Shibboleth, 学認 を知ろう

国立情報学研究所・佐賀大学　大谷　誠

学認CAMP
～ GakuNin Campus Architecture and Middleware Planning ～

話の流れ

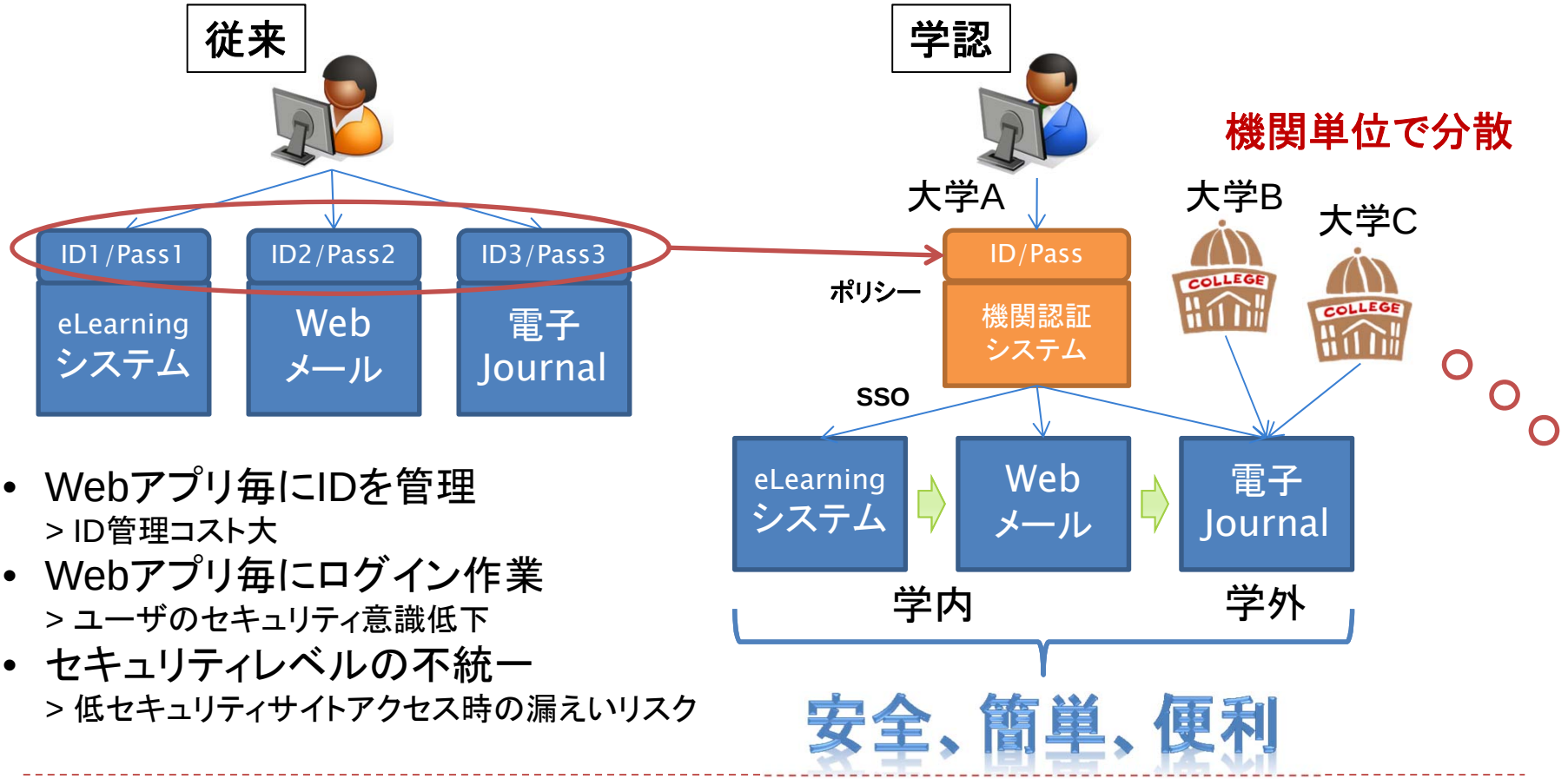
- 学術認証フェデレーション(学認)とは
- 学認の現状
- Shibboleth の概要とその動作

話の流れ

- 学術認証フェデレーション(学認)とは
- 学認の現状
- Shibboleth の概要とその動作

学術認証フェデレーション「学認」とは

- Webアプリケーションへのシングル・サイン・オン（SSO）技術を、組織を越えて活用する分散型学術認証基盤



- Webアプリ毎にIDを管理
  > ID管理コスト大
- Webアプリ毎にログイン作業
  > ユーザのセキュリティ意識低下
- セキュリティレベルの不統一
  > 低セキュリティサイトアクセス時の漏えいリスク

学術認証フェデレーション「学認」とは

- 学術認証フェデレーション
  - Webアプリケーションへのシングル・サイン・オン（SSO）技術を、組織を越えて活用する分散型学術認証基盤
    - 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
    - **機関（IdP）がIDと個人の情報(属性)**を管理し，**サービス提供者（SP）**がそれを利用して認可
- プライバシ保護を考慮したシングルサインオン（SSO）技術
  - 一度の認証で複数のSPを利用
  - ユーザの一意性を保証しつつ、必要な個人情報以外は出さない
    - 必要な属性のみをIdPから取得
  - ユーザは、各SPに対する属性の公開を、制御(制限)することも可能

学認で主に利用されているミドルウエア

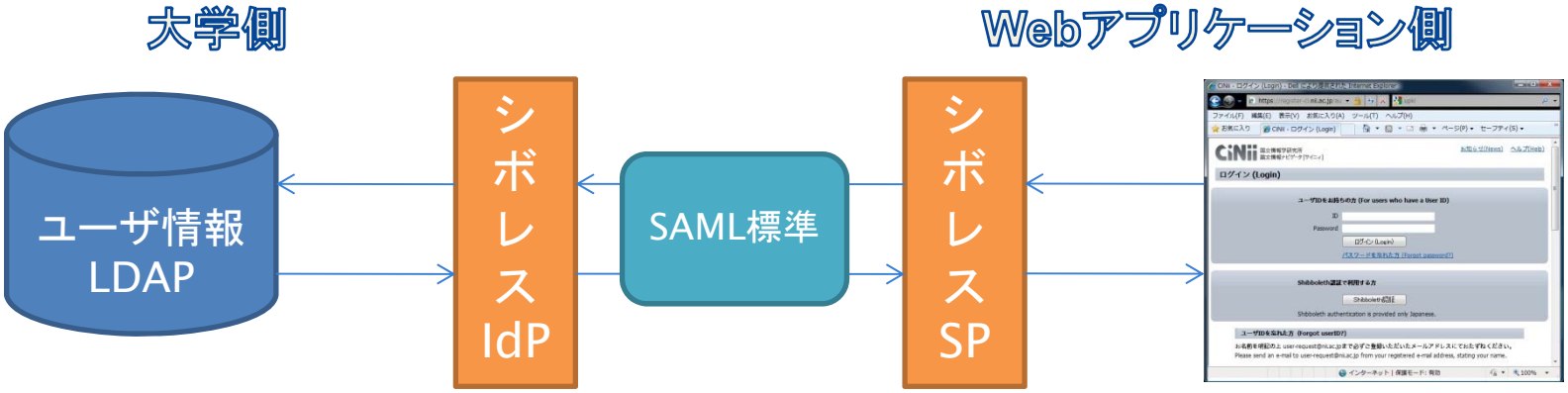
SAML（サムル：Security Assertion Markup Language）

- セキュリティや個人情報保護法に配慮して，認証・認可の情報交換を行うためのデータ形式
- 標準団体OASISにより策定

Shibboleth（シボレス）

ShibbolethはSAMLを実現するミドルウエア

- 米国EDUCAUSE／Internet2にて2000年に発足したオープンソースプロジェクト
  - http://shibboleth.internet2.edu/
- SAMLによる認証連携方法として学術界ではデファクトスタンダード
  - 米国、欧州でShibbolethによる学術認証フェデレーションが拡大

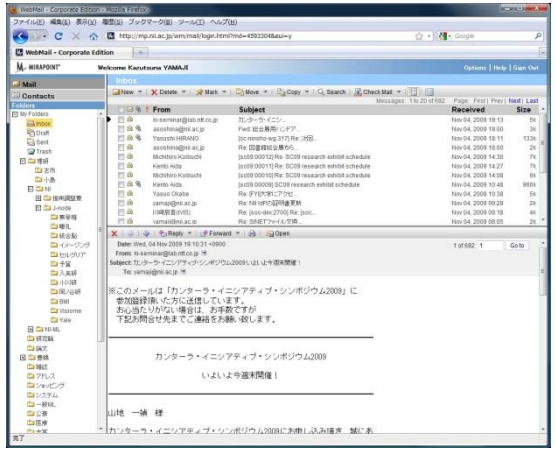


SAML通信のためのフィルタのようなもの

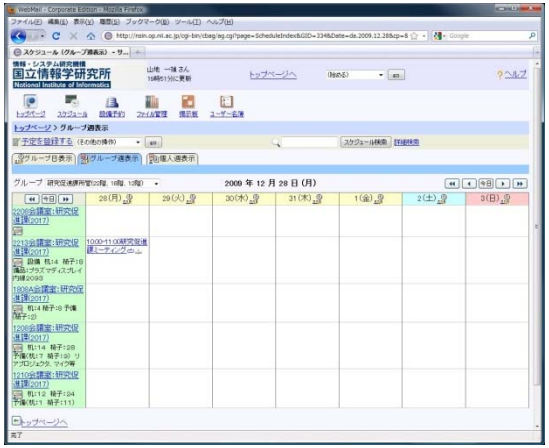
具体的な利用例（学内SSOの整備）

- 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の構築を加速化
  - 学内システムのSSO化を加速化
- 学内の公開Webサービスのセキュリティレベルの向上

