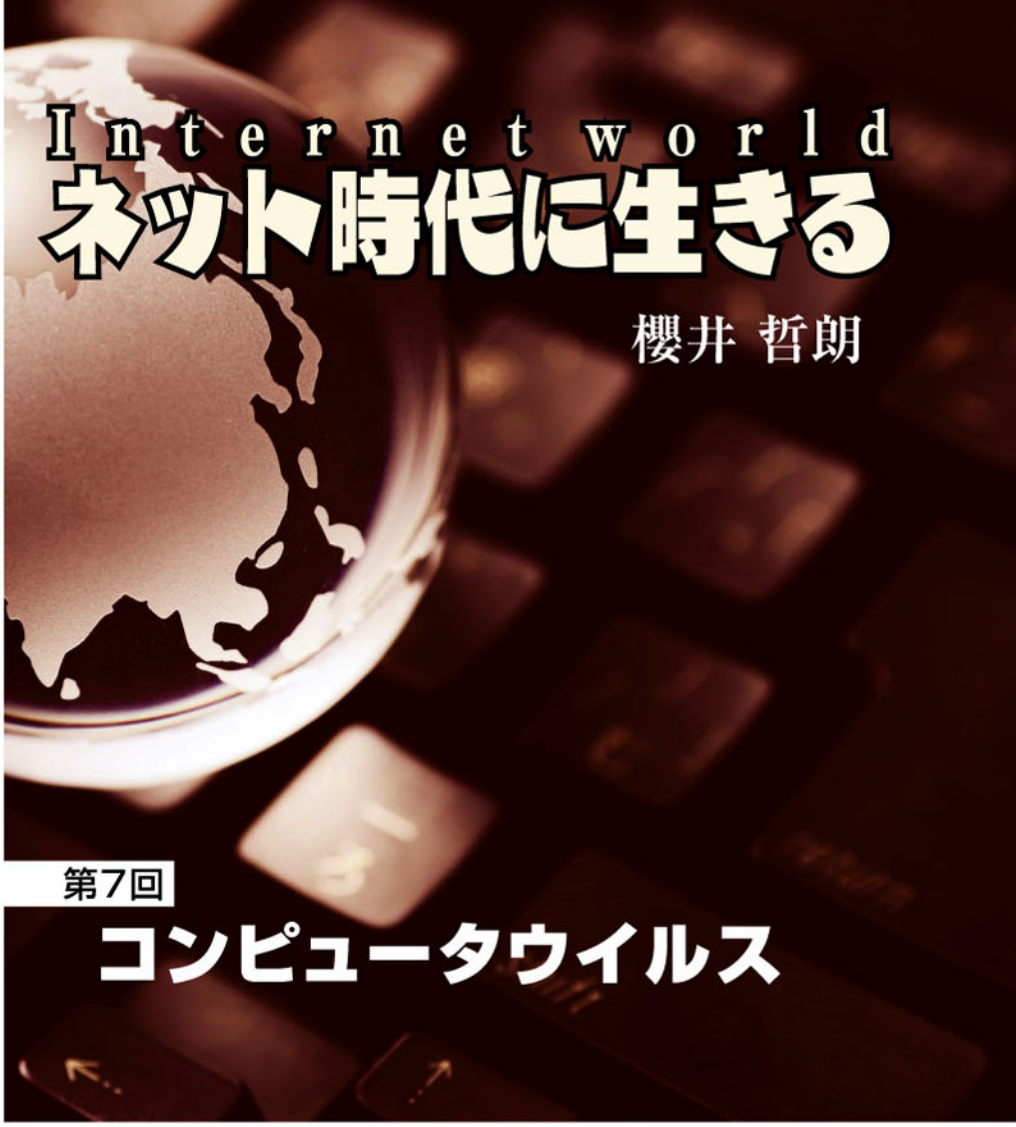


Internet world

ネット時代に生きる

櫻井 哲朗

第7回

コンピュータウイルス

被害者のつもりが加害者
急増のスマホ攻撃を警戒

桜の花も散り、春の不安定な天候も一段落した今日この頃、みなさんはいかがお過ごしですか。どうやら今年の桜は例年よりも1週間から2週間ほど早い開花となったようです。みなさんも何となくではありますが、例年よりも早いかなと思ったかもしれません。桜の開花は、冬と春の気温が密接に関係しています。今年は寒い冬と暖かい春が桜の開花を早めたようです。

