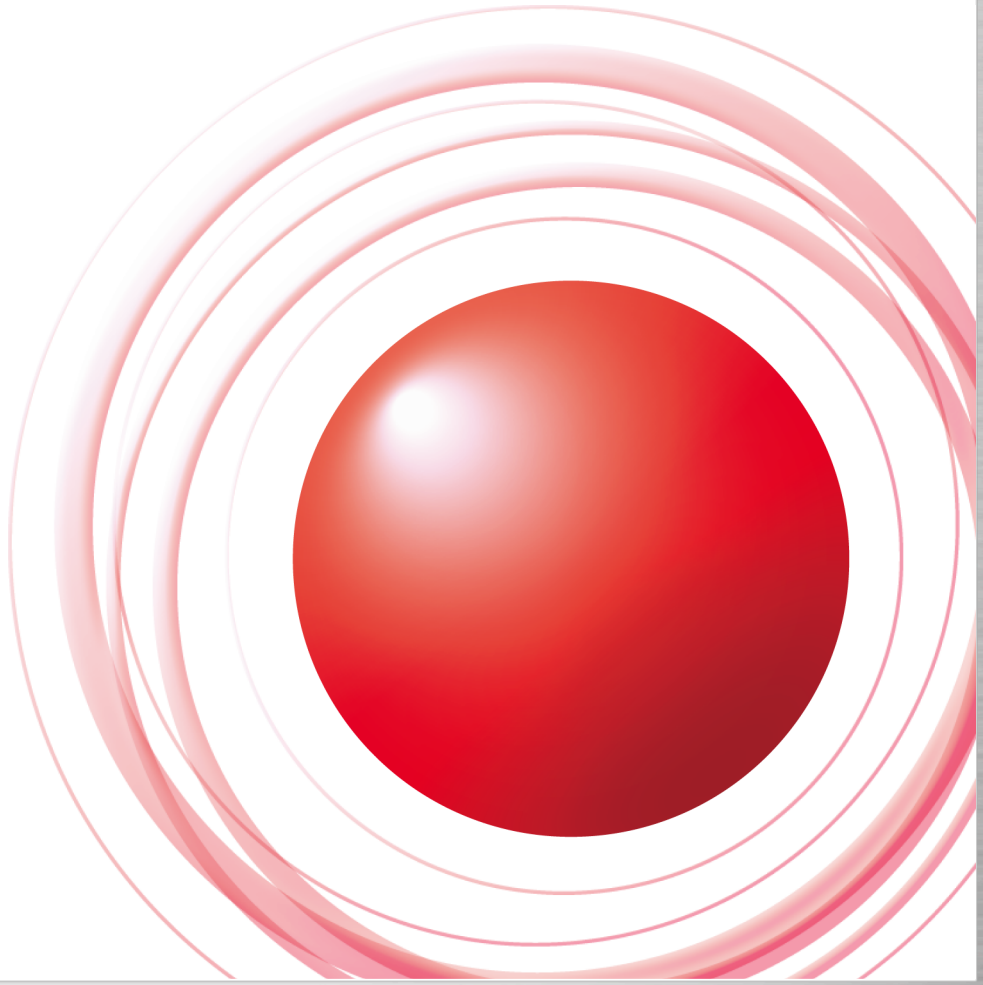
迷惑メール対策セミナー[大阪]

