サイエンティフィック・システム研究会　　2006 年 1 月 18 日
システム技術分科会 2005 年度第 2 回会合資料

利用者用ネットワークと統合認証

佐賀大学学術情報処理センター
只木進一
tadaki@cc.saga-u.ac.jp

教員は自分の研究室だけではなく、講義室でもネットワークを使いたい。学生も自分のノート型 PC を携行し、大学でもネットワークを使いたい。ネットワークの普及は、教育と研究、さらに組織運営などのためにオンライン情報へ常にアクセスしたいという要求を生み出した。それに応える利用者用ネットワークが求められている。認証と記録が行える利用者用ネットワークシステムである Opengate についてその概要を紹介する。また Opengate を全学的に展開するための基盤が、全構成員の情報を統括する統合認証である。組織の情報システムの合理化の要点として共通情報の統合が重要とされている。統合認証システムは、その核となるものである。

キーワード: 無線 LAN、情報コンセント、認証、利用記録、オープンシステム

1　序論 : 新しいタイプの情報基盤の必要性

情報処理技術は、今や日常的な技術となった。今日の大学において、コンピュータとネットワークからなる情報基盤は、教育と研究だけでなく、大学運営のまさに基盤となっている。その結果、例えば、教員は講義にノート型パーソナルコンピュータ (PC) を持っていき、講義でもインターネットを使いたいと考える。あるいは、会議資料もインターネットに置き、会議中にそれを見せたいと考える。もちろん、学生も自分の PC を講義中や、図書館でネットワークに繋ぎ、資料収集や就職活動に使いたいと考える。

一般社会でも同様な状況がある。ホテルでインターネットサービスを行うところは珍しくなくなった。客室で有線のインターネットサービスを行ったり、ロビーで無線のインターネットサービスが行われている。また、空港や駅、喫茶店でもインターネットサービスが受けられる。つまり外出先でも、自分のノート型 PC を接続したいと考える人が増えている。大学でも、来学者にインターネット接続サービスをしたいと考えている。

上記のようなサービスは、従来から組織内でサービスされてきたネットワークとは質的に異なるものである。通常の組織内ネットワークは、部局や建物に対応するようにサブネットに分割され、各情報機器に固定の IP アドレスが割り当てられている。これにより、端末とその利用者の対応付けを行い、障害時に迅速に対応できる体制となっている。

これを可能にするために、新しい機器を接続するたびに申込手続きなどが必要とされている。一方で、使わなくなった機器の削除手続きが行われにくく、IP アドレスが不足したり、不正に IP アドレスが使われる危険性がある。

このような従来型のネットワークでは、ノート型 PC を持って、他の建物や部署に移動してネットワークを使うことが通常は困難である。また、来訪者や接続権限の無い人を、一時的に接続させる手順が無い場合が多い。その結果、適切な手続き無しで接続資格の無い機器を接続させてしまう危険性も発生する。

以上から、ノート型 PC など移動できる端末に対応でき、また来訪者なども利用できる端末専用の利用者用ネットワークが必要となる [1]。このようなネットワークに対応するための技術的研究は、1990 年代末から行われ、様々なタイプのものが提案されてきた [2–6]。特に近年では、学生がノート PC を携行することを前提とした教育基盤として、利用者用ネットワークの運用技術に関する研究が行われている。

2　利用者用ネットワークの要件

利用者が携行するノート型パーソナルコンピュータに対応できるネットワークには、どのような機能が必要であろうか。もちろん、そのようなネットワークが無法地帯でないために、認証と利用記録が適切に行われるネットワークの場合である。

第一に必要なことは、利用者にとって負荷のないものであることである。有線または無線のネットワークアダプタがあれば、特別な周辺機器や特別なソフトウェアなしで、そのネットワークを利用できなければならない。また、認証のために普段使わないような操作を行わなくてよいことが望ましい。

第二に、大学のように構成人数が多く、かつ毎年大量の移動がある組織の場合、そのネットワークを利用するための特別な利用登録を行う必要がないものでなければ、実際的な運用は困難である。また、来訪者も比較的単純な利用申込で利用できることが望ましい。

第三に、管理者にとって構築と運用が容易であることが必要である。特殊なネットワーク機器を必要とするものでは、大規模に展開することは不可能である。また、設置や運用の手間が小さいことも必要である。

