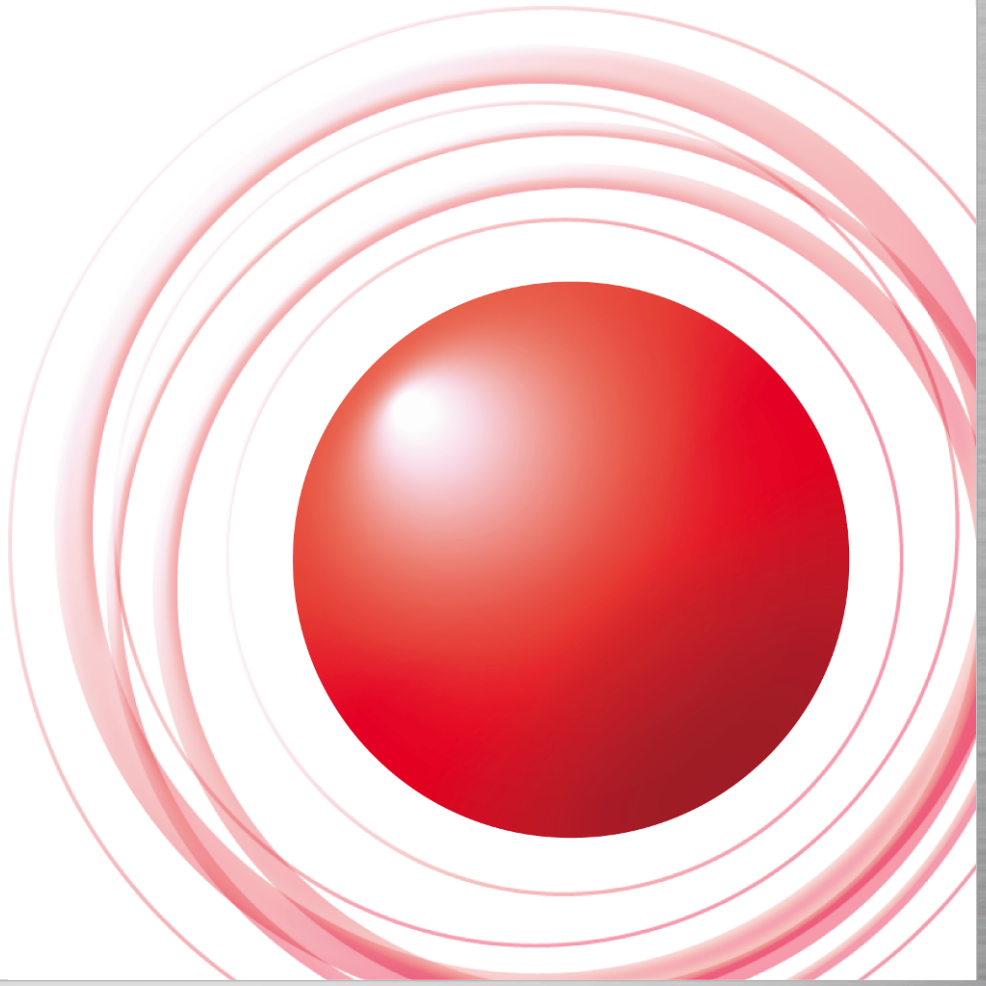
第7回迷惑メール対策カンファレンス

JEAG Updates: 送信ドメイン認証技術の普及に向けて

IIJ Internet Initiative Japan



2009.05.19

櫻庭 秀次 *(SAKURABA Shuji)*

Internet Initiative Japan Inc.

