JEAG テクニカルアップデート
～　迷惑メールの現状と技術的課題等について　～

KDDI株式会社
本間　輝彰

2008/5/23

Agenda

- 迷惑メールの動向について
- Outbound Port25 Blocking（OP25B）
- メール配信業者（送信代行者）を踏み台にした迷惑メール
- 送信ドメイン認証

- 海外発メールの対策と海外連携について
- まとめ

本資料での記述範囲

迷惑メールの動向について

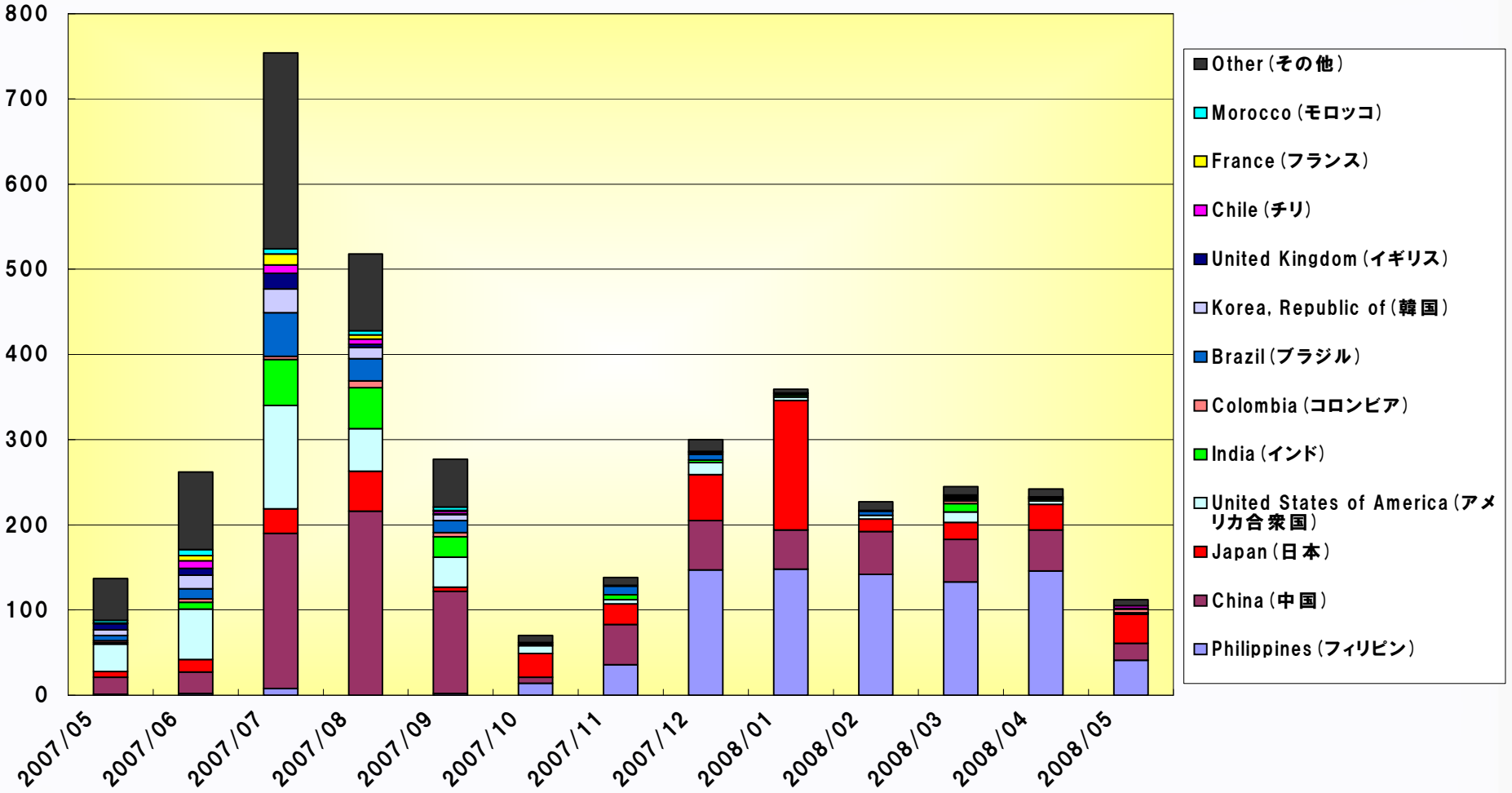
迷惑メールの最新動向

- 日本国内における迷惑メールに対する状況は、送信ドメイン認証、OP25B（Outbound Port25 Blocking）により一定の効果が見られるもの、海外発の迷惑メールを始めその脅威は以前継続しており、危機的状況と言って過言ではない。

  （迷惑メールが減っていると感じるのは、受信側の努力により、ユーザに到達している迷惑メールを抑制しているだけにすぎない。）
- 送信先は、ISP/ASPのみならず、企業や学校等、相手を問わない状況になっており、一部の企業ではメールの利用が困難な状況に陥っているという話も聞くようになってきた。

