サーバ証明書の設定(IdP)

サーバ証明書の取得とApacheの設定（★）

１．「UPKIオープンドメイン証明書自動発行検証プロジェクト」の利用の手引における加入者編をご覧いただき、サーバ証明書を申請します。機関の審査手続きによっては証明書の交付までには数日を要する場合がありますので、お早めに申請してください。
接続実験をするだけであれば、IdPインストール時に作成された証明書（自己署名証明書）をそのまま利用してテストフェデレーションに参加することも可能です。その場合は、以降の記述のうち「中間CA証明書」の部分は無視してください。

実習セミナー

・証明書は、初期設定で「/root/GETFILE」に取得したファイルを使用します。
サーバ証明書：**server.crt**
秘密鍵：**server.key**
中間CA証明書：**server-chain.crt**

上記ファイルを使用して、以降の設定（ssl.conf、relying-party.xml）を行ってください。

２．入手したサーバ証明書をもとに、以下のファイルに設定してください。（★）

■/etc/httpd/conf.d/ssl.conf（★）

実習セミナー

・各証明書と秘密鍵を「/root/GETFILE」配下よりコピーしてください。
 # cp /root/GETFILE/server{,-chain}.crt /etc/pki/tls/certs/
 # cp /root/GETFILE/server.key /etc/pki/tls/private/

/etc/httpd/conf.d/ssl.conf を以下のように編集してください。（★）

```
（省略）
SSLCertificateFile /etc/pki/tls/certs/server.crt            ← サーバ証明書の格納先
（省略）
SSLCertificateKeyFile /etc/pki/tls/private/server.key       ← 秘密鍵の格納先
（省略）
SSLCertificateChainFile /etc/pki/tls/certs/server-chain.crt ← 中間CA証明書の格納先
↑ 先頭の「#」を削除して、コメントを解除してください。
```

※端末のサイズによっては表記がずれる可能性がございます。画面を広くしてご覧ください。

詳しくは、サーバ証明書インストールマニュアルの Apache 2 + mod_ssl 編を参照してください。

■/opt/shibboleth-idp/conf/relying-party.xml（★）

参照先ディレクトリ（/opt/shibboleth-idp/credentials）に、サーバ証明書と秘密鍵をコピーしてください。（★）

実習セミナー

・サーバ証明書と秘密鍵を「/root/GETFILE」配下よりコピーしてください。
 # cp /root/GETFILE/server.crt /opt/shibboleth-idp/credentials/
 # cp /root/GETFILE/server.key /opt/shibboleth-idp/credentials/

/opt/shibboleth-idp/conf/relying-party.xml を以下のように編集してください。（★）

```
（省略）
<security:Credential id="IdPCredential" xsi:type="security:X509Filesystem">
    <security:PrivateKey>/opt/shibboleth-idp/credentials/server.key</security:PrivateKey>
                                ↑ ssl.confと同一のものを上記のパスにも格納
    <security:Certificate>/opt/shibboleth-idp/credentials/server.crt</security:Certificate>
                                ↑ ssl.confと同一のものを上記のパスにも格納
</security:Credential>
（省略）
```

※端末のサイズによっては表記がずれる可能性がございます。画面を広くしてご覧ください。

メタデータの作成と提出（★）

実習セミナー

・メタデータテンプレートは、初期設定で「/root/GETFILE」に取得したidp-metadata.xmlを使用します。rootのホームディレクトリに「"ドメインなしホスト名".xml」のファイル名でコピーします。
例）1番を割り振られた場合
ホスト名：ex-idp-test01.gakunin.nii.ac.jpとなり、ファイル名：ex-idp-test01.xmlです。
以下のコマンドでファイルをコピーします。
cp /root/GETFILE/idp-metadata.xml /root/ex-idp-test01.xml

コピー後、IdPメタデータテンプレートを参考に**必要な項目を変更**します。
（証明書部分には、/opt/shibboleth-idp/credentials/server.crtの内容を使用します。）

学認申請システム（テストFed）から登録を行います。入力したデータから自動的にメタデータが生成されますのでメタデータ作成の必要はありません。詳細は参加のページをご覧ください。
⇒参加
学認申請システムから登録を行います。入力したデータから自動的にメタデータが生成されますのでメタデータ作成の必要はありません。詳細は参加のページをご覧ください。
⇒参加

実習セミナー

・作成したメタデータは**学認申請システムではなく、実習セミナー内のDSサーバに転送**します。
以下は、転送コマンドの例です。
メタデータファイル名を各自のファイル名に変更して実行してください。
例）ホスト名：ex-idp-test01.gakunin.nii.ac.jpの場合
scp /root/ex-idp-test01.xml test@ex-ds.gakunin.nii.ac.jp:METADATA

転送したメタデータは、1分周期で他のメタデータとマージ処理を行い、実習セミナー内のフェデレーションメタデータが更新されます。
※1分周期で行う為、最大約1分登録までに時間がかかります。

Back-Channelの設定

Shib1.3のSPにも接続する場合は、IdPとの通信時にTLS接続を行うため、下記にしたがいBack-Channelの設定を行ってください。 このTLS接続ではポート8443を利用します。

