セキュリティ関係情報

- 毎月第2水曜日は、「Windows Updateの日」とマイクロソフトが定めました。
- Microsoft社製品のセキュリティ情報は、こちらをご覧下さい。

より詳しいセキュリティ情報は、次のサイトにアクセスして確認しましょう。

- IPA/ISEC（情報処理振興事業協会･セキュリティセンター）
  - http://www.ipa.go.jp/security/
- JPCERT/CC（JPCERTコーディネーションセンター）
  - http://www.jpcert.or.jp/
- セキュリティホールmemo（龍谷大･小島先生）
  - http://www.st.ryukoku.ac.jp/~kjm/security/memo/

ウィルス対策７箇条

IPAの「パソコンユーザのためのウィルス対策７箇条」を一部改変。

完璧なウィルス対策はない。いくつもの対策することで、安全性を高める。

1. ワクチンソフトで予防と検査（ウィルス定義ファイルは最新に）
   - 予防のためにはまずワクチンソフトを導入して、定期的にコンピュータ全体をウィルスチェック。そして新種のウィルスに対応するために、ウィルス定義ファイルは常に最新に更新。
2. メールの添付ファイルとHTMLメールには注意
   - よく知らない人からのメールは削除。添付ファイルのあるメールは本文に添付ファイルの記述があるか確認（なければあやしい）。添付ファイルは直接開かず、ダウンロードしてウィルス検査。送信する場合も添付する前に検査。HTMLメールも危険性が高い。
3. ダウンロードしたファイルは開く前にウィルス検査
   - ウィルス検査をしていない可能性があるので、開く前にはかならず検査。また、ワクチンソフトで発見できないもの（国際電話やQ2ダイヤルに接続するもの）もあるので、あやしいサイトからはダウンロードしない。
4. ソフトのセキュリティ機能を活用
   - ブラウザやメーラーのセキュリティレベルを適切に設定して、被害を未然に防ぐ。WordやExcelのマクロ自動実行機能を無効に。
5. セキュリティパッチをあてる
   - セキュリティホールはなくならない。使用しているソフトのサイトを確認して、セキュリティパッチをあてる。
6. ウィルス情報を見逃さない
   - インターネットや雑誌等のウィルス情報を確認する。コンピュータのウィルスの兆候を見逃さない。
7. データの定期的なバックアップ
   - ワクチンソフトの駆除は、ファイルを消す場合もある。ウィルス被害からの復旧のために、日ごろからデータのバックアップを。そして、感染した後は、再インストールを。

「ウィルス被害の現状」編

ウィルス感染の状況（学内）

正確なデータはないが、学内システムのリプレース（2002年4月）でわけると、おおよそ次のような状況。

- リプレース前
  - 実習室：報告は若干（マシンが古いため？）
  - 学生：ノートパソコンへの感染が若干
  - 教職員：年に数人
- リプレース後
  - 実習室：感染はほぼ皆無
  - 学生：ノートパソコンの被害がちらほら（拡大しつつある？）
  - 教職員：リプレース前よりは増えているかも

結果としては、個別の被害はあるものの、大規模な被害はまだない。

ウィルス感染の状況（国内外）

IPA/ISECより。

- 1999年
  - Ska(Happy99)（2月）
  - PrettyPark（9月）
- 2000年
  - LOVELETTER（5月）
  - MTX（10月）
  - Hybris（11月）
- 2001年
  - SST(AnnaKournikova)（2月）
  - Badtrans、その2（5月）
  - Sircam（8月）
  - Nimda（9月）
- 2002年
  - Klez（1月）
  - Bugbear（10月）
  - Opaserv（10月）
- 2003年
  - SQL Slammer（1月）
  - Blaster（8月）
  - Welchi,Nachi（8月）
  - Sobig.F（8月）
- 最近の傾向
  - ネットワーク（メールやファイル共有）を使って自己増殖
  - セキュリティホールを悪用

なぜウィルス対策は必要なのか？

- 感染した人に及ぶ被害
  - ファイルやコンピュータが使えなくなる
  - パスワードや暗証番号が盗まれる
  - ファイルやコンピュータの復旧のための手間･時間
- まわりの人に及ぶ被害
  - 感染したコンピュータを踏み台に他のコンピュータに感染
  - 大量のデータを送信してネットワークに高負荷

加害者が被害者になってしまい、他人に迷惑をかけ信用を失うことになる。（あそこは対策をしていないっ） 場合によっては、法的責任と損害賠償もありうる。だから対策が必要。

