

接続テスト

テストアカウントで接続確認する

1. httpdとTomcatの再起動 (★)

接続確認前にhttpdとTomcatを再起動します。 (★)

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

2. テストSPにアクセス (★)

テストSPにアクセスしログインを行ってください。学認のテストSPは[技術ガイド](#)に記載しています。画面中央の「接続テスト」リンクをクリックしてください。



実習セミナー

- ・実習セミナー内のSPサーバにアクセスして、確認します。
<https://ex-sp.gakunin.nii.ac.jp/>

3. DSのIdP選択画面が表示 (★)

DSのIdP選択画面から構築した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選択時にブラウザにエラー (HTTPステータス 404 -)

IdPを選択した際に、ブラウザに下記のエラーが出力されます。



```
HTTPステータス 404 -
type ステータスレポート
メッセージ
説明 The requested resource () is not available.
```

→IdPの各種設定ファイルにて記述ミスの可能性があります。

ログファイル /opt/shibboleth-idp/logs/idp-process.log を確認して下さい。（下記の"HandlerManager"や"RelyingPartyConfigurationManager"の部分で、どの設定ファイルに問題があるか判別可能です）

- /opt/shibboleth-idp/conf/handler.xml にて記述ミスがある場合

```
00:00:00.000 - ERROR [edu.internet2.middleware.shibboleth.common.config.BaseService:188] - Configuration was not loaded for
shibboleth.HandlerManager service, error creating components. The root cause of this error was: org.xml.sax.
SAXParseException: The content of elements must consist of well-formed character data or markup.
```

- /opt/shibboleth-idp/conf/relying-party.xmlにて検証用証明書の設定が間違っている場合

```
00:00:00.000 - ERROR [edu.internet2.middleware.shibboleth.common.config.BaseService:188] - Configuration was not loaded for shibboleth.RelyingPartyConfigurationManager service, error creating components. The root cause of this error was: java.io.FileNotFoundException: /opt/shibboleth-idp/credentials/gakunin-signer-2010.cer (No such file or directory)
```

→実習セミナー環境での検証用証明書は「**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検証用証明書については技術ガイドの[relying-party.xml ファイルの確認](#)を参照ください。

- /opt/shibboleth-idp/conf/relying-party.xmlのMetadata Configuration付近にて記述ミスがある場合

```
00:00:00.000 - ERROR [edu.internet2.middleware.shibboleth.common.config.BaseService:188] - Configuration was not loaded for shibboleth.RelyingPartyConfigurationManager service, error creating components. The root cause of this error was: org.xml.sax.SAXParseException: cvc-complex-type.2.3: Element 'metadata:MetadataProvider' cannot have character [children], because the type's content type is element-only.
```

- /opt/shibboleth-idp/conf/relying-party.xmlのProfileConfiguration付近にて記述ミスがある場合

```
00:00:00.000 - ERROR [edu.internet2.middleware.shibboleth.common.config.BaseService:188] - Configuration was not loaded for shibboleth.RelyingPartyConfigurationManager service, error creating components. The root cause of this error was: org.xml.sax.SAXParseException: Element type "rp:ProfileConfiguration" must be followed by either attribute specifications, ">" or ">".
```

- idp-process.logにエラーが出ていない場合、\$CATALINA_HOME/endorsedフォルダにjarファイルがコピーできていない可能性もあります
参考情報：[貴学にてIdPをインストールする場合の構築手順](#) - 4. Shibbolethのインストール (★) - 4. Tomcatの設定 (★)

IdP選択時にページが見つからない (404 Not Found)

IdPを選択した際に、Webページが見つからない、404 Not Foundといったエラーがブラウザに表示されます。



IE :

Webページが見つかりません。HTTP 404

可能性のある原因:

- ・アドレスに入力ミスがある。
- ・リンクをクリックした場合に、リンクが古い場合があります。

Firefox :

サーバが見つかりませんでした。

→/etc/httpd/conf.d/ssl.conf にて記述ミスの可能性があります。

参考情報：[貴学にてIdPをインストールする場合の構築手順](#) - 3. jdk6、tomcat6をインストールする (★) - 5. httpd の設定 (★)

IdP選択時にブラウザにエラー (HTTPステータス 404 - /idp/profile/SAML2/Redirect/SSO)

IdPを選択した際に、ブラウザに下記のエラーが出力されます。



HTTPステータス 404 - /idp/profile/SAML2/Redirect/SSO

type ステータスレポート

メッセージ /idp/profile/SAML2/Redirect/SSO

説明 The requested resource (/idp/profile/SAML2/Redirect/SSO) is not available.

