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

大谷 誠[†] 江口勝彦[††] 渡辺健次[†††]

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．このとき，既存の IPv4 ネットワークを IPv4/IPv6 のデュアルスタックネットワークに変更することで，スムーズな IPv6 ネットワークの導入が可能となる．このような IPv4/IPv6 デュアルスタック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．佐賀大学では，利用者移動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” の開発を行っている．本研究では，Opengate の利便性を引き継ぎつつ IPv6 に対応させ，また IPv4/IPv6 の両通信を統合的に制御可能な利用者認証システムの開発を行った．そしてこのシステムの有用性を，運用実験により確認した．本稿では，この IPv4/IPv6 の統合的な利用に対応したネットワーク認証システムの開発について述べる．

Development of a Network User Authentication System for IPv4/IPv6 Dual Stack Network

Makoto Otani,[†] Katsuhiko Eguchi[††] and Kenzi Watanabe[†††]

In recent years, IPv6 network is operated in many campus and research networks. IPv4/IPv6 dual stack network model is one of the approaches for deploying IPv6 smoothly. Users of IPv4/IPv6 dual stack network can use both IPv4 and IPv6 without a special setup. 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 a network user authentication system “Opengate” in Saga University. We have implemented functions for IPv6 into Opengate without changing characteristic features of the system. This function can control both communication of IPv4 and IPv6, simultaneously. And we verified the availability of this system by the experiment network. This paper describes about implementation of a network user authentication system for IPv4/IPv6 dual stack network.

1. はじめに

近年，多くの研究用ネットワークでは，IPv6 への対応が行われている．また大学などの教育・研究機関にも 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 のネットワークをいっせいに 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，望ましいと考えられる．

このようなネットワークの移行方法の 1 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．すでに，一般的な OS（Windows XP，Mac OS X など）も IPv6 を標準でサポートしているため，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．

一方，ネットワークの利用が日常的に行われるようになった現在，その利便性を最大限に活用するために，公開端末の設置や，情報コンセント，無線 LAN の利用環境を整備している組織が増えている．しかしながら，不特定多数の利用者に対してネットワークを公開する場合に，その利用者が特定されず犯罪に利用されるなどの恐れがある．これらの問題点を解決するため

† 佐賀大学総合情報基盤センター
Computer and NetworkCenter, Saga University
†† 佐賀大学大学院工学系研究科
Graduate School of Engineering, Saga University
††† 佐賀大学理工学部
Faculty of Science and Engineering, Saga University

には，ネットワークの利用認証や利用記録の保存を行うシステムが重要となる．

近年，このような利用者認証システムの開発がさかんに行われている．事前に利用者や利用者端末に関する情報を登録したり，あるいは専用ソフトウェアをインストールしたりするものから，認証などを通じてゲートウェイを開閉するものまで，いくつかの方式が提案されている[3)~7)]．

今後急増するであろう IPv4/IPv6 デュアルスタック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 の両通信に対応した利用者認証システムが必要であると考えられる．ネットワーク利用者は，IPv4/IPv6 の両通信を意識せずに併用して利用するため，この両通信に対する認証を統合し，また通信路の開閉を同時に行う必要がある．そのため，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．また，IPv6 においては，マルチホームや，匿名アドレスなどによって利用者端末が複数の IPv6 グローバルアドレスを利用する場合があるため，これら複数のアドレスへの対応も必要となる．

佐賀大学においても，利用者移動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” の開発・運用を行っている．本研究では IPv4 のみを想定して開発された，この Opengate を，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の利用に対応させ，運用実験を行い，利用者端末の IPv4/IPv6 の両通信を統合的に制御可能であることを確認した．また上記に述べたマルチホームや，匿名アドレスなどによって，利用者端末が複数の IPv6 アドレス利用する場合にも，それらすべての IPv6 アドレスを把握して扱うことも可能とした[8)]．

本稿では，この Opengate の IPv6 対応と運用実験による評価について述べる．この Opengate に対する IPv6 対応の手法は，Opengate と同様に OSI 参照モデルにおけるネットワーク層で通信を制御する，ネットワーク利用者認証システムに適応が可能であると考える．

まず 2 章において，Opengate の概要について述べ，次に 3 章で，IPv6 対応 Opengate の設計について述べる．4 章において，IPv6 対応 Opengate の実装について述べ，5 章で運用実験について述べる．6 章において考察し，最後に 7 章でまとめる．

2. Opengate について

2.1 概　　要

Opengate の概要について述べる．Opengate は，不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 は，佐賀大学において開発され，2001 年より佐賀大学の全域規模で利用されている[9)~11)]．また，いくつかの大学でも運用されている[12)]．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**，動作の流れを**図 2** に示す．

利用者端末が，初めに 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．

なお，Opengate は NAT や DHCP を用いたネット

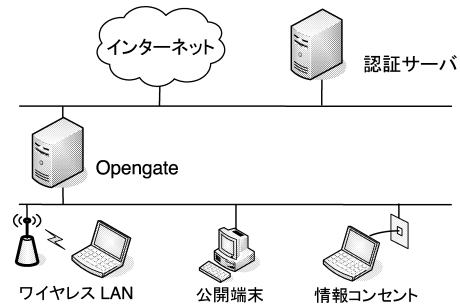

図 1 Opengate のシステム構成例
Fig. 1 Example of Opengate system architecture.

