
大学間認証連携とその未来

中村 素典

国立情報学研究所

2009/5/22

最先端学術情報基盤 (Cyber Science Infrastructure :CSI)

人材育成及び推進体制の整備
(推進組織・人材確保等)

バーチャル研究組織 / ライブ
コラボレーションの育成・支援

学術コンテンツの確保・発信システム

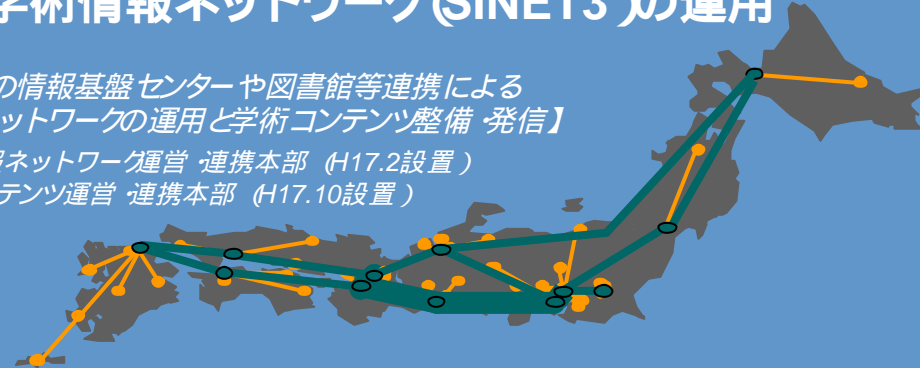
コンピュータ資源を結ぶグリッドの実用展開

大学・研究機関のための認証システムの開発 (UPKI)

学術情報ネットワーク (SINET3) の運用

【NII大学の情報基盤センターや図書館等連携による
学術情報ネットワークの運用と学術コンテンツ整備・発信】

- ・学術情報ネットワーク運営・連携本部 (H17.2設置)
- ・学術コンテンツ運営・連携本部 (H17.10設置)

