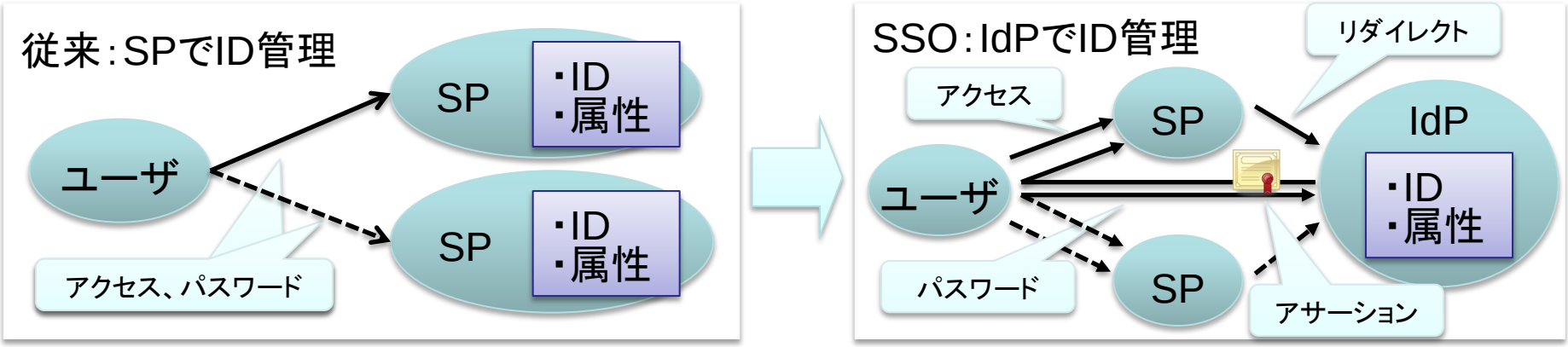
学術認証フェデレーションの概要

国立情報学研究所

National Institute of Informatics

学術認証フェデレーションとは

- 学術認証フェデレーションとは
  - 定められた規程（ポリシー）を信頼しあうことで，相互に認証連携を実現し，学術リソースを利用・提供する機関や組織から構成された連合体のこと
  - 機関（IdP）がIDと属性を管理し，サービス提供者（SP）がそれを利用して認可
- プライバシ保護
  - ユーザのユニークネスを保証しつつ個人情報は出さない
  - SPは必要な情報のみをIdPに要求
  - ユーザは各SPに対する各属性の公開を制御可能



National Institute of Informatics

Shibboleth（シボレス）

- 米国EDUCAUSE／Internet2にて2000年に発足したプロジェクト
  - http://shibboleth.internet2.edu/
- 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ミドルウェア （オープンソースソフトウェア）
- 最新はShibboleth V2.1
- 米国、欧州でShibbolethによるFederationが運用、拡大

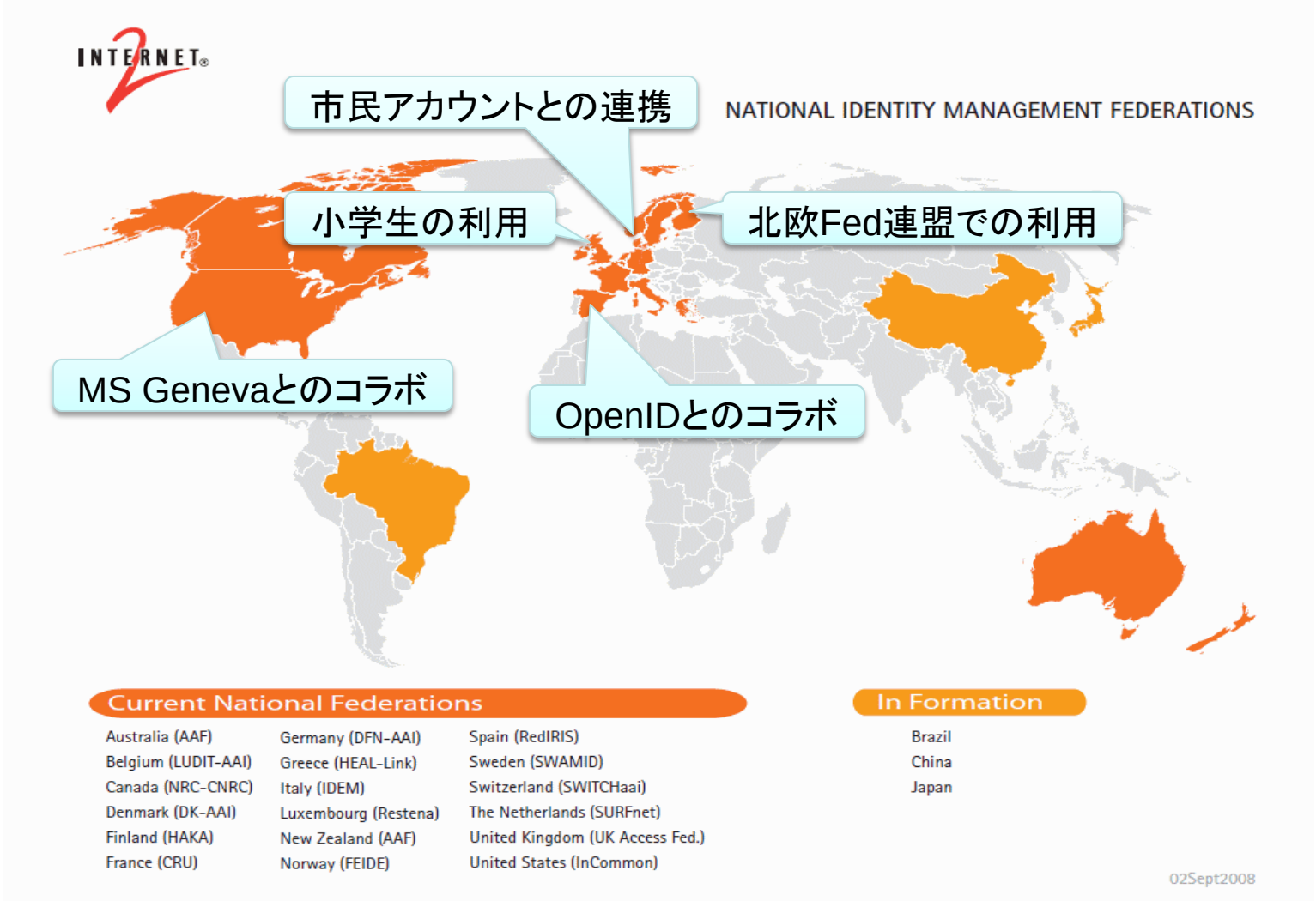
cf.

