トラブルシューティング

IdP関連

IdP起動時のエラー(The entity name must immediately follow the '&' in the entity reference)

IdPを起動時に下記のエラーが idp-process.log に出力されます。

```
14:51:13.419 - INFO [edu.internet2.middleware.shibboleth.common.config.BaseService:158] - Loading new configuration for service
shibboleth.RelyingPartyConfigurationManager
14:51:13.506 - ERROR [edu.internet2.middleware.shibboleth.common.config.BaseService:188] - Configuration was not loaded for
shibboleth.RelyingPartyConfigurationManager service, error creating components.  The root cause of this error was: org.xml.sax.
SAXParseException: The entity name must immediately follow the '&' in the entity reference.
```

→上記のエラーは relying-party.xml にXML文法としての間違いがある場合に出力されます。
→例えば relying-party.xml にパスフレーズ付きの証明書を設定するとき、パスフレーズに '&' や '<' を含む場合はこれらの文字列をそのまま設定することはできません。これらの文字を含む場合は文字参照で & や < のように記述してください。

- 誤ったパスフレーズ設定例

```
    <security:Credential id="IdPCredential" xsi:type="security:X509Filesystem">
        <security:PrivateKey Password="myKeyPa$$word&">
                /opt/shibboleth-idp/credentials/server-enc.key
        </security:PrivateKey>
```

- 正しいパスフレーズ設定例

```
    <security:Credential id="IdPCredential" xsi:type="security:X509Filesystem">
        <security:PrivateKey Password="myKeyPa$$word&amp;">
                /opt/shibboleth-idp/credentials/server-enc.key
        </security:PrivateKey>
```

これはXML形式の表記上の問題ですので、relying-party.xmlに限らず全ての設定ファイルが対象となります。例えばattribute-resolver.xmlのLDAPのパスワード（principalCredential）も同様です。

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。

IdPで認証前にブラウザにエラー(SAML 2 SSO profile is not configured for relying party)

```
Error Message: SAML 2 SSO profile is not configured for relying party https://sp.example.ac.jp/shibboleth-sp
```

→relying-party.xmlにこのSPだけに対する特殊な<RelyingParty>設定があり、かつその中に SAML2SSOProfile の設定が抜けているとこのエラーになります。
　もしくは、このSPが最近追加されたものである場合、IdPが最新のメタデータ取得に失敗している可能性があります。

IdPで認証時にブラウザにエラー(Message was signed, but signature could not be verified)

Shibboleth認証時にブラウザに下記のエラーが出力されます。

```
opensaml::FatalProfileException
The system encountered an error at Tue Apr 30 12:13:14 2013
To report this problem, please contact the site administrator at root@localhost.
Please include the following message in any email:
opensaml::FatalProfileException at (https://sp.example.ac.jp/Shibboleth.sso/SAML2/POST)
Message was signed, but signature could not be verified.
```

→IdPの設定ファイル idp.properties で idp.signing.cert に設定している証明書（対応する秘密鍵は idp.signing.key で指定されていること）と、学認申請システムに登録した証明書が一致することを確認してください。不一致である場合は上記のエラーが出力されます。

→IdPのサーバ証明書を更新するときに idp.properties にて示される証明書ファイルを誤って上書きすると、学認申請システムに登録した証明書と一致しない状態となりエラーとなるケースがあるようです。このケース含め証明書更新過程でのエラーを避けるため、IdPにおけるサーバ証明書の更新方法は技術ガイド：メタデータ記載の証明書更新手順（IdP） をご参照ください。

IdPで認証時にブラウザにエラー(Message expired, was issued too long ago)

Shibboleth認証時にブラウザに下記のエラーが出力されます。

```
opensaml::SecurityPolicyException
The system encountered an error at Tue Apr 30 12:13:14 2013
To report this problem, please contact the site administrator at root@localhost.
Please include the following message in any email:
```

```
opensaml::SecurityPolicyException at (https://sp.example.ac.jp/Shibboleth.sso/SAML2/POST)
Message expired, was issued too long ago.
```

→IdPが動作しているホストの時刻がずれている場合に出力されます。NTPなどでホストの時刻を修正してください。
→参考情報：https://wiki.shibboleth.net/confluence/display/SHIB2/NativeSPTroubleshootingCommonErrors#NativeSPTroubleshootingCommonErrors-opensamlSecurityPolicyExceptionMessageexpiredwasissuedtoolongago

