やさしいネットワーク・セキュリティ（3）
コンピュータ・ウイルスへの対策技術

連載 IT技術

村山　純一
MURAYAMA　Junichi
東海大学大学院情報通信学研究科
情報通信学専攻主任教授

コンピュータも風邪をひく？

これまでに，暗号通信とサーバ認証について紹介してきた。これらは，盗聴対策や詐称対策に効果的である。適切に活用すれば，インターネット・ショッピングを安心・安全に行える。一方で，コンピュータの操作を誤ると，個人情報が流出する恐れがある。十分な注意が必要である。

ところで，コンピュータが勝手に動作し，個人情報が流出する事件も数多く報道されている。あたかも，コンピュータが病気になったようである。このため，コンピュータを異常動作させるソフトウェアは，「ウイルス」と総称されることも多い[注1]。

今回はこのコンピュータ・ウイルスとその感染対策について紹介する。

スパムメールにご用心！

インターネットでメールを使用していると，様々なスパムメールが送られてくる。謎のファイルが添付されていることもある。この多くは，コンピュータ・ウイルスのインストーラである。気になるとは思うが，メール本体も含めて，無視すべきものである。もし，ファイルにアクセスすると，コンピュータがウイルスに感染する。注意されたい。

多くのウイルスは，コンピュータの使用自体には影響を与えない。密かに潜伏し続け，機密情報を外部に流出させる。他のウイルスと協調して，特定のサーバを攻撃することもある。コンピュータの使用者は，気が付かないことも多い。大変にやっかいである。

少数だが，感染したコンピュータを使用不能にするウイルスもある。回復のためと称して金銭を要求することが多い。こちらはすぐに気が付くが，やっかいなことに変わりはない。

ウェブサーバにもご用心！

ウェブは，インターネットでの情報収集に，大変便利なツールである。ウェブブラウザは，ウェブサーバから送られた通信データを，見やすく視覚的に表示する。テキストデータだけでなく，画像データや動画データも表示する。また，複数のウェブサーバから同時に通信データを受けて，これらをまとめて表示することもある。

悪性のウェブサーバは，ウイルスのインストーラも送ってくる。ウイルスは視覚的に表示されないため，気が付かないことが多い。しかし，ウェブブラウザを経由して，密かにコンピュータへの感染を試みている。このため，見知らぬウェブサーバへのアクセスは控えたい。

一般のウェブサーバも，ハッカーによって，改ざんされることがある。ホームページに悪性ウェブサーバへの隠しリンクを仕込まれることが多い。文献1）にあるように，データに直接ウイルスを仕込まれることもある。人気のウェブサーバが改ざんされると，短時間で多くのコンピュータにウイルスが拡散してしま

う。ニュース等で日頃から気を付けたい。

セキュリティホールとは？

コンピュータ・ウイルスは，ソフトウェアの一種である。一般のアプリケーション・ソフトウェアと同様に，動作するためには，インストール作業が必要である。スパムメールの添付ファイルをダブルクリックするような操作は，この作業に該当する。

一方で，多くのウイルスは，自動的にインストールされる。代わりに踏み台として，セキュリティが脆弱なアプリケーション・ソフトウェアを必要とする。

ところで，ソフトウェアのセキュリティが脆弱とはどういうことだろうか?ソフトウェアは，コンピュータ上で，入力されたデータを目的に従って加工し，これを出力するものである。それぞれのソフトウェアには使用目的があり，この目的通りに動くよう作られている。ソフトウェアの公開前には，使用目的に沿った動作試験が念入りに行われる。

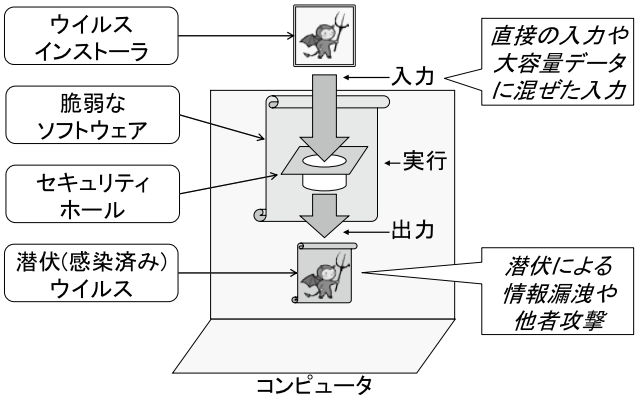
これに対して，ハッカーは，目的外の使用を試みる。すなわち，ソフトウェアに対して想定外の異常なデータを入力する。想定外のデータが入力されると，想定外に振る舞うことがある。まれに，ウイルス感染を許すように振る舞うこともある。このような，脆弱な欠陥は，「セキュリティ・ホール」と呼ばれる。

