ポータルサイトを核とした仮想ネットワークの構築

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

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可能に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．

このようなネットワークを全学規模で実現するためには，多数のサーバを準備し，統合的に管理・運用をしていく必要がある．この多数のサーバの運用の冗長性確保とコスト削減には，仮想化技術が有用であり，本ネットワークの実現においても仮装化技術を用いたネットワークの構築を計画している．本稿では，このポータルサイトを核とした仮想ネットワークの構築とシステムの実現について述べる．

Construction of the virtual network based on the portal site

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

In Saga University, the construction of a campus network with the portal site which provides information effectively is planned from 2010. In this network, when users use Web, they need authentication. And, the portal site according to a user's attribute information is displayed after authentication. This authentication is single sign-on authentication, and can use again without authentication the Web information system linked from the portal site.

Many systems are needed in order to realize this network at the whole university. To reduction of this cost, the system management by the virtual server technologeies is useful, and such technology is used for this network. This paper describes the construction of virtual network and systems which display the portal site.

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，近年，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それぞれ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[1]が行われている．

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においても，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，リンクされた各情報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要因となってしまう．

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

†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

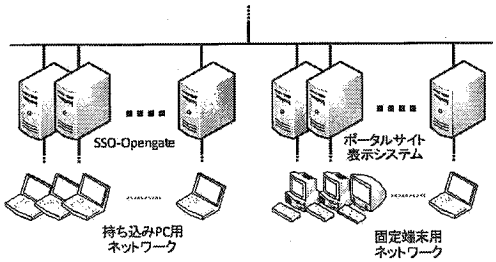

図 1 仮想ネットワークイメージ図
Fig. 1 Virtual network image.

テムは，再認証なしに利用可能となる．

また佐賀大学では現在，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 (SSO-Opengate) を実現する[3]．

このようなシステムを用い，ポータルサイトを核としたキャンパスネットワークを全学規模で実現していくためには，多数のサーバを準備し，統合的に管理・運用を行っていく必要がある．このような多数のサーバの冗長性確保と運用コスト削減には，仮想化技術が有効であり，本ネットワークにおいてもこの仮想技術を用いてネットワークを構築することを予定している．本稿では，このポータルサイトを核とした仮想ネットワークやシステムについての詳細について述べる．

2. ポータルサイトを核とした仮想ネットワーク

ポータルサイトを核としたキャンパスネットワークでは，Web ブラウザに定期的にポータルサイトを表示する．また，この際に利用者が認証を行うことで，利用者の属性情報に応じた情報をポータルサイトを表示する．よってネットワーク構成のどこかに，利用者の Web の通信を制御し，ポータルサイトを表示する仕組みを導入する必要がある．本システムでは，負荷分散や冗長性を考慮し，学内の各サブネットワークのゲートウェイに，この仕組みを実装することを想定する (**図 1**)．

利用者が出勤・登校し，Web ブラウザを用いて最初にネットワークを利用しようとする際に，ゲートウェイにおいて通信を制御し，ここでシングルサインオン認証を行う．また，この認証成功後に Web の利用を許可するとともに，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 (授業/勤務時間終了等) に Web への通信路を閉じ，その後の Web 利用時に再度ポータルサイトを表示可能な状態にする．また，これらネットワーク利用の記録を行う．その他に，これらのシステムと連携するポータルサイトおよび Web 情報システムを準備する必要がある．

このようなネットワーク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．

また，このシステムの導入の際には，学内の各サブネットワークのゲートウェイそれぞれに，ポータルサイトを表示する仕組みを導入する必要がある，よって，複数のサーバを準備し，システム全体を構成する必要がある．このサーバの構築に仮想化技術を行い，冗長性を確保しつつ運用コストを押さえる機器構成を検討した．

3. ポータルサイト表示システム

この章では，ポータルサイト表示システムの構成や利用，各機能について述べる．

3.1 概　　要

ポータルサイト表示システムは，主に常時接続されるデスクトップ PC 等，あらかじめ接続を把握しているクライアント機器が接続されるネットワークでの利用を想定している．

