利用と管理が容易で適用範囲の広い利用者認証ゲートウェイシステムの開発

渡辺義明[†] 渡辺健次[†]
江藤博文[††] 只木進一[††]

大学の教育と研究を支援するため，キャンパス全域に公開端末や情報コンセント，無線 LAN 等の配備が進んでいる．我々は，このような不特定多数が多様な端末を接続して利用するネットワーク環境に適用可能な，利用者認証と利用記録を行うためのゲートウェイシステム Opengate を開発した．本システムは，閉鎖状態の端末からゲートウェイを通過する Web アクセスを行うと認証画面が表示される平易なインタフェースを持つ．認証には POP や FTP サーバが利用できる．認証後には端末へ Java Applet を送って利用終了を監視する．このような方法により，ゲートウェイシステムの設定だけで，個人持参の PC から固定設置の Web 専用端末まで，多様な端末群を利用者の事前設定なしに制御できる．本システムはすでに，学内において約 9 カ月にわたり支障なく稼動している．

An User Authentication Gateway System with Simple User Interface, Low Administration Cost and Wide Applicability

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

To support educational and research activities, a lot of “terminals for public use,” “network sockets” and “wireless LAN” are implemented in the whole area of the campus. We have developed a gateway system named “Opengate” to authenticate and record users in such an open network environment. When an user accesses from a terminal in closed state to any web site through the gateway system, the system returns the page for authentication. To authenticate the user, POP and FTP servers are applicable. After the authentication, the system sends Java Applet to the terminal and watchs the usage. The setup procedure is needed only for gateway system. Without any setup of each terminal, the system controls wide variety of terminals, from web specific terminals for public use to personal PCs connected to network socket or wireless LAN. The system has been working for 9 months in our campus.

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（ホール等のパブリックスペースに設置された端末）や情報コンセント・無線 LAN を，キャンパス全域で整備する大学が増えている．研究者だけでなく，学生にとっても電子メールが日常的なツールとなり，Web で情報を収集・発信することが一般的に行われるようになった現在，容易にネットワークへアクセスできる環境は，大学が整備すべきものの 1 つとなっている．

ところが公開端末においては，利用者の認証や利用記録の保存といった機能がシステムとして備わっていない機器がすでに多数設置されており，今後も Web 専用端末等において増えると予想される．また認証機能があってもパブリックスペースに広く分散配置された機器を適切に管理することはきわめて困難である．情報コンセントや無線 LAN の場合には，利用者が自ら携帯したコンピュータを接続するだけで，即座にネットワークが利用できるようになる．これらの結果，大学のネットワークの利用資格がない者（たとえば大学に無関係の人物）に，大学が設置しているネットワークを利用されてしまうことを防ぐことができないだけでなく，ネットワークの利用者を後から特定することが難しいという問題が生じている．

大学のネットワークは，大学における教育研究を支

† 佐賀大学理工学部
Faculty of Science and Engineering, Saga University
†† 佐賀大学学術情報処理センター
Computer and Network Center, Saga University

援することを目的として構築され，原則として大学の構成員が利用資格を持つものである．したがって，情報コンセントや公開端末においても，利用資格を有する者のみが利用できるようにする仕組みが必要である．また，インターネットが社会における情報流通の基盤となった現在では，利用者の無制限なネットワーク利用を放置することは許されなくなっている．特に，大学から他サイトへの攻撃，不適切な内容のメールの送信やWebへの書き込み等が行われた場合を想定して，そのような利用を行った者を事後に特定できる仕組みを持つことが必要である[1]．

このようなネットワークの利用者認証と利用者記録を行うシステムの構築を考える場合，利用者の操作容易性，端末や接続形態の適用範囲の広さおよび管理の容易性について配慮が必要である．しかし，従来提案されているシステム[4)~10)]では，キャンパス規模の運用において，これらの条件を十分に満たしているとはいい難い．本論文では，汎用の技術を組み合わせることにより，これらの条件を満たし，現実にキャンパス規模で運用可能である利用者の認証と記録のためのシステムOpengateを提案する[2),3)]．

