2024年11月8日

attribute-filterの自動生成演習

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)

[2.1 前提条件 2](#_heading=h.4sakf8v1y6up)

[2.2 SPの受信する属性情報の設定（学認申請システムで設定） 2](#_heading=h.jpbns6xcamhb)

[2.3 IdPの利用可能なSPの設定（学認申請システムで設定） 3](#_heading=h.j4vv60jc7e49)

[2.4 読み込み方法について 4](#_heading=h.1w9cbogx6wv)

[**3. 設定手順 5**](#_heading=h.2et92p0)

[3.1 attribute-filterのダウンロード設定 5](#_heading=h.f8xhtor1y3rw)

[3.2 attribute-filter-fromoffice-backing.xmlを作成 5](#_heading=h.py29utwa56y0)

[**4. 動作確認 6**](#_heading=h.tyjcwt)

# **1. はじめに**

本メニューでは、IdPをカスタマイズします。また学認申請システムを使ったIdPとSPの設定も行います。

内容としては、学認申請システムにてIdPに対しては使用するSPを設定し、SPに対しては受信する属性情報を設定します。IdPに対しては、自動生成されたattribute-filterを読み込ませる設定を行います。

# **2. 実習セミナーでは**

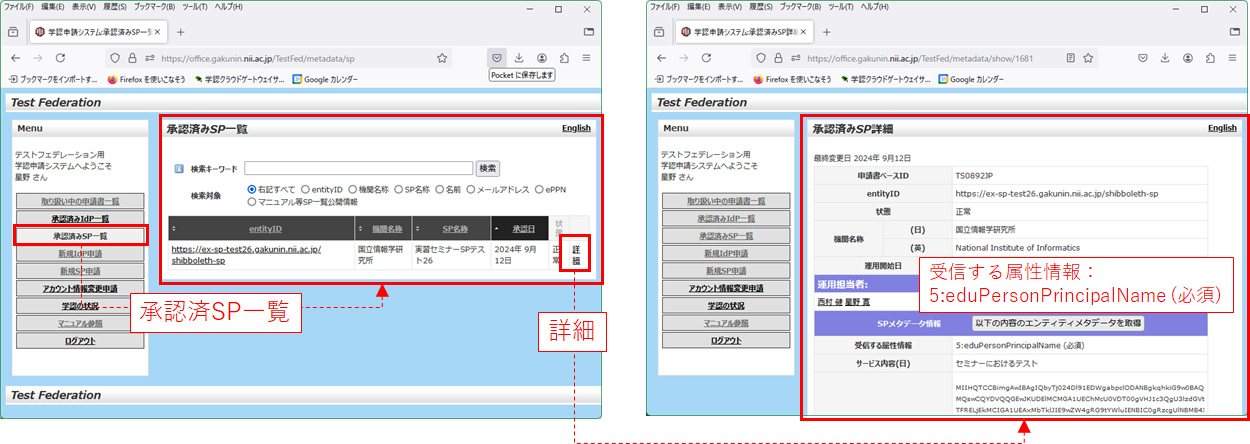
以下のような設定を事前に行っておきます。

## 2.1 前提条件

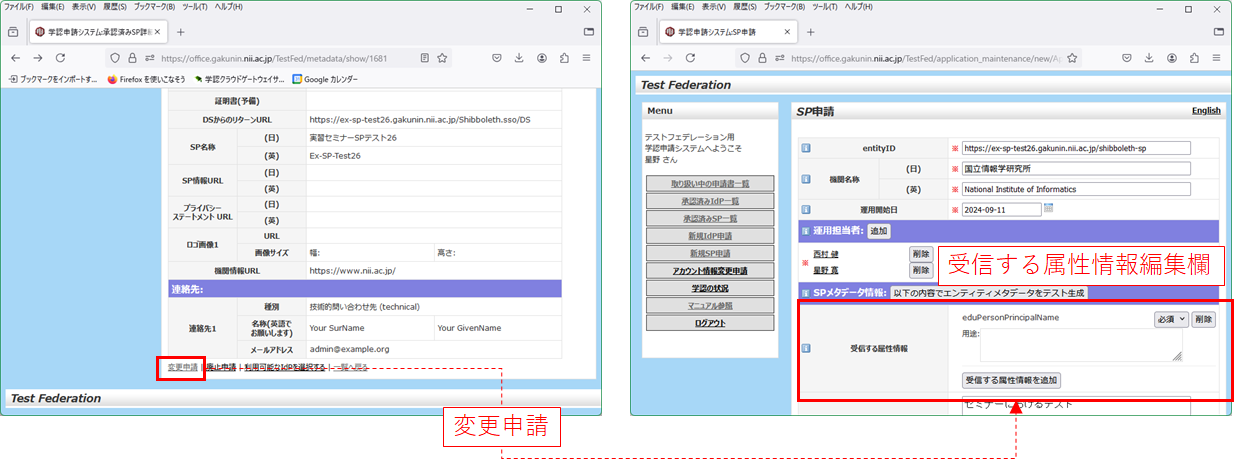
活用編メニュー「学認申請システムを使ってテストフェデレーションに参加する」を実施し、IdPとSPをテストフェデレーションに登録しておく必要があります。

## 2.2 SPの受信する属性情報の設定（学認申請システムで設定）

学認申請システムにアクセスし、承認済みSP一覧から各自が登録したSPの情報を開きます。「受信する属性情報」を設定してください。本メニューでは、「eduPersonPrincipalName」のみを設定します。