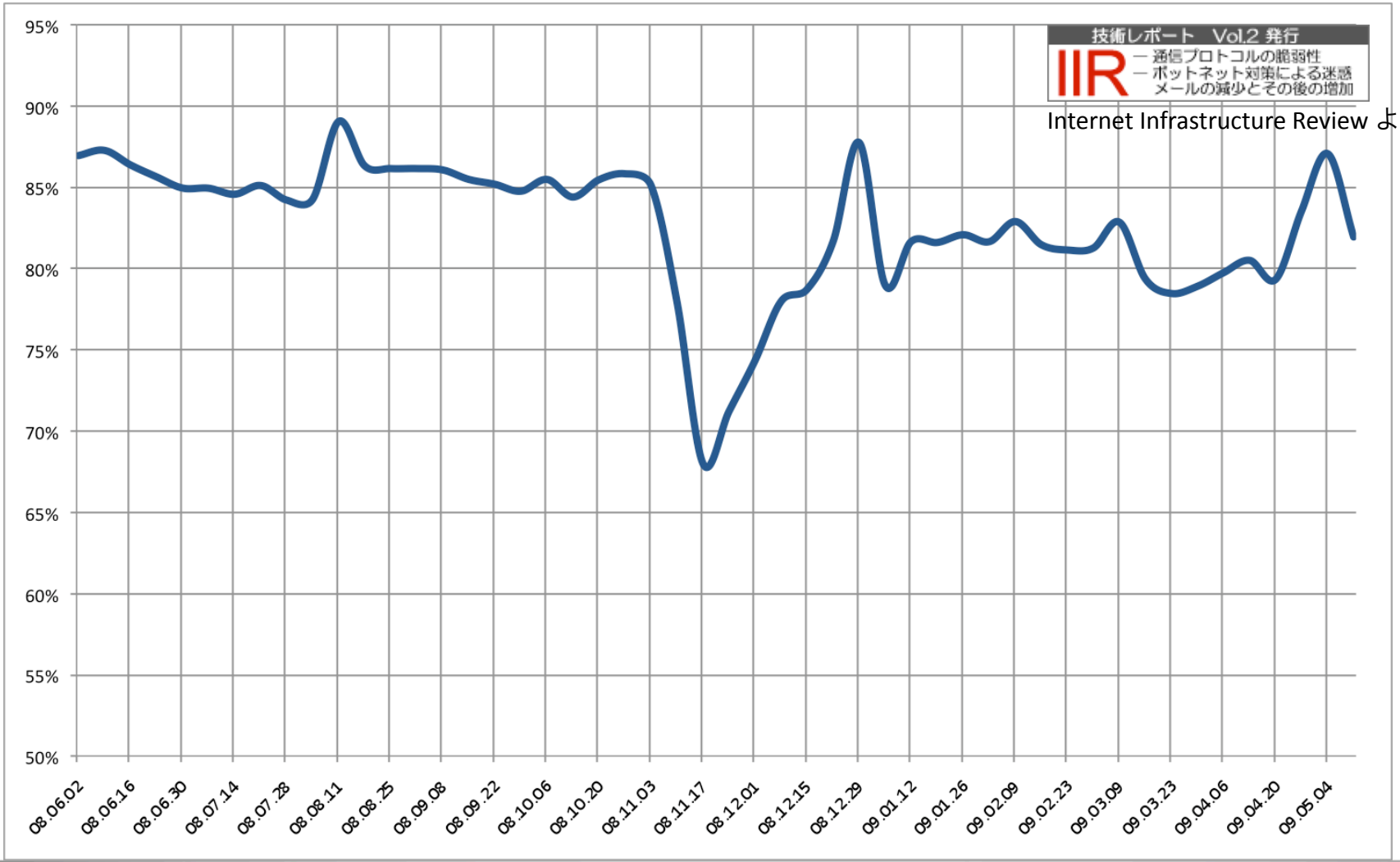
Ongoing Innovation

Agenda

- **迷惑メールと送信ドメイン認証技術**
  - 迷惑メールの現状
  - 迷惑メール対策の難しさ
- **送信ドメイン認証技術**
  - 概要
  - 導入状況
  - 導入に向けての課題
  - 解決案
  - 認証結果の利用
- **まとめ**

迷惑メールの現状 - I

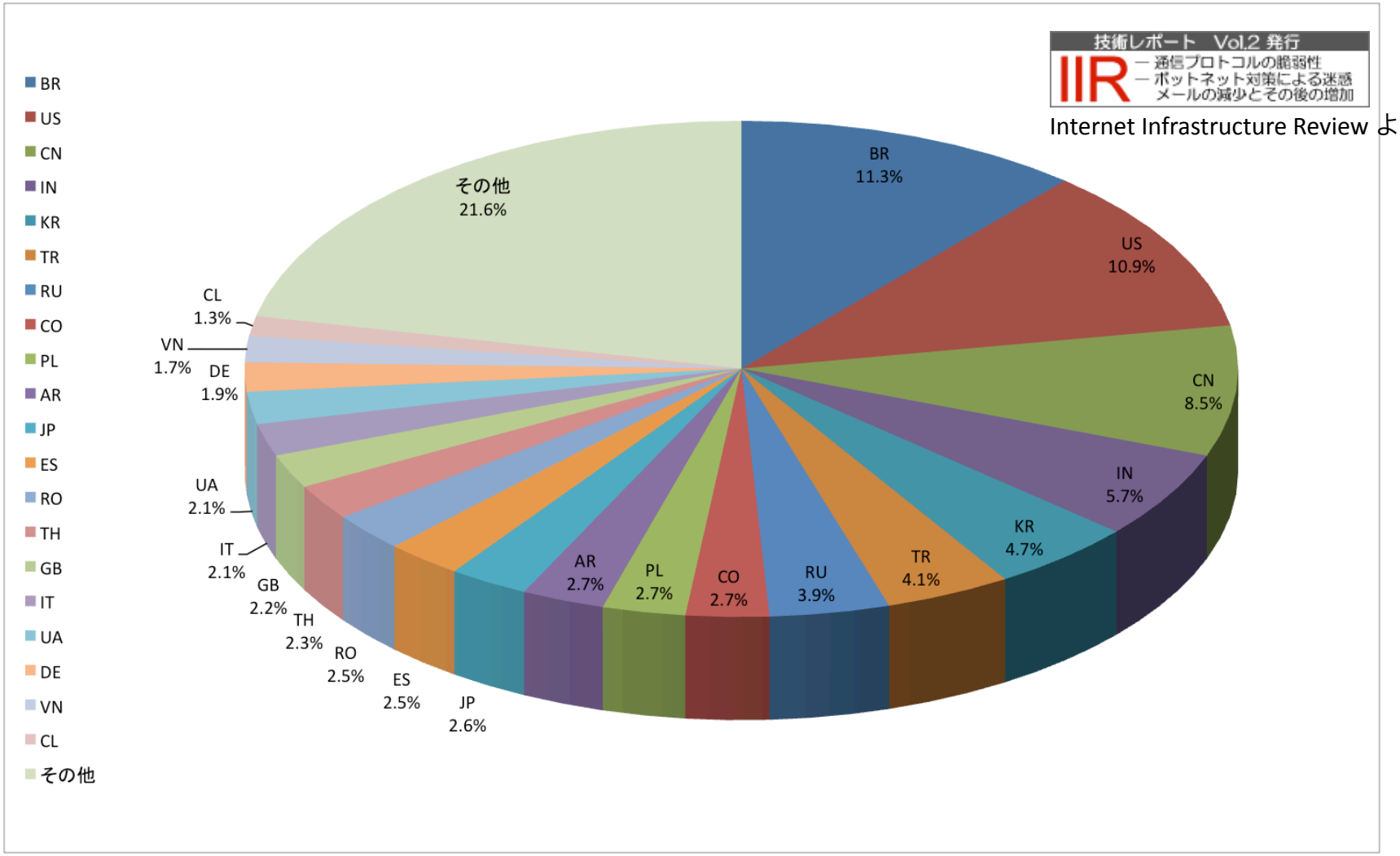
- **迷惑メールの割合の推移 (2008.06.02 - 2009.05.17)**



