ORACLE

Oracle Database 12cで進化したセキュリティ機能

NECラーニング株式会社
テクノロジー研修事業部
オラクル認定トレーナー
門間　義尚

#odddtky

日本オラクル、今年最大の技術トレーニング・イベント
Oracle DBA & Developer Day 2013

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。

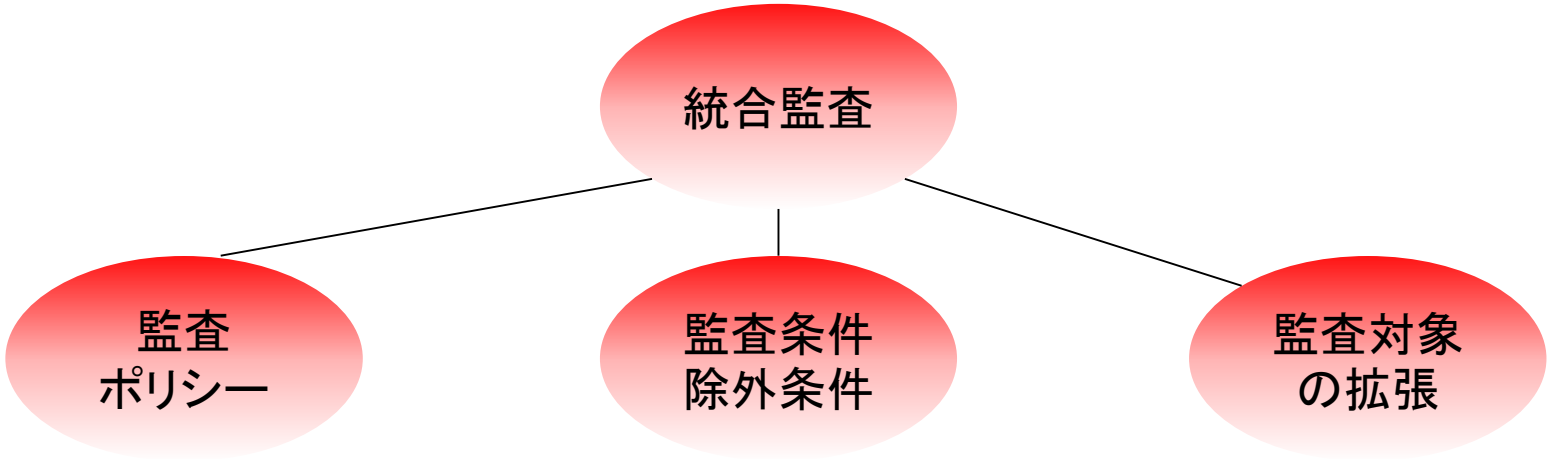
Program Agenda

- 12c新機能　統合監査
- 12c新しい権限と権限分析

12c新機能　統合監査

統合監査

従来は別々になっていた監査証跡を1つに統合



権限、ロール、オブジェクト、アクション毎の監査設定をグループ化

DBユーザー、OSユーザー、IPアドレス、アプリケーション等監査実行のための条件。または監査から除外する条件

DataPump、Rman、Database Vault,OLS等

統合監査変更点

11gまでの監査機能との比較

	~11g	12C~
監査の定義方法	監査対象オブジェクト毎に定義が必要	1つの監査ポリシーで複数の監査設定をグループ化可能
監査条件	細かい設定は不可	ユーザー、クライアント識別子、インスタンス等の条件設定が可能
ユーザーの指定	BYで監査ユーザー指定可能 ユーザーの除外設定は不可	BYで監査ユーザー指定可能 EXCEPTで除外ユーザーの指定可能
監査証跡の場所	SYSスキーマのAUD$表とFGA_LOG$表 OS上の監査証跡ファイル （テキスト形式・XML形式）	AUDSYSスキーマの読み取り専用表（CLI_SWP$...で始まる表）

統合監査のセキュリティ

セキュリティ

- 読み取り専用の監査証跡表に格納
  - 監査証跡が誤操作で削除される心配が不要
- 監査構成に関連する操作の監査
  - 監査ポリシーの作成、変更、削除、有効化は強制的に監査
- SYSユーザーのアクションの監査
- 監査管理用のロールの導入により監査管理職務が分離
  - AUDIT_ADMINロール　　監査構成の管理用
  - AUDIT_VIEWERロール　監査証跡の参照用

