



知っておくべき

ウイルス感染

防御術

<誰もが驚く、スマホやタブレット、PCの新たなウイルス感染手法>

ここ数年、情報端末（PC、スマホ、タブレット）をウイルスに感染させる手法がかなり変わってきており、その中には「ええ？こんな簡単にウイルス感染させられるの!？」とびっくりする物もあります。

ここ数年で出てきた「新たな感染手法」の中には、かなり巧妙にやられる方法があったりするのです。

従来知識のままでセキュリティ対策をしていると、いつの間にか会社や個人のスマホ、タブレット、PCがウイルスに感染し、大事な情報がダダ漏れ状態になってしまいます。

日本においては、ウイルス防御の知識が不完全な方が多く、その啓蒙のために本書を公開するに至った次第です。

（本書の内容は、サイトで公開した情報をベースに記載しております）

<アンチウイルスソフトは、全てのウイルスを防御する物ではない>

PCの場合、最低でもまともな会社が製作したアンチウイルスソフトを入れておくべきです。

(フリーソフトの中には、実はそのアンチウイルスソフト自体がウイルス感染させるソフトだったりするので注意を。もしお金がなくてフリーのアンチウイルスソフトを使う場合は、有名な物を使用するように。)

しかし、『アンチウイルスソフトを入れても、全てのウイルスを防御してくれるものではない』という事を、きちんと理解しておかないといけません。

『アンチウイルスソフト入れたから、もうウイルスには感染しない』ではなく、どうしても新種とかだと検知できず、入れててもウイルス感染してしまう事があるのです。

アンチウイルスソフトを入れた上で、これ以降に記す色々な事に注意しないと、結局あなたのPCやスマホ、タブレットが簡単にウイルス感染させられ、大事なデータが勝手に消されたり、重要な情報やあなたの趣味・嗜好がネットにダダ漏れになるのです。

<メールによる感染いろいろ>

昔からよくある、『メールの添付ファイルを開いたらウイルス感染した』は未だにあるので、基本的にメールに添付されたファイルは開かない事。

最近でも、アホな国会議員がこれをやってしまい、官公庁のPCを大量にウイルス感染させたって話がありました。

あからさまに怪しいメールの添付ファイルを開かないのはもちろん、知り合いや取引先企業を装って添付ファイルを開かせようとするケースもあるので注意を。

メールについては添付ファイルにだけ注意しておけばいいかというと、そうではなく、『htmlメール』についても気をつけないといけません。

一時期、『html形式のメールを閲覧しただけでPCがウイルスに感染した』という事がありました。

現在はアンチウイルスソフト側でこういうメールに対処するようになりましたが、いつ新しいコードが開発されてまた感染させられるかわかりません。

メールソフトについては、基本的に『html表示』はOFFにして『テキスト表示』のみで閲覧するようにしましょう。

どうしてもhtml形式で確認する必要があるメールのみ、html表示で閲覧してください。

なお、アマゾンのアソシエイト成果のメールを装って、html形式のメールを閲覧させてウイルス感染させようとしたケースも過去にありましたので注意してください。

<外部メディアからの感染>

ウイルスに感染したUSBメモリや外付けHDDを接続してウイルス感染させられるケースもあります。

オートランとか切っておくべきです。詳しいやり方は検索エンジンで調べましょう。

<現在のウイルス感染の主流は……>

で、最近のウイルス感染は、『ウイルス感染させるコードを仕込んだサイトを閲覧させて感染させる』が主流になっています。

これには本当に注意しないとイケません。

みなさんのところにも毎日大量の迷惑メールが届いていると思いますが、その大半はウイルス感染させるのが目的だったりします。

詐欺や勧誘目的もありますが、実は迷惑メールのその大半が、日本語で書かれていながら、ウイルス感染させる目的で海外から送信されたりしているのです。

色々な面白文章、勧誘文章を書いています、実はその中身にはあまり意味はないのです。

迷惑メールは、そのどれもが色々な文面で気をひいて、メール本文中のurlリンクをクリックさせようという風になっています。

で、ついそのurlリンクをクリックすると、ウイルス感染させるコードを大量に仕込んだサイトが開かれて、色々なウイルスに知らないうちに感染させられると。

最初の方に書いたとおり、アンチウイルスソフトを入れてても、それが反応しないような新種のコードが日々開発されて、サイトを開いただけで普通に感染させられるのです。

だから、一目で迷惑メールとわかる物は、メール本文中のurlリンクは絶対クリックしない事。

というか、タイトル見ただけで迷惑メールとわかったら、メール自体開かずに削除しましょう。フィルタリングソフトでゴミ箱にそのまま選り分けるのもいいですが、普通のメールまで間違っ
て振り分けされないよう、キーワードの設定には注意してください。

