利用者移動端末に対応したネットワークの運用
– 佐賀大学での Opengate の運用 –

只木進一* 、江藤博文
佐賀大学学術情報処理センター
渡辺健次、渡辺義明
佐賀大学理工学部知能情報システム学科

概 要

利用者がノート型などの移動型端末を携行している状況が日常化している。こうした移動型端末の接続環境の整備も進んでいる。我々は、利用者移動端末や公開端末からのネットワーク利用を認証する Opengate を開発してきた。その全学規模での運用に向けた技術と運用上の問題点について報告する。

1 はじめに

コンピュータとインターネットの利用は、生活のあらゆる部分に普及している。大学においては、学生や教職員など利用者個人がノート型パーソナルコンピュータ (PC) を携帯する姿が増えている。学生がこうした移動型端末を携帯していることを前提とした教育カリキュラムも増えつつある。

利用者の移動型端末を大学内で有線あるいは無線を介してインターネットへ接続するための、ネットワークシステムの開発も近年盛んに行われている。事前に利用者や端末に関する情報を登録したり専用ソフトウェアをインストールするものから、単に認証などを通じてゲートウェイを開閉するものまで、いくつかの方式が提案されている [1–5]。

我々は、利用者の移動型端末から Web を利用する際に認証を行う Opengate システムを提案し、運用してきた [6, 7]。Opengate では、利用者は特別な申請やソフトウェアの準備なしに、利用することができる。また、システムも、平均的な機器構成で構築することができる。また、大規模に運用するために、Opengate をディスクレス化し、集中管理する手法の開発も行ってきた [8]。

実際に、利用者の移動型端末に対応したネットワークを全学規模で運用すると、様々な問題が発生する。大学ネットワークの管理者の手が届かない端末が多数発生することで、不適切なネットワーク利用に使われる端末やコンピュータウィルスを感染させる端末が多数発生する。

本稿では、ディスクレス化することによる Opengate の大規模運用と、実際に運用した際の障害と対策について報告する。

2 Opengate の仕組み

Opengate は、利用者が持ち込むノート型 PC などの移動型端末を接続するネットワークとインターネットの間に設置するゲートウェイである。利用者が Web を介してインターネットへ接続しようとする要求を契機に、利用者の Web ブラウザに認証画面をダウンロードし、認証によってファイアウォールを開閉する [6, 7]。

動作の流れを図 1 に示す。利用者が Web を介してインターネットへ接続しようとする要求は、Opengate 上で稼働するファイアウォールによって Opengate 上の Web サーバへと転送され、利用者の Web ブラウザに認証画面がダウンロードされる。

Web ブラウザから送られた利用者名とパスワードを使って、別に設置された認証サーバへの認証が行われ、成功するとファイアウォールが開かれる。Web ブ

*e-mail:tadaki@cc.saga-u.ac.jp

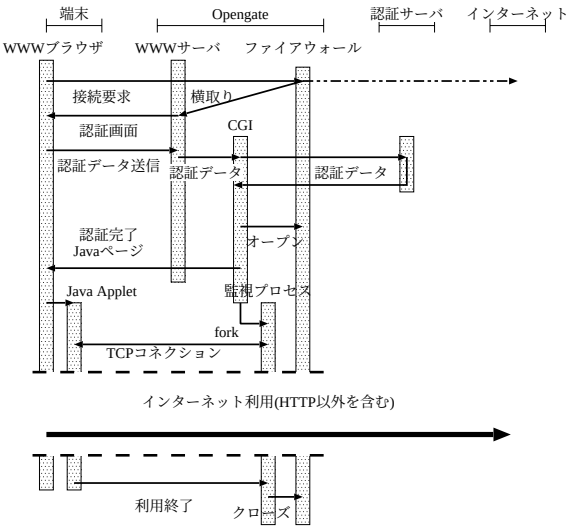

図 1: Opengate の動作の流れ

ラウザには認証成功を知らせるページとともに Java Applet がダウンロードされ、監視プロセスとの通信で利用していることをモニタする。

Java Applet が停止する、あるいは一定時間の間通信が行われないと監視プロセスは利用終了と判断し、ファイアウォールを閉じる。Java Applet が動作しない端末でも、あらかじめ設定された時間の間、通信が可能なようにすることも可能である。

