Oracle Direct Seminar

ORACLE®

データベース・セキュリティを見直す7つの方法

日本オラクル株式会社
Oracle Direct

Oracle Direct Seminar

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。

Oracle、PeopleSoft、JD Edwards、及びSiebelは、米国オラクル・コーポレーション及びその子会社、関連会社の登録商標です。その他の名称はそれぞれの会社の商標の可能性があります。

Copyright© 2010, Oracle. All rights reserved.

見直すべき7つの項目

1. 初期設定
2. 認証
3. 権限管理
4. 特権ユーザ管理
5. 不正アクセス
6. 暗号化
7. 監査

無償技術サービスOracle Direct Concierge

- Oracle Database バージョンアップ支援
- Oracle 構成相談(Sizing)サービス
- パフォーマンス・クリニック・サービス
- SQL Serverからの移行アセスメント
- DB2からの移行支援サービス
- Sybaseからの移行支援サービス
- MySQLからの移行相談サービス
- PostgreSQLからの移行相談 サービス
- Accessからの移行アセスメント
- Oracle Developer/2000 Webアップグレード相談
- 仮想化アセスメントサービス
- ビジネスインテリジェンス・エンタープライズ エディション・アセスメントサービス
- 簡易業務診断サービス

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

Copyright© 2010, Oracle. All rights reserved.

デフォルト・ユーザーと初期パスワード

- デフォルト・ユーザーがそのまま初期パスワードを使用しているかどうかを確認
  - ～10g　DBA_USERSに格納されているパスワード・ハッシュを比較する
  - 11g～　DBA_USERS_WITH_DEFPWDビューを使用

- 初期パスワードを使用しているデフォルトユーザは、パスワード変更を検討

～10g 初期パスワードを使用しているデフォルト・ユーザーを確認するスクリプト

```
select username "User(s) with Default Password!", account_status "Status"
 from dba_users
 where password in
('E066D214D5421CCC','24ABAB8B06281B4C','72979A94BAD2AF80','9AAEB2214DCC9A31','C252E8FA117AF049',
'A7A32CD03D3CE8D5','88A2B2C183431F00','7EFA02EC7EA6B86F','9B616F5489F90AD7','4A3BA55E08595C81',
'F894844C34402B67','3F9FBD883D787341','79DF7A1BD138CF11','7C9BA362F8314299', '88D8364765FCE6AF',
'F9DA8977092B7B81','9300C0977D7DC75E','A97282CE3D94E29E','AC9700FD3F1410EB','E7B5D92911C831E1',
'AC98877DE1297365','66F4EF5650C20355','84B8CBCA4D477FA3', 'D4C5016086B2DC6A','5638228DAF52805F',
'D4DF7931AB130E37');

User(s) with Default       Password!   Status
-------------------------------  -----------------------------
XDB                            EXPIRED & LOCKED
EXFSYS                         EXPIRED & LOCKED
```

Copyright© 2010, Oracle. All rights reserved.

デフォルト・ユーザーと初期パスワード

11g～ DBA_USERS_WITH_DEFPWDを使用した初期パスワードのデフォルト・ユーザーの一覧

```
SELECT d.username, u.account_status FROM DBA_USERS_WITH_DEFPWD d, DBA_USERS u
  WHERE d.username = u.username ORDER BY 2,1;

USERNAME              ACCOUNT_STATUS
----------------------        ------------------------------------
APPQOSSYS             EXPIRED & LOCKED
BI                    EXPIRED & LOCKED
DIP                   EXPIRED & LOCKED
SCOTT                 OPEN
SH                    OPEN
HR                    LOCKED(TIMED)
```

※ユーザーのパスワードは、11g移行は、ランダム値とパスワードを結合してハッシュ化されるように変更されているそのため、11gでハッシュ値を比較するスクリプトは使用できない

Copyright© 2010, Oracle. All rights reserved.

DBSNMPユーザのパスワード

- DBSNMPは、Oracle Enterprise Managerで使用されるユーザで、高いシステム権限を保持している
  - CREATE PROCEDURE
  - CREATE TABLE
  - SELECT ANY DICTIONARY
  - UNLIMITED TABLESPACE
- 複雑なパスワードに変更することを検討

10g ～ DBSNMPのパスワード変更手順

1.Database Control を停止します。
  % emctl stop dbconsole

2.dbsnmpのパスワードを変更
  SQL> alter user dbsnmp identified by <new_password> ;

3.target.xmlの編集
  $ORACLE_HOME/ホスト名_SID/sysman/emd/targets.xml
 <Property NAME="password" VALUE="暗号化パスワード" ENCRYPTED="TRUE"/>
  暗号化パスワードの部分に新しいパスワードを設定し、TRUE を FALSE に変更します。

4.DB controlの起動
 % emctl start dbconsole
 (Database Control の起動が完了すると、targets.xml に設定されたパスワードは暗号化される)

Copyright© 2010, Oracle. All rights reserved.

PUBLICロールの管理

- PUBLICは、Oracleデータベースのすべてのユーザーに付与されるデフォルトのロール
  外部ネットワークへアクセスに関するPL/SQLパッケージ(UTL_SMTP, UTL_TCP, UTL_HTTP, UTL_FILE)は、必要なユーザのみに付与するように変更

- アクセスできるディレクトリにもread, writeを区別して管理することも検討
  ※ CREATE ANY DIRECTORY 権限を持つ一般ユーザが、Unix プラットフォーム上にディレクトリを作成する場合、このユーザは、その対象のディレクトリについて、READ および WRITE 権限を自動的に保持する

```
/* PUBLICからはrevokeして、必要なユーザーにごとにgrantする
REVOKE execute on utl_file from public;
GRANT execute on utl_file to scott, jen;


/*アクセス可能にするディレクトリを作成
CONNECT system/manager
CREATE OR REPLACE DIRECTORY my_dir as ‘ディレクトリパス名';
GRANT read,write ON DIRECTORY my_dir TO scott;
```

Copyright© 2010, Oracle. All rights reserved.

Critical Patch Update

- 以下の視点から、セキュリティ・パッチを適用することを検討
  - 対象となるバージョン、機能が含まれているか
  - Risk MatrixのBase Metrixsの値（深刻度）はどうか
  - システムへの影響や適用時間など総合的に検討し、そのリスクを受容できるかできないかを判断

Critical Patch Update

- Critical Patch Update (CPU)は、四半期に一度、その月の15日に最も近い火曜日に公開される、最重要セキュリティ修正をまとめたもの
- CPUには、新規のセキュリティ修正だけでなく、そのパッチ・セットに対して過去に提供されたCPUに含まれる全ての修正（パッチ競合を避けるための非セキュリティ系の修正も）が含まれる
- 主にセキュリティ系の修正のみをCPUに含めるようにしていますが、場合によっては非常に重要度の高い非セキュリティ系の修正もCPUに含んでいる場合もある
- CPUの適用にあたっては、最も確かな方法として、予め本番環境を模したテスト環境で適用テストを行ってから本番環境に適用することを推奨
- セキュリティ・アラート
  http://www.oracle.com/technology/global/jp/deploy/security/alerts.htm

Copyright© 2010, Oracle. All rights reserved.

見直すべき7つの項目

1. 初期設定
2. 認証
3. 権限管理
4. 特権ユーザ管理
5. 不正アクセス
6. 暗号化
7. 監査

無償技術サービスOracle Direct Concierge

- Oracle Database バージョンアップ支援
- Oracle 構成相談(Sizing)サービス
- パフォーマンス・クリニック・サービス
- SQL Serverからの移行アセスメント
- DB2からの移行支援サービス
- Sybaseからの移行支援サービス
- MySQLからの移行相談サービス
- PostgreSQLからの移行相談 サービス
- Accessからの移行アセスメント
- Oracle Developer/2000 Webアップグレード相談
- 仮想化アセスメントサービス
- ビジネスインテリジェンス・エンタープライズ エディション・アセスメントサービス
- 簡易業務診断サービス

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

Copyright© 2010, Oracle. All rights reserved.

認証の強度向上

- SYSDBA権限での、パスワード無しのログインを禁止にする
  - バックアップのスクリプトやアプリケーションで sqlplus / as sysdba 接続を使用している場合があるのでその影響度合いを検討
- リモートからのOS認証の禁止
  - DBリンクで使用されている可能性がある

```
/* SYSDBAのパスワード無しログインを禁止
$ORACLE_HOME/network/admin/ sqlnet.ora
SQLNET.AUTHENTICATION_SERVICES=NONE        <<sqlnet.oraに追記

$ sqlplus / as sysdba
ERROR: ORA-01031: insufficient privileges

/*リモート認証の禁止
初期化パラメータファイル remote_os_authent= FALSEに設定   <<通常はデフォルト

※ remote_os_authent= TRUEの場合、ネットワーク経由での不正アクセスの可能性が高まる危険性
sqlplus /@node1
```

Copyright© 2010, Oracle. All rights reserved.

ユーザーの使用状況

- データベース内にある作成されたすべてのユーザーの状態をdba_users表から確認し、OPENされている不必要なユーザーが作成されていないか調査
  - DEVELOPERやTESTなどの開発用と思われる名前
  - 長期間使用されていない (login監査を取得している場合は、そのログイン日付から判断)
  - 作成した覚えがない等
- 必要ないと判断できる場合は、一時的にアカウントをロック (Alter user ～ account lock)し、一定期間後に削除を検討

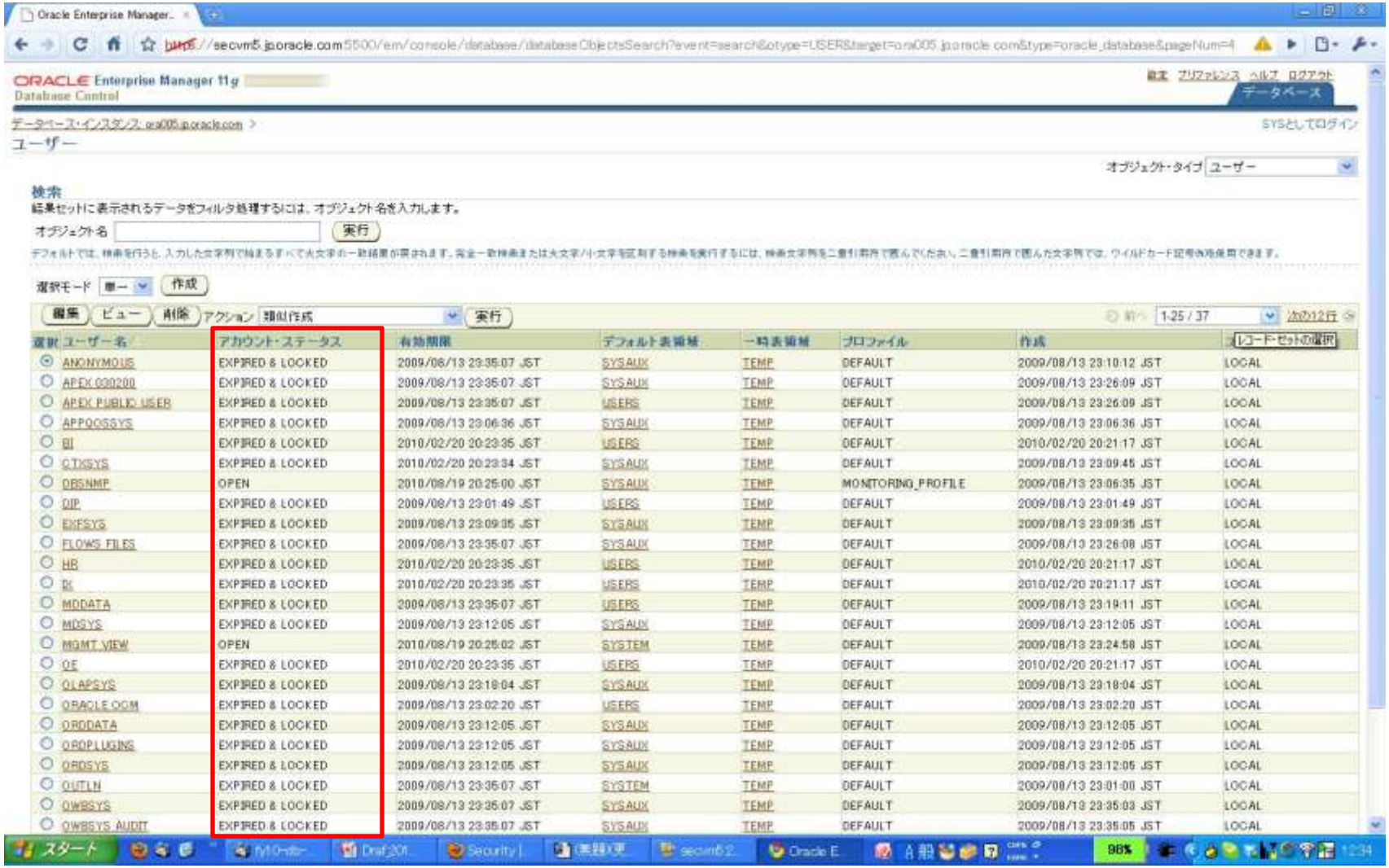
10g,11g DB内にあるすべてのユーザーの状態

```
select username,ACCOUNT_STATUS, LOCK_DATE,EXPIRY_DATE from dba_users;

USERNAME                       ACCOUNT_STATUS                 LOCK_DAT EXPIRY_D
------------------------------ ------------------------------ -------- --------
OPS$ORACLE                     OPEN                           10-08-25
MASK                           OPEN                           10-08-19
SCOTT                          OPEN                           10-09-04
SYSMAN                         OPEN                           10-08-02
SYSTEM                         OPEN                           10-08-02
SYS                            OPEN                           10-08-02
DBSNMP                         OPEN                           10-08-02
HR                             LOCKED(TIMED)                  10-03-11 10-08-17
OE                             EXPIRED & LOCKED               10-02-03 10-02-03
PM                             EXPIRED & LOCKED               10-02-03 10-02-03
BI                             EXPIRED & LOCKED               10-02-03 10-02-03
```

Copyright© 2010, Oracle. All rights reserved.

ユーザーの使用状況

Oracle Enterprise Managerで確認



Copyright© 2010, Oracle. All rights reserved.