ちなみに、北海道では5月の中ごろに開花日もむかえるところもあり、お花見がまだという方は北海道に行けば楽しめるかもしれませんね。なんで、こんなに桜のことについて詳しく書いたのかと謎に思った方もいるかもしれませんが、答えは単純、それは私が櫻井だからです。

刑事罰が適用され

さて先週は新年度の始まりということでインターネット犯罪に焦点を当てて書いていきました。そこで、2011年に施行された通称「サイバー刑法」について触れさせていただきました。これは、「情報処理の高度化等に対処するための刑法等の一部を改正する法律」のことであり、同法はサイバー犯罪に対応するため刑法ならびに関連法の改正を行う法律です。この法律の改正によって、ウイルスの作成・提供・取得・保管した場合に刑事罰が適用できるようになりました。

また、たとえ自分が作成した場合でなくても他のコンピュータにウイルスを感染してしまった場合、業務妨害罪が適用される可能性があります。このとき、5年以下の懲役又は100万円以下の罰金が課せられます。さらにウイルスに感染させられた相手側から損害賠償を請求される場合もあります。このようなことから、前回と同様に被害者にも加害者にもならないために、今回はコンピュータウイルスとそれに対するセキュリティについて説明させていただきます。

コンピュータウイルスとは？

人間に感染して？

みなさんはコンピュータウイルスと聞くとどのようなイメージをもたれるでしょうか。一昔前ですと、コンピュータウイルスに感染したコンピュータは爆発させられるようなイメージもありました。有名なハリウッド映画では、コンピュータウイルスを使って異星人の戦艦を叩くという描写があったりもしました。

有名なアニメ「エヴァンゲリオン」では、コンピュータウイルス

に化けた使徒という架空の生物が登場したりしました。またパチンコにもなっております攻殻機動隊というアニメでは、未来の日本が舞台となっており、そこでは科学技術が発展して脳から直接インターネットに接続できるようになった世界を描いています。そこでは、コンピュータウイルスに感染した人間が自殺するというストーリーがあったりしました。

不正なプログラム

現実の私たちの世界でも、脳波を解析してそれを電気信号に変換することによって機械を動かすブレイン・マシン・インターフェイス(Brain Machine Interface：BMI）という技術の研究が行われております。皆さんに身近なものですとNeuroSky社から販売されている脳波で動く猫耳のかぶりもの「necomimi」などがあったりします。

ちなみに著者の密かな野望のひとつに、この猫耳の技術と防衛省が開発した「空飛ぶ球体」の技術をあわせることでガンダムに出てくるようなフィン・ファンネルのようなものが作れるのではと画策しております。すみません、話がそれました。

コンピュータウイルスとは、広い意味でコンピュータに被害を及ぼす不正なプログラムを指します。また経済産業省のコンピュータウイルス対策基準ではコンピュータウイルスの定義を次のように定めています。

