ネットワークとセキュリティ
「本学の現状と今後へむけて」

高瀬　剛

1　はじめに

1.1 本稿の目的

インターネットの商用利用が開始されて以来、インターネットを取り巻く状況はずいぶん様変りしてきた。

現在ではパーソナルコンピュータが無くとも、携帯電話があればE-mailやWorld Wide Web（以下WWWと略記）等の基本的なネットワークサービスが受けられるようになってきている。このように現在ではインターネットは生活に密着したものとなっている。

インターネットは新しいコミュニケーション＝インフラストラクチャである。この基盤の上でのコミュニケーションは、我々がかつて経験した事の無いような問題をいくつも抱えている。それらの問題は、コンピュータ・ネットワークに特有な問題もあれば、社会システムに起因するものもあり、単純には解決不可能である。

大学などの研究機関のコンピュータ・ネットワークについては比較的オープンであることが多く、ネットワークで起こり得る問題点を十分理解したうえで、管理・運用しなければならない。本稿ではインターネットの実情を踏まえ、教育機関のものとしてふさわしいネットワークを構築することを考えていく。

1.2 教育用ネットワークの意義

インターネットの特性と、今後の発展を見据えると、大学の教育用ネットワークの在り方が見えてくると考える。ここで言うインターネット特性とは、

「ディジタルデータに変換できものならなんでも双方向でやりとりできる」ことを指している。この本質そのものは変化することは無いが、「ディジタルデータに変換できもの」として思いもよらぬ物がでてきたり、あるいは「データのやりとりの速さ」が劇的に高速化するすることは十分に考えられる。これらを踏まえて、教育用ネットワークの意義としては

(1) 社会システムに組み入れられたインターネットの仕組みを良く理解することができる。
(2) ネットワークコミュニティを良く理解することで、コミュニケーションそのものや社会そのものについて理解を深めることができる。
(3) 国境を越えた所にいる人々との現地語でのコミュニケーションにより、現地の文化への理解やその言語の習得を促すことができる。
(4) Webなどでオリジナル作品を公開することができる。
(5) 国際的な研究基盤として利用できる。

などが挙げられる。現在の技術発展の速度は「秒進分歩」と評されているようにとてつもなく速い。しかも、大学で教育を受ける学生は初めてコンピュータについてを学んでから数年後に社会に出ることになるので、学生の時分に学んだ事の大半は社会に出ると直接役にたたないことが多い。この問題に対処するためには

(1) コンピュータ・ネットワーク教育の際にはできる限り普遍的な部分をきちんと理解させ、現在表面に見えている問題が、その普遍的な部分から導き出せる事を理解させる。

だけでなく

(2) コンピュータ・ネットワークそのものを静的なものとせず、実時間的に改良・発展させていく。

必要がある。大学ではこのようなコンピュータ・ネットワークを構築し、運用する事が教育的見地からも、研究機関としても今後ますます重要になってくると予想される。

1.3 Windows NTシステムの問題点

最近まで本学で用いられていた各種サーバ用OSであるMicrosoft社のWindows NTが抱える問題点を以下に述べる。

(1) 導入／維持費用が高い。

Windows NT が稼働するホストコンピュータで予定しているネットサービスを提供するのにも、専用のソフトウェアを別途用意する必要がある。そのためオペレーティングシステム（以下OSと表記）そのものに費用がかかるだけでなく、その専用ソフトウェアにも費用がかかる。

また、OSのバージョンがあがるたびにメイカーの思惑で使い勝手が大幅に変更されてしまう。そのため管理者を育てても、その管理者が一人立ちできるころにはそのバージョンのOSは古くさいものになり、その管理者自身も新しいシステムでは使いものにならない。そのため、このOSの管理者を育成するには定常的に管理者教育コストを支払わなければならない。

(2) セキュリティに問題がある。

(2.1) クラッキングに対して脆弱

ユーザの見掛け上の利便性を追求するあまり、売り物の割には粗野なOSの設計あるいは実装である。これは、ソースコードを公開しないからこそ可能な方法である。しかし、ソースコードが無くとも世界中のユーザがハッキングあるいはクラッキングによりその粗野な部分を暴き出すことは不可能でない。実際にそのように暴き出されたセキュリティ上の不具合は表面化して対処されたものだけで144個にのぼる。ソースコードが公開されていないので事実関係は不明だが、相当数のセキュリティ上の不具合が表面化しないまま存在しているといわれている。

