山形大学のLoA1の申請と認定まで

山形大学 大学院　理工学研究科
伊藤　智博

tomohiro_ito@ieee.org, https://upki.yamagata-u.ac.jp/

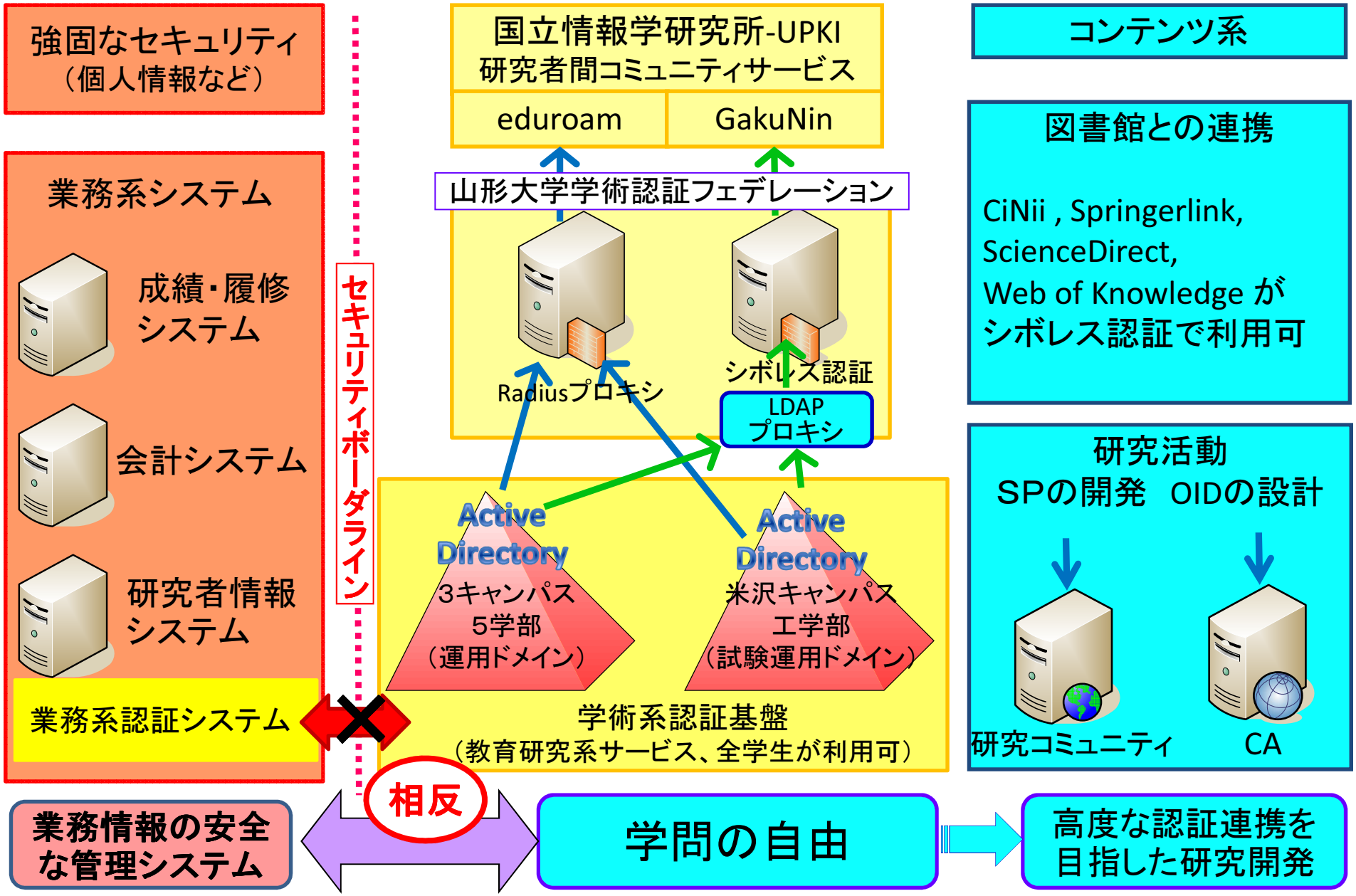
山形大学の紹介

山形県を北から南まで縦断する
分散キャンパス
（米沢-鶴岡間は，3時間ぐらい ）

結果的にどうなのLoA1

- LoA1の認定は簡単です.
- 手間もかかりません. 詳しくは後程
- とにかく楽です. JABEEと比べたら…

山形大学の認証基盤とGakuNinとの関係



本題のLoA1の話です

E1482 - 山形大学の事例からはじまる学認の次世代認証基盤構想

カレントアウェアネス-E
No.245 2013.09.26

E1482

山形大学の事例からはじまる学認の次世代認証基盤構想

現在、大学ではユーザのIDを集中管理することで、一つのIDとパスワードで全ての学内サービスにログインでき、さらに

学認では，それらの情報を正確にSPに伝えることができる。学認の信頼性を最大限活用した学割サービスなどの検討も進められており，こうしたサービス革新により多くの参加校がメリットを受けられる時代は，もうそこまできている。

（国立情報学研究所・山地一禎）
（国立情報学研究所・中村素典）

標準化について考えよう。

- なぜ、標準化？　ISO ？HACCP？

　ISOがなかったら、企業間で「規格の標準化」争いが起き、企業が本来力を入れるべき課題である品質向上やコスト削減が遅れる？

非常口を表すマークは、
ISO(国際標準化機構）で
定められた世界共通のもの

ISOは世界共通のルール、松林光男、渡辺弘, *イラスト図解　工場のしくみ*, 日本実業出版社, 150, (2004).

認証連携の標準化？

- プライベートな外部サービスと認証連携するなら、認証情報は各機関のポリシーによる運用でよい。
- パブリックなサービスで使うときはどうしよう。
- お互いの認証情報の運用レベルが同じでないと，SPの認可が難しくなる

学内の申請手順を思いついたのは‥

- 2012年9月，学認CAMPのあと，
  香川のうどんをすすりながら.
  東大の佐藤先生と‥‥

- ISOやJABEEの認定と同じ考え方でやることに.
  → 認定のために何かするのは？
  → 現状のありのままで，審査をしてもらおう