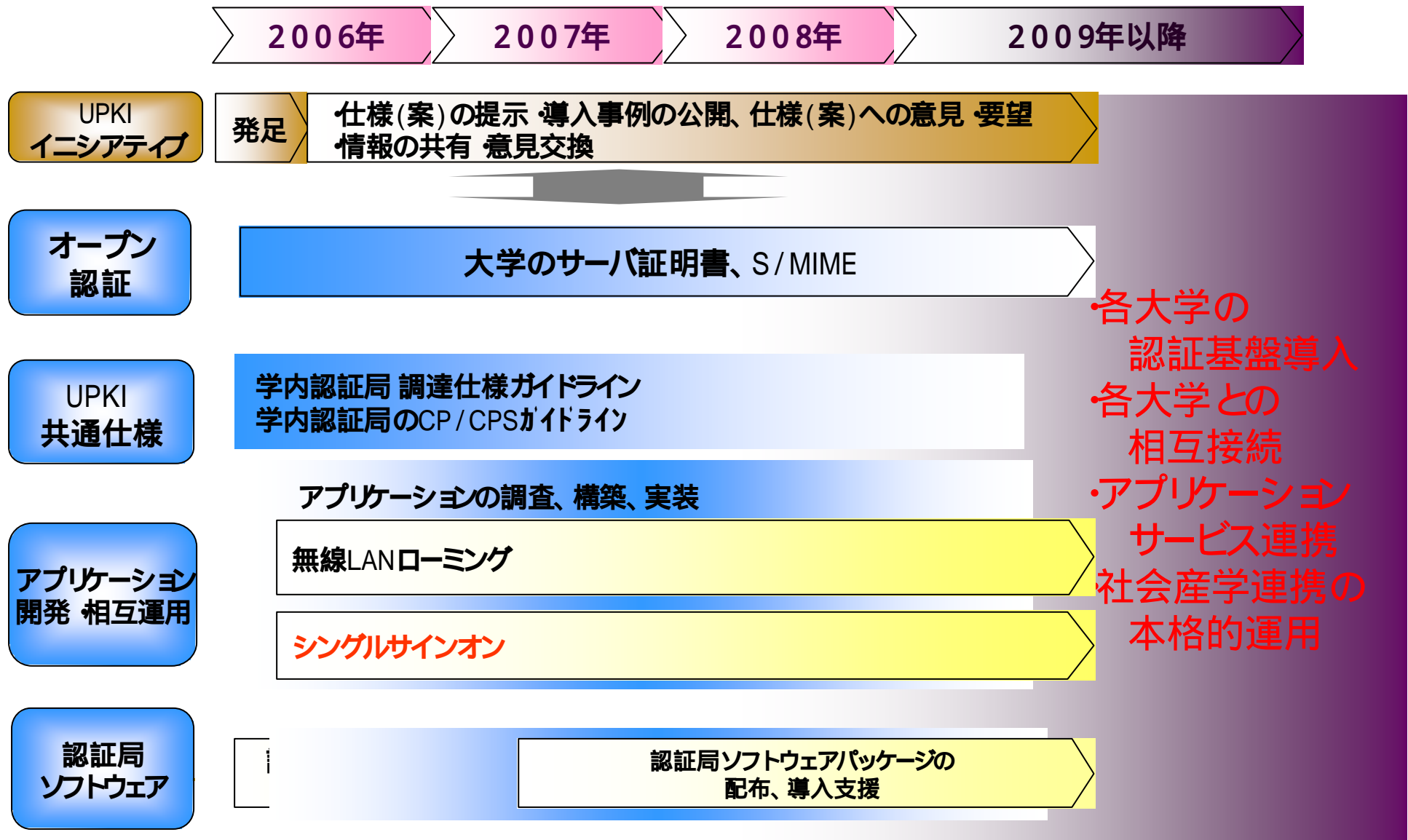


大学・研究機関の研究リソース整備・研究成果等の発信

産業・社会貢献

国際貢献・連携

UPKI構築の全体スケジュール



UPKIの2009年度の活動内容

- 学術認証フェデレーションの構築
 - Shibboleth/SAMLを利用したシングルサインオン技術の活用 (Pアドレスベース認証?から個人認証へ)
 - オープンドメイン証明書自動発行検証プロジェクト
 - これまでのサーバ証明書発行を引き継ぐとともにより効率的なシステムの構築を目指す
 - 無線LANローミング技術の展開
 - eduroam
-

Shibbolethの特徴

(1)属性の分散管理 = Federation

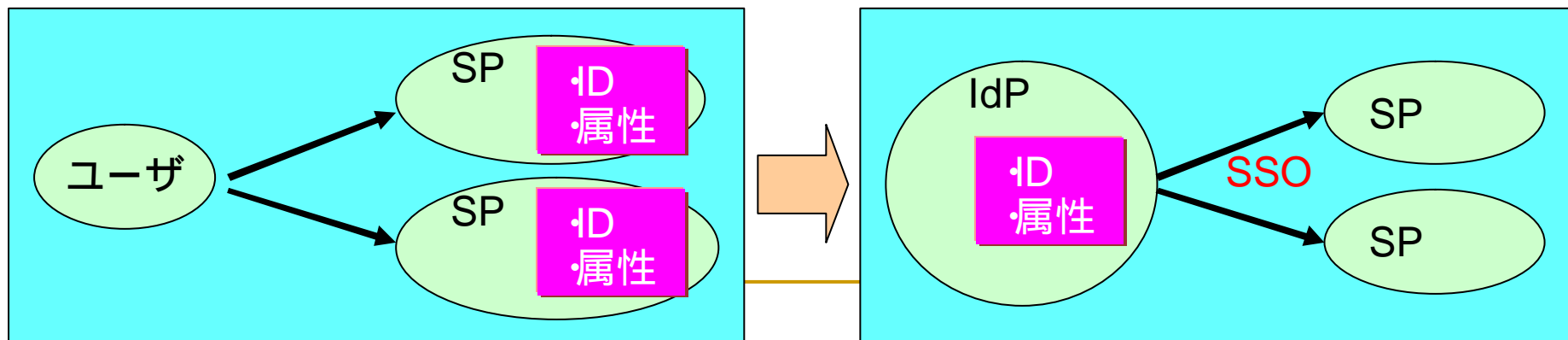
- IdP (大学)がIDと属性を管理して、SPがこれを利用

(2)プライバシー保護

- ユーザの識別情報をIdP外部に公開しない仕組み
- ユーザは各SPに対する各属性の公開を制御可能

(3)SSO

- Webサービスのシングルサインオン



昨年度の成果 :電子ジャーナルの認証

- 学術フェデレーション構築に向けた電子ジャーナル利用の認証 (シングルサインオンの実現)は,昨年度の実証実験で実現 (CiNii, Elsevier社)
- 平成21年度は,対象となるサービス (電子ジャーナル等)を拡大する

