社団法人 情報処理学会 研究報告
IPSJ SIG Technical Report

2007－DSM－44 (12)
2007／3／9

HTTP Keep-Aliveによる利用終了検知機能を実装した新しいOpengateの開発

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:

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LDAPやRADIUSサーバなどを利用することができる．

Opengateはネットワークの利用終了の即時検知にJava Appletを用いている．そのため，Java環境を持たない端末における利用終了の即時検知には対応していなかった．そこで，この問題の解決とともに，起動の高速化を目的として，HTTP Keep-Aliveによる利用終了検知機能を実装した新しいOpengateの開発を行った．本稿では，HTTP Keep-Alive機能による終了検知を行う新しいOpengateの詳細について述べる．

Development of the new Opengate capable of detecting usage termination by HTTP Keep-Alive

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:

We have developed and distributed a network user authentication system "Opengate". It has been operated in Saga University. 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 LDAP and RADIUS, are applicable for authentication. 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 using "HTTP Keep-Alive". New Opengate requires no plug-ins and responses faster than previous one. This paper describes development of the new Opengate capable of detecting usage termination by HTTP Keep-Alive.

1 はじめに

インターネットの普及に伴い，コンピュータを利用した情報処理や，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ている．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．このため，公開端末や情報コンセント，無線LANの設置が大学において進んでいるが，不正な利用に起因したトラブルも多い．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，無線 LAN においても，利用資格を有する者のみが利用できるとともに，利用記録が取れる仕組みが必要である．大学でサービスを提供することを考慮すると，多様な知識レベルのユーザが，多様な端末と多様な接続形態で，多様なアプリケーションを扱える必要がある．また多くの利用者が毎年入学と卒業をすることから，その利用指導や利用者管理の負担が少ない方が望ましい．さらには，サーバ導入コストや管理コストも少ないことが望ましい．

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[1)-3)]．また 2005 年からは IPv6 に対応した Opengate の試験運用を行っている[4),5)]．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，認証には既設の LDAP や RADIUS サーバなどを利用することができる．

従来，Opengate では，利用者端末に送った Java Applet と監視プロセスとの間の TCP コネクションを監視することで，利用終了を即時検知する仕組みを導入している．

しかし，利用者端末に必ずしも Java 環境が実装されているとは限らないため，利用前に Java 環境を導入する必要性が生じてしまう．また，環境によっては Java を導入できない場合もあるため，このような端末にも対応可能な利用終了の即時検知の仕組みが望まれる．

そこで，Java Applet に代えて，HTTP/1.1[6)] において標準となった Keep-Alive 機能（以下，HTTP Keep-Alive) を用い，Web ブラウザと監視プロセスとの間で TCP コネクションを維持することで，利用終了を即時検知する方法を考案した．この方法は，追加プラグインを持たない標準的な Web ブラウザのみの利用者端末にも対応できる．また Java Applet を使用しないため，ブラウザの起動も高速という利点もある．

本稿では，この HTTP Keep-Alive による終了検知を行う新しい Opengate の詳細について述べる．

2 Opengate の概要

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を準備する必要なしに，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 に，ソフトウェアの構成を図 2 に示す．

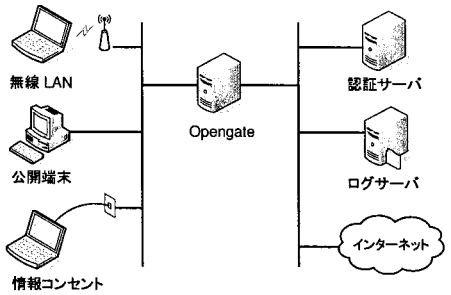

図 1　Opengate のシステム構成例

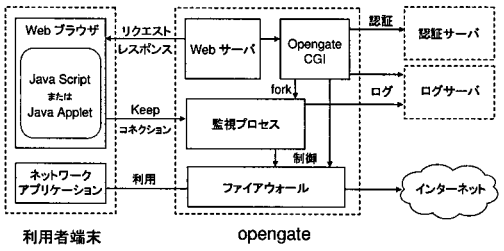

図 2　Opengate のソフトウェア構成

Opengate は，利用者端末を接続するネットワークの出口に，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 Web サイトを表示しようとする際に，Opengate はその通信を奪い取り，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する．入力された利用者情報を認証サーバへ問い合わせて，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．

その後，利用終了を監視するために，利用者端末の Web ブラウザと，Opengate の監視プロセスの間に TCP コネクションを張る．利用者が Web ブラウザ，もしくはシステムを終了すると，TCP コネクションの切断が検知され，その際にファイアウォールの開放ルールを除く．

