2024年11月8日

GakuNin mAPを使ったグループの活用

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 3**](#_heading=h.3znysh7)

[**3. 設定手順（割り振られたIdP, SPでの設定） 6**](#_heading=h.30x3if5bl1b4)

[3.1 IdP管理者に必要な情報 6](#_heading=h.ng7vxnn5zq2x)

[3.2 SP管理者に必要な情報 7](#_heading=h.mr3f7ap0mau7)

[**4. GakuNin mAPの設定 10**](#_heading=h.os0uqvrj6yny)

[4.1 GakuNin mAPにログイン 10](#_heading=h.sci154bmgjvo)

[4.2 SPコネクタの作成 13](#_heading=h.cuaf28ptoh1b)

[4.3 グループの作成 14](#_heading=h.ubciicyjd8ys)

[4.4 グループをSPコネクタに接続する 17](#_heading=h.2gtdq74hwpa3)

[**5. 動作確認 19**](#_heading=h.8mjthnj28yog)

# **1. はじめに**

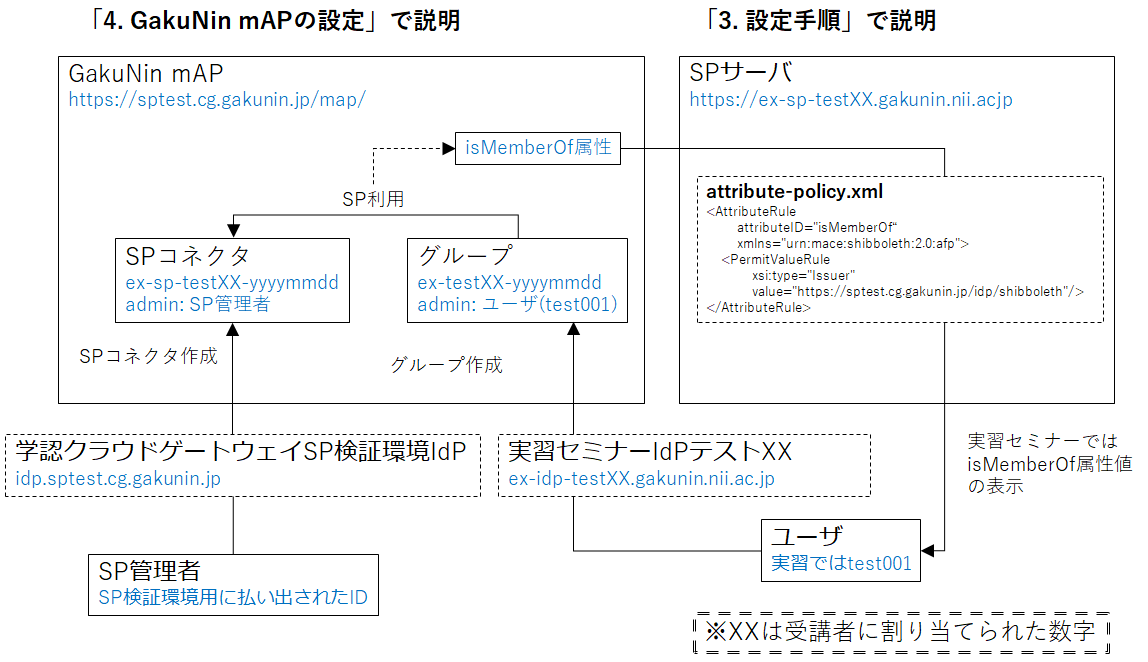
本メニューでは、IdPとSPを共にカスタマイズします。

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。

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



#### **図　本課題の全体像**

# **2. 実習セミナーでは**

以下は、実習セミナーでの前提条件となります。

・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。

・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、ホスト名は「sptest.cg.gakunin.jp」となります。

