



Shibbolethを用いた フェデレーション構築計画

国立情報学研究所
学術情報ネットワーク研究開発センター
特任准教授
片岡 俊幸

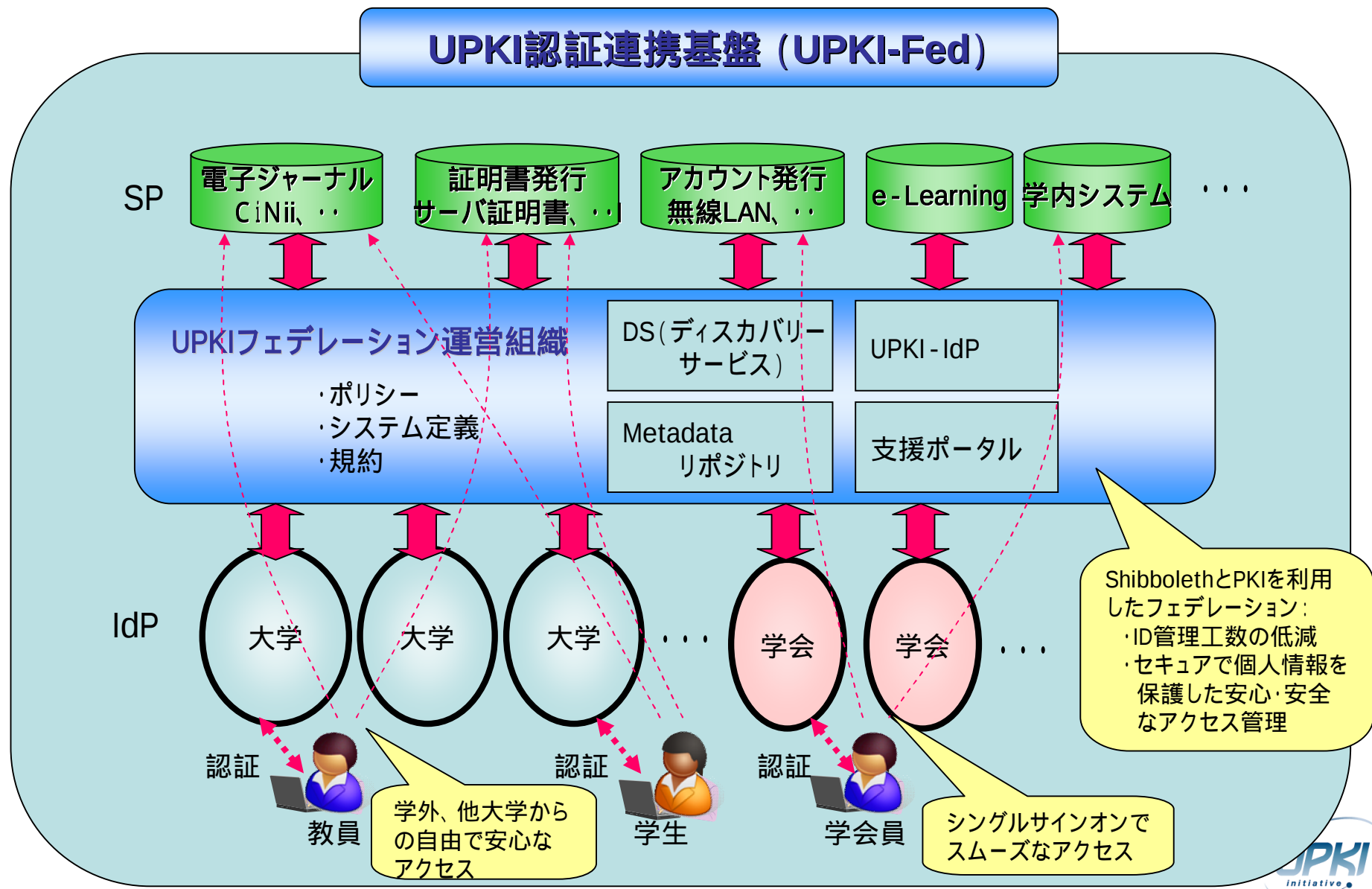


1 . UPKI認証連携基盤 (UPKI - Fed)

