UPKI 認証連携基盤に基づく安全なデータ共有システム構築の試み

Construction of data sharing systems based on the UPKI Federation

松平 拓也†，笠原 禎也†，高田 良宏†，井町 智彦†
Takuya MATSUHIRA†, Yoshiya KASAHARA†,Yoshihiro TAKATA†,Tomohiko IMACHI†

takusng@kenroku.kanazawa-u.ac.jp, kasahara@is.t.kanazawa-u.ac.jp,
yosihiro@kenroku.kanazawa-u.ac.jp,imachi@kenroku.kanazawa-u.ac.jp

†金沢大学総合メディア基盤センター

† Information Media Center of Kanazawa University

概要

金沢大学では，平成 20 年度より実施された「UPKI 認証連携基盤によるシングルサインオン実証実験」に積極的に参加してきた．これは国立情報学研究所及び全国共同利用情報基盤センターにより，大学が所有する教育研究用計算機，電子コンテンツなどのリソースを大学間において安全・安心に有効活用することを目的として 3 年計画で行われた全国大学共同電子認証基盤構築事業の一環を担うプロジェクトである．この取り組みにおいて，我々は UPKI 認証連携基盤の性質を利用した「ファイル送信サービス」,「デジタルコンテンツ公開サービス」という，安全にデータ共有を行うことが可能なシステムの構築に成功し，またそれらのシステムの実運用において今後必要となりうる項目について，考察を行うとともに検証を行った．

本稿では，本実証実験で構築したシステムについて説明し，技術的に考察する．

キーワード

UPKI，Shibboleth，シングルサインオン，認証，認可

Abstract

Kanazawa University has participated in the "Experiment of single sign-on based on the associated authentication infrastructure of UPKI", which is a part of "Cyber Science Infrastructure Project" conducted by the National Institute of Informatics and collaborative information technology centers. In the collaborative project, we have constructed two systems, "File Transfer Service" and "Opens Digital Contents Service", in order to handle data files and digital contents safely making use of the advantages of UPKI. We also took into account the several issues to be solved in the actual operations of these systems.

In the present paper, we introduce configuration of the systems and discuss the prospects of technical solutions.

Keywords

UPKI, Shibboleth, Single Sign On, Authentication, Authorization

1. はじめに

金沢大学では，従来は，各部署・部局が独立して構築・運用していた全学的な情報システムの融合化を進める必要性から，総合メディア基盤センター（以下センターと呼ぶ）が中心となり，今後の金沢大学における統合認証基盤のあり方について議論・検討を行っている．そして，教職員・学生向けの全学的な情報サービスを統一的に提供できる全学ポータルシステムや，それを支える統一認証機構の研究開発を進めている．

大学内において，多数の全学向け情報システムが独立して構築されているのは，金沢大学に限らず，他大学においても多くみられる．そして，いくつかの大学においては，先行的にその解決策としての仕組みを構築している．例として，名古屋大学では，CAS（Central Authentication Service）[1]を拡張したCAS^2(Central Authentication and Authorization Service)を開発し，統一認証を実現している[2][3]．また，大阪大学では，PKI(Public Key Infrastructure)を用いて全学 IT 認証基盤を構築している[4]．但し，これらの取り組みは，大学内に閉じた環境での情報システムの融合化であり，アカウントとパスワード管理を，学内でひとつの認証機構で一元化することが目的である．しかしながら，今後は複数の大学間での情報システムの共有，相互乗り入れの必要性が高まると予想されるが，まだ実用レベルでは実現に至っていない．

一方で，平成 18 年度から，国立情報学研究所（以下 NII と呼ぶ）及び全国共同利用情報基盤センターが中心となり，全国大学共同電子認証基盤構築事業[5]を 3 年計画で行ってきた．本事業では，大学が共有する教育研究用計算機，電子コンテンツ，ネットワークなどのリソースを大学間において安全・安心に有効活用することを目的としている．本事業における認証基盤は University Public Key Infrastructure（以下 UPKI と呼ぶ）と呼称される．

本事業の最終年度である平成 20 年度に，UPKI 認証連携基盤実現のために技術的及び制度的な検証を行うことを目的とした，「UPKI 認証連携基盤によるシングルサインオン実証実験（以下，実証実験と呼ぶ）」が実施された．金沢大学では，全学ポータルシステムや統合認証基盤を立ち上げるにあたり，単に大学内に閉じた環境ではなく，将来的な大学間連携にも活用できることを視野に入れた研究開発の一環として，本実証実験に積極的に参加した．その結果，センターでは UPKI の性質を利用した非常に有効なシステムを構築することができた．そして，今回構築したシステムを実運用していくにあたり，考察すべきことについてもいくつか検証を行った．

