UPKI認証連携基盤の概要

国立情報学研究所
片岡　俊幸

1. Shibbolethについて
2. Federationとは？
3. 海外動向
4. 実証実験

1．Shibbolethについて

１－１．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
- 最新版はShibboleth V2.0
  （SAML2.0ベース、2008年3月リリース）
- 米国、欧州でShibbolethのFederationが運用、拡大

１－２．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

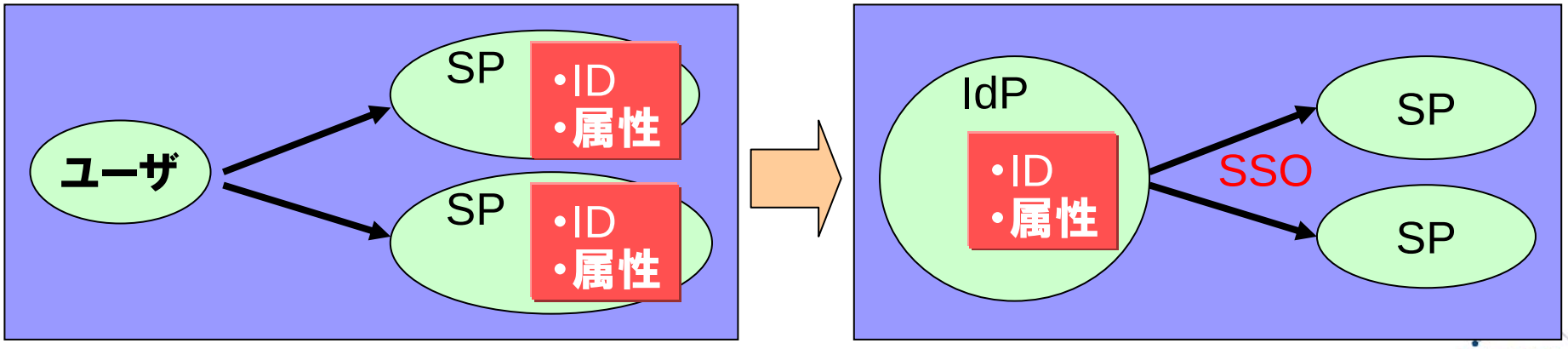
（２）SSO

　Webサービスのシングルサインオン

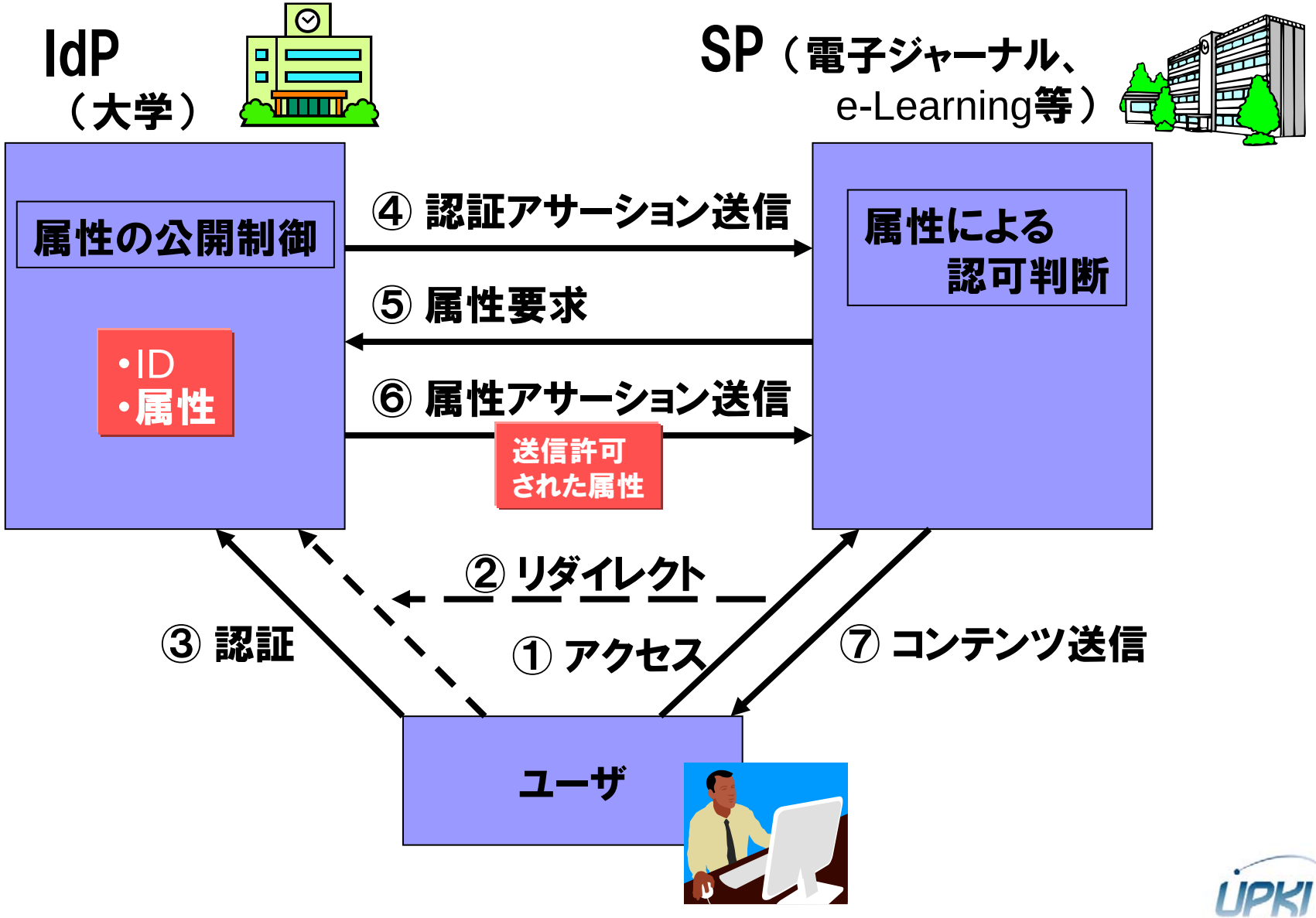
