



実証実験の状況と フェデレーション (UPKI-Fed) 構築について

国立情報学研究所
片岡 俊幸



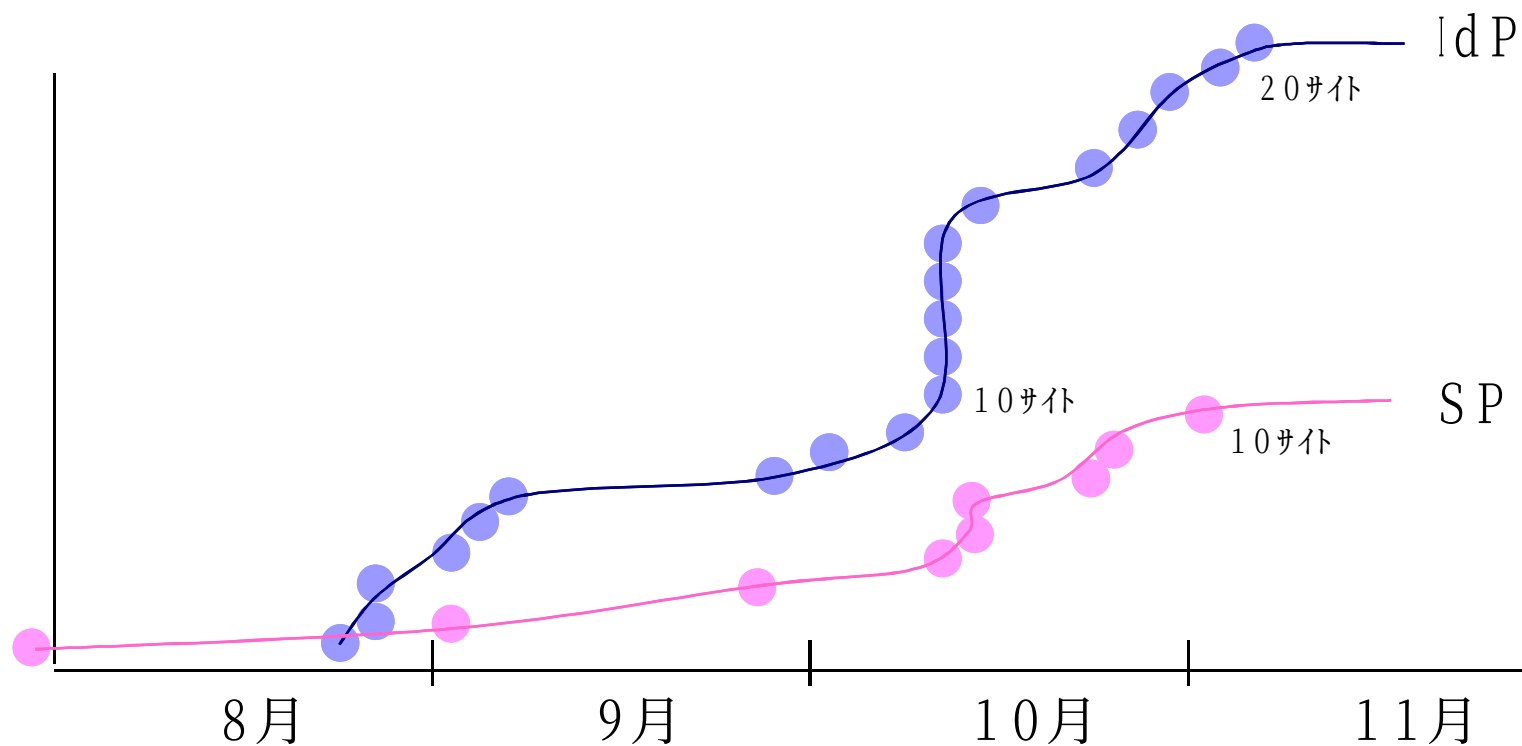
1. 実証実験の概要報告
2. フェデレーション (UPKI-Fed) の構築について
3. 実証実験の進め方



1. 実証実験の概要報告

1-1. 参加機関

- 参加機関 (26 機関)
- IdP (18 機関、20 サイト)
- SP (9 機関、10 サイト、公開3 サイト)



