GakuNin

新しい学認機能のご紹介
DS, uApprove.jp, OpenIdP

学認CAMP / 三重大学 / 2011年9月14日

中村　素典 / 国立情報学研究所

トピック

- 埋め込みDS (embedded DS)
- IdP機関のためのユーザ同意機構 (uApprove.jp)
- OpenIdP（特定組織に属さないIdP）

1. 埋め込みDS (embedded DS)

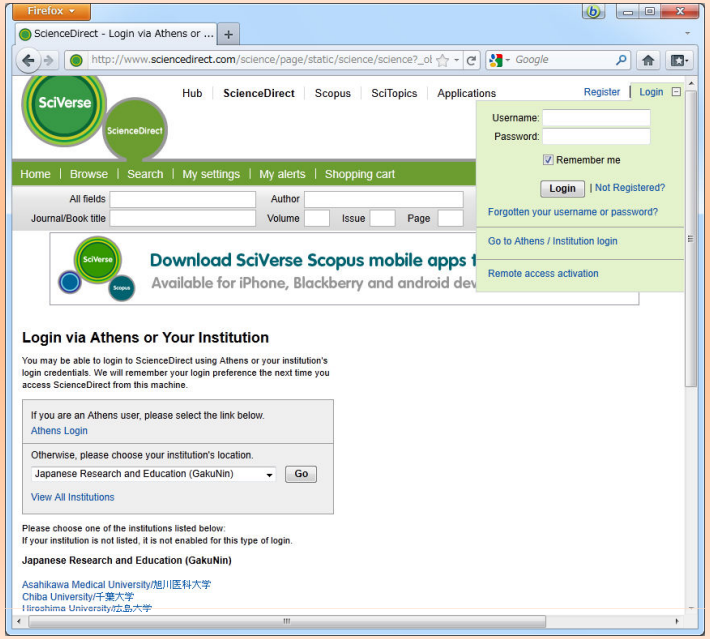
学認におけるサービス利用時の一般的な手順

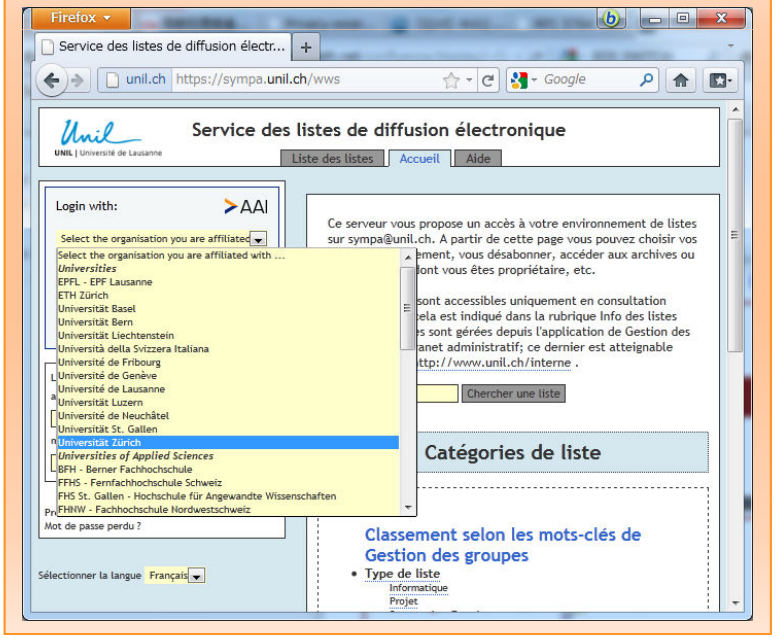
① サービスにアクセス
② 学認ログインを選択
③ DSに飛ぶ
④ IdP一覧から選択
⑤ IdPに飛ぶ
⑥ 認証情報を入力
⑦ SPに戻って
サービス開始

サイトが何度も
切り替わると
ユーザが混乱する

SP埋め込みのDSの登場 (EDS: Embedded DS)

