ネットワーク利用者認証システム Opengate の改良と運用について

Improvement and operation of the network user authentication system Opengate

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

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

〒840-8502 佐賀市 本庄町 1 番地
1 Honjo, Saga, Saga 840-8502

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，学内において 2001 年より運用を行ってきた．この Opengate は， Web アクセスによって認証画面が提供される平易なインタフェースを持ち， 認証には POP3 や Radius サーバなどを利用することができる．認証によって 利用者端末には Java Applet が送信され利用状況を監視し， 利用が終了すると即時に通信路を閉鎖する．現在，この Opengate は IPv4/IPv6 のネットワークに対応し，学内において試験運用等を行っている．

これまでの運用経験をもとに従来の Opengate を見直し，改良を行った．本稿では，改良点である設定の統合や XML 化，IPv4/IPv6 アドレスの取得方式の変更などについて述べる．

キーワード：Opengate，ネットワーク認証，ファイアウォール，IPv6

We have developed and distributed a network user authentication system “Opengate”. It has been operated in Saga University since 2001. When a user accesses from his terminal to any web site through the gateway, the system returns the page for authentication instead. Various types of protocols, including POP3 and Radius, are applicable for authentication. After the authentication, the system sends Java Applet to the terminal and watches the usage. The new version of Opengate is compatible with IPv4/IPv6 network environment. And it is under experimental operation.

Based on the operation experience in the campus, we improved Opengate. This paper describes improvement of the acquisition method of IPv4/IPv6 address of the user terminal and integration of parameter setting to a XML-formed configuration file.

KEYWORDS: Opengate, Network Authentication, Firewall, IPv6

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．

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いる．2005 年には IPv6 ネットワークにおける利用にも対応し，一部運用を行ってきた [1, 2, 3]．

このような運用経験をもとに従来の Opengate を見直し，改良を行った．本稿では，改良点である設定の統合と XML 化，IPv4/IPv6 アドレスの取得方式の変更などついて述べる．また，その運用についても触れる．

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．

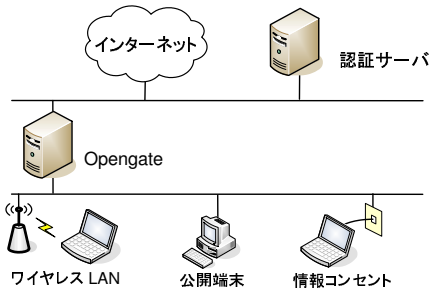

図 1　Opengate のシステム構成例

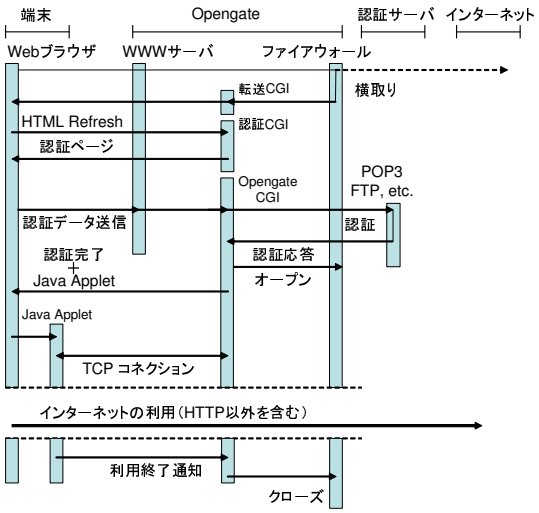

図 2　Opengate の動作の流れ

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 を用いてアクセスする．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．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．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．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 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 の改良

Opengate は，2001 年から安定して運用している．多数の利用者に活用され，佐賀大学における教育研究の不可欠な基盤となっている．一方で，IPv6 への対応など，機能拡張と改善を継続的に行っている．本節では，IPv6 への対応や機能拡張について述べる．

3.1 主要ページの CGI 化

従来の Opengate では，利用者 ID とパスワードを取得し認証を行う部分のみで CGI を利用していた．新 Opengate では，IPv6 ネットワークに対応するため，利用者端末の IPv4/IPv6 アドレスの受け渡しが必要となる．そこで，主要なページの CGI 化を行った．認証ページの表示と，利用者端末の IPv4/IPv6 アドレスの受け渡しの他, 時刻情報なども CGI を使って受け渡している．詳細は後述する．