「ウィルスの実態」編

コンピュータウィルスの定義

フレデリック・コーヘン（F.Cohen カリフォルニア大）が米セキュリティ学会（DOD/NBS Computers & Security Conference）で初めて使った言葉

- 「他のコンピュータプログラムに自身のコピーを含ませるために、それらのプログラムを修正することによって伝染することが出来るプログラム」

「コンピュータウィルス対策基準」（通商産業省告示 第952号）によると、次のとおり。

- 「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、次の機能を1つ以上有するもの」
  - 自己伝染機能（自分自身または宿主の機能を利用して自分を他のシステムにコピー）
  - 潜伏機能（特定時刻や一定期間･処理回数まで症状を出さない）
  - 発病機能（ファイルの破壊やコンピュータに異常な動作をさせる等）

ウィルスの種類

- 機能･活動で分類
  - ウィルス
    - 宿主となるプログラムやファイルに感染。宿主が起動されたときに発病。
  - トロイの木馬
    - 通常のプログラムやファイルに化ける。伝染が目的ではなく、情報の漏洩やシステムの破壊が目的（バックドア）。
  - ワーム
    - ネットワークを通じて、自分のコピーを他のコンピュータに拡散する。
- 宿主（感染する場所）で分類
  - ファイル感染型
    - プログラムファイルに感染。一般的なタイプ。
  - ブートセクタ感染型
    - コンピュータが起動するときに実行されるシステム領域（ブートセクタ）に感染。

    - 複合感染型
        - ファイルとブートセクタの両方に感染。
    - マクロ感染型
        - WordやExcelのデータファイルのマクロ部分に感染。
- メモリへの常駐で分類
    - メモリ非常駐型
        - 感染したファイルが実行されたときだけ、ウィルスが活動する。
    - メモリ常駐型
        - 感染したファイルが一度実行されると、電源を切るまで常駐し活動しつづける。

最近は、ソフトウェアのセキュリティホール（安全上の不具合）を悪用するものが目立つ。

感染したらどうなる？

- 動作が遅くなる（メモリの不足、ディスクへの頻繁なアクセス）
- 画面表示が乱れる
- 音が鳴る
- 異常なメッセージが表示される
- コンピュータが起動しない
- コンピュータが勝手に再起動する
- ファイルが削除･破壊される
- ディスクが破壊される
- ウィルス画像
    - http://www.nai.com/japan/security/virusgazox.asp ウィルス画像事典（ネットワークアソシエイツ）
    - http://www.sophos.co.jp/pressoffice/imggallery/virusimg/ イメージギャラリー（ソフォス）
    - http://kosuge.kdn.jp/anti/info/viinfo1.html ウィルス発病（コンピュータウィルス対策）

どこからやってくるか？

IPAセキュリティセンターの2003年9月の報告より。

感染経路	届出件数			
	2003年（9月まで）		2002年	
メール	11,446	90.9%	19,767	97.1%
ダウンロード	133	1.1%	121	0.6%
外部・海外からの媒体	169	1.3%	123	0.6%
不明・その他	837	6.7%	341	1.7%

- メール
    - 添付ファイルが感染していたり、メーラーのセキュリティホールを悪用
        - 例：W32/Klez, W32/Bugbear, W32/Sircam
- ダウンロード
    - インターネットからダウンロードしたファイル、ホームページ上のコード（Java、ActiveX）
        - 例：VBS/Redlof, W32/Nimda

- 外部・海外からの媒体
    - 記録媒体（FD、MO、CD-ROM）の貸し借り、雑誌などの付録CD-ROM
- 不明・その他
    - ネットワーク経由（ファイル共有、セキュリティホール等）

最近は、経路が複雑になり、複数の経路から伝染しようとするものが登場。

- W32/Nimda
- W32/Klez

「ウィルス対策」編

どうやって感染を防ぐ

まず「ウィルス対策７箇条」を実施。具体的な対策はこちら（http://kosuge.kdn.jp/anti/measure/vime.html）を参考に。

最近は「プロバイダのサービスを使う」を追加するとよい（有料）。ワクチンソフトと２重の検査ができる。（持っているワクチンソフトと違う会社のサービスを選ぶと効果的）

- メールのウィルス検査サービスを行ってくれているプロバイダがある
    - ワクチンソフトベンダと協力したサービス
    - 自分でチェックする必要がない（時間がかからない）
    - 自分のパソコンの種類に関係ない
- 代表的なプロバイダとサービス
    - @nifty ウィルスバスターfor @nifty Mail http://www.nifty.com/mail/virusbuster/index.htm
    - BIGLOBE メールウィルスチェックプラス http://email.biglobe.ne.jp/vcheck/
    - OCN ウィルスチェックサービス http://www.ocn.ne.jp/option/vcheck/mail/
    - So-net
    - DION

