# 安全・安心な大学間情報共有を実現するサービスプロバイダの構築と今後の展開

金沢大学　松平 拓也　笠原 禎也　高田 良宏

takusng@kenroku.kanazawa-u.ac.jp

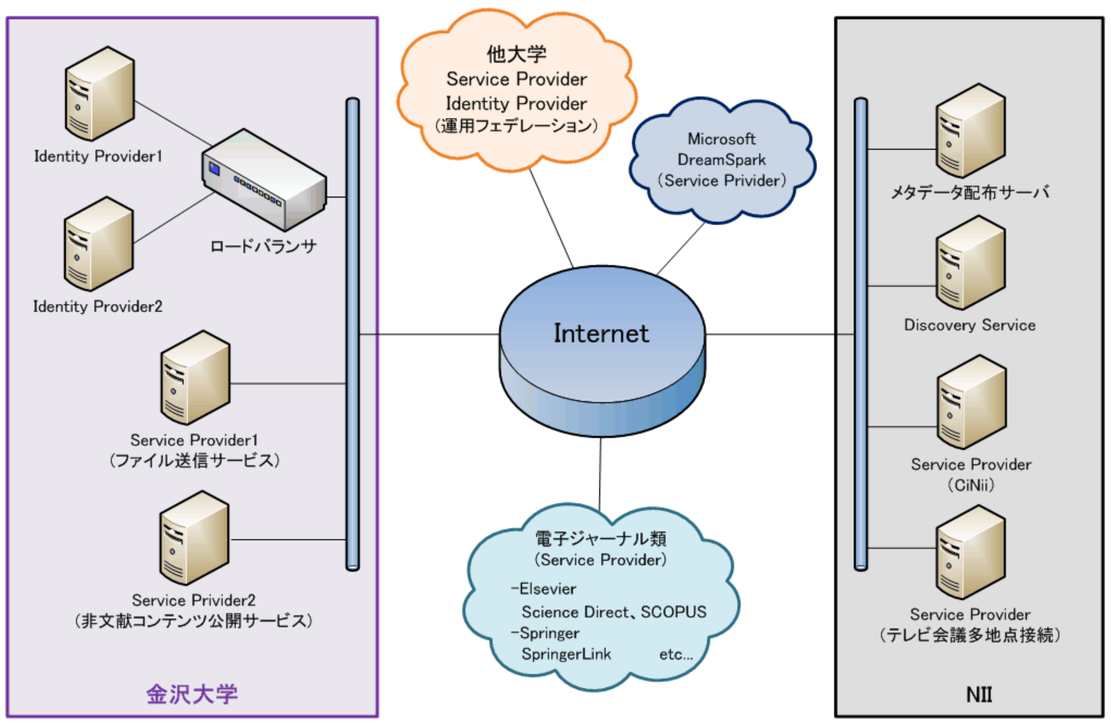
## 研究の概要

研究・教育・業務など大学における様々な活動において，ユーザ間で情報共有を行う場面が数多く存在する．その際，少数かつ容量の小さなデータであれば電子メールでやりとりすることができるが，少し扱うデータの規模が大きくなると，ユーザ同士だけでは情報を共有することが難しくなる．その結果，物理的に距離が近い場合はUSBメモリなどを利用したり，他大学のユーザとの共有の場合は外部のファイル転送サービスを利用したりしているのが現状である．その結果，ユーザが不便を感じるだけではなく，データが流出する危険性を常に孕んでいる．

そこで本研究ではUPKI認証連携基盤を利用し，大学内はもちろんのこと，大学間においても安全・安心に情報を共有できるシステムの開発を目的としている．UPKI認証連携基盤を用いる最大のメリットは，他大学のユーザをこちらで管理することなく身元を保証することができることにある．この性質を利用し，現在金沢大学では「ファイル送信サービス」と「非文献コンテンツ公開サービス」の2つのシステムを開発し，運用を行っている．本システムを利用することにより，UPKIを利用できる環境にあるユーザ同士であれば，安全・安心に情報を共有することが可能になった．

