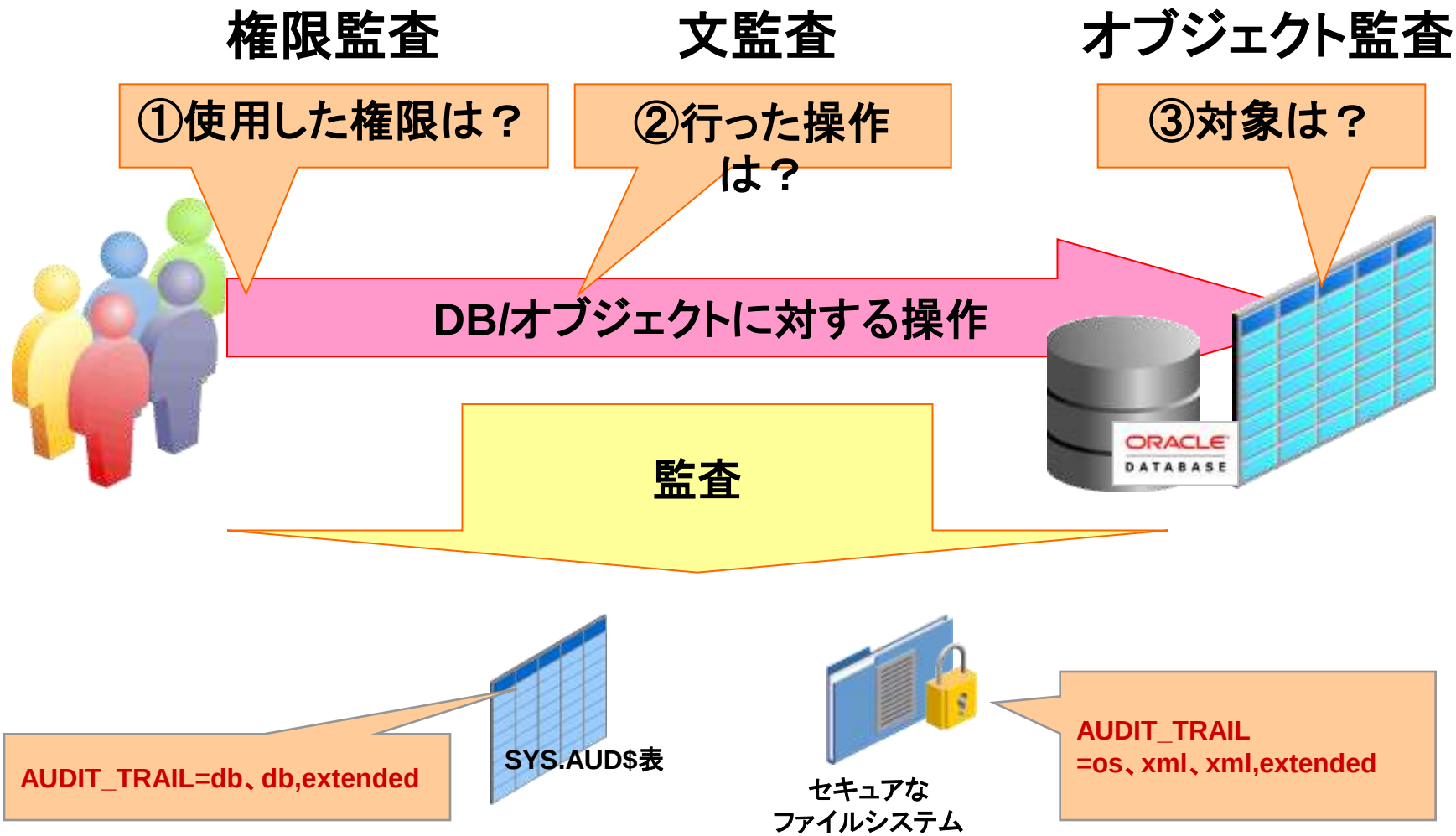
標準監査（詳細）1/2

監査対象	管理者以外のユーザによるデータベースへの操作 **■文監査** 特定のDDL文(データベース構造の変更)による操作 例) TABLE の作成・変更をするDDL文を監査 **■権限監査** 特定の権限による操作やログインを監査 例) CREATE ANY TRIGGER 権限が必要な処理を監査 **■オブジェクト監査** 特定のオブジェクトへの操作を監査 例) TABLE SCOTT.EMP に対するSELECT文を監査
初期化パラメータの設定	■AUDIT_TRAIL=os OSファイルにテキスト形式で監査ログを出力。出力される情報は少ない。 ■AUDIT_TRAIL=xml、xml,extended OSファイルにXML形式で監査ログを出力 ※XMLでの出力は Oracle 10gR2 以降で可能 ■AUDIT_TRAIL=db SYS.AUD$表に監査ログを出力 ■AUDIT_TRAIL=db, extended（10gR1 では db_extended） SYS.AUD$表に監査ログを出力。**SQL全文及びバインド変数の値も出力**。 ※AUDIT_TRAIL 設定後、インスタンスの再起動が必要 ※Oracle 9i 以前はSQL全文を記録できない

標準監査（詳細）2/2

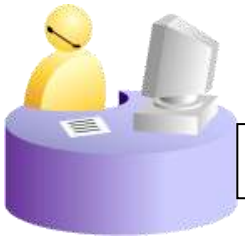
監査証跡出力先	AUDIT_TRAIL=os　の場合 UNIX: ＜AUDIT_FILE_DEST 初期化パラメータで定めた出力先＞/ora_<*pid*>.aud Windows: イベント・ビューアのログファイル -- AUDIT_TRAIL=xml、xml,extended　のいずれかの場合 ＜AUDIT_FILE_DEST 初期化パラメータで定めた出力先＞/ora_<*pid*>.xml -- AUDIT_TRAIL=db、db,extended　のいずれかの場合 SYS.AUD$表（DBA_AUDIT_TRAIL ビューで参照可能）
Audit 文の実施	文、権限、オブジェクトのいずれかを指定 ※AUDIT文を使用して文オプションおよび権限オプションを設定するには、 　AUDITSYSTEM 権限が必要 ※AUDIT文を使用してオブジェクト監査オプションを設定するには、監査対象のオブジェクト 　を所有しているか、またはAUDIT ANY 権限が必要
解除方法	NOAUDIT 文の実施

標準監査の種類



権限監査 - 使用した権限は？

DBユーザーには権限、ロールが割り振られ使われている
権限の利用に対して監査を設定する



SQL> AUDIT CREATE SESSION BY scott BY SESSION;

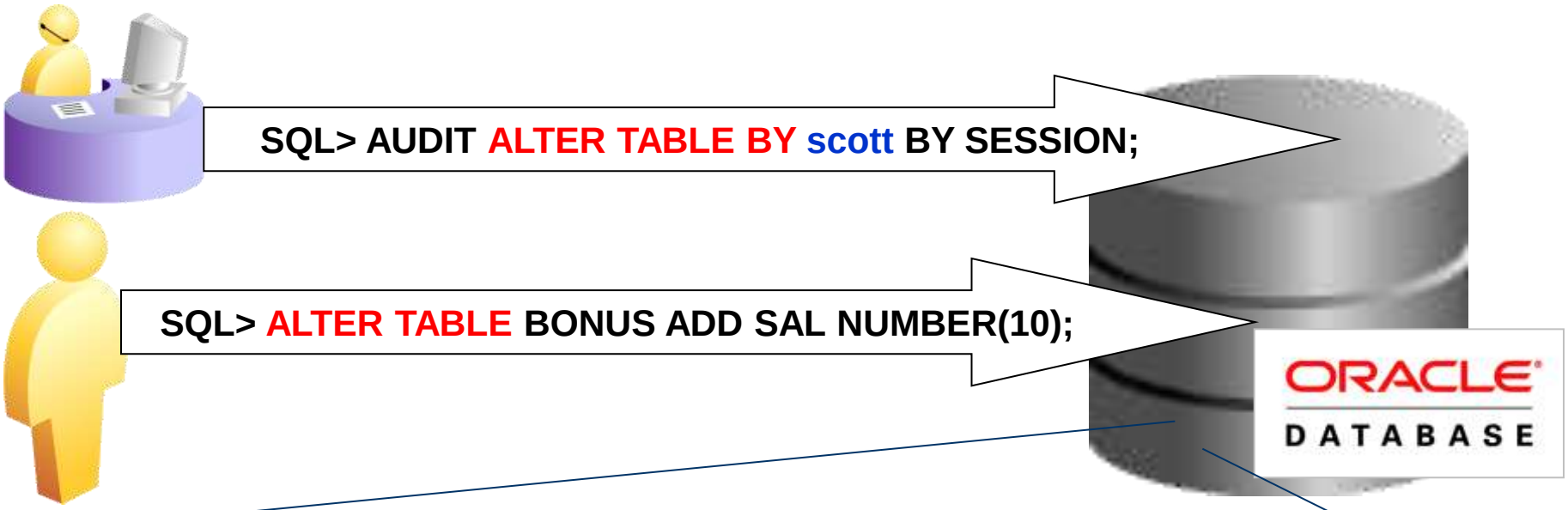
SQL> CONNECT scott/tiger@company

USERNAME	COMMENT_TEXT
SCOTT	Authenticated by: DATABASE

DBA_AUDIT_TRAILビュー

文監査・行った操作は?

DBユーザーが行う、一般的なSQL操作を対象として監査を実施する

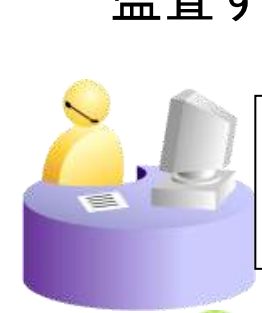


USERNAME	SQL_TEXT
SCOTT	ALTER TABLE BONUS ADD SAL NUMBER(10);

DBA_AUDIT_TRAILビュー

オブジェクト監査 – 対象は？

DBユーザーが行う、表をはじめとした各種オブジェクトに対する操作を監査する



SQL> AUDIT SELECT ON SCOTT.BONUS BY SESSION;

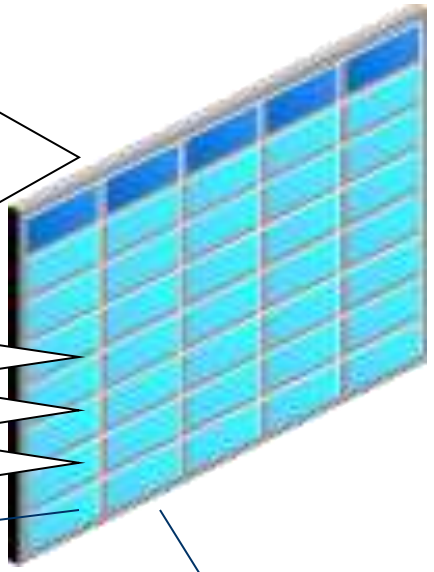
SQL> AUDIT INSERT ON SCOTT.BONUS BY SESSION;

SQL> AUDIT UPDATE ON SCOTT.BONUS BY SESSION;

SQL> SELECT ename,sal FROM SCOTT.BONUS

SQL> INSERT INTO SCOTT.BONUS values('sugisawa', 'CIO', '300000', '10')

SQL> UPDATE SCOTT.BONUS set sal='10000000' where comm='10'



USERNAME	SQL_TEXT
SCOTT	SELECT ename,sal FROM SCOTT.BONUS
SCOTT	INSERT INTO SCOTT.BONUS values('sugisawa', 'CIO', '300000', '10')
SCOTT	UPDATE SCOTT.BONUS set sal='10000000' where comm='10'

DBA_AUDIT_TRAILビュー

標準監査の構文

SQL> AUDIT SELECT ON*1 SCOTT.BONUS*2 BY SCOTT*3 BY ACCESS*4 BY PROXY*5 ;

*1 監査対象となる操作・権限

*2 監査対象となるオブジェクト

*3 操作ユーザー

*4 アクセスごとか、セッションごとに

*5 OS認証や連携を利用した場合に利用するオプション

他にも、多数オプションがあります。詳しくは下記マニュアルをご参照ください。（11gR1）
http://otndnld.oracle.co.jp/document/products/oracle11g/111/doc_dvd/server.111/E05750-03/statements_4.htm#14679

DB 10gでのDBA_AUDIT_TRAIL(1/2)

列	説明
OS_USERNAME	操作が監査対象となったユーザーのオペレーティング・システムでのログイン・ユーザー名
USERNAME	操作が監査対象となったユーザーの名前(ID番号ではない)
USERHOST	クライアントのホスト・マシンの名前
TERMINAL	ユーザーの端末の識別子
TIMESTAMP	ローカル・データベースのセッション・タイム・ゾーンでの監査証跡エントリの作成日時(AUDIT SESSIONで作成されたエントリに対するユーザー・ログインの日時)
OWNER	操作の影響を受けたオブジェクトの作成者
OBJ_NAME	操作の影響を受けたオブジェクトの名前
ACTION	操作の数値による型コード。対応する操作タイプ名はACTION_NAME列に含まれる。
ACTION_NAME	ACTION列の数値コードに対応する操作タイプの名前
NEW_OWNER	NEW_NAME列に指定されたオブジェクトの所有者
NEW_NAME	RENAME後のオブジェクトの新規名、または基礎となっているオブジェクトの名前
OBJ_PRIVILEGE	GRANT文またはREVOKE文によって付与または取り消されたオブジェクト権限
SYS_PRIVILEGE	GRANT文またはREVOKE文によって付与または取り消されたシステム権限
ADMIN_OPTION	ロールまたはシステム権限がADMIN OPTION付きで付与されたかどうか
GRANTEE	GRANT文またはREVOKE文で指定された権限受領者の名前
AUDIT_OPTION	AUDIT文で設定された監査オプション
SES_ACTIONS	セッションのサマリー(16文字で構成される文字列で、ALTER、AUDIT、COMMENT、DELETE、GRANT、INDEX、INSERT、LOCK、RENAME、SELECT、UPDATE、REFERENCES、EXECUTEの順に各操作の状態を1文字で表す。14、15および16の位置は、将来の使用のために確保されている。各文字の意味は次のとおり。 - – 情報がない場合 S – 成功の場合 F – 失敗の場合 B – 両方の場合
LOGOFF_TIME	ユーザー・ログオフの日時
LOGOFF_LREAD	セッションの論理読取り
LOGOFF_PREAD	セッションの物理読取り
LOGOFF_LWRITE	セッションの論理書込み
LOGOFF_DLOCK	セッション中に検出されたデッドロック

DB 10gでのDBA_AUDIT_TRAIL(1/2)

列	説明
COMMENT_TEXT	監査された文についての詳細情報を提供する、監査証跡エントリについてのテキスト・コメント ユーザーが認証された方式も示す。認証方式は、次のいずれか。 DATABASE – パスワードで認証された。 NETWORK – Oracle Net ServicesまたはAdvanced Security Optionで認証された。 PROXY – クライアントは、別のユーザーによって認証されている。プロキシ・ユーザー名は、認証方式に従う。
SESSIONID	各Oracleセッションの数値ID
ENTRYID	セッションの各監査証跡エントリの数値ID
STATEMENTID	文の実行ごとの数値ID
RETURNCODE	操作によって生成されたOracleエラー・コード。有効な値の例は次のとおり。 0 – 操作は成功 2004 – セキュリティ違反
PRIV_USED	操作の実行に使用されたシステム権限
CLIENT_ID	各Oracleセッションでのクライアント識別子
ECONTEXT_ID	アプリケーション実行コンテキスト識別子
SESSION_CPU	各Oracleセッションで使用されたCPUタイム
EXTENDED_TIMESTAMP	UTC（協定世界時）タイム・ゾーンでの監査証跡エントリで作成されたタイムスタンプ（AUDIT SESSIONで作成されたエントリに対するユーザー・ログインのタイムスタンプ）
PROXY_SESSIONID	プロキシ・セッション・シリアル番号（エンタープライズ・ユーザーがプロキシの機能を使用してログインした場合）
GLOBAL_UID	ユーザーのグローバル・ユーザー識別子（ユーザーがエンタープライズ・ユーザーとしてログインした場合）
INSTANCE_NUMBER	INSTANCE_NUMBER初期化パラメータで指定されたインスタンス番号
OS_PROCESS	Oracleプロセスのオペレーティング・システムのプロセス識別子
TRANSACTIONID	オブジェクトがアクセスまたは変更されたトランザクションのトランザクション識別子
SCN	問合せのシステム変更番号（SCN）
SQL_BIND	問合せのバインド変数データ
SQL_TEXT	問合せのSQLテキスト

DB 9iでのDBA_AUDIT_TRAIL(1/2)

列	データ型	NULL	説明
OS_USERNAME	VARCHAR2(255)		操作が監査対象となったユーザーのオペレーティング・システムでのログイン・ユーザー名
USERNAME	VARCHAR2(30)		操作が監査対象となったユーザーの名前（ID 番号ではない）
USERHOST	VARCHAR2(128)		ユーザーが Oracle インスタンスからデータベースにアクセスしている場合の Oracle インスタンスの数値インスタンス ID。分散ファイル・システムと共有データベース・ファイルを使用する環境でのみ使用される。
TERMINAL	VARCHAR2(255)		ユーザーの端末の識別子
TIMESTAMP	DATE	NOT NULL	監査証跡エントリの作成または CONNECT 文のログイン時刻のタイムスタンプ
OWNER	VARCHAR2(30)		操作の影響を受けたオブジェクトの作成者
OBJ_NAME	VARCHAR2(128)		操作の影響を受けたオブジェクトの名前
ACTION	NUMBER	NOT NULL	操作の数値による型コード。対応する操作タイプ名は ACTION_NAME 列に含まれる。
ACTION_NAME	VARCHAR2(27)		ACTION 列の数値コードに対応する操作タイプの名前
NEW_OWNER	VARCHAR2(30)		NEW_NAME 列に指定されたオブジェクトの所有者
NEW_NAME	VARCHAR2(128)		RENAME 後のオブジェクトの新規名、または基礎となっているオブジェクトの名前
OBJ_PRIVILEGE	VARCHAR2(16)		GRANT 文または REVOKE 文によって付与または取り消されたオブジェクト権限
SYS_PRIVILEGE	VARCHAR2(40)		GRANT 文または REVOKE 文によって付与または取り消されたシステム権限
ADMIN_OPTION	VARCHAR2(1)		ロールまたはシステム権限が ADMIN OPTION 付きで付与されたかどうか
GRANTEE	VARCHAR2(30)		GRANT 文または REVOKE 文で指定された権限受領者の名前
AUDIT_OPTION	VARCHAR2(40)		AUDIT 文で設定された監査オプション

DB 9iでのDBA_AUDIT_TRAIL(2/2)

列	データ型	NULL	説明
SES_ACTIONS	VARCHAR2(19)		セッションのサマリー（16 文字で構成される文字列で、ALTER、AUDIT、COMMENT、DELETE、GRANT、INDEX、INSERT、LOCK、RENAME、SELECT、UPDATE、REFERENCES、EXECUTE の順に各操作の状態を 1 文字で表す。14、15 および 16 の位置は、将来の使用のために確保されている。各文字の意味は次のとおり。 ■ - ― 情報がない場合 ■ S ― 成功の場合 ■ F ― 失敗の場合 ■ B ― 両方の場合）
LOGOFF_TIME	DATE		ユーザー・ログオフのタイムスタンプ
LOGOFF_LREAD	NUMBER		セッションの Logical Reads（論理読取り）
LOGOFF_PREAD	NUMBER		セッションの physical reads
LOGOFF_LWRITE	NUMBER		セッションの論理書込み
LOGOFF_DLOCK	VARCHAR2(40)		セッション中に検出されたデッドロック
COMMENT_TEXT	VARCHAR2(4000)		監査された文についての詳細情報を提供する、監査証跡エントリについてのテキスト・コメント ユーザーが認証された方式も示す。認証方式は、次のいずれか。 ■ DATABASE ― パスワードで認証された。 ■ NETWORK ― Oracle Net Services または Advanced Security で認証された。 ■ PROXY ― クライアントは、別のユーザーによって認証されている。プロキシ・ユーザー名は、認証方式に従う。
SESSIONID	NUMBER	NOT NULL	各 Oracle セッションの数値 ID
ENTRYID	NUMBER	NOT NULL	セッションの各監査証跡エントリの数値 ID
STATEMENTID	NUMBER	NOT NULL	文の実行ごとの数値 ID
RETURNCODE	NUMBER	NOT NULL	操作によって生成された Oracle エラー・コード。有効な値の例は次のとおり。 ■ 0 ― 操作は成功 ■ 2004 ― セキュリティ違反
PRIV_USED	VARCHAR2(40)		操作の実行に使用されたシステム権限
CLIENT_ID	VARCHAR2(64)		各 Oracle セッションでのクライアント識別子
SESSION_CPU	NUMBER		各 Oracle セッションで使用された CPU タイム

Agenda

- Oracle Database監査機能
  - 必須監査
  - 標準監査
  - FGA監査
  - DBA監査
  - Log Miner
- ユーザ特定のポイント
- Oracleのセキュリティ・ソリューション
- Appendix
  - ログ監査の実践例
  - Oracle Audit Vault

FGA（ファイングレイン）監査とは

通常監査と比較した、きめ細かな監査ポリシーを施行可能：

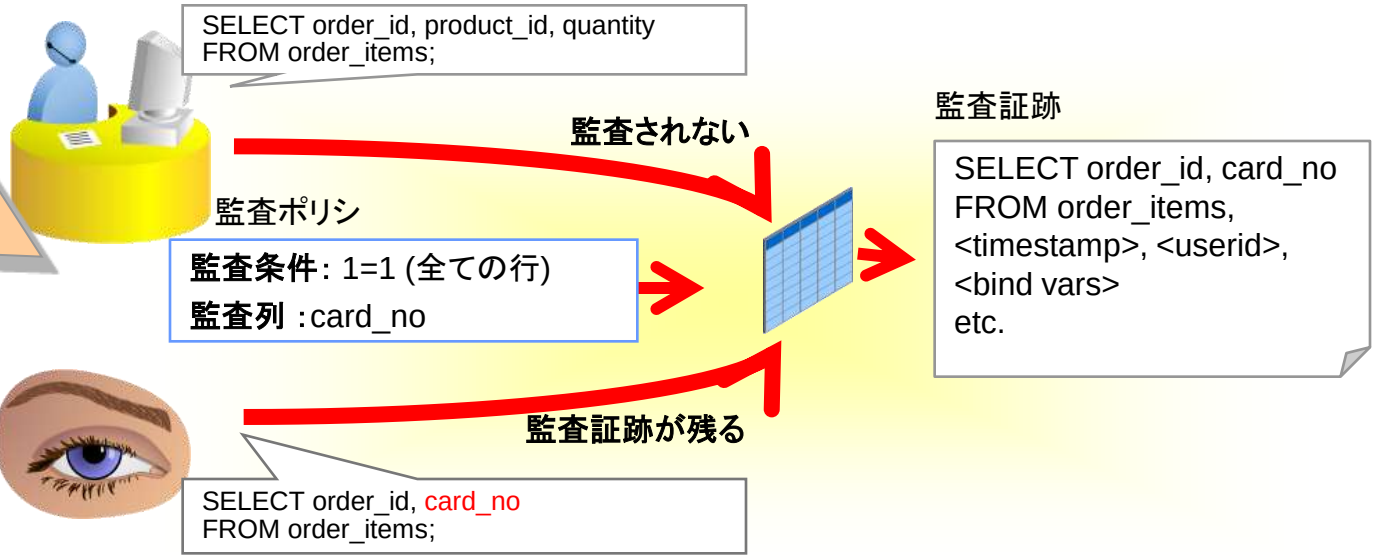
・処理対象の行（検索条件）、列、実行された文の種類等の条件を元に、監査証跡を残すか否かをきめ細かく指定することが可能

