学生生活におけるネットワークの危険性と心得

電子制御工学科　センター員　滝本 裕則

1章　はじめに

近年の高度情報化社会における情報通信ネットワークのインフラ整備に伴い、私達の生活は劇的に変化してきました。私が四国の高専に通っていた10年ほど前、家のパソコンを使ってインターネットに接続するためダイヤルアップ接続を用いていました。今でこそADSLや光通信などにより数十Mbpsでの通信があたりまえですが、ダイヤルアップ接続を用いていたころはMAX 56kbps（当時憧れのISDNでさえ128kbps）であり、Yahoo! Japanのトップサイトを表示するのに何秒も必要でした。また、当時の学生に人気だったコミュニケーションツールはポケットベルであり、日本各地で公衆電話に群がる学生を見かけました。現在では、携帯電話がコミュニケーションツールの標準となり、ハード面では高性能化・小型化に加え、メガピクセルのCMOS素子を備えた端末があたりまえとなっています。ソフト面ではメール機能だけではなく、フルブラウザと呼ばれるソフトウェアが標準搭載されてきており、パソコン用に設計されたインターネット上のウェブサイトを閲覧することが可能となりました。

このように、本格的なユビキタス情報社会になりつつあるなかで、パソコンや携帯電話を対象としたネットワークにおけるトラブルも年々増加傾向にあり、そのトラブル内容も複雑化しています。また、佐世保高専の大多数の学生が携帯電話を所持しており、高専という環境柄、パソコン端末やインターネットを上手に使用するスキルが問われています。したがって、ネットワークという便利なツールをどう上手に使いこなすかが技術者として問われています。そこで、今回は学生生活において遭遇する可能性の高いネットワークトラブルについて、その特徴と事例、さらにトラブルの解決・回避方法について述べたいと思います。先に述べたように、パソコンや携帯電話を対象としたトラブルは増加・複雑化の一途をたどっており、その全てについて紹介することは困難です。よって、今回は学生生活に身近な2つのテーマに絞り、2章では「ネットワークに潜むコンピュータウイルス」を、3章では「携帯電話ネットワークに潜む危険性」について紹介します。

2章　ネットワークに潜むコンピュータウイルス

2.1　ネットワークと人の心に潜むウイルス

みなさんは「ラブレターを書いて逮捕された学生」を知っていますか。このラブレターというのは2005年5月に世界中で猛威を振るったワーム型コンピュータウイルス「LOVE LETTER」のことです。（ちなみに、ウイルスとは不正プログラムのことであり、プログラムを作成することを一般的に「書く」と表現します。）ウイルスを作成したのはフィリピンのコンピュータ専門学校に通う学生で、全世界での被害増額は88億ドルにも上りました。このウイルスは電子メールを媒体とし感染するタイプ「ワーム型」と呼ばれるもので、メールの件名に「あなたが好きです：I love you」、メール本文に「私からのラブレターを添付しました。どうぞ読んでみて下さい。：kindly check the attached LOVE LETTER coming from me」と書かれており、添付ファイルとし「LOVE-LETTER-FOR-YOU.TXT.vbs」がついていました。この添付ファイルがウイルスであり、添付ファイルにアクセスするとコンピュータがウイルスに感染するという手口をとっていました。メールを受け取ったユーザは、メールの件名や本文にさぞかしドキドキしながら添付ファイルを開いたことでしょう。それゆえ多くのユーザがウイルスに感染してしまいました。

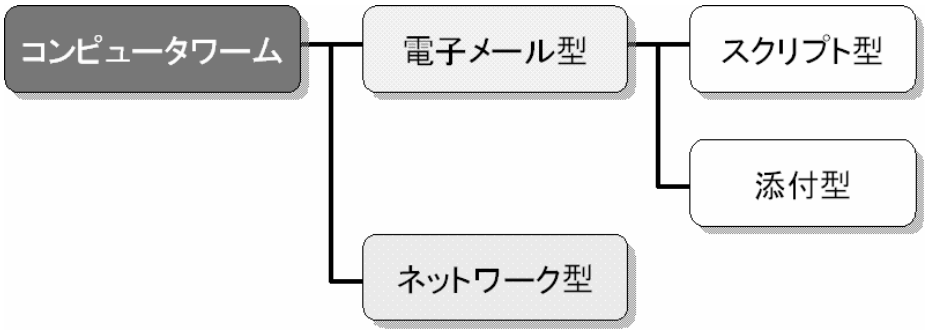

図１　コンピュータワームの分類

このような、人のちょっとした隙をついて感染・増殖を繰り返す不正プログラム（ウイルス）をコンピュータワームと呼び、図１のように分類されます。ワームウイルスは、自己複製能力と他への伝染能力を有しており、脅威度・感染能力が高いといった特徴を持っています。ワームウイルスはその感染経路から電子メール感染型とネットワーク感染型に分類されます。さらに、電子メール感染型はスクリプト型と添付型に分類されます。スクリプト型は、電子メールやブラウザなどが持つスクリプト言語（プログラム言語）を利用し、添付ファイルではなくメッセージに直接付随します。よって、各メーラー（メールソフト）固有のスクリプトを用いているため、固有のメーラー以外に感染が広がることはありません。

