情報処理学会論文誌　Vol. 50　No. 3　1–9 (Mar. 2010)

シングルサインオンに対応したネットワーク利用者認証システムの開発

大谷　誠[†1]　江藤博文[†1]　渡辺健次[†2]
只木進一[†1]　渡辺義明[†2]

近年，大学などにおいて，情報提供や各種情報サービスを目的として，Web を用いた情報システムが運用されるようになってきた．このような Web 情報システムは用途毎に構築される場合が多い．そのため，通常は利用者が利用するサービスに対応した情報システムにアクセスし，それぞれのシステムで認証して利用することになるため不便である．

我々はシングルサインオンに対応したネットワーク利用者認証システムの開発を行った．これにより，ネットワークの利用認証の後に，再認証なしに各 Web 情報システムが可能となるため，利便性が向上する．本論文では，このシングルサインオン対応ネットワーク利用者認証システム (SSO-Opengate) の詳細を述べる．

Development of the Network User Authentication System Supporting Single Sign-On

Makoto Otani,[†1] Hirofumi Eto,[†1] Kenzi Watanabe,[†2]
Shin-ichi Tadaki[†1] and Yoshiaki Watanabe[†2]

Recently, Web information systems are used for providing information and services, in the university etc. Such web information systems are developed for each service in many cases. Users are inconvenient in order to use different Web information systems according to the service to be used.

We developed the network user authentication system which supports a single sign-on. So, Web information systems can be used without authentication after network use authentication, improve convenience and user-friendliness in using information systems. This paper describes the network user authentication system (SSO-Opengate) according to the single sign-on.

1. はじめに

情報提供や各種情報サービスを目的として，Web を用いた多種多様な情報システムが大学などで運用されるようになってきた．このような Web 情報システムは用途毎に構築される場合が多く，通常は利用者が用途に応じて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．このような情報システムの利用者認証の共通化を行うものとして統合認証システム[1,2]がある．しかしながら，利用者認証の共通化を行っても，各情報システムを使用するたびに利用者認証が行われるので，利用者にとっては不便である．よって，各情報システムに１度の利用者認証でログインすることが可能となるシングルサインオンの導入が望まれる[3]．

一方，近年多くの大学において，ネットワーク利用者認証および記録機能を備えた，個人のノート PC を接続可能な情報コンセント，無線 LAN などの設置が進んでいる．このような認証の仕組みを実現するシステムの 1 つとして Web ブラウザを使った Captive Portal 型のネットワーク利用者認証システムが多く利用されている．認証に Web ブラウザのみを用いるため，利用者にも使いやすく，管理も容易である．

この Web によるネットワーク利用者認証システムと，認証後に利用する Web による情報システムがシングルサインオンに対応すれば，何度も利用者認証を行う必要がなくなり，利用者の利便性が向上すると考えられる．

佐賀大学では，ネットワーク利用者認証システムである Opengate[4,5]を全学的に整備しており，学内ネットワークを利用するための認証として利用されている．我々はシングルサインオンに対応した Opengate (以下，SSO-Opengate) の開発を行った．この SSO-Opengate は，Shibboleth によるシングルサインオンに対応しており，ネットワーク利用者認証を行うだけで，Shibboleth に対応した Web 情報システムにおいて認証を再度行う必要はない．また，SSO-Opengate は，認証後に任意のページを表示することが可能である．たとえばここで，情報システムをまとめたポータルサイトのようなものを表示することで，利用者を情報システムに導くと行ったことにも利用できる．利用者を確実に情報システムに導くことは，組織の情報伝達にとっても非常に有効である．

†1 佐賀大学 総合情報基盤センター
Computer and Network Center, Saga University
†2 佐賀大学 理工学部
Faculty of Science and Engineering, Saga University

本稿では，シングルサイン対応ネットワーク利用者認証システムである SSO-Opengate の詳細について述べる．

2. 背　　景

2.1 Opengate の概要

佐賀大学では 2001 年より，ネットワーク利用者認証システムとして Opengate を開発・改良し，全学規模で運用を行ってきた．

Opengate では，利用者が Web 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．

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．

Opengate は，認証を行った Web ブラウザのウィンドウの閉鎖をネットワーク利用終了と判断し，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，学生だけでなく教員も利用している．

2.2 シングルサインオンの必要性

佐賀大学の Opengate では，利用者認証基盤として総合情報基盤センターの統合認証システム[1]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．各情報システムが総合情報基盤センターのユーザ ID とパスワードで利用者認証を行うことで，統合認証システムは学内の認証基盤として位置づけられている．