フェデレーション構築は各国で進められており
方式の統一でサービスの拡大が容易

機関単位の Pアドレスに基づく契約をベースに
フェデレーション経由の認証を展開

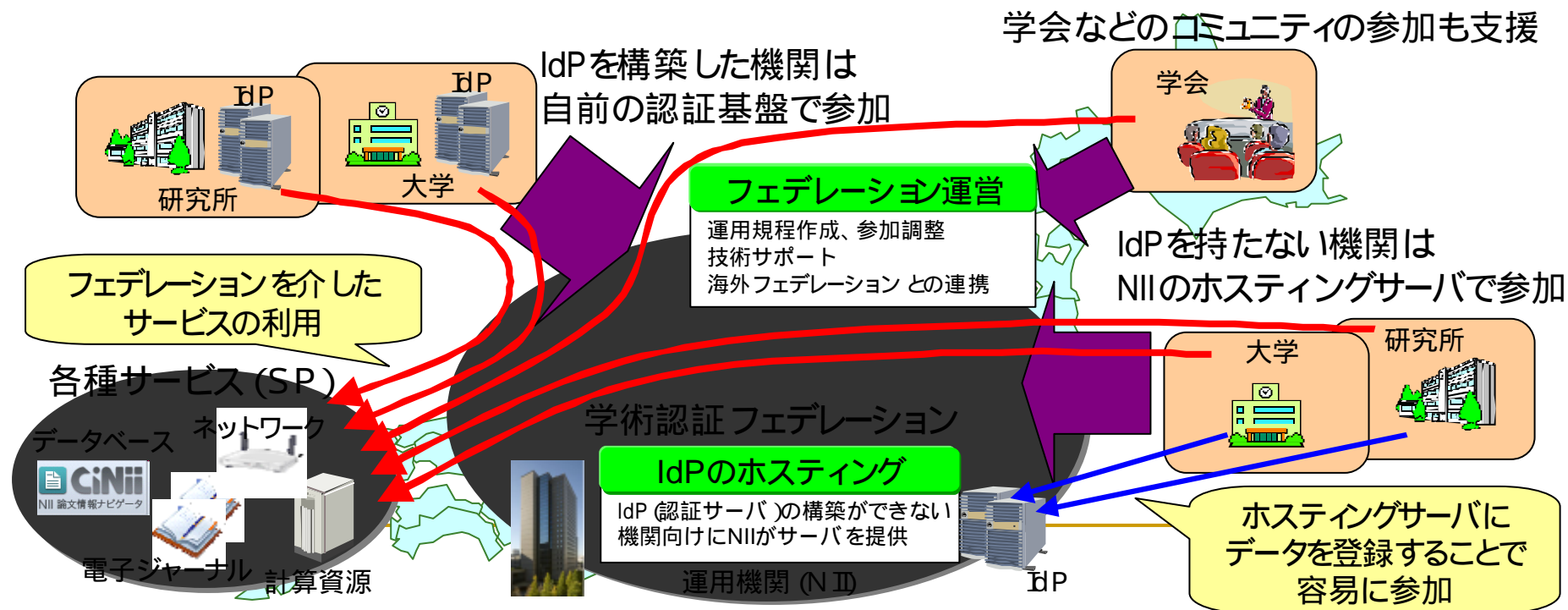
The composite image illustrates the authentication process for electronic journals. It features three main components:

- ScienceDirect Login Options:** A screenshot of the ScienceDirect website showing the 'Login via Athens or Your Institution' section. A red circle highlights the dropdown menu for 'Japanese Research and Education (UPKI-Fed)'. A yellow arrow labeled '認証' (Authentication) points from this menu towards the Shibboleth login page.
- Shibboleth Identity Provider Login:** A screenshot of the 'NII Single Sign On Powered by UPKI-Fed' login page. It includes fields for 'Username:' and 'Password:' and a 'Login' button. A yellow box labeled '所属機関のIdP' (Institution's IdP) is positioned below the login fields.
- CiNii Website:** A screenshot of the CiNii website showing the '新規登録' (New Registration) link circled in red. Below the CiNii logo, it states 'NII 論文情報ナビゲータ[サイニィ]' and '収録件数: 12216043件(2009/05/17 現在)'.

At the bottom center, a yellow box labeled 'Shibboleth対応サービス' (Shibboleth-compatible services) is present.

認証フェデレーション普及に向けて

- 大学全体のIdP構築には学内調整等の時間が必要
 - フェデレーションの早期拡大のため,調整がついた学部単位や一部のユーザグループでの参加も可能とする
- IdPの構築・運用の負担が大きい可能性
 - NIIでIdP用のホスティングサーバを用意
 - 参加希望の機関は,データのメンテナンスのみでも参加可能



フェデレーションの効果

- 学内基盤との連携によるシームレスな認証の実現
 - 少ないコスト負担でユーザ利便性が向上
 - ユーザ毎のカスタマイズが可能に
- 大学、国の枠を超えたサービスの展開
 - 大学間連携による教育 (単位互換制度等) の支援
 - サービス統合の促進 (提供コスト削減、マッシュアップ化)
- 研究コミュニティの形成と活性化
 - 横型連携フレームワークにより実現
 - 特定分野の研究者に対するサービス創出・提供
- 産業から学術へのアプローチを活性化
 - ユーザ管理・確保コストの削減
 - 学術に特化した効率的なサービス開発が可能