デフォルト・プロファイル

Oracle Database では、アカウント管理に関しての定義情報は、プロファイルによって設定される
デフォルト・プロファイルを変更することで、割り当てられパスワード・ポリシーや使用可能リソースの制限が可能

属性名	10gR2	11gR1	説明
FAILED_LOGIN_ATTEMPTS	10	10	許容されるログインの連続失敗回数。これを超えるとアカウントはロックされる。
PASSWORD_LIFE_TIME	UNLIMITED	180	同一パスワードの有効期間(日数)。これを過ぎるとパスワードは 期限切れ となる。UNLIMITED は永続的に使用できることを示す。
PASSWORD_GRACE_TIME	UNLIMITED	7	パスワードが 期限切れ となってから 無効化 されるまでの猶予期間(日数)。その間ユーザーはパスワードを変更することが許可される。UNLIMITED は制限なし。
PASSWORD_LOCK_TIME	UNLIMITED	1	ログインに連続失敗した際のアカウントのロック期間(日数)。UNLIMITED は自動ロック解除が無効。
PASSWORD_REUSE_MAX	UNLIMITED	UNLIMITED	過去と同一のパスワードの使用を許容しない変更回数。UNLIMITEDでは即再利用可能。
PASSWORD_REUSE_TIME	UNLIMITED	UNLIMITED	過去と同一のパスワードの使用を許容しない期間(日数)。UNLIMITED では即再利用可能。
PASSWORD_VERIFY_FUNCTION	NULL	NULL	設定したパスワードの複雑さを、ユーザー任意の条件に基づいて検証したいときに設定する。※FUNCTIONのサンプル有り (次頁参照)

※上記設定内容は、次のSQLで確認可能

```
SQL> SELECT * FROM dba_profiles WHERE profile='DEFAULT'
  2   AND resource_type='PASSWORD';
```

※変更する場合は次のように実行

```
SQL> ALTLER PROFILE default
  2   LIMIT <属性名> <新しい値>;
```

Copyright© 2010, Oracle. All rights reserved.

複雑なパスワード設定の導入

- パスワード・ポリシーの属性 PASSWORD_VERIFY_FUNCTION を使用すると、ユーザーにパスワードを設定した際、それが十分に複雑であるかどうかを自動的に検証させることが可能
  検証用のファンクションを用意し、それを属性値として割り当てる

- サンプルとして、予め 2つのファンクションを用意 (カスタマイズ可能)
  - **verity_function** :
    11g以前から提供されている検証用サンプル・ファンクション
  - **verify_function_11G** :
    11gから新たに提供された、より詳細な条件の加わったサンプル・ファンクション

- これらは SYSで $ORACLE_HOME/rdbms/admin/ 配下の utlpwdmg.sql を実行することにより SYS スキーマに作成される。
- このとき、PASSWORD_VERIFY_FUNCTION の値は **VERIFY_FUNCTION_11G** に設定されます。なお、その他のパスワード関連属性も初期状態に再設定されますので、実行のタイミングに注意。あるいは不要なコマンドをコメントアウトしてから実行すること

verify_function_11G 内で定義されている "複雑さ" の条件

- 8文字以上である。
- ユーザー名、またはその逆順、あるいはユーザー名の後ろに 1～100 の数値を付加したものではない。
- サーバ名、またはサーバ名の後ろに 1～100 の数値を付加したものではない。
- 単純すぎない。
  例) welcome1, database1, account1, user1234, password1, oracle, oracle123, computer1, abcdefg1, change_on_install etc…
- 少なくとも1文字以上の数値およびアルファベットを含む
- 前回のパスワードと少なくとも3文字以上異なること

Copyright© 2010, Oracle. All rights reserved.

見直すべき7つの項目

1. 初期設定
2. 認証
3. **権限管理**
4. 特権ユーザ管理
5. 不正アクセス
6. 暗号化
7. 監査

無償技術サービスOracle Direct Concierge

- Oracle Database バージョンアップ支援
- Oracle 構成相談(Sizing)サービス
- パフォーマンス・クリニック・サービス
- SQL Serverからの移行アセスメント
- DB2からの移行支援サービス
- Sybaseからの移行支援サービス
- MySQLからの移行相談サービス
- PostgreSQLからの移行相談 サービス
- Accessからの移行アセスメント
- Oracle Developer/2000 Webアップグレード相談
- 仮想化アセスメントサービス
- ビジネスインテリジェンス・エンタープライズ エディション・アセスメントサービス
- 簡易業務診断サービス

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

Copyright© 2010, Oracle. All rights reserved.

ユーザーの所有するシステム権限

- ユーザーに割り当てられているシステム権限・ロールから、不必要なシステム権限が割り当てられていないか確認
  - DBAロールの割り当て
  - any権限(create any , select any….)などの強い権限
- 以下の例は、SCOTTがCONNECTとRESOURCEロール、UNLIMITED TABLESPACEのシステム権限が与えられていることがわかる。また、CONNECTロールにはCREATE SESSIONが割り当てられている
  ※10gR2からは、CONNECTロールにはCREATE SESSIONのみに変更された

10g,11g ユーザーの所有するシステム権限、ロールを表示 (※スクリプトは次ページ)

```
Enter username to show SYSTEM privileges of:  scott
SYSTEM PRIVILEGES

CONNECT                 CREATE SESSION
RESOURCE                CREATE CLUSTER
                        CREATE INDEXTYPE
                        CREATE OPERATOR
                        CREATE PROCEDURE
                        CREATE SEQUENCE
                        CREATE TABLE
                        CREATE TRIGGER
                        CREATE TYPE
SCOTT                   UNLIMITED TABLESPACE
```

Copyright© 2010, Oracle. All rights reserved.

ユーザーの所有するシステム権限

10g,11g ユーザーの所有するシステム権限、ロールを表示するスクリプト

```
set verify off
      set head off
      set feedback off
      set pages 20
      set linesize 200
      undef naam
      accept naam char prompt 'Enter username to show SYSTEM privileges
      of: '

      set termout off
      drop table testpriv;
      create table testpriv  (grantee varchar2(30),
                        granted_set verify off
      set head off
      set feedback off
      set pages 20
      undef naam
      accept naam char prompt 'Enter username to show SYSTEM privileges
      of: '

      set termout off
      drop table testpriv;
      -- DBA_ROLE_PRIV indicates which role is granted to which user
      create table testpriv  (grantee varchar2(30),
                        granted_role varchar2(32),
                        ptype varchar2(1));

      insert into testpriv (
      select grantee,granted_role,'R'
      from sys.dba_role_privs);
```

```
-- DBA_SYS_PRIV indicates which privilege is granted to
      which user
      --             directly (without using roles).
      insert into testpriv
      select distinct grantee,
            decode(grantee, 'DBA', 'DBA-role (+- 80 privs)',
                        'IMP_FULL_DATABASE','Role of 35 privs',
                        'EXP_FULL_DATABASE','Role of 2 privs',
                         privilege),
            'P'
      from sys.dba_sys_privs
      --where grantee != 'DBA'  ;

      set termout on
      -- testpriv now contains:
      --  (user, role)
      --  (role, privs)
      --  (user, privs)
      -- So display it in a connect by format:
      col title format a30 heading "System privileges" trunc
      prompt SYSTEM PRIVILEGES
      break on title

      select distinct(grantee) title,
            decode (ptype,'R',null,'P',granted_role)
      from testpriv
      connect by grantee = prior granted_role
      start with grantee = upper('&naam')
      order by 1
      /
```

Copyright© 2010, Oracle. All rights reserved.

ユーザーの所有するオブジェクト権限

- ユーザーが与えた・与えられたオブジェクト権限の確認
  - 不必要なオブジェクト権限を与えていないか(SELECT,UPDATE,DELETE,INSERT,MERGE….)
  - 不必要にwith grant optionを付与していないか

- 以下の例は、OEにはCOUNTRIES表、SHにはEMPLOYEES表へのオブジェクト権限を与えている。
  また、SYSからはDBMS_STSTSを実行する権限と、SCOTTからはEMP表へのSELECT権限をwith grant option付きで与えられている。※ with grant optionは、その権限を別のユーザーに与えることができることを意味する

10g,11g ユーザーの所有するオブジェクト権限を表示 (※スクリプトは次ページ)

```
Enter user to evaluate:  hr
Table privileges GIVEN:
======================
REFERENCES   ON        HR.COUNTRIES        TO       OE
SELECT       ON        HR.EMPLOYEES        TO       SH

Table privileges RECEIVED:
==========================
EXECUTE      ON        SYS.DBMS_STATS      FROM     SYS
SELECT       ON        SCOTT.EMP           FROM     SCOTT  +GRANT OPT

Column privileges GIVEN:
========================
Column privileges RECEIVED:
==========================
```

Copyright© 2010, Oracle. All rights reserved.

ユーザーの所有するオブジェクト権限

10g,11g ユーザーの所有するオブジェクト権限を表示するスクリプト

```
set head off
set verify off
set feed off
set pause off
col pr format a10
col tn format a22
col tn2 format a30
col gr format a20
accept person char prompt 'Enter user to evaluate:  '
ho clear

prompt      Table privileges GIVEN:
prompt      ======================
select  privilege pr,
        'ON',
        owner||'.'||table_name tn,
        'TO',
     grantee gr,
        decode(grantable,'YES','+GRANT OPT')
from sys.dba_tab_privs
where owner = upper('&person');

prompt
prompt      Table privileges RECEIVED:
prompt      ==========================
```

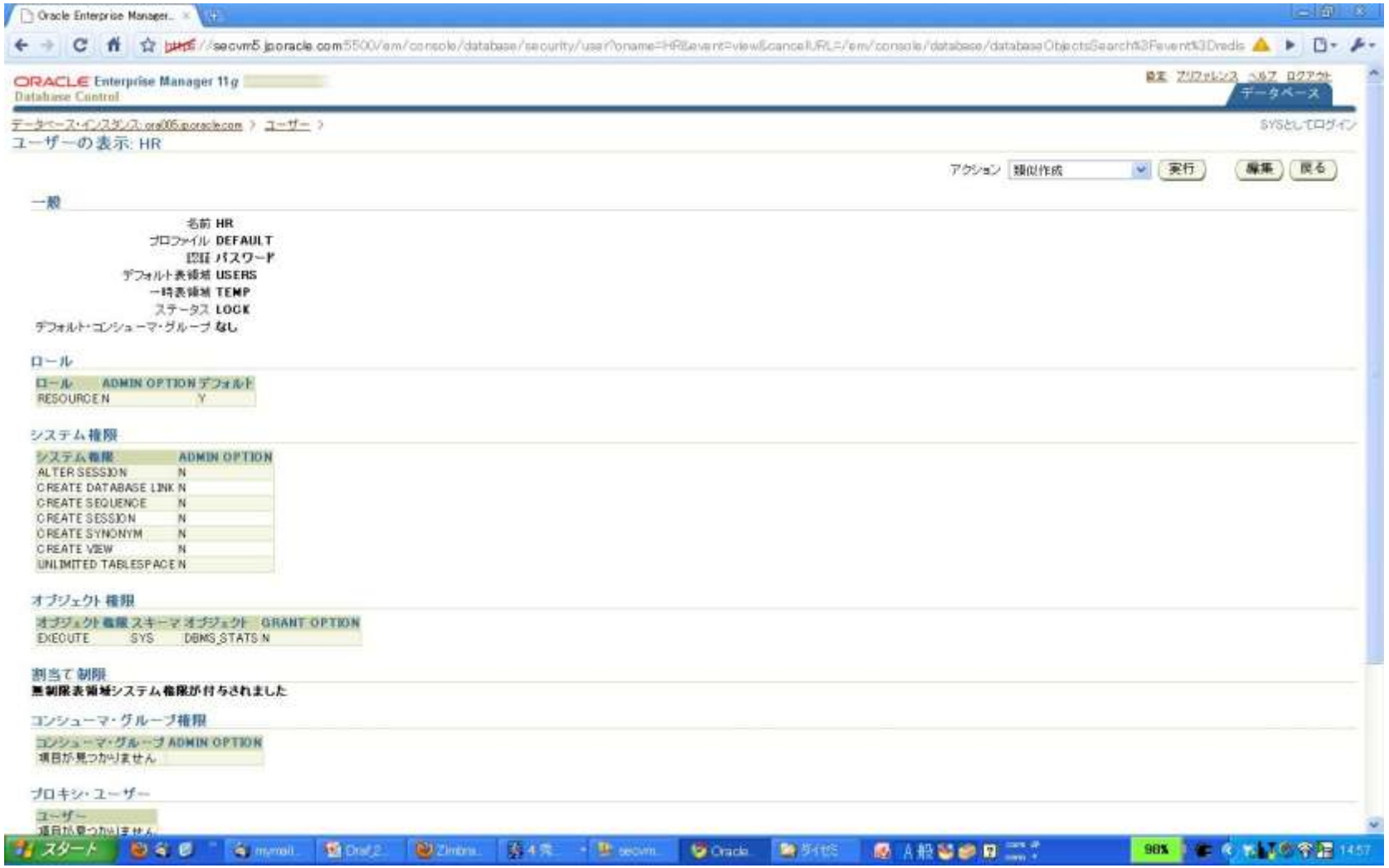
```
select  privilege pr,
  'ON',
        owner||'.'||table_name tn,
        'FROM',
        grantor gr,
        decode(grantable,'YES','+GRANT OPT')
from sys.dba_tab_privs
where grantee = upper('&person');

prompt
prompt
prompt      Column privileges GIVEN:
prompt      ========================
select  privilege pr,
        'ON',
        owner||'.'||table_name||'('||column_name||')' tn2,
        '-->',
      grantee gr,
        decode(grantable,'YES','+GRANT OPT')
from sys.dba_col_privs
where owner = upper('&person');
```

```
prompt
prompt      Column privileges RECEIVED:
prompt      ===========================
select  privilege pr,
     'ON',
        owner||'.'||table_name||‘
           ('||column_name||')' tn2,
 'FROM',
        grantor gr,
        decode(grantable,'YES','+GRANT OPT')
from sys.dba_col_privs
where grantee = upper('&person');

set head on
set verify on
set feed on
```

Copyright© 2010, Oracle. All rights reserved.

