情報処理学会論文誌　Vol. 50　No. 3　1–11 (Mar. 2009)

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[†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，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，学内で運用を行ってきた．この Opengate は，利用者が Web サイトにアクセスする際に，Web ブラウザに認証ページを強制的に表示させ，認証を行わせるシステムである．Opengate は，ネットワークの利用終了の即時検知に Java Applet を用いるため，Java の実行環境を持たない端末における利用終了の即時検知には対応していなかった．そこで，このような端末に対応するため，プラグイン等に依存せず HTTP の標準機能のみで利用終了の即時検知を実装した新たな Opengate を開発した．その結果，新たな Opengate は，ほとんど全ての Web ブラウザにおいて利用でき，キャンパス規模の運用においても利用可能であることを確認した．また，検知方式に関しては後方互換性を保って拡張を行うとともに，認証画面のインタフェースや利用方法もそのまま引き継いだため，従来システムから円滑に移行できた．本稿では，この新しいネットワーク利用者認証システム Opengate の詳細とその運用について述べる．

Development and Smooth Installation of a Network Authentication System with Detecting Usage Termination by Watching HTTP Connection

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

We have developed and distributed a network user authentication system “Opengate”. It has been operated in Saga University. When an user accesses from his/her terminal to any web site through the gateway, the system returns the page for authentication instead. After the authentication, the system sends Java Applet to the terminal and watches the usage. Therefore, on a terminal without Java plug-in, usage termination is not detected immediately. We developed new Opengate which solves this problem by only standard functions of HTTP without using plug-in etc. So, new Opengate can be used by various web browsers. And, service of new Opengate was started at our university, and verified that it operated in a large-scale network. The function of new Opengate was implemented by adding to the old Opengate. Old functions can be called when a trouble happens in the new function. And, the interface is the same as the old Opengate. So, the user can use the system without worrying about the change. This paper describes development and management of the new Opengate capable of detecting usage termination.

1. まえがき

近年，多くの大学において，コンピュータリテラシ教育やコンピュータの利用を支援するために，自由に利用できる公開端末や，個人所有のノート PC が接続可能な情報コンセント，無線 LAN などの設置が進んでいる．しかし，これらは手軽に利用できる反面，不正利用に起因するトラブルが発生しやすい．よって，利用者を有資格者に限定するとともに，その利用を記録する仕組みが必要である．

また，利用記録だけではなく，利用終了を即時に検知し，ネットワークを閉鎖することが重要となる．公開端末では，同一の端末を複数の利用者が共用するため，ネットワークの利用終了を即時に検知しなければ，利用者を特定することが困難となる．個人所有のノート PC をネットワークに接続して利用する場合も，利用を終了してからネットワークが閉鎖されるまでの間に，利用資格のない者がそれまで接続されていた端末情報を偽装し，ネットワークを不正に利用するといったことが考えられる．よって，利用者を有資格者のみに制限し，また特定するためには，利用終了を即時に検知する仕組みが必要になる．

このような仕組みを実現する 1 つの方法として，認証に対応したスイッチを導入する方法がある．この方法では，専用の機器の導入が必要であり，ネットワーク規模の大きな大学などでは，導入コストが掛かるとともに，保守・運用コストが発生する場合も考えられる1),2)．無線 LAN を利用できる端末では，WEP や WPA-TKIP などのセキュリティ機能

[†1] 佐賀大学 総合情報基盤センター
Computer andNetworkCenter，Saga University
[†2] 佐賀大学 理工学部
Faculty of Science and Engineering，Saga University

を使って，認証の仕組みを実現可能であるが，対応アクセスポイントの整備，利用指導などの運用コストや互換性の問題が生じてしまう．

そこで現在は，Web ブラウザを使った Captive Portal 型のネットワーク利用者認証システムが一般的に多く利用されている3)–5)．認証に Web ブラウザのみを用いるため，利用者にも使いやすく，管理も容易である．

佐賀大学では，Opengate と呼ばれる Web ブラウザを使った Captive Portal 型のネットワーク利用者認証システムを開発・公開している．また，学内において全学規模で運用を行っている6)–8)．この Opengate は，認証に Web ブラウザを用いることにより，公開端末や個人所有のノート PC などの様々な種類の端末利用者に，共通の認証機構を提供する．認証には既設の LDAP や RADIUS サーバなどの認証サーバを利用することができる．

しかし Opengate では，利用者のネットワークの利用終了の即時検知に Java Applet を用いていたため，Java の実行環境のない端末では，事前に環境を導入する必要性があり，これに伴う指導も必要であった．そこで新たに，HTTP の標準機能のみを用いる利用終了の即時検知の手法を開発した．この手法では，Java Applet を用いる事なく，認証を行った Web ブラウザと Opengate サーバ間で HTTP コネクションの維持する．そして，この HTTP コネクションの切断を検知することで，ネットワークの利用終了と判断する．

また，この新たな Opengate を全学規模で導入し，運用した．Opengate は既に数年にわたり教育研究の現場で利用しているため，円滑に移行が行えるように後方互換性を保って拡張を行うとともに，認証画面のインタフェースも従来のものを引き継ぐなどの配慮を行った．これにより，新たな Opengate の導入後も，利用者がその導入を意識せずにネットワークを利用できた．

本稿では，HTTP の標準機能のみを利用した終了検知 (以下，HTTP による利用終了の検知) を行う Opengate の詳細と佐賀大学における運用，考察を述べる．

