DMARC and Domain Reputation

第11回 IAjapan 迷惑メール対策カンファレンス

2014.10.8

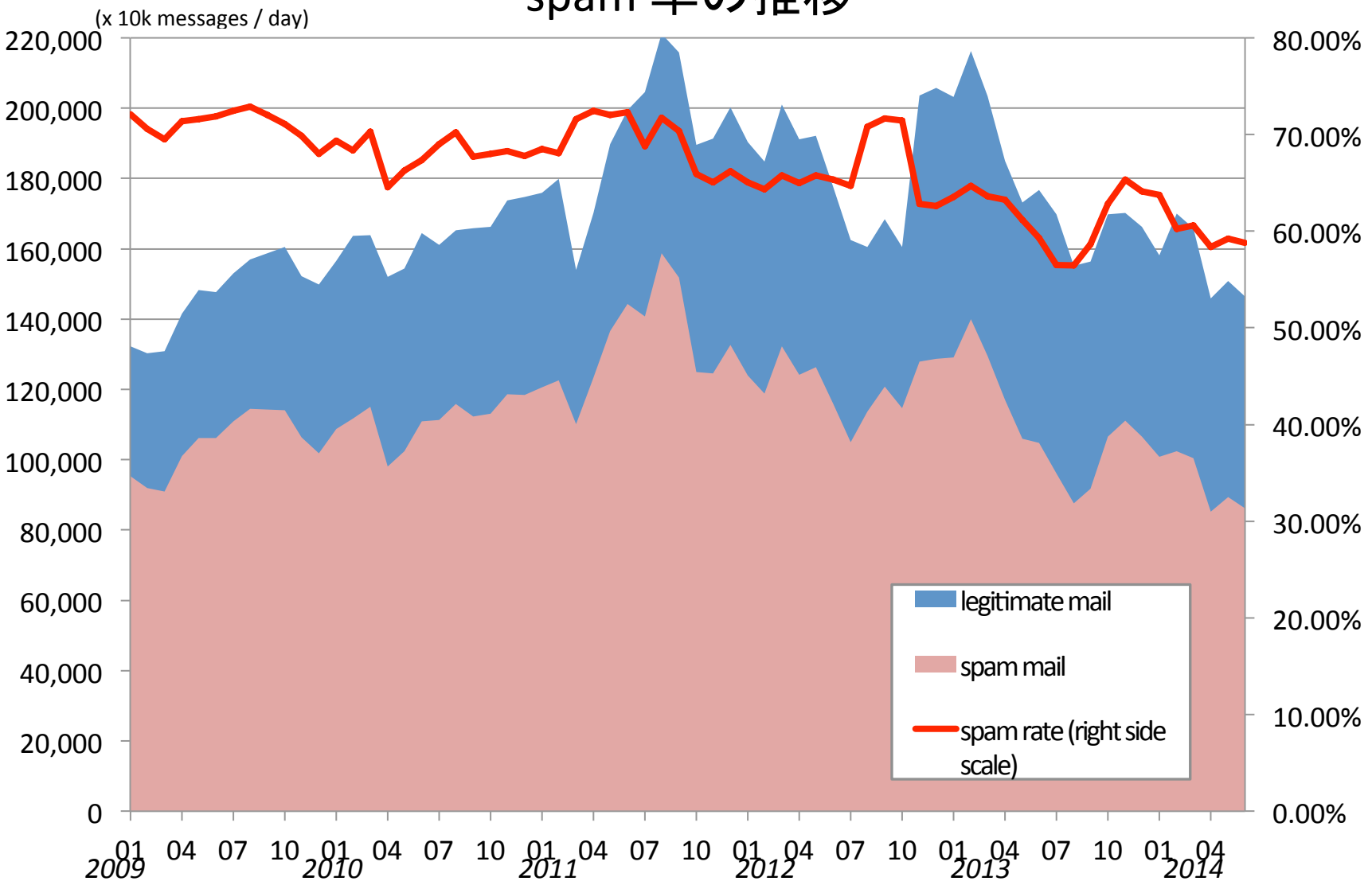
Shuji SAKURABA
Internet Initiative Japan Inc. (IIJ)

