スマートデバイスに対応した本学学内LAN向け ネットワーク認証統合システムの開発

黒田　学　中島　潤
北海道情報大学

Development of the Integrated Network Authentication System Which Supports Smart Device for Campus LAN in Hokkaido Information University

Manabu Kuroda and Jun Nakajima
Hokkaido Information University

平成25年11月

北海道情報大学紀要　第25巻　第１号別刷

〈論　文〉

スマートデバイスに対応した本学学内 LAN 向けネットワーク認証統合システムの開発

黒田　学 *　中島　潤 †

Development of the Integrated Network Authentication System Which Supports Smart Device for Campus LAN in Hokkaido Information University

Manabu Kuroda *　Jun Nakajima †

要旨

本研究では，スマートデバイス等により各種学内 LAN サービスを利用する際のユーザ認証に関わるユーザ操作の煩雑さを，マ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(Single Sign On)と認証スイッチを有機的に連携させるネットワーク認証統合システムを構築することにより低減することを提案した。また本提案を実証するための試験環境を構築し，実現可能性の検証と提案の有効性の確認を行った。

Abstract

In this study, we propose to reduce the complications related to user authentication which is needed when students use various services provided through LAN in Hokkaido Information University with smart device. The means for accomplishing the reduction that we propose is developing the new integrated network authentication system, which links the existing one to Shibboleth SSO (Single sign-on) efficiently in the system environment, which is composed of instruments supplied by multi-vendor. In addition, we verified the feasibility of the new system and affirmed the effectiveness by building an experimental environment and demonstrating the proposal in it.

キーワード

SSO(Single Sign On)　ネットワーク認証　スマートデバイス　学術認証フェデレーション

*北海道情報大学大学院経営情報学研究科, Graduate School of Business Administration and Information Science, Hokkaido Information University
†北海道情報大学経営情報学部, Faculty of Business Administration and Information Science, Hokkaido Information University

1. はじめに

1-1 研究の背景

1-1-1学内LAN利用におけるユーザ認証

多くの大学などにおいて，ポータルサイトやe-ラーニング，Webメール，教務システムなど多種多様のWebサイトが開発され利用されている[1][2][4]。これらのWebサイトは用途毎に独立したシステムとして構築されることが多く，これらを利用する際はWebサイト毎にユーザ認証が必要とされる。ユーザに事前発行されたID／パスワードを用いたユーザ認証の場合，Webサイト毎のユーザ情報管理ではWebサイト毎に個別のID／パスワードを使用しなければならないため，LDAP等を用いユーザ情報を一元管理する統合認証システムの導入が一般的である[1][6]。しかしながら，統合認証システムによりユーザ情報が一元管理されている場合であっても，ユーザが学内Webサイトを渡り歩く度に同一のID／パスワードを何度も入力しなければならず不便である。

また個人のモバイル端末などを接続するために無線LANや情報コンセントの設置が行われており，セキュリティ意識の高まりから，ネットワーク接続を許可するためのネットワークユーザ認証を導入することが多い。この認証ではユーザ端末にインストールされた電子証明書を利用する方式もあるが，多くの大学ではCaptive Portal方式が多く採用されている。Captive Portalは，ネットワークユーザ認証の際にHTTPプロトコルを使用し，端末側は一般的なWebブラウザのみで実現可能であるため，利用者にとって取り扱いやすく，運用もしやすいため多くの大学で採用されている[2][3][4][5]。

上記のような環境下では，Webサイトを利用する場合に，ネットワーク接続のためのユーザ認証とWebサイトのユーザ認証の双方を行う必要がある。ユーザ認証にはタイムアウト時間が設定されており，ユーザ認証を行なってから予め設定された時間経過により認証無効となり，再度ユーザ認証が要求される。複数の学内Webサイトを渡り歩く場合，利用の仕方によっては同一のID／パスワードを何度も入力する場合があり煩雑である。

本学においても，学生及び教職員向けのポータルサイトや，e-ラーニング，Webメールなど多数のWebサイトが学内関係者向けに運用されており，セキュリティ対策の一環として外部からはSSL-VPNを通じてのみしか，これらの学内Webサイトにアクセスできない運用を行っている。認証統合システムによりユーザ情報は統合されているが，ユーザが学内Webサイトを渡り歩く度に同一のID／パスワードを何度も入力しなければならない。また，学内Webサイトを利用するには，まずCaptive Portalによるネットワークユーザ認証を経た後，Webサイトごとにユーザ認証を行う必要がある。また,ネットワークユーザ認証後1時間が経過した場合や，無通信時間が一定限度を超えた場合，認証タイムアウトとなり再度ユーザ認証を要求する運用を行っている。さらに,Webサイト毎に個別のタイムアウト時間が設定されており，学内ネットワーク利用時はしばしばユーザ認証を行わなければならず煩雑となっている。

そして，近年iPadやAndroid端末などのスマートデバイスが普及し，利便性の高さから大学内においてもスマートデバイスを導入した授業が行われたり，個人所有のスマートデバイスを持ち歩いたりする光景がよく見られる。スマートデバイスでは，画面上のソフトウェアキーボードをタッチすることでID／パスワード入力を行うが，通常のキーボードよりも入力が煩雑である。本学のように学内ネットワーク利用時にしばしばユーザ認証を行わなければならない環境において，ソフトウェアキーボードによるユーザ認証はユーザにとって負担となっている。