利用者用ネットワークに限らず、情報システムが特定のハードウェアや OS に依存していることは好ましくない。多数の利用者が関与する場合や規模が大きい場合には尚更である。利用者用ネットワークの場合、利用者が使っている PC のハードウェアや OS には多様性があるのが当然である。また、大規模にネットワークを運用する場合には、ネットワーク機器を部分的に更新する必要もある。つまり、利用者ネットワークの大規模運用は、オープンスタンダードがどこまで通用するかの実験場という側面がある。

3　Opengate

前節で述べたような要件を満たす利用者用ネットワークシステムとして、筆者らは Opengate と呼ばれるシステムを開発し、2001 年から全学規模で安定に運用をしている [7,8]。このシステムは、佐賀大学の半数以上の構成員が利用したことがあり、学生が日常的にインターネットに接続するための必須の情報基盤となっている。また、研究会や集中講義などでの来学者の利用に供し、高い評価を得ている。

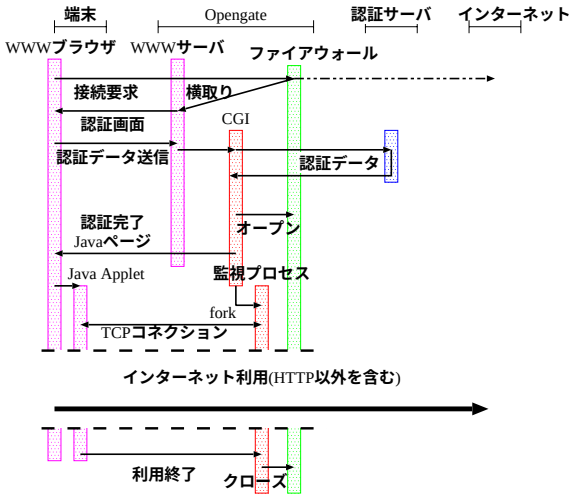

図 1: Opengate の処理の流れ

Opengate を利用するために利用者が用意するのは、有線または無線でネットワークに接続できるコンピュータ、適当な Web ブラウザ、そして JRE (Java Runtime Environment) である。処理の流れを図 1 に示す。コンピュータを起動し、Web ブラウザで適当な URL へ接続しようとすると、認証ページが表れる。認証が成功すると利用開始が記録され、Firewall が開く。また、ブラウザには applet がダウンロードされ、TCP コネクションが張られる。認証後は他のネットワークポートを利用することもできる。Web ブラウザが止まる、あるいは端末が停止し、applet が停止すると利用終了が検知され、Firewall が閉じられる。

上述のように、Opengate の大きな特徴は、利用者に特殊な機器、特殊なソフトウェアを求めないことと、もっとも日常的に行われる Web へのアクセスを通じて認証を行うことである。当然、Web ブラウザを有し、JRE を有する多様な OS で利用することができる。

認証と Firewall 操作がひとつのゲートウェイに集約されているため、Opengate はスイッチや無線 LAN 局などの通信機器に特殊な機器を求めない。現在サービスされている Opengate は FreeBSD を用いているが、OS に依存している部分は Firewall 操作部だけである。

Opengate それ自体は認証サーバ機能を有していない。認証は、Opengate の設定ファイルにサーバとプロトコルを指定することで行われる。また、認証サーバは複数設定可能である。従って、組織全体にわたる既存の認証を活用することで、特別な利用申込を行わ

ないようにすることができる。また、ゲスト専用認証サーバを設定することで、組織内利用者と別の認証を常時準備しておくことも可能である。もちろん、組織内ユーザとゲストが同じ Opengate を利用し、かつ認証サーバを区別することができる。

Opengate による認証後、Web ブラウザには java applet がダウンロードされ、Opengate との間に TCP コネクションが確立される。このコネクションによって、Opengate は利用をモニタしている。Web ブラウザの停止やクライアントそのものの停止などで applet が停止すると、Opengate は利用停止を検知して、Firewall を閉鎖する。この迅速な Firewall 閉鎖も Opengate の大きな特徴であり、他のクライアントによる不正な Firewall 通過を阻止することができる。

