HIU-NETにおける利用者認証基盤の構築
学内向け情報システムの利用者認証基盤

中　島　　潤
北海道情報大学

A Development of Authentication Plat-home for HIU-NET

Jun NAKAJIMA
Hokkaido Information University

平成28年11月

北海道情報大学紀要　第28巻　第１号別刷

〈論　文〉

HIU-NETにおける利用者認証基盤の構築

学内向け情報システムの利用者認証基盤

中島　潤 *

Jun Nakajima

A Development of Authentication Plat-home for HIU-NET

要旨

多様なサービスに対応可能な利用者認証基盤を整備することにより，本学の学内ネットワーク（HIU-NET）上で提供される各種情報システムのSSO(Single Sign On)を実現する試みを約２年間に渡り行ってきた。

マルルチベンダにより構成される本学の情報システム環境において，Shibbolethによる SSO 環境の実現と,それを核とする各種サービスを有機的に連携させるネットワークサービス利用認証統合システムを拡張することにより，利用者の利便性の向上，新たなサービスの提供とその管理コストの低減を図った。本稿では，HIU-NETにおける認証基盤の構築について述べる。

Abstract

In order to improve of the convenience of the network user, the offer of new services and reduction of the management cost by expanding use of network service, new user authentication plat-home was reconstructed in HIU-NET.

This paper report new SSO environment by Shibboleth on HIU-NET.

キーワード

認証(Authentication)　ネットワーク(Network)　Web
シングルサイオンオン(Single Sign On)

* 北海道情報大学経営情報学部システム情報学科准教授，Associate Professor, Department of Business and Information Systems (Dept. of BIS), HIU

1. はじめに

北海道情報大学では学内構成員向けに多くの情報システムが構築され提供されている。例えば,実習室に設置されている実習用パソコン群,メールシステムや,学生ポータルサイト,教職員ポータルサイト,教育用LMSであるPoliteなど, 様々な目的毎のコンテンツ・サービスが多数存在している。これらに対して,各利用者が円滑に利用するためには,各システムで必要な利用者情報が効率よく安全に交換される情報基盤整備が重要となる。

特に大学のように開かれた場では,ネットワーク利用時に利用者認証を行い,構成員のみに利用させる必要があり，本学では従来から情報コンセントや無線LANの利用者認証のためにWeb認証機能を備えたLANスイッチを導入してきた。また,各種Webベースの情報システムについては,LDAPを中心として統合認証システムにより,利用者ID/パスワードの共通化が図られている。

本学の多くの情報サービスは,情報センターが管理運用する「統合認証システム」を基礎として構築・運用されてきたが,さまざまな不満や問題,要望が明らかとなってきていた。

利用者の視点では,

・異なるシステムへのアクセス毎に何度も同じID・パスワードの入力が必要とされること。特にiPadのようなソフトキーボードによるパスワード認証が煩わしい,

・リモートアクセスの手段としてサービスをしているSSL VPNでは,端末やOS，ブラウザの組み合わせによって，正常に接続ができないケースがある,

・他大学や学会会場等で,無線LANを利用したい,

・卒業生に対しても,メールアドレスの生涯化など,何らかのサービスを提供したい

システム管理者の視点では,

・学生の入学・卒業等,教職員の採用・退職,さらには非常勤職員,研究員等の異動に伴うアカウントのライフサイクルを実現するための個人情報の流れが複雑化しすぎていたので,これを単純化したい,

・ID・パスワードのみの認証では,セキュリティ管理上の限界が見え始めているので,何らかの多要素認証に対応したシステムとしたい,

・採用を検討していたインターネット上で提供されているGoogle社のGoogle Appsやマイクロソフト社のOffice365等のクラウドサービスにおいて,利用者管理・認証を，管理コストをかけずにいかにして実現するか,

等である。これらの要求を満たすため,数年間に渡り本学学内ネットワーク（HIU-NET）環境におけるSSOの実現,他組織が提供するクラウド型サービスの利用,学外からのリモートアクセスの容易化,無線LANの共同利用について取り組んで来たので報告する。

