大学における情報ネットワークセキュリティ

佐伯　勇

Information Network Security of Campus Network

SAEKI Isamu

Abstract : In modern days, all organizations are requested to strictly protect information such as individual information. If the information network security was not improved, social credit might be lost. To keep the information security level high, it is necessary to spend enough human resources and the budget. However, it is not easy to say that management and operation of the information network at the university is more enough than the enterprise. In this paper, I explain a background of the information network security problem of campus network. I also show concrete threats to campus network and discuss effective measures that can be taken now.

はじめに

本学では，2000年にギガビットイーサネットワークスイッチをコアスイッチとする全学情報ネットワークシステムを導入した。この年以降，教職員や学生は，キャンパスネットワークとインターネット接続を前提として学内のコンピュータを利用するようになった。翌年には，Yahoo! BB や NTT の「フレッツADSL」など，主要な電気通信事業者による ADSL サービスが開始され，インターネットに接続する家庭が急速に増加した。それからわずか5年の間に，学内でのファイルサーバやネットワークプリンタの利用，インターネットを経由した Web メール，シラバス公開，図書メディア資料検索，履修管理，グループウェアなど，全学情報ネットワークを利用した多くのサービスが提供され，利便性が大幅に向上した。

大学が所有するコンピュータに加え，教職員や学生の自宅でも私物のコンピュータがネットワークに接続されるようになると，コンピュータシステム全体のセキュリティ問題の重要度が増してきた。キャンパスネットワークにはインターネットを経由して様々な攻撃が日々行われるようになり，大学のファイアウォールをすり抜けて，ウイルス・ワーム・スパイウェア・アドウェアなど不正なプログラムがユーザのコンピュータにまで届くようになった。本学でも，教員のコンピュータが電子メールの添付ファイルを媒介としてワームに感染し，学内のコンピュータに攻撃を仕掛けるという事例が発生した。

個人情報保護など情報管理の厳格化が叫ばれる中，大学としても情報ネットワークセキュリティを高めなければ，社会的信用を失いかねない時代となった。セキュリティ対策には予算と人的資源を投入する必要があるが，企業と比較すると大学の情報ネットワーク運用管理は十分であるとは言いがたい。そこで本稿では，大学における情報ネットワークセキュリティ問題の背景と具体的な脅威について説明し，現在取りうる対策について論じたい。

1. 問題の背景

本節では，近年情報ネットワークセキュリティが重要な問題として認識されるようになった背景と，セキュリティ問題を考える上で大学に共通して見られる特徴について説明する。

1.1 インターネット人口の増加

情報通信白書平成19年版によれば，世界のインタ

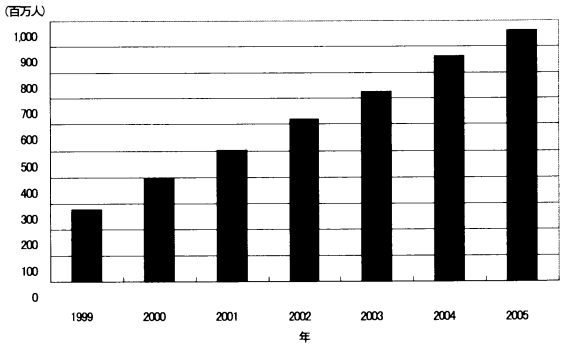

図1　世界のインターネット利用者数

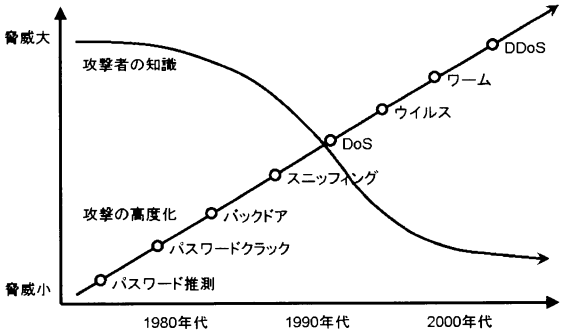

図2　攻撃ツールの高度化と侵入知識の低下

ーネット利用者数は1999年頃よりほぼ線形的に増加し，現在では既に10億人を突破していることが確実である（図1）。したがって，不正を行う者の絶対数も利用者数に比例して増加していることになる。一方で，インターネットや携帯電話などネットワークメディアには，使用する人数が増加すればするほど参加者が得るメリットは階乗的に増加するという特徴がある。不正使用を目論む者の立場から見れば，ネットワークを利用して不正を行う動機が階乗的に高まるということになる。

