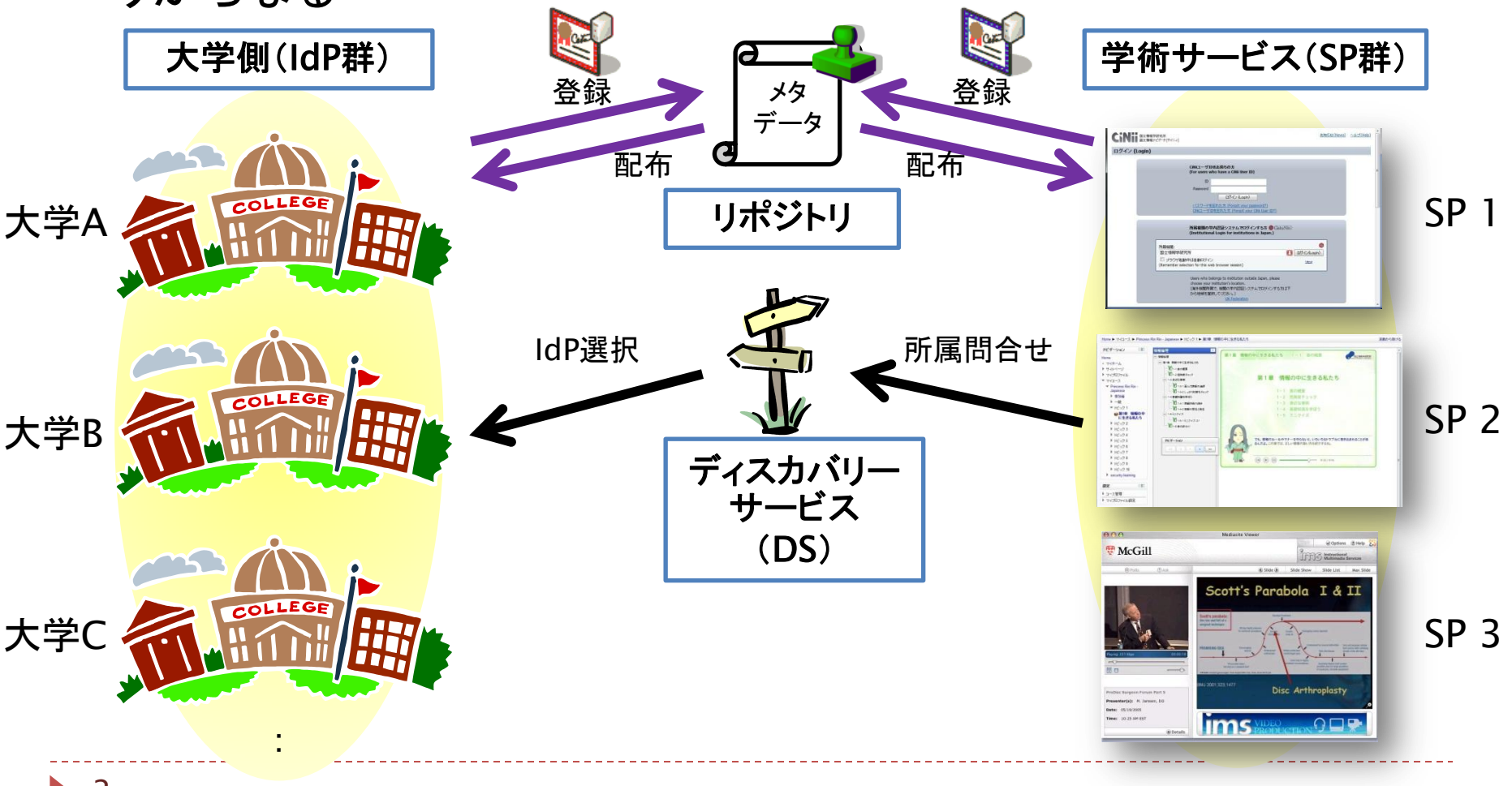
新しくなった学認申請システムの紹介

国立情報学研究所　学術認証推進室

フェデレーションの概要

- 最も単純なフェデレーションはIdP群・SP群・DSおよびリポジトリからなる

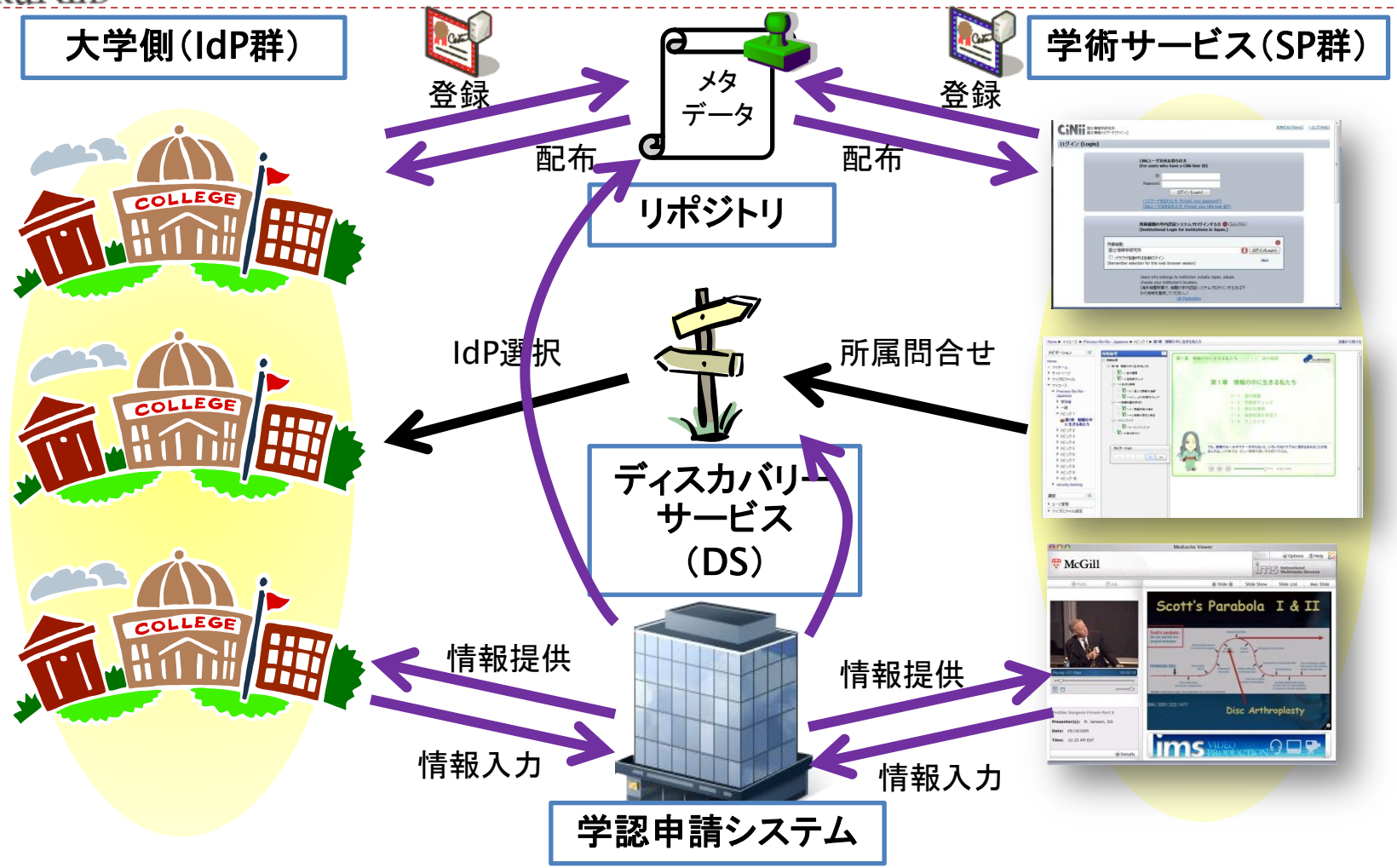


IdP管理者・SP管理者へのさまざまな要求

- 「参加するにはメタデータを作成して提出してください」
  - →メタデータって何？？
- 「新しいSPに〇〇属性を送信してください」
  - →新しいSPが出てくる度に作業しなきゃいけないの？
- 「××大学のIdP経由で認証できないんですけど」
  - →IdPの方の設定に問題があるんじゃないの？

IdP・SP・DSのインストールだけではカバーできない部分が存在

学認申請システムの位置付け



リポジトリ・DSと並んでIdP–SP間を仲介する立場で機能不足を解消

従来の「学認申請システム」の機能

- 学認への参加・変更申請書の作成
  - 入力された申請者・機関の情報からPDFを出力する
- テンプレートを元にしたメタデータの自動生成
  - 申請者・機関の情報
  - 証明書の登録

申請して，最低限のメタデータを作る機能のみ提供

新しい「申請システム」の新機能

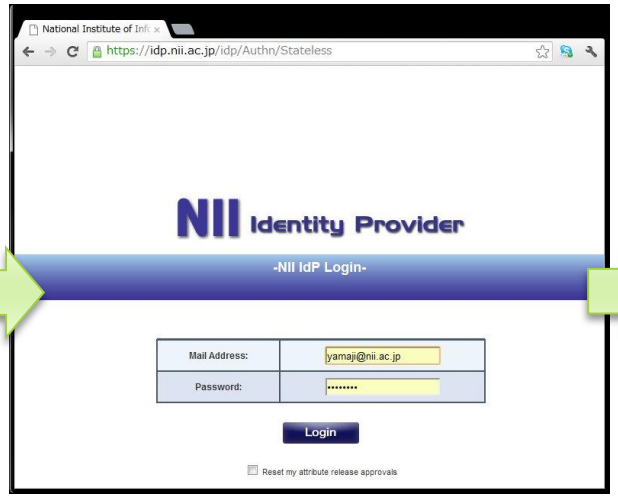
- (1)利用可能SP/IdPの取捨選択
  - DSで表示されるIdPリストを制御
- IdP/SPメタデータに情報付与
  - (2)属性情報対応
    - 利用者による送信属性制御
    - IdP送信属性フィルタ自動生成
  - (3)mdui対応
    - ログイン画面でのSP視覚化
    - IdPの地理的分類
    - 選択IdP候補提示

いきなり番外編:
SPのページにDSを埋め込める機能

- DSの新(?)機能
  - JavaScriptで実装されたEmbedded DS
- SPにDS機能を埋め込める！
  & 他SPで選択したIdPを覚えてくれる！

