・・・・6・・・・・

油断大敵ウイルスまみれ？

59 回生 Jack

今、話題沸騰の彼をご存知ですか？ 彼は多くの人に影響を及ぼし、多数の企業が彼に出資するお金は相当な物です！ マスコミも彼をこぞって取り上げ、彼についての記事やウェブサイトが五万とあります。そう、この記事はそんな彼「コンピューターウイルス」とそれを巡る攻防についてお話しします。

なお第 1 章は基本的な知識の解説の為、分かる人は読み飛ばして頂いて構いません。

基本知識

『実行ファイル』と『データファイル』

パソコン上にあるファイル（データ）は大きく分けると 2 つに分けられます。『実行ファイル』と『データファイル』です。『データファイル』は文字や画像のデータなどが格納されています。一方『実行ファイル』にはパソコンに対する命令が格納されています。『データファイル』と『実行ファイル』を見分けるには拡張子を見るのが一番です。拡張子とはファイルの末尾についている『.txt』や『.jpg』などの文字です。この部分で Windows はファイルの種類を見分けています。『.txt』はメモ帳などで作成される、文字データで出来たファイルで、『.jpg』は写真のデータなどを格納する画像ファイルです。『実行ファイル』はファイルの末尾に『.exe』や『.com』がついているもので、コンピューターに対する命令が格納されています。また、厳密には実行ファイルではありませんが拡張子が『.vbs』や『.js』はスクリプトファイルと言って、実行ファイルに比べて機能の制限がありますが、実行ファイルのようにコンピューターへの命令が格納されています。

「ファイルの後ろにそんなのついてないよ？」といわれる方がいるかもしれませんが、それは Windows の設定で表示しないようにしているだけで、設定を変更すれば表示されます。この拡張子は非常に重要で、これを変えると Windows はそのファイルに対する動作を変更してしまいます。例えば日記を書いた『Nikki.txt』を『Nikki.mp3』にファイル名を変更すると、本来メモ帳が起動し『Nikki.txt』の内容を表示する筈が、『Nikki.mp3』を起動して音楽を再生しようとします。当然、Nikki.mp3 の中には音楽のデータは入っていないため音楽は再生されません。

感染までの攻防

知らない人はあまりいないと思いますが、コンピューターウイルスとは単純に言えば感染したコンピューターに使用者が望まない動作をさせるものです。私たちが覚えなければいけないのは「コンピューターウイルスを感染させるにはコンピューターに命令を実行させなければならない」という非常に重要な事実です。すなわちデータファイルを開いただけでは、基本的には（あくまで基本的には）ウイルスに感染しません。危険な

のは『実行ファイル』を開いた時です。実行ファイルにはコンピューターに対する命令が含まれるため、色々な悪意に満ちた行動をコンピューターに行わせる事が出来ます。例えばデータを全部消したり、無意味に CD トレイを開け閉めしまくったり。

そこでコンピューターウイルスが狙ってくるのは常に『相手にウイルスを感染させる実行ファイルを実行させる』事なのです。それを巡ってウイルス作者とウイルス対策側は常に知恵を働かせます。その知恵の数々を紹介しようというのがこの章の趣旨です。

ケース：Happy99

コンピューターウイルスが狙ってくるのは常に『相手にウイルスを感染させる実行ファイルを実行させる』事、と言いましたが、その『ウイルスを感染させる実行ファイル』はどこから来るのでしょうか？もちろん人間にとってのウイルスの様に空気に漂って来るなんていう事はありません（そんな事になると大惨事）。昔は、CD やフロッピーディスクに入っている事が多かったのですが、最近の実行ファイルは大半がインターネットからやってきます。インターネットにある『ウイルスを感染させる実行ファイル』をダウンロードして実行すれば、そこでもう負けです。ウイルスに感染してしまいます。しかし、普通は『ウイルスを感染させる実行ファイル』をインターネットで配布すればたちまち「あそこはやばい」と噂がたちばれてしまいます。そこで電子メールに実行ファイルを添付して相手にダウンロードさせる手法がかなり用いられています。

