ネットワークセキュリティとは

総合情報処理センター
鶴　正人
tsuru@net.nagasaki-u.ac.jp

1　本特集について

「セキュリティ(セキュリティ管理)」は、広く、自然災害／物理的故障／人的過失／犯罪などの脅威に対して、安全を確保し、危機を管理する、という意味で使われるが、中でも、最近、「コンピュータセキュリティ」、「情報セキュリティ」、「ネットワークセキュリティ」という言葉をよく耳にする。ニュアンスとしては、「コンピュータセキュリティ」は、計算機の利用／運用に関するセキュリティを広く一般的に指し、「情報セキュリティ」は、「価値の高い情報を守る」、という見方からのセキュリティで、狭義には、暗号化、改竄防止、認証などの技術を用いた情報保全を指す場合が多い。

さて、「ネットワークセキュリティ」とは、それらの中で、特に計算機のネットワーク化によって重要／深刻になってきた問題を指すものだと考えられる[†1]。「インターネット」の爆発的普及に伴い、「ネットワークセキュリティ」の重要性はますます高まっている。

インターネットは、国境を越えて世界につながっており、研究や教育やビジネスにも、そして事故や犯罪にも新しいチャンスを与えうる、可能性と危険とが混在する未知の仮想社会と言える。しかも、現状では、「利用者」が「セキュリティ」に対する認識が希薄なままにインターネットにつながった計算機を使っていることがままある。車の運転に例えると、道路標識の見方とか、ナンバープレートの重要性とか、飲酒運転の危険性というような「常識」を知らないままの無免許ドライバが、公道に出てきていることに相当し、本人も周りの人も非常に危険である。さらに、当り屋には気をつけろとか、キーを掛けずに車を離れると盗まれる(さらには盗まれた車は犯罪に使われて社会に迷惑を懸ける)ので注意しろ、というような認識も必要になる。日本は、インターネットの歴史が浅く、また元々平和(?)なせいか、特にネットワークセキュリティに対する認識が甘いと言われている。

しかし、車は危険だから使うな、ということが現実解にならないのと同様に、ネットワークは怖いから使わない、というのは非現実的である。ネットワークを活用することの重要性は今後も増えることはあっても、減ることはない。ネットワークのリスクを認識した上で、それを安全に使いこなす常識を持ち、そして実践すれば、怖がることはないと思われる。

そこで、本特集は、ネットワークに接続された計算機(パソコンやサーバ)を使っている方々に、現時点での基本的な情報や常識を提供し、是非一度「ネットワークセキュリティ」について考える機会を持って欲しいという願いから企画された。全体構成は、表1のようになり、本稿(1)及び(2)で、ネットワークセキュリティの概要を述べた後、重要なトピックスに関して、学内の利用者の方からの寄稿を中心に記事を並べた。トピックスの(3)と(4)は、パソコンのウイルスの話である。ネットワークが普及する以前からあった問題／脅威であるが、最近ますます増えている。(5)は、安全な遠隔ログインのためのSSHというツールの勧めである。特にインターネットを経由してログインする場合、古典的なtelnetなどに代って暗号化や安全な認証の機能を持つツールを使用することは、世間では常識になりつつある。(6)は、電子メールを安全に使うための電子署名や暗号化の話である。電子メール

[†1] 過去の詳しい解析は、http://www.cert.org/research/JHThesis/Start.html など参照。

は電話やFAXに取って代わる勢いで普及したが、悪意のプログラム付きのメール、にせメール、盗聴や改竄などの危険を知らずに使っている人も見受けられる。(7)は、最近世間でブームになり、学内でも利用者が増えてきた、安価なハードウェア(PC/AT互換機)上で動作するUNIX(特にその代表格であるLinux)を運用する人への注意である。いままでDOSやWindowsの世界に居た人がUNIXの奥の深い便利さや面白さに魅せられて使い始める場合、潜在的に強力なサーバ機能を忘れてセキュリティへの注意を怠るのは大きな危険を孕んでいる。(8)は、一般にサーバ機能を持つ計算機の運用における基本的問題を述べ、サーバ管理者がワッチすべき情報へのポインタを示している。

