メタデータのvalidUntilを検証する設定方法

ここでは、新しいシステム運用基準(Ver.1.1?)(2010年11月29日公開)から新たに要求されている、メタデータに記載された有効期限(validUntil)に従うようにIdP/SPを設定する方法を説明します。

学認では有効期間が14日になるようにメタデータを生成・公開しています。ダウンロードしたメタデータが有効期間内、つまり最新のものであることを確認することによって、IdP/SPが他の危殆化したIdP/SP、不正を行っていることが発覚したIdP/SP、既に脱退したIdP/SPを誤って信頼することを防ぎ、安全な運用につながります。必ず下記設定を行っていただきますようお願いします。

IdP/SP側では、validUntilチェックを有効化するとともに、validUntilとして受け入れることが可能な最長期間を設定します。メタデータ更新時のタイミングを考慮して、15日間（1296000秒, "P15D"）を設定します。つまり、validUntilが過去のものを拒否するだけではなく、15日間以上未来のものも不正なものとして拒否します。

以下に記載したIdP/SP向けの設定方法は、現行の技術ガイドにすでに取り込まれておりますので、技術ガイドに従って構築した場合は追加の作業は不要です。

IdPの設定方法

relying-party.xmlにおいて，以下のようにvalidUntilのためのMetadataFilterの設定を有効にします．赤字の部分がコメントアウトされている場合は，有効化して下さい．

```
<MetadataProvider id="URLMD" xsi:type="FileBackedHTTPMetadataProvider" xmlns="urn:mace:shibboleth:2.0:metadata"
            metadataURL="http://metadata.gakunin.nii.ac.jp/gakunin-metadata.xml"
            backingFile="/opt/shibboleth-idp/metadata/gakunin-metadata-backing.xml">
   <MetadataFilter xsi:type="ChainingFilter" xmlns="urn:mace:shibboleth:2.0:metadata">
      <MetadataFilter xsi:type="RequiredValidUntil" xmlns="urn:mace:shibboleth:2.0:metadata"
            maxValidityInterval="P15D" />
      <MetadataFilter xsi:type="SignatureValidation" xmlns="urn:mace:shibboleth:2.0:metadata"
            trustEngineRef="shibboleth.MetadataTrustEngine"
            requireSignedMetadata="true" />
      <MetadataFilter xsi:type="EntityRoleWhiteList" xmlns="urn:mace:shibboleth:2.0:metadata">
         <RetainedRole>samlmd:SPSSODescriptor</RetainedRole>
      </MetadataFilter>
   </MetadataFilter>
</MetadataProvider>
```

maxValidityIntervalには，validUntilとして受け入れることが可能な，最長期間を設定します．学認の場合は，validUntilが14日間であるため，メタデータ更新時のタイミングを考慮して，15日間（1296000秒）を設定して下さい．この設定が不適切だと，メタデータダウンロード時に以下のようなエラーになりIdPが立ち上がりません（1296000を129600とした場合のエラー例）．

```
ERROR [edu.internet2.middleware.shibboleth.common.config.BaseService:187] - Configuration was not loaded for shibboleth.
RelyingPartyConfigurationManager service, error creating components. The root cause of this error was: org.opensaml.saml2.metadata.
provider.FilterException: Metadata's validity interval, 1073358297ms, is larger than is allowed, 129600000ms.
```

参考URL: https://wiki.shibboleth.net/confluence/display/SHIB2/IdPMetadataProvider...

SPの設定方法

shibboleth2.xmlにおいて，以下のようにRequireValidUntil MetadataFilterの設定を有効にします．赤字の部分がコメントアウトされている場合は，有効化して下さい．

```
<MetadataProvider type="XML" uri="https://metadata.gakunin.nii.ac.jp/gakunin-metadata.xml"
      backingFilePath="/etc/shibboleth/metadata/backingMetadata.xml" reloadInterval="7200">
    <MetadataFilter type="RequireValidUntil" maxValidityInterval="1296000"/>
    <MetadataFilter type="Signature" certificate="/etc/shibboleth/credentials/gakunin-signer-2010.cer"/>
</MetadataProvider>
```

maxValidityIntervalには，validUntilとして受け入れることが可能な，最長期間を設定します．学認の場合 は，validUntilが14日間であるため，メタデータ更新時のタイミングを考慮して，15日間（1296000秒）を設定して下さい．

なお、SAML 2.0 の仕様ではメタデータに記述された validUntil 属性に指定された時間制限を越えてメタデータをキャッシュすることは禁止（MUST NOT）とされていますが（Metadata for the OASIS SAML V2.0 4.3.1 節を参照）、SP v2.4 未満のバージョンでは MetadataProvider タグの type 属性値が「XML」の場合、ダウンロード間隔を表すreloadInterval 属性が 0 かまたは省略された場合にはリロードが発生しないため、メタデータに記述された validUntil を有効にするためには直前行にある reloadInterval 属性を明示的に 0 以外に指定しなければなりません。

参考URL: https://wiki.shibboleth.net/confluence/display/SHIB2/NativeSPMetadataFilter