ユーザーの所有する権限

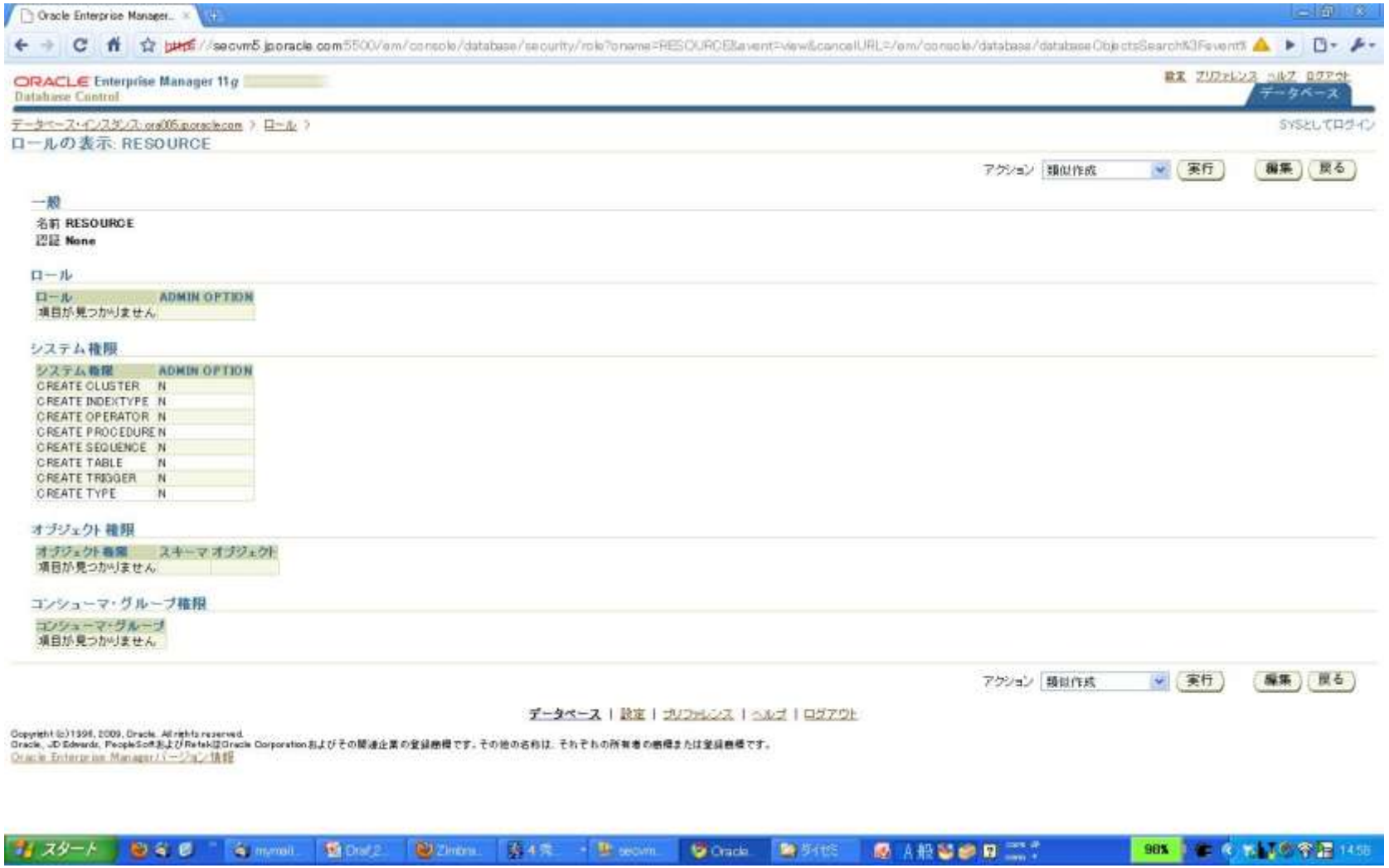
Oracle Enterprise Managerで確認



Copyright© 2010, Oracle. All rights reserved.

ロールの所有する権限

Oracle Enterprise Managerで確認



Copyright© 2010, Oracle. All rights reserved.

システム権限から見た割り当て範囲

- システム権限が必要のないユーザーに割り当てられていないかを確認
  - any権限(create any , select any….)などの強い権限
  - with admin optionの割り当て

- 以下の例は、すべての表を参照できるSELECT ANY TABLE権限をHRユーザーが保有し、新たにユーザーを作成することができるCREATE USER権限をHRが保有している。また、with admin optionが付いているのでその権限を別のユーザーに付与することができるため大きな脆弱性になる危険性がある

10g,11g システム権限の視点から、だれが保有しているか (※スクリプトは次ページ)

PRIVILEGE	GRANTEE	ADMIN
SELECT ANY DICTIONARY	DBSNMP	NO
	HR	NO
	IX	NO
SELECT ANY TABLE	HR	YES
	EXP_FULL_DATABASE	NO
	IMP_FULL_DATABASE	NO
CREATE USER	HR	YES
	SCOTT	NO

Copyright© 2010, Oracle. All rights reserved.

システム権限から見た割り当て範囲

10g,11g システム権限ごとに保有しているユーザーを表示

```
set pages 50000
set linesize 100
col privilege format a30
col grantee format a30
col admin_option format a5
break on privilege skip 1

select privilege, grantee, admin_option
from dba_sys_privs
where privilege not in
(
  /* list any other privilege here you don't find "sweeping"  */
  'ALTER SESSION',
  'QUERY REWRITE',
  'CREATE DIMENSION',
  'CREATE INDEXTYPE',
  'CREATE LIBRARY',
  'CREATE OPERATOR',
  'CREATE PROCEDURE',
  'CREATE SEQUENCE',
  'CREATE SESSION',
  'CREATE SNAPSHOT',
  'CREATE SYNONYM',
  'CREATE TABLE',
  'CREATE TRIGGER',
  'CREATE TYPE',
  'CREATE VIEW',
  'UNLIMITED TABLESPACE'
)
and grantee not in
 ('SYS','SYSTEM','WKSYS','XDB',
  'MDSYS','ORDPLUGINS','ODM','DBA')
   /* Place all the user names you want to exclude */
order by privilege, grantee
/
```

Copyright© 2010, Oracle. All rights reserved.

With Grant Optionの割り当て

- with grant optionは、オブジェクトへのアクセス権とその権限を別のユーザーに付与することができる
  - 通常は、A to B, A to Cという権限の与え方だが、A to B, B to Cという権限付与が可能になる。
- しかし、管理が複雑化し脆弱性になり得るため、使用しないことを推奨

```
/* 以下は、HRがSHにSCOTT.EMP表のSELECT権限を付与している
select grantor,grantee,privilege, owner, table_name from dba_tab_privs where grantor != owner;

GRANTOR   GRANTEE   PRIVILEGE    OWNER           TABLE_NAME
----------  ----------  ---------------  --------------------  -----------------
HR            SH          SELECT        SCOTT            EMP
```

```
REVOKEするSQL文を生成
select 'connect '||grantor conn,
        'revoke '||privilege||' on '||owner||
        '.'||table_name||' from '||grantee||';' line
    from dba_tab_privs
    where GRANTOR != 'SYS'
    and grantor != owner
    order by 1,2
    /
revoke SELECT on SCOTT.EMP from SH;
```

```
GrantするSQL文を生成
select 'grant '||privilege||' on '||owner||
        '.'||table_name||' to '||grantee||';'
    from dba_tab_privs
    where grantor != owner
/

grant SELECT on SCOTT.EMP to SH;
```

Copyright© 2010, Oracle. All rights reserved.

表領域の制限

- 一般ユーザーのデフォルトの表領域がSYSTEMになっていないか、また、SYSTEM表領域にオブジェクトを置いていないか

- UNLIMITED TABLESPACEは、データベースのすべての表領域に無制限に領域割り当てができるので注意が必要
  - 9iまでは、RESOURCEロールに含まれている。10g移行は、含まれない

```
/*SYSTEM表領域にあるSYS,SYSTEM以外のユーザーが持っているオブジェクト
select owner, segment_type, segment_name from dba_segments where tablespace_name = 'SYSTEM‘
and owner not in ('SYS','SYSTEM');

OWNER        SEGMENT_TYPE    SEGMENT_NAME
---------------  ------------------------    -------------------------
OUTLN          TABLE                 OL$
APP1           TABL                  SALES_1

/*デフォルトがSYSTEM表領域のユーザ  (SYS,SYSTEM,OLTLNはOK)
select username from dba_users where default_tablespace = 'SYSTEM';
USERNAME
---------------
SYS
SYSTEM
APP1
```

Copyright© 2010, Oracle. All rights reserved.

表領域の制限

```
/* デフォルト表領域の設定変更、持っているオブジェクトを移動
    ※移動によるrowidが変更されるので、索引やマテリアライズド・ビューなどの再作成に注意
alter user scott default tablespace user_data;
alter table scott.tab1 move tablespace user_data;



/* unlimited tablespaceをrevokeする
select 'revoke unlimited tablespace from '||grantee||';' from dba_sys_privs where privilege = 'UNLIMITED
TABLESPACE'
'REVOKEUNLIMITEDTABLESPACEFROM'||GRANTEE||';'
--------------------------------------------------------------------------------
revoke unlimited tablespace from SPATIAL_CSW_ADMIN_USR;
revoke unlimited tablespace from PM;



/* unlimited tablesapace権限ではなく、自分のオブジェクトがある表領域のみにunlimitedでgrantするSQLを生成
select 'alter user '||grantee||' quota unlimited on '|| tablespace_name||';' from dba_sys_privs p,
dba_tablespaces t where p.grantee in (select username from dba_users) and p.privilege = 'UNLIMITED
TABLESPACE'
and t.tablespace_name not in ('SYSTEM','SYSAUX') order by grantee, tablespace_name;

'ALTERUSER'||GRANTEE||'QUOTAUNLIMITEDON'||TABLESPACE_NAME||';'
--------------------------------------------------------------------------------
alter user MDDATA quota unlimited on USERS;
alter user MDSYS quota unlimited on APP_DATA;
```

Copyright© 2010, Oracle. All rights reserved.

見直すべき7つの項目

1. 初期設定
2. 認証
3. 権限管理
4. 特権ユーザ管理
5. 不正アクセス
6. 暗号化
7. 監査

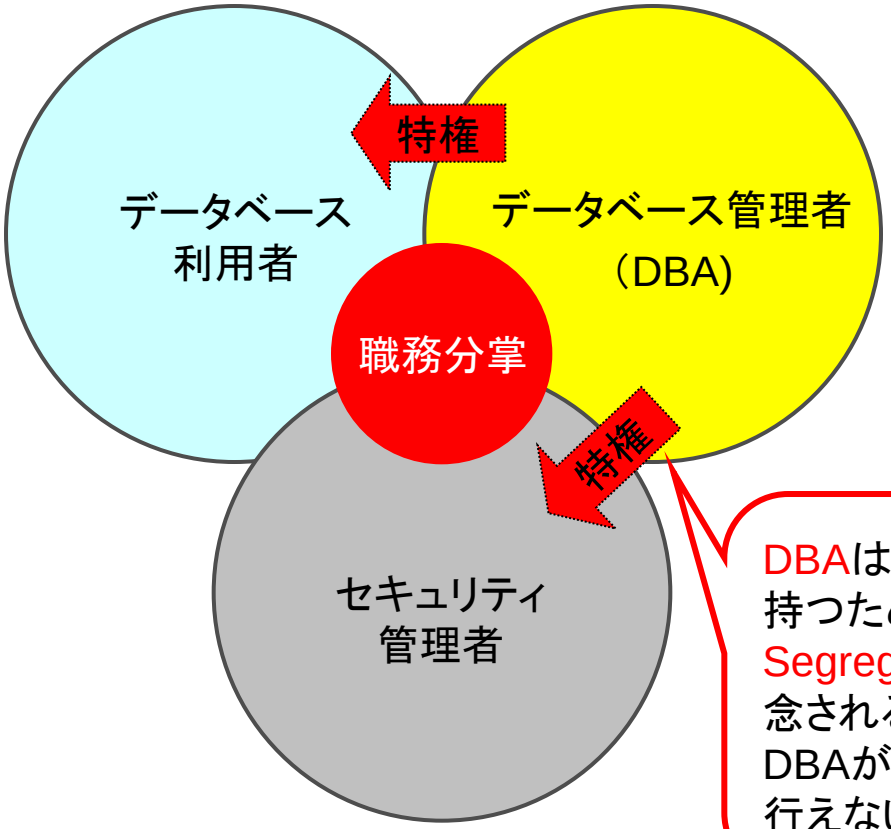
無償技術サービスOracle Direct Concierge

・Oracle Database バージョンアップ支援
・Oracle 構成相談(Sizing)サービス
・パフォーマンス・クリニック・サービス
・SQL Serverからの移行アセスメント
・DB2からの移行支援サービス
・Sybaseからの移行支援サービス
・MySQLからの移行相談サービス
・PostgreSQLからの移行相談 サービス
・Accessからの移行アセスメント
・Oracle Developer/2000 Webアップグレード相談
・仮想化アセスメントサービス
・ビジネスインテリジェンス・エンタープライズ エディション・アセスメントサービス
・簡易業務診断サービス

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

Copyright© 2010, Oracle. All rights reserved.

データベースに関わる職務分掌



- 開発作業
- アプリケーション管理
- ユーザー利用

- データベースの起動・停止
- バックアップ・リカバリ
- ストレージ管理
- チューニング作業

DBAはあらゆる操作が行える特権を持つため、職務分掌（SoD: Segregation of Duties）の観点から懸念される。
DBAが故意または過失による不正が行えない環境にすることが必要。

- ユーザーと権限の管理
- ログの管理と分析・レポート

Copyright© 2010, Oracle. All rights reserved.

Database Vault による権限分離

～ 今までの Oracle Database ～
DBAに管理権限が集中

データベース
管理者

- データベース管理
- ユーザー・アカウント管理
- セキュリティ・ポリシー管理
- アプリケーション・データの管理

データベースの起動/停止、全ユーザー・データの操作や、セキュリティ設定の変更などあらゆる操作が実行可能

データベース管理者による
不正なデータ操作や情報漏えいのリスク！

～ Oracle Database Vault ～
複数の管理者が管理権限を分担

データベース管理

データベースの起動/停止 など
※実データへのアクセスは不可！

データベース
管理者

ユーザー・アカウント管理

ユーザーの作成/削除
※実データへのアクセスは不可！

アカウント
管理者

セキュリティ・ポリシー管理

セキュリティの設定/監視
※実データへのアクセスは不可！

セキュリティ
管理者

アプリケーション・データの管理

ユーザー・データの管理、
アクセス権の設定

アプリケーション
管理者

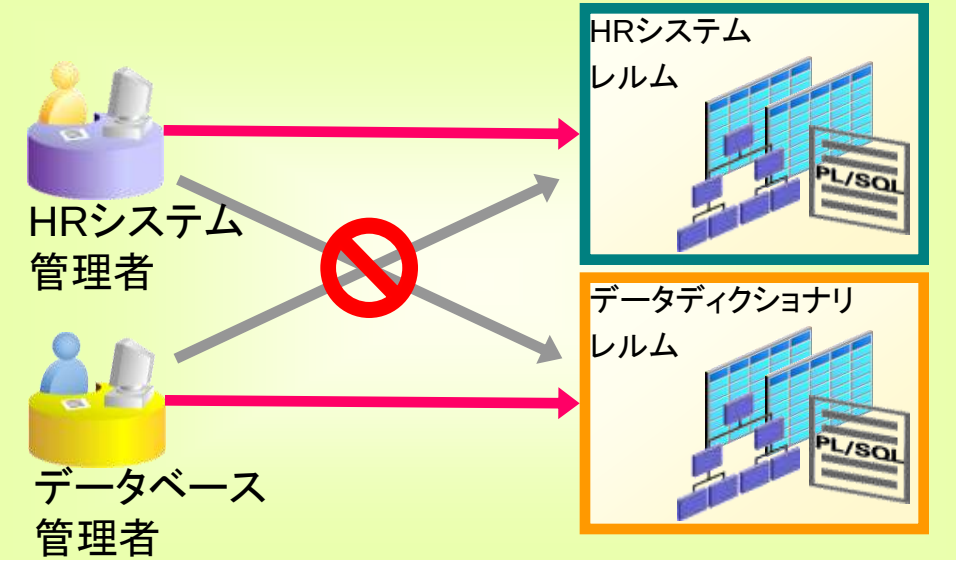
- DBAの特権を制御
  - ✓ 管理権限を分割し、SYS/SYSTEMへの権限集中によるリスクを回避

Copyright© 2010, Oracle. All rights reserved.

