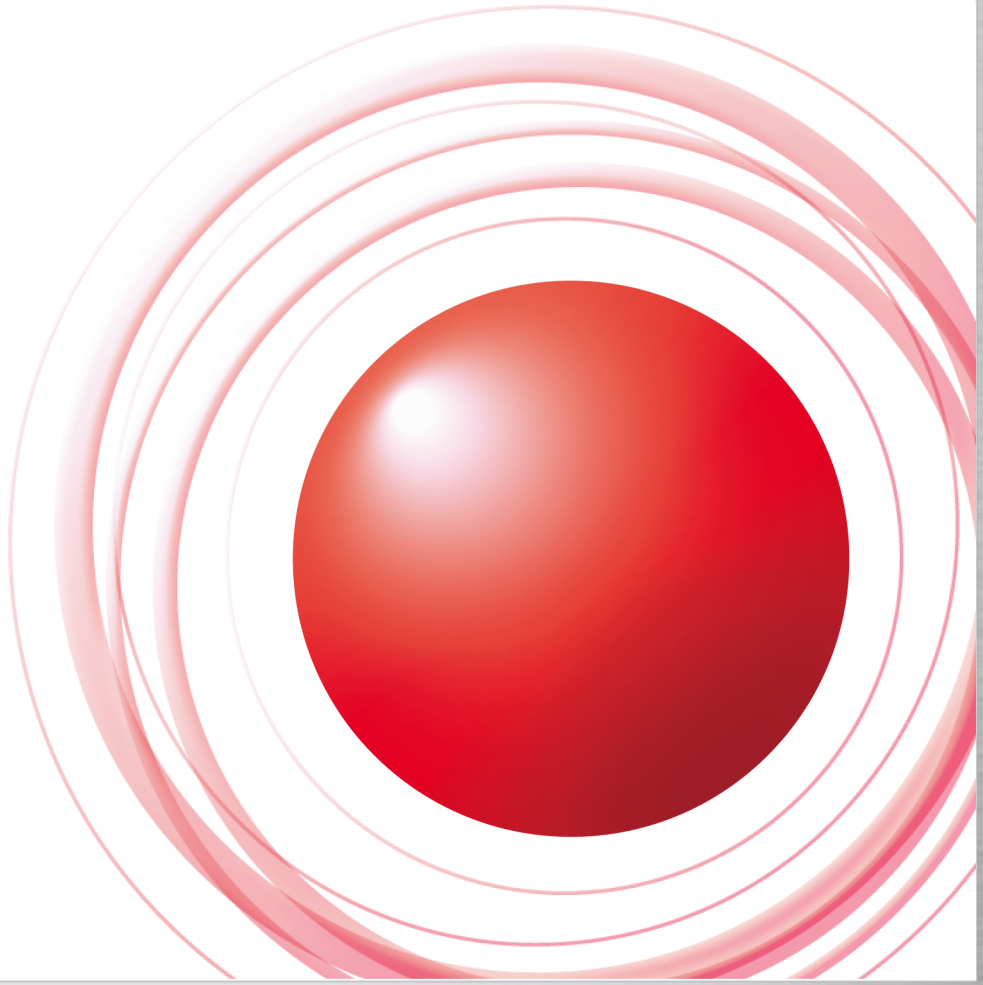
資料6

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2回会合）

迷惑メールに対するJEAGの取り組み

IIJ Internet Initiative Japan



2010.10.21

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