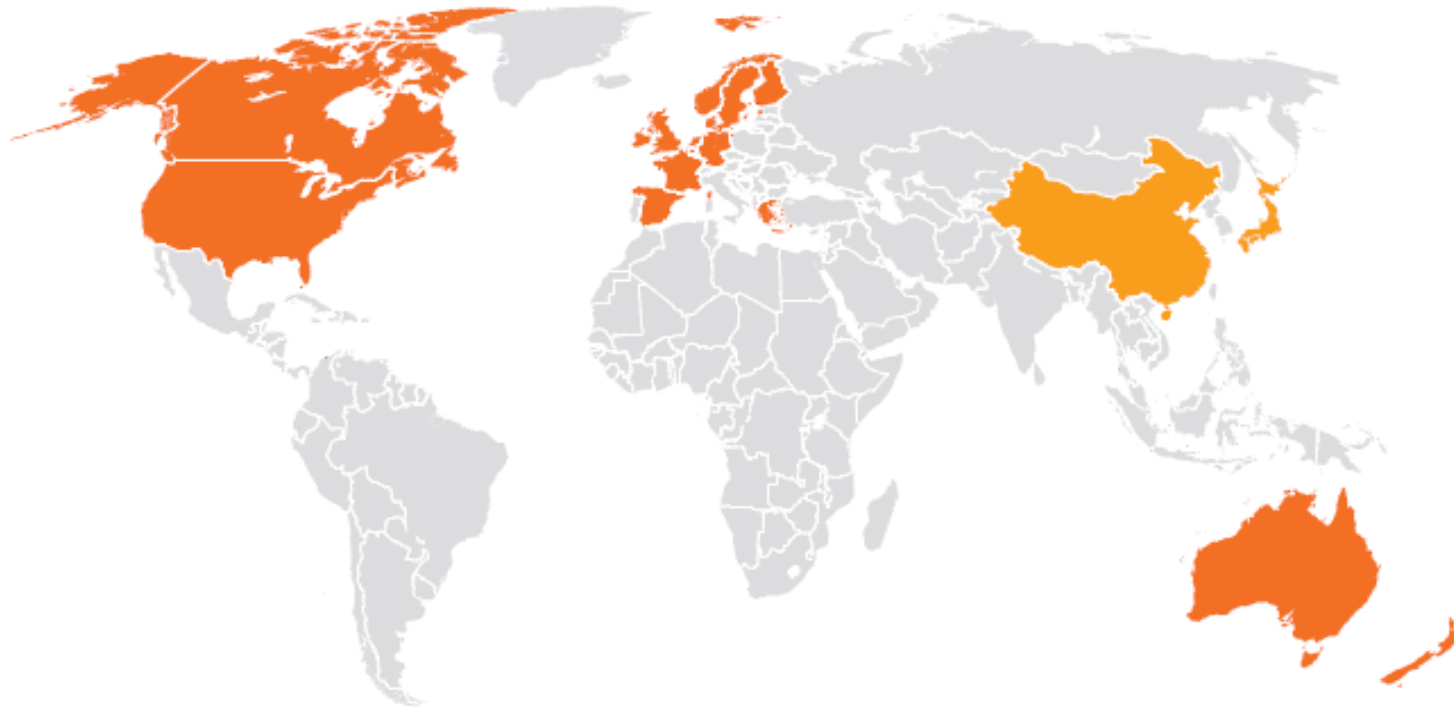
海外での状況

- 世界のIdP ;
 - 米国 : InCommon
 - 英国 : The UK Access Management Federation
 - スイス : SWITCHaai
 - オーストラリア : MAMS、AAF
 - フィンランド : HAKA
 - フランス : CRU
 - ノルウェー : FEIDE
 - デンマーク : WAYF
 - ドイツ : DFN-AAI
- 世界のSP ;
 - ScienceDirect、Ovid Technologies、JSTOR、ExLibris、Digitalbrain、Thomson Gale等
 - Blackboard、WebCT、Moodle、OLAT、WebAssign等
 - DSpace、uPortal、Napster、Sharepoint、Symplcity、TWiki、Zope+Plone、eAcademy等

