GakuNin mAPを使ったグループの活用

1. はじめに

本メニューでは、学術認証フェデレーション内のSPであるGakuNin mAPを使ったグループ属性値を送信する設定を行います。
内容としては、IdPにGakuNin mAPを使用できるようにし、GakuNin mAPにグループなどを作成します。
またSPに対しては、GakuNin mAPに作成するSPコネクタと連携できるように設定します。

※前提条件として、活用編メニューにある「学認申請システムを使ってテストフェデレーションに参加する」を実施しておく必要があります。

※現在は「学認クラウドゲートウェイサービス」と呼ばれており、GakuNin mAPは当該サービスのグループ機能として統合されておりますが、本ページでは旧称のGakuNin mAPで説明しています。

---

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。

・前提条件

「学認申請システムを使ってテストフェデレーションに参加する」を実施し、IdPとSPをテストフェデレーションに登録しておく必要があります。
また、テストフェデレーションに存在するクラウドゲートウェイのSP検証環境を使用するので、ホスト名を「sptest.cg.gakunin.jp」に置き換えて設定します。

また、テストフェデレーションのIdPのIDは学認のIDほどしっかり管理されていないため、SP管理者としてのIDは特別なIdP(idp.sptest.cg.gakunin.jp)から払い出しています。本メニュー希望者はスタッフにその旨連絡しIDの払い出しを受けてください。IDに関する情報の連絡は学認申請システムに登録したメールアドレス宛に行います。

・IdP管理者に必要な情報

手順書の「クラウドゲートウェイ連携のための情報」内にある「IdP管理者に必要な情報」を参照し、IdPに必須属性である「ePPN (eduPersonPrincipalName)」を
送信できるよう/opt/shibboleth-idp/conf/attribute-filter.xmlに設定を追加します。

```
<!-- Release attributes to mAP -->
<AttributeFilterPolicy id="PolicyforCloudGateway">
<PolicyRequirementRule xsi:type="Requester" value="https://sptest.cg.gakunin.jp/shibboleth-sp" />

<AttributeRule attributeID="eduPersonPrincipalName">
    <PermitValueRule xsi:type="ANY" />
</AttributeRule>

</AttributeFilterPolicy>
```

・SP管理者に必要な情報

手順書の「クラウドゲートウェイ連携のための情報」内にある「SP管理者に必要な情報」を参照し、手順にそって進めていきます。「attribute-policy.xmlの編集」まで行います。
以下のように置き換えることを忘れないように設定してください。

クラウドゲートウェイ（IdP）のメタデータは、以下のように実習セミナー用DSサーバよりダウンロードして、/etc/shibboleth/metadata配下に配置します。

```
# wget https://ex-ds.gakunin.nii.ac.jp/sptestcgidp-metadata.xml
# mkdir -p /etc/shibboleth/metadata
# mv sptestcgidp-metadata.xml /etc/shibboleth/metadata
```

手順書の「shibboleth2.xmlの編集」にあるメタデータのファイル名「cgidp-metadata.xml」を「sptestcgidp-metadata.xml」に置き換えて設定します。
また、「SimpleAggregationの追加」、「attribute-policy.xmlの編集」では、設定値にホスト名があるので、「sptest.cg.gakunin.jp 」に置き換えることを忘れないでください。

・GakuNin mAPの設定：　GakuNin mAPにログイン

払い出されたIDを使ってSP管理者としてクラウドゲートウェイにログインします。（グループ機能の所在がわからない場合は左上の「MYグループ」をクリックしてください。）

テストフェデレーションのクラウドゲートウェイSP検証環境にアクセスします。
IdPは「クラウドゲートウェイSP検証環境IdP」を選択し、払い出されたIDでログインします。
https://sptest.cg.gakunin.jp/map/

アカウント作成画面が表示されるので、以下のように設定してください。

氏名：　任意
メールアドレス：　任意

・GakuNin mAPの設定：　SPコネクタの作成

各自のSPを設定し、GakuNin mAPから属性値を取得できるようにします。
手順書の[SP管理者]-[SPコネクタを作成する]を行ってください。

SPコネクタ名、SPコネクタID（英数記号）、紹介文は任意の文字列でかまいませんが、例えば「ex-sp-test**-年月」（例:ex-sp-test01-201811）を入力してください。
その他の項目は、デフォルト値で問題ありません。

対象SPには、各自のSPを指定することを忘れないでください。

※**は、各自の番号に置き換えてください。

・GakuNin mAPの設定：　グループの作成

使用するグループを作成します。 ここで登場人物を区別するため、一旦ログアウトし構築IdPのIDでログインしてください。
手順書の[グループ管理者]-[グループを作成する]を行ってください。

グループ名、グループID（英数記号）は任意の文字列でかまいませんが、例えば「ex-test**-年月」（例:ex-test01-201811）を入力してください。
その他の項目は、デフォルト値で問題ありません。
※**は、各自の番号に置き換えてください。

・GakuNin mAPの設定：　グループをSPコネクタに接続する

グループ情報をSPコネクタで使用できるように設定します。
手順書の[グループ管理者]-[サービスを利用する]を行ってください。

「利用するWebサービスを追加」ボタンをクリックして、作成したSPコネクタ（例:ex-sp-test01-201811）を選択します。

---

3. 手順書

下記の設定手順書を参照し、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。

- 設定手順書
  の「SP管理者に必要な情報」の項

---

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 ログインボタンをクリックします。

```
IdP

IdPUsername/Password
```

isMemberOfSP