2. Opengate の概要

2.1 概　　要

Opengate は，佐賀大学において開発され，2001 年から学内において全学規模で運用を行っている．また 2005 年からは，IPv6 に対応した Opengate の運用も行っている9)．Opengate が設置されたネットワークでは，Web ブラウザさえあれば，特別な申請やソフトウェアの準備なしに，有資格者のみが，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** に，ソフトウェアの構成を**図 2** に示す．また，認証時のインタフェースと認証後の表示をそれぞれ，**図 3**，**図 4** に示す．

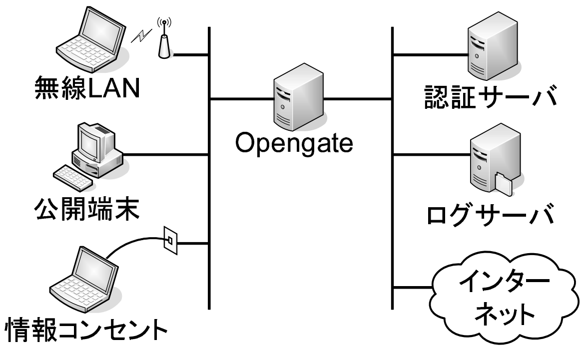

図 1　Opengate のシステム構成例
Fig. 1　Sample configuration of Opengate system

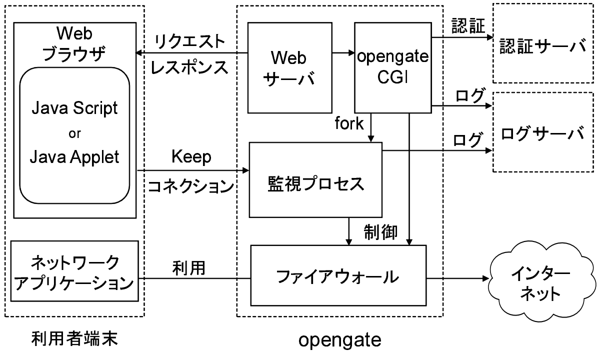

図 2　Opengate のソフトウェア構成
Fig. 2　Opengate software architecture

2.2 動　　作

Opengate は，利用者端末を接続するネットワークに，ゲートウェイとして設置され，次のように動作する．

ネットワーク利用者が，始めに任意の Web サイトにアクセスした際に，Opengate はその通信を奪い取り，代わりにネットワーク利用の認証ページを利用者の Web ブラウザに提供する．利用者は，この認証ページに利用者 ID とパスワードを入力する．この認証の際に，

ネットワーク利用者認証

[English version]

ネットワークの利用を始める前に、利用資格の確認を行ってください。

利用資格の確認には、ユーザ名とパスワードが必要です。自分のユーザ名やパスワードが解らない場合は、総合情報基盤センターに尋ねてください。

下の入力欄に、ユーザIDとパスワードを入力して、「送信」ボタンを押して下さい。

ユーザID: otani
パスワード: ●●●●●●●●●

以下は、切断が頻発して利用継続できない場合に限って設定して下さい（推奨されません）。
必要とする利用継続時間: □ 分(指定可能:1〜60分)。この時間が経過するまで、ネットワークをあなたの利用資格で開放しています。あなたが去った後で他人が不正利用すると、それに伴うトラブルに巻き込まれます。指定した時間より前に利用を終わるには、許可ページにある「利用中断」のリンクをクリックして下さい。

不明な点などがありましたら、ネットワーク管理者にお尋ねください。
佐賀大学

図 3　認証インタフェース
Fig. 3　Authentication interface

Web ブラウザで SSL(HTTPS) 通信が可能であれば，利用者 ID とパスワードは，SSL によって暗号化されて Opengate に送信される．Opengate は，入力された利用者情報を認証サーバへ問い合わせ，認証に成功した場合，当該端末の IP アドレスの開放ルールをファイアウォールに加える．

従来の Opengate では，認証成功後，認証完了ページとともに Web ブラウザに Java Applet をダウンロードさせる．Opengate は利用者端末ごとの監視プロセスを起動する．Java Applet はこの監視プロセスとの間に，TCP コネクションを維持することによって，ネットワークの利用を監視する．利用者が Web ブラウザを終了，もしくは利用者端末の OS が終了すると，TCP コネクションが切断される．その切断を Opengate の監視プロセスが検知し，ファイアウォールの開放ルールを削除する．

なお，HTTP 以外の通信プロトコルも，まず始めに Web ブラウザで任意の Web サーバへアクセスし，認証を行えば利用できる．

Opengate は，FreeBSD 上で動作し，ファイアウォールには ipfw/ip6fw，Web サーバには Apache を利用する．制御を行うプログラムは，C 言語で開発している．この他の Opengate の詳細については，参考文献6)–10) を参照されたい．

ネットワークを利用できます。

利用が終ったら必ずWebブラウザを終了してください。ネットワーク利用許可も自動的に取り消されます。

このページを移動したり閉じたりすると、ネットワークが閉鎖されます。

Webの利用には下のボタンを押して表示される別ウインドウを使ってください。

または、このページを最小化しておいて、別プログラムでネットワークを利用してください。

ネットワーク利用許可　ユーザ名 otani　接続確認　16:01

上の2本の線の間に黄色のバーが表示されなかったりネットワークが閉鎖されるなど動作がおかしい場合は、利用中断 をクリックしてからブラウザを終了してください。また認証ページが表示されない場合は、通常とは別のページをアクセスしてみてください。

