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。

2023年8月9日水曜日

直リンクでフォームを開く際にユーザー・レベルのチェックサムを使ってページを保護する

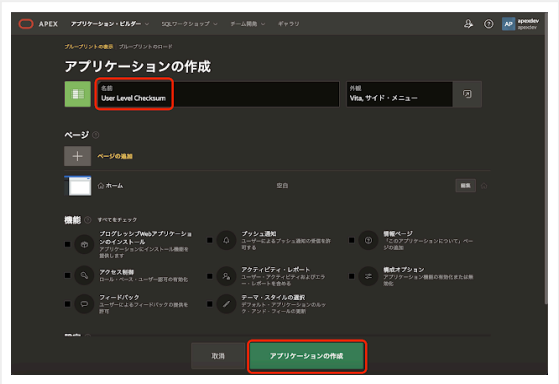
特定のユーザーに電子メールなどの手段を使って編集フォームの直リンクを送付する際に、指定したユーザー以外のアクセスおよび、指定したユーザーでもURLで指定したデータのみ編集できるように限定します。直リンクのURLへのこのような保護を、ユーザー・レベルのチェックサムを付加することにより実現してみます。

以下より実装方法について紹介します。

アプリケーション作成ウィザードを起動します。アプリケーションの**名前**は**User Level Checksum**とします。

今回のサンプルで使用する対話モード・レポートと**ページ・モードが標準のフォーム**は**ページ作成ウィザード**でないと作成できないため、このまま空のアプリケーションを作成します。

アプリケーションの作成をクリックします。



アプリケーションが作成されたら、**ページ作成ウィザード**を起動します。

ページの作成をクリックします。

対話モード・レポートを選択します。

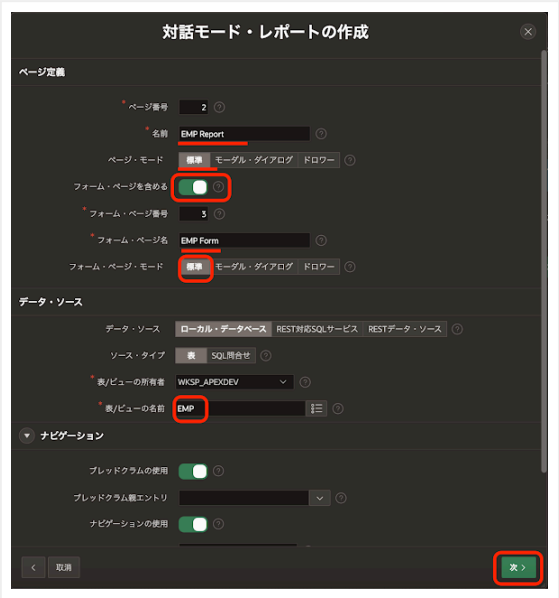
対話モード・レポートの**名前**は**EMP Report**、**ページ・モード**は**標準**です。**フォーム・ページを含める**に**チェック**を入れます。

フォーム・ページ名を**EMP Form**とし、**フォーム・ページ・モード**に**標準**を選択します。モーダル・ダイアログとドロワーの場合、ページを直接URLを指定して開くことはできません。モーダル・ダイアログとドロワーは必ず対話モード・レポートに重なる形で表示されるため、対話モード・レポートから開く必要があります。

データ・ソースの**表/ビューの名前**に**EMP**を指定します。

ナビゲーションはデフォルトから変更しません。

次へ進みます。



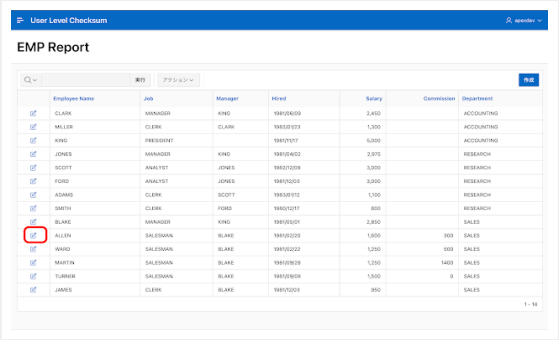
主キー列 1 として**EMPNO (Number)**を選択します。

ページの作成をクリックします。

以上で今回のサンプルを実装する準備ができました。

最初にフォームを開く際のURLを確認します。

対話モード・レポートを開き、任意の従業員を編集フォームで開きます。



フォームが開くので、URLを確認します。

URLのアプリケーションの別名以降は、次のようになっています。

/user-level-checksum/emp-form?p3_empno=7499&session=115160286541908&cs=3SMx19onQOI7QzYFv9fydpYl2NslAjSk_s70DVyc7JOBflP00q3GB7UV7HLHdM6vjBu_jPQvI-J1COuhPFYZNWA

