relying-party.xml ファイルの確認

relying-party.xml ファイルの確認（★）

ホスト名を修正します。（VMイメージ利用の場合）

ホスト名が正しいことを確認します。（貴学でインストールの場合）（★）

実習セミナー

・構築中の**IdPのホスト名が正しく記述されていることを確認**してください。
例）1番を割り振られた場合
ex-idp-test01.gakunin.nii.ac.jp

/opt/shibboleth-idp/conf/relying-party.xml ファイルを確認してください。（★）

```
<!-- ========================================== -->
<!--      Relying Party Configurations          -->
<!-- ========================================== -->

<rp:AnonymousRelyingParty provider="https://example-idp.nii.ac.jp/idp/shibboleth"
                                                ↑ ホスト名
                    defaultSigningCredentialRef="IdPCredential">
<rp:DefaultRelyingParty provider="https://example-idp.nii.ac.jp/idp/shibboleth"
                                               ↑ ホスト名
                    defaultSigningCredentialRef="IdPCredential">
```

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

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。

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。

実習セミナー

・**学術認証フェデレーションのメタデータは、使用しません。**
実習セミナー内のDSサーバからダウンロードする設定を行います。
以下のアドレスをダウンロード先に設定してください。
https://ex-ds.gakunin.nii.ac.jp/fed/ex-fed-metadata.xml

- 運用フェデレーション用メタデータ
  https://metadata.gakunin.nii.ac.jp/gakunin-metadata.xml
- テストフェデレーション用メタデータ
  https://metadata.gakunin.nii.ac.jp/gakunin-test-metadata.xml

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。

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IdP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IdP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。

/opt/shibboleth-idp/conf/relying-party.xml ファイルを以下のように編集してください。（★）

```
    <!-- ========================================== -->
    <!--      Metadata Configuration                -->
    <!-- ========================================== -->
    <!-- MetadataProvider the combining other MetadataProviders -->
    <metadata:MetadataProvider id="ShibbolethMetadata" xsi:type="metadata:ChainingMetadataProvider">

        <!-- Load the IdP's own metadata.  This is necessary for artifact support. -->
        <!-- ← 自動ダウンロードのメタデータを参照する為、コメントアウト
        <metadata:MetadataProvider id="IdPMD" xsi:type="metadata:FilesystemMetadataProvider"
                                   metadataFile="/opt/shibboleth-idp/metadata/idp-metadata.xml"
                                   maxRefreshDelay="P1D" />
        --> ← コメントアウト

        <!-- Example metadata provider. -->
        <!-- Reads metadata from a URL and store a backup copy on the file system. -->
        <!-- Validates the signature of the metadata and filters out all by SP entities in order to save memory -->
        <!-- To use: fill in 'metadataURL' and 'backingFile' properties on MetadataResource element -->
        <!-- --> ← コメントアウト解除
        <metadata:MetadataProvider id="URLMD" xsi:type="metadata:FileBackedHTTPMetadataProvider"
                        metadataURL="https://metadata.gakunin.nii.ac.jp/gakunin-metadata.xml"
                                                  ↑ 参照先ダウンロードメタデータのアドレス
                        backingFile="/opt/shibboleth-idp/metadata/some-metadata.xml">
                                                                  ↑ メタデータは、このファイル名で保存
            <metadata:MetadataFilter xsi:type="metadata:ChainingFilter">
                <metadata:MetadataFilter xsi:type="metadata:RequiredValidUntil"
                                maxValidityInterval="P15D" />
                <metadata:MetadataFilter xsi:type="metadata:SignatureValidation"
                                trustEngineRef="shibboleth.MetadataTrustEngine"
                                requireSignedMetadata="true" />
                    <metadata:MetadataFilter xsi:type="metadata:EntityRoleWhiteList">
                    <metadata:RetainedRole>samlmd:SPSSODescriptor</metadata:RetainedRole>
                </metadata:MetadataFilter>
            </metadata:MetadataFilter>
        </metadata:MetadataProvider>
        <!-- --> ← コメントアウト解除

    </metadata:MetadataProvider>
```

※端末のサイズによっては表記がずれる可能性がございます。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）

メタデータを検証する設定をします。（★）

実習セミナー

・初期設定で「/root/GETFILE」に取得した、ex-fed.crtが検証用証明書です。
「/opt/shibboleth-idp/credentials」にコピーしてください。
cp /root/GETFILE/ex-fed.crt /opt/shibboleth-idp/credentials/
以下の設定では、証明書のファイル名を「**ex-fed.crt**」と設定します。

検証用証明書（https://metadata.gakunin.nii.ac.jp/gakunin-signer-2010.cer）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）

（上記は運用フェデレーションの場合で、テストフェデレーションの場合はgakunin-test-signer-2011.cerをダウンロードして使用してください。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）

/opt/shibboleth-idp/conf/relying-party.xml ファイルを以下のように編集してください。（★）

```
    <security:Credential id="IdPCredential" xsi:type="security:X509Filesystem">
        <security:PrivateKey>/opt/shibboleth-idp/credentials/idp.key</security:PrivateKey>
        <security:Certificate>/opt/shibboleth-idp/credentials/idp.crt</security:Certificate>
    </security:Credential>

    <!-- Trust engine used to evaluate the signature on loaded metadata. -->
    <!-- --> ← コメントアウト解除
    <security:TrustEngine id="shibboleth.MetadataTrustEngine" xsi:type="security:StaticExplicitKeySignature">
        <security:Credential id="MyFederation1Credentials" xsi:type="security:X509Filesystem">
            <security:Certificate>/opt/shibboleth-idp/credentials/gakunin-signer-2010.cer</security:Certificate>
        </security:Credential>
    </security:TrustEngine>
    <!-- --> ← 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ございます。画面を広くしてご覧ください。

Tomcatを”tomcat”ユーザで実行する場合かつ当該ディレクトリの所有者が適切に設定されていない場合は、Tomcatが自動取得したメタデータを保存できるよう、ディレクトリの所有者を変更します。

```
# chown -R tomcat /opt/shibboleth-idp/metadata/
```

BACK TOP NEXT