1-1-2学術認証フェデレーション

個々の大学内におけるユーザ認証に関する課題を前節で述べたが，日本全体に視点を変えると，大学間でのユーザ認証に関する学術認証

フェデレーション（学認）の整備という新たな動きがある。学認は，全国の大学などの学術機関でのSSO（Single Sign On）を実現する認証連携で，学認に参加すれば，例えば自大学で使用しているID／パスワードで他大学の無線LAN を利用可能になったり，自大学が契約しているCiNiiなどの電子ジャーナルサービスを，自宅等を含めた出先から利用することも可能になる。2013年2月現在で国内50以上の大学や研究期間,100以上のSP（Service Provider）が学認に参加しており，既に70万人程のユーザが利用可能となっている[9]。参加には，学認対応の認証連携機能を持ったSSOシステムであるShibbolethを用いた学内SSO環境が必要であるが，大学において一般的に利用される情報システムの多くはShibbolethによるSSOに未対応である[4][10]。そのため，既存のネットワーク構成に対して，ShibbolethによるSSOに対応する仕組みが必要である。

本学においては，ネットワークユーザ認証を行う機器や，学内 Web サイトのほとんどがShibbolethに未対応の現状にある。

1-2　Shibboleth

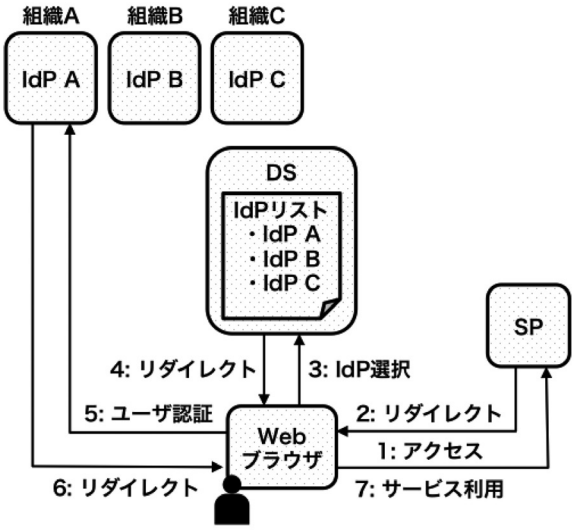
ここで，本研究で提案する本学学内向けSSOシステムの中核となる Shibboleth について述べる。

Shibbolethとは，学術認証フェデレーションにおいても利用されている，SSOを実現するオープンソフトウェアの一つである[11]。

Shibbolethは，LDAPやDBなどを参照することによりユーザを認証し，ユーザの属性情報を送信するIdP（Identify Provider）と，IdPからユーザの属性情報を受信し，それに応じたサービスをユーザに提供する SP（Service Provider），SPに対応する複数のIdPが存在する場合に，IdP のリストをユーザに提供するDS（Discovery Service）から構成される。SPは信頼関係にある複数の IdP とフェデレーションを形成し，他組織の IdP であってもユーザ認証を行うことが可能である。ユーザが SP にアクセスすると，Web ブラウザが SP からDSにリダイレクトされ，そのSPで利用可能なIdPのリストが表示される。DSのリストから選択したIdPでユーザ認証を行うと，初めにアクセスしたSPにリダイレクトされサービスを利用することができる。Shibbolethを用いたSSOの動作を図1-1に示す。IdPとSP間で送受信されるユーザの属性情報はIdPとSPとの信頼関係に基づいて設定できる。IdPによってユーザ認証がなされたユーザは，事前に設定しているSP内の任意のリソースにアクセスできる。Shibboleth認証を必要とするSP内のリソースの設定には，ディレクトリやURLによる指定が可能である。Apache Web Serverでは，Shibboleth 認証機能がモジュールとして提供されているため,設定ファイルにて location ディレクティブや directory ディレクティブによりアクセス権限をコントロールできる。

学認は，国立情報学研究所が主体となり全国の大学などの学術機関による Shibboleth を用いた認証フェデレーションであると言える。

図 1-1 Shibboleth



1-3　研究の目的

前述の背景を踏まえ，本研究の目的を次の3点とした。第1に，本学学内向けの既存 Web サイトやネットワーク構成を維持したまま，ユーザ認証の煩雑さを低減することである。本学学内向けの既存Webサイトやネットワークは，

毎日 24 時間，学内からも，自宅からも SSL-VPN を通じてサービスを行っている。学生が e-ラーニングシステムに完了した課題を夜間にアップロードしたり，教職員が教材作成や，出席数管理などの授業関連業務を行ったり，時間帯を問わず大学における活動に重要な役割を担っており，サービスの可用性が求められている。このようなサービスに対して機能変更を行うには，メンテナンスに起因するダウンタイム発生などのリスクが伴う。このことから，本学の既存 Web サイトやネットワークに対し変更などの手を加えないことが望ましい。また，情報システムにおけるユーザ認証に関わるユーザ操作の煩雑さの低減には SSO の導入が有効であり，SSO の導入はベンダによるトータルパッケージによって可能である。しかし学生ポータルサイトや，教職員ポータルサイト，e-ラーニングシステムは，本学のネットワーク環境や，授業形態に合わせてカスタマイズされ続けてきており，利用者にとっても使い慣れたシステムであるため，既存 Web サイトやネットワーク構成をベンダによる商用のトータルパッケージで置き換えることは困難である。