このシステムを利用するには、クライアント側に Web ブラウザ以外の特別なソフトウェアを必要としない。また、認証サーバへは ftp や pop などを使うため、既に運用している情報システムを利用することが可能である。つまり、特別な利用登録も必要としない。

従って、Opengate は利用者が携帯する移動型 PC だけでなく、利用者認証機構を持たない固定の公開端末群のゲートウェイとしても利用することが可能である。

Opengate 本体は、FreeBSD 上で動作している。ファイアウォールには ipfw、Web サーバには Apache が、監視プロセスには C プログラムが使われている。その他、必要なソフトウェアは、DHCP と NAT である。つまり、NIC を 2 枚以上持つ通常の PC-UNIX で構築することが可能である。主要ソフトウェアを表 1 に示す。

表 1: Opengate を構成する主要ソフトウェア

種類	ソフトウェア名
OS	FreeBSD5.1
ファイアウォール	ipfw(OS 附属)
NAT	natd(OS 附属)
Web サーバ	Apache 2.0
DHCP	isc-dhcp3

3 ディスクレスによる Opengate の大規模運用

3.1 ディスクレスの必要性

1 台の Opengate で全学規模の運用することには問題がある。第一の問題は、処理能力の問題である。通常の利用であれは、100 台規模のクライアント数であっても問題なく動作することが確認されている。しかし、後述する MSBlaster のようなネットワーク帯域を消費するタイプのウィルスが活動する場合には、10 台程度の MSBlaster を有するクライアントの存在でシステム停止を招く。

第二の問題は、障害や不適切な利用があった場合への対応である。そのような場合に、迅速にクライアントの場所と利用者を特定し、対処する必要がある場合がある。また、そのようなクライアントからの影響が他のクライアントへ及ぶことを最小限にする必要がある。そのため、適当に分割されたネットワークごとに Opengate を設置することが望ましい。

第三に、冗長性の確保と拡張性が必要である。多くの利用者が個人の移動型 PC を携行するようになっており、そのような移動型 PC を接続できるネットワークを安定してサービスするには、機器の障害時に迅速に復旧できることと、対象箇所の拡大が容易である必要がある。

そこで、佐賀大学では、ほぼ建物ごとに設置された 21 台の Opengate を運用し、二つのキャンパスにわたって利用者移動端末の接続サービスを行っている (図 2)。

多数の Opengate を運用するために、佐賀大学ではそれらをディスクレスで運用している [8]。ディスクレスで運用することで、各 Opengate の IP アドレスなど少数の個別設定以外を共通として、多数の Opengate

図 2: ディスクレス Opengate 群

を安定運用することが可能となる。

Opengate 運用のネットワーク構成を図 3 に示す。各 Opengate の起動と NFS マウント、ログ収集のための専用閉鎖ネットワークを設定してセキュリティの保持をしている。認証は、研究教育用システムと同じ利用者認証が可能な汎用認証サーバを利用している [9]。

3.2 ディスクレスシステムとファイアウォール

FreeBSD のディスクレス起動では、DHCP サーバからネットワーク情報と起動プログラム PXEBOOT の場所に関する情報を得た後、TFTP を使って PXEBOOT をダウンロードする。PXEBOOT は NFS を介して kernel を取得し、OS を起動する。ルートパーティション以下全てを NFS でマウントするが、/var と/etc はメモリ上に置かれる。FreeBSD5 からは、ブートサーバの/usr もマウントする仕様となっている。ルートパーティション下の/conf/IP アドレス/etc 以下に端末固有の情報を格納すると、ディスクレス起動時に/etc に

