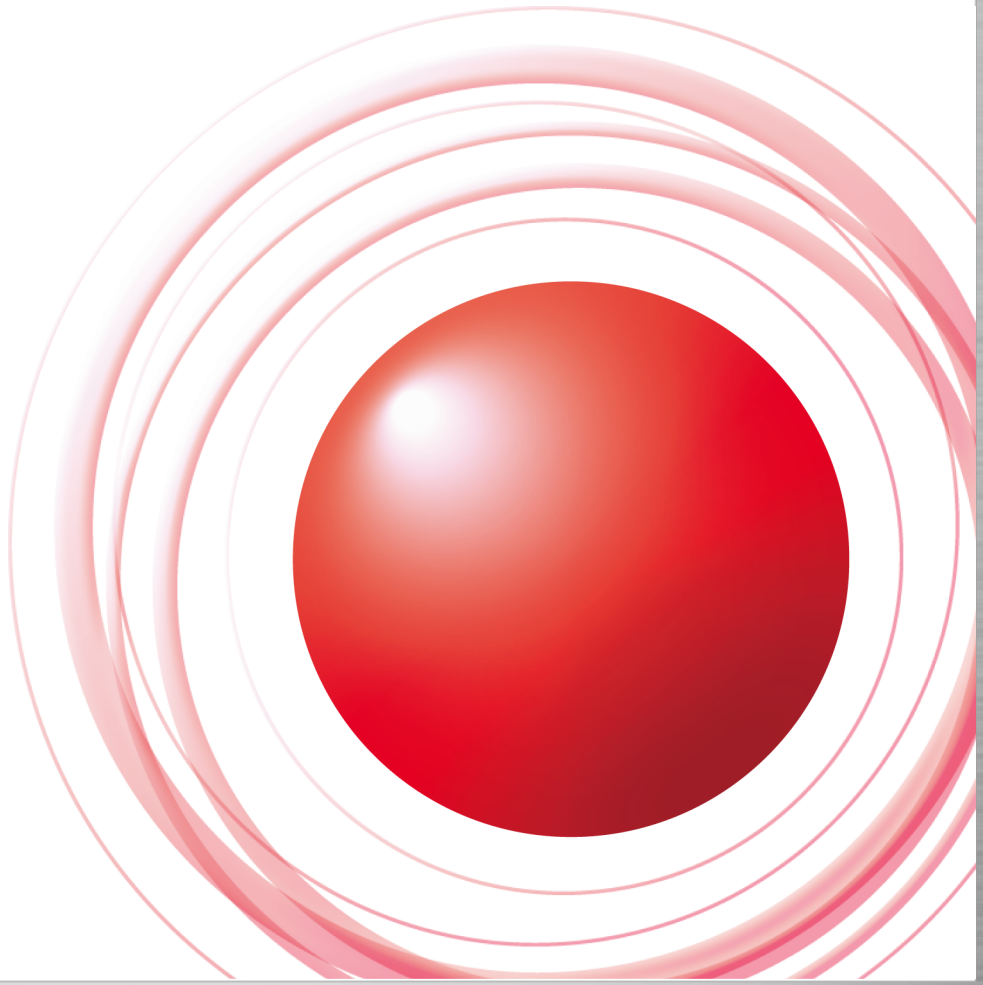
迷惑メール対策と送信ドメイン認証技術

電子メールセキュリティーセミナー [熊本]

IIJ Internet Initiative Japan



2011.03.08

Internet Initiative Japan Inc. (IIJ)
Shuji SAKURABA (櫻庭秀次)

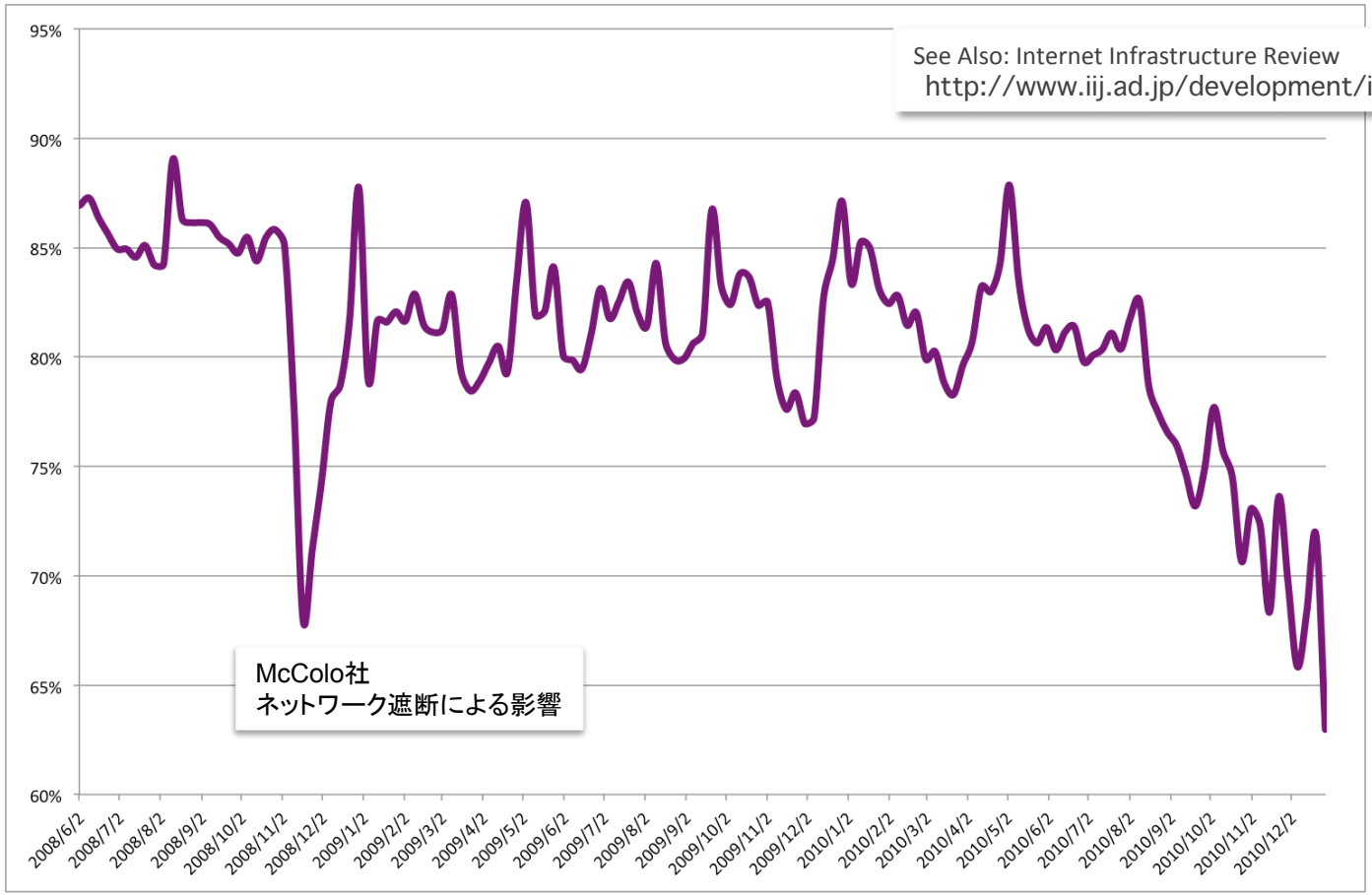
Ongoing Innovation

Agenda

- 迷惑メールの現状
- 対策の強化とその懸念
- 送信ドメイン認証技術
  - 概要解説
  - 導入状況
  - 導入効果
  - 運用
- 迷惑メール対策の取り組み
  - JEAG
  - 国際連携
- おわりに

