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

An Authentication System for Public and Mobile Terminals and Its Operation with Diskless Boot Mechanism

只木進一、江藤博文
Shin-ichi TADAKI, Hirofumi ETO
佐賀大学学術情報処理センター
Computer and Network Center, Saga University
840-8502 佐賀市本庄町 1
1 Honjo, Saga 840-8502
tadaki@cc.saga-u.ac.jp, etoh@cc.saga-u.ac.jp

渡辺健次、渡辺義明
Kenzi WATANABE, Yoshiaki WATANABE
佐賀大学理工学部知能情報システム学科
Department of Information Science, Saga University
840-8502 佐賀市本庄町 1
1 Honjo, Saga 840-8502
watanabe@is.saga-u.ac.jp, watanaby@is.saga-u.ac.jp

我々は、公開端末及び有線・無線を介した利用者移動端末に対応した認証システム Opengate を開発している。Opengate は、利用者の最初の WWW 要求を契機に認証画面を WWW ブラウザへ表示し、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り、利用者登録以外の登録作業及び端末の設定を必要としないことを大きな特徴とする。利用者が移動端末を携帯して全学を移動することを考え、本システムを全学規模で運用するためには、多数のシステムを運用しなければならない。そのコスト削減のため、ディスクレスマシンでの運用を提案する。ディスクレスマシンでの運用によって、設定から運用までのコストを大幅に削減できるとともに、保守及びログ収集なども容易に行えるようになる。

キーワード：ネットワーク認証、ファイアウォール、Java、ディスクレスブート

We are developing an authentication system, *Opengate*, for public terminals, wired and wireless mobile terminals carried by users. At the first WWW request by user, Opengate shows an authentication form to the WWW browser and controls a firewall system. The important feature of the system is that the system does not require any setting on user's terminals and any registrations except usual user registrations. Many systems should be operated over whole campus, because users use the network with their mobile terminals. To reduce the cost for operation, we suggest an operation method with diskless boot mechanism. By the diskless operation method, we can reduce the cost for introducing and operating the system. It also simplifies the procedure for maintaining the system and collecting user logs.

KEYWORDS : Network Authentication, Firewall, Java, Diskless Boot

1　序論

コンピュータを利用した情報処理やインターネットを介した情報取得及び情報交換は、分野を問わず、大学における研究教育の上で不可欠な技術となりつつある。そのための情報処理リテラシ教育は、ほぼ全ての学生の必須科目となりつつある。専門教育にあっても様々な形でコンピュータとネットワークを利用するようになりつつある。

このような状況に対応して、情報処理教育のための演習用端末の充実も進んでいる。学習活動の様々な側面でコンピュータとネットワークが利用され、特に自習でも利用されるようになることを考えると、十分数の端末を演習室という形で準備することは現実的ではない。利用者の持ち込む有線及び無線の移動端末も視野に入れ、大学のネットワーク基盤の整備を検討するべきである。

大学のネットワークは、大学における研究教育を支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有するものである。従って、自由に利用できることを目的として設置される公開端末や利用者の移動端末を接続する情報コンセントにおいても、利用資格を有する者のみが利用できる仕組みが必要である。

インターネットは社会における様々な面での情報流通の基盤となりつつある。そのような状況下で、無制限なインターネット利用を放置することは、ネットワーク設置者には許されない。更に、他サイトへの攻撃、不適切な内容のメール送信や WWW への書き込みなど、不適切なネットワーク利用が行われた場合には、利用者を特定する必要もある [1]。

大学の構成員にネットワーク利用を制限する方法の一つは、全ての端末で認証を行うことである。しかし、パーソナルコンピュータで確実に認証を行うことは一般に困難である。また、利用者の移動端末が持ち込まれる場合には、そのような認証は機能しない。従って、機器そのものに付随する認証機構によって、インターネット利用を制限するのは現実的ではない。

我々は、情報機器の認証機構ではなく、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 Opengate を開発した [2, 3, 4]。本システムは、公開端末、及び有線・無線の利用者の移動端末への対応を考え、情報機器の利用のための認証ではなく、ネットワーク利用の認証を全学共通の環境として提供することを目的としている。

このようなシステムを運用する場合に、公開端末の設置者や移動端末の利用者に特殊なソフトウェアのインストールや機器の事前登録などの準備作業を要求しないことが望ましい。公開端末の数の増加や移動端末の利用の一般化によって、機器の事前登録やソフトウェアインストール作業への対応そのものが、認証システム運用者への大きな負担となってしまうからである。