Webメール



グループウエア

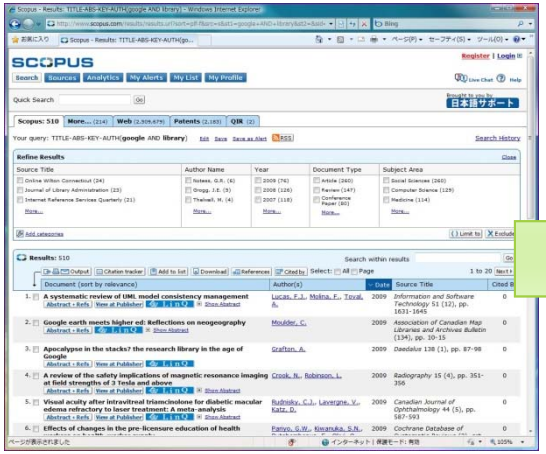


図書館システム

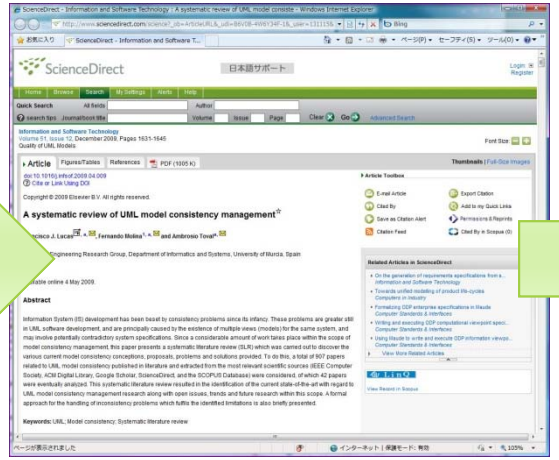
具体的な利用例（電子ジャーナル）

- 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

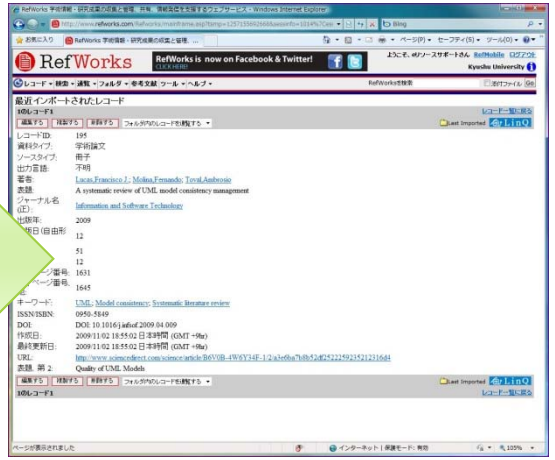
論文を探して



論文を取得して（読んで）



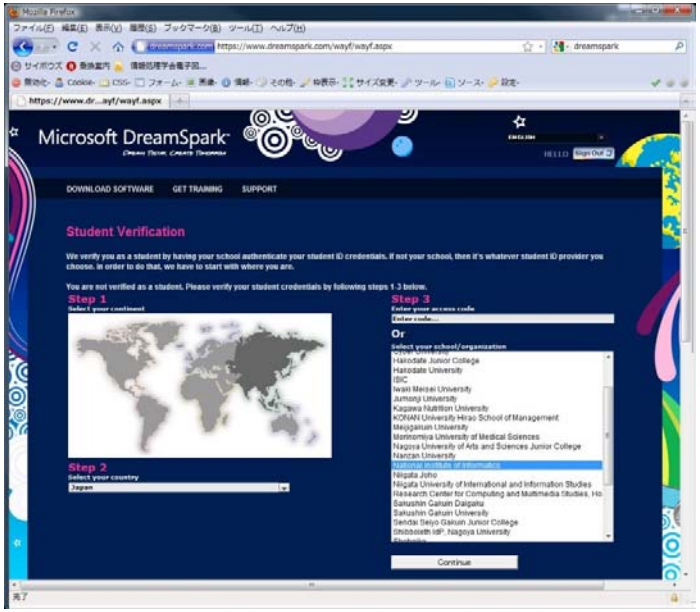
論文を管理する



認証連携によるディープなマッシュアップ

具体的な利用例（アカデミック配付）

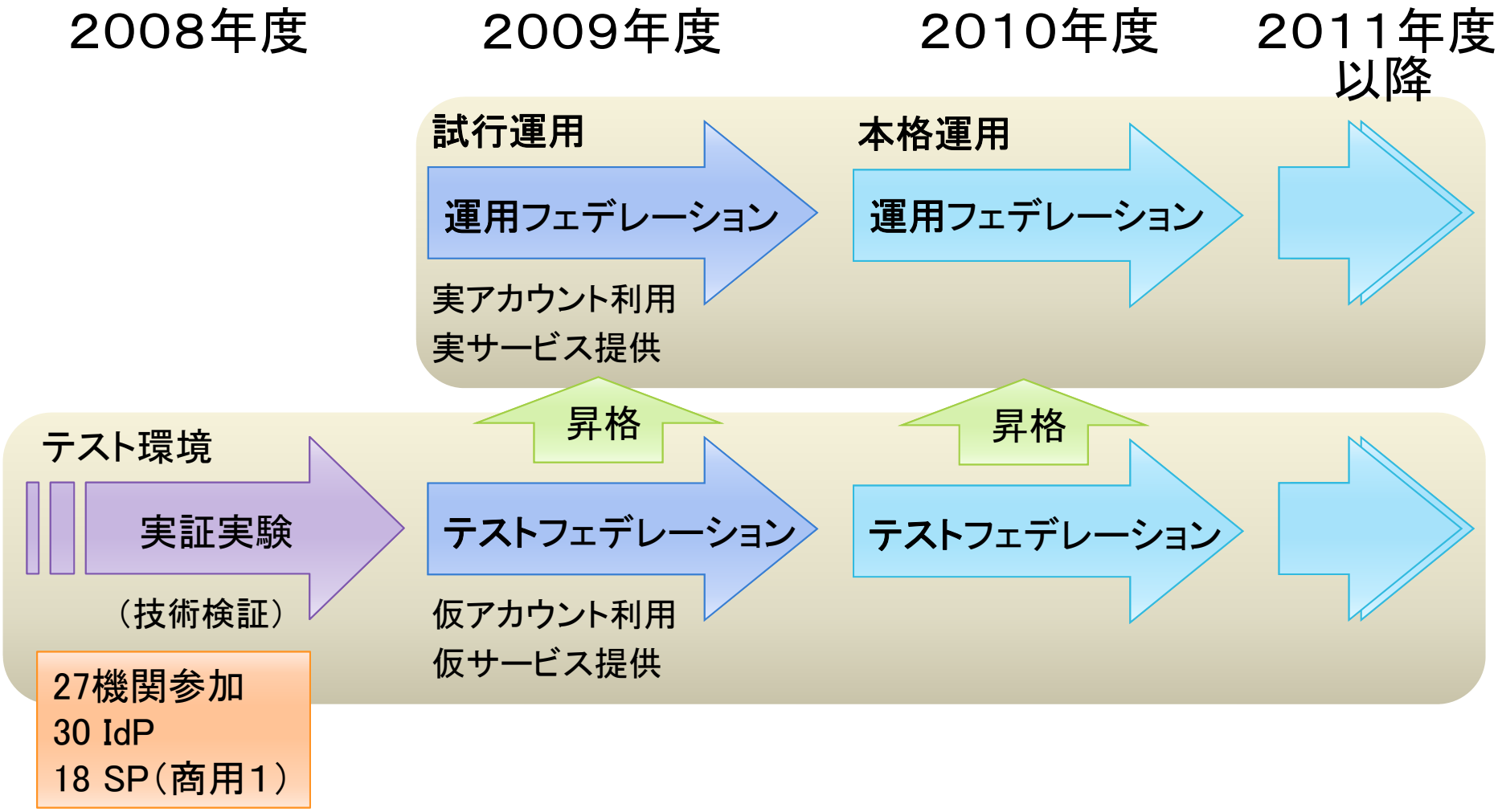
- Microsoft DreamSpark
  - 学生を対象にMSのソフトウエア開発環境を無償で提供するプログラム
- 属性により大学構成員であり、学生であることを確認
  - eduPersonTargetedID（SP毎に異なるハッシュ化された一意のID）
  - eduPersonScopedAffiliation（例：student@nii.ac.jp）



話の流れ

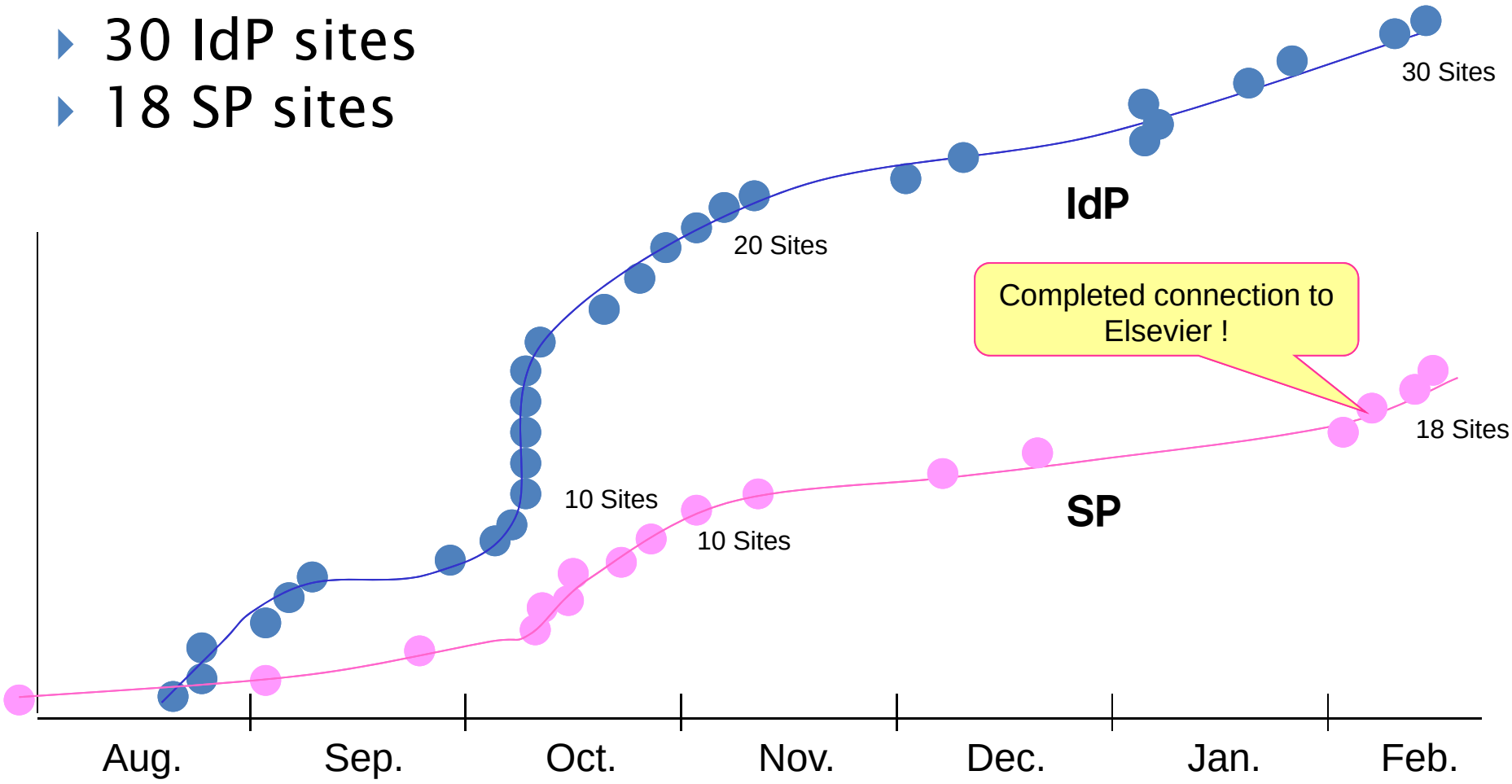
- 学術認証フェデレーション(学認)とは
- 学認の現状
- Shibboleth の概要とその動作

