スパムの現状と対策

第５回CAUA合同研究分科会

東京大学情報基盤センター
安東孝二
<ando@itc.u-tokyo.ac.jp>

self intorduction

- 安東孝二（あんどうこうじ）
- 東京大学情報基盤センター情報教育メディア部門
- 教育用計算機システム設計・管理
- メールシステム設計・管理
- 日本*Apache*ユーザ会
- インターネット協会迷惑メール対策委員m.

スパム

- spam
  - 従来の説明は省略:-)　小文字でどうぞ
  - UCE,UBEの総称からもっと大きな意味へ
    - （参考）Unsolicited Commercial/Business E-mail
  - S/N比を下げる数の暴力全般？
    - コメントスパムなど
  - 本日のテーマでは　spam≒迷惑メール

spamが来る理由

- 悪戯
  - chain mail, mail bomb
- ビジネス
  - ダイエット、バイアグラ、韓国海苔

spamが来る理由

- phishing詐欺
  - 数打ちゃ当たる方式のpassiveなもの
    - 宝くじが当たりました！
    - ナイジェリアの将軍の隠し財産がぁ！
  - 巧妙に仕組まれたtargetを絞ったもの
    - "業者がメールを開かざるを得ないようにするため、件名を「苦情」などとし「不良品だった。添付ファイルの写真を見て」と書き込んでいた。"（2005.11.10 毎日新聞）

spamのインパクト

- 管理者の視点
  - サーバの負荷とそれに伴うコスト増
  - バウンスメールなど外部への悪影響
  - 正常なメールへの影響
    - それに伴う内外ユーザからの苦情

spamのインパクト

- ユーザの視点
  - うざい
  - 大事なメールを見落とす
  - スパイウェア・フィッシングの危険
  - メールというコミュニケーション手段が崩壊？

日本の特徴

- Emailに対する厚い信頼
  - mailing listの普及
  - 携帯メールもemailと互換
  - ５秒で届くemail

日本の特徴

- Emailに対する厚すぎる信頼とanti spam教育の遅れ
  - 誤検出(false positive)、見逃し(false negative)を許さない風潮

そもそもemailとは

- RFC2822
  - 2001.4.24
  - 19年間放置されたrfc822を踏襲

そもそもemailとは

- 何時でも誰でも誰とでも
  - 基本的に郵便や電話とおなじ
- プライベートな分散システム
- 最もインターネットらしい
  - 性善説に基づく

性善説に基づくemail

- 穴がいっぱいお人好しの規格
  - 認証がない
  - DNS poisoningの危険
  - Harvestingの危険

当然の帰結

- お人好しのemailの規格と根拠のない信頼がリスクを増やす
  - spywareからの情報流出
  - メールシステムの停止と生産性の低下
  - spamやbounce mailによる企業イメージの低下

spamの現状

- 日本でも急増
  - 世界では60%がspam
    - ひどい国では80%以上
  - 携帯各社は経験済み
  - ISPでの対策は待ったなし
    - 大学はこれからか？

spamの現状

- Third Party RelayからBOT（ゾンビ）送信へ
  - スパムビジネスモデルの確立
    - アドレス収集業者
    - Cracking業者
      - Harvestingでさらに迷惑
    - Botマシンおよびクラスタ(botnet)のレンタル業者　$300/hr?

spamの現状

- Bot
  - 世界で１５万７千台のゾンビが生まれ、その２割は中国(CypherTrust社 Apr.10
  - 国内インターネットユーザの40〜50人に一人がBotになっている。そのトラフィックは10Gbpsにおよび未対策PCはネットに繋ぐと4分で感染する。(Telecom-ISAC Japan Jul. 27)

管理者のspam対策の観点

- 世の中的にspamをなくすための方策
  - Domain Keys, DKIM, SPF
- spamを出さないための方策
  - Outbound Port 25 Blocking

管理者のspam対策の観点

- spamを受け取らないための方策
  - Blocking
  - Throttling
  - Filtering

管理者のspam対策の観点

- Blocking
  - ORBL etc.
  - White/Black List
  - Gray List
  - Reputation

管理者のspam対策の観点

- Throttling
  - Greeting Pause
  - IPベースのトラフィック制御

管理者のspam対策の観点

- Filtering
  - ***Bayesian***
  - Heuristic
  - Pattern matching
  - Contents

ユーザのspam対策の観点

- アドレスを収集されない努力
- アドレスを変更（携帯系？）
- メールソフト(MUA)での対策
  - Pattern matching
  - Bayesian filtering
    - Thunderbirdなど

身近な対策

- Greeting Pause, Gray Listing
- Secondary MXの再考
  - Local Recipient Check?
- Reachabilityのないバウンスメールの配送経路を分ける
  - fallbackをうまく利用する

商用製品

- （たとえば）Mirapoint社Razorgate
  - ウイルス対策よりは安い
  - 楽をしたければRapid AntiSpam（reputation系）

spam対策総括

- コスト増大・対策必須
- 少なくとも第三者に迷惑を掛けない
- フリーソフトでの限界
- 出来るところからこつこつと