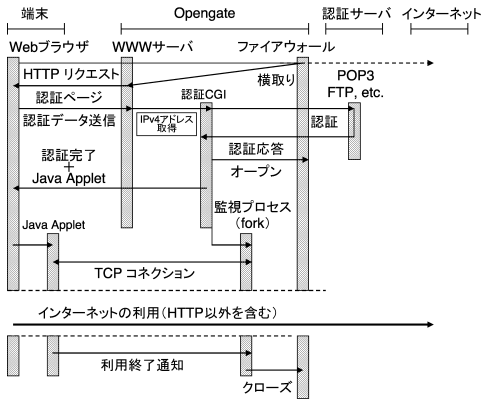

図 2 Opengate の動作の流れ
Fig. 2 Operation flow of Opengate.

ワークにおいても使用可能である．

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，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 は利用状態を監視せず，設定時間経過後に利用者端末の通信路を自動的に閉鎖する．

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（以下，この Web サーバをスタートアップ Web サーバと記す）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．これらは Opengate の CGI に POST され，CGI は外部の認証サーバに対して認証を行う．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 IP アドレスの取得

Opengate は上記の POST が実行された際，利用者端末の IP アドレスを Web サーバから環境変数 “REMOTE_ADDR” を用いて取得し，この IP アドレスに対して通信路の開閉を行う．

2.5 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．

2.6 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．

2.7 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，利用開始時刻，利用終了時刻を SYSLOG 機能を用いて記録する．また Opengate を利用者端末と同一セグメントに設置している場合は，MAC アドレスの記録も行う．

3. IPv6 対応 Opengate の設計

この章では，IPv6 対応 Opengate の設計について述べる．

3.1 IPv6 対応 Opengate が利用される環境について

IPv6 対応 Opengate では，IPv4/IPv6 デュアルスタックネットワークにおいて，利用者端末が，IPv4 または IPv6 を用いてインターネットを利用することを想定している．ここで，IPv4/IPv6 デュアルスタックネットワークとは，同一の物理ネットワーク内で IPv4 と IPv6 が同時に利用されているネットワークのことを指す．

IPv4/IPv6 デュアルスタックネットワークでは，以下のような利用者端末が接続される．

- IPv4 のみをサポートした利用者端末
- IPv4 と IPv6 をサポートした利用者端末
  - Web ブラウザが IPv4 を優先利用する利用者端末
  - Web ブラウザが IPv6 を優先利用する利用者端末

IPv4 と IPv6 をサポートした利用者端末において，Web ブラウザが IPv4 の通信を優先するものと，IPv6 の通信を優先するものがある．これについては，4.2.3 項で詳しく述べる．

なお，本提案方式は，IPv6 のみをサポートした利用者端末をサポートしていない．これは，本方式で認証ページを提供する際に必要となるファイアウォールのパケット転送機能が，FreeBSD の IPv6 のファイアウォールに実装されていないからである．さらに，本方式では利用者端末の利用状況を監視するための Java Applet と通信を行うが，利用者端末に導入されている Java VM が必ずしも IPv6 に対応していると限らない．このため，利用者端末の監視ができない可能性がある．よって IPv6 のみを利用する端末は対象外としている．

3.2 IPv6 対応に対する方針

これらの利用者端末を考慮して，以下のような方針で，IPv6 へ対応させることとした．

(1) 従来の Opengate の利用方法の維持
認証などの利用者側の操作方法は，従来の Opengate と同様とする．また IPv6 を利用しない利用者端末も従来どおり利用可能とする．

(2) IPv4/IPv6 の両プロトコルに同時に対応
利用者端末の IPv4/IPv6 の両アドレスを同時に管理し，利用開始および終了時に，両プロトコルによる通信の開閉を同時に行うものとする．

(3) IPv6 特有の問題に対応
マルチホーム環境や，匿名アドレス[13] や IPv6 のアドレス自動設定機構により付与されたアドレスなど，複数の IPv6 アドレスを扱う利用者端末にも対応するものとする．

3.3 必要な機能

上記の方針に基づき，以下の機能を実現する IPv6 に対応した Opengate の開発を行った（以降，IPv6 に対応した Opengate を “Opengate_v6” と記述し，従来の Opengate については “Opengate” と記述する）．

