インターネットにおける技術的脆弱性の与える影響と対策

インターネットを安心して使うには？

筑波大学図書館情報学系
阪口哲男 <saka@slis.tsukuba.ac.jp>

本日のお題

- 最近インターネットが物騒に？
  - 今夏のBlaster/Welchiaワーム流行
  - OS(基本ソフト)の欠陥頻出
  - SPAM(迷惑メール)の増加
- インターネットを安心して利用するには
  - 技術者やシステム管理者はどうすればよいか？
  - (一般の)利用者に何ができるか？(してはいけないか？)

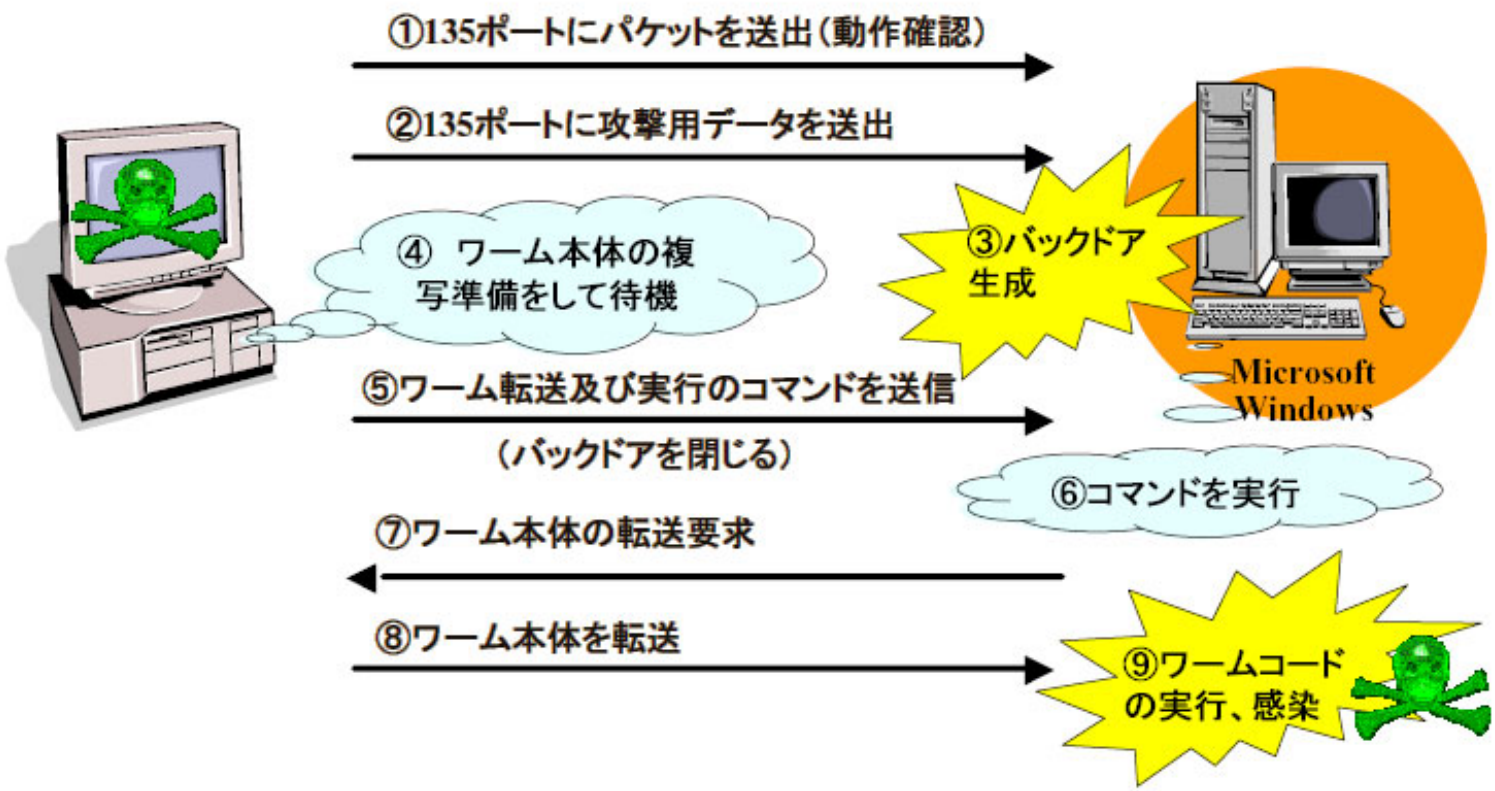
Blaster/Welchiaワーム流行

- 症状は？
  - Blaster: 頻繁な再起動（リブート）
  - Welchia: 自覚症状なし
- Welchiaに害はないのか？
  - 他のPCを攻撃するために頻繁にネットワークにデータを送り出すため、ネットワークの混雑や麻痺の原因になる。

