IdPv3アップデートに関する情報

Shibboleth SPのアップデートに関してはこちらをご覧ください。⇒SPv3アップデートに関する情報

Shibboleth IdPバージョン4がすでにリリースされております。V4へのアップデートに関してはこちらをご覧ください。⇒IdPv4アップデートに関する情報

バージョン共通

1. アップデート前の注意点

1. $CATALINA_BASE/conf/Catalina/localhost/idp.xml に unpackWAR="false" が含まれると構成が大きく変更されるアップデート時（自動デプロイ時）にエラーが発生する場合があるようです。当該ファイルを確認し指定があれば削除しておいてください。（技術ガイドに沿った構築では含まれません）

2. アップデート手順

shibboleth-identity-provider-3.x.x.tar.gzパッケージを展開したディレクトリで、以下のコマンドで設定ファイルの変更点を確認し、適宜反映した上で、アップデートを実行します。

/opt/shibboleth-idp/以下に存在しないファイル/ディレクトリはアップデート時に自動的に作成されますが、インストール後修正したファイルのほか、修正していないファイルも一切上書きはされませんので、新バージョンの内容を適宜反映してください。各自で修正していないファイルはdist/以下のファイルで上書きする、各自で修正したファイルは新バージョンでの変更点をマージする形になります。

反映しない場合、旧来の機能は変わらず動作することが保証されますが、新バージョン以降の新機能が（デフォルトで有効な場合と有効化した場合いずれも）正しく動作することが保証されません。このため、将来的な新機能利用も見据えて、アップデート後でもかまいませんのでなるべく早く反映するようにしてください。

uApproveJPをインストールしている場合はsystem/以下の修正が元に戻ってしまうので、アップデート前に展開したディレクトリの当該ファイルを修正した上でアップデートを行うのがお勧めです。system/以下の修正箇所をパッチ形式にしたものを置いておきますので、展開したディレクトリにて適用してください。
uapprovejp3-system.patch

```
$ patch -p0 < .../uapprovejp3-system.patch
```

3.3.xおよびそれ以前から3.4.xへのアップデートの場合はディレクトリ構造が変わっておりますので、展開したインストールパッケージ同士を比較して設定ファイルの変更点を確認してください。例：

```
# diff -rb ../shibboleth-identity-provider-3.3.3/ ../shibboleth-identity-provider-3.4.0/
```

なお、**3.3.xへ**のアップデートの場合は以下のようにdistディレクトリ同士を比較していました。（dist/以下のファイルにはファイル名の末尾に .dist が付いていました）

```
# diff -rb /opt/shibboleth-idp/dist/ dist/
```

```
# diff -rb -x LICENSE.txt -x bin -x credentials -x doc -x idp_ant¥¥.log -x logs -x metadata -x system /opt/shibboleth-idp/dist/ .
（配布物として旧バージョンからの変更点の確認）
# bin/install.sh -Didp.conf.filemode=640 -Didp.conf.credentials.filemode=640
```

```
Source (Distribution) Directory (press <enter> to accept default: [/root/shibboleth-identity-provider-3.3.0]
[Enter] ←入力なし
Installation Directory: [/opt/shibboleth-idp]
[Enter] ←入力なし
Rebuilding /opt/shibboleth-idp/war/idp.war ...
...done

BUILD SUCCESSFUL
Total time: 5 seconds
#
```

本アップデート手順はTomcatを起動したまま行うことを前提としております。もしTomcatが起動していない状態の場合は、古いバージョンのキャッシュを削除するため以下のコマンドを実行してください。

```
# rm -r $CATALINA_BASE/webapps/idp $CATALINA_BASE/work/Catalina/localhost/idp
```

なお、Tomcat 8.0.21およびそれ以降を使っており、autoDeploy="true"およびdeployOnStartup="true"の設定になっている場合は、上記操作の必要なく、起動したままでも停止した状態でも、自動デプロイが機能するはずです。

アップデート後、以下のコマンドでバージョンが更新されていることを確認してください。

```
$ /opt/shibboleth-idp/bin/status.sh | grep idp_version
idp_version: 3.3.1
```

