2024年11月8日

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

国立情報学研究所

教育研修事業

**目次**

[**1. はじめに 2**](#_heading=h.3znysh7)

[**2. 事前準備 2**](#_heading=h.2et92p0)

[**3. 実習セミナーでは 3**](#_heading=h.tyjcwt)

[**4. IdP/SP申請 4**](#_heading=h.3dy6vkm)

[① ログイン 4](#_heading=h.dxrnzek18633)

[② 新規IdP申請 5](#_heading=h.c6fnuhp8lsw9)

[③ 新規SP申請 5](#_heading=h.jzvy9kkgqg3y)

[**5. 動作確認 7**](#_heading=h.1t3h5sf)

[・構築SPとテストフェデレーションテスト用IdPの間での接続テスト 7](#_heading=h.4d34og8)

[・構築IdPとテストフェデレーションテスト用SPの間での接続テスト 10](#_heading=h.2s8eyo1)

[・構築SPと構築IdPとの間での接続テスト 12](#_heading=h.17dp8vu)

[**6. 本セミナーを終了する際に 13**](#_heading=h.c328c5pionxw)

# **1. はじめに**

本メニューでは、IdP・SPを学認申請システム（テストFed）を使用して、実際にテストフェデレーションへ登録します。

テストフェデレーションに関して、詳しくは「[テストフェデレーションルール](https://www.gakunin.jp/join/test/rule/)」を参照してください。

# **2. 事前準備**

以下は、本課題を実施するために必要となる事前準備です。

Orthrosへの登録と使用できるWebメールアカウントの準備が必要です。  
Orthrosアカウントが未登録の場合、以下の手順で登録してください。

① [学認申請システム(テストFed)](https://office.gakunin.nii.ac.jp/TestFed/)ページの所属機関リストの一番下から「Orthros」を選択してください。

② Orthrosログインページから「今すぐサインアップ」をクリックし、登録ページに移動します。

③ 「アカウントを作成後、再度サービスへサインインしてください。」の下の「続行」ボタンをクリックします。

④ メールアドレス（入力必須）欄にメールアドレスを入力して、「認証コードを送信する」ボタンをクリックします。

⑤ 次のようなメールが届くので、認証コードを覚えてください。

|  |
| --- |
| メールアドレスの検証  認証コードをお知らせいたします。  コード: XXXXXX  Orthros |

⑥ ④の画面の「認証コード」欄にメールで届いた認証コードを入力し、「コードの確認」ボタンをクリックします。

⑦ 「メールアドレスが確認されました。 続行することができるようになりました。」というメッセージが表示されるので、残りの入力必須欄に入力し、「作成」ボタンをクリックします。

⑧ 登録された名前とメールアドレス等が表示される完了画面が表示されたら完了です。

# **3. 実習セミナーでは**

以下のような設定で行います。

「[4. IdP/SP申請](#_heading=h.3dy6vkm)」の申請書フォームへの入力項目及び「[5. 動作確認](#_heading=h.1t3h5sf)」の手順での設定項目と照らし合わせながら、作業を進めてください。

* アカウント作成時のメールアドレスについて

ここで設定したメールアドレスに申請システムからの確認メールが届くので、必ず使用可能なメールアドレスを設定してください。

* 申請（IdP）entityID

例）1番を割り振られた場合

　https://ex-idp-test01.gakunin.nii.ac.jp/idp/shibboleth

* 申請（SP）entityID

例）1番を割り振られた場合

　https://ex-sp-test01.gakunin.nii.ac.jp/shibboleth-sp

* スコープについて

例）1番を割り振られた場合

　ex-idp-test01.gakunin.nii.ac.jp

* 申請(IdP)証明書

# cat /opt/shibboleth-idp/credentials/server.crt

* 申請(SP)証明書

# cat /etc/shibboleth/cert/server.crt

* DSからのリターンURL

https://ex-sp-testXX.gakunin.nii.ac.jp/Shibboleth.sso/DS

* 連絡先

ここに限りませんがメタデータとして公開されますので、個人メールアドレス等公開して問題のある情報を入力することは避けてください。身の回りに公開メールアドレス等適当なものがなければ、ご相談ください。

* その他の項目について

各自の名前、所属機関などを設定してください。

# **4. IdP/SP申請**

以下の手順書は一般的な手順を説明しています。本活用編では以下の①以降を実行してください。

* [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)  
  4. IdP/SPの申請方法  
  5. 学認申請システムの利用方法  
  6. 申請時に必要な情報について

