IIJ
Internet Initiative Japan

Ongoing Innovation

Internet Initiative Japan Inc.

迷惑メールの現状とその対策

~第2回迷惑メールへの対応の在り方に関する研究会~

2007.8.22

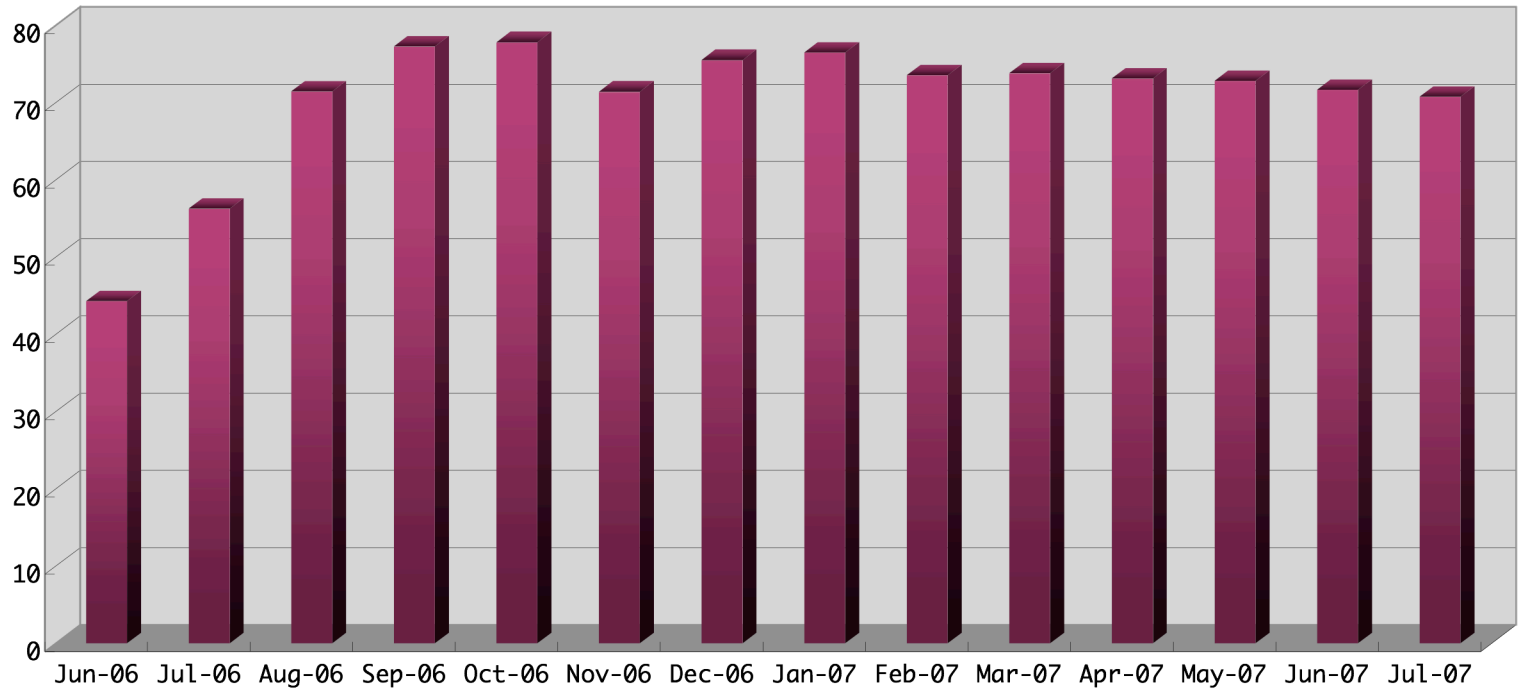
櫻庭 秀次

株式会社インターネットイニシアティブ

Copyright © 2007 Internet Initiative Japan Inc.

