校内ネットワーク関係危機事例と考察

情報処理センター員（専門技術班）大渕　寛

１．はじめに

佐世保高専の LAN が整備されたのは平成８年（西暦 1996 年）３月である。パソコンがネットワークに接続されている事が当たり前の時代になってから既に 10 年以上も経った。今や LAN やインターネット無しでは事務や教育ができないほどの状況であり、ネットワークに関係するトラブル等の発生がすぐに学校の危機となることもある。この約 10 年間で本校でも多くの問題が発生した。悪意のあるプログラムや侵入に対抗するためセキュリティシステムが必要になり、設備投資が増大した。また、文字によるコミュニケーションでのトラブルが多発したことは意外であった。外部に迷惑をかけた例や誘惑や脅しを受けた例もあった。これらは技術による対処ができる範囲外なので、利用者への教育や相談対応などが必要になる。校内 LAN の構築後に校内で新たに発生した問題の中から学校の危機と言える事例をあげて総括すれば、今後の危機への対策に役立つのではないかとないかと考えた次第である。

２．事例の分類

情報処理センター運営委員会の記録や校内の通知文、電子メールの記録から危機と言える事例を抜粋してみると、性質により次の４種類に大別できる。

①技術の悪用による被害や脅威

これはプログラムや通信の技術を悪用した類で、被害発生時には加害者の手から離れて自動的に被害を拡大していることがほとんどである。コンピュータウィルスが代表的な例で、感染後の通信による攻撃やホームページの改ざんも含む。スパイウェアやアドウェアと呼ばれるものも同じと考える。校内マシンに蔓延しなくても、威力のあるものが世界的な流行になればその脅威だけでも危機と言える。

②コミュニケーションによる被害やトラブル

インターネットでは電子メールやホームページなど文字情報によるコミュニケーションは黎明期から現在まで主要な位置を占めている。インターネットによって、良くも悪くも文字や文章が持つ力が大変大きいことが証明された。悪意があって他人を騙したり威嚇したりするのは分かりやすい例であるが、悪意が無くても議論や批評によりトラブルを起こすこともある。ほんの一言で被害者と加害者が逆になるともある。うかつに書いた冗談が人を傷つけることもある。掲示板やチャットでのトラブルが代表的なもので、電子メールの場合もある。学校の信用に関わる問題に発展すれば正に重大な危機と言える。

③インターネットの罠

公開サイト上で悪意を持って待ち構えているタイプで、言葉や画像で誘い込む点は

「②」の要素と言えそうであるが、応答のプログラムや被害者の端末情報を収集する機能がある点では「①」の要素も持っている。代表的なものはフィッシングと呼ばれるもので、被害者は不当請求を受けたり脅されたりする。被害は心理的なものだけで、プログラムが端末に残ることがないタイプである。スパイウェアやアドウェアと呼ばれるものは似ているが、プログラムとして端末に残って活動を続けるタイプなので、それらはウィルスと同じく「①」の分類と考える。

④西暦 2000 年問題

これは滅多にない特別な例であるが、全てのコンピュータで心配された問題であったことから、今までで最大の危機であったとも言える。西暦 1999 年（平成 11 年）末までに対策を終える必要があったので大きな重圧になった。

以下、この分類に従って本校での事例をとりあげる。これら四つのタイプは根本的に原因が違うのだが、しかし高専規模のネットワーク管理者にとっては同じようにネットワーク関係の危機として対応しなければならない問題である。

３．事例紹介

３－１．技術の悪用による被害や脅威

３－１－１．MTXウィルス被害

（１）経緯

- 平成 12 年（西暦 2000 年）９月 20 日、教員室（当時は教官室）の３台のパソコン(Windows)で被害が発生した。本校では初めてのコンピュータウィルスによる被害となる。受信した電子メールの添付ファイルを実行したことにより感染したことが分かった。
- OS のダメージは深刻でウィルス・ファイルの除去は容易ではなく、ウィルスはアクセス妨害やメールの自動送信の活動を示した。
- まだウィルス対策ソフトが校内に普及していなかったので、ウィルスのファイルをフロッピーディスクにセーブして、ウィルス対策ソフトがインストールされたパソコンで検査して確認した。その後急遽ウィルス対策ソフトを購入して駆除にあたった。
- ９月 21 日、被害調査と通知を兼ねた文を電子メールと掲示により全教職員に周知した。
- ９月 28 日、当該ウィルスの被害について本省に報告した。
- 10 月５日に「コンピュータウィルス説明会」を教職員向けに開催して各種コンピュータウィルスの対策の説明や対策を紹介した。

（２）考察

- それまでにウィルス対策ソフトが必要であることは何度も聞いていたにもかかわらず、これを導入していなかったために被害を受けたと言わざるを得ない。これをきっかけに端末へのウィルス対策ソフト導入を組織的実施するようになった。
- 「コンピュータウィルス説明会」を開催したことによりユーザの関心が高まった。

