フィッシング対策協議会　説明資料
～Outbound Port25 Blocking ＆ 送信ドメイン認証技術 ～

JEAG Board Member
KDDI株式会社　本間 輝彰
株式会社インターネットイニシアティブ　櫻庭 秀次

※：注意

本資料は、IAJapan主催の第4回迷惑メールカンファレンスのJEAG UPDATEの講演に用いた資料、総務省主催のフィッシング対策推進連絡会等を元に作成しております。

したがって、本資料を引用する際には、その引用元を明確にするようにお願い致します。

第4回迷惑メールカンファレンス（主催：IAJapan）
2．JEAGアップデート迷惑メールの現状とその対策について
講師：櫻庭秀次（株式会社インターネットイニシアティブ）
講師：若松広司（ソフトバンクモバイル株式会社）
講師：赤桐壮人（日本オープンウェーブシステムズ株式会社）
講師：本間輝彰（KDDI株式会社）
http://www.iajapan.org/anti_spam/event/2007/conf0528/program.html

フィッシング対策推進連絡会第9回会合（主催：総務省）
4．**送信ドメイン認証技術の概要と普及促進についてJEAG**（Japan Email Anti-Abuse Group）
講師：櫻庭秀次（株式会社インターネットイニシアティブ）

2005年3月15日設立

電子メールに携わる通信事業者やメーカーの集まり

- 法人格は所有していない
- 現在、３１社が参画

手弁当による運営

- ボランティアベース
- フラットな組織

オブザーバ

- 総務省
- 経済産業省
- 日本データ通信協会

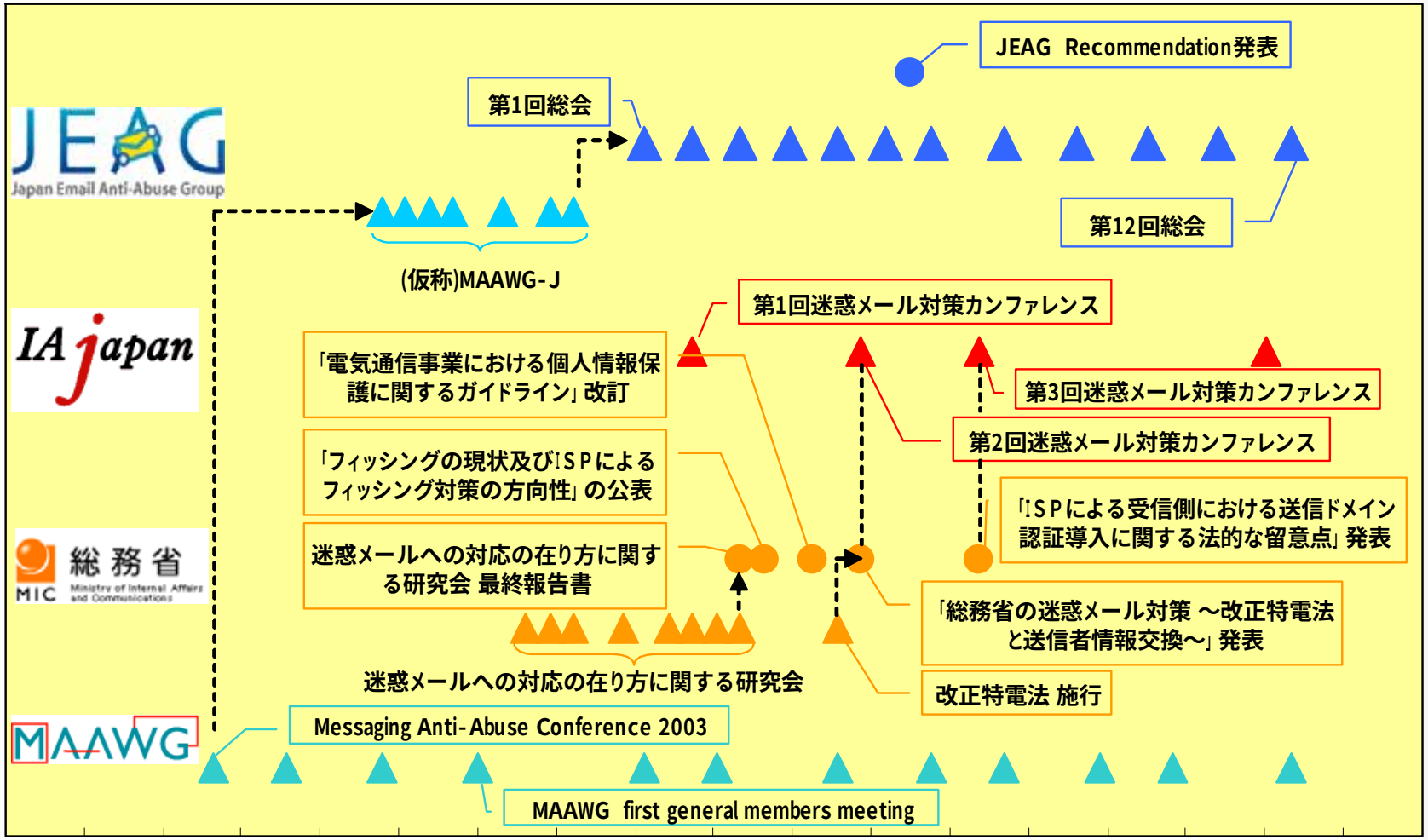
JEAG（Japan Email Anti-Abuse Group）

迷惑メール対策を
- 技術的見地から
- 業界全体で連携し
- 具体的な対策を検討

業界が連携して実施する対策にフォーカス
- 個々の受信フィルタリングに関しては議論しない

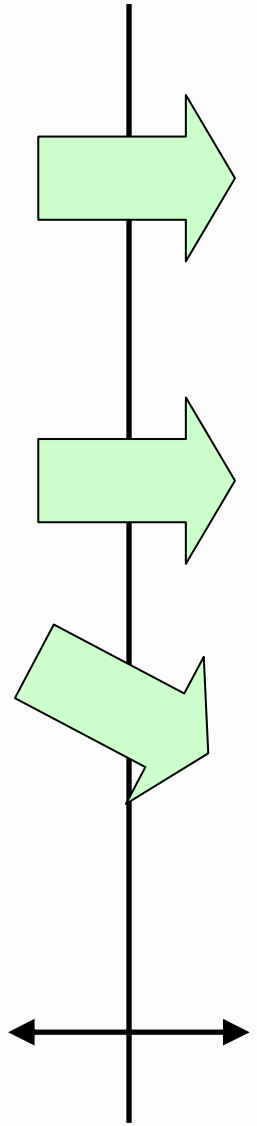
Recommendationを通して検討結果を公開
- 2006年2月

迷惑メール対策に関する関係団体の動き



JEAG 内 Working Group の変遷

- 送信ドメイン認証 SWG
  - ドメイン認証
- OP25B SWG
  - OP25B
  - IP25B
  - SMTP Auth
- 啓蒙 SWG
- Wireless (携帯) SWG