IdPにエラー(net.shibboleth.idp.attribute.resolver.NoResultAnErrorResolutionException: No entries returned from search)

個別のページに移動

学認テンプレートattribute-resolver.xmlをお使いの場合、Shibboleth IdP 3.3.x向け（テンプレートバージョン3.3.0）およびそれ以降では、参照したLDAPにエントリがない場合に以下のエラーが記録されるようになりました。3.3.0より古いテンプレートとエラーとして記録される以外の差異はありません。

認証のためのLDAPルックアップには成功し、属性送信のためのルックアップに失敗しているという異常事態ですので、LDAPに関する設定を今一度ご確認ください。

この状況でSPに遷移せずIdP上でエラーにするには（そうすることを推奨します）以下をご参照ください。
⇒ LDAPにエントリがない場合にIdP上でエラーにする方法

```
20XX-XX-XX XX:XX:XX,XXX - ERROR [net.shibboleth.idp.profile.impl.ResolveAttributes:299] - Profile Action ResolveAttributes: Error resolving attributes
net.shibboleth.idp.attribute.resolver.NoResultAnErrorResolutionException: No entries returned from search
        at net.shibboleth.idp.attribute.resolver.dc.ldap.impl.StringAttributeValueMappingStrategy.map(StringAttributeValueMappingStrategy.java:62)
```

IdPで認証時にエラー

→ IdPが運用フェデレーションとテストフェデレーションの双方に同一のentityIDで参加している場合に、認証エラーとなることがあります。これはテストフェデレーション側のメタデータに掲載されている証明書情報が誤って取り込まれることが原因と推定されています。テストフェデレーション側のIdPについて実運用のIdPと異なるentityIDを利用するなどし、テストフェデレーション側のIdPは廃止申請すると問題の切り分けが行いやすくなります。

→ 関連して、運用フェデレーションで実運用中のIdPにおいて、テストフェデレーションのメタデータを読み込んでいる場合には、テストフェデレーションのメタデータ読み込み設定を削除してください。運用フェデレーションのメタデータのみを読み込む設定としたほうがより原因を追究しやすい状態となります。

→ transientIdが必須となっているSPにおいて、IdP側でtransientIdの送出が制限されている場合にエラーとなる場合があります。要求されている属性が正しく送出されているにも関わらず認証エラーとなる場合にはtransientIdの送出の有無を確認しておくと問題の切り分けに役立ちます。

→ SPが要求している属性と異なる属性を送出している場合にもエラーとなります。学認のIdP・SP一覧（https://www.gakunin.jp/participants/）で指定されている属性とattribute-filter.xmlの設定が一致しているか見直してください。attribute-filter.xmlを設定後、 設定・運用・カスタマイズ#SPに対してどのような属性が送出されるか確認する方法 の手順で実際に送出される属性を確認することができます。特に「eduPersonAffiliation （スコープなし）」と「eduPersonScopedAffiliation （スコープあり）」は似ていることもあり、間違えやすいことから注意が必要です。

IdPで認証時のエラーにより再ログインが要求される (Exception unwrapping data: Tag mismatch!)

IdPでログイン済みなのにSSOせず、下記のエラーが idp-process.log に出力されて、再度ログイン画面が表示されます。

```
2020-11-27 13:12:52,167 - xxx.xxx.xxx.xxx - ERROR [net.shibboleth.utilities.java.support.security.DataSealer:252] - Exception unwrapping data: Tag mismatch!
2020-11-27 13:12:52,178 - xxx.xxx.xxx.xxx - ERROR [org.opensaml.storage.impl.client.ClientStorageService:453] - StorageService shibboleth.ClientSessionStorageService: Exception unwrapping secured data
net.shibboleth.utilities.java.support.security.DataSealerException: Exception unwrapping data
        at net.shibboleth.utilities.java.support.security.DataSealer.unwrap(DataSealer.java:253)
Caused by: javax.crypto.AEADBadTagException: Tag mismatch!
        at java.base/com.sun.crypto.provider.GaloisCounterMode.decryptFinal(GaloisCounterMode.java:623)
```

IdPは、コンポーネントDataSealerにてAES秘密鍵を使ってcookie等を暗号化しています。詳細は SecretKeyManagement を参照してください。