/アプリケーション別名/ページ名?p3_empno=編集対象の従業員番号&session=セッションID&cs=チェックサム

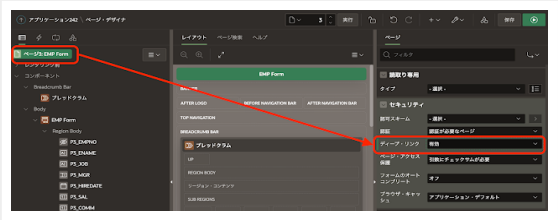
例えばこのURLを電子メールに含めて送信しても、電子メールでURLを受け取った人は編集フォームを開くことができません。ページ**emp-form**をAPEXセッション外から開けないように保護されている（**ディープ・リンク**が**無効**になっている）ことと、ページ・アイテムP3_EMPNOを保護するた

めに生成されているチェックサムが、同じAPEXセッション内にあるときに限り有効（**セッション・ステート保護**が**チェックサムが必要 - セッション・レベル**）であるためです。

これから、電子メールでURLを受け取ったユーザーが編集フォームを開けるようにする設定を行います。

ページ・デザイナにてフォームのページ**EMP Form**を開きます。

セキュリティの**ディープ・リンク**を**有効**にします。直接フォームのページを開くことを許可します。

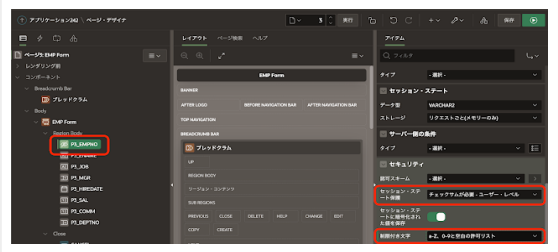


ページ・アイテム**P3_EMPNO**を選択します。

セキュリティの**セッション・ステート保護**を**チェックサムが必要 - セッション・レベル**から**チェックサムが必要 - ユーザー・レベル**に変更します。

これで、このフォームにアクセスするための**URLを生成したユーザーであれば**、そのURLを使って（APEXセッションの有無に関わらず）フォームを開くことができるようになります。

URLの引数としてページ・アイテム**P3_EMPNO**に値が設定されるため、**制限付き文字**に**a-Z、0-9と空白の許可リスト**を選択し、**制限なし**よりは安全に配慮します。



以上で、従業員を指定してフォームを直接開くことができるようになりました。

対話モード・レポートを開き、任意の従業員の編集フォームを開きます。

ユーザー・レベルのチェックサムが生成されているため、このURLをコピーし別のブラウザで開くことができます。ユーザー認証を要求されるため、対話モード・レポートを開いたユーザーと同じユーザーでサインインする必要があります。

バッチでURLを生成する場合は、APEX_SESSION.CREATE_SESSIONを呼び出して、URLを開くユーザーでAPEXセッションを開始した上でURLを生成します。

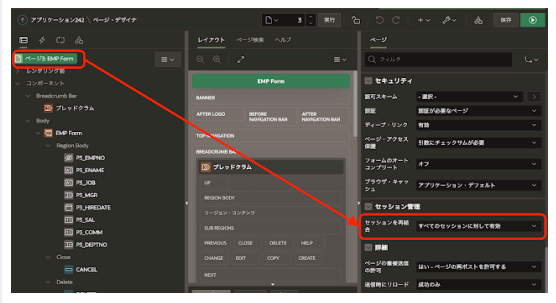
直リンクのURLを生成するサンプルです。

```
set serveroutput on
set define off
declare
    l_url varchar2(400);
    ----
    l_app_id    number := 242;
    l_page_id   number := 3;
    l_username  varchar2(80) := 'APEXDEV';
    l_empno     number := 7839;
begin
    apex_session.create_session(
        p_app_id    => l_app_id
        ,p_page_id  => 1 -- ホーム・ページを指す
        ,p_username => l_username
        ,p_call_post_authentication => false
    );
    l_url := apex_page.get_url(
        p_application => l_app_id
        ,p_page       => l_page_id
        ,p_session    => 0
        ,p_items      => 'P3_EMPNO'
        ,p_values     => l_empno
    );
    apex_session.delete_session(
        p_session_id => v('APP_SESSION')
    );
    --  必ずしも必要ないがURLを短くするため引数sessionを削除している。
    l_url := regexp_replace(l_url, '&session=[0-9]+','');
    dbms_output.put_line(l_url);
end;
/
```