表1: 本特集の構成

(1)	ネットワークセキュリティとは	– 本稿
(2)	初心者のためのセキュリティー講座	– JPCERT/CC
	(パスワードについて心がけてほしいこと)	
	(電子メールの安全性に関する基本的な知識を身に付ける)	
	(自ら負うべきさまざまなリスクについて)	
	(ソフトウェアのバグとセキュリティ)	
(3)	Windowsとウイルスの話	– 藤田 渉(経済学部)
(4)	マウスはお病気 ~ Macとウイルスの話	– 宮西 隆幸(環境科学部)
(5)	安全なリモートアクセス	– 池永 全志(総合情報処理センタ)
(6)	メールにおける信頼性	– 鈴木 斉(経済学部)
(7)	Linuxユーザのためのネットワークセキュリティ	– 桃木 悟・古賀 掲維(工学部)
(8)	サーバ管理者のためのセキュリティ	– 鶴 正人(総合情報処理センタ)

ただし、網羅的に話題をカバーしているわけでもなく、特に、技術や原理、社会や法律との関係、歴史や将来の動向などはあまり触れることができなかった[†2]。計算機やネットワークは、技術及びそれを取り巻く社会状況がどんどん変っている。セキュリティの問題にしても、今後も新しい脅威とそれに対抗する技術や制度が次々現れるだろう。基本的な考え方は本特集で説明されていることと大きくは変らないと思うが、具体的なノウハウは常に変化するので、最新の情報に基づいて自分の身を守っていく必要がある。インターネット上で利用できるup-to-dateな情報を参照して欲しい[†3]。

なお、「ネットワーク利用者に最低限知っていて欲しい」ことには、他に、「モラル」、「エチケット(ネチケット)」や「プライバシ」といった事項もある。技術的には「セキュリティ」とオーバラップする部分も多いが、話としては別の視点から論じられる。それらについても、上記のインターネット上で利用できる(ただし信用できそうなサイトの)情報を参照して欲しい。

2 各個人が知っておくべきこと

自分の計算機をネットワークに接続したとたんに、通信可能なすべての相手からの、悪戯や悪意の攻撃にさらされる危険が生じる。また、他人に迷惑をかける危険も生じる。特にそのネットワークがインターネットとつながっている場合は、全世界からの脅威/全世界への悪影響の可能性がある。悪意を持って攻撃してくる相手のことを、クラッカ(cracker)や侵入者(intruder)などと呼ぶ[†4]

ネットワークは音も立てないし臭いもしないので、その中にどういう通信が通っているかは普段は気にも止めない。メールが読めなくなったり、WWWページが見えなくなった時にだけ、その存在

[†2] なお公開鍵暗号の原理については、本レポートのもう一つの特集「新しい情報教育を目指して」の中の工藤先生(工学部)の記事で触れられている。

[†3] `http://www.nagasaki-u.ac.jp/internet/internet-jis.html` からリンクを辿ることができる。

[†4] ハッカ(hacker)と呼ぶこともあり、多くのマスコミでもそう呼んでいるが、正しくは"hacker"は高度な技術を持ったマニアのことを指すので、"悪意を持つ"場合は、crackerやintruderを使うべきである。

(というより不在) に気づく。しかし、学外と長崎大学との間には、一日に片方向で 10 ギガバイト以上のデータが流れている。この中には全世界 (もちろん国内も) のクラッカたちから長崎大学への無差別あるいは特定の計算機への攻撃が含まれている。

仮に自分の計算機は、信用できる範囲としか通信できないような設定になっていたとしても、その「信用できる」ネットワークの中の計算機の一台でも「信用できない」ネットワークとつながっていれば、そこが破られて攻撃される可能性がある。つまり、完全に孤立したネットワークでない限り、危険は避けられない。よって、大原則は 以下の 3 点である。