３－１－２．ホームページ改ざん被害

（１）経緯

・平成 13 年（西暦 2001 年）５月 7 日、本校行政文書ファイル公開用ホームページが改ざんされる被害が発見された。後で同様の被害がほとんど同時に全国で 27 箇所で発生していたことが分かった。幸い被害発生から約 30 分後に異状を発見してサーバを停止したので改ざん後のホームページを長時間外部に見せずに済んだ。

・これは sadmind/IIS　worm　と呼ばれるワームに犯された外部のサーバから自動的に侵入され、www サーバである IIS の脆弱性につけこまれたことによる被害であった。

・被害について本省や県警に報告し、県警からの調査を受けた。

（２）考察

・被害を受けたページのサーバにセキュリティホール修正用のパッチがあたっていなかったことが分かった。本校公式ホームページは複数のサーバ上のページをリンクして構成していた。サーバの管理分担が曖昧になっている部分があり、それで点検が手薄な状態になっていたと反省された。

３－１－３．世界的流行のコンピュータ・ウィルスが多数出現

（１）経緯

・平成 13 年～ 15 年（西暦 2001 年～ 2003 年）にかけて世界をパニックに陥れるほどのコンピュータウィルスが次々と出現した。本校でも大きな脅威と認識し警戒通知や対策支援を実施した。ウィルスの種類毎に時系列に記録を書き上げれば次のとおり。

KLEZ（クレズ）に関する記録

平成 14 年４月 22 日　当該ウィルスが添付された電子メールが校内で受信される。

平成 14 年５月１日　当該ウィルス対策等の情報を本センターから電子メールで全教職員に配布する。

平成 14 年７月 18 日　当該ウィルスが校内のパソコンに潜伏していることが心配されたので、検査と駆除方法の説明文を電子メールで全教職員に配布する。

メールサーバにウィルス対策を施す

平成 14 年６月 28 日　メールサーバでウィルス検査・駆除を開始（TrendMicro InterScanVirusWall を使用）

Frethm.K（フレゼム・K）に関する記録

平成 14 年７月 15 日　当該ウィルスが添付された電子メールが校内で多数受信される。すぐに校内放送で警戒を呼びかける。

平成 14 年７月 17 日　当該ウィルスやその他のウィルス対策を利用者に促すために「コンピュータウィルス対策のお願い」と題した対策説明文を電子メールで全職員に配布する。これで MS-Outlook, Outlook expressd での電子メールのプレビューによる自動実行を防ぐための手順などを説明する。

（２）考察

・ウィルス対策ソフトをメールサーバで稼働していても最新のもに対応できないことがあり、対応できる定義ファイルを取得するまでの間に端末で受信してまう。これに対しては、まずユーザからの通報を受けてから速やかに警報を校内に周知することが肝要だ。周知手段としては校内放送が最も確実だった。即時性があり注意喚起の効果が高い。そして電子メールで重ねて周知することにより効果を上げることができた。

３－１－４．MSブラストの脅威

（１）経緯

平成 15 年８月 13 日　当該ウィルスの被害が世界中で急激に広がっていることが報道される。世界中がパニックに陥るほどの大ニュースとなった。非常に感染力が強く、電子メール添付に頼らずいきなりネットワークのラインから侵入して感染するという点が最大の特徴であり、恐れられた。

平成 15 年８月 18 日　当該ウィルスの蔓延状況と対策について短い説明文を電子メールで全教職員に配布する。

平成 15 年８月 19 日　長崎大学で当該ウィルスによる大きな被害が発生したという情報を受け、更に詳しい対策説明文を電子メールで全教職員に配布する。

平成 15 年８月 21 日　当該ウィルス対策のために Windows の修正パッチやウィルス駆除ツール（無償公開されたもの）をまとめた CD を作成し、校内要所に配布する。これによるパソコン検査や Window のセキュリティパッチあての作業を校内全部のパソコンに実施した。

平成 15 年９月 18 日　専攻科学生が使用しているノート型パソコンで当該ウィルスが発見される。校外で感染し、幸いその後は校内 LAN には接続していないことが分かった。

（２）考察

・本校 LAN はファイヤーウォールで守られているので外部インターネットからの直接の被害は心配は低かった。しかし、外部からの持込パソコンや記録メディアからの感染が心配された。むしろ今までファイヤーウォールで守られていたことにより、校内にはウィルス対策ソフト無し、かつ Windows のアップデートを怠っているパソコンでも危機感なく使われていたことが問題となった。もし校内で１台でも犯されたら、それから一気に被害が拡大する恐れが十分にある。本校 LAN は例えれば抵抗力の無い子供を大勢かかえている保育園のような立場になっていたと言える。