利用者が PC を学内ネットワークに接続し，各種 Web 情報システムを利用することを考える．利用者はネットワーク利用者認証システムにより認証を行ったあと，教務・財務システム，e ラーニング，Web メールなど，各種 Web 情報システムで個別に認証し，それぞれのサービスを利用することとなる．そのため，たとえ同じユーザ ID とパスワードであったとしても利用者認証が何度も行われることになり，利用者にとっては非常に不便である．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，各種 Web 情報システムのログインの手間を省けるとなれば，利便性が大幅に向上すると考えられる．

3. SSO-Opengate

この章では，SSO-Opengate で用いた Shibboleth の概要と，シングルサインオンの機能を実装した SSO-Opengate について述べる．

3.1 Shibboleth によるシングルサインオン

我々は SSO-Opengate におけるシングルサインオン機能の実現に，Shibboleth を利用した[6]．Shibboleth は，Internet2 の教育機関向けプロジェクトである MACE (Middleware Architecture Committee for Education) で開発された SAML ベース (OpenSAML) の認証システムである．

Shibboleth は，利用者の認証と利用者の属性を提供する IdP (Identity Provider)，IdP からの属性情報によりサービスを提供する SP (Service Provider)，IdP が複数存在する場合に，IdP のリストを提供する DS (Discovery Service) で構成される．IdP,SP,DS として動作させるためのソフトウェアは，Internet2 から公開され，このソフトウェアと Web サービスを連携させることにより，シングルサインオンの実現が可能となる．

Shibboleth を用いたシングルサインオンの流れを**図 1** 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．SP 上の Shibboleth によって保護されたコンテンツにアクセスがあった場合は，SP はそのリクエストを IdP にリダイレクトし，利用者は IdP において認証を行う．IdP で認証に成功すると，SP に認証アサーション (Assertion) が送信される．SP は IdP にアプリケーション実行に必要な利用者の属性 (所属, 身分等の情報) を要求し，IdP は要求された属性アサーションを返す．この属性情報に基づき SP 上の Web サービスから利用者にコンテンツが送信される．

SP を利用可能な IdP が複数存在する場合には，DS が IdP のリストを提供し，利用者はその中から自分が利用する IdP を選択することによって認証を行い，コンテンツにアクセスを行う．

すでに IdP による認証が行われている場合，Web 情報システム (SP) にアクセスし，その通信が IdP にリダイレクトされた際に，IdP が管理している Shibboleth のセッション情報により認証済みと判断されるため，認証画面の提示および認証情報の入力を求められることなく (図 1 における，2 および 3 の動作の省略)，IdP から Web 情報システム (SP) に対して属性情報が提供される．

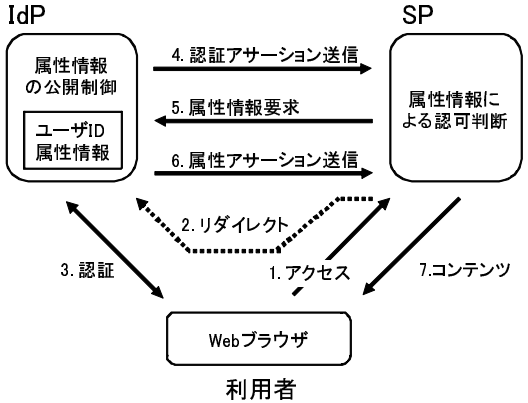


図 1　Shibboleth の動作

表 1　IdP,SP ソフトウェア構成

IdP	OS	FreeBSD 6.4-RELEASE
	シングルサインオン	Shibboleth IdP 2.1.2
	Web サーバ	Apache 2.2.11
	認証データベース	OpenLDAP 2.4.15
SP& SSO-Opengate	OS	FreeBSD 6.4-RELEASE
	シングルサインオン	Shibboleth SP 2.1
	Web サーバ	Apache 2.2.11
	ファイアウォール	ipfw(OS 付属)

3.2　SSO-Opengate のシステム構成

SSO-Opengate は，Opengate と同様に利用者端末のネットワークとの間に，ゲートウェイとなるよう設置し，そこを通過する IPv4/IPv6 パケットをファイアウォールで制御することによってネットワーク認証を行うシステムである．利用者の認証は，シングルサイン認証を行うために IdP を用いる．**図 2** にシステムの構成を示す．

SSO-Opengate は，Web サーバから CGI として起動され，利用者のインターネット利用のためのファイアウォールの制御を行う．SSO-Opengate は，FreeBSD 上で構築されており，ファイアウォールの制御には ipfw，Web サーバには Apache を用いて実現した．SSO-Opengate および IdP のソフトウェア構成を**表 1** に示す．

