ふつうの人のための セキュリティ対策

小島　肇
龍谷大学理工学部 実習助手
コンピュータ緊急対応センター (JPCERT/CC) 専門委員

今日のお話

- コンピュータウィルス対策
- 不正侵入対策

コンピュータウィルス対策

蔓延するコンピュータウィルス

- 毎日、数～十数種類の新しいウィルス
- 新作のほとんどは Windows を標的とする
  - たまに Linux / UNIX 用
  - Mac OS 用はほとんどない（昔は多かった）
    - その古いやつがいまだに流通しているらしい…

最悪自分がやられるだけでしょ?

- 取り付いたウィルスが他人を攻撃する、ことに注意
  - 他人にウィルスをばらまく(しかも、たくさん)
  - バックドアを仕掛けられ、他人を攻撃するためのアジト(踏み台)にされる
  - 分散型使用不能攻撃 (DDoS 攻撃) のプラットホーム
  - 損害賠償請求がくる可能性
- 情報漏洩が発生する場合あり
  - 情報漏洩機能つきウィルス (sircam, klez)
  - バックドアから侵入され、ファイルを奪われる
  - 盗聴ソフトを仕掛けられネットワーク全体が丸裸にされる
  - 漏洩した情報はたちまち WinMX で全世界的に共有されてしまったり

最近のウィルスの特徴

- メールなどネットワークを利用した拡散
  - ファイルにとりつくタイプはあまり見かけない
- ついついダブルクリックしたくなる、巧妙な添付ファイル名 (2 重拡張子偽装つき)
  - たとえば「人妻.jpg.exe」なんてのが来たら…
- セキュリティホールを利用した拡散
  - 電子メールを開いただけで感染
- 高機能・複合化
  - いくつもの攻撃・拡散手段を用いる
  - ウィルス・ワーム・トロイの木馬・バックドアの機能をあわせ持つ

Internet Explorer について

- 多くのウィルスが Internet Explorer (IE) / Outlook Express (OE) を主要なターゲットに
  - 圧倒的なシェアが背景
- それらを使わなければ安全に?
  - 現状では確かにリスクは減るが、もちろん本質的な対応ではない
  - Windows では多くのソフトが IE コンポーネントを利用しているため、IE の利用を完全に排除するのは困難
  - IE 6 SP1 は、以前に比べればずいぶん改善された

なにはなくともアンチウィルスソフト

- 3 つのプラットホーム全てに装備すると効果的
  - メールゲートウェイ
  - ファイルサーバ
  - クライアント
- 全部そろえようとすると、けっこうなお金がかかる
  - まずは最も効果の高いところへ配備
  - その後必要なら整備

メールゲートウェイ

- 最近のウィルスの多くは電子メールを利用して繁殖
  - 水際で対処可能
  - 既存環境を変更せずに導入可能
- けっこうなお値段、負荷もそれなりにかかる
  - 安いものもある (例: RAV AntiVirus)
  - いまどきの dual CPU GHz サーバなら ok?
- ISP が対応している例多数
  - ただしオプション、しかも受信時のみ対応である例が多い
  - 送信時にも対応する ISP の例:TTNet

ファイルサーバ

- 2001 年に流行した Nimda ウィルスが利用
  - 共有フォルダに MS Word が利用する .dll ファイルを設置
  - Word 文書を開くと……ドカン!
- 最近の例: Bugbear, Opaserv ウィルス
  - 使い方は Nimda とは違うが
- サーバとクライアントを区別しないようなライセンス形態であれば、サーバだけ特別高価ということはない
- それなりな負荷

クライアント

- 最終防衛ライン
- いまどきの PC であれば負荷は苦にならず
- 最近の付加機能 (企業向け製品だと省かれている?)
  - proxy server 形式によるメール検査機能
  - パーソナルファイアウォール機能
  - インスタントメッセージ対応
- クライアント数が多いと
  - それなりな出費 (ボリュームディスカウントはあるが)
  - 管理コスト

ソフトを入れれば ok か?

