



# 金沢大学における IdP , SP構築の現状と今後の展望

金沢大学

松平拓也 , 笠原禎也 , 高田良宏 , 井町智彦

金沢大学 UPKI SSO 実証実験 WG

# 推進体制

## プロジェクト代表者・担当者

- 代表者：井町 智彦  
総合メディア基盤センター助教
- 担当者：松平拓也  
情報部情報企画課基盤整備第2係（総合メディア基盤センター）技術職員

## 金沢大学 UPKI SSO 実証実験 WG

- 金沢大学総合メディア基盤センター
  - 笠原 禎也（准教授）
  - 高田 良宏（助教）
  - 井町 智彦（助教）
- 金沢大学情報部
  - 村田 勝俊（情報企画課副課長）
  - 橋 洋平（情報企画課情報企画係係長）
  - 堀井 孝一（情報企画課基盤整備第3係主任）
  - 松平 拓也（情報企画課基盤整備第2係技術職員）

# 報告概要

- 実証実験概要
- 実験環境
- 実証実験において構築したSP
  - 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
- 全学的UPKI対応への取り組み
- SPにおける認可実験
- まとめ、今後の展望

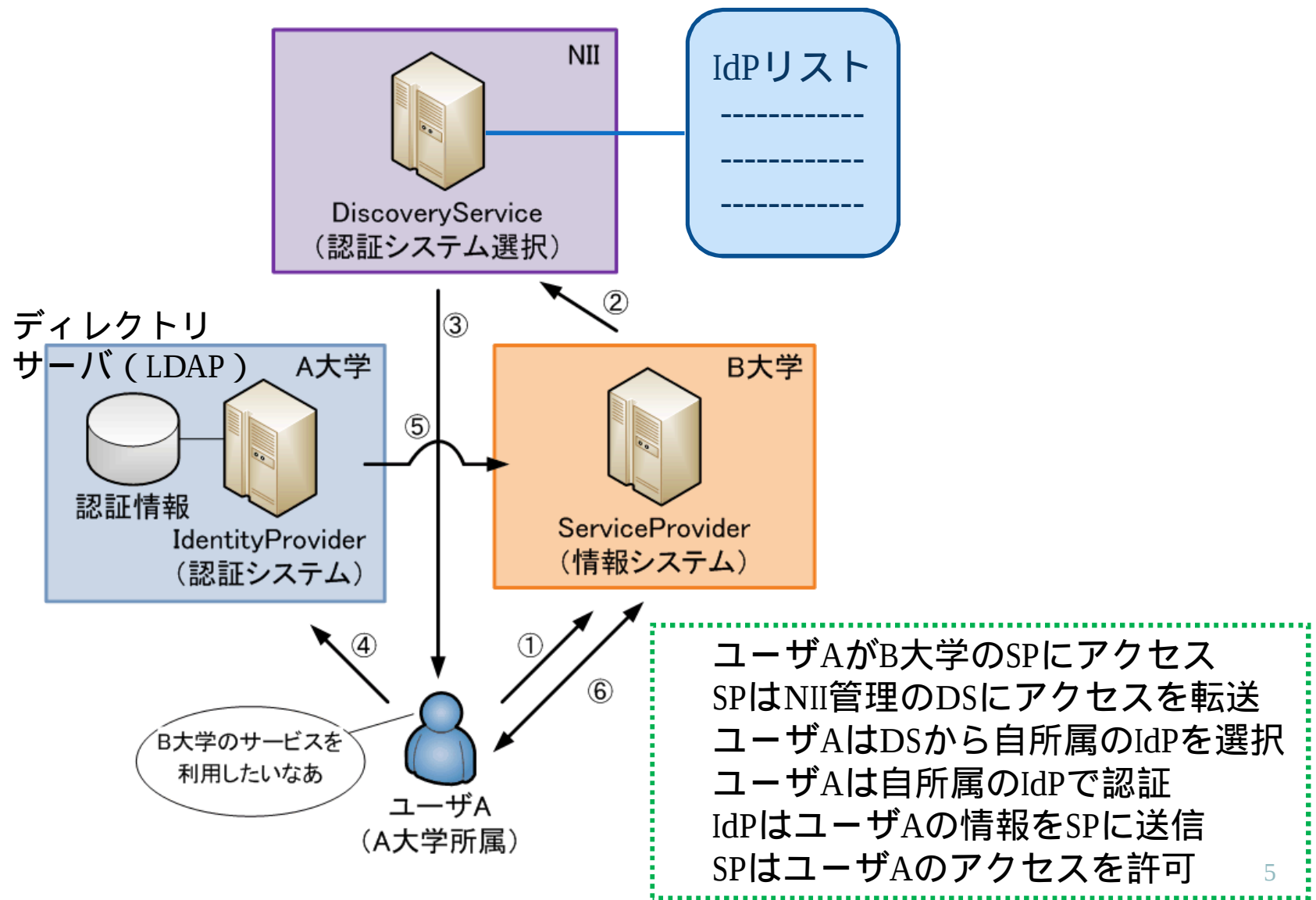
# 実証実験概要

- 「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

- 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 SSO 概念図



# 実験環境

## ■ IdP用サーバ（1台）

CPU : Core2DuoE8400 ( 3GHz )

メモリ : 2GB

HDD : 160GB

OS : CentOS5.2

## ■ SP用サーバ（2台）

1.IdPのVMware上で動作

メモリ : 256MB

OS : CentOS5.2

アプリケーション : php5.1.6

「UPKIを用いたファイル送信サービス」

2.CPU : Core2DuoE8400 ( 3GHz )