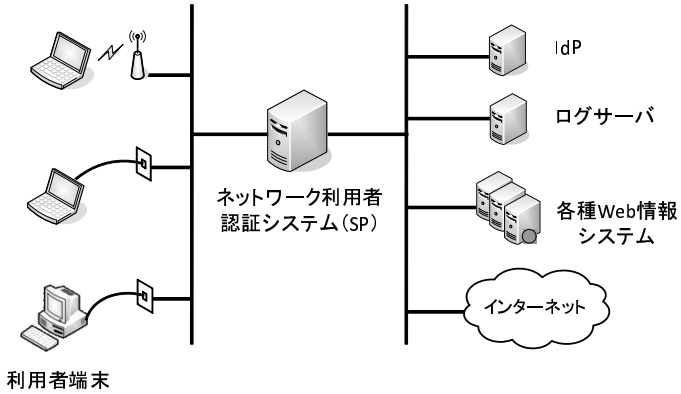


図 2　システム構成

3.3　SSO-Opengate の動作

SSO-Opengate の構成と動作を**図 3** に示す．また，以下に SSO-Opengate の動作の流れを示す．

(1) 認証を終えていない利用者端末の HTTP パケットがゲートウェイとして動作する SSO-Opengate に届くと，ファイアウォールの ipfw は，ローカルの Web サーバの HTTP ポートへとフォワードし，認証を処理する CGI (opengateauth.cgi) の表示を行おうとする．

(2) opengateauth.cgi は，Shibboleth の SP によって保護されており，表示には認証が必要となる．認証をさせるために，SP は IdP へ通信をリダイレクトする．

(3) 利用者によって IdP でユーザ ID とパスワードが入力され，認証に成功すると，IdP は，認証アサーションを SP に送る．これを受けて SP は，IdP に属性情報 (ユーザ ID) を要求する．

(4) IdP は，属性情報の応答の可否を判断し，属性情報の応答が許可されている SP であれば，属性情報 (ユーザ ID) を応答する．

(5) opengateauth.cgi は，環境変数より属性情報 (ユーザ ID) の取得を行い，ファイアウォールを制御する CGI (opengatesrv.cgi) に処理を渡す．

(6) opengatesrv.cgi は，ファイアウォールでインターネットへの通信を開放するとともに，

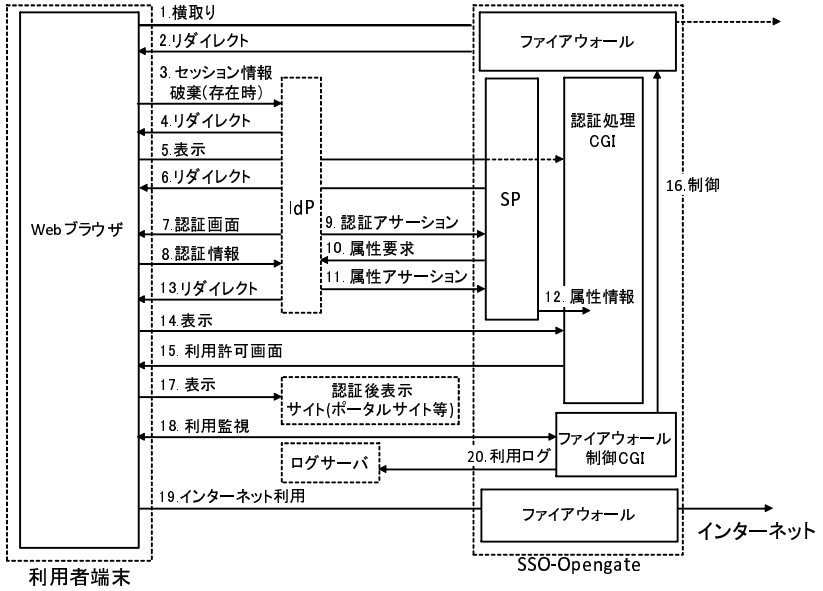


図 3　SSO-Opengate の構成と動作

ネットワーク利用許可ページ，認証後に表示するよう設定された Web サイトを表示する．

(7) opengate.cgi は，利用者のインターネット利用を監視するとともに，利用者認証に用いた Web ブラウザのページが閉じられるとそれを検知し，インターネットへの通信路を閉鎖する．インターネットの利用の監視と Web ブラウザの閉鎖検知は従来の Opengate と同様である．詳しくは参考文献[5] を参照されたい．

