cybozu.com

# 学認（Shibboleth）との認証連携


サイボウズ株式会社

第 1 版

Cybozu

# 目次

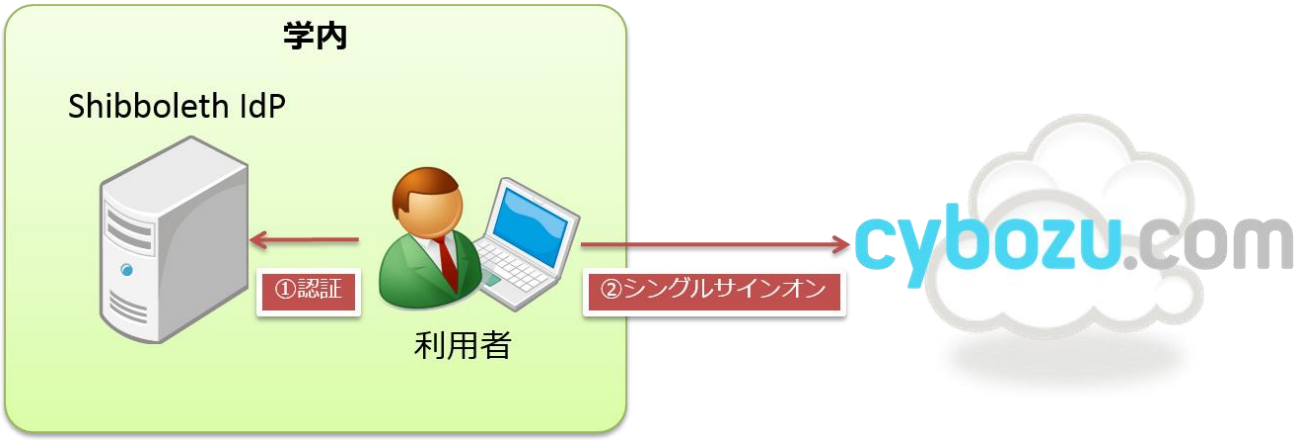
1 はじめに....2
2 前提....2
3 事前準備....3
3.1 cybozu.com 環境の準備....3
3.2 Service Provider メタデータのダウンロード....4
4 Shibboleth のインストール....4
5 Shibboleth のセットアップ....4
5.1 relying-party.xml....4
5.2 attribute-resolver.xml, attribute-filter.xml....6
5.3 cybozu.com 共通管理の設定....7
5.4 ユーザーアカウントの作成....8
6. cybozu.com へのアクセス....9

# 1 はじめに

Shibboleth は、学術認証フェデレーション（学認：GakuNin）で標準的に利用されているシングルサインオンを実現するためのソフトウェアです。

学術認証フェデレーション
https://www.gakunin.jp/

Shibboleth は SAML を利用しているため、cybozu.com との連携が可能です。
本書では、Shibboleth を使って cybozu.com へシングルサインオンを行う手順を説明します。



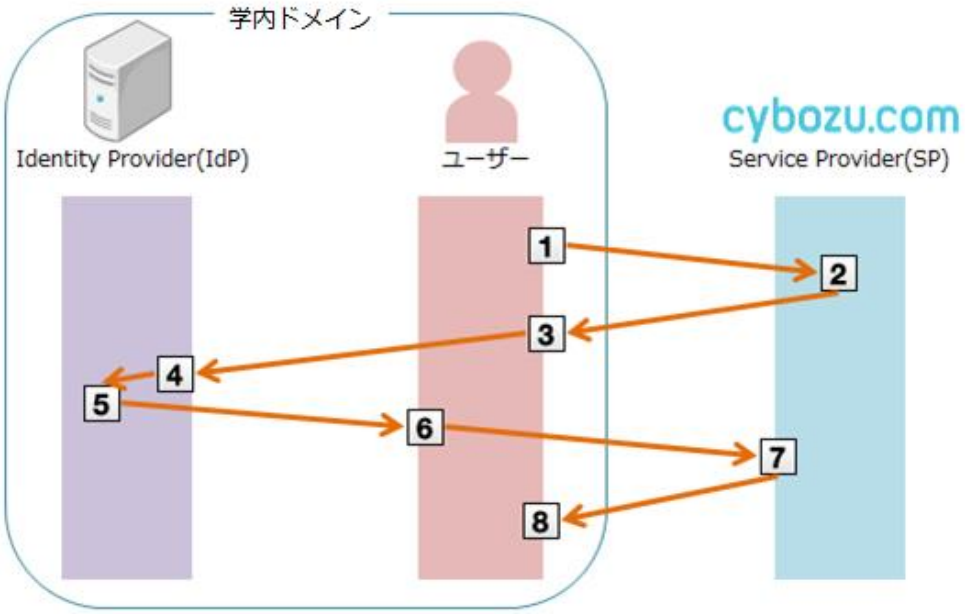

※ Shibboleth は IdP と SP の機能を持ちます。

本書の構成は、Shibboleth が IdP、cybozu.com が SP となります。

# 2 前提

- 学認（Shibboleth）との連携について、基本的な手順を把握されている方を対象としています。cybozu.com の連携に必要な箇所のみ記載していますので、記載されていない内容については、学認の技術ガイドに従い、設定を行って下さい。
- 設定ファイルの変更箇所のみ記載しています。サービスの再起動等は適時実施して下さい。
- クライアント PC の OS は Windows 7 Professional(SP1)、ブラウザは Internet Explorer 11 で確認を行っています。