2. 利用者認証ゲートウェイシステムに必要な機能とその実現

ネットワークの利用における利用者の認証と記録を，ゲートウェイシステムとして実現することを考える．具体的には，利用者がネットワークを利用する際にゲートウェイ部で認証を行い，利用の開始と同時に通信路を開き，利用の終了と同時に通信路を閉じる機能，および利用の際の記録を行う機能を備えたシステムである．

このようなシステムを構築するためには，次に示すそれぞれの機能を実現する必要がある．また，これらの機能の実現にあたっては，利用者の操作容易性，端末や接続形態の適用範囲の広さおよび管理の容易性について考慮する必要がある．

(1) 利用受付を行うユーザインタフェース
(2) 利用者の認証を行う機能
(3) 通信路の開放閉鎖を行う機能
(4) 利用終了を判断する機能
(5) 利用者の情報を記録する機能

すでにネットワーク利用者の認証と記録を行うシステムが，いくつか提案されている[4)~10)]．これらのシステムでは，上記の各機能について様々な実現方法をとっている．特に(4)の利用終了を判断する機能について，多様な工夫がなされている．しかし，操作容易性，汎用性または管理容易性について難がある．

まず，利用者にTelnetでサーバへ接続させ，このコネクションが切断された時点を利用終了と見なす方式がある[4),5)]．この方式は，ウインドウシステムや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．また，Telnet機能のない端末では利用できない．

次に，端末に専用クライアントソフトをインストールしておき，これによって終了を監視する方式がある[4),6),7)]．しかし，端末へのインストール作業等を行わなければならない点が管理者または利用者の負担となり，また稼動機種が制限されることにもなる．

また，HUBのリンクダウンを監視する方法がある[6)~9)]．この方式は，利用終了とともに端末のシャットダウンが行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をシャットダウンしない公開端末では，利用終了の判断ができない．

さらに，ARPエントリの消滅を監視する方法[10)]や，HUBの接続状況を定期的にチェックする方法[8)]では，公開端末に適用できない点に加えて利用終了の判断が即座にできない点が問題である．

一方Opengateでは，多数の利用者にとって馴染みやすいWebによるインタフェースを機能(1)のインタフェースに採用し，認証後に端末側にJava Appletを送りこんで終了を監視する方式を，機能(4)に対して新しく考案した．Javaの稼動するWebブラウザは，現在のネットワーク利用端末には，ほぼ標準の機能として備わってきているため，利用者は標準設定のままで，このシステムを利用できる．

機能(2)の個人識別については，パスワードによる方式が現状では一般的である[4)~10)]が，他に端末のMACアドレスを個人識別に利用する方法も考えられる．しかし各個人の所有する機器のMACアドレスを事前に登録する作業が管理負担となる．また機器の廃棄や譲渡にともなうMACアドレスの変更，削除の申請は期待できない．

機能(3)の通信路制御については，ファイアウォールを利用するシステムが多い[4),5),8),10)]．HUB装置の持つフィルタリング機能を利用するもの[6)]やVLAN機能を利用するもの[7),9)]も提案されているが，広範囲に適用するには，対応HUB装置を多数個揃え，その設定を行う必要がある．また開放・閉鎖の制御はファイアウォールの方が容易である．

Opengateでは，機能(2)にはパスワードによる方法を，機能(3)にはファイアウォールを利用する．また機能(5)の記録にはSYSLOGを用いる．

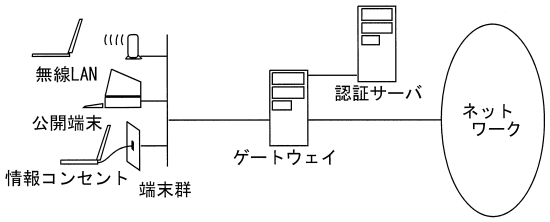

図 1 ハードウェア構成
Fig. 1 The hardware configuration.