図 4　認証後の表示
Fig. 4　Web page displayed after authentication

3. HTTP による利用終了の検知を行う新たな Opengate

3.1　Java Applet による終了検知の問題点と新たな検知方法

第 2.2 節で述べたように，従来の Opengate では，利用者端末の Web ブラウザに送った Java Applet と監視プロセスとの間の TCP コネクションを監視し，そのコネクションの終了によって，利用の終了を即時に検知する仕組みを導入していた．

Opengate を設置したネットワークで利用される端末の多くは，学生や教職員が個人で所有するノート PC であるが，これらの端末の多くには，購入時から Java の実行環境が導入されていたため，Java Applet による即時検知が有効に機能した．しかし，近年の利用者端末の多くは，購入時にあらかじめ Java の実行環境が導入されていない．このような端末で即時検知を行うためには，Opengate の利用前に Java の実行環境を導入する必要性があり，これに伴う指導も必要であった．

そこで HTTP の標準機能のみで利用終了を検知する仕組みを実装した．本来，HTTP は，一度のデータ送受信で切断される一過性の TCP コネクションを用いる．よって，その TCP コネクションの終了をもって利用終了とすることはできない．しかし HTTP/1.111) において，HTTP Keep-Alive 機能が追加され，多くの Web ブラウザに実装されている．そこで HTTP アクセスを繰り返し，HTTP Keep-Alive によって TCP コネクションを維持し，こ

れを監視する方法を試した．しかし HTTP Keep-Alive によって TCP コネクションを維持する時間は Web ブラウザに大きく依存することが分かった．

HTTP Keep-Alive による TCP コネクションは，一定時間以上データのやり取りを行わなわなければ，タイムアウトとなり切断される．このタイムアウトまでの時間は，Web ブラウザによって大きく異なる．また，Web ブラウザ (Safari2 等) によっては，利用状態に関係なく一定時間 (30 秒) で切断されてしまう．このように，Web ブラウザによって，TCP コネクションを維持可能な時間が異なるため，HTTP Keep-Alive のみでは，TCP コネクションの長時間維持が困難である．

これに対応するため，HTTP の応答を遅延することで，HTTP Keep-Alive による維持時間を短くしたまま，繰り返しの周期を延ばす手法を考案した．

Opengate では，Web ブラウザと定期的に hello メッセージの交換を行う．Web ブラウザからの hello メッセージに対して監視プロセスが一定時間遅延させて返答する．この際の応答 (HTTP 遅延応答) までの時間は，HTTP Keep-Alive ではなく，Web ブラウザの標準的な機能によって TCP コネクションの維持が可能である．Web ブラウザが応答を受けて, 再度 hello メッセージを送信する短時間の間は，HTTP Keep-Alive による TCP コネクションの維持が可能である．

このように HTTP 遅延応答を HTTP Keep-Alive と併用することによって，TCP コネクションの長時間維持を実現した．HTTP の応答遅延を許容する時間長もまたブラウザに依存したが，この時間長が短い Web ブラウザ (Safari3) でも 60 秒程度維持できる．ただし，Opengate は遅延応答の間隔で利用者端末の生存確認を行うため，標準設定で 30 秒の遅延応答を行うこととした (第 3.3 節)．

この手法は，標準の HTTP のみで TCP コネクションを維持することができるため，追加プラグインや拡張機能を持たない標準的な Web ブラウザのみで動作させることができる．

3.2　HTTP による利用終了の検知

実装した HTTP による利用監視を行う際の動作を，以下に述べる (**図 5**)．

(1)　認証終了後，Opengate CGI は，許可ページを Web ブラウザに送信するとともに，監視プロセスを起動する．

(2)　許可ページ内において JavaScript を実行し，監視プロセスに対して監視ページを要求する．

(3)　監視プロセスは，監視ページを Web ブラウザに送信する．

(4)　監視ページ内において JavaScript を実行する．JavaScript は，サーバと非同期で HTTP 通信を行うための “XMLHttpRequest” を発行し，監視プロセスに対して “hello メッセージ” を送信する．

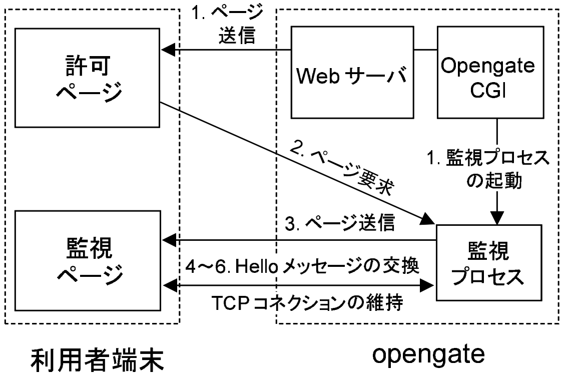

図 5　利用監視の動作
Fig. 5　The operation of watching the usage

(5)　監視プロセスは，XMLHttpRequest による hello メッセージに対して，一定時間 (標準設定で 30 秒) 遅延させ，返答する．これが HTTP 遅延応答である．

(6)　Web ブラウザは，hello メッセージに対する返答を監視プロセスから受け取ったら，すぐに次の XMLHttpRequest を発行し，hello メッセージを送信する．以降は (4) の hello メッセージ送信からの処理を繰り返す．この HTTP コネクションは，HTTP Keep-Alive によって永続的に維持される．