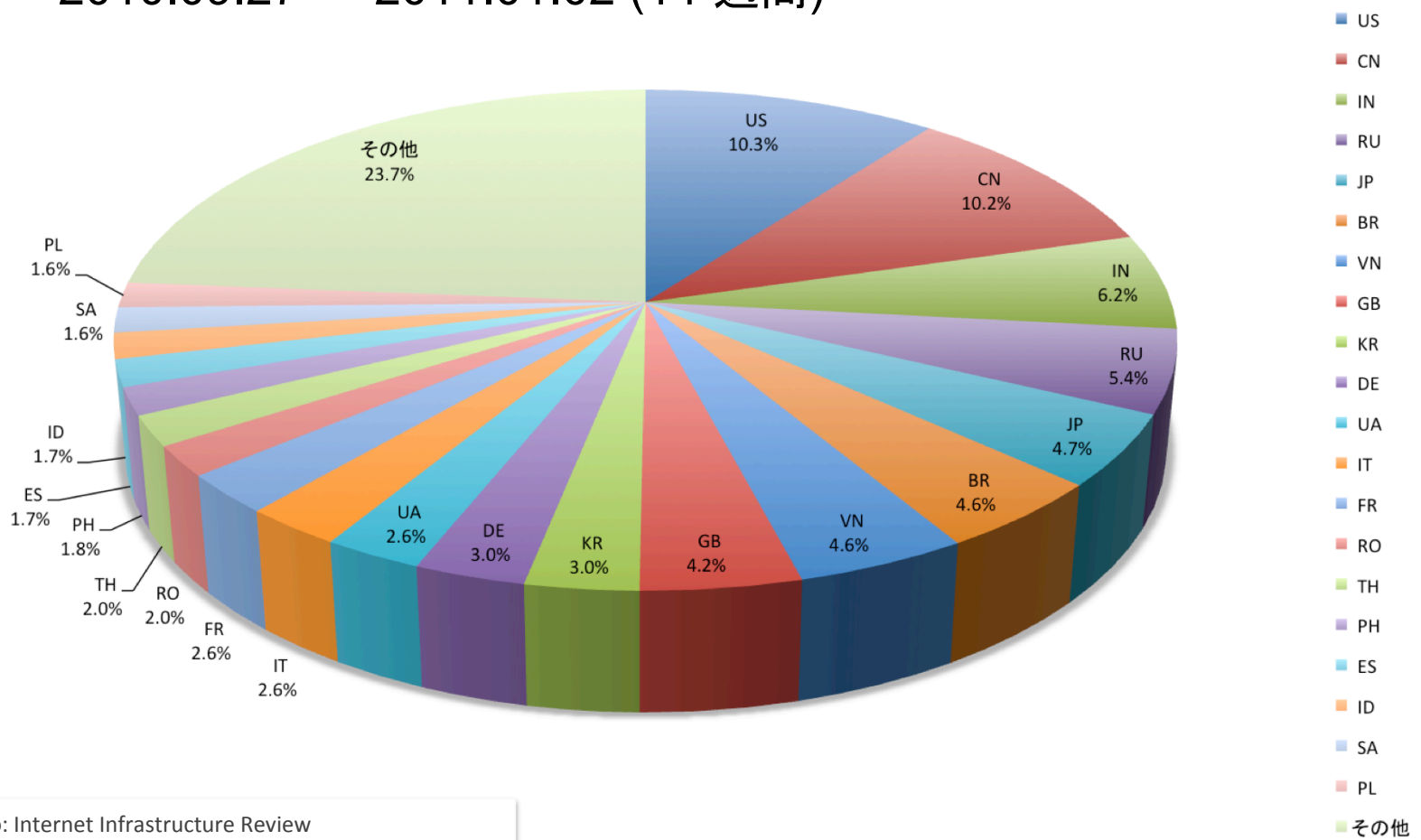
迷惑メールの現状 - I

- **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
  - 2008.06.02 ～ 2011.01.02 (135週間)



迷惑メールの現状 - II

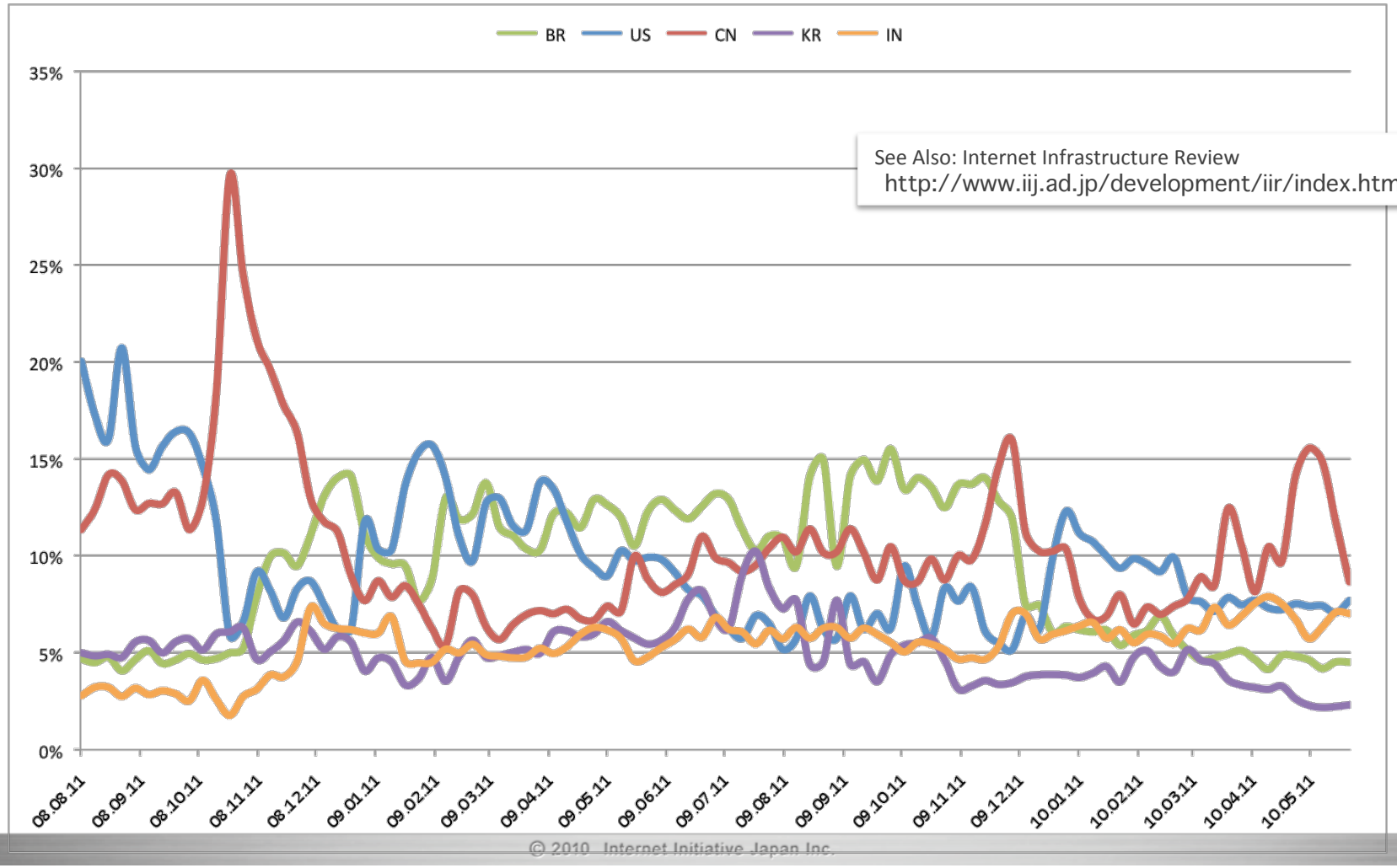
- 送信元の地域別分布
  - 2010.09.27 ～ 2011.01.02 (14 週間)



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

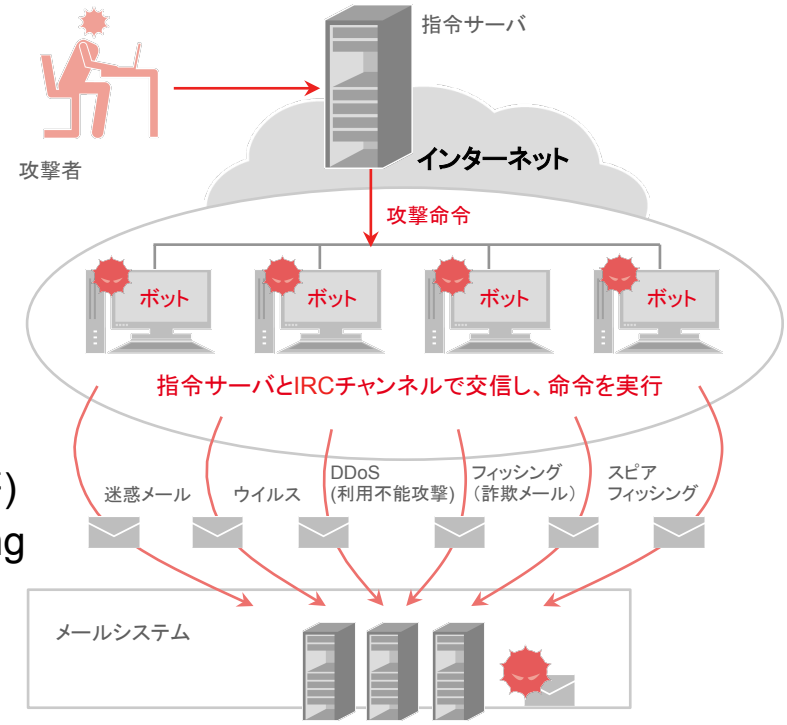
迷惑メールの現状 - III

- 主要送信元の推移
  - 2008.08.11 ～ 2010.06.06 (95週)



