送信属性同意機能の設定（IdPv4対応uApproveJP）

1. はじめに

本メニューでは、IdPをカスタマイズします。
uApproveJP-4をインストールして実現します。
送信属性の設定をオプショナルとしたり、また必須属性と設定するなど組み込み機能と比べ
柔軟な設定が可能となっています。

---

2. 実習セミナーでは

一般的な手順は「3. 手順書」に記載されています。ただし、本実習セミナー特有の設定内容等を以下に記載しています。
両方を参照しつつ作業を進めてください。

・前提条件

実習セミナーでは、リレーショナルデータベースを用いたものとします。
事前準備として、以下のようにCentOS 7の標準であるMariaDBをインストールし、
起動させておいてください。

```
# yum install mariadb-server
# systemctl start mariadb
```

なお、実習では不要ですが実運用の場合は以下を実行してください。
（OS起動時の自動起動および、rootアカウントにパスワードを設定します）

```
# systemctl enable mariadb
# mysql_secure_installation
```

なお、手順書中mysqlコマンドはMariaDBのものが使われ、プロンプトが mysql> ではなく mariadb> になりますが問題ありません。

・インストール

uApproveJPのパッケージは、「３．手順書」に記載されていますが、実習セミナーでは
予めダウンロードした「/root/PKG」内の uApproveJP-4.0.0-bin.zip を使います。
以下のコマンドを実行して、手順書の記載に合わせて「/usr/local/src」配下に展開しておきます。

```
# cd /root/PKG
# unzip -d /usr/local/src uApproveJP-4.0.0-bin.zip
```

以降、手順書中の $UAPPROVE_INSTALL$ の部分は /usr/local/src/uApproveJP-4.0.0/ と読み替えてください。

・AttributeInMetadataマッチングルール

/opt/shibboleth-idp/conf/attribute-filter.xmlを設定します。

AttributeFilterPolicyGroupタグにuApproveJP用の設定を2箇所に追加します。

```
<AttributeFilterPolicyGroup id="ShibbolethFilterPolicyForGakuNinTestFed"
xmlns="urn:mace:shibboleth:2.0:afp"
xmlns:uajpmf="http://www.gakunin.jp/ns/uapprove-jp/afp/mf"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation="urn:mace:shibboleth:2.0:afp http://shibboleth.net/schema/idp/shibboleth-afp.xsd
http://www.gakunin.jp/ns/uapprove-jp/afp/mf http://www.gakunin.jp/schema/idp/gakunin-afp-mf-uapprovejp.xsd">
```

```
実習セミナーでは、「sn、givenName、mail、eduPersonAffiliation」をオプショナル属性とします。
以下のように4つの属性を全て変更してください。
例）eduPersonAffiliation属性の設定
<!--
<AttributeRule attributeID="eduPersonAffiliation" permitAny="true" />
-->
<AttributeRule attributeID="eduPersonAffiliation">
   <PermitValueRule xsi:type="uajpmf:AttributeInMetadata"
                            matchIfMetadataSilent="true"
                            onlyIfRequired="false"
                            onlyIfChecked="true" />
</AttributeRule>
```

・Java11で動作するように切り替え

mysql-connector-javaインストール時にJava8がインストールされ、Java11ではなくJava8に切り替わっている可能性があります。
以下の手順で確認して、Java8が設定されている場合は、再度Java11を利用できるように切り替えます。

```
# alternatives --config java

There are 2 programs which provide 'java'.

Selection Command
-----------------------------------------------
1 java-11-openjdk.x86_64 (/usr/lib/jvm/java-11-openjdk-11.0.7.10-4.el7_8.x86_64/bin/java)
*+ 2 java-1.8.0-openjdk.x86_64 (/usr/lib/jvm/java-1.8.0-openjdk-1.8.0.262.b10-0.el7_8.x86_64/jre/bin/java)

Enter to keep the current selection[+], or type selection number: 1[Enter] ← Java11が表示されている「1」を選択
```

・Jettyの再起動

Jettyを再起動して、更新した設定ファイルを読み込ませます。

```
# systemctl restart jetty
```

---

3. 手順書

下記の設定手順書を参照し、作業を行います。
※セミナー環境ではShibboleth IdP 4.2.1がインストールされていますので、最新版のuApproveJPバージョン4.0.0をお使いください。
※リンク先のページを開くと、それぞれのバージョンの「インストールおよび設定方法」と記載されたリンクがあるので、
　そのリンクをクリックしてください。
※「1 基本的なデプロイ」から「2.3 ローカライズ」まで行います。ただし「1.6 カスタムテンプレート」および「2.2 テンプレート」は、読み飛ばしてください。
※「1.5 設定のカスタマイズ」では、services-system.xmlとattribute-release-beans.xmlの編集を「Shibboleth IdP 4.1以降では...」の手順で行ってください。
※「3 AttributeInMetadata」については、上記実習セミナーの設定を行います。

