旧：貴学にてIdPをインストールする場合の構築手順

旧：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からShibboleth(IdP)までインストール・設定を行い、構築する方式です。

本ページおよび後続のページの内容は古いものです。Shibboleth IdPの最新版は3.2.1であり、バージョン2系のサポートは2016年7月に終了しました。特に新規構築の場合は3.2.1以降を使用することを推奨します。

Shibboleth IdPバージョン3(IdPv3)の情報については、設定・運用・カスタマイズのアップデート手順の3.0.0の項に情報を掲載しております。

IdPv3のインストール手順については以下のページをご参照ください。
⇒貴学にてIdPv3をインストールする場合の構築手順

---

1. Shibboleth IdP (version 2.3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 2.2 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。

- Apache Tomcat 6.0.17以上
  - Tomcat 7およびそれ以降でSOAP接続を行う場合は、`tomcat6-dta-ssl-x.x.x.jar` を使うのではなく https://wiki.shibboleth.net/confluence/display/IDP30/ApacheTomcat8#ApacheTomcat8-SupportingSOAPEndpoints でIdPv3向けに用意されております `trustany-ssl-x.x.x.jar` をお使いください。
- Java 6 or 7
  - Java 7を使用する場合は、IdPバージョン2.4.0以降を使用してください。2.3.xにはJava 7上でのみ特定条件で発生するバグがあります。
  - Java 8 は IdP v2 では公式にはサポートされません。IdP v3 でサポート予定です。
    IdP v2をJava 8上で使うと Script Attribute Definition で不具合があることが確認されています。
    詳細: Shibboleth Wiki: IdPJava1.8
  - CentOSに付属する GNU Javaは利用できません。 OracleのJavaもしくはOpenJDKを利用してください。

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, Jetty 7, Apache Tomcat, JBoss Tomcat

---

2. OSをインストールする

1. OSでの設定

・OS（CentOS 6）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Tomcat 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５分を越えるとエラーになります。

---

3. jdk6、tomcat6をインストールする（★）

1. 古いtomcatの削除

tomcat5-5.5.25以前のバージョン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 6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-1.7.0-openjdk
```

http://java.sun.com/javase/downloads/index.jsp にあります"Java SE 7u??"の項にある"JDK"の項より構築環境に合わせてダウンロードしたパッケージを適当なフォルダに置いて、以下のコマンドを実行してください（??は用意されているjdkのリビジョン番号にあわせて記述して下さい）。

```
# rpm -ivh jdk-7u??-linux-x64.rpm
```

```
# chmod a+x jdk-6u??-linux-x64-rpm.bin
# ./jdk-6u??-linux-x64-rpm.bin
```

3. tomcat 6のインストール（★）

CentOS 6の場合、標準パッケージでTomcat 6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 tomcat6
```

http://tomcat.apache.org/download-60.cgi よりダウンロードした apache-tomcat-6.?.??.tar.gz を/usr/javaにを置いて、以下のコマンドを実行してください（?は用意されているtomcatのリビジョン番号にあわせて記述して下さい）。

```
# tar zxv -C /usr/java -f apache-tomcat-6.?.??.tar.gz
# ln -s /usr/java/apache-tomcat-6.?.?? /usr/java/tomcat
```

自動起動スクリプトを利用すると便利です。ZIPを解凍後にtomcat6起動スクリプトファイルをコピーします。

主な変更点は以下の通りです。

- 一部環境でOS停止時にTomcat停止処理が実行されなかったのを修正
- 一部環境で日本語表示が?になるのを修正
- Tomcat停止待ちに上限を設定(1分)

/etc/init.d/tomcat6 を更新する場合はTomcat停止後に行なうのがお勧めです。そうでないとPIDファイル等に不整合が生じます。

Oracle(Sun) JVM / OpenJDK 以外をご使用の方は適宜オプションを調整してください。

```
# unzip tomcat6.zip
# chmod a+x tomcat6
# cp tomcat6 /etc/rc.d/init.d/
```

自動起動の設定 (このオプション指定では マイナス ‘ー’ が２つ必要です)

```
# chkconfig --add tomcat6
# chkconfig --level 345 tomcat6 on
# service tomcat6 start
```