そして第 2 に，学認参加への条件を満たす学内 SSO システムを構築することである。学認参加により，例えば本学の学生や教職員が学会などで他大学を訪問した際，本学のユーザ ID／パスワードによって他大学の学内無線 LAN に接続しインターネットなどを利用できるようになり，無線 LAN 使用のための事前申請などが不要になることが期待される。本学では学認参加の具体的な計画はまだないが，学認参加大学や SP は全国の国公立大学を中心に徐々に増加している。マ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 を構築するには様々な課題があり，その解決方法を提案することを本研究の目的とする。

また第 3 に，スマートデバイスによる学内ネットワーク利用時のユーザ認証の煩雑さを低減することである。SSO システムを構築しても，従来の ID／パスワードによるユーザ認証は，ソフトウェアキーボードにより文字入力を行うスマートデバイスにとって使用しにくい。本研究では，スマートデバイスを用いて本学向けのネットワーク認証統合システムを利用する際の利便性を高めるスマートデバイス用ネットワーク接続アプリケーションの提案を行う。

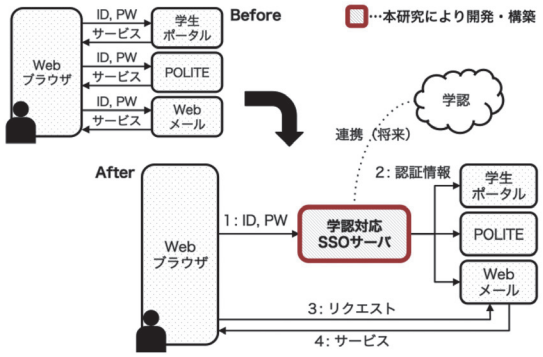
2．　スマートデバイスに対応したネットワーク認証統合システムの提案

本研究では，スマートデバイスなどにより各種学内 LAN サービスを利用する際のユーザ認証に関わるユーザ操作の煩雑さを低減するために，将来的に本学が学認に参加することを想定し，学認対応 SSO サーバである Shibboleth を導入した SSO とネットワークユーザ認証を有機的に連携させるネットワーク認証統合システムの構築をすることを提案する。また，Shibboleth による SSO に対応していない既存の本学学内 Web サイトに対して，Web サイト側に変更を加えることなく Shibboleth に対応させるための認証モジュールの導入を行う。この認証モジュールを組み込んだ Shibboleth SSO システムとネットワーク認証を統合するために，Shibboleth と連携して動作するブリッジインタフェースを用いる。さらに，ID／パスワードの入力が煩雑であるスマートデバイスの利便性を向上させる総合的な SSO システムの開発を提案する。

2-1　SSO システム構築と Shibboleth 対応

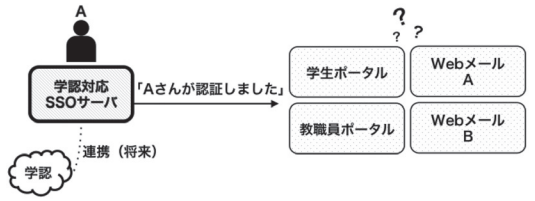
本学の学内 Web サイトやネットワーク機器は多様なベンダのシステムにより構成されているため，SSO の導入が行いづらい。本学の学内 Web サイトやネットワーク機器にそのまま適用可能な SSO システムは今のところ存在しないため，ベンダの垣根を越えた多様なシステムを包括可能な SSO システムの構築が求められる。そして，本学が将来的に学認に参加することになった際，既に Shibboleth が導入されていれば新規導入する場合よりもシームレスに移行可能である（図 2-1）。

図 2-1 Shibboleth による SSO



本学学内 Web サイトの中でも Shibboleth に対応しているのは，Moodle によって構築された e-ラーニング用の POLITE のみである。Moodle には Shibboleth による SSO に対応するプラグインが用意されており，プラグインをインストールし設定するだけで Shibboleth によって認証を行ったユーザを Web サイト内で認証済みのユーザとして扱うことができるが,POLITE 以外の Web サイトは Shibboleth による SSO に対応していない（図 2-2)。

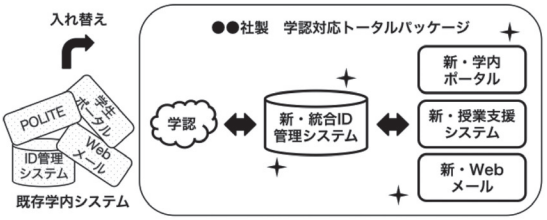
図 2-2 本学学内 Web サイト



Shibboleth を組み込んだ商用のトータルパッケージがベンダから販売されているが，既存の Web サイトやネットワーク構成を変更しなければならず，コスト面からも現実的ではない（図 2-3)。

Shibboleth の導入に際して，このような Shibboleth 非対応 Web サイトの SSO 化を行うために, SSO サーバ用認証モジュールの開発を提案する（図 2-4)。認証モジュールは，通常ユーザが Web ブラウザによって各 Web サイトに対してユーザ認証を行う HTTP 通信を，

