京都大学の統合認証システムにおける SAML プロキシの活用

池田 健二 [1)], 古村 隆明 [1)], 片桐 統 [1)]

1) 京都大学 情報環境機構

ikeda.kenji.8s@kyoto-u.ac.jp

Leveraging SAML Proxy in Kyoto University Integrated Authentication System

Kenji Ikeda[1)], Takaaki Komura[1)], Osamu Katagiri[1)]

1) Information Management and Communication, Kyoto University

概要

SAML（Security Assertion Markup Language）は、IdP（Identity Provider）と SP（Service Provider）の間でユーザの認証情報や属性情報を主に Web ブラウザを介して安全にやり取りするための XML ベースのプロトコルである。通常、SAML 認証では IdP と SP の間で信頼関係を直接築くことで認証連携を実現するが、IdP と SP の間に SAML プロトコルのプロキシサーバを挟んで認証を行うことも可能である。本稿では、京都大学情報環境機構の統合認証システムにおける、SAML プロキシ技術の活用について述べる。

1 はじめに

京都大学情報環境機構では、SAML 認証方式を用いた統合認証システムを運用し、本学構成員に対してシングルサインオンの仕組みを提供している。統合認証システムは、パスワード認証に対応した IdP（以下、パスワード認証サーバ）と多要素認証に対応した IdP（以下、多要素認証サーバ）の 2 種類のサーバから構成されている。パスワード認証サーバは Shibboleth IdP で構築しており、多要素認証サーバはセシオス社の Secioss Access Manager Enterprise を利用している。パスワード認証サーバと認証連携している SP の数は約 100、多要素認証サーバと認証連携している SP の数は約 20 である。統合認証システムと連携する SP は多種多様で、学内システムの他に、学認に登録された学外システムやクラウドベンダーが提供するクラウドサービスも含まれる。

情報環境機構では以前より、学生用メールとして Microsoft 社のクラウドサービス Microsoft365 のメール機能を利用しており、統合認証システムのパスワード認証サーバと認証連携させて学生への提供を行ってきた。2023 年より、学生と教職員が Microsoft365 の機能を使って資料共有できるように、教職員に対しても Microsoft365 サービスの提供を開始した。運用方針として、学生と教職員を同一テナントで異なるカスタムドメインを割り当てて運用することとなった。 Microsoft365 の SAML 認証連携設定において、Microsoft365 の仕様では、異なるカスタムドメインに同じエンティティ ID の IdP を設定することができない。Microsoft365 の教職員用カスタムドメイン設定のために専用の IdP サーバを新規構築することは現実的ではないため、SAML の認証・属性送出の処理を中継する SAML プロキシを用意することとした。

この SAML プロキシの構築をきっかけに、IdP 同士で信頼関係を確立しておくことで柔軟な認証連携を組み立てられることがわかった。たとえば、パスワード認証サーバに登録された SP の認証処理を多要素認証サーバに渡すような連携を行えば、SP 側の設定を一切変更することなく、その SP の認証方式をパスワード認証から多要素認証に切り替えることが可能となる。

本稿では、情報環境機構の統合認証システムにおける SAML プロキシの活用について、システム構成や運用状況と合わせて説明する。

2 SAML プロキシ

2.1 SAMP プロキシの概要

SAML 認証では SP は認証連携する IdP との信

頼関係を確立しておき、SP は IdP から認証情報と属性情報を含んだ SAML アサーションを受け取ることでユーザの認証を実現する。SAML 認証の構成要素の関係を図 1 に示す。SP と IdP の間の信頼関係を両者を結ぶ線分で表現し、SP 側には赤色の円印を、IdP 側には青色の三角印を付している。