(2.2) ウィルス／ワームに対して脆弱

これも粗野なOSの設計あるいは実装であるために引き起こされることが多い。幸い、Windows NTの場合、管理者権限でコンピュータを利用していなければほとんど問題になることはない。ただし、Windows NTを利用するユーザ層はコンピュータを管理する上での基本をきちんと学んでいない人が多いように見受けられる。そして、そのようなユーザは常に管理者権限でコンピュータを利用している傾向が強いようである。つまり、このようなWindows NTのユーザに対してはウィルス／ワー

ムは容赦なくそのコンピュータを荒すこと可能性がある。これが端末コンピュータであれば被害は比較的小さくて済む可能性が高いが、各種サーバの動いているコンピュータである場合、その被害は甚大なものになる可能性が高い。

(3) OSの不具合への対処

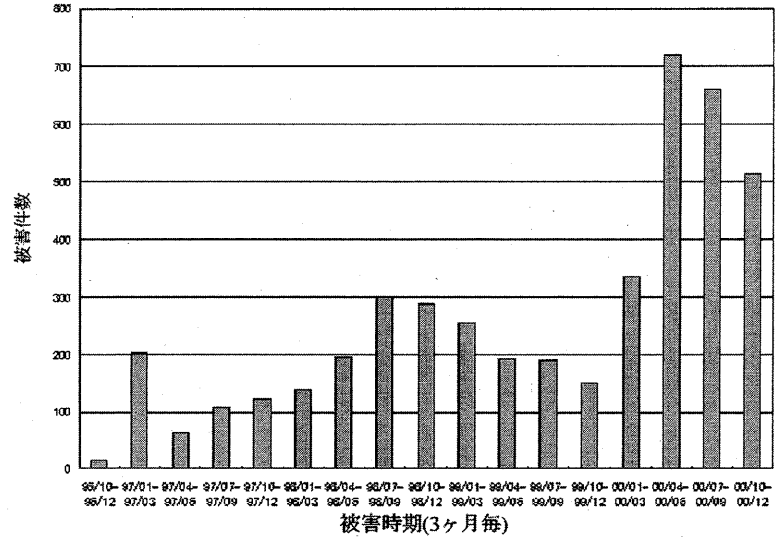
もし、OSにバグまたはセキュリティホールがあった場合、メイカーが対処するまでそのBUGやセキュリティホールは無くなることはない。もし仮に、そのWindows NTが動いているホストコンピュータが非常に重要な役目を負ったものである場合でかつそのOSにバグやセキュリティホールがあった場合、そのホストコンピュータを利用するサイトにとっては致命的な損害を与える可能性がある。他のネットワークサイトに迷惑を掛けないためにも、このような不具合は早急に修正されなければならない。しかし、数年前までメイカー製のOSの場合、優秀な技術者の人数的あるいは経済的な制限から、この様な不具合に対して修正をする事は稀であった。ごく最近では、不具合に対して、メイカーの方から以前に比べれば迅速にWWWなどを通じて不具合修正用プログラムが配付されている。しかし、例えばMicrosoft社では1999年の8月20日からこのような不具合対策のWebPageを設けて不具合修正に努めているが、修正の頻度は1ヶ月で8件程度とそれほど多くはない。これに対してFreeBSDなどでは半年に一度新しいリリースが出てくるが、この際には数百件程度のバグやセキュリティホールが修正されており、また、リリース後でも致命的な不具合が発見された場合には、メイリングリストやWWWなどを通じてすぐにユーザに知らせる仕組みになっている。つまり、FreeBSDなどの場合では、OSの不具合の対処に関してユーザが十分了解した上で利用できる体制が出来上がっていると考えて良い。逆にWindows NTなどの場合、バグやセキュリティホールなどの不具合への対処に関してはあまり考慮されていないと考える。