しかし、もし知らない人から「これはウイルスですよー」というタイトルのメールに添付ファイルがついていたら貴方は実行しますか？しませんよね。しないで下さい。

この Happy99 もそんなメールの添付ファイルによって広がるウイルスの一つです。このウイルスはメールに添付された『Happy99.exe』というファイルを実行すると感染します。このファイルを実行すると花火の絵が表示されるのですが、そんな物は囮で、実際はインターネットに接続する際に実行されるソフトを改ざんして、メールを送るたびに『Happy99.exe』を添付させる様にします。

そう、このウイルスの凄い所はここです。これによって受け取った側は「おっ、○○からじゃーん」と知り合いからと油断して添付ファイルを実行してしまいます。そして感染した人からも『Happy99.exe』が添付して送信され、その知り合いにも……。と、どんどんウイルスは拡大していきます。

教訓：メールに実行ファイルが添付されていても開かない。それがたとえ知り合いからのメールでも。

ケース：ラブレター

このウイルスも Happy99 と同じ様にメールで広がるウイルスです。このウイルスは感染した人から「I love you」というタイトルで送られて来て、本文には「私のラブレターを添付しました。是非読んでください」と書かれており、「LOVE-LETTER-FOR-YOU.TXT.vbs」というファイルが添付されています。

このウイルスで注目すべき点は 2 つあり、ひとつは添付ファイルである「LOVE-LETTER-FOR-YOU.TXT.vbs」の拡張子です。本来、このファイルの拡張子は「.vbs」で、スクリプトファイルです。普通スクリプトファイルを受け取ると、「うわっ、あやしー。こんなファイル開けねーよ」と言う事になるのですが、この場合 Windows で『拡張子を表示しない』という設定にしていれば本当の拡張子「.vbs」は消され、拡張子が

「.txt」であるかの様に表示されます（LOVE-LETTER-FOR-YOU.TXT）。それを実行すると、はいアウト。ウイルスに感染です。

もうひとつはそのタイトルです。「I love you」、……いい響きです。私はこの学校に入ってからラブレターなんざ貰った事がありません（同級生にもらっても嫌ですが）。もし、このウイルスの発信主がウイルスに感染した知り合いの女の子だった場合は思わず開いてしまうかもしれません。そういう人間心理をついたタイトルでこのウイルスは拡大していきました。このウイルスの作者は悪魔だと思います。

教訓：拡張子は表示する。冷静に考えて、来ないラブレターは警戒する。

ケース：山田ウイルス

ファイル共有ソフト上で配布されている事が多いウイルスです。このウイルスは正常なファイルを装っています。稚拙な物は「ファイル名.txt　　.exe」と本来の拡張子を遥か後ろにする事によって、ファイルを一覧表示した場合に「.exe」の部分を画面外にはみ出させ、無害なファイルと思わせ実行させます。

なお高度な物は、本来のソフトウェア（ゲームのインストーラー）を装い、起動すればゲームが動くのですが、それと同時にウイルスに感染させます。この場合、拡張子は「.exe」だと分かってファイルを開く為、拡張子でウイルスだと判断するのは不可能です。

近頃話題の Winny による情報流出はだいたいこのウイルスと似た構造を持っています。まあファイル共有をしない限りは触れる機会はあまり無いと思われるので、そんなに警戒しなくてもいい様な気がします。

教訓：とにかく拡張子に注意。怪しい実行ファイルは実行しない。

ケース：メリッサ

さて、今までのウイルスの拡張子は『.exe』や『.vbs』など、実行ファイルのものでした。ですがこのウイルスの拡張子は『.doc』、そう Word と同じなのです。このウイルスは Word ファイルのマクロ機能を使って命令を実行させます。そのため、一見普通の Word ファイルにしか見えません。そのためこのウイルスもかなり感染が拡大したらしいです。似たようなものに Excel のマクロ機能を使った Laroux（ラルー）というウイルスがあります。

またこのウイルスは、メールのアドレス帳にある人に自分を送信しまくります。これによって『Happy99』や『ラブレター』の様に、「知り合いからのメールやから大丈夫やろー」と油断させて感染を広げるのです。しかも拡張子が『.doc』であるため警戒はしづらいです。しかも、本文には「ご依頼の文章です」とどうとでもとれるものが入れられます。