本稿では，まず UPKI の概要について述べ，実際に構築したシステムについて述べた後，考察を行う．

2. UPKI 概要

UPKI では各大学が保有する学術リソースや学内無線 LAN などの学術情報資源を安全・安心に利用できる環境を実現することを目的としている．そのために必要な技術として，シングルサインオン及び属性共有がある．シングルサインオンとは，ユーザが 1 度認証手続きを行えば，同様の認証を必要とする他のサービスにおいては認証手続きが不要になる技術をいう．また属性共有とは，ユーザに関する属性情報を複数のサービスで安全に共有する仕組みを示す．それを実現するために，実証実験では Shibboleth[6]と呼ばれるソフトウェアを用いている．本節では Shibboleth の説明を行った後，UPKI の概要について述べる．

2.1. Shibboleth

Shibboleth は Internet2/MACE[7]プロジェクトの 1 つで，SAML2.0[8]をベースとした認証連携を実現するオープンソースソフトウェアである．SAML とは，XML を基盤にした，異なる Web サービス間で認証情報，属性情報，認可情報を交換するための標準の仕様である．また，フェデレーションと呼ばれる，お互いに信頼されたサーバ間で組織を構成し，フェデレーション内でのみ各種情報の交換を可能とすることができる．

Shibboleth では，Identity Provider（以下 IdP と呼ぶ），Discovery Service（以下 DS と呼ぶ），Service Provider（以下 SP と呼ぶ）の 3 つによって構成される．以下にそれぞれの役割を述べる．

① IdP

IdP は主にユーザを認証する役割と，ユーザの属性情報を SP に送信する役割を持つ．ユーザが SP にアクセスすると，SP は IdP にリダイレクトを行う．IdP は ID/パスワード認証やクライアント証明書認証などの方法で認証を行う．そして，SP が要求する属性を SP に対して送信する．

② SP

SP は主に，ユーザの認証を IdP に要求する役割とユーザの属性を IdP から受信し，アプリケーションに渡す役割を持つ．ユーザが SP にアクセスすると，IdP にリダイレクトを行い，IdP から認証結果を受け取る．認証が成功したのち，IdP に対して必要とする属性を要求し，受け取ったものをアプリケーションに渡す．

③ DS

複数の IdP が存在する場合に，ユーザが適当な IdP を決定するための情報を提供する役割を持つ．ユーザが SP に対してアクセスした時，フェデレーション内における IdP の一覧を提示する．ユーザは提示された一覧から適当な IdP を選択し，認証を行う．

2.2. UPKI の動作

UPKI の動作概念図を図 1 に示す．UPKI 動作の手順は以下のとおりである。説明文中の括弧内の数字は，図に記載された矢印の番号と対応する．

A 大学所属のユーザ A が B 大学の SP を利用したい場合を例に示す．まず，ユーザ A は B 大学の SP にアクセスを試みる（①）．SP は DS にリダイレクトを行う（②）．DS はユーザ A に対して UPKI の IdP リストを提示する（③）．ユーザ A は DS から，自分の所属である A 大学の IdP を選択し，A 大学から与えられた ID とパスワードで認証を行う（④）．認証に成功すると，IdP はユーザ A の情報を SP に送信する（⑤）．SP はその情報を基に，ユーザ A のアクセスを許可する（⑥）．このように各大学のユーザは，自組織の ID，パスワードで認証を行うだけで，他大学のサービスを利用できるようになる．