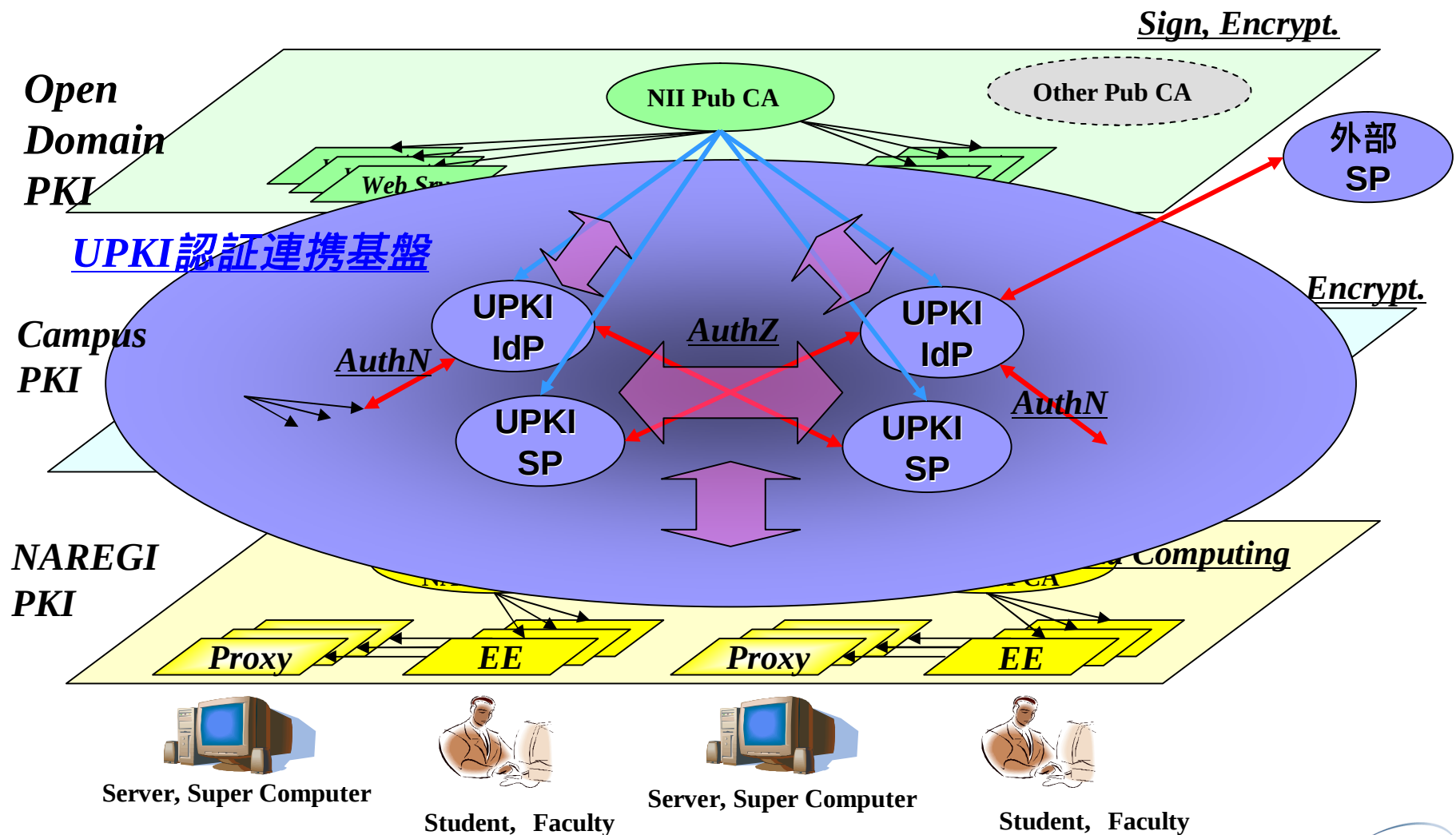
2 . 実証実験

3 . 今後の方針

UPKI認証連携基盤



UPKIの3層構造におけるUPKI認証連携基盤



Shibboleth概要



- 米国EDUCAUSE / Internet2にて2000年に発足したプロジェクト
- SAML、eduPerson等の標準仕様を利用した、認可のための属性交換を行う標準仕様とオープンソフト
- 最新はShibboleth V2.1
- 米国、欧州でShibbolethのFederationが運用、拡大

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

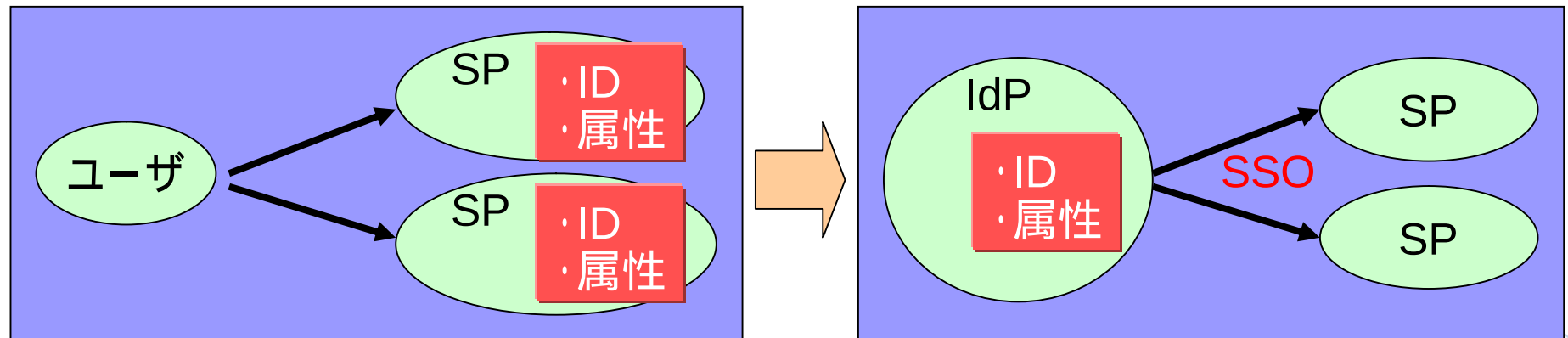
(2) プライバシ保護

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



Federationについて

- あるルール(ポリシー)のもとで属性交換の相互運用に合意した組織(IdP、SP)の集合
- Federation運営組織が、ポリシー策定や認証局の認定、DS、メタデータDLサイトの提供を行う
- 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
 - ノルウェイ: 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、Symplicity、TWiki、Zope+Plone、eAcademy等

