Microsoft Active Directoryの活用

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

資料は多めにつくってあります.

アジェンダ

1. なぜ，Active Directory？

2. 学認への参加，シボレスとADFS

山形大学の特徴

山形市： 本部，基盤教育院，理学部，人文学部，
地域教育文化学部，医学部
米沢市： 工学部
鶴岡市： 農学部

分散管理でも十分に対応できる
認証データベースが必要

AD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系をAD認証に統合したシステムの運用試験開始

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

Windows系とUNIX系のパスワードは別々

- 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

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

（学内はユーザ認証ベースに移行）

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

AD統合認証基盤の経緯

工学部学術情報基盤センター　　データベースアメニティ研究所

- 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系をAD認証に統合したシステムの運用試験開始
- 2007年　教育用実習システムの更新、教育系は統合認証移行（学内は認証ページに移行）
- 2008年　UPKIサーバ証明書、eduroamへの参加

- 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、ラオブジェクト化
- 2005年 CAのテスト開始、OID取得、PKIの勉強を開始
- 2006年 Gmailに証明書に変更
- 2008年UPKIサーバ証明書に変更

Windows系とUNIX系のパスワードは別々

なぜ、Active　Directoryなの？

- ほかのディレクトリツールもあるよね？（Sun One Directory，　OpenLDAPなど・・・）

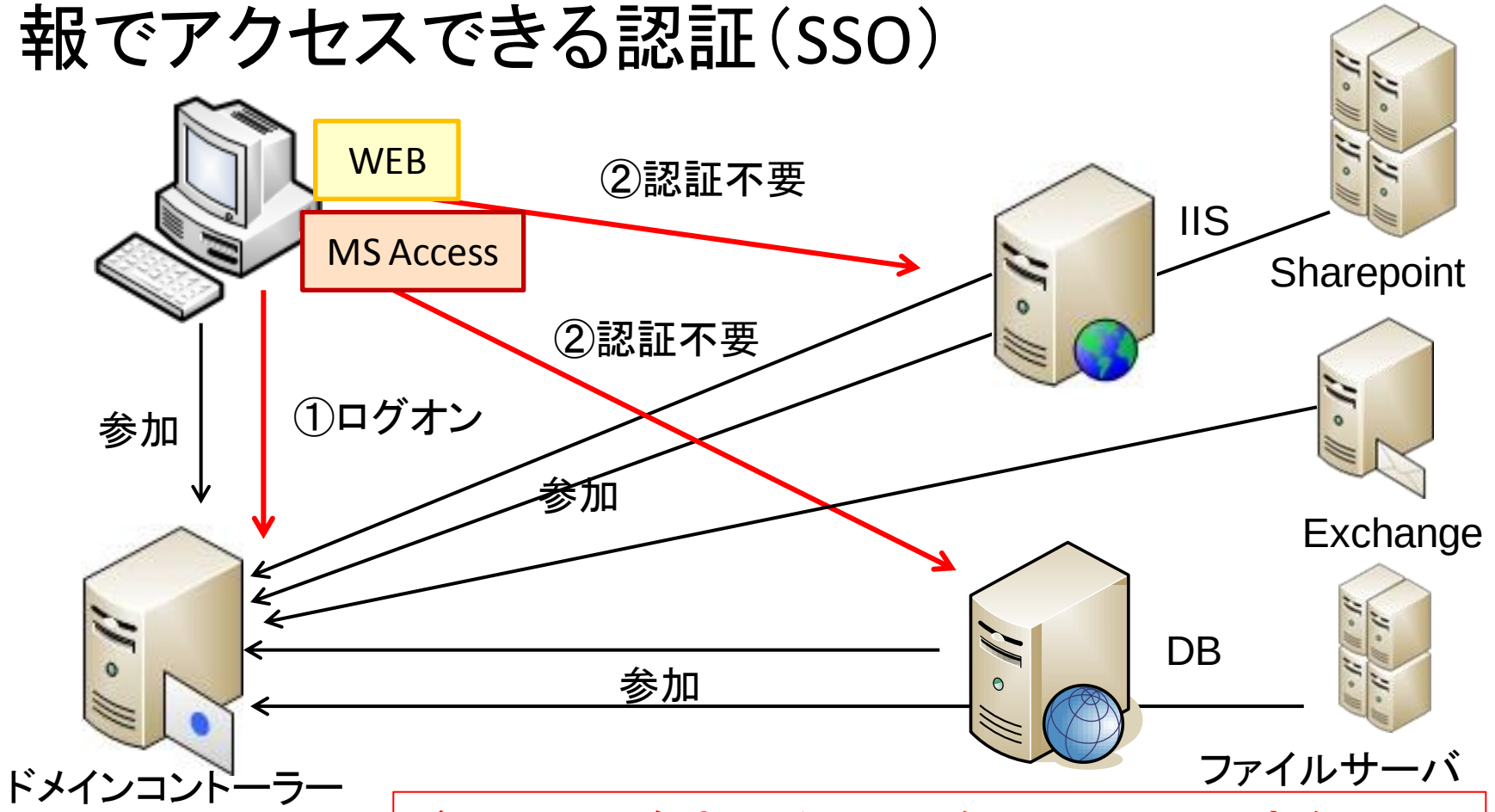
→ ADについて，調べた．

→ SQLサーバを使っている僕としては，ADには魅力的な機能があった．

2009年9月 UPKI-学術認証フェデレーション（運用）に参加

ADの技術①： 統合 Windows 認証

- ドメインに参加したクライアントからIISやSQLサーバにクライアントにログオンした認証情報でアクセスできる認証（SSO）

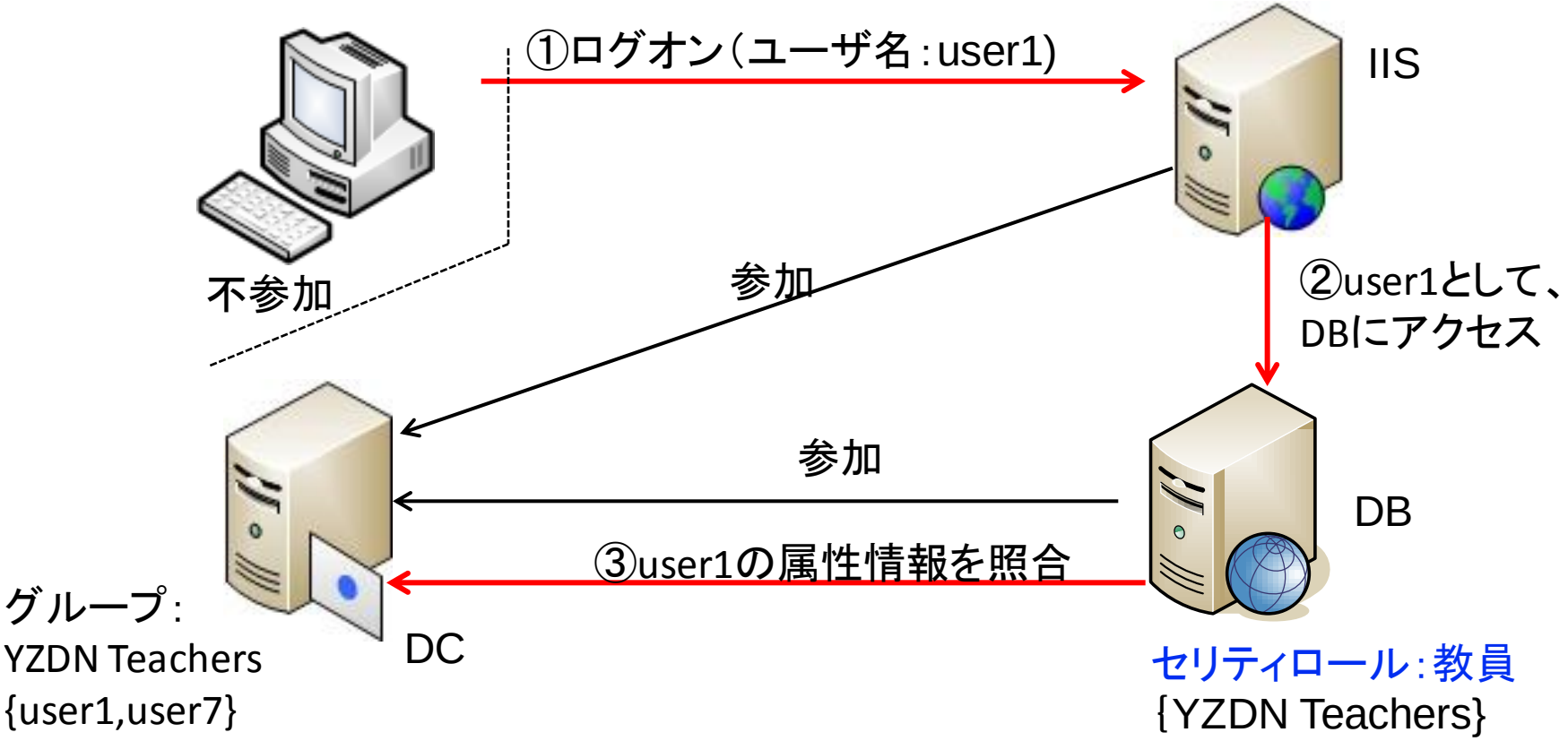


ドメインに参加したPCでないと利用できない！

ADの技術②: 偽装 (Impersonation)