XMLHttpRequest から応答 (HTTP 遅延応答) までの間は，Web ブラウザの標準的な機能によって TCP コネクションは維持され，(6) における返答を受けて再度 XMLHttpRequest を発行する間も，HTTP Keep-Alive によって TCP コネクションが維持されると期待できる．監視プロセスは，この間 TCP コネクションを監視し続ける．この TCP コネクションが切断されたら，これを検知し，利用者がネットワーク利用を終了したと判断する．

なお，上記動作において許可ページと監視ページを分離したのは以下の理由による．一部のブラウザでは，ページを取得したポート番号 (Web サーバ) と，そのページからの XMLHttpRequest 先のポート番号 (監視プロセス) が異なると，XMLHttpRequest を発行できない．この問題を解決するため，許可ページ内で監視プロセスに対して XMLHttpRequest の発行を記述したページ (監視ページ) を要求し，受け取ったページで XMLHttpRequest

の発行を行うことにより同一ポート番号とした．

3.3 動作検証

HTTPによる検知方法は，認証成功後にWebブラウザとOpengateとの間に，HTTPによるTCPコネクションを維持する．そして，Webブラウザが正常に終了した際のTCPコネクションの切断をOpengateで検知することによって，通信路を閉鎖する．よって，LANのパケット伝送遅延程度の時間で即時に通信路を閉鎖することが可能である．

ただし，この検知方式は，Webブラウザが直接制御するHTTPコネクションを利用する．このため独自のTCPコネクションを新規に作成し利用するJava Appletによる検知よりも，Webブラウザの挙動の影響を受けやすい．そこで，現在多く利用されている各種の端末(PC, PDAなど)，OS (Windows, Mac OS, Linuxなど)やWebブラウザでTCPコネクションが長期間維持できるかの動作検証を行った．

その結果，主にPC端末で利用される主要なWebブラウザ(Internet Explorer, Firefox, Opera,Safariなど)においては，Webブラウザの終了後にLANのパケット伝送遅延程度(おおよそ1秒程度)の短時間に正常に通信路が閉鎖されることが確認できた．

また，HTTPによる検知方式が正常に利用できないWebブラウザとして，Windows CE.NETで利用されるInternet Explorer 4.0，Palm OSで利用されるWebPro，PlayStation Portable(PSP)やZaurusで利用されるNetFrontを確認した．これらのWebブラウザがHTTPによる検知方式を正常に利用できない理由は，JavaScriptや，HTTP Keep-Aliveの機能が実装されていないのが原因と考えられる．また，シングルタスクOSの端末では，TCPコネクションを維持しているWebブラウザと,他のネットワークアプリケーションを同時に利用できない場合があるため，これも正常に利用できない原因の1つである．

しかしながら，Webブラウザの世界的な利用シェアを考えると，利用者端末の約99.90%以上(2008年2月)$^{12)}$で問題ないと考える．

ただし，利用者は必ずしも，Webブラウザを閉じることによってネットワークの利用を終了するとは限らない．Webブラウザを閉じる前に，LANケーブルを外したり，無線LANの通信範囲外にPCを運んでしまうとこも考えられる．また，PCを休止状態やスリープ状態にしてPCの利用を終了する場合も考えられる．

そこで，このような状態に対応するために，WebブラウザとOpengateは，HTTPによるTCPコネクションを維持するとともに，そのTCPコネクションを利用し定期的に“helloメッセージ”を交換する．この交換が行われなくなった場合も，利用終了と判断する．この方法は，Webブラウザを正常に終了した場合の閉鎖と比べ遅延した閉鎖となるが，この仕組みも正常に動作していることを確認した．

なお，helloメッセージの交換については，負荷軽減の目的もあり，SSL(HTTPS)による暗号化を行っていない．TCPコネクションの乗っ取りなどのセキュリティ対策を考えた場合，SSL(HTTPS)による暗号化は有用であると考えられるが，これについては動作検証とともに今後の課題である．

4. 他の終了検知方法とその併用

4.1 実装した終了検知方法

第3.3節で述べたように，現在利用されているほぼ全てのWebブラウザで，新たなOpengateのHTTPによる終了検知が利用できる．しかし，新たなOpengateを実際に運用することを考えると，更に多種多用なWebブラウザが利用されることを想定しなければならない．特に，HTTPによる終了検知で利用しているHTTP Keep-AliveはHTTP/1.1から標準となっているため，HTTP Keep-Aliveが実装されていない古いWebブラウザが利用されることも考えられる．またシングルタスクOSの端末では，HTTPによる検知方式に対応していても，TCPコネクションを維持しているWebブラウザと,他のネットワークアプリケーションを同時に利用できない場合がある．

このようなHTTPによる検知方法が利用できないWebブラウザが利用されることも想定し，HTTPによる終了検知を標準的な検知方法としながら，以下の6つの検知方法を組み合わせて利用することで，様々なWebブラウザに対応した．

- HTTP-CLOSED

  HTTPが維持するTCPコネクションの切断を検知する方法である．これは，第3.2節で説明した方法である．この方法は，利用終了が即時に検知できる．この方法を標準的な検知方法とする．

- JAVA-CLOSED

  クライアントに送付したJava Appletとの間に維持するTCPコネクションの切断を検知する方法である．これは，第2.2節で説明した従来のOpengateの検知方法である．この方法も，利用終了が即時に検知できる．

