山形大学における『学認』対応認証基盤整備と e-サイエンスへの取り組み

山形大学大学院　理工学研究科
山形大学　情報ネットワークセンター
伊藤　智博
TEL 0238-26-3021, e-mail tomohiro_ito@ieee.org
https://upki.yamagata-u.ac.jp/

学内統合認証基盤の経緯

工学部学術情報基盤センター

- 2004年　AD認証によるリモート接続サービス開始
- 2004年　学内ネームスペースの調整開始（DNSの調整）
- 2004年　UNIX系の統合開始（SFUの導入）
- 2004年末　ネットワーク利用者認証開始（ウィルス対策）
- 2005年夏　SFUスキーマによるUNIX系のLDAP認証統合システムの試験開始

2007年　教育用実習システムの更新、教育系は統合認証に移行

（学内は認証ベースに移行）

データベースアメニティ研究所

- 2004年　Verisign サーバ証明書導入
- 2004年夏　S/MIME証明書の試験
- 2005年　ASP .NETに90%以上移行完了 → オブジェクト化
- 2005年 CAのテスト開始、OID取得、PKIの勉強を開始
- 2006年Comodoに証明書に変更
- 2008年UPKIサーバ証明書に変更

2008年　UPKIサーバ証明書、UPKI-シングルサイオン、eduroamへの参加

2009年9月 UPKI-学術認証フェデレーション（運用）に参加

UPKI-SSO参加のための学内調整

- ポリシー：　学術情報基盤センター（現　情報ネットワークセンター）の認証統合実証試験プロジェクトとしてスタート

- 体制

  機関責任者：　学術情報基盤センター　センター長

  学内担当者：　吉田浩司(3キャンパス計5学部)、
  田島靖久(図書館との調整;2009年～）、
  伊藤智博(工学部)

  実証試験担当者：　伊藤智博

- 予算：　特になし（使用済みの旧サーバを再活用）
- 業務のバランス（人手不足など）から、伊藤の実験・研究としてUPKI-SSOに参加することで、学内決済を得た。

