Javaを用いたOpengateクライアントの開発
Development of Opengate client by Java

真鍋 憲市 †, 江口 勝彦 †, 渡辺 健次 ‡
† 佐賀大学大学院工学系研究科知能情報システム学専攻
‡ 佐賀大学理工学部知能情報システム学科
840-8502 佐賀市本庄町 1

Ken-ichi Manabe, Katsuhiko Eguchi, Kenzi Watanabe
Department of Information Science, Saga University
1 Honjo, Saga 840-8502

概要

佐賀大学では、公開端末及び利用者移動端末に対応したネットワーク利用認証システム Opengate を開発・運用している。Opengate は、利用者のブラウザが送信する最初の HTTP 要求に対して認証画面を返し、認証によってファイアウォールを制御するシステムである。ブラウザのみで利用可能であるため、端末側に特別な設定やソフトウェアのインストールを必要としないことが大きな特徴である。しかし、ブラウザ上で運用するために、予期せぬ終了の発生やネットワークの切断に対する再接続の手間などが Opengate 常用者にとって負担となることがある。本研究で開発した Opengate クライアントは、ブラウザと Opengate のクライアント側機能を分離することで、このような負担を克服することを目的としている。Java を用いているためクライアントの環境を問わず利用することが出来る。

キーワード

ネットワーク認証, Opengate, Java

1 はじめに

Opengate とは、ネットワークを利用する際に利用者認証と利用記録を行うゲートウェイシステムである [1][2]。Opengate では、認証、利用開始、利用停止、の全てを Web ブラウザ上で行うことによって、利用者端末への特別な設定やソフトウェアのインストールを不要とし、学会や研究会などでの来校者、図書館などの学内組織固有の学外利用者のネットワーク利用への柔軟な対応を可能としている。

しかし、Opengate には、ブラウザ上での運用ならではの問題点が存在し、Opengate を普段から利用する者にとってそれが負担となることがある。本稿では、Opengate の基本動作を説明した後に運用上の問題点について言及し、解決策の一つとして本研究で開発したクライアントソフトウェアを利用する方法を議論する。

本 Opengate クライアントでは、起動と同時に Opengate サーバを探索し、認証と利用確認を行うことが出来る。また、各 Opengate サーバ毎にユーザ名とパスワードを暗号化して保存する機能や、ネットワークが切断された場合に再接続を行う機能を追加することで、ユーザの手間を軽減することが出来る。

2 Opengate の基本動作

Opengate は、利用者が Web ブラウザを開いて任意の Web ページへアクセスしようとする際の HTTP 要求を横取りして、認証画面を返す。認証画面によって利用者から送られたユーザ名とパスワードによって、認証サーバへの認証が成功した場合、当該端末に関するパケットの透過許可がファイアウォールのルールに登録される。同時に利用者側 Web ブラウザでは Java Applet が起動し、Opengate との間に TCP コネクションを確立して利用状況を監視する。利用者がこの Web ブラウザを終了し、Java Applet を終了することで利用終了となり、ファイアウォールのルールから当該端末に関するパケット透過の規則を削除する。また、認証記録と利用開始、利用終了がログとして残される。これらの流れを図 1 に示す。

利用者が電子メールなどの WWW 以外のサービスを利用する場合、一旦 Web ブラウザによって認証を行い、ブラウザを起動したままで利用することになる。

3 運用上の問題点

Opengate は利用者の利用状況を Java Applet との TCP コネクションによって判断するため、Java Applet が終了すると、Opengate は利用終了と認識する。このため、Web ブラウザ側の動作によって利用者の意図しない不都合を起こす。

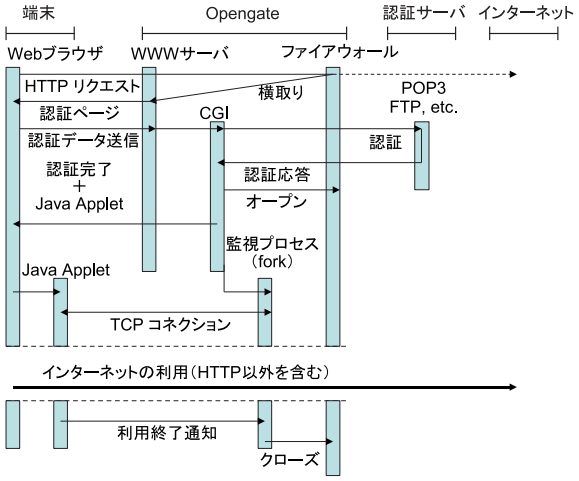

図 1: Opengate の動作

3.1　Java Applet が意図しない終了を起こす

通常の動作では、ブラウザの終了によって Java Applet が破棄される際に利用終了となる。しかし、利用中にブラウザが別のページを表示した場合、Java Applet の動作はブラウザや Java の実行環境によっても異なるが、最終的に TCP コネクションが切断されてしまうことになる。