IISサーバに、基本認証したときに、認証ユーザがIISサーバ上で、作業をしてるようにする技術。

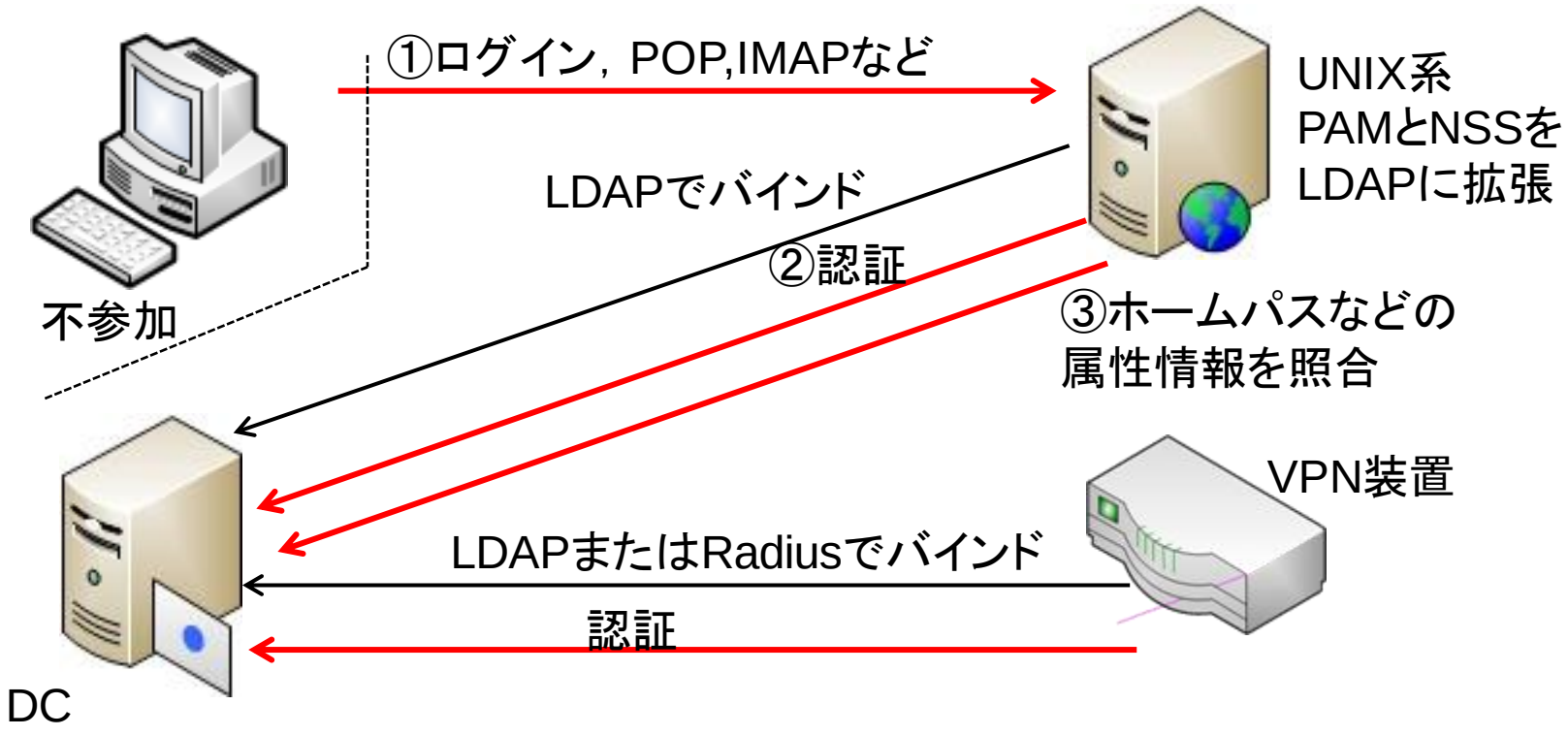
データベースのセキュリティに利用可能



ADの技術③: ネットワーク装置やUNIXの認証も可能

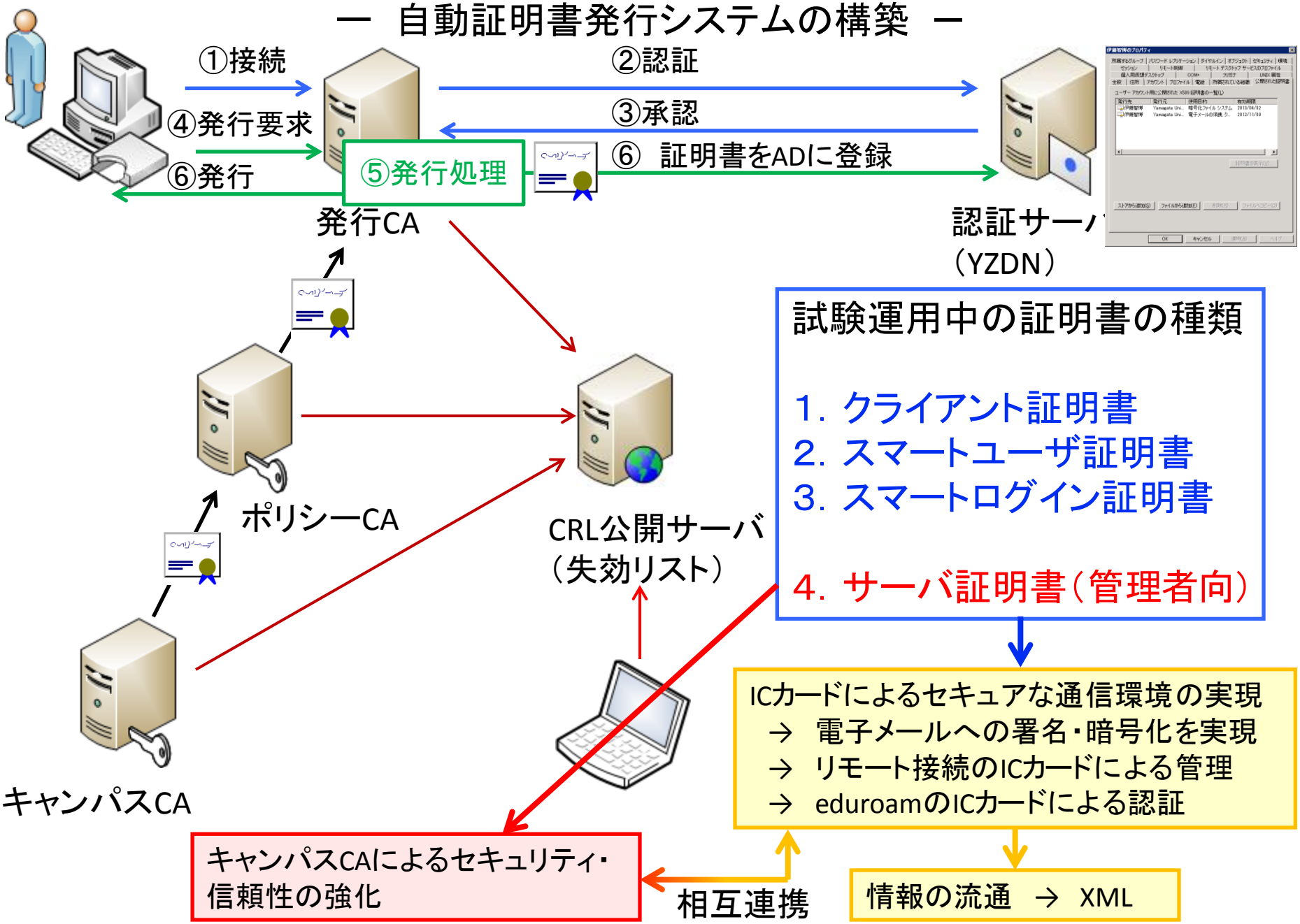
UNIXサーバやネットワーク装置の認証もAD可能

UNIXの場合，SFU（SUA)によるスキーマの拡張が必要