Internet Infrastructure Review より

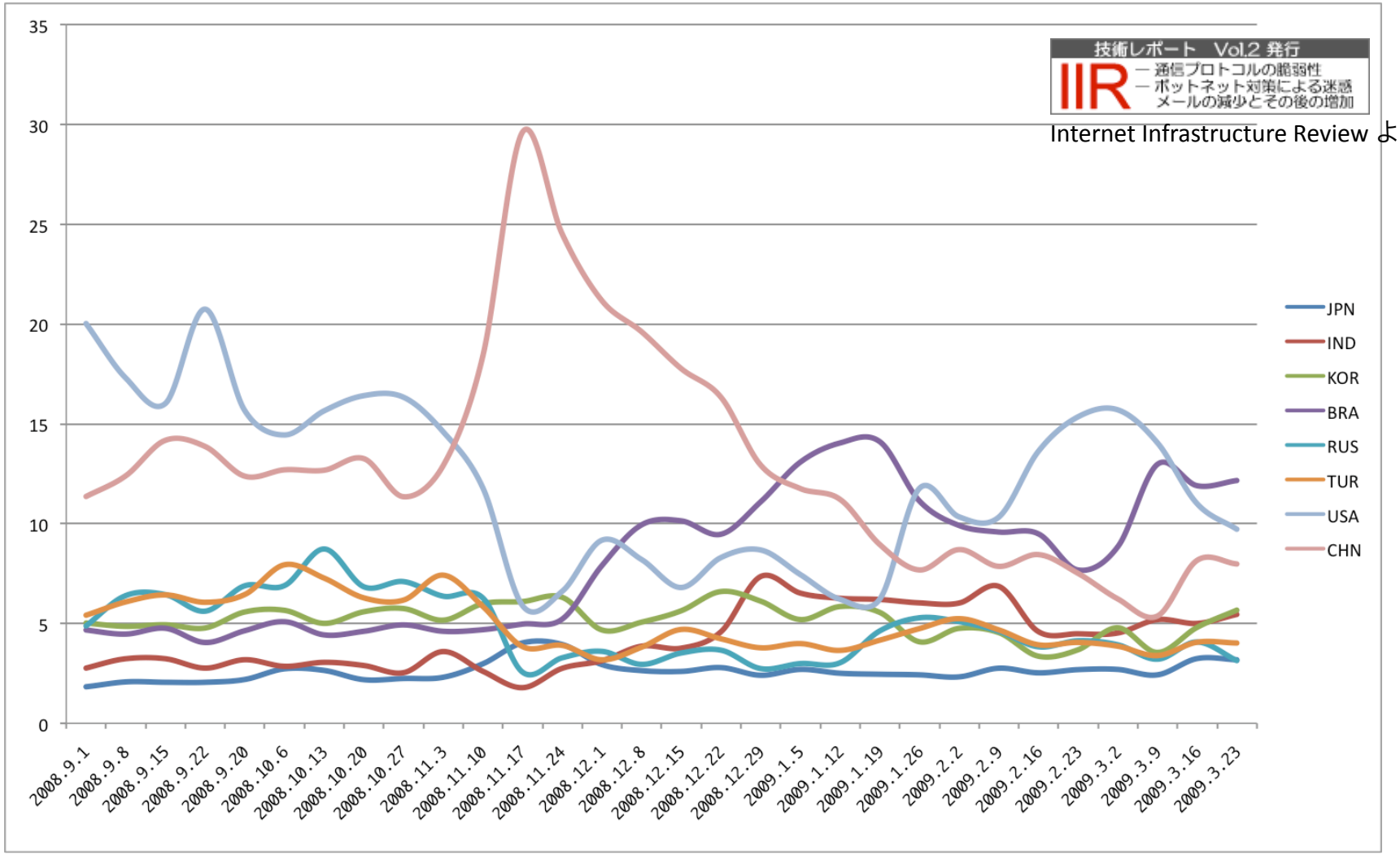
迷惑メールの現状 - II

- **迷惑メールの送信元分布 (2008.12.29 – 2009.03.29)**



迷惑メールの現状 - III

- **迷惑メールの主要送信元の割合の推移 (2008.09.01 – 2009.03.23)**

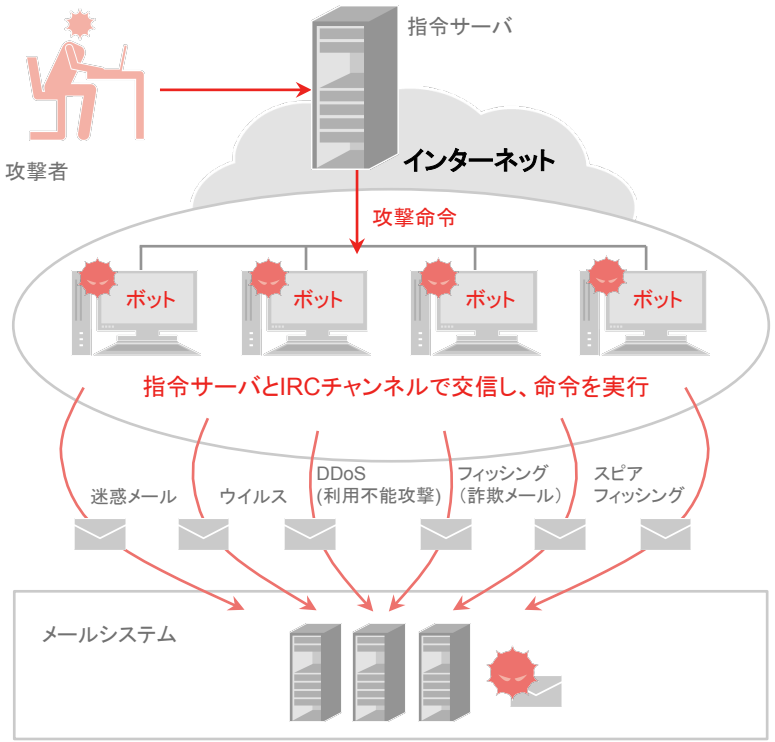


Internet Infrastructure Review より

迷惑メール対策の難しさ - I

- **送信手法の高度化**
  - Botnet (Zombie PCs) を利用した少量大規模分散
    → RBL (Realtime Black/Block List) では対応が難しい
  - 送信元の多くは海外 (Botnet, 海外への送信拠点の移動)
    → 苦情先，管理元が不明
  - ISP/ESP のメールサーバーを踏台に利用する Reputation Hijacking