（３）プライバシ保護

　ユーザの識別情報をIdP外部に公開しない仕組み

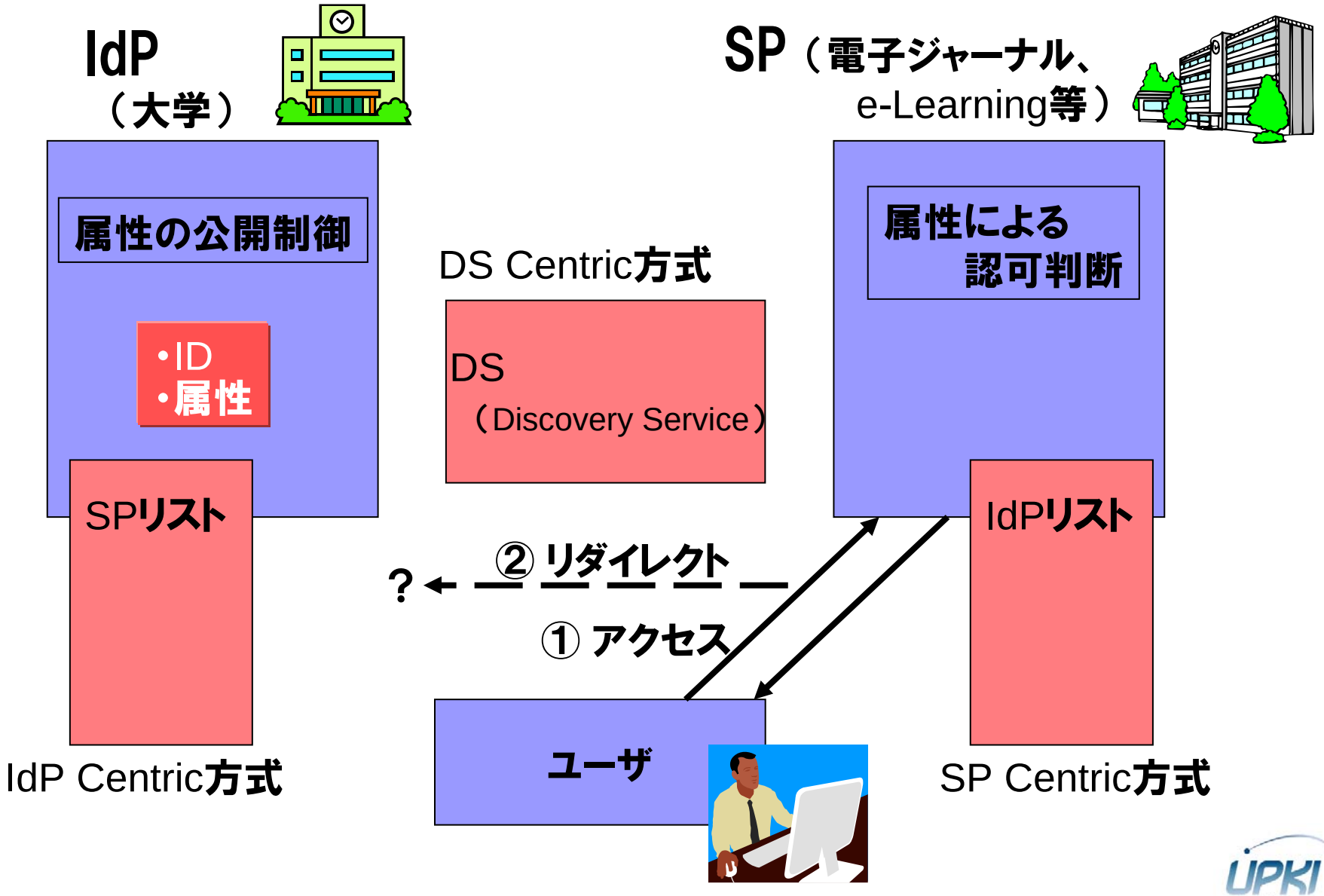
　ユーザは各SPに対する各属性の公開を制御可能



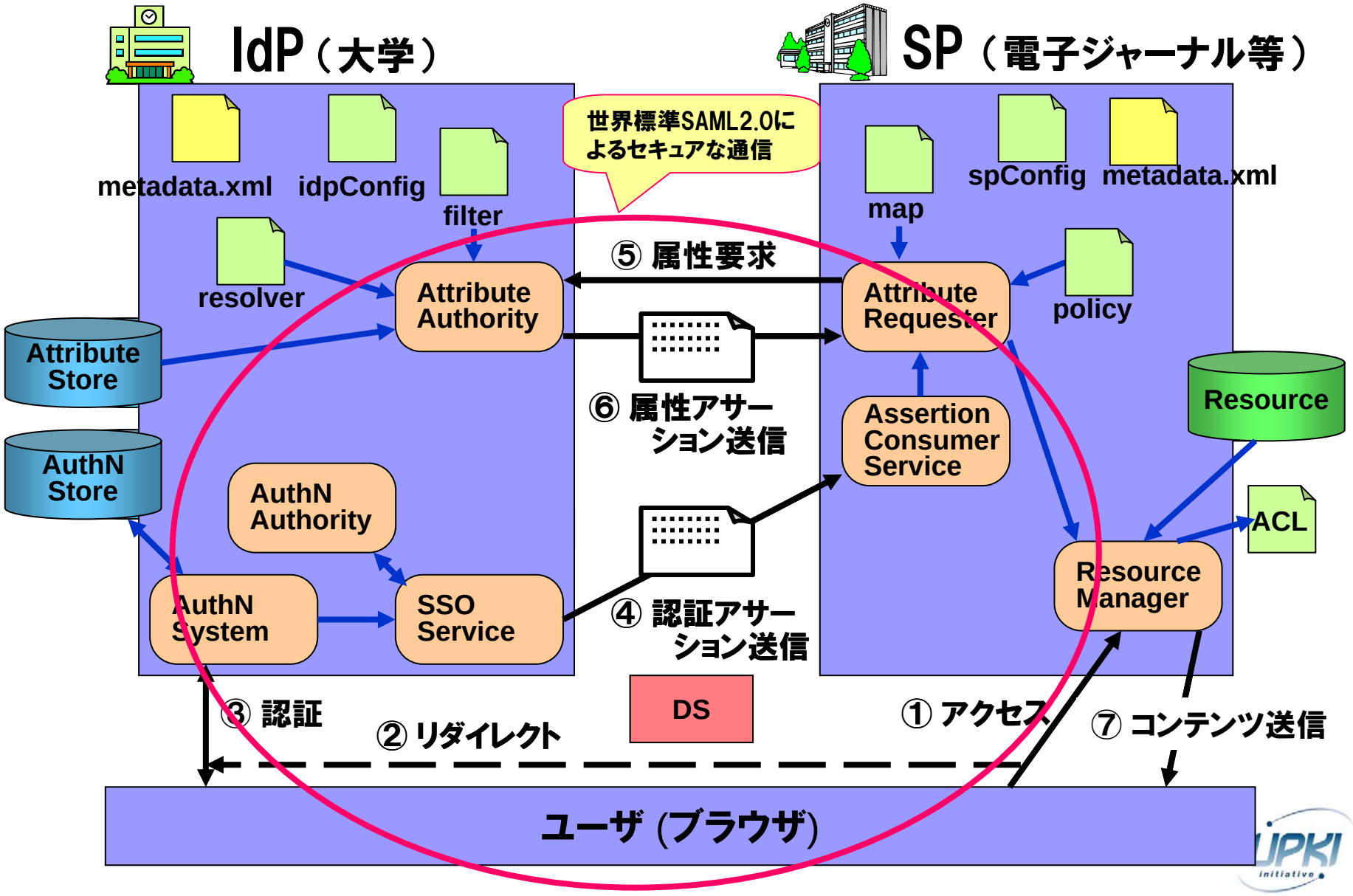
１－３．Shibbolethの基本動作



1－4. IdP Discovery

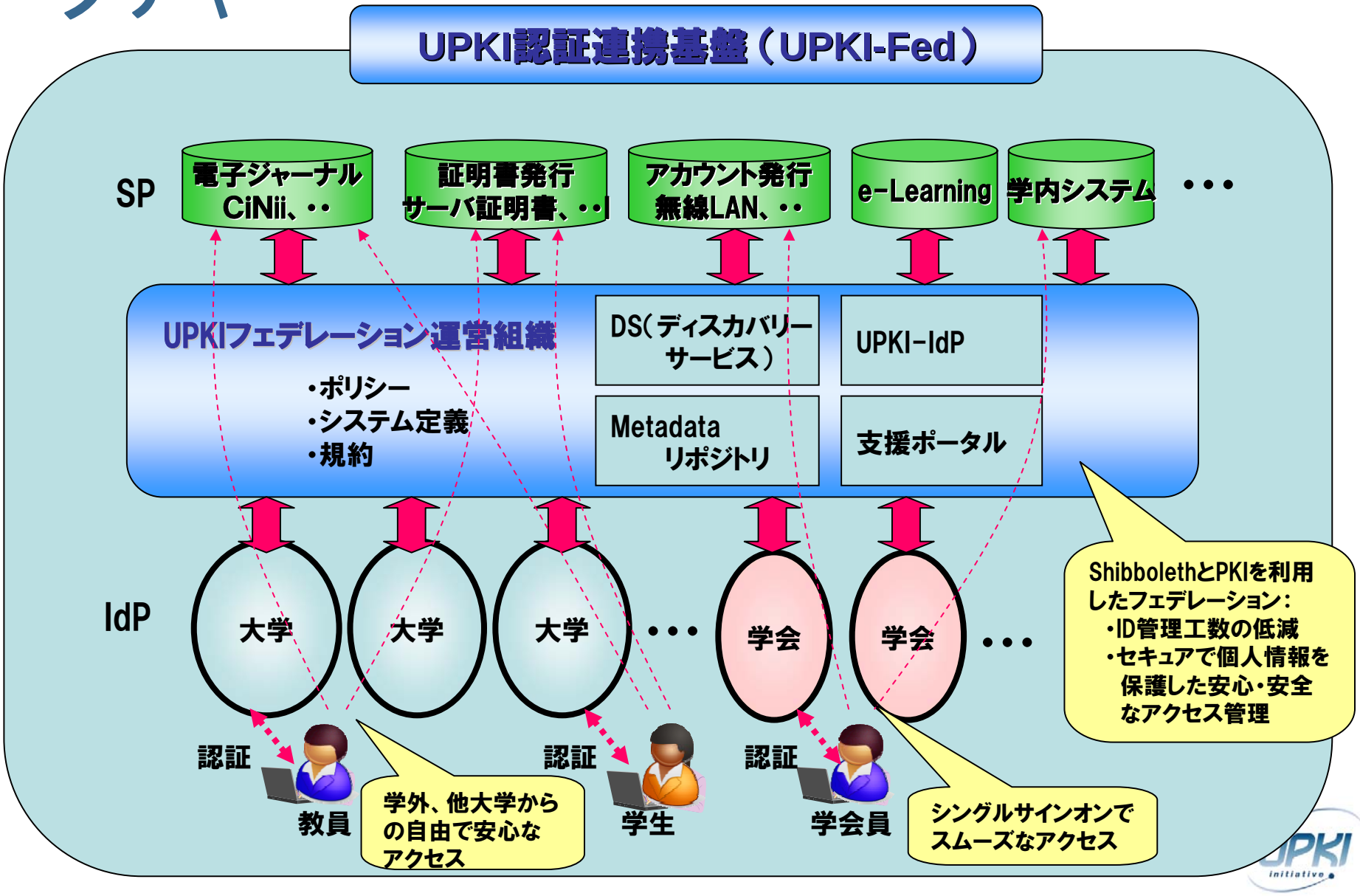


1－5. Shibbolethの動作



2. Federationとは？

2－1．UPKI認証連携基盤のアーキテクチャ



２－２. Federation概要

- 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

（参考）Shibbolethの対応アプリケーション

Information Providers:

