# 迷惑メール対策を中心としたメールシステム構築 闘う ISP 編

株式会社インターネットイニシアティブ
プロダクト推進部
近藤学

IIJ
Internet Initiative Japan

Copyright © 2004, Internet Initiative Japan Inc,

## Agenda



- Abuse message に関する現状
- 業界動向
- spam 技術動向
- ISP としての取り組み
- Abuse message 対策を考えたメールシステム



Copyright © 2004, Internet Initiative Japan Inc,

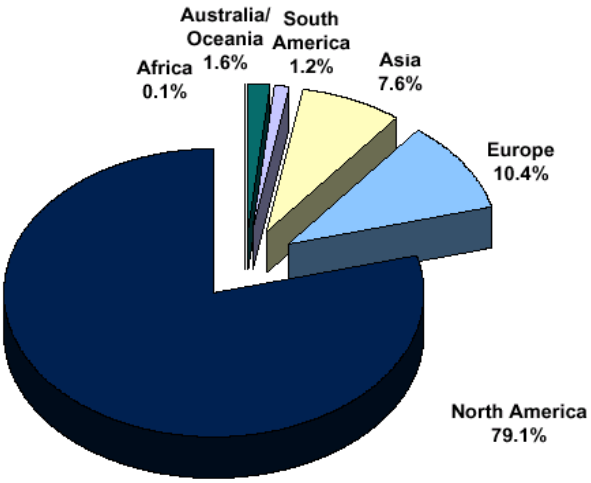
# Abuse message に関する現状

IIJ
Internet Initiative Japan

Copyright © 2004, Internet Initiative Japan Inc,

# Primarily North American Problem – TODAY






- Spam appears to be a primarily North American problem to-date
- Claimed country of origin is 80% North America
- Growth accelerating from CHINA and EASTERN EUROPE as sources of hybrid spam/virus threats

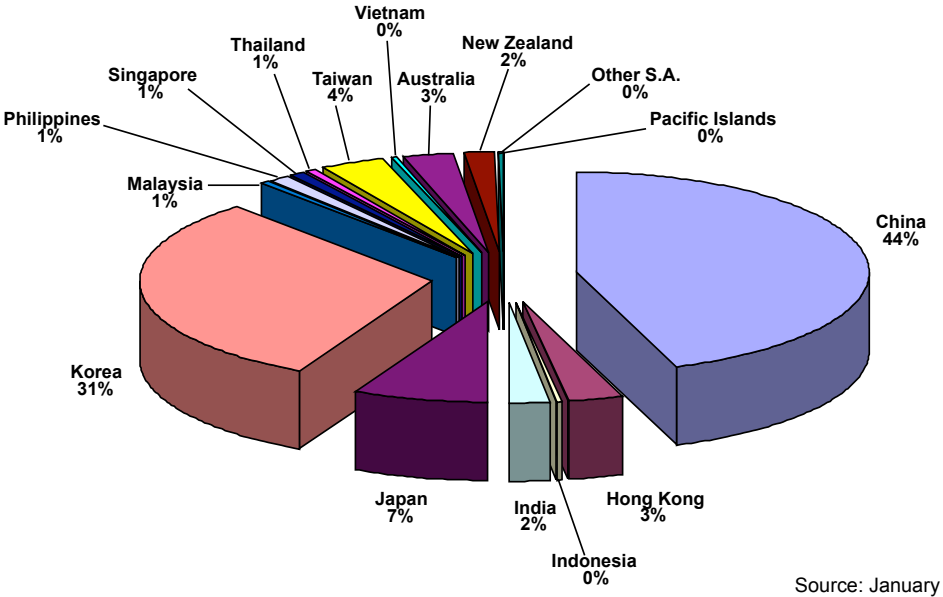
Source: January 2004
As measured by Probe Network

IIJ
Internet Initiative Japan

Copyright © 2004, Internet Initiative Japan Inc,

# Spam and Abuse Originating From APAC






Source: January 2004
As measured by Probe Network

IIJ
Internet Initiative Japan

Copyright © 2004, Internet Initiative Japan Inc,

# Worldwide な現状



- 死活問題
  - 事実上 email が使えないくらいの spam 量
  - ISP/キャリア側の対応コストは増大する一方
- 現状，我々はほとんど「負け」ている
  - 受け身であるし，後手後手に回っている
- 個別にやっても勝ち目は薄い
  - 「出されてしまった側」「送りつけられた側」の両方で取り組まないといけない
  - Trusted and Clean SMTP network

