大規模計算機センターのセキュリティ対策事例

安東 孝二　吉岡 顕　田中哲朗

東京大学情報基盤センター情報メディア教育研究部門

概要

東京大学は約3,500名の新入生の全員に情報処理教育を必修化し、その講義を情報基盤センターの教育用計算機システムを利用して行っている。また、約1,600台の同システムの端末はキャンパスの随所に配置されており、20,000名を大きく超える数のユーザーの情報基盤となっている。様々な制限が課せられる大学の教育用システムにおいてのシステム設計時から運用に至るまでのセキュリティ対策を具体的に紹介するとともに、今後の問題点に言及する。

Case study of secure & large scale campuswide computing system

Koji ANDO, Akira YOSHIOKA, Tetsuro TANAKA
Campuswide Computing Division,
Information Technology Center, Univ. of Tokyo

Abstract

In Univ・ of Tokyo, every year, more than 3,500 freshmen must take course for learning how to use computers and the Internet, making use of Educational Campuswide Computing System of Information Technology Center・ Our system is also actually the information infrastructure of more than 20,000 users, because we locate about 1,600 terminals here and there in the campus・ It is generally very difficult to design this kind of system because of its variety of requirements and its security issues・ I will show you the detail of our way against security issue from the time of design to management, and refer to the unresolved problem・

1　はじめに

東京大学では1994年度より情報処理教育が必修となった。そのため利用者層は学生のほぼ全員に広がり、今や電子メールとWWWは学生の情報基盤となっている。その利用頻度・利用時間は今もなお増加し続けている。ユーザーが増えるにつれ、セキュリティに関する問題はますます深刻さを増している。外部からのアタックを始め、SPAM、初心者をターゲットにしたTrojan、システムへの悪戯などさ様々なトラブルがも多く見られるようになった。

その一方で、従来UNIXベースでシステム運営を行って来た我々に対し、センター方式の管理には向かないと思われるMS Windowsおよびそれで動作するアプリケーションを利用したいというユーザーの声も大きくなってきていた。これらを状況を背景に、

1998年度に新システムの設計・構築を行い、1999年度に教育用計算機システム(Educational Campuswide Computing System)の運用を開始した。そのセキュリティを考慮した設計と運用におけるセキュリティ対策について述べる。

2　教育用計算機システムの概要

教育用計算機システム(以下ECCSと呼ぶ)は東京大学の本郷・駒場の両キャンパスをカバーする大規模システムである。登録ユーザーは約30,000名であり、端末数は約1,600を数える。駒場キャンパスではセンタービル2棟に900を超える端末が収容され、192名までの大人数での講義も可能な教室も2つ用意されている。一方、本郷キャンパスでは各学部・学科に数台から90台の規模で分散して配置した端末(分散端末と呼ぶ)が中心となっており、キャンパスに散在する30箇所を超える場所(分散サイトと呼ぶ)で稼動している。性格の異なる2つのキャンパスのシステムはATM専用線によりシームレスにつながり、全ての端末で完全に均質なサービスを提供することが可能になっている。(図1)

これだけ大規模なシステムではあるが、利用率も非常に高い。駒場キャンパスの教室の端末の利用率を示したのが図3である。5分毎に端末の利用の有無を調べ部屋ごとに利用されている端末の割合をグラフ化したものである。システムとしての規模だけでなくユーザーのアクティビティも非常に高いことがわかる。

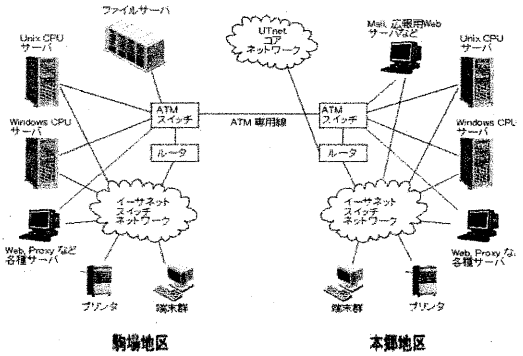

図1　システム全体イメージ

このようにECCSは、講義のための均質な環境を提供するとともに、学生の情報基盤システムとしての役割も担っている。計算機についての知識の少ない学生も多く利用することが予想されるため、簡便でかつ安全に使わせるための配慮も必要になる。