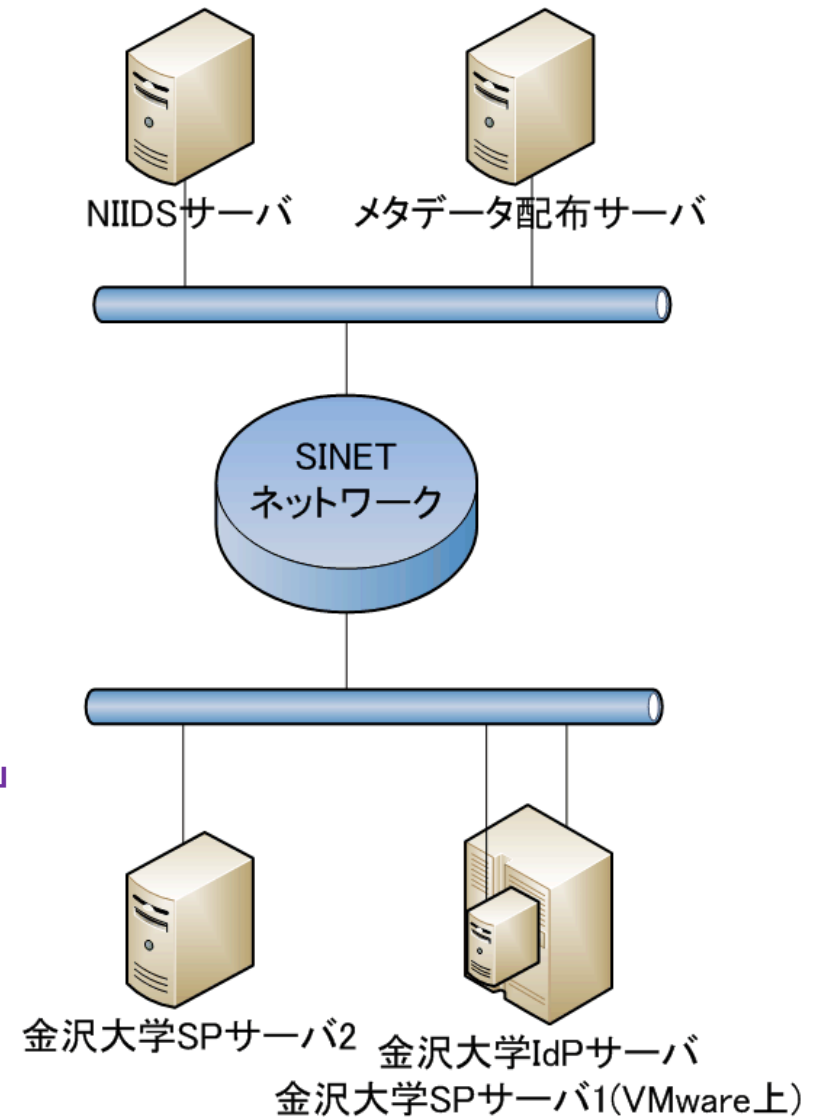
メモリ : 2GB

OS : OpenSUSE11.0

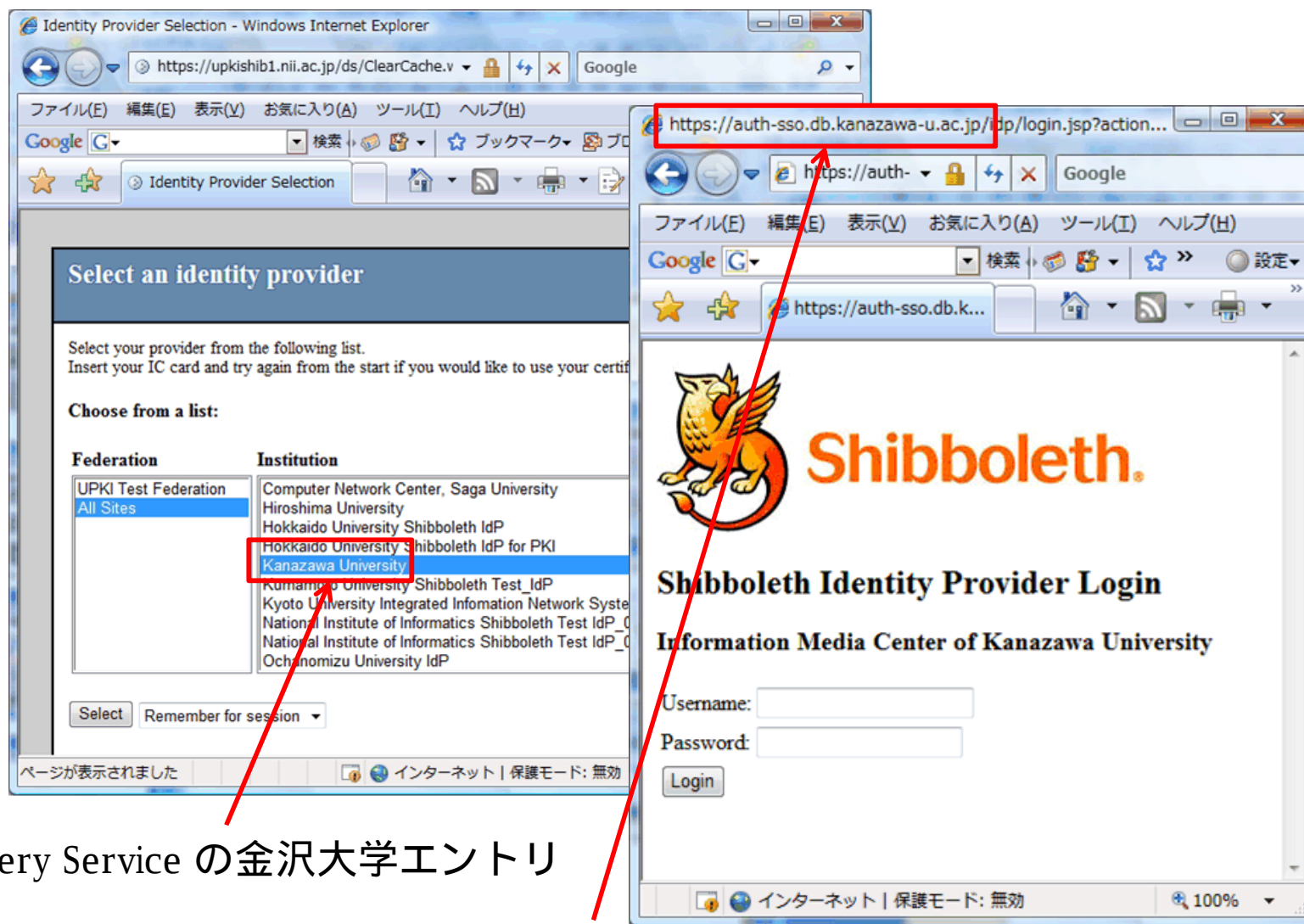
HDD : 160GB

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認証の動作確認



Discovery Service の金沢大学エントリ

金沢大学の IdP 認証画面

# 実証実験において構築したSP

- .UPKIを用いたファイル送信サービス  
( <https://sp1.db.kanazawa-u.ac.jp/sendfile/> )
  - 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  
( <https://sp2.db.kanazawa-u.ac.jp/dspace/> )
  - 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

# . ファイル送信サービス ( 1 )

ファイル送信サービス - Windows Internet Explorer

https://sp1.db.kanazawa-u.ac.jp/sendfile/

ファイル(E) 編集(E) 表示(V) お気に入り(A) ツール(I) ヘルプ(H)

Google C 検索 ブックマーク ブロック数: 1 チェック 次へ送信 設定

7 スケジュール (グループ... ファイル送信サービス x

## ファイル送信サービス

File Transfer Service

TOP

使用方法

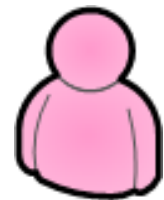
複数のファイルを送るには (Windows)

### 1. 送り主 (自分) の情報の入力

|            |                                                                          |                                 |
|------------|--------------------------------------------------------------------------|---------------------------------|
| 送り主名       | 松平 拓也                                                                    | 例: 山田 太郎                        |
| E-mailアドレス | takusng@kenroku.kanazawa-u.ac.jp                                         | 例: yamada@aaaa.kanazawa-u.ac.jp |
| 件名         | 名古屋大学出張報告書                                                               |                                 |
| 添付ファイル1    | C:\Users\TakuyaMatsuhira\Desktop\NagoyaUnivReport.docx                   | 参照...                           |
| 添付ファイル2    |                                                                          | 参照...                           |
| 添付ファイル3    |                                                                          | 参照...                           |
| 本文         | 車古先生<br>高田先生<br><br>お疲れ様です。松平です。<br>名古屋大学出張報告を添付します。<br>以上、よろしくお願いいたします。 |                                 |