- **コンテンツの巧妙化**
  - 巧妙な画像添付 spam
  - URL による Web Site への誘導
  - 誘導先ドメインの巧妙化 (Fast Flux)
  - メールマガジンや SNS に似せる等ソーシャルテクニックの駆使



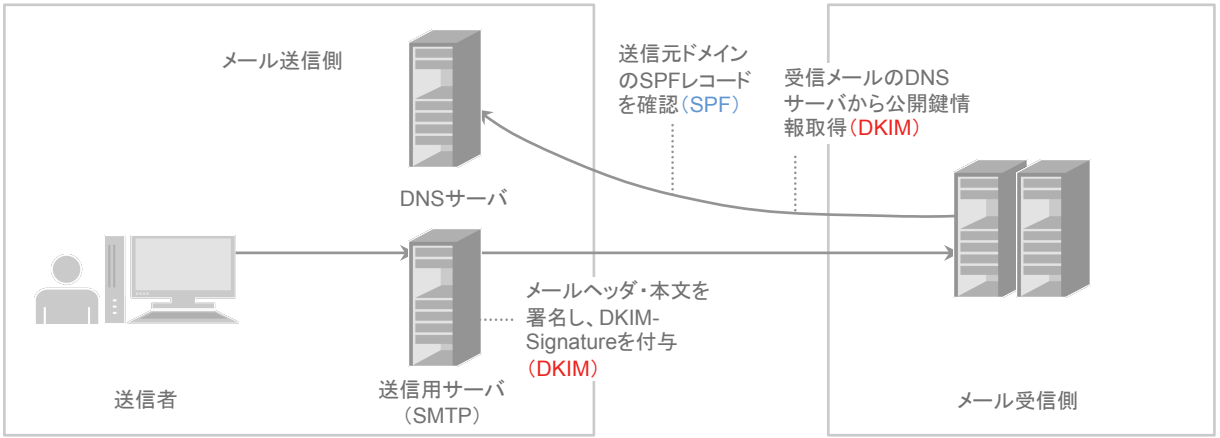
迷惑メール対策の難しさ - II

- **安易な対策による弊害**
  - RBL (Realtime Block/Black List) 利用による受信拒否
    - → IP アドレスベースの受信拒否は手間に対対する効果が一見大きいが，送信側からの苦情が来ないと誤判定がわからないなど弊害も大きい
      メール内容に基づいて自動的に BlackList 化するような仕組みも危険 (共有型サービス等)
  - Greylisting によるメールの遅延や不達
    - → 応答コードとして一時拒否を返すことにより再送を促すことにより正規のメールサーバかどうかを判定する greylisting は一時的な対策．送信側は技術的にいくらでも対応可能．むしろメールの利点である即時性や不特定からの受信などを損なう場合が多い
  - 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する場合が多いため，宛先不明の場合に詐称元に bounce mail が送信される．有名ドメインの場合は膨大な量となるため bounce mail の受信拒否が行われる
      拒否の仕方によっては送信元にメール (bounce mail) が滞留するため，メールシステムの構成によっては通常のメール配送にも影響を与えてしまう

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 (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
- **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)



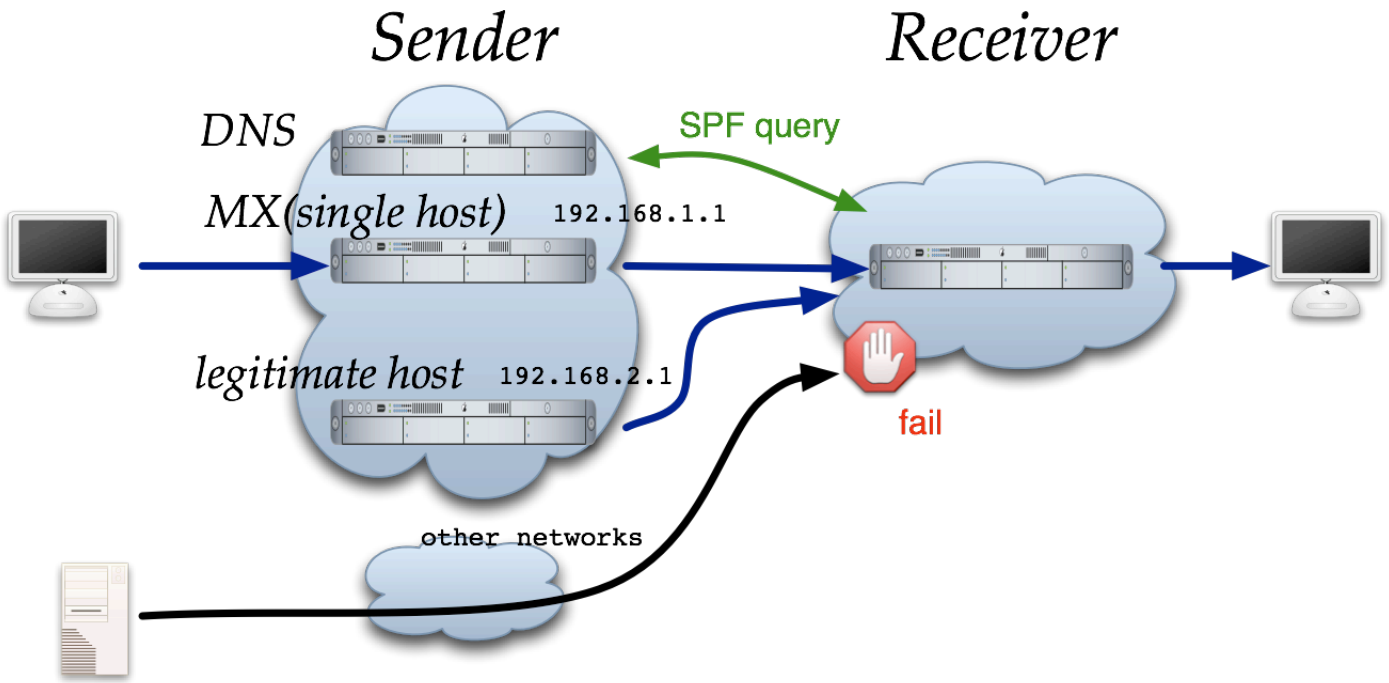
送信ドメイン認証技術 – 概要 II

- **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), ADSP (draft-ietf-dkim-ssp-09.txt)

