Microsoft 認証基盤を用いた学認対応 IdP による IAL2,AAL2 対応方針検討報告書

2023 年 3 月

目次

1. はじめに

本書は、Microsoft 社製認証基盤を用いて作られている学術認証フェデレーション IdP システムについて IAL2,AAL2 に関する取り扱いにどの程度の汎用性があるかを確認するための対応計画書である。

2. 目的・ゴール

Microsoft 社製認証基盤を用いて作られている学術認証フェデレーション IdP システムの検証環境にて、以下機能の実現可否を調査し、調査報告書を提示する。

2.1. IAL2 について

(1) Shibboleth IdP の属性ストアに格納されているユーザの身分が教員、職員、学生だった場合に、
SAML の eduPersonAssurance 属性として、以下の識別子を SP に対して送出することを調査する
「https://www.gakunin.jp/profile/IAL2」

2.2. AAL2 について

(1) SP から送信される認証要求の AuthnContextClassRef 要素に以下が含まれる場合、Azure MFA による多要素認証が行われることを調査する
「https://www.gakunin.jp/profile/AAL2」
(2) 上記(1)の多要素認証が成功した場合、認証応答の AuthnContextClassRef 要素に、以下を設定して SP に応答を送出すること調査する
「https://www.gakunin.jp/profile/AAL2」
(3) 上記(1)の多要素認証が失敗した場合、条件ごとに適切な応答が行われることを調査する
(a) SP にログインできないこと
(b) SP からの認証要求に多要素認証以外の方式(パスワード認証等)が追加で指定された場合
(AuthnContextClassRef 要素に他の識別子が含まれる場合)は、AuthnContextClassRef 要素で指定された認証が行われ、SP に応答を送出すること。この際、認証応答の AuthnContextClassRef 要素には以下が含まれないこと
「https://www.gakunin.jp/profile/AAL2」
(4) 多要素認証対応していない SAML1.x の要求において、以下 SP を用いてどのような応答となるかを調査する
「https://attrviewer13.gakunin.nii.ac.jp/」

3. スコープ

3.1. 環境

Microsoft 社製認証基盤を用いて作られている学術認証フェデレーション IdP システムの検証環境を準備して検証する。

3.2. サービス・機能

以下の製品・アプリケーション機能を対象として検証を行う。

- ADFS
- Shibboleth IdP
- Shibboleth SP
- Azure MFA

3.3. シナリオ

以下のシナリオ範囲内で検証を行う。

1. ユーザが IAL2 及び AAL2 に対応した SP にアクセスする
2. SP が認証要求を IdP に送出する
3. IdP が SP からの認証要求をもとに認証方法を判断し、ユーザに認証を要求する
4. ユーザが認証を行う
5. ユーザの認証情報をもとに IdP が SP に対して認証応答を送出する
6. SP が認証応答をもとにユーザの認可を行う
7. ユーザが SP にログインする

4. システム・環境

以下の環境で実施する。

「ADFS＋AzureMFA＋Shibboleth-IdP（Shibboleth-SP 認証連携）」

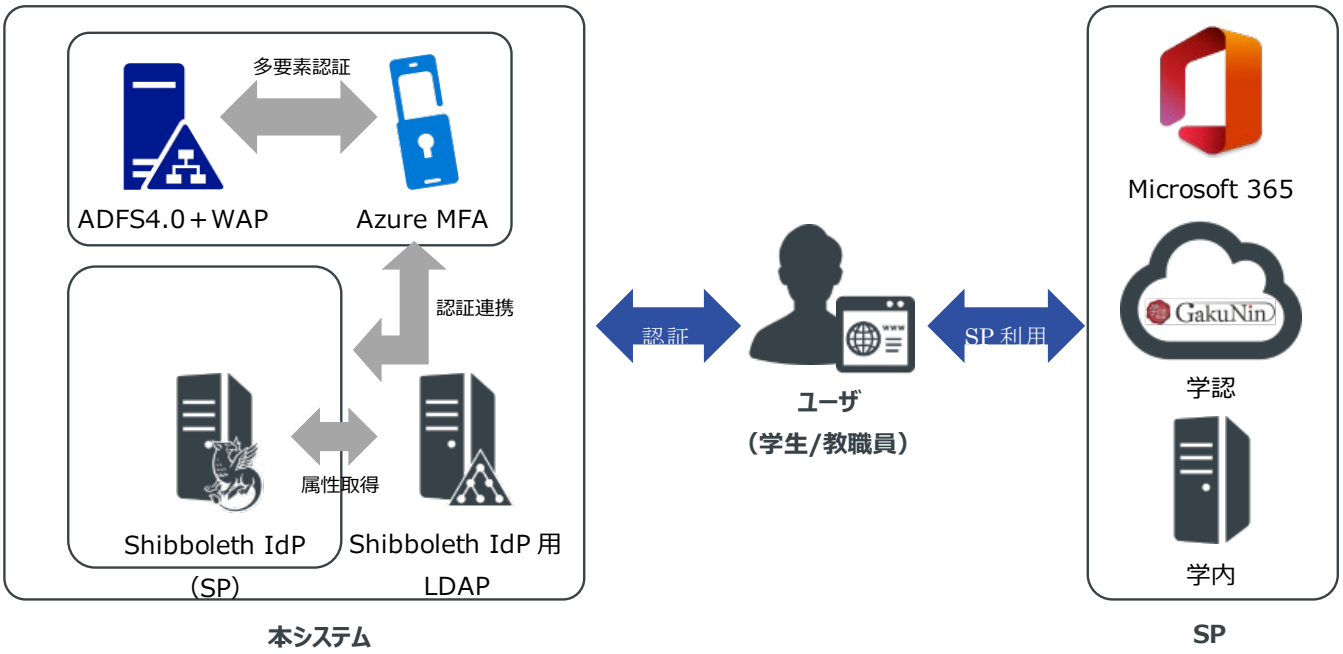

図 4-1　検証環境

- データは検証環境用のダミーデータを用いる
- データは検証環境のユーザとする

表 4-1 検証用アプリケーション構成

アプリケーション	バージョン
Azure MFA	Microsoft Azure サービス
ADFS+WAP	Windows Server 2019
Shibboleth IDP	Apache 2.4 系
	Apache-Tomcat9 系
	shibboleth-identity-provider-4 系
	shibboleth-sp-3 系
Shibboleth IDP 用 LDAP	389 Directory Server2.2 系

