ウィルスの現状と対策　2009

総合情報基盤センター　技術職員　山田 純一

1.　はじめに

「富山大学総合情報基盤センター広報 vol.1,No.1 2004」では、コンピュータウィルス（以下、ウィルスと呼ぶ）について、記述させて頂いた。それから 5 年、ウィルスは減少することがなく、増加し、進化し続けている。ここでは 2008 年のウィルス感染状況から、ウィルスの現状とウィルス動向、その対策について説明する。

2.　過去のウィルスとの比較

通商産業省（現、経済産業省）の「コンピュータウィルス対策基準」では、ウィルスとは

①　自己伝染機能
②　潜伏機能
③　発病機能

のいずれかの機能を 1 つ以上持っているものとある。2008 年に猛威をふるった、外部記憶メディアを介して感染するウィルスも同様な機能を 1 つ以上持っている。しかし、5 年前に学内で猛威をふるった Blaster（別名、WORM_MSBLAST.A、W32.Blaster.Worm、W32/Lovsan.worm 等）と比較すると、感染してもパソコンの動作が遅くなることはなく、ユーザが全く気付かない。また、Blaster はソフトウェアの脆弱性を突いてネットワーク経由で感染したが、最近のウィルスはホームページ上に配置し、メール等で誘導して、ユーザにウィルスをダウンロードもしくは実行させ、感染させる。

3.　新しい形のウィルス

2008 年に学内で猛威をふるったウィルスは USB メモリ等の外部記憶メディアを介して感染するウィルスであった。本学における感染状況は図 1 のとおりである。ただし、総合情報基盤センターに届出のあった状況を集計したものであるため、届出のないものを含めると、実際のウィルス感染台数は数件多くなると推測される。

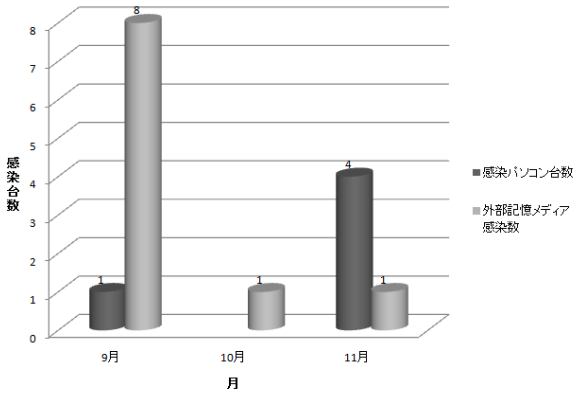

図 1　外部記憶メディアからの感染状況

このウィルスは 9 月に最初の報告があり、その後、感染の拡大が予測されたため、学内にはウィルスへの対策依頼等の啓蒙活動を行ってきた。

啓蒙活動の結果及びウィルス発生時の早期駆除を行った結果、図 2 の Blaster 発生時と比べて、学内の感染拡大を大幅に防ぐことができた。

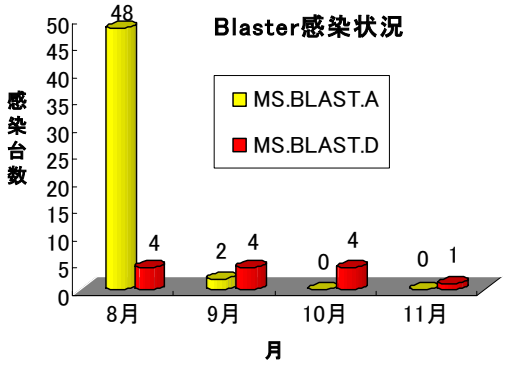

図 2　5 年前の Blaster 感染状況

このウィルスの特徴としては、Windows に実装されている自動実行機能の AutoRun を悪用する手口を用いる。そして、USB メモリ等の外部記憶メディアを介して感染を拡大させる。ここで、図を用いながら感染拡大までの順序を説明する。

