インストール（SP）2023

インストール

実習セミナー内に準備されたLinuxサーバに、Shibbolethをインストールする手順となっています。

---

1. 実習に使用する仮想サーバについて

以下は本技術ガイドで構築する前提となる環境です。

- OS、DNS、ネットワーク、時刻同期などは設定済みとなっています。（Apache HTTP Server、mod_sslもインストール済み）
- CentOS7
- メモリ2GB以上
- Apache HTTP Server 2.4 と mod_ssl
- Shibboleth SP v3

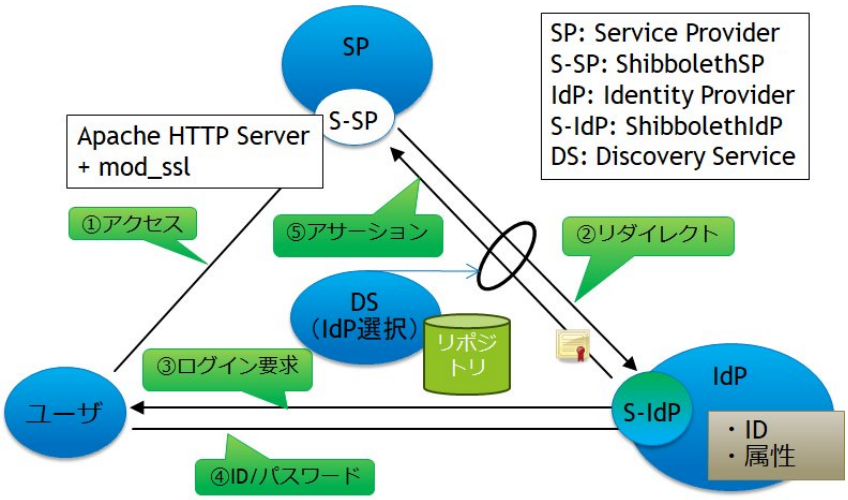
用語	
DNS	DNSは、Domain Name Systemの略で、インターネット上でドメイン名を管理・運用するためのシステム。
Apache HTTP Server	Apache License2.0の条件でリリースされるフリーでオープンソースのクロスプラットフォームの Webサーバソフトウェア。
mod_ssl	mod_sslはOpenSSLを使ってApache HTTP Serverを通信の暗号化（SSL(Secure Sockets Layer), TLS(Transport Layer Security)）に対応させるモジュール。
Shibboleth SP	Shibbolethは、組織内および組織を超えてWeb上でシングルサインオン（SSO）を実現し認証フェデレーションを構成するための、標準的なオープンソースソフトウェアのパッケージです。 Shibbolethを用いた認証はShibboleth（シボレス）認証と呼ばれます。 Shibboleth SPはSP(Service Provider)側にインストールするソフトウェアです。

SPサーバにインストールするのは、

- Apache HTTP Server
- mod_ssl
- Shibboleth SP

の３つのパッケージで、下図で背景色が白である図形部分です。

但し、本実習ではApache HTTP Server、mod_sslはインストール済（下図、白背景の四角で示しています）のサーバを準備しており、Shibboleth SPをインストールする実習になります。（下図、白背景の楕円形で示しています）



なお、以降の節ののコマンド投入と実行結果のメッセージを示す枠（ライトグレー背景色）内では、以下のように文字の色分けをしています。

緑色の文字	端末画面にキーボード入力する行。 この文字列をコピー＆ペーストして端末画面に入力もできる。
黒色の文字	コマンド実行結果のメッセージ。 行数が多い時は<中略>と表記し、メッセージ全部の表記を省略している。
赤色の文字	コマンド実行結果のメッセージで注意する部分。
青色の文字	前後の行を説明する。

また、実習環境ではSELinuxは無効化されているものとして手順を記載しています。下記コマンドでSELinuxが無効化されていることを確認してください。

```
$ /usr/sbin/getenforce
Disabled
```