4 Opengate の利用と運用

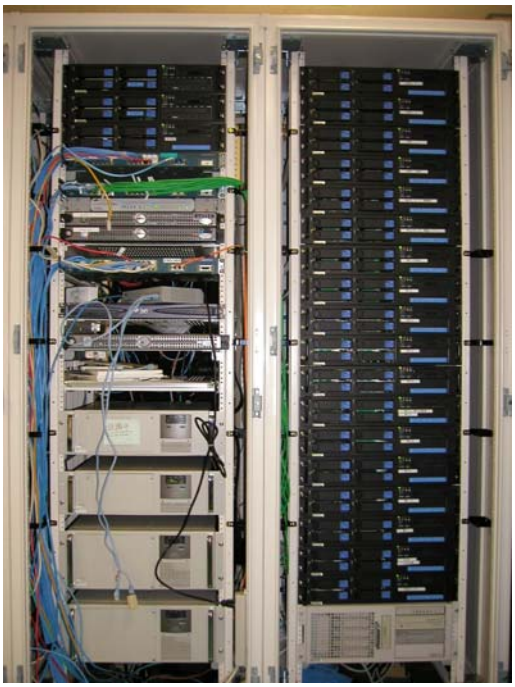

図 2: Opengate サーバ

Opengate は 100 台以上の端末を配下に置いた状況や DVTS などの大容量データ転送でも動作可能である実績がある。しかし、利用者が持ち込む移動型端末を接続するためのネットワークゲートウェイであるため、全学など大規模な利用者用ネットワークを一つの Opengate で運用することは好ましくない。ウィルスの活動や P2P による著作権侵害の恐れのある場合、迅速に当該端末を特定し対処しなければならないからである。そのため、佐賀大学では概ね建物ごとに Opengate を設置し、20 台程度の Opengate を運用している (図 2)。

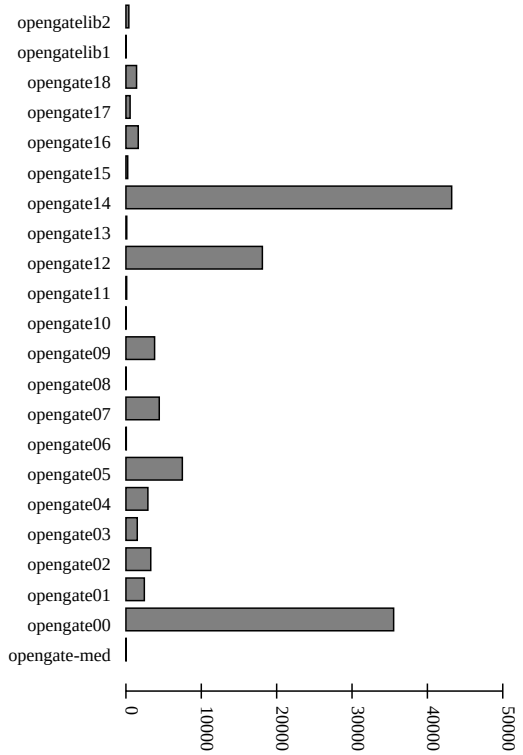

図 3: Opengate の利用状況 (2003/9/29 から 2004/6/8)

2003 年 9 月 29 日から 2004 年 6 月 8 日までの利用状況 (累積利用時間) を図 3 に示す。Opengate14 が最も利用時間が長い。ここは化学系学科の建物であり、学生が個人 PC を Opengate に接続している。夜間の長時間接続が多いようである。情報系学科は Opengate12 に接続している。学生にはノート型 PC の購入が義務付けられており、100 人規模のプログラミング演習など日常的に教育で利用されている。附属図書館は Opengate00 であり、固定の公開端末約 60 台が常時接続されている。また、ノート型 PC 用の情報コンセントが館内に多数用意されている。

各 Opengate は IP アドレスと若干のファイアウォール規則の違いを除くと同じ構成である。そのため、佐賀大学ではこれらをディスクレスにすることで運用し

ている [9]。起動サーバは各 Opengate ごとに異なる設定をデータベースとして保持している。設定はこのデータベースからほぼ自動的に生成される。このため、機器の障害時の迅速に代替機への移行や新規の導入が可能である。ネットワーク構成を図 4 に示す。