ファイアウォールに加える開放ルールによって，Opengate は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．

この 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 言語で開発されている．

2.2 利用終了の監視

閉鎖状態にある利用者端末からの Web アクセスは，ファイアウォールによって，Opengate が動作するゲートウェイ上の Web サーバに転送され，CGI を起動する．CGI は認証サーバに認証情報を問い合わせた後，利用者端末ごとに 1 つの監視プロセスを起動し常駐させる．監視プロセスはファイアウォールを制御するとともに，利用者端末からの接続を待ち受け，TCP コネクションを維持して利用状況を監視する．

従来の Opengate では，利用者が認証に成功すると，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．

この方式では，利用者端末に Java の環境が必要となるため，新 Opengate では，Java の環境を必要としない HTTP Keep-Alive による利用終了の即時検知の方式を導入した．この詳細については，第 3 章で述べる．

2.3 認証と利用者情報の記録

認証時に入力された，利用者 ID やパスワードは，Opengate の CGI に渡され，CGI は認証サーバを使用し認証する．なお，認証には POP3, POP3S, FTP, RADIUS, LDAP，LDAPS や PAM から既設の認証方式を利用することが可能である．認証が成功すると認証が成功したことを示す Web ページが表示される．

また，Opengate は利用者の情報として，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 機能を用いてログサーバ上に記録する．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のみ意味がある．

3 新 Opengate の利用終了の監視

この章では，新 Opengate における利用者端末の利用終了の監視について述べる．

3.1 HTTP Keep-Alive による利用終了の監視

まず始めに，HTTP Keep-Alive を利用して TCP コネクションを維持し，利用者端末のネットワーク利用終了を監視する方法を以下に述べる．

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，XMLHttpRequest を発行し，監視プロセスに hello メッセージを送信する．その返答を受け取ったら，すぐに次の XMLHttpRequest を発行し，hello メッセージを送信することを繰り返す．

これらの処理の流れを図 3 に示す．

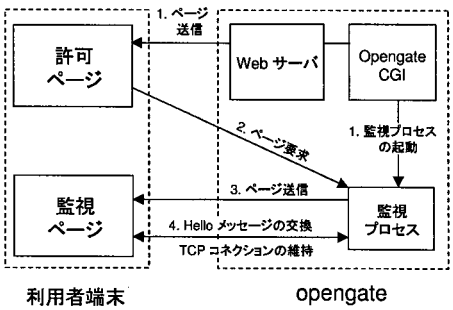

図 3 利用監視の処理の流れ

Opengate の監視プロセスは，XMLHttpRequest に対して，一定時間 (標準設定で 100 秒) 遅延させ，返答する．監視プロセスは，返答遅延の間も，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，利用者端末のネットワーク利用の終了と判断する．

なお，一部のブラウザでは，ページを取得したポート番号と，そのページからの XMLHttpRequest 先のポート番号が異なると，XMLHttpRequest を発行できなかった．よって，同一ポートとするために，許可ページ内で監視プロセスに対して JavaScript 記述のページを要求し，受け取ったページで処理することとした．

以上の方法により，XMLHttpRequest から返答までの間は，TCP コネクションは維持される．また，返答

から次の XMLHttpRequest の間は短時間であり，これらの時間の間は，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．ただし，HTTP Keep-Alive は，稀に途切れる可能性があるため，返答送信後の短時間 (標準設定で 10 秒) は，TCP コネクションの再接続を認めることで対応した．この TCP コネクションの再接続までの時間は通常 1 秒以下である．再接続の際には，同一の利用者端末からの接続であることを確認するために SSL などを用いて暗号化し，端末を認証するなどの対応を行うのが望ましいが，新 Opengate では，以下の簡単な処理を付加した．

XMLHttpRequest の発行のたびに，ランダム値 (R_N) とセッション ID から MD5 ハッシュ値 (H_N) を生成し，これを前回の XMLHttpRequest の際のランダム値 (R_{N-1}) とともに Opengate の監視プロセスに送付する．監視プロセスでは，前回取得したハッシュ値 (H_{N-1}) と，新たに送付されたランダム値 (R_{N-1}) から生成したハッシュ値を比較することで，同一の利用者端末であることを確認する．初期値 (R_0, H_0) は，セッション ID のハッシュ値を基に生成する．