なお、sudoコマンドを実行し、rootユーザで以降のコマンドを実行するようにします。

```
$ sudo -i
#
```

2.Shibbolethのインストール

1. repositoryファイル追加

Shibboleth用のrepositoryファイルをダウンロードします。

```
# curl -O 'https://shibboleth.net/cgi-bin/sp_repo.cgi?platform=CentOS_7'
 % Total  % Received % Xferd  Average Speed  Time    Time     Time   Current
                                Dload    Upload Total   Spent    Left   Speed
100 372   0   372    0     0    472       0     --:--:-- --:--:-- --:--:--  472

ダウンロードされたファイルを確認する
# ls -l
-rw-r--r-- 1 root root 372  6月 20 23:04 sp_repo.cgi?platform=CentOS_7
```

yumにrepositoryファイルを追加します。

```
# cp sp_repo.cgi¥?platform=* /etc/yum.repos.d/shibboleth.repo

repositoryファイルが追加されたことを確認

# ls -l /etc/yum.repos.d/shibboleth.repo

-rw-r--r-- 1 root root 372  6月 20 23:42 /etc/yum.repos.d/shibboleth.repo
```

2. インストール

yumコマンドを使用する為、依存関係のあるunixODBCなども同時にインストールされます。

```
# yum install shibboleth
```

shibbolethパッケージの依存性、インストール容量等表示され、インストールするかの確認があります。

```
(中略)

総ダウンロード容量: 5.0 M

インストール容量: 28 M
Is this ok [y/d/N]: y
```

インストールが始まり、途中でPGP鍵のインポートに関して確認があります。

```
(中略)
https://shibboleth.net/downloads/service-provider/RPMS/repomd.xml.key から鍵を取得中です。
Importing GPG key 0x7D0A1B3D:
 Userid : "security:shibboleth OBS Project <security:shibboleth@build.opensuse.org>"
 Fingerprint: 6519 b5db 7c1c 8340 a954 ed00 73c9 3745 7d0a 1b3d
 From   : https://shibboleth.net/downloads/service-provider/RPMS/repomd.xml.key
上記の処理を行います。よろしいでしょうか？ [y/N] y
```

Fingerprint: に表示されている文字列が上記と一致することを確認の上、y[ENTER] を入力してください。同様に2つ目のPGP鍵の確認がありますので、

```
https://shibboleth.net/downloads/service-provider/RPMS/cantor.repomd.xml.key から鍵を取得中です。

Importing GPG key 0x02277962:

 Userid : "Scott Cantor <cantor.2@osu.edu>"

 Fingerprint: dcaa 1500 7bed 9de6 90cd 9523 378b 8454 0227 7962

 From   : https://shibboleth.net/downloads/service-provider/RPMS/cantor.repomd.xml.key

上記の処理を行います。よろしいでしょうか？ [y/N] y
```

Fingerprint: に表示されている文字列が上記と一致することを確認の上、y[ENTER] を入力してください。

なお、OSインストール直後の状態でyum install shibbolethでインストールされるパッケージは以下の通りです。
（2022年7月現在, CentOS 7にて）

```
libcurl-openssl-7.86.0-1.el7

libsaml12-3.2.1-1

liblog4shib2-2.0.1-1

xmltooling-schemas-3.2.4-1

shibboleth-3.4.1-1

libxerces-c-3_2-3.2.4-1

libxmltooling10-3.2.4-1

libxml-security-c20-2.0.4-1

unixODBC-2.3.1-14.el7

libmemcached-1.0.16-5.el7

opensaml-schemas-3.2.1-1
```

3. httpd 設定

/etc/httpd/conf.d/ssl.confにて、ServerNameを設定します。

```
#ServerName www.example.com:443
        ↓
ServerName ex-sp-test??.gakunin.nii.ac.jp:443 ← ホスト名を設定（??には、割り振られた番号を設定）
```

4. shibd 起動

以下のコマンドでshibdを起動します。

```
# systemctl start shibd      ←サービスの起動
# systemctl enable shibd    ←サービスの自動起動

Created symlink from /etc/systemd/system/multi-user.target.wants/shibd.service to /usr/lib/systemd/system/shibd.service.
```

3.サービスの起動・停止方法

サービス	起動コマンド	停止コマンド	再起動コマンド
httpd	systemctl start httpd	systemctl stop httpd	systemctl restart httpd
shibd	systemctl start shibd	systemctl stop shibd	systemctl restart shibd

※shibdと同様、httpdもSPの設定ファイル（shibboleth2.xml等）を読み込みますので、設定ファイルを変更した際はhttpdの再起動もしくは再読み込み(reload)もあわせて行うようにしてください。httpdに含まれるShibbolethモジュール(mod_shib)が当該ファイルを読み込みます。

インストールが完了したら，サイト情報等の設定を行って下さい．