キャンパスポータルを核としたネットワークの構築

Construction of the network based on a campus portal

大谷 誠 †, 江藤 博文 †, 渡辺 健次 ‡, 只木 進一 †, 渡辺 義明 ‡

Makoto Otani†, Hirofumi Eto†, Kenzi Watanabe‡, Shin-ichi Tadaki†, Yoshiaki Watanabe‡

otani@cc.saga-u.ac.jp, etoh@cc.saga-u.ac.jp, watanabe@is.saga-u.ac.jp
tadaki@cc.saga-u.ac.jp, watanaby@is.saga-u.ac.jp

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

概要

近年，大学などにおいて，利用者への Web による情報提供や複数の Web 情報システムの連携を行うために，それらのポータルとなるサイトが必要とされるようになってきた．しかしながら，通常，このようなポータルサイトを用いて様々な情報を効果的に提供するには，利用者に能動的かつ定期的にアクセスを行ってもらう必要がある．

そこで佐賀大学では平成 22 年度に向けて，ポータルサイトを用い効果的な情報提供を実現するキャンパスネットワークの構築を進めている．このネットワークでは，Web を利用する際に定期的に認証し，認証後に利用者の属性情報に応じたポータルサイトを表示する．この際の認証はシングルサインオン認証に対応し，ポータルサイトからリンクされた Web 情報システムには，再認証なしに利用可能となる．

本稿では，このキャンパスポータルを核としたネットワークの構築と，それを実現するためのシステムについて述べる．

キーワード

シングルサインオン，ポータルサイト，認証ネットワーク，Opengate

1 はじめに

近年，大学などにおいて，利用者への Web による情報提供や各種情報サービスを目的とした多種多様な Web 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それぞれ構築されることが多く，通常は目的に応じて利用者がそれぞれのシステムにアクセスする必要がある．このため，各システムを利用しやすいようにポータルサイトにまとめるといった，利便性を向上させる取り組みが行われている [1]．

しかしながら，このようなポータルサイトを用いて情報提供を行う場合，利用者にポータルサイトへ能動的かつ定期的にアクセスしてもらえないと，様々な情報を効果的に提供することはできない．よって，ポータルサイトへ定期的にアクセスする習慣が身についていない利用者に対しては，情報提供自体が難しくなってしまう．また，ポータルサイト上で Web 情報システムをまとめて提供しても，リンクされた各システムごとに利用者認証が

行われると，利便性が損なわれ，結果としてポータルサイトへのアクセスを減らしてしまう．

情報を提供するその他の手段としては，メールを用いた方法が一般的である．所属するグループや組織ごとにメーリングリストを構築し，これを用いて，情報提供やファイル提供等が行われる．メーリングリストによる情報提供は，受信者に必要のない情報が提供されることも多く，受信者に取捨選択を行わせることになる．多数のメールから必要なメールを取捨選択することを受信者に強いることにより，メーリングリストによる情報提供は，その有効性を低下させることになる．

佐賀大学では平成 22 年度に向けて，ポータルサイトを用いた効果的な情報提供が可能なキャンパスネットワークの構築を進めている．このネットワークでは，Web を利用する際に定期的に認証を行い，認証後に利用者の属性情報に応じたポータルサイトを表示する．この際の認証はシングルサインオン認証に対応しており，ポータルサイトからリンクされた Web 情報システムは，再認証なしに利用可能となる．

また佐賀大学では，ネットワークの利用者認証を行うシステム (Opengate[2]) を，個人のノート PC を接続可能な有線・無線ネットワークにおいて運用している．このネットワークにおいても同様にポータルサイトを表示する仕組みを実現する [3]．

このようにキャンパスのポータルサイトを核としたネットワークを構築することで，大学の全構成員に必要な情報を定期的かつ効果的に提供可能になると考える．本稿では，このキャンパスポータルを核としたネットワークと，このネットワークを実現するためのポータルサイト表示システムおよびネットワーク利用者認証システム (SSO-Opengate) について述べる．

2 ネットワークの実現に必要な機能

ポータルサイトを核としたネットワークを構築する際に，ポータルサイトを表示する仕組みを，学内の各サブネットワークのゲートウェイに実装することを考える．利用者が Web を利用しようとする際に，ゲートウェイにおいてシングルサインオン認証を行い，認証成功後に Web への通信路を開くとともに，ポータルサイトを表示し利用者に応じた情報提供を行う．

