

既存の複数認証基盤を統合した UPKI-SSO・eduroam対応認証基盤の構築

山形大学 学術情報基盤センター

伊藤智博、吉田浩司、鈴木勝人、青木和恵

実施内容

- 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
- eduraom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

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。

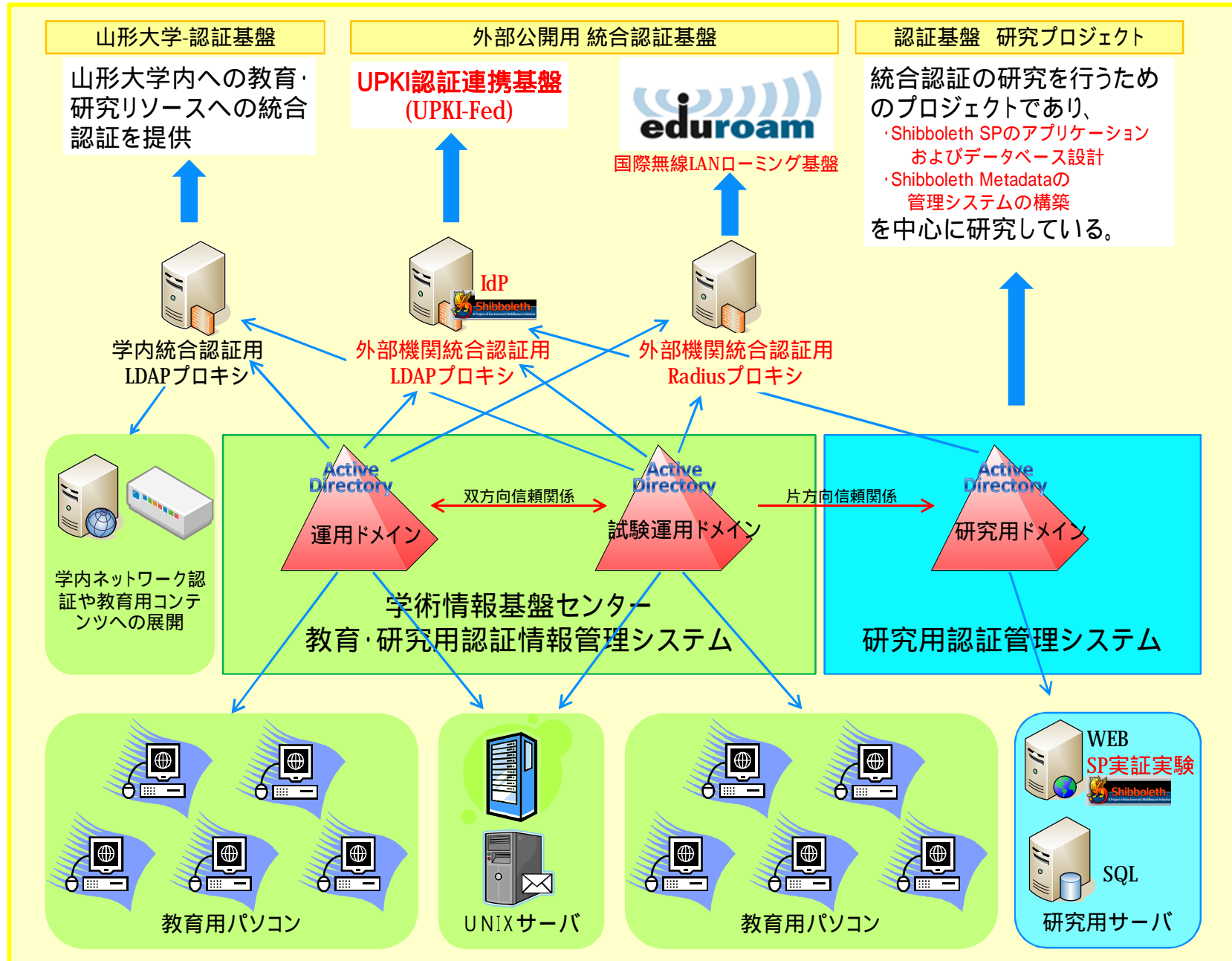
複数ドメインを構成している理由としては、