IIJ
Internet Initiative Japan

Copyright © 2004, Internet Initiative Japan Inc,

## Worldwide な現状 (cont.)



- Outbound Port25 blocking
  - 動的 IP address から外向けに port25 で出て行けないようにする
    - すべての email は ISP の MTA 経由に
  - US では一般的な手法になりつつある
  - 似たような手として，受け取り側で動的 IP address 群からの SMTP connect を refuse するという手を使っているところもある
  - Q1: これをやると困る人，いますか?
  - Q2: これをやると問題だと考える人，いますか?

IIJ Internet Initiative Japan
Copyright © 2004, Internet Initiative Japan Inc,

## 日本の現状

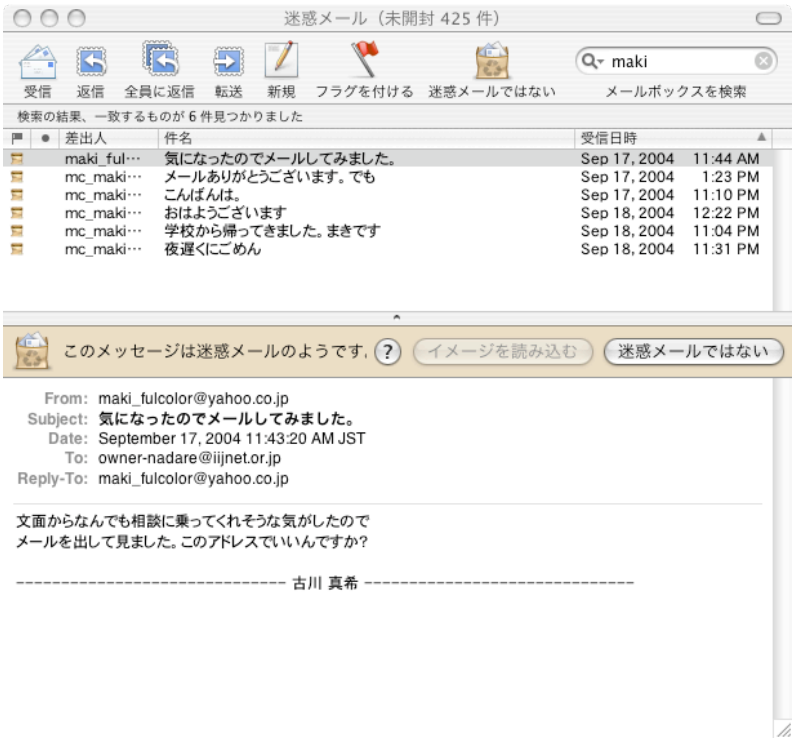


- FLET'S 契約して打ち逃げ
  - ISP を渡り歩く
  - 初期費用かからないし FLET'S も引いちゃえばあとは楽だし
- Zombie クラスタからの攻撃やツールによる大規模な spam ばらまき
  - spam を打たれるだけではなく，大量の spam の結果としてのエラーメール戻り先として利用されるケースも多い
  - この夏あたりからかなり酷くなってきた
- ハーベスティング(アドレス収集)も活発
- Social Engineering 的 spam