- 欧州（特に北欧）では，simpleSAMLphpも利用

  - ノルウェ—UNINETT
    - http://rnd.feide.no/simplesamlphp
  - 日本語化プロジェクト
    - http://sourceforge.jp/projects/ssp-japan/

National Institute of Informatics

世界のフェデレーションと動向



http://www.internet2.edu/pubs/national_federations.pdf

ID空間とサービス空間の創造

Web空間

学術認証フェデレーション

サービス空間KnowledgeBase

従来の分断サービス空間

National Institute of Informatics

フェデレーション構築に必要なサーバ

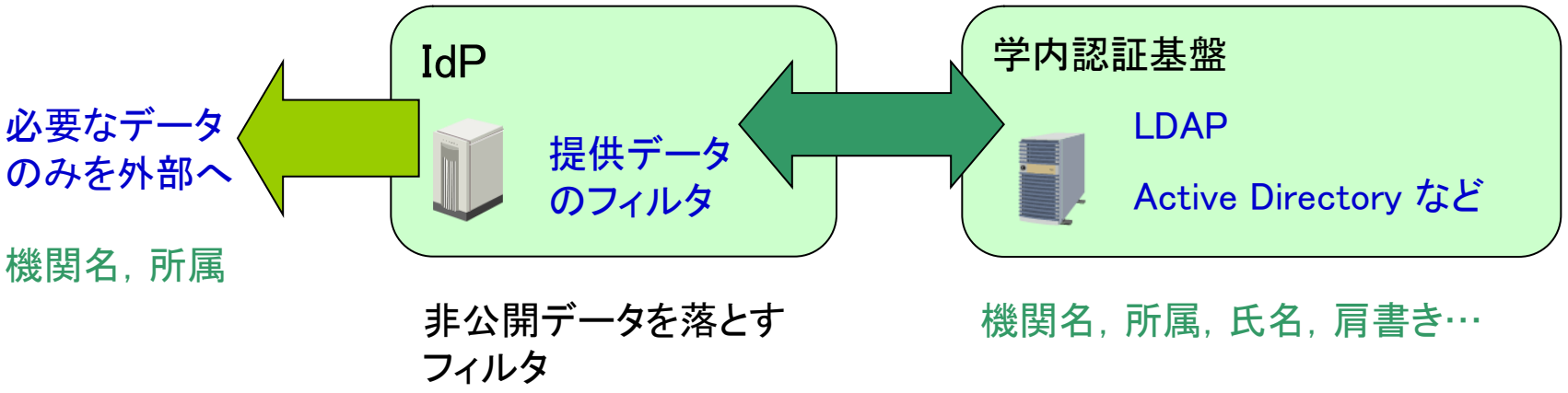
- **IdP（ID Provider）大学(サービス利用者側)が用意**
  - フェデレーション内に構成員の情報を提供するサーバ
  - フェデレーションに参加する大学等が構築

- **SP（Service Provider）大学他(サービス提供側)が用意**
  - 認証を受けた人に対してサービスを行うサーバ
  - 電子ジャーナル，データベース，E-ラーニング等 Webベースのシステムであれば何でも可

- **DS（Discovery Service）フェデレーションが用意**
  - SPへのアクセスの際にIdPを検索するシステム
  - フェデレーションが運用
  - ここに名前がのることにより「フェデレーションに参加」

IdP (ID Provider)とは

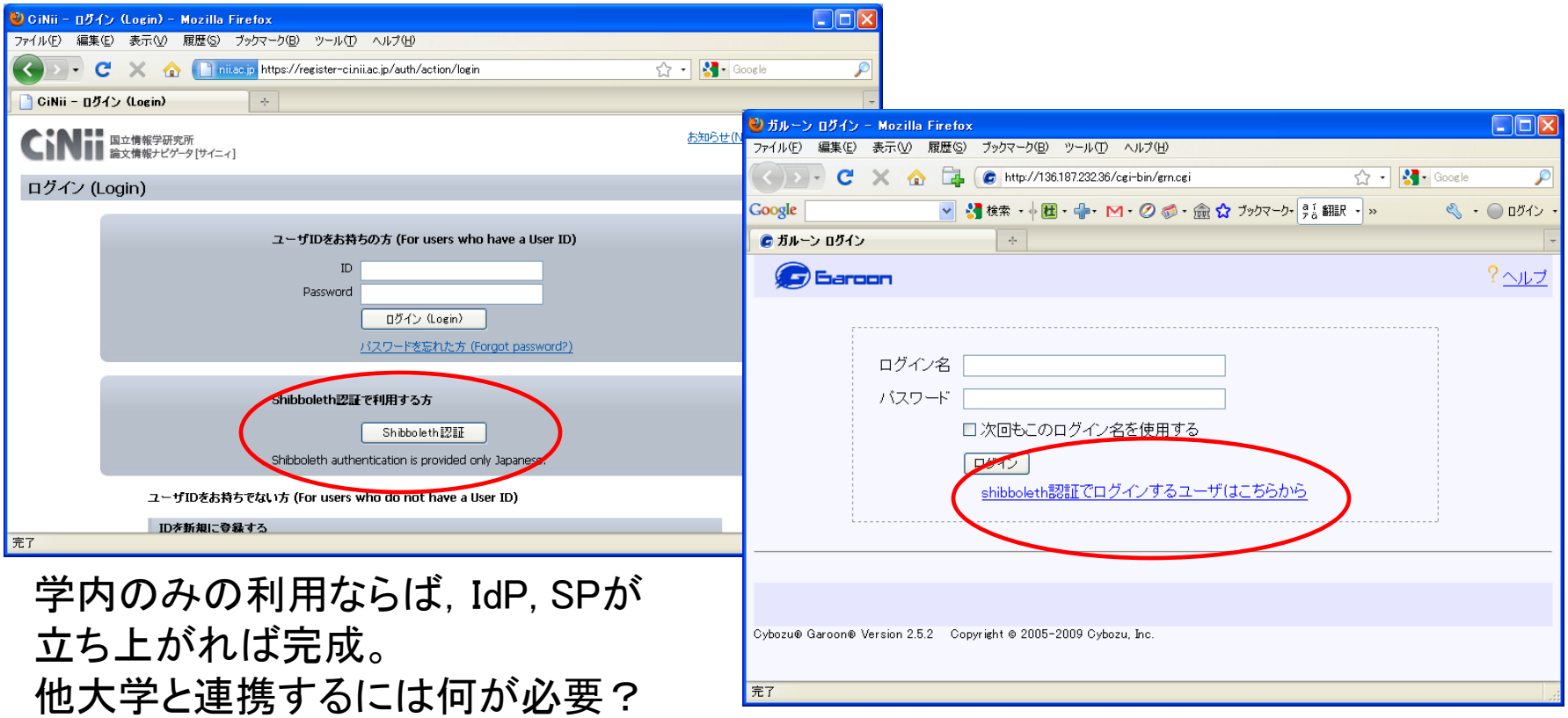
- フェデレーション内に情報を提供するサーバであり，大学等が構築
- IdP自身は情報を持たない
- 情報はLDAPやActive Directory等，既存の認証基盤を参照
- IdPは単なるフィルタであり，学内認証基盤から特定のデータのみを抽出して提供する
- 公開できるデータの制御が可能である
  - このため，Shibbolethはしばしば個人情報保護に優れていると言われるが，サーバ自体がハッキングに強固という意味ではない。
  - 慎重な操作が必要なのは，LDAPやActive Directoryと同じ