迷惑メールの現状 - I

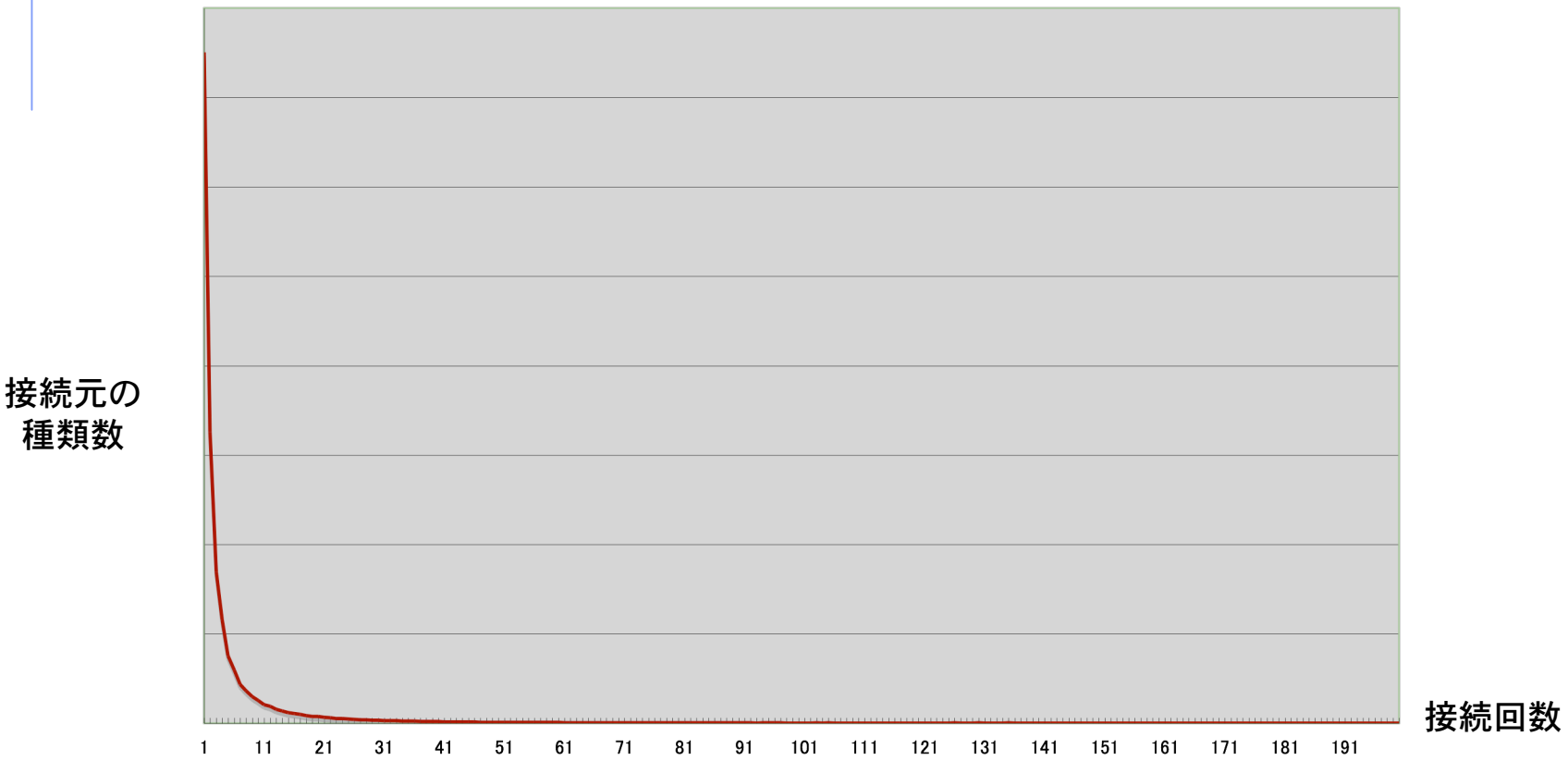
- 迷惑メールフィルタによる検知率の推移
  - 2006年夏以降急増し高水準を維持
  - 総受信量は現在も増加傾向
  - 現在は迷惑メールフィルタ以外の手法を併用し総合的に対処



Copyright © 2007 Internet Initiative Japan Inc.