このように SSO-Opengate は，Shibboleth による認証を用いるため，システムそのものは，認証に直接関与していない．Shibboleth の SP が，認証の成功した利用者のユーザ ID 等の属性情報を Shibboleth に IdP に要求・取得し，その情報を SSO-Opengate に仲介することによってネットワークの利用を許可する．SSO-Opengate も SP として属性情報を取得できるため，この属性情報に応じたファイアウォールルールを用いることで，利用者に応じた通信許可のポリシーを適用することが可能である．

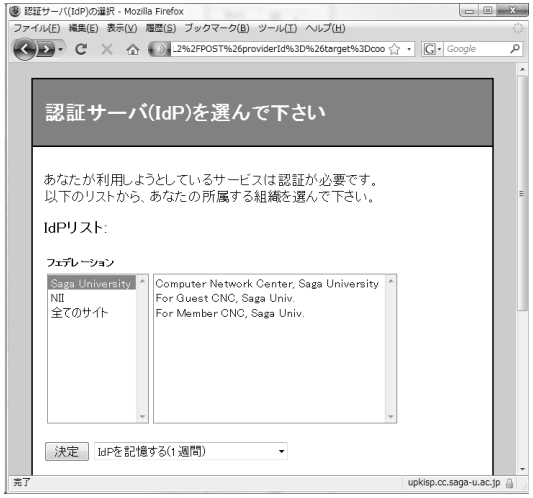


図 4　DS による IdP の選択

また SSO-Opengate は，複数の IdP を利用する必要がある場合でも，設定により Shibboleth の DS (**図 4**) を用いて IdP の選択を行い，認証を行うことが可能である．

3.4　SSO-Opengate の利用手順

SSO-Opengate が動作している環境で，インターネットを利用する手順を以下に示す．

(1) 利用者が Web ブラウザを用いて任意の URL へアクセスを行うと，通信が奪い取られ，ユーザ ID とパスワードを要求する認証ページ (**図 5**) が送られてくる[⋆1]．

(2) 利用者は，この認証ページにユーザ ID とパスワードを入力する．

(3) 認証に成功すると，認証が成功したことを示す認証許可ページ (**図 6**) が表示されるとともに，認証後に表示するように設定されているサイト (**図 7**) が別ウィンドウ (ブラウザの設定によっては，別タブ) で表示される．

(4) ネットワークの利用を終了する際には，認証許可ページを閉じる．これによりインターネットへの通信路が閉鎖され，(1) の状態に戻る．

SSO-Opengate では，自分自身ではなく IdP を経由して認証を行うが，利用者の操作は変わらないため，従来の Opengate 利用していた利用者に対しては，特に利用指導を行うこ