図 2-3 学認対応トータルパッケージ

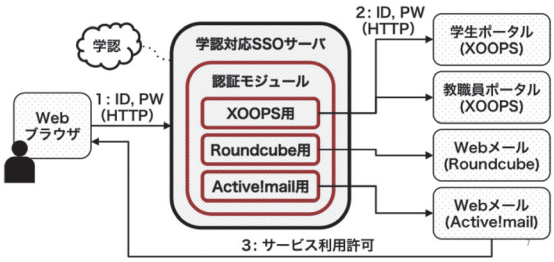


認証モジュールがユーザの代わりに各 Web サイトに対してエミュレートする。ユーザが Web ブラウザを用いて Shibboleth による認証に成功すると，認証モジュールは Web サイトに対してユーザの Web ブラウザによる通信を再現し，ユーザに代わってログインする。Web サイトからサービスを利用するための Cookie を受け取り，ユーザの Web ブラウザに保存させる。ユーザが Web ブラウザを用いて Web サイトにアクセスすると，Web ブラウザに保存されている Cookie が Web ブラウザによって自動的に送信される。そのため，ユーザは Web サイトに対して再びユーザ認証を行わずに，正当なユーザとしてサービスを受けられる。認証モジュールに，Web サイトに対し通常の Web ブラウザによるアクセスとして振る舞わせることで，Web サイトに一切変更を加える必要をなくした。

開発した認証モジュールは本学学内 Web サイトの使用ソフトウェア毎に開発し，XOOPS 用，Roundcube 用，Active!mail 用はそれぞれの Web ソフトウェアのユーザ認証における HTTP 通信をエミュレートする。ユーザが IdP にてユーザ認証に成功すると，SP 内に配置された認証モジュールは認証に用いられた認証情報を取得し，ユーザの代わりに Web サイトに対してユーザ情報を送信しユーザ認証を行う。

このように，マルチベンダ環境である本学学内 Web サイトを，認証モジュールを用いることで Shibboleth による SSO に対応させる。本認証モジュールは汎用性を持たせているため，本学と同じソフトウェアによりサービス提供している他大学でも，Shibboleth を用いた SSO の導入にあたりそのまま利用できる。

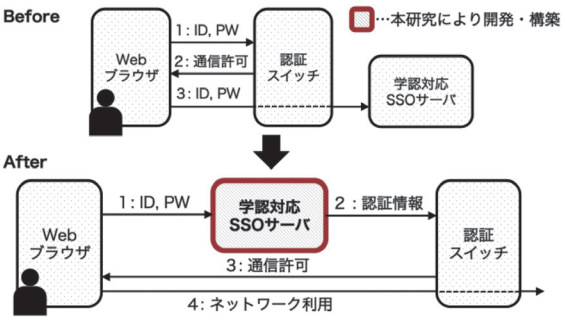
図 2-4 認証モジュール



2-2　ブリッジインタフェース

Shibboleth の導入と，認証モジュールの開発により，Web サイト群が SSO 環境となるが，さらにこの SSO 環境とネットワークユーザ認証を統合するシステムの構築が必要である（図 2-5）。

図 2-5 ブリッジインタフェース

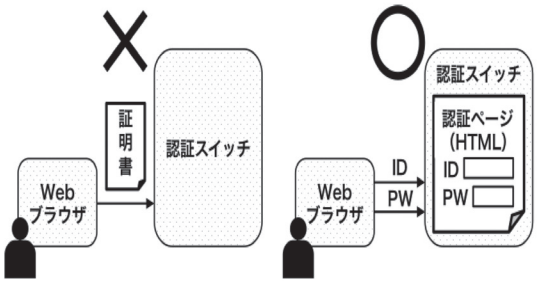


本学でネットワークユーザ認証を行うために採用している認証スイッチ（日立電線製 Apresia）は，Shibboleth 認証に未対応であるが，ハードウェアベースのネットワーク機器であり，ユーザの立場で Shibboleth 認証機能の追加は困難である（図 2-6）。

図 2-6 認証スイッチ

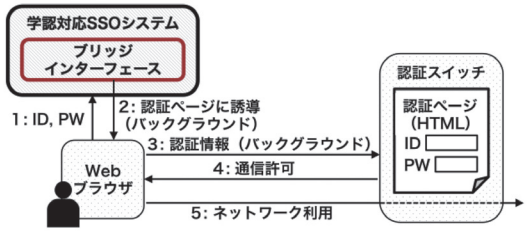
また，ユーザ端末に電子証明書のインストールを必要とする PKI 認証（IEEE802.1x）は，すべてのユーザにとって設定が容易なものではなく，本学内での運用が困難なため PKI 認証は導入しない。（図 2-7）。