National Institute of Informatics

SP (Service Provider)とは

- サービスを提供するWebサーバのこと
- “シボレスログイン”等のボタンがあればShibbolethで利用可能なSPである
- 電子ジャーナルに限らず，いろいろなサービスをShibboleth化することが可能（例：無線LAN認証，サイボウズ）



学内のみの利用ならば，IdP，SPが立ち上がれば完成。
他大学と連携するには何が必要？

National Institute of Informatics

現時点で利用可能なSP

（12月1日現在）

- Science Direct / SCOPUS (Elsevier)
- SpringerLink (Springer)
- Web of Knowledge / EndNote (Thomson Reuters)
- OvidSP (Ovid)
- RefWorks (ProQuest)
- Pathology Images (Atlases)
- DreamSpark (Microsoft)
- CiNii (NII)
- FReCS MCU (テレビ会議多地点接続)サービス (NII)

学生を対象に、開発環境（ソフトウェア）を提供

最新情報：https://upki-portal.nii.ac.jp/docs/fed/participants

National Institute of Informatics

海外フェデレーションのSP数

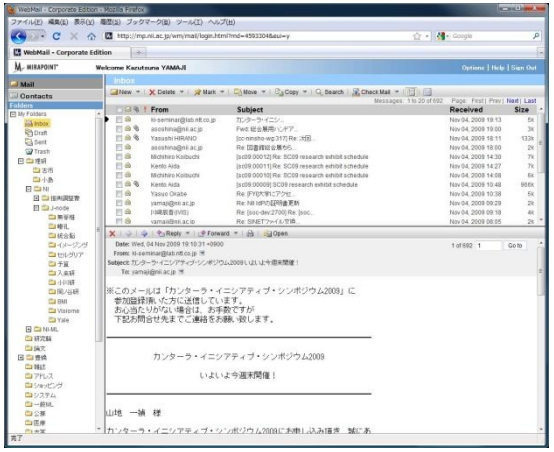
- スイスSWITCHaai：382
- イギリスUK-FAM：190
- アメリカInCommon：150以上
- ドイツDFN-AAI：60
- フィンランドHaka：65
- フランスFédération Éducation-Recherche ：54
- ノルウェーFEIDE：50以上

日本国内のサービスの展開がポイント

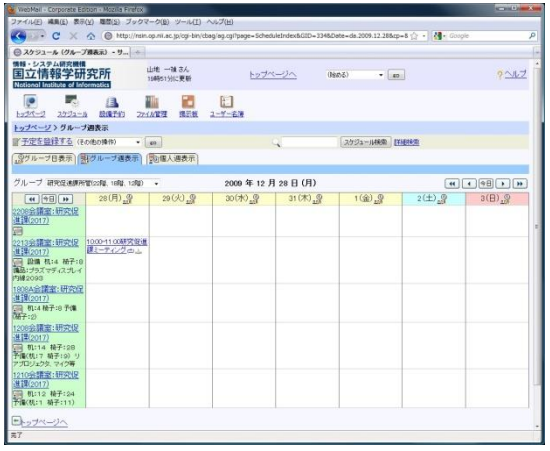
具体的な利用例（学内SSOの整備）

- フェデレーション自体は学外リソース利用のためのもの
- フェデレーションへの参加により
  - 学内の統合認証システム構築を加速化
  - 学内システムのSSO化を加速化
- シボレス化による学内の公開Webサービスの
  セキュリティレベルの向上