送信ドメイン認証技術の普及に向けて

IIJ Internet Initiative Japan



2009.11.19

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

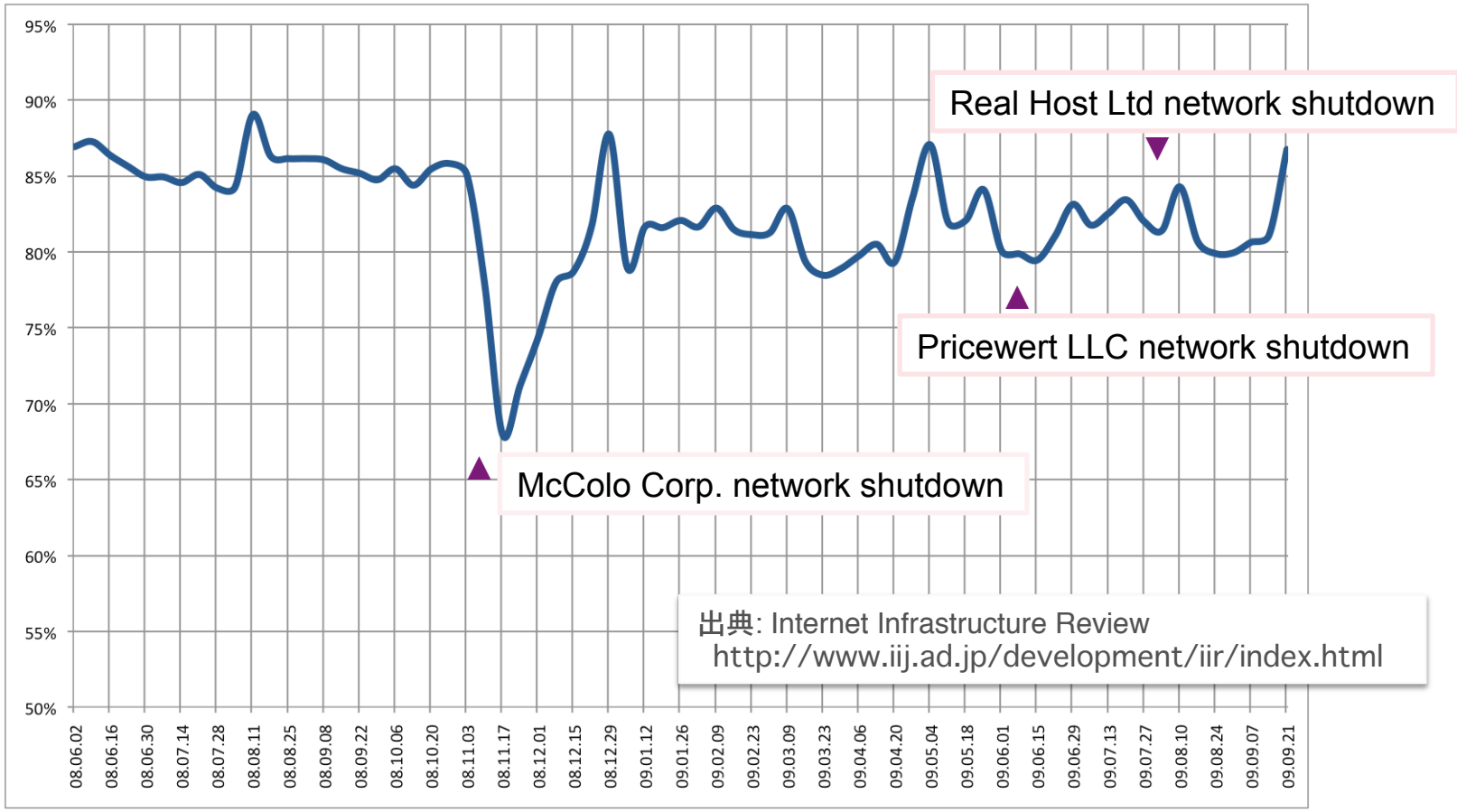
Ongoing Innovation

Agenda

- **迷惑メールの動向**
  - 迷惑メール割合の推移と送信元
  - 送信手法
- **迷惑メール対策**
- **送信ドメイン認証技術**
  - 概要
  - 導入状況
  - SPF レコード / SIDF
  - DKIM
  - 認証結果の利用
- **まとめ**

