第9回東海地区CSI事業報告会@名古屋大学
2008/12/24（Wed）

UPKIに基づく金沢大学での Shibbolethを用いた IdP及びSP構築について

金沢大学総合メディア基盤センター
松平拓也、井町智彦、笠原禎也、高田良宏

目次

- 自己紹介
- UPKI実証実験概要
- 金沢大学におけるIdP・SP実装
- 金沢大学のSP構築例
  - 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
- 金沢大学の認証基盤の現状と今後
- まとめ、今後の展望

自己紹介

- 金沢大学総合メディア基盤センター
  技術職員
- 担当業務
  - spamメール対策
    - 金沢大学独自の対策システムを構築・運用
    - SymantecMailSecurity、SpamAssassin、InterscanMessageSecuritySuite（TrendMicro）を多段化して95%以上のspamメール隔離率を達成
  - 今年度より、金沢大学統合認証システムの開発に着手
    - その一環としてUPKI実証実験に参加

UPKI実証実験概要

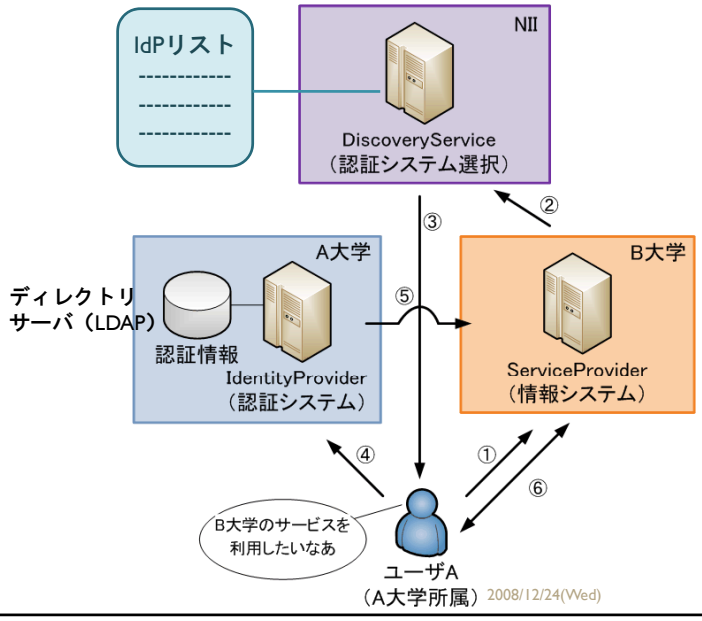
- 「UPKI認証連携基盤による
  シングルサインオン実証実験」

目的：シングルサインオンの技術で電子ジャーナルなど
のコンテンツ利用や大学間認証連携の検証を行う

金沢大学
- UPKIへの貢献
- シングルサインオンなどの技術要素の取得

- IdP連携実験
  - IdP（Identity Provider）の構築（認証サーバ）
  - IDの発行（LDAP構築）（ディレクトリサーバ）
  - SP（Service Provider）の構築（サービス提供サーバ）
- IdP、SP実装にはShibbolethを使用
  - SAML（XML仕様）を標準実装したオープンソースソフトウェア

UPKI概念図



IdPサーバ構成

- IdP用サーバ（１台）

CPU　：Core2DuoE8400（3GHz）
メモリ：2GB
HDD　：160GB
OS　：CentOS5.2
アプリケーション：Apache2.2.3、Tomcat6.0.18、Shibboleth-idp-2.0.0