・Webアプリケーション等、コネクション・プールを利用した構成においても、エンド・ユーザーを特定可能な監査証跡を取得することが可能

ファイングレイン監査の例

特定の条件（列、データの値等）に基づいた細かな監査ポリシーを定義可能

監査証跡の格納先のカスタマイズや、ユーザー定義の監査アクションの定義も可能



FGA監査（詳細）

監査対象	特定のデータに対する SELECT、INSERT、UPDATE、DELETE によるアクセス（列名、条件の指定可能） DBA_FGA.ADD_POLICY プロシージャを使用し、監査対象を指定 ※ Oracle 9i ではSELECT文のみ監査可能 ※ Oracle 10g 以降では SELECT文 および DML 文(INSERT、UPDATE、DELETE)を監査可能
初期化パラメータの設定	不要
監査証跡出力先	SYS.FGA_LOG$表 （DBA_FGA_AUDIT_TRAIL ビューで参照可能）
Audit コマンドの実施	不要
解除方法	DBA_FGA.DROP_POLICY プロシージャを使用

FGA監査 設定例

設定

```
SQL> execute dbms_fga.add_policy(
  object_schema   => 'scott',
  object_name     => 'emp',
  statement_types => 'SELECT',
  audit_column    => 'SAL',
  audit_condition => 'job=''MANAGER''',
  policy_name     => 'emp_fga');
/
```

ポイント：条件に文字列を指定

audit_condition パラメータに
文字列型のカラムを指定する時は、
値を「‘」（シングルクォーテーション）
2つで囲みます。
※ダブルクォーテーションではない
ことに注意。

解除

```
SQL>execute dbms_fga.drop_policy(
  object_schema=>'scott',
  object_name=>'emp',
  policy_name=>'emp_fga');
/
```

http://otndnld.oracle.co.jp/document/products/oracle10g/102/doc_cd/appdev.102/B19245-01/d_fga.htm#CIAFBIDH

Agenda

- Oracle Database監査機能
  - 必須監査
  - 標準監査
  - FGA監査
  - DBA監査
  - Log Miner
- ユーザ特定のポイント
- Oracleのセキュリティ・ソリューション
- Appendix
  - ログ監査の実践例
  - Oracle Audit Vault

DBA監査とは

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監査証跡に残すことにより、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

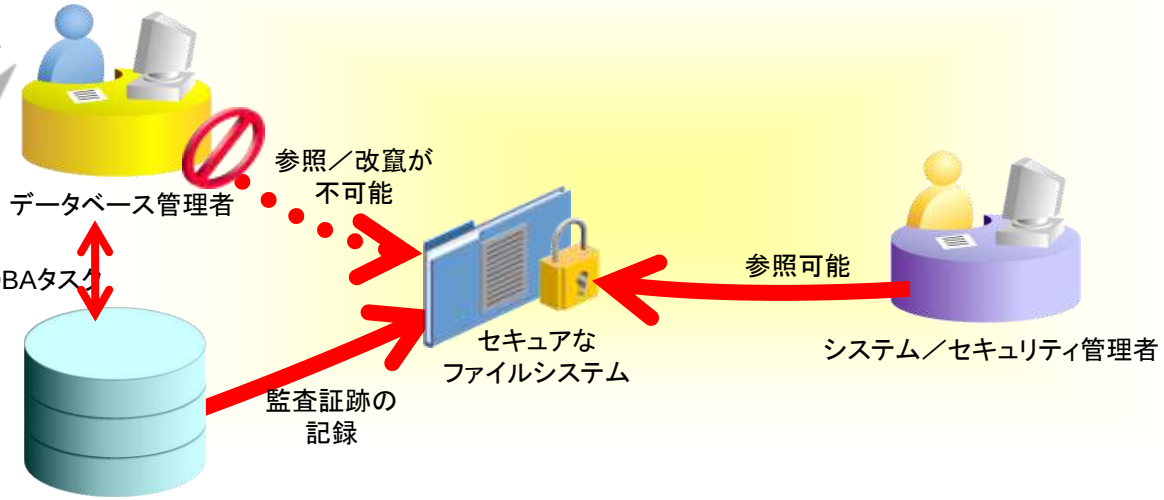
監査対象

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



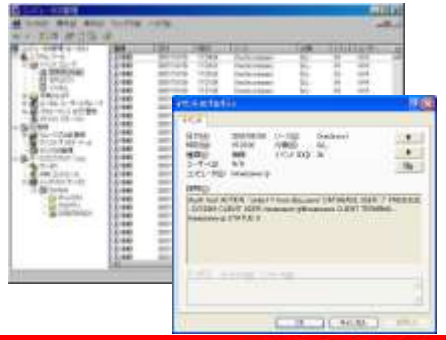
DBA監査（詳細）

監査対象	データベース管理者としてログインしたユーザ(SYSDBA、SYSOPER権限を持つユーザ)のデータベース操作
初期化パラメータの設定	AUDIT_SYS_OPERATIONS=TRUE ※設定後、インスタンスの再起動が必要
監査証跡出力先	AUDIT_TRAIL=os、db、db,extended、設定なし の場合 UNIX: ＜AUDIT_FILE_DEST 初期化パラメータで定めた出力先＞/ora_<pid>.aud Windows: イベント・ビューアのログファイル -- AUDIT_TRAIL=xml、xml,extended　のいずれかの場合 ＜AUDIT_FILE_DEST 初期化パラメータで定めた出力先＞/ora_<pid>.xml ※XMLでの出力は Oracle 10gR2 以降で可能
取得可能監査ログ	時刻、アクション(SQL全体)、DBユーザ、システム権限、OSユーザ/端末情報、終了コード
Audit 文の実施	不要
解除方法	AUDIT_SYS_OPERATIONS=FALSE ※設定後、インスタンスの再起動が必要

Unix

```
Instance name: orcl
:＜中略＞
Thu May  8 16:59:53 2008
ACTION : 'select * from dba_users'
DATABASE USER: '/'
PRIVILEGE : SYSDBA
CLIENT USER: oracle
CLIENT TERMINAL: pts/2
STATUS: 0
```

イベント・ビューア



DBA監査 設定方法

```
[oracle@direct24 ~]$ sqlplus / as sysdba
SQL*Plus: Release 10.2.0.3.0 - Production on 水 10月 17 14:22:46 2008
Copyright (c) 1982, 2006, Oracle.  All Rights Reserved.
アイドル・インスタンスに接続しました。
SQL> startup mount;
ORACLEインスタンスが起動しました。

Total System Global Area  536870912 bytes
Fixed Size                 1262788 bytes
Variable Size            415238972 bytes
Database Buffers         113246208 bytes
Redo Buffers               7122944 bytes
データベースがマウントされました。
SQL> alter system set audit_sys_operations=true scope=spfile;
システムが変更されました。

SQL> alter database open;
データベースが変更されました。
```

初期化パラメータで設定します。

通常は無効(FALSE)

DBA監査の実行例

■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>
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

（略）

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

（略）

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

（略）

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
```

Agenda

- Oracle Database監査機能
  - 必須監査
  - 標準監査
  - FGA監査
  - DBA監査
  - Log Miner
- ユーザ特定のポイント
- Oracleのセキュリティ・ソリューション
- Appendix
  - ログ監査の実践例
  - Oracle Audit Vault

LogMinerとは

ORACLE DATABASE ENTERPRISE EDITION

Oracle Databaseは更新トランザクション保護のため
オンラインREDOログに内容を記録しています。
またREDOログをアーカイブすることにより、過去の更新履歴から
復旧に利用することも可能です。
LogMinerはこれらログファイルより履歴を解析し可読化します。
また逐次ログを出力する方法とくらべ、必要時に取り出すため負荷
を軽減できます。

LogMiner
更新履歴を解析

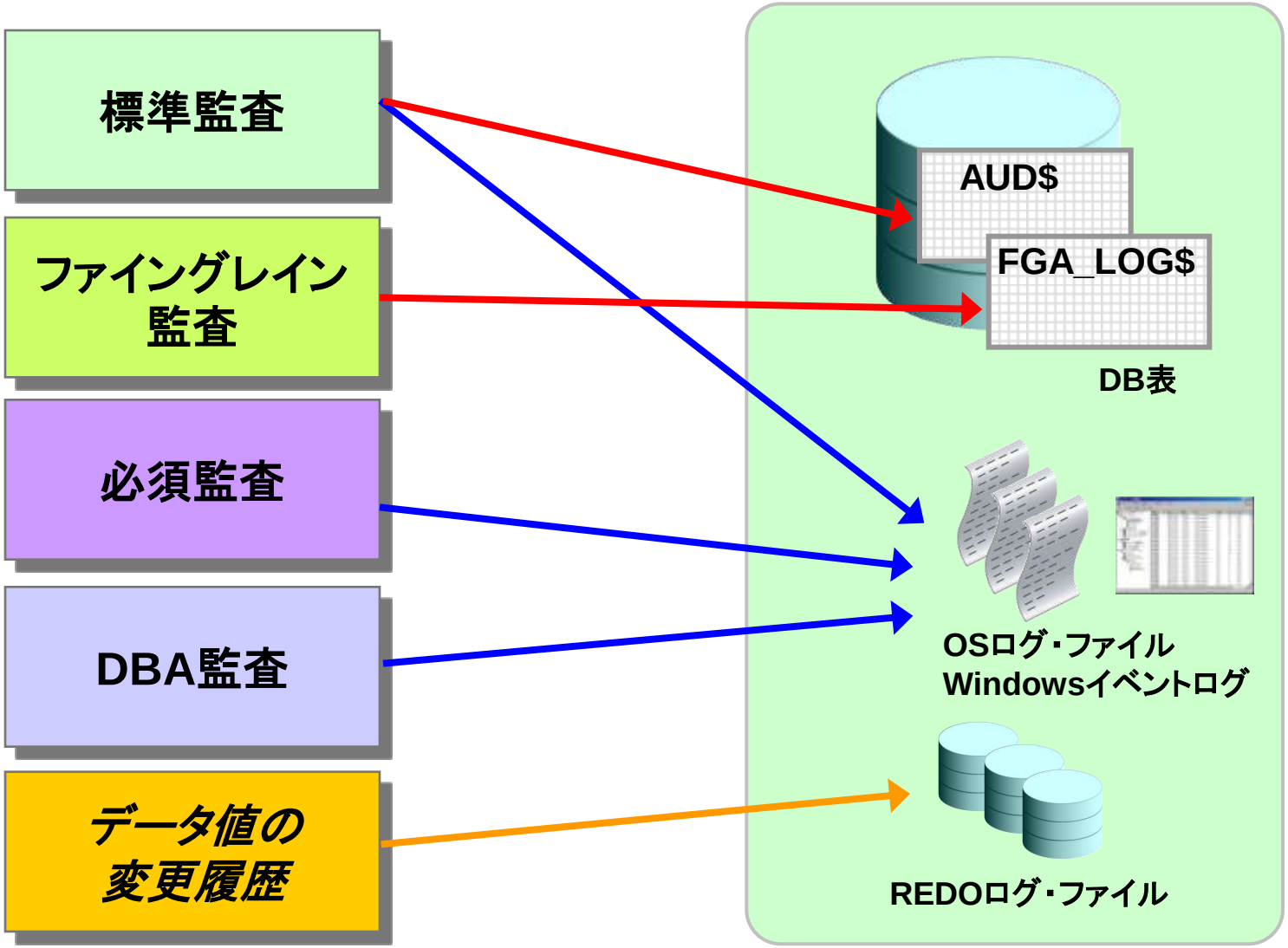
```
SQL> -- find session id and misc. info. of the TXN
select unique session#,session_info-
from v$logmnr_contents where XID = '0002001E00000209';