このウイルスはウイルス対策ソフトが無いとちょっと対応しづらいですね。

教訓：がんばって！

ケース：Blaster

これはエグい。今まで紹介したウイルスはコンピューターの使用者が注意すれば防げ

ましたが、このウイルスは違います。このウイルスは Windows のセキュリティ上の欠陥を利用して、知らない内にウイルスに感染する命令が実行されます。しかもこのウイルスはコンピューターをつけてもつけても強制的に終了させるため、コンピューターに詳しく無い人にとっては対策は困難です。

とりあえず対策としては WindowsUpdate を使用して、Windows のセキュリティ上の欠陥を訂正するしかありません。パーソナルファイアーウォールやルータのパケットフィルタリングを使用する方法もありますが、少し知識が無いと難しいと思います。

まあ最近では、Windows 上での対策も進んでおり、自動的に WindowsUpdate をしてくれたり簡単なファイアーウォールを設定してくれたりはするみたいなので、そんなに心配する必要は無いと思いますが、一応自分のパソコンの状態を確認してみるのがいいと思います。

ケース：Nimda

このウイルスは色々な感染経路がありますが、私たち一般ユーザーに主に関連があるのは、『ウェブページを見ると感染する』ケースです。

私たちが Nimda に感染したウェブページにアクセスすると、Internet Explorer というウェブブラウザ（ウェブページを見るときに起動する青い『e』の奴）のセキュリティ上の欠陥を利用してウイルスに感染する命令が実行されます。これも上にある Blaster ウイルスと同じで、注意すればなんとかなるというものではありません。とにかく WindowsUpdate で欠陥を訂正して下さい。なお、この Nimda に利用されるセキュリティ上の欠陥は Internet Explorer の『Java スクリプト』や『ActiveX』といった機能に含まれる物なのでその機能を切る事によって対策は可能です。まあ一部のページが見れなくなっちゃうんですけどね。

後、もう一つ私たちに関わりがある感染経路は『メールを見ると感染する』です。添付ファイルを開いたらでは無く、メールを見ると感染してしまうため、これも注意してなんとかなるものではありません。Outlook Express などの内部で Internet Explorer を使用しているメールソフトの脆弱性を利用するため、もっとマイナーなソフトを使えば防げます。

また、メールには 2 種類あって、文字だけの普通のメールとウェブページの形式を使用した html メールがあります。このウイルスは html メールでのみ作動するため、『html メールを受信しない』設定をＯＮにしていれば防げます。

教訓：

このウイルスは非常に多くの教訓を含んでいます。まず、『WindowsUpdate をこまめに行う』です。マイクロソフトもウイルスが出たらあらかたちゃんと対応してくれています。『WindowsUpdate』を行う事は脆弱性を利用するウイルスを防ぐために必須です。

次に『Java スクリプトや ActiveX をなるべく切っておく』です。まあ、これらを利用しているページも多いため、絶対にしろとは言えないのですが……。あとこれと同じで『html メールを受信しない』もＯＮにした方がいいです。また html メールを送らないのも礼儀だと思います。

後、やはり Internet Explorer を使わないという手があります。表示できないページもありますが、ウイルスの作者は感染を拡大させるべくメジャーなソフトを狙います。

Opera や Netscape などのウェブブラウザを使っていれば感染しないウイルスも結構あると思いますよ。

まとめ〜

ウイルスの感染経路に注目して書いてきました。ウイルスに恐怖心を持たれた方がいるかもしれません。ですが、私は『ちゃんと対策していればウイルスは容易に防げる』と考えています。添付ファイルなんか開かなければいいんです。Internet Explorer も使わなきゃいいんです (Windows を使わなければもっといいんですが)。WindowsUpdate も設定すれば自動でやってくれます。さらにウイルス対策ソフトをいれれば余程運が悪くない限り大丈夫でしょう。

とにかく知識さえあればウイルスは防げます。余裕です（たぶん)。肩の力を抜いて頑張ってください。