- 他人に見られたら困る情報は、そういうネットワークにつながった計算機上には置かない。
- 消失したら困る情報は、安全な場所へ複製 (バックアップ) を持つ。
- 自分の計算機をネットワークにつなげる以上は、利用妨害、プライバシ侵害、犯罪への利用 (踏台) などの **"間接的加害者"** にならないためにも、セキュリティ対策の努力は社会的要請である。

もう一つ本質的に重要なことは、一般に、利便性とセキュリティは相反するという点である。例えば、家には鍵を掛けない方が、鍵を持ち歩かなくてもいいので便利である。しかし、だからと言って、外出の時に家の鍵を掛けない人はいないだろう。逆に、何重にも鍵を付けると、開け閉めが大変である[†5] 。計算機ネットワークの利便性には、コミュニケーションや情報発信、資源の共有、遠隔利用などいろいろな面があるが、それらはすべて何らかの危険と隣り合わせている。利便性を単純に追求すると危険性が増すし、また、利便性と安全性を両立させようとするとハード／ソフト／管理 (人) のコストが増すことを認識しておく必要がある。

利便性	セキュリティ確保のために必要なこと
コミュニケーションや情報発信	情報の信用度のチェック。
資源の共有や遠隔利用	アクセス制限 (定めた範囲でのみ利用できる仕組み) の徹底。

さて、ネットワークセキュリティ上の脅威の急増に対抗するために、IPA [†6] 内に、1997 年に「セキュリティセンター」が設立された[†7] 。その組織には、ウイルス対策室、不正アクセス対策室、暗号技術調査室があるが、この観点に立つと、ネットワーク上の脅威 (攻撃方法) の代表的なものには 3 つの種類 (互いに密接に関係した) があると言える。

- 悪意のプログラム (malicious program)
- ネットワーク経由の不正アクセス
- 通信の盗聴、改竄、なりすまし

これら以外に、もっと人間寄りの直接的な攻撃として、**詐欺**や**デマ**や**中傷**などがある。例えば、電子メールや電子ニュース、あるいは WWW ページを使ったネズミ講[†8] や詐欺 (知らない間に国際電話をかけていて多額の請求が来た等々) の被害が多数出ていることはご存じの通りである。

さて、"攻撃" を成功させてしまう原因には、以下のようなものがある。

- 利用者が騙される場合。一般に、情報が信用できるのかどうかを判断する常識や知識、そして何より、"知ってはいたけどうっかり騙された" ということを防ぐための注意深さが必要である。

[†5] 一方、鍵の掛っていない家を見つけた時に勝手に入ってもいいのか？、というモラルの問題も存在する。

[†6] 通産省系の政府関係機関である情報処理振興事業協会。

[†7] **http://www.ipa.go.jp/SECURITY/index-j.html**

[†8] **http://www.npa.go.jp/koho/nezumiko.htm**

- 利用者が使い方や設定を間違って (うっかりの場合や元々無知の場合など) 無防備な状態になってしまう場合。先に述べたように利便性とセキュリティは相反するので、多くのプログラムは場合／状況に応じて最適な選択ができるように、これらの匙加減は、利用者が設定するようになっている。当然、どんなセキュリティ機能の高いプログラムを使っていても、設定を間違ったら、非常に危険である。
- 使っているプログラムのバグを悪用される場合。このようなバグを一般に“セキュリティホール”と呼ぶ。ご存じのように、大規模プログラムの場合、バグがないものはほとんどあり得ない。“プログラム”を使う以上、それには“セキュリティホール”が内在し、いつかは発見されると思った方がいい。これに対しては、こまめに、“セキュリティホール”の情報をワッチし、危険が判明したプログラムは使わない、迅速に修正版 (パッチとか bug fix とかサービスパックとか呼ぶ) に変更する必要がある。
- 開放型のネットワークの性格上、原理的に避けることが困難な場合。例えば、盗聴は避けられないとしたら、中身を暗号化する、などの対策をするしかない。

セキュリティを維持するには、日頃から最新の情報に注意し、その予防策を継続的に実践していくという覚悟と習慣が、最も重要である。防犯／防災と同じで油断が大敵なのである。