- MAC-CHANGED

  MACアドレスが変更されたことを検知する方法である．端末のMACアドレスをARP (Address Resolution Protocol)によって定期的にチェックし，MACアドレスの変更があったら，利用終了と判断する．

- NO-PACKET
  利用者端末が送受するパケットが長期にわたって無いことを検知する方法である．ファイアウォールを通過するパケット数を定期的に調べ，長期に渡って利用者端末からのパケットが検知されなければ，利用終了と判断する．これによって，ネットワークを利用せずに長時間放置した端末の通信路の閉鎖を行う．
- TIME-EXCEEDED
  利用者が入力した利用時間が経過したことをチェックする方式である．認証情報取得の際に，希望する利用時間を認証ページより利用者から得て，その時間だけネットワークを利用可能とする．ただし設定限度 (標準設定で 60 分) を設けて，一時的利用に限定する．
- LINK-CLICKED
  利用者が利用終了リンクをクリックしたことをチェックする方式である．認証成功後の利用許可ページに利用中断を依頼するためのリンクを設置する．これを利用者がクリックすると，利用終了と判断する．

4.2　検知方法の併用と選択手順

Opengate は，HTTP-CLOSED による検知が主である HTTP 監視モード，JAVA-CLOSED が主である JAVA 監視モード，それらが利用できないときの BASIC 監視モードの，3 つの監視モードを持ち，それらを自動的に選択する．以下に，第 3.2 節で示した HTTP による利用終了の検知方法を拡張した，自動選択の流れを示す．

(1)　Opengate は，認証後に許可ページをクライアントに送るとともに，監視プロセスを起動する．

(2)　許可ページでは，監視ページへの自動移動を行う JavaScript が動く．自動移行が失敗した場合には，Java Applet が起動する．Java Applet の起動にも失敗した場合は，(7) に移行する．

(3)　監視プロセスは，クライアントからの接続要求を待ち受け，自動移動に対応するページ要求があれば，監視ページを送付する．

(4)　監視ページでは，XMLHttpRequest の発行と受信を繰り返す JavaScript が動く．XMLHttpRequest の発行が失敗した場合には Java Applet が起動する．Java Applet の起動にも失敗した場合は，(7) に移行する．

(5)　監視プロセスは，監視ページとの XMLHttpRequest 交信が可能であることを確認した後に HTTP 監視モードに移る．HTTP 監視モードでは，hello メッセージの受信と遅延応答（標準設定で 30 秒）を繰り返す．HTTP-CLOSED または MAC-CHANGED が検出された場合はネットワークを閉鎖し終了する．

(6)　監視プロセスは，クライアントからの接続を待ち受けている際に，Java Applet からの接続要求があれば，JAVA 監視モードに移る．JAVA 監視モードでは，hello メッセージの送受信を一定間隔（標準設定で 30 秒）で繰り返す．JAVA-CLOSED または MAC-CHANGED が検出された場合はネットワークを閉鎖し終了する．

(7)　監視プロセスに対して接続要求がない場合や，あらかじめ利用時間が入力されていた場合は，BASIC 監視モードとして動作する．BASIC 監視モードでは，MAC-CHANGED, NO-PACKET, TIME-EXCEEDED, LINK-CLICKED のいずれかを検出するとネットワークを閉鎖し終了する．

すなわち，JavaScript が実行可能で，XMLHttpRequest の発行も可能な場合は，HTTP 監視モードが自動的に選択される．HTTP 監視モードが利用できず，Java Applet の実行が可能な場合は，JAVA 監視モードが自動的に選択される．HTTP 監視モードおよび JAVA 監視モードがともに利用できない場合は，BASIC 監視モードとなる．

4.3　後方互換性の確保

新たな Opengate では，互換性の確保のために，さらに以下の機能を追加した．

- HTTP/1.1 に非対応な Web ブラウザを検知し，自動的に HTTP 監視モードを無効にする機能
- 不具合を起こす Web ブラウザを設定ファイルに記述することで，その Web ブラウザ利用時に HTTP 監視モードを無効にする機能
- 標準で利用する監視モードを設定ファイルによって変更できる機能
  通常は，標準で HTTP 監視モードが利用されるが，設定ファイルによって標準で利用する監視モードを JAVA または BASIC に変更できる機能である．
- 利用者から能動的に BASIC 監視モードを選択できる機能
  利用者が認証時に利用時間を入力すると，自動的に BASIC 監視モードが選択される機能である．

  以上の機能によって，HTTP による監視モードが正常に利用できない Web ブラウザなどに柔軟に対応することが可能である．

5.　従来の Opengate からの円滑な移行

佐賀大学では，全学規模で安定かつ低運用コストでサービスを行うために，若干の設定だ

表 1　Opengate の利用者
Table 1　User of Opengate

	利用者数	利用回数
学生	1,814 (86.88%)	41,485 (81.66%)
教職員	250 (11.97%)	8,996 (17.71%)
学外一時利用者	24 (1.15%)	322 (0.63%)

けが異なる多数の Opengate をディスクレスで運用する仕組みを導入している．これまで，ソフトウェアのバグも無く安定的にサービスを行っている8)．

2007年4月から，新たな Opengate に移行し，ディスクレスによる運用を開始した．ディスクレスのブートイメージに，新たな Opengate を導入した後，ディスクレス環境の再起動を行った．再起動による10分程度のサービス停止が必要となったが，停止を事前にアナウンスしていたこともあり，円滑に導入作業を行うことができた．導入後，利用トラブルや利用の問い合わせも特になく，これまで不具合によるサービスの停止も一度も起きていない．

