シングルサインオン導入事例と導入戦略(1)
― 山形大学UPKI認証基盤の状況 ―

山形大学　学術情報基盤センター
伊藤智博

情報処理軽井沢セミナー　2009年9月3日（木）

本日の課題

- ✔導入事例の背景
- 学内調整、学内交渉
- 導入事例（システム設計、ポリシーなど）
- 山形大学の現状と今後の展開
- ミニッツペーパーの提出

目標

山形大学のシングルサインオン導入の背景

情報社会の生き残りを賭けて
分散キャンパスの学内認証統合から
世界のユニバーサル認証統合へ！

分散キャンパスのため、キャンパスごとの事情によりアカウントの発行・管理・課金などのポリシーが異なる。

→ 米沢キャンパス（工学部）では、2005年に、学術系はシングルサインオンに移行。

2005年ごろの工学部の技術的な背景

○運用試験ベース

- SFUによるUNIX-AD間のパスワード同期
- VPNのユーザ認証にADを活用
- ネットワーク利用者認証システムの導入
- ADのSFUスキーマ拡張によるメールサーバのLDAP統合認証基盤への移行試験

→ 事実上、UNIXシステムの認証基盤をADに統合

○研究ベース(データベースアメニティ研究所の協力)

- Webサーバ証明書に導入(VeriSign, Comodo)
- S/MIME証明書の導入試験、OID取得
- IISサーバのAD認証(薬品管理、ALCネットアカデミー)

2007年教育計算機システム更新

ポリシー：　同一アカウントでPCおよびサーバを利用する。

工学部で実施した技術開発を活用して、事実上の全学統合認証を構築する。

- Active Directoryのドメインを2ドメインに変更。
- UNIX系システムを4キャンパス配置から2キャンパス配置に変更。
- UNIX系システムの認証システムをADにLDAPまたはNISバインドに変更（事実上の統合認証基盤）
- メールシステム（UNIX)もADによる認証。
- LDAP　プロキシなどによる統合認証基盤の構築

本日の課題

- 導入事例の背景
- 学内調整、学内交渉、実証試験ポリシー策定
- 導入事例（システム設計、ポリシーなど）
- 山形大学の現状と今後の展開
- ミニッツペーパーの提出

目標

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)、
  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。

苦労したことやうまくいった体制

- 苦労したこと

  タイミング　→　平成20年度のTOPIC講習会などで、UPKI事業が学術情報基盤センター内で浸透してきた頃合いを見計らってスタート。

- うまくいった体制

  ・既に学内の認証基盤が統合完了。

  ・少数規模の研究プロジェクトとして、スタート。

  →その後、関連部署（図書館）に研究への協力を依頼

  ・NIIさんによって、基本スキーマなどの情報を提供して頂けるので、非常に楽。

本日の課題

- 導入事例の背景
- 学内調整、学内交渉、実証試験ポリシー策定
-  導入事例（システム設計、ポリシーなど）
- 山形大学の現状と今後の展開
- 目標 ミニッツペーパーの提出

導入事例(システム設計、ポリシーなど)

✔山形大学の認証情報の調査

- 統合認証基盤の全体設計
- Shibboleth IdPの構築
- eduroam用radius プロキシの構築と電子ジャーナルに関するライセンス問題検討

山形大学の認証状況

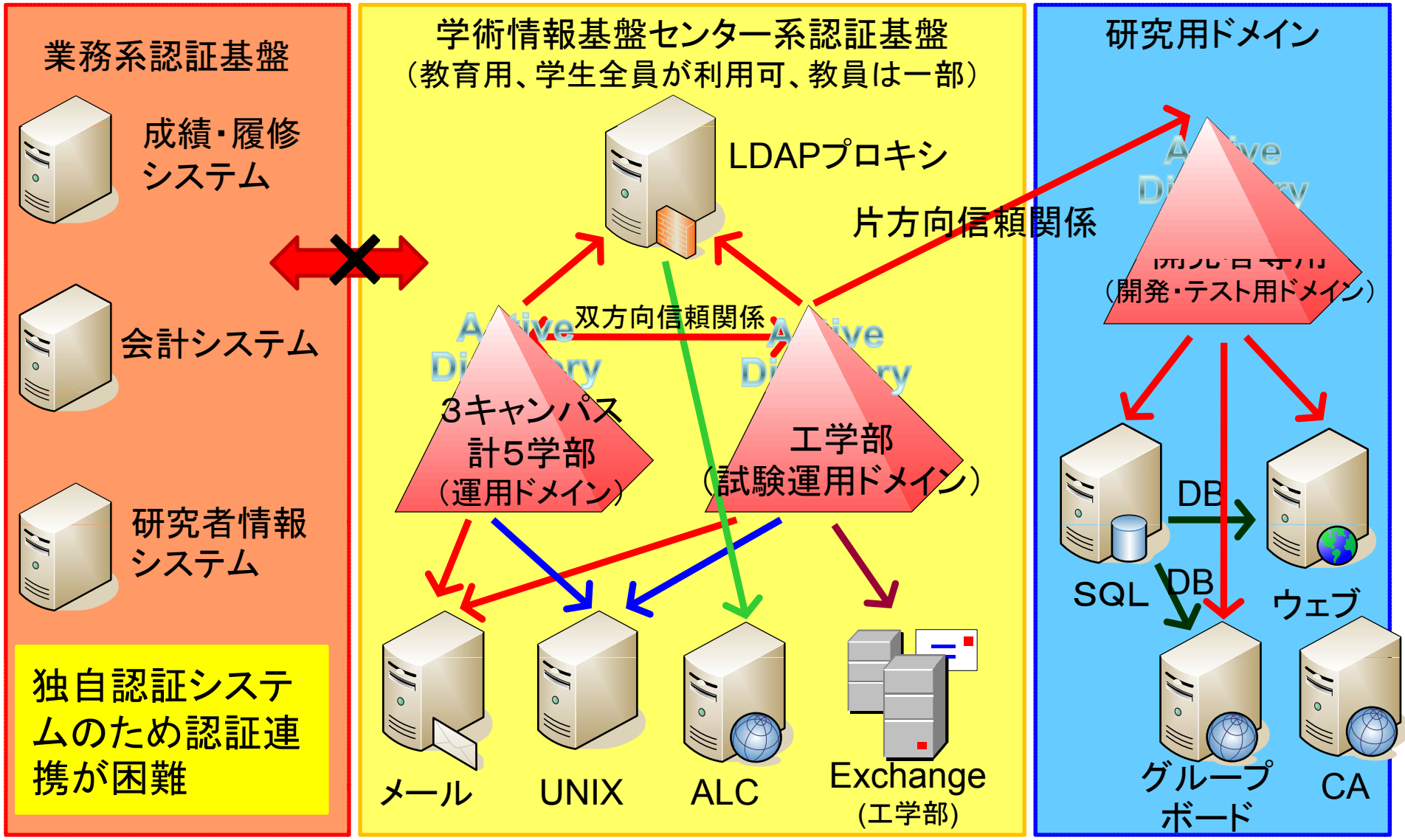
・独立したアカウントによる認証
学務情報システム（シラバス、成績管理）、会計システム、
研究者情報、etc