アップデート直後は古いバージョンを示すことがあるので、その場合はしばらくしてから再度確認してください。

3. アップデート後の注意点

1. /opt/shibboleth-idp/の下にold-2016MMDD-XXXX/というようなディレクトリが作成されるようですが、運用には不要です。

```
# ls /opt/shibboleth-idp/old-20160509-0810/
bin/    dist/   doc/    system/ webapp/
```

2. $CATALINA_BASE/lib/等に/opt/shibboleth-idp/webapp/WEB-INF/lib/以下もしくは/opt/shibboleth-idp/dist/webapp/WEB-INF/lib/以下のJARファイルへのシンボリックリンクがある場合は、アップデート後にバージョンが変わりファイル名が変更になっている可能性があるのでその場合はシンボリックリンクを変更し、Tomcatを再起動すること。
3. 次節以降で取り上げたバージョン間の変更点以外にも、細かな変更が存在する場合があります。変更点はShibboleth WikiのReleaseNotesに網羅されていますのでご参照ください。
   ⇒https://wiki.shibboleth.net/confluence/display/IDP30/ReleaseNotes

IdP 3.4.x から IdP 3.4.x へのアップデートに関する情報

3.4.6でのコード変更により一部の特殊なIdPプラグインを使っている場合にエラーが発生するという報告が上がっていますのでご注意ください。またそのようなプラグインがありましたら学認事務局まで情報提供いただけましたら幸いです。
詳細: https://wiki.shibboleth.net/confluence/display/IDP30/ReleaseNotes#ReleaseNotes-3.4.6(Oct2,2019)
参考: https://marc.info/?l=shibboleth-users&m=157019539119083&w=2

3.4.2に限らないと思われますが、Mapped AttributeDefinitionにて空文字列になる属性値を生成した場合、エラーになるという情報があります。このような使い方は想定されておりませんのでご注意ください。
詳細: https://issues.shibboleth.net/jira/browse/IDP-1389

3.4.2固有の問題で、Template AttributeDefinitionにてDependencyを用いた古い記法を使っている場合にエラーになります。記述をInputAttributeDefinitionおよびInputDataConnectorを用いた新しい記法に改めるか、3.4.3もしくはそれ以降にアップデートしてください。
詳細: https://issues.shibboleth.net/jira/browse/IDP-1386

3.4.2にて以下のDEPRECATED warningを出力するようになりましたが、実際には<SourceAttribute>を使用していなくても出力されることがあります。<SourceAttribute>を使用していない場合は無視してください。

```
08:38:46.114 -  - WARN [DEPRECATED:118] - XML Element 'SourceAttribute', (file [/opt/shibboleth-idp/conf/attribute-resolver.xml]):
This will be removed in the next major version of this software; replacement is by using <InputAttributeDefinition> and
<InputDataConnector>
```

詳細: https://issues.shibboleth.net/jira/browse/IDP-1383

3.4.1までで認証後に下記エラーが出るときがあるとの報告があります。該当する場合は3.4.2もしくはそれ以降にアップデートしてください。

```
org.springframework.binding.expression.EvaluationException: An ELException occurred getting the value for expression
'authenticationContext.setAttemptedFlow(thisFlow)' on context [class org.springframework.webflow.engine.impl.
RequestControlContextImpl]
```

詳細: https://issues.shibboleth.net/jira/browse/IDP-1163

attribute-resolver.xmlで記述する sourceAttributeID はDEPRECATEDでv4で削除予定ですが、3.4.1まではComputedIdおよびStoredIdDataConnecterにおいて代替の記述をするとエラーで起動できなくなります。申し訳ありませんが該当するバージョンをお使いの場合は当該DataConnectorのみ古い記述をお使いください。
詳細: https://issues.shibboleth.net/jira/browse/IDP-1359