認証フェデレーションの運用ポリシー

- アカウント管理業務コストを最少にすること。

  → 将来的な運用コストを最少にする。

- 楽になる技術を開発

  → LDAP Proxyによるスキーマの異なる複数認証基盤の統合化

  → 無線LANのセキュリティ向上 → eduroam

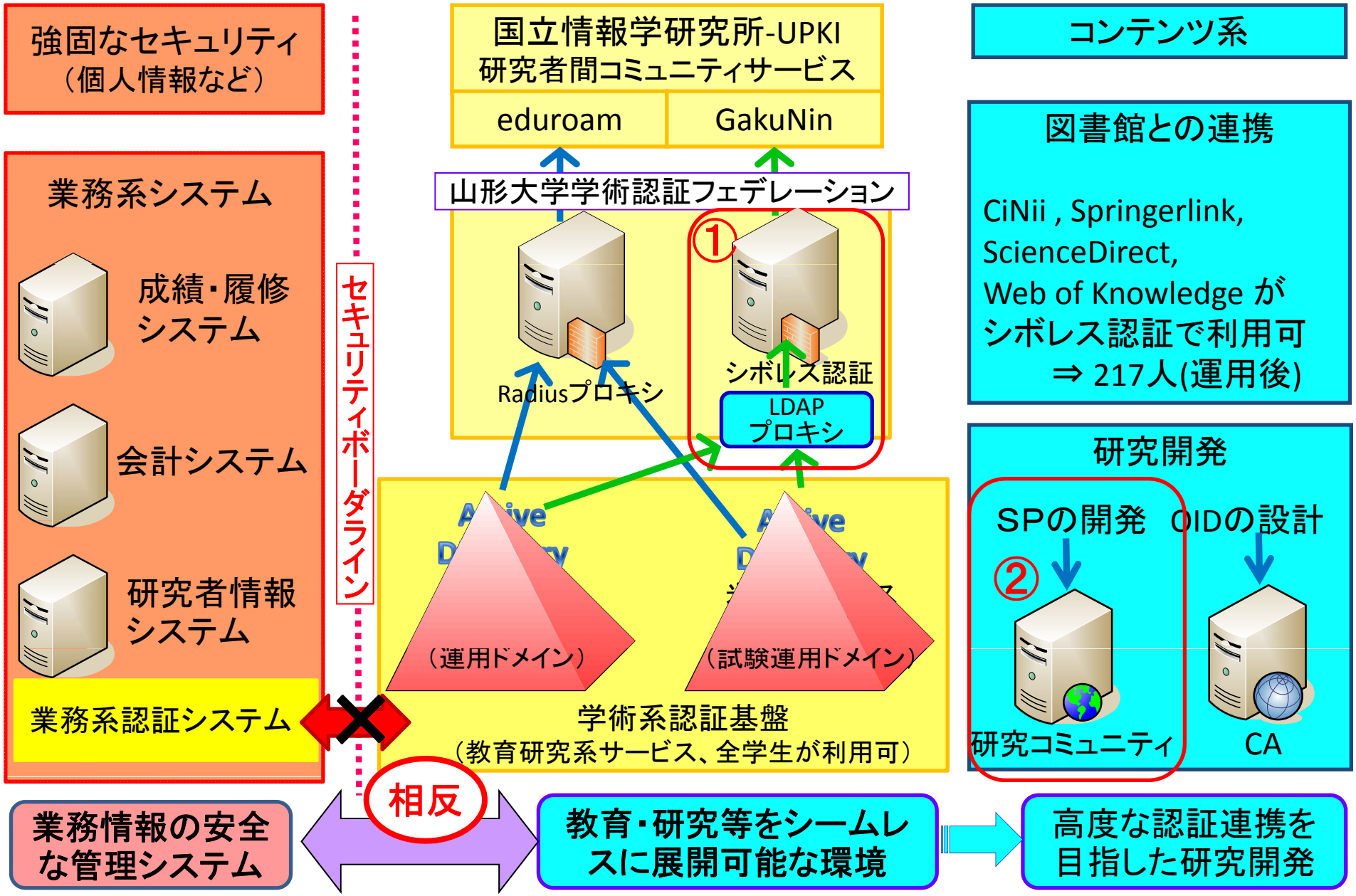
  → シームレスな通信を目指して、IPv6の実証実験

- システム構築コストが高くても、運用コストを最小にすることが継続性への鍵。

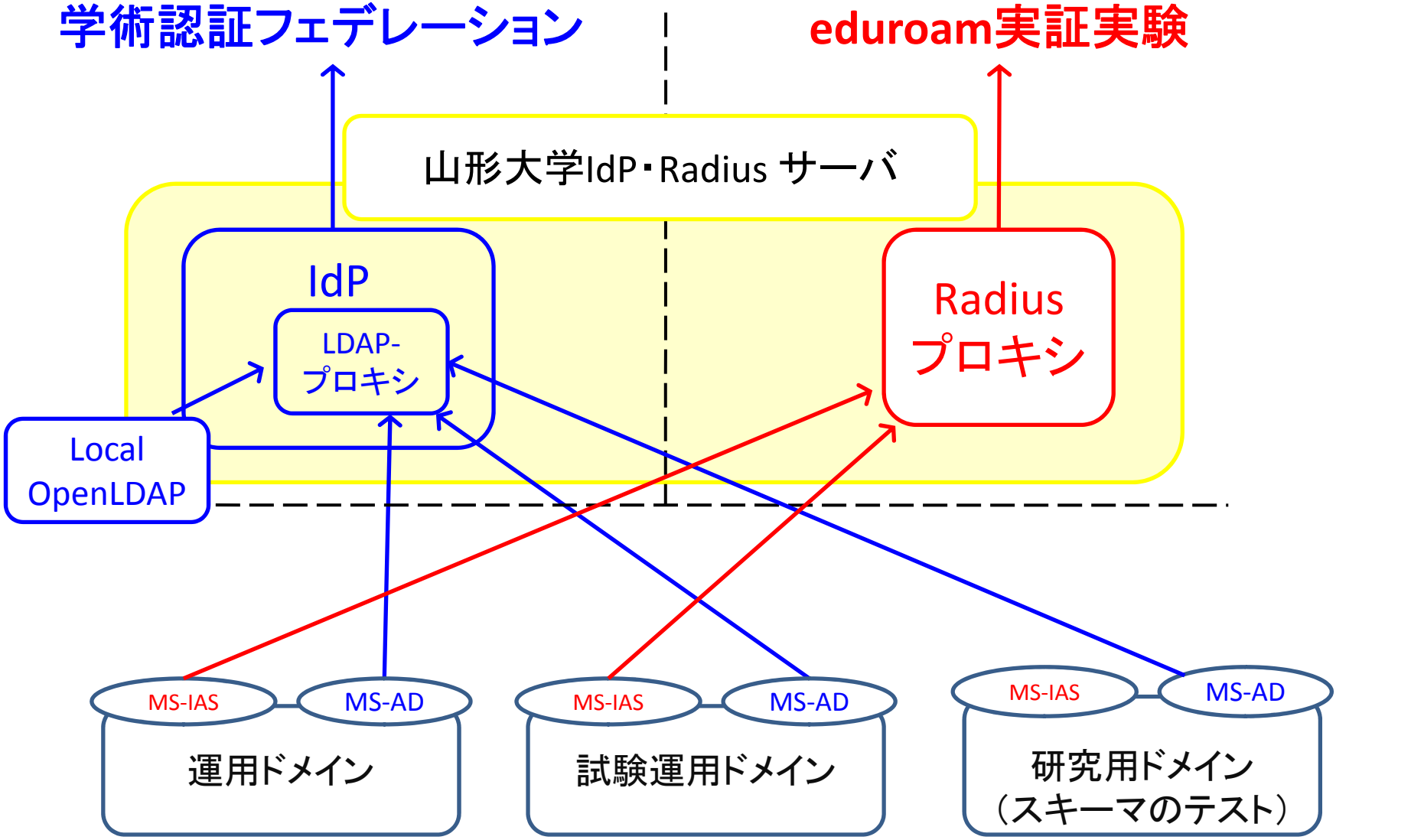
- 目的：外部機関のサービスとの認証連携技術の確立

  → 教育への活用（人材育成）

山形大学の認証基盤とGakuNinとの関係



統合認証基盤のIdP・Radiusサーバの構築



異なる認証システムでも、接続が可能（スキーマの変換が可能）
学内で認証基盤の追加および削除が自由自在
フィルタ機能も動作する（rwm-map)。

認証情報の取り扱いで決めたこと

•プライマリーキー（主キー）の取り扱い

主キーとは、個人ごとに一意性を保った属性

⇒　受益者がサービスを受けるために最低限必要な情報

→　ePPN(eduPersonPrincipalName；アカウント毎に一意）

→　ePTID(eduPersonTargetedID;リンク毎に一意）

【OASISのドキュメントより】

•EPPN

→　ADのuserprincipalnameを使い、自動生成。

例：dG9tb2hpcm9AYW0ueXoueWFtYWd・・・・・@yamagata-u.ac.jp

•eduPersonTargetedIDの生成方法の決定

→ StoredIDを利用（京都産業大学提供）。

→ DBには、mySQLを利用。

→ DBの情報のデータハウスに集約 (MS-SQL, SSIS)