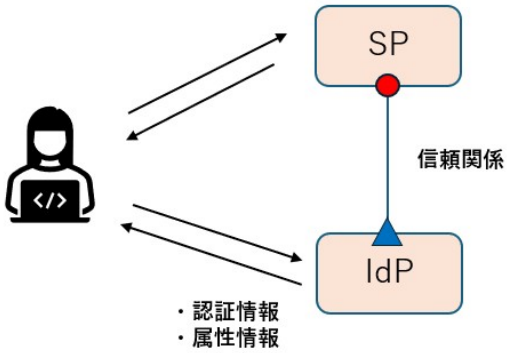

図 1　SAML 認証の構成要素

このとき、認証処理や属性準備処理を SP に設定した IdP 自身が実際に行う必要はなく、別の IdP に各処理を委任することもできる。つまり、SP と IdP の間に入り、SAML 認証を中継する SAML プロキシを用意して連携させることができる。図 2 に SAML プロキシの構成例を示す。

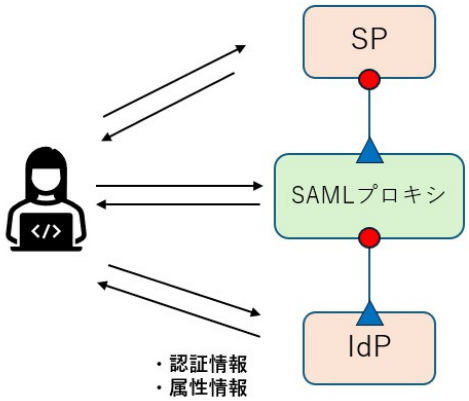

図 2　SAML プロキシの構成例

SAML プロキシサーバは SP と IdP の両方と信頼関係を確立する。SAML プロキシは SP と IdP のどちらとも SAML プロトコルで通信を行うが、SP に対しては IdP として振る舞い、IdP に対しては SP として振る舞うように構築する。

2.2 Shibboleth IdP の SAML プロキシ機能

Shibboleth IdP には SAML プロキシの機能が搭載されており、自身を IdP として動作させながら、同時に別の IdP に対して SP として動作させて認証を中継することが可能である[1]。

SAML プロキシの構築にあたっては、認証処理と属性準備処理の両方を別 IdP に委任してプロキシサーバは単純に中継だけを行う構成と、認証処理のみを別 IdP に委任して属性準備処理はプロキシサーバ自身で行う構成の 2 種類がある。後者の場合、プロキシサーバは委任した別 IdP での認証結果を受け取ってその認証情報をもとに属性を準備し、元の SP に認証情報と属性情報を合わせて返す構成となる。

2.3 Shibboleth IdP の SAML プロキシ設定

Shibboleth IdP で SAML プロキシ機能を利用するためには、SAML プロキシサーバで以下の設定を行う必要がある。なお、本稿では Shibboleth IdP の Web サイトの解説記事[1]に倣い、認証処理や属性準備処理を委任する IdP のことを SAML プロキシから見て上流 IdP と呼ぶこととする。

- **上流 IdP のメタデータ登録**

SAML プロキシサーバと上流 IdP の間で信頼関係を構築するために、上流 IdP のメタデータを登録する。metadata-providers.xml ファイルに上流 IdP のメタデータ情報を記述する。なお、上流 IdP 側にも SAML プロキシのメタデータ情報を登録しておく。

- **上流 IdP を利用して認証を実施する設定**

別の IdP に認証処理を委任するための設定を行う。authn.properties ファイルに上流 IdP のエンティティ ID を記載するとともに、idp.authn.flows の値を「SAML」と設定する。

- **上流 IdP とやり取りする属性の設定**

上流 IdP とやり取りする属性の設定を行う。上流 IdP から送出される属性と SAML プロキシサーバが受け取る属性は一致させておく。上流 IdP と SAML プロキシサーバともに attribute-filter.xml ファイルに属性情報を記述する。

- **上流 IdP の uid 属性を利用する設定**

上流 IdP での認証時にユーザが入力した ID は uid 属性として SAML アサーションに含まれる。SAML アサーションから uid 属性を proxied-uid 属性として取り出し、SAML プロキシサーバ内で

扱うための設定を行う。attribute-resolver.xml、subject-c14n.properties、subject-c14n.xml の 3 つのファイルで設定を行う。この設定により、SAML プロキシサーバでは、proxied-uid 属性をユーザ ID として内部で扱うことができる。