3.4.0で配布されている設定ファイルのうち conf/admin/general-admin.xml に誤字がありましたので、3.4.0の配布ファイルをご利用の場合は以下を参考に修正してください。

```
--- shibboleth-idp-3.4.0/dist/conf/admin/general-admin.xml    2018-10-15 02:46:42.799299813 +0900
+++ shibboleth-idp-3.4.1/dist/conf/admin/general-admin.xml    2018-11-02 13:22:41.215327718 +0900
@@ -39,7 +39,7 @@
         <!-- Metadata Query -->
         <bean parent="shibboleth.AdminFlow"
             c:id="http://shibboleth.net/ns/profiles/mdquery"
-            p:loggingId="MetadataQuery}"
+            p:loggingId="MetadataQuery"
             p:policyName="AccessByIPAddress" />

         <!-- REST AccountLockoutManager Access -->
```

v4へ向けて

Shibboleth IdPバージョン4では3系で非推奨とされている記法のいくつかが削除され、そのままの設定ファイルでは動かない可能性があります。ただし、v2→v3のときのようにファイル構成自体が変更されることは予定されていません。また、新機能を除いてv4で許容される記法は3.4系の最新版でも有効であることが保証されます。つまり、3.4を動かしている間に将来v4で問題にならないように設定ファイルを変更しておくことが推奨されています。

詳細を別ページにまとめました。
⇒IdPv4アップデートに関する情報

その他の情報

- 3.4およびOracle JDK / OpenJDK 11を使っており、LDAPサーバへの接続にLDAPSを使っている場合、以下のエラーになるという情報があります。

  ```
  java.lang.NullPointerException: Thread local SslConfig has not been set
  ```

原因はJDKのバグであるとのことです。該当する場合、以下でUnboundIDを使う回避策が提示されています。
https://wiki.shibboleth.net/confluence/display/IDP30/LDAPonJava>8
詳細: https://issues.shibboleth.net/jira/browse/IDP-1357

- OpenJDK 8u272固有の問題（ただしOracle JDKについては不明）で、LDAPサーバへの接続にTLS（つまりStartTLSとLDAPS両方）を使っている場合に以下のエラーが発生するという問題が報告されております。原因はJDKのバグでありこれを含めた修正版の8u275がリリースされておりますのでそちらをお使いください。
8u272を使う必要性がある場合は、上述のUnboundIDを使う回避策をご検討ください。

```
  org.ldaptive.provider.ConnectionException: javax.net.ssl.SSLPeerUnverifiedException: hostname of the server '' does not
match the hostname in the server's certificate.
```

詳細:https://marc.info/?l=shibboleth-users&m=160430766512138&w=2

IdP 3.3.x から IdP 3.4.x へアップデートする場合の注意点

1. 3.4.0以降Shibboleth IdPのディレクトリ構成が webapp/ から dist/webapp/ に変更になりました。以前のバージョンから該当するバージョンへアップデートする場合は、$CATALINA_BASE/lib/等に当該ディレクトリへのシンボリックリンクがないか確認し、もしあれば修正しておいてください。
2. 3.4.0以降ではserver.keyのパーミッションへの特殊な扱いが不要になりました。3.3.xおよびそれ以前から3.4.xおよびそれ以降へのアップデートの場合は、技術ガイドにおける設定と一致するように、以下を実行してください。

```
# chown root:tomcat /opt/shibboleth-idp/credentials/server.key
# chmod 640 /opt/shibboleth-idp/credentials/server.key
```

3. 3.4.0へのアップデートで、idp.sealer.storePasswordもしくはidp.sealer.keyPasswordにシングルクオートを含む場合、アップデート後の起動に失敗するという情報があります。該当する場合は3.4.0を避け3.4.1およびそれ以降にアップデートしてください。
4. attribute-resolver.xmlにおいて厳密な記述が不可能だった<Dependency>要素は非推奨となり、代わりに<InputAttributeDefinition>要素および<InputDataConnector>要素が導入されました。
5. 3.4.0よりcommons-dbcp2-2.x.x.jarが同梱されるようになっています。つまりTomcatのバージョン等によらずMySQL等のデータソースの指定に以下のclassが指定できます。

```
class="org.apache.commons.dbcp2.BasicDataSource"
```