そして，一定時間経過後に Web への通信路を閉じ，再度ポータルを表示する．また，これらネットワーク利用の記録を行う．

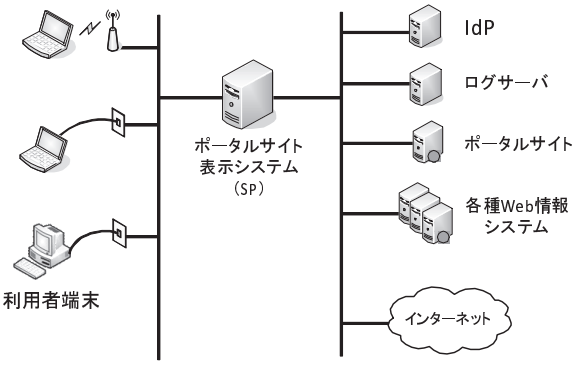

図 1: システム構成

このような仕組みを実現するネットワークを構築するためには，次に示す機能を実現するシステムを構築する必要がある．

認証画面およびポータルサイトを定期的に表示する機能
シングルサインオン認証を行う機能
利用者の情報を記録する機能

これらの機能を実現するシステムとして，ポータルサイト表示システムおよび，Opengate にポータルサイトを表示する機能を実装した SSO-Opengate の構築を行った．これらについては，それぞれ第 3 章および第 4 章に示す．

3 ポータルサイト表示システム

この章では，ポータルサイトの表示システムの構成や利用，各機能について述べる．

3.1 構成

図 1 にシステム構成を示す．ポータルサイト表示システムは，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 HTTP パケットをファイアウォールで制御することによってポータルサイトを表示する．

図 2 にソフトウェア構成を示す．ポータルサイトの表示システムは，Web サーバから CGI として起動される．利用者の Web ブラウザにポータルサイトを表示するとともに，ポータルサイトの再表示のためのファイアウォールの制御を行う．

またこのシステムは 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 を用いている．

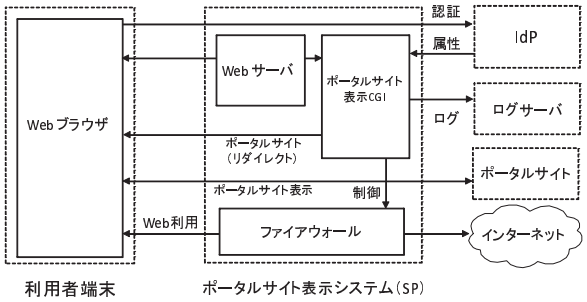

図 2: ソフトウェア構成

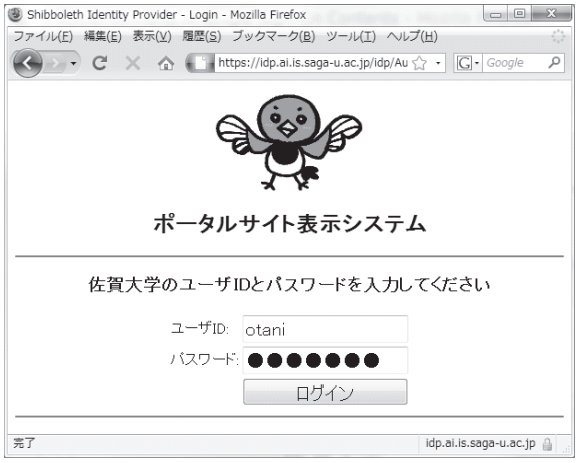

図 3: 認証ページ

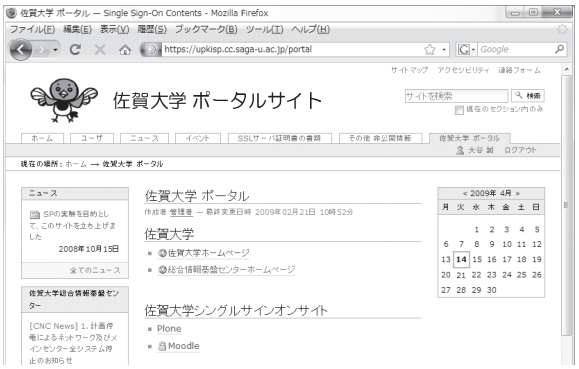

図 4: ポータルサイト (例)