レルム（保護領域）

- 任意のスキーマ・オブジェクトのセットを保護・管理するための論理的な領域
- レルムの認可を受けたユーザのみが、そのレルムで保護されたオブジェクトにアクセス可能
  - レルムごとにデータベース管理者を作成することが可能
  - レルム上のオブジェクトに対する SELECT/DML/EXECUTE 権限を含む適切なロールを作成し、適切にユーザーに付与することによるアクセス制御を実現
  - 認可を受けていないレルムに対する、システム権限でのアクセスや DDL はレルム違反エラーとなり、監査ログとして保存される

ポイント：
- 例えば、HRユーザーの持っているオブジェクトをすべてHRレルムで保護すれば、SYS権限を持つデータベース管理者であったとしてもHRオブジェクトへのアクセスは許可されない。
（特権ユーザーの排除）



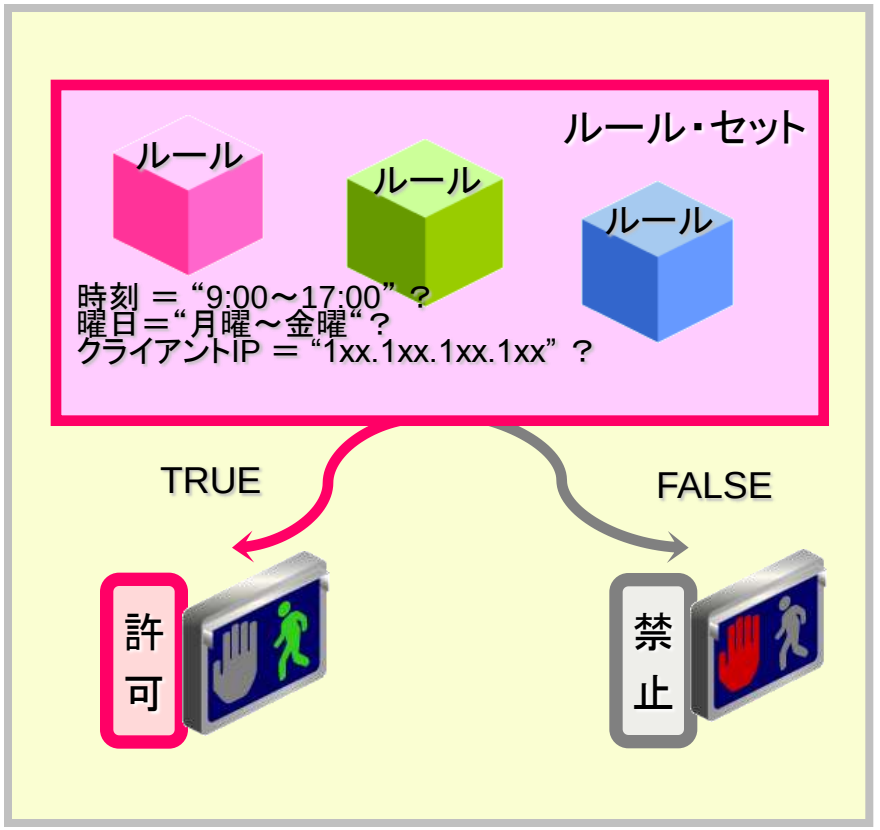
Copyright© 2010, Oracle. All rights reserved.

ルール、ルール・セット（アクセス条件）

- レルムによって保護されているオブジェクトにアクセスするためには、ルールに許可される必要がある

- ルール は、データベースで取得できる情報（ex 時刻、IPアドレスなど）を利用して「*<IPアドレス>* が ○○ という条件を満たす場合に “許可” or “不許可” となる」という形で作成

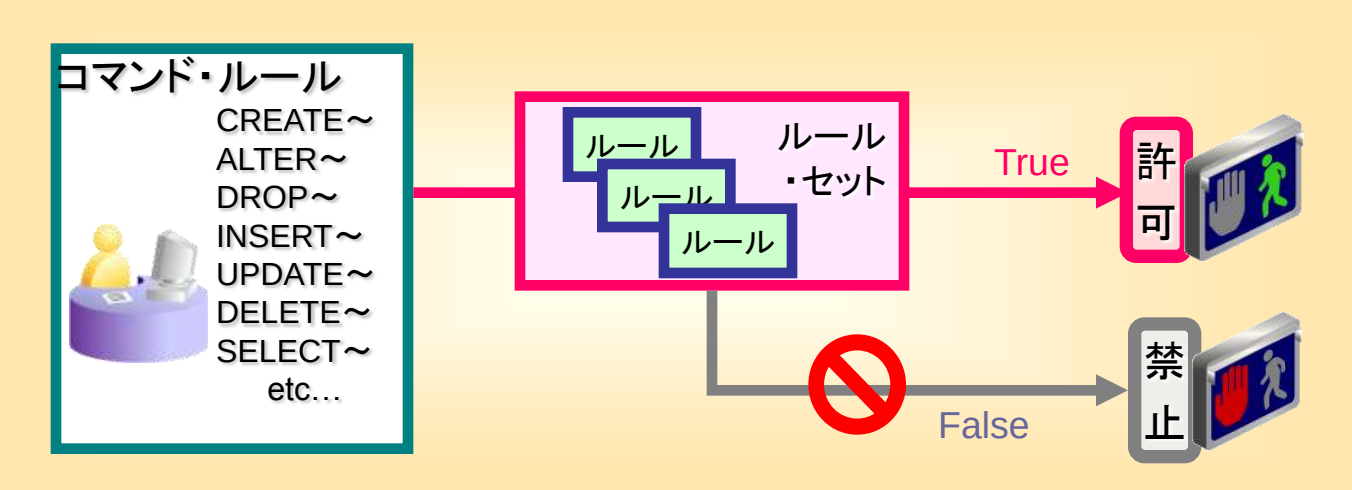
- 1つのアクセス制御を構成する条件のセットを ルール・セット 、それに含まれるそれぞれの条件を ルール と呼ぶ
- ルール・セットに含めるルールを増やし条件を厳しくすることで、アクセス制御の条件を強化可能



Copyright© 2010, Oracle. All rights reserved.

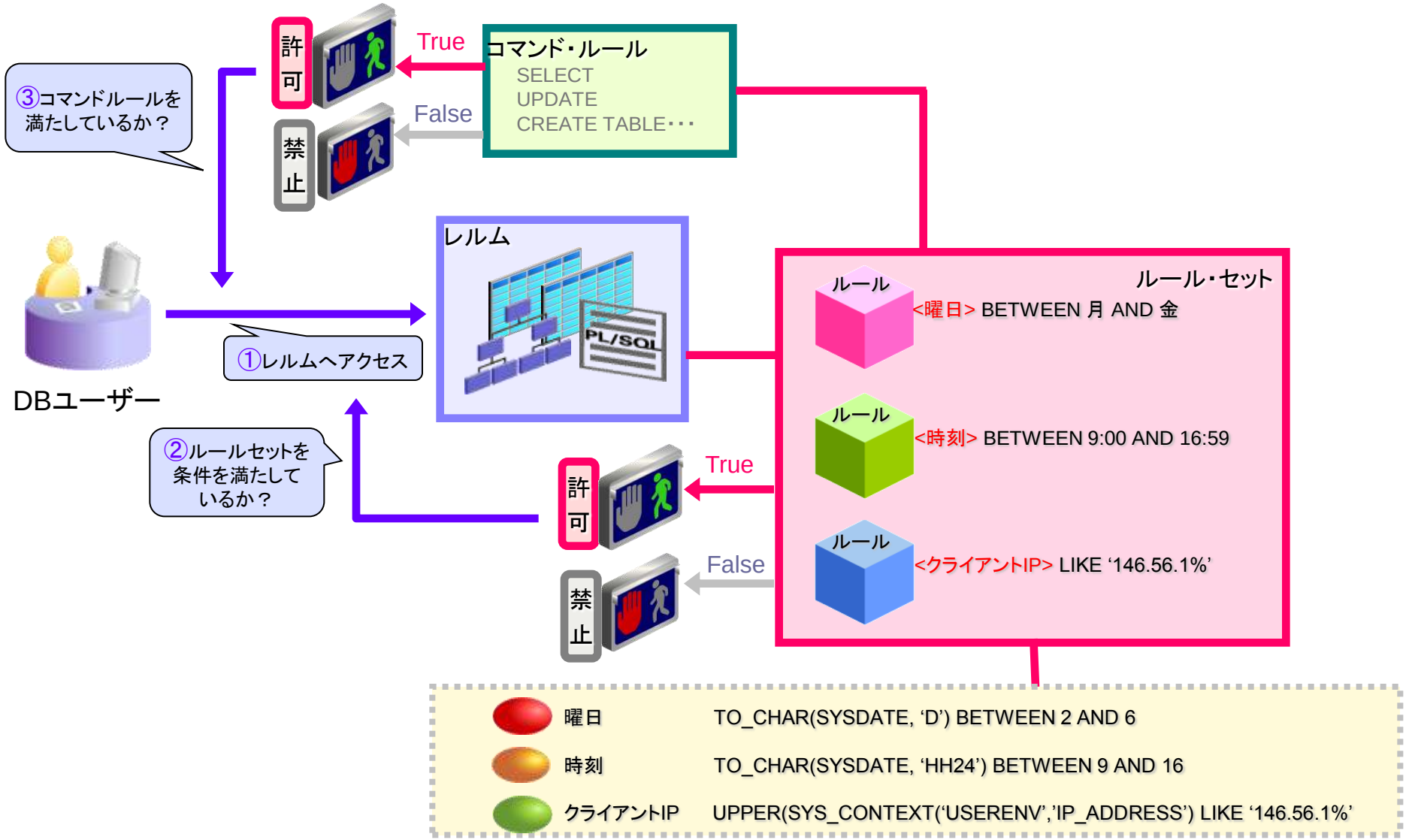
コマンド・ルール

- SQLコマンドの発行を、ルール・セットに基いて制限するためのもの
- SQLコマンドに特定のルール・セットを紐付けておくと、ルール・セットがtrue となった場合のみ、そのSQLコマンドを発行する許可が与えられる
  ※注：SQLコマンドの実行権限(システム権限やオブジェクト権限)は別途必要



Copyright© 2010, Oracle. All rights reserved.

Database Vaultでのアクセス・コントロールの動作



Copyright© 2010, Oracle. All rights reserved.

見直すべき7つの項目

1. 初期設定
2. 認証
3. 権限管理
4. 特権ユーザ管理
5. 不正アクセス
6. 暗号化
7. 監査

無償技術サービスOracle Direct Concierge

・Oracle Database バージョンアップ支援
・Oracle 構成相談(Sizing)サービス
・パフォーマンス・クリニック・サービス
・SQL Serverからの移行アセスメント
・DB2からの移行支援サービス
・Sybaseからの移行支援サービス
・MySQLからの移行相談サービス
・PostgreSQLからの移行相談 サービス
・Accessからの移行アセスメント
・Oracle Developer/2000 Webアップグレード相談
・仮想化アセスメントサービス
・ビジネスインテリジェンス・エンタープライズ エディション・アセスメントサービス
・簡易業務診断サービス

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

Copyright© 2010, Oracle. All rights reserved.

特定のクライアントのみ接続を限定する

- リスナーへ接続を許可するクライアントを設定することで、データベースへ接続可能な範囲を絞り込む
  ただし、リスナー接続の場合のみ、ローカル接続には効果がない
- データベースへのログイントリガーを利用して、ログイン時にIPアドレスをチェックしてアクセスコントロール。ただし、特権ユーザーには効果がないので、別途 Database Vaultが必要

リスナー、トリガーによるクライアント制御

```
/* リスナーでのクライアント制御は、sqlnet.oraに以下の項目を追加する
tcp.validnode_checking = yes
tcp.invited_nodes =(secvm6,10.185.235.68)   < 許可するホスト名またはIPアドレス   ※自ホストは必ず記述


/*トリガーでクライアント制御   ※system,sysには効果なし
create or replace trigger valid_ip
  after logon on database
    begin
     If sys_context('USERENV','IP_ADDRESS') not in (
      '100.14.32.9'      < 許可するホストを記述
     ) then
    raise_application_error (-20001,'Login not allowed from this IP');
   end if;
 end;
```

Copyright© 2010, Oracle. All rights reserved.