## ① ログイン

(1)学認申請システムトップページをブラウザで開いてください。

<https://office.gakunin.nii.ac.jp/TestFed/>

(2)「所属機関」プルダウンメニューからアカウント作成時に使用した IdP(Orthros) を選択してください。

(3) 表示されたログインフォームに ID/Password を入力してください。

(4) 学認申請システム上の新規アカウント登録画面になったら、各欄に入力し、「登録」ボタンをクリックしてください。

(5) 登録したメールアドレスに次のようなメールが届きます。

|  |
| --- |
| 件名：　[テストフェデ学認申請システム]メールアドレスのご確認のお願い  —---------------  XXXXXX 様  学認申請システムへのご登録ありがとうございます。  入力いただいたユーザー情報の登録を完了させるため、下記URLにアクセスしてください。  https://office.gakunin.nii.ac.jp/TestFed/auth/activate?register\_hash=\*\*\*\*\*\*\*\*\*\*  URLの有効期限は、このメールの送信日から一週間です。  もし、この通知に心当たりがない場合は、ご面倒ですがこのメールの破棄をお願いいたします。  ------------------------------------------------  学認申請システムに対するお問い合わせはこちらまで。  gakunin-office@nii.ac.jp |

(6) メール中のURLをクリックし、登録を完了させます。

## ② 新規IdP申請

1. 登録が完了するとログインした状態になりますので、左メニューの「新規IdP申請」ボタンをクリックし、新規IdP申請フォームを開いてください。

# 

1. 申請フォームの各欄に記入して、ページ下の「申請」ボタンをクリックしてください。
2. 申請した IdP の申請内容が事務局によりチェックされ問題がなければメタデータの生成および登録が学認申請システム(テストFed)によって自動的に行われます。登録完了後、その旨のメールがあなた宛に送られます。

## ③ 新規SP申請

1. 左メニューの「新規SP申請」ボタンをクリックし、新規SP申請フォームを開いてください。

# 

1. 申請フォームの各欄に記入して、ページ下の「申請」ボタンをクリックしてください。
2. 申請した SP の申請内容が事務局によりチェックされ問題がなければメタデータの生成および登録が学認申請システム(テストFed)によって自動的に行われます。登録完了後、その旨のメールがあなた宛に送られます。

# **5. 動作確認**

以下の動作確認手順は、IdP・SPの両方を参加させた場合です。

## ・構築SPとテストフェデレーションテスト用IdPの間での接続テスト

① DSをテストフェデレーションのものに変更

構築したSPの

/etc/shibboleth/shibboleth2.xml

にて、DSをテストフェデレーションのものに変更します。

|  |
| --- |
| <Sessions lifetime="28800" timeout="3600" relayState="ss:mem"  checkAddress="false" handlerSSL="false" cookieProps="http"  　　　　　　redirectLimit="exact">  （省略）  <!-- Session diagnostic service. -->  <Handler type="Session" Location="/Session" showAttributeValues="false"/>  <!-- JSON feed of discovery information. -->  <Handler type="DiscoveryFeed" Location="/DiscoFeed"/>  <SessionInitiator type="Chaining" Location="/DS" isDefault="true" id="DS">  <SessionInitiator type="SAML2" template="bindingTemplate.html"/>  <SessionInitiator type="Shib1"/>  <SessionInitiator type="SAMLDS" URL="https://test-ds.gakunin.nii.ac.jp/WAYF" />  </SessionInitiator>  </Sessions> |

② テストフェデレーションメタデータ検証用の証明書のダウンロード

テストフェデレーションメタデータ検証用の証明書を

https://metadata.gakunin.nii.ac.jp/gakunin-test-signer-2020.cer

からダウンロードします。

|  |
| --- |
| cd /etc/shibboleth/cert  wget https://metadata.gakunin.nii.ac.jp/gakunin-test-signer-2020.cer |

③ shibboleth2.xmlのメタデータダウンロード元と証明書を変更

|  |
| --- |
| <!--  Allows overriding of error template information/filenames. You can  also add your own attributes with values that can be plugged into the  templates, e.g., helpLocation below.  -->  <Errors supportContact="root@localhost"  helpLocation="/about.html"  styleSheet="/shibboleth-sp/main.css"/>  （省略）  <!-- Example of remotely supplied batch of signed metadata. -->  <!-- -->  <MetadataProvider type="XML" validate="true"  url="https://metadata.gakunin.nii.ac.jp/gakunin-test-metadata.xml"  backingFilePath="federation-metadata.xml" reloadInterval="7200">  <MetadataFilter type="RequireValidUntil" maxValidityInterval="1296000"/>  <MetadataFilter type="Signature"  certificate="/etc/shibboleth/cert/gakunin-test-signer-2020.cer"  verifyBackup="false"/>  <DiscoveryFilter type="Blacklist" matcher="EntityAttributes" trimTags="true"  attributeName="http://macedir.org/entity-category"  attributeNameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"  attributeValue="http://refeds.org/category/hide-from-discovery" />  <TransportOption provider="CURL" option="64">1</TransportOption>  <TransportOption provider="CURL" option="81">2</TransportOption>  <TransportOption provider="CURL" option="10065">  /etc/pki/tls/certs/ca-bundle.crt</TransportOption>  </MetadataProvider>  <!-- -->  <!-- Example of remotely supplied "on-demand" signed metadata. -->  <!--  <MetadataProvider type="MDQ" validate="true" cacheDirectory="mdq" |