- Technical WG
  - ドメイン認証
- Operational WG
  - IP25B
  - OP25B (Bot対策)
  - RBL
- Collaboration WG
  - SMTP Auth

～2006年

2007年～

迷惑メールをとりまく状況

単なる迷惑からより深刻な問題へ

- phishing など個人情報の不正入手による直接的な金銭被害
  →*2006年の金融被害額は26億ドルを予想（Gartner 2006.11.9）"*
- malware 配布の手段としての利用 → 知らない間に加害者へ（bot 化）
- フィルタ回避のための技術改革（image spam, 目くらまし words, botnet, etc）

制限を強めると届かなくなる

- 迷惑メールフィルタの機能を強めると届かなくなる可能性
  →False Positive はなるべく避けたい
- DNSBL/Real Time Black/Block Listの利用増加
  →登録された場合の送信側の被害が大きい
  →解除方針が不明瞭，連絡先が分かりづらい等の問題点も
- 独自の Block Policy による防御も増える傾向に
  →要因が複雑なためより解除が難しく

国内の迷惑メールの動向

- フィッシングそのものの被害はそれほど多くない（ようだ）
  - 2005年UFJ銀行（当時）を騙る大規模なphishing
  - 度々発生する、Yahoo! Japan及びオークションを語るphishingなど
- 国内でそれほど広まっていないように見えるのは何故か？
  - → 別のbusiness modelが確立しているのでは
- 事例：“迷惑メール54億通送信、「出会い系」社長ら逮捕　中国のPC遠隔操作（毎日新聞　2007/1/17）
  - 国内の法人・個人アドレス230億件を違法購入　←　名簿業者
  - 中国から9,000万通/日送信　←　配信方法の工夫 or　配信業者
  - 1億2,000万円/月の収入　←　完全なbusiness model（利益、contents）
- 高度な技術を駆使しなくても、利益を得られる環境がある
  - → フィッシングをするまでもない
  - → 状況が変われば、広まる可能性は大

フィッシングを防ぐ為には

フィッシングの大半が、メールを起点にしたものであり、その為にはまずは迷惑メール対策を推し進める必要がある。

■ 受け取らないよりまず出さない努力を

- 受信側に届くまでの Internet 上を流れている → 無駄な通信
- 受信に対応するにもコストが必要 → 受信設備の増加
- 無駄なメールを無くすことにより正しいメールがきちんと届く仕組みを
- 正しいメールはどれかを送信側が示すことが必要

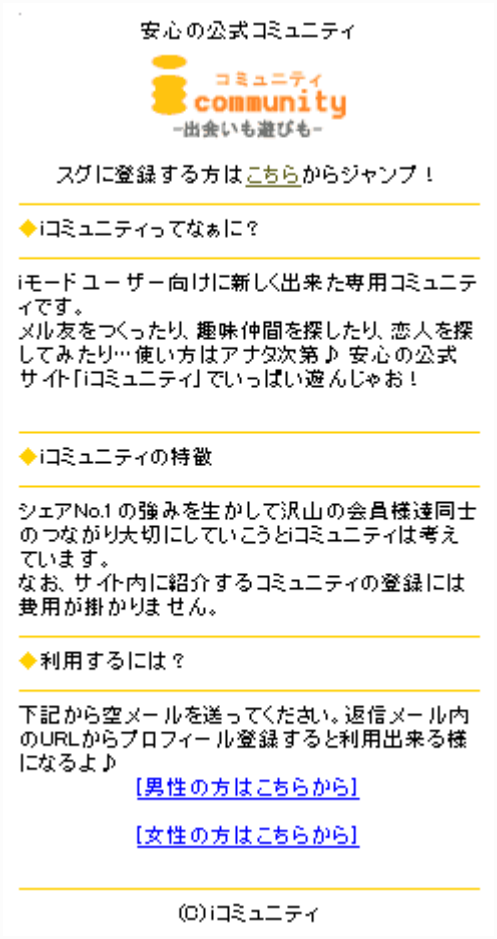
→ OP25B（Outbound Port 25 Blocking）
→ 送信ドメイン認証（Sender Authentication Technology）

