利用者認証と利用記録機能を実現するゲートウェイシステム Opengate の開発

渡辺健次† 只木進一† 江藤博文‡ 渡辺義明†

†佐賀大学理工学部 ‡佐賀大学情報処理センター

〒 840-8502 佐賀市本庄町 1

E-mail: watanabe@is.saga-u.ac.jp

あらまし: ネットワークを大学のあらゆる活動で活用するために、公開端末や情報コンセントを、キャンパス全域で整備する大学が増えている。しかしながら、本来大学のネットワークは、利用資格を有している者のみが利用できるものである。また、例えば不正行為を行なった者を特定するような場合には、ネットワークを利用した者の記録が残っている必要がある。我々は、これらの問題を解決するために、公開端末と情報コンセントの両方に対して、ネットワークを利用する際の利用者認証と利用者記録が行なえるゲートウェイシステム Opengate を開発した。Opengate は、利用者側で事前設定することなく、容易に利用できるという特徴を持つ。

キーワード: 学内 LAN 管理, ネットワークセキュリティ, ファイヤウォール, ユーザ認証, Java Applet

"Opengate": A Gateway System Which Can Authenticate And Record Users

Kenzi Watanabe†, Shin-ichi Tadaki†, Hirofumi Eto‡ and Yoshiaki Watanabe†

†Faculty of Science and Engineering, Saga University
‡Information Processing Center, Saga University

1, Honyo, Saga 840-8502, Japan
E-mail: watanabe@is.saga-u.ac.jp

Abstract: Recently, network facilities are available for educational and research activities in universities. To support such activities, a lot of "public-terminals" and/or "network sockets" are implemented in the whole area of the campus. We have developed a gateway system named "Opengate". The system can authenticate and record users without any setups by users. In this paper, we describe the design and the implementation of the system.

Keywords: LAN, Network Security, Firewall, User Authentication, Java Applet

1　はじめに

ネットワークを大学のあらゆる活動で活用するために、公開端末や情報コンセントを、キャンパス全域で整備する大学が増えている。電子メールが日常的なツールとなり、就職情報を Web で収集することが広く行なわれるようになったことを考えると、容易にネットワークへアクセスできる環境は、現在の大学に欠かすことのできないものと言える。

しかし、本来大学のネットワークは、利用資格を有している者のみが利用できるものである。公開端末や情報コンセントからのネットワーク利用や、学外から学内へのアクセスについては、まず利用資格の確認を行ない、許可を得た利用者のみが利用できるようにすることが望ましい。

一方、例えば不正行為を行なった者を特定するような場合を考えると、ネットワークを利用した者の記録が残っている必要がある。今後のネットワーク利用の多様化に対応するためにも、ネットワーク利用の記録保持は欠かすことのできない機能である。

これらに対して、これまで情報コンセント利用の際の認証と情報記録を目的とした研究がいくつか行なわれている [1] [2] [3] [4] [5]。しかしこれらのいくつかのシステムでは、利用者の利用終了を判断する方法が、情報コンセントのみを想定しており、公開端末には適用できないものがある。また、認証受付を telnet コマンドで行なうものもあるが、telnet によるインタフェースは使い易いものとは言えない。

そこで我々は、公開端末と情報コンセントの両方に対して、ネットワークを利用する際の利用者認証と利用者記録が行なえるゲートウェイシステム Opengate を開発した。Web という利用者にとって使いやすいインタフェースを採用しており、また、利用者の利用終了と同時にファイアウォールを閉じる機能を有している。

本稿では、Opengate について、システム構成、システムの利用と動作の流れ、システムの実現、そして他の研究との比較について述べる。

2　システム構成

Opengate は端末群とネットワークの間に位置し、認証に応じて端末単位のアクセスコントロールを行なうことで、認証を受けた利用者のみがネットワークを利用できるようにするシステムである。

図 1 に、Opengate を利用するシステムの構成を示す。現在、Opengate は FreeBSD 3.3-RELEASE 上で運用されており、ファイヤウォールの開閉には FreeBSD 付属の ipfw を用いている[1]。また Web サーバには Apache を用いている 。