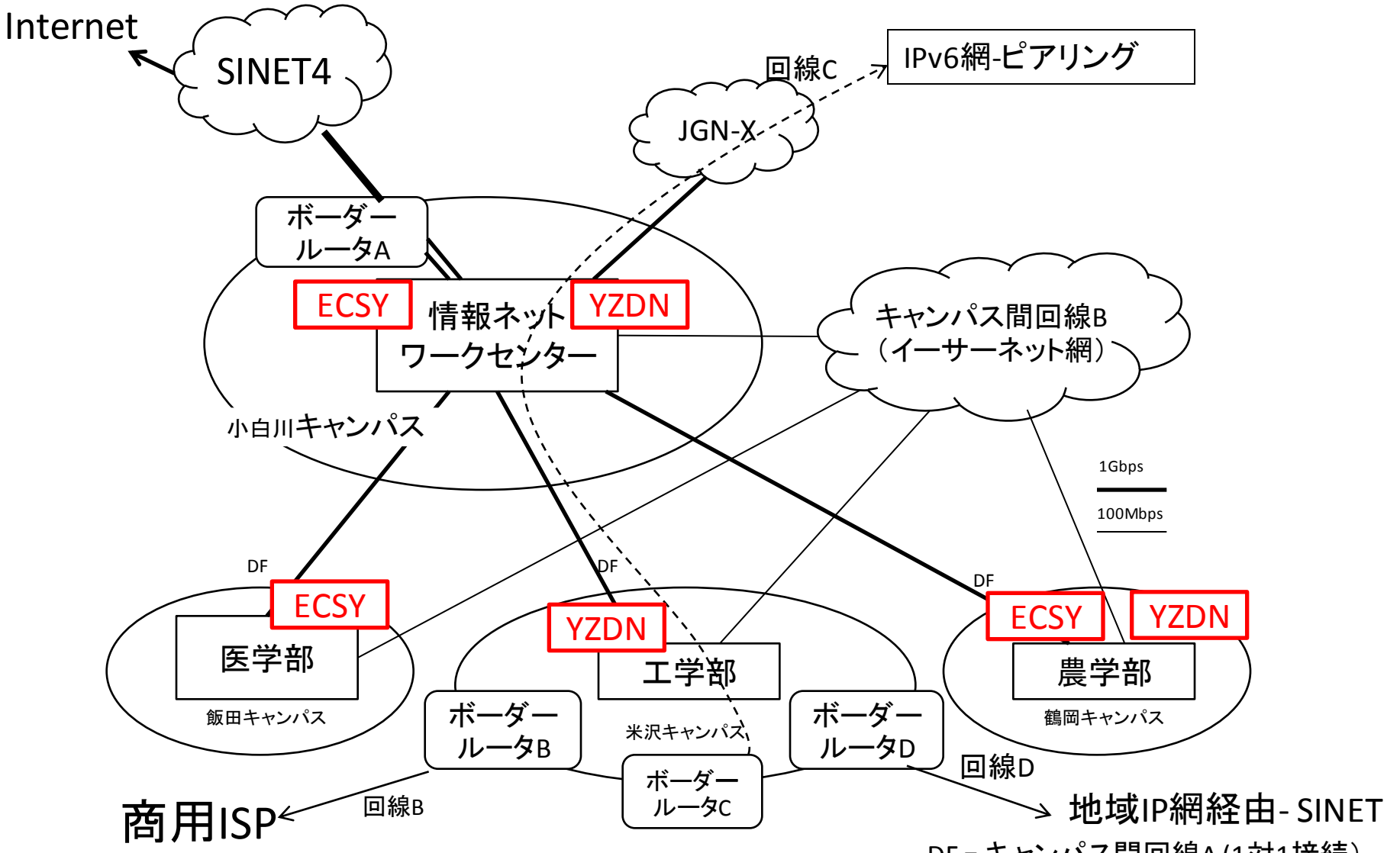


ADとCAの連携：証明書によるセキュリティ強化

― 自動証明書発行システムの構築 ―

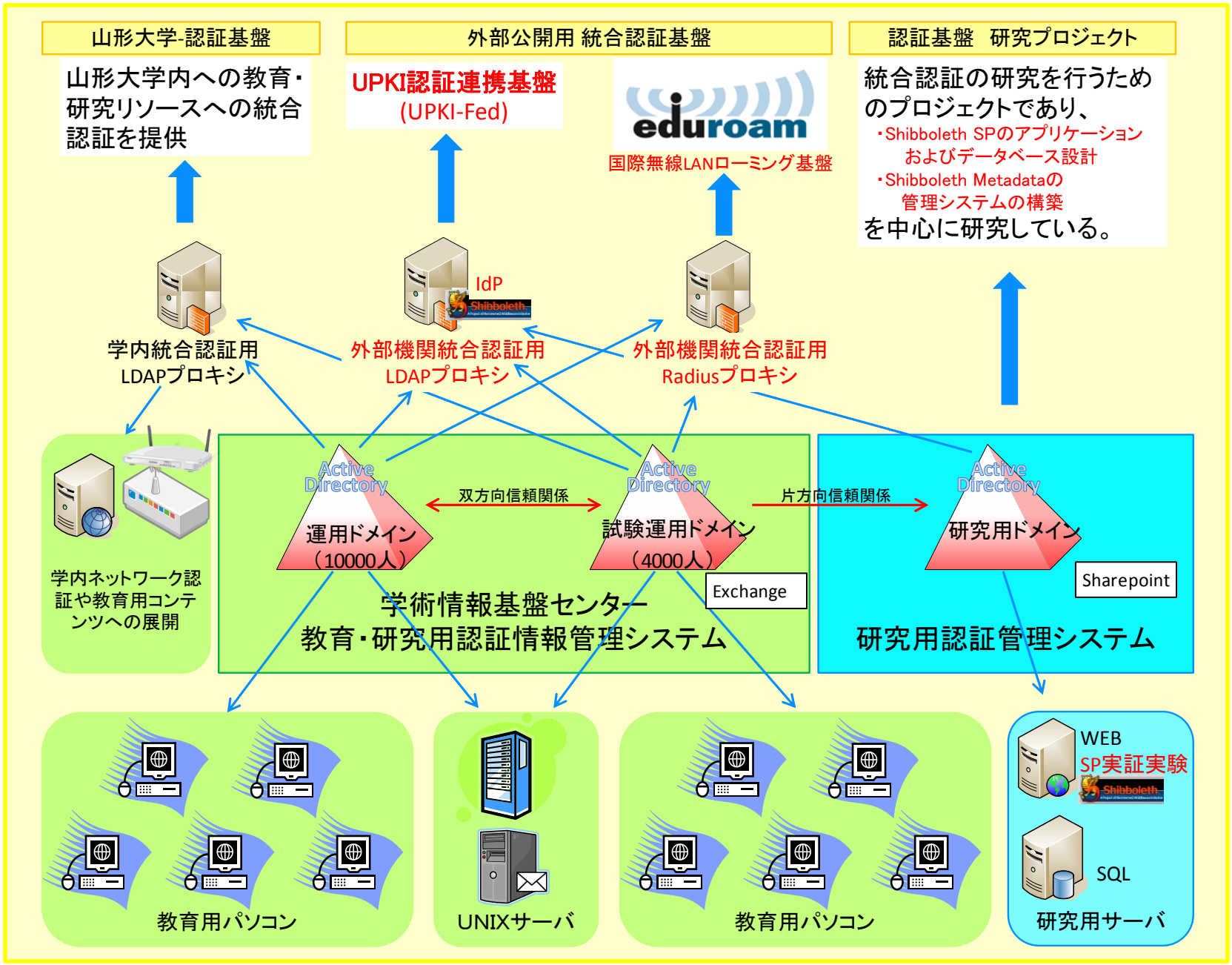


ドメインコントローラーの配置と対外回線



複数キャンパスに分散配置したことによって高可用性を実現

統合認証基盤の全体構想



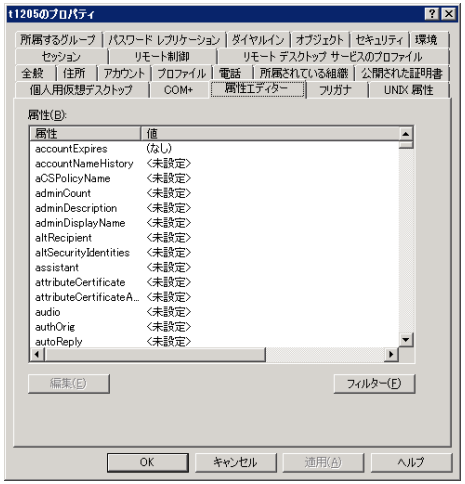
結論：なぜ，AD？

- 教育用システムの利用者端末のOSはWindows

  → ADの導入は必須

- Windows統合認証を利用することによって，SQLサーバなどWindows系のアプリケーションサーバの認証を統合できる(.NET のライブラリーの充実）
- UNIX系もADを認証基盤として統合可能
- クライアント証明書との連携可能
- リーズナブル
- 分散DBを利用可能（分散管理に適する）
- 属性エディタなどの