(1) 利用者端末のアドレスの取得
認証の過程で Web サーバを介して，利用者端末の IPv4/IPv6 アドレスの両方を取得する．

(2) IPv4/IPv6 両通信路の同時開放
認証の過程で得られた利用者端末の IPv4/IPv6 アドレスに関する通信路を同時に開放する．

(3) 利用者端末の監視と閉鎖
Opengate と同様に Java Applet によって利用者端末の存在を監視し，利用終了時に，IPv4/IPv6 の両通信路を同時に閉鎖する．

(4) 通信状況の監視
一定時間以上，利用者端末が IPv4 および IPv6 の通信を行わなかった場合に，両通信路を同時に閉鎖する．

(5) 複数 IPv6 アドレスを持つ利用者端末への対応
利用者端末が複数の IPv6 アドレスを有しているとき，認証の際に利用されない IPv6 アドレスも取得し，あわせて扱うことを可能にする．

4. IPv6 対応 Opengate の実装

4.1 Opengate_v6 の動作環境

Opengate_v6 は，Opengate と同様に FreeBSD 上で開発を行った．Opengate_v6 では，IPv4 と IPv6 の両通信路を開閉する必要があるため，Opengate と同様に IPv4 の開閉には ipfw を用い，IPv6 の開閉には，ip6fw を用いた．また，利用者端末への IPv4 のアドレス割当てには DHCP サーバである dhcpd を，IPv6 アドレスの割当てにはルータ通知デーモンである rtadvd を使用し，動作確認を行ったが，アドレスの割当て方法は，Opengate_v6 の動作に影響しない．

そのほかに，利用者端末の IPv6 アドレスを，IPv6 に対応した Web サーバから取得するため，IPv6 に対応した Apache を利用した．動作環境の例は，5 章の運用実験を参照されたい．

4.2 利用者端末の IPv4/IPv6 アドレスの取得

3.3 節で示したように，Opengate を IPv6 に対応させるうえで必要な機能の 1 つが，利用者端末の IPv6 アドレスの取得である．

4.2.1 スタートアップ Web サーバの多様性

Opengate を利用したネットワークでは，利用者はまずスタートアップ Web サーバにアクセスする必要がある．これは Opengate_v6 においても同様であるが，IPv6 を考慮すると，このスタートアップ Web サーバには，以下の 3 種類があることになる．

- IPv4 アドレスのみを持つ Web サーバ
- IPv4/IPv6 アドレスを持つ Web サーバ
- IPv6 アドレスのみを持つ Web サーバ

よって Opengate_v6 では，これらのスタートアップ Web サーバを考慮する必要がある．

4.2.2 環境変数によるアドレスの取得

Opengate_v6 においても Opengate と同様に Web インタフェースにより認証を行う．ネットワーク利用者は，認証ページより利用者 ID とパスワードを入力する．これらの情報によって，外部の認証サーバに対して認証を行う．Opengate_v6 では，この認証ページを表示する過程において，利用者端末の IPv4 と IPv6 の両アドレスの取得しなければならない．

IPv4/IPv6 に対応した利用者端末は IPv4 アドレスと IPv6 アドレスの 2 種類を所有することになる．従来の Opengate 同様，IPv6 に対応した Web サーバから環境変数 “REMOTE_ADDR” を利用して IPv6 アドレスを取得することは可能であるが，この方法では，HTTP リクエストが送信された際に用いられたプロトコルの IP アドレスしか，取得できない．

そこで，利用者端末の IPv4/IPv6 アドレスの情報を，環境変数 “REMOTE_ADDR” から取得するためには，利用者端末からそれぞれ，IPv4 の HTTP および IPv6 の HTTP の通信を行わせる必要がある．

4.2.3 IPv6 対応 Web ブラウザの挙動

IPv4/IPv6 デュアルスタック対応の利用者端末では IPv6 のみ，あるいは IPv4 のみを用いて通信すると

いったことはなく，IPv4 と IPv6 が複合的に利用される．そこでまず，利用者端末で使用される IPv6 対応 Web ブラウザの挙動の分析を行った．

現在，広く利用されている IPv6 対応 Web ブラウザの 1 つとして，IPv6 の利用を有効にした Windows XP 上で利用される Internet Explorer 6（以下，XP+IE6 と記す）がある．この XP+IE6 の環境では，接続先の URL の FQDN について DNS に IPv4（A レコード）と IPv6（AAAA レコード）の両方が登録されていた場合，まず IPv6 を利用して通信を試みる．そして，この通信が失敗した場合にあらためて IPv4 で通信を試みる．IPv4（A レコード），または IPv6（AAAA レコード）のみが DNS に登録された FQDN に対しては，それぞれのプロトコルのみを用いて通信を試みる．

Windows XP 上で動作する Firefox や Opera，FreeBSD 上などで動作する Mozilla なども，XP+IE6 と同様に IPv6 を優先して用い，失敗すると IPv4 を用いる．また，Mac OS 10.4 に標準に搭載されている safari も，XP+IE6 と同様に IPv6 を優先して利用する．