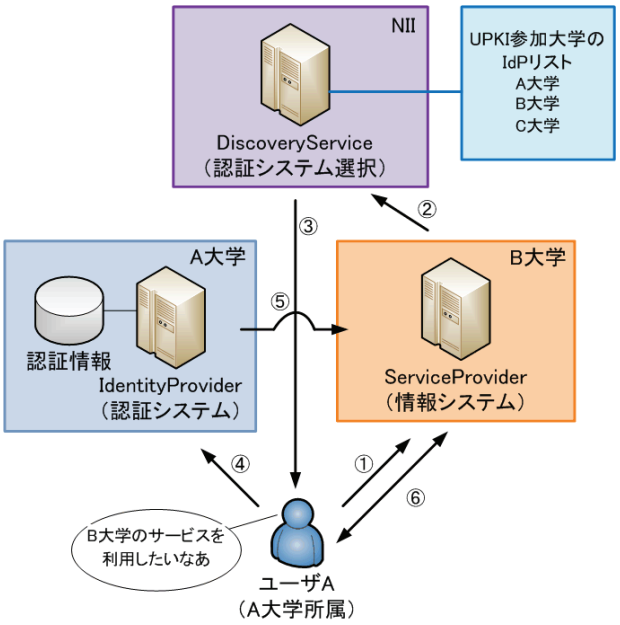

図 1 UPKI 動作概念図

今回の実証実験において，IdP 及び SP の構築は各参加大学が担当し，DS の構築は NII が担当した．そして，それらを用いて大学間で連携が取れるか実験を行った．

3. システム実装

3.1. 構築したシステムの概要

UPKI 認証連携基盤を利用する最大のメリットは，他大学からの利用者について身元が保証されることである．我々は今回の実証実験において，この性質を利用し，これまで当センターにおいて管理運用の実績がある 2 つの情報システムに対して，UPKI 認証を導入する方法について検討した．具体的には，「UPKI を用いたファイル送信サービス[9]」と「DSpace[10]によるデジタルコンテンツ公開サービス[11]」の 2 つの SP の構築を行った．

まず，「UPKI を用いたファイル送信サービス」は，メールでは添付できない大容量のファイルを相手に送信したい場合に，ファイルの転送を行う SP である．業務や研究など様々な場面において，メールでは添付できない大容量のファイルをやり取りしたいケースは非常に多く，このようなサービスのニーズは非常に高い．事実，センターでは 2005 年から金沢大学構成員を対象にファイル送信サービスを提供しており，毎月 600 件程度の利用がある．しかしながら，このようなサービスを行う上で問題となるのは利用者の管理である．金沢大学構成員だけに提供する場合は問題にはならないが，他大学の構成員に対してデータを送信する場合や逆に受信する場合，あるいは他大学の構成員同士で利用する場合は，悪意ある第三者に不正利用されるのを防ぐため，他大学の構成員の本人性を確認する必要がある．しかし，現状ではこの問題を解決する根本的な手立てが存在しなかった．そこで，UPKI を利用して認証に成功したユーザだけ利用できるように設計することで，本人性を確認したうえでサービスを提供することができるようになると考え，本 SP の構築を行った．

一方，「DSpace によるデジタルコンテンツ公開サービス」は大学で生産された様々な実験データ等を共有したり，公開したりするサービスである．DSpace は，オープンソースのリポジトリ構築ソフト

ウェアである．本 SP では，学術論文，紀要，研究報告書等の書誌系の情報ではなく，自然科学系実験データ等の画像や動画などの実験観測データをリポジトリ化し公開することを目的としている．実験観測データ等は貴重なデータであるため，原則として誰にでも公開する書誌系の情報とは異なり，特定の組織やグループ限定で見せたいケースが多い．そこで，本実証実験においては UPKI で認証が成功したユーザだけにデータを公開するように SP の構築を行った．

3.2. 各サーバのスペック

実証実験において，センターでは IdP を 1 つ，SP を 2 つ構築した．センターで構築した IdP 及び SP のスペックは以下のとおりである．

[IdP 用サーバ]
CPU：Intel Core2DuoE8400（3GHz）
メモリ：2GB
HDD：160GB
OS：CentOS5.2
[SP 用サーバ 1（UPKI を用いたファイル送信サービス）]
IdP 用サーバの VMWare 上で動作
メモリ：256MB 割当
OS：CentOS5.2
アプリケーション：apache2.2.3, php5.1.6, PostgreSQL8.1.11
[SP 用サーバ 2（DSpace によるデジタルコンテンツ公開サービス）]
Intel Core2DuoE8400（3GHz）
メモリ：2GB
HDD：160GB
OS：OpenSUSE10.2
アプリケーション：DSpace1.4.2