研究用フェデレーション

- 学内・学外で、シボレスに関する研究活動をするためのフェデレーションを準備

- 活動内容

  1.メタデータ管理システムの構築

  2.メタデータ作成支援ツールの構築

  3.IPv6への対応状況のテスト

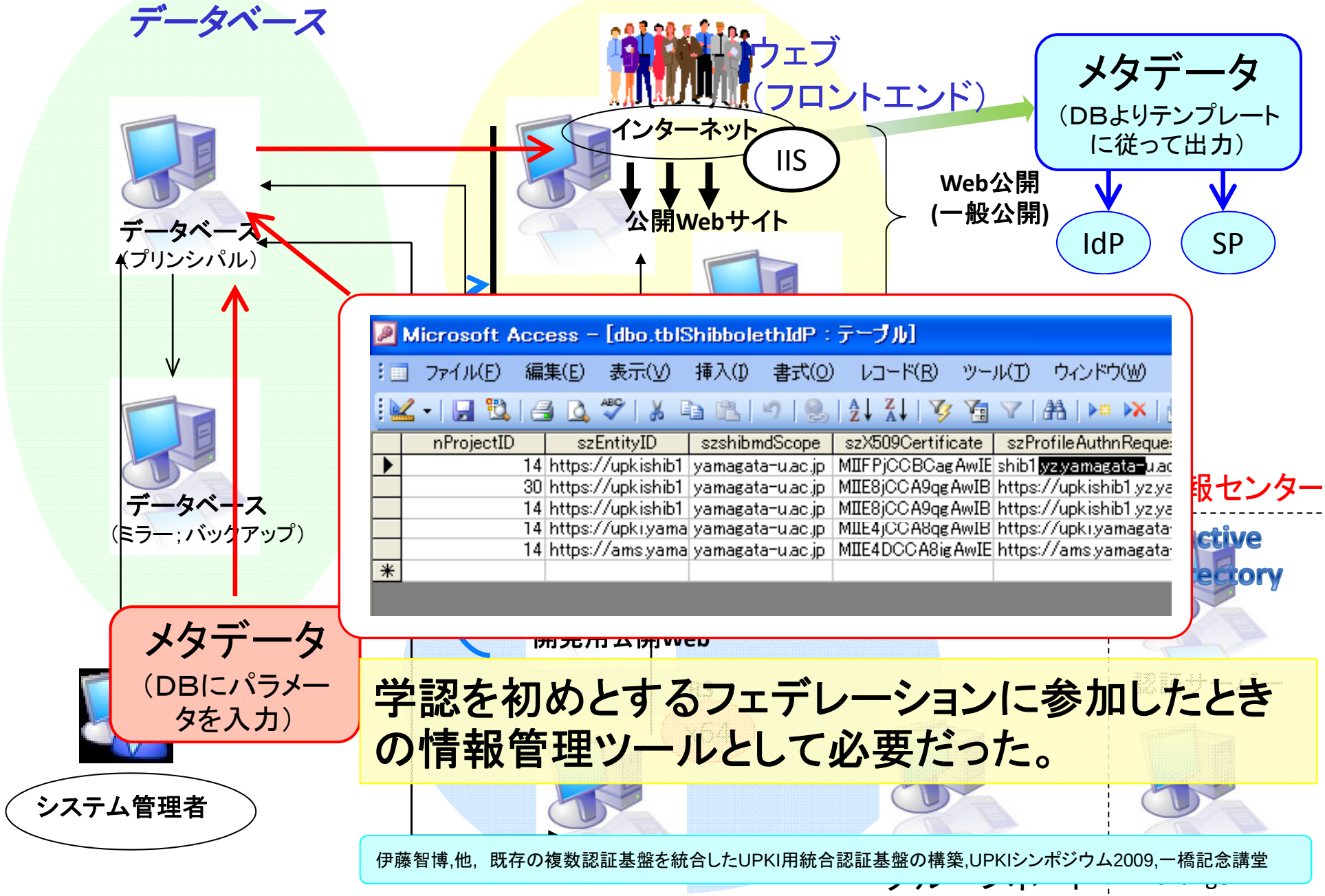
  → IdPは問題なく動作

  → SPは現在検証中

- その他

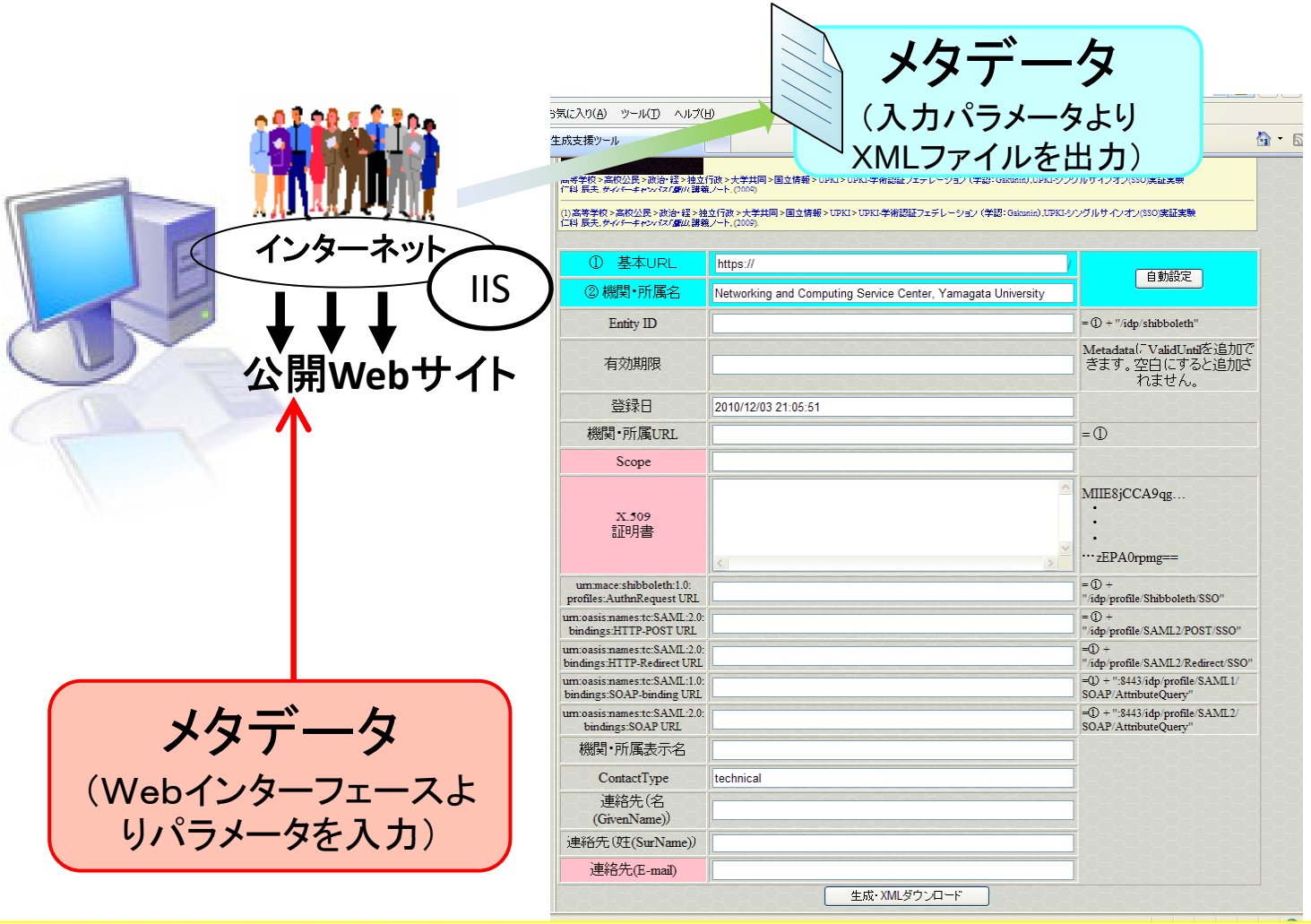
  学認用IdPによるGoogle Appsの動作試験→OK