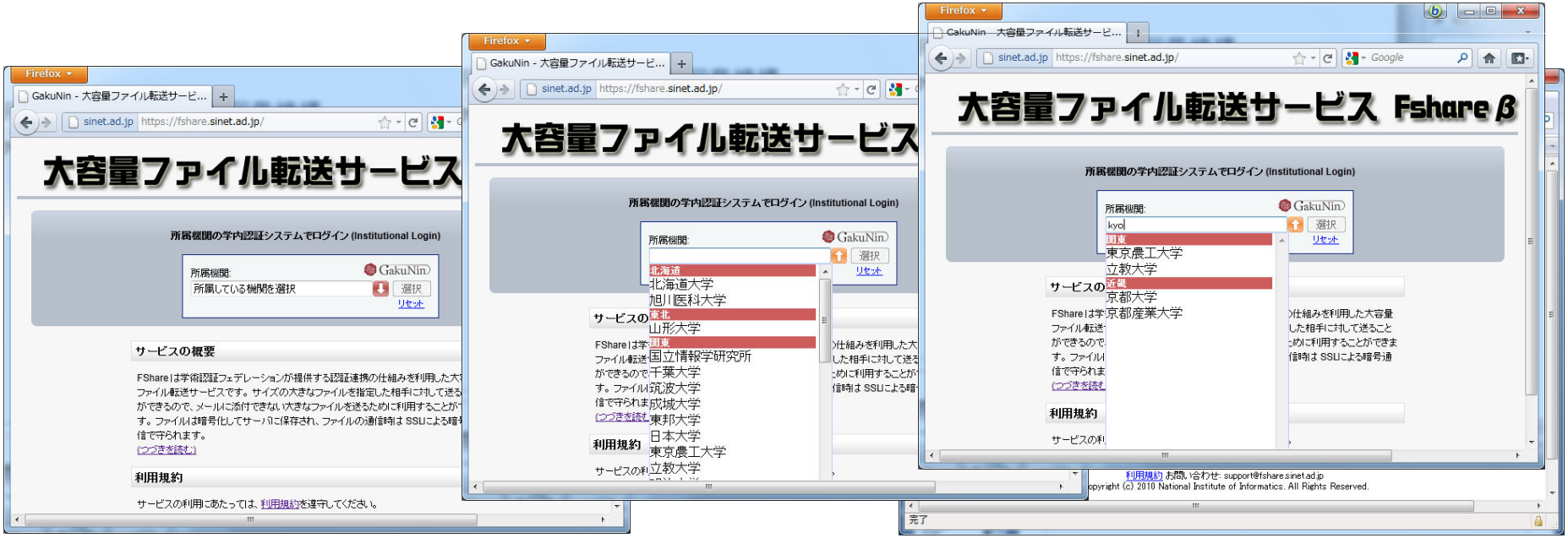
- 独自方式（eJサイト等）
  - 契約のある機関のみのリストを提供
- Shibboleth方式
- SWITCH方式





DSを埋め込んだサービス

- DSに飛ばないため、画面遷移が1回減り、ユーザの不安解消につながる
- 一度選択したIdP情報はSP間で共有される
- その他様々な使い勝手の向上



学認版EDS

- SWITCH方式EDSをベースに改良
  - 使い勝手の良いインクリメンタルサーチ
    - 大学数が多い国では、絞り込み機能は必須
  - 選択は、マウスでもキーボードの矢印キーでも可能
  - IdPの名前が長くても、横スクロールで確認可能
  - どのIdPを選択したかの情報を、異なるSPで共有可能
    - 不正サイトへの情報漏洩（フィッシング支援）を防止する工夫
      - 怪しいサイトから利用された場合は警告を表示し、選択情報はSP間で共有しない
  - 一覧で表示するSPの事前の絞り込み
    - SPがサービス可能なIdPのみを提示可能（DiscoFeedの利用）
  - JavaScriptがブラウザで許可されていない場合は、従来通りにDSサイトに飛ぶリンクを表示
    - DSサイトでもJavaScriptなしで動作