学認の歩み

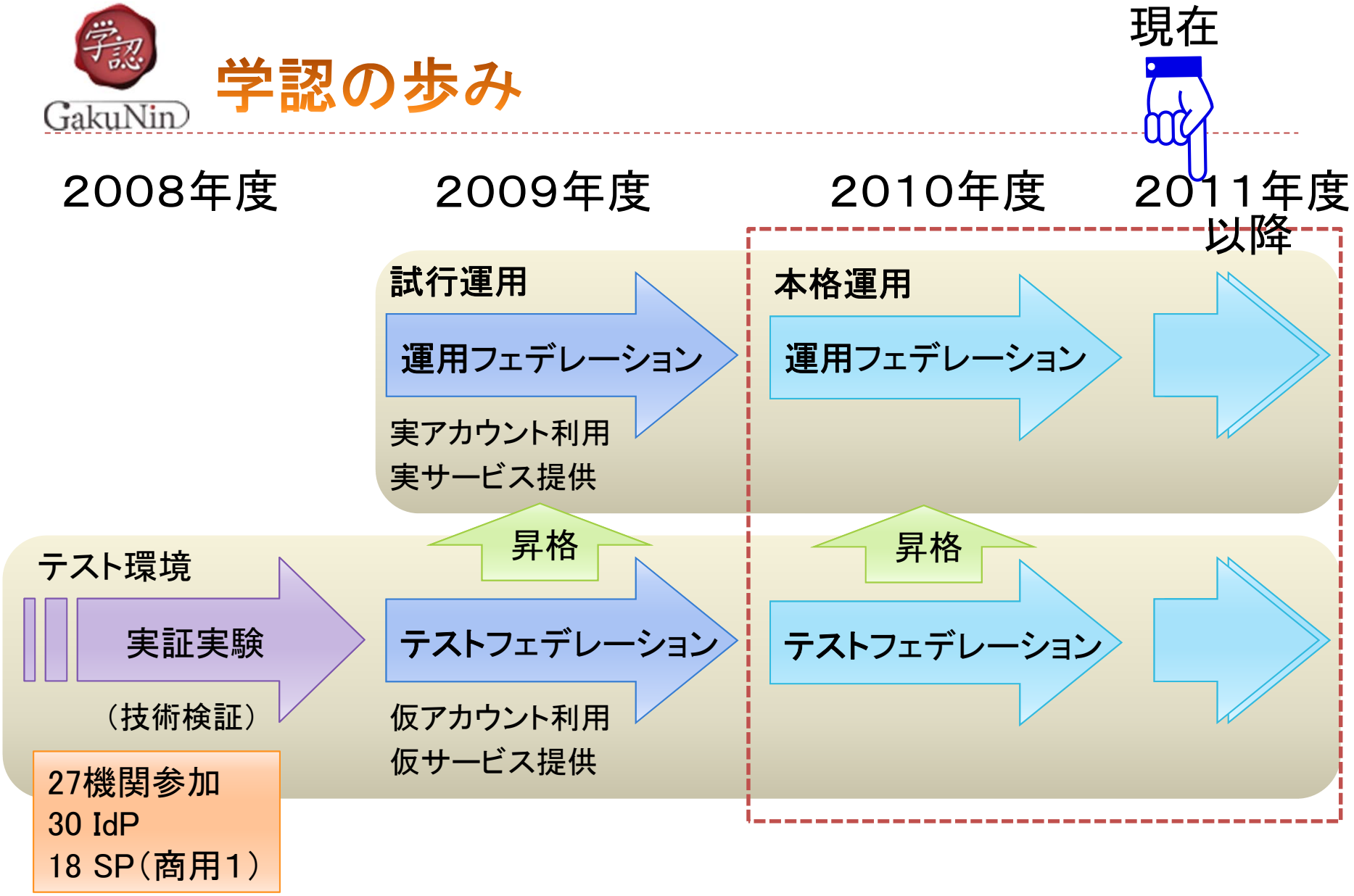

2008年度
2009年度
2010年度
2011年度以降
試行運用
運用フェデレーション
実アカウント利用
実サービス提供
本格運用
運用フェデレーション
昇格
昇格
テスト環境
実証実験
（技術検証）
テストフェデレーション
仮アカウント利用
仮サービス提供
テストフェデレーション
27機関参加
30 IdP
18 SP（商用1）

2008年度　実証実験参加機関

- 27 Institutions
- 30 IdP sites
- 18 SP sites



学認の歩み


現在
2008年度
2009年度
2010年度
2011年度以降
試行運用
運用フェデレーション
実アカウント利用
実サービス提供
本格運用
運用フェデレーション
昇格
昇格
テスト環境
実証実験
（技術検証）
テストフェデレーション
仮アカウント利用
仮サービス提供
テストフェデレーション
27機関参加
30 IdP
18 SP（商用1）

運用フェデレーション参加IdP (28)（9月14日現在）

- 国立情報学研究所
- 名古屋大学
- 山形大学
- 千葉大学
- 京都大学
- 広島大学
- 金沢大学
- 北海道大学
- 筑波大学
- 佐賀大学
- 山口大学
- 成城大学
- 東邦大学
- 三重大学
- 日本大学
- 旭川医科大学
- 東京農工大学
- 岡山大学
- 九州工業大学
- 京都産業大学
- 立教大学
- 九州大学
- 東京大学
- 明治大学
- 神戸大学
- 信州大学
- 自治医科大学
- 名古屋工業大学

（参加順）

総ID数≒45万ID

テストフェデレーション参加機関

旭川医科大学、北見工業大学、東北大学、福島大学、高エネルギー加速器研究機構、筑波技術大学、東京工業大学、お茶の水女子大学、産業技術大学院大学、慶應義塾大学、東京電機大学、愛知県立大学、鈴鹿工業高等専門学校、奈良教育大学、大阪大学，大阪教育大学、徳島大学、愛媛大学、広島工業大学、九州工業大学、熊本大学 etc…

参加検討中機関（by オープンフォーラムアンケート）

姫路獨協大学、静岡大学、中部大学、福井大学、東京学芸大学、京都女子大学、岩手大学、浜松医科大学、東京都医学研究機構、宮崎大学、南山大学、岐阜大学、鹿屋体育大学、京都工芸繊維大学、京都府立大学、高知大学、茨城大学、同志社大学、室蘭工業大学、金城学院大学、福井県立大学、北見工業大学、東京都市大学、北九州工業高等専門学校、島根大学、大阪教育大学

最新情報：https://www.gakunin.jp/docs/fed/participants

現時点で利用可能なSP

（9月14日現在）

- 学術コンテンツ (13)
  - Science Direct / SCOPUS (Elsevier)
  - SpringerLink (Springer)
  - Web of Knowledge / EndNote (Thomson Reuters)
  - OvidSP (Ovid)
  - RefWorks (ProQuest)
  - Cambridge Journals Online (CUP)
  - Pathology Images (Atlases)
  - EBSCOhost (EBSCO)
  - KOD (研究社)
  - CiNii (NII)
  - IEEE Xplore (IEEE)
  - 360 Search, 360 Link, Electronic Journal Portal (Serials Solutions)
  - IMCデータリポジトリ（金沢大学）
- 接続作業中
  - Sunmedia
  - IOP
  - PubMed
  - ebrary
  - Karger
  - Emerald
  - 朝日新聞
  - 医中誌
  - 有斐閣
  - 三省堂
  - …

最新情報：https://www.gakunin.jp/docs/fed/participants

現時点で利用可能なSP

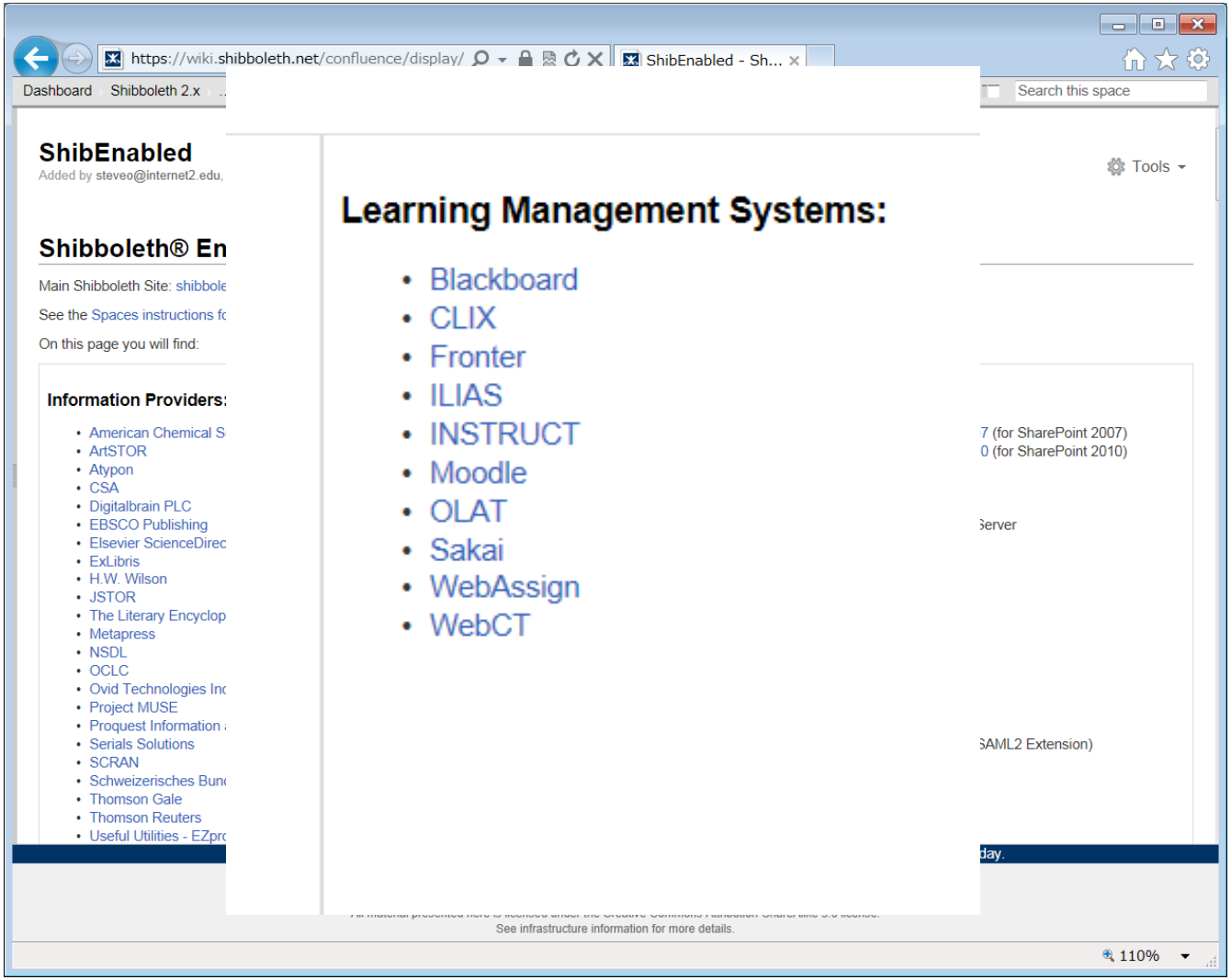
（9月14日現在）

- 開発環境(1)
  - DreamSpark (Microsoft)

- ネットワークサービス(10)
  - Fshare（大容量ファイル交換）サービス（NII）
  - FaMCUs (テレビ会議多地点接続)サービス (NII) – 収容拠点数拡大予定
  - Eduroam-Shib（eduroam用一時アカウント発行）サービス（京大&NII）
  - SecurityLearningシステム(e-Learning)（NII）
  - WebELS eLearningシステム(e-Learning)（NII）
  - edubase Cloud(クラウドサービス)（NII）
  - Foodle(予定調整サービス) (UNINETT)
  - ゲスト用ネットワークアクセス認証（佐賀大学、広島大学）
  - ファイル送信サービス（金沢大学）
  - 科学技術の学術情報共有のための双方向コミュニケーションサービス（山形大学）

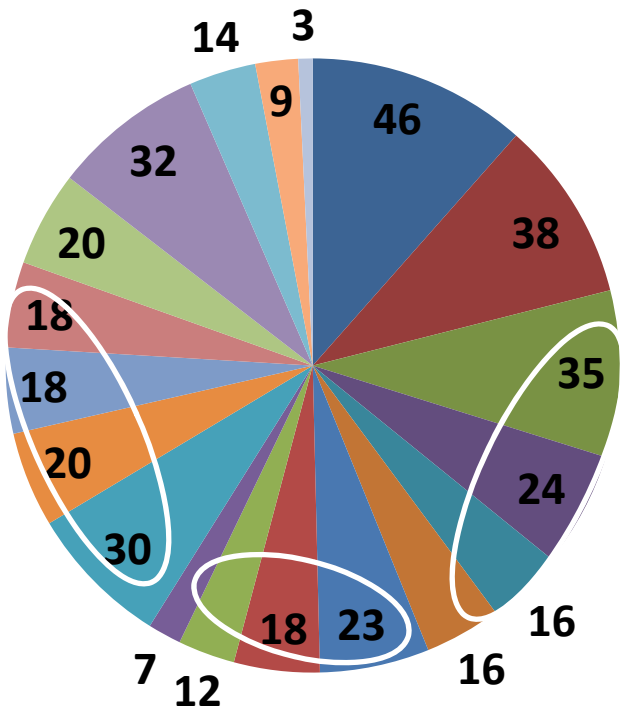
最新情報：https://www.gakunin.jp/docs/fed/participants