・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。

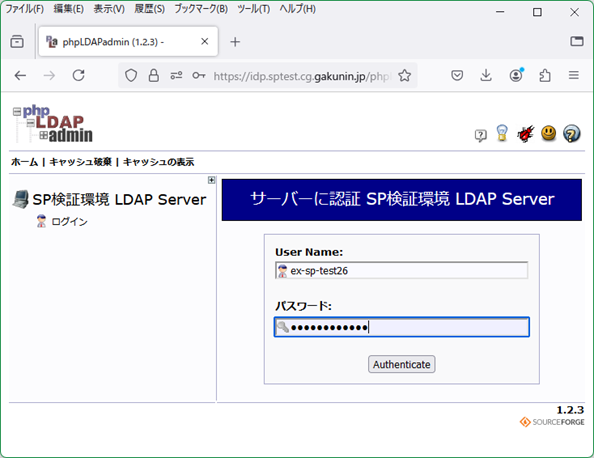
・テストフェデレーションに存在するクラウドゲートウェイのSP検証環境を使用するので、本メニュー希望者はスタッフにその旨連絡しIDの払い出しを受けてください。IDに関する情報の連絡は学認申請システムに登録したメールアドレス宛に行います。

|  |
| --- |
| ご担当者さま  お世話になっております。学認クラウドゲートウェイサービスサポートです。  機密情報を含みますので個人宛でご連絡しています。  SP管理者としてSP検証環境を利用できるように、「学認クラウドゲートウェイサービスSP検証環境IdP」から以下のアカウントを作成しました。  初期パスワードをお送りいたしますので、手順に従ってパスワードの変更を行ってください。  アカウント名 : ex-sp-testXX  初期パスワード : ■■■■■■  パスワード変更手順は<https://idp.sptest.cg.gakunin.jp/index.html> をご参照ください。  ※ パスワードは以下のルールを満たすように設定してください。  ・最低8文字以上の長さをもつこと  ・以下のア〜エの文字集合から各最低1文字を含むこと  ・ア ) 英大文字 (A〜Z)  ・イ ) 英小文字 (a〜z)  ・ウ ) 数字 (0〜9)  ・エ ) システムで使用可能な特殊文字 (@!#$%&=-+\*/.,:;[]|) |

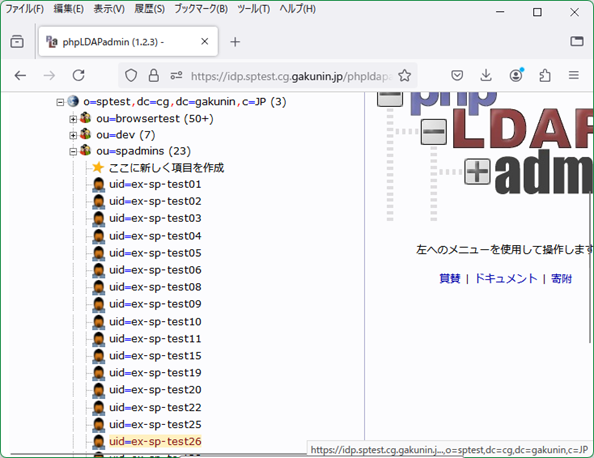
#### **図　IDの払い出しのメール例**

**※払い出されたIDのパスワード変更の手順を示しておきます。**

<https://idp.sptest.cg.gakunin.jp/phpldapadmin> にアクセスし、初期パスワードを入力します。



パスワード変更したいアカウントを選びます。



右欄に新しいパスワードを入力し、次ページで「オブジェクト更新」を押せば完了です。



# 

# **3. 設定手順（割り振られたIdP, SPでの設定）**

以下の手順で設定を行ってください。

## 3.1 IdP管理者に必要な情報

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。

|  |
| --- |
| <AttributeFilterPolicyGroup id="ShibbolethFilterPolicyForGakuNinTestFed"  xmlns="urn:mace:shibboleth:2.0:afp"  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"  xsi:schemaLocation="urn:mace:shibboleth:2.0:afp http://shibboleth.net/schema/idp/shibboleth-afp.xsd">  <!-- 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>  <!-- Policy for ex-sp --> |