(4) オープンソースでない。

(2)、(3)にかかわる事であるが、Windows NTのソースコードを一般のユーザ（管理者もユーザのひとり）が手にいれる事ができない。もしオープンソースであれば、(2)、(3)の様な場合に対しては、ユーザレ

ベルでも迅速かつ的確に対処する事が可能である。オープンソースの場合、悪意をのこもったソースコードの混入を危惧する話をよく耳にすることがある。しかし、これらのソースコードは十分良く管理され、しかも世界中の開発者達がソースコードの内容を理解してるので、少なくともオープンソースOSの場合には実際にそのような問題が生じることは無い。逆に、オープンソースでない単一のメイカーのOSであった場合を考えるとそのOSに悪意のこもったコードが入っていても、ソースコードが一般ユーザには手に入らないためその悪意のコードの存在を一般のユーザは知ることができない。会計などの監査と同様に、第三者が監査できないようなOSはその公平性が保たれていることを保証するのは困難である。

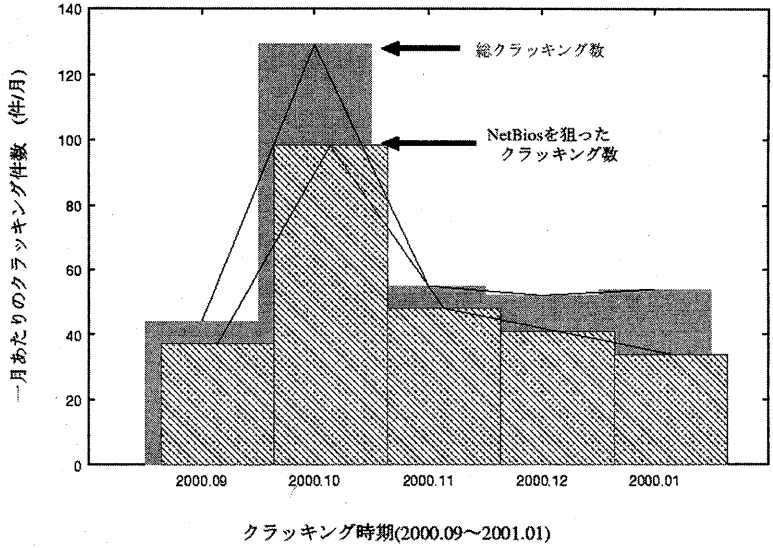
1.4 クラッキングの現状



[図1:JPCERT／CCへの不正アクセス届出状況（JPCERT／CC資料より)]

図1はコンピュータ緊急対応センター（以下JPCERT／CC）によせられた、不正アクセス状況の報告である。このグラフからここ数年、不正アクアセス届出がかなり増加していることがみてとれる。図2に本学へのここ数か

月のネットワーク攻撃の状況を示す。これをみると、実害は無かったものの毎月約40件～50件の不正アクセスの痕跡が残っている。この数か月の本学への不正アクセス攻撃のうち、Windowsネットワークのプロトコルである NetBIOSを狙ったネットワーク攻撃が全体の77%にのぼっている。