迷惑メールの現状 - II

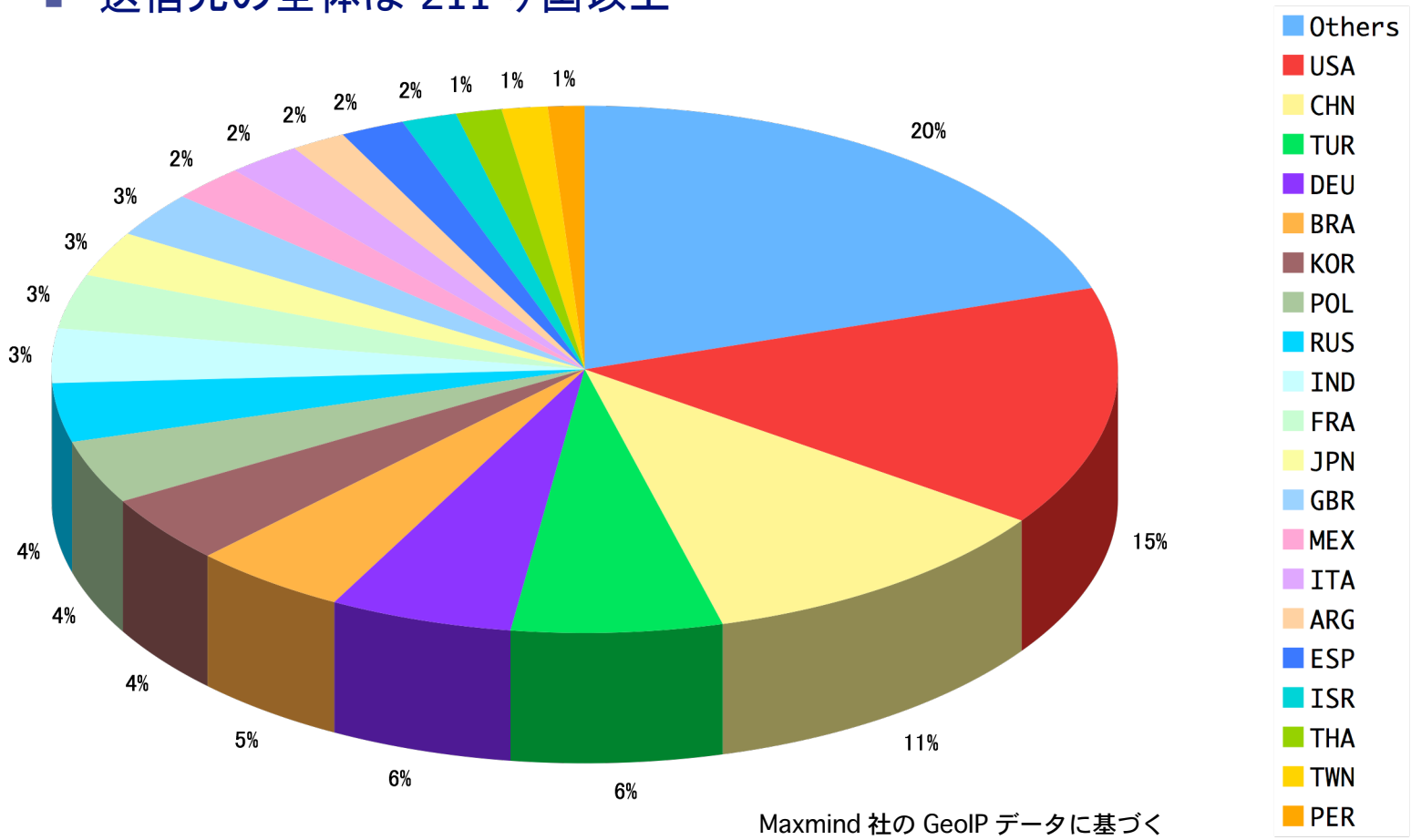
- 送信元の特徴
  - 同一送信元 (IP address) からはごく少数の mail しか送信しない
  - 大量送信をしている送信元も迷惑メールの場合が多い (二極化傾向)



Copyright © 2007 Internet Initiative Japan Inc.

