実習セミナー環境について（研究クラウド）

事前作業（研究クラウド環境）

IdP、又はSPの構築を行うサーバ (Linux/CentOS)のインスタンスは、既に研究クラウド上に起動されており、
Tera Termでログインすることができます。以下の手順に従って、初期設定を実施してください。
※使用するサーバは、「**CentOS7 64bit**」です。

1. VPN接続　**※旧環境の説明の為、実施不要**

タスクバー上のVPNクライアントソフトをクリックして起動します。
上部にある「GakuNin」をダブルクリックします。
接続が完了すると「VPN通信が可能になりました。」とダイアログが表示されます。
接続後、VPNクライアントソフトは閉じて問題ありません。

2. 初期設定ツールの実行　**※旧環境の説明の為、実施不要**

割り当てられた作業を行うサーバにTera Termでログインします。
Tera Termを起動するとIdP構築用とSP構築用のホスト名が選択できます。
例）1番を割り振られた場合のIdP
ex-idp-test01.gakunin.nii.ac.jp

例）10番を割り振られた場合のSP
ex-sp-test10.gakunin.nii.ac.jp

ユーザ名／パスフレーズを入力後、秘密鍵ボタンより秘密鍵を選択してください。
選択画面に表示された「id_rsa」を選択し、OKボタンをクリックしてログインします。
ログイン後、以下のように初期設定シェルスクリプトを実行してください。

/root/TOOL/initSetting.sh *割り振られた番号 構築サーバ種別*
※構築サーバ種別は、”idp”か”sp”を選択します。

例）1番を割り振られた受講生がIdPを構築する場合
/root/TOOL/initSetting.sh 1 idp

例）10番を割り振られた受講生がSPを構築する場合
/root/TOOL/initSetting.sh 10 sp

初期設定スクリプトが取得したファイルは、「/root/GETFILE」に保存されます。

注意：作業を行なっているサーバのシャットダウンは、行わないでください。
　　再起動は良いですが、シャットダウンしてしまうと、インスタンスが停止してしまい、
　　構築を行った設定やファイルがなくなってしまいます。

Shibboleth構築作業について

1. IdP構築：接続確認までの流れ

1) Javaのインストール

2) Jettyのインストール

・Shibboleth用各種設定ファイル群(jetty-base)の設定など

3) Shibboleth-IdPのインストール

4) Shibboleth-IdPの設定
・メタデータの自動ダウンロード設定
・証明書の設定
・認証時のLDAP接続設定

・NameIDの設定

・LDAPのパスワードやSalt値の設定

変更ファイル: metadata-providers.xml, idp.properties, ldap.properties, saml-nameid.properties, secrets.properties

5) SPへの送信属性に関する設定
※実習セミナーでは、設定済みファイルに置き換え
変更ファイル: attribute-resolver.xml, attribute-filter.xml

6) ApacheおよびIdPへの証明書の設定
変更ファイル: ssl.conf

7) メタデータの作成と提出

8) 講師用のSPを使った接続確認

2. SP構築：接続確認までの流れ

1) Shibboleth-SPのインストール
変更ファイル: ssl.conf

2) Shibboleth-SPの設定
・EntityIDの設定
・DSの参照設定
・メタデータの自動ダウンロード設定
変更ファイル: shibboleth2.xml

3) ApacheおよびSPへの証明書の設定
変更ファイル: ssl.conf, shibboleth2.xml

4) メタデータの作成と提出

5) IdPからの受信属性に関する設定
※実習セミナーでは、設定済みファイルに置き換え
変更ファイル: attribute-map.xml, attribute-policy.xml

6) 講師用のIdPを使った接続確認

実習セミナー環境での設定ホスト一覧（研究クラウド環境）

```
DS：
  ex-ds.gakunin.nii.ac.jp
  ※SPに設定するDSのURL
    →https://ex-ds.gakunin.nii.ac.jp/WAYF

LDAPサーバ：
  ex-ldap.gakunin.nii.ac.jp

レポジトリサーバ（メタデータ自動ダウンロードで参照）：
  ex-ds.gakunin.nii.ac.jp
  ※実習セミナー内公開メタデータのURL
    →https://ex-ds.gakunin.nii.ac.jp/fed/ex-fed-metadata.xml

メタデータ提出先：
  ex-ds.gakunin.nii.ac.jp
  ※このホストのtestユーザのホーム配下にある「METADATA」ディレクトリ配下にアップロードします。

接続確認用SP ：
  ex-sp.gakunin.nii.ac.jp
  ex-sp2.gakunin.nii.ac.jp

接続確認用IdP：
  ex-idp.gakunin.nii.ac.jp

接続確認のURL：
  https://ex-sp.gakunin.nii.ac.jp/
  ※SP構築時の接続確認は、”ex-sp.gakunin.nii.ac.jp”の部分が各自
    構築したSPのホスト名となります。
```

基礎編のIdP構築は、こちらへ。SP構築は、こちらへ。　また活用編は、こちらへ。