サーバ証明書の設定(IdPv4)

サーバ証明書の取得とApacheの設定

１．「UPKI電子証明書発行サービス」の利用管理者編をご覧いただき、サーバ証明書発行を申請します。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。

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

まず、秘密鍵を"root"ユーザのみが参照できるようにアクセス制限がかかっているか確認してください。確認できない場合は以下のようにして所有者・グループ・パーミッションを設定してください。

```
chown root:root /etc/pki/tls/private/server.key       ← 秘密鍵の格納先
chmod 400 /etc/pki/tls/private/server.key
```

/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。

メタデータの作成と提出

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

Back-Channelの設定

SAML 1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。

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
# UMASKORIG="`umask`" ; umask 0077
# openssl pkcs12 -export -out server.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を後述のidp-backchannel.iniの「P12パスワード」に指定します。任意のものを設定できます）
# umask "$UMASKORIG"
（上記一連のumaskコマンドは"chmod 600 server.p12"と同義）
```

Jettyを"jetty"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Jettyが読み取れるようにします。

```
# chgrp jetty /opt/shibboleth-idp/credentials/server.p12
# chmod g+r /opt/shibboleth-idp/credentials/server.p12
```

２．ライブラリのコピー

https://build.shibboleth.net/nexus/content/repositories/releases/net/shibboleth/utilities/jetty9/jetty94-dta-ssl/1.0.0/jetty94-dta-ssl-1.0.0.jar よりダウンロードします。
jetty94-dta-ssl-1.0.0.jar を /opt/jetty-base/lib/ext 配下にコピーします。

```
# wget https://build.shibboleth.net/nexus/content/repositories/releases/net/shibboleth/utilities/jetty9/jetty94-dta-ssl/1.0.0/jetty94-dta-ssl-1.0.0.jar
# cp jetty94-dta-ssl-1.0.0.jar /opt/jetty-base/lib/ext
```

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 jetty94-dta-ssl-1.0.0.jar
5e5de66e3517d30ff19ef66cf7a4aa5443b861d83e36a75e85845b007a03afbf  jetty94-dta-ssl-1.0.0.jar
```

なお、配置したファイルはデフォルトでは使用されません。すでに /opt/jetty-base/lib/ext 配下に存在する jetty9-dta-ssl-1.0.0.jar が使用されます。併存していても問題ありません。もしデフォルトの設定で問題がある場合は（一部の証明書で問題になるという情報があります）、etc/idp-backchannel.xml の以下の部分を修正し新しいライブラリを使用するようにしてください。

```
@@ -6,7 +6,7 @@
   <!-- and no container trust (delegate to application)             -->
   <!-- for backchannel (SOAP) communication to IdP                  -->
   <!-- ============================================================= -->
-  <New id="shibContextFactory" class="net.shibboleth.utilities.jetty9.DelegateToApplicationSslContextFactory">
+  <New id="shibContextFactory" class="net.shibboleth.utilities.jetty94.DelegateToApplicationSslContextFactory">
     <Set name="KeyStorePath"><Property name="idp.backchannel.keyStorePath" default="../credentials/idp-backchannel.p12" /></Set>
     <Set name="KeyStoreType"><Property name="idp.backchannel.keyStoreType" default="PKCS12" /></Set>
     <Set name="KeyStorePassword"><Property name="idp.backchannel.keyStorePassword" default="changeit" /></Set>
```

３．SOAP設定

/opt/jetty-base/start.d/idp-backchannel.ini ファイルを以下のように作成します。

```
# cd /opt/jetty-base/start.d
# cp idp-backchannel.ini.dist idp-backchannel.ini
# chgrp jetty idp-backchannel.ini
# chmod 640 idp-backchannel.ini
```

/opt/jetty-base/start.d/idp-backchannel.ini ファイルを以下のように修正します。

```
# ----------------------------------------
# Module: idp-backchannel
# Shibboleth IdP Dedicated SOAP Connector
# ----------------------------------------
--module=idp-backchannel

## Backchannel connector port to listen on
#idp.backchannel.port=8443
↑コメントアウト（#）を削除。以下同様
## Backchannel keystore file path (relative to $jetty.base)
#idp.backchannel.keyStorePath=../shibboleth-idp/credentials/server.p12

## Backchannel keystore password
#idp.backchannel.keyStorePassword=P12パスワード

## Backchannel keystore type
#idp.backchannel.keyStoreType=PKCS12
```