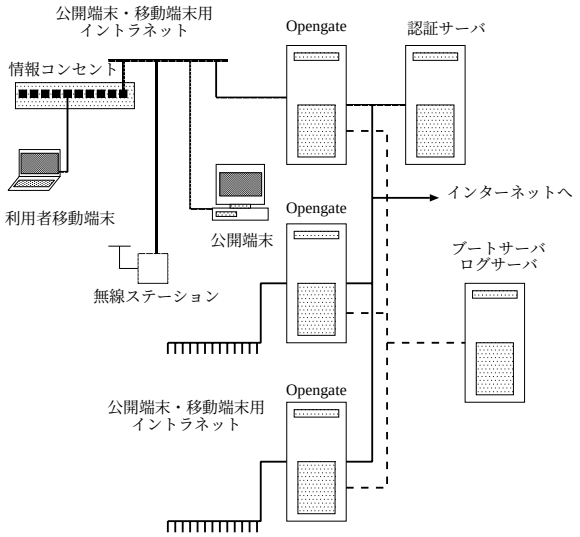

図 3: ディスクレス Opengate の運用ネットワーク

上書きが行われる。

Opengate はファイアウォールと NAT を利用するシステムである。このようなシステムをディスクレスで運用するためには、注意が必要である。第一は起動時に、ファイアウォールが開放になっていなければ、NFS マウントそのものができなくなってしまう。FreeBSD では、デフォルト設定がファイアウォールを完全閉鎖するようになっている。kernel の設定を変更するとともに、ファイアウォール規則 (/etc/rc.firewall) で、最後に全てを閉じる記述が必要である。

NAT はファイアウォールからパケットを転送される。しかし、FreeBSD の起動順序では、ファイアウォール起動時には NATD が起動されておらず、この時点で通信が停止してしまう。そこで、ファイアウォールへの転送は起動時には行わず、起動順序の最後にファイアウォール規則に NAT への転送を追加するように変更が必要となる。

各 Opengate のログは、syslog を通じてログサーバへ集約している。集約されているログは、Opengate の開閉、Web サーバのアクセス及びエラー及びファイアウォールのログである。

3.3 ホストごとの設定

各 Opengate ごとに異なる設定は、データベースに情報が蓄積され、テンプレートからスクリプトで生成するなどでほぼ自動生成することができる。各 Opengate ごとに異なる情報の中心は、IP アドレス、ネットワークアドレス、NIC のデバイス名であり、これらはほぼ `/etc/rc.conf` を通じて設定することができる。

各 Opengate ごとの dhcp サーバの設定は、テンプレートから生成した後、各 Opengate 下に設置されている固定端末の情報をデータベースから取得して追加する。この設定は`/etc/`に置かれるように設定している。

附属図書館用 Opengate には、OPAC(Online Public Access Catalog) や電子ジャーナルなど認証無しで通過させる設定が必要となっている。今のところ、この特殊設定は、一旦生成された`/etc/rc.firewall` に手動で挿入している。

Web サーバの設定及び Web ページも`/etc/apache` の下に設置し、Opengate ごとに異なる設定が可能となっている。SSL のキーも各 Opengate に設定されている。

4 利用状況

佐賀大学は、2003 年 10 月の佐賀医科大学との統合によって、新たに医学部が増え、5 学部で構成されている。医学部のあるキャンパスへの Opengate の設置は附属図書館分館に限られているが、佐賀大学の医学部以外があるキャンパスの全域で Opengate を介して有線無線のインターネット利用が行える。

最近の利用状況を表 2 に示す。利用数は Opengate を通じた認証成功数をのべで表している。附属図書館 (Opengate00) がもっとも利用が多いが、ここには 50 台以上の固定端末があり、認証に Opengate が利用されている。Opengate12 下には情報系学科があり、学生個人の移動型 PC を教育に利用しているため、利用が多い。Opengate14 下にあるのは化学系学科だが、個人の固定型 PC を Opengate 下に置くことを許可しているため、多数の利用がある。

利用時間の累計を図 4 に示す。化学系学科、附属図書館、情報系学科の順に利用時間累計が多い。化学系学科が接続時間が長いのは、学生個人の PC が常時接続された形態が多く、夜間などに長時間の連続接続が多いためと予想される。