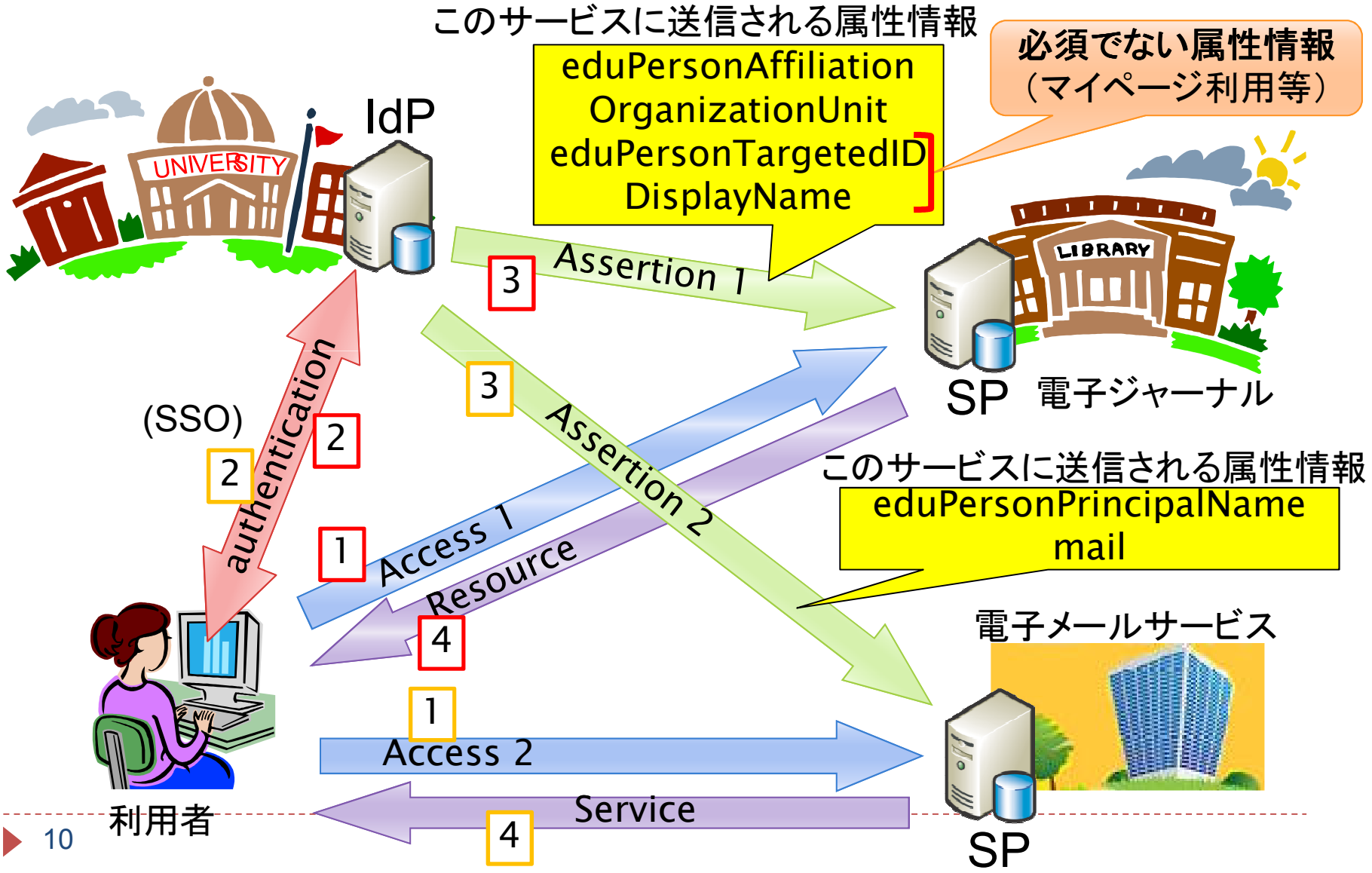
参考情報

- https://www.gakunin.jp/docs/fed/technical/embeddedds

- https://ds.gakunin.nii.ac.jp/WAYF2/index.php/embedded-wayf.js/snippet.html

2. IdP機関のためのユーザ同意機構

サービス利用時の個人情報送信



学認で利用されている属性情報

個人情報

Name (abbreviation)	Description
OrganizationName (o)	組織名
jaOrganizationName (jao)	組織名（日本語）
OrganizationalUnit (ou)	部門名
jaOrganizationalUnit (jaou)	部門名（日本語）
eduPersonPrincipalName (eppn)	フェデレーション内で固有の個人識別子
eduPersonTargetedID	SP毎に固有の個人識別子（匿名識別子）
eduPersonAffiliation	Staff, Faculty, Student, Member
