National Institute of Informatics

平成21年度情報処理軽井沢セミナー

2009年9月1日

シングルサインの基礎知識

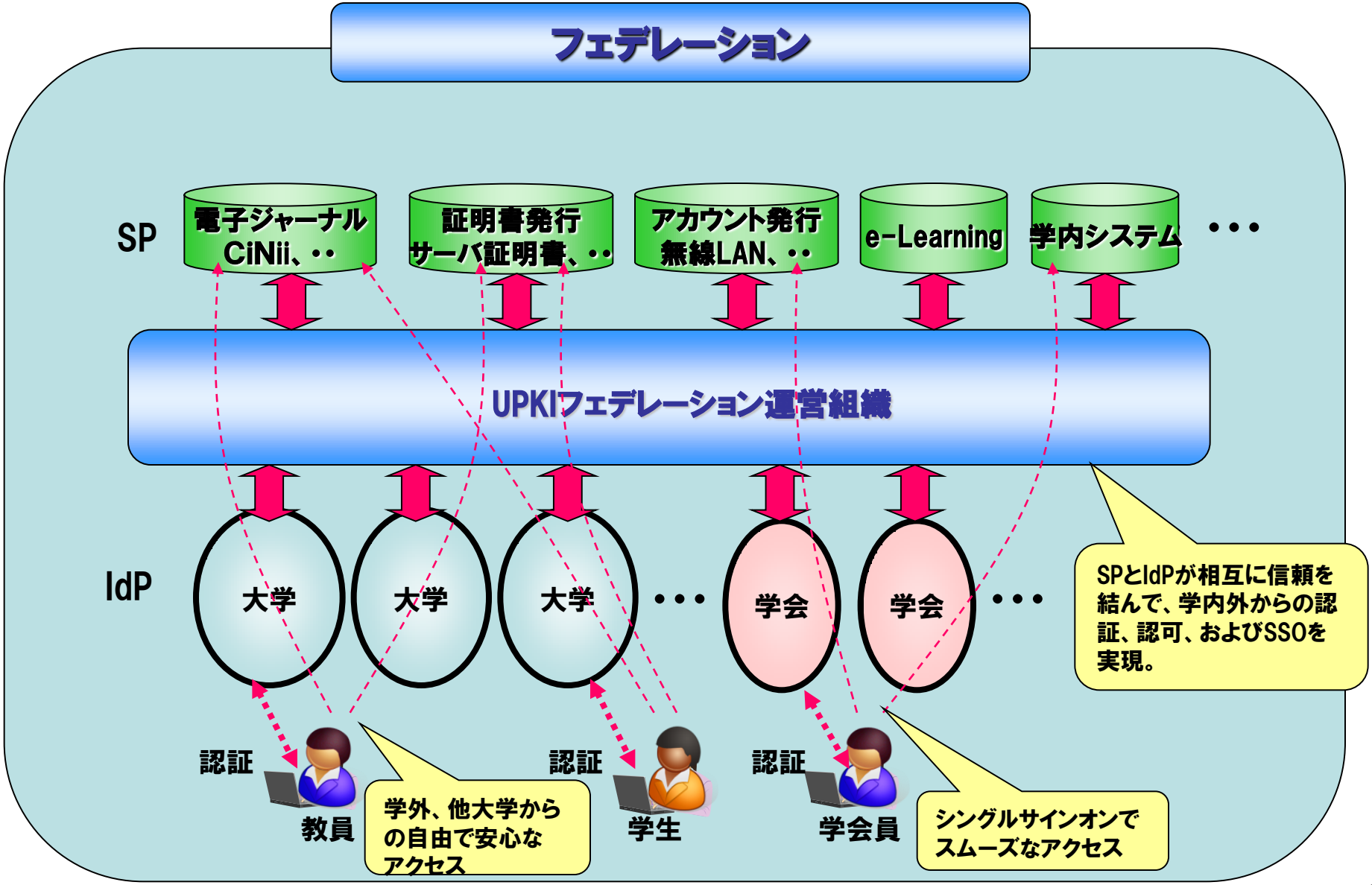
～ 学術認証フェデレーションについて ～

国立情報学研究所

片岡　俊幸

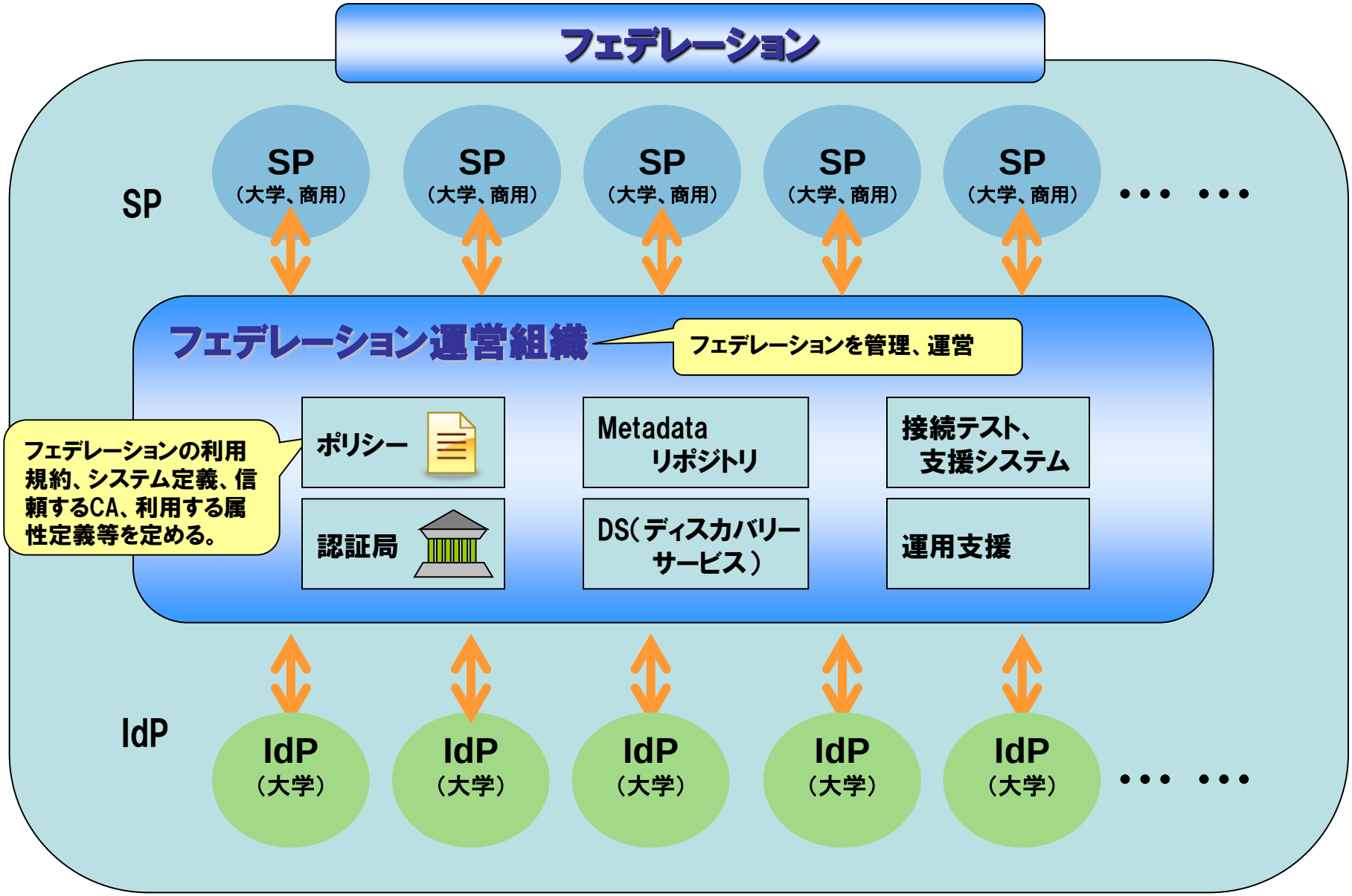
National Institute of Informatics

フェデレーションとは？



National Institute of Informatics