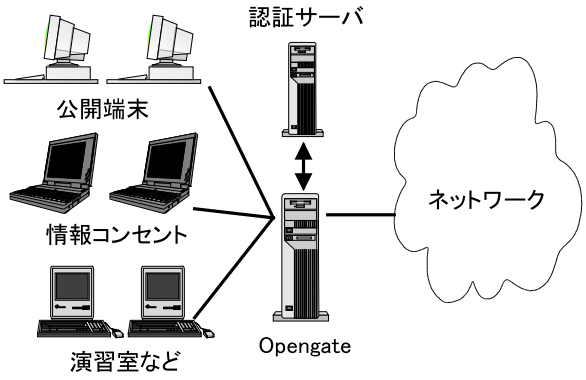

図 1: システム構成

3　システムの利用と動作の流れ

Opengate は、Web サーバ、ipfw に加えて、新たに Web ページ、CGI プログラム、Java Applet を作成して、システムを構成した。これらの動作の流れを、時系列に沿って表したものが図 2 である。

ネットワークを利用する端末の利用者は、まず Web ブラウザを起動して Opengate にアクセスする。Opengate はユーザ名とパスワードを入力する Web ページを返し (図 3)、利用者は自らのユーザ名とパスワードを入力する。

入力されたユーザ名とパスワードは、CGI プログラムに渡される。CGI プログラムは、認証サーバと通信することで認証を行なう。

認証が成功すると、CGI プログラムはファイヤウォールを開き、利用者の情報を記録する。それと共に、CGI プログラムは利用者の Web ブラウザに Java Applet を送り、その Java Applet からの TCP コネクションを待つ。

利用者の Web ブラウザに送られた Java Applet は、図 4 に示す利用許可ウインドウを開き、CGI プログラムとの間に TCP コネクションを張る。利用者は、このウインドウが表示されている間、ネットワークを利用することができる。