- ウィルスデータのアップデート
  - 毎日? 毎時間? 数分おき?!
  - 自動的に行うプロダクトもある
  - 大規模環境では集中管理ソフトを利用
    - 別売りの場合あり
  - ASP (Application Service Provider) 型ソフト
    - トレンドマイクロ eDoctor, NAI VirusScan ASaP
  - ネットワークトラフィックに注意
- 誤判定、異常動作
  - まれにある

ソフトを入れれば ok か? (続)

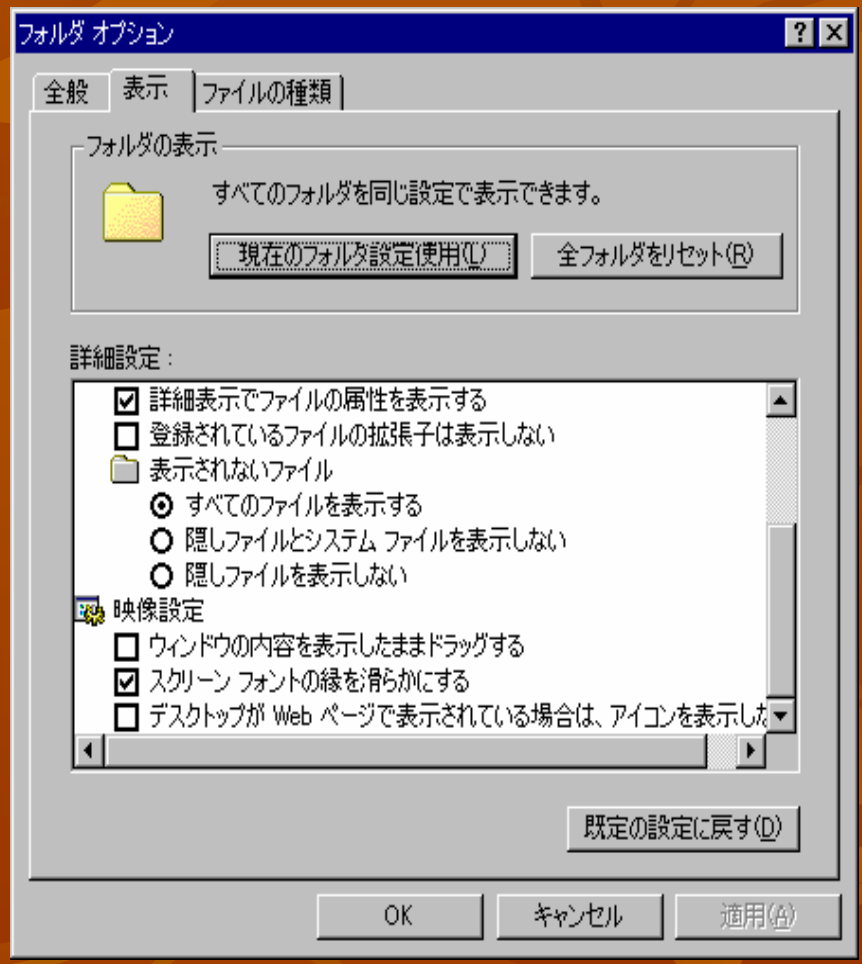
- 新種ウィルスへの対応時差
  - ウィルス発見 → アンチウィルスソフトベンダー送付→ 解析 → ウィルスデータ作成 → 配布 → 取得
  - どう急いでも半日～一日はかかる
  - 最初の流行が日本だと、対応が間に合わなかったり…
- 緊急対応
  - メールサブジェクト名、添付ファイル名などに対し注意喚起
  - これもふまえたサービスが各社から登場中
    例: トレンドマイクロ TM EPS, NAI McAfee MVP[2]
- 事後確認
  - ディスク全体を定期的に検査
- ウィルス情報を注視
  - アンチウィルスソフトベンダーの情報通知サービス
  - 自分が使っていないベンダーの情報も入手

ソフトを入れれば ok か? (続^2)

- セキュリティホールをねらうウィルスの増加
  - 「メールを開いただけで感染」の実現
  - CodeRed / Nimda ウィルスは web サーバ (IIS) を攻撃
  - Windows Media Player や MSN Messenger を狙うものも
- 利用するソフトウェアは最新の状態に!
  - Windows Update で OS への修正プログラムを適用
  - IE, OE は可能な限り新しいものを
    - 最新: IE 6 SP1
  - MS Office への修正プログラムの適用
  - 3rd party ソフトも忘れずに