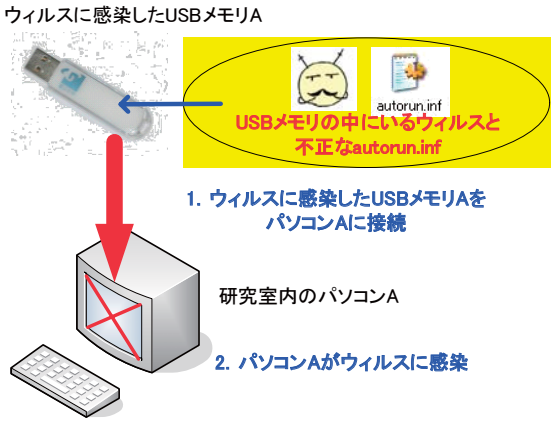

図 3　ウィルスの感染拡大順序 1

① 学外で USB メモリ A がウィルスに感染する。このとき、USB メモリ A にはウィルスによって、標準設定では Windows で表示されない autorun.inf と呼ばれるファイルが生成される。autorun.inf を USB メモリ内に作成することで、ウィルス自身が自動実行される状態にする。

② 図 3 のように、USB メモリ A を研究室内のウィルスに感染していないパソコン A に接続する。パソコン A で USB メモリの自動実行機能が許可されている場合、もしくはマイコンピュータから USB メモリのアイコンをダブルクリックした際に、USB メモリ A 内にある autorun.inf によって、ウィルス自身が自動実行され、パソコン A の内蔵ハードディスクにウィルスが感染する。

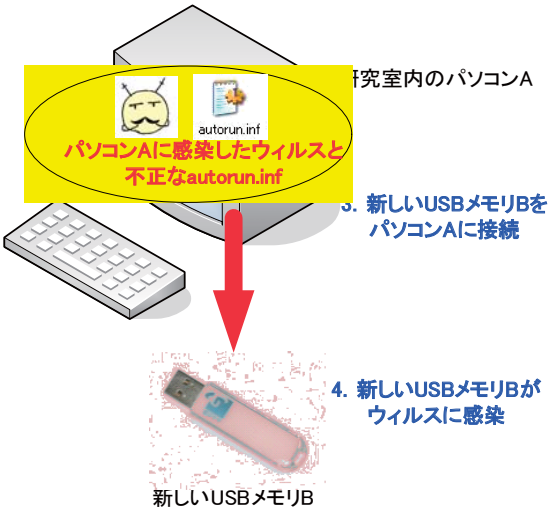

図 4　ウィルスの感染拡大順序 2

③ 続いて、図 4 のように、今度はウィルスに感染していない USB メモリ、もしくは新しい USB メモリをパソコン A に接続する。

④ USB メモリを接続した途端、ウィルス自身が自動実行され、USB メモリがウィルスに感染する。

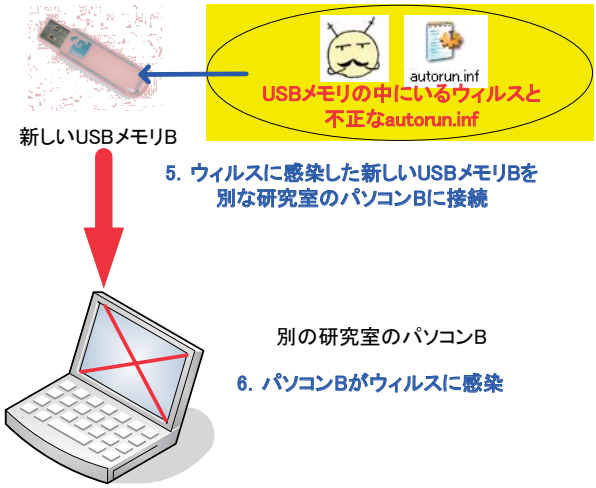

図 5　ウィルスの感染拡大順序 3

⑤ この後、USB メモリがウィルスに感染していると知らずに、別な研究室のパソコン B に USB メモリを接続する。

⑥ その結果、パソコン B もウィルスに感染する。

これが USB メモリ等の外部記憶メディアを介して感染するウィルスの感染拡大順序である。この他に、USB メモリ A をさらに別なパソコンに接続する。パソコン A に別の USB メモリを接続することにより、次々に USB メモリ及びパソコンがウィルスに感染していく。

