HTTP コネクションの維持による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運用

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

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‡

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

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，学内で運用を行っている．この Opengate は，ネットワークの利用終了の即時検知に Java Applet を用いていたため，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対応していなかった．そこで，HTTP の遅延応答と HTTP Keep-Alive 機能を用いた利用終了の即時検知機能を実装した，新たな Opengate を開発し，2007 年 4 月より学内で運用を開始した．

本稿では，HTTP の遅延応答と HTTP Keep-Alive 機能を用いた新しいネットワーク利用者認証システム Opengate の概要と，佐賀大学での導入・運用について述べる．

キーワード

認証ネットワーク，統合認証，Opengate, Keep-Alive, ネットワーク運用

1 はじめに

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，近年，多くの大学などにおいて，自由に利用できる公開端末や情報コンセント，無線 LAN などの設置が進んでいる．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も発生しやすい．

よって，利用者を有資格者のみ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，利用終了を即時に検知し，ネットワークを閉鎖することも，セキュリティの面で重要である．

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の認証・記録を行う Opengate と呼ばれるシステムを開発・公開し，2001 年より学内において全学規模で運用を行っている [1, 2]．この Opengate は，ネットワークの利用終了の即時検知に Java Applet を用いていた．このため Java の実行環境のない利用者端末で利用終了の即時検知を行うには，事前に Java の実行環境を導入する必要性が生じ，これに伴う指導も必要であった．

そこで，HTTP の遅延応答 (以下，HTTP 遅延応答) と，HTTP/1.1 [3] において標準となった Keep-Alive 機能（以下，HTTP Keep-Alive) を用いる利用終了の即時検知 (以下，HTTP による終了検知) の手法を開発し，

新たに Opengate に実装した [4]．これにより追加プラグインや拡張機能を持たない標準的な Web ブラウザにおいて，利用終了の即時検知が可能となった．

この新たな Opengate を，学内において 2007 年 4 月より全学規模で運用を開始した．この新たな Opengate では，利用者が円滑に移行できるよう，従来の検知方式に付加する形で新たな検知方法を導入し，さらにインタフェースも従来のものを引き継いでいる．

本稿では，HTTP による終了検知を行う Opengate の概要と，佐賀大学での導入・運用について述べる．

2 Opengate の概要

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．

利用者は，始めに Web ブラウザで任意の Web サイトにアクセスする．Opengate はその通信を奪い取り，代わりにネットワーク利用のための認証ページを利用者の Web ブラウザに表示する．

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．Opengate は，入力された利用者情報を認証サーバに問い合わせ，認証に成功した場合，当該利用者端末の 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検知する．利用者が Web ブラウザを終了，もしくは利用者端末の OS を終了すると，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を使用する場合も，まず始めに任意の Web サーバへアクセスし，認証ページから，認証を行わなければならない．

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．

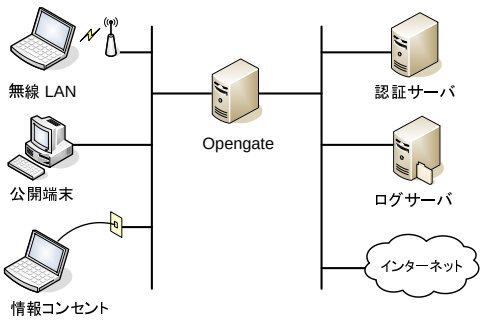

図- 1: Opengate のシステム構成例

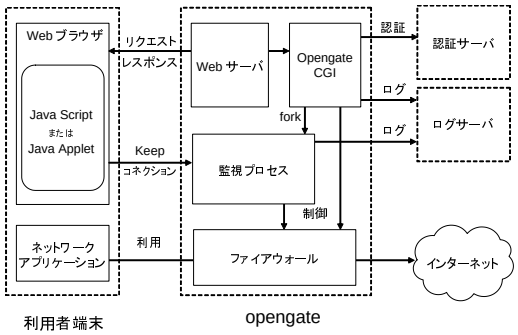

図- 2: Opengate のソフトウェア構成

3 HTTP による利用終了の検知を行う新たな Opengate

3.1 概要

Opengate を開発した当初，利用者端末の多くに購入時から Java の実行環境が導入されており，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．

そこで，追加プラグインや拡張機能を持たない標準的な Web ブラウザにおいても利用可能な，HTTP による終了検知方法を考案し，実装した．また，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ことも期待できる．

