津山高専におけるネットワークセキュリティに関する現状と取り組み

宮下卓也、寺元貴幸、日下孝二、岡田正、最上勲
津山工業高等専門学校　総合情報センター
{miyasita, teramoto, kusaka, okada, mogami}@tsuyama-ct.ac.jp

１　はじめに

津山高専総合情報センター（以下、センターと略記）は、情報処理教育で利用する計算機環境の管理・運用と、基幹ネットワークの管理・運用を、主な業務としている。近年の情報利用の多様化に加え、個人情報漏洩等の深刻な社会問題の発生を受け、センターの責務はますます重くなってきている。

本校のネットワークセキュリティに関する概要と取り組みについては、これまでに幾度か報告をしてきた[1]-[5]。本稿では、その後に発生した問題やセキュリティ対策などの現状と、啓発活動等の取り組みについてまとめる。

２　セキュリティに関する現状

２．１　背景

津山高専では、プライベートＩＰアドレスでネットワークを運用している。そのため、外部から直接本校の計算機にアタックをしたり踏み台にしたりすることは、特定の計算機を除き、できないようになっている。また、学内から学外に対しての通信も、Web についてはプロキシ経由での接続を許可しているが、その他の通信は基本的に全て遮断している。このような環境であるため、セキュリティに関する深刻な事態はほとんど発生していない。

以下では、個別のセキュリティ対策と問題点に関して説明する。

２．２　電子メール

本校の電子メールサーバは、研究などの特別なものを除くと、センターにしか存在しない。それゆえ、電子メールのサービスについてはセンターで一極集中管理を行っている。最近は、コンピュータウイルスの侵入を防ぐ為、ウイルス用のファイアウォールを設置する事例が増えてきていると思うが、本校では未設置である。ただし、以下のような方針に基づき独自の方法で迷惑メール対策を行っている[6]。

＜方針１＞基本的に以下のようなホストからの電子メールについては、受信を拒否する。

- 正しい完全なドメイン名(FQDN)を持たないホスト
- 固定 IP アドレスを割り振られていないホスト
- 一度でも迷惑メールを送信（中継）したホスト
- 存在しないドメイン名を持つホスト

＜方針２＞必要に応じて、受信許可リスト(white list)や受信拒否リスト(black list)に個別に登録し、柔軟かつ迅速な対応をする。

上記の対策の結果、本校教職員および学生に対して、広告や勧誘などの迷惑メールはほとんど届いていないという声が利用者からよく寄せられている。ただし、例えば筆者のように、以前の勤務先のメールサーバから本校に電子メールを転送している場合には、本対策による効果は無く、迷惑メールが本校に届く事態となっている。

２．３　コンピュータウイルス

先述のように、本校ではウイルス用ファイアウォールを設置していない。そこで、Symantec 社の AntiVirus Corporate Edition のサイトライセンスを購入し、全学に配布している。すなわち、本校では各クライアントでウイルス対策を行うことになっている。

しかしながら、上記のウイルス対策ソフトウェアは Windows 用のものしか購入していないので、

Macintosh や UNIX/Linux の利用者については各自に対応を任せている。そのため、非 Windows 利用者の実情は把握できていない。

表１は、平成 18 年 4 月から原稿執筆時点までの約半年におけるコンピュータウイルスの検出結果のワースト５である。なお、ウイルスの名称は AntiVirus で表示されたものである。

表１　ウイルス検出結果ワースト５

(H18.4～H18.9)

ウイルス名	件数
W32.Blackmal.E@mm	107
Trojan Horse	38
VBS.Redlof.A	20
Unix.Penguin	17
Download.Trojan	15

表１を見ると、ワースト１位のものが突出していることがわかる。Symantec 社の WWW ページ[7]によると、「このウイルスはネットワーク共有を介して拡散し、セキュリティ設定を低下させようとする、大量メール送信ワームである」と説明されている。

本校の基幹ネットワークでは、Windows のファイル共有機能に対する制限を一切行っていない為、学内のどこからでも各共有リソースにアクセスできるようになっている。その結果、一度コンピュータウイルスが学内に持ち込まれると、ファイル共有機能を悪用され、学内のいたるところでウイルスプログラムの侵入が試みられることになる。その結果、ウイルス検出件数が多くなっていた。

ウイルス検出結果のワースト２位以降は、WWW ページを閲覧していた時にウイルスが発見された事例がほとんどである。特に、WWW ページの２ｃｈ[8]の閲覧中の検出が多かった。

３　セキュリティ向上に関する取り組み

３．１　電子メール

２．２節で記したように、本校の迷惑メール対策については、前職のメールサーバなど、正しく運用されているホストからの電子メールならば迷惑メールでも受信してしまうという問題がある。このような事例は、構成員数から考えれば、あくまでも稀な例である。

そこで、現状としては学外から本校へのメールを転送しているユーザに対して、ある程度の期間が経過したら学外からのメールの転送をしないように、個別に連絡を取っている。

３．２　コンピュータウイルス

先述したように、Windows のファイル共有機能を悪用するウイルスが最近多数検出されている。最初の感染源と思われるコンピュータを確認したところ、コンピュータの管理方法に問題があり、ウイルス対策ソフトウェアが正常に動作していなかったと思われる状況であった。

ただし、学内でのウイルス検出数がこれほどまでに多くなった原因は、Windows 初心者が誤って書き込み可能な共有フォルダを公開していたことにある。特に Windows XP の利用者が、セットアップ中に「共有ドキュメント」を公開していた。これについては、ファイル共有の利便性だけを表示する Windows のセットアップ画面が本質的な原因であると考える。

