# 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～

12. コンピュータウイルスとは　－2－



## 目　　次





## 1. コンピュータウイルスに感染する危険性

『添付ファイルは注意しているから･･･』

－メールのプレビューウインドウは閉じていますか？
－ホームページ閲覧で情報収集されてますよね？
→ 見るだけで感染する時代です！

『じぶんは関係ないから･･･』

－感染するとアドレス帳を利用してウイルスメール送信
→ 知らない間に加害者に･･･
→ 被害状況により信用問題、損害賠償



## 2. コンピュータウイルスに感染したら

- もし、あなたのパソコンが（学校のパソコンが）ウイルスに感染してしまい他の人に迷惑を掛けた場合、どういった事が起こるのか
  - **社会的信用の維持**
    - 感染したウイルスが交流先へ送信したメールで2次感染。交流先の学校内で繁殖し、**相手先のコンピュータシステム停止を招く**･･･
  - **情報保持の義務**
    - 感染したウイルスによりPC内のファイルが送信される。そのファイルには**個人情報**が記載されていた･･･
  - **情報資産の保全**
    - データを蓄積していたサーバのファイルがウイルスによって破壊された。
    - バックアップを取っていた以降の**データは紛失**
    - 復旧に数日費やす･･･
  - **機会の維持**
    - ウイルスの感染により校内システムのネットワーク接続が不可能に。
    - 本日配布する資料などのデータは**配布不可能**･･･

■感染するとどうなる？

データ/PC破壊　不正侵入　不正サイト接続
メール自動送信　動作不良　Dos攻撃
なりすまし　情報漏洩　通信阻害

■メールを利用してウイルスをばらまかれる
■ファイルやデータが第三者に見られてしまう
■データが破壊される
■コンピュータを乗っ取られる
■他のコンピュータを攻撃する
■大量の通信を行いネットワーク不通
・・・ETC

被害者から一転、加害者に

5

■ウイルス被害もいろいろ

■ 直接被害
- システム領域の破壊・改変
- ファイルやフォルダーの削除・改変
- メールの不正送信
- ネットワーク負荷の増大
- 不正アクセスされやすくなる
- 不正アクセスを実行
- DOS攻撃を実行

■ 二次的被害
- 復旧コスト
- 生産性の低下
- イメージの悪化



7

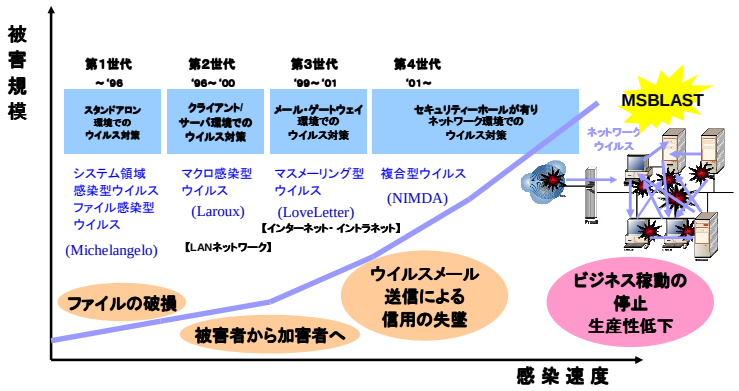
■感染するとどうなる？

『パソコンにこんな症状はないですか？』

- 動作速度が遅くなる
- 画面上に覚えのないメッセージ、アニメーション、絵、図形が表示
- 勝手にインターネットに接続しようとする
- ダイヤルアップの接続先が変更されている
- アプリケーションプログラムが起動しなくなる
- データファイルが破壊される
- 覚えのないファイルが作成されている
- アイコンが変更されている
- メールソフトの送信済みトレイに覚えのない履歴がある
- エラーメッセージが出る
- プログラムファイルのサイズが大きくなる

