日日是Oracle APEX

Oracle APEXを使った作業をしていて、気の付いたところを忘れないようにメモをとります。

2021年8月16日月曜日

データベース・セキュリティの活用(6) - 権限分析(Privilege Analysis)

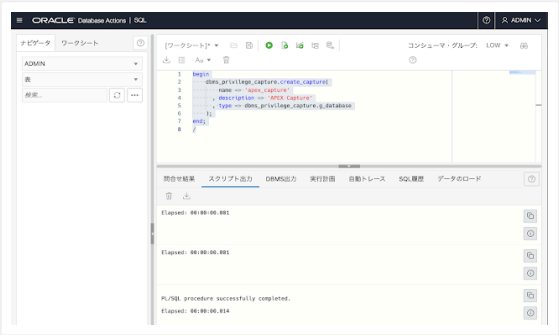
今回はロール**HR_ROLE**を作成しユーザーAPEXDEVに割り当てています。スキーマHRの表EMP, DEPTおよびビューEMP_DEPT_Vへのアクセス権限をこのロールに与えていますが、権限が適切に割り当たっているか、不要な権限が割り当たっていないかを確認します。

権限の使用状況を確認するために、**権限分析(Privilege Analysis)**を実施します。

権限分析ポリシーを**apex_capture**として作成します。**データベース・アクション**にユーザー**ADMIN**で接続して実行します。プロシージャDBMS_PRIVILEGE_CAPTURE.CREATE_CAPTUREを呼び出します。

```
begin
    dbms_privilege_capture.create_capture(
        name => 'apex_capture'
      , description => 'APEX Capture'
      , type => dbms_privilege_capture.g_database
    );
end;
/
```

seminar200825-create_capture.sql hosted with ❤️ by GitHub view raw

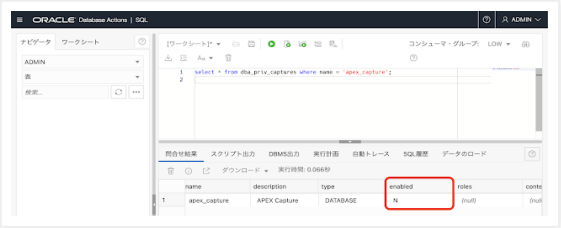


確認した範囲では、APEXアプリケーションからのアクセスがキャプチャされるのは、typeがdbms_privilege_capture.g_databaseのときだけでした。

ビューDBA_PRIV_CAPTURESから、作成した権限分析ポリシーを確認します。

```
select * from dba_priv_captures where name = 'apex_capture';
```

seminar200825-dba_priv_captures.sql hosted with ❤️ by GitHub view raw

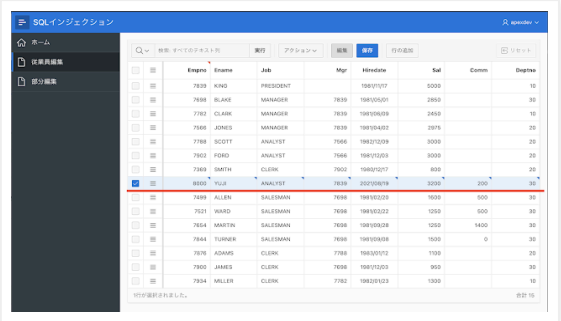


この時点ではキャプチャは開始されていません。プロシージャDBMS_PRIVILEGE_CAPTURE.ENABLE_CAPTUREを呼び出し、キャプチャを開始します。

```
begin
    dbms_privilege_capture.enable_capture(
        name => 'apex_capture'
      , run_name => 'RUN_FOR_SEMINAR'
    );
end;
/
```

seminar210825-enable_capture1.sql hosted with ❤️ by GitHub view raw

キャプチャを開始したので、APEXアプリケーションより実施する可能性のある操作をすべて実施します。表HR.EMPへ新規行の追加、更新、削除を行います。



キャプチャを停止します。プロシージャDBMS_PRIVILEGE_CAPTURE.DISABLE_CAPTUREを呼び出します。

```
begin
    dbms_privilege_capture.disable_capture(
      name => 'apex_capture'
    );
end;
/
```

seminar200825-disable_capture.sql hosted with ❤️ by GitHub view raw

今までキャプチャした内容から、権限分析レポートを生成します。プロシージャDBMS_PRIVILEGE_CAPTURE.GENERATE_RESULTを呼び出します。終了までに、それなりの時間がかかります。

```
begin
    dbms_privilege_capture.generate_result(
        name => 'apex_capture'
      , run_name => 'RUN_FOR_SEMINAR'
    );
end;
/
```

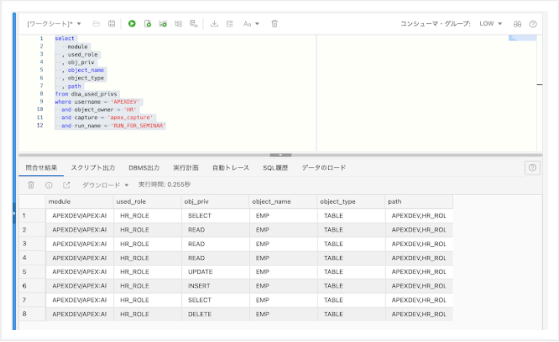
seminar200825-generate_report.sql hosted with ❤️ by GitHub view raw

