特集3 ❑ＰＣとウィルス

ネットワークを快適に安全に利用するために

情報処理・視聴覚専門委員会委員長　宮　川　　修

本学ネットワーク（NINES）が稼働した平成6年の学部利用者は数十人。それが現在は360人を越える。NINESは基本的インフラになり、これの停止は教育・研究活動を滞らせる。最近、学部の2つの支線が相前後して停止し利用者に迷惑をかけた。実のところ、7年が経過して設備が老朽化し、ここ数年は綱渡り的運用であった。ただ、幸いにも本年12月にケーブルとシステムが同時に更新されることとなり、新システムの仕様が検討された。老朽化が解消し一安心と思ったら、今回の仕様策定ではセキュリティーが最重要問題になり、特に学生用端末について非常にホットな議論が交わされた。少ない人員でのセキュリティー確保は困難として、情報処理センターは学生用端末の集中配置・一元管理を主張したのに対し、一部の部局は利便性を犠牲にする集中配置に反対し真っ向からぶつかった。

ネットワークのセキュリティーを脅かし混乱に陥れる意図的アタック。中央省庁のホームページが書き換えられたのはさほど昔のことでない。こうしたアタックは決して対岸の火事でなく我々も既に被害を被っている。たとえば、昨年秋に、学部図書閲覧室の学生用端末20台がMicrosoft Wordのマクロウィルスに感染し、学生有志からセンターの教官まで出動していただいてウィルス駆除をするはめになった。本年早々には、ある歯学研究者から「ウィルス感染事故に関する緊急のお知らせとお詫び」と題するファックスが全国に配信された。友人のメールに添付されたファイルを不用意に開いたため、彼のアドレス帳に記載の人達へそれが自動的に再配信され、さらに回り回って彼と面識がない私にも届いた。また、ウィルスがしこまれたファイル添付メールが国立情報学研究所のsinet上で全国にばらまかれたのはつい最近のことである。もし、これらの添付ファイルを私が開いていたらどうなったか。自分のコンピュータシステムは破壊されても、手間（ほぼ1日）はともかく、再インストールして回復できるが、文書や画像ファイルの破壊は悲劇的だ。もっと深刻なのは、被害が自分だけにとどまらず、友人・知人を介して彼らの友人・知人へとネズミ算式にひろがっていっただろう。それを思うと背筋に悪寒が走った。

セキュリティー問題はネットワークを根底からおびやかす大変やっかいな問題である。一台の端末がアタックされただけで被害は瞬時に全国的・世界的規模で拡大する。セキュリティーを確保する方法の一つはその便利な機能を制限することであろう。これを追求するとそれはネットワークでなくなるが、我々はそれなしではすまされなくなっている。セキュリティーの確保。それはもはやネットワーク管理者の努力だけでは不可能になっている。**学生も教職員も、利用者一人一人がネットワークセキュリティーについて認識を深め適切に対応していただくことが重要である。**

そこで、このたびは広報委員会のはからいにより、学部ネットワーク管理の実際を行っていただいている小林博先生と鈴木一郎先生に、ネットワークを快適に安全に利用するための心得などを解説していただく。

歯学部を不正アクセスから守るために

ネットワークのセキュリティーについて

口腔外科学第一講座　鈴　木　一　郎

1．はじめに

昨年から大学や官公庁の web ページが書き換えられるという事件が度々報道されています。これらの多くは Script Kiddie[1] と呼ばれる悪戯者による一種の愉快犯的な仕業で、実害はそれほど大きなものではありません。しかし、これと同じことがもし大切な職場のデータやあなたが書いたメールで起こったらどうでしょうか。“I love you” と書いたメールを恋敵は “I hate you” と書き換える可能性があるのです。これらの事件の教訓はインターネット上にある情報は常に一定の危険にさらされているということを認識しなくてはいけないということです。コンピュータネットワークはわれわれの生活から切り離せないインフラとなっています。そして、インターネットが実現するバーチャルな社会が拡大し、そこで e コマースや電子マネーといった商業活動が行われるようになった現在、いたずらや泥棒などの犯罪者が増えるのは必然でしょう。泥棒どころか、最近では政治的な背景をもつテロリストの標的にさえなっています。一方で、インターネットの仕組みは驚くほど原始的なもので（そういう単純性こそインターネットの最大の特徴です)、また私たちがネットワークに接続しているパソコンも見かけの向上の割には外敵に対する防御は決して充分ではありません。こそ泥対策くらいならまだしも、犯罪のプロの手にかかってはひとたまりもありません。

実社会の中で身を守るためには、家にカギをかけるといった個々が果たすべき役割、そして個人では防ぎきれない部分は社会の仕組みとしてカバーする必要があります。バーチャルな社会であるコンピュータネットワークでもこれと同じ仕組みが必要となります。このうち前者の個々の問題についてはコンピュータウィルスの問題を中心として小林先生に担当していただきましたので、本稿ではネットワークシステム全体のセキュリティー管理についてまとめてみます。

2．インターネットの脆弱さ

インターネットが軍事目的のプロジェクトとして誕生したことは良く知られていますが、これは分散通信環境を実現する研究プロジェクトであって、インターネットそのものが軍事利用されることはありませんでした。結局、インターネットはアメリカの中で研究者を結ぶ情報交換網として発達し、全世界に広がっていったわけです。元々研究者のためのネットワークですから、「利用者は全員善人である」つまり性善説が前提となっています。最低限のセキュリティーはあるものの、悪人がなにかよからぬことをしでかすことはあまり想定されていませんので犯罪には大変脆いのです。ついでですが、マスコミでネットワーク上で悪事をはたらく者をハッカー（hacker）と呼んでいますが、本来ハッカーとは、知識を駆使して技術的好奇心や技術的可能性を追求する人をさすのであって、そういう知識や技術を悪事に転用する者はクラッカー（cracker）と呼ぶのが正しい使い分けです。

電子メールや web などインターネット上のサービスの多くはサーバと呼ばれる常時稼動のコン

1）Script Kiddie
インターネットから攻撃ツールをダウンロードして、面白半分で第三者のシステムに侵入しようとする者の総称。一般にコンピュータに関する知識はそれほどなく、罪の意識はほとんどない。