ブラウザが別ページを表示する例として、以下のような場合がある。

- **利用者の動作によってページを移動する**
  Opengate 利用中に、利用者がブックマークなどを用いて Java Applet のあるページから移動する場合がある。これに関して、Java Applet のあるページに警告文を表示することで警戒を促しているが、たびたびこれを行う利用者がある。

- **外部アプリケーションからの Web ページ呼び出し**
  メールクライアントやオフィス製品などの外部アプリケーションからのハイパーリンクによって Web ページが呼び出された場合、どこに表示するかはブラウザによって異なる。Internet Explorer の場合、最初に作成したウィンドウに表示されるため、利用開始時に作成される、認証ページから移動した Java Applet のあるページに表示され、Java Applet が停止することになる。

- **ブラウザを終了する**
  ブラウザが別ページを表示する以外にも、別のページを表示していた他ウィンドウが強制終了した場合に、ブラウザごと終了してしまうというケースがある。また、特にタブブラウザを利用している場合には、Web ブラウズを終了するときにブラウザを終了してしまい、その後例えばメールを見るためにブラウザを再び起動して認証し直すというケースもある。

3.2　ネットワークが切断された場合

Opengate を利用中にネットワークが切断された場合、Opengate と Java Applet との間の TCP コネクションが切断されることになり、再び認証を行わなければならない。

無線ネットワークを利用する端末の場合、移動に際するアクセスポイントの変更によってネットワークの切断が起こることがある。

4　Opengate クライアントの開発

4.1　概要

前述したような問題点は、特に日常的に Opengate を利用する場合に、負担と感じている利用者が多い。このような利用者の中では、普段常用しているブラウザではないブラウザで Opengate を開き、最小化して触らないようにするという利用法が取られることがある。

Opengate クライアントはこのような利用者を対象として、Opengate のクライアント側機能をブラウザから切り離したソフトウェアである。ブラウザのみで利用できるという Opengate の特性を損ねることになるが、常に Opengate の下にある移動端末などでは負担を軽減することができる。

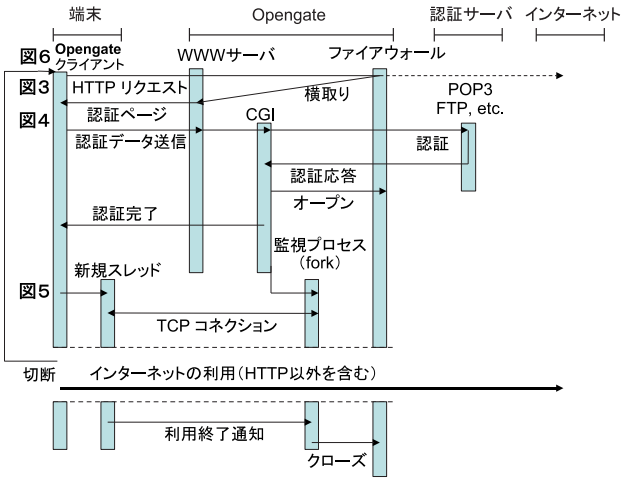

図 2: Opengate クライアントの動作

クライアントを起動すると、Opengate の外側にある架空の Web サーバに対して HTTP 要求を送る。Opengate はその要求を横取りして認証ページを返すが、そのデータから Opengate のアドレスを特定すると、認証プロンプトを表示する。プロンプトによって得られたユーザ名とパスワードを Opengate に渡した結果、認証に成功した場合に Opengate へ TCP コネクションを確立する。これらの流れはブラウザが Opengate に対して行うものと同一である。Opengate クライアントの流れを図 2 に示す。

Opengate クライアントは、接続が切断される度に再接続を試みる。また、各 Opengate のアドレスごとにユーザ名とパスワードを暗号化して保存することが出来るため、複数の Opengate サーバ下で利用する場合でも、ワンクリックで認証から接続までを行うことが出来る。

4.2　Opengate クライアントの動作

4.2.1　Opengate サーバを探索する

クライアントは、まず Opengate サーバを見つけなければならない。Opengate サーバを特定する方法として、設定ファイルによって直接指定する方法と、クライアント自身が Opengate サーバを探索する方法を用意した。

Opengate サーバを探索するために、クライアントは Opengate の外側にある架空と思われる Web サーバに対

して HTTP 要求を送る[1]。この端末が Opengate の下にある場合、Opengate はこの要求を横取りして認証ページへ REFRESH タグがある HTML を返すため、これにより認証ページのアドレスを知ることが出来る。この端末が Opengate の下にない場合、クライアントの要求は横取りされることなく送信されるが、IP アドレスは架空のものなので例外を引き起こしてエラーとなる。このエラーを検知して、クライアントが Opengate の下にいないこと (もしくは既にファイアウォールが開いている) を知ることが出来る (図 3)。