迷惑メールの現状 - IV

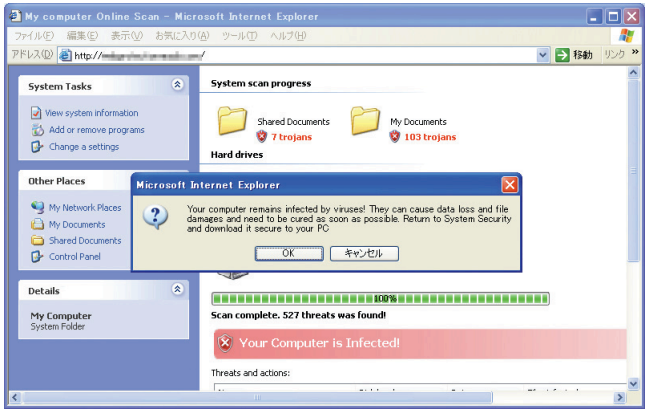
- **送信手法の高度化・多様化**
  - 高速回線を利用した短時間での大量送信 (主に国内からの送信)
  - 海外拠点からの大量送信 (OP25B による国内送信の抑制: 後述)
  - Botnet の利用
    - 不正プログラム (malware: malicious software) に PC を感染させる
    - インターネット経由で外部から制御
    - ロボットのように操られることから Bot
    - 複数の Bot をネットワーク化 (Botnet)
    - Botnet を様々な用途に悪用
  - 正規メールサーバを踏み台に利用
    - フリーメールのアカウントを大量取得
    - メール受信側はブロックしづらいことを悪用
    - CAPTCHA を解読するための様々な試み
    - ISP のメールサーバを利用
      (安易なパスワード設定、spyware の利用等)
    - 評判を乗っ取る意味で Reputation Hijacking
  - 代理サーバ (socks, http, proxy, etc) の利用およびその国際化

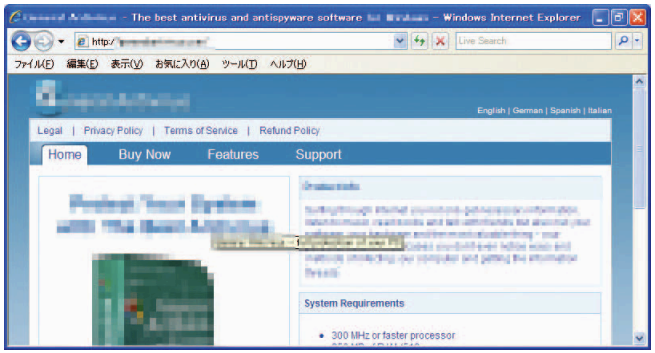


CAPTCHA: Completely Automated Public Turing test to tell Computers and Humans Apart

迷惑メールの現状 - V

- **被害の多様化**
  - 偽のWebサイトへの誘導による個人情報の搾取 (phishing)
    - 短縮 URL の悪用、弊害
  - 偽のセキュリティソフトを装った脅迫による金銭搾取 (scareware)
    - ウイルスチェックの実行を装い感染を警告 (例えばここまでは無料)
    - 除去のためにはセキュリティソフトの購入が必要と警告 (有料)
    - アプデート称して別の不正プログラムを誘導
    - 日本語版も出回っている





- **構造の多様化**
  - 分業体制
    - malware の開発
    - botnet の構築 (bot の拡散)
    - メールアドレスの収集, etc
  - ブラックマーケット
    - 搾取した個人情報 (カード情報等) の売買
    - 正規アカウント情報の売買
    - ボットネットの時間貸し出し (クラウドサービス?)

迷惑メールの現状 - VI

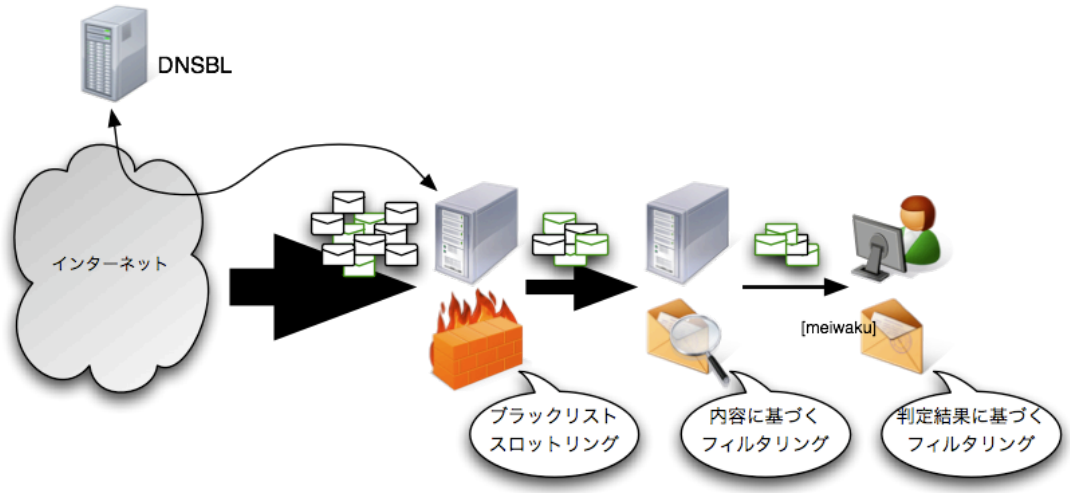
- **動機**
  - 金銭目的
    - 2007年1月逮捕のタクミ通信の事例: 中国黒竜江省に設置した128台のPCから9,000万通/日送信、1億2,000万円/月の利益
    - 2011年1月逮捕のUNIVERSAL FREAKSの事例: 海外5カ国 (中国、フィリピン、タイ、バングラディッシュ、韓国) のメールサーバを経由して送信、一度に500万通送信、利用料として約5億円/1年半
  - Less Risk
    - Less Violence
    - Less Jail Time
    - More Profit

「UNIVERSAL FREAKS」の事務所の家宅捜索に入る捜査員ら＝1月17日、東京・池袋
(msn 産經ニュースより)

対策の強化とその懸念 - I

- **迷惑メール対策手法**
  - 送信元情報などによるネットワークレベルでの抑制
  - メールの内容による判断
  - 最終的には受信者の判断によるフィルタリング (が望ましい)

- **懸念点**
  - 判定処理の負荷 (設備，運用，コスト)
  - 判定精度
    - 正しいメールを迷惑メールと誤判定 (false positive)
    - 迷惑メールを正しいメールと誤判定 (false negative)
    - 判定を回避するための様々な手法と急激な増加への対応遅れ (ウイルス対策と同根の問題)



対策の強化とその懸念 - II

- **送信元による判断 – 外部データの利用**
  - DNS の仕組みを利用した IP アドレスによる Black List (DNSBL)
  - 接続時点での判断が可能で設備負荷も比較的小さい
  - 判定精度と運用方針の問題
    - データの信憑性 (データの収集方法や偏り)
    - 運用方針 (誤判定時の解除手続きが不明瞭)
    - 正規のメールサーバが登録された場合の影響 (送信側のみならず受信側も)
    - 汚れた IP アドレス再割当の問題
  - IPv6 の利用が進むと既存の仕組みでは困難
    - 広大なアドレス空間
      - IPv4: 約 2^{32} (= 約42億) 個
      - IPv6: 約 2^{128} (=約340澗) 個　　(cf. 億、兆、京、垓、秭(秭)、穣、溝、澗)
    - DNS の仕組み (キャッシュ含む) では事実上提供困難
    - 新たなデータ参照のための方法が必要
    - ホワイトリスト (正規メールサーバ) を提供する方式への転換?