背景

- 送信者(ドメイン)を認証しただけでは不十分
  - Spammer は既に認証できるドメインを利用している
    - spam rate が約60%なのに SPF の “pass” 率は86.32%
    - “pass” したドメインの中に相当数 spam が含まれている (はずだ)
- 送信ドメイン認証技術の普及
  - 少なくとも SPF の高い導入率を利用しない手は無い
  - 導入のハードルが高い DKIM を普及させる後押しも必要
    - DKIM はメールの配送経路に依存せず認証できる利点がある
  - さらなる普及のためにも導入のための incentive が必要 → spam を確実に排除できることが必要
- より良いメール環境のために
  - Blocking は送信事業者や ISPs にとって好ましいものではない (誤判定があれば尚更)
  - 送信事業者や ISPs では実際の送信者を識別できる (はず) ← 何か問題が発生しても対応できる (はず)
  - 一律に過度なコストをかけてフィルタリングするのではなく、良い送信者を判別しフィルタリグコストを軽減しても良いのでは → White List Domains

迷惑メールの現状

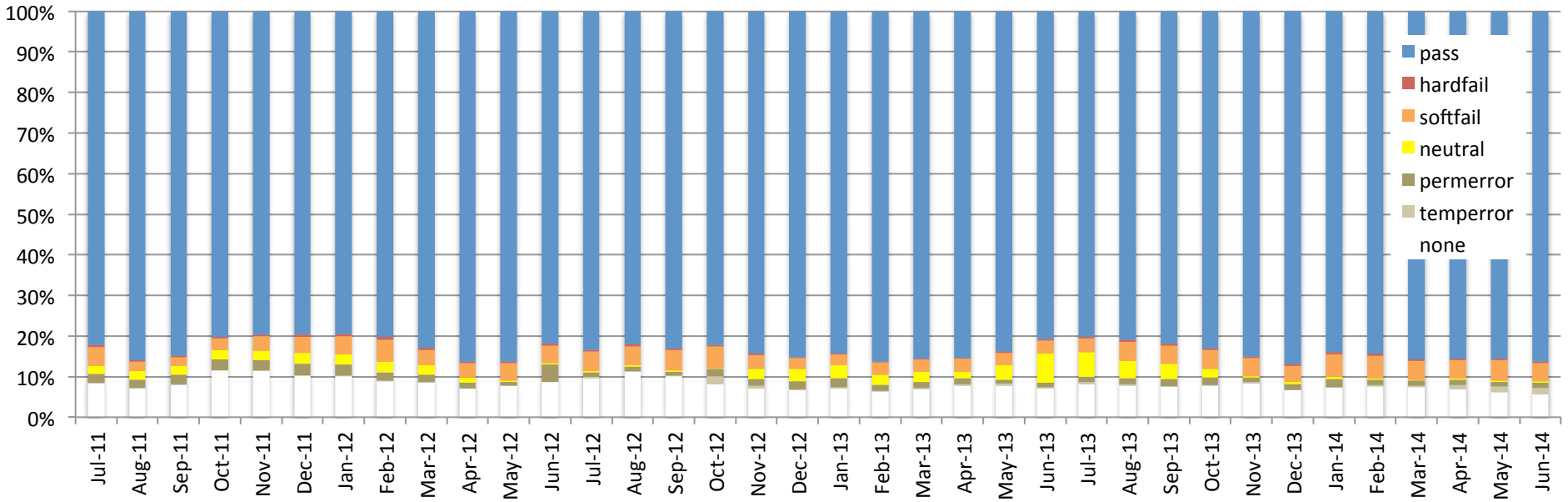
spam 率の推移



source: 電気通信事業者13社のデータを総務省がとりまとめ

SPF の動向

- SPF の導入状況
  - 総務省のとりまとめ (電気通信事業者7者の協力)
  - 94.31% 認証可能メールの割合 (2014.06)
  - 86.32% 認証結果が “pass” の割合 (2014.06)
    - 全体の迷惑メール割合と比べても高い (認証可能メールの 91.53% が “pass”)



