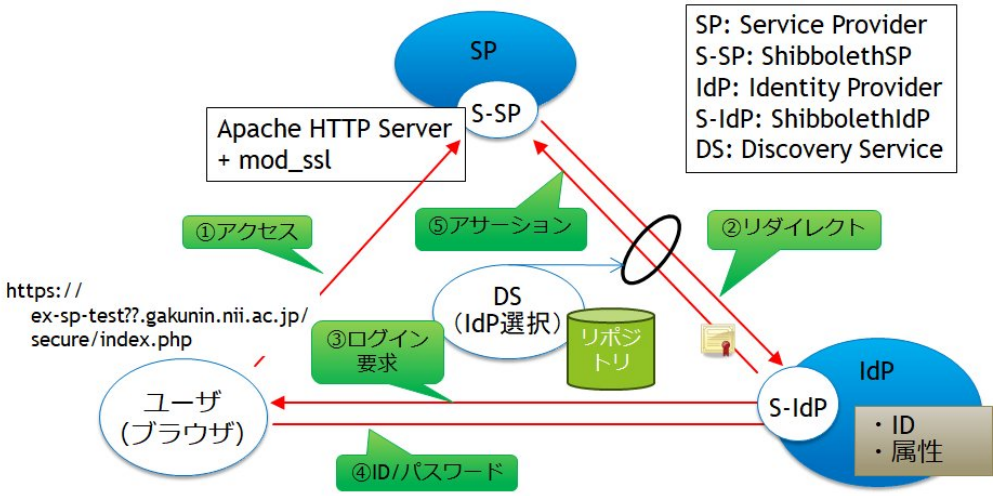
接続確認（IdPとのSP）2023

2. IdPとのSP接続確認

これは、下図のようにユーザ端末のブラウザからhttp://…というURLにアクセスし、①から⑤の機能が赤線のように通信しあって結果を表示する動作を確認するものです。



2.1. attribute-map.xml, attribute-policy.xmlの準備

attribute-map.xml、attribute-policy.xmlファイルを差し替えます。

初期設定で「/root/GETFILE」に取得している実習セミナー用のattribute-map.xml、attribute-policy.xmlファイルを「/etc/shibboleth」配下にコピーし、デフォルトのファイルを差し替えてください。
この設定ファイルは、実習セミナー内のIdPサーバから全属性値を受け取る設定となっています。

```
確認（cpコマンド実行前）

# ls -l /etc/shibboleth/attribute-*.xml

-rw-r--r-- 1 root root 9565  1月 11 05:25 /etc/shibboleth/attribute-map.xml
-rw-r--r-- 1 root root 3084  1月 11 05:25 /etc/shibboleth/attribute-policy.xml

# /bin/cp -f /root/GETFILE/attribute-*.xml /etc/shibboleth/

確認(ファイルの日付けが更新されていること)

# ls -l /etc/shibboleth/attribute-*.xml

-rw-r--r-- 1 root root 11739  7月  5 18:33 /etc/shibboleth/attribute-map.xml
-rw-r--r-- 1 root root  4068  7月  5 18:33 /etc/shibboleth/attribute-policy.xml
```

2.2. shibdとhttpdの再起動

設定ファイルを差し替えたら、shibdおよびhttpdを再起動してください。

接続確認前にshibdとhttpdを再起動します。

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

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

```
2023-06-21 00:31:15 WARN Shibboleth.DEPRECATION : MetadataGenerator handler
```

→/etc/shibboleth/shibboleth2.xml ファイルに次のような行がありますが、本メッセージは無視して下さい。

```
<Handler type="MetadataGenerator" Location="/Metadata" signing="false"/>
```

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

```
2023-06-22 18:41:55 WARN Shibboleth.DEPRECATION : legacy Attribute Filter namespace 'urn:mace:shibboleth:2.0:afp:mf:basic'
```