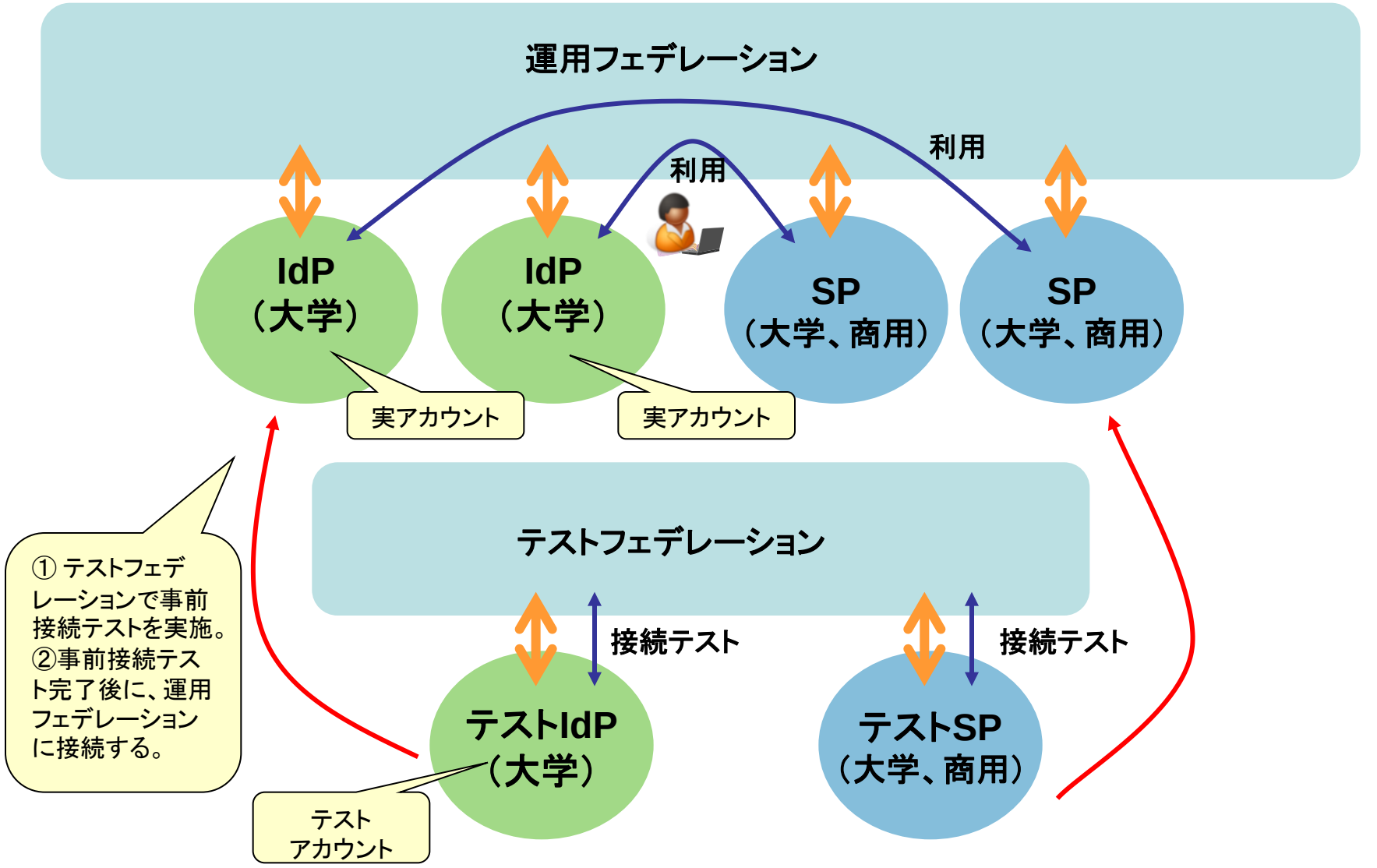
フェデレーションとは？



学術認証フェデレーション

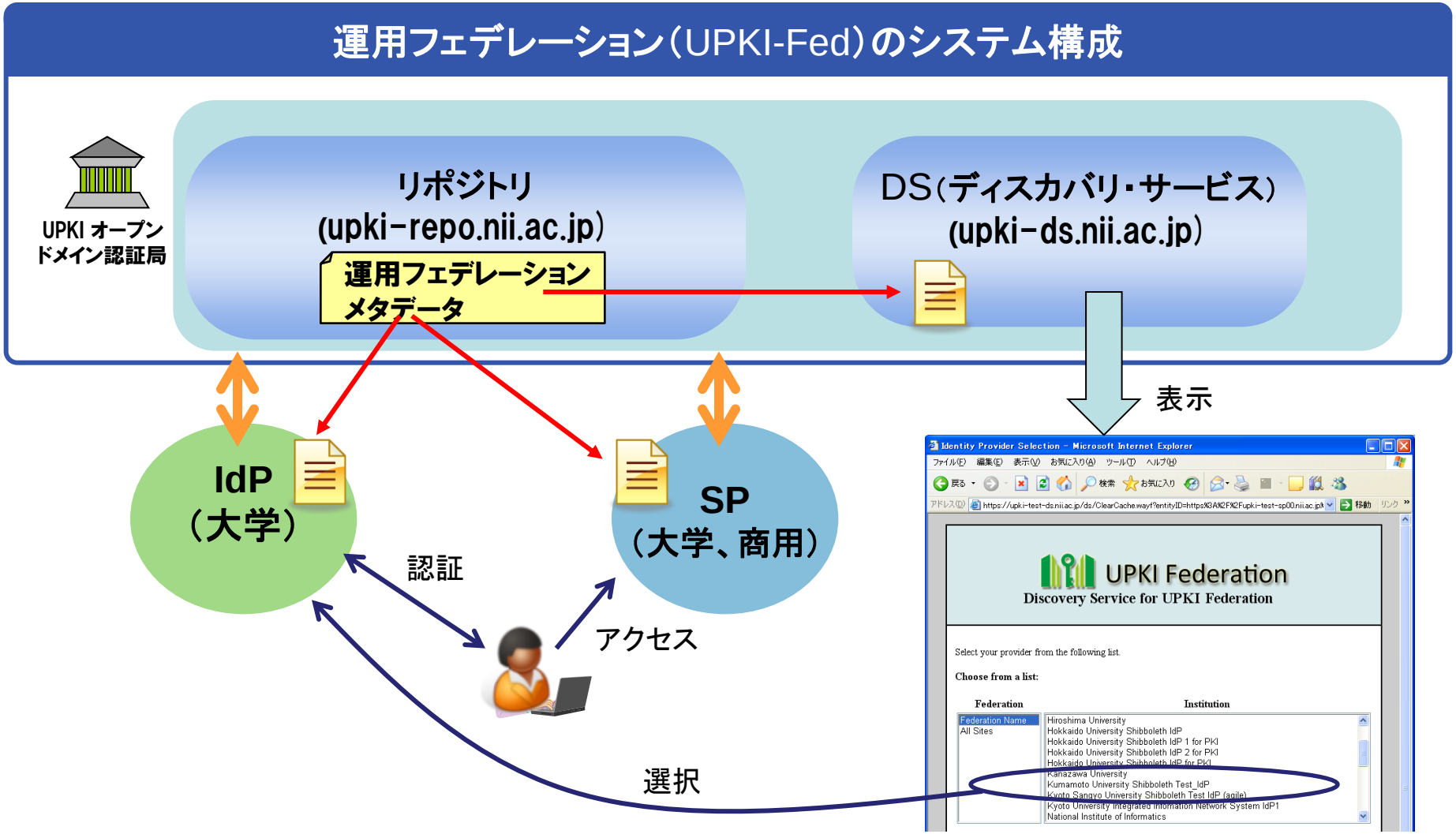
National Institute of Informatics

学術認証フェデレーションの構成



運用フェデレーション

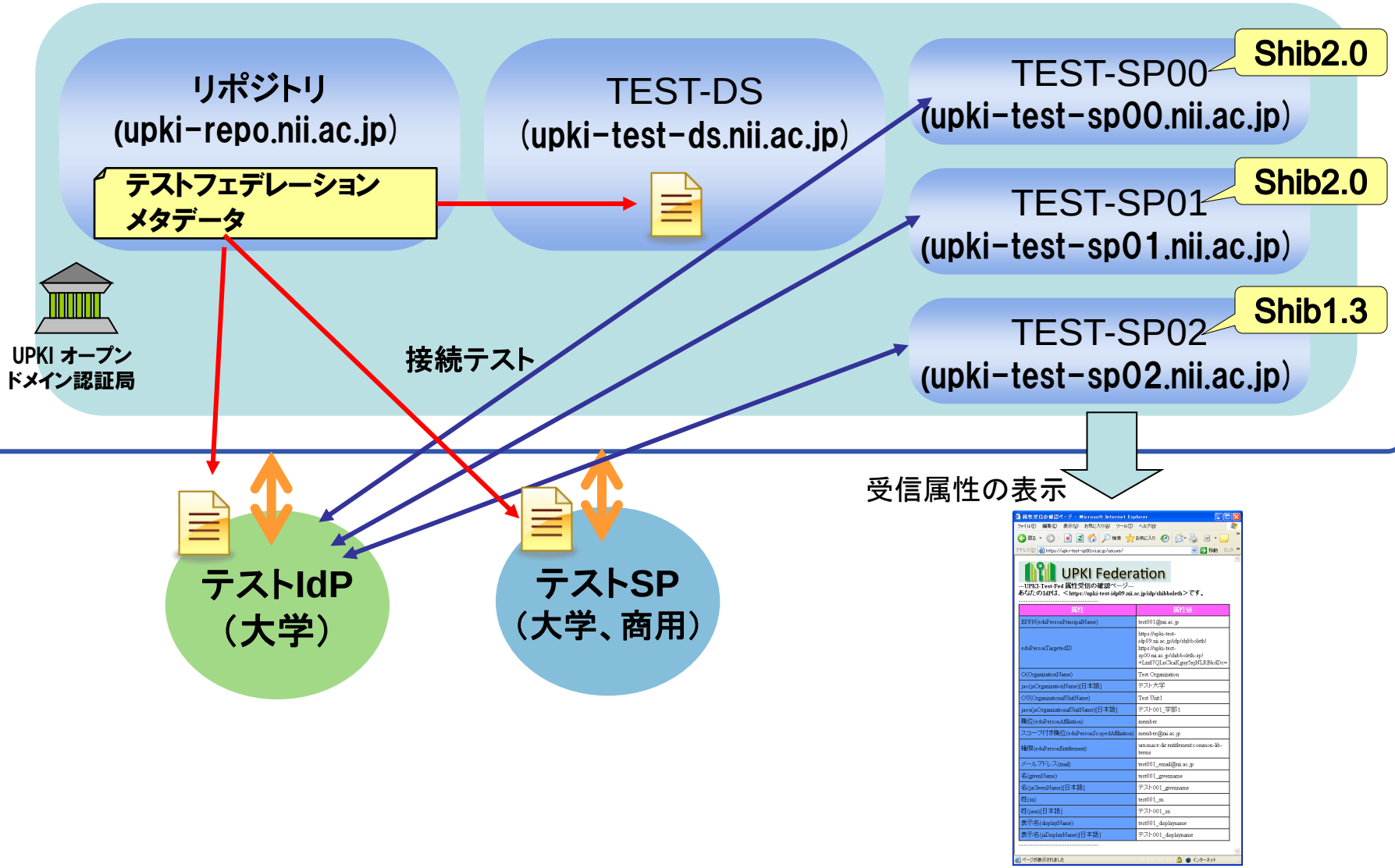
運用フェデレーション（UPKI-Fed）のシステム構成