上記エラーは、バージョンアップ等によりIdPに切り替えた際、または複数のIdPによるIdPクラスタリング環境において、コンポーネントDataSealerのAES秘密鍵が異なるため暗号化されたcookie等が復号できなかったことを示すエラーメッセージです。

復号できなかったことにより、IdPは認証済みの情報が取得できず再度ログイン画面を表示して再認証を要求します。

IdPを切り替えた場合は、利用者が新IdPで再認証することで順次新しい秘密鍵で暗号化したcookie等に置き換わりますので、無視しても大丈夫です。無視できない場合は旧IdPからコンポーネントDataSealerのAES秘密鍵をコピーしてください。

IdPクラスタリング環境では、基本的に共通のAES秘密鍵を使う必要があります。1台目のコンポーネントDataSealerのAES秘密鍵をその他のIdPにコピーしてください。

コピーするファイルは下記になります。

- /opt/shibboleth-idp/credentials/sealer.*

IdPで認証時にTomcatのエラー

Shibboleth認証時にブラウザに503エラーが出力され、Tomcatに下記のログが出力されます。

```
[Thu Jun 19 17:00:00 2014] [error] (70007)The timeout specified has expired: ajp_ilink_receive() can't receive header
[Thu Jun 19 17:00:00 2014] [error] ajp_read_header: ajp_ilink_receive failed
[Thu Jun 19 17:00:00 2014] [error] (120006)APR does not understand this error code: proxy: read response failed from [::1]:8009
(localhost)
```

→ IdPが正しく動作していない可能性があります。Tomcatを再起動することで解消するとの報告があります。

→ [upki-fed:00493] でも同様の問題が発生していたとの報告があります。

Tomcat 6.0.43およびそれ以降でのBack-Channel接続のエラー

IdPで使用しているTomcatについて、Tomcat 6.0.43およびそれ以降にアップデートしたあとにSPのログ（/var/log/shibboleth/shibd.log）に以下のエラーが出力され、Back-Channelの接続に失敗します。　（[upki-fed:00925] Tomcat 6.0.43でのBack-Channel接続の不具合について）

```
ERROR Shibboleth.AttributeResolver.Query [3]: exception during SAML query to https://IdPのホスト名:8443/idp/profile/SAML1/SOAP
/AttributeQuery: CURLSOAPTransport failed while contacting SOAP endpoint (https://IdPのホスト名:8443/idp/profile/SAML1/SOAP
/AttributeQuery): error:14094416:SSL routines:SSL3_READ_BYTES:sslv3 alert certificate unknown
ERROR Shibboleth.AttributeResolver.Query [3]: unable to obtain a SAML response from attribute authority
```

→ この問題に対応した tomcat6-dta-ssl-2.0.0.jar が公開されました （Updated Tomcat 6 Connector, JCONN-2）。

→ Tomcat 6.0.43およびそれ以降のバージョンをご利用の場合は学認技術ガイドの手順（IdP > IdPセッティング > サーバ証明書の設定(IdP) > ２．ライブラリのコピー）に従い tomcat6-dta-ssl-**2.0.0**.jar を導入し、旧jarファイル tomcat6-dta-ssl-**1.0.0**.jar（もしあれば tomcat6-dta-ssl-**1.1.0**.jar も）を削除してください。

なお、IdPv3への移行を考慮して「Tomcat 7/8上でIdPバージョン2を動かしたい」という場合には、tomcat6-dta-ssl-x.x.x.jar を使うのではなく、IdPv3向けに用意されております `trustany-ssl.x.x.x.jar` をお使いください。

一部の古いバージョン(tomcat6-dta-ssl-1.1.0.jar)はJava 6の環境では動きません。起動時にcatalina.outに以下のエラーが出力されます。最新版を使うようにしてください。

```
Caused by: java.lang.UnsupportedClassVersionError: edu/internet2/middleware/security/tomcat6
/DelegateToApplicationJSSEImplementation : Unsupported major.minor version 51.0
```