シボレス化されたアプリケーション例



https://wiki.shibboleth.net/confluence/display/SHIB2/ShibEnabled

学認に対し、今後の充実を期待するサービス



オープンフォーラム向けアンケート
回答結果より

- 電子ジャーナル
- 電子書籍
- e-Learning（他機関から提供されるサービス）
- e-Learning（民間企業から提供されるサービス）
- e-Learning（機関内へ提供するサービス）
- e-Learning（他機関へ提供するサービスとして）
- ソフトウェア配布（他機関から提供されるサービス）
- ソフトウェア配布（民間企業から提供されるサービス）
- ソフトウェア配布（機関内へ提供するサービス）
- ソフトウェア配布（他機関へ提供するサービス）
- 遠隔講義・遠隔会議システム（他機関から提供されるサービス）
- 遠隔講義・遠隔会議システム（民間企業から提供されるサービス）
- 遠隔講義・遠隔会議システム（機関内へ提供するサービス）
- 遠隔講義・遠隔会議システム（他機関へ提供するサービス）
- 参加各機関による研究成果の公開
- 電子メールやオンラインストレージなどのクラウドサービスとの連携
- 学務情報システム
- 人事給与・財務会計システム
- その他

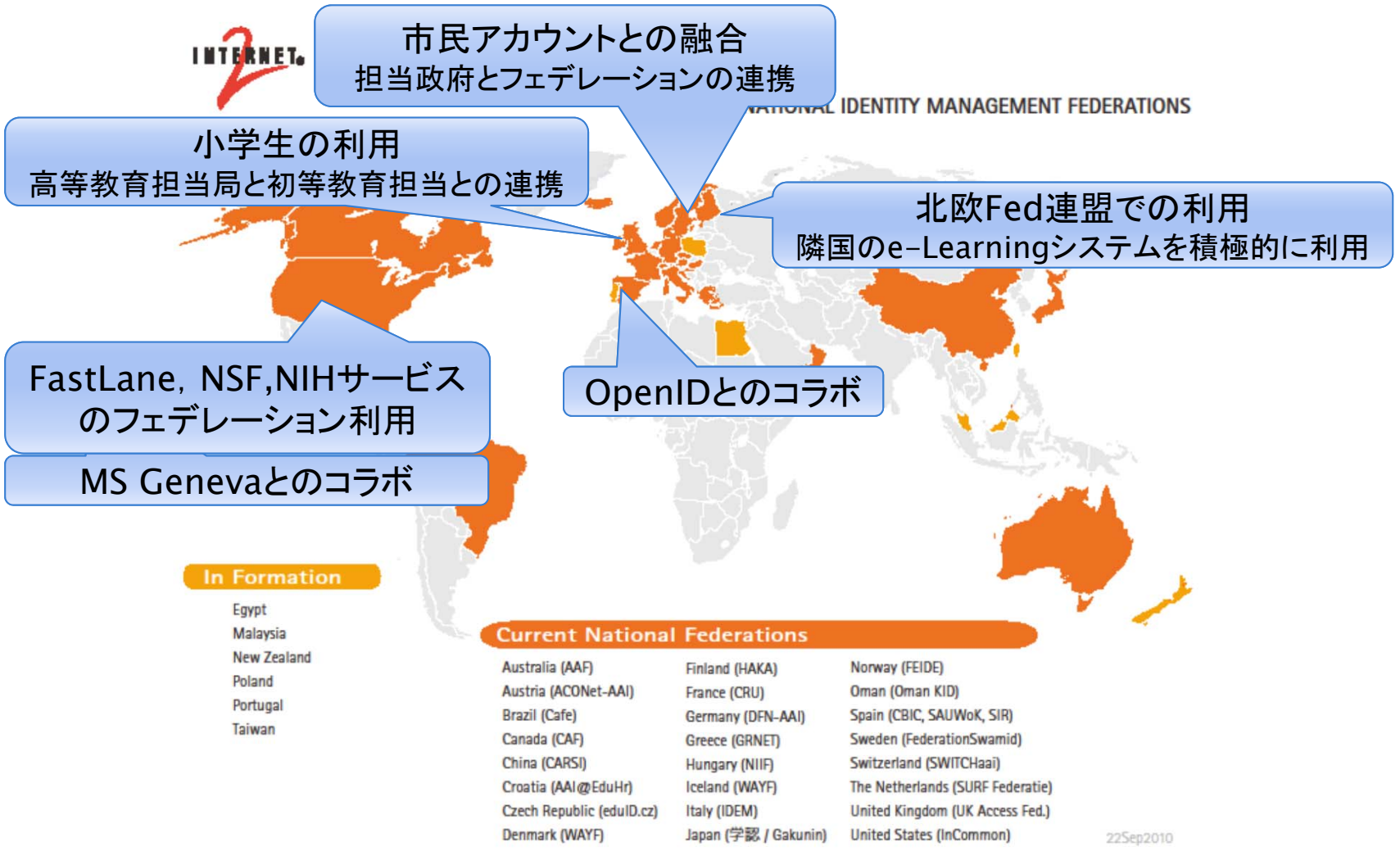
海外フェデレーションのSP数

- スイス SWITCHaai：515
- イギリス UK-FAM：219
- アメリカ InCommon：140
- フランス Fédération Éducation-Recherche ：123
- フィンランド Haka：115
- ノルウェー FEIDE：80
- ドイツ DFN-AAI：60
- デンマーク WAYF：26

日本国内のサービスの展開がポイント

https://refeds.terena.org/index.php/Federations

世界のフェデレーションと動向



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

2011年度の主なイベント

学認CAMP	09/14	三重大学
第8回全国大学コンソーシアム研究交流フォーラム　分科会	09/11	熊本学園大学
New Education Expo「学術認証フェデレーションによる 新たな大学ICT利活用の展開」	06/15-16	大阪マーチャンダイズ・マート
学術情報基盤オープンフォーラム「学認を活用した地域連携に向けて」	06/03	国立情報学研究所
情報処理技術セミナー「Shibboleth環境の構築」(第3回)	11/01-02	国立情報学研究所
情報処理技術セミナー「Shibboleth環境の構築」(第2回)	08/04-05	国立情報学研究所
情報処理技術セミナー「Shibboleth環境の構築」(第1回)	06/20-21	国立情報学研究所

Shibboleth環境の構築セミナー

- 2009年度までは，NII情報処理軽井沢セミナーにて実施
- 2010年度からは，NII講習システムを用いて実施
  - 2日間コース
    - IdP構築実習（1日目）
    - SP構築実習（2日目）
  - 計8回実施
    - 大学向け3回
    - 大学＋企業向け5回
      - 計120名以上が受講
- 2011年度も引き続き実施
  - 大学向け（3回を予定）
    - 6/20-21，8/4-5，11/1-2
  - 大学＋企業向け（調整中）

大学向け研修会詳細
http://www.nii.ac.jp/hrd/ja/joho-karuizawa/index.html　に掲載

学認への参加方法

- 学認申請システム
  - 学認への参加申請，メタデータ登録・更新等がWebを通してオンラインで可能
- テストフェデレーション
  1. 申請情報登録（およびアカウント作成）
  2. 事務局での参加承認
  3. フェデレーションメタデータの自動更新

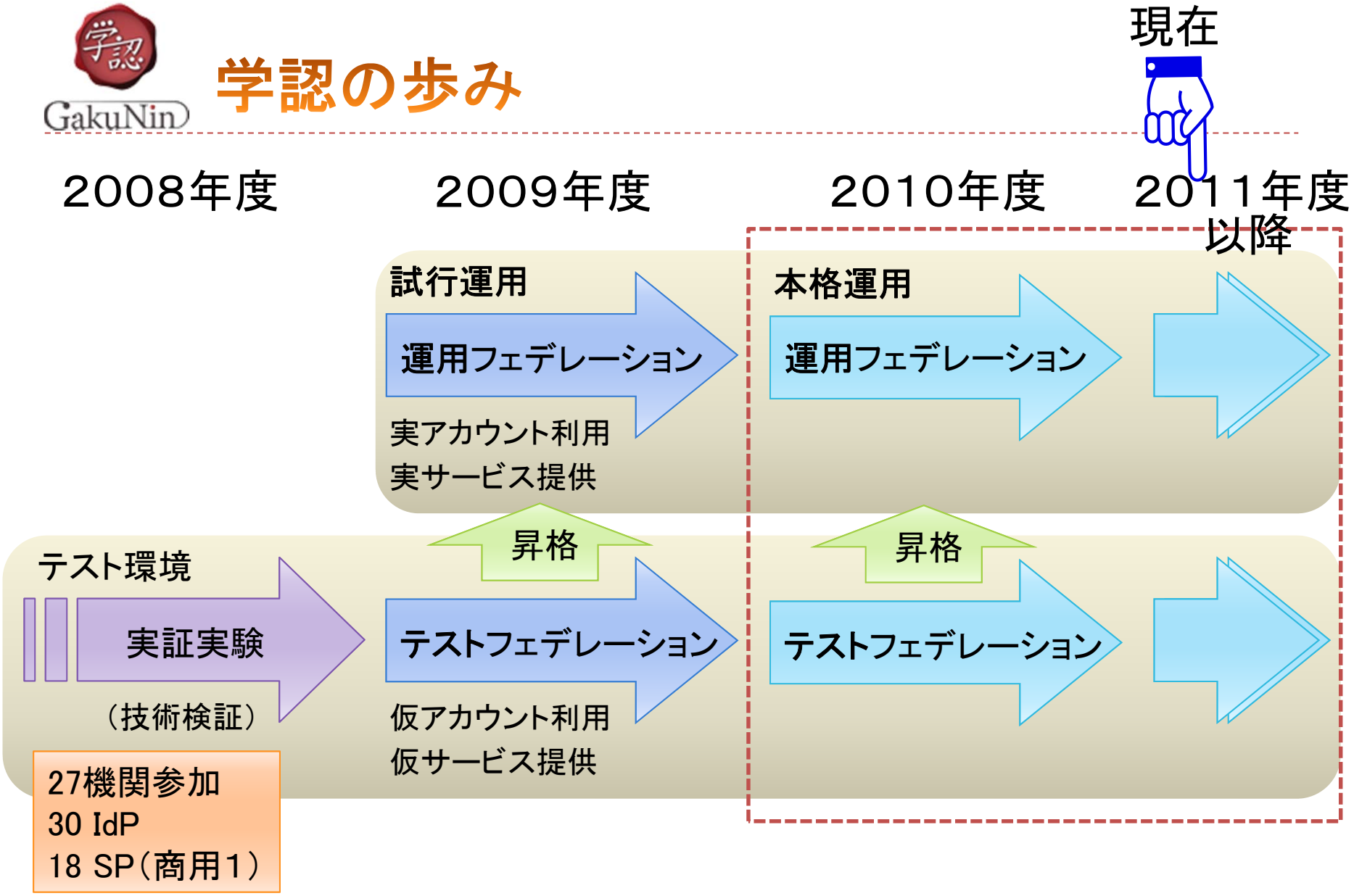
学認が提供するテストSPやIDPを利用して接続確認

通常一日で
参加完了
利用開始可能

- 運用フェデレーションの場合は？
  - オフラインによる確認が1ステップ増えるだけ

実施要領，システム運用基準が守られていることが前提

学認の歩み


現在
2008年度
2009年度
2010年度
2011年度以降
試行運用
運用フェデレーション
実アカウント利用
実サービス提供
本格運用
運用フェデレーション
昇格
昇格
テスト環境
実証実験
（技術検証）
テストフェデレーション
仮アカウント利用
仮サービス提供
テストフェデレーション
27機関参加
30 IdP
18 SP（商用1）

ケーススタディー覧

1. 学外サービスとの認証連携に備えて／北海道大学
2. 認証基盤も冗長構成化して可用性を向上／山形大学
3. 電子図書館サービスにShibbolethを導入／筑波大学
4. 図書館主導で実現したShibboleth認証／千葉大学
5. 情報リソースの共有で運用コストを低減／東京農工大学
6. 学認が実現する日本の学力水準の向上／成城大学
7. キャンパス間をつなぐ遠隔授業／日本大学
8. 学認のサービスが応える医療系大学のニーズ／東邦大学
9. 学内/学外サービスの双方に認証基盤を用意／金沢大学
10. 京都大学 独立した組織間での認証連携を実現／京都大学
11. 大学間共用e-ラーニングシステムへの活用／京都産業大学
12. ゲスト利用者のネットワーク認証に活用／広島大学
13. 大学間認証連携のキラーコンテンツLMS／徳島大学
14. 統合認証基盤とSingle Sign-On連携／佐賀大学

