



学認への参加手続きと申請システム

国立情報学研究所 学認事務局

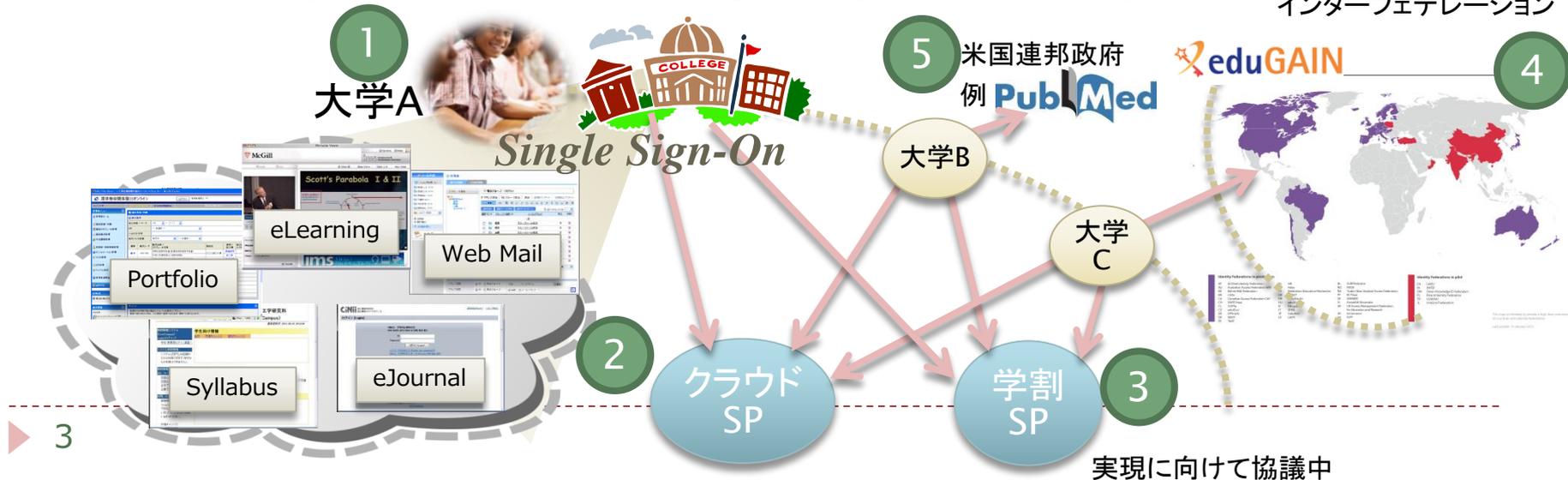
学術認証フェデレーション 「学認」の今



GakuNin

学術認証フェデレーション「学認」 (2009～)

