

shibboleth2.xml ファイル

shibboleth2.xml ファイル

1. entityIDを設定します。

/etc/shibboleth/shibboleth2.xml ファイルを以下のように編集してください。

※「ApplicationDefaults entityID」を検索し、場所を特定してください。
<ApplicationDefaults entityID="https://sp.example.ac.jp/shibboleth-sp"
↑ ホスト名変更 ↑ 後ろに「-sp」追記
REMOTE_USER="eppn subject-id pairwise-id persistent-id"
cipherSuites="DEFAULT:!EXP:!LOW:!aNULL:!eNULL:!DES:!IDEA:!SEED:!RC4:!3DES:!kRSA:!SSLv2:!SSLv3:!TLSv1:!TLSv1.1">

※端末のサイズによっては表記がずれる可能性があります。画面を広くしてご覧ください。

2. DSサーバの参照設定を行います。

/etc/shibboleth/shibboleth2.xml ファイルを以下のように編集してください。

※DSサーバのURLはフェデレーション毎に異なります。

運用フェデレーションの場合	https://ds.gakunin.nii.ac.jp/WAYF
テストフェデレーションの場合	https://test-ds.gakunin.nii.ac.jp/WAYF

※「</Sessions>」の直前に行を挿入してください。
<!-- JSON feed of discovery information. -->
<Handler type="DiscoveryFeed" Location="/DiscoFeed"/>
<SessionInitiator type="Chaining" Location="/DS" isDefault="true" id="DS">
<SessionInitiator type="SAML2" template="bindingTemplate.html"/>
<SessionInitiator type="Shib1"/>
<SessionInitiator type="SAMLDS" URL="https://test-ds.gakunin.nii.ac.jp/WAYF"/>
↑ DSサーバの設定
</SessionInitiator>
</Sessions>
(省略)

※端末のサイズによっては表記がずれる可能性があります。画面を広くしてご覧ください。

3. メタデータの自動更新設定を行います。

- SPのトラストアンカーの確認と必要なCA証明書の導入
[SPのトラストアンカーの確認と必要なCA証明書の導入](#) のページを参照して必要なCA証明書が導入されていることをご確認ください。
- 証明書を格納するディレクトリを作成します。

```
# mkdir /etc/shibboleth/cert
```

- 検証に用いる検証用証明書をダウンロードして、/etc/shibboleth/cert/ に置きます。
検証用証明書は以下からダウンロードして使用してください。

運用フェデレーションの場合	gakunin-signer-2017.cer
テストフェデレーションの場合	gakunin-test-signer-2020.cer

- メタデータを自動的にダウンロードする設定を行います。

/etc/shibboleth/shibboleth2.xml ファイルを以下のように編集してください。

```

<!-- Example of remotely supplied batch of signed metadata. -->
<!-- --> <!-- コメントアウト解除
<MetadataProvider type="XML" validate="true"
    url="https://metadata.gakunin.nii.ac.jp/gakunin-metadata.xml"
        ↑ 参照先のURLを設定
    backingFilePath="federation-metadata.xml" maxRefreshDelay="7200">
<MetadataFilter type="RequireValidUntil" maxValidityInterval="1296000"/>
        ↑ validUntilの検証設定
<MetadataFilter type="Signature" certificate="/etc/shibboleth/cert/gakunin-signer-2017.cer" verifyBackup="false"/>
        ↑ 自動更新メタデータの検証用証明書設定
<DiscoveryFilter type="Blacklist" matcher="EntityAttributes" trimTags="true"
    attributeName="http://macedir.org/entity-category"
    attributeNameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"
    attributeValue="http://refeds.org/category/hide-from-discovery" />

<TransportOption provider="CURL" option="64">1</TransportOption>
<TransportOption provider="CURL" option="81">2</TransportOption>
<TransportOption provider="CURL" option="10065">/etc/pki/tls/certs/ca-bundle.crt</TransportOption>
        ↑ HTTPSサイトの証明書検証を有効化（メタデータのダウンロード時に利用）
</MetadataProvider>
<!-- --> <!-- コメントアウト解除

```

※端末のサイズによっては表記がずれる可能性があります。画面を広くしてご覧ください。

※ 上記設定によってダウンロードされたメタデータは /var/cache/shibboleth/federation-metadata.xml に配置されます。これはバックアップファイルと呼ばれます。



バックアップファイルが他者によって変更されないことが確実でない場合、MetadataFilter type="Signature"の行の「verifyBackup="false"」の部分削除してください。

verifyBackup="false"は、起動時のメタデータ読み込み時にバックアップファイルの署名検証をスキップし起動を速くするためのものです。

※ 上記は運用フェデレーションでの設定で、テストフェデレーションの場合はメタデータダウンロードURLも異なります。詳しくはテストフェデレーションルールをご参照ください。

⇒ [テストフェデレーションルール](#)



メタデータの読み込みについての注意

運用フェデレーション用メタデータと、テストフェデレーション用メタデータを同時に読み込まないようにしてください。テストフェデレーションから運用フェデレーションへの移行時にテストフェデレーション用メタデータの自動読み込み設定を削除せず、運用フェデレーション用メタデータの自動読み込み設定を追記した場合に、両方のメタデータを読み込んだ状態となります。

運用フェデレーション用メタデータ・テストフェデレーション用メタデータの両方を自動読み込みする設定になっていると、意図せずテストフェデレーション用メタデータの情報が利用されることで運用フェデレーションIdPとの認証でエラーが発生する可能性があります。

また、テストフェデレーションから運用フェデレーションへ同一entityIDで移行する場合には、テストフェデレーション側のSPは廃止申請を行ってください。テスト用途でテストフェデレーションにSPを登録する場合には運用フェデレーションと異なるentityIDで登録してください。

※ maxValidityIntervalおよびメタデータのvalidUntilについては以下をご参照ください。

⇒ [メタデータのvalidUntilを検証する設定方法](#)

参考資料

- Shibboleth SP 3の設定ドキュメント
<https://wiki.shibboleth.net/confluence/display/SP3/ReloadableConfiguration>
<https://wiki.shibboleth.net/confluence/display/SP3/MetadataProvider>

TOP

NEXT