2. 従来環境における課題

2-1 統合認証システム

本学では,当初は実習室のパソコン群及びメールサーバの認証を目的として，Microsoft社のActive Directoryと標準的なディレクトリサービスを提供するLDAPサーバ間の連携と,これを管理するためのWebシステムから構成される「統合認証システム」を2003年から構築し運用してきた。本学ではこれによって実習室の実習用パソコンと,メールのアカウントを統一することが実現され，また学生ポータルサイト，教

職員ポータルサイト，Polite 等の LMS では,LDAP によりアカウント統合と認証を実現してきた。

さらに,情報コンセントや無線 LAN によるネットワークアクセス,学外からのリモートアクセスのための SSL VPN アクセスサーバの認証のために,統合認証システムと連携した RADIUS サーバを別途構築し運用していた。

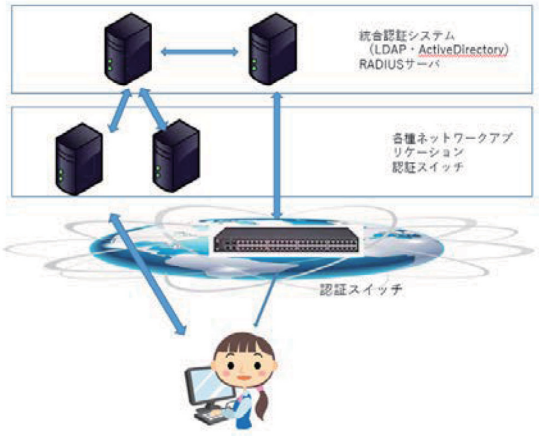

図１ 統合認証システム

2-2 他大学等の動向

国内外問わず,多くの大学・研究機関では本学と同様の不満や要求が存在し,機関毎に様々な方法で解決を図っている[1][2][3]。

特に SSO の実現については,独自システム構築や,既存の商用製品の導入等を行っている事例もあるが,日本国内の多くの大学では,SAML（Security Assertion Markup Language）ベースの OSS による無償の SSO パッケージ製品を導入している機関が多く,OpenAM もしくは,後で述べる Shibboleth を採用している大学・機関が多い。

OpenAM は,Web アプリケーションやクラウドサービスへの SSO を実現するための Java ベースの認証ソフトウェアで,認証,認可,フェデレーション等の機能を備えるオープンソースソフトウェアである。元々商用製品であったことを背景に,高機能で,日本を含む全世界で多くの導入実績があり,大規模な環境での稼動も実証されている。

OpenAM も Shibboleth も,SAML ベースで,OSS・無償という点で共通点がある。OSS の場合,ソースコードが手元にあることを活かし,詳細仕様の確認,仕様に沿った切り分け手順の組み立てと実行など,原因特定に近づくための主体的なアクションを採ることができ,また本学で独自にソフトウェアの修正を行なうことにより，将来的な機能拡張の余地を期待できる。

SAML ベースの ID 連携プラットフォームでは,個々のユーザ認証を行ったのち,そのユーザに関する属性情報に基づいて認可判断を行い,そのサービスを提供する形態をとる。SAML は,Web サービスに関する標準化組織である OASIS によって策定された,認証情報を実現するための XML 仕様であり,Web サイトや Web サービスの間で,ユーザ認証やユーザの属性,認可に関する情報を,SAML で記述されたアサーションの形で交換することで,一度の認証で複数のサービスが利用できるシングルサイオンが実現される。認証情報の交換方法は,SAML プロトコルとしてまとめられており,メッセージの送受信には HTTP もしくは SOAP が使われている。

2-3 学術研究機関における世界的な動向

世界中でオープンな e-learning や e-science プラットフォームが提供されつつあるが,これらのための認証基盤として，世界的な潮流として Shibboleth[4]が用いられている。

Shibboleth は米国 EDUCAUSE・Internet2 で 2000 年に発足したプロジェクトで,SAML, eduPerson 等の標準仕様を利用した認証・認可のための標準仕様策定と