紹介：メタデータ管理システムの論理構成



伊藤智博,他，既存の複数認証基盤を統合したUPKI用統合認証基盤の構築,UPKIシンポジウム2009,一橋記念講堂

紹介：メタデータ作成支援ツール



メタデータのXMLファイルのNIIに提出するときに、間違えることがあったので、ツールを開発した。

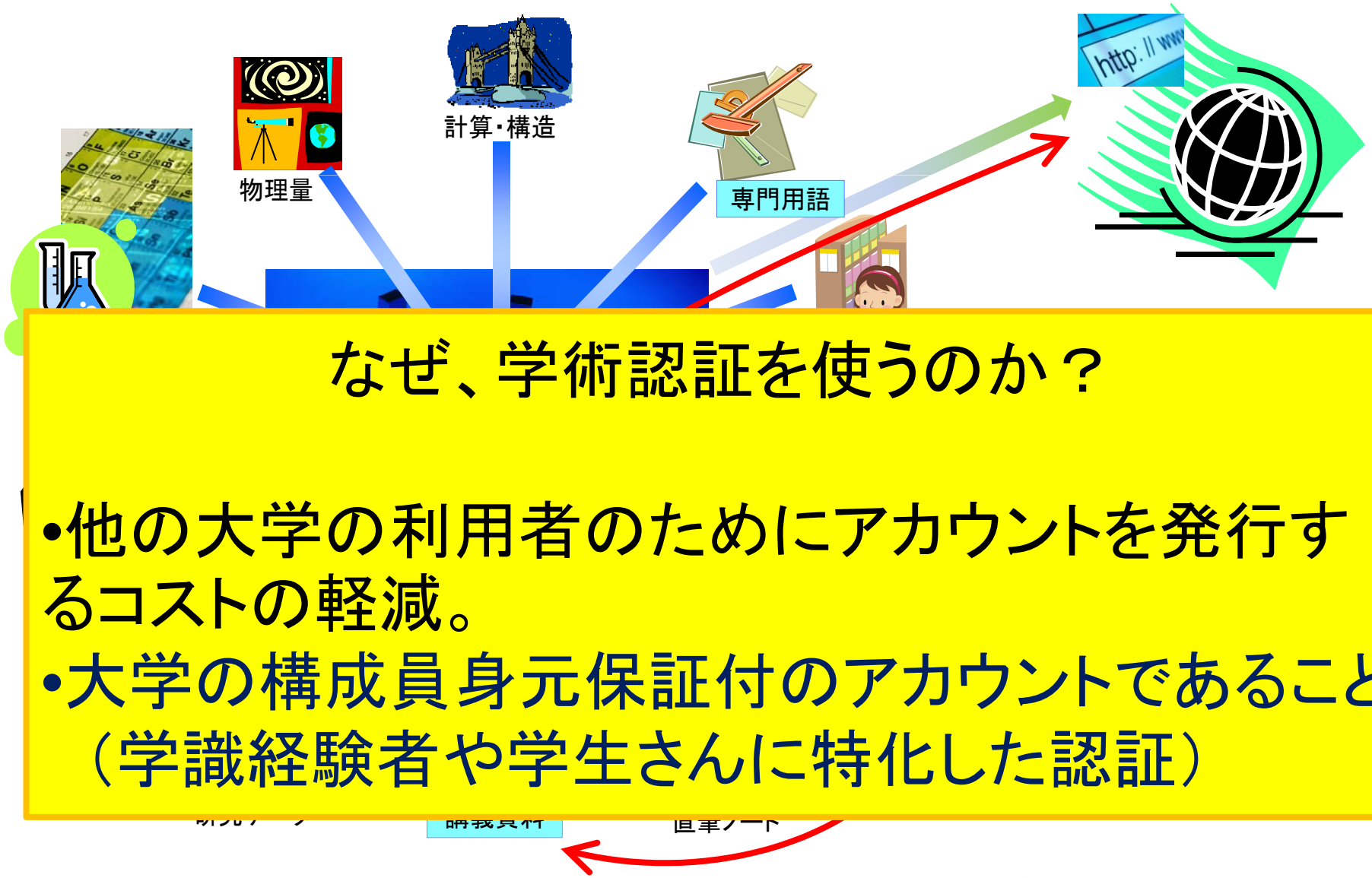
IdP用： https://a.yamagata-u.ac.jp/amenity/network/ShibbolethIdPGenerateXML.aspx

