オペレーティングシステム

第14回(2009.07.16)

コンピュータへの脅威とOS

コンピュータへの脅威

- ウィルスの感染
  - パソコンが起動しなくなる。
  - データが破壊される。
  - 個人情報が流出する。
- 不正アクセス
  - WEBページの書き換え
  - 外部の人間による情報アクセス
  - コンピュータの乗っ取り
- 不正利用
  - 「職員」による不正・情報流出

ウィルスとは

- 「コンピュータウィルス」と「ウィルス」
- ウィルス
  - インフルエンザ、AIDSなどの原因生物（物質?）
  - 相手の「核」に入って、生物細胞の「増殖機能」を利用して増殖する。
    - 単体では増殖できない⇒生物ではない？
    - 感染、増殖能力
  - 何らかの症状をひき起こす
    - 病原性（発病）
- 「感染性」のあるプログラム
  - その「感染性」や「病原性（破壊力）」から、「ウィルス」と呼ばれるようになった。

自己増殖オートマトン

- オートマトン（オートマータ）
  - ＝「自動機械」
  - 現在のコンピュータより遥か以前に、「機械仕掛け」などで自動動作を行う機械を指す言葉として、オートマータがあった。
  - 「カラクリ人形」(江戸時代の日本）など
- このオートマトンに（自己増殖）の機能を持たせたソフトウェア

  ＝　自己増殖オートマトン

  ＝　ウィルスの定義に極めて近い（同じ？）

ウィルスの種類

- ファイル感染型
  - システムプログラムなどに「感染」
    - ドライバなどとして「常駐」する。
- マクロ型
  - WORDやEXCELの文書に、スクリプトとして添付される。
- トロイの木馬型
  - プログラム本来の機能に隠れて、全く別の機能を実現する。
- ワーム型
  - 厳密にはウィルスと異なり、自己増殖の機能がある。
- ボット型
  - 「ロボット」から名前が来ている。システムに侵入して、内部で「スパイ」行為を働く。

スパイウェア

- 「感染の方法」や「動作」による分類ではなく、「何を目的として開発されたウィルスか」という「目的」からつけられた名称。

- 進入した相手システムから
  - 著作権侵害がないか監視する、
  - その人のIDやパスワードを盗み出す、
  - データを自由に読み出して外部に送信する、
  - などの動作を行う。

