情報学概論A

情報と社会　～コンピュータとインターネット～

11. コンピュータウイルスとは　－1－

1

目　　次

- 1. コンピュータウイルスとは
- 2. コンピュータウイルスの歴史
- 3. コンピュータウイルスの変遷
- 4. コンピュータウイルスの分類
- 5. まとめ

- 参考資料
  資料協力　トレンドマイクロ株式会社

2

1. コンピュータウイルスとは

- 何故ウイルスと呼ばれるのだろう

自然界のウイルスと似通った動きをする

1984年9月に米国のセキュリティ学会でフレドリック・コーヘン博士が「コンピュータウイルス」という言葉を論文の中で発表し、世界で初めて使用されました

3

1. コンピュータウイルスとは

- コンピュータウイルスの定義
  - **コンピュータウイルス**（computer virus）とは、広義では**コンピュータに被害をもたらす不正なプログラムの一種**である
    日本工業規格（JIS X0008「情報処理用語－セキュリティ」）では単に「ウイルス」（virus）と定義され、一般に医学・生物学上の原義のウイルスと混同する恐れがない場合は「ウイルス」と呼ぶことが多い
    （なお、英語ではヴァイラスと発音する）

    コンピュータウイルスの感染を妨害したり、感染したウイルスを検出したりする技術をアンチウイルス（anti-virus）と呼び、それらを支援するソフトウェアを**アンチウイルスソフトウェア**や、ワクチンなどと呼ぶ

4

1. コンピュータウイルスとは

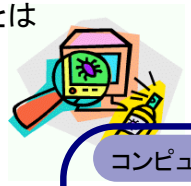
感染 → 潜伏 → 発病

第三者に対して迷惑行為を目的とした
不正プログラム全体を意味する！！

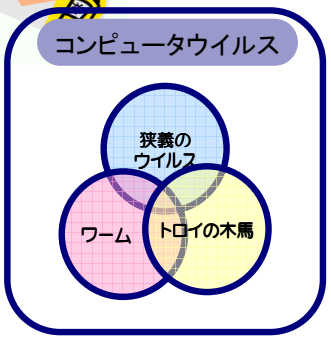
10年で40倍！
2007年には550万
種類のウイルスが出現！

5

1. コンピュータウイルスとは



- コンピュータウイルス
  - 単独のファイルでは動作せず、他のファイル（宿主）に寄生する
  - 感染・潜伏・発病　の動作を行う
- ワーム
  - 単体のプログラムとして動作し、ネットワークを利用して自分自身のコピーを送り込む
- トロイの木馬
  - 単体のプログラムで動作し、一見有益そうなプログラムを装う
    実行するとバックドア（不正な仕掛け）やPCの情報取得を行う



6

1. コンピュータウイルスとは

- ウイルス作者の横顔（やっかいな物を作った奴ら）

  - プログラミングを趣味とする人
  - コンピュータのプログラムを修正したり、改良したりする人
  - 自分の能力を試したい、誇示したい
    自分の作ったものがどれほどの威力があるのか見てみたい
  - コンピュータウイルスを作成し、世の中への広めたい
  - 余計なおせっかい　　～セキュリティ対策の甘さに対する警鐘～

  - 実際にあった話（2004年3月）
    MyDoomとBagleと言うコンピュータウイルスのそれぞれ作者がNetskyというコンピュータウイルスの作者をそれぞれのウイルスの中に卑俗な言葉を入れ込んで侮辱した
    それにNetskyの作者が言い返すという痕跡が見つかった・・・
    互いをウイルスのコードの中で罵りあっていたようだ