図 2-7 ネットワークユーザ認証



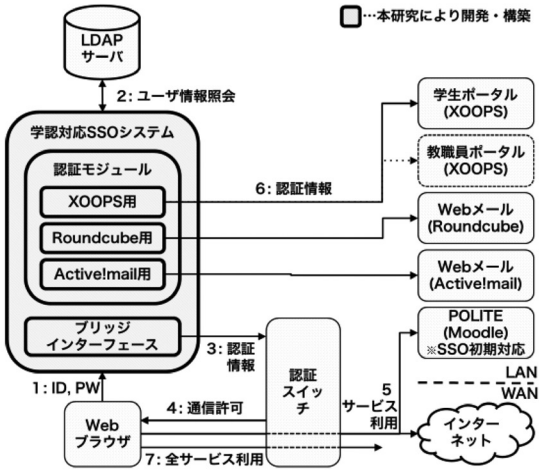
そこで，ユーザが Shibboleth によって認証を行うと，ユーザの Web ブラウザから認証スイッチに，Shibboleth による認証で用いた認証情報が JavaScript によって自動入力された認証スイッチの認証ページを介して送信するブリッジインタフェースを導入する（図 2-8）。これにより，認証スイッチへの設定は代理認証の設定だけで済み，Shibboleth による SSO を用いずにネットワークユーザ認証をする場合は，従来の Capital Portal のよるユーザ認証を利用することができる。本研究では，ネットワーク階層の異なる Web サイトにおけるユーザ認証とネットワークユーザ認証を橋渡しすることから，ブリッジインタフェースという名称を用いた。

図 2-8 ブリッジインタフェース



ユーザが Shibboleth による認証を行った時に認証モジュールとブリッジインタフェースを連動させることで，本学学内 Web サイトと認証スイッチへのログインを一括して行うことが可能となる（図 2-9）。

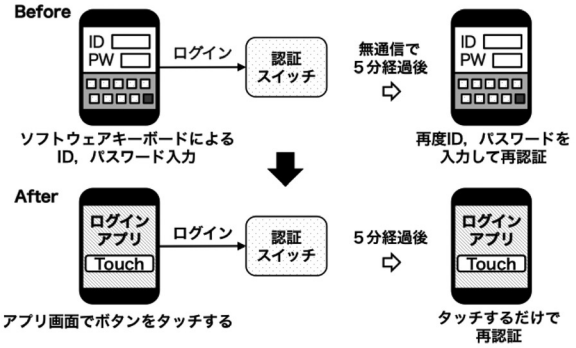
図 2-9 Shibboleth による SSO



2-3　スマートデバイス用ネットワーク接続アプリケーションの開発

スマートデバイスの使用を考慮して総合的にユーザ認証の煩雑さの低減を行うことが本研究の目的であり，本学学内 Web サイト毎のユーザ認証とネットワークユーザ認証を SSO 化し，その SSO 環境とスマートデバイスでのタッチ操作を連動させるシステムが必要であると考えた。そこで，ソフトウェアキーボードでの ID／パスワード入力の代わりにワンタッチ操作で SSO 環境にログインできるシステムを提案する（図 2-10）。

図 2-10 スマートデバイス用ネットワーク接続アプリ



3.　ネットワーク認証統合システムの設計と構築

3-1　Shibboleth

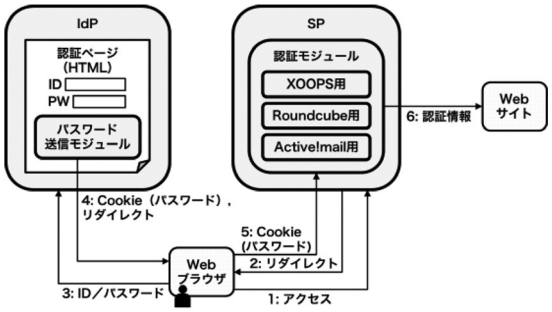
本学学内LANにおけるSSO基盤の中心とするのが Shibboleth IdP および Shibboleth SP である。IdP および SP は Debian 上に試験環境を構築した。本学が将来的に学認に参加した場合，学認の運用する DS を利用することになる。

3-2　本学学内 Web サイトの SSO 化

3-2-1 属性情報の送受信

Shibboleth における認証は IdP によって行われる。Web SSO のためにユーザが IdP にログインした際に認証情報を本学学内 Web サイトに対し送信する認証モジュールを，SP 内に設置した。認証モジュールにアクセスすることにより本学学内 Web サイトに対し SSO ログインが可能となるが，認証モジュールへのアクセスには IdP によるユーザ認証が必要である。ユーザが IdP の認証ページで ID／パスワードを入力後，認証ページに埋め込まれた JavaScript コードにより，入力したパスワードが Web ブラウザの Cookie に保存される。ユーザが SP にアクセスすると，SP 内の認証モジュールは Web ブラウザ内の Cookie に保存されたパスワードを取得する。認証モジュールは，Cookie から取得したパスワードを用いて本学学内 Web サイトに認証情報を送信することで，Shibboleth を用いた本学学内 Web サイトへの SSO を実現している。これは，本学の LDAP サーバがユーザのパスワード属性をセキュリティへの配慮からサーバ外に送信しない運用を行っているためである。Shibboleth と認証モジュールの動作フローを図 3-1 に示す。

図 3-1 認証モジュール



Cookie は送信が許可されているホスト名やドメインの情報を持ち，Web ブラウザで指定したホストやドメインの中のホストにアクセスした場合，Cookie が Web サイトに対して送信される。指定されたホストやドメイン外の Web サイトへのアクセス時には Cookie が送信されることはない。IdP の FQDN を「idp.do-johodai.ac.jp」，SP を「sp.do-johodai.ac.jp」とすると，IdP から SP へのユーザパスワードの送信のための Cookie について，Cookie 発行時のドメインは IdP と SP のホスト名を取り除き，共通のドメインである「do-johodai.ac.jp」を明示的に使用している。これは，明示的に指定しない場合，IdP の FQDN が Cookie のドメインとして指定され，Cookie が SP に送信されないためである。IdP の認証ページは IdP 内の login.jsp ファイルに HTML によって記述されており，ここにパスワードを Cookie として送信する JavaScript のコードを挿入した（図 3-2）。IdP の認証ページを図 3-3 に示す。

