送信属性同意機能の設定（組み込み機能）

1. はじめに

本メニューでは、IdPをカスタマイズします。
組み込み機能を使って実現します。
送信属性の選択を有効にする設定や送信属性同意機能に表示する属性の設定などを行います。

---

2. 実習セミナーでは

以下の手順で作業を進めてください。

・relying-party.xmlの確認

/opt/shibboleth-idp/conf/relying-party.xmlに以下の設定が入っていることを確認してください。

```
（省略）

<bean parent="SAML2.SSO" p:postAuthenticationFlows="attribute-release" />
<ref bean="SAML2.ECP" />
<ref bean="SAML2.Logout" />

（省略）
```

・idp.propertiesの修正

/opt/shibboleth-idp/conf/idp.propertiesに同意確認の対象となる属性にチェックボックスを表示し
ユーザが送信する属性を選択できるように設定します。
この設定を行わなければ、デフォルト設定である確認のみの表示となります。

```
#idp.consent.allowPerAttribute = false
idp.consent.allowPerAttribute = true
```

consent-intercept-config.xml

/opt/shibboleth-idp/conf/intercept/consent-intercept-config.xmlに同意確認対象とする属性を設定します。
ここでは、デフォルト設定では表示されている「eduPersonTargetedID」をIgnoredAttributeIDsに追加して、
確認を行わず（表示されない）に送信されることを試してみます。
※通常は追加しなくて良いかと思います。再度、設定を外して表示されることも試してみてください。

```
<util:set id="shibboleth.consent.attribute-release.IgnoredAttributeIDs">
<value>samlPairwiseID</value>
<value>eduPersonTargetedID</value>
</util:list>

※補足
<util:set id="shibboleth.consent.attribute-release.PromptedAttributeIDs">に
属性を設定すると、設定した属性のみが同意確認の対象となります。
```

・Jettyの再起動

Jettyを再起動して、更新した設定ファイルを読み込ませます。

```
# systemctl restart jetty
```

---

3. 手順書

以下は、英語での情報が記載されたwiki.shibboleth.netのURLです。
手順の詳細にご興味がある方はご参照ください。

参考: ConsentConfiguration

---

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。

③ 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。

④ IdPのログイン画面が表示されます。

⑤ Username/Passwordを入力して認証を行います。

⑥ 送信属性同意画面が表示されるので、 eduPersonTargetedID（画面上は、「サービス毎のユニークID」）が表示されない事と各属性に
チェックボックスが表示されていることを確認してください。
また、2番目のラジオボタンが選択されていること（今後同じ情報を同じSPに送信する場合は再度同意画面を表示しない）を確認してください。

⑦ 適当にチェックを入れて「同意」を押し、チェックを入れた属性値が正しく属性受信の確認ページに表示される事を確認してください。

⑧ このページの下部「ログアウト」リンクをクリックしSPからログアウトし、再度同じ手順を実行してください。ただしSSOにより④,⑤はスキップされます。加えて同意画面も表示されないことを確認してください。

※組み込み機能をそのまま（デフォルト設定で）使用すると送信属性の同意情報がクライアント側（ブラウザのCookie）に
保存されるため、違うブラウザを使用したり、 Firefoxで言うCookieなど保存されないプライベート
ウィンドウを使用すると保存していても、再度同意画面が表示されてしまいます。
（違うブラウザなど異なる環境からのアクセスやCookieを保持しないブラウザの場合、保存した同意情報が無効）
⑧まで確認ができたら、IEなど違うブラウザを使用するか、プライベートウィンドウを使用して同じ手順を実行し、保存した情報が
有効にならない事を確認してください。

BACK TOP NEXT