3.2 利用手順

ポータルサイト表示システムが動作しているネットワーク環境で，PC を利用した際の利用手順を以下に示す．

(1) 利用者は，Web 以外の通信を特に制限なく利用できる．

(2) 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，その通信が奪い取られ，ユーザ ID とパスワードを要求する認証ページ (図 3) が Web ブラウザに表示される．

(3) 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．

(4) 認証に成功すると，ユーザの属性情報に応じたポータルサイト (図 4) の内容が表示されるとともに，(2) で最初にアクセスしようとしていた URL の Web ページも別ウィンドウ (ブラウザの設定によっては，別タブ) で表示される．

(5) 認証成功後，設定時間 (標準設定:12 時間) が経過するまで，利用者は Web やその他の通信を自由に利用することができる．

(6) 設定時間経過後または，ネットワークの利用を終了してから設定時間経過後 (標準設定:2 時間) に，(1) の動作に戻る．

3.3 各機能

この節では，ポータルサイト表示システムの各機能について述べる．

3.3.1 認証画面およびポータルサイトの表示機能

ポータルサイト表示のための Web 通信の制御は，FreeBSD 標準のパケットフィルタリング型のファイアウォールである ipfw を用いている．ipfw は制御ルールを列挙することで，パケットの送信元，送信先，ポート番号などとルールを比較し，最初に合致したルールに従い，パケットの制御を行う．

ポータルサイトの表示のための HTTP に対する制御ルール (表示ルール) を優先度の低い位置に置き，認証成功後に CGI が追加するルール (ポータルを表示しないルール) を表示ルールよりも優先順位の高い位置に追加することで，認証後に Web アクセスも通常どおり利用可能となる．

設定時経過後に CGI が追加したポータルを表示しないルールを自動的に削除することにより，再度ポータルサイトの表示が可能な状態となる．ポータルサイトを表示してから再度ポータルサイトを表示するまでの時間は設定により柔軟に変更することが可能である．

3.3.2 シングルサインオン認証を行う機能

ポータルサイトの表示システムは，シングルサインオンによる認証を行う．このシングルサイン

オン機能の実現に，Shibboleth を利用した [4].

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，それぞれ 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．

ポータルサイト表示システムは，上記のように Shibboleth による認証を用いたため，システムそのものは，認証処理は行わない．システムが Shibboleth の SP として動作し，認証の成功した利用者のユーザ ID を IdP に要求・取得することによってポータルサイトを表示する．また，このポータルサイト表示システムは，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 を用いて IdP の選択することで，異なる IdP による認証を行うことが可能である．

3.4 利用者の情報を記録する機能

利用情報として，Shibboleth における IdP および SP の利用ログの他に，syslog によって，ポータルサイト表示システムの利用状況を記録する機能を実装する．これにより，利用者のポータルサイトへのアクセス状況を一元的に把握することができる．

4 SSO-Opengate

ポータルサイトの表示システムでは，Web 以外のサービスは認証せずに利用可能であり，Web 利用の際には認証を行わせることにより，設定時間置きにポータルサイトを Web ブラウザに表示する．

Web サービス以外を利用する際も，まず Web ブラウザを用いた認証を行わせることで，ネットワーク利用者認証システムとして利用することが可能である．これによって，特定多数が個人所有の PC を接続するようなネットワークにおいて利用者認証を行うとともに，ポータルサイトの提示を行うことが可能となる．

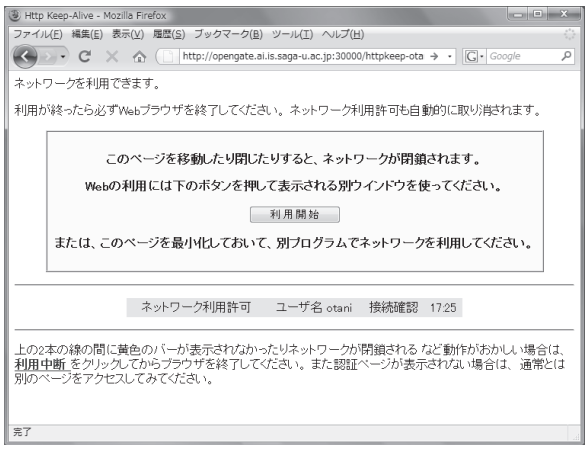

図 5: 認証許可ページ

そこで，現在学内で運用中の Opengate に，ポータルサイト表示機能，およびシングルサインオン認証機能を持たせた SSO-Opengate の開発も行った．これにより，学内の固定端末の設置を目的としたネットワークおよび，移動 PC 等の接続を目的としたネットワーク全てにおいて，ポータルサイトを表示する機能が実現できる．

