富山大学総合情報基盤センター広報 vol.6 （2009） 37-40頁.

Virus 被害の現状

総合情報基盤センター　助教　沖野 浩二

1.はじめに

2009 年､年明けのセキュリティの大ニュースとして、独立行政法人　情報処理推進機構（以下、IPA という）の職員が自宅で P2P ソフトを利用し暴露 Virus に感染するという事件が発生した[1]。

この事件では、セキュリティおよび知的財産への意識が高いはずである IPA 職員が、商用プログラムや違法なコンテンツを入手するために P2P を利用し、

・Virus に感染

という事態を引き起こした。また、結果、

・著作権法違反の事実が暴露
・個人的な情報が漏洩
・職員が過去所属していた会社関係の業務情報が漏洩

という事態を引き起こした。

結局、この職員は、IPA の信用を傷つけ、名誉を汚したこと等を理由として、就業規則に基づき、懲戒処分「停職３月」となった[2]。

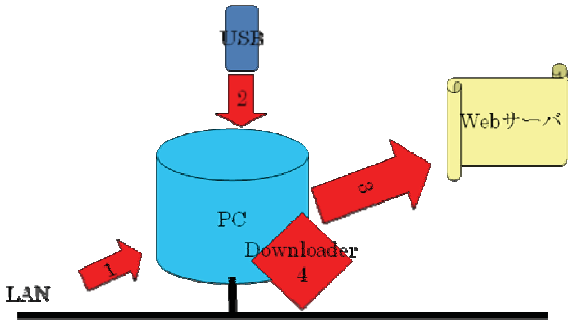
このようなインシデントは身近でもあり、近隣大学にて類似の事件が発生している。これも自宅の PC にて P2P ソフトを利用し、格納されていた情報が Internet へ漏えいしたものである[3]。

現在、本学においては、情報漏えいが発生したことはないが、今後発生しないとは限らない。また、教職員及び学生が ComputerVirus に感染する事例は後を絶たず発生している。ここでは、Virus の感染までのメカニズムとターニングポイントに注目し、Virus 被害について検討を行う。

2.本学における Virus 対策

本学にでは、多重の Virus 対策を行っている。Virus の感染経路は、PC に接続される幾つかの経路に整理される。

1．LAN（Worm 等）
2．外部デバイス（USB メモリ等の接続）
3．Web アクセス時（改ざんされた WebPage の閲覧）
4．コンピュータ内部に仕組まれた Downloader
　4-1.Download したソフト
　4-2.メール添付ファイル



これらの経路に対応するために、セキュリティ対策製品として、

・Viru 対策ソフト導入（1,2,3,4）
・Virus 検出機能付き FireWall（2,4）
・メール添付ファイルの Virus 検査（4-2）

を導入している。Virus 対策ソフトは検出能力の向上のため学内配布は２種類準備し、メールの検査システムとは別会社のものとしている。また、学内広報などを通して、

・Download したソフトの利用禁止（4.1）
・不必要なサイトの閲覧禁止（3）

を教育している。

3.Virus 感染経路

2008 年の Virus の感染経路を分類したところ、大きく分けて次の 2 種類に分けられた。

・Web 改ざんにより埋め込まれた Script 実行による感染（以下 Web 感染）

・USB メモリ Autorun 実行による感染（以下 USB 感染）

過去にあった、メール添付ファイルや LAN による感染は報告されなかった。これは、OS 等のアプリケーションのセキュリティ向上をベースとして、ユーザの意識レベルの向上等により減少したと思われる。ここでは、2 つの経路の問題点を検討する。

3.1 Web 感染

Web 感染は、ユーザが日ごろ利用している Web サーバがクラックされ、SQL injection[4]などにより悪意ある Script が埋め込まれるために発生している。実際の攻撃手法から考えた場合には、ユーザがこれらの影響を回避する手段は少ないと考えられる。しかし、Virus の配布サイトを調査した結果、ほとんどが教育・研究や業務に関係のないページであった。業務 PC では必要以外のページをアクセスしないことも必要だと思われる。