National Institute of Informatics

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

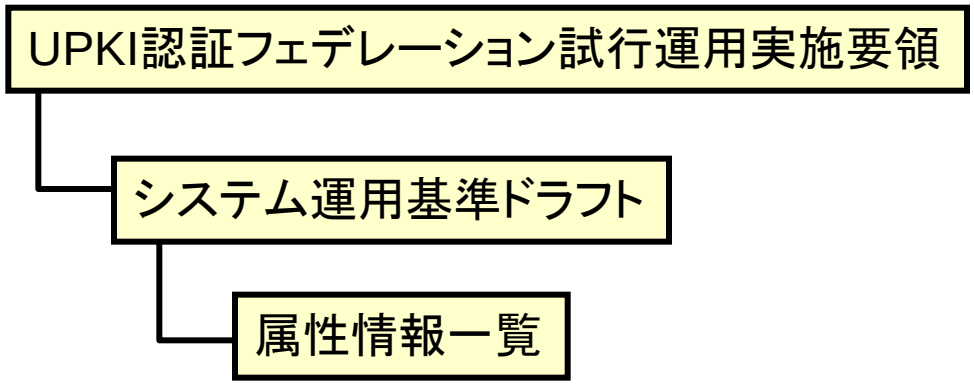


National Institute of Informatics

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、ポリシー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

