クライアント証明書認証を使った認証

1. はじめに

本メニューでは、IdPをカスタマイズします。
インストール状態ではID/パスワード認証となっていますが、クライアント証明書による認証を行う設定です。

---

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。

・認証局のCA証明書

以下のコマンドで入手してください。
wget https://ex-ds.gakunin.nii.ac.jp/cacert.pem

以下のようにCA証明書を配置します。
cp cacert.pem /opt/shibboleth-idp/credentials

・クライアント認証局のサブジェクト

使用するクライアント証明書のサブジェクト"O"は、「National Institute of Informatics」となります。
クライアント証明書のサブジェクト"O"をチェックする設定を行う箇所があるので、設定値を置き換えてください。

```
/etc/httpd/conf.d/ssl.conf

SSLRequire %{SSL_CLIENT_S_DN_O} eq "National Institute of Informatics"
```

なお、本メニューで使用するクライアント証明書のサブジェクトDNは以下のようなものです。CNがID(Username)と一致するのがポイントです。
CN = test001, OU = Cyber Science Infrastructure Development Department, O = National Institute of Informatics, L = Chiyoda-ku, ST = Tokyo, C = JP

---

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。

- 設定手順書

---

4. 動作確認

・クライアント証明書インストール

```
証明書認証の動作確認を行う為、使用するブラウザにクライアント証明書をインストールする必要があります。
以下の説明を参考に、実習セミナーで使用するブラウザ（Firefox）にインストールしてください。

・クライアント証明書
  クライアント証明書は、実習セミナー用DSサーバよりダウンロードしてください。
  https://ex-ds.gakunin.nii.ac.jp/client_shib.p12 (client_shib.p12)

・インストール
  以下の手順でインストールします。

  ① ブラウザ（Firefox）を起動します。
  ② メニューのツール内にあるオプション、または右上にある三本線のアイコンをクリックし
     中にあるオプションを選択します。
  ③ 右上の検索窓に「証明書」と入力します。
  ④ 下にある「証明書を表示...」ボタンをクリックします。
  ⑤ 証明書マネージャー画面が表示されるので、「あなたの証明書」タブを選択し「インポート（M）...」をクリックします。
  ⑥ 証明書の選択する画面が表示されるので、デスクトップ上にある「client_shib.p12」を
     選択し開くボタンをクリックします。
  ⑦ パスワードの入力を求められるので、「shibcert」と入力してOKボタンをクリックします。
```

① 設定後、ApacheやJettyの再起動を行ってない場合は行ってください。

```
systemctl restart httpd

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 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。

BACK TOP NEXT