第8回金沢大学データベースフォーラム
2009/3/19（Thu）

UPKIにおける金沢大学の取り組み
～学内認証基盤から大学間連携まで～

金沢大学総合メディア基盤センター
松平拓也、笠原禎也、高田良宏、井町智彦

1

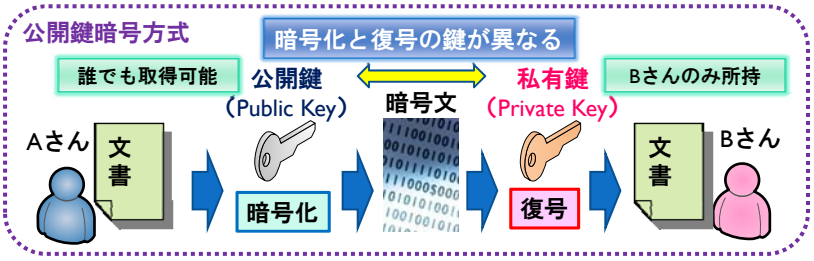
目次

- UPKIとは
- UPKI実証実験概要
- 金沢大学におけるIdP・SP構築
- 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

2

UPKIとは

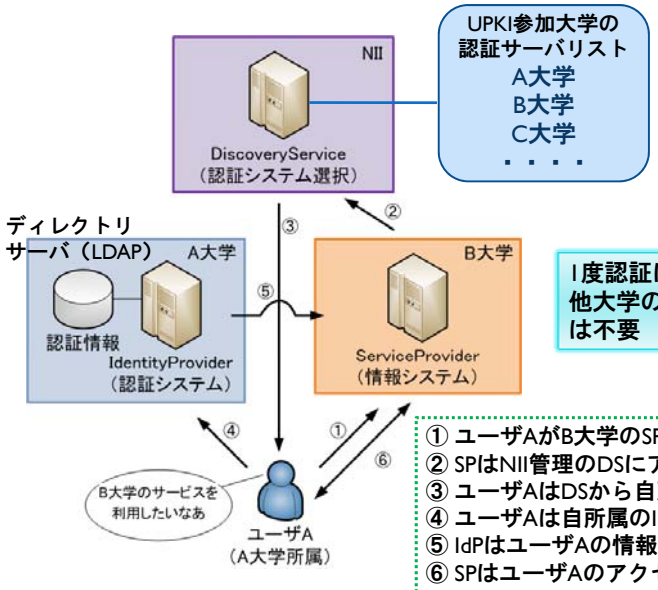
- **U**niversity **P**ublic **K**ey **I**nfrastructure
  全国大学共同電子認証基盤
  - PKIを利用してセキュアな大学間連携を実現
    大学等が保有する電子コンテンツ等の学術情報資源を共有可能
- PKIとは
  - 公開鍵暗号技術を使って、インターネット上で安全な通信ができるようにするための環境（インフラ）



大学間でセキュアで信頼されたネットワーク環境を構築

3

UPKI概念図



I度認証に成功すれば他大学のSPで認証作業は不要

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

4

UPKI実証実験概要

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連携の検証を行う

参加大学が行うこと

1. IdP（Identity Provider）サーバの構築
   ユーザ情報を管理して認証を行う（認証サーバ）
2. LDAPサーバの構築
   IdPが参照するユーザ情報を格納する（ディレクトリサーバ）
3. SP（Service Provider）サーバの構築
   IdPに認証を要求するとともに、IdPから送られてくる属性
   （ユーザ情報）を基にサービスを提供する（サービス提供サーバ）