#### **図　承認済みSP一覧画面の遷移と受信する属性情報**

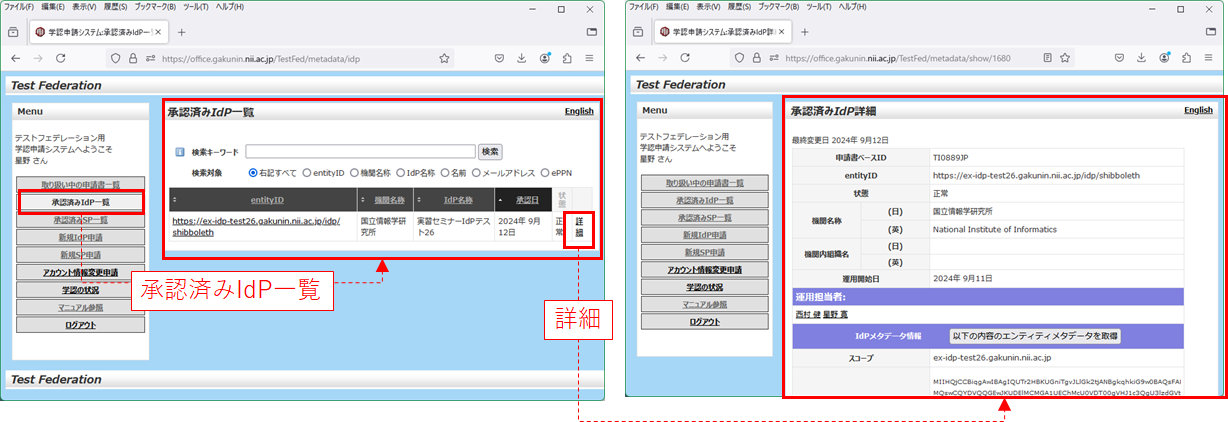


#### **図　変更申請画面と受信する属性情報の編集**

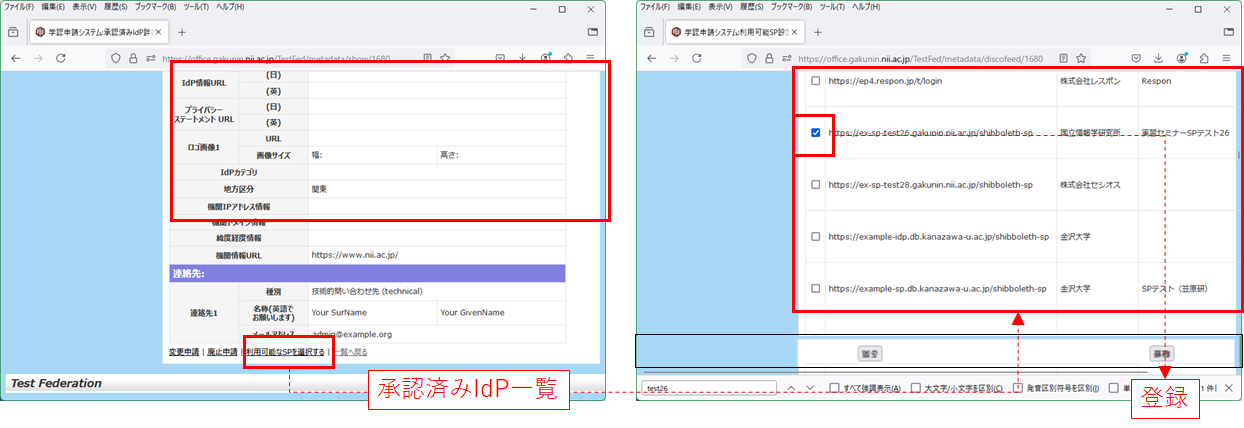
※詳しくは、活用編メニュー「学認申請システムを使ってテストフェデレーションに参加する」の[学認申請システム利用マニュアル（テストFed）](https://office.gakunin.nii.ac.jp/TestFed/manual.pdf) を参照してください。

## 2.3 IdPの利用可能なSPの設定（学認申請システムで設定）

学認申請システムにアクセスし、承認済みIdP一覧から各自が登録したIdPの情報を開きます。画面の一番下にあるリンク「利用可能なSPを選択する」から設定をしてください。実習セミナーでは、各自が登録しているSPのみを設定します。

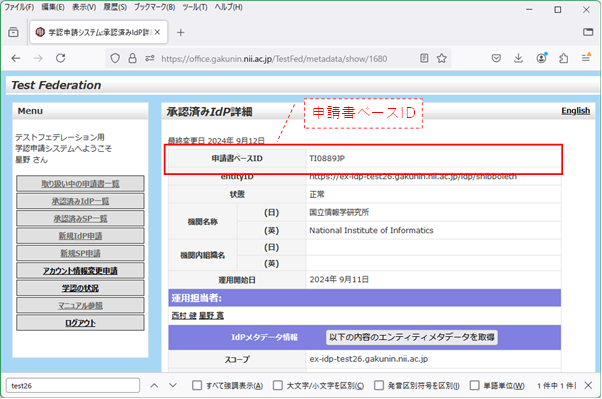


#### **図　承認済みIdP一覧と詳細情報**



#### **図　利用可能なSPから属性送信するSPを設定**

この時、設定時に使用するIdPの「申請書ベースID」をメモ帳などにコピーしておいてください。自動生成されたattribute-filterを取得するURLで使用します。



#### **図　承認済みIdP詳細画面の申請書ベースID**

## 2.4 読み込み方法について

自動生成されたattribute-filterを自動的に読み込み、直接設定ファイルを編集しない方法を行います。

IdPの申請書ベースIDについては上述の通り学認申請システムで確認してください。

# **3. 設定手順**

以下の手順で設定を行ってください。

※実習セミナーでは、管理者ユーザー（root）で作業を行います。

## 3.1 attribute-filterのダウンロード設定

/opt/shibboleth-idp/conf/services.xml に学認申請システムからattribute-filterをダウンロードするための設定を追加します。

