

金沢大学における大学間連携への取り組み ～UPKI仕様に基づくShibbolethを用いたIdP及びSP構築～

金沢大学 松平 拓也、井町 智彦、笠原 禎也、高田 良宏

takusng@kenroku.kanazawa-u.ac.jp

1. 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

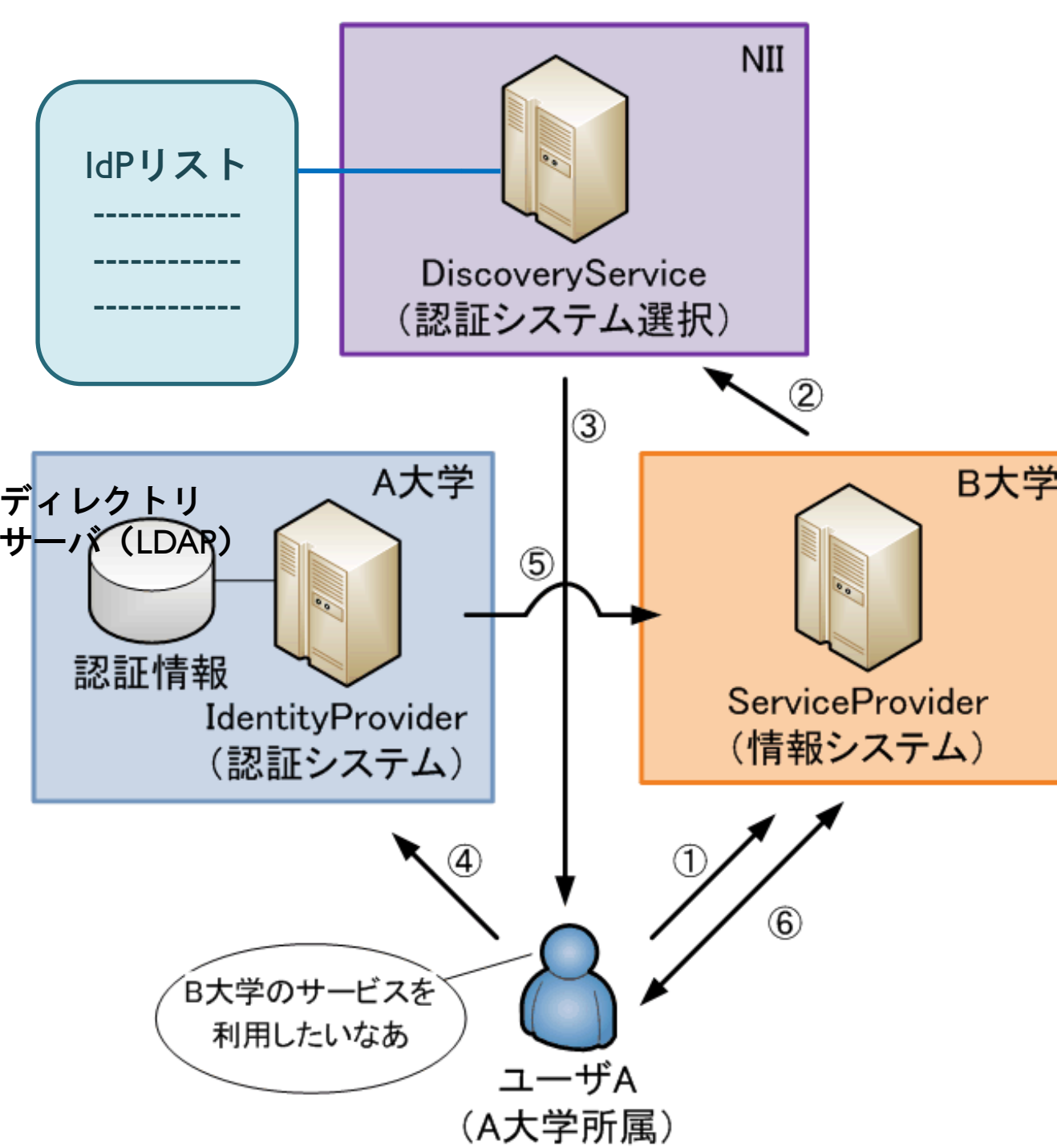
IdP連携実験

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及びSPの実装にはShibboleth※を使用
(※SAML2.0(XML仕様)を標準実装したOSS)