また、一見迷惑メールには見えず、偽装されたメールでurlリンクをクリックするよう促してくる物もあります。

大手サイトの名前を騙ったり、銀行の名前で『すぐにこちらのページにアクセスしてください』だったり。

最近ではショッピング情報を装って、悪意あるサイトへのurlリンクを踏ませようとするのがあります。

「お買い得セール情報」みたいな感じで。

こちらのNAVERまとめで色々な迷惑メールのパターンが紹介されていますので、一読しておくといいでしょう。

[ウイルスに感染させたくて必死な迷惑メール。メールをタイプ別に分けてみた](#)

<掲示板やブログ、動画のコメント欄でのurlリンク誘導もある>

urlリンクをクリックさせて、悪意あるサイトを開かせてウイルス感染させる・・・というのは迷惑メールだけじゃなく、掲示板や、ブログのコメント欄、youtubeやニコニコ、など動画サイトのコメント欄、twitterなどで短縮urlをクリックさせて飛ばす、というのもあります。迷惑メールだけでなく、色々な場所でもurlリンクは気軽に踏まないようにすべきです。

掲示板で、『新作ゲームの画像です』みたいな感じでurlリンクが貼られるとつい踏んだりする人がいますが、その中には悪意あるリンクも普通にあったりするのです。

末尾がjpgとかpngとかでも、画像ファイルだけ開かれるのではなく、サイトごと開かれて感染させられるケースもあります。

開いた本人は感染させられた事にすら気づかず.....。

掲示板やブログのコメント欄、動画サイトでの各動画についてのコメント、twitterでのurlリンクなどは、くれぐれも気軽に踏まないように。

<トラップサイトの話>

ウイルス感染させるのが目的で記事内に悪意あるサイトへのurlリンクを貼りまくってるブログやサイトもあります。

健康に関する情報を紹介するブログやサイトが大量に作られています。その中には、役に立つ情報を紹介しつつ、実は変なサイトへのリンクがあちこちに貼られている物があったり.....。

役に立つ情報は『撒き餌』で、それで油断させて悪意あるサイトへ転送して感染させるのが目的です。

(中には、アフィリエイトが目的のもありますが)

<改竄されたサイトは、しばらくは見に行くな>

たまに、特定のサイトが改変されて話題になる事もあります。

政府や有名メーカーのサイトの一部が改変されて、それがニュースになると、まだサイト内の全ての安全が確認されていないのに、つい覗きにいく人がいるでしょう。

これは、自分からウイルス感染しにいくような馬鹿な行為なので、絶対やめておくべき。

改竄されたサイトは、アンチウイルスソフトが検知できないような新種のウイルスを仕込まれている事が多く、アンチウイルスソフトをインストールしてても簡単にウイルス感染してしまうのです。

あからさまに改変されたページではなく、それにつながったページが、見た目は改変されず、それでいて変なコードが仕込まれる場合もあつたりします。

<ネット閲覧に特化した端末を持つのがおすすめ>

『迷惑メールや色々な場所でurlリンクを気軽にクリックするな』と言っても、それを全てやりきれるものではありません。

実際、これをやろうとすると、本当に不便になってしまう。

だから、以下の方法を是非おすすめしたい。

最近、スマホ・タブレットで一部flashサイトを除きネットを問題なく閲覧できるようになっているので、今後はもうPCのブラウザでサイトを見るのをやめて、サイト閲覧は安物のスマホ・タブレットをそれ専用にとって、見るのです。

二、三万円くらいで買えてしまえるので、安めのスマホ・タブレットを買って、webサイトを見なくなったらこっちで閲覧するように。

海外直輸入の激安タブレットだと、コストを抑えるために危険なリチウムバッテリーを搭載している物もあり、突然家が火事になる恐れもあります。

安めのスマホ・タブレットと言っても、国内で流通しているきちんとした製品を買うようにしましょう。

ネット閲覧専用の安物スマホ・タブレットを買って、それでウェブサイト閲覧だけし、メールのやり取りや大事なデータはそのスマホ・タブレットではやらない・入力しない。

こうすると、万が一、そのスマホやタブレットがウイルス感染しても、大事なデータは漏れなくなります。

そもそも、PCのウェブブラウザと、スマホ・タブレットのブラウザでは、マルウェアの感染しやすさが全然違ったりします。

PCだと、紹介したように悪意あるサイトを開くとjavaスクリプトやその他のコード、ブラウザのセキュリティホールを使って、PCに勝手にウイルスファイルがダウンロードされ、勝手にインストールされて常駐する事になります。

WINDOWSのUACをONにしていると、警告してくれたりするけど、これも万全ではありません。

一方、スマホやタブレットでは、標準のブラウザでjavaスクリプトなどの機能はついているものの、OSやブラウザがサンドボックス化されているせいで、javaスクリプトでOSの領域に勝手にウイルスプログラムをインストールして起動させる、なんて事はできないのです。