## 3.2 SP管理者に必要な情報

まず、他の活用編メニューで構築SPが特定の認証方式／レベルを要求するようにしていると構築IdPからログインできなくなっている場合がありますのでこれを解除してください。以下のように/etc/httpd/conf.d/shib.confを変更します。

|  |
| --- |
| <Location /secure>  AuthType shibboleth  ShibRequestSetting requireSession 1  # ShibRequestSetting authnContextClassRef urn:mace:gakunin.jp:idprivacy:ac:classes:Level2 ↑上記のような行が存在する場合は先頭に#を挿入してコメントアウトしてください  require shib-session  </Location> |

クラウドゲートウェイ（IdP）のメタデータは、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 |

学認クラウドゲートウェイサービス (IdP)メタデータの読み込み設定を行います。

/etc/shibboleth/shibboleth2.xmlに設定を追加します。

|  |
| --- |
| <!-- Example of locally maintained metadata. -->  <!--  <MetadataProvider type="XML" validate="true" path="partner-metadata.xml"/>  -->  <MetadataProvider type="XML"  path="/etc/shibboleth/metadata/sptestcgidp-metadata.xml"/> |

通常の認証フローの後にeppnを手がかりとして学認クラウドゲートウェイサービス (IdP)からisMemberOf属性を取得するよう、SimpleAggregation設定を行います。

同じく、/etc/shibboleth/shibboleth2.xmlに設定を追加します。

|  |
| --- |
| <!-- Map to extract attributes from SAML assertions. -->  <AttributeExtractor type="XML" validate="true" reloadChanges="false" path="attribute-map.xml"/>  <AttributeResolver type="SimpleAggregation" attributeId="eppn" format="urn:oid:1.3.6.1.4.1.5923.1.1.1.6">  <Entity>https://sptest.cg.gakunin.jp/idp/shibboleth</Entity>  <saml2:Attribute xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion" Name="urn:oid:1.3.6.1.4.1.5923.1.5.1.1" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri" FriendlyName="isMemberOf"/>  </AttributeResolver>  <!-- Default filtering policy for recognized attributes, lets other data pass. --> |

他のIdPからのisMemberOf属性を拒否し、学認クラウドゲートウェイサービスからのisMemberOfのみを利用する設定を行います。

/etc/shibboleth/attribute-policy.xmlに設定を追加します。

|  |
| --- |
| <!-- Enforce that the values of schacHomeOrganization are a valid Scope. -->  <afp:AttributeRule attributeID="schacHomeOrganization">  <afp:PermitValueRule xsi:type="saml:AttributeValueMatchesShibMDScope"/>  </afp:AttributeRule>  <AttributeRule attributeID="isMemberOf" xmlns="urn:mace:shibboleth:2.0:afp">  <PermitValueRule xsi:type="Issuer"  value="https://sptest.cg.gakunin.jp/idp/shibboleth"/>  </AttributeRule>  <!-- Catch-all that passes everything else through unmolested. -->  <afp:AttributeRule attributeID="\*" permitAny="true"/> |

以上の更新を反映してください。

|  |
| --- |
| 以下を割り当てられたIdPで実行  # systemctl restart jetty 以下を割り当てられたSPで実行 # systemctl restart httpd  # systemctl restart shibd |

# **4. GakuNin mAPの設定**

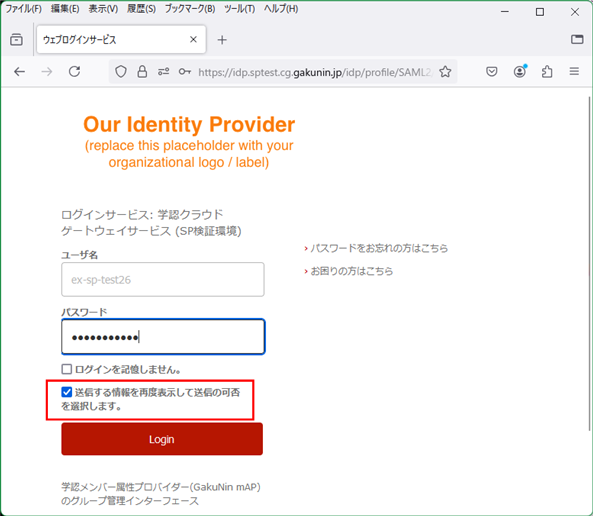
## 4.1 GakuNin mAPにログイン

「[2. 実習セミナーでは](#_heading=h.3znysh7)」で払い出された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。  https://sptest.cg.gakunin.jp/map/ IdPは「学認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。 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 |