・ディレクトリーサービスによる認証
学術情報基盤センター（Active Directory)
教育用パソコン、教育用UNIX実習システム、無線LAN、
VPN、LAN、ALC NetAcademy2、メールシステム、
Google Apps（ID, Password 同期を含む），
LMS（WebClass），自動講義収録システム,etc
学部独自のコンピュータシステムなど

・磁気カード・バーコードを使った認証
駐車場、入退室管理、学生用証明書発行機、etc

山形大学の認証基盤の概要

－　Shibboleth統合前　－



認証基盤の概要のまとめ

- 学術（教育・研究）系　と　業務系（成績、会計など）の認証基盤はユーザ名　も　パスワードも統合されていない。

  →　アカウントのセキュリティレベルが2つ

  →　学術系アカウントがクラックされても重要情報の流出は難しい。

- 学術系は、複数認証基盤を統合しながら、協調運用を行っている。

  →　学術系は、学内としては統合済み

  →　学術情報基盤センターのポリシーは、同一アカウントでサービス(PC,コンテンツなど)を展開する。

学術情報基盤センターの認証システム

山形大学の学術情報基盤センターでは、教育・研究用認証基盤として、Microsoft® Active Directory ®(AD)を使用している。ドメイン構成としては、「運用ドメイン」、「試験運用ドメイン」の2つのドメインがある。「試験運用ドメイン」は、工学部の学生・教職員の約4000人アカウントが登録されており、「運用ドメイン」には、工学以外の学生・教職員・事務組織などの約10000人のアカウントが登録されている。
複数ドメインを構成している理由としては、

- 運用ポリシーが異なること。
- 将来、セキュリティポリシーの変更により円滑にドメインの追加・拡張ができ、かつ、統合認証を構築できるようにする複数ドメインによる統合認証システムの運用実験を行うこと(例えば、事務系情報のセキュリティ強化に伴うドメインの追加などを容易に可能にする)。

の2点である。

既存の2ドメインの認証基盤を統合し、Shibboleth対応することにより利用者への負担が少なく、UPKIプロジェクトへの参加が可能になる。

実証試験のポリシー

- 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による複数認証基盤の統合化
  → 無線LANのセキュリティ向上 → eduroam
  → IPv6の無線LAN認証実験(IEEE 802.11i)

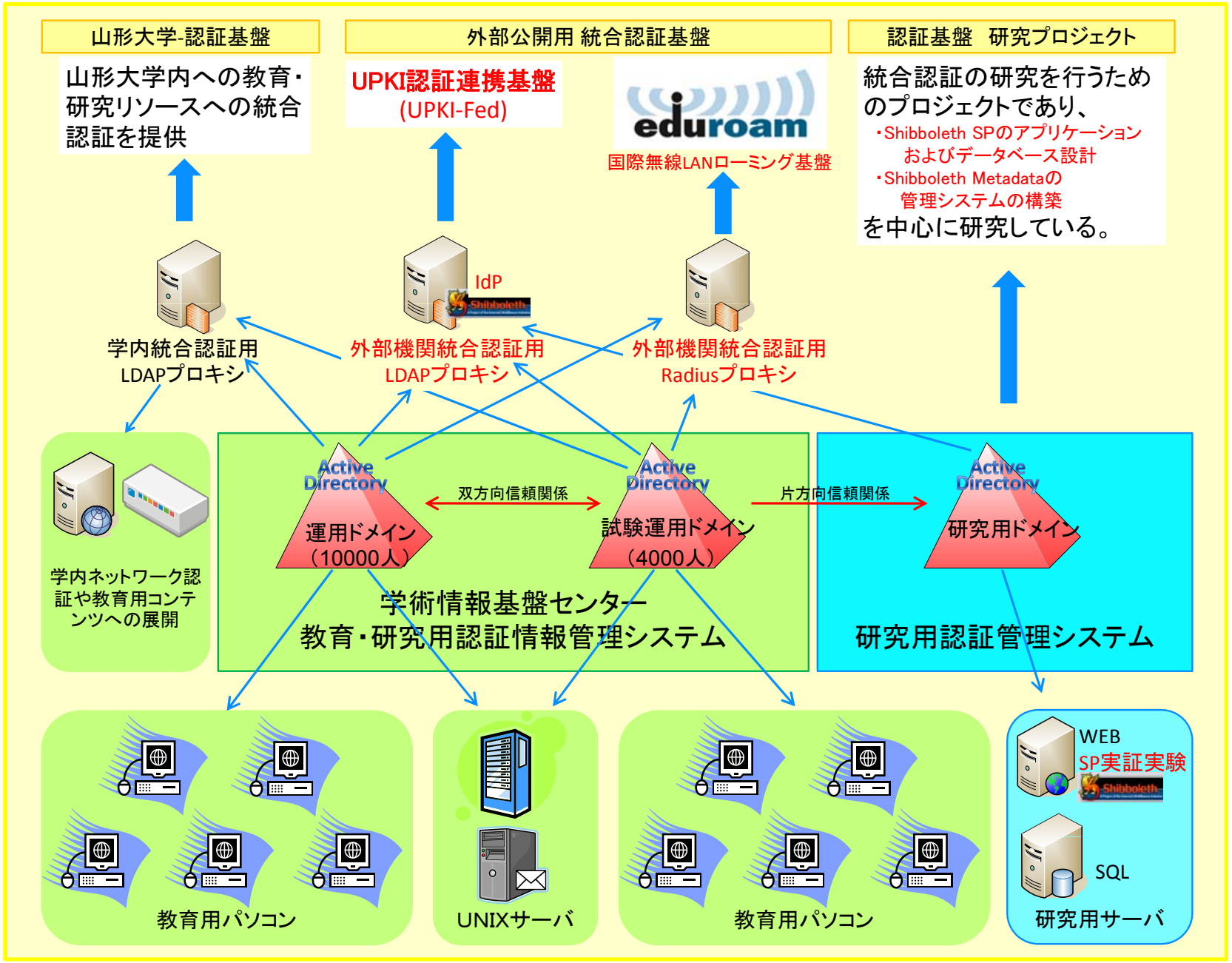
- システム構築コストが高くても、運用コストを最小にすることが継続性への鍵。

- 目的:外部機関の認証基盤との連携技術の確立
  → 教育への活用(人材育成)