基本動作が重要

- 怪しい添付ファイルは開かない
- 添付ファイルを開く前にウィルスチェック
- ファイルの拡張子は表示するよう設定する
- むやみにファイルをダウンロードしない
- 定期的にディスク全体をウィルスチェックする



何かおかしいときは…

- なんだか動作がおかしい
  - やたら重い
  - 動作が不安定
  - 大量のネットワークトラフィック (メール送信など)
- ウィルスに感染?!
  - ネットワークから切り離す (トラフィック異常があれば)
  - 冷静に状況を把握する
  - 最新のウィルスデータ・複数のワクチンソフトでチェック
  - あやしいファイルがあった場合はアンチウィルスベンダーに送付
- 単に OS / アプリがおかしいだけかも (^^;;)

関連情報

- IPA セキュリティセンター (IPA ISEC)
  http://www.ipa.go.jp/security/
- アンチウィルスベンダー

トレンドマイクロ	http://www.trendmicro.co.jp/
シマンテック	http://www.symantec.com/region/jp/
ネットワークアソシエイツ (NAI)	http://www.nai.com/japan/
ソフォス	http://www.sophos.co.jp/
エフ・セキュア	http://www.f-secure.co.jp/
Code Logical	http://www.code-logical.com/
RAV	http://www.ravantivirus.com/ (安い) http://www.rav-japan.com/ (高い)
アンラボ	http://www.ahnlab.co.jp/

関連情報

- マイクロソフト
  - セキュリティ総合ページ
    http://www.microsoft.com/japan/security/
  - TechNet セキュリティ (セキュリティ詳細情報)
    http://www.microsoft.com/japan/technet/security/
  - 上記ページにはセキュリティ関連ドキュメントが多数ある。たいへん参考になるのでぜひ参照されたい。

不正侵入対策

日々発生する侵入事件

- 日本語サイトを対象とした愉快犯的なものだけでも１日１件以上
  - 日本のくらっくサイト情報 http://tsukachan.dip.jp/
- ウィルス・ワームによる侵入
  - 日常的に発生
- あまり公にならない侵入事件
  - 内部者による犯行
  - プロフェッショナルによる犯行

どこから侵入されるのか

- セキュリティホール
- 脆弱なパスワード
- 甘い設定

セキュリティホール

- 悪用可能なプログラム上の間違い (バグ)
- セキュリティホールのある場所
  - サーバ: web サーバ, mail サーバ, …
  - クライアント: web ブラウザ, mail ソフト, …
- 攻撃が開始される場所
  - 外部 (リモート) から攻撃可能
  - そのホスト上 (ローカル) でのみ攻撃可能
- 攻撃の方法
  - 能動的攻撃: web サーバを攻撃され、…
  - 受動的攻撃: web ページを閲覧して、mail を読んで、…

脆弱なパスワード

- あまりにもあまりなパターン
  - パスワードなし
  - ログイン名、名字、名前、社員番号と同じ
- 物理アクセスできる場合…
  - ポストイットに書いて貼ってある…
  - 引き出し・財布に紙が入ってる…
  - 内部・知人による犯行の可能性は念頭においておく
- パスワード解読攻撃を受けると弱いもの
  - 辞書にある単語
  - 7 文字以内

甘い設定

- Windows, Linux (UNIX) いずれも、デフォルトの状態がものすごくセキュアである、ということはまれ
  - Windows .NET Server 2003 はセキュアになるらしい?
- 不要な / 意図しないサービスプログラム
  - telnet, ftp, mail, web, …
  - 何が動いているのかを確認する必要あり
    - 特にプリインストール OS
  - 不要であれば止める
- 甘いパーミッション (ファイルアクセス制限)
  - 誰でも書き込める C:¥InetPub
  - 誰でも書き込める C:¥
  - 誰でも読める場所に顧客情報を置いてしまった…

侵入を防ぐ – ファイアウォール

- 許可するサービスを除いて全て遮断
- 数万円程度の安価なブロードバンドルータでも、ステートフルインスペクションなど高度なファイアウォール機能を持つ
- 自分で設定するには、TCP/IP プロトコルに関するそれなりな知識が必要
  - 「わかっている」SI 屋の援助が得られるとうれしい
- ファイアウォールは、許可するサービスについては防衛できないことに注意
  - 「その他多数」を守るための設備
  - 許可するサービスは十分な注意を払って管理・監視