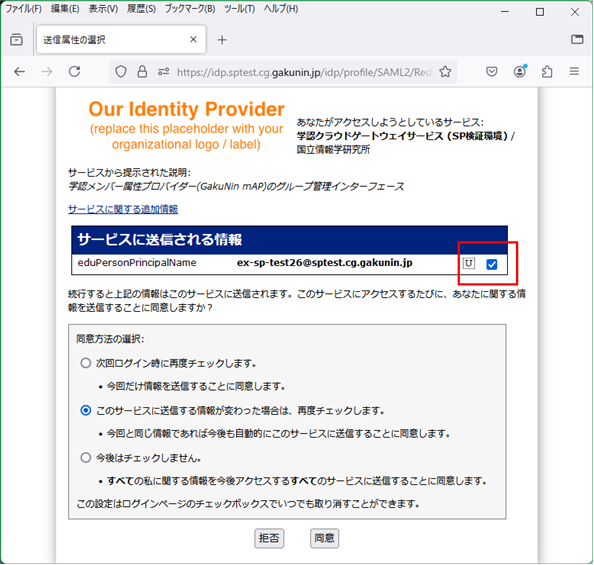


#### **図 「学認クラウドゲートウェイサービスSP検証環境IdP」を選択**



#### **図　払い出されたIDでログイン**

「送信する情報を再度表示して送信の可否を選択します」にチェックを入れます。



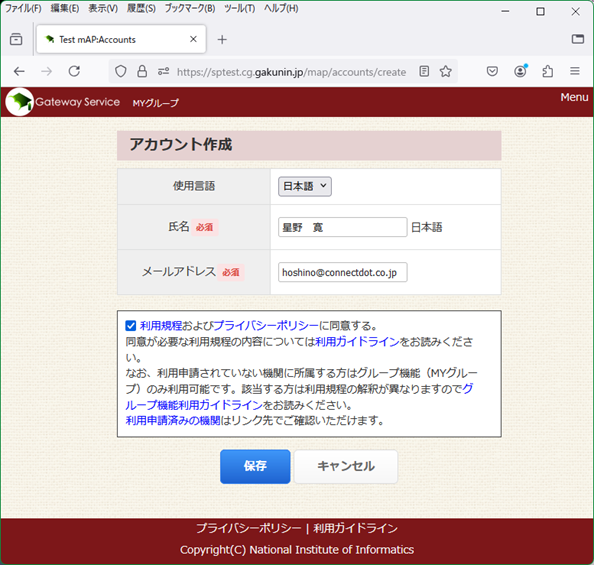
#### **図　送信する情報の確認画面**

「サービスに送信される情報　eduPersonPrincipalName」にチェックを入れます。

※なお、「eduPersonPrincicalName」にチェックを入れず、この属性が送信されなかった場合は、次のような画面になり、ログインできません。



#### **図　ePPN属性が送信されずログインできない画面**



#### **図　ログイン後、氏名・メールアドレス入力画面**

「保存」ボタンをクリックすると、初期画面に「アカウント情報を保存しました」というメッセージが表示されます。

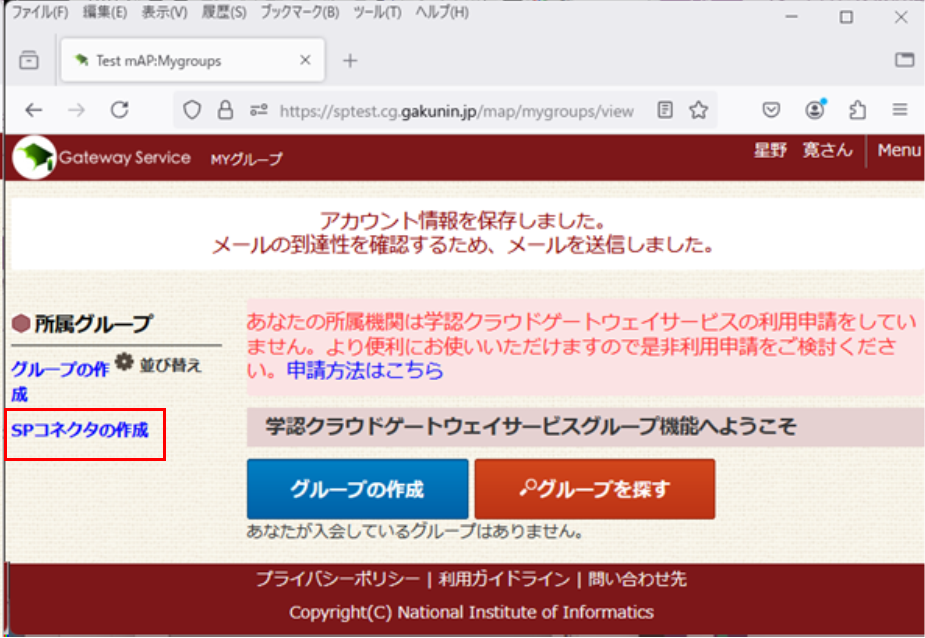
## 4.2 SPコネクタの作成

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](https://meatwiki.nii.ac.jp/confluence/pages/viewpage.action?pageId=20873902)]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。 |

「SPコネクタ作成」メニューをクリックします。



