IdP Key Rollover

メタデータ記載の証明書更新手順（IdP）

※ SPのメタデータ記載証明書更新の手順については次のページをご参照ください。
⇒メタデータ記載の証明書更新手順（SP）

目次：

- IdPの証明書更新手順:
  - ※1「Apacheに対して証明書の更新」の手順
  - ※2「IdPに対して証明書の更新」の手順
  - ※3 「server.p12を更新」の手順
  - ※4 attrviewer13でSAML1のテストについて
  - ※ メタデータ伝播待ちの期間について

IdP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。以下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。

この手順を始める際にすでに学認申請システム上で予備の証明書が登録されている場合は、必ず現在IdPがどちらの証明書を使う設定になっているか確認してください。idp.propertiesに記載されているファイル（通常server.crtおよびserver.key）を確認すればよいです。

確認できましたら下記「学認申請システムにて証明書を追加（予備の欄に）」の手順では、入力する場所によらず、またどちらの証明書が新しいか／古いかによらず、IdPで使う設定になっている証明書を残し、使う設定になっていない証明書の欄のほうを上書きして新しい証明書を登録するようにしてください。

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 IdP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 IdP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 IdP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 IdP
  - 設定が記述されているファイル: /opt/shibboleth-idp/conf/idp.properties
  - 証明書ファイルパス: /opt/shibboleth-idp/credentials/server.crt
  - 秘密鍵ファイルパス: /opt/shibboleth-idp/credentials/server.key

SpringerLinkと連携している場合、IdPが有効期限切れの証明書をアサーションの署名に使っているとエラーになることが確認されていますので、証明書の有効期限内にメタデータ記載の証明書更新手順(IdP)の手順に従って証明書を更新するようご注意ください。
⇒SpringerLinkに関する情報

サーバ証明書の有効期限については、Apacheに対して設定する証明書については有効期限切れにならないようご注意ください。

加えて上記SpringerLinkのほか、WebExやBoxなど学認参加SP以外のSPにてメタデータ記載証明書の有効期限がチェックされる例がみられるようです。「X+15日目」が有効期限を越える場合は、これを伝播期間も考慮した上で短縮し「IdPに対して証明書の更新」が有効期限を越えないようにご注意ください。有効期限をチェックするSPについて学認で認識しているものは以下にまとめております。有益な情報等ありましたら事務局までお知らせください。
⇒個々のソフトウェア／サービスのシボレス対応状況

この証明書を暗号化にも使用している場合にはこの手順の限りではありません。特殊なSPと連携していてIdPへ送信されるデータを暗号化していることが確かな場合には、下記手順を修正してSPと同様の手順を取り、IdPへの証明書追加設定については `conf/credentials.xml` のコメントを参照してしかるべき変更を行ってください。

例えば、（Shibboleth SPからのSP-initiatedな）Single Logout (SLO)を使っている場合、NameIDが暗号化される場合があるようですので、上記のような対応を行う必要があります。

⚠ 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　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
＜公開されているメタデータに新証明書が追加される＞
＜メタデータ伝播待ち＞
X+15日目　attrviewer13でSAML1のテスト（運用フェデレーションに参加している場合）（※4）
X+15日目　IdPに対して証明書の更新（※2）
X+15日目　再びattrviewer13でSAML1のテスト（運用フェデレーションに参加している場合）（※4）
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
＜公開されているメタデータから旧証明書が削除される＞
＜attrviewer13へのメタデータ伝播待ち＞
Y+1日目　最後にattrviewer13でSAML1のテスト（運用フェデレーションに参加している場合）（※4）

ⓘ **「X日目」「Y日目」について：**

人手によるチェックを挟むため、変更申請から承認までには数日を要します。1回目の変更申請の承認日をX日目、2回目の変更申請の承認日をY日目と表現しています。X≧1, Y≧X+15 です。

要する日数は、繁忙期か閑散期かにもよりますが、2営業日～1週間を目安にしていただければと思います。

※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(IdPv4)
2. httpdを再起動する

※2「IdPに対して証明書の更新」の手順

1. /opt/shibboleth-idp/credentials/server.key
   /opt/shibboleth-idp/credentials/server.crt
   を新証明書のもので上書きする
   参考: idp.properties ファイルの変更
   ※Jettyプロセスからserver.keyが読み取れるよう、パーミッションにはご注意ください
2. /opt/shibboleth-idp/credentials/server.p12
   を更新する（※3）
   ※同様にserver.p12のパーミッションにはご注意ください
3. Jettyを再起動する

※3 「server.p12を更新」の手順

サーバ証明書の設定(IdPv4)
の「Back-Channelの設定」の「１．キーストアの設定」にある手順のうち、最後の2つを実行して、
サーバ証明書の部分を更新します。具体的には以下のような手順になります。

```
# cd /opt/shibboleth-idp/credentials
# 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はidp-backchannel.iniに指定した「P12パスワード」を入力してください。もしくは任意のものを設定し、idp-backchannel.iniを修正してください。）
```

エラーが表示されなければserver.p12は更新されました。

※4 attrviewer13でSAML1のテストについて

運用フェデレーションに参加している場合は、attrviewer13でSAML1のテストを行なうことを推奨します。（テストの際には事前にattrviewer13に属性送信する設定にしておいてください）
計3回テストを挿入していますが、前2回は更新前に正常な動作をしているかを確認するためのもので、万一更新作業に失敗していてもテストは成功する可能性があります。
通常のSPには属性送信できているが最後のテストでattrviewer13には属性送信できなくなった場合、上記※3「server.p12を更新」の手順を再度ご確認ください。

※ メタデータ伝播待ちの期間について

メタデータ伝播待ちの期間は学認技術運用基準（メタデータの有効期限(validUntil)）で規定される最大マージンを取ったものです。各SP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。