(例) A大学所属のユーザAがB大学のサービスを利用したい場合

- ① ユーザAがB大学のSPにアクセス
- ② SPはNII管理のDSにアクセスを転送
- ③ ユーザAはDSから自所属のIdPを選択
- ④ ユーザAは自所属のIdPで認証
- ⑤ IdPはユーザAの情報をSPに送信
- ⑥ SPはユーザAのアクセスを許可

2. 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

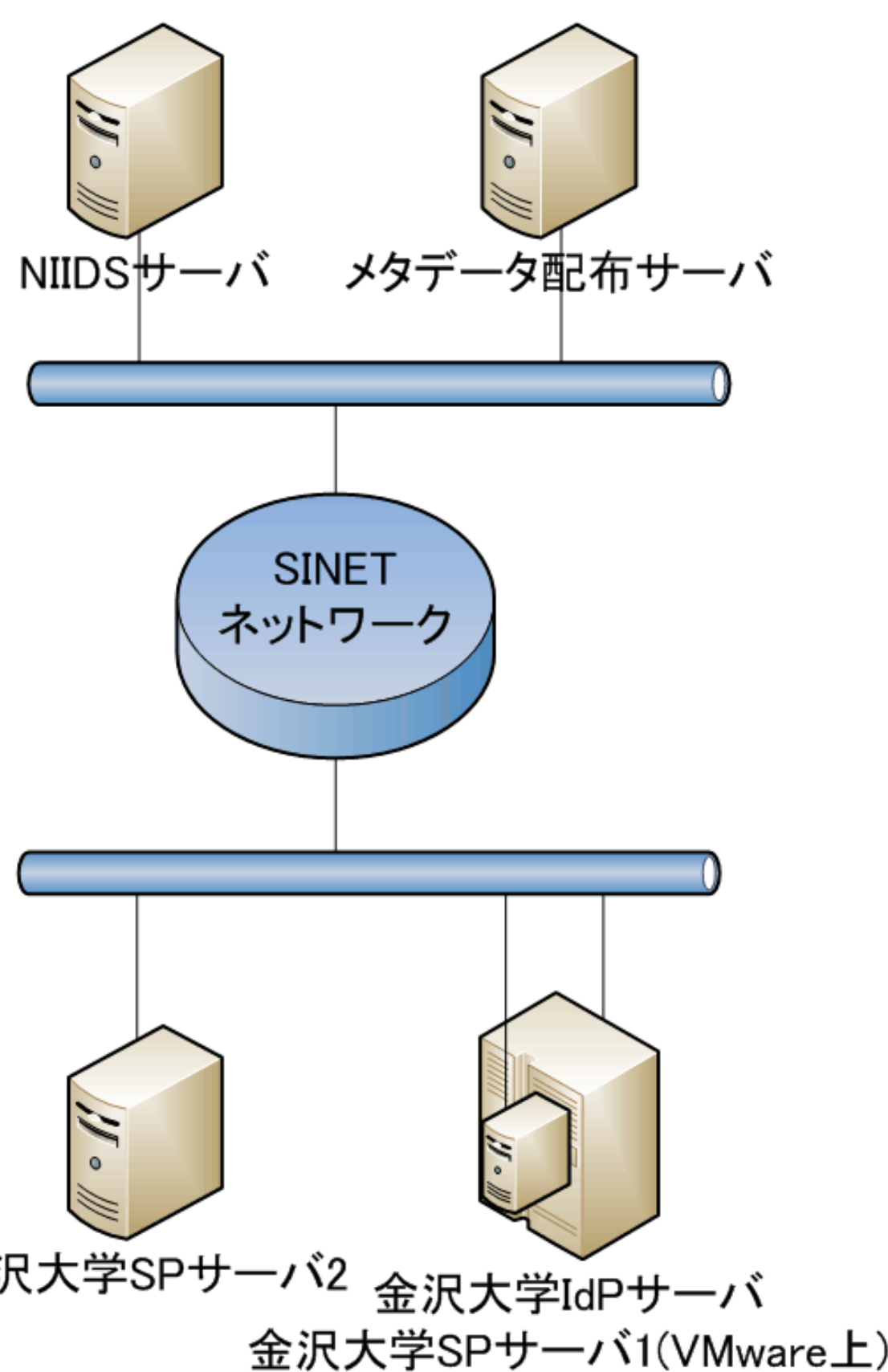
メモリ: 256MB
OS: CentOS5.2
アプリケーション: php5.1.6