2.1 悪意のプログラム

“悪意のプログラム”には、ウイルス、ワーム、トロイの木馬、などいろいろな種類があり、微妙に意味が異なるが、一方、排他的な定義でもない。

ウイルスとは、他の（通常の）プログラムに寄生／伝染するプログラム (の断片) を指すことが多い。感染したプログラムを「実行」すると、何かの悪さをするだけでなく、他のプログラムを書換え、その中に自身をコピーして伝染していく。

ある計算機に最初にそのウイルスがやってくるのは、人間が（そうとは知らずに）ある感染したプログラムを外部から持ち込んでインストールした時である。以前は、他の計算機で使っていたフロッピーディスク内のプログラムから感染する場合が主であったが、その後、インターネットの普及に伴い、電子メールに添付されたプログラムや、WWW/FTP サイトからダウンロードしたプログラムからの感染が急増している。

ワームとは、ネットワークを介して他の計算機にも自分のコピーを送りつけ、虫 (worm) のようにネットワーク上を動き回るプログラムを指す。(半) 自動的に他の計算機への転移を試みるので、成功する場合には、ウイルスに比べて広まる速度が早い。

なお、悪意を持たないもの (例えば、最近流行りのモーバイルエージェントはワームの一種とも言える) を含んでそう呼ぶ場合がある。

トロイの木馬とは、一見悪意のないプログラムのような振りをして、利用者が間違ってそのプログラムを利用してしまうことを誘い、利用してしまった時には何かの悪さを行うような、罠が仕掛けられたプログラムを指す。

トロイの木馬が持ち込まれる時は、ウイルス同様、媒介として、フロッピーディスク、プログラム添付電子メール、インターネットからのダウンロードなどが使われるが、場合によっては“不正アクセス”によって、クラッカが直接的に送り込んでくる／置いて帰ることもある。

これらは、特にパソコン系の OS(Windows, Macintosh など) で脅威になる。それらの OS では一般利用者の実行したプログラムでもシステムを書換えてしまう (感染させる、壊す、改竄する) ことができるからである。本特集の“Windows とウイルスの話”及び“Mac とウイルスの話”参照。

それに比べてUNIXのような、マルチユーザを前提としたOSでは、一般利用者の実行したプログラムは、原則的には自分の所有するファイルしか書換えることができないので、システム機能に悪さをしたり、他人のファイルを壊したりするような直接的な危険は少い[†9]

しかし、いずれにせよ、大きな脅威であることには変りない。例えば、画面上に、「接続が切れました。あなたのパスワードをもう一度入力して下さい。」というメッセージとパスワード入力欄を表示するような“トロイの木馬”がある。うっかり騙されて自分のログインパスワードを入力すると、その内容は自動的に電子メールなどに乗せてそれを仕掛けたクラッカの元へと送られる。こうして盗まれたログインパスワードは不正侵入に使われる。あるいは、システム管理者(root)が騙される危険もある。例えば、UNIXにおいて、`/tmp`ディレクトリに、`ls`という最も頻繁に使われるコマンドと同名の“トロイの木馬”を仕掛ける手口がある。rootが`/tmp`ディレクトリに`cd`し、`ls`した時、場合によっては非常に危険であることは想像できるだろう[†10]。

また、WWWページにアクセスした時に、Java(applet)、Javaスクリプト、Active-X、VBスクリプトなどのいわゆるネットワークローダブルオブジェクトが自動的にダウンロードされてきてWWWブラウザ上で実行される場合がよくある。これらは、“ネットワーク”経由でやって来たプログラムを、中身を知らずに(知らされずに)自分の計算機で実行するわけなので、WWWブラウザには、一般にそれなりのフェールセーフなアクセス制限に仕組みが入っているが、実はピンからキリまであり、使う人の設定次第では非常に危険な状態になり得る。また、Java appletのような、比較的(Active-Xなどに比べると)セキュリティに配慮した仕組みの場合でも、それを実行するブラウザのバグ(セキュリティホール)によって危険な状態になることが今までもしばしばあった。

対策:

“悪意のプログラム”の実行を防ぐには、「怪しいプログラムは実行しない」、「外部から持ち込んだプログラムは必ず改竄チェックやウイルスチェックをする」が基本である。また、通産省告示として「コンピュータウイルス対策基準」が作られており、先に述べたIPAのセキュリティセンターのページから見ることができる。

最近、ネットワーク経由で「トロイの木馬」を持ち込んで被害に会う例が増えている。知らない相手からのメール(差出人は偽装できるのでFrom: 行がもっともらしくても安全とは限らない)に添付されたプログラムや、あやしげなWWW/FTPサイトからダウンロードしたファイルを、不用意に「自己解凍(実行)」してはいけない。ここでいう、プログラムには、WordやExcel用の「マクロ」や、VBスクリプトなども含む。

よくある手口は、ゲームやポルノを連想させる名前にしておき、起動を誘うというものである。あるいは、最近の実例で、「マイクロソフト社のInternet Explorerにバグが見つかったのでその無償のアップグレードをお送りします」、という電子メールが送られてきて、添付されたプログラムを解凍すると悪意のプログラムが実行される、という手口のトロイの木馬があった[†11]。

特に危険なのは、Windows上などでメールを読む時に、添付されたWordなどのマクロを自動で実行してしまうような設定にしている場合である。すぐに設定を変更すべきである。

また、UNIXのような共用計算機の場合の(自分の)ファイル/ディレクトリのアクセス権の厳しい設定は、一般には有用で、他人からの防御にはなるが、自分が騙されて実行するトロイの木馬には

[†9] ただし、一般にファイル/ディレクトリのアクセス権の設定が不適切だとパソコン同様に危険である。また、“rootにsetuidされたプログラム”のような例外もあり、クラッカの執拗な攻略対象になっている。

[†10] コマンドサーチパスにカレントディレクトリを含めることは一般に危険であるということは常識になっているが、ベンダ提供の標準環境では危険な状態のままになっていることがあるので、注意が必要である。

[†11] `http://www.cert.org/advisories/CA-99-02-Trojan-Horses.html`

無力である。

一方、このような悪意のプログラムの脅威を逆手にとった悪戯 ("偽ウイルス情報") も後を絶たない[†12]。典型的には、以下のような内容のメールがチェーンメールとして広まる。

1. 何々というタイトルのメールを受取ったら、それを読む前に消さないといけない。読んでしまうと、あなたのファイルの中身は消えてしまう。
2. これは緊急の事件なので、あなたの知っている人全員にすぐこのメールを転送しなさい。

まず、原理的にメールを読んだだけでファイルが消えることはない。ただし、読むと画面が乱れたり、変な状態になってしまったり、特定のプログラムが起動されたり[†13]することはあり得る。先に述べたように、添付されているマクロを読むだけで自動で「実行」してしまうような危険な設定で使っているならば、もちろん何でも起り得る。

次に、この「無差別に連絡のメールを送れ」という指示には一般には従うべきではない。皆が無差別に送ると、メールの嵐になるので、(仮にこのウイルス情報が本当でも) しかるべき安全／効率的なルートで情報を広めるべきである。

2.2 ネットワーク経由の不正アクセス

"不正アクセス" にもいろいろなレベル／種類がある。

不正な遠隔ログインは、クラッカから計算機に「侵入 (遠隔ログイン)」されることである。通常、侵入には誰かのログインパスワードが必要であり、それを何らかの手段で得ようとして、クラッカはいろいろな手口を講じる。その手口は必ずしも計算機やネットワーク上の活動とは限らない。ある計算機の利用者に、その計算機の管理者を名乗って電話をかけ、「システムに緊急事態が発生しており、作業上、どうしてもあなたのパスワードが必要になった。これがないとあなたのデータが失われるかも知れない。」と騙すなどという手口は簡単に予想できる。

最も危険なのはシステム管理者 (root) として侵入されることである。一般利用者のパスワードを盗んで侵入するのは、多くの場合[†14]、root 権限を取得するためのスキを探すのが目的である。