3.2 他の監視方式の併用

第 3.1 節で示した方式は，Web ブラウザに，プラグインなどの追加することなしに終了を即時に検知できる．また，この方式は，一般的に利用されている代表的なブラウザにおいて有効である．

しかし，HTTP Keep-Alive は HTTP/1.1 から標準となっているため，これが実装されていない古い Web ブラウザが，Opengate の環境で利用される場合も考えられる．またシングルタスク OS の機器では，TCP コネクション維持している Web ブラウザと他のネットワークを利用するアプリケーションを同時に動かすことはできない．

そこで，HTTP の TCP コネクションを監視する方法を標準的な監視方法としながら，以下の監視方法を組み合わせて利用する．

1. HTTP-CLOSED
   HTTP が維持する TCP コネクションの切断を検知する方式である．これは，第 3.1 節で説明した方式である．Web ブラウザとの間に TCP コネクションを維持し，これを待ち受け状態に保つ．利用者端末が Web ブラウザもしくは OS を終了すると，TCP コネクション切断が検知され，利用終了と判断する．
2. JAVA-CLOSED
   クライアントに送付した Java Applet との間に維持する TCP コネクションが切断を検知する方式である．これは，第 2.2 節で説明した従来の Opengate の監視方式である．認証許可ページにおいて Java Applet を Web ブラウザに送付し，これと TCP コネクションを維持する．利用者端末が Web ブラウザもしくは OS を終了すると，TCP コネクション切断が検知される．さらに，TCP コネクション切断の検知だけでは，物理線の切断など，通信が遮断された場合に対応できないため，定期的に hello メッセージを交換して，利用者端末の生存を確認する．
3. MAC-CHANGED
   MAC アドレスが変更されたことを検知する方式である．端末の MAC アドレスを定期的にチェックし，MAC アドレスに変更があったら，利用終了と判断する．
4. 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式である．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．
5. TIME-EXCEEDED
   利用者が入力した利用時間が経過したことチェックする方式である．認証情報の際に，希望する利用時間を利用者から得て，その時間だけネットワークを利用可能とする．ただし設定限度を設けて，一時的利用に限定する．
6. QUIT-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終了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．

第 4 章では，上記の監視方法の選択の手順について説明する．

4 監視方法選択の手順

今回開発した新 Opengate では，監視方法を以下の手順で選択する．

1. Opengate は，認証後に許可ページをクライアントに送る．
2. 許可ページ には，JavaScript を記述した監視ページへの自動移行が記述されている．さらにこの移

行が失敗した場合には，Java Applet を読み込むように記述されている．監視ページには，XMLHttpRequest の発行と返答受け取りを繰り返す JavaScript が記述されている．さらにそれが失敗した場合には Java Applet を読み込むように記述されている．

3. 許可ページ送付後に Opengate は，クライアントの接続を待ち受ける．クライアントの接続があるまでは，MAC-CHANGED, NO-PACKET, TIME-EXCEEDED, QUIT-CLICKED のいずれかを検出するとネットワークを閉鎖して，終了する．
4. Java Applet からの接続があれば，JAVA 監視モードに移る．JAVA 監視モードでは，TCP コネクションを維持し，それを介して定期的 (標準設定で 100 秒) に hello メッセージ を送付し，hello メッセージ の返答を受ける．JAVA-CLOSED, MAC-CHANGED のいずれかを検出した場合はネットワークを閉鎖して，終了する．
5. HTTP 接続で監視ページの要求があれば，当該ページを送付してから，XMLHttpRequest の交信を確認する．確認に成功すれば HTTP 監視モードに移る．HTTP 監視モードでは，hello メッセージのリクエストが来ると一定時間 (標準設定で 100 秒) 遅延させて，hello メッセージを返答することを繰り返す．HTTP-CLOSED, MAC-CHANGED が検出された場合はネットワークを閉鎖して終わる．

従来の Opengate は Java Applet による監視を基本として 2001 年から長期にわたり，佐賀大学内で安定運用を行っているが，新 Opengate においては HTTP による監視を基本とするように変更した．しかし，利用される様々な Web ブラウザに柔軟に対応できるよう，以下の機能も設けている．

- HTTP/1.1 に非対応な Web ブラウザで，HTTP 監視モードを無効にする機能
- 各監視モードに非対応な Web ブラウザを設定ファイルに記述することで，その監視モードを無効にする機能