- **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 – SPF / Sender ID

- **概要**




```
jeag.jp      TXT   "v=spf1 +mx +ip4:192.168.2.1 -all"
jeag.jp      MX    mx.jeag.jp
mx.jeag.jp   A     192.168.1.1
```

送信ドメイン認証技術 – SPF / Sender ID

- **主な違い**
  - SPF は配送上の送信者情報 (envelope from, SMTP MAIL コマンド) を利用
  - Sender ID は上位互換 (SPF と同じ envelope from も利用可能)
  - Sender ID は送信者情報に PRA (Purported Responsible Address) も利用可能
  - 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:
  - 送信側が SPF レコードのバージョンでどちらかを指定 (両方指定することも可能)
  - SPF レコードのバージョン番号の違い
    SPF: “v=spf1”
    Sender ID: “spf2.0/mfrom,pra”
- **それぞれの特徴**
  - Sender ID はメール受信者が表示可能なヘッダ情報を利用するのでわかり易い
    ⇔ PRA を標準で表示する MUA が少ない，認証結果をヘッダとして残せば表示可能
  - Sender ID は転送元ドメインを PRA　ヘッダに記述すれば認証の失敗は無い
    ⇔ 転送時に PRA ヘッダを付加する MTA はまだ少ない
  - SPF は SMTP 上本文を取得する前に認証判断が可能
    ⇔ 本文を受け取る場合，最後まで受信するまで応答コードが返せない
  - 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

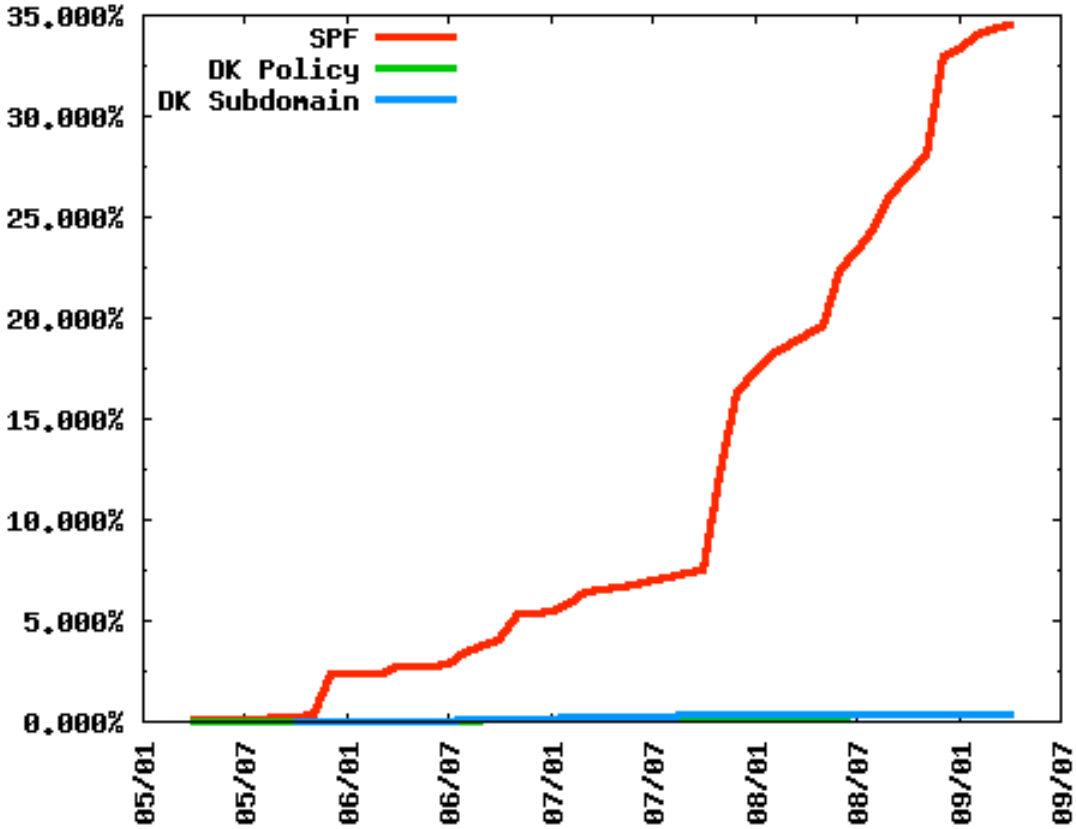
送信ドメイン認証技術 - DKIM

- **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
  - 公開鍵暗号技術を利用し秘密鍵を持っている送信側でなければ作成できない電子署名を付加することで送信元を特定
  - 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**
  - ハッシュ値と公開鍵暗号技術を利用 (rsa-sha1, rsa-sha256 は必須)
  - 署名情報は DKIM-Signature: ヘッダに記述，タグ (key=value) で各パラメータを設定
  - メールヘッダと本文それぞれでハッシュ値を計算
  - 本文のハッシュ値を “bh=“ タグに格納，ヘッダのハッシュ値は “b=“ タグに格納 (DKIM-Signature: ヘッダは必須)
  - 公開鍵の取得方法 (q=dns/txt)，ドメイン名 (d=example.net)，セレクタ名 (s=brisbane) は DKIM-Signature: ヘッダに記述