generate_direct_link.sql hosted with ❤️ by GitHub view raw

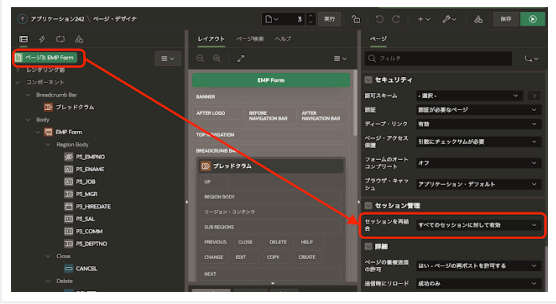
ユーザーが電子メールに添付されたURLをクリックした場合、今までの設定では必ずユーザー認証が行われ、新規にセッションが開始します。ユーザーがすでにAPEXアプリケーションにサインイン済みで作業をしていると、そのセッションが無効になります。

ページ・プロパティの**セッション管理**の**セッションを再結合**を**すべてのセッションに対して有効**にすると、既存のAPEXセッションがあれば、そのセッションを利用します。そのため、再度ユーザー認証を要求されることが無くなります。

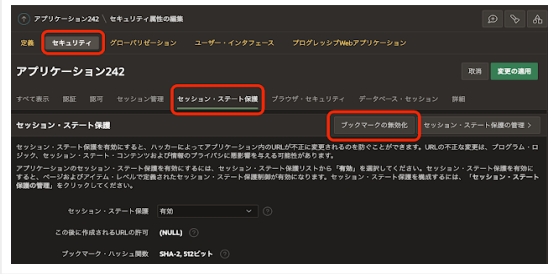


一般にセッションの再結合は、セキュリティ上問題が発生しないパブリック・ページに対してのみ設定します。セッションの再結合が有効になっているページは、ユーザー認証をせずにアクセスできるようになるためです。

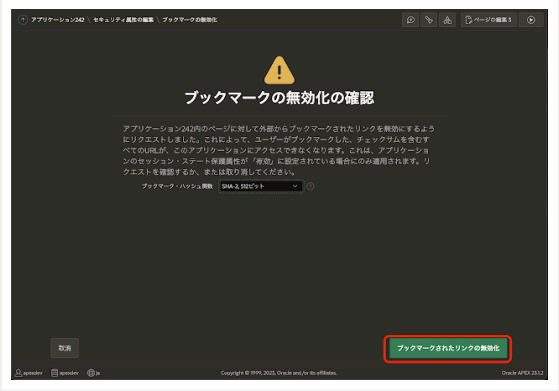
今回の例では、ユーザー・レベルのチェックサムがURLに含まれています。別のユーザーで認証されたAPEXセッションに再結合したときは、URLにアクセスしてもチェックサムのエラーが発生しアクセスが禁止されます。そのため、セッションの再結合を有効にしてアプリケーションの利便性を上げるという選択肢を採用することができます。



ユーザー・レベルのチェックサムはセッション・レベルと異なり、有効期限がありません。今までに生成されたユーザー・レベルのチェックサム（を含むURL）を無効にするには、**アプリケーション定義**の**セキュリティ**の**セッション・ステート保護**の**ブックマークの無効化**を実行します。



ブックマークされたリンクの無効化をクリックして、今までに生成されたURLを無効にします。

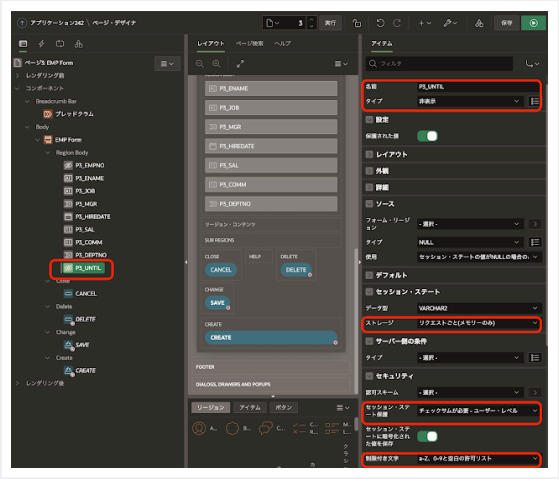


ただし、この無効化はセッション・レベル、ユーザー・レベル、アプリケーション・レベルのすべてのチェックサムを無効にします。Oracle APEXは、個別のURLに含まれるチェックサムに限定して無効化する手段を提供していません。

