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。

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

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

```
(省略)

    # Regular expression matching login flows to enable, e.g. IPAddress|Password
    idp.authn.flows= X509

(省略)
```

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

```
(省略)
<VirtualHost _default_:443>
(省略)
ProxyPass /idp ajp://localhost:8009/idp
<Location /idp/Authn/X509>
  SSLCACertificateFile /opt/shibboleth-idp/credentials/Camp-CA.crt
  SSLVerifyClient require
  SSLVerifyDepth 3
  SSLRequireSSL
  SSLOptions +ExportCertData +StdEnvVars
  SSLUserName SSL_CLIENT_S_DN_CN
  SSLRequire %{SSL_CLIENT_S_DN_O} eq "Test_University_A"
</Location>
(省略)
</VirtualHost>
```

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

LDAP から属性を取得する際のキーとなる属性はデフォルトでは uid ですが変更したい場合は下記の場所を変更します。

```
(省略)
idp.attribute.resolver.LDAP.trustCertificates   = %{idp.authn.LDAP.trustCertificates:undefined}
idp.attribute.resolver.LDAP.searchFilter        = (uid=$resolutionContext.principal) ←必要に応じて変更
idp.attribute.resolver.LDAP.returnAttributes    = cn,homephone,mail
(省略)
```

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、デフォルトの認証手段（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認証手段）を指定したい場合には、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、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

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