情報セキュリティ対策講習会の学習効果を高める疑似ウィルスの開発
Development of Fakevirus Effective in Information Security Learning

松澤英之，青木謙二，園田誠，黒木亘
Hideyuki Matsuzawa, Kenji Aoki, Makoto Sonoda, Wataru Kuroki

matuzawa@cc.miyazaki-u.ac.jp, aoki@cc.miyazaki-u.ac.jp,
sonoda@cc.miyazaki-u.ac.jp, wata-k@cc.miyazaki-u.ac.jp

宮崎大学 情報基盤センター

University of Miyazaki, Information Technology Center

概要

宮崎大学では、教職員に対して情報セキュリティ対策講習会を年 1 回以上開催し、学部 1 年生が受講する情報科学入門(半期)で情報セキュリティ教育を行っている。これらの講習会、講義の学習効果を高める疑似体験ツールとして疑似ウィルスの開発を行い、その効果を検証した。

キーワード

情報教育, 情報セキュリティ

1. はじめに

宮崎大学では、教職員、および学生に対して定期的に情報セキュリティに関する広報を行う一方、教職員に対しては情報セキュリティ対策講習会を年 1 回以上、 1 回 1 時間程度の内容で開催、学部 1 年生が受講する情報科学入門(半期)で情報セキュリティ教育を行っている。

情報セキュリティ対策講習会と同じように啓蒙のための講習会として、免許更新時の交通安全講習会、地震対策を訴える講演会がある。これらの講習会では、映像、シミュレータ等を用いた疑似体験を通じて講習の学習効果を高め、受講者が率先して対策を取ることを促している。

そこで、情報セキュリティにおいても学習効果を高めるために、セキュリティ事故に会ったときの状況を疑似体験してもらうことを目指した。セキュリティ事故としては、パスワード流出による情報漏洩などがあるが、情報処理推進機構の調査による「2012 年度 情報セキュリティの脅威に対する意識調査」報告書 4-4-1-1.情報セキュリティ対策の実施状況と今後の実施意向[1]によると、現在実施している情報セキュリティ対策として「セキュリティソフトの導入・活用」がトップに挙げられているにもかかわらず、4-2-1.情報セキュリティの脅威に関する攻撃・脅威の認知[2]によると、「ボット」「マルウェア」の認知度は 4 割程度と低い。そこで、疑似体験として最も身近であるにもかかわらず、認知度が低い情報セキュリティの脅威であるマルウェアに罹患した時のパソコンの挙動を再現することで、セキュリティ事故に会ったときの状況を疑似体験し、情報セキュリティ対策を積極的に行ってもらう事を目的に、疑似ウィルスの開発を行い、その効果を検証した。

2. 情報セキュリティ対策講習会

情報セキュリティ対策を広く理解してもらうために、情報セキュリティ対策講習会を開くことは重要なことである。宮崎大学では、教職員に対しては、情報セキュリティ講習会を、学部生に対しては、情報科学入門を開講している。情報科学入門の内容については、担当教員に任されているので、詳しい講義内容については言及できない。そこで、情報基盤センターが主催し、教職員に対して行われる情報セキュリティ講習会について説明する。情報セキュリティ講習会は、年１回以上、１回１時間程度、教職員(学生の参加も可能)を対象に開いており、以下の内容で開催してきた。

1. 規程等のついては、必要最小限の紹介にとどめる。
2. 情報セキュリティ対策を実施する理由・効果を、対策毎に具体的に説明する。
3. 各パソコンのOS毎に作られた実施手順書を元に、各自のノートパソコンを持参してもらい、その場で実施手順書通りにセキュリティ対策が行われているか確認する。

3. 疑似ウィルス

昨今のマルウェアは、バックグランドでの情報収集、及びボットネットとしての動作するものが多いため、ウィルス等に罹ったことを極力パソコンユーザから隠し、長く情報収集、或はボットネットを広げる等などの活動を行うものが多い。[3]そのため、パソコンユーザは日々のパソコンの動作を見ただけでは、マルウェアに罹った状態であるのかどうか分からないことが多い。しかし、マルウェアのこのような動作は、パソコンユーザと同様、講習会参加者にマルウェアへの罹患状態を疑似体験させる際に、マルウェアがどの様に働き、その結果罹患したパソコンがどの様な動きをするのか分からないだけでなく、実際の疑似体験の効果を高める役に立たないと考える。そのため、"Happy99"[4]の様な、マルウェアが出現し始めた当時の愉快犯的な目的で作られたマルウェアの動きを参考にして、疑似ウィルスの開発を行った。疑似ウィルスの開発にあたっては、以下の様な方針を採った。