#### **図　ログイン直後の画面で「SPコネクタの作成」メニューを選ぶ**

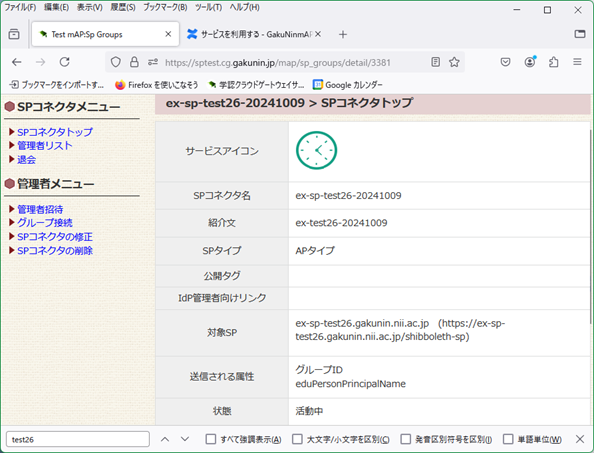
次の入力画面で、

送信される属性：「eduPersonPrincipalName (APIでの利用)」

対象SP：「ex-sp-test\*\*.gakunin.nii.ac.jp

（https://ex-sp-test\*\*.gakunin.nii.ac.jp/shibboleth-sp）」

を設定後、「保存」ボタンをクリックします。



#### **図　SPコネクタ確認画面**

## 4.3 グループの作成

作成したSPを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（実習セミナー環境では、「実習セミナーIdPテストXX」：XXは各自の番号）のID（実習セミナー環境では、test001）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](https://meatwiki.nii.ac.jp/confluence/pages/viewpage.action?pageId=20873785)]を行ってください。

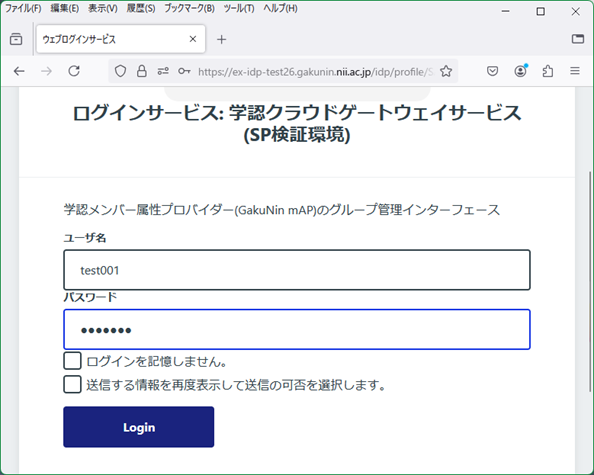
|  |
| --- |
| グループ名、グループID（英数記号）は任意の文字列でかまいませんが、例えば「ex-test\*\*-年月」（例:ex-test01-201811）を入力してください。  その他の項目は、デフォルト値で問題ありません。  ※\*\*は、各自の番号に置き換えてください。 |