7

2. コンピュータウイルスの歴史

- すべては1972年から始まったと言われる
  - 1972年
    SF小説　デイヴィッド・ジェロルドの『H・A・R・L・I・E When Harlie Was One』の中で初めてコンピュータウイルスという言葉が使われた
  - 1982年
    ゼロックスのPARC（パロアルトリサーチセンター）で自己複製型コードの実験が行なわれた（ハッキリ言ってウイルスの試作品）
  - 1984年
    フレドリック・コーヘンがウイルスに関する論文を発表
    コンピュータ業界で「コンピュータウイルス」という言葉が初めて使われたが、当時の専門家は、ウイルスはあり得ないと笑っていたという

8

2. コンピュータウイルスの歴史

- 世界初のコンピュータウイルスの登場
  - 1986年（発見数　910種類）
    パキスタンで**「ブレイン」**という名前のウイルスがはじめて発見された
    パソコンショップを経営していた兄弟が違法コピー防止のメッセージ
    を出すだけの仕組みだったが、発見された時はデータを破壊するよう
    な物になっていた（誰かが悪意ある改造を施した？）
  - 1987年（発見数　389種類）
    ドイツ製　**「CASCADE：カスケード」**
    発病すると画面の文字が滝のように落ちて下に積み重なる

    イスラエル製　**「JERUSALEM：エルサレム」**
    13日の金曜日ウイルスとも呼ばれ、13日の金曜日にパソコンが
    起動するとファイルを削除すると言う仕組み

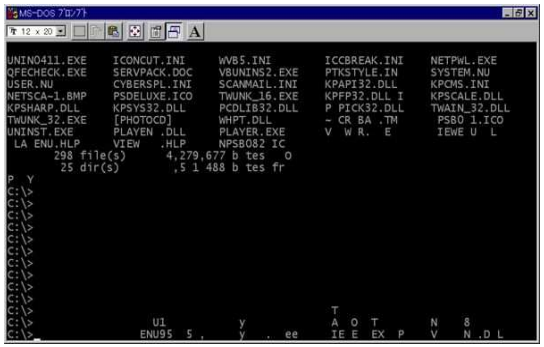
2. コンピュータウイルスの歴史

- 国産のウイルスも登場
  - 1989年（発見数　2604種類）
    国産コンピュータウイルス　**クリスマス**登場
    12月25日に「A merry christmas to you!」というメッセージが表示さ
    れるだけであったが、国産ということで話題になった

    オーストラリア製**「Yankee Doodle：ヤンキードゥードゥル 」**
    感染後17時になると「Yankee Doodle（アルプス一万尺）」が演奏され
    る、破壊活動はない
  - 1991年（発見数　18，384種類）
    スウェーデン製　**「MICHELANGELO：ミケランジェロ」**
    ミケランジェロの誕生日3月6日に発病し、ディスクをフォーマットして、
    ランダムな文字列でディスクを上書きする

2. コンピュータウイルスの歴史

- **CASCADE：カスケード**



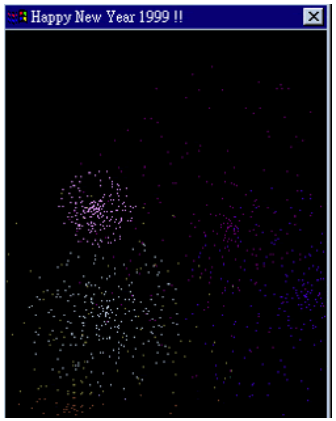
2. コンピュータウイルスの歴史

- **マクロウイルス**の登場
  - 1995年（発見数　15，988種類）
    米国製　**「WM_CONCEPT.A」**
    初のマクロウイルスで、マイクロソフトのWord文書に感染する
    実行されると標準テンプレートにウイルスをコピーし、保存するとウイ
    ルス付き文書ができあがる

  - 1996年（発見数　36，816種類）
    アフリカ製？　**「X97M_LAROUX.A：ラルーX」**
    Excelに感染する初のマクロウイルスで感染するだけ
    実害はないが、その後のExcel用マクロウイルスの原種となる

