2009-IOT-4 (45)
2009 / 3 / 6

Opengate とシングルサインオン

江藤 博文† 大谷 誠† 渡辺 健次†† 只木 進一†

† 佐賀大学大学総合情報基盤センター 〒840–8502 佐賀県佐賀市本庄町 1
†† 佐賀大学理工学部 〒840–8502 佐賀県佐賀市本庄町 1
E-mail: †{etoh,otani,tadaki}@cc.saga-u.ac.jp, ††watanabe@is.saga-u.ac.jp

あらまし 学内の複数の情報システムの連携とそれらのポータルサイトの構築が必要とされており、その基礎技術としてシングルサインオン導入が必要である。こうしたポータルサイトの入り口の一つとして、ネットワーク利用者認証として佐賀大学で開発している Opengate を活用することを検討する。これにより、学生がネットワーク接続すると、学生用ポータルサイトに導くことが可能となる。Opengate をシングルサインオンの入り口とするための、課題と現状について報告する。

キーワード ポータルサイト, シングルサインオン，Opengate，利用者認証

Single Sign-On with Opengate

Hirofumi ETO†, Makoto OTANI†, Kenzi WATANABE††, and Shin-ichi TADAKI†

† Computer and Network Center, Saga University 1 Honjo-machi, Saga-city, Saga, 840-8502 Japan
†† Faculty of Science and Engineering, Saga University 1 Honjo-machi, Saga-city, Saga, 840-8502 Japan
E-mail: †{etoh,otani,tadaki}@cc.saga-u.ac.jp, ††watanabe@is.saga-u.ac.jp

Abstract Information systems in a university need inter-cooperation mechanisms and their portal sites. This requires single-sign-on infrastructure. We examine to use Opengate, which was developed as a network user authentication system in Saga University, as one of entrances for such portal sites. With this method, a student, who connects his terminal to a network, is lead to portal sites for students. The current status of the development and its problems are reported.

Key words Portal Site, Single Sign-On ,Opengate ,User Authentication

1. はじめに

学内には複数の情報システムが存在している。統合認証システム [1], [2] は、そうしたシステムの利用者認証の共通化を図る基盤である。利用者認証の共通化だけでは、利用者は用途ごとにそれぞれの情報システムにアクセスしなければならない。このため、情報システムを大学ポータル [3] としてまとめることも行われている。しかし、大学ポータルとしてまとめても、各情報システムを使用する度に利用者の認証が行われては、利用者にとっては不便である。そのため、各情報システムを大学ポータルとしてまとめ、1 回の利用者認証で各情報システムにログインすることが可能なシングルサインオンの導入が必要である。

我々は、こうしたポータルへの入り口の一つとして佐賀大学で開発したネットワーク利用者認証システム Opengate [4] を検討している。佐賀大学では Opengate は全学的に整備されており、多くの学生や教職員が学内ネットワークを利用するための最初の認証として利用されている。そこで、ネットワークの利用と同時に大学ポータルにシングルサインオンできれば、情報システムごとにログインするという手間が省け、多くの利用者の利便性の向上が期待できる。

ネットワーク利用開始と同時に大学ポータルに利用者を導くことで、大学ポータルに管理者や大学からの広報、連絡事項、予定などを表示し、利用者への情報の伝達をスムーズに行うことが可能である。このような情報はメールによる連絡が一般的であるが、必要な情報がトップページに表示されるので、必要な情報のメールを取捨選択して読む作業が必要が無くなる。利用者をポータルに確実に導くことは、組織の情報伝達にとって非常に有効な方法である。