3.2 動作

HTTP による終了検知方法の流れを，以下に述べる (図 3)．

(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．

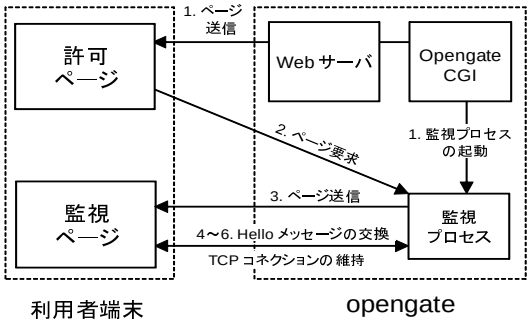

図- 3: 利用監視の動作

(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 100 秒) 遅延させ，返答する．

(6) Web ブラウザは，hello メッセージに対する返答を受け取ったら，すぐに次の XMLHttpRequest を発行し，新たな 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．

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る．(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．

4 従来の終了検知方法の併用

第 3 章で述べた方法で，一般的に利用されている多くの Web ブラウザで，HTTP による終了検知が利用できる．しかし，新たな Opengate を実際に大学において運用することを考えると，更に多種多様な 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．このため 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．

つまり，HTTP による終了検知を標準的な検知方法としながら，上述のような HTTP による検知方法が利用できない Web ブラウザも利用されることを想定する．そのため，従来利用していた終了検知方法 (Java Applet による検知や一定時間経過後の強制閉鎖など) も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．

5 新たな Opengate の運用

5.1 導入

2007 年 4 月 6 日から，新たな Opengate に移行し，ディスクレスによる運用を開始した．移行の際に，ディスクレス環境の再起動などによる 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 Opengate の不具合によるサービスの停止も起きていない．

新たな Opengate は利用終了の検知方法が異なるものの，インタフェースやその利用方法は，従来の Opengate と同じになるよう実装した．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．

5.2 動作検証

新たな Opengate 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って利用する Java 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確認を行った．

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/Mobile で利用される Pocket Internet Explorer や Internet Explorer Mobile, 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．これ以外の多くの Web ブラウザで正常に動作することが確認できた．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) [7] で HTTP による利用終了の即時検知が可能であると考えられる．なお，即時検知ができない Web ブラウザの場合は，一定時間後に通信路が閉鎖となる．

新たな Opengate を導入後，約 3ヶ月間 (2007 年 5 月〜7 月) の間に即時検知が利用できなかった割合は，1.18 %であった．従来の Opengate では，約 24.5 % (2007 年 1 月) であったため，即時検知の割合が大きく向上した．

同期間において Java Applet を利用した終了検知では，端末側の起動時間が平均で約 12.34 秒であった．一方，HTTP による終了検知では平均で約 1.77 秒であり，利用者端末での起動時間が大幅に減少した．

5.3 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) である．これまでの運用では，月平均で約 2〜3 万回の利用があり，多い時には，約 200 人前後が同時に利用している．

新たな Opengate を導入後，約 3ヶ月間の利用者は 2,511 人で，利用回数は，のべ 73,261 回であった．また，平均利用時間は，約 4,412 秒 (中央値: 約 2,946 秒) であった．利用者のうち，2,231 人 (88.85 %) が学生であり，これらの利用状況は，新たな Opengate の導入前とほぼ同様となった．

6 Opengate に関する考察

ここでは，Opengate の導入や管理・運用コストなどについて述べる．

6.1 導入コスト

Opengate は，FreeBSD や，Apache，ipfw などの設定が必要となるものの，特殊な設定は必要としないため，導入は容易である．さらに新たな Opengate は，コンパイルとインストール後に，認証サーバの設定を行うのみで動作し，導入がより容易となった．認証も従来の POP，POPS，Radius や PAM に加えて LDAP，LDAPS を使える．また複数の認証サーバへの問い合わせを付加 ID(「利用者 ID@」の後に記述する文字列) で振り分ける機能に加えて，複数の認証サーバへ次々に問い合わせることも可能とした．よって全学共通の認証サーバがない場合でも利用することができる．

新たな Opengate は，起動後は 100 秒に一度の交信を行うプログラムであるため，その負荷は極めて小さく，通常の利用であれば数 100 台規模の端末数であっても問題なく動作する．佐賀大学における約 3ヶ月間の運用において，全 Opengate の最大同時利用は 210 台であり，1 つの Opengate の最大同時利用は 88 台であった．よって少数台で運用することも可能である．