Mac OS X 10.3 に標準でインストールされている safari は，XP+IE6 とは逆に，IPv4 を優先するようになっており，IPv4 および IPv6 アドレスの両方が登録された FQDN が URL に指定された場合には，まず IPv4 で通信を試みる．そして，この通信が失敗した場合にあらためて，IPv6 で通信を試みる．ところが，HTTPS に対する通信は，XP+IE6 と同様に IPv6 を優先して用いる．特に HTTPS に関しては，調査したすべての Web ブラウザが IPv6 を優先する．

以上のように，IPv6 対応 Web ブラウザの分析の結果，ほぼすべての Web ブラウザが IPv6 を優先して利用することが分かった．

なお，佐賀大学の Opengate 環境下で利用されている Web ブラウザの調査を行ったところ，IPv6 対応 Web ブラウザの約 96.8%は，IE6 であった．

4.3 考案した利用者端末の IPv4/IPv6 アドレスの取得方法

そこで我々は Opengate_v6 では，多くの Web ブラウザが IPv6 を優先し，IPv6 の利用に失敗した場合に IPv4 を利用するという挙動をもとにして，IPv4/IPv6 アドレスを取得する方法を考案した．

まず，Opengate_v6 を導入するゲートウェイのために，2 つの FQDN を用意する．1 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 1 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．ここでは，例として FQDN_4 を opengate4.example.jp（IPv4 アドレス 192.168.55.1），FQDN_64 を opengate64.example.jp（IPv6 アドレス 2001:db8:3661:1a5::1，IPv4 アドレス 192.168.55.1）として説明する．

先に述べたように，IPv4/IPv6 デュアルスタックの利用者端末が，任意の Web サイトの FQDN に対してアクセスする際，その Web サイトの IPv4 アドレスのみ DNS に登録されていれば IPv4 を用いてアクセスする．もし，IPv4/IPv6 の両方が登録されている場合は，IPv6 を用いてアクセスする．このとき，IPv6 によるアクセスに失敗した Web ブラウザは，IPv4 で再度アクセスを試みる．

この挙動を利用して，以下の 2 つの条件において，認証の際に IPv4/IPv6 アドレスを取得する流れを述べる．

- スタートアップ Web サーバが IPv4/IPv6 アドレスを持つ場合（4.3.1 項）
- スタートアップ Web サーバが IPv4 アドレスを持つ場合（4.3.2 項）

4.3.1 Web サーバが IPv4/IPv6 アドレスを持つ場合

(1) 利用者端末の Web ブラウザは，スタートアップ 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 リクエストはタイムアウトする．

(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，ファイアウォールによって，IPv4 HTTP リクエストを Opengate_v6 上の Web サーバ（http:// opengate4.example.jp）へ転送する．

(3) 次に Opengate_v6 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（http://opengate4.example.jp）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) 認証ページより，利用者 ID とパスワードを入力し，これと一緒にページに埋め込まれた IPv4 アドレスを Opengate_v6 の CGI へ送信（POST）する．この際，送信先の Opengate_v6 CGI の URL に，FQDN_64（http://opengate64.example.jp）

を指定する．

(5) Opengate_v6 CGI において，URL が FQDN_64（http://opengate64.example.jp）で指定されているので，IPv6 の優先利用により，IPv6 アドレス 2001:db8:3661:1a5::1 に対して HTTP 通信が行われる．そこで Opengate_v6 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．

認証の際に，IPv4/IPv6 アドレスを持つスタートアップ Web サーバへアクセスする場合の，利用者端末情報の取得の流れを**図 3** に示す．

図 2 と比較すると分かるように，認証ページの提供の際に，ブラウザのクライアントプル機能を用いてページを自動再表示をすることにより，従来のインタフェースを変更することなく，IPv4 と IPv6 の両方のアドレスの取得を可能にした．

(1) に記したように，最初の IPv6 HTTP リクエストを Opengate_v6 上の Web サーバに転送できない．これは，IPv6 ファイアウォール ip6fw が転送機能を実装していないためである．このため，利用者は IPv6 による HTTP リクエストがタイムアウトする時間を待たなければならない．各種ブラウザの仕様によってタイムアウトまでの時間は異なるものの，約 5〜15 秒を要する．

ただし，ip6fw のバージョン（FreeBSD4.10 または FreeBSD5.2 以上に付属の ip6fw）によっては，ブラウザに “TCP reset（RST）notice メッセージ” を送信することができるため，タイムアウトによる待ち時間をなくすことができる．

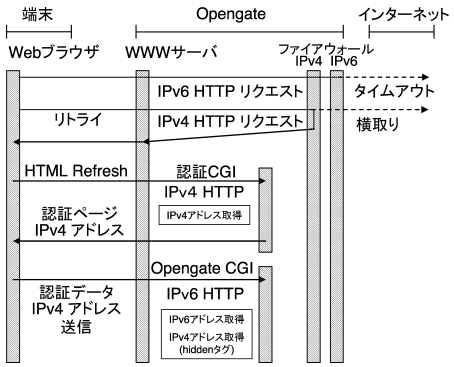

図 3 Opengate_v6 における利用者端末情報取得
Fig. 3 Acquisition of terminal information in Opengate_v6.