ピュータおよびその上で動くプログラムによって提供されていますが、プログラムにはバグと呼ばれる予期せぬ不具合が潜んでいます。このような不具合のうちセキュリティー的な弱点はセキュリティーホールとよばれていますが、ネットワーク犯罪者はそこをついてサーバに対して様々な弱点探しを試みます。このような他人の家を用事もなく覗くような行為を「不正アクセス」とよびます。もちろんサーバやプログラム側でも日夜対策を行っているわけですが、対策をすると犯罪者はまた新たなセキュリティーホールを見つけ出すといういたちごっこのような状況となっています。不正アクセスによってサーバにセキュリティーホールが見つかると犯罪者は次に管理権限の奪取を試みます。不幸にもサーバ乗っ取りが上手くゆくと、ネットワーク犯罪者は次にそのサーバを経由(「踏み台」といいます）して他のサーバやネットワークに触手を伸ばします。乗っ取られたサーバの管理記録（ログ）は証拠隠滅され、またバックドアと呼ばれる裏口が作成されたりしますので、後に乗っ取りが判明しても犯罪者の足取りをたどるのは大変困難となります。甘い管理をしていると、知らないうちに踏み台にされて犯罪者に荷担していた、などということにもなりかねません。

なお、皆さんが利用しているパソコンは常時稼動ではありませんし、サーバのように多種多様なサービスを行っているわけではありませんが、ネットワークに接続されている限りは不正アクセスを受ける可能性がありますのでそれに対する注意と対策は必須です。最近では不正アクセスを防ぐためのソフトウェア[2)]が販売されていますからそれらをインストールしておくとよいでしょう。

3．安全性と利便性

不正アクセスなどのネットワーク犯罪に対する対策は安全性と利便性とコストなどのバランスをよく考える必要があります。これがセキュリティーポリシーです。建物の防犯を強固にするためには、鍵は１個よりも２個、２個よりも10個、多ければ多いほど安全性は高まりますが、そのために要する費用は増大しますし、10個も鍵があったら建物の出入りに不便で仕方ありません。その建物が自宅であれば鍵は１個か２個もあれば充分と考えるでしょうし、銀行ならば10個でも足りないかもしれません。ネットワークやコンピュータのセキュリティーもこうした建物の防犯対策と同様、組織ごとにバランスのとれたセキュリティーポリシーを決める必要があります。そしてどこの組織でも以前と比べて、そのバランスをより安全性寄りに重みをかけざるを得ないのが現状といえるでしょう。

4．大学ネットワークの特徴と新潟大学のネットワーク（NINES）

大学というところは、一般企業などとは異なり部門や個人の独立性が大変高い組織です。このためコンピュータやネットワーク運用に関しても、組織全体の利益のために一貫したセキュリティーポリシーをトップダウンで決めるといったことは一般に困難です。とりわけ新潟大学のような総合大学では、学部・学科によってもネットワークの利用形態が大きく異なり、利用者は自由な環境を望み、管理者はボランティア、というような条件のもとで結果として安全性よりも利便性寄りの運用がなされてきました。

図１は現在の新潟大学のキャンパスネットワーク（NINES）の概略を図示したものです。ここで注意していただきたいことは、キャンパス内のネットワークがグローバルネットワークつまりインターネットそのものとなっていることです。「インターネットに接続しているのだから当たり前じゃないか」と思われるかもしれませんが、通常企業などでは、組織の出入口（図１の「WAN ルータ」の部分）にファイアウォールという機器を入れて内外のネットワークを遮断するのが通例です。孤立した組織内ネットワークを作った上で、インタ

2)　不正アクセスを防ぐためのソフトウェア
例えば、Norton Internet Security という製品にはウィルスソフトとともに不正アクセスを防ぐためのソフトウェアが同梱されている。

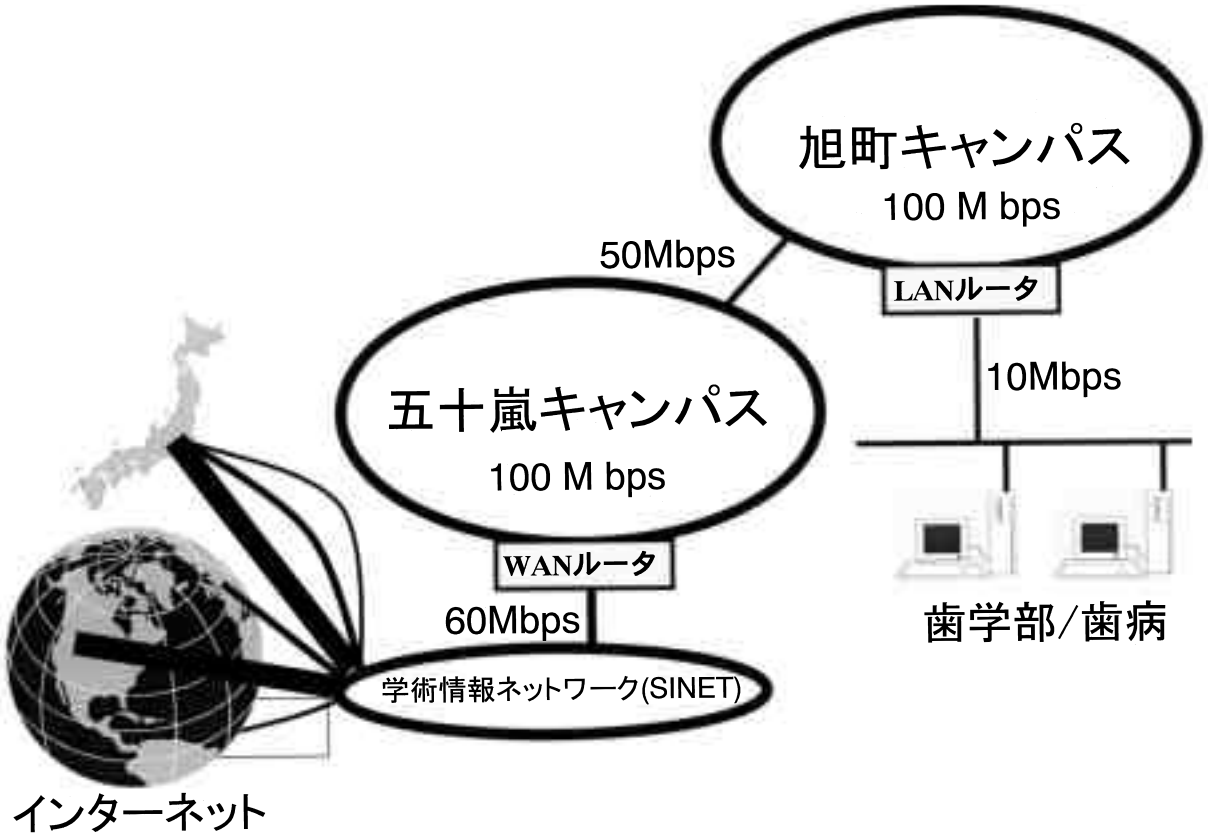

図１　新潟大学のキャンパスネットワーク（NINES）

ーネットとは間接的に接続し[3)]、外部からの侵入を防ぐわけです。ファイアウォールとは文字通りネットワークの防火壁で、外から内向、内から外向の通信をすべてチェックして、その組織にとって不要な通信や怪しい通信はブロックします。また、外部から内部のネットワークを直接参照できないように設定するのが通例です。新潟大学の場合は、現在のところ Windows ネットワークの共有機能に必要な通信をブロックする設定などがなされていますが、キャンパス内でネットワーク接続されているコンピュータは外部のネットワークから（つまりインターネット上のどこからでも）丸見えとなっています。利便性や自由度が大変高いネットワークですが、その分セキュリティーは個々のコンピュータで守らなければならない割合が高いわけです。