これは、あくまで現時点の話で、将来的にも保証できるものではありませんが、今のところは悪意あるサイトをいくら開いても、スマホ・タブレットでは本体のシステム領域に常駐して悪さをするウイルスには感染させられないのです。

PCでも、そういうサンドボックス化して、『悪意あるサイトを閲覧してもウイルス感染しないブ

ブラウザ』ってのが一部開発されていますが。

ただし、android端末の場合は、「ウェブブラウザでのアプリインストール」をONにしていると、知らないうちにウイルスアプリをインストールしてしまうので、基本的にアプリ開発者以外はこの機能はOFFにしましょう。

<公式マーケットでも悪意あるアプリが大量に登録されている>

スマホやタブレットの場合、ブラウザで悪意あるサイトを閲覧しても問題はないのですが、『自分から悪意あるアプリをインストールしてしまう』という事があります。

アップルのストアはアプリ登録時やバージョンアップ時に、厳重にプログラム内容を審査して、不正なアプリでないかどうか確認するようになっています。

おかげで、ほとんど不正なアプリはストアに登録できないようになっています。

でもゼロではありません。過去に変なアプリが登録された事がありました。

一方、androidの場合、googleの審査が緩いせいで、android公式のマーケットであるgoogle playに、悪意あるアプリが頻繁に登録されてしまっているのです。

で、そういう悪意あるアプリをインストールしてしまうと、端末内の色々なデータを漏洩したりするのです。

ぱっと見は普通の役に立つアプリに見えて、実は情報漏洩のために開発されたアプリが、googleの公式アプリマーケット、google playでは大量に登録され、後でセキュリティ会社の検査で頻繁に見つかったりしているのです。

<パスワード記憶アプリによるパスワード情報漏洩>

最近よく利用されている『パスワードを記憶してくれるアプリ』も注意しないといけません。

『色々なサイトのパスワードを暗号化して記憶できる安全なアプリですよ』とうたっておいて、実際は外部にじゃんじゃんパスワード情報を漏洩したりするのが結構あるのです。

見た目だけではどの記憶アプリが安全でそうでないかは判別できないため、セキュリティ会社各社は有名メーカーの出しているパスワード記憶アプリ以外は絶対使用しないよう呼び掛けています。

また、twitterやpixivの閲覧アプリでも、ログイン時のパスワード情報を外部に送信する不正なアプリがありますので、有名どころの安心できるtwitterやpixivビューワーアプリ以外は使わないようにしましょう。

<PC用おすすめフリーソフト、スマホ・タブレット用おすすめアプリの『まとめ』には注意すべき>

ウイルス感染させる側は、『どれだけ多くの人を感染させるか』を日々考えていたりします。その際に利用されるのが、『PC用お薦めフリーソフト』や、『スマホ・タブレット用お薦めアプリ』を紹介する掲示板のスレッド

悪意あるPC用ソフトや、スマホ・タブレット用アプリを開発してandroidのマーケットに登録したら、後は自演でそういうスレッドに「おすすめソフト（アプリ）」として書き込むと、数多くある2chまとめサイトが勝手に転載して、インストールする被害者を増やしてしまう……。

かなり歴史のあるフリーソフトならともかく、聞いた事もないようなソフトの場合、『おすすめソフトとして紹介されているから』という事で安易にインストールすると、PCやスマホ・タブレットがマルウェアに感染させられるので注意を。

最近2chまとめサイトで紹介された「おすすめアプリ」をスマホやタブレットにインストールする方も多いですが、実はこれはものすごく危険な事です。

転載したサイト管理人は一つ一つのアプリの安全性を全然確認しておらず、中には「情報漏洩系のアプリが、（アプリ作者の自演で）おすすめアプリとして紹介される」という事もあり、そういうのを「2chまとめサイトで便利アプリとして紹介されているから」という事でインストールしてしまうと、知らないうちにあなたの大事な情報がダダ漏れ状態になってしまうのです。

同じような感じで、「このサイトはブックマークしておくべき」というまとめでも、役に立つサイトに紛れて、悪意あるサイトまでが平然と紹介されて、「urlを開いただけで、知らないうちにウイルス感染させられる」という被害者を増やしているケースがあるので注意してください。

<MODや日本語化ファイルはありがたいけど……>

ちょっと変わった方法としては、PCゲームのMODファイルや日本語化ファイルにウイルスを仕込ませて配布する方法もあります。

グラフィックやゲームバランスを改変したりマップを拡張できるMODは面白いのだけど、MODファイルや日本語化ファイルをダウンロードすると、ウイルスファイルも一緒に入っていた、なんて事もあるから注意。

