

metadata-providers.xml ファイルの変更

metadata-providers.xml ファイルの変更

メタデータの自動ダウンロードやローカルのメタデータを参照するためにmetadata-providers.xml ファイルを変更します。

学術認証フェデレーションのメタデータを自動的にダウンロードするために [IdP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。

また検証用証明書をダウンロードして、任意のディレクトリに置き、そのパスを設定します。
以下では「/opt/shibboleth-idp/credentials/」に置いたものとして説明しています。

[テストフェデレーションルール](#)

/

	メタデータのダウンロードURL	検証用証明書
運用フェデレーション	https://metadata.gakunin.nii.ac.jp/gakunin-metadata.xml	gakunin-signer-2017.cer
テストフェデレーション	https://metadata.gakunin.nii.ac.jp/gakunin-test-metadata.xml	gakunin-test-signer-2020.cer

1

学術認証フェデレーションのメタデータを自動的にダウンロードする設定をします。



メタデータの読み込みについての注意点

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SPとの認証でエラーが発生する可能性があります。

同様の理由でSP側の混乱を避けるため、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IdPは廃止申請を行ってください。その後テスト用途でテストフェデレーションにIdPを登録する場合には運用フェデレーションのものとは異なるentityIDで登録するようにしてください。

/opt/shibboleth-idp/conf/metadata-providers.xml ファイルを以下のように編集してください。

```
The EntityRoleWhiteList saves memory by only loading metadata from SAML roles
that the IdP needs to interoperate with.
-->

<!-- --> ← コメントアウト解除

<MetadataProvider id="HTTPMetadata"
  xsi:type="FileBackedHTTPMetadataProvider"
  backingFile="%{idp.home}/metadata/gakunin-metadata-backing.xml"
  metadataURL="https://metadata.gakunin.nii.ac.jp/gakunin-metadata.xml">

<MetadataFilter xsi:type="SignatureValidation" certificateFile="%{idp.home}/credentials/gakunin-signer-2017.cer" />
<MetadataFilter xsi:type="RequiredValidUntil" maxValidityInterval="P15D"/>
<MetadataFilter xsi:type="EntityRoleWhiteList">
  <RetainedRole>md:SPSSODescriptor</RetainedRole>
</MetadataFilter>
</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。

(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)