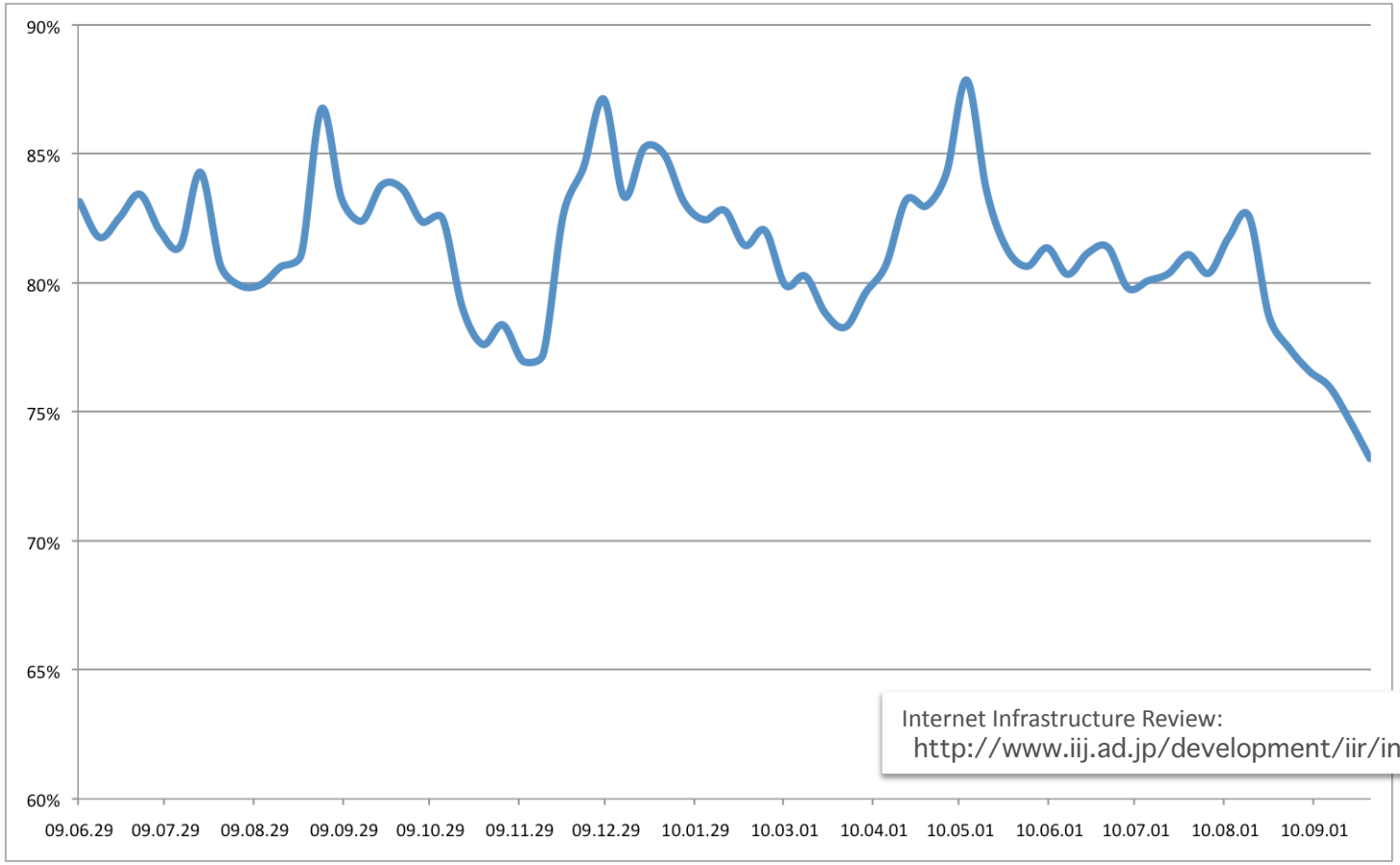
Ongoing Innovation

Agenda

- 迷惑メールの現状
- JEAG の概要
- JEAG の取り組み
  - OP25B
  - 送信ドメイン認証技術
  - 快適なメール環境を目指して

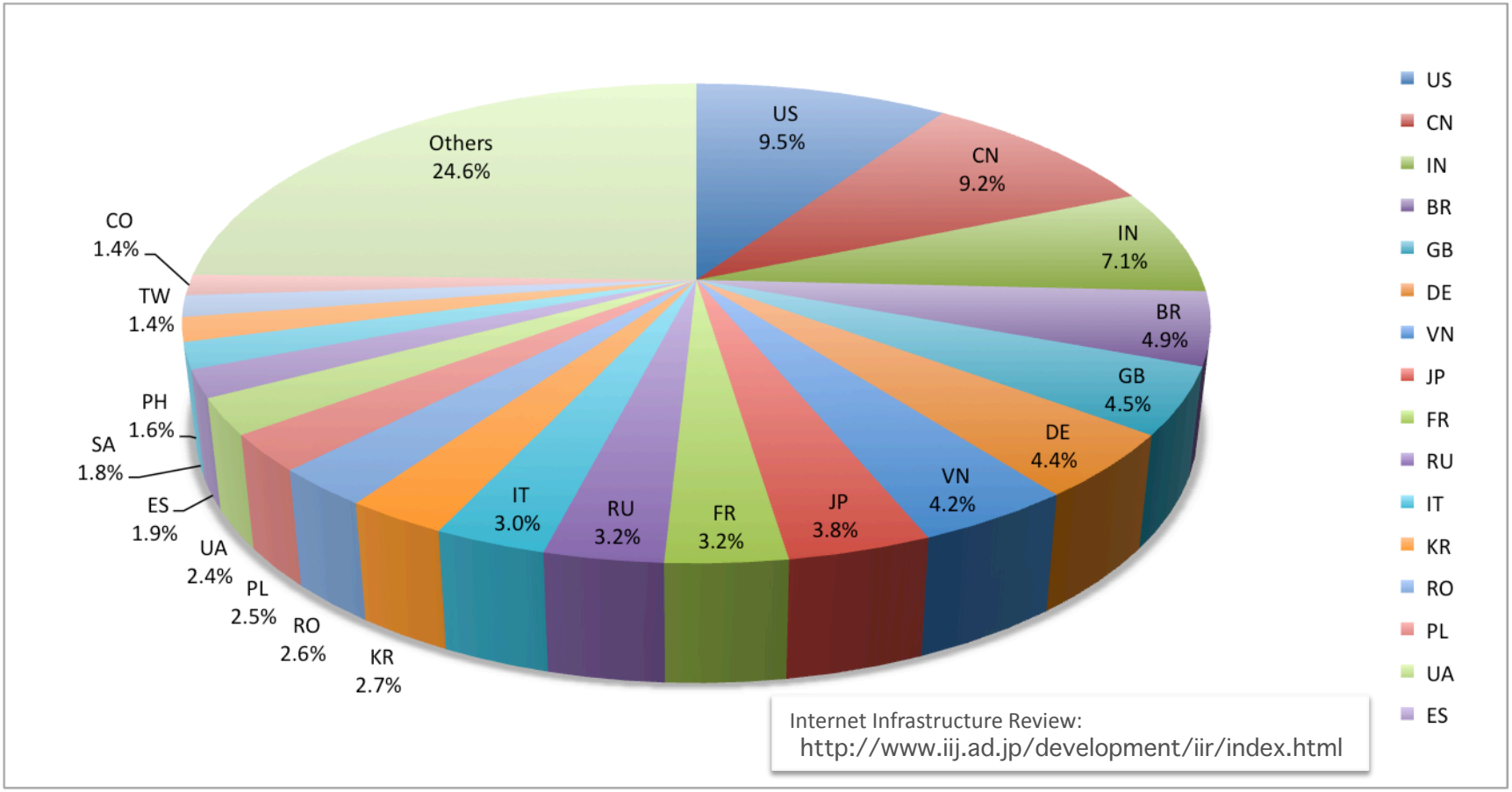
迷惑メールの現状

- **迷惑メール割合の推移**
  - IIJ が提供する迷惑メールフィルタによる検知率 (52週, 364日)
  - IIR (Internet Infrastructure Review) にて定期報告



迷惑メールの現状 (cont.)

- **迷惑メールの送信元分布**
  - IIJ が提供する迷惑メールフィルタのデータを利用
  - 期間: 2010.03.29 ～ 2010.09.26 (26週, 182日間)