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

(1)利用可能SP/IdP取捨選択



使えないのならIdPをリストに出さないでよ！

(1)利用可能SP/IdP取捨選択

IdP管理者が，フィルタ設定を行ったSPを選択

SP管理者が，利用可能IdPを選択

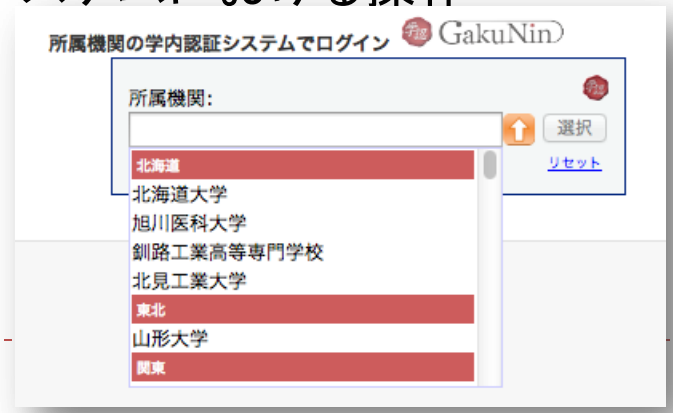
AND

https://office.gakunin.nii.ac.jp/ProdFed/export/discofeed/PSxxxxJP

```
[{
 "entityID":
     "https://idp.example.ac.jp/idp",
 "DisplayNames": [{
  "value": “Test IdP",
  "lang": "en"
  }]
},
{
 "entityID":
 "https://idp2.nii.ac.jp/idp/shibboleth",
…
```