１．感染はしない
２．破壊活動はしない
３．情報流出を行わない
４．疑似ウィルスの活動が視覚、聴覚から分かるようにする

感染、破壊活動、情報流出等の機能は、「情報処理の高度化等に対処するための刑法等の一部を改正する法律」[5]に抵触する恐れがある。また、実際にこの疑似ウィルスが流出、悪用される可能性も考慮して、今回はこれらの機能を疑似ウィルスに加えなかった。

疑似ウィルスの機能として、視覚的には、マウスの反応が悪くなる、ディスプレイにランダムにウィンドウを表示する、アクセスランプなどパソコンのランプを点滅させた。一方、聴覚的には、パソコンのビープ音を鳴らした。

疑似ウィルスは、広く使われている Windows OS を対象に開発した。また、簡単に利用できる様に、疑似ウィルスを動かす時に、疑似ウィルス以外のソフトウェア、DLL 等を必要としないようにした。疑似ウィルスのインストールによってシステムが影響を受けないように、ファイルは動作するパソコンにコピーすることで動作し、インストール作業等を行わないようにした。

疑似ウィルスは、各機能をつかさどるプログラム FakeVirusImage.exe、FakeVirusDisk.exe とこれらのプログラムの起動タイミング及びオプションパラメータをコントロールするバッチファイル FakeVirus.bat からなる。

・FakeVirusImage.exe：視覚部分 (図-1)

Windows OS の共通機能として組み込まれている Win32API[6]を利用して作成した。このプログラムは、図-1 に示すように Windows の画面上に位置、大きさ、背景色をランダムに選択したコマンドプロンプト画面を表示する。パソコン上に現れる効果としては、視覚的に異常動作を確認できること、また、CPU の使用率が上がり、キーボード操作等が滞ることである。

・FakeVirusDisk.exe：視覚、聴覚部分(図-2)

このプログラムは、指定したフォルダの下層の

フォルダに含まれるファイルと、指定したフォルダにある全てのファイル(バイナリーファイルも含む)を 1 文字ずつ読み込み、コマンドプロンプト画面に表示する。バイナリファイルを含むファイルの読み込み、表示をするため、図-2 に示すように意味不明な文字列が表示される。また、ディスクアクセスが急激に上がり、パソコンのディクスへのアクセスランプが激しく点滅するようになる。更に、CPU 使用率が跳ね上がり、キーボード操作等が滞る。副次的な効果として、バイナリファイルを表示するため、ランダムにビープ音が発生する。

・バッチファイル FakeVirus.bat

FakeVirusImage.exe を起動した場合、画面全体にコンソール画面が表示されるため、同時に FakeVirusDisk.exe を起動すると、動作が見えなくなる。そこで、プログラムの起動タイミングをバッチファイルでコントロールすることで、各プログラムの効果を確実に見せることが出来る。又、新しいプログラムをバッチファイルに登録することができるので、簡単に疑似ウィルスの機能を拡張できる。

4. 疑似ウィルスの効果を測定するアンケート

実際にこの疑似ウィルスを使った実験を行った。被験者は、平成 25 年度宮崎大学学部 1 年生(農学部 32 名、教育文化学部 93 名 計 124 名)で、被験者全員がノート型 PC を所有している。疑似ウィルスの効果を測定するために、疑似ウィルスを見せる前後で、アンケートを 1 回ずつ行った。アンケートの内容は以下の通りである。

1. ”情報セキュリティ対策”について、具体的な情報を得ようと思いますか?
　はい、　いいえ
2. 自分、或は自分のパソコンが不正侵入者に狙われていると考えたことはありますか?
　　はい、　いいえ

問い 1 は疑似ウィルスを体験することでどの程度情報セキュリティ対策を行う必要性を感じるようになるかを、問い 2 は自分が利用しているパソコンの利用環境に対する安全性の認識がどの程度変化するかを調べるために行った。

一回目のアンケートの後、これから動作させる疑似ウィルスについて以下の様な説明を行った。「現在のウィルスは、潜伏して長期間パソコンの情報を送ったり、踏み台になるため、感染したことを隠す。しかし、これでは、ウィルスの動きが分からないので、この疑似ウィルスは、昔のウィルスの動きを再現した。この疑似ウィルスは、感染、システムの破壊は一切行わない。」

次に、以下の通り疑似ウィルスの動作の説明を行った。

- ファイルの表示：ディスクアクセスランプの点滅、ランダムにビープ音の発生、CPU負荷の増大
- ウィンドの表示：不正プログラムが動いていることが視覚的に分かる

この後、疑似ウィルスを見せ、再度前出のアンケートに答えてもらった。結果を、表−2、表−3 に示す。

5. まとめ

疑似ウィルスを見せた前後で、各設問ごと、”はい”の回答数が約 1/4 程度増加した(表-1)。又、ウィルス体験前後の回答において χ^2 検定を行ったところ、回答 1 で χ^2=25.3、回答 2 で χ^2=33.7 となった。危険率 1%、自由度=1 として χ^2 検定を行ったところ、統計的に有意差が認められた。つまり、疑似ウィルス体験によって有意に変化したことが分かった(表-2)。この結果から今回開発した疑似ウィルスを見せることで、情報セキュリティ対策について興味或は必要性を向上させ、自分のパソコン環境が安全ではないことを感じさせる事ができることを確認できた。