統合監査のパフォーマンス

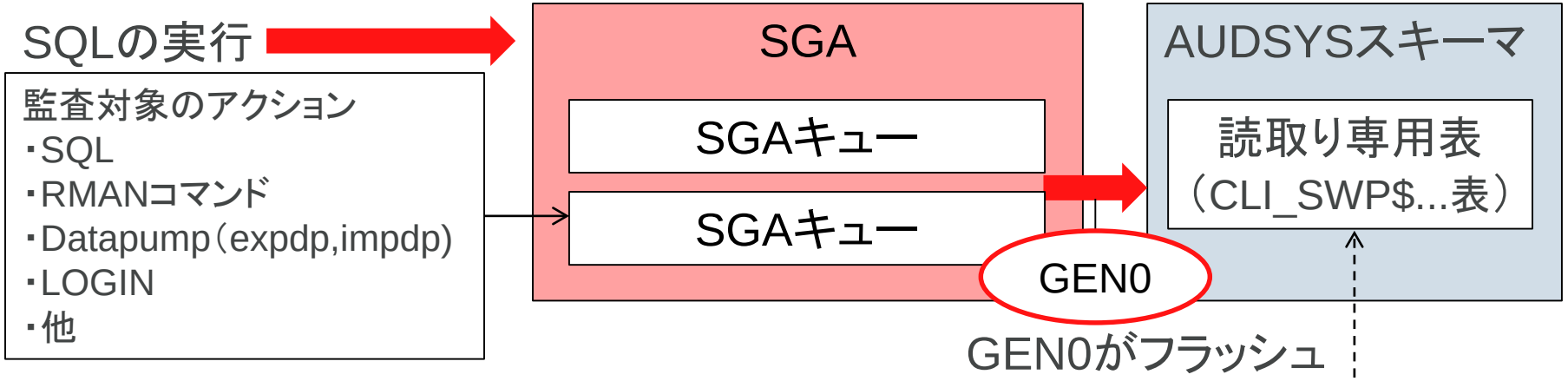
パフォーマンス（11gとの比較）

- 11gまでは監査証跡が作成される度にディスクにフラッシュ
  - パフォーマンスに多少の影響

- 12cの監査はメモリーに監査証跡を蓄積
  - パフォーマンスへの影響はごくわずか

統合監査のアーキテクチャ

SGAキューへの書き込み



SGAキュー

- SGA内の監査証跡を格納する領域
- クライアント毎に2つのキューがある
- 1つ目のキューが書込み中でもクライアントは2つ目のキューに書込みをする

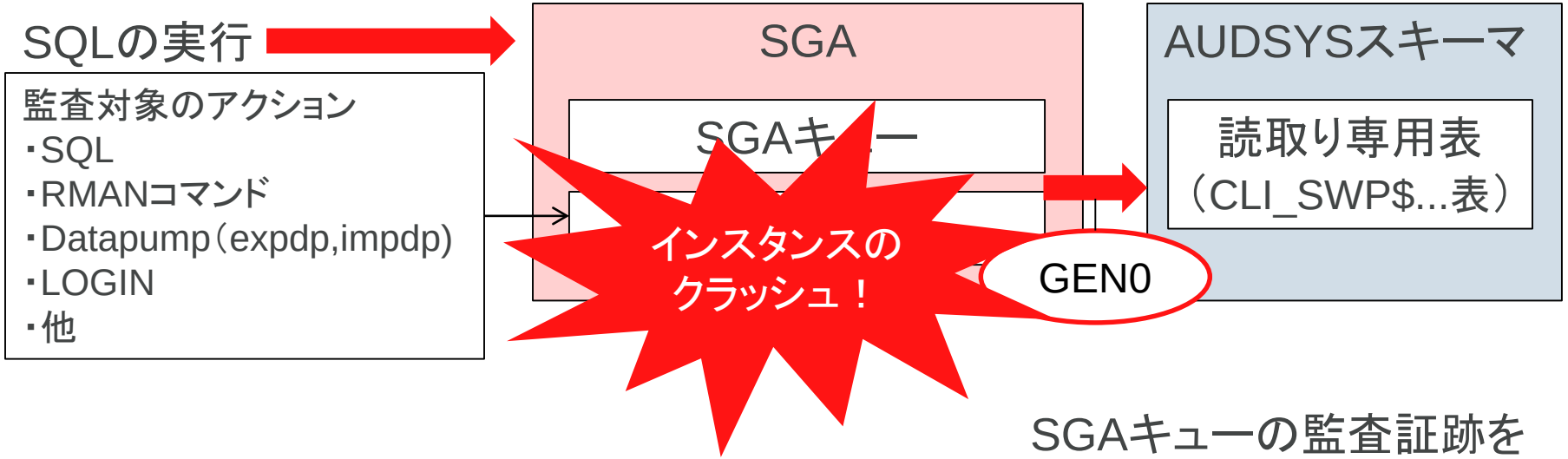
統合監査証跡のフラッシュ

GEN0による書込み

- 監査証跡のフラッシュはバックグランドプロセスのGEN0が行う
- AUDSYSスキーマの読み取り専用表に出力
- 自動フラッシュ
  - 3秒毎
  - SGAキューのしきい値に達した時
- 手動フラッシュ
  - EXECUTE DBMS_AUDIT_MGMT.FLUSH_UNIFIED_AUDIT_TRAIL;

監査証跡の損失

インスタンスのクラッシュ時



SGAキューの監査証跡を
損失する可能性がある

監査証跡の書き込みモード

キュー書き込みモードと即時書き込みモード

書き込みモード	特徴
キュー書き込みモード	・SGAキューへの非同期書き込み ・UNIFIED_AUDIT_SGA_QUEUE_SIZE初期化パラメータでSGAキューのサイズを指定 ・インスタンスクラッシュやABORT停止等でSGAキュー内の監査証跡を損失する可能性 ・12cのデフォルト
即時書き込みモード	・11g同様の同期書き込み ・インスタンスクラッシュでも監査証跡は損失しない ・パフォーマンスへの悪影響は従来と同じ程度