今後の展開として，現在共有したいデータの保管は本学のサーバが担っているが，今後はNIIやデータセンターなど，信頼性の高い場所に保管できるようにしたり，ファイルサーバを各大学が持ち，データも各大学で保管できる機構を構築したりなど，さらに安全性を高めていく必要性があると考えている．

## 金沢大学におけるUPKI構成状況




### 金沢大学サーバ概要

**ロードバランサ**
富士通 IPCOM EX1200 LB

**Identity Provider1**
Dell PowerEdge T300
CPU：Intel Core2Duo E6305
メモリ：4GB
HDD：500GB(RAID1)
OS：CentOS5.4(64-Bit)

**Identity Provider2**
Epson Endeavor NP11-V
CPU：Intel Atom230(1.6GHz)
メモリ：1GB
HDD：160GB
OS：CentOS5.4(64-Bit)

**Service Privider1**
**（ファイル送信サービス）**
Dell PowerEdge T300
CPU：Intel Core2Duo E6305
メモリ：4GB
HDD：500GB(RAID1)
OS：CentOS5.4(64-Bit)

**Service Privider2**
**（非文献コンテンツ公開サービス）**
CPU：Intel Core2Duo E8400
メモリ：2GB
HDD：250GB
OS：CentOS11.1(64-Bit)

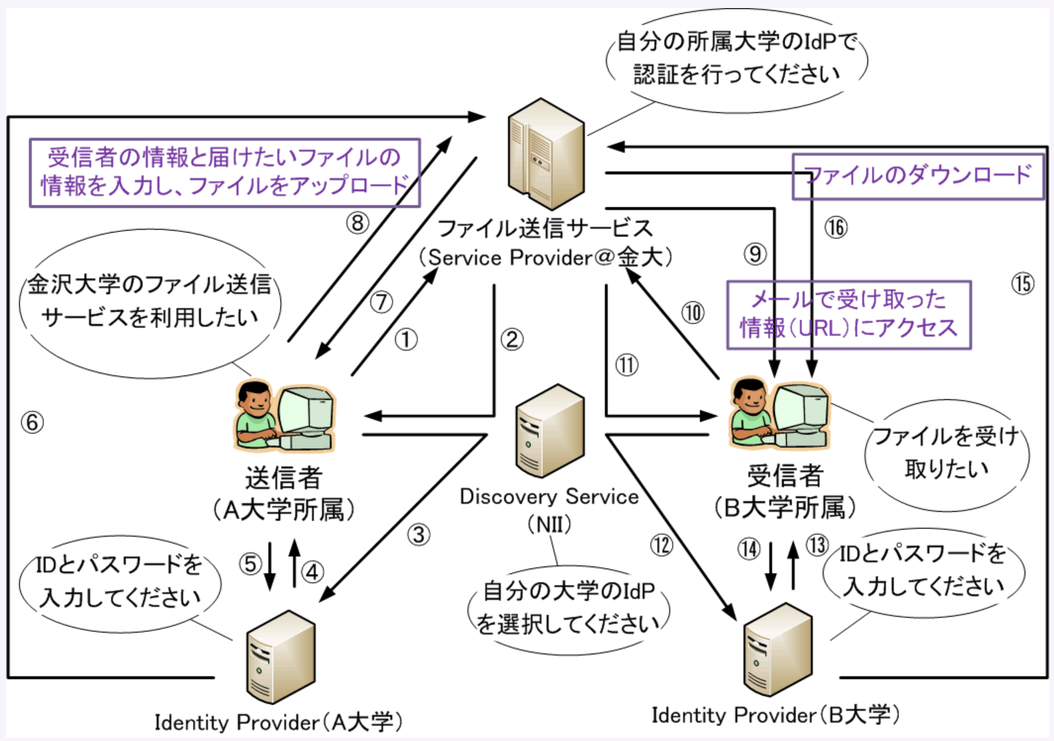
- ロードバランサは，IdP1：IdP2 が 3：1 の割合となるよう分散を行っている
- IdPはTerracottaによるクラスタリングを行い，信頼性を高めている

