貴学にてIdPv4をインストールする場合の構築手順

貴学にてIdPをインストールする場合の構築手順

貴学にて、貴学のサーバにOSを含めShibboleth IdPならびに必要なパッケージのインストール・設定を行う手順を説明します。

---

1. Shibboleth IdP (version 4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。

- メモリ3GB以上
  Java実行環境への推奨割り当てメモリ量が1.5GBですので、その動作に支障がないようにしてください。
- Apache HTTP Server 2.4 以上　と mod_ssl

以下のパッケージはインストール方法も含めて以降の手順で説明します。

- Jetty 9.4
  - jetty-distribution-9.4.32.v20200930を使った手順となっています。
    ※いずれも以下のShibbolethのサイト「Jetty94」が情報源です。
  - 以前の技術ガイドではサーブレットコンテナとしてTomcatを用いたものをご案内しておりました。その関係で継続してTomcat利用を強くご希望の方向けに、暫定的にShibboleth IdP V4をTomcat 9で構築する方法を別途ご案内しております:
    ⇒旧: 貴学にてIdPv4（Tomcat）をインストールする場合の構築手順
    - いずれにしろTomcat 10およびそれ以降はサポートできかねますのでご了承ください。
    - あくまでも暫定版です。すでに運用中でTomcatをお使いの方は動作確認の上Jettyへの移行をご検討ください。
- Java 11
  - Java 11以降のバージョンのみ対応しています。

    > ⚠ 文字列置換のためのJavaScriptメソッド "abc".replace("a", "b") について、Java 7では全置換されていたものがJava 8では先頭の一致した部分しか置換されなくなるという情報があります。
    > 当該メソッドを使って全置換を行っている場合は正規表現 replace(/a/g, "b") を使うようにしてください。

  - Oracle JDK / OpenJDK 11にてLDAPサーバへの接続にLDAPSを使う場合、以下のエラーになるという情報があります。

    ```
    java.lang.NullPointerException: Thread local SslConfig has not been set
    ```

    原因はJDKのバグであるとのことです。該当する場合、以下でUnboundIDを使う回避策が提示されています。
    https://wiki.shibboleth.net/confluence/display/IDP30/LDAPonJava>8
    詳細: https://issues.shibboleth.net/jira/browse/IDP-1357
  - エントロピー不足で起動が遅くなる場合があるという情報があります。jre/conf/security/java.securityやシステムプロパティ等で対処してください。
    確認方法および手順例: IdPのサービス動作状況の確認の「よくあるエラー」の503エラーの項
    - この問題はCentOS 7を使っている場合に顕著です。
    - VMで稼働させていてこの問題がある場合、ホストマシンでHavegedを導入しVMからこれを参照する等で十分なエントロピーを生成できる場合があるようですので、合わせてご検討ください。
  - GNU Javaは利用できません。 OpenJDKもしくはOracleのJavaを利用してください。

最新の情報はShibbolethのサイトでご確認ください:
全体, Jetty 9.4

---

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

インストーラでインストールするもの。

Webサーバー (HTTPのみ)
OpenLDAP

その他のパッケージは必要に応じてインストールしてください。
ただし、Java開発とJettyは後の手順で別にインストールします。

運用フェデレーション参加後に、ホスト名を変更する場合はいくつか考慮・解決すべき点があります。
ホスト名は十分ご検討いただいた上で設定してください。詳しくは IdPのホスト名変更に関する注意点 をご参照ください。
※このテキストはSELinuxはPermissiveに設定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下さい。

2. DNSへ登録する

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. 時刻同期を設定する

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. jdk 11、jetty 9.4をインストールする

1. tomcatの削除

tomcat が入っている場合は、削除してください。

2. jdk のインストール

CentOS 7にはOpenJDKのパッケージが用意されていますので、これをyumにてインストールします。

```
# yum install java-11-openjdk-headless
```