6

■ウイルスの進化と感染規模の拡大






8

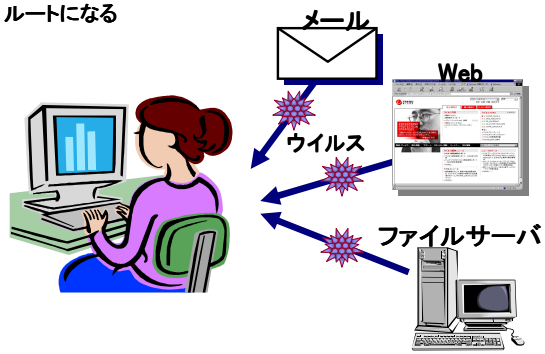
## ■コンピュータウイルスの感染経路

- **メールに添付**されてやって来るタイプ
  - NETSKY（ﾈｯﾄｽｶｲ）、Klez（ｸﾚｽﾞ）、Bugbear（ﾊﾞｸﾞﾍﾞｱ）
- **ネットワークを利用**してやって来るタイプ
  - MS-Blast（ﾌﾞﾗｽﾄ）、SQLスラマー、Sasser（ｻｯｻｰ）
- **ホームページを見る**とやって来るタイプ
  - Nimda（ﾆﾑﾀﾞ）、Redlof（ﾚｯﾄﾞﾛﾌ）
- **ファイルのダウンロード**、ファイル交換でやって来るタイプ
  - Antinny（ｱﾝﾃｨﾆｰ）、Fizzer（ﾌｨｻﾞｰ）

9

## ■コンピュータウイルスの感染経路

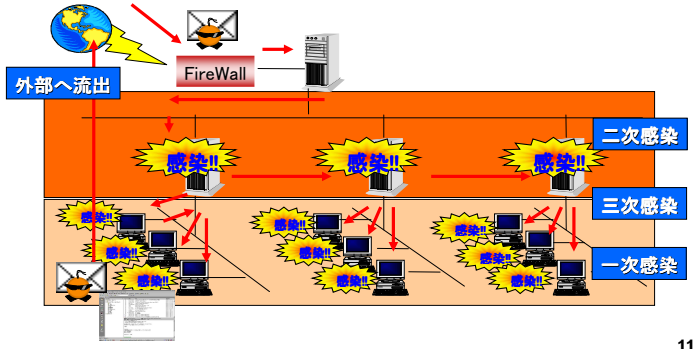
- 個人の場合
  **コンピュータを使って情報を入手する手段が、そのままウイルス感染ルートになる**




10

## ■コンピュータウイルスの感染経路

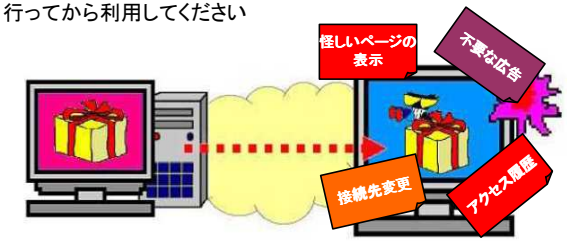
- ネットワークの場合
  **ウイルスが蔓延しやすく共有プログラムにでもファイル感染型が感染あるいは電子メール送信により添付ファイルから驚異的な速さで感染する**




11

## ■コンピュータウイルスの感染経路

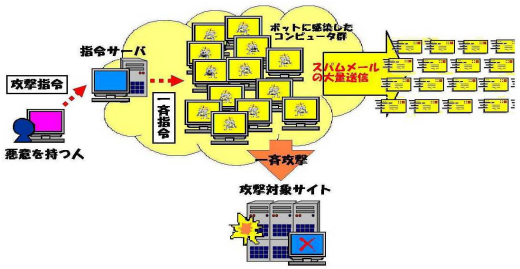
- スパイウェア・ボットの侵入経路
  スパイウェア・ボットはウイルスとしての区別が難しい
  感染経路はウイルスとよく似ているが、フリーソフトウェア（無料のソフト）に仕込まれていたりする場合もある（特に海外製ソフト）
  インターネットでダウンロードしたファイルにはウイルス検査を行ってから利用してください