eduPersonScopedAffiliation	Staff, Faculty, Student, Member（@scopeつき）
eduPersonEntitlement	SP毎に固有の付加情報
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	表示用氏名
jaDisplayName	表示用氏名（日本語）
mail	E-mail アドレス
gakuninScopedPersonalUniqueCode	学生番号、職員番号（@scopeつき）

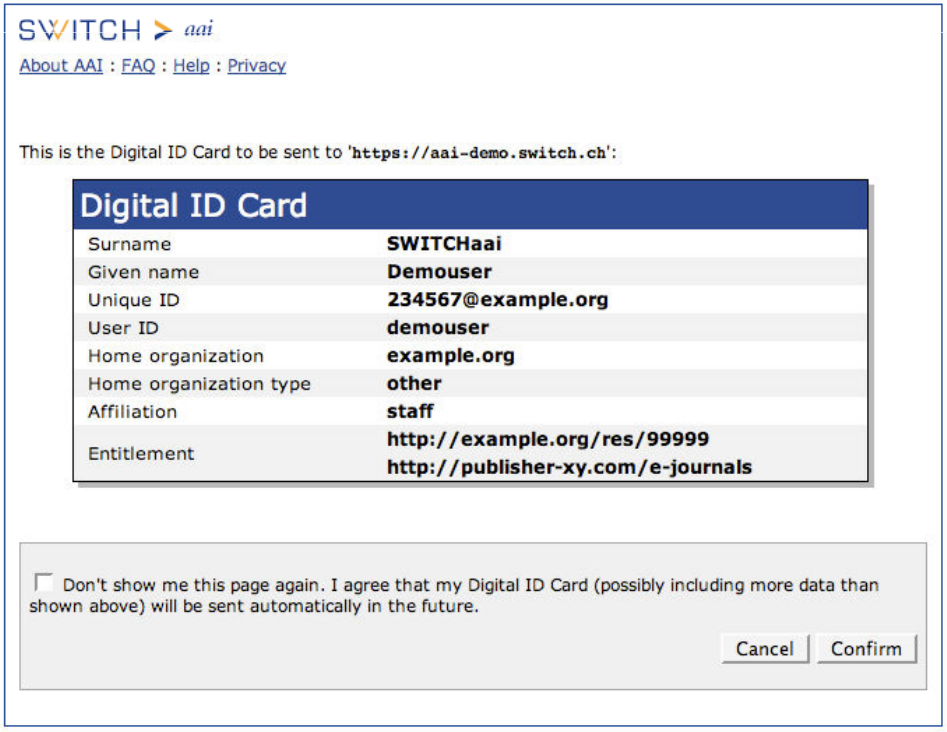
学認参加以前に収集した個人情報は目的外利用となるため本人同意が必要

個人情報保護法

- 個人情報の保護に関する法律（平成15年5月30日法律第57号）
  - 私立大学
- 独立行政法人等の保有する個人情報の保護に関する法律（平成15年5月30日法律第59号）
  - 国立大学（公立大学もこちらに準じる）
  - 利用目的以外の目的での保有個人情報の提供には、本人の同意が必要
    - 全てのSP（将来の追加を含む）に対する包括的な同意
    - SPごとの個別の同意

IdPにおけるユーザ同意機構の実装(uApprove)