1.2　攻撃ツールの高度化

米国CERT/CC（Computer Emergency Response Team Coordination Center）が作成した資料を基に，攻撃ツールの高度化と侵入知識の低下の関係を示したものが図2である。（攻撃ツールの詳細はそれぞれ第2節で説明する。）

1980年代初頭には他人のパスワードを推測して入力するという非効率的な攻撃方法しか見られなかったが，同年代半ばには攻撃ツールの元祖とも言えるパスワードクラッキングプログラムが登場し，自動的にシステム侵入を試みる時代へと突入した。その後，通信内容の傍受，特定サイトへのパケット大量集中送信によるサービス妨害など様々な攻撃手法が考案されてきた。攻撃手法が年々高度化するにつれて，攻撃ツールの使用はますます容易になった。インターネットの普及に伴い，アンダーグラウンドサイト等で配布される攻撃ツールが誰でも手軽に入手できるようになり，スクリプト・キディと呼ばれるレベルの低い攻撃者による攻撃が急増した。現在，インターネットでは日常的に様々なクラッキング被害が発生しているが，その多くはスクリプト・キディによるものだと言われている。

1.3　大学の低い運用管理能力

ほとんど全てのコンピュータがインターネット使用を前提としている現在，インターネットに接続する全ての組織に適切な運用管理能力が求められている。ところが，以下に述べる大学特有の問題が，キャンパスネットワークでセキュリティを確保することを難しくしている。ここでは，運用と管理の両面からこの問題について説明する。

まず運用面では，人的資源と付随する予算の乏しさが問題である。一般的に企業では，全社の情報ネットワークシステムを統括する部門を設置し，その管理下に置かれた端末を社員に貸与する形で全体のシステムを管理している。一方大学では，柔軟な運用ポリシーを要求する研究用コンピュータが多数存在し，縦割りの組織運営がシステム管理にも波及しているために，キャンパスネットワーク全体の管理が比較的困難になっている。本学でも，本年度よりIT推進室と称するキャンパスネットワーク管理部門が設置されたが，現在のところ職員数は1名のみであり，600台を超えるコンピュータから構成されるシステム全体を統括することは現実的には不可能な状況である。

次に管理面では，セキュリティポリシーの策定とその効果的な実施が不十分であるという問題が存在する。私立大学情報環境白書（平成17年度版）によれば，全国の私立大学の中で全学的なセキュリティポリシーを策定しているのは21%であり，その実施細則まで含めてセキュリティポリシーが有効に機能していると考えている大学は極めて少数である。大学組織は，教育研究組織と業務組織の二重構造となっており，情報管理の徹底が教育研究活動の大きな妨げとならないよう十分配慮しなければならない。また，本来は雇用契約を結ぶ際に規定されるべき大学と教職員の責任所在が曖昧なまま放置されており，教員や研究者としての行動に対し，大学がどこまで責任を取るのか

という点に関する線引きが難しくなっている。

以上の運用・管理両面の問題を抱えたキャンパスネットワークは，ごく少数の管理者に多大な負担を強いる形で運用されていることが多く，踏み台・不正中継・不正侵入など様々な攻撃の対象となる可能性が高いのである。

2. 情報ネットワークセキュリティ上の脅威と対策

本節では，主として情報ネットワークシステム管理者の視点から，現在の情報ネットワークセキュリティを理解する上での具体的な脅威と現在考えられる対策について個別的に説明する。

2.1 ポートスキャン

ポートスキャンとは，ネットワークプログラムにおいて仮想的な情報送受信の窓口となるポートが使用可能な状態にあるか否かを外部から調査する行為である。OS やアプリケーションにセキュリティホール（セキュリティ上の欠陥）があり，当該プログラムの使用するポートがインターネットに対して開いていれば，ポートスキャンによって「攻撃を仕掛けやすいコンピュータ」として発見される可能性がある。インターネットに常時接続する全てのコンピュータはポートスキャンに晒されていると見なすべきである。

