クライアントセキュリティを考える

中京大学
情報理工学部情報システム工学科
長谷川明生

いまさらながらのCIA

- Confidentiality
  - 学生向け供用端末にはどう？
  - 外部メモリーの大容量化小型化
  - 多様化するクライアント問題
- Integrity
  - クライアントについてはどうだろう？
  - データの保全？
- Availability
  - これが一番めにつくか？

クライアント機器概念の変容

- パソコン
- ポータブルゲーム機器
- スマートフォン、PDA
- ICプレーヤ
- デジカメ
- プリンタ
- クラウドの普及
  - Chrome OS等々
  - Netbook

クライアントの問題点

- 情報漏えいの問題
- 情報保全の問題
- 可用性の問題
  - 故障、製品寿命
  - ソフトウェアトラブル
- 不正ソフトウェアの問題
  - パーソナルファイアウォールは使える？
- ブラウザ利用にまつわる問題
- Social Engineering

可用性にかかわる問題

- ３年未満で壊れるパーツ
  - ディスク
    - 中の情報は(去年だけで3/11台）
  - コンデンサー等
- ポータブル記録メディアの小型化大容量化
  - 壊れたら痛い
  - 無くしたら痛い
  - 自動実行の問題
- ソフトの高機能化

とかく便利なソフトは・・・

- ある日メールを読もうとしたらOutlookが
- セーフモードでもクラッシュ
- 2度と起動しないし・・・
- 今日のメールが読めない・・・
- 過去3年ほどのメールが
  - Thunderbirdに吸い上げ
- なによりスケジュール管理に困った
  - 暇な私でもぽつぽつと半年先くらいは

とかく便利なソフトは・・・

- メールデータ
  - Thunderbirdに吸い上げて救済
  - でも、フォルダからフィルタ設定から面倒
- 予定データ
  - Googleカレンダーにバックアップが
    - Google calendar syncさまさま

とかく便利なソフトは・・・

- 依存度が高いほど影響も大きい
- Windows mobileとsyncの母艦が
- 復旧対応に複数日
  - Officeのアカウント削除と再追加
  - レジストリいじって
    - プロファイルの削除
  - ソフトウェアの更新
  - Officeの再インストール等々
  - FAQ等々にあることはためしたが

とかく便利なソフトは・・・

- たまたまWin7にするつもりでパーツー式
  - 急きょ組み立て
- 新マシンでもデータ移行では相変わらずダメ
  - セーフモードでは起動するけど救いには
- 結局新規ユーザーを作ってデータだけを移行
  - Outlookは補助的利用に格下げ
    - Googleカレンダー
    - Thunderbird
- 普通の人には、こんな対処絶対に無理
  - パソコンはやっぱり特殊なまま

データや設定の移行

- 便利にはなったけれど
- ネットワーク移行では、しばしば切れる
- ディスクを使った移行が安全
- でもMS製品とファイルだけ
- 長期間使っているとユーザプロファイルが腐る
  - たしかにXPからアップグレードを繰り返し
- Linuxなんかだと相変わらず面倒

Googleカレンダーに救われたが

- Gmail
- Google calendar
- Google携帯
- Google Apps
- Google map
- Google Earth
- Google street view
- Google携帯
- Google public DNS

