＜実践報告・資料＞

職業能力開発における情報セキュリティ教育の実践報告

ー職業能力開発総合大学校電子計算機室での取り組みについてー

浜松職業能力開発短期大学校　三木　寅太

Report on the Practice of Intelligence Security Lesson in Vocational Training
—Contents on Activities in the Computer Room of Polytechnic University—

Torata MIKI

要約　今日、世界的なサイバー攻撃の多発に伴い、情報セキュリティのリスクが高まっており、情報セキュリティ教育の重要性がクローズアップされている。職業能力開発総合大学校（以下、「職業大」）においては、平成 21 年度からユーザの情報セキュリティへの意識を高めることを目標に情報セキュリティ分野の専門家を講師に招いて講習会を開催している。講習会では、情報セキュリティの基礎知識に加えて、最新の情報セキュリティのリスクについてもその発生要因および防止策を内容に盛り込んでいる。本報告では、職業大で取り組んできた情報セキュリティ教育について報告するものである。

Ⅰ　はじめに

インターネットの普及に伴い、利便性が高くなった反面、サイバー攻撃による情報セキュリティのリスクが高まっている。最近はマスコミでも頻繁に情報セキュリティインシデントについて取り上げられており、遠隔操作ウィルスインシデント、官公庁・大企業における個人情報漏洩インシデント等がある。これらのインシデントの多くはユーザの情報セキュリティへの意識が不十分なことが起因している。

最近は攻撃手法が巧妙になっており、情報セキュリティに関する基礎知識を持っているユーザであっても、最新の巧妙な攻撃手法を認知していなかったためにインシデントの被害者となるケースがある。セキュリティインシデントにおいては、被害者が知らないうちに次の加害者になることも多い。

今やシステムのみで完璧にセキュアなコンピュータネットワークシステムを構築することは困難であり、システムを利用するユーザ一人一人が情報セキュリティについて正しい知識を持ち、適切な情報セキュリティ対策を実施し、更には常に最新の情報セキュリティインシデントの要因や留意事項等について熟知してコンピュータネットワークシステムを利用していくことが重要である。職業能力開発の分野においても安全衛生教育同様、情報セキュリティ教育も重要である。

本報告では、職業大電子計算機室において平成 21 年度から学生および教職員を対象に取り組んできた情報セキュリティ教育について報告するものである。

Ⅱ　背景

職業大には教育訓練および研究用のコンピュータネットワークシステム（以下、「電子計算機システム」）の導入・運用管理・ユーザサポートを主な業務としている電子計算機室という部署がある。筆者は平成 20 年 4 月から平成 27 年 3 月まで電子計算機室で業務に携わっていた。この章では、社会で多く被害が報告されているセキュリティインシデント、筆者が実際に遭遇したことのあるセキュリティインシデントおよび筆者が在籍していた時に職業大電子計算機室で取り組んでいたセキュリティ対策の一部を紹介する。

職業大では、教育訓練用のメールアカウントを個人

論文受付日　H27.12.18

に付与して利用しているが、平成 20 年度頃から迷惑（スパム）メールが多数届くようになった。当時導入していたスパム対策フィルタでスパムメールのブロック作業を試みたが、スパムメールの種類が多く、完全にブロックするまでには至らなかった。この傾向は職業大だけでなく、社会全体の問題となりつつあった。多様化し増大する迷惑メールに対してメールシステムに様々な対策が講じられてきたが、対策が講じられると更に巧妙な手段で迷惑メールが送信されるようになるという繰返しが現在も続いている。迷惑メールに対してはスパム対策フィルタやウィルス対策ソフトに頼るだけでなく、ユーザ自身が危険なメールを察知することが必要である。

筆者はこれまでに様々なコンピュータウィルスに遭遇したが、中でも一番グロテスクだったのは、パソコンで作業をしていると動作が突然遅くなり、デスクトップにゴキブリが 1 匹、2 匹、4 匹、8 匹・・・と現れてデスクトップ上を動き回るウィルスであった。ドイツのサイトからファイル等をダウンロードした後に現象が発生したとのことだったので、ウィルスを含むファイルをダウンロード・実行して感染したものと思われる。このコンピュータウィルスはグロテスクではあるが、端末がウィルスに感染していることが一目で分かるので、対策をとりやすいウィルスと言える。コンピュータウィルスが登場した当時は、このような一目で分かるウィルスが多かったが、攻撃者の観点では、一目で分かるウィルスは短期間でユーザに対処されてしまうため、次第に、感染したことがユーザに分かり難いウィルスが広く蔓延するようになった。

