

# インストール（SP）

## 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](#)
- [2.Shibbolethのインストール](#)
- [3.サービスの起動・停止方法](#)

### 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

本手順における用語の解説：

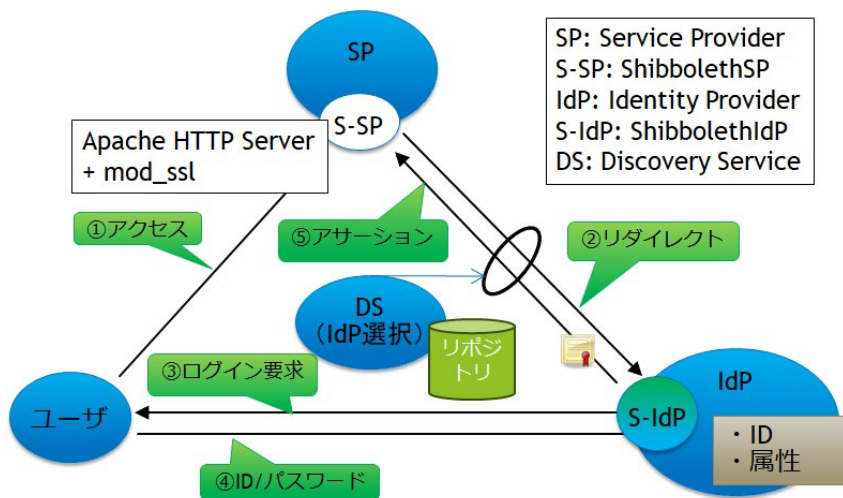
用語	説明
DNS	DNSは、Domain Name Systemの略で、インターネット上でドメイン名を管理・運用するためのシステム。
Apache HTTP Server	Apache License2.0の条件でリリースされるフリーでオープンソースなクロスプラットフォームのWebサーバソフトウェア。
mod_ssl	mod_sslはOpenSSLを使ってApache HTTP Serverを通信の暗号化（SSL(Secure Sockets Layer), TLS(Transport Layer Security)）に対応させるモジュール。
Shibboleth SP	Shibboleth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はインストール済み（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）



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設定が確認できます。

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

実行していなければ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てください。あくまで実習の効率化のためであり、実環境ではコマンドごとにrootユーザでの実行の必要性の有無を確認してください。

```
$ sudo -i
```

```
#
```

## 2. Shibbolethのインストール

### 1. repositoryファイル追加

Shibboleth SP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'
```

yumにrepositoryファイルを追加します。

```
# cp sp_repo.cgi?platform=* /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)
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。

```
Retrieving key from https://shibboleth.net/downloads/service-provider/RPMS/repomd.xml.key
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]
```

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、

```
Retrieving key from https://shibboleth.net/downloads/service-provider/RPMS/cantor.repomd.xml.key
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]
```

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。  
(2023年7月現在, CentOS 7にて)

```
shibboleth 3.4.1-1
libcurl-openssl
liblog4shib2
libmemcached
libsaml12
libxerces-c-3_2
libxml-security-c20
libxmltooling10
opensaml-schemas
unixODBC
xmltooling-schemas
```

### 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 ← 先頭の#を削除しホスト名を設定 (??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設定
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](#)を行ってください。