IdPとのSP接続確認

IdPとのSP接続確認

※接続確認に使用する IdP の設定変更も必要となります。設定変更は IdP の管理者に依頼して下さい。

1. SP にテスト用のWebページを準備

以下のような/var/www/html/secure/phpinfo.phpを作成します。

```
<?php phpinfo(); ?>
```

または、属性確認用の簡単なPHPプログラムをご利用下さい。　ダウンロード 説明

---

2. shibdとhttpdの再起動

接続確認前にshibdとhttpdを再起動します。

```
# systemctl restart shibd
# systemctl restart httpd
```

```
  # service shibd restart
  # service httpd restart
```

---

3. 構築したSPにアクセス

https://sp.example.ac.jp/secure/phpinfo.php

SPへのアクセス時にエラー

SPにアクセスした際に、ブラウザに下記のエラーが出力されます。

```
shibsp::ListenerException

The system encountered an error at Wed Aug 17 19:09:20 2016

To report this problem, please contact the site administrator at
root@xxxxx.

Please include the following message in any email:

shibsp::ListenerException at (https://xxx.xxxxx.xx.xx/secure)

Cannot connect to shibd process, a site adminstrator should be notified.
```

SELinuxがenabledになっている場合、このメッセージが表示されます。

SELinuxを無効にしてください。

ログインボタンを押した際にエラー（エラー：無効なクエリです）

SP画面にてログインを押した際に、ブラウザに下記のエラーが出力されます。 

```
エラー: 無効なクエリです
The Service Provider 'https://xxx.xxx.xx.xx/xxx' could not be found in metadata and is therefore unknown.
```

→/etc/shibboleth/shibboleth2.xmlファイルのentityID設定が間違っている場合に表示されます。

参考情報： SPセッティング ー shibboleth2.xml ファイル（★）

ログインボタンを押した際にエラー（サーバが見つからない）

SP画面にてログインを押した際に、ブラウザに下記のエラーが出力されます。 

```
IE:
このページは表示できません
Web アドレス https://xxx.xxx.xxx.xx が正しいか確かめてください。


Firefox:
サーバが見つかりませんでした
xxx.xxx.xxx.xx という名前のサーバが見つかりませんでした。
```

→/etc/shibboleth/shibboleth2.xmlファイルのDSサーバ参照設定のURLが間違っている可能性があります。

参考情報： SPセッティング ー shibboleth2.xml ファイル（★）

---

4. DSのIdP選択画面が表示

DSのIdP選択画面で、対象となるテストIdPを選択します。

※学認DSについての注意点：
一度選択したIdPが表示されている状態で、別のIdPを選択したい場合は、
「リセット」リンクをクリックすると選択可能な全てのIdPが表示されます。

IdPを選択した際にエラー（shibsp::ConfigurationException）

所属機関の選択画面にてIdPを選び「選択」ボタンを押した際に、ブラウザに下記のエラーが出力されます。 

```
shibsp::ConfigurationException
The system encountered an error at Tue Jan 01 00:00:00 2013
To report this problem, please contact the site administrator at root@localhost.
Please include the following message in any email:
shibsp::ConfigurationException at (https://ex-sp-testxx.gakunin.nii.ac.jp/Shibboleth.sso/DS)
No MetadataProvider available.
```

また、/var/log/shibboleth/shibd_warn.log に下記のエラーが出力されます。

```
2013-01-01 00:00:00 ERROR OpenSSL : error code: 33558530 in bss_file.c, line 355
2013-01-01 00:00:00 ERROR OpenSSL : error data: fopen('/etc/shibboleth/cert/xxxx.cer','r')
2013-01-01 00:00:00 ERROR OpenSSL : error code: 537346050 in bss_file.c, line 357
2013-01-01 00:00:00 ERROR OpenSAML.Metadata : caught exception while installing filters: Unable to load certificate(s) from file (/etc
/shibboleth/cert/xxxx.cer).
```

→/etc/shibboleth/shibboleth2.xmlにてメタデータ署名検証用証明書の設定が間違っている可能性があります。
実習セミナー環境での当該証明書は「ex-fed.crt」となっています。ファイルが指定場所にあるか、ファイル名が間違っていないか確認ください。
テストフェデレーション、運用フェデレーションにおける当該証明書については技術ガイドのSPセッティング ー shibboleth2.xml ファイルを参照下さい。

---

5. ログイン

IDとPasswordを入力してログインします。

ID, パスワードを入力してログインした後、表示される環境変数に、IdPで公開するように設定した値(LDAPに保存されている eduPersonPrincipalNameなど)が含まれていることを確認します。
これが、IdPから渡されたユーザの属性情報となります。

属性値が全てNOT RECEIVEDになってしまう

ログイン後の各属性値の表示画面にて、値を取得できずにNOT RECEIVEDが表示されます。
また、/var/log/shibboleth/shibd_warn.log に下記のエラーが出力されます。

```
2013-01-01 00:00:00 ERROR Shibboleth.AttributeResolver.Query [1]: exception during SAML query to https://xxx.xxx.xxx.xx:8443/idp
/profile/SAML2/SOAP/AttributeQuery: CURLSOAPTransport failed while contacting SOAP endpoint (https://xxx.xxx.xxx.xx:8443/idp/profile
/SAML2/SOAP/AttributeQuery): Failed connect to xxx.xxx.xxx.xx:8443; Connection refused
2013-01-01 00:00:00 ERROR Shibboleth.AttributeResolver.Query [1]: unable to obtain a SAML response from attribute authority
```

→接続先IdPのattribute-filter.xmlにSPが設定されていない可能性があります。実習環境では、IdP選択時に「選択ボタン」下のリセットを押し、実習セミナー接続確認用IdPを選択しなおして下さい。

表示例）
phpinfoの場合

PHP Variables

variable	value
_SERVER["unscoped-affiliation"]	faculty

---

6. メタデータ署名検証が正常に機能していることの確認

shibboleth2.xmlに設定した取得するメタデータを改竄されたものに変更して、適切に署名検証が失敗することを確認してください。

shibboleth2.xmlの以下の部分を修正し、shibdを再起動してください。（元がgakunin-test-metadata.xmlの場合はgakunin-test-metadata-tampered.xmlに修正してください）

```
        <MetadataProvider type="XML" uri="https://metadata.gakunin.nii.ac.jp/gakunin-metadata-tampered.xml"
```

メタデータの署名検証に失敗した場合には、SPのログファイル(/var/log/shibboleth/shibd_warn.log)に以下の様なメッセージが出力されます。

```
2012-08-30 14:45:07 WARN OpenSAML.MetadataFilter.Signature : filtering out group at root of instance after failed signature check:
Unable to verify signature with supplied key(s).
```

ただし、検証に失敗しても、以前に検証にパスしたメタデータがバッキングファイルにあればそれを読み込んでSPは起動するのでご注意ください。バッキングファイルが存在しなければ、信頼するメタデータが無い状態で起動します（いずれのIdPに接続しようとしてもそのIdPのメタデータが見つからない旨エラーが表示されます）。

バッキングファイルは /var/cache/shibboleth/federation-metadata.xml にあります。

確認後は、元に戻すのを忘れないでください。

BACK TOP