送信国状況について　その1

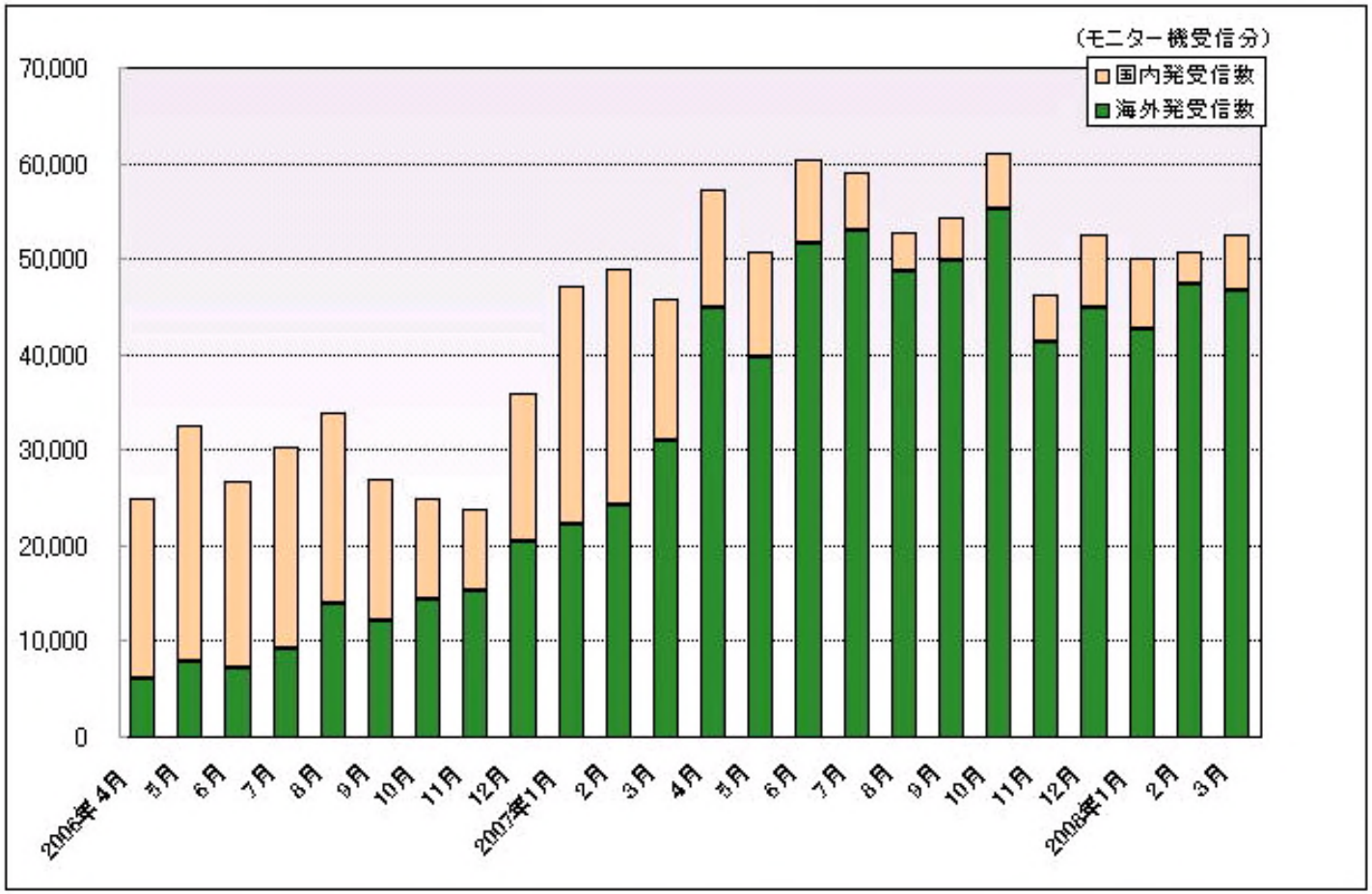
2007年5月1日～2008年5月11日の調査データを下記に示す。受信データから多くが、海外発の迷惑メールであると確認出来る。



※:本データは、個人が所有する携帯電話一台に送信されたメールを集計したものであり、全体の傾向を表す物ではありません。　（サンプル数:3,641通）

送信国状況について　その2

日本産業協会のモニター機受信分析結果においても、海外発が増えているのが確認出来ている。



※：日本産業協会：　迷惑メールの統計　http://www.nissankyo.or.jp/mail/graph/graph.html

迷惑メールの主な送信手法について

- **海外発**
  - 送信元のユニークIP数の増加、広い範囲の国からの送信状況を踏まえると***Botを用いた***送信が増加していると推測出来る。
  - 突出した送信状況から、spam送信者が***海外を活動拠点にして送信***して送信していると推測出来る。

- **国内発**
  - ***OP25B未実施の動的IP***（xDSL、FTTH等の高速回線のみならず、Narrow Bandoの動的IPも含む）から送信されている。
  - ***メール配信業者を踏み台***にして、送るケースが非常に増加している。
  - OP25Bを回避する為に、***固定IP***を取得して堂々と送信しているケースも見受けられる。（NICの登録も個人名でしているものが多々見受けられる。）