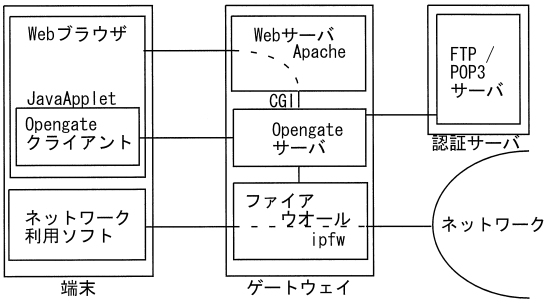

図 2 ソフトウェア構成
Fig. 2 The software configuration.

3. Opengate の概要

本章では我々が開発した Opengate の構成と利用者からの見え方，システム内部の流れについて述べる．

3.1 構　　成

図 1 にハードウェア構成を示す．Opengate は，端末群と利用ネットワークとの間にゲートウェイを設置し，そこを通過するパケットをフィルタリングするシステムとして実現した．利用者の認証は別に設置した認証サーバを用いる．

図 2 にソフトウェアの構成を示す．Opengate のサーバ側プログラムは，Web サーバから CGI として起動される．このプログラムは，認証を行いファイアウォールを制御するとともに，端末側にクライアントとなる Java Applet を送り，利用終了を監視する．

現在，Opengate は FreeBSD 上に構築されており，ファイアウォールの開閉には ipfw を，また Web サーバには Apache を用いている．これらは，他のプラットフォーム上を含めて様々な実装方法が可能なものである．

3.2 利 用 手 順

Opengate が動いている環境で，ネットワークを利用するときの手順を以下に示す．

(1) 端末を準備して Web ブラウザを起動する．
(2) 任意の URL へのアクセスを行うと，ユーザ ID とパスワードを要求する認証ページ（**図 3**）が送られてくる．
(3) ユーザ ID とパスワードを返答する．
(4) 認証を通れば，その由を知らせる Web ページ（**図 4**）が送られてくる．
(5) 認証後，Web ブラウザが終了するまでネットワークを自由に利用することができる．なお，Telnet や FTP 等，Web 以外のネットワークアプリケーションを利用する場合も，まず上記の手続きをとって認証を受け，Web ブラウザを保持することが必要である．
(6) 利用終了時には Web ブラウザを終了する．

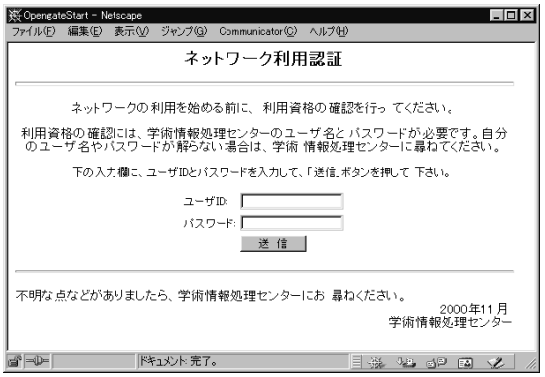

図 3 ネットワーク利用認証を受けける Web ページ
Fig. 3 The interface for user authentication.

図 4 利用許可ウインドウ
Fig. 4 The windows displayed to an authenticated user.

3.3 システムの流れ

利用者が，上で示した手順を行った場合のシステム内部の流れを**図 5** に示す．

(1) Web アクセスのパケットがゲートウェイに届くと，ファイアウォール ipfw は，そのパケットの通過可否を判断し，通過不可のときはローカルの HTTP ポー

トへ Forward する．ローカルの Web サーバは，認証要求のページを利用者の Web ブラウザへ返送する．

(2) 利用者によって認証要求のページに入力された利用者 ID とパスワードは，CGI に渡される．

(3) CGI は，ARP から MAC アドレスを取得し，端末を同定する情報として保持する．また認証サーバと通信することで利用者の認証を行う．

(4) 認証が成功すると，CGIはファイアウォールを開き，SYSLOG により利用者の情報を記録する（**図 6**）．さらに，CGI は利用者の Web ブラウザに Java Applet 付きの許可表示のページを送り，その Java Applet からの TCP コネクションを待つ．