ウイルスの機能

第三者のプログラムやデータベースに対して意図的に何らかの被害を及ぼすように作られたプログラムであり、次の機能を一つ以上有するもの。

(1)自己伝染機能

自らの機能によって他のプログラムに自らをコピーし又はシステム機能を利用して自らを他のシステムにコピーすることにより、他のシステムに伝染する機能

(2)潜伏機能

発病するための特定時刻、一定時間、処理回数等の条件を記憶させて、発病するまで症状を出さない機能

(3)発病機能

プログラム、データ等のファイルの破壊を行ったり、設計者の意図しない動作をする等の機能

感染を拡大し拡散

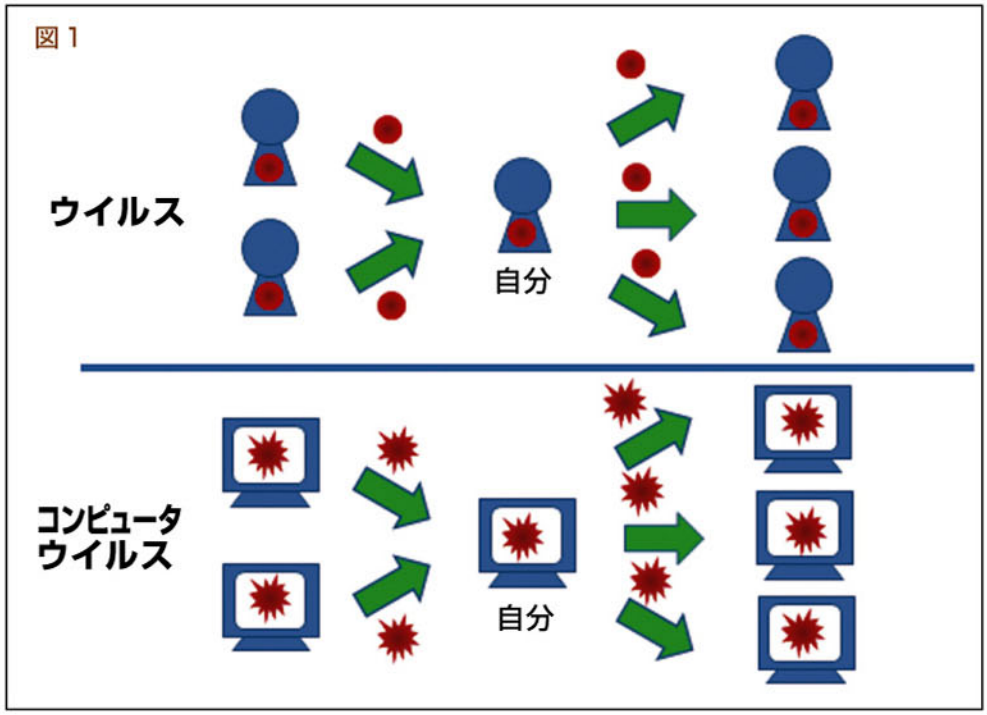
それぞれの機能について説明したいと思います。

はじめに自己伝染機能、これはウイルスの名前の通り、自然界のウイルス同様に自己複製を行い拡散していく機能をさしています。これは図1のような関係として表すことができます。例えば、我々が住む世界ではインフルエンザのなどのウイルスは図1の上図のように人から人に感染していきます。

このときに、感染経路としてはくしゃみや咳などと一緒にウイルスが飛ばされ感染する飛沫感染や感染者がくしゃみや咳を押さえた手で触れたものにウイルスが付着し、それに触れることによって感染する接触感染などいろいろなものがあります。

感染するとウイルスは自己複製を増殖していきます。そして次の新たな感染者を求め拡散していきます。コンピュータウイ

図1



ルスでも同じ事が起こっており、感染したコンピュータからメールやメールに添付してあるファイルなどを通して感染を拡大していきます。

そして新たに感染したコンピュータにおいてコンピュータウイルスであるプログラムを複製し、それをメールやメールの添付ファイルとして拡散していきます。また最近では、自己複製能力や拡散能力を持たないコンピュータウイルスも出現してきました。これを区別するために、後者をマルウェア（Malware）と呼ぶこともあります。

条件満たせば発病

次に潜伏機能、これも自然界のウイルスが有する機能と同様のものです。自然界のウイルスは、ウイルスを拡散するためにすぐに発病するわけではなく潜伏期間が存在します。ウイルスの種類によって期間の長短はありますが、この期間中はウイルスに感染しているが発病はしておらず日常の生活をすることができ、そのため感染が拡大していきます。

それと同様に、コンピュータウイルスにおいてもある特定の条件を満たすまでは通常となんらかわらない動作をし、条件を満たすとコンピュータウイルスが発病する、つまりコンピュータに被害を及ぼす不正なプログラムが動作する機能のことです。

これを有するコンピュータウイルスとしてチェルノブイリというものがあります。これは毎年チェルノブイリ原子力発電所事故の起きた4月26日に作動するように設計されているため、このような名前がつけられました。

