福井大学バイオ実験機器部門における コンピューターウイルス感染の現状と対策

高木 均（福井大学　ライフサイエンス支援センター　バイオ実験機器部門）

TAKAGI Hitoshi : Computer virus infection at Division of Bioresearch, University of Fukui: Current status and countermeasures

1. はじめに

近年、コンピューターウイルスによる感染が非常に問題になっており、当部門においても実験装置制御用パソコンがウイルスに感染した事がある。実験装置に付属する制御用パソコンの特徴として、特別な装置以外は基本的に LAN に接続しないで使用している。また、装置稼働時のトラブルを防ぐため、多くの実験装置メーカーはウイルス対策ソフトの導入及び LAN 接続に対し消極的である。このため、ほとんどの実験装置制御用のパソコンはウイルス対策ソフトをインストールしておらず、ウイルスに感染しやすい特殊な状況にある。そこで、当部門におけるコンピューターウイルスの感染事例と対策について報告する。

2. 感染事例

当部門でこれまでにウイルス感染した件数は 11 件あった（表 1）。感染の特徴としては、次のようなことがあげられる。

1) 年間の使用頻度が高い装置が感染しやすい。
2) 同時期に 2 つの装置から同じウイルスが検出されているケースが 3 件あった。これは、USB メモリーを介して感染が広がったと考えられる。
3) 感染したウイルスは、ウイルスパターンファイルが発表されてから数年経過した古いタイプが多い。

3. ウイルス対策

当初、バイオ実験機器部門において行っていたウイルス対策は、使用者に USB メモリーのチェックを行うように注意を促すだけであったが、ウイルス感染が続くため、実験装置メーカーにウイルス対策について問い合わせた。その結果、一部のメーカー及び装置については、制限付きであるがウイルス対策ソフトがインストール可能であった。そこで、当部門では、以下の様な対策を行った。

1) 使用頻度が高く、これまでにウイルス感染したことがある装置には、表 2 のようにウイルス対策ソフトをインストールする。
2) 利用者が装置の近くで USB メモリーをチェックできるように、チェック用パソコンを設置する。（5 台：機器予約端末を兼ねる。）

表 1　ウイルス感染の事例

感染確認日	感染した装置	年間使用回数	ウイルス名	ウイルスパターンファイル発表日
H21．4．6	プレートリーダー（紫外可視用）	759 回（H21 年度）	Win32.Agent	H17.4.18
H21．5.14	化学発光検出・ゲル撮影装置	518 回（H21 年度）	Win32.Agent	H17.4.18
H21．6．2	顕微鏡デジタルカメラ	169 回（H21 年度）	WORM_TATERF.BU	?
H21．6．4	プレートリーダー（紫外可視用）	759 回（H21 年度）	WORM_TATERF.BU	?
H22．1.29	化学発光検出・ゲル撮影装置	518 回（H21 年度）	（未記録）	?
H24．1.23	セルアナライザー	156 回（H23 年度）	WORM_SPYBOT.BAN	H21.12.3
H24．3．2	定量 PCR　No1	149 回（H23 年度）	W32.Downadup.B	H20.12.30
H24．3．2	定量 PCR　No2	168 回（H23 年度）	W32.Downadup.B	H20.12.30
H25．1.16	チップ型電気泳動装置	11 回（H24 年度）	WORM_PALEVO.SMG	H23.1.6
H25．8.19	DNA シーケンサー	2347 サンプル（H24 年度）	TROJ_SPNR.21HH13	?
H25．9.19	プレートリーダー（万能型）	140 回（H24 年度）	WORM_RIMECUD.SM1	H22.11.10

3) 当部門の職員は、ウイルス感染防止機能付き USB メモリーを使用する。

ウイルス感染防止機能付き USB メモリーの使用については、自分自身の USB メモリーがウイルスに感染するのを防ぐことができるだけでなく、USB メモリーにウイルスが感染しようとすると警告のウインドウが表示されるため、感染したパソコンの早期発見にもつながる。