Source: MIC survey (cooperate with 7 ISPs)

DMARC + Reputation

- 目的
  - 正しく送信者情報を設定した、受け取るべきメールを確実に受信者に届ける
- 手法
  - 送信ドメイン認証技術 (SPF, DKIM) の認証結果と、受信者が参照できる送信者情報 (RFC5322.From) を元に送信者をドメイン単位で確認 (認証) する

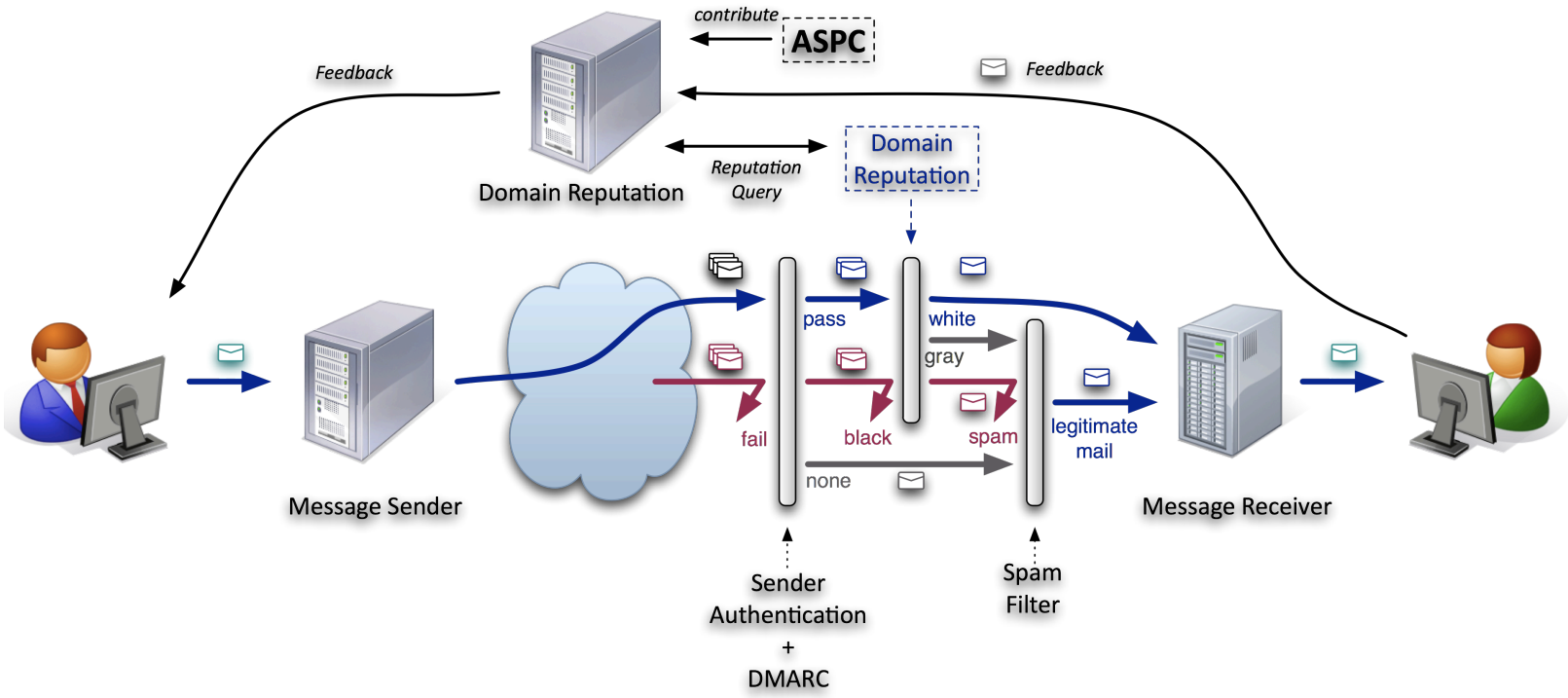
    → DMARC
  - 認証されたドメインを評価して受け取るべきメールを判断する