最近はさらに進化し、ホームページの閲覧時のウィルスもチェックするものもある。

- @nifty BBセキュリティ http://www.nifty.com/security/bbsec/
- BIGLOBE ホームページウィルスチェック http://hpcheck.biglobe.ne.jp/

ブロードバンド時代のウィルス対策

- パーソナルファイアウォール
    - ファイアウォールは、「ネットワークの防火壁」
    - ソフトウェアで外部からのアクセスを制限
    - Windows XPには簡易機能がある
    - 主なパーソナルファイアウォールソフト
        - Norton Internet Security
- ブロードバンドルータ
    - 家庭で複数のパソコンがある人向き
    - ネットワークの通信を制御
    - 必要ない通信を遮断（不正アクセスの防止）

学内システムの対策

教育環境を中心に対策。

- 計算機実習室のパソコン
  - ワクチンソフト Norton AntiVirus Corporate Edition (シマンテック)
- 貸与しているノート型パソコン
  - ワクチンソフト ウィルスバスターコーポレートエディション (トレンドマイクロ)
- メールとホームページ閲覧
  - ゲートウェイ対策 InterScan VirusWall (トレンドマイクロ)
- ファイアウォール

今後の課題は、研究環境や学生のノートパソコンへの対策。

発見したらどうする？

- ネットワーク･ケーブルを抜く
- ウィルス検査･駆除
  - ウィルス定義ファイルは最新に
  - ワクチンソフトのメッセージをよく見る (ウィルスの名前は？駆除できたか？)
- 届け出る
  - IPAに届出
    - 所定の届出様式で、郵便･FAX、E-mail (記入例)
  - コンピュータウィルス110番
    - 03-5978-7509 (10:00-12:00, 13:30-17:00)
  - 大学 (情報科学センター)
- FDやCD-ROMを検査
- まわりの人に連絡

最後に

完璧なウィルス対策はない。でもいくつもの対策を組み合わせれば、安全性はずっと高くなる。

しかし、ウィルスをなくならない。人の好奇心・いたずら心・犯罪性がウィルスを生む。

したがって、ウィルス問題を他人事だと思わず、日ごろから心がけるのが大切。

参考リンク

- セキュリティ全般
  - http://www.ipa.go.jp/security/ IPA (情報処理振興事業協会) セキュリティセンター
  - http://kosuge.kdn.jp/anti/ コンピュータウィルス対策
  - http://www.cyberpolice.go.jp/ @police (警視庁)
- 有名ワクチンソフトベンダー
  - http://www.symantec.com/region/jp/ シマンテック (Norton AntiVirus)
  - http://www.trendmicro.co.jp/ トレンドマイクロ (ウィルスバスター、InterScan)

- http://www.nai.com/japan/ ネットワークアソシエイツ (Mcafee VirusScan)

- 市販ワクチンソフト
  - Norton AntiVirus, Norton Internet Security（シマンテック）
  - ウィルスバスター（トレンドマイクロ）
  - VirusScan（ネットワークアソシエイツ、McAfee）
- 無償ワクチンソフト
  - http://www.grisoft.com/ AVG Anti-Virus
- オンラインスキャン
  - http://www.trendmicro.co.jp/hcall/index.asp ウィルスバスターオンラインスキャン (トレンドマイクロ)
  - http://www.symantec.com/region/jp/securitycheck/index.html ウィルススキャン (シマンテック)
- リアルタイム感染情報
  - http://www.trendmicro.com/jp/security/map/overview.htm ウィルストラッキングセンター (トレンドマイクロ)
  - http://mast.mcafee.com/default.asp Virus Map (米McAfee社)
- Windows
  - Microsoft セキュリティ http://www.microsoft.com/japan/security/
  - Microsoft セキュリティスクエア http://www.microsoft.com/japan/security/square/default.asp
  - Windows Update http://windowsupdate.microsoft.com/
  - Office Update http://office.microsoft.com/officeupdate/default.aspx