- IdP、SP構築にはShibbolethを使用（オープンソースソフトウェア）

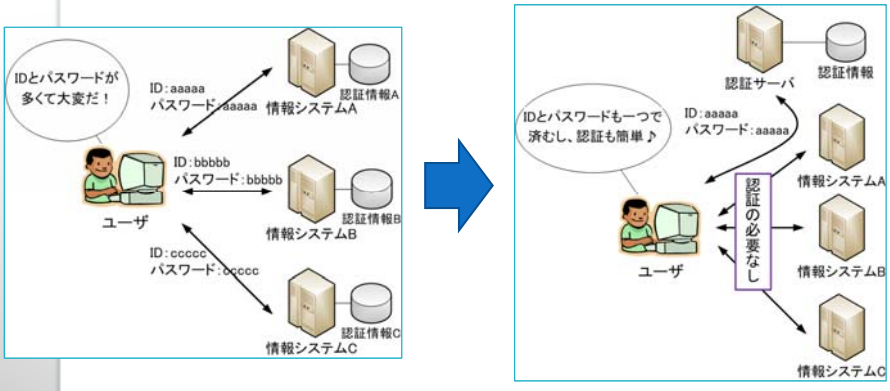
UPKIフェデレーション※の構築

※あるポリシ（規定）のもとで相互に信頼し認証情報を交換する
ことに合意した組織（サービス）の集合

5

シングルサインオンとは

**ユーザが1度認証を受けるだけで、認証を必要とする
複数のサービスを利用できるシステム**



6

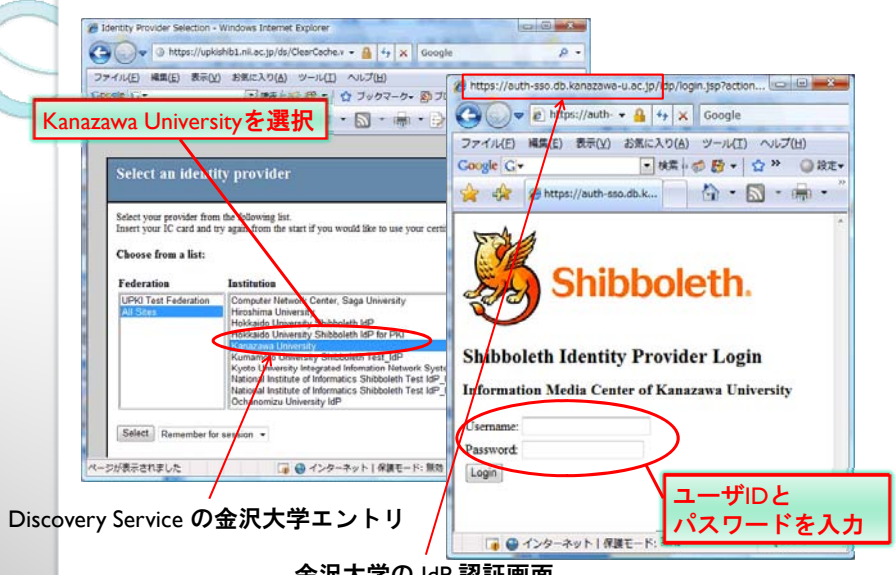
LDAPとは

- **L**ightweight **D**irectory **A**ccess **P**rotocol
- ディレクトリサービスを利用するためのプロトコルの一つ
  - ディレクトリサービス
    - ネットワークを利用するユーザ名やマシン名などの様々な情報を管理するためのサービス
    - ユーザ名などのキーとなる値から様々な情報を検索することが可能
  - 特徴
    - 読み取りが高速（ほとんど読み取りのみに使用）
    - 情報を1か所で集中管理可能