4. profileの修正（★）

/etc/profileを下記のように修正します。
どこでもよいのですが、下記の例では「# /etc/profile」の下（ファイルの2行目）に挿入しています。

下記のJAVA_HOMEは、OpenJDKを使ったパスとなります。
また、CATALINA_HOMEおよびCATALINA_BASEは、yumでtomcat6をインストールした場合のパスとなります。
環境に合わせて変更してください。

```
# /etc/profile
JAVA_HOME=/usr/lib/jvm/jre
MANPATH=$MANPATH:$JAVA_HOME/man
CATALINA_HOME=/usr/share/tomcat6
CATALINA_BASE=$CATALINA_HOME
PATH=$JAVA_HOME/bin:$CATALINA_BASE/bin:$CATALINA_HOME/bin:$PATH
export PATH JAVA_HOME CATALINA_HOME CATALINA_BASE

# System wide environment and startup programs, for login setup
```

追加した環境変数を読み込みます。

```
# source /etc/profile
```

5. tomcat6.confの修正（★）

Shibboleth IdP 2.4.3およびそれ以降をインストールする場合はこの手順は不要です。次の「6. httpd の設定」から先を行ってください。
バージョンが不明な場合は実行してかまいません。

$CATALINA_BASE/conf/tomcat6.conf を下記のように修正します。

CentOS 6 tomcat6パッケージにおいて、/usr/share/tomcat6/conf/XXX.conf と /etc/tomcat6/XXX.conf は同一ファイルです。

Apache Software FoundationのパッケージよりTomcatをインストールした場合は、本手順は必要ありません。（endorsedについては後の手順で設定します）

```
# Where your tomcat installation lives
CATALINA_BASE="/usr/share/tomcat6"
CATALINA_HOME="/usr/share/tomcat6"
JASPER_HOME="/usr/share/tomcat6"
CATALINA_TMPDIR="/var/cache/tomcat6/temp"
JAVA_ENDORSED_DIRS="${CATALINA_HOME}/endorsed"
```

6. httpd の設定（★）

実習セミナー

・ここで設定するホスト名は、各自IdPサーバのホスト名を設定してください。
例）1番を割り振られた場合
ex-idp-test01.gakunin.nii.ac.jp

/etc/httpd/conf/httpd.conf の修正

```
（省略）
ServerName example-idp.nii.ac.jp:80  ←ホスト名
（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
ProxyPass /idp/ ajp://localhost:8009/idp/    ←追加
（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
```

7. server.xmlの修正（★）

$CATALINA_BASE/conf/server.xmlを下記のように修正します。
他の用途で使用する予定がなければConnector port="8080"をコメントアウトしてください。

```
<!--
    <Connector port="8080" protocol="HTTP/1.1"
               connectionTimeout="20000"
               redirectPort="8443" />
-->
```

Connector port="8009"に以下のように追加してください。

```
<Connector port="8009" protocol="AJP/1.3" redirectPort="8443"
           enableLookups="false" tomcatAuthentication="false" address="127.0.0.1" maxPostSize="100000" />
```

---

4. Shibbolethのインストール（★）

各ファイル名等の指定は，Version 2.4.0に準拠しています。

1. shibboleth-IdP のダウンロード

Shibboleth IdPの最新版はバージョン3.0.0ですが、本技術ガイドは2.x.xをベースにしており、一部設定ファイルに互換性がありません。本技術ガイドの手順でIdPを構築する場合は、http://shibboleth.net/downloads/identity-provider/2.4.3/ からバージョン2.4.3(shibboleth-identityprovider-2.4.3-bin.zip)をダウンロードし続きを行ってください。

http://www.shibboleth.net/downloads/identity-provider/latest/から最新版のIdP
（shibboleth-identityprovider-2.?.?-bin.zip ）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（★）

実習セミナー

・shibboleth-IdPのパッケージは、「/root/PKG」配下にあります。
以下のコマンドで移動して、以降の手順を実施してください。
cd /root/PKG

shibboleth-idp-2.?.?-bin.zip 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。

```
# unzip shibboleth-identityprovider-2.?.?-bin.zip
# cd shibboleth-identityprovider-2.?.?
# ./install.sh
```