IIJ Internet Initiative Japan
Copyright © 2004, Internet Initiative Japan Inc,

# Social Engineering というかなんというか...

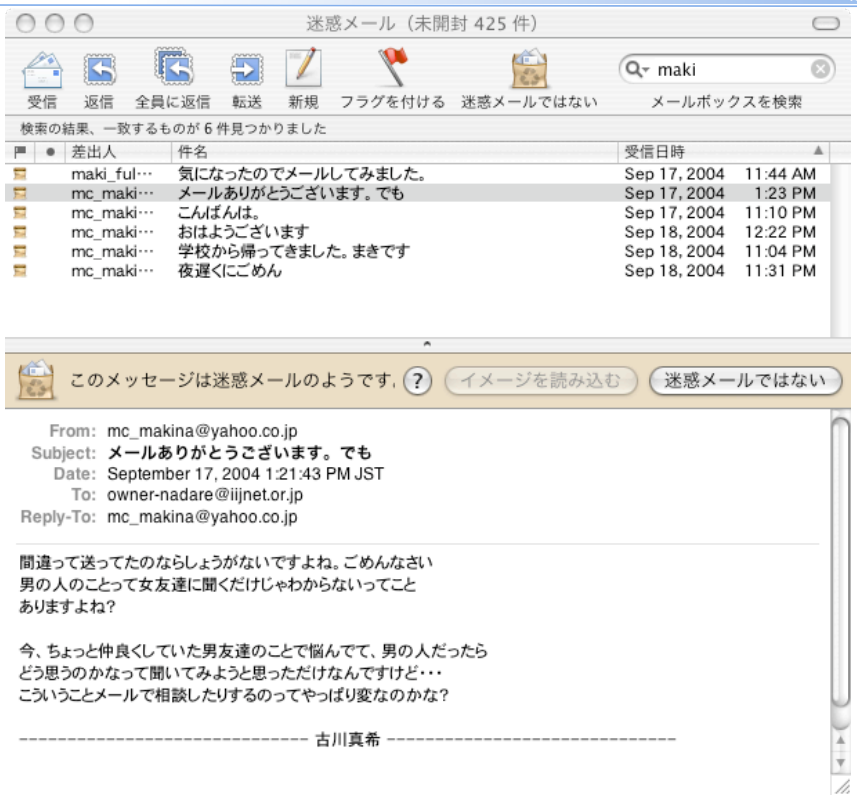





Copyright © 2004, Internet Initiative Japan Inc,

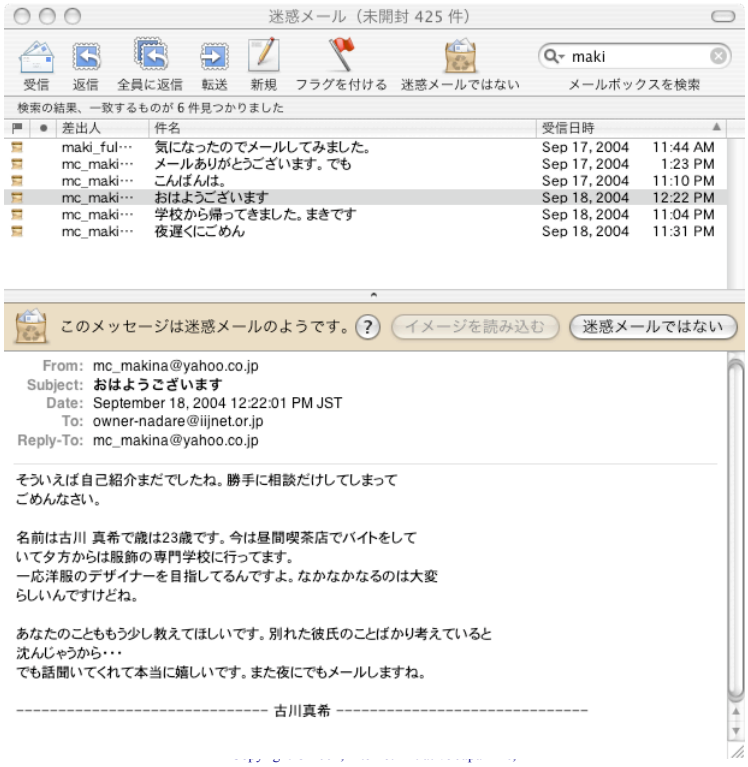
# さらに...





# さらにさらに...






# こういうのって...



- ひっかけるまでのメール(の本文)には違法性がない
- なので取っ捕まえにくい
- あまりに普通の文章だし，phishing のように URL signature などから判定することも難しい
  - antispam filter でひっかけにくい
- きっとひっかかる人は結構いるだろうなあ... (^^;

Copyright © 2004, Internet Initiative Japan Inc,

# 日本の現状(cont.)



- エンドユーザレベルでは個人差が大きい
  - Spam Divide
  - 来る人はいっぱいくる(数百通/日)けど，来ない人は来ない(ほとんど 0)
  - Q: 個人，あるいは管理している mailbox へくる spam の量をざっくりでいいのでパーセンテージで教えてください
- ISP レベルでは…まだなんとかなっているかも
  - 確かに酷くなってきている
  - でも生き死にというほどではない
- しかし，早かれ遅かれ酷い状況になっていくのは明らか