５．不正アクセスの実例とセキュリティー対策

実際に歯学部で過去に起こった不正アクセスの一例をあげてみます。

事例１：phf アタック

4 年ほど前に、web サーバに対する phf アタックというものが世界中を席捲し、セキュリティー対策が他人事ではないことを思い知らされました。phf アタックはサーバのパスワードファイルを web ページから覗けてしまう、というもので、歯学部のサーバのログ（サーバではいつ誰がそのサーバのどんなサービス/ファイルにアクセスしたかを記録しています）を詳細に調べてみたところ、学内外からアタックを受けた形跡が残っていました。元来パスワードファイルはそのサーバのユーザならば誰でも見ることができてしまうもの

3)　インターネットとは間接的に接続する
　歯学部ニュースの前号で紹介した附属病院の医療情報システムでは、何重ものバリアを設けて唯一 UMIN を経由したインターネットサービスのみを実現している。

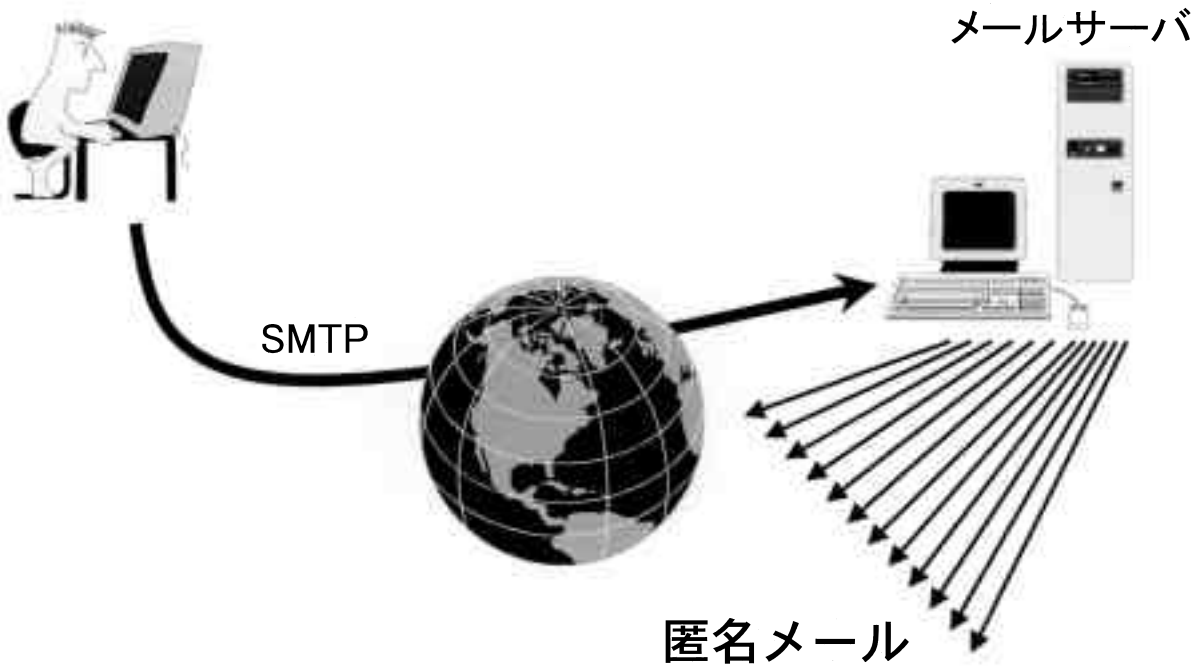

図 2　Spam Mail（メールの不正中継）
他の組織のメールサーバに多量の匿名メールを中継させる、あるいはメールサーバを妨害する。

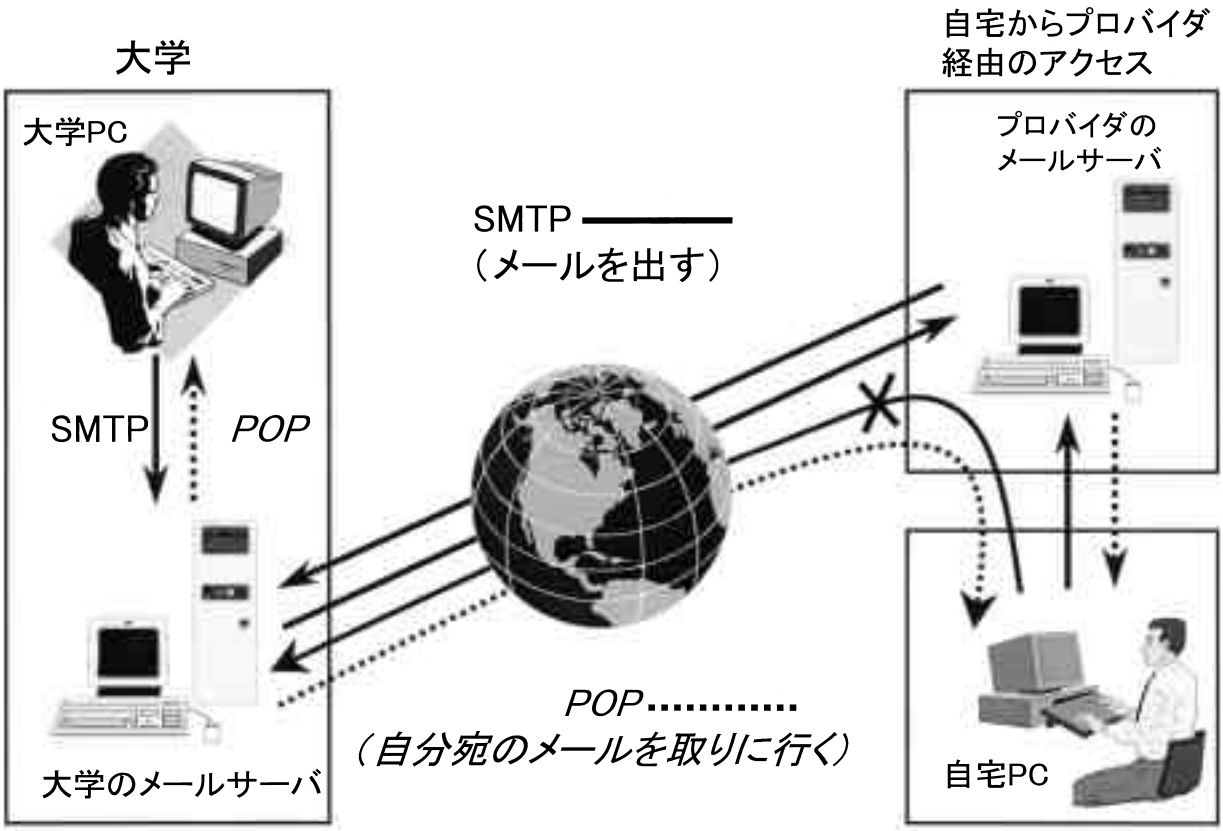

図 3　Spam Mail 対策
外部のネットワークからメールの不正中継を許さない設定のため、プロバイダ経由で大学メールサーバへメールを投函することはできない。

で、もちろん暗号化はされていますが、力技でそれを解読することは難しいことではありません。学内からのアタックは単なるいたずらだったことが判明しましたが、学外からのアクセスについては悪意で行われた可能性があります。この事例はサーバのセキュリティーもさることながら、各ユーザのパスワード管理（安易なパスワードはクラックツールというソフトウェアで容易に解読できてしまう）がいかに重要であるかをも示しています。

事例２：ポートスキャン

サーバに対して、手当たり次第にそのサーバがどんなサービスを行っているのかを調べる行為です。セキュリティーホールなどをついてサーバ乗っ取り行為を行う前段階のいわば下調べとして行われます。３年くらい前から流行しはじめ、現在でも学内のサーバのログを見ると国内外を問わず頻繁にポートスキャンの痕跡がみられます。実際にサーバが乗っ取られて、そこを踏み台として他のサイトにポートスキャンを行っていた学内のサーバの事例があります。相手のサイトからの指摘で初めて乗っ取りが判明しました（犯罪者に荷担してしまった例です）。

さて、このような不正アクセスをもふまえて、現在歯学部内のサーバではいくつかのセキュリティー対策を行っています。このような対策の詳細を記載することは本稿の趣旨ではありませんので省略しますが、ユーザの皆さんに利用上、注意していただきたい点を記載しておきます。

A）Spam Mail 対策

なんらかの意図を持って匿名で電子メールをばらまきたい、ということを考える者がいて、このようなばらまきメールを Spam Mail とよびます（図２）。Spam Mail は近所のポストに投函したのでは足がついてしまいますので、よその組織のメールサーバが不正利用されます。この中にはダイレクトメールのように鬱陶しい以外は大して害のないものもありますが、悪意をもってメールサーバに多量のメールを送り障害を与えるといった妨害目的[4]で行われる場合は深刻です。このようなメールは自組織以外から投函されたメールを拒否することにより防ぐことができますので、現在インターネット上のメールサーバのほとんどはそのような設定がなされています。

この設定のために、プロバイダ経由で大学のメールサーバを利用している方に注意していただきたいことがあります。