この制限に対応するため、直リンクに有効期限を含めてみます。

直リンクの宛先となるページにページ・アイテム**P3_UNTIL**を作成します。

タイプは**非表示**、**セッション・ステート**の**ストレージ**は**リクエストごと(メモリーのみ)**とします。**セキュリティ**の**セッション・ステート保護**に**チェックサムが必要 - ユーザー・レベル**を選択し、チェックサムの計算に含めるようにします。これでURLに現れる有効期限を直接編集するとチェックサムの不一致のエラーが発生するようになるため、勝手に有効期限を変えることができなくなります。念のため**制限付き文字**として**a-z、0-9と空白の許可リスト**を選択します。



有効期限を確認するプロセスを作成します。**レンダリング前**に実行します。

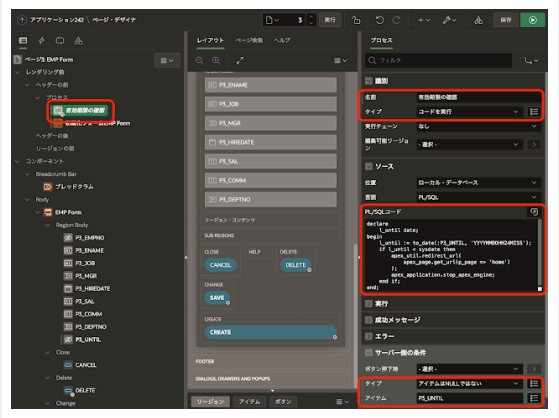
識別の**名前**を**有効期限の確認**とします。**タイプ**として**コードの実行**を選択し、**ソース**の**PL/SQLコード**として以下を記述します。

```
declare
    l_until date;
begin
    l_until := to_date(:P3_UNTIL, 'YYYYMMDDHH24MISS');
    if l_until < sysdate then
        apex_util.redirect_url(
```

```
            apex_page.get_url(p_page => 'home')
        );
        apex_application.stop_apex_engine;
    end if;
end;
```

check-expiration-date.sql hosted with ❤️ by GitHub view raw

サーバー側の条件の**タイプ**に**アイテムはNULLではない**を選択し、**アイテム**として**P3_UNTIL**を指定します。



直リンクの生成を行うコードは、以下のように変更します。有効期限を 1 分に設定しています。この他にも操作を一回だけ有効にするといった実装も、少々コードを変えることで実現できるでしょう。

```
set serveroutput on
set define off
declare
    l_url varchar2(400);
    ----
    l_app_id    number := 424;
    l_page_id   number := 3;
    l_username  varchar2(80) := 'APEXDEV';
    l_empno     number := 7499;
    l_valid_min number := 1;
begin
    apex_session.create_session(
        p_app_id    => l_app_id
        ,p_page_id  => 1
        ,p_username => l_username
        ,p_call_post_authentication => false
    );
    l_url := apex_page.get_url(
        p_application => l_app_id
        ,p_page       => l_page_id
        ,p_session    => 0
        ,p_items      => 'P3_EMPNO,P3_UNTIL'
        ,p_values     => apex_string.join(
```

```
            apex_t_varchar2(l_empno, to_char(sysdate+l_valid_min/1440,'YYYYMMDDHH24MISS')), ','
        )
    );
    apex_session.delete_session(
        p_session_id => v('APP_SESSION')
    );
    l_url := regexp_replace(l_url, '&session=[0-9]+','');
    dbms_output.put_line(l_url);
end;
/
```

generate_direct_link_scope.sql hosted with ❤️ by GitHub view raw

リンクの有効期限が過ぎている場合は、ホーム・ページを開くようにしています。

今回の記事は以上になります。

今回作成したAPEXアプリケーションのエクスポートを以下に置きました。
https://github.com/ujnak/apexapps/blob/master/exports/user-level-checksum.zip

Oracle APEXのアプリケーション作成の参考になれば幸いです。

完

Yuji N. 時刻: 13:39

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