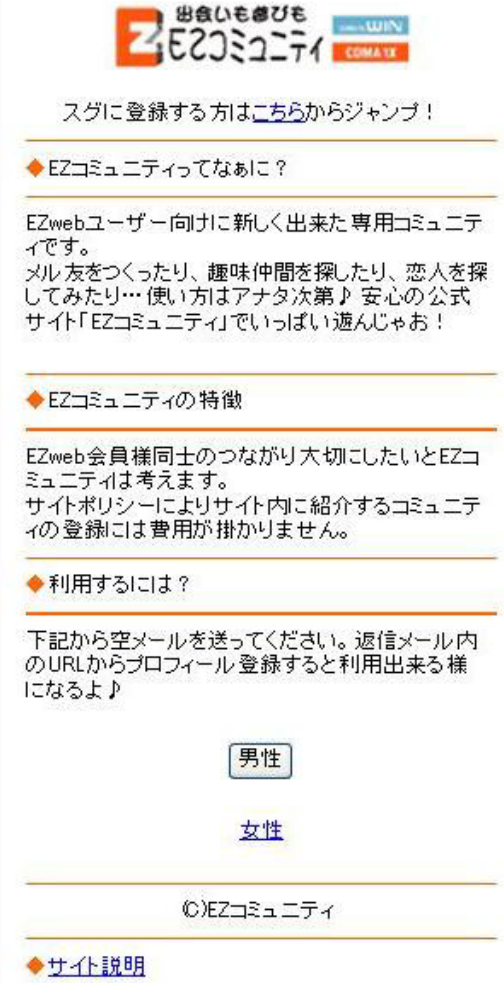
→ これらを 日本国内にとどまらず、global で普及させることが必要

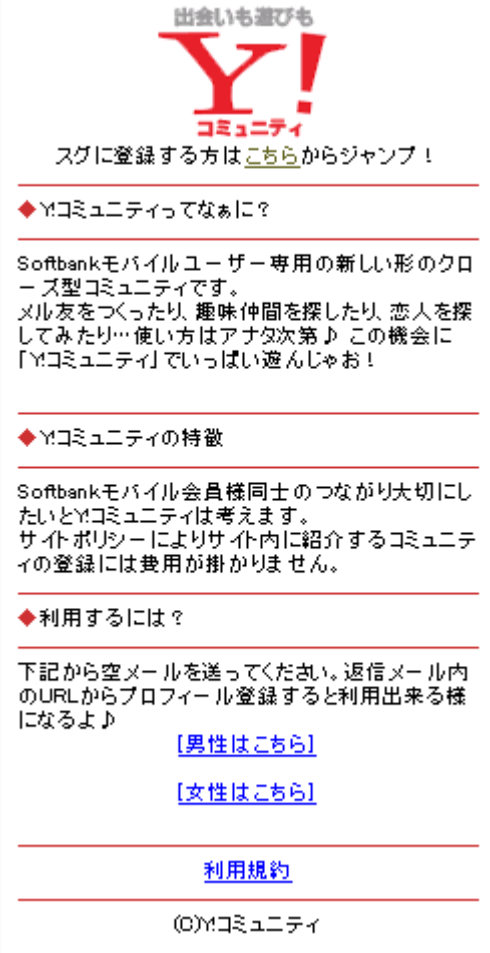
また、日本国内においては、フィッシングというよりは騙り系が多く、ドメインの存在意義が成り立たなくなってきている。したがって、受信したメールが信頼出来るメールかどうかを判別する必要がある。

携帯キャリアを模倣したサイトの一例

携帯各社が提供しているサイトのように見せかけて（実際には関係ないと記載している）、URLもそれらしいものを名乗って、ユーザを誘導する。







なぜ、OP25Bなのか！

- 迷惑メールはどこから来るのか？
  - 「届く」と言うことは、誰かが「どこか」から送っている
  - ほとんどがISPの動的IPを発信源としていた
- どこで止める？
  - 送信側で止める、送信させない

Outbound Port 25 Blocking

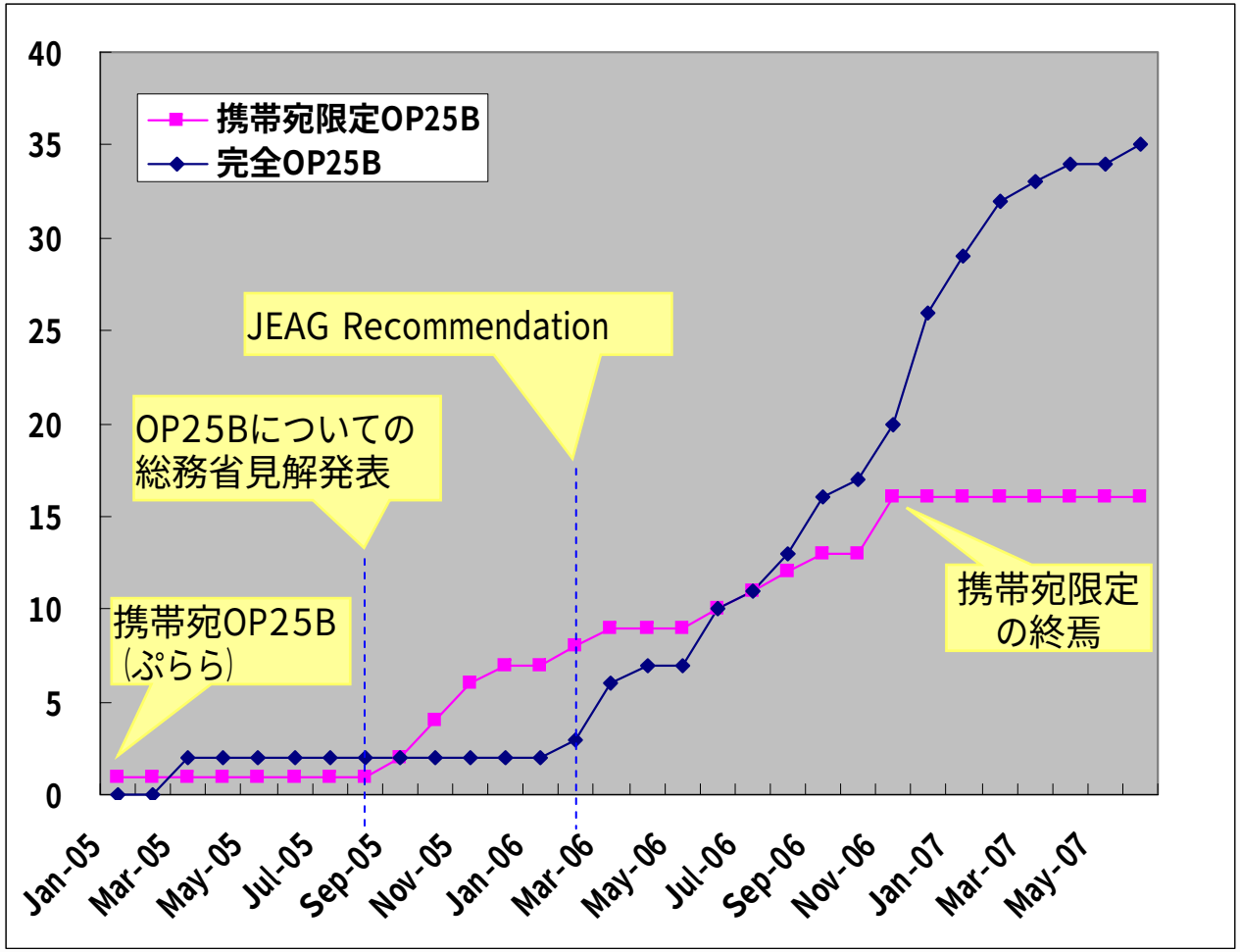
- Outbound Port 25 Blocking (OP25B)
  - Source IP Address が動的 IP 、かつ、Destination Port が 25 である TCP トラフィックを遮断すること （JEAG Recommendationより）
- 特徴
  - メールの送信自体ができないので、動的IPをSource IPとするspamが完全に止まる