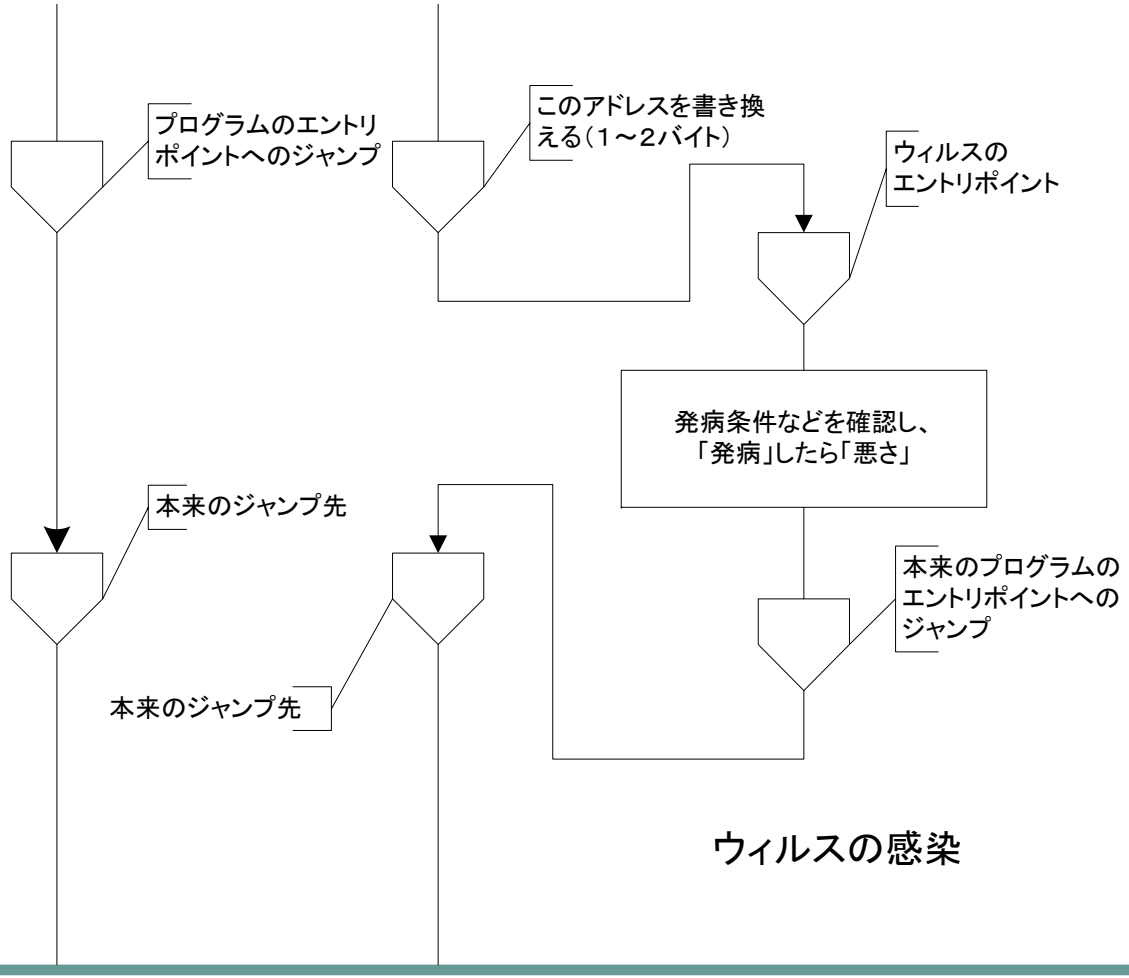
ウィルスの感染経路

- 電子メールの添付ファイルによるもの
  - かなりを占める。
- WEBサイトに置かれたプログラムを実行
  - 「良心的」なサイトばかりではない。
  - フリーウェアからの感染
- LANに接続しているだけで感染するもの
  - LANに接続された他のPCを「検索」して、直接ファイルを送り込む。（セキュリティホール）

ウィルスの手口（ファイル感染型）

- システムの「実行プログラム」を書き換える
  - プログラムは「名称」で識別される。
  - 「同じ名称」にしておくと、そのプログラムの「実行条件」が整えば、呼び出される。
- 書換え方
  - 根こそぎ、「不正プログラム」と置き換えるもの
    - すぐに発病
  - パッチコードを組み込むもの
    - プログラム本来の機能を残すので、発見しにくい
- 「システムプログラム」は、削除できない。
  - だから、「ウィルス」に感染しても削除できない。

実行プログラムのウィルス感染



ウィルスの感染

ウィルスの作り方（作られ方）と防御

- ファイルを「データ」として扱い、書き換える。
  - 特定のデータパターン、領域を検索する。
- 実行プログラムの構造、ファイルへのデータの保存様式（フォーマット）を熟知する。
  - どの部分が「攻撃対象になるか」を熟知する。

- 「プログラム」も「ファイル」である。
  - 「ファイル」は「バイナリデータ」として編集できる。
  - つまり、「システムプログラム」も編集できる。

- 「仕様を公開しない」領域にチェックコードを書き込み、自己診断させることで、検出する。
  - 「いたちごっこ」ではある。
  - 発見できれば、「対処」は可能　　⇒　リバースエンジニアリング

ウィルスなどの検出

- プログラムの先頭で、通常あり得ない「番地」へのジャンプ命令がある。
- マクロの不要な文書に「マクロ」が組み込まれている。
- 通信機能の不要なプログラムに、「通信接続」の実行命令が組み込まれている。