- ・ **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)。

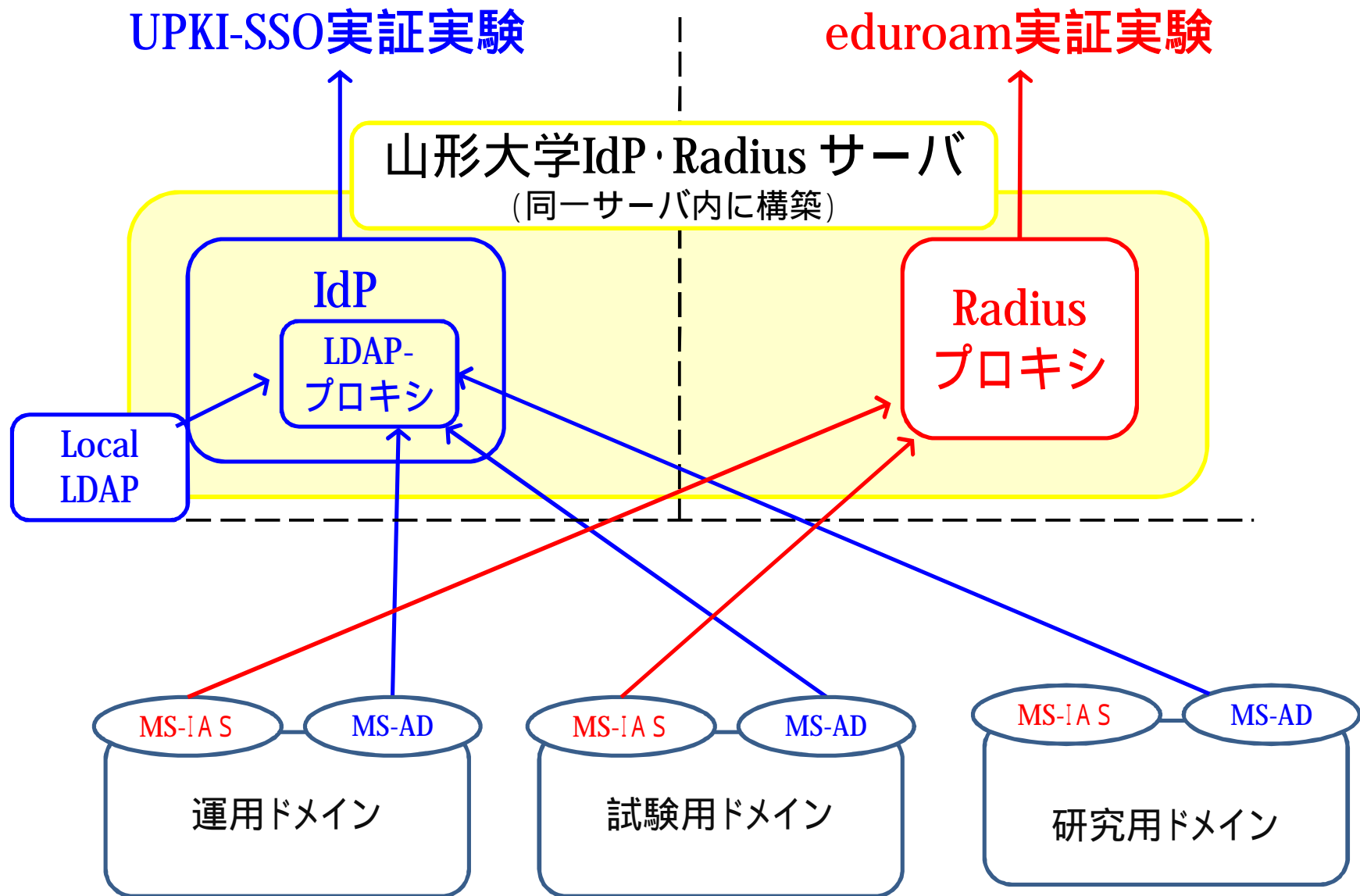
の2点である。

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。

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



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。

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>
