

ユーザによる認証方式が選択できる設定

以下で認証方式を選択できる簡便な方法（Extendedフロー）を説明していますが、3.3以降であればより汎用的で複雑な挙動が実現できる[MFAによる方法](#)もご参照ください。

特にTOTPとの共存はNGですので、TOTPを認証方式の一つとして選択させたい場合は[MFAによる方法](#)をご検討ください。

もしくは、未検証ですが以下のforkで解消している可能性がありますのでお試しください。検証結果を学認事務局と共有いただければ幸いです。

<https://github.com/joeFischetti/Shibboleth-IdP3-TOTP-Auth>

1. はじめに

※前提として、「[セキュリティレベルを設定したSPに対する認証](#)」が実施済みであるとします。
本メニューでは、IdPをカスタマイズします。

ログイン時に対象SPが使用できる認証方式をユーザが選択してログインできるようになります。
セキュアなクライアント証明書認証などが行えるユーザは、ID/パスワードの入力が必要なく、SPにアクセスできます。

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。

・ Password認証フローの設定

以下のように/opt/shibboleth-idp/conf/authn/authn.propertiesを変更します。
※「Level3」は追加せず、「Level2」のみ設定を追加します。

(省略)

```
saml2/urn:oasis:names:tc:SAML:2.0:ac:classes>PasswordProtectedTransport, ¥
saml2/urn:oasis:names:tc:SAML:2.0:ac:classes>Password, ¥
saml1/urn:oasis:names:tc:SAML:1.0:am:password, ¥
saml2/urn:mace:gakunin.jp:idprivacy:ac:classes:Level1, ¥
saml2/urn:mace:gakunin.jp:idprivacy:ac:classes:Level2
# Validators are controlled in password-authn-config.xml
```

(省略)

・ Extendedフローの設定

以下のように/opt/shibboleth-idp/conf/authn/password-authn-config.xmlを変更します。
※「X509」は設定せず、「RemoteUser」のみ設定します。

※4.2からExtendedフローのサンプルが削除されておりますので、最終行の1行上に以下の赤字部分を挿入します。

```
<bean id="shibboleth.authn.Password.ExtendedFlows" class="java.lang.String" c:_0="RemoteUser" />
<util:list id="shibboleth.authn.Password.ExtendedFlowParameters">
</util:list>
<util:list id="shibboleth.authn.Password.PrincipalOverride">
  <bean parent="shibboleth.SAML2AuthnContextClassRef"
    c:classRef="urn:oasis:names:tc:SAML:2.0:ac:classes>PasswordProtectedTransport" />
  <bean parent="shibboleth.SAML2AuthnContextClassRef"
    c:classRef="urn:oasis:names:tc:SAML:2.0:ac:classes>Password" />
  <bean parent="shibboleth.SAML1AuthenticationMethod"
    c:method="urn:oasis:names:tc:SAML:1.0:am:password" />
  <bean parent="shibboleth.SAML2AuthnContextClassRef"
    c:classRef="urn:mace:gakunin.jp:idprivacy:ac:classes:Level1" />
</util:list>
</beans>
```

・ ログイン画面(login.vm)の置き換え

同様に4.2以降のログイン画面ではExtendedフローのコードが削除されておりますので、[添付](#)のもので置き換えます。

```
# wget https://ex-ds.gakunin.nii.ac.jp/login.vm
# chown root:root login.vm
# mv -f login.vm /opt/shibboleth-idp/views/
```

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。

※手順書内の「Password認証フローのExtendedフロー」を実施し、確認します。

- [設定手順書](#)

4. 動作確認

※確認手順の説明に記載されている「[動作確認用のSP](#)」は、現在使用しているフェデレーションによってアクセス先が変わります。（どちらかのフェデレーションに参加して利用できる状態にしておいてください。）

実習セミナーフェデレーション	https://ex-sp.gakunin.nii.ac.jp/
テストフェデレーション	https://test-sp1.gakunin.nii.ac.jp/

- ① 設定後、Jettyの再起動を行ってない場合は行ってください。

```
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の設定を行っている場合、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 認証方式を選択する画面が表示されるのですが、[各自が使用するSP](#)のセキュリティレベルが証明書認証が必要と設定しているので、RemoteUserボタン（クライアント証明書）のみ表示され、選択可能となります。
- ⑥ 個人証明書の要求というダイアログが表示されるので、対象となるクライアント証明書を選択して、OKボタンをクリックします。
※送信属性同意画面が表示される場合は、そのまま設定値を送信します。
- ⑦ 正しく属性受信の確認ページが表示される事を確認してください。
- ⑧ この状態で[動作確認用のSP](#)にアクセスすると、セキュリティレベルが低いためSSOにより認証がスキップされます。
- ⑨ 一度ブラウザを閉じて、[動作確認用のSP](#)にアクセスします。
- ⑩ 進めていくと[動作確認用のSP](#)はID/パスワード認証でも認証が可能であるため、認証方式を選択する画面では、Loginボタン（ID/パスワード）とRemoteUserボタン（クライアント証明書）の2つのボタンが表示されます。
- ⑪ Loginボタン（ID/パスワード）を選択する場合は、ユーザ名とパスワードを入力してボタンをクリックしてください。
- ⑫ 認証後、正しく属性受信の確認ページが表示される事を確認してください。
- ⑬ この状態で[各自が使用するSP](#)にアクセスすると、セキュリティレベルが上なので⑤と同じ画面が表示されます。