リスナーへのパスワード設定

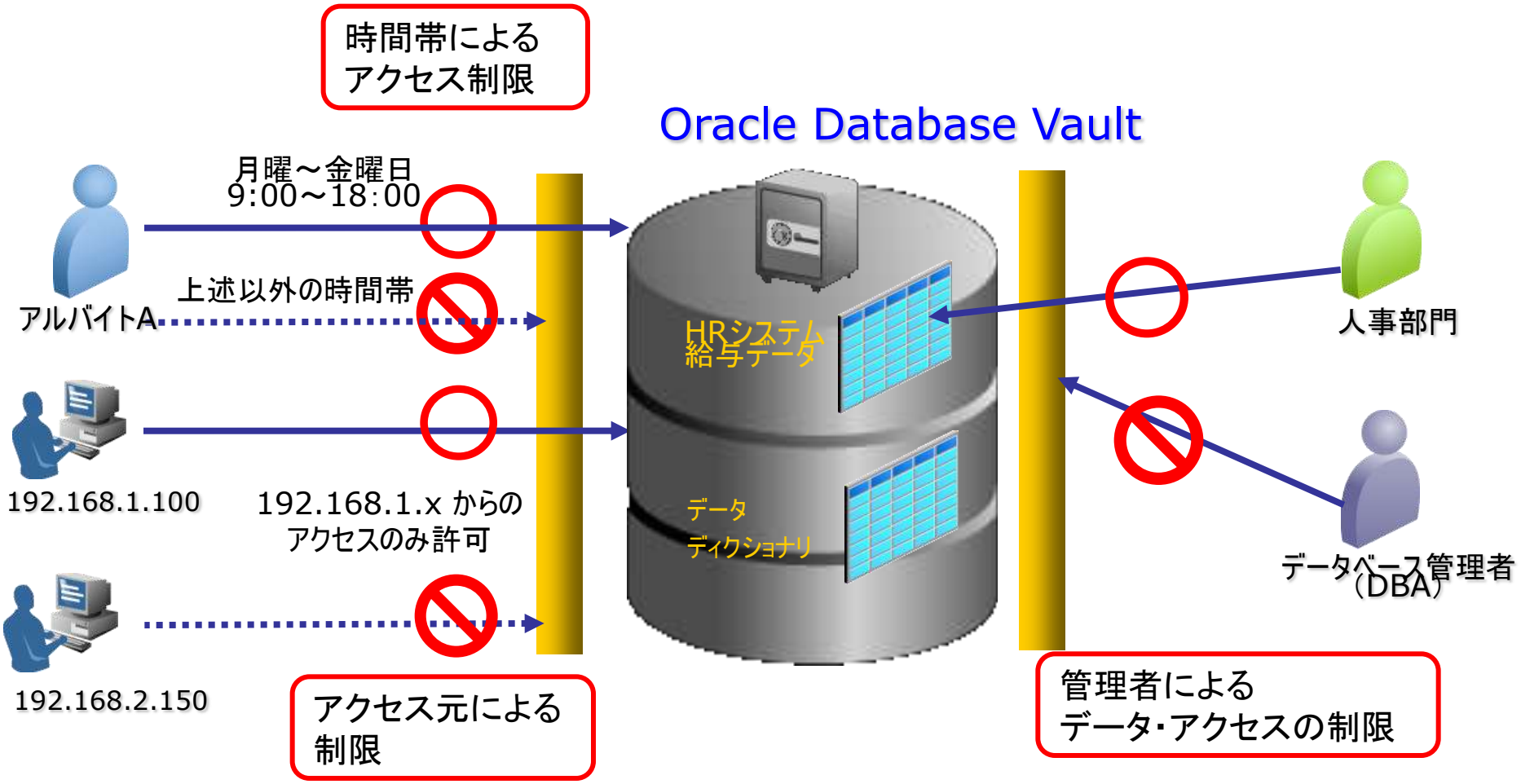
- リスナーにパスワードを設定することで、リスナーを起動した以外のユーザーがリスナーを停止することができないようにする

リスナーへのパスワード設定

```
/* リスナーパスワードの設定
LSNRCTL> change_password
LSNRCTL> パスワード入力
LSNRCTL> save_config

listener.oraに以下が追加される。
PASSWORDS_LISTENER = 1DF5C2FD0FE9CFA2

/* listenerを起動したユーザー以外がリスナーと停止しようとすると
(DESCRIPTION=(ADDRESS=(PROTOCOL=TCP)(HOST=secvm6.jp.oracle.com)(PORT=1521)))に接続中
TNS-01190: ユーザーに、リクエストされたリスナー・コマンドを実行する権限がありません

/* パスワードを入力
LSNRCTL> set password パスワード
LSNRCTL> stop
(DESCRIPTION=(ADDRESS=(PROTOCOL=TCP)(HOST=secvm6.jp.oracle.com)(PORT=1521)))に接続中
コマンドは正常に終了しました。
```

Copyright© 2010, Oracle. All rights reserved.

Database Vault によるアクセス・コントロールの利用例



Copyright© 2010, Oracle. All rights reserved.

見直すべき7つの項目

1. 初期設定
2. 認証
3. 権限管理
4. 特権ユーザ管理
5. 不正アクセス
6. 暗号化
7. 監査

無償技術サービスOracle Direct Concierge

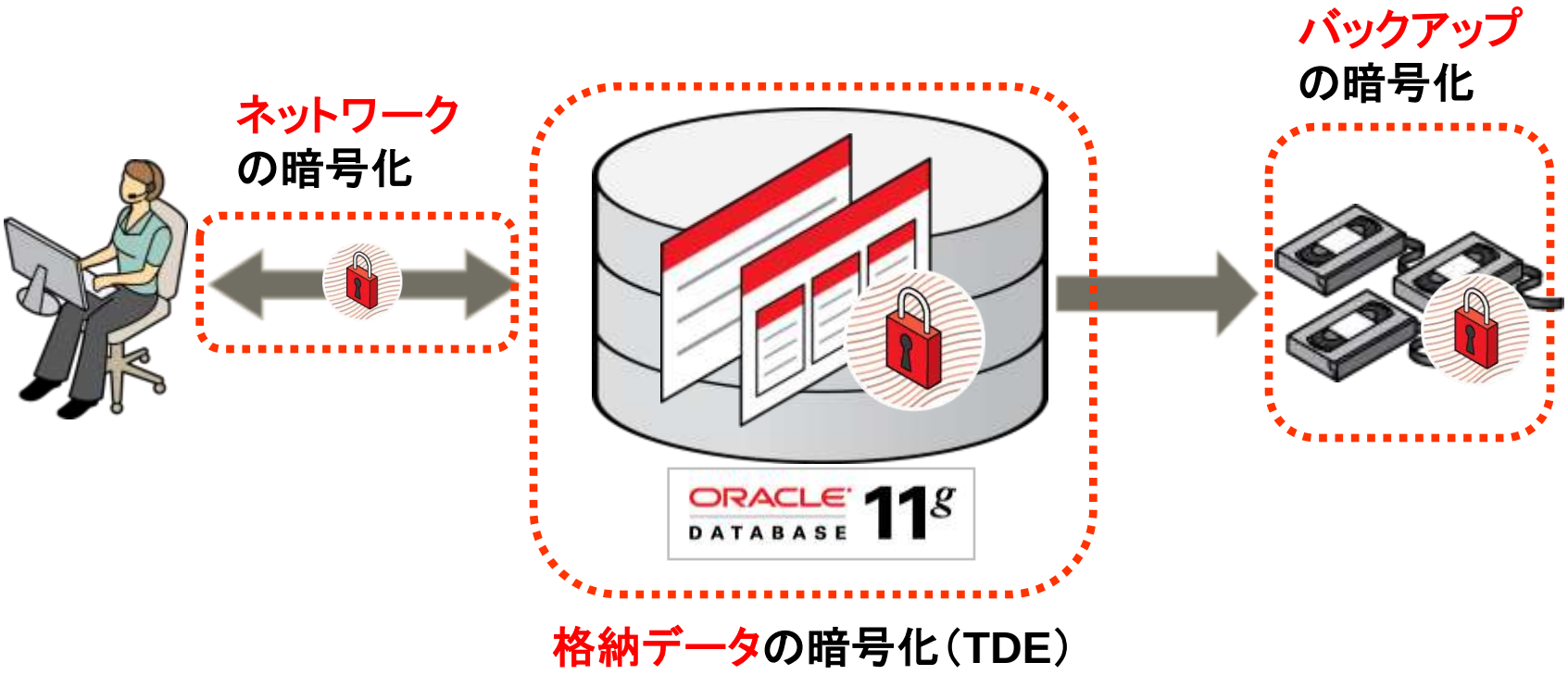
- Oracle Database バージョンアップ支援
- Oracle 構成相談(Sizing)サービス
- パフォーマンス・クリニック・サービス
- SQL Serverからの移行アセスメント
- DB2からの移行支援サービス
- Sybaseからの移行支援サービス
- MySQLからの移行相談サービス
- PostgreSQLからの移行相談 サービス
- Accessからの移行アセスメント
- Oracle Developer/2000 Webアップグレード相談
- 仮想化アセスメントサービス
- ビジネスインテリジェンス・エンタープライズ エディション・アセスメントサービス
- 簡易業務診断サービス

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

Copyright© 2010, Oracle. All rights reserved.

Oracle Advanced Security

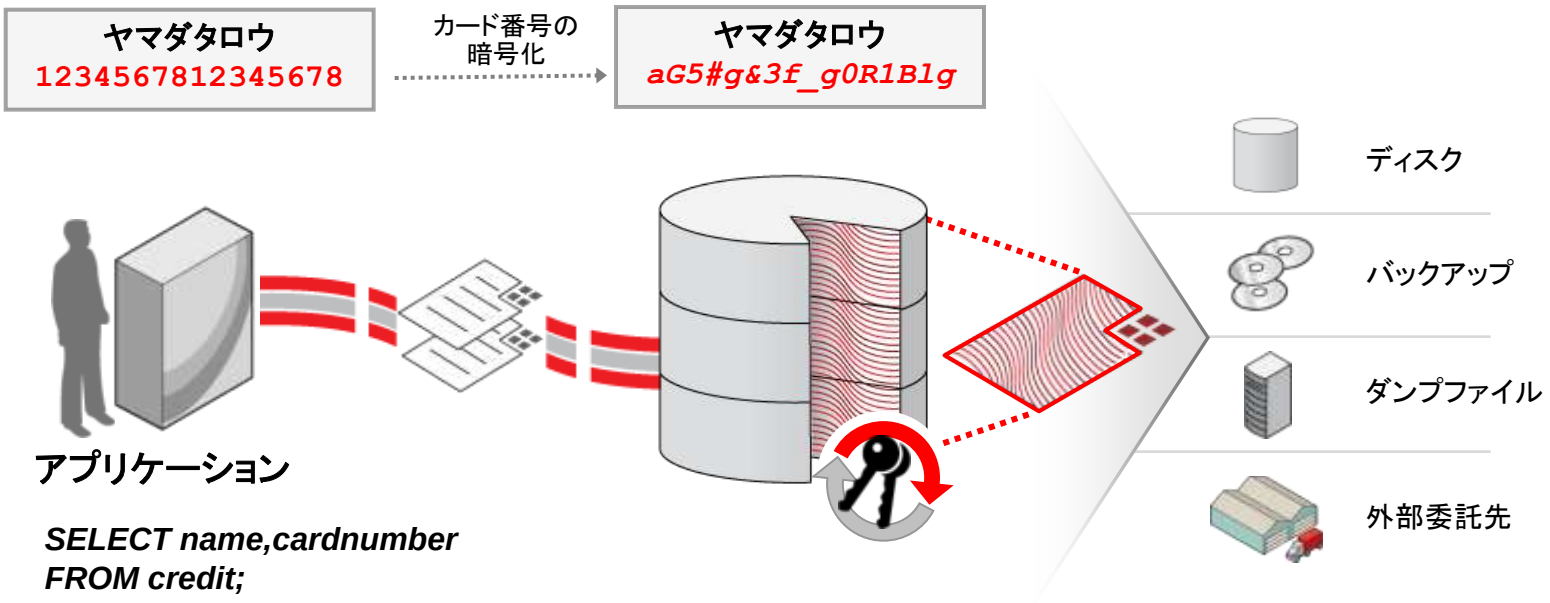
- 可用性と機密性を両立したOracleデータベース暗号化機能
- アプリケーションからは透過的に暗号化を実施するため、SQLの変更は不要
- 暗号化が求められるセキュリティ要件、コンプライアンス要件への対応を支援



Copyright© 2010, Oracle. All rights reserved.

Transparent Data Encryption（TDE）

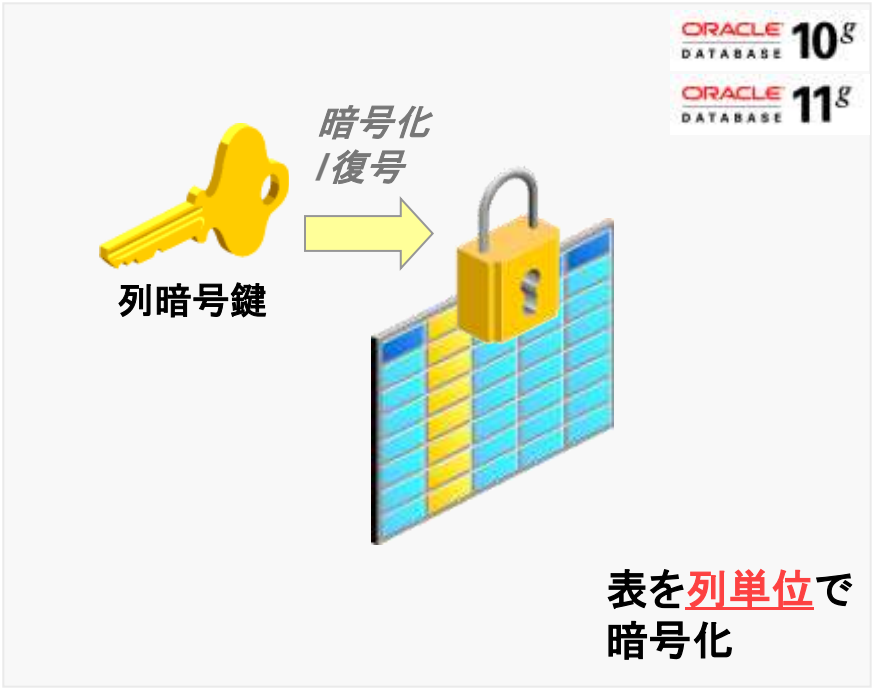
- 強力な暗号アルゴリズムを利用した暗号化を実施
  - NISTの標準共通鍵暗号方式 AES(128/192/256bit) に対応
- Oracle Wallet やHardware Security Moduleを利用した暗号鍵管理メカニズム
- アプリケーションからは透過的にデータの暗号化/復号
  - 既存のアプリケーション（SQL）を改修する必要はない

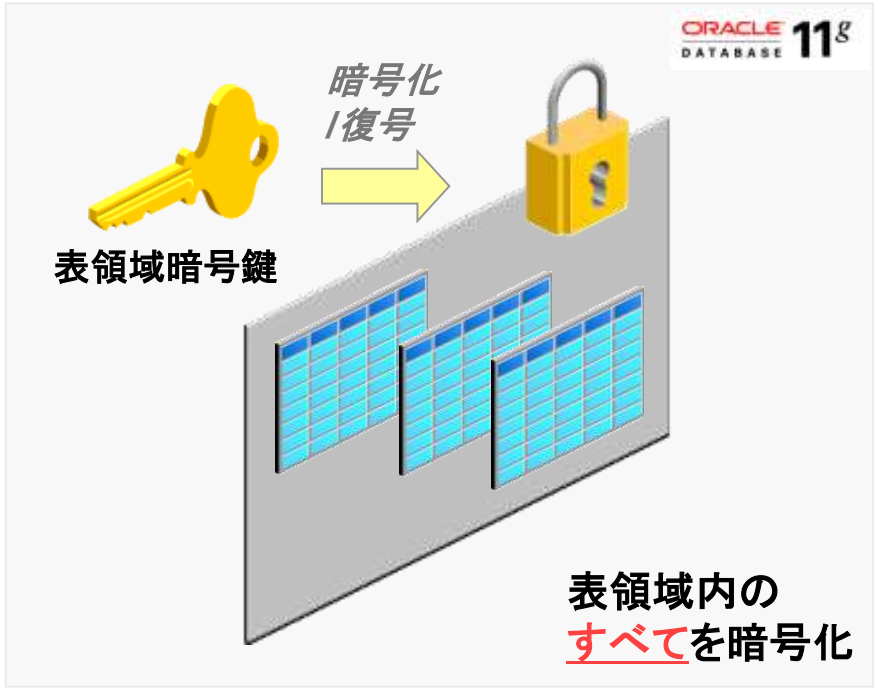


Copyright© 2010, Oracle. All rights reserved.