各情報システムが認証情報を持つ必要がなくなる

7

Shibboleth認証の動作確認



8

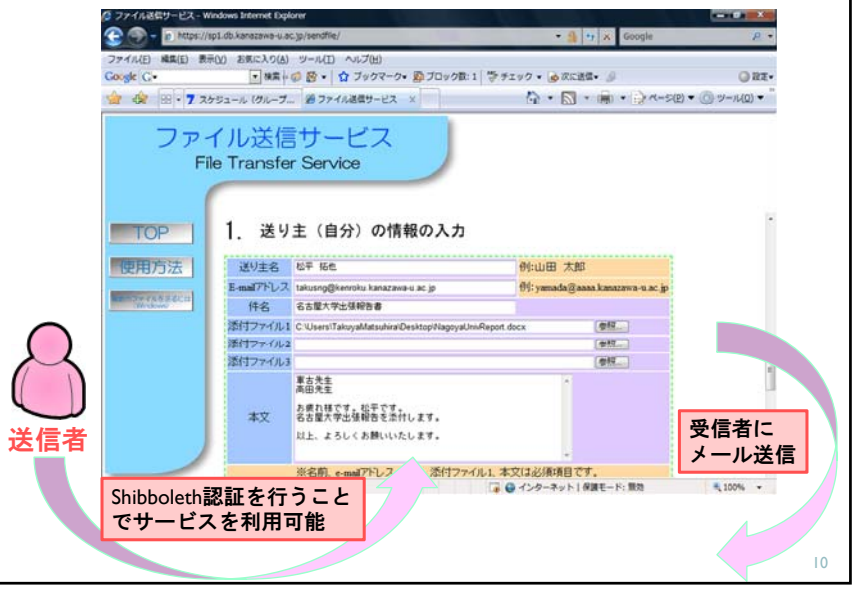
実証実験において構築したSP

- Ⅰ.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
- Ⅱ.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

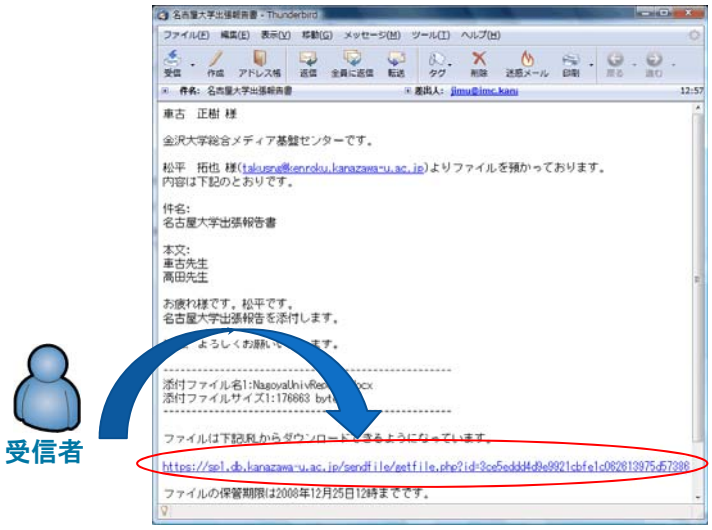
9

ファイル送信サービス（１）



10

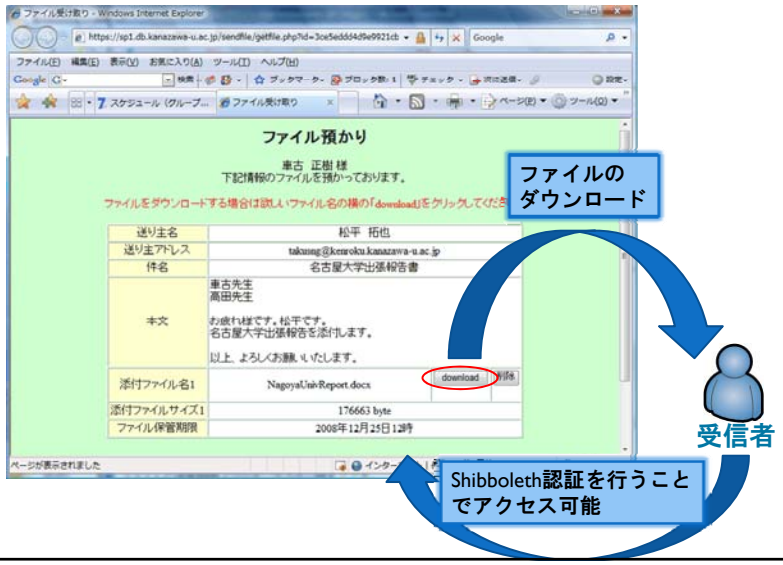
ファイル送信サービス（２）



受信者はメールに記載されたURLにアクセス

11

ファイル送信サービス（３）



12

デジタルコンテンツ公開サービス

- DSpace
  - オープンソースのリポジトリ構築ソフトウェア
- 機関リポジトリ
  - 大学などの研究機関において学術論文，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し，インターネット上で公開するシステム
  - 書誌コンテンツ以外の画像，動画など
    - 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
  - 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）

