

貴学にてSPをインストールする場合の構築手順

貴学にてSPをインストールする場合の構築手順

1. Shibboleth SP (version 3.0以降) の動作要件
2. OSをインストールする
3. Shibbolethのインストール
4. サービスの起動・停止方法

1. Shibboleth SP (version 3.0以降) の動作要件

以下は本技術ガイドで構築する前提となる環境です。

- Apache HTTP Server 2.4以上と mod_ssl

他の環境および最新の情報はShibbolethのサイトでご確認ください:
[全体](#), [Linux](#), [macOS](#), [Windows](#), [Java Servlets](#)

2. OSをインストールする

1. OSでの設定

- OS (CentOS 7) インストール
インストーラを起動してOSのインストールを行ってください。途中表示されるパッケージ選択画面では「Webサーバー」を選択してください。その他に必要なパッケージがある場合は、適宜インストールしてください。
※このテキストはSELinuxは無効化されているものとして書かれております。下記コマンドでSELinux設定を確認してください。

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

- ネットワーク設定
環境に合わせ、ホスト名・ネットワーク・セキュリティを設定してください。
SPでは shibd サービスが通信を行います。

2. DNSへ登録

新しいホスト名とIPアドレスをDNSに登録してください。

3. 時刻同期の設定

ntpサービスを用い、貴学環境のntpサーバと時刻同期をしてください。
※Shibbolethでは、通信するサーバ間の時刻のずれが約5分を越えるとエラーになります。

3. Shibbolethのインストール

SPバージョン2.3からはrepositoryが用意され、yumに対応したのでインストールが大変楽になりました。
ここで説明するのは、以下のOSについてのインストール方法となります。

- CentOS 6/7, Red Hat Enterprise Linux 6/7 (i386) ※ただし7はx86_64しかなくOpenSSLのバージョンの関係で7.4以降向け
- SUSE Linux Enterprise Server 11(SP3/SP4), 12(SP2/SP3) (i386)

その他のOSについては、以下を参照してください。

※上記OSでx86_64の場合
⇒下記の"yum install shibboleth"を"yum install shibboleth.x86_64"と読み替えてください。
※Linuxの他のディストリビューションの場合
⇒[こちら](#)
※他のOSの場合
⇒[こちら](#)

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。
(下記コマンドは、CentOS 7 の場合です。他のディストリビューションの場合はURLの "CentOS_7" の部分を適宜読み替えてください。ただし、RHEL 7 の場合は "CentOS_7" をご利用ください。)

対応表：

OS/バージョン	URL
CentOS 6	CentOS_CentOS-6
CentOS 7, RHEL 7	CentOS_7

※ここに掲載されていないOSについては[こちら](#)を参照してください

```
# wget 'https://shibboleth.net/cgi-bin/sp_repo.cgi?platform=CentOS_7'
```

yumにrepositoryファイルを追加します。(ファイル名も標準的なものに変更しています。)

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

2. インストール

yum コマンドの実行前に、まず[※PGP鍵のインポート](#)を参照してください。
yumコマンドを使用する為、依存性のあるunixODBCなども同時にインストールされます。

```
# yum install shibboleth
```

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。
(2018年7月18日現在, CentOS 7にて)

```
shibboleth 3.0.0-1.1  
libcurl-openssl  
liblog4shib2  
libmemcached  
libsaml10  
libxerces-c-3_2  
libxml-security-c20  
libxmltooling8  
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 sp.example.ac.jp:443 ← ホスト名を設定
```



加えて、SSL 3.0プロトコルに対する攻撃が発見されておりますので、当該プロトコルを無効化することをお勧めします。⇒[SSLバージョン3の脆弱性について \(CVE-2014-3566\)](#)

```
SSLProtocol all -SSLv2 -SSLv3
```

4. shibd 起動

以下のコマンドでshibdを起動し、自動起動設定も行います。

```
# systemctl start shibd  
# systemctl enable shibd
```

```
# service shibd start
```

4. 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

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

※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。