ローカルに配置したSPメタデータの証明書更新時のエラー

フェデレーションに参加していないローカルのSPなどにおいて、SP管理者からの指示に従って「https://sp.example.ac.jp/Shibboleth.sso/Metadata」といったURLから取得したメタデータをIdPのローカルに配置して運用している場合、SP側の証明書更新時にエラーが発生する場合があります。（「.../Shibboleth.sso/Metadata」からダウンロードできるファイルはShibboleth SPが自動生成するメタデータです）

例え学認の「メタデータ記載の証明書更新手順（SP）」に倣ってSPが慎重に証明書更新を行っている場合でも、SPメタデータとして /Shibboleth.sso/Metadata を参照している限り発生する可能性があります。以下でその理由をステップバイステップで見ていきます。

1. メタデータ記載の証明書更新手順（SP） の「1日目　SPに対して設定変更1（新証明書を暗号化用として追加）」をSPで実施すると、「.../Shibboleth.sso/Metadata」からダウンロードできるSPメタデータにも新しい証明書が追加されます。新しいメタデータはShibboleth SPの設定に従ってKeyDescriptorに use="encryption" という暗号化用途のみで利用するための設定が追加されます。

SPの設定	SPが自動生成するメタデータ	⇒伝播中⇒	IdPのローカルに配置したメタデータ
旧証明書：署名&暗号化用途 新証明書：暗号化用途	旧証明書：use指定なし 新証明書：use="encryption"		旧証明書：use指定なし

2. SP管理者からの通知に従い、IdP管理者はSPが自動生成するファイルを取得してIdPのローカルにあるメタデータを更新します。

   学認に参加しているSPでは メタデータ記載の証明書更新手順（SP） の「X日目　承認、学認メタデータに反映」に該当する部分です。

SPの設定	SPが自動生成するメタデータ	=伝播済=	IdPのローカルに配置したメタデータ
旧証明書：署名&暗号化用途 新証明書：暗号化用途	旧証明書：use指定なし 新証明書：use="encryption"		旧証明書：use指定なし 新証明書：use="encryption"

3. メタデータ記載の証明書更新手順（SP） の「X+15日目　SPに対して設定変更2（新証明書をメインにし旧証明書を暗号化用に変更）」をSPで実施します。この瞬間、SPに設定された証明書の用途とIdPが想定する証明書の用途に不一致が発生してしまいます。つまりSPは設定通り署名用途として新証明書を使いますが、IdPは新証明書は暗号化用途のみに使えるものと考えているためにこれを受け付けません。IdPでローカルに配置したメタデータが更新されるまでの間この状態が続き、エラーとなることが考えられます。

SPの設定	SPが自動生成するメタデータ	⇒伝播中⇒	IdPのローカルに配置したメタデータ
旧証明書：暗号化用途 新証明書：署名&暗号化用途	旧証明書：use="encryption" **新証明書：use指定なし**		旧証明書：use指定なし **新証明書：use="encryption"**

4. その後「Y+15日目　SPに対して設定変更3（旧証明書削除）」でも問題が生じます。この時点で3.で自動生成されたメタデータがIdPのローカルに配置されていますが、これに暗号化用途の旧証明書が含まれているため、依然としてIdPは旧証明書を暗号化用途に用い、設定変更3が行われたSPではそれを復号できずにエラーとなります。このエラーもIdPでローカルに配置したメタデータが更新されるまで続くことになります。

SPの設定	SPが自動生成するメタデータ	⇒伝播中⇒	IdPのローカルに配置したメタデータ
旧証明書：不使用 新証明書：署名&暗号化用途	**旧証明書：存在しない** 新証明書：use指定なし		**旧証明書：use="encryption"** 新証明書：use指定なし

→ この問題の原因はSPが自動生成したメタデータをそのままIdP側で利用することにあります。 2. において、IdPのローカルに配置するメタデータから新証明書のKeyDescriptorに設定されているuse属性を削除することで、SPの設定変更に影響を受けずにメタデータの更新を行うことができます。（useを指定しない場合は暗号化用途 (encryption) 、署名用途 (signing) のどちらにも利用できるため）
同様に、3.（設定変更2）の後でIdPのローカルに配置するメタデータからは旧証明書を削除しなければなりません。

→ 学認申請システムでは、上記でご紹介した手順と同じで メタデータ記載の証明書更新手順（SP） の「1日目　学認申請システムにて証明書を追加（予備の欄に）」を行ったときには、新証明書のKeyDescriptorのuse属性は設定していません。もちろんX+15日目の旧証明書を削除する申請が承認された段階でSPメタデータから旧証明書が削除されます。