2024年11月8日

Webアプリケーションのシボレス化実習

国立情報学研究所

教育研修事業

**目次**

[**1. はじめに 2**](#_heading=h.1fob9te)

[**2. 実習セミナーでは 2**](#_heading=h.3znysh7)

[**3. 設定手順 2**](#_heading=)

[3.1 テストWebアプリケーションについて 2](#_heading=h.uux433if77ed)

[3.2 認証をShibbolethを利用するように変更 3](#_heading=h.2xg733vcnkq)

[3.3 ログイン処理を受信した属性値を使うように変更 3](#_heading=h.pjiihpe6fevx)

[3.4 ログアウト処理も変更 4](#_heading=h.hp940oc10lw1)

[**4. 動作確認 5**](#_heading=h.tyjcwt)

# **1. はじめに**

本メニューでは、SPをカスタマイズします。

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。

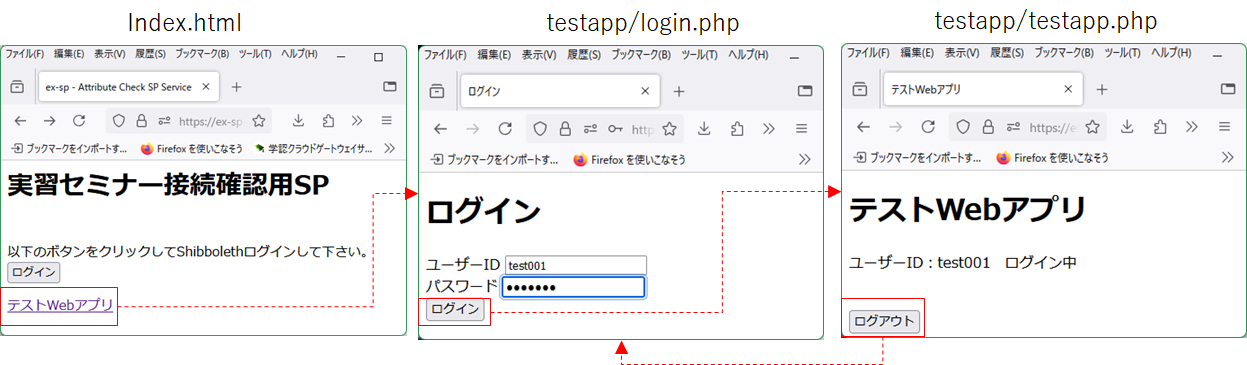
# **2. 実習セミナーでは**

実習セミナーとして、すでに用意されている内容を設定して動作を確認します。

# **3. 設定手順**

## 3.1 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-testXX.gakunin.nii.ac.jp/　※XX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（testapp.php, login.php） |



#### **図 テストWebアプリのリンクからの遷移**

## 3.2 認証をShibbolethを利用するように変更

以下のように /etc/httpd/conf.d/shib.conf の最終行に設定を追加します。

|  |
| --- |
| /etc/httpd/conf.d/shib.confの末尾に以下の設定を追記します。  #  # Configure the module for content.  #  # You MUST enable AuthType shibboleth for the module to process  # any requests, and there MUST be a require command as well. To  # enable Shibboleth but not specify any session/access requirements  # use "require shibboleth".  #  <Location /secure>  AuthType shibboleth  ShibRequestSetting requireSession 1  require shib-session  </Location>  <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 |

## 3.3 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。';  # }  # } |

## 3.4 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。

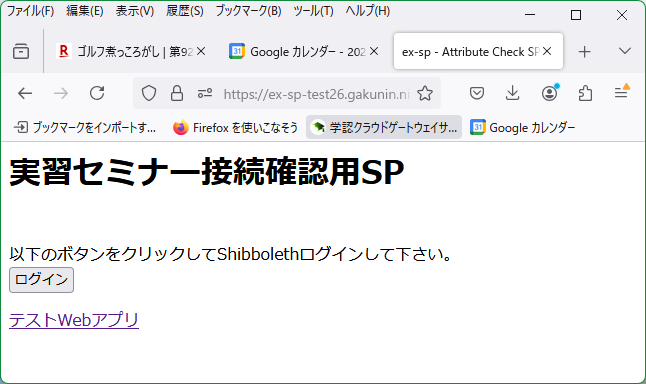
/var/www/html/testapp/testapp.phpを以下のように変更します。

|  |
| --- |
| # 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。  //「XX」の部分は、割り振られた番号に置き換えてください。  header('Location: https://ex-sp-testXX.gakunin.nii.ac.jp/Shibboleth.sso/Logout?return=https%3A%2F%2Fex-sp-testXX.gakunin.nii.ac.jp%2F'); |