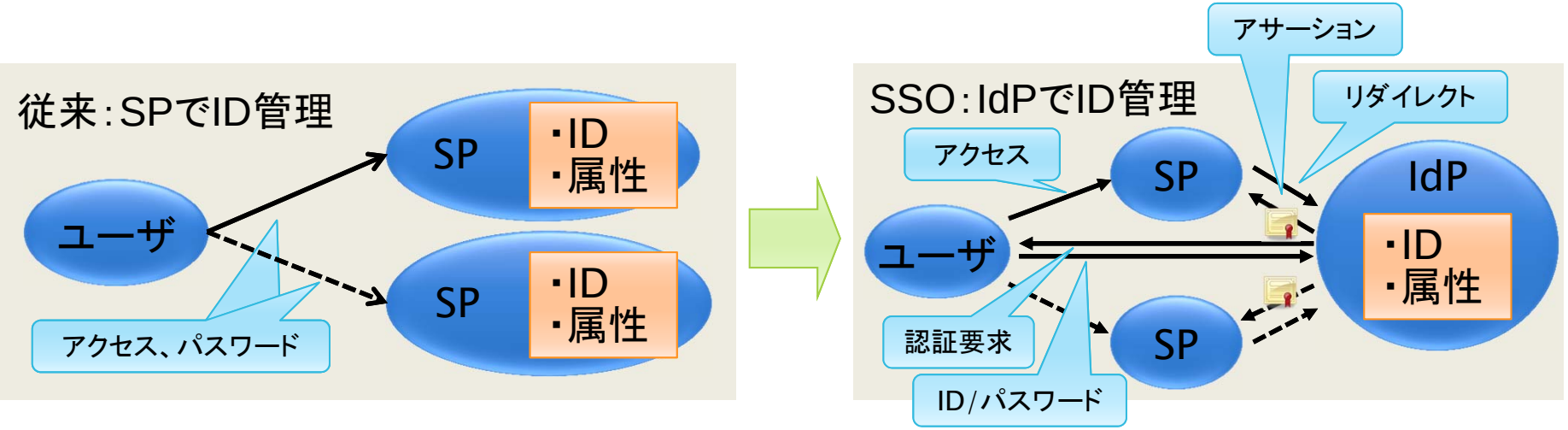
http://www.gakunin.jp/docs/fed/info から参照可能

話の流れ

- 学術認証フェデレーション(学認)とは
- 学認の現状
- Shibboleth の概要とその動作

学術

- 学術認証フェデレーション
  - Shibboleth による運用
  - 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
- プライバシ保護を考慮したシングルサインオン（SSO）技術
  - 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



Shibboleth(シボレス)

- バージョン1.3系と2.0系が広く利用されている（プロトコルが少し異なる）
  - 最新は IdP 2.3.2, SP 2.4.3 （学認ではまだ IdP 2.1.5が主流 ?）
  - Linux, FreeBSD, Solaris, Windows (IIS) など主要なOSに対応

cf.

- 欧州（特に北欧）では，simpleSAMLphpも利用されている
  - 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/

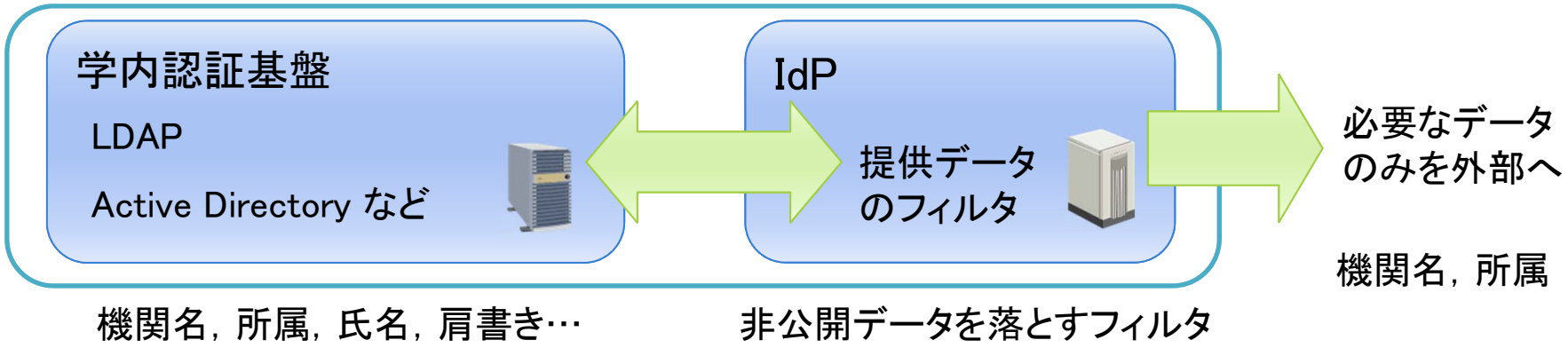
- Microsoft ADFS 2.0 とも連携可能
  - AD FS 2.0 デザイン ガイド
    - http://technet.microsoft.com/ja-jp/library/gg308546.aspx

フェデレーション構築に必要なサーバ

- IdP（Identity 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」

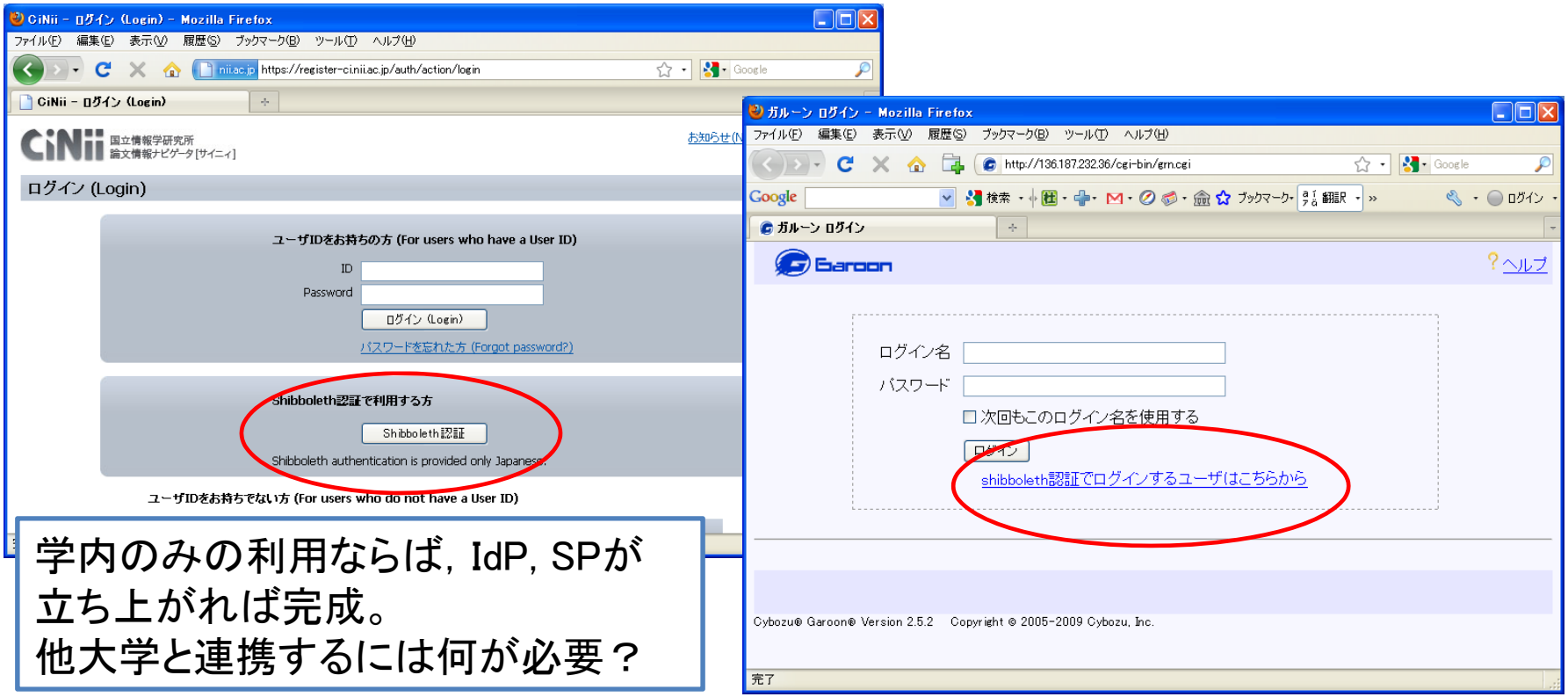
IdP (Identity Provider)

- 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



SP (Service Provider)

- 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）



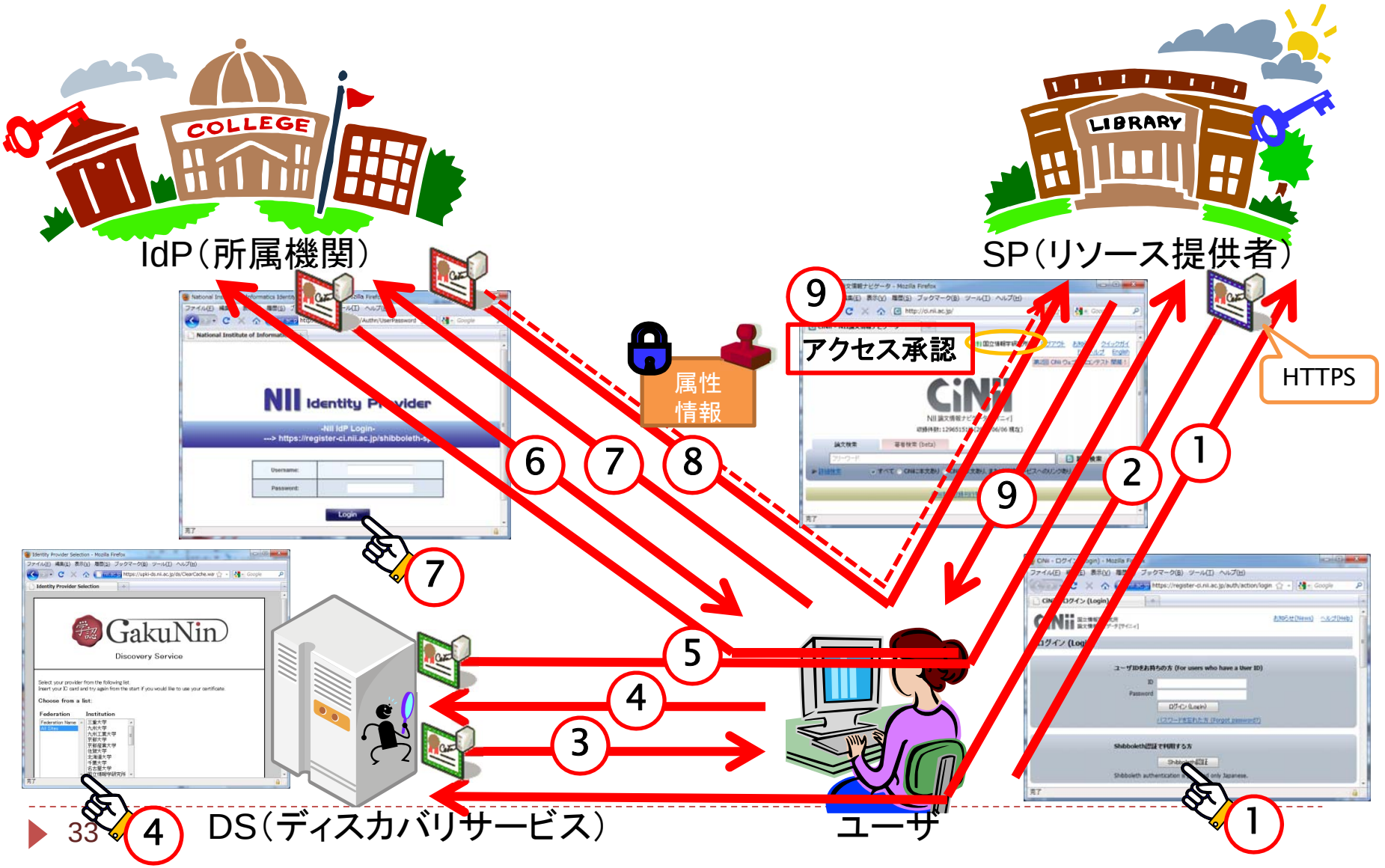
学内のみの利用ならば，IdP，SPが
立ち上がれば完成。
他大学と連携するには何が必要？