1－2. 構築状況一覧

参加機関名称	Id P	S P
北海道大学	○	—
東北大学	○*	—
山形大学	—	—
高エネルギー加速器研究機構	—	—
筑波大学	○	(未公開)
筑波技術大学	—	—
千葉大学	△	—
東京大学	○*	—
東京工業大学	○	(未公開)
お茶の水女子大学	—	—
産業技術大学院大学	○2	マルチマウスAP、 (構築中)
慶応義塾大学	—	—
国立情報学研究所	○2*	CiNiiテスト*

参加機関名称	Id P	S P
金沢大学	○	ファイル送信サービス、 (DSpace)
名古屋大学	○	—
愛知県立看護大学	○	—
京都大学	○	(無線LANアカウント発行)
京都産業大学	—	—
大阪大学	○	(グリッド証明書発行)
愛媛大学	—	—
徳島大学	—	(OpenPNE)
広島大学	○	—
山口大学	○*	(未公開)*
九州大学	○	—
熊本大学	○	—
佐賀大学	○*	(未公開)

- : 構築済み
 2 : 2サイト構築
 △ : 接続実験中
 * : メタデータ自動更新設定済み

1－3. 実験と構築の課題

- メタデータ自動更新設定：
プロキシの設定で、ダウンロードできない。(1件)
- メタデータの個人情報の扱い：
管理者情報→管理機関情報に変更
- 利用する証明書：
UPKIサーバ証明書(16機関)
Campus証明書(1機関)
- eppnのScopeの問題提起(1件)
- ID/パスワード認証、証明書認証の混在？(1件)