SQL> >

 SESSION#
----------
SESSION_INFO
--------------------------------------------------------------------------------
        ZZ
login_username=MALLOR client_info= OS_username=dmwong Machine_name=dlsun1417 OS
_terminal=pts/1 OS_process_id=16372 OS_program name=sqlplus@dlsun1417 (TNS V1-V3
)
```

Userを特定可能

LogMiner（詳細）

監査対象	DML 文(INSERT、UPDATE、DELETE)による変更履歴 ※ REDOログに記録されない情報（SELECT文など）は対象外 ※ アーカイブログモードでの運用が必要 ※ Database Enterprise Editionの機能を使用
設定方法	ALTER DATABASE ADD SUPPLEMENTAL LOG DATA　で設定 PL/SQLパッケージの実行によりログを抽出する
監査証跡出力先	V$LOGMNR_CONTENTS表

監査ログの出力先



[参考]監査ログの出力先ファイル名

①OSファイル出力先

初期化パラメータの確認

audit_file_dest = *$ORACLE_HOME*/admin/*{DBNAME}*/adump

本パラメータにより、必須監査、DBA監査およびOS,XMLとして指定した標準監査で出力される監査証跡が保存されます。

②標準監査

1.SYS.AUD$表 (実証跡データの保管先）

- DBA_AUDIT_TRAIL (証跡データを見やすい形にした管理ビュー

2.ora_<*プロセスID*>.aud（テキストファイル）

3.ora_<*プロセスID*>.xml (XMLテキストファイル）

- **V$XML_AUDIT_TRAIL　(XMLで指定し、出力したXMLファイルを見る動的ビュー）**

③ファイングレン監査

1. SYS.FGA_LOG$ (実証跡データの保管先）

- DBA_FGA_AUDIT_TRAIL (証跡データを見やすい形にした管理ビュー)

2.ora_<*プロセスID*>.aud（テキストファイル）

3.ora_<*プロセスID*>.xml (XMLテキストファイル）

- **V$XML_AUDIT_TRAIL　(XMLで指定し、出力したXMLファイルを見る動的ビュー）**

Agenda

- Oracle Database監査機能
- ユーザ特定のポイント
- Oracleのセキュリティ・ソリューション
- Appendix
  - ログ監査の実践例
  - Oracle Audit Vault

Oracle Databaseのユーザー情報を確認する

1. USERENVコンテキスト
   - どのようなクライアントからのアクセスか、詳細な情報を格納します

2. V$SESSION
   - ユーザーセッションの中から、固有の情報を把握します
   - 動的管理の一種

1. USERENVコンテキスト

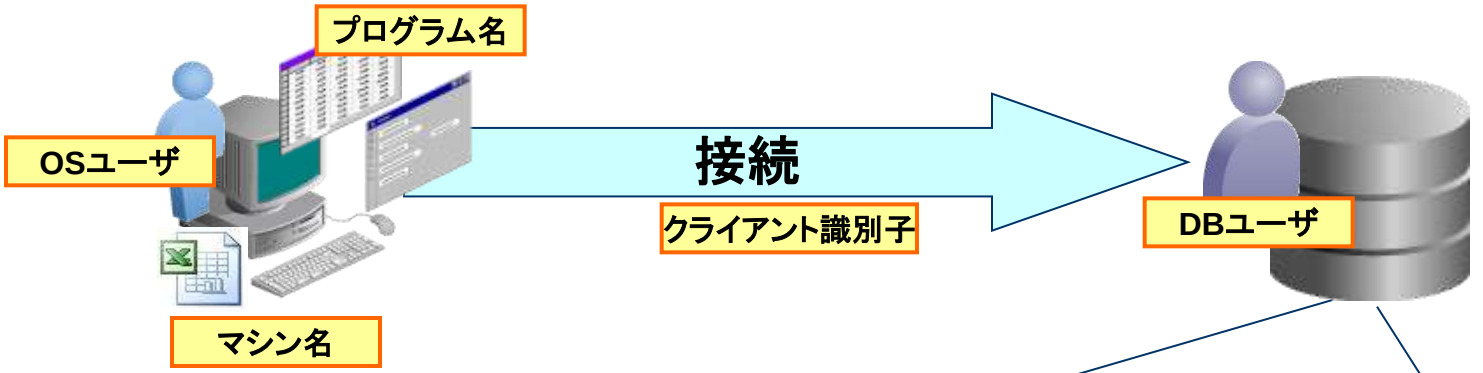
USERENVコンテキスト

- セッション情報の元となるデータを保持
- セッションにかかわる認証の情報を確保

USERENV内容（一部）

AUTHENTICATED_IDENTITY	認証されたユーザー名を記録します 例(DB認証) scott 例(LDAP認証) cn=scott dn=jp dn=oracle dn=com
CLIENT_IDENTIFIER	**任意で設定できる識別子**
GLOBAL_UID	Oracle Internet Directoryからユーザーのログイン名
HOST	クライアントのホスト名
OS_USER	データベース・セッションを開始するクライアント・プロセスのオペレーティング・システム・ユーザー名を戻します。
PROXY_USER	SESSION_USERの代理としてカレント・セッションを開いたデータベース・ユーザー（通常は中間層）の名前を戻します。

2. V$SESSION



セッション情報内にユーザー情報が格納

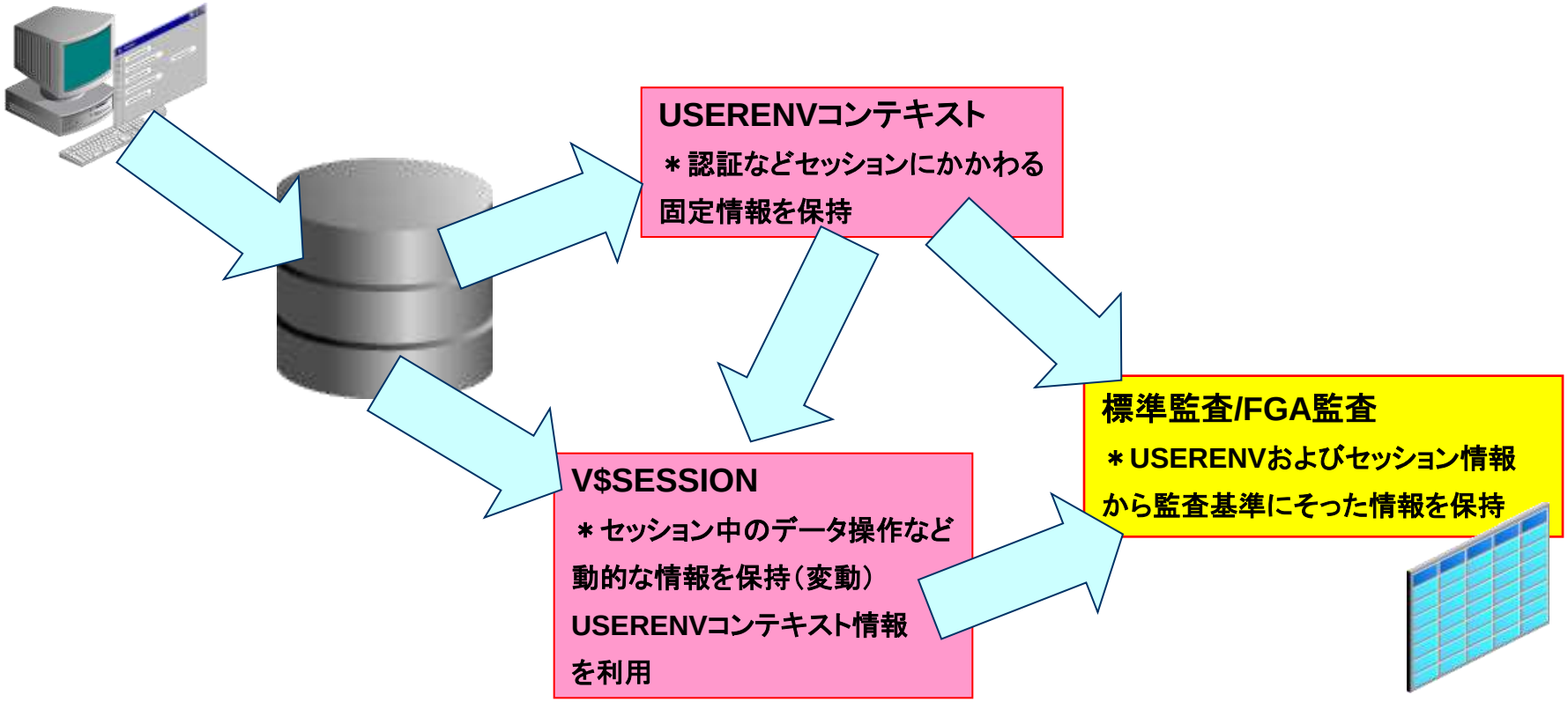
OSユーザ	マシン名	プログラム名	クライアント識別子	DBユーザ
OSUSER	MACHINE	PROGRAM	CLIENT_IDENTIFIER	USERNAME
ksugisaw	PC1	MsQRY.EXE	任意の文字列	SCOTT
hkatsuya	PC98	ACCESS.EXE	任意の文字列	SCOTT

V$SESSION表

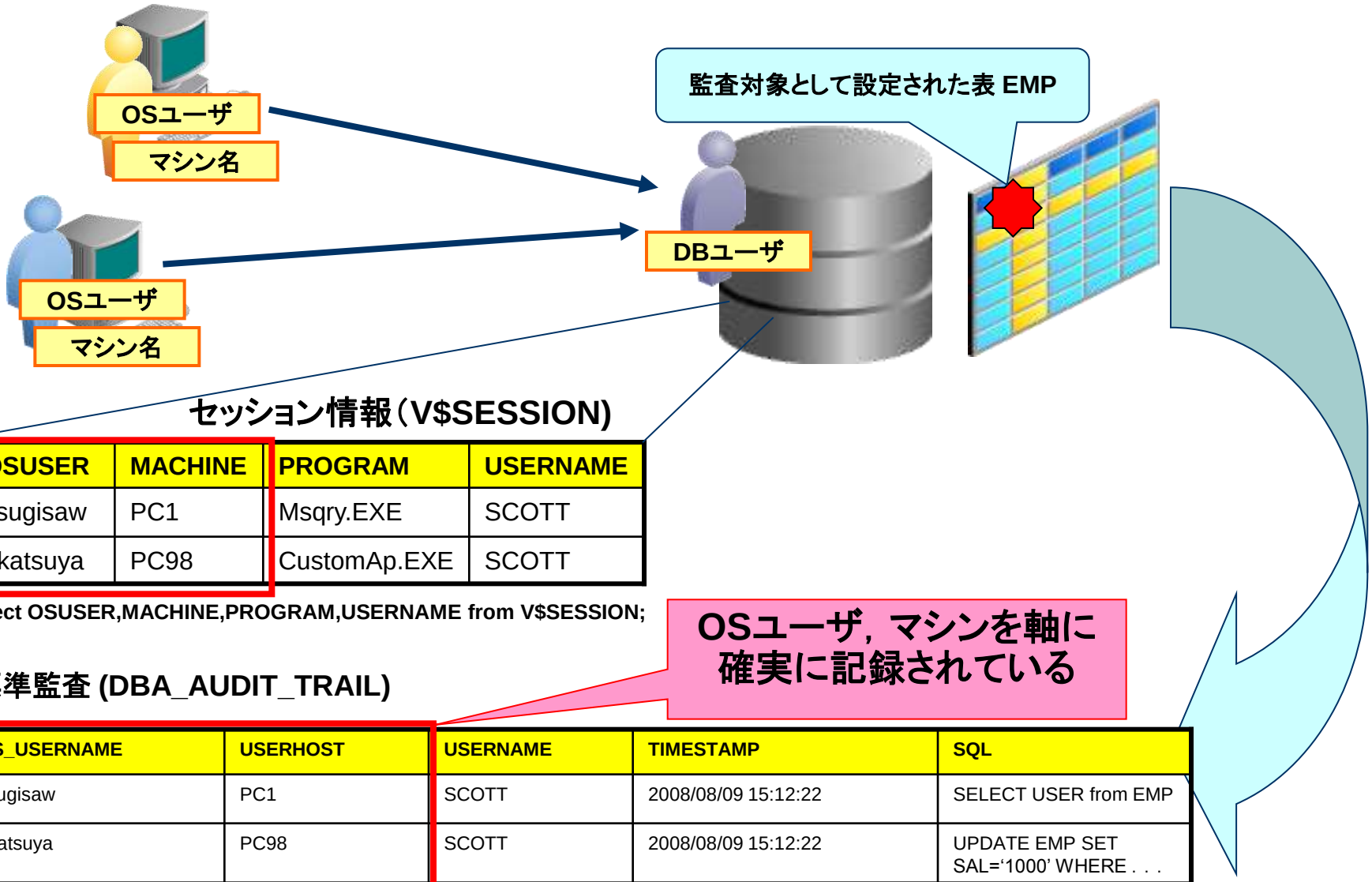
```
SQL>SELECT OSUSER,MACHINE,CLIENT_IDENTIFIER,PROGRAM FROM V$SESSION;
```

DBコネクションとセッションの考え方

USERENVコンテキスト、V$SESSION、監査機能の関係



クライアント・サーバー型のユーザー特定



セッション情報（V$SESSION)

OSUSER	MACHINE	PROGRAM	USERNAME
ksugisaw	PC1	Msqry.EXE	SCOTT