利用者が「利用終了」のボタンを押し Java Applet を終了させるか、Web ブラウザを終了すると (この時

[1] Linux などの他の OS への移植、IPF などの他のツールの利用に変更することは容易である

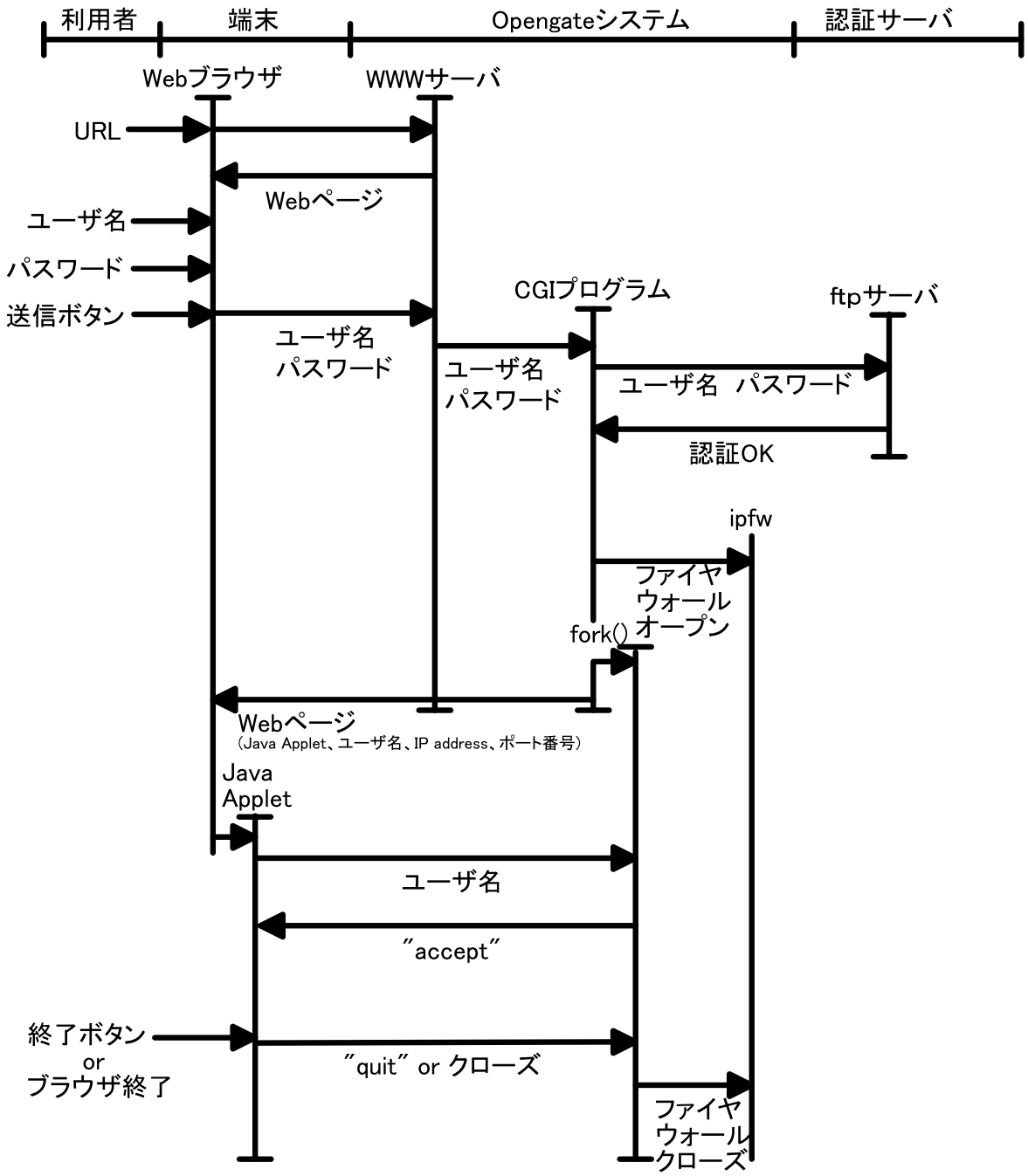

図 2: **システムの動作の流れ**

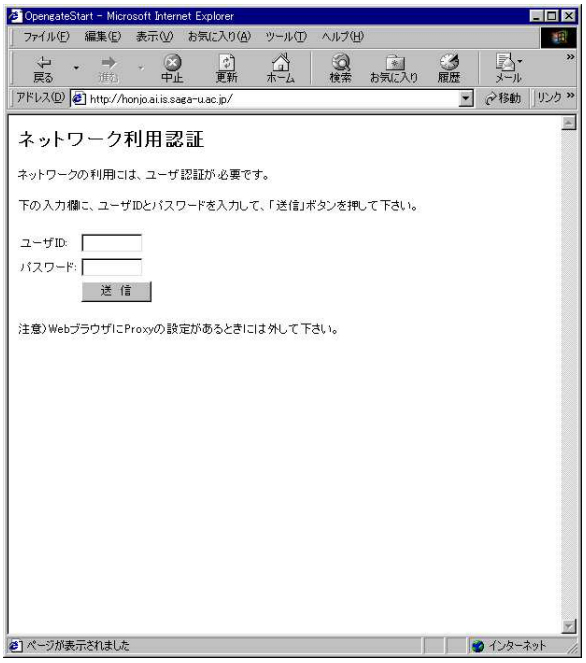

図 3: Web **ページ**

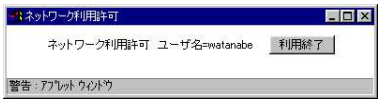

図 4: Java Applet **による利用許可ウインドウ**

Java Applet **は自動的に終了する**)、CGI **プログラムは、それを検知してファイアウォールを閉じ、利用終了を記録して終了する。**

TCP **コネクションが一定時間内に張られない場合は、**CGI **プログラムはファイアウォールを閉じて終了する。よって、**Java Applet **対応でない端末は、一定時間の利用となる。**

4 システムの実現

4.1 システムに求められる機能

Opengate **には、次のような機能が必要である。**

利用者がネットワークを利用する場合、ゲートウェイ部で認証が行われ、利用の記録が残される機能が必要である。この時のインタフェースは、多様な利用者に対応できるように、Web **などの簡便なインターフェイスである必要がある。また、利用の終了と同時に、ファイヤウォールを閉じる機能が必要である。しかもこの機構は、情報コンセントに接続された端末だけでなく、公開端末にも対応できる必要がある。**