- American Chemical Society
- ArtSTOR
- Atypon
- CSA
- Digitalbrain PLC
- EBSCO Publishing
- Elsevier ScienceDirect
- ExLibris
- JSTOR
- The Literary Encyclopedia
- NSDL
- OCLC
- Ovid Technologies Inc.
- Project MUSE
- Proquest Information and Learning
- Serials Solutions
- SCRAN
- Thomson Gale
- Thomson ISI/Scientific
- Useful Utilities - EZproxy

Learning Management Systems:

- Blackboard
- CLIX
- ILIAS
- Moodle
- OLAT
- Sakai
- WebAssign
- WebCT

Other Systems:

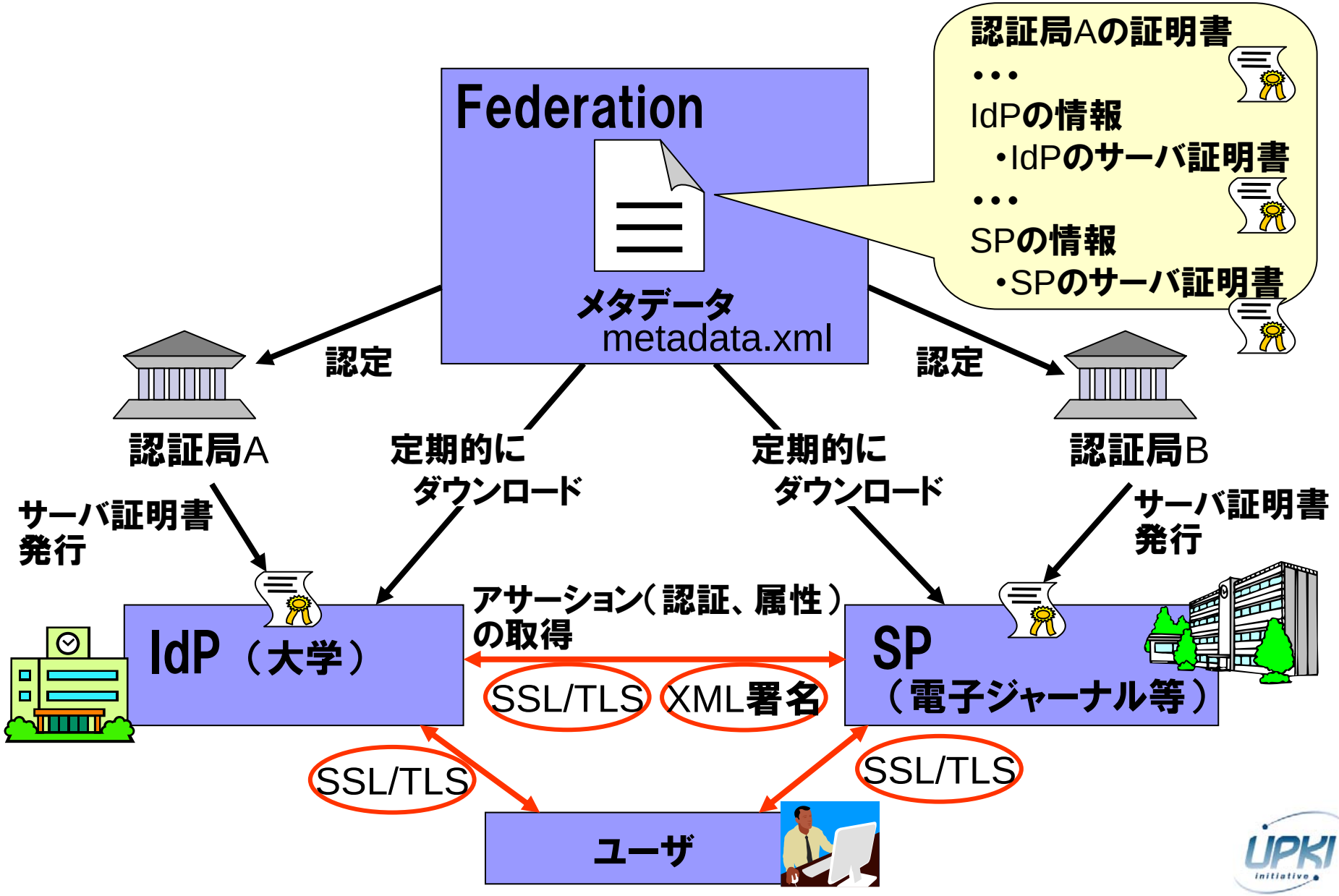
- Bodington.org
- Condor
- Confluence Wiki
- Darwin Streaming Server
- DSpace
- eAcademy
- Fedora
- GridSphere
- GridShib
- Higher Markets
- Horde
- Hupnet
- JISCmail
- LionShare
- Media Wiki
- MyProxy
- Napster
- PHEAA
- Sharepoint® from Microsoft
- SYMPA
- Symplicity
- TurnItIn
- TWiki
- uPOrtal
- Zope + Plone

＊ “https://wiki.internet2.edu/confluence/display/seas/Home”**より引用**

２－３．Federationの構成要素

- 運営組織：
  Federationを管理、運営する組織。
- ポリシー：
  Federationに加入するための条件、利用規約、信頼するCA、定義する属性等を定める。
- 認証局：
  Federationが信頼する認証局を定める。IdP、SPはこの信頼する認証局から発行されたサーバ証明書を利用する。
- 属性：
  IdP、SPが利用する共通の属性を定義。
  eduPerson（Internet2のMACE-Dirで規定）が標準。
- メタデータ：
  信頼する認証局の証明書やIdP,SPの情報。
- DS：
  IdPディスカバリ・サービス。