対策の強化とその懸念 - III

- **送信元による判断 – 自身の判断**
  - 正規のメールサーバかどうかを接続元情報から独自に判断
    - IP アドレスの逆引きが設定されているかどうか (IPv6 の逆引き設定は?)
    - 単位時間あたりの接続数や宛先不明の割合から判断
  - 未知の送信元を一時保留 (greylisting) することによる判定
    - 送信元の大規模分散への対応 (一時保留した接続元の保持が必要)
    - 配送経路が変更されること (Fallback MTA) の考慮がなされているか
    - 一時保留することによるメール配送の遅延は許容できるのか

- **対策手法の法的留意点**
  - 電気通信事業法の範囲では制約がある (原則利用者の同意が必要)
  - 幾つかの技術 (OP25B, 送信ドメイン認証技術) に関しては法的整理が行われている

    ご参考:

    http://www.soumu.go.jp/main_sosiki/joho_tsusin/d_syohi/jigyosha.html

対策の強化とその懸念 - IV

- **迷惑メール対策の今後**
  - 迷惑メール送信で利益を得られる間は減少はあまり期待できない
  - 迷惑メールが減少しない限りは今後も対策の強化は避けられない
  - 対策には誤判定のリスクが常に存在
  - メールはコミュニケーションのための重要なツール

正しいメールがきちんと到達できる環境作りが必要

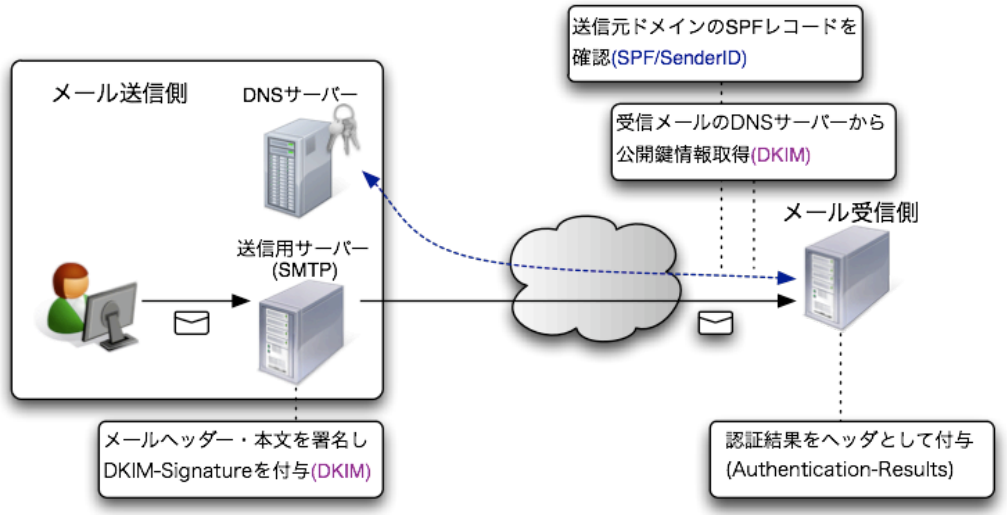
正しいメールを判断するための共通基盤としての

送信ドメイン認証技術

送信ドメイン認証技術 – 概要

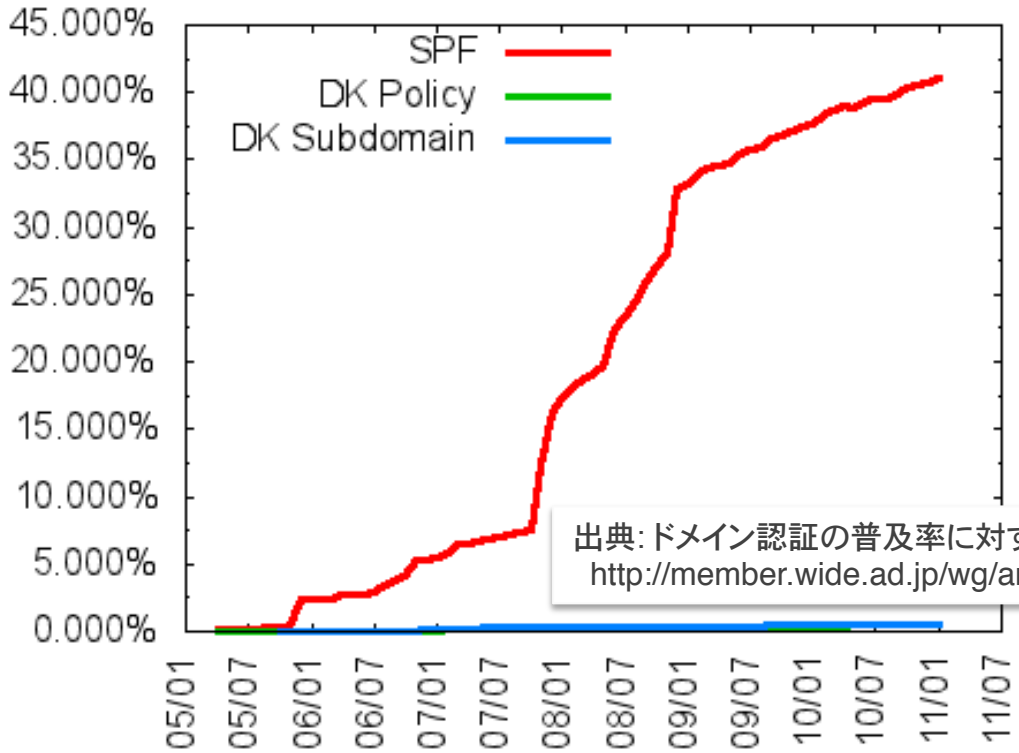
- **基本的な仕組み**
  - 送り手は送信元 (メールの出口) を明確に表明
  - 受け手は送信者情報が正しく表明されているか確認 (認証)

- **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下位互換を維持
  - 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



送信ドメイン認証技術 – 導入状況 I

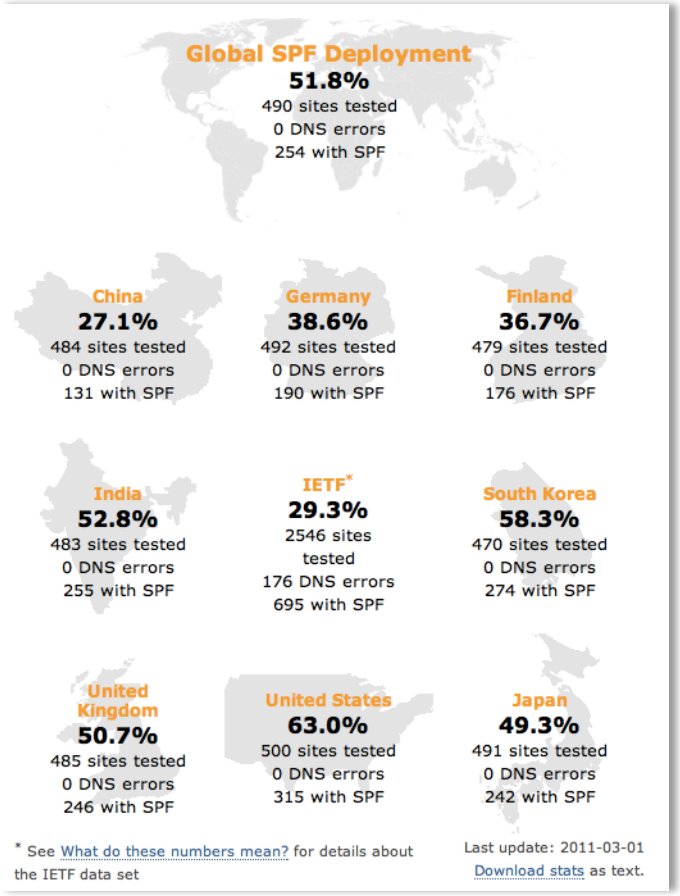
- **日本 (jp) の導入状況**
  - WIDE プロジェクトと JPRS による共同研究による調査
  - 2011年1月時点で “jp” ドメインの SPF 宣言率は 40.98%
  - “co.jp” ドメインについては 48.04%