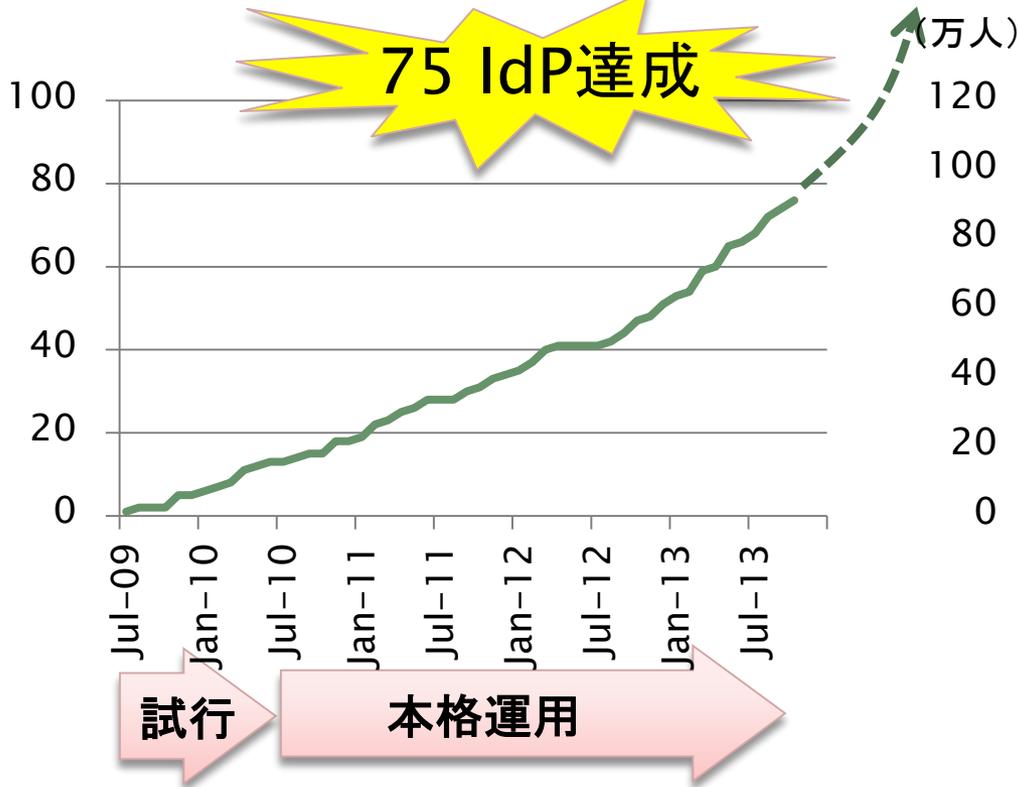
1. 大学におけるオンライン認証機構のデファクトスタンダード
 - ・ 国際標準のSSO機構によるスムーズなアクセスが大学に急速に波及中
2. 大学ICTインフラのクラウド活用のカギ
 - ・ 利便性の高いサービスを低コストで導入
3. 信頼性の高いID情報をセキュアに提供
 - ・ インターネット学割にも利用できる仕組みとして企業も注目
4. 全世界の学術インフラが繋がる標準認証機構
 - ・ 日本からの積極的な伝道によりアジア各国も準備中
5. 米国政府系サービスにも接続可能な学認の高信頼性



学認参加IdPの推移(2013/10/15現在)

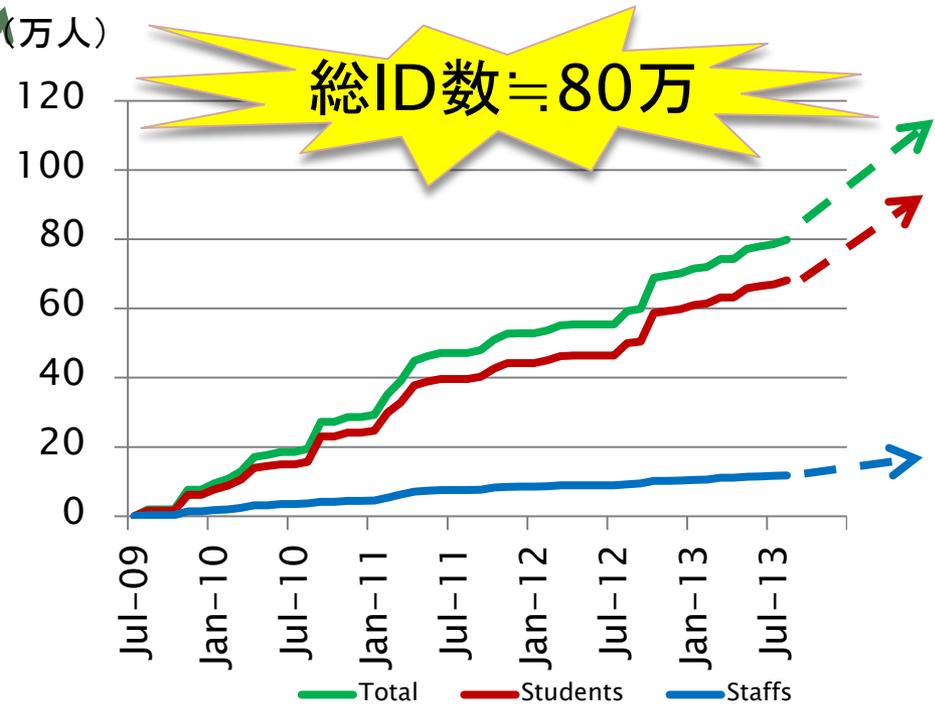
機関数

75 IdP達成



ユーザ数

総ID数=80万



高等教育人口は350万人(文部科学省)

学生の割合は、80%強

学認参加IdP (2013年10月現在)