4.1. IAL2 について

eduPersonAssurance 属性を表示する機能を SP に持たせる

4.2. AAL2 について

SP からの認証要求内の AuthnContextClassRef に「https://www.gakunin.jp/profile/AAL2」が含まれる場合に、多要素認証を要求するように Shibboleth IdP を設定する

5. 実施内容

5.1. IAL2 について

5.1.1. 検証用 SP の構築

Shibboleth SP を用いて検証用 SP を構築する。

表 5-1 検証用 SP のアプリケーション構成

アプリケーション	バージョン
Shibboleth SP	Apache 2.4 系
	shibboleth-sp-3 系

5.1.2. 属性確認用テストアプリケーションの作成

- 以下の情報を参考に属性確認用テストアプリケーションを作成する

・学認の IAL2 および AAL2 の技術情報
https://meatwiki.nii.ac.jp/confluence/pages/viewpage.action?pageId=91396040

- eduPersonAssurance 属性を表示する機能を持たせる

5.1.3. 検証作業

1. Shibboleth IdP の設定変更
   検証用 SP の設定
2. シナリオに従ってブラウザから SP にアクセス
3. IAL2 についての目的・ゴールが実現可能か検証
   (1) Shibboleth IdP の属性ストアに格納されているユーザの身分が教員、職員、学生だった場合に、
   SAML の eduPersonAssurance 属性として、以下の識別子を SP に対して送出すること
   「https://www.gakunin.jp/profile/IAL2」

5.2. AAL2 について

5.2.1. 検証用 SP の構築

Shibboleth SP を用いて検証用 SP を構築する。

表 5-2 検証用 SP のアプリケーション構成

OS・アプリケーション	バージョン
Shibboleth SP	Apache 2.4 系
	shibboleth-sp-3 系

5.2.2. 属性確認用テストアプリケーションの作成

➢ 以下の情報を参考に属性確認用テストアプリケーションを作成する

・学認の IAL2 および AAL2 の技術情報

https://meatwiki.nii.ac.jp/confluence/pages/viewpage.action?pageId=91396040

AuthnContextClassRef の値を表示する機能を持たせる

5.2.3. 検証作業

1. Shibboleth IdP の設定変更
   検証用 SP の設定
   AuthnContextClassRef 送信設定
2. ADFS の設定変更
   AuthnContextClassRef 受信設定
   AuthnContextClassRef による認証方法変更設定
   AuthnContextClassRef 送信設定
3. シナリオに従ってブラウザから SP にアクセス
4. AAL2 についての目的・ゴールが実現可能か検証
   (1) SP から送信される認証要求の AuthnContextClassRef 要素に以下が含まれる場合、Azure MFA による多要素認証が行われること
   「https://www.gakunin.jp/profile/AAL2」
   (2) 上記(1)の多要素認証が成功した場合、認証応答の AuthnContextClassRef 要素に、以下を設定して SP に応答を送出すること
   「https://www.gakunin.jp/profile/AAL2」
   (3) 上記(1)の多要素認証が失敗した場合、条件ごとに適切な応答が行われること
   (a) SP にログインできないこと
   (b) SP からの認証要求に多要素認証以外の方式(パスワード認証等)が追加で指定された場合(AuthnContextClassRef 要素に他の識別子が含まれる場合)は、AuthnContextClassRef 要素で指定された認証が行われ、SP に応答を送出すること。この際、認証応答の AuthnContextClassRef 要素には以下が含まれないこと

「https://www.gakunin.jp/profile/AAL2」

(4) 多要素認証対応していない SAML1.x の要求において、以下 SP を用いてどのような応答となるかを確認する

「https://attrviewer13.gakunin.nii.ac.jp/」

6. 計画

6.1. 計画 1

6.1.1. 期間

2023 年度

6.1.2. 実施内容

- 計画書作成
- IAL2 AAL2 対応
  - 検証環境構築
  - 属性確認用テストアプリケーション実装

成果物

- Microsoft 認証基盤を用いた学認対応 IdP による IAL2,AAL2 対応方針計画書（本文書）

6.2. 計画 2（予定）

6.2.1. 期間

2023 年度 2 ヶ月間程度（2023 年 6 月から 7 月末を想定）

6.2.2. 実施内容

- IAL2 対応
  - SP 側での eduPersonAssurance 受信確認
- AAL2 対応
  - ADFS での AuthnContextClassRef 受信設定
  - ADFS での AuthnContextClassRef による認証方法変更設定
  - ADFS 及び Shibboleth IdP での AuthnContextClassRef 属性送信設定
  - SP 側での AuthnContextClassRef 受信確認

成果物

- Microsoft 認証基盤を用いた学認対応 IdP による IAL2,AAL2 対応調査結果報告書
  - 実施環境概要図
  - 設定パラメータ例（AzureMFA, ADFS, Shibboleth IdP, Shibboleth SP）
  - 実施結果

以上