新たな Opengate は，利用終了の検知方法が異なるものの，インタフェース (図3, 図4) やその利用方法は，従来の Opengate と同じになるよう開発した．よって，利用者は新たな Opengate の導入後も，利用終了の検知方法の違いを意識せず，従来の Opengate と同じように利用できる．このため，導入に伴う新たな利用指導も特に必要なく，使い方の問い合わせなども，新たに発生しなかった．

6. 新たな Opengate の利用状況

Opengate の利用対象者は，佐賀大学の構成員である学生 (約7,500人)，教職員 (約1,500名)，学外一時利用者で，これまでの運用では，月平均で約2〜3万回の利用がある．新たな Opengate の2ヶ月間 (2007年10月〜11月) の利用者は2,088人で，利用回数はのべ50,803回であった．その利用者のうち，86.88 % (**表 1**) が学生であった．

同期間における，利用開始時刻 (1時間ごと) と利用日 (曜日) のヒストグラムを**図 6** に示す．利用の多くが平日であり，その利用開始時刻も授業時間 (8時40分〜17時40分) であるため，学生が授業で利用しているものと思われる．

また，HTTP 監視モードおよび JAVA 監視モードでの Opengate の利用時間 (秒) のヒストグラム (60秒ごと) を**図 7**，**図 8** に示す．HTTP 監視モードによる利用時間 (平均 2.06 時間) が，JAVA 監視モードの利用時間 (平均 1.24 時間) に比べ比較的長いことが分かった．また，HTTP 監視モードの導入による利用トラブルも発生しなかった．

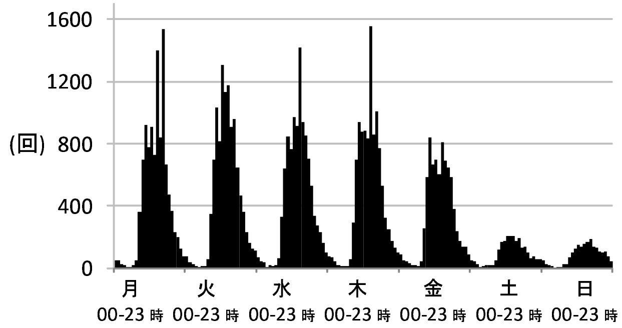

図 6　利用開始時刻，利用日のヒストグラム
Fig. 6　Histogram of time to start network usage

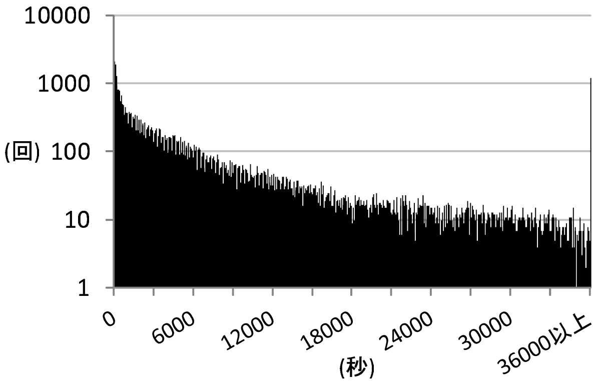

図 7　利用時間 (秒) のヒストグラム (HTTP 監視モード)
Fig. 7　Histogram of usage duration in HTTP mode(sec.)

以上の Opengate の運用状況から，HTTP による終了検知が実運用でも問題なく利用できることが確認できた．

7. 考　察

7.1 HTTP による利用終了の即時検知の有用性

佐賀大学での運用において，従来の Opengate では，利用の約 24.50%(2007年1月の統

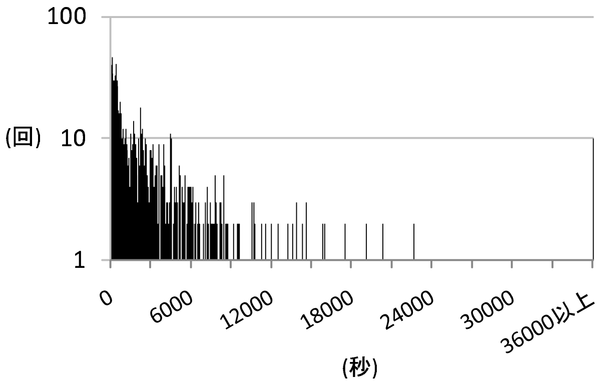

図 8　利用時間 (秒) のヒストグラム (JAVA 監視モード)
Fig. 8　Histogram of usage duration in JAVA mode(sec.)

計) で，Java Applet による利用終了の即時検知ができていなかった．

Opengate の利用記録には，認証時に利用した Web ブラウザも記録される．利用記録から判断すると，その多くが個人所有のノート PC であり Java の実行環境が導入されていない一般的な Web ブラウザを用いて認証を行ったものと思われる．

新たな Opengate では，利用者が認証時に利用時間を入力 (能動的に BASIC 監視モードを選択) しなければ，通常 HTTP または JAVA 監視モードが選択され，利用終了の即時検知が行われる．もし即時検知ができない場合は，BASIC 監視モードが自動選択され，どのモードが利用されたかは，利用履歴として記録される．