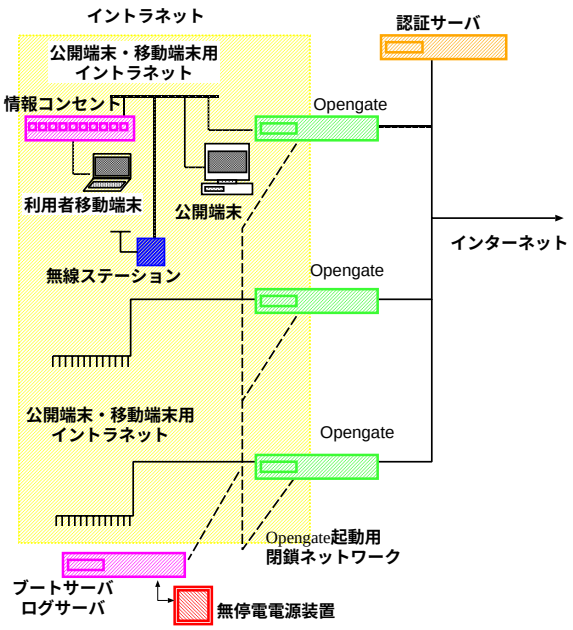

図 4: Opengate のネットワーク構成

利用者用ネットワークのゲートウェイとして開発された Opengate には、認証と記録を行うことの結果として検疫的効果がある。利用者用端末は一般に管理が十分でない場合が多く、ウィルスの活動の機会を与えるとともに、P2P などによる不適切な利用の危険性も多い。認証と記録により、ネットワークに負荷をかけている利用者とその居場所を迅速に特定し、ウィルス感染拡大や著作権侵害の事象に対応することができる。

大学の場合、就職情報収集などを目的として認証の無い端末が設置される場合がある。そのような端末がインターネットに接続する際には、Opengate を利用して利用者を学内者に限定できる。

こうした端末が起動のまま放置されるとキーボード打鍵を記録するソフトウェアが仕掛けられ、Opengate 利用時に使う利用者名とパスワードを不正に取得される恐れもある。こうした小規模端末群のために認証サーバを設置するのは、コスト面から困難な場合が多い。そこで、Windows のログオンを Opengate 認証で行うような仕組みの導入も可能である [10]。

5 統合認証

情報処理技術が様々な業務に浸透するに従って、日常業務の中で複数の情報システムに認証を通じて接続する必要が発生している。大学においても、端末の利用、メールの利用、シラバスや成績登録、物品購入などで認証のある情報システムに日常的に接続する。

これらの認証がばらばらに構築されていると、管理者と利用者の双方にとって不幸である。利用者は多数の利用者名とパスワードの組を持たされて忘れてしまうか、全てに共通のパスワードをつけたり、それらを端末周辺に紙の形で張り付ける。管理者はシステムごとの利用者情報管理を行うだけでなく、利用者側のセキュリティーホールの対応に追われてしまう。

大学だけでなく、行政や民間の組織においても、これまでの情報システムの構築は、各担当課などで行われ、それぞれの情報システムが独立して必要な情報を保持していた。そのため、組織全体としては同じ情報の登録作業を多重に行うとともに、相互の情報の不整合の調整に多大なコストを払っていた。

認証だけでなく、組織全体にわたる情報システムが利用する利用者情報を管理するシステムが統合認証である。佐賀大学では 2002 年に、学術情報処理センターと附属図書館の間で利用者情報の共有を開始し、全学的利用者情報管理システムとして拡張を行っている [11]。

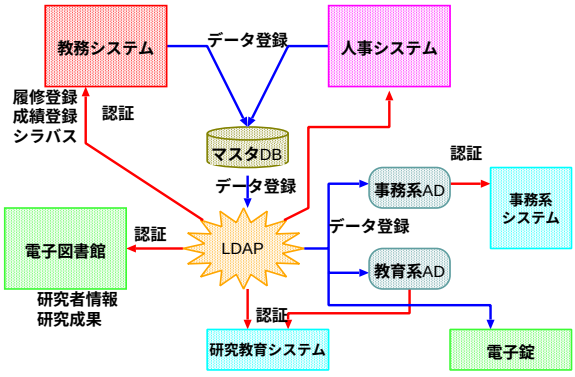

図 5: 統合認証システムの概要

統合認証システムは、全学的な利用者情報管理システムである。学内に設置される様々な共通的情報シス

テムへの利用者登録を一元管理するとともに、共通認証を提供することを目的としている。認証対象としては、教育・研究用システム及び事務情報システムの端末やコンピュータへのログイン時の認証だけでなく、各種 Web システムでの認証も含んでいる。また、図書館業務システムや教務システム、電子錠システムへの利用者情報提供も行う。

統合認証システムは、中心に全構成員のデータベースを有している。このデータベースは、全構成員の利用者 ID、氏名、所属など共通データから構成されている。ここから LDAP へのデータ登録が行われ、さらに AD へのデータが提供され、端末やアプリケーションでの認証に利用される。また、様々なプロトコルによる認証を行うためのサーバが設置され、Web システムからの認証などを可能としている。

統合認証システムが大学の全構成員の情報を有していることが Opengate の全学的展開に決定的な役割りを果たしている。Opengate それ自体は認証サーバ機能を持たず、外部に複数の認証サーバを設定できる。認証サーバへのアクセスプロトコルも多様に設定できる。つまり、Opengate は統合認証システム配下で全構成員の利用を可能としている。