２－４．FederationとPKI



アニメーション
by AAF（Australian Access Federation）

Federated access management

3. 海外動向

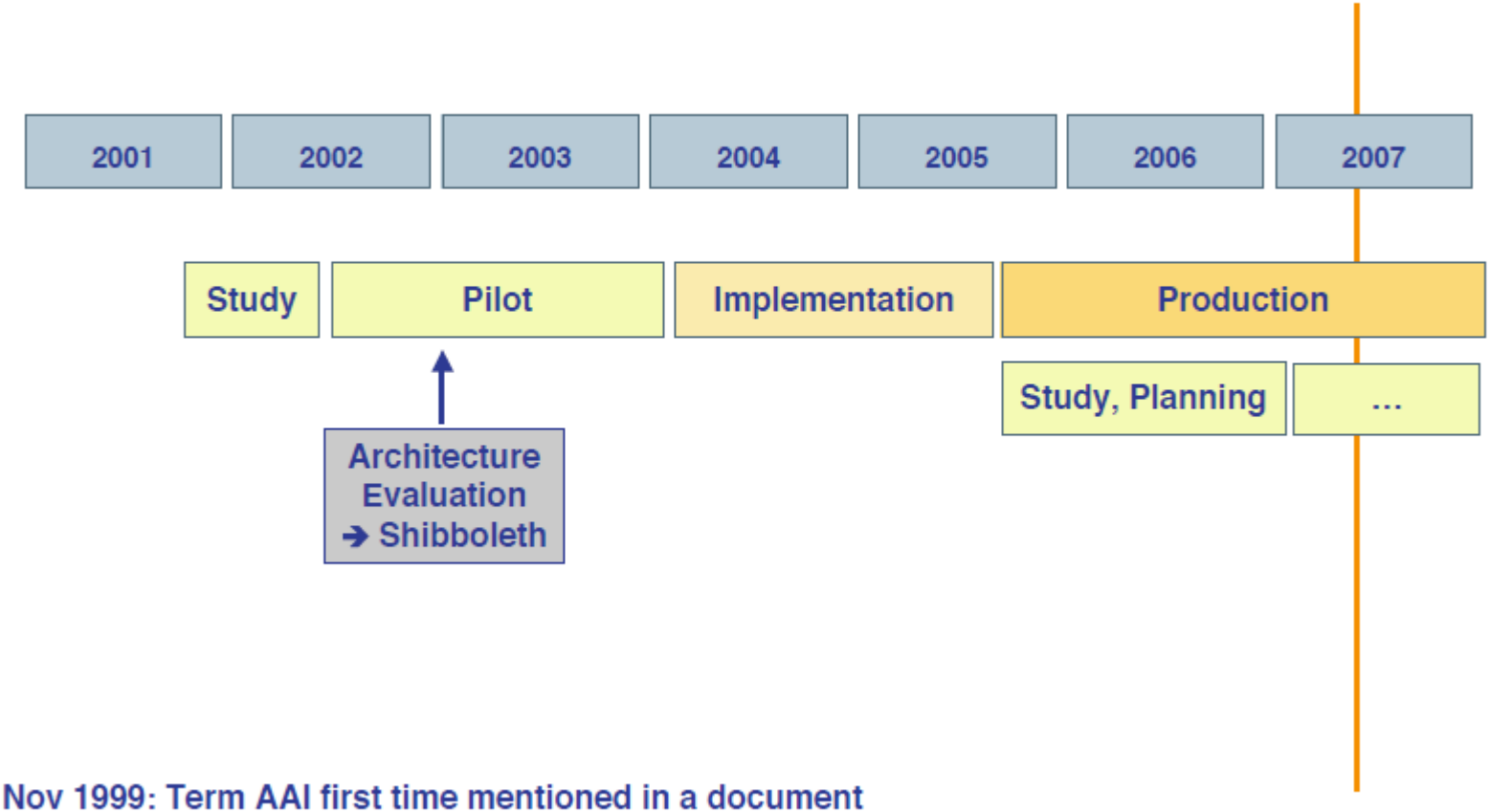
３－１．SWITCH（スイス）

- SWITCH（１９８７年設立）：
  スイスの大学が出資するPrivate Company。
  スイスの大学に、認証認可基盤を含むネットワークサービス（AAI、Grid、PKI、Mobile）を幅広く提供。
- SWITCHaaiの構築（２００５－２００７）：
  Shibbolethベースの認証・認可フェデレーションを構築。
  スイス国内75%の大学が利用。
  e-Learning利用基盤からスイス国内標準基盤へ。
- 今後はAAA/SWITCHを展開（２００８－２０１１）：
  ・AAA（Auditing/Accounting/Assurance）
  ・Grid middleware
  ・VO
  ・e-Learning

３－２．SWITCHaaiのスケジュール

SWITCHaai Project Timeline

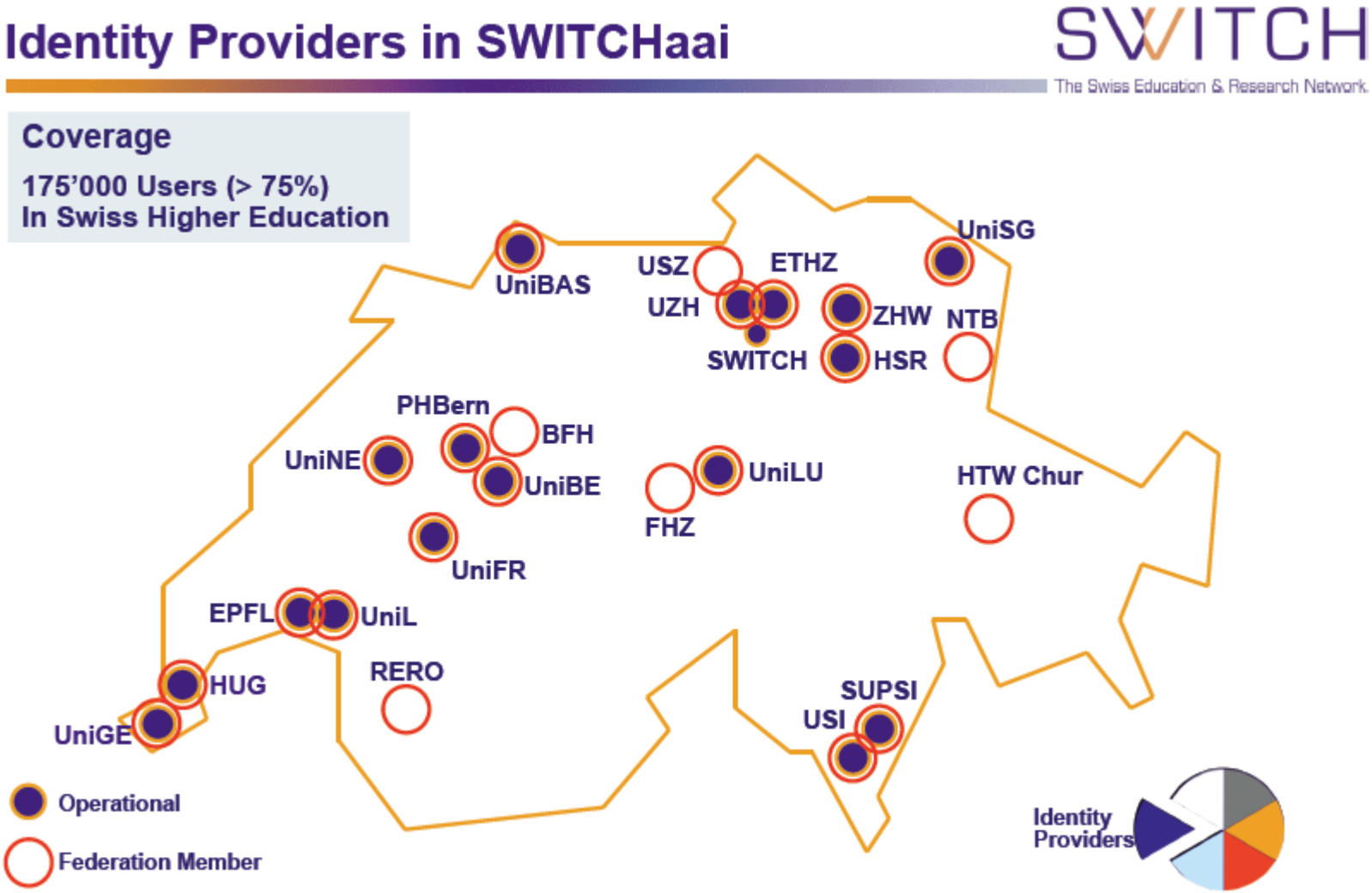
SWITCH
The Swiss Education & Research Network



Nov 1999: Term AAI first time mentioned in a document
Nov 2000: AAI Workshop

＊ SWITCH “AAI Introductory Tutorial”**より引用**

3－3. SWITCHaaiの導入状況



∗ SWITCH “AAI Introductory Tutorial”**より引用**

３－４．SWITCHaaiの属性

Authorization Attributes

SWITCH
The Swiss Education & Research Network

Personal	Group Membership
Unique Identifier	Home Organization Name
Surname	Home Organization Type
Given name	Affiliation (student, staff, …)
E-mail	Study branch
Address(es)	Study level
Phone number(s)	Staff category
Preferred language	Group membership
Date of birth	Organization Path
Gender	Organizational Unit Path

- Implementation of Attributes
  - Mandatory
  - Recommended or optional
- Based on
  - eduPerson Attributes
  - “Schweizerisches Hochschulinformationssystem” (SHIS)
- NO username, password