オープンソース提供を行っている。Shibboleth は国立情報学研究所による学術認証フェデレーション（GakuNin）（以下,学認）[5]でも利用され,学術研究分野での標準的なOSSによる認証システムとなっている。認証はSAML標準を用いて行われ,シングルサインオンを提供する際に,ネットワーク構成やホスト名・ドメイン名にも制約はないため,クラウドサービスに対する親和性も高い。

学認へ参加することにより,個人情報の露出機会を大幅に軽減しながら,個人情報の保存場所が各大学等の所属機関内で完結するため，個人情報の外部流出リスクを軽減し,記憶すべきパスワードの数を減らせるなどの効果が期待できる[6]。

3 SSOの実現と認証基盤の検討

一般的にシングルサインオン(SSO)の実現方式として,1. エージェント方式 2. リバースプロキシ方式 3. 代理認証方式 4. フェデレーション がある。

エージェント方式は,Webサーバやアプリケーションサーバーにエージェントソフトウェアを導入し,SSOを実現する方式で,エージェントがブラウザとアプリケーションの通信の間に入り込み,SSOサーバと認証状態を確認することで,SSOを実現する。

リバースプロキシ方式は,ブラウザとWebサーバの間にリバースプロキシサーバを設置し,リバースプロキシサーバにエージェントソフトウェアを導入することで,SSOを実現する。個々のWebサーバー・アプリケーションサーバへのエージェント導入が不要のため,複数のアプリケーションへ展開しやすいメリットがある。

代理認証方式は,対象アプリケーションのログインページに対して,ユーザの代わりにIDとパスワードを送信し,ログインを完了させることで,SSOを実現する方式で,古いアプリケーションや,パッケージソフトウェアを利用している場合,SSOを実現するためのアプリケーション側の修正対応ができない場合があるが,そのようなアプリケーションに対応するための方式として使われている。

フェデレーションは,異なるドメイン間でもパスワード等の情報を渡すことなく,安全に認証されたユーザ情報を連携することでSSOを実現する。フェデレーションのためのプロトコルは標準化が進められており,SAMLやOpenID Connectが使われている。

本学のHIU-NETでは,多数の大学等の学術機関において多数の導入実績がある，エージェント方式で，かつフェデレーションも可能な Shibboleth を用いることとした[7]。OpenAM認証を導入するには,認証サーバではtomcatが必要となり,tomcat利用のためにJavaの稼働環境も必要となる。また,Webサーバとしては,Apache httpdの他,IISサーバ,tomcatでも利用が可能だが,本学の場合は,いわゆるLAMPで構築された情報システムがほとんど全てであり， Linux＋Apache httpd 環境での導入の容易さから Shibboleth を採用することとした。

1． で上げた多くの問題・要求は,シングルサインオンシステムとして Shibboleth を導入することによってほぼすべてが解決され， SSOの認証基盤を統一することで利用者や管理者の負荷軽減を図ることができた。

4 ShibbolethによるSSO環境の構築と既存サービスへの適用と新たなサービスの提供

4-1 Shibboleth SSO環境の構築

前章で述べたように,HIU-NETでは,SSOとして Shibboleth を採用することとし，大学のユーザ情報を利用してログイン環境を構築するために Shibboleth ID Provider(IdP)

を構築し，Shibboleth の認証バックエンドは既存の統合認証システムの LDAP を利用することとした。

既存の Web ベースの各種情報サービスについては,容易に Shibboleth Service Provider(SP)化に対応できるものは対応させ,困難なものについては代理認証やリバースプロキシにより実現する方針でシステム改修を行った。構想は数年前から行ってきたが,実際に改修作業を行ったのは 2015 年 1 月から 3 月にかけてである。

Shibboleth は,米国 Internet2 が主導する学術系の ID 連携基盤のアーキテクチャとそのオープンソースによる実装を創出するプロジェクトである。アーキテクチャおよび,そのソフトウェア実装にも Shibboleth の名称が用いられている。Shibboleth のアーキテクチャは,SAML に基づきそのサブセットとして IdP と SP の間で認証と属性交換,認可が行われる。

