実習セミナー環境について（AWS）2023

目次

事前説明（AWS）

学認認証フェデレーションは、Webアプリケーションへのシングル・サイン・オン（SSO）技術を、組織を超えて活用する分散型学術認証基盤です。

大学等機関（IdP: Identify Provider）がユーザIDと個人の属性情報を管理し、サービス提供者（SP: Service Provider）がそれを利用してサービスの利用を許可する仕組みを提供します。

本実習セミナーでは、IdPサーバ及びＳＰサーバを構築する手順を体験し、大学等機関はIdPサーバを、サービス提供者はSPサーバを容易に構築、学認認証フェデレーションへの参加を促進することを目指しています。

IdP、又はSPの構築を行うサーバ (Linux/CentOS)は、既にAWS上に起動されており、Tera Term等SSHクライアントでログインすることができます。
※使用するサーバは、「**CentOS7 64bit**」です。

1.ホスト名

IdP構築用とSP構築用のホスト名は以下の通りです。?? の部分は数字2桁で、受講者の番号で置き換えてください。
※ 活用編でも同じホスト名となります。ただしIdP/SPの基本的な部分は構築済みです。
ex-idp-test??.gakunin.nii.ac.jp
ex-sp-test??.gakunin.nii.ac.jp

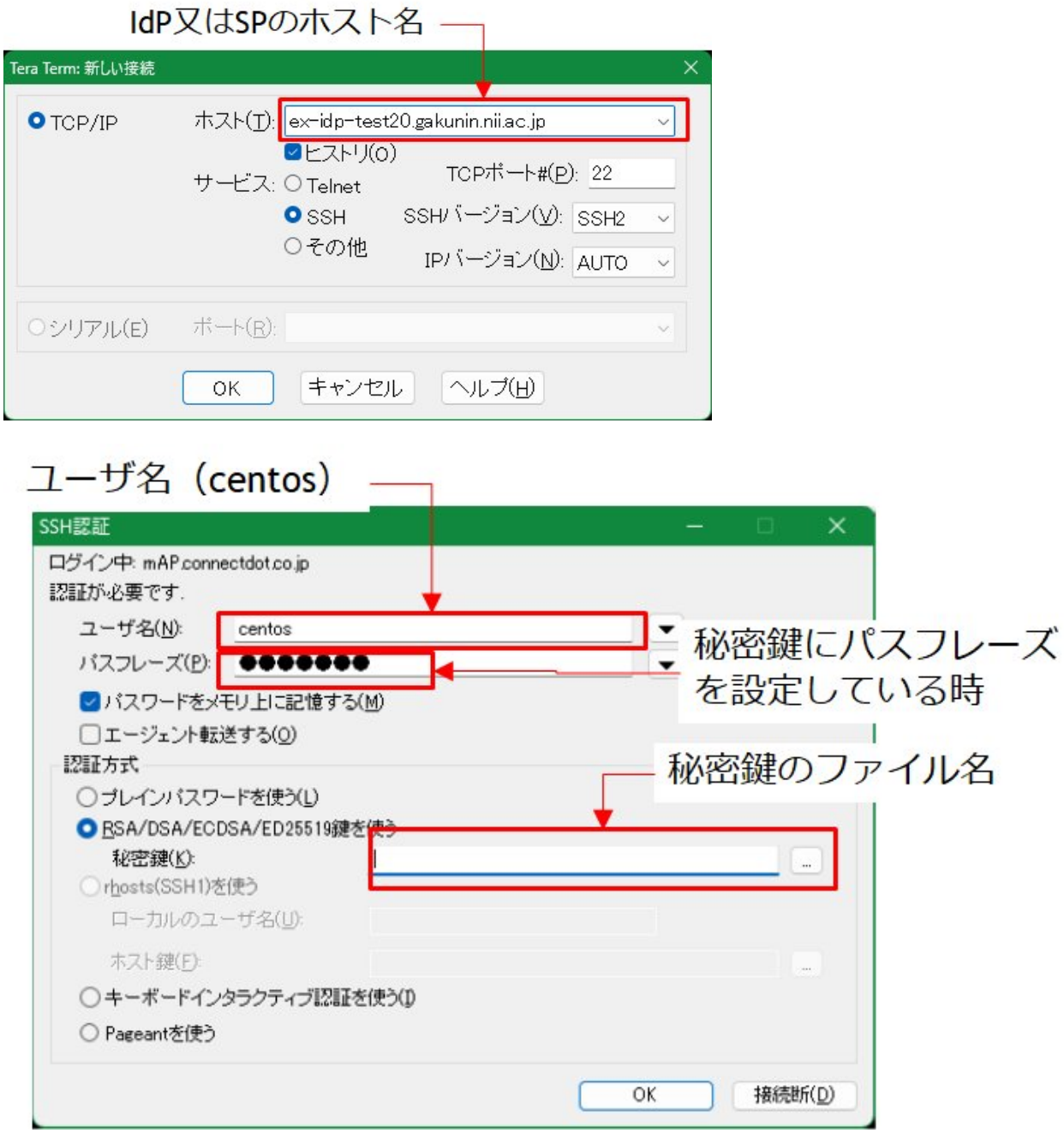
例）**1番**を割り振られた場合の**IdP**
ex-idp-test01.gakunin.nii.ac.jp