図 3: Opengate サーバを探索する

4.2.2　認証を行う

クライアントは Opengate のユーザ名とパスワードを各サーバ毎に保存しておくことが出来る。Opengate サーバを特定できたクライアントは、まずそのサーバ用のユーザ名とパスワードが存在するかどうかをチェックする。存在する場合、認証プロンプトを表示せずに認証を行う。存在しない場合、認証プロンプトを表示し、ユーザ名とパスワードを求める (図 4)。

図 4: 認証画面
(ユーザ名とパスワードを暗号化して保存することができ、その場合この認証プロンプトは表示されない)

認証は、CGI に対してユーザ名とパスワードを POST することで行うため、認証には HTTPS を用いるべきである。クライアントでは以下の 3 つの方法で HTTPS を扱うことが出来る。

- Java VM で用意されている証明書によって検証できる Opengate サーバであれば、HTTP と同じ扱いで適宜 HTTPS を利用できる。
- Sun Microsystems が提供する Java 実行環境には、複数の証明書をストアファイルという形式で管理する keytool というコマンドが含まれる。この keytool で作成したストアファイルを利用して Opengate サーバを検証することが出来る。
- Opengate サーバを検証せずに、無条件に信頼して HTTPS 通信を行うことが出来る。

これらの動作は、設定ファイルによって切り替えるようになっている。

4.2.3　IPv6 対応版への対応

現在、佐賀大学では Opengate を IPv6 ネットワークに対応させる研究を行っている。この IPv6 対応版 Opengate では、認証ページが従来の静的な HTML ではなく、クライアントの IPv4 アドレスをユーザ名、パスワードと共に POST する HTML を出力する CGI となっている。その上で、認証時に IPv6 アドレスを取得することで、IPv4、IPv6 アドレス両方に対してファイアウォールを開けることが出来る [3]。

クライアントは Opengate を探索する際、認証ページに IPv4 アドレスが含まれていた場合、これを保持して認証時に POST する。また、特に Sun Microsystems の Java 実行環境の場合、IPv4、IPv6 アドレス共に持つ名前を解決する際 IPv4 を優先するので、システムプロパティを変更して IPv6 アドレスを優先するようにする。これによって、認証時に Opengate サーバはクライアントの IPv6 アドレスを取得できる。

4.2.4　Opengate との TCP コネクションを確立する

認証に成功した場合、認証 CGI は Java Applet を呼び出すタグを含む HTML を返す。このタグには Opengate サーバが TCP コネクションを確立するために開いているポートが含まれているため、このポートに対して別スレッドで TCP コネクションを開く (図 5)。また、このとき HTML 内に IP アドレスが表記してあれば、これを表示しクライアント側の IP アドレスが分かるようになっている[2]。

図 5: 認証に成功した場合
(表示されている IP アドレスは、ファイアウォールが開放された、クライアントのアドレスである)

TCP コネクションを開くと、Opengate サーバは一定間隔で文字列 “hello” を送信してくる。この文字列に対して同じ文字列 “hello” をサーバに送り返すことで接続を確認する。

[1] 今回開発したクライアントは IP アドレス (1.0.0.1) を利用している。

[2] IPv6 対応版では認証成功ページにクライアント側の IP アドレスが表記される。

4.2.5　再接続を行う

Java においては、TCP コネクションが途中で切断された場合にそのメソッドが例外を引き起こす。これをきっかけにして、クライアントは再接続のために再び Opengate サーバの探索を行う (図 6)。TCP コネクションの切断によって Opengate が正常に終了した場合、直ちにファイアウォールが閉じられるため、再接続時にも正常に探索を行うことが出来る。しかし、なんらかの事情でファイアウォールが閉じられなかった場合、4.2.1 節に従って例外が起こるため、これを検知することが出来る。

図 6: 再接続中の画面

5　まとめ

本稿では、Opengate 利用端末において、ブラウザと Opengate のクライアント側機能を分離することによって、ブラウザにまつわる Opengate のトラブルを回避するためのソフトウェアについて提案した。また、Opengate を常用する際に必要と思われる機能を備えることで、Opengate を意識せずにネットワーク利用認証を済ませることができる。

このクライアントソフトウェアは Java で開発されているため、プラットフォームを問わないという Opengate のポリシーに添うものとなっている。現在このソフトウェアは、Windows、Mac において動作確認を取っている。

このように、Opengate クライアントの目的は、利用者への負担を軽減することを最大の目的としているため、今後の課題として出来るだけ目立たないように利用できるようにすることが挙げられる。

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] 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 IPSJ-DSM04036002