  → スパイラルアップの一環

学内での承認を得るために

- IdPや認証基盤の客観的な評価を得るため
  → IdP管理者の身を守るため

- 審査は上手に使おう.
  LoA1を審査を通して，情報系センターの認証基盤を第3者に確認してもろう.
  → スパイラルアップの一環，
  → 教育環境の改善の一環

- PubMedなどのサービスのためではありません.

実際の審査の手順

- 2012年10月頃，LoA1の申請窓口にメールを書いた.

→　正式な審査申請を行う前に，プレ審査を依頼

- 2012年11月頃，学内文書を審査員に開示
- 2012年12月頃，　ヒアリングを実施
- 2013年1月頃，　ヒアリングでわかった不足文書を新規文書として作成，会議で承認
- 2013年1月末，事務的に正式な審査申請書を提出

NDA相当の管理レベルで進められます

審査のポイント

- アカウントのライフサイクル（発行-更新-削除）
  → IdP運用マニュアルに記述
  → LoA1なので，発行がポイント

- IdPの運用基準について
  → IdP運用マニュアルと
  IdPの運用ポリシーに記述

工数　30時間人の内訳

- 申請窓口との対応：15時間人（一人で対応）
- 担当者間での不足規則の文書化の打合せ
  2時間人（二人で対応）
- 学内会議による文書の承認
  5時間人（15人程度の会議）
- 事務・センター長の署名や郵送手続き
  2時間人（数人で対応）

申請の事務的な扱いのために

- 申請書は，英語です．
  契約書なので，ハードルが高い
  → プロに依頼するしかない

- 東京大学の佐藤先生にご協力いただき，申請書の書き方の手引きを作成
  → 事務的に流せるようにすることが大切

申請書の手引きの補足例

The following sections of this form must be completed before this Application and Agreement can be accepted by OIX. If you do not yet have this information, you may still submit this Application and Agreement to OIX, but it will remain pending until this information is received.