「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

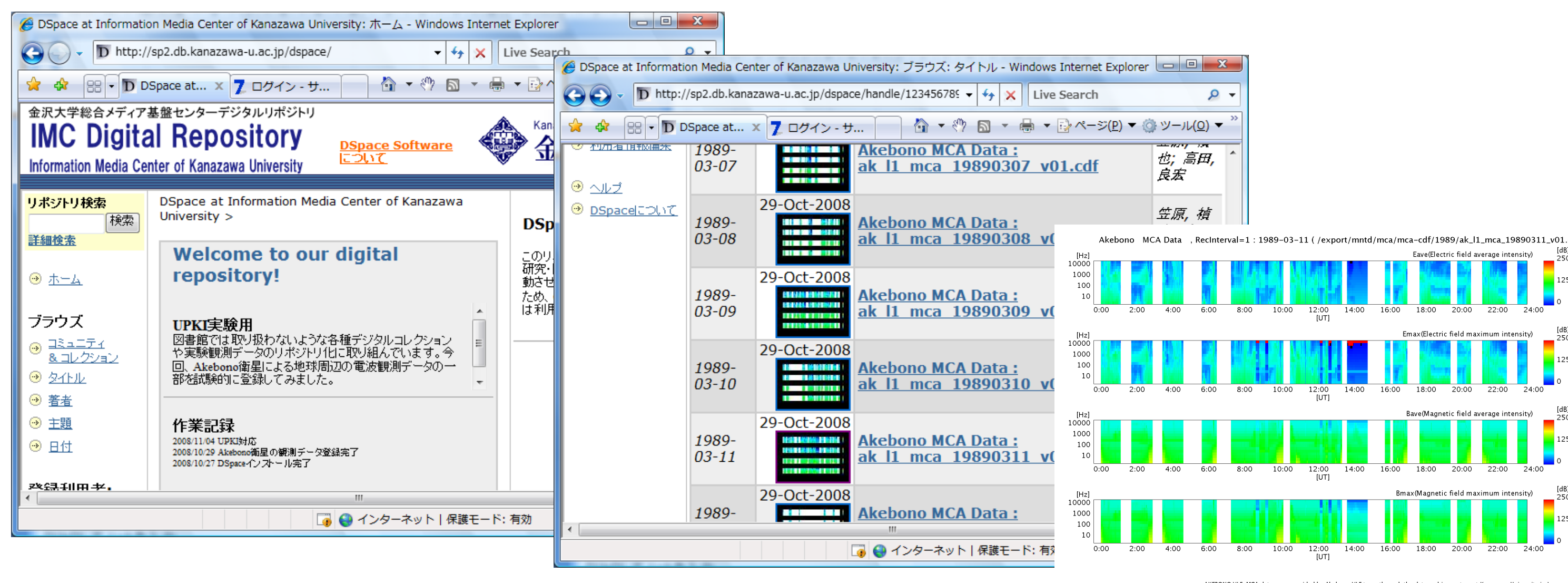
「Dspaceによるデジタルコンテンツ公開サービス」



4. 構築したSP(2)

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)