SP用： https://a.yamagata-u.ac.jp/amenity/network/ShibbolethSPGenerateXML.aspx

科学技術の学術情報共有システムの概要

サイバーキャンパス「鷹山」の様々なコンテンツに学認ユーザからご意見・質問・コメントを頂き、公開する。→　社会からのフィードバック機能の追加。

科学技術の学術情報共有システムの概要

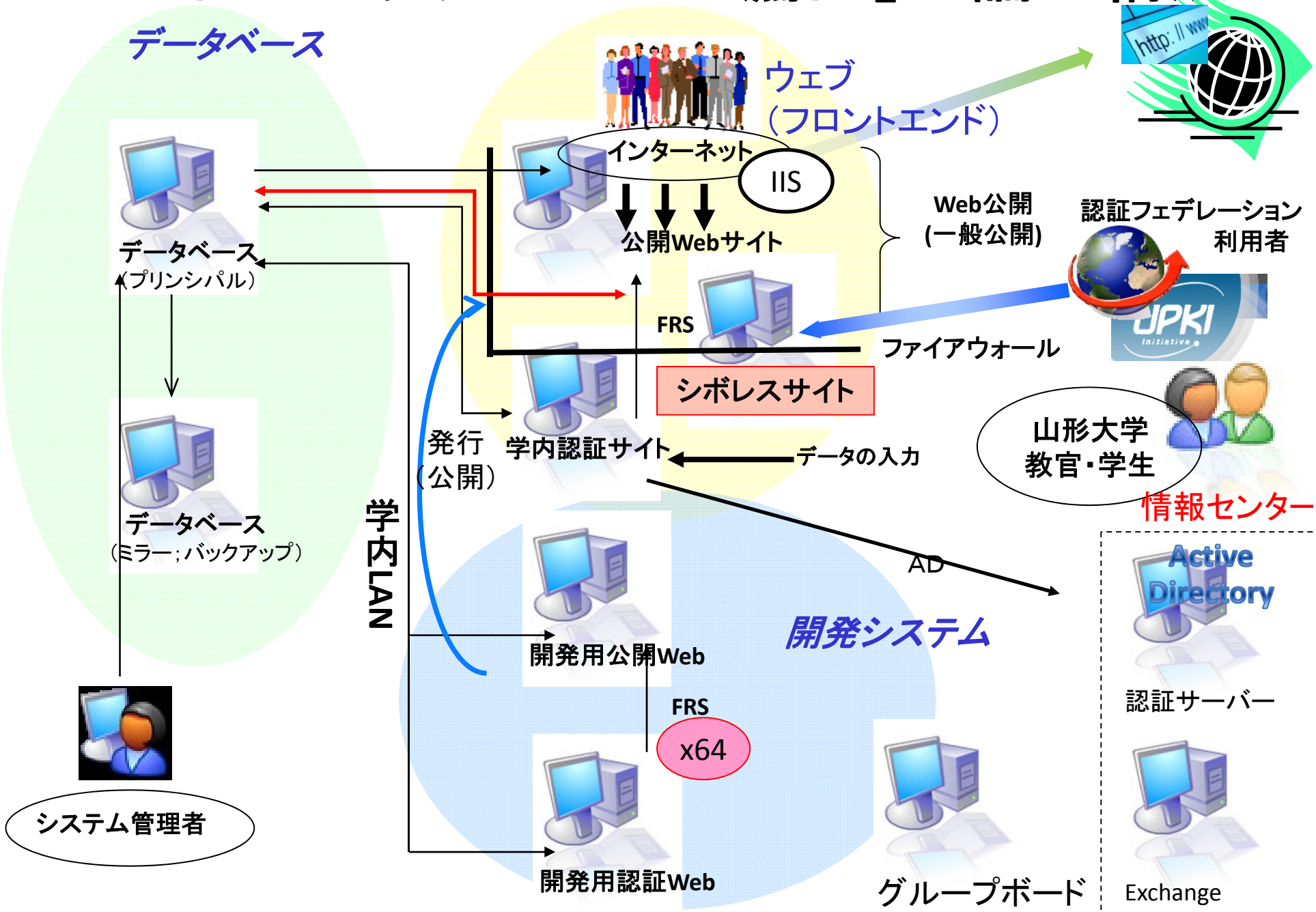


なぜ、学術認証を使うのか？

- 他の大学の利用者のためにアカウントを発行するコストの軽減。
- 大学の構成員身元保証付のアカウントであること。
  （学識経験者や学生さんに特化した認証）

サイバーキャンパス「鷹山」の様々なコンテンツに学認ユーザからご意見・質問・コメントを頂き、公開する。→　社会からのフィードバック機能の追加。

サイバーキャンパス「鷹山」の論理構成



運用ポリシー

- レビューなどを書き込むためには、利用登録が必要。
  →利用登録時に、公開用ニックネームを決めてもらう。
- 個人の識別子には、ePPNを利用。
- 書き込み内容は、原則公開とする。ただし、今後機能を拡張する個人の情報に近い情報は、非公開とする。