6. 以前同梱されていたconf/mvc-beans.xmlは同梱されなくなりました。特に修正していなければ削除しても大丈夫です。

以下準備中

< #idp.authn.flows.initial = Password
< #idp.authn.resolveAttribute = eduPersonAssurance
web.xml COOKIE http-only secure
idp.hsts idp.frameoptions idp.csp -> web.xml DynamicResponseHeaderFilter 2か所
テストはweb.xml更新してから SLO省かれているカスタマイズして 空にすれば出さなくできる
diff -r ../shibboleth-identity-provider-3.3.3/views/logout.vm ./views/logout.vm
"Use of secure property is strongly advised" WARNログ
AttributeQuery Consent
> <bean id="shibboleth.consent.AttributeQuery.Condition" parent="shibboleth.Conditions.FALSE" />
attended restart
impersonate
> p:checkAddressCondition="#{getObject('%{idp.session.consistentAddressCondition:null}'.trim()) ?: %{idp.session.consistentAddress:true}}"
/>
p:reuseCondition="false" MFA
shibboleth.ComputedIdExceptionMap

IdP 3.3.x から IdP 3.3.x へのアップデートに関する情報

3.3.xにて（3.2.xでも同様かは不明）、かつTomcat 8.0.xを使用している一部の環境の場合、IE / EdgeでSLOした後再度認証しようとするとエラーになるという問題があります。同様の問題で困っているかたはidp.xmlの記述を最新版にしてください。
詳細その1: https://issues.shibboleth.net/jira/browse/IDP-1141
詳細その2: 貴学にてIdPv3をインストールする場合の構築手順 の「5. idp.war の登録」の<CookieProcessor alwaysAddExpires="true" />の行

3.3.1にて、relying-party.xmlのp:defaultAuthenticationMethodsで従来使えていた文字列として記述する記法が使えなくなりました。エラーメッセージ：

```
Caused by: java.lang.IllegalStateException: Cannot convert value of type [java.lang.String] to required type [java.security.
Principal] for property 'defaultAuthenticationMethods[0]': no matching editors or conversion strategy found
```

以下のように記述することができますが、以下のようにいずれの用途にも適さないためお勧めしません。①デフォルトで表示される認証方式を変更したい場合は conf/authn/general-authn.xml のbeanの順序を変更してください。（上にあるものが優先的に選択されます）
②ある特定のSPに対して利用できる認証方式を制限する用途には、relying-party.xml にて p:authenticationFlows="#{{'X509'}}" のように認証方式を指定してください。

1. 一般的に他の認証方式が使用不可能になる
2. 認証方式を特定のものに制限する目的として見た場合、回避手段が存在する

```
...
                <bean parent="Shibboleth.SSO">
                    <property name="defaultAuthenticationMethods">
                        <list>
                            <bean parent="shibboleth.SAML1AuthenticationMethod"
                                c:method="urn:ietf:rfc:2246" />
                        </list>
                    </property>
                </bean>
...
                <bean parent="SAML2.SSO">
                    <property name="defaultAuthenticationMethods">
                        <list>
                            <bean parent="shibboleth.SAML2AuthnContextClassRef"
                                c:classRef="urn:oasis:names:tc:SAML:2.0:ac:classes:TLSClient" />
                        </list>
                    </property>
                </bean>
...
```

3.3.1へのアップデートで system/messages/ に配置した日本語リソースが削除されるとの情報があります。お手数ですが messages/ に再度配置してください。
詳細: GakuNinShare:Shibboleth IdP 3 - メッセージの多言語化
詳細: Shibboleth Wiki:MessagesTranslation のコメント欄