4. Trust Framework Role Identity Service Providerにチェック

Select the checkboxes below to indicate which roles you are applying to be listed for as trust framework (you must choose at least one and may check more than one):

- ☐ Identity Service Provider
- ☐ Relying Party
- ☐ Academic Federation Assessor
- ☐ Assessor
- ☐ Auditor
- ☐ Dispute Resolution Service Provider

5. Technical Profiles SAML 2.0と書く

Indicate the Technical Profile(s) that you are applying to be listed for (you must check a may check more than one):

- ☐ OpenID 2.0
- ☐ IMI 1.0

6. Assessor 「GakuNin」と書く

Indicate the OIX Listed Assessor that will verify your certification*

---

* The name entered MUST match a Listed Assessor for this trust framework, EXCEPT if a Role

Technical Profiles SAML 2.0と書く

ate the Technical Profile(s) that you are applyir
check more than one):

☐ OpenID 2.0

☐ IMI 1.0

本学の規則などのサマリーの英文作成は？

- LoA1の審査側で作成してもらいました.

  → 契約に関わるので，プロの訳が望ましい.

  → 本学で作成する必要があった場合，プロに依頼するつもりでした.

- 海外の認定機関なのに，日本語で十分なのは，うれしいです.

LoA1の技術的な問題点

- LoA1の設定を行うと，SpringerのSSOが正常に動作しない．→ 解決済
- 原因は，LoA1のAuthn Context Classの値である

”http://idmanagement.gov/icam/2009/12/saml_2.0_profile/assurancelevel1” をエラーとして表示する．

技術や仕組的に解決すべき課題は多い． → 研究段階
→ 商用ベースなった後で参加したほうが，お得です．
⇔ あれでも大学だよね．商用ベースになったら大学は…
→ 公的機関としての研究なら… ← 70機関以上参加