表 2: Opengate の利用状況 (2003 年 9 月 20 日 18 時から 10 月 23 日 13 時)。利用数はのべ数。

gateway	利用数	設置場所
opengate00	7046	附属図書館
opengate-med	14	医学分館
opengate01	264	文化教育学部
opengate02	386	就職相談室を含む
opengate03	27	
opengate04	231	教養教育機構を含む
opengate05	869	経済学部、サークル棟
opengate06	10	理工学部
opengate07	362	
opengate08	0	改修
opengate09	253	国際交流会館を含む
opengate10	1	
opengate11	0	
opengate12	1618	
opengate13	45	
opengate14	3575	
opengate15	41	農学部、宿泊施設を含む
opengate16	10	
opengate17	297	大学会館
opengate18	295	科学技術協同開発センター
opengatelib2	44	学術情報処理センター内

Opengate は認証サーバを複数指定することができる。そこで、学生及び教職員などの通常の利用者の他に、一時利用者が Opengate だけを利用することができるゲストアカウントと専用認証サーバを用意している。ゲストアカウントは常時用意されており、利用希望者は、身分証などを提示し、申込書に署名するだけで利用できる。このアカウントは、附属図書館を利用する学外者、研究会や短期訪問などで佐賀大学を訪れる研究者などが利用している。

5 ウィルス対策など

前述のように、Opengate を介してインターネットへ接続する多数の利用者がおり、多くの個人の移動端末が接続されている。また、適切な管理が行われていない端末も接続されている。そのため、ウィルスを持っている端末や、大量のファイルダウンロードなどの不適切な利用が行われる端末もある。それらへの対策状況を報告する。

MSBlaster は 2003 年 8 月上旬に発見されたワーム型ウィルスであり、135 番ポートを使ってコピーを配

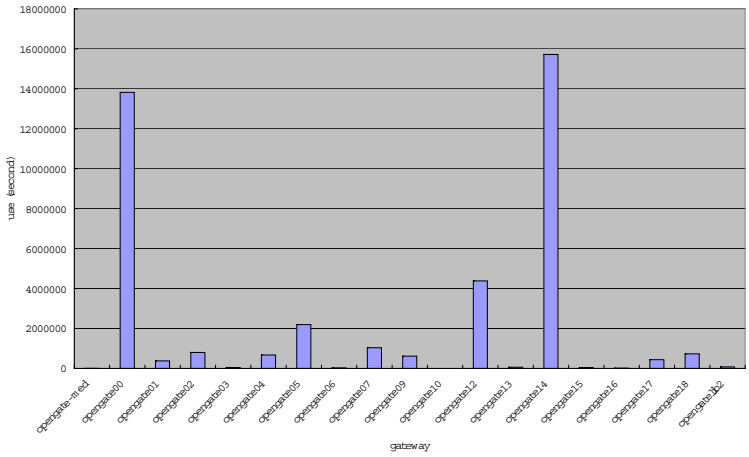

図 4: Opengate の累計利用時間 (2003 年 9 月 20 日 18 時から 10 月 23 日 13 時)。

布する [10]。通常は、ファイアウォールなどを通じて 135 番ポートの通信が行われない設定を行えば侵入を防げるはずである。しかし、自宅で感染したものを学内に持ち込まれるという形で、8 月下旬から感染が広がった。学生たちが夏休みを終えて戻ると Opengate の下でも MSBlaster 及びその亜種が活動する状況となった。

MSBlaster は毎秒、数 10 箇所へ接続を試みる。また、その亜種の中には接続の前に ping を試みるものもある。Opengate は NAT を利用しているため、MSBlaster が接続を試みるたびに NAT の変換テーブルを消費する。Opengate を稼働しているマシン (Pentium III 1GHz, 512MB メモリ) の場合、一クライアントが MSBlaster を保有している場合、CPU の約 20%が NAT プロセスに使われてしまい、10 クライアントが MSBlaster を保有していれば、Opengate が機能不全となることが判明した。

そこで、135 番ポートアクセスを Opengate のファイアウォールのログから検索し、発見次第、利用者に直接、あるいはその所属に対して対策依頼を行った。また、MSBlaster を持つクライアント数が多い場合には、一時的に ping を拒否する設定を行ってシステム停止を防いだ。利用者によっては、学術情報処理センターへ直接機器を持ち込んでもらい、センター職員が対策を行った。現在は、ほぼ収束した状況である。