また、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など、大学の構成員以外のネットワーク利用への柔軟な対応も求められている。これらの学外利用者を学内利用者と同様に利用者登録を行ったり、専用の認証なし端末や情報コンセントを設置することは、ネットワークセキュリティー保護と利用者管理コスト低減という認証システム導入の趣旨と相反することとなる。

本稿では、これらの問題を解決できる認証システム Opengate を提案するとともに、ディスクレスシステムとすることで、複数の認証システムを若干の多様性を許容しつつ、ほぼ同一環境で運用する手法について議論する。

2　システムの基本構造

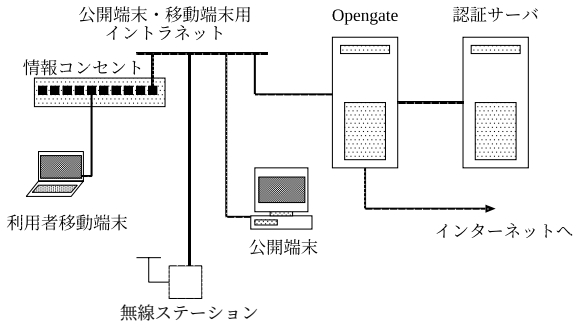

図 1: Opengate の設置場所

本システム Opengate は、公開端末や利用者持ち込みの移動端末が、ネットワークを利用する際に認証を行うシステムである。従って、本システムは、インターネットと公開端末や移動端末を接続する情報コンセント群用イントラネットとの間に設置するゲートウェイ

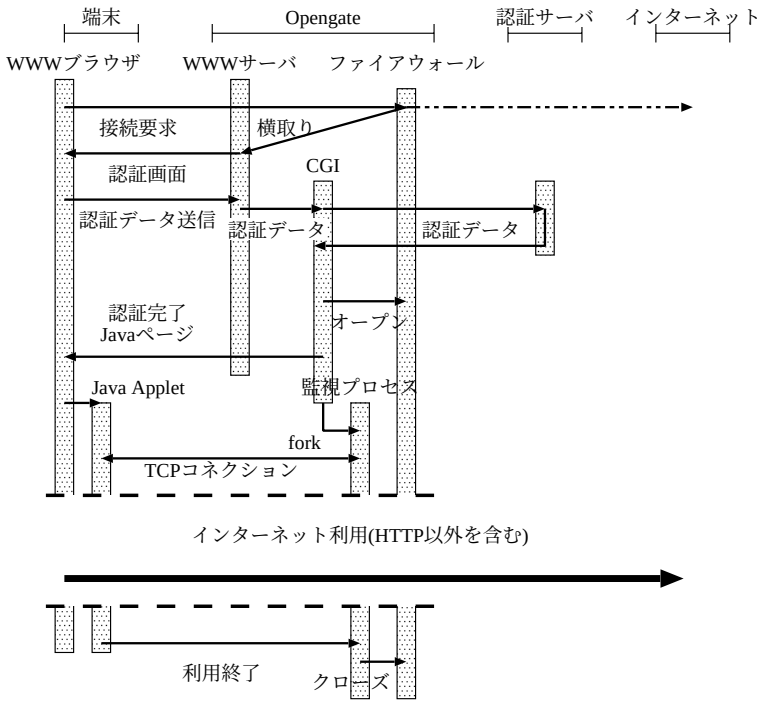

図 2: Opengate の動作

である (図 1)。

システムの流れを図 2 に示す [2, 3]。利用者が WWW ブラウザを起動しインターネット上の URL へ最初に接続しようとすると、Opengate がその要求を横取りし、認証画面を利用者のブラウザへ表示する。利用者から送られたユーザ名とパスワードを使って認証サーバへの問い合わせが行われる。認証に成功した場合には、当該端末に関するパケットの透過がファイアウォールに登録される。同時にシステムは、利用者ブラウザに Java Applet を起動し、Opengate との間に TCP コネクションを張り利用状況を監視する。利用者が WWW ブラウザを終了するか Opengate が起動した Java Applet を終了することで、利用終了が認識され、ファイアウォールから当該端末に関するパケット透過の規則が削除される。ファイアウォールへの登録及び削除の記録が認証記録とともにログとして残される。