ポートスキャンによる攻撃対象調査で「攻撃を仕掛けやすいコンピュータ」として発見されることを防ぐためには，少なくとも OS やアプリケーションの既知のセキュリティホールを修正しておく必要がある。修正方法は，通常当該ソフトウェアのホームページに掲載されているが，Microsoft Windows など特定のソフトウェアは自動的に修正の有無を検知しアップデートする機能を有する。また，ルータやファイアウォールを適切に設定することや IDS（Intrusion Detection System）を導入することにより，コンピュータに対するポートスキャンの多くを防ぐことも可能である。

2.2 不正侵入

不正侵入とは，他人の識別符号（ユーザ ID，パスワード，生体認証情報，署名など）または OS やアプリケーションのセキュリティホールを使用してアクセスが制御されているシステムを利用する行為である。具体的被害としては，個人情報などシステムに保存されているファイルの奪取，ウェブサイトの改ざんなどがあり，不正利用の例としては，迷惑メール中継やプロキシ不正利用などが挙げられる。一旦システムに侵入されると，さらに高度な機能を有するバックドアと呼ばれるプログラムを送り込まれることがあり，最悪の場合，コンピュータの全機能を掌握される危険性がある。また，ユーザがバックドアプログラムとは知らずにプログラムをインストールしてバックドアを仕掛けられることもある（トロイの木馬型コンピュータウイルス）。

ポートスキャンによる被害の予防方法と同様，OS やアプリケーションのアップデート，ルータやファイアウォールの適切な導入は不正侵入にも有効である。また，ウイルス対策ソフトも多くの「トロイの木馬型コンピュータウイルス」を検知し削除するが，何よりも出所不明のプログラムを安易に実行しないなど基本的なセキュリティ意識を持つことが重要である。

2.3 ウイルスとワーム

通商産業省（現経済産業省）によれば，ウイルスは次の機能のうち少なくとも 1 つを有するものと定義されている。

(a) 自己伝染機能

自らの機能によって他のプログラムに自らをコピーし又はシステム機能を利用して自らを他のシステムにコピーすることにより，他のシステムに伝染する機能。

(b) 潜伏機能

発病するための特定時刻，一定時間，処理回数等の条件を記憶させて，発病するまで症状を出さない機能。

(c) 発病機能

プログラム，データ等のファイルの破壊を行ったり，設計者の意図しない動作をする等の機能。

ウイルス自身は独立して作動するプログラムではなく，他のファイルに感染することによりその機能を発揮する。このため，あるコンピュータから別のコンピュータに感染する際には，媒介するファイルが必要となるので，フロッピーディスクや USB メモリなどのリムーバブルメディアや電子メールの添付ファイルを経由して感染することが多い。情報処理推進機構によれば，ウイルスの 90% 以上は電子メールで感染することが明らかになっている。一方ワームは，それ自体が単体で実行可能なプログラムであるため，あるコンピュータから別のコンピュータに感染する際に別の媒介ファイルを必要としない点がウイルスとは異なる。

ポートスキャンによる被害の予防方法と同様，OSやアプリケーションのアップデート，ルータやファイアウォールの適切な導入がウイルス・ワーム対策として有効である。これらに加えて，ウイルス対策ソフトウェアの導入が簡易かつ効果的である。ただし，ウイルス対策ソフトウェアが対応するウイルスはメーカや製品ごとに異なるため，プロキシ，サーバ，クライアントコンピュータに異なるタイプの製品を導入し併用することが望ましい。その他ユーザが注意すべき事項としては，現在でも多くのウイルスが電子メール経由で送信されているため，不審な添付ファイルは安易に開いてはいけないことが挙げられる。