⋆1 DS を用いている場合は，まず DS による IdP 選択の画面が現れるので，利用する IdP を選択する

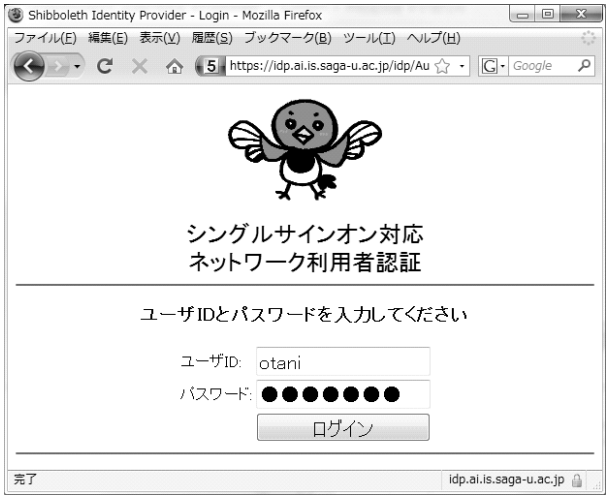


図 5　認証ページ

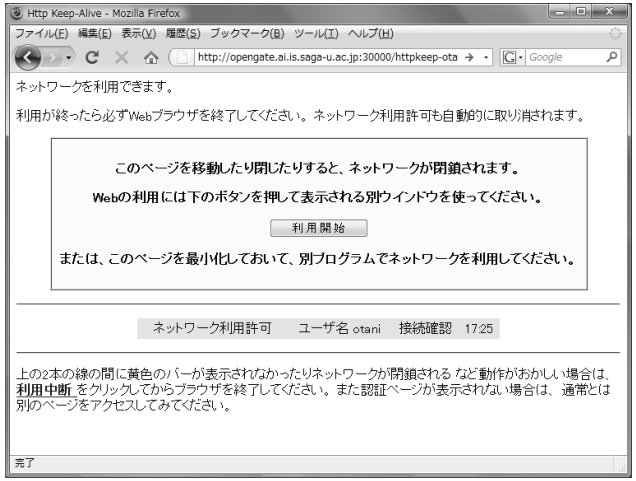


図 6　認証許可ページ

となく，この SSO-Opengate を導入することができる．

3.5　利用者情報の記録

SSO-Opengate は，ネットワークの認証後に，利用者のユーザ ID，利用者端末の IP アドレス (IPv4/IPv6) ，Mac アドレス[⋆2]，利用開始時刻を syslog の機能を用いて記録を持つ．

Web 通信の閉鎖の際は，上記の情報に加えて，利用終了の際はその時刻を記録する．また，Shibboleth における IdP での認証，SP の利用状況などは，別途 Shibboleth の利用履歴として記録される．

4. 動 作 検 証

2009 年 5 月の 1ヶ月間，SSO-Opengate を小規模なネットワーク (30 人規模) に導入し試験運用を行った．また SSO-Opengate を動作させる上で必要となる Shibboleth IdP,Web 情報システム (Moodle) 等をそれぞれ試験的に構築した．

試験運用中に，のべ 203 回の利用が行われたが，特に問題も発生することなくシングルサインオンによるネットワークの利用認証が行われた．

この際に認証に利用された Web ブラウザは，主要なブラウザである Internet Explorer 8, 7, 6，Firefox 3,2，Safari 4,3 であり，正常に動作した．

認証成功後に表示するサイト (図 7) として，各種 Web 情報システムのポータルとなるようなサイトを想定し，このサイトを Plone 3.2.2[7] を用いて構築した．Plone はコンテンツを統合的に管理・配信することができる CMS (Content Management System) の機能を有し，モジュールを追加することにより Shibbleth によるシングルサインオンに対応させることができる．SSO-Opengate では，ネットワークの利用者認証後に，Plone が表示され，表示される際にはこの Plone にすでにログインした状態となっている．

また，Web 情報システムの 1 例として，Moodle 1.9.3[8]を構築し動作を検証した．Moodle は，オープンソースの e ラーニングシステムであり多くの大学で利用されている．佐賀大学においてもこの Moodle を用いて，全学的に e ラーニングのサービスを提供している．Moodle もジュールを追加することにより Shibbleth によるシングルサインオンに対応させることができる．上述の Plone から，この Moodle に対するリンクを作成し，正常にシングルサインオンが動作していることを確認した．

⋆2 Mac アドレスは SSO-Opengate から把握できる Mac アドレスであり，ルータ配下からの利用の場合は，ルータの Mac アドレスとなる

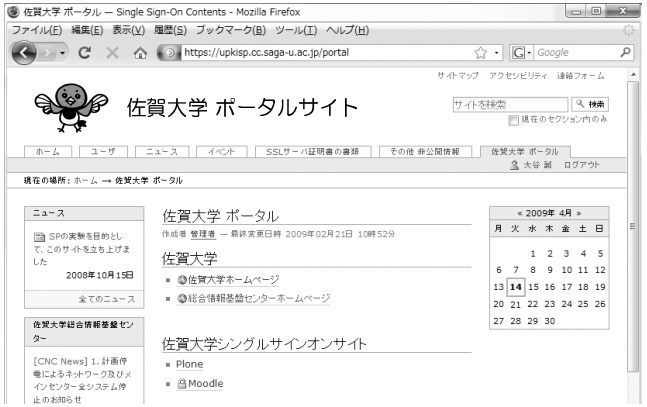


図 7　表示設定されたサイト (例)

5. 考察と課題

この章では，SSO-Opengate の課題や考察について述べる．

5.1 ゲスト用利用者認証と外部 IdP, DS との連携

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するためのゲスト用認証サーバがある．利用者は，特定の期間のみ利用できるゲスト用ユーザ ID とパスワードを用いて，ゲスト用認証サーバで Opengate の認証を行う．

一方，Shibboleth を用いる SSO-Opengate では，他大学等で構築された IdP と DS を用いて認証連携することで，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 といった臨時の ID 発行や管理が不要となる[9]．

ただし，このように外部ネットワークにある IdP, DS を利用する場合は，SSO-Opengate において利用者端末からの IdP, DS に対する HTTPS (443) のポートを事前に開放しておく必要がある．よってこれらの IdP や DS に対する匿名の攻撃を許す可能性がある．これに対する対策は課題の 1 つである．また，IdP,DS 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う必要がある．