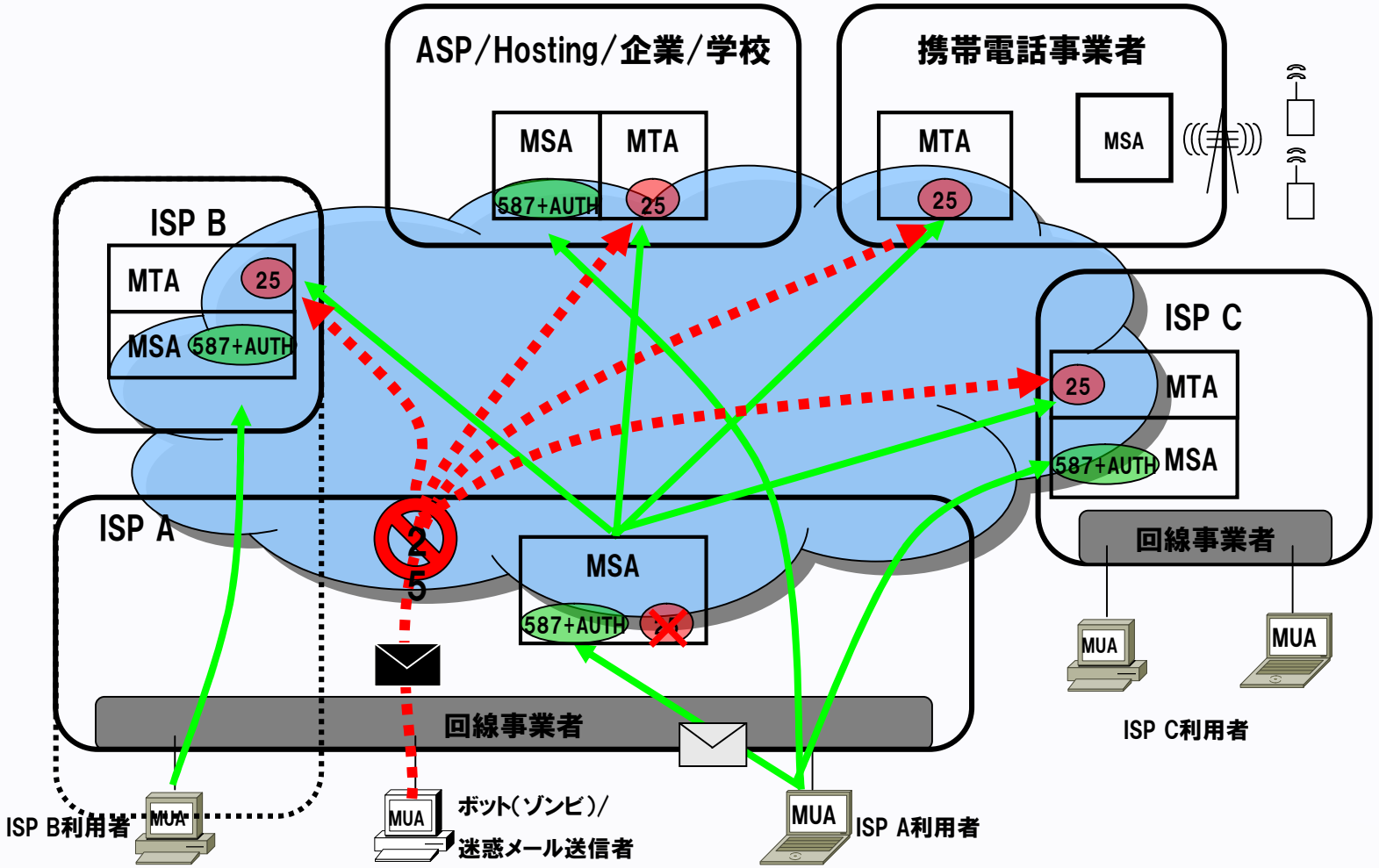
Outbound Port25 Blocking（OP25B）

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）

メール送信自体ができないので、動的IPをSource IPとするspamが完全に止める事が出来る。

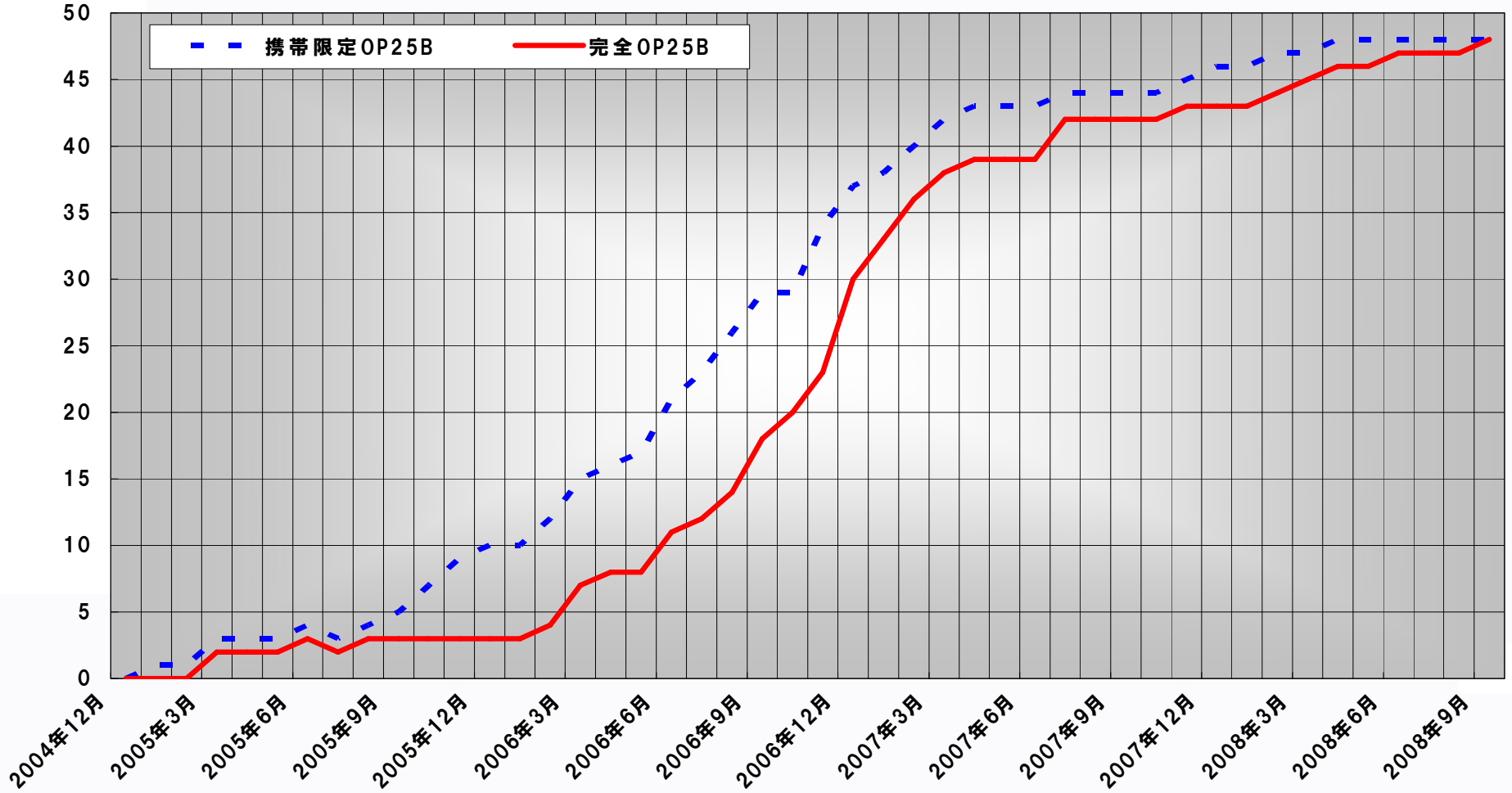
OP25Bの目指すべきゴール(理想型)について

すべてのMSAは587番(Submission Port)+SMTP AUTHを提供し、ユーザがメールを送信する際には、本接続を利用する。また、ISPはすべての動的IPからの25番Portをブロックを行う。