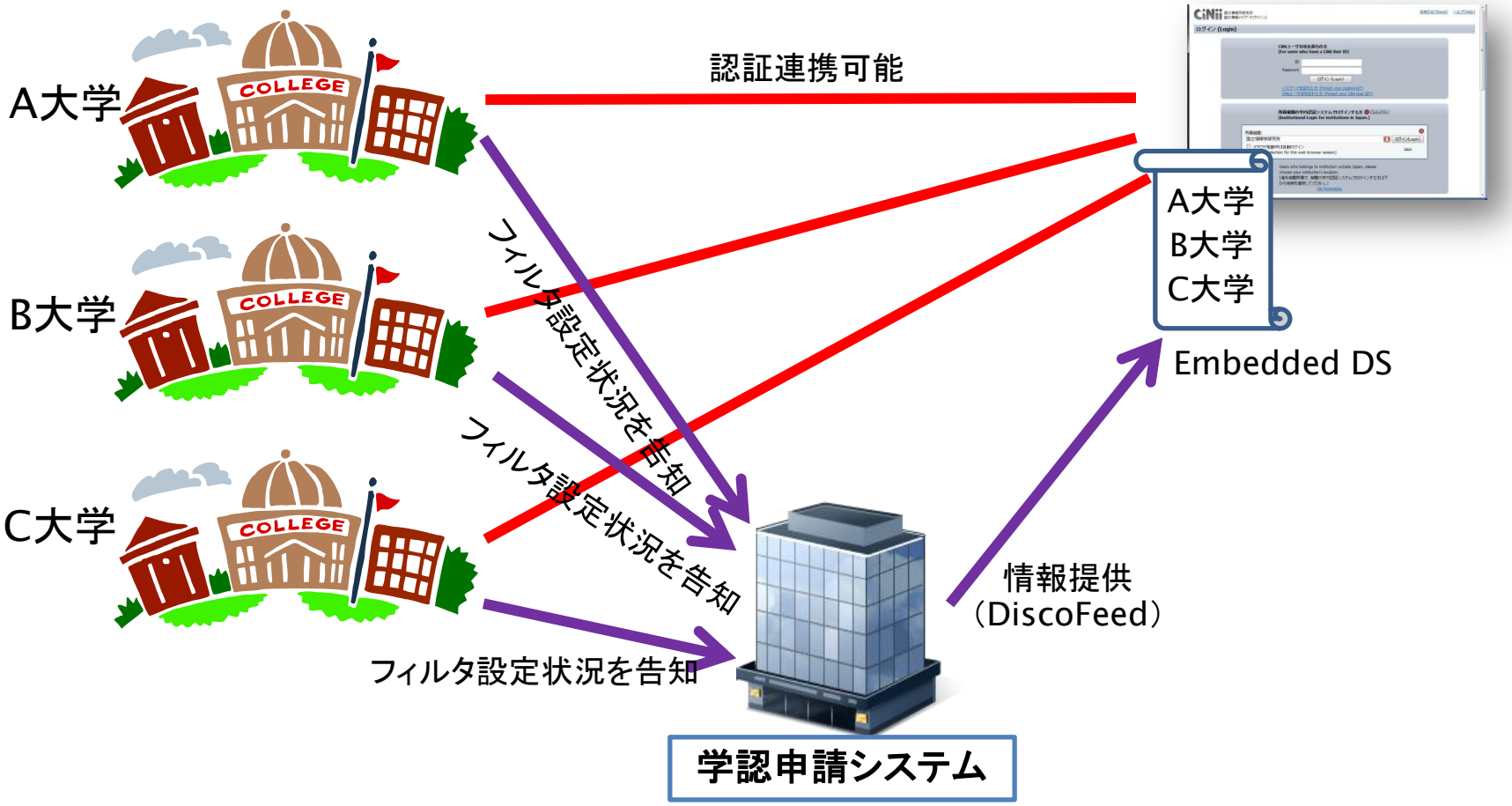
JSON形式（DiscoFeed形式）

①学認申請システムにおける操作

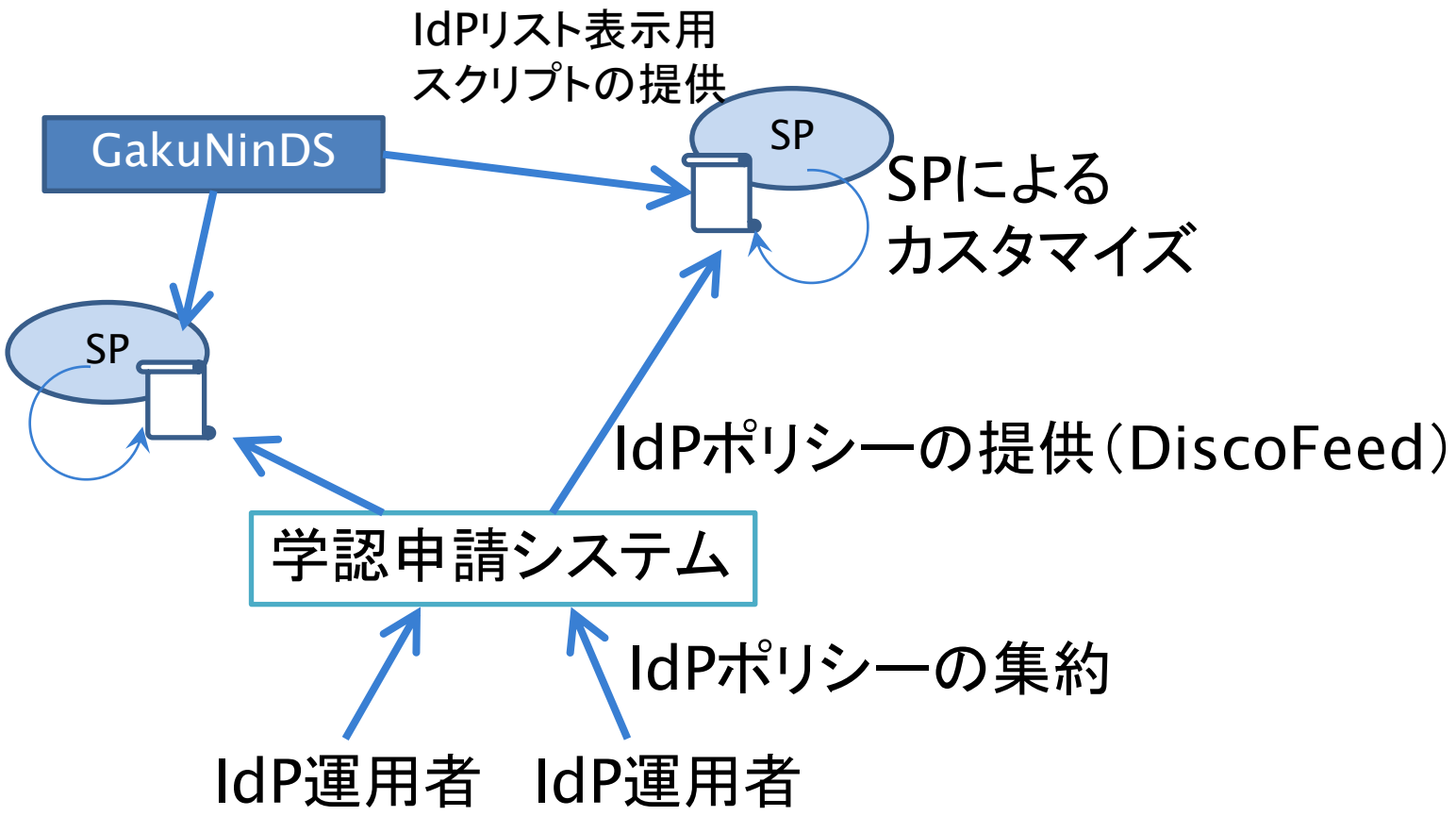


②IdP管理者が設定を行っている場合，かつSP管理者が選択した場合のみEmbedded DSにIdPを表示する

(1)利用可能SP/IdP取捨選択: 使用例



(1)利用可能SP/IdP取捨選択



新しい申請システムでできるようになったこと

- (1)利用可能SP/IdP取捨選択
  - DSで表示されるIdPリストを制御

- IdP/SPメタデータに情報付与
  - (2)属性情報対応
    - 利用者による送信属性制御
    - IdP送信属性フィルタ自動生成
  - (3)mdui対応
    - ログイン画面でのSP視覚化
    - IdPの地理的分類
    - 選択IdP候補提示

メタデータ
(2)属性情報対応

