D10-1

# 分散配置されたアクティブディレクトリを利用した高可用性認証連携システムの実現

伊藤智博，齊藤純一郎，位多，立花和宏

山形大学大学院　理工学研究科

株式会社ショーワ

tomohiro@yz.yamagata-u.ac.jp

**概要**：山形大学の認証基盤は，複数キャンパスに分散配置されたアクティブディレクトリ（AD)サーバによって構成されており，複数キャンパスの AD サーバ間で同期され，大規模災害時にも対応できるような可用性を有する設計になっている．さらに本学では，この AD サーバの基盤に，学術認証フェデレーション（学認）などの認証連携型シングルサインオンに対応し，学認が提供する様々なサービスプロバイダーを利用できるようにした．本発表では，これまで，本学が AD を基盤に，実現してきた学内外のサービスに向けたシングルサインオンを実現するための技術情報などを説明し，さらに，将来に向けた認証連携による学術教育活動への展望を述べる．

## 1　はじめに

山形大学は，平成 20 年度から実施された UPKI シングルサインオン実証実験に参加し，シボレスや学内認証基盤に関する技術的な問題解決を行ってきた．平成 21 年度からは，UPKI 学術認証フェデレーション（現在の Gakunin; 学認）の運用フェデレーションに参加し，電子ジャーナルを始めとする外部コンテンツの利用を開始した．特に，本学の学内認証基盤は，分散キャンパスであるがゆえに，複数キャンパスに設置された複数の認証基盤によって構成されている．本学では，複数キャンパスに認証サーバを分散配置したことにより，大規模災害が発生した場合の認証情報のディザスタリカバリーを可能にしている[1]．学認に認証情報を提供するためには，一つの Shibboleth IdP サーバから複数の認証基盤を参照することが必要であり，LDAP プロキシ技術によって，複数認証基盤を 1 つに束ね，かつ，属性名を変換することにより解決した．さらに，学内向けに展開している研究用フェデレーションでは，次世代 IP(IPv6)の IdP/SP の実証実験を行っている．

一方，本学では学認へのサービス提供として，「科学技術の学術情報共有のための双方向コミュニケーションサービス」を提供した[2]．さらに，e-サイエンスへの試みの 1 つして，「スマートグリッド実現へ向けたフェデレーションアーキティクチャによる電池劣化管理システム」を開発している[3].

本発表では，本学が学認への参加に至った経緯と現在の運用状況，さらには，本学が AD を基盤に，実現してきた学内外のサービスに向けたシングルサインオンを実現するための認証技術の情報などを説明し，サイバーサイエンスの実現に向けた認証連携による学術教育活動への展望を述べる．

## 2　認証システム

### 2.1 認証システムの概要

山形大学では，センター系認証基盤として，Microsoft Active Directory(AD)を採用している．2007 年以前は，分散キャンパスであるため，キャンパス毎にドメインが分かれている分散管理を採用してきたが，2007 年に実施された教育システム更新のときに，工学部のドメインとそれ以外のドメインの 2 つのドメインに統合した．2 つのドメインにした理由は，工学部では認証やネットワークの次世代試行運用を行っており，運用ポリシーや AD のスキーマの変更が行われるなどの運用方針が異なるためである．すなわち，工学部で利用している試行運用ドメインとそれ以外に部局で利用している運用ドメインの 2 つのドメインが存在する．実際は，試行運用ドメインで試行運用を行う前に，様々なテストをするテストドメインと研究活動をサポートする研究ドメインが存在するため，4 つドメインを連携して様々なシステム構築が行われている．このような複数の認証基盤

を，1 つの認証基盤としてシングルサインオン（SSO）提供できる方法を検討した．具体的には，学認で採用されている Shibboleth IdP に対して認証と属性情報を提供するための LDAP プロキシと eduroam で採用されている Radius 認証を可能にするための Radius プロキシの 2 つを構築した．

### 2.2 2.2. 各認証サーバのスペック

実験において，センターでは Shibboleth IdP を 1 つ，eduroam 用 Radius プロキシを 1 つ構築した．それぞれのサーバのスペックは以下のとおりである．

[VMwre ホストサーバ]
CPU: Intel Xeon MP (2.0 GHz)
メモリ: 8 GB
HDD: 1.7 TB
OS: VMware ESXi 3.5

[IdP 用サーバ]
VMware ホストサーバ上で動作
メモリ：512 MB
HDD: 32 GB
OS: CentOS 5.4
アプリケーション：OpenLDAP 2.3.43, Apache 2.2.x, Apache Tomcat 6.0.20, JDK 6 Update 14, Apache Ant 1.7.1, BerkeleyDB 4.3, OpenSSL 0.9.8p, MySQL 5.1.38, Shibboleth IdP 2.3.x

[eduroam 用 Radius サーバ]
CPU: Intel Celeron CPU 2.6 GHz
メモリ: 512MB
HDD: 40 GB
OS: CentOS 5.2
アプリケーション：OpenSSL 0.9.8p, freeRadius 2.1.6