OP25Bの実施状況

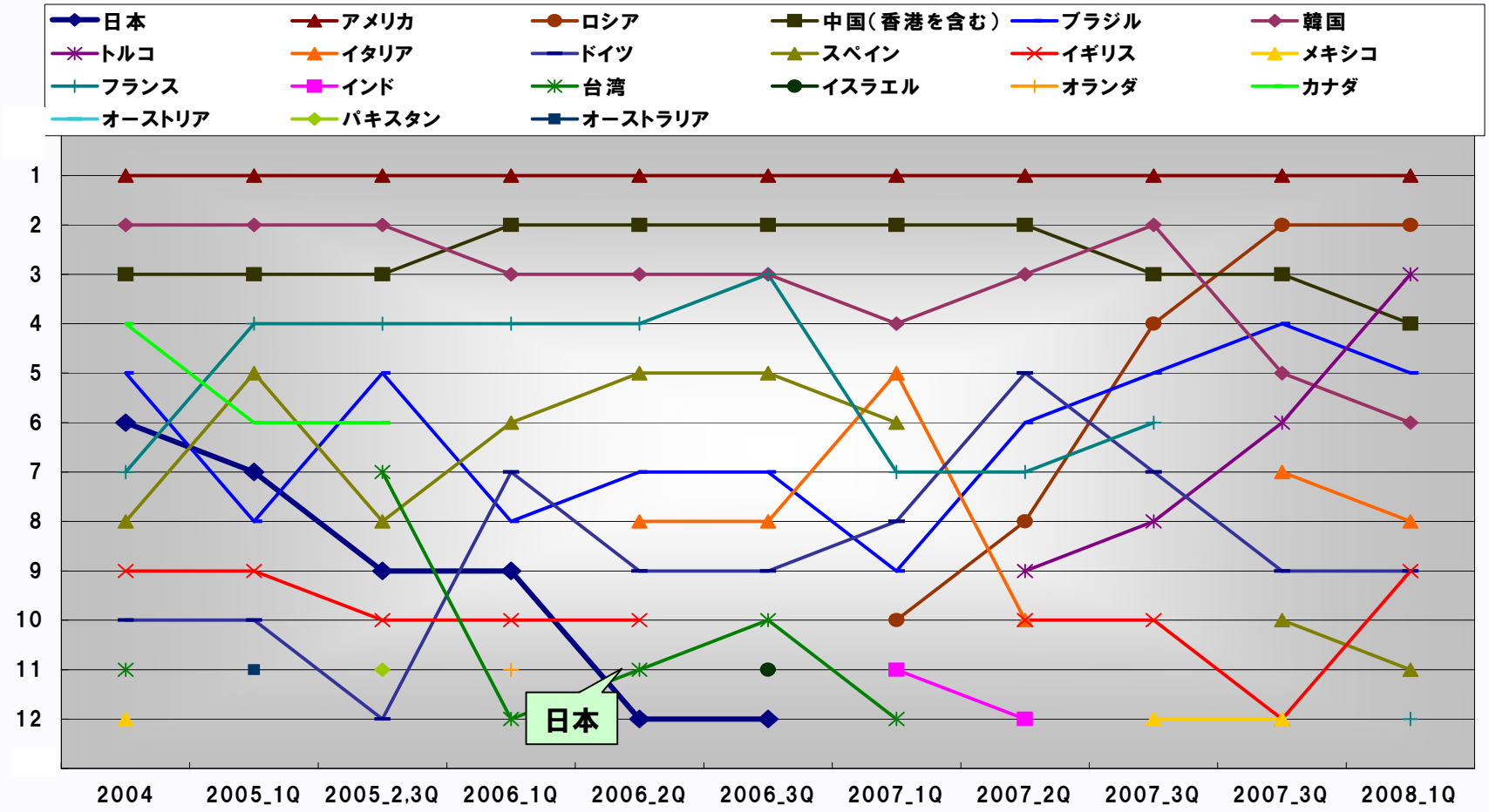
日本データ通信協会にて調査した国内ISPのOP25B実施状況※1を下記に示す。2006年から2007年にかけて、多くのISPがOP25Bを実施した状況ではあるが、引き続き実施しているISPもわずかながら増えている状況ではある。



※1：日本データ通信協会： ISPによるOP25B 実施状況 より http://www.dekyo.or.jp/soudan/taisaku/i2.html

OP25B効果について(スパム送信国ランキング)

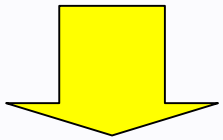
ソフォス社が四半期毎に発表しているスパム送信国ベスト12のデータにおいて、日本発は2006年3Q以後は圏外となっている。最新のデータでは、全体の33位となっており、その割合も昨年の同時期から1.5%減の0.5%となっている。



※:ソフォス社: スパム送信国Best12データより http://www.sophos.com/

OP25Bの現状の課題について

- OP25Bを実施していないISPからの迷惑メールが増加している。
  - xDSLやFTTHのみならず、Narrow Bandからの送信も見受けられるようになっている。
- OP25Bの導入障壁を解消する為に、網外からメール送信出来なくなるという問題に対する対策として、587Port＋SMTP AUTHへの移行を推奨しているが、現実的には進んでいない。



これらをどう解決していくかが、OP25Bの成功の可否を決めると言って過言ではない。

OP25Bを成功させる為には（動的IP発の迷惑メール根絶へ）

- 日本国内発の迷惑メールを分析すると、OP25B未実施の動的IPからのメールが多く含まれている。
  - OP25B未実施のISPは、OP25B導入を推奨する。
  - OP25B実施ISPにおいても、Narrow Band等全てに対してOP25Bを実施していない場合が多い。したがって、すべての動的IPにOP25Bを導入する事を推奨する。
    - ソフトバンクモバイルでは、携帯電話やデータカードをパソコンやPDAに接続してインターネットに接続するサービスに対してOP25Bの導入を実施を発表。（2007/11/25）
    - KDDIでは、パケット通信・ダイヤルアップなどのNARROW回線においても、ブロードバンド回線同様、動的IPからのOP25B導入を発表。（2008/04/25）
- OP25B導入の障壁として、接続ISP以外のメールサーバ経由でメールを送信する経路がブロックされる懸念がある。
  - メール送信（投稿）する際は、25番ポートの接続から***587番ポート***への移行を推奨する。また、この際に送信時には***SMTP AUTH***による認証を実施する事を推奨する。
    - 現状は、大半のISP/ASPが***587＋SMTP AUTHをサポート***しており、実際には障壁とはなる可能性はなくなっていると言える。
    - メールクライアントのデフォルト設定が、587+SMTP AUTHとするような対応も必要である。
  - 587+SMTP AUTHを普及させる為に、自網外からのメール送信の際によく使われていたPBS（POP before SMTP）は廃止すべきである。（PBSはネットワーク認証であり、個人認証ではない為、セキュリティを高める為にも廃止する事が望ましい。）
    - いくつかのISPでは、すでに***PBSを廃止した***所もある。