- 2004年秋のspamの状況
  - 発信源：ISPの動的IP
  - 受信者：携帯電話

※この当時、日本におけるspamには上記のような顕著な特徴があった。現在は当時とは異なる特徴を示している

普及の状況

(社)

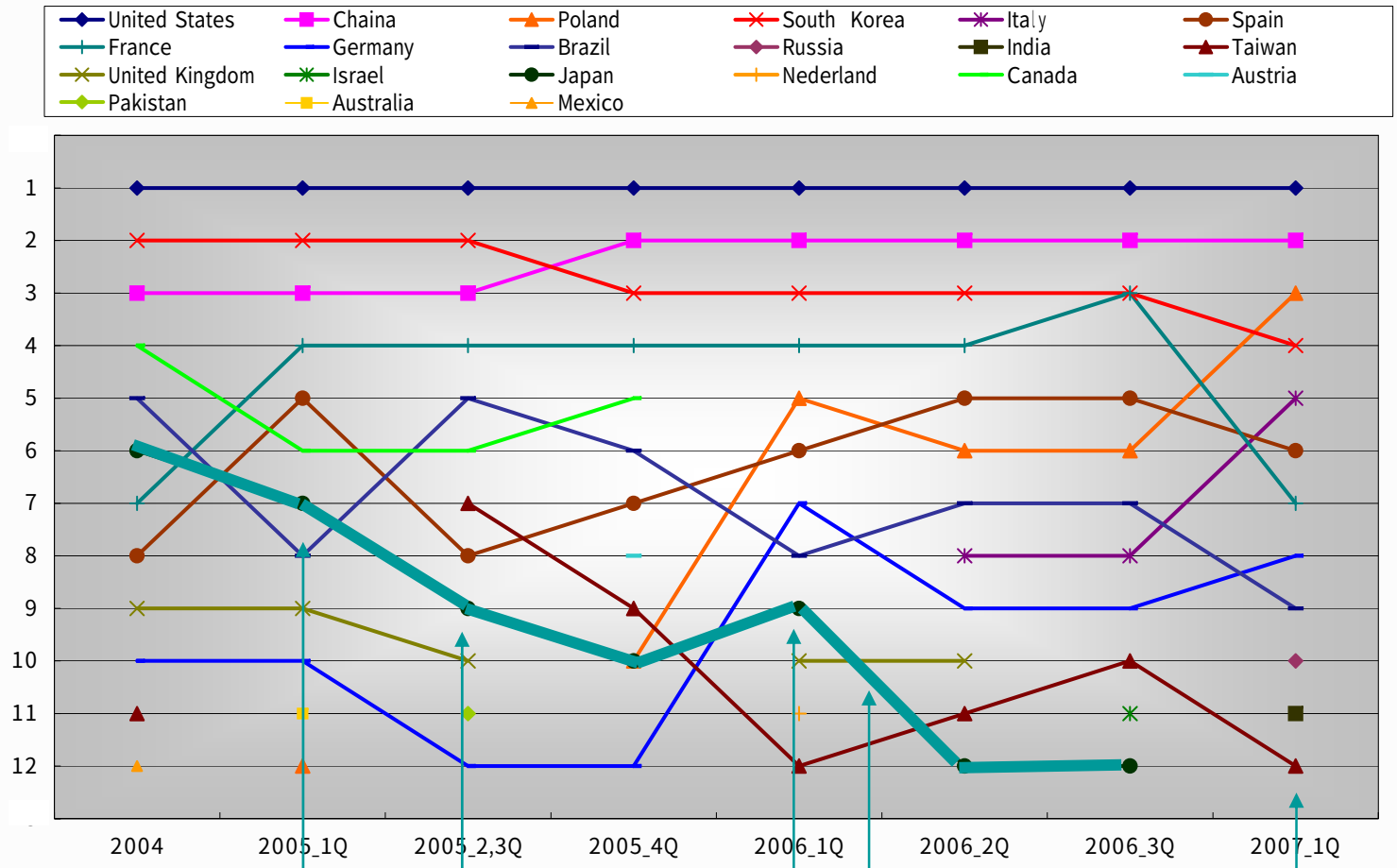


http://www.dekyo.or.jp/soudan/taisaku/i2.htmlより集計

普及の状況

- 2005.8　OP25Bに対する総務省見解の公表
  - *携帯宛限定OP25Bの普及が進む*
- 2006.2　JEAG Recommendation発表
  - *完全なOP25Bの普及が進む*
- 現在 JEAG内のOP25B実施率、ほぼ100%達成
  - *日本のOP25Bは「完成期」を迎えている*
  - *spam発信源は海外へ*

効果　～Spam発信国ランキング～ (順位)