迷惑メールの現状 - III

- 送信数が 10 以下の送信元の国別割合
  - 送信元の全体は 211 ヶ国以上



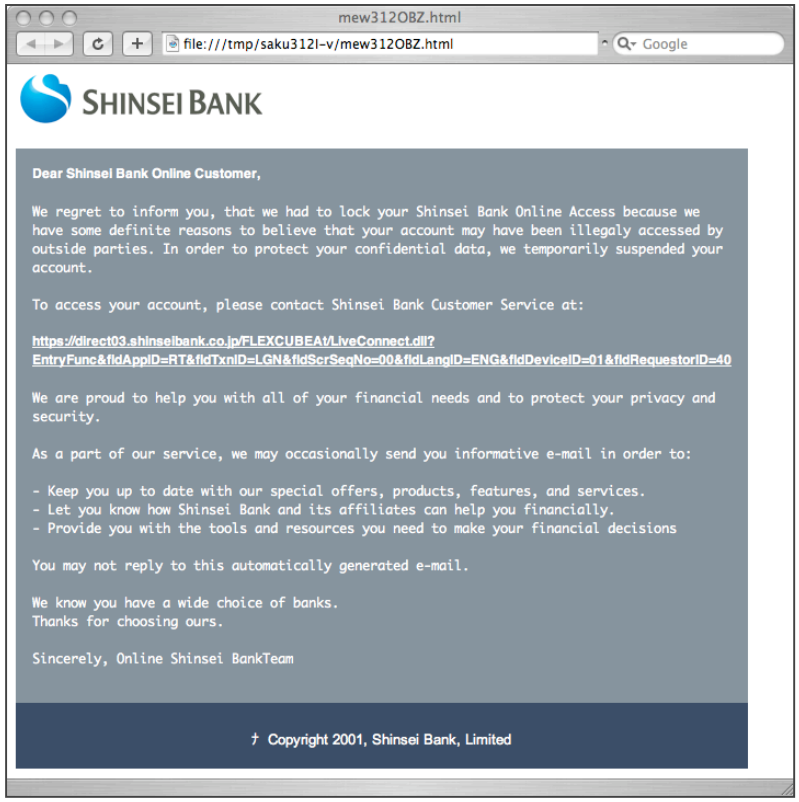
Maxmind 社の GeoIP データに基づく

Copyright © 2007 Internet Initiative Japan Inc.

フィッシングの実例 - I

- 新生銀行を騙るフィッシングが広範囲に出回る
  - 2007.07.11-12 と 2007.07.25 の二度 (HTML 形式)
  - 手口としては 2005 年の UFJ 銀行 (当時) と同様に単純ではあるが大規模に送信
  - グローバルな環境を利用

- メールの実態
  - ヘッダ From は以下のいずれか
    security@shinseibank.co.jp
    support@shinseibank.co.jp
    no_reply@shinseibank.co.jp
  - envelope From は多様
    - 把握しているだけで 21種類
    - 送信元は 10ヶ国 (フランス, ブラジル, マレーシア, トルコ, 米国, 中国, ドイツ, 英国, ギリシャ, インド)



Copyright © 2007 Internet Initiative Japan Inc.

フィッシングの実例 - II

- フィッシングサイト
  - 入力画面は本物の英語版とほぼ同じ
  - 把握しているだけで 22 種類 (2回目がより広範囲)

Copyright © 2007 Internet Initiative Japan Inc.

Botnet について

- 前置き
  - 提供サービスの性質上 bot (zombie PC) 及び botnet (zombie cluster) の存在確認は一般に難しい
  - OP25B (Outbound Port 25 Blocking) の導入により，メール送信者としての spam に関するクレームが少なくなったため，自社の顧客が bot 化されているかを把握することが難しくなっている
  - しかしながら OP25B で実際に drop している packet 数は多く，bot 感染者が存在している可能性は高いと思われる
  - 現段階では状況証拠的に botnet の存在を推測

- Botnet の脅威
  - 広範囲に分散する botnet を利用すれば，spam 送信のみならず，DDoS 攻撃，phishing site の構築 (DNS, Web, etc)，新たな犠牲者の獲得，内部情報 (各種 ID, パスワード等) の取得などが可能
  - Bot の制御手法や発見回避手法といった技術革新が早く，social engineering 的手法等感染させるための手段も巧妙化している

Copyright © 2007 Internet Initiative Japan Inc.

