迷惑メールの最新動向と
実施すべき技術的対策等について

KDDI株式会社
FMCプラットフォーム開発部
本間　輝彰

2008/3/26

迷惑メールの最新動向

- 日本国内状況はよくなっておらず、悪化の一途であり、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。
  - 日本国内発における状況（問題点）
    - →OP25B（Outbound Port 25 Blocking）の効果により、*動的IP発の迷惑メールを削減し大きな効果*を上げた。しかしながら、*OP25B未実施*の動的IPからの*未だ迷惑メールを送信し続けている*ようである。
    - →迷惑メール送信者の一部はメール配信業者のサービスを利用しての送信や固定IPから送信を行っており、*国内発*についてはこの点が*最大の問題点*である。
  - 海外発における状況（問題点）
    - →*依然Bot発*と思われるメールが*増え続*けている。（迷惑メールを送信して来る国が世界中に広がっている。）
    - →迷惑メール配信業者の一部は、*海外を活動拠点にして送信*していると推測出来る。

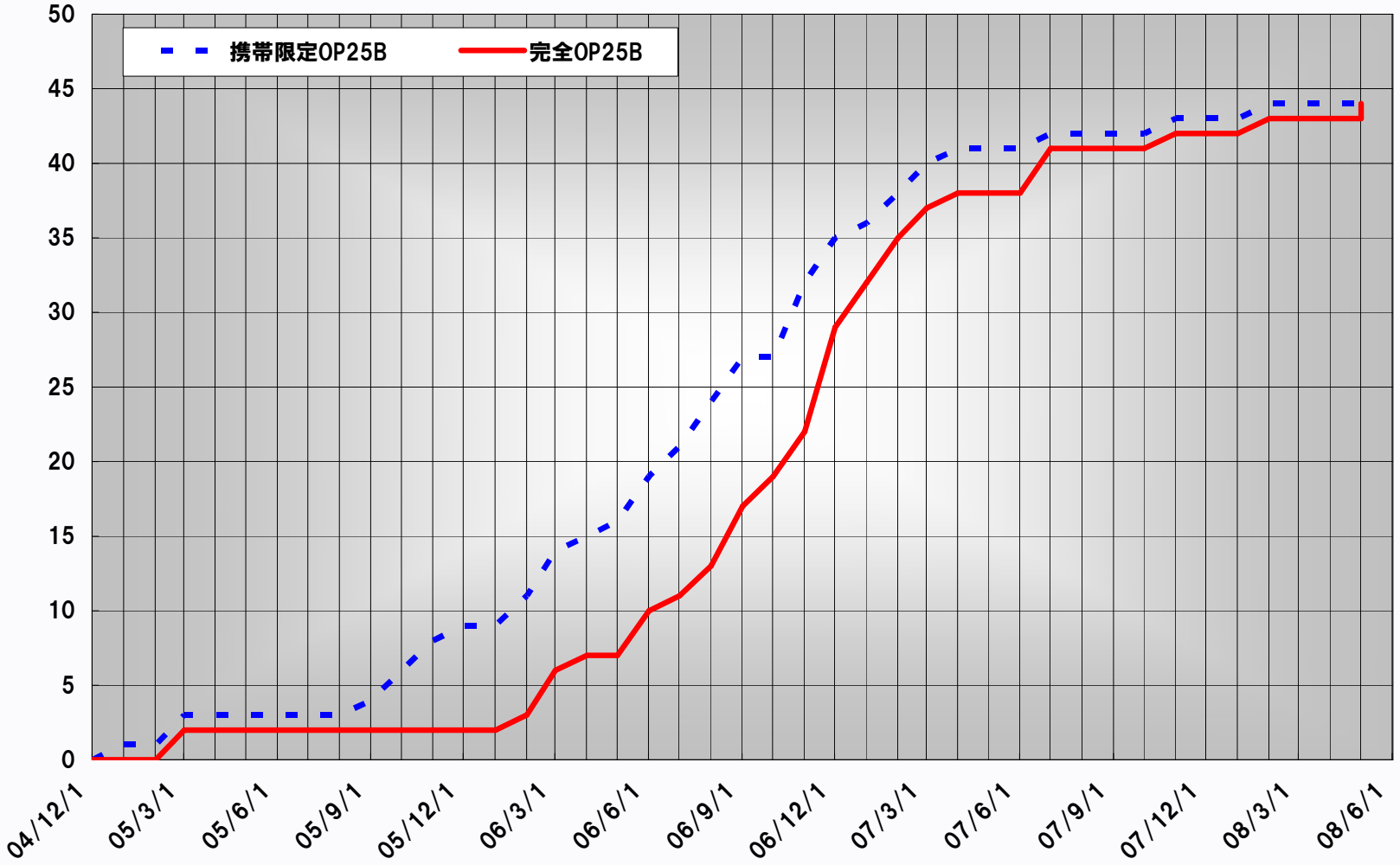
Outbound Port25 Blocking（OP25B）

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の実施状況

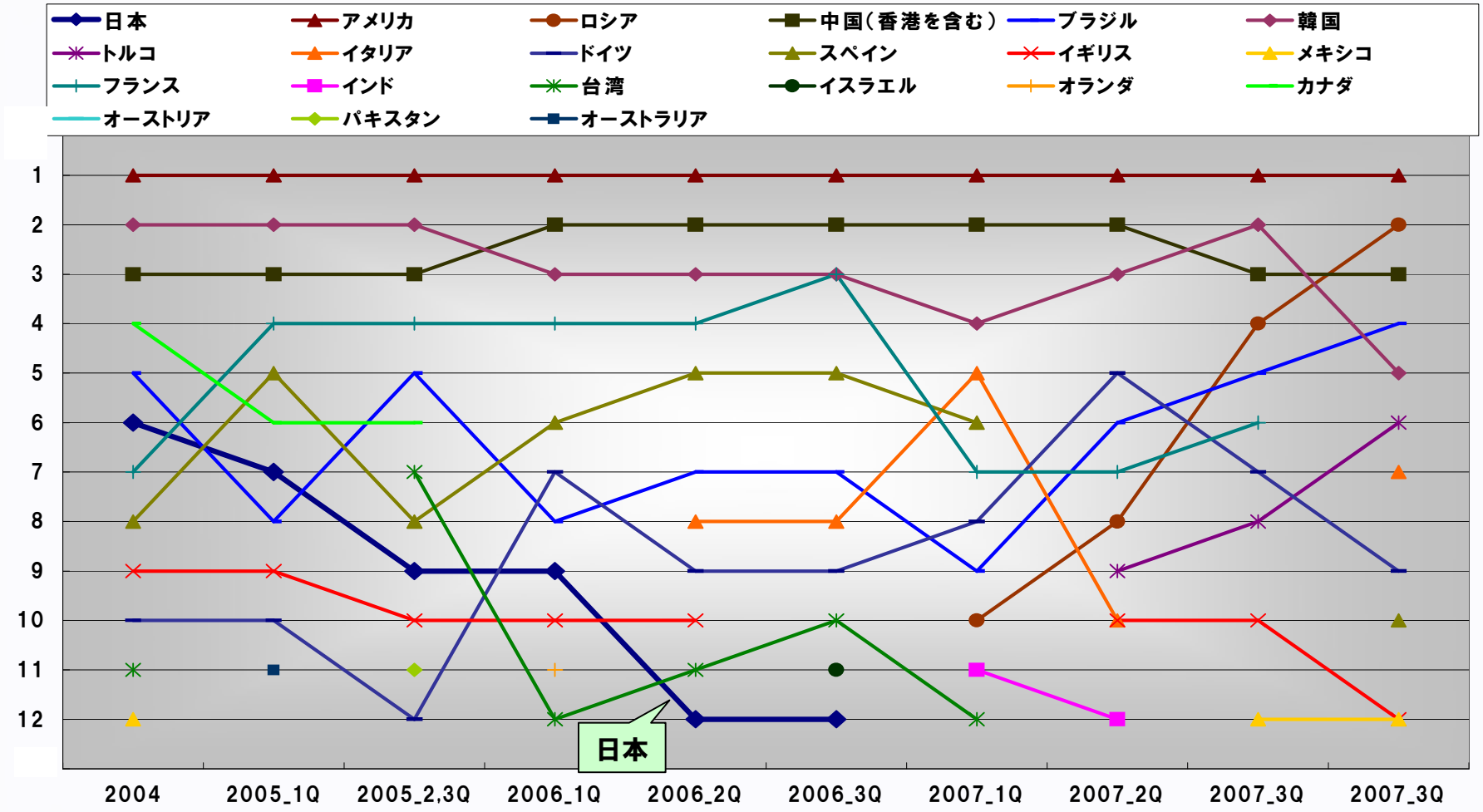
日本データ通信協会にて調査データでは、国内ISPのOP25B実施している数は以下の通りであり、最近の実施はわずかである。



※：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

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のデータにおいても、日本発は2006年3Q以後は圏外となっており、この結果はOP25Bの実施による効果と想定している。