携帯宛限定加速

完全OP25B加速

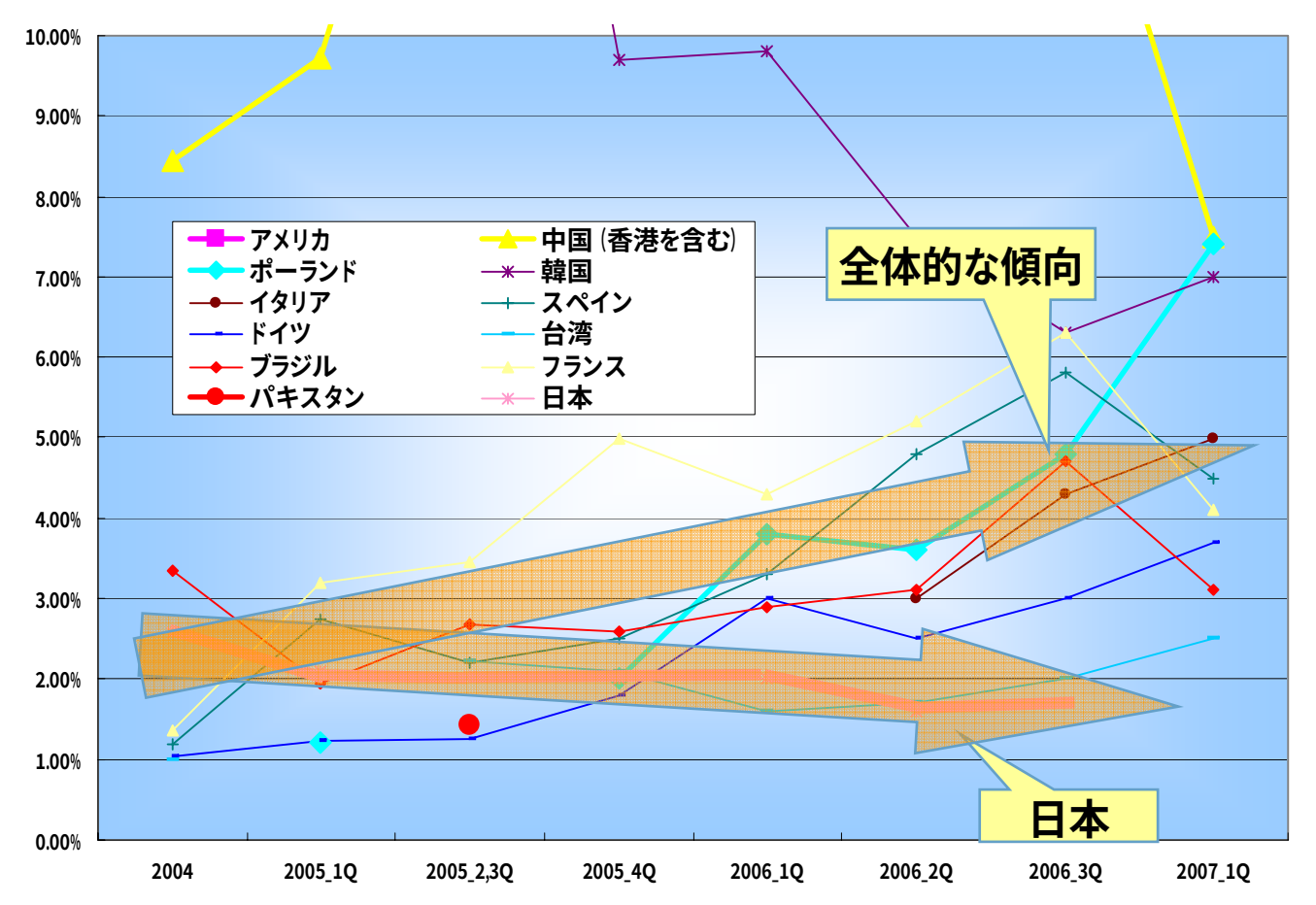
ランク外へ

2005.2 携帯宛限定(plala)

2006.2　JEAG Recommendation

http://www.sophos.comの発表を集計

効果　～Spam発信国ランキング～ (割合)



US,CNを除いた各国発のspamの割合が増加している中、日本は減少傾向を示している

http://www.sophos.comの発表を集計

効果　～Spam発信国ランキング～（割合）

- 日本発のspamについては割合としては減少傾向
  - ➢ *OP25B 普及の成果である*
    - →実数の統計でも減少しているのでは？
    - →近い将来実数も減少すると予想できる

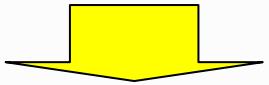
※世界的にspamの総数は増加傾向にある。
※ISPの受信するspamもここ1年で数倍になっている。
※spamの発信源は海外のbotへ移行している。

➡ *OP25Bの普及が遅れれば、botの被害はもっと深刻だった*

なぜ、送信ドメイン認証技術が必要か！

■ 迷惑メールに多く見受けられる特徴

- *迷惑メールの多くは送信元を詐称*
- *正規のメールサーバを経由せず専用サーバから直接送信*
  →送信元が固定でなくなっている（Bot経由が主流へ）
- フィッシングなどの詐欺行為の出現



■ 迷惑メールの対策には

- 送信者情報を詐称出来ない仕組みの導入が必要
  →SMTP AUTH
  →*送信ドメイン認証技術*
- 送信元が明確になれば対策がし易くなる
- 正規の送信元からのメールを正しく受信出来る