3.2 USB 感染

USB 感染は、利用者が Virus に汚染された USB の利用を通して、データ交換を行うことにより広がる。汚染された USB メモリには、autorun.inf ファイルが作成され USB 接続時に自動的に Virus が実行される。また、実行ファイルは、attrib 属性により不可視等が設定され、GUI から確認することができない。これらの Virus に感染しているかは、autorun.inf の中身や DOS 窓からの attrib 属性の確認などにより判別できる。ただし、これらの Virus はレジストリに複数ポイントを記載し、手動で削除しても自動的に復活するなど、通常の削除では回復できないことも多い。また、自分の発見を遅らせるために、一定条件時には自分自身を削除するなど証拠隠滅することがある。現在の USB 感染型の Virus については、これらの点について注意が必要である。

3.3 感染経路の問題点

これらの Virus 感染の問題点は、日ごろならば問題のない行為又はどうしても必要な行為が、ある日突然問題を発生されるということである。Web 閲覧や USB の利用は教育・研究にはなくてはならない行為であり、これらをルールにより一律禁止することは現実的ではない。実際の対応策としては、JavaScript の実行禁止や USB の自動実行の禁止があげられるが、リスクを軽減だけであり、完全ではない。また、攻撃者側のスキルは技術面だけでなく、心理学や社会学な面からも著しく向上しており、守備側の過去の対策を徹底的に研究していると考えられる。例えば、USB 感染では、自動実行の禁止の対策として、icon 偽造等偽造し、File 閲覧と誤認させ、ユーザ実行をさせようとするものが標準となっている。

3.4 本学対策の有効性

2 章の述べたように、本学では複数の Virus 対策を行っているが、これらの有効性を評価する。現在、上記 2 つの感染経路に関しては、これらの対策が有効であるとは言えない。

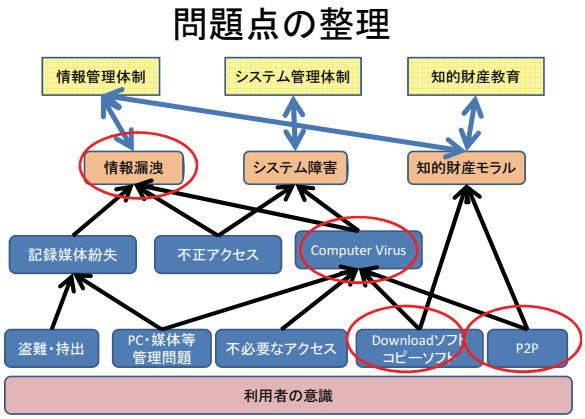
Web 感染に関しは、悪意あるコードの埋め込み後、時間が経過すれば FireWall にて検出できるが、攻撃直後は検出でき

ず攻撃が成功する。

USB 感染の場合は、本体の Virus 対策ソフトにより検出されるが、Internet による Virus 自体の改変が頻繁に行われるため、対策ソフトのパターンの更新が対応できず、検出できない場合が多い。

4.情報インシデントの影響

ユーザの行動からみた情報インシデントと発生した事例、それに伴う、組織の社会的責任の関係を図に示す。



利用者の意識の元、不注意や倫理意識のない行動が、結果として大きな問題となる。特に次の 2 点に関しては、強く意識する必要がある。

4.1 ComputerVirus に繋なるパス

ComputerVirus に繋がる Download したコピーソフトや P2P の利用は、情報漏洩・システム障害という問題だけでなく、知的財産モラルに関係する問題としても認識され、社会的に高等教育機関である大学構成員には、高度な倫理感が求められる。IPA の事例からもわかるように、Virus に感染し情報漏えいが発生した場合には、本人に対しては、懲戒等の処分が発生し、組織の信用失墜に繋がることを意識すべきである。

4.2 情報漏洩に繋がるパス

現在の Virus は、感染した PC 内に保存されている情報を外部に送信する機能がある。この機能が ComputerVirus の被害の一番怖い点である。

総合大学にある富山大学では、学内には大学固有の情報だけでなく、病院などの医療情報・教育実習における生徒学生情報、共同研究などによる研究情報など、大学だけでその管理が完結しない情報が多数ある。これらの情報が大学の管理範囲で漏洩した場合には、その責任を負わなければならないことは、容易に想像が付く。