  充実したツールが利用可能(ADSI EDITなど)



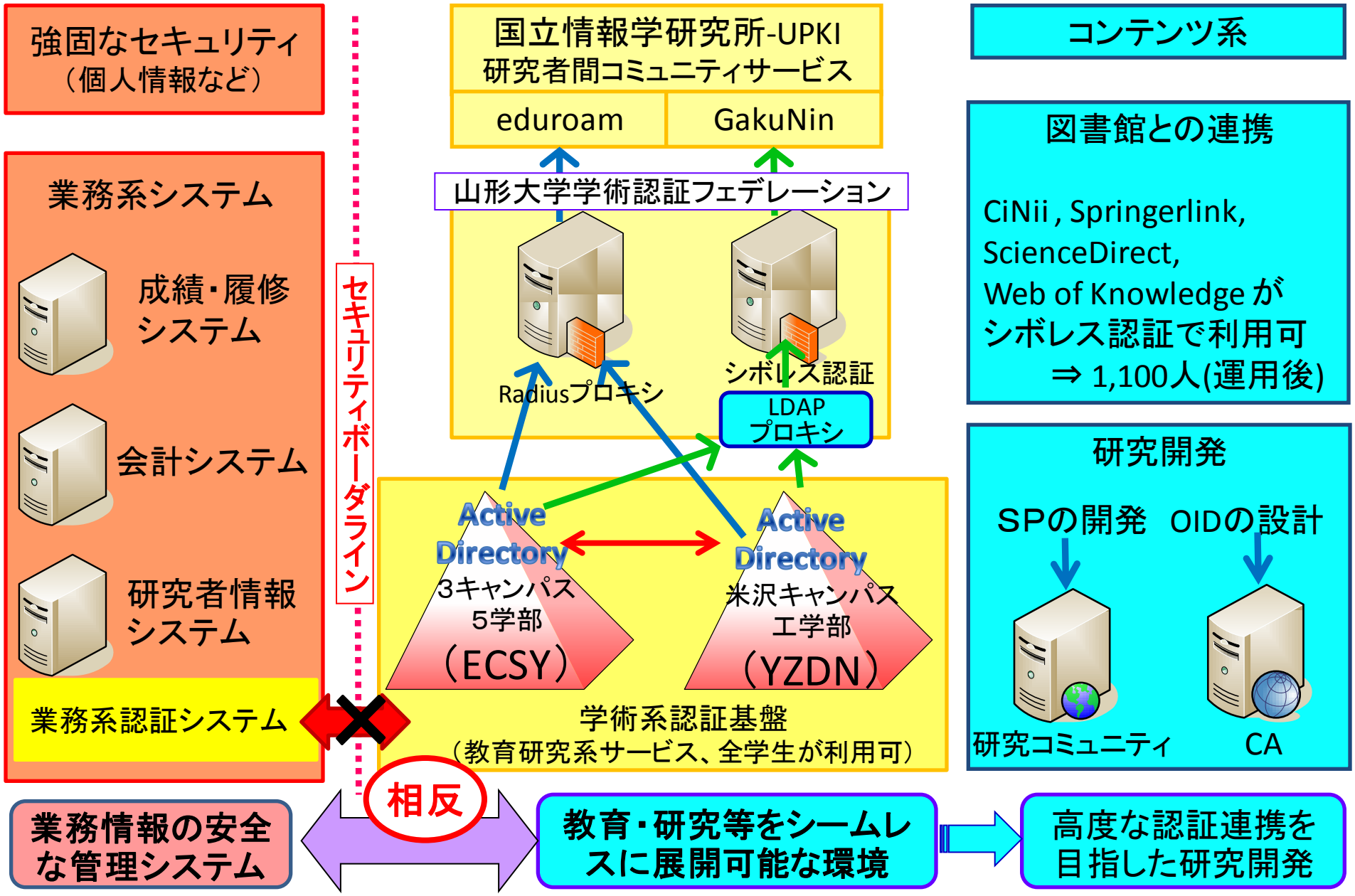
使おうと思えば 充分元が取れると踏んで，展開した.