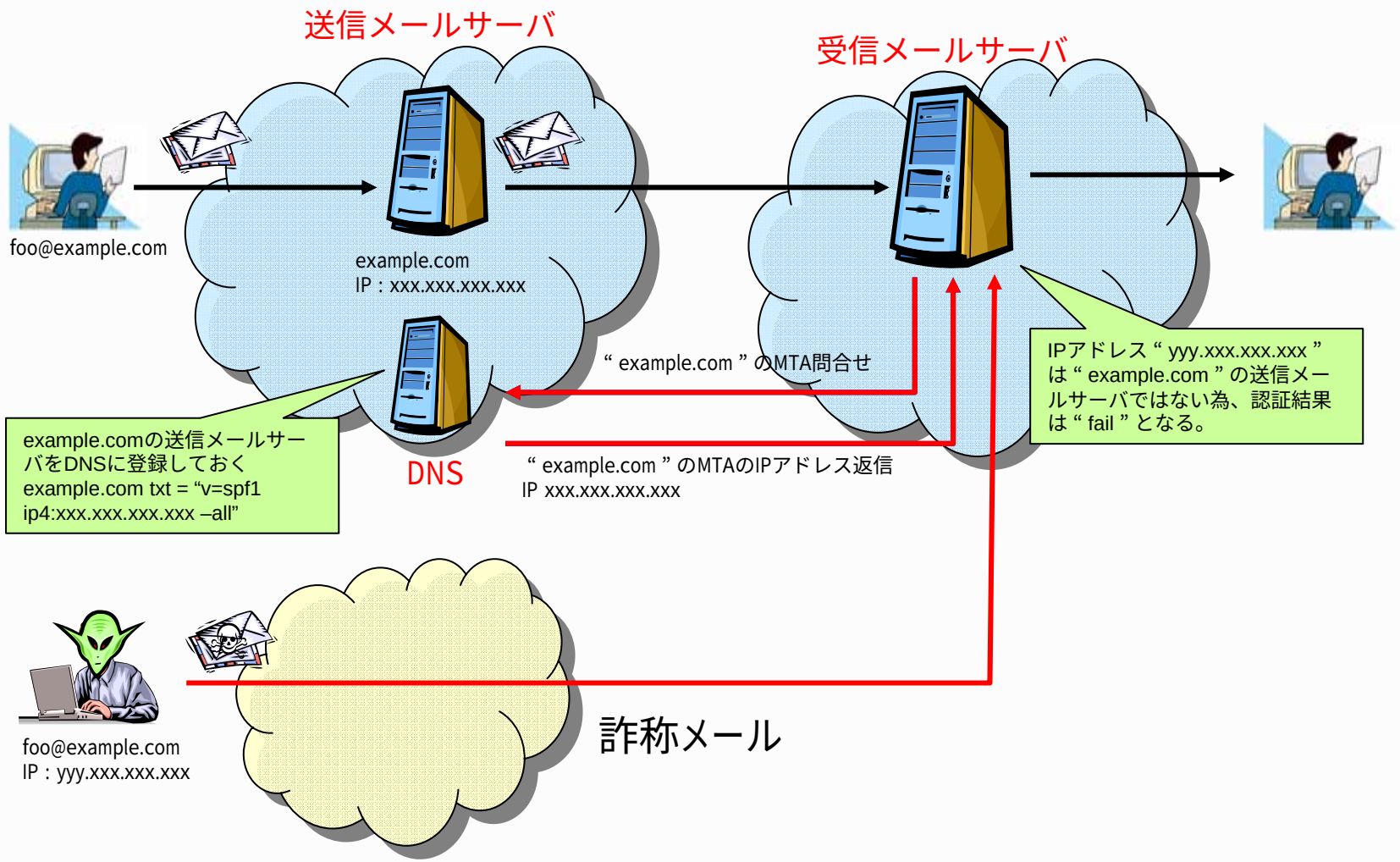
送信ドメイン認証技術とは

- 送信側がドメイン単位でメール送信元情報を表明
- 受信側が正規のメールサーバから出たものかを認証
- *送信側と受信側で協力して初めて成立する技術*
- 既存のメール配送の上位互換として存在

送信ドメイン認証技術には二つの種類が存在

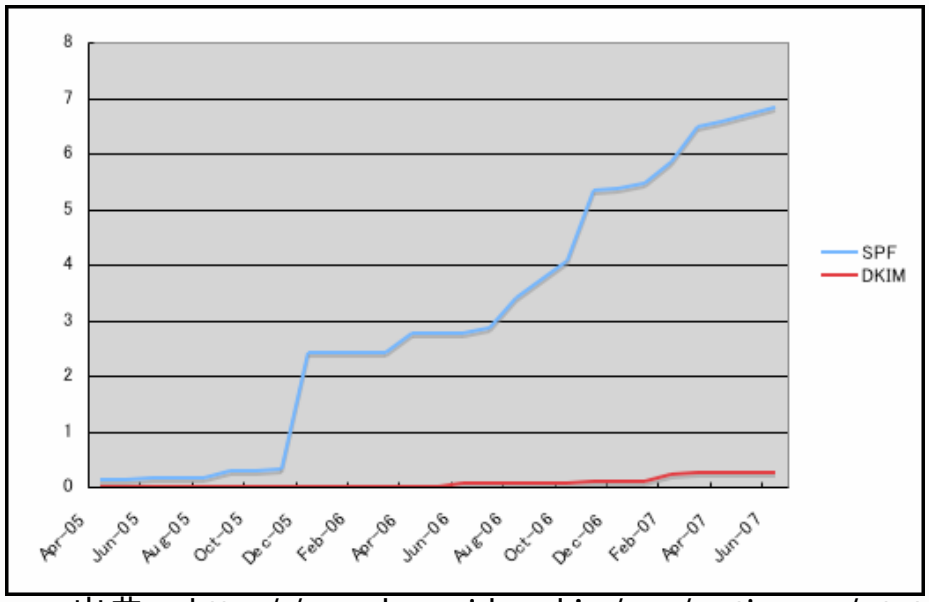
- 送信元をネットワーク的に判断
  （*SPF : Sender Policy Framework*）
- 送信時に電子署名をメールに付与
  （DKIM : DomainKeys Identified Mail）

送信ドメイン認証（SPF）のしくみ



送信ドメイン認証の国内の普及状況

WIDE プロジェクトは、JPRS と共同研究契約を結び、2005年4月から送信ドメイン認証の普及率測定しており、その調査結果を以下に示す。



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

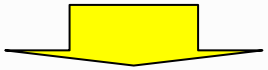
登録型	登録数	MX	SPF	DK
AD(JPNIC会員)	291	248	37	2(4)
AC(大学系教育機関)	3368	3184	189	2(6)
CO(一般企業)	305042	284775	26660	614(630)
GO(政府機関)	884	746	46	0(1)
OR(会社以外の団体)	22703	21283	1949	31(35)
NE(ネットワークサービス)	17435	13358	745	43(54)
GR(任意団体)	8513	7275	546	13(16)
ED(小・中・高校など主に18歳未満を対象とする各種学	4447	4059	191	2(2)
地域型(都道府県名、政令指定都市名、市町村名)	3265	2699	76	2(3)
汎用JPドメイン	540168	363424	15716	905(977)
合計	908329	702092	46161	1614(1728)

2007年4月末現在、JPドメインにおける送信ドメイン認証技術のおおよその普及率

着実に、国内のSPFの記述率は増えている
（6月末現在、約6.84%）

送信ドメイン認証普及にむけての課題認識

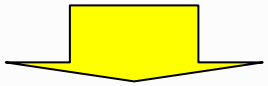
- 送信ドメイン認証の仕組み、影響、効果が認知されていない。
- 社内へ十分説明出来ない、もしくは、そもそも十分理解していない。
  - 導入のインパクト、影響、等
- SPFの記述方法や設定方法などを説明する媒体が無い。（少ない）
  - 記述したくても、記述方法が判らない為、導入できない。
- 受信側の対応が少なく、書くメリットがない。
  - 実影響が出ていない為
  - 認証結果をどう扱うかが不明確。（passとnoneの区別がない）
- メールを受信するエンドユーザに効果を訴求しづらい。
  - エンドユーザへの効果に対して、導入の障壁が高い。
  - 顧客へどのようなメリットがあるのか見えにくい。



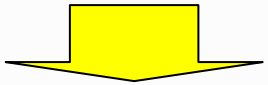
実際の問題として、ISP/ASPのSPFレコードの記述率は高いが、業界によっては全く対応出来ていない所もある。