何が起きたのか？

NPA 技術対策課　警察庁技術対策課

Blasterワームの感染動作概要

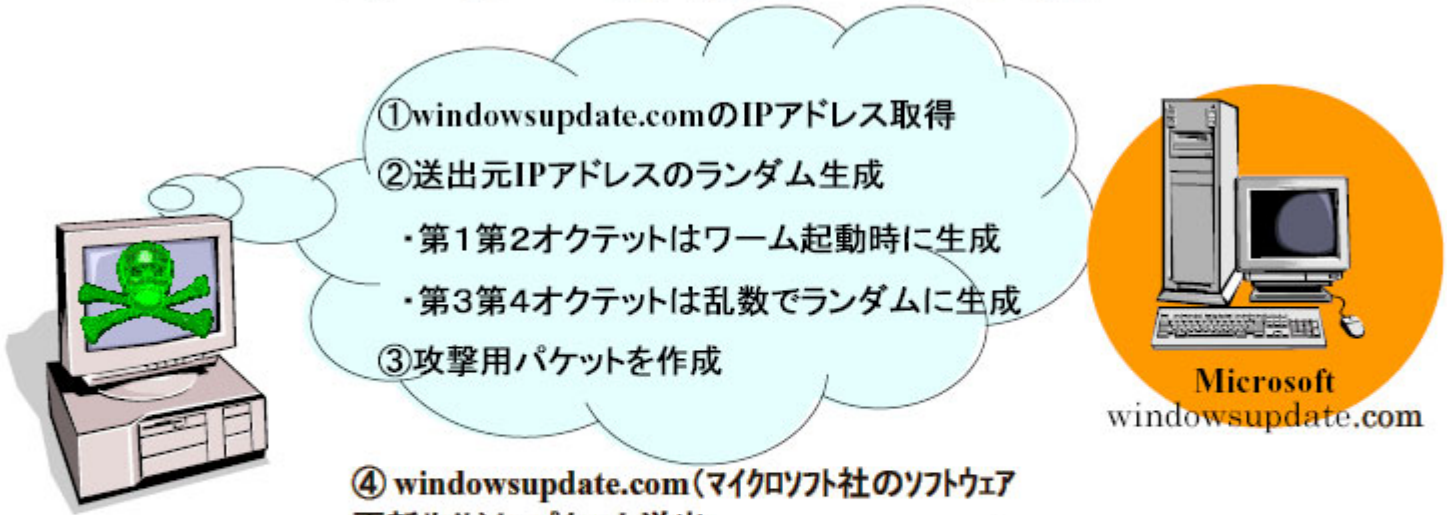


何が起きたのか？(続き)