2. コンピュータウイルスの歴史

- 1999年（発見数　98，428種類）
  米国製 「**Happy99**」
  「Happy New Year 1999!!」
  というメッセージが表示され、
  同時に新しいウィンドウが現れ
  花火の画像を表示



13

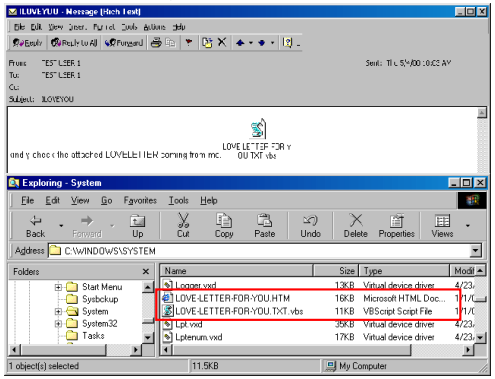
2. コンピュータウイルスの歴史

- ワームと呼ばれるウイルス急造
  - 2000年（発見数　176，329種類）
    フィリピン製 「**LOVELETTER:ラブレター**」
    添付ファイルを実行すると、Microsoft Outlookに登録されたメールアドレスすべて（！）に対して『LOVE-LETTER-FOR-YOU.TXT.vbs』というウィルスプログラム自身を添付したメールを送信
    マシン内に保存されている、一定の拡張子を持つファイルを検索し、それらのファイルを破壊
  - 2001年（発見数　155，528種類）
    ？製 「**Sircam:サーカム**」
    無作為に文書ファイルを選び出し自身に取り込んでメールに添付して拡散し、ネットワーク上のドライブに自身のコピーを作成

14

2. コンピュータウイルスの歴史

- **LOVELETTER:ラブレター**



15

2. コンピュータウイルスの歴史

- 世間を騒がせたワーム（ネットワーク管理者が悲鳴を上げた年）
  - 2001年
    「**Code Red:コードレッド**」
    バッファオーバーフローにより侵入し、無作為に次の侵入先を探す
    Webページの改ざんやDoS攻撃を行う
    「**Code RedⅡ:コードレッドツー**」
    上記の改良型
    「**Nimda:ニムダ**」
    Webページを改ざんし、IE5.0を使用して閲覧するとウイルスが実行され、OutlookExpressではメールをプレビューしただけで感染する
    ネットワークの共有ディスクへコピーCode Red IIを利用する
    「**Klez:クレズ**」
    感染したパソコンからメールアドレスを収集し、メールの送信者を偽装（差出人アドレス詐称）する初のウイルス？
    jpegまたはHTMLファイルを選択して添付ファイルにする

16

2. コンピュータウイルスの歴史

- 強力なネットワーク型ウイルス
  - 2003年（発見数　178，825種類）
    「MSBlaster：エムエスブラスター」
    パソコンが再起動する不具合が発生する不具合をついて侵入し、
    次の侵入先を検索して拡散する
    2003.8.16にWindowsUpdateを攻撃する

    「Antinny：アンティニー 」
    P2PソフトWinnyを利用してワーム活動を行い、ファイルが実行されると感染する
    2006年自衛隊の極秘情報が流出、岡山東警察署で個人情報1500人分（2006.3.6）が流出などは、このウイルスによるもの

17

2. コンピュータウイルスの歴史

- 強力なネットワーク型ウイルス（変種も多いワーム）
  - 2004年（発見数　142，321種類）
    「Netsky.P：ネットスカイP」
    ネットスカイの改良版で、メールを見ただけで感染するように改良されている
    某コンピュータ会社N社の社内ネットワークも停止したらしい

  - 2004～2005年（発見数　333，425種類）
    「MyDoom.AG ：マイドゥーム」
    最新のIEの脆弱性を突いて侵入しメールで拡散、
    メール内のURLをクリックさせ、Webページが表示されると感染する
    感染後、メールアドレスを収集し、拡散を計る

