CTF通信　集う・遊ぶ 学ぶ・働く
第120号　2013年3月　発行：CTF松阪

パソコン遠隔操作ウイルス事件解決か

昨年夏から秋にかけて、無差別殺人や爆破などの犯罪予告メールを送ったとして５人の男性が逮捕されたが、いずれもパソコンがウイルスに感染した結果、本当の犯人から遠隔操作されていたためとわかり、警察が捜査の不備を認めて謝罪したという事件があった。

このような他人のパソコンを乗っ取りその人になり済まして悪事を働く手法は、以前からも知られており別に珍しいことではないのに、今回このように大きく報道されるのは、５人もの人が誤認逮捕・一部起訴されたということで、警察・検察に対する批判のあらわれだと言える。

それはさておき、容疑者とならないためにパソコンユーザーとして守るべきことの再確認をする必要がある。

- ○ フリーソフトのダウンロードは信頼あるサイトから行う
- ○ 心当たりがないメールの添付ファイルは開かない（差出人詐称もある）
- ○ OS をはじめ各種ソフトの更新を励行し、常に最新の状態にしておく
- ○ ウイルス対策ソフトを導入し、常に最新の状態にしておく

なお、この事件の真犯人と見られる男が２月 10 日に逮捕された。容疑者は否認をしているということで、取り調べが続いているものと思われるが、これまた誤認逮捕となったのでは笑い話にもならない。

私は三重難病連の代表をしております。昨今の動きから、すべての難病が難病対策の対象となること」、「病気であっても必要な社会的支援を必要に応じて受けることのできる社会を」というスローガンを掲げて活動しています。

その立場から、ようやく難病対策要綱がつくられて以来、40 年を経て初めて、抜本的に新しい難病対策の実現への道筋ができかかっている時であり、またいきなりすべての要求が一気に実現する状況ではない現実もあることから、専門医や患者団体代表も含めて真摯に検討されてきた

難病対策委員会の「提言」の実現に向けて、すべての患者団体が前向きに協力して取り組み、検証しつつ、残された課題と次の目標に向けて、力を合わせて取り組んでいきたいものです。

M. W

今月号は文字数が多いので、第１ページと第２ページ、第４ページに SP コードを２個付けてあります。第１ページと第２ページ、第４ページでは、先に左下の SP コードを、次に右下の SP コードを読んでください。

セキュリティ入門　９

ウイルス検知法(3)　ジェネリック手法

今までの手法はすべてファイルからウイルスを検知する話だった。しかしこの方法ではどうしても対処できないウイルスがある。それは既にコンピュータ上に常駐しているウイルスや、ネットワーク経由で侵入してくるウイルスである。

例えば「SQL Slammer」と呼ばれるウイルスは「メモリー常駐型」と呼ばれファイルには感染しない。パターン・マッチングでは検出不能だ。ではメモリー上に直接感染して既に活動を開始しているウイルスを検知する方法はあるのだろうか。