    → Domain Reputation

DMARC + Reputation

(sample model)

- 3段階の対策
  - Sender Authentication (SPF, DKIM) + DMARC
  - Domain Reputation
  - Spam Filter (Contents Filter)



Domain Reputation
仕組み

- Reputation Data
  - 受け取るべきドメインを White List として登録する
  - DMARC で pass したドメインのうち、明らかに迷惑メールしか送信しないドメインを Black List として登録する
    → (迷惑メールフィルタ等で) 受信拒否 (reject)
- Feedback Loop
  - 受信したメールで不要なものを申告 ("spam" ボタン)
  - 申告したメールを ARF (Abuse Reporting Format, RFC5965, RFC6650) で送信 → Domain Reputation 管理元で集約
    - White List ドメイン: Contact Point に連絡
    - Black List ドメイン: Black の重みを強化
    - 未登録ドメイン: Black List に登録 (しきい値をこえた場合)

DMARC + Reputation
要件1

- Reputation データの品質
  - 判定基準の根拠となる Reputation データには (なるべく) 誤りがあってはならない
  - 特に White List に入れる際には慎重に (何らかの基準を設ける必要があり)
- Feedback の必要性
  - White List (正しいメールの送信元) ドメインであっても踏み台問題など知らずに不正利用される場合がある → spam 送信を完全に防ぐことは難しい
  - 不正利用時になるべく早く検知したい ← DNSBL に登録される前に対応したい
  - Black List のデータを増やしたい (精度を上げたい)
- Contact Point の整備
  - White List 登録時の条件として、spam 送信時の対応ができることを条件として追加するのはどうか (防げないなら対応を迅速にしたい)

Domain Reputation
要件2

- Contact Point
  - 踏み台問題など、本来は受け取るべきドメインであっても、迷惑メールであることも予想されるため
    - Whilte List にはドメインの管理者への連絡先情報もあわせて登録する
    - Whilte List ドメインからのメールが迷惑メールであると判断された場合、当該ドメインの管理者に連絡する
    - 連絡を受けたドメイン管理者は、迷惑メールの送信者を特定し、速やかに対処する (こと)
  - ドメイン管理者 (送信側) の役割
    - 送信されるメールの実際の送信者が誰であるかを把握できる仕組みを備えていること (ISP であれば SMTP-AUTH 等)
    - メールの送信者毎に一時的にメール送信を抑制できる仕組みを備えていること (SMTP-AUTH 等)

Domain Reputation
より進んだ対応(案)

- Reputation Data の提供方法
  - 実験的なフェースではリスト配布で対応することもあり得る
    - まずは効果の程度を測定
  - Reputation の参照は実時間で行う
    - 実用段階ではメール受信時の都度 Reputation サーバを参照
    - Reputation サーバへの参照には標準技術を利用 (RFC7070～RFC7073)
- Feedback の応用
  - メール受信者は不要なメールを申告する仕組みを提供 (Webmail での spam ボタンなど)
    - 申告されたメールが DMARC で認証(pass)されている場合
      - 当該ドメインが White List に登録され、opt-out 可能であれば opt-out 処理を行う (ex. RFC2369)
        "List-Unsubscribe:" ヘッダの利用
      - 悪用を防ぐため White List ドメインであることが前提
    - DMARC で pass 以外の認証結果 (今後の検討課題)
      - 認証結果 reject: 受信側のポリシーで判断 (ex. filtering)
      - 認証結果 none: SPF, DKIM の認証結果が pass の場合、それぞれで利用等