(5) 利用者の Web ブラウザに送られた Java Applet は，CGI との間に TCP コネクションを張る．

(6) CGI は，Java Applet との TCP コネクションのクローズを監視するとともに，定期的に Java Applet とメッセージを交換する．さらに，通過パケット数をファイアウォールから定期的に取得する．

(7) 以下のいずれかから利用終了を検知すると，CGI は，ファイアウォールを閉じ，利用終了を記録して終了する．

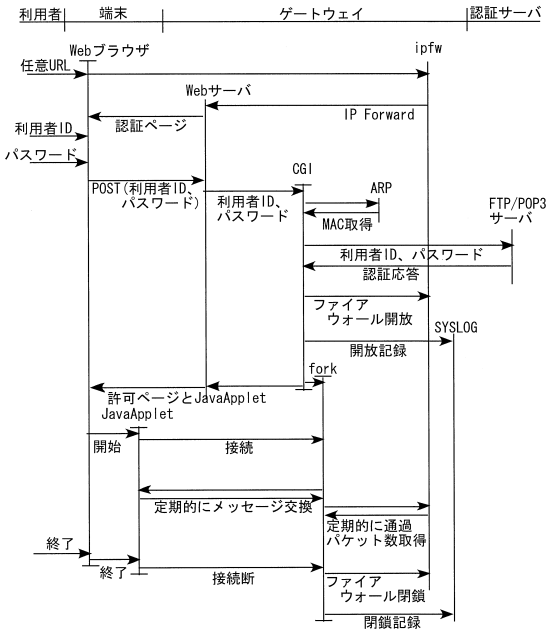

図 5 システムの流れ
Fig. 5 Work flow of the system.

(a) Web ブラウザの終了によって Java Applet が終了し TCP コネクションがクローズした．(b) ネットワーク切断やシステムの強制終了等によって Java Applet との定期的メッセージ交換に失敗した．(c) 一定期間にわたり当該端末との間にパケットが流れない．

4. Opengate の各機能

本章では，2 章で述べた，システムに必要な機能について，Opengate の実装方法について述べる．

4.1 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 は一般的で分かりやすく，多くの人にとって使いやすいインタフェースである．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り，多くのプラットフォームで利用できる．さらに，任意の URL へのアクセスで認証画面が表示されるようになっており[8]，認証のための特別な URL への接続を利用者に求める必要がない．

ただし，Opengate は Java Applet が動作するブラウザでの利用を前提としている．このため，Java が実行できないプラットフォームでは利用できないという制約がある．しかし現在，多くのブラウザで Java Applet が実行できることを考えると，大きな制約ではないと考える．

Opengate は図 4 に示すように 2 つのウインドウを表示する．1 つは（図 4 で後ろに隠れているウインドウ）は，Java Applet を起動し，認証が行われたことを示すものである．もう 1 つは，通常の HTML で記述されたページで，よく使うページへのリンク等を含むものである．この前面のウインドウから，利用者はそれぞれの目的とする URL へ移動することができる．

このように 2 つのウインドウを表示する理由の 1 つは，Web ブラウザによっては，Java Applet を表示したウインドウから他の URL へ移動することによって，Java Applet が停止してしまうことがあったためである．また試験運用中に指摘された，ウインドウが誤って閉じられたときに認証からやり直しとなる煩わしさを，2 つのウインドウを用意することで緩和できる．

```
Mar  7 11:51:53 adam opengate.cgi[327]: OPEN: user wata from 192.168.0.2 at 0:0:f8:1a:68:6b
Mar  7 11:53:14 adam opengate.cgi[332]: CLOS: user wata from 192.168.0.2 at 0:0:f8:1a:68:6b ( 00:01:21 )
```

図 6 利用者情報の記録
Fig. 6 Examples of the records in log file.

```
default:tc=cc
cc:address=server.cc.saga-u.ac.jp:protocol=ftp:
is:address=server.is.saga-u.ac.jp:protocol=pop3:
```

図 7 設定ファイルの例
Fig. 7 An example of the configuration file.