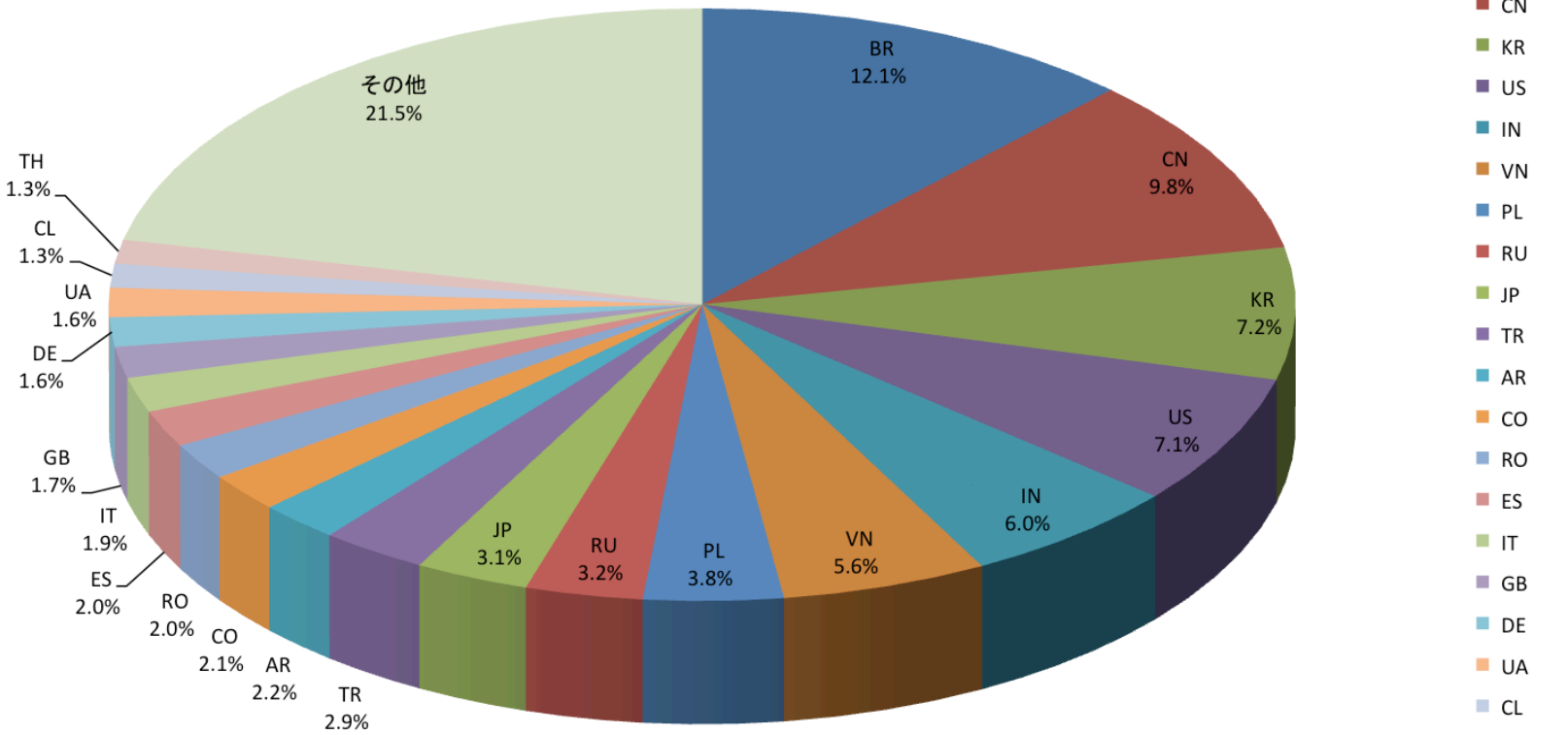
迷惑メール割合の推移

- **調査概要**
  - IIJ が提供している迷惑メールフィルタによる検知率
  - 期間: 2008.06.02 ～ 2009.09.27



迷惑メールの送信元

- **迷惑メールの送信元分布**
  - 迷惑メール判定されたものの一部を国別に分類
  - 期間: 2009.06.27 ～ 2009.09.27



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

迷惑メールの送信手法 - I

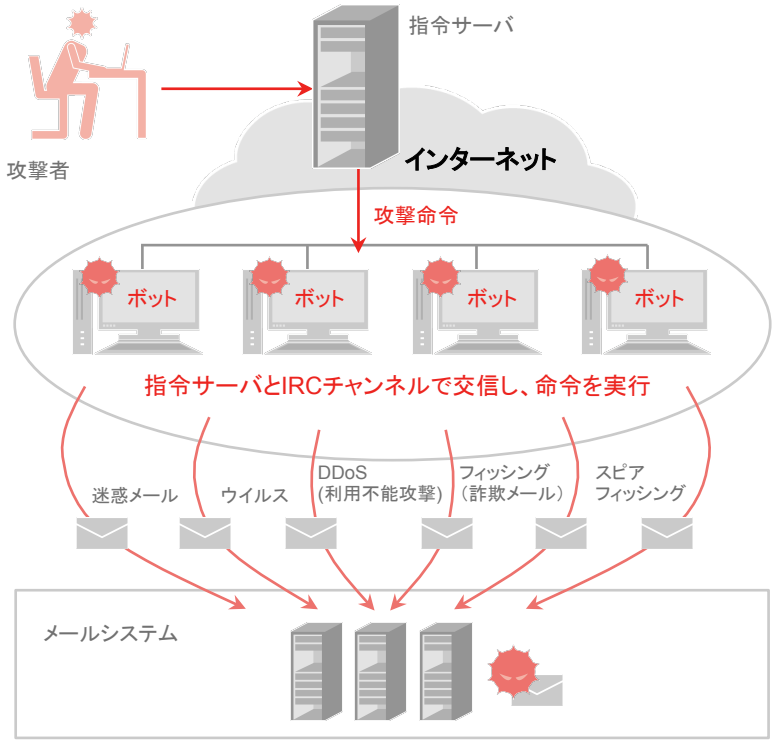
- **全体的な傾向**
  - メールサービスの顧客層にもよるが送信元の大部分は海外発
  - 日本向けの日本語迷惑メールも海外発が多くなっている
  - 迷惑メールの送信元の分散傾向