Botnet の実例 - I

- 概要
  - 小規模な法人顧客が対象となった例
  - 少なくとも 2006年夏頃から大量に宛先不明のメールを受信
  - Botnet (推測) 以外にも踏み台 (国内の ASP 業者) も利用
  - 顧客と調整し，幾つかの対策を順次実施，現在も攻撃は継続中

- 経緯
  - 2006.11 法人向けメールサービスの監視で異常を検知
  - 宛先不明メールの大量受信とそれに伴うエラーメール(bounce mail)の生成処理で高負荷状態
  - 顧客と相談し入り口で存在する mail address 以外は受け付けない処理 (white list) を設定 → bounce mail 生成負荷の抑制
  - その後も段階的に対策を実施

Copyright © 2007 Internet Initiative Japan Inc.

Botnet の実例 - II

- 概要
  - 送信元は 150ヶ国以上に分布 (CHN, USA, ITA, POL, DEU, KOR, RUS, ..etc)

(1) User Unknown (宛先不明) 率
(2) 送信元 Unique IP address 数
(3) (2) のうち1通しか送信しないものの割合
(4) (2) のうち5通以下の割合

発生日時	(1)	(2)	(3)	(4)
2006.12.25	99.70%	44,726	55.9%	86.4%
2007.01.11	99.93%	38,176	42.6%	65.0%
2007.01.30	99.84%	35,404	47.2%	83.3%

  - 連続する 2日で 1通のみの送信元の重複率は 2.8%，全送信元でも 5.8% → 単純な black list では対処できない

Copyright © 2007 Internet Initiative Japan Inc.

迷惑メールの対策技術

- 既存の対策技術の弱体化
  - Botnet の利用などによる送信技術の高度化により単純な Black/Block List, throttling, graylisting では効果が得られにくくなっている
  - コンテンツフィルタを回避するため pump-and-dump に代表される画像 spam や PDF spam が急増している
  - 制限を強めればメールの不達や配送遅延等の問題が発生

- 今後の対策
  - 送信側と受信側相互の協力が必要不可欠
  - OP25B (Outbound Port 25 Blocking) は迷惑メールを送信しないために接続業者はまず導入すべき
  - メールサーバを介した送信を抑制するための SMTP-AUTH による送信者確認および通数制限 (必要に応じて)
  - まず送信元情報を詐称できなくする送信ドメイン認証技術の導入が必要不可欠，その後送信者情報に基づいて判断を

Copyright © 2007 Internet Initiative Japan Inc.

国際的な取り組み - I

- 国際協調の必要性
  - 国内発の迷惑メールは OP25B などの導入により大幅に減少
  - 現在受信している迷惑メールの大部分は国外発
  - 迷惑メールの受信側は被害を把握できるが送信側は問題を認識していない場合が多い
  - インターネット環境が整備されるに従い迷惑メールの送信数が増加する傾向 (欧米 → 南米，中国，東南アジア, etc) → 早い段階で対処を
  - フィッシング等による犠牲者を増やさないためには web site の早期閉鎖が必要不可欠 → ほとんどが国外に開設
- 日本としてできること
  - 問題認識の共有 (お互いが被害であり加害者でもある)
  - OP25B, 送信ドメイン認証など送信側で対処できる技術の普及
  - 問題が発生した場合の迅速な対応のためのネットワークの構築

Copyright © 2007 Internet Initiative Japan Inc.

国際的な取り組み - II

- 迷惑メール対策に関わる国際的組織
  - MAAWG (Messaging Anti-Abuse Working Group): 欧米の主要な通信事業社，ISPs，ベンダ等 114社から構成され，日本からは唯一 IIJ が創設から参画しメンバとなっている
  - IETF (The Internet Engineering Task Force): 送信ドメイン認証技術 (SPF, DKIM) などインターネット上の技術標準の検討を行っている
  - ITU Partnerships for Global Cybersecurity: WSIS (world summit on the information society) Action Line C5 に対応した ITU 内の活動
  - OECD Task Force on Spam: spam 問題に対処するための政策等について提言する Anti-Spam Toolkit を作成
  - APCAUCE (Asia Pacific Coalition Against Unsolicited Commercial Email): 1回/年程度状況を報告し合う meeting を開催
  - StopSpamAlliance: ITU, OECD, APEC TEL, CNSA, LAP, Seoul-Melbourne MoU それぞれの情報共有のための portal site
  - IGF (Internet Governance Forum): WSIS の Tunis Agenda for the information society を受けて作られた forum, spam 問題も主要テーマの一つ

Copyright © 2007 Internet Initiative Japan Inc.