DS (Discovery Service)

- SPへのアクセスの際に認証するIdPを選択するシステム

d)方式もある

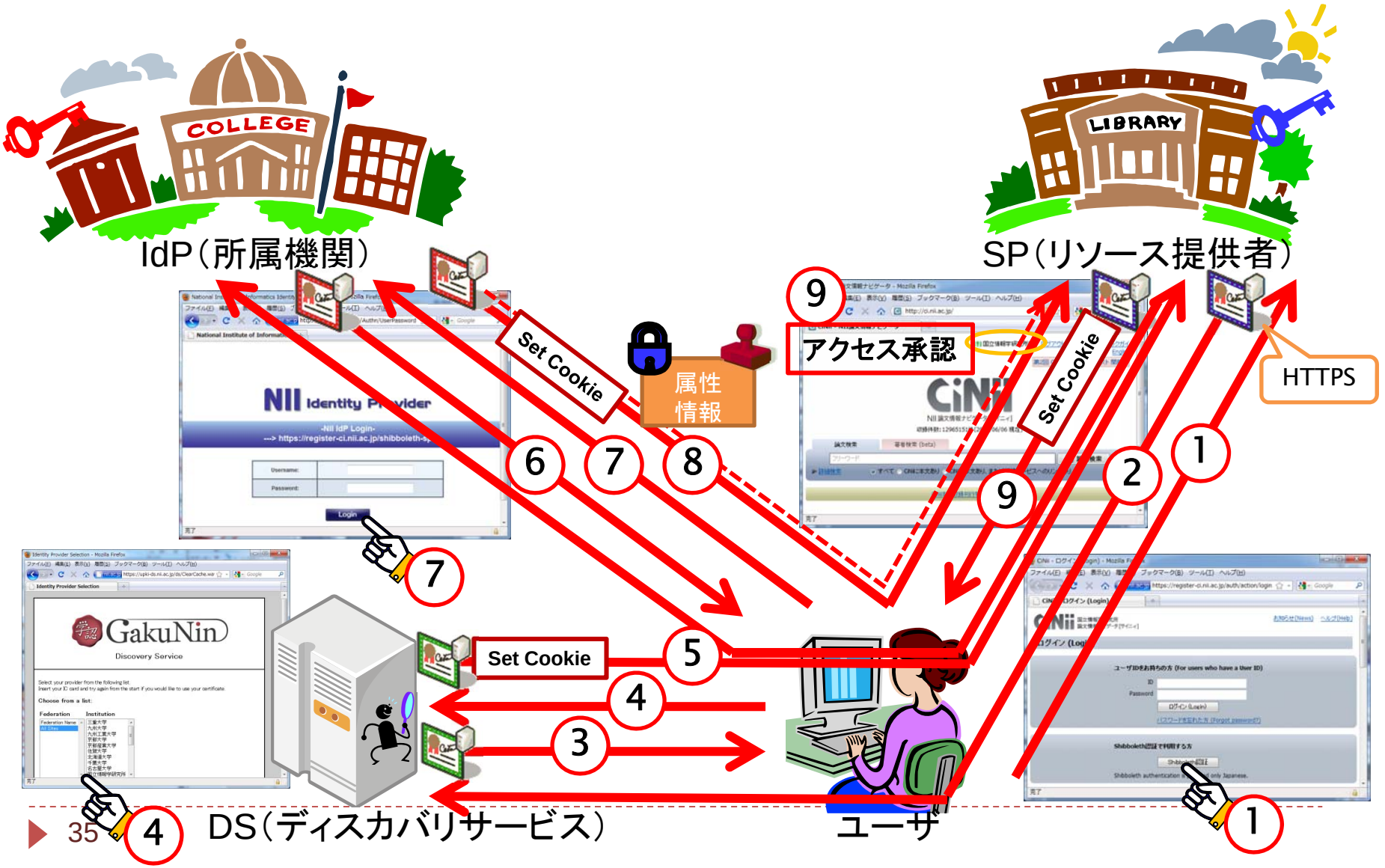
Shibbolethの基本動作(最初の動作)



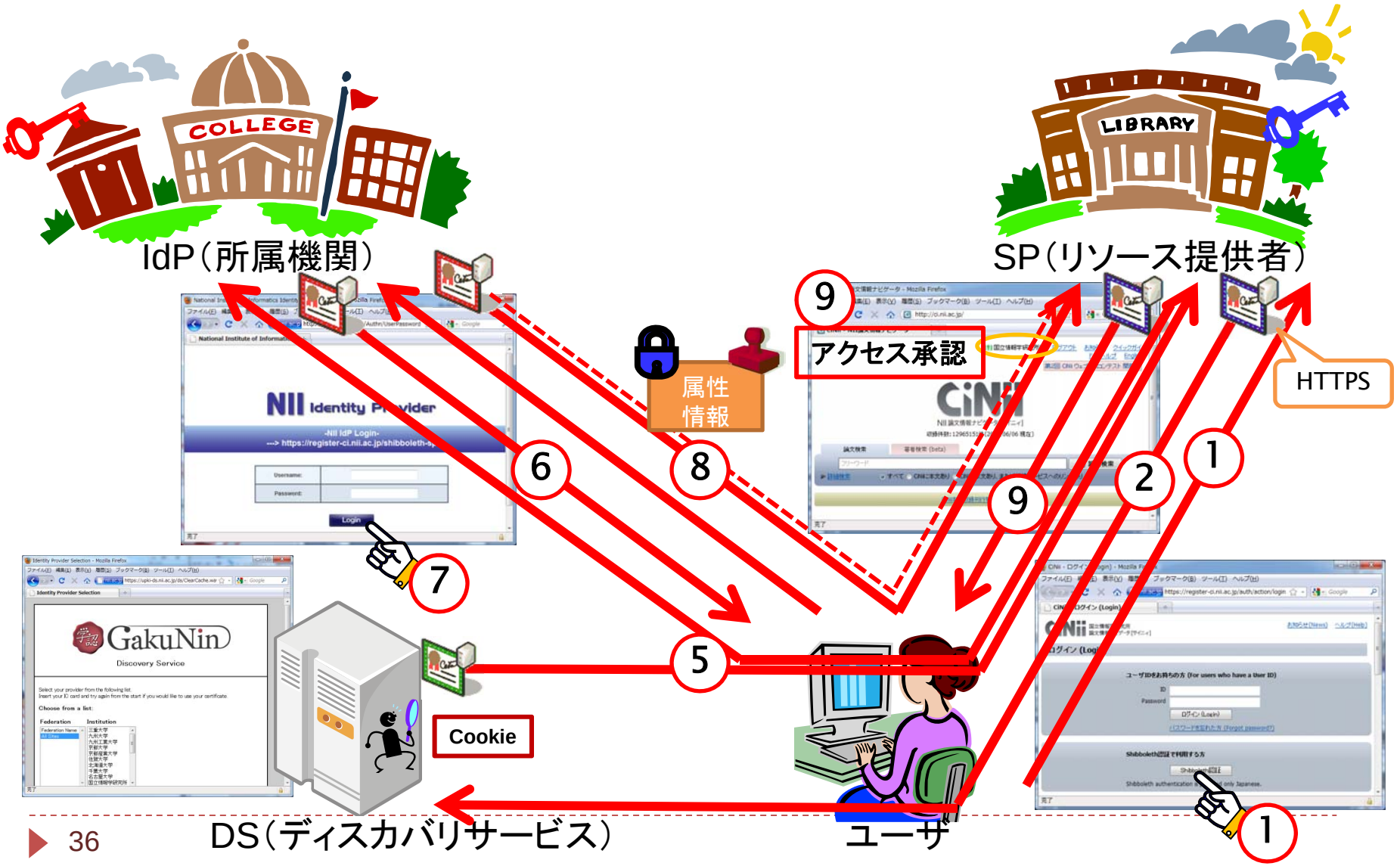
Cookieによる処理の記憶

- 認証の処理(状態)を記憶するためにCookie を使用
  - どのIdPを選択したか（DS:Cookie）
    - 一定期間保持(例: 一週間、永久…)
  - IdPによる認証が成功しているか（IdP:Cookie）
  - SPへのアクセスが承認されているか（SP:Cookie）
  - 基本的にブラウザを閉じるまで
    - 別途、タイムアウトもあり
    - 個別にログアウトも