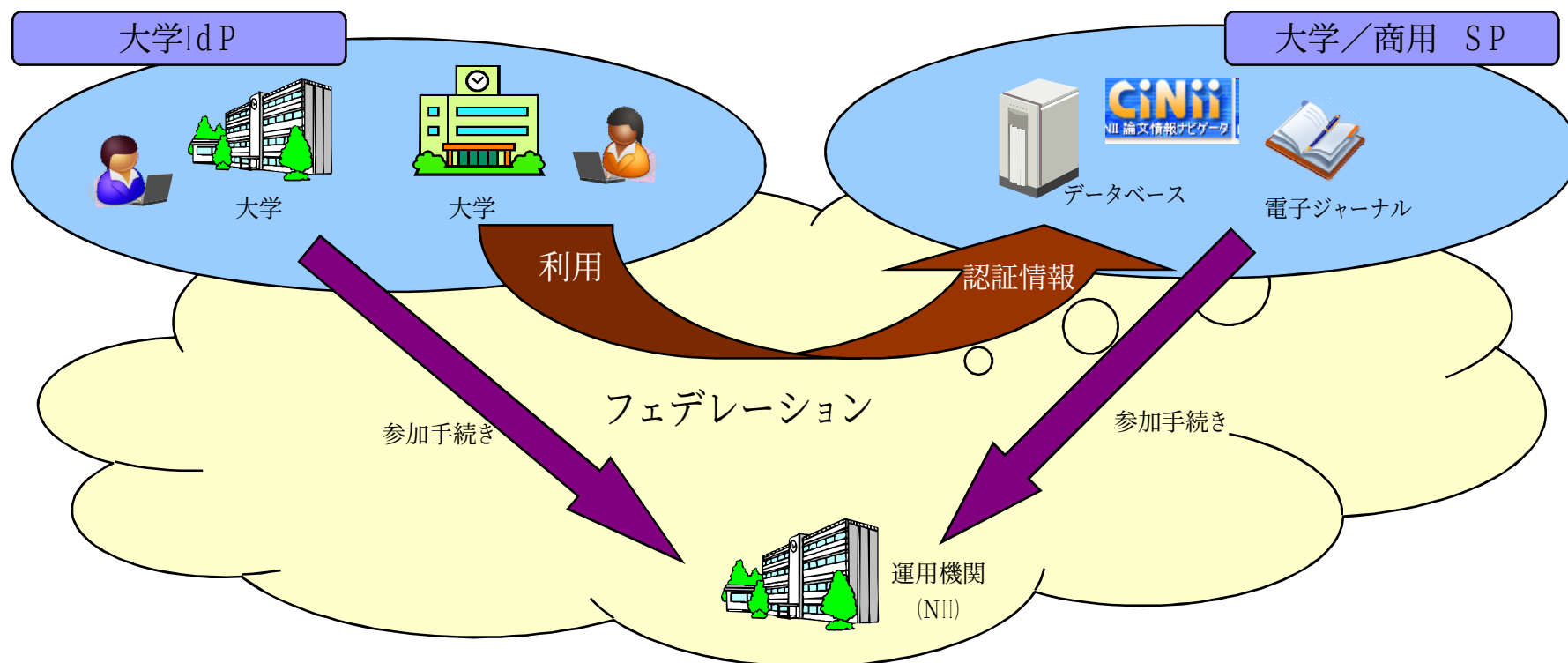
→ 支援状況から見て、大きな問題無く構築が進んでいると考えられる。

→ 構築したサイト間では、問題無く連携できていると考えられる。



2. フェデレーション (UPKI-Fed) の構築について

2-1. フェデレーションの構築 (平成21年度～)



- 大学等とNIIが連携してフェデレーションを構築・運用する。
- フェデレーションへの電子ジャーナル等出版社の参加を交渉し、対象コンテンツの拡充を図る。(Elsevier社は、平成20年11月中に実現予定)
- NIIが提供するコンテンツのシングルサインオン化を実現。