brisbane._domainkey.example.net

導入状況

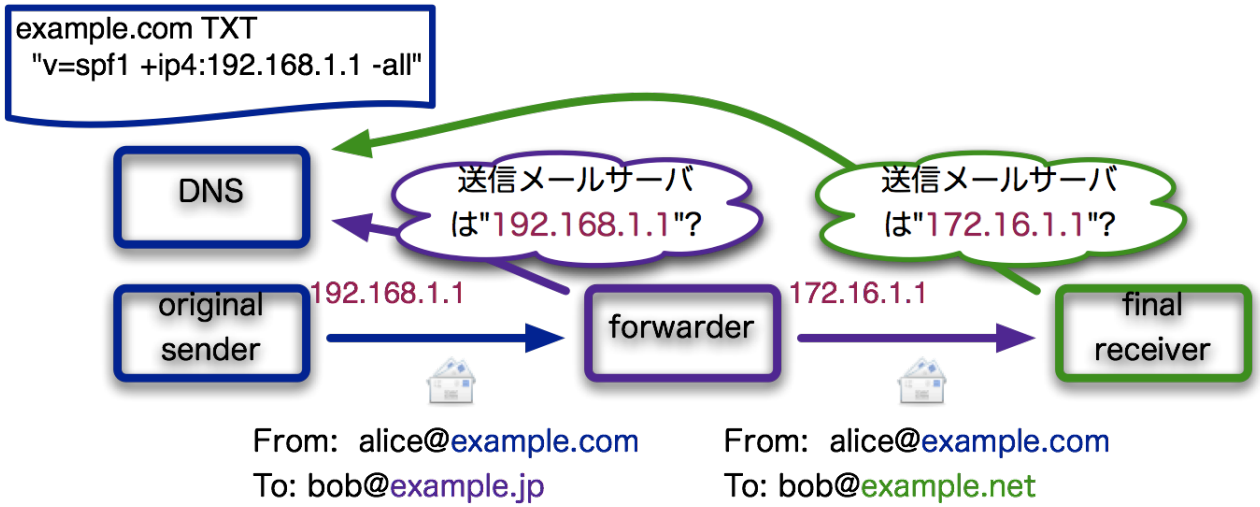
- **WIDE プロジェクトによる jp ドメインの調査結果 (2009.04)**
  - SPF: 34.56 % (co.jp ドメインは 41.65%)
  - DK: 0.37%



URL: http://member.wide.ad.jp/wg/antispam/stats/index.html.ja

送信ドメイン認証技術の課題

- **SPF の転送問題**
  - 通常のメール転送の仕組みでは転送先で認証が失敗する
- **メール転送手順**
  - メール転送とは宛先メールアドレスが一旦したのち設定された転送先メールアドレスへ再配送
  - 転送時ほとんどのメールヘッダは変更されない
  - 転送時配送上 (envelope) の情報は宛先以外変更されない



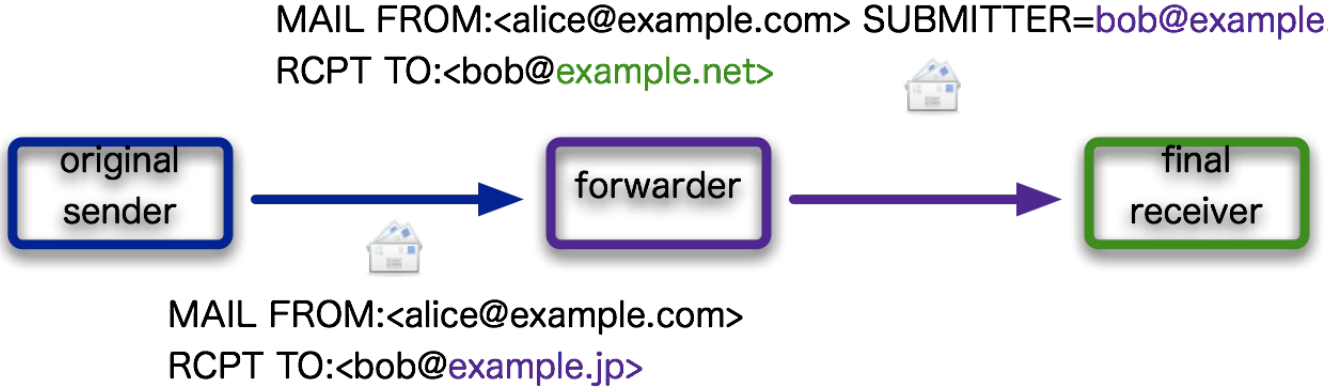
送信ドメイン認証技術の課題 – 解決案

- **背景**
  - SPF は特に送信側の導入が容易であることから高い導入率となっているが，この転送問題のために SPF だけで完全に送信者情報の詐称を防ぐことが難しい
  - メール転送は実際は特定の条件下で行われているレアケースだが，背景を抜きに問題視し広く普及している SPF を利用しないのは残念
  - 解決策を模索する過程で理解を深めて行きましょう

- **注意事項**
  - これまでのもろもろの検討過程から得られた改善案を提示しますが今の段階でどれかを強く推奨するものではありません
  - これまでの経緯の参考として，また今後の議論の参考として提示しているものもあります

解決案 - I

- **Submitter の利用**
  - 直近の投稿者を示す SUBMITTER パラメータが SMTP の拡張機能として提案されている (RFC4405)
  - MAIL コマンドのパラメータとして指定
  - メールの送受信側双方での対応が必要
- **HELO/EHLO ドメインの利用**
  - SPF (RFC4408) で HELO/EHLO のドメイン (identity) を送信者ドメインとして認証することが仕様として決められている
  - RFC4408　にも書かれているが実態としてあまり正しく表明されていない



解決案 - II

- **Sender ID の利用**
  - SIDF (Sender ID Framework) は送信者情報として PRA を利用
  - 転送時に転送元のドメインを正しく優先度の高い PRA をとして追加すれば認証は正しく行われる