IIJ
Internet Initiative Japan

Copyright © 2004, Internet Initiative Japan Inc,



# 業界動向

IIJ
Internet Initiative Japan

Copyright © 2004, Internet Initiative Japan Inc,

# 最近の動き



- Sender ID などに代表される新しい技術スキーム
- 業界団体
  - MAAWG (Messaging AntiAbuse WG)
  - Anti Phishing Working Group
  - AMY(AOL, MSN, Yahoo)
  - 迷惑メール対策研究会
  - MAAWG-J (仮称: 名称は近々変更予定)
  - OECD antispam workshop
- 法制度
  - CAN-SPAM Act
  - ITPEA (Identity Theft Penalty Enhancement Act)

IIJ Internet Initiative Japan

Copyright © 2004, Internet Initiative Japan Inc,

# MAAWG 発足



- MAAWG (Messaging AntiAbuse Working Group) 立ち上げ (2004 年 1 月 14 日 press release)
- Abranet, Adelphia, Bell Canada, BellSouth, Cox, IIJ, IIJ America, NII Holdings Inc., NTL, TELUS, Openwave Systems Inc, 他 9 社が Founder として立ち上げ
- 2004 年 6 月より NPO として活動中
- 現在の参加メンバは,
  Bell South, EarthLink, Verizon Online, Bell Canada, Charter Communications, Cloudmark, Cox Communications, Goodmail Systems, IIJ, Openwave, TDS, AOL, France Telecom, MX Logic

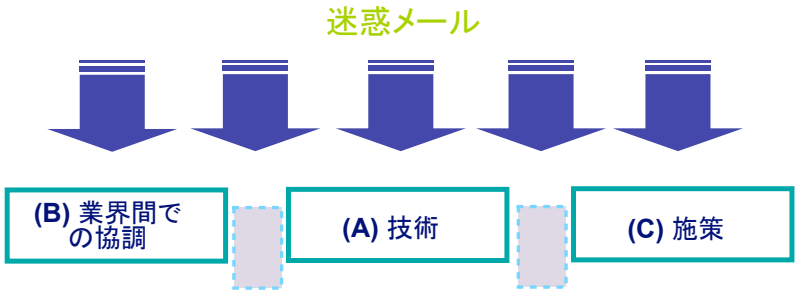
IIJ Internet Initiative Japan

Copyright © 2004, Internet Initiative Japan Inc,

# MAAWG の活動 (I)



- 作業グループ毎に活動
  - 協調の枠組み (Collaboration)
    - Code Of Conduct
  - 技術(Technology)
    - Sender Authentication Protocol の適用, テスト
  - 施策 (Policy)
    - Policy maker, 政府機関との連携
- 技術だけではなく複合的に検討




Copyright © 2004, Internet Initiative Japan Inc,

# MAAWG での活動(II)



- Code Of Conduct
  - ISP/ASP が成すべき規範をまとめたもの
  - 遵守するのが望ましいが, 強制するものではない
  - Objectives:

    a. Establish principles for responsibly operating a messaging service taking into account the ramifications for messaging as a tool, the Internet messaging community, and the Internet at large, of failing to responsibly operate such services;
    b. Establish a framework for communication between messaging operators in which new strategies, technologies, and standards for combating abuse can be discussed, developed, and deployed;
    c. Facilitate communication among operators to ensure that all parties to an abuse issue are aware of the issue, aware of plans to rectify the issue, and if possible agree on the best course of action;
    d. Serve as an instrument of reference to help operators clarify the rationale for actions taken to reduce abuse, and aid those against whom action has been taken in rectifying practices that lead to abusive behavior;
    e. Promote Internet messaging as a useful and positive tool by eliminating negative and abusive uses of the medium.

Copyright © 2004, Internet Initiative Japan Inc,

# MAAWG での活動(III)



- Technology Sub-Group
  - Reference Architecture の策定
  - 送信者認証技術をどう apply していくか
    - ISP としてのいろいろ(タイミングとかポリシとかカスタマーサポートとか)
    - ISP のスケールで果たしてちゃんと動くかどうか

Copyright © 2004, Internet Initiative Japan Inc,

# MAAWG での活動(IV)



- Policy Maker (政府組織など)との連携，協調
  - 技術ややる気だけあっても work しない
  - 政府もしくは法律の後ろ盾が必要な場面は往々にしてある