一度ログオンすることで認証が継続されるので,対応しているサービスを使った場合,ID とパスワードを再度入力する必要がない。

IdP はディレクトリサービスやデータベースを用いてユーザの情報を保持している。SP から認証リクエストを受け取るとユーザ認証を行い，認証に成功したユーザに対してアサーションを発行し,SP への処理を返す。

SP はリソースを保護し,リソースへアクセスするユーザに認証を行わせるために IdP へと画面をリダイレクト転送する。アサーションを受け取ると,ユーザの属性情報をもとにリソースへアクセスする資格があるかチェックする。

本学の学生向けポータルサイト,教職員向けポータルサイトは,いずれも PHP で記述された OSS の CMS パッケージである XOOPS で構成されており,XOOPS のユーザログインを Shibboleth SSO に対応させるために,XOOPS モジュールとして Shibboleth SP を独自に開発し対応させた。

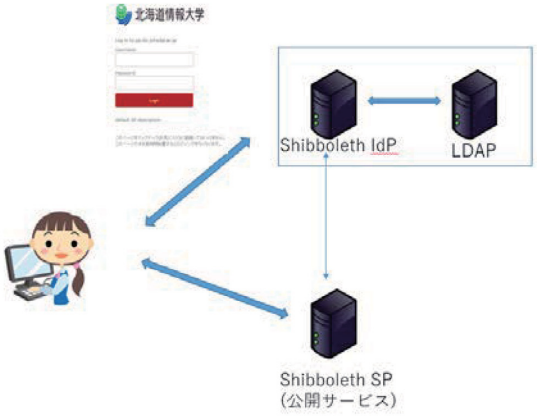

図２ Shibboleth

これにより,SSO を実現すると同時に,ユーザ情報は Shibboleth IdP から提供される属性情報により自動登録させる形態とし，ユーザ管理負荷を軽減せさた。

4-2 Google Apps

Google Apps for Education は,グループウェアとしても使える統合型のオフィスアプリで,学校,大学,認可されている教育機関,資格を満たした非営利団体は無料で利用できる。Google 社が提供するサービスはパソコン,スマホ,タブレットなど端末を選ばないことから，すでに多くの学生が個人として利用していたが,大学として Google Apps for Education の契約を行い,学生は大学のドメイン・個人 ID により電子メール(Gmail)や Google Drive, Google カレンダーなどの各種サービスを 2015 年４月から利用できるようにした。Google Apps for Education へのユーザ登録は,学生の入学時に一括して行い,学内から Google Apps for Education を利用する際の認証は，本学が構築した Shibboleth IdP と認証連携することにより,SSO が出来るようにした。また,学生用の電子メールを Gmail に移行したことに伴い,卒業後も引き続き本学ドメインのメールアドレスを使い続けることができる

ようにした。

4-3 Microsoft Office365

Microsoft Office 365 はマイクロソフト社から提供される商用のソフトウェアおよびクラウドサービスで,デスクトップアプリケーションである Microsoft Office スイートの月額課金版と,サーバ製品である Exchange Server,SharePoint Server,Skype for Business Server 等をマイクロソフトがホスティングして提供されるクラウド サービスをセットにしたものである。本学は以前からマイクロソフト社とボリュームライセンス契約を持っており，このライセンス契約の範囲内で学生に Microsoft Office365 のサービスを提供できた。2016 年 6 月から，このサービスよって学生は Web あるいは,自宅等のパソコンに Office 2016 等のソフトウェアをダウンロードしインストール・利用できるようになった。このためには，Office365 のディレクトリにユーザを登録する必要があったが，管理負荷を軽減するために，Shibboleth から提供される属性情報を元に Microsoft Office365 のディレクトリへユーザを自動登録する SP を開発することで対応した。

4-4 リモートアクセス

本学では,学外から学内の各種リソースにアクセスさせることを目的として,SSL VPN を 8 年間に渡り運用してきた。しかしながら,多様なユーザ端末をサポートする,SSL VPN リモートアクセスサーバ機器の老朽化・更新の必要性を機として,新たなリモートアクセスの仕組みが必要とされた。そこで,Shibboleth 認証を応用したリバースプロキシ型の Web 認証ゲートウェイを独自開発し,運用することとした。