ECCSの基本クラスタは図2のような構成になっている。UNIXをベースとした構成をとっており、端末にはNC(ネットワークコンピュータ)を採用している。UNIXサーバー1台を最大40台のNCがブートサーバーとして利用する。WindowsサーバーはNCとは直接関係しておらず、どのNCからもすべてのWindowsサーバーが利用できる。

NCでは、独自のOSが稼動しており、Netscape Navigatorやメールクライアント、簡単なアプリケーションが動作する。EmailやWWWのために、各サーバーマシンを使う必要はない。UNIXサーバーはXプロトコルを通じて利用する。同じくWindowsサーバーもXプロトコルを通じて利用することができる。認証システムはすべてNISで統一しており、同じ認証情報でECCSのあらゆるリソースが利用可能である。

このように3種の環境(図4)を自由に利用できるため、Emailについては従来のpopによるソリューションは考えられない。そのため、imap4rev1をメッセージングプロトコルとして採用している。

その他にユーザーがリムーバーブルメディアを用いてファイルの入出力を行うための端末と、情報コンセントを用意している。

3　ECCSに求められるセキュリティレベル

大学の大規模システムにおいて、企業で求められるようなレベルのセキュリティを維持することは困難である。企業とはシステム運営に関する予算・人員もまったく異なる上に、ユーザーのレベル・アクティビティも異なる。しかしながら、教育機関のシステムとして守らなければならないセキュリティレベルも存在する。一般にセキュリティに関する運用コストを押さえるためには、システム設計の段階から目標を明確に設定し、初期投資と運用にかかるコストを評価しなければならない。しかし、特に国立大学においては制度上、運営費は非常に乏しいので初期投資で最低限のレベルをクリアしておくことが重要である。また、大学のシステムの場合、ユーザー数が多く、ま