4.2 利用者の認証

現在運用中のシステムでは，利用者 ID とパスワードを受け取った CGI は，利用者がアカウントを持つワークステーションに FTP または POP を用いてログインを試みることで，利用者の認証を行う．

この認証の際，Web ブラウザと Web サーバの間，および CGI と認証サーバの間のセキュリティを確保する仕組みが必要である．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 を利用している．CGI と認証サーバ間は，物理的にネットワークを分けることや各種セキュリティプロトコル層を挟むことで対策が可能である．また RADIUS や APOP 等の安全な認証サーバへの対応も可能である．

利用者の管理が学部等複数組織に分散している場合のために，認証サーバを複数設置して利用者を振り分けることも可能としている．すなわち，利用者 ID の代わりに，“利用者 ID@認証サーバ名” の形式で入力すると，設定ファイル（**図 7**）で指定したサーバに，指定したプロトコルで認証を要求する．

4.3 通信路の開放閉鎖

通信路の開放閉鎖は，FreeBSD 標準のパケットフィルタリング型ファイアウォールソフトウェアである ipfw を利用した．ipfw は制御ルールを列挙することで，パケットの送信元，送信先，ポート番号等とルールを比較し，最初に合致したルールに従い，パケットの制御を行う．制御ルールの最後尾にはすべて拒否のルールを置き，その上位に各端末に対する通過許可のルールを CGI が挿入することで通信路の開放を行い，削除することで取り消す．

また，HTTP に対する IP Forward ルールを，CGI が挿入するルールよりも優先順位の低い位置に置くことで，挿入した許可ルールのどれとも一致しない HTTP パケットはローカルの Web サーバへ向き，許可ルールと一致したパケットは通過するようにした．

さらに，CGI が挿入するルールよりも優先順位の高い位置に通過や拒否のルールを設定することで，つねに開放もしくは閉鎖状態に置くサービスを指定することができる．たとえば，特定のメールサーバや Web サーバを認証なしでアクセスさせる等の制御が容易である．

4.4 利用終了の監視

ネットワーク利用が終了したら，それと同時にファイアウォールを閉じる必要がある．そのためには利用者の利用終了を即座に知る必要がある．Telnet や FTP では，コネクションがなくなれば，利用が終了したと見なすことができる．しかし，現在よく利用される HTTP や POP 等では，コネクションは間欠的であり，利用者の利用終了まで継続しない．よってコネクションの状態からは利用終了を判断できず，利用状況を監視する仕組みが別に必要である．

そこで 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 と Java Applet との間で TCP コネクションを張ることによって利用状況の監視を行っている．Opengate は，このコネクションのクローズで利用者の利用終了を検知する．これは，利用者が Web ブラウザを終了した場合，ログオフした場合，シャットダウンした場合に対応できる．

さらに，正常な終了処理をせずに，強制終了やネットワークからの切断等を行った場合に対応するため，端末との間に定期的なメッセージ交換を行っている．また，終了処理をせずに放置した場合に対応するため，ファイアウォールを通過したパケット数を定期的に取得し，利用が継続しているか否かを判断する方法を付加した．

4.5 利用者情報の記録

Opengate は，利用者の認証の際に，利用を開始した利用者 ID，端末の IP アドレス，MAC アドレス，利用開始時刻を SYSLOG の機能を用いて記録する．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．

これらの情報により，たとえば不正行為等が発生しても，ネットワークの利用者を事後に特定することができる．なお，MAC アドレスはゲートウェイ側から見えるアドレスであり，また Ethernet 以外の環境では意味を持たない等の難点があるが，個人特定時の参考情報として記録している．

5. 運 用 評 価

5.1 環　　境

今回開発した Opengate は，発生した障害や誤操作への対策を行いながら，徐々に運用範囲を拡大している．現在，以下の環境で長期運用している．

(1) 佐賀大学学術情報処理センター：情報コンセントおよび無線 LAN に持参 PC を接続して利用している．同時使用は数台であるが約 9 カ月の実績を持つ．

表 1 利用者の評価
Table 1 Rating by users.