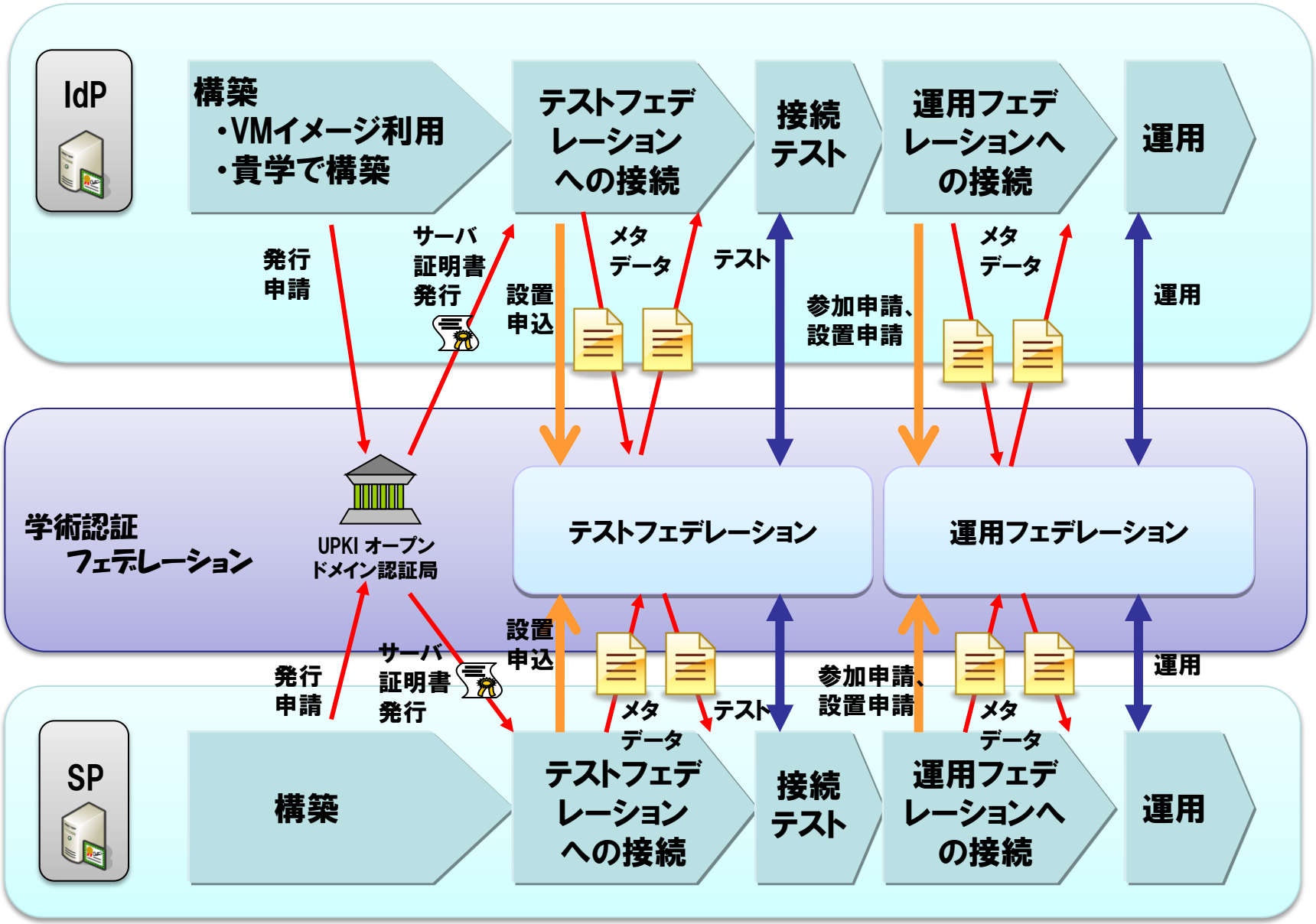


- **システム運用基準は、現在ドラフトであり、試行運用を実践しながらブラッシュアップを行い、システム運用基準V1.0策定を目指しています。**
  そのため、各参加機関の状況、視点から様々なご意見をお伺い、また、一緒に協議しながら策定していく予定です。

- **テストフェデレーションでは、できる限り本ポリシーの遵守をお願い致しますが、各システム、および、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。**

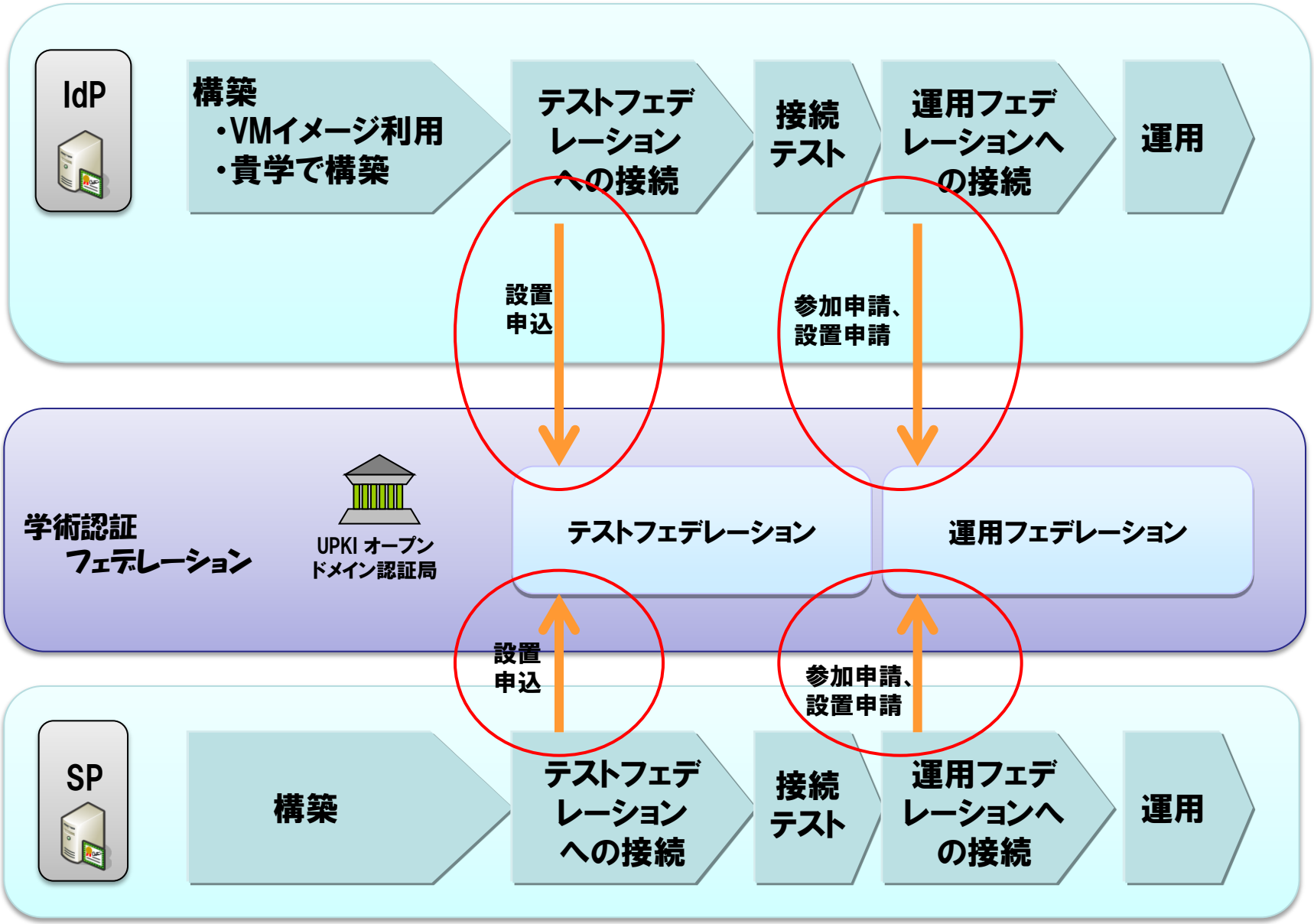
National Institute of Informatics

IdP／SPの構築と参加フロー



National Institute of Informatics

IdP／SPの構築と参加フロー



National Institute of Informatics

テストフェデレーション参加手続き

1. IdP／SP設置申込

参加機関（運用担当者） → 学術認証フェデレーション試行運用PJ事務局

必要項目：運用担当者 および EntityIDの決定
提出書類：「IdP設置申込書」（様式1） または「SP設置申込書」（様式2）
送付先：　NII 基盤企画課 認証担当
送付媒体：　エクセルファイル

詳細は、「各種申請書記入のてびき」をご覧下さい。
また、てびき、および各様式は、下記に掲載しております。
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

IdP設置申込書（様式1記入例）

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		

運用フェデレーション参加手続き

1. 参加申請

参加機関（申請者） → NII学術情報ネットワーク運営・連携本部長

必要項目：運用責任者の決定
参加機関名称（英語、日本語）の確認
提出書類：「学術認証フェデレーション試行運用 参加申請書（様式3）
送付先： NII 基盤企画課 認証担当
送付媒体： エクセルファイル および 原紙（押印必要）

2. 参加承認通知

NII学術情報ネットワーク運営・連携本部長 → 参加機関（申請者）

3. IdP／SP設置申請

参加機関（運用責任者） → NII学術情報ネットワーク運営・連携本部長

必要項目：EntityIDの決定
提出書類：「IdP設置申請書」（様式4）または「SP設置申請書」（様式5）
送付先： NII 基盤企画課 認証担当
送付媒体： エクセルファイル および 原紙（押印必要）

詳細は、「各種申請書記入のてびき」をご覧下さい。
また、てびき、および各様式は、下記に掲載しております。
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

National Institute of Informatics

参加申請書（様式3記入例）

様式 3

平成21年7月1日

UPKI認証フェデレーション試行運用 参加申請書

国立情報学研究所
学術情報ネットワーク運営・連携本部長　殿

申請者役職：情報センター長
申請者氏名：認証 太郎

印

UPKI認証フェデレーション試行運用実施要領を遵守し，次のとおり試行運用に参加申請いたします。

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。）

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

運用責任者	フリガナ	タケバシ　ハナコ	所　属	情報センター
	氏　名	竹橋　花子		
	職　名	准教授	電話番号	03-4212-xxxx
	E-Mail	hanako@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	