IdP の構築を行っていない組織の学外者に，SSO-Opengate を用いてネットワークを利用させる場合は，ゲスト用の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，SSO-Opengate と DS を用いて認証連携を行えばよく，実現も容易である．

5.2 Web 情報システムのシングルサインオン対応

通常，大学内には既存の Web 情報システムが多数ある．また，大学では次々の新しい Web 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にすることで，利用者の利便性が向上する．よって，今後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．

しかし，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と思われる．このようなシステムのために，擬似的なシングルサインオン等を検討する必要がある．また，シングルサインオンの仕組みは，Shibboleth だけでなく，OpenID や CAS などいくつかの手法がある．これら複数のシングルサインオンの仕組みに対応することは今後の課題である．

5.3 SP としての SSO-Opengate と Web 情報システムの運用

Shibboleth を用いたシングルサインオンでは，IdP による認証の後に，Web 情報システム (SP) へ IdP より認証を行ったユーザの属性情報 (身分，所属，メールアドレスなど) が提供される．この際にどのような属性情報を個々の Web 情報システムに提供するかは，IdP によって制御される．IdP から提供される属性情報をもとに，各 Web 情報システム (SP) が実際のアクセス (情報提供) を許可するかを決定する．

よって，Web 情報システム毎に必要となる属性情報の提供は IdP が，その属性情報に基づく許可レベルは，SP である Web 情報システムで個別に管理することとなる．これについては，それ自身が SP として動作する SSO-Opengate についても同様である．このような許可レベルの管理は，SSO-Opengate を導入する場合に限らず，シングルサインオンを行う場合に必要な要件である．

今回提案するシステムでは，ネットワークの利用者認証の際に Shibboleth による認証を行うとともに，認証後にポータルサイトを表示する枠組みを提供する．Web 情報システムに対する許可レベルについては，個々の Web 情報システムが SP として個別に管理することを想定している．

学内で運用されるような Web 情報システムについては，セキュリティの観点からも各 Web 情報システムが最低限必要な属性情報のみを用いてサービス提供を行うべきである．各 Web 情報システムがサービスする上で，最低限必要で利用者の属性情報を Web 情報シ

ステムの管理者が明確に管理していくとともに，属性情報を提供する IdP の管理者が，その属性情報の利用が適切かどうか判断し，かつ適切と判断した属性情報のみを提供することが重要となる．

また SSO-Opengate は，ネットワークの利用時に SP としてシングルサインオンを必須とするため，シングルサインオンを望まない利用者に対してもシングルサインオンを強要することとなる．このようなシングルサインオンを望まない利用者に対応するためには，シングルサインオンを行うかどうか選択可能にするなどといった機能の実装が有効であると考えられるが，これについては今後の課題である．

5.4　利用終了と再認証

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[10]．しかし，現在のところ，Shibboleth の IdP はシングルログアウトに対応していない．そのため，すべてのシステムからログアウトするには，認証に利用した Web ブラウザのソフトウェアのウィンドウをすべて閉じることによって，Shibboleth が発行した Cookie によるセッション情報を破棄する必要がある (Web ブラウザの種類によっては必ずしもすべてを閉じる必要はない)．

しかし SSO-Opengate では，図 6 が表示されている Web ブラウザのウィンドウを閉じることにより，ネットワークの利用終了と判断し，ファイアウォールによりネットワークを閉鎖する．この際に，別のウィンドウとして Web ブラウザが起動されていた場合，シングルサインオンが有効な状態のままとなっている．

このまま，その Web ブラウザのウィンドウを閉じることなく再度 Web アクセスを行った場合，IdP でユーザ ID とパスワードの入力を求められず認証が成功し，ネットワーク利用許可ページが表示される．これは，同一の利用者が利用する場合は便利な機能となるが，共有端末など複数の利用者が端末を利用する環境では，セキュリティ上の問題が発生する可能性がある．

この対策として，SSO-Opengate では，Web ブラウザの通信を奪い取って IdP へ通信をリダイレクトする際に，Shibboleth が管理するセッション情報 (Cookie) を破棄することで，利用終了後に Web ブラウザを終了しない場合でも再度認証を行う機能を実装した (図 3 における, 3 および 4 の動作)．ただし，この機能を有効にするかどうかは，設定によって変更可能である．

