津山高専における教職員のセキュリティ意識向上に関する取り組み

寺元貴幸　岡田 正　日下孝二　最上 勲

（津山工業高等専門学校 総合情報センター）

E-mail: {teramoto, okada, kusaka, mogami}@tsuyama-ct.ac.jp

概要　津山高専総合情報センターでは演習室を使った教育システムの運営・管理にとどまらず、学内LANを利用しての教育・研究や教職員に対して各種サービスを提供している。あわせて、学内全体の情報セキュリティに対する意識を向上させるために、各種の案内やセミナーを開催している。今回は情報セキュリティに関する意識調査を行ったので、この調査結果を基に高専で行うべき効果的なセキュリティ対策を検討してみたい。

1. はじめに

津山高専総合情報センターでは教育用電子計算機システム[1]-[6]をサポートするだけではなく、学内外のネットワークおよび事務系も含めた教職員への全般的なサービスなど、コンピュータおよびネットワーク利用に関する幅広い支援を行っている。昨年までに総合情報センターが行っている日常のサービスの概要を報告した[5][8]。

そのサービスの中核をなすものとして、学内における情報セキュリティの向上がある。これは、コンピュータシステムやネットワークシステムを技術的・物理的に堅牢・強固に作ること[7]も重要であるが、いくらハードウェアやソフトウェアの対策を講じたとしても、使うユーザの意識や知識が十分でなければ、それらの対策は効果を発揮することができない。また、セキュリティに関しては、全体の中に含まれるわずかな人数の設定ミスや不注意からでも重大な情報漏洩やシステム障害を起こす危険性が常にあり、100％完全な運用が期待されているという難しい点がある。

本報告では、津山高専が昨年度に行った情報セキュリティに関する取り組みを紹介すると同時に、今年度行った教職員の意識調査に関するアンケートに関して報告したい。これらのデータを元に今後どのような改善や検討が必要なのか考察してみたい。

2. 日常的なセキュリティ対策

2.1 ウイルス対策ソフト

総合情報センターの日常的な業務のうち、もっとも多くの労力が必要な仕事の1つがコンピュータウィルスの対策である。センターでは、mailサーバ等で集中的にウィルスチェックを行う方式ではなく、末端であるパソコンに最新のウイルス対策ソフトウェアを導入する方式を採用している。ウイルス対策ソフトウェアについては、契約費用の関係で平成16年度末にウイルスバスター[9]からシマンテックアンチウイルス[10]へ切り替えを行った。

ウイルス対策ソフトウェアに関しては、学内にダウンロードサーバを設置し、そのサーバ上でプログラムやパターンファイル管理をはじめ各パソコンで発見されたウイルスの報告・集計処理を行っている。平成17年5月に発見されたSasserや7月に発見されたLOVGATEの亜種以降は、影響の大きなウイルスはあまり発見されず、全体に影響が及ぶような深刻な問題は発生していない。学外からのメールもゾンビパソコンと思われるパソコンからのNETSKYが中心であり、大きな問題は発生していない。ただ、シマンテックアンチウイルスに関しては、管理サーバの設定やクライアントパソコンのアップデート機能の使い勝手がウイルスバスターとはかなり異なり、しかも複雑になっている。このため、今まで以上にシステムのメンテナンスに時間が必要となっている。

ウイルスによる問題が発生するのは、長く使われて

いなかったパソコンを学内LANにつないだときや、新品のパソコンをネットワークに接続してしばらく放置していた場合に多く発生している。そのため3.で述べるセキュリティセミナーでは特にこの部分に関して注意を喚起した。

システム管理者には管理サーバから毎日多数のウイルス発見を知らせるメールが届けられる。これらの内、次のような場合は総合情報センターからパソコンの管理者である各教職員、ならびに関係する総合上センター運営委員に現状と対策を連絡することとしている。

- 大量のウイルスが発見された場合
- システム領域でウイルスが発見され、発病の可能性が高い場合
- 不正なサイトより悪意のあるスクリプトがダウンロードされた恐れがある場合
- 明らかにマナー違反的な使い方がされている場合
- ウイルス対策ソフト自身で不具合が発生した場合

ちなみに平成16年4月～17年4月の期間に、上記のような問題によりパソコンのある場所までいって対策を講じた要件は約30件となっており、概ね1週間に1度程度といえる。電話等による問い合わせはもっと多く、詳細なデータはないが感覚的には日に数件～5件程度ある。

2.2 Windows Updateの告知

Microsoft社のWindows系パソコンに対するアップデートの情報は、深刻度が「緊急」と発表されたものか、もしくはそれに類すると判断した場合、総合情報センターから教職員全員にメールで連絡している。ちなみに平成16年度にMicrosoft社の脆弱性に関連して連絡したのは次の10回である。