National Institute of Informatics

IdP設置申請書（様式4記入例）

様式4

平成21年7月1日

UPKI認証フェデレーション試行運用　IdP設置申請書

国立情報学研究所
学術情報ネットワーク運営・連携本部長　殿

運用責任者役職：情報センター事務課長
運用責任者氏名：連携　次郎

印

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

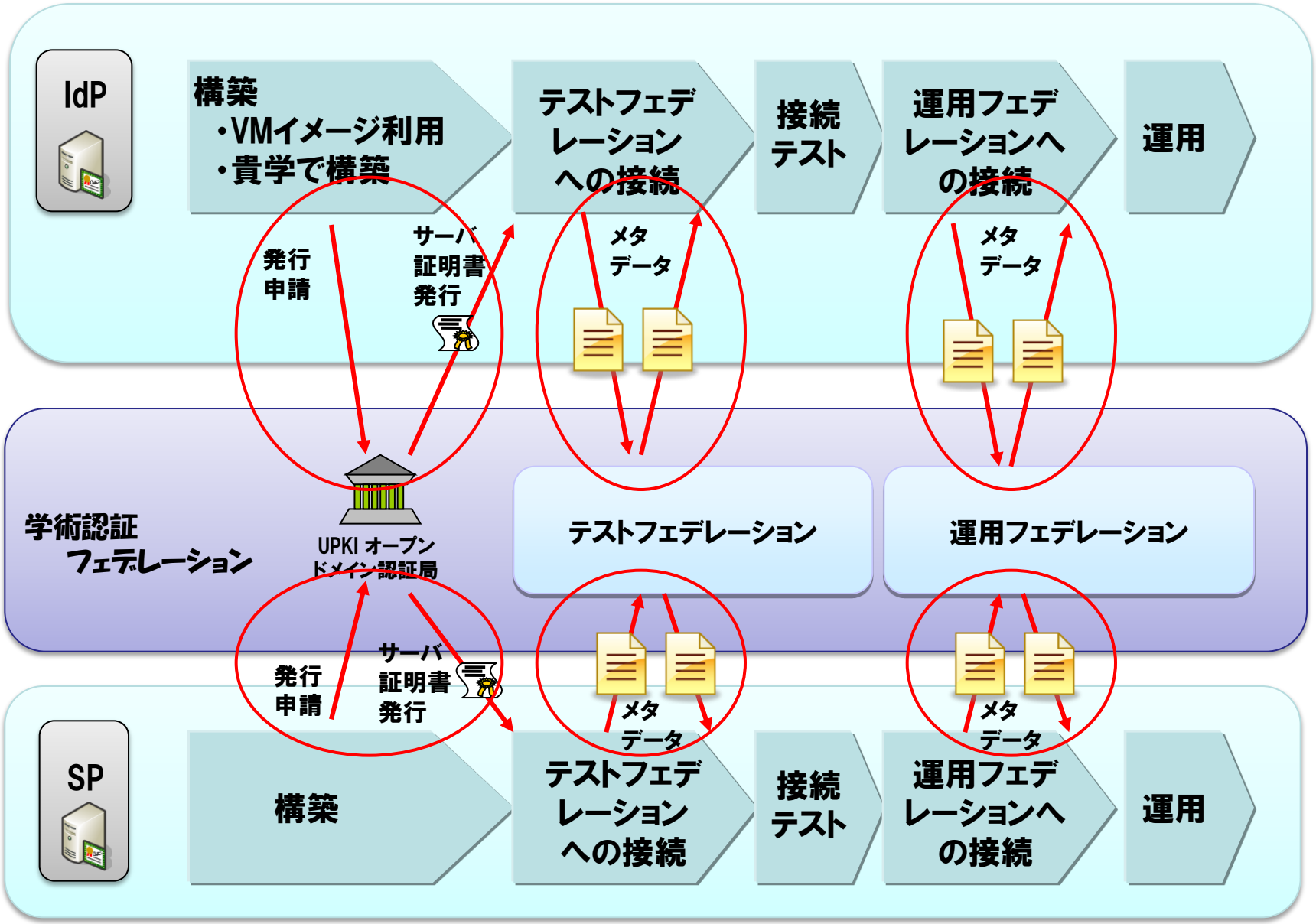
申込区分	☑ 新規　☐ 変更　☐ 中止	（中止の場合は，連絡欄にその理由をご記入ください。）

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
	対象とする構成員の範囲	工学部の構成員（学生・教職員）を対象とする。
運用開始日	平成21年10月1日	

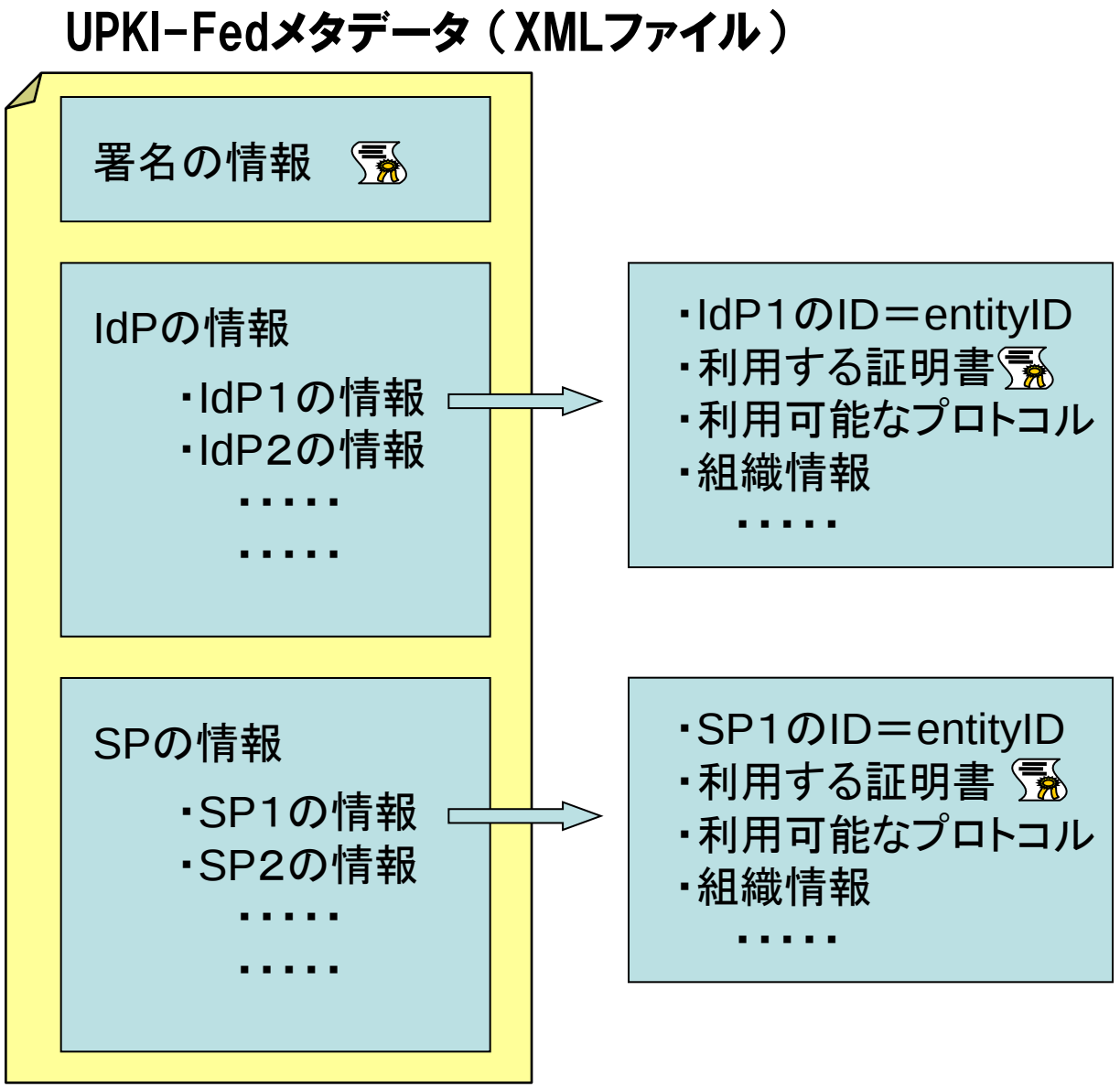
運用担当者	フリガナ	コクジョウ　イチロウ	所　属	情報センター
	氏　名	国情　一郎		
	職　名	技術職員	電話番号	03-4212-xxxx
	E-Mail	kokujo@fed.ac.jp		
	所属住所	〒101-0003　東京都千代田区一ツ橋2-1-2		