本章の以降の節では、Opengate **のユーザインタフェース、利用者の認証とそのセキュリティ、利用終了の監視、そして利用者情報の記録について述べる。**

4.2 ユーザインタフェース

Opengate **では、利用者とのインタフェースに** Web **を採用した。**Web **による** GUI **は一般的で解り易く、使い易いインタフェースとなっている。また、**Web **ブラウザ以外の特殊なプログラムを用いていないため、端末の事前設定が不要である。**

ただし、Opengate **は** Web **ブラウザ (第** 4.4 **節にあるように** Java Applet **が動作することが必要) がインストールされた端末でしか利用できない。しかし、**Web **ブラウザの急速な普及のため、現在では十分一般性を持った** GUI **であると期待できる。**

4.3 利用者の認証とそのセキュリティ

現在のシステムでは、ユーザ名とパスワードを受け取った CGI **プログラムは、利用者がアカウントを持つワークステーションに、**ftp **を用いてログインを試みることで利用者の認証を行なう**[2]**。**

この認証の際、Web **ブラウザと** Web **サーバの間、および** CGI **プログラムと** ftp **サーバの間を、パスワードが生のまま流れることになるため、これらのセキュリティを確保する仕組みを導入する必要がある。**

現在は、Web **ブラウザと** Web **サーバの間のセキュリティについては、**SSL **に対応した** Web **サーバを利用することで、通信内容のセキュリティを確保している。**CGI **プログラムと** ftp **サーバ間は、ネットワークのセグメントを物理的に分けること等で、対策が可能である。**

4.4 利用終了の監視

利用者のネットワーク利用が終了したら、それと同時にファイヤウォールを閉じる必要がある。これを行なうために、Opengate **は、何らかの手段で利用者の利用終了を知る必要がある。**

Opengate **では、利用者の認証が成功すると、利用者の** Web **ブラウザに** Java Applet **を送り、**CGI **プログラムと** Java Applet **との間で** TCP **コネクション**

[2]Radius **や** NIS **等の認証サーバを用いるようにすることも容易である**

```
Dec 23 12:58:22 honjo opengatesrv.cgi[272]: OPEN: user watanabe from 192.168.1.100
Dec 23 15:10:23 honjo opengatesrv.cgi[276]: CLOS: user watanabe from 192.168.1.100 ( 02:12:01 )
```

図 5: 利用者情報の記録

表 1: 各システムの比較

	システム	利用受付の方法	通信路の開放閉鎖の方法	利用終了の判断
1.	山口大方式	Web + CGI にて認証	ipfw 利用	ARP エントリーが消えると閉鎖
2.	東大方式	telnet にて認証	市販 Firewall 利用	telnet 断で閉鎖
3.	慶応大方式	telnet にて認証	IPF 利用	telnet 断で閉鎖
4.	大阪市大方式	専用 ClientSoft	HUB の機能利用	HUB からの通知などで閉鎖
5.	京大方式	Web + CGI にて認証	ipfw 利用	端末監視サーバによる閉鎖
6.	Opengate	Web + CGI にて認証	ipfw 利用	Java Applet との接続断で閉鎖

を張る。Opengate は、このコネクションが切れると、利用者の利用が終了したと判断する。

利用者の利用終了によるコネクション断には、以下の 3 つの場合が考えられる [3]。いづれの場合も Opengate は利用者の利用終了と判断し、ファイヤウォールを閉じる。

1. 利用者が利用許可ウインドウにある「利用終了」ボタンを押した場合。
   この場合は、Java Applet が終了を CGI プログラムに告知する。CGI プログラムはコネクションを切断し、終了する。
2. 利用者がログオフした場合。
   Web ブラウザが終了するため、Java Applet が終了し、コネクションが切断される。
3. 端末がシャットダウンされた場合。
   システムが終了するため、同時に Java Applet が終了し、コネクションが切断される。

利用者が利用中に Web ブラウザを終了すると、Java Applet が終了し、コネクションが切れる。この場合も Opengate はファイヤウォールを閉じるため、継続してネットワークを利用する場合は、再度ブラウザを起動して認証を行なわなければならない。