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（10g～）
  - 表領域暗号化: 表領域内のすべてのデータを暗号化（11g～）





Copyright© 2010, Oracle. All rights reserved.

列暗号化、表領域暗号化の特徴

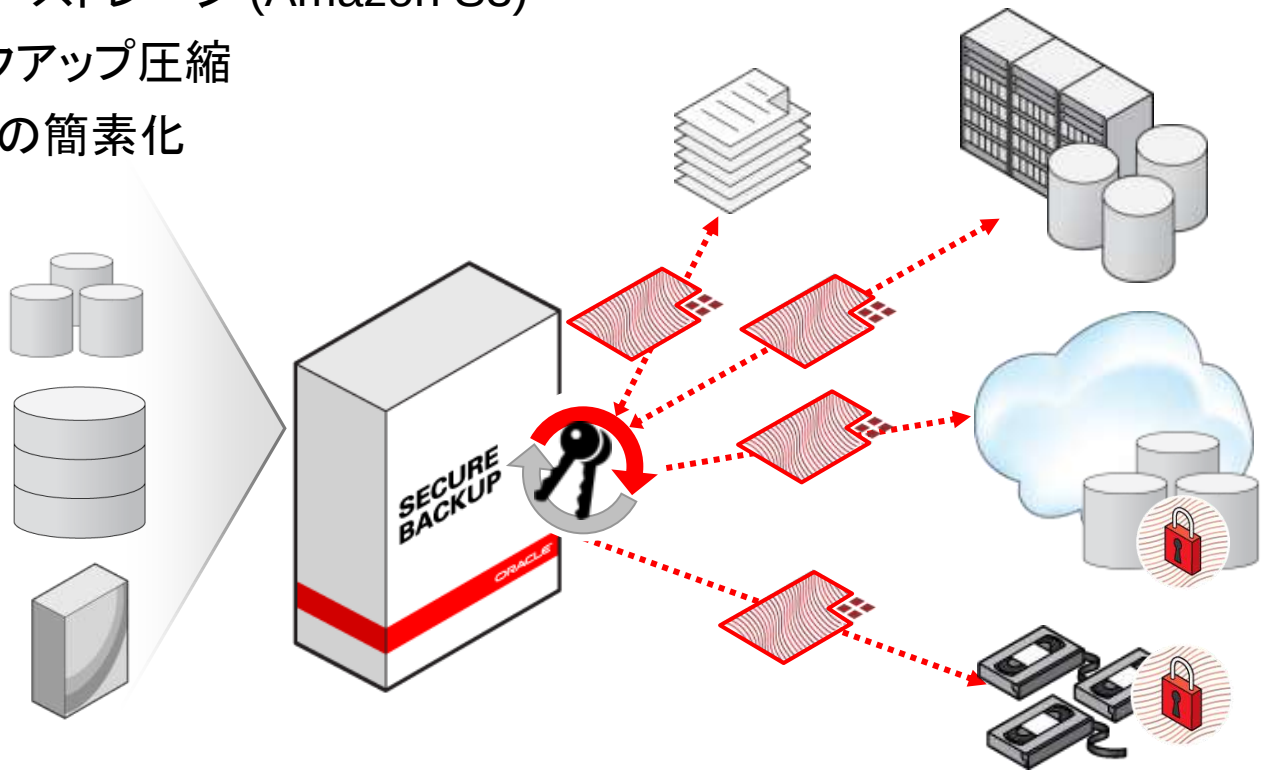
	列暗号化	表領域暗号化
暗号化のタイミング	行アクセス時	データ・ブロックに対する I/O発生時
暗号化アルゴリズム	3DES168, AES128 ,AES192 ,AES256	
暗号化により保護される場所	メモリ、ディスク	ディスク
データサイズ	暗号化対象データの量に比例して増加	暗号化前と変わらない
性能への影響	暗号化列へのアクセス頻度に応じて劣化	暗号化表領域のディスクI/O頻度に応じて劣化
対象オブジェクト	列のみ 暗号化列に対する索引は、 B-Tree索引の一意検索のみ可能	表領域内のすべてのオブジェクト BITMAP索引の作成やB-Tree索引の範囲検索も利用可能

目標とするセキュリティ・レベルと許容できる可用性のトレードオフが重要

Copyright© 2010, Oracle. All rights reserved.

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
  - クラウド・ストレージ (Amazon S3)
- 高速なバックアップ圧縮
- 暗号鍵管理の簡素化



Copyright© 2010, Oracle. All rights reserved.

外部パスワード・ストア

- クライアントアプリケーション・コードやバッチジョブのスクリプト内に埋め込まれているユーザIDとパスワードを隠蔽化
- DBへアクセスするためには、クライアント側にOracle Walletが必要
- ユーザー名やパスワードを変更する場合は、Oracle Walletのみの変更で対応可能

10gR2～ 接続名ora003 、ユーザー SCOTTで接続できる外部パスワード・ストアの作成

```
/* クライアント側にOracle Walletを作成
mkstore -wrl /home/oracle –create

/* データベースへ接続するID・パスワード情報をOracle Walletに格納
mkstore -wrl ./ewallet.p12 -createCredential ora003 scott

/*  sqlnet.oraにOracle Walletの格納場所とSQLNET.WALLET_OVERRIDE =TRUEを記述
WALLET_LOCATION = (SOURCE =
                                (METHOD = FILE)
                                   (METHOD_DATA =
                                    (DIRECTORY =/home/oracle)))
SQLNET.WALLET_OVERRIDE = TRUE

/* 接続は、conn / @接続名
sqlplus /nolog
conn /@ora003
```

Copyright© 2010, Oracle. All rights reserved.

PL/SQLコードの不明瞭化

- PL/SQLのソースコードを不明瞭化することで、リバース・エンジニアリングの防止
- PL/SQL内のパスワードの隠蔽化という意味合いとして使用することもできるが、必ずしも完全とは限らないので、補助的に使用することを推奨

Wrapコマンドを使用したPL/SQLコードの不明瞭化

```
wrap iname=testpkg.sql oname=testpkg.msk

/*  testpkg.sql  <<  ラップ前
CREATE PROCEDURE wraptest IS
  TYPE emp_tab IS TABLE OF employees%ROWTYPE INDEX BY PLS_INTEGER;
  all_emps      emp_tab;
BEGIN
  SELECT * BULK COLLECT INTO all_emps FROM employees;
  FOR i IN 1..10 LOOP
    DBMS_OUTPUT.PUT_LINE('Emp Id: ' || all_emps(i).employee_id);
  END LOOP;
END;

/* testpkg.msk      <<  ラップ後
Abcd
JyCqeg/SBs0t2VaEY1VRHFP5vRMwg+nw2SdqfC/pmDzqaC76Czjsee0Y2FIEZTznoRsI8o6D
AaigN36bCI0uBXR0TkX+WeOD9/3v7jOBn74/zw+v+qZCnjar5voSunhN6eeDctqz9BYAgABi
xTNK/0u2rBoVIus34LrzEvcJPb0M5MKjCyndvEG2vTKIurTMSn3Dpy2Sge6KjMvQ0IKgsefi
xYrsyf7hzLLJ1NraGlELywtIJ284rh6UEIfdu2RU7j+1sOJC6+R/mZjXX2y7byv2J7GrTtIdTlxafg==
```

Copyright© 2010, Oracle. All rights reserved.

見直すべき7つの項目

1. 初期設定
2. 認証
3. 権限管理
4. 特権ユーザ管理
5. 不正アクセス
6. 暗号化
7. 監査

無償技術サービスOracle Direct Concierge

- Oracle Database バージョンアップ支援
- Oracle 構成相談(Sizing)サービス
- パフォーマンス・クリニック・サービス
- SQL Serverからの移行アセスメント
- DB2からの移行支援サービス
- Sybaseからの移行支援サービス
- MySQLからの移行相談サービス
- PostgreSQLからの移行相談 サービス
- Accessからの移行アセスメント
- Oracle Developer/2000 Webアップグレード相談
- 仮想化アセスメントサービス
- ビジネスインテリジェンス・エンタープライズ エディション・アセスメントサービス
- 簡易業務診断サービス

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

Copyright© 2010, Oracle. All rights reserved.

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	
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） ・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)

Copyright© 2010, Oracle. All rights reserved.

DBA監査

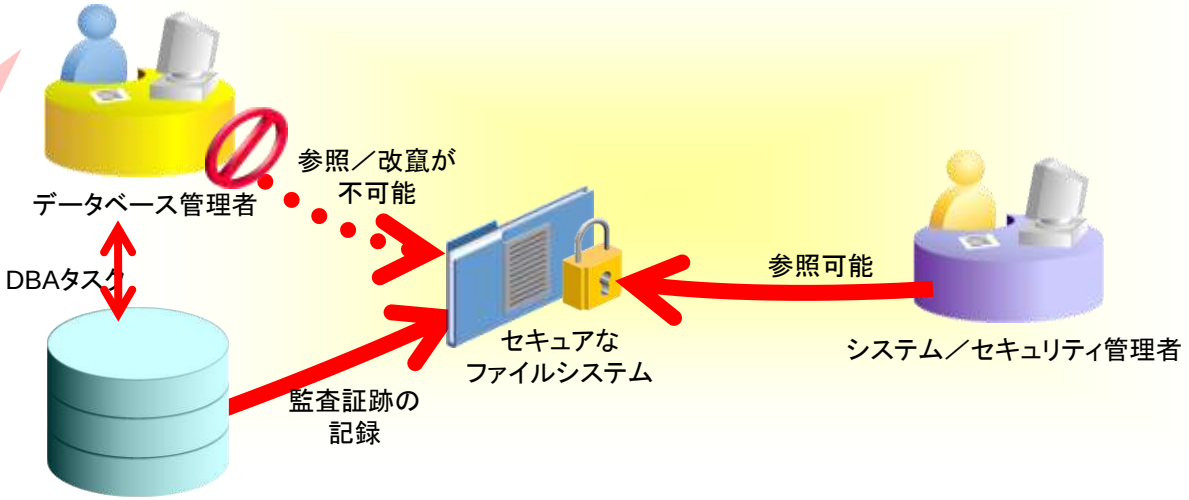
正当なDBA権限を持ったユーザーによる不正アクセスへの対策:

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



Copyright© 2010, Oracle. All rights reserved.