先にも述べたように，利用者が Web ブラウザを用いて最初にネットワークを利用しようとする際に，ゲートウェイにおいて通信を制御し，ここでシングルサインオン認証を行う．認証成功後は，ポータルサイトによって利用者毎の情報の提供を行う．また，一定時間経過後に Web への通信路を閉じ，その後の Web 利用において，再度ポータルサイトが表示される状態に戻る．

このシステムでは，あらかじめ接続されている機器を把握していることを前提としているため，認証 (シングルサインオン) は，利用者の属性に応じた情報の提供と，Web 情報システム利用時の認証の省略のために用いられる．Web 以外の通信は，特に認証等を行うことなく利用可能である．

一方，個人所有の持ち込み PC などの接続を想定したネットワークにおけるポータル表示には，ネットワークのの利用自体の認証機能も有する SSO-Opengate (第 4 章) を用いる．

3.2 構　　成

図 2 にポータルサイト表示システムの構成を示す．このシステムは，利用者端末のネットワークとの間

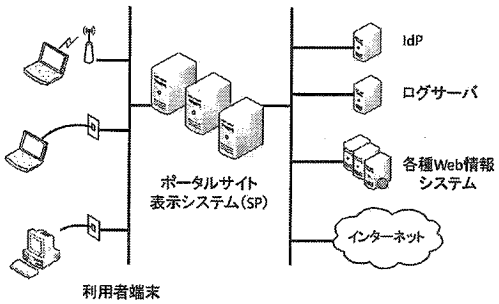

図 2　システム構成
Fig. 2　System architecture.

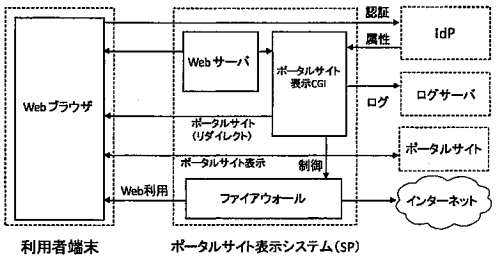

図 3　モジュール構成
Fig. 3　Module architecture.

に，ゲートウェイとなるよう設置し，そこを通過する HTTP パケットを制御することによってポータルサイトを表示する．この制御には，ファイアウォールの機能を用いる．

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 OS 付属の ipfw，認証などの Web 表示には，Web サーバの Apache を用いている．

表 1，**図 3** に実際に動作の確認を行った，ソフトウェアとモジュールの構成を示す．ポータルサイト表示システムは，Web サーバから CGI としてプロセスが起動される．利用者の Web ブラウザに認証画面や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．

3.3　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 4**) が Web ブラウザに表示される．

(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．

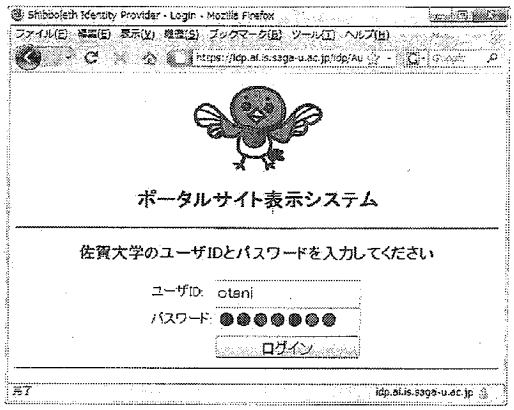

図 4　認証ページ
Fig. 4　Authentication page.

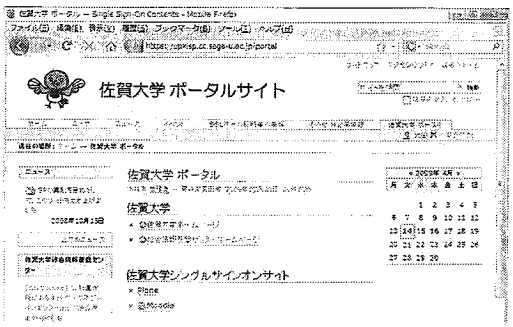

図 5　ポータルサイト (例)
Fig. 5　Portal site (example).