ユーザが Shibboleth 認証を済ませ，ユーザの Web ブラウザが SP にリダイレクトされると，認証モジュールのトップページが表示される（図 3-4）。認証モジュールは PHP セッションを生成し，IdP から送信されたユーザの属性情報からユーザ ID と姓名，所属部署，身分情報を取得し，Cookie からパスワードを取得するとセッション変数に格納する。セッション変数への格納が済めば Cookie は削除される。セッション変数に保存する属性情報を表 3-2 に示した。

図 3-4 中のグローバルログアウトのリンクは，本学内のネットワークユーザ認証と学内 Web サイトからログアウトするものである。学認による認証連携によって利用可能となる他機関のサービスからログアウトするものではない。

認証モジュールは Web SSO 実現のためにユーザが持つ ID／パスワードを利用する。Shibboleth による認証を行った際に IdP で入力された ID／パスワードを，IdP から SP に送信されるユーザ属性情報や Cookie を用いて SP 内に設置された認証モジュールに渡している。

図 3-2 login.jsp

```
（認証ページHTML）・・・

<script type="text/javascript">  ←  Cookie送信用
<!--                                  JavaScript

window.onload = function()
{
   document.getElementById("username").focus();
}

function setCookie()
{
   document.cookie =
      "passwd=" + document.getElementById("password").value +
      ";path=/; domain=do-johodai.ac.jp";  ←  IdPおよびSPの
}                                              共通ドメインを指定

// -->

・・・（認証ページHTML）
```

図 3-3 認証ページ

図 3-4 トップページ

3-2-2 認証モジュール

認証モジュールは，本学学内 Web サイトの使用ソフトウェア毎に，Web ブラウザによるユーザ認証時の HTTP 通信をエミュレートするように開発した。HTTP 通信の解析には，Wireshark などを使用し，本学学内 Web サイトにおけるユーザ認証時の Web ブラウザと Web サイト間の通信を，ユーザ端末側で取得し

表 3-1 認証モジュールと本学 Web サイト使用ソフトウェア

関数名	ファイル名	使用 ソフトウェア	Web サイト
xoops	xoops.php	XOOPS	学生ポータルサイト, 教職員ポータルサイト
roundcube	roundcube.php	Roundcube	Web メール①
activemail	activemail.php	Active!mail	Web メール②

表 3-2 ユーザ属性情報

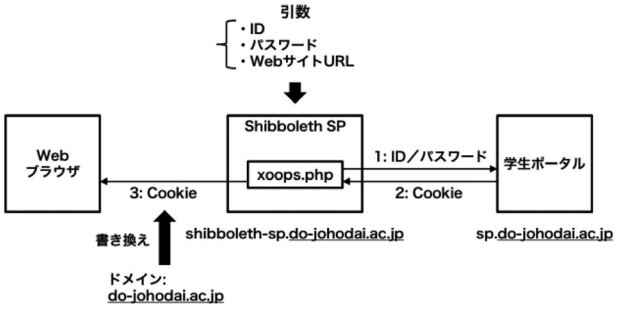
属性名	説明
uid	ユーザ ID
mail	メールアドレス
sn	姓
givenName	名
description	学科／所属部署
ou	身分

た。

各認証モジュールは PHP の関数として実装しており，関数名をファイル名とする PHP ファイルに保存した。認証モジュールと本学学内 Web サイトにおける使用ソフトウェアの関係を表 3-1 に示す。

各関数は，引数にユーザ ID，パスワード，Web サイトの URL などを必要とし，引数で与えられた URL の Web サイトに対し，HTTP によって ID／パスワードを送信する。送信先の URL は，ユーザが Web ブラウザによってユーザ認証時にユーザが ID／パスワードを入力する HTML のフォームの送信先 URL である。送信方法は HTTP の POST メソッドを用いた。引数で与えられた ID／パスワードを用いて Web サイトに対してユーザ認証が成功すると，認証モジュールは Web サイトから Cookie を取得し，ドメインを SP と Web サイトのドメインに書き換えてユーザの Web ブラウザに保存する。本学学生ポータルに対して認証モジュールが ID／パスワードを送信し，Cookie をユーザの Web ブラウザに保存する流れを図 3-5 に示す。

図 3-5 学生ポータルサイト用認証モジュール



1 度ユーザ認証を行った Web サイトは Web ブラウザに Cookie が保存されるため，以降にアクセスするときは，再度 ID／パスワードを Web サイトに送信する必要がない。認証モジュールでは，ユーザが 1 度認証モジュールを用いてユーザ認証を行った Web サイトの情報を PHP セッション変数に保持し，ユーザの 2 度目以降のアクセスでは，認証モジュールは既にユーザの Web ブラウザに Web サイトから発行された Cookie が保存されていると判断して代理認証機能を使用せず，ユーザの Web ブラウザを Web サイトにリダイレクトさせる。