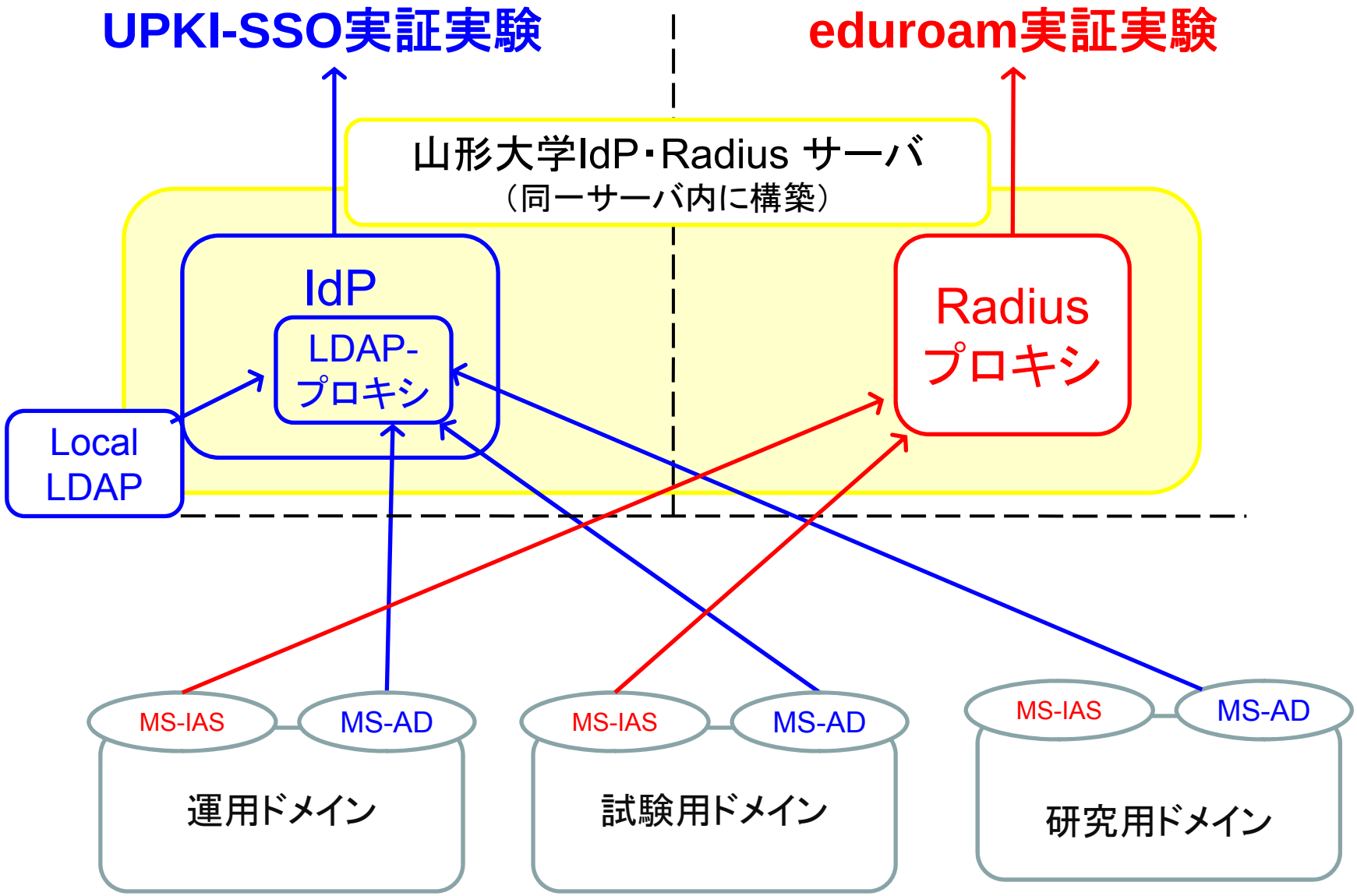
導入事例(システム設計、ポリシーなど)

- 山形大学の認証情報の調査
- ✔統合認証基盤の全体設計
- Shibboleth IdPの構築
- eduroam用radius プロキシの構築と電子ジャーナルに関するライセンス問題検討

統合認証基盤の全体設計



統合認証基盤のIdP･Radiusサーバの設計



導入事例(システム設計、ポリシーなど)

- 山形大学の認証情報の調査
- 統合認証基盤の全体設計
- ✔Shibboleth IdPの構築
- eduroam用radius プロキシの構築と電子ジャーナルに関するライセンス問題検討

外部機関用統合認証基盤システムのハードウェア構成

- ハードウェアの構成

  HP Proliant ML110；メモリ 512MB; HDD 20GB *2 (RAID 1); OS CentOS 5.2

- ソフトウェアの構成

  共通ソフトウェア

  OpenLDAP 2.3.43, Apache 2.2.9, Apache Tomcat 6.0.18, JDK 6 Update 10, Apache Ant 1.7.1, BerkeleyDB 4.3, OpenSSL 0.9.8i

  UPKI-SSO関係

  Shibboleth® IdP 2.0.0, Shibboleth® DS 1.0 (学内テスト用)

  eduroam関係

  freeradius-server 2.1.1

Shibboleth IdPの構築手順

1. 「IdP構築・運用手順書ver1.2」に従って作業(VMイメージは使用しない)。
2. UPKI「サーバ証明書発行・導入における啓発・評価プロジェクト」よりサーバ証明書を取得。
3. IdPサーバ上のLDAPデータベース上に、テストアカウントの発行（ローカルアカウント）。
4. 「研究用ドメイン」のドメインコントローラーとLDAPプロキシの接続。
   接続は、ユーザバインドで行い、rwm-mapを利用して、ADスキーマとeduPersonスキーマにマッピング。
5. Shibboleth IdPのlogin.configとattribute-resolver.xmlに、ADに対応するように設定(紹介の設定が必要。詳細は別紙参照のこと)。
6. 動作確認として、ローカルアカウントと「研究用ドメイン」のアカウントで動作検証。
7. 「試験運用ドメイン」、「運用ドメイン」のADとも同様に接続。
8. 動作確認として、「試験運用ドメイン」、「運用ドメイン」のアカウントで動作検証。

OpenLDAPのプロキシ機能による属性の変換設定

○Compile時の注意

```
./configure --enable-overlays --enable-dyngroup --enable-dynlist ¥
--enable-rwm --enable-crypt --enable-ldap
```

○設定例

slapd.confに、

```
overlay rwm
rwm-map attribute    uid     sAMAccountname
rwm-map attribute    eduPersonPrincipalName     userprincipalname
rwm-map attribute    mail    mail
rwm-map attribute    jasn      sn
```

のように記入。

IdPをADに対応する設定例

login.configとattribute-resolver.xmlを下記に示すような紹介設定を追加することにADの認証情報で正常に認証・属性の取得ができた。

例）login.config

```
edu.vt.middleware.ldap.jaas.LdapLoginModule sufficient
  host="localhost"
  base="dc=xxxxx,dc=yamagata-u,dc=ac,dc=jp"
  ssl="false"
  userField="eduPersonPrincipalName"
  subtreeSearch="true"
  serviceUser="cn=xxxx,CN=Users,dc=xxxx,dc=yamagata-u,dc=ac,dc=jp"
  serviceCredential="xxxxx"
  referral=“follow”      ← 重要
```

例）attribute-resolver.xml

```
<resolver:DataConnector id="myLDAP2" xsi:type="LDAPDirectory"
xmlns="urn:mace:shibboleth:2.0:resolver:dc“
  ldapURL="ldap://localhost" baseDN="dc=xxxx,dc=yamagata-u,dc=ac,dc=JP“
  principal="cn=xxxxx,CN=Users,dc=xxxx,dc=yamagata-u,dc=ac,dc=jp“ principalCredential="xxxxx">
    <FilterTemplate>
      <![CDATA[
      (eduPersonPrincipalName=$requestContext.principalName)
       ]]>
    </FilterTemplate>
    <LDAPProperty name=“java.naming.referral” value=“follow”/>        ← 重要
</resolver:DataConnector>
```