- IdPの運用では，Shibbolethのattribute-filter.xmlのメンテナンスが必要
  - SPが増えるごとに，SPが要求する属性をattribute-filterに手作業で追加していく必要あり

なんとかメンテナンス性を向上できないか？

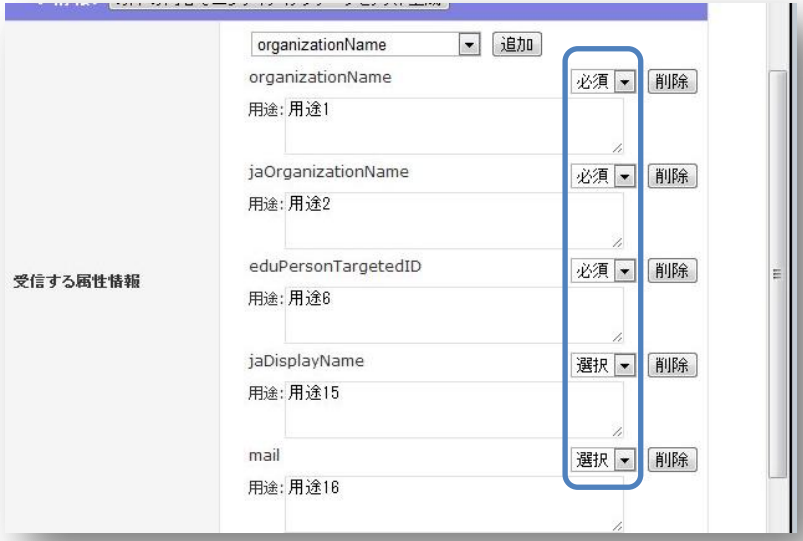
まずは，SPが要求する属性情報を電子的に取得する必要あり

さらに　必須属性／任意属性の問題

- 大学は，なるべく個人情報は送りたくない
  - しかし個人情報を送らないと一部機能が使えない場合がある
    - e.g. パーソナライズ機能
      eduPersonTargetedID / eduPersonPrincipalName
      アカウント作成時の自動フィル（氏名，メールアドレス，機関名等）
- 大学（IdP管理者）が「送らない」を選択すると，機能を使いたい利用者が不満を持つし，
  「送る」を選択すると，その機能が不要な利用者が不満を持つ