hkatsuya	PC98	CustomAp.EXE	SCOTT

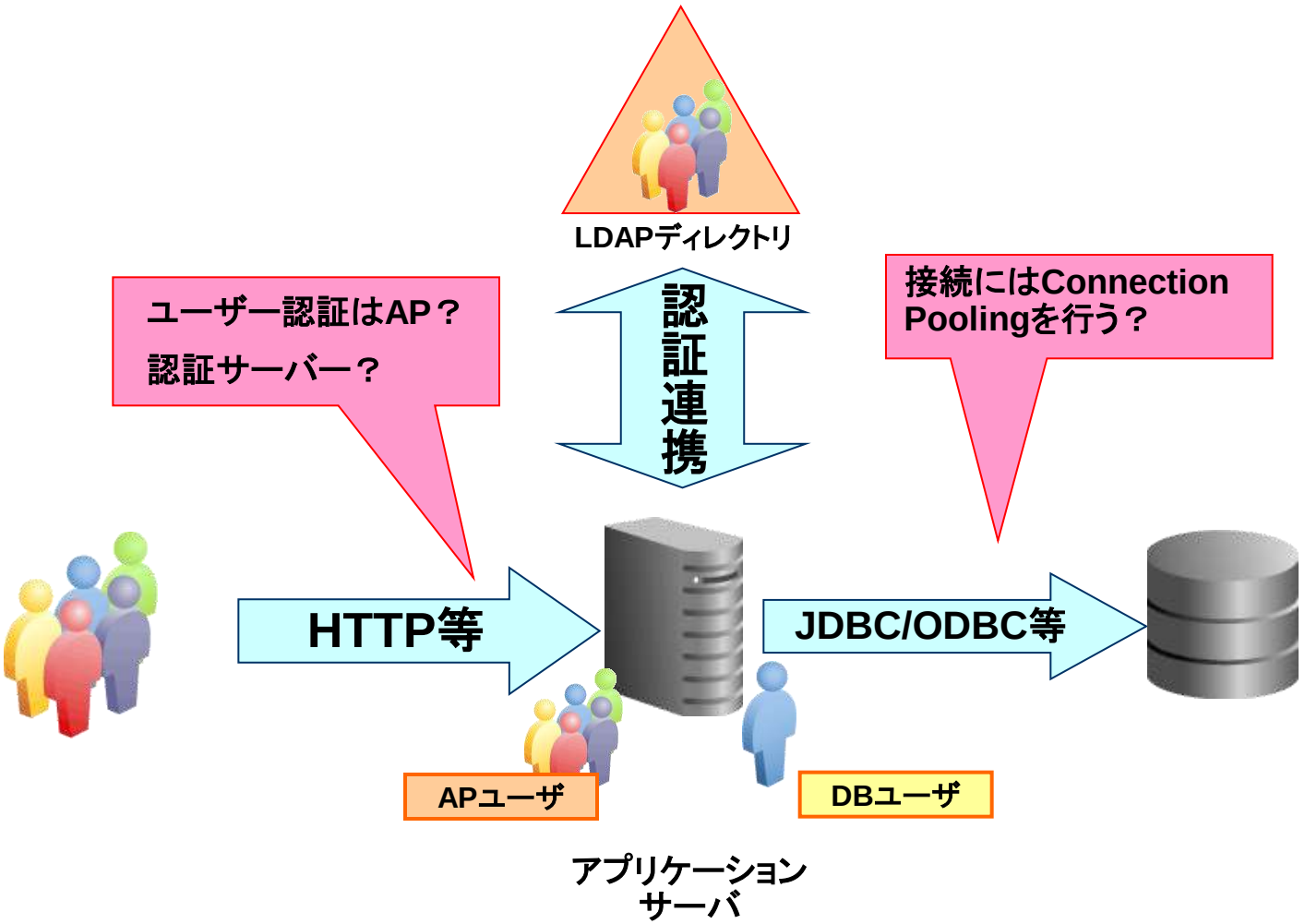
Select OSUSER,MACHINE,PROGRAM,USERNAME from V$SESSION;

OSユーザ，マシンを軸に
確実に記録されている

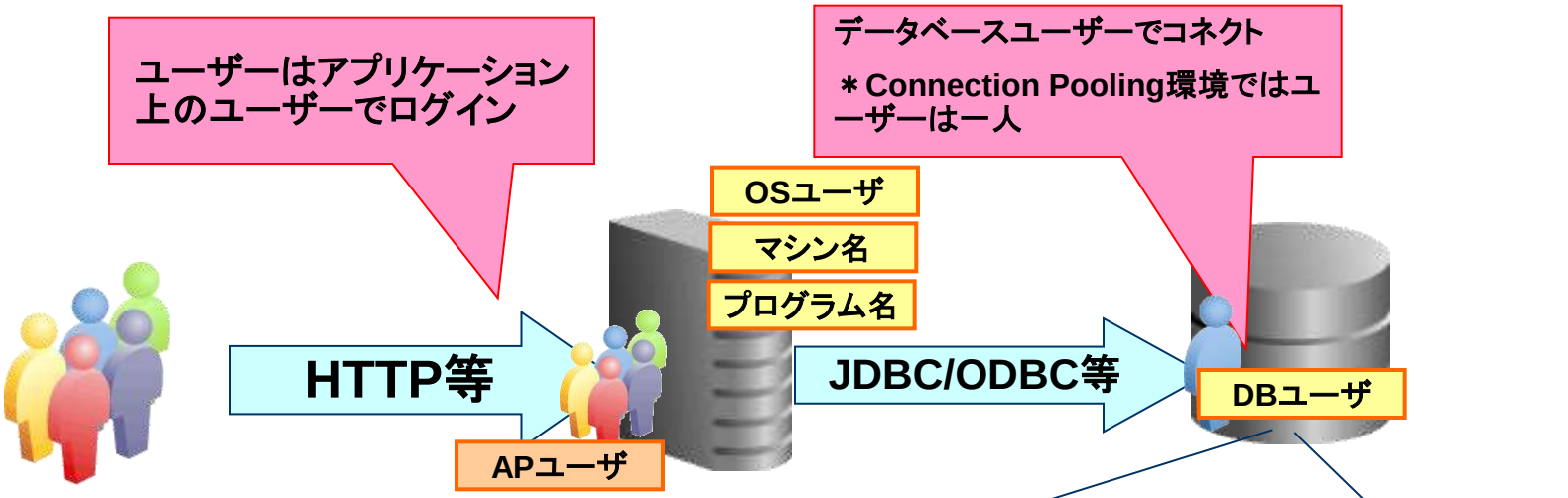
標準監査 (DBA_AUDIT_TRAIL)

OS_USERNAME	USERHOST	USERNAME	TIMESTAMP	SQL
ksugisaw	PC1	SCOTT	2008/08/09 15:12:22	SELECT USER from EMP
hkatsuya	PC98	SCOTT	2008/08/09 15:12:22	UPDATE EMP SET SAL='1000' WHERE . . .

三層型アプリケーション



問題となるポイントの把握



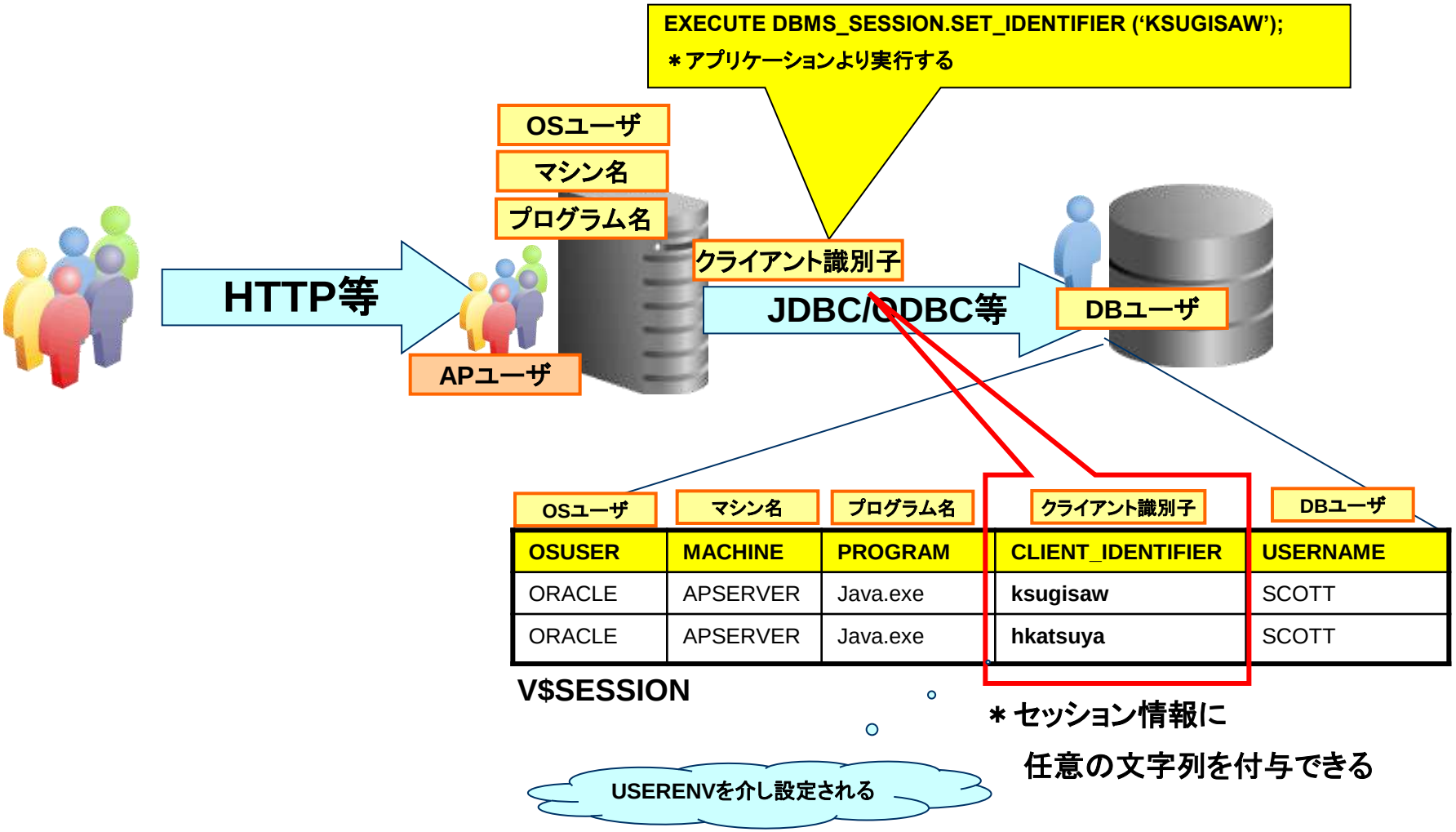
DB側ではアプリケーションサーバーからの接続情報のみ

OSユーザ	マシン名	プログラム名	DBユーザ	
OSUSER	MACHINE	PROGRAM	USERNAME	・・・
ORACLE	APSERVER	Java.exe	SCOTT	・・・
ORACLE	APSERVER	Java.exe	SCOTT	・・・

セッション情報(V$SESSION)

三層型のアプリケーションでは、ユーザーの特定が難しいケースが多い

CLIENT_IDENTIFIERの利用



CLIENT_IDENTIFIERと監査ログ

監査ログへの対応

OSUSER	MACHINE	PROGRAM	CLIENT_IDENTIFIER	USERNAME
ORACLE	APSERVER	Java.exe	**ksugisaw**	SCOTT
ORACLE	APSERVER	Java.exe	**hkatsuya**	SCOTT

セッション情報(V$SESSION)

OS_USERNAME	USERNAME	HOST	CLIENTID	・・・
ORACLE	SCOTT	APSERVER	**KSUGISAW**	・・・

標準監査/ファイングレン監査(DBA_AUDIT_TRAIL, DBA_FGA_AUDIT_TRAIL)

監査証跡にも確実に残すことが可能

CLIENT_IDENTIFIER - メリット・デメリット -

- メリット
  - 任意の文字列をログイン時に入力することができる
  - アプリケーションレベルで一意のIDを入力できる
    - 最初に一度実行するのみ
- デメリット
  - アプリケーション上のプログラムでの実装が必要

***アクセスコントロールはアプリケーションの仕様/特性で**
実装されるケースがほとんどであり、別途検討する必要性がある

Agenda

- Oracle Database監査機能
- ユーザ特定のポイント
- Oracleのセキュリティ・ソリューション
- Appendix
  - ログ監査の実践例
  - Oracle Audit Vault

サーバサイドセキュリティの重要性

企業情報の重要度 → 高い

クライアントサイド

出口で止める
セキュリティ

- Winny対策
- アンチウイルスソフトの導入
- Thin Clientの導入
- HDD/外部メモリデバイスの撤去
- 指紋認証など生体認証の導入
- 入館証の導入、監視カメラ

サーバサイド

大元を正規化する
セキュリティ

**根本からの本格的な
セキュリティ対策が必要**

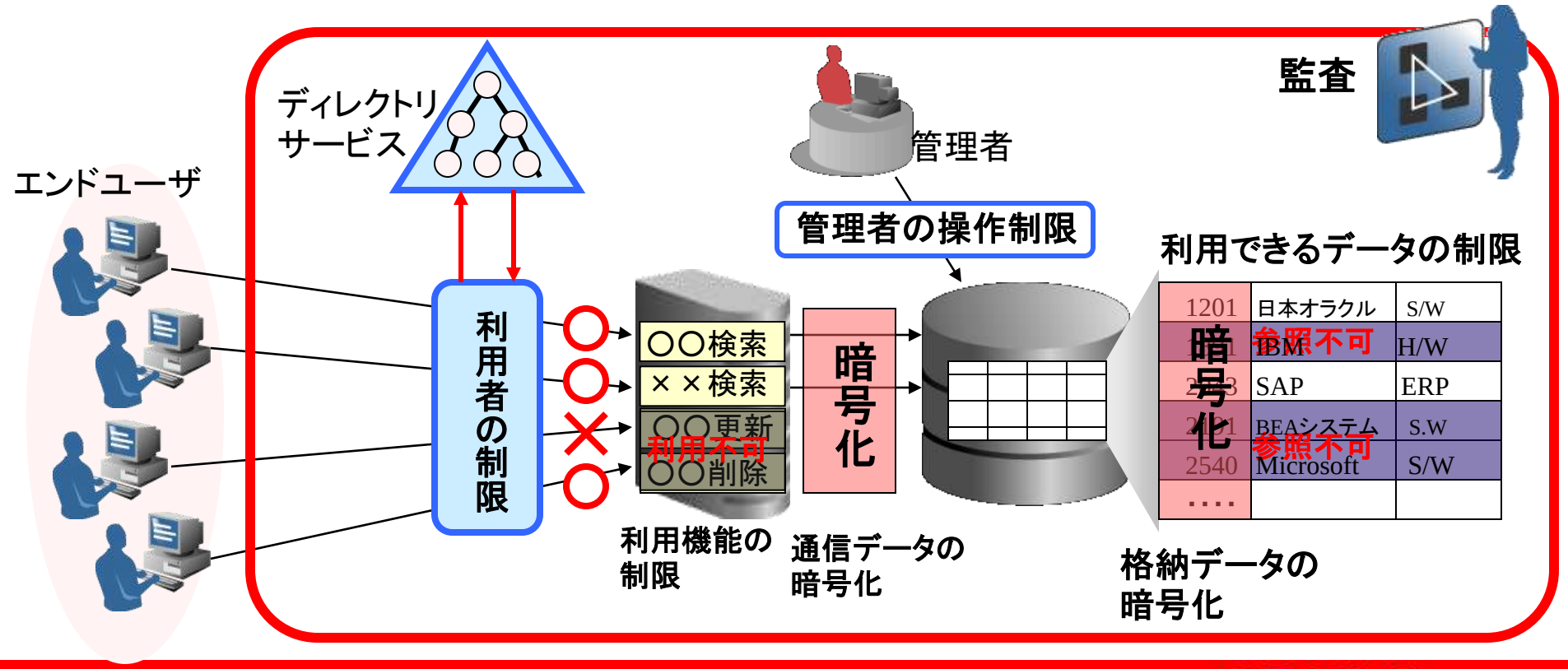
“サーバサイド･セキュリティ”

サーバサイドセキュリティのポイント

1. 認証・アクセスコントロール
2. 暗号化
3. 監査

- 通信データの暗号化
- 格納データの暗号化

1. 利用者の制限（認証）
2. 利用機能の制限
3. 管理者の制限（職掌分化）
4. データの制限（アクセスコントロール）

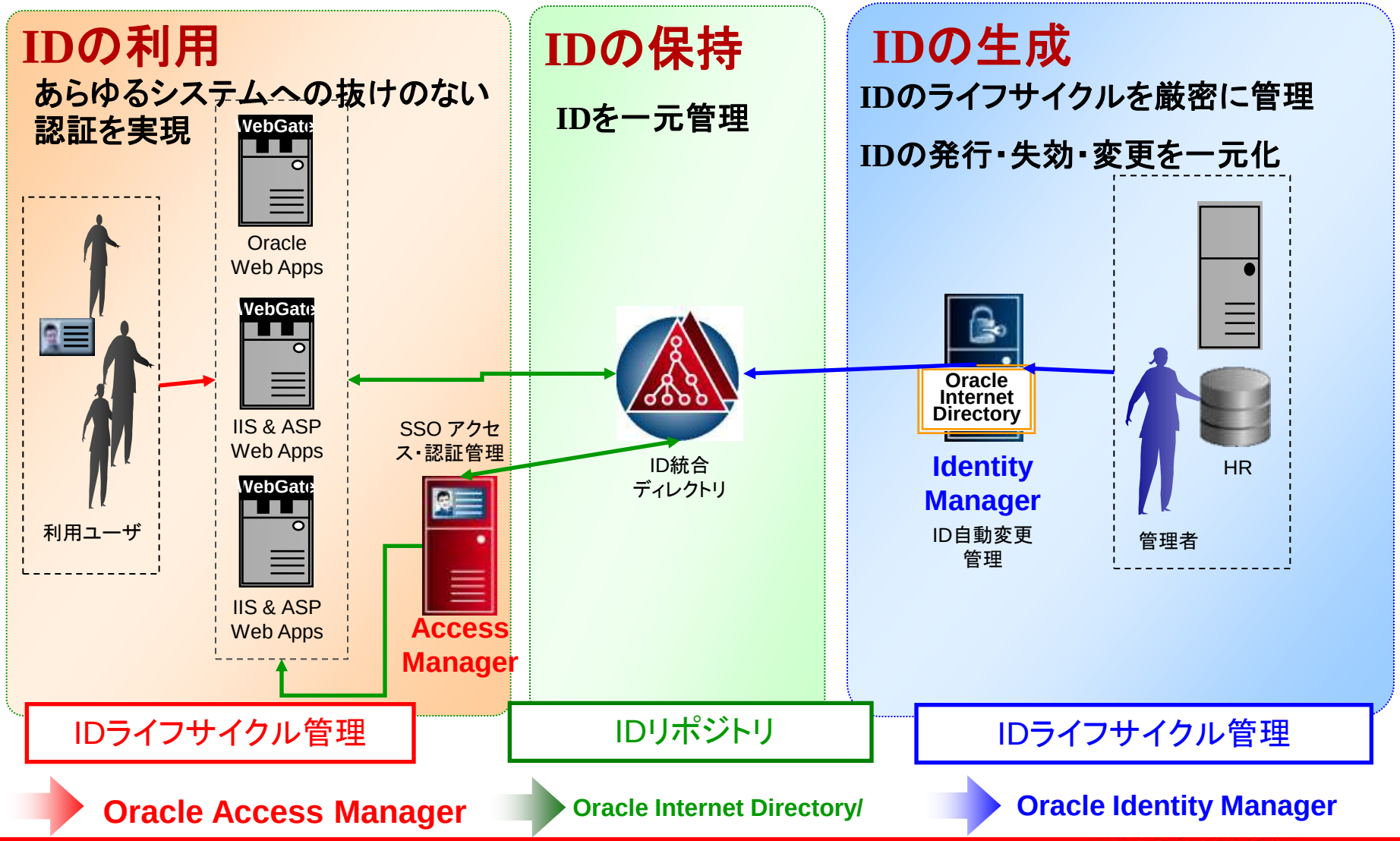


Oracleのセキュリティ・ソリューション

1. 認証・アクセスコントロール
    1. 利用者の制限（認証）
       Oracle Identity & Access Management
    2. 利用機能の制限
       Oracle Web Service Manager
    3. 管理者の制限（職掌分化）
       Oracle Database Vault
    4. データの制限（アクセスコントロール）
       Oracle Virtual Private Database
2. 暗号化 Advanced Security Option
    1. 通信データの暗号化
    2. 格納データの暗号化
3. 監査 Oracle Audit Vault

認証・アクセスコントロール

Oracle Identity Management



認証・アクセスコントロール

Oracle Access Manager

Oracle Access Managerとは？

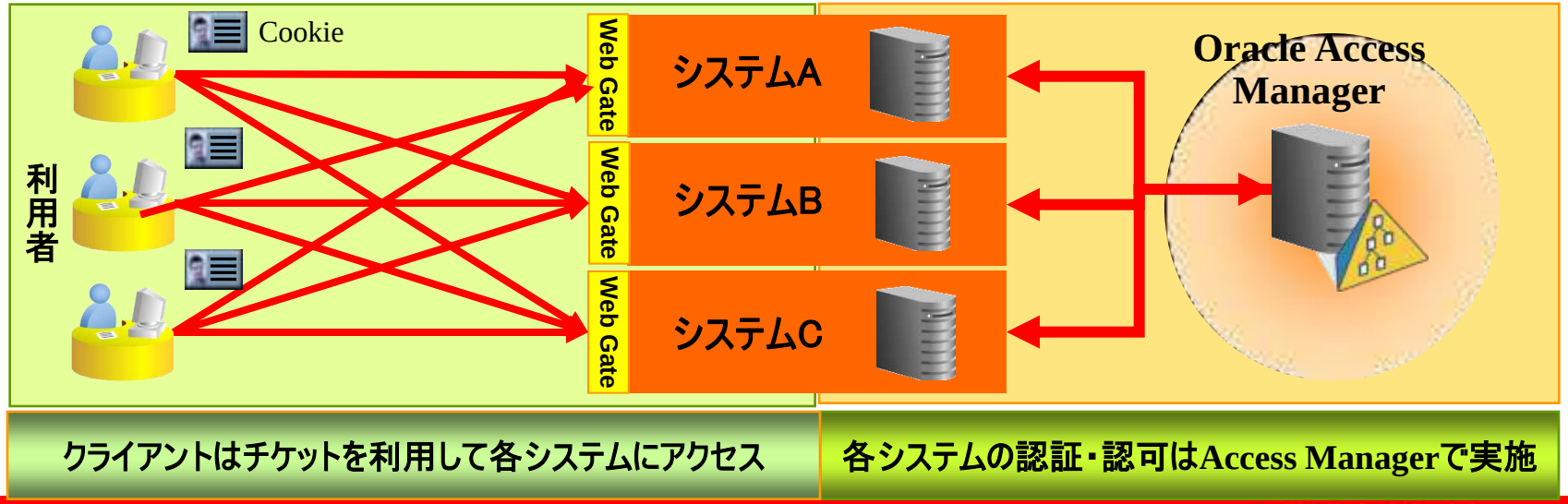
- Agent型のシングルサインオンサーバー

Oracle Access Managerの機能

- **統合認証管理**：シングルサインオン環境の提供
