コンピュータ ウイルスについて

2013月10月15日

株式会社アイ・シー・アイ

■はじめに

コンピュータを利用していると、必ず聞くことになる単語。

「コンピュータウイルス」

皆さんも
「これに感染することは大変危険なこと」
「怪しいメールなどは開かない」
などという認識は当然、お持ちかと思いますが、

では
「どういうものがあるのか？」

そう問われると「・・・？」となってしまいませんか？

今回はそんなウイルスについて簡単ではありますが、まとめてみました。

■コンピュータウイルスとは

コンピュータウイルスとは本来、「ユーザの意図とは無関係に他のプログラムに寄生し、自己複製を行い、不利益をもたらすプログラム」です。
しかしながら近年では自己複製をしなく、寄生することもなく（ウイルス単体で）機能するウイルスも多く、通商産業省ではウイルスを以下と定義しています。

「コンピュータウイルス対策基準」（経済産業省告示）

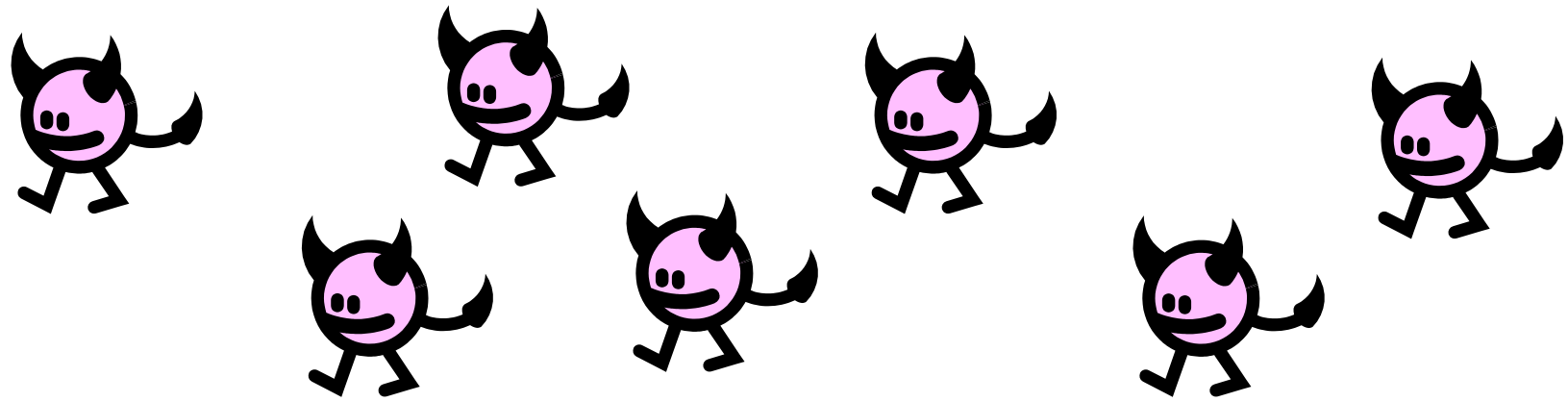
「第三者のプログラムやデータベースに対して意図的に何らかの被害を及ぼすように作られたプログラムであり、次の機能を一つ以上有するもの。
１．自己伝染機能
　自らの機能によってほかのプログラムに自らの複製、
　又はシステム機能を利用して自らをほかのシステムに複製することにより、
　他のシステムに伝染する機能
２．潜伏機能
　発症するための特定時刻、一定時間、処理回数等の条件を記憶させて
　発病するまで症状を出さない機能
３。発病機能
　プログラム、データ等のファイルの破壊を行ったり、
　設計者の意図しない動作をする等の機能　　」

■最近のコンピュータウイルスの種類

近年のコンピュータウイルスの大まかな種類としては
大まかに下記に分類されます。

・トロイの木馬
・ボット
・ワーム
・ロジックボム
・スパイウェア

各ウイルスの詳細については次のページ以降、簡単に説明します。



■トロイの木馬

ギリシャ神話の「トロイの木馬」になぞらえて名前が付けられたウイルスです。
兵士を潜ませた大きな木馬を贈り物として相手に送付し、内部から
崩壊させた故事と同様、一見有用なアプリに見せかけ、
インストールさせパソコン内部に潜伏し様々な悪さを行います。

悪さの一例）

・バックドアの作成

ネットワークを介して外部からパソコンを操作させるための裏口を作成し
このバックドアを通じ、パソコンの外部から侵入し、別のPCから様々な操作を
行うことができるようにします。