※名前、e-mailアドレス 添付ファイル1、本文は必須項目です。

インターネット | 保護モード: 無効 100%

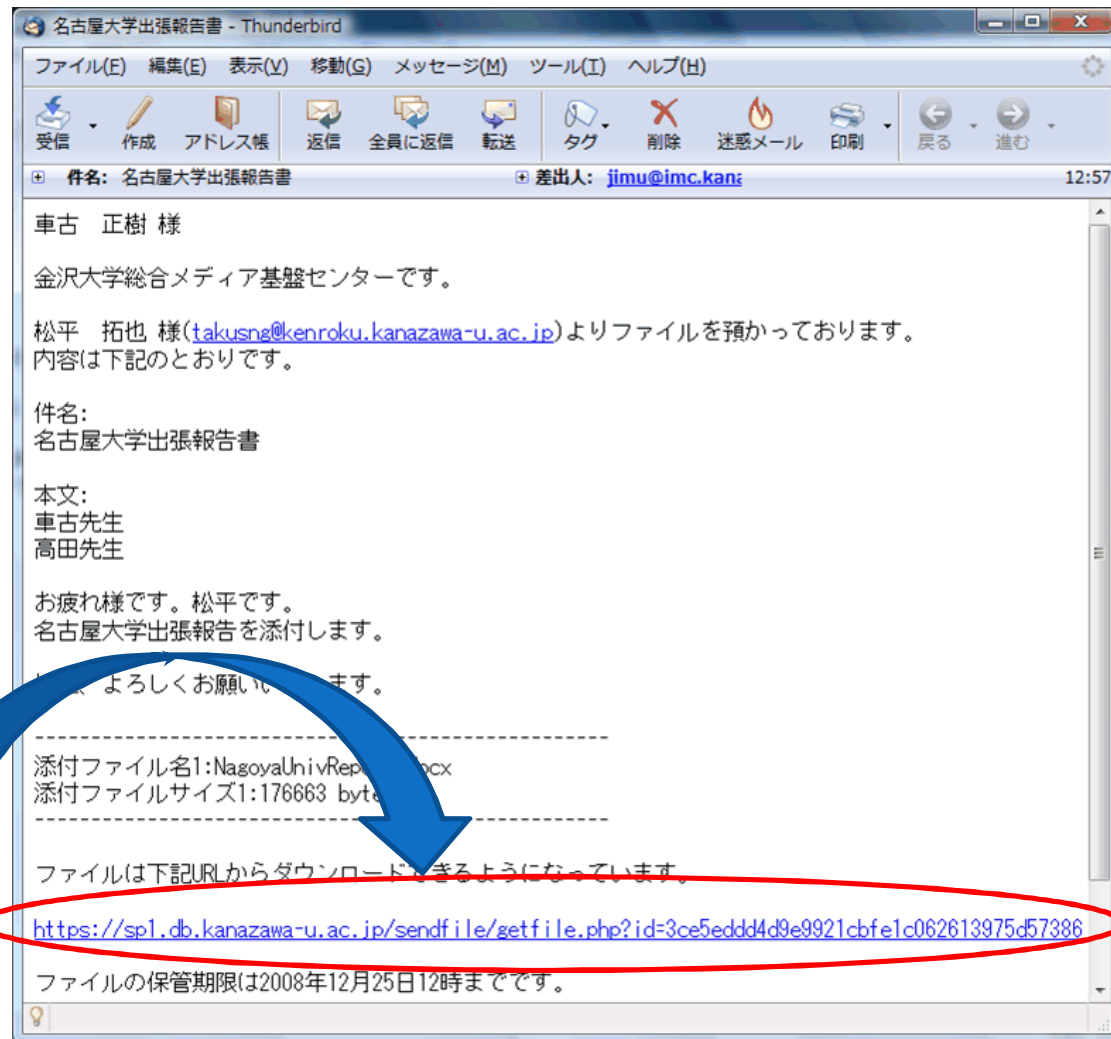


送信者

Shibboleth認証を行うことでサービスを利用可能

受信者にメール送信

## . ファイル送信サービス ( 2 )



受信者はメールに記載されたURLにアクセス

# ファイル送信サービス ( 3 )

ファイル受け取り - Windows Internet Explorer

https://sp1.db.kanazawa-u.ac.jp/sendfile/getfile.php?id=3ce5eddd4d9e9921cb

ファイル(E) 編集(E) 表示(V) お気に入り(A) ツール(I) ヘルプ(H)

Google G 検索 ブックマーク ブロック数: 1 ABC チェック 次送信 設定

7 スケジュール (グループ...) ファイル受け取り

### ファイル預かり

車古 正樹 様  
下記情報のファイルを預かっております。

ファイルをダウンロードする場合は欲しいファイル名の横の「download」をクリックしてください

|            |                                                                      |
|------------|----------------------------------------------------------------------|
| 送り主名       | 松平 拓也                                                                |
| 送り主アドレス    | takusng@kenroku.kanazawa-u.ac.jp                                     |
| 件名         | 名古屋大学出張報告書                                                           |
| 本文         | 車古先生<br>高田先生<br>お疲れ様です。松平です。<br>名古屋大学出張報告を添付します。<br>以上、よろしくお願いいたします。 |
| 添付ファイル名1   | NagoyaUnivReport.docx                                                |
| 添付ファイルサイズ1 | 176663 byte                                                          |
| ファイル保管期限   | 2008年12月25日 12時                                                      |