また、139 番ポートや 445 番ポートなどを通じて感染するワームの活動も検出し、対策を行っている。

P2P 型のファイル共有ソフトウェアは、著作権侵害などの問題を引き起こすとともに、ネットワーク帯域を占有することがある。主要な P2P 型ソフトウェアが使用するポートをファイアウォールで閉じても、ランダムに相手先のポートをスキャンするものや、プロキシサービスを利用するものなどが利用される場合がある。

これらのソフトウェアの特徴としては、接続先をランダムにスキャンする場合も、プロキシサービスを利用して相手先を固定している場合でも、長時間にわたって自分のポート番号を一つずつ増やしながら通信するという特徴を持っている。そのような特徴のあるファイアウォールログから、該当者への注意を行っている。

6 まとめと議論

Opengate は、利用者が自らの端末を特別な手続きなしに接続することができる仕組みとして、佐賀大学で定着している。学生が利用するだけでなく、教員が

学内を移動して、講義や会議の際にネットワーク上の資源を利用しながら講義や議論ができる基盤として有効性を発揮している。本節では、サービス内容と管理手法の発展方向について議論する。

一つは、IPv6 への対応である。IPv6 は次世代のインターネットプロトコルとして注目され、SINET での運用も開始されている。通常利用される多くの OS も IPv6 に対応している。通常は、IPv4 とのデュアルスタックで実装されている。Opengate を IPv6 化するためには、デュアルスタックに対応して、IPv4 と IPv6 のファイアウォール操作を同時に行うことが望ましい。

IPv6 サービスを行うことは、クライアントに IPv6 グローバルアドレスを割り当てることと等価である。各クライアントが自らセキュリティー対策を講じられない現状では、IPv6 への移行にはセキュリティーなど解決すべき他の課題がある。

現在の Opengate では、利用者ごとに異なるファイアウォール規則を適応することを行っていない。学生、教職員、学外者に応じたファイアウォール規則は必要になる可能性は大きい。佐賀大学では、認証の統合化を行っている [9]。現在の認証サーバもこの統合認証システムを利用しているが、更にこのシステムから提供される身分情報を利用して、サービス内容を決定することも可能であろう。

前述のように、各 Opengate の個別設定は、データベース化されている。これらの情報は、各 Opengate を再起動する際に反映することができる。しかし、サービス中にファイアウォール規則を変更するなどの操作は、各 Opengate にログインすることで行っている。また、現在のファイアウォール規則や arp テーブルの状況を知るにも各 Opengate にログインしなくてはならない。こうした運用手法の改善が必要である。

利用者の持ち込む端末は、OS へのセキュリティーパッチが適切に適応されていないものや、ウィルス対策ソフトウェアを持たないものなどが多く含まれている。MSBlaster のような型のウィルスの場合、ファイアウォールに活動記録が残るが、もっとも一般的なウィルス付きメールを送るタイプのものはファイアウォールでは活動状況は分からない。Opengate を通過する SMTP パケットをウィルスフィルタなどを通すなどの処理を行う必要もある。

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 **2** 77–81 (1998).

[2] 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, 情報処理学会研究会報告 99-DSM-14 131–136 (1999).

[3] 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 **40**(12) 4353–4361 (1999).

[4] 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 **42**(1) 79–88 (2001).

[5] 西村浩二、秋成秀紀、野村嘉洋、相原玲二: 遠隔機器制御プロトコルを用いた有線/無線 LAN 用情報コンセントシステム, 情報処理学会論文誌 **43**(2) 662–670 (2002).

[6] 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の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 **42**(12) 2802–2809 (2001).

[7] `http://www.cc.saga-u.ac.jp/opengate`

[8] 只木進一、江藤博文、渡辺健次、渡辺義明: 公開端末及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 **5** 15–20 (2001).

[9] 江藤博文、渡辺健次、只木進一、渡辺義明: 大学における情報基盤の中核となる統合認証システム, 情報処理学会シンポジウムシリーズ **2003**(6) 43–48 (2003).

[10] MSBlaster の情報については、例えば以下を参照: `http://www.symantec.co.jp/region/jp/sarcj/data/w/w32.blaster.worm.html`