それに加え、実際のインシデント対応では、漏洩していないことを、確認しなければならないことがある。特に現在の USB 感染では改変により、その動作が変わる。このような Virus に感染した場合には、漏えいした可能性の推定には多大なコストが発生する。最悪の場合、感染したコンピュータに格納されている情報のすべてが漏洩した可能性があるという前提で対応しなければならない。

5.Virus 対策の今後

実際にこれらの問題に対応するには、以下の Point が重要となる。

Point1. 自分が持つ情報を最小限にすること

情報漏洩リスク対応を考えた場合、一番の基本は、漏れたときの影響を低くすることであり、情報が漏れない体制を作ることが第一ではない。なぜならば、漏れない状態を維持することは大変なコストがかかり、実際に漏洩にゼロにすることは不可能であるからだ。現在の業務と関係のないデータや必要以上に収集したデータを持つこと自体のリスクを意識すべきである。情報がなければ、漏れる心配

はないのである。

Point2 リスク行為の禁止

Virus 感染の多くは、P2P の利用や違法コピーなどにより感染している。これらの行為自身の問題点や、利用した結果引き起こす自体を認識すべきである。

Point3 バックアップ

必ずデータのバックアップを定期的に取る。Virus の中には感染した場合、取り除くことが難しいものがある。完全に回復する場合には、これらのバックアップが必要である。また、セキュリティの面からだけでなく、故障などの障害から守るためにも必要である。

Point4. ソフトウェアは常に最新に

OS の場合には、Windows 系では WindowsUPDATE、Mac 系では、ソフトウェアアップデートを利用し、常に OS は最新状態になるようにする。また、IE などのブラウザ上で動作する、PDF Reader や Java、QuickTime などのアプリケーションも必ず最新版を利用する。現在の攻撃は、OS の脆弱性を利用したものだけでなく、アプリケーションの脆弱性を利用した攻撃が増加している。

Point5. Virus 対策ソフトの導入

Virus 対策ソフトは必ず導入する。PC 購入時に付いてくる Virus 対策ソフトは、有効期限がある。有効期限が切れたソフトウェアは役には立たないので、必ず、有効期限の更新を行う。また、定期的には、全体 scan を行い、log に感染記録がないことを確認する。log に多数の感染が記録されている場合は、PC が Virus に汚染されている可能性が大きい。この場合には、パソコンショップなどで専門家に相談する。

注意点:Free の AntiVirus ソフトの中には、自宅での非営利にのみ利用が許可されているものがある。これらを大学での利用することは契約違反となる。利用時には必ず利用条件を確認すること。

Point6 通信制御の強化

Personal FireWall を導入することで外部からの攻撃や内部からの不正な通信を抑制することができる。また、自宅の PC を守るためには、Router などを利用することも外部からの攻撃を防ぐという面では効果的である。

6.まとめ

Virus による情報漏洩は至る所で発生している[5]。まずはこの事実を認識すべきである。

次に Virus に感染した場合には、個人だけでなく所属している組織にも影響し、事後対策には莫大な費用が発生する。場合によっては、その被害は金銭面だけでなく、本人の名誉などにも影響する。

現在のところ、Virus への完全な対策手法はない。しかし、先に述べた Point を守ることにより感染確率を下げ、感染した場合の影響を低減できる。

利用者には、リスクある行動がどのような結果を引き起こすか認識し、正しい知識を持ち対応する必要がある。

参考資料

[1]http://www.ipa.go.jp/about/press/20090106.html
[2]http://www.ipa.go.jp/about/press/20090119.html
[3]http://www.kanazawa-u.ac.jp/university/administration/prstrategy/release/pdf/08/080708.pdf
[4]http://www.lac.co.jp/news/press20080312.html
[5]http://www.geocities.jp/winny_crisis/