旧: FPSPの導入

本メニューはShibboleth IdPバージョン2向けです。

1. はじめに

本メニューでは、IdPをカスタマイズします。
FPSPを導入し、IdP側でアクセス制御を可能とします。
例えば、あるSPにはeduPersonAffiliationが「student」のみアクセスを許可し、
「student」以外のユーザはSPへアクセスできないといった事が可能となります。

---

2. 実習セミナーでは

以下のような設定で行います。
手順書と照らし合わせながら、作業を進めてください。

・commons-configuration-1.3入手について

```
予めサーバ内の/root/PKG配下にあるので、こちらを使用してください。
 (commons-configuration-1.3.zip)

# cd /root/PKG
# unzip commons-configuration-1.3.zip
```

・SampleFilterPerSP.javaについて

```
予めサーバ内の/root/PKG配下にあるので、こちらを使用してください。
 (SampleFilterPerSP.tgz)

# cd /root/PKG
# tar zxvf SampleFilterPerSP.tgz

また、アサーション送信拒否時に画面に日本語メッセージを表示させると文字化けが
発生してしまうので、以下のように一行追加します。
SampleFilterPerSP.javaを編集してください。

private void doError(ServletResponse servletResponse, String spEntityId, String userName) throws IOException {
    // エラーメッセージの表示など
    servletResponse.setContentType("text/html");
    servletResponse.setCharacterEncoding("utf-8");  //←追加
```

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

・SampleFilterPerSP.javaのコンパイル

```
予め準備しているファイルの文字コードはutf-8となっていますので、コンパイル時のオプション
「-encoding shift_jis」は、必要ありません。
# javac -Xlint:unchecked  SampleFilterPerSP.java
```

・SampleFilterPerSP_allow.xmlについて

```
/root/PKG配下にあるSampleFilterPerSP.tgzに同封されているので、
展開先ディレクトリ内のSampleFilterPerSP_allow.xmlを使用してください。
```

・制御する設定をアドバンスド実習用に修正

```
制御対象のSPを設定します。
entityIDが「https://shiken-sp00.nii.ac.jp/shibboleth-sp」と設定されている箇所を各自の
SPのentityIDに修正します。SampleFilterPerSP_allow.xmlを編集してください。

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

---

3. 手順書

下記の導入手順書を参照し、作業を行います。
※実習時の設定値に置き換える事を忘れないようにしてください。

- 導入手順書

---

4. 動作確認

① 設定後、Tomcatの再起動を行ってない場合は行なってください。

```
service tomcat6 restart
※起動後は、正常にidp.warが展開されたか/usr/java/tomcat/logs/catalina.outを確認します。
```

② 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/
```

③ ログインボタンをクリックします。

④ DSの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。

⑤ 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。

フィルタ条件は、eduPersonAffiliationが「student」か「member」の場合にアクセスを許可する設定に
なっているので、それ以外の値を持ったユーザでログインします。
※LDAPを変更してなければ、test002ユーザが「faculty」です。test002でログインしてください。
※uApproveが稼働している場合、eduPersonAffiliation属性を送信してください。

```
Username：test002、Password：test002
```

⑥ アサーション送信拒否時の画面が表示される事を確認してください。

⑦ アクセス出来ない事が確認できたら、一旦ブラウザを閉じ、test001やtest003ユーザでも同様にログインしてみてください。

test001は「member」で、test003は「student」なので、共にアクセス許可され属性受信の確認ページが表示されます。