3.3.2にてIDP-1207への対処のため views/login.vm に変更が入っております。dist/views/login.vm.dist と比較して必要な修正を取り込んでください。配布物での差分は以下の通りで、「ログインを記憶しません。」チェックボックスが特定の条件下（forceAuthn時）に指定通りにならないため当該条件の下では表示しないようにするものです。コメントにある通り多要素認証等を使っている場合は適宜修正してください。

```
@@ -66,12 +66,16 @@
                  <input class="form-element form-field" id="password" name="j_password" type="password" value="">
                </div>

+               ## You may need to modify this to taste, such as changing the flow name its checking for to authn/MFA.
+               #if (!$authenticationContext.getActiveResults().containsKey('authn/Password'))
                <div class="form-element-wrapper">
                  <input type="checkbox" name="donotcache" value="1" id="donotcache">
                  <label for="donotcache">#springMessageText("idp.login.donotcache", "Don't Remember Login")</label>
                 </div>
+               #end
+
              #end

                <div class="form-element-wrapper">
                  <input id="_shib_idp_revokeConsent" type="checkbox" name="_shib_idp_revokeConsent" value="true">
                  <label for="_shib_idp_revokeConsent">#springMessageText("idp.attribute-release.revoke", "Clear prior granting of
permission for release of your information to this service.")</label>
```

3.3.xからのアップデートに限りませんが、秘密鍵server.keyのパーミッションが600で上書きされるため、Tomcatをtomcatユーザで起動している場合はserver.keyの所有者をtomcatにしておく必要があります。またtomcatユーザによる上書きを防ぐため、アップデート後に、アップデートプロセスにより変更されたserver.keyのパーミッションを元に戻します。

```
# chmod 400 /opt/shibboleth-idp/credentials/server.key
```

その他の情報

- 3.3.xに限りませんが、/opt/shibboleth-idp/webapp/ がまだ存在するバージョン（3.3.xおよびそれ以前）の場合、サードパーティ製のJARファイルのアップデートのみを行う場合に注意が必要です。
例えば tiqrshibauthn-2.0.jar から tiqrshibauthn-2.1.jar に更新する場合、古いファイルを削除する

```
rm /opt/shibboleth-idp/edit-webapp/WEB-INF/lib/tiqrshibauthn-2.0.jar
```

とともに webapp/ 配下の同名ファイルを削除しておいてください。

```
rm /opt/shibboleth-idp/webapp/WEB-INF/lib/tiqrshibauthn-2.0.jar
```

- 3.3.xに限りませんが、Java 7からJava 8へ移行する場合は以下の情報を参照してください。
⇒貴学にてIdPv3をインストールする場合の構築手順の動作要件の「Java 7 or 8」の項
- 3.3.xに限りませんが、Tomcatの起動に10分前後時間がかかり、それが問題になるような場合は以下の情報を参照してください。
⇒貴学にてIdPv3をインストールする場合の構築手順の動作要件の「Java 7 or 8」の項
- 2.xからのアップグレードの項に追記した通りスクリプトやQueryTemplateでの$requestContextの使用が制限されておりますが、V4では$requestContext自体がなくなる見込みです。代替手段をご検討ください。
⇒ScriptedAttributeDefinitionの"V2 Compatibility"の項, QueryTemplate
- 2.xからのアップグレードの項に追記した通り、NameIDの送出方法が大幅に変更されており、Transient ID送出に関する従来の記述は不要になっております。当該記述は削除することをお勧めします。

IdP 3.2.x から IdP 3.3.x へアップデートする場合の注意点

3.2.1およびそれ以前で発見されていた<ResultCache>要素の脆弱性が修正されましたので、LDAP result caching機能が必要な方は再度有効化してください。
2016-11-21 [upki-fed:01087] 【補足情報】【注意喚起】Shibboleth IdPの脆弱性について

また、上記メールに記載がありますが、3.2.1およびそれ以前で以下のログが記録されしばらくすると認証処理がストップする（通信環境が不安定な場合にロックする）という問題にも対処が入っておりますので、この問題に遭遇されていた方は今一度ご確認ください。

```
2016-09-13T08:37:30.402+01:00 - WARN [org.ldaptive.AbstractOperation$ReopenOperationExceptionHandler:277] - Operation exception
encountered, reopening connection
```