リバースエンジニアリング

- Reverse Engineering
  - 「完成品」を分解して、設計図を作る、
  - という感じで、逆向きの動作で「設計」する。
  - コンピュータのプログラムは、すべてロジックなので、論理的には完全なリバースエンジニアリングが可能。
    - （「なぜ」は、作った人でないとわからないが。）
- ウィルスのプログラムを解析する際も行われるし、ウィルスを作るときも行われる。

トロイの木馬

- トロイという難攻不落の城塞都市を攻める際に、「巨大な木馬」の中に兵士を潜ませ、「木馬」ごと都市に潜入し、夜襲に成功したという伝説から「トロイの木馬」と名づけられた。

- 「全然別のもの」に見せかけて、内部に入ってしまったら、「不正機能」が働きだす種類のウィルス。
  - データの破壊、よりも、「データの盗み出し」が多い

不正アクセス

- WEBページの書き換え
  - システムのIDとパスワードを盗めれば、簡単に進入できる。（FTPパスワード、など）
    - 「主義主張」や、嫌がらせ
- 不正なデータの取得
  - 権利がないのにデータを盗む
    - （企業スパイ、政治的スパイ）
  - 名簿などの「売却」による小遣い稼ぎ（私的犯罪）

セキュリティホール

- コンピュータどうしの接続は「ポート」と呼ばれる「接続番号」へのアクセスで実現する。
- 特定のサービスのポート番号は固定
  - TCP　Port番号
    - TCP = (Transmission Control Protocol)
  - 特定のロジック、特定のアクセス権でポートに接続要求すると、つながってしまうような、「防犯上の盲点」のことを、「セキュリティホール」という。

ポートスキャン

- 鍵の「開いている」ポート番号はないか、順番に片端から「接続要求」を投げる。
  - プログラムで、自動的に「ポート番号」を変えながら、応答を調べる。
  - スキャン　＝　しらみつぶしに全部を調べる
- 同じ相手から、「番地」だけ変えて「接続要求」が来た、このポート[スキャン」を疑う。

  ⇒　その「相手」をblack listに載せて、無視する。

ルートキット

- Root (Administrator)は、特権ユーザ
  - root (admin)で侵入・接続すると、何でもできる。
- 「バックドア」（裏口）から侵入されると、事実上PCが乗っ取られる。
- バックグラウンドで実行されているタスクを監視する。
  - 不必要に外部に送信していないか。

迷惑メール

- スパムという呼び名は、歴史のある「缶詰」の名前だが、「迷惑メール」の代名詞になった。
  - 不名誉な名称になっているので、「スパム」を避けて「迷惑メール」と呼ぶようにしている。
- 無作為に、「存在している可能性があるメールアドレス」に送りつける。
- エラーにならないアドレス」がリスト化されて売買？されている？
  - 決して、「メールは不要」という「返事」を出してはならない。（悪用されるだけ）

逆探知(？)ツール

- http://www.cybersyndrome.net/
- プロキシ・サーバなどの登録者を確認
  - 迷惑メールの場合、差出人が匿名でも「誘導先」のURLが存在するため、確認できる。
  - ドメイン名の登録などは、「更新」が必要なため、架空の住所では手続きできない。
- 誘導先が同じ「URL」の場合は、black listに登録しておき、受信を拒否することができる。

脅威に対抗するには

- まず、「危険」の存在を自覚すること
  - 何も知らなければ、対処しようがない。
- 「危険」の種類と性質を理解する。
  - それぞれのマシン環境ごとに、「危険」の種類が異なる。
    - 例：スタンドアロンのマシンを使っている人は、アンチウィルスの心配がない。
  - ネットに接続する必要がないなら、つながない。
- 「ワクチンソフト」などの利用も有効

まとめ

- コンピュータには様々な脅威がある。
  - ウィルス、不正アクセス、迷惑メールなど
- 「脅威」のメカニズムを正確に理解する。
  - メカニズムを理解しなければ「対処」ができない。
  - どんな「損失」が考えられるか、把握する。
    - スパイウェアなどは、経済的損失を誘発。
  - 簡単に実行できる対策は確実に実行する。
  - セキュリティホールは、見つけたらすぐに閉じる。
- ツールを有効に活用する。
  - ワクチンソフトなどは有効