・不正なプログラムのダウンロード

パソコンの利用者が意識することなく、不正なプログラムなどを
インターネットからダウンロードし、実行します。

・利用者パソコンの情報収集

利用者の意図にかかわらず勝手にパソコンに感染し、
パソコン内の情報や利用者の操作を記録し、必要に応じて外部に送信します。

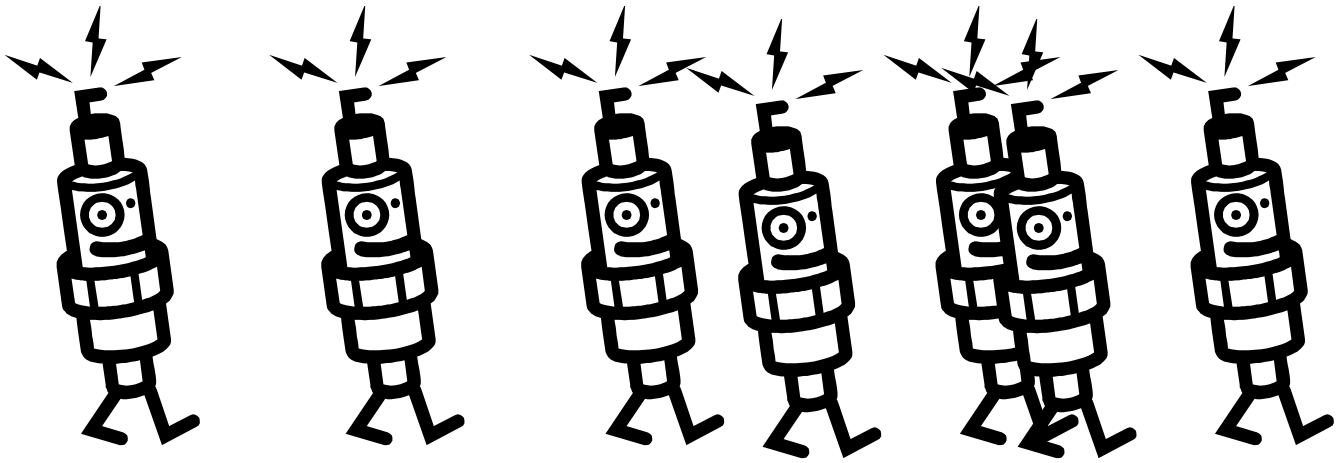
・プロキシ型（攻撃の踏み台）

ほかの人が利用者のIPアドレスを使用することが可能となり、
気づかぬうちにサイバー犯罪の片棒を担ぐ羽目になってしまう
可能性があります。

■ボット

ボットとはパソコンに感染し、そのパソコンをネットワークを通じて
外部から操ることを目的として作成されたプログラムです。
感染すると一定間隔で指令サーバと連絡を取り指示を待ち、
与えられた指示に従い、内臓された処理を実行します。
この動作がロボットに似ていることからボットとよばれています。

また、ボットに感染したパソコンが多数集まるとそれらが指令サーバを介してネットワーク（ボットネット）を構成することが可能で
それらから一斉にスパムメールを発信したり、
特定の攻撃先にアクセスすることでシステムやサーバを利用不可にするDos攻撃の尖兵として利用されてしまいます。



■ワーム

ワームとは、他のプログラムやファイルに寄生することなく、
パソコンにインストールされ実行される自己完結型のプログラムで
自分自身の複製を作成することで感染活動を行います。
単独でパソコン内で破壊活動や自己増殖活動などの悪さをするために
うごめく様からウジやミミズを連想させるため「ワーム」と呼ばれています。

現在、多くの種類や亜種が出現しているタイプです。

プログラミングができる人であるならば誰でも作成できるものですが、
普通は利用者によって起動してもらう必要があるため、
トロイの木馬と同様、利用者にとって有用なプログラムを装って
実行させたりするものがほとんどです。

■ロジックボム

ロジックボムとは指定時刻の到来など、システム上における条件が満たされると
自動的に動作を開始するプログラムです。

多くのデータの破壊・盗用などを行った後、役目が終わったら
最終的に自分をも消滅させる
スパイ映画の指令を伝えるビデオテープみたいなウイルスです。

なお、自滅の際に、あらかじめ搭載されたプログラムを拡散させる
厄介な種類もあります。

■スパイウェア

スパイウェアとは、利用者の意図にかかわらず勝手にパソコン内の情報や
利用者の操作を記録し、必要に応じて外部に送信するプログラムです。
感染能力がないものが多く、ウイルスと定義されないこともありますが、
悪さをすることには変わらないので記載いたします。
バックグラウンドでのスパイのような情報収集するプログラムももちろんながら、
下記のようなプログラムもスパイウェアと定義されます。