    Resent-Sender:

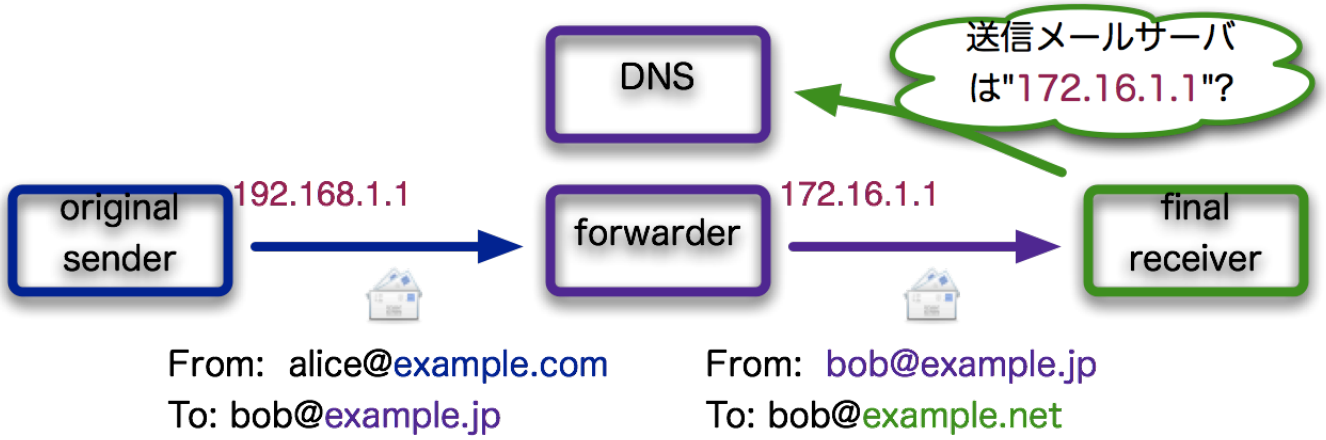
    Resent-From:

    Sender:

    (From:)
  - 転送時に PRA を付けるメールサーバはそれほど多く無いので機能追加が必要になる (場合が多い)
  - 実際に SIDF (“spf2.0/pra”) を宣言しているドメインはそれほど多く無い (ようだ)
  - 受信側の認証処理としては SPF と Sender ID 両方を認証するものが多い

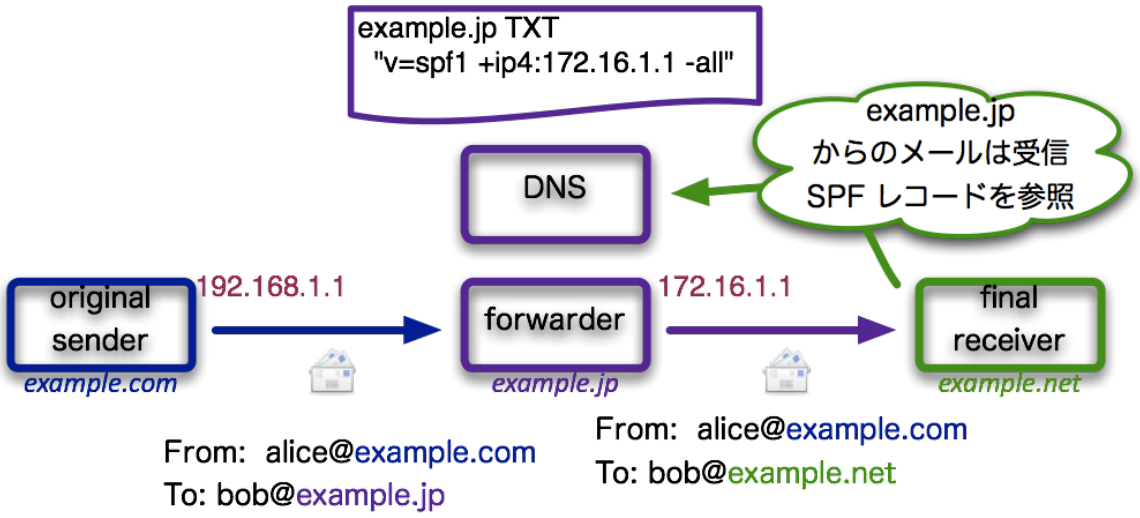
解決案 - III

- **送信元情報の変更**
  - 転送時に送信者情報を転送元のドメインに変更
  - エラーメール (bounce mail) に対しては単純書き換えをしない (loop が発生する可能性が高いため)
  - そのため送信者情報が null (“<>”) の場合，あるいは bounce mail と判断できる場合は転送しないなどの処理が必要
  - 送信者情報書き換え方法の例:
    - SRS (Sender Rewriting Scheme)
    - VERP (Variable Envelope Return Path)
    - BATV (Bounce Address Tag Validation)