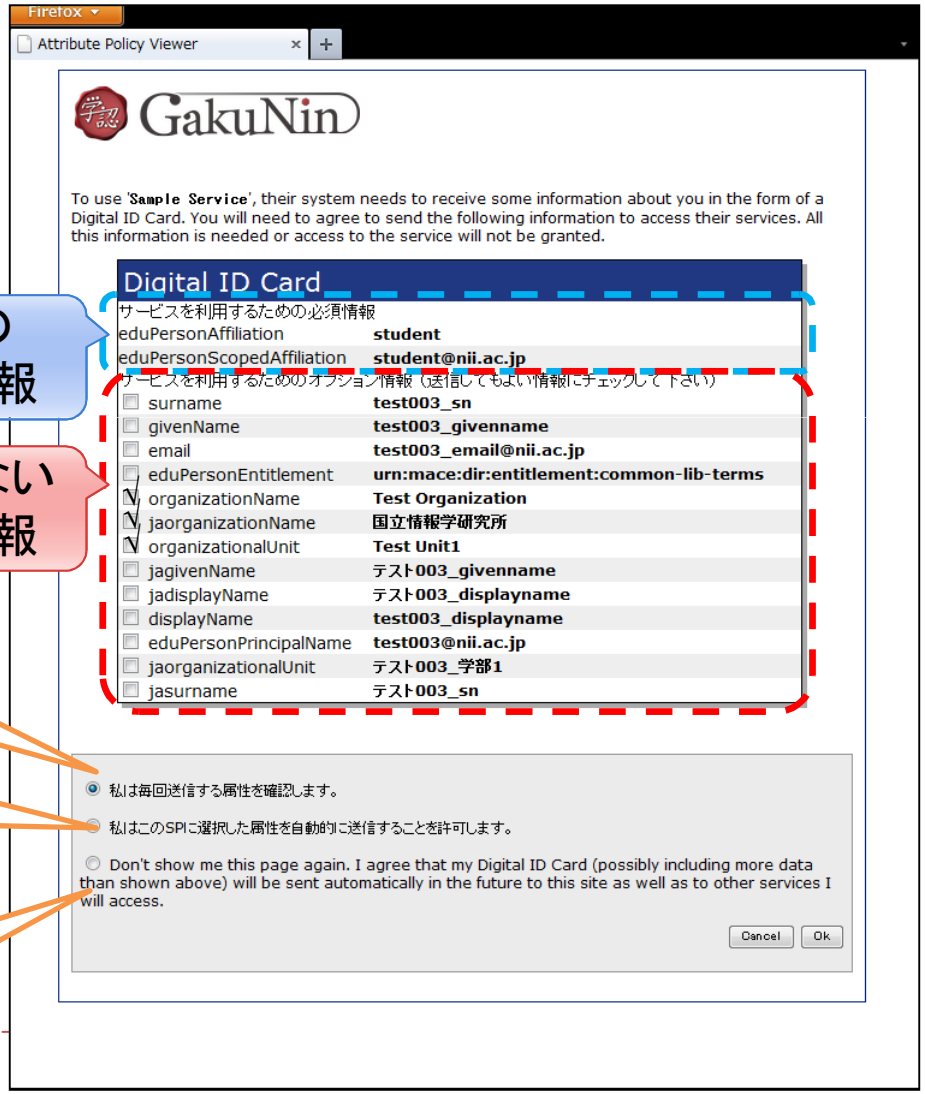
- SWITCH（スイス）から提供
  - Shibboleth IdPのプラグイン
- 送信される属性情報全てに対する、まとめての同意
  - どの属性情報が送信されるかは、IdPの管理者が指定する



http://www.switch.ch/aai/support/tools/uApprove.html

ユーザに選択権を与える拡張：uApprove.jp

- 送信が必須でない属性情報に関して、ユーザが送信の可否を個別に選択できる
- 将来の挙動について指定できる



設定の方法

- SPが用意するメタデータ中に必須かどうかの区別を定義

```
<md:RequestedAttribute isRequired="true"
FriendlyName="eduPersonAffiliation">
</md:RequestedAttribute>
```