認証サーバへの問い合わせは、POP や FTP など複数の標準のプロトコルに対応している。そのため、認証サーバは利用者が通常登録されているシステムを利用することが可能であり、特別な利用者登録を必要としない。

利用者が電子メールや TELNET などの WWW 以外のサービスを受ける場合には、一旦 WWW ブラウザを介して認証を受け、WWW ブラウザを起動したままで、これらのネットワークサービスを利用する形を基本としている。もちろん、Opengate では、特定電子メールサーバへの要求の透過を認証なしで認めるなどの柔軟な対応が可能である。

上述のように、本システムは、WWW 利用開始と終了を契機にファイアウォール規則を動的に登録・削除することで動作するゲートウェイシステムである。従って、Opengate システムは、ファイウォール機能及び WWW サーバから構成されている。運用システムにおいては、利用者端末群のネットワークへの外部からのアクセスを制限するための NAT や移動端末群に IP アドレスを配布するための DHCP が併存する。現在、Opengate は FreeBSD4.2 で上で、ipfw をファイアウォール開閉に利用し、apache1.3 を WWW サーバとして実装している。

Opengate は、利用者が最初に行う WWW 要求を契機に認証を行うシステムである。従って、端末に WWW ブラウザ以外の特殊なソフトウェアのインストールや

設定などを行う必要が無く、多様なプラットフォームを利用する多様な利用者に対応することができる。また、利用者が特定の認証サイトに一旦アクセスするのではなく、最初の WWW 要求を横取りするため、確実に、かつ WWW という容易な GUI を介した認証が可能である。

端末の利用状況監視は、端末に起動した Java Applet との通信によって行う。従って、固定的に設置されている公開端末だけでなく、有線及び無線の利用者移動端末に対応することができる。さらに、端末群を接続するスイッチなどのネットワークハードウェアにも依存しない。更に、一般的な利用者の登録以外の事前登録が不要である。

3 運用状況と問題点

Opengate は、2000 年から試験運用を開始している。

1. 佐賀大学学術情報処理センター内の情報コンセント及び無線ステーション用の認証として利用している。利用数は少数であるが、約 1 年以上の運用実績を有する。

2. 佐賀大学文化教育学部情報処理演習室には約 40 台の Windows 端末が設置され、それらの認証として Opengate が利用されている。Opengate が動作する機器は上記 1 と共用している。当該演習室は、講義及び自習に利用され、認証機能は約 1 年間の運用実績を有する。

3. 佐賀大学附属図書館では、windows 端末が約 40 台、WWW 専用端末が約 20 台、情報コンセント及び無線ステーションが設置され、それらの認証として Opengate が利用され、約半年の運用実績を有する。

更に、佐賀大学学術情報処理センターでは、全学の教室へのネットワーク環境の整備を行い、各教室から Opengate を介してインターネットが利用できる準備を行っている。

公開端末及び利用者の移動端末の認証システムを設置する場合、全学で共通の認証環境の提供が求められる。特に、利用者が、共通科目の講義室、専門科目の講義室、附属図書館、会議室、及びロビーなどの開放空間を移動しながら移動端末を利用することを考えた場合、全学共通の認証環境は必須である。

しかし、全学に対して単一の認証サーバの設置は困難である。公開端末の設置は既に開始されており、プリンタの有無や IP アドレスの設定されているネットワーク機器など、公開端末や移動端末の利用できる環境は一様ではない。更に、障害やクラッキングが起こった場合、場所を特定するとともに被害を最小限に押えるために、あまり大規模な端末用イントラネットを構成することは好ましくない。従って、相当数の認証ゲートウェイの設置が必要となる。

更に、附属図書館には大学構成員以外の市民利用者が存在し、学内の各部局にも定常的なゲスト利用者が存在するであろう。また、学会や研究会などで来訪する学外者も存在する。これらの学外者にも、ネットワークの利用を期間を限定して提供することへの要請も強い。Opengate では、複数の認証サーバを指定することが可能であり、学内利用者用の認証サーバとは別の専用認証サーバを設定することで、上記のような学外利用者へのサービスに対応できる。これらの利用者を附属図書館内のみや、学会や研究会の会場のみでネットワークを利用可能とする柔軟な設定に対応するためにも、建物単位などでの Opengate の設置が必要である。

