IPv4/IPv6に対応したネットワーク利用者認証システム Opengateの改良

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

† 佐賀大学 総合情報基盤センター
‡ 佐賀大学 理工学部

概要:

近年，大学などの教育・研究機関において，IPv6 ネットワークの導入が進んでいる．よって将来，IPv6 ネットワークの利用者に対して，安全に公開端末や情報コンセントを提供するためには，IPv4/IPv6 の通信を統合的に制御可能とする新たな利用者認証システムの実現が必要となってくる．

佐賀大学では，ネットワークの利用者認証と利用記録を行うためのゲートウェイシステム Opengate を開発・公開し，学内において 2001 年より運用を行ってきた．この Opengate は，2005 年に IPv4/IPv6 の両ネットワークに対応し，学内において試験運用を行っている．この試験運用から，利用者端末の IPv4/IPv6 アドレスの取得方法の改良策を考案し，新たに実装した．本稿では，Opengate における利用者端末の IPv4/IPv6 アドレスの取得方式の改良について報告する．

Improvement of the network user authentication system Opengate for IPv4/IPv6 network

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

† Computer and Network Center, Saga University
‡ Faculty of Science and Engineering, Saga University

Abstract:

In recent years, IPv6 network is operated in many campus and research networks. From this background, it is important to implement a network user authentication system that can control both communications of IPv4/IPv6, simultaneously.

We have developed and distributed a network user authentication system "Opengate". It has been operated in Saga University since 2001. Currently, this Opengate can be used in the network of IPv6, and is operated on campus since 2005. From operation experience, we contrived and implemented the new getting method of IPv4/IPv6 address of a user terminal. This paper describes improvement of the getting method of IPv4/IPv6 address of the user terminal in the new Opengate.

1 はじめに

コンピュータを利用した情報処理や，インターネットによる情報収集・交換は，大学における研究教育上で必要不可欠な技術となっている．このような背景から，コンピュータリテラシ教育は，学生のほぼ必須科目となった．専門教育においても様々な形で，コンピュータやインターネットを利用するようになっている．大学のネットワークは，大学における研究教育を支援することを目的として構築され，原則として大学の構成員が利用資格を有するものである．従って，自由に利用できることを目的として設置される公開端末や利用者の移動端末を接続する情報コンセントにおいても，利用資格を有する者

のみが利用できる仕組みが必要である．

近年，大学などの教育・研究機関に IPv6 ネットワークの導入が進んでいる．IPv6 ネットワークを導入する際に，既存の IPv4 のネットワークを一斉に IPv6 のみのネットワークに変更するのではなく，緩やかに IPv4 から IPv6 ネットワークに移行する方がネットワーク利用者への影響も少なく，望ましい．このようなネットワークの移行方法の一つとして，ネットワークの IPv4/IPv6 デュアルスタックネットワーク化がある [1][2].

この方法では，IPv4 ネットワークに IPv4/IPv6 両通信に対応した機器を導入し，IPv4/IPv6 の両方を利用可能とする．既に，一般的な OS (Windows XP，Mac OS X など) が IPv6 を標準でサポートしている．このため，ネットワーク利用者は，IPv4/IPv6 を意識することなく使い分けることができ，徐々に IPv6 へ移行していくことが可能である．

佐賀大学では，利用者端末や公開端末からのネットワーク利用を認証・記録する “Opengate” を開発・公開し，2001 年より学内においてディスクレスで運用を行ってきた [3, 4, 5]．2005 年には，その利用方法を変えずに，IPv4/IPv6 デュアルスタックネットワークで利用するための利用者端末のアドレス情報の取得手法を提案し，実装した [6].

この手法では，利用者端末の IPv4 アドレスを取得するために IPv4 アドレスのみを持つドメイン名を準備し，そこに接続させることによって利用者端末の IPv4 アドレスを取得する．このため，別途ドメインを準備する必要があった．SSL を使用する場合には，このドメイン名の為の SSL 証明書も別途準備する必要があった．

そこで，新たに別途ドメイン名を準備する必要のない手法を考案し，実装した．本稿では，この新しい手法を実装した IPv4/IPv6 に対応する Opengate について記述する．