1）自宅から大学のメールサーバにアクセスして大学に届いたメールを読みたい。

2）自宅から大学のメールサーバにアクセスしてメールを出したい。

1)は問題ありませんが、2)についてはあて先が学内のもの以外は拒否されますので、メールソフトの SMTP サーバの指定を契約しているプロバイダのものに変更してください（図３）。

B）サーバへの不正アクセスに対する対策

不正アクセス対策のため、歯学部のメールサーバや web サーバへのアクセスは一定の制限を行っています。このため大学外から telnet ログインや ftp による web サーバコンテンツのアップデート作業はできません。

また、アクセス元のコンピュータの IP アドレスからドメイン名が引けない場合[5]は接続を拒否するようになっています。学内でのネットワーク利用でも、端局設置申請書で正式に登録されていない IP アドレスを流用すると拒否にあいます。

4） 妨害目的

メールに限らず特定のコンピュータに多量のデータ（パケット）を送り続けて正常な機能を妨害する攻撃方法を DoS アタック（Denial of Service）と呼ぶ。店の前で大騒ぎして営業妨害するようなもの。不正アクセスとは少々意味が異なるが、方法が単純な割にはなかなか良い対策がない。

5） IP アドレスからドメイン名が引けない場合

インターネットに接続されている機器は IP アドレスというユニークな番号でお互いを識別しているが、人間にもわかりやすいように文字列によるドメイン名というニックネームをつけることが可能である。IP アドレスとドメインを相互変換するデータベースを DNS と呼ぶが、端局登録されていない IP アドレスはそのデータベースにドメイン名が記述されていない。余談だが、電話番号にもこのようなニックネームをつける仕組みがあると便利ではないだろうか？

6．インターネット上のデータは丸見え

電話回線に何らかの仕掛けをすればその回線の盗聴ができてしまうように、インターネットも通信経路上のデータ盗聴は比較的簡単にできてしまいます。しかも、メールの内容もパスワードも原則として生のデータのまま流れています。実際にはインターネットの通信経路上には断片化された複数の通信が多重していますから、元データを復元することはそう容易ではありませんが、手間暇をいとわなければそれは可能なのです。また、盗聴以外にもデータの「改ざん」（冒頭の“I　love you”の例がそれです）や「なりすまし」といった行為が行われる可能性もあります。

通信に秘匿性を持たせるために誰もが思いつく方法はデータを暗号化することです。暗号を使う上で重要なことは、鍵が簡単には破られないこと、そして鍵を盗まれないようにすることです。電子データの暗号化は「解読するのに多大な時間がかかる」という数学的な原理に依存するのですが、これもまた家の鍵と同様に複雑な鍵を使えば安全性は増しますが、暗号化処理に多大な時間を費やすようでは現実的ではありません。最速のコンピュータで解読に1000年かかるような計算であればかなり強力な鍵でしょうし、単純な鍵であっても解読するのに100万円かかる鍵であれば100円の価値をもつ情報を守るには充分といえます。一方、鍵の盗難については、遠方の相手にどうやって安全に鍵を渡すのか、がポイントとなります。鍵をインターネット経由で渡そうとすると、その鍵を盗聴により奪取される可能性があります。そこで、公開鍵暗号という手法の登場です。公開鍵暗号では暗号化するための鍵（公開鍵）と復号化するための鍵（秘密鍵）とが異なり、秘密鍵の管理さえしっかり行えば鍵の安全性は保証されます。公開鍵暗号は、秘密鍵でサインして公開鍵でそれを確認する、という方法により電子署名にも利用されます。