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

2.ログイン方法（例は、ホスト名に20番が割当てられた時）

受講者から事前に頂戴した公開鍵は上記ホストに設定済みです。また事前に頂戴したIPアドレスからのSSHアクセスを許可しております。SSH（公開鍵認証）でログインして操作してください。
SSHでのログインはユーザーcentosで行ってください。

2.1. Tera Termからログインする時



2.2.Linuxサーバ（openSSH）からログインする時

```
$ ssh centos@ex-idp-test20.gakunin.nii.ac.jp
```

```
$ ssh centos@ex-sp-test20.gakunin.nii.ac.jp
```

※但し、公開鍵ファイル（id_rsa.pub）及び秘密鍵ファイル（id_rsa）は、~/.sshディレクトリの下に配置し、パーミションは各々644, 600とします。

OpenSSHをお使いの場合、.ssh/configに以下の設定をしておくとSSH先の指定が楽になります。

```
Host ex-idp-test00
HostName ex-idp-test00.gakunin.nii.ac.jp
User centos
Port 22
IdentityFile ~/.ssh/秘密鍵ファイル
Host ex-sp-test00
HostName ex-sp-test00.gakunin.nii.ac.jp
User centos
Port 22
IdentityFile ~/.ssh/秘密鍵ファイル
```

上記設定をした場合のSSHコマンド例：

```
# ssh ex-idp-test00

# ssh ex-sp-test00
```

3.ログイン後の状態

作業の効率化のため、sudoでrootユーザーになっておいてください。

```
$ sudo -i
```

あらかじめインターネットから取得したファイルならびに構築に必要なファイルが、「/root/PKG」および「/root/GETFILE」に保存されています。

```
# ls -l /root

drwxr-xr-x. 4 root root 197  7月 12  2022 GETFILE

drwxr-xr-x. 2 root root 140  7月 19  2022 PKG
```

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操作できなくなります。なお、本セミナーでサーバの再起動を必要とする箇所はありません。説明の中で再起動と言った場合、IdPやSPのプロセス再起動を指しています。

IdPとSPの双方を操作することになります。自分がどちらのサーバを扱っているのか、常時意識してください。

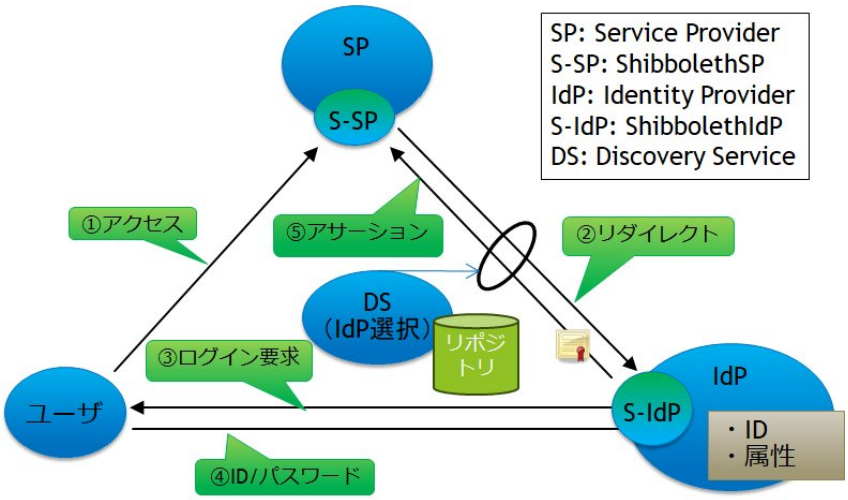
Shibboleth構築作業について

Shibbolethは、組織内および組織を超えてWeb上でフェデレーション・シングルサイオン（SSO）を実現する、標準的なオープンソースソフトウェアのパッケージです。