任意属性については利用者が送信可否を選択できるべき

メタデータ
(2)属性情報対応



①学認申請システムにSPが要求する

```
<EntityDescriptor …>
  …
 <AttributeConsumingService index="1"
isDefault="true">
    …
<RequestedAttribute
FriendlyName="eduPersonPrincipalName"
Name="urn:oid:1.3.6.1.4.1.5923.1.1.1.6"
NameFormat="urn:oasis:names:tc:SAML:2.0:at
trname-format:uri" isRequired="true“/>
…
```

生成されるSPのメタデータ

'GakuNin mAP (SP)' を利用するためにはユーザ情報のフォームの中のあなたについての情報をシステムに送信する必要があります。あなたはサービスにアクセスするために以下の情報を送信することに同意する必要があります。

ユーザ情報

サービスを利用するための必須情報

eduPersonPrincipalName	takeshi@nii.ac.jp

サービスを利用するためのオプション情報
(送信してもよい情報をチェックして下さい)

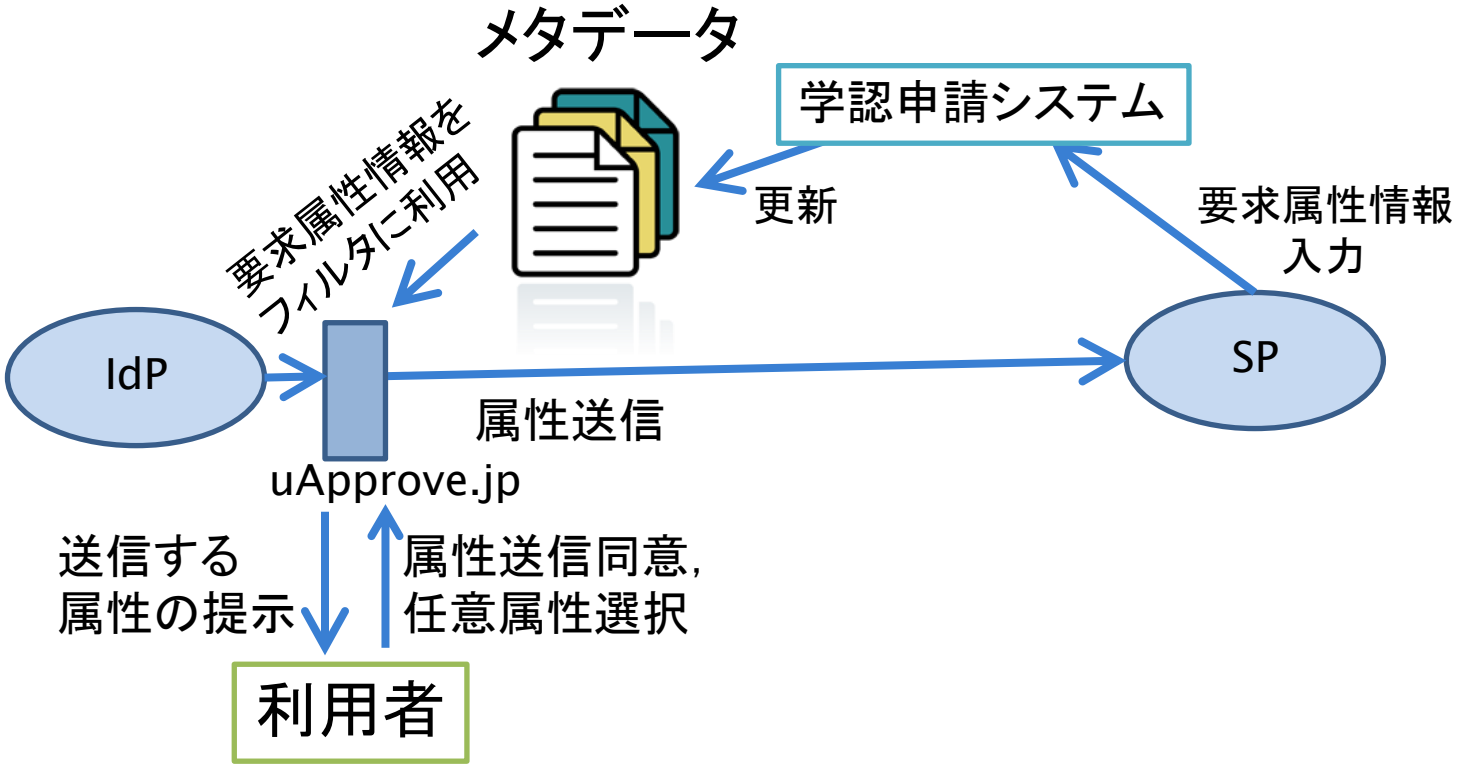
☐ organizationName	National Institute of Informatics
☐ email	takeshi@nii.ac.jp
☐ jaDisplayName	西村　健
☐ jaOrganizationName	国立情報学研究所

