2024年11月8日

クライアント証明書認証を使った認証﻿﻿

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

[**3. 設定手順 3**](#_heading=h.2et92p0)

[3.1 CA証明書の確認 3](#_heading=h.1bmk4rgqpm24)

[3.2 ssl.confの設定 4](#_heading=h.bebfmdtpvog3)

[3.3 /opt/shibboleth-idp/conf/authn/auth.propertiesの変更 6](#_heading=h.n2c7kn82d3ze)

[**4. 動作確認 7**](#_heading=h.tyjcwt)

[① クライアント証明書の取得とインストール 7](#_heading=h.5ga5v3rr0hov)

[② 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。 10](#_heading=h.qn2ouoz07qxn)

[③ 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。 10](#_heading=h.u7ap83z259ch)

[④ ログインボタンをクリックします。 11](#_heading=h.5foomub94q2m)

[⑤ 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。 11](#_heading=h.5waepf2avgoc)

[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。 11](#_heading=h.4owqlz5g90g)

[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。 11](#_heading=h.ymbm3hzdskv0)

# **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**

実習セミナーでは、予め用意した認証局のCA証明書とクライアント証明書を利用します。

* 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の設定  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. 設定手順**

以下の手順で設定を行ってください。

※実習セミナーでは、管理者ユーザー（root）で作業を行います。

## **3.1 CA証明書の確認**

CA証明書のサブジェクト"O"が「National Institute of Informatics」となっていることを確認して下さい。

|  |
| --- |
| $ openssl x509 -noout -text -in /opt/shibboleth-idp/credentials/cacert.pem Certificate:  Data:  Version: 3 (0x2)  Serial Number:  9c:98:69:6b:84:15:43:c6  Signature Algorithm: sha256WithRSAEncryption  Issuer: C=JP, ST=Tokyo, O=National Institute of Informatics, OU=Cyber Science Infrastructure Development Department, CN=GakuNin Private CA  Validity  Not Before: Nov 1 04:58:51 2018 GMT  Not After : Oct 29 04:58:51 2028 GMT　↓/etc/httpd/conf.d/ssl.confと合致していること  Subject: C=JP, ST=Tokyo, O=National Institute of Informatics, OU=Cyber Science Infrastructure Development Department, CN=GakuNin Private CA  Subject Public Key Info:  <以下省略> |

## **3.2 ssl.confの設定**

実習セミナーで用意している認証局のCA証明書の参照設定やクライアント証明書のサブジェクトを設定します。  
/etc/httpd/conf.d/ssl.confに次の赤字の部分を追記（挿入）します。

|  |
| --- |
| <省略>  <VirtualHost \_default\_:443>  # General setup for the virtual host, inherited from global configuration  #DocumentRoot "/var/www/html"  <省略>  ProxyPass /idp/ http://localhost:8080/idp/ connectiontimeout=5 timeout=15  <Location /idp/Authn/RemoteUser>  SSLVerifyClient require  SSLVerifyDepth 3  SSLRequireSSL  # SSLOptions +ExportCertData +StdEnvVars  SSLUserName SSL\_CLIENT\_S\_DN\_CN  SSLRequire %{SSL\_CLIENT\_S\_DN\_O} eq "**National Institute of Informatics**"  RequestHeader set REMOTE\_USER %{REMOTE\_USER}s  RewriteEngine On  RewriteCond %{SSL:REMOTE\_USER} =""  RewriteRule .\* - [E=REMOTEUSERNULL]  RequestHeader unset REMOTE\_USER env=REMOTEUSERNULL  </Location>  SSLCACertificateFile /opt/shibboleth-idp/credentials/cacert.pem  <省略>  #SSLProtocol all -SSLv3  #SSLProxyProtocol all -SSLv3 ← コメントアウトする  SSLProtocol all -SSLv3 -TLSv1.3 |

※ /etc/httpd/conf.d/ssl.confのSSLRequireディレクティブとして使えるものは以下の通りです。（参考まで）

|  |
| --- |
| クライアント証明書に含まれる情報やそれ以外のクライアント情報を判定し、認証を行うことができます。  よく使われるのが「SSL\_CLIENT\_S\_DN」による判定です。「SSL\_CLIENT\_S\_DN」はクライアント証明書名を示します。  SSL\_CLIENT\_S\_DN —————- 証明書 Subject  SSL\_CLIENT\_S\_DN\_C —————- 国名  SSL\_CLIENT\_S\_DN\_ST —————- 都道府県名  SSL\_CLIENT\_S\_DN\_L —————- 都市名  SSL\_CLIENT\_S\_DN\_O —————- 組織名  SSL\_CLIENT\_S\_DN\_OU —————- 部署名 |

※ また、TLSバージョンが1.3の場合に一部のパスに限定したクライアント証明書認証が機能しないため、TLSv1.3を使わないよう「-TLSv1.3」を含むSSLProtocolを追加しています。  
 ※ SSLVerifyClientがrequireのため問題ないはずだが、万が一証明書認証に失敗してもIdPに到達した場合REMOTE\_USERヘッダに"(null)"が入ってくるため、フェイルセーフとしてrewriteの条件を入れています。