操作で使用された権限は、ビューDBA_USED_PRIVSより確認することができます。

```
select
    module
  , used_role
  , obj_priv
  , object_name
  , object_type
  , path
from dba_used_privs
where username = 'APEXDEV'
  and object_owner = 'HR'
  and capture = 'apex_capture'
  and run_name = 'RUN_FOR_SEMINAR'
```

seminar210825-dba_used_privs.sql hosted with ❤️ by GitHub view raw

以下のような結果が得られます。



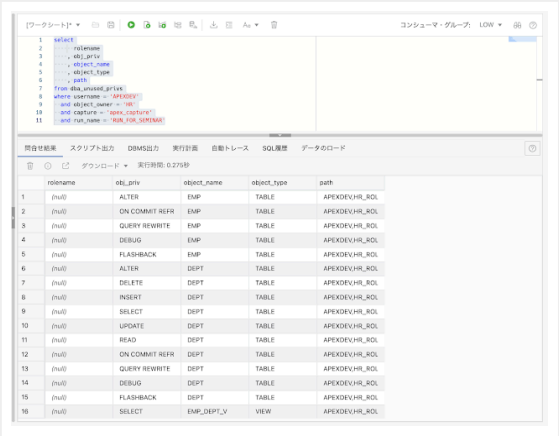
使用されなかった権限はビューDBA_UNUSED_PRIVSより確認できます。

```
select
      rolename
    , obj_priv
    , object_name
    , object_type
    , path
from dba_unused_privs
```

```
where username = 'APEXDEV'
  and object_owner = 'HR'
  and capture = 'apex_capture'
  and run_name = 'RUN_FOR_SEMINAR'
```

seminar200825-dba_unused_policies.sql hosted with ❤️ by GitHub view raw

以下のような結果が得られます。



今回の例ではAPEXアプリケーションより表DEPTを編集することはないため、SELECT以外の権限は不要です。SELECT以外の権限を表HR.DEPTより除いてみます。

```
revoke all on hr.dept from hr_role;
grant select on hr.dept to hr_role;
```

seminar210825-revoke_unsed_privs.sql hosted with ❤️ by GitHub view raw

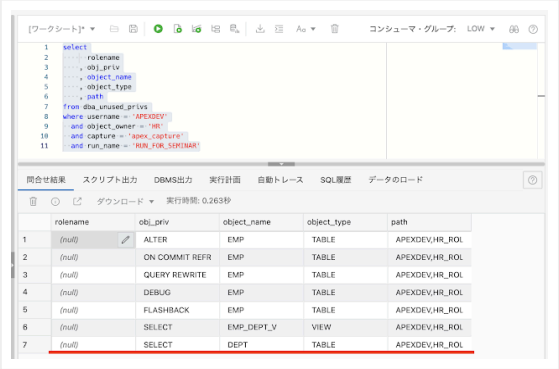
run_nameを変更してキャプチャし直すこともできますが、今回は、生成したレポートを削除して再実行します。プロシージャDBMS_PRIVILEGE_CAPTURE.DELETE_RUNを呼び出します。

```
begin
    dbms_privilege_capture.delete_run(
        name => 'apex_capture'
      , run_name => 'RUN_FOR_SEMINAR'
    );
end;
/
```

seminar200825-delete_run.sql hosted with ❤️ by GitHub view raw

再度、DBMS_PRIVILEGE_CAPTURE.ENABLE_CAPTURE、APEXアプリケーションの操作、DBMS_PRIVILEGE_CAPTURE.DISABLE_CAPTURE、そしてDBMS_PRIVILEGE_CAPTURE.GENERATE_RESULTを繰り返します。

ビューDBA_UNUSED_PRIVSを確認すると、表DEPTに対する未使用権限はSELECTのみになっています。



以上の操作を繰り返し、アプリケーションの接続ユーザーが本当に必要な権限だけを持つようにします。結果として、アプリケーションに不具合があっても、情報の流出や改ざんが発生しにくくなります。

権限分析ポリシーを削除するには、プロシージャDBMS_PRIVILEGE_CAPTURE.DROP_CAPTUREを呼び出します。

```
begin
    dbms_privilege_capture.drop_capture(
        name => 'apex_capture'
    );
end;
/
```

seminar200825-drop_capture.sql hosted with ❤️ by GitHub view raw

続く

Yuji N. 時刻: 17:50

共有

‹ ホーム ›

ウェブ バージョンを表示

自己紹介

Yuji N.

日本オラクル株式会社に勤務していて、Oracle APEXのGroundbreaker Advocateを拝命しました。
こちらの記事につきましては、免責事項の参照をお願いいたします。

詳細プロフィールを表示