ウィルスの感染拡大順序では USB メモリだけを取り上げたが、ウィルスに感染する外部記憶メディアは USB メモリだけではなく、外付けハードディスク、デジタルカメラのメモリースティックもウィルスに感染する。

実際、ウィルスに感染した人の話を伺うと、

- データの受け渡しで同じ研究室の学生の USB メモリを自分のパソコンに接続したらウィルスに感染した。
- 自宅のパソコンで使用していた USB メモリにデータをコピーし、その USB メモリを研究室のパソコンで使用したらウィルスに感染した。
- 落し物の USB メモリをそのまま使ったところ、ウィルスに感染した。

等々によってウィルスに感染したとの話である。

もしパソコンがウィルスに感染した場合だが、

- Windows が正常に動作するための必要なファイルシステムが破壊される。
- オンラインゲームのユーザ ID やパスワード等の情報が盗まれる。
- 別のウィルスをダウンロードする。

以上のような被害が発生する。

独立行政法人情報処理推進機構のプレスリリース「コンピュータウイルス・不正アクセスの届出状況[2008 年 11 月分] について」でも同様に、USB メモリ等外部記憶メディアを介して感染した届出が多く報告されている。また、このプレスリリースでは、USB メモリ等外部記憶メディアを介して感染を広げるウィルスの検出数が 2008 年 9 月に 11722 件、10 月に 62555 件、11 月に 101090 件と急増していることが報告されている。

4. ウィルスに対する意識

ウィルスの感染が拡大した要因として、ユーザのウィルスに対する誤った意識が最も大きな要因として考えられる。メールに添付されるウィルスに対しては意識が高いが、特に USB メモリへのウィルス対策にはあまり意識が行き届いていない。2008 年には 32GB の USB メモリが 1 万円を割り、USB メモリの大容量化と低価格化が進み、利用機会が増えている。また USB メモリだけではなく、その他の外部記憶メディア（外付けハードディスク、メモリースティック等）も大容量化と低価格化によって、利用機会が増えている。しかし、ウィルス対策にはあまり意識が行き届いていない。

実際、ウィルスに感染した学生の一部には、「メールに添付されるウィルスにさえ気をつけていれば良い。」、「自分の知らないファイルを開けたりしない限りウィルスには感染しない。」、「Windows Update をしていれば問題ない。」、「ウィルス対策ソフトウェアを導入さえすれば問題ない。」のような、誤った意識をしている学生が存在する。

このような意識から、今回のウィルス感染は、USB メモリ等の外部記憶メディアを不特定多数のユーザが利用し、かつパソコンへ安易に接続したことが感染拡大の要因として大きい。今一度、USB メモリ等の外部記憶メディアのウィルス対策を見直す必要がある。

5. ウィルスへの対策

特に学生が使用しているパソコンでたまに見かけるのは

- ウィルス対策ソフトウェアを使用していない。
- ウィルス対策ソフトウェアが期限切れになっている。
- ウィルス対策ソフトウェアが常駐していない。

以上のようなパソコンである。

ウィルス対策ソフトウェアの常駐（以下、常駐機能と呼ぶ）とは、ウィルスを監視する常駐プログラムのことである。常駐機能はソフトウェアのメーカーによって、呼称が異なる場合がある。この常駐機能はパソコンの動作速度に影響を与えるため、パソコンの動作速度が遅いからと常駐機能を使用していない学生もいるが、これではウィルス対策になっていない。