これは，Shibboleth ではセッション情報を用いて，IdP ですでに認証済みかどうか判断し，認証を必要とするかの判断を行うが，この判断の前に，Shibboleth のセッション情報 (Cookie) を破棄することで，必ず認証を行わせるものである．セッション情報 (Cookie) の破棄を行う際は，ネットワークが閉鎖状態であるため，SSO-Opengate がファイアウォールと連携し通信を奪い取り，セッション情報 (Cookie) の破棄の後にネットワーク利用のためのシングルサインオン認証が行われる．よって，セッション情報 (Cookie) の破棄を行っても，認証後に新たなセッション情報が生成されるため，Web 情報システムを使用する際には，認証画面の提示および認証情報の入力を求められることはない．

5.5　スケーラビリティ

この SSO-Opengate の目的は，ネットワークの利用の際にシングルサインオン認証を行うことで，各種 Web 情報システムの利便性向上を行うことである．よって，ネットワークを利用する全構成員が利用することが想定される．たとえば佐賀大学の全構成員は約 1 万人であり，この利用規模においても，SSO-Opengate,Web 情報システム (SP)，認証を行う IdP それぞれが，負荷なく利用できる必要がある．これについてはシングルサインオンサービスの運用として別途検討する必要がある．

5.6　関 連 研 究

SSO-Opengate では，DS を用いて複数の IdP と連携し，学内だけでなく学外者へネットワークの利用を提供することができる．このような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[11] 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，SSO-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．

しかしながら，SSO-Opengate では Web による認証を行うため，偽証サーバが設置されてしまうと，ユーザ認証情報を不正に収集されてしまう可能性がある．また，NAT 機器を設置された場合，認証を行わないユーザに対してネットワークの利用を許可してしまう可能性もある．よって，このようなインシデントを防ぐためには，情報コンセントや無線 LAN 機器を正しく管理するなど，ネットワークの運用において対応していく必要がある．たとえば佐賀大学においては，持ち込み PC が接続されるネットワーク (従来の Opengate を運用する端末用ネットワーク) を他のネットワークと隔離し，厳格な運用管理を行うことで対処している．また SSO-Opengate は，従来の Opengate が持つセキュリティ機能 (セッション

情報の管理，通信状況の監視，MAC アドレス変更の検知など) を継承しており，これらをセキュリティ対策の 1 つとして利用することができる[4,5]．

その他の関連研究として，Kerberos を用いたシングルサインオン型のネットワーク認証システムがある[12]．このシステムは，OS へのログイン認証時に Kerberos を用いた認証を行い，この認証をもってインターネットの利用を許可するものである．OS のログイン認証とネットワークの利用認証を連携し一度の認証でネットワークの利用許可までをできるため，大学に常時設置されるような端末でネットワークの利用を許可する際には非常に有用である．しかしながら，OS のログイン認証が Kerberos に対応する必要があり，かつその認証が学内の認証サーバと連携するように設定される必要がある．よって，多種多様な端末 (個人所有のノート PC 等) が持ち込まれ接続されるようなネットワークで導入することは難しいと考える．また，このシステムは Web 情報システムのシングルサインオンを実現するものではない．SSO-Opengate は，Web におけるシングルサインオンに対応したネットワーク利用者認証システムであり，Web による情報システムが多く利用されている現状から，有用なシステムであると考える．

6. ま と め

大学などにおいて，情報提供や各種情報サービスを目的として，Web を用いた情報システムが運用されるようになってきた．このような Web 情報システムは用途毎に構築される場合が多い．よって通常は利用者が利用するサービスに対応した情報システムにアクセスし，それぞれのシステムで認証してサービスを利用することになるため不便である．

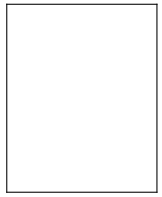
我々は，シングルサインオン対応ネットワーク利用者認証システムである SSO-Opengate の開発を行った．ネットワーク利用開始と同時に Web 情報システムへシングルサインオンすることで，多くの利用者の利便性が向上した．

また SSO-Opengate は，認証後に任意のページを表示することが可能であり，情報システムをまとめたポータルサイトのようなものを表示することで，利用者を情報システムに導くといったことも可能である．利用者を確実に情報システムに導くことは，組織の情報伝達にとっても非常に有効である．