不正な遠隔データアクセスは、ネットワーク越しにデータを共有／公開するようなサーバ機能を悪用し、重要なデータを盗もうとする攻撃である。一般に、ログインしなくともその計算機上のデータを見ることはできる。例えば、WWW ページの閲覧や電子ニュースの購読はその (正常な) 例である。一般にこのようなサーバは、"アクセス制限機能" を持ち、このデータは信用できる人からしか見えない／変更できない、というような制御ができる。しかし、機能が不十分であったり、サーバ管理者が設定を間違ったり、あるいはそのプログラムがセキュリティホールを持っていてそこを突かれたりした場合、攻撃者に対してデータ取得や改竄を許してしまう。

よく狙われるものがパスワードファイルである。これを盗まれると (たとえ暗号化されていても)、パスワードを推定されてしまい、先の "不正なログイン" を許してしまう。

また、知らずに使っている人も多いが、X Window のようなネットワーク型ウインドシステムも危険である。例えば、X Window で言えば、UNIX ワークステーション、Winodws 上や Macintosh 上で動く X エミュレータ、X 専用端末などは、X サーバと呼ばれ、ネットワーク上の他の計算機上で動くプログラム (X クライアント) に対して、入力デバイスであるキーボードやマウスと、出力デバイスであるグラフィックディスプレイを提供している。その X サーバのアクセス制限の設定がいい

[†12] http://www.symantec.com/avcenter/venc/data/jesus-hoax.html

[†13] 例えばあるエスケープシーケンスが来ると、以降のデータをプリンタに送るような設定の端末ソフト。

[†14] その個人に恨みでもあれば別であるが。

加減だと、ネットワーク経由の攻撃者は、あるウインドウに表示されてる内容を覗き見たり、偽のウインドウを表示したりできてしまう。

不正な遠隔実行は、ここでは、利用者のログインなしに、サーバがネットワーク経由のサービス要求メッセージを契機にして自動で何かの処理を実行してしまう場合を指す。

元々サーバがそのような機能 (遠隔実行) を持っていて、それを悪用する場合もあるが、そうでなくても、どのようなサーバでも、プログラムのセキュリティホールがあった場合に、巧妙にしつらえられたサービス要求メッセージを受取ると、それを処理しようとして暴走し、この "暴走" 具合いを事前に計算することで、不正な処理を実行してしまう可能性がある。よくあるのが、いわゆるスタックオーバーフロー問題である。

運用の妨害は、メールを大量に送りつけたり、特別なアクセスをずっと繰り返したりして、ある計算機やネットワークを麻痺させたり、最悪は計算機やルータをダウン／クラッシュさせるような攻撃 (妨害) で、一般に、**"Denial of Service"** と呼ばれる。

業務上重要な計算機やネットワークが麻痺したり、ダウンしたりすると大変であるが、そうでない計算機でも、Denial of Service 攻撃を受ける時は、他の攻撃の補助を意図している可能性が高く、注意が必要である。例えば、その計算機が通信不能に陥っている間に、その計算機の IP アドレスを使って (その計算機になりすまして) 不正を行う場合がある。

対策:

ログインパスワードが破られて侵入されることを防ぐには、まず、**各人がパスワードを厳重に管理する**必要がある。自分のパスワードは他人に知られないよう、口座の暗証番号などと同等に厳重に扱う必要がある。誰かにパスワードを破られると、完全に自分になりかわってログインされ、その侵入者は、パスワードの持ち主のメールを読む、ファイルを書き換える、名前をかたって悪事をはたらく等、なんでもできる上に、他の人のパスワードを破る足掛かりを提供してしまうことになる。例えば、通産省の「コンピュータ不正アクセス対策基準」でも各利用者が守るべき最重要事項としてログインパスワードの厳重管理を要請している[†15] 。