選択項目	パーセント
問題なく使える	16
まあまあ使える	34
面倒だが使える	47
使えない	3

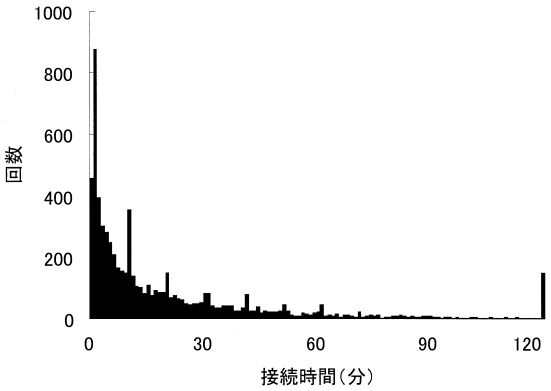

図 8 接続時間ヒストグラム
Fig. 8 Histogram of connection time.

(2) 佐賀大学文化教育学部演習室：Windows98 ベースの PC が 44 台設置されていた演習環境に，後から Opengate を導入した．演習および自習に利用されており約 6 カ月の運用実績がある．ゲートウェイは上記 (1) と共用している．

(3) 佐賀大学附属図書館：ロビーと閲覧室に，Windows98 および WindowsNT ベースの PC が 15 台，WindowsCE ベースの Web 専用端末が 20 台，多数の情報コンセントおよび無線 LAN 装置が設置されている．PC と Web 専用端末は頻繁に利用されているが，情報コンセントと無線 LAN の利用は，現時点ではきわめて少数である．この環境に独立のゲートウェイを設置し，運用を開始してから約 2 カ月となる．

5.2 結　　果

文化教育学部演習室の利用者に対してアンケートを行い，32 名から回答を得たところ，**表 1** のとおりに許容できる範囲との評価であった．

また，24 台の PC からいっせいに認証要求を行う負荷実験を行った．その結果，送信ボタンを押してから利用許可のページが表示されるまで，通常は数秒以内であるところ，最大約 15 秒を要したが，エラーを起こすことなく正常に動作した．

図 8 は，附属図書館環境における 2 カ月間の利用記録ファイルから利用者の接続時間長を調べたものである．1 分刻みに集計しており，右端は 2 時間を超す利用回数を示す．これから広範な利用がされていることが分かる．運用では，Java Applet を送付した後 TCP コネクションを待つ時間を 2 分に，また定期的メッセージ交換の間隔を 10 分に設定している．図 8 中のピークは，これらのタイミングに端末が反応しないことによる強制終了の結果である．

表 2 利用記録回数
Table 2 Counts of log records.

利用記録	回数
認証を通過して利用を開始した	6,642
パスワードが誤っている	1,963
同一端末から重複して認証要求があった	1,158
端末との TCP コネクションに失敗した	465
端末がメッセージ交換に返答しない	455
認証サーバとの接続に失敗した	77
長期間にわたりパケットの通過がない	52

同じ利用記録ファイル中のエラー記録状況を調べたところ，**表 2** のようにパスワードの入力誤りが最も多くあった．重複認証要求と Java Applet 接続障害の多くは，Java Applet の起動完了を待てないことに起因すると思われる．これらのエラーは利用に習熟するとともに減少するであろう．

