Shibboleth IdP SP利用同意プラグイン (SPToUプラグイン) インストールマニュアル

---

1. インストール

1.1 前提条件

1.1.1 Shibboleth IdPのみで使用する場合

- Shibboleth Identity Provider 2.4.0以降
- MySQL 5.1

1.1.2 uApprove.jpと併用する場合

- Shibboleth Identity Provider 2.4.0以降
- MySQL 5.1
- uApprove.jp-2.2.1c以降

1.2 環境変数

- **$CATALINA_HOME**
  Tomcat のインストール先 (例: /usr/java/tomcat)
- **$IDP_HOME**
  Shibboleth IdP のインストール先 (例: /opt/shibboleth-idp)
- **$IDP_INSTALL**
  Shibboleth IdP をzipファイルを展開したディレクトリ (例: /opt/shibboleth-identityprovider-#version#)
- **$SPTOU_INSTALL**
  sptou-plagin-#version#-bin.zip を展開したディレクトリ (例: /tmp/sptou-plagin-#version#)

1.3 設定ファイルのインストール

設定ファイルを Shibboleth IdP の${IDP_HOME}/conf ディレクトリにコピーしてください:

```
# mkdir ${IDP_HOME}/conf/SPToU
# cp ${SPTOU_INSTALL}/configuration/* ${IDP_HOME}/conf/SPToU/
```

1.4 ライブラリのインストール

ライブラリを Shibboleth IdP の${IDP_INSTALL}/libにコピーしてください:

```
# cp ${SPTOU_INSTALL}/lib/* ${IDP_INSTALL}/lib/
```

1.5 Web アプリケーションファイルのインストール

webapp ディレクトリの Web アプリケーションファイルを Shibboleth IdP の${IDP_INSTALL}/webappディレクトリにインストールしてください:

```
# cd ${SPTOU_INSTALL}
# ant install -Didp.install=${IDP_INSTALL}
```

1.6 データベースの準備

⚠ 以下のデータベースパラメータは一例です。実際の値は必要に応じて変更してください。特にパスワードは安全なものを用意してください。

- **sptou** という名前のデータベースを作成します。
- ユーザ名 **sptou**, パスワード **sptou**　でデータベースのユーザを作成します。
- このユーザに INSERT, SELECT, UPDATE, DELETE 権限を与えます。
- 以下のスキーマ定義をつかってテーブルを作成します。

  ${SPTOU_INSTALL}/storage/sptou-schema.sql

2. Shibboleth IdPの再インストール

2.1 web.xml の編集

${IDP_INSTALL}/src/main/webapp/WEB-INF/web.xmlを編集します:

```
<web-app ...>
    <context-param>
        <param-name>contextConfigLocation</param-name>
        <param-value>$IDP_HOME$/conf/internal.xml; $IDP_HOME$/conf/service.xml; $IDP_HOME$/conf/SPToU/sptou-plugin.xml;</param-value>
    </context-param>
    <!-- Other Filters ... -->
    <!-- (GakuNin) SP Terms of Use -->
    <filter>
        <filter-name>SPToUFilter</filter-name>
        <filter-class>jp.gakunin.shibboleth.idpplugin.sptou.SPToUFilter</filter-class>
    </filter>
    <filter-mapping>
        <filter-name>SPToUFilter</filter-name>
        <url-pattern>/profile/Shibboleth/SSO</url-pattern>
        <url-pattern>/profile/SAML2/Redirect/SSO</url-pattern>
    </filter-mapping>
    <!-- Other Servlets ... -->
    <!-- (GakuNin) SP Terms of Use -->
    <servlet>
        <servlet-name>SPToUServlet</servlet-name>
        <servlet-class>jp.gakunin.shibboleth.idpplugin.sptou.SPToUServlet</servlet-class>
    </servlet>
    <servlet-mapping>
        <servlet-name>SPToUServlet</servlet-name>
        <url-pattern>/SPToU/SPToUServlet</url-pattern>
    </servlet-mapping>
    <!-- Others ... -->
</web-app>
```

ⓘ

- filterおよびfilter-mappingの定義はweb.xmlの他のfilterおよびfilter-mappingより後に記述しなければなりません。
- uApprove.jp と併用する場合は、 uApprove.jp の定義より前に記述しなければなりません。

uApprove.jpと併用する場合は、uApprove.jpの<filter-mapping>は、以下のように修正する必要があります:

変更前:

```
    <filter-mapping>
        <filter-name>uApprove.jp IdP plugin</filter-name>
        <url-pattern>/*</url-pattern>
        <dispatcher>REQUEST</dispatcher>
        <dispatcher>FORWARD</dispatcher>
    </filter-mapping>
```

変更後:

```
    <filter-mapping>
        <filter-name>uApprove.jp IdP plugin</filter-name>
        <url-pattern>/profile/*</url-pattern>
        <url-pattern>/AuthnEngine</url-pattern>
        <url-pattern>/Authn/*</url-pattern>
        <dispatcher>REQUEST</dispatcher>
        <dispatcher>FORWARD</dispatcher>
    </filter-mapping>
```

