Shibboleth IdP 3のユーザ同意機能とuApproveJPとの相違点

Shibboleth IdP 3のユーザー同意機能とuApproveJPの相違点をまとめているページです。

- 属性選択画面
  - 必須属性とオプショナル属性
  - 再同意時の属性選択画面
  - 属性の表示順のカスタマイズ
  - 属性の説明
  - 属性のSPでの使用用途の通知
- 属性送信確認画面
- Attribute Query
- 属性送信済みSPの一覧
- ストレージ

属性選択画面

必須属性とオプショナル属性

uApproveJPでは、conf/attribute-filter.xmlの<PermitValueRule xsi:type="uajpmf:AttributeInMetadata" onlyIfChecked="true">とSPメタデータの//md:SPSSODescriptor/md:AttributeConsumingService/md:RequestedAttributeに基づいて属性を必須属性とオプショナル属性にわけ、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。<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。

		<md:AttributeConsumingService>なし	<md:AttributeConsumingService>あり		
			<md:RequestedAttribute>なし	<md:RequestedAttribute>あり	
				isRequired="false"	isRequired="true"
<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

Shibboleth IdP 3では、conf/idp.propertiesのidp.consent.allowPerAttributeプロパティをtrueに変更することでチェックボックスを表示することは可能ですが、conf/attribute-filter.xmlやSPメタデータによらず表示される全ての属性がチェックボックスが選択済みとして表示されます。

再同意時の属性選択画面

uApproveJPでは、下記の場合に、前回送信した属性のチェックボックスを選択済みとし、前回送信した属性と変化がある属性については変化を表すアイコンを表示します。

- 前回の属性選択画面で「毎回確認」を選択した場合
- 前回の属性選択画面で「保存する」を選択した場合、送信属性が変化している場合

Shibboleth IdP 3には同等の機能はありません。

属性の表示順のカスタマイズ

uApproveJPでは、conf/uApprove.propertiesのar.attributes.orderプロパティで表示する属性の順序をカスタマイズ可能で、かつar.attributes.orderプロパティにない属性についてはar.attributes.orderプロパティの属性の後に属性idの文字列順で表示します。

Shibboleth IdP 3では、属性idの文字列順で表示します。3.2.0以降よりconf/idp.propertiesのidp.consent.attributeOrderプロパティで表示する属性の順序がカスタマイズ可能になる予定です。[IDP-624]

属性の説明

uApproveJPでは、conf/attribute-resolver.xmlの//resolver:AttributeDefinition/resolver:DisplayDescriptionで定義されている属性毎の説明を表示する機能があります。

Shibboleth IdP 3では、3.2.0以降よりviews/intercept/attribute-release.vmから$attributeDisplayDescriptionFunctionを呼び出すことで属性毎の説明を表示できる予定です。[IDP-637]

属性のSPでの使用用途の通知

uApproveJPでは、SP管理者がSPメタデータに記述した//md:SPSSODescriptor/md:Extensions/uajpmd:RequestedAttributeExtensionを利用して、SPが使用する属性についてユーザに属性の使用用途(例えば、「mail属性を登録ページのメールアドレス欄の初期値として使用します」など)を通知する機能を有しています。

Shibboleth IdP 3には同等の機能はありません。

属性送信確認画面

uApproveJPでは、属性送信確認画面にてSPに送信する必須属性、属性選択画面で選択した属性を表示して最終確認を促します。

Shibboleth IdP 3には同等の機能はありません。

Attribute Query

uApproveJPでは、SPからのpersistent-idによるAttribute Queryに対して、ユーザの同意に基づいて応答を返します。具体的な挙動は下記の通りです。

- 「毎回確認」の場合は、同意済みの属性情報がない場合と同じ形式の応答を返します。
- 「保存する」の場合は、ストレージから取得した同意済み属性情報と比較して値が変化していない属性だけを応答します。
- 「表示しない」の場合は、最新の属性情報をすべて応答します。

Shibboleth IdP 3では、persistent-idによるAttribute Queryに対して、ユーザの同意に基づかずに、常に最新の属性情報をすべて応答します。

属性送信済みSPの一覧

uApproveJPでは、属性を送信したSPを一覧にして表示する機能があり、サービス名やバックチャネルによる取得状況がわかり、また個々のSPの同意の削除ができます。

Shibboleth IdP 3には同等の機能はありません。

ストレージ

uApproveJPでは、送信情報の記録をJDBCを利用してMySQLやHSQLに保存します。

Shibboeleth IdP 3では、送信情報の記録をストレージ機能を介してブラウザのCookie、Java Persistence API(JPA)を利用してSQLデータベース、Memcachedなどに保存します。uApproveJPと同じSQLデータベースを利用したとしても使用するテーブルが異なるためuApproveJPからアップグレードすることはできません。