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

OP25B実施にむけて

- 多くのISPがOP25Bを実施しており、導入の障壁はなくなりつつある。（日本でOP25Bが普及した理由）
  - ISP/ASPの多くは、自社で提供しているメールサーバについては、SMTP AUTH＋Submission Port（Port 587）を提供している為、25番Portをブロックした際に、自網外のメールサーバ経由でメール送信出来ないという問題はほぼ無くなっている。
  - あるISPがOP25Bを実施すると、そのISPを利用していた迷惑メール送信者がOP25B未実施のISPに移行する為、OP25Bを実施しないと自社に迷惑メール送信者を抱える可能性が出てくる。
- OP25Bの導入をし易くする為、メールを送信時にSMTP AUTH＋Submission Portの利用を促進して行く事が望ましい。
  - SMTPプロトコルは通常は認証を実施していない為、OP25B実施後でも自網内のユーザであれば自ISPのメールサーバを踏み台にして迷惑メール送信が可能である。これを抑止する為に、認証を実施し、もし踏み台とされても、送信者を特定し易い仕組み、さらには通数制限を入れるなどの対応する事が望ましい。
  - SMTP AUTH＋Submission Portを普及させる為に、MUA（メールクライアント）のデフォルト設定にする、自動設定ツールを提供する等の対応がしてくると普及が加速すると可能性があると想定する。
  - セキュリティを高める為には、送信時に認証を行う事は必要不可欠であり、この意味でもSMTP AUTH＋Submission Portを使う価値がある。

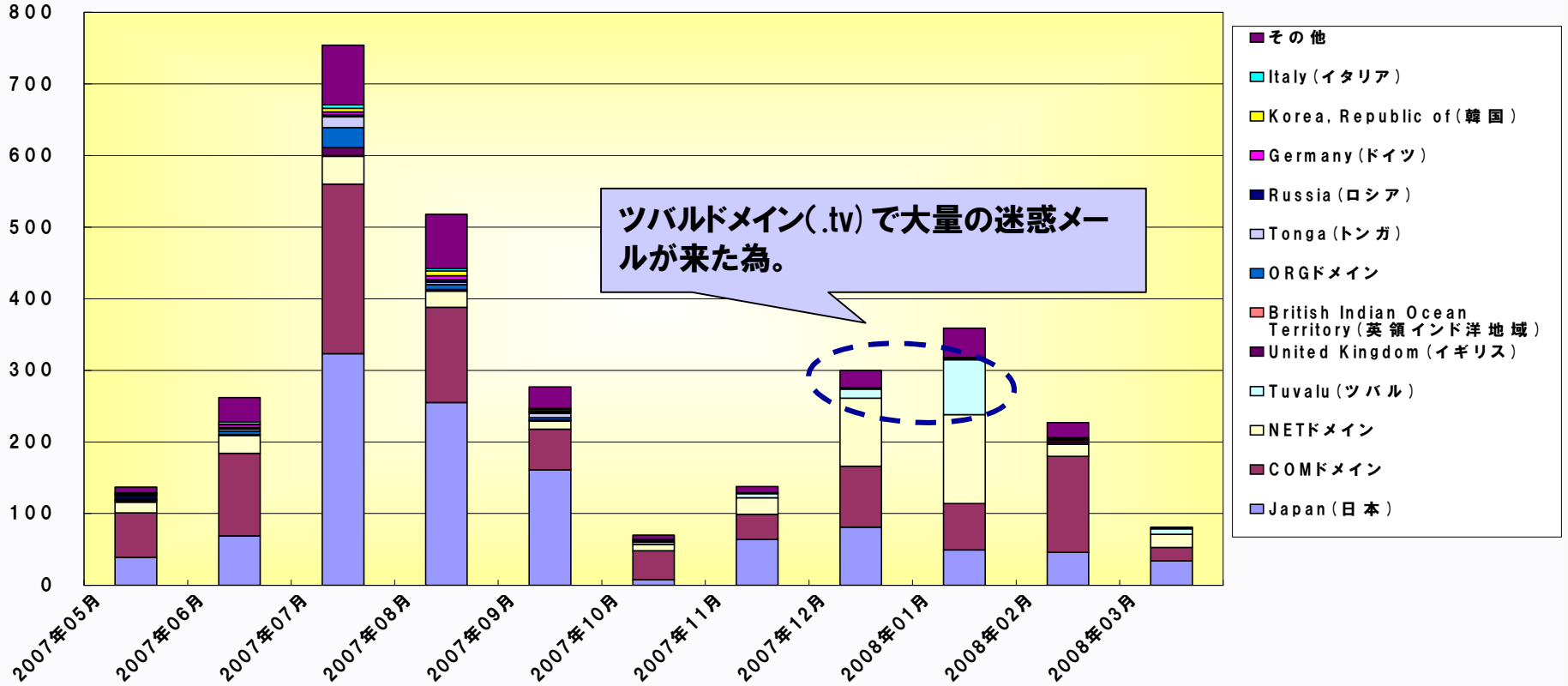
送信ドメイン認証

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)

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3月5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。
これの受信データの大半は詐称ドメインと想定され、これをドメイン認証で詐称と判定出来れば、除去する事も可能となる。