- ▶ 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
- ▶ 北海道大学
- ▶ 筑波大学
- ▶ 佐賀大学
- ▶ 成城大学
- ▶ 東邦大学
- ▶ 三重大学
- ▶ 日本大学
- ▶ 旭川医科大学
- ▶ 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
- ▶ 山梨大学
- ▶ 広島市立大学
- ▶ 大阪大学
- ▶ 宮崎大学
- ▶ 横浜国立大学
- ▶ 放射線医学総合研究所
- ▶ 釧路工業高等専門学校
- ▶ 北見工業大学
- ▶ 広島工業大学
- ▶ 金沢大学
- ▶ 愛媛大学
- ▶ 鈴鹿工業高等専門学校
- ▶ 奈良先端科学技術大学院大学
- ▶ 奈良教育大学
- ▶ 立命館大学
- ▶ 東京医科歯科大学
- ▶ 札幌医科大学
- ▶ 国立高等専門学校機構
- ▶ 関西大学
- ▶ 大阪教育大学
- ▶ 京都教育大学
- ▶ 京都府立大学
- ▶ 豊橋技術科学大学
- ▶ 福井工業高等専門学校
- ▶ 静岡大学
- ▶ 宮城教育大学
- ▶ 帝塚山大学
- ▶ 東京歯科大学
- ▶ 昭和大学
- ▶ NTT東日本関東病院
- ▶ 東京海洋大学
- ▶ 創価大学
- ▶ 東京都医学総合研究所
- ▶ CCC-TIES
- ▶ 中部大学
- ▶ 国立女性教育会館
- ▶ 琉球大学
- ▶ 東京農工大学
- ▶ 芝浦工業大学
- ▶ 東京学芸大学
- ▶ 福井大学
- ▶ 苫小牧工業高等専門学校
- ▶ 大阪体育大学
- ▶ 北九州工業高等専門学校
- ▶ 福岡工業大学
- ▶ 武蔵学園
- ▶ 長岡工業高等専門学校
- ▶ 千葉工業大学
- ▶ 広島修道大学
- ▶ 徳島大学