NPA 技術対策課　警察庁技術対策課

BlasterワームのDoS攻撃動作概要

（1月から8月は16日以降で動作、9月から12月は連日動作）

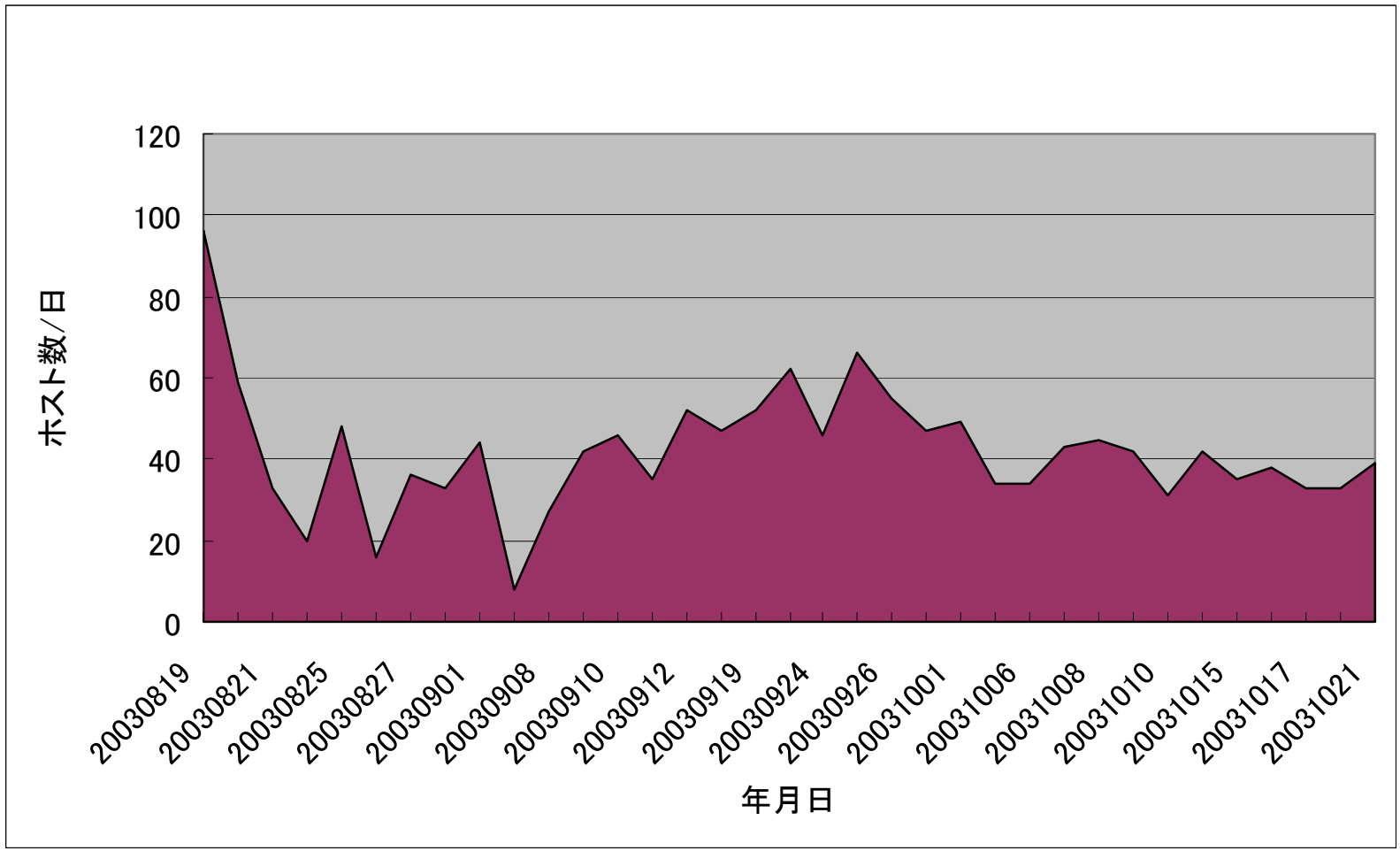


②から④が無限ループで繰り返される

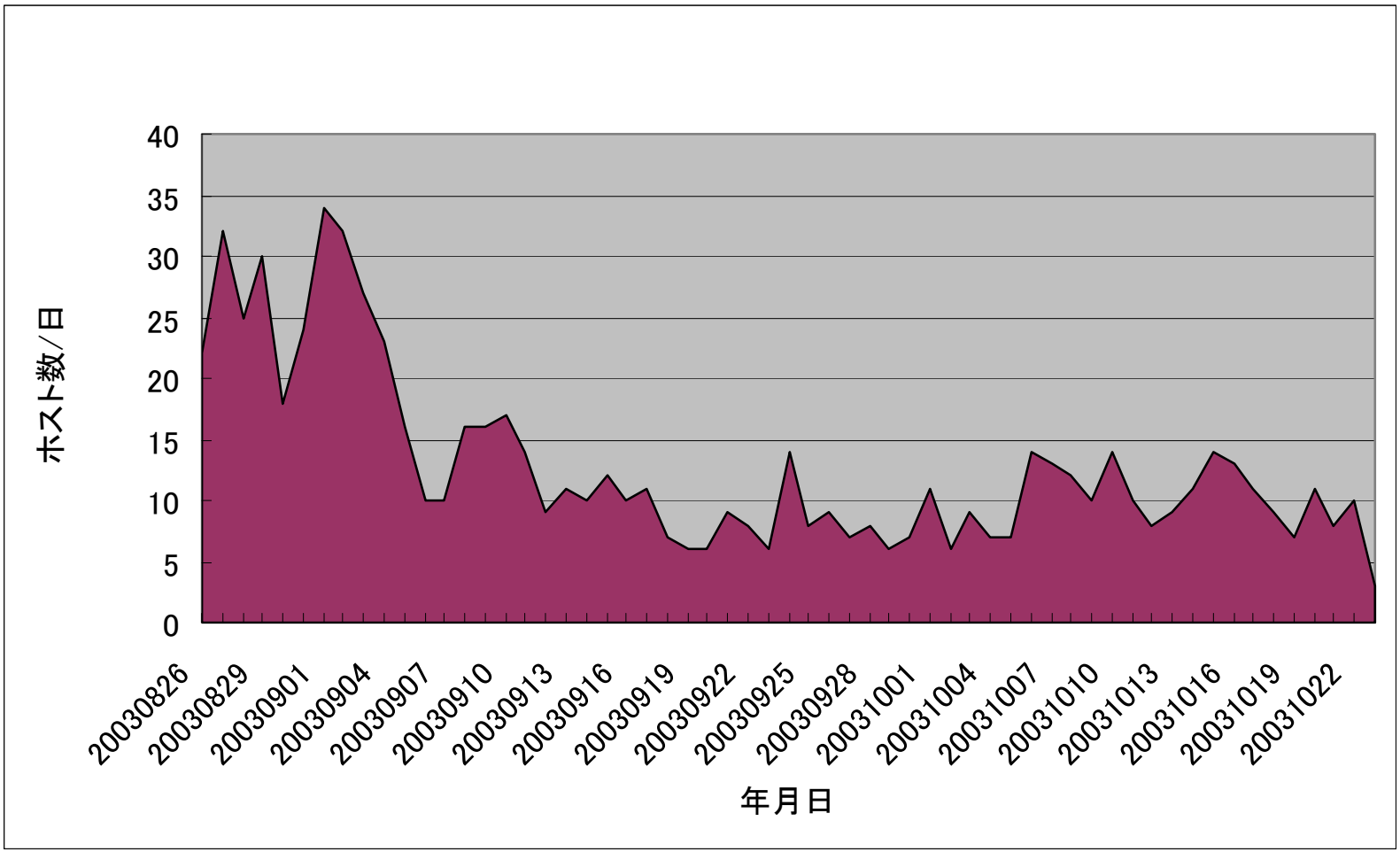
OS	パッチ	
	未適用	適用
WindowsNT（JP）	○	－
Windows2000（JP）	×	○
Windows XP（JP）	×	○
Windows 2003（JP）	※	○