ウィルスへの対策だが、基本的なセキュリティ対策が不可欠になる。基本的なセキュリティ対策とは、ウィルス対策ソフトウェアの導入と常駐機能の有効、ソフトウェアのウィルス定義ファイルを常に最新の状態に更新すること、セキュリティの修正プログラム（Windows Update 等）の適用である。

その他に基本的なこととして、配布元や作者が不明のファイルは開かない、覚えのないメールのリンクはクリックしない、信頼できないホームページにはアクセスしないことも大事である。

ただし、これだけでは今回の USB メモリ等の外部記憶メディアを介して感染するウィルスは防ぎ切れない。このウィルスに対しての対策としては、

① USB メモリ（外部記憶メディア）を不用意にパソコンに接続しない

当たり前のことだが、不審な外部記憶メディアを不用意に自分のパソコンに接続しないことが重要である。前述のように、USB メモリの大容量化と低価格化が進んだこともあり、情報教育用端末室には USB メモリの落し物が年々増えてきている。特に落し物の USB メモリにもウィルスが含まれている可能性があるので、落し物の USB メ

モリは不用意に自分のパソコンに接続しないよう十分注意しなければならない。自分が管理していないUSBメモリや所有者の不明なUSBメモリを自分のパソコンに接続させないことも大事である。

また、研究室共用のパソコンでは個人の USB メモリだけではなく、個人の外部記録メディアを使用させないことも対策の１つである。言い過ぎかもしれないが、個人の USB メモリを研究室共用のパソコンには接続させない、また学内所有の USB メモリは自宅のパソコンに接続しないことも効果の高いウィルス対策といえる。

② USBメモリ（外部記憶メディア）のチェック

外部記憶メディアを接続した際は、必ずウィルスチェックしてから使用することが必要である。時間はかかるが、パソコンのハードディスクと同じように定期的なウィルスチェックを実施することが大事である。

③ USBメモリ（外部記憶メディア）の自動実行機能を無効にする

独立行政法人情報処理推進機構のホームページ等にも記載されているように、Windows の設定を変更して、外部記憶メディアを自動実行させない設定にすることが推奨されている。

以上のような対策を行うことで、外部記憶メディアからのウィルス感染は防げると考えられる。

6. まとめ

5 年前と同様だが、インターネットがある限り、ウィルスは決してなくなることはない。そして、ウィルスに感染した時点で他人事ではなく、他のパソコンへの不正攻撃を行うこと、パソコン内のデータが盗まれている可能性があることを念頭に置かなければならない。また、5 年前にはこのような外部記憶メディアを通じて、ウィルスが学内で感染を拡大することは考えられなかった。

今後もウィルスは進化し、現在は考えられない経路で感染する可能性がある。そのためにも、ウィルス対策は外部記憶メディアへの対策も踏まえ、見直す必要がある。

参考文献

1) 富山大学総合情報基盤センター広報 vol.1,No.1 2004
2) 経済産業省のコンピュータウィルス対策基準：http://www.meti.go.jp/policy/netsecurity/CvirusCMG.htm
3) アイティメディア株式会社　ITmedia エンタープライズ:http://www.itmedia.co.jp/enterprise/articles/0811/21/news033.html
4) トレンドマイクロ株式会社　USB メモリで広まるウイルスへの対策：http://jp.trendmicro.com/jp/threat/solutions/usb/
5) 日経 BP 社 ITpro　USB ウイルス　何でも感染源に：http://itpro.nikkeibp.co.jp/article/COLUMN/20071130/288477/
6) 独立行政法人情報処理推進機構　プレスリリース　第 08-27-137 号　2008 年 12 月 2 日　コンピュータウイルス・不正アクセスの届出状況[2008 年 11 月分] について、独立行政法人情報処理推進機構、2008 年
7) 日経パソコン　2005 年 12 月号、日経 BP 社、2005 年