JDK 8u60 , 8u51 , 7u85 , 6u101でのメタデータ取得エラー

IdPで利用しているJDKを JDK 8 update 51もしくは60, 7 update 85, 6 update 101 へアップデートした場合に、メタデータ取得にてエラーとなる問題が報告されています。　（Shib Users ML: Shib IdP - Metadata Download and Java 1.7.0_85）
該当するJDKにアップデートした場合、新規に参加したSPとの連携ができない、また保持しているメタデータの有効期限が切れたあとにはすべてのSPと連携できない状態となりますのでご注意ください。

```
ERROR [org.opensaml.saml2.metadata.provider.HTTPMetadataProvider:273] - [Timer-0:] - Error retrieving metadata
from https://metadata.gakunin.nii.ac.jp/gakunin-metadata.xml javax.net.ssl.SSLPeerUnverifiedException: SSL peer
 failed hostname validation for name: (メタデータリポジトリのIPアドレス)
```

※適宜改行を入れていますが実際には一行で出力されます。
→ Tomcatを起動するときのオプションに「-Djdk.tls.trustNameService=true」をつけて起動することで問題が回避できます。

CentOS 6のtomcat6パッケージを使っている場合には、/etc/sysconfig/tomcat6 にてJAVA_OPTSを設定可能ですので、末尾に以下の行を追加してください。

```
JAVA_OPTS="${JAVA_OPTS} -Djdk.tls.trustNameService=true"
```

学認提供自動起動スクリプト(/etc/init.d/tomcat6 or /etc/init.d/tomcat)を使っている場合には、CATALINA_OPTSにて設定しておりますので、以下の行を修正してください。

```
export CATALINA_OPTS="-Djava.endorsed.dirs=${CATALINA_HOME}/endorsed -Djdk.tls.trustNameService=true "
```

※端末のサイズによっては複数行で表示されているかもしれませんが、一行で入力してください。

この問題はOracle JDKだけでなくOpenJDKでも発生します。
OpenJDKの問題のあるバージョンは以下です（RHEL/CentOS上）。
java-1.6.0-openjdk-1.6.0.36-1.13.8.1.el5_11
java-1.6.0-openjdk-1.6.0.36-1.13.8.1.el6_7
java-1.6.0-openjdk-1.6.0.36-1.13.8.1.el7_1
java-1.7.0-openjdk-1.7.0.85-2.6.1.3.el5_11
java-1.7.0-openjdk-1.7.0.85-2.6.1.3.el6_6
java-1.7.0-openjdk-1.7.0.85-2.6.1.3.el6_7
java-1.7.0-openjdk-1.7.0.85-2.6.1.2.el7_1
java-1.8.0-openjdk-1.8.0.51-0.b16.el6_6
java-1.8.0-openjdk-1.8.0.51-1.b16.el6_7
java-1.8.0-openjdk-1.8.0.51-3.b16.el6_7
java-1.8.0-openjdk-1.8.0.51-1.b16.el7_1

以下のバージョンで問題が解消されたことを確認しています。
Oracle JDK 8u65
6b37-1.13.9-1ubuntu0.{15.10,15.04,14.04,12.04}.1 (Ubuntu 15.10/15.04/14.04 LTS/12.04 LTS 上)
7u91-2.6.3-0ubuntu0.{15.10,15.04,14.04,12.04}.1
java-1.6.0-openjdk-1.6.0.37-1.13.9.4.el5_11
java-1.6.0-openjdk-1.6.0.37-1.13.9.4.el6_7
java-1.6.0-openjdk-1.6.0.37-1.13.9.4.el7_1

attribute-filter.xmlに属性を送信するように設定しているはずなのに送信されない。

→attribute-filter.xml中のAttributeFilterPolicy要素のidが重複していると、最後のものしか有効にならないようです。idが重複しないように修正してください。

2.3.8もしくはそれ以前のIdPで認証前にログにエラー

```
1:19:57.770 - ERROR [org.opensaml.xml.security.SigningUtil:250] - Error during signature verification java.security.
SignatureException: Signature length not correct: got 256 but was expecting 128
```

ブラウザには以下のエラーが表示されます。

```
Error Message: Message did not meet security requirements
```

以下の条件を全て満たす場合、認証要求(AuthnRequest)の署名検証時に確率的に問題が発生することが確認されています。IdPのバグで、2.4.0で修正されました。SPメタデータに記載されている不要な証明書を削除することにより回避可能です。
詳細: https://issues.shibboleth.net/jira/browse/JXT-99