※「TXXXXXJP」には、「２．」でメモ帳に貼り付けた各自の申請書ベースIDに置き換えてください。

|  |
| --- |
| <util:list id ="shibboleth.AttributeFilterResources">  <!--  <value>%{idp.home}/conf/attribute-filter.xml</value>  -->  <bean class="net.shibboleth.ext.spring.resource.FileBackedHTTPResource"  c:client-ref="GakuNinAttributeFilterHttpClient"  c:url="https://office.gakunin.nii.ac.jp/TestFed/export/attribute\_filter/TXXXXXJP?target=idp4"  c:backingFile="/opt/shibboleth-idp/conf/attribute-filter-fromoffice-backing.xml" />  </util:list>  <bean id="GakuNinAttributeFilterHttpClient" parent="shibboleth.HttpClientFactory"  p:connectionTimeout="%{idp.httpclient.connectionTimeout:PT1M}"  p:connectionRequestTimeout="%{idp.httpclient.connectionRequestTimeout:PT1M}"  p:socketTimeout="%{idp.httpclient.socketTimeout:PT1M}"  p:maxConnectionsTotal="%{idp.httpclient.maxConnectionsTotal:100}"  p:maxConnectionsPerRoute="%{idp.httpclient.maxConnectionsPerRoute:100}" />  <util:list id ="shibboleth.NameIdentifierGenerationResources"> |