アドレス詐称の実態

これまでの迷惑メールのアドレス詐称状況は、大手ASP等のフリーメールアドレスのドメインを詐称してメールを送信するケースが多かった。
しかしながら、最近では大手ISPのドメインを詐称して送信される数も多くなってきている。



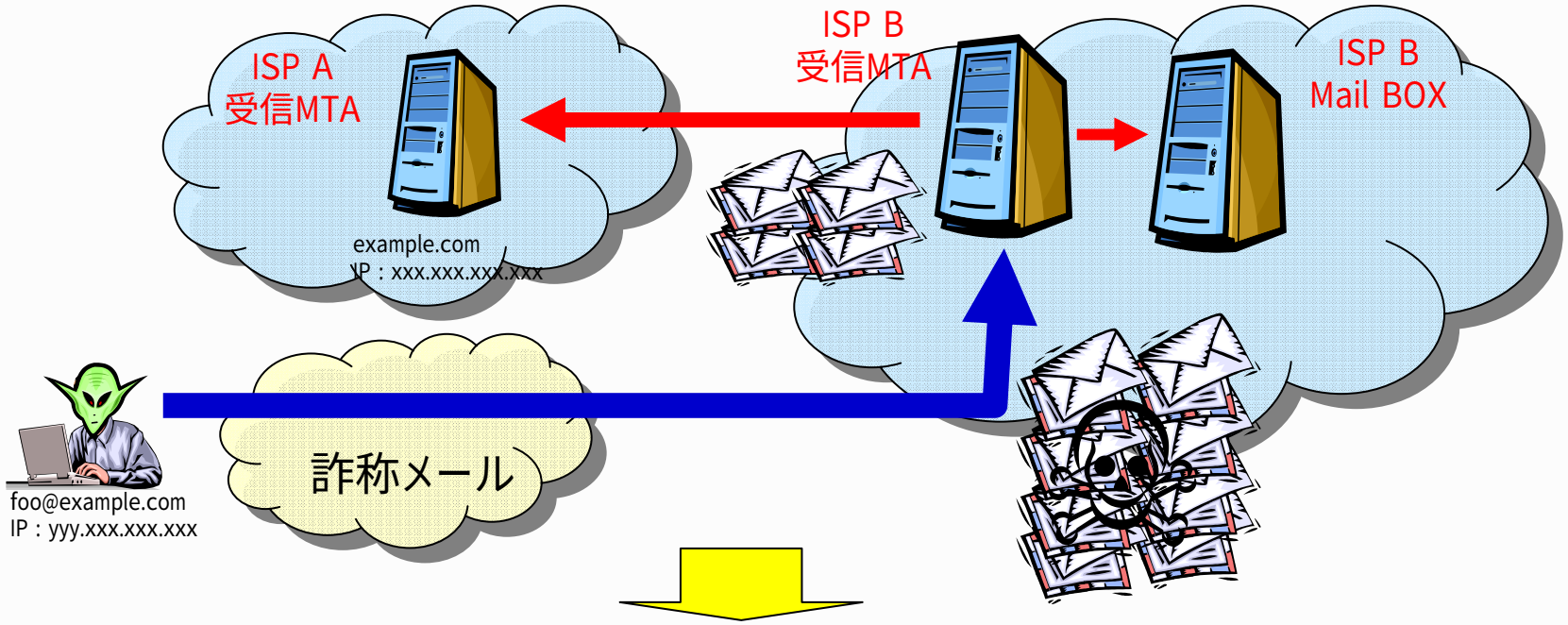
さらには、メールマガジン等のメールアドレスを詐称して、あたかもそのメールマガジンを語って送ってくるメールも出始めている。
最近では、一般企業のドメインを詐称した迷惑メールも出現している。



自社のドメインを守る為にも、SPFの記述は必須となってきている。

Bounce spamの問題

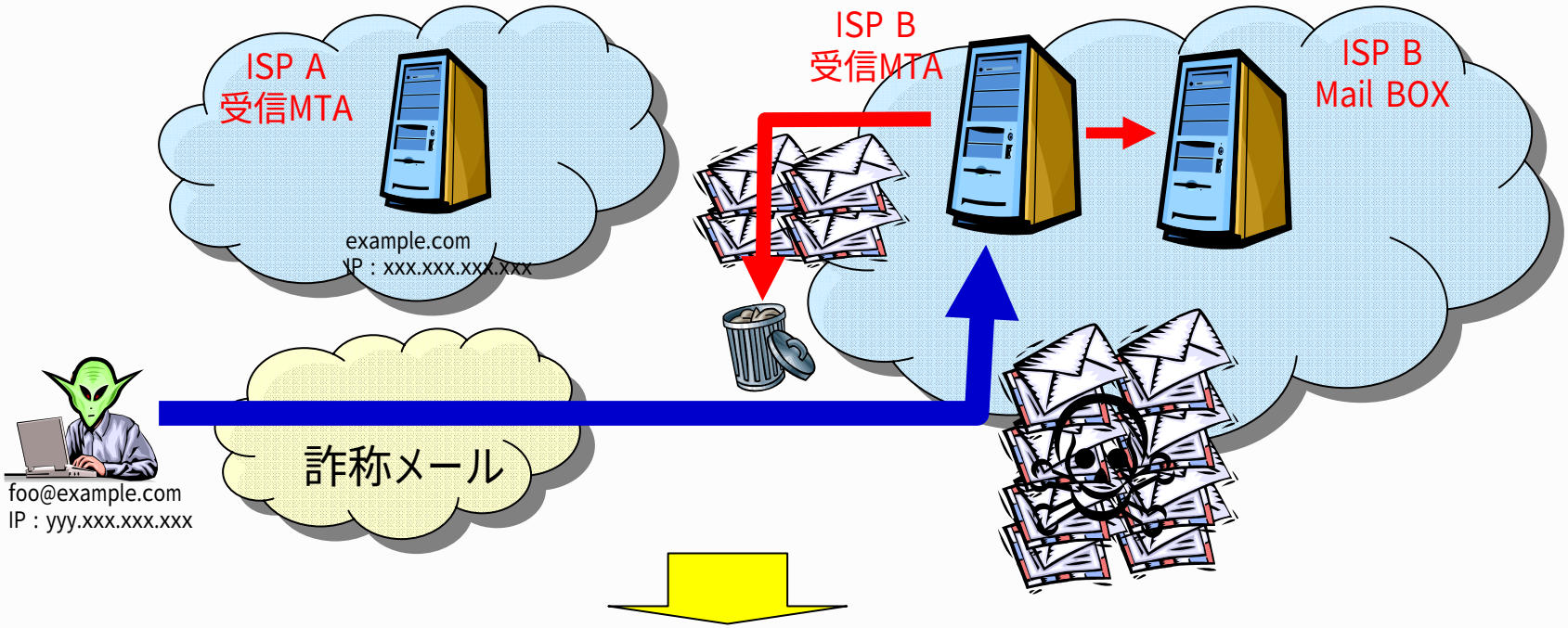
メールサーバの構成によっては、受信MTAでユーザ情報を持っていない、ハーベスティング対策でメールをすべて受信する設定としている、等の場合、存在しない宛先へメールが来た場合、エラーメール（NDR）返信が一般的である。しかしながら、迷惑メールで送信ドメインを詐称され大量の存在しない宛先のメールが送信された場合、受信側ではなりすまされたドメインに大量のNDRを返信する事となり（Bounce spam）問題となる。