3. jetty 9.4 のインストール

https://www.eclipse.org/jetty/download.html より最新版のパッケージ(.tgz)をダウンロードしてインストールします。
さらに、Shibboleth Projectが配布しているJetty向け設定ファイル群(jetty-base)を配置します。

```
※以下は手順書作成時の最新
# wget https://repo1.maven.org/maven2/org/eclipse/jetty/jetty-distribution/9.4.44.v20210927/jetty-distribution-9.4.44.v20210927.tar.gz
# tar zxv -C /opt -f jetty-distribution-9.4.*.v????????.tar.gz
# ( cd /opt ; ln -s jetty-distribution-9.4.*.v???????? /opt/jetty )
# wget https://build.shibboleth.net/maven/snapshots/net/shibboleth/idp/idp-jetty-base/9.4.1-SNAPSHOT/idp-jetty-base-9.4.1-20220208.135650-767.tar.gz
# tar zxv -C /opt -f idp-jetty-base-9.4.?-????????.*.tar.gz
```

サービス起動には、jetty起動用のユーザを使用することを推奨します。

ここでは、一般的な"jetty"ユーザを作成します。（以降、"jetty"ユーザを使用する事を前提として説明します。）なお、下記コマンドでユーザID・グループIDは /usr/share/doc/setup-2.8.71/uidgid の値を利用していますが他の値でも問題ありません。既存のユーザ・グループと重複しない値を指定してください。

```
# groupadd -g 110 jetty
# useradd -u 110 -g jetty -d /opt/jetty-base -s /sbin/nologin -c "Jetty daemon" jetty
```

以下のコマンドでその他Jetty関連の設定ファイルやディレクトリの所有者、パーミッションを設定します。

```
# chown -R root:root /opt/jetty-distribution-9.4.*.v???????? /opt/jetty-base

# chmod -R g-w /opt/jetty-base

# chown jetty:jetty /opt/jetty-base/{logs,tmp}
```

以下の内容で /etc/sysconfig/jetty を作成します。

```
JAVA=/usr/lib/jvm/jre/bin/java
JETTY_HOME=/opt/jetty
JETTY_BASE=/opt/jetty-base
JETTY_RUN=/opt/jetty-base/tmp
JETTY_STATE=/opt/jetty-base/tmp/jetty.state
```

ここで JAVA= で指定しているコマンドの存在・バージョンを確認しておくとよいでしょう。javaコマンドにパスが通っている場合はこの行を削除してもかまいません。

```
$ /usr/lib/jvm/jre/bin/java -version
openjdk version "11.0.10" 2021-01-19 LTS
OpenJDK Runtime Environment 18.9 (build 11.0.10+9-LTS)
OpenJDK 64-Bit Server VM 18.9 (build 11.0.10+9-LTS, mixed mode, sharing)
```

起動スクリプトを以下のように配置します。

```
# sudo cp -ip /opt/jetty/bin/jetty.sh /etc/init.d/jetty
# sudo cp -ip /opt/jetty/bin/jetty.service /etc/systemd/system/
```

/etc/systemd/system/jetty.serviceを以下のように修正します。

```
[Service]
Type=forking
EnvironmentFile=-/etc/sysconfig/jetty
PIDFile=/opt/jetty-base/tmp/jetty.pid
ExecStart=/etc/init.d/jetty start
ExecStop=/etc/init.d/jetty stop
ExecReload=/etc/init.d/jetty restart
SuccessExitStatus=143
User=jetty
Group=jetty
```

設定を反映させ、自動起動の登録を行います。

```
# sudo systemctl daemon-reload
# sudo systemctl enable jetty
```

4. jetty-baseの設定

/opt/jetty-base/webapps/idp.xmlを以下のように修正します。（idp.warファイルのパス修正）

```
<Configure class="org.eclipse.jetty.webapp.WebAppContext">
<Set name="war"><SystemProperty name="idp.war.path" default="/opt/shibboleth-idp/war/idp.war" /></Set>
<Set name="contextPath"><SystemProperty name="idp.context.path" default="/idp" /></Set>
<Set name="extractWAR">false</Set>
<Set name="copyWebDir">false</Set>
<Set name="copyWebInf">true</Set>
</Configure>
```

idp-backchannel.iniを読み込まないようにします。

```
# sudo mv -i /opt/jetty-base/start.d/idp-backchannel.ini /opt/jetty-base/start.d/idp-backchannel.ini.dist
```