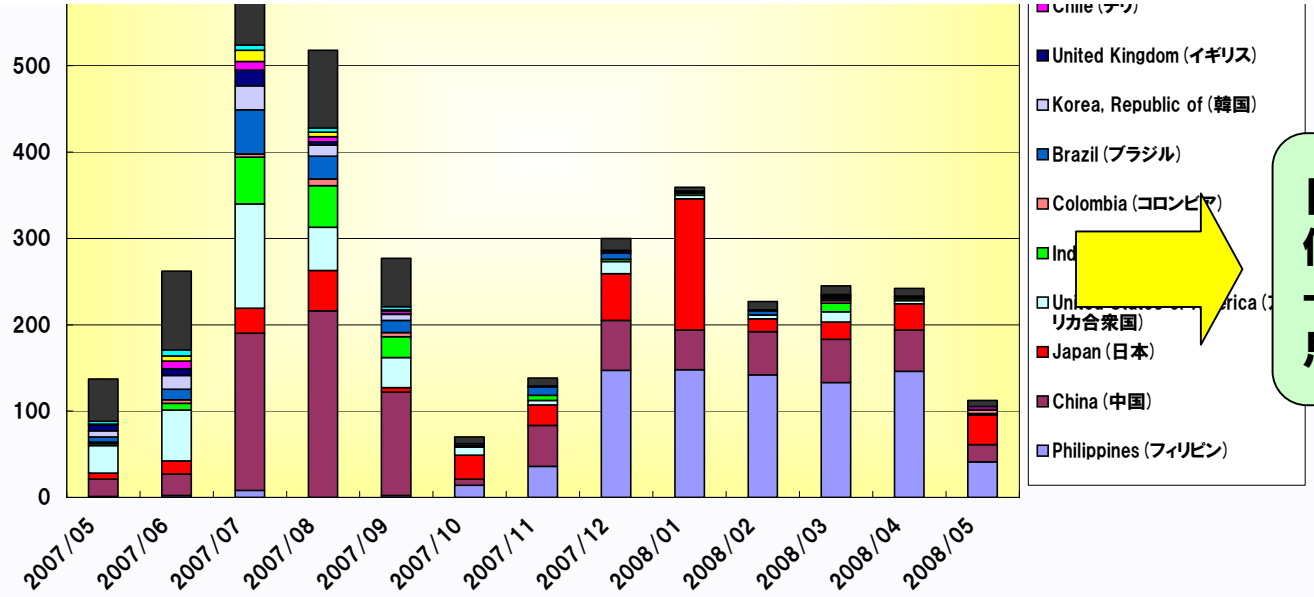
メール配信業者(送信代行者)を踏み台にした迷惑メール

昨今増えている迷惑メール送信の手法の一つである。

海外発同様、OP25B実施により、動的IPからの送信元を失った迷惑メール送信業者が利用していると思われるケースが多い。

メール配信業者を踏み台にした迷惑メールの状況について

- 日本国内発の迷惑メールにおいて、メール配信業者を踏み台にした迷惑メールが目立つようになってきた。
  - メールサーバ経由のメールの為、OP25Bの影響を受けない為、国内から容易に送信が可能である。
  - 善良が配信者も多く含まれており、受信側での対処が非常に難しい状況である。
  - Botと異なり、短時間に大量に送信してくるケースもある。



日本国内発の迷惑メールの送信元を分析すると、かなりのメールがメール配信業者経由と思われるメールになっている。

メール配信業者経由と思われる迷惑メールについて

国内発の迷惑メールを分析して行くと、OP25B未実施の動的IP発とメール配信業者等を経由に(それ以外のパターンもあるが)大別される。
特に、最近では配信業者経由が増えているように想定しており、その送信方法も、短時間に連続して送信して来るケースと、日数をかけて定期的に送信してくるケースに分類出来る。

ヘッダFrom	エンベロープFrom	タイトル	月日	時間	送信IP
mail@***.***.***	<error-*****=ezweb.ne.jp/3069688/1@error.***.***.***>	【緊急】松本美佐子様より譲渡依頼↓	07/8/23	11:10	***.***.***.33
mail@***.***.***	<error-*****=ezweb.ne.jp/3069688/1@error.***.***.***>	私からのポイント届きませんか？	07/8/23	11:42	***.***.***.46
mail@***.***.***	<error-*****=ezweb.ne.jp/3069688/1@error.***.***.***>	本日出張ホスト可能かしら？	07/8/23	12:27	***.***.***.46
mail@***.***.***	<error-*****=ezweb.ne.jp/3069688/1@error.***.***.***>	この写真見ても感じない？	07/8/23	13:03	***.***.***.47
mail@***.***.***	<error-*****=ezweb.ne.jp/3069688/1@error.***.***.***>	【緊急】松本美佐子様より譲渡依頼↓	07/8/23	13:10	***.***.***.41
mail@***.***.***	<error-*****=ezweb.ne.jp/3069688/1@error.***.***.***>	貴方は40歳の私を抱けますか？	07/8/23	13:51	***.***.***.57
mail@***.***.***	<error-*****=ezweb.ne.jp/3069688/1@error.***.***.***>	今何処に居るのでしょうか？	07/8/23	14:03	***.***.***.37
mail@***.***.***	<error-*****=ezweb.ne.jp/3069688/1@error.***.***.***>	H教えて…今日中に会えますか	07/8/23	15:20	***.***.***.53
mail@***.***.***	<error-*****=ezweb.ne.jp/3069688/1@error.***.***.***>	もう学校早退しました　今から、	07/8/23	15:58	***.***.***.58