一方、添付型は添付ファイルの形でウイルスがメール等に付随し、ユーザが添付ファイルにアクセスすることで感染が広がるタイプのワームです。ワーム型コンピュータウイルス「LOVE LETTER」もこの添付型に分類されます。

最後に、ネットワーク感染型は、TCP/IP や FTP といった（電子メール以外の）通信プロトコルを使用して感染するタイプのウイルスを指しています。学校や会社などのローカルエリアネットワーク（LAN）を介して、接続されているコンピュータを次々に感染していきます。さらに最近では、これらを組み合わせた感染力の強い「複合型ウイルス」も世に出てきています。

では、なぜこのような新しいウイルスが世にでてくるのでしょか。ウイルスを作成する人のタイプをいくつか紹介すると、ただ騒ぎを起こしたい愉快犯タイプ、自分の技術を誇示・技術を試したい技術者タイプ、他の作者やアンチウイルスメーカーと競いたい競技者タイプなどが存在するようです。どれも人の心にあるちょっとした不正な願望や不正な欲望（ウイルス）が、実際のコンピュータウイルスへと形を変えてしまうのではないでしょうか。よって、新たなコンピュータウイルスを生み出させないためには、人の心に寄生するウイルスを駆除しなければなりません。早期技術者教育カリキュラムによって、本校の学生は情報やコンピュータに関しても高い技術力を持っています。このような技術的な教育だけではなく、技術者倫理や情報・ネットワークリテラシー教育を早期から行い、ウイルスを作る側の自己中心的な社会性の無い人間にならないよう、技術者としてのプライドとモラルをもって行動してもらいたいと願っています。

２．２　危険と遭遇しないために

現在、ネットワーク上には様々な種類のウイルスが蔓延しており、その感染手法、被害の程度、駆除の方法も様々です。したがって、これらウイルスから自分のコンピュータを守ることは難しそうに感じるかもしれませんが、実はそうではありません。自分のコンピュータの状態をしっかり把握しておき､基本的な対策をとっておけば､既知のウイルス被害を防ぐことが可能であるといわれています。ＩＰＡ（情報処理振興事業協会）では、以下の７項目を「ウイルス対策」として提唱しています。や

- 最新のウイルス情報定義ファイルに更新し、ウイルス対策ソフトを活用すること
- メールの添付ファイルは、ファイルを開く前にウイルス検査をすること
- ダウンロードしたファイルは使用する前にウイルスの検査を行うこと
- アプリケーションのセキュリティ機能を活用すること
- セキュリティパッチをあてること
- ウイルス感染の兆候を見逃さないこと
- ウイルス感染被害から復旧するための、データバックアップを行うこと

はり自分の身は自分で守る意識が大切だということです。

最近はパソコンを買うとウイルス対策ソフトが入っています。しかし、新種のウイルスが次々と出てくる状況では、新しいワクチンデータ（ウイルス定義ファイル）を更新しなければ意味がありません。週に一度（最低でも月に一度）は、新しいワクチンに更新するようにしてください。

3 章　携帯ネットワークに潜む危険

3．1　技術編

1999 年ごろより爆発的に普及し始め、すっかり私達の生活に浸透した携帯電話。カメラやゲーム、お財布、音楽プレーヤーなどの機能も備え、1 台で何役もこなす優れた必需品に進化してきました。しかし、携帯電話が普及していくにつれ、様々なトラブルが報告されてきました。いわゆる悪徳業者による迷惑メール（スパム）やワンコール・コールバック方式（ワン切り）と呼ばれるものです。これらは携帯キャリア会社の努力によって収束しつつあるのが現状です。しかし、安心してはいけません。今、新たな危険が我々の生活を脅かそうと息を潜めています。

それは「携帯電話ウイルス」と「フィッシング詐欺」です。これまで、ウイルスやフィッシング詐欺はパソコンネットワーク上の危険として認識されてきました。けれども、近年の携帯電話におけるハード面・ソフト面の高機能化によって、パソコンと同様にネットワークを利用した認証や決済を行うことが可能となりました。このような急速な技術進歩により、利便性が向上した反面、新たな脅威を生むという皮肉な結果となってしまいました。