<中古PCや中古スマホ・タブレットはお薦めできない>

中古のパソコンやタブレット・スマホは、新品で買うより安く買えたりするのが利点ですが、ウイルス感染予防の観点からはあまりお薦めできません。

前の所有者が使用中にウイルスに感染していた場合もあり、そのまま気づかずに使用してしまっ
て情報漏洩や大事なデータが消えてしまう事があるからです。

どうしても中古のパソコンやタブレット、スマホを使う場合は、

1・機器のウイルスチェックが終了するまでは、USBメモリやUSB HDDを接続しない事（スマホ
やタブレットの場合はPCに接続しない事）

どこかのサイトにログインしてパスワードを入力すると、そのパスワード情報が漏れる場合があ
るので注意。

2・中古パソコンやタブレット、スマホを受け取ってすぐやるべき事は、工場出荷段階への初
期化と、その次にはダウンロード販売サイトからウイルス対策ソフトを買って入れ、さらに全領
域ウイルスチェックをやる事。

を必ず守ってください。

お店によっては、中古ハードは初期化やウイルスチェックをやってから販売しているところもあ
りますが、オークションなどで個人売買した場合はそういう事がきちんとされておらず、ハード
がウイルス感染してる場合があります。

上記の事をきちんとやっても、スマホやタブレットの場合、ウイルスチェックの際に完全にウ
イルスを取りのぞけない場合もあります。

また、パソコンの場合も、ウイルスがアンチウイルスソフトメーカーに報告されていない特殊な
ウイルスの場合は、ウイルスが発見されずにそのまま残る場合もあります。

やはりそういう観点からも、中古ハードを買って使用するというのは、お薦めできません。

<悪意あるサイトへのurlリンクをブログや掲示板、その他の場所に貼ると逮捕されます>

ところで、愉快犯的に掲示板や、ブログや動画サイトのコメント欄など、あちこちに、『ウイルス感染する悪意あるサイトへのurlリンク』を書き込むとどうなるか、みなさん知っていますか？
ウイルス保管・作成・配布罪が施行された今では、普通に逮捕されちゃいます。

『不特定多数をウイルス感染させちゃえ』と思ってurlリンクを貼ると、ある日あなたの家に突然警察が来る事になるので注意してください。

ブログだけど、悪意あるサイトへのurlリンクを貼っていたやつが逮捕された事が実際にあり、
ニュースで紹介されました。

自分がやらない事はもちろん、家族がこういう事をやっってしまうわないよう、日頃から注意しておくべき。

まとめると……。

- ・ アンチウイルスソフトは、全てのウイルスを防御できる物ではない。それを念頭に置いてしっかり対策せよ。
- ・ メールのお添付ファイルは基本的に開くな。
- ・ メールソフトでhtml表示はOFFにすべき。
- ・ USBメモリや外付けHDDからのウイルス感染には注意。
- ・ 迷惑メールや偽装メールでは、絶対urlリンクはクリックするな。
- ・ 掲示板やブログ、動画サイトのコメント欄などでもurlリンクはクリックするな。（PCのブラウザでは）
- ・ twitterで短縮urlをクリックさせてウイルス感染するサイトへ飛ばすケースもある。
- ・ PCのブラウザでなく、スマホやタブレットのブラウザで今後はサイトやtwitterなどを見るようにした方が安全
- ・ 大事なデータを入れてないスマホ・タブレットを用意して、それでサイト閲覧するようにしたら、もっと安全
- ・ 改変されたと話題になっているサイトを自分から見に行くな。ウイルス感染の元。
- ・ パスワードを記憶してくれるアプリは便利だが、逆にパスワード情報がダダ漏れになる事がある。
- ・ pixivやtwitterアプリでもパスワード情報を外部に送信する物がある。
- ・ 『PC用おすすめフリーソフトまとめ』や『スマホ・タブレット用おすすめアプリまとめ』を見て安易にソフトをインストールすると、悪意あるソフトウェアを入れてしまう事がある。2chまとめサイト管理人は、個々のソフトを検証せずにスレッドを転載してるだけ
- ・ 悪意あるサイトへのurlリンクを掲示板やブログ、動画サイトのコメント欄など、色々な場所

に愉快犯的に貼ると、警察に捕まるので注意。

これらの事は、『自分だけ』が注意して、家族がおざなりになっているとダメです。一台のPCを家族で共用していると、家族がひっかかってPCがウイルス感染してしまいます。共用していなくても、同一家庭内LANで、一部の端末がウイルス感染するのは危ないです。自分はもちろん、家族もウイルス感染予防のためにきちんと勉強すべき。

また、対策を覚えても、人は時が経つにつれ忘れてしまいます。本書は必ず半年に一回は見返すようにして、個人や会社の情報端末がウイルス感染して、大事な情報がダダ漏れ状態にならないように気をつけてください。

漏れた情報によっては、長くついていた仕事を辞める事になったり、恥ずかしい個人の嗜好がネットに永遠に残る事になって、今後の人生がかなり苦しくなる事もあります。