- SAML を使った連携の流れは以下の通りです。




1. ユーザーが cybozu.com にアクセスします。
2. cybozu.com が SAML リクエストを生成します。
3. ユーザーが SP（cybozu.com）から SAML リクエストを受け取ります。
4. IdP（Shibboleth）がユーザーを認証します。
5. IdP（Shibboleth）が SAML レスポンスを生成します。
6. ユーザーが IdP（Shibboleth）から SAML レスポンスを受け取ります。
7. SP（cybozu.com）が SAML レスポンスを受け取り、検証します。
8. SAML レスポンスの内容に問題がない場合は、ユーザーが cybozu.com にログインした状態になります。

# 3 事前準備

## 3.1 cybozu.com 環境の準備

cybozu.com に環境が必要となります。
環境が無い場合は、「サイボウズドットコム ストア」から試用環境を申し込んで下さい。

サイボウズドットコム ストア
https://www.cybozu.com/jp/service/com/trial/

※ 「お試しになるサービス」は任意のサービスを選択して下さい

※ 本書ではドメインを「gakunin-test.cybozu.com」と設定しました

### 3.2 Service Provider メタデータのダウンロード

後の手順で必要となる Service Provider メタデータをダウンロードしておきます。

1. cybozu.com 共通管理に cybozu.com 共通管理者でログインします。
2. 「システム管理 > セキュリティ > ログイン」画面に移動し、「SAML 認証を有効にする」にチェックを入れます。


3. 「Service Provider メタデータのダウンロード」をクリックし、spmetadata.xml を保存します。

※ ダウンロードが完了したらブラウザは終了して構いません

## 4 Shibboleth のインストール

詳細手順は割愛します。学認の技術ガイドに記載された手順に従って実施して下さい。

VMware イメージを利用した構築
https://meatwiki.nii.ac.jp/confluence/pages/viewpage.action?pageId=12158255

※ 本書ではホスト名を cybozu.example.ac.jp としています

## 5 Shibboleth のセットアップ

Shibboleth の設定ファイルを cybozu.com との連携用に変更します。

### 5.1 relying-party.xml

1. cybozu.com メタデータの参照

```
<metadata:MetadataProvider id="ShibbolethMetadata"
xsi:type="metadata:ChainingMetadataProvider">
```

上記の子要素として以下を追記します。

```
<MetadataProvider xsi:type="FilesystemMetadataProvider"
xmlns="urn:mace:shibboleth:2.0:metadata"
      id="CybozuCom"
      metadataFile="/opt/shibboleth-idp/metadata/spmetadata.xml" />
```

※ id には設定ファイル内でユニークとなる値を記述します

※ 「3.2 Service Provider メタデータのダウンロード」でダウンロードしたファイルを Shibboleth サーバーの「/opt/shibboleth-idp/metadata」に保存し、「metadataFile」に指定します

2. アサーションの署名・暗号化の設定

以下の手順に従い、cybozu.com 用の設定を追記します。

特定の SP へのアサーションを暗号化しない設定
https://meatwiki.nii.ac.jp/confluence/pages/viewpage.action?pageId=10226458#id-設定・運用・カスタマイズ-特定の SP へのアサーションを暗号化しない設定

- 設定例

```
<RelyingParty id=" https://gakunin-test.cybozu.com"
   provider=" https://cybozu.example.ac.jp/idp/shibboleth"
   defaultSigningCredentialRef="IdPCredential">

   <ProfileConfiguration xsi:type="saml:SAML2SSOProfile"
      includeAttributeStatement="true"
      assertionLifetime="300000"
      assertionProxyCount="0"
      signResponses="conditional"
      signAssertions="never"
      encryptAssertions="never"
      encryptNameIds="never" />

</RelyingParty>
```

■ 補足

cybozu.com の仕様は以下の通りとなっています。

- レスポンス、アサーションのいずれかに署名が必要
  - signResponses、signAssertions のいずれかが conditional もしくは always になっている必要があります
- アサーションを暗号化しない
  - encryptAssertions、encryptNameIds の両方が never になっている必要があります

## 5.2 attribute-resolver.xml, attribute-filter.xml

1. NameID に eduPersonPrincipalName（ePPN）を設定する
   以下の手順に従い、cybozu.com 用の設定を追記します。

   特定の SP に対し ePPN を NameID に入れて送る設定方法
   https://meatwiki.nii.ac.jp/confluence/pages/viewpage.action?pageId=10226458#id-設定・運用・カスタマイズ-特定の SP に対し ePPN を NameID に入れて送る設定方法