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):

<http://wiki.rediris.es/tf-emc2/index.php/Federations>

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な検討。

第一回:2007年9月

第二回:2008年6月

第三回:2008年12月

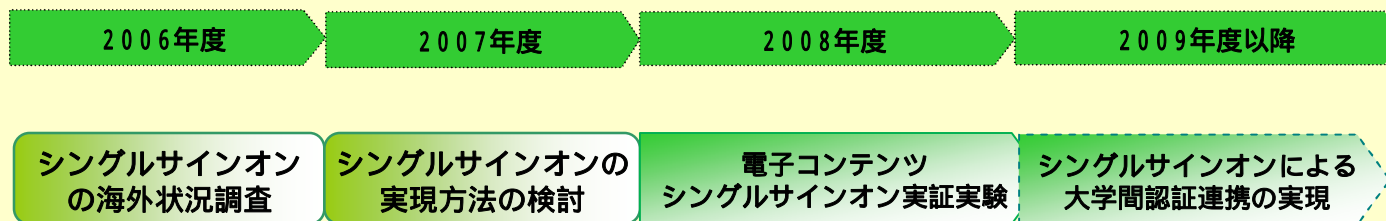


1 . UPKI認証連携基盤 (UPKI - Fed)

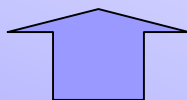
2 . 実証実験

3 . 今後の方針

シングルサインオン実証実験について



「各大学の利用者が、安全・安心かつ有効に
学術サービスを利用するための基盤の実証と検討を行う。」



- ・ 各大学間を実際に接続して、ユーザ利便性向上、管理工数削減等、UPKI認証連携基盤が各大学の現実の状況に適合すること、効果があること、運用可能であること等を実証・評価する。
- ・ 今後のUPKI認証連携基盤を実現、運用していくための、アーキテクチャ、運用ポリシー等を検討・策定する。

UPKI認証連携基盤の利便性

実証実験で、様々な利便性を検証して、枠組みの検討・定義を行う。

シングルサインオン

学術サービスの連携を促進
スムーズな学術サービス利用

簡単なID管理

個人情報保護

ユーザ中心の考え方
漏えいリスクの低減
利用者への権限移譲
安心なサービス利用

信頼基盤 (フェデレーション)