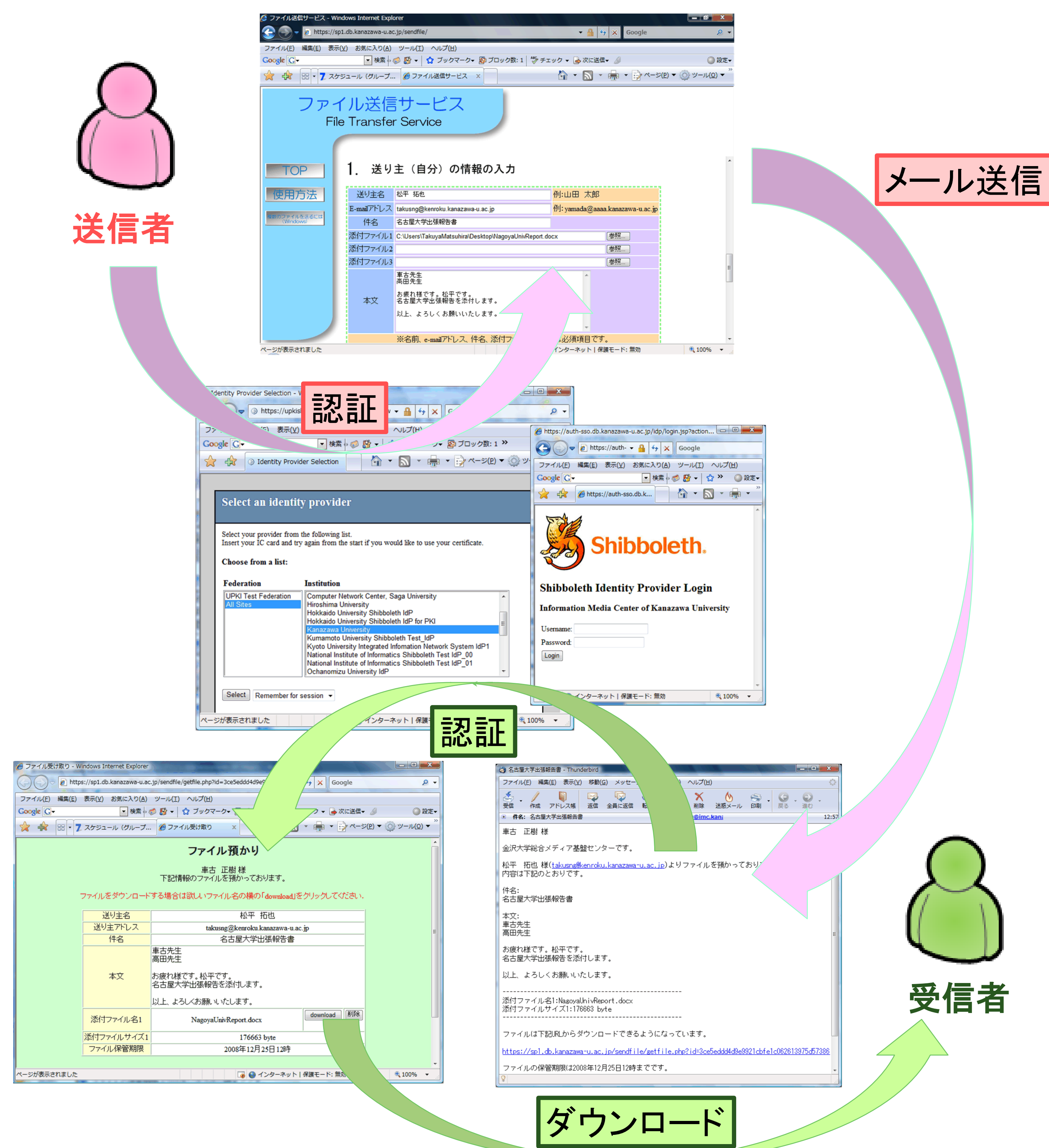
サムネイルの一覧を表示し、汎用的なフォーマットに変更した観測データを表示可能

3. 構築したSP(1)

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



5. 金沢大学におけるUPKI対応への取り組み

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

→ ほぼ全構成員が既に取得済み

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マが必要

eduPersonスキーマの追加

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を利用予定)



匿名性を保ちつつ、ユーザを一意に識別可能

現在、UPKI認証連携基盤属性仕様(案)の必須属性であるeduPersonPrincipalName、eduPersonAffiliation、o、ouを全学用LDAPサーバに追加中

6. まとめと今後の課題

- 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
- 現在、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

来年度も引き続き、UPKIの実証実験に積極的に参加していく予定