3.3.UPKI を用いたファイル送信サービス

まず，「UPKI を用いたファイル送信サービス」について説明する．本 SP は，ユーザ間で安全に大容量のデータを共有することを目的としたサービスである．

UPKI を利用したファイル送信サービスの動作概念図を図 2 に示す．説明文中の括弧内の数字は，図に記載された矢印の番号と対応する．

送信者は A 大学所属，受信者は B 大学所属とする．最初に送信者は，金沢大学の SP であるファイル送信サービスにアクセスする（①）．ファイル送信サービスは，送信者に認証を促すため，NII の Discovery Service にリダイレクトし，送信者に IdP を選択させる（②）．送信者は A 大学の IdP を選択し，認証を行う（③，④，⑤）．A 大学の IdP は送信者の情報をファイル送信サービスに送信する（⑥）．ファイル

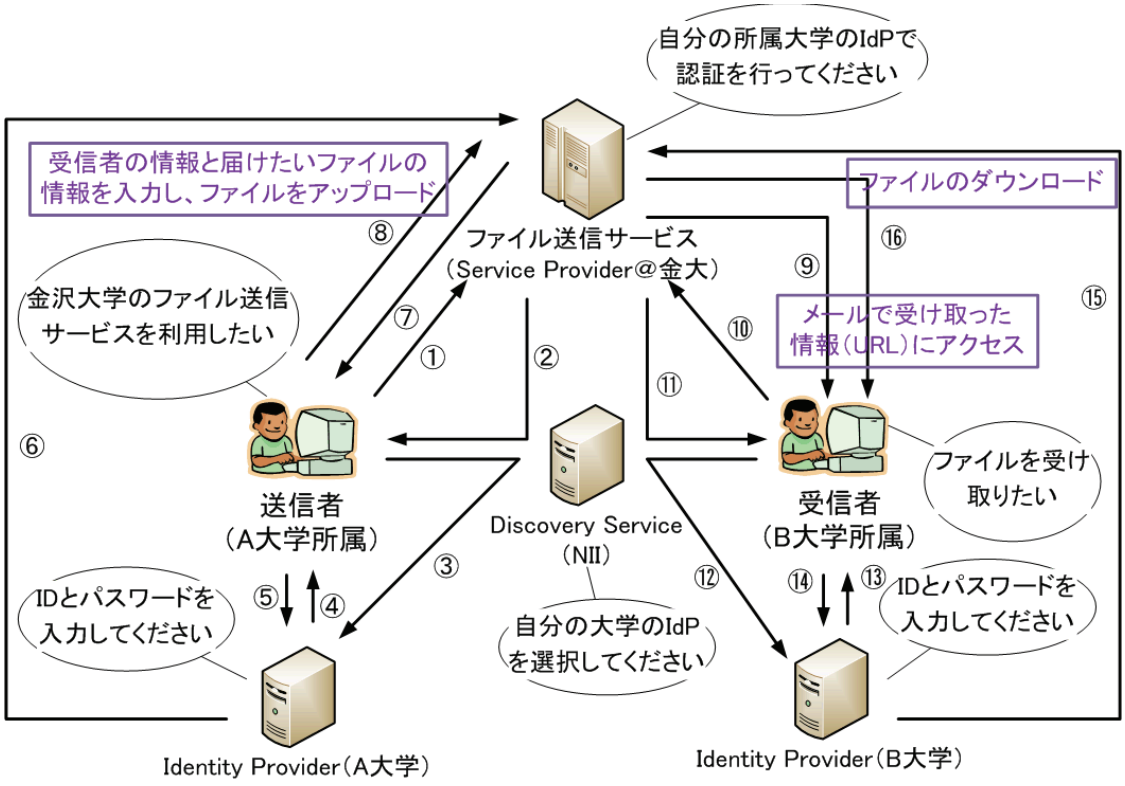

図 2　UPKI を用いたファイル送信サービス概念図

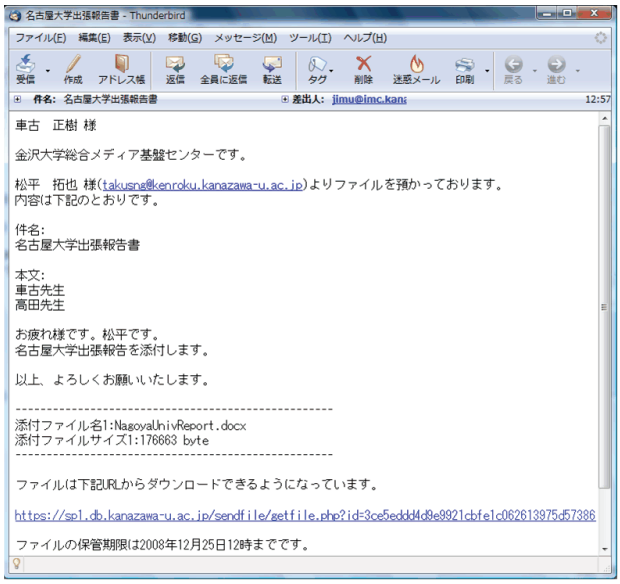

図 3 受信者通知メール

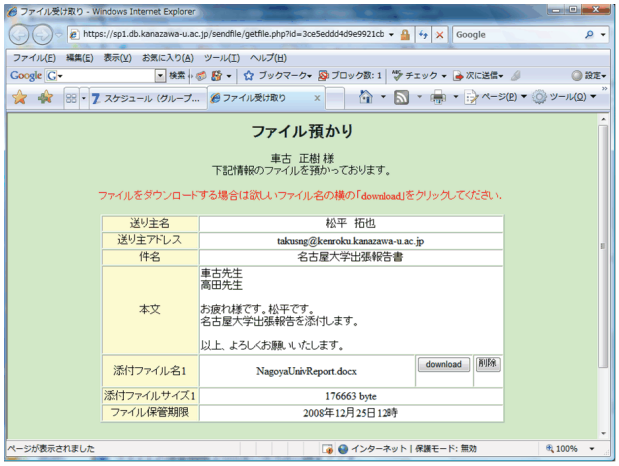

図 4 ファイル取得画面

送信サービスはユーザの確認を行い，ファイル送信サービスの画面を表示する（⑦）．送信者は自分の情報の入力及び，受信者の情報を入力する（⑧）．受信者は図 3 に示すメールを受け取り（⑨），メールに記載されている URL にアクセスする（⑩）．受信者も送信者と同様に DS にリダイレクトされ（⑪），受信者は B 大学の IdP を選択し，認証を行う（⑫，⑬，⑭）．B 大学の IdP は受信者の情報をファイル送信サービスに送信する（⑮）．認証後，受信者は図 4 の画面が表示され，ファイルをダウンロードすることができる（⑯）．