管理工数削減

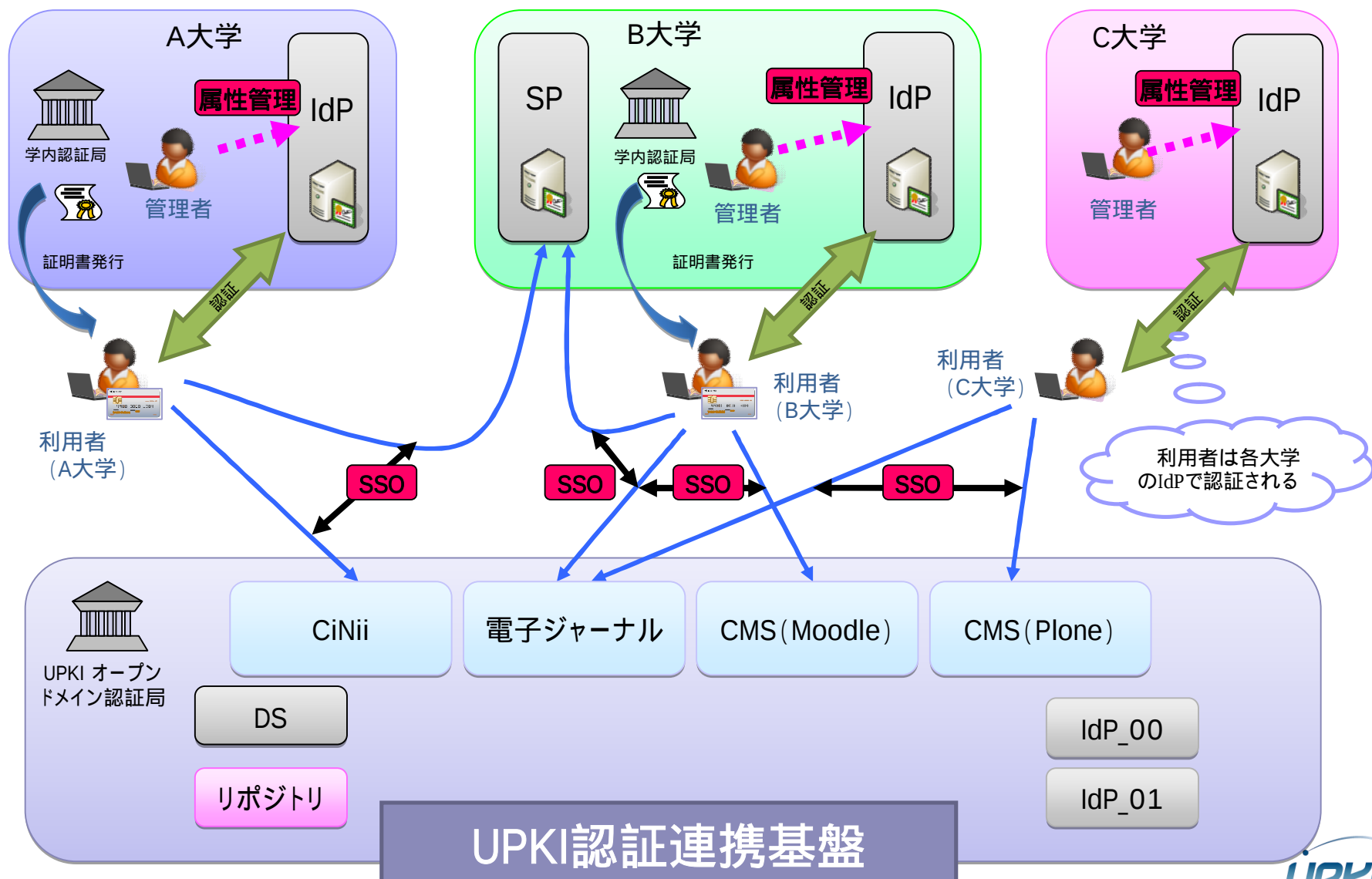
学内のサービス連携を促進
学内のID管理統合
インシデント対策工数の低減

疎な信頼連携

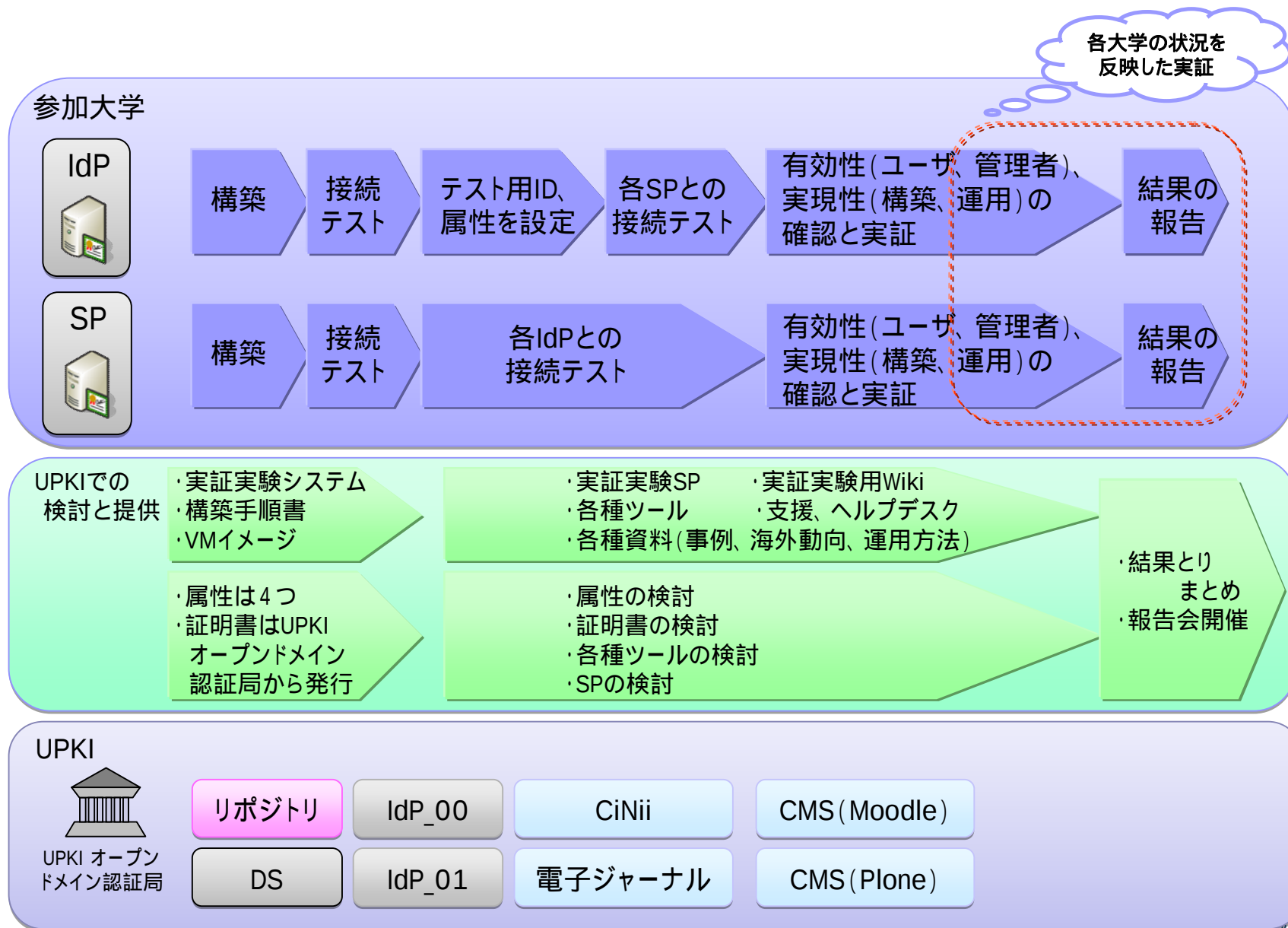
学外での利用 (リモートアクセス)