パッチ有効性検証結果
○：感染しない
×：感染する
※：感染しないが再起動する
－：感染しないため検証せず

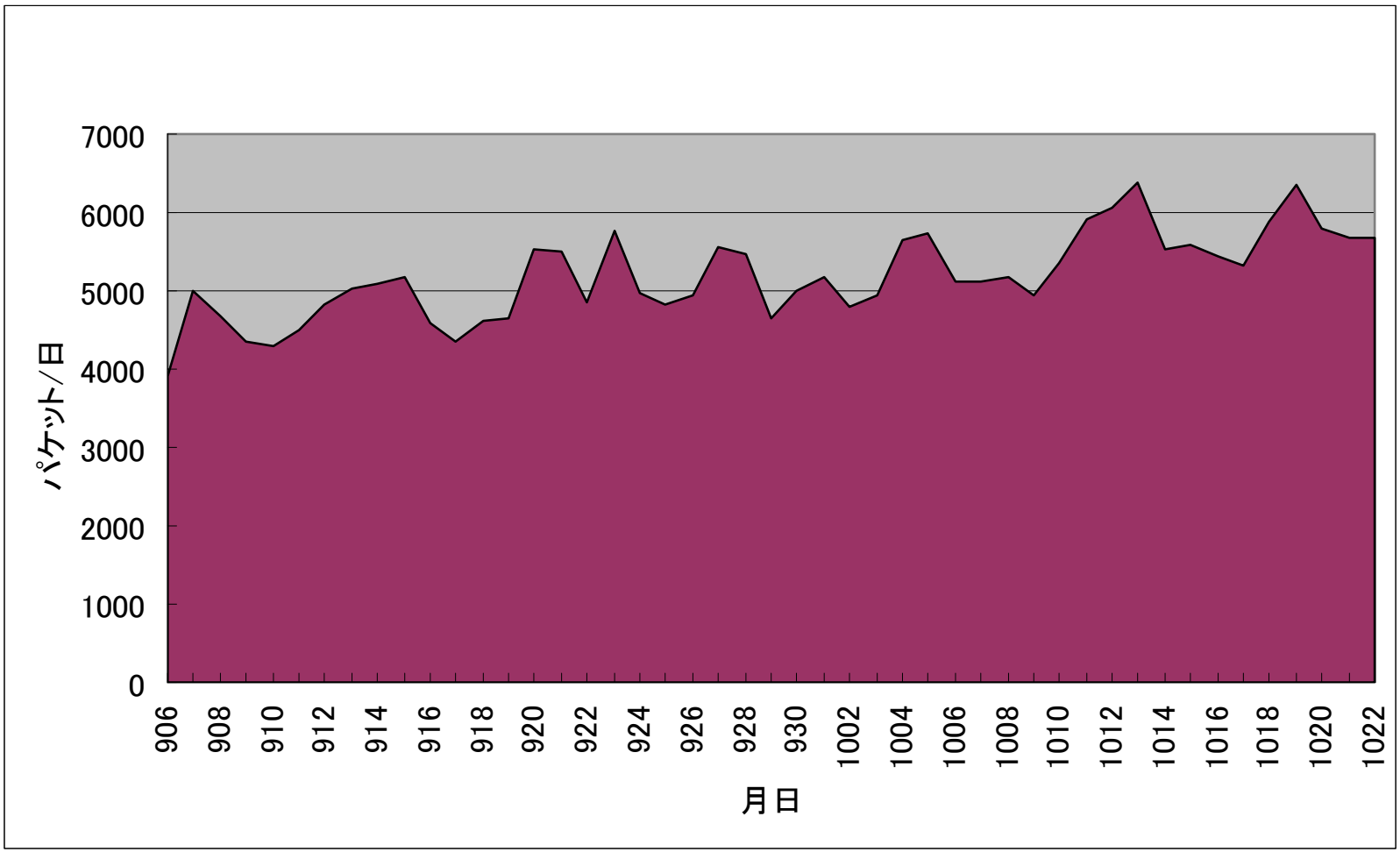
某大学における感染状況



同大内某地区の感染状況



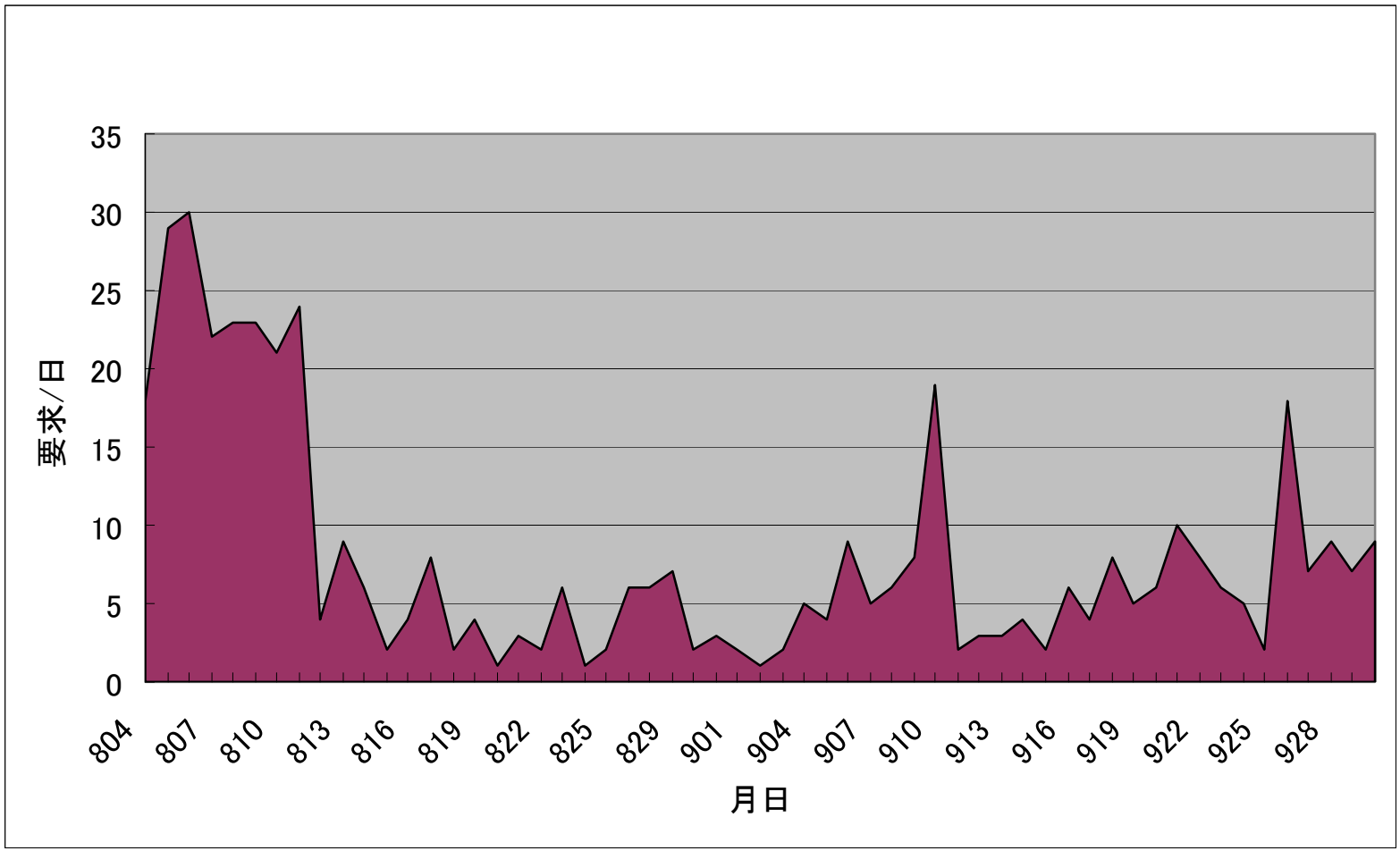
世界的にも根絶されていない



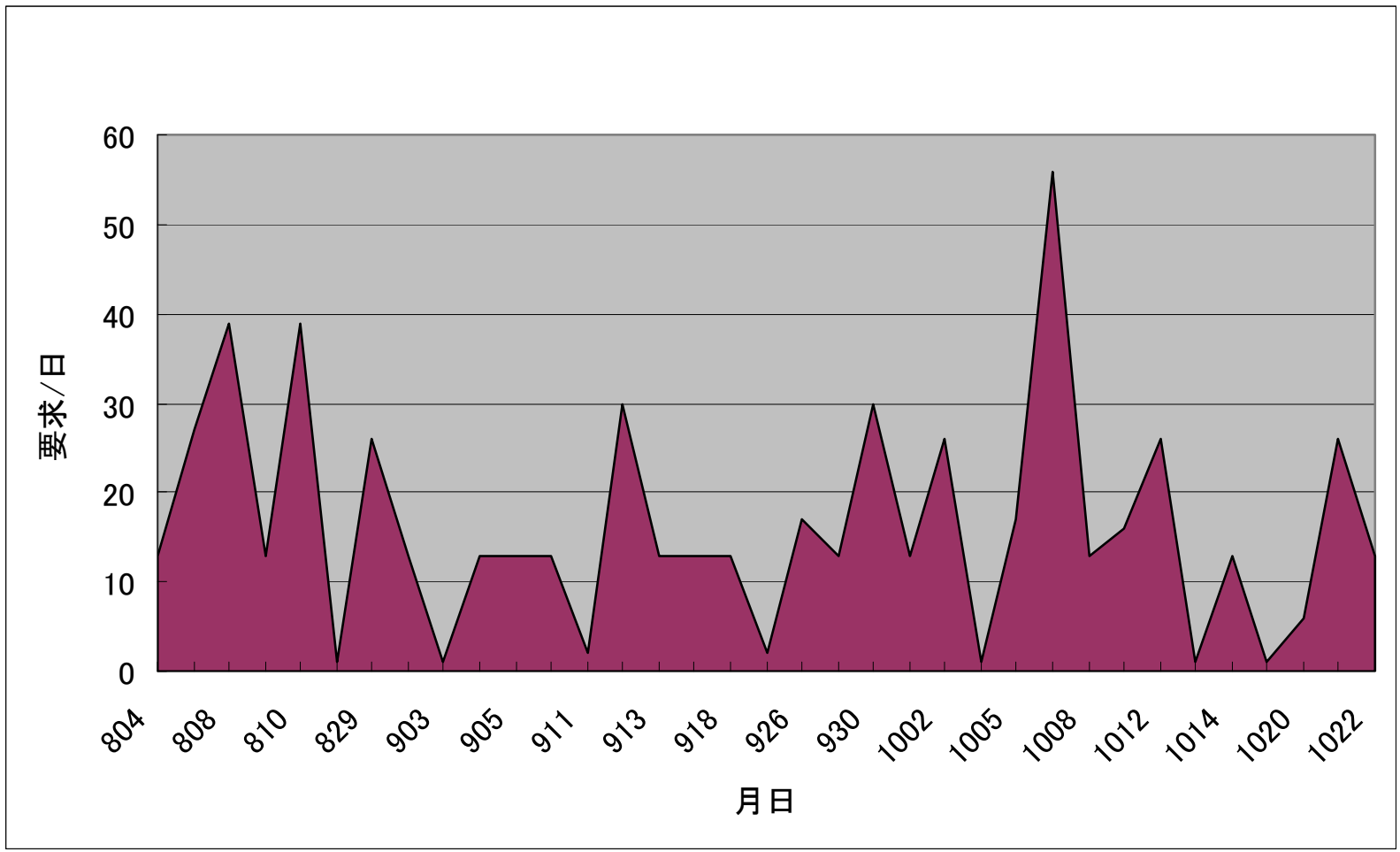
根絶はできないのか？

- 過去の事例から考える
  - Code Redとその亜種
    - マイクロソフト製WWWサーバソフトに感染
    - 発見日: 2001年7月16日
  - InternetWeek2001のセキュリティBOF
    - 「**ブロードバンド時代のセキュリティを考える ～ Code Redの教訓～** 」
    - Code Redはまだまだ残っている
  - 今はどうなのか？