アジェンダ

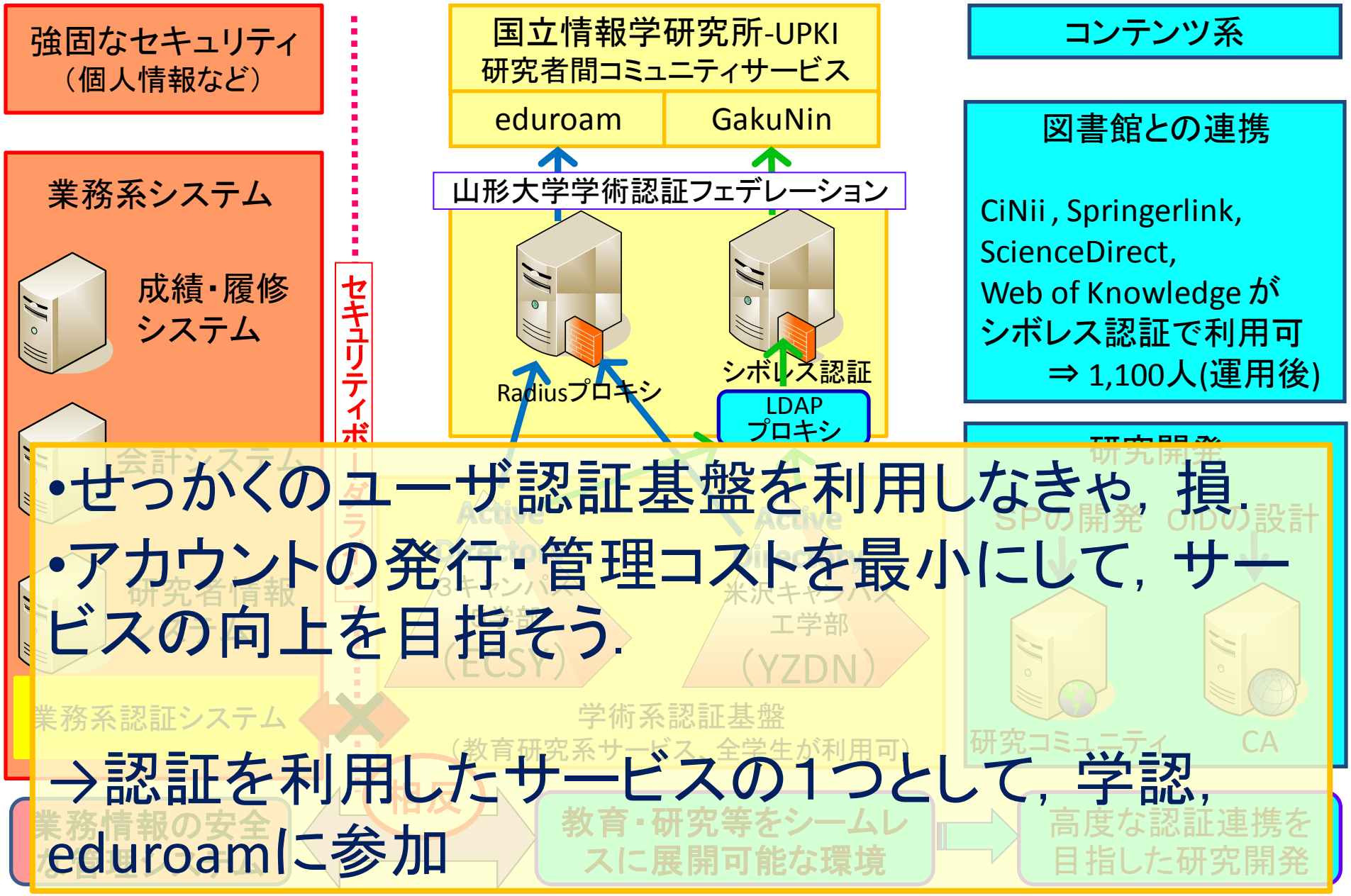
1. なぜ，Active Directory？

2. 学認への参加，シボレスとADFS

山形大学の認証基盤とGakuNinとの関係



山形大学の認証基盤とGakuNinとの関係



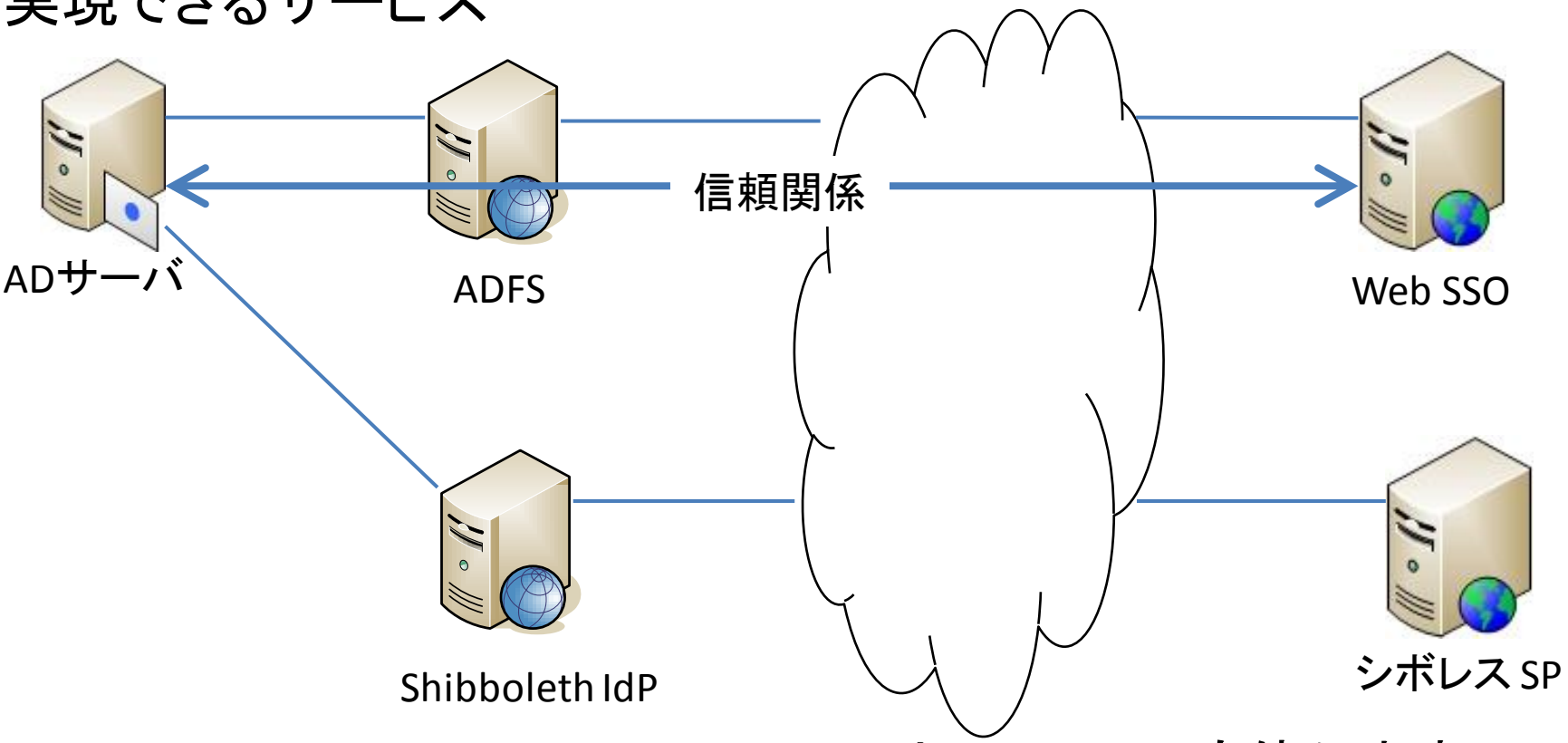
- せっかくのユーザ認証基盤を利用しなきゃ，損．
- アカウントの発行・管理コストを最小にして，サービスの向上を目指そう．

→認証を利用したサービスの1つとして，学認，eduroamに参加

ADFSって何？

ADFS　=　Active Directory フェデレーション サービス

〇何ができるの？
　外部のWebサーバとADFSサーバ経由でシングルサインオンを実現できるサービス



ADFS 2.0は，SAML 2.0も使えます．

ADFSが使える認証の種類

Web.configより

```
<localAuthenticationTypes>
    <add name="Integrated" page="auth/integrated/" />
    <add name="Forms" page="FormsSignIn.aspx" />
    <add name="TlsClient" page="auth/sslclient/" />
    <add name="Basic" page="auth/basic/" />
</localAuthenticationTypes>
```

⟶ Windows統合認証
(Authentication Context = urn:federation:authentication:windows)