3-3　Shibboleth SSO と ネットワーク認証の統合

認証スイッチはユーザ端末を認証する際，ユーザ端末の MAC アドレスを記憶するため，ユーザ端末上の Web ブラウザから直接認証スイッチに ID／パスワードが送信される必要がある。ブリッジインタフェースは，認証モジュールによってセッション変数に保存された ID／パスワードを，JavaScript によって認証スイッチの認証ページに送信しネットワークユーザ認証を行う。認証スイッチへの ID／パスワード送信の手順を以下に示す。

(1) ユーザが Web ブラウザにより IdP 上の認証ページで Shibboleth による認証を行い，ユーザの Web ブラウザが SP 内の認証モジュール／ブリッジインタフェースにリダイレクトされる。この時，SP 内で PHP セッションが生成され，ユーザの ID／パスワードと属性情報はセッション変数に格納される。

(2) 本学のネットワークユーザ認証は HTTP の Basic 認証によって行われるため，これまでの HTTPS から HTTP による通信に切り替えられる。Web ブラウザをネットワークユーザ認証用の HTML ページにリダイレクトする。

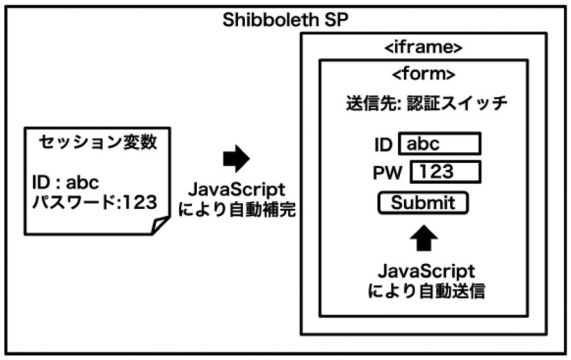
(3) Web ブラウザは，認証スイッチに対し ID／パスワードを送信する HTML のフォームを，非表示のインラインフレームとして読み込む。JavaScript によってセッション変数に格納された ID／パスワードは，フォーム内に補完された後，自動的に送信される（図 3-6）。

(4) ID／パスワードが認証スイッチに送信されネットワークユーザ認証が行われると，認証モジュール上の学内 Web サイトへのリンク集を提供するページにリダイレクトされる。

(3)においてインラインフレームを使用したのは，ID／パスワードが認証スイッチに送信されたあと，認証スイッチの認証成功ページにリダイレクトされることを防ぐためである。

また，ネットワークユーザ認証を行う前に IdP において Shibboleth による認証を行う必要があるため，ネットワークユーザ認証を必要とせずに IdP と SP へアクセス可能とする認証バイパス設定を認証スイッチに対して行う必要がある。

図 3-6 認証スイッチへの ID／パスワード送信



3-4　スマートデバイス用ネットワーク接続アプリケーション

スマートデバイスによって各種学内 LAN サービスを利用する際のユーザ認証におけるユーザ ID／パスワードの入力は，ソフトウェアキーボードにより文字入力を行うスマートデバイスにとって煩雑なユーザ操作である。さらに，本学におけるネットワークユーザ認証は，ユーザがログインしてから無通信時間が 30 分経過すると再認証が行われるため，ユーザにとって大変な負担となる。本研究で提案したネットワーク認証統合システムをスマートデバイスから容易に利用するためには，従来の ID／パスワードによるユーザ認証方法からタッチ操作によるネットワーク認証統合システムへのログインが可能になる仕組みが必要であることを 2 章で提案した。検証のために，スマートデバイス内にユーザの ID／パスワードをあらかじめ記憶しておき，アプリケーション画面上のボタンをタッチ操作により，認証スイッチに対してネットワークユーザ認証を行えるアプリケーションを開発した（図 3-7）。開発環境には，Titanium Studio[12]を使用し，ネットワーク接続アプリケーションを iOS 上で動作

可能とした。アプリケーションの切り替え動作により本アプリケーションが非アクティブになった場合，本アプリケーションをアクティブ化し本アプリケーション上のボタンをタッチする操作は煩雑なため，本アプリケーションをアクティブ化するだけでネットワークユーザ認証が可能な動作をするように実装した。

本アプリケーションのログインボタンをタッチすると，Shibboleth SSO にログインするのではなく，認証スイッチに対して ID／パスワードを送信し，ネットワークユーザ認証を行う仕様とした。これはスマートデバイス内に記憶しているユーザの ID／パスワードを自動送信させる動作は JavaScript ではクロスドメインの制約により不可能だったためである。

図 3-7 認証アプリケーション画面

図 3-8 アクティブ化

また認証モジュールのように,IdP におけるユーザ認証を,サーバ上で Web ブラウザの代わりに行う機能を設け，ブリッジインタフェースのような方法でクロスドメイン制約を回避する方法も検討したが,Shibboleth の仕様上の理由から実現出来ないことが判明したため見送った。IdP では，Web ブラウザによって IdP の認証ページ内の HTML フォームを用いて ID／パスワードを POST した後，IdP から Web ブラウザに暗号化された SAML メッセージが送信され，それを JavaScript によって自動的に送信することによって，ユーザ認証が成功する。これを復号化することにより SAML メッセージが得られるが，これにはパスワード情報が含まれておらず、自動的にパスワードを送信する動作を再現することが困難であった。そこで本アプリケーションでは，スマート端末内に事前に設定しておいた ID／パスワードをワンタッチ操作で認証スイッチへ送信し，ネットワークユーザ認証に伴うユーザ操作を容易にする方法により実現した。

