

SeciossLink と Shibboleth-SP の認証連携設定方法

Shibboleth-SP を使うと比較的に容易に Web アプリケーションの SAML SP 化が行えます。

以下は、SeciossLink の SAML サービスプロバイダとして Shibboleth-SP を登録する手順となります。

※実際に Web アプリケーションと連携させる場合は、導入した Shibboleth-SP と Web アプリケーション間でユーザ ID などの認証情報を引き継ぎ、認証を通す仕組みの開発が必要となります。

1. Shibboleth-SP のインストール

Web アプリケーションが動作しているサーバに Shibboleth-SP をインストールします。

ここでの説明は、サーバ OS が CentOS6 の場合とします。

1.1. リポジトリの登録

```
# wget
http://download.opensuse.org/repositories/security://shibboleth/CentOS_CentOS-6/security:sh
ibboleth.repo
# cp security¥:shibboleth.repo /etc/yum.repos.d/shibboleth.repo
```

1.2. yum インストール

```
# yum install shibboleth
```

2. Shibboleth-SP の設定

本説明では、認証連携を行うための基本的な設定のみとなります。

また SP に設定する証明書はインストール時に配置されたものを使用します。

設定が完了しましたら、Shibboleth-SP と Apache を再起動してください。

(/etc/init.d/shibd restart、/etc/init.d/httpd restart)

2.1. shibboleth2.xml を修正

```
# vi /etc/shibboleth/shibboleth2.xml
```

2.1.1. SP の entityID を設定

```
...省略...
<!-- The ApplicationDefaults element is where most of Shibboleth's SAML bits are defined. -->
<ApplicationDefaults entityID="https://FQDN/shibboleth" ←Web アプリケーションの FQDN
                    REMOTE_USER="eppn persistent-id targeted-id">
...省略...
```

2.1.1. SeciossLink の entityID を設定

```
...省略...  
<SSO entityID="https://slink.secioss.com" ←SeciossLink の entityID を認証サーバとして設定  
    discoveryProtocol="SAMLDS" discoveryURL="https://ds.example.org/DS/WAYF">  
    SAML2 SAML1  
</SSO>  
...省略...
```

2.1.2. SeciossLink のメタデータを設定

SeciossLink のメタデータは、「https://slink.secioss.com/saml/metadata.php?tenant=テナント ID」にアクセスすると取得することができます。

取得したメタデータを「/etc/shibboleth」配下に配置してください。

```
...省略...  
<!-- Example of locally maintained metadata. -->  
<!-- --> ←コメント解除  
<MetadataProvider type="XML" file="SlinkMetadata.xml"/> ←SeciossLink のメタデータを設定  
<!-- --> ←コメント解除  
...省略...
```

2.2. attribute-map.xml を修正

```
# vi /etc/shibboleth/attribute-map.xml
```

2.2.1. 受信属性のマッピング設定

SeciossLink で設定したユーザ ID の属性値が渡されるので、SP 側で環境変数より参照できるようマッピングの設定を行います。

```
<Attributes xmlns="urn:mace:shibboleth:2.0:attribute-map"  
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">  
上記の直ぐ下辺りに追加してください。  
<!-- Persistent ID Attribute map -->  
<Attribute name="urn:oasis:names:tc:SAML:2.0:nameid-format:persistent" id="name-id">  
    <AttributeDecoder xsi:type="NameIDAttributeDecoder" formatter="$Name"  
defaultQualifiers="true"/>  
</Attribute>
```

※php であれば、\$_SERVER["name-id"]より参照することができます。

3. サンプルページの作成

動作確認時に正しくユーザ ID 属性値が取得できているか確認するためのページを事前に準備しておきます。Shibboleth の認証とするパスは、デフォルトで設定されている「/secure」配下とします。

「/var/www/html/secure」を作成します。その配下に以下の内容で test.php を作成します。

```
<?php
echo $_SERVER["name-id"];
?>
```

※shibboleth 認証を行うパスは、「/etc/httpd/conf.d/shib.conf」で設定されています。

4. SeciossLink にてサービスプロバイダ登録

管理画面より連携するサービスプロバイダとして Shibboleth-SP を登録します。

本説明での前提条件として、Assertion Consumer Service は1つとし、ユーザ ID 以外の属性値は送信しないものとします。またエンティティ ID、Assertion Consumer Service、ログアウト URL は、SP のメタデータより読み込む方法で設定します。