また不具合を発見した場合，利用者が JavaScript を無効にすると，HTTP 監視モードを省略して別の監視モードを選択できる．

5 試験運用

2006 年 12 月から，本稿で報告した新 Opengate の試験運用を小規模なネットワークにおいて開始した．新 Opengate は，利用監視の方法が異なるものの，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．この新 Opengate の利用に関するトラブルも特になく，主要なブラウザである Internet Explorer 7, 6, 5 や，Firefox 2.0, 1.5, Opera 9, 8, Netscape 7, Safari 2, 1 などで正常に動作した．

また，試験環境において，Java Applet を利用した終了監視では，Opengate の起動時間が平均で約 11.6 秒であったが，HTTP Keep-Alive では平均で約 1.6 秒となり，起動時間が大幅に減少した．

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 4，図 5 に示す．また新 Opengate は，表 1 に示す環境における動作を確認している．

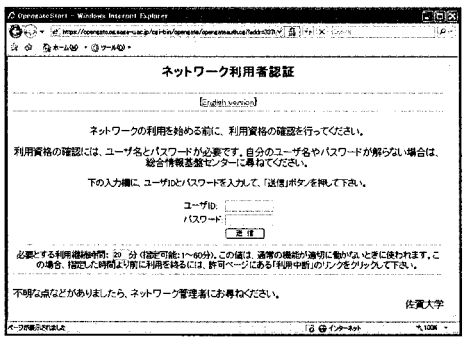

図 4 認証インタフェース

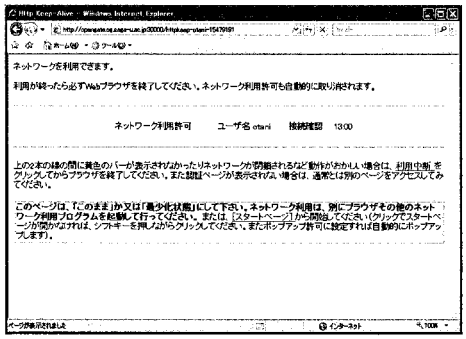

図 5 認証後の表示

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 6.1
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 2.2
DHCP	isc-dhcp 3
Opengate	opengate 1.4.12

6 考察

我々は，端末の利用終了を即時検知する方法として，新たに HTTP Keep-Alive を利用し，Web ブラウザと監視プロセス間で，TCP コネクションを維持する方法を考案した．この方法は，Java プラグイン などの付加ソフトウェアを導入していない，一般的な Web ブラウザにおいて即時閉鎖を実現する．この方法は，Java Applet を使った監視方法に比べ，起動時間が大幅に減少するという利点もある．

HTTP Keep-Alive は，HTTP/1.1 から標準となっているが，一般的な Web ブラウザである Internet Explorer, Firefox, Opera, Netscape, Safari といった Web ブラウザは既に対応している．よって，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 99.8% 以上 (2007 年 1 月) に対応すると考えられる．

また，学内で運用中の従来の Opengate では，利用の約 24.5% (2007 月 1 月) で，Java Applet による利用終了の即時検知ができず，TIME-EXCEEDED による閉鎖となっていた．Opengate の利用記録から判断して，その多くが Java が導入されていない一般的な Web ブラウザであると考えられる．よって，HTTP Keep-Alive を利用することで，学内で利用される多くの利用者端末の即時検知に対応すると考えられる．

しかし，ネットワーク利用時に，PDA や携帯ゲーム機などの機器を使う利用者や，古い OS とブラウザを使う利用者もわずかながら存在している．このような端末では，必ずしも HTTP Keep-Alive を利用できるわけではない．そこで，新 Opengate では，古いブラウザに対しては JAVA-CLOSED を，低機能システムに対しては，TIME-EXCEEDED, MAC-CHANGED, NO-PACKET, QUIT-CLICKED 等を組み合わせた方式を採用し，Web ブラウザを持つほとんどの利用者端末に対応する．

7 まとめ

本稿では，HTTP Keep-Alive による利用終了の即時検知を行う新しい 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 Keep-Alive による利用終了検知機能を実装した新しい 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った．また，Java Applet を使用しないことによって，Opengate の起動も高速化した．この方式で利用者端末のほとんどで，利用終了の即時検知に対応すると考えられる．

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．またディスクレスによる運用も今後の課題である．

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) 渡辺義明 他：「Opengate ホームページ」 http://www.cc.saga-u.ac.jp/opengate/
2) 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)
3) 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)
4) 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)
5) 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”，情報処理学会研究報告，2006-DSM-43 (2006.9)
6) Request for Comments: 2616 , Hypertext Transfer Protocol - HTTP/1.1