Shibbolethを用いた認証を、Shibboleth（シボレス）認証と呼びます。

本実習は、実習用IdP, SP サーバにShibbolethパッケージをインストールする手順を体験することによって、自機関のIdp又はSPサーバを学認フェデレーションに参加させる参考としていただくことを目的としています。

下図に、サーバと認証手順（ユーザがSPのサービスを受けるまで）を示すが、「S-SP」, 「S-IdP」がインストール・設定するShibbolethパッケージを示しています。



次の節で、IdP及びSP構築の簡単な手順を示しますが、詳しくは、

- Shibboleth環境構築セミナー（基礎編：IdP）
- Shibboleth環境構築セミナー（基礎編：SP）

のテキストを参照してください。

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（AWS）

```
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uploader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。
```

動作確認時のTips

各種作業後にブラウザを用いてテストしますが、そのときはブラウザのプライバシーモードを使うとよいでしょう。ID・パスワードの入力状態やDSでの選択状態など過去の操作をリセットし、まっさらな状態から動作確認を行うことができます。
Chrome: シークレットウィンドウ
Firefox: プライベートウィンドウ

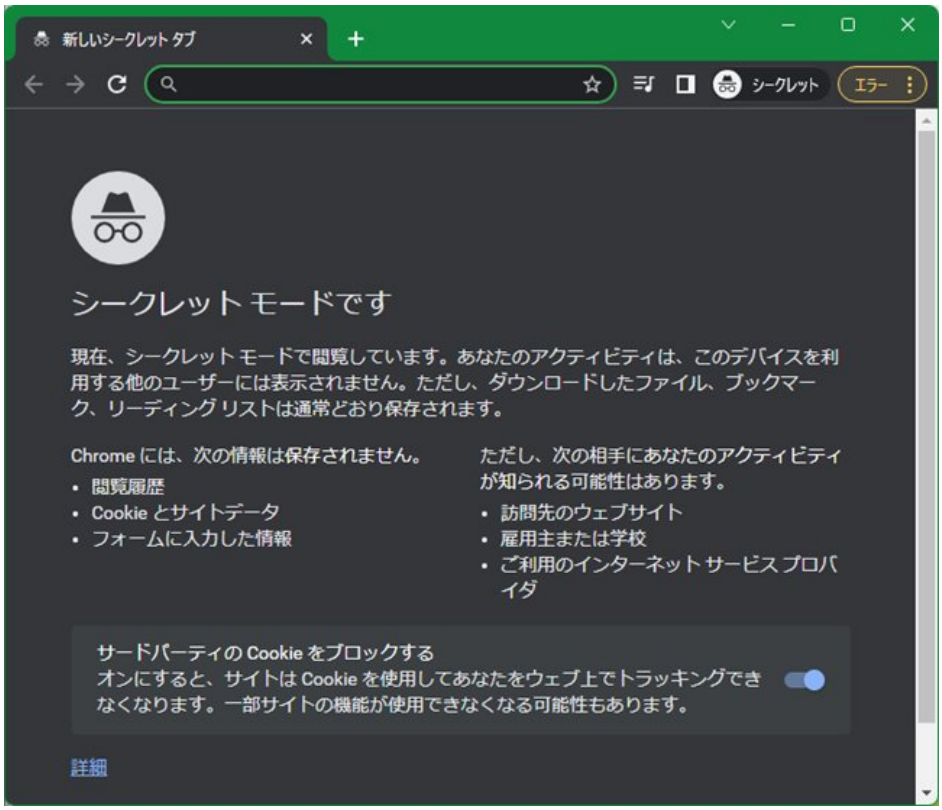
1. Chrome: シークレットウィンドウの設定方法

Windowsパソコンの場合：Google Chromeを起動している状態で「Ctrlキー + Shiftキー + nキー」を同時押しすると別ウィンドウが開き、シークレットモードが使えます。