GakuNin

学認参加SPの推移（2013/10/15現在）

メタデータ登録数（公開準備中を含む）

▶ コンテンツ系サービス

- ▶ 電子ジャーナル
- ▶ 機関リポジトリ
- ▶ 文献検索
- ▶ 論文・業績情報管理
- ▶ 開発環境（ソフトウェア）

▶ 基盤系サービス

- ▶ 無線ネットワークアクセス
- ▶ Eラーニング
- ▶ テレビ会議
- ▶ ファイル共有
- ▶ クラウド環境

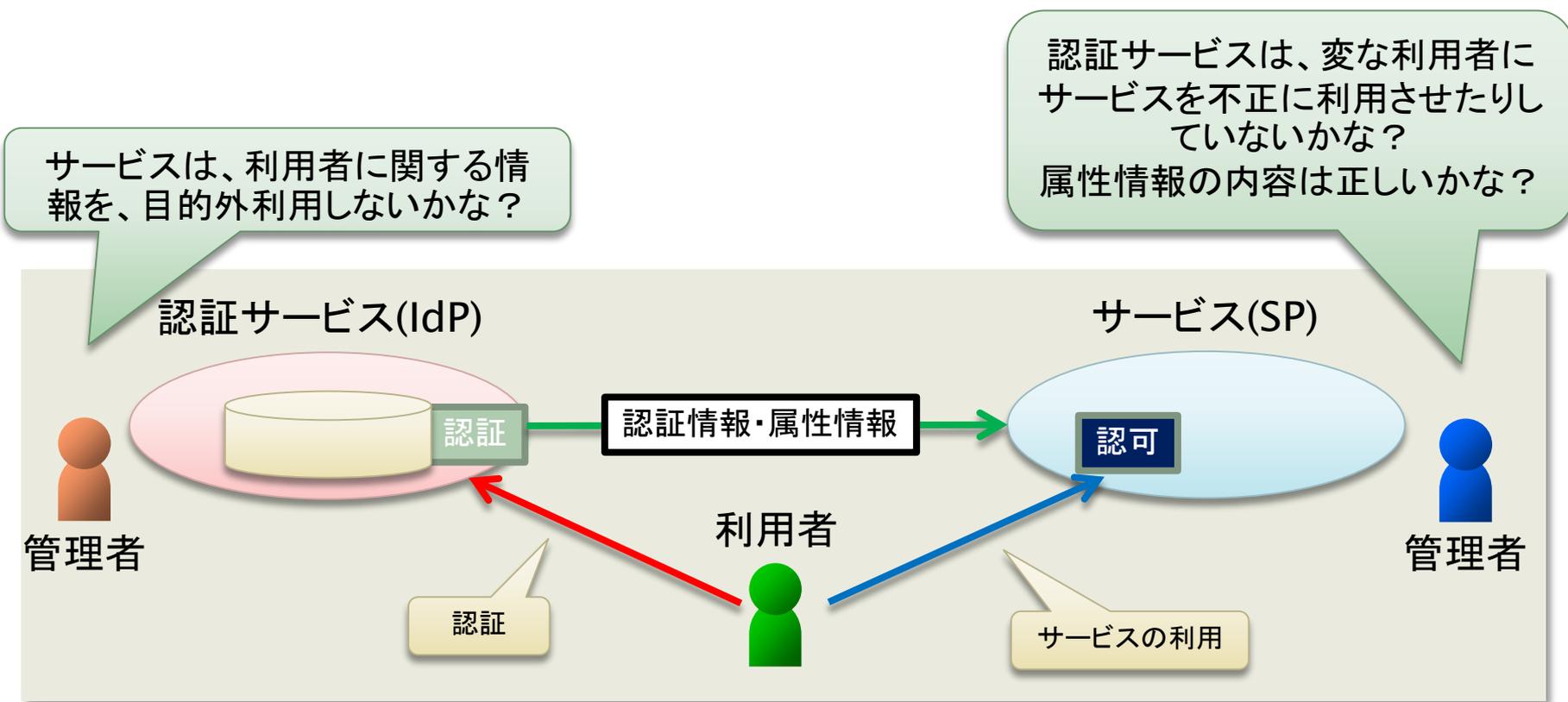
- ▶ SITF (Student Identity Trust Framework) による学割サービスの実現を検討中





SSO技術の組織間利用での信頼

- ▶ 認証と認可の分離
- ▶ 異なる組織が個別に管理するため、相互の信頼が重要





GakuNin

学認で定めるIdPの要件 (運用基準)

- ▶ 組織の構成員であることの保証
 - ▶ 卒業、退職などによる異動の適切な反映
 - ▶ 名誉教授、OB、図書館の地域内利用者、その他ゲスト等の扱い
- ▶ 識別子再利用についての考慮
 - ▶ 同一識別子を利用する場合は、一定期間あける
- ▶ ユーザの同一性の保証
 - ▶ パスワード配布時の本人確認
 - ▶ 適切に管理された役職アカウント
- ▶ 個人情報保護への対応
 - ▶ 国公立大学ではオプトインが原則
- ▶ ログの保存
 - ▶ インシデント対応のための、eduPersonTargetdIDやtransient-idの記録

機関として責任を持った
IDおよび属性の保証

⇒定期アンケート（毎年）によるチェックとフィードバックで維持

- ▶ IdP of The Year 2012 を大阪大学が受賞
- ▶ 今年もアンケートを実施いたしました！



学認にどのようにして
参加すればいいのか？



参加の流れ (IdPの場合)

- ▶ テストフェデレーションIdP設置申し込み
 - ▶ 学認申請システムを操作
- ▶ IdPメタデータ登録完了のお知らせ
 - ▶ メールでお知らせ (おおむね1週間以内)
- ▶ テストフェデレーションでテスト
- ▶ 運用フェデレーションIdP設置申し込み
 - ▶ 学認申請システムを操作
 - ▶ 申請書をNIIへ送付
- ▶ IdPメタデータ登録完了のお知らせ
 - ▶ メールでお知らせ (最長で1ヶ月以内)
- ▶ 本格運用の開始



GakuNin

まずは入り口

- ▶ <https://office.gakunin.nii.ac.jp>
- ▶ 学認への参加申請は、必ずここを通じて行われます

学認申請システム / GakuNin Registration System

- [運用フェデレーションに対する申請はこちらへ](#)
- [テストフェデレーションに対する申請はこちらへ](#)