/opt/jetty-base/etc/idp-backchannel.xml ファイルを以下のように修正します。

```
（省略）

  <New id="shibHttpConfig" class="org.eclipse.jetty.server.HttpConfiguration">
    <Arg><Ref refid="httpConfig"/></Arg>
↑上の行を削除し↓で置き換え
    <Set name="secureScheme"><Property name="jetty.httpConfig.secureScheme" default="https" /></Set>
    <Set name="securePort"><Property name="jetty.httpConfig.securePort" deprecated="jetty.secure.port" default="8443" /></Set>
    <Set name="outputBufferSize"><Property name="jetty.httpConfig.outputBufferSize" deprecated="jetty.output.buffer.size" default="
32768" /></Set>
    <Set name="outputAggregationSize"><Property name="jetty.httpConfig.outputAggregationSize" deprecated="jetty.output.aggregation.
size" default="8192" /></Set>
    <Set name="requestHeaderSize"><Property name="jetty.httpConfig.requestHeaderSize" deprecated="jetty.request.header.size" default="
8192" /></Set>
    <Set name="responseHeaderSize"><Property name="jetty.httpConfig.responseHeaderSize" deprecated="jetty.response.header.size"
default="8192" /></Set>
    <Set name="sendServerVersion"><Property name="jetty.httpConfig.sendServerVersion" deprecated="jetty.send.server.version" default="
true" /></Set>
    <Set name="sendDateHeader"><Property name="jetty.httpConfig.sendDateHeader" deprecated="jetty.send.date.header" default="false"
/></Set>
    <Set name="headerCacheSize"><Property name="jetty.httpConfig.headerCacheSize" default="1024" /></Set>
    <Set name="delayDispatchUntilContent"><Property name="jetty.httpConfig.delayDispatchUntilContent" deprecated="jetty.
delayDispatchUntilContent" default="true"/></Set>
    <Set name="maxErrorDispatches"><Property name="jetty.httpConfig.maxErrorDispatches" default="10"/></Set>
    <Set name="blockingTimeout"><Property deprecated="jetty.httpConfig.blockingTimeout" name="jetty.httpConfig.blockingTimeout.
DEPRECATED" default="-1"/></Set>
    <Set name="persistentConnectionsEnabled"><Property name="jetty.httpConfig.persistentConnectionsEnabled" default="true"/></Set>
    <Set name="requestCookieCompliance"><Call class="org.eclipse.jetty.http.CookieCompliance" name="valueOf"><Arg><Property name="
jetty.httpConfig.requestCookieCompliance" deprecated="jetty.httpConfig.cookieCompliance" default="RFC6265"/></Arg></Call></Set>
    <Set name="responseCookieCompliance"><Call class="org.eclipse.jetty.http.CookieCompliance" name="valueOf"><Arg><Property name="
jetty.httpConfig.responseCookieCompliance" default="RFC6265"/></Arg></Call></Set>
    <Set name="multiPartFormDataCompliance"><Call class="org.eclipse.jetty.server.MultiPartFormDataCompliance" name="valueOf"
><Arg><Property name="jetty.httpConfig.multiPartFormDataCompliance" default="RFC7578"/></Arg></Call></Set>
    <Set name="relativeRedirectAllowed"><Property name="jetty.httpConfig.relativeRedirectAllowed" default="false"/></Set>
    <Call name="addCustomizer">
      <Arg>
（省略）
```

<Arg><Ref refid="httpConfig"/></Arg> の部分を削除していることによりhttp-forwardedモジュールの他rewriteモジュールの設定がBack-Channelに反映されない可能性がありますのでご注意ください。Back-Channelに対するこれらのモジュールの使用は避けてください。

４．有効化

/opt/shibboleth-idp/conf/relying-party.xml ファイルを以下のように修正します。

以下ではSAML 1.x自体の有効化（デフォルトでは無効）も行っておりますが、SAML 2.0 Attribute Queryのみ必要な場合は前半のコメント解除は不要です。

```
<bean id="shibboleth.DefaultRelyingParty" parent="RelyingParty">
<property name="profileConfigurations">
<list>
<!-- SAML 1.1 and SAML 2.0 AttributeQuery are disabled by default. -->
<!-- -->  ←  コメントを解除
<bean parent="Shibboleth.SSO" p:postAuthenticationFlows="attribute-release" />
<ref bean="SAML1.AttributeQuery" />
<ref bean="SAML1.ArtifactResolution" />
<!-- -->  ←  コメントを解除
<bean parent="SAML2.SSO" p:postAuthenticationFlows="attribute-release" />
<ref bean="SAML2.ECP" />
<ref bean="SAML2.Logout" />
<!-- -->  ←  コメントを解除
<ref bean="SAML2.AttributeQuery" />
<!-- -->  ←  コメントを解除
<ref bean="SAML2.ArtifactResolution" />
<ref bean="Liberty.SSOS" />
</list>
</property>
</bean>
```

設定変更後は、Jettyの再起動を行います。

```
# systemctl restart jetty
```