Internet Infrastructure Review:
http://www.iij.ad.jp/development/iir/index.html

JEAGの概要

- **JEAG (Japan Email Anti-Abuse Group)**
  - 発起人 6社により 2005年3月15日発足
  - 主要 ISPs, 携帯電話事業者, ベンダなどメンバ企業 30社で構成
  - オブザーバ: 総務省, 経産省, (財)日本データ通信協会
  - 外部団体, 組織との連携
    - MAAWG (Messaging Anti-Abuse Working Group)
    - APCAUCE (Asia Pacific Coalition Against Unsolicited Commercial Email)
    - Email Security Expo & Conference (主催 (株) ナノオプト・メディア)
    - 迷惑メール対策カンファレンス (主催 (財)インターネット協会 迷惑メール対策委員会)
  - 目的: 技術的な見地およびサービス事業者間の連携による迷惑メール対策の推進

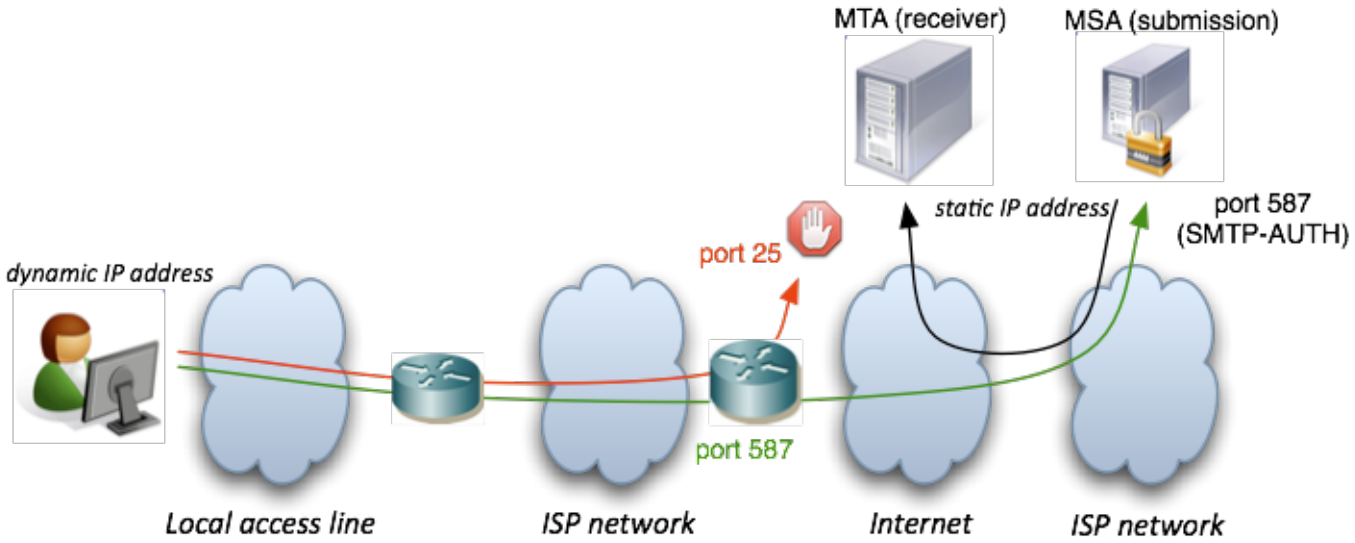
JEAG
Japan Email Anti-Abuse Group

- **JEAG Recommendation (2006.02.23 発行)**
  - OP25B (Outbound Port 25 Blocking)
  - 送信ドメイン認証技術
  - 携帯電話宛て迷惑メール対策

JEAGの取り組み – OP25B

- **OP25B (Outbound Port 25 Blocking)**
  - 迷惑メール送信に使われる動的 IP アドレスからのメール送信 (受信メールサーバの port 25 への直接接続) を制限
  - メール送信には ISP が提供するメールサーバ (投稿サーバ) を利用
  - 送信時は投稿ポート (port 587) を利用し送信者認証 (SMTP-AUTH) を行う
  - 管理元が明確な固定 IP アドレスは規制の対象外