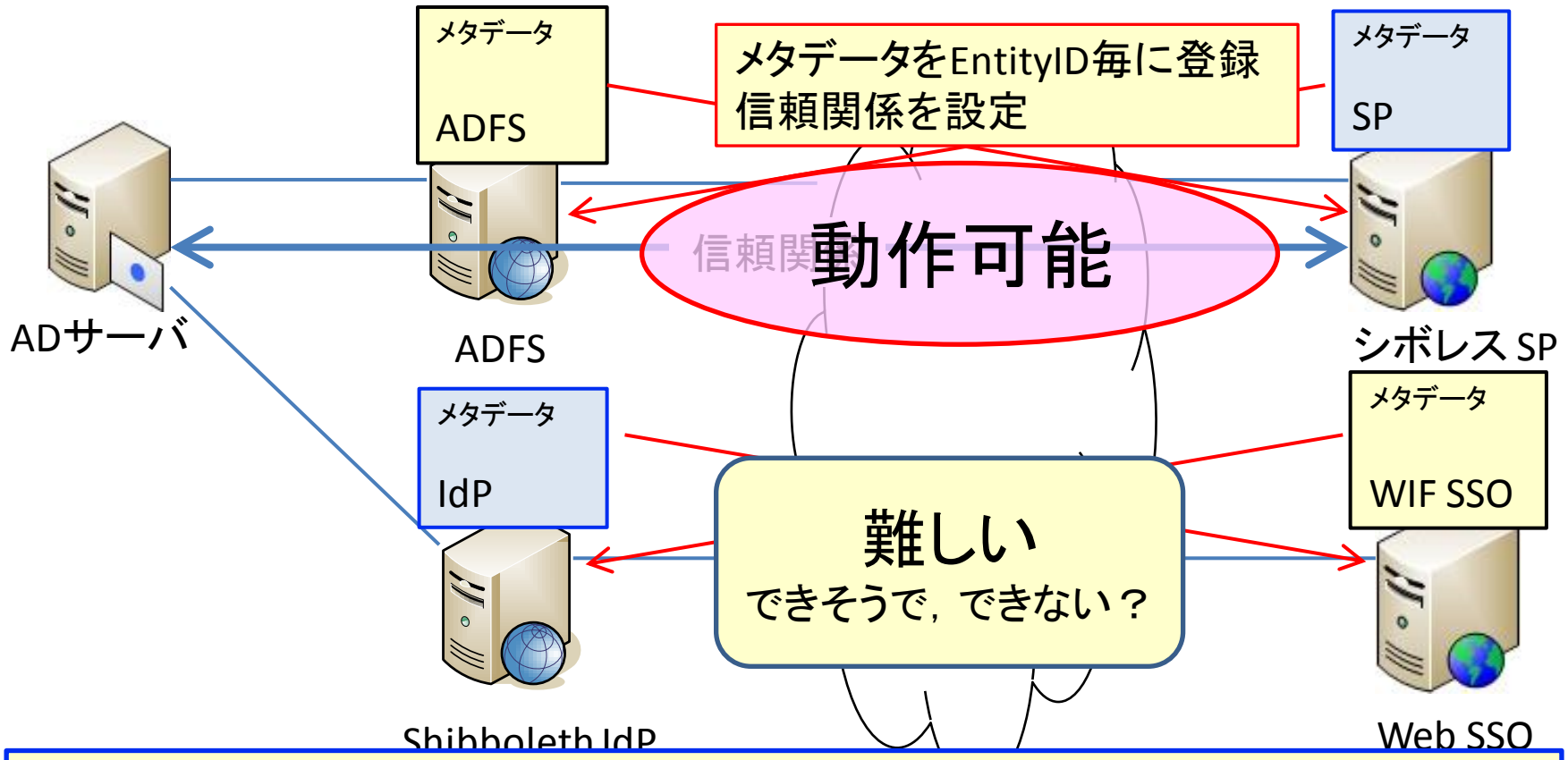
⟶ フォームベース認証

⟶ クライアント証明書認証
（Windows CA, スマートカードOK)

⟶ 基本認証

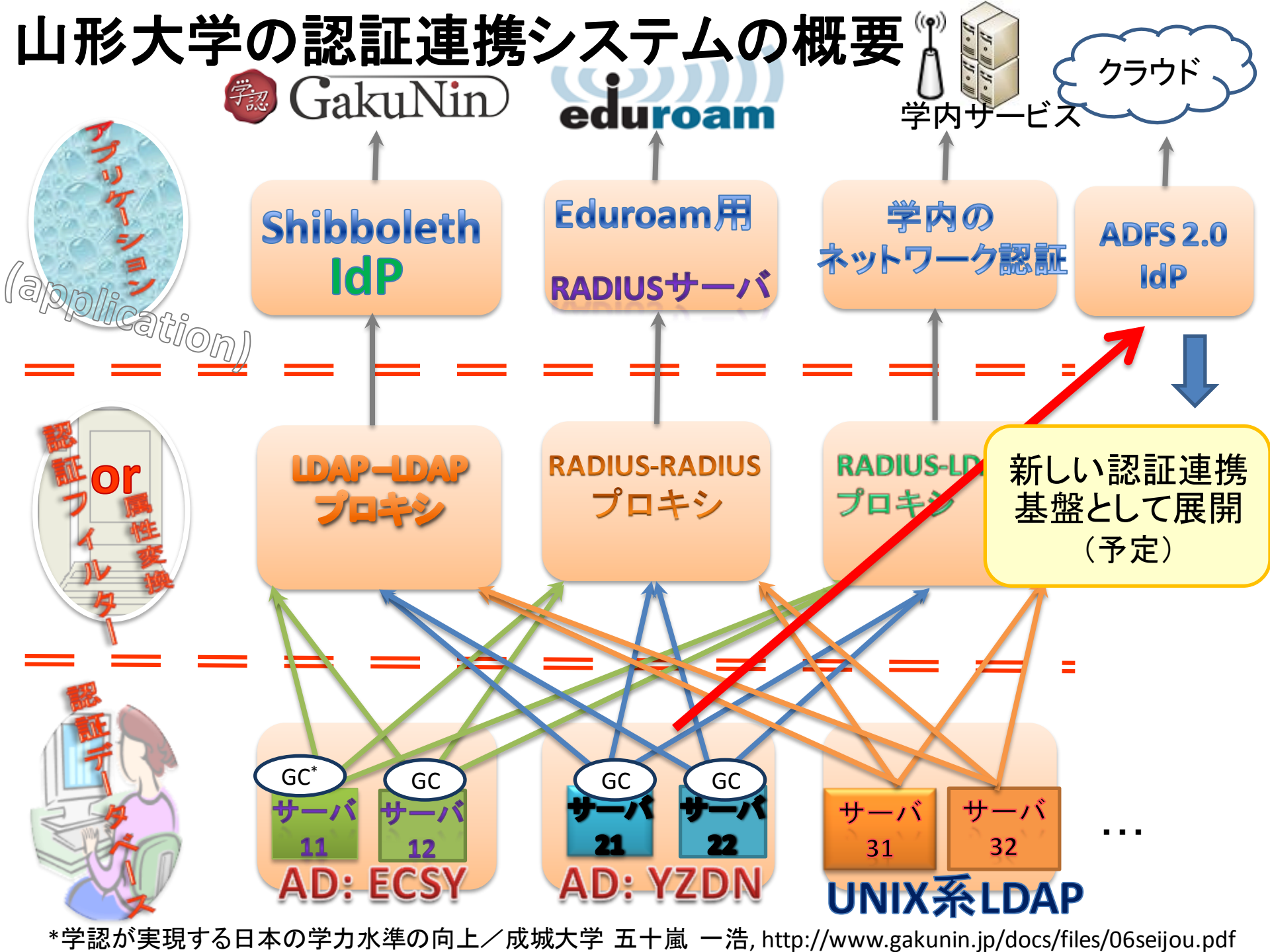
ADFSとShibboleth IdPは，Identity Providerとしては，同等の機能を有する．　→　上手に使うとShibboleth IdPの代替手段になる．