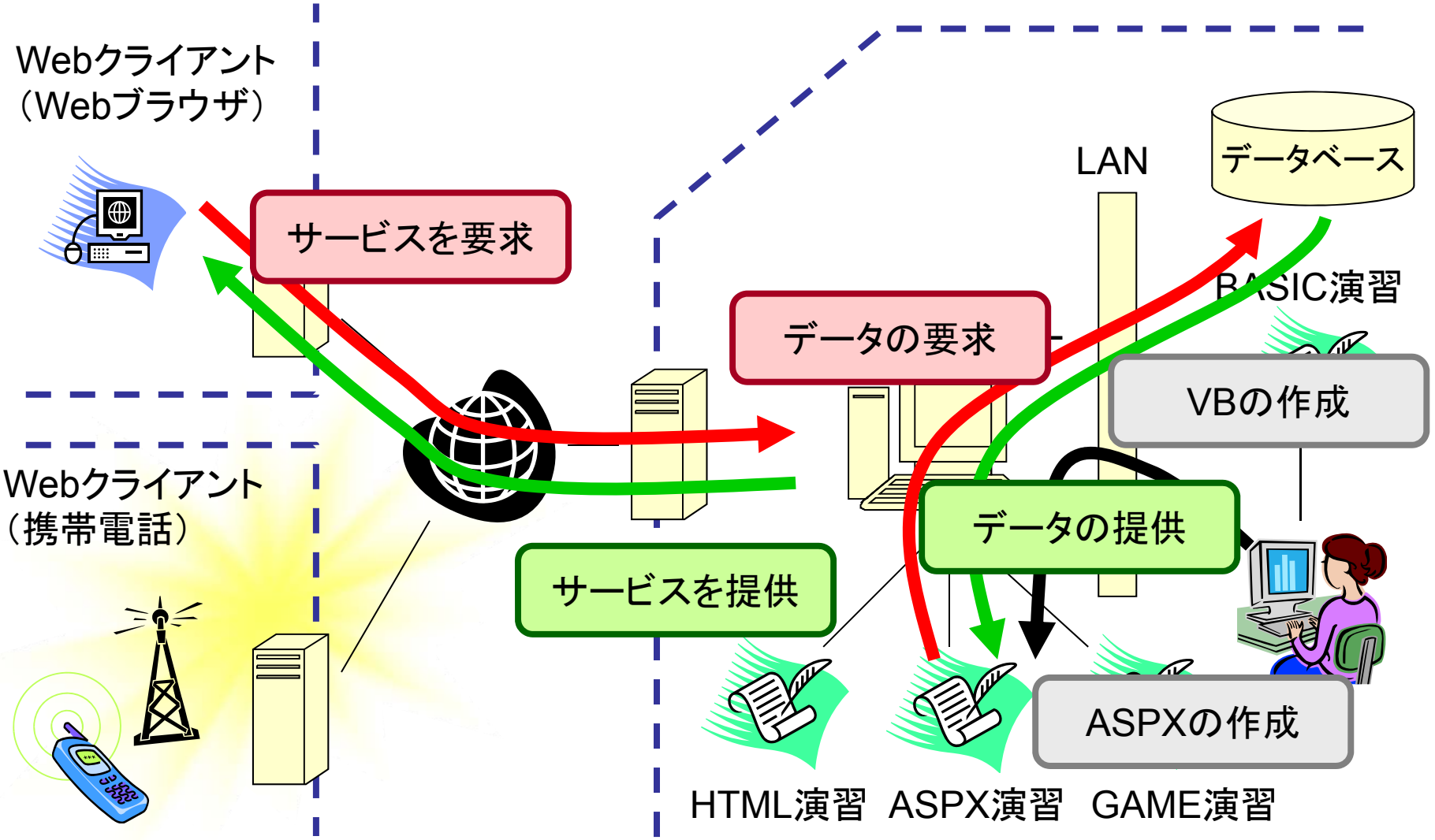
山形大学のIdPのまとめ

1. ユーザIDのフォーマットは、複数ドメインに多対応するため、eduroamフォーマットである「xxx@yyy.yamagata-u.ac.jp」とする（暫定）。

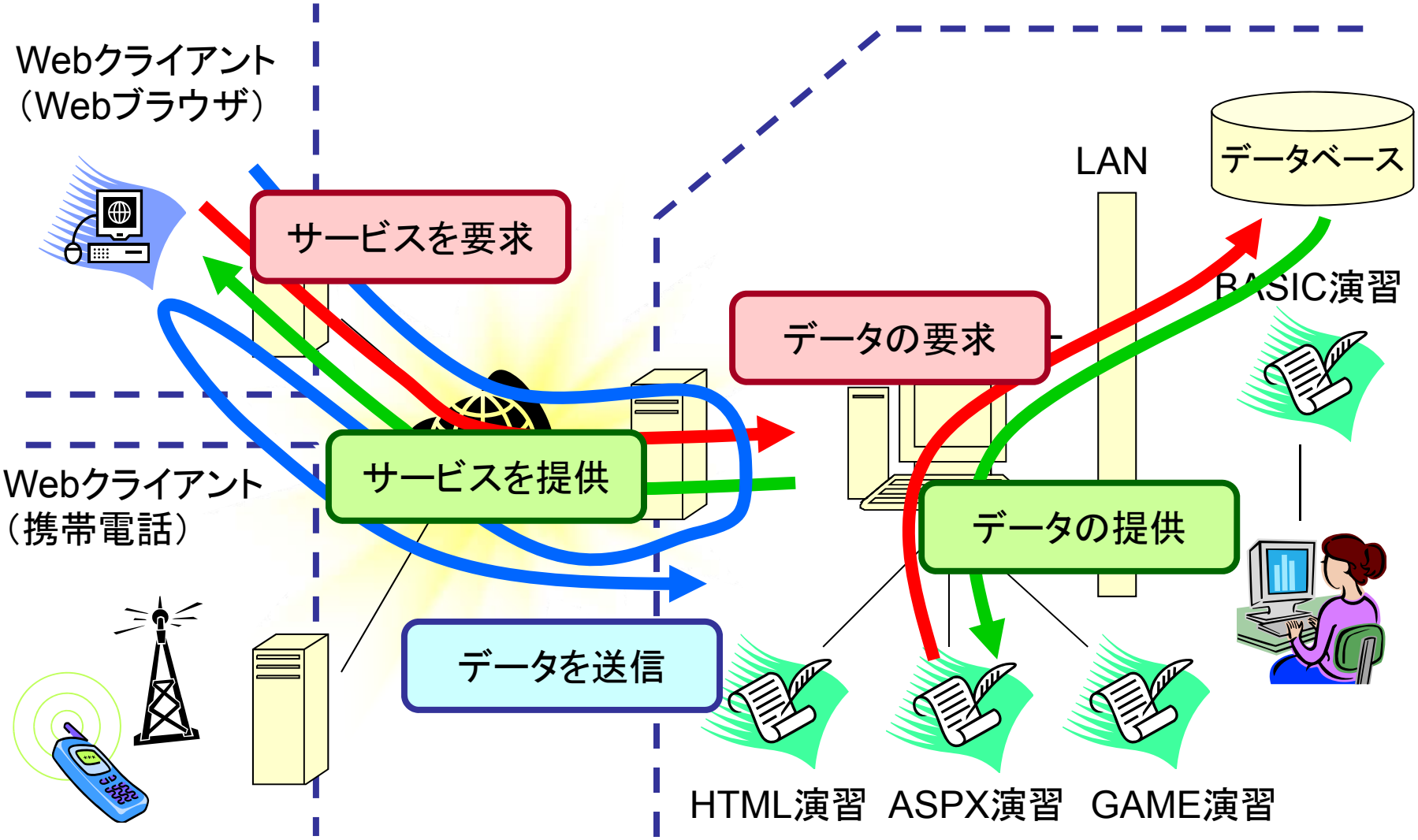
2. ADスキーマとedupersonスキーマの変換テーブルを検討する必要がある。または、ADのスキーマを拡張して、eduPersonスキーマに対応することも検証が必要であろう。