2ヶ月の同期間において，即時検知が利用できずに遅延閉鎖 (BASIC 監視モード) となった利用の割合は，利用履歴から約 1.72 %であった．また利用履歴から得られる利用者端末の OS および Web ブラウザの情報から，即時検知できなかった利用の多くは，Java Applet や HTTP Keep-Alive がサポートされていない Web ブラウザを利用する端末 (PDA など) であったため，遅延閉鎖が自動的に選択されたものと思われる．即時に利用終了を検知できない利用者端末は存在するものの，即時検知率が大きく向上した．この向上は，HTTP による利用終了の即時検知が，Web ブラウザの標準的な機能のみで実装されているためである．よって，HTTP による利用終了の即時検知は，Opengate において有効に機能していると考えられる．

7.2　その他の利用終了の即時検知手法の検討

Web ブラウザを用いて，TCP コネクションの維持が可能なものとして，Java Applet の他に，Adobe 社の Flash プラグインや，Microsoft 社の ActiveX アドオンなどがある．Flash プラグインは，Java Applet よりも普及しているが，Java と同様に，実行環境の事前導入が必要である．また，Flash 等のプラグインは，頻繁にバージョンアップが行われる．このため，バージョンアップを行う際に，TCP コネクションの維持ができず，利用終了と判断してしまう可能性がある．また，ActiveX は，利用できる Web ブラウザの種類が少ない．

7.3　Ajax および Comet との関係

HTTP の標準機能のみを用いて高度なアプリケーションを実現する技術として Ajax13) および Comet14),15) が注目されている．Ajax は，ページ遷移を伴わずに非同期通信を行いページ内容を更新する技術の総称であり，Comet はサーバ側で発生したイベントをブラウザ側にプッシュ配信する技術の総称である．新たな Opengate は，ページ遷移を伴わずに通信を行っている点で Ajax の一つといえる．また，Comet の実現方法の一つである long-poll15) と類似の通信手順を取っている．

long-poll では，Web クライアントから要求を受けた Web サーバが，その応答を保留し，Web サーバ側でのイベント発生時に応答する．Web クライアントは応答を受けた後に Web サーバに再度要求を送る．すなわち保留した応答をイベント発生時に返すことでサーバプッシュ機能を実現している．

新たな Opengate も long-poll と同様に HTTP の応答を保留する．しかし Web サーバ側のイベント処理は実装していない．Web ブラウザの終了検知のために TCP コネクションを監視し，一定時間後に応答する処理を行う．

以上のように，新たな Opengate は long-poll と類似の通信手順を取っているが，Comet が目的とするサーバプッシュを目的とするものではない．本研究の目的は，セキュリティと利便性が両立する利用者認証システムを実現することであり，実際に運用を行って，その手法の有用性を検証できている．

7.4　起動速度の高速化

HTTP による利用終了の即時検知では，Java の実行環境の起動を必要としないため，従来の Opengate と比べ，端末側の起動速度が高速化すると考えられる．実際の運用においても，その起動速度の高速化が確認できた．

佐賀大学での 2ヶ月の運用において，Java Applet を利用した方法では，端末側の起動時間が平均で約 11.89 秒であったが，HTTP による方法では平均で約 1.98 秒となり，起動

時間が大幅に減少した．これらの結果は，利用される端末の性能によっても影響されるが，利用者の待ち時間の減少が確認できた．

7.5 運　用

Opengate では，認証に Web ブラウザを用いる．このため，Web 以外の通信を行う場合にも，まず始めに Web ブラウザ起動し，認証を行う必要がある．また，利用者端末に IP アドレスを自動的に割り当てる場合は，利用者端末において，自動割り当てが有効になっていなければならない．よって，Opengate によるネットワークを運用する場合，これらの利用方法は，あらかじめ周知しておく必要がある．

しかし，近年，個人所有 PC のネットワークの利用の多くは Web であり，ネットワークの設定も自動設定となっている場合が多い．佐賀大学の運用においては，Opengate の利用方法を主に Web ページに掲載しているのみだが，Opengate の利用に関する問い合わせなどは，ほとんど発生していない．

ただし，Opengate ではブラウザの終了を検知することにより，通信路を閉鎖するため，Web ブラウザを誤って閉じてしまった場合は，通信路が閉鎖しまう．認証後に表示される許可ページから移動してしまった場合も同様である．この場合，利用者に再認証の手間が発生してしまう．このような利用者認証に関わる手間の軽減は今後の課題である．

7.6 新たな Opengate の有用性

近年，空港やホテル，大学などにおいて Apresia(1) や，POPCHAT(2) といった製品を使用して，ネットワークの接続サービスを提供するところが増えてきている．

これらの製品の多くは，Opengate と同様，Web インタフェースを用いるものが多いが，認証時に特定の URL へのアクセスが必要なものや，MAC アドレスのみで利用者端末を識別するもの，一定時間経過後に再度利用認証が必要であったり，利用終了後もネットワークが一定時間開放されたままになったりするものがあるなど，利用目的によっては不便な場合やセキュリティ上の問題が発生する場合がある．またネットワークの規模によっては，これら製品の導入・保守費用などのコストが発生する．

大学においても，これらネットワーク利用者認証を行うシステムが研究されており，目的に応じて有用に利用されている16)–19)．しかし，これらのシステムにおいても，製品化されたシステムと同様に，MAC アドレスのみで利用者端末を識別していたり，利用終了後もネットワークが一定時間開放されるといった問題が生じる場合がある．