12

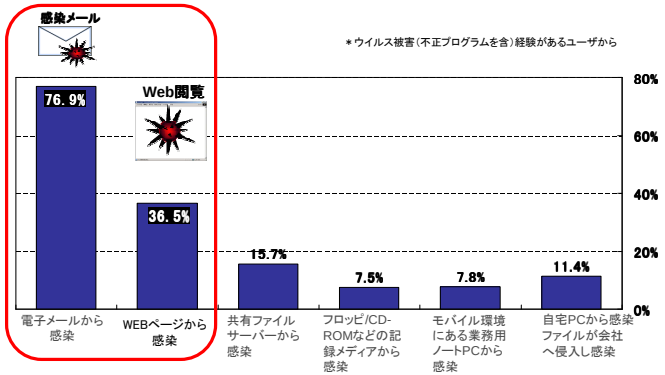
## ■コンピュータウイルスの感染経路

- ボットのネットワークは恐ろしい
  近年非常に耳にするようになってきたのがボットである
  ボットはもっとも悪意あるプログラムの代表といえる
  ボットネットワークという悪の組織のようなネットを構築して
  手先となったPC達を外部から一気に操る事も可能




13

## ■アクセスメディアインターナショナル主催
**Webアンケート調査**（2003年4月　有効回答数＝255件）






15

## ■コンピュータウイルスの感染経路

- **キーロガー**って何？
  **キーボードからの入力を監視して入力情報を**
  **コンピュータ内部に記録する為のソフトウェア**である
  元々はコンピュータソフトをデバックする為に使われてきた物だが
  これを悪用し、IDやパスワードを盗用する為に使われる場合がある

  インターネット・カフェや公共の設置パソコンなどに仕込まれ
  利用した人間のクレジットカード番号やネットバンキングの
  パスワード等を盗み取る犯罪が発生している

  不特定多数の人が使う端末での情報入力には注意する必要がある

  ボットやスパイウェアがこの機能を持ちパソコンの中から
  情報を外部に送信する場合もある

14

## 3．やってみようウイルス対策

- **ウイルス対策ソフトウェアの導入**
  - パソコン使用中は常に起動していて、ウイルスからの感染を監視している。ウイルス感染時の駆除機能を持つ。
  - 無料の物と有料の物（市販の物）がある。
- **パーソナルファイアーウォールの導入**
  - パソコンが勝手な通信をしないように常に監視しているソフト。
- **スパイウェアの対策ソフトウェアの導入**
  - パソコンの情報を勝手に送信したり、インターネット広告を勝手に表示するようなプログラムの駆除を行う。
- **セキュリティパッチの適用**
  - マイクロソフトやその他メーカーから配布される修正ソフトをパソコンにインストールする。
- **情報の収集**
  - 常に最新のコンピュータウイルス情報を気にしておく。

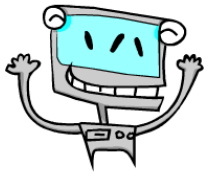
16

## 3．やってみようウイルス対策

- **ウイルス対策ソフトウェアの導入**
  **代表的なウイルス対策ソフト（市販の物）**
  - **ウイルスバスター2008**
    トレンドマイクロ株式会社
    http://www.trendmicro.com/
  - **Kaspersky Internet Security 7.0**
    株式会社ジャストシステム
    http://www.just-kaspersky.jp/
  - **ノートンインターネットセキュリティ2008**
    株式会社 シマンテック
    http://www.symantec.co.jp/
  - **ウイルスセキュリティZERO**
    ソースネクスト株式会社
    http://www.sourcenext.com/

17

## 3．やってみようウイルス対策



- **ウイルス対策ソフトウェアの導入**
  **無料配布されているウイルス対策ソフトウェア**
  - **avast! 4 Home Edition 日本語版**
    http://www.avast.com/jpn/download-avast-home.html
  - **AVG Free Edition　v7.5**
    http://www.avgjapan.com/avgfree75.html