2　Opengate について

まず初めに，Opengate の概要や基本的な機能について説明する．

2.1　概要

Opengate は，特定多数の利用者が多様な端末を接続するネットワーク環境において，利用者認証と利用記録を行うことができるシステムである．この Opengate では，特別な申請やソフトウェアの準備なしに，利用者端末をインターネットに接続することができる．

Opengate のシステム構成例を図 1，基本的な動作の流れを図 2 に示す．

利用者が，始めに Web サイトを閲覧しようとする際に，Opengate はその通信を横取り，代わりに認証ページを利用者に提供する．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し，認証サーバを利用した認証に成功すると，ネットワークの利用が可能となる．

Opengate では，ファイアウォールの設定によって任意の通信プロトコルを常時開放・常時閉鎖・認証後開放に選択制御できる．ただし Web 以外の通信プロトコルを使用する利用者も，任意の Web サーバへ HTTP アクセスすることから始める必要がある．

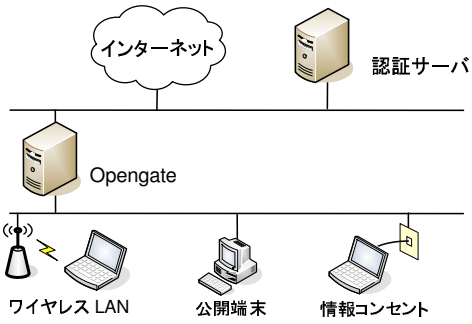

図 1　Opengate のシステム構成例

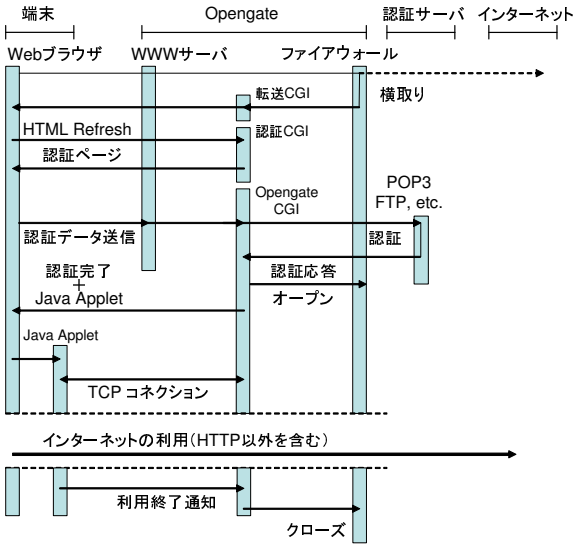

図 2　Opengate の動作の流れ

2.2　Opengate の動作環境

Opengate は FreeBSD 上で開発を行っている．ファイアウォールには ipfw，Web サーバには Apache を利用し，利用状態を監視するプログラムを C 言語で開発した．上記のプログラムが，認証後にダウンロードされる利用者端末の Java Applet と通信することにより利用状

態を監視する．そのため，利用者端末に Java Applet が動作する Web ブラウザが必要となる．もし利用者端末に Java Applet が動作する Web ブラウザがない場合，Opengate は，あらかじめ設定された時間経過後に利用者端末の通信路を自動的に閉鎖する．また開放中には arp や ipfw コマンドを定期的に実行し，端末の MAC アドレスが変更された場合や端末からのパケットが無い場合は閉鎖する．

2.3 認証

Opengate を利用したネットワークでは，利用者はまず任意の Web サーバへ HTTP を用いてアクセスしなければならない．このとき，Opengate は，ファイアウォールの転送機能を用いて HTTP リクエストを自身の Web サーバへ転送する．これによって，利用者端末に認証ページが表示されることになる．ネットワーク利用者は，この認証ページより利用者 ID とパスワードを入力する．これら利用者 ID やパスワードは，Opengate の CGI に POST され，CGI は外部の認証サーバを使用し認証する．なお，認証には POP3, POP3S, FTP, RADIUS や PAM を利用することが可能である．

2.4 利用者端末の監視と閉鎖

認証後，利用者端末に認証完了ページが表示される．さらに，この認証完了ページとともにブラウザに Java Applet がダウンロードされる．この Java Applet が監視プロセスとの間に TCP コネクションを張ることによって，ネットワークの利用を監視する．この Java Applet と監視プロセスとの TCP コネクションが切れた場合，あるいは Java Applet が監視プロセスからの応答メッセージに応答しなかった場合に利用終了と判断し，通信路を閉鎖する．利用者端末に Java Applet が動作する Web ブラウザがない場合，設定時間経過後に通信路を閉鎖する．