1. IdPがJava 7を使用している。
2. 接続しようとしているSPのメタデータに1024bitの証明書と2048bitの証明書が混在している。
3. SPが認証要求(AuthnRequest)に署名している。

aacli.shが実行できない問題の対処（その1）

Shibboleth IdPにはaacli.shというコマンドがあり、任意のSP(entityID)と任意のユーザ名を引数に与えることでSPに送出される属性がXMLで取得できます。IdP 2.3.5 ～ IdP 2.3.8ではIdPに含まれるファイルが変更となった影響でそのまま実行すると NoClassDefFoundError となります。

```
$ sudo -u tomcat /opt/shibboleth-idp/bin/aacli.sh --configDir /opt/shibboleth-idp/conf/ --principal=test001 --requester=https://sp.
example.ac.jp/shibboleth-sp
Exception in thread "main" org.springframework.beans.factory.BeanCreationException: Error creating bean with name 'shibboleth.
HandlerManager': Initialization of bean failed; nested exception is java.lang.NoClassDefFoundError: javax/servlet/ServletRequest
        at org.springframework.beans.factory.support.AbstractAutowireCapableBeanFactory.doCreateBean
(AbstractAutowireCapableBeanFactory.java:480)
                    :
```

→ 上記エラーが出力された場合はTomcatのjarファイルを参照するようにしてください。

```
$ sudo ln -s $CATALINA_HOME/lib/servlet-api.jar /opt/shibboleth-idp/lib/
```

> CentOS 6のyumでインストールされるtomcat6パッケージについてはファイル名が tomcat6-servlet-2.5-api-6.0.24.jar となっているようですので、これへのシンボリックリンクを作成してください。

→ aacli.shコマンドの詳細は 設定・運用・カスタマイズ > SPに対してどのような属性が送出されるか確認する方法 と https://wiki.shibboleth.net/confluence/display/SHIB2/AACLI をご参照ください。
→ 参考情報 : 情報交換メーリングリストupki-fed:00419

> この問題はIdP 2.4.0で修正されました。https://issues.shibboleth.net/jira/browse/SIDP-557 "servlet-api-2.5.jar"のようなファイル名で自動的に /opt/shibboleth-idp/lib/ にコピーされているはずです。
> IdP 2.4.0にバージョンアップしたあとに以前作成した $CATALINA_HOME/lib/servlet-api.jar へのシンボリックリンクがある場合は削除してください。

aacli.shが実行できない問題の対処（その2）

StoredIDを用いている場合、mysql-connector-java-5.1.xx-bin.jar等のJDBCドライバーが適切に配置されていないと、下記のエラーになります。Shibboleth IdPでStoredIDを利用するための設定方法(MySQL)を参照して /opt/shibboleth-idp/lib/ および /usr/java/tomcat/webapps/idp/WEB-INF/lib/ に配置されていることを確認してください。

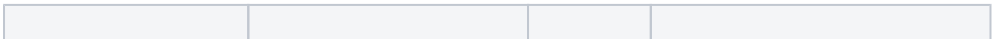
```
# ./bin/aacli.sh --configDir=conf/ --principal="test001" --requester="https://test-sp1.gakunin.nii.ac.jp/shibboleth-sp"
Exception in thread "main" org.springframework.beans.factory.BeanCreationException: Error creating bean with name 'shibboleth.
AttributeResolver': Invocation of init method failed; nested exception is edu.internet2.middleware.shibboleth.common.service.
ServiceException: Configuration was not loaded for shibboleth.AttributeResolver service, error creating components.
...
Caused by: edu.internet2.middleware.shibboleth.common.service.ServiceException: Configuration was not loaded for shibboleth.
AttributeResolver service, error creating components.
...
Caused by: org.springframework.beans.factory.BeanCreationException: Unable to create relational database connector, JDBC driver can
not be found on the classpath
        at edu.internet2.middleware.shibboleth.common.config.attribute.resolver.dataConnector.
StoredIDDataConnectorBeanDefinitionParser.buildApplicationManagedConnection(StoredIDDataConnectorBeanDefinitionParser.java:169)
...
```

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。

SAMLレスポンスを取得する方法

トラブルシューティングのときにSPからSAMLレスポンスを確認したいとの要望を受けることがあります。SAMLレスポンスを取得する方法としてブラウザのJavaScriptを無効にすることでPOSTするデータを取得する方法がありますので、以下に手順を示します。