・結果として被害が１件だけで済んだことは幸運であったかもしれないが、対策用 CD 配布などの実施の効果があったとも考えられる。

結果として得られた教訓は次のとおり。

・まず初めに脅威の情報を速やかに校内に周知することが肝要である。情報不足の時点でも分かる範囲内の情報を周知すれば危険を回避できる。
・ファイヤーウォールで守られた校内のパソコンは端末単位での防御が疎かになりやすい。
・フロッピーディスクや CD-ROM などのメディアからのウィルス感染を組織的に防ぐためには、ウィルス対策ソフトと共にユーザへの教育が必要だ。
・OS は、特に Windows は頻繁にアップデートにより常に脆弱性を無くすよう努めなければならない。
・各自の全てのパソコンにウィルス対策ソフトをインストールして、かつウィルス定義ファイルを最新に保たなければならない。

３－２．コミュニケーションによる被害やトラブル

３－２－１．ネズミ講メール事件

（１）経緯

・平成 12 年（西暦 2000 年）11 月 29 日、本校学生２名がいわゆるネズミ講の勧誘メールにそそのかされ、友人などに同様のメールを出して勧誘していたことが発覚した。その手口は、自分の銀行口座と勧誘文を書いたメールを多数の相手に送って無限に拡大しようとするものであった。しかしその勧誘メールを受けたある人が親切に本校に知らせてくれたことで発覚した。
・12 月１日、学校側はその行為が極めて違法性が高いことに気づき、すぐにその銀行口座を閉鎖させ、校内には事件の概要と警告を書いたメールを全教官に配布した。
・結局、実際の金銭被害が発生する前に行為をやめさせることができた。

（２）考察

結果として得られた教訓は次のとおり。

・インターネットでは誰もが簡単に犯罪を犯してしまう危険がある。
・ネチケットとしてチェーンメールを許さないという意識が学生にあれば問題は発生しなかったと考えられる。
・学生に対してネットワークを利用する場合の倫理教育が絶対に必要である。当該学生は問題を起こした時点では罪を意識していなかった。

３－２－２．外部掲示板での誹謗中傷

（１）経緯

・平成 18 年（西暦 2006 年）７月 12 日、外部掲示板に本校名を題名に含む掲示板が存在し、ここで本校学生や OB によると思われる個人攻撃や無責任な発言が発見された。被害者の保護者からの苦情を本校が受けたことで発覚した。
・７月 20 日、教務主事を中心としてネットワークマナーの掲示をしするとともに、学生全員を集めて説明会を実施。
・９月８日、問題の掲示板（２ちゃんねる）で更に本校学生に危害を加える予告と思える記述が発見された。そしてその応答として警視庁に通報をしたことが書き込まれていた。

・９月 11 日、サイバーテロ専門の刑事（佐世保署　二人）が来校し情報処理センター長と面談した。
・９月 12 日～１５日、全学生に対し教務主事がネット犯罪に関する説明会を実施。
・その後は幸いにも事件は収束したが、問題の掲示板には本校学生に危害を加える予告とも思える記述があったので、しばらくは警察と学校側で警戒態勢とった。

（２）考察

・警察が出動する事件に発展し、ネットワーク社会の危険性を目の当たりにした事件であったが、本校としても危険を認識したので積極的に警察に相談し、経緯や対策を説明した。速やかに学校方針を決定して協力したことで事態を悪化させずに済んだと考えられる。

結果として得られた教訓は次のとおり。

・インターネット上に公開された掲示板の書き込みは、書きようによってはほんの短い文章だけでも威力業務妨害という犯罪行為になることがある。
・学生への倫理教育が重要なことはもちろんで、その上に各種事件の実例をあげて違法性や結末を説明する必要がある。
・違法性や危険性が明らかならば警察への通報も必要になる。

３－２－３．その他web上での記述によるトラブル等

（１）経緯

平成 12 年（西暦 2000 年）頃から校内外の掲示板での発言や学生が運営する非公式なホームページでの記述で非常識な表現が問題になることが多数あった。特に悪質なものの例をあげれば次のとおり。

・ギャンブルなど学生としてあるまじき趣味へ固執したホームページ公開やリンクの設置
・ソフトウェアの違法複製を誘いかける記述
・担任教師や学友について個人を特定できる文脈で誹謗中傷

特に掲示板での誹謗中傷が多発し、深刻な悩みを抱える被害者が出たので学校側は校内での掲示板システムを禁止した。

（２）考察

コミュニケーションでのトラブルに共通して見られることとして、

「軽い気持ちでやってしまった」ことがあげられる。しかしこれが後で大きな問題に発展することがある。文字情報では実際に物を盗んだり物理的な暴力のような手ごたえが無いので、うっかり一線を越えてしまうと考えられる。

