セキュリティレベルを設定したSPに対する認証

> 以下で認証方式をレベルで指定する簡便な方法（認証フローの階層化）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。

1. はじめに

※前提として、「クライアント証明書認証を使った認証」が実施済みであるとします。
本メニューでは、IdPとSPを共にカスタマイズします。
IdPには、ID/パスワード認証とクライアント証明書認証を使って、セキュリティレベルに応じた認証方式を設定します。
またSPには、認証のセキュリティレベルを設定します。

上記の設定により、セキュリティレベルが低くて問題ないSPにはID/パスワード認証でアクセスが行えるが、
セキュリティレベル高いSPにアクセスした場合、認証済みであってもクライアント証明書認証などセキュアな
認証方式を行わなければアクセスできないようになります。

なお、本メニュー（認証フローの階層化）に依らなくても、SP側でIdPのauthn.propertiesに記載されているURIを直接指定する（SP設定の ShibRequestSetting authnContectClassRef ... に指定する）ことによってIdPが定義している特定の認証手段を用いることを強制することは可能です。ただしSP側がIdPの設定内容を熟知している必要があります。

---

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。

＜IdP側の設定＞

・/opt/shibboleth-idp/conf/authn/authn.properties の変更

前段で設定したクライアント証明書強制を無効化します。パスワード認証を追加します。

```
# Regular expression matching login flows to enable, e.g. IPAddress|Password
#idp.authn.flows = Password
idp.authn.flows = RemoteUser|Password
```

・認証フローの階層化

実習セミナーでは、ID/パスワードと証明書の２つの認証方式で確認します。

手順書内では、/opt/shibboleth-idp/conf/idp.propertiesとなっていますが、/opt/shibboleth-idp/conf/authn/authn.propertiesを以下のように変更します。

※「X509」及び「Level3」の設定は、行いません。

```
（省略）

# Whether to prioritize "active" results when an SP requests more than
# one possible matching login method (V2 behavior was to favor them)
idp.authn.favorSSO = true

※アンコメントして、true（有効）にします。
```

また、その他においても/opt/shibboleth-idp/conf/authn/authn.propertiesを手順書に沿って変更します。
※Level3の設定を除いた、Level1～Level2の設定とします。「X509」に関する設定は不要です。

＜SP側の設定＞

・SP毎にセキュリティレベルを設定

各自作成したSPの認証をセキュリティレベル２に設定し、クライアント証明書を使った認証が必要と設定します。
以下のように/etc/httpd/conf.d/shib.confを変更します。
「/secure」に設定している内容に、IdPで設定したセキュリティレベル2を指定する設定を追加します。

```
<Location /secure>
  AuthType shibboleth
  ShibRequestSetting requireSession 1
 ShibRequestSetting authnContextClassRef urn:mace:gakunin.jp:idprivacy:ac:classes:Level2
 require shib-session
</Location>
```

---

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「認証フローの階層化」を実施し、確認します。
（「Password認証フローのExtendedフロー」の設定については、
「ユーザによる認証方式が選択できる設定」で実施します。）

- 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、IdPはJetty、SPはApacheの再起動を行ってない場合は行ってください。

```
IdP側
systemctl restart jetty

SP側
systemctl restart httpd
```

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 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します。

⑥ 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。

※ID/パスワードを入力するログイン画面は表示されず、クライアント証明書で認証が行われ、
ログインする事ができます。

⑦ 次に動作確認用のSPにアクセスし、認証要求がなくシングルサインオンにてログインできます。

⑧ 一度ブラウザを閉じて、再度動作確認用のSPにアクセスします。

⑨ セキュリティレベルが動作確認用SPには設定されていないため、進めていくとデフォルト設定の
Loginボタン（ID/パスワード）となります。ID/パスワードを入力してログインしてください。

⑩ 次に各自が作成したSPにアクセスします。今回はシングルサインオンとして認証済みですが、
アクセスレベルが動作確認用SPよりも高いため、証明書認証が要求されます。

⑪ 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。