- **送信手法**
  - 特定の送信元からの大量送信とボットネットを利用した少数分散型
  - 日本国内発は OP25B (Outbound Port 25 Blocking) の導入によりかなり抑えられている → 依然として他の脅威が残されている
  - 分業化と組織化
    - アドレス収集
    - 海外拠点の構築
    - ボットネットの管理と運用
    - 不正プログラム (malware: malicious software) の開発と配布

迷惑メールの送信手法 - II

- **ボットネットの仕組みと手法**
  - 不正プログラム (malware) に感染させることにより外部から制御
  - 迷惑メール送信以外にもDDoS攻撃，ウェブサイトなどにも利用
  - 不正プログラムの配布にメール送信やウェブに悪用 → 増殖
  - 多様な亜種及び急速な広がりに検知がより困難に

- **様々な被害**
  - 個人情報の搾取による正規アカウントの不正取得 → 直接的な金銭被害
  - 正規アカウントを利用した迷惑メール送信 → 踏み台利用
  - 動機 (Less Risk)
    - Less Violence
    - Less Jail Time
    - More Profit



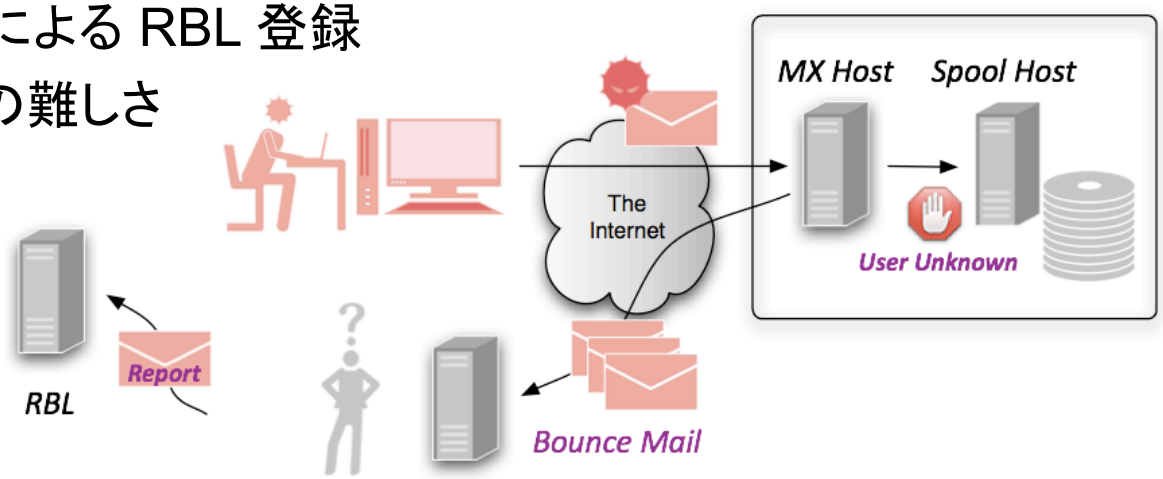
迷惑メール対策 - I

- 安易な対策による弊害
  - RBL (Realtime Block/Black List) 利用による受信拒否
    - 送信元の IP アドレスをリスト化しネットワーク的に接続の拒否や制御を行う
    - 外部組織が集めたデータが DNS の仕組みを利用して参照可能
    - 手間に対する効果は大きいが送信側から苦情が来ないと誤判定がわからない
    - 外部データを利用しない場合でも運用コストは大きい (内容に基づいて自動的に判断する場合など)
    - ホワイトリストによる正規の送信元の管理が必須
  - Greylisting によるメールの遅延や不達
    - 一時拒否を応答することにより再送を促し正規のメールサーバかどうかを判定
    - メール配送の遅延をまねき送信側サーバに負担を強いる (queueing 等)
    - 迷惑メール送信側も対策することが可能
  - エラーメール (Bounce Mail) の一律送信拒否や受信拒否
    - 迷惑メール送信者は到達性を確保するために実在するドメイン名を詐称
    - 宛先メールアドレスが存在しない場合も多いため (DHA: Directory Harvesting Attack) 宛先不明のエラーメール (bounce mail) が大量に発生
    - 詐称に使われる良く知られたドメイン名の場合は膨大な量の bounce mail が送られる
    - このような背景から bounce mail を配送しなかったり受信拒否を行うことによる様々な弊害も発生
    - Bounce mail を迷惑メールと判断することによる送信元の一律受信拒否 (ex. Black List に登録)