Copyright © 2004, Internet Initiative Japan Inc,

# 日本での活動



- MAAWG-J(仮称:近々名称変更予定)として，十数社の ISP やベンダで活動を開始
  - 月例会実施中
- テーマ(現在進行中のもの)
  - Sender-ID の実証実験/情報共有
  - 動的 IP address からの SMTP をどう取り扱うか
  - ISP 間での情報共有のあり方
- MAAWG との橋渡し
  - 日本の要望，事情を MAAWG に反映
  - MAAWG の活動を報告
- 日本独自の問題を検討し，対策を考え，協調する枠組みをつくることを目標
  - ISP の運用管理担当者に限定
  - 具体的な形で実現することが目的

IIJ Internet Initiative Japan
Copyright © 2004, Internet Initiative Japan Inc,

# 日本での活動 (cont.)



- 迷惑メール対策に関する技術交流会
  - 9/16 at IIJ office
  - ISP/ASP 等のメール運用に関わる方を中心に
  - 130 名以上 (70 組織以上) の参加
  - ML 作っていろいろ議論やってます
- JAIPA さん
- IAJapan さん
- 迷惑メール対策研究会 (総務省)

IIJ Internet Initiative Japan
Copyright © 2004, Internet Initiative Japan Inc,

# spam 技術動向

IIJ
Internet Initiative Japan

Copyright © 2004, Internet Initiative Japan Inc,

## 最近の迷惑メールの実態



- Virus/Worm
  - 「亜種」問題
  - DoS 機能付き
- spam
  - From 詐称
  - Worm + spam
- Phishing
  - 日本上陸



Copyright © 2004, Internet Initiative Japan Inc,

# Virus/Worm



- 「亜種」問題
  - パターンファイル更新が頻繁
  - パターンファイル更新前に Outbreak!!
- Massmail 型
  - 自身が SMTP 喋って大量のメールを送信する
  - 自社/他社メールシステムへの影響大
- DoS/DDoS 型
  - 特定 Site を攻撃するタイプ (Antinny とか)

IIJ
Internet Initiative Japan

Copyright © 2004, Internet Initiative Japan Inc,

# spam



- 「変なメールがくるんだけど…」という話ではなくなってきている
- From: 詐称
  - 対応コスト(人的)大 -> 本来発生する必要のないコスト
  - 対外的な reputation/イメージの悪化
  - メールシステムに対する DoS 的インパクト
    - 存在しない From を詐称されて spam を打たれる
      -> User Unknown 多発
      -> 自組織メールシステムへのエラーリターンが大量発生

IIJ
Internet Initiative Japan

Copyright © 2004, Internet Initiative Japan Inc,

## spam (cont.)



- Worm 作者(業者)と spam 業者とのコラボレーション
  - いわゆるゾンビクラスタモデルの発展
  - 最近あちこちの ISP でもゾンビクラスタからの spam を大量に受け始めている
- ビジネスモデルとしては，確かにそのとおり
  - 力のある配信技術(Worm)の上にコンテンツ(spam)を載せる
- spam の出し元が一般の PC になってしまう
  - IP address base での Blacklisting が無意味になる
  - 組織内からも spam が出る可能性がある