④ shibdおよびhttpdを再起動

|  |
| --- |
| systemctl restart httpd  systemctl restart shibd |

⑤ テストフェデレーションDSから接続テスト用IdPを選択

* 各自構築したSP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/ |

* ログインボタンをクリックします。
* テストフェデレーションDSが表示されるので、所属している機関リストから関東カテゴリの「GakuNin テスト IdP」(英語表示の場合はKantoカテゴリの「GakuNin Test IdP」)を選択します。
* ログイン画面が表示されるので、ユーザtest001、パスワードtest001を入力して認証を行います。
* 正しく属性受信の確認ページが表示されます。

(IdPエンティティIDが”https://test-idp1.gakunin.nii.ac.jp/idp/shibboleth”となっていることを確認してください)

## ・構築IdPとテストフェデレーションテスト用SPの間での接続テスト

① テストフェデレーションメタデータ検証用の証明書をダウンロード

構築IdPにて、テストフェデレーションメタデータ検証用の証明書

https://metadata.gakunin.nii.ac.jp/gakunin-test-signer-2020.cer

からダウンロードします。

|  |
| --- |
| cd /opt/shibboleth-idp/credentials  wget https://metadata.gakunin.nii.ac.jp/gakunin-test-signer-2020.cer |

② メタデータ自動ダウンロード設定を変更

/opt/shibboleth-idp/conf/metadata-providers.xml

のメタデータ自動ダウンロード設定を変更します。

|  |
| --- |
| <?xml version="1.0" encoding="UTF-8"?>  <MetadataProvider id="ShibbolethMetadata" xsi:type="ChainingMetadataProvider"  （省略）  <!--  Example HTTP metadata provider. Use this if you want to download the metadata  from a remote source.  （省略）  <!-- -->  <MetadataProvider id="HTTPMetadata"  xsi:type="FileBackedHTTPMetadataProvider"  backingFile="%{idp.home}/metadata/gakunin-metadata-backing.xml"  metadataURL=  "https://metadata.gakunin.nii.ac.jp/gakunin-test-metadata.xml"  failFastInitialization="false">  <MetadataFilter xsi:type="SignatureValidation"  certificateFile="%{idp.home}/credentials/gakunin-test-signer-2020.cer" />  <MetadataFilter xsi:type="RequiredValidUntil" maxValidityInterval="P15D"/>  <MetadataFilter xsi:type="EntityRole">  <RetainedRole>md:SPSSODescriptor</RetainedRole>  </MetadataFilter>  </MetadataProvider>  <!-- --> |

③ jettyを再起動します。

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

④ テストフェデレーションの接続テスト用SPにアクセス

<https://test-sp1.gakunin.nii.ac.jp> にアクセスします。

* 「接続テスト」ボタンをクリックします。
* テストフェデレーションDSの所属している機関から「**各自の構築したIdP名称」**があるかどうかを確認し、選択をします。

　（※ここで選択するIdPは **GakuNin テスト IdPではありません**。

/opt/shibboleth-idp/metadata/gakunin-metadata-backing.xmlのentityIDがhttps://ex-idp-test??.gakunin.nii.ac.jp/idp/shibbolethである<mdui:DisplayName xml:lang="ja">要素で定義されているIdP名称になります。）

* IdPのログイン画面が表示されるので、**ユーザtest001**、**パスワードtest001**を入力して認証を行います。
* 正しく属性受信の確認ページが表示されることを確認してください。（本確認についてのみ、属性が全て"NOT RECEIVED"になっていても問題ありません。そうなっていることを確認した上で次の確認に進んでください。）

## ・構築SPと構築IdPとの間での接続テスト

① 各自構築したSP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 テストフェデレーションDSの所属している機関から「**各自の構築したIdP名称**」を選択します。

④ IdPのログイン画面が表示されるので、**ユーザtest001**、**パスワードtest001**を入力して認証を行います。

⑤ 正しく属性受信の確認ページが表示されることを確認してください。

# **6. 本セミナーを終了する際に**

受講している本セミナーを終了する際に、今回作成したOrthrosアカウントを削除してください。詳細は [Orthros利用マニュアル > アカウント削除](https://meatwiki.nii.ac.jp/confluence/pages/viewpage.action?pageId=118168818#id-%E5%88%A9%E7%94%A8%E3%83%9E%E3%83%8B%E3%83%A5%E3%82%A2%E3%83%AB-%E3%82%A2%E3%82%AB%E3%82%A6%E3%83%B3%E3%83%88%E5%89%8A%E9%99%A4delete_account) の項を参照してください。

なお、登録されたIdP/SPは自動的に削除されます。今回学認申請システムに登録されたアカウントも後日自動的に削除されます。