IPアドレスを“Whois”で調べて出てくる組織名を調べると、メール配信サービス業者が管理しているIPである事が確認出来る。

ヘッダFrom	エンベロープFrom	タイトル	月日	時間	送信IP
<info@****.***>	<846144@ret.****.***>	お願いがあります。	08/1/4	10:21	***.***.***.180
<info@****.***>	<846144@ret.****.***>	新人研修の為、無料で女の子をデリバリーします。	08/1/4	17:45	***.***.***.224
<info@****.***>	<846144@ret.****.***>	777万円の当選にはお気づきでしょうか。	08/1/5	9:08	***.***.***.166
<info@****.***>	<846144@ret.****.***>	単刀直入に	08/1/5	13:20	***.***.***.180
<info@****.***>	<846144@ret.****.***>	慰謝料が発生しています。	08/1/6	9:39	***.***.***.180
<info@****.***>	<846144@ret.****.***>	1月末日で慰謝料が1000万円発生します。	08/1/6	19:16	***.***.***.236
<info@****.***>	<846144@ret.****.***>	割り切りで考えてくれる人ですか？	08/1/7	11:16	***.***.***.236
<info@****.***>	<846144@ret.****.***>	今日気分がいいので、おごっちゃいます	08/1/7	15:44	***.***.***.180
<info@****.***>	<846144@ret.****.***>	777万円ご当選の件で連絡致しました。ご連絡頂けますでしょうか。	08/1/7	20:01	***.***.***.180

このような送信について法的な対処も必要ではあるが、**未然に送信を防ぐ工夫**も必要であると考える。

メール配信業者を踏み台にした迷惑メールの対策について

- メール配信業者による管理の強化が必要。
  - メール配信業者の一つと取り組みとして、MAAWG(Messaging Anti-Abuse Working Group)に加盟しているメール配信業者は、“MAAWG Sender Best Communications Practices”※1を作成し、メール配信する際のガイドラインを作成している。
  - ISPが過去に迷惑メール送信者に対して、すみやかな利用停止措置を実施して対策した事と同様に、迷惑メール送信が確認された時点で利用停止するような仕組みも必要であると考える。
- 改正される特定電子メール法、特定商取引法により、迷惑メール送信を確認出来た時点で、法的に罰する等の対策を実施する事で、これら経路からの迷惑メールからのメール削減に寄与に期待したい。

※1:http://www.maawg.org/about/publishedDocuments

送信ドメイン認証

メール送信元情報のうち、ドメイン名が送信元に対して正当であるかを確認するための認証技術である。

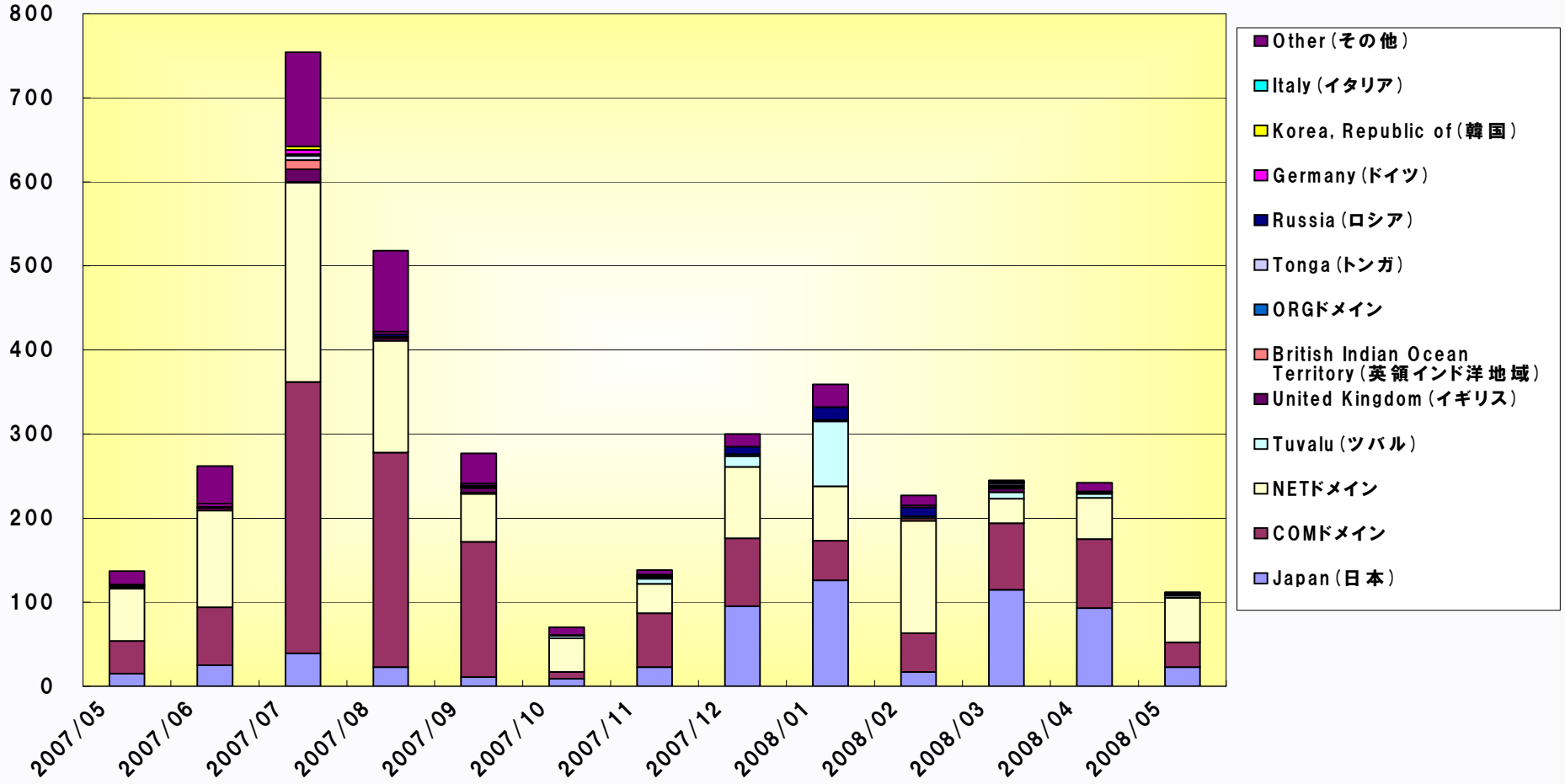
送信ドメイン認証はあくまでも認証技術であって、その結果だけでは迷惑メールであるか判定は出来ない。しかしながら、送信元のドメインの詐称判定や、送信元の特定が可能になる。そこで、受信ブロックやフィルタリング技術、レピュテーション技術などを組み合わせることで、迷惑メールを効果的に減少させられると期待できる。(JEAG Recommendation より)