ウイルス感染の手口

アプリケーション・ソフトウェアのハッキングにも基本的な手口がある。図－1に示すように，ウイルスのインストーラそのものをソフトウェアに入力することである。

脆弱なソフトウェアの中には，テキストデータとして入力されたはずのプログラムをそのまま実行してしまうものがある。このようなソフトウェアに，ウイルス・インストーラを入力すると，これがそのまま実行されてしまう。この結果，コンピュータがウイルスに感染する。このようなハッキングへの対策としては，どのようなデータが入力されても，単なるテキストデータとして強制的に認識させる処理が有効である。

人間に例えると，ウイルスを口にすると，直接的に感染してしまうようなものである。このため，口に入れるものは殺菌処理してウイルスを無効化するような対策が有効となる。



図－1　ソフトウェアのハッキング

ハッキングとして，アプリケーション・ソフトウェアに大容量のデータを入力する手口もある。このデータには，ウイルスのインストーラを含めておく。入力データ量があまりにも大きいと，脆弱なソフトウェアはパンクする。過剰に入力されたデータは，コンピュータ・メモリ上のプログラム格納領域まで溢れ出ることがある。この領域に溢れ出たウイルスのインストーラは，プログラムとして実行されてしまう。この結果，コンピュータがウイルスに感染する。このようなハッキングへの対策としては，過剰なデータが入力されないよう，受付容量を制限する処理が有効である。

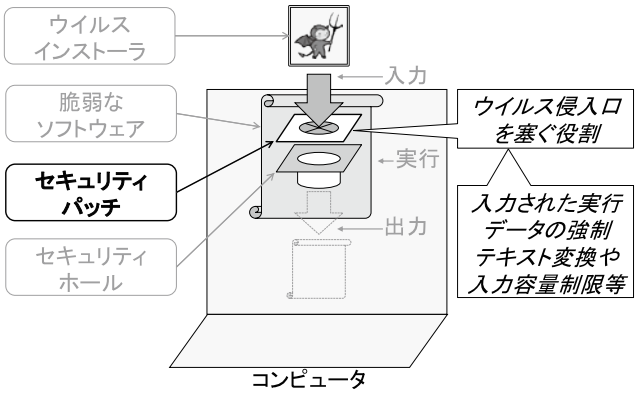
人間に例えると，食べ過ぎてお腹を壊した結果，普段は防げるウイルスに感染してしまうようなものである。このため，食事量を制限するような対策が有効となる。

ハッカーは，これら以外にも，次から次へと様々なデータ入力を試行する。想定外のデータは無限にある。いつかは，新たなセキュリティ・ホールが見つかってしまう。セキュリティの世界は，いたちごっこなのである。

セキュリティ・アップデート

ソフトウェアにセキュリティ・ホールが見つかると，直ちに，その脆弱性を解消する修正プログラムが配布される。この修正プログラムは「パッチ」と呼ばれる。また，パッチによる補強は，「セキュリティ・アップデート」と呼ばれる。パッチは，図－2に示す通り，

ウイルスの侵入口となるセキュリティ・ホールを塞ぐ役割を担う。具体的には，入力データの強制テキスト化や入力容量制限などで，プログラムとしての実行を防いでいる。



図－2　セキュリティホールへのパッチ当て

ハッキング技術は日々進化している。このため，セキュリティ・ホールは次から次へと見つかる。結果的に，ソフトウェアの多くがパッチだらけである。しかし，セキュリティ・アップデートは，セキュリティ・ホールの発見を意味する。すなわち，ウイルス感染の手口が明らかになったことを意味する。このため，セキュリティ・アップデートは迅速に行うべきである。

ところが，現実には，セキュリティ・アップデートを先延ばしするコンピュータの使用者も多い。作業が面倒なことも災いしている。この結果，ウイルス感染のリスクを非常に高めている。世界中で多くのコンピュータがウイルス感染している一因でもあるため，気を付けたい。

古いソフトウェアは危険！

アップデートによって，ソフトウェアの一般的な不具合も解消される。アップデートを重ねるにつれて，このような不具合は減る。このため，アップデートの頻度も低くなる。最後は，ソフトウェアがサポート対象から外される。