- IdPのフィルタリングルール(attribute-filter.xml)でuApprove.jpの結果に従うように指示

```
<PolicyRequirementRule
xsi:type="uapprove:AttributeUapprove" />
<AttributeRule attributeID="eduPersonAffiliation">
    <PermitValueRule xsi:type="uapprove:AttributeUapprove"
isApproved="“true" />
</AttributeRule>
```

  - 詳細についてはWebをご参照ください。

uApprove.jpの開発状況

- 試験実装公開中(IdP 2.1.3, 2.1.5, 2.2.0)
  - http://www.gakunin.jp/docs/fed/uapprove-jp
- 実運用に耐えるバージョンを公開予定(IdP 2.3.x)
  - IdPでは、IdP 2.3.2以降の利用を推奨
    - Vulnerability of OpenSAML library included in prior to version 2.3.2

3. OpenIdP （特定組織に属さないIdP）

- OpenID と似ていますが、関係ありません。

学認利用支援に向けて

- 学認は2010年度から本格運用を開始
  - IdPは28機関が構築し、ユーザ総数は概算で45万（2011年9月14日現在）
- 各機関での整備は進んでいるが、まだまだこれから
  - 日本国内の高等教育機関は1200以上、ユーザ総数は350万以上（文部科学省、平成23年度学校基本調査）
    - 大学 780校、学生290万人、教員36万人（兼務含む）
    - 短大 387校、学生15万人、教員6500人（兼務含む）
    - 高専 64校、学生6万人、教員5000人（兼務含む）
- 学認利用を支援・促進する仕組みが必要
  - IdPホスティング
  - OpenIdP

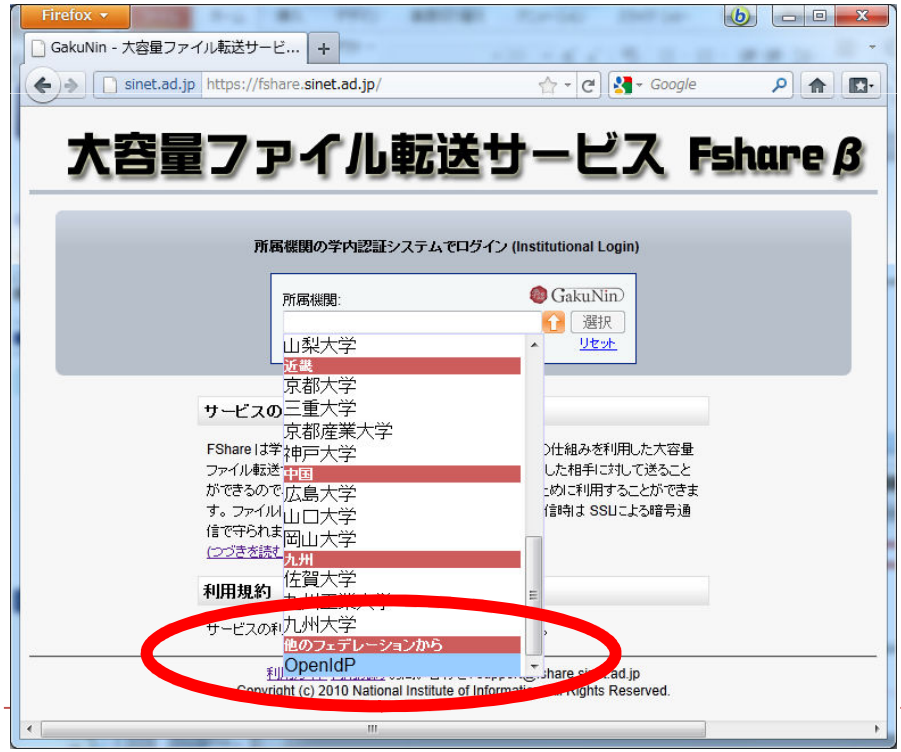
OpenIdP

- IdPの構築が完了していない機関ユーザ向けサービス
  - 学認には属さないIdP
- 学認サービスの「一部」が利用可能
  - 大容量ファイル転送サービス Fshare β
  - Communications service for sharing academic information
  - meatwiki
  - FaMCUs（テレビ会議用MCU）