できるだけ、自由な使い方。機能追加の要望は大歓迎！

認証フェデレーションのための技術的な検証を進める。

実装課題

- データベースのセキュリティの確保
  → 偽装(Impersonate)や特権ユーザによる保護。

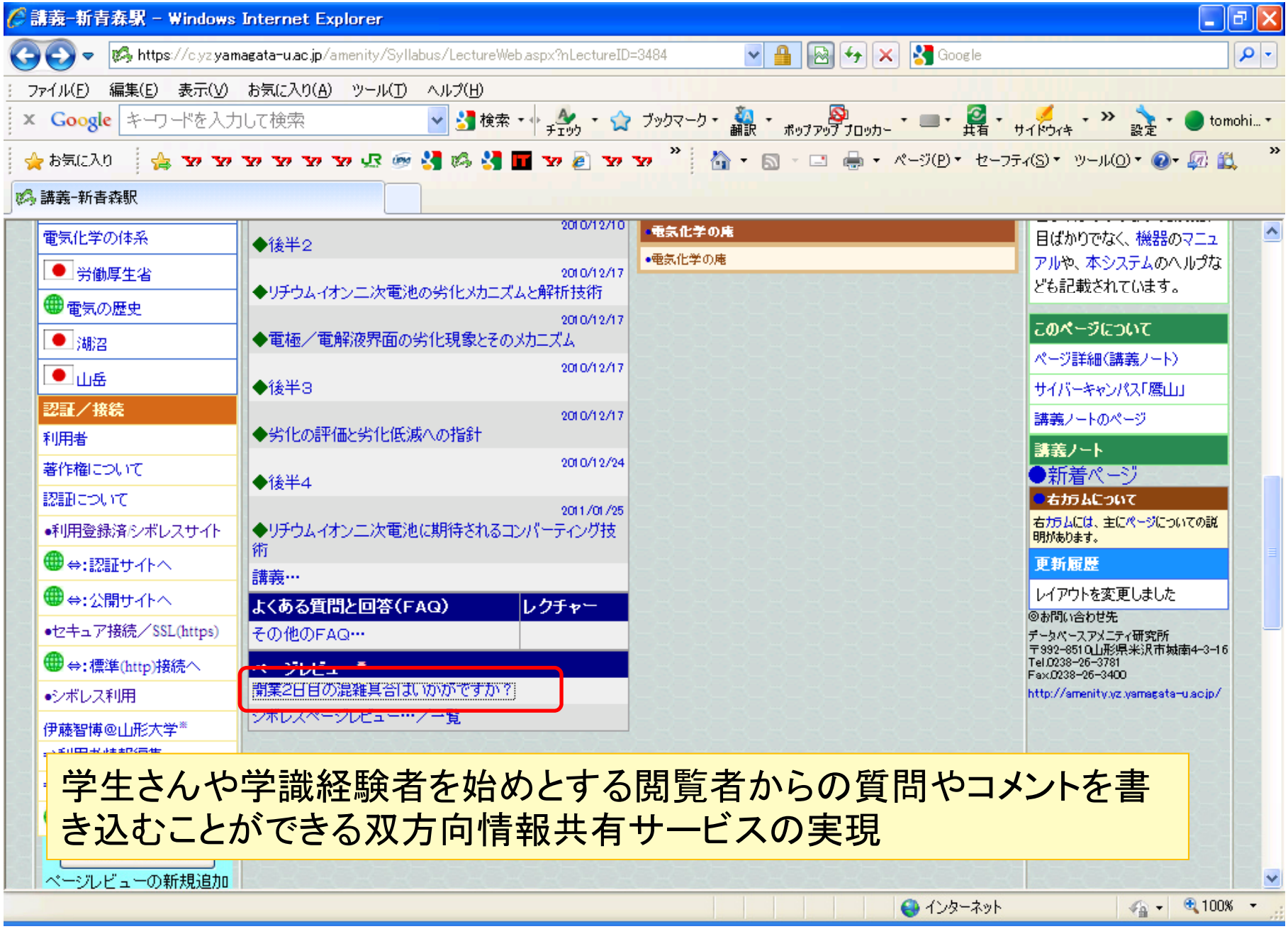
実際の画面①


⇔:標準(http)接続へ
Institutional Login
レビューの追加
シボレス認証によって、このページの感想やコメント、質問などを記入できます。学術認証フェデレーション(学認)参加機関から利用できます。
→ シボレスログイン
RSS FEED
シボレストップメニュー
学認参加機関／一覧
ページレビュー説明書
山形大学 学術認証fed
新青森駅
項目
値
ID
⇒#3484@講義;
要約
新青森駅…は、東北新幹線⇒#1272@講義;の終着駅。2010年12月4日から開業。新青森駅から函館までは、スーパー白鳥で移動できます。2015年には、新函館駅まで、北海道新幹線が開業される…ことが知られている⇒#3484@講義;。
題名
【関連講義】電気化学の庵,新青森駅 ⇒#3484@講義;
リーダー
実施日/時間帯
2010/12/05/
場所／教室・会場
講師
CODE
関連外部URL
http://amenity.y…
関連内部URL
https://gb.yz.ya…
共有フォルダ
¥¥yzdn¥dfs¥share…
科目
学問 > 総記 > 知識・学 > 電気化学の庵
東北新幹線[1]の終着駅。
2010年12月4日から開業。
新青森駅から函館までは、スーパー白鳥で移動できます。
2015年には、新函館駅まで、北海道新幹線が開業されるようです[2]。
高等学校 > 高校地理 > 交通 > 鉄道 > 新幹線 > 東北新幹線,新幹線
仁科 辰夫, 電気化学の庵 講義ノート, (1987).
ページが表示されました
インターネット