Copyright © 2004, Internet Initiative Japan Inc,

## Phishing

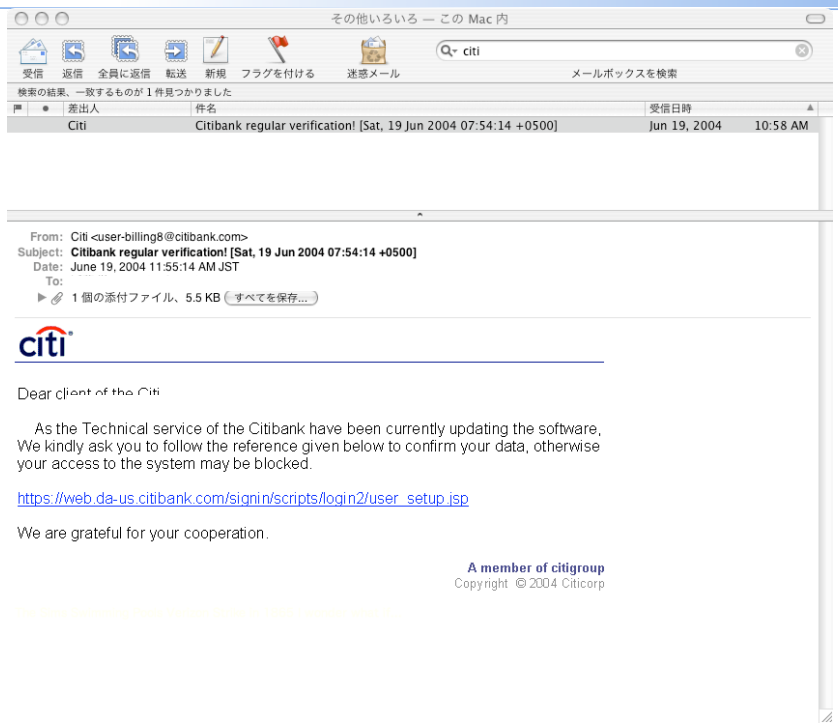


- 例えばオンラインバンキングなどの Site を偽装し，そこへユーザを誘導，アカウントやパスワードを入力させて盗み取る
- 誘導させるための「撒き餌」としてメールが使われる
- ヘッダ，内容とも巧妙に偽装され，一般のユーザにはまず見抜けない

Copyright © 2004, Internet Initiative Japan Inc,

# Phishing メールの例

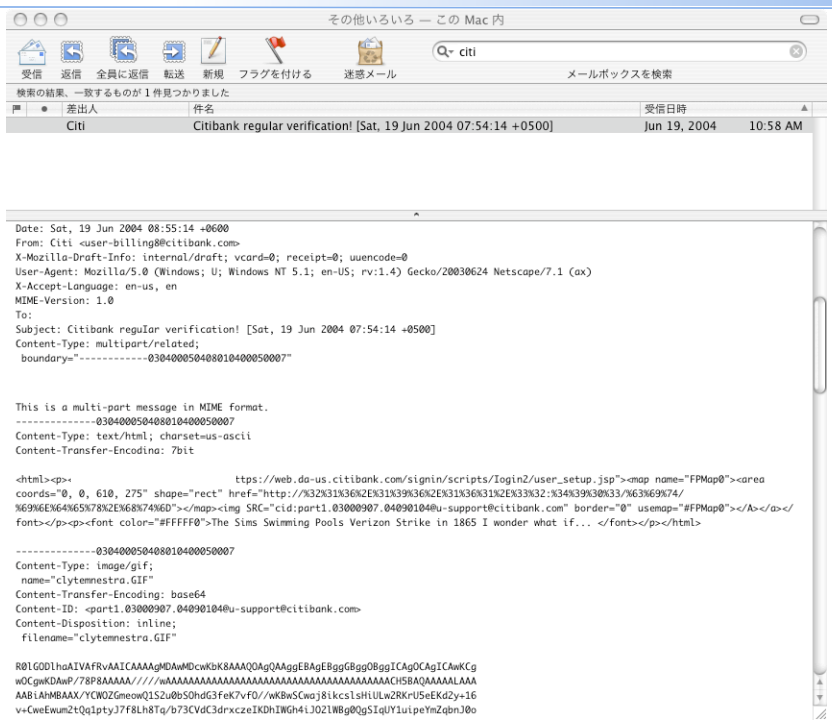





Copyright © 2004, Internet Initiative Japan Inc,

# Phishing メールの例 (cont.)






Copyright © 2004, Internet Initiative Japan Inc,

## Counter Measures



- 送信者認証技術(Sender Authentication Protocol)の導入
- Antispam filter の導入
- 業界全体での対応
- エンドユーザの教育/啓蒙

IIJ
Internet Initiative Japan

Copyright © 2004, Internet Initiative Japan Inc,

## 送信者認証技術



- 「誰が出したのか?」+「どこから出たのか?」
- Sender ID
  - SPF + Caller-ID(Microsoft)
  - SMTP の拡張 + DNS
- DomainKeys
  - Gmail が採用
  - ISP としては...今の段階ではちょっと難しいかも

IIJ
Internet Initiative Japan

Copyright © 2004, Internet Initiative Japan Inc,

# Antispam filter



- spam の多様化，高度化に追従できるものを
  - 単一の判定エンジンのみだと厳しくなってくる
- 誤認識率 (false-positive rate) の低いものを
  - 種々の判定基準を総合して判断することが必要
- Outbreak 対応力
  - Worm を spam として防ぐ
  - 発症 (Outbreak) から治療薬(パターンファイル)登場までの間を出来るだけケアしたい

