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(5) - ファイングレイン監査

統合監査ポリシーでは、表やビューを単位として操作ごとに監査証跡を取得します。現実には表のデータすべてについて監査が必要ということはなく、アクセス頻度の高い表ではパフォーマンス低下や大量に発生する監査証跡も負担になります。

ファイングレイン監査では監査証跡の取得を、特定の行および列に限定できます。

表HR.EMPのDEPTNO = 30の行の列SAL、COMMへのSELECTとUPDATEの実行に限定して監査証跡を取得する設定を行ってみます。

ファイングレイン監査ポリシーを、**EMP_DEPTNO_30**として作成します。監査ポリシーの作成にはDBMS_FGA.ADD_POLICYを使用します。**audit_condition**として**DEPTNO = 30**を指定することにより、監査証跡を取得する行を限定します。さらに**audit_column**として**SAL,COMM**を指定することにより、監査証跡を列**SAL、COMM**へのアクセスに限定します。**statement_types**に**SELECT,UPDATE**を指定することにより、操作の対象をSELECTとUPDATEに限定しています。**enable**を**TRUE**としているため、監査ポリシーは作成と同時に有効になります。(ポリシーの有効化はDBMS_FGA.ENABLE_POLICYで行います。)

```
begin
    dbms_fga.add_policy(
        object_schema => 'HR'
      , object_name => 'EMP'
      , policy_name => 'EMP_DEPTNO_30'
      , audit_condition => 'DEPTNO = 30'
      , audit_column => 'SAL,COMM'
      , handler_schema => NULL
      , handler_module => NULL
      , enable => TRUE
      , statement_types => 'SELECT,UPDATE'
      , audit_column_opts => DBMS_FGA.ANY_COLUMNS
    );
end;
/
```

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

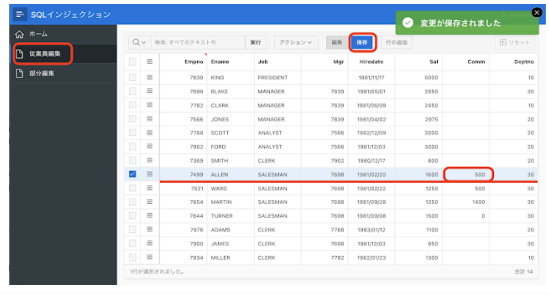
作成したポリシーはビューALL_AUDIT_POLICIESより確認できます。

```
select * from all_audit_policies where policy_name = 'EMP_DEPTNO_30';
```

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

テスト用のアプリケーションから表HR.EMPにアクセスし、ファイングレイン監査による監査証跡を確認します。

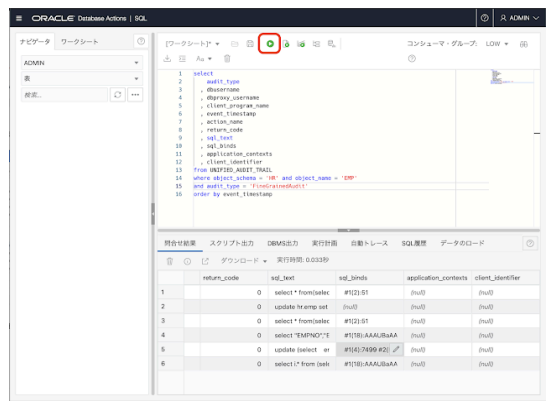
従業員編集のページを開き、**DEPTNO**が**30**である従業員**ALLEN**の列**COMM**を変更します。



監査証跡をビューUNIFIED_AUDIT_TRAILより確認します。**audit_type**に**FineGrainedAudit**を指定します。

```
select
    audit_type
  , dbusername
  , dbproxy_username
  , client_program_name
  , event_timestamp
  , action_name
  , return_code
  , sql_text
  , sql_binds
  , application_contexts
  , client_identifier
from UNIFIED_AUDIT_TRAIL
where object_schema = 'HR' and object_name = 'EMP'
and audit_type = 'FineGrainedAudit'
order by event_timestamp
```