Opengate は，全てオープンソースソフトウエアで構成され，認証も LDAP や POP，Radius や PAM など多くの認証に対応し，既存のネットワークにシームレスな導入が容易である．また，一度の認証でネットワークを長時間利用可能で，利用終了時には認証ページを閉じることによって，ネットワークが即時閉鎖するため，ネットワークが不正に利用される危険性も少ない．

利用者端末や公開端末からの不正利用を防ぐためには，利用者のネットワークの利用終了を即時に検知し，ネットワークを閉鎖することが重要である．本稿における即時検知の手法は，一般的な Web ブラウザの標準機能のみを用いて実現するものであり，導入の際に特殊な装置も必要としない．

よって，新たな Opengate は，新規に認証機器の整備が困難なネットワーク環境において，導入が容易で，セキュリティと利便性を両立可能な認証システムの１つとして有用に機能すると考えられる．

8. まとめ

本稿では，HTTP による利用終了の即時検知を行う新たな Opengate について述べた．

従来の Opengate は，利用終了の即時検知に Java Applet を用いていたため，Java 環境を持たない端末における利用終了の即時検知に対応できなかった．この問題の解決のために，HTTP の標準機能のみを用いた利用終了検知機能を実装した，新たな Opengate を開発した．これにより，Java 環境が導入されていない利用者端末への対応が可能となり，より多くの利用者端末で即時検知が可能となった．

また，Java Applet を利用しないため，端末側の起動が高速化し，利用者端末の負荷軽減にも繋がった．その他に，従来の Opengate と利用方法を変えていないため，移行も円滑に行うことができた．

この新たな Opengate は，導入の際に特殊な装置を必要とせず，認証も標準的な Web ブラウザのみで行うことができる．よって，新規に認証機器の整備が困難なネットワーク環境において，有用な利用者認証システムであると考えられる．

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) 日立電線 APRESIA , http://www.apresia.jp/
2) POPCHAT , http://www.popchat.jp/
3) 無線 LAN サービス HOTSPOT, `http://www.hotspot.ne.jp`

4) 公衆無線 LAN サービス BB ポイント，`http://www.softbanktelecom.co.jp/consumer/wlan/`
5) ドコモ公衆無線 LAN サービス MZONE, `http://www.nttdocomo.co.jp/service/data/mzone/`
6) 渡辺義明 他 : 「Opengate ホームページ」，`http://www.cc.saga-u.ac.jp/opengate/`
7) 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).
8) 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).
9) 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).
10) 大谷誠，江藤博文，渡辺健次，只木進一，渡辺義明: “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”， 情報処理学会 DSM 研究会，2006-DSM-43 (2006).
11) Request for Comments: 2616 , Hypertext Transfer Protocol - HTTP/1.1 (1999).
12) OneStat.com, “News and press releases: Mozilla’s Firefox global usage share is still growing”, `http://www.onestat.com/html/aboutus_pressbox.html`
13) Ajax アプリケーション & Web セキュリティ, Christopher Wells 著, 牧野 聡訳, オライリー・ジャパン (2008)
14) Comet: Low Latency Data for the Browser, `http://alex.dojotoolkit.org/?p=545`
15) 技術レポート: Web アプリケーション Push 型技術について (Comet,Long-poll), P・A NetWork Laboratory Co., Ltd., `http://www.panet.co.jp/report/`
16) 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).
17) 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).
18) 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 (1999).
19) 福田浩章, 山本喜一, “XFW:アドレス偽造に対応したオープンスペース用ネットワークアクセスサービスの実装と導入”, 情報処理学会論文誌，Vol.47 No.8 (2006).

(平成 20 年 9 月 29 日受付)
(平成 20 年 11 月 8 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 (現総合情報基盤センター) 講師．インターネットの研究に従事．博士 (工学).

江藤　博文（正会員）

平成元年佐賀大学理工学部物理学科卒業．同年日本電気航空宇宙システム株式会社入社．平成 5 年佐賀大学情報処理センター (現総合情報基盤センター) 助手．平成 19 年同助教．画像データの曖昧検索の研究に従事．平成 10 年教育システム情報学会論文賞受賞.

渡辺　健次（正会員）

昭和 62 年佐賀大学理工学部物理学科卒業．平成元年同大大学院理工学研究科物理学専攻修士課程修了．同年同大情報処理センター助手．1993 年和歌山大学経済学部産業工学科講師．平成 8 年同大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．平成 18 年同教授，同大総合情報基盤センター副センター長，現在に至る．教育システム，インターネット応用，分散システム運用技術の研究に従事．博士 (工学).

只木　進一（正会員）

昭和 62 年東北大学大学院理学研究科物理学第二専攻博士後期課程修了．日本学術振興会特別研究員 (京都大学) を経て平成 2 年佐賀大学理工学部情報科学科 (現知能情報システム学科) 助教授．平成 12 年同教授．同年同大学学術情報処理センター (現総合情報基盤センター) 教授，副センター長．平成 18 年同センター長．計算物理学，統計力学，学術情報システムの研究に従事．理学博士．

渡辺　義明（正会員）

昭和 52 年九州大学大学院工学研究科通信工学専攻博士後期課程単位取得退学．同年九州大学工学部助手を経て同大学医学部附属病院講師．昭和 61 年佐賀大学理工学部電子工学科助教授．平成 2 年同大学理工学部情報科学科 (現知能情報システム学科) 教授．平成 8 年同大学情報処理センター長．平成 12 年同大学学術情報処理センター長．生体情報工学，計算機科学の研究に従事．工学博士．