IIJ Internet Initiative Japan

Copyright © 2004, Internet Initiative Japan Inc,

# spam の進化



```
<p>G<!--12d0213ogwc-->et Vi<!--4d70jt3plvk-->a<!--doflso30s8-->gra o<!--
   arnjfh2xn480sm-->nline N<!--xbicry2ek79ir3-->ow <!--un40nv29u4lz-->!
   <br>

  <br>

  W<!--ztzz1n1pdkqs7n-->e ar<!--945nx822vi0-->e th<!--72lydb3nybe-->e
   che<!--xejikmr3c3d-->ape<!--fvh7nt3pr5htm-->st sup<!--jr7qf83rmvk58--
   >plier o<!--83fl612dx6e-->n <!--fr1dg53a9e9-->the n<!--1nzphb1rgle--
   >et <br>

  10<!--azeauv3xsnh-->0 <!--6cbmwg28ij945-->% g<!--tuy4v313lijzs--
   >uarant<!--vq6i8g3f31e2w1-->ee !<br>

  a<!--2aso8s0m8kakl-->t 3 <!--og334s3bm0dfy1-->$ a<!--z52dpv3ph7t63-->
   do<!--04wgbd1e1dbz7-->se, tr<!--1rlwme3gan4-->y i<!--w5edo32alv6row--
   >t no<!--tfv8du3vb9tu-->w. <a href="http://www.meds4yourlife.biz/
   index.php?id=9999">C<!--itnmq02gxs-->lic<!--jtcolj3tg5zfb-->k

  he<!--g6f84l2drh-->re</a></p>

<br><br><br><br><br>
```

IIJ Internet Initiative Japan

Copyright © 2004, Internet Initiative Japan Inc,

# spam の進化(cont.)




Copyright © 2004, Internet Initiative Japan Inc,

# Anti-Spam Classification Framework

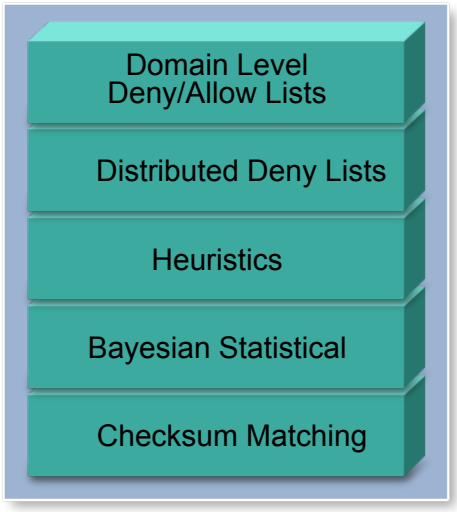


- 最も効果のある5種類のスパムフィルタとスパム可能性スコアのダイナミックな集約と解析
- 分類テクニックと方法の集約:

  より正確で効果的な分類スキームを提供

  - 各Classifierでは確信的な要因とともに “committee chairman” に投票
  - 結果は単一の見込みフレームワークに変換される
- 傾向分析:各Classifierの有効性を測定

MX Logic's Stacked Classification Framework℠




Copyright © 2004, Internet Initiative Japan Inc,

# ユーザ教育/啓蒙



- 状況は，数年前の Virus に対するそれと同じ
  - 「なんでもかんでもクリックするんじゃない!!」 :-)
- 特に対 Phishing という観点からは重要
  - 今のところ日本語の phishing はあまり出てないけど，出たらひっかかる人，多数な気がする
- 業界団体が一体となって取り組んでもいいのでは?
  - マテリアル
  - セミナー
  - デモサイト(って有効?)

IIJ
Internet Initiative Japan

Copyright © 2004, Internet Initiative Japan Inc,



# ISP としての取り組み

IIJ
Internet Initiative Japan

Copyright © 2004, Internet Initiative Japan Inc,

# 現状



- 受け取り手からの苦情 driven
- 先手を打って押さえることは事実上できない
  - 「通信の秘密」
- 打ち逃げ対策
  - 事実上なし
  - やはり後手(打っている途中 or 打ったあとでの対応)
  - 強制解約者情報などを ISP 間で共有できれば「渡り」を押さえられるのに...
    - 現状不可 (個人情報保護)
- SPF check? Reputation?
  - ISP が顧客の通信を ISP の判断で遮断してもいいのか?
  - 役務提供義務との関係は?