```

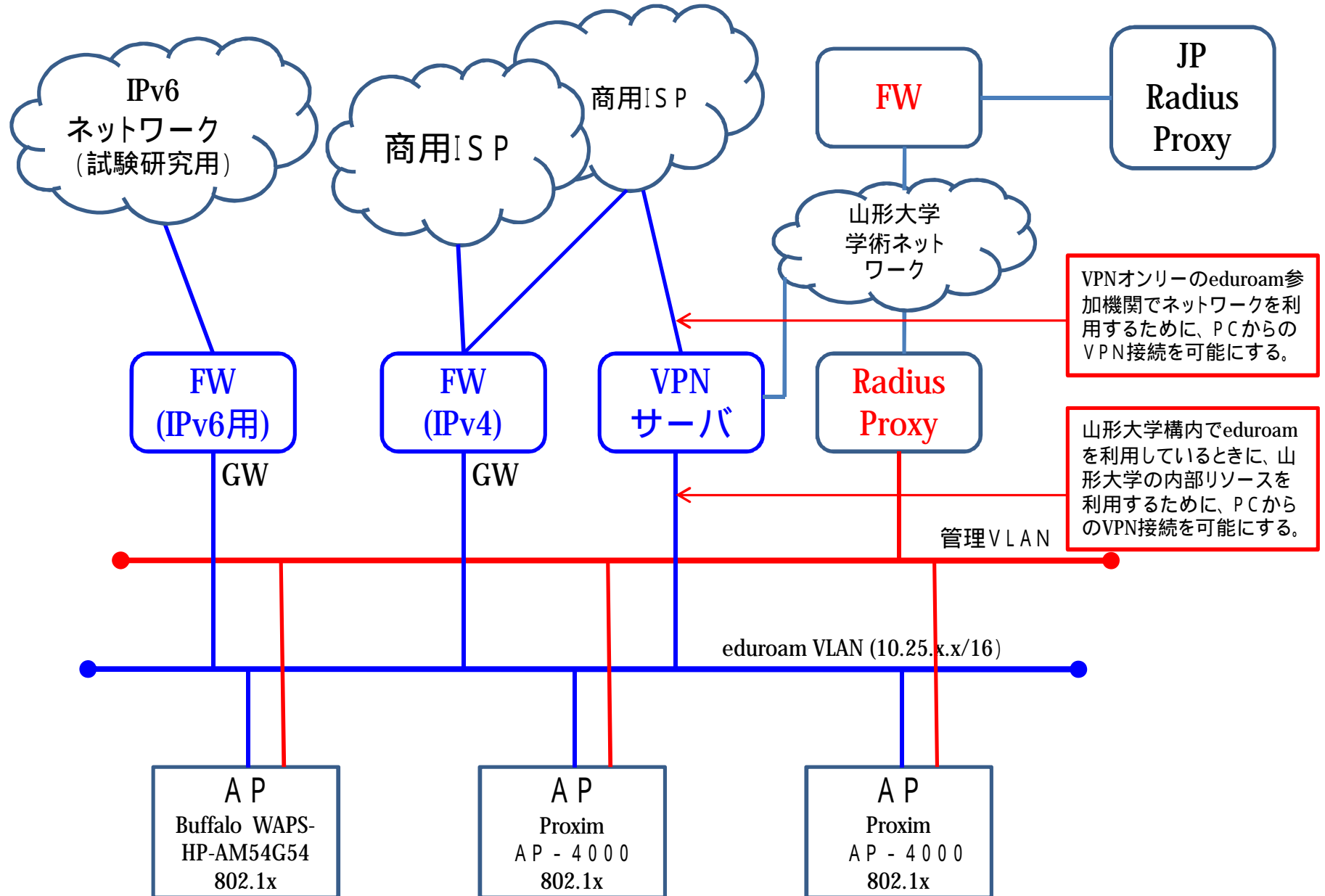
山形大学のIdPのまとめ

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必要がある。
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。

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。

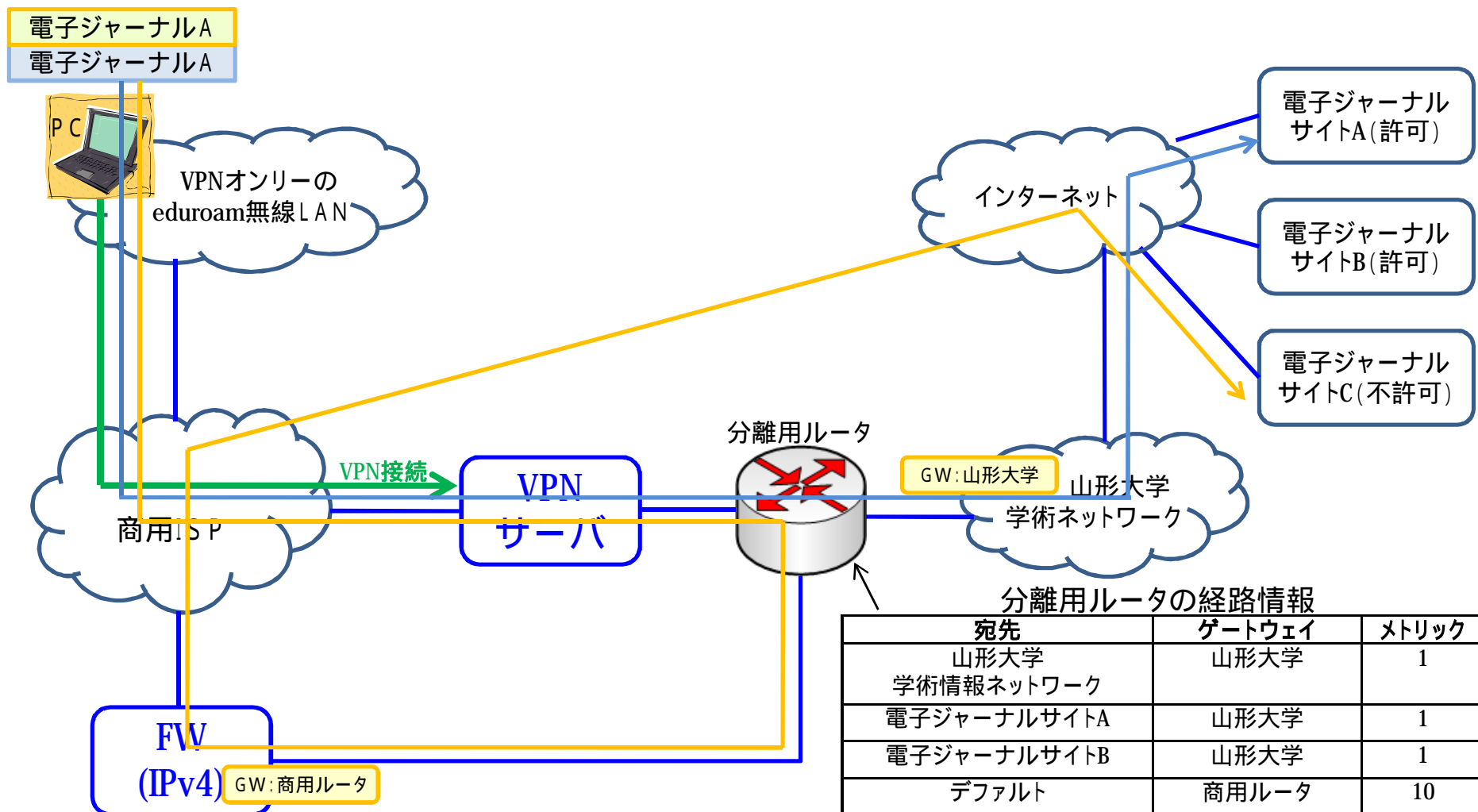
1. コンテンツ提供会社に、VPN経由時の閲覧の可否を確認。
2. VPN経由時に利用可能コンテンツと利用不可能コンテンツを分離するためのシステムの構築。

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、C S D L、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アドレスが変更になると、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。

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に深く感謝申し上げます。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。