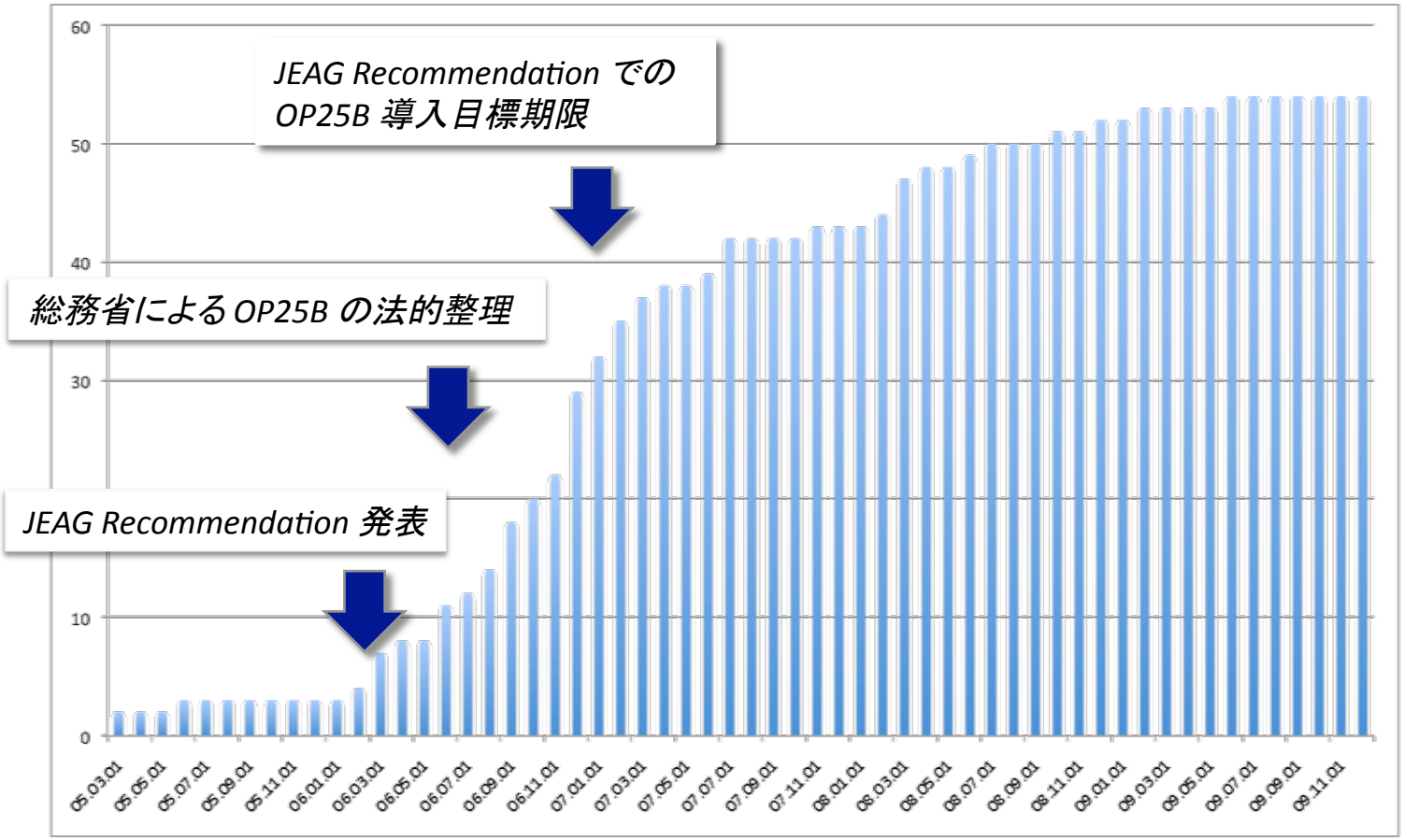
- **導入効果**
  - オンラインサインアップ等を利用した短時間での迷惑メールの大量送信 (打ち逃げ) の防止
  - Botnet (不正プログラムに感染させられた PC の集まり) を利用した迷惑メール送信の防止



JEAGの取り組み – OP25B (cont.)