IIJ
Internet Initiative Japan

Copyright © 2004, Internet Initiative Japan Inc,

# 対策(や希望，願望等)



- 法的お墨付き or バックアップ
  - 通秘に対する特例みたいな扱いとか?
  - 違法性判定?
- SPF や Sender ID，Reputation などを組み合わせてチェック
  - できるだけ水際で弾きたい
  - でもエンドユーザに理解してもらえるだろうか?
  - 役務提供義務との関係もクリアにしたい
- 情報交換/協調したアクション
  - やはり spammer の情報は交換したい
  - 第三者機関?
  - 五月雨的にアクションをとるのではなく，一斉にアプローチした方がいいかも

IIJ
Internet Initiative Japan

Copyright © 2004, Internet Initiative Japan Inc,

# 対策 (cont.)



- Outbound Port25 Blocking
  - ISP の MTA を経由した spam って少ない
  - ISP の MTA を通っているから対応しやすい
  - MSA をおいてそこで SMTP Auth 必須にするとか
  - 大半のユーザは ISP が提供しているメールサーバを利用している
  - となると動的 IP から出てくるメールってほとんどが spam か Virus/Worm ではないだろうか?
    - もちろんそうじゃないケースがあることは承知してます

IIJ
Internet Initiative Japan

Copyright © 2004, Internet Initiative Japan Inc,



# Abuse message 対策を考えたメールシステム

IIJ
Internet Initiative Japan

Copyright © 2004, Internet Initiative Japan Inc,

# ISP におけるメールシステムの原則(その 1)



- エンドユーザの mailbox へ配送すべきメールはすべて受け付けなくてはならない
  - 役務提供義務
  - なので RBL とかは使えない
  - でも，約款や規約で握れてれば自由度はあがる
  - 今後は自由度をあげた対応が必要になってくるだろう
    - 逆引きブロックとか SPF check とか Reputation check とか

IIJ
Internet Initiative Japan

Copyright © 2004, Internet Initiative Japan Inc,

# 原則(その 1) を実現する為に...



- キャパシティプランニング
  - Connection 数
  - queue の設計
  - fallback の設計
- バースト的な Inbound Traffic への対応
  - ぶっちゃけた話，キャパシティを越えちゃうようなバーストはやってくる
  - どう捌くかが運用チームの腕の見せ所
  - Connection Rate や queue の調整，fallback 系を自由度高く使えるような設計と運用のコンビネーション
  - これって，大量高速配信用 MTA 群の設計と一緒だよね

IIJ
Internet Initiative Japan

Copyright © 2004, Internet Initiative Japan Inc,

# ISP におけるメールシステムの原則(その 2)



- 遅延は許されない
  - 10 年前ならいざしらず，現在は「メールは遅延する可能性がある」なんて理解されない
  - メールがビジネスのインフラストラクチャとして使われている以上，遅延がある状況というのはトラブルが発生していることと同義
  - なので，こと ISP においては Graylisting のような手法はなかなか使えない

IIJ
Internet Initiative Japan

Copyright © 2004, Internet Initiative Japan Inc,

# 原則(その 2)を実現する為に...



- パフォーマンス向上という観点だと原則(その 1)と一緒
- 特に queue control と fallback がポイント
- 優先度付け
- Outbound 方向での遅延対策には専用 Outbound MTA を
  - retry でメールがいっぱい溜まってる queue があると I/O で他が引きずられる
  - ここでも queue control や queue flush に知恵と工夫が必要
  - よく遅延する相手先の洗い出しや挙動観察も有効

IIJ
Internet Initiative Japan

Copyright © 2004, Internet Initiative Japan Inc,

# 今後必要になってくるであろう要素



- Inbound
  - SPF なりなんなりの大きな篩
  - 自由度の高い rate control/queue control メカニズム
  - システムワイドでの Body scan 系 antispam filter
  - エンドユーザレベルでの filtering (allow/deny)
- Outbound
  - SMTP Auth 必須
  - MSA も必須
  - Body scan 系 antispam filter (zombie cluster 対応)
  - 自由度の高い rate control/queue control メカニズム
  - Port25 blocking

IIJ
Internet Initiative Japan

Copyright © 2004, Internet Initiative Japan Inc,