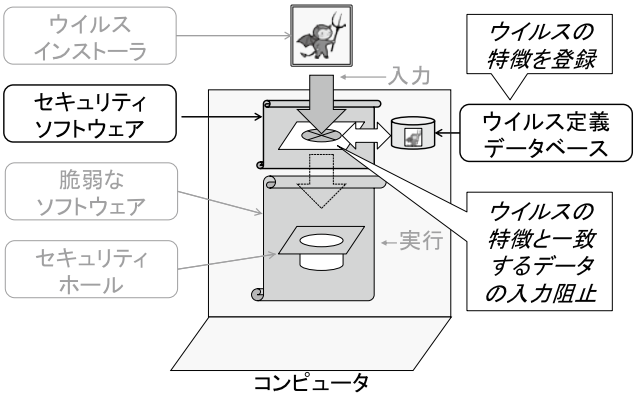
一方で，ハッキング技術の進展で，セキュリティ・ホールは次から次へと見つかっている。このことは，古いソフトウェアにも当てはまる。サポートが終了すると，セキュリティ・アップデートも行われない。この状況では，ウイルス感染のリスクが極めて高い。

このようなソフトウェアの使用は，できる限り控えたい。しかし，ソフトウェアの買い換えは，セキュリティ・アップデートよりも障壁が高い。このため，先延ばしされることも多い。有名な例は，既にサポートが終了しているWindows XPである。当時，ニュース報道でも，買い換えが呼びかけられた。それでも，文献2）によれば，現在でも相当数のコンピュータで使われている。現実の環境は，ハッカーにとって天国なのである。

ウイルス侵入のブロック

ウイルスに感染したコンピュータは，放置してはいけない。自分だけでなく他人にも被害をもたらす恐れがある。ウイルスの駆除には，セキュリティ・ソフトウェアを使用するのがよい。

セキュリティ・ソフトウェアは，図－3に示すように，ウイルスを検出するためのウイルス定義データベースを保有する。このデータベースには，ウイルスの特徴が数多く登録されている。セキュリティ・ソフトウェアは，コンピュータ上で常に動作し続けている。



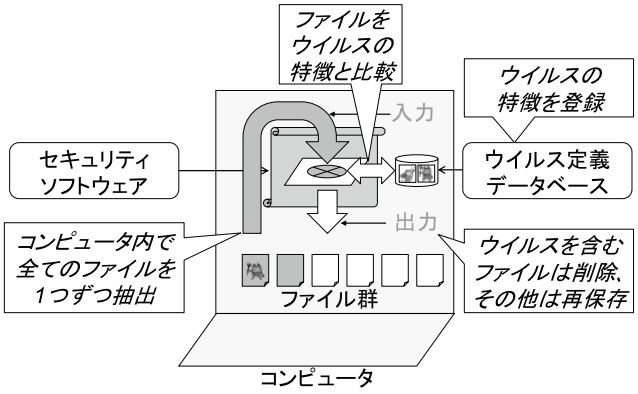
図－3　入力データのウイルスチェック

ウェブやメールを使用すると，コンピュータに外部からの通信データが入力される。セキュリティ・ソフトウェアは，入力がある度に，このデータベースを検索する。ウイルスの特徴と一致するデータがあると，該当データの入力をブロックする。また，その旨をコンピュータの使用者に警告する。このような動作で，常にウイルスの侵入を防いでいる。

感染したウイルスの駆除

ウイルス定義データベースに特徴が登録されていないウイルスもある。主に最新のウイルスが該当する。このため，セキュリティ・ソフトウェアを使用しても，最新のウイルスには感染することがある。しばらくすれば，このウイルスの特徴も，ウイルス定義データベースに登録される。しかし，ウイルスは既に感染してしまっている。このままではコンピュータ内に潜伏し続けることになる。

潜伏ウイルスの駆除には，図－4に示すように，コンピュータ内の全てのファイルについて，ウイルスチェックを行う必要がある。このような操作は，「完全スキャン」や「フルスキャン」などと呼ばれている。全てのファイルをウイルス定義データベースと照合するので，かなりの時間を要する。それでも，ウイルス感染の被害の大きさを考えれば，高い頻度で定期的に実施することが望ましい。