/opt/jetty-base/start.d/start.ini を以下の内容で作成します。

```
# Any other required Jetty modules...

# Allows setting Java system properties (-Dname=value)
# and JVM flags (-X, -XX) in this file
# NOTE: spawns child Java process
--exec

# Uncomment if IdP is installed somewhere other than /opt/shibboleth-idp
#-Didp.home=/path/to/shibboleth-idp

# Newer garbage collector that reduces memory needed for larger metadata files
-XX:+UseG1GC

# Maximum amount of memory that Jetty may use, at least 1.5G is recommended
# for handling larger (> 25M) metadata files but you will need to test on
# your particular metadata configuration
-Xmx1500m

# Prevent blocking for entropy.
-Djava.security.egd=file:/dev/./urandom

# Set Java tmp location
-Djava.io.tmpdir=tmp
```

/opt/jetty-base/modules/idp.mod を修正します。（https と ssl をコメントアウト）

```
[depend]
annotations
deploy
ext
#https
jsp
jstl
plus
resources
server
servlets
#ssl
```

/opt/jetty-base/start.d/idp.ini を修正します。

```
# ----------------------------------------
# Module: idp
# Shibboleth IdP
# ----------------------------------------
--module=idp
--module=http
--module=http-forwarded


## Keystore file path (relative to $jetty.base)
jetty.sslContext.keyStorePath=../credentials/idp-userfacing.p12


（省略）

※末尾に以下を追加

## Connector port to listen on
jetty.ssl.port=443    ※利用されない
jetty.http.host=127.0.0.1
jetty.http.port=8080
```

/opt/jetty-base/start.d/idp-logging.ini を修正します。

```
（省略）

# Override logback version pinned in jetty-home/modules/logback-impl.mod
logback.version=1.2.10
# Override SLF4J version pinned in jetty-home/modules/slf4j-api.mod
slf4j.version=1.7.32
```

ここで記載しているバージョンは lib/logback/ および log/slf4j/ 以下に配置されているライブラリのバージョンです。展開したjetty-baseが本技術ガイドに記載のものと異なる場合は、実際に配置されているライブラリのバージョンを logback.version= および slf4j.version= に記述してください。

/opt/jetty-base/etc/tweak-ssl.xmlを以下の内容で作成します。

```
<!DOCTYPE Configure PUBLIC "-//Jetty//Configure//EN"
         "http://www.eclipse.org/jetty/configure_9_4.dtd">
<Configure id="sslContextFactory" class="org.eclipse.jetty.util.ssl.SslContextFactory">
    <Set name="IncludeProtocols">
        <Array type="String">
            <Item>TLSv1.3</Item>
            <Item>TLSv1.2</Item>
        </Array>
    </Set>
    <Set name="ExcludeProtocols">
        <Array type="String">
            <Item>TLSv1.1</Item>
            <Item>TLSv1</Item>
            <Item>SSL</Item>
            <Item>SSLv2</Item>
            <Item>SSLv3</Item>
        </Array>
    </Set>
    <Set name="IncludeCipherSuites">
        <Array type="String">
            <Item>TLS_AES.*</Item>
            <Item>TLS_CHACHA20.*</Item>
            <Item>TLS_ECDHE.*</Item>
            <Item>TLS_EMPTY_RENEGOTIATION_INFO_SCSV</Item>
        </Array>
    </Set>
    <Set name="ExcludeCipherSuites">
        <Array type="String">
            <Item>.*NULL.*</Item>
            <Item>.*RC4.*</Item>
            <Item>^.*_(MD5|SHA|SHA1)$</Item>
            <Item>.*DES.*</Item>
            <Item>.*DSS.*</Item>
            <Item>^TLS_DHE_.*$</Item>
            <Item>^TLS_RSA_.*$</Item>
        </Array>
    </Set>
</Configure>
```