Web 認証ゲートウェイの動作フローを以下に示す。

（1）利用者が自宅などの端末/Web ブラウザにより,学内のネットワークサービスにアクセスする。

（2）学外から学内のネットワークサービスにアクセスした場合,DNS 上，IP アドレスが Web 認証ゲートウェイを指しており,Web 認証ゲートウェイでは,この通信を横取りし未認証端末からのアクセスの場合は,IdP へリダイレクトし,ID パスワードを入力させる。

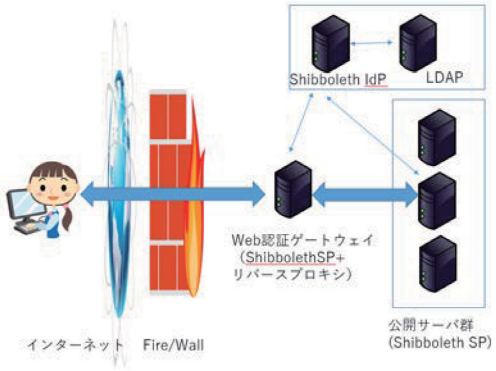

図 3 Web 認証ゲートウェイ

（3）IdP で認証を行い,当該ユーザの権限情報をアサーションとして SP であるリバースプロキシにリダイレクトさせると同時に返す。

（4）Web 認証ゲートウェイでは,IdP から返送されるアサーションを元に権限の確認を行い,お知らせなども表示したポータルの画面を表示させる。

これにより，Web 認証ゲートウェイのポータル画面が表示されている時点で，SSO に対応したサイト間で自由に行き来できるようにした。

開発した Web 認証ゲートウェイは,リバースプロキシと Shibboleth 認証を用いてネットワーク利用者と学内の Web サービスとの間の通信制御を行う構造としている。また,BASIC 認証や FORM 認証に対しての代

行認証機能を実装し,Web サービスの認証連携で属性情報を用いてサービスプロバイダが認可判断を行う場合において,Web 認証ゲートウェイを経由することで,LDAP が提供する個々の属性情報の詳細をサービスプロバイダに対して秘匿すると同時に,サービスプロバイダの認可条件を LDAP に対して秘匿したいという相反する要求に対応するための仕組みを持たせるようにした[8]。

なお，リモートアクセスの手段として，Web 認証ゲートウェイによるものとは別に，L2TP/IPSec 及び SSTP による VPN アクセスも提供しているが，これらの認証は統合認証システムと連携した RADIUS サーバを通じて行っている。

4-5 eduroam

eduroam[9]は,無線 LAN の相互利用（ローミング）を実現する，国立情報学研究所（NII）が提供するサービスである。本学も eduroam のプロジェクトに 2015 年 3 月から参加することとした[10]。eduroam による無線 LAN ローミングは本学だけでなく，他大学や研究機関でも本学が発行する利用者アカウントにより無線 LAN の利用可能である。eduroam は，業界標準である IEEE802.1x 認証に基いており，安全で利便性の高い無線 LAN アクセス環境が機関をまたがって提供される。

本学が eduroam に参加するためには,本学の RADIUS サーバをインターネットに公開し,eduroam の RADIUS サーバと連携させることが必要だったが,本学で運用中の RADIUS サーバと連携関係にある LDAP サーバは,IEEE802.1X 認証の運用が考慮されたものではなかったため,権限や属性の付与に関して別途特別な対応が必要であった。このために,FreeRADIUS を用いて eduroam 用の RADIUS サーバを構築することにより,LDAP サーバとリレーショナルデータベースに記録された利用者の属性情報を組み合わせによって,必要なアクセスポリシを実現できるように対応し，なお本学構成員の eduroam 利用は,セキュリティ上の観点から当面は教職員にのみ公開することとした。

eduroam に参加したことにより,本学で開催された学会等において,来訪者による学内無線 LAN の利用,国内・外の大学,国際会議の会場で,本学発行の利用者アカウントにより eduroam 加入の他機関での無線 LAN の利用ができることを確認している。