  など
- ac.jpのメールアドレスを持つユーザであれば自由に登録可
  - メールの到達性を確認します
  - ac.jpドメイン以外にも対応可能
  - 登録可能ドメインの追加は openidp-admin@nii.ac.jp へ

大容量ファイル転送サービス Fshare β

- 電子メールの添付ファイルのようにして、学認参加機関のユーザどおしで、ファイルをやりとりできるサービス
- 送信先も学認参加機関のユーザでないといけない、という制約が厳しすぎる、という声を受け、OpenIdPでも利用可能にした



Communications service for sharing academic information

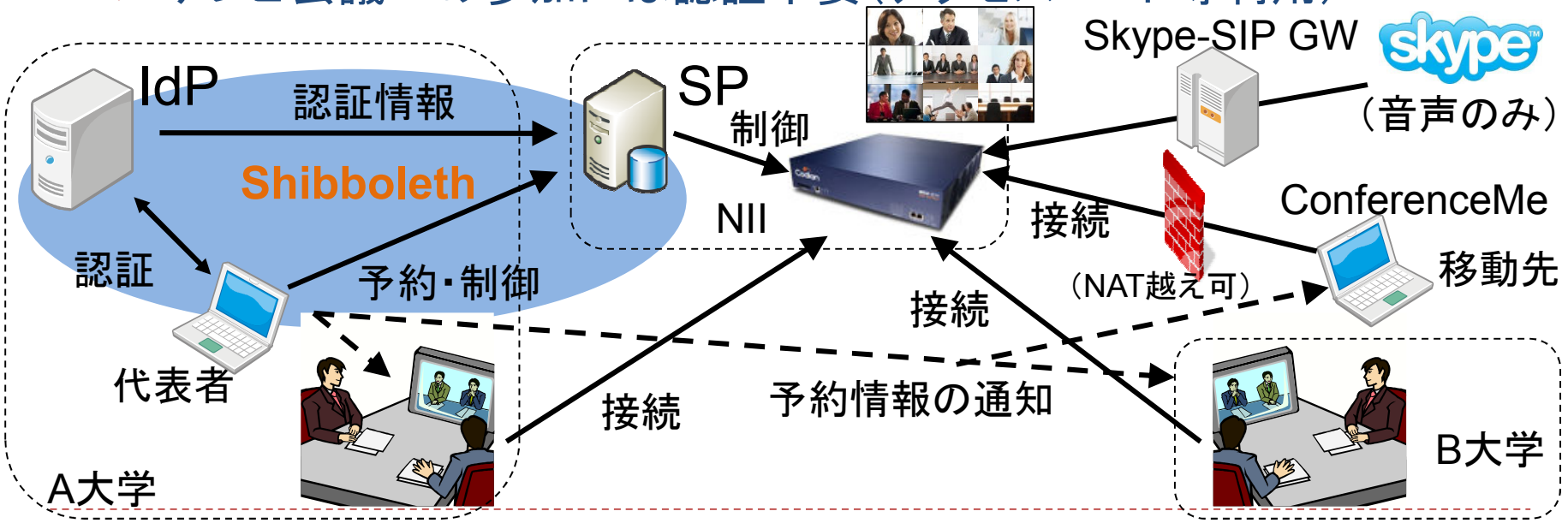
- 山形大学が提供する、科学技術の学術情報共有のための双方向コミュニケーションサービス