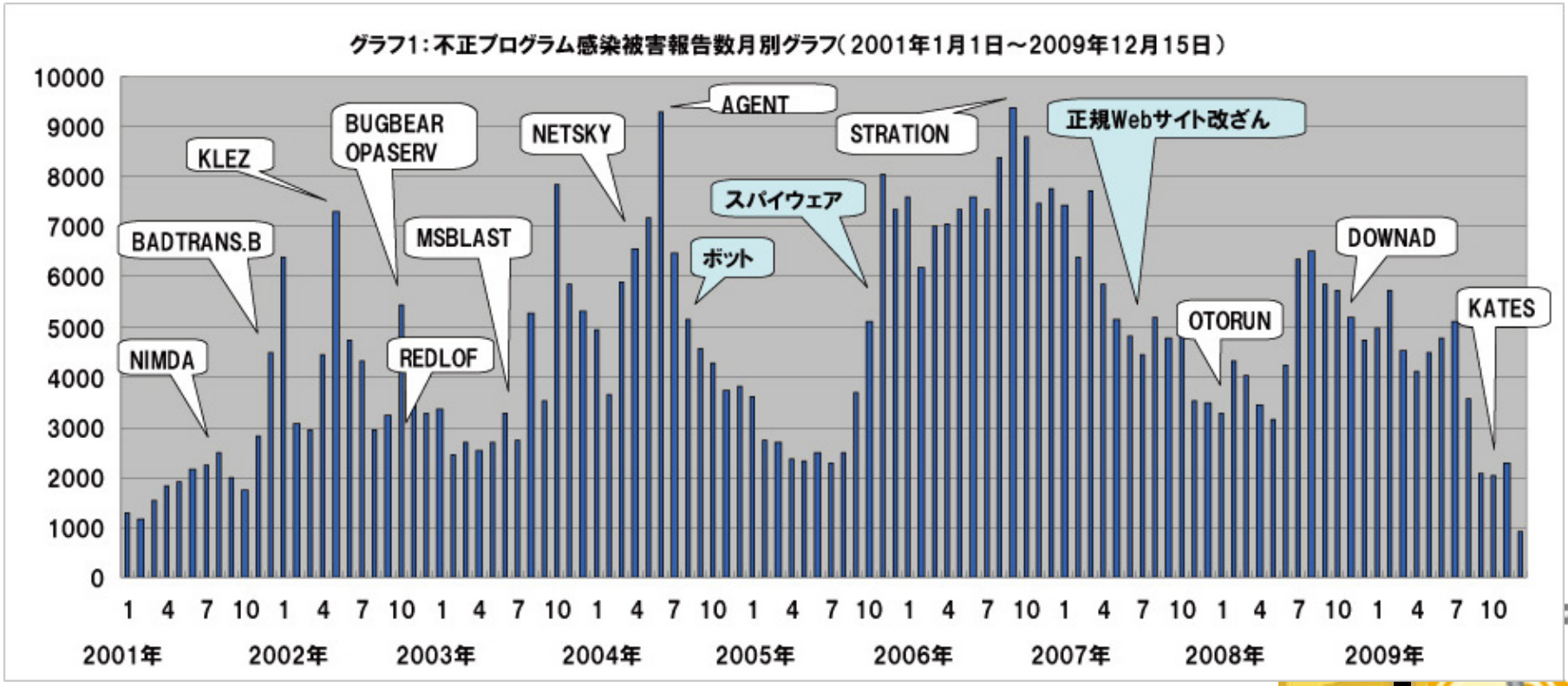
(Google)だけでいいの？

- 携帯サービス
- 時刻表を買わなくなった
  - 路線検索
- 地図もオンライン
  - GPS携帯等
  - ナビ機能
- カタログショッピング
- 携帯までも
- アクセス回線だけ

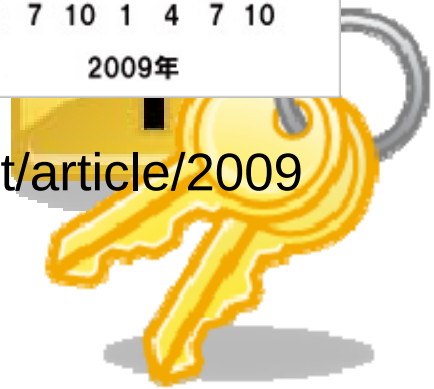
クラウドは万全？

- クラウドに置いたデータの保全は可能？
  - 他のベンダーにデータ簡単に移行できる？
  - Popで持ってこれればいいけれど。
  - 連絡帳等は
- プライバシーは
  - メールやアプリのデータだけじゃなく
  - DNSの検索記録だって
- いつも使えるの？
  - DNSは弱点