このように，UPKI 認証基盤を用いることにより，ユーザ間において安全に大容量のデータを共有するサービスを構築することができる．

3.3. Dspace によるデジタルコンテンツ公開サービス

次に「DSpace によるデジタルコンテンツ公開サービス」について説明する．本 SP は，大学で生産された実験観測データなどを特定の組織やグループに限定して公開を行うことを目的としたサービスである．今回の実証実験では，科学観測衛星「あけぼの」による地球周辺の電波観測データのスペクトル画像を PNG 化したものを，UPKI で認証が成功したユーザだけにデータを公開するように構築を行った．

図 5 に DSpace によるデジタルコンテンツ公開サービスの画面を示す．UPKI を用いたファイル送信サービス同様，本 SP にアクセスに来ると，自組織内の IdP での認証を求められる．そして認証に成功したのち，データの閲覧を行うことができる．サムネイルの一覧を表示でき，汎用的なフォーマットに変更したデータを表示する．

このように UPKI 認証連携基盤を利用することにより，実験観測データ等を，特定の組織やグループ限定で見せるサービスを構築することができる．

4. 考察

本章では，今回の実証実験で構築したシステム及び今後の取り組み方について考察する．

4.1.SP における認可設定

以下において，今回の実証実験で構築したシステムについて考察する．今回構築したシステムにおい

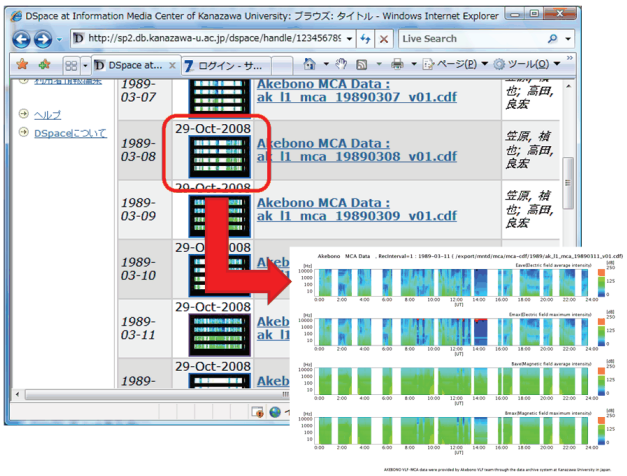

図 5 デジタルコンテンツ公開サービス

てはUPKI認証連携基盤での認証が成功したユーザすべてに対してサービスが利用できる設定にしている．UPKIという信頼されたフェデレーションで認証されたユーザということが特定できている限り，サービスを悪用される可能性は低い．しかし，今後はセキュリティを考慮し，構築したそれぞれのSPにおいて，特定のユーザや組織などに限定して利用を許可したいといったケースが存在することが十分考えられる．