4.3.2 Web サーバが IPv4 アドレスのみを持つ場合

(1) スタートアップ Web サーバに IPv4 HTTP リクエストを送信する．ここで，ファイアウォールによって，HTTP リクエストはゲートウェイ上の Web サーバへ転送される．

以降は，IPv4/IPv6 アドレスを持つ Web サイトにアクセスした場合における (3)〜(5) と同様である．

つまり，初回の HTTP リクエストが IPv4 を用いて行われるため，IPv4/IPv6 アドレスを持つ Web サイトにアクセスした際の (1) の手順が省略され，(2) 以降と同様の処理となる．

以上のように，Opengate_v6 の IPv4/IPv6 アドレス取得では，利用者端末がスタートアップ Web サーバにアクセスする際，通信先の Web サーバの FQDN は，少なくとも IPv4 アドレスが登録されていて，場合によっては IPv6 アドレスが登録されていることを前提としている．スタートアップ Web サーバが IPv6 アドレスしか持っていない場合の認証ページへの転送には，対応できていない．これは先にも述べたが，Opengate_v6 の動作環境である IPv6 ファイアウォール ip6fw が転送機能を実装していないためである．ただし，現在はこのような Web サーバは少ないため，スタートアップ Web サーバに指定されることも少なく，事実上問題にならないと考える．

4.4 通信路の開放

認証を終えると，次に利用者端末のための通信路の開放を行う．認証過程で得られた利用者端末の IPv4/IPv6 アドレスに対するファイアウォールのルールを，ipfw，ip6fw にそれぞれ追加することによって通信路を開放する．

4.5 利用者端末の監視

利用者端末の利用状況を監視するために，従来どおりゲートウェイ側の利用監視プロセスと利用者端末にダウンロードされた Java Applet 間で TCP 接続を行い，利用状況を監視する．このとき，IPv4/IPv6 デュアルスタックの利用者端末の利用状況を監視する際は，IPv4 で TCP 接続を行うように実装している．これは，利用者端末側に導入される Java VM の仕様のためである．

Java VM には，Microsoft 社のものと Sun Microsystems 社の 2 つがある．最新の Sun Microsystems 社の VM（Java Runtime Environment（JRE）1.4 以上）を利用した場合は，IPv6 を利用することは可能であるが，IPv4 が利用可能な場合は IPv4 を優先するように実装されている．すなわち，IPv4/IPv6

デュアルスタックの利用者端末の場合でも，必ずしもJava VM で IPv6 が利用可能であるとは限らないため，Opegate_v6 では利用者端末の監視の際に，IPv4を用いてコネクションを確立する．

4.6 通信状況の監視

Opengate_v6 は利用者端末から送信されゲートウェイを通過したパケット数を監視する．この際，一定時間以上 IPv4 と IPv6 の両パケットについて，ともに通過が確認できなかった場合に，利用終了を判断して両通信路を閉鎖する．どちらか一方のパケットが通過している場合は，両通信路ともに閉鎖しない．

4.7 利用される IPv6 アドレスの監視

マルチホーム環境下や，Windows XP における匿名アドレスと IPv6 のアドレス自動設定機構により付与されたアドレスのように，IPv6 では 1 つの端末が，複数のグローバルアドレスを持つことがある．Opengate_v6 は，認証時の HTTP に用いられた IPv6 アドレスについてのみ通信路を開くため，他の IPv6 アドレスに対する通信路は閉じたままである．

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）[14] 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．また IPv6 アドレスが NDP エントリの一覧から削除された場合は，その IPv6 アドレスに対する通信路を閉鎖する．

これにより，認証時に用いられなかった IPv6 アドレスも途中から利用できるようになるだけでなく，4.10 節で述べるように IPv4 を優先利用する IPv6 対応端末に対応することができる．

4.8 利用者情報の記録

従来の Opengate 同様に，SYSLOG 機能を用いて利用者情報を記録する．

利用者端末が IPv4/IPv6 デュアルスタック対応であるならば，利用者 ID，IPv4/IPv6 両方のアドレス，MAC アドレス，利用開始時刻，利用終了時刻を記録する．利用者端末が IPv4 のみ対応であるならば，IPv6 アドレスを省いたものを記録する．また，ネットワーク利用途中に利用開始された IPv6 アドレスについても同様に記録する．

4.9 利 用 終 了

先に述べたように，利用監視プロセスと Java Applet 間の通信が途絶えたとき（Web ブラウザの正常終了，異常終了時など），または一定時間以上 IPv4 と IPv6 の両パケットが Opengate_v6 を通過しなかった場合に，Opengate_v6 の利用終了と判断し，IPv4/IPv6 の両方の通信路を閉鎖する．