・スケアウェア
ユーザのコンピュータに「重大な問題がある」といった偽りのメッセージを
表示し、ソフトの購入するように促します。

・ダイヤラー
ダイヤルアップ接続時に国際電話やダイヤルQ2へ接続させます。

・暴露ウイルス
利用者のコンピュータを勝手にインターネットに向け公開されたWebサイトにして
コンピュータの中身をインターネットにさらしてしまします。

■猛威を振るったウイルス　1

過去に実際に猛威を振るったウイルスをいくつか簡単に紹介していきます。

※あくまで筆者の個人的な選択で恐縮ですが・・・

・原田ウイルス

ウイルスソフトを起動してしまったときに原田と名乗る人物画像が
表示されるウイルスの総称。専用のソフトウェアにて容易に作成が
可能で、亜種は100種類を超え、その挙動も一つではない。
一番の被害者は勝手に自分の画像を使用された原田さんなのかもしれない・・・

・Antinny（アンチニー / アンティニー）

ファイル交換ソフトを媒介に、日本国内で猛威を振るった暴露ウイルス。
感染したPCから政府や各企業の機密情報が洩れ、ニュースをにぎわせた。
なお、Microsoft発表によると、このウイルスに対応したMicrosoft製の
ウイルス除去ツールではリリース後約1か月にて11万台のPCから
20万以上のAntinnyを削除したとしている。

■猛威を振るったウイルス　２

・チェルノブイリ

最初に発見されたものが毎年、チェルノブイリ原発事故が起きた日に
作動するように設計されていたためこの名前をつけられたウイルス。
非常に破壊力の強いウイルスでハードディスクやBIOS-ROMの情報を破壊する。
BIOSが破壊されるため、PCの起動すらできなくなる。
トルコや韓国などで１００万台ものコンピュータで発症した。

・Nimda（ニムダ）

某テロ組織が作成したのでは？憶測もされた歴代最悪ともいわれるウイルス。
強い感染力をもつ、インターネット上で最も拡散したウイルスで
その世界一を奪取するための所要時間はわずか22分しか掛からなかったともいわれる。
システムファイルを破壊し、感染過程で帯域を食いつぶし、サーバダウンや通信障害を
世界中で引き起こした。

・LOVE　LETTER

「I Love you」というタイトルのメールに添付されている
「LOVE-LETTER-FOR-YOU」というファイルを実行することで感染するウイルス。
感染後、ハードディスクの中身を破壊するだけでなく、
アドレス帳に登録されているメアド全てに同様のメールを送信する　厄介な機能がついているため、
これに泣かされた片思いの人は少なく無いとおもわれる。
※同様のメール拡散タイプのウイルスなら「メリッサ」のほうが有名かもしれないですね。

■ウイルスに感染しないためには　1

一度コンピュータウイルスは感染してしまうと
自分どころか、他人にまで被害を及ぼしてしまいます。

このようなウイルスに感染しないためにも
最低限、以下のような対策をとることが必要です。

1.ウイルス対策ソフトの導入
　ウイルスの感染を防ぐにはウイルス対策ソフトの導入が最も効果的です。
　しかしながら、一度ウイルス対策ソフトを導入したからと言って
　安心してはいけません。残念なことにウイルスは日々進化していますので
　最新のウイルス定義ファイルをアップデートすることを忘れないでください。

2. 見知らぬ相手先から届いた添付ファイル付のメールは厳重注意！！
　現在、多くのウイルスはEメール経由にて感染します。
　見知らぬ人から届いた添付ファイルはもちろんのこと、
　よく知った相手だとしても本文にファイルを添付した旨が書かれていない場合、
　その添付ファイルには十分に注意したほうがいいでしょう。

■ウイルスに感染しないためには　２

３．最新のセキュリティバッチをあてておく
前項のNimdaのようにOSやアプリの脆弱性（セキュリティホール）を狙った
ウイルスも数多く存在します。
この脆弱性によっては恐ろしいことに
ネットワークにつないだだけで感染するものや
メールをプレビューしただけで感染するウイルスもありますので
必ず、最新のものをあてるようにしましょう。

４．ダウンロードしたファイルに気を付けて！！
画像や音楽、映像など様々なファイルを自分の趣味に合わせて
ダウンロードすることもインターネットの魅力のひとつですが
そのファイルにウイルスを仕掛ける人もいることを忘れないでください。
怪しいサイトからダウンロードしたファイルは
必ずウイルスチェックを忘れずに！！

■最後に

コンピュータウイルスは残念なことに常に進化を続けています。
上記のような対策や、さらに一つ上の対策を実施したとしても
感染してしまう可能性は0ではありません。

少しでも自分のコンピュータがおかしいな？と感じたら
一度、下記へ相談してみてはいかがでしょうか。

独立行政法人　情報処理推進機構（IPA）
情報セキュリティ安心相談窓口

電話番号　　03-5978-7509
受付時間　　平日　10:00～12:00、13:30～17:00
E-mail ： anshin@ipa.go.jp
URL　　：http://www.ipa.go.jp/security/anshin/