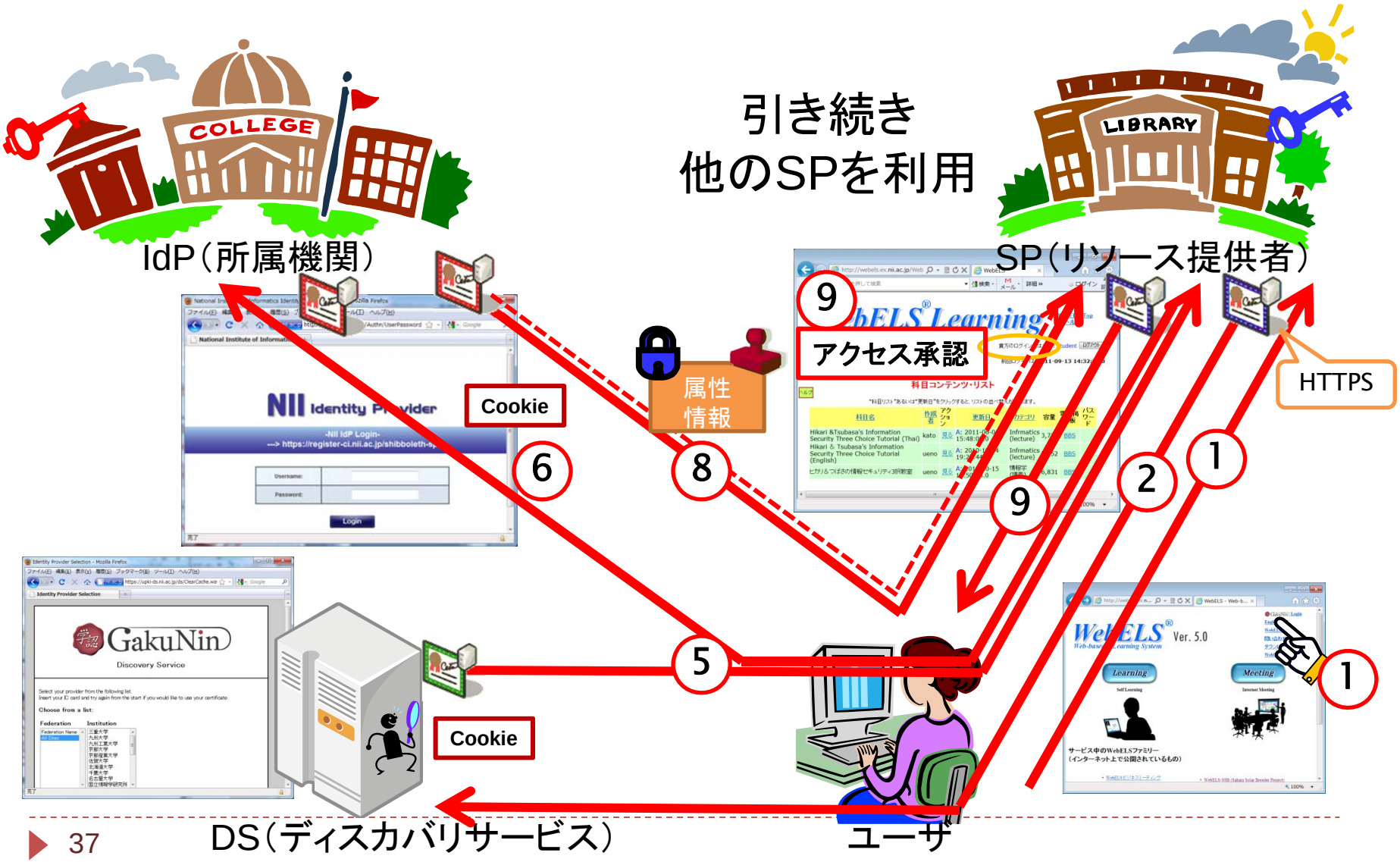
Cookieによる処理の記憶



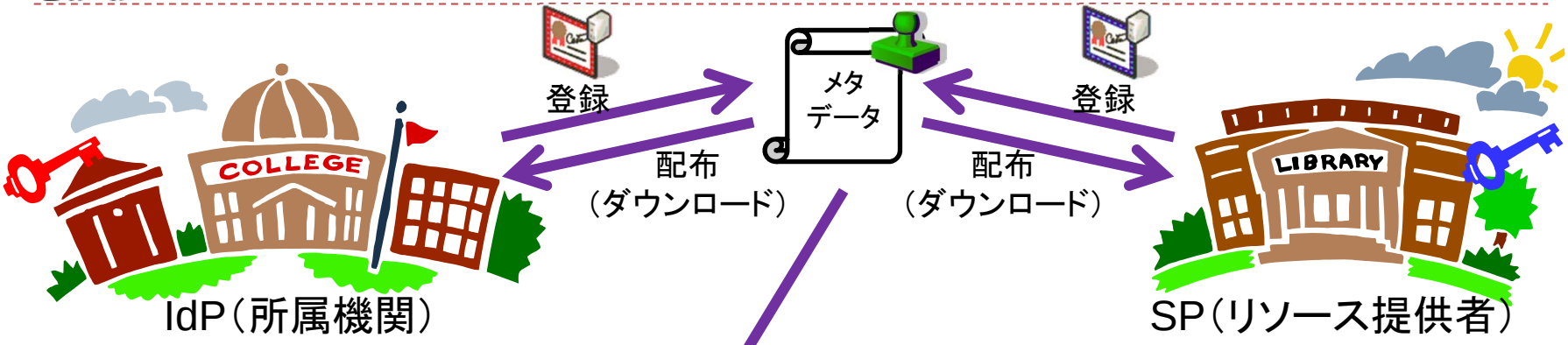
Shibbolethの基本動作(IdPの記憶)



Shibbolethの基本動作(シングルサインオン)