実習セミナー

・実習セミナーではShibboleth SPバージョン1.3は対象としていないため以下の設定は不要です。

1．キーストアの設定

サーバ証明書を格納したキーストアを作成します。

```
# cd /opt/shibboleth-idp/credentials
# openssl pkcs12 -export -out pkcs12.p12 -in サーバ証明書.crt -inkey サーバ秘密鍵.key -name サーバ名
 （ここで聞かれるエクスポートパスワードにはキーストアパスワードと同じものを指定してください）
# keytool -importkeystore -srckeystore pkcs12.p12 -destkeystore keystore.jks ¥
 -srcstoretype pkcs12 -deststoretype jks -srcalias サーバ名 -destalias サーバ名 ¥
 -storepass キーストアパスワード
# rm pkcs12.p12
# chmod 600 /opt/shibboleth-idp/credentials/keystore.jks
```

Tomcatを"tomcat"ユーザで実行する場合は、さらに以下のコマンドを実行しTomcatが読み取れるようにします。

```
# chgrp tomcat /opt/shibboleth-idp/credentials/keystore.jks
# chmod g+r /opt/shibboleth-idp/credentials/keystore.jks
```

2．ライブラリのコピー

https://build.shibboleth.net/nexus/content/repositories/releases/edu/internet2/middleware/security/tomcat6/tomcat6-dta-ssl/2.0.0/tomcat6-dta-ssl-2.0.0.jarよりダウンロードします。
tomcat6-dta-ssl-2.0.0.jarを$CATALINA_HOME/lib配下にコピーします。

```
# wget https://build.shibboleth.net/nexus/content/repositories/releases/edu/internet2/middleware/security/tomcat6/tomcat6-dta-ssl/2.0.0/tomcat6-dta-ssl-2.0.0.jar
# cp tomcat6-dta-ssl-2.0.0.jar $CATALINA_HOME/lib
```

ダウンロードされるJARファイルのSHA-256ハッシュ値は以下の通りです。さらに真正性を確認したい場合はPGP署名をご利用ください。

```
# sha256sum tomcat6-dta-ssl-2.0.0.jar
d7b0cf2ebcad28bb5037b2c35891e8d8fa0a0f853f61d51039776d6261111535  tomcat6-dta-ssl-2.0.0.jar
```

この手順は古いものです。特に理由がなければ上記のtomcat6-dta-ssl-*.jarを使用してください。

```
# cp /opt/shibboleth-idp/lib/shibboleth-jce-1.1.0.jar $JAVA_HOME/jre/lib/ext
```

※ 2.3.4以降には当該ファイルが同梱されていません。⇒情報交換ML:00414, 情報交換ML:00513

さらに、 $JAVA_HOME/jre/lib/security/java.security ファイルに以下を追加します。

```
#
# List of providers and their preference orders (see above):
#
security.provider.1=sun.security.provider.Sun
 （省略）
security.provider.7=org.jcp.xml.dsig.internal.dom.XMLDSigRI
security.provider.8=sun.security.smartcardio.SunPCSC
security.provider.9=edu.internet2.middleware.shibboleth.DelegateToApplicationProvider
  ↑ 行を追加
```

番号:9 は、既に記載されている番号に合わせて順番にして下さい。
（9が既に記載されている場合は、10に修正して行を追加）

3．SOAP設定

$CATALINA_BASE/conf/server.xml ファイルに以下を追加します。

```
<Connector port="8443"
           protocol="org.apache.coyote.http11.Http11Protocol"
           SSLImplementation="edu.internet2.middleware.security.tomcat6.DelegateToApplicationJSSEImplementation"
           scheme="https"
           maxPostSize="100000"
           SSLEnabled="true"
           clientAuth="want"
           sslProtocols="TLSv1,TLSv1.1,TLSv1.2"
           sslEnabledProtocols="TLSv1,TLSv1.1,TLSv1.2"
           keystoreFile="/opt/shibboleth-idp/credentials/keystore.jks"
           keystorePass="キーストアパスワード" />
```

sslProtocols と sslEnabledProtocols はどちらもSSLv3を無効にするための記述です。Tomcatのバージョンによって参照されるものが異なります。マイナーバージョンにも影響を受けるため、安全のため両方を記載しています。なお、TLSv1.1とTLSv1.2の記載がありますが、実際に使用できるか否かはJava(JVM)のバージョンに依存します。

```
<Connector port="8443"
           maxHttpHeaderSize="8192"
           maxSpareThreads="75"
           scheme="https"
           secure="true"
           clientAuth="want"
           SSLEnabled="true"
           sslProtocol="TLS"
           sslProtocols="TLSv1,TLSv1.1,TLSv1.2"
           sslEnabledProtocols="TLSv1,TLSv1.1,TLSv1.2"
           keystoreFile="/opt/shibboleth-idp/credentials/keystore.jks"
           keystorePass="キーストアパスワード"
           truststoreFile="/opt/shibboleth-idp/credentials/keystore.jks"
           truststorePass="キーストアパスワード"
           truststoreAlgorithm="DelegateToApplication"/>
```

BACK TOP NEXT