た入退室管理も不十分な場合が多く、外部ネットワーク
クからのアクセスに対する対策よりも、ユーザーに対する
対策がメインになる点も企業とは大きく異なる。

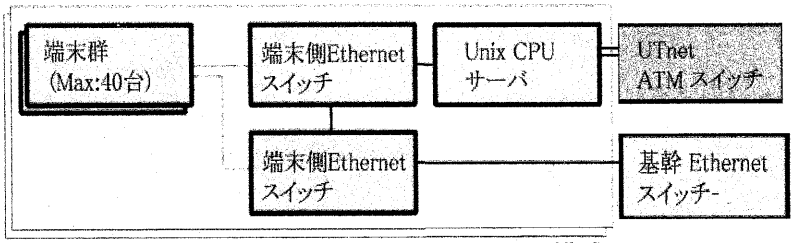

図2　システムクラスタ構成

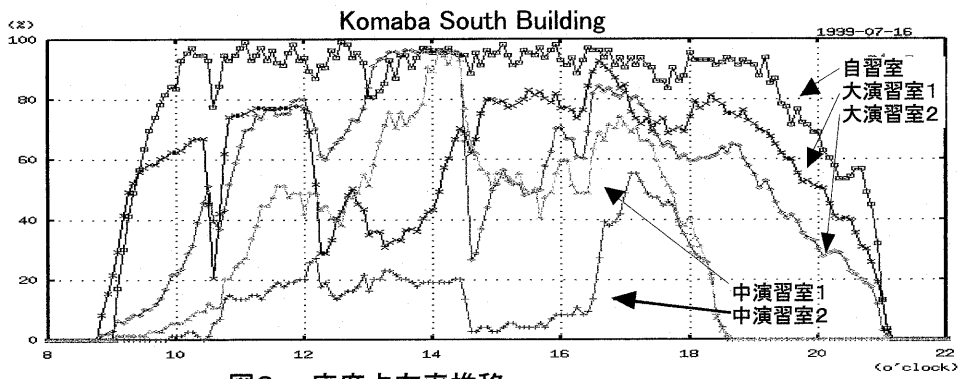

図3　座席占有率推移

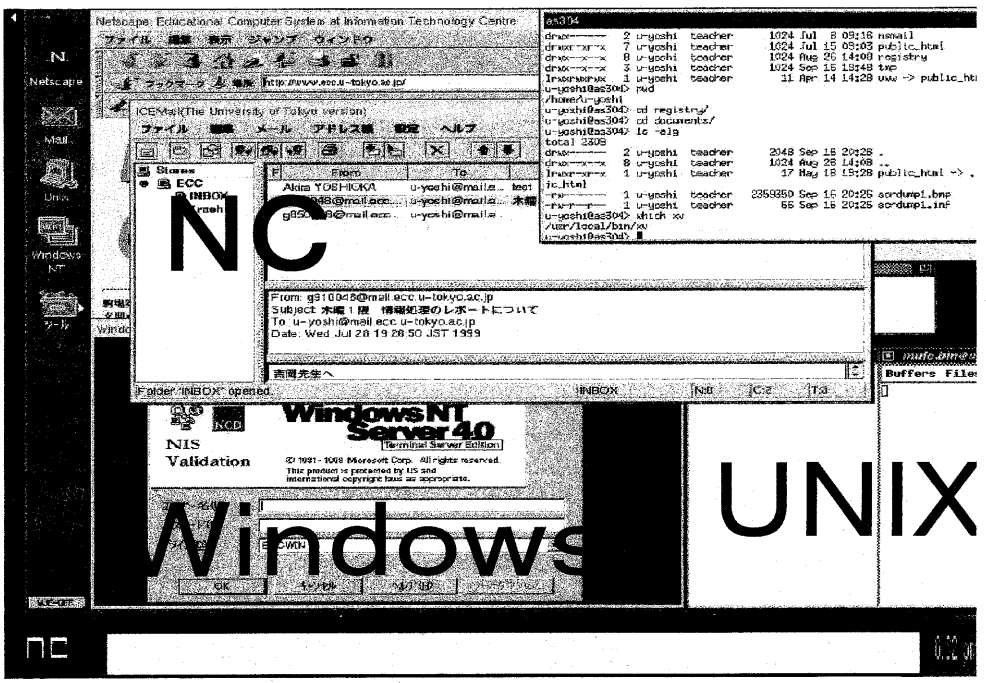

図4　3種類の環境を同時に利用した画面

4　過去のトラブルの事例

前システムでに見られたトラブルの事例を基に対策を行った。

4—1　ネットワークに関する事例

- ユーザーが端末のIPアドレスを勝手に変更し、ゲートウェイアドレスとduplicateさせたため、同じクラスタのすべての端末が使用不能となった。
- ユーザーが自分のノートPCを端末の代わりにつないだ。

ともにシステムに致命的な結果を招きかねないが、抜本的な対策は難しい。基本的にユーザーが設定を変更できたり、ケーブルやデバイスを触ることが出来ないことが望ましい。極論すれば、キーボードとマウスとディスプレイ以外をサーバー室に収納すればよいが、通常は場所の制約などで不可能なことが多い。我々は次のような対策を行った。

1. ユーザーが設定できるデバイスをなくすために、端末は全てDHCPでIPアドレスを取得するようにする。さらにその設定がユーザーに変更できないようにする。一部導入されたX端末については、ネットワークプリンタについてはプログラムの変更を行った。
2. 盗聴を防ぐためネットワークは全てスイッチで構成した。想定外のマシンの接続を防ぐため、スイッチのポートセキュリティ機能を有効に利用した。ポートセキュリティ機能とはスイッチのポート毎に登録されたMACアドレス以外のMACアドレスが検出された場合、そのポートの通信を遮断する機能である。2,000に近い数のMACアドレスを登録することは容易ではないが、初期の仕事量に比べて得られるメリットは大きい。さらに、可能な場合はスイッチ自体もサーバー室内に設置する。スイッチのようなネットワーク機器もパスワードを忘れるなどの緊急時の手順がマニュアルに示されていることが多く、物理的にアクセスできるスイッチはもはや安全ではないため、最終的にはサーバー室などの物理的なアクセスが制限された場所にあるスイッチで制限する必要がある。