暗号化や電子認証についてはまだなじみが少ないと思いますが、インターネット上での医療データの交換や電子カルテには欠かすことのできないものです。

7．新しいキャンパスネットワーク

今年は新潟大学に新しいキャンパスネットワーク（新 NINES）が構築されます。新 NINES では現在の10倍から100倍高速なネットワークが実現されますが、セキュリティー的にも様々な配慮がなされることになります。ネットワーク構成は現在よりはるかに融通性の高いものとなりますから、現在は不可能な学部・学科ごとのセキュリティーポリシーによる運用も可能となるかもしれません。

自宅など学外から大学ネットワークへのアクセスは大変需要が多いのですが、組織内のダイアルアップサーバ（電話によるネットワーク接続の受け口）は裏口となりやすく危険と考えられています。このため、新 NINES ではプロバイダ等の外部ネットワークから、VPN[6] という方法で安全にキャンパスネットワークにアクセスできるサービスが提供される予定です。

8．おわりに

安全に、そして便利にコンピュータやインターネットを利用するために、ネットワークやサーバのセキュリティー管理は手を抜くことのできない重要な仕事です。しかし、メールに添付されてくるウィルスや悪意をもった Java スクリプトなどから身を守るのは基本的に個々のユーザの責任です。これをネットワーク側で防御することは不可能ではありませんが、膨大なコストと手間の対価を払ってさえ万全ではなく、なにより利便性が大きく損なわれ不自由を強いられることとなります。繰り返しになりますが、ネットワーク社会も自由であるためにはユーザ各自の責任が大変重大なのです。

6）VPN（Virtual Private Network）
異なる複数のネットワークをあたかも一つのネットワークであるかのようにみせかける技術。強力な認証機能を持ち、また途中のネットワーク上ではデータは暗号化される。現在の Windows 系 OS では標準でサポートされている。

さて、コンピュータやネットワークのセキュリティーも結局は建物のセキュリティーだといわれています。どんなに強力なファイアウォールを立てたところで、コンピュータを盗まれたり破壊されたら元も子もないからです。歯学部や歯学部附属病院にはセキュリティーの塊である医療情報が山のようにあります。電子情報に限らず、紙情報なども含めて、私たちは情報というものにもう少し慎重な配慮をすべきではないでしょうか。

歯学部をパソコンウイルスから守るために

コンピュータウイルスについて

歯科補綴学第一講座　小　林　　博

1.　はじめに

今日、コンピュータウイルスという言葉を聞いたことがない方はいらっしゃらないと思います。新潟大学歯学部の中でも感染の被害が少なくありません。対岸の火事というわけにはいかなくなっています。ウイルスソフトを導入すれば安心かというと、ウイルス自体常に新種が作られていくために、古い版のソフトのままですと役に立たなくなっている場合があり、なんとも厄介です。ここでは基本的なウイルスの話と、現在流行している物をとりあげて、皆様の快適なコンピュータ環境を守る一助となるお話にまとめたいと考えています。

2.　おいたち

機械がウイルスに感染するということ自体おかしな話ですが、このウイルスは、昔（もう昔になってしまいました）プログラムを機械語で書いていた時代に、なんとかコンピュータの記憶装置上で増殖する生物もどきをプログラムで作ってみたいということに端を発しています。種々の機械（計算機）上でいろいろな実行プログラムが作られました。マイコン（microcomputer）（パソコンではありません）が普及しはじめた頃にはいかに短く“自己増殖”プログラムを書くかというコンテストが行われたこともありました。つまりこの頃は、単にプログラム技術の問題で、人に被害をおよぼすものではなかったわけです。

ところが、いたずら者がこの技術を利用してこっそりと、一般のプログラムのなかに自分の作った“虫”を入れることを始めたわけです。このころは技術力の誇示を目的としていた風潮があってあまり害が無いものが多く、洒落た文句が画面に出て被害者がにやっと笑えるようなものでした。これがエスカレートして多大な害を及ぼすものが出てきたわけです。

ここで覚えておいていただきたいことは、ウイルスがプログラムであるということです。計算機にかけてそのプログラムを動かさなければ、単なる情報（いわば紙に書いた文字）の集まりに過ぎません。うまく計算機上で動いて初めて、増殖なり感染なりなにか動作をすることが可能になります。昔は計算機の種類が違えばプログラムは動きませんでしたので、その間の感染はありえませんでした。またプログラムを他の計算機に移動する手段もフロッピーディスクなど限られたものしかありませんでしたので、それに気をつければ感染は防げました。

ところが、ソフトウエア技術と通信技術の発達で、事態は急展開をすることになったわけです。

3. 現　状

コンピュータ間通信特にインターネットが普及し、情報やプログラムが頻繁に短時間でコンピュター間を移動するようになったために、“ウイルス”の伝搬（感染）経路が多岐になり、スピードが非常に早くなりました。また、パーソナルコンピュータが普及しそれらが共通の基本ソフト（windows，マッキントッシュＯＳ）上で動くようになり、感染対象が以前に比べて非常に大きくなりました。経路、対象の両方の増大効果でウイルスの勢いが急激に盛んになりました（文末参考6-1)(1))。

ウイルスの種類を分類して説明するのも一面では興味ある事ですが､この原稿の主旨からすると、冗長となりますので、現在代表的なものを、感染手段別に、新潟大学で発見された例を挙げて説明いたします。従って分類としては、一般的な分類法ではありませんが分かり易いと思います。

1)　メール添付型（happy 99，MTX，Navidad，TROJ _ HYBRIS.D)

最近話題になるものはこれが多くなりました（参考6-1)(2)(3)(4))。電子メールの添付ファイルとして感染するものです。メール本文は基本的に（outlook の HTML メールなど例外もありますが）テキスト file（文字列のみ）ですので、メールを読んだだけで感染することはまずあり得ません(注意)。それに添付された file を実行して活動を開始します。知り合いから来た本文ナシ（あるいは非常に簡単な本文）のメールに添付された file をダブルクリック（実行）しただけで感染します。歯学部の中でも多数発見されました。

注意)（セキュリティホールを利用して HTML メールそのものがウイルスとして機能するものが発見されていますが、現在の OutlookExpress ではこのような HTML メールの表示による各種スクリプトの自動実行を防ぐセキュリティパッチが公開されています。6-5)(1))