3 統合認証システムの構成

3.1 全体の構成

情報環境機構の統合認証システムでは 2023 年に、それまで運用していたパスワード認証と多要素認証の 2 種類の IdP サーバに加えて、SAML プロキシを行う新たなサーバを用意した。新サーバには Shibboleth IdP をインストールし、SAML プロキシ機能の設定を行っている。この新サーバは SAML プロキシサーバとして 3 つめの IdP として動作している。これら 3 種類の IdP と、各 IdP と認証連携する SP の信頼関係の構築状況を図 3 に示す。

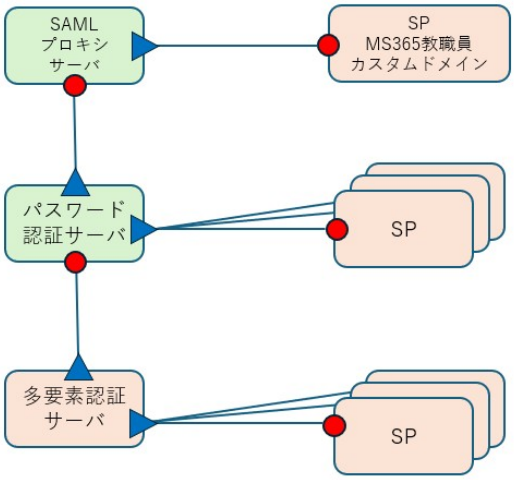

図 3　統合認証システムの全体構成

IdP と SP の間だけでなく、3 種類の IdP の間でも信頼関係を構築している点が特徴である。SAML プロキシサーバとパスワード認証サーバの間、パスワード認証サーバと多要素認証サーバの間の 2 箇所で信頼関係を構築し、SAML プロキシを構成して認証処理を委任できるように設定している。

3.2 SAML プロキシサーバとパスワード認証サーバ間の連携構成

図 4 に示すように SAML プロキシサーバとパスワード認証サーバの間で信頼関係を構築し、パスワード認証サーバが上流 IdP となるように構成している。

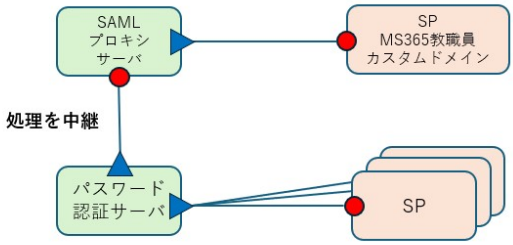

図 4　パスワード認証サーバに中継する構成

SAML プロキシサーバは認証処理と属性準備処理の両方をパスワード認証サーバに委任しており、完全に中継だけを行う構成となっている。

3.3 パスワード認証サーバと多要素認証サーバ間の連携構成

図 5 に示すようにパスワード認証サーバと多要素認証サーバの間で信頼関係を構築し、多要素認証サーバが上流 IdP となるように構成している。

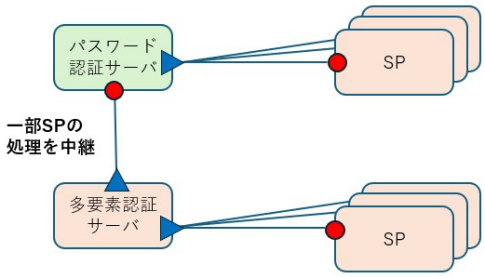

図 5　多要素認証サーバに中継する構成

パスワード認証サーバでは Shibboleth IdP の機能を利用して SAML プロキシのための設定を新たに追加した。パスワード認証サーバは基本的には IdP サーバとして振る舞い、連携している SP に対して認証・属性送出の処理を直接行っている。ただし、一部の SP に対しては、認証処理を多要素認証サーバに委任するように設定している。委任するのは認証処理のみで、SP に返す属性を準備する処理はパスワード認証サーバ自身が行う構成となっており、パスワード認証サーバと連携した LDAP を参照して属性情報を生成する。

なお、統合認証システムにおいては、パスワード認証サーバと多要素認証サーバで同じエンティティ ID を設定している。

4 SAML プロキシの運用状況

統合認証システムでは、SAML プロキシサーバがパスワード認証サーバを上流 IdP として、パスワード認証サーバが多要素認証サーバを上流 IdP としてそれぞれ SAML プロキシを構成している。