→/etc/shibboleth/attribute-policy.xmlファイルに次のような行がありますが、本メッセージは無視して下さい。

```
<afp:AttributeFilterPolicyGroup
  xmlns="urn:mace:shibboleth:2.0:afp:mf:basic"
  xmlns:saml="urn:mace:shibboleth:2.0:afp:mf:saml"
  xmlns:basic="urn:mace:shibboleth:2.0:afp:mf:basic"
  xmlns:afp="urn:mace:shibboleth:2.0:afp"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
```

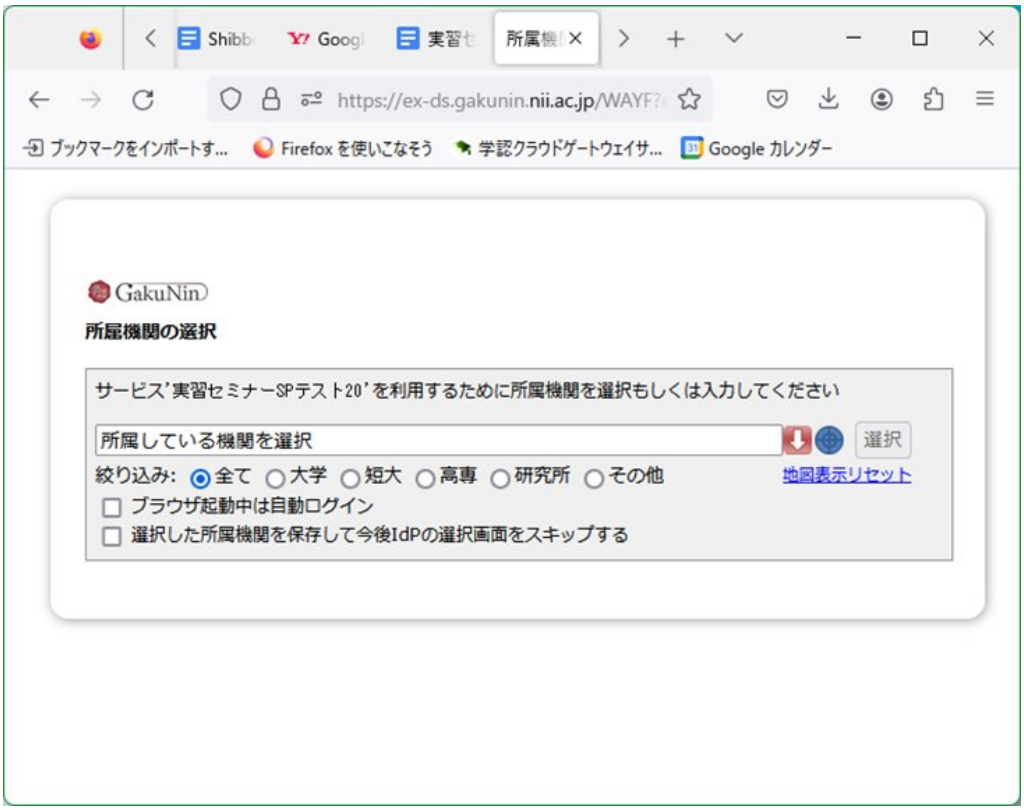
2.3. 構築したSPにアクセス

SPサーバへアクセスします。

以下のアドレスを各自のホスト名に変更してアクセスしてください。