意図しない動作が

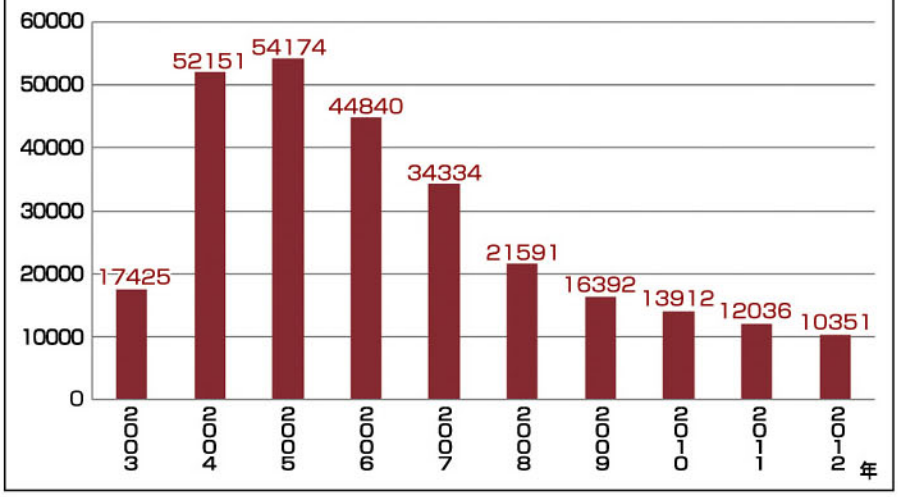
最後に発病機能についてですが、これも自然界のウイルスの同様の機能です。自然界のウイルスも、ウイルスが発病すると体になんらかの害があります。たとえば発熱や嘔吐下痢などの症状が発症します。それと同様にコンピュータウイルスが発病すれば、体にあたるコンピュータ自身に被害がでてきます。それはデータファイルの消去であったり、こちらが意図しない動作だったりします。こちらが意図しない動作とは、次のような動作です。

- コンピュータが勝手に再起動する
- 印刷ができなくなる
- 異常なエラーメッセージが表示される
- ウイルス対策プログラムが動作しなくなる
- インストールした憶えのないプログラムのアイコンがデスクトップに表示される
- 突然、画面が消えたりついたりする
- 突然、音楽などがスピーカーから再生される

ウイルスの変化

ここでは、コンピュータウイルスに関するデータを紹介しながら最近の傾向を探っていきます。図2は独立行政法人情報処理推進機構によせられたウイルス届出件数の年別推移です。こちらを見ますと2005年をピークに徐々に減少傾向にあることがわかります。

図2：ウイルス届出件数の年別推移



最初はフロッピー

2012年に初めて届出されたウイルスは14種類あり、その内の5種類はスマートフォンのウイルスで全てAndroidOSを感染対象としたウイルスだったそうです。このように、コンピュータウイルスにも流行のような時代ごとの特徴があります。1990年の初めでは、フロッピーディスクなどを使って感染するウイルスが多くありました。こ

れは、コンピュータの多くがスタンドアローンで利用されていたためです。スタンドアローンとは、ネットワークに接続されていない環境を表しています。

1990年中頃からは、メールの添付ファイルで感染するタイプのウイルスが増えてきました。これは、インターネットが普及してコンピュータの多くがネットワークに接続されるようになったからです。そして近年では、スマートフォンを対象にしたコンピュータウイルスが出まわってきています。

亜種アプリの恐怖

コンピュータセキュリティ業界大手マカフィー社の行った調査では、合計120件以上の亜種アプリケーションをGoogle Play上で発見したそうです。これらの動作は全て同じで最終的に詐欺Webサイトへユーザーを誘導します。より危険な機能を持った亜種が存在し、スマートフォン内に記憶されているユーザーのGoogleアカウントや電話番号を取得し、それらの情報を勝手にどこかのサーバーに送信し保存します。

つまり情報を抜き取るアプリケーションが存在します。収集された情報は悪用される可能性がとても高く非常に危険なアプリケーションであるといえます。

またマカフィーの調査から、これらのサイバー犯罪者はGoogle Play上の複数のディベロッパーアカウントを使用しており、詐欺アプリの亜種を作成・拡散していると推測しています。実際、マルウェア報告によって自分のアカウントが使用できなくなると、すぐに新しいアカウントを作成し、多少の変更を加えたほとんど同じアプリを新しいアカウントから掲載しています。（参考文献[1]、[2]より）