IdP／SPの構築と参加フロー



National Institute of Informatics

メタデータの構成



サーバ証明書取得とメタデータ提出

1. サーバ証明書の取得

「UPKIオープンドメイン証明書自動発行検証プロジェクト」
（https://upki-portal.nii.ac.jp/docs/odcert）
の「利用の手引き」にしたがい、サーバ証明書発行申請を行い、サーバ証明書を取得下さい。

2. メタデータの作成

メタデータのテンプレートをリポジトリ（https://upki-repo.nii.ac.jp/Template）からダウンロードします。1. で入手した証明書の内容を入れ、サーバ名、組織名等を修正します。

テンプレートは、下記を提供しています。

（1）idp-metadata-template.xml
（2）sp-metadata-template.xml

3. メタデータの提出

参加機関（運用責任者、運用担当者） → NII 基盤企画課 認証担当

必要項目：メタデータの作成
提出書類：メタデータファイル
送付先：　ヘルプデスク（upki-sso-help@nii.ac.jp）
送付媒体：xmlファイル

学術認証フェデレーションの属性

学術認証フェデレーションでは、下記16種類の属性を定めています。

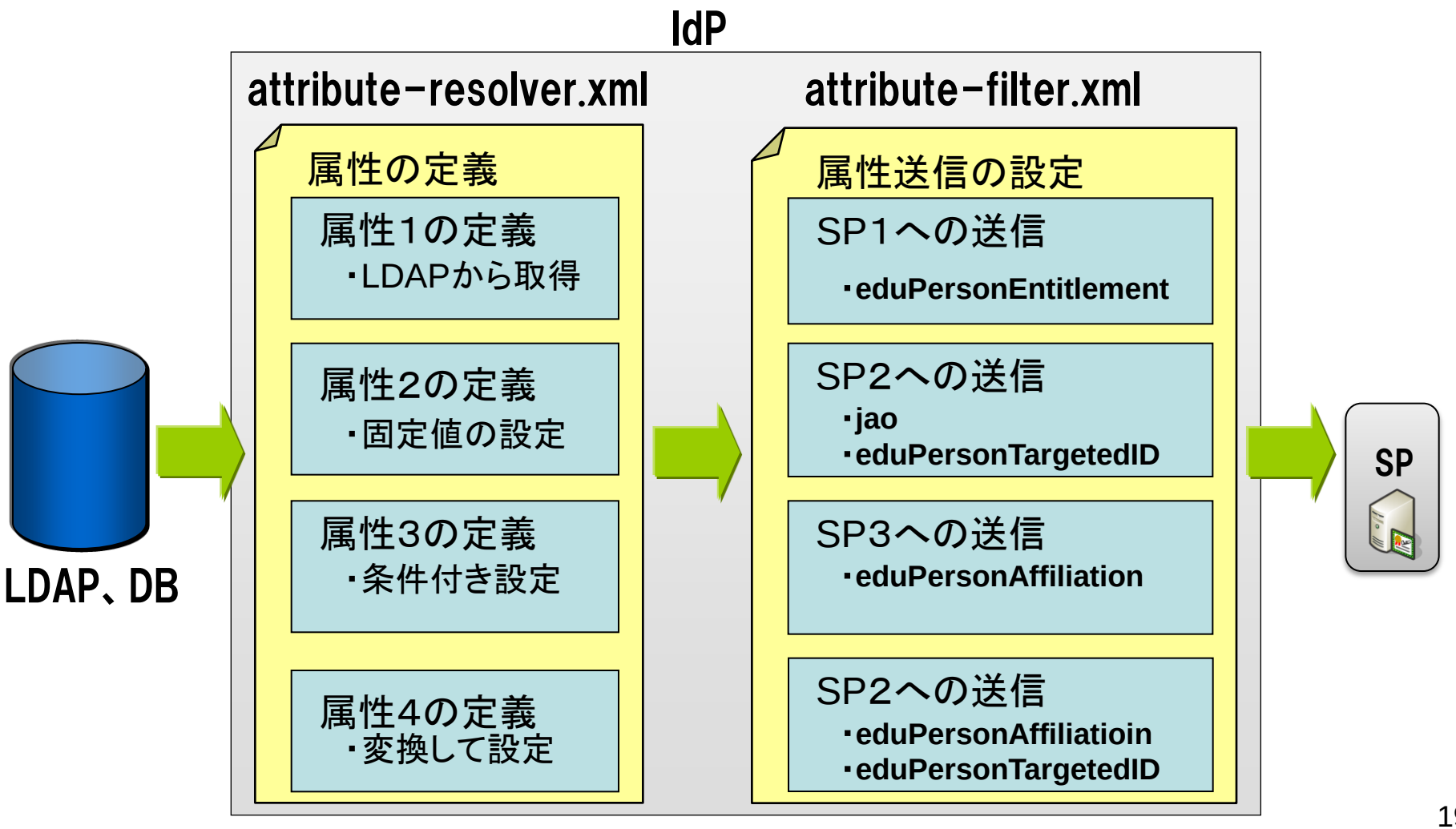
属性	内容
OrganizationName (o)	組織名
jaOrganizationName (jao)	組織名（日本語）
OrganizationalUnit (ou)	組織内所属名称
jaOrganizationalUnit (jaou)	組織内所属名称（日本語）
eduPersonPrincipalName (eppn)	フェデレーション内のアイデンティティ
eduPersonTargetedID	フェデレーション内のアイデンティティ
eduPersonAffiliation	職種
eduPersonScopedAffiliation	職種（スコープ付き）
eduPersonEntitlement	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

属性の送信管理

属性管理ファイルのテンプレートを提供しています。
リポジトリ（https://upki-repo.nii.ac.jp/Template）からダウンロード下さい。



Shibbolethとは？

Shibboleth公式ページ: http://shibboleth.internet2.edu/

Shibbolethの情報: https://spaces.internet2.edu/display/SHIB2/Home

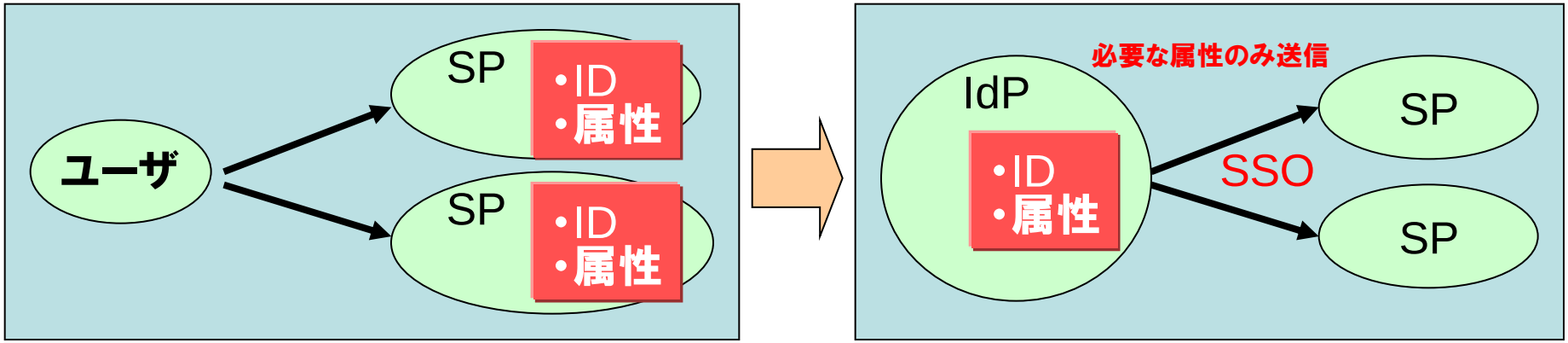
- 米国EDUCAUSE／Internet2にて2000年に発足したプロジェクト
- SAML、eduPerson等の標準仕様を利用した、認可のための属性交換を行う標準仕様とオープンソフト
- 最新版はShibboleth V2.2