メタデータの自動生成

- ▶ 学認申請システムに入力した情報から、自動でメタデータが生成されます
 - ▶ DSでの表示
 - ▶ 利用可能SP/IdPの取捨選択

メタデータの活用：DSでの表示

▶ 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>

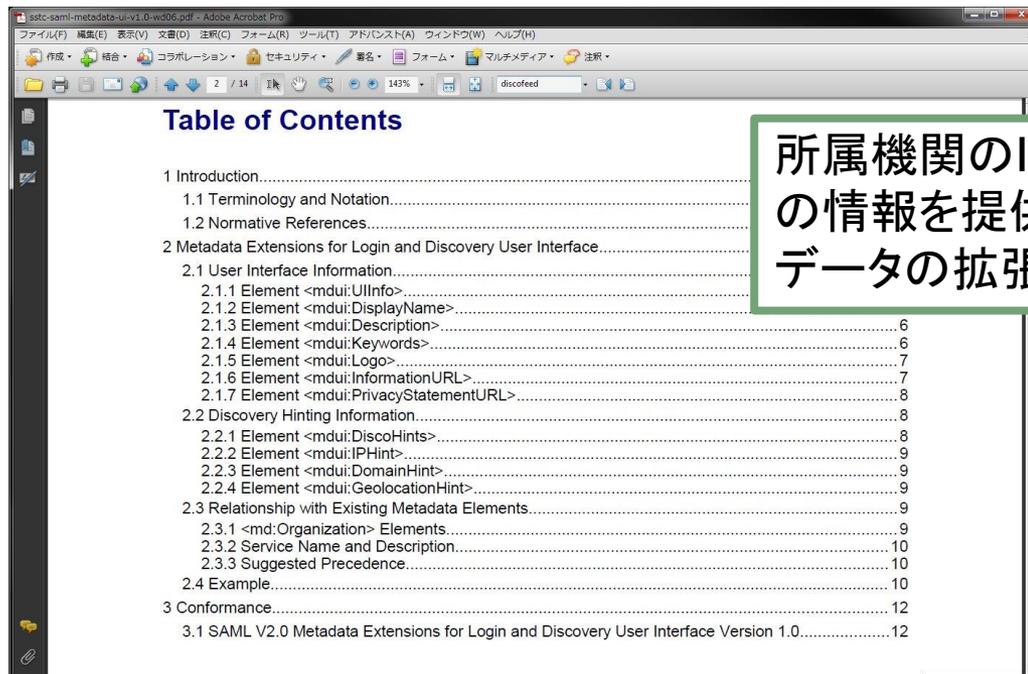


Table of Contents	
1	Introduction.....
1.1	Terminology and Notation.....
1.2	Normative References.....
2	Metadata Extensions for Login and Discovery User Interface.....
2.1	User Interface Information.....
2.1.1	Element <mdui:UInfo>.....
2.1.2	Element <mdui:DisplayName>.....
2.1.3	Element <mdui:Description>.....
2.1.4	Element <mdui:Keywords>.....
2.1.5	Element <mdui:Logo>.....
2.1.6	Element <mdui:InformationURL>.....
2.1.7	Element <mdui:PrivacyStatementURL>.....
2.2	Discovery Hinting Information.....
2.2.1	Element <mdui:DiscoHints>.....
2.2.2	Element <mdui:IPHint>.....
2.2.3	Element <mdui:DomainHint>.....
2.2.4	Element <mdui:GeolocationHint>.....
2.3	Relationship with Existing Metadata Elements.....
2.3.1	<md:Organization> Elements.....
2.3.2	Service Name and Description.....
2.3.3	Suggested Precedence.....
2.4	Example.....
3	Conformance.....
3.1	SAML V2.0 Metadata Extensions for Login and Discovery User Interface Version 1.0.....