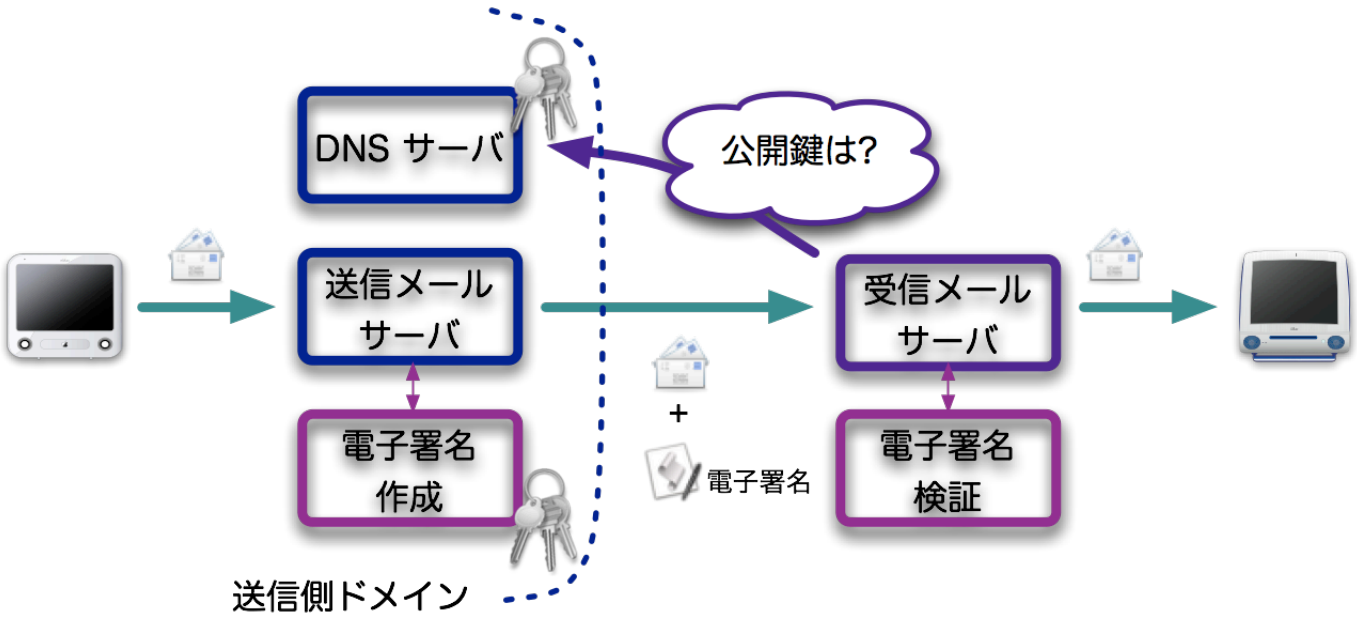
解決案 - IV

- **個別フィルタリング**
  - 転送者と転送先は同一受信者である場合が多い
  - 特定の送信元からのメールは無条件で受信するようなフィルタ設定機能 (white list) を提供できれば受信可能
  - 特定の送信元を判断する手法
    - ヘッダ上の宛先 (cf. 携帯電話などでの宛先指定受信機能)
    - 転送元のメールサーバを white list 登録 (メールサーバの IP アドレスは変更される可能性があるので，転送元ドメインの SPF レコードなどを利用)
  - フィルタ機能の提供及び受信者による設定が必要



解決案 - V

- **DKIM の利用**
  - ネットワークベースではなく公開鍵暗号方式による電子署名により送信者を特定
  - 署名対象部分（本文，ヘッダ）への変更が加えられない限り転送しても正しく認証される
  - 送信側への機能追加が必要

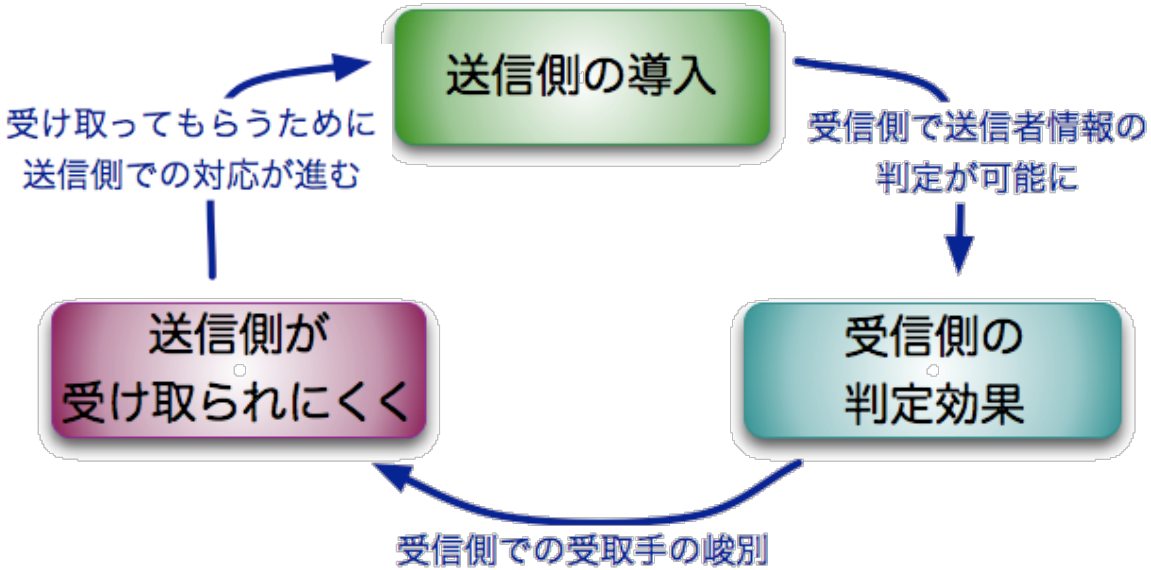


送信ドメイン認証技術の利用 - I

- **SPF / Sender ID**
  - White List 的な使い方: 認証結果の利用, ドメイン単位での受信 (SPF レコードを参照すればドメイン単位で出口が明確)
  - Backscatter 抑制: 認証が失敗した送信元への bounce 抑制
- **DKIM と FBL**
  - FBL (Feedback Loop): 受信者側から送信側への苦情申し立て
  - 正規の送り手としては不要な受信者への送信は抑制したいが, それが正規の受信者からの苦情かどうかの判断が難しい
  - DKIM で電子署名されたメールを (ヘッダ付きで) きちんと返してもらえばそれが正しく送信したメールかどうかが区別できる
  - 例: ARF (Abuse Reporting Format, *draft-shafranovich-feedback-report-07*)

まとめ

- **送信ドメイン認証技術普及のためには以下のサイクルを回していくことが必要**
- **普及率の高い SPF を有効に活用すべき**
- **利用局面に応じた技術対策の利用を**
  - それぞれの長所，短所を把握した上で判断が必要
  - ビジネスで重要な情報をメールで連絡する場合には DKIM の導入を



IIJ Internet Initiative Japan

ご清聴ありがとうございました

Ongoing Innovation