アンチウイルスソフトウェアが役に立たない件

小島 肇

kjm@rins.ryukoku.ac.jp

去年、自分で言ったこと

- Windows ではアンチウイルスソフトウェアは必須だが、「入れれば安心」というものではない
- Mac, Linux における費用対効果はかなり低い
  - 現時点ではマルウェアは流行っていないから
  - Windows を併用している場合は別
- 忘れずに
  - 他のセキュリティ対策
  - アンチウイルスがもたらす不具合の可能性
  - トレードオフは主観に基づく

2009年2月以降の学内における ウイルス感染状況

- アンチウイルスソフトウェアは無力
  - 導入していてもやられる
  - ウイルス定義ファイルを最新の状態に更新していてもやられる
- やられるとアンチウイルスソフトウェアの更新機能が停止される
  - 一方、ウイルスは時々刻々と自動更新され続ける
  - 絶対に無くせない
- にもかかわらず、やられている本人には妙な安心感が
  - 「アンチウイルス入れてるから大丈夫ですよね？」

アンチウイルスもうイラネ？

- 対応遅い・対応されない
- 金かかる
- 手間かかる
- PC 遅くなる
- Microsoft から ‘Morro’ が無償提供される予定
  - 2009年後半に登場予定

アンチウイルスソフトよりも重要なこと

- ソフトウェアの更新
  - Windows Update
  - Office Update
  - 3rd party ソフトウェアも忘れずに更新。特に Adobe Reader、Flash Player、QuickTime

アンチウイルスソフトよりも重要なこと

- 権限分離
  - 管理者権限ダメ、ゼッタイ
  - Windows Vista を使うのがオススメ
    - ユーザー アカウント制御（UAC）を有効に
  - Windows XP の場合は、一般ユーザー権限のアカウントを作成し、そのユーザーとしてログオンして使う
    - 学内のコンピュータ演習室はこの状態

入れるなら……

- ホストベースの侵入阻止システム（Host-based IPS）のようなもの
  - 例: FFR yarai
  - 誤検出は免れ得ないので注意
- シグネチャベースのアンチウイルスソフト
  - あくまで HIPS の補助として
  - Microsoft Morro で十分か
- くれぐれも、これらに頼らないこと
  - どちらもあくまで補助手段。基本はソフトウェア更新 + セキュアな設定・運用
  - クスリに頼るのではなく、攻撃を受けても耐えられる体力をつける

質問？