download 削除

ファイルの  
ダウンロード



受信者

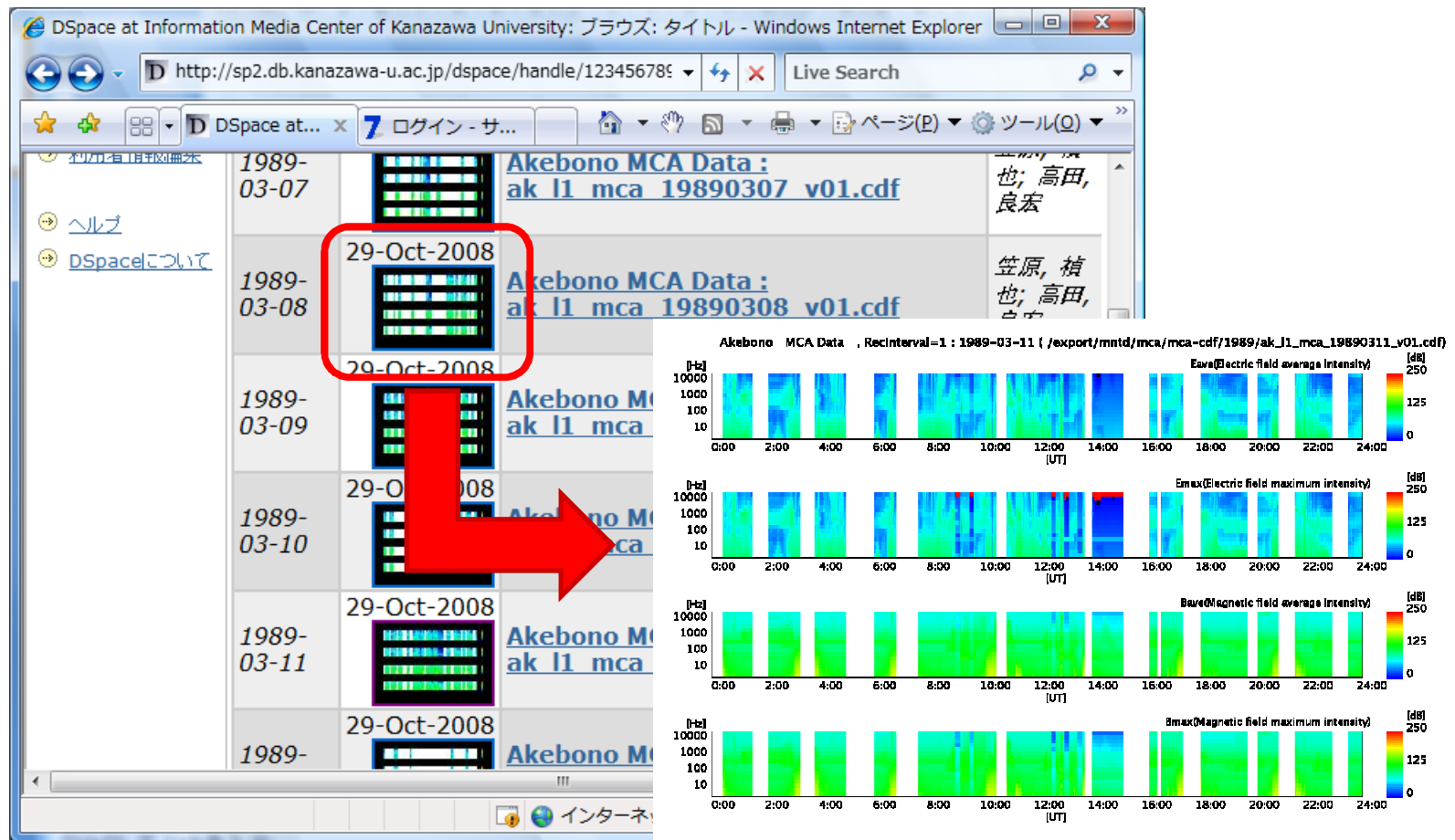
Shibboleth認証を行うこと  
でアクセス可能

# . 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ほぼ同じ

## . 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し、汎用的な  
フォーマットに変更した観測データを表示可能

# Shibboleth認証設定

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

```
<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  
SP側で認証機構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

# 全学的UPKI対応への取り組み（１）

UPKIによって大学間連携を実現するためには、金沢大学内でUPKIを利用できる環境を整備する必要がある

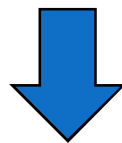
- 全学用LDAPサーバを認証・認可に利用
  - ネットワークID（uid）
    - ・ 金沢大学構成員がセンター提供のサービスを利用する際に使用する識別子
  - ネットワークID利用例
    - ・ 学内ネットワーク利用認証
    - ・ 学内無線LAN認証（Radius）
    - ・ VPN認証



ほぼ全構成員が既に取得済み

## 全学的UPKI対応への取り組み（２）

但し、ネットワークID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と対応したユニークなIDを別途生成する必要がある



UPKIの大学間連携では別途スキームを使用

eduPersonスキーム

eduPersonPrincipalName ( PrincipalName )

大学間連携の際に学外で使用するID

学外に送信してもユーザを特定されないように設計

但し、インシデント発生時には自組織でユーザを特定可能

eduPersonAffiliation ( Affiliation )

大学間連携の際に学外で使用する職種区分を識別

（ 学内のemployeeTypeを利用 ）



匿名性を保ちつつ、ユーザを一意に識別可能

# 全学的UPKI対応への取り組み（ 3 ）

## IdPのAttribute-resolver.xmlへの実装例（ 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>
```

LDAPにスキーマや属性を追加しなくても、マッピングによりネットワークIDを学外に送信しなくて済む

# SPにおける認可実験

IdPから送信された属性情報に基づく、SPでの認可実験を実施中