> システムを利用する者（以下「システムユーザ」とする）が実施すべき対策についてまとめたもの。
> Ｖ．基準項目
> 　１．システムユーザ基準
> 　（１）パスワード及びユーザＩＤ管理
> 　　１．ユーザＩＤは、複数のシステムユーザで利用しないこと。
> 　　２．ユーザＩＤは、パスワードを必ず設定すること。
> 　　３．複数のユーザＩＤを持っている場合は、それぞれ異なるパスワードを設定すること。
> 　　４．悪いパスワードは、設定しないこと。
> 　　５．パスワードは、随時変更すること。
> 　　６．パスワードは、紙媒体等に記述しておかないこと。
> 　　７．パスワードを入力する場合は、他人に見られないようにすること。
> 　　８．他人のパスワードを知った場合は、速やかにシステム管理者に通知すること。
> 　　９．ユーザＩＤを利用しなくなった場合は、速やかにシステム管理者に届け出ること。

最近、深刻なのは、認識なしに "パスワード" を使う人が急増してる点である。UNIX のようなサーバ計算機に "ログイン" して使う場合は、教育なしに使える人は稀なので、いやおうなしに教育も受け、その最初の教程で必ず "パスワード" の重要性が説かれる。しかし、パソコンから電子メールを読むだけの人は、パスワードのへの認識 (悪用されると何が起きるかの) は甘い。さらに恐ろしいことに、パソコン系の OS において、簡単に遠隔資源共有／遠隔操作ができるようになり、それらは、

[†15] 先に述べた IPA のセキュリティセンターのページから見ることができる。

"安全なパスワードを設定すれば" 安全に使えることになっている。しかし、元々パスワードのないパソコンの世界で暮していた人が急に "安全なパスワードの設定に気を配る" だろうか? 人間は一般に易きに流れるものであり、一見 "便利な" 道具が、売ったが勝ちの論理でどんどん広まっているが、利便性と引き替えにした潜在的危険性は計り知れない。

また、ネットワーク経由 (特にインターネット経由) でログインする場合は、ログインする時に入力したパスワードは盗聴される危険性が高い。そこで、SSH、SSL、ワンタイムパスワードなどの安全な認証方法を使うツールが普及してきている。本特集の "安全なリモートアクセス" 参照。

さらに、トロイの木馬に引っ掛って、"不正アクセス" を助ける悪意のプログラム (一般に "裏口" とも呼ばれる) を知らずに実行してしまう場合もある[†16] 。

一方、サーバの設定ミスまたはセキュリティホールが原因である場合も多い。本特集の "サーバ管理者のためのセキュリティ" 参照。

2.3 通信の盗聴、改竄、なりすまし

離れた2地点間で通信する2者の間に物理的に第3者が存在する可能性は排除できないので、基本的に 盗聴、改竄、なりすまし の危険は付きまとう。**盗聴**とはメッセージの中身を盗み見することであり、**改竄**とは転送途中のメッセージの中身を変更することであり、**なりすまし**とはメッセージの送り主を騙ることである。例えば、

- 電子メールで重要な情報を送る場合、内容の機密性、改竄防止、発信者の認証 (なりすまし防止) が必要になる。本特集の "メールにおける信頼性" 参照。
- WWW ページでオンラインショッピングをする場合、(偽のサーバで買い物してないことをチェックするため) サーバの認証や、クレジットカードの番号を送信するときの機密性の保持が必要になる。通常、SSL という仕組みを用いるが、既に Netscape や IE などのブラウザではその機能が付いている。
- 携帯端末から、遠隔ログインによって大学のサーバにログインして仕事する場合、利用者の認証や、端末からの入力/端末への表示データの機密性の保持が必要になる。本特集の "安全なリモートアクセス" 参照。

これらは、技術的には暗号化及びその関連技術である改竄検出や電子署名を使って防ぐことができる。ただし、実際の社会における運用の仕組みはまだ不十分であり、これから急速に整備され、普及していくと思われる。

3 組織として考えなければならないこと

3.1 ファイアウォール

ファイアウォールは、組織の内と外の間の通信に対し、セキュリティ上の危険防止のために何らかの制限を行うものである。長崎大学でも、現在、学内・学外間の通信のうちで危険/不要なものを遮断するためにファイアウォールを置いている。また、学内の組織単位でも、その中のネットワークに要求される機密性/安全性に応じて、独自でファイアウォールを置いている場合もある。