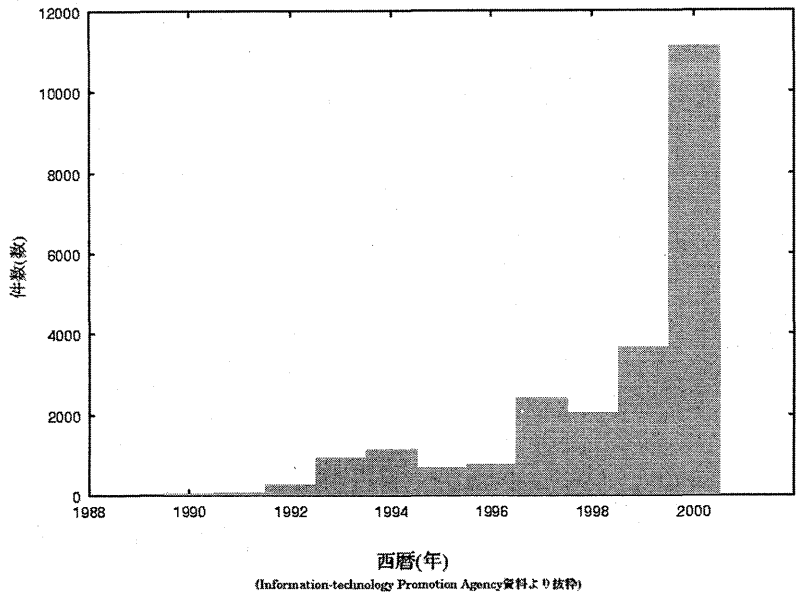


[図2:梅光女学院大学のサーバー群に対する月毎のクラッキング件数]

NetBIOSはWindowsネットワークの要のプロトコルであり、Windowsネットワークを構成するWindows 95／98／NTの脆弱性をつこうとする攻撃である。したがって、管理者の立場で外部からのクラッキングに強いネットワークを作る際にはWindowsプラットホームはその脆弱性をクラッカーに狙われやすい危険なOSであるということを考慮する必要がある。自サイトへのクラッキングを防止するためには、数段階の安全策を講じる必要があるが、Windows 95／98／NTはそのためのOSとしては完全に不適格である。

1.5 コンピュータウィルス／ワームの現状

図3はInformation-technology Promotion Agency（以下IPA）に届けられたウィルス被害状況である。特に2000年中にはMTX（2000.8.30)、Hybris



[図3:IPAへのコンピュータウィルスの届出状況（IPA資料より)]

(2000.9.25)、Navidad (2000.11.3) などの凶悪なコンピュータウィルス(以下単にウィルスと表記）が発見され、様々なサイトがこれらのウィルスの被害に遭った。この3つのウィルスの危険性に関して、発見当初からアンチウィルスソフトウェアベンダ各社は警告を発していたが、本学情報センターの端末コンピュータもMTXに2回程感染し、被害に遭った。これらのウィルスはいずれもWindows 95／98／NTの設計・実装上の不具合を悪用したものである。近年、ほぼ全てのウィルスはWindows 95／98／NT上の同様の脆弱性をついて動作するように設計されている。この脆弱性はWindows 95／98／NTとそのOS上で動作するアプリケーションとのデータの連係の見掛け上の利便さを提供する機能の実装に起因している。

現状では、ほとんどのウィルスがE-mailの「添付文書」経由で感染してゆくが、E-mail本来の利用（「添付文書」などは使わない）をしているだけであれば特別なソフトウェアを用いる事無くウィルスを撃退する事ができる。しかし、現実に多くのユーザはユーザ自身が認識すること無しに「添付文書」

を利用しており、一般ユーザのレベルでは特別なソフトウェア無しにはウィルスを撃退するのはほぼ不可能である。また、最近のウィルスは適当な手段を用いて自分自身を変化させて発見されにくくなるようにプログラムされている。したがって、長い間コンピュータをウィルスに感染したままにしておくと最悪の場合、OSを再度セットアップする必要に迫られる可能性がある。

1.6 解決策

今まで述べてきたような問題点を総合して考えると

(1) 柔軟なネットワーク構築・改変が容易なシステム
(2) クラッキング耐性、ウィルス耐性の高いシステム
(3) 教育用ネットワークシステムとして十分高いパフォーマンスを発揮する、コストパーフォーマンスの高いできる限り安価なシステム

のような条件を満たすシステムが本学にとっては必要なシステムである。このような条件を満たすシステムとしてはLinux各ディストリビューション、FreeBSD、NetBSD、OpenBSD、Solaris8が挙げあられる。これらのOSはUNIX系統のOSであるため(1)を容易に実現できる。また、ソースコードが公開されているので(2)も容易に実現できる。さらに、これらのOSは無償で提供されているため、(3)のコストパフォーマンスは十分高く、また、世界中の開発者によって日々開発が続けられているため、十分高いパフォーマンスが得られる。よって、本学のネットワークシステムにふさわしいOSは上に挙げたものから選択することができると考える。

2 システムの構成

2.1 FreeBSD3.xRELEASEによる教育用サーバの構築

教育用システムのOSとして1999年8月当時、FreeBSDシリーズの中で最も安定して稼働していたFreeBSD-3.xを選択した。FreeBSDを選択した理由として