Opengate_v6 では，認証時に使用しなかった IPv6 アドレスに対しても通信路を開放するため（4.7 節参照），利用終了の際に，これらの IPv6 アドレスに対する通信路も閉鎖する．

4.10 IPv4 を優先利用する IPv6 対応利用者端末について

4.3 節で示した IPv4/IPv6 アドレスを取得する方法は，4.2.3 項で述べたように，IPv6 と IPv4 アドレスの両方が DNS に登録されているサーバに対する，ブラウザの挙動をもとにしたものである．多くのブラウザは IPv6 を優先して利用するため，この方法で IPv6 と IPv4 の両方のアドレスが取得できるが，一部の IPv4 を優先して利用するブラウザについては，IPv6 アドレスが取得できないことになる．

しかし，このような利用者端末がネットワーク利用の途中で IPv6 を使ったとき，NDP エントリの一覧に IPv6 アドレスが登録される．4.7 節で述べたように，Opengate_v6 は NDP エントリの一覧を監視しており，MAC アドレスをもとに追加された IPv6 アドレスを検知し，そのアドレスに対して通信路を開く機能を有している．

この機能によって，IPv6 を優先して使用しない利用者端末においても，IPv6 による通信が可能となる．

4.11 IPv4 のみを利用する利用者端末ついて

Opengate_v6 が利用される環境において，IPv4 のみを利用する利用者端末が接続された場合にも，従来どおりの方法で利用できる必要がある．

IPv4 のみを利用する利用者端末では，4.3.1 項で述べた手順の (3) で IPv4 アドレスを取得された後，手順の (5) で行われる URL の FQDN_64（http://opengate64.example.jp）に対する通信に IPv4 が用いられるため，IPv4 アドレスが再度取得されることとなる．

すなわち IPv4 のみを利用する利用者端末では，すべての HTTP リクエストは IPv4 を用いて行われ，環境変数 “REMOTE_ADDR” から IPv4 アドレスのみが取得される．この場合は，Opengate_v6 は，IPv4 通信のみを開閉する．これによって従来の Opengate との互換性を提供している．

5. 運 用 実 験

今回開発した Opengate_v6 では，認証インタフェースやその利用方法は従来の Opengate から変更してい

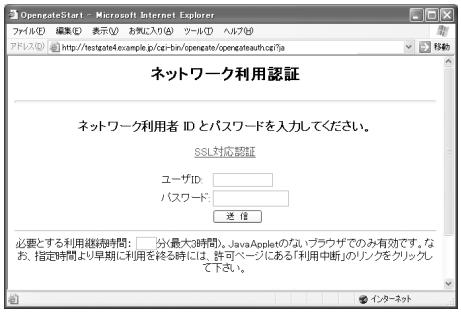

図 4 認証インタフェース
Fig. 4 Authentication interface.

図 5 認証後の表示
Fig. 5 Screen of after authentication.

ない．認証インタフェースと認証後の動作状態を**図 4**, **図 5** に示す．

利用者数が 30 人ほどの小規模なネットワークにおいて，Opengate_v6 の運用実験を行った．実験に用いたネットワークは IPv4/IPv6 デュアルスタックネットワークであり，IPv4/IPv6 デュアルスタック対応の利用者端末と IPv4 のみ対応した利用者端末の利用者が混在している．実験ネットワークでは，Opengate_v6 上で IPv4 DHCP サーバが動作し，また IPv6 RA（Router Advertisement）が送信されているため，利用者端末は IPv4 アドレスを自動的に取得し，また IPv6 アドレスを自動的に生成することが可能である．運用実験を行ったネットワークを**図 6** に示す．また，Opengate_v6 を構成するソフトウェアを**表 1** に示す．

実験ネットワークにおいて 2004 年 11 月 9 日から 2005 年 6 月 30 日までの利用記録を**表 2** に示す．全利用数の約 3 割が IPv6 を利用しているが，問題なく利用者認証が行われ，ネットワークを利用している．異常終了が約 2 割ほど発生しているが，これは利用者が Java Applet が起動している Web ブラウザで他のページを読み込んでしまったなどの利用上の問題で，TCP 接続が切断したものである．この場合，一定時間経過

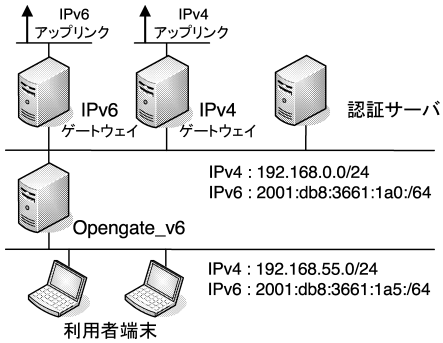

図 6 実験ネットワーク
Fig. 6 Experiment network.