ともかく、感染源を特定すると共に、学内において無用な共有フォルダを公開しないようにしたところ、ウイルスの発見件数は激減した。

また、WWW ページ閲覧におけるコンピュータウイルスの危険性については、３．４節で述べる学生に対する啓発活動に注力することで、対応をしている。

３．３　教職員に対する啓発活動

本校では、平成 16 年 10 月にセキュリティポリシーを策定している。これに併せて、「セキュリティポリシー全校的実施手順」も定め、情報セキュリティに関して責任を持つ教職員に周知している。その他の教職員に対しては、平成 18 年１月に、「セキュリティポリシー職員向けマニュアル」を作成

し、学内への周知と徹底に努めている。

また、教職員を対象としたセキュリティに関する講習会を平成16年度から毎年開催している。これまでの講習会の参加人数の推移を表２に示す。

表２　セキュリティセミナーのべ参加者数

年度	１回目	２回目	合計
１６	４２人	２４人	６８人
１７	３１人		３１人
１８	２５人		２５人

注：18年度の２回目は今後実施予定

平成17年度は、2回目の講習会を開催する予定であったが、結果的に開催することができなかった。そのため、参加者数が少なくなってしまっている。ただし、本校の教職員数は110名程なので、各回の出席率は 20%以上の状況を維持していることも確認できる。

電子メールやWWWなどのサーバについては、センターでセキュリティパッチの適用作業を適宜行っている。一方パソコンについては、利用者が自らセキュリティホールを塞ぐ必要がある。そのためには、セキュリティに関する情報を知っておく必要がある。そこで、例えばMicrosoft社から毎月第2水曜日に公開されるWindowsやMS-Officeの更新情報[9]や、多くの教職員が利用しているソフトウェアのセキュリティホール情報および更新情報、Apple セキュリティアップデート[10]などを、電子メールにて教職員に一斉に通知している。

３．４　学生に対する啓発活動

学生に対しては、入学年度において学科ごとに初等教育の一環として、ネットワーク利用のマナーやエチケット、ネットワークや計算機に関係する各種法律などの説明を行っている。

実際に高専の学生がネットワーク等を利用するのは、５年生となって卒業研究に着手する頃からである。その頃には、先述の１年生の時に指導した内容はほぼ忘れてしまっている。そこで今年度は、卒業研究にこれから取り組む４年生を対象として、遵守すべき事項などを改めて指導するようにした。指導内容の一例を以下に示す。

［高学年学生への指導事項］

- ネット詐欺への注意
- Ｐ２Ｐの危険性と問題点
- アカウントの管理
- 無線ＬＡＮ利用時の注意
- パソコンのセキュリティ対策方法

上に記しているように、２ｃｈなどのWWWページ閲覧中のウイルス発見の件や、最近問題となっているＰ２Ｐ利用に関する問題に対して、特に注意を喚起している。

先に述べたように、本校ではプライベートIPアドレスで基幹ネットワークを運用している関係で、学生が学校でＰ２Ｐソフトウェアを利用することはできない。しかしながら、家庭へのブロードバンドネットワーク環境の普及に伴い、学生が自宅でＰ２Ｐを利用している状況である。そこで、これについても４年生に対して指導を行っているのが実情である。

４　おわりに

本報告では、原稿執筆時点での津山高専におけるネットワークセキュリティに関する実情について、概要を示した。

今後の課題としては、高等教育機関として、学生に対する啓発活動により一層努力し、セキュリティに関する知識・技術を身につけさせることが挙げられる。また、これまでの学校という場は、例えば学生掲示板などに個人情報として扱われるべき内容のものが、無配慮に公開されていた。個人情報保護あるいは情報漏洩防止という観点から、教職員に対しての指導・教育の強化も取り組むべき課題である。

参考文献

[1]大西淳、岡田正、“情報教育システムのセキュリティ管理と学生教育”、平成 12 年度情報処理教育研究集会講演論文集、pp.180-190、2000.

[2]寺元貴幸、日下孝二、大西淳、岡田正、“多目的なコンピュータシステムの構築と安全な運用”、平成 13 年度情報処理教育研究集会講演論文集、pp.378-381、2001.

[3]寺元貴幸、日下孝二、大西淳、岡田正、“多目的なコンピュータシステムの構築と安全な運用 II”、平成 14 年度情報処理教育研究集会講演論文集、pp.343-345、2002.

[4]寺元貴幸、日下孝二、大西淳、岡田正、“多目的なコンピュータシステムの構築と安全な運用 III”、平成 15 年度情報処理教育研究集会講演論文集、pp.614-616、2003.

[5]寺元貴幸、岡田正、日下孝二、最上勲、“情報教育システムのセキュリティ管理と学生教育 II”、平成 16 年度情報処理教育研究集会講演論文集、pp.564-567、2004.

[6]岡田正、寺元貴幸、日下孝二、最上勲、“プライバシーと視認性を考慮した迷惑メール対策と効果”、第 25 回(平成 17 年度)高等専門学校情報処理教育研究委員会研究発表会論文集、25、pp.56-59、2005.

[7] W32.Blackmal.E@mm、http://www.symantec.com/region/jp/avcenter/venc/data/jp-w32.blackmal.e@mm.html

[8]２ｃｈ、http://www.2ch.net/

[9]Microsoft TechNet、http://www.microsoft.com/japan/technet/security/default.mspx

[10] Apple セキュリティアップデート、http://docs.info.apple.com/article.html?artnum=61798-ja