2.5 通信状況の監視

利用者端末の存在が確認できたとしても，必ずしも利用者がネットワークを利用しているとは限らない．そこで Opengate を通過する，利用者端末から送信されたパケット数を監視し，設定時間内にパケットの通過が確認できない場合も利用終了と判断し，通信路を閉鎖する．

2.6 利用者情報の記録

Opengate は利用者の情報として，認証，ネットワーク利用開始の手続きで取得した利用者 ID，利用者端末 IP アドレス，MAC アドレス，利用開始時刻，利用終了時刻を SYSLOG 機能を用いて記録する．ただし MAC アドレスは Opengate を利用者端末と同一セグメントに設置している場合に意味がある．

3 Opengate の IPv4/IPv6 化の改良

この節では，利用者端末の IPv4/IPv6 アドレス取得方法の改良を行った Opengate の概要について述べる．

3.1 IPv4/IPv6 アドレス取得方法の改良

Opengate では，認証後に利用者端末が利用する IP アドレスに対する通信を，ファイアウォールによって開放する．IPv4/IPv6 デュアルスタックネットワークにおいては，IPv4/IPv6 の通信を意識せずに併用するため，従来の IPv4 のみに対応した利用者認証システムを，単に IPv6 対応にするだけでなく，IPv4/IPv6 の両通信を統合的に制御可能する新たな利用者認証システムの実現が必要となる．つまり，IPv4/IPv6 に対応する Opengate は，利用者端末が利用する IPv4/IPv6 アドレスを把握し，統合的に管理する必要がある．

3.1.1 従来の IPv4/IPv6 アドレス取得方法

Opengate は，2005 年に試験的に IPv6 に対応した．この試験的に対応した Opengate の利用者端末の IPv4/IPv6 アドレス取得方法 (従来手法) について述べる．

従来手法では，Opengate のサーバ名として二つの FQDN を用意する必要がある．一つには，DNS に IPv4 アドレス (A レコード) のみを持つ FQDN(以下，FQDN_4 と記述する) を登録する．もう一つには，DNS に IPv4(A レコード) と IPv6 アドレス (AAAA レコード) の両方を持つ FQDN (以下，FQDN_64 と記述する) を登録する．この 2 つの FQDN を利用者端末のアドレス情報の取得に利用する．

Opengate は，利用者が初めて Web サイトを閲覧する際に，この通信を横取り，認証ページを利用者に提供する．利用者端末が IPv6 に対応している場合，Web サイトへの通信は，Web サイトが IPv6 に対応していれば IPv6，そうでなければ IPv4 で行われる．以下に，IPv6 で通信が行われた場合の従来手法の流れを示す．

(1) 利用者端末の Web ブラウザは，Web サーバに IPv6 HTTP リクエストを送信する．しかし，通信路は閉鎖されているため，IPv6 HTTP リクエストは遮断される．

(2) Web ブラウザは, 同じ Web サーバに IPv4 HTTP リクエストを送信する．ここで Opengate は, ファイアウォールの転送機能を用いて HTTP リクエストを自身の Web サーバへ転送する．

(3) 次に Opengate の認証のページの CGI に，ブラウザのクライアントプル機能 (html の meta タグ: http-equiv=”Refresh”) を用いた自動再表示により転送する．この際，転送する URL を FQDN_4 で指定する．認証ページを提供する CGI では，利用者端末の IPv4 アドレスを環境変数 “REMOTE_ADDR” より取得し，認証ページに hidden タグを用いてこの IPv4 アドレスを埋め込む．

(4) 認証ページに，利用者 ID とパスワードを入力すると，これと一緒にページに埋め込まれた IPv4 アドレスを Opengate の CGI へ送信 (POST) する．この際, 送信先の Opengate CGI の URL に, Opengate 自身の FQDN_64 を指定する．

(5) Opengate CGI において，URL が FQDN_64 で指定されているので，Opengate の IPv6 アドレスに対して HTTP 通信が行われる (通常のブラウザは, IPv6 を優先して利用する)．そこで Opengate は，環境変数 “REMOTE_ADDR” より利用者端末の IPv6 アドレスを取得する．IPv4 アドレスは，認証データとあわせて POST されているため，これより取得する．