> 上記の3.3.0での対処は、上記のようにログが表示される状況でも認証処理がストップしないようにするものですので、ログ出力自体がなくなる訳ではありません。当該ログはLDAPのコネクションプールを維持する処理で接続が切断されており再接続の必要が生じた場合に記録されます。なお、接続が切断される要因として、長期のLDAP接続をファイアウォールが切断している例があるようです。

以下で指摘されていたSLOのエラーについては、3.3.0で解消されています。詳細についてはFull SLO(Single Logout)の設定方法の末尾の注意事項をご覧ください。
2016-01-15 [upki-fed:01005] Re: Shibboleth 3.2 Logout時エラーについて

メッセージファイルのファイル構成が変更されています。旧構成でも新機能を使わない限り運用可能ですが、新構成に切り替えるにはservices.xmlのshibboleth.MessageSourceResourcesを/opt/shibboleth-idp/dist/conf/services.xml.distを参考に更新してください。その際、idp.logoなど従来の3ファイルに加えていた変更を/opt/shibboleth-idp/messages/messages.propertiesに追記して変更を維持してください。
3.3.0以降向けの日本語メッセージファイルも Shibboleth IdP 3 - メッセージの多言語化 のリンク先から提供されています。/opt/shibboleth-idp/messages/以下に配置して利用してください。すでに同名のファイルが存在する場合はマージしてください。か、3.3.0以降での手順では/opt/shibboleth-idp/system/messages/以下に配置するようになっています。

3.2でのattribute-filter.xmlに続き、3.3ではattribute-resolver.xmlについて名前空間のフラット化（resolver:やdc:等の除去）が行われております。ただし従来の記法も使えますので、アップデートに際して書き換えなくても大丈夫です。
フラット化の対応手順は別ページに記載しておりますのでご参照ください。

3.3.0にて認証処理時のリグレッションが発生しています。詳細はReleaseNotesに記載されていますので"IDP-1101"で検索してください。

以前のバージョンにて/idp/statusにアクセスすると以下のような不要なERRORログが記録される問題に対処が入っております。ただし以前のバージョンの conf/logback.xml を引き続き使っている場合は修正されませんので、dist/conf/logback.xml.dist を参考に修正してください。

```
2016-06-27 12:34:56,760 - ERROR [org.apache.velocity:96] - ResourceManager : unable to find resource 'status.vm' in any resource
loader.
```

2016年11月21日以前の技術ガイドに沿って構築した場合、設定ファイルのパーミッションに問題がありアップデート後に正常に起動しない可能性があります。以下にならってパーミッションを修正した上でアップデートを適用してください。

```
# find /opt/shibboleth-idp/conf -type d -exec chmod g+s {} ¥;
# chown tomcat:root /opt/shibboleth-idp/credentials/server.key
# chmod 400 /opt/shibboleth-idp/credentials/server.key
```

1行目の修正点は、アップデート時に新規ファイル/ディレクトリが作成される場合も適切なowner/groupを維持するためのものです。
2,3行目は、server.key（に限らずcredentials/以下の.keyで終わるファイル）はアップデートプロセスによりrw-------に強制されるので、ownerがrootでかつTomcatをtomcatユーザで起動していると動作しなくなることに対する対処です。

その他の情報

Tomcatの脆弱性およびそれに関連してyumパッケージのパーミッション修正が不完全な件が流れています。
2016-11-21 [upki-fed:01086] 【補足情報】【注意喚起】Tomcatの脆弱性修正版リリースについて(2016/11/1)

IdP 3.2.x から IdP 3.2.x へのアップデートに関する情報

JVMヒープサイズの推奨値が1.5GB(-Xmx1500m)に上方修正されておりますので、適宜自動起動スクリプトを更新してください。
2016-05-16 [upki-fed:01048] Re: Shibboleth IdP実行環境におけるJVMのヒープサイズについて

古いJavaを使っているとメタデータ取得に失敗するという情報がありました。
2015-08-21 [upki-fed:00954] 最新のJava(Oracle JDK/OpenJDK)を使った場合のメタデータ取得エラー

