キャンパスネットワークにおける安全管理体制

大型計算機センター助教授　沢　田　篤　史

1．はじめに

コンピュータネットワークは人々の様々な活動に浸透するにつれ、大学の構成員にとっても必要不可欠な存在となってきた。各構成員が利用するコンピュータを大学内外と接続するキャンパスネットワークはもはや、水道や電力や電話と同様のライフラインであるといって良い。それほど重要な存在であるにも関わらず、日本の大学(とくに本学)におけるその管理体制はあまりにも脆弱なものであるといわざるを得ない。

近年、コンピュータネットワークにおけるセキュリティ対策の重要性が強く指摘されるようになってきており、キャンパスネットワークにおいても安全管理体制の早急な整備が求められている。しかしながら、ボランティア的労働に支えられた管理体制のままで可能な対策は残念ながら限られており、大学構成員すべての活動を支えるライフラインは常に危険にさらされ続けているといっても良い。このような現状の中、キャンパスネットワークの利用者はどう行動すべきであろうか。

2．大学におけるセキュリティ対策の困難さ

1999年11月、文部省は全国99国立大学および14共同利用機関を対象として、セキュリティ対策に関する調査を行った。2000年6月に発表されたその結果によると、そのうちの106機関が1997年度以降に何らかの不正アクセスを経験したとされている。不正アクセスの内容は、電子メールの不正中継、情報改竄など様々であるが、その多くは大学のセキュリティ対策が不十分であることに起因するもので、改善を検討する必要があることが指摘されている。

一方、侵入を企てるクラッカーにとって日本の大学（あるいは本学）はどう映っているのだろうか。一人のクラッカーの発信する情報が瞬時に世界中を駆け巡る今日において、大学における安全管理体制の甘さは、上のような調査結果を待つまでもなく、すでに広く知れ渡っている。一般にクラッカーは、攻撃対象のコンピュータシステムに不正侵入を企てるさい、その対象に直接攻撃を仕掛けることはない。まずは一旦別のシステムを乗っ取り、それを踏み台とし（あるいは複数の踏み台を経由し）、目的のシステムへの侵入を試みる。身元の判明を困難にするためである。安全管理体制が未熟なネットワークを抱える大学は、そのような踏み台として絶好の狙い目とされている。本学に至っては、踏み台としての利用どころか、不正侵入の練習台（しかも初級！）と紹介されているという噂さえ耳にする。

大学、とりわけ本学におけるセキュリティ対策がこれほどまでに遅れているのはなぜだろうか。その要因として第一に挙げられるのは、その組織の大きさである。学内でアカウント、メールアドレスを持つ関係者は三万人以上にのぼるとされているが、その正確な数さえ定かではない。また大学においてコンピュータネットワークを利用する関係者の身分は実に多様であり、学生、教官、事務官といった枠で簡単に整理することができない上、年度や月度といった区切りとは関係なく頻繁に変動する。このようにキャンパスネットワークは、その利用者が大量かつ多様でしかも流動的という、管理を難しくする性質を兼ね備えているうえ、利用者は原則自由に行動し、それに何らかの規制や歯止めをかけるメカニズムが貧弱であるという体制上の問題も併せ持った、セキュリティ対策を施すには最も困難な対象であるといえる。

このように安全体制を整えることが困難なキャンパスネットワークであるが、なおかつそこで守るべきものが非常に多いという特徴も持っており、これもネットワーク管理者にとっては

頭の痛い問題となっている。大学の持つ機密情報や個人情報を守らなければならないのはもちろんであるが、不正侵入によりネットワークの正当な利用が妨げられることがあってはならないし、不法行為の踏み台となってしまうことにより大学の信用が失墜するようなことがあってもならず、安全管理体制に期待されている役割は重大であるといえる。にもかかわらず、学内で日常的に利用しているネットワークの管理体制はどうなっているかを振り返ってみると、多くの場合、コンピュータ上のアカウントやサーバ機能等の管理は、教官や学生のボランティア的労働によってかろうじて支えられている状況ではないかと想像する。

