旧: 実習セミナー環境について(シンクライアント環境)

事前作業 (シンクライアント環境)

IdP、又はSPの構築にあたって、ベースとなるOS (Linux/CentOS)の起動と初期設定 (ネットワークの設定など) を以下の手順にて行ってください。

※使用するサーバは、「CentOS5 32bit」です。

※VMwareを使用していますが、必ずしも推奨している訳ではありません。

1. VMイメージよりOS起動

VMware Playerを起動させてください。

画面左のリストより実習用Shibboleth-IdP、又は実習用Shibboleth-SPを選択し、

画面右下にある「仮想マシンの再生」をクリックしてください。

※初回起動時には、イメージをコピーしたか移動したかの確認メッセージが表示されます。

その際は、「コピーしました」を選択してください。

※OSのインストールと、DNS登録、時刻同期の設定のみ完了している状態です。

2. ゲストOSの初期設定

・VMware Playerのコンソールで操作

VMware Playerの画面をクリックすると操作対象がVMwareのコンソールに移ります。

OSのサービスが全て起動し、ログインプロンプト(login:)が表示されたら、

rootユーザでログインします。

※「Ctrl+Alt」キーで、操作対象をWindowsに戻す事ができます。

・初期設定シェルスクリプトの実行

実習セミナー環境での初期設定は、コンソール画面よりシェルスクリプトを実行して行います。

シェルスクリプトがネットワークの設定を行うとともに、実習セミナー内のDSサーバから

証明書、メタデータのテンプレート取得などを行います。

以下のコマンドラインを実行してください。

```
# /root/TOOL/initSetting.sh 割り振られた番号
```

例) 1番を割り振られた場合 (PC : cb0001)

```
# /root/TOOL/initSetting.sh 1
```

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。

初期設定が完了すると、以降はTeraTermで操作していきます。

表示されるホスト名を接続先として、TeraTermで接続してください。

(コンソール画面は、閉じないで最小化しておいてください。)

注意 : 1日目終了時点では、ゲストOSのシャットダウンは、行わないでください。ゲストOSは、必ず×をクリックして、そのままコンソール画面を閉じます。(サスペンドする設定になっています。メニューの「仮想マシン」→「パワー」→「サスペンド」を選択しても同じです。) このようにすると、構築した情報が保存されるので、2日目にその状態から再開することができます。

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) Tomcatのインストール
変更ファイル: /etc/profile, httpd.conf, ssl.conf, server.xml
- 3) Shibboleth-IdPのインストール
変更ファイル: java.security
- 4) Shibboleth-IdPの設定
 - ・メタデータの自動ダウンロード設定
 - ・認証方法をID/パスワード認証に設定
 - ・認証時のLDAP接続設定変更ファイル: relying-party.xml, handler.xml, login.config
- 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, relying-party.xml
- 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サーバの参照設定
 - ・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

DSサーバ :

training-ds.nii.ac.jp

※SPに設定するDSのURL

→<https://training-ds.nii.ac.jp/discovery/WAYF>

LDAPサーバ :

training-ds.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) :

training-ds.nii.ac.jp

※実習セミナー内公開メタデータのURL

→<http://training-ds.nii.ac.jp/fed/training-fed-metadata.xml>

メタデータ提出先 :

training-ds.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 :

training-sp.nii.ac.jp

training-sp2.nii.ac.jp

接続確認用IdP :

training-idp.nii.ac.jp

接続確認のURL :

<https://training-sp.nii.ac.jp/>

※SP構築時の接続確認は、「training-sp.nii.ac.jp」の部分が各自構築したSPのホスト名となります。

IdP構築は、[こちら](#)へ。 また、SP構築は、[こちら](#)へ。