なりすまされ易いドメインは、これが大きな問題となっているらしい。

SPF認証結果の応用（NDR破棄）

SPF認証結果で、エラーとなった場合、そのメールは詐称したアドレスからのメールと判断し、NDRを破棄する事で、受信側は不要な送信なくすことが出来、詐称されたドメイン側も不要なメールを受信しないですむ事となる。

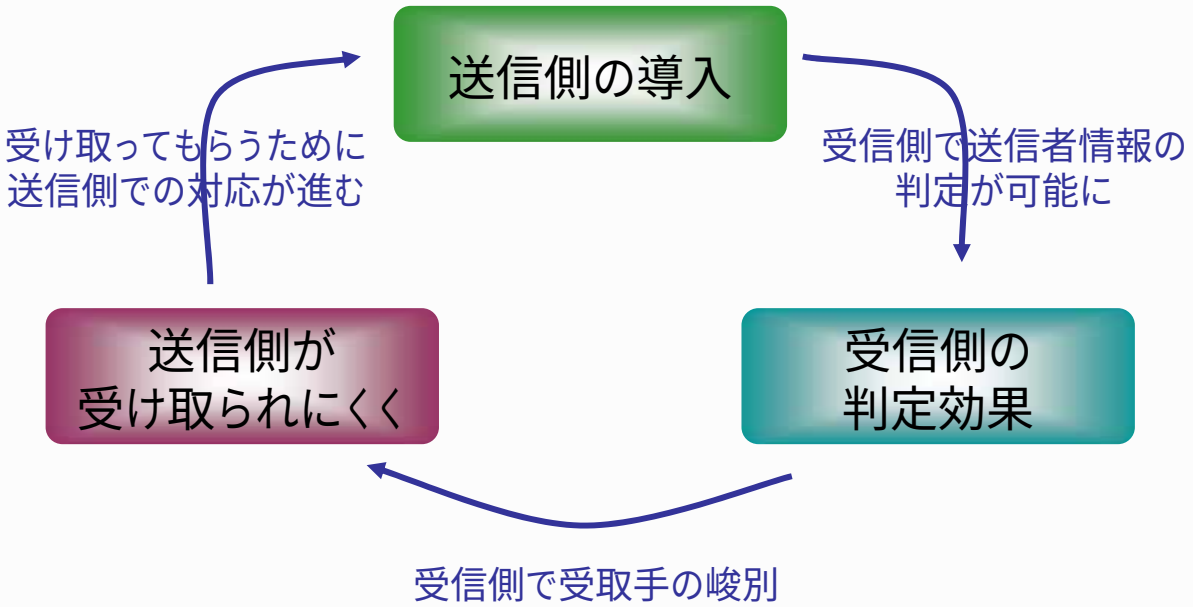


本対応は、JEAG Recommendationでも、参考情報として提案をしている。また、総務省にて、正当業務行為（違法性阻却事由あり）と解釈出来ると提示されている。

ISPによる受信側における送信ドメイン認証導入に関する法的な留意点（第3回迷惑メール対策カンファレンス）
http://www.soumu.go.jp/joho_tsusin/d_syohi/m_mail.html#jigyosha

送信ドメイン認証 (SPF) の普及にむけて

- メール送信側でまず導入すべき
- 送信側のSPFの導入は容易
  - DNSへのSPFレコード追加で済む
- 利用局面に応じて導入技術を判断
  - それぞれの長所、短所を把握して判断
  - ビジネスとして連絡、情報提供に使うメールはDKIMで



これからの迷惑メール対策 (国際的な取り組みの重要性)

- Internet は Global な Infrastructure
  - 国内発の迷惑メールは減少傾向 ← 様々な取り組みにより
  - 海外からの迷惑メール送信は増加傾向
  - Internet が整備されるにつれて迷惑メールも増加 → 新興国の出現
  - Botnet により送信元の拡散化 → もはや特定の国だけの問題ではない
  - 迷惑メール（spam）送信は既にビジネスとして確立
    - →Less Risk: less violence, less jail time, more profit
- Global な視点
  - 日本の対策状況の説明
    - →対策事例（OP25B, SenderAuth, 携帯事業者の取り組み）の共有
    - →日本がもはや迷惑メール送信国ではないことの認知
    - →日本の評判（reputation）の向上 → 大きな単位でのブロック抑制
  - 意思疎通の確保
  - JEAG: 国内での話し合いの場 → 同じ枠組みを Global でも

まとめ

- 迷惑メールをなくす事が、フィッシングを始め、架空請求、ワンクリック詐欺をなくす為の第一歩となる。
  - 迷惑メールをなくす為には、これらのメールを出さない（出せない仕組み作りが必要。）
    - →ISPは、Outbound Port25 Blockingの導入
    - →メールを送信するすべての人は、送信ドメイン認証の導入
- 迷惑メールの発信拠点は海外。海外との協調も必要である。
  - 日本の成功事例をもとに、海外への訴求して行くことが必要。
- ドメイン名は、もはや信用出来ないものになっており、新たな枠組みが必要。
  - 信頼出来る情報か否かを判別する仕組みが必要となる。