4. ウイルス感染した場合の対応

ウイルス対策ソフトをインストールできない装置が感染した場合の対応であるが、当然ながら、最初に装置を使用禁止にし、ウイルス駆除を行う。次に使用記録簿より感染の可能性のある使用者へ連絡し、使用者の USB メモリーのチェック及びウイルス駆除を行っている。使用者の USB メモリーのウイルス駆除を確実に行わないと、ウイルスの再感染や他の装置に感染が広がる恐れが高くなるため、絶対に行わなければならない。最後に、ウイルス感染した情報をメール及びホームページを使用して全講座に連絡し注意を喚起している。

ウイルス駆除の方法であるが、ウイルス対策ソフトを一時的にインストールして、ウイルス駆除後にアンインストールする方法では、かなり面倒な作業となる。そこで、当部門では USB メモリーからウイルス駆除を行うことができる、オフライン端末向けウイルス検索・駆除ツール : Trend Micro Portable Security を使用している。この駆除ツールは、ウイルス対策ソフトをパソコンにインストールする必要がないため、簡単にウイルス駆除を行うことができる。フリーウエアーのソフトでも同様のソフト（Dr.Web CureIt!、ClamWin Portable 等）があるが、実際に使用してみるとウイルス駆除できない場合があった。

表 2　ウイルス対策を行った装置と運用方法

装置名	ウイルス対策ソフト	LNA 接続の可否	Windows アップデートの可否
セルアナライザー (FACSCanto II)	装置起動中はウイルス対策ソフト停止	定義ファイル更新時にのみ接続	×
化学発光検出装置 (LAS4000mini)	ノートン (クワイエットモード*)	○	手動
プレートリーダー (SPECTRA MAX)	ノートン	○	手動
顕微鏡デジタルカメラ (DP70、DP72、FX380)	ウイルスバスター	○	○

＊クワイエットモード

- 登録したソフト（例えば分析装置制御用ソフト）が起動すると、ウイル対策スソフトはバックグラウンドでの活動を中断する。しかし、警告と通知は行われる。また、完全な停止状態ではないため、このモード中にウイルス感染した USB メモリーをパソコンに接続しても感染は防げる。
- クワイエットモード中は、ウイルス定義ファイルのダウンロードが行われないため、定期的に手動でダウンロードを行う必要がある。

5. 分析装置のウイルス対策に効果的なソフト？

分析装置のウイルス対策に効果的であると思われるソフトとして、Trend Micro Safe Lock がある。このソフトは予め登録したアプリケーションのみ実行を許可し（ホワイトリスト）、それ以外のソフト（ウイルス等）の実行は不可能なため不正プログラムの侵入・実行を防止することが可能である。

【Trend Micro Safe Lock の特徴】

1)ホワイトリスト方式のため、パターンファイルの更新が不要。
2) 導入対象機器中にある全ての実行可能ファイルを自動で収集し、許可リストへ登録。
3) LAN 接続していない端末を保護することが可能。
4) システムの重要な通信を阻害しない。

但し、当部門でもこのソフトの導入を検討してみたが、どのような影響が出るのか未知数なため、導入はしていない。

6. まとめ

当部門におけるウイルス対策をまとめると、以下のようになる。

1) 使用頻度の高い装置では、可能であればウイルス対策ソフトを入れる。
2) 早期に発見し対応する。
3) 感染者を探してウイルスを駆除する。
4) 使用者に注意を促す。

ウイルス感染を防ぐためには、USB メモリーの使用を禁止するのが一番効果的だと思われるが、実際に行うのは大変困難である。当部門のような不特定多数の研究者や学生が使用する共同利用施設の場合、今の所、根本的な解決策は無いと思われる。現状では、ウイルス感染は必ず起こると考えて、使用者へ注意を促すと同時に、ウイルスの早期発見に努めるしかない。