4.　おわりに

本研究では，スマートデバイスなどにより各種学内 LAN サービスを利用する際のユーザ認証に関わるユーザ操作の煩雑さを，マ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 と認証スイッチを有機的に連携させるネットワーク認証統合システムを構築することにより低減することを提案した。また本提案を実証するための試験環境を構築し，実現可能性の検証と提案の有効性の確認を行った。その結果，Shibboleth を本学の情報システム環境に適用させるための認証モジュール，ブリッジインタフェースを導入することで，本学の情報システム構成を維持したまま，ユーザ操作の煩雑さを低減可能であることを確認した。従来は本学学内 LAN を利用するためのネットワークユーザ認証と，学内 Web サイト毎のユーザ認証を行うために同じ ID／パスワードを何度も入力しなければならず，大変不便であった。このようなユーザ操作を 1 度の ID／パスワード入力に集約でき，ユーザ操作の煩雑さを低減することが可能であることを確認した。また，Shibboleth の導入により学認参加への条件を整備するとともに，本学学内の

SSO 基盤の構築を実現した。スマートデバイスにおけるユーザ認証の煩雑な操作に対して，本研究ではSSOとスマートデバイスによるタッチ操作を連動させる，総合的なシステムの提案を行った。学内LANにおけるSSOの実現に関して，他の大学でも組織内の情報システム環境に適応した研究が行われている。本研究で提案したSSOシステムは，Shibbolethを稼働させるためのサーバがあれば構築可能である。本研究で用いた解決方法は，HTTPなどの一般的なプロトコルを使用し，JavaScript，PHPによって実現したので，既存の情報システム環境に依存しない方法を採っている。本研究のアプローチは，他大学において，学認に参加したいが学内システムが Shibboleth に対応していないために，ShibbolethによるSSOを導入できずにいる場合に有効であると考えている。また，ベンダによる商用のトータルパッケージを導入することで，カスタマイズやメンテナンスが行われ続けてきた既存の学内情報システムと置き換えることが現実的に難しい場合においても，本研究による提案が有効であると考えている。

参考文献

[1] 大谷誠, 江藤博文, 渡辺健次, 只木進一, 渡辺義明, シングルサインオンに対応したネットワーク認証システムの開発, 情報処理学会論文誌 51(3), 1031-1039, 2010-03-15, 一般社団法人情報処理学会, 佐賀大学

[2] 飯田勝吉, 野本義弘, ウェブシングルサインオン認証と無線 LAN 認証の連携に関する研究, 電子情報通信学会総合大会講演論文集 2010 年_通信(2), "S-126"-"S-127", 2010-03-02, 一般社団法人電子情報通信学会, 東京工業大学

[3] 藤村喬寿, 学術認証フェデレーションに基づくキャンパスネットワークの認証機構, 情報処理学会研究報告. IOT, [インターネットと運用技術] 2010-IOT-8(37), 1-6, 2010-02-22, 一般社団法人情報処理学会, 広島大学

[4] 藤村喬寿, 西村浩二, 相原玲二, 大規模キャンパスネットワークにおけるSSO認証の設計と実装, 電子情報通信学会技術研究報告. IA, インターネットアーキテクチャ 109(299), 13-18, 2009-11-18, 一般社団法人電子情報通信学会, 広島大学

[5] 相原玲二, 西村浩二, 岸場清悟, 田島浩一, 近堂 徹, 利用者認証機能を持つ大規模キャンパスネットワークの構築, 電子情報通信学会総合大会講演論文集 2008 年_通信(2), "S-116"-"S-117", 2008-03-05, 一般社団法人電子情報通信学会, 広島大学

[6] 白濱成希, 認証サーバを基盤とした教育・研究用ネットワークシステムの構築について, 北九州工業高等専門学校研究報告 45, 43-46, 2012-01, 北九州工業高等専門学校

[7] 新里卓史, 飯田勝吉, 岸本幸一, 太刀川博之, 昆野長典, 山崎孝治, 伊東利哉, 渡辺治, 大学内の業務・システムと連携するキャンパス共通認証認可システムの構築と運用, 電子情報通信学会技術研究報告. NS, ネットワークシステム 106(577), 201-206, 2007-03-01, 一般社団法人電子情報通信学会, 東京工業大学

[8] 梶田将司, 内藤久資, 小尻智子, 平野靖, 間瀬健二, CAS によるセキュアな全学認証基盤の構築, 情報処理学会研究報告. DSM, [分散システム/インターネット運用技術] 2005(39), 35-40, 2005-05-12, 一般社団法人情報処理学会, 名古屋大学

[9] IdP, SP一覧, http://www.gakunin.jp/docs/fed/participants

[10] 学認対応学内システム情報, https://meatwiki.nii.ac.jp/confluence/pages/viewpage.action?pageId=8717006

[11] Shibboleth 公式Webサイト http://shibboleth.net

[12] Titanium Studio 公式Webサイト http://www.appcelerator.com/titanium/titanium-studio