監査証跡の書き込みモード

キュー書き込みモードと即時書き込みモード：設定方法

```
EXECUTE DBMS_AUDIT_MGMT.SET_AUDIT_TRAIL_PROPERTY(-
  DBMS_AUDIT_MGMT.AUDIT_TRAIL_UNIFIED,-
  DBMS_AUDIT_MGMT.AUDIT_TRAIL_WRITE_MODE,-
  DBMS_AUDIT_MGMT.AUDIT_TRAIL_IMMEDIATE_WRITE);
```

即時書き込み：AUDIT_TRAIL_IMMEDIATE_WRITE
キュー書き込み：AUDIT_TRAIL_QUEUED_WRITE

基本監査情報と拡張監査情報

コンポーネントの固有のアクションの監査

- 基本監査情報
  - ユーザー名
  - インスタンス番号
  - データベースID
  - 実行されたアクション、SCN、オブジェクト名、SQL文
- 拡張監査情報の列
  - DP_XXX列　　DataPump操作
  - RMAN_XXX列　RMAN操作
  - OLS_XXX列　　Oracle Label Security操作
  - FGA_XXX列　　FGA監査証跡

基本監査情報と拡張監査情報は両方1つのビュー(UNIFIED_AUDIT_TRAIL)から参照できる

2つの監査モード

混在監査モードと統合監査モード

- 混在監査モード（12cのデフォルトモード）
  - 11gまでの従来式と12cからの新しい監査の仕組みを同時に実行
  - 従来式が動作するためパフォーマンスへの悪影響の可能性
- 統合監査モード
  - 新しい統合監査のみが使用可能。従来式の監査の仕組みは使用不可
  - 従来使用していたAUDIT_XXX初期化パラメータは受け付けなくなる