いつでも、どこでも
学術サービスにアクセス可能
構築費の低減
オープンソース

実証実験の概要

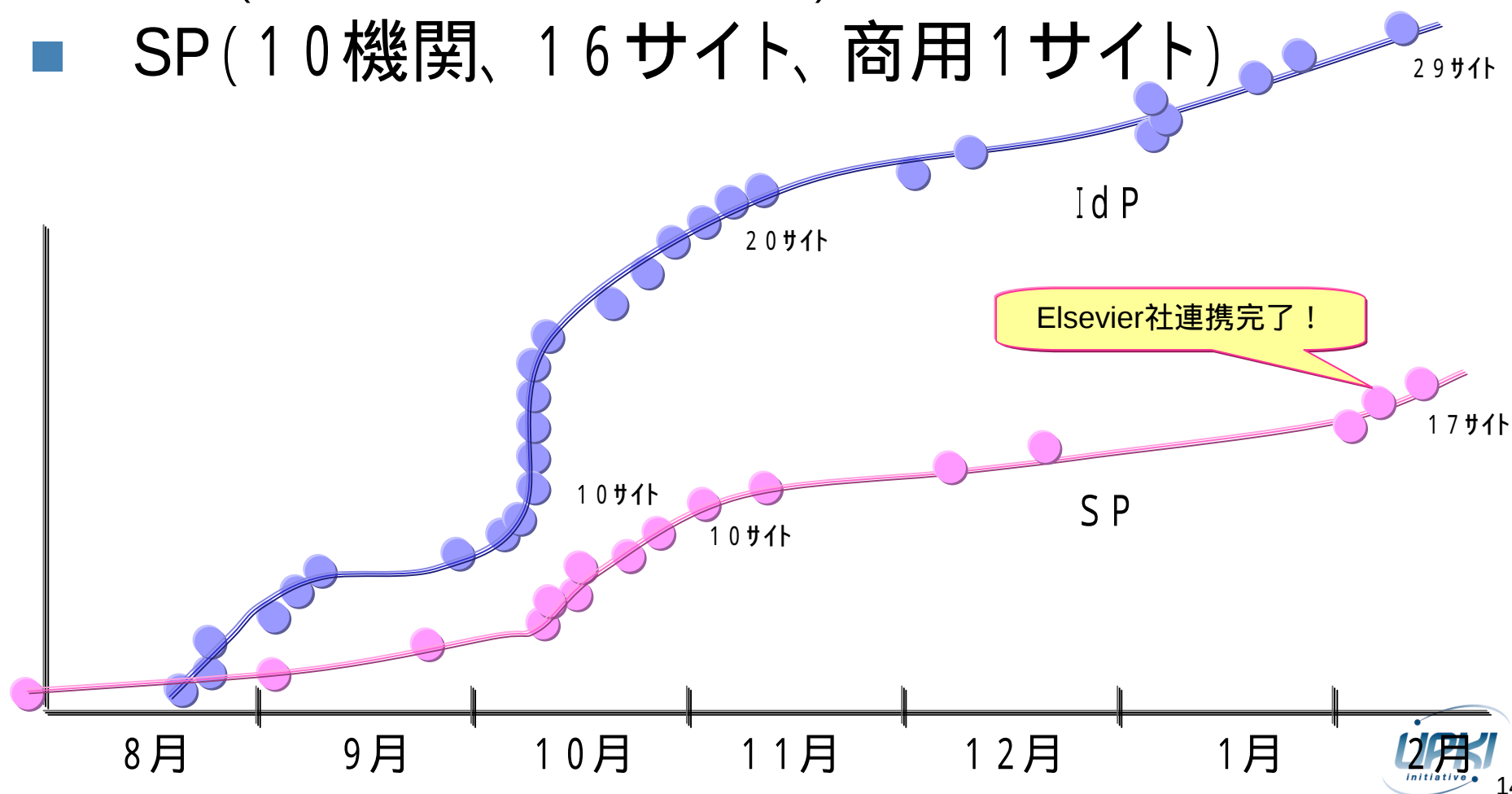


実証実験のスケジュール



実証実験の参加機関

- 参加機関(27機関)
- IdP(20機関、29サイト)
- SP(10機関、16サイト、商用1サイト)



参加機関名称	Id P	S P
北海道大学	○	-
東北大学	○ *	-
山形大学	-	-
福島大学	-	-
高エネルギー加速器研究機構	-	-
筑波大学	○ 2	(未公開) 2
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	○ 3 *	CiNiiテスト*