迷惑メール対策 - II

- **エラーメールに関する問題**
  - 送信者情報の詐称に利用されることによるエラーメールの大量流入 (後方散乱: backscatter)
  - 迷惑メール配送手段としてのエラーメール利用
  - 内部 PC の不正フログラム感染による迷惑メール送信，外部メールサーバへの転送設定による迷惑メール送信

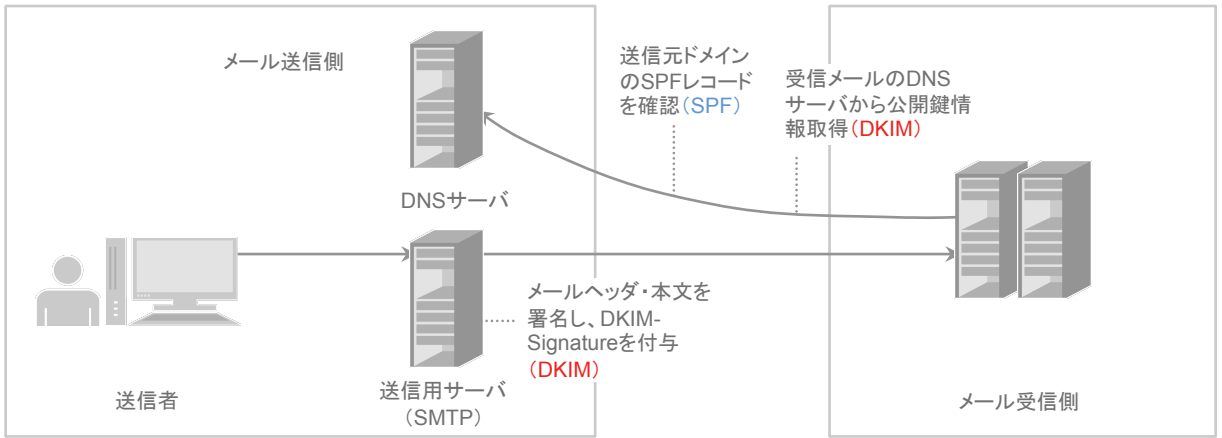
    → 評判 (reputation) 低下や RBL 登録
  - エラーメール送信による RBL 登録
  - RBL の登録解除の難しさ



→ **正しいメールがきちんと到達できる環境作りが必要**

送信ドメイン認証技術 – 概要 I

- **基本的な仕組み**
  - 送り手は送信元を明確に表明
  - 受け手は送信元情報が正しく表明されているか確認
  - 迷惑メールを判定する技術ではなく送信者情報を認証する技術
- **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上位互換を維持
  - DNS の利用により第三者認証機関が不要
  - 仕組みの違いによる複数の認証方法 (SPF/SIDF, DKIM)