データを保存するメディアとして USB メモリが普及すると、USB メモリを介して拡散するコンピュータウィルスが多く現れるようになった。筆者も様々な USB メモリ経由のウィルスに遭遇したが何れも対処に労力を要した。一つ目のケースとして、ウィルス対策ソフトで検索はできるが、駆除・隔離できないケースがあった。セキュリティベンダーのウィルスデータベースで対処方法を確認し、マルウェアにより変更された可能性のあるレジストリの修正等を試みたが、解決には至らなかった。最終的にシステムをリカバリして解決させた。また、二つ目のケースとして、ウィルス対策ソフトで検索できないウィルスもあった。新種のウィルスでウィルス対策ソフトが未対応だったものと思われる。システムをリカバリして解決させた。

USB メモリは便利であるが、このようなウィルス感染のリスクがあるため、使用は控えるべきである。また、コンパクトで携帯性に優れているため、USB メモリにデータを保存して学外に持ち出すことも可能ではあるが、誤って紛失して情報漏洩につながるケースや、学外の端末がウィルス感染していて USB メモリにウィルスが仕掛けられるケースも十分に想定されるので、USB メモリの持ち出しは行うべきではない。

最近は、メールの添付ファイルからウィルスに感染するケースも見受けられる。以前は、件名（subject）が英語のメールにはウィルスが仕掛けられている可能性があるので注意した方が良いと言われていたが、今や、英語のメールだけではなく、一見、業務関係と思われる日本語のメールにウィルスが仕掛けられていたり、不正サイトへ誘導されたりすることがある。このようなメールを誤って開き、添付ファイルを見るように指示されていたため、開いたところ端末がウィルスに感染するケースが多発している。また、メール本文内のリンクを読むよう誘導し、そのリンク先サイトにアクセスすると、端末がそのサイトに仕掛けられているウィルスに感染するケースも多発している。この種のメールの事を標的型メール攻撃と呼んでいる。

官公庁・企業の Web サイトが改ざんされてウィルスが仕掛けられるケースも多発している。平成 24 年に国外と推測されるサイバー攻撃集団から、官公庁等が公開している複数の Web サイトに対してサイバー攻撃が予告されたことがあった。その中には職業大に関係する Web サイトも含まれていたが、その後そのサイトへの攻撃はなく、実際に被害を受けることはなかった。

多数のウィルスに感染していて危険であるという偽の警告メッセージを端末の画面上に表示し、ユーザに偽ウィルス対策ソフト（実質はウィルス）をインストールさせるという手口による被害も一般には多く発生している。遭遇したことはないが、端末のハードディスクを暗号化して、暗号化解除のためお金を要求する身代金要求型のランサムウェアというウィルスが現在流行している。この手のウィルスのほとんどは、お金を支払っても元には戻らない。データの内容にもよるが、クラウドのファイルサーバ等も活用して、端末内の必要なデータを二重・三重にバックアップしておくことが求められる。

パソコン以上に個人情報が詰まっているスマートフォンやタブレット端末の情報セキュリティ対策も重要である。ソーシャル・ネットワーキング・システム（SNS）も身近なツールになっているが、これらのツールを扱う際の情報セキュリティ対策およびマナーにつ

いても正しく理解しておく必要がある。

情報セキュリティ対策の基本として、端末へのウィルス対策ソフト導入が挙げられる。マスコミでも頻繁に取り上げられているため、ユーザの常識となりつつあるが、端末購入時にプレインストールされているウィルス対策ソフトを、期限切れで無効になっていることに気付かずに使い続けてしまうユーザが一般にはいるようである。また期限切れで無効になっていることは認知しているが、費用を支払うのが勿体ないため、そのままにしているユーザも中にはいるようである。職業大では、主要な OS に対応したウィルス対策ソフトを電子計算機室が管理するサーバで提供しているため、有効期限が切れたウィルス対策ソフトは利用されていないと思われる。しかし、学生が個人で保有するパソコン等はセキュリティ対策が不完全である可能性がある。そのような端末で作成されたファイルを、USB メモリ等を介して、教職員の端末にコピーするという行動も危険だと考えるべきである。

また、以前は、オペレーティングシステム（OS）やアプリケーションソフトへのセキュリティパッチ当て作業の重要性を認知していないユーザも見受けられた。平成 15 年頃に猛威を振るった MSBlaster (Blaster) および Wechia (Nachi) と呼ばれるワームは、OS の脆弱性を悪用したもので、セキュリティパッチを当てていないパソコンに爆発的に感染が広がった。このインシデントにより、OS のアップデートの重要性が一般のユーザにも認識されるようになった。しかし、セキュリティパッチが公表されて間もない脆弱性を狙った攻撃や、公表される前の脆弱性を悪用する攻撃（ゼロデイアタック）も現れている。ユーザは、常に最新のセキュリティパッチを適用するとともに、被害を受けてしまった場合の対策も考えておく必要がある。