- **統合アクセス管理**：複数Webシステムへの一元的なアクセス制御
- **アクセスポリシー管理**：柔軟できめ細かいアクセス認可ルールの設定

Oracle Access Manager導入のメリット

- シングルサインオンによるユーザ利便性の向上
- 本人確認、権限付与の一元化による信頼性向上
- グループ管理による組織変更への動的かつ迅速な対応
- 委任管理、パスワード管理による管理コスト低減



Oracle Web Services Manager

Webサービスのセキュリティ

メッセージをインターセプトし、セキュリティを付加

- ✓ アクセス制御（認証/認可）
- ✓ 暗号化、デジタル署名
- ✓ Aceess Manager連携
- ✓ WS-Security、SAMLのサポート

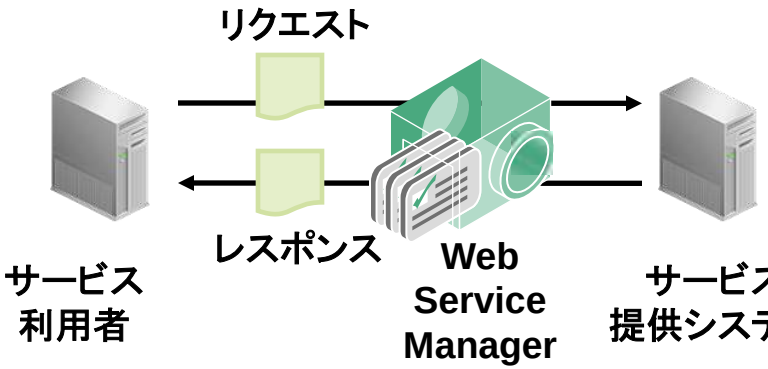
➢既存のサービスに手を加えることなく、付加価値を追加可能

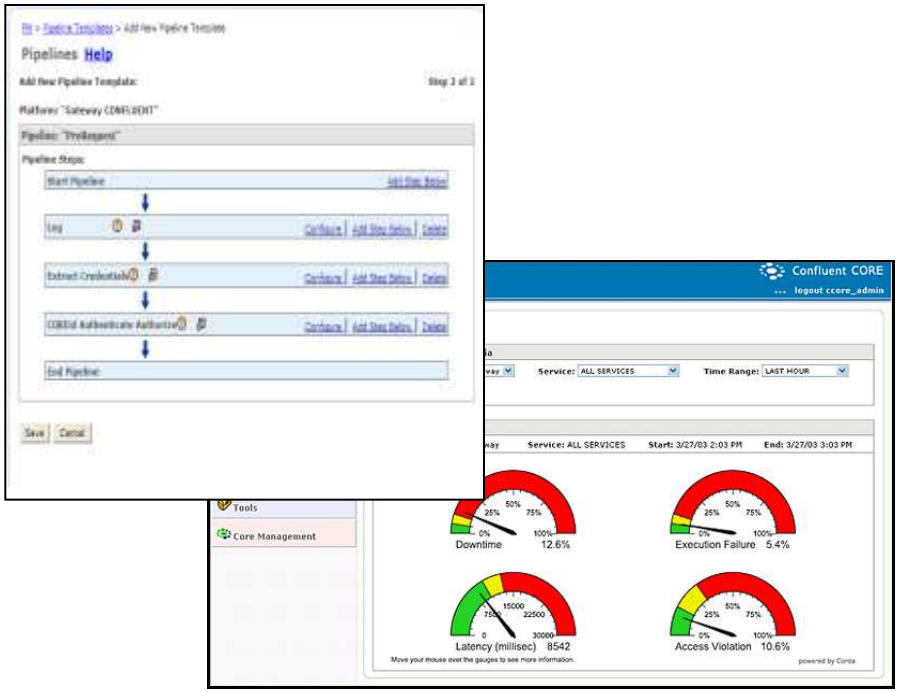
➢柔軟な稼動アーキテクチャ
- ✓ ゲートウェイ（個別のサーバとして動作）
- ✓ エージェント（APサーバに組み込み）

➢GUIで宣言的にポリシーを定義

➢モニタリング結果の可視化

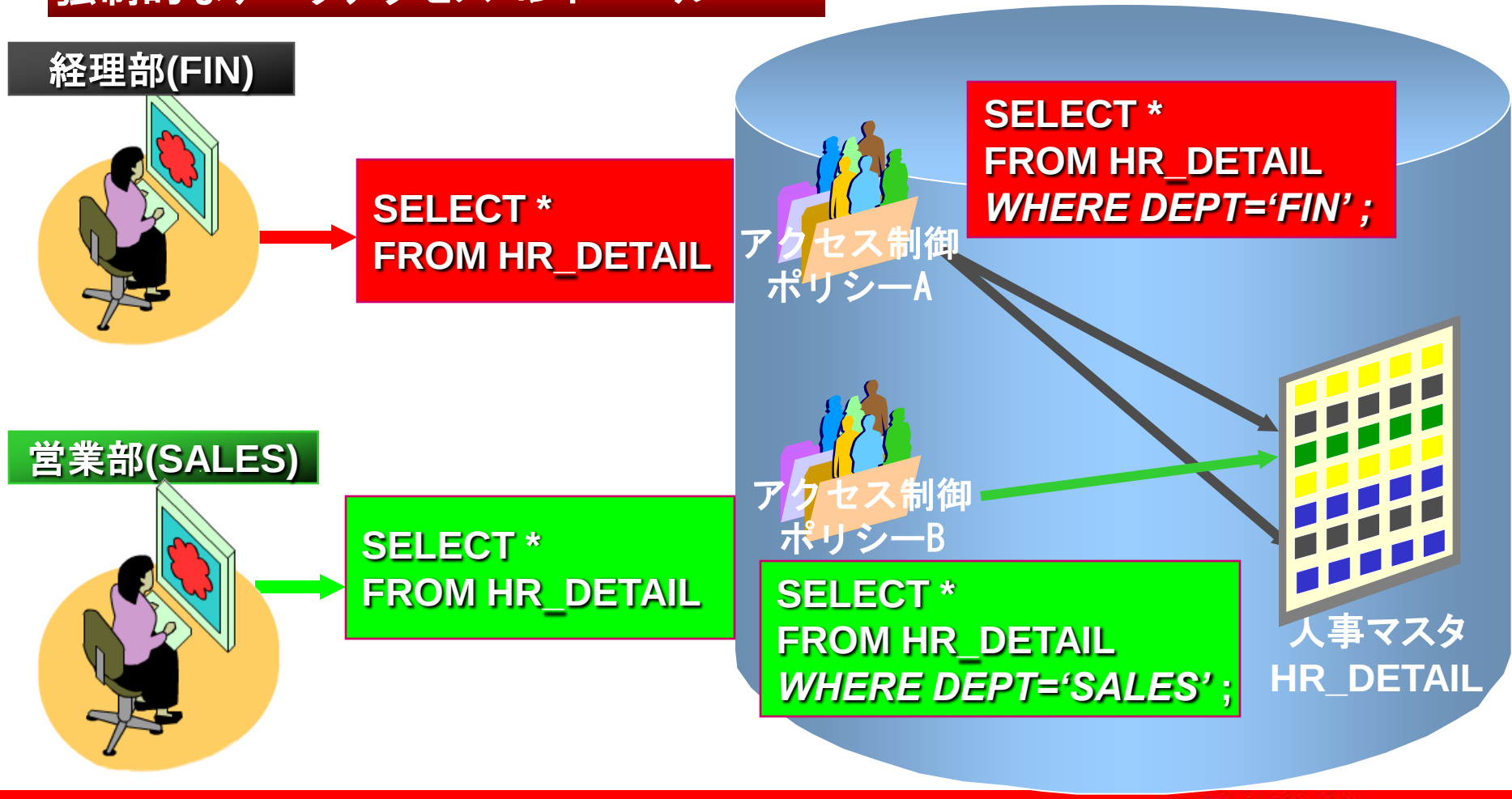
➢BPEL Process Managerとの連携





Virtual Private Database

Databaseの中で実現する
強制的なデータアクセスコントロール



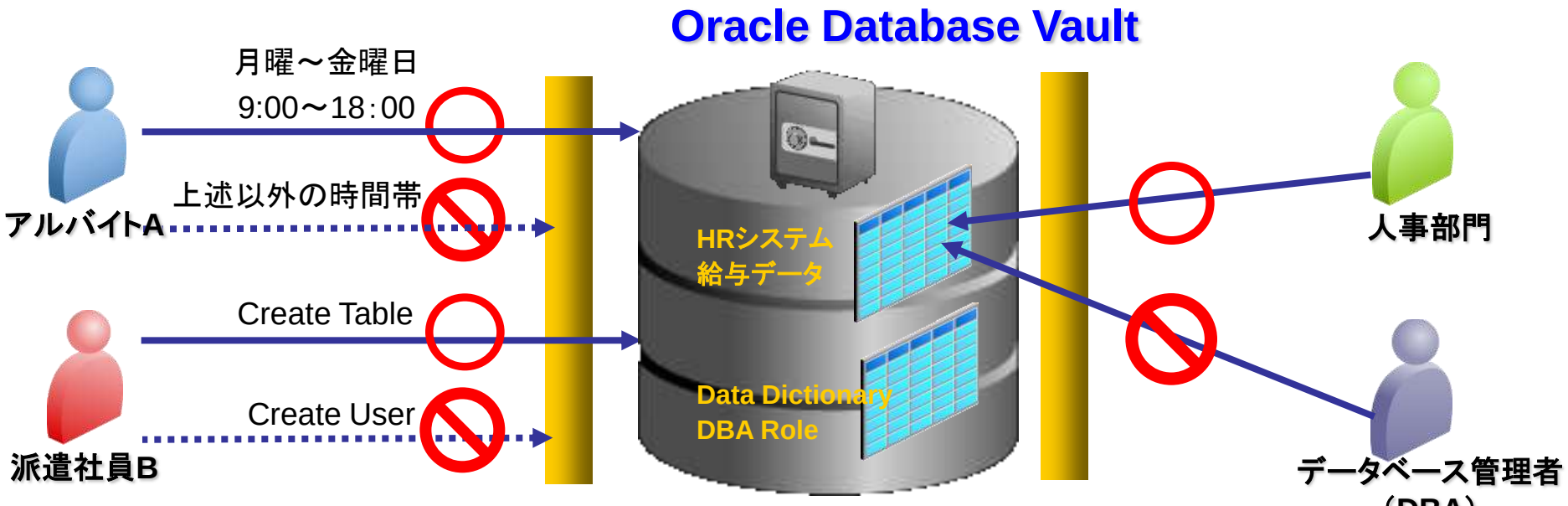
認証･アクセスコントロール

Oracle Database Vault

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



暗号化 通信データの暗号化機能

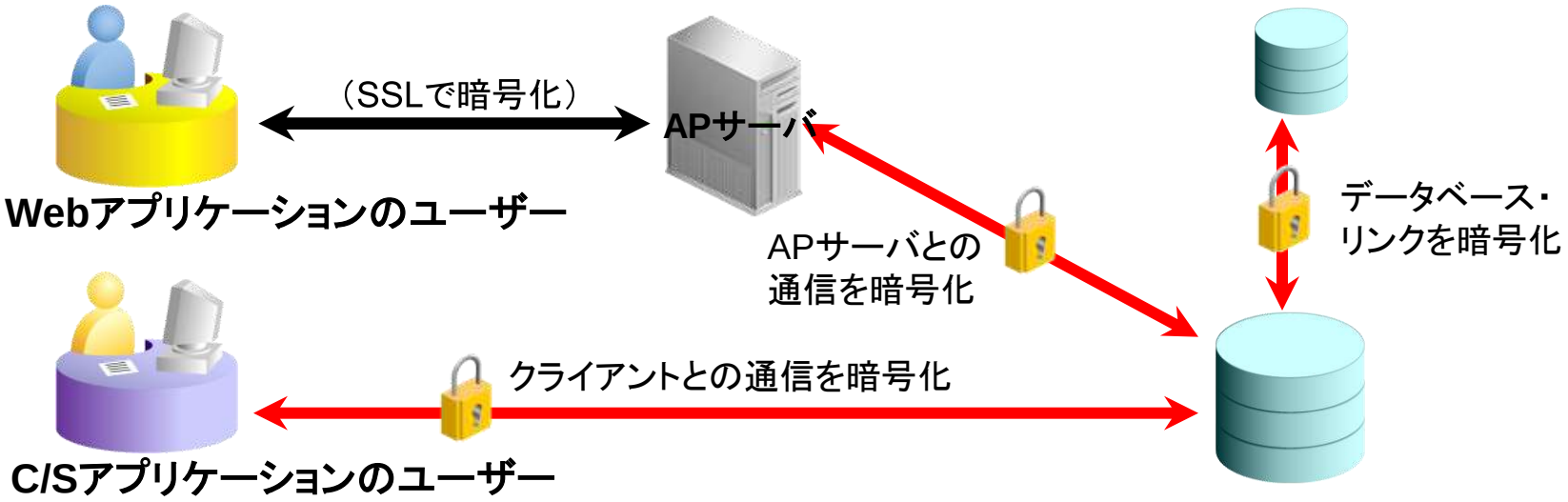
Advanced Security Option

データベースにおけるリスク

機密性の高いデータを**通信経路上で不正に奪取、あるいは改ざん**されてしまう可能性があるため、ネットワーク上のOracle通信データを保護する必要がある。

Oracle Databaseにおける対策

Oracle Netの通信データを暗号化・符号化することで
ネットワーク上における盗聴・改ざんを防ぎます



暗号化 格納データの暗号化

Advanced Security Option

データベースにおけるリスク

Oracleにログインをせずに、**OS上、あるいはバックアップ・メディアから機密性の高いデータを含むファイルを読み取られる**可能性があるため、格納されているデータ自体を保護する必要がある。

Oracle Databaseにおける対策

透過的な格納データの暗号化

アプリケーションを変更することなく、機密データを含む列をディスク上で暗号化

バックアップデータの暗号化

RMANで取得するバックアップセットに含まれる全てのデータの暗号化

名前	電話番号	住所
本社	1234	千代田区紀尾井町4－1
用賀事業所	5678	世田谷区用賀4－10－5
渋谷事業所	9012	渋谷区渋谷2－15－1

ディスク上で暗号化

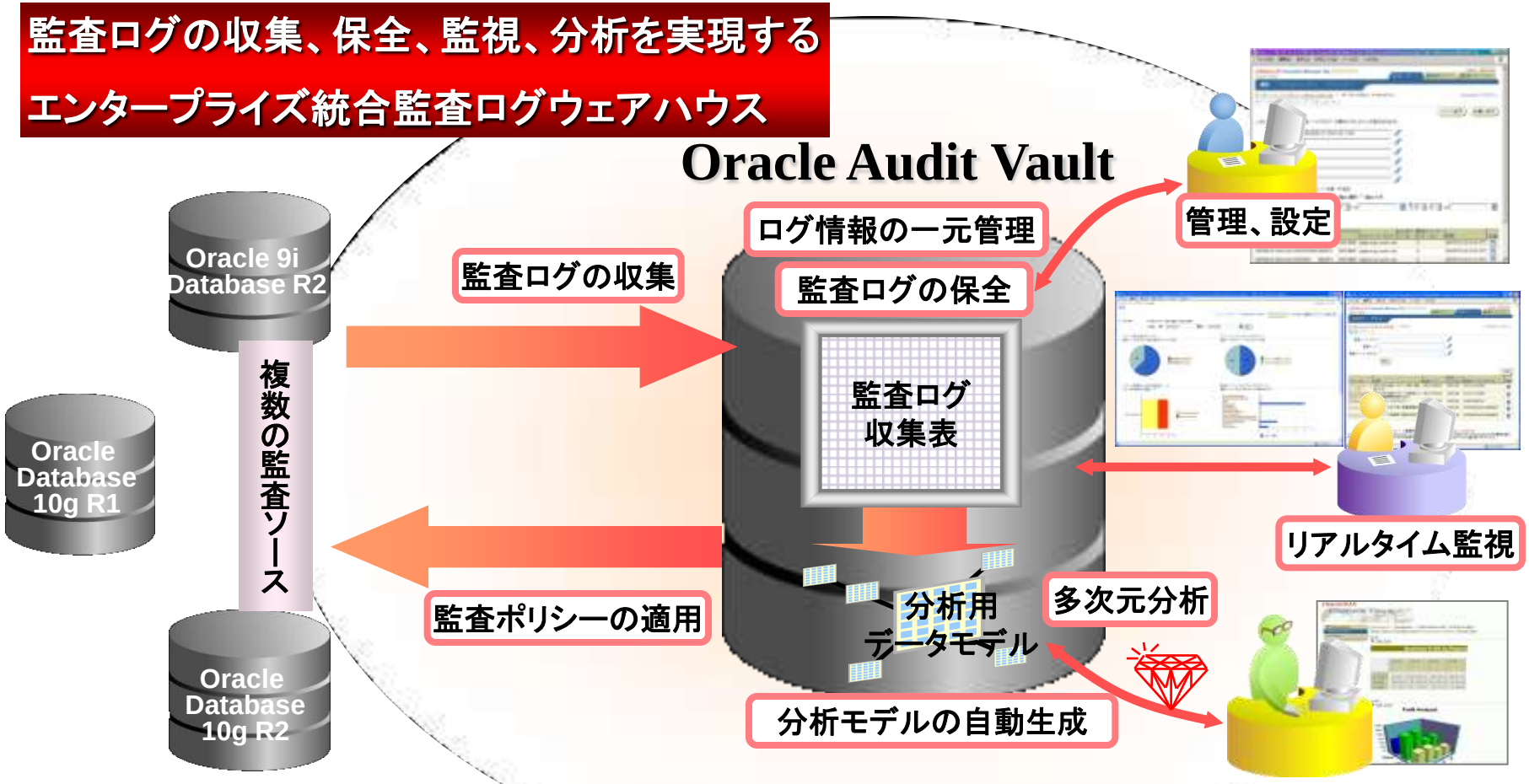
ｲyﾍ}e=捜「餌]・賢pMﾒ$
ﾇﾊ群。?・ｹMﾒ!e2a =捜「
32$5r″!e2aSge1?L3

格納データの暗号化例

監査

Oracle Audit Vault

監査ログの収集、保全、監視、分析を実現する
エンタープライズ統合監査ログウェアハウス



- Oracle Database の監査機能により監査ログを取得

- 監査ログを一箇所に収集し 安全かつ効率的に管理
- 監視、レポーティング、高度な分析が可能

まとめ

- 何を監査すべきか？
  - 監査要件を整理することで、重要な情報は限られてきます
  - すべてをとることではなく、把握することそのものが重要です
- 監査ログの管理
  - 監査ログはデータベースの機能で確実に取得できます
  - 内部統制の証拠として使用するためには、正当性を証明する必要もあります
  - 監査ログを確実に取り、守り、把握できるようにすることが重要です

OTN×ダイセミ　でスキルアップ!!

・技術的な内容について疑問点を解消したい！
・一般的なその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

技術的な疑問点は、OTN掲示版の「データベース一般」へ

※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

期間限定にて、ダイセミの人気セミナーを動画配信中!!
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

ORACLE

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=1

※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

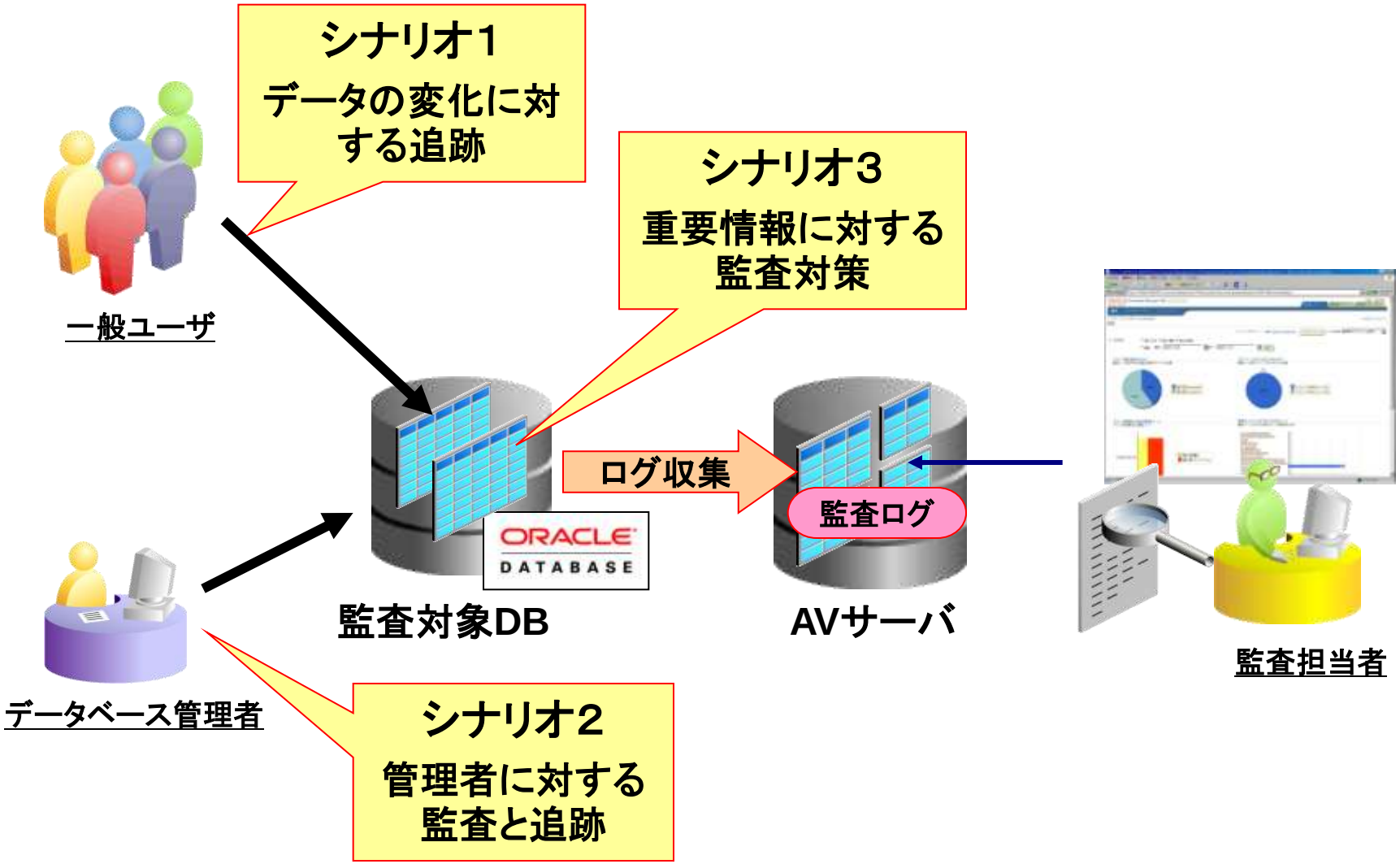
※月曜~金曜　9:00~12:00、13:00~18:00