今後の検討課題として以下の点が挙げられる。農学部の学生に対して実験を行った時に、ディスクスキャンを行う FakeVirusDisk.exe の動作中は、静かに疑似ウィルスの動きを見ていたが、画面を表示させる FakeVirusImage.exe 起動後は笑い出すなど、切迫感にかけるところが見られた。今後は、

疑似ウィルス罹患後にパソコンの動きがおかしくなるなど、コンピュータにダメージを与える機能を加える必要がある。

また、疑似ウィルスの運用において、問題点がある。今回は疑似ウィルスの効果を測定する実験のため、実際の講習会等で行われるような情報セキュリティ対策に対する説明等は行っていない。そのためか、アンケートに自由回答欄を設けてはいなかったが、余白に「怖い感じは伝わってきたけど、何」との書き込みが見られた。疑似ウィルス体験の本来の目的である”情報セキュリティ対策への積極的な対応”を実現するためには、疑似ウィルスの体験だけでなく、従来の情報セキュリティ対策講習会で行ってきた情報セキュリティに対する講習内容も同時に教える必要がある。

6. 参考文献

[1]情報処理推進機構「2012 年度情報セキュリティの脅威に対する意識調査」p46
http://www.ipa.go.jp/security/fy24/reports/ishiki/
[2]情報処理推進機構「2012 年度情報セキュリティの脅威に対する意識調査」p25
http://www.ipa.go.jp/security/fy24/reports/ishiki/
[3]情報処理推進機構 「2012 年版 10 大脅威 変化・増大する脅威！」p5、
http://www.ipa.go.jp/security/publications/hakusyo/2012/hakusho2012.html
[4]W32/Ska(Happy99)に関する情報、
http://www.ipa.go.jp/security/topics/ska.html
[5]情報処理の高度化等に対処するための刑法等の一部を改正する法律、
http://www.moj.go.jp/content/000072565.htm
[6]Win32API、
http://msdn.microsoft.com/en-us/library/cc433218.aspx

	農学部 31 人		教育文化学部 A 40 人		教育文化学部 B 53 人		計 124 人	
	はい	いいえ	はい	いいえ	はい	いいえ	はい	いいえ
体験前 1	15	16	29	11	40	13	84	40
2	16	15	9	31	14	39	39	85
体験後 1	25	6	38	2	50	3	113	11
2	22	9	22	18	30	23	74	50

表-1 疑似ウィルスの効果を測定するアンケート結果 1

回答 1	体験前 はい	体験前 いいえ	回答 2	体験前 はい	体験前 いいえ
体験後 はい	84	29	体験後 はい	38	36
体験後 いいえ	0	11	体験後 いいえ	1	49