システムのトラブルは，プログラミングの誤りを除くと，主として利用者側インタフェースである Web ブラウザの不具合によるものであった（たとえば SSL 処理や POST 処理等の不具合）．Web ブラウザとして新しいバージョンのインストールを依頼することが複数発生した．

代表的な適用環境として考えられる演習教育環境および開放利用環境の双方において，数十人規模の利用者が頻繁に利用しているが，長期にわたり大きなトラブルもなく稼動している．利用者の観察においても適切に利用できている様子が見られる．

6. 考　　察

6.1 スケーラビリティ

現在の Opengate では，確実に動作する単純なプログラムの作成に重点を置いて，1 つの端末に対してサーバプロセスが 1 つ動作するマルチプロセスの構成となっている．多数の端末を制御する場合の負荷軽減を目的として，複数の端末を 1 つのサーバプロセスで一括管理する方式は今後の課題である．ただし，サーバプロセスは認証時の処理を除くと数分に 1 度の定期的な端末監視処理だけであり，他の時間は入出力またはタイマ割込みを待つ状態にある．実際にネットワークを利用中のゲートウェイの負荷は，主としてファイアウォールやパケット転送等の処理にある．

ゲートウェイの負荷分散の点，さらに管理区分ごと

に個別の制御方針をとれる点から，複数台のゲートウェイを用意し，各々が最大クラスC程度のアドレス空間を制御するように分散配置することが適当であると考える．複数ゲートウェイを管理する負荷は，ゲートウェイをディスクレスとし[11]統合管理することで軽減が可能である[12]．

6.2 利用の容易性

Opengateは，Webブラウザを利用者インタフェースとしている．専用クライアントソフトやTelnetを利用するシステムに比較して，設定と利用が容易である．また，指定したURLへのアクセスではなく，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[8]となっている．実際の運用においても簡単な説明書を置くだけで特に戸惑うことなく使えている．アンケート結果から見ても許容できるという答えがほとんどであった．

6.3 管理の容易性

Opengateは，各端末やHUB装置等の個別の設定は不要であり，持参の端末をそのまま利用できる．また，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することも可能である．ゲートウェイの設定のみで制御可能であるため，端末やHUB装置等の設定を行う必要のあるシステムに比較して作業量が少なく設定変更が容易である．

認証のためには利用者IDとパスワードを必要とするが，大学の正規構成員であれば情報処理センター等ですでにその情報を所持しているであろう．複数の認証サーバに利用者を振り分けることも可能としており，利用者を学部別等に分散管理している環境でも適用できる．

図書館利用や学会等で訪問した正規構成員以外の一時的利用者には，現在のところ以下の運用を行っている．一時利用者用の認証サーバを用意する．必要数の利用者IDを利用期限付きで登録し，同時に利用者IDとパスワードおよび利用上の注意を書いた用紙を利用者IDごとに印刷する．利用希望者が来訪すれば，身元を確認して用紙を1枚渡す．当然ながら本利用者IDは学内のサーバへのログイン等は利用できない．

6.4 汎 用 性

Opengateは，標準的なソフトウェアで構成している．現状では，ファイアウォールにはFreeBSDのipfwを使用しているが，同等の機能があれば他のファイアウォールにも対応可能である．また，EthernetやHUB装置等のハードウェア仕様にも依存していない．これらに依存するシステムに比較して広範な用途に適用可能である．たとえば以下のような利用方法が考えられる．

(1) セキュリティ保護のないPCで構成されている遠隔の演習室や公開端末等に対してセキュリティを付加することに利用する．

(2) DHCPやNATと組み合わせて，情報コンセント，無線LANに対する認証システムとして利用する．

(3) 学外から学内を利用するときの入り口として利用する．ファイアウォールの設定により，特定のサーバやサービスのみを開放することも可能である．

(4) 学内から学外への出口として利用する．標準では許可できないが，認証を受ければ許可するサービスを設定できる．

6.5 制 限

Opengateは，利用者認証を通ったIPアドレスに対して，ネットワーク利用の許可を与えるシステムとして構成したため，IPアドレスの詐称には注意を払う必要がある．