相互連携はできるかなぁ？



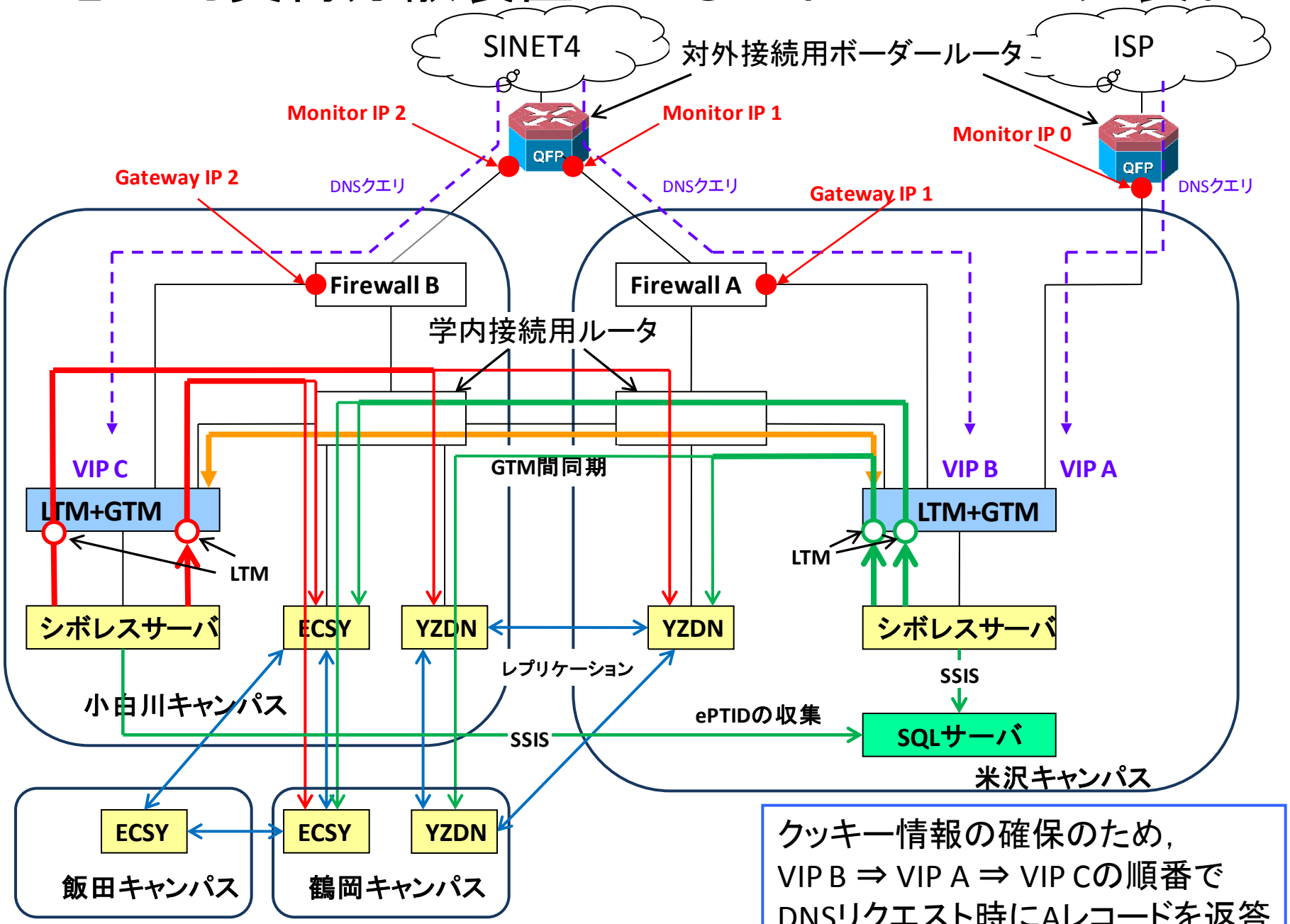
・1:1でメタデータを交換して，信頼関係を設定すれば，ADFSを認証連携サービスとして利用可能.
　→　Shibboleth IdPの同等の機能あり（StoredIDを除く）
・SPのメタデータを自動登録するには，技が必要.

山形大学の認証連携システムの概要



*学認が実現する日本の学力水準の向上／成城大学 五十嵐 一浩, http://www.gakunin.jp/docs/files/06seijou.pdf

地理的負荷分散装置によるシボレスIdPの冗長化



クッキー情報の確保のため，
VIP B ⇒ VIP A ⇒ VIP Cの順番で
DNSリクエスト時にAレコードを返答

設計： 東京エレクトロンデバイス

まとめ

１．なぜActive Directory？

センター端末や利用者の端末のOSが主にWindowsであるので，それらの端末との親和性を考慮するとADが最適であると判断した．Windows系の統合認証は，問題なし．

機能も十分であり，UNIXなどとの連携ができ，かつ，リーズナブルであるので，ADを採用した．

２．学認への参加，シボレスとADFS

ADの認証基盤にシボレスやADFSを認証連携アプリケーションとして接続することで，学認や外部のサービスの認証連携可能である．

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。

一部のシステムは、文部科学省　平成22年度補正予算のご協力により、構築されております。