本システム Opengate は、WWW 要求を契機としてファイアウォールの制御を行うシステムである。また、それは FreeBSD という汎用 UNIX システム上に構築される。汎用 UNIX 上のシステムであるため、中心となる Opengate システムと他の WWW サーバ、認証システムなどを組み合わせて構成することが可能である。

一方、本システムが汎用 UNIX 上のシステムであるため、カーネルの再構成、ファイアウォール規則の記述、更に WWW サーバや DHCP サーバの記述など、設定項目を多く有している。そのため、学内に多数の Opengate システムを提供し、かつある程度バラツキのある設定を行うのは容易ではない。また、セキュリティー管理のためのログの収集及び解析も管理者の大きな負担となる。

これらの問題を解決するために、Opengate システムを少数のブートサーバから起動するディスクレスブートシステムとし、単一のログサーバへログを収集・解析する運用形態を提案する。

4 ディスクレスブートシステム

本システムを実装している FreeBSD では、NIC が有する PXEBOOT(Preboot Execution Environment Boot) という仕組みを利用したディスクレスでのシステム起動の方法がある[1]。FreeBSD システムをディスクレスで起動する場合の基本的流れを図 3 に示す。システムや NIC の BIOS などにネットワークからの起動を指定すると、システムは DHCP サーバなどから起動の情報を得る。その起動情報を基に、システムは TFTP を使って起動用プログラム `pxeboot` を得たのち、NFS を通じて kernel を取得し起動する。kernel の起動後、ルートパーティション等を NFS マウントしてシステム起動を継続する [5]。

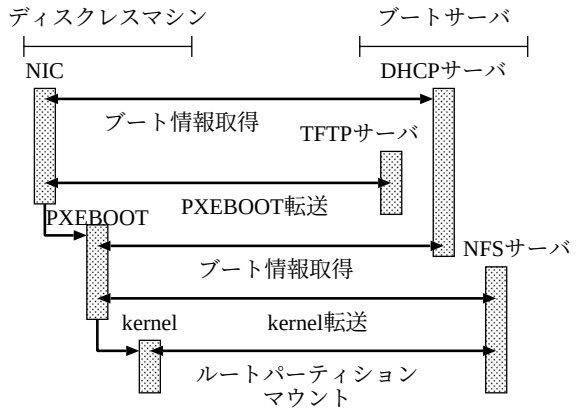

図 3: ディスクレスブートの基本的流れ

ディスクレスで Opengate システムを起動する場合、次のような点での検討が必要となる。第一は、Opengate システムが、ファイアウォールや NAT など、ネットワーク機能の制限を加えるシステムであることである。第二は、ファイアウォール規則を含め、一台ごとに異なる設定が必要な点である。

ファイアウォールや NAT を有するシステムをディスクレスで起動するのは一般に困難である。ファイアウォールシステムは、通常は、kernel の一部として実装される。また、システム自身との外部を含めて全ての通信を拒否した設定をデフォルトとして、許可する設定を追加する場合が多い。

[1]PXEBOOT を利用したディスクレスブートは、Linux などの他の PC-UNIX 及び Windows でも可能である。ただし、手順は OS によって異なる。

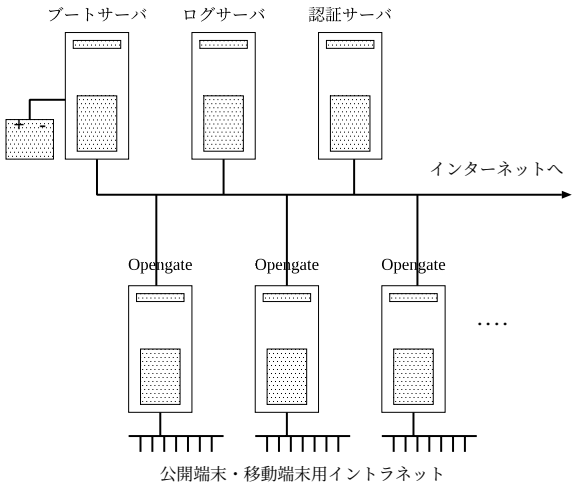

図 4: ディスクレス Opengate の設置概念図

システムをディスクレスでネットワークから起動しようとすると、前述のように kernel 及びシステムに必要なファイルシステムを NFS を介して取得する。従って、Opengate を通常の形態でディスクレス起動を行うと、kernel のファイアウォールが起動した段階で外部との接続が不可能となり、起動することができない。そこで、ファイアウォールシステムを全ての通信を許可した状態を基本として拒否する規則をその上から設定する方式で構築することで、kernel 起動直後にネットワークを閉鎖するのを防ぐ。