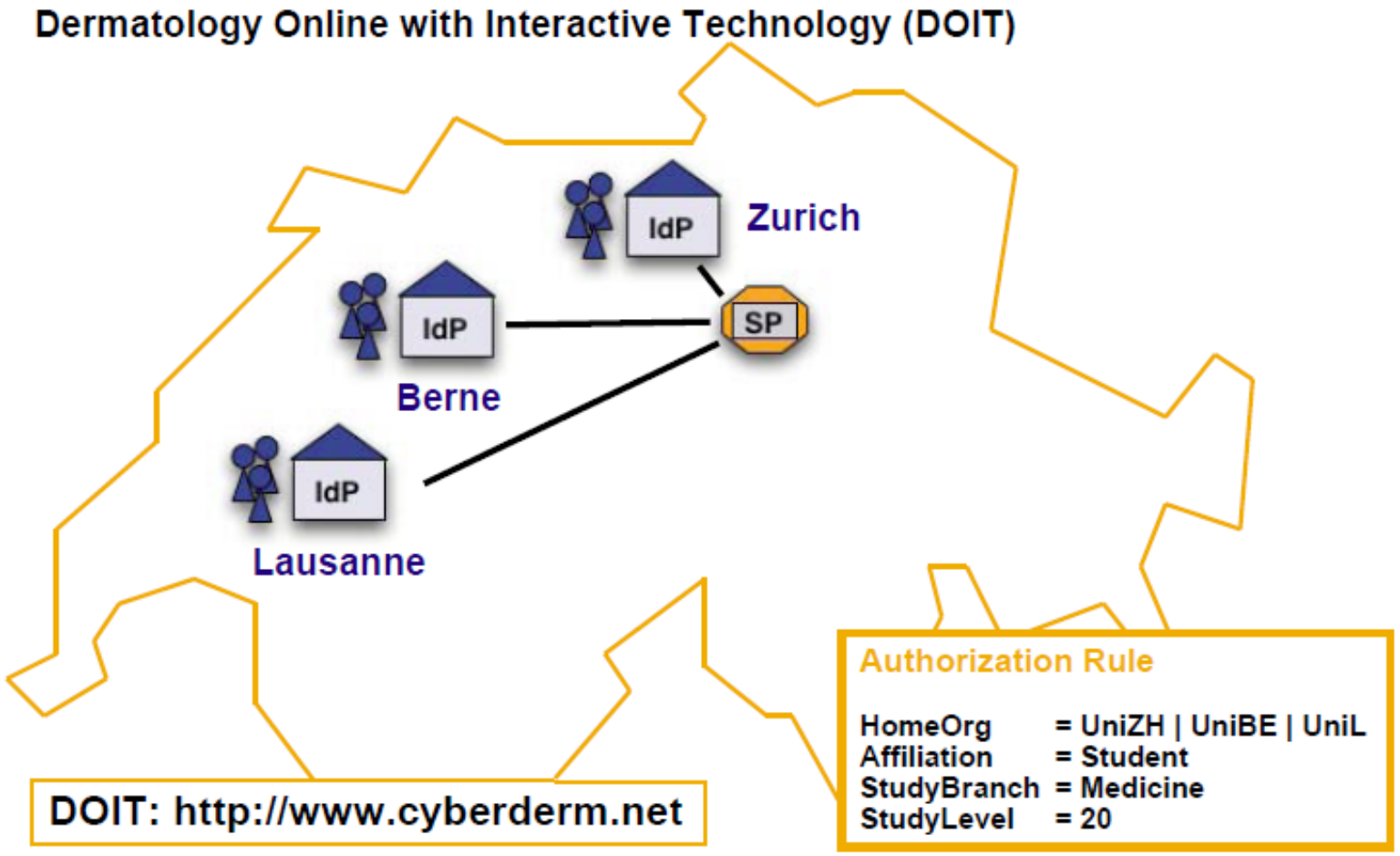
http://www.switch..ch/aai/docs/AAI_Attr_Specs.pdf

∗ SWITCH “AAI Introductory Tutorial”**より引用**

UPKI initiative

３－５．SWITCHaaiのアクセス管理例

Attribute Based Authorization Example



＊ SWITCH “AAI Introductory Tutorial”**より引用**

3－6. SWITCHaaiのSP

Service Providers in SWITCHaai

E-Learning

OLAT Moodle WebCT CE
WebCT Vista VITELS
Dokeos
ADlearn DOOR
DOIT CASUS ILIAS
Claroline Blackboard

Libraries

EZproxy JSTOR
ScienceDirect Ovid
VirtualLib DigiTool RERO
EBSCO Aleph

Other Web Applications

eConf Portal BSCW EVA SLCS
Compicampus Plone VASH
OpenCMS WebSMS Sympa
ESN Fedora TWiki Blue Coat
Jahia Lenya uPortal IS-Academia