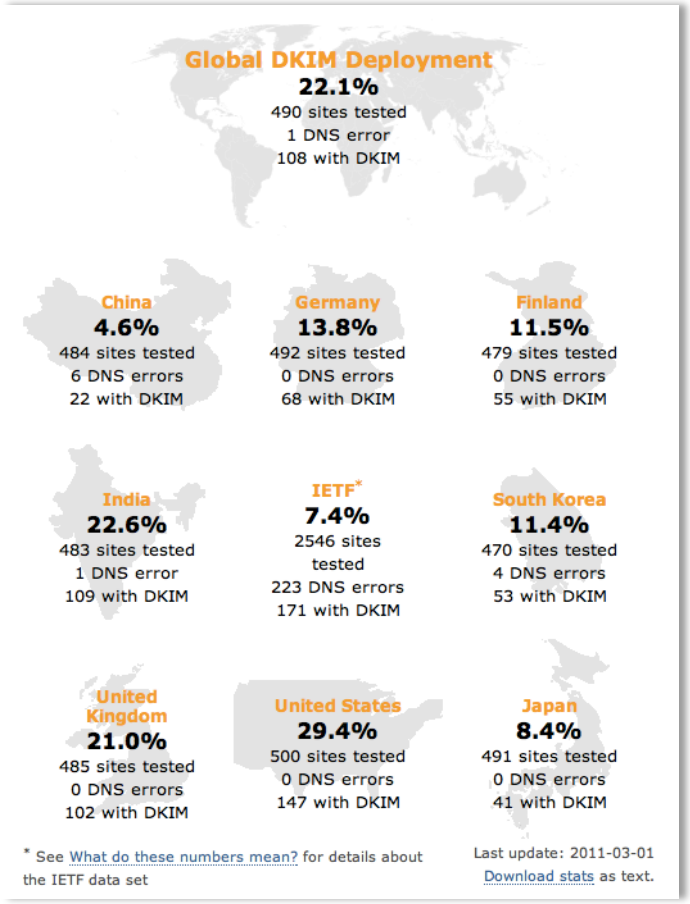


出典: ドメイン認証の普及率に対する測定結果
http://member.wide.ad.jp/wg/antispam/stats/index.html.ja

送信ドメイン認証技術 – 導入状況 II

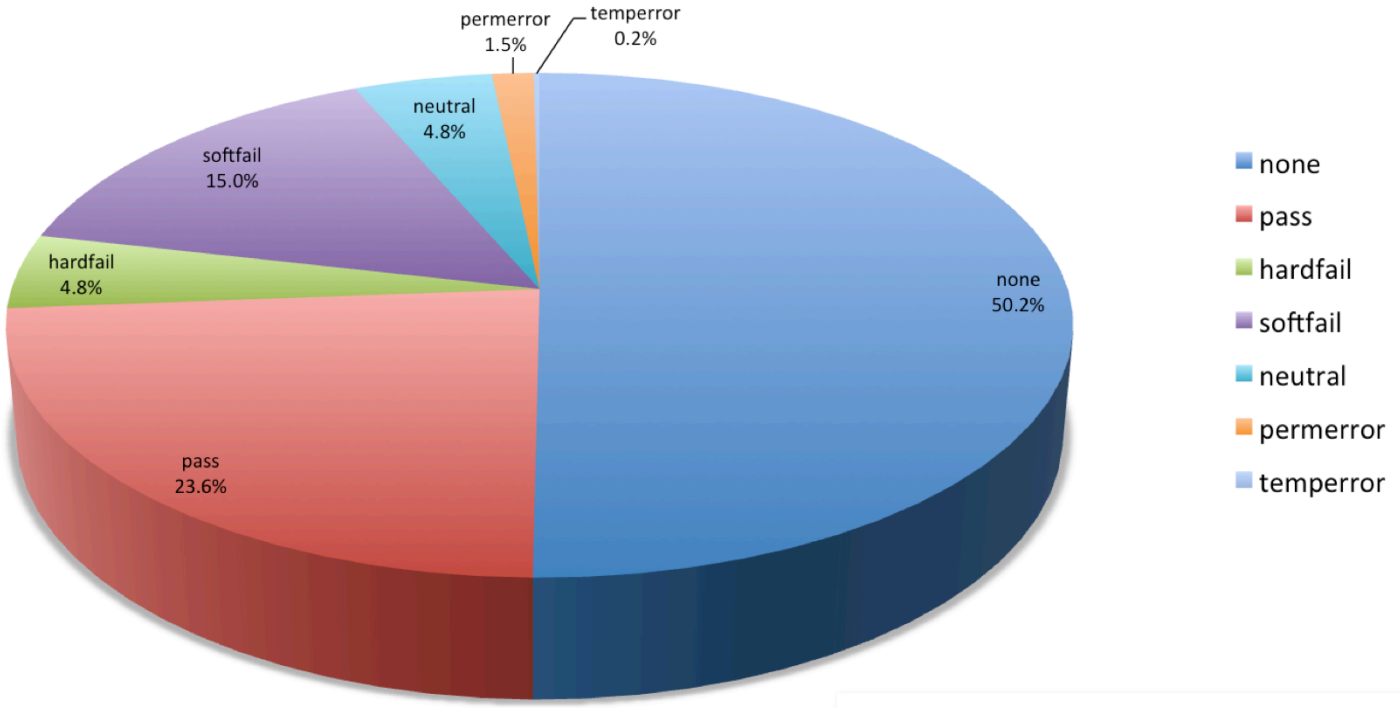
- グローバルでの導入状況
  - Lars Eggert @ Nokia による調査 (https://fit.nokia.com/lars/)
  - alexa.com による上位 web site のドメインを調査





送信ドメイン認証技術 – 導入状況 III

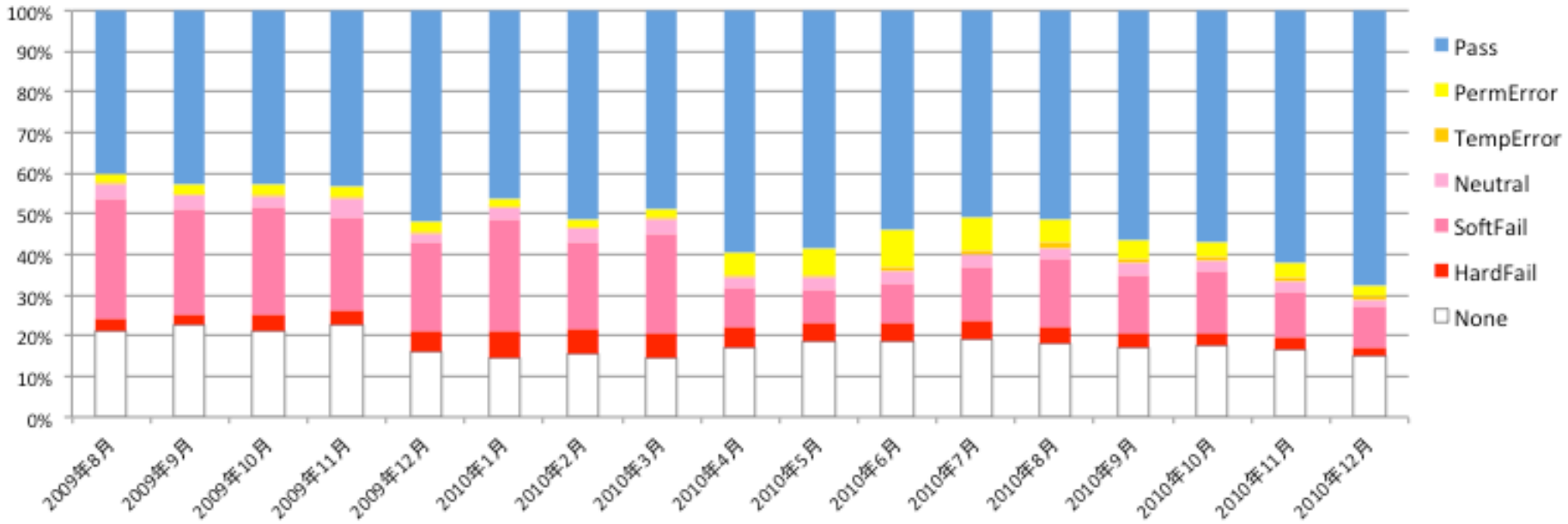
- 受信メールによる調査
  - 期間: 2010.09.27 ～ 2011.01.02
  - 受信メールの 49.8% のドメインが SPF レコードを宣言



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

送信ドメイン認証技術 – 導入状況 IV

- **受信メールによる調査**
  - 電気通信事業者7社のデータを総務省がとりまとめ
  - 期間: 2009.08 ～ 2010.12
  - 受信メールの 85.1% のドメインが SPF レコードを宣言 (2010.12)