1. 対象のSPへアクセスし、DSを経由してIdPのログイン画面を表示します。
2. 末尾に記載した手順でJavaScriptを無効にします。
3. 続けてIdPで認証すると、SPにリダイレクトされるときに以下のページが表示されます。

> *Note: Since your browser does not support JavaScript, you must press the Continue button once to proceed.*

4. 右クリックで表示されるメニューから「ページのソースを表示する」を選択してください。「`input type="hidden" name="SAMLResponse" ～`」行の value の値がSAMLレスポンスとなります。
5. SAMLレスポンスの取得が完了したら、以下の手順の逆の操作を行い設定を元に戻してください。

Firefoxの場合は、以下の手順でJavaScriptを無効にできます。

1. アドレスバーに「about:config」を入力します。検索窓に「javascript.enabled」を入力すると現在の設定値が出てきますので、ダブルクリックして`true`から`false`に変更します。

Internet Explorerの場合は、以下の手順でJavaScriptを無効にできます。

1. インターネットオプションから「セキュリティ」タブを開きます。
2. レベルのカスタマイズをクリックし、スクリプト > アクティブスクリプト で「無効にする」を選択後、OKをクリックします。

学認申請システムが自動生成するattribute-filter取得時のエラー

attribute-filterの自動生成機能を使う で紹介されている学認申請システムが生成するattribute-filterを自動取得しているIdPで次のエラーが発生します。（upki-fed:00948）

- 「a) 学認申請システムが生成したattribute-filterを直接読み込む方法」を採用している場合

```
12:55:10.810 - WARN [org.opensaml.util.resource.ResourceChangeWatcher:168] - Resource https://office.gakunin.nii.ac.jp/ProdFed
/export/attribute_filter/PIxxxxJP?target=uapprovejp221 could not be accessed
org.opensaml.util.resource.ResourceException: Unable to contact resource URL: https://office.gakunin.nii.ac.jp/ProdFed/export
/attribute_filter/PIxxxx?target=uapprovejp221
        at org.opensaml.util.resource.HttpResource.exists(HttpResource.java:94) ~[openws-1.4.4.jar:na]
        at org.opensaml.util.resource.FileBackedHttpResource.exists(FileBackedHttpResource.java:120) ~[openws-1.4.4.jar:na]
        at org.opensaml.util.resource.ResourceChangeWatcher.run(ResourceChangeWatcher.java:149) ~[openws-1.4.4.jar:na]
        at java.util.TimerThread.mainLoop(Timer.java:534) [na:1.6.0_22]
        at java.util.TimerThread.run(Timer.java:484) [na:1.6.0_22]
Caused by: javax.net.ssl.SSLHandshakeException: sun.security.validator.ValidatorException: PKIX path building failed: sun.
security.provider.certpath.SunCertPathBuilderException: unable to find valid certification path to requested target
        at sun.security.ssl.Alerts.getSSLException(Alerts.java:192) ~[na:1.6.0_22]
        at sun.security.ssl.SSLSocketImpl.fatal(SSLSocketImpl.java:1697) ~[na:1.6.0_22]
        (...省略...)
Caused by: sun.security.validator.ValidatorException: PKIX path building failed: sun.security.provider.certpath.
SunCertPathBuilderException: unable to find valid certification path to requested target
        at sun.security.validator.PKIXValidator.doBuild(PKIXValidator.java:324) ~[na:1.6.0_22]
        at sun.security.validator.PKIXValidator.engineValidate(PKIXValidator.java:224) ~[na:1.6.0_22]
        at sun.security.validator.Validator.validate(Validator.java:235) ~[na:1.6.0_22]
        at sun.security.ssl.X509TrustManagerImpl.validate(X509TrustManagerImpl.java:147) ~[na:1.6.0_22]
        at sun.security.ssl.X509TrustManagerImpl.checkServerTrusted(X509TrustManagerImpl.java:230) ~[na:1.6.0_22]
        at sun.security.ssl.X509TrustManagerImpl.checkServerTrusted(X509TrustManagerImpl.java:270) ~[na:1.6.0_22]
        at sun.security.ssl.ClientHandshaker.serverCertificate(ClientHandshaker.java:1144) ~[na:1.6.0_22]
        ... 21 common frames omitted
Caused by: sun.security.provider.certpath.SunCertPathBuilderException: unable to find valid certification path to requested
target
        at sun.security.provider.certpath.SunCertPathBuilder.engineBuild(SunCertPathBuilder.java:197) ~[na:1.6.0_22]
        at java.security.cert.CertPathBuilder.build(CertPathBuilder.java:255) ~[na:1.6.0_22]
        at sun.security.validator.PKIXValidator.doBuild(PKIXValidator.java:319) ~[na:1.6.0_22]
        ... 27 common frames omitted
```