- 設定手順書

※補足：属性選択画面の必須属性とオプショナル属性について
　uApproveJPでは、IdP側の設定（conf/attribute-filter.xmlの<PermitValueRule xsi:type="uajpmf:AttributeInMetadata" onlyIfChecked="true">）と
　SPメタデータの設定（//md:SPSSODescriptor/md:AttributeConsumingService/md:RequestedAttribute）に基づいて属性を必須かオプショナルにわけられます。（詳細は後述）
　オプショナル属性はチェックボックスによりユーザに属性の送信を委ねます。必須属性はユーザによる属性毎送信拒否の設定が行えません（チェックボックスにチェックが入った状態でグレーアウトしています）。
　また、IdP側の設定にある<PermitValueRule xsi:type="uajpmf:AttributeInMetadata" onlyIfChecked="true">以外のルールで、送信が許可された属性は全て
　必須属性となります。ここで「<PermitValueRule ...>以外」とは、onlyIfChecked="false"の場合の他、xsi:type="ANY"等のルールも含まれます。

PermitValueRuleに与える設定と属性選択画面の表示の組み合わせを表にすると、以下のようになります。

	SPメタデータ	
	<md:AttributeConsumingService>なし	<md:AttributeConsumingService>あり

				<md:RequestedAttribute>なし	<md:RequestedAttribute>あり	
					isRequired="false"もしくは指定なし	isRequired="true"
IdP設定（attribute-filter）	<PermitValueRule xsi:type="uajpmf:AttributeInMetadata" onlyIfChecked="true">	onlyIfRequired="false" matchIfMetadataSilent="false"	表示しない	表示しない	オプショナル属性	必須属性
		onlyIfRequired="false" matchIfMetadataSilent="true"	オプショナル属性	表示しない	オプショナル属性	必須属性
		onlyIfRequired="true" matchIfMetadataSilent="true"	オプショナル属性	表示しない	表示しない	必須属性
		onlyIfRequired="true" matchIfMetadataSilent="false"	表示しない	表示しない	表示しない	必須属性
	<PermitValueRule xsi:type="uajpmf:AttributeInMetadata" onlyIfChecked="true">　以外		必須属性	必須属性	必須属性	必須属性

なお、「表示しない」については属性送信もされません。

---

4. 動作確認

① 設定後、Jettyの再起動を行ってない場合は行なってください。

```
systemctl restart jetty
```

② 各自が使用するSPの接続確認用ページにアクセスします。

```
例）1番を割り振られた場合 https://ex-sp-test01.gakunin.nii.ac.jp/
```

③ ログインボタンをクリックします。

④ DSの所属機関の選択画面が表示されるので、各自が使用するIdPを選択します。

⑤ IdPのログイン画面が表示されるので、Username/Passwordを入力して認証を行います。

⑥ 送信可能な属性値の一覧画面が表示されます。オプショナル属性と指定したsurname、givenName、mail、eduPersonAffiliation
のみ選択できるチェックボックスが表示され、その他の属性にはチェックの入ったチェックボックスが
グレーアウトして表示され、チェック解除できないことを確認してください。
次に、「次回ログイン時に再度チェックします。」を選択し、同意ボタンをクリックします。
※オプション情報を全て選択せずに行います。（surname、givenName、mail、eduPersonAffiliation）

⑦ 属性受信の確認ページが表示されるので、オプション情報の属性が送信されていない事を確認します。

⑧ 一旦ブラウザを閉じ、再度ログインします。オプション情報の「surname」を選択し、同意ボタンを
クリックします。

⑨ 属性受信の確認ページで「surname」が正しく受信された事を確認してください。

※送信可能な属性値の一覧画面にある「同意方法の選択」を「このサービスに送信する情報が
変わった場合は、再度チェックします。」などに変更して、次回も送信属性同意確認が行われるか、
試してみてください。（同意確認時の設定が保存されます）
保存した対象となるSPにアクセスしても同意確認が行われなくなるのですが、ログイン画面にて
「このサービスへの属性送信の同意を取り消します。」にチェックしてログインしてください。
すると、保存されていた情報がクリアされ、再度送信属性確認が行われます。

※送信属性の同意情報は、組み込み機能と違いサーバ側（リレーショナルデータベース）に保存している為、
はじめに認証し同意情報を保存したブラウザと違うものを使用しても、Firefoxで言うCookieなどが保存
されないプライベートウィンドウを使用しても、保存した情報が有効になります。
（どこからアクセスしても、同一ユーザが同一サービスに対して保存した同意情報が有効）
⑨まで確認できたら、IEやFirefoxのプライベートウィンドウを使うなどして、保存した同意情報が有効であるか
確認してみてください。