(1) 管理者（つまり筆者）が1995年以降使用しており、システムを熟知している。
(2) 管理者は1991年以来BSD由来のUNIXsystemを手掛けており、FreeBSDのみならず、BSD由来のUNIXシステムを良く理解している。
(3) FreeBSDはYAHOOなどの名の通ったサイトが利用しており、

FreeBSDに起因するトラブルの報告を受けた事が無い。

(4) 各種サーバ用のOSとしては、Linuxや他のBSD由来OS（NetBSD、OpenBSD）と比較して、ネットワーク周りのドライバの熟成度が高く、OSの標準設定でのセキュリティポリシーの高いFreeBSDが最も実用的である。

(5) Linuxや他のBSD由来OS（NetBSD、OpenBSD）、または最近のSolarisと同様に、ソースコードが公開されている。

(6) FreeBSDは既に10年間程インターネット上で使われ続けており、ほとんどの不具合は修正され尽くしていることが期待できる。

などが挙げられる。ここでは細かく挙げていないが(5)に付随するセキュリティ面の安心感はコンピュータ・ネットワークの管理者の精神衛生上とてつもなく有利な点である。

本学で利用している各種サーバ用のホストコンピュータ（コンピュータ名KIBOU）は管理者自身が組み立てた物を利用している。主だった部品の規格は表.1の通りである。このホストコンピュータは学内用のWebサーバや、

表1:大学用サーバのスペック

CPU	AMDK6-2／500MHz
Mother Board	Freeway TI5VGF（VIA Appollo MVP3チップセット）
Memory	PC／100 SDRAM 128MByte
Hard Disk Drive(1)	QUANTUM FireballSE2.1A 2GByte（OS用）
Hard Disk Drive(2)	IBM DJNA-352030 20GByte（ユーザデータ用）
Network Interface	3Com 3c905-TX（Fast Etherlink XL）

Windowsネットワーク・クローンのファイルサーバ、あるいはE-mailサーバなどとして利用されているが、この程度の負荷であれば経験的に問題無く処理できるようである。現状では実際に使用されているユーザのデータ領域の容量は約6.3GByteであり、その他のデータが約6 GByte程度で、既に合計12GByte程度のディスクスペースを使用している。今後、ネットワークの増強に伴ってユーザ数が増加することにより、ファイルサーバのディスクスペースが枯渇することが懸念される。

2.2 ユーザ管理

ユーザデータの管理は、伝統的なUNIXのNISで行っている。「UNIXのユーザ」と「Windowsのユーザ」ではOSの実装の段階で意味が異なっているため、相互のOSでユーザの概念そのものが完全に互換ではない。そのため、後述のsamba（2.3節）ではユーザデータベースをNISとは別に持っている。いいかえれば、ユーザ管理データは、ネットワークサービス毎に2種類のユーザ管理データベースが使用されることになる。つまり、UNIXの直接的なサービス（例えば??）では、NISのユーザ認証が使われ、sambaを経由して行われるサービス（すなわちWindowsネットワークサービス）にはsambaのユーザ認証が利用される。そこで、本システムの管理者は新規ユーザにパスワードを入力させる際にはこの2つのデータベース（NISとsamba）を同時に登録した方が効率良く管理できるであろう。

2.3 samba-2.0.xによるWindowsネットワークの構築

sambaとはWindowsネットワークサーバを置き換えるもので、Windows NTを代替するUNIX上のデーモンプログラムである。以前利用していたWindows NTを置き換えるため、Windows用の設定を全て継承した上で、ユーザへの新たなネットワークサービスの提供を開始するための準備を行った。具体的には

(1) samba用のユーザデータベースの作成
(2) Windowsネットワークで利用される標準的な「Profileデータ」の準備
(3) Windowsネットワークで利用される標準的な「Netlogonフォルダ」と「ログオンスクリプト」の準備

などが必要である。クライアントコンピュータ側では、特に設定の変更の必要は無い。

また、必要に応じて、全てのユーザあるいは特定のユーザだけが利用できる共有フォルダも作成することができる。2001年1月の時点では大学の全ユーザが利用可能な共有フォルダを作成している。