表 1 Opengate_v6 を構成する主要ソフトウェア
Table 1 Software components for Opengate_v6.

種類	ソフトウェア名
OS	FreeBSD 4.10
ファイアウォール	ipfw（OS 附属）
	ip6fw（OS 附属）
NAT	natd（OS 附属）
RA	rtadvd（OS 附属）
Web サーバ	Apache 2.0
DHCP	isc-dhcp3
Opengate_v6	opengate090i+IPv6

表 2 Opengate_v6 の利用記録
Table 2 Statistics of Opengate_v6.

全利用数	4,679
IPv6 利用数	1,302
認証失敗数	511
異常終了数	880

後に再度認証を行う必要がある．この問題は Opengate_v6 特有の問題ではなく，利用者が Opengate の利用に習熟することで解決されると考えられる．

6. 考　　察

6.1 スケーラビリティ

Opengate_v6 では，従来の Opengate と同様に 1 つの利用者端末に対して，CGI によるサーバプロセスが 1 つ動作する構成になっている．佐賀大学において全学で利用されている Opengate では，最大 256 程度の IPv4 アドレス空間を管理し，分散配置するように運用されている[11]．

IPv4/IPv6 デュアルスタックネットワークにおいて運用する場合，IPv6 の膨大なアドレス空間に対して IPv4 のアドレス空間による制約が大きい．そのため Opengate 同様に分散配置することが適当であると考えられるが，IPv4/IPv6 デュアルスタックネットワークにおけるアドレスの割当ては今後の課題であり，よ

り大規模な運用実験を通じて考察する必要がある．

6.2 利用制限

4.7 節で述べたように，Opengate_v6 は，認証時に用いられた IPv6 アドレスについてのみ通信路を開くため，他の IPv6 アドレスに対する通信路は閉じたままである．そこで，通信状況を監視する際，NDP エントリの一覧も監視している．ただし，この NDP はルータを越えて配送されない．よって，Opengate_v6 では，Opengate_v6 を利用者端末間と同一セグメントに設置する必要ある．

また，Opengate_v6 を導入したネットワークに，IPv6 のみを利用する利用者端末が接続される場合が考えられる．3.1 節でも述べたが，本方式で認証ページを提供する際に必要となるファイアウォールのパケット転送機能が，IPv6 のファイアウォールに実装されていない．さらに，利用状況を監視するために使用する利用者端末の Java VM が必ずしも IPv6 に対応していると限らない．このため，利用者端末の監視ができない可能性がある．そのほかに，Opengate_v6 が利用者端末の IPv4/IPv6 アドレスを取得する際，IPv6 と IPv4 の通信を複合的に利用しているため，IPv6 のみを利用する利用者端末は利用できないといった制限がある．現状では，IPv6 のみを利用する利用者端末を使うユーザは少ないと考えられるが，これについては今後の課題である．

6.3 IPv6 パケットの転送機能への対応

Opengate_v6 に使用した ip6fw は，IPv6 パケットの転送機能が実装されていない．このため，認証の手順で一度 IPv6 の通信がタイムアウトするのを待ち（あるいは，TCP RST を用いて），次に IPv4 を用いて認証ページを提供している．

しかし，今後 ip6fw に IPv6 パケットの転送機能が実装，またはこれに代わる同様のプログラムが登場することを仮定すると，IPv6 パケット転送機能を用いて認証ページを提供することも可能となる．ここで，転送機能が実装された場合における Opengate_v6 の認証手順は以下のようになる．

(1) スタートアップ Web ページに IPv6 アドレスを送信する．ここで，ファイアウォールによって，IPv6 HTTP リクエストはゲートウェイ上の Web サーバに転送する．

以降は，4.3.1 項で述べた IPv4/IPv6 アドレスを持つ Web サイトにアクセスした場合における (3)〜(5) と同様である．

このように，IPv6 のパケット転送機能が実装された場合においても，Opengate_v6 は容易に対応可能である．

ただし，現在は NDP エントリの一覧を一定時間間隔で監視しているため，タイミングによっては，認証時に使用しなかった IPv6 アドレスを使った Web 通信に対して，ユーザ認証ページを表示してしまうといった問題が発生すると考えられる．この問題に対応するには，利用者端末にユーザ認証ページを提供しようとする際に NDP エントリの一覧を閲覧し，すでに認証が終了している利用者端末からの通信であれば，即座に通信路を開放し，認証ページを提供しないといったような対応が必要である．

6.4 アドレス偽造に関する危険性

従来の Opengate も同様であるが，Opengate_v6 は利用者認証に成功した IP アドレスに対して通信の許可を与えるシステムのため，悪意を持った利用者が，すでに認証に成功した IP アドレスを偽装し，悪用するといった危険性が考えられる．

