SP Key Rollover

メタデータ記載の証明書更新手順（SP）

SPの証明書更新手順:

サーバ証明書の有効期限が切れる場合の新しい証明書への切り替え手順をご紹介します。ポイントは、メタデータ上の記載変更とIdP/SPの設定変更の間にタイムラグを置いて、メタデータ伝播中にもIdP/SPが利用できない期間が発生しないようにしているところです。本手順の記述は学認ウェブサイトの技術ガイドに従って構築した場合の記述です。そうでない場合は適宜読み替えてください。

証明書の設定について

証明書については、多くの場合そして多くの時間Webサーバ(Apache)およびShibboleth SPの双方で同じものを使用することになります。ただし本手順のようにごく短期間別のものを使用する必要がありますのでそれぞれ必要な場所に証明書ファイルと秘密鍵をコピーしてください。

万が一同じ証明書・鍵ファイルをApacheおよびShibboleth SPで参照している場合はコピーしてから本手順を始めてください。そうでなければApacheの証明書更新のつもりがShibboleth SPの証明書も更新することになり、認証連携エラーを引き起こす原因となります。

それぞれの設定ファイルおよび本手順で想定しているパスを示します：

- Apache
  - 設定が記述されているファイル: /etc/httpd/conf.d/ssl.conf
  - 証明書ファイルパス: /etc/pki/tls/certs/server.crt
  - 秘密鍵ファイルパス: /etc/pki/tls/private/server.key
- Shibboleth SP
  - 設定が記述されているファイル: /etc/shibboleth/shibboleth2.xml
  - 証明書ファイルパス: /etc/shibboleth/cert/server.crt
  - 秘密鍵ファイルパス: /etc/shibboleth/cert/server.key

テンプレート外メタデータをお使いの場合、特に use="signing" / use="encryption" を指定している場合は学認申請システムのフォームでの証明書追加・更新では期待する状態にならない場合がございます。お手数ですがアップロードいただいたメタデータを手で編集いただき、再度アップロードしてください。

1日目　更新用証明書発行
鍵およびCSR生成、申請、証明書受領
（詳細は各機関の登録担当者に確認のこと）
＜証明書取得＞
1日目　Apacheに対して証明書の更新（※1）
1日目　SPに対して設定変更1（新証明書を暗号化用として追加）（※2）
1日目　学認申請システムにて証明書を追加（予備の欄に）
＜承認待ち＞
X日目　承認、学認メタデータに反映
（ほとんどの場合数日のうちに承認されますが、そうでない場合
を考慮してX日目としています）
＜メタデータに追加＞
＜メタデータ伝播待ち＞
X+15日目　SPに対して設定変更2（新証明書をメインにし旧証明書を暗号化用に変更）（※3）
X+15日目　問題がなければ、学認申請システムから古い証明書を削除
（ついでに、新しい証明書を予備の欄から移動）
＜承認待ち＞
Y日目　承認、学認メタデータに反映
（同上）
＜メタデータから旧証明書を削除＞
＜メタデータ伝播待ち＞
Y+15日目　SPに対して設定変更3（旧証明書削除）（※4）

※1「Apacheに対して証明書の更新」の手順

1. /etc/pki/tls/private/server.key
   /etc/pki/tls/certs/server.crt
   を新証明書のもので上書きする
   参考: サーバ証明書の設定(SP)
2. httpdを再読み込み(reload)する

※2 SP設定変更1

1. /etc/shibboleth/cert/new.key
   /etc/shibboleth/cert/new.crt
   に新証明書および鍵を配置する（この段階では旧証明書を上書きしないこと！）
   new.keyのパーミッションについては、shibdからアクセスできるように注意すること(例えばCentOSではowner:groupが shibd:shibd でパーミッションが r--r----- とすればOK)。
2. 以下、全て/etc/shibboleth/shibboleth2.xmlに対する変更である。
   --
   <CredentialResolver type="File" key="cert/server.key" certificate="cert/server.crt"/>
   --
   ↓
   --
   <CredentialResolver type="Chaining">
   <CredentialResolver type="File" key="cert/server.key" certificate="cert/server.crt"/>
   <CredentialResolver type="File" key="cert/new.key" certificate="cert/new.crt" use="encryption"/>
   </CredentialResolver>
   --
3. 変更後shibdを再起動しhttpdを再読み込みする

```
$ sudo /sbin/service shibd restart
$ sudo /sbin/service httpd reload
```

※3 SP設定変更2
（同じ部分の変更につき変更後のみ記載）
--
<CredentialResolver type="Chaining">
<CredentialResolver type="File" key="cert/server.key" certificate="cert/server.crt" use="encryption"/>
<CredentialResolver type="File" key="cert/new.key" certificate="cert/new.crt"/>
</CredentialResolver>
--
変更後shibdの再起動とhttpdの再読み込みを行うこと

```
$ sudo /sbin/service shibd restart
$ sudo /sbin/service httpd reload
```

※4 SP設定変更3
（同じ部分の変更につき変更後のみ記載）
--
<CredentialResolver type="File" key="cert/server.key" certificate="cert/server.crt"/>
--
このように戻した上で、
/etc/shibboleth/cert/server.key
/etc/shibboleth/cert/server.crt
を新証明書および鍵で上書きする
最後にshibdの再起動とhttpdの再読み込みを行うこと

```
$ sudo /sbin/service shibd restart
$ sudo /sbin/service httpd reload
```

※IdPとSPで更新手順が異なる理由について
　SPの証明書は暗号化にも使用されるため、上記のように複雑な手順になります。

※ メタデータ伝播待ちの期間は学認技術運用基準(validUntil)で規定される最大マージンを取ったものです。各IdPでは1日1回は更新することが推奨されておりますので、伝播待ち期間を1日2日短縮しても通常は問題になることはありません。