4.5 利用者情報の記録

Opengate は、利用者の認証の際、利用を開始したユーザ名、端末の IP address、利用開始時刻を SYSLOG に記録する (図 5)。

また、利用終了の際は、上記の情報に加えて、利用時間を記録する。

[3] ネットワークのトラブルによる切断は除外している。

5 他の研究との比較

Opengate と同様に、ネットワークの利用に際して、特に情報コンセントからのネットワーク利用に際して、利用者の認証と記録を行なうシステムの研究がいくつかある [1] [2] [3] [4] [5]。

それぞれのシステムは (a) 利用受付を行う機能、(b) 利用者の認証を行う機能、(c) 通信路の開放閉鎖を行う機能 (d) 利用終了を判断する機能、(e) 通信守秘の確保に関する機能の 5 つが総合されたシステムとなっている。

それぞれについて、(a) 利用受付を行う機能、(c) 通信路の開放閉鎖を行う機能 (d) 利用終了を判断する機能についてまとめると、表 1 のようになる。

表 1 を元に、まずこれらのシステムが、情報コンセントと公開端末の両方に対応しているかを考える。1、4 及び 5 の方式では、利用終了と共に端末のシャットダウンが行なわれる情報コンセントの場合は有効であるが、利用が終了しても端末のシャットダウンが行なわれない公開端末では、利用終了の判断ができない。また、4 の方式では HUB の機能を利用しているため、利用条件が制限される。

次に、利用者へのインタフェースを考えると、2 と 3 の telnet を使う方式は、Web ブラウザ等の GUI を主に使う一般的な利用者には、使いやすいものではないと考えられる。

最後にシステム利用に先立つ設定に関して考える。4 の方式は、専用クライアントを必要とし、利用者側が事前の設定を行わなければならない点が利用者の負担となる。

これに対して Opengate はユーザインタフェースは Web + CGI による一般的なインタフェースを備え、かつ端末側に特別なソフトウェアを事前に導入する必

要がない。また、Java Applet とのコネクション断で利用者の終了を判断する方式のため、情報コンセントと公開端末の両方に対応し、かつ、HUB などの使用する機器に依存しない。

また Opengate は、(b) 利用者の認証を行う機能、(c) 通信路の開放閉鎖を行う機能、(e) 通信守秘の確保に関する機能については、一般的な方法を採用している。そのため、システムの利用環境に応じて他の実装を利用することや、セキュリティーのより強力な実装に置き換えることが可能である。

6 まとめと議論

我々は、公開端末と情報コンセントの両方に対して、ネットワークを利用する際の利用者認証と利用者記録が行なえるゲートウェイシステム Opengate を開発した。Opengate は、以下の特徴を持っている。

1. Web による GUI
2. 情報コンセントと公開端末の両方に対応
3. 利用者の利用終了と同時にファイヤウォールを閉じる機能

Opengate は、利用者の認証と、それに連動してファイヤウォールの開閉を行なう汎用性を持ったシステムである。特定のハードウェアやソフトウェアに依存していないため、DHCP や NAT と組み合わせて情報コンセントの認証システムとして利用する、適当な認証サーバと組み合わせることで一時利用者のネットワーク利用の際の認証システムとして利用する、学外から学内へのアクセスの認証システムとしての利用するなど、さまざまな応用が可能である。

参考文献

[1] 久長穣, 岡田隆, 刈谷丈治: “情報コンセントのユーザ認証について”, 学術情報処理研究誌 No.2, pp. 77 - 81 (1998).

[2] 東京大学情報基盤センター: “ユーザ携帯端末接続環境の試験運用の開始について”, http://www.ecc.u-tokyo.ac.jp/announce/1999/07/09_dhcp.html (1999).

[3] ほそかわ たつみ: “xfw - オープンスペース用 IP 認証システム -”, http://www.itc.keio.ac.jp/%7Ehosokawa/xfw/ (1999).

[4] 石橋勇人, 阪本晃, 山井成良, 安部広多, 大西克美, 松浦敏雄: “情報コンセントにおける認証とアドレス偽造防止を VLAN 機能により実現するシステム LANA2”, 情報処理学会研究報告 99-DSM-14, pp. 137 - 142 (1999).

[5] 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”, 情報処理学会研究報告 99-DSM-14, pp.131 - 136 (1999).