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

送信ドメイン認証技術 – 効果 I

- **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**
  - 認証が通った送信者ドメインの精査 (ドメインレピュテーションの利用)
  - 紛らわしいドメインの峻別
- **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
  - 信頼できる送信元は迷惑メールフィルタを通さず優先受信 (設備負荷の軽減)
- **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) での機能拡張等で利用可能
  - ISP や携帯電話でのフィルタ設定機能等 (なりすまし対策フィルタ)
- **オプトアウトや苦情等の連絡先の信頼性判断**
  - ARF (RFC5965) などを利用した FBL (Feedback Loop) での利用

送信ドメイン認証技術 – 効果 II

- **メール受信者への認証結果の通知**
  - 受信メールサーバ側でフィルタリングが難しい場合でも受信者の MUA で個別に判断
  - 認証結果を記録する統一的なフォーマット (RFC5451, Message Header Field for Indicating Message Authentication Status) を利用

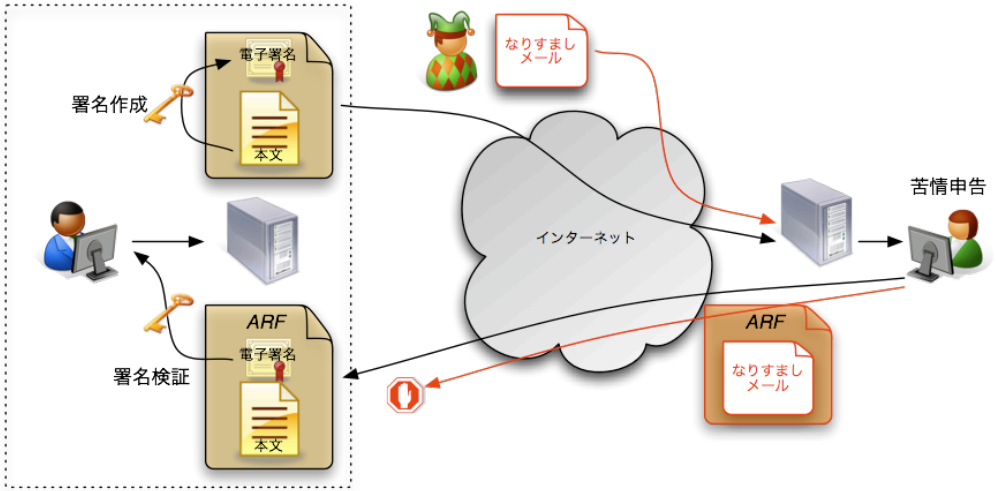
```
Authentication-Results: example.com;
    sender-id=hardfail header.from=example.com;
    dkim=pass (good signature) header.i=sender@example.com
```

  - MUA (Mail User Agent) の機能を用い受信者がフィルタリング

Apple Mail のフィルタリング例

送信ドメイン認証技術 – 効果 III

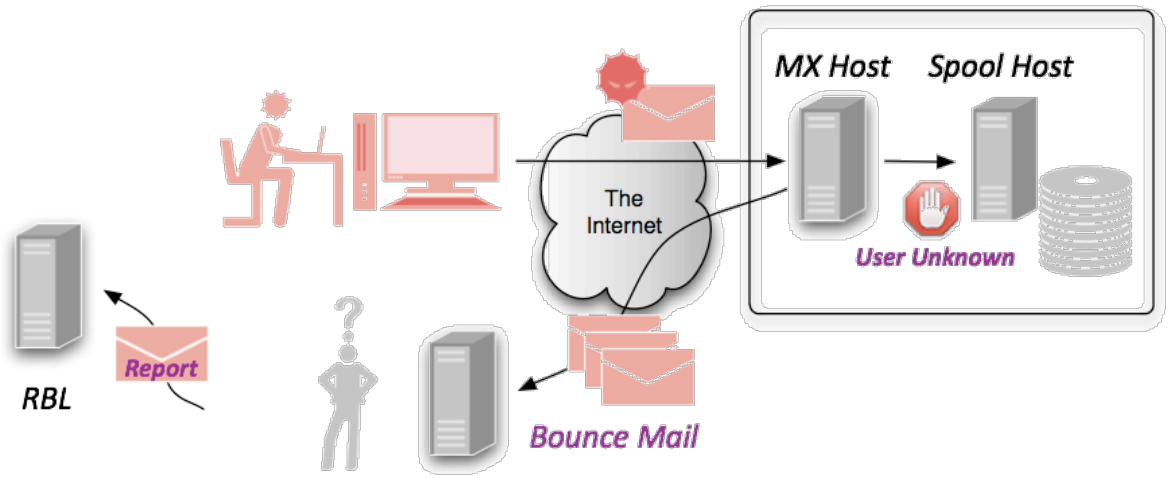
- **FBL (Feedback Loop)**
  - FBL とはメール受信者から送信側への苦情等の申し立て
  - 米国では中間事業者が仲立ちを行う事例もあり
    - 予め送信事業者は送信側の情報と連絡窓口を登録
    - 受信側で Webmail 等でのボタンによる申告 → 中間事業者への通知
    - 登録されている事業者であれば報告
  - 送信事業者の利点
    - 送信先リストからの削除 (opt-out)
    - 苦情のあったメールの識別 → 依頼元との今後の調整
    - 送信間隔の調整, etc
  - 受け取る苦情が本当に送信側が送ったものであるかの検証が必要
  - 申告メールに DKIM ヘッダ (DKIM-Singnature) があれば再検証可能
  - ARF (Abuse Reporting Format) 形式であればヘッダ情報も含まれる
    - An Extensible Format for Email Feedback Reports (draft-ietf-marf-base-06)



送信ドメイン認証技術 – 効果 IV

- **Backscatter 問題**
  - 迷惑メールの多くは送信元情報が詐称されている
  - 宛先不明メールに対するエラーメールの送信先は送信者情報を利用
  - 詐称された側へ送信される大量のエラーメール
  - 無関係なエラーメールが迷惑メールと判断
    → エラーメールの送信元が Black List へ登録されるなど二次的な問題も発生

- **回避策**
  - 送信ドメイン認証技術により送信者情報が詐称されていると思われる ("fail" or "softfail") 送信者へエラーメール送信は行わない
  - または宛先不明のメールを受け取らない → 別途 DHA (Dictionary Harvesting Attack) 対策も必要



送信ドメイン認証技術 – 運用

- **送信側の運用**
  - SPF レコードの宣言はもはや必須
  - より重要なメール (顧客連絡等) には DKIM の導入を
  - ドメイン名の評判 (reputation) が下がらないような運用 (迷惑メールを送信しない) が必要
  - メール送信経路の確認 → メールシステム，利用方法 (利用ルール)
  - 送信時の送信者認証 (SMTP-AUTH) による管理 → 事後対処等
  - 送信者情報 (SPF/Sender ID) が正しく設定されているか確認
  - DNS の負荷，RR (Resource Record) の伝播時間の考慮 (TTL値)
  - DKIM ADSP (Author Domain Signing Practices) による署名方針の表明

- **メールサービスでの運用**
  - 複数ドメインを扱う場合にはお隣さん問題に注意
    → それぞれの送信メールが正しい送信者情報を利用しているか確認
  - 転送時の PRA (Resent-* ヘッダ) 付加，リバースパスの書き換え (タグ付きによるループの回避)
  - DNS とメールサービスが分離されている場合のサポート
    → SPF/Sender ID: “include” 用の SPF レコードを提供
    → DKIM: “_domainkey” サブドメインの委譲や設定用公開鍵の提供