Webメイル



グループウエア



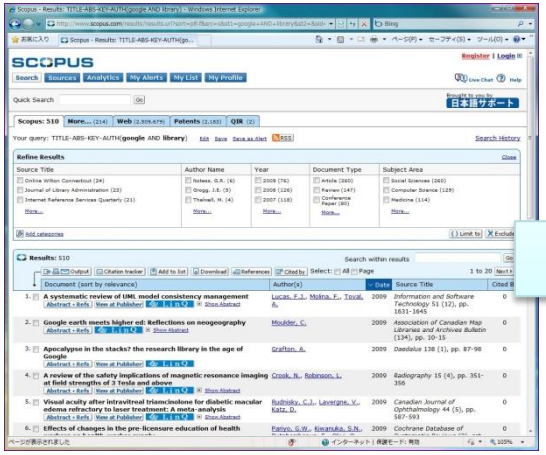
図書館システム

具体的な利用例（電子ジャーナル）

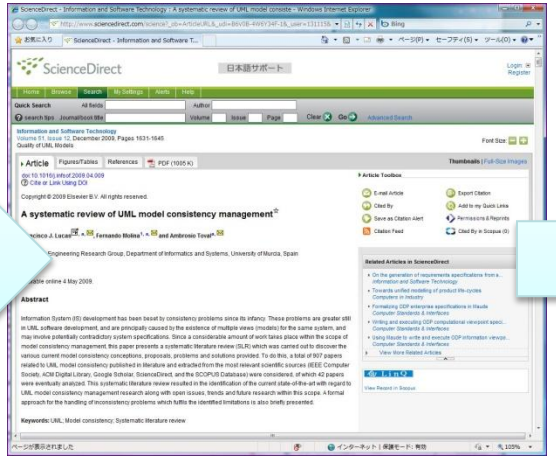
「Shibboelth経由のe-リソース利用」でデモ＋詳細を説明

- リモートアクセスによる利用頻度の向上
- SSOによるユーザエクスペリエンスの向上
- マッシュアップの促進

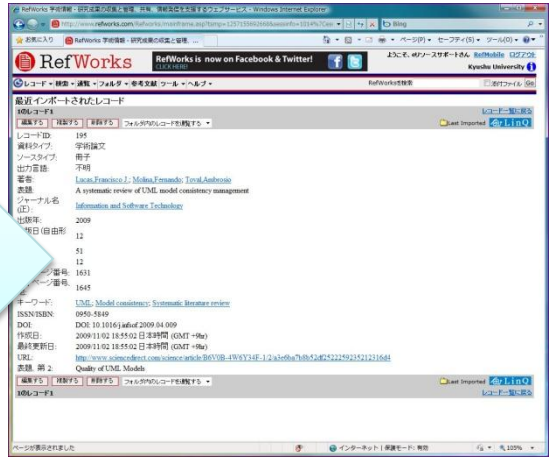
論文を探して



論文を取得して（読んで）

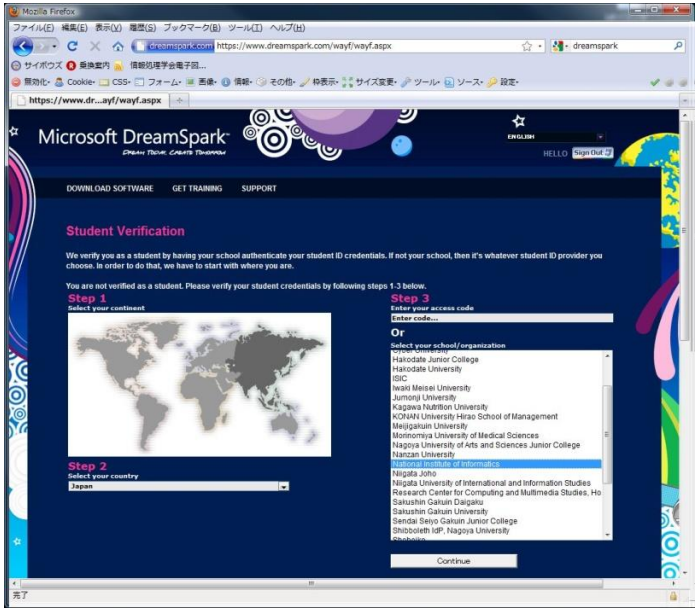


論文を管理する



具体的な利用例（アカデミック配付）

- Microsoft DreamSpark
  - 学生を対象にMSのソフトウエア開発環境を無償で提供するプログラム
- 属性により大学構成員であり学生であることを確認
  - eduPersonTargetedID（SP毎に異なるハッシュ化された一意のID）
  - eduPersonScopedAffiliation（例：student@nii.ac.jp）
- 運用フェデレーション参加24時間後に利用可能

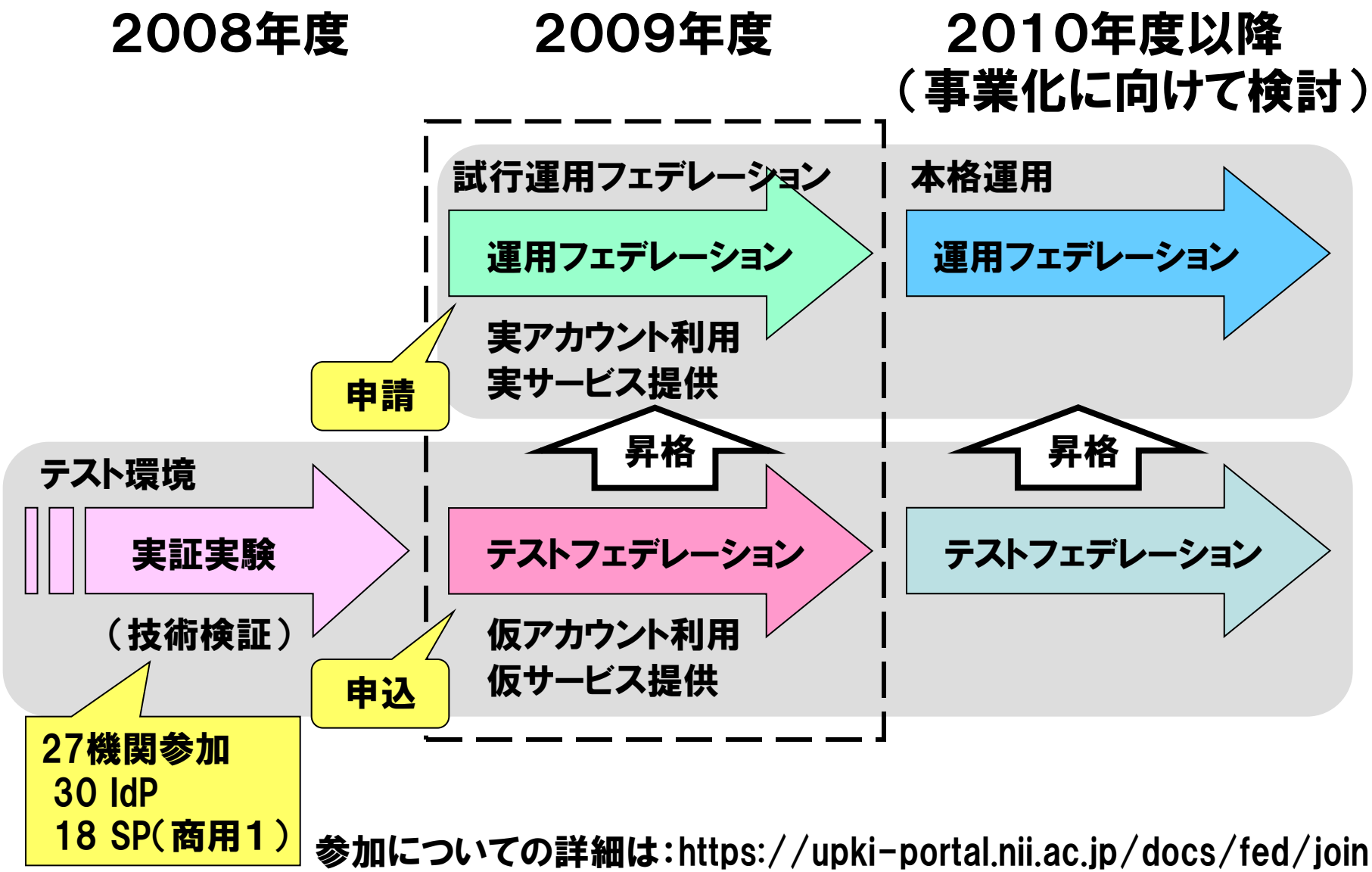


National Institute of Informatics

フェデレーション参加のメリット

- **ID管理側（IdP）メリット**
  - 大学など情報セキュリティ準拠，個人情報保護などへの対応
  - ID管理など運用管理業務，ユーザサポート業務の軽減
  - シームレス（学内外）なアクセス管理システム統合
- **サービス側（SP）メリット**
  - 学術分野へのサービスのビジビリティの向上
  - ID管理からの解放，ユーザサポート業務の軽減
  - ライセンス条件にそった適正な利用
- **サービス利用者メリット**
  - SSOによるユーザエクスペリエンスの向上
  - ID/パスワード管理からの解放
  - 各リソースでマイページ等のパーソナライズ機能の充実化
- **大学経営者メリット**
  - ユーザへの利便性向上を提供
  - 経費削減への展開