## 金沢大学で運用中のService Provider

### ファイル送信サービス

https://sp1.db.kanazawa-u.ac.jp/sendfile/　日本語版
https://sp1.db.kanazawa-u.ac.jp/sendfile/ en/　英語版

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するService Provider
一度に3つのファイルを5人のユーザに送信可能（3つのファイルの合計が100MBまで）




### ファイル送信サービスの動作

① 送信者がファイル送信サービスにアクセス
②③送信者の身元確認・利用権限を確認するため，NIIのDiscovery Serviceにリダイレクトし，自大学のIdentity Providerを選択
④⑤ 自大学のIdentity Providerで認証（自大学で配布されたIDとパスワードで）
⑥ 送信者の認証の成否および，属性情報をIdentity Providerから受け取る

**サービスを利用するのに必要な属性情報**

eduPersonPrincipalName
フェデレーション内で一意な，かつ，永続的な利用者識別子
組織で一意な利用者識別子とスコープ（kanazawa-u.ac.jpなど）を合わせることで，フェデレーション内での一意性を保証
例）matsuhira@kanazawa-u.ac.jp

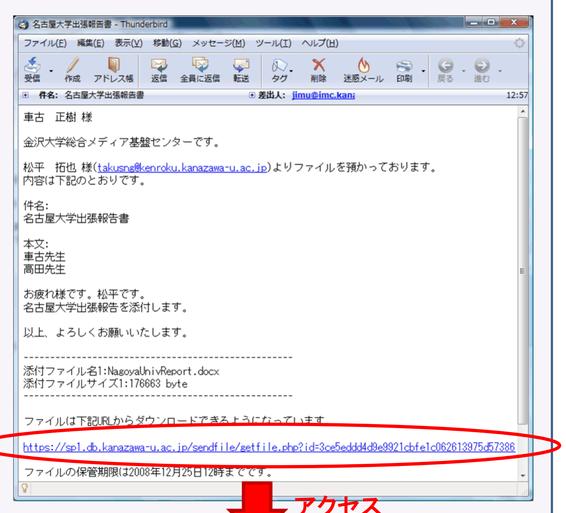
eduPersonScopedAffiliation
利用者の職種などをあらわすことが可能で，@以下にスコープを付加
faculty, staff, student, member,なし（空白）を設定可能
例）staff@kanazawa-u.ac.jp

eduPersonPincipalNameに値がセットされていて，eduPersonScopedAffiliationがfacultyまたはstaffの場合のみ利用可能（各大学の教職員のみ利用許可）

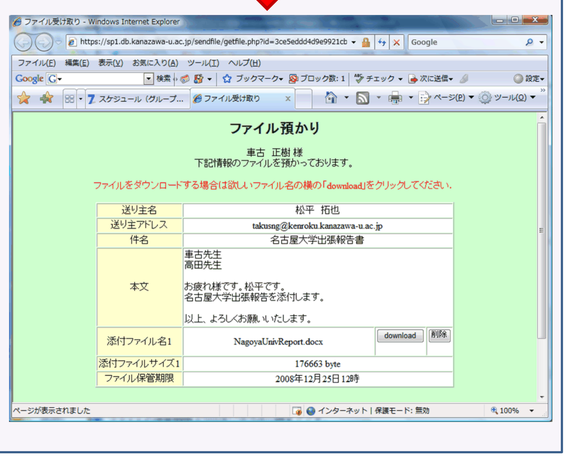
上記のほか，サーバ環境変数から**Shib-Identity-Provider**（利用したIdentity Privider 情報），**REMOTE_ADDR**（利用者IPアドレス）を取得し，不正な利用があった場合等に，ユーザを迅速に特定できるように設計