NAT はデーモンプロセスを kernel と別に起動するものの、パケットを NAT デーモンへ転送するのは kernel 内のファイアウォール機能である。標準の FreeBSD 起動では、ファイアウォール機能が先に設定され、遅れて NAT デーモンが起動される。ディスクレスブートの場合には、ファイアウォールに NAT への転送が設定された途端にパケットが NAT デーモンへ転送されるが、この段階では NAT デーモンは起動しておらず、システムが停止する。これを避けるために、ファイアウォールへの NAT 転送設定は、NAT デーモン起動後のシステム起動最終段階で行うことにする。

マシンごとに異なる設定については、FreeBSD の場合、次のような方式を採用することができる。FreeBSD のディスクレスブートの場合、`/etc/rc.diskless1` によって、ルートパーティションの内容がメモリ上に置かれる。その際に、`/conf/IP` アドレス`/etc` の内容が `/etc` に上書きされる。従って、マシンごとに異なる起

動情報、WWW サーバや DHCP サーバの情報を/etc に集約するような設定を行えば、マシンごとに異なる設定で起動することができる。

ディスクレスブートの場合、ルートパーティションはメモリ上に置かれるため、ログはシステムダウンによって全て失われてしまう。そこで、syslog 及び logger の機能を使って、ログサーバへ集約する。

5 まとめと議論

我々は、公開端末、有線及び無線の利用者持ち込み移動端末に対応したネットワーク利用認証システム Opengate の開発を行っている。Opengate は、最初の WWW 要求のパケット通過を契機として、利用者の WWW ブラウザに認証画面を送信し、それに応じてファイアウォールを制御するシステムである。

Opengate は、共通科目及び専門科目の講義室から、附属図書館、会議室、ロビーなどの公開空間まで、学内に共通的認証環境を提供することを目的としている。そのため、設定環境に対する若干の多様性を許した形で多数のシステムを運用することが必要となる。

多数の Opengate を運用するために、ディスクレスでの起動とログの集約のための方法を提案した。ファイアウォール設定手順の変更及び設定ファイルの/etc ディレクトリの集中で、ディスクレスでシステムを起動することができる (図 4)。これにより、システム設定コスト及び管理コストの低減が可能となり、若干の多様性を許容して、多数の Opengate を全学共通の認証環境として提供することが可能となる。

更に、個々の Opengate がディスクを持たないために、停電時の停止作業などの電源管理作業が不要となる。また、BIOS が持つ電源復旧時の自動起動の機能を使って、迅速にシステムの再起動を行うことが可能となる。また、個々の Opengate のハードウェア障害時には、ブートサーバの DHCP 設定を変更することで、容易に代替機を導入することができる。

一方で、ディスクレスでの起動を行うために、認証機構の中枢が少数台のブートサーバに集中する。従って、それに対応した別の障害対策を講じる必要がある。ブートサーバの多重化が必要である。また、ディスクレスマシンの電源投入時の自動起動に対応するため、サーバは常時稼働していることが求められる。それに対しては、十分長時間の耐久性を有する無停電電源などをブートサーバに設置するなどの対策が必要である。これらの障害対策は、個々の Opengate に対する対策よりも小さな負担とすることが可能である。

ディスクレスでのシステム起動のために、ディスクレス Opengate とそのブートサーバ間のネットワークが安定していることが運用には不可欠である。更に、TFTP と NFS というファイル転送プロトコルを利用しているため、サーバへのアクセス制限などの安全性確保にも注意が必要である。外部からのアクセスを制限した専用ネットワーク上での運用などの対策が必要である。

参考文献

[1] JPCERT/CC「技術メモ – コンピュータセキュリティーインシデントへの対応」 JPCERT-ED-20000-0007 (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」信学技報, Vol. **99**, No. 591, 43 (2000).

[3] 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, Vol. **42**, No. 12 (2001), 印刷中.

[4] 渡辺義明 他 「Opengate ホームページ」
http://www.cc.saga-u.ac.jp/opengate

[5] 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、2001).