構築スケジュール

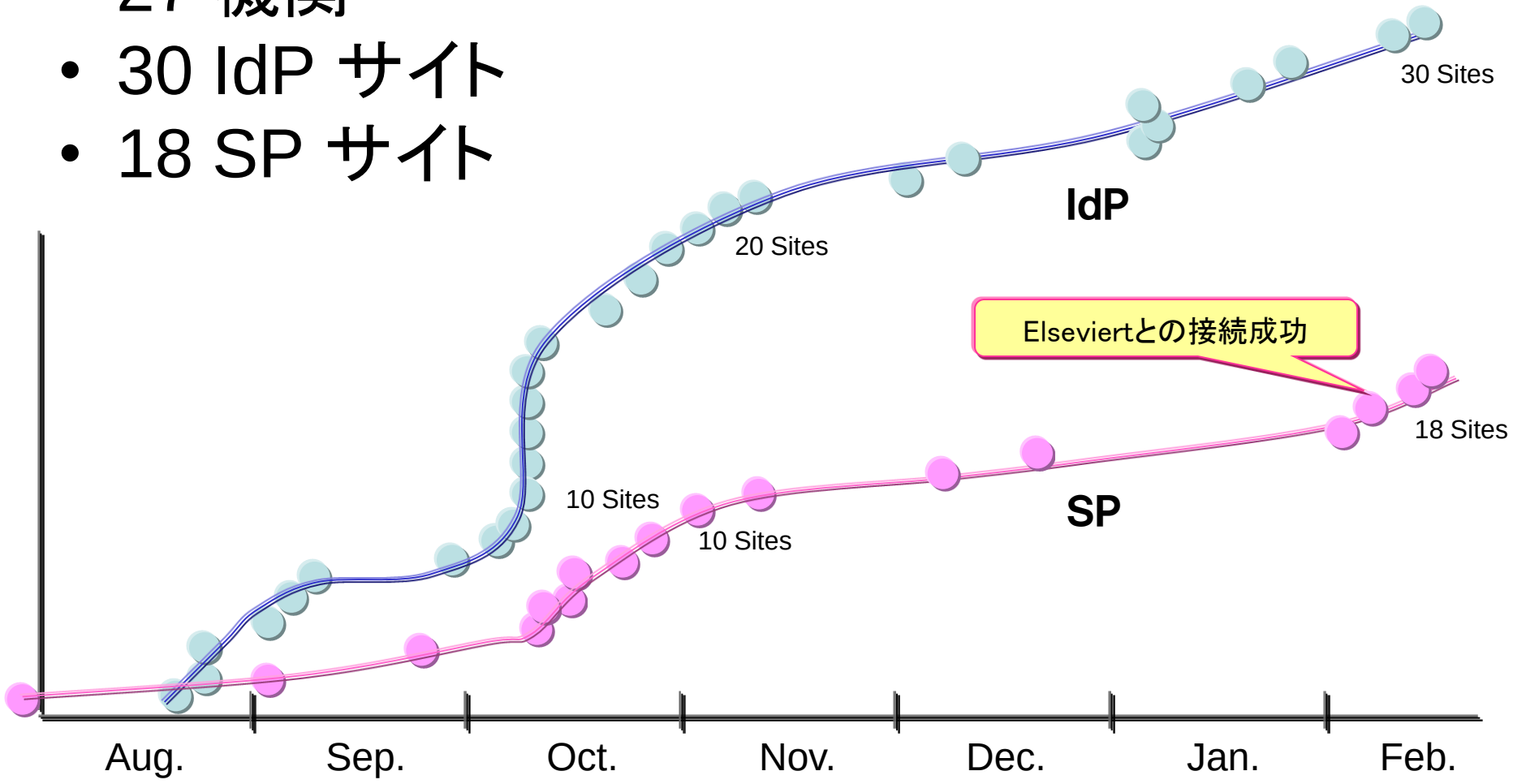


参加についての詳細は：https://upki-portal.nii.ac.jp/docs/fed/join

National Institute of Informatics

実証実験参加機関数推移

- 27 機関
- 30 IdP サイト
- 18 SP サイト



学術認証フェデレーション試行運用(2009~)

学術認証フェデレーション

1. テストフェデレーションで事前接続テストを実施
2. 事前接続テスト成功後、運用フェデレーションへ移行

テストフェデレーション

接続テスト

接続テスト

テストIdP
（大学）

テストSP
（大学、商用）

テストアカウント・関係者のみ

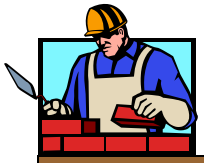
運用フェデレーション

運用IdP
（大学）

SP
（大学、商用）

実アカウント

利用

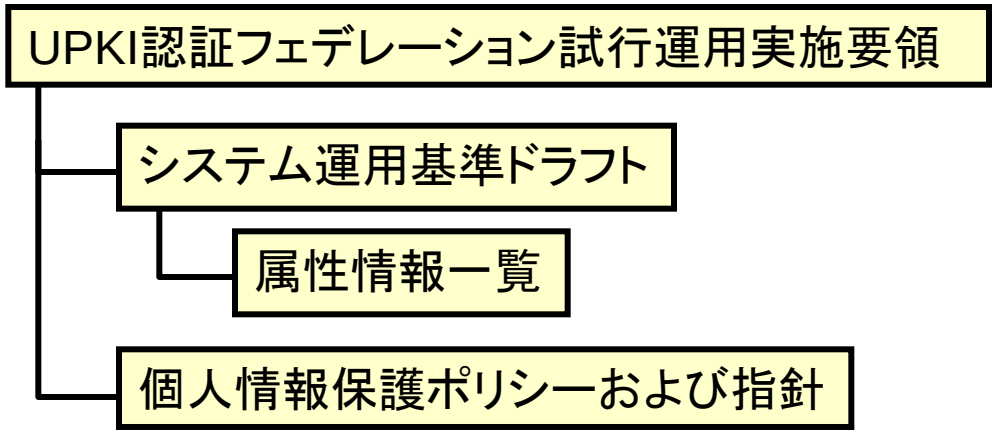


フェデレーション・ポリシー

フェデレーション・ポリシー

学術認証フェデレーションでは、下記の規程(ポリシー)を定めています。
試行運用への参加にあたっては、規程の遵守をお願い致します。

※ Web掲載場所: UPKIイニシアティブ「学術認証フェデレーション」ー「参加」 https://upki-portal.nii.ac.jp/docs/fed/join



- **システム運用基準は、現在ドラフトであり、試行運用を実践しながらブラッシュアップを行い、現在のシステム運用基準はV1.0です。(完成版ではありません)**
  同様に、実施要領も今後の試行運用を行いながら運用しやすいよう改訂していきます。

- **テストフェデレーションは、できる限り本ポリシーの遵守をお願いしますが、各システム及びアカウント等がテスト用であることから、必ずしも全てを遵守する必要はありません。**