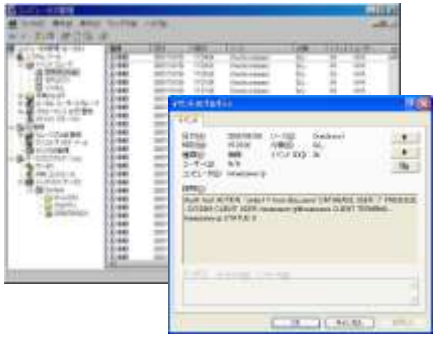
DBA監査（詳細）

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
```

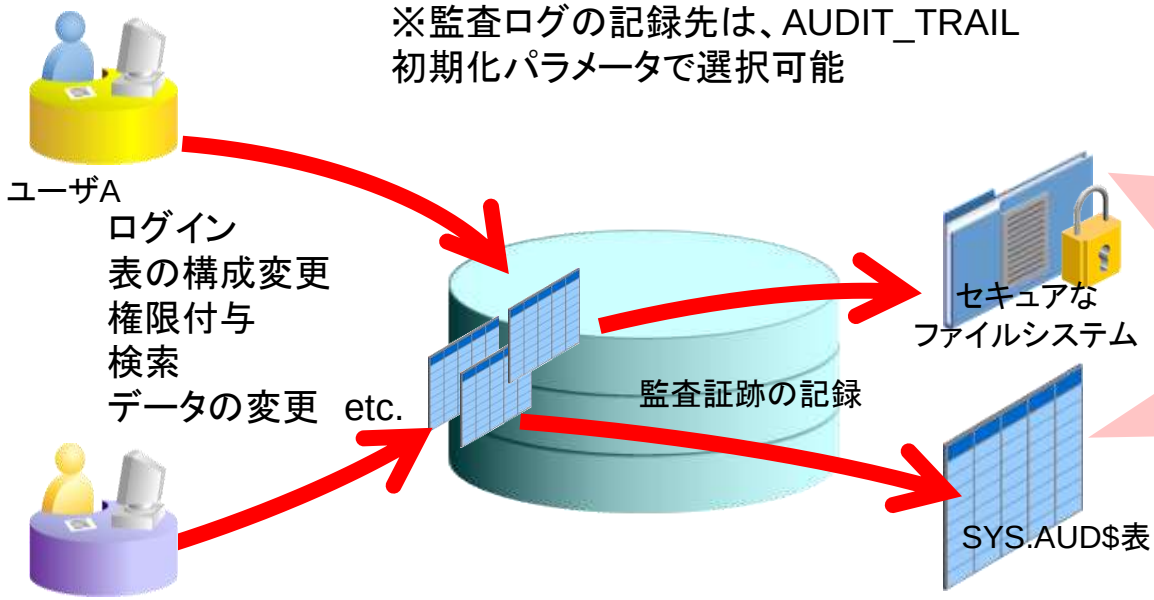
イベント・ビューア



Copyright© 2010, Oracle. All rights reserved.

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、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

Copyright© 2010, Oracle. All rights reserved.

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

Copyright© 2010, Oracle. All rights reserved.

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

Copyright© 2010, Oracle. All rights reserved.

FGA（ファイングレイン）監査

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

SELECT order_id, product_id, quantity
FROM order_items;

監査されない

監査ポリシ

監査条件: 1=1 (全ての行)
監査列 :card_no

監査証跡が残る

SELECT order_id, card_no
FROM order_items;

監査証跡

SELECT order_id, card_no
FROM order_items,
<timestamp>, <userid>,
<bind vars>
etc.

Copyright© 2010, Oracle. All rights reserved.

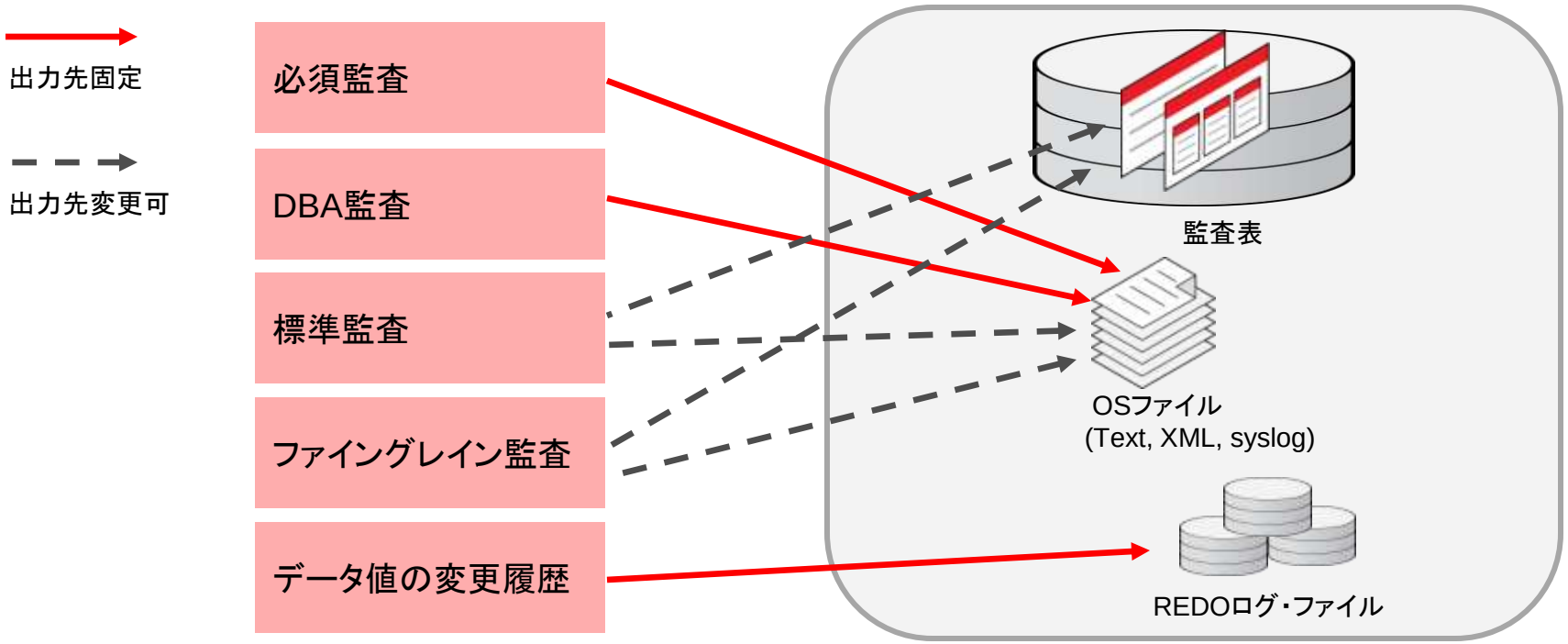
FGA監査（詳細）

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

Copyright© 2010, Oracle. All rights reserved.

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)



Copyright© 2010, Oracle. All rights reserved.

監査設定で考えるべきポイント

- Oracle Databaseの監査機能によって、性能へ影響を与える要素は主に以下の二つ
  - 監査ログのDisk I/O

✓ DB内に監査ログを出力する場合は、AUD$表へのINSERT処理が発生するためDIskの性能に大きく依存する。そのため、ディスクのストライピングやデータファイルとRedoログファイルを配置するディスクとは別にするなど、I/Oを分散するなどの対処が必要

✓ OSへの出力は、上記のようなチューニングしなくても性能への影響が低いため、OSやXMLで出力することも検討すべき

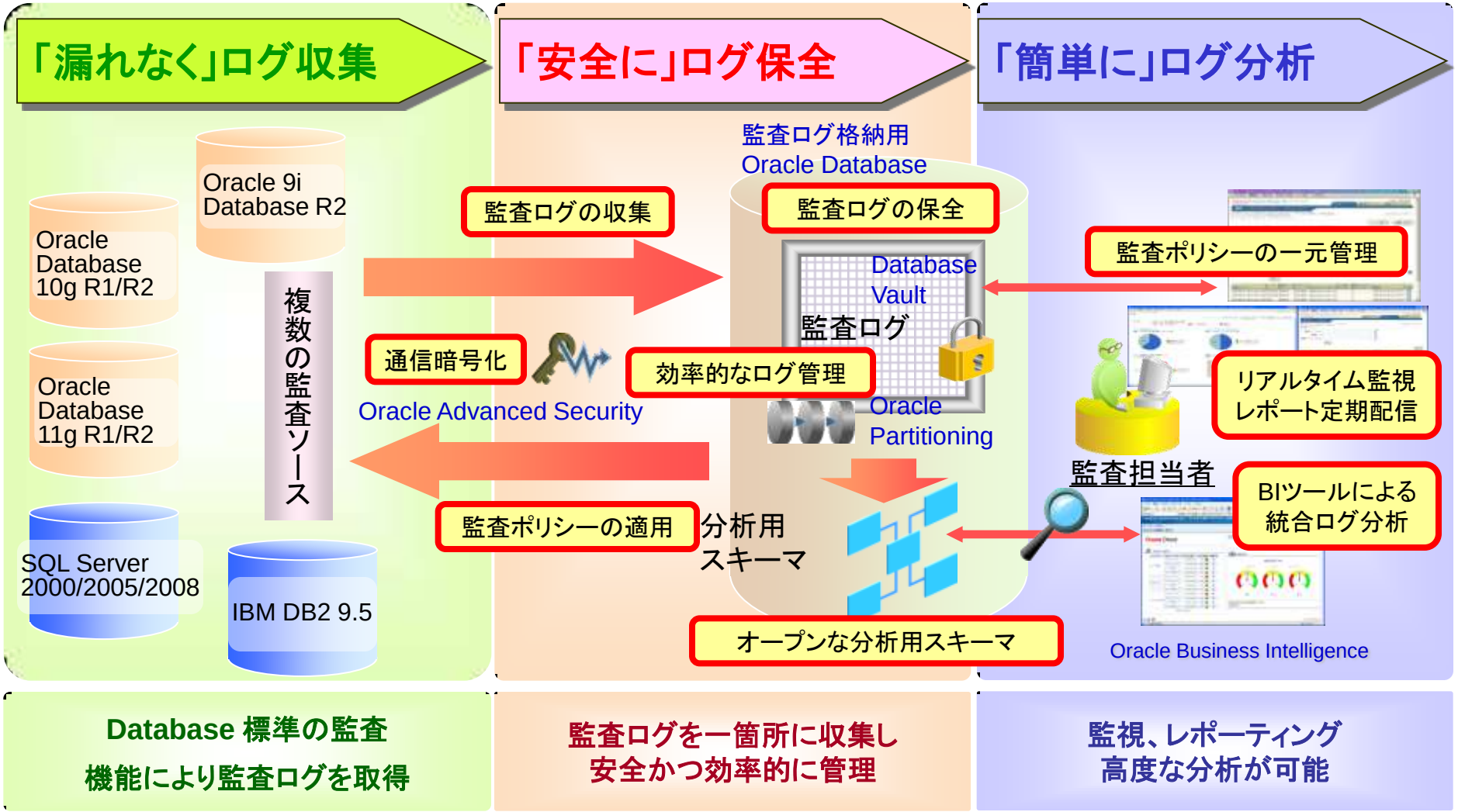
  - 監査対象へのヒット率

✓ 実際のシステムでは、すべての表やSQLに対して監査設定をすることは、監査ログを格納するディスク領域やログ分析の観点から見ても現実的ではない。
この事から、全体のSQLに対して何%が監査対象になるかというのが影響への目安となる

✓ データの機密度レベル、対応すべきコンプライアンス、法的証拠としてのログ、事故が発生した場合の追跡に役立つログなど、本当に必要なログのみを取捨選択することが必要

Copyright© 2010, Oracle. All rights reserved.

Oracle Audit Vaultによるログ管理の自動化



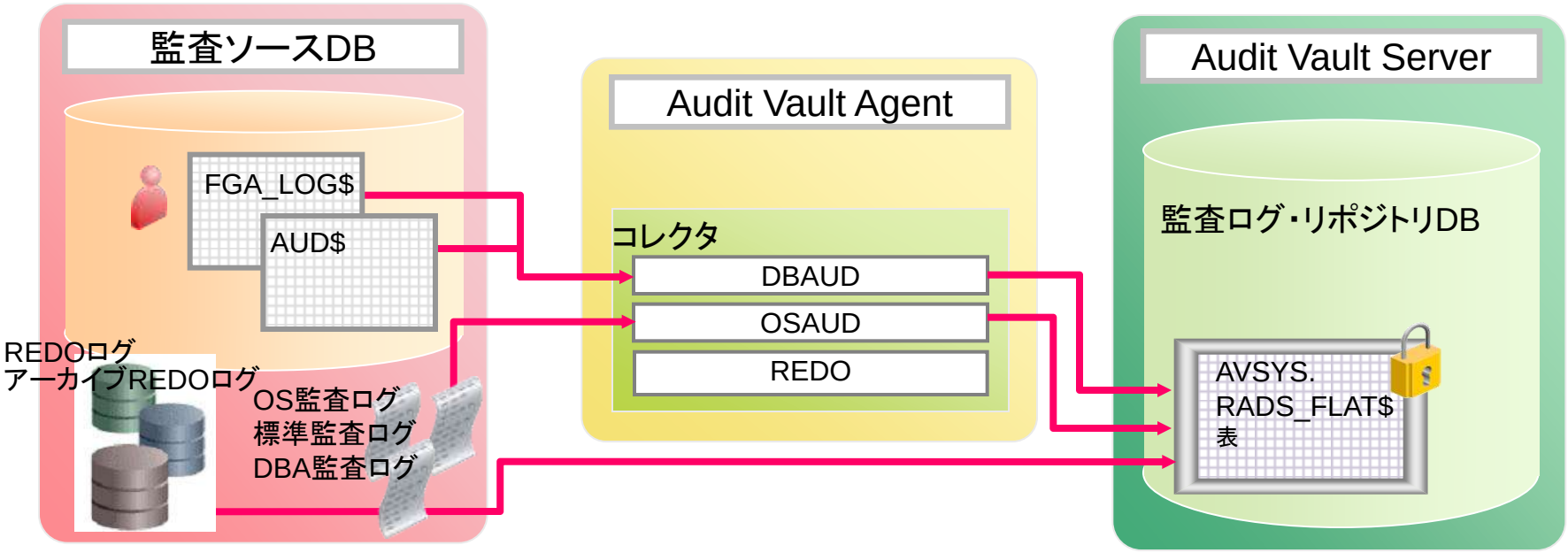
Database 標準の監査機能により監査ログを取得

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

Copyright© 2010, Oracle. All rights reserved.

ログ収集機能



監査ログの確実な収集

データベースの監査機能で生成されるログを収集するため、