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。

https://sptest.cg.gakunin.jp/map/

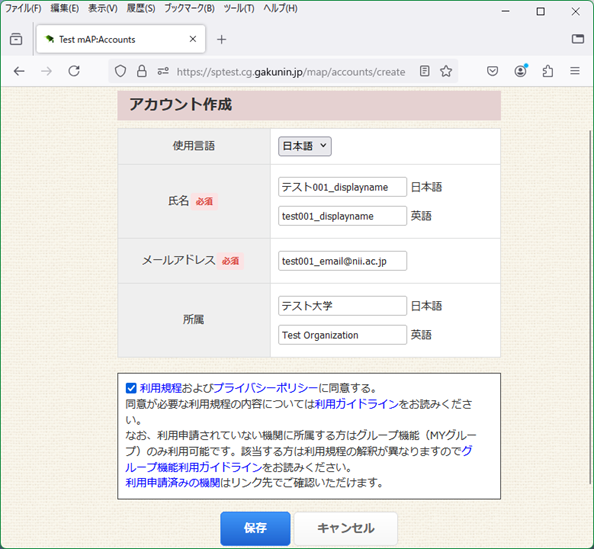


#### **図　IdPとして「実習セミナーIdPテストXX」を選択する**

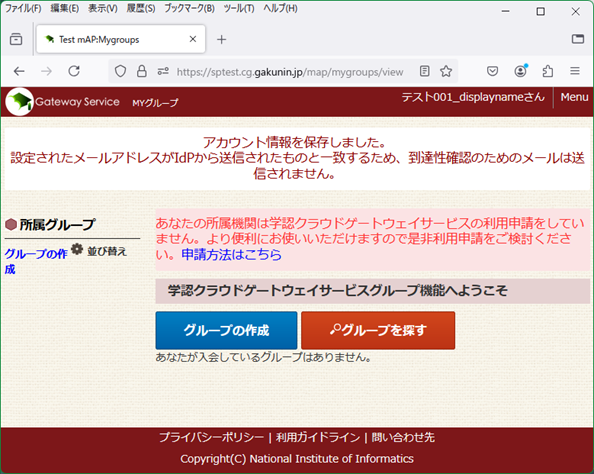


#### **図　test001でログイン**

最初は「アカウント作成画面」になるので、「利用規程およびプライバシーポリシーに同意する」にチェックし、「保存」ボタンを押します。



#### **図　アカウント作成画面**



#### **図　グループの作成メニュー**

グループ名、グループIDに、例えば「ex-test\*\*-年月」（例:ex-test01-201811）を入力してください。



#### **図　グループ作成完了画面**

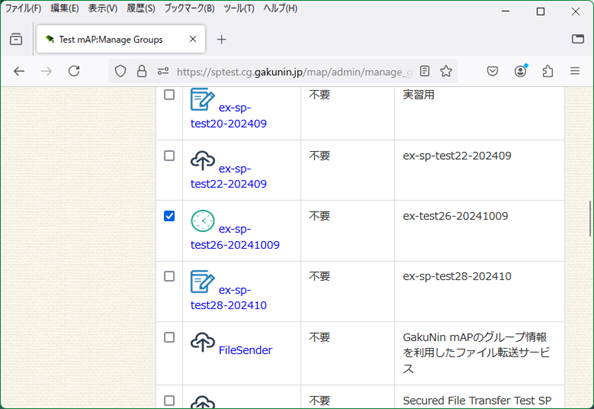
## 4.4 グループをSPコネクタに接続する

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](https://meatwiki.nii.ac.jp/confluence/pages/viewpage.action?pageId=20873789)]を行ってください。