一般にファイアウォールは2つの目的に使える。

1. 組織外から組織内へのネットワーク経由の不正アクセスを防ぐ。1台1台の計算機での防御も重要であるが、共通的に防ぐことのできる部分は一括して防御 (アクセス禁止) にした方が効率

[†16] 最近の例として、`http://www.cert.org/vul_notes/VN-98.07.backorifice.html` がある。

的である。ちなみに、この遮断に引っ掛る通信 ("学外からの不審なアクセス") は一日に数百件ある。つまり、大学というのは、ほとんど常時、学外からの攻撃にさらされている。これらはいろんな計算機にアクセスしてみてセキュリティホールを探し回り、一旦不注意な (間違って設定が甘いとか、セキュリティホールを抱えたままのプログラムを放置しているとか) 計算機が見つかったらそれを徹底的に攻めるようになっている。

2. 組織内から組織外へのネットワーク経由の不正アクセスを防ぐ。組織内の計算機が踏台として使われることや、内部の人が組織外へ不正アクセスを行うことを防止／検出できる。内部の人による不正アクセスは、故意でなくても、セキュリティチェック用のソフトの操作ミスでも発生する (実際、しばしば発生している)。

しかし、大きな問題はある。元々ファイアウォールで防ぐのは、"ネットワーク経由の不正アクセス" だけである。先に見たように、"悪意のプログラム" や通信路での "盗聴、改竄、なりすまし" には無力である。しかも、"外部" からの攻撃を防ぐだけで、"内部" からの攻撃にも無力である。つまり、内部の計算機の1台でも、例えば、電子メールに付いてきたトロイの木馬に感染し、そのプログラムが自動的に内部の他の計算機に不正アクセスを試みたとしても、ファイアウォールは関知しないことである。さらに、一番怖いのは、「ファイアウォールの中だから安心」と誤解する利用者や、あるいは啓蒙を怠る管理者が出現することである。

また、一般にファイアウォールは画一的な防御であり、それなりに利便性を損なう面はある。学術研究組織や教育組織にどういうファイアウォールモデルが適切かはまだ議論のあるところである。

3.2 セキュリティ及びモラルの教育

ネットワークセキュリティは、ネットワークを使っている全員の協力がないと守れない。自分の計算機には守るべきデータはなにも持たないから関係ない、という立場は許されない。そこを踏台にされることで近所の人の計算機の危険度を高めるからである。さらには、その踏台から日本あるいは世界の他組織への攻撃を行った場合、社会的非難とともに、法的責任さえ発生する可能性がある。

もう一点は、自組織からクラッカを出さない努力[†17]も必要である。特に大学は、学生の教育の責任を負っているので、教育／研究活動の一貫として学生にネットワークを利用させる以上は、セキュリティ及びモラルの教育は必須である。

先日も大学宛にある法律事務所から、発信元 IP アドレスが長崎大になってるアクセスに関して、脅しめいた手紙が舞い込んだ。これ自体は言い掛かりとしか思えない内容であったが、一般に今後こういうケースが増えると思われる。

余談:

ところで、一般のコンピュータセキュリティの問題として、「西暦2000年問題 (Y2K problem)」が目の前に迫ってきた。大学では、クリティカルな用途で使われるプログラムが少ないのか、お役所やメーカの対応を信じて疑わないのか、あまり騒がれてはいないようである。

しかし、米国の FEMA [†18] のページ (`http://www.fema.gov/y2k/ccmp.htm`) によれば、万一の事態に準備するための危機管理のガイドラインが作られているし、中国では、航空会社の社長に、来年の1月1日を飛行中の飛行機の中で迎えるように命令することで、2000年問題への対応を真剣に行わせる、という新聞記事も目にした。日本では何事も起らなければいいのだが、、、:-)

[†17] それでいて良いハッカーは育てる必要があるのだが、、、

[†18] 連邦緊急事態管理庁 (The Federal Emergency Management Agency)