○ : 構築済み : 接続実験中
数字: 複数サバ構築 * : メタデータ自動更新設定済み

参加機関名称	Id P	S P
金沢大学	○	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 (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	○	(未公開)
大阪大学	○	(グリッド証明書発行)
愛媛大学	-	-
徳島大学	-	キャンパス間SNS (OpenPNE)
広島大学	○	-
山口大学	○ *	山口大学SSO実証実験 (Plone) *
九州大学	○	(未公開)
熊本大学	○	-
佐賀大学	○ *	(未公開) 2



実証実験

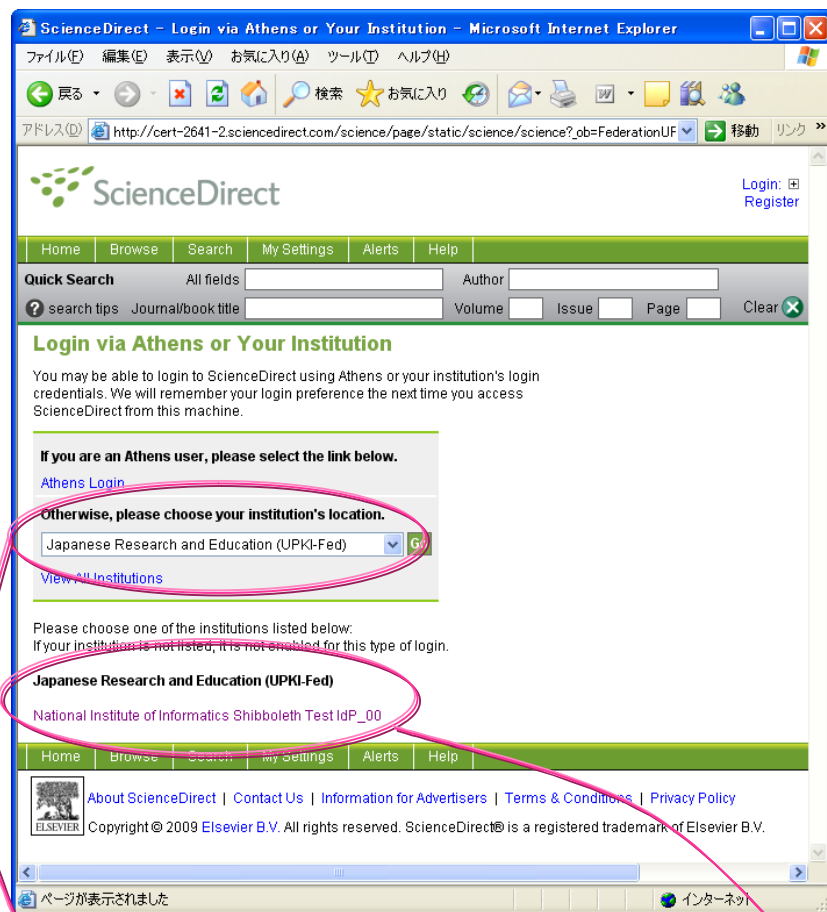
■ Shibboleth2.xを用いた連携実験

- 各大学で構築したIdPとSP、さらに商用SPを含むフェデレーションにおいて、学内外からのSSO連携を実現
- Shibboleth2.0プロトコルに加え、Shibboleth1.3プロトコルによる連携完了
- メタデータの自動ダウンロード、署名 & 検証実験
- 学内LDAP、および、学内ADとの連携実験
- 学内LDAP、ADから必要な属性(日本語属性を含む)を取得して、各SPに対応した送信を行う実験
- ツール(ArpViewer)の利用実験