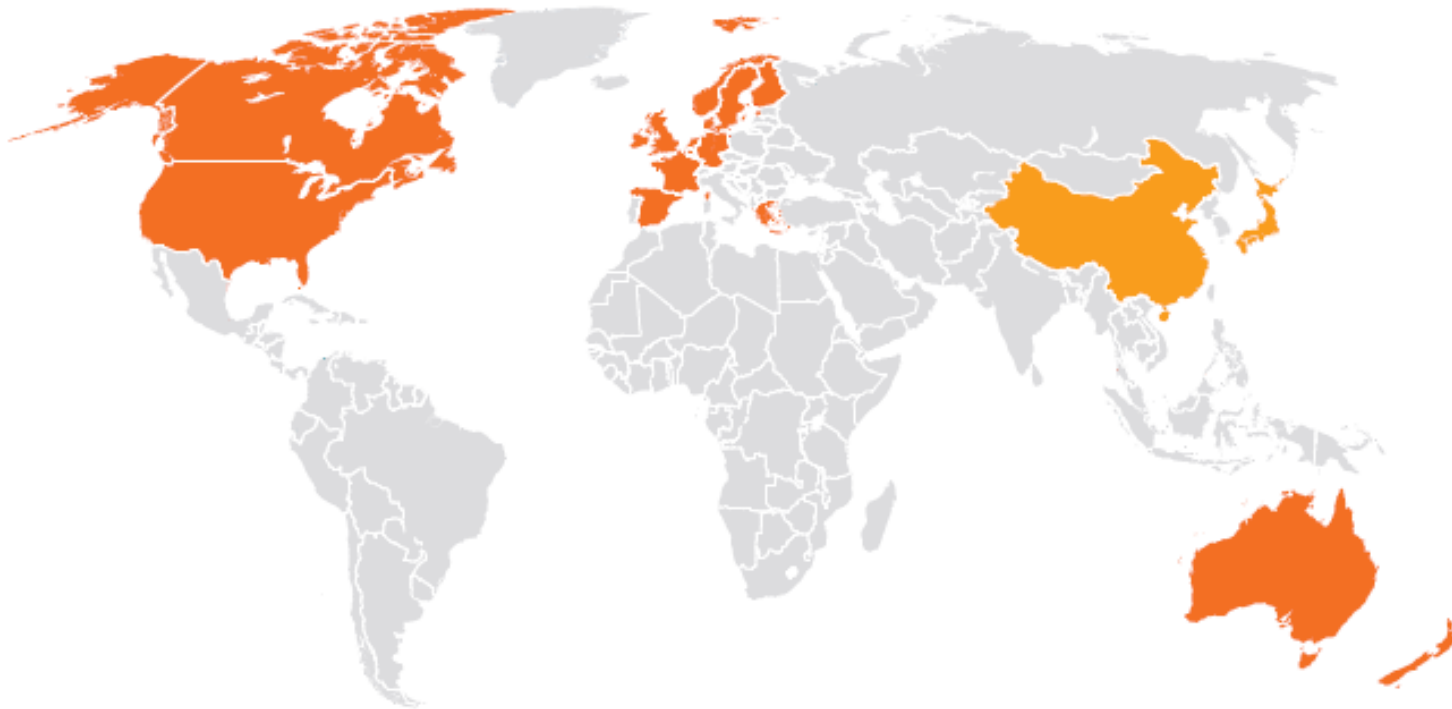
2ー2. フェデレーション構築スケジュール

事 項	内 容
実証実験の成果の利用	(平成21年1月～3月) ■ 実証実験で使用したIdP, SPを継続して運用 ■ 大学で構築されたIdP, SPの, フェデレーションへの移行
規程 (ポリシー) の作成	■ フェデレーションの規程 (ポリシー) を年度内に作成 ■ パブリックコメントを実施予定
対象コンテンツの拡充	■ 国立大学図書館協議会等の協力により, 商用電子ジャーナル各社と交渉を実施 (Elsevier社のScience Directについては, 平成20年11月中に実現予定) ■ NIIコンテンツサービスのシングルサインオン化実施
フェデレーション試行運用の実施	■ 平成21年度は, 試行運用としてフェデレーションを運用 ■ 試行運用を行いながら, 問題点の改善, 規程の改訂を実施 ■ 引き続き, 大学への参加を広く呼びかける

2-3. (参考) 世界のフェデレーション



NATIONAL IDENTITY MANAGEMENT FEDERATIONS



Current National Federations

Australia (AAF)	Germany (DFN-AAI)	Sweden (SWAMID)
Belgium (LUDIT-AAI)	Greece (HEAL-Link)	Switzerland (SWITCHaai)
Canada (NRC-CNRC)	Luxembourg (Restena)	The Netherlands (SURFnet)
Denmark (DK-AAI)	New Zealand (AAF)	United Kingdom (UK Access Fed.)
Finland (HAKA)	Norway (FEIDE)	United States (InCommon)
France (CRU)	Spain (RedIRIS)	

In Formation

Japan
China

02Sept2008

Internet2 informatin kits http://www.internet2.edu/pubs/national_federations200809.pdf から引用





3. 実証実験の進め方



3－1. 実証実験の進め方

I. 利用方法の検証:

1. ユーザの視点
2. 運用者の視点 (IdP)
3. 運用者の視点 (SP)

II. 連携実験の検証:

1. 属性管理
2. セキュリティ設定実験
3. ツール利用実験

3－2. 利用方法の検証（ユーザ）

■ 【想定するユーザのメリット】

□ シングルサインオン

IDの統合、（少なくとも）1つのパスワードを削減

□ 学外からのアクセス

□ ユーザは本人性（身元）を明かす機会が減少

個人情報 は 本人 と 所属機関 で 管理 される

□ 出版社からより良いサービスを提供される

個人情報 を 保護 した マイページ の 提供

■ 【検証項目】

□ 学内、学外からのログイン

□ シングルサインオンの利便性

□ 操作性

□ 安心感

□ 従来方法との比較

3－3. 利用方法の検証 (IdP)

■ 【想定するIdPサイトのメリット】

- 個人情報保護法の遵守
- ユーザへの、より良いサービスの提供
- 既存のアクセス管理システムとの連携
- 学内、学外含めた全てのリソースに対する管理方法の統一化
- 集中管理によるサポート問題の削減

■ 【検証項目】

- 構築状況
難易度、サーバ証明書の種類、認証方式、
ネットワーク構成等
- 運用状況
個人情報管理、属性リリースの設定方法、
学内ポリシーとの関係等
- 構築、運用の課題等

3－4. 利用方法の検証 (SP)

- 【想定するSPサイトのメリット】
 - ユーザデータベースの運用・管理がいらなくなる
認証はIdPで実行
認可は機関、職位、権限で判断
 - ユーザサポート工数の削減
 - 規程遵守のための工数削減
個人情報の蓄積、処理を削減
 - 厳格なライセンス制御管理の実現
 - ID統合により、ユーザのID／パスワード管理が向上
 - サービス利用機関は集中管理により正確な認証を運用・管理可能となる
- 【検証項目】
 - 構築状況
難易度、提供するアプリケーション、必須属性、
ネットワーク構成等
 - 運用状況
個人情報管理、ユーザ管理工数等
 - 構築、運用の課題等

3－5. 連携実験の検証

- 属性管理
 - 各属性の交換
 - 学内LDAPとの接続性
 - SPに対応した属性リリース制御
 - 日本語への対応
- セキュリティ設定実験
 - Metadata自動ダウンロード (実施済み)
 - Metadataの署名と検証
 - SP、IdP間のTLS通信等 (UPKI内で実施予定)
- ツール利用実験
 - ArpViewerのインストールと利用