Commercial & other Partners

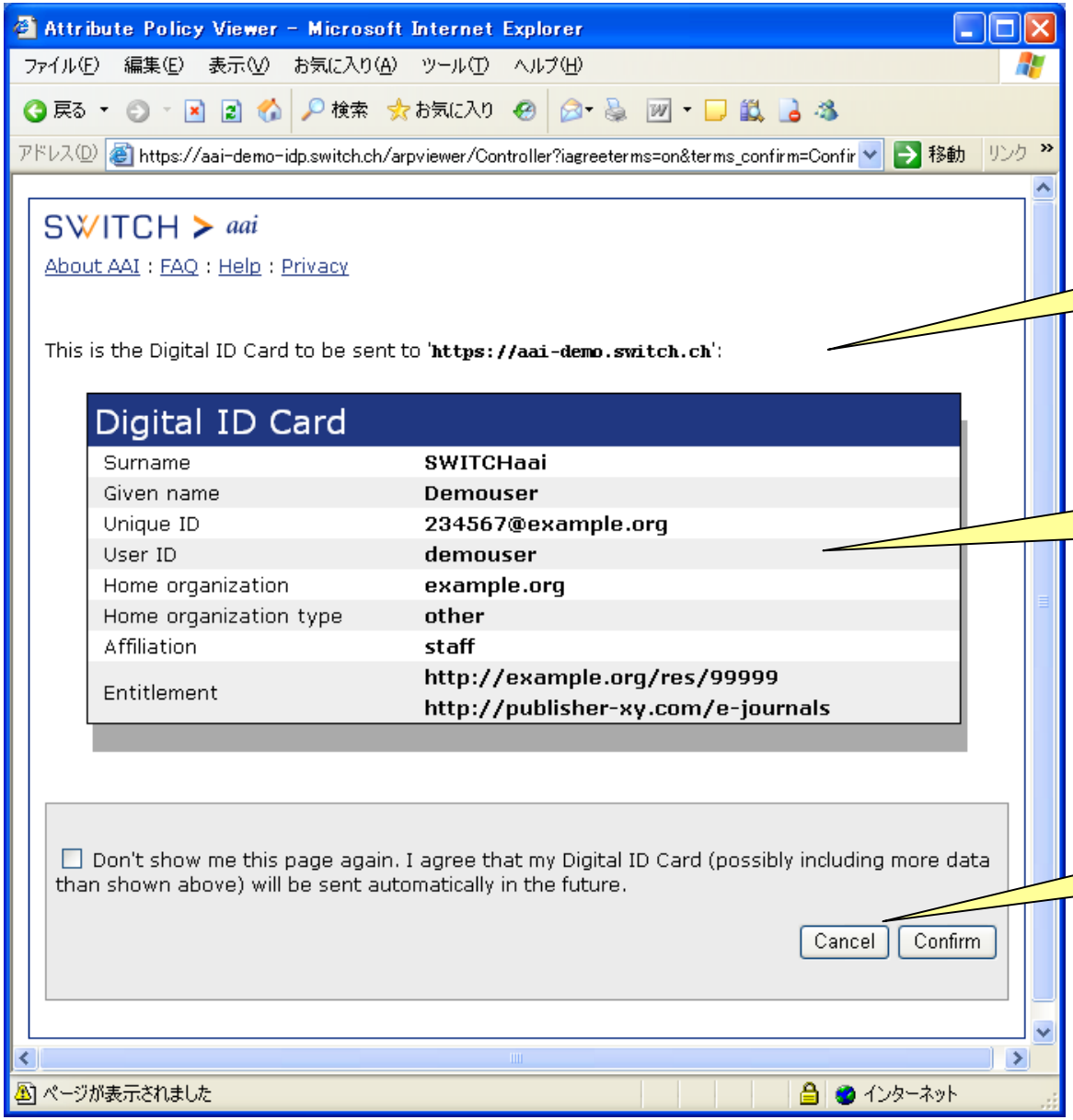
MSDNAA Neptun Store
Swiss Federal Court

operational
in pilot ideas

>210 Resources

＊ SWITCH “AAI Introductory Tutorial”**より引用**

3－7．SWITCHaaiのツール



このSPに送付します！

あなたのこれらの情報を送付します！

送付しても良いですか？

＊ SWITCH “ArpViwer Demo”より

３－８. 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

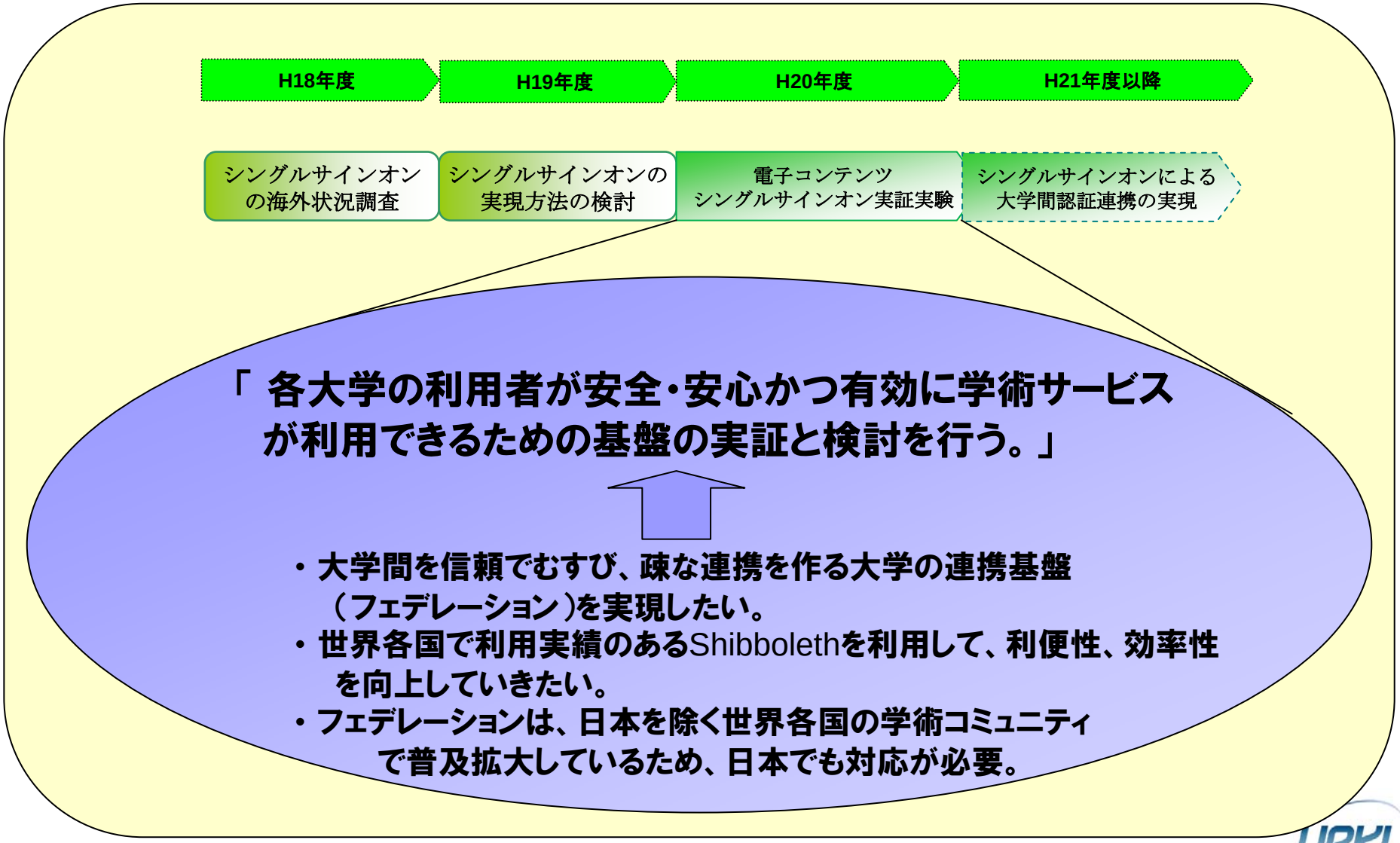
  米国、欧州の各フェデレーション同士で連携するための国際的な検討。