本稿では、Opengate のシングルサインオンの入り口とするための課題と現状について報告する。

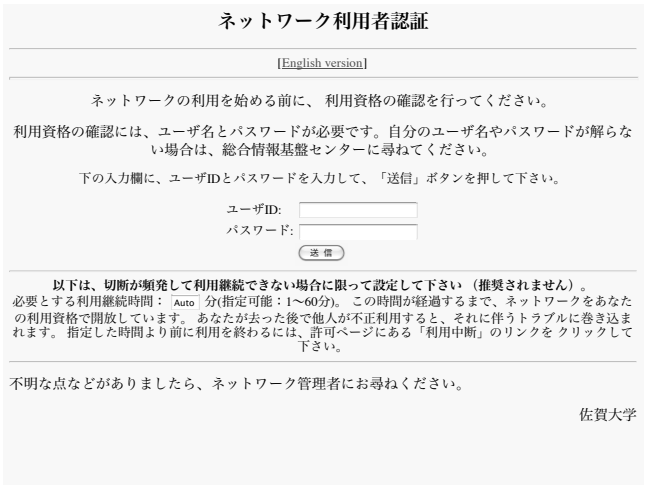

図 1　Opengate の認証ページ

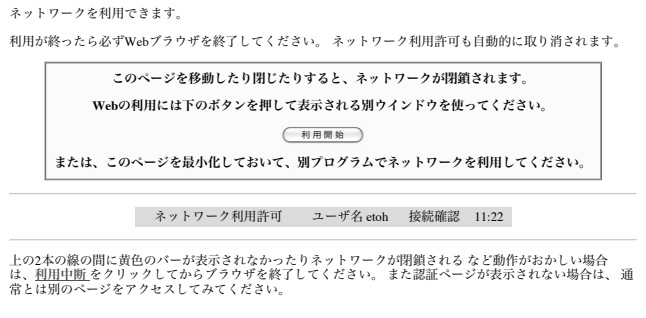

図 2　ログイン状況ページ

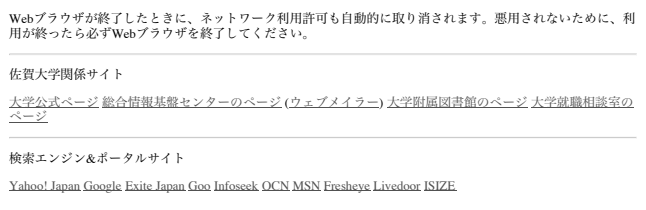

図 3　利用案内のページ

2. 背　　景

2.1 Opengate の概要

佐賀大学では 2000 年より、ネットワーク利用者認証システムとして Opengate の開発・改良し、全学規模で運用を行ってきた。Opengate は利用者がブラウザを起動し、任意のページにアクセスする通信を横取りして、認証ページを表示する。Opengate の認証ページを図 1 に示す。

認証ページからログインすることでファイアウォールが開き、ネットワークの利用が可能となる。認証後は、ログインの状況を表示するとともに、同時に利用案内のページが表示される。ログイン状況のページを図 2 に、利用案内のページを図 3 に示す。

Opengate は、ブラウザ終了をネットワーク利用終了ととらえて、ファイアウォールを閉鎖する。Opengate では、認証で得られた利用者の情報、端末情報、利用開始・終了時刻を記録する。佐賀大学では、現在は学内のほぼ全ての教室の情報コンセントおよび無線 LAN で Opengate の使用が可能となっている。会議室や研究室にもサービスを提供し、学生だけではなく教員も利用している。

Opengate の利用者認証は POP3、IMAP、LDAP、FTP、Radius などの外部の認証システムを使用することができる。佐賀大学の Opengate では、利用者認証として総合情報基盤センター (以下、センターという) の統合認証システムを使用している。統合認証システムは 2003 年に導入され、Opengate を含む学内の情報システムに認証情報を提供している。各情報システムがセンターのユーザ名とパスワードで利用者認証を行うことを可能としたことで、統合認証システムは学内の認証基盤情報として位置づけられている。

2.2 ネットワーク利用者認証システムのシングルサインオン対応

持ち込み端末を学内ネットワークに接続し、大学ポータルを利用することを考える。学生はネットワーク利用者認証システムにより認証を行い、大学ポータルで再度認証を行うことで学内の情報システムを利用することとなる。同様の利用者認証を二度行っており、利用者にとっては不便である。