不正侵入の手口はその防止策とともに次々に高度化して行くため、ネットワークの安全を管理するためには最新の技術動向を常に追い、それを実際のネットワークに適用するという、技術的にも高度で煩雑な作業が継続的に必要となる。ネットワークを正常に機能させるだけでなくその安全性も管理するとなると、もはやこれまでのボランティアに支えられる体制のままでは対応しきれないことは明らかである。

3．本学(KUINS)における対策の現状

部局や研究室の安全管理と同様の困難さを、本学全体のネットワーク管理組織であるＫＵＩＮＳも抱えているといえる。その組織自体が部局としての実体を持たないことに象徴されるように、ＫＵＩＮＳにおける管理体制もボランティア的労働を前提とした脆弱なものである。実際、1997年度までのＫＵＩＮＳでは、全学規模でのセキュリティ対策はまったく行われていない状況であった。1998年度に、危険性が強く指摘されている通信に関する例外的な制限を行ったが、基本的には通信に何ら制限を設けることなく運用が行われ、セキュリティの保持は各部局あるいは末端の利用者自身の取り組みに任せられてきた。

ネットワークの普及と高速化に伴い、1998年頃から官公庁のホームページ改竄事件をはじめ、ネットワークセキュリティ関係の事故が頻繁に報告されるようになった。ＫＵＩＮＳもその例外ではなく、同じ頃からいわゆるスパムメールの不正中継行為に対する苦情が多く寄せられるようになった。当時は設定が不完全なままのコンピュータがキャンパスネットワークに多数接続されていたため、匿名で大量の商用メールを配布するための踏み台として悪用されてしまったのである。このような踏み台となるコンピュータが一台でも放置されると、何千、何万通も匿名メールを転送してしまうことになり、一時期はそれを送りつけられた人からネットワーク管理者宛てに毎日のように大量の苦情が殺到し、その対応のため、管理者の日常業務が阻害されてしまう事態に至った。

このように、接続されたコンピュータが不正に利用され、意図しないまま学外組織へ攻撃（迷惑）をかけ、結果として日常の業務が阻害される事態に至り、ＫＵＩＮＳでも次の三つの対策を行うこととした。

・対外セグメントの新設
・セキュリティ監視装置の導入
・スパムメール不正中継対策の実施

これらの対策の主目的は、キャンパスネットワークを壊されないようにすることと、外部組織に迷惑をかけないようにすることにある。

対策の結果、キャンパスネットワークとインターネットの接続点には、ファイアウォール（防火壁）らしきものが構築され、学内外間の通信のうちセキュリティ上きわどい事象をセキュリティ監視装置によって検出することが可能となった。セキュリティ監視装置の運用では、危険度の高い事象を管理者宛てにメールで通知しているが、平均して一日に500件近くの事象が検出されている。監視装置の性質上、危険な事象を漏らすことなく報告しようとすることから、この中には通常のネットワーク利用に起因する誤報が相当数含まれていると考えられるが、今後も各事象について注意深く追跡する予定である。

また、スパムメール不正中継対策では、各部局の管理者からの協力を得てメールサーバを届け出ていただいた上で、それ以外のコンピュータに対する学外からのメール通信を遮断した。その結果、以前は毎日のように大量に寄せられたスパム中継に関する苦情が激減し、対策の効果が上がっていることが確認されている。今後は、届け出されたサーバが使用不能の場合にバックアップを行う経路の確保などを充実させる予定である。

このように、遅ればせながらＫＵＩＮＳにおいてもセキュリティ保持のための対策に取り組みはじめ、それなりの効果があがっていると見ることもできる。しかしながら、その対策はまだまだ不十分であり、またその取り組みも「事件が起ったから対策する」という後手にまわったものであるといえる。「積極的な対策を」という要望は利用者からも常に寄せられるのだが、前述のように限られた人的資源では予防作業を行う余裕はなく、通常の管理業務と目先の処理に手一杯の状況である。

4．利用者によるセキュリティ対策の重要性

ここまで述べたことをまとめると、

・セキュリティ対策を行うのに、大学のキャンパスネットワークは非常に困難な対象である反面、大学には守るべきものが非常に多い。
・ネットワークの安全管理体制を整備して積極的にセキュリティ対策を行うことが重要であるにも関わらず、多くの大学でそれが不十分なまま放置されている。
・とくに本学おける全学規模のセキュリティ対策は遅れており､安全管理体制も脆弱である。