１台数万円程度のサーバでスタート
（全学展開など大規模運用を行うにはやや能力不足）

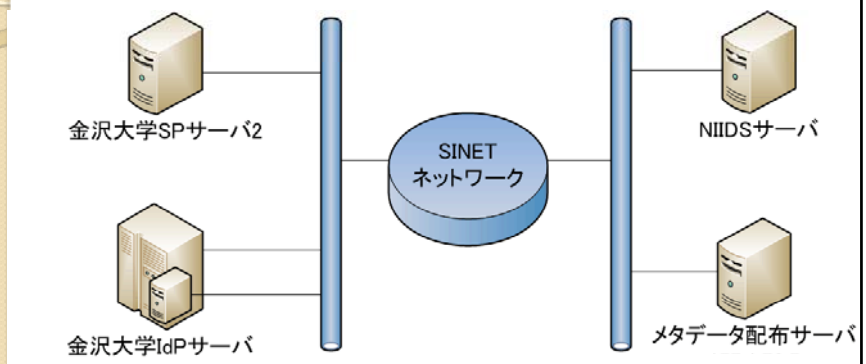
SPサーバ構成

- SP用サーバ（2台）
  1．IdPのVMware上で動作（IdPサーバの負荷要因の一つ）
  メモリ：256MB
  OS：CentOS5.2
  アプリケーション：Apache2.2.3、Tomcat6.0.18、
  shibboleth-2.1.1 、php5.1.6
  「UPKIを用いたファイル送信サービス」

  2．CPU：Core2DuoE8400（3GHz）
  メモリ：2GB
  OS：OpenSUSE11.0
  HDD：160GB
  アプリケーション：Dspace1.4.2
  「DSpaceによるデジタルコンテンツ公開サービス」

※Shibbolethについて
CentOSはrpm、OpenSUSEはsrc.rpmでリコンパイル後にインストール

金沢大学UPKI実験構成図



金沢大学SPサーバ1(VMware上)

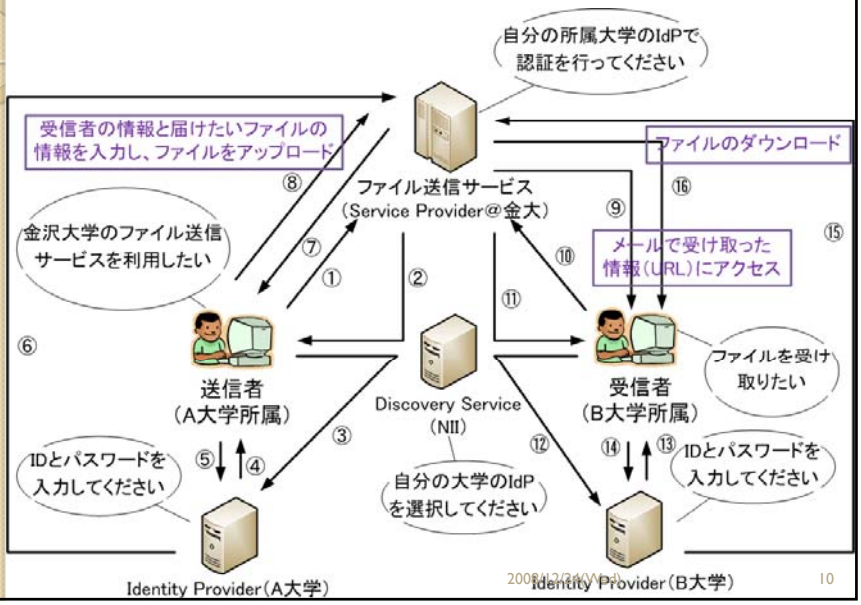
メタデータの
自動更新

金沢大学におけるSP実装例

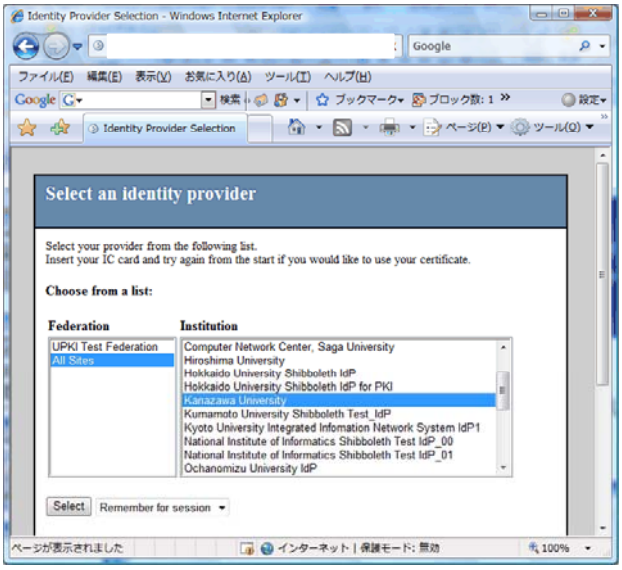
- UPKIを用いたファイル送信サービス
  - メールでは添付できない大容量のファイルを送信したい場合に利用
  - ファイルを一時的にサーバにアップロードし、その情報を送り先に通知し、送り先はサーバにアクセスして受信
- DSpaceによるデジタルコンテンツ公開サービス
  - 図書館では取り扱わないような各種デジタルコレクションや実験観測データのリポジトリ化
  - Akebono衛星による地球周辺の電波観測データのスペクトル画像（PNG）