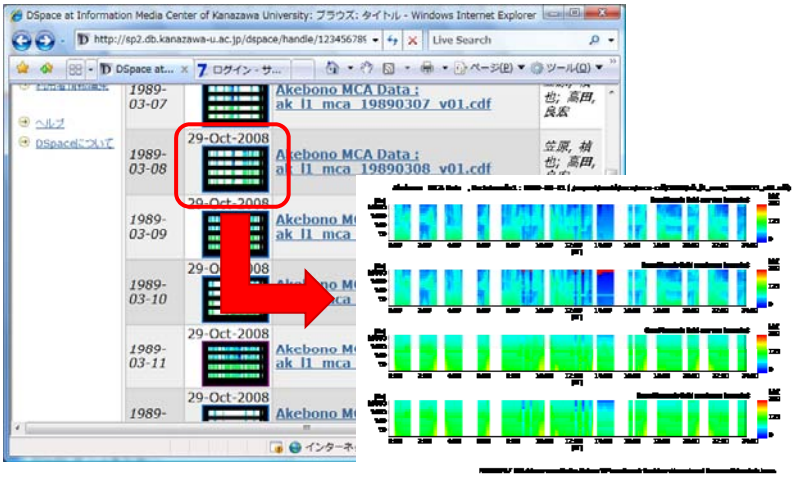
13

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

14

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

15

実演

16

全学的UPKI対応への取り組み

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
    - 学内無線LAN利用認証（Radius）
    - VPN利用認証