(3) 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 5**) の内容が表示されるとともに，(1) 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．

(4) 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．

(5) (4) の設定時間経過後に (1) の動作に戻る．ただし一定時間 (標準設定:2 時間) の間，ネットワークの利用がない場合も同様に (1) の動作に戻る．

3.4　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．

3.4.1　認証画面およびポータルサイトの表示機能

ポータルサイトを表示するための Web 通信の制御は，先に述べたように FreeBSD 標準のパケットフィ

表 1　ソフトウェア構成
Table 1　Software architecture.

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)

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 アクセスが他のプロトコルと同様に利用可能となる．

設定時間経過後に 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．

3.4.2　シングルサインオン認証を行う機能

ポータルサイト表示システムは，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 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，IdP からの属性情報をもとにサービスを提供する SP，複数の IdP を利用する場合に，IdP 選択のための情報を提供する DS で構成される．

ポータルサイト表示システムは，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 (**図 6**)．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(**図 7**) を用いて IdP の選択することで，複数の IdP による認証を行うことが可能である．

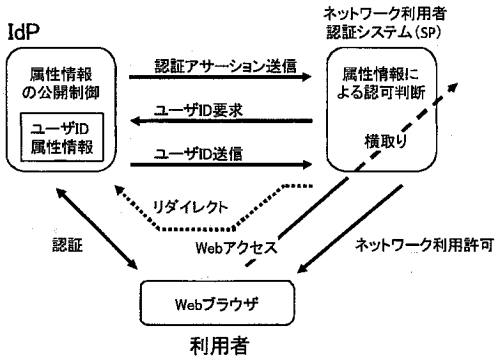

図 6　シングルサインオン認証の流れ
Fig. 6　Flow of single sign-on authentication.

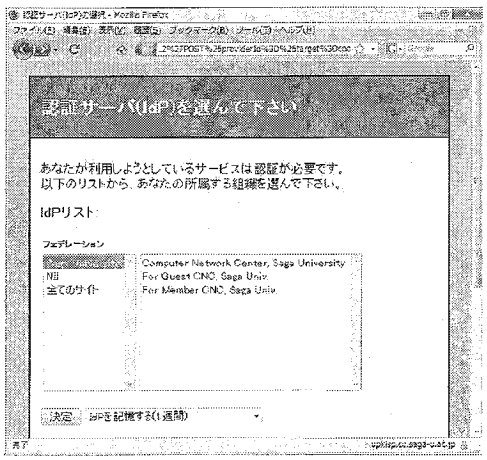

図 7　DS による IdP の選択
Fig. 7　Selection of IdP using DS.

3.4.3　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，複数のサーバ等の機器によってシステム全体を構成しても，利用者のシステムの利用状況を一元的に把握することができる．

4. SSO-Opengate

SSO-Opengate は，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での利用を目的としている．ポータルサイト表示システムでは，Web 以外のサービスは認証せずに利用可能であり，Web 利用の場合には認証を行わせることにより，設定時間お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，ポータルサイトの表示により情報提供を行うことが可能となる．

この仕組みの実現には，現在全学的に運用中の 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ることにより SSO-Opengate を実現した．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 8**) 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．ネットワーク利用の監視と Web ページの閉鎖検知は従来の Opengate と同様である．詳しくは参考文献[2]を参照されたい．

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，来学者の所属する組織の IdP を用いて認証することでネットワークサービスを提供することも可能となる．

5. システムおよびネットワークの仮想化

本研究で実現するネットワークの目的は，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，過負荷にならず安定して動作する必要がある．

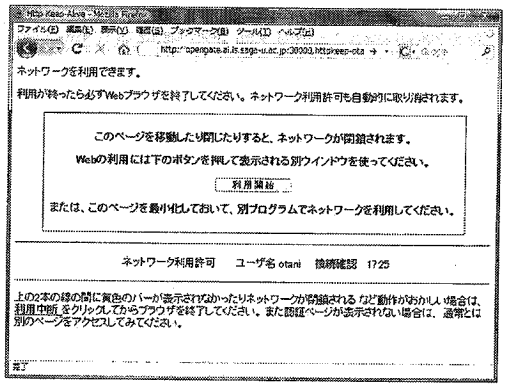

図 8 認証許可ページ
Fig. 8 Authentication accept page.