→\$CATALINA_HOME/webappsにidp.warファイルがきちんとコピーできていない可能性があります。

参考情報：[貴学にてIdPをインストールする場合の構築手順](#) - 4. Shibbolethのインストール (★) - 5. idp.war の配置 (★)

4. ログイン (★)

設定したIDとPasswordを利用してログイン (★)



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。
これが、SPへ送信したユーザの属性情報となります。

IdPで認証時にエラー (Error Message:Error decoding authentication request mesaage)

IdP選択後、認証画面にてログインした際に、ブラウザに下記のエラーが出力されます。



Error Message:Error decoding authentication request mesaage

また、/opt/shibboleth-idp/logs/idp-process.log に下記のエラーが出力されます。

```
00:00:00.000 - ERROR [edu.internet2.middleware.shibboleth.idp.authn.AuthenticationEngine:618] - No user identified by login handler.  
00:00:00.000 - ERROR [edu.internet2.middleware.shibboleth.idp.authn.AuthenticationEngine:563] - Authentication failed with the error:
```

→/opt/shibboleth-idp/conf/handler.xml にて記述ミスの可能性があります。

参考情報 : [IdPセッティング - handler.xml ファイルの変更 \(★\)](#)

IdPで認証時にエラー (Credentials not recognized.)

IdP選択後、認証画面にてログインした際に、ブラウザに下記のエラーが出力されます。



Credentials not recognized.

また、/opt/shibboleth-idp/logs/idp-process.log に下記のエラーが出力されます。

```
00:00:00.000 - WARN [edu.vt.middleware.ldap.auth.SearchDnResolver:1105] - Error performing LDAP operation, retrying (attempt 0)
```

→/opt/shibboleth-idp/conf/login.config にて記述ミスの可能性があります。

参考情報 : [IdPセッティング - login.config ファイルの変更 \(★\)](#)

IdPで認証時にエラー(Message was signed, but signature could not be verified)

IdP選択後、認証画面にてログインした際に、ブラウザに下記のエラーが出力されます。



```
opensaml::FatalProfileException at (https://ex-sp.gakunin.nii.ac.jp/Shibboleth.sso/SAML2/POST)
Message was signed, but signature could not be verified.
```

→ [トラブルシューティング](#) を参照下さい。

表示例) phpinfoの場合

PHP Variables

variable	value
_SERVER["unscoped-affiliation"]	faculty

5. メタデータ署名検証が正常に機能していることの確認



実習セミナー

- ・実習セミナーでは改竄されたメタデータが用意されていないのでこの項目は飛ばしてください。

relying-party.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。
relying-party.xmlの以下の部分を修正し、Tomcat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）

```
<metadata:MetadataProvider id="URLMD" xsi:type="metadata:FileBackedHTTPMetadataProvider"
    metadataURL="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、IdPのログファイル(/opt/shibboleth-idp/logs/idp-process.log)に以下の様なメッセージが出力されます。

```
11:44:03.060 - ERROR [org.opensaml.saml2.metadata.provider.SignatureValidationFilter:311] - Signature trust establishment failed for
metadata entry URLMD
11:44:03.067 - ERROR [org.opensaml.saml2.metadata.provider.AbstractReloadingMetadataProvider:393] - Error filtering metadata from
https://metadata.gakunin.nii.ac.jp/gakunin-metadata-tampered.xml
org.opensaml.saml2.metadata.provider.FilterException: Signature trust establishment failed for metadata entry
    at org.opensaml.saml2.metadata.provider.SignatureValidationFilter.verifySignature(SignatureValidationFilter.java:312) ~
[opensaml-2.5.3.jar:na]
(...略...)
11:44:03.071 - ERROR [org.opensaml.saml2.metadata.provider.AbstractMetadataProvider:411] - Metadata provider failed to properly
initializing, halting
org.opensaml.saml2.metadata.provider.MetadataProviderException: org.opensaml.saml2.metadata.provider.MetadataProviderException: Error
filtering metadata from https://metadata.gakunin.nii.ac.jp/gakunin-metadata-tampered.xml
    at org.opensaml.saml2.metadata.provider.AbstractReloadingMetadataProvider.refresh(AbstractReloadingMetadataProvider.java:266)
~[opensaml-2.5.3.jar:na]
(...略...)
11:44:03.073 - ERROR [edu.internet2.middleware.shibboleth.common.config.BaseService:188] - Configuration was not loaded for
shibboleth.RelyingPartyConfigurationManager service, error creating components. The root cause of this error was: org.opensaml.saml2.
metadata.provider.FilterException: Signature trust establishment failed for metadata entry
```

検証に失敗した場合、起動に失敗しますのでIdPで認証しようとする代わりにエラー画面(HTTP Status 404)が表示されます。また、この時点でバック
キングファイルは改竄されたもので上書きされていますので、バックキングファイルを使って復旧することもできません。

バックキングファイルは /opt/shibboleth-idp/metadata/some-metadata.xml にあります。

確認後は、設定を元に戻すのを忘れないでください。