Code Red(亜種)はまだいた



その他のWWWサーバ攻撃も



なぜ根絶できないか？

- 技術者(開発者)やメーカは脆弱性(ソフトに残っている隙)を見つけると大抵その修正版や対策を提供している
- ワーム・ウィルスが侵入に使う脆弱性を放置している利用者・管理者がいる
- 自覚症状（あるいは自らに対する実害）がない限り利用者は意識しない

ファイアウォールはあるが

- 内側(LAN)に感染したマシンをつながれると無力
- 自宅、学会会場など外で感染してくる
- たとえば、エントランスが管理されていても住人の部屋が施錠されてなければ無意味
  - そういうエントランスもすり抜けることはできる

SPAM(迷惑メール)

- 何らかの手段で手に入れた（機械的に生成した）多量のメールアドレスをあて先として、受け取り手の意志とは無関係に送りつけられるメール
- 郵便でもダイレクトメールがあるが、ここまで多量になるのは、ディジタルだからというだけではない

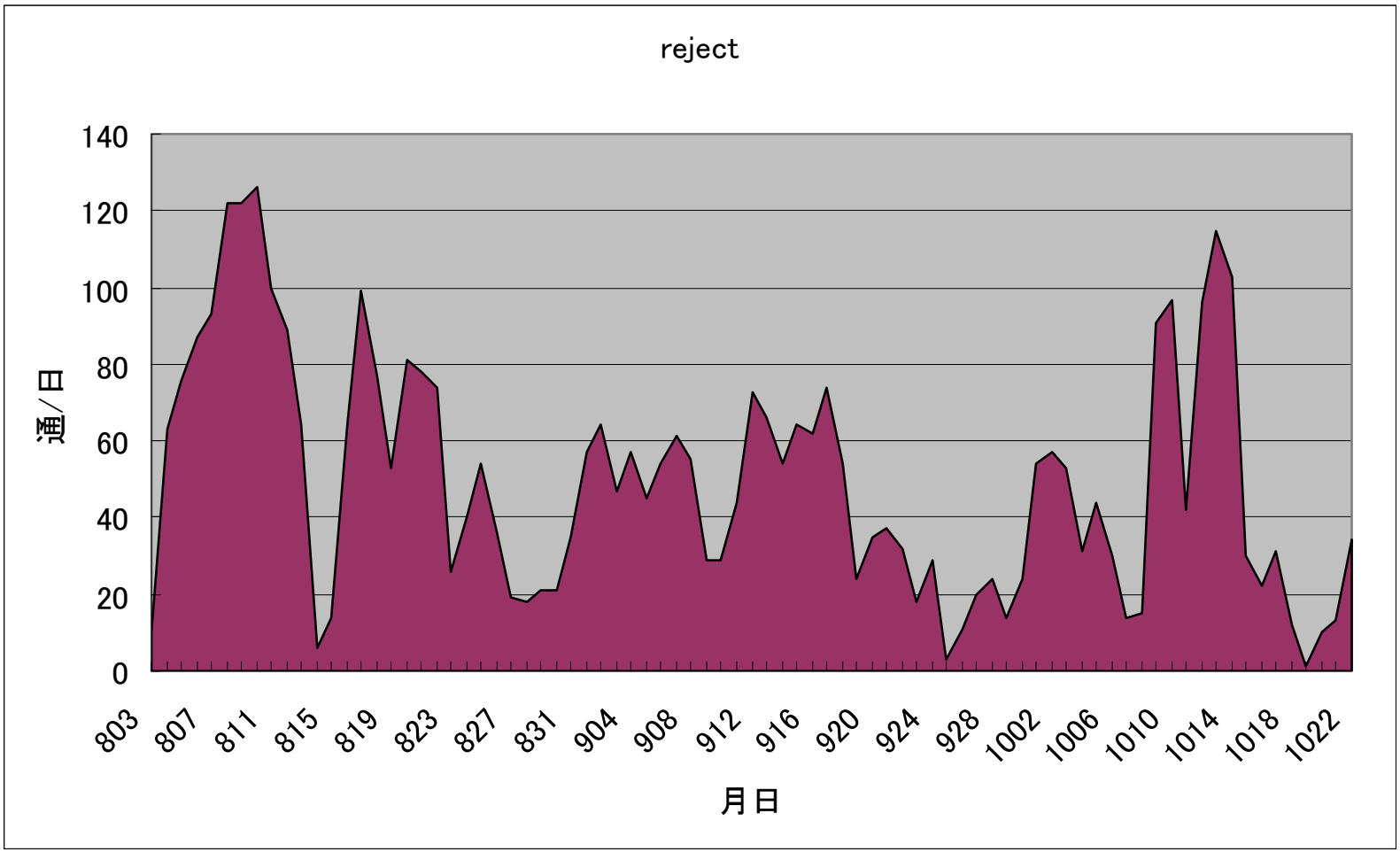
電子メール配送とコスト

- 通常の郵便
  - 一通毎に送信者が料金を支払う
- 電子メール
  - 送信者は自分の身近なメールサーバまでの通信料・使用料を払うのみ
  - 受信者のメールサーバまでの通信料は世界で薄く負担を分け合っている
  - 受信者は自分のメールサーバから手元までの通信料・使用料を支払う