2.4 スパイウェア

スパイウェアとは，ユーザの操作やウェブサイトの閲覧履歴等の個人情報を監視・記録し，予め設定された受信者に密かに送信する機能を持つソフトウェアである。スパイウェアは，ユーザの了承無しにインストールされ，コンピュータシステムを不安定にさせたり望まない情報漏えいを引き起こしたりする点でウイルスと似ているが，次の2点で違いがある。まず，ウイルスは自己増殖機能を持ち，できる限り自分のコピーを他のコンピュータに広めようとするが，スパイウェアは通常自己増殖機能を持たない。次に，ウイルスは作成したプログラマによって，システムを使用不能にしたり，ファイルを削除したり，画面上に無意味な表示をするなどの機能が仕組まれており，容易に感染に気づくことができるが，スパイウェアはなるべくユーザに気づかれないように動作する。このため，ユーザはスパイウェアの存在を意識することが少なく，結果として被害が長期間継続することが多い。無料のソフトウェアにはスパイウェアが仕組まれていることもあるが，長文の利用規約の中に個人情報を送信する旨の説明がなされているため，その規約を十分理解せずに同意するユーザが多い。

スパイウェアの中には，OSやアプリケーションの既知のセキュリティホールを利用してインストールされるものもが多く，OSやアプリケーションのアップデートはスパイウェア対策としても有効である。ウイルス対策ソフトもスパイウェアへの対応を急いでいるが，Ad-Aware, Soybot, Spyware Blasterなど，スパイウェア専門の検索・除去機能を持ったスパイウェア対策ソフトも併用すべきである。

2.5 DoSとDDoS

DoS（Denial of Service）とは，特定のサーバに対し，短時間に大量のネットワークトラフィックを送信し，サーバに接続する回線やサーバの処理能力を占有し，システムのサービス提供を阻害する行為である。さらに，踏み台と呼ばれる複数のコンピュータを用いてDoS攻撃を行うことをDDoS（Distributed DoS）攻撃と呼ぶ。踏み台は，管理者の知識不足や怠慢などにより，既知のセキュリティホールが放置されたために攻撃用のエージェントが組み込まれたコンピュータであることが多い。近年は，一般家庭のインターネット接続速度が向上し，ウイルスに感染したパーソナルコンピュータがDDoS攻撃に利用されるケースが増えてきた。これまでに，Yahoo!, CNN.com, amazon. comなど有名企業の大規模システムがDDoS攻撃により一時サービス不能になるなど経済的被害も莫大になりつつある。さらに，DDoSの協調分散機能を用い，迷惑メール送信，感染パケット送信などさらに機能を高めたBOTNETと呼ばれる攻撃手法も問題化している。Telecom-ISAC Japanの調査では，セキュリティホールのあるパソコンを直接インターネットに接続しただけで，わずか4分程度でBOTウイルスに感染することが確認されている。

DoS攻撃に対しては攻撃を行うコンピュータからの通信を遮断すればよいが，DDoS攻撃に対しては，攻撃元のコンピュータが数千，数万に及ぶため，現時点では完全に防御する方法は存在しない。一方，自分の所有するコンピュータがDoSやDDoS攻撃に加担しないための対策方法は存在する。例えば簡易な方法として，サイバークリーンセンターが提供する無償アプリケーション「CCCクリーナー」を定期的に実行して，BOTウイルス等DoS攻撃を行うプログラムを検出・除去することが考えられる。

3. 基本的なセキュリティ対策

本節では，前節での議論を踏まえ，管理者とユーザの視点で基本的なセキュリティ対策法をまとめる。

3.1 管理者の視点から

前節で述べたそれぞれの脅威への対応策に実効性を持たせるためには，セキュリティポリシーの策定とPDCAサイクルの実施が重要となる。特に，クライアントコンピュータの管理方法，アップデートプログラムの適用方法，問題発生時の対処方法などを明文化

し，周知徹底する必要がある。また，インターネットを使用した攻撃方法は日々進化するため，ある時点でセキュリティ検査に合格したとしても，翌日の安全性を保障することはできない。PDCA サイクルに従い，継続的にセキュリティ検査と対策を繰り返すことにより，一定のセキュリティレベルを確保する取り組みが必要である。