山形大学

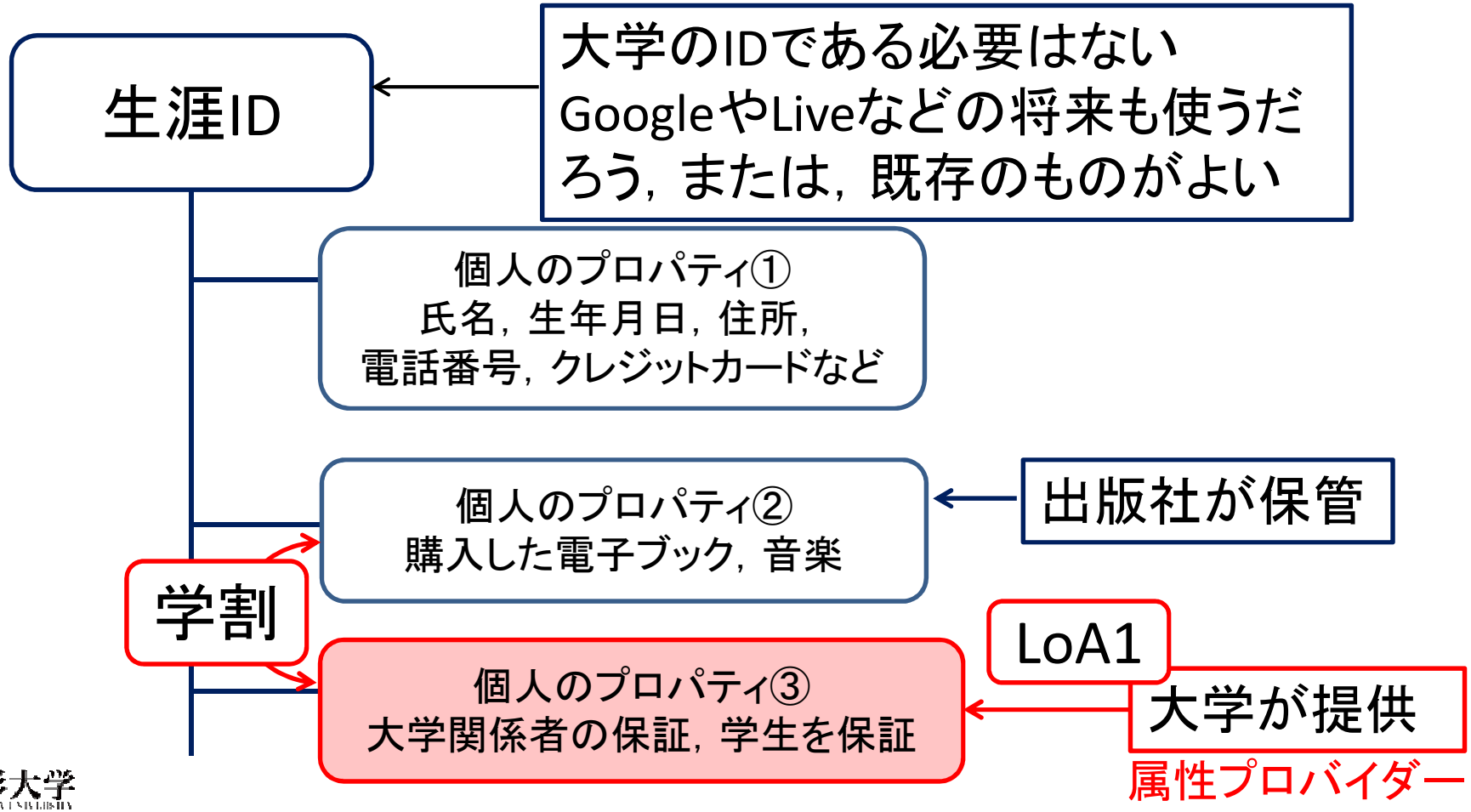
・LoA1に対応したIdPの設定, https://a.yamagata-u.ac.jp/amenity/Laboratory/LaboNoteWeb.aspx?nLaboNoteID=1998
・GakuNinShibInstall / Home/ SP接続情報 SpringerLinkに関する情報,
https://meatwiki.nii.ac.jp/confluence/pages/viewpage.action?pageId=14647303 (2013年9月)

LoA1と学割

- 標準化された第１保証水準
  → Googleなど同じ商用レベルのアカウント
- 金の絡む話もできるよね
  → 教育目的であることを保証できる
  → 学割 → 学生サービスの向上
- 商用サービスとコラボして賢い学生を育成できたら…