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



- ▶ 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

mdui対応: UIInfoの使用例

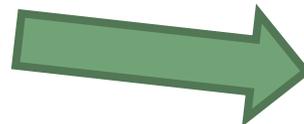
IdPの地理的分類



データ情報: 以下の内容でエンティティメタデータを

地域	*	北海道
スコープ	*	東北

北海道
東北
関東
中部
近畿
中国
四国
九州
その他



```
<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>
...
```

①学認申請システムにて地域を入力



所属機関の学内認証システムでログイン GakuNin

所属機関:

北海道
北海道大学
旭川医科大学
釧路工業高等専門学校
北見工業大学
東北
山形大学
関東

↑ 選択
リセット

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

mdui対応: Discovery Hinting Information

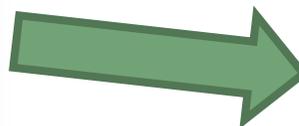
- ▶ Discovery Hinting Information (DiscoHints)
 - ▶ <mdui:IPHint>
 - ▶ 登録されたIPアドレス範囲内からのアクセスならばDSで優先表示
 - ▶ <mdui:DomainHint>
 - ▶ 登録されたドメインからのアクセスならばDSで優先表示
 - ▶ <mdui:GeolocationHint>
 - ▶ 登録された緯度経度情報の近くからのアクセスならばDSで優先表示 (今年度中に実装予定)



GakuNin

メタデータ mdui対応: DiscoHintsの例

検索情報URL	http://www.nii.ac.jp
IPアドレス情報	157.1.120.0/24 157.1.130.0/24 157.1.140.0/24
ドメイン情報	nii.ac.jp
緯度経度情報	35.692559,139.758022
種別	※ 技術的問い合わせ先 (technical)



```

<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>
...

```

①学認申請システムにて条件入力

②生成されるIdPのメタデータ



(テストフェデレーション) 所属機関:

↑ 選択
リセット

ヒント! (テストフェデレーション) 所属機関

NII認証Gテスト

関東

⊗ GakuNin テスト IdP

山梨大学

東京大学 情報システム

の情報が渡り

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

リファラチェックを試す場合は、Firefoxにてabout:configを

mdui対応: UIInfoの使用例

ログイン画面でのSP視覚化

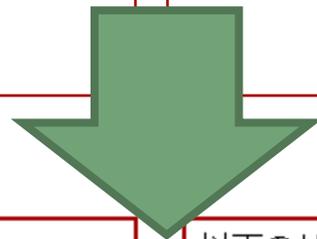
GakuNin-Test-Fed Test IdP 1 Login

Username:

Password:

以下のサービスに接続しようとしています:
test-sp2.gakunin.nii.ac.jp

学認テストフェデレーション テストSP2



GakuNin-Test-Fed Test IdP 1 Login

Username:

Password:

以下のサービスに接続しようとしています:

学認テストフェデレーション テストSP1

 **GakuNin**

SAML2で利用できる属性表示サービスその1

[このサービスのプライバシーステートメント](#)
[このサービスについて詳しくはこちら](#)

サービス名

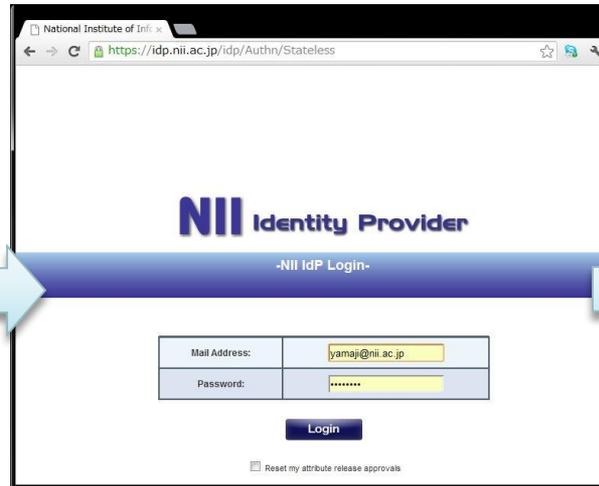
ロゴ

サービス内容

詳細URL

メタデータの活用： 利用可能SP/IdPの取捨選択

利用可能SP/IdPの取捨選択



使えないのならIdPをリストに出さないでよ！



利用可能SP/IdPの取捨選択

IdP管理者が、フィルタ設定を行ったSPを選択

利用可能SP設定

こちらで設定していただくことで、利用可能なSPを制限することができます。

全てのSPを許可する。

接続許可	entityID	機関名称	SP名称	運用開始日
<input checked="" type="checkbox"/>	https://example.com/sp	example日本語	org name	2011-12-08
<input checked="" type="checkbox"/>	https://sp.example.ac.jp/shibboleth-sp	example日本語	SP名称日	2012-06-11
<input type="checkbox"/>	https://sp.example.com	テスト	日本語名称	2011-12-07