それぞれに商用利用してはならない、**個人利用に限る**などの使用条件がありますが
ウイルス対策ソフトとしての機能を持っています。
また、上記以外にも数多くの無償ソフトがありますが、英語版のソフトウェアも多い。

18

## 3．やってみようウイルス対策

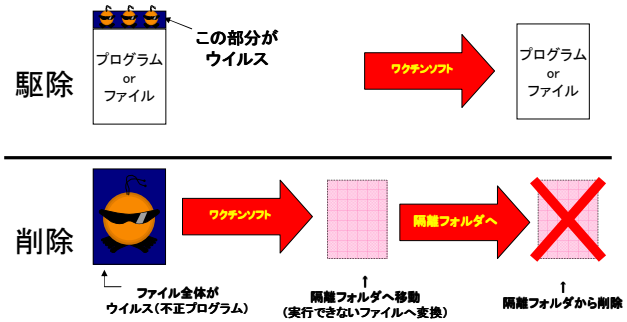
- **ウイルス対策ソフトウェアが出来ること**
  - スケジュール機能によりパソコンのウイルスチェックを自動で行う。
  - 新種のウイルス対策用データファイルの更新を行う。
  - パソコンが使われている間は、常にウイルス感染を監視している。
  - 電子メールの送信や受信時にウイルスのチェックを行う。
- **ウイルス対策ソフトウェアで出来ないこと**
  - **感染時の完全な駆除**
    →専用の駆除ツールを使う場合がある。
  - **Windowsの設定情報を元に戻す**
    →手作業で設定情報を修正する場合がある。

**ウイルス対策ソフトウェアは駆除することよりも、感染を予防する事に主眼を置いています。**

19

## 3．やってみようウイルス対策

■駆除と削除の違い




**最近は「削除」が必要なウイルスが急増しています**

20

## 3. やってみようウイルス対策

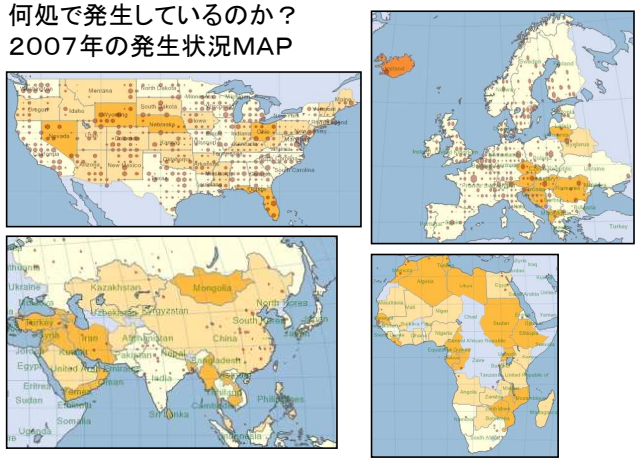
**ウイルス対策ソフトウェア導入後の注意点**
ウイルス対策ソフトウェアはパソコンにインストールしたら終わりではありません

- 常に**ウイルス対策用データファイルを最新の状態**にしておく必要があります。（頻繁な場合は毎日アップデートされます。）
- それぞれのメーカーに**年会費**を支払う必要があります。
- 市販のウイルス対策ソフトは概ね年1回、ソフト自身をバージョンアップを行っています。（2005年版→2006年版）
- 1つのパソコンに**複数のウイルス対策ソフトウェアをインストールしない**でください。（誤動作の原因となります。）
- パソコンを購入した時に付属しているウイルス対策ソフトウェアは試用期間がある**お試し版**である場合があります。