ウイルスの種類

ここでは、いくつかの有名なコンピュータウイルスについて紹介していきます。

ワーム

独立、感染力が強い

これは、他のプログラムに寄生するわけではなく独立したプログラムであり、自身を複製して他のシステムに拡散する特徴を持ったコンピュータウイルス。そのため感染力が強く、ネットワーク全体に広がり感染したコンピュータからメールなどを使って他のコンピュータに拡散していきます。

名前の由来はSF小説から。有名なものとしてメリッサ(Melissa)、ラブレター（LoveLetter）などがある。これらはメールの添付ファイルとして送付され、このファイルを開くと同様のウイルスファイルを添付し大量送信をする。

トロイの木馬

これは、普通のアプリケーションに見えるが、実はインストールしたコンピュータから情報を抜き出し他の場所に送信するコンピュータウイルス。なかに不正な動作をさせるものもある。このウイルスはコンピュータを破壊することが目的ではなく情報を抜き出すことを目的とする。そのため、このようなウイルスは「スパイウェア」とも呼ばれる。名前の由来は、ギリシャ神話におけるトロイア戦争の伝説で用いられたトロイの木馬から来ている。

情報を盗み出す手口としては、メールやバックドアを用いたものがある。バックドアとは、本来ならパスワードなどを知らないと入れないコンピュータ内部に無許可で侵入できる機能を指す。そのため、バックドアが仕掛けられると、ネットワーク通じて外部からコンピュータを操作できるようになってしまい内部のデータを盗み出されたり不要なプログラムをインストールさせられたりする。

ワンクリック詐欺

またトロイの木馬には、インターネットブラウザの情報を改変し、ある特定のサイトに誘導させようとするものもある。最近は、スマートフォンでも、このようなアプリが見受けられ誘導されたサイトをクリックすると、架空請求されたりします。いわゆる「ワンクリック詐欺」と呼ばれる手口です。

さくらいてつろう

中央大学大学院理工学研究科を卒業し、専攻は統計学。コンピュータなどによって計測される大量のデータをまとめる多変量解析の研究。現在は、諏訪東京理科大学共通教育センター講師。東京都出身、30歳。

コンピュータウイルス

セキュリティ会社大手のマカフィー社が行った調査「2012年世間を騒がせたウイルスランキング」（表1）によると第5位に「Fake Alert」というトロイの木馬型のコンピュータウイルスがランクインされています。

表1

第1位	W32/Autorun.worm	USBメモリなどのリムーバブルドライブから感染するウイルス
第2位	W32/Conficker.worm	Windows OSの脆弱性を利用してウイルスを拡散させる
第3位	Generic PWS.ak	セキュリティなどの脆弱性を利用して不正なソフトをインストールさせる
第4位	Blackhole	メール内にあるリンクをクリックすると特定のサイトに飛ばされ不正なソフトをインストールされる
第5位	Fake Alert	偽のアラートを表示させ、ユーザーにマルウェアをインストールさせようとする

ボット

これは、いくつかのコンピュータウイルスの特徴を兼ね備えたコンピュータウイルス。よくある機能としてバックドアを仕掛けパソコンを不正に利用できたり、感染拡大を目的とした不正動作を実行できたり、広範囲に感染したコンピュータ群を操作して、ある特定のサイトに一斉にアクセスしたりする機能を有する。

ネットを不正制御

このようにボットは、これまでのウイルスとは違い、ネットワークを不正にコントロールする。ボットによって構築されたネットワークはボットネットワークと呼ばれる。名前の由来は、「ロボット」から。

ボットという言葉は、コンピュータウイルス以外にも使われる。例えば、インターネット上にあるHPなどのデータを自動で収集しデータベースの構築を行う検索エンジンのサーチボットや、FPSやMMORPGなどのネットゲームにおいてプレイヤーのかわりに地味な経験値稼ぎなど作業を自動で進めてくれるボットがある。