Macの場合：Google Chromeを起動している状態で「⌘キー+ Shiftキー+ nキー」を同時押ししてください。

マウスによる操作：Google Chromeの右上の設定ボタンをクリックして、「シークレットウィンドウを開く」をクリックすれば新しいシークレットウィンドウを開くことができるのです。

下図は、Windowsパソコンで、「Ctrlキー + Shiftキー + nキー」を同時押した時の別ウィンドウを表示しています。

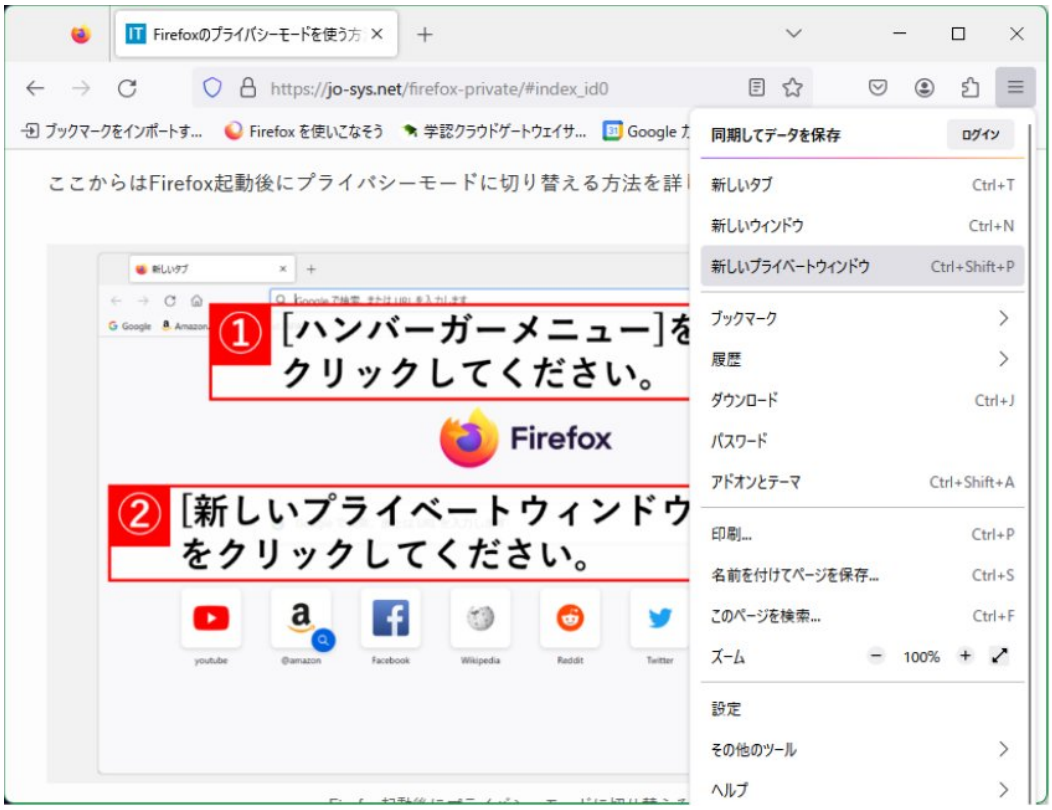


2. Firefox: プライベートウィンドウの設定方法

３つの方法があります。

2.1 Firefox起動後にプライバシーモードに切り替える方法

「新しいプライベートウィンドウ」を選択します。



すると次の新しいプライベートウィンドウが開きます。

2.2 キーボードショートカットを使ってプライバシーモードに切り替える方法

Firefoxをアクティブウィンドウにした状態でキーボードショートカットの[Ctrl]＋[Shift]＋[P]を押してください。

プライベートウィンドウが開きます。

2.3 すべてのアプリからFirefoxをプライバシーモードで起動する方法

タスクバーにあるWindowsボタンをクリックして（又は、キーボードのWindowsキーを押して）ください。

その表示中の右上にある[すべてのアプリ]をクリックしてください。

「FireFoxプライベートブラウジング」を選択すると、プライベートウィンドウが開きます。

又は、「FireFox」を選択し、マウス右ボタンクリックで「新しいプライベートウィンドウ」を選択すると、プライベートウィンドウが開きます。

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。