メタデータを用いた信頼の構築



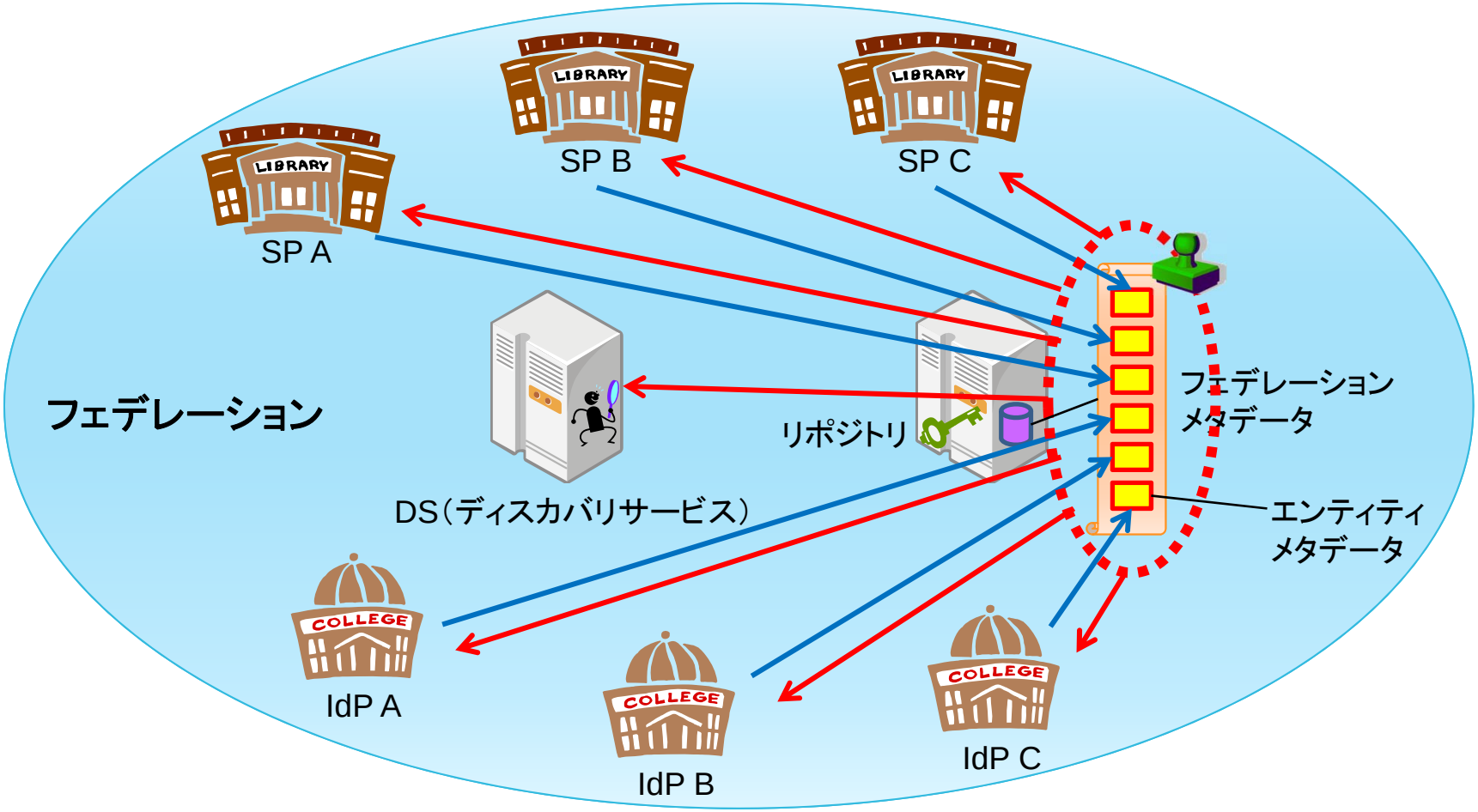
IdP（所属機関）

SP（リソース提供者）

DS（ディスカバリサービス）

ユーザ

メタデータを用いた信頼の構築

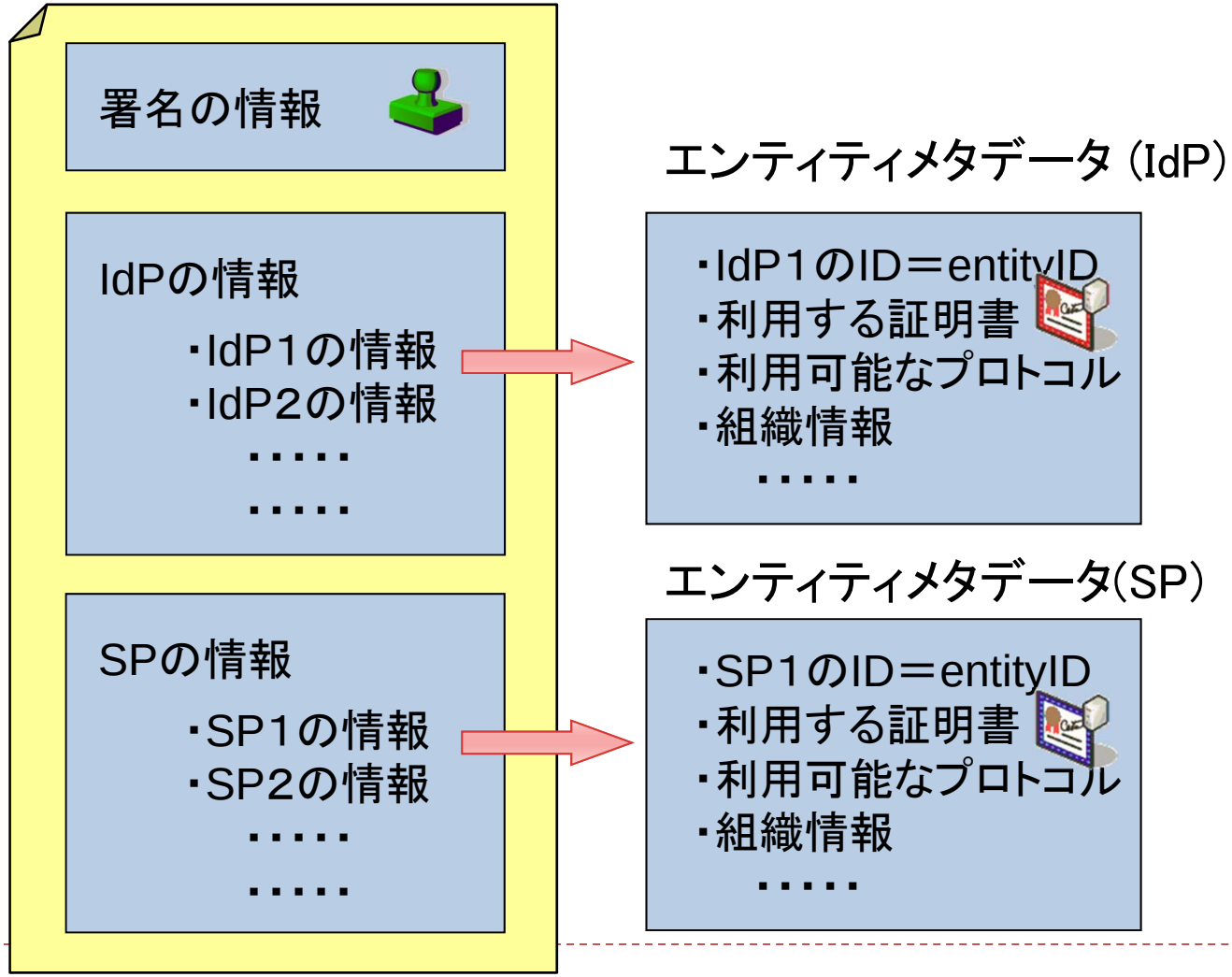


自動ダウンロードするフェデレーションメタデータの信頼性は、フェデレーションの証明書 で担保（事前に入手・検証し、事前にIdP/SPにインストール）

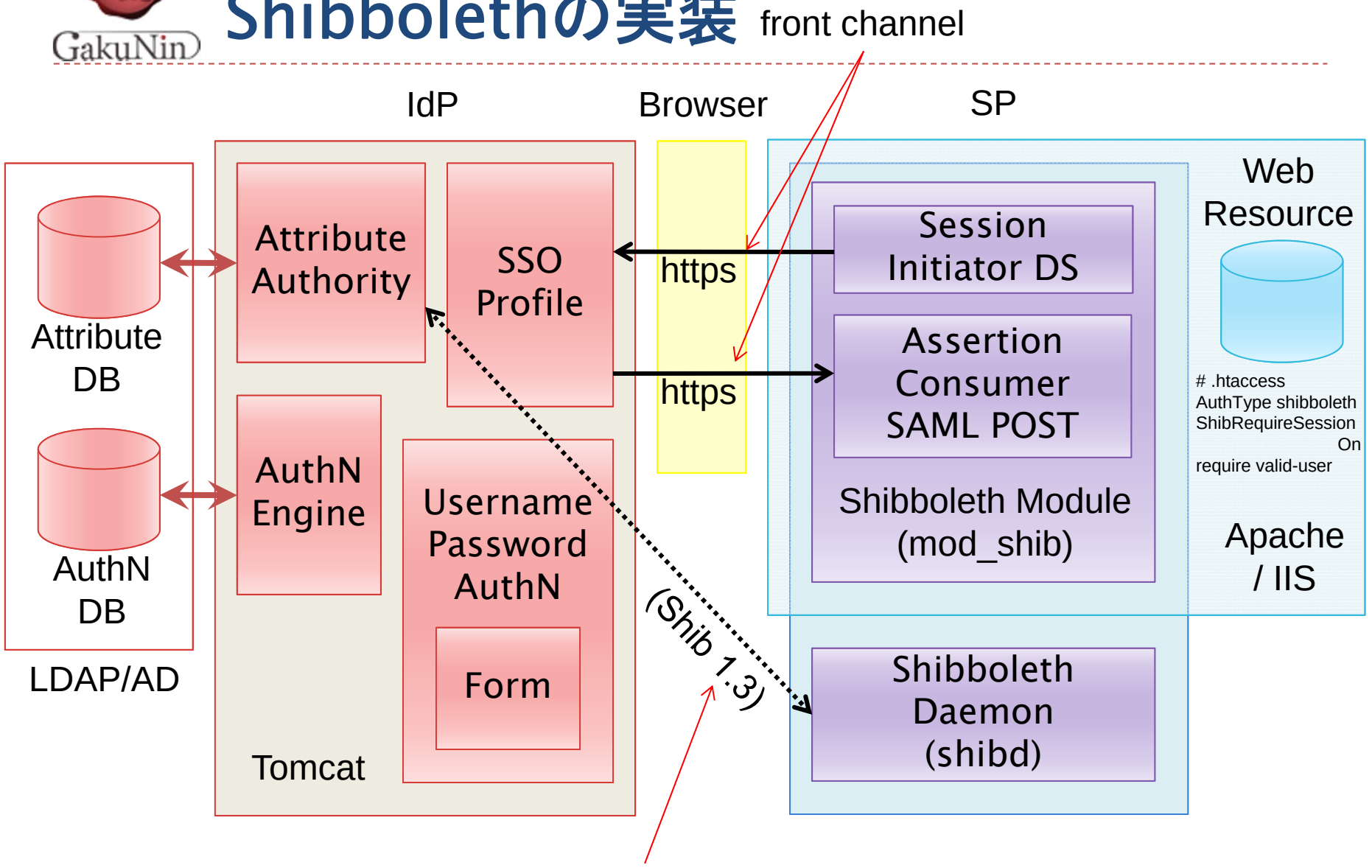
（検証は、別チャンネルで入手したfingerprintとの比較等による）

メタデータ(XML形式)の構成

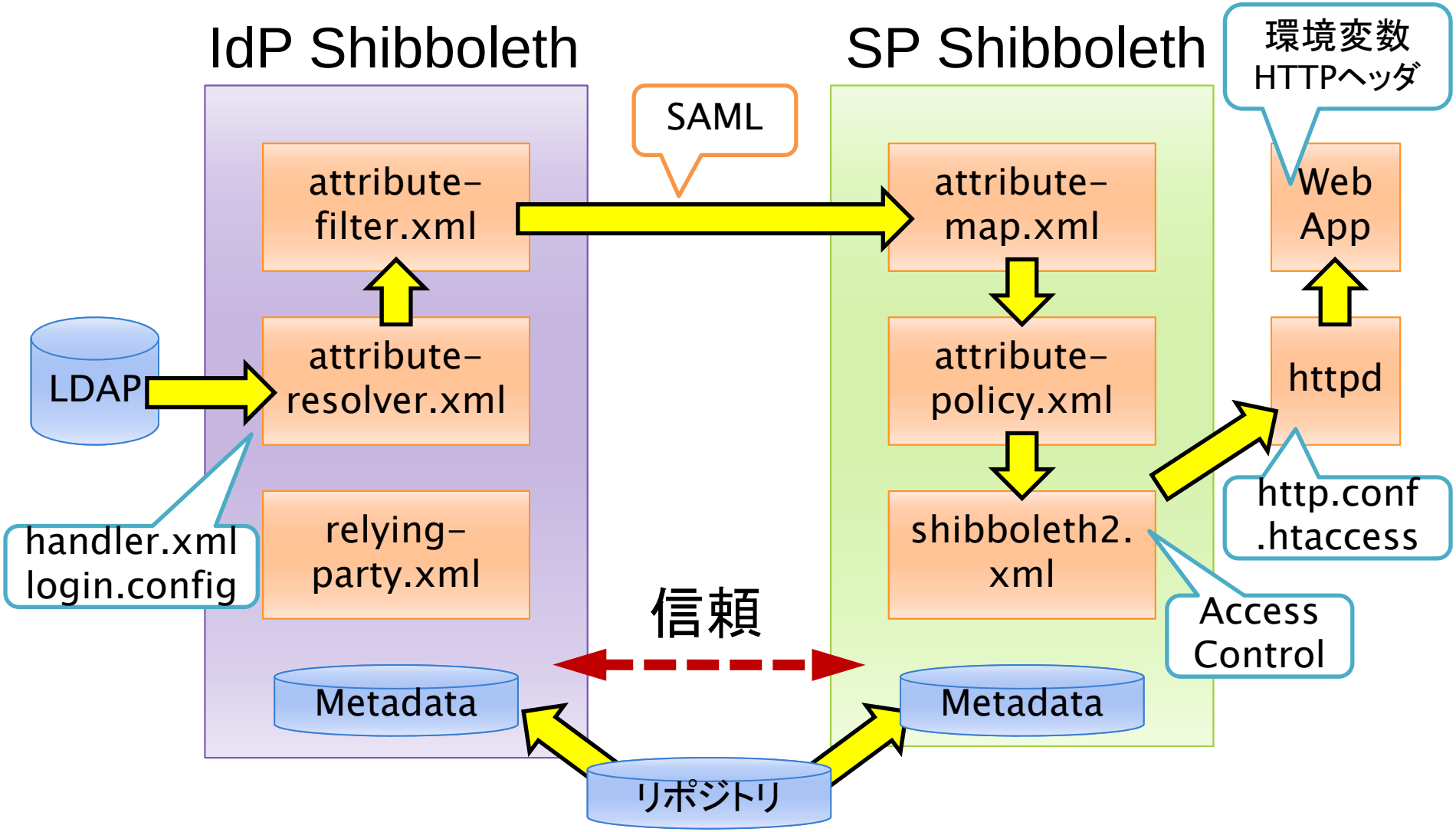
フェデレーションメタデータ ≒ relying party（信頼関係）



Shibbolethの実装



属性情報のフィルタリングと認可制御



属性情報の受け渡し

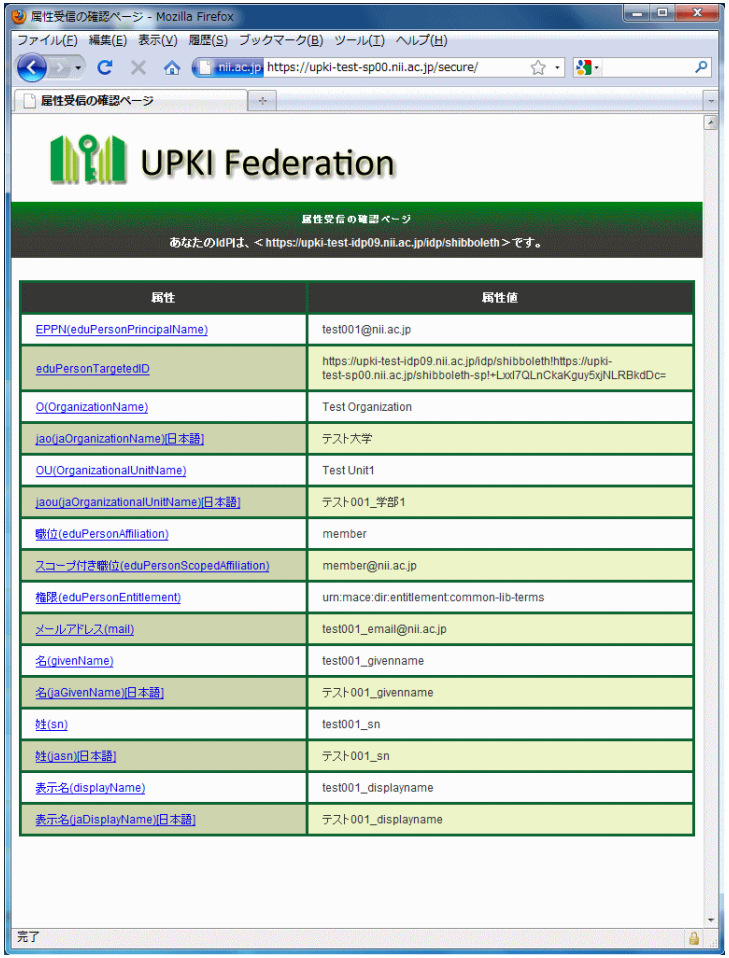
- IdPは必要な属性のみ提供し
  - IdPのattribute-filter.xmlに定義された属性が送出され(SP毎に設定可)
- SPがその中から必要なもの のみを選択
  - SPのattribute-map.xmlに定義された属性を受け取る(SPが必要な属性を要求するわけではない)

フェデレーションで扱う「属性」

フェデレーションで認証に使用する属性は16種類。これらを用いて認可を行う。

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://www.gakunin.jp/docs/fed/technical/attribute

SPでの属性情報の利用方法

- Apache の httpd.conf , .htaccess等での設定例
  - Basic認証等の代替（ユーザの区別なし）

```
<Location /App>
 AuthType shibboleth
 ShibRequireSession On
 require valid-user
</Location>
```

  - ユーザを区別して認可

```
<Location /App>
 AuthType shibboleth
 ShibRequireSession On
 # ShibUseHeaders On（属性をHTTPのヘッダに含めて受け渡す場合）
 require affiliation student@nii.ac.jp
</Location>
```

SPでの属性情報の利用方法

- アプリケーション側で属性情報を参照して、細かな認可
  - 環境変数を参照する
  - HTTPヘッダを参照する
    - ShibUseHeaders On

https://www.gakunin.jp/docs/fed/technical/sp/WebApp

環境変数

- affiliation: member@nii.ac.jp
- displayName: test001_displayname
- entitlement: urn:mace:dir:entitlement:common-lib-terms
- eppn: test001@nii.ac.jp
- givenName: test001_givenname
- jaDisplayName: テスト001_displayname
- jaGivenName: テスト001_givenname
- Jao: 国立情報学研究所
- Jaou: テスト001_学部1
- Jasn: テスト001_sn
- mail: test001_email@nii.ac.jp
- o:Test Organization
- ou:Test Unit1
- persistent-id:https://shib-sample.ac.jp/idp/shibboleth!https://shib-sample.ac.jp/shibboleth-sp!EXBYRzIELL0FlV3kWiFI7jtTApo=
- sn: test001_sn
- unscoped-affiliation: member

  ……

SPでの属性情報の利用方法

- アプリケーション側で属性情報を参照して、細かな認可
  - 環境変数を参照する
  - HTTPヘッダを参照する
    - ShibUseHeaders On

環境変数(またはHTTPヘッダ) から、属性を簡単に

- もちろん、IdPから渡されるのだけ
- Shibboleth 対応サービスの作成はとても簡単！
- 皆さま、魅力あるサービスSPの提供をお願いいたします！

https://www.gakunin.jp/docs/fed/technical/sp/WebApp

テストフェデレーションでお試し

- テストフェデレーション
  1. 申請情報登録（およびアカウント作成）
  2. 事務局での参加承認
  3. フェデレーションメタデータの自動更新

学認が提供するテストSPやIDPを利用して接続確認

通常一日で
参加完了
利用開始可能

技術的検証のみを行うフェデレーションなので、お気軽に
参加ください(うまくいけば、運用フェデレーションへ)

https://www.gakunin.jp/docs/fed/join

まとめ

- Shibboleth, 学認 を知ろう
  - 学認
    - 学認とは
    - 学認の現状
    - ケーススタディ …
  - Shibboleth の概要
    - IdP, SP, DS
    - 基本動作
    - 属性情報の利用

各種情報

1. 学術認証フェデレーション（学認）に関するWebサイト

   https://www.gakunin.jp/

2. ポリシー、申請書

   「学術認証フェデレーション」ー「参加」
   https://www.gakunin.jp/docs/fed/join

3. 情報交換メーリングリスト（アーカイブ）

   「学術認証フェデレーション」ー「情報交換ML」
   https ://www.gakunin.jp/docs/fed/ml