

# 日々は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。

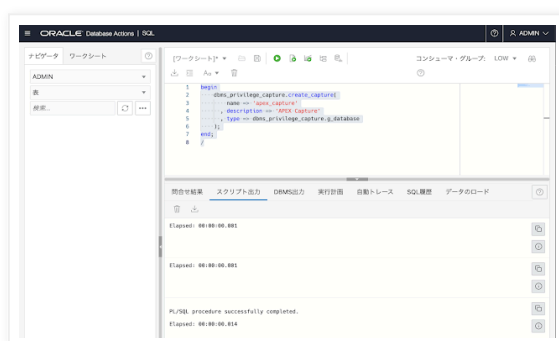
権限の使用状況を確認するために、**権限分析(Privilege Analysis)**を実施します。

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

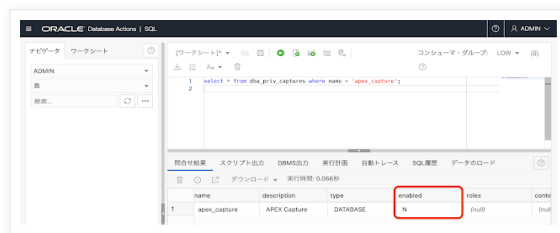
[view raw](#)



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';
```



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。

| Empno | Ename  | Job       | Mgr  | Hiredate   | Sal  | Comm | Empdate |
|-------|--------|-----------|------|------------|------|------|---------|
| 7229  | KING   | PRESIDENT |      | 1981/11/17 | 5000 |      | 12      |
| 7698  | BLAKE  | MANAGER   | 7619 | 1981/05/01 | 2850 |      | 20      |
| 7782  | CLARK  | MANAGER   | 7619 | 1981/06/09 | 2450 |      | 10      |
| 7660  | JONES  | MANAGER   | 7619 | 1981/04/02 | 2975 |      | 20      |
| 7788  | SCOTT  | ANALYST   | 7566 | 1982/07/09 | 3000 |      | 20      |
| 7802  | FORD   | ANALYST   | 7566 | 1981/12/03 | 3000 |      | 20      |
| 7369  | SMITH  | CLERK     | 7566 | 1980/12/17 | 800  |      | 20      |
| 8100  | TOL    | ANALYST   | 7619 | 2022/08/18 | 3000 | 20%  | 30      |
| 7299  | ALLEN  | SALESMAN  | 7619 | 1981/09/19 | 1600 | 30%  | 20      |
| 7511  | WARD   | SALESMAN  | 7619 | 1981/02/22 | 1050 | 30%  | 20      |
| 7654  | MARTIN | SALESMAN  | 7619 | 1981/09/28 | 1200 | 1400 | 30      |
| 7644  | TURNER | SALESMAN  | 7619 | 1981/09/08 | 1500 | 0    | 20      |
| 7676  | ADAMS  | CLERK     | 7788 | 1983/12/17 | 1100 |      | 20      |
| 7800  | JAMES  | CLERK     | 7698 | 1981/12/03 | 950  |      | 20      |
| 7934  | MILLER | CLERK     | 7782 | 1982/12/23 | 1300 |      | 10      |

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。

|   | module          | used_role | obj_priv | object_name | object_type | path            |
|---|-----------------|-----------|----------|-------------|-------------|-----------------|
| 1 | APEXDEV/APEXDEV | HR_ROLE   | SELECT   | EMP         | TABLE       | APEXDEV/HR_ROLE |
| 2 | APEXDEV/APEXDEV | HR_ROLE   | READ     | EMP         | TABLE       | APEXDEV/HR_ROLE |
| 3 | APEXDEV/APEXDEV | HR_ROLE   | READ     | EMP         | TABLE       | APEXDEV/HR_ROLE |
| 4 | APEXDEV/APEXDEV | HR_ROLE   | READ     | EMP         | TABLE       | APEXDEV/HR_ROLE |
| 5 | APEXDEV/APEXDEV | HR_ROLE   | UPDATE   | EMP         | TABLE       | APEXDEV/HR_ROLE |
| 6 | APEXDEV/APEXDEV | HR_ROLE   | INSERT   | EMP         | TABLE       | APEXDEV/HR_ROLE |
| 7 | APEXDEV/APEXDEV | HR_ROLE   | SELECT   | EMP         | TABLE       | APEXDEV/HR_ROLE |
| 8 | APEXDEV/APEXDEV | HR_ROLE   | DELETE   | EMP         | TABLE       | APEXDEV/HR_ROLE |

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。

| rowname | obj_priv | object_name    | object_type | path  |
|---------|----------|----------------|-------------|-------|
| 1       | (null)   | ALTER          | EMP         | TABLE |
| 2       | (null)   | ON COMMIT RSTR | EMP         | TABLE |
| 3       | (null)   | QUICK REWRITE  | EMP         | TABLE |
| 4       | (null)   | DEBUG          | EMP         | TABLE |
| 5       | (null)   | FLASHBACK      | EMP         | TABLE |
| 6       | (null)   | ALTER          | DEPT        | TABLE |
| 7       | (null)   | DELETE         | DEPT        | TABLE |
| 8       | (null)   | INSERT         | DEPT        | TABLE |
| 9       | (null)   | SELECT         | DEPT        | TABLE |
| 10      | (null)   | UPDATE         | DEPT        | TABLE |
| 11      | (null)   | READ           | DEPT        | TABLE |
| 12      | (null)   | ON COMMIT RSTR | DEPT        | TABLE |
| 13      | (null)   | QUICK REWRITE  | DEPT        | TABLE |
| 14      | (null)   | DEBUG          | DEPT        | TABLE |
| 15      | (null)   | FLASHBACK      | DEPT        | TABLE |
| 16      | (null)   | SELECT         | EMP_DEPT_V  | VIEW  |

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。

SQL Worksheet

```

1 select
2     rolename
3     , obj_priv
4     , object_name
5     , object_type
6     , path
7 from dba_unmasked_privs
8 where username = 'APEXDEV'
9 and object_name = 'HR'
10 and capture = 'APEX_CAPTURE'
11 and role_name = 'HR_ROLE_SIGNON!';
  
```

コンシューマ・グループ LOW (0)

問合せ結果 スクリプト出力 DBMS出力 実行計画 自動トレース SQL履歴 データのロード

ダウンロード 実行時刻: 0.263秒

|   | rolename | obj_priv      | object_name | object_type | path            |
|---|----------|---------------|-------------|-------------|-----------------|
| 1 | (null)   | ALTER         | EMP         | TABLE       | APEXDEV/HR_ROLE |
| 2 | (null)   | ON COMMIT REF | EMP         | TABLE       | APEXDEV/HR_ROLE |
| 3 | (null)   | QUERY REWRITE | EMP         | TABLE       | APEXDEV/HR_ROLE |
| 4 | (null)   | DEBUG         | EMP         | TABLE       | APEXDEV/HR_ROLE |
| 5 | (null)   | FLASHBACK     | EMP         | TABLE       | APEXDEV/HR_ROLE |
| 6 | (null)   | SELECT        | EMP_DEPT_V  | VIEW        | APEXDEV/HR_ROLE |
| 7 | (null)   | SELECT        | DEPT        | TABLE       | APEXDEV/HR_ROLE |

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

&gt;

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](#)

Powered by Blogger.