ネットワーク利用者認証システムがシングルサインオンに対応し、大学ポータルへのログインも同時に行うことが可能となれば、利便性が大幅に向上する。新入生に対する導入教育では、学生生活に必要な情報の所在を指導する必要が無く、ネットワーク利用者認証の使用方法だけを指導すれば良い。入学時の指導のコストが削減され、利用者にとっても容易に情報の取得が可能となる。

前述のように、Opengate では、認証後に利用案内のページを表示する。この利用案内のページが、大学ポータルサイトであれば、利用者の利便性が増すだけでなく、利用者を確実にポータルに導き、大学からの情報提供がスムーズになる。

3. UPKI 情報基盤によるシングルサインオン実証実験

3.1 概　　要

国立情報学研究所 (以下、NII という) は UPKI(全国大学共同電子認証基盤) 構築事業において 2008 年度に UPKI 情報基盤によるシングルサインオン実証実験 [5] を実施している。この実験は、シングルサインオンによる電子ジャーナルの利用や、大学間の認証連携を行うことを目的としたものである。我々はこの実験に参加し、シングルサインオンの運用と活用について検討を行っている。

この実証実験では、Internet2 の MACE (Middleware Architecture Committee for Education) プロジェクトで開発された SAML ベースの Shibboleth [6] を使用している。Shibboleth は、利用者の認証と利用者の属性を提供するアイデンティティプロバイダ (Identity Provider、以下、IdP という)、IdP からの情報によりサービスを提供するサービスプロバイダ (Service

表 1　Shibboleth の構成

アイデンティティプロバイダ (IdP)	認証及び属性の提供
サービスプロバイダ (SP)	IdP の情報によりサービスを提供
IdP ディスカバリーサービス (DS)	IdP のリストを提供
メタデータ	信頼する認証局の証明書、IdP、SP の情報

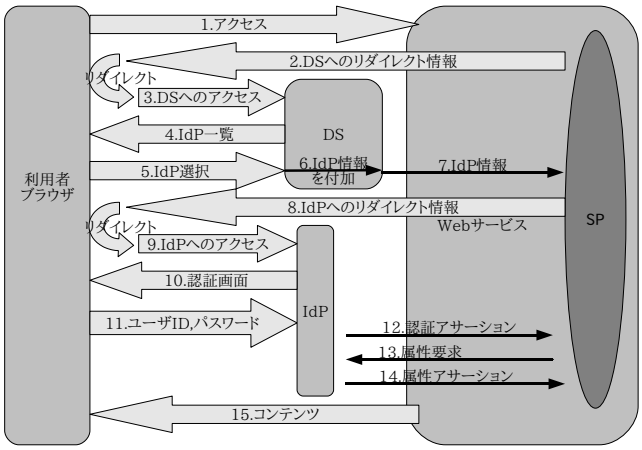

図 4　Shibboleth の処理の流れ

Provider、以下、SP という)、SP に IdP のリストを提供する IdP ディスカバリーサービス (Discovery Service、以下、DS と言う)、相互の信頼のため信頼する認証局の証明書や IdP、SP の情報を持つメタデータで構成される。Shibboleth の構成を表 1 に示す。

実証実験で使用するサーバ証明書は、サーバ証明書発行・導入における啓発・評価研究プロジェクト [7] を使用する。

Shibboleth の処理の流れを図 4 に示す。利用者は初めに SP 上に構築されたウェブサービスにアクセスする。リクエストは SP から DS にリダイレクトされ、利用者はそこで認証可能な IdP を選択する。選択された IdP の情報がリダイレクトで SP に返され、IdP にリダイレクトされ、IdP での認証画面が表示される。

IdP での認証に成功すると、SP に認証アサーション (Assertion) が送られる。SP は IdP にアプリケーション実行に必要な利用者の属性を要求し、IdP は属性アサーションを返す。この属性に基づき SP 上のウェブサービスからコンテンツが送信される。