マルウェア動向



http://jp.trendmicro.com/jp/threat/security_news/monthlyreport/article/20091216084357.html



マルウェアの動向

- なくならないUSBメモリー経由の感染
  - ゼミ生10人のうち3人が感染に気付かず
- 電子メール添付での感染は減少？
  - 最近は見かけていない。
  - いわゆるナイジェリア系やFBI系の釣りは多いが
- WEB経由に移行？
  - GUMBLARとか
- 学生からの相談はハードが多い
  - たまにソフト設定もあるが

傾向としては減少？

- SMTPからHTTPへ(セキュリティ各社レポート)
  - スクリプト埋め込み
  - 検索エンジン
  - ウエブ広告

不正ソフトウェア対策ソフト

- 最近は常時オンラインが前提になっている
  - たまにしか電源を入れないと時間がかかる
- 安くなってきているが
  - ３年とか３台まで等々
- 高機能化
  - ファイアウォール
  - ウィルス
  - スパイウェア・トロイの木馬対策
  - パスワード管理機能

学生がよく使っているソフトは

- AVG
- AVIRA
- AVAST
- MSEはどう？
- K〇〇g　ソフトは・・・
  - 某ASC〇〇誌が推奨していたけれど
  - 使ってみたら・・・

使いこなせるのか高機能

- パスワード機能のために追加のパスワード
  - もうひとつ管理すべきパスワードが増える。
- ファイアウォールの自動フィルタリング
  - ファイル共有やプリンタ共有の手間増加
    - 勝手にフィルタ
  - Port randomizeとのミスマッチ
    - セキュリティ対策が裏目
  - 対話型でのメッセージ
    - svchost.exeといわれても

高度の暗号化

- 暗号化キーの保管
  - キーをなくすと大変
    - パスワードリセット
  - Bit Lockerドライブ
    - 安全なのだろうが
    - キーの破損

いろいろなツール

- Secunia　PSI, OSI
  - http://www.secunia.com
- netcraftツールバー
  - http://www.netcraft.com
- WOT
  - 検索の精度のチェック
- no script

IPの問題点

- DNSの問題
  - Kaminskyアタックの全貌は公開されていない
  - 相変わらず設定が問題なDNSサーバ
  - 最近もDNS　Hijacking（twitter)
- ARP spoofing
- TCP等の脆弱性の報告
  - シーケンス番号が推測可能
  - 特殊なパケットで問題

ネット広告の問題

- 話題の単語を検索すると
  - マルウェアサイトに
  - 検索エンジンの表示順位
- 有名サイトの広告だからといって
  - Tenki.jpに販売方法に問題商法の会社広告
- Twitter等の短縮urlの問題

迷惑メール

- 個人的には減っている？
  - 観測では減っていないという報告も
  - 年末はブルーピルのCM増加
- FBIを騙る送金詐欺
  - 新手のナイジェリア
- Freeチケット風マルウェア（2009年当初）
  - Zip圧縮＋パスワード（ウィルス対策回避）
  - Virustotalで捕捉率30%程度

WEBの問題

- 不用意な検索エンジンのキャッシュの利用
- クッキーの扱いの問題
  - CSRF
  - http://www.kb.cert.org/vuls/id/261869
- スクリプトの多用
  - ブラウザも進化したが

ソフトウェアが勝手に通信

- Windows update等（LinuxやFreeBSDでも）
- Adobe updater
- Java updater
- Google updater

信頼性の問題

- 私の見ているオブジェクトは正しいものか？
  - 通販サイト
  - Win7補助ディスク、F-Secureオンラインショップ
    - 別サイトに転送される
  - SSL証明書は簡単に入手できる
    - EV-SSLは確認が厳しいらしいが
- 私のPCは正しい状態にあるか
  - たぶんとしか言えない

なくならないP2P問題

- JASRACからの手紙