- **導入状況と効果**
  - 日本の ISP での導入数の推移 (2005～2009)
  - 迷惑メールの送信国ランキングの推移 (WG第1回資料)
  - 迷惑メールの送信元分布 (page 4)

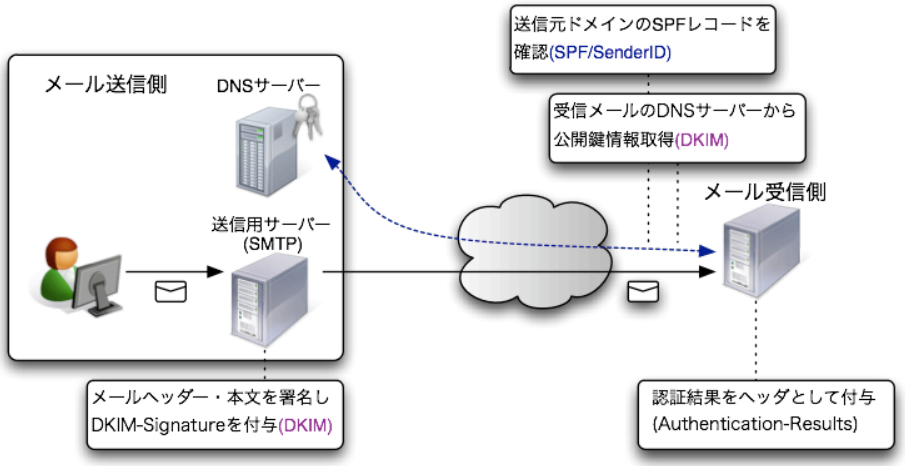
source: JADAC survey



JEAGの取り組み – 送信ドメイン認証技術

- **基本的な仕組み**
  - 送り手は送信元 (メールの出口) を明確に表明
  - 受け手は送信者情報が正しく表明されているか確認
  - メールの送信側と受信側双方が導入することにより認証が可能となる

- **送信ドメイン認証技術の特徴**
  - 既存のメール配信の仕組みを変更することなく互換性を維持
  - DNS の仕組みを利用することにより新たな認証機関等を必要としない
  - 送信者情報や認証の仕組みの違いによる複数の認証方法
    - SPF (Sender Policy Framework) / SIDF (Sender ID Framework)…ネットワーク方式
    - DKIM (DomainKeys Identified Mail)…電子署名方式

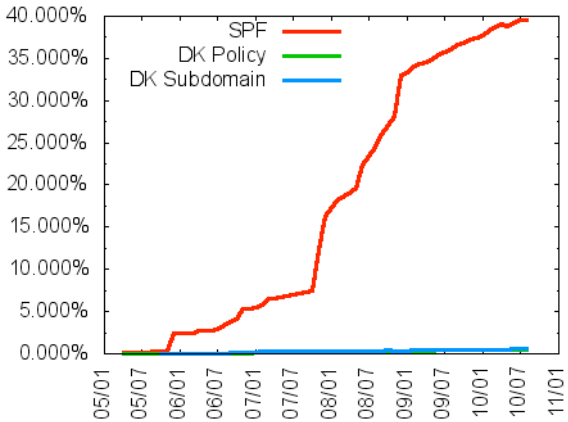


JEAGの取り組み – 送信ドメイン認証技術 (cont.)

- **期待できる効果**
  - 送信者情報を詐称したメールの峻別
    → フィッシング対策
    → 迷惑メール対策 (送信者情報を詐称している場合が多い)
  - 迷惑メール対策 → ドメインレピュテーションの利用
  - 受け取るべきメールの識別 (ホワイトリストとしての利用)
  - 受信者側での認証結果を利用した個別フィルタリングの利用 (認証結果の提示形式の統一, RFC5451)
    → MUA (Mail User Agent) での機能拡張等の利用
    → ISP が提供する個別フィルタ設定機能の利用
    → 携帯電話でのフィルタ設定機能等
  - オプトアウトや苦情等の連絡先の信頼性判断 (FBL: Feedback Loop)

- **導入状況**
  - “.jp” ドメインの 39.59% が SPF レコードを宣言
    (2010年8月, WIDEプロジェクト調査)
  - 流量ベースでは約80%のドメインがSPFに対応
    (電気通信事業者6社の協力により総務省がとりまとめ)

    http://www.soumu.go.jp/main_sosiki/joho_tsusin/d_syohi/m_mail.html#toukei



JEAGの取り組み – 送信ドメイン認証技術 (cont.)