実証実験では、各大学に IdP の構築が必須であり、必要な場合に SP を構築する、DS は NII で準備される。各大学は IdP 及び SP のメタデータを作成し、NII に送付する。NII は各大学から送付された IdP と SP のメタデータを DS に登録するとともに、共有メタデータとしてとりまとめ、リポジトリに登録する。各大学は、リポジトリから共有メタデータを取得し、IdP 及び SP に登録する。実証実験参加大学の IdP、SP のメタデータを登録した NII の DS で、大学間の認証連携の実証実験が行われる。

図 5　佐賀大学 IdP の認証画面

3.2　佐賀大学での取り組み状況

3.2.1　IdP の構築

IdP は、HTTPS プロトコルを通じて SP から認証要求を受け取り、認証画面を表示し、認証後に認証結果と属性を SP に戻す。

Shibboleth の IdP は servlet として配布されている。このため、IdP を構築する際の基本要素は、HTTP リスナーの Apache、Java Servlet コンテナの Tomcat、及び Shibboleth である。IdP を構築するにあたり、Apache の SSL 対応のため、サーバ証明書を取得するが、このサーバ証明書は IdP のメタデータの作成でも使用する。作成したメタデータを NII に送付し、NII から共有メタデータを取得する。お互いのメタデータが揃うことで、認証の信頼関係が確立される。IdP による認証結果は、ブラウザの Cookie に保存される。

IdP が使用する認証情報は LDAP により提供する。実証実験では、LDAP 中に eduperson スキーマが必須となっている。

構築した認証連携確認のために Plone サイト [8] を含むいくつかのサイトが NII に用意されている。これらのサイトに佐賀大学の IdP の利用者認証でログインが可能なこと、サイト間でのシングルサインオンが可能なことで、IdP の動作確認と NII との認証連携が行われていることを確認した。佐賀大学 IdP の認証画面を図 5 に示す。

IdP が LDAP 中のどの属性を送信するのかは、IdP のポリシ及び設定による。SP がどの属性を要求するかについても、SP のポリシ及び設定に依存する。通常 LDAP は組織内の利用者認証を前提にしているため、情報セキュリティ上、外部に出すことが適切でない情報も有している。このため、SP との認証連携において、お互いのポリシに応じて必要な情報を取り決める必要がある。

3.2.2　SP の構築

SP は、ブラウザの Cookie を確認し、すでに認証されているか否かを判断する。認証されていなければ、IdP にリダイレクトし認証要求する。すでに認証されていれば、必要な情報を IdP から取得する。利用者情報は HTTP ヘッダや環境変数として Web アプケーションに渡される。

Shibboleth の SP は C++で書かれたモジュールであるが、

プラットフォームごとにバイナリも配布されている。SP を構築する際の基本要素は、HTTP リスナーの Apache と Shibboleth である。SP でも Apache の SSL 対応のため、サーバ証明書を取得するが、このサーバ証明書は IdP と同様に SP のメタデータの作成でも使用する。作成したメタデータを NII に送付し、NII から共有メタデータを取得する。お互いのメタデータが揃うことで、認証の信頼関係が確立される。

IdP との接続確認のため、IdP と SP 間でメタデータの相互交換を行い、IdP の認証で SP へのログイン可能なことを確認した。

NII の認証連携確認のため、佐賀大学 SP 上に構築した Plone に NII の DS を登録した。ログイン時に DS を選択すると、NII の DS に接続し、IdP の一覧が表示される。これにより、佐賀大学の SP が NII の DS に登録されている事を確認した。また、NII の DS で佐賀大学以外の IdP を選択し、ログイン画面が表示される事で、他大学との IdP と認証連携が行われていることも確認した。