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

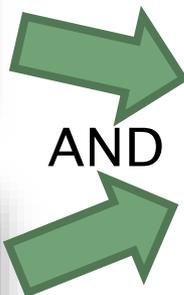
SP管理者が、利用可能IdPを選択

利用可能IdP設定

こちらで設定していただくことで、利用可能なIdPを制限することができます。

全てのIdPを許可する。

接続許可	entityID	機関名称	IdP名称	運用開始日
<input type="checkbox"/>	http://mcus.nii.ac.jp/idp/shibboleth	イグザンプル大学	イグザンプル大学	2012-05-21
<input checked="" type="checkbox"/>	https://acm.ixsq.nii.ac.jp/shibboleth	山地	やまじ	2012-05-24
<input type="checkbox"/>	https://example.com/shibboleth/idp	example日本語	example 日本語	2011-12-07



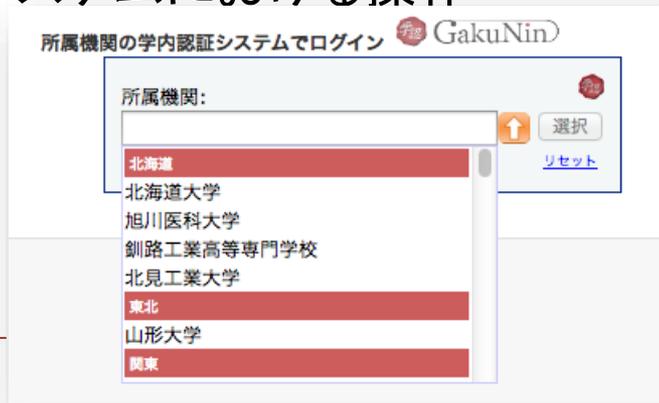
```

[
  {
    "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



GakuNin

利用可能SP/IdPの取捨選択

- ▶ 現在、下記SPで利用可能です
 - ▶ ReaD & Researchmap



GakuNin

他にも： WebサイトのIdP/SP一覧に表示

- ▶ 学認WebサイトのIdP/SP一覧に、自分が管理するIdP/SPを掲載するか否かを選択できる

その他の他:	
<input type="checkbox"/> 一覧に表示する	<input checked="" type="checkbox"/> フェデレーションの参加機関一覧への掲載を許可する
<input type="checkbox"/> eduGAIN	<input type="checkbox"/> eduGAINへ参加する



他にも： SPではさらに・・・

- ▶ 学認WebサイトのSP一覧に、自分が管理するSPでのIdP管理者向け/図書館向け/利用者向けマニュアルを掲載、あるいはリンクでき、自由に更新可能

その他:

フェデレーションの参加機関一覧への掲載を許可する

一覧に表示する

テキストを登録して表示する 外部URLにリンクする

テキスト:

URL:

IdP管理者向けマニュアル



まとめ

▶ 学認の今

- ▶ IdP/SPとも増加中
- ▶ 相互の信頼を維持できるよう、チェックとフィードバックも実施中（学認アンケート）
- ▶ 大学や機関単位でIdPを構築して参加してください

▶ 学認申請システム

- ▶ 参加申請時に利用します
- ▶ 申請システムに入力してもらった情報に基づいて、メタデータを自動生成します

- ▶ ログ画像URL

- ▶ IPアドレス情報

- ▶ ドメイン情報

- ▶ 地域情報

- ▶ 緯度経度情報

- ▶ IdP/SP取捨選択

- ▶ IdPカテゴリ

- ▶ 大学

- ▶ 短期大学

- ▶ 高等専門学校

- ▶ 研究所

- ▶ その他

おわりに：
学認から大切なお知らせ



学認 事業化のお知らせ

- ▶ 2013年10月、学認の事業化が内定しました
 - ▶ NIIのプロジェクト（有期）から事業へ
- ▶ NIIに学術認証運営委員会が設置されました
 - ▶ 認証作業部会から学認の運営を引き継ぎます
- ▶ 新体制移行のスケジュール
 - ▶ 現在の参加機関は、原則引き継ぎます
 - ▶ 学認参加機関の皆様への告知・確認
 - ▶ とくにお申し出がなければ、そのまま新体制へ
 - ▶ 2014年1月より新体制スタート予定

今後とも「学認」をよろしくお願い申し上げます！