2)　Java/ActiveX 型（JAVA _ TRIPLETRT）

比較的新しい感染方法です。インターネットのホームページを閲覧したときに、絵が動いたり音がでたりする華やかな頁をご覧になったことがあると思います。このようなことを実現する方法はいくつかありますが、そのなかで接続したあなたのコンピュータを動かして実現させる方法が開発されています。いわば知らないうちにむこうのホームページに自分のコンピュータが躍らされているわけです。単にきれいなら良いのですが、悪意のある頁には罠が仕掛けられていて、知らないうちにウイルスを感染実行させられることがあります。特にアダルトサイトや、ハッカーが集まるサイトに多いようです。

3)　マクロ型

いわゆるプログラムでなくて、ワープロソフトの文書ファイルなどに付加できるもので、操作手順実行手続きを記録して実行できるようにしたものをマクロと呼びます。これも実行可能（コンピュータに動作を命令できる）なファイルであるために、ウイルスを記述することかできます。この型は、コンピュータの種類を選びません。同じワープロソフトが動けば windows であろうが、マッキントッシュであろうが感染します。Melissa（MicrosoftWord）や Laroux（Excel）が有名です。

4)　ダウンロード型

トロイの木馬のように、何か良いものの見せかけをもっていて、実は内部にウイルスが仕組まれています。プログラムをダウンロード（外部から自分のコンピュータに取り込むこと）して実行すると感染します。この中にはダイヤルＱ２に自動的に電話をかけて、ダイヤルアップ接続をしてしまい、法外な電話料金を請求されて初めて気がつくようなものがあります(参考6-5)(2))。

5)　旧来型（CIH，Cascade）

最近はあまり騒がれませんが、忘れてはいけません。フロッピーディスクなどを介して感染します。この種類のものは、歴史が古いためによく作りこまれていて、発見されにくくするために自己変形したり、感染場所もシステム領域など発見し

にくい場所に感染するものがあります。実行 file に感染するもの(Cascade)が多いため、発見が遅れるとよく使用される file にすべて感染が広がってしまう場合があります。

6) デマ型（ウイルスではありません）

http://www.ipa.go.jp/security/topics/virus_hoax.html

ウイルスではないのですが、あっという間に広がりますので、ご注意ください。実態は実在しないウイルス情報をメールを介して不特定多数の人にばらまくことです。受取った人は善意でその情報を知り合いに知らせるということがおこり、不幸の手紙の電子メール版になるわけです。特にメーリングリストを介して多数の人に伝わって短時間に世界に広がるケースが増えています。自分が確認していない情報（伝聞情報）は流さないように気をつけましょう。

7) 迷惑メール（スパムメール）

これは、鈴木先生の担当に入るかもしれませんが、ダイレクトメールのように、不特定多数のひとにコンピュータで大量のメールを送りつける事をいいます。受け手としては最初は、防ぎようがありませんが、繰り返し同じ所から来るような場合には、設定によって受取りを拒否できます。コンピュータ利用者の立場からできることは、ウイルスに感染した機械を使用したり、パスワードを盗まれたりしてスパムメール発信の手助けをしないことです。

4. 被害

被害の主なものを分類してみます。

(1) ウイルス付きメール発信

ウイルスのなかで、感染した計算機から勝手にウイルス付きメールを持ち主の名前で発信するものが目立つようになりました。このために知り合いから来たメールを送り主の名前だけで信用してはいけなくなりました。(happy 99，MTX，Navidad)

(2) 裏口作成（MTX，QAZ）

悪さの中で気がつきにくく、困るものがこの形です。感染したウイルスが計算機の中に裏口を作っていしまいます。この裏口を利用して、ウイルスを発信した人は感染した計算機に入り込み、自由に閲覧操作出来るようできます(QAZ)。知らないうちに、他人に、自分の計算機の中がのぞかれ、勝手に操作されてしまうのです。大事なパスワードを盗まれたり、コンピュータ自体が、犯罪に踏み台のようなかたちで利用されたりします。

(3) 破壊

以前からよくあるものが、ハードディスクに対する書き込みです。大事なプログラムやデータに被害が及びます。最悪の場合ハードディスク全体が読み書きできなくなります。さらに悪質なものは、BIOS とよばれるコンピュータ起動のためのデータを書き換え、コンピュータ自体を起動不能（CIH）にしてしまうものも存在します。

5. 対策

ウイルスソフトも頼りっきりにできないとなるとどうしたらいいでしょうか。

1) 大事なものは複製を別な所にしまう。

電子媒体の便利な所は、簡単に複製ができることです。この特徴を生かして別な場所にしまっておきましょう。データや原稿など再生不可能なものは一ヶ所のハードディスクに入れておくだけでは取り返しがつかなくなります。ウイルスでなくともハードディスクはいつか（あなたが一番必要としているときに）壊れます。

最近のシステムは大きなハードディスクを必要としますが、大切なものはそれほど多くないはずです。どんなに高価でも、システムやアプリケーションは再インストールできます。あなたの作った文書類は世界中に一つしかありません。それだけであれば、画像 file を除けば、CDROM か MO 一枚で十分でしょう。

2) 知らない郵便物は開封しない。

現在はこのルートが一番多い (6-1)(4)) のでメールの添付ファイルには十分気をつけましょう。知人からの手紙でも、本文が無かったり本人の書

きそうもないものであれば、添付ファイルは読まずに本人に確認することが必要です。

3) 怪しげな所に行くときには防備を固めて、自分の責任で。前に書きましたようにインターネットのサイトも安心して覗けません。とくにいかがわしいサイトはお気をつけてください。ブラウザーの設定（6-5)(3)）でjavaなどスクリプトを実行できないような設定が可能です。またファイルの共有設定も変更できますので、なるべく共有設定は外した状態にしておきましょう。とくに学生用等、不特定多数の人が使用する計算機では、あやしいサイトには近づかないでください。何も知らない次の使用者に対して、あなたが加害者となってしまいます。

4) 定期健康診断を

もちろん、きちんと更新して最新のデータがあればウイルスソフトは有効です。時々ウイルス検査をしてみましょう。潜伏期間中で発病前で、特定のきっかけで活動しだすウイルスが見つかるかもしれません。発症する前に把握駆除できれば被害は最小限にとどまります。しかし、最新のウイルス情報を自分で維持するのは大変です。最新のウイルス情報を教えてくれたり、自分のコンピュータを、オンラインでスキャンできるサイト（6-4)）がありますのでこれらが便利かと思います。

5) 病状の記録

ウイルスに感染したら、どういう状態であるかを記録しておきましょう。特にfileの名前やメールの題名は手がかりになります。感染したウイルスの種類が分かると、駆除の手間も少なくなります。

6) 感染したら、報告を

基本的に大学の情報処理センターへ。

(1) 新潟大学総合情報処理センター
〒950-2181 新潟市五十嵐2の町8050番地
TEL：(025)262-6230
FAX：(025)262-6232
E-Mail:www-admin@cc.niigata-u.ac.jp