3. LDAPプロキシ経由でAD認証基盤を利用するときは、リフェラルの設定が必要である。

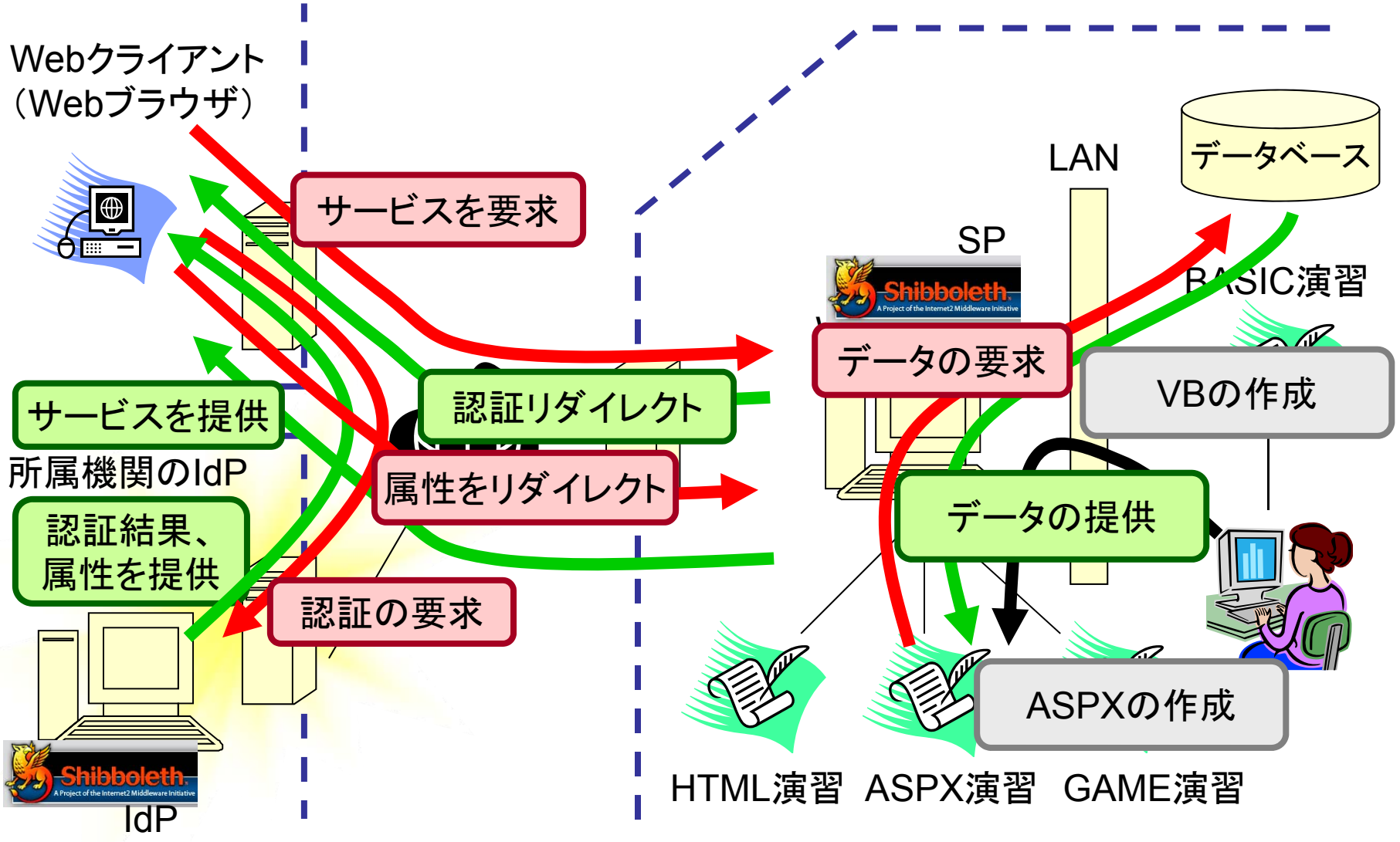
サーバーアプリケーションとは？



POSTを使ったデータの送信



サーバーアプリケーション
― Shibboleth SPの設計―



演習問題

- データベース、ShibbolethおよびWebサービスを活用したサービスモデルを図と下記のキーワードの含む文章で説明せよ！（キーワード：HTTPS、GET、POST、データベース、Webサーバー、Webクライアント、防火壁、Shibboleth SP, Shibboleth IdP）

山形大学用メタデータ管理システム

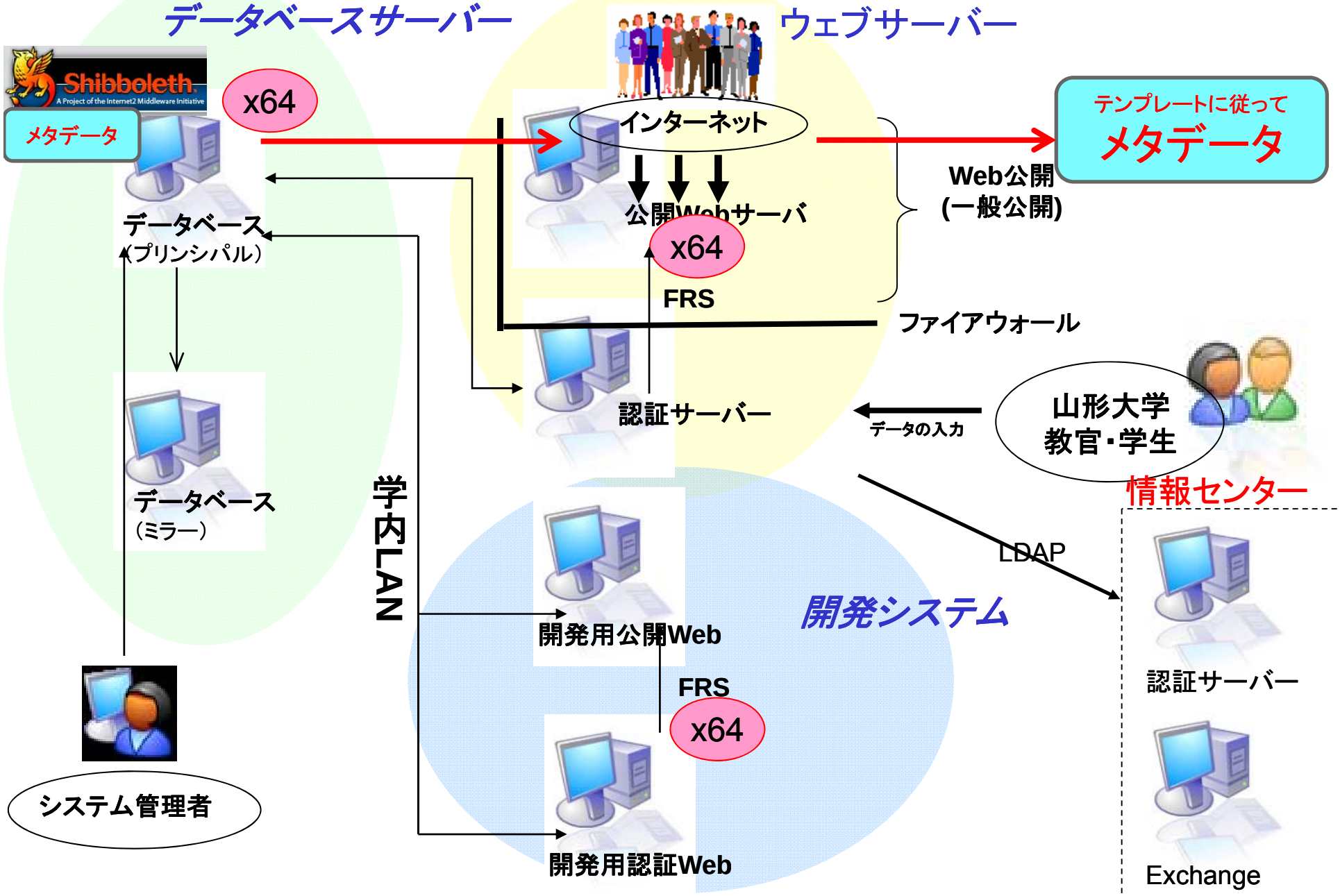
山形大学では、IdPおよびSPの実証試験および開発を円滑に実施するために、メタデータの管理システムを開発した。システムの特徴は、データベースを基盤にASP .NETによってダイナミックにメタデータを発行し、管理の簡素を図った。