## 3　認証システムの動作

山形大学の認証システムは, 図 1 に示すように, 複数の AD ドメインから構成されている．学認に認証情報を提供する Shibboleth　IdP では LDAP プロキシを，eduroam に提供する Radius サービスでは Radius プロキシを利用して，複数の認証基盤を活用できるようにしている．

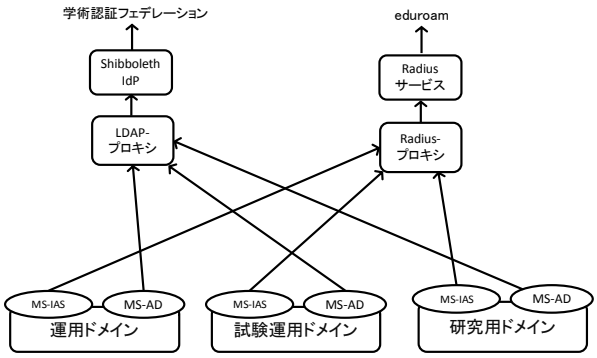
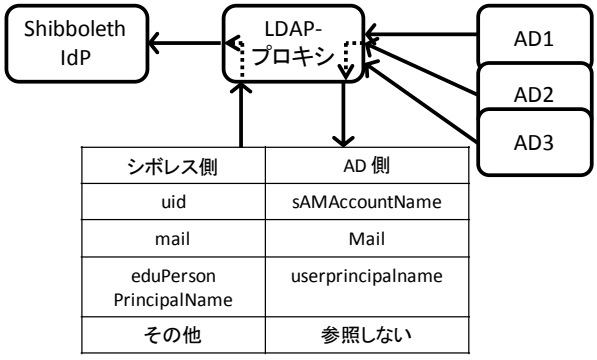



**図 1.　認証システムの概略図**

学認証フェデレーションの認証システムは，利用者が SP に接続した後に，DS にリダイレクトされ，さらに，DS のリストより山形大学の IdP を選択することにより，山形大学の Shibboleth IdP に接続される．Shibboleth IdP の認証画面で，「ユーザ名」と「パスワード」を入力すると，LDAP プロキシを経由し，運用ドメイン，試験運用ドメイン，研究用ドメインの順番に認証要求を行う．認証が許可されると，属性情報を，同様の順番で検索し，Shibboleth IdP が属性情報を取得する．Shibboleth IdP は，SAML アサーションに基づき，認証及び属性情報を SP に送信する．図 2 に示すように，LDAP プロキシでは，rwm-map 機能を利用して，AD のスキーマと OpenLDAP のスキーマの変換とフィルター機能を提供した．この機能により，属性名の変換とセキュリティ機能強化が可能になった．




| シボレス側 | AD 側 |
|---|---|
| uid | sAMAccountName |
| mail | Mail |
| eduPerson PrincipalName | userprincipalname |
| その他 | 参照しない |

**図 2 LDAP プロキによる属性名の変化とセキュリティ機能の概略図**

eduroam では, 無線 LAN の認証方式が 802.1x であるため, Radius サーバが必要である. そこで, Radius プロキシサーバを経由して, 複数ドメインの Microsoft インターネット認証サービスに接続した．無線 LAN に接続するときのユーザ名は，AD の userprincipalname とし, Radius サーバのレルム機能を利用して，自動的に該当ドメインを

選択するようにした.

## 4 まとめ

複数認証基盤を LDAP や Radius プロキシを利用して，Shibboleth IdP システムや eduroam の認証システムを構築することにより，既存の AD の認証基盤に全く修正しなくても可能であることが分かった．個人識別情報である EPPN を生成するための AD の属性を userprincipalname とした．また，EPPN には，スコープ文字列の区切り文字である「@」と AD の userprincipalname に含まれるユーザ名とドメイン名の区切り文字である「@」が存在し，2 つ「@」文字が含むことにより，Shibboleth SP サイトで不具合が発生することが分かった．この解決法として，AD の userprincipalname を機械的に変換することで解決した.

今後，学術認証フェデレーションの特徴の１つである他大学の利用者の身元が保証されていることは，様々な e-サイエンスの情報共有サイトの構築が促進されることであろう．さらに，電子証明技術(PKI)などの普及により，よりセキュリティレベルの高い認証への対応やコンピュータ間通信の認証への対応が可能になり，学術教育活動のシームレスな通信環境整備が進むであろう.

## 参考文献

[1] 伊藤智博,高野勝美,田島靖久,吉田浩司，「災害時に備えた分散キャンパスによる情報基盤の整備」，学術情報処理研究，15, 5-11，2011.
[2] 伊藤智博,立花和宏,奥山澄雄,仁科辰夫,田島靖久,吉田浩司，「学術認証フェデレーションによる科学技術の学術情報共有システム」，学術情報処理研究，14，135-139，2010.
[3] 伊藤智博,立花和宏,仁科辰夫,尾形健明，「1.スマートグリッド実現へ向けたフェデレーションアーキティクチャによる電池劣化管理データベースの構築」，平成 22 年度化学系学協会東北大会講演要旨集, 230 (2010).