3.2.3 DS の構築

DS は認証連携のポリシを定めており、NII の DS は大学認証連携のポリシーで構築されている。大学内でシングルサインオン環境を構築するためには、大学内の独自の認証連携のポリシが必要となり、独自の DS の構築が必要となる。また、IdP や SP は、DS にメタデータを登録する事で連携が可能であるため、NII の DS 以外に複数の DS が存在しても問題は無い。

DS は、HTTPS プロトコルを通じて SP に IdP の一覧を表示し、選択された IdP へリダイレクトを行う。

Shibboleth の DS は servlet として配布されている。DS を構築する際の基本要素は、HTTP リスナーの Apache、Java Servlet コンテナの Tomcat、及び Shibboleth である。DS に IdP と SP のメタデータを登録すると、DS は登録されたメタデータから IdP の一覧を作成し、登録された SP からの接続を許可する。

動作確認のため、佐賀大学の IdP 及び SP のメタデータと NII の共有メタデータを佐賀大学 DS に登録する。次に、佐賀大学 SP 上の Plone に佐賀大学 DS を登録する。Plone でログインから佐賀大学 DS に移ると、NII のグループと佐賀大学のグループの一覧が表示される。各大学の IdP を選択し、ログイン画面が表示される事で、DS の動作を確認した。佐賀大学 DS の IdP 選択画面を図 6 に示す。

4. Opengate のシングルサインオン対応

4.1 Shibboleth 対応 Opengate の処理の流れ

Shibboleth 対応 Opengate の処理の流れを図 7 に示す。利用者が初めに任意のページにアクセスしようとすると、Opengate が横取りし、SP 上に構築された Opengate のページにアクセスする。以降、IdP から属性アサーションが返ってくるところまでは Shibboleth の流れ (図 4) と同じである。その後、Opengate は端末へのネットワークを開放し、ログイン状況とシングルサインオンした大学ポータルの画面を送信する。

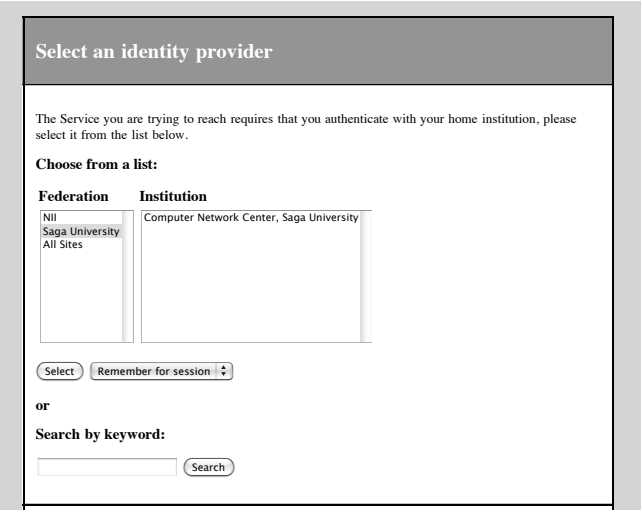

図 6　佐賀大学 DS IdP 選択画面

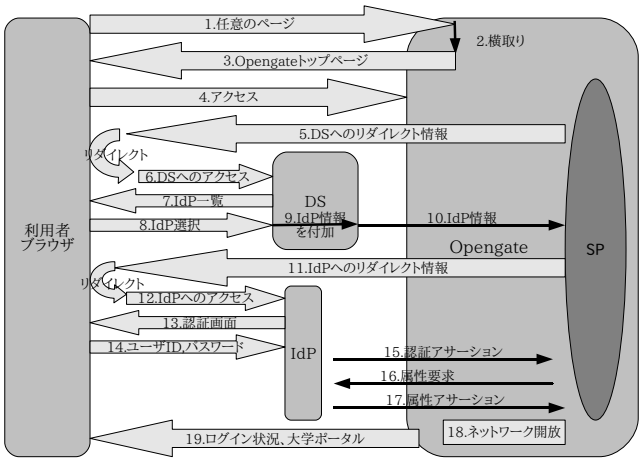

図 7　Shibboleth 対応 Opengate の処理の流れ

4.2 Opengate への SP 組み込み

現在の Opengate の認証手順は、初期画面 (図 1) で利用者にユーザ名とパスワードを入力させ、ユーザ名とパスワードを認証システムに合わせたプロトコルで通信して、その結果を取得してログインの許可を決定している。