実際の画面②

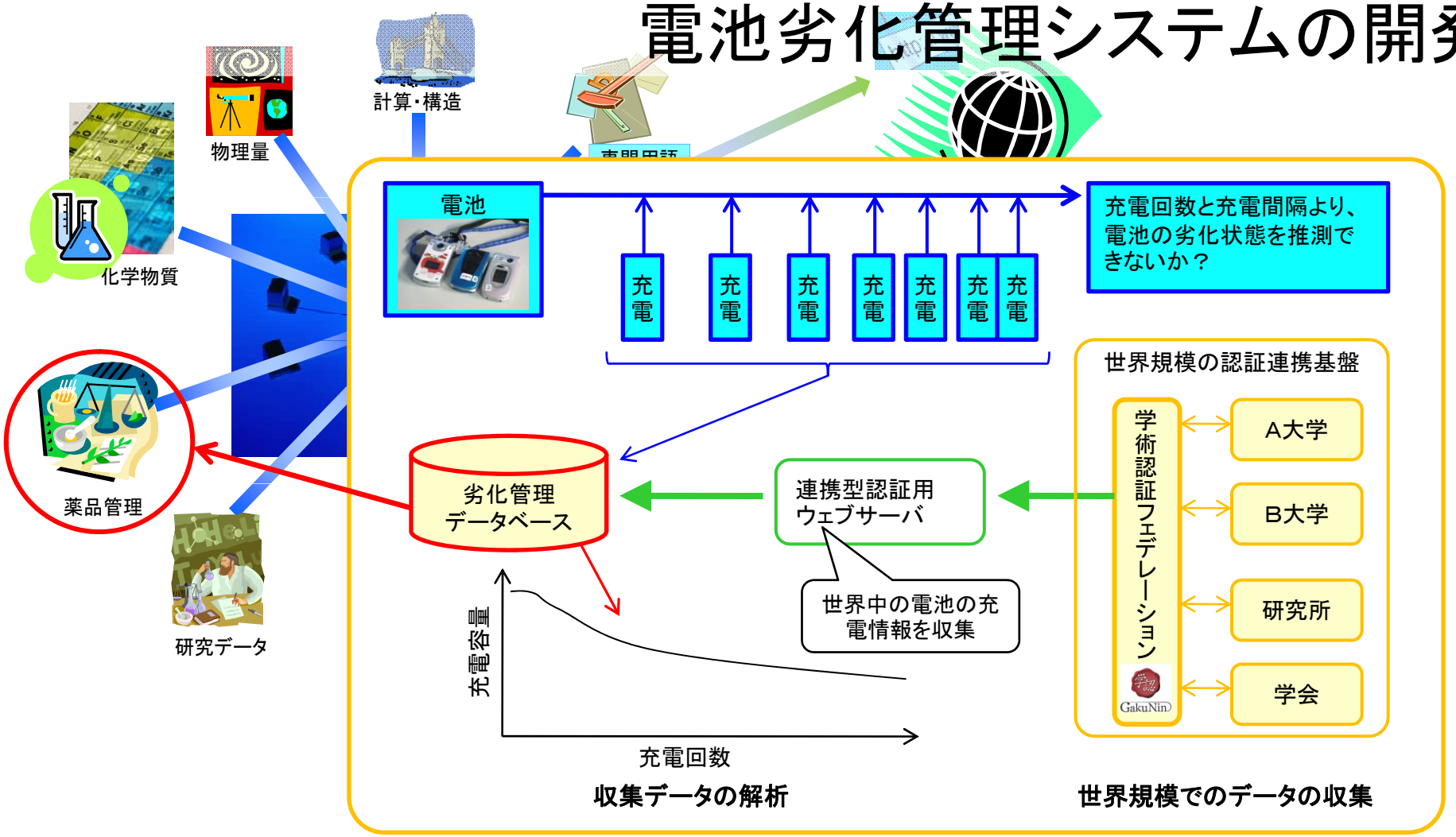
コメントを入力して、「レビューの追加」をクリック

実際の画面③



学生さんや学識経験者を始めとする閲覧者からの質問やコメントを書き込むことができる双方向情報共有サービスの実現

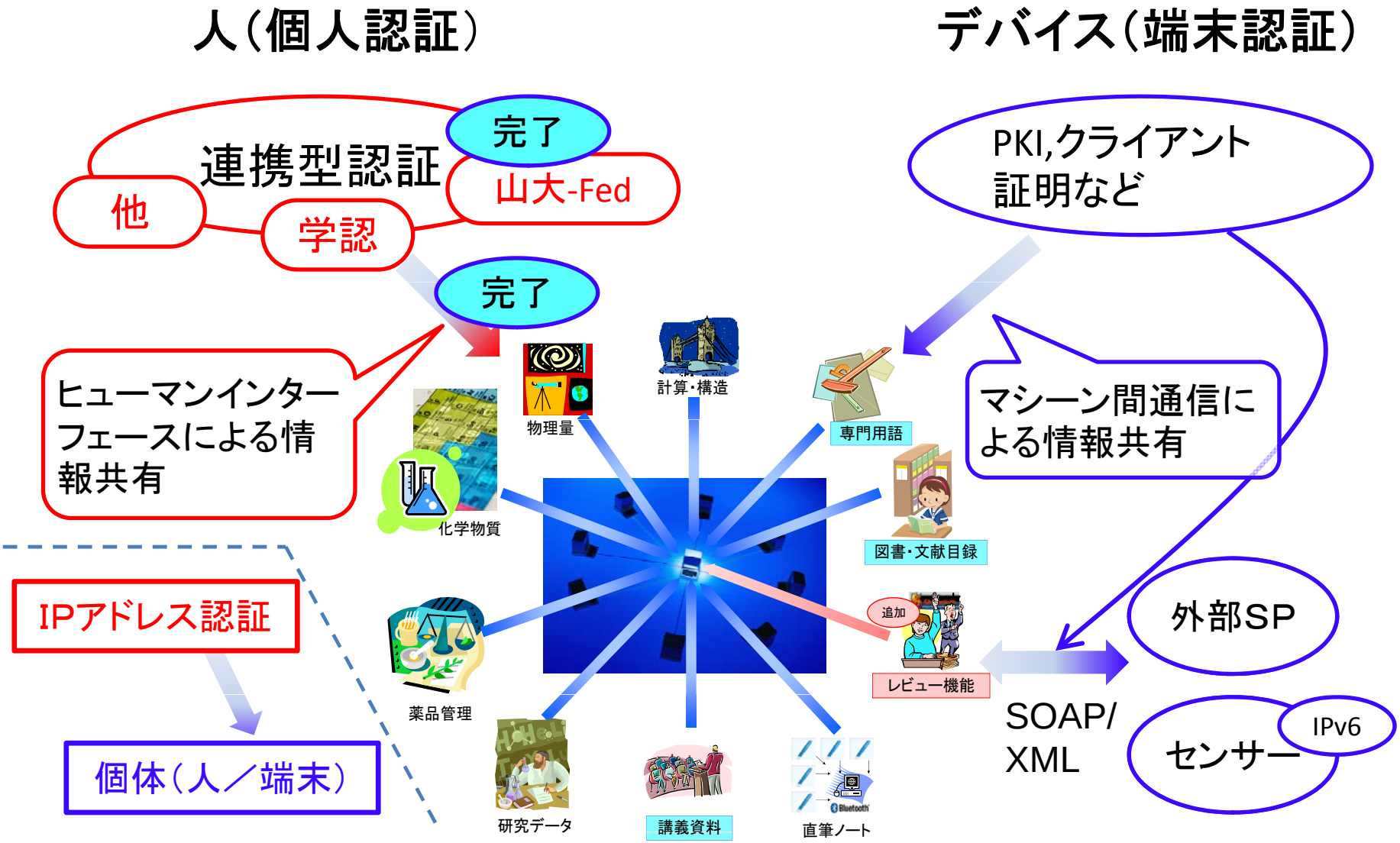
スマートグリッド実現へ向けた連携型認証による電池劣化管理システムの開発



既存の薬品管理システムに、試料名として、「電子」と「不可逆容量」を追加し、単位として、「mol」を取り扱えるようにした。個人識別を利用して、本人が登録した試料のみについて、電池を充電したときなどに電子の使用した履歴を追加することができるようになった。

○伊藤智博, 他,平成22年度化学系学協会東北大会講演要旨集, 230 (2010).

e-サイエンスに向けて（将来構想）



ユビキタスネットワークによる科学技術の学術情報の共有システムの開発
→　次の世代の人材教育と研究

謝辞

本研究を進めるにあたり、ご指導を賜りました情報担当副学長、情報系センター、図書館の皆様に深く感謝申しあげます。

日頃から、様々な情報を収集する機会を与えて頂いた東北学術研究インターネットコミュニティ (TOPIC) の皆様に深く感謝申し上げます。

IPv6ネットワークを提供していただきましたJGN2plusおよびWIDEプロジェクトの皆様に深く感謝申し上げます。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。