システムの構成：　Microsoft ® Windows ® Server 2003,
Microsoft ® SQL Server 2005,
Visual Studio 2005 professional

山形大学のメタデータ管理システムのまとめ

・SQLサーバよりテンプレートに準拠し、メタデータを生成できる。
・メタデータは、IdP情報、SP情報の両方を管理できる。

データベースによるメタデータの管理システム



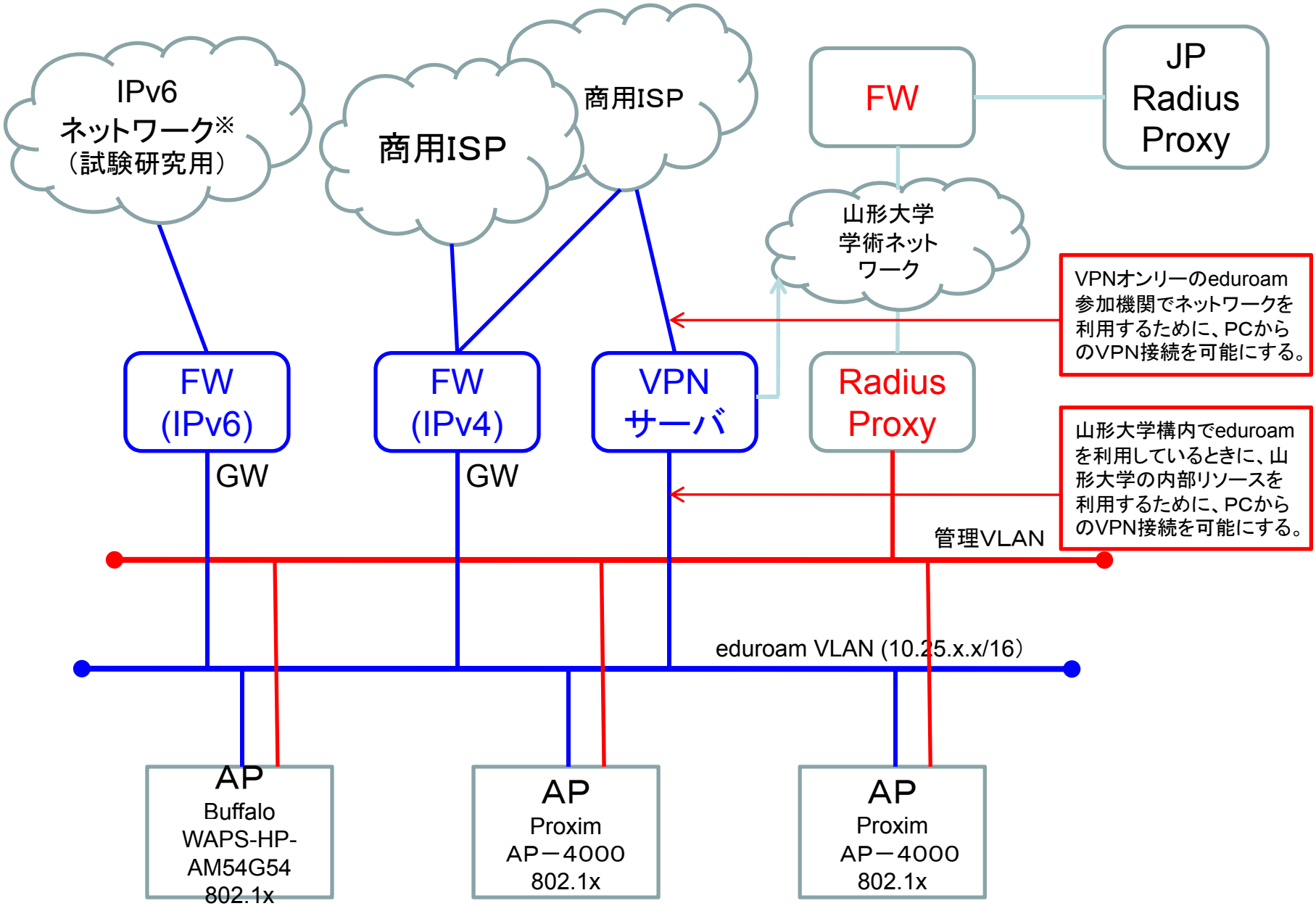
導入事例(システム設計、ポリシーなど)

- 山形大学の認証情報の調査
- 統合認証基盤の全体設計
- Shibboleth IdPの構築
- ✔eduroam用radius プロキシの構築と電子ジャーナルに関するライセンス問題検討

山形大学のeduroamシステムの仕様

1. 認証トークンは、新規に構築するRadius プロキシを経由して、ADのIASで認証する。
2. PEAP およびTTLSのSSLセッションはRadius プロキシで完結。(SSL証明書の管理コストの削減のため)
3. 無線APは、
   ESSID: eduroam
   暗号: WPA-AES または WPA2-AES
   認証: EAP-PEAP または EAP-TTLS、MS-CHAPv2
   とする。
4. IPv6の無線LAN運用試験系。
   → 802.11x認証なので、Web認証などが不要。
5. eduroam接続時の学外接続回線は、商用ISPを経由することにより、外部機関利用者の山形大学の契約電子ジャーナルなどの利用不可とし、かつ、外部機関利用者の利便性を確保する。山形大学の利用者は、eduroam専用VPN接続で電子ジャーナルを閲覧可能にする。
6. VPNオンリーの参加機関でのネットワーク利用を可能にするため、電子ジャーナルのVPN経由による利用に関する情報を出版社に調査し、解決策を検討。

eduroam無線LANシステムの概要



※IPv6ネットワークは、JGN2plusおよびWIDEプロジェクトの協力により、実験として実証試験を行っております。

VPNオンリーのeduroam機関において無線LANを利用したときのサービス展開

VPNオンリーのeduroam機関では、外部のWeb閲覧すらできないために、外部から大学へのVPN接続を許可し、かつ、全ての通信を所属大学のVPNサーバを経由する構成になる[1)]。しかし、電子ジャーナルなどの契約コンテンツを利用するにあたり、VPNサービスによる利用が許可されていないこと（契約書には明記されていないこと）が多く、VPN接続の許可が困難になる。そこで、この問題を解決するために、次の2つの課題を行い、解決の糸口を導き出した。