最初の Web サイトのアクセスが IPv4 で行われた場合，上記の (1) の手順が省略され，後は同様である．

利用者端末が IPv6 に対応していない場合も同様に (1) の手順が省略される．また，(5) の手順の POST の通信が IPv4 で行われるため，ここで再度 IPv4 アドレスが取得される．

3.1.2 改良を行った IPv4/IPv6 アドレス取得方法

従来手法では，認証ページを表示する際に，IPv4 アドレスのみを持つドメイン名 (FQDN_4) を準備し，そのドメイン名に一度，ブラウザのクライアントプル機能を用いて転送することによって，利用者端末の IPv4 アドレスを把握していた．このため，FQDN_4 を，IPv4/IPv6 アドレスを両方持つドメイン (FQDN_64) とは別に準備する必要があった．また，SSL を使用する場合には，この FQDN_4 の為の SSL 証明書も別途準備する必要がある．

佐賀大学では Opengate を全学規模で運営しており，Opengate のサーバ台数は数十台にも及ぶ．このように複数台の Opengate を運営するといった場合に，従来手法ではドメイン名や SSL 証明書の管理コストがとても大きくなってしまう．

よって別途ドメイン名を準備する必要のない，新たな手法を考案し，実装した．以下にこの新手法の手順を示す．

(1) 利用者端末の Web ブラウザは，Web サーバに IPv6 HTTP リクエストを送信する．しかし，通信路は閉鎖されているため，IPv6 HTTP リクエストは遮断される．

(2) Web ブラウザは, 同じ Web サーバに IPv4 HTTP リクエストを送信する．ここで Opengate は, ファイアウォールの転送機能を用いて HTTP リクエストを自身の Web サーバへ転送する．

(3) 上記の (2) における転送は，必ず IPv4 通信によって行われる．この際に，利用者端末の IPv4 アドレスを環境変数 “REMOTE_ADDR” より取得する．取得した IPv4 アドレスを URL の引数に付加し，認証を行うページ (CGI) に，クライアントプル機能を使って転送する．この引数は他のデータと共にコード化されているが，これについては第 3.2 節において述べる．

(4) 認証ページに，利用者 ID とパスワードを入力すると，これと一緒に hidden タグによってページに埋め込んだ利用者端末の IPv4 アドレスを Opengate の CGI へ送信 (POST) する．この際, 送信先の Opengate CGI の URL に，FQDN_64 を指定する．

(5) Opengate CGI において, URL が FQDN_64 で指定されているので, IPv6 アドレスに対して HTTP 通信が行われる．こで Opengate は，環境変数 “REMOTE_ADDR” より利用者端末の IPv6 アドレスを取得する．IPv4 アドレスは，認証データとあわせて POST されているため，これより取得する．

最初の Web サイトのアクセスが IPv4 で行われた場合，従来手法と同様に上記の (1) の手順が省略され，後は同様である．

利用者端末が IPv6 に対応していない場合も同様に (1) の手順が省略される．また，(5) の手順の POST が IPv4 によって行われるため，ここで利用者端末の IPv4 アドレスが再度取得される．

以上の利用者端末のアドレス取得の流れを，図 3 に示す．

3.2 取得情報の受け渡し

新しい Opengate は最初に取得した IPv4 アドレスを認証 CGI の引数として，コード化して受け渡している．この際に，コード化した IPv4 アドレスのチェックデジッ