統合認証システムが認証を提供するシステムは多肢にわたっており、その OS も多様である。また、認証を受けるシステムも更新時期がばらばらである。従って、統合認証システムもオープンシステムとして構築されなければならない。同時に、認証を受けるシステムもオープンスタンダードに対応できるものでなければならない。

6　まとめと議論

利用者がノート型パーソナルコンピュータを接続して利用できる利用者用ネットワークの必要性とそれを実現する Opengate について紹介した。利用者の立場からは、そのようなネットワークの利用手続きが簡単である必要がある。管理者の立場からは、少ないコストで適切に管理が行える必要がある。Opengate は両者の必要を満たすシステムである。

また、Opengate は既存のフリーウェアに立脚し、構造も単純であり、また特殊な機器を必要としない。そのため導入のコストが小さい。さらに、大規模運用のためのディスクレス化も可能である。Opengate の今後の展開としては、利用者の身分などに応じたファイアウォールルールの設定や、管理ソフトウェアの開発などがある。

Opengate を含めた利用者が持ち込む PC をインターネットに接続する仕組みによって、大学では学生個人の PC を前提とした教育に対応するネットワーク的基盤は整備されつつある。しかし、学生が保有する PC への支援体制や教育に活用できるソフトウェア環境の整備は十分ではない。ライセンス形態の検討だけでなく、オープンソフトウェアを活用できる教育内容の検討も必要である。

大学だけでなくほとんどの組織に持ち込まれるコンピュータのほとんどが端末として利用されている。従って組織外から接続される必要はない。しかし、ウィルスの侵入や P2P ソフトウェアによって、その端末の利用者に認識されずにサーバ機能が有効になっている場合がある。特に P2P ソフトウェアは、多くの利用者にとってはファイルを取得する手段であって、自分が提供する側にあることは理解されていない。その結果、著作権侵害や重要情報の流出などの問題が発生する。

Opengate が提供する利用者用ネットワークは、上記の問題への有効な解の一つではないだろうか。Opengate は認証を行うとともに、ネットワークの開閉の記録を行う。Firewall を使うことで、不適切なポートを閉じたりモニタすることも可能である。従って、端末の不適切な挙動を把握し、必要に応じて接続を禁止することが可能である。

Opengate を全学規模で展開することを可能にしているのが統合認証システムである。統合認証は、全学の全構成員に関するデータベースを核に、多様な認証サービス提供が可能である。このシステムの下で、全学共通の情報システムの構築が進行中である。

統合認証システムの運用では、データ登録体制の整備が大きな問題となる。大学のような組織の場合、人事、教務、教育研究の各部署の連携が必須である。大学の事務情報の統合の一環として統合認証を導入すべきである。

利用者用ネットワークと統合認証システムは、対象となる機器のハードウェア及びソフトウェアが多様であることを前提に設計されなければならない。多数の利用者、多数の機器が関係するだけでなく、個々の要素が順次更新されていくことが前提であるからである。

従ってオープンなシステム構成が必須の要件である。

参考文献

[1] 江藤博文、只木進一、渡辺健次、渡辺義明「新しい教育用情報基盤の実現へ向けて」、学術情報処理研究 No.6 (2002) 13.

[2] 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 No.2 (1998) 77.

[3] 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 (1999) 131.

[4] 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 アドレス義存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 (1999) 4553.

[5] 石橋勇人、山井成良、安部広多、阪元 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防止方式」、情報処理学会論文誌 Vol.**42** No.1 (2001) 79.

[6] 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 用コンセントシステム」、情報処理学会論文誌 Vol.**43** No.2 (2002) 662.

[7] 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) 2802.

[8] Opengate ホームページ `http://www.cc.saga-u.ac.jp/opengate/`.

[9] 只木進一、江藤博文、渡辺健次、渡辺義明「利用者移動端末に対応した大規模ネットワークの Opengate による構築と運用」、情報処理学会論文誌 Vol.**46** No.4 (2005) 922.

[10] 安田伸一、羽石寛志、渡辺健次、渡辺義明、江藤博文、只木進一「Opengate 認証の公開端末への適用」、学術情報処理研究 No.8 (2004) 9.

[11] 江藤博文、渡辺健次、只木進一、渡辺義明「全学的な共通情報アクセス環境のための統合認証システム」、情報処理学会研究報告 2002-DSM-27 (2002) 31.