1．コンテンツ提供会社に、VPN経由時の閲覧の可否を確認。

2．VPN経由時に利用可能コンテンツと利用不可能コンテンツを分離するためのシステムの構築。

1. eduroamの構築と参加方法，後藤英昭, グリッド・UPKI活用のためのCSI講演会(古牧温泉), 2007/10/12, http://www.eduroam.jp/docs/grid-upki-071012.pdf

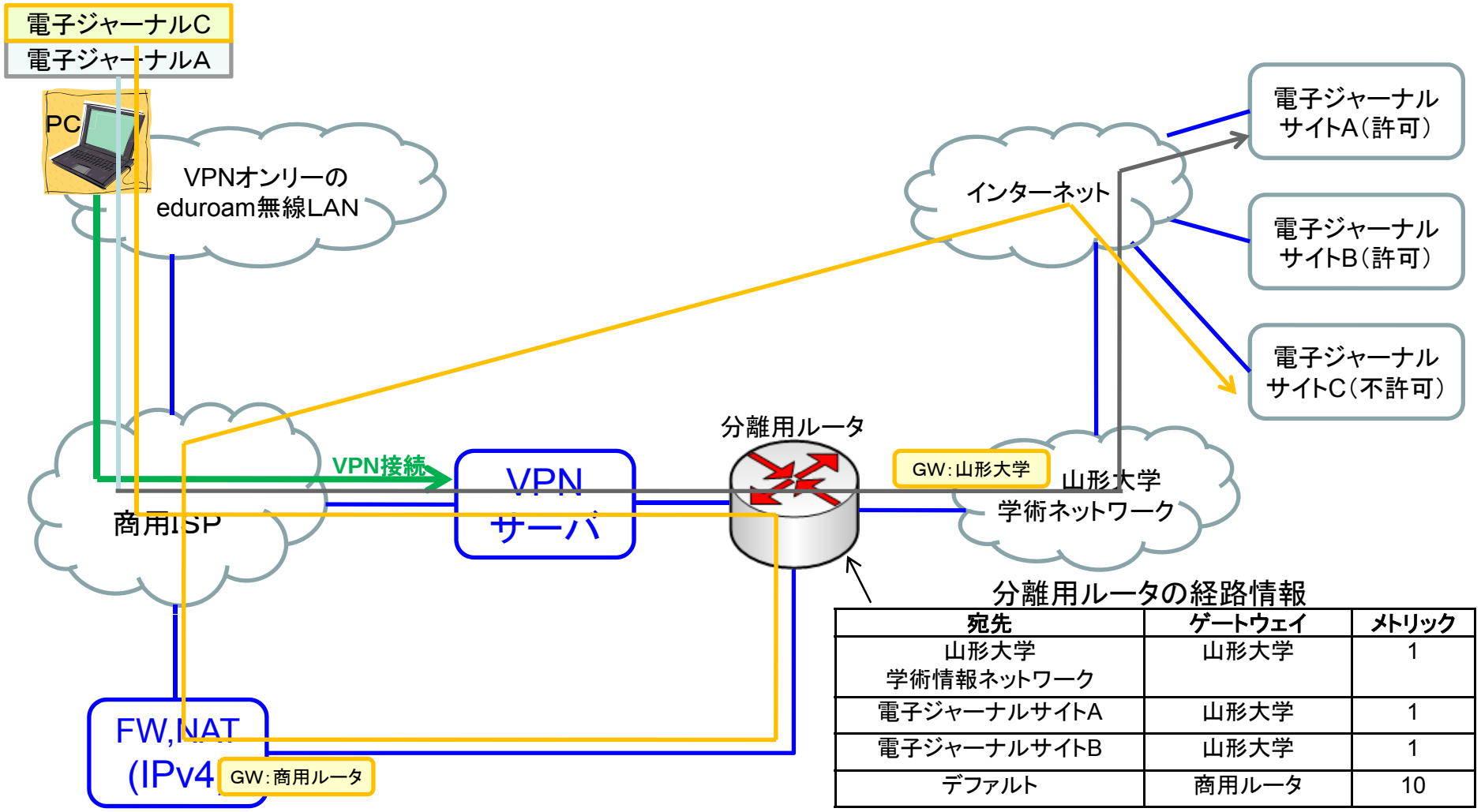
電子ジャーナルなどのVPN経由時の利用調査

- サイエンス・ダイレクト、CSDL、SpringerLink、Oxford Journal、JSTOR、Web of Science、ACM Portal、Science Online、InterScienceのコンテンツ提供サービス会社に、「VPN経由での利用の可否」および「契約の変更の有無」を調査した。

- 回答結果をまとめると、「契約の変更の有無」については、必要な会社はなかった。「VPN経由での利用の可否」については、正規ユーザに限定することなどのセキュリティの確保についての注意はあったが、VPN経由による利用不可といった回答はなかった。

注意：調査したコンテンツ提供サービス会社は、各大学の契約によって回答が異なることがありますので、注意してください。

電子ジャーナル対応VPNサービス



分離用ルータの経路情報

宛先	ゲートウェイ	メトリック
山形大学 学術情報ネットワーク	山形大学	1
電子ジャーナルサイトA	山形大学	1
電子ジャーナルサイトB	山形大学	1
デファルト	商用ルータ	10

分離用ルータに、利用可能な電子ジャーナルの経路を追加することによって、特定の電子ジャーナルのみ、閲覧を可能にできる。問題点としては、電子ジャーナルサイトのIPアドレスが変更なると、経路情報も変更が必要になり、管理コストが大きい。

→ Shibboleth認証などを活用したユーザ認証コンテンツサービスへの移行が必要であろう。

eduroamシステムのまとめ

- Radiusプロキシによって、複数ADの認証情報によって802.1x認証を行い、eduroamが利用できる無線LAN環境を整備可能になった。

- 山形大学のeduroam無線LANの利用者は、山形大学契約の電子ジャーナルは利用できない。山形大学の利用者は、VPNを経由することにより、電子ジャーナルを閲覧できるシステムを構築した。

- 電子ジャーナルについては、セキュリティの確保などの利用条件はあるが、VPN経由による電子ジャーナルの利用は許可されている。今後、実験的にVPN経由による電子ジャーナルの利用を検討し、eduroamの展開を進める。