※eduPersonPrincipalName以外の情報だけではSP側でユーザの特定まではできないため，ログを残しても個人情報保護の観点からは問題ないと考える

⑦⑧ 自分の情報および，受信者の情報を入力
⑨⑩ 受信者は受け取ったメールアドレスに記載されたURLにアクセス
⑪⑫⑬⑭⑮ 送信者と同様，受信者の身元および利用権限を確認
⑯ ファイルのダウンロード




アクセス




### 非文献コンテンツ公開サービス

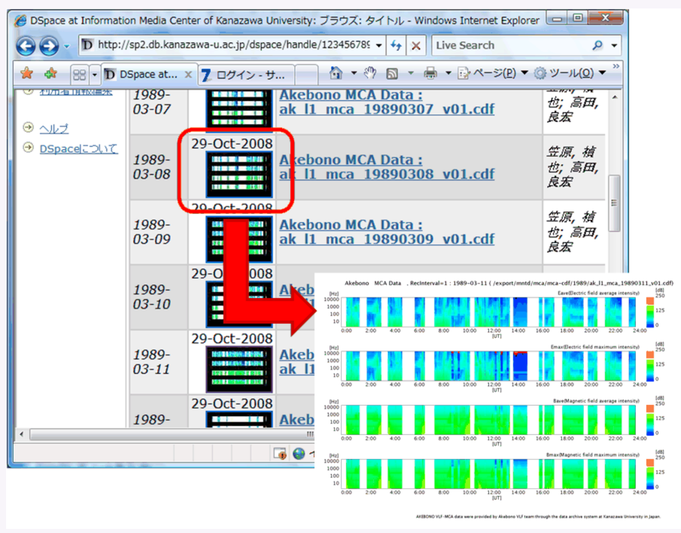
https://sp2.db.kanazawa-u.ac.jp/dspace/

大学で生産された実験観測データ等を特定の組織やグループに公開するService Provider
学術論文等の書誌系以外の非文献コンテンツ公開を目的に改良したDspaceで構築

原則として誰にでも公開する書誌系とは異なり，特定の組織やグループに限定での公開を目的

**サービスを利用するのに必要な属性情報**
eduPersonPrincipalName
eduPersonScopedAffiliation
※利用傾向の把握を行うため，eduPersonScopedAffiliationの情報のみログに記録

現在はUPKI認証に成功し，上記の属性情報がセットされていて，IdPの環境に問題がないと判断したユーザは閲覧可能




## まとめと今後の展開

UPKIの最大のメリットである，他大学からの利用者について身元が保証されるという性質を利用することで，大学間において，ユーザが安全・安心に情報共有できるサービスを構築することができた．

今後の展開として，一つはデータの保管場所をどうするかという問題がある．現在は金沢大学のサーバに保管されているが，将来的には，NIIやデータセンターなどがデータの管理を担っていくか，各UPKIフェデレーション参加大学がファイルサーバを構築し，Identity Providerによるユーザの管理だけではなく，データの管理まで行う必要があると考えている．

もう一つは，個人情報保護の問題である．現在は個人情報保護の観点から，個人が特定できる手前のデータのみ残している．しかし，さらにきめ細かいアクセス制限をかける場合は，個人が特定できるデータを用いる必要がある．そのため，現在UPKIフェデレーションで推奨している属性の中でも，eduPersonPrincipalNameをはじめとした，mail，sn，o，ou，givenName，displayNameなどといった個人の特定に結び付く属性情報の利用について慎重に検討を行いながら，より大学間で安全・安心な情報共有を行うことが可能なサービスへとこれらのService Providerを発展させていきたいと考えている．

### 参考文献

松平 拓也，笠原 禎也，高田 良宏，井町 智彦，“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”，学術情報処理研究，No13，pp.84-90，2009