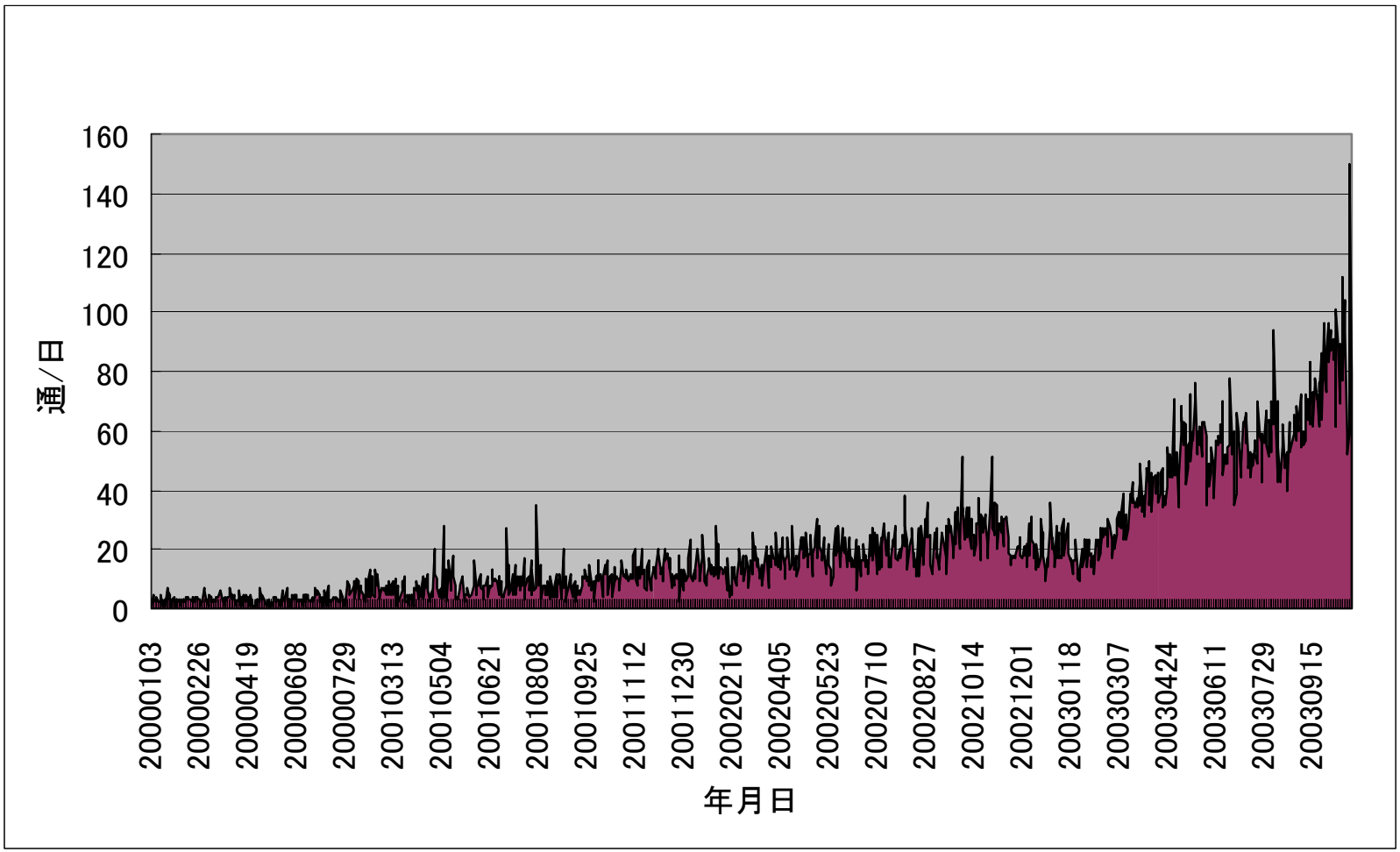
SPAMの問題

- 通信料などの負担を他者に押し付けている
- 受信するメールの量が増えるとそれから本来必要なメールをより分ける手間がかかる
  - メールでの仕事が、、、、

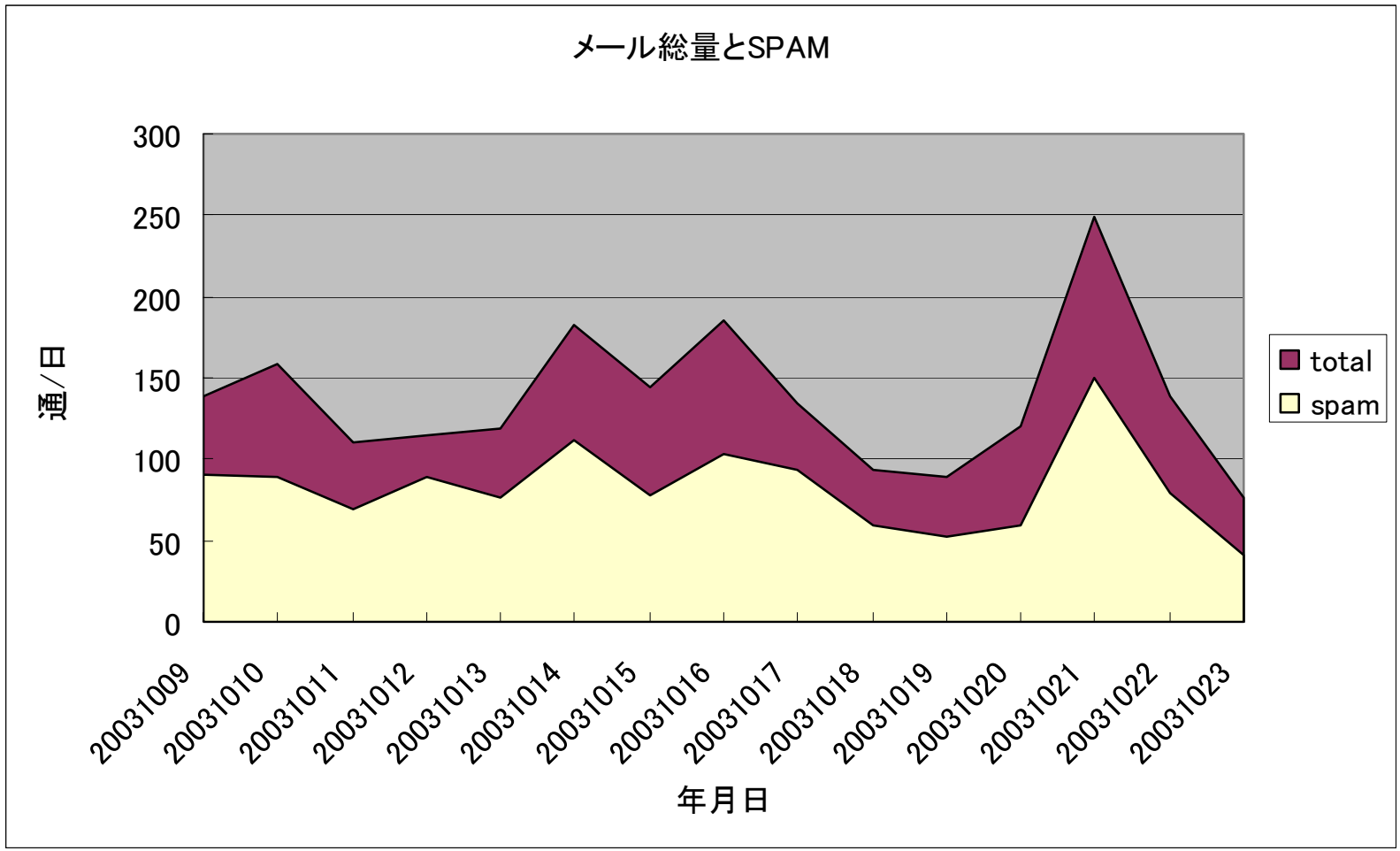
SPAM事例(無効なアドレスから)



SPAM事例(ある個人)


160
140
120
100
80
60
40
20
0
通/日
20000103
20000226
20000419
20000608
20000729
20010313
20010504
20010621
20010808
20010925
20011112
20011230
20020216
20020405
20020523
20020710
20020827
20021014
20021201
20030118
20030307
20030424
20030611
20030729
20030915
年月日

SPAM事例(ある個人、割合)



メールアドレス入手手段

- 入手先
  - WWWページ
  - ネットニュースなどの記事
  - その他
- ロボットで機械的にかき集める
- 多少間違ったアドレスや無効なものがあっても構わない
  - 10万通送って1%が反応すれば1000人、、。

SPAMの中身は？

- 「メールアドレス10万件売ります」
- アダルトサイトもの
- ドメイン名割り当てなどインターネット関連サービス安売り
- プリンタのインクなどパソコン関連
- 違法コピーソフトの売り込み
- その他(最近は中国語、韓国語が増えて読めない)

SPAMの出し方

- アドレスを何らかの手段で入手
- 普通のメールソフトでもできる
  - Bcc
- それ用のソフトもある
- SPAMを送るサービスをしている連中もいる

SPAMが届いたときは？

- 禁止事項
  - 返事を出す(ちゃんと読んでいるアドレスだと知らせるようなもの)