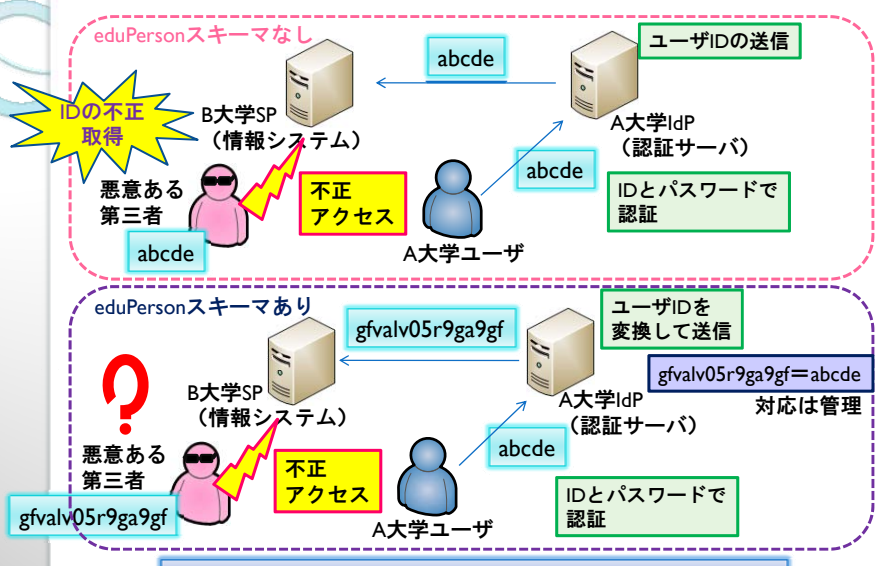
ほぼ全構成員が既に取得済み

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

eduPersonスキーマの利用

17

eduPersonスキーマ使用のメリット

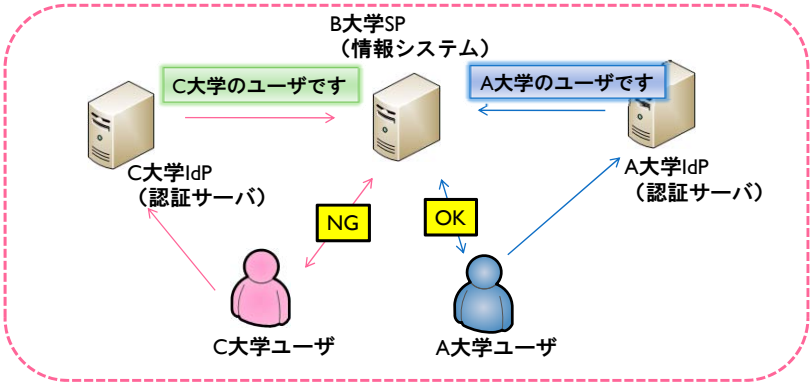


学外でIDが漏れた場合でも本当のユーザIDは特定不可能

18

SP側での認可対応

認可（Authorization）
認証済みの利用者に対して、何らかのサービスの利用やリソースへのアクセスなどに対する権限を与えたりすること



特定の組織やユーザだけにサービスを利用させることも可能

19

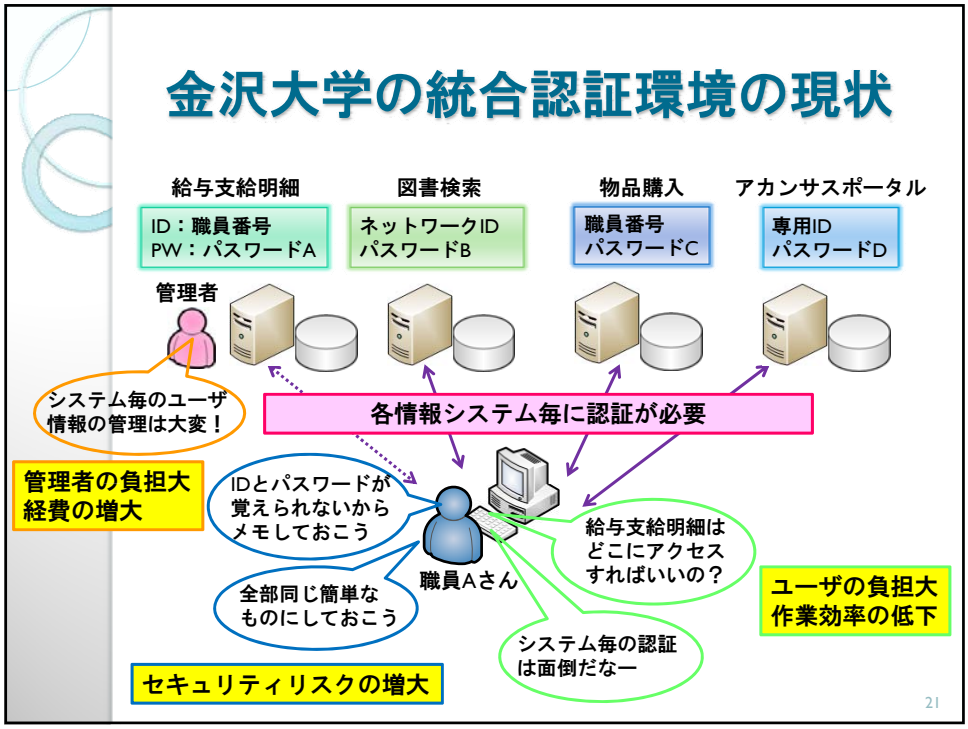
SPにおける認可設定例

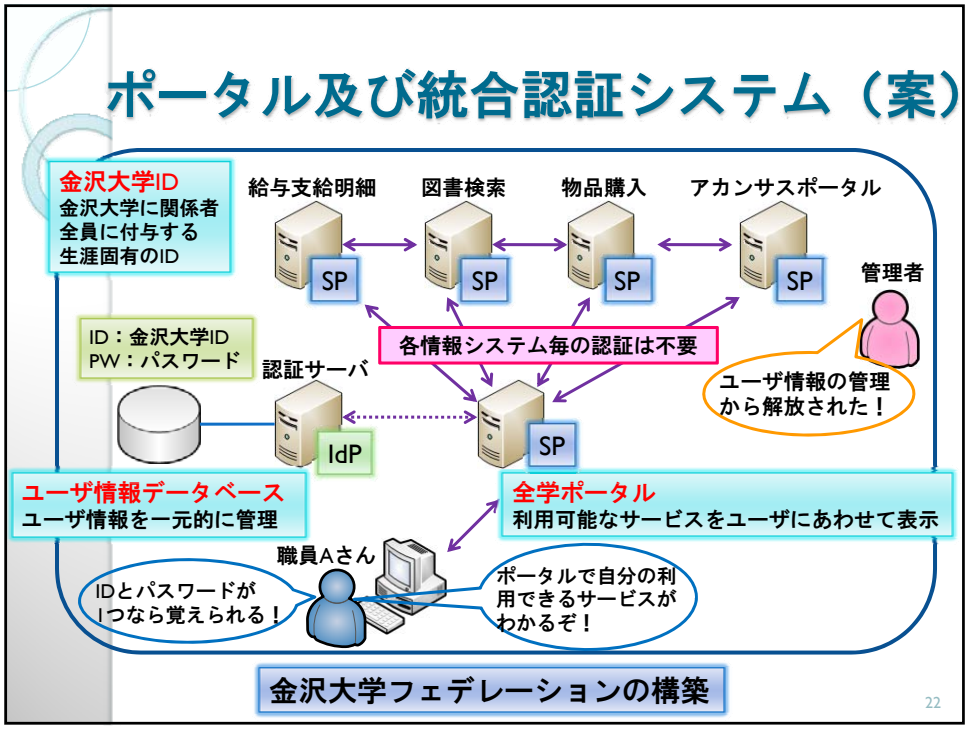
SPの設定ファイルに下記のように記述

```
<Host name="sp1.db.kanazawa-u.ac.jp" authType="shibboleth"　・・・>
    <Path name="secure">
        <AccessControl>
            <AND>
              <Rule require="o">A University</Rule>
              <OR>
                 <Rule require="principalName">abcde</Rule>
                 <Rule require="principalName">efghi</Rule>
              </OR>
              <NOT>
                 <Rule require="principalName">vwxyz</Rule>
              </NOT>
            </AND>
        </AccessControl>
    </Path>
</Host>
```

