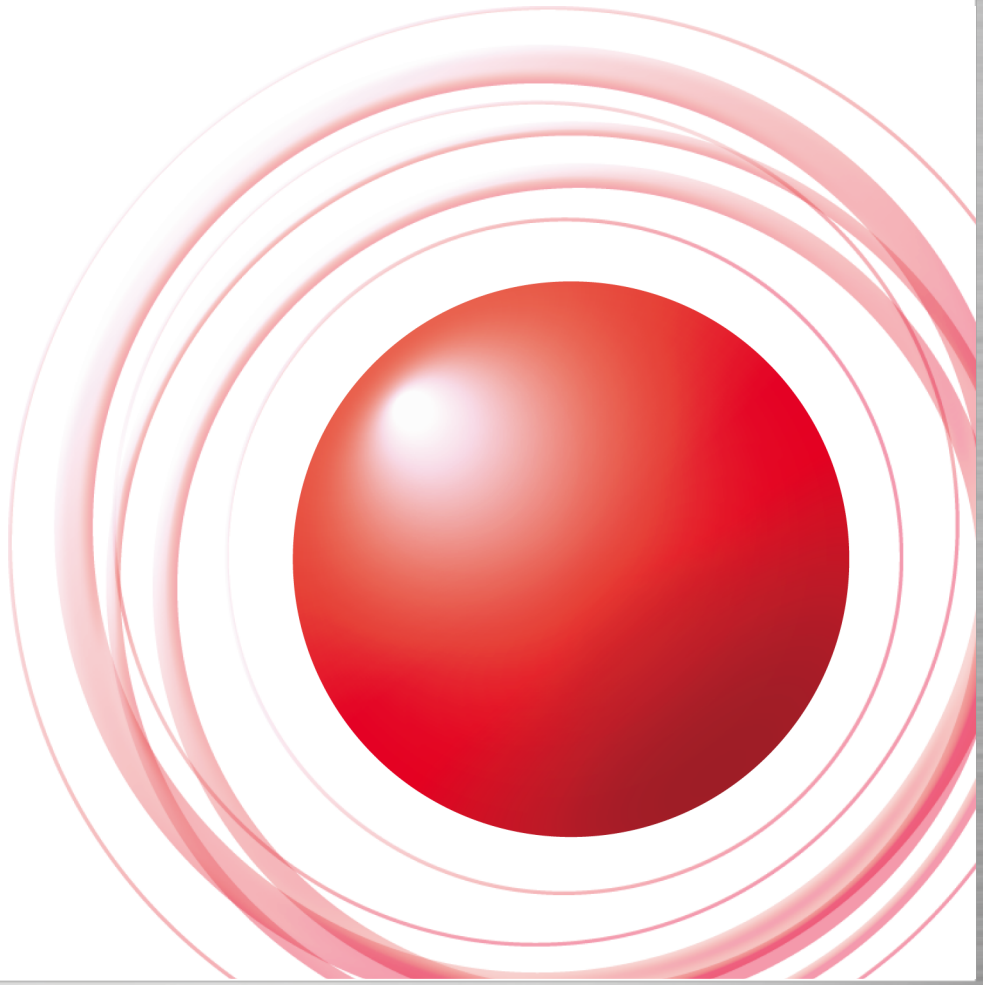
資料２－１

利用者視点を踏まえたICTサービスに係る諸問題に関する研究会
迷惑メールへの対応の在り方に関する検討WG（第5回会合）

迷惑メールに対する技術的対策

IIJ Internet Initiative Japan



2011.01.25

株式会社インターネットイニシアティブ
櫻庭秀次（SAKURABA Shuji）

Ongoing Innovation

Agenda

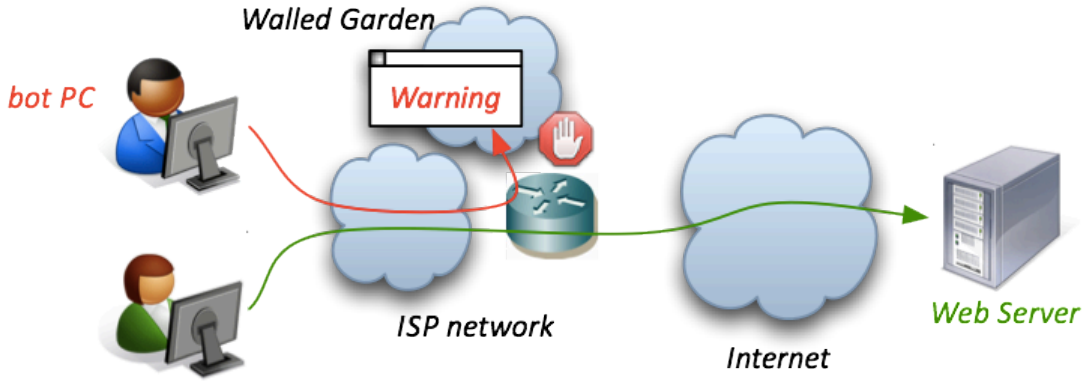
- 送信側の対策技術
- 受信側の対策技術
- その他

送信側の対策技術 - I

- **OP25B (Outbound Port 25 Blocking)**
  - 迷惑メールを送信させないための対策 (WG第2回資料)
  - 費用対効果の大きい効果的な対策
  - 導入手順やサポート体制が重要
  - 海外発が9割以上 (WG第1回資料) という現実をふまえると海外への導入働きかけも重要
- **送信者認証 (SMTP-AUTH)**
  - 送信者を特定することにより事後対策に有効
  - 単位時間あたりの送信数制限を設けることで大量送信を予防
  - 安易なパスワード設定の対策が必要 (メールサーバの踏み台防止)
- **送信ドメイン認証技術 (送信側)**
  - 送信者情報を詐称されないための基本的な対策
  - メールの用途や使い方に応じた技術の選択が必要
  - メール転送時の対策(ネットワーク方式)や第三者署名(電子署名方式)など課題への対応が必要

送信側の対策技術 - II

- **Walled Garden**
  - 不正プログラム (malware) に感染されられた PC を特定、インターネットへアクセスできないように制限
  - ウェブアクセス時に対策方法 (Windows Update, ウイルス除去等) を案内し、解決するまで外部にアクセスさせない
  - DNS への問い合わせ内容、Honeypot、DPI (Deep Packet Inspection)、OP25B による blocking などの情報を利用して感染 PC を特定