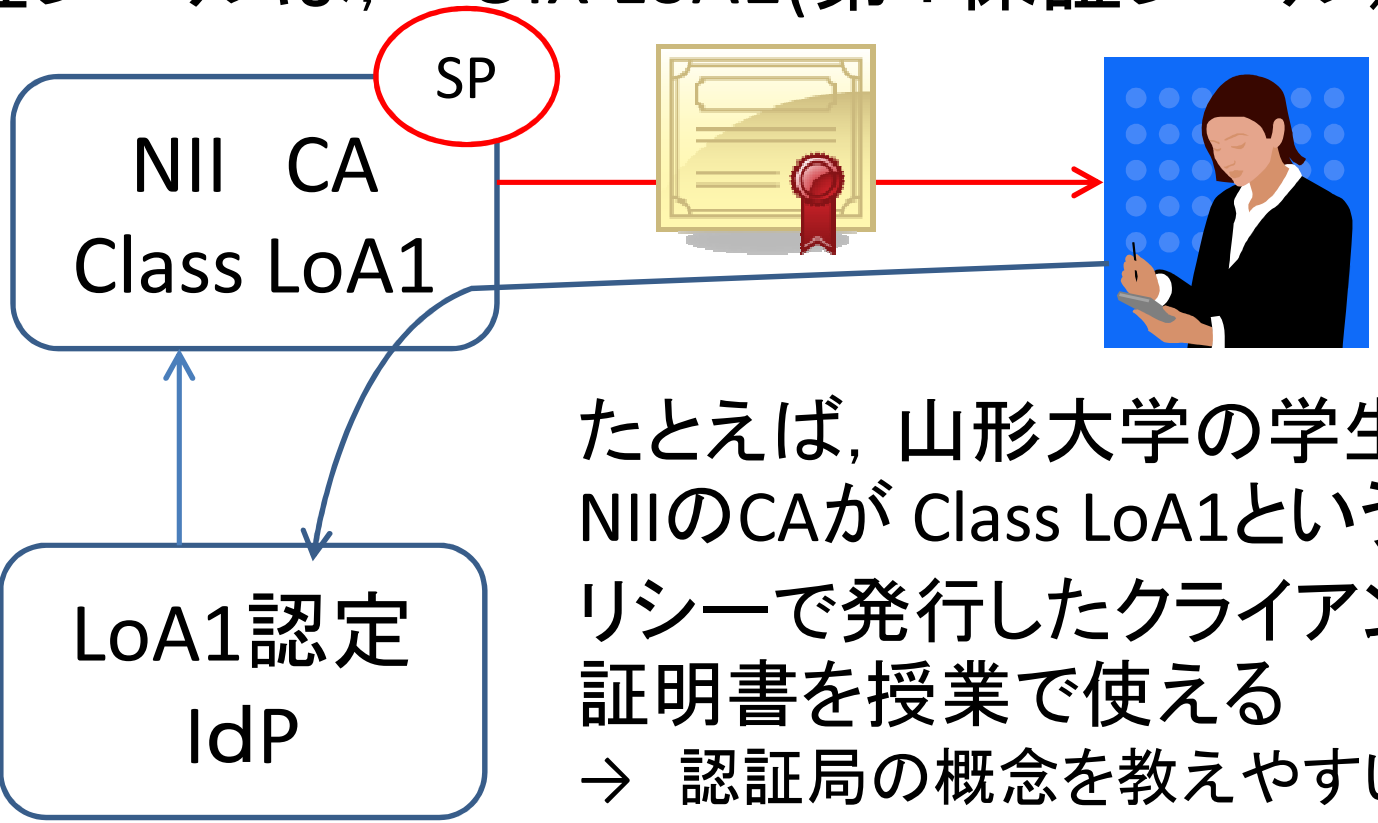
どんな使い方ができるの

- 学認を使って教育関連の人であること保証



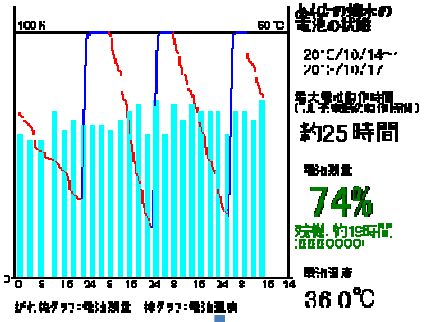
クライアント証明書を発行したら

- 学認を使って教育関連の人であること保証
- 保証レベルは，　OIX LoA1(第１保証レベル）



たとえば，山形大学の学生にNIIのCAが Class LoA1というポリシーで発行したクライアント証明書を授業で使える
→　認証局の概念を教えやすい

タブレット端末と学認



充放電の線と何時間使えるかを生成してスマートフォンで表示

劣化チェッカー

スマートフォン

UUID

学認ID

フル充電時に何時間使えるか計算する

充電記録

鷹山

データベースサーバー

VB.NET
SQL Server

Web

記録の閲覧

充電レベル53
5/27 22:00
放電中s

充電レベル80
5/27 22:00
充電中

XMLファイルでHTTPSで送信

学認は研究段階

山形大学

開発チーム： 山形大学　お鷹ぽっぽ

http://mri.yz.yamagata-u.ac.jp/rekkachecker.htm

まとめ

- 学認は，研究段階
  → LoA1もフェデレーション研究の1つ

- LoA1の認定は簡単

謝辞

- 日頃から、様々な質問にお答えいただきました国立情報学研究所の皆様に深く感謝申し上げます。
- 本学のクラウド認証連携システムの構築は，平成22年度国立大学法人設備整備費補助金事業の補助によって実施されました.