このようなモラルに関する問題は学生への教育によって改善される例が多かったが、しばらくするとまた次の事件が起こった。学生には最低年に１回は情報倫理に関する教育を行う必要がある。

３－３．インターネットの罠

（１）経緯

・平成 17 年度初め頃から外部ホームページ上のアイコンをクリックしただけで「あなたは会員に登録されました。」、「すぐに会費を振り込んでください。」、「会費滞納の

場合は直接請求に伺います。」などのメッセージが表示されたという報告が多数あった。
・客観的に見るとメッセージは単なる脅しであることはすぐに分かったが、被害者の心理的ダメージは大きい場合が多かった。
・対策として電子メールと掲示でフィッシングの説明を周知した。

（２）考察
・フィッシングの存在を知らない者がこれに会うと心理的なショックが大きいようだ。そのときアクセスしたサイトが如何わしい場合が多いので、学生の場合は特に相談を躊躇することが多いと考えられる。その結果、被害者が大きな精神的ダメージを受けてしまうこともあるかもしれない。知っているだけでダメージは少ないはずだ。
・情報の周知で被害は聞かなくなったが、毎年繰り返し周知しておく必要があると考えられる。

３－４．西暦2000年問題
（１）経緯
・平成 11 年（西暦 1999 年）１月８日、教育用電子計算機システムの MS-Windows3.1 を使ったコンピュータ（クライアント PC ×４９台、サーバ１台）について当該問題の有無と修正費用の調査を開始。以後校内各システムについても調査する。
・９月１日、情報処理センターに「西暦 2000 年問題対策室」なる組織を設置。
教官２名と技官２名の構成
・９月２日、第１回西暦 2000 年問題対策室会議
・９月 17 日、当該問題についての連絡用にメーリングリストを設置。
メンバーは西暦 2000 年問題対策室員の他、教官２名と事務官２名。
・11 月 11 日、第１回西暦 2000 年問題対策室会議
・12 月 27 日、全てのシステムで対策を終了したことを確認
・平成 12 年（西暦 2000 年）１月１日、校内 LAN と教育用電子計算機システムについて点検したが、異状を認めなかった。
・１月８日、一部のメーリングリストで動作異常が発見された。メーリングリストのプログラムのバージョンアップ漏れが原因と分かり、即日修正できた。

（２）考察
・今から考えると、ネットワーク関係危機としては最初で、それも大規模な例であったと言える。このとき設置した対策室やメーリングリスト、対処の記録はその後の危機で度々参考になっている。
・最終的に特に大きな問題は発生しなかったので、情報処理センターに「西暦 2000 年問題対策室」を設置して対策を促進した成果があったと思われる。
・メーリングリストにより情報交換することにより校内各方面への情報周知が促進された。
・各システムのプログラム修正はほとんど漏れなく完了できたと思っていたが、UNIX サーバの各ユーザのホームディレクトリ内にあるプログラムまでは点検していなか

ったので、一部のメーリングリストで異状がでた。
・問題に対する対策室など、まず組織を編成することによって構成員の責任感が生まれ、対策が促進されたと考えられる。

４．おわりに

本年６月８日、校内の FD 講演会で危機管理についての講演があった。本稿での問題は正にこの危機にあてはまることばかりなので、この講演を聞いて合点することが多かった。公演での語句を思い出せば、確かにネットワーク関係の危機にも当てはまるものと思われる。

以下は広報・危機管理アドバイザー伊原正俊先生によるその講演内容の抜粋である。

> ① ハインリッヒの法則（大事件とその底部にある多数の前兆事件の件数についての法則）を理解し、大事件を防げ。
> ② リスクの芽に気づく「異変センサー」を全職員一丸となって高めよう。
> ③ コンプライアンス（社会秩序を乱す行動や社会から非難される行動をしないこと）を常に念頭に置くこと。
> ④ 我らの常識ではなく、社会の常識で判断せよ。

上記引用の言葉をネットワーク関係危機にあてはめれば次のようなケースが想像できる。

①： ユーザからの報告やサーバからのメッセージを軽視しないよう心がけ、危機発生の前兆を見逃さないこと。サーバや通信装置の異状の発見、コンピュータウィルスの蔓延防止など。

②： 危険の要素に誰かが気づけば、問題が大きくなる前に対処でき、危機となる前に解決できる。コミュニケーションによるトラブルなどが大きくなる前に対処すること。

③： 特に学生に倫理や法律について教育することにより、文字表現での外部とのトラブル、ホームページの低俗化を防止する。

④： LAN はインターネットで全世界に繋がっているのだから、文字どおりである。web での非常識な行動や態度をマスコミなどで叩かれる場合もあるだろう。