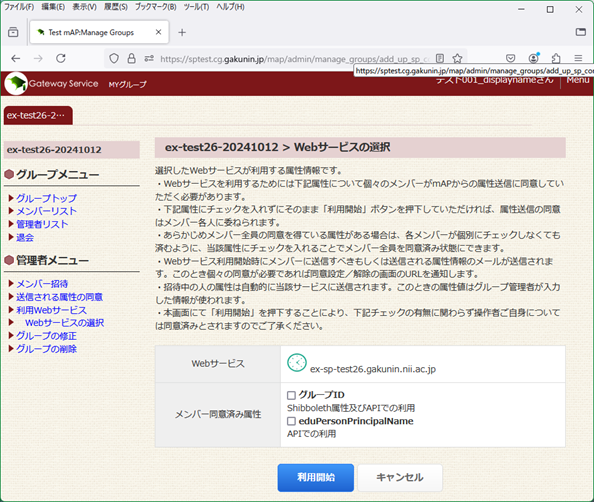
|  |
| --- |
| 「利用するWebサービスを追加」ボタンをクリックして、作成したSPコネクタ（例:ex-sp-test01-201811）を選択します。 |

「利用Webサービスの選択」メニューをクリックすると、利用可能なサービスの一覧が表示されます。

****

#### **図　利用可能サービス一覧画面**

作成したSP（ex-sp-testXX-yyyymmdd）にチェックを入れ、「確認」ボタンをクリックして下さい。次の画面で「利用開始」をクリックします。



#### **図　サービスの利用を開始する**

# **5. 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/ |

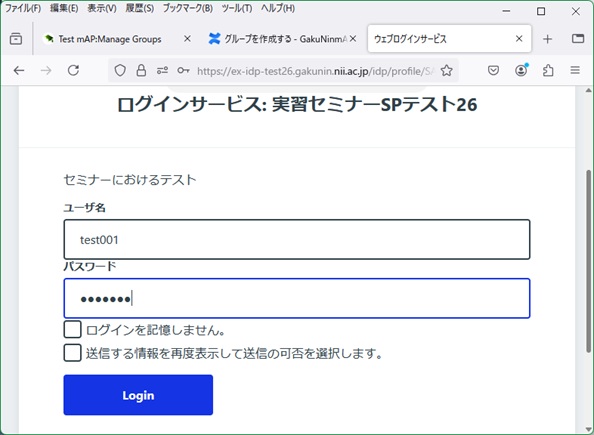
② ログインボタンをクリックします。

③ テストフェデレーション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。



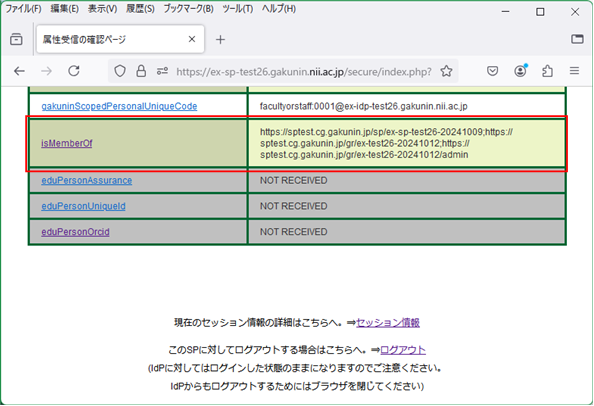
#### **図　「実習セミナーIdPテストXX」を選択**

④ 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。（実習では、test001でログインします）



#### **図　test001でログイン**

⑤ 正しく属性受信の確認ページが表示され、isMemberOf属性にSPコネクタ名やグループ名が送信できていることを確認します。



#### **図　isMemberOf属性値を受信し表示されている画面**

※isMemberOf属性値の意味は以下の通りです。

|  |  |
| --- | --- |
| 内容 | 意味 |
| https://sptest.cg.gakunin.jp/sp/ex-sp-test26-20241009 | 「ex-sp-test26-20241009」サービスと接続  test001が所属する「ex-test26-20241012」グループが「ex-sp-test25-20241009」サービスを利用できる |
| https://sptest.cg.gakunin.jp/gr/ex-test26-20241012 | test001が「ex-test26-20241012」グループに所属している |
| https://sptest.cg.gakunin.jp/gr/ex-test26-20241012/admin | test001が「ex-test26-20241012」グループのadminである |