→ JDKのトラストアンカーに必要なCA証明書が入っていないことが原因です。「IdPのトラストアンカーの確認と必要なCA証明書の導入」にしたがって， パッケージのアップデート，またはCA証明書の導入を行ってください。

- 「b) 学認申請システムが生成したattribute-filterをローカルにダウンロードした上で読み込む方法」を採用している場合

```
$ wget https://office.gakunin.nii.ac.jp/ProdFed/export/attribute_filter/PIxxxxJP?target=uapprovejp221
--2015-06-29 19:12:37--  https://office.gakunin.nii.ac.jp/ProdFed/export/attribute_filter/PIxxxxJP?target=uapprovejp221
office.gakunin.nii.ac.jp をDNSに問いあわせています... 157.1.67.71
office.gakunin.nii.ac.jp|157.1.67.71|:443 に接続しています... 接続しました。
エラー: office.gakunin.nii.ac.jp の証明書(発行者: /C=JP/O=SECOM Trust Systems CO.,LTD./CN=SECOM Passport for Web EV 2.0 CA)の
検証に失敗しました:
  発行者の権限を検証できませんでした。
office.gakunin.nii.ac.jp に安全の確認をしないで接続するには、`--no-check-certificate’を使ってください。
SSL による接続が確立できません。
```

→ wget等のコマンドが参照するトラストアンカーに必要なCA証明書が入っていないことが原因です。「SPのトラストアンカーの確認と必要なCA証明書の導入」にしたがって， パッケージのアップデート，またはCA証明書の導入を行ってください。SP向けの手順としてご紹介していますが，今回のようなIdPにおけるwgetコマンド等の対処でも手順は同じです。

SP関連

SPで認証後にエラー(A valid authentication statement was not found in the incoming message)

```
opensaml::FatalProfileException
...
opensaml::FatalProfileExceptionat (https://sp.example.ac.jp/Shibboleth.sso/SAML2/POST)
A valid authentication statement was not found in the incoming message.
```

→SPメタデータに記載されている証明書がSPにインストールされていない。
加えて、SPメタデータに複数証明書が記載されており、その一部がインストールされていない場合、タイミングによってエラーになったりならなかったりするので特に注意が必要。

また、比較的最近構築されたIdPを用いている場合、IdPが利用する暗号アルゴリズムをSPがサポートしていない場合（例えば古いOS上でShibboleth SPを動作させている場合）にこのエラーが発生する場合があるようです。詳細およびIdP側での一時的対処方法は以下をご参照ください。
⇒SPにおけるAES-GCM暗号対応状況

SPからDSに遷移したときにDSでエラー （その1）

SPからDSに遷移したときにDSにて以下のようにブラウザにエラーが表示される。

```
    エラー: 無効なクエリです
    The return URL 'https://sp.example.ac.jp/Shibboleth.sso/DS' could not be verified for Service Provider 'https://sp.example.ac.jp
/shibboleth-sp'.
```

→学認技術ガイドに従ってSPを設定した場合、DSからのリターンURLは 'https://HOSTNAME/Shibboleth.sso/DS' となります。学認申請システムでSPの登録を行なうときに「DSからのリターンURL 」項目がこの値になっていない場合には上記のエラーが表示されます。

→なお、学認技術ガイドの「２．DSサーバの参照設定を行います。」において、SessionInitiatorのLocationを変更した場合にはDSからのリターンURLも変わります。例えば <SessionInitiator type="Chaining" Location="/ABC"...> としたときのDSからのリターンURLは 'https://HOSTNAME/Shibboleth.sso/ABC' となります。また、shibboleth2.xmlにSessionInitiatorが1つも存在しない場合にはデフォルト値の 'https://HOSTNAME/Shibboleth.sso/Login' を使用してください。

SPからDSに遷移したときにDSでエラー （その2）

```
エラー: 無効なクエリです
リターンURL 'https://sp.example.ac.jp/Shibboleth.sso/DS' はSP 'https://SP.example.ac.jp/shibboleth-sp' のものとみなされません
```

