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5月20日木曜日

Oracle APEX 21.1で追加されたReferrer Policy属性について

Oracle APEX 21.1での新機能のセキュリティの向上として、以下の記載があります。

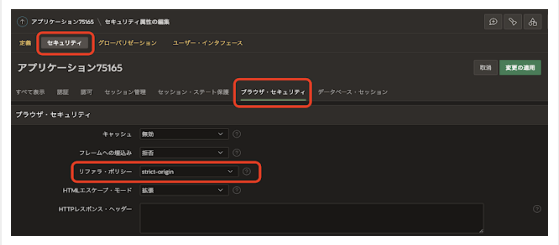
> **Referrer-Policy HTTPヘッダー**
> APEXは、デフォルトのReferrer-Policy HTTPヘッダーを送信するようになったため、セッションIDは外部リンクのReferrerヘッダーで送信されなくなりました。

ちょっと意味が掴めなかった(英語でも記載内容は同じ)ので、実際にどうなっているのか確認しました。

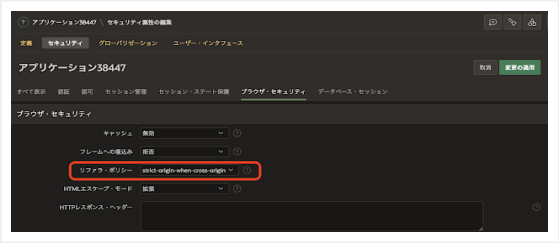
ここで説明されているOracle APEX 21.1で追加された機能とは、HTTPレスポンス・ヘッダーとしてReferrer-Policyを含めるようにし、そのデフォルトをstrict-originとする、というものでした。

Oracle APEX 21.1で新規に作成したアプリケーションが対象で、それ以前に作成されたアプリケーションについてはstrict-origin-when-cross-originを維持します。

アプリケーション定義の**セキュリティ**に含まれる**ブラウザ・セキュリティ**に**リファラ・ポリシー**の属性が追加されています。



21.1以前に作成したアプリケーションの場合、リファラ・ポリシーはstrict-origin-when-cross-originになっていることが確認できます。



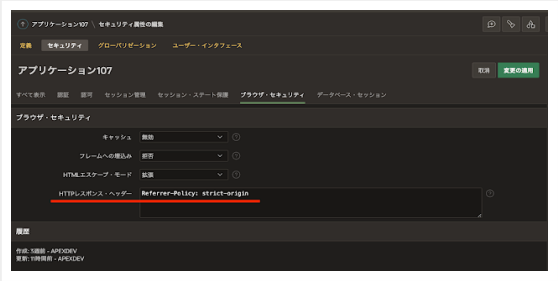
レスポンス・ヘッダーにReferrer-Policyが含まれていない場合、ブラウザがどのようにRefererヘッダーを送信するか判断しますが、一般的にはstrict-origin-when-cross-originの動作を選択するようです。そのため、以前からあるアプリケーションについては、Referrer-Policyをstrict-origin-when-cross-originにすることで、挙動を変えないようにしています。

ビューAPEX_APPLICATIONSに列REFERRER_POLICYが追加されていて、ビューからも設定値を参照することができます。

あまり知られていないと思いますが、Oracle APEXでは、送信するHTTPレスポンス・ヘッダーを設定することができます。

アプリケーションごとの設定では、**アプリケーション定義**の**セキュリティ**の**ブラウザ・セキュリティ**にある**HTTPレスポンス・ヘッダー**に、送信したいヘッダーを定義します。今回のケースでは、以下のように**Referrer-Policy**ヘッダーを記述します。

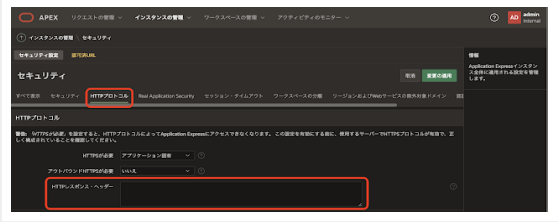
以下はOracle APEX 21.1以前のバージョンで、Referrer-Policyを制御する方法です。



Oracle APEX 21.1から追加されたリファラ・ポリシーは、HTTPレスポンス・ヘッダーでの設定で上書きされるので、21.1以前に設定したReferrer-Policyはバージョン・アップ後も維持されます。

とはいえ、もし、このような設定をしていた場合はHTTPレスポンス・ヘッダーからReferrer-Policyを削除し、新しく追加されたリファラ・ポリシーをstrict-originに設定するべきでしょう。

HTTPレスポンス・ヘッダーはインスタンス・レベルでも設定できます。**インスタンスの管理**の**セキュリティ**に含まれる**HTTPプロトコル**のセクションの**HTTPレスポンス・ヘッダー**です。



Autonomous Databaseではインスタンスの管理からセキュリティの設定は取り除かれています。そのため画面からの設定の代わりにAPEX_INSTANCE_ADMINパッケージのプロシージャSET_PARAMETERを使います。

```
begin
    apex_instance_admin.set_parameter('HTTP_RESPONSE_HEADERS','Referrer-Policy: strict-origin');
end;
/
```

しかしAutonomous DatabaseでパラメータHTTP_RESPONSE_HEADERSを操作すると、ORA-20987が発生します。

ORA-20987: APEX - Instance parameter not found

現時点ではパラメータHTTP_RESPONSE_HEADERSは、Autonomous Databaseでは設定不可のようです。アプリケーションごとに設定を行うことで、こちらの不備については対応が可能です。

Referrer-Policyについての説明は以上になります。

完

Yuji N. 時刻: 23:24

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