（祝日および年末年始除く）

Agenda

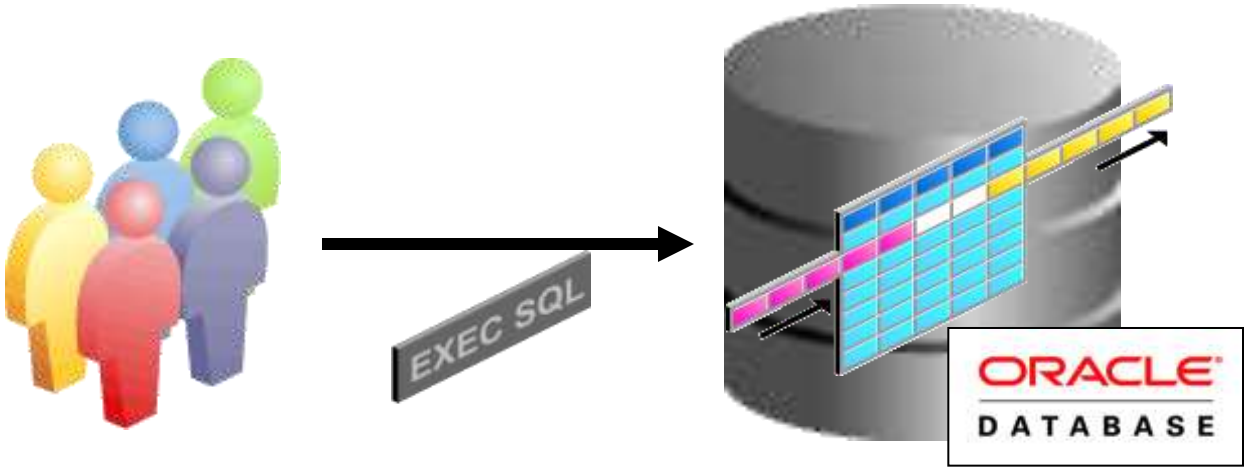
- Oracle Database監査機能
- ユーザ特定のポイント
- Oracleのセキュリティ・ソリューション
- Appendix
  - ログ監査の実践例
  - Oracle Audit Vault

ログ監査の実践シナリオ



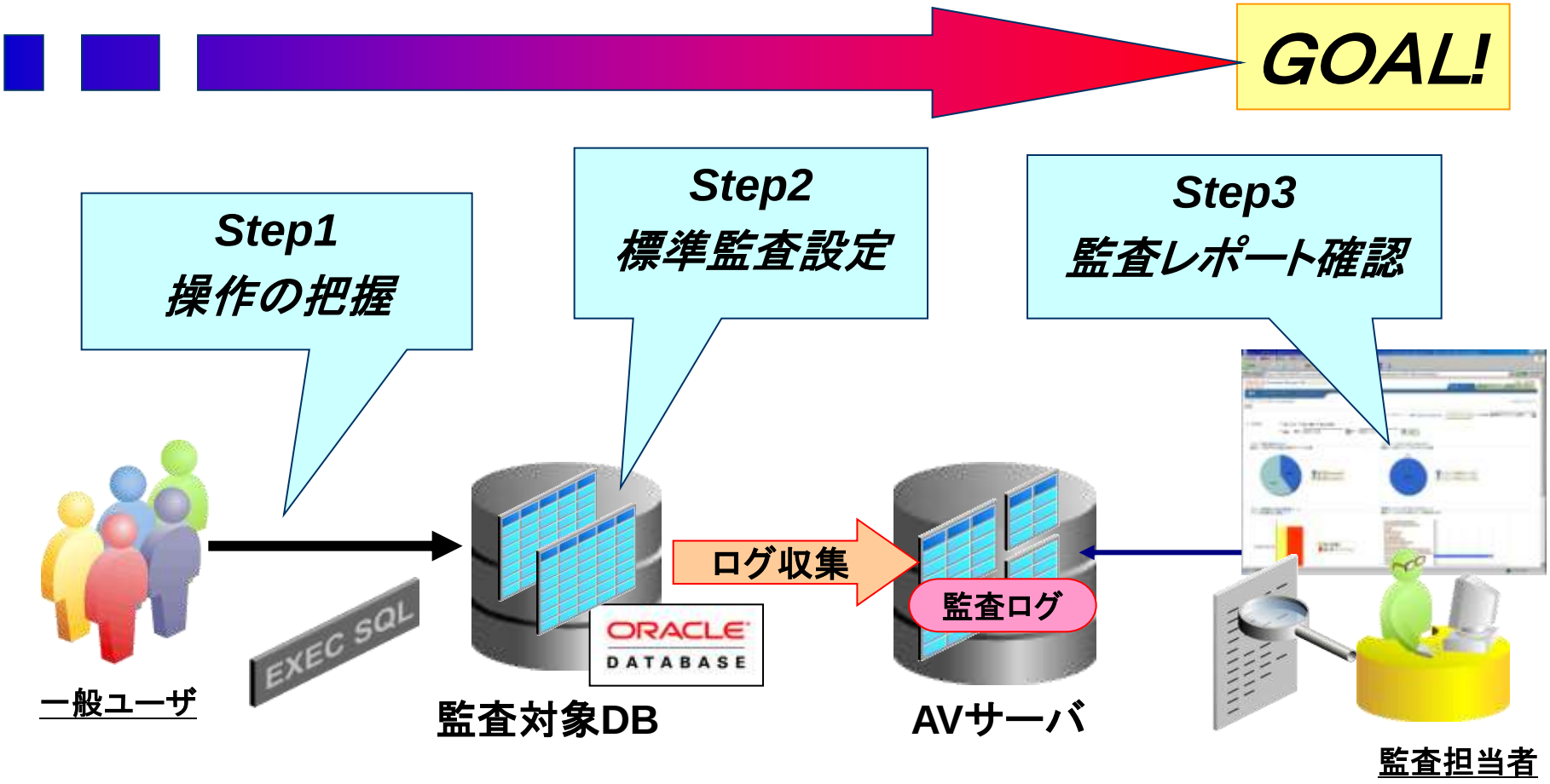
シナリオ1:データの変化に対する追跡

- オブジェクトに対して権限を持つユーザーはデータを書き換える可能性が常に存在。
- 本シナリオではデータそのものを変更する文をベースに監査・追跡を実施。



一般ユーザ　　監査対象DB

ユーザーに対するセキュリティ設定と追跡

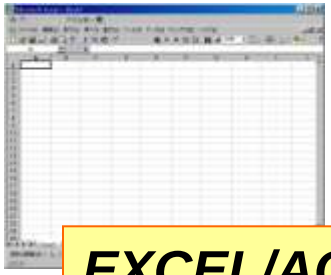


Step1:操作の把握

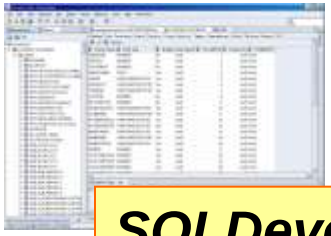
監査対象DB

ユーザは
様々なツールを用いて
アクセスを行う

*SQL*PLUS*



EXCEL/ACCESS

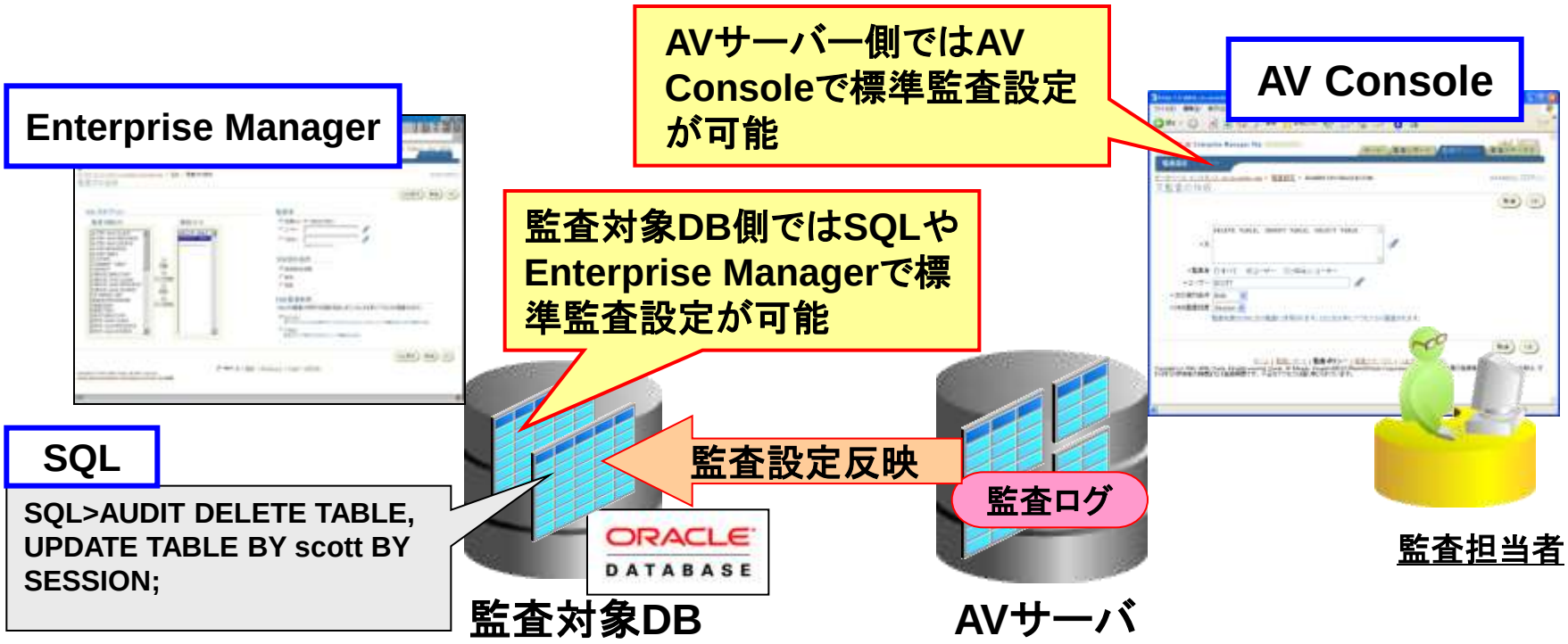


SQLDeveloper

一般ユーザ

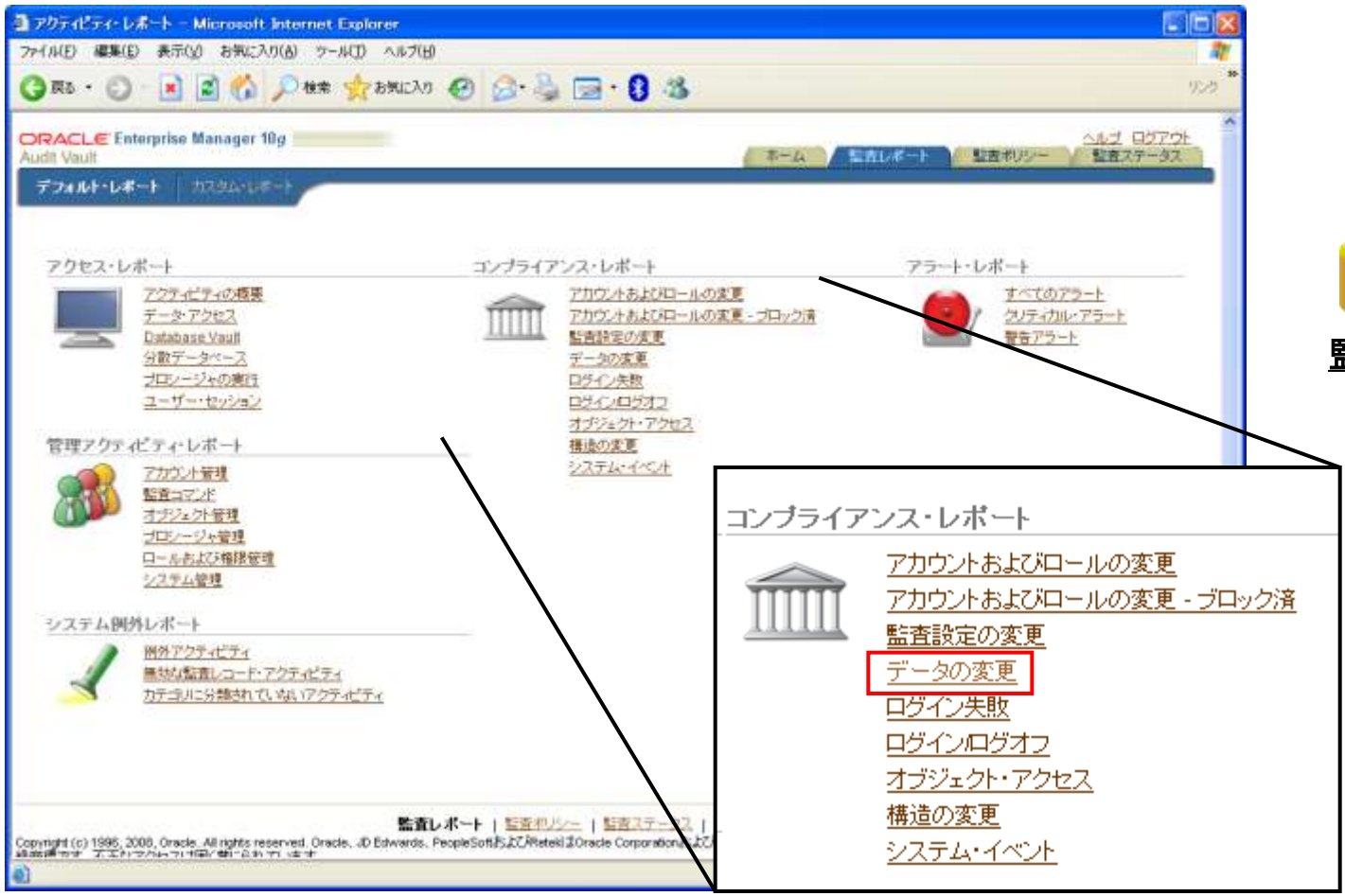
Step2:標準監査設定

- データを変更するSQL文（Delete,Update）を監査
  → 標準監査（文監査）参照（P62）
- 標準監査はAVサーバー側のAV ConsoleかDB側のSQLもしくはEnterprise Managerで設定を行うことが可能



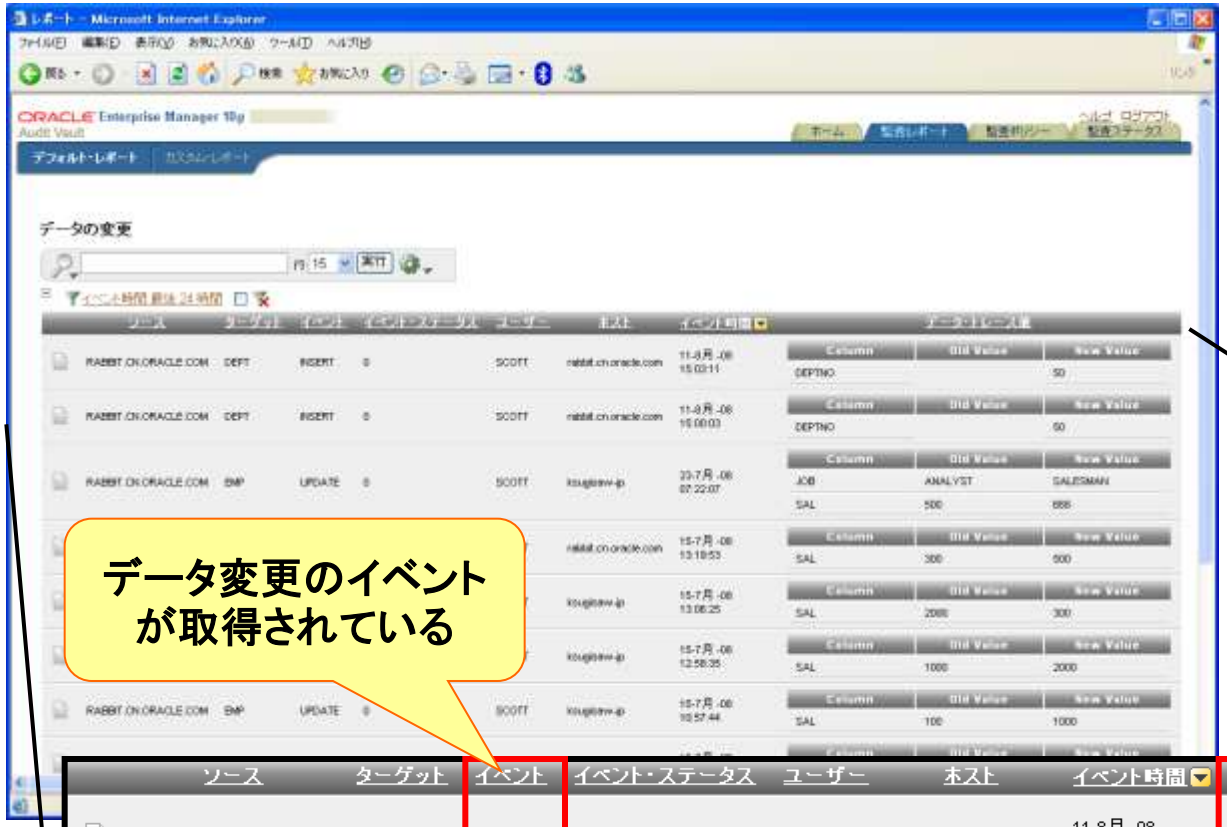
Step3:監査レポート確認①

- デフォルトで用意されているレポートテンプレートのうち「コンプライアンス・レポート」の「データの変更」を使用



監査担当者

Step3:監査レポート確認②



データ変更のイベントが取得されている

REDOログからの情報により変更前後の値も確認可能

ソース	ターゲット	イベント	イベント・ステータス	ユーザー	ホスト	イベント時間	データ・トレース値
RABBIT.CN.ORACLE.COM	DEPT	INSERT	0	SCOTT	rabbit.cn.oracle.com	11-8月 -08 15:03:11	Column: DEPTNO / Old Value: / New Value: 50
RABBIT.CN.ORACLE.COM	DEPT	INSERT	0	SCOTT	rabbit.cn.oracle.com	11-8月 -08 15:00:03	Column: DEPTNO / Old Value: / New Value: 50
RABBIT.CN.ORACLE.COM	EMP	UPDATE	0	SCOTT	ksugisaw-jp	23-7月 -08 07:22:07	Column: JOB / Old Value: ANALYST / New Value: SALESMAN Column: SAL / Old Value: 500 / New Value: 666

Step3:監査レポート確認③

詳細確認

単一行ビュー – Microsoft Internet Explorer

ファイル(F) 編集(E) 表示(V) お気に入り(A) ツール(T) ヘルプ(H)

戻る 検索 お気に入り リンク

ソース

ソース・タイプ	ORCLDB
ソース	RABBIT.CN.ORACLE.COM
ホスト	rabbit.cn.oracle.com
バージョン	10.2.0.3.0
IPアドレス	10.182.112.117

イベント

Audit Vault時間	11-8月 -08 15:03:12
イベント時間	11-8月 -08 15:03:11
イベント・ステータス	0
イベント	INSERT
カテゴリ	DATA ACCESS
ソース・イベント	2

ターゲット

所有者	SCOTT
ターゲット	DEPT

クライアント/ユーザー情報

ユーザー	SCOTT
OSユーザー	oracle
ホスト	rabbit.cn.oracle.com
端末	14627
プログラム名	sqlplus@rabbit.cn.oracle.com

文

SCN	16863253
オブジェクトID	51249

セッション

プロキシ・セッションID	117

その他

セッションID	125265
トランザクションID	7.41.15452

データ・トレース値

Column	Old Value	New Value
DEPTNO		50

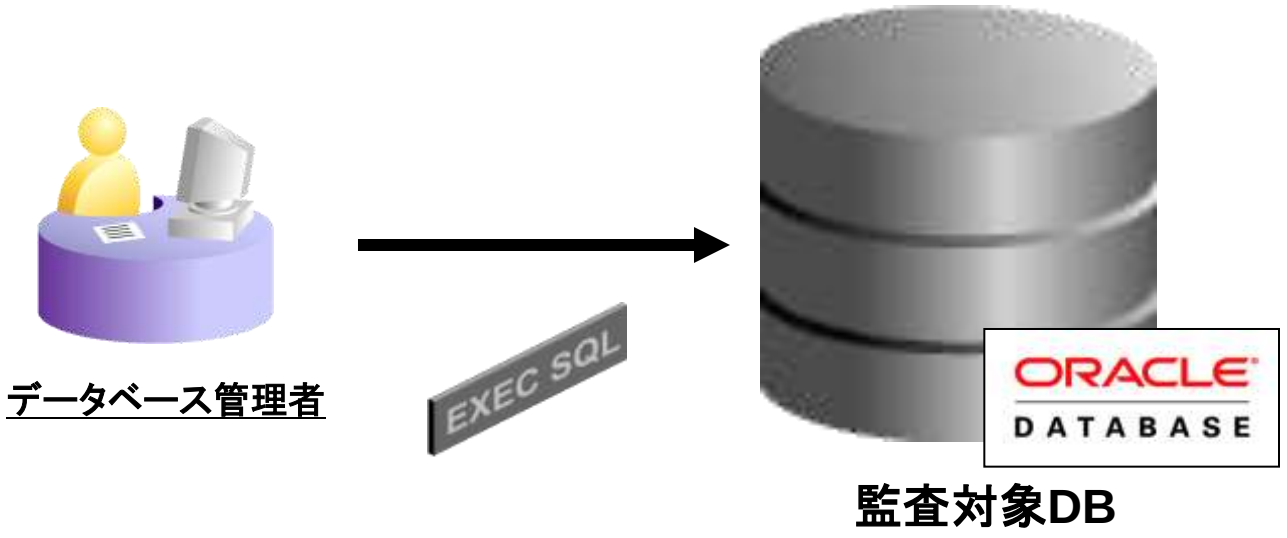
ページが表示されました イントラネット

アプリケーションを使用していれば記録されています

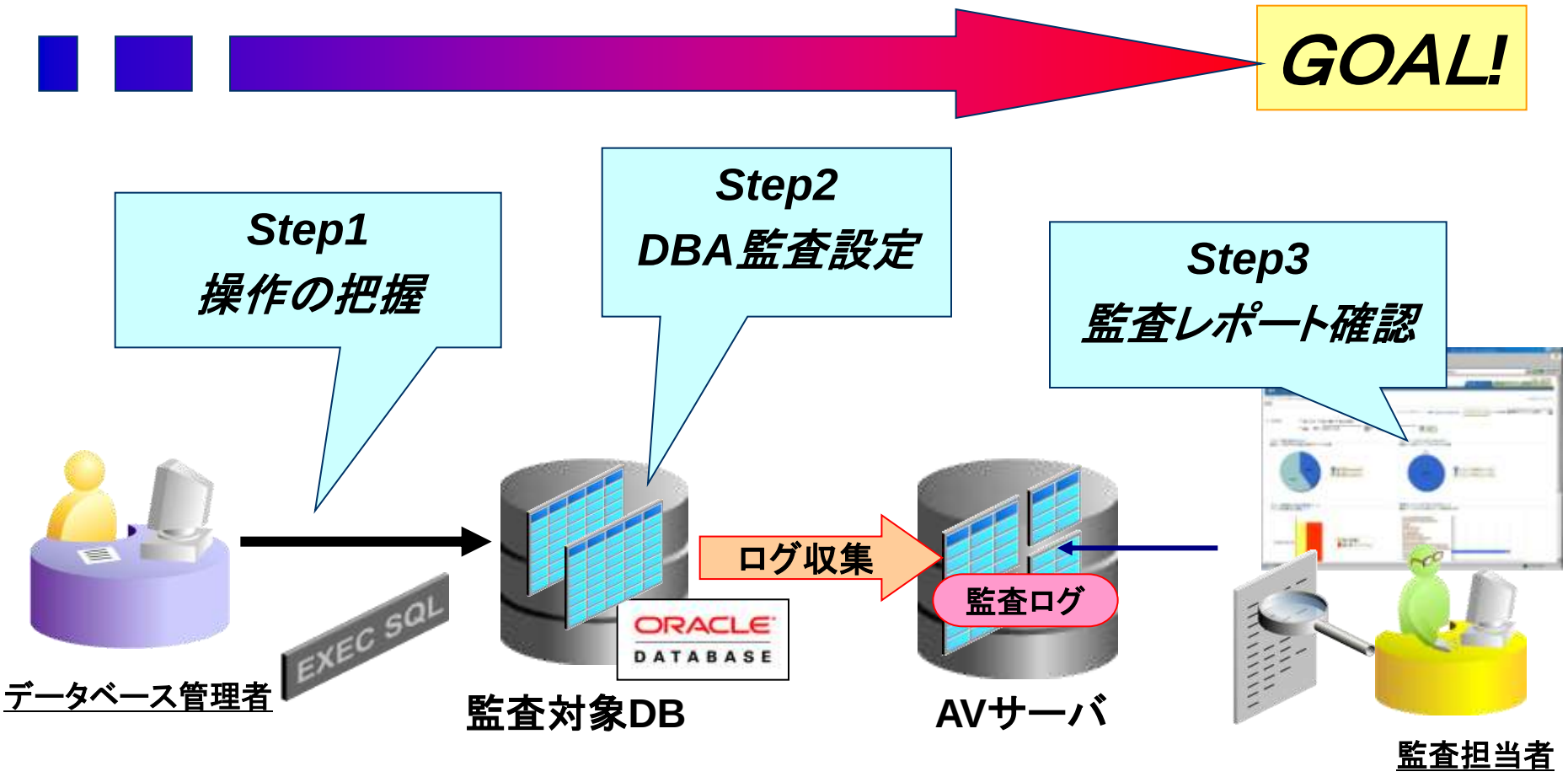
Ex: msqry.exe (Excelなど)

シナリオ2 管理者に対する監査と追跡

- 管理者(SYSDBA権限者）はシステム運用にかかわる全権限を持ち、ユーザーデータの改竄、また監査ログそのものを改竄する可能性も否定できない。



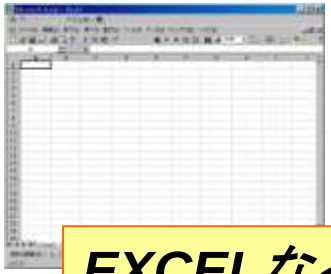
管理者に対するセキュリティ設定と追跡