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



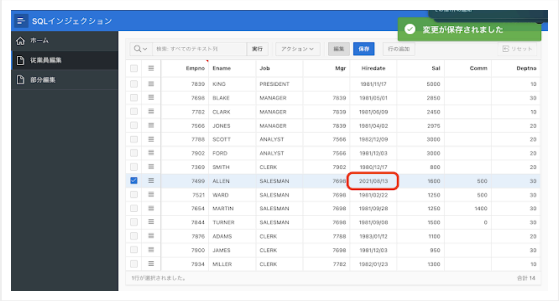
監査証跡が取得されていることが確認できます。直近で実行されたUPDATE文を確認します。記録されているsql_textは以下です。

変更した列COMM以外にも、対話グリッドのソースとして記載したSELECT文に含まれる列すべてについて、値が設定されています。

sql_bindsとして記録されているバインド変数の値を確認しても、主キーを条件句として、すべての列の値が設定されています。

Oracle APEXにてデータ操作に使用されるのは、主に対話グリッドとフォームです。これはソース定義に含まれる列は、値の変更がなくても以前の値で更新します。今回の例では仮に列SAL、COMMに変更がなくても、例えばHiredateが変更されても、列SAL、COMMともに（以前と同じ値にて）更新されるため、その操作は監査証跡に残ります。

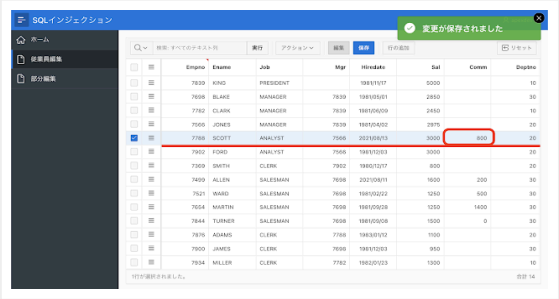
従業員**ALLEN**の**Hiredate**を**2021/08/13**に変更してみます。



ビューUNIFIED_AUDIT_TRAILを確認すると、監査証跡がとられていることが確認できます。

またaudit_conditionとしてDEPTNO = 30が設定されていますが、対話グリッドからのアップデートの場合、DEPTNOが30でなくても監査証跡が取得されます。

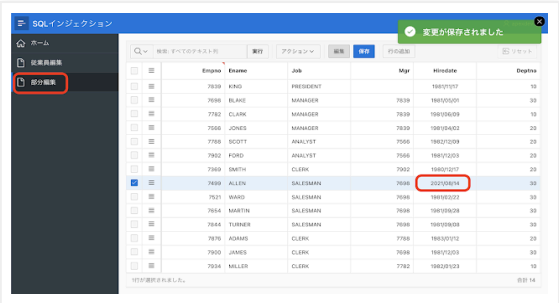
DEPTNOが20の従業員SCOTTのCOMMを800に変更してみます。



このアップデート操作の監査証跡が取得されています。

列DEPTNOが20であっても、DEPTNOは更新の対象なので監査証跡が取得されます。

部分更新の対話グリッドのソースには列SALとCOMMが含まれていないため、監査証跡は取得されません。



Oracle APEXのアプリケーションを対象として、ファイングレイン監査によって監査証跡を取得する際には、考えている以上に監査証跡が取得されるケースが多いです。これは気に留めておく必要があります。

ファイングレイン監査ポリシーを無効にするにはプロシージャDBMS_FGA.DISABLE_POLICYを使用します。ファイングレイン監査ポリシーの削除にはプロシージャDBMS_FGA.DROP_POLICYを使用します。今回は後続の作業にて監査証跡を参照するため、以下のコマンドはすべての作業を終えた時に実行します。

```
begin
    dbms_fga.disable_policy(
        object_schema => 'HR'
      , object_name => 'EMP'
      , policy_name => 'EMP_DEPTNO_30'
    );
    dbms_fga.drop_policy(
        object_schema => 'HR'
      , object_name => 'EMP'
      , policy_name => 'EMP_DEPTNO_30'
    );
```

```
end;
/
```

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

続く

Yuji N. 時刻: 17:49

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