→ 例えば、学認申請システムにentityIDを「https://SP.example.ac.jp/shibboleth-sp」（ホスト部の SP だけが大文字）のように登録したときにDSでこのようなエラーが発生します。DSでは大文字・小文字を区別して動作しますが、DNSにおいてホスト名は大文字・小文字を区別しないことが一般的です。利用する環境によっては大文字のホスト名が自動的に小文字で処理されることがあり、エラーとなります。エラー画面が表示されているときのアドレスバーに注目しますと、 return= から始まる部分が自動的に小文字となってしまっていることが確認できると思います。

> *https://test-ds.gakunin.nii.ac.jp/WAYF?entityID=https%3A%2F%2FSP.example.ac.jp%2Fshibboleth-sp&return=https%3A%2F%2Fsp.example.ac.jp%2FShibboleth.sso%2F...*

SAML2でバックチャネル接続エラー

SAML2でIdPに接続したときに下記のようなバックチャネルの接続エラーが発生することがあります。

```
2012-11-16 17:45:00 ERROR Shibboleth.AttributeResolver.Query [6]: exception during SAML query to https://idp.example.ac.jp:8443/idp
/profile/SAML2/SOAP/AttributeQuery: CURLSOAPTransport failed while contacting SOAP endpoint (https://idp.example.ac.jp:8443/idp
/profile/SAML2/SOAP/AttributeQuery): connect() timed out!
2012-11-16 17:45:00 ERROR Shibboleth.AttributeResolver.Query [6]: unable to obtain a SAML response from attribute authority
```

→上記のエラーはIdP(idp.example.ac.jp)のattribute-filter.xmlに接続元SPへの属性送出設定がない(属性が受け渡されない)とき、SAML2でBack-Channelポートにfallbackするため発生します。IdP側のファイアウォールなどでBack-Channel(ポート8443)への接続が許可されていない場合にタイムアウトとなることがあります。いずれにしろ設定により属性は渡されませんので、このエラーによる実害は（ブラウザ表示の遅延以外は）特にありません。
→SAML2対応IdPのみ接続するときに「SPでBack-Channelを使用しないようにする設定」を以下に記載します。学認外のIdPと連携する場合など、SAML1で属性受け渡しをする可能性があるときは属性取得できなくなりますので、SAML2でかつBack-Channelを利用しないときだけに用いてください。

- /etc/shibboleth/shibboleth2.xml で次の部分をコメントアウト

```
        <!-- Use a SAML query if no attributes are supplied during SSO. -->
        <!--
        <AttributeResolver type="Query" subjectMatch="true"/>
        -->
```

SP起動時のエラー(error while loading resource (/etc/shibboleth/shibboleth2.xml): XML error(s) during parsing, check log for specifics)

SPを起動時に下記のエラーが出力されます。

```
$ sudo /etc/init.d/shibd start
Starting shibd: configuration is invalid, check console for specific problems
                                                           [FAILED]
```

また /var/log/shibboleth/shibd.log には下記のエラーが出力されています。

```
2013-02-12 14:36:06 ERROR XMLTooling.ParserPool : fatal error on line 105, column 145, message: expected entity name for reference
2013-02-12 14:36:06 ERROR Shibboleth.Config : error while loading resource (/etc/shibboleth/shibboleth2.xml): XML error(s) during
parsing, check log for specifics
2013-02-12 14:36:06 FATAL Shibboleth.Config : caught exception while loading configuration: XML error(s) during parsing, check log
for specifics
```

→上記のエラーは shibboleth2.xml にXML文法としての間違いがある場合に出力されます。
→例えばCredentialResolverにパスフレーズ付きの証明書を設定するとき、パスフレーズに '&' や '<' を含む場合はこれらの文字列をそのまま設定することはできません。これらの文字を含む場合は文字参照で & や < のように記述してください。

- 誤ったパスフレーズ設定例

```
<CredentialResolver type="File" key="cert/server-enc.key" certificate="cert/server-enc.crt" password="myKeyPa$$word&"/>
```

- 正しいパスフレーズ設定例

```
<CredentialResolver type="File" key="cert/server-enc.key" certificate="cert/server-enc.crt" password="myKeyPa$$word&amp;"/>
```