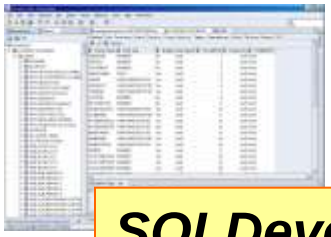
Step1:操作の把握

管理者は
様々なツールを用いて
管理業務を行う

SQL*PLUS



EXCELなど

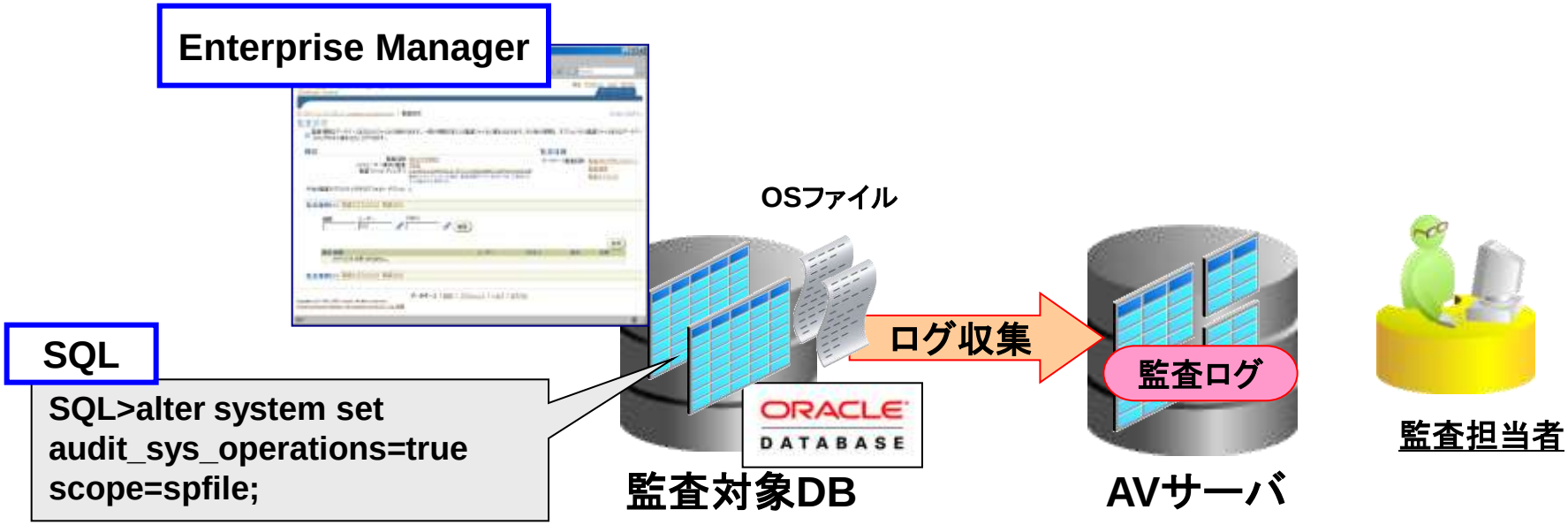


SQLDeveloper

データベース管理者

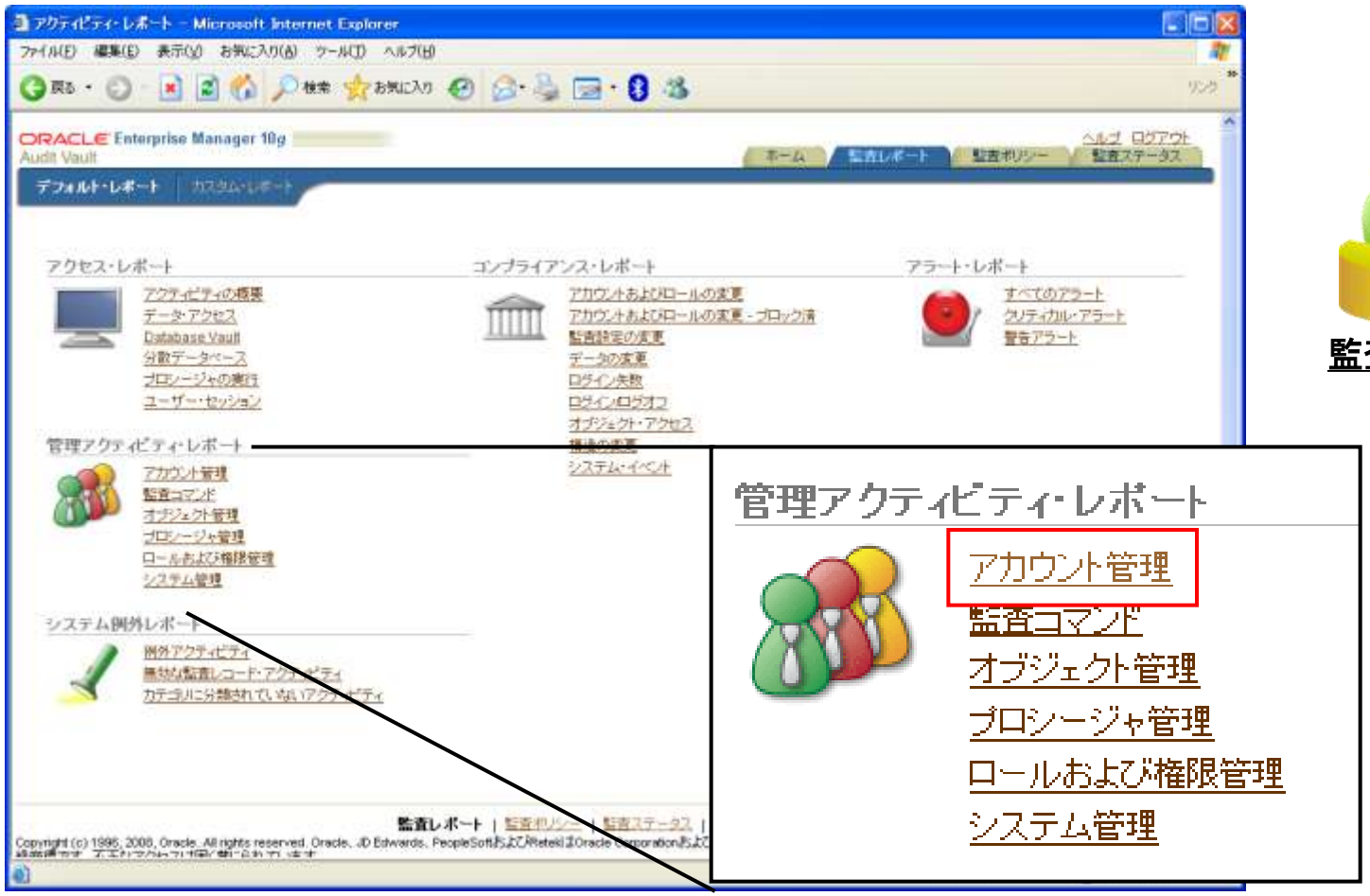
Step2:DBA監査設定

- 管理者のデータベースに対する操作をすべて監査
  → DBA監査参照（P57）
- DBA監査はDB側のSQLもしくはEnterprise Managerで設定を行うことが可能（パラメータの変更）
- DBA監査のログはOS上のファイルとして出力される



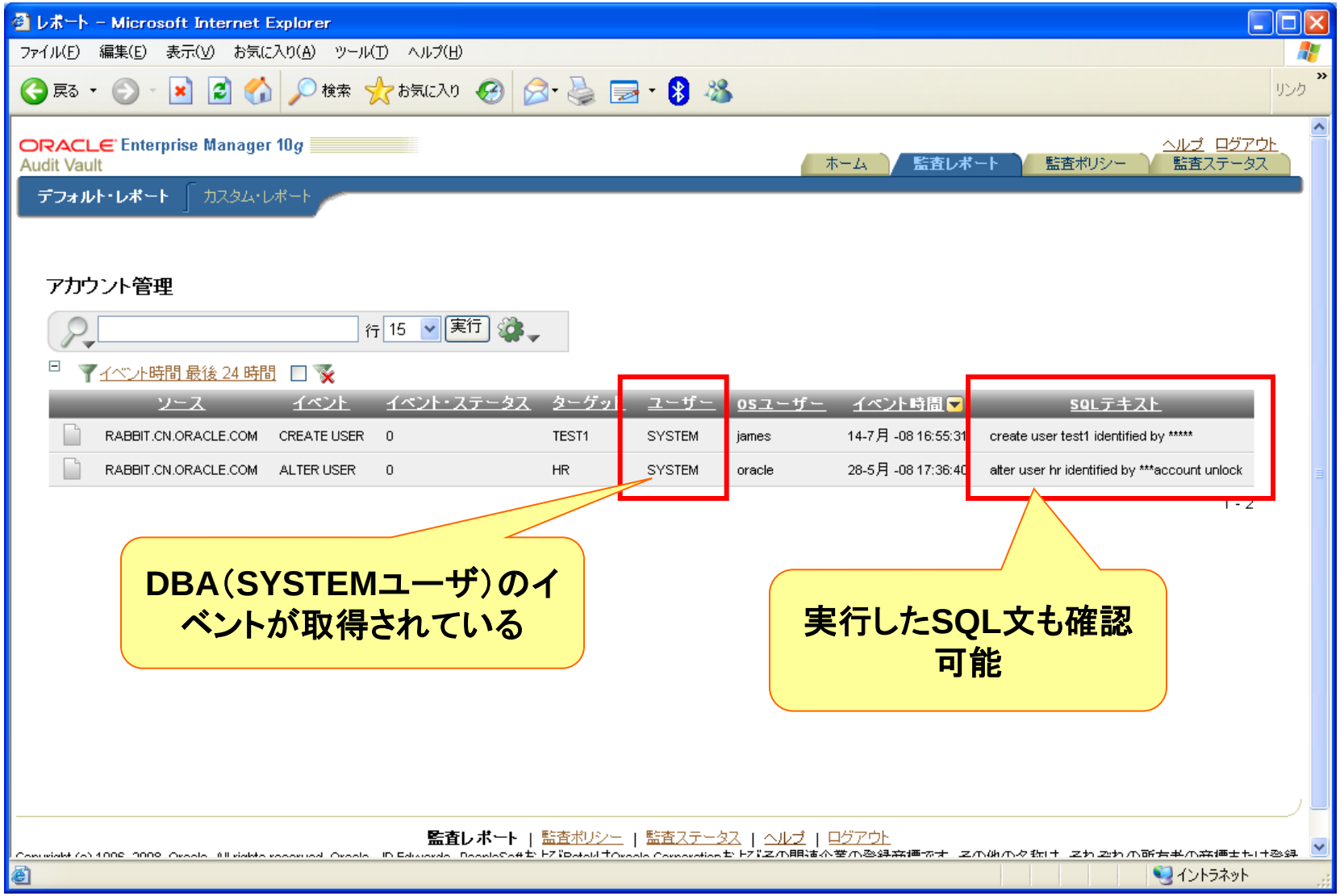
Step3:監査レポート確認①

- デフォルトで用意されているレポートテンプレートのうち「管理アクティビティ・レポート」の「アカウント管理」を使用



監査担当者

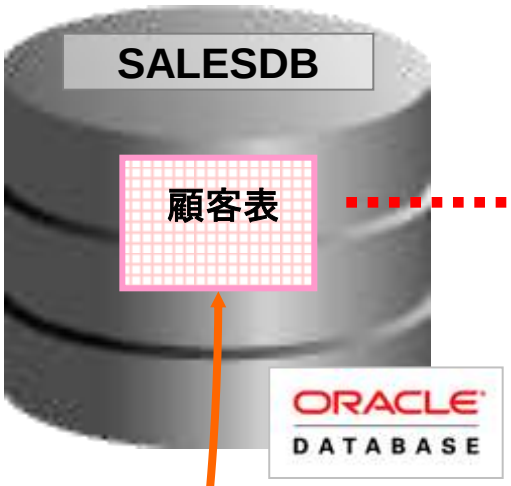
Step3:監査レポート確認②



シナリオ3 重要情報に対する監査対策

監査対象データベース

- オンライン・ショッピングサイトのシステム
- 顧客表にはサイト会員の個人情報を含む



不正アクセス者

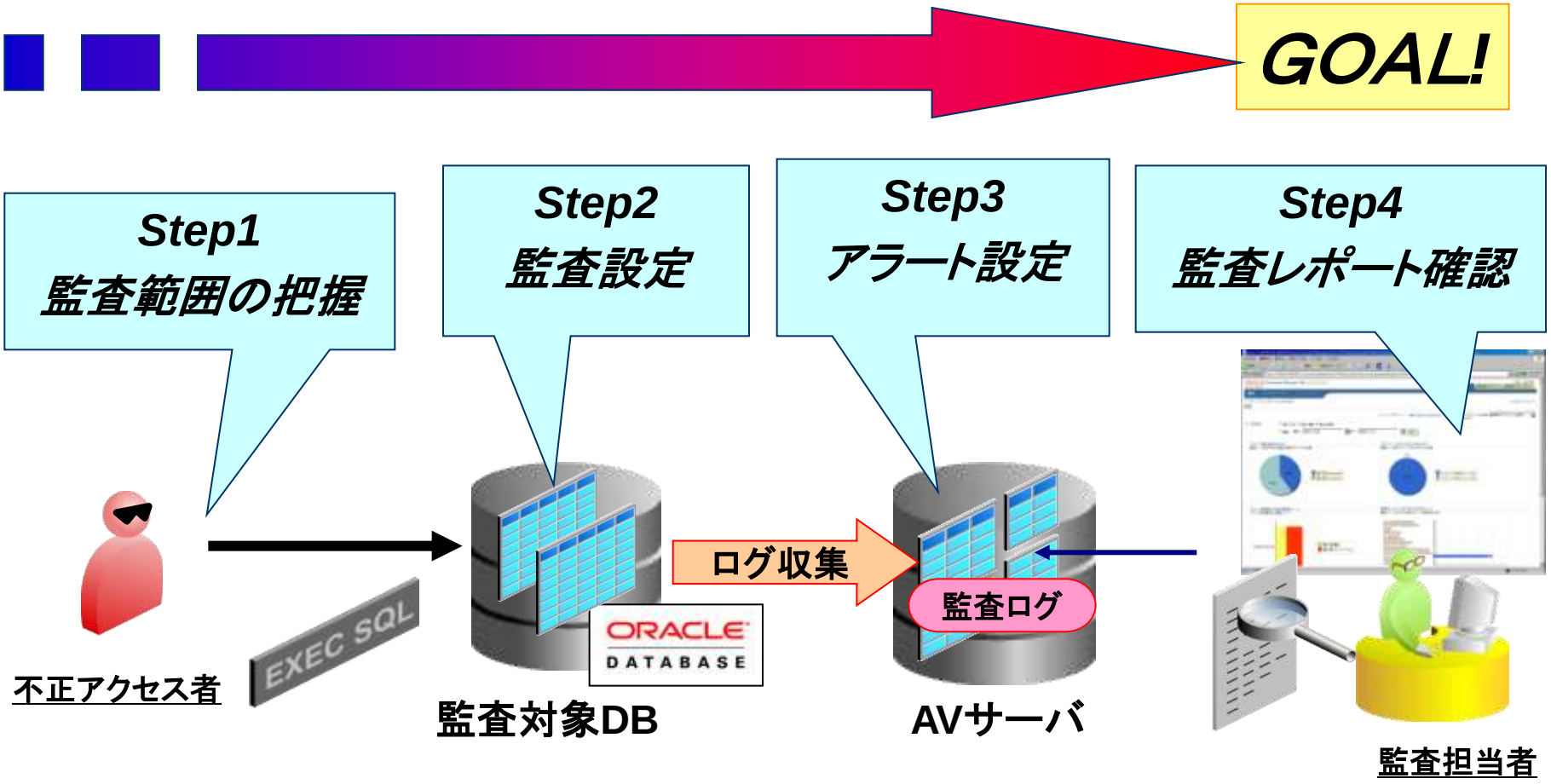
- 深夜に特権ユーザーのアカウントで侵入
- 山田太郎 の個人情報を盗む
- 山田太郎 のログイン用パスワードをリセット

Audit Vault サーバー

監査担当者

- アラートから異常を検知
- レポートから犯人を追跡調査

監査の設定と手法



Step1:監査範囲の把握

SALESDB

金額は重要だが、特定できなければ意味のない情報

売上表

USERID	ITEM	AMOUNT	TOTAL
X092124	A01	3	300,000
X092125	B01	4	420,000

扱う商品がわかってもあまり意味がない

商品マスター

ITEMNAME	DESC	PRICE
A01	足つぼマッサージ	100,000
B01	フットバス	105,000

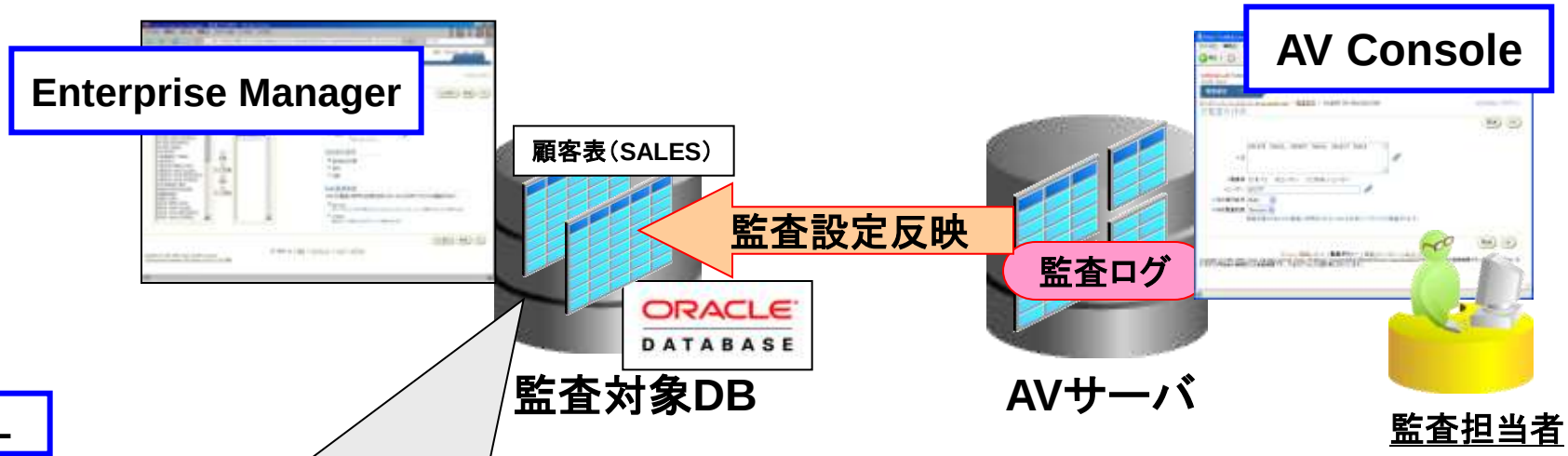
顧客表（SALES）

USERID	LASTNAME	FIRSTNAME	ADDRESS	TEL	EMAIL
X092124	山田	太郎	茨城県守谷市・・	0297-XX-0000	Yuto@XXXX.net
X092125	北条	早雲	神奈川県小田原市・・	046-XXXX-0000	Soun@XXXX.net

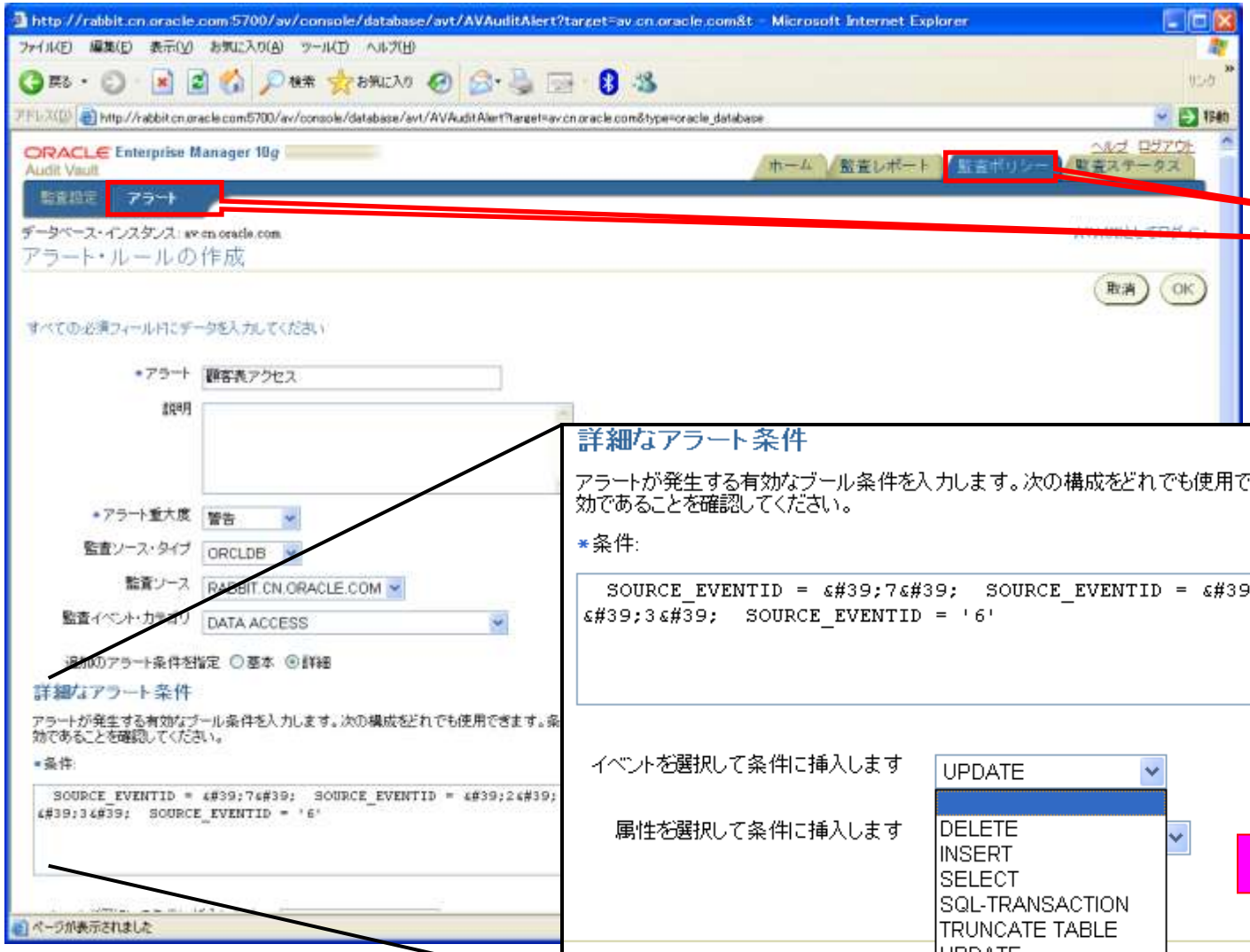
固有の情報が含まれ扱いに対してもっとも重要な情報

Step2:監査設定

- 特定表（Sales）に対する操作を監査
  → 標準監査（オブジェクト監査）参照（P63）
- FGA監査により列単位での監査も実現可能
  → FGA監査参照（P65）
- 標準監査、FGA監査はAVサーバー側のAV ConsoleかDB側のSQLもしくはEnterprise Managerで設定を行うことが可能



Step3:アラート設定

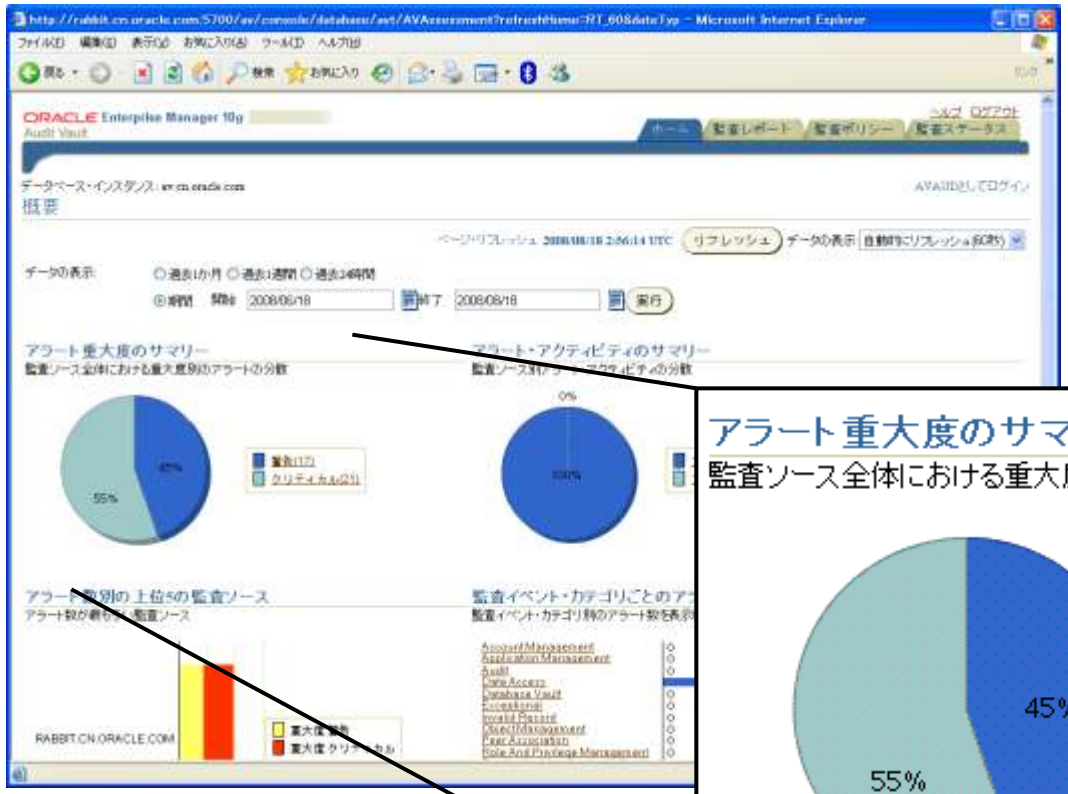


監査ポリシーのアラートの設定

監査担当者

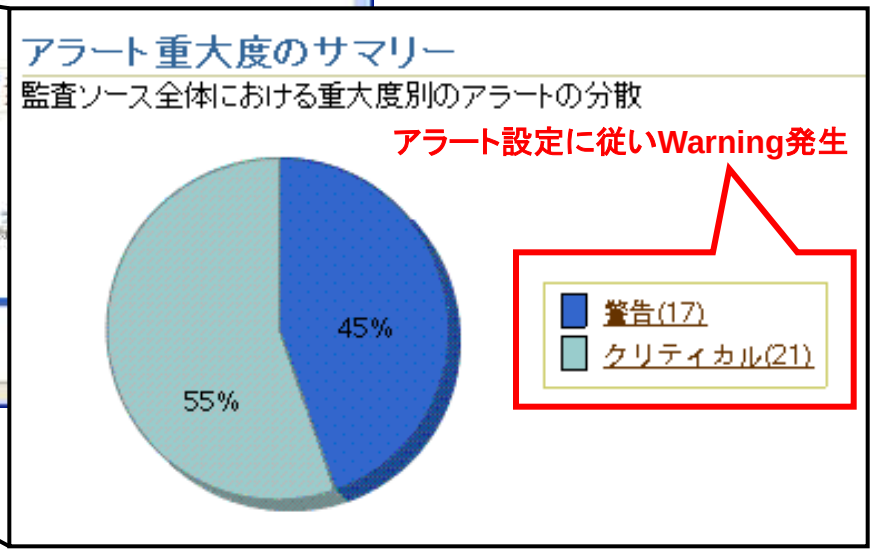
Step4:監査レポート確認①

- アラート設定したイベントが発生すると監査担当者に通知

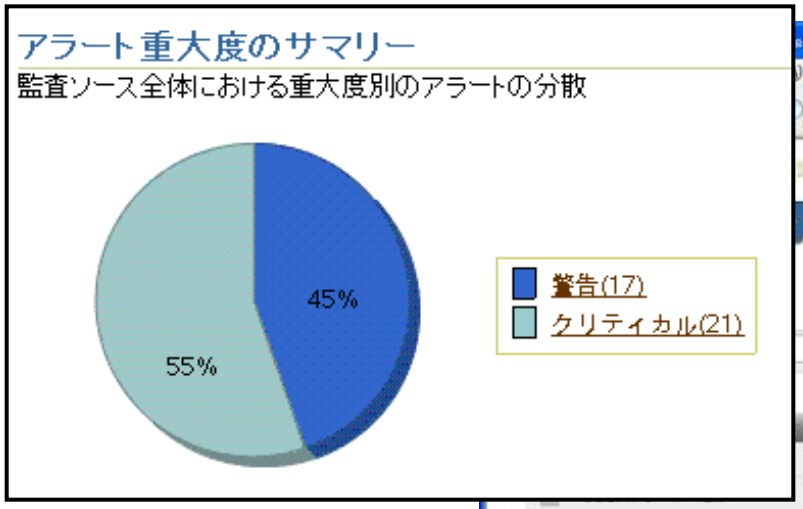


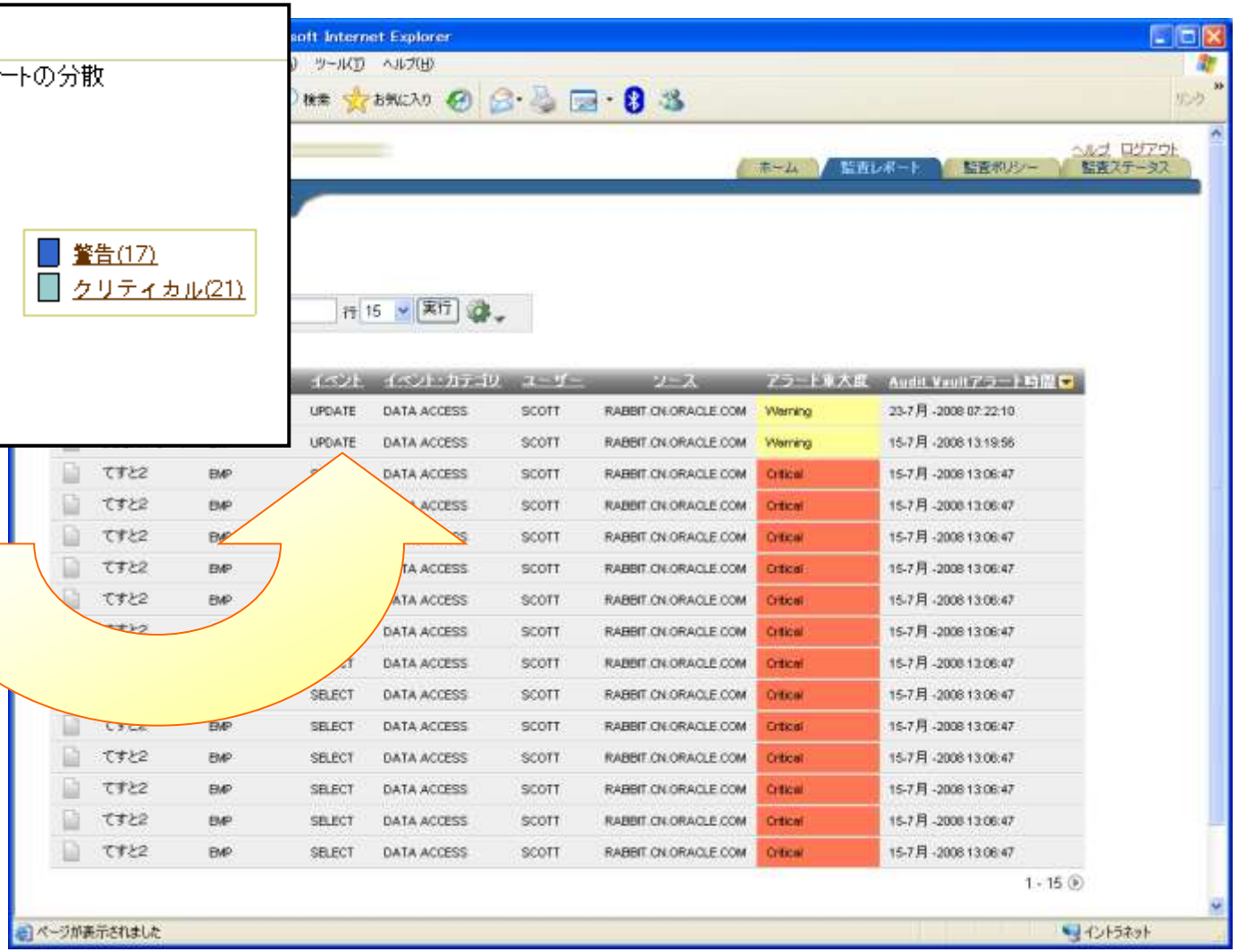
ダッシュボード（Pull型）
やメール通知（Push型）
での確認が可能

監査担当者



Step4:監査レポート確認②





監査担当者

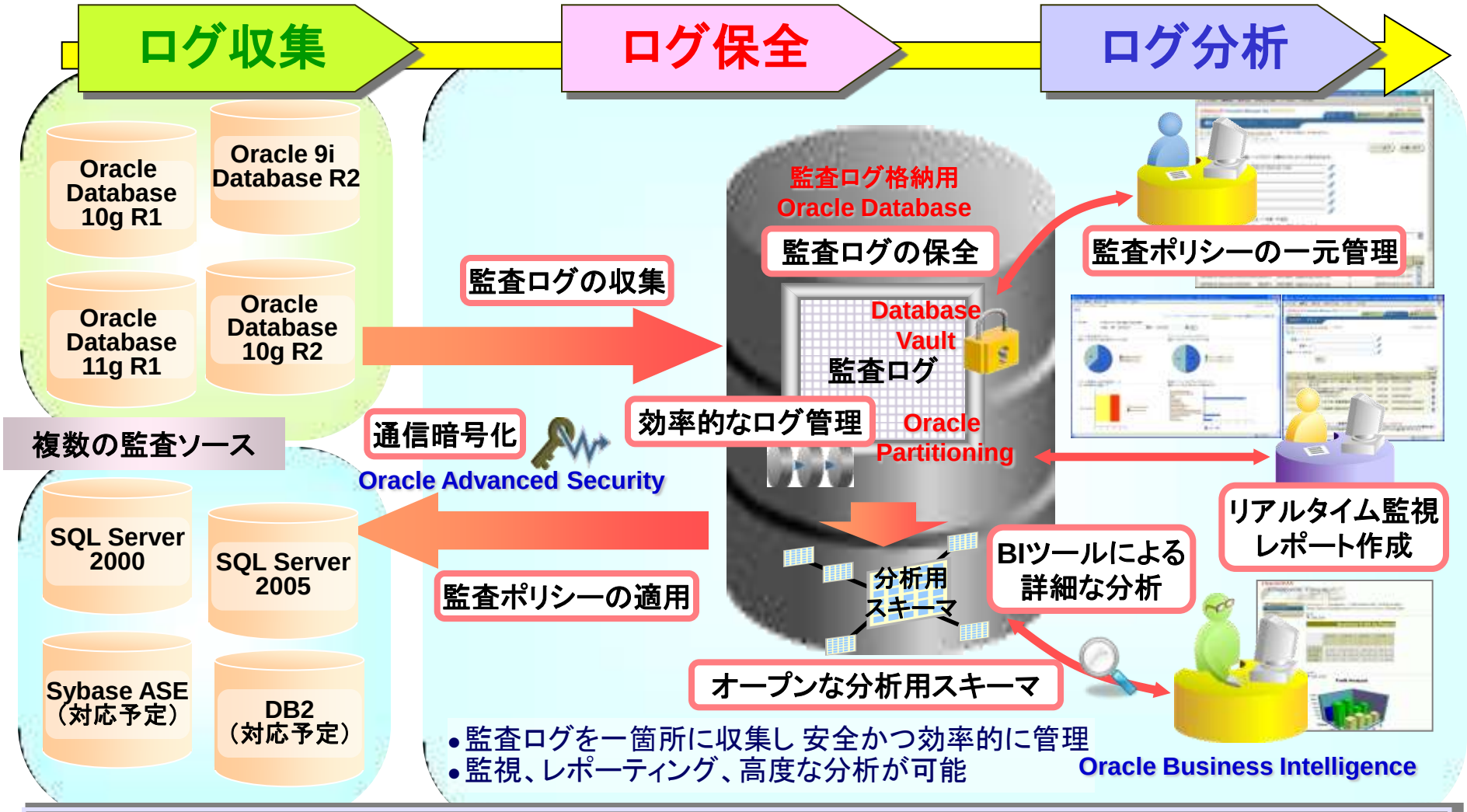
Step4:監査レポート確認③

監査担当者

Agenda

- Oracle Database監査機能
- ユーザ特定のポイント
- Oracleのセキュリティ・ソリューション
- Appendix
  - ログ監査の実践例
  - Oracle Audit Vault

Oracle Audit Vault



監査ログの収集、保全、分析を実現する エンタープライズ統合監査ログウェアハウス

Oracle Audit Vault 主な特徴

ログ収集

- **確実な監査**
  - Oracle Database の監査機能で取得した監査ログを収集するため、取りこぼすことがありません。
- **監査ポリシーの一元管理**
  - 複数の監査ソース・データベースの監査ポリシーを一元管理(確認・変更・適用)することが可能です。

ログ保全

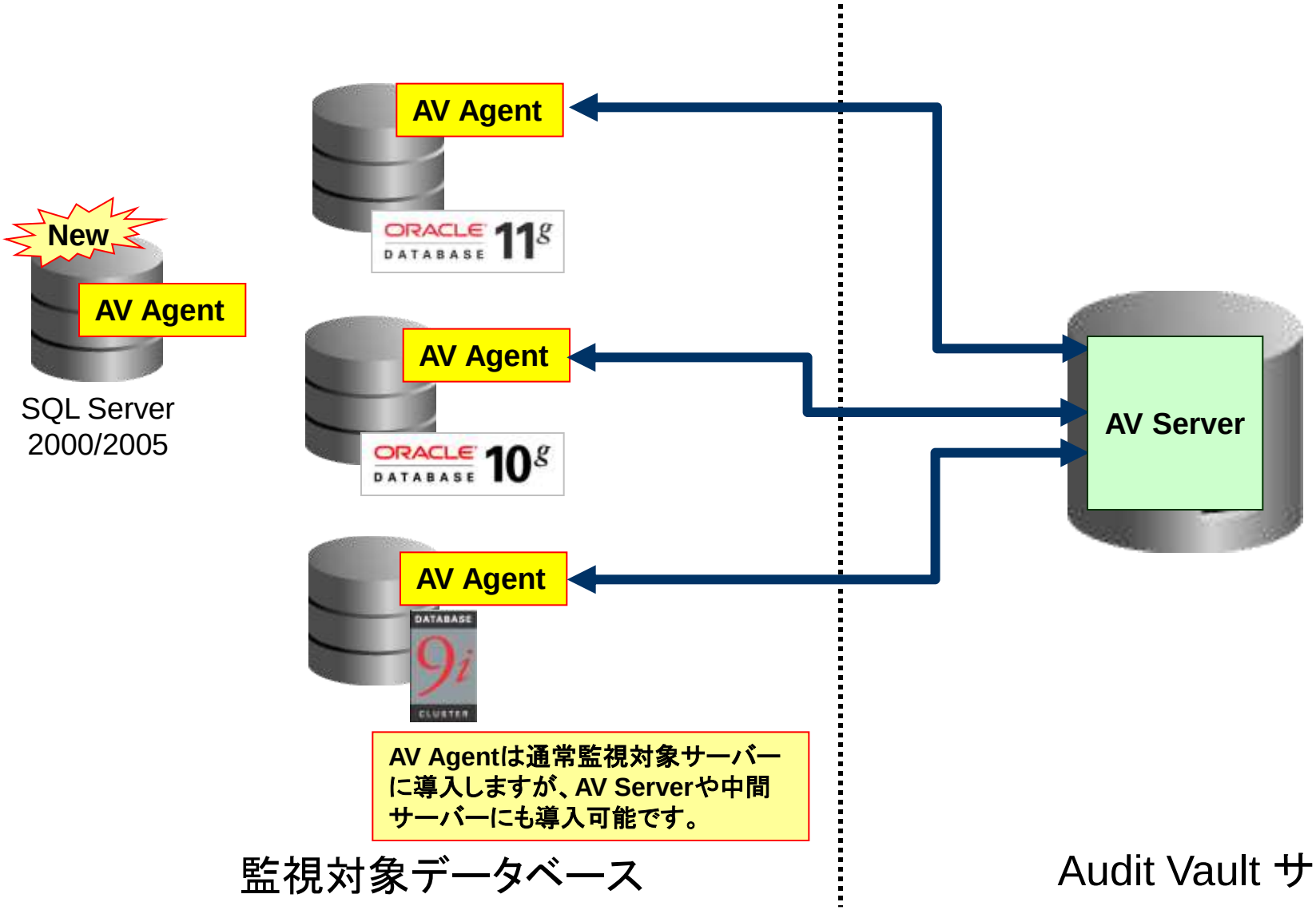
- **複数監査ソースの監査ログの一元管理**
  - 複数の監査ソース・データベースで取得した各々の監査ログを一箇所に収集し、一元的に管理します。
- **監査ログの安全かつ効率的な管理**
  - 一箇所に収集した監査ログは、管理者に対してもアクセス制御、通信とバックアップの暗号化機能、および Partitioning による拡張性を備えることで、安全かつ効率的な管理が可能です。