(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

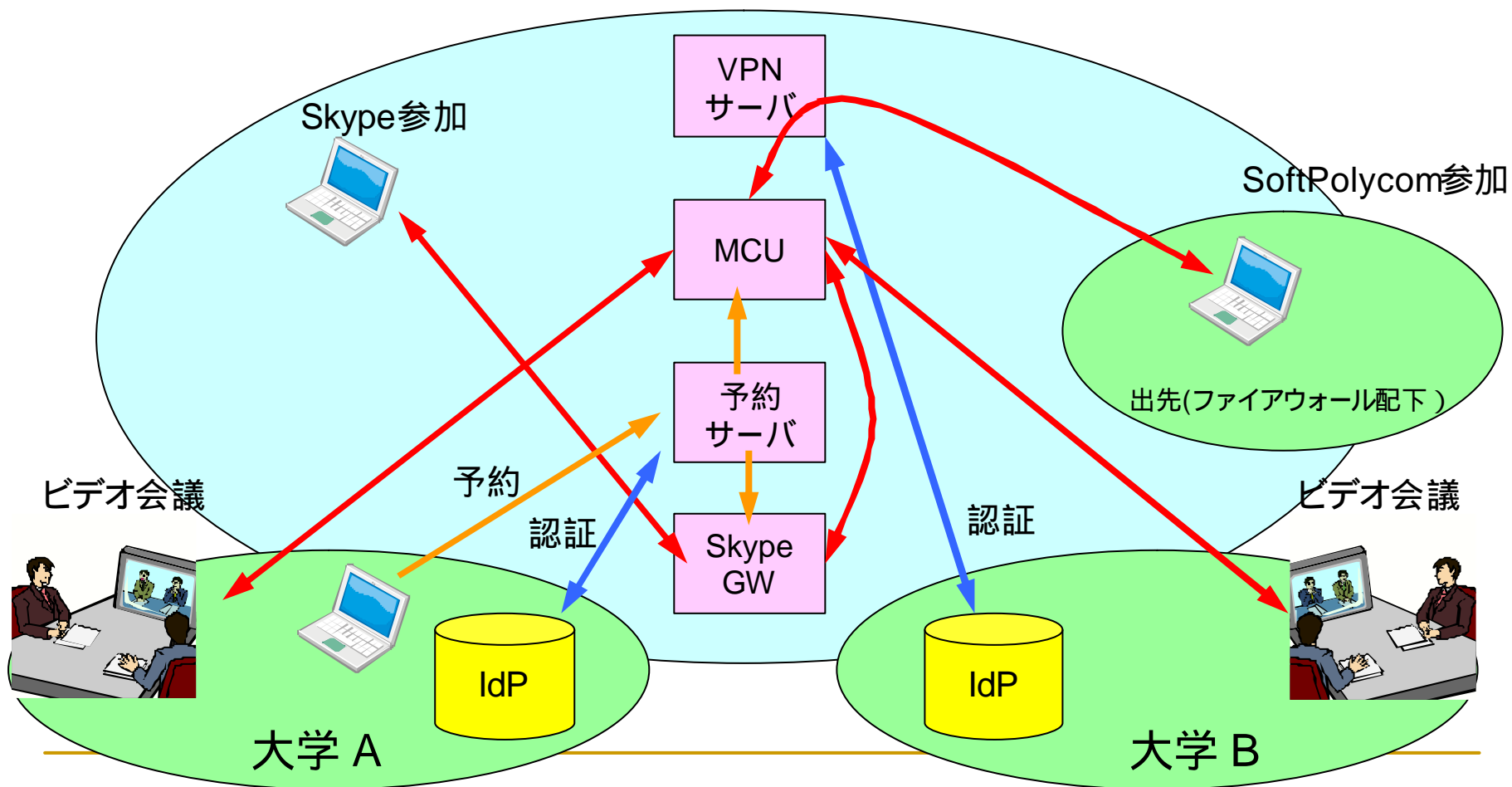
Inter-Federations

Federationの次は、Inter-Federations

- 米国では、InCommonとU.S. E-Authentication Identity Federationが連携したPilot Programを実施 (2006年12月)
 - スペイン、ドイツ、スウェーデンはフェデレーション間ブリッジを利用
 - REFEDS (Research and Education Federations):
 - https://refeds.terena.org/index.php/Main_Page
 - 米国、欧州の各フェデレーション同士で連携するための国際的検討 (2007年9月に第1回会合)
-

SP構築例 : ビデオ会議支援サービス

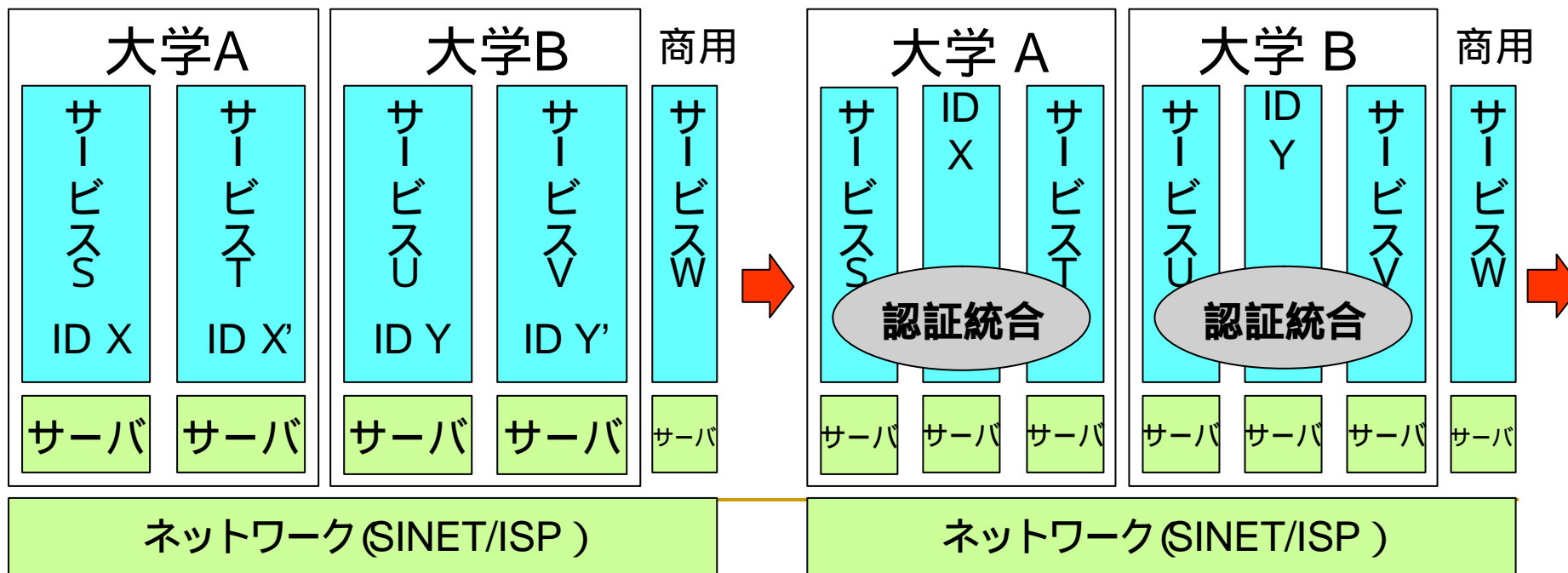
■ MCUの共同利用



[サービスアーキテクチャの変遷]