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装置を，このシステムで置き換える必要がある．従って，本システムは，安定なサービス提供とともに適切な負荷分散と冗長性を確保するためにも，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 (約 20 台: **図 9**) で構成している．この複数のサーバの構築には，ディスクレスによるネットワークブートが可能な機器を用い，マスターサーバによって設定等を一元管理することで，管理コストを抑えている[7]．しかしながら，この方法では一台のサーバを構築するために，それに対応する物理サーバをそれぞれ一台準備する必要がある．

本研究で実現するネットワークは，持ち込み PC が主に接続される Opengate が想定する利用 (最大同時利用者 300 人 程度) より，遙かに多くの利用が想定され，それに伴い従来の Opengate を運用するのに比べより多くのサーバが必要となる．よってこれらのサーバを柔軟にかつ統合的に管理するために，仮想サーバを用いたシステムを検討した．

図 10 に仮想サーバによるシステムの構成を示す．物理サーバの 1 台のスペックは，

- CPU: Xeon E5540 2.53GHz (Quad Core) × 2
- Memory: 20GB

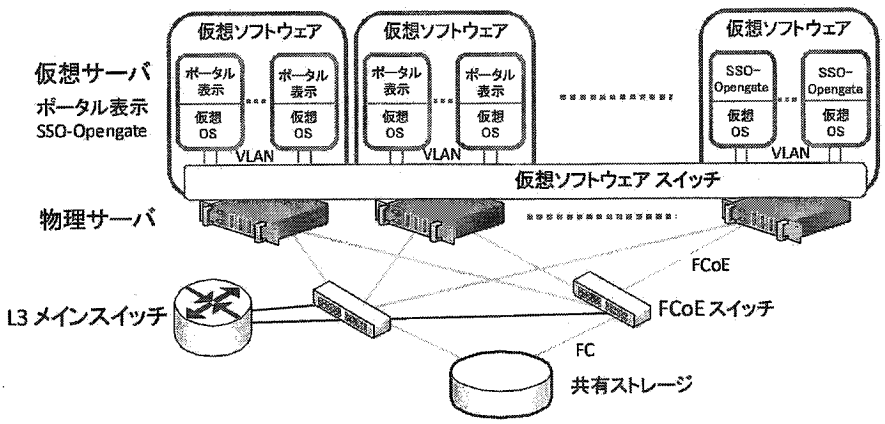

図 10　仮想サーバによる本システムの構成
Fig. 10　System architecture by virtual server system.

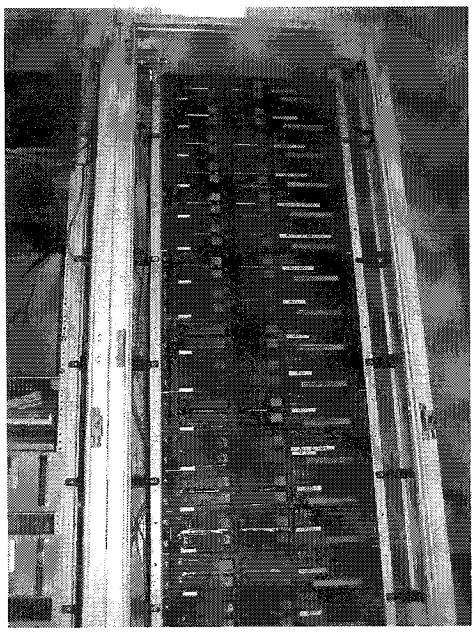

図 9　ディスクレスブートによる Opengate の運用
Fig. 9　Operation of Opengate by diskless boot.