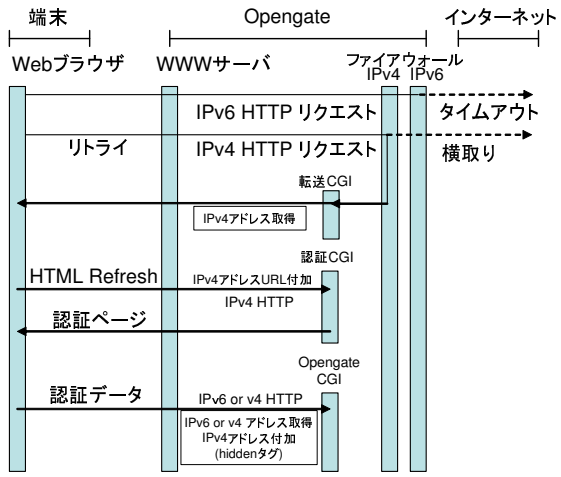

図 3　利用者端末のアドレス取得の流れ

トや，時刻情報なども同時に受け渡している．図 4 にそのフォーマットを示す．

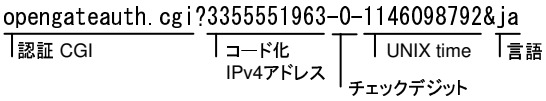

図 4　認証 CGI の引数フォーマット

IPv4 アドレスのコード化は，引数の安易な改ざんの防止を目的として行っている．引数が変更され正しいフォーマットではない場合，図 5 を表示し，再度利用者 ID とパスワードの入力を促す．

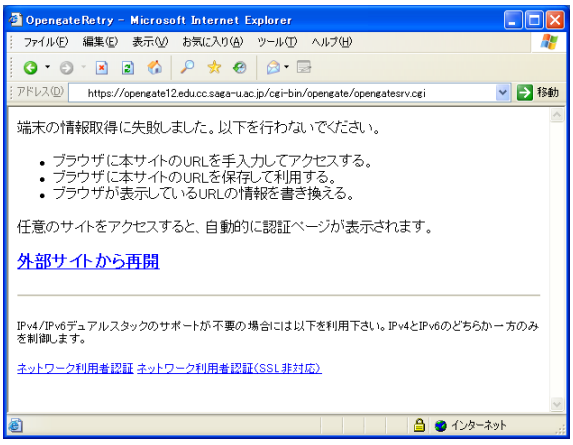

図 5　引数変更時の表示画面

引数として IPv4 アドレスをコード化して渡しているが，認証時の POST が IPv4 通信によって行われた場合は，この通信に使われた IPv4 アドレスへの通信路を開放し，引数から渡されたアドレス情報は使用しない．

また，引数として “0-0-0” を指定した場合は，再度認証情報の入力を促さずに，認証時の POST に使用されたアドレス (IPv6 または IPv4) のみの通信路を開放する．これによって，IPv6 に対応した利用者端末において，IPv6 通信路のみを開放する，ということが可能となる．この “0-0-0” の指定は，図 5 の一番下に表示されているリンクをクリックすることによっても利用可能である．

3.3　利用者端末の複数の IPv6 アドレスの取得

IPv6 では，利用者端末が複数の IPv6 アドレスを利用する場合があるため，認証時に使用された IPv6 アドレスに対する通信のみを，ファイアウォールで開放しただけでは，十分ではない．そこで，通信状況を監視する際，近隣探索プロトコルである NDP(Neighbor Discovery Protocol) エントリの一覧から得られるアドレス情報と MAC アドレスも監視している．NDP エントリの一覧に，利用者端末の MAC アドレスに対応する IPv6 アドレスが新たに追加された場合は，その IPv6 アドレスに対しても通信路を開放する．これについては従来手法においても同様である．

3.4　IPv6 における動作環境

IPv6 に関する動作環境について，ファイアウォールには ip6fw， Web サーバには IPv6 に対応した Apache を利用した．また，利用者端末への IPv4 のアドレス割り当てには DHCP を，IPv6 アドレスの割り当てにはルータ通知デーモンである rtadvd を使用し，動作確認を行った．アドレスの割り当て方法は，Opengate の動作には直接影響しない．

4　試験運用

佐賀大学では，2001 年より佐賀大学の全域規模で，Opengate をディスクレスによって運用しており，約 5 年間の運用実績を持っている．

理工学部において，2005 年 6 月より，従来手法における IPv4/IPv6 に対応した Opengate の試験運用を開始した．2006 年 8 月からは，本稿で報告した新手法の Opengate での運用を開始している．新 Opengate のインタフェースやその利用方法は，従来の Opengate のものと基本的には変更されておらず，利用者はその変更を意識せずに利用することができる．新 Opengate の利用に関するトラブルも特になく，これまで正常に動作している．また，試験期間 (2005 年 6 月 1 日〜2006 年 8 月 19 日) における Opengate の利用回数は 37,837 回であっ

た．そのうち，IPv6 に対応した利用者端末からの利用が 1,805 回 (約 4.8%) であった．少ないながらも，IPv6 に対応した利用者端末からの利用が確認できた．