携帯電話ウイルスとは、携帯電話端末の通信機能を介して他の携帯電話に感染するウイルスの一種であり、2004 年に海外で初めて発見されました。コンピュータセキュリティを専門とするフィンランド F-Secure 社がまとめたところによると、全世界において 2004 年から 2006 年の 2 年間で、約 200 種類以上の携帯電話ウイルスが確認されました。スパイウエア機能を持つ「Flexispy」や、携帯版トロイの木馬「RedBrowser」などが我々の携帯ライフを脅かすのもそう遠い話ではなさそうです。

また、「フィッシング詐欺」とは、悪意の第三者が会員制ウェブサイトや有名企業など実在するサイトを模倣し、クレジットカードの会員番号といった個人情報や、銀行預金口座を含む各種サービスの ID やパスワードを獲得することを目的とする犯罪行為を指します。これまではパソコンによるアクセスがターゲットとされてきましたが、先に述べたように携帯ネットワークを利用した認証や決済を行う人が増加したため、自然と携帯電話がターゲットとなったようです。

この問題への対策として、より確かに本人だと証明するために「電子証明書」による認証が可能な携帯電話が増えてきています。大切な情報を安全にやり取りするため、ID、パスワード、電子証明書、暗号化など様々な技術を知っておきたいものです。

3．2　モラル編

携帯電話の魅力とは、それは「ユビキタス」であると私は考えています。「ユビキタス」とは、「いつでも、どこでも、だれでも（だれとでも）」が利用できる、そして恩恵を受けることができる環境や技術を意味しています。携帯電話は我々の生活に無くてはならないものとなり、その携帯電話ネットワークを利用して、私達は多くの人とコミュニケーションをとり、新しい情報を得ています。その携帯電話ネットワークは、さながら実世界における人間同士のコミュニケーションネットワークのようであり、当然のことながら一般社会と同様のマナーやモラルを守る必要があります。しかし、今の若い世代（特に学生）はネットワーク上のマナーに無頓着（無知）であり、また新しい技術ばかりに目がいってしまいがちです。

インターネットや携帯電話が一般に普及する以前に盛んであったパソコン通信では、通常各個人に対して個別の ID が発行されており、通信ネットワーク上での活動は全てその ID を用いて行っていました。そのため、その ID（自身）に対して責任を持った発言や行為を行っていました。しかし、インターネットが普及するなかで、匿名性ばかりがクローズアップされ、ネットワークマナーやモラルに関する教育は十分であったとはいえません。その結果、匿名掲示板「2 ちゃんねる」の台頭などもあり、公序良俗に反する行為（無責任な発言や誹謗中傷、名誉毀損などの犯罪行為）の低年齢化が問題となっています。

このような人の心に潜む弱い心・不正な気持ちであるウイルスを退治するためには、技術・スキルの教授だけではなく、技術者としての倫理教育やリテラシー教育を充実させる必要があると考えています。また、そのようなウイルスに犯されない強い信念と技術者としてのプライドを持ち、佐世保高専生としての誇りを持って行動することを望んでいます。

4 章　おわりに

「無知は罪である」という言葉があります。個人や企業のコンピュータ端末がウイルスに感染し、その端末が第三者に対して攻撃してしまう可能性が指摘されています。いつの間にか、被害者から加害者になってしまう危険性が潜んでいるのです。「知らなかった」では済まされないのが責任ある大人の世界であり、己の無知が招いた不利益は責任として粛々と受け入れなければなりません。結果として、対外的な信用低下はもちろんのこと、復旧費用や対策費用が発生し多大なる影響を及ぼしてしまうのです。学生の皆さんは未来の技術者として、これらを静粛に受け止め、自ら何をしなければならないかを考え行動しなければなりません。

参考文献

[毎日コミュニケーションズ]　なぜコンピュータウイルスは悪さができるのか？
[株式会社ナツメ社]　コンピュータウイルス
[秀和システム]　UNIX ネットワークセキュリティ導入・運用ガイド

参考 URL

[情報処理推進機構]　http://www.ipa.go.jp/
[シマンテック]　http://www.symantec.com/ja/jp/index.jsp
[F-Secure]　http://www.f-secure.com/
[日経 BP 社]　http://itpro.nikkeibp.co.jp/article/USNEWS/20060301/231354/
[日経 BP 社]　http://itpro.nikkeibp.co.jp/article/NEWS/20060501/236710/