21

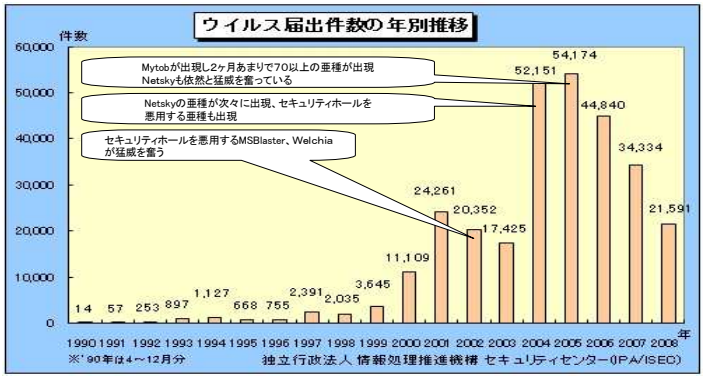
## 4. ウイルスのトラブル事例

- 何処で発生しているのか？
  2007年の発生状況MAP



22

## 4. ウイルスのトラブル事例




23

## 4. ウイルスのトラブル事例

- 郵政公社のブラスター感染（2003年8月）

日本郵政公社は、ワーム型ウイルスの「Blaster（ブラスター）」と亜種の「Welchi（ウェルチ）」に感染し、二度にわたるワームの被害を受けたブラスターに感染した原因がNECの作業ミスであることが、雑誌社の取材でわかり、NECへ損害賠償を求める検討を始めた

ブラスターの感染は、NECの保守作業員がルールを守らず、郵政公社内部に設置した保守用のパソコンを勝手にインターネットへ接続した時に起きた

**6000台のパソコンを一時的にLANから切り離し、復旧に3日間かかった**

24

## 4. ウイルスのトラブル事例

- 岡山県警倉敷署、巡査長の個人PCがWinnyウイルス感染で捜査資料が流出（2006.3.6）

  岡山県警倉敷署は、同署に勤務する巡査長の個人用PCから個人情報を含む捜査資料などがネット上に流出していたことが判明したと発表した

  流出した個人情報は**約1,500名分**で、事件の被害者などであるという

  これらの情報を持ち帰り、保存していた個人用PCがWinnyウイルスに感染、情報が流出した

  **情報が流出した全員を対象に県警職員が戸別訪問して謝罪することを決めた**

25

## 4. ウイルスのトラブル事例

- 国交省関東運輸局のパソコン35台がウイルスに感染（2005.12.17）

  国土交通省関東運輸局（横浜市中区）は17日、同局と、東京都など1都6県にある同局管轄の七つの支局、事務所のパソコン計**35台**がコンピューターウイルスの一種「WORM　NACHI」に感染したと発表した

  除去作業に伴い、一部でシステムの**再インストールが必要**になった
  同局はネットワークを遮断し、すでにウイルスを除去し終えたという
  感染したのは同局の19台と支局、事務所の16台
  業務には支障は出ていないという

  同局は「ウイルスに感染した**個人所有のパソコンを局内**のネットワークにつないだのが原因ではないか」と話している

26

## 4. ウイルスのトラブル事例

- ファイル交換ソフトWinny・Shareの被害が急増している

| | | |
|---|---|---|
| 2008.3.14 | 東京消防庁深川消防署 | 火災原因調査書が流出 |
| 2008.3.12 | 大阪近鉄百貨店 | 1107人の顧客データ流出 |
| 2008.2.9 | JA越後ながおか | 2266件の農家データ流出 |
| 2008.2.20 | 日立製作所 | 約6000人の顧客データ流出 |
| 2007.12.4 | セコム | ATMの作業手順書流出 |
| 2007.11.17 | オーバーチェア | 28,157件の個人流出 |
| 2007.11.16 | 広島大学病院・原爆病院 | 195人のデータ流出 |

「Winny個人情報流出まとめ」サイトより
http://www.geocities.jp/winny_crisis/

27

## 5. まとめ

- **ウイルスに感染した場合の被害と症状**
- **ウイルスの感染経路**
- **ウイルスへの対策について**
- **ウイルスの感染事例**

28