5 さいごに

本稿では HIU-NET における Shibboleth を中心とした,新たな利用者認証システムの導入について示し，これを元にした既存の各種 Web 情報システム間での SSO の実現,他機関が提供するクラウドサービスの利用,卒業生への do-johodai.ac.jp の生涯メール化や,より多くの Web ベースのネットワークアプリケーションの提供への対応について示した。

ネットワーク利用におけるセキュリティ確保に関する話題は絶えず,常に新たな課題に対応せざるを得ない。本学としても他大学並みの利用者認証基盤と，それに基づくサービス提供がやっと構築できたところと考えているが,近い将来には多要素認証の導入が必要にせまわれると考えている。このためには,現在運用中の統合認証システムの再構築と,学生・教職員の属性情報等のマスタを管理している，キャンパスシステム間の結合・連携等が必要となってくると考えており,今後のシステム更新のタイミングで改善を図って行きたいと考えている。

また,今後の課題として学認の認証フェデレーションに参加することがる。学術認証フェデレーション学認には,接続試験を中心としたテスト環境であるテストフェデレーションと,実運用を行うための運用フェデレーションがあるが,学認に参加して

Shibboleth IdP や SP を構築する際には,まずテストフェデレーションに参加して動作確認を行った後で,運用フェデレーションへ参加することとなっている。本学はテストフェデレーションには参加しているが,運用フェデレーションに参加するためには,連携に必要な属性情報の付与に関する問題を解決しなければならない等の技術的な課題が残されていることが判明しており,今後の統合認証システムの改修等で対応していく必要がある。

さらには,近年のネットワーク技術のひとつとして，SDN という概念が注目されているが,これはソフトウェアによってネットワーク全体を制御しようという考え方である。その SDN の標準として着目されている技術として OpenFlow があり,OpenFlow を用いることによって,プログラミングによってパケットの制御が可能になる[12]。OpenFlow と Shibboleth の連携によって,より柔軟なネットワーク利用者認証・運用システムが構築可能であるため,これらについても今後検討していく必要があると考えている。

参考文献

[1] 佐藤聡･櫻井孝一･吉田健一･新城靖(2013),高度な利用者認証が利用可能なネットワークを対象とした柔軟なアクセス制御の一実装，情報処理学会論文誌 Vol54,No.3,pp.1099-1。

[2] 岡部寿男・古村隆明・佐藤周行・山地一偵・中村素典(2014),属性情報と認可条件を相互に秘匿する認証連携プロキシ,電子情報通信学会信学技法 IA2013-88,pp.67-71。

[3] 鈴木美幸・岡本康介(2006),認証プロキシによる統合認証基盤の実現,第５回情報科学技術フォーラム,pp.233-234

[4] Shibboleth, https://shibboleth.net/ （2016 年 8 月 31 日アクセス)。

[5] 学術認証フェデレーション GakuNin, https://www.gakunin.jp/（2016 年 8 月 31 日アクセス)。

[6] 西村健・中村素典・山地一禎・大谷誠・岡部寿男・曽根原登（2012）,日本における学術認証フェデレーションとその役割および効果, ,電子情報通信学会信学技法 IA2011-55,pp.5-8。

[7] 伊藤栄典・片岡真・牧瀬ゆかり(2010),Shibboleth 認証基盤構築と学術認証フェデレーションへの参加,九州大学附属図書館研究開発研究室年報, pp.11-15。

[8] 矢野真也・中西透・船曳信芳(2009),プロキシを用いた匿名認証システムの改良と匿名掲示板への応用,電子情報通信学会信学技法 IA2009-46,pp.45-50。

[9] eduroam JP, http://www.eduroam.jp/（2016 年 8 月 31 日アクセス)。

[10] eduroam 基地局マップ, http://monitor.eduroam.org/eduroammap.php?type=jp（2016 年 8 月 31 日アクセス)。

[11] 山下祥平・田中久治・堀良彰・大谷誠・渡辺健次(2013),「OpenFlowShibboleth 認証を用いた利用者認証システムの開発」インターネットと運用技術シンポジム, pp.103-106。