サーバ証明書の設定(SP)

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。
所属機関が対象外等の理由で上記証明書サービスから証明書を入手できない場合、商用のパブリックな証明書でも代用可能な場合があります。

> 基本的に主要なブラウザ(Firefox, Google Chrome, Safari等)で検証できる証明書であればご利用になれます。詳細は学認技術運用基準の7.4)をご確認ください。
>
> ただし、Let's Encryptのような有効期限が1年未満の証明書は更新頻度が高くなり、学認への変更申請を含む証明書更新作業の手間が増えるため、現状おすすめしておりません。

> 接続実験をするだけであれば、**SP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、以降の記述にある ssl.conf および shibboleth2.xml の修正は不要です。なお、その場合にSPで使用されるサーバ証明書および秘密鍵は以下のファイルと対応します。中間CA証明書は不要です。
>
> - サーバ証明書(server.crt) → /etc/shibboleth/sp-cert.pem
> - 秘密鍵(server.key) → /etc/shibboleth/sp-key.pem
> - 中間CA証明書(server-chain.crt) → 不要

２．入手したサーバ証明書を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。
```

ssl.conf設定後、httpdを再起動します。

```
# systemctl restart httpd
```

```
# service httpd restart
```

設定について詳しくは、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。

■/etc/shibboleth/shibboleth2.xml

「/etc/shibboleth/cert」配下に、サーバ証明書と秘密鍵をコピーしてください。

/etc/shibboleth/shibboleth2.xml を以下のように編集してください。

```
（省略）
        <!-- Simple file-based resolvers for separate signing/encryption keys. -->
        <CredentialResolver type="File" use="signing"
            key="cert/server.key" certificate="cert/server.crt"/>
                    ↑秘密鍵の格納先                    ↑サーバ証明書の格納先
        <CredentialResolver type="File" use="encryption"
            key="cert/server.key" certificate="cert/server.crt"/>
                    ↑秘密鍵の格納先                    ↑サーバ証明書の格納先
```

※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。

/etc/shibboleth/cert/server.key はユーザshibdによって読み取れる必要があります。Shibboleth SPのデフォルト設定である以下を参考にパーミッションを限定してください。

```
# chown shibd:shibd /etc/shibboleth/cert/server.key
# chmod 440 /etc/shibboleth/cert/server.key
```

メタデータの作成と提出

テストフェデレーション用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
運用フェデレーション用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