各所属機関のIdPで認証を受けることにより
サービスを利用可能

UPKIによるファイル送信サービス



ファイル送信サービス（１）

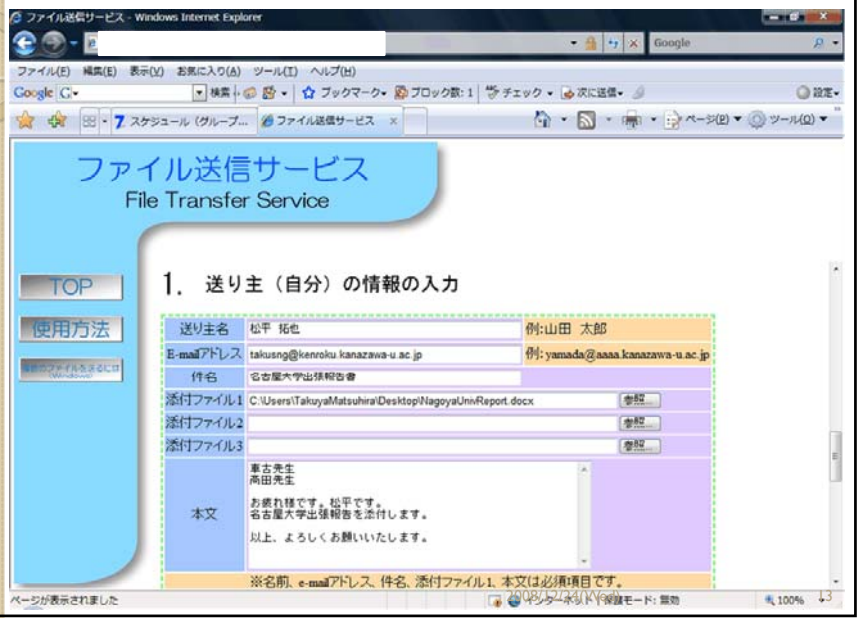


DiscoveryServiceで自分の所属する大学を選択

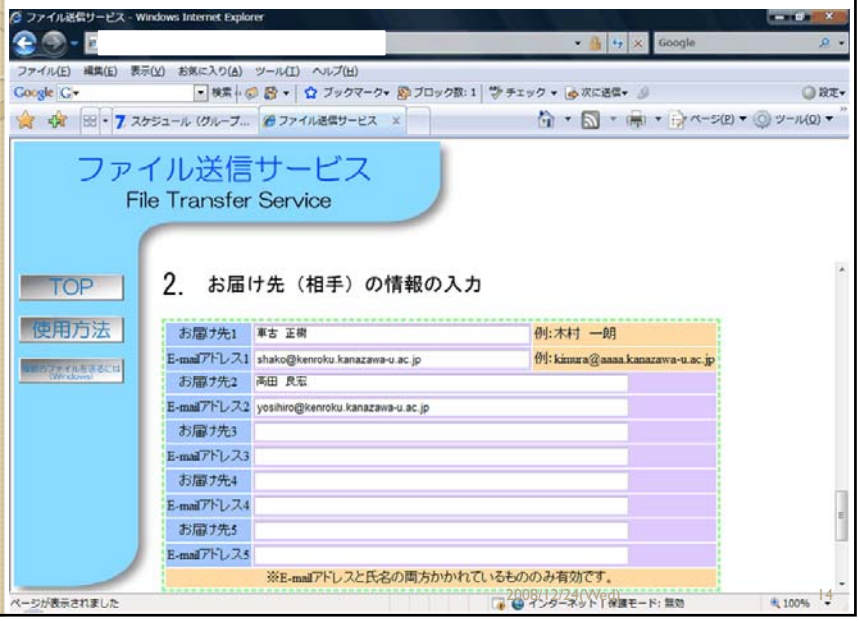
ファイル送信サービス（２）

自分の所属する大学のIdentityProviderで認証

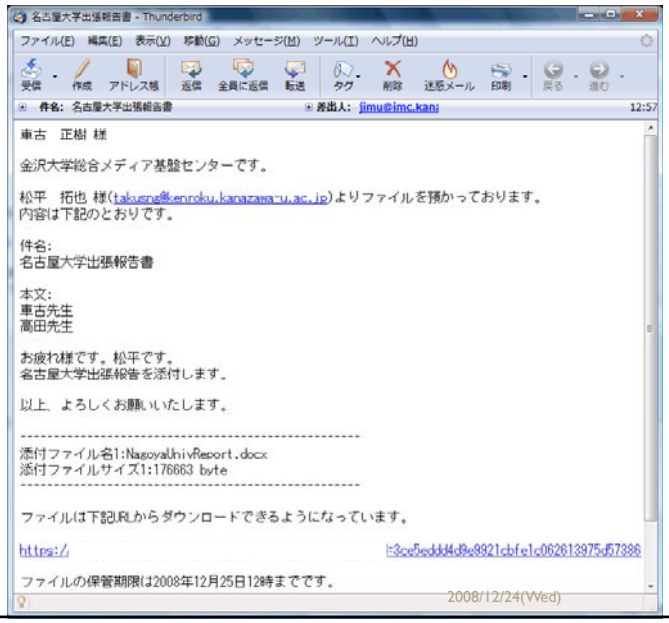
ファイル送信サービス（３）



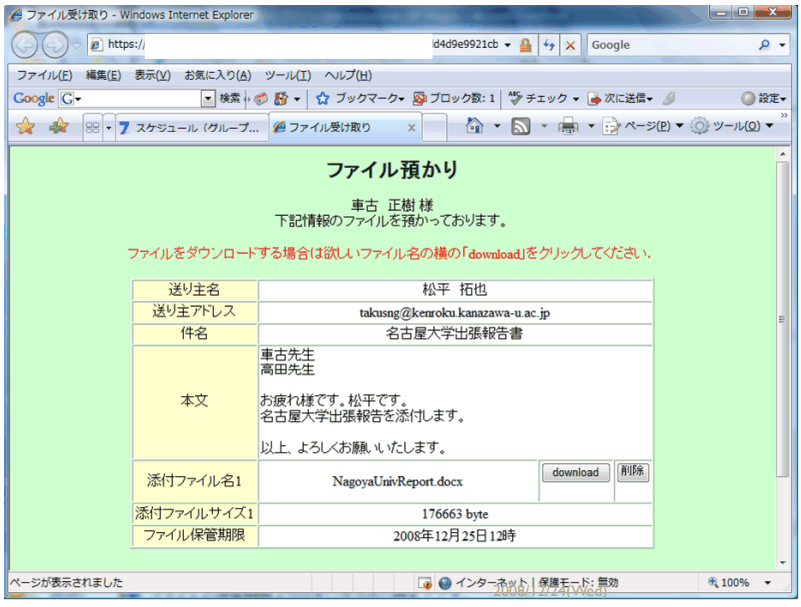
ファイル送信サービス（４）



ファイル送信サービス（５）



ファイル送信サービス（６）



DSpaceとは

- 2000年からMITとHPで共同研究・開発してきたオープンソースのリポジトリ構築ソフトウェア

リポジトリ：データやプログラムなどを体系化した情報を保管している場所（データ貯蔵庫）