アドレス詐称の状況とその問題点について

- 迷惑メールの大半が、ドメイン詐称や架空のドメインを用いて送信している状況である。
  - 詐称するアドレスは、実在する他人のアドレスを用いて送信しているケースも見受けられる。
    - ✓ 詐称されたドメインが、宛先不明等のエラーメールで詐称された側のメールサーバに大量のメールが送信され、場合によっては障害となるケースもある。
    - ✓ 送信失敗により、詐称されたユーザに対してエラーメールが送信され、そのメールを受け取ったユーザが疑心、不安になるケースがある。
- 詐称されるドメインの多くは、“jp”、“com”、“net”等、日本国内で多く使用されているドメインが多い。
  - 一部上場企業から、各種団体、政治家のドメインまでありとあらゆるドメインから送信している。
- もう一つの傾向として、紛いドメインも多く用いられてている。
  - この場合は、サブジェクトや本文も騙っているような文言を使う場合が多い。
    - ✓ 詐称方法によっては、ユーザも信用してしまう可能性もある。

送信に用いるドメイン分布について

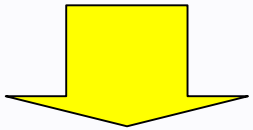
迷惑メールの多くは、依然として送信元を詐称して送信している状況である。
2007年5月1日～2008年5月11日の調査データにおいて、送信に用いられているドメインの大半は、“.jp”、“.com”、“.net”が占めいている。