上記ファイルを参照するように /opt/jetty-base/modules/idp-backchannel.mod に追記します。

```
（省略）

[xml]
etc/idp-backchannel.xml
etc/tweak-ssl.xml
```

5. httpd の設定

/etc/httpd/conf/httpd.conf の修正

```
（省略）
#ServerName example-idp.nii.ac.jp:80  ←ホスト名
↑コメントアウト（#）を削除
（省略）
```

/etc/httpd/conf.d/ssl.conf の修正

```
（省略）
<VirtualHost _default_:443>
（省略）
#ServerName example-idp.nii.ac.jp:443  ←ホスト名
↑コメントアウト（#）を削除
↓以下を追加
RequestHeader set X-Forwarded-Port 443
RequestHeader set X-Forwarded-Proto https
RequestHeader unset Forwarded
RequestHeader unset X-Forwarded-For
ProxyPass /idp/ http://localhost:8080/idp/ connectiontimeout=5 timeout=15
（省略）
```

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
```

/etc/httpd/conf.d/virtualhost-localhost80.conf を以下の内容で作成してください。
これはShibboleth IdPが提供するreload-metadata.sh等のコマンドを使った操作を可能にするためのものです。

すでに同一のvirtual hostを別のところで定義している場合は、そちらに含めてください。
また、すでに _default_:80 のVirtualHostが定義されている場合はその中の宣言が localhost:80 に適用されなくなりますので、
必要であればその宣言をこのファイルにも含めてください。

default:80 が定義されているファイルに下記ProxyPassを含める方法もありますが、外部からの通常のアクセスがセキュア
でない80番ポートに対しても行えることになりますので推奨しません。
（もちろん、ファイアウォール等で適切に対処されていれば問題ありません）

```
<VirtualHost localhost:80>
ProxyPass /idp/ http://localhost:8080/idp/ connectiontimeout=5 timeout=15
</VirtualHost>
```

---

4. Shibbolethのインストール

各ファイル名等の指定は，Version 4に準拠しています。

1. Shibboleth IdP パッケージのダウンロード

http://shibboleth.net/downloads/identity-provider/latest/から最新のIdP（ shibboleth-identity-provider-4.?.?.tar.gz ）をダウンロードします。

ダウンロードしたファイルの真正性を確かめるにはPGP署名（ダウンロードURLに".asc"を追加したもの）を確認してください。

2. インストール

shibboleth-identity-provider-4.?.?.tar.gz を適当なディレクトリに置いて、以下のコマンドを実行してください。

```
# tar xzvf shibboleth-identity-provider-4.?.?.tar.gz
# cd shibboleth-identity-provider-4.?.?
# sudo ./bin/install.sh -Didp.conf.credentials.filemode=640 -Didp.conf.credentials.group=jetty
```

install.shシェルスクリプトを実行すると、以下のような問い合わせがあります。
手順に従って、進めてください。

⚠ インストール時に入力するパスワードを本運用で使う場合は、推測されにくいものを使用してください。
※ここで入力した Cookie Encryption Key Password は、/opt/shibboleth-idp/credentials/secrets.propertiesに記載されます。
一方 Backchannel PKCS12 Password は記録されません。

```
Buildfile: /root/shibboleth-identity-provider-4.0.1/bin/build.xml

install:
Source (Distribution) Directory (press <enter> to accept default): [/root/shibboleth-identity-provider-4.0.1] ?
[Enter]  ←入力なし

Installation Directory: [/opt/shibboleth-idp] ?
[Enter]  ←入力なし

INFO [net.shibboleth.idp.installer.V4Install:151] - New Install. Version: 4.0.1
Host Name: [upkishib-idp.nii.ac.jp]
[Enter]  ←入力なし ※表示されたホスト名が違う場合、設定してください。