機関リポジトリ：大学などの研究機関において、生産された研究成果を電子的な形態で蓄積・保存し、インターネット上で公開するシステム

- 図書館等が中心となって構築
- 主に，学術論文，紀要，研究報告書などの書誌系の情報をデジタル化して格納
  ⇒ 書誌コンテンツ

デジタルコンテンツ公開サービス

- 書誌コンテンツ以外の画像，動画などのコレクション
  ⇒デジタルコンテンツ

  機関リポジトリの対象外とされている場合が多い

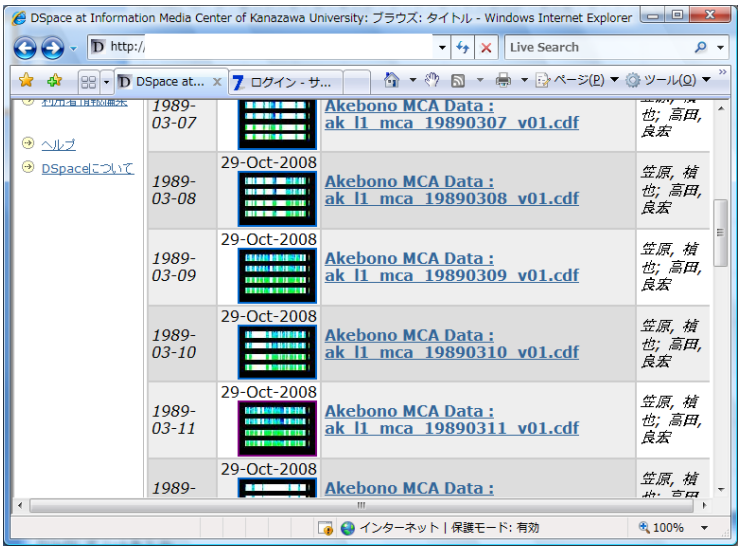
  流通性，コスト，先行する書誌コンテンツでの実績のある機関リポジトリで対応

- DSpaceによるデジタルコンテンツ公開サービス
  - 図書館では取り扱わないような各種デジタルコレクションや実験観測データのリポジトリ化
  - Akebono衛星による地球周辺の電波観測データのスペクトル画像（PNG）

デジタルコンテンツ公開サービス（1）

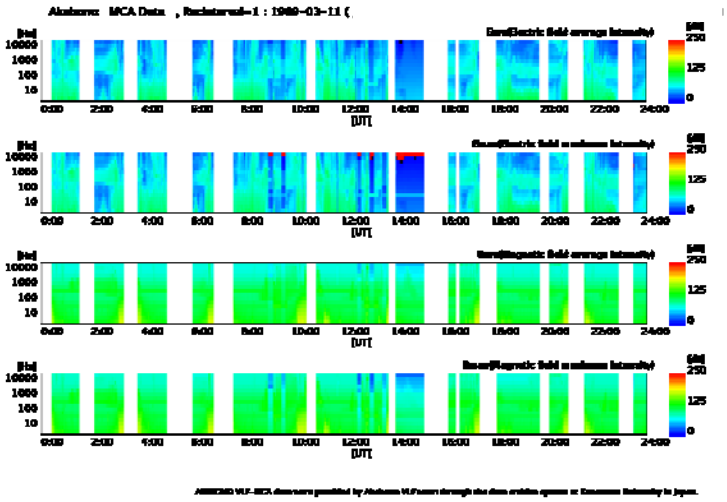
見た目は機関リポジトリと同じ

デジタルコンテンツ公開サービス（2）



サムネイルの一覧を表示可能

デジタルコンテンツ公開サービス（３）



観測データを汎用的なフォーマットに変更したもの
（特定のユーザには魅力的）

Shibboleth制限方法

- Apacheによる制限
  （shibboleth2.xmlで<RequestMapper type="Native">）
  - httpd.conf or .htaccess or shib.conf（rpmでインストールした場合のみ）

```
<Location /sendfile>
    AuthType shibboleth
    ShibRequireSession On
    require valid-user
</Location>
```

- SPにアクセスするとIdPの認証画面にリダイレクトされるため、SP側で認証の実装や属性情報を持つ必要なし
- 認可のための属性情報は環境変数でIdPからSPへの送信が可能 ⇒ アプリケーションでアクセス制限が容易に可能