  （SAML2.0ベース、Shib2.0は2008年3月リリース）
- 米国、欧州でShibbolethのFederation利用が拡大

National Institute of Informatics

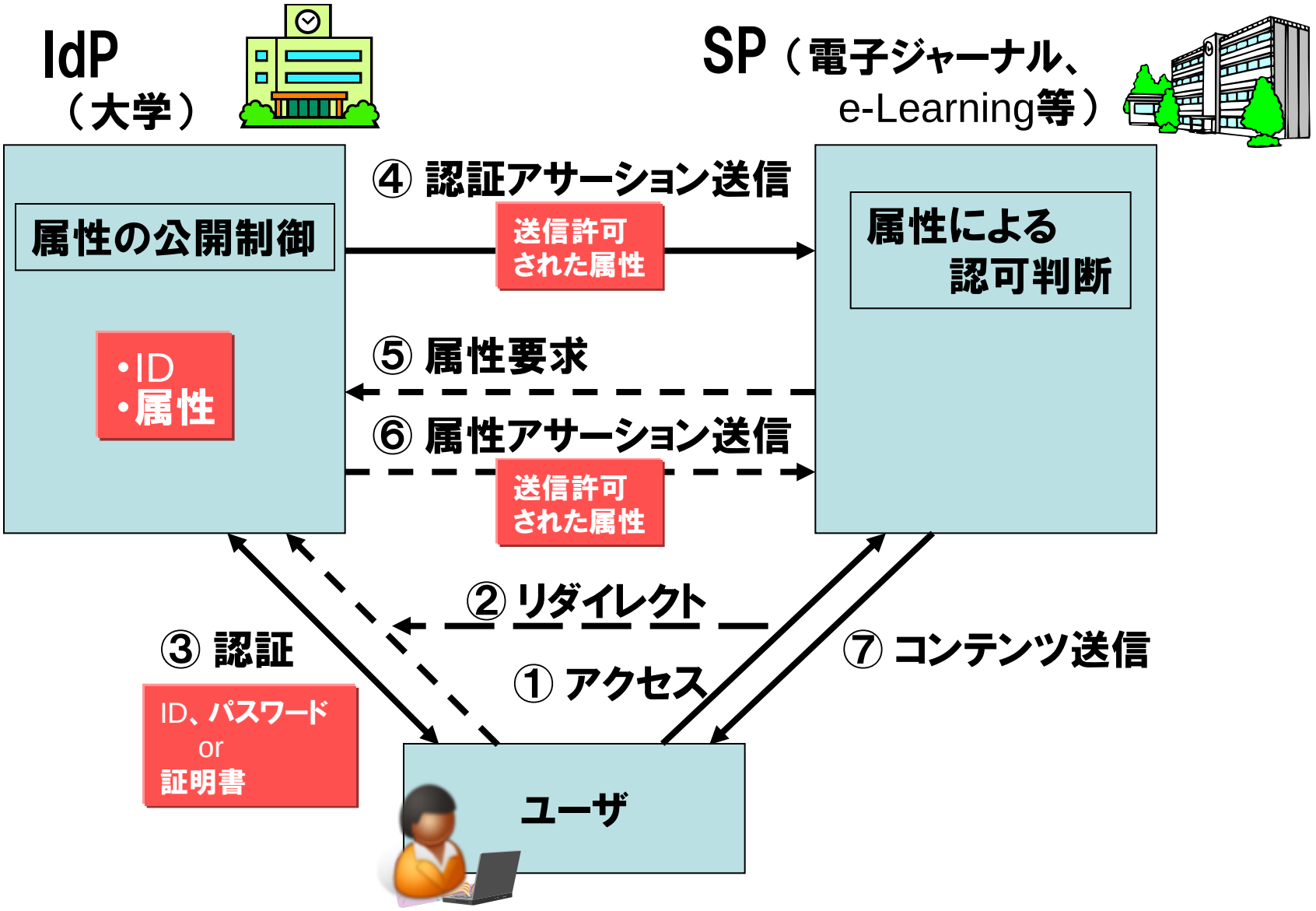
Shibbolethの特徴

（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
　学内外のWebサービスへのシングルサインオンを実現
（3）プライバシ保護
　ユーザはID、パスワードを常に自学のIdPにのみ入力
　IdPは各SPが必要とする最小限の属性のみを送付