監査ポリシー

監査設定をグループ化

- 監査ポリシーの作成
- 監査ポリシーの有効化.
- 監査ポリシーの表示
  - ポリシー名、監査対象の権限・ロール・アクション等
- 監査ポリシーの削除

監査ポリシーの作成

CREATE AUDIT POLICYコマンド 1

・システム権限の使用を監査

```
CREATE AUDIT POLICY AUDIT_DML_ANY
                PRIVILEGES UPDATE ANY TABLE,DELETE ANY TABLE;
```

・ロールの使用を監査

```
CREATE  AUDIT POLICY AUDIT_RESOURCE_ROLE
                ROLES RESOURCE;
```

監査ポリシーの作成

CREATE AUDIT POLICYコマンド 2

・アクションを監査

```
CREATE AUDIT POLICY AUDIT_TABLE_CREATE
            ACTIONS CREATE TABLE;
```

・1つの監査ポリシーに複数の監査設定を含める

```
CREATE AUDIT POLICY AUDIT_MIX
            PRIVILEGES SELECT ANY TABLE
            ACTIONS DROP TABLE,TRUNCATE TABLE
            ROLES SCHEDULER_ADMIN;
```

監査ポリシーの作成

CREATE AUDIT POLICYコマンド 3

・オブジェクト固有の監査

```
CREATE AUDIT POLICY AUDIT_DEPT
            ACTIONS SELECT,UPDATE,DELETE
            ON SCOTT.DEPT;
```

・データベース上の全ての操作を監査対象とする

```
CREATE AUDIT POLICY AUDIT_ALL
            ACTIONS ALL;
```

監査ポリシーの作成

CREATE AUDIT POLICYコマンド 4

・ユーザー指定の監査ポリシー

```
CREATE AUDIT POLICY AUDIT_SCOTT
            ACTIONS RENAME ON HR.DEPARTMENTS
WHEN ‘SYS_CONTEXT(‘’USERENV’’,’’SESSION_USER’’)=‘’SCOTT’’’
EVALUATE PER SESSION;
```

・EVALUATE PER SESSION　　セッション単位
・EVALUATE PER STATEMENT　　SQL文単位
・EVALUATE PER INSTANCE　　インスタンス存続期間中に1回のみ評価

監査ポリシーの有効化

AUDIT POLICYコマンド1

- 監査ポリシーの有効化

```
AUDIT POLICY AUDIT_DML_ANY;
```

- 特定のユーザーにのみ監査ポリシーを有効化

```
AUDIT POLICY AUDIT_RESOURCE_ROLE BY SCOTT;
```

- 特定のユーザーを監査対象から除外

```
AUDIT POLICY AUDIT_TABLE_ACTION EXCEPT JACK;
```

監査ポリシーの有効化

AUDIT POLICYコマンド2

・アクションの成功のみ監査

```
AUDIT POLICY  AUDIT_MIX WHENEVER SUCCESSFUL;
```

・アクションの失敗のみ監査

```
AUDIT POLICY  AUDIT_MIX WHENEVER NOT SUCCESSFUL;
```

・監査ポリシーの無効化

```
NOAUDIT POLICY AUDIT_MIX;
```

作成済み監査ポリシーの確認

AUDIT_UNIFIED_POLICIESとAUDIT_UNIFIED_POLICIESビュー

- AUDIT_UNIFIED_POLICIESビュー
  - 作成済み監査ポリシーの確認
- AUDIT_UNIFIED_ENABLED_POLICIESビュー
  - 有効化済み監査ポリシーの確認

監査ポリシーの削除

```
DROP AUDIT POLICY AUDIT_DML_ANY;
```

12c　新しい権限と権限分析

これまでの問題…

強すぎるSYSDBA権限

- SYSDBA管理権限は権限が非常に強い！
  - STARTUP,SHUTDOWN,データベースの作成削除、他
  - ほぼ全ての操作を実行可能
- 不正ユーザーにSYSDBAユーザーを使われると大問題！
- 12cではタスク固有の管理権限を導入！
  - SYSBACKUP
  - SYSDG
  - SYSKM

従来からの管理権限

SYSDBA、SYSOPER、SYSASM権限

権限	説明	ユーザー
SYSDBA	STARTUP,SHUTDOWN,データベースの作成・削除 等のデータベース管理に必要な全ての操作が可能。	SYS
SYSOPER	下記以外の管理操作全般が可能。 （データベースの作成・削除、不完全リカバリ、 キャラクタセットの変更、 PUBLIC以外のスキーマオブジェクトへのアクセス）	PUBLIC
SYSASM （11gNew!）	ASMインスタンスの管理権限。 データベースインスタンスへのアクセス権はなし	SYS