  第一回：2007年9月

  第二回：2008年6月

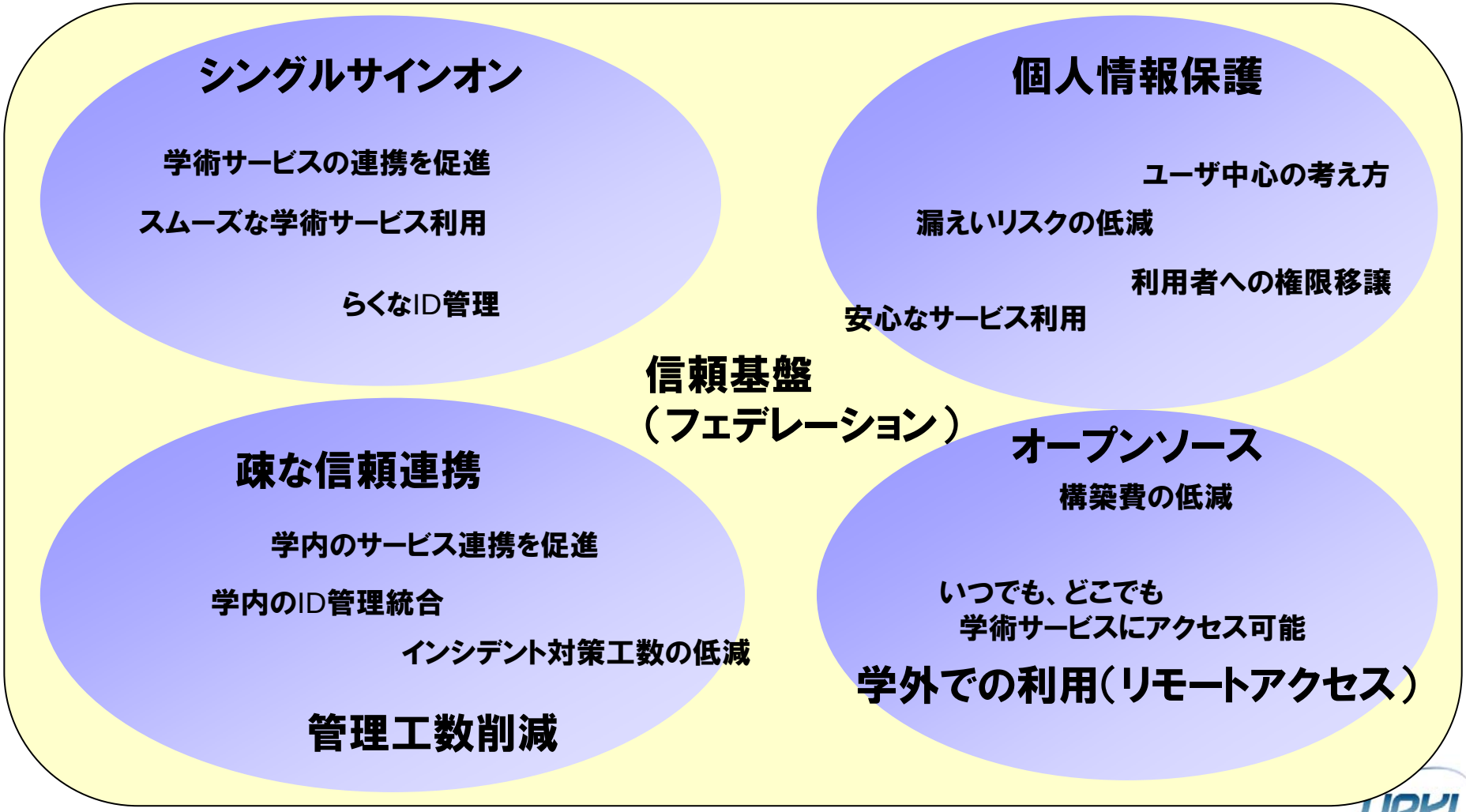
4. 実証実験

４－１．実証実験について

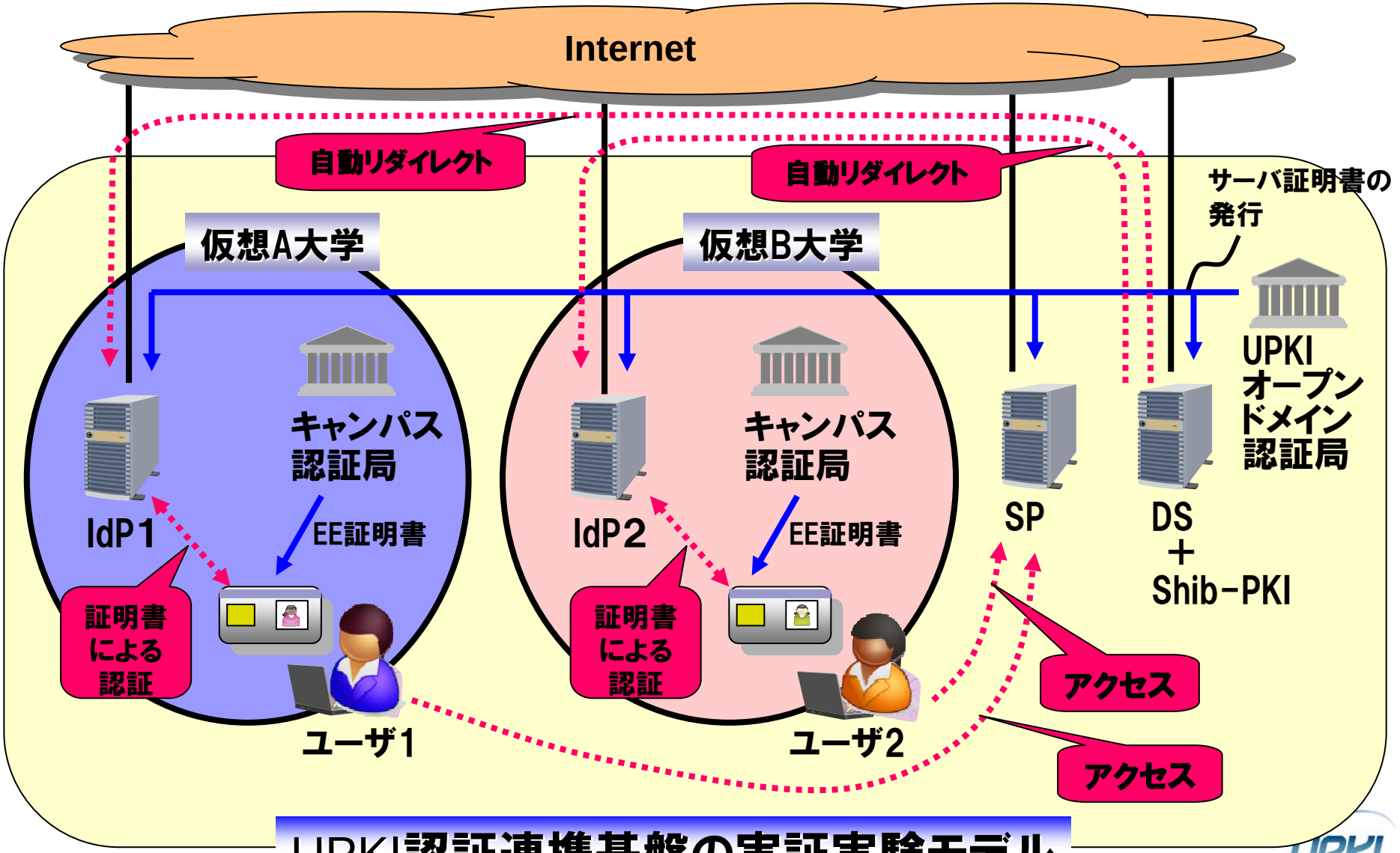

H18年度
H19年度
H20年度
H21年度以降
シングルサインオンの海外状況調査
シングルサインオンの実現方法の検討
電子コンテンツシングルサインオン実証実験
シングルサインオンによる大学間認証連携の実現
「 各大学の利用者が安全・安心かつ有効に学術サービスが利用できるための基盤の実証と検討を行う。」
・大学間を信頼でむすび、疎な連携を作る大学の連携基盤（フェデレーション）を実現したい。
・世界各国で利用実績のあるShibbolethを利用して、利便性、効率性を向上していきたい。
・フェデレーションは、日本を除く世界各国の学術コミュニティで普及拡大しているため、日本でも対応が必要。