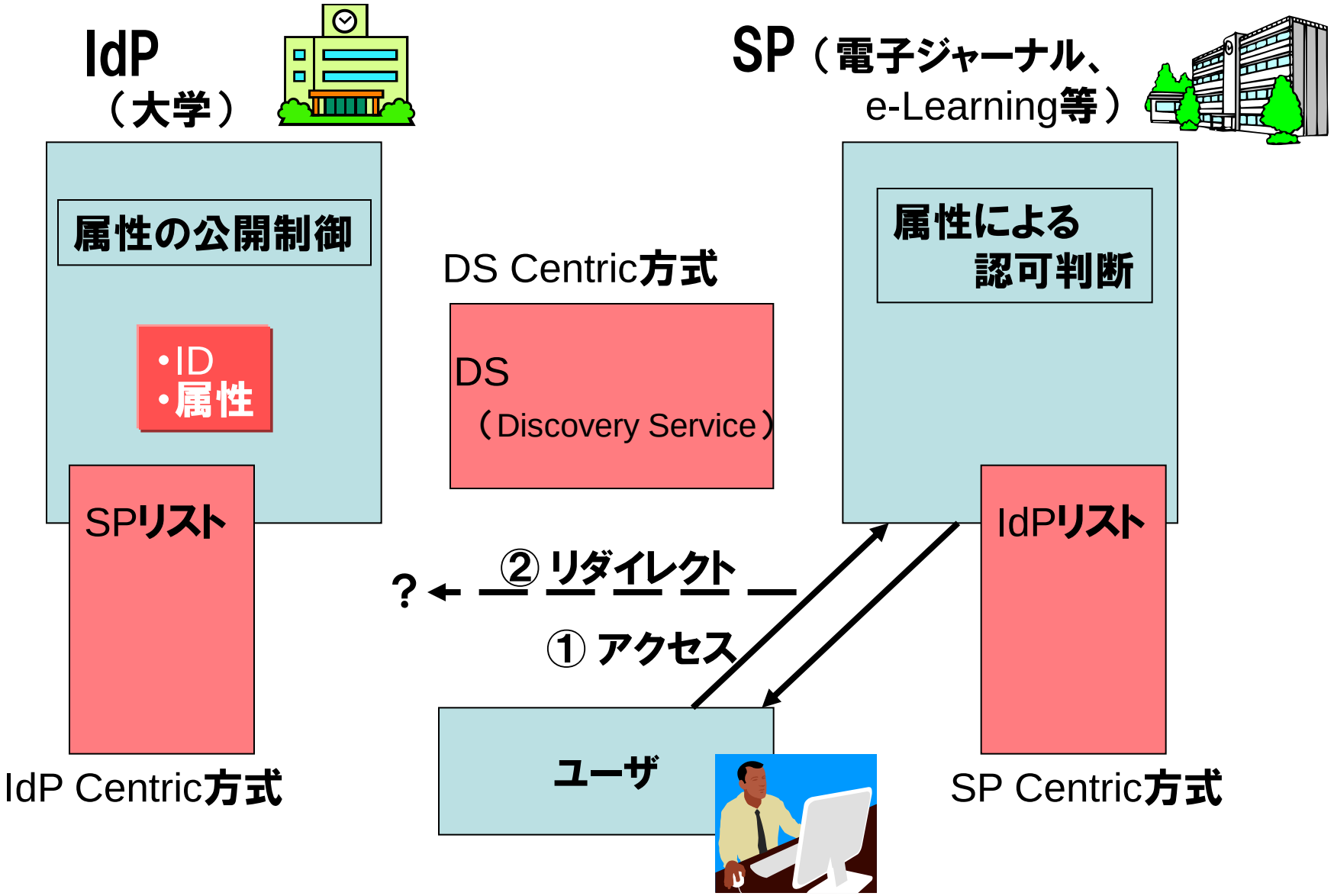


National Institute of Informatics

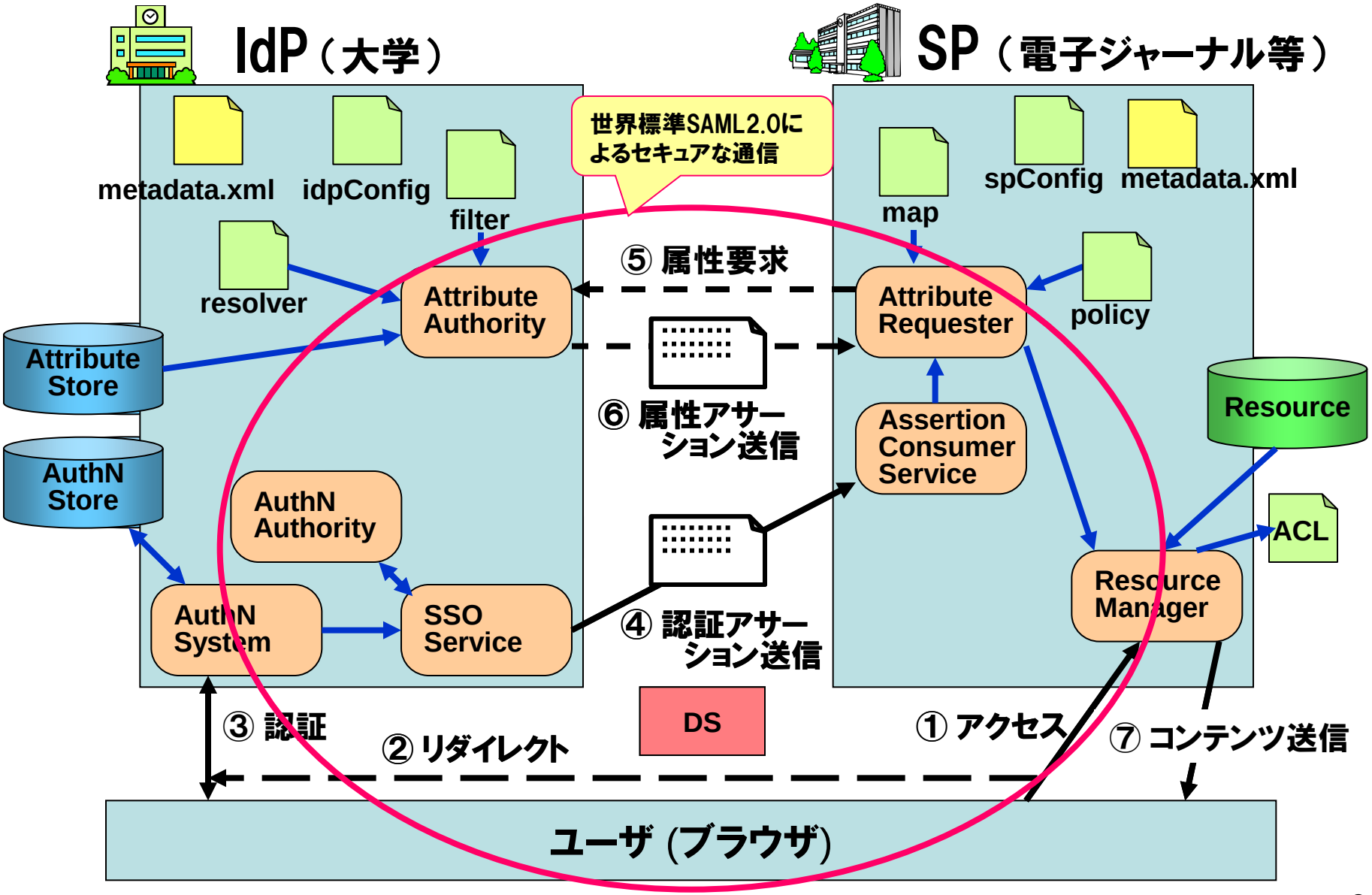
Shibbolethの基本動作



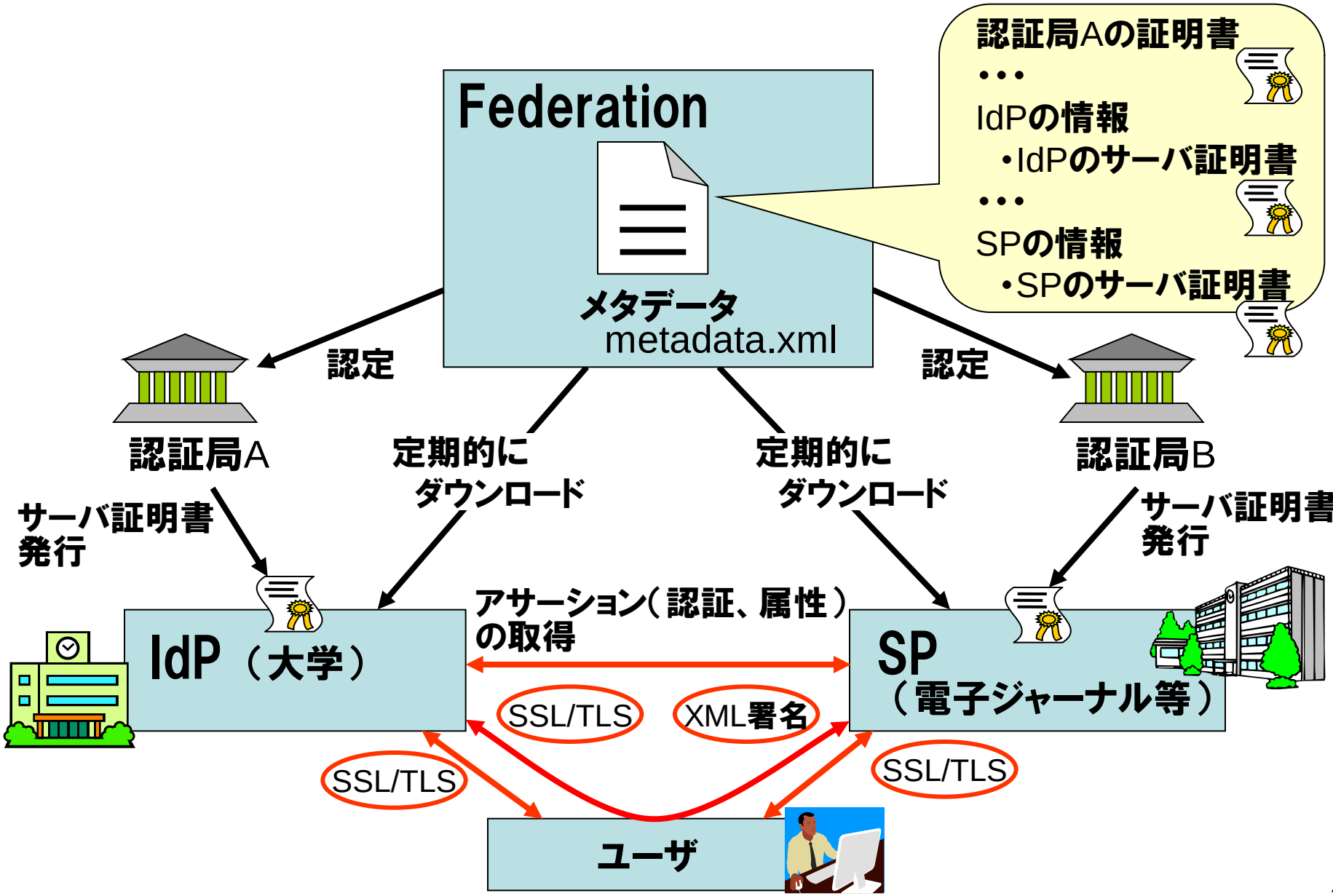
IdP Discovery



1－5．Shibbolethの動作



2－4．FederationとPKI



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