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。

実習セミナー

・インストール時に設定するホスト名は、各自IdPサーバのホスト名を設定してください。
例）1番を割り振られた場合
ex-idp-test01.gakunin.nii.ac.jp

```
Buildfile: src/installer/resources/build.xml

install:
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Be sure you have read the installation/upgrade instructions on the Shibboleth website before proceeding.
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Where should the Shibboleth Identity Provider software be installed? [/opt/shibboleth-idp]
[Enter] ←入力なし
What is the fully qualified hostname of the Shibboleth Identity Provider server? [idp.example.org]
upkishib-idp.nii.ac.jp[Enter] ←ホスト名
A keystore is about to be generated for you. Please enter a password that will be used to protect it.
keystore[Enter] ←任意のパスワード
Updating property file: /root/PKG/shibboleth-identityprovider-2.4.0/src/installer/resources/install.properties
（省略）
BUILD SUCCESSFUL
Total time: 54 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。
※途中で入力するパスワードはデフォルトで作成されるキーストアファイル(credentials/idp.jks)のパスワードとなります。このテキストでは使用しません。

3. SOAP通信用モジュール配置

（以前ここに記述されていた手順は、後の サーバ証明書の設定(IdP) の ２．ライブラリのコピー に移動しました。この段階でやるべきことはありません。）

4. Tomcatの設定（★）

⚠ Shibboleth IdP 2.4.3およびそれ以降をインストールする場合は本手順の endorsed/ ディレクトリの作成は不要です。次のディレクトリの所有者変更から先を実行してください。

/opt/shibboleth-idp/lib/endorsed/ にある5つの jarファイルを $CATALINA_HOME/endorsed ディレクトリを作成してそこへコピーします。

```
# mkdir $CATALINA_HOME/endorsed
# cp /opt/shibboleth-idp/lib/endorsed/*.jar $CATALINA_HOME/endorsed
```

以下はIdP 2.4.0の場合のファイル名例

serializer-2.10.0.jar
xalan-2.7.1.jar
xercesImpl-2.10.0.jar
xml-apis-2.10.0.jar
xml-resolver-1.2.jar

これらの jar ファイルが有効となるよう、tomcat 起動スクリプトを変更します。
前出の tomcat6 自動起動スクリプトを利用した場合は、以下のような有効化が記述されていることを確認してください。
（/etc/rc.d/init.d/tomcat6）

```
export CATALINA_OPTS="-Djava.endorsed.dirs=${CATALINA_HOME}/endorsed"
```

CentOS 6のtomcatパッケージではTomcatを”tomcat”ユーザで実行するため、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も変更します。

```
# chown -R tomcat: /opt/shibboleth-idp/logs
# chown -R tomcat: /opt/shibboleth-idp/metadata
```

5. idp.war の配置（★）

/opt/shibboleth-idp/war/idp.war ファイルを、${CATALINA_BASE}/webapps ディレクトリにコピーします。

```
# cp /opt/shibboleth-idp/war/idp.war ${CATALINA_BASE}/webapps/
```

httpdとTomcatを再起動します。

```
# service tomcat6 stop
# service httpd restart
# service tomcat6 start
```

Tomcatの起動後、${CATALINA_BASE}/logs/catalina.out にエラーが出力されていない事を確認してください。

※catalina.outにTomcat終了時（再起動時）のタイミングで以下のようなエラーが表示されることがありますが問題ありませんので無視してください。

```
致命的: A web application appears to have started a TimerThread named [Timer-0] via the java.util.Timer API but has failed to stop
it. To prevent a memory leak, the timer (and hence the associated thread) has been forcibly cancelled.
```

```
致命的: A web application created a ThreadLocal with key of type [null] (value [ch.qos.logback.core.
UnsynchronizedAppenderBase$1@XXXXXXXX]) and a value of type [java.lang.Boolean] (value [false]) but failed to remove it when the web
application was stopped. To prevent a memory leak, the ThreadLocal has been forcibly removed.
```

(関連するバグレポート)

---

5. サービスの起動・停止方法

httpd の起動方法

service httpd start

tomcat の起動方法

service tomcat6 start
sh /usr/java/tomcat/bin/startup.sh (起動スクリプトを利用しない場合)

httpd の停止方法

service httpd stop

tomcat の停止方法

service tomcat6 stop

sh /usr/java/tomcat/bin/shutdown.sh (起動スクリプトを利用しない場合)

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．