表-2 疑似ウィルスの効果を測定するアンケート結果 2

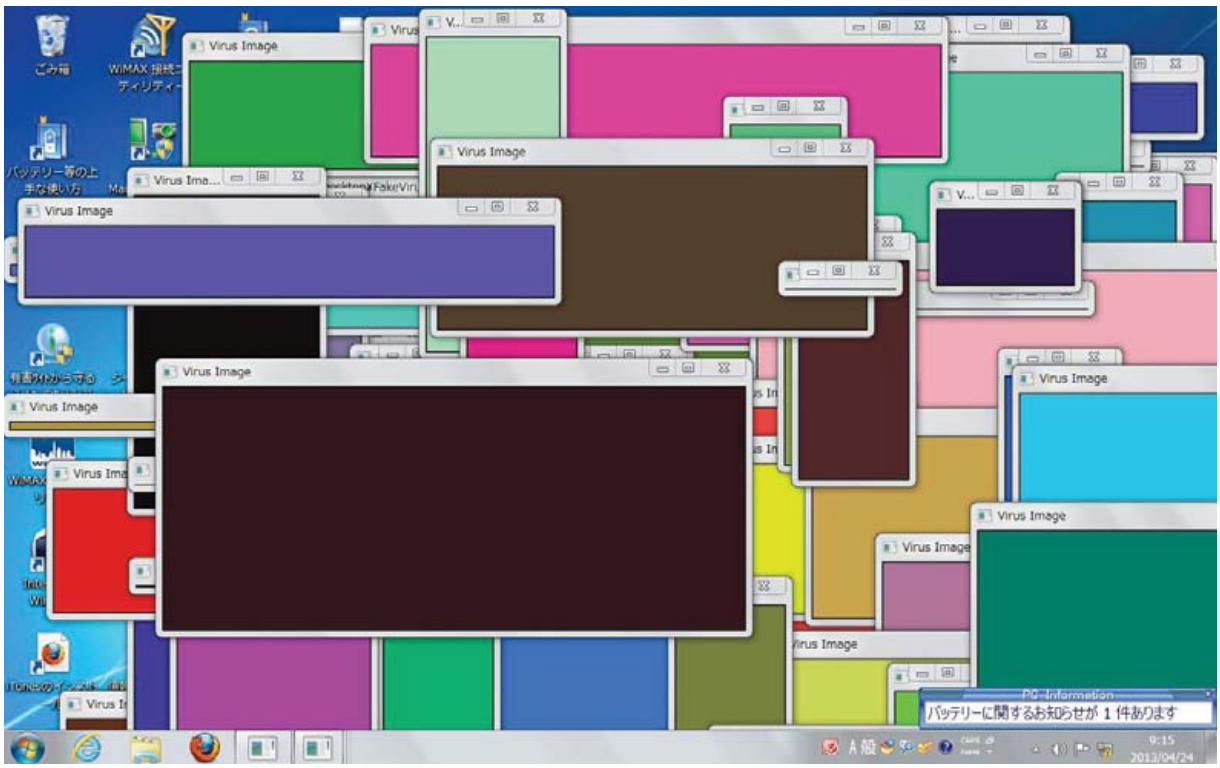

図-1 FakeVirusImage.exe：視覚部分

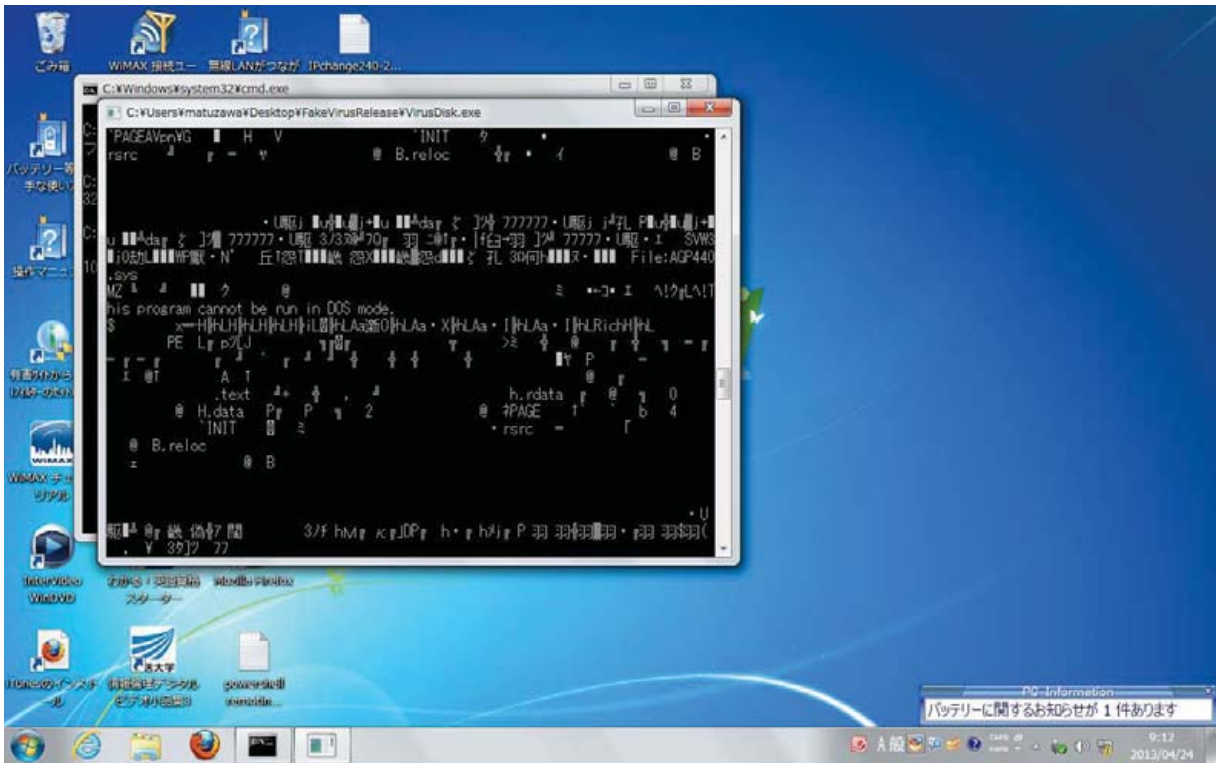

図-2 FakeVirusDisk.exe：視覚、聴覚部分