認証方法の変更、設定（証明書による認証）

認証方法の変更、設定（証明書による認証）

LDAPを利用したID/パスワード認証の他に、様々な認証方法を利用することが可能です。以下では、クライアント証明書を利用した認証の設定方法を示します。

この例では、

- クライアント証明書を発行するキャンパス認証局のCA証明書＝Camp-CA.crt
- クライアント証明書のサブジェクト”O”の値＝“Test_University_A”
- クライアント証明書のサブジェクト"CN"の値と一致するuidを持つLDAPエントリとして認証される

として設定を行い、クライアント証明書が有効な証明書であり、かつ、上記の条件を満たす場合に認証を行う設定としています。

こちらの手順は、RemoteUserを使いクライアント証明書での認証を行えるような設定となります。

・RemoteUserを有効にする

4.1.0以降では同意機能はモジュール化されており、利用するには有効化操作が必要です。以下のコマンドを実行してください。（当該モジュールがすでに有効化されているかを確認し、有効化されていない場合に有効化するものです）

```
# /opt/shibboleth-idp/bin/module.sh -t idp.authn.RemoteUser || /opt/shibboleth-idp/bin/module.sh -e idp.authn.RemoteUser
```

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

クライアント証明書を用いた認証のために authn.properties ファイルを変更します。

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

このままだとRemoteUserが証明書認証とみなされないので、以下の設定も加える。

```
#### RemoteUser ####
(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
```

・/etc/httpd/conf.d/ssl.confへの追加（赤文字の個所を追加）

※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の条件を入れている。

```
(省略)
<VirtualHost _default_:443>
(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 ”Test_University_A”
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) </VirtualHost>
```

・/opt/shibboleth-idp/edit-webapp/WEB-INF/web.xmlに対象ヘッダREMOTE_USERを追加

web.xmlに以下の内容を追加します。

```
(省略)

<!-- Servlet protected by container used for RemoteUser authentication -->
<servlet>
<servlet-name>RemoteUserAuthHandler</servlet-name>
<servlet-class>net.shibboleth.idp.authn.impl.RemoteUserAuthServlet</servlet-class>
<init-param>
<param-name>checkHeaders</param-name>
<param-value>REMOTE_USER</param-value>
</init-param>
<load-on-startup>2</load-on-startup>
</servlet>
<servlet-mapping>
<servlet-name>RemoteUserAuthHandler</servlet-name>
<url-pattern>/Authn/RemoteUser</url-pattern>
</servlet-mapping>

(省略)
```

以下を実行して、反映させます。

```
# /opt/shibboleth-idp/bin/build.sh
```

またApacheとJettyも再起動します。

```
# systemctl restart httpd

# systemctl restart jetty
```

複数の認証手段を使う場合

複数の認証手段を使うのでなければ以上で完了です。

複数の認証手段（ログインフロー）を使う（冒頭のidp.authn.flowsに Password|X509 のように複数記述する）場合で、デフォルトのログインフロー（SPからの認証要求時に認証手段についての指定がない場合に遷移するログインフロー）を指定したい場合には、4.1以降の場合は、各ログインフロー idp.authn.*.order プロパティを調整してください。数字を指定し、小さいものが高優先度となります。
4.0.xおよびそれ以前の場合は、conf/authn/general-authn.xmlのbeanの順序を変更してください。上にあるものが優先的に選択されます。例えば3.4.0の初期設定では authn/X509 のbeanが authn/Password のbeanより上にあるため、証明書認証が優先されます。

さらに、一部の条件で（例えば特定のSPに対して）証明書認証以外を利用させたくない場合は、relying-party.xmlのshibboleth.RelyingPartyOverrides設定で p:authenticationFlows="#{{'X509'}}" のように利用可能な認証手段を指定してください。

トラブルシューティング

Tomcatを使っている場合で、Apacheではクライアント証明書が認識されているがその情報がTomcatに伝わっていない場合、/usr/share/tomcat/conf/server.xmlの8009番ポートConnectorにtomcatAuthentication="false"が設定されていることを確認してください。
参考: jdk 8、tomcat 7をインストールする

参考

IdPv3の証明書認証の詳細: Shibboleth Wiki: X509AuthnConfiguration