3.2 IPv4/IPv6 アドレス取得方式

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路を，ファイアウォールによって開放する．よって，Opengate は，利用者端末が利用する IPv4/IPv6 アドレスを把握し，管理する必要がある．

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 を用いて通信する．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．この転送の通信は，必ず IPv4 によって行われる．この際に利用者端末の IPv4 アドレスを取得することができる．

もし利用者端末が IPv6 通信に対応し，かつ最初にアクセスした任意の Web サーバも IPv6 通信に対応していた場合は，最初の通信は IPv6 によって行われる．この通信をファイアウォールによって遮断すると，通常の Web ブラウザは自動的に同一の Web サーバに IPv4 によって再度通信を試みる．後はこの HTTP リクエストを自身の Web サーバへ転送することにより，利用者端末の IPv4 アドレスを取得することができる．

以上のように取得した 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 (html の meta タグ: http-

equiv=”Refresh”) 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 3.3 節において述べる．

ネットワーク利用者は，認証ページに利用者 ID とパスワードを入力する．これらの認証データは Opengate CGI に POST され，CGI は外部の認証サーバに対して認証を行う．この POST の際，利用者端末が IPv6 に対応しており，かつ POST 先の Opengate が IPv6 に対応していれば，IPv6 で通信が行われる．この際に利用者端末の IPv6 アドレスが取得できる．もし IPv4 で POST で行われた場合は，利用者端末の IPv4 アドレスが再度取得される．

また，先に引数によって取得された IPv4 アドレスは, POST の際に hidden タグを用いて Opengate CGI に渡される．

以上の利用者端末のアドレス取得の流れを，図 3 に示す．

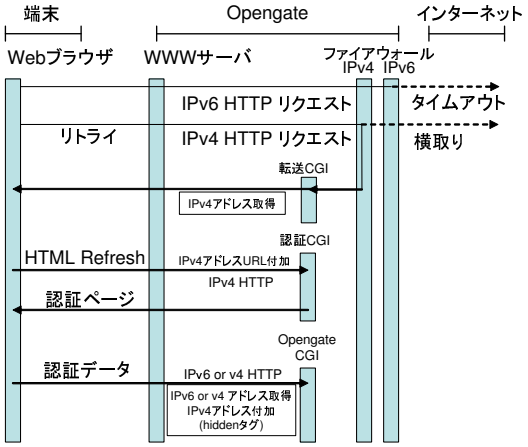

図 3　利用者端末のアドレス取得の流れ

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．

3.3　取得情報の受け渡し

新 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．

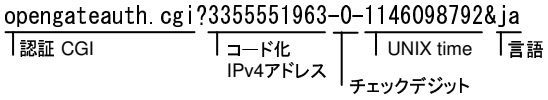

図 4　認証 CGI の引数フォーマット

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．

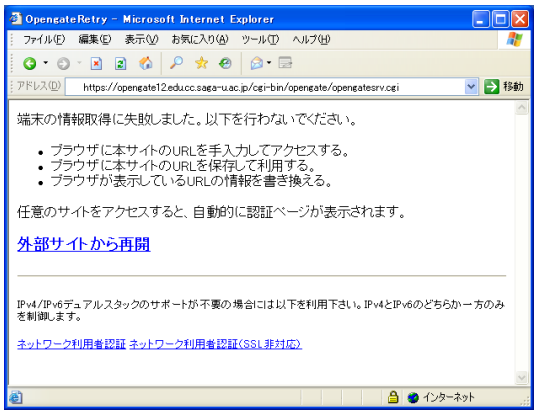

図 5　引数変更時の表示画面

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．

3.4　再認証による閉鎖

Opengate では，認証終了後に，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．

利用者端末に Java Applet が動作する Web ブラウザがない場合，ユーザが設定した時間経過後に通信路を閉鎖する．この通信路の開放時間は，設定で最大値が設定できるものの，長時間開放された場合の閉鎖手段が，従来の Opengate では用意されていなかった．しかし，新 Opengate では，再度認証ページから認証を行うことによって，能動的に通信路を閉鎖することが可能となっている．

4 設定の統合と XML 化

新 Opengate は，設定についても改良を行った．この節では，設定の統合と設定ファイルの XML 化について述べる．

4.1 設定ファイルの XML 化

従来の Opengate は，設定ファイルは termcap や printcap で使用されるケーパビリティデータベース形式を採用していた．新 Opengate は，設定ファイルの形式を XML とした．