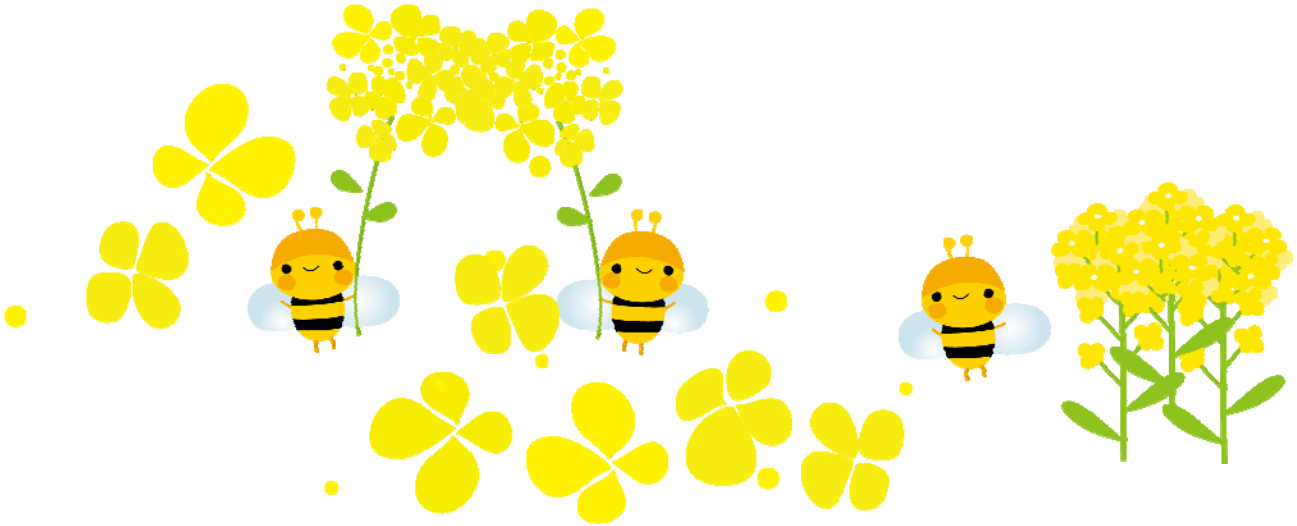
このような場合に有効な検知法は「ジェネリック手法」である。ヒューリスティック手法がまだ活動していないウイルス（ファイル）を対象にしているのに対して、ジェネリック手法は既に動作しているウイルスが検知の対象となる。

ジェネリック手法は、特定のアプリケーションを「モニタリング」する常駐プログラムが重要な役割を果たす。このモニタリング・プログラムは、アプリケーションが「OS に対して不正な動作を要求するシステム・コールを実行していないか」「不正にファイルを変更したり削除したりしていないか」といった事項を常に監視している。もし活動中のウイルスが一連の命令を実行しようとすると、モニタリング・プログラムはアプリケーションと OS の間に割り込んで命令の伝達を遮断する。このような手法を「ビヘイビア・ブロッキング」と呼ぶ場合もある。

実際にジェネリック手法を用いるには高度な解析技術が必要となる。正常なプログラムもファイルの書き換えや削除は常に行うので、このような挙動の中からウイルスによる不正な命令だけを見抜くのは簡単ではないからだ。これは他の検知法にも共通することだが「何をもってウイルスと判断するか…」というルール（ウイルス定義ファイル）作りこそが各ウイルス対策ソフト・ベンダーの腕の見せどころとなる。

一方で、ウイルス作者はきっと「ウイルス対策ソフトに対する対策」を講じてくるはずだ。つまり私たちはウイルス対策ソフトにすべて頼り切るのではなく、常に最新ウイルスの動向に注意を払い、できる対処はすべて実施するということを肝に銘じておく必要がある。

