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

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3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 7/8, Red Hat Enterprise Linux 7/8 ※ただし7はOpenSSLのバージョンの関係で7.4以降向け
- Rocky Linux 8/9, Amazon Linux 2

その他のOSについては、以下を参照してください。

※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" の部分を下記対応表を参考に適宜読み替えてください。特に RHEL 7/8 の場合は CentOS_7/8 をご利用ください。）

対応表：

OS/バージョン	URLの赤字部分
CentOS 7, RHEL 7	CentOS_7
RHEL 8	CentOS_8
Rocky Linux 8	rockylinux8
Rocky Linux 9	rockylinux9

※ 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
```

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
Is this ok [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
Is this ok [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 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．