2.4 IMAP4によるE-mailサービスの構築

IMAP4とはE-mailを受け取ったユーザがそのE-mailを閲覧するための

サービスを提供する、UNIX上のデーモンプログラムである。IMAP4自体のインストールや設定は至って簡便である。ただし、IMAP4単体ではそれほど安全性が高くないので2.6節で後述する設定を施し、アクセス可能なコンピュータを制限する必要がある。またユーザがE-mailの読み書きを行えるように、クライアントコンピュータ側にE-mailリーダ（ここではNetscape Messenger）をインストールする必要がある。E-mailリーダ自身で複数ユーザ管理機能を持ったものもあるが、本学のシステムとしては、E-mailリーダの管理機能ではなく、より安全なホストコンピュータによる管理を基本としているため、ここでは全ユーザに共通の設定をする。これにより、第三者への個人情報（E-mailの内容）の漏洩を防ぐことが可能となる。

2.5 Apache-1.3.Xによる学内Webサーバの構築

Apacheは世界で最も多く利用されているWebサーバであり、UNIX上のデーモンプログラムとして動作する事ができる。本ホストコンピュータでのWebサーバは学内への情報発信と、コンピュータ教育への活用が目的であるため学外からのアクセスは一切受け付けない設定にする。この措置を講ずることで、万が一、ユーザがユーザ自身のウェブページに個人情報を載せていたとしても、ネットワークを通じて学外へ漏洩することが無い。また、学内向けの情報が外部に漏洩するのは好ましいことではない。それゆえ、この様な設定は本学の場合妥当な設定であると考える。

2.6 各種セキュリティの設定

ホストコンピュータ（KIBOU）で利用するFreeBSD3.Xはインターネットスーパーデーモン（inetd）にセキュリティ機能（tcpwrapper）が標準で搭載されている。厳密にはネットワークポート毎にアクセス可能なIPアドレスを指定できる機能である。この機能を使うことにより、標準では脆弱なプロトコルを用いなければならないプログラムでも高い安全性を確保できる。また不要なネットワークサービス用のポートは塞いでおけばより安全な状態に保つことが可能である。また、sshをリモートシェルとしてあるいはsshのポートフォワード機能を利用することで、より高い安全性を確保できる。

3　本システムの効果

3.1 セキュリティの観点

以前のWindows NTでは他のサイトへの攻撃の足場として使用されており、大変な不名誉であった。しかし、現在では図2で示されているような不正なアクセスは全て拒否されている。いまのところ、全体的な基本設計がきちんとしており、セキュリティ的に非常にきつい設定となっているので、ネットワークを通じた直接的な情報の漏洩や、不正アクセスによるネットワーク的な攻撃は全て撃退している。

3.2 利便性の観点

(1) ユーザの利便性

まず、以前のネットワークに比べて、ユーザ自身のディスクスペースを提供できることがユーザの利便性を大きく向上させていると考える。近年のデータファイルの肥大化で、一つのファイルサイズが通常のフロッピーディスクで収まる容量ではなくなってきており、主なデータ保存媒体はフロッピーディスクからCD-Rへとすでに交替している。このような状況でアクセス速度の遅いフロッピーディスクを主体としたデータの保存を推奨するのは好ましいと考えるのには疑問を感じる。本学のコンピュータは少なからずネットワークに接続されているのであるから、そのことも十分活かしたデータの保存をすることが望ましい。

(2) 管理者の利便性

現管理者にとっては使いなれたシステムであるため、これといった不都合もなく操作できる。また、このシステムは遠隔操作によるシステム管理が可能であり、管理者の人材が不足している場合でも、少数精鋭で組織の情報ネットワーク管理を行うことが可能である。しかし、コンピュータの初心者に対してUNIXシステムの管理者教育を行おうとすると、みための素朴さと、呪文のようなコマンドに閉口するようである。