特に，利用者の端末とゲートウェイとの間にIPアドレスを集約・変更するNATやProxy等の装置を挟まれないようにする必要がある．端末のIPアドレスを詐称することも考えられるが，使用していないIPアドレスを詐称しても意味がなく，使用中のIPアドレスを単純に重複使用すると通信誤りを起こす．なお，Opengateは利用者の認証と記録を行うシステムとして実現したものであり，悪意を持った利用者への対策は別のシステムとして実現し，組み合わせて利用することを想定している．

7. ま と め

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えるゲートウェイシステムOpengateを開発した．Opengateは，公開端末と情報コンセント，無線LAN等に接続された端末に対して利用終了を即座に検出でき，また利用者側で事前設定することなく容易に利用できるWebによるインタフェースを持つという特徴を有している．管理負担も少ない．すでに長期にわたり安定して運用できている．

今後，大学教育におけるインターネット利用の重要性が，いっそう増すことが考えられる．そのためには，コンピュータ演習室だけでなく，一般教室や自習室への情報コンセントや無線LANの整備，ホール等への公開端末の設置が必要であると考えられる．このような，多様な機器が接続され，また，多様な利用者が利用するオープンスペースのネットワークに対して，Opengateの利用者認証および利用記録機能は有効である．

参 考 文 献

1) JPCERT/CC：技術メモ—コンピュータセキュリティインシデントへの対応，JPCERT-ED-2000-0007 (2000). http://www.jpcert.or.jp/ed/2000/ed000007.txt
2) 渡辺健次，江藤博文，只木進一，渡辺義明：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，信学技法，Vol.99, No.591, pp.43–48 (2000).
3) 渡辺義明ほか：Opengate ホームページ (2000). http://www.cc.saga-u.ac.jp/opengate/
4) 株式会社ピーエフユー：Safegate (1999). http://www.pfu.co.jp/sales/safegate.htm
5) 細川達己：xfw—オープンスペース用 IP 認証システム (1999). http://members.itc.keio.ac.jp/~hosokawa/xfw/
6) 石橋勇人，山井成良，安部広多，大西克美，松浦敏雄：IP アドレス/MAC アドレス偽造に対応した情報コンセント不正アクセス防止方式，情報処理学会論文誌，Vol.40, No.12, pp.4353–4361 (1999).
7) 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).
8) 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).
9) 広島大学総合情報処理センター：PortGuard (2001). http://www.portguard.org/
10) 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).
11) 山森丈範：PXE で FreeBSD をディスクレスブートしよう，パワーアップ FreeBSD（Software Design FreeBSD Issue），pp.166–175，技術評論社，東京 (2001).
12) 只木進一，江藤博文，渡辺健次，渡辺義明：公開端末および利用者移動端末の認証システムとそのディスクレスマシンによる運用，学術情報処理研究，No.5, pp.15–20 (2001).

(平成 13 年 4 月 20 日受付)
(平成 13 年 9 月 12 日採録)

渡辺 義明（正会員）

昭和 24 年生．昭和 52 年九州大学大学院工学研究科博士課程通信工学専攻単位取得退学．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．

渡辺 健次（正会員）

昭和 39 年生．平成元年佐賀大学大学院理工学研究科物理学専攻修士課程修了．同年同大学情報処理センター助手．平成 5 年和歌山大学経済学部産業工学科講師．平成 8 年同大学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．教育システム，インターネット，分散システム運用技術の研究に従事．博士（工学）．平成 7 年情報処理学会全国大会奨励賞，平成 10 年教育システム情報学会論文賞受賞．

江藤 博文（正会員）

昭和 40 年生．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助手，現在佐賀大学学術情報処理センター助手．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．

只木 進一（正会員）

昭和 34 年生．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．平成 12 年 10 月から同大学学術情報処理センター教授．計算物理学，統計力学を専門とする．理学博士．