   - 設定例（attribute-resolver.xml）

```
<resolver:AttributeDefinition id="nameIdEPPN" xsi:type="Template"
xmlns="urn:mace:shibboleth:2.0:resolver:ad">
    <resolver:Dependency ref="eduPersonPrincipalName"/>
    <resolver:AttributeEncoder xsi:type="SAML2StringNameID"
                               xmlns="urn:mace:shibboleth:2.0:attribute:encoder"
                               nameFormat="urn:oid:1.3.6.1.4.1.5923.1.1.1.6" />
    <Template>
        <![CDATA[
            ${eduPersonPrincipalName}@example.ac.jp
        ]]>
    </Template>
    <SourceAttribute>eduPersonPrincipalName</SourceAttribute>
</resolver:AttributeDefinition>
```

   - 設定例（attribute-filter.xml）

```
<afp:AttributeFilterPolicy id="PolicyforCybozuCom"
xmlns:afp="urn:mace:shibboleth:2.0:afp">
  <afp:PolicyRequirementRule xsi:type="basic:AttributeRequesterString"
   value="https://gakunin-test.cybozu.com" />
```

```
    <afp:AttributeRule attributeID="transientId">
        <afp:DenyValueRule xsi:type="basic:ANY" />
    </afp:AttributeRule>
    <afp:AttributeRule attributeID="nameIdEPPN">
        <afp:PermitValueRule xsi:type="basic:ANY" />
    </afp:AttributeRule>
</afp:AttributeFilterPolicy>
```

※ id には設定ファイル内でユニークなる値を記述します

■ 補足（NameID に ePPN を渡す理由）

cybozu.com ではログイン時にユーザーを一意に識別する情報として、「ログイン名」を使います。
SAML を使った連携時は、SAML レスポンスの NameID の値が「ログイン名」と一致している必要があります。
通常、Shibboleth では NameID として transientId（ログインの度に異なる ID が割り当てられる）が使われますが、ユーザーを一意に識別できません。
そのため、cybozu.com との連携においては、ユーザーの識別が可能な ePPN を NameID として受け渡す方法を採用しています。

## 5.3 cybozu.com 共通管理の設定

1. cybozu.com 共通管理に cybozu.com共通管理者でログインします。
2. 「システム管理 > セキュリティ > ログイン」画面に移動し、「SAML認証を有効にする」にチェックを入れます。
3. 以下のように設定し、「保存」をクリックします。

| 設定項目 | 設定内容・設定例 |
|---|---|
| Identity ProviderのSSOエンドポイントURL（HTTP-Redirect） | IdPのエンドポイントURLを指定します。<br>https://cybozu.example.ac.jp/idp/profile/SAML2/Redirect/SSO |
| cybozu.com からのログアウト後に遷移する URL | IdPのログアウトURLを指定します。<br>検証時はダミーのURLを指定しました。 |
| Identity Providerが署名に使用する公開鍵の証明書 | IdPが署名時に使う証明書を指定します。<br>/opt/shibboleth-idp/credentials/server.crt を使うか、学認申請システムに入力したものを使います。 |


## 5.4 ユーザーアカウントの作成

cybozu.com にユーザーアカウントを作成します。
ShibbolethをVMイメージから構築した場合、LDAPにユーザーが作成済みのため、そのユーザーを利用します。

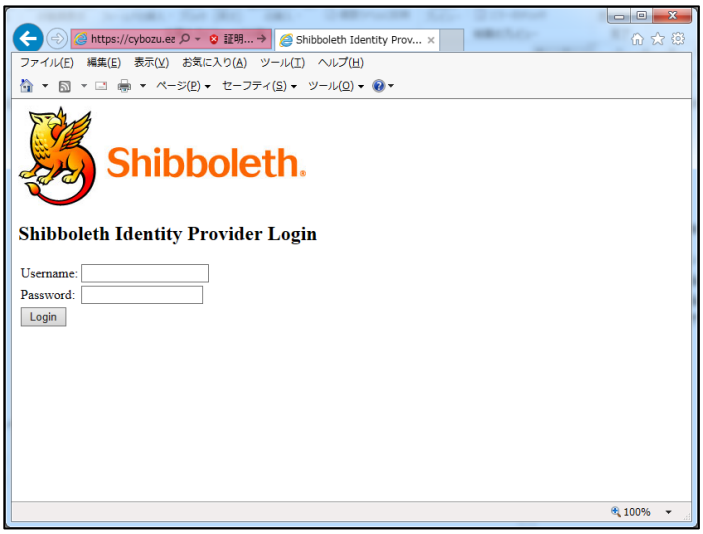
1. 以下の手順に従い、ユーザーを追加します。

   ユーザーを追加する / cybozu.com ヘルプ
   https://help.cybozu.com/ja/general/admin/add_user.html

※ 前述の通り、ShibbolethのePPNをNameIDとして受け渡しますので、cybozu.comの「ログイン名」として、ePPNと同じ情報を設定します。

## 6. cybozu.com へのアクセス

1. クライアント PC で Internet Explorer を起動し、cybozu.com にアクセスします。
2. Shibbolethのログイン画面にリダイレクトされます。




3. Shibboleth にログインします。
4. シングルサインオンが行われ、cybozu.com へログインされます。