https://ex-sp-test??.gakunin.nii.ac.jp/secure/index.php
↑「??」には割り当てられた番号を記述

次のような画面が表示されます。



実習セミナー

・「/var/www/html/secure/index.php」という属性確認用のPHPファイルが既に配置済みです。

・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:
正常に接続できませんでした
xxx.xxx.xxx.xx への接続中にエラーが発生しました。
```

→/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。

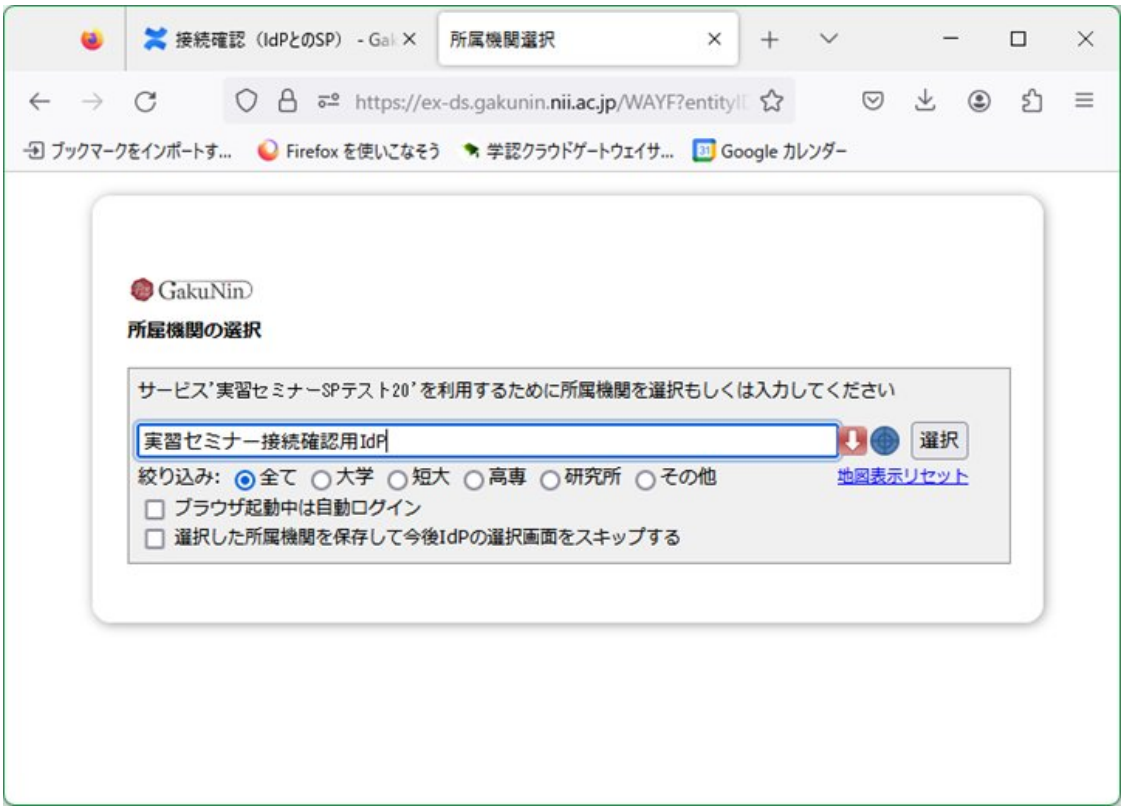
参考情報： SPセッティング ー shibboleth2.xml ファイル（★）

2.4. DSのIdP選択画面が表示

実習環境内にある確認用のIdPサーバを選択します。

以下を選択してください。

実習セミナー接続確認用IdP