4—2　メール、WEBに関するトラブル

- .forwardに数Kbyteのアドレスを羅列し、sendmailが処理しきれなくなる。
- メールアドレスを偽ってメールを発信する、WEBの掲示板に書き込みをするなど匿名で騒ぎを起こす。
- 同級生3,500名にメールを送る。さらに3,500名に返事を書く。
- 外部からのpopアクセスを盗聴し、システムに侵入する。

大学においてもメールに関するトラブルは尽きない。しかし、今まで大学でよく運用された来たsendmail(qmail)+qpopperのシステムでは解決できないことも多い。特にpopについてはネットワークに頻繁にパスワードを流すため論外である。popについてはapopという解決も出来るが、我々のシステムではimap4を採用するため、SSL(Secure Socket Layer)を用いたimap4-ssl,pop3-sslを用いることとした。また、スケーラビリティや各種ユーザーインターフェイスの面から商用のメールサーバーであるSun Internet Mail Serverを採用している。これにより、ユーザーに対する各種の制限が容易に行えるようになった。なお、リモートアクセスによるパスワードの漏洩は他のプロトコル(rlogin,telnetなど)でもありうるので、外部からのアクセスは上記のimap4-ssl,pop3-sslの他はssh(Secure Shell)に限っている。

4—3　初心者をねらったTrojan、その他

1. UNIXシステムで他人のファイルのモードの不備をついてTrojanを仕掛ける。

UNIX系のシステムにおいて最も悪戯をされやすいのが、このような古典的な手法によるものである。大学の計算機センターでこれを根本的に防ぐのは困難であるが、有効な手法がいくつか考えられる。

1. ファイルシステムのマウントオプションで、SetUID,SetGIDを無効化する
2. デフォルトでは他人のホームディレクトリは

見えないようにしておく。デフォルトのumaskの値も厳しくしておく。初心者の多くは設定変更を行わないので、この作業によって悪戯は激減する。

5 新システムでのその他の対策

1. ネットワークはほとんどをプライベート空間に閉じ込めた。NATは行わない。グローバルアドレスを持った一部のマシンのみ、SSHに限ってログを取った上でアクセスを許可する。
2. WEBは必ずPROXYサーバーを経由して見させ、ログを保管する。
3. syslog専用サーバーを用意し、syslogをリモートマシンにも保管することによって、もしもクラックされた場合でもsyslogの改竄が出来ないようにする。
4. UNIX, Windows両システムが相手側からクラックされることを防ぐため、ユーザーのホームディレクトリは両システムで別個に用意した上で、互いにロードオンリーにする。
5. ネットワークプリンタの不正利用を防ぐため特殊なヘッダを付けないとPSファイルを印刷できないように変更した。
6. Windowsシステムのレジストリ、ファイルシステムについて、すべてのアプリケーションをチェックし、必要最小限の許可を出すように調整した。
7. Windowsシステムには商用のウイルスチェックソフトウェアを導入した。
8. パスワードの変更を推奨するため、パスワード変更をWEBベースで行うインターフェイスを導入した。
9. 情報コンセントはファイヤーウォールを介してインターネットにつながるようにし、登録ユーザー以外の者が利用できないよう構成した。
10. キーボード・マウスなどのケーブルを南京錠で固定し盗難防止を図った。

6 解決できなかった問題

いくつか解決策を見出さないまま実験的に導入したものもある。

1. 情報コンセントにおいて、同じスイッチにつながる他のユーザーPCのファイルシステムその他が見えることがある。
2. 情報コンセントにつなげたPCでDHCPサーバーを動かされると他のユーザーが正常に利用できなくなる。

これらの問題は根本的に解決するのは非常に困難であるが、今後VLAN技術によって解決できる可能性は皆無ではない。

7 まとめ

大学の計算機センターという様々な意味で条件の厳しい場所でのシステムインテグレーションにおいて有効なセキュリティ対策を行うことが出来た。