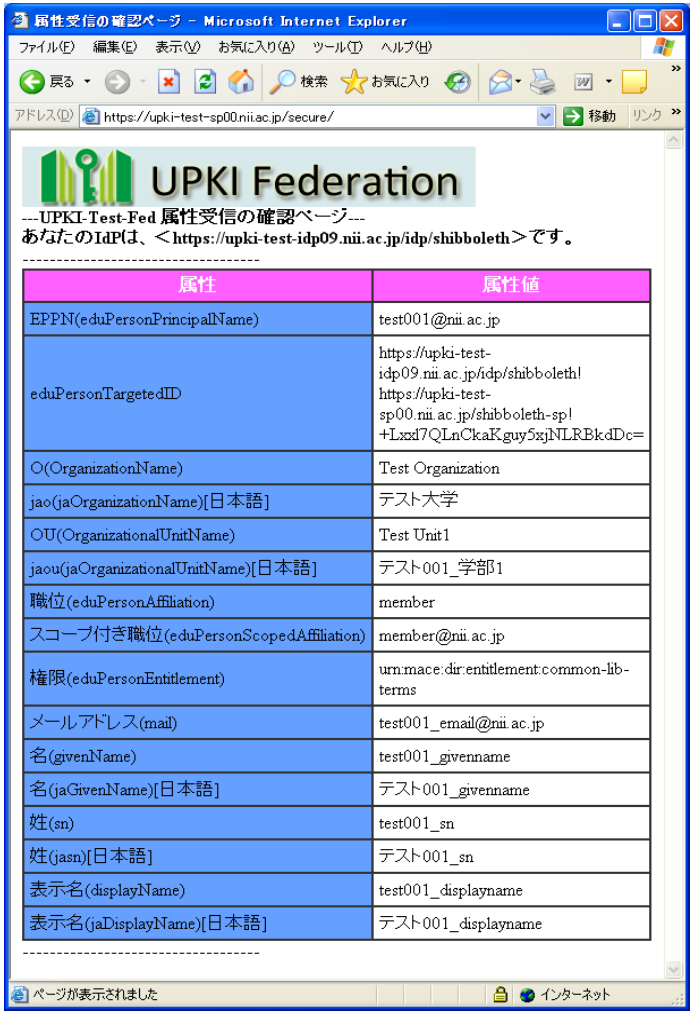
National Institute of Informatics

認証で使用する「属性」

フェデレーションで認証に使用する属性は、フェデレーションポリシーで16種類を定めています。これらのデータを用いて認証を行います。

属性	内容
OrganizationName (o)	組織名
jaOrganizationName (jao)	組織名（日本語）
OrganizationalUnit (ou)	組織内所属名称
jaOrganizationalUnit (jaou)	組織内所属名称（日本語）
eduPersonPrincipalName (eppn)	フェデレーション内の共通識別子
eduPersonTargetedID	フェデレーション内の匿名識別子
eduPersonAffiliation	職種
eduPersonScopedAffiliation	職種（スコープ付き）
eduPersonEntitlement	資格
SurName (sn)	氏名（姓）
jaSurName (jasn)	氏名（姓）（日本語）
GivenName	氏名（名）
jaGivenName	氏名（名）（日本語）
displayName	氏名（表示名）
jaDisplayName	氏名（表示名）（日本語）
mail	メールアドレス

