IdPv4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

V3内のアップデートに関してはこちらをご覧ください。⇒IdPバージョン3アップデートに関する情報

2020年3月11日にリリースされたShibboleth IdP V4に関する情報です。

https://wiki.shibboleth.net/confluence/display/NEWS/2020/03/11/Shibboleth+Identity+Provider+V4.0.0+Released
上記の通りバージョン4.0.0が3/11にリリースされました。下記の注意事項および手順をご確認の上、バージョンアップを行ってください。

なお、バージョン3のEoLは2020年末と公表されました。バージョン3を運用している機関様におかれましてはV4へのバージョンアップのスケジューリングをお願いします。
http://shibboleth.net/pipermail/announce/2020-March/000213.html

学認が提供している技術ガイドも順次更新していきます。uApproveJPやTiqrShib等のNIIが提供しているIdPプラグインは現在バージョン4対応の改修中です。4月に入ってからの公開を予定しております。

また、アップデート時のノウハウなど情報をお持ちの方がいらっしゃいましたら、情報交換ML等で共有いただけましたら幸いです。

Javaのバージョン

- Java 11以上が必須です。
- 公式サポートはJavaのLTSのみなので、2019年12月現在では Java 11 のみとなります。

Javaコンテナ

- Shibboleth IdP v3で利用されていたTomcat 7はサポート対象外となりました。
- Shibboleth開発元がサポートしているのはJetty 9.4、またはTomcat 9以上（参照: SystemRequirements）
    - 開発元はJettyを推奨しています
    - 少なくともServlet 3.1をサポートしたJavaコンテナでなければ動作しません

設定ファイルの移行について

- 名前空間のフラット化が強制され、プレフィックスありの（v2由来の名前空間を使用した）設定ファイルが使用できなくなります
- IdP v3.4ではフラット化していない場合、DEPRECATEDのwarningとしてログに出力されます
    - 3.4.0以降も細かい改善が続けられていますので、v3.4系の最新版で確認してください
    - 静的に解析しているものと動的に解析しているものがあり、3.4系の最新版でしばらく動かしてみることが必要です
    - フラット化の対応手順はこちら
- その他にも、DEPRECATEDのwarningとなる対象が複数あります
    - 影響の大きいものとしては<Dependency>要素は内容によって<InputAttributeDefinition>と<InputDataConnector>に変更が必要
    - 詳細はShibbolethの本家の情報を参照してください。
        - 変更のある要素への置き換え方法へのリンクを含めて記載されています
    - **Shibboleth IdP v4への準備として、v3.4系最新版にてwarningが出なくなるまで設定ファイルを修正することを推奨します**
- すでにフラット化とDEPRECATED対応の学認テンプレートを配布中ですのでこちらも参考にしてください
- LDAP周りで、使用するライブラリがJNDIからUnboundIDに変更になることにより以下の通り設定によってはv4への移行後にエラーになる可能性が若干ございます。
    - LDAPのURL（ldap.propertiesの `idp.authn.LDAP.ldapURL` ）がスラッシュ(/)で終わる場合はうまく動作しませんのでスラッシュを除去してください。
    - 検索フィルタ（ldap.propertiesの `idp.attribute.resolver.LDAP.searchFilter` ）に空白が含まれるとActive Directory等との連携に問題が発生する場合がございますので、空白を除去してください。
    - LDAPConnectorもしくはJAASAuthnConfigurationにてJNDI特有のプロパティを使っている場合問題が発生します。プロパティ名に"jndi"を含むものもしくは下記"binary"にご注意ください。代替のものに置き換えてください。
        - 特にバイナリ属性（objectGUID等）については3.4.5よりLDAPConnectorにて`<BinaryAttributes>`要素がサポートされておりますのでこれで代替してください。プロパティ名は"java.naming.ldap.attributes.binary"となっております。
        - JNDI特有のプロパティとは、例えば、attribute-resolver.xmlの<DataConnector>に以下のような指定がある場合該当します。

```
<LDAPProperty name="com.sun.jndi.ldap.connect.timeout" value="500"/>
```

その他、IdPのディレクトリの中やJavaのディレクトリの中に `jndi.properties` というファイルが存在しその中で指定しているという場合があるようですのでご注意ください。

- **上記問題の対象の場合は、v3.4系最新版で以下に記載されている手順でUnboundIDを使うようにして動作確認することを推奨します**
    - v3.4.4以降で以下の行をldap.propertiesに追加すればJNDIでなくUnboundIDを使うようになります。

```
idp.ldaptive.provider=org.ldaptive.provider.unboundid.UnboundIDProvider
```

- V3系でUnboundIDが使われていることの確認は、idp.propertiesに

```
idp.loglevel.ldap=INFO
```

を追加してログレベルを変更の上再起動し、下記のように"Setting ldap provider to"が UnboundIDProvider になっていることを確認してください。

```
2020-03-02 09:46:50,446 -  - INFO [org.ldaptive.DefaultConnectionFactory:192] - Setting ldap provider to org.ldaptive.provider.unboundid.UnboundIDProvider
2020-03-02 09:46:50,453 -  - INFO [org.ldaptive.DefaultConnectionFactory:192] - Setting ldap provider to org.ldaptive.provider.unboundid.UnboundIDProvider
2020-03-02 09:46:50,453 -  - INFO [org.ldaptive.DefaultConnectionFactory:192] - Setting ldap provider to org.ldaptive.provider.unboundid.UnboundIDProvider
```

確認後、idp.propertiesに追加した行を削除してログレベルを元に戻してください。

- 詳細はこちら: LDAPonJava (v4) および LDAPonJava>8 (v3)

アップデートの手順

shibboleth-identity-provider-4.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。

※手順はTomcatを適用したShibboleth IdP v 3.x からのアップデートを想定しています。

/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
```

```
# 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.credentials.filemode=640 -Didp.conf.credentials.group=tomcat
```

```
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
#
```

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: 4.0.0
```

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。