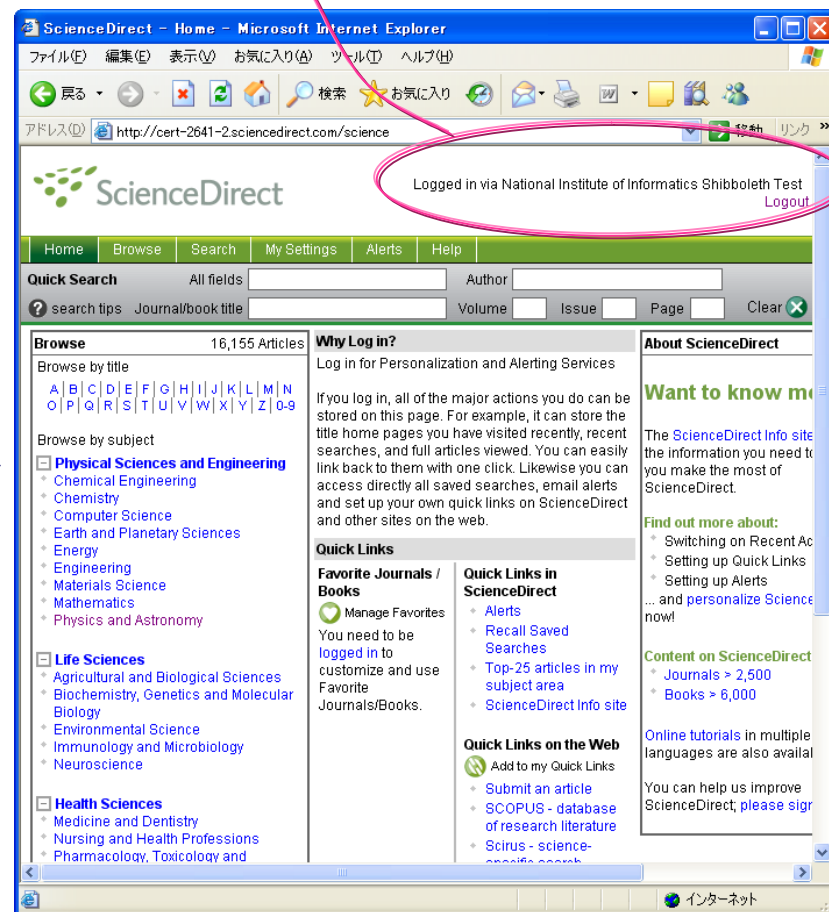
海外商用SPとの接続

- Elsevier社のScienceDirectと接続完了！
 - プロトコル = Shibboleth1.3:
UPKI-FedのプロトコルをShib2.0からShib2.0 / Shib1.3に変更
 - 証明書:
海外商用SPでは、UPKIサーバ証明書ではなく、
商用パブリック証明書を利用してもらう
 - メタデータへの署名:
信頼性確保のため、メタデータへの署名は必須
- 今後の接続予定(接続交渉を継続中)
 - 接続可能:
Refworks、Nature、OUP (Oxford University Press)、
LWW/Ovid、Springer、Thomson、EBSCO
 - 近い将来に接続可能:
CUP (Cambridge University Press)、Wiley - Blackwell、SAGE、
ProQuest、JSTOR、Serials Solutions、Taylor&Francis、APS
(American Physical Society)

Elsevier社との接続



ログイン



Otherwise, please choose your institution's location.

Japanese Research and Education (UPKI-Fed) Go

[View All Institutions](#)

Japanese Research and Education (UPKI-Fed)

National Institute of Informatics Shibboleth Test IdP_00



1 . UPKI認証連携基盤 (UPKI - Fed)