侵入を防ぐ – きっちり管理

- 不要なサービスは停止
- 起動するサービスについては、最新のバージョンを利用する
  - 修正プログラムはすぐさまきちんと適用する
  - テスト環境をつくっておき、そこでテスト後に本番に適用できると better
- 強固なパスワードを選択する
- むやみに logon / login を許可しない
  - 特に特権ユーザ (administrator / root) による login
  - 一般ユーザで logon / login し、runas (Windows 2000/XP) や su, sudo (UNIX) を活用

侵入を防ぐ – クライアント

- 受動的攻撃を受ける場合が多い
  - 特に mail と web
- やるべきことはウィルス対策と同じ

侵入を防ぐ – モバイル端末

- CodeRed / Nimda の教訓
  - 自宅・出先で note PC が感染
  - 仕事場にそのまま挿す
  - 攻撃開始
  - 被害額が数億円
- きちんとウィルス対策・侵入対策しておく
  - 特に、私用 note PC を持ってきたりする場合
  - 私物は禁止したいところだが…

侵入を防ぐ – 状態を監視

- 攻撃の兆候を見つける
  - ログをチェック
  - CPU、ディスク、ネットワークの状態
    - 利用率が高い場合、それは妥当なのか、それとも異常な状態なのか?
  - 侵入検知システム (IDS) の導入
    - Network IDS (NIDS)
    - host IDS
    - 監視カメラだと思ってください

管理なんてやってらんない!

- アウトソースという選択: 最近はいろいろある
  - サーバ管理
  - ファイアウォール管理
  - 侵入検知システム管理
- アウトソースするに足りる SI 屋探しが重要
  - ダメなところは本当にダメ
  - 評判がよくても、自分たちに有能な担当者が割り当てられるとは限らない
    - 東京では評判のいい会社なんだけどねー
  - ダメならさっさと乗り換えた方がいい

アウトソースなんてできない!

- 最低限必要なのは…
  - ファイアウォール
  - 修正プログラムのすばやい適用
  - ユーザ・パスワード管理
  - ウィルス対策
- 侵入検知システムは何かと便利なので、余裕があればぜひ
  - ただし、それなりの運用コストがかかる

侵入されてしまった!

- 対応
  - 該当機器をネットワークから切り離す
  - 冷静に状況を調査し、何が原因で侵入されてしまったのかを確認する
  - 関係機関 (JPCERT/CC や警察など) に連絡する
  - 2 次被害などがないかどうか慎重に確認する
- 復旧
  - 機器にはバックドアなどが仕掛けられている可能性があるため、OS・アプリは全く新規にインストールし直す
  - 最新の修正プログラムを適用する (必要なら独自に修正する)
  - データ部分をバックアップから慎重にリストアする

関連情報

- JPCERT/CC (http://www.jpcert.or.jp)
  - **JPCERT/CC レポート**
    http://www.jpcert.or.jp/wr/
  - **コンピュータセキュリティインシデントの報告**
    http://www.jpcert.or.jp/form/
  - **管理者のためのセキュリティ推進室**
    http://www.jpcert.or.jp/magazine/atmarkit/
- IPA ISEC (http://www.ipa.go.jp/security/)
  - **脆弱性関連情報**
    http://www.ipa.go.jp/security/news/news.html
  - **情報セキュリティ対策実践情報**
    http://www.ipa.go.jp/security/awareness/administrator/administrator.html

関連情報

- ZDNet Security How-to
  http://www.zdnet.co.jp/help/howto/security/
- @IT
  - Windows Insider
    http://www.atmarkit.co.jp/fwin2k/index.html
  - Linux Square
    http://www.atmarkit.co.jp/flinux/index.html
  - Security
    http://www.atmarkit.co.jp/fsecurity/
- セキュリティアンテナ
  http://www.st.ryukoku.ac.jp/~kjm/security/antenna/
- セキュリティホール memo
  http://www.st.ryukoku.ac.jp/~kjm/security/memo/