まず，ファイル送信サービスにおいては，学生に閲覧されることが好ましくない大学運営や業務に関わる情報ファイルの交換の用途で利用するときは，大学構成員の中でも教職員だけにアクセスを制限したい．その解決策として，ShibbolethではApache[12]のアクセス制御ファイルである.htaccessで認可を行うという方法がある．図6にその設定例を示す．この例では，この.htaccessが配置されたディレクトリについては教員と職員だけがアクセス可能という意味を持つ．そのため，たとえ学生がUPKIフェデレーションに属している組織に在籍していたとしても，サービスへのアクセスを制限することができる．このように設定することで，職種区分に応じた特定のユーザだけにサービスを提供することができるようになる．

さらに，DSpaceによるデジタルコンテンツ公開サービスでは，職種区分だけではなく，組織情報や，所属情報などさらに詳細な公開範囲を指定する必要がある．その場合，Apacheによる認可設定では不十分と考えられる．そのため，このようなケースにおける解決策として，Shibbolethの XMLファイルを用いて認可を行う方法がある．図7に設定例を示す．この例では，secureディレクトリでは，A大学の工学部または理学部に所属する教職員に対してアクセスを許可するが，それに所属する学生のアクセスに関しては許可しないという設定になる．

このように，XMLを用いる方法では，AND，OR，NOTの論理式を用いて，より柔軟に認可設定を行うことができるため，DSpaceによるデジタルコンテンツ公開サービスでの複雑な認可を実現できると考えられる．

4.2.全学的UPKI対応への取り組み

つづいて，今後の取り組み方について考察する．UPKIによって大学間連携を実現するためには，各大学においてUPKIを利用できる環境構築が必須である．金沢大学内においても，全構成員がUPKIを利用できる環境を整備する必要がある．つまり，金沢大学の全構成員にUPKIで利用できるIDを提供する必要がある．

金沢大学においては，全学構成員を対象に交付されるIDとして，「ネットワークID」と呼ばれるものが既に存在する．本研究においては，これを用いた認証・認可を全学用LDAPサーバで構成することを検討した．ネットワークIDは任意で取得するIDあるが，金沢大学構成員がセンター提供のサービスを利用する際に使用するIDで，現在，センターが提供するサービスとして，学内ネットワーク利用認証やVPN認証などに用いている．そのため，ネットワークIDはほぼ全構成員が既に取得済みであり，UPKIを用いた大学間連携においても，このネットワークIDを用いるのが最も有効と考えられる．但し，現在運用されているネットワークIDをUPKIに使用する際には下記の2つの問題点を解決する必要がある．

1つ目は，既存のLDAPサーバを使用する場合，その属性情報にUPKIで必要とされるものが，必ずしもすべて存在するとは限らない点である．UPKIにおいて，SPに送信するIDは，eduPersonスキーマ[13]のeduPersonPrincipalName属性を用いる．しかし，eduPersonスキーマは標準的なものではないため，金沢大学のLDAPにも設定されていない．

2つ目はIDの外部への漏えいの問題である．UPKIで使用するIDは組織外のSPに送信されるため，アクセス先のSPが不正アクセスされた場合にネットワークIDの漏えいにつながる危険性がある．4.1節ではSP側である程度ユーザの情報を受け取った上で認可を行うことを検討したが，個人情報であるIDについては情報を保護する方法を検討する必要がある．

これらの問題の解決策として，IdPにおいてeduPersonへのマッピングを，IDそのものでなく対応付けられた異なる文字列にする方法がある（図8）．Shibbolethでは，設定ファイル内で各属性値の定義を行う．その際に，IDの文字列をeduPersonPrincipalNameにマッピングして送信することができる．そのことで，既存のLDAPに新たにスキーマを追加する必要がなくなる．そして，設定ファイル内でECMA Scriptを使用して，値の変換を行うことができる．図8ではネットワークIDであるuidをmd5に変換したものを16進数にし，@kanazawa-u.ac.jpを付加している．そうすることで，変換後の値からネットワークIDを割り出すのは難しく，この値が万一外部に漏えいしても問題ないと考えることができる．なお，IdP側でこれらの設定を行っても，SP側では

eduPersonPrincipalName の値が送られてくるだけであるため，特に変更は不要である．

```
AuthType shibboleth
ShibRequireSession On
requireAffiliation faculty staff
```