現在のところ，佐賀大学では，同一ネットワーク内での不正アクセスやウィルスによる障害拡大の防止，障害発生時の位置特定を容易とするため，運用当初から若干の設定だけが異なる 20 数台の Opengate をディスクレスで運用する仕組みを採用している．物理的な障害時には，各 Opengate が相互にバップアップ機器として機能する冗長構成となっている．台数の削減は今後の課題である．

6.2 運用コスト

Opengate は，各利用者端末や，HUB 装置などに個別の設定は不要であり，セキュリティが考慮されていない端末が配置された環境に後から設置ができるなど，シームレスな導入が容易である．また Opengate の設定のみでシステムを制御可能であるため，端末や HUB 装置の設定を行う必要のあるシステムと比較して作業量が少なく，設定変更も容易で，設定変更によるサービスの停止も発生しない．新たな Opengate においては，ほとんど全ての設定が XML 形式の設定ファイルにまとめられており，その設定変更は，サーバ等の再起動なしに，次に接続してくる利用者から適用される．

佐賀大学では，総合情報基盤センター内に全ての Opengate を集約し，VLAN によってサブネットを各拠点に配備している．日常的な管理作業は，Opengate のログや，トラフィックや利用者数などを MRTG などのツールを使って定期的に確認するのみであり，手間も少ない．また，新たな Opengate では，端末への Java の導入作業が不要となり，利用者対応がより容易となった．

6.3 汎用性

佐賀大学では，学会などで大学を訪問する一時的利用者のための認証サーバを用意しており，身元確認後に期限付き利用証をその場で発行することで，学外者にもネットワークサービスを提供している．また，ファイアウォールの設定で，特定ポートの常時閉鎖や，P2P などの監視も行っている．また Opengate を遠隔施設のネットワークサービスにも利用している．遠隔施設では，様々な学生・教員などの一時滞在が多いためネットワーク利用者の管理が難しい．そこで，Opengate を利用しインターネット利用の管理を行っている．学科によっては，学生の居室のネットワークサービスとして利用している．

Opengate では付加 ID によって認証サーバを切り替えることが可能となっていた. さらに新たな Opengate においては，付加 ID や利用者 ID によって，特定の利用者のみ，認証サーバや認証方式を変更したり，認証後に開放するプロトコルを細かく設定したりすることも可能とした．特定の利用者 ID を一時的に拒否することも可能である．

6.4 使いやすさ

Opengate は，Web ブラウザを利用者インタフェースとしている．専用のクライアントソフトや telnet などを

利用するシステムと比べ，設定や利用も容易で，多様な端末で利用可能である．また，利用時に特定の URL へのアクセスは必要なく，任意の URL へのアクセスで認証画面が表示されるインタフェースとなっている．よって，実際の運用においても簡単な説明を行うだけで，コンピュータに詳しくない利用者でも容易にネットワークを利用できる．

新たな Opengate では，Java 環境を必要とせず，より容易に利用できるようになった．さらに HTTP による検知ができない場合も，利用者が指定した時間長（上限あり）の間だけネットワークを開放する仕組みを入れており，端末に Web ブラウザさえあれば利用できる．

6.5 関連製品

現在，ネットワークの利用者認証を行うシステムが多く研究されている．近年では，空港やホテル，企業や大学などにおいて Apresia[8] や，POPCHAT[9] 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も増えてきている．

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ているが，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，これら製品の導入費用などのコストも無視できない．

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．

7 まとめ

本稿では，HTTP 遅延応答と HTTP Keep-Alive による利用終了の即時検知を行う新たな Opengate の概要と，佐賀大学での導入・運用について述べた．

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 遅延応答と HTTP Keep-Alive による利用終了検知機能を実装した新たな Opengate を開発し，2007 年 4 月より運用を開始した．

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，端末での起動が高速化し，利用者端末の負荷軽減にも繋がった．従来の Opengate の利用方法とインタフェースを引き継いだため，移行も円滑に行うことができた．

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] 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] Request for Comments: 2616 , Hypertext Transfer Protocol - HTTP/1.1 (1999).

[4] 大谷 誠，江藤博文，渡辺健次，只木進一，渡辺 義明: “ 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”, 情報処理学会研究報告, 2007-DSM-44 (2007).

[5] 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).

[6] 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).

[7] OneStat.com
http://www.onestat.com/html/aboutus_pressbox50microsoft-internet-explorer-7-usage.html

[8] Apresia
http://www.apresia.jp/

[9] POPCHAT
http://www.popchat.jp/