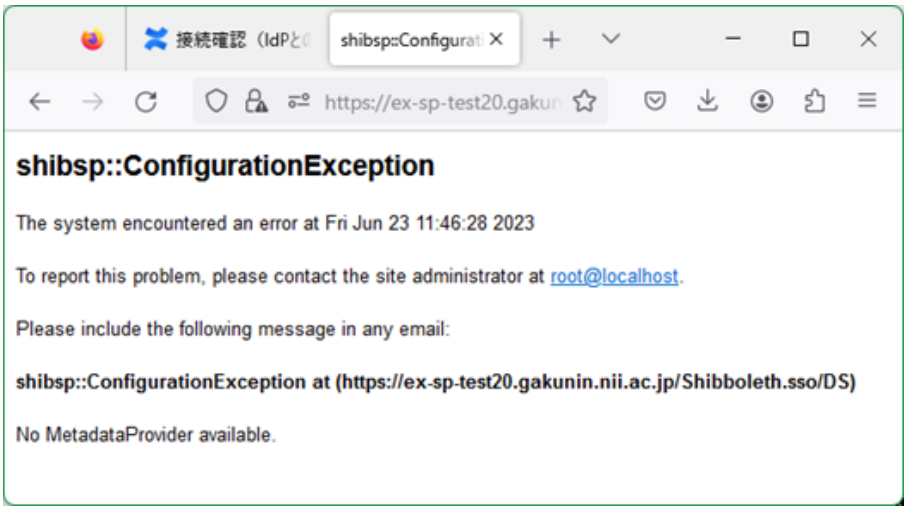


実習セミナー

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。

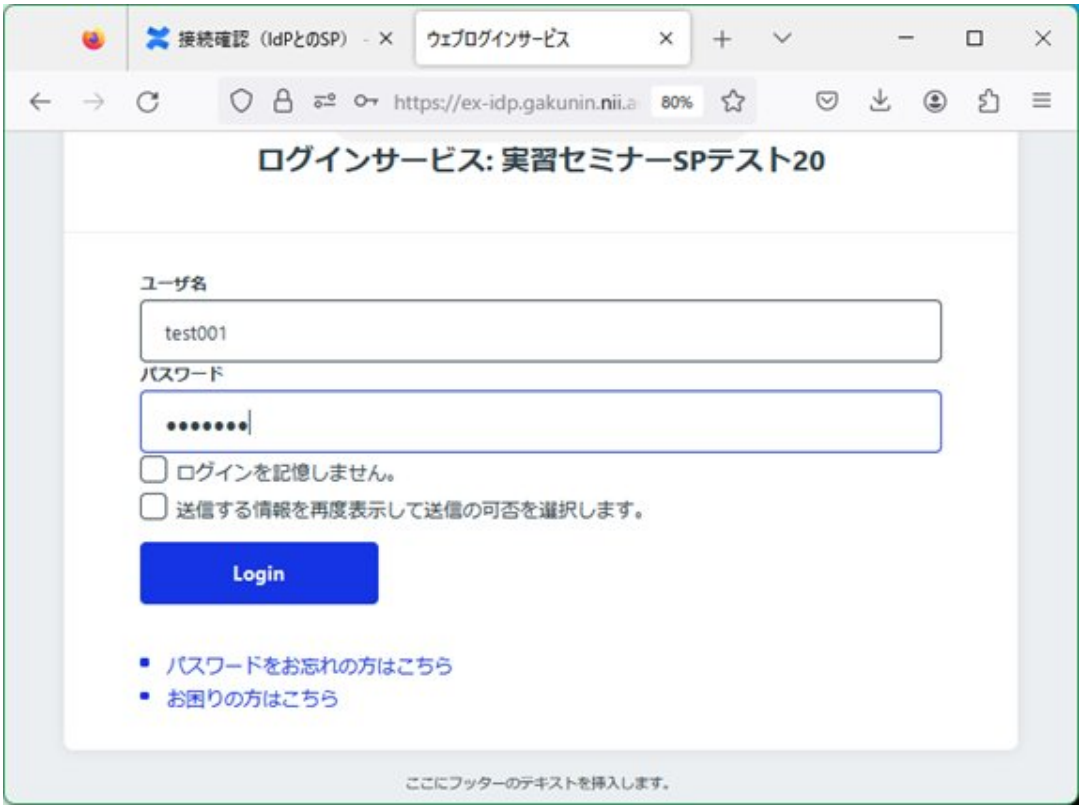
```
2013-01-01 00:00:00 ERROR OpenSSL : error code: 33558530 in bss_file.c, line 355
2013-01-01 00:00:00 ERROR OpenSSL : error data: fopen('/etc/shibboleth/cert/xxxx.cer','r')
2013-01-01 00:00:00 ERROR OpenSSL : error code: 537346050 in bss_file.c, line 357
2013-01-01 00:00:00 ERROR OpenSAML.Metadata : 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