予算面でも重要なポイントがある。ネットワーク機器，サーバ，ソフトウェア等を導入する場合，一般的には故障や不具合に備えた保守費用を予算として確保する。ところが，他の組織で新しい攻撃手法による被害事例が発生した場合，仮に保守契約を結んでいたとしても，メーカがシステムの修正版を提供するまでの間は，システムを一時的に停止するか脅威に晒したまま運用を続けるかの選択を迫られる。情報ネットワークシステムが，教育・研究・業務の重要なインフラになった現在，緊急の脅威に対する迅速な調査，代替手段の一時的導入，修正などが行えるよう，セキュリティ対策費用を予算計上しておく必要がある。

3.2　ユーザの視点から

利用しているコンピュータを安全な状態に保つために，次のような基本的対策を講じる必要がある。

(a) Windows 98, 98 SE, Me など，サポートの切れた OS やアプリケーションは使用しない。どうしても使用する場合は，ネットワークに接続せずスタンドアロンで利用する。

(b) OS やアプリケーションを常に最新の更新が適用された状態に保つ。

(c) パーソナルファイアウォール，ウイルス対策ソフト，スパイウェア対策ソフトなどを導入し，パターンファイルを最新の状態に保つとともに，定期的に検査を実施する。

(d) 万が一のために，必要なファイルのバックアップを定期的に取る。

また，ファイル交換ソフトや信用できないウェブサイトから入手したソフトウェアやデータには，ウイルスやスパイウェアなどが付属していることがあるので基本的には利用しないほうが良いが，どうしても利用するのであれば，ウイルス対策ソフト等での検査が必須である。正規のソフトウェアであっても，スパイウェアをインストールするものも存在するので，表示される使用許諾契約書を注意深く確認すると同時に，他のウェブサイト等で第三者の評価を収集し，客観的に判断する必要がある。

ま　と　め

本稿で述べた情報ネットワークシステムセキュリティ上の脅威に関しては，日々新しい攻撃手法が考案され，あるいは脅威が組み合わされ，より気づかれにくい形で攻撃に使われるように進化していくであろう。新たな脅威に対応するためには，個々の脅威について知識を持っているだけでは不十分で，複数の脅威同士の関係性や対策方法の限界を良く理解しておく必要がある。

ユーザは，常に自分のコンピュータが脅威に晒されていることを意識してコンピュータを安全に保つ努力をし，管理者は実効的なセキュリティポリシーを定めて PDCA サイクルに従ってセキュリティレベルを維持しようと努めるべきである。それぞれの立場でセキュリティを意識して行動することによって初めてセキュリティ対策が有効に機能するのである。

キャンパスネットワークの運用管理においても，システム全体の統括部門が専門的知識を蓄積し，ユーザの啓蒙・教育に時間を費やす必要があり，人的資源と予算の投入によるセキュリティポリシーの策定とその効果的な実施が急がれる状況にある。

参考文献

1）『情報通信白書平成 19 年版』，総務省，p. 238, 2007, http : //www.johotsusintokei.soumu.go.jp/whitepaper/ja/cover/index.htm.

2）大塚秀治，牧野晋，『情報ネットワークのセキュリティ』，私立大学情報教育協会平成 16 年度学内 LAN 運用管理講習会資料，pp. 139–153, 2004.

3）情報セキュリティ検討会，『情報セキュリティ白書 2007 年版』，独立行政法人情報処理推進機構，2007.

4）Tim Shimeall, “Cyberterrorism”, Computer Emergency Response Team Coordination Center, 2002, http : //www.cert.org/archive/ppt/cyberterror.ppt.

5）『私立大学情報環境白書（平成 17 年度版）』，私立大学情報教育協会，2006, http : //www.juce.jp/LINK/report/youran 2005/hakusho_index.html.

6）コンピュータウイルス対策基準，通商産業省告示第 952 号，2000, http : //www.ipa.go.jp/security/antivirus/ki-jun 952.html.

7）Wikipedia, http : //ja.wikipedia.org/.

8）独立行政法人情報処理推進機構，http : //www.ipa.go.jp/.

9）サイバークリーンセンター，http : //www.ccc.go.jp/.

10）Telecom-ISAC Japan, http : //www.telecom–isac.jp/.