システム構築から学内認証統合へ

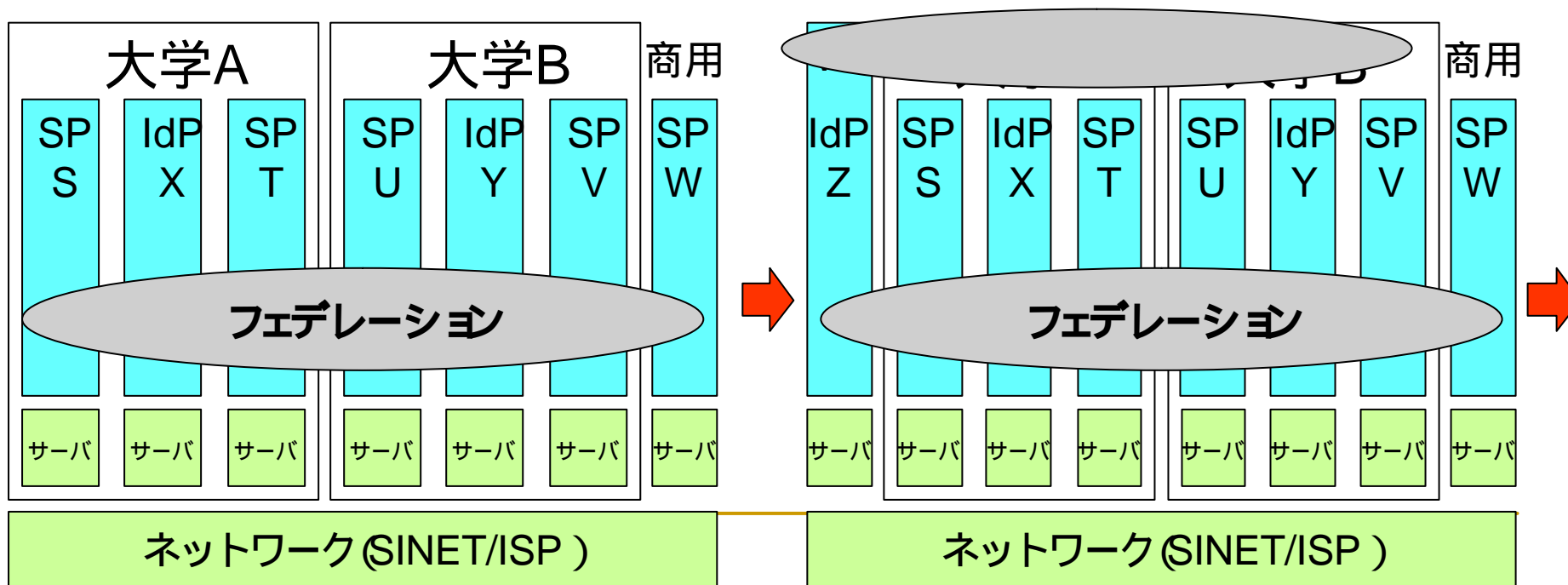
- システム、サービスの乱立
 - ダウンサイジングによる分散化
- ID統合によるシングルサインオン



[サービスアーキテクチャの変遷]

フェデレーション構築、VO支援

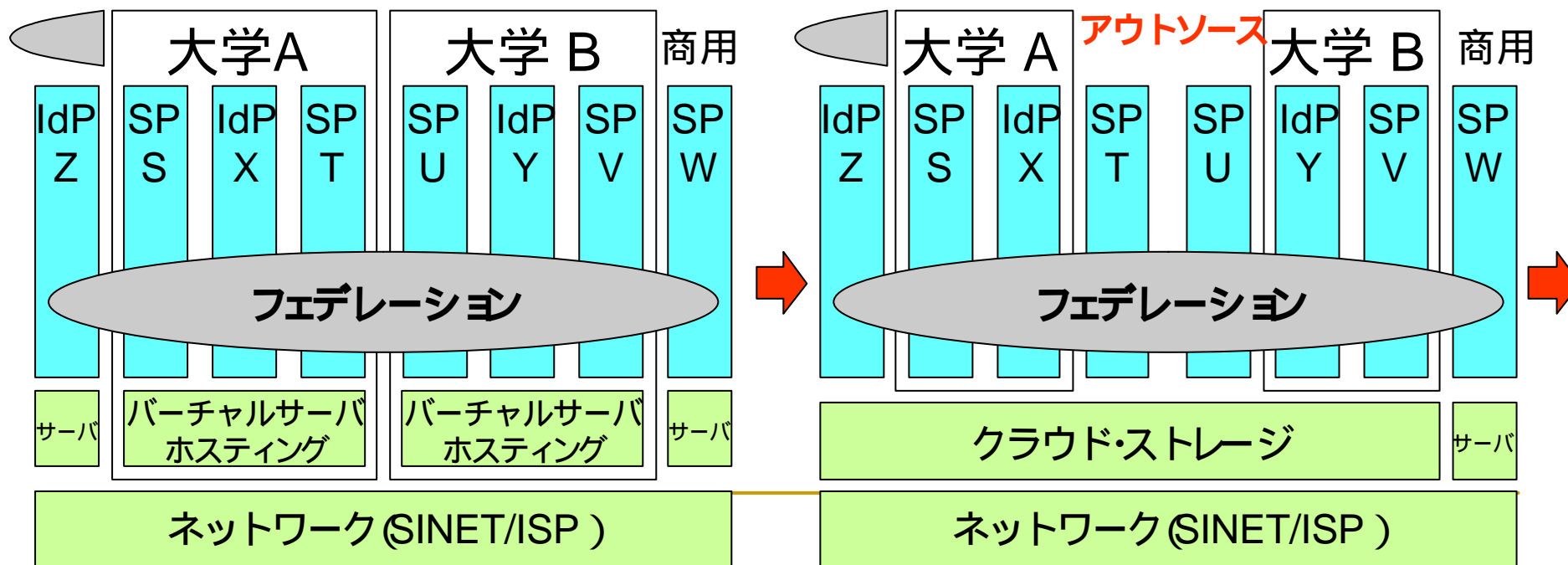
- 外部サービスとのID共通化
- コミュニティ、VO (Virtual Organization)のサポート
- サービス共用、大学間連携支援