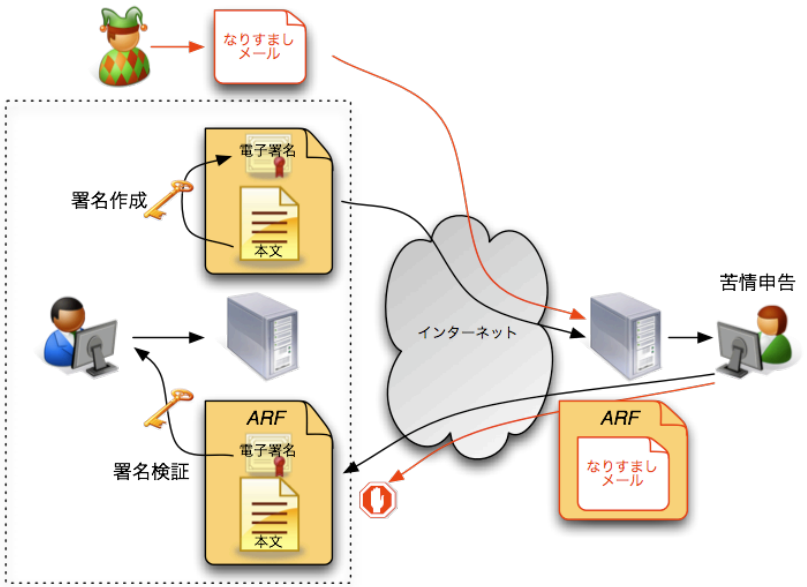
- **JEAG Recommendation 改訂**
  - 送信ドメイン認証技術の普及や技術的な進展を踏まえて議論中
    (注: 内容は変更される可能性があります)

- **改訂のポイント**
  - 送信ドメイン認証が失敗しないような運用
    - 送信者情報が正しく設定されるかの確認 ← 送信者認証 (SMTP-AUTH) 情報の活用
    - 外部ネットワーク利用時の運用指針 ← モバイル環境等外部ネットワーク利用時の企業内サーバの利用等
    - ネットワーク方式での転送問題の回避方法の提示
    - 電子署名方式 (DKIM) での運用方法 (メール配信代行時, メーリングリスト運用等), IETF で継続議論中
  - 認証結果の有効利用
    - 詐称された送信者情報元へのエラーメールの配送抑制 (Backscatter 問題への対応)
    - 認証結果提示形式の統一化 (Authentication-Results ヘッダ, RFC5451)
    - Feedback Loop 時の送信元の確認, 発信側の送信メール確認

JEAGの取り組み – 送信ドメイン認証技術 (cont.)

- **Feedback Loop**
  - 受信者から (広告宣伝メール) 送信者への意見等連絡 → 本来は送信者，受信者ともに有益な情報
  - オプトアウトや苦情等 (内容，送信頻度等) を連絡したいと思っても送信者がオプトインした事業者であるのかが判断が難しい
  - 送信事業者は受け取った Feedback が本当に送ったメールであるかの判断が難しい

- **送信ドメイン認証技術の利用**
  - 受信者は認証結果から判断
  - 送信者は DKIM 利用により再認証可能なメールであれば，ARF (Abuse Reporting Format, RFC5965) 形式での連絡で判断可能
  - 米国では中間事業者が仲介する場合が多い



JEAGの取り組み –快適なメール環境を目指して

- **メール利用環境**
  - 短時間で大量送信するなど過度にメール受信設備に負担をかけるような送信の在り方の是正
    → メール本来の仕組みに基づいた運用を
  - 自組織が送信しているメールの適正な管理
    → メールの送信数制限，送信者認証とログの管理による事後対応
  - 不正なメール利用者の事前対策
    → サポート等に関する BCP (Best Current Practices) の共有

- **国際連携**
  - 迷惑メールの大部分は海外から送信
  - 日本での成功事例 (OP25B，送信ドメイン認証技術，etc) の海外への普及によるグローバルでの迷惑メール抑制
    - MAAWG, APCAUCE, 中国 ISC, 韓国 KISA, ブラジル cert.br，LAP, et
  - 日本発のメールが海外でブロックされないための関係づくり