18

2. コンピュータウイルスの歴史

- 届け出件数自体は減少の傾向が出てきた
  - 2006年～2007年（2006年発見数　972，606種類）
    「w32/Netsky：ネットスカイ」シリーズが猛威を奮う
    亜種がどんどん製造され、2年連続で届け出件数1位となる
    IPAでの検出も70%以上を占める

    「w32/Mytob：マイトブ」
    コンピュータワームで、メール型とネットワーク型の2つの感染ルートを持ったタイプで拡大を一気に広げた

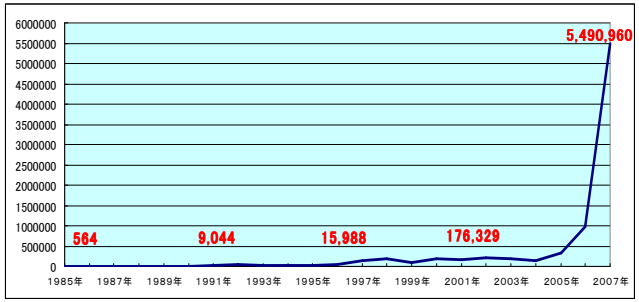
    「w32/Sober：ソバー」
    独自のメール送信機能によりワークを大量拡散させ、
    PCのセキュリティ設定を低下させ、亜種も非常に多い

    「w32/Stration：ストレーション」
    ソバーと同様にメールを大量送信するコンピュータワーム

19

2. コンピュータウイルスの歴史

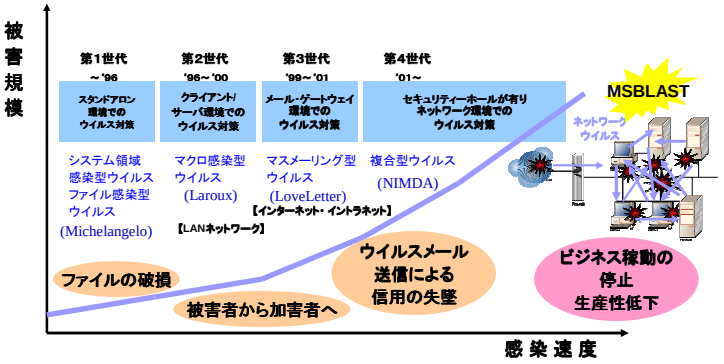
- コンピュータウイルスの発見数
  - 1985年当時は564種類だったが、2007年急激に増加した
    原因は亜種（作り変えられたウイルス）が増加した為