※サービスプロバイダへのパスワード送信、パスワード暗号化用公開鍵の設定は必要ありません。

4.1. 登録画面

以下の手順で画面を開きます。

- ① 管理画面にログイン後、上部のメニューよりシングルサインオンをクリックします。
 - ② 左にあるシングルサインオンのメニューより SAML サービスプロバイダをクリックします。
 - ③ SAML サービスプロバイダ内の上部にあるメニューのサービスプロバイダ登録をクリックします。
- 以下がサービスプロバイダの登録画面となります。

Copyright © SECIOSS

4.2. 設定値の入力

まずサービス ID とサービス名については、他の SP と同じ値にならないように任意の値を設定します。例として、ここではサービス ID に「testsp」、サービス名に「TestSP」を設定しています。次に以下の手順でメタデータを読み込み、残りの必要な値を設定します。

① Shibboleth-SP のメタデータ取得

Shibboleth-SP のメタデータは、「<https://FQDN/Shibboleth.sso/Metadata>」（Shibboleth-SP をインストールした Web アプリケーションが動作するサーバ）にアクセスすると取得することができます。（FQDN は、SP の環境に合わせて置き換えてください）

② Shibboleth-SP のメタデータを選択

メタデータ項目にある「参照...」ボタンをクリックします。



The screenshot shows a configuration window for Shibboleth-SP. The 'Metadata' section is highlighted, and the '参照...' button is circled in red. The text next to it says 'ファイルが選択されていません。' (No file selected). Other options include 'サービスプロバイダへのパスワード送信' (Service Provider Password Transmission) set to 'なし' (None), and 'パスワード暗号化用公開鍵' (Password Encryption Public Key) with a '参照...' button. A '保存' (Save) button is at the bottom.

選択画面が表示されるので、取得した Shibboleth-SP のメタデータを選択します。

例として、ここでは「Metadata」という Shibboleth-SP のメタデータを選択した場合です。



The screenshot shows the same configuration window as before, but now the 'Metadata' button is circled in red. The text next to it says 'Metadata'. The '参照...' button is no longer visible. The '保存' (Save) button is still at the bottom.

③ Shibboleth-SP のメタデータを読み込む

メタデータ項目にある「読み込む」ボタンをクリックします。



The screenshot shows the same configuration window as before, but now the '読み込む' (Load) button is circled in red. The text next to it says 'Metadata'. The '参照...' button is no longer visible. The '保存' (Save) button is still at the bottom.

以下のように Shibboleth-SP のメタデータが読み込まれ、エンティティ ID、Assertion Consumer Service、ログアウト URL が自動的に設定されます。

サービスプロバイダ登録	
割り当てるライセンス*	SAML 3: 10 ユーザ
サービスID*	testsp -test.com
サービス名*	TestSP
エンティティID*	https://shibsp-test1.secioss.co.jp/shibboleth
Assertion Consumer Service	https://shibsp-test1.secioss.co.jp/Shibboleth.sso/SAML2/POST 追加
ログアウトURL	https://shibsp-test1.secioss.co.jp/Shibboleth.sso/SLO/POST 追加
ユーザーIDの属性	ユーザーID
送信する属性	<input type="checkbox"/> メールアドレス <input type="checkbox"/> 社員番号 <input type="checkbox"/> 氏名 <input type="checkbox"/> 組織 <input type="checkbox"/> 地域 <input type="checkbox"/> 言語 <input type="checkbox"/> ユーザーグループ <input type="checkbox"/> セキュリティグループ
サービスプロバイダへのパスワード送信	なし
パスワード略号化用公開鍵	参照... ファイルが選択されていません。
メタデータ	参照... ファイルが選択されていません。読み込む

保存

Copyright © SECIOSS

「保存」ボタンをクリックして、登録を完了させます。

5. 動作確認

以下の手順で認証連携が行えることを確認します。

(FQDN は、SP の環境に合わせて置き換えてください。)

- ① ユーザの許可するサービスにある「TestSP」にチェックを入れます。
- ② 「https://FQDN/secure/test.php」(Shibboleth-SP をインストールした Web アプリケーションが動作するサーバ) にアクセスします。
- ③ SeciossLink の認証画面が表示され、ID/パスワードなどの認証を行います。
- ④ 「https://FQDN/secure/test.php」が表示されます。

最後に表示された画面にユーザー ID の属性値が表示されていれば、正しくユーザー ID 情報が渡されたこととなります。

— 以上 —