平成16年4月14日:Windows の深刻な脆弱性
平成16年4月14日:Windows の深刻な脆弱性
平成16年4月21日:Windows の深刻な脆弱性
平成16年4月29日:Windows の深刻な脆弱性
平成16年4月4日:Internet Explorerの脆弱性
平成16年8月15日:Windows の深刻な脆弱性
平成16年10月13日:Windows の深刻な脆弱性
平成16年12月2日:Windows の深刻な脆弱性
平成17年1月12日:Windows の深刻な脆弱性
平成17年2月9日:Windows の深刻な脆弱性

セキュリティ情報が月例で公開される第二火曜日を中心として、ほぼ一ヶ月に一回の連絡となっている。これより少ないと正しい情報が伝わらないが、逆に多すぎると情報が無視され定着されないおそれがある。そのためあまり細かい脆弱性に関しては連絡を行わないようにしている。

3. 情報セキュリティセミナー

津山高専では、学内の教職員を対象とした情報セキュリティセミナーを平成16年度から始めた。セミナーは同じ内容を2回開催し(平成16年7月26日、9月29日)、各教職員は出席できる方に参加するという方法をとった。セミナーの内容は以下の通りであり、1時間で説明と質疑応答を行った。

「概要」
- セキュリティ向上のポイント
- ネットワークを利用する場合の注意点

「セキュリティ対策」
- 業務停止・データ破壊の防止(コンピュータウィルス、対策ソフト、学生が利用するパソコン、普段使わないパソコン、個人のパソコン)
- 情報漏洩の防止(スパイウェア、パスワード、ブラウザの設定他)
- 情報の安全性(バックアップ、パソコンやデータ、メディアの管理、パソコンの購入、廃棄)

「マナー向上」
- メールの使い方(あて先、添付ファイル、転送、外字, SPAMメール)
- サイボウズ
- ドキュメントサーバ、ファイルサーバなどの共有フォルダ(ログインユーザ名)

3.1 情報セキュリティに関する意識調査

今回、学内教職員の情報セキュリティに関する意識を調査するために全教職員にアンケート(無記名)を実施した。アンケートの項目は以下の通りである。

3.2 アンケート項目

○パソコンの利用状況に関して
Q1-1「パソコンの利用(共有・占有)状況」
Q1-2「1日の平均使用時間」
Q1-3「パソコンの管理状況」
Q1-4「ネットワーク利用の実情」
Q1-5「パソコンの管理体制」
Q1-6「パソコンのパスワード」

○コンピュータウィルスに関して
Q2-1「ウイルス対策ソフトの導入状況」

Q2-2「対策ソフトをインストールしていない理由」
Q2-3「パターンファイルの更新」
Q2-4「ウイルスが来る頻度」
Q2-5「ウイルスの感染経験」

○OSに関して
Q3-1「使用しているOSの種類」
Q3-2「Windowsシステム」
Q3-3「Windows Update」
Q3-4「卒研室のパソコン」

○総合情報センターの対策・対応に関して
Q4-1「総合情報センターからのお知らせメール」
Q4-2「お知らせメールの必要性」
Q4-3「トラブルシューティング」
Q4-4「総合情報センターの対応状況」
Q4-5「情報セキュリティセミナーの内容」
Q4-6「セミナーの難易度」
Q4-7「セミナーの必要性」
Q4-7「セミナーの必要性」
Q4-8「セミナーの時間」
Q4-8「セミナーの開催時期と回数」

○総合情報センターの対策・対応に関して
Q5-1「個人情報保護法案について」
Q5-2「学校全体の対応について」
Q5-3「内部からの機密情報漏洩を防ぐために」
Q5-4「津山高専において発生しうる問題」

○津山高専の情報セキュリティ全体（自由記述）
Q6-1「他の組織に比べ優れていると思う事柄」
Q6-2「現状では問題だと思う事柄」
Q6-3「今後の対策」
Q6-4「情報セキュリティポリシー」

3.3　アンケート結果

以上のようなアンケートに対して全教職員の約半数から回答を得ることができた。ここでは全てのアンケート結果を報告することはできないが、その一部を掲載し分析してみる。

パソコンの利用時間に関しては、約3分の1の教職員が6時間以上パソコンを使用していることが分かり、業務の多くがパソコンに依存していることがいえる。利用内容に関しては、ほとんど全員が「電子メール」「Web閲覧」「共有ファイルへのアクセス」と答えており、現在の業務がパソコンだけでなくネットワークに強く依存していることが明確となった。

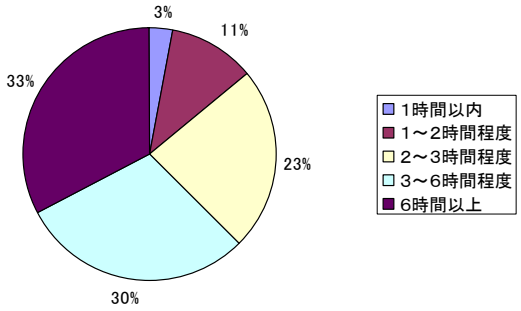

図1　1日のパソコンの利用時間

このように日常的に使われるパソコンおよびネットワークであるが、その利用状況は必ずしもセキュアとは言えない状況である。学生や他の教職員など、本人以外の他人が絶対に使えないような工夫をしているパソコンは全体の6割程度となっていて、残りの4割のパソコンに関しては、共同利用が中心であったり、他人が容易に操作できるような環境にあることが分かった。