20

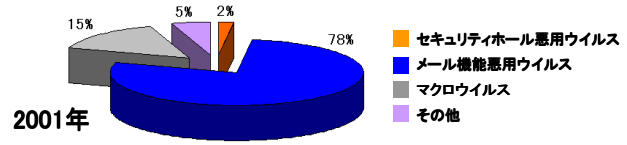
3. コンピュータウイルスの変遷

- ウイルスの進化と感染規模の拡大

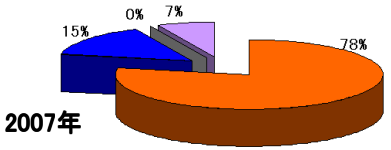


3. コンピュータウイルスの変遷

- コンピュータウイルスの変化



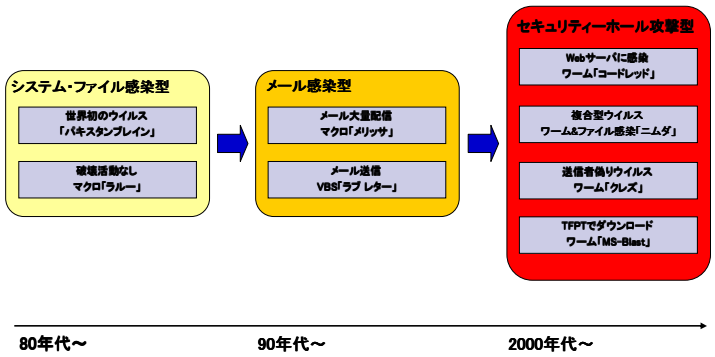
セキュリティホールを悪用するネットワークウイルス増加



※IPA情報処理振興事業協会　2001年7月/2007年12月コンピュータウイルス発見届出状況から

3. コンピュータウイルスの変遷

- コンピュータウイルスの進化



4. コンピュータウイルスの分類

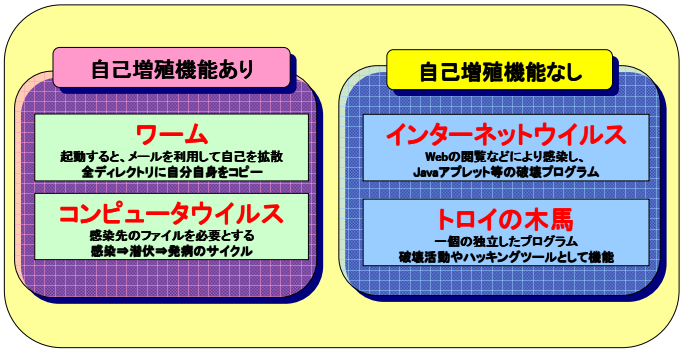
- **ウイルスは誰が名前を付けるのか？**
  - じつは、公式に命名する機関は存在しません。
  - ウイルス対策製品の開発・販売を行っている会社毎にバラバラなのが実情です。

例　ワーム　Klez(クレズ)　2002年に大流行	
①IPA	W32／Klez
②シマンテック	W32. Klez. A@mm
③トレンドマイクロ社	WORM_KLEZ. A
④日本ネットワークアソシエイツ	W32／Klez@MM

  - 接頭語－名前－接尾語のような構成になっていて、固有の特徴がある場合は、その文字などが付けられます。
    ウイルス対策ソフトメーカーのホームページで命名規則が掲載されています。

4. コンピュータウイルスの分類

- 不正プログラム



4. コンピュータウイルスの分類

- スパイウェアとボットと呼ばれる物
  - **スパイウェア**とは
    利用者や管理者の意図に反してインストールされ、利用者の
    個人情報やアクセス履歴などの情報を収集するプログラム等
    収集した情報を保存したり外部に送信したりする物が多い
    また、ブラウザを乗っ取り不要な広告表示を行う物もある
  - **ボット**とは
    コンピュータウイルスの一種で、コンピュータに感染し外部から
    そのコンピュータを操る事を目的として作られたプログラム
    ロボットのように操られる事から、ボットと呼ばれる
    感染した場合、外部のコンピュータにDoS攻撃を行ったり
    大量にメールを送信したり色々な仕掛けを実行する

4. コンピュータウイルスの分類

- **感染先による分類**
  ファイル感染型　システム領域感染型　複合感染型
  マクロ型　マルチプラットフォーム型　携帯端末型
- **活動手法による分類**
  メモリ常駐型　直接感染型　コンパニオン型
- **隠蔽(いんぺい)方式による分類**
  ステルス型　ミューテーション型
- **ウイルスが利用する技術による分類**
  VBスクリプト型　Javaスクリプト型　Javaアプレット型
  ActiveXコントロール型
- **ウイルスの活動による分類**
  ワーム型　ウイルスドロッパー型　情報漏洩型
  バックドア型　ダイレクトアクション型　DoSツール

5. まとめ

- **コンピュータウイルスとは悪意あるプログラム**
- **コンピュータウイルスの歴史は1972年から始まる**
- **コンピュータウイルスも改良・改造で進化している**
- **コンピュータウイルスの命名について**
- **ウイルスの分類**
- IPAセキュリティセンターの分かりやすい？　配布物
  http://www.ipa.go.jp/security/antivirus/shiori.html