3.2.xで特定の条件で認証応答に署名がないという問題に遭遇した場合は3.3.0以降にアップデートしてください。詳細はReleaseNotesに記載されていますので"IDP-920"で検索してください。

その他の情報

四半期に一度のペースでJava(OpenJDKおよびOracle JDK)のセキュリティアップデートがリリースされています。
2016-05-16 [upki-fed:01049] Re: 【注意喚起】OpenJDKおよびOracle Javaの脆弱性について(2016/4/22)
今回の内容としては、JMXポートの脆弱性、毎回恒例の暗号系の改善(GCM, DSA)、MD5withRSAの拒否、（今回のものではありませんが）OpenJDK 7のECC対応、など。

IdP 3.1.x から IdP 3.2.x へアップデートする場合の注意点

以下のページを参照のこと。
⇒https://www.switch.ch/aai/guides/idp/installation/#keepinguptodate

3.1.xの時代から edit-webapp/WEB-INF/ 以下にweb.xmlを配置している場合、この記述が古くなっている可能性があります。インストールパッケージを展開したディレクトリの webapp/WEB-INF/web.xml と比較し必要な変更を取り込んでください。

3.2ではattribute-filter.xmlについて名前空間のフラット化（afp:やbasic:等の除去）が行われております。ただし従来の記法も使えますので、アップデートに際して書き換えなくても大丈夫です。
フラット化の対応手順は別ページに記載しておりますのでご参照ください。

3.2未満から3.2およびそれ以降にアップデートする場合で、StoredIDを使っている場合、DBのテーブルに変更を加える必要がありますのでご注意ください。詳細は以下をご参照ください。
⇒Shibboleth Wiki > PersistentNameIDGenerationConfiguration > Migrating from Older Versions

IdP 2.x.x から IdP 3.x.x へアップグレードする場合の手順および関連情報

- シボレス実習活用編旧メニュー
- NIIオープンフォーラム2016の「IdP ver.3に向けたNIIの取り組み」および「Shibboleth IdP ver.3との戦い」
- GakuNinShare:Shibboleth IdP 3
- 貴学にてIdPv4をインストールする場合の構築手順
- 上記資料で網羅されておりませんが、スクリプトやQueryTemplateで$requestContextを使っている場合、メソッド等が存在しない場合があるという情報があります。以下を参考に修正してください。
  ⇒ScriptedAttributeDefinitionの"V2 Compatibility"の項, QueryTemplate
- NameIDにTransient IDを入れて送る方法、および他のIDを入れて送る方法が大幅に変更になっており、従来の方法は使えません。紛らわしさをなくすため、attribute-resolver.xmlおよびattribute-filter.xmlにおける従来の設定（IdPv3では意味を持ちません）を削除しておくことをお勧めします。

  以下の記述があれば、丸ごと削除可能です。ただし少しでも変更があれば意図しない挙動の変化を生じる可能性がありますので、一字一句差異がないことを確認してください。

  attribute-resolver.xml:

```
<!-- Name Identifier related attributes -->
<resolver:AttributeDefinition id="transientId" xsi:type="TransientId" xmlns="urn:mace:shibboleth:2.0:resolver:ad">
    <resolver:AttributeEncoder xsi:type="SAML1StringNameIdentifier" xmlns="urn:mace:shibboleth:2.0:attribute:encoder"
        nameFormat="urn:mace:shibboleth:1.0:nameIdentifier" />

    <resolver:AttributeEncoder xsi:type="SAML2StringNameID" xmlns="urn:mace:shibboleth:2.0:attribute:encoder"
        nameFormat="urn:oasis:names:tc:SAML:2.0:nameid-format:transient" />

</resolver:AttributeDefinition>
```

attribute-filter.xml:

```
<!--  Release the transient ID to anyone -->
<AttributeFilterPolicy id="PolicyforAnyone">
    <PolicyRequirementRule xsi:type="basic:ANY" />

    <AttributeRule attributeID="transientId">
        <PermitValueRule xsi:type="basic:ANY" />
    </AttributeRule>
</AttributeFilterPolicy>
```