メモリ・アクセス型やネットワーク・スニファ型のようなログの取りこぼしは発生しない。

Oracle Database との親和性

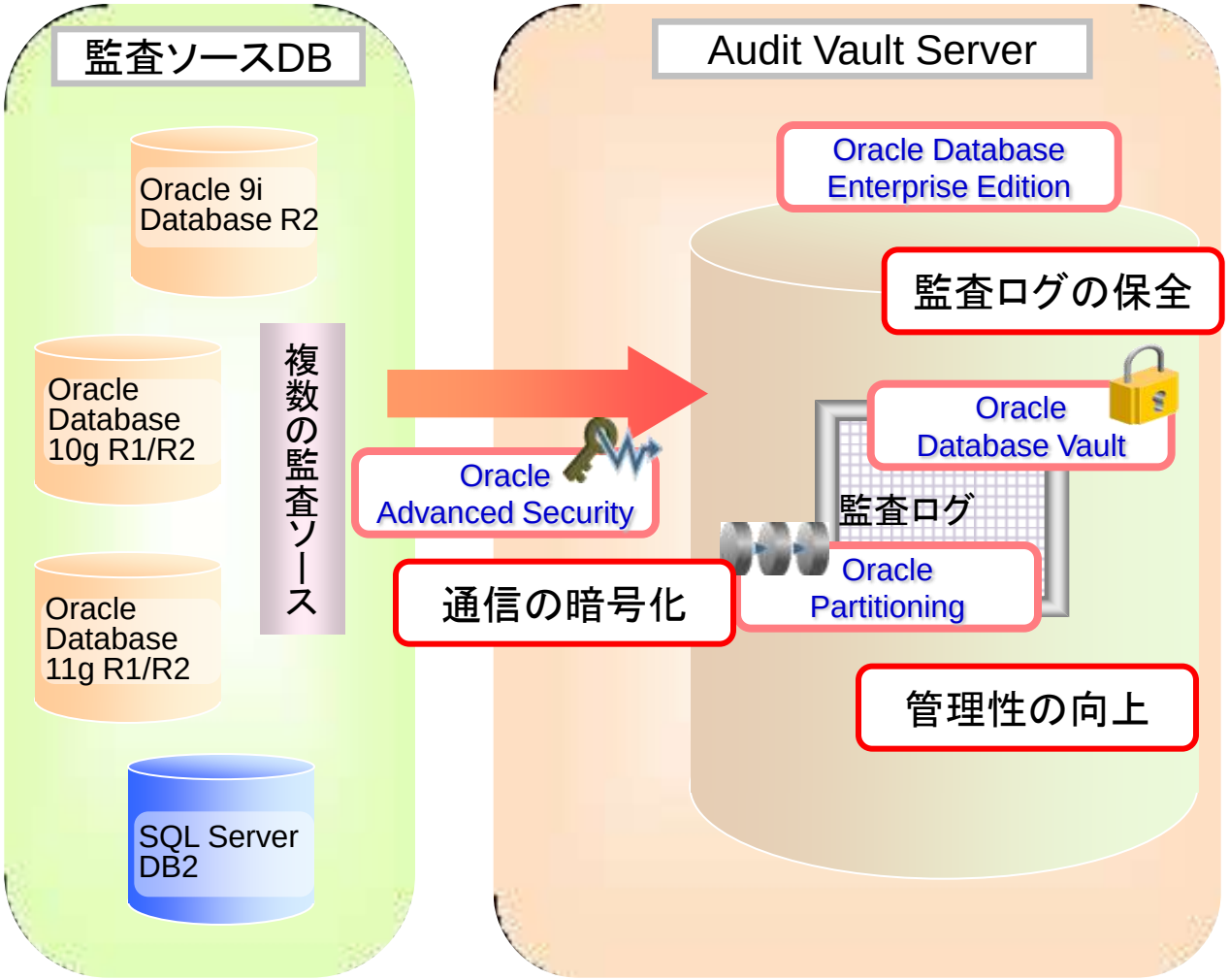
標準監査だけではなく、ファイングレイン監査(FGA)や、REDOログの変更履歴からも監査ログを収集することが可能。また、監査ログの形式もDB、OSファイルともに対応。

複数データベースの監査ログの一元管理

複数の監査対象データベースから取得した監査ログを一元管理。また、ログの種類や形式を正規化するため、一元的な分析が可能。

Copyright© 2010, Oracle. All rights reserved.

ログ保全/管理機能



ログの保全と効率的な管理

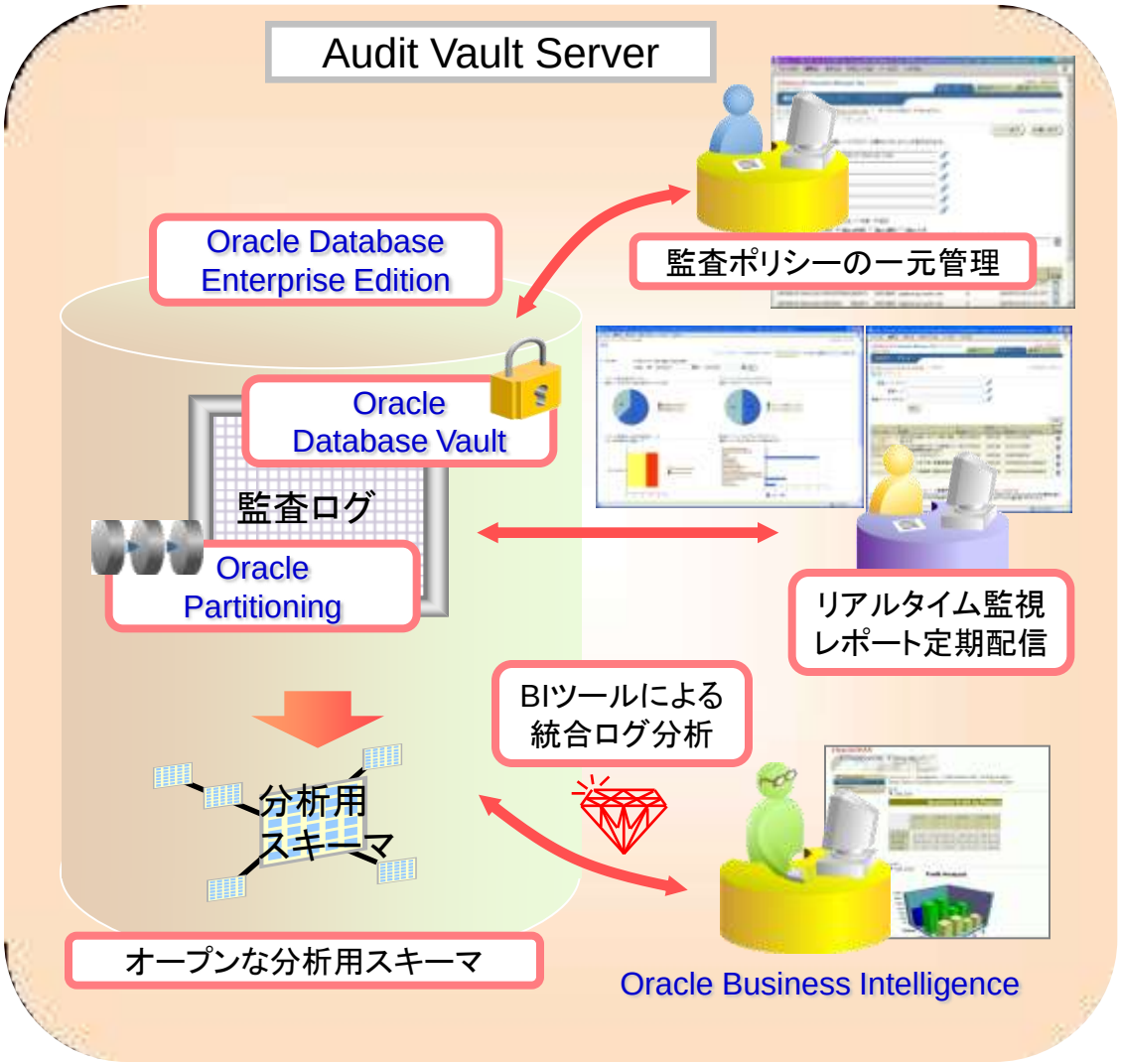
Audit Vault Serverには、Oracle Databaseの下記ライセンスが含まれており、Oracle Database Enterprise Editionの持つ高度なセキュリティ機能、管理機能をベースとして使用

- Oracle Advanced Security
- Oracle Database Vault
- Oracle Partitioning

監査ログの収集および格納時の安全性や管理性を向上させることで、ログの保全を実現

Copyright© 2010, Oracle. All rights reserved.

ログ分析/レポート機能



モニタリング・レポーティング

専用コンソールを利用した監査ログの監視や分析、用途に応じたレポートの生成が可能。

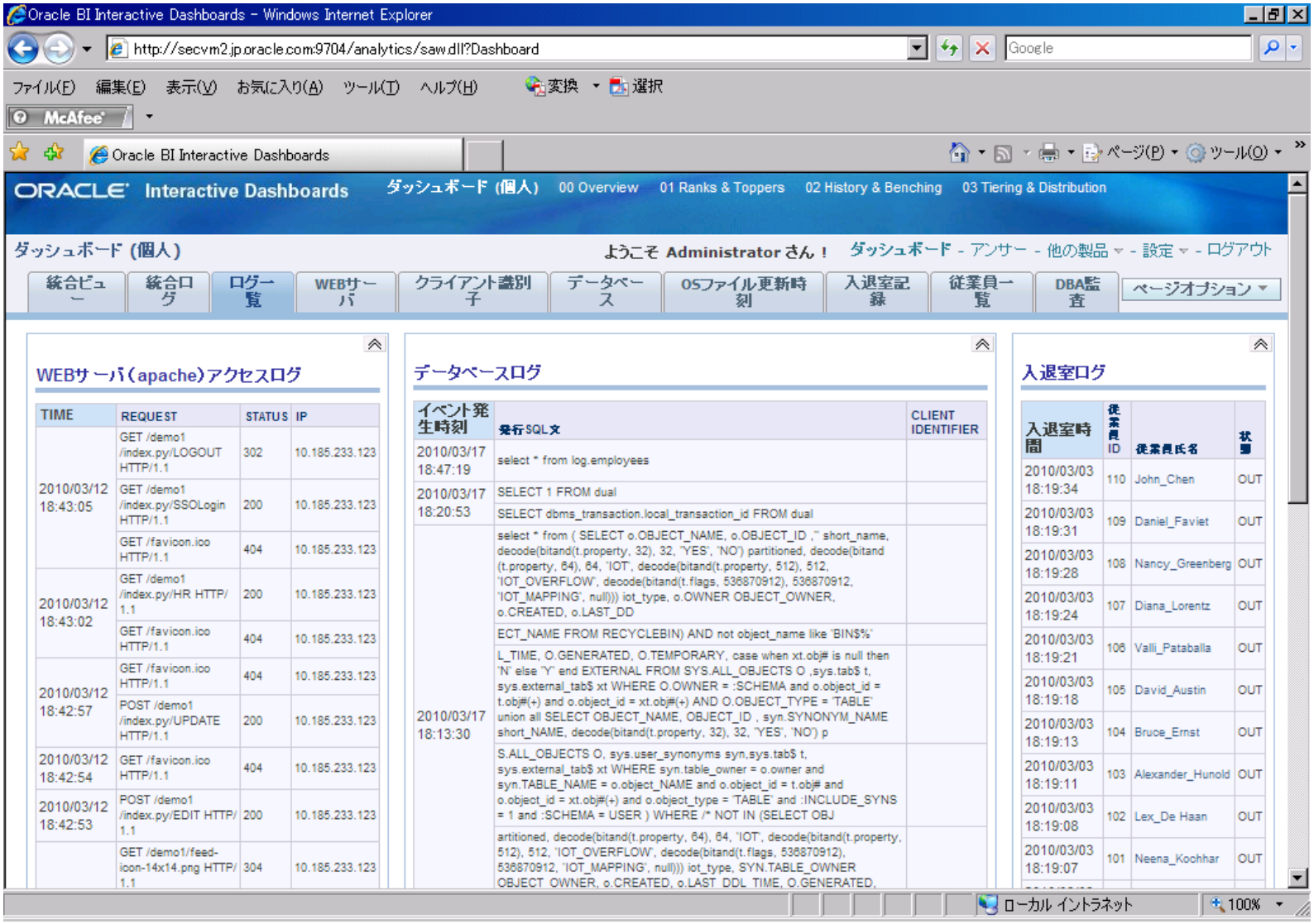
また、監査対象データベースの監査ポリシー設定の閲覧、変更が可能。

詳細かつ高度な分析

監査ログの分析用スキーマが公開されているため、Oracle BI 等の分析ツールを利用して詳細な分析を行うことが可能。

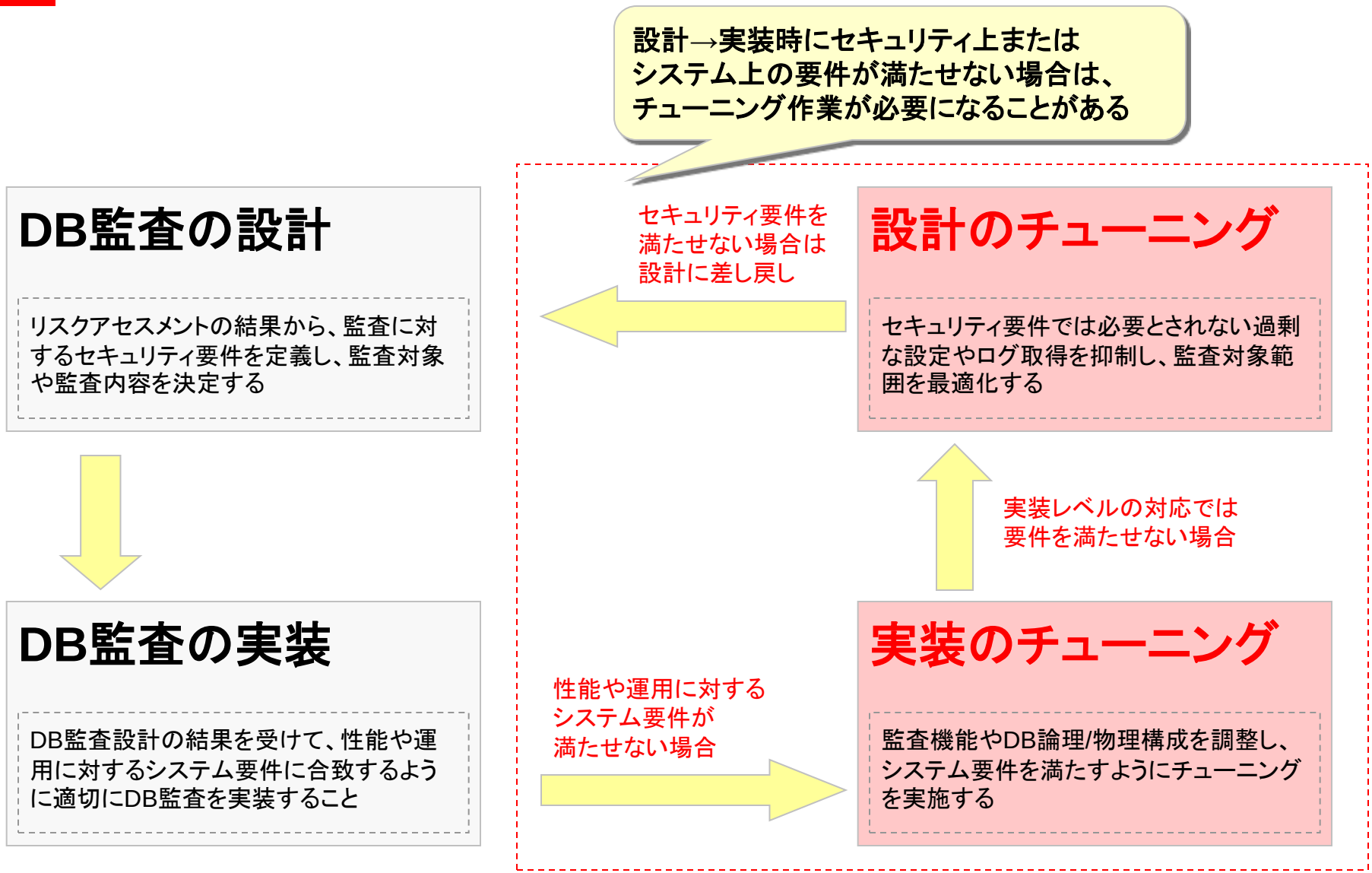
Copyright© 2010, Oracle. All rights reserved.

統合ログ分析



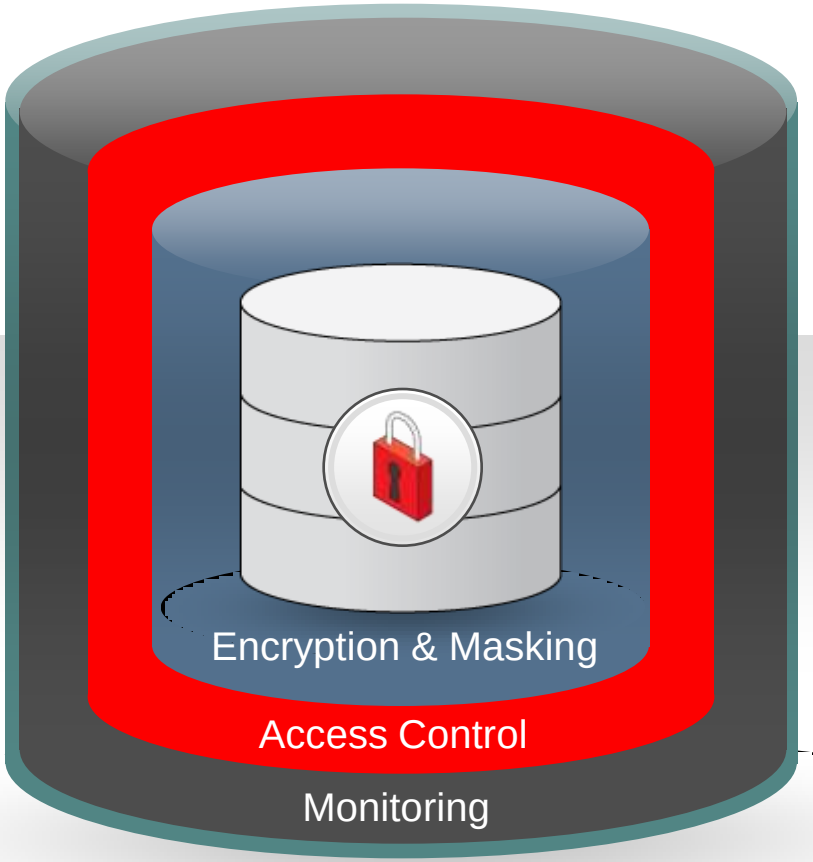
Copyright© 2010, Oracle. All rights reserved.

DB監査の設計と実装



Copyright© 2010, Oracle. All rights reserved.
62

Oracle Database Security



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)

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)

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

Copyright© 2010, Oracle. All rights reserved.

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。

Copyright© 2010, Oracle. All rights reserved.

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。

Copyright© 2010, Oracle. All rights reserved.

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

Copyright© 2010, Oracle. All rights reserved.

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）

ORACLE

Copyright© 2010, Oracle. All rights reserved.

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。

OracleとJavaは、Oracle Corporation 及びその子会社、関連会社の米国及びその他の国における登録商標です。
文中の社名、商品名等は各社の商標または登録 商標である場合があります。

Copyright© 2010, Oracle. All rights reserved.