※：本データは、個人が所有する携帯電話一台に送信されたメールを集計したものであり、全体の傾向を表す物ではありません。　（サンプル数：3,641通）

アドレス詐称した迷惑メールの対策する上において・・・

- 既存のメールの仕組みの中で対応出来る事が必要。
- 当然ではあるが、詐称している事が判別可能である事。



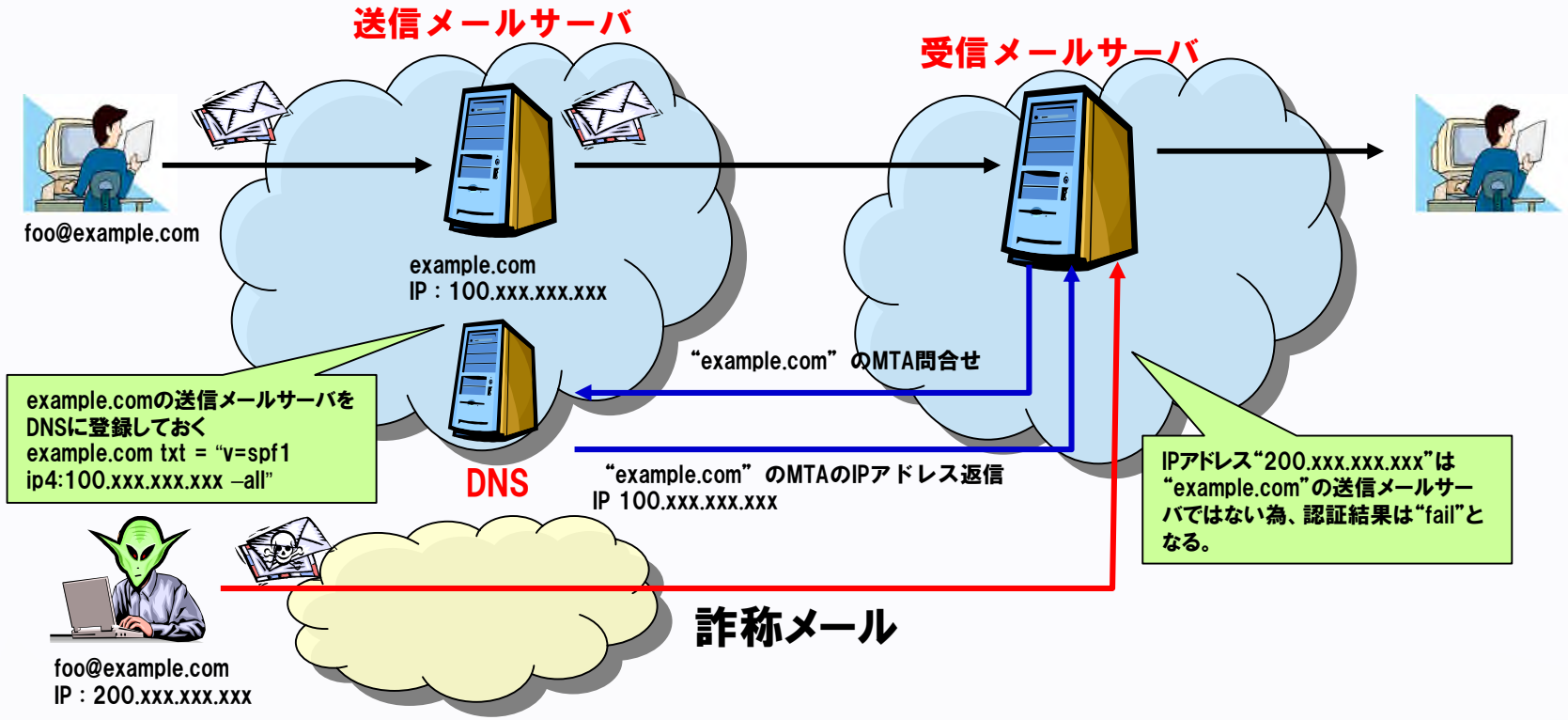
これを実現出来るのが、
「送信ドメイン認証技術」である。

- 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）

送信ドメイン認証とは

送信側と受信側が協力して、成り立つ技術である。

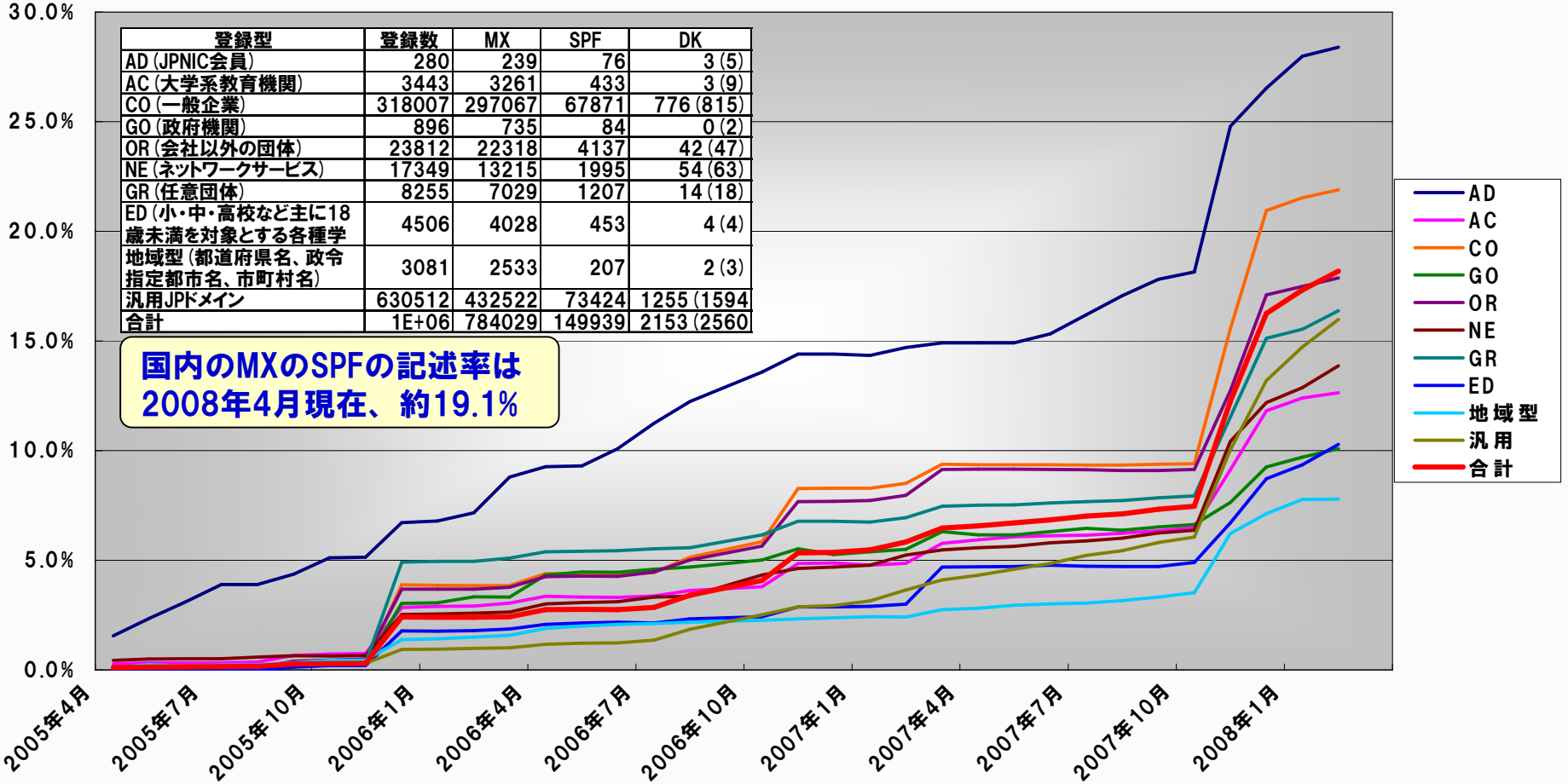
- 送信側は、自分が管理しているドメインのメールを送るサーバを宣言する。
  - 例えば、“example.com”のドメインのメールを送るサーバのIPアドレスが“100.xxx.xxx.xx”であれば、“example.com”のメールを送信するサーバは“100.xxx.xxx.xx”ですとDNSにSPFレコードを記述するだけである。したがって、**送信側は開発の特に必要はない**。
- 受信側は、受信したメールアドレスのドメイン情報から、そのドメインのメールを送るサーバのIPアドレスをDNSサーバに問い合わせて認証し、その結果をメールヘッダに記述を行う。



送信ドメイン認証(SPF)の普及状況について

WIDE プロジェクトが、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いる調査結果を以下に示す。データでは“co.jp”ドメインのSPF記述率が22.8%となっており、2008年5月12日時点での株価時価総額TOP100企業における、SPF記述率も22%となっており、約4～5社に1社はSPFを記述している状況になっている。

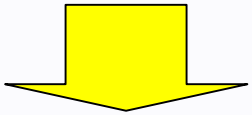
登録型	登録数	MX	SPF	DK
AD (JPNIC会員)	280	239	76	3 (5)
AC (大学系教育機関)	3443	3261	433	3 (9)
CO (一般企業)	318007	297067	67871	776 (815)
GO (政府機関)	896	735	84	0 (2)
OR (会社以外の団体)	23812	22318	4137	42 (47)
NE (ネットワークサービス)	17349	13215	1995	54 (63)
GR (任意団体)	8255	7029	1207	14 (18)
ED (小・中・高校など主に18歳未満を対象とする各種学	4506	4028	453	4 (4)
地域型 (都道府県名、政令指定都市名、市町村名)	3081	2533	207	2 (3)
汎用JPドメイン	630512	432522	73424	1255 (1594
合計	1E+06	784029	149939	2153 (2560



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

送信ドメイン認証(SPF)記述時の注意点

- SPFを記述する際に、記述内容が間違っている場合が、多々見受けられる。（記述が間違うと、PermErrorになってしまう。）
  - スペルミス（ipv4と“vが余計に入っている）
  - 不要なスペースが入っている
  - SPFを複数行記述している
  - include文がお互いを参照している
  - 不要なダブルクォーテーションが入っている、等々
- 本来記述すべきIPアドレスが含まれていない。（管理上のミス？）
  - 有名なメルマガ等でも確認事例がある



記述ミスがあると、正しいメールも詐称とされる場合があり、本来の目的が達成出来なくなる。
したがって、記述後は、SPF認証しているサービスにテストメールを送信して確認する等、確認作業を実施する事を推奨する。