2.2 idp.warのデプロイ

プラグインを有効にするため、idp.warを再デプロイします:

```
# cd ${IDP_INSTALL}
# ./install.sh
```

idp.warを${CATALINA_HOME}/webappsにコピーします:

```
# cp ${IDP_HOME}/war/idp.war $CATALINA_HOME/webapps/
```

3. SPToUプラグイン設定

3.1 ${IDP_HOME}/conf/SPToU/sptou-plugin.xml

3.1.1 context:property-placeholder

locationの値を設定します:
変更前:

```
<context:property-placeholder location="file://$IDP_HOME$/conf/SPToU/sptou.properties" />
```

変更後:

```
<context:property-placeholder location="file:///opt/shibboleth-idp/conf/SPToU/sptou.properties" />
```

3.1.2 SPToUMapping

propertyfileの値を設定します:
変更前:

```
    <bean id="SPToUMapping" class="jp.gakunin.shibboleth.idpplugin.sptou.SPToUMapping" init-method="initialize">
        <property name="propertyfile">
            <value>$IDP_HOME$/conf/SPToU/sptoumapping.properties</value>
        </property>
    </bean>
```

変更後:

```
    <bean id="SPToUMapping" class="jp.gakunin.shibboleth.idpplugin.sptou.SPToUMapping" init-method="initialize">
        <property name="propertyfile">
            <value>/opt/shibboleth-idp/conf/SPToU/sptoumapping.properties</value>
        </property>
    </bean>
```

3.1.3 AcceptanceStorage

sqlStatementsの値を設定します:
変更前:

```
     <bean id="AcceptanceStorage"
             class="jp.gakunin.shibboleth.idpplugin.sptou.StorageImpl"
             init-method="initialize" p:dataSource-ref="gakunin.dataSource">
        <property name="sqlStatements">
            <value>$IDP_HOME$/conf/SPToU/sql-statements.properties</value>
        </property>
    </bean>
```

変更後:

```
     <bean id="AcceptanceStorage"
             class="jp.gakunin.shibboleth.idpplugin.sptou.StorageImpl"
             init-method="initialize" p:dataSource-ref="gakunin.dataSource">
        <property name="sqlStatements">
            <value>/opt/shibboleth-idp/conf/SPToU/sql-statements.properties</value>
        </property>
    </bean>
```

3.2 ${IDP_HOME}/conf/SPToU/sptou.properties

あなたのデータベース環境に合せて、${IDP_HOME}/conf/SPToU/sptou.propertiesのプロパティを修正します:

```
database.driver     = com.mysql.jdbc.Driver
database.url        = jdbc:mysql://localhost:3306/sptou?characterEncoding=utf8
database.username   = sptou
database.password   = sptou
```

3.3 ${IDP_HOME}/conf/SPToU/sptoumapping.properties

SP のエンティティID(sp.*N*.entityID)とSPの利用条件定義ファイル(sp.*N*.ToU)を関連づけて定義します:

sptoumapping.propertiesの設定例

```
sp.1.entityID=https://sp1.example.ac.jp/shibboleth
sp.1.ToU=/opt/shibboleth-idp/conf/SPToU/tou-example.ac.jp.xml
sp.2.entityID=https://sp2.example.ac.jp/shibboleth
sp.2.ToU=/opt/shibboleth-idp/conf/SPToU/tou-example.ac.jp.xml
sp.3.entityID=https://sp.example2.co.jp/shibboleth
sp.3.ToU=/opt/shibboleth-idp/conf/SPToU/tou-example2.co.jp.xml
sp.5.entityID=https://sp.example.com/shibboleth
sp.5.ToU=/opt/shibboleth-idp/conf/SPToU/tou-example.com.xml
```

*N*の値は連番である必要はありません。

- sp.X.entityIDに対応するsp.X.ToUが存在しない場合は、sp.X.entityIDの設定は無視されます。
- sp.Y.ToUに対応するsp.Y.entityIDが存在しない場合は、sp.Y.ToUの設定は無視されます。
- sp.*N*.ToUに設定したファイルが読めない場合(ファイルが存在しない、パーミッションが間違えているなど)は、IdPの起動に失敗します。

3.4 利用条件定義ファイル

利用条件はXML形式で定義します:

利用条件定義ファイルの設定例

```
<?xml version="1.0" encoding="UTF-8"?>
<TermsOfUse>
        <version>1.0</version>
        <text><![CDATA[Example Service Terms of use (ToU) version 1.0

This is an empty template for the sptou-example.xml version.
Please adjust it according to the terms of use.
]]></text>
</TermsOfUse>
```

- **<version>**: 利用条件のバージョン (104 字以下)
- **<text>**: 利用条件のテキスト (8190 字以下)

4. Tomcatの再起動

Tomcatを再起動します:

```
# service tomcat6 restart
```

5. トラブルシューティング

5.1 ログ出力

ログを出力するには、Shibboleth IdPの${IDP_HOME}/conf/logging.xmlで設定します:

```
    <logger name="jp.gakunin.shibboleth.idpplugin.sptou" level="WARN"/>
```