②要求属性に応じた属性送信，利用者の送信可否選択

uApprove.jpプラグインによる選択画面

(2)属性情報対応
使用例: uApprove.jpとの連携

IdPプラグインであるuApprove.jpと連携することにより,
送信が任意な属性を送信するかどうかを利用者が決めることができるようになる



cf. https://www.gakunin.jp/docs/fed/uapprove-jp

(1)SP取捨選択と(2)属性情報を利用して: IdP送信属性フィルタ自動作成対応

- 例 https://office.gakunin.nii.ac.jp/ProdFed/export/attribute_filter/PI0001JP

attribute-filter.xml - TeraPad

ファイル(F) 編集(E) 検索(S) 表示(V) ウィンドウ(W) ツール(T) ヘルプ(H)

```
<?xml version="1.0"?>
<afp:AttributeFilterPolicyGroup xmlns:afp="urn:mace:shibboleth:2.0:afp" xmlns:basic="urn:mace:shibboleth:2.0:afp
  <!--  Release the transient ID to anyone -->
  <afp:AttributeFilterPolicy id="releaseTransientIdToAnyone">
    <afp:PolicyRequirementRule xsi:type="basic:ANY"/>
    <afp:AttributeRule attributeID="transientId">
      <afp:PermitValueRule xsi:type="basic:ANY"/>
    </afp:AttributeRule>
  </afp:AttributeFilterPolicy>
<afp:AttributeFilterPolicy id="PolicyFor_example_com_sp">
  <afp:PolicyRequirementRule value="https://example.com/sp" type="basic:AttributeRequesterString"/>
  <afp:AttributeRule attributeID="organizationName">
    <afp:PermitValueRule type="ANY"/>
  </afp:AttributeRule>
  <afp:AttributeRule attributeID="jaOrganizationName">
    <afp:PermitValueRule type="ANY"/>
  </afp:AttributeRule>
  <afp:AttributeRule attributeID="organizationalUnitName">
    <afp:PermitValueRule type="ANY"/>
  </afp:AttributeRule>
  <afp:AttributeRule attributeID="jaOrganizationalUnitName">
    <afp:PermitValueRule type="ANY"/>
  </afp:AttributeRule>
  <afp:AttributeRule attributeID="eduPersonPrincipalName">
    <afp:PermitValueRule type="ANY"/>
  </afp:AttributeRule>
  <afp:AttributeRule attributeID="eduPersonTargetedID">
    <afp:PermitValueRule type="ANY"/>
```

新しい申請システムでできるようになったこと

- (1)利用可能SP/IdP取捨選択
  - DSで表示されるIdPリストを制御

- IdP/SPメタデータに情報付与
  - (2)属性情報対応
    - 利用者による送信属性制御
    - IdP送信属性フィルタ自動生成
  - **(3)mdui対応**
    - **ログイン画面でのSP視覚化**
    - **IdPの地理的分類**
    - **選択IdP候補提示**

メタデータ (3)mdui対応

- mduiとは？
  - SAML V2.0 Metadata Extensions for Login and Discovery User Interface Version 1.0
  - https://www.oasis-open.org/committees/download.php/40270/sstc-saml-metadata-ui-v1.0-wd06.pdf