## **3.3 /opt/shibboleth-idp/conf/authn/authn.propertiesの変更**

/opt/shibboleth-idp/conf/authn/authn.propertiesを以下のように設定します。

|  |
| --- |
| # Regular expression matching login flows to enable, e.g. IPAddress|Password  # idp.authn.flows = Password ← コメントアウト  idp.authn.flows = RemoteUser  <省略>  #### RemoteUser ####  <省略>  idp.authn.RemoteUser.checkHeadersをREMOTE\_USERに設定します。  # idp.authn.RemoteUser.checkHeaders = REMOTE\_USER ← コメントを外す  <省略>  # Most other settings need to be supplied via web.xml to the servlet  idp.authn.RemoteUser.supportedPrincipals = \  saml2/urn:oasis:names:tc:SAML:2.0:ac:classes:X509, \  saml2/urn:oasis:names:tc:SAML:2.0:ac:classes:TLSClient, \  saml1/urn:ietf:rfc:2246  <省略> |

※idp.authn.RemoteUser.checkHeadersは、ユーザー名（認証するアカウント）をチェックするリクエストヘッダーのカンマ区切りのリストです。

# **4. 動作確認**

## ① クライアント証明書の取得とインストール

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）にインストールします。

・クライアント証明書の取得

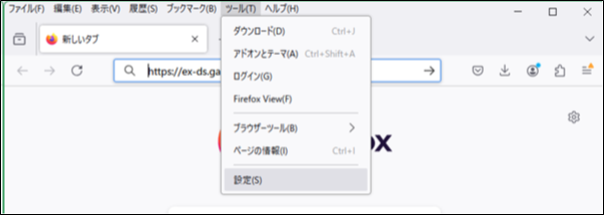
　クライアント証明書は、実習セミナー用DSサーバよりダウンロードしてください。

　https://ex-ds.gakunin.nii.ac.jp/client\_shib.p12（client\_shib.p12）

・クライアント証明書のブラウザへのインストール

　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「設定」、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「設定」を選択します。



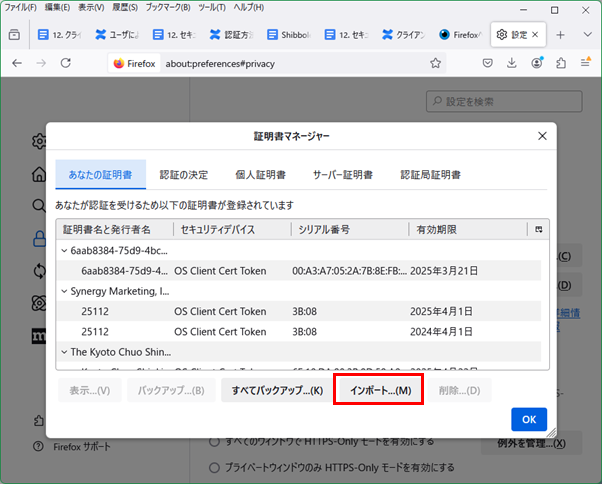
#### **図　Firefoxの設定画面を開く**

1. 設定画面の左メニュー「プライバシーとセキュリティ」を選び、右タブの「証明書を表示」ボタンをクリックします。



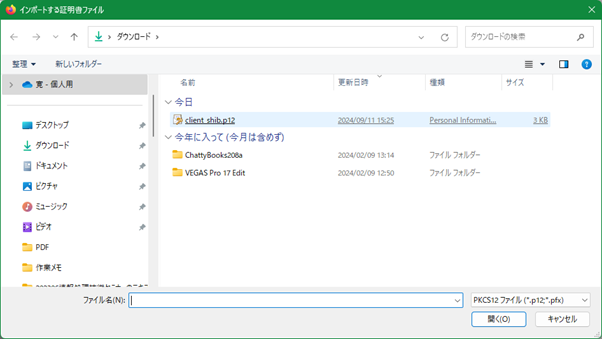
#### **図　「証明書を表示」をクリック**

1. 証明書マネージャーの「インポート」ボタンをクリックします。



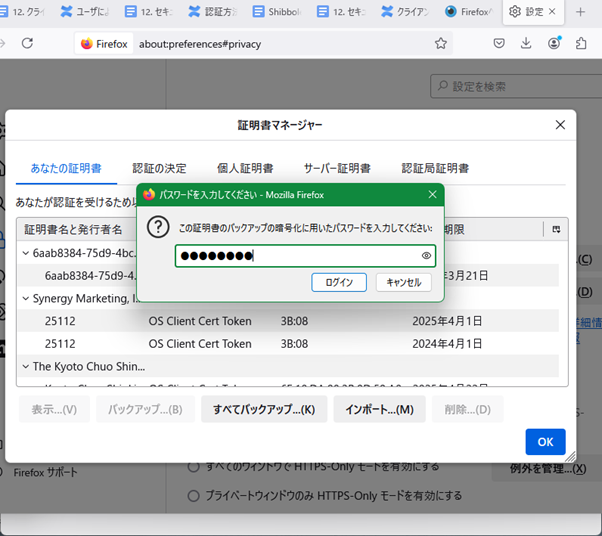
#### **図　証明書一覧表示画面**

1. 実習セミナー用DSサーバよりダウンロードした証明書ファイル（client\_shib.p12）を選択し、インポートします。



#### **図　インポートする証明書ファイルの選択**

1. 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。



#### **図　証明書のパスワード入力**

※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（共通名）がID(Username: test001)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 |

Firefoxの場合、インポートしたクライアント証明書を証明書マネージャーの「表示」ボタンで確認できます。



#### **図　クライアント証明書のDN確認**

## ② 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 |

## ③ 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）XX番を割り振られた場合  　https://ex-sp-testXX.gakunin.nii.ac.jp/ |

## ④ ログインボタンをクリックします。

## ⑤ 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。

## 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。

※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。