のようになるが、セキュリティ対策が大変だからといって、この現状をそのまま放置することは､社会的に許されなくなってきている。2000年２月に施行された「不正アクセス行為の禁止等に関する法律」でも、管理者は「不正アクセス行為から防御するため必要な措置を講ずるよう努めるものとする」とされている。意図しないまま不正アクセスの踏み台となり、他の組織に被害が加わったような場合でも、管理義務怠慢で訴えを受けかねないのである。しかも、訴えは全世界からやってくる可能性がある。

このように差し迫った状況では、キャンパスネットワークの利用者にも、セキュリティ対策に関する意識改革を求め、協力を得なければならない。まずは利用者ひとりひとりが「誰かが管理して守ってくれるだろう」という考えを捨て、知らない間に犯罪に関わらないよう、個人や組織の自衛が必要であるという意識を持っていただきたいと考える。

さらには、ネットワーク犯罪は人災であり、「少しでも可能性のあることは必ず起る」という考えのもとに各部局等で危機管理体制を確立することを求めたい。災害を予防することが大切なのはもちろんであるが、災害が起ってからどう対応するかについて充分な検討を行い、その体制を整えておくことも重要であるといえる。

このような個人や部局レベルでの意識改革を効率的にすすめるためには、ネットワークサービスやネットワーク研究を行う組織だけでなく、法律関係、防災関係など様々な部局の構成員が連携して取り組んで行かなければならないだろう。また、当然のことながら、セキュリティ対策には機器だけでなく人にも相当のコストが必要であることを共通の認識とし、ボランティア的労働に頼らない安全管理体制作りを行うことも急務である。

5．おわりに

大学のキャンパスネットワークには本学のものをはじめ、研究者主導の手作りネットワークに端を発しているものが多い。ネットワーク技術が熟成し、キャンパスネットワークそのものが研究的な興味の対象となりづらくなるにつれ、管理者の不足は深刻度を増している。一方で、ネットワークをライフラインとして利用する傾向がますます強まるにつれ、安全管理体制のさらなる充実が求められているにも関わらず、その受け皿がなかなか整わない。

このような状況にあり、なおキャンパスネットワークのセキュリティレベルを向上させるために最も重要な課題は、個々の利用者の意識改革であるといえる。まずは是非とも「ネットワーク上においても自分の身は自分で守る」という心構えを持っていただくようお願いしたい。

（さわだ　あつし）

謝辞

本稿執筆にあたって、本学情報学研究科の岡部寿男助教授をはじめ、ＫＵＩＮＳ機構の関係諸氏からの助言をいただいた。ここに感謝する。

（平成12年9月25日「京都大学附属図書館講演会」から）

2000年京都電子図書館国際会議開かれる

11月13日から17日にかけて、京都大学、BL（英国図書館）、NSF（米国国立科学財団）主催で「2000年京都電子図書館国際会議：研究と実際」が、アジア、欧米10カ国の最先端技術の研究者と図書館関係者約200人が参加し、附属図書館3階AVホールと同４階大会議室で行われました。

この国際会議は研究者、図書館関係者双方の立場から電子図書館についての説明及び研究発表、パネル討論が行われ、資料の電子化、検索システム、著作権問題、国際協力等について電子図書館の課題を探るために日本ではじめて行われたものです。

初日オープニングは佐々木丞平館長、尾崎春樹文部省学術国際局学術情報課長の挨拶に始まり、長尾眞総長の基調講演「情報技術の発展と図書館機能の拡大」があり、2日目午前中にかけて電子図書館の概観、実際、未来について研究発表がありました。午後からEnglish Programに入り、基調講演、Future Librariesについてのパネル討論があり、4階大会議室でテレビ表示をもとに日本語通訳も行われました。英国図書館理事会長（前英国図書館長）J.M.アッシュワース氏の講演では、デジタル化技術や新しい電子コミュニケーションが従来提供してきた図書館サービスに与える影響について説明され、デジタル化が進む中で、将来に役立つ結果を得るためには図書館の相互協力と国際的な共同研究の必要性が強調されました。このほか、最新技術の紹介や参加者による懇親の会も開催されました。

英国図書館理事会長　J.M.アッシュワース氏