- CNA (Converged Network Adapter): 2 ポート
- Ethernet: 10/100/1000BASE-T 2 ポート

とし，この物理サーバを計 7 台準備することによりシステムを運用する予定である．また，この物理サーバのネットワークおよびストレージ (SAN:Storage Area Network) 接続は，10Gbps の FCoE (Fiber Channel over Ethernet) を用いる．これにより高速な通信を実現するとともに I/O の統合が実現でき，ケーブリングの煩雑さの軽減にも貢献する．

この物理サーバ上にポータルサイト表示システムおよび SSO-Opengate をそれぞれ仮想に数十台構築し，それぞれ動作させることになる．これらのシステムは，先にも述べたように学内の各サブネットワークのゲートウェイとして動作する．よって，このシステム自体がネットワークのルータとして動作することで仮想ネットワークが構築されることになる．数十台のルータを，仮想サーバを用いて実現し，かつその上でポータルサイトの表示サービスを提供する必要があるため，冗長性や柔軟性，帯域の確保が重要な課題となる．

このような要件を満たし，かつ既存のネットワークから柔軟に移行を行うことを想定すると，仮想サーバを用いてネットワークを構成する場合においても，ネットワークの設定が既存の物理ネットワーク機器と同様に行えることが望ましいと考えられる．

そこで，仮想サーバ全体のネットワークの統合的な管理を実現し，かつ物理ネットワーク機器 (L2 スイッチ) と同様に設定可能となる仮想ソフトウェアスイッチ (Nexus 1000V[8]) を導入することとした．Nexus 1000V は，Cisco Nexus スイッチをソフトウェアとして実装するものである．このソフトウェアは，仮想システム上に常駐し，仮想 OS を管理するハイパーバイザに統合され，仮想マシン対応のネットワークサービスを実現する．

これにより仮想で構築され，それぞれルータとして数十台が動作する本システムの場合において，移行コストやケーブリングの煩雑さの軽減，ネットワーク構

成の柔軟な変更などが可能となるため，管理・運用コストを大幅に軽減することが期待できる．現在は，これら仮想サーバおよび仮想スイッチを用いたネットワークを平成22年度の運用に向けて構築を進めている．

6. ポータルサイトとWeb情報システムのシングルサインオン

ネットワークの利用者に情報を提供する他の手段としては，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ため，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りかねない．

ポータルサイトを核にしたネットワークにおいては，ネットワークの利用者認証の際に，大学のポータルサイトを表示し，そこで大学からの広報，連絡事項，予定など，利用者毎の情報を提供する．しかし，これを実現するためには，ポータルサイトに，利用者毎に伝達するための情報を登録していく必要がある．今回構築したポータルサイト表示システムおよびSSO-Opengateは，シングルサインオンに対応したポータルサイトを表示するための枠組みを提供するだけであり，ポータルサイトへの情報登録手段や，効率的な表示のさせ方，運用体制などについては，ポータルサイトの運用として別途検討の必要がある．

その他に，ポータルサイトからリンクを行うWeb情報システムについて，シングルサインオンへの対応の検討を行う必要がある．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．これらの対応は今後の課題である．

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効果的な情報提供を可能に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．

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，ポータルサイト表示システム，およびSSO-Opengateの開発を行った．このネットワークを全学規模で実現するためには，多数のサーバを準備し，統合的に管理・運用をしていく必要がある．これを解決するために，仮想サーバ技術を用いたシステム構成を検討した．

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/
7) 公開端末及び利用者移動端末の認証システムとそのディスクレスマシンによる運用，只木進一，江藤博文，渡辺健次，渡辺義明，学術情報処理研究, No.5, pp.15-20 (2001)
8) Cisco Nexus 1000V, http://www.cisco.com/web/JP/product/hs/switches/nexus1000/