(2) 情報処理振興事業協会 セキュリティセンター
〒113-6591 東京都文京区本駒込２－28－８
TEL 03-5978-7509 FAX 03-5978-7518
E-mail virus@ipa.go.jp

6. 参考資料

1) 2000年ウイルス発見届出状況（情報処理振興事業協会セキュリティセンターより）
http://www.ipa.go.jp/security/topics/2000sum.html

(1) 感染実害の割合

	1998年		1999年		2000年	
感染被害	1619件	79.6%	1953件	53.6%	2182件	19.6%
発見のみ	416件	20.4%	1692件	46.4%	8927件	80.4%
届出合計	2035件		3645件		11109件	

(2) メール悪用ウイルス

ウイルスのタイプ	1998年		1999年		2000年	
メール悪用ウイルス	0件	0%	1197件	32.6%	7288件	65.5%
その他のウイルス	2072件	100%	2478件	67.4%	3832件	34.5%
全体合計	2072件		3675件		11120件	

(3) 届出ウイルス名称

ウイルス名称	1999年	2000年
* W 32/MTX	—	2136件
* VBS/LOVELETTER	—	1221件
* W 32/Navidad	—	1202件
XM/Laroux	998件	1041件
* W 32/Ska(Happy 99)	992件	683件
* W 32/PrettyPark	121件	569件
X 97M/Divi	—	541件
* Wscript/KakWorm	—	507件
* VBS/Stages	—	414件
W 97M/Marker	116件	343件
*その他メール悪用	84件	556件
その他上記以外	1364件	1907件
全体合計	3675件	11120件

注） *印は、メール悪用ウイルスを示す。

(4) ウイルス感染経路

感染経路	1998年	1999年	2000年
メール(海外含)	826件 40.6%	2443件 67.0%	10014件 90.1%
ダウンロード	77件 3.8%	195件 5.3%	82件 0.7%
外部媒体(海外含)	700件 34.4%	611件 16.8%	428件 3.9%
不　明	432件 21.2%	396件 10.9%	585件 5.3%
全体合計	2035件	3645件	11109件

2) 心得（情報処理振興事業協会セキュリティセンター)

(1) メールの添付ファイルの取り扱い5つの心得

http://www.ipa.go.jp/security/antivirus/attach5.html

1. 見知らぬ相手先から届いた添付ファイル付きのメールは厳重注意する
2. 添付ファイルの見た目に惑わされない
3. 知り合いから届いたどことなく変な添付ファイル付きのメールは疑ってかかる
4. メールの本文でまかなえるようなものをテキスト形式等のファイルで添付しない
5. 各メーラー特有の添付ファイルの取り扱いに注意する

(2) パソコン・ユーザのためのウイルス対策7箇条

1. 最新のワクチンソフトを活用すること
2. 万一のウイルス被害に備えるためデータのバックアップを行うこと
3. ウイルスの兆候を見逃さず、ウイルス感染の可能性が考えられる場合ウイルス検査を行うこと
4. メールの添付ファイルはウイルス検査後開くこと
5. ウイルス感染の可能性のあるファイルを扱う時は、マクロ機能の自動実行は行わないこと
6. 外部から持ち込まれたＦＤ及ダウンロードしたファイルはウイルス検査後使用すること
7. コンピュータの共同利用時の管理を徹底すること

3) ウイルスの簡単な説明

Cascade（1701）（カスケード（1701））

常駐型でCOMファイルに感染する。発症時は画面上の文字を滝のように落とす。

CIH（W 32/CIH）

常駐型でWindows 95/98の32ビット実行形式ファイル（PEファイル、拡張子がEXE）に感染する。発病するとハードディスクの先頭部分を無意味なデータで上書きするため、ディスク内容にアクセスできなくなる。また、チップセットが、インテル430 TX互換の場合には、BIOS ROMのブートブロックを破壊し、起動不能にする。4月26日発病、6月26日発病等の種類がある。

Happy 99（W 32/Ska）

Skaとも言われ、トロイの木馬の一種である。このウイルスは、通常、電子メールやニュースグループ上の添付ファイルとして拡がっていく。電子メールの場合、「Happy 99.exe」というファイルだけが添付されたメールが届く。このファイルを実行すると「Happy New Year 1999」というタイトルの花火の画像が表示され、「WSOCK 32、DLL」の一部を書き換える。感染後電子メール（またはニュース）を送ると、そのメッセージと同じ宛て先、同じ件名のメールをコピーして、「Happy 99.exe」を添付して送信する。

JAVA＿TRIPLETRT（TripleTrt，TripleThreat)

Java appletを悪用したインターネットウイルスで、ユーザーの使用しているWindowsを大きく黒く塗りつぶし 、恐ろしい音を出す。

Laroux（ExcelMacro/Laroux）

マイクロソフト社のExcel（以下MS Excel）で動作するウイルスで、感染したExcel文書ファイルをオープンすると「PERSONAL.XLS」という名称のファイルを作成し、ウイルスのマクロ（非

表示設定）を登録する。「PERSONAL.XLS」はMS Excel起動時に読み込まれlaroux マクロが実行されて使用したMS Excelデータファイルにlaroux マクロを追加し、感染する。このウイルスは発病しない。

Melissa（Word 97Macro/Melissa）

マイクロソフト社のWord（以下MS Word）を介して感染するウイルスで、ウイルスに感染した文書ファイルを読み込むとそのMSWordに感染する。そして感染したMS Wordで作成、更新した文書ファイルに感染する。また、Outlookのアドレス帳に登録されているメールアドレス50カ所に対して、ウイルスに感染した文書を添付したメールを送信する。

MTX（W 32/MTX，I－WORM.MTX，MATRIX，PE＿MTX.A，TROJ＿MTX.A，TROJ＿MTX.B，TROJ＿MTX.C，TROJ＿MTX.D，W 32/APOLOGY＿B）

ワーム部分とハッキングツール部分がある。ワーム部分はE-Mailを通じて自分のコピーをばら撒く能力を持つ。感染により、E-Mailが送信されると同時にウイルスファイルを添付した空のメールを同じ宛て先に送信する。Happy 99と同様の方法である。メールに添付されるファイルのファイル名はいくつかの中からシステム日付の条件を元に決められ、また特定の文字列を含むURLへのネットワークアクセスを妨害する。

NAVIDAD（TROJ＿NAVIDAD.A，W 32.Navidad，W 32/Navidad@M）

ワームに分類されるトロイの木馬型不正プログラム。自身を“NAVIDAD.EXE”のファイル名でメールにコピーを添付して送信し、自己増殖する能力を持っている。他のファイルへの感染活動は行わない。別ファイル名でも動作しますので注意が必要。単純な除去によっては、exeファイルが使用できなくなることがある。