  - 検知手法、コスト、問い合わせの対応など課題は多い
  - 欧米やアジアの一部の ISP で導入
  - MAAWG Best Practices for the Use of a Walled Garden (2007.10.01)
    http://www.maawg.org/sites/maawg/files/news/MAAWG_Walled_Garden_BP_2007-09.pdf



受信側の対策技術

- **ネットワークベースでの制限**
  - 瞬間的な大量受信の制限 (送信元毎のスロットリング)
  - **あきらかに不正な送信元からの接続制限(DNSBL, IP25B)**
- **迷惑メールフィルタの導入**
  - メールの内容を分析して迷惑メールかどうかを判断
- **送信ドメイン認証技術**
  - 送信者情報が詐称されているかどうかを判断
  - 認証パス ≠ 正規のメール、あくまで送信者情報のなりすまし対策
  - 認証をパスしたドメインの評価が必要
  - FBL(Feedback Loop)やopt-outのための信頼できる送信者の特定

その他

- **IPv6 の導入**
  - MSA (メール投稿サーバ) など IPv6 が使われる可能性が高い部分への対応がまず必要
  - OP25B の導入は必須だが事前の整理が必要
    - 動的 IP アドレスと固定 IP アドレスの区別、法的整理の関連
  - MTA への導入時期と既存対策 (DNSBL) との関連
    - アドレス空間が広大なことによる懸念 → 送信毎に IP アドレス変更も可能？
    - DNSBL が IPv6 のブラックリストを管理できるか
    - DNS キャッシュなどが引き続き有効に機能するのか
    - IP アドレスの逆引きは引き続き設定されるのか、それを用いた動的 IP 判定は?
- **国際連携**
  - 日本の Best Practices の海外展開、海外の有効な手法の適用
  - 日本向けの迷惑メールが海外から送信される現状、事業者および執行機関の国際連携は今後ますます重要