[サービスアーキテクチャの変遷]

プラットフォーム共通化、クラウドの活用

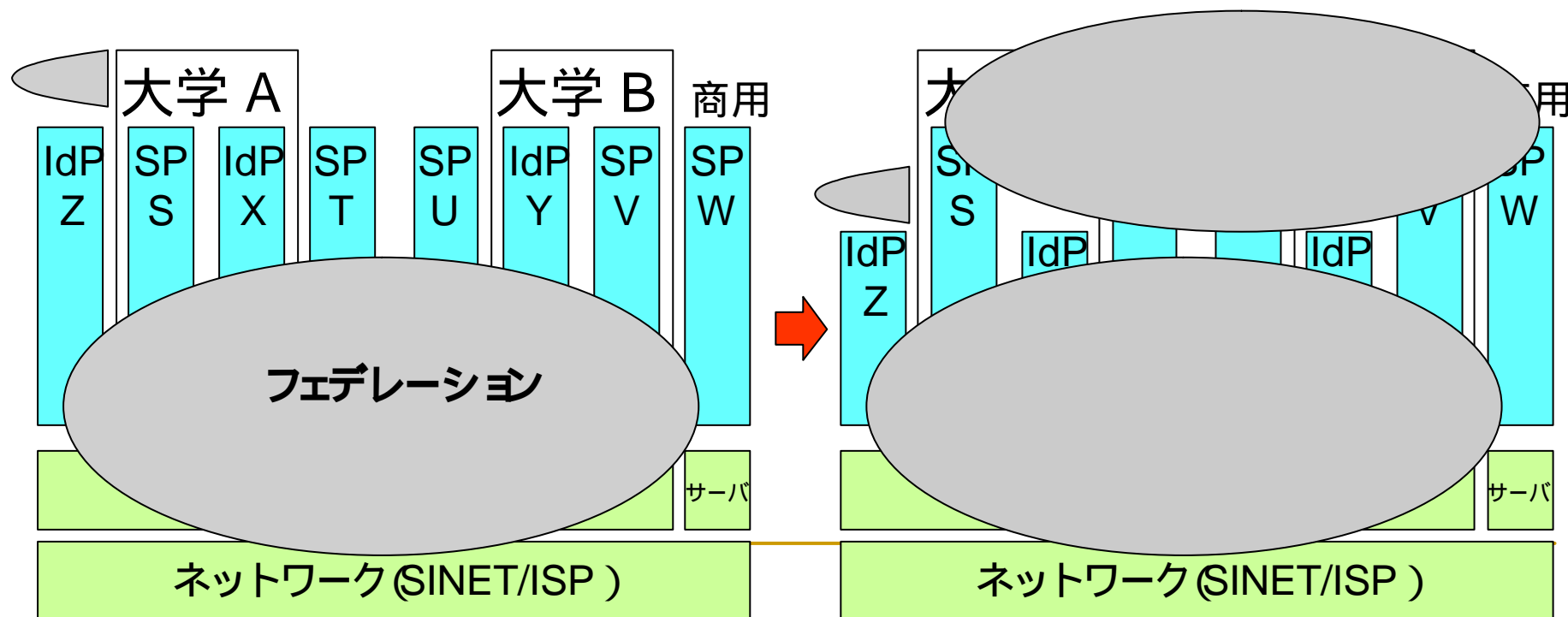
- プラットフォーム共通化による効率化、コスト削減
 - バーチャルホスト、クラウド技術の導入
- アウトソーシング、外部サービスの参入



[サービスアーキテクチャの変遷]