参 考 文 献

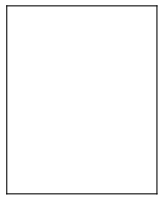
1) 江藤博文, 渡辺健次, 只木進一, 渡辺義明, 大学における情報基盤整備の中核となる統合認証システム, 分散システム/インターネット運用技術シンポジウム,2003
2) 江藤博文, 只木進一, 総合情報基盤センター新システム概要〜学内組織との連携強化〜, 学術情報処理研究,No.10,2006
3) 大学内の業務・システムと連携するキャンパス共通認証認可システムの構築と運用, 新里 卓史, 飯田 勝吉, 岸本 幸一, 太刀川 博之, 昆野 長典, 山崎 孝治, 伊東 利哉, 渡辺 治, 電子情報通信学会技術研究報告,IEICE Technical Report NS2006-197 (2007)
4) 大谷誠, 江藤博文, 渡辺健次, 只木進一, 渡辺義明: “ HTTP コネクションの監視により利用終了検知を行うネットワーク利用者認証システムの開発とその円滑な導入”, 情報処理学会論文誌, Vol. 50, No. 3,2009
5) HTTP コネクションの監視により利用終了検知を行うネットワーク利用者認証システムの開発とその円滑な導入, 大谷誠, 江藤博文, 渡辺健次, 只木進一, 渡辺義明, 情報処理学会論文誌,Vol.50, No.3, pp.1032-1042 (2009)
6) Shibboleth, http://shibboleth.internet2.edu/
7) Plone ウェブサイト, http://plone.org/
8) moodle ウェブサイト, http://moodle.org/
9) UPKI イニシアティブ 学術認証フェデレーション, https://upki-portal.nii.ac.jp/SSO
10) Shibboleth Single Logout, https://spaces.internet2.edu/display/SHIB2/SLOIssues
11) eduroam, http://www.eduroam.jp/
12) シングルサインオン型ネットワーク認証システムの開発 - Kerberos におけるゲートウェイ認証システムの開発, 原 元司, 月刊自動認識, Vol.22 No.1 (2009)

(平成 21 年 6 月 15 日受付)
(平成 ？ 年 ？月 ？ 日採録)



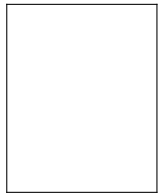
大谷　　誠（正会員）

平成 10 年佐賀大学理工学部情報科学科卒業．平成 12 年同大学大学院工学系研究科博士前期課程情報科学専攻修了．平成 15 年同大学大学院工学系研究科博士後期課程システム生産科学専攻修了．同年海洋エネルギー研究センター COE 研究員．平成 16 年同大学学術情報処理センター (現総合情報基盤センター) 講師，平成 21 年同准教授．インターネットの研究に従事．博士 (工学)．



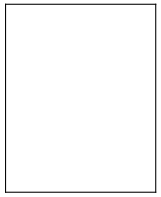
江藤　博文（正会員）

平成元年佐賀大学理工学部物理学科卒業．同年日本電気航空宇宙システム株式会社入社．平成 5 年佐賀大学情報処理センター (現総合情報基盤センター) 助手．平成 19 年同助教．画像データの曖昧検索の研究に従事．



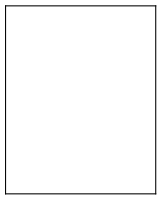
渡辺　健次（正会員）

昭和 62 年佐賀大学理工学部物理学科卒業．平成元年同大大学院理工学研究科物理学専攻修士課程修了．同年同大情報処理センター助手．平成 5 年和歌山大学経済学部産業工学科講師．平成 8 年同大システム工学部情報通信システム学科講師．平成 10 年同助教授．平成 11 年佐賀大学理工学部知能情報システム学科助教授．平成 18 年同教授，同大総合情報基盤センター副センター長．教育システム，インターネット応用，分散システム運用技術の研究に従事．博士 (工学)．



只木　進一（正会員）

昭和 62 年東北大学大学院理学研究科物理学第二専攻博士後期課程修了．日本学術振興会特別研究員 (京都大学) を経て平成 2 年佐賀大学理工学部情報科学科 (現知能情報システム学科) 助教授．平成 12 年同教授．同年同大学学術情報処理センター (現総合情報基盤センター) 教授，副センター長．平成 18 年同センター長．計算物理学，統計力学，学術情報システムの研究に関心を持つ．理学博士．



渡辺　義明（正会員）

昭和 52 年九州大学大学院工学研究科通信工学専攻博士後期課程単位取得退学．同年九州大学工学部助手を経て同大学医学部附属病院講師．昭和 61 年佐賀大学理工学部電子工学科助教授．平成 2 年同大学理工学部情報科学科 (現知能情報システム学科) 教授．平成 8 年同大学情報処理センター長．平成 12 年同大学学術情報処理センター長．生体情報工学，計算機科学の研究に従事．工学博士．