IdP起動時のエラー (javax.net.ssl.SSLPeerUnverifiedException: SSL peer failed hostname validation for name: null)

IdP起動時のメタデータ取得に際し、下記のエラーが idp-process.log に出力されます。

```
javax.net.ssl.SSLPeerUnverifiedException: SSL peer failed hostname validation for name: null
```

→ SSLv3のみをサポートしたWebサーバ（TLSv1.0, TLSv1.1, TLSv1.2等をサポートしていない）からメタデータを取得するときに出力されるエラーメッセージです。

→ relying-party.xmlのメタデータ取得の設定で、MetadataProviderのオプション `disregardSslCertificate="true"` を設定した場合、もしくはIdP 2.3.xの場合には下記の通りエラーログが変化します。 disregardSslCertificate の詳細は https://wiki.shibboleth.net/confluence/display/SHIB2/IdPMetadataProvider#IdPMetadataProvider-FileBackedHTTPMetadataProvider をご参照ください。

```
javax.net.ssl.SSLException: Received fatal alert: bad_record_mac
```

→ 上記「`SSL peer failed hostname validation for name: null`」、「`Received fatal alert: bad_record_mac`」のエラーはIdP 2.4.0, 2.4.3 で確認しています。

→ IdP 2.4.3においてはMetadataProviderのオプション `disregardSslCertificate` の設定の有無に関係なく、JDKのオプション `-Dcom.sun.net.ssl.rsaPreMasterSecretFix=true` を設定することで、SSLv3のみをサポートしたWebサーバからメタデータの取得ができることを確認しています。
※SSLv3のみサポートしたWebサーバとして CentOS 6 (httpd-2.2.15-39.el6.centos.x86_64) で確認していますが、他のWebサーバ実装ではJDKのオプションを設定せずにメタデータが取得できるかもしれません。この場合上記オプションを設定することで逆にエラーになる可能性がありますのでご注意ください。

→ IdP 3.0.0-beta1ではSSLv3のみをサポートしたWebサーバへは上記設定に関わらずアクセスできないことを確認しています。Webサーバ側でTLSのサポートをご検討ください。