本章では、これら 2 つの構成において SAML プロキシ機能がどのように利用されているか、その運用状況について述べる。

4.1 SAML プロキシサーバの SAML プロキシ

SAML プロキシサーバは、Microsoft365 の教職員用カスタムドメインの認証連携設定を目的として構築され、その後も当初と同じ運用が続いている。SAML プロキシサーバを認証連携 IdP として動作している SP は Microsoft365 サービス（教職員用カスタムドメイン）の 1 件だけであり、その他の SP とは連携していない。

4.2 パスワード認証サーバの SAML プロキシ

4.2.1 Microsoft365 サービスの多要素認証化

情報環境機構はインターネットにおけるフィッシング詐欺増加への対策として、2024 年 6 月に Microsoft365 サービスの認証をパスワード認証から多要素認証に切り替えることとした。この対応のために、パスワード認証サーバの SAML プロキシ機能を初めて利用した。

多要素認証に切り替えるまでは、Microsoft365 サービスの学生用カスタムドメインはパスワード認証サーバと直接認証連携を行い、教職員用カスタムドメインは SAML プロキシサーバを経由してパスワード認証サーバで認証を行っていた。パスワード認証サーバに SP として登録されていた Microsoft365 学生用カスタムドメインと SAML プロキシサーバの 2 つのシステムに対して、認証処理のみを多要素認証サーバに中継するように構成を変更した。

この構成変更により、SP である Microsoft365 サービス側での認証連携設定を変更することなく、Microsoft365 サービスの教職員用カスタムドメインおよび学生用カスタムドメインでの多要素認証を実現できた。なお、教職員が Microsoft365 サービスにログインする場合、ユーザのブラウザは Microsoft365（SP）→SAML プロキシサーバ（IdP）→パスワード認証サーバ（IdP）→多要素認証サーバ（IdP）の順に 3 つの IdP の画面を開く動きをするが、画面は瞬時に遷移されるため、ユーザには多要素認証サーバの認証画面に切り替わったように見える。

4.2.2 検証用環境で簡易に多要素を試行したい SP

以前からパスワード認証サーバを利用していた SP で、検証用 SP と本番用 SP の 2 つのサーバをパスワード認証サーバに認証連携させているシステムが存在していた。このシステムの管理者から検証用 SP で多要素認証を試してみたいという要望があった。さらに、同じ管理者から SP 側の設定変更を省略して IdP 側の設定変更だけで対応してほしいという速やかな構成変更の要望があった。そこで、SAML プロキシ機能を利用して検証用 SP をパスワード認証サーバと認証連携させたまま、認証処理を多要素認証サーバで行うように構成した。

このシステムの管理者は本番用 SP についても今後多要素化する検討を行っているが、その際は、検証用 SP のように SAML プロキシを利用せずに、本番用 SP と多要素認証サーバを直接連携するように設定する方針で調整している。

4.2.3 パスワード認証サーバ内にのみ存在する属性を利用する SP

パスワード認証サーバ内にのみ存在する属性を必要とし、さらに多要素認証の利用を希望している 6 つのシステムと新規に認証連携を行うこととなった。この対応のために、パスワード認証サーバの SAML プロキシ機能を利用した。

6 つの SP システムが必要とする属性はパスワード認証サーバ内で生成しており、多要素認証サーバが利用する LDAP は属性情報を持っていない。パスワード認証サーバと多要素認証サーバで同一の属性値を送出できるようにするためには、全学アカウント管理システムを含めた LDAP の全体的な構成変更が必要となり、変更の対応には多大な時間を要する。そこで、属性準備処理はパスワード認証サーバが行い、認証処理は多要素認証サーバが行う構成を提案・実装し、SAML プロキシの機能を活用した。

5 SAML プロキシを構成する際の実装上の工夫

5.1 属性送出同意確認の抑制

SAML プロキシを利用する場合、SP にアクセスしたブラウザは SAML プロキシサーバ、上流 IdP サーバの順にページ遷移を行うことになる。このとき、遷移するすべてのページで属性送出の同意確認画面を表示させてしまうとユーザの利便性が損なわれるため、SAML プロキシを利用する場合は属性準備処理を行う IdP サーバでのみ同意確認を行い、その他のサーバでは同意確認を行わないように設定している。