図 6 .htaccess による認可設定例

```
<Host name="sp2.db.kanazawa-u.ac.jp" authType="shibboleth" requireSession="true">
    <Path name="secure">
      <AccessControl>
        <AND>
          <Rule require="o">Auniversity</Rule>
          <OR>
            <Rule require="ou">Engineering</Rule>
            <Rule require="ou">Science</Rule>
          </OR>
          <NOT>
            <Rule require="Affiliation">student</Rule>
          </NOT>
        </AND>
      </AccessControl>
    </Path>
</Host>
```

図 7 XML による認可設定例

```
<resolver:AttributeDefinition id="principalName" xsi:type="Script"
   xmlns="urn:mace:shibboleth:2.0:resolver:ad"sourceAttributeID="uid">

    <Script>
      <![CDATA[
        importPackage(・・・・);
        uniqueValue = uid.getValues().get(0) + "xxxxx";
        localpart = DigestUtils.md5Hex(uniqueValue);
        principalName = new BasicAttribute("principalName");
        principalName.getValues().add(localpart + "@kanazawa-u.ac.jp");
      ]]>
    </Script>
</resolver:AttributeDefinition>
```

図 8 IdP 設定ファイル（一部）

5.まとめ

金沢大学では実証実験において独自の IdP 及び SP の構築を行った．UPKI フェデレーションを使用することにより，他大学からの利用者について身元が保証され，大学間においてサービスを安全に提供することができるようなった．そして，その性質を利用して，これまでは学内のみで提供していた「ファイル送信サービス」，「デジタルコンテンツ公開サービス」を，大学間においても安全にサービスを提供できるシステムを構築することができた．さらに，今回構築した SP における認可の方法及び UPKI で利用する ID の秘匿性について考察を行い，個人情報を保護しながらも，適切に認可を行う方法を示すことができ，セキュリティ面においても検証することができた．

今後は考察で述べた UPKI で利用する ID の検討や SP の認可の方法をさらに発展させ，現在金沢大学で進めている全学ポータルシステム及び統合認証基盤の構築において，本実証実験で培った経験を生かし，UPKI と連携可能なシステムとして，大学間連携への活用を視野に入れて構築を進めていきたいと考えている．

参考文献

[1] Central Authentication Service：http://www.ja-sig/cas/

[2] 内藤久資，梶田将司，小尻智子，平野靖，間瀬健二：“大学における統一認証基盤としての CAS とその拡張”, 情報処理学会論文誌, Vol. 47, No. 4, pp.1127-1135 (2006)

[3] 梶田将司，内藤久資，小尻智子，平野靖，間瀬健二：“CAS によるセキュアな全学認証基盤の構築”，情報処理学会研究報告，Vol.2005，No.39，pp.35-40 (2005)

[4] 秋山豊和，寺西裕一，岡村真吾，坂根栄作，長谷川剛 ほか 4 名：“大阪大学における全学 IT 認証基盤の構築”，情報処理学会論文誌，Vol．49，No．3，pp.1249-1264 (2008)

[5] UPKI イニシアティブ：https://upki-portal.nii.ac.jp/

[6] Shibboleth：http://shibboleth.internet2.edu/

[7] Middleware Architecture Committee for Education ：http://middleware.internet2.edu/MACE/

[8] SAML2.0：http://www.oasis-open.org/specs/index.php

[9] 松平 拓也，車古 正樹，井町 智彦：“Spam メール及びウイルスメール対策システムの構築と運用”, 学術情報処理研究，No9，pp.45-54，(2005)

[10] DSpace：http://www.dspace.org/

[11] 高田 良宏, 笠原 禎也, 西澤 滋人, 森 雅秀, 内島 秀樹：“デジタルコンテンツに適した学術情報リポジトリの構築”，第 7 回情報科学技術フォーラム（FIT2008）講演論文集,pp.391-392, (2008)

[12] Apache Http Server Project：http://httpd.apache.org/

[13] EDUCAUSE：http://www.educause.edu/eduperson/