迷惑メール対策の取り組み – JEAG

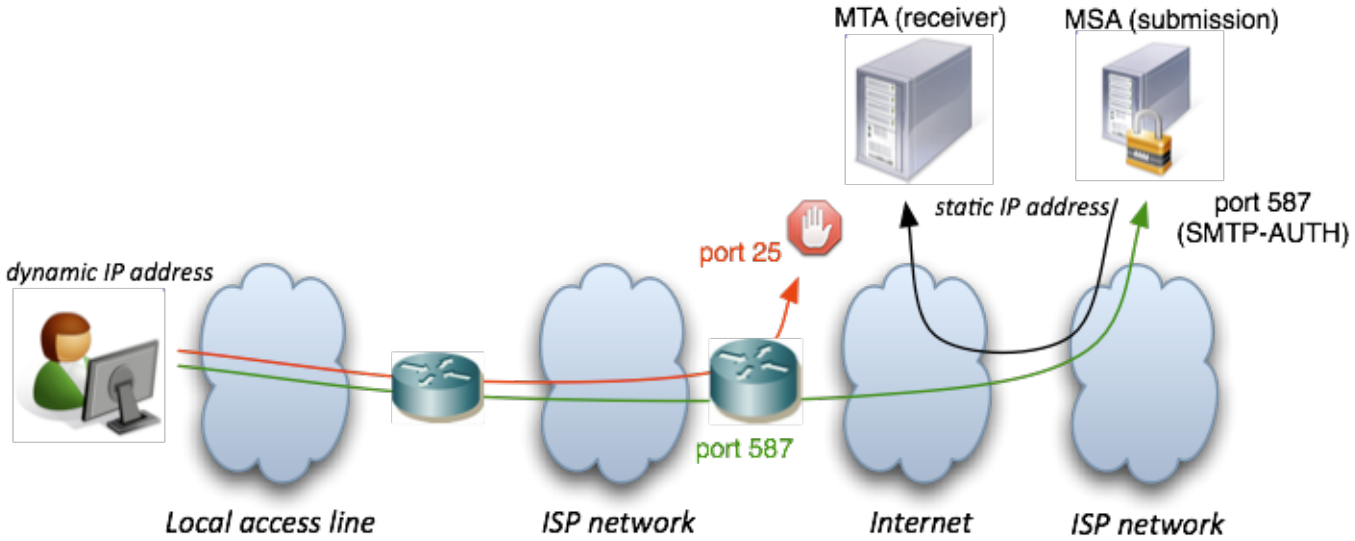
- **JEAG (Japan Email Anti-Abuse Group)**
  - MAAWG の設立 (2004.1.19) を背景として 2004 年から有識者間で活動
  - 発起人 6社により正式に発足 (2005.3.15)
  - 主要 ISPs, 携帯電話事業者, ベンダなどメンバ企業 30社で構成
  - オブザーバ: 総務省, 経産省, (財)日本データ通信協会
  - 外部団体, 組織との連携
    - MAAWG (Messaging Anti-Abuse Working Group)
    - APCAUCE (Asia Pacific Coalition Against 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)**
  - 送信ドメイン認証技術
  - OP25B (Outbound Port 25 Blocking)
  - 携帯電話宛て迷惑メール対策

迷惑メール対策の取り組み – JEAG (cont.)

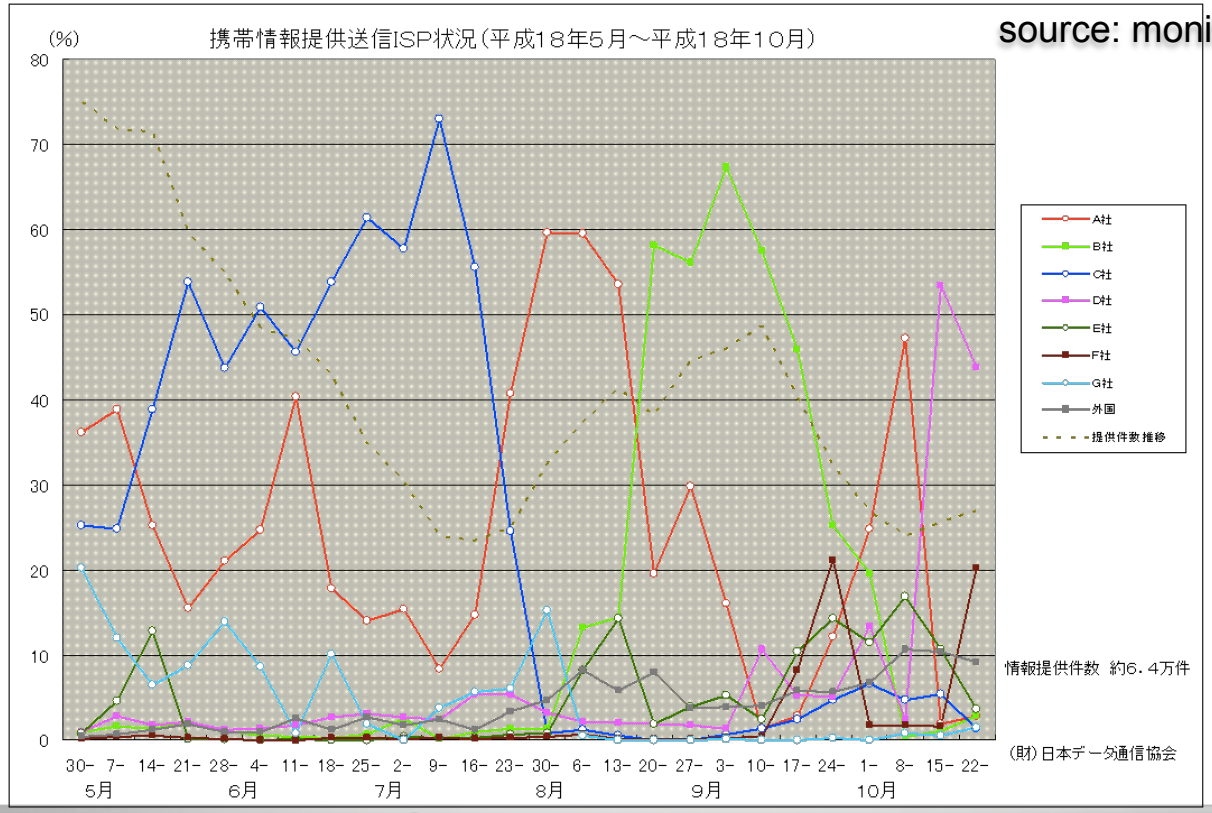
- **OP25B (Outbound Port 25 Blocking)**
  - 迷惑メール送信に使われる動的 IP アドレスからのメール送信 (受信メールサーバの port 25 への直接接続) を一律に規制
  - メール送信には ISP が提供するメールサーバ (投稿サーバ) を利用
  - 送信時は投稿ポート (port 587) を利用し送信者認証 (SMTP-AUTH) を行う
  - 管理元が明確な固定 IP アドレスは規制の対象外
- **導入方法**
  - 適切なアクセスポイントでルータに ACL (Access Control List) などのフィルタルールを導入
  - 十分な利用者周知と段階的な導入を推奨



迷惑メール対策の取り組み – JEAG (cont.)

- **迷惑メール送信者の渡り**
  - OP25B を導入すると迷惑メール送信が行えない
  - 導入していない別の ISP を契約して迷惑メール送信
    ex. C社 → A社 → B社 → D社…
  - ISP は苦情が増えることにより OP25B 導入を早める