AND、OR、NOTを使用して細かい認可が可能

20


金沢大学の統合認証環境の現状
給与支給明細
ID：職員番号
PW：パスワードA
図書検索
ネットワークID
パスワードB
物品購入
職員番号
パスワードC
アカンサスポータル
専用ID
パスワードD
管理者
システム毎のユーザ情報の管理は大変！
各情報システム毎に認証が必要
管理者の負担大
経費の増大
IDとパスワードが覚えられないからメモしておこう
全部同じ簡単なものにしておこう
職員Aさん
給与支給明細はどこにアクセスすればいいの？
システム毎の認証は面倒だなー
ユーザの負担大
作業効率の低下
セキュリティリスクの増大
21


ポータル及び統合認証システム（案）
金沢大学ID
金沢大学に関係者全員に付与する生涯固有のID
給与支給明細
図書検索
物品購入
アカンサスポータル
SP
管理者
ID：金沢大学ID
PW：パスワード
各情報システム毎の認証は不要
認証サーバ
IdP
ユーザ情報の管理から解放された！
ユーザ情報データベース
ユーザ情報を一元的に管理
全学ポータル
利用可能なサービスをユーザにあわせて表示
職員Aさん
IDとパスワードが1つなら覚えられる！
ポータルで自分の利用できるサービスがわかるぞ！
金沢大学フェデレーションの構築
22

まとめ

- 金沢大学ではUPKI実証実験において独自の IdP および SP を構築し動作を検証した
- 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の利用を検証中
- 金沢大学統合認証システムにShibbolethを導入できるか技術的な側面から検証中

UPKIの感想

- 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の構築が今後のUPKIの発展には必要不可欠であると思われる
  - 電子ジャーナル購読
  - 無線LANローミング（他大学のネットワーク利用）

23

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
- 金沢大学統合認証システムにおけるシングルサインオンの検討
  - Shibbolethを利用した全学統合認証システムの検討

24