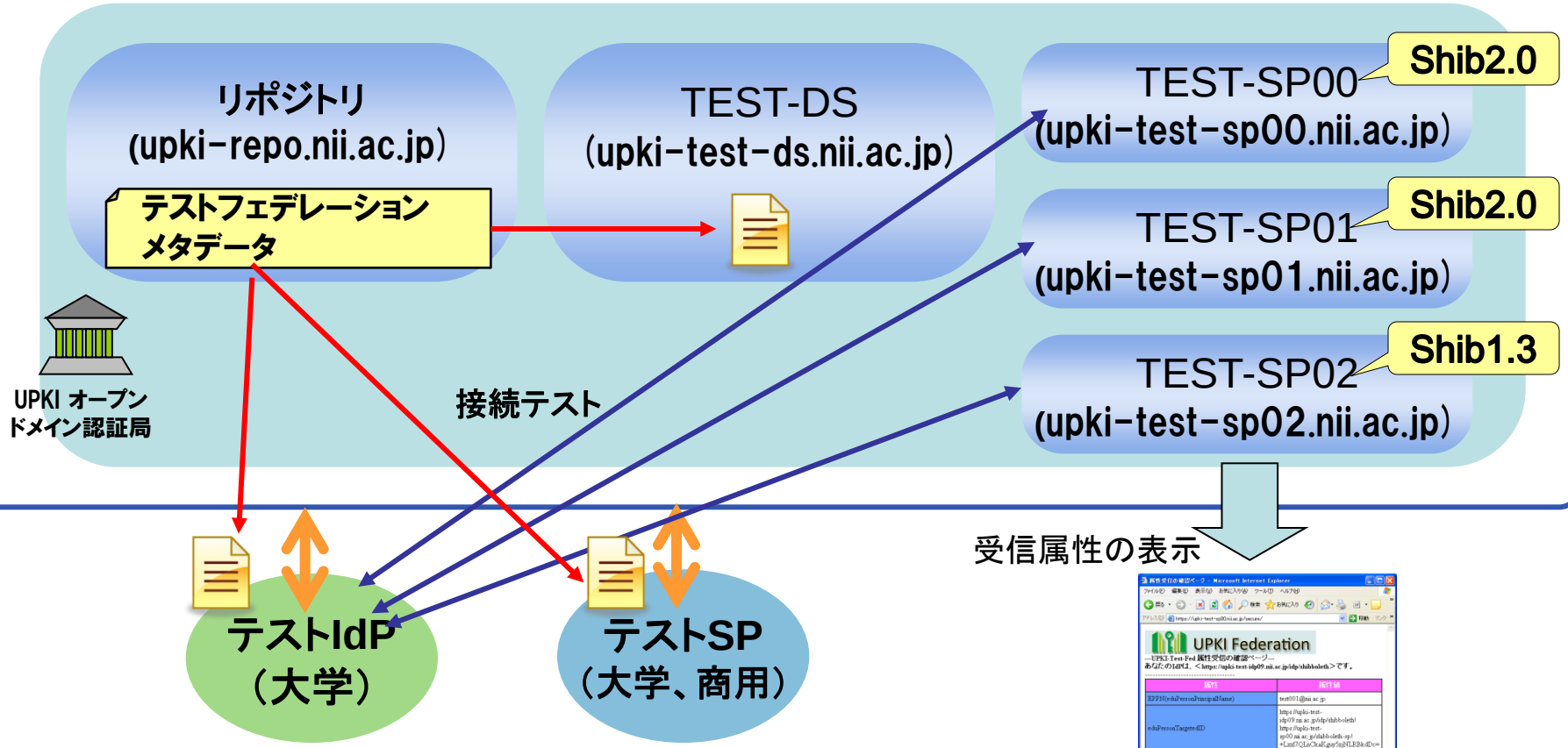
テストSPでの表示例



掲載場所：https://upki-portal.nii.ac.jp/docs/fed/technical/attribute

テストフェデレーション

テストフェデレーション（UPKI-Test-Fed）のシステム構成

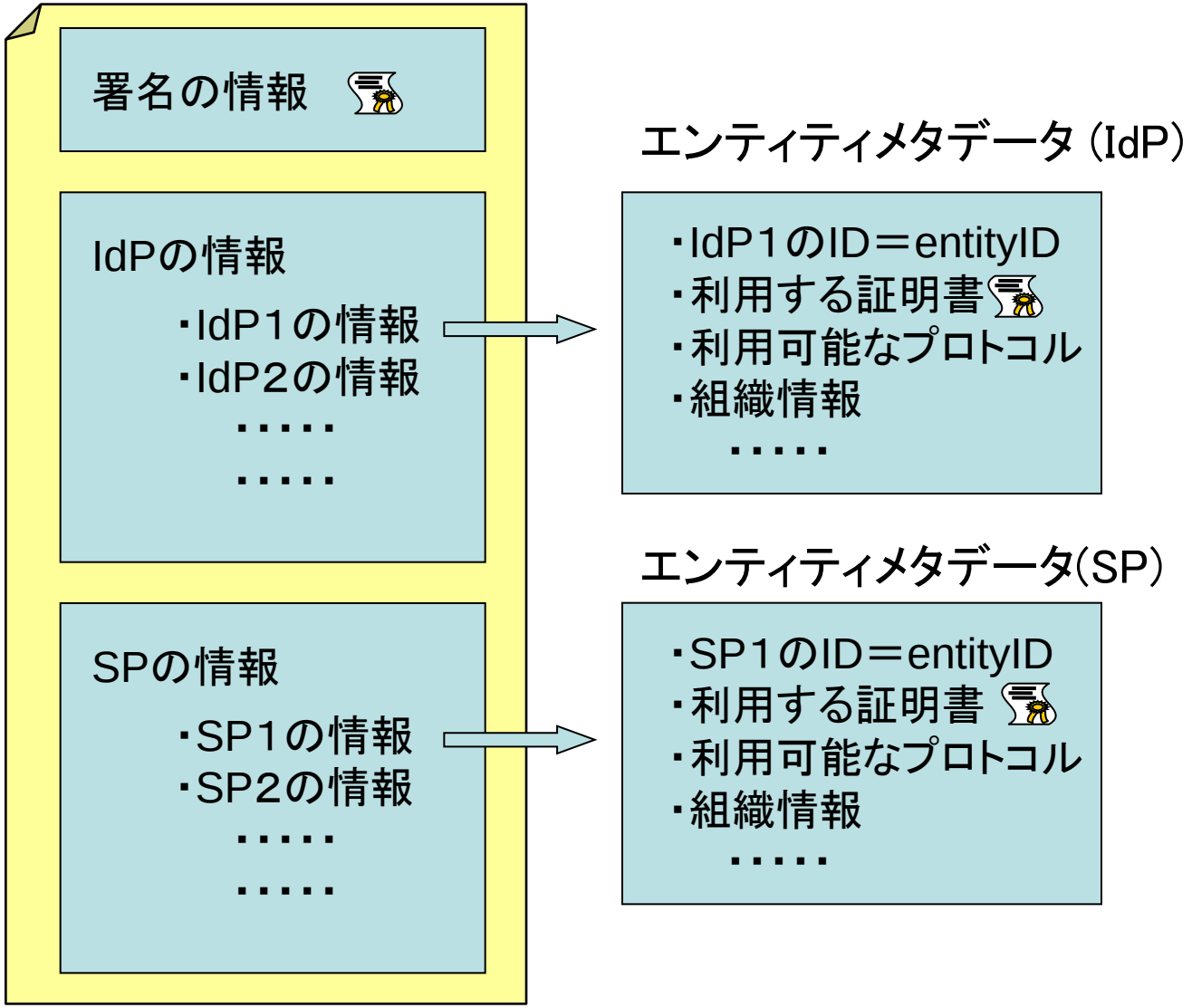


- SP，IdPは1対1で存在確認しているわけではない
- 同じフェデレーションのメンバーであることがわかるものがいる
  → メタデータ
- 3つのテスト用SPをNIIに準備，大学のIdPの動作確認が可能

National Institute of Informatics

メタデータ(XML形式)の構成

フェデレーションメタデータ ≒ **relying party（信頼関係）**



テストフェデレーションIdP設置申込書

様式　1

平成21年7月1日

UPKI認証フェデレーション試行運用（テストフェデレーション）IdP設置申込書

国立情報学研究所
UPKI認証フェデレーション試行運用プロジェクト事務局　御中

UPKI認証フェデレーション試行運用実施要領を遵守し，次のとおり申込いたします。

申込区分	☑ 新規	□ 変更	□ 中止	（中止の場合は，連絡欄にその理由をご記入ください。）

EntityID	https://example.fed.ac.jp/shibboleth-idp

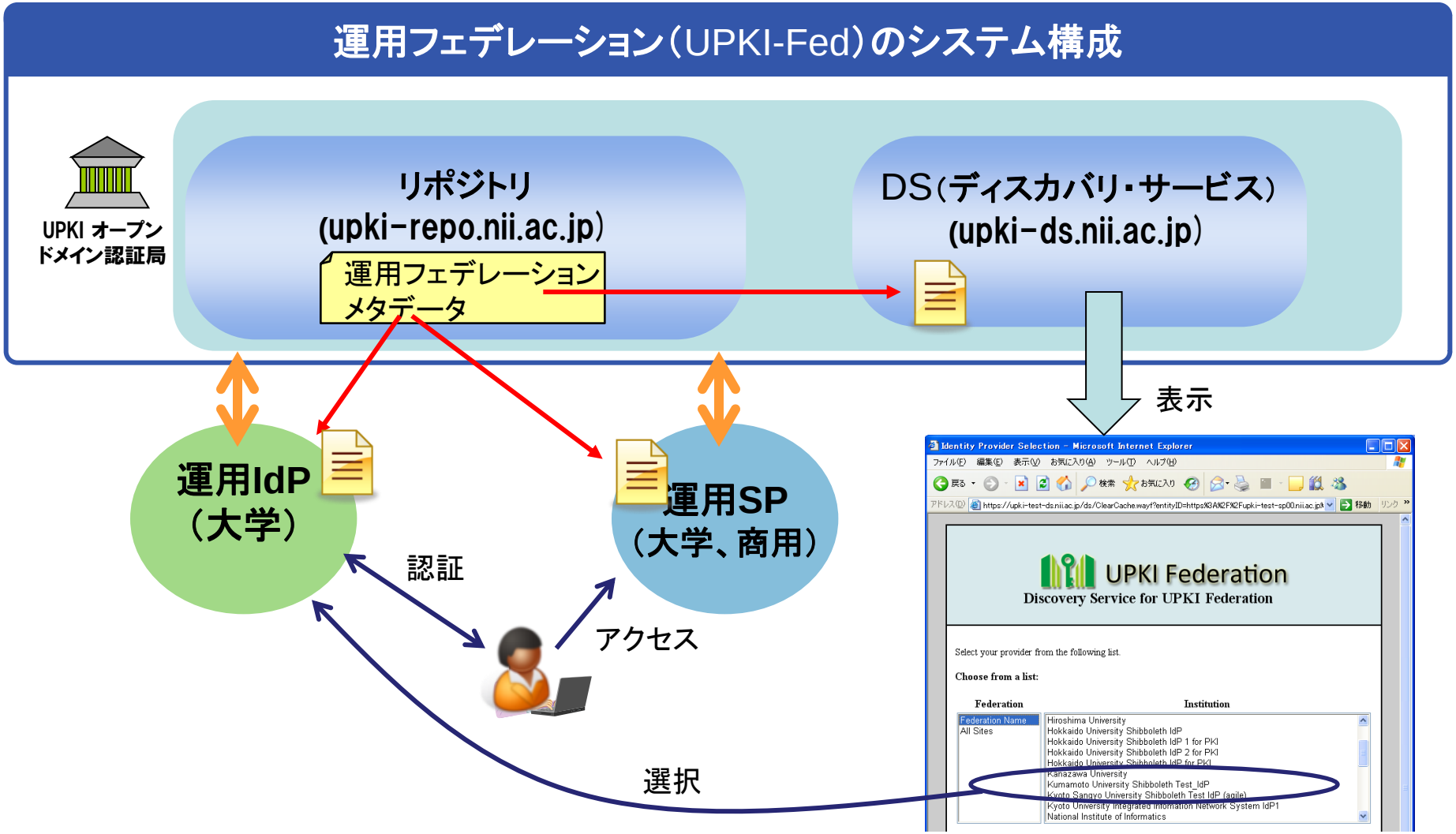
参加機関	機関名称	フェデレーション大学
	機関名称（英語表記）	The University of Federation