meatwiki

- 学認mAP機能を活用したグループベースのwikiサイト
- システムとしてconfluenceを採用

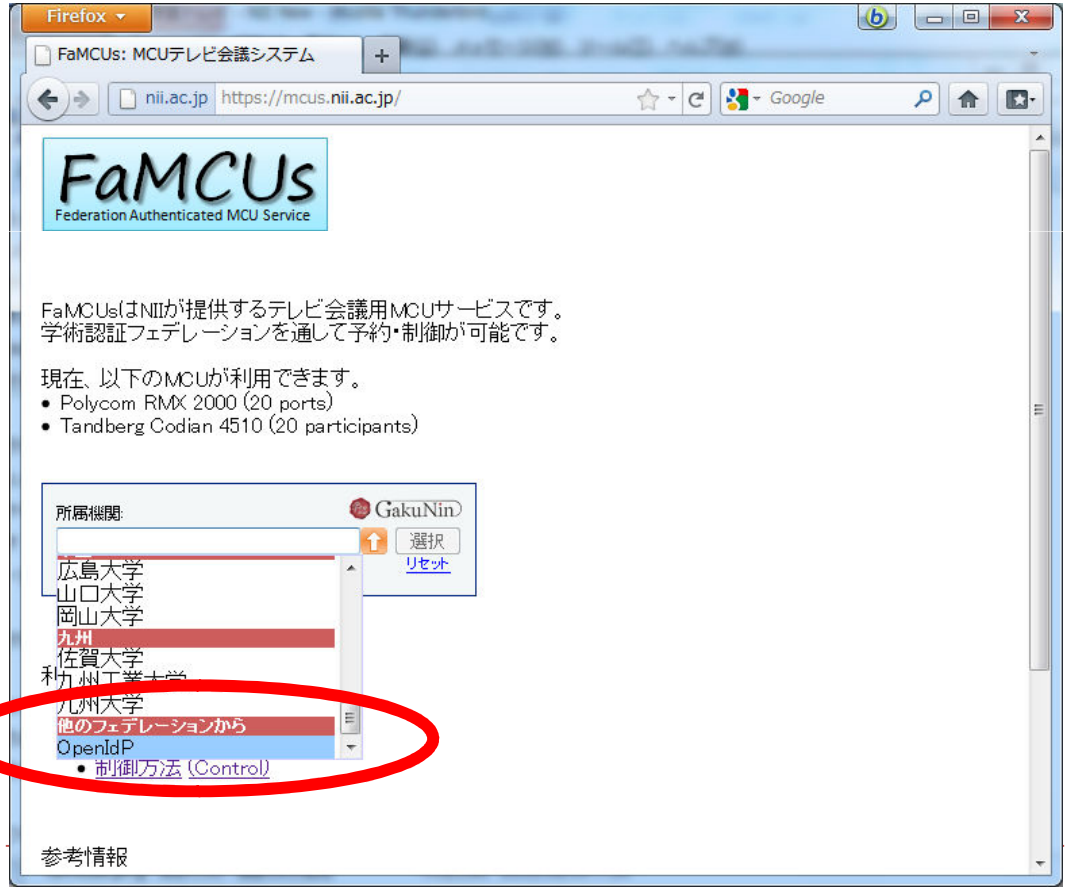
シボレスを用いたテレビ会議用MCU予約・制御システム

- 提供するMCU
  - Tandberg Codian MCU 4510 (最大12地点、HD対応)
  - Polycom RMX 2000 (最大20ポート、HD対応)
- 学認への対応
  - 予約と制御に認証を要求(教職員に限定、学生に権限委譲可)
  - テレビ会議への参加には認証不要(アクセスコード等利用)



FaMCUs（テレビ会議用MCU）へのアクセス

- MCUの予約は、学認参加機関の教職員に限るが、予約の変更やMCUの制御は、予約者の責任の下で委譲可



おわりに

- 今回紹介した新機能
  - 埋め込みDS (embedded DS)
  - IdP機関のためのユーザ同意機構 (uApprove.jp)
  - OpenIdP（特定組織に属さないIdP）
- この他にも
  - 学認事務システムの改良
  - IdP選択、確認のためのブラウザプラグイン
  - 学認mAP対応メーリングリストサービス

  などなど
  - 是非とも改善への
    ご要望をお寄せ下さい。

連絡先
国立情報学研究所（学認担当）
gakunin-office@nii.ac.jp