## SPのshibboleth2.xmlにへの実装例

```
<RequestMapper type="XML">
  <RequestMap applicationId="default">
    <Host name="sp1.db.kanazawa-u.ac.jp" authType="shibboleth" requireSession="true">
      <Path name="secure">
        <AccessControl>
          <AND>
            <Rule require="eduPerson_Affiliation">staff</Rule>
            <OR>
              <Rule require="principalName">abcde</Rule>
              <Rule require="principalName">efghi</Rule>
            </OR>
            <NOT>
              <Rule require="principalName">vwxyz</Rule>
            </NOT>
          </AND>
        </AccessControl>
      </Path>
    </Host>
  </RequestMap>
</RequestMapper>
```

AND、OR、NOTを使用した細かいAuthorizationが可能

# まとめ

- 金沢大学では独自の IdP および SP を構築し、フェデレーション経由での認証を伴う動作を確認した。
- 全学的な UPKI 対応のため、既存の全学 ID であるネットワーク ID の LDAP サーバに、必要な属性を追加している。
- SP における IdP から送信された属性情報に基づく認可について、検証を行っている

## 感想

- 他大学からの利用者について身元が保証されることは、大学間においてサービスを安全に提供するために大変有意であると思われる
- 魅力のある SP の具体的内容については金沢大学内においても検討中であるが、各大学の足並みを揃えるべきものについては一元的に提案されることが望ましい
- 実験のサポート体制が充実しており、こちらからの質問に対して丁寧に教えていただいた

# 今後の展望

- 全学用LDAPサーバのUPKI対応
  - 全学用 LDAP サーバによる UPKI シングルサインオンの動作確認
  - ユーザ数の増加に伴う IdP サーバの負荷調査
- SPへ認可機構の実装
  - 認可実験の結果を基にした認可機構の SP への実装
  - 全学用LDAPサーバから取得した属性の SP での認可における活用
- 平成21年度から開始予定の「学術フェデレーション（UPKI-Fed）試行運用」への積極的参加
  - 今回構築したシステムを使用しての、「属性情報の送信確認」実証等の運用実験への参加

来年度のUPKIシングルサインオン試行運用にも積極的に参加していく予定