INFO [net.shibboleth.idp.installer.V4Install:549] - Creating idp-signing, CN = upkishib-idp.nii.ac.jp URI = https://upkishib-idp.nii.
ac.jp/idp/shibboleth, keySize=3072
INFO [net.shibboleth.idp.installer.V4Install:549] - Creating idp-encryption, CN = upkishib-idp.nii.ac.jp URI = https://upkishib-idp.
nii.ac.jp/idp/shibboleth, keySize=3072

Backchannel PKCS12 Password: backpass[Enter]  ←任意のパスワード
Re-enter password: backpass[Enter]

INFO [net.shibboleth.idp.installer.V4Install:592] - Creating backchannel keystore, CN = upkishib-idp.nii.ac.jp URI = https://upkishib-
idp.nii.ac.jp/idp/shibboleth, keySize=3072

Cookie Encryption Key Password: cookiepass[Enter]  ←任意のパスワード
Re-enter password: cookiepass[Enter]

INFO [net.shibboleth.idp.installer.V4Install:633] - Creating backchannel keystore, CN = upkishib-idp.nii.ac.jp URI = https://upkishib-
idp.nii.ac.jp/idp/shibboleth, keySize=3072
INFO [net.shibboleth.utilities.java.support.security.BasicKeystoreKeyStrategyTool:166] - No existing versioning property,
initializing...
SAML EntityID: [https://upkishib-idp.nii.ac.jp/idp/shibboleth] ?
[Enter]  ←入力なし

Attribute Scope: [nii.ac.jp]
[Enter]  ←入力なし ※表示されたスコープが違う場合、設定してください。

  （省略）

BUILD SUCCESSFUL
Total time: 2 minutes 9 seconds
```

上記のような質問に答えながら、インストールを行います。

3. パーミッションの調整

”jetty”ユーザがログファイルを出力できるようディレクトリの所有者を変更します。

同様に、メタデータの保存ディレクトリの所有者・パーミッションも変更します。

```
# sudo chown -R jetty:jetty /opt/shibboleth-idp/logs
# sudo chgrp jetty /opt/shibboleth-idp/metadata
# sudo chmod g+w /opt/shibboleth-idp/metadata
# sudo chmod +t /opt/shibboleth-idp/metadata
```

✓ IdPが実際に使用する証明書の秘密鍵はまだ配置されておりませんので、所有者・パーミッションは後の手順で設定します。

4. jstl-1.2.jar の配置

※jstlの別途インストールは不要

5. ディレクトリインデックスの禁止

edit-webapp内にweb.xml を作成します。

```
# sudo cp -ip /opt/shibboleth-idp/dist/webapp/WEB-INF/web.xml /opt/shibboleth-idp/edit-webapp/WEB-INF/web.xml
# sudo chmod u+w /opt/shibboleth-idp/edit-webapp/WEB-INF/web.xml
```

作成したweb.xml を以下の内容で修正します。
※既存の<servlet>の前に設定を追加します。

```
<filter-mapping>
<filter-name>SLF4JMDCServletFilter</filter-name>
<url-pattern>/*</url-pattern>
</filter-mapping>

<!-- Servlets and servlet mappings -->
<servlet>
<servlet-name>default</servlet-name>
<servlet-class>org.eclipse.jetty.servlet.DefaultServlet</servlet-class>
<init-param>
<param-name>dirAllowed</param-name>
<param-value>false</param-value>
</init-param>
<load-on-startup>0</load-on-startup>
</servlet>

<servlet>
<servlet-name>idp</servlet-name>
```

以下を実行して反映させます。

```
# sudo /opt/shibboleth-idp/bin/build.sh
```

httpdの再起動とJettyの起動を行います。（すでにJettyが起動している場合はstopしてから行ってください）

```
# systemctl restart httpd
# systemctl start jetty
```

⚠ ※jetty起動に失敗したら設定修正後、/opt/jetty-base/tmp/下にファイルが残っていたら削除してから再度起動してください。
※build.shしたら sudo systemctl restart jetty しないと反映されません。

---

5. 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
jetty	systemctl start jetty	systemctl stop jetty	systemctl restart jetty

---

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．