ログ分析

- **モニタリング、レポーティング**
  - 疑わしい操作をリアルタイムに監視するアラート機能、収集した監査ログから用途に応じた情報を抽出するレポーティング機能を実装しています。
  - Oracle BI と連携することによって、レポーティング機能よりも詳細かつ高度な分析を行うこともできます。

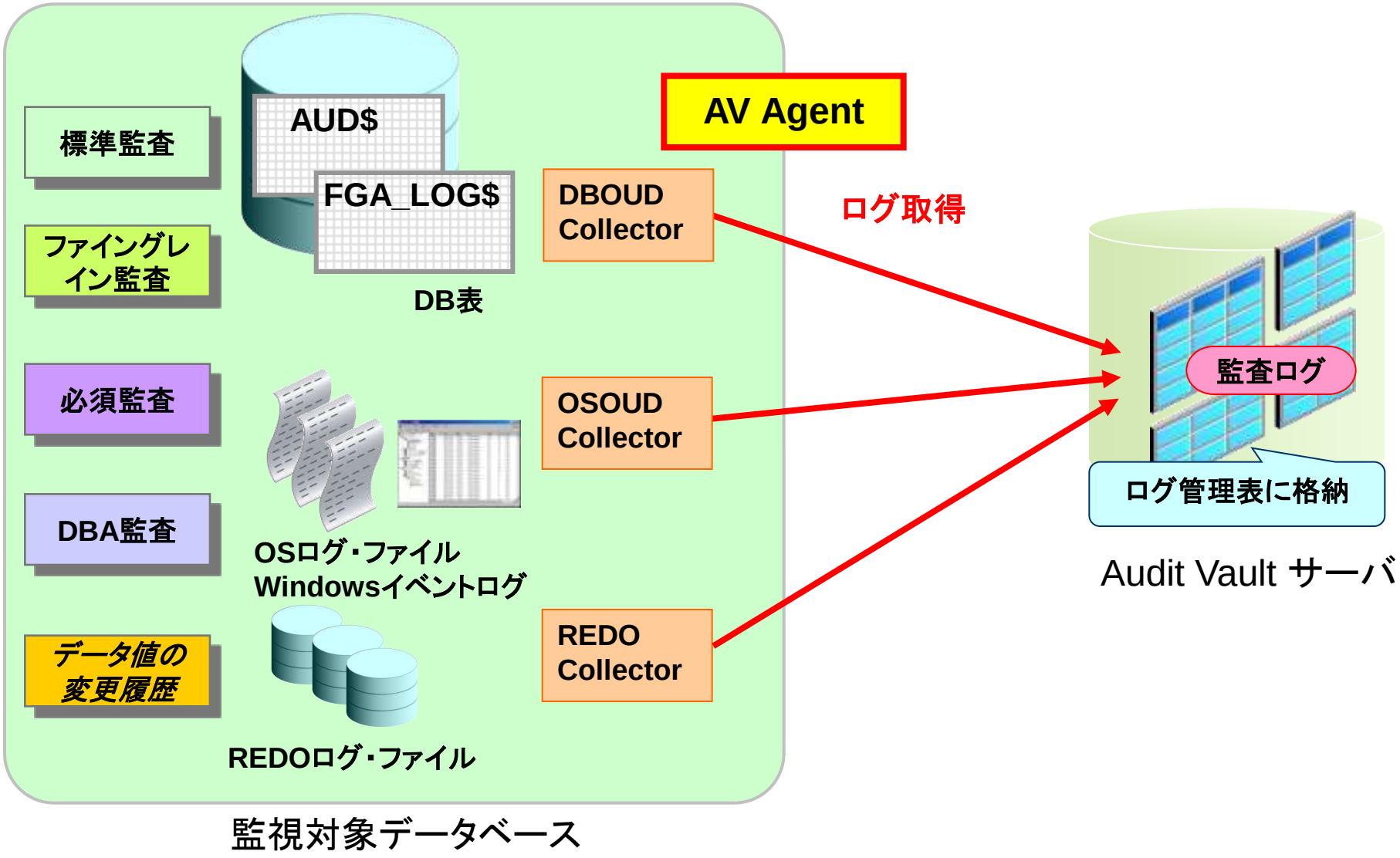
監査対象データベース

ログ収集



点在するログ取得の自動化

ログ収集



取りこぼしなくログ収集

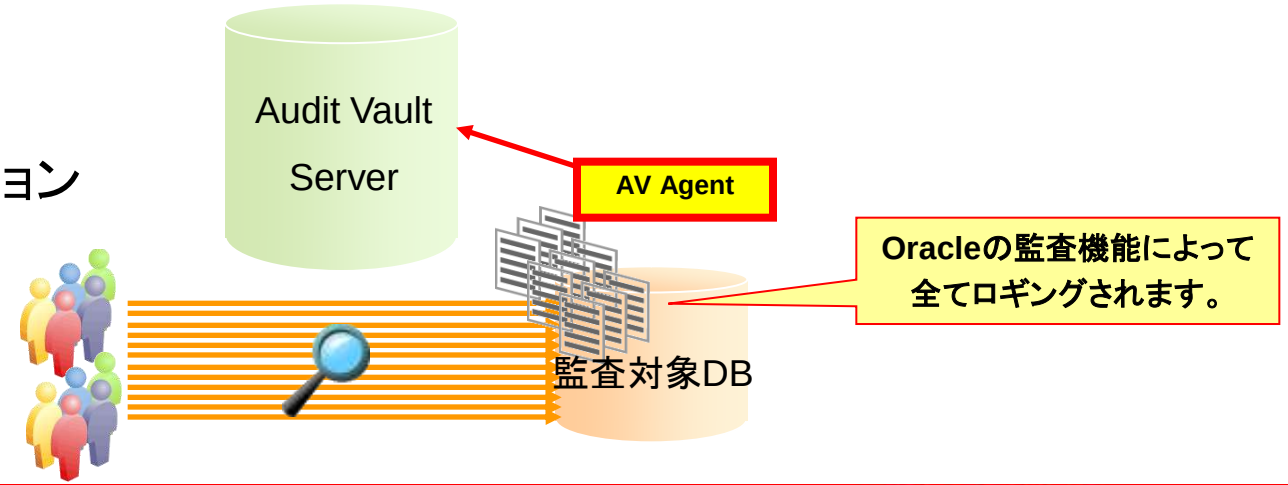
ログ収集

- Oracleの監査機能によって全て収集可能
- 大量トランザクション発生時でもログの取りこぼしが発生しない

5－(2)－②－ロ	連続したモニタリングでないと、不正等を検出できない。	モニタリングのログ等の情報収集は連続して収集されている。	・モニタリング対象として選んだログが、24 時間 365 日収集されていることを確かめる。 ・内部監査部門等が実施したログ収集の分析を行っているか確かめる。

経済産業省「システム管理基準 追補版（財務報告に係るIT 統制ガイダンス）

大量トランザクション発生時



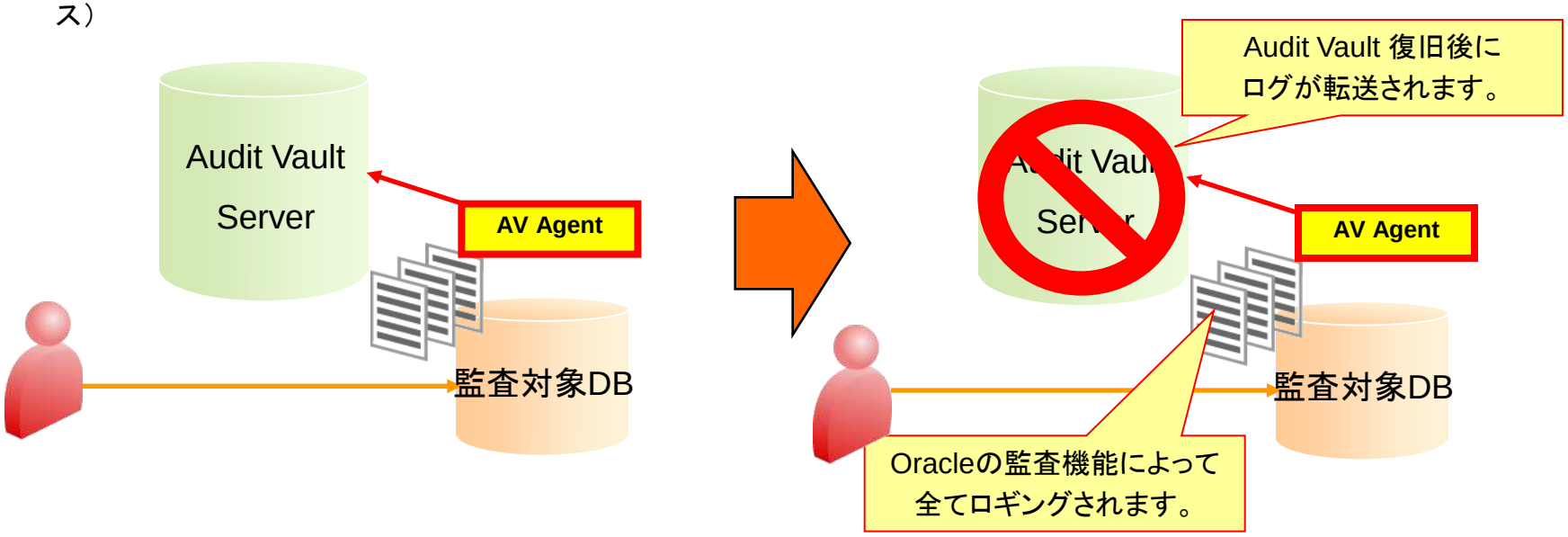
24時間365日のログ収集

ログ収集

- 万が一Audit Vaultサーバが停止してもログの収集を保証
- AV Serverのクラスター構成（RAC）により高可用性を実現可能

5－（2）－②－ロ	連続したモニタリングでないと、不正等を検出できない。	モニタリングのログ等の情報収集は連続して収集されている。	・モニタリング対象として選んだログが、24 時間 365 日収集されていることを確かめる。 ・内部監査部門等が実施したログ収集の分析を行っているか確かめる。

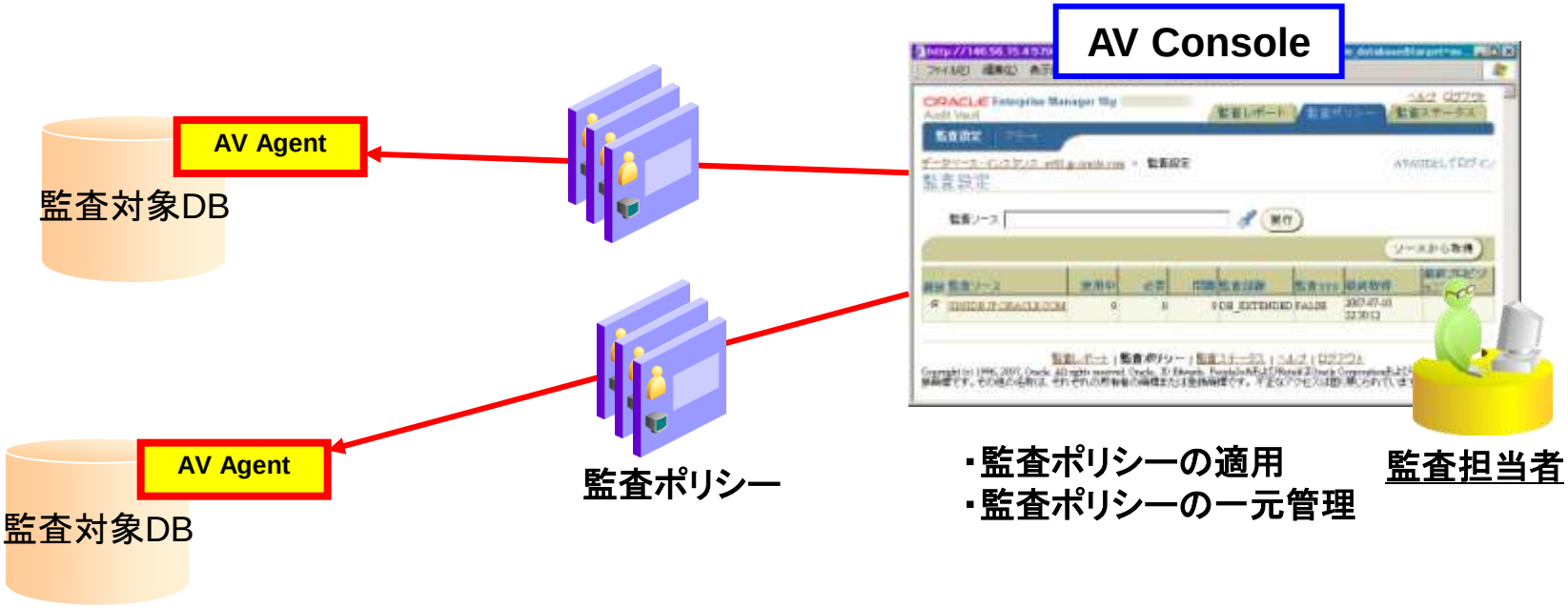
経済産業省「システム管理基準 追補版（財務報告に係るIT 統制ガイダンス）



監査ポリシーの一元管理

ログ収集

- 監査ソース・データベースの監査ポリシー（設定内容）を、Web管理画面（AV Console）から一元的に管理
- 監査ポリシーの変更・追加、ソース・データベースへの適用
- プロビジョニング機能による即時適用の実現



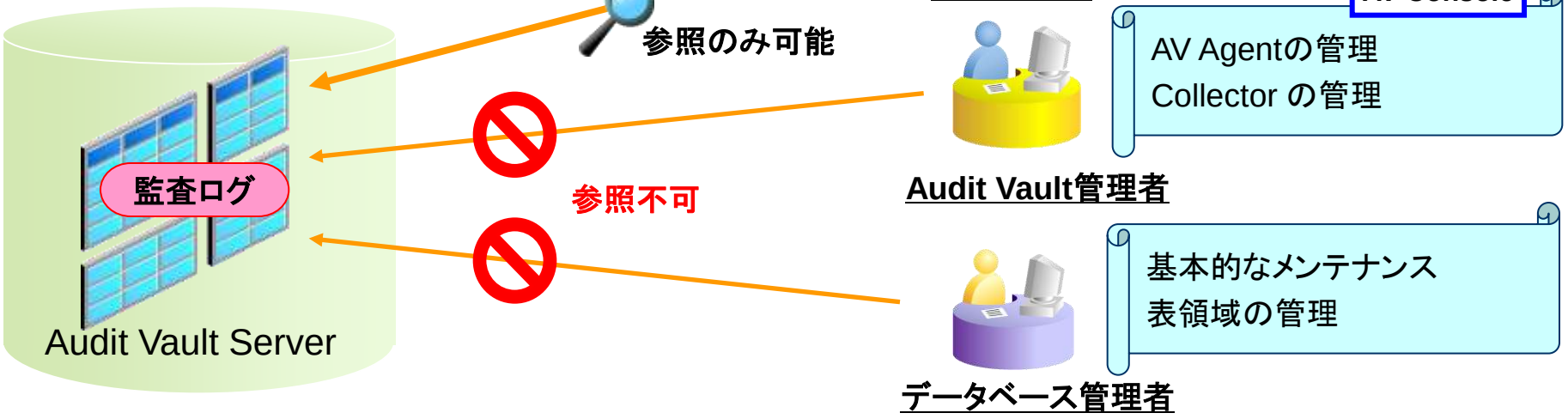
監査ログの改竄防止

ログ保全

- 強力なログ保全機能により監査ログを管理者からも保護
- 監査担当者も参照のみ（編集・削除は行えない

3-(2)-①-ハ	情報システムが処理するデータの信頼性が保証されない。	情報システムとデータ処理のログが取得されて、ログファイルの完全性、正確性、正当性を保証される（ログが改ざんされずに記録され、保管されている）。	ログの記録や保管に際して、改ざんや削除ができないかについて確かめる。 （例えば、情報システムとデータ処理に関する操作状況を調査する。調査した時間帯のログのサンプルを取得する。入手したサンプルをもとに、取得されたログの完全性と正確性を確かめる）。

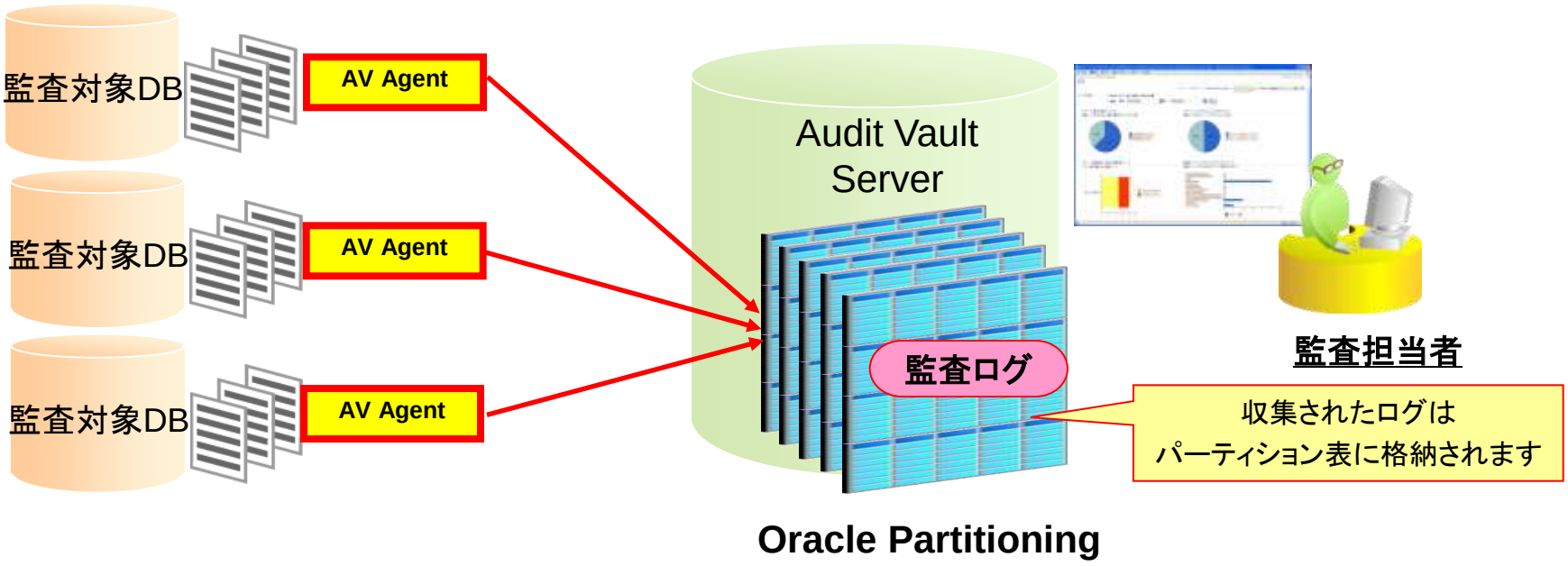
経済産業省「システム管理基準 追補版（財務報告に係るIT 統制ガイダンス）



大量ログの効率的な管理

ログ保全

- 大量に蓄積されるログの管理にOracle Partitioning機能を内蔵
  - 大規模な表やインデックスを内部的に複数の領域に分割
  - 分割しても「1つの表」として扱う
  - 3つのメリット（検索の高速化、管理性、可用性）



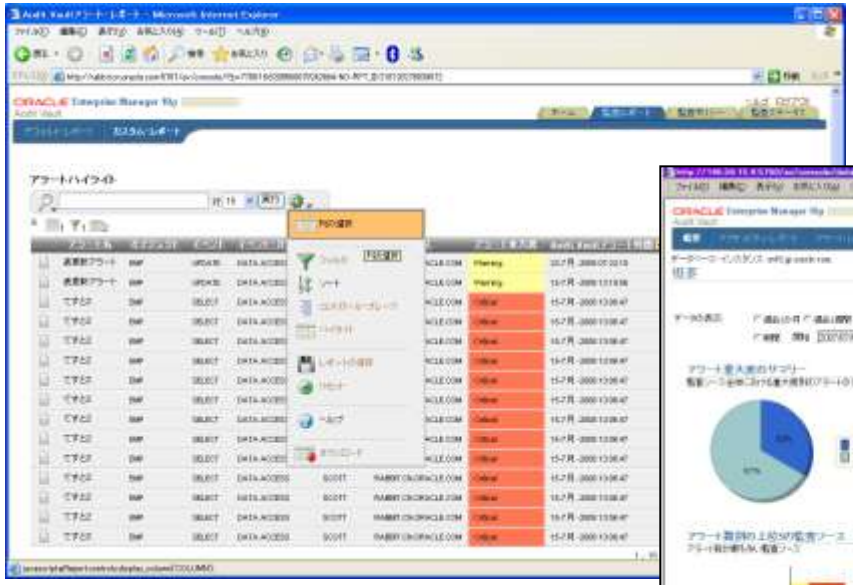
柔軟なレポート機能

ログ分析

- Web上でのレポート参照・作成
- 事前準備された定型レポート（システム管理・データアクセス・例外等）
- 任意の重要な監査イベントのアラート表示設定

5-(2)-②-イ	IT 全般統制についてモニタリング機能がないため、不正や誤り等を検出できない。	IT の日常的なモニタリングに関するポリシや手続、ルールが定められ、これに基づいてモニタリング活動が実施され、記録が保存されている。	・日常的なモニタリングについて適切なポリシや手続があるか確かめる ・ポリシや手続に基づいて、モニタリングが行われていることを内部監査部門等が確かめる。（例えば、ログ等の収集と分析が行われていることを確かめる）。

経済産業省「システム管理基準 追補版（財務報告に係るIT 統制ガイダンス）



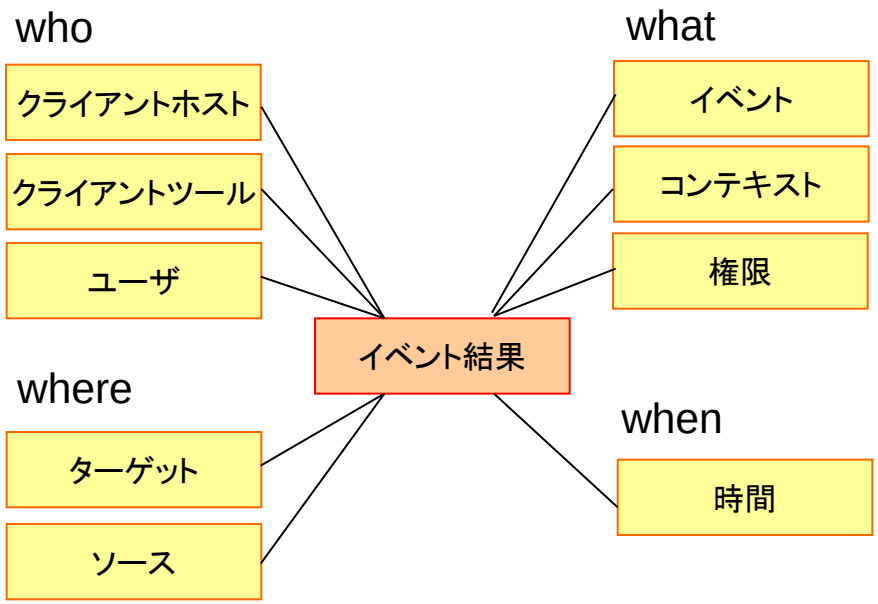
レポート作成
アラート表示

監査担当者

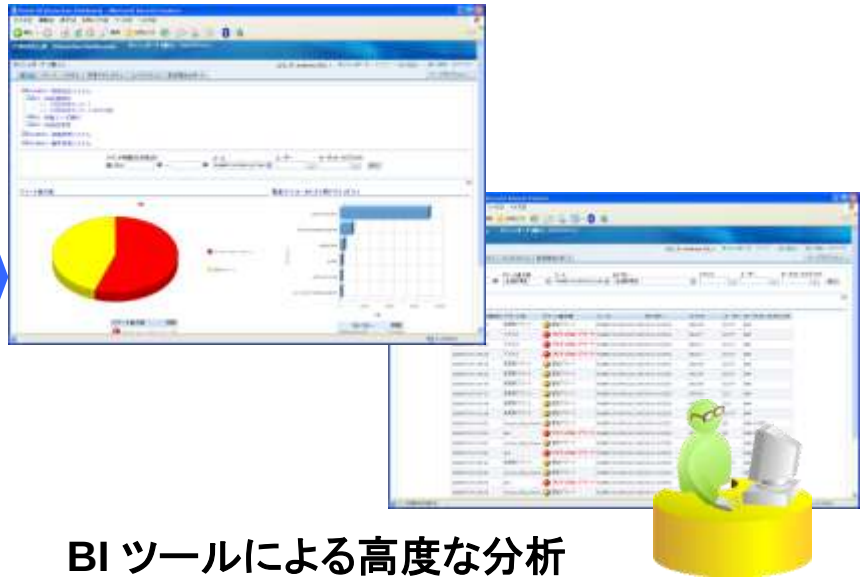
BIツールによる分析

ログ分析

- Audit Vault Server のリポジトリ・データベースに収集した監査ログは、レポーティング機能によるレポートの参照だけでなく、高度な分析にも活用することが可能
- ウェアハウス用のスキーマは、予めスタースキーマ 構成となっているため、Oracle BIツールと容易に組み合わせることが可能



Audit Vault ウェアハウス用スキーマ構造



BI ツールによる高度な分析

監査担当者