４－２．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。

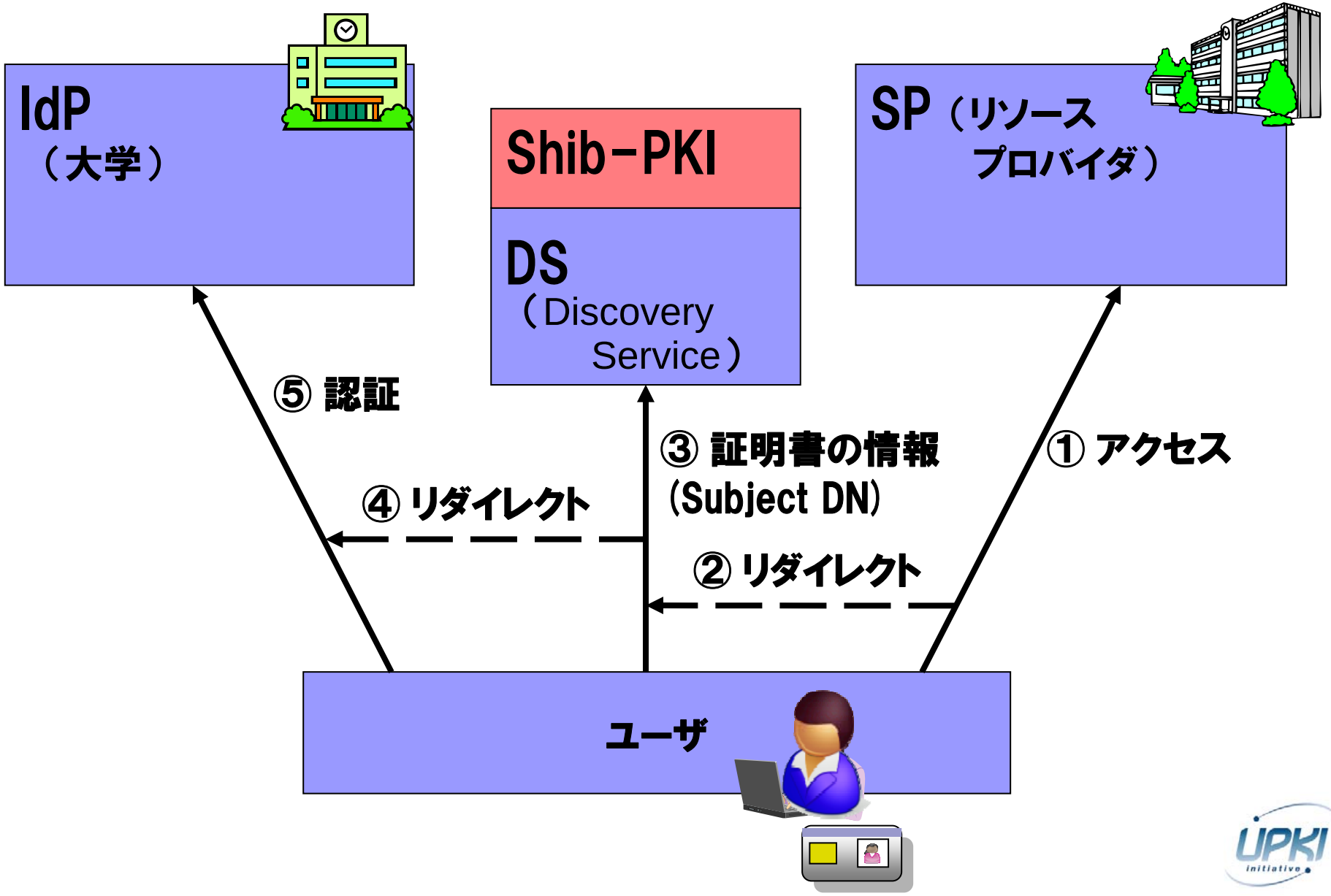


4－3. 実証実験モデル

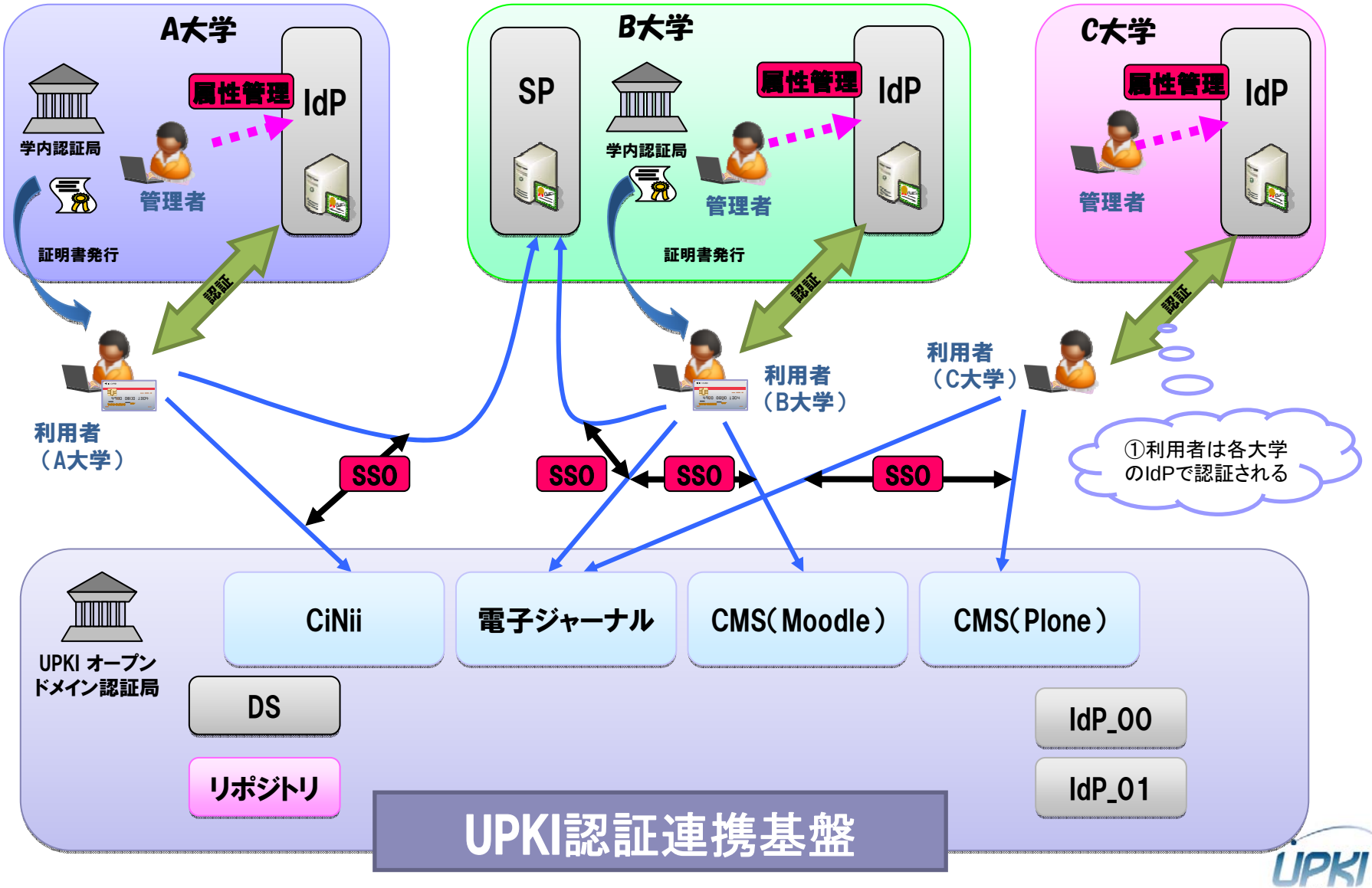


UPKI認証連携基盤の実証実験モデル

4－4. Shib-PKIモジュールの開発



4－5. 実証実験の概要


A大学
属性管理
IdP
学内認証局
管理者
証明書発行
認証
B大学
SP
属性管理
IdP
学内認証局
管理者
証明書発行
認証
C大学
属性管理
IdP
管理者
認証
利用者
（A大学）
利用者
（B大学）
利用者
（C大学）
SSO
SSO
SSO
SSO
①利用者は各大学
のIdPで認証される
UPKI オープン
ドメイン認証局
CiNii
電子ジャーナル
CMS(Moodle)
CMS(Plone)
DS
リポジトリ
IdP_00
IdP_01
UPKI認証連携基盤

4－5. 実証実験の概要（2）

参加大学

各大学の状況を反映した実証

IdP

構築 → 接続テスト → テスト用ID、属性を設定 → 各SPとの接続テスト → 有効性（ユーザ、管理者）、実現性（構築、運用）の確認と実証 → 結果の報告

SP

構築 → 接続テスト → 各IdPとの接続テスト → 有効性（ユーザ、管理者）、実現性（構築、運用）の確認と実証 → 結果の報告

UPKIでの検討と提供

- ・実証実験システム
- ・構築手順書
- ・VMイメージ

→ ・実証実験SP　・実証実験用Wiki
・各種ツール　・支援、ヘルプデスク
・各種資料（事例、海外動向、運用方法）

- ・属性は4つ
- ・証明書はUPKI オープンドメイン 認証局から発行

→ ・属性の検討
・証明書の検討
・各種ツールの検討
・SPの検討

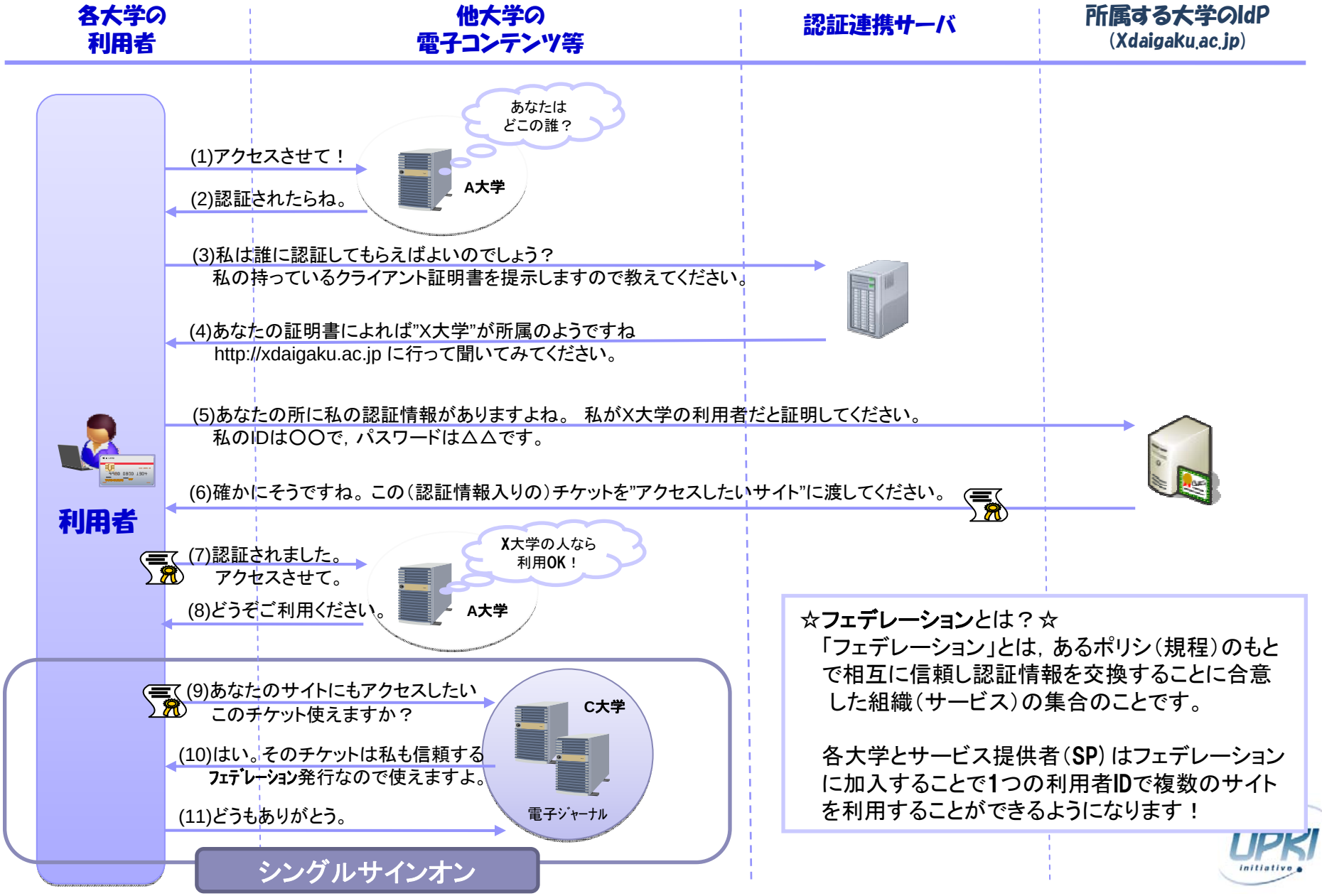
→ ・結果とりまとめ
・報告会開催

UPKI

UPKI オープンドメイン認証局

リポジトリ	IdP_00	CiNii	CMS（Moodle）
DS	IdP_01	電子ジャーナル	CMS（Plone）

（参考）認証とシングルサインオンの処理の流れ



☆**フェデレーション**とは？☆

「フェデレーション」とは，あるポリシ（規程）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）の集合のことです。

各大学とサービス提供者（SP）はフェデレーションに加入することで**1**つの利用者**ID**で複数のサイトを利用することができるようになります！

４－６. UPKI認証連携基盤の構成案

【方針】:
「想定される具体的なサービスと連携するための最低限の
構成を策定し、実証実験でこれを検証する。」

- ポリシー、システム定義:
  下記を案として、実証実験の中で詳細を検討していく。
  （参考資料）UPKI認証連携基盤 運用ポリシー（案）
  （参考資料）UPKI認証連携基盤 システム定義（案）
- 認証局:
  基本は、UPKIオープンドメイン認証局として、他の商用認証局の利用も
  検討する。
- 属性:
  約40の属性を利用可能とするが、必須は下記の4つの属性とする。
  ① UPKI-Fed用ID（eduPersonPrincipalName）
  ② 組織名（Home Organization）
  ③ 所属（Organization Unit）
  ④ 役職（eduPersonAffiliation）
  （参考資料） UPKI認証連携基盤 属性仕様（案）

デモ

UPKIの実証実験システム

- CiNii
- DSpace
- NetCommons
- Plone