メタデータ

学認メタデータ

学認メタデータの読み込みはconf/metadata-providers.xmlで設定します。

- conf/metadata-providers.xml

conf/metadata-providers.xml

```
    <!-- -->
    <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" requireSignedRoot="true"
                        certificateFile="%{idp.home}/credentials/gakunin-signer-2010.cer"/>
        <MetadataFilter xsi:type="RequiredValidUntil" maxValidityInterval="P15D"/>
        <MetadataFilter xsi:type="EntityRoleWhiteList">
            <RetainedRole>md:SPSSODescriptor</RetainedRole>
        </MetadataFilter>
    </MetadataProvider>
    <!-- -->
```

差分

```
-    <!--
+    <!-- -->
     <MetadataProvider id="HTTPMetadata"
                       xsi:type="FileBackedHTTPMetadataProvider"
-                      backingFile="%{idp.home}/metadata/localCopyFromXYZHTTP.xml"
-                      metadataURL="http://WHATEVER">
+                      backingFile="%{idp.home}/metadata/gakunin-metadata-backing.xml"
+                      metadataURL="https://metadata.gakunin.nii.ac.jp/gakunin-metadata.xml">
-        <MetadataFilter xsi:type="SignatureValidation" requireSignedRoot="true">
-            <PublicKey>
-                MIIBI.....
-            </PublicKey>
-        </MetadataFilter>
-        <MetadataFilter xsi:type="RequiredValidUntil" maxValidityInterval="P30D"/>
+        <MetadataFilter xsi:type="SignatureValidation" requireSignedRoot="true"
+                        certificateFile="%{idp.home}/credentials/gakunin-signer-2010.cer"/>
+        <MetadataFilter xsi:type="RequiredValidUntil" maxValidityInterval="P15D"/>
         <MetadataFilter xsi:type="EntityRoleWhiteList">
             <RetainedRole>md:SPSSODescriptor</RetainedRole>
         </MetadataFilter>
     </MetadataProvider>
-    -->
+    <!-- -->
```


Shibboleth IdP 3.2からSignatureValidationFilterのrequireSignedMetadataがrequireSignedRootに変更となりました。
requireSignedMetadataの場合、下記のwarningメッセージが表示されます。

```
2015-12-18 18:33:35,232 - WARN [net.shibboleth.idp.profile.spring.relyingparty.metadata.filter.impl.
SignatureValidationParser:128] - file [/opt/shibboleth-idp/conf/metadata-providers.xml] Use of the attribute
'requireSignedMetadata' is deprecated, use 'requireSignedRoot' instead
```

Shibboleth IdP 3.1の情報

学認メタデータの読み込みはconf/metadata-providers.xmlで設定します。

- conf/metadata-providers.xml

conf/metadata-providers.xml

```
<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="RequiredValidUntil" maxValidityInterval="P15D" />
    <MetadataFilter xsi:type="SignatureValidation"
                    requireSignedMetadata="true"
                    certificateFile="%{idp.home}/credentials/gakunin-signer-2010.cer"/>
    <MetadataFilter xsi:type="EntityRoleWhiteList">
        <RetainedRole>md:SPSSODescriptor</RetainedRole>
    </MetadataFilter>

</MetadataProvider>
```

ローカルSPメタデータ

ローカルSPのメタデータはmetadata以下に配置して、conf/metadata-providers.xmlで設定します。

- conf/metadata-providers.xml
  SP1のメタデータ sp1-metadata.xmlとSP2のメタデータ sp2-metadata.xmlをmetadata以下に配置して、conf/metadata-providers.xmlでそれぞれのメタデータを読み込む設定例を以下に示します。

conf/metadata-providers.xml

```
    <!--
    Example file metadata provider.  Use this if you want to load metadata
    from a local file.  You might use this if you have some local SPs
    which are not "federated" but you wish to offer a service to.

    If you do not provide a SignatureValidation filter, then you have the responsibility to
    ensure that the contents are trustworthy.
    -->

    <!--
    <MetadataProvider id="LocalMetadata"  xsi:type="FilesystemMetadataProvider" metadataFile="PATH_TO_YOUR_METADATA"/>
    -->
    <MetadataProvider id="LocalMetadataForSP1"  xsi:type="FilesystemMetadataProvider" metadataFile="%{idp.home}/metadata/sp1-
metadata.xml"/>
    <MetadataProvider id="LocalMetadataForSP2"  xsi:type="FilesystemMetadataProvider" metadataFile="%{idp.home}/metadata/sp2-
metadata.xml"/>
```

差分

```
     <!--
     Example file metadata provider.  Use this if you want to load metadata
     from a local file.  You might use this if you have some local SPs
     which are not "federated" but you wish to offer a service to.

     If you do not provide a SignatureValidation filter, then you have the responsibility to
     ensure that the contents are trustworthy.
     -->

     <!--
     <MetadataProvider id="LocalMetadata"  xsi:type="FilesystemMetadataProvider" metadataFile="PATH_TO_YOUR_METADATA"/>
     -->
+    <MetadataProvider id="LocalMetadataForExampleSP1"  xsi:type="FilesystemMetadataProvider" metadataFile="%{idp.home}
/metadata/examplesp1-metadata.xml"/>
+    <MetadataProvider id="LocalMetadataForExampleSP2"  xsi:type="FilesystemMetadataProvider" metadataFile="%{idp.home}
/metadata/examplesp2-metadata.xml"/>
```

参考: 学内システムとして構築する場合の設定