サーバ証明書設定(SP)

サーバ証明書の設定

1. Apacheの設定

■/etc/httpd/conf.d/ssl.conf

実習セミナー

・証明書は、初期設定で「/root/GETFILE」に配置されている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**

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/ex-sp-certs/ex-sp-test??.gakunin.nii.ac.jp.cer /etc/pki/tls/certs/server.crt ← ??は各自割り振られた番番号（0番なら「00」）

# cp /root/GETFILE/ex-sp-keys/ex-sp-test??.gakunin.nii.ac.jp.key /etc/pki/tls/private/server.key ← ??は各自割り振られた番番号（0番なら「00」）
```

秘密鍵を"root"ユーザのみが参照できるように所有者・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
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
```

2. Shibboleth SPの設定

■/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。

サーバ証明書と秘密鍵を「/root/GETFILE」配下よりコピーします。

```
# cp /root/GETFILE/ex-sp-certs/ex-sp-test??.gakunin.nii.ac.jp.cer /etc/shibboleth/cert/server.crt ← ??は各自割り振られた番番号（0番なら「00」）

# cp /root/GETFILE/ex-sp-keys/ex-sp-test??.gakunin.nii.ac.jp.key /etc/shibboleth/cert/server.key ← ??は各自割り振られた番番号（0番なら「00」）
```

/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のデフォルト設定にならってパーミッションを設定してください。

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

/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。

BACK TOP