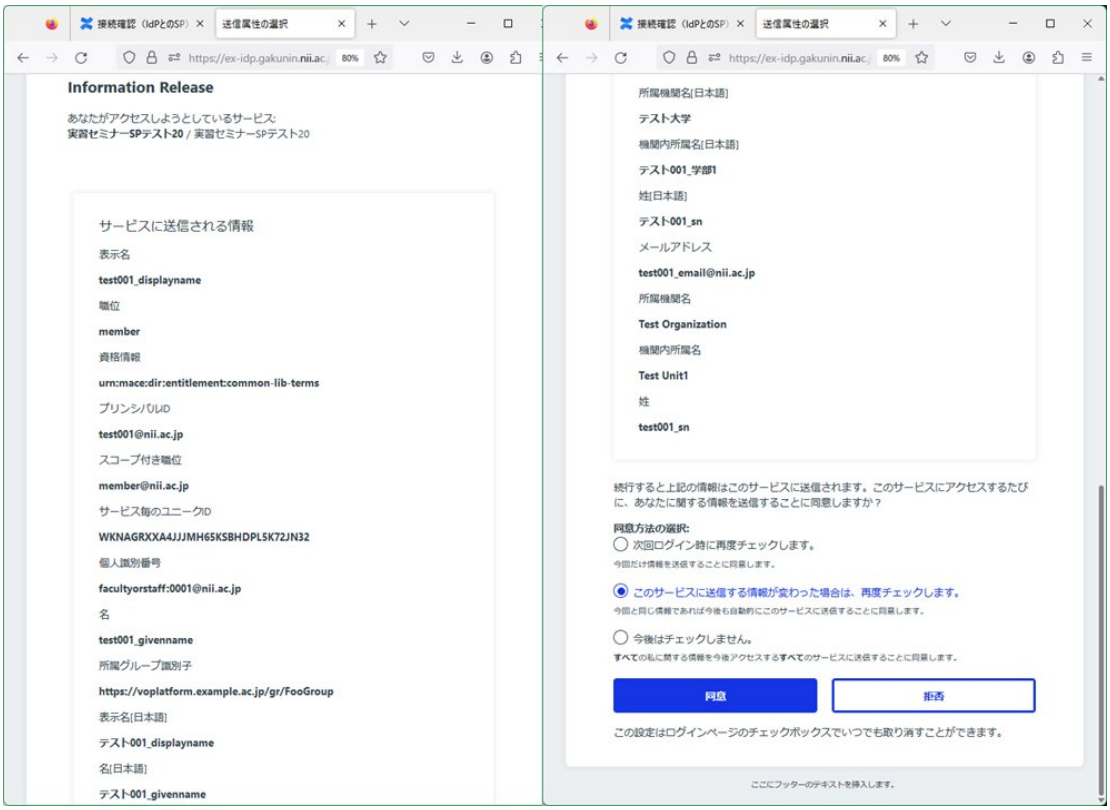
IDとPasswordを入力してログインします。



実習セミナー

・接続確認用ユーザ情報は、以下のようになっています。
ID：test001、パスワード：test001
ID：test002、パスワード：test002
ID：test003、パスワード：test003
何れかを使用して、ログインしてください。

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。（次の図）



「同意」ボタンをクリックすると、次の画面に遷移する。
これが、IdPから渡されたユーザの属性情報となります。
eduPersonPrincipalNameが含まれていることを確認できます。

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
```

または、

```
2023-07-18 15:21:28 CRIT Shibboleth.Application : error building AttributeFilter: Unable to access local file (/etc/shibboleth/attribute-policy1.
xml)

2023-07-18 15:21:28 CRIT Shibboleth.Application : installing safe AttributeFilter in place of failed version

2023-07-18 15:22:14 WARN Shibboleth.AttributeFilter.Dummy [1] [default]: filtering out all attributes
```

→/etc/shibboleth/shibboleth2.xml ファイルのAttributesFilter参照設定忘れや設定ミスの可能性があります。

参考情報：

SPセッティング ー shibboleth2.xml ファイル（★）

2.1.attribute-map.xml, attribute-policy.xmlの準備

BACK TOP