運用担当者	フリガナ	コクジョウ	イチロウ	所　属	情報センター
	氏　名	国情	一郎		
	職　名	技術職員		電話番号	03-4212-xxxx
	E-Mail	kokujo@fed.ac.jp			
	所属住所	〒101-0002　東京都千代田区一ツ橋2-1-2			

通信欄	

運用フェデレーション

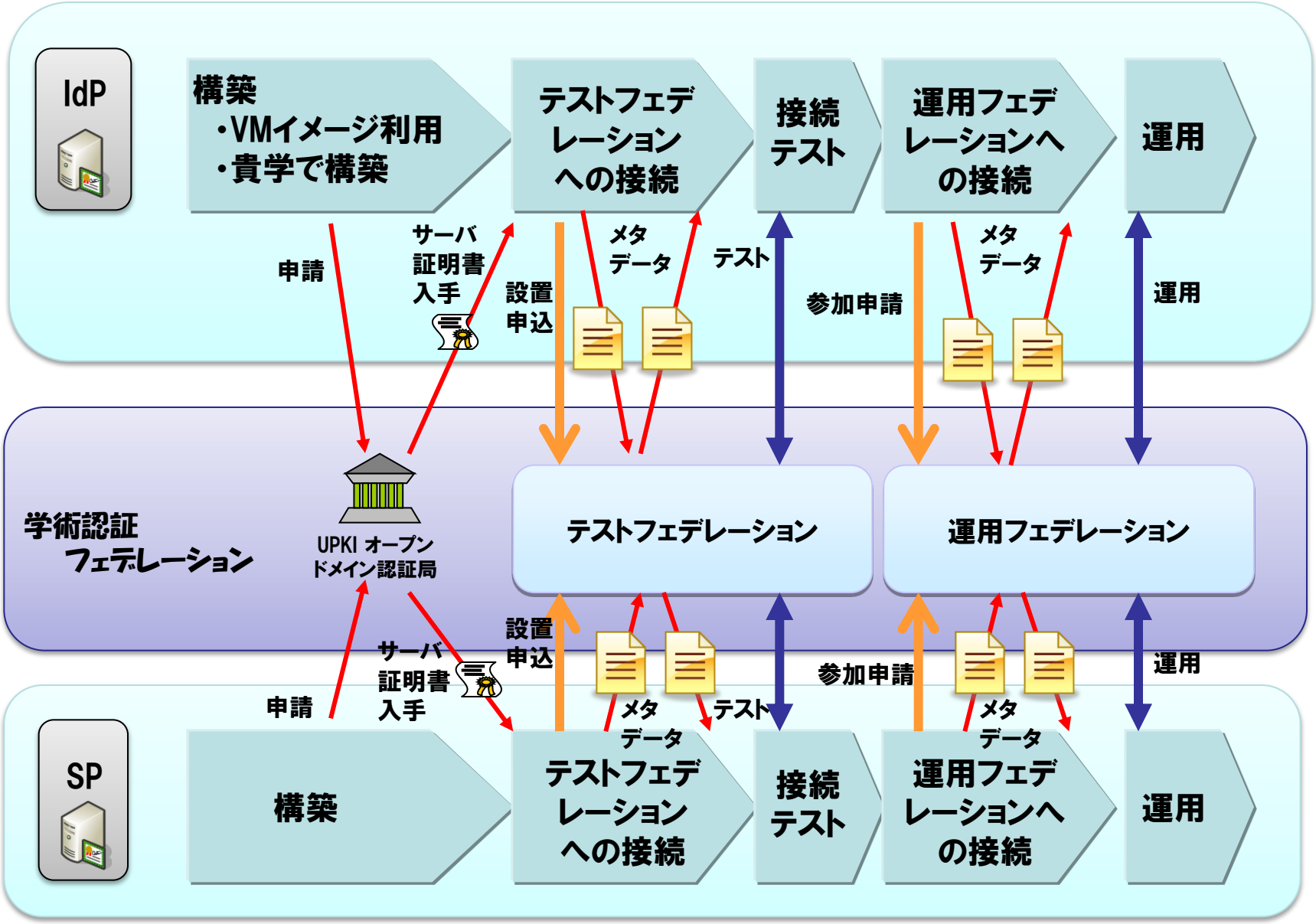
運用フェデレーション（UPKI-Fed）のシステム構成



- SPは，接続した人がどこの大学か判断できない
- DNSのようなもの必要 → DS

National Institute of Informatics

IdP／SPの構築と参加フロー



National Institute of Informatics

各種情報

1. 学術認証フェデレーションに関するWebサイト

   UPKIイニシアティブ 「学術認証フェデレーション」
   https ://upki-portal.nii.ac.jp/docs/fed

2. ポリシー、申請書

   UPKIイニシアティブ 「学術認証フェデレーション」ー「参加」
   https ://upki-portal.nii.ac.jp/docs/fed/join

3. IdP、SP構築ガイド

   UPKIイニシアティブ 「学術認証フェデレーション」ー「技術ガイド」
   https ://upki-portal.nii.ac.jp/docs/fed/technical

4. IdP構築用VMWareServerイメージ

   UPKIイニシアティブ 「学術認証フェデレーション」ー「技術ガイド」ー「IdP構築関連ファイル」
   https ://upki-portal.nii.ac.jp/docs/fed/technical/idp/files

5. テンプレート（メタデータ、IdP属性管理）

   学術認証フェデレーションのリポジトリ
   http ://upki-repo.nii.ac.jp/Template/index.html

6. 情報交換メーリングリスト（アーカイブ）

   UPKIイニシアティブ 「学術認証フェデレーション」ー「情報交換ML」
   https ://upki-portal.nii.ac.jp/docs/fed/ml