- 電子ジャーナルは、IP認証には限界がある。Shibboleth認証による電子ジャーナルの閲覧サービスを活用することが必要であろう。

山形大学のまとめ

1. 既存の認証基盤であるADを利用したShibboleth IdPシステムを構築。ADを利用するときは、リフェラルの設定が必要な可能性が高い。

2. 複数認証基盤（AD）を統合して、IdPおよびeduroam用認証基盤として利用可能なシステムを構築。

3. 暫定的ではあるが、ユーザ名のフォーマットは、eduroamフォーマットを採用。（eduroamとの混乱を避けるため）

4. VPNオンリーのeduroam参加機関利用時に、VPNサービスを展開するための情報収集および技術要素が完了した。

5. ADスキーマとedupersonスキーマの違いを考慮して、ADのスキーマの拡張など検討が必要。

6. 外部機関との認証連携時に使用するプライマリキーは、ADのuserprincipalnameをベースに生成する。

本日の課題

- 導入事例の背景
- 学内調整、学内交渉、実証試験ポリシー策定
- 導入事例（システム設計、ポリシーなど）
- ✔山形大学の現状と今後の展開
- 目標 ミニッツペーパーの提出

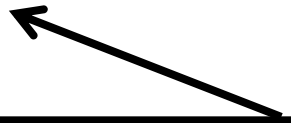
プライマリーキー

― リレーショナルデータベース ―

・複数の表(テーブル)を同じキーワードで接続して、関係付け表現することができるデーターベース。

tblKokyaku

顧客番号	顧客氏名	よみがな	住所	電話番号	生年月日	暗証番号
1	情報太郎	じょうほうたろう	山形県米沢市	0238-2x-xxxx	1975/x/x	xxxx
2	山形花子	やまがたはなこ	山形県米沢市	0238-3x-xxxx	1978/x/x	yyyy



tblKiroku

	顧客番号	日付	金額	コメント	残高
1	1	2007/6/10	10000	新規作成	10000
2	1	2007/6/11	100000	ATM	110000
3	2	2007/6/12	1000	新規作成	1000
4	1	2007/6/12	-5000	電気	105000
5	2	2007/6/14	100000	ATM	101000

一意性（ unique）とは

Shibboleth SPを構築するにも、対象情報から1つのみのレコードをSELECT文で抽出するし、個人情報の特定作業が必要です。どのような情報（フィールド）を設計すればよいか？

・データベースの基本設計が必要

・人を一意にするには？

たとえば、

いとう　ともひろ

を一意にするためには？

問題2

- 人を一意に定義するためには、データベースの表（テーブル）の列の項目をどのように設計するのがよいか？

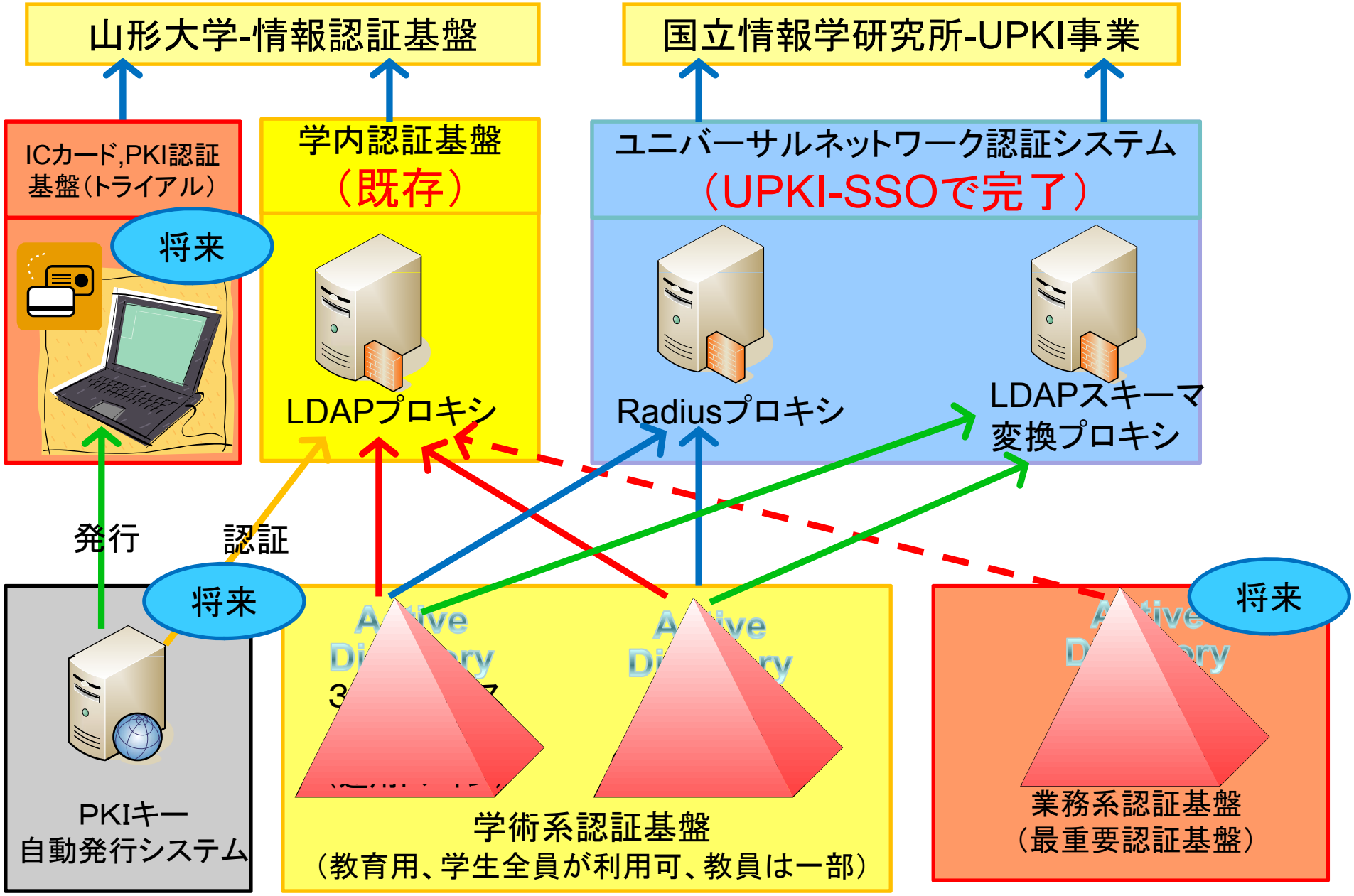
最近の取り組みと重要課題

- プライマリーキー（主キー）を決めよう。
  → EPPN(eduPersonPrincipalName)
  → eduPersonTargetedID

- eduPersonTargetedIDの生成方法の決定
  → StoredIDを推奨（京都産業大学提供）。
または、 ComputedID から徐々にStoredIDに移行（注意：Shibboleth IdP 2.1.2のStoredIDにバグあり。）

- EPPNは現在、検討中。

山形大学のUPKI対応認証基盤の現状と将来構想



現状の協力・連携体制

- 大学全体の理解：　情報担当副学長
- 電子ジャーナル関係：　図書情報企画ユニット
- アカウント管理業務：　学術情報基盤センター
- 研究協力：　山形大学　バーチャル研究所
  データベースアメニティ研究所

謝辞

本実証試験を進めるにあたり、ご指導を賜りました情報担当副学長、学術情報基盤センターセンター長および学術情報基盤センターの皆様に深く感謝申しあげます。また、電子ジャーナルの契約について、調査にご協力いただきました図書情報企画ユニット津田ひろ子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、質問にお答えいただいいてる国立情報学研究所の皆様に深く感謝申し上げます。