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(4) - 統合監査

どのようなアクセスがあったのか記録していなければ、不正を見つけることもできません。統合監査ポリシーを設定することにより、表HR.EMPに対するすべての操作を監査証跡を取得してみます。

統合監査ポリシーの作成にはCREATE AUDIT POLICY文を使用します。作成した統合監査ポリシーを有効にするにはAUDIT文を使用します。

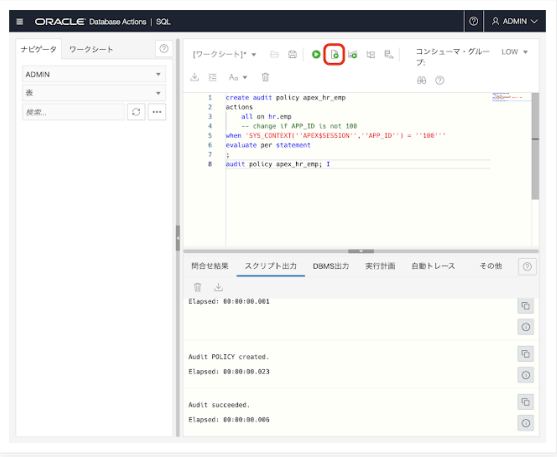
SYS_CONTEXT('APEX$SESSION','APP_ID')の結果が**100**、つまりアプリケーションIDが100番のAPEXアプリケーションから実行された表HR.EMPへのアクセスのみ監査証跡の取得対象にしています。

```
create audit policy apex_hr_emp
actions
    all on hr.emp
    -- change if APP_ID is not 100
when 'SYS_CONTEXT(''APEX$SESSION'',''APP_ID'') = ''100'''
evaluate per statement
;
audit policy apex_hr_emp;
```

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

データベース・アクションにユーザー**ADMIN**で接続し、統合監査ポリシー**APEX_HR_EMP**を作成します。作成後にポリシーを有効にします。

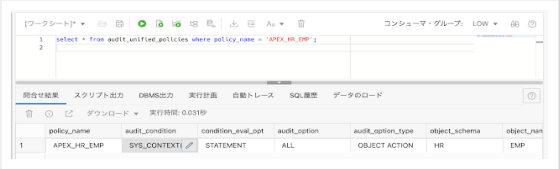
開発の**SQL**より実行します。



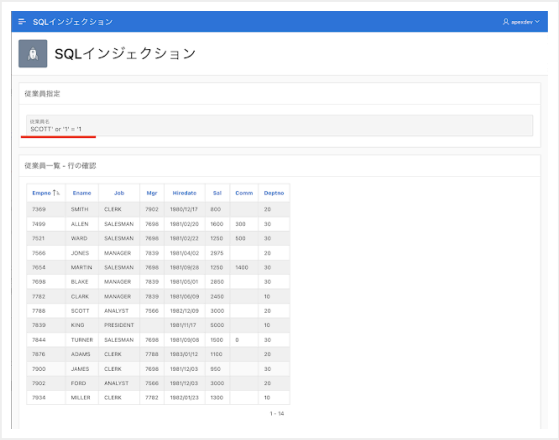
作成した統合監査ポリシーは、ビューAUDIT_UNIFIED_POLICIESより確認できます。

```
select * from audit_unified_policies where policy_name = 'APEX_HR_EMP';
```

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



テスト用アプリケーションを実行し、SQLインジェクションの確認作業を再度行います。表HR.EMPにAPEXアプリケーションからアクセスが発生します。アプリケーションIDは100番であることを想定していますが、そうでない場合は作成するポリシーを変更しておきます。

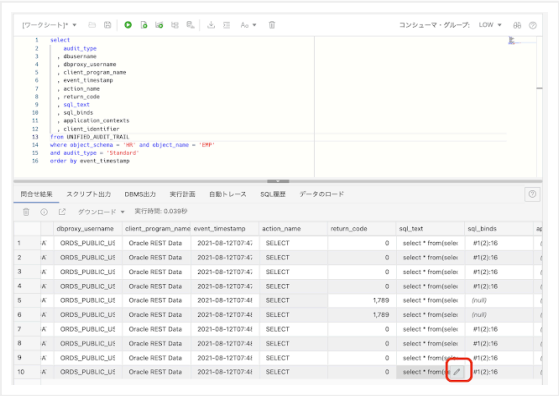


監査証跡を確認します。データベース・アクションにユーザーADMINで接続し、ビューUNIFIED_AUDIT_TRAILを検索します。

```
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 = 'Standard'
order by event_timestamp
```

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

検索結果より実行されたSQL文等、どのようなアクセスが行われていたのか確認できます。



実行されたSQL文や与えられたバインド変数なども確認できます。

リレーショナル・データベースでのデータ操作は必ずSQLによって行われるため、監査証跡としての網羅性は非常に高いといえます。また、監査証跡はデータベース側で取得すればよいので、APEXアプリケーションに実装する必要がありません。市民開発者によるアプリケーション開発など、いわゆるプロではない人にとってアプリケーション開発の負担が減るため、特に効果があるでしょう。

統合監査ポリシーを無効にするにはNOAUDIT文を使用します。統合監査ポリシーの削除にはDROP AUDIT POLICY文を使用します。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。

```
noaudit policy apex_hr_emp;
drop audit policy apex_hr_emp;
```

seminar210825-drop_audit_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