また，Opengate_v6 は，NDP エントリの一覧を監視することによって，新たに利用が開始された IPv6 アドレスの通信を開放するため，MAC アドレスの偽装に対しても同様の危険性が考えられる．よって，これらの問題に対応するためには，セキュリティ上の対策を行う必要がある．

ただし，Opengate_v6 は利用者の認証と記録を行うシステムとして実現したものであり，悪意を持った利用者への対策は別のシステムとして実現し，組み合わせて利用することを想定しているが，これについては今後の課題である．

6.5 研究の応用

現在，ネットワーク利用者認証を行うためのシステムは幅広く研究されている．これらの研究における通信の制御を大きく 2 つに分類すると，OSI 参照モデルにおけるデータリンク層で制御する方式[3),4)] とネットワーク層で制御する方式[6),7)] に分類できる．本研究において IPv6 対応を図った Opengate_v6 はネットワーク層において通信を制御する方式をとっている．

データリンク層において通信の制御を行うネットワーク利用者認証システムについては，通信路の開閉に IP アドレスを用いないため，特に IPv6 を考慮する必要はない．しかし，ネットワーク層において通信を制御するネットワーク利用者認証システムにおいては，IPv6 を考慮しなければならない．

ネットワーク層で通信を制御するシステムで IPv6 対応を図る場合は，本研究において用いた以下の手法や，考察は適用できると考えられる．

- IPv4/IPv6 アドレスの取得

- 通信路の開閉
- 通信状態の監視
- IPv6 の複数アドレスへの対応

7. ま と め

利用者認証ゲートウェイシステム “Opengate” の IPv6 対応に関する研究と開発を行った．今回，開発した Opengate_v6 は，動作実験において IPv4/IPv6 デュアルスタックネットワークで問題なく動作し，利用者端末において IPv6 を利用することが可能となった．IPv4 と IPv6 を同時に利用することが可能で，IPv6 アドレスを複数持つ利用者端末も利用可能である．

今後，IPv6 ネットワークの整備が進むにつれて，すでに導入されているネットワーク利用者認証システムの IPv6 対応が求められる．よって，本研究における IPv6 に対応するための手法は有用であると考えられる．

謝辞 システムの開発に際し，有益な議論をしていただいた，佐賀大学理工学部知能情報システム学科渡辺義明教授，佐賀大学総合情報基盤センター只木進一教授，江藤博文助手に感謝します．また，システムの運用実験に参加していただいた佐賀大学理工学部知能情報システム学科第 5 研究グループの皆様に感謝します．

なお本研究は，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) 石橋勇人，山井成良，安部広多，阪本 晃，松浦敏雄：利用者ごとのアクセス制御を実現する情報コンセント不正利用防止方式，情報処理学会論文誌，Vol.42, No.1, pp.79–88 (2001).
4) 西村浩二，秋成秀紀，野村嘉洋，相原玲二：遠隔機器制御プロトコルを用いた有線/無線 LAN 用情報コンセントシステム，情報処理学会論文誌，Vol.43, No.2, pp.662–670 (2002).
5) 広島大学総合情報処理センター「PortGuard」(2001). http://www.portguard.org/
6) 久長 穣，岡田 隆，刈谷丈治：情報コンセントのユーザ認証について，学術情報処理研究，No.2, pp.77–81 (1998).
7) 丸山 伸，浅野善男，辻 斉，藤井康雄，中村順一：既存の DHCP 端末で利用できる利用者にも管理者にも安全な情報コンセントシステムの構築，情報処理学会研究会報告 99-DSM-14，pp.131–136 (1999).
8) 江口勝彦，渡辺健次：Opengate の IPv6 対応に関する研究，情報処理学会研究報告，2004-DSM-36, pp.7–12 (2005).
9) 渡辺義明ほか：Opengate ホームページ. http://www.cc.saga-u.ac.jp/opengate/
10) 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).
11) 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).
12) 文京学院大学. http://www.shijokyo.or.jp/LINK/journal/0501/05_02.html
13) RFC3041 (Privacy Extensions for Stateless Address Auto configuration in IPv6).
14) RFC2461 (Neighbor Discovery for IPVersion 6 (IPv6)).

(平成 17 年 7 月 8 日受付)
(平成 18 年 2 月 1 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．同年同大学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講師．平成 18 年同大学総合情報基盤センター講師．博士（工学）．インターネットの研究に従事．

江口 勝彦

平成 16 年佐賀大学理工学部知能情報システム学科卒業．平成 18 年同大学大学院工学系研究科博士前期課程知能情報システム学専攻修了．インターネットの研究に従事．

渡辺　健次（正会員）

平成元年佐賀大学大学院理工学研究科物理学専攻修士課程修了．同年同大学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助手．平成8年同大学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．教育システム，インターネット，分散システム運用技術の研究に従事．博士（工学）．平成7年情報処理学会全国大会奨励賞，平成10年教育システム情報学会論文賞受賞．