  - クレームを出す(送信者アドレスを偽っているものが多い)
  - 機械的にはじいてエラーメールなど返す(同上、メール流量を増やすだけ)

SPAM対策は？

- 管理者
  - 無効なアドレスのメールは中継しない
  - ブラックリストを利用してSPAM発信元サーバからのメールを受け付けない
- 利用者
  - メールソフトなどの機能を使う
    - 発信者アドレスによる振り分け
    - 最近はメール内容を統計的に処理して振り分ける手法もある (例: A Plan for SPAM)

SPAM対策は？(続き)

- 利用者(続き)
  - 一度SPAMに使われだしたアドレスには永遠にSPAMが届くといっても良い
  - メールアドレスを極力伏せるしかないのか？
- 技術者
  - SPAMをやりにくくするような新たな電子メール配送方式の開発が求められているのでは？

まとめ

- (準備不足でまとまっていませんが)
- いまやインターネットは技術者の村ではなく、圧倒的多数の一般利用者が命運を握っている
- 町の治安と同様に利用者も自覚症状や直接被害を受けなくても対策などをしっかりする必要があるだろう

おまけ

- InternetWeek2003(パシフィコ横浜、2003年12月2日から5日）
  - 12月3日のメインプログラム
  - **「Security Day～技術だけでは守れない～(仮題)」**
  - つまり、技術が問題ではないので、技術を知っている人に頼れる時代はもう終わった？

参照・引用

- 警察庁@police. Blasterワームの**DoS攻撃動作概要. http://www.cyberpolice.go.jp/server/virus/pdf/Blaster_worm.pdf**
- **InternetWeek. http://internetweek.jp/**
- **Paul Graham. A Plan for SPAM. http://www.paulgraham.com/spam.html.**
- **(WWWページ類は10月23日参照)**