4　本システムの問題点

本学の現システムに対して、管理者は以下の様な問題があると考えている。

それぞれが独立した問題であるため、別々に述べる。

(1) ディスクスペース枯渇問題

現在20GByteのハードディスクドライブを使用しているが、このうち約12GByteの領域を使用している。今後も継続して、本ネットワークの拡大が予定されているのでこのホストコンピュータのユーザディスクスペースを早急に確保する必要がある。

(2) ユーザデータのバックアップ

データのバックアップも目的により採用すべき方法が異なる。現状では、バックアップ用の装置が全く無いためにデータのバックアップをとることができない。ここでは、ユーザもしくは管理者のそれぞれの立場でディスククラッシュに備えたバックアップの取り方を検討しておく。

(i) ユーザ自身によるバックアップ

ネットワークに接続されているある1台のコンピュータでCD-RやMOあるいはDVD-RAMなどを利用できるようにしておく。このコンピュータはバックアップ専用とし、それ以外の目的では使用しない。このようなコンピュータを設置することにより、ユーザ本人が自身のデータをバックアップし、責任を持って管理することが可能となる。

(ii) 管理者によるバックアップ

近年のハードディスクドライブの大容量化により、全ユーザ領域全体のバックアップを取る手段はほぼ無くなりつつある。しかし、ハードディスクドライブでバックアップをとることが可能ならば容量的な問題は即座に解消される。実際にはホットスペアに対応したRAID5システムなどをホストコンピュータに組み込み、バックアップの必要度合に応じてバックアップ用ハードディスクドライブを用意し、一日に1台ずつ交換してゆく。こうすることで、バックアップを取るためにわざわざ時間を掛けることもなく、大容量のデータをバックアップ可能である。しかも、ハードディスクドライブの価格は劇的に下がってきており、このような運用をするのも現実的になっている。

(3) 管理者育成問題

ネットワーク管理者は本来業務とネットワーク管理業務の二重労務を強いられる場合が多い。この問題は十年程前から既に指摘されていたが、その主な原因は人材不足である。ネットワーク管理業務を行うことは管理者個人のスキル（技能）には無関係であり、ネットワーク管理を行う場合は、むしろきちんとしたテクノロジを身につけ、ネットワークをきちんと理解していることの方が重要である。管理業務の一極集中を避けるためには、管理業務に堪える様な人材を育成することが必要で、そのためにはまず管理者の組織を整備することが重要である。管理者となったそれぞれが現状の業務に関する自己の理解段階を認識し、それぞれが次の段階へと進めるように自己学習あるいは上位の管理者からの指導という形を取れば内部で継続的に人材を育成してゆくことができる。これができない場合は外部から、それなりの人材を雇いれることも考慮した方が良い場合もある。いずれにせよ、情報ネットワークを維持・管理してゆくためには、それなりのマンパワーが必要である。またそれを確保するためには、管理者自身を強化するための管理者組織が必要である。

5　最後に

コンピュータ・ネットワークは大学における研究教育にとって今後ますます重要になっていくと感じられる。コンピュータ・ネットワークは一度走り出すと、少しのことでは止めることができなくなり、これを維持してゆくのはかなり面倒なことである。また、ネットワークサービス自身も進化し続けているため、安全で便利な新サービスは採り入れてゆかなければならない。このような社会的状況を視野にいれると、本学においては今後特にコンピュータ・ネットワークの管理のできる人材を一人でも多く育てることが急務であると考える。

参　考

- IPAセキュリティセンター情報セキュリティセミナー資料「コンピュータ不正アクセスの現状」
- IPAセキュリティセンター情報セキュリティセミナー資料「コンピュータウィルス被害の現状と対策管理」

・ネットワークワーキンググループBarbara Fraser編集 RFC2196「サイトセキュリティハンドブック」
・コンピュータ緊急対応センターウェブページ　http://www.jpcert.or.jp/
・情報処理振興事業協会ウェブページ　http://www.ipa.go.jp/
・マイクロソフト社セキュリティ勧告ウェブページ
http://www.microsoft.com/japan/technet/security/current.asp
・Symantec社ウェブページ　http://www.symantec.co.jp/

注　意

・本文中のWindows 95、Windows 98、Windows NTはMicrosoft社の登録商標です。