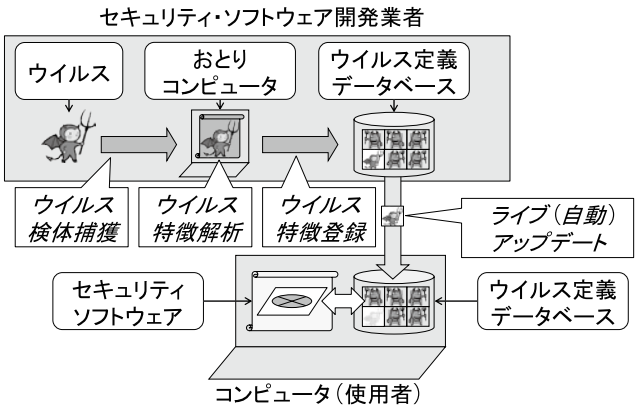


図－4　保存ファイルのウイルスチェック

ウイルス定義データベースの更新

ウイルスには亜種が数多く存在する。亜種のウイルスは，同じセキュリティ・ホールから同じ手段で感染する。しかし，プログラムの特徴が微妙に異なっている。これは，セキュリティ・ソフトウェアによるウイルス検知を免れるためである。

ウイルスの亜種は，次から次へと作成される。文献3）によれば，一日に約3万種類とも言われる。その都度，ウイルス定義データベースへの登録が必要である。図－5に示すように，セキュリティ・ソフトウェアの開発業者は，おとりのコンピュータを使用して，ウイルスを集めている。新種の検体を捕獲すると，これを解析し，その特徴を明らかにする。また，この特徴をマスターとなるウイルス定義データベースに登録する。この後，新ウイルス情報がセキュリティ・ソフトウェアの使用者に配布され，各コンピュータのウイルス定義データベースがアップデートされる。多くの場合，このアップデート作業は自動化されている。データベースの更新頻度はかなり高く，毎日何回か行われる。この更新を，コンピュータの使用者側で妨げないよう，十分に注意されたい。



図－5　データベースへのウイルス登録

コンピュータをしばらく使用しないと，ウイルス定義データベースも陳腐化する。久しぶりにコンピュータ使用する場合には，まず，このデータベースを更新したい。面倒ではあるが，大変重要である。

ウイルスの新種が生成されてから，ウイルス定義データベースが更新されるまでには，それなりの時間を要する。この間は，該当ウイルスが容易に侵入できてしまう。このため，ウイルス定義データベースを最新化した状態での完全スキャンも，忘れずに定期実施したい。

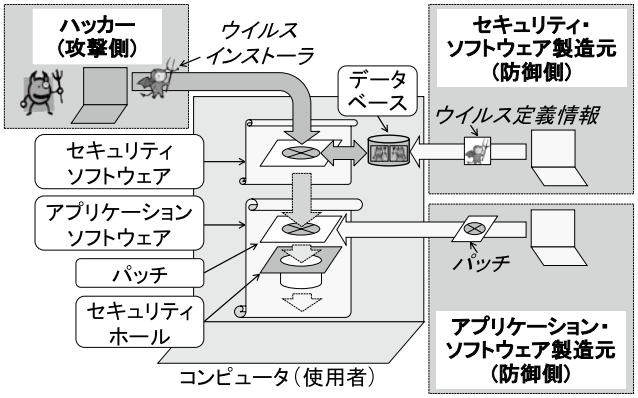
ウイルス対策は時間との競争！

これまで述べたとおり，ウイルス対策はいたちごっこである。図－6にも示す通り，時間との競争でもある。

ハッカーは日夜，セキュリティ・ホールの発掘を行っている。セキュリティ・ホールが発見されると，この脆弱性を利用した新ウイルスのインストーラが迅速に作成される。また，ありとあらゆる手段で拡散される。

一方，アプリケーション・ソフトウェア側でも，パッチが迅速に配布される。セキュリティ・アップデートを行うことで，新ウイルスへの感染リスクが低減する。このため，迅速なアップデートが重要である。

さらに，セキュリティ・ソフトウェア側でも，ウイルス定義データベースの更新が迅速に行われ，新ウイルスの特徴が登録される。これにより、新ウイルスが侵入するリスクを低減できる。



図－6　ウイルス対策における時間との競争

時間との競争で問題になるのは，コンピュータ使用者側の意識である。セキュリティ・アップデートの遅れや，ウイルス定義データベースの更新遅れなどは致命的である。しかし，現実には，ここがボトルネックとなっている。この結果，ウイルスに感染しているコンピュータが，世界中には数多く存在しているのである。

【参考文献】

1）配布ファイルの一部が不正改ざん，
<https://internet.watch.impress.co.jp/docs/news/651306.html>
2）「Windows XP」はなぜ今後も死なないのか，
<https://japan.cnet.com/article/35099761/>
3）データベースはどのくらいの頻度でアップデート，
<https://support.kaspersky.co.jp/2820>

（注1）専門用語では、「マルウェア」と呼ばれる。