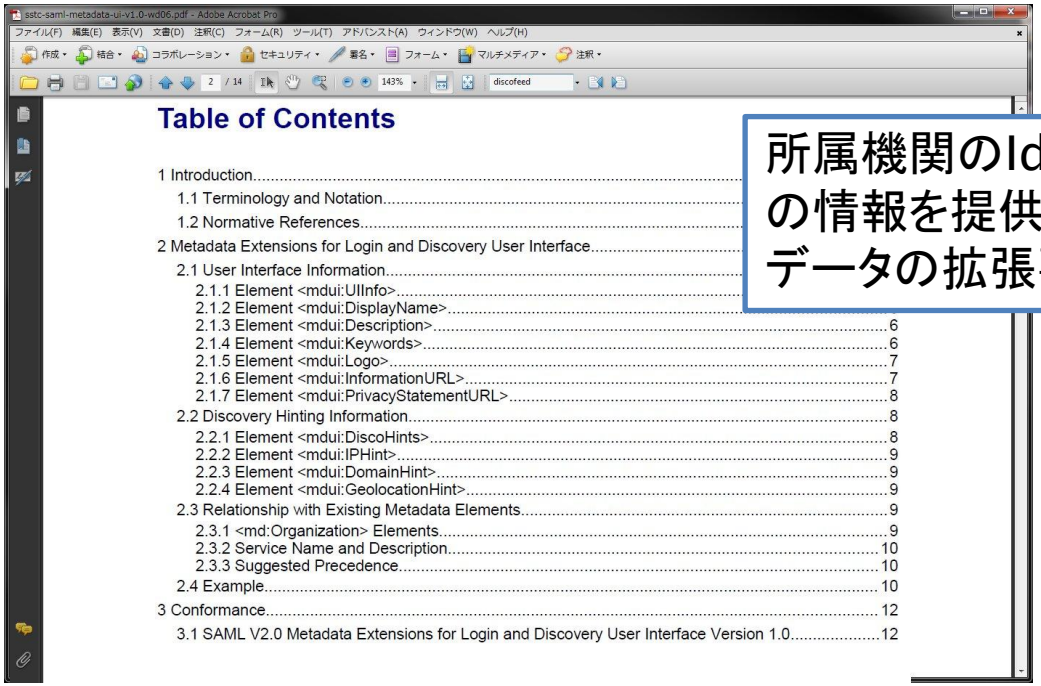


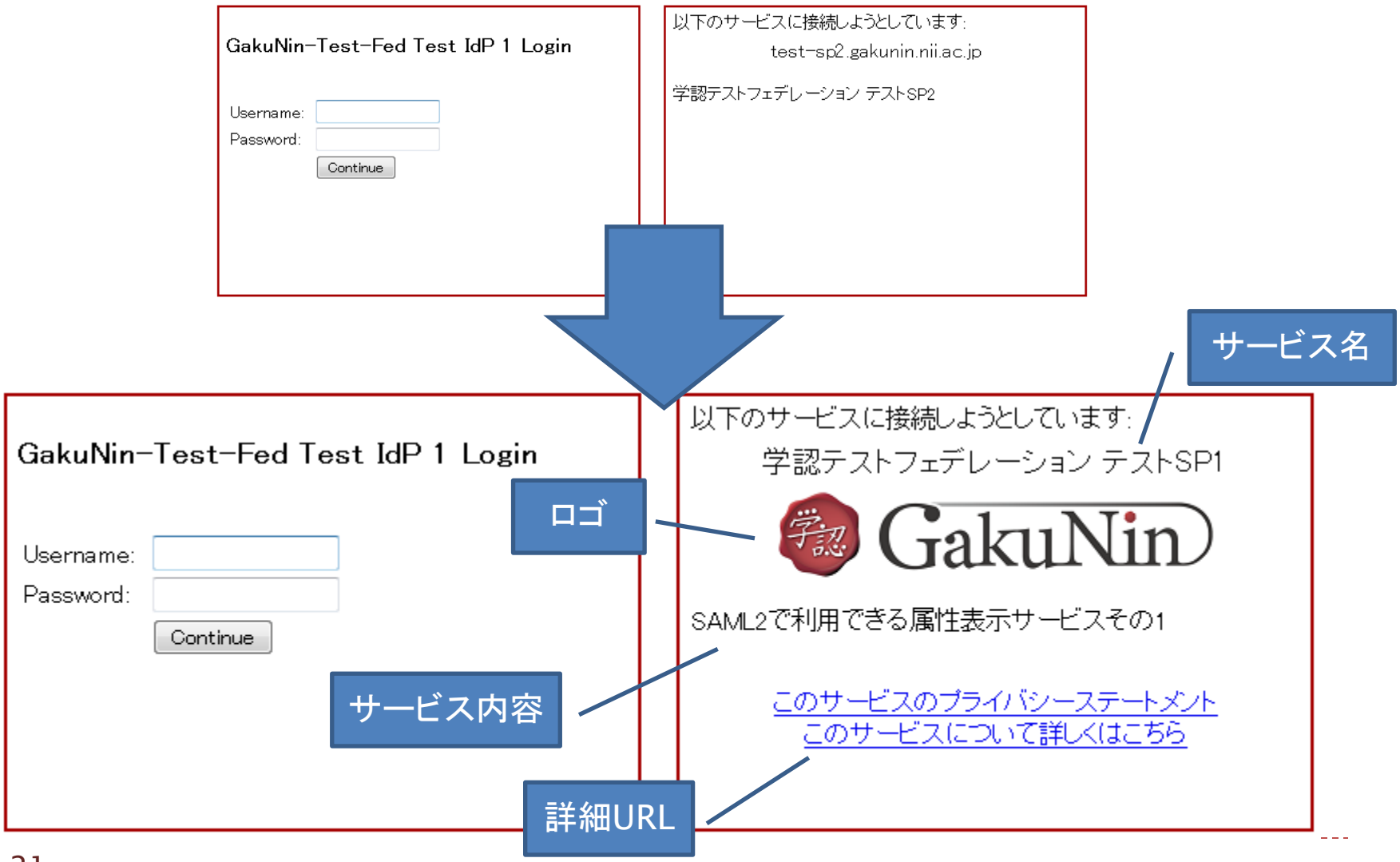
Table of Contents

所属機関のIdPが簡単に探せるなどの情報を提供するためのSAMLメタデータの拡張要素

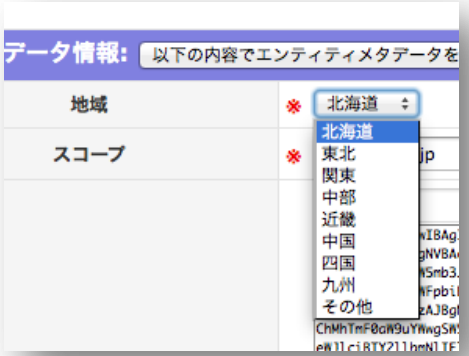
メタデータ
(3)mdui対応: User Interface Information

- User Interface Information (UIInfo)
  - <mdui:DisplayName>
    - DSでの表示名に利用
  - <mdui:Description>
    - 新しいShibbolethではログイン画面でSPのサービス内容を表示
  - <mdui:Keywords>
    - IdPの場合はDSの地域分類に用いる地域名（北海道，東北，…）
  - <mdui:Logo>
    - 新しいShibbolethではログイン画面でSPのロゴを表示
  - <mdui:PrivacyStatementURL>
    - 新しいShibbolethではログイン画面でSPのポリシーURLを表示