Shibboleth に対応した Opengate の場合、IdP が利用者認証を行うため、初期画面にユーザ名とパスワードの入力フォームは必要無く、IdP へのリンクがあれば良い。リンク先の IdP の認証画面でユーザ名とパスワードを入力させ、認証が通ることで Opengate に情報が戻ってくる。このため、Opengate は認証成功を IdP から返事が戻ってくることで判断することになる。

上記のような認証手順の違いを考慮し、Shibboleth 対応 Opengate を試作した。初期画面に IdP へのリンクのみがあり、リンクをクリックすることで佐賀大学の IdP の認証画面 (図 5) が表示される。Shibboleth 対応 Opengate の初期画面を図 8 に示す。

認証画面でユーザ名、パスワードを入力し、認証に成功する

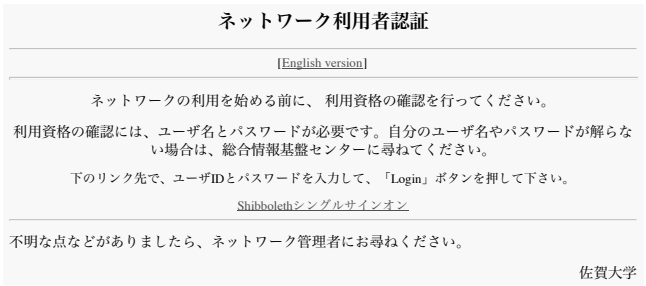

図 8　Shibboleth 対応 Opengate 初期画面

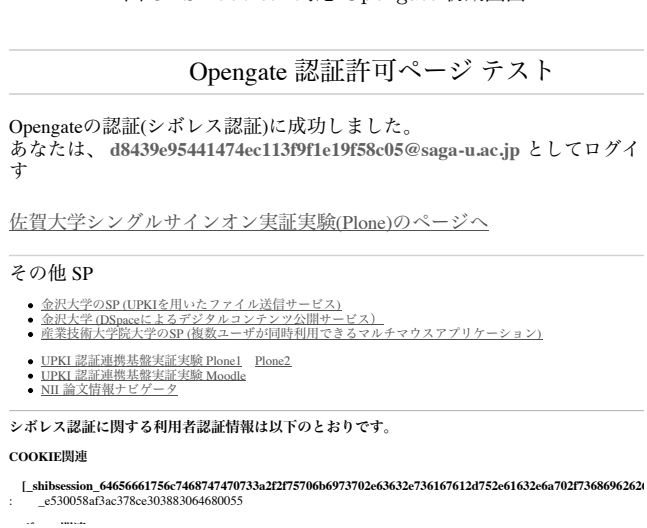

図 9　Shibboleth 対応 Opengate 認証後画面

と、Opengate の認証後の画面に移り、ネットワークの利用が可能となる。IdP からは利用者の情報が Apache 環境変数として渡される、Shibboleth 対応 Opengate はその情報を利用して記録を行う。利用者がブラウザを終了するまで、ネットワークの利用が可能となる。Shibboleth 対応 Opengate 認証後の画面を図 9 に示す。

4.3　他のサービスへのシングルサインオン

次に、Shibboleth 対応 Opengate と他の情報サービスとのシングルサインオンの確認を行った。他の情報サービスとして使用したのは、実証実験で構築した佐賀大学 Plone である。Shibboleth 対応 Opengate にログインし、佐賀大学 Plone に移ると、ログイン状態となった。