QAZ（TROJ＿QAZ.A，NOTEPAD.TROJAN，QAZ.TROJAN，W 32.HLLW.QAZ.A）

トロイの木馬型（ハッキングツール）。遭遇の可能性は高い。破壊活動としては、ファイルを作成と、システム改変（裏口から操作する）がある。

4） 有用なウイルス関連サイト

◎ウイルスバスターOnline Scanトレンドマイクロ社
http://www.trendmicro.co.jp/hcall/scan.htm

［主なワクチンベンダー］（五十音順） （IPA届出に基づく）

◎株式会社アラジンジャパン
http://www.aladdin.co.jp

◎コンピュータアソシエイツ株式会社
http://www.caj.co.jp/

◎株式会社シマンテック
http://www.symantec.com/region/jp/

◎株式会社シー・エス・イー
http://www.cseltd.co.jp/security/

◎トレンドマイクロ株式会社
http://www.trendmicro.co.jp/

◎日本ネットワークアソシエイツ株式会社
http://www.nai.com/japan/

◎株式会社バーテックスリンク
http://www.vertexlink.co.jp/index2.html

◎株式会社山田洋行
http://www.fs－support.yamada.co.jp/df/index.html

［日本のサイト］

◎ ENC電子ネットワーク協議会
（Electronic Network Consortium）
http://www.enc.or.jp/

◎ IPA情報処理振興協会
（TheInformation－technology Promotion Agency， Japan）
http://www.ipa.go.jp/

◎ JAIPA日本インターネットプロバイダー協会
（Japan Internet Providers Association）
http://www.jaipa.org/

◎ JPCERT/CCコンピュータ緊急対応センター
（Japan Computer Emergency Pesponse Team）

http://www.jpcert.or.jp/

◎ VCON ウイルスコンサルティングセンター
(Virus Consulting Center)
http://www.vcon.dekyo.or.jp/

◎警察庁　http://www.nepa.go.jp/

◎郵政省　http://www.mpt.go.jp/

［海外のサイト］

◎ CERT
(Computer Emergency Pesponse Team)
http://www.cert.org/

◎ EICAR
(Europian Insritute for Computer Anti-Virus Reserch)
http://www.eicar.com/

◎ ICSA
(International Computer Security Association)
http://www.icsa.net/

◎ Virus Bulletin
http://www.virusbtn.com/

◎ハンブルグ大学 VTC (Virus Test Center)
http://agn-www.informatik.uni-hamburg.de/vtc/

5）　そのほか

(1) Outlook Express セキュリティ情報（microsoft 社より）
MS00-043　「改ざんされた電子メール ヘッダ」の脆弱性に対する対策　00/12/07
MS00-045　「メールとブラウザがリンクしつづけてしまう」脆弱性に対する対策 00/12/01
MS00-046　「キャッシュ バイパス」の脆弱性に対する対策　00/09/07
MS99-060　「HTML メール添付ファイル」の脆弱性に対する対策　99/12/24

(2) 「国際電話番号・ダイヤルQ 2 検知ソフト＝ダイヤルアップチェッカー」
http://www.kddi.com/topics/atx/image.html

(3) ブラウザの設定等に関して「ブラウザの設定例」
http://www.ipa.go.jp/security/ciadr/browser.html

「歯学部ネットワーク・コンピューター勉強会」設立

去る 2 月23日に本学総合情報処理センターの滝沢先生を招いて第 1 回勉強会が開催された。学部外からも数名の参加があり盛況であった。**滝沢先生**からは、SINET レベルからサーバー・個人レベルに至るまでのセキュリーティの考え方と対策について具体的な説明および提案があった。なかでも、「古いパソコンがセキュリティホールになる」というお話は、個人持ちの PC も LAN の安全のために定期的に更新する必要があるということで、「水と安全はただ」と思いこんでいるわれわれには耳の痛い話であった。


滝沢先生

また、この機会を利用して、「歯学部・歯病内でネットワークやコンピュータに関する勉強会を立ち上げたい」という希望を常々持っていた世話人の**鈴木先生**（口腔外科 1 ）にその経緯などについてうかがった。

そもそもの設立の動機はなんですか？

―学内のネットワークセキュリティ対策の一環としてのユーザ教育だったのですが、一挙に意識/知識レベルの異なる学部・病院内の全ユーザを

対象とすることは無理がありますので、まず、管理者レベルあるいはコンピュータやネットワークのアクティブなユーザを対象に勉強会行うことを考えました。

確かに、昨今の急速な技術進歩は「IT 革命」の異名を取るほどで、なかなかフォローが難しいようですが？

―コンピュータやネットワーク技術の中には我々の教育・研究・診療に有用な技術やアプリケーションが数多くあると考えられますが、これらの技術は dog year といわれるほど急速な進歩をとげ、個人レベルで進歩に追随するのは大変困難な状況となっています。

そこで、ネットワークセキュリティーに限らず、広くネットワークやコンピュータについて定期的に勉強会を開催してはどうかと考えました。

具体的なテーマとしては、どのような事を取り上げる予定ですか？

―そうですね、たとえば、

1. キャンパスネットワークのセキュリティーについて
2. 新しいキャンパスネットワークについて
3. インターネットの最新動向
4. セキュリティーを中心にした電子メール・Web 活用法
5. プレゼンテーション Tips
6. パソコン技術の最新動向
7. コンピュータネットワークの法的問題について
8. 病院医療情報システムについて
9. UNIX の基礎

などを考えています。

勉強会は具体的にどのような会員から構成されているのですか？

鈴木先生

―大島先生（口腔解剖 2）とわたくしが世話人となって、当初は歯学部・歯病内のコンピュータ/ネットワークのアクティブユーザ10数名程度を中心にして発足させましたが、希望者なら誰でも参加歓迎です。

今後の活動計画について教えてください。

―勉強会は毎月あるいは隔月の決まった曜日・時間で、一回 2 時間程度としています。夕方になると思います。講師は情報処理センター、工学部、法学部、学外の方に広くお願いする予定です。

また、テーマによっては一般向けとして、他のものも公開でもよいと思いますが、広く学部・病院に広報して行ってはどうかと考えています。

インタビューを終えて、このような活動がトップダウンによる命令形式ではなく、一部のボランティアを中心に上下一体となった「草の根」的な運動から生み出されてきたというのに意義があると感動すら覚えた。また、新潟大学歯学部のコンピューターネットワークは全国の歯学部のなかでもさきがけとなったもので、現在でもその充実度は高い評価を得ているが、それを維持し発展させていくためにはこのような日々の努力も大切なのだと痛感した。（か）