5.2 Shibboleth IdP の IdP プロパティの利用

パスワード認証サーバは認証連携している一部の SP のみを多要素認証サーバに認証処理を委任し、その他の SP に対しては自身が IdP として認証処理を行う。多要素認証サーバに認証を委任する SP を効率よく指定するために、idp.properties ファイルで以下のように記述し、プロパティ設定を行っている。

```
idp.redirect.services.list = ‘http://sp-entityid1’,¥
  ‘https://sp-entityid2’, ‘https://sp-entityid3’
```

プロパティを設定しておくことで、Shibboleth IdP の他の設定ファイル中でも、認証処理を委任する SP を表すために${idp.redirect.services.list} のように記述することができる。

前節で説明した、属性送出の同意確認を行わない SP についても同様にプロパティ設定を利用している。注意点として、idp.properties ファイルのプロパティ設定を更新して SP を追加・削除した場合は、shibboleth.RelyingPartyResolverService サービスをリロードしても変更内容は反映されない。変更内容を反映するために、Jetty を再起動して対応している。

5.3 上流 IdP が自身と同じエンティティ ID のときの SAML プロキシ設定

パスワード認証サーバと多要素認証サーバはエンティティ ID が同じでありながら、多要素認証サーバが上流 IdP となるように SAML プロキシを構成している。この場合、両サーバでやり取りする属性の設定を適切に行わないと、認証連携している他の SP システムにも影響が発生する危険がある。

パスワード認証サーバの attribute-filter.xml ファイルに、上流 IdP である多要素認証サーバとやり取りする属性を記述する。通常の SAML プロキシの設定であれば、uid 属性を受け取るために

```
<AttributeFilterPolicy>
  <PolicyRequirementRule
      xsi:type="Issuer" value="idp-entid" />
  <AttributeRule attributeID="uid">
    <PermitValueRule xsi:type="ANY"/>
  </AttributeRule>
</AttributeFilterPolicy>
```

のように記述すればよい。なお、記載した設定中の idp-entid は上流 IdP の多要素認証サーバのエンティティ ID を指すものとする。しかし、パスワード認証サーバも上流 IdP と同じエンティティ ID であるため、この記述ではパスワード認証サーバが認証処理を行うすべての SP システムに対して uid 属性を送出してしまう。そこで、SAML プロキシ処理を行うときのみ上流 IdP の多要素認証サーバから uid 属性を受け取ることを明示して次のように記述する。

```
<AttributeFilterPolicy>
  <PolicyRequirementRule xsi:type="AND">
    <Rule xsi:type="Issuer" value="idp-entid" />
    <Rule xsi:type="Requester" value="idp-entid"/>
  </PolicyRequirementRule>
  <AttributeRule attributeID="uid">
    <PermitValueRule xsi:type="ANY"/>
  </AttributeRule>
</AttributeFilterPolicy>
```

6 おわりに

本稿では、情報環境機構の統合認証システムにおける SAML プロキシの活用について述べた。当初、SAML プロキシは SP の仕様による制約を解決するために導入した機能であったが、この機能を上手く活用することで SP の認証設定を変更することなくパスワード認証から多要素認証に切り替えるなどの対応が実現できた。

ただし、SAML プロキシを利用した設定構成はあくまでも複数の IdP システムを運用していることが前提となっている。将来、パスワード認証サーバの運用を停止して多要素認証サーバへの集約を進めることになった場合には、SAML プロキシを利用している SP 側の認証連携設定の更新が必要になるとともに、パスワード認証サーバのみが送出していた属性への対応も必要となる。

今後、統合認証システムの全体構成の変化に応じて、認証サーバの設定や構成も柔軟に変化させたいと考えている。

参考文献

[1] “Using SAML Proxying to another IdP” . shibboleth.atlassian.net . https://shibboleth.atlassian.net/wiki/spaces/KB/pages/1459979597/Using+SAML+Proxying+to+another+IdP, （参照 2025-09-10）.