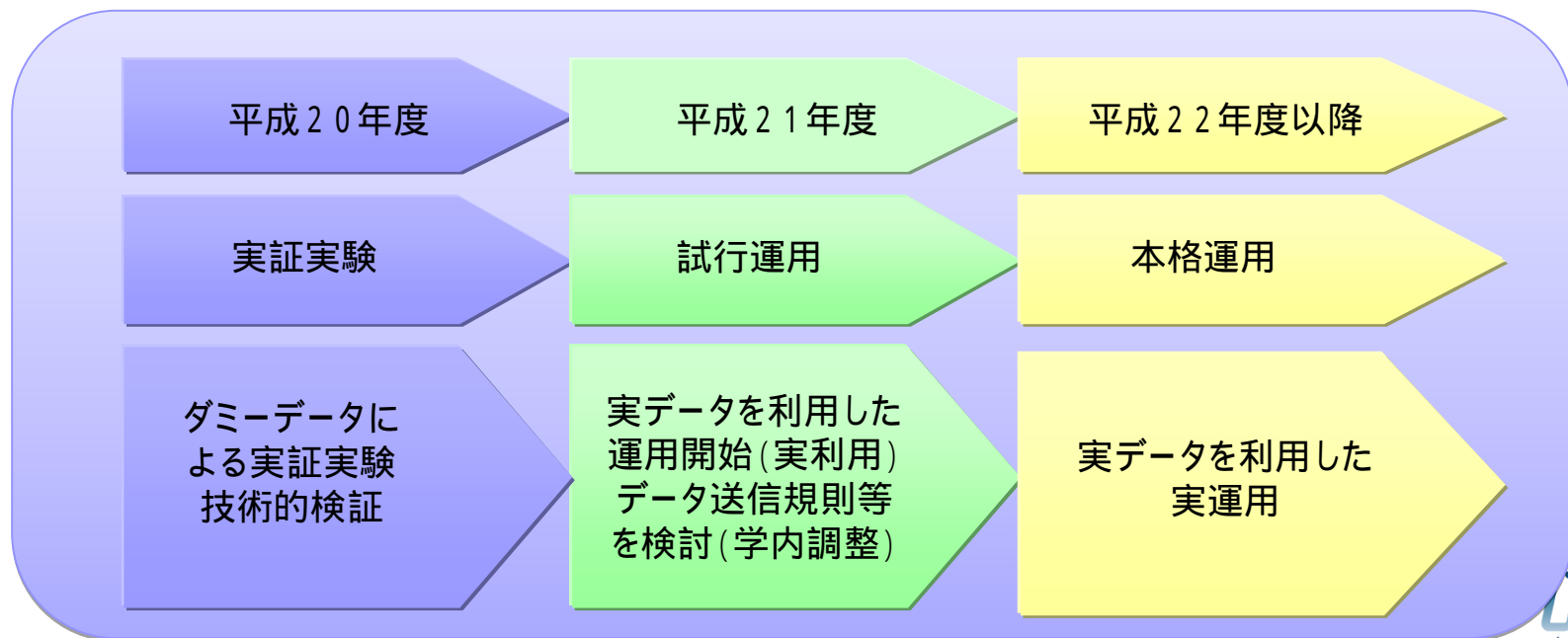
2 . 実証実験

3 . 今後の方針

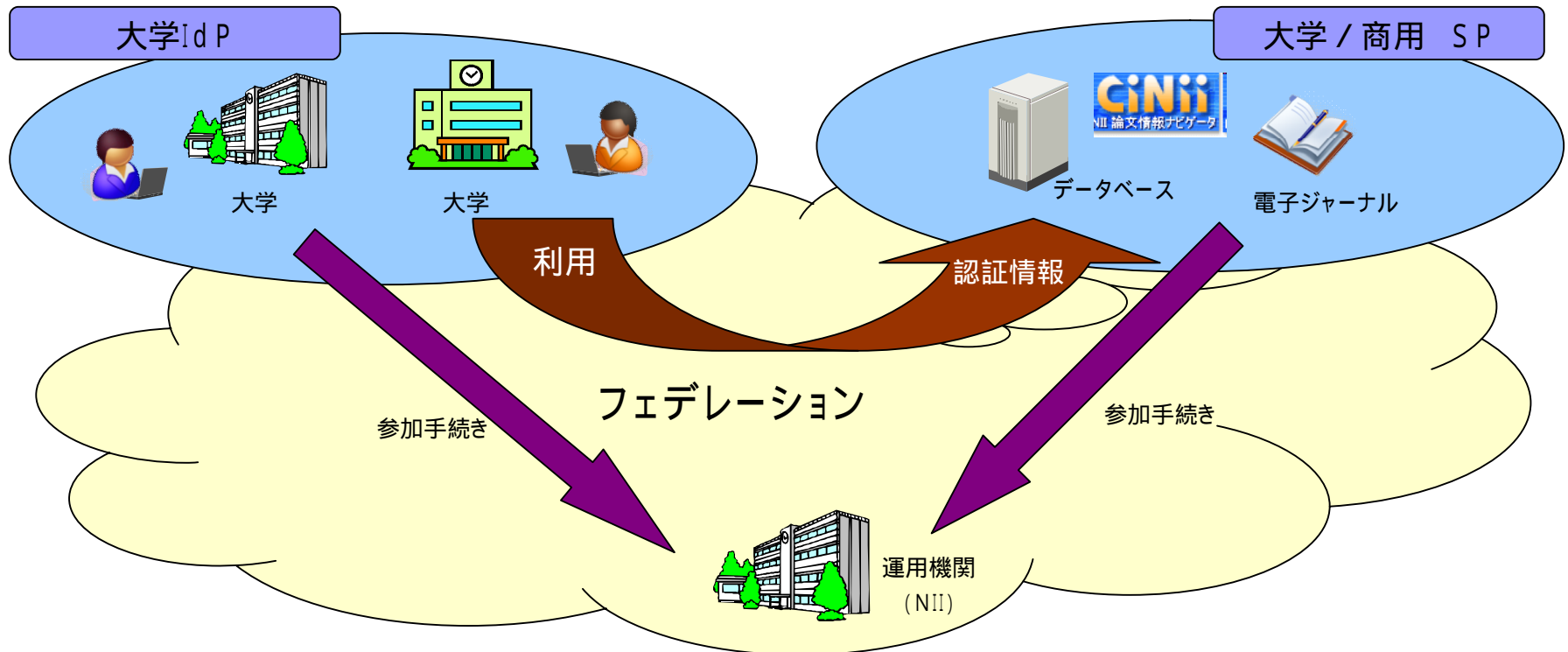
今後の方針

■ UPKI認証連携基盤プロジェクト

- 「シングルサインオン実証実験」は、平成21年3月末終了
- 新規に、「学術フェデレーション(UPKI-Fed)試行運用(仮称)」を平成21年4月からスタートする予定



学術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21年2月に連携済み)
- 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。

学術フェデレーションの構築スケジュール

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連携完了、他と交渉継続中) ■ 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

試行運用の準備状況

- UPKI - Fed運用規程(作成中)
 - 「UPKI認証フェデレーション試行運用実施要領」
 - 「UPKI認証フェデレーション試行運用システム定義(仮称)」
- 利用属性定義(上記、システム定義に含む)
 - eduPersonPrincipalName、O、OU等
 - 日本語対応の属性を新たに定義
 - 所属、所属ユニット、性、名、表示名
- 設定ファイルのサンプルを準備
 - IdP用設定ファイル、SP用設定ファイル



UPKI認証連携基盤に関する情報

- プロジェクトの情報発信ページ
UPKIイニシアティブ
URL: <https://upki-portal.nii.ac.jp/SSO/>
- 情報発信ML
E-Mail: upki-fed@nii.ac.jp
- お問い合わせ・ML参加申し込み先
国立情報学研究所 学術基盤推進部 基盤企画課
E-Mail: upki@nii.ac.jp