職業大の学生には、入学時のオリエンテーションでの説明時に、教職員については転入時に書面で、また適時メールや学内ポータルサイトで情報セキュリティ対策について周知した。

職業大では独自に様々なセキュリティ対策を講じていたが、その一つは個人認証を確実に行うため、ワンタイムパスワードシステムを導入したことである。職業大が採用したワンタイムパスワードシステムでは、ユーザにトークンあるいはカードを配布して、ユーザがシステムにログインする際にトークンあるいはカードが出力する 6 桁のパスワードとユーザに固定で割り当てている PIN 番号 4 桁の合計 10 桁をパスワードとして使用するものである。トークンあるいはカードが出力する 6 桁のパスワードは約 1 分間のみ有効で、約 1 分間過ぎるとそのパスワードは無効になり、次に使用するときは異なるパスワードとなる。現在では、トークンやカード等のハードウェアは使用せずソフトウェアを使用するシステムもある。

職業大ではこれまで重大な情報セキュリティインシデントは発生していなかったものの、学内で重大な情報セキュリティインシデントが発生した場合、機構および大学校の信用が低下し、社会的な責任が果たせなくなることが懸念される。電子計算機室では、システム側でセキュリティ対策を実施するだけでなく、ユーザである教職員や学生の情報セキュリティに対する意識を高め、ルールやマナーを再確認してもらうことが重要であるとの認識を共有した。そこで、次章に示すセキュリティ講習会を企画するとともに、キャンパスの小平移転に併せ、平成 25 年度に電子計算機システム運用ガイドラインを策定した。

Ⅲ　講習会の企画・実施

情報セキュリティに関する情報は、参考文献に URL を示す警察庁セキュリティポータルサイト @police[(1)]、独立行政法人情報処理推進機構（IPA）情報セキュリティサイト[(2)]、JPCERT コーディネーションセンター[(3)] 等の Web サイトから取得することができ、全ユーザがこれらのサイトをこまめに閲覧して適時対応すればよいが、一般ユーザにそれを求めるのは難しい。

独立行政法人高齢・障害・求職者雇用支援機構が業務用に構築している情報ネットワークのように、学内の全端末を一括管理して端末起動時に OS 等のバージョンを管理して情報セキュリティ対策が必要な端末については、起動直後に自動で実施する仕組みを構築していれば、ユーザが意識することなく情報セキュリティを高めることができる。一方、職業大の電子計算機システムには、コンピュータだけでなく、ネットワークを介して制御される機器等が接続され、訓練や研究のためにさまざまなアプリケーションソフトが利用されていた。利用目的や利用形態がさまざまであるため、OS やアプリケーションソフト等を電子計算機室で一律に管理することは難しい状況であった。このような状況でセキュリティレベルを一定以上に保つためには、教職員や学生等のユーザに対して、情報セキュリティ教育を行い、コンピュータ利用時のルールやマナーを再確認してもらうことが重要であると考えた。

以上を鑑み、学内のユーザの情報セキュリティへの

意識を高める一つの方法として情報セキュリティ講習会の開催がよいのではないかとの結論に至り、電子計算機室主催で情報セキュリティ講習会を企画することにした。情報セキュリティ講習会の企画に際し、最新の情報セキュリティ事情を熟知していて、他企業においても講義実績のある情報セキュリティ分野の専門家に講師を担当してもらうのが妥当との結論に至り、情報セキュリティ関連企業から講師を派遣してもらい開催することとした。講習時間は、休憩も入れて 90 分～ 120 分程度で企画した。

表 1 に各年度の講習会の受講対象者と主眼を置いたテーマを示す。毎回において、その年度のニュース等で取り上げられた大きなインシデントからニュースには取り上げられなかったが情報セキュリティの分野では注目されたインシデントについて内容・要因・防止策等について解説するようにした。また、開催時期に特に注意すべき事項を講習会の内容に含めるようにした。

平成 21 年度については受講対象者を教職員のみとし、可能な限り各科・各部署 1 名以上受講してもらうようにした。年度末で業務多忙なこともあり、電子計算機室で想定していた人数は集まらなかったが、概ねの部署で最低 1 名は参加してもらった。平成 23 年度以降については、対象を教職員だけでなく学生も含めることにした。

平成 24 年度は、話だけではなく実際にウィルスのデモもしてもらい受講者の関心を引くようにした。また、年度末にキャンパス移転が控えていて、端末、CD・DVD・USB メモリ等の情報メディアの廃棄が想定されたため、端末、情報メディアを廃棄する際の留意点についても内容に盛り込んだ。