従来の Opengate の設定は，ヘッダファイルやメイクファイル，設定ファイルに分散していた．これを一元化し，全ての設定が XML 形式の設定ファイルによって設定可能とした．この設定ファイルには，基本的に，Opengate の WWW サーバ名，認証サーバアドレスとそのプロトコルの 3 点のみを設定するだけで，利用可能である．

また，これらの設定は CGI の起動時に読み込まれる．従って設定変更は，その以降に接続してくる利用者端末に直ちに適用される．

4.2 利用者 ID と付加 ID による設定切り替え

従来の Opengate は，「利用者 ID@」の後に，認証サーバを指定することによって，認証サーバを切り替えることが可能であった．新 Opengate では特定の利用者 ID や付加 ID によって，個別に設定を切り替えることが可能である．

設定 1 に利用者 ID による設定切り替えの設定例を示す．利用者 ID が user1 及び user2 の場合は，認証を拒否し，ログを別 (syslog の Facility を local2) に生成する．

設定 1: 利用者 ID による設定切り替え

```
<ExtraSet ExtraId="default" \
        UserIdPattern="^user1$|^user2$">
    <AuthServer>
        <Protocol>deny</Protocol>
    </AuthServer>
    <Syslog>
        <Enable>1</Enable>
        <Facility>local2</Facility>
    </Syslog>
</ExtraSet>
```

設定 2 に，付加 ID による設定切り替えの設定例を示す．「ユーザ ID@」の後に，「guest」という付加 ID が付加される場合の設定例である．付加 ID として「guest」を付けた場合に，認証サーバを 192.168.0.1，プロトコルを POP3S，また最大利用許容時間が 1200 秒までとなる．

設定 2: 付加 ID による設定切り替え

```
<ExtraSet ExtraId="guest">
    <AuthServer>
        <Address>192.168.0.1</Address>
        <Protocol>pop3s</Protocol>
    </AuthServer>
    <Duration>
        <Default>1200</Default>
        <Max>1200</Max>
    </Duration>
</ExtraSet>
```

5 試験運用について

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，主に IPv6 に対する機能追加を行った Opengate の試験運用を開始した [3]．2006 年 8 月からは，本稿で報告した新 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．

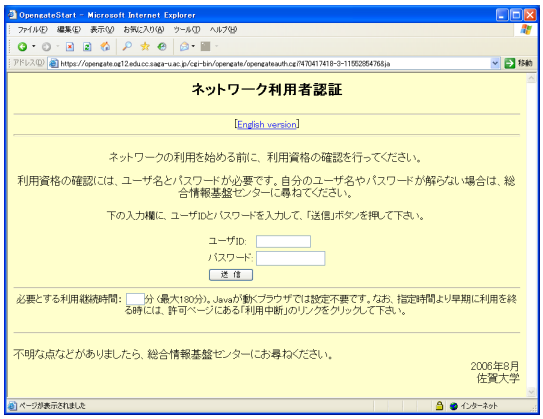

図 6　認証インタフェース

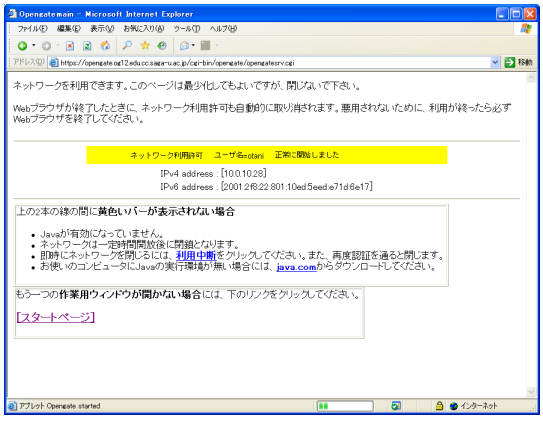

図 7　認証後の表示

6　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．

本稿では，ネットワーク利用を認証し，記録する “Opengate” の機能拡張と改善について報告した．特に，設定の統合及び XML 化と IPv6 への対応について報告した．

今後の課題としては，今回紹介した新 Opengate の全学的な運用があげられる．また新 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] 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)

[2] 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)

[3] 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)