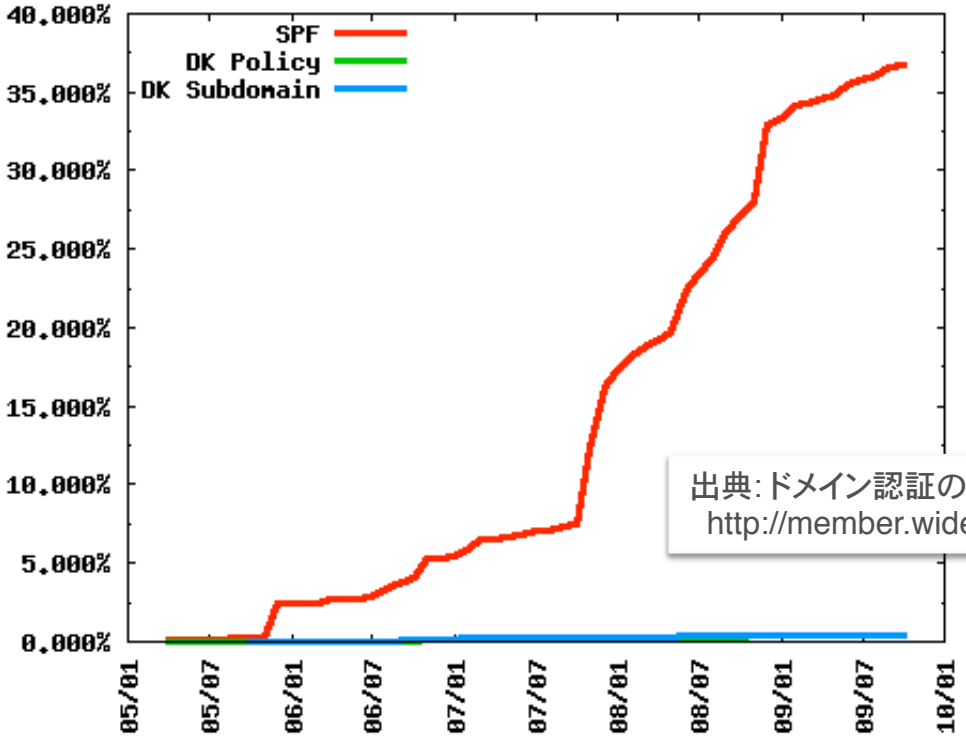
送信ドメイン認証技術 – 概要 II

- **送信元を確認する手法の違いによる二つの認証技術**
  - 送信元をネットワーク的に判断 (SPF: *Sender Policy Framework*)
    SPF (RFC4408), SIDF (RFC4406, RFC4407)
  - 電子署名を利用 (DKIM: *DomainKeys Identified Mail*)
    DKIM (RFC4871, RFC5672), ADSP (RFC5617)

- **それぞれの特徴**
  - メール送信側と受信側それぞれの対応が必要
  - 取り出す送信者情報の種類，認証の方式に違い
  - 導入コストに大きな差 (特に DKIM の送信側)
  - それぞれ長所と短所があり相互補完的に利用可能
  - いずれも導入の有無に関して，既存のメール配送の仕組みに影響を与えない

送信ドメイン認証技術 – 導入状況 I

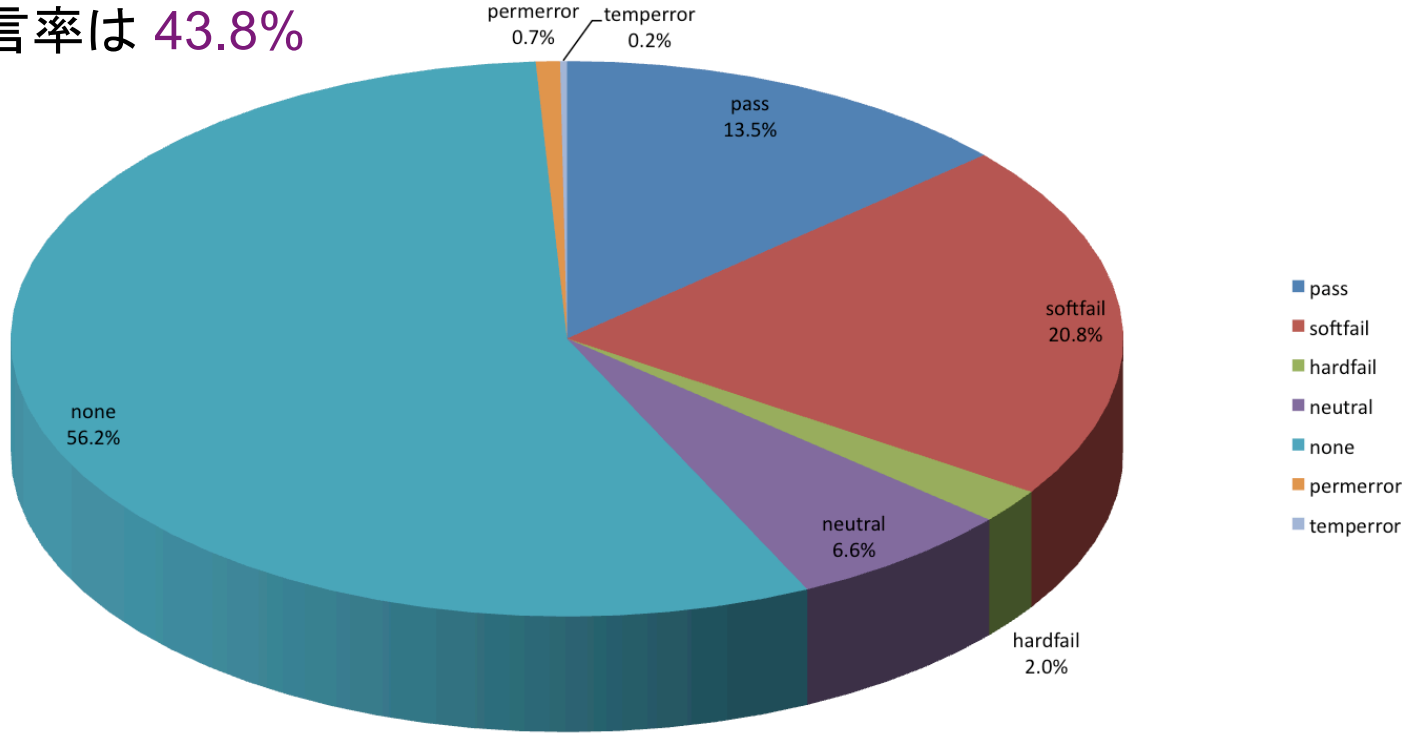
- **日本の導入状況**
  - WIDE プロジェクトと JPRS による共同研究による調査
  - 2009年10月時点で “jp” ドメインの SPF 宣言率は 36.79%
  - “co.jp” ドメインについては 43.21%