マッシュアップ

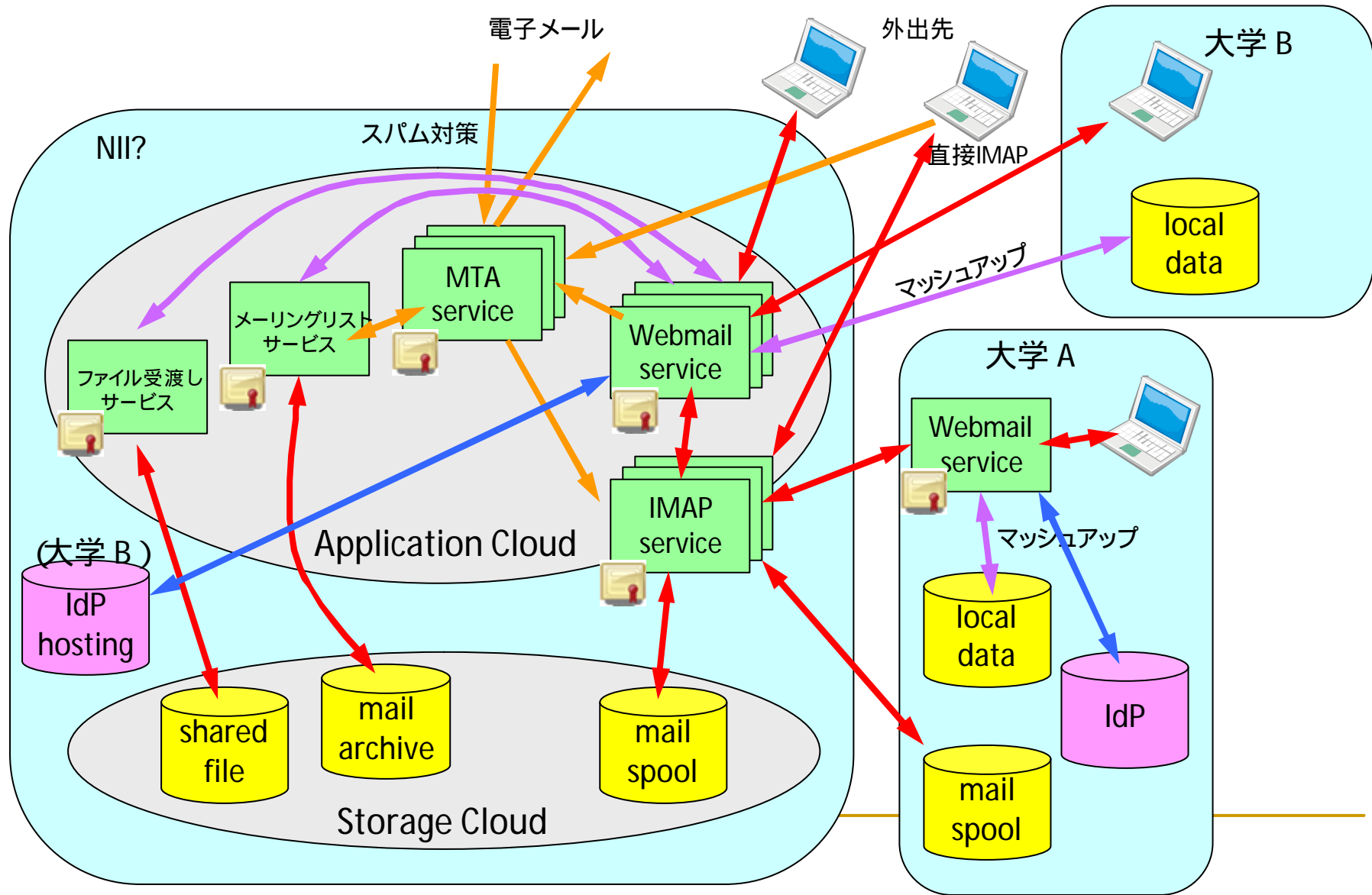
- クラウド、ストレージ、ネットワーク (VPN等) もSP化
- マッシュアップによるSP間の密な連携の実現
- サービス多様化、連携によるユーザ利便性の向上



大学におけるメールサービスの危機

- 電子メールは必要不可欠な情報通信基盤
 - 運用のための予算、人材が厳しくなっている
 - 際限のないスパム対策
 - より良いシステムへの要望
- 学術向け無料サービスが出てきたけれど...
 - データを預けてしまうことへの危惧
 - 運用主体が海外企業であることの懸念
 - 中身がブラックボックスで手が出せない
 - きめ細かなユーザサポートは期待できるのか
 - サービスの継続性への保証はあるのか

クラウド上での電子メールサービス？



認証フェデレーションとクラウド環境

- グリッド、ストレージ等が整備されつつある
- 計算機資源の集約、サービス統合によるコスト削減への要望
- 認証フェデレーションはクラウド環境の構築と活用を進める上でも重要な役割を持つ
 - より高度なサービスへの展開
- 課題
 - どこが整備・運用するのか
 - 保守性の低下はないのか
 - 特定プロバイダへの依存を避けたい

まとめ

- 学術連携 (大学間、産学) に向けての認証フェデレーションの構築
 - Shibbolethの利用で海外との連携も容易に
- サービス統合によるコスト削減
 - 格差是正効果への期待
- 新規サービスの構築・参入コストの抑制
 - 自分専用カスタマイズドサービスとか
- コミュニティの形成支援
 - 特定コミュニティ向けサービスの創出
- アウトソース、クラウドの活用促進効果への期待