12cの新しい管理権限

SYSBACKUP、SYSDG、SYSKM権限

権限	説明	ユーザー
SYSBACKUP	バックアップ・リカバリ担当者向けの権限	SYSBACKUP
SYSDG	Oracle Data Guard操作の担当者向けの権限	SYSDG
SYSKM	暗号化鍵の管理者向けの権限	SYSKM
SYSDBA,SYSOPER, SYSASM	11gと同様	SYS/PUBLIC

SYSBACKUP権限

バックアップリカバリ担当者のための管理権限

- STARTUP,SHUTDOWN
- RMANのBACKUP,RESTORE,RECOVER
- データベースの作成・削除
- 制御ファイルの作成
- SPFILE,PFILEの作成
- ARCHIVELOGモードの有効・無効の切り替え
- データディクショナリ、V$ビュー、GV$ビューへの問い合わせ
- 他

SYSDG権限

Oracle Data Guard担当者のための管理権限

- STARTUP,SHUTDOWN
- ARCHIVELOGモードの有効・無効の切り替え
- データベースのフラッシュバック
- 保証付きリストアポイントの作成・削除
- プライマリデータベースとスタンバイデータベースの管理
- データディクショナリ、V$ビュー、GV$ビューへの問い合わせ
- 他

SYSKM権限

暗号化鍵の管理者向けの権限

- TDE（Transparent Data Encryption）操作が可能
  - キーストアの作成、オープンとクローズ
  - マスターキーの作成と変更
  - 列および表領域の鍵の管理
  - TDE情報を返すビューへのアクセス
- アプリケーションのデータにはアクセス不可
  - DESCRIBEは実行できない
  - アプリケーションデータへのSELECT、DMLも不可

ごみ箱内をパージする権限

新しいシステム権限 PURGE DBA_RECYCLEBIN

- （~11g）ごみ箱内のオブジェクトを全削除するにはSYSDBA権限が必要
  - CONNECT / AS SYSDBA
  - PURGE DBA_RECYCLEBIN

- （12c~）新しいシステム権限**PURGE DBA_RECYCLEBIN**を使用します
  - GRANT PURGE DBA_RECYCLEBIN TO SCOTT;
  - CONNECT SCOTT/tiger
  - PURGE DBA_RECYCLEBIN

権限分析

使われていない権限を検出

SELECT
DDL
DML
他

DB

権限分析
1. 分析ポリシー
2. 分析開始
3. 分析終了
4. レポート生成

使用されている権限
・SELECT ANY TABLE
・UPDATE ANY TABLE
・・・

使用されていない権限
・DELETE ANY TABLE
・CREATE TABLE
・・・

- 分析期間中に使用された権限、未使用の権限を検出
- データディクショナリビューからレポートを確認
- 未使用の権限を剥奪することで権限最小化の原則を実現。不正アクセスを防止

権限分析の手順

DBMS_PRIVILEGE_CAPTUREパッケージの使用

- 分析ポリシーの作成
  - ポリシー名、分析対象の指定
  - DBMS_PRIVILEGE_CAPTURE.CREATE_CAPTUREを使用
- 分析の開始と停止
  - DBMS_PRIVILEGE_CAPTURE.ENABLE_CAPTUREで分析開始
  - DBMS_PRIVILEGE_CAPTURE.DISABLE_CAPTUREで分析終了
- 分析レポートを生成
  - DBMS_PRIVILEGE_CAPTURE.GENERATE_RESULTを使用

権限分析の対象の指定

分析ポリシーで対象を指定

- データベース全体
  - データベース内の全ての権限の使用状況を分析
- ロール
  - 特定のロールの権限の使用状況を分析
- 条件
  - 特定の条件に合致する場合の権限の使用状況を分析
    （ユーザー名やアプリケーションコンテキストを条件にする）
- ロール + 条件

ポリシーの作成①

データベース分析ポリシーとロール分析ポリシー

・データベース分析ポリシーの作成

```
EXECUTE DBMS_PRIVILEGE_CAPTURE.CREATE_CAPTURE(-
        NAME => 'ALL_PRIVS',-
        DESCRIPTION => 'ALL PRIVS USED',-
        TYPE => DBMS_PRIVILEGE_CAPTURE.G_DATABASE);
```