この SSO-Opengate は，利用者のネットワーク利用を監視しておき，認証を行った際の Web ページ (認証許可ページ：図 5) を表示している間は，再度ポータルサイトを表示させない仕組みとなっている．

また，外部組織に設置されている IdP と連携することによって，外部組織の所属者が来学した際に，ゲスト用のアカウントを発行することなく，外部 IdP の認証によってネットワークサービスを提供することも可能となる．

5 試験運用

2009 年 5 月からの約 3ヶ月半の間，ポータルサイトの表示システム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．またポータルサイトの表示システムを動作させる上で必要となる Shibboleth IdP,Web 情報システム (Moodle[5]) 等をそれぞれ試験的に構築した．

試験運用中に，のべ 2,434 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．

この際に利用された主な Web ブラウザは，主要なブラウザである Internet Explorer 8,7,6，Firefox 3.5,3,2，Safari 4,3 であり，これらは正常に動作した．

認証成功後に表示するサイト (図 4) 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[6] 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 Shibboleth によるシングルサインオンに対応することができる．試験運用中のポータルサイトの表示システムでは，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．

その他に，SSO-Opengate についても同様の期間に，同規模のネットワークにおいて試験運用を行ったが (のべ利用回数:763 回)，正常に動作した．

6　ネットワークの全学運用に向けて

このポータルサイトを表示するネットワークの運用の目的は，多くの人が日常的に利用する Web 利用時に認証を行い，ポータルサイトを定期的に表示することで利用者毎の情報伝達を円滑に行うことである．よって，大学の全構成員の多くが利用すると想定される．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，ポータルサイト表示システム，SSO-Opengate，ポータルサイト，認証を行う IdP，DS それぞれが，負荷なく利用できる必要がある．

また，ポータルサイト表示システムおよび SSO-Opengate は，学内の各サブネットのゲートウェイとして動作することを想定しているため，現行のネットワークにおいて機能しているルーティング機器を，このシステムで置き換える必要が生じる．従って，システムは，適切な負荷分散と冗長性を確保するため，一つのサーバとしてではなく，複数のサーバとして導入し，これらを一括して管理・運用していく必要がある．現在，学内で運用している Opengate は，複数のサーバで構成しているが，この複数の各サーバは，ディスクレスによるネットワークブートを行える機器で構成することにより，大幅に管理コストを抑えている．

よって，ポータルサイトの表示の仕組みも同様に，仮想サーバやディスクレス運用技術などを用い，負荷分散を行いつつ管理コストを抑える仕組みを導入する準備を進めている．

7　まとめ

多くの人が日常的に利用する Web 利用時に認証を行い，大学のポータルサイトを提示することで，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円滑に行うことが可能となる．しかし，このようなポータルサイトを用いて様々な情報を効果的に提供するには，利用者に能動的かつ定期的にアクセスを行ってもらう必要がある．

佐賀大学では平成 22 年度に向けて，ポータルサイトを用いた効果的な情報提供が可能なキャンパスネットワークの構築を進めている．このネットワークでは，Web を利用する際に定期的に認証を行わせる．この認証後に利用者の属性情報に応じたポータルサイトを表示する．この際の認証はシングルサインオン認証に対応しており，ポータルサイトからリンクされた Web 情報システムには，再度認証を必要としない．

このキャンパスポータルを核としたネットワークを実現するために，このネットワークを実現するためのポータルサイト表示システム，およびネットワーク利用者認証システム (SSO-Opengate) の開発を行い，学内において試験運用を行った．

現在は運用へ向けて，負荷分散と冗長性確保と運用コスト削減を両立する準備を進めている．

参考文献

[1] 名古屋大学ポータルによる情報サービスの統合と課題, 梶田将司, 内藤久資, 平野靖, 瀬川午直, 小尻智子, 間瀬健二, 情報処理学会研究報告, 2007-DSM-046, pp.1-6 (2007)

[2] 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)

[3] 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, 情報処理学会研究報告, 2009-IOT-4, pp.259-264 (2009)

[4] Shibboleth, http://shibboleth.internet2.edu/

[5] Moodle, http://moodle.org/

[6] Plone, http://plone.org/