(3)mdui対応: UIInfoの使用例 ログイン画面でのSP視覚化



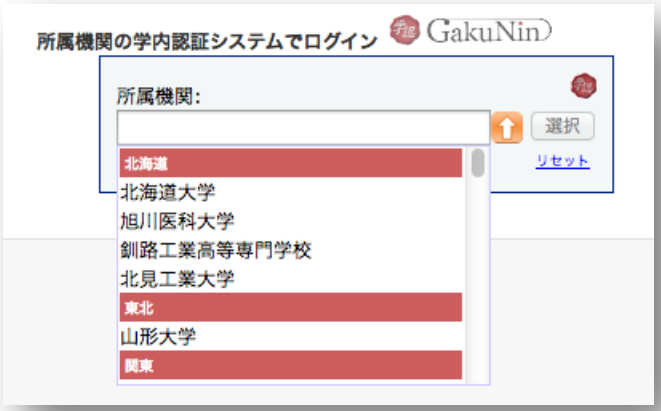
(3)mdui対応: UIInfoの使用例
IdPの地理的分類



①学認申請システムにて地域を入力

```
<EntityDescriptor ...>
 ...
 <Extensions>
  <mdui:UIInfo
       xmlns:mdui="urn:oasis:names:tc:
SAML:metadata:ui">
        <mdui:Keywords xml:lang="en">
           category:location:hokkaido
        </mdui:Keywords>
  </mdui:UIInfo>
 </Extensions>
...
```

②生成されるIdPのメタデータ



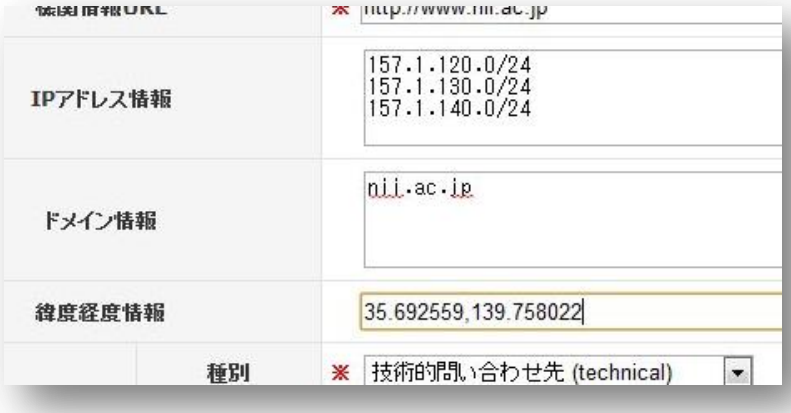
③DSに分類として反映される

※ 初期値は運用責任者の住所から自動推定されます

メタデータ
(3)mdui対応: Discovery Hinting Information

- Discovery Hinting Information (DiscoHints)
  - <mdui:IPHint>
    - 登録されたIPアドレス範囲内からのアクセスならばDSで優先表示
  - <mdui:DomainHint>
    - 登録されたドメインからのアクセスならばDSで優先表示
  - <mdui:GeolocationHint>
    - 登録された緯度経度情報の近くからのアクセスならばDSで優先表示（今年度中に実装予定）

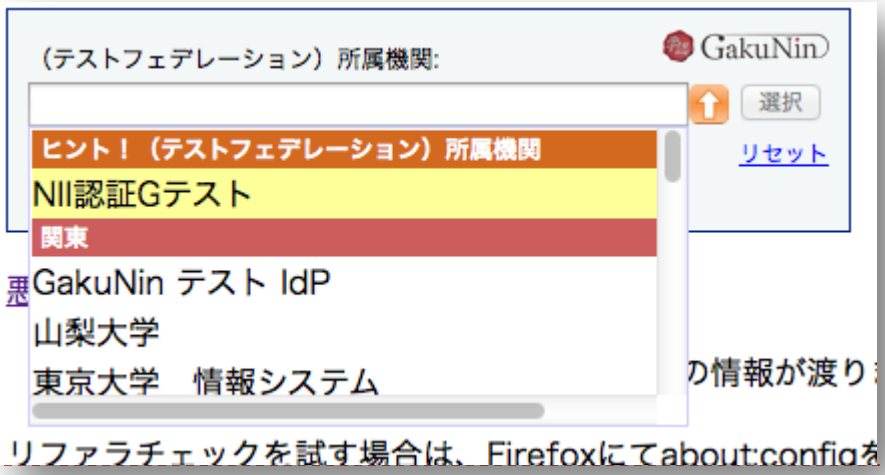
メタデータ
(3)mdui対応: DiscoHintsの例



①学認申請システムにて条件入力

```
<EntityDescriptor ...>
 ...
 <Extensions>
   <mdui:DiscoHints xmlns:mdui="urn:
oasis:names:tc:SAML:metadata:ui">
      <mdui:IPHint>136.187.0.0/16
      </mdui:IPHint>
      <mdui:IPHint>157.1.0.0/16
      </mdui:IPHint>
   </mdui:DiscoHints>
</Extensions>
...
```

②生成されるIdPのメタデータ



③条件にマッチすればヒントとして
IdPリストの最上部に当該IdPを表示

学認申請システム新機能のまとめ

- (1)利用可能SP/IdP取捨選択
  - DSで表示されるIdPリストを制御

メタデータ

- (2)属性情報対応
  - 利用者による送信属性制御
  - IdP送信属性フィルタ自動生成
- (3)mdui対応
  - ログイン画面でのSP視覚化
  - IdPの地理的分類
  - 選択IdP候補提示

他にも，申請関係の新機能

- 運用責任者による電子的な確認機能（申請書の押印・郵送不要）
- 複数担当者への対応
- OpenIdP対応
- IdPアンケート機能

学認申請システムが各種情報を仲介し、より良い環境を提供します

もっと詳しい情報は

- 学認ホームページ – 参加について
  - https://www.gakunin.jp/docs/fed/join
    - 学認申請システムのURL，操作マニュアル等

- 学認への参加に関するお問い合わせ
  - gakunin-office@nii.ac.jp