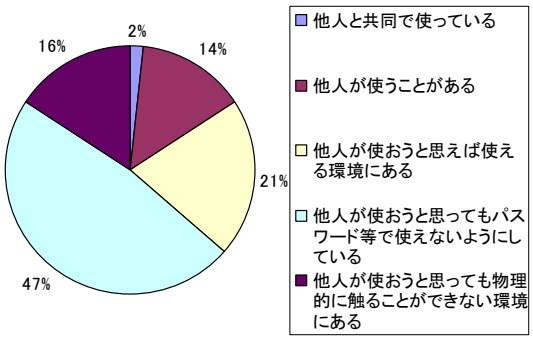

図2　業務で使っているパソコンの管理

さらに憂慮すべき状況としては、それぞれのパソコンの認証に使用されているパスワードの管理に関する問題がある。事実上パスワードが有効でないパソコンが2割、同じパスワードを使い回していて一度パスワードが発覚すると連鎖的に認証が脆弱化するパソコンまで含めると、7割以上のパソコンではパスワード認証が十分安全とは言えない状況である。

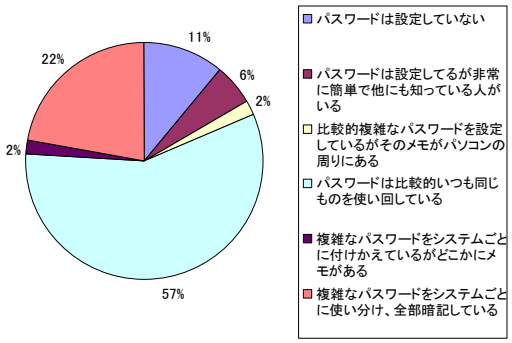

図3　パスワードの設定

これ以外にも、ウイルス対策ソフトのパターンファイルやWindows Updateに関して、ほとんど無関心と思える教職員が2～3割程度存在していることが分かった。これらの数値が高い背景には、Windowsシステムの持つ独特の閉鎖性とわかりにくさ、そして完全には自動化されていない更新システムなどに問題があると考えられる。しかし、最大の要因は認識の甘さと啓蒙不足と考えられる。

4.　あとがき

本論文では、津山高専総合情報センターが日常的に行っているサービスのうち、情報セキュリティの意識向上に関するサービスの現状を報告した。ハードウェアやソフトウェア、そしてネットワークの構成など管理者側でコントロールできる事柄に関しては毎年、少しずつではあるが向上してきていると考えている。しかし、ユーザとして特に重要な情報に触れる機会の多い教職員のセキュリティ意識は決して安心できるレベルでないことがアンケート結果から浮き彫りとなった。

今後は、ますます教職員の情報セキュリティに対する意識向上と、システムや対策に対する知識の共有化が重大なテーマとなることは間違いない。しかし、ただ単に電子メールで情報を流したり、同じようなセキュリティセミナーを多数開催してもその効果は定着しないと予想される。今後は、これらの意識をいかに効率的に徹底させるか、またセキュリティポリシーと連動させて、継続的に改善を進めることが大きな課題になると考えられる。

そのための方法として抜き打ちの火災訓練のような「実被害の出ない問題発生」が有効ではないだろうか。高専のように小規模な組織では、このような多少荒療治的な意識改革が可能であり、非常に有効と思われる。

参　考　文　献

[1]大西・岡田:“津山高専の新しい教育用システムについて”、情報処理教育研究発表会論文集、20、pp.59-62 (2000-8).

[2] 寺元・日下・大西・岡田:“広範な目的に利用可能な教育用システムの設定と運用”、情報処理教育研究発表会論文集、21、pp.178-181 (2001-8).

[3] 寺元・岡田・日下・大西・最上:“教育用システムの運用と新キャンパスネットワークの構築”、情報処理教育研究発表会論文集、22、pp.111-114 (2002-8).

[4] 寺元・岡田・日下・最上:“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 (2002-10).

[5] 寺元・岡田・日下・大西淳・最上:“総合情報センターにおける各種サービスとセキュリティ対策について”、情報処理教育研究発表会論文集、23、pp.74-77 (2003-8).

[6] 寺元・岡田・日下・最上:“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 (2003-10).

[7]岡田:“安全性と保守性を考慮したネットワークサーバの更新”、情報処理教育研究発表会論文集、21、pp.182-185(2001-8).

[8] 寺元・岡田・日下・大西・最上:“総合情報センターにおける各種サービスとセキュリティ対策についてII”、情報処理教育研究発表会論文集、24、pp.209-212(2004-8).

[9]トレンドマイクロ株式会社:
http://www.trendmicro.com/jp/home/enterprise.htm.

[10]株式会社シマンテック:
http://www.symantec.co.jp/