おわり



活動報告

【2 月】

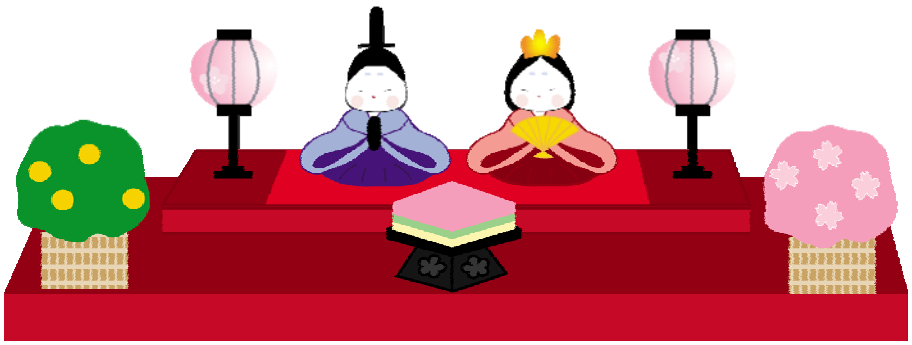
障がい者対象個人向けパソコン講座
（5 日、12 日、19 日、26 日）

訪問 IT サポート
（6 日）

活動予定

【3 月】

障がい者対象個人向けパソコン講座
5 日、12 日、19 日
9:30～11:30
松阪市障害者福祉センターにて



続・松阪食べある記

和みキッチン　星

「太陽」、「月」に続く今月は「お星さま」ということで、CTF 松阪と同じ町にある「和みキッチン星」を訪れました。

御厨神社の向かい側に去年の 7 月に開店したばかりの、端正な外観とオシャレな店内のお店です。

ランチメニューは、ドリアやピザ、パスタが中心で、テーブル席が 2 卓（8 席）とカウンターが 7 席あり、カウンターではオープンキッチンの料理人さんとの会話が楽しめます。

ドリア	950 円（写真上）
味噌カルボナーラ	830 円（写真中）
サーモンきのこパスタ	800 円（写真下）

所 在 地：松阪市本町 2303-1
電　　話：0598-31-3950
営業時間：11:00～16:00　（LO 15:30）
　　18:00～24:00　（LO 23:00）
定 休 日：毎週日曜日

リレー随筆

今月は、先月号に引き続きH．O様から、Windows 8 の使い心地などについてのご投稿をいただきました。

118

Windows 8 を使ってみて･･･(2)

H. O

無事にシャットダウンできたので今度は起動である。電源スイッチをオン、20 秒余りという早さで最初の画面（空と山と海と展望タワーのイラスト＝ロック画面というそうだ）が現れた。さてこれからどうするか？　雑誌に出ている､アイコンがタイル状に並んでいるスタート画面を予想していたので、ここで二度目のつまづき。

ここでは画面をクリックするか､エンターキーを押せば次へ進むことがわかったが､このように『ここではどうするの？』と立ち往生する場面がこれから何度も出てくるのである。

エンターキーを押して、やっと雑誌に出ているスタート画面が表示された。

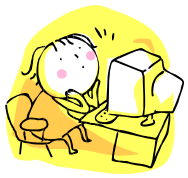
このアイコンの中の「デスクトップ」をクリックすると Windows 7 とよく似た画面になり、なぜかホッとした気分になる。

さてこのパソコン､孫が来るとよく勝手に使っているので､ユーザーの追加をしようとコントロールパネルを開くが､「ユーザーアカウントの追加」の項目がない、またまた雑誌のご厄介に。

ユーザーの追加は画面右上端をポイントすると現れる「チャーム」というメニューの中から､「設定」→「PC 設定の変更」→「ユーザー」→「ユーザーの追加」の順に行う、コントロールパネルからはできないとのこと。反対にユーザーの削除は､「PC 設定の変更」からはできなくて、コントロールパネルから行うとのこと。頭が混乱してしまう。

ともかくデスクトップ画面を表示することができるので、ワードやエクセルが使えるように Office 2007 をインストールした。インストールも無事に完了したが、ワードを起動しようとして何度目かのつまづき。「スタートボタン」がないので「ワード」を起動することができない。どうするのかというと、スタート画面に戻ってデスクトップアプリの「ワード」アイコンをクリックしなければならない。続けてエクセルを起動したいときも、またスタート画面に戻ってデスクトップアプリの「エクセル」アイコンをクリックしなければならない。こんな面倒なことはとてもできない。

どうしたかについては次号で・・・　　（つづく）



編集後記

桃の節句・お雛様ですね。
まだまだ此の時期は寒い！
松阪の初午さんの頃には雪花が舞う事がよくあります。今年の初午さんはどうでしょうね。・・二月堂のお水取が済み、やっと春の声が聞こえてきます。

早咲きの桜が咲き始めます。一年で一番季節の変わる月です。お花見ですね！！

CTF 通信第 119 号

2013 年（平成 25 年）３月発行

発行者　IT を活用した障がい者支援 NPO 法人
CTF 松阪

発行責任者　川　口　保　美

住　所　〒515-0081
松阪市本町 2181-1

電　話　0598-21-7268

ＵＲＬ　http://ctf.dip.jp/