・ロール分析ポリシーの作成

```
EXECUTE DBMS_PRIVILEGE_CAPTURE.CREATE_CAPTURE(-
        NAME => 'DBA_ROLE_PRIVS',-
        DESCRIPTION => 'DBA ROLE USED',-
        TYPE => DBMS_PRIVILEGE_CAPTURE.G_ROLE,-
        ROLES => ROLE_NAME_LIST('DBA'));
```

ポリシーの作成②

コンテキスト分析ポリシー

・コンテキスト分析ポリシーの作成

```
EXECUTE DBMS_PRIVILEGE_CAPTURE.CREATE_CAPTURE(-
        NAME => 'SCOTT_USED',-
        DESCRIPTION => 'SCOTT PRIVS',-
        TYPE => DBMS_PRIVILEGE_CAPTURE.G_CONTEXT,-
        CONDITION =>  -
            'SYS_CONTEXT(''USERENV'',''SESSION_USER'')=SCOTT'');
```

分析の開始と停止

ENABLE_CAPTUREとDISABLE_CAPTURE

・作成済みの分析ポリシー名を指定して分析を開始

```
EXECUTE DBMS_PRIVILEGE_CAPTURE.ENABLE_CAPTURE(-
              NAME => 'ALL_PRIVS')

---SQLの処理を実行---
---一定時間が経過後---
```

・分析を停止

```
EXECUTE DBMS_PRIVILEGE_CAPTURE.DISABLE_CAPTURE(-
              NAME => 'ALL_PRIVS')
```

レポートの生成

GENERATE_CAPTURE

・分析結果のレポートを作成します

```
EXECUTE DBMS_PRIVILEGE_CAPTURE.GENERATE_RESULT(-
              NAME => 'ALL_PRIVS')
```

使用された権限の表示

DBA_USED_PRIVSビュー

・使用されたシステム権限・オブジェクト権限を表示

```
SELECT USERNAME,SYS_PRIV,OBJ_PRIV,OBJECT_OWNER,OBJECT_NAME
FROM DBA_USED_PRIVS;
```

```
USERNAME   SYS_PRIV,              OBJ_PRIV,OBJECT_OWNER,OBJECT_NAME
---------------  --------------------------  -----------  ------------------------  --------------------
SCOTT          CREATE SESSION
SCOTT                                  SELECT    SYS                  DUAL
SCOTT                                  EXECUTE  SYS                  DBMS_OUTPUT
SCOTT          SELECT ANY TABLE                  HR                   DEPARTMENTS
SH             CREATE SESSION
SH                                     SELECT    SYSTEM               PRODUCT_PRIVS
```

使用されなかった権限の表示

DBA_UNUSED_PRIVSビュー

・使用されなかったシステム権限・オブジェクト権限を表示

```
SELECT USERNAME,SYS_PRIV,OBJ_PRIV,OBJECT_OWNER,OBJECT_NAME
FROM DBA_UNUSED_PRIVS WHERE USERNAME = 'SCOTT';

USERNAME   SYS_PRIV,                 OBJ_PRIV,OBJECT_OWNER,OBJECT_NAME
---------- -------------------------- ---------- ------------------------ --------------------
SCOTT      CREATE TABLE
SCOTT      CREATE CLUSTER
SCOTT      CREATE PROCEDURE
```

分析期間中、これらの権限は
使用されなかった。
それなら、これらの権限は不要なのでは？

NECラーニング
Oracle認定研修の紹介

■ORACLE トレーニング・オンデマンド
・インターネット接続により、いつでもお好きな時間に講義を視聴することができます。
・わからないところは何度でも繰り返して学習することができます。
・12月24日 まで申込いただくと、AMAZONギフト券10,000円分をプレゼント！！
・12月24日まで、無料体験キャンペーンを実施中！

詳しくは、こちらへ
HTTP://WWW.NECLEARNING.JP/TRAINING/ORACLE_TOD.HTML

■ORACLE認定 集合研修
・ORACLE認定集合研修も、常時開催中です！
・ORACLE DATABASE 12Cの研修も、2014年1月より開催します！

詳しくは、こちらへ
HTTP://WWW.NECLEARNING.JP/CO_RECOMMEND/SELECTION_ORACLE.HTML

Hardware and Software

ORACLE

Engineered to Work Together


ORACLE®