# **4. 動作確認**

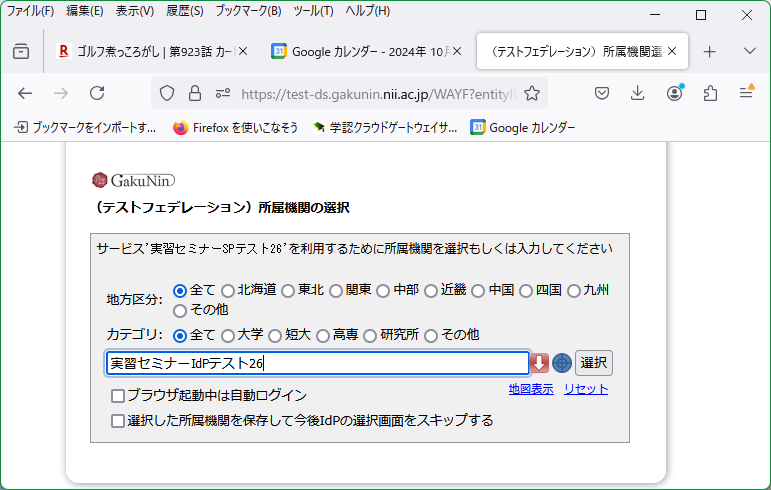
1. 各自が使用するSPの接続確認用ページにアクセスします。

|  |
| --- |
| 例）XX番を割り振られた場合  https://ex-sp-testXX.gakunin.nii.ac.jp/ |



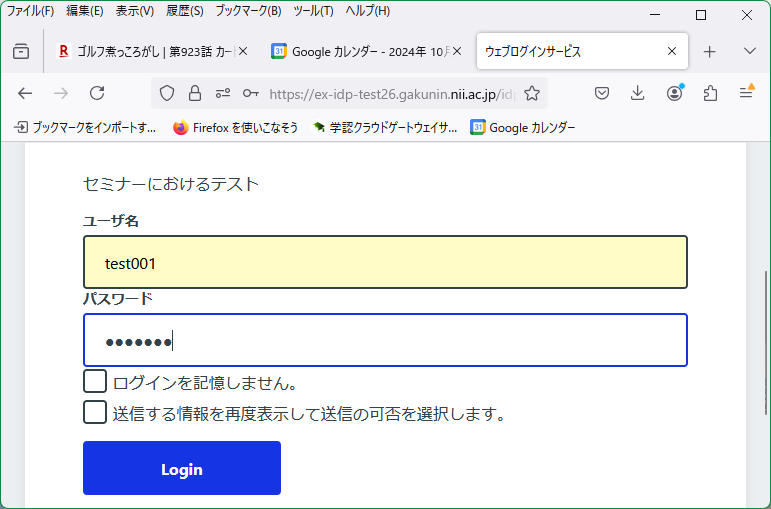
#### 図　https://ex-sp-testXX.gakunin.nii.ac.jp/へ接続画面

1. テストWebアプリのリンクをクリックします。
2. 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。



#### 図　各自のIdPを選択

1. 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。



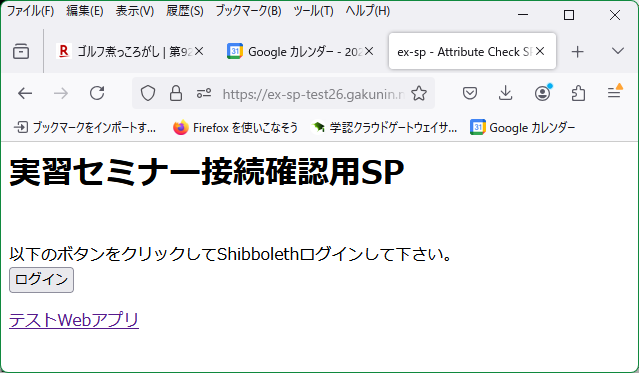
#### 図　UserName/Passwordでログイン

1. 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。



#### 図　正しくログインできた画面

1. 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。



#### 図　ログアウト後のSPサーバのトップページ

1. 再度「2」から行うと認証要求がある事を確認します。

　　※ログアウトは、ローカルログアウトのURLとなっている為、SPサーバ側のテストWebアプリからログアウトはされますが、IdP側で認証済みの状態となっています。  
この場合、ログイン画面が表示されずにテストWebアプリにアクセスできます。  
一瞬ですが、アクセス時にURLを見て頂くと、IdP側にアクセスしていることが分かります。