平成 25 年度は、翌年 4 月に特定のバージョンの OS がサポート終了となることから、サポートを終了した OS をコンピュータネットワークに接続して使用し続けることのリスクと対処方法を内容に盛り込んだ。併せて、学生･教職員の多くが利用しているソーシャル･ネットワーキング・システム（SNS）利用においての情報セキュリティ対策についても内容に盛り込んだ。講師の許可が得られた場合は、配布資料をメールまたは学内ポータルサイトで配信し、講習会に参加できなかった受講者に情報提供した。

講習会の効果の定量的な測定はしていないが、ユーザの情報セキュリティに対する意識は講習会前と比べて一層高まった感触があった。講習会以前より､学生･教職員からの情報セキュリティに関する問い合わせが増えた。学生・教職員が情報セキュリティに対してより敏感になった感触があった。各年度につき 1 回のみの開催であり、受講ユーザは限られているが、受講者から未受講者に口頭で伝わっている感触もあった。

Ⅳ　職業能力開発における情報セキュリティ教育について

海外からのサイバー攻撃や、官公庁・大学・企業における個人情報漏洩がマスコミで取り上げられたこともあり、官公庁･教育機関･企業において、情報セキュリティ保持の重要性は改めて認知されつつある｡また、マイナンバー制度の導入により、更なるサイバー攻撃の増加が見込まれる。組織の情報セキュリティ維持に欠かせないことは、組織内の全員が自分の組織における情報セキュリティに関するルールを遵守し、なおかつ､最新の情報セキュリティ対策について十分理解し、現場で実践できる必要がある。

表 1　各年度の講習会の受講対象者と主眼を置いたテーマ

年度	受講対象者	主眼を置いたテーマ
平成 21 年度	教職員	最新の情報セキュリティ事情および情報セキュリティ対策の基本
平成 23 年度	教職員、学生	
平成 24 年度	教職員、学生	最新の情報セキュリティ事情およびキャンパス移転に際して留意したいパソコン・フロッピーディスク・CD・USB メモリ等の廃棄方法
平成 25 年度	教職員、学生	最新の情報セキュリティ事情、OS のサポート終了に伴うリスクと対処方法、ソーシャル・ネットワーキング・システム（SNS）利用に際して知っておきたい情報セキュリティ
平成 26 年度	教職員、学生	最新の情報セキュリティ事情および情報セキュリティ対策の基本

職業能力開発の分野においても､安全衛生教育同様、情報セキュリティ教育にも力を入れるべきで、通常の訓練に支障を来たさないよう短時間で習得可能な情報セキュリティ訓練カリキュラムモデルを構築するべきである。ものづくりの分野でもコンピュータネットワークは欠かすことができない存在になっており、コンピュータネットワークを使用する以上、情報セキュリティのリスクを有するためである。

これまでの経験から筆者は、情報セキュリティの訓練は、基礎知識の訓練、実践技術の訓練、最新対策の訓練の 3 本立てで実施する必要があると考える。基礎知識の訓練においては、情報セキュリティ保持の基盤となる知識を座学形式で訓練する。実践技術の訓練では、情報セキュリティ保持に必要な実践技術を実習形式で訓練する｡最新対策の訓練では､最新の情報セキュリティインシデントとその要因および対策を座学と実習で訓練するものとし､常に時代に合った内容とする。各訓練とも時間は 1h 以内とする。情報セキュリティが専門ではない指導員でも指導できるよう詳細な指導案も構築するべきである。

Ⅴ　おわりに

職業大電子計算機室に所属していた 7 年間で改めて情報セキュリティの重要性を認識した。現在は電子情報技術科の訓練を担当しているので、学生に情報セキュリティの基本から専門的な技術まで習得させる所存である。併せて、余裕があれば、Ⅳ節で提案した情報セキュリティ訓練カリキュラムモデルの構築・試行をしたいと考えている。

最新の情報セキュリティ関連情報は、Web サイトから入手可能である。また、マスコミでもしばしば情報セキュリティインシデントについて取り上げられているので、その報道に遭遇した際は、聞き流すのではなく傾聴し、自身の情報セキュリティへの意識を高めていくことが必要である。参考文献に最新の情報セキュリティ関連情報を入手可能な Web サイトを紹介する[(1)-(4)]。

［参考文献］

(1) 警察庁 情報セキュリティポータルサイト
https://www.npa.go.jp/cyberpolice/index.html
(2) 情報処理推進機構 (IPA) 情報セキュリティサイト
https://www.ipa.go.jp/security/index.html
(3) JPCERT コーディネーションセンター
https://www.jpcert.or.jp/
(4) トレンドマイクロ株式会社 セキュリティ情報
http://www.trendmicro.co.jp/jp/security-intelligence/