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

- 量流ベースの調査 - I
  - IIJ のメールサービスでの認証結果の割合 (SPF)
  - 期間: 2009.09.01 ～ 2009.09.30
  - 宣言率は 43.8%



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

送信ドメイン認証 – SPF レコード I

- **SPF レコードの概要**
  - 送信側は対象とするドメインに SPF レコード (TXT RR) を記述
  - 記述内容はテキスト (ASCII 文字列)
  - 先頭はバージョン番号 (“v=spf1”) から始める
  - 対象ドメインが送信されるメールサーバ (最終出口) を IP アドレス (CIDR 含む) やホスト名など DNS 情報を利用して記述
  - 区切りは空白 1文字 (0x20)
  - 先頭 (左側) から順番に解釈され，メール受信時の送信元 IP アドレスが適合する部分の条件 (qualifier) が認証結果となる
  - SPF レコードを記述する送信側が認証結果を決める

例 (実際とは異なります)

```
iij.ad.jp    TXT  “v=spf1 +ip4:192.0.2.1 +ip6:2001:db8::1 -all”
```

送信ドメイン認証 – SPF レコード II

- SPF レコードの構成要素
  - 送信メールサーバの情報を機構 (mechanism) により指定
    - `a:` A レコードで示される IP アドレス (CIDR の幅を指定可)
    - `mx:` MX レコードで示されるホストを参照 (CIDR の幅を指定可)
    - `ptr:` 接続元 IP アドレスの逆引きが指定された (上位) ドメインとの整合性
    - `ip4:` 指定された IPv4 アドレス (CIDR の幅を指定可, ex. "/24")
    - `ip6:` 指定された IPv6 アドレス (CIDR の幅を指定可)
    - `all:` 全てに適合 (それ以外の場合に利用, 詐称時の結果)
    - `exists:` 指定されたドメインが存在する場合 (DNSBL などに利用)
    - `include:` 入れ子構造を参照
  - 接続元 IP アドレスが上記範囲に含まれる場合に認証結果が得られる
  - 認証結果は機構前の限定子(qualifier,"+–~?"のいずれか), 省略時は "+"

- SPF の多重構造
  - 他のドメインの SPF レコードを参照することができる
    - `include:` 指定された ":" に続くドメインの SPF レコードを再帰的に評価
      pass 以外は見つからなかったことになる
    - `redirect:` 全て fail した場合に "=" に続くドメインを評価

送信ドメイン認証 – SPF レコード III

- **SPF レコードの注意事項**
  - 受信側にとって DNS の参照 (lookup) は負荷の増大につながるため最小限の lookup にとどめるべき (`"ip4"` or `"ip6"` で済めばそれが better)
  - SPF の仕様では DNS 参照の上限は10回 (`include` なども含む)
  - `"mx"` や `"ptr"` レコードの利用は DNS 参照を増加させる
  - 参照先が設定変更する可能性があるので，管理外のホスト名を勝手に記述したり SPF レコードを `"include"` しない

- **メールの送信出口の確認**
  - 対象ドメインのメールがどこから出ているのかを把握
  - 地方拠点や外部委託しているアナウンスメール等も要注意
  - メール配信業者やホスティング業者は，include 用の SPF レコードを用意するべき
  - 送信者情報 (From) に設定可能なドメインは制限させる