新 Opengate の認証インタフェースと認証後の表示をそれぞれ，図 6，図 7 に示す．また，試験運用中の新 Opengate を構成するソフトウェアを表 1 示す．

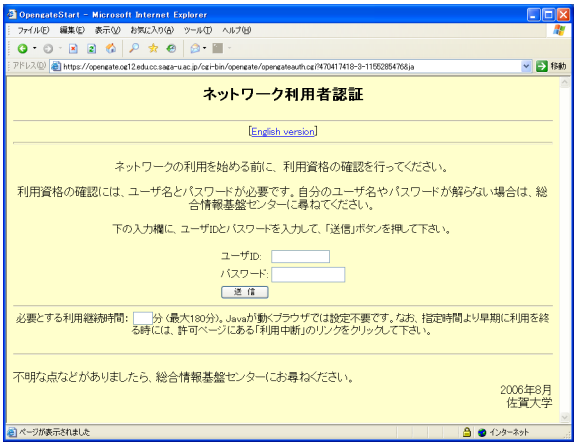

図 6　認証インタフェース

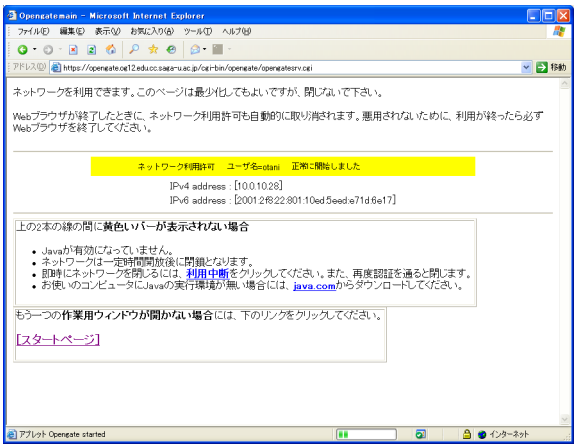

図 7　認証後の表示

5　まとめ

大学のネットワークは，大学における研究教育を支援することを目的として構築され，原則として大学の構成員が利用資格を有するものである．従って，自由に利用できることを目的として設置される公開端末や利用者の移動者端末を接続する情報コンセントにおいても，利用資格を有する者のみが利用できる仕組みが必要である．

また，近年，大学などの教育・研究機関において，IPv6 ネットワークの導入が進んでいる．よって将来，IPv6 ネットワークの利用者に対して，安全に公開端末や情報コンセントを提供するためには，IPv4/IPv6 の通信を統合的に制御可能とする新たな利用者認証システムの実現が必要となってくる．

本稿では，IPv4/IPv6 に対応したネットワーク利用を認証し記録する “Opengate” の，利用者端末の IP アドレス取得方式の改良と実装について報告した．

今後の課題としては，今回紹介した新しい Opengate の全学的な運用があげられる．また新しい Opengate のディスクレスによる運用も今後の課題である．

表 1　新 Opengate を構成する主要ソフトウェア

種類	ソフトウェア名
OS	FreeBSD 5.4
ファイアウォール	ipfw (OS 付属)
	ip6fw (OS 付属)
NAT	natd (OS 付属)
RA	rtadvd (OS 付属)
Web サーバ	Apache 2.0
DHCP	isc-dhcp3
Opengate	opengate1.3.14

謝辞

本研究は，平成 17 年度文部省科学研究費補助金 (基盤研究 (C) 課題番号 17500040) の援助を受けている．

参考文献

[1] 平成 16 年度総務省 IPv6 移行実証実験に基づく『IPv6 移行ガイドライン』，総務省 (2005)

[2] 2005 年 IPv6 移行ガイドライン，IPv6 普及・高度化推進協議会 (2005)

[3] 渡辺義明 他：「Opengate ホームページ」 http://www.cc.saga-u.ac.jp/opengate/

[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，No.12 pp.2802-2809 (2001)

[5] 只木進一，江藤博文，渡辺健次，渡辺義明：利用者移動端末に対応した大規模ネットワークの Opengate による構築と運用，情報処理学会論文誌，Vol.46，No.4，pp.922-929 (2005)

[6] 大谷誠，江口勝彦，渡辺健次：IPv4/IPv6 デュアルスタックネットワークに対応したネットワーク利用者認証システムの開発，情報処理学会論文誌，Vol. 47，No. 4，pp. 1146 - 1157 (2006)