このように人の代わりに自動で処理をするプログラムをボットと呼ぶ。また、FPSとはファーストパーソン・シューティングゲームの略称でゲームの世界を自由に動き回れ銃などの武器を使って敵を倒す一人称視点シューティングゲーム。MMORPGはマッシブリー・マルチプレイヤー・オンライン・ロール・プレイング・ゲームの略称で大規模多人数同時参加型オンラインRPGなどと訳される。簡単に説明するとテレビゲームのRPGをインターネットなどのネットゲームを通じて多人数でプレイするゲーム。日本のメジャーなRPGであるファイナルファンタジーやドラゴンクエストのシリーズからもMMORPG型の作品が出ている。

セキュリティー対策

このように、簡単にではありますがコンピュータウイルスの定義から変化、そして種類について解説させていただきました。では、コンピュータウイルスに感染しないための対策について考えていきたいと思います。まず基本となるセキュリティ対策が次の2つとなります。

アップデート

OSやブラウザなどのソフトは常に最新のものをインストールする

これは脆弱性を利用したウイルスに対する対策です。ソフトウェアのなかにはプログラムのミスや設計上の不具合によって発生したセキュリティ上の抜け穴となるセキュリティホールが出てきてしまうものがあります。

そのため、これらの欠陥を利用されないためにもOSやブラウザ

参考文献

[1] ワンクリック詐欺の亜種によるGoogle Playへの攻撃は続く、中島大輔、McAfee Labs Blog、2013/04/04

[2] Google Play上のワンクリック詐欺アプリ、ユーザー情報も収集、中島大輔、McAfee Labs Blog、2013/04/10

などのソフトウェアはこまめにアップデートをしましょう。最近のソフトウェアでは自動でアップデートをする機能を持つもありますので、それを使うとあまり意識せず対策をすることができます。

対策ソフト

ウイルス対策ソフトをインストールする

ウイルス対策ソフトをインストールすることによってコンピュータウイルスを未然に防いでくれます。このソフトを導入することによってウイルスの特徴を記憶したデータベースからコンピュータ内に、それにマッチするプログラムはないかを常時チェックするようになります。

もしも、そのようなプログラムが見つかったならば警告メッセージを出してくれます。またウイルス対策ソフトを使うことでコンピュータウイルスを削除することができます。

コンピュータウイルスの削除は、既存のプログラム中に隠れていたりして削除ツールを使用しないと困難な場合が多く、たとえ自分自身で見つけ出せ削除することができたとしてもコンピュータウイルスが再インストールされてしまう場合があります。削除ツールを使えば再インストールを防ぎ完全に削除することができます。以上よりコンピュータウイルスを検出・削除するためにもウイルス対策ソフトの導入が必要となります。

対策7か条

またIPA（独立行政法人情報処理推進機構セキュリティセンター）では「IPA対策のしおりシリーズ」という情報セキュリティ対策についてまとめ情報を提供しています。そこにウイルス対策7か条として次のものが挙げられています。

1 ワクチンソフトは最新版を活用すべし
2 メールの添付ファイルはまず、ウイルス検査すべし
3 ダウンロードしたファイルはまず、ウイルス検査すべし
4 アプリケーションはセキュリティ機能を活用すべし
5 セキュリティパッチをあてるべし
6 ウイルス感染の兆候を見逃すなかれ
7 万一のためにデータは必ずバックアップを行うべし

危険性により注意

以上2週にわたりまして、ネットワーク利用犯罪やコンピュータウイルスといったインターネットの危険な側面について解説してきました。たしかにインターネットは私たちの生活を豊かにする便利な道具なのですが、それらを悪用する人達もいるということを忘れないで下さい。とくにスマートフォンにおけるコンピュータウイルスは増加傾向にありますので、より注意が必要です。

また知らず知らずのうちに加害者となってしまう場合もあります。コンピュータウイルスへの対策を怠っていると、自分自身のコンピュータから他のコンピュータにウイルスを送ってしまう場合があります。このとき、損害賠償を請求される場合があります。また送られる相手も、見ず知らずの他人ではなく知人に送られる場合があります。このように自分のコンピュータをウイルスから守ることは知人のコンピュータも守ることにつながります。これは著者自身もいえることですが、自分のためにも知人のためにもコンピュータウイルスへの対策をしっかり行っていきたいと思います。