SPの現状

- アクセスログを参照すると、現段階では利用者があまりいない
  - UPKI自体の利用者が少ない？

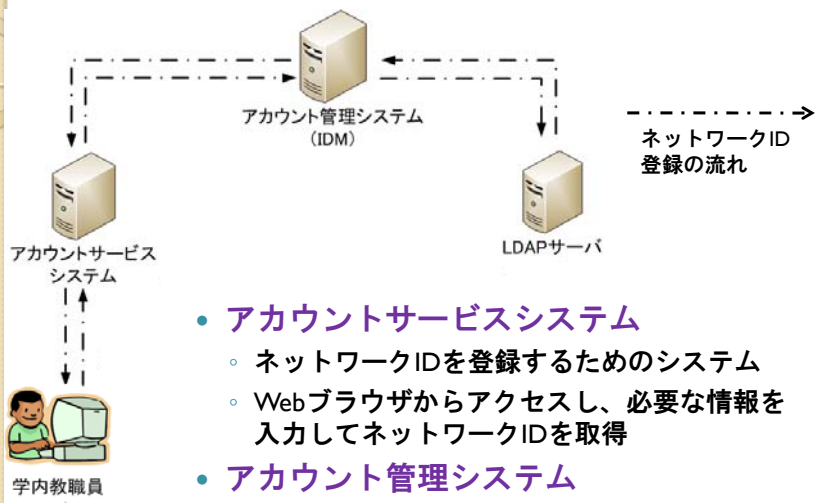
    or
  - 金沢大学のSPに魅力がない？
- 各大学のIdP構築の推進及び利用者の拡大
- NIIや各大学からの魅力的なSPの提供

金沢大学全体へのUPKI普及

- 全学用LDAPサーバを認証・認可に利用
  - ネットワークID（uid）
    - 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識別子
    - ユーザが登録・変更可能

      職員番号等のユーザ固有のIDを使用すると、万一情報が漏れた場合変更ができないため
  - ネットワークID利用例
    - 学内ネットワーク利用認証
    - 学内無線LAN認証（Radius）
    - VPN認証

ネットワークID登録



- アカウントサービスシステム
  - ネットワークIDを登録するためのシステム
  - Webブラウザからアクセスし、必要な情報を入力してネットワークIDを取得
- アカウント管理システム
  - アカウントサービスシステムで入力した情報をLDAPサーバに反映
    （認証情報の統合管理を目的）

ネットワークIDとUPKIの連動

- UPKIの大学間連携では別途スキーマが必要
- eduperson
  - eduPersonPrincipalName（Principal Name）
    - 大学間連携の際に学外で使用するID
    - ネットワークID（uid）を学外に送信するのはセキュリティ上好ましくない
    - ネットワークIDをベースとしたユニークなIDを生成する必要がある
  - eduPersonAffiliation（Affiliation）
    - 大学間連携の際に学外で使用する職種区分を識別
    - employeeTypeを利用予定

ネットワークID利用例

Attribute-resolver.xmlに下記のように記述（ECMAScript）

```
<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>
```


UPKIの感想

- 他大学の構成員の身元が判別できる
  - なりすましを回避でき、大学間においてセキュアにサービスを提供できる
- 各大学の足並みをもっと揃える必要
  - IdP、SPがまだあまり普及していないように感じる
    ⇒UPKI化により得られるメリットが欲しい
- IdP、SP構築をもう少し簡単に
  - 構築は設定者のある程度のスキルが必要
  - 設定手順書をもう少し充実する必要がある
- 金沢大学の統合認証に本技術の利用検討
  - 金沢大学の既存のシステムに手をできるだけ加えない

今後の展望

- 金沢大学で全学規模でのシングルサインオン環境及び認可機構の導入を検討
  ⇒管理の分散化
- シングルサインオンに使用するソフトウェアの選定
  ⇒shibbolethを使用するか
- UPKIに対応できる（SAML2.0）システムの設計を行い、テストする