これにより、Shibboleth 対応 Opengate がシングルサインオンに対応していることを確認した。認証後の佐賀大学の Plone を図 10 に示す。

5.　課　　題

5.1　ゲスト用認証

佐賀大学での Opengate には学外者が一時的にネットワークを利用できるゲスト用認証がある。あらかじめ複数のユーザを登録したゲスト用認証サーバで Opengate が認証を行う。利用者には、特定の期間のみ利用できるゲスト用ユーザ ID を渡している。

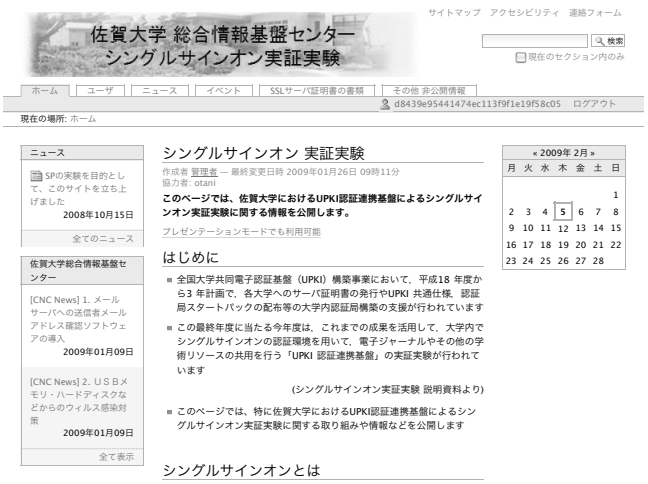

図 10　認証後の佐賀大学 Plone

Shibboleth 対応 Opengate でもゲスト用認証を行わせる必要がある。これには、ゲスト認証用の IdP を構築し、Shibboleth 対応 Opengate の SP と認証連携を行うことで、実現が可能と考えられる。

5.2　他大学との認証連携

NII の実証実験は他大学の IdP を信用する事で、その IdP で認証した利用者も信用する認証連携の仕組みである。Shibboleth 対応 Opengate が他大学の IdP と認証連携を行うと、他大学の利用者が来学した際、すぐにネットワークサービスの提供が可能になる。これにより、認証連携している大学の利用者にはゲスト用 ID の申し込みが不要となる。

認証連携により学外者へのネットワークの利用を提供するものとして、無線 LAN ローミング基盤 eduroam [9] がある。eduroam の場合は事前に利用者の端末に VPN クライアント、サプリカントの導入が必要である。一方、Shibboleth 対応 Opengate では、利用者はブラウザさえあれば良く、簡単にネットワークが接続できる。つまり、認証連携によって、使いやすいローミング環境を提供できる。

5.3　ファイアウォールルール

今までの Opengate は、Opengate が認証機能を持っていたため、利用者認証されるまでは外部ネットワークへのほとんどのポートを閉じて運用する事が可能であった。Shibboleth 対応 Opengate では、外部ネットワークにある IdP で利用者認証を行うため、IdP に対する https(443) のポートを常時開けておく必要がある。常時ポートを開けておくことによるセキュリティ上の問題を考慮する必要がある。

実証実験による他大学との認証連携機能を Shibboleth 対応 Opengate に導入した場合、NII の DS と各大学の IdP に対する https(443) のポートを常時開放する必要がある。

他大学の IdP の IP アドレスの変更が行われた場合、変更に応じてファイアウォールルールの設定の変更を行わなければならない。IdP の変更は NII の共有メタデータに反映されるため、共有メタデータの変更に応じてファイアウォールルールを動的に変更するような仕組みが必要である。

5.4 情報システムのシングルサインオン対応

大学内には既存の情報システムが多数ある。また、大学に次々の新しい情報システムが発生する。これらをシングルサインオン対応とすることで、利用者の利便性が向上するとともに、シングルサインオン環境及びそれと連携したポータルの価値が向上する。情報システムをシングルサインオン対応とするための、手順の整理や支援体制の構築が必要である。

