

Webアプリケーションのシボレス化実習

1. はじめに

本メニューでは、Shibboleth化を行うWebアプリケーションとしてログイン機能を持つ簡易的なテストページ（テストWebアプリ）を使用します。このテストWebアプリのID/パスワードのログイン機能部分をShibbolethを使ったログイン処理に変更します。

2. 実習セミナーでは

プラグインの手順書もありますが、以下の手順で作業を進めてください。

・テストWebアプリケーションについて

SPサーバのトップページにテストWebアプリのリンクがあります。

予めShibbolethを使った認証でない状態を確認してください。

URL : <https://ex-sp-test01.gakunin.nii.ac.jp/> ※1番を割り振られた場合
アカウント : 簡易的なもので ID : test001 、パスワード : test001 のみログインできます。
ソース : /var/www/html/testapp 配下

※端末のサイズによっては表記がずれる可能性があります。画面を広くしてご覧ください。

・認証をShibbolethを利用するように変更

/etc/httpd/conf.d/shib.confの末尾に以下の設定を追記します。

```
<Location /testapp/login.php>
AuthType shibboleth
ShibRequestSetting requireSession 1
require shib-session
</Location>
```

設定ファイルの変更後、Apacheの再起動します。
systemctl restart httpd

・ログイン処理を受信した属性値を使うように変更

ここでは、ePPN(eduPersonPrincipalName)をIDとして取得し、セッションに設定します。

/var/www/html/testapp/login.phpを以下のように変更します。

```
if (isset($_SESSION['USER'])) {  
    header('Location: testapp.php');  
    exit;  
}  
  
//ログイン  
if (isset($_SERVER["Shib-Identity-Provider"]) and isset($_SERVER["eppn"])) { //正しく属性値を受信しているか確認  
    $user = explode( '@', $_SERVER["eppn"] );  
    $_SESSION["USER"] = $user[0]; //ローカルパート部分を取得してセッションにセット  
    header("Location: testapp.php"); //認証できているのでテストWebアプリに遷移  
    exit;  
}  
  
# $message = '';  
# if(isset($_POST['login'])){  
# if ($_POST['uid'] == 'test001' && $_POST['password'] == 'test001'){  
# $_SESSION["USER"] = 'test001';  
# header("Location: testapp.php");  
# exit;  
# }  
# else{  
# $message = 'ユーザーIDかパスワードが間違っています。';  
# }  
# }
```

・ログアウト処理も変更

ここでは、ローカルログアウト機能を使用しています。

/var/www/html/testapp/testapp.phpを以下のように変更します。

```
# header('Location: login.php');  
//ログアウト後、「テストWebアプリ」のリンクがあるトップページが表示されます。  
header('Location: https://ex-sp-test*.gakunin.nii.ac.jp/Shibboleth.sso/Logout?return=https://ex-sp-test*.gakunin.nii.ac.jp/');
```

※端末のサイズによっては表記がずれる可能性があります。画面を広くしてご覧ください。

3. 手順書

本メニューでは、ありません。

「2. 実習セミナーでは」を順に設定してください。

4. 動作確認

① 各自が使用するSPの接続確認用ページにアクセスします。

例) 1番を割り振られた場合
<https://ex-sp-test01.gakunin.nii.ac.jp/>

② テストWebアプリのリンクをクリックします。

③ DSの設定を行っている場合、所属機関の選択画面が表示されるので、各自が使用するIdPを選択します。

④ IdPのログイン画面が表示されるので、Username/Passwordを入力して認証を行います。

⑤ Shibboleth認証時ユーザのeppnのローカルパートがユーザIDとなり、正しくログイン出来る事を確認します。

⑥ ログアウト後、SPサーバのトップページが表示されることを確認します。

⑦再度「②」から行くと認証要求がある（再度ログインから行う必要がある）事を確認します。

