学認のIAL2およびAAL2の技術情報

学認が提供しておりますIAL2およびAAL2文書に準拠していることを示すための技術情報を記します。

IALおよびAALを格納する要素・属性

SAMLでの規定およびREFEDS等での利用から、下記要素・属性を用いることとする。

- 学認のAALを格納するために AuthnContextClassRef を用いることとする
  参照: https://docs.oasis-open.org/security/saml/v2.0/saml-core-2.0-os.pdf
- 学認のIALを格納するために eduPersonAssurance属性を用いることとする
  参照: https://meatwiki.nii.ac.jp/confluence/display/GakuNinShibInstall/eduPersonAssurance

SPからの多要素認証要求

SAMLの規定により、認証要求(AuthnRequest)には AuthnContextClassRef という認証方式に関するパラメーターを含めることができる。
通常は無指定であり、どんな認証方式でもOKであることを表す。
例えば、パスワード認証は以下の識別子で指定できる：
urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtectedTransport

認証要求の AuthnContextClassRef を使うと、通常はパスワード認証でOKだが、機密度・重要度の高いサービスは「パスワードでない何か」を求めることができる。

学認のIAL2/AAL2を示す識別子

AAL2については認証要求およびアサーションのAuthnContextClassRefに下記識別子を格納することとする。

- 識別子: “https://www.gakunin.jp/profile/AAL2”

IAL2についてはアサーションのeduPersonAssurance属性に下記識別子を格納することとする。

- 識別子: “https://www.gakunin.jp/profile/IAL2”

Shibboleth SPでの記述例

AAL2を要求する記述例

Apache設定

```
<Location /restricted-attrviewer/ialaal.php>
    ShibRequestSetting authnContextClassRef https://www.gakunin.jp/profile/AAL2
</Location>
```

IAL2を受信する記述例

PHPコード

```
$ary = preg_split("/(?<!￥￥);/", $_SERVER["assurance"]);
foreach ($ary as $val) {
    if ($val == "https://www.gakunin.jp/profile/IAL2") {
        ....
    }
}
```

AAL2を受信（要求に応えるのはSAML的にMUSTだが念の為）

PHPコード

```
if ($_SERVER["Shib-AuthnContext-Class"] == "https://www.gakunin.jp/profile/AAL2") {
```

Shibboleth IdPでの設定方法例

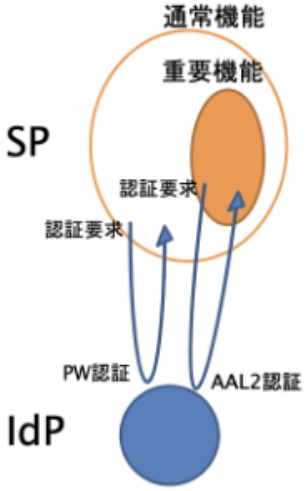
AAL2について:

- MultiFactor認証フロー(MFA)を用いた認証設定
  https://meatwiki.nii.ac.jp/confluence/x/UJSPAQ
  - これは、SPからの要求に合わせてIdPが持っている複数のログインフロー（認証手段）から適切なものを組み合わせて実行するもの
  - 以下の識別子で挙動を変える例を提示している
    urn:mace:gakunin.jp:idprivacy:ac:classes:Level1
    urn:mace:gakunin.jp:idprivacy:ac:classes:Level2
    urn:mace:gakunin.jp:idprivacy:ac:classes:Level3
- 認証フローは別途用意しなければならない。例えば：
  - パスワード認証
  - TLSクライアント証明書認証 https://meatwiki.nii.ac.jp/confluence/x/34W5
  - TOTP認証 https://shibboleth.atlassian.net/l/c/DH9FeWJv
  - tiqr認証 https://meatwiki.nii.ac.jp/confluence/display/tiqr
    など
- 他のIdPにプロキシする場合などは設定方法が異なる

IAL2について：

- eduPersonAssurance属性の設定は通常の属性と同じ

AAL2利用シナリオ例：ステップアップ認証パターン



1. (SP)AAL2に限定しないログインを行う
   - ここでAAL2で認証された場合はセッションにフラグを立てる
2. (SP)ログイン後の処理・ユーザー操作を受け付ける
3. (SP)AAL2を要求する機能を要求された場合
   a. (SP)AAL2で認証したことがない場合
      i. (SP)AAL2限定のログインを行う
         - DSにてAAL2をサポートしたIdPのみ表示する
      ii. (SP)AAL2で認証されたことが確認できればフラグを立てる
   b. (SP)フラグが立っていれば当該機能を提供する

他の考慮点：AAL2付与されないIDへの救済措置

メタデータへの記載

IdPのIAL2/AAL2対応状況やSPの要求状況を示すための、メタデータへの記載方法については検討中である。

関連資料

IdP側改修における要求仕様例：

- IdPIAL2AAL2対応.docx（Wordファイル）

東京大学での試行における技術情報提供：

- Shibboleth単体ではなく、Azure ADで多要素認証を行いShibboleth IdPと連携して属性送出を行うことを試みています。
- NIIオープンフォーラム2022発表資料
  （オープンフォーラム内次世代認証連携における学認のポリシとサービス技術トラックにおけるパネルディスカッションより）