既存の情報システムの中には、シングルサインオン対応が困難なものがあることが予想される。擬似的シングルサインオン環境なども検討する必要があるであろう。

5.5 シングルログアウト

3.1 節で述べたように、Shibboleth は SAML ベースのシングルサインオンソフトウェアである。SAML には、特定のサービスのログアウトで、シングルサインオンしている全てのサービスからログアウトするシングルログアウトの仕様がある。しかし、現在のところ、Shibboleth はシングルログアウトに対応していない。ブラウザを終了し、シングルサインオン時に使用していた Cookie を開放することで、シングルサインオン状態を抜けることができる。

Opengate でもブラウザを終了する事で、Opengate でもログアウトとなる。しかし、Opengate は、パケットが流れない時間が長時間になると、自動的にファイアウォールを閉鎖し、Opengate のログアウトとなる機能がある。Shibboleth 対応 Opengate がこの機能と整合的に動作するためには、ファイアウォール閉鎖時に Cookie を強制的に開放するなどの仕組みが必要である。

6. ま と め

本稿では、ネットワーク利用者認証システムである Opengate のシングルサインオン対応により、持ち込み PC の認証後、利用者をポータルサイトに誘導することについて、その現状と課題について報告した。

Shibboleth によるシングルサインオンの構築、運用に関するノウハウを蓄積し、それを Shibboleth 対応 Opengate の試作に活用した。Shibboleth 対応 Opengate は現在の Opengate と同様の動作を行うとともに、シングルサインオンに対応し、他のシステムへのシングルサインオン対応も可能となった。Shibboleth 対応 Opengate で実運用を行うにはいくつかの課題があるが、順次解決することが可能である。

ネットワーク利用者認証がシングルサインオンに対応し、ネットワーク利用開始と同時に大学ポータルへのログインが可能となることは多くのメリットがある。ネットワーク接続時に大学ポータルにログインするため、学内の情報システムをあらためて探す必要が無い。新入学生には、ネットワーク利用者認証による接続の方法さえ指導すれば、学生が必要としている情報システムが全て表示されるため、入学時の導入教育の削減を行うことができる。利用者を確実に大学ポータルに導くことで、大学からの情報提供をスムーズに行う事もできる。また、事務職員用、教員用の大学ポータルを作成すれば、同様の利点を学生以外の大学の構成員にも提供することが可能である。

このように、ネットワーク利用者認証認証システムのシングルサインオン対応は、ネットワーク利用者認証システムを単なるネットワーク接続のための認証システムとしてではなく、大学の基本的情報システムへアクセスするためのゲートウェイとし、大学の情報基盤の一つとして位置付けることができる。

文　献

[1] 江藤博文, 渡辺健次, 只木進一, 渡辺義明, 大学における情報基盤整備の中核となる統合認証システム, 分散システム/インターネット運用技術シンポジウム,2003

[2] 江藤博文, 只木進一, 総合情報基盤センター新システム概要〜学内組織との連携強化〜, 学術情報処理研究,No.10,2006

[3] 梶田将司, 内藤久資, 平野靖, 瀬川午直, 小尻 智子, 間瀬 健二, 名古屋大学ポータルによる情報サービスの統合と課題, 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], Vol.2007,No.72(20070719)

[4] 渡辺義明, 渡辺健次, 江藤博文, 只木進一, 利用と管理が容易で適用範囲が広い利用者認証ゲートウェイシステムの開発, 情報処理学会論文誌,Vol.42,No12,2001

[5] 国立情報学研究所 UPKI シングルサインオン実証実験 ホームページ, https://upki-portal.nii.ac.jp/SSO/

[6] Shibboleth ホームページ, http://shibboleth.internet2.edu/

[7] 国立情報学研究所 サーバ証明書発行・導入における啓発・評価研究プロジェクト ホームページ, https://upki-portal.nii.ac.jp/cerpj/

[8] 国立情報学研究所 UPKI 認証連携基盤実証実験 Plone1 サイト, https://upkishib1.nii.ac.jp/

[9] eduroam ポータルサイト, http://www.eduroam.jp/