## 3.2 attribute-filter-fromoffice-backing.xmlを作成

|  |
| --- |
| ⚠️この方法では、Jettyを非root権限で動かしている場合は、confディレクトリに新規ファイル（本課題の場合”attribute-filter-fromoffice-backing.xml”）を書き込めない可能性があります。その場合は c:backingFile に指定するファイルをあらかじめ作成し、ownerを変更するなどの事前準備が必要となります。  　# touch /opt/shibboleth-idp/conf/attribute-filter-fromoffice-backing.xml  　# chown jetty:jetty /opt/shibboleth-idp/conf/attribute-filter-fromoffice-backing.xml |

# **4. 動作確認**

|  |
| --- |
| ⚠️attribute-filter.xml（自動取得でない方）に構築SPへの属性送信を入れているかたは、動作が確認できない（全ての属性が送信されるのが正）ので、一時的にその部分（<AttributeFilterPolicy id="PolicyforExSP">から直近の</AttributeFilterPolicy>まで）をコメントアウトして、属性を送信しない設定にしてください。  こうすることで自動取得されたattribute-filterで属性送信が許可されていることが確認できます。 |

**/opt/shibboleth-idp/conf/attribute-filter.xml**

|  |
| --- |
| <!-- Policy for ex-sp -->  <!--  <AttributeFilterPolicy id="PolicyforExSP">  <PolicyRequirementRule xsi:type="NOT">  <Rule xsi:type="Requester" value="https://ex-sp2.gakunin.nii.ac.jp/shibboleth-sp" />  </PolicyRequirementRule>  <AttributeRule attributeID="o" permitAny="true" />  <AttributeRule attributeID="jao" permitAny="true" />  <AttributeRule attributeID="ou" permitAny="true" />  <AttributeRule attributeID="jaou" permitAny="true" />  <AttributeRule attributeID="eduPersonPrincipalName" permitAny="true" />  <AttributeRule attributeID="eduPersonTargetedID" permitAny="true" />  <AttributeRule attributeID="eduPersonAffiliation" permitAny="true" />  <AttributeRule attributeID="eduPersonScopedAffiliation" permitAny="true" />  <AttributeRule attributeID="eduPersonEntitlement" permitAny="true" />  <AttributeRule attributeID="sn" permitAny="true" />  <AttributeRule attributeID="jasn" permitAny="true" />  <AttributeRule attributeID="givenName" permitAny="true" />  <AttributeRule attributeID="jaGivenName" permitAny="true" />  <AttributeRule attributeID="displayName" permitAny="true" />  <AttributeRule attributeID="jaDisplayName" permitAny="true" />  <AttributeRule attributeID="mail" permitAny="true" />  <AttributeRule attributeID="gakuninScopedPersonalUniqueCode" permitAny="true" />  <AttributeRule attributeID="isMemberOf" permitAny="true" />  <AttributeRule attributeID="eduPersonAssurance" permitAny="true" />  <AttributeRule attributeID="eduPersonUniqueId" permitAny="true" />  <AttributeRule attributeID="eduPersonOrcid" permitAny="true" />  </AttributeFilterPolicy>  --> |

① 設定後、設定変更が反映されたattribute-filterを読み込むため、Jettyを再起動してください。

|  |
| --- |
| # systemctl restart jetty |

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。



#### 図　各自が使用するIdPにtest001でログインする画面

⑥ 正しく属性受信の確認ページが表示され、eduPersonPrincipalNameのみ属性値が送信できていることを確認します。



#### **図　eduPersonPrincipalNameのみ属性値が送信された画面**