旧: uApprove.jp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。
uApprove.jpを導入し、属性値を送信する前にユーザの承認を得る事ができます。

---

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。

・Identity ProviderのDNS名

```
例）1番を割り振られた場合
  ex-idp-test01.gakunin.nii.ac.jp
```

・前提条件

```
実習セミナーでは、ストレージの種類をSQLデータベース（MySQL）とします。
事前準備として、以下のようにMySQLをインストールし、起動させておいてください。
※手順書内にあるファイルベースの説明は、読み飛ばしてください。

# yum install mysql-server
# service mysqld start

なお、実習では不要ですが実運用の場合は以下を実行してください。（OS起動時の自動起動および、rootアカウントにパスワードを設定します）

# chkconfig mysqld on
# mysql_secure_installation
```

・インストール

```
uApprove.jpのパッケージは、「３．手順書」に記載しています「uApprove.jpについて」
URLwget


2.2.1b
 # wget https://meatwiki.nii.ac.jp/confluence/download/attachments/13501031/uApprove.jp-2.2.1b-bin.zip
```

・Viewer

```
Viewer設定ファイルをコピーするとIdP-Plugin設定ファイルとファイル名が重複し、
上書き確認が表示されますが、同様な設定ファイルなので構わず上書きしてください。
```

・Shibboleth IdP を再デプロイ

```
shibboleth-identityproviderのinstall.shを実行します。
# cd /opt/shibboleth-identityprovider-2.x/
# ./install.sh
```

・SP ブラックリスト

実習セミナーでの導入手順としては、読み飛ばしてください。

・Tomcat のフロントエンドとしての Apache

```
# vi /etc/httpd/conf.d/ssl.conf

<VirtualHost _default_:443>
   （省略）
ProxyPass /idp/ ajp://localhost:8009/idp/
ProxyPass /uApprove ajp://localhost:8009/uApprove  ←追加
   （省略）
```

設定後、Apacheを再起動します。

```
service httpd restart
```

・ルールの定義

```
実習セミナーでは、「surname、givenName、mail、eduPersonAffiliation」をオプショナル属性
とします。以下のように4つの属性を全て変更してください。
例）surname属性の設定
<afp:AttributeRule attributeID="surname">
    <afp:PermitValueRule xsi:type="uajpmf:AttributeUapprove" />
</afp:AttributeRule>
```

・Reset-approvals 設定

```
In-flowモードで操作します。$CATALINA_HOME/webapps/idp/login.jspを編集してください。
変更後は、Tomcatを再起動します。
# service tomcat6 restart
```

手順書の「1.5 実行」まで行ったら、動作確認へ進んでください。

---

3. 手順書

下記は、uApprove.jpについての説明です。

- uApprove.jpについて

手順書は、上記ページ内にリンク（「installation document in Japanese」）としてありますが、下記のリンクからも直接参照できます。

- 導入手順書

⚠ 導入手順書は単体のHTMLファイルですがブラウザで直接開くことができませんので、一旦ダウンロードしてから開いてください。

---

4. 動作確認

① 設定後、TomcatやApacheの再起動を行ってない場合は行なってください。

```
service tomcat6 restart
service httpd restart
```

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。
　※ログイン画面にリセット用チェックボックスが表示されている事を確認します。
　　（Reset my attribute release approvals）

⑥ 送信可能な属性値の一覧画面が表示されるので、そのまま次ボタンをクリックします。
　※オプション情報を全て選択せずに行います。（surname、givenName、mail、eduPersonAffiliation）

⑦ 送信される属性値の一覧画面が表示されるので、オプション情報が表示されていない事を確認します。

⑧ 送信ボタンをクリックすると属性受信の確認ページが表示されるので、オプション情報の属性が
　送信されてない事を確認します。

⑨ 一旦ブラウザを閉じ、再度ログインします。次は、オプション情報の「surname」を選択します。

⑩ 送信される属性値の一覧画面で「surname」が選ばれている事を確認します。
　送信ボタンをクリック後、属性受信の確認ページで受信された事を確認してください。

BACK TOP NEXT