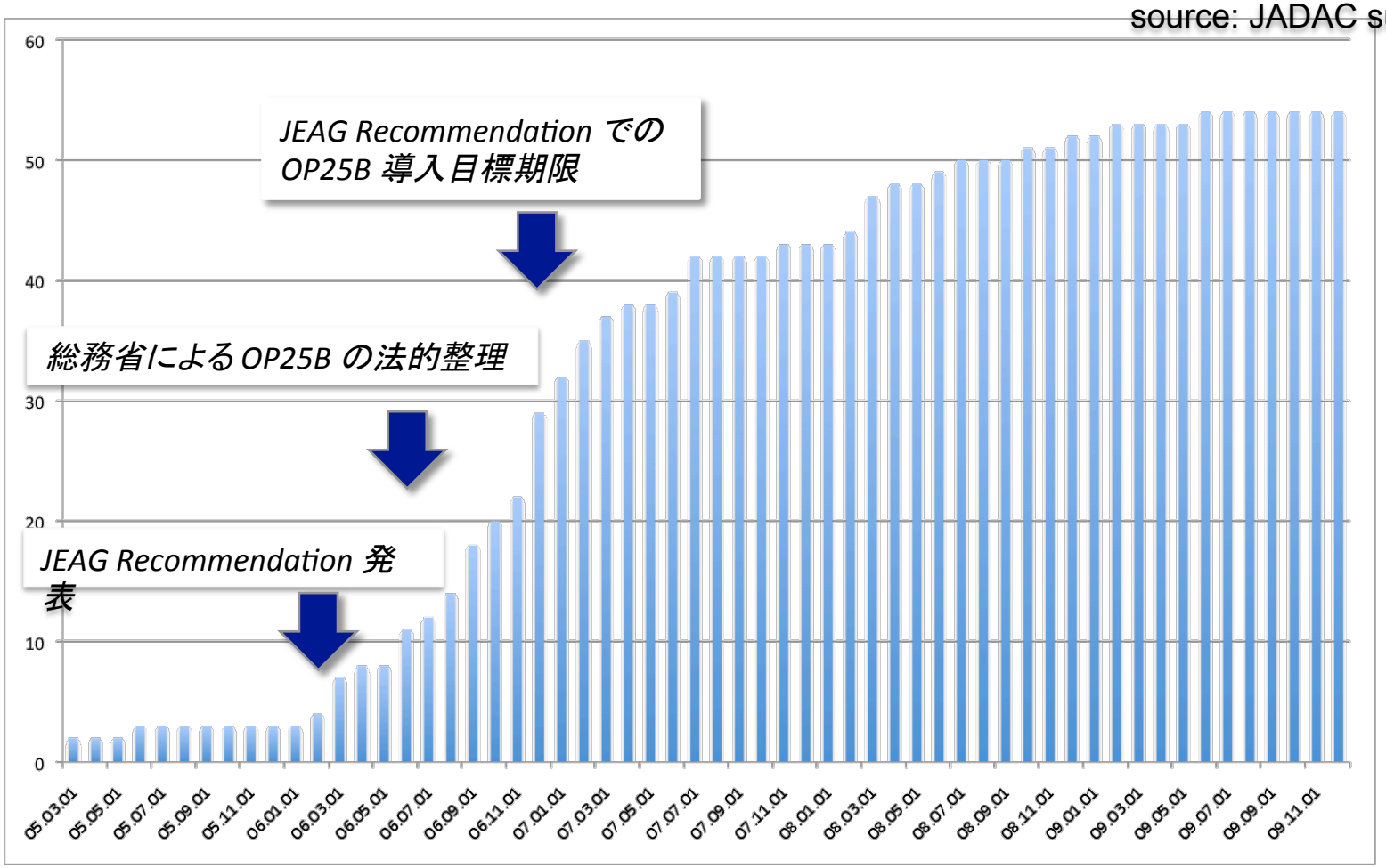
source: monitoring by JADAC



迷惑メール対策の取り組み – JEAG (cont.)

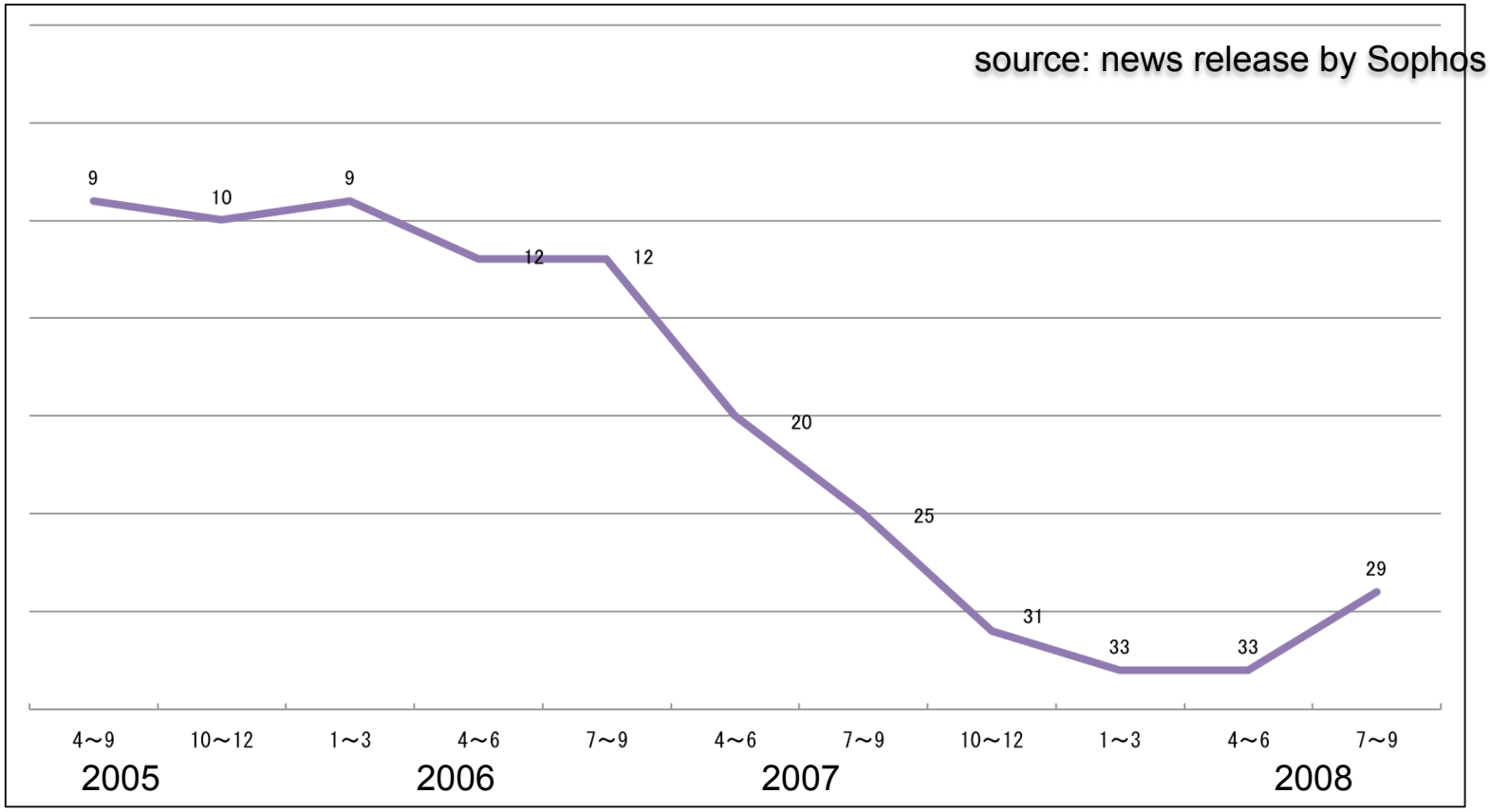
- **導入状況**
  - 日本の ISP での導入数の推移 (2005～2009)

source: JADAC survey



迷惑メール対策の取り組み – JEAG (cont.)

- **導入効果**
  - spam 送信地域ランキングでの日本順位の推移



迷惑メール対策の取り組み – 国際連携

- **MAAWG**
  - 欧米を中心とした約190社の IT 企業による Working Group
  - 年3回開催される General Meeting や mailing list での議論
    - 2010.06.08-10: 19th MAAWG General Meeting @ Barcelona, Spain
    - 2010.10.04-06: 20th MAAWG General Meeting @ Washington DC, USA
  - 分野別のグループ
    - Technical Committee
    - Public Policy Committee
    - Anti-Phishing SIG
    - Botnet/Zombie Subcommittee
    - ISPCC (Closed Coloquium), etc
- **行政主体の多国間グループ**
  - LAP (London Action Plan)
    - 2009.10.07-09: 5th Joint-LAP/CNSA Workshop @ Lisbon, Portugal
  - Seoul-Melbourne MoU Meeting
  - 日ASEAN情報セキュリティ会合
  - ITU, OECD, etc
- **二国間協議**
  - 中国 (中国工業･情報化部, ISC: Internet Society of China)
  - 韓国 (KISA)
  - ブラジル (CGI.br / cert.br)
    - 2010.05.07: Brazil-Japan Anti-Spam Workshop

まとめ

- **迷惑メールの今後**
  - 利益効率が良い間は今後も迷惑メールは増加
  - 新たな送信手法，受け取ってもらうための技術は今後も進化

- **メール利用環境の整備を**
  - 今後は受信側への導入を促進し認証結果を有効活用
  - 詐称されないための対策 (送信ドメイン認証など) はもはや必須
  - メールの疎通は今後も悪化する可能性あり
    → 過度な対策は利便性を低下させる
    → 正しいメールを受け取る仕組み (送信ドメイン認証技術) を活用

- **様々な取り組み**
  - 迷惑メール対策推進協議会による “迷惑メール対策ハンドブック” の発行
  - 迷惑メール対策推進協議会に送信ドメイン認証技術 WG を設置し，普及のための具体的な情報の整理など活動中
  - JEAG (Japan Email Anti-Abuse Group) Recommendation の改訂を検討中
  - MAAWG (Messaging Anti-Abuse Working Group) との実運用上の連携
  - IETF による標準技術の採用と普及

JEAG Japan E-mail Anti-Abuse Group　MAAWG　IETF

IIJ Internet Initiative Japan

ご清聴ありがとうございました

お問い合わせ先　IIJインフォメーションセンター
TEL：03-5205-4466（9：30～17：30 土/日/祝日除く）
info@iij.ad.jp
http://www.iij.ad.jp/

Ongoing Innovation