送信ドメイン認証 – SIDF

- **SIDF (Sender ID Framework) 概要**
  - 基本的な仕組みは SPF と同じ
  - 送信者情報に配送上の送信元 (envelope from) ではなく PRA (Purported Responsible Address) を利用
  - PRA はメールヘッダ情報のうち，以下の順番で取得

    Resent-Sender: → Resent-From: → Sender: → From:
  - SPF レコードのバージョン番号が異なる (他の項目は同じ)

    “v=spf1” → “spf2.0/mfrom,pra”

- **利点と欠点**
  - メール受信者にとって表示可能な情報を利用するのでわかり易いが，MUA が必ずしも表示しないヘッダの優先順位が高い
  - 転送時にヘッダを付加すれば認証は失敗しない
  - メール本文 (ヘッダ) を受信するまで認証ができない
  - 転送時にヘッダを付加する MTA はほとんどない
  - envelope-from 及び ヘッダ from (PRA) がそれぞれ異なった場合の判断基準の問題，送信側のポリシー設定の問題

送信ドメイン認証 - DKIM

- **DKIM (DomainKeys Identified Mail) の概要**
  - Yahoo! 社の DomainKeys と Cisco 社の IIM (Identified Internet Mail) を統合した技術, RFC4870 として標準化 (改訂部分 RFC5672)
  - 電子署名技術を利用し，メールが正しい送信元から送信されているか，内容が改ざんされたメールでないことが認証可能
  - 電子署名を検証するための仕組みとして，第三者機関 (S/MIME など) や公開鍵の事前配布 (PGP/MIME など) を必要としない
    → DNS 上に公開鍵を設置
  - DKIM に対応していない送信者あるいは受信者でも，不便を感じない (メールが見にくくなったりしない)

- **技術的概要**
  - ハッシュ関数と公開鍵暗号技術を利用 (rsa-sha1, rsa-sha256 は標準で対応が必要)
  - 署名情報は DKIM-Signature: ヘッダに記述 (対象ヘッダ，公開鍵の取得先，正規化方法，署名情報, etc)

送信ドメイン認証技術 – SPF/DKIM 認証結果の利用 I

- **迷惑メールフィルタでの利用**
  - 認証結果だけで迷惑メール判定は難しいが参考情報としては有益
  - 最近は none ドメインが増えている → SPF レコードの記述率が増加しているのでそろそろ none ドメインの評価を下げても良いのでは
  - 悪質な pass ドメイン (どこから送信されても pass するような SPF レコード) 自体の評価見直し
- **ドメイン White List (reputation)**
  - IP Black List より一般的に情報量が少なくて済む
  - 利用環境によっては誤認証が発生しないケースも (ex. 携帯電話)
- **転送問題の緩和**
  - 転送者と転送先 (最終受信者) はほぼ同一人物
  - 受信者が White List を個別設定 (無条件に受け取る送信元を設定)
  - White List 設定にも SPF レコードを利用 (IP アドレスよりはシステム変更に関して柔軟)

送信ドメイン認証技術 – SPF/DKIM 認証結果の利用 II

- **Backscatter 問題への対応**
  - 送信者情報が詐称されている (“fail” or “softfail”) 送信者へは bounce mail (エラーメール) は返す必要はない
- **MUA との連携によるフィルタリング**
  - ISP では認証結果をラベリング (RFC5451, Message Header Field for Indicating Message Authentication Status)
  - MUA (Mail User Agent) の機能を用い受信者がフィルタリング

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

- **FBL への応用**
  - FBL (Feedback Loop) とはメール受信者から送信側への苦情等の申し立て
  - 送信事業者からみるとリストからの削除 (opt-out) や苦情の識別，送信間隔の調整等に役立てることができる
  - 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
  - ARF (Abuse Reporting Format) 形式であればヘッダ情報を含めた送信メールが返される
    → DKIM ヘッダが付加 → DKIM 再認証 → 自身のメールかを検証可能
    → 送信側は DKIM を導入し検証可能に!

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**
  - 受信側の対策だけでなく送信側にも注意
  - 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 → 正しい受信対策を

- **様々な取り組み**

JEAG Japan E-mail Anti-Abuse Group　MAAWG

  - 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 2009” の発行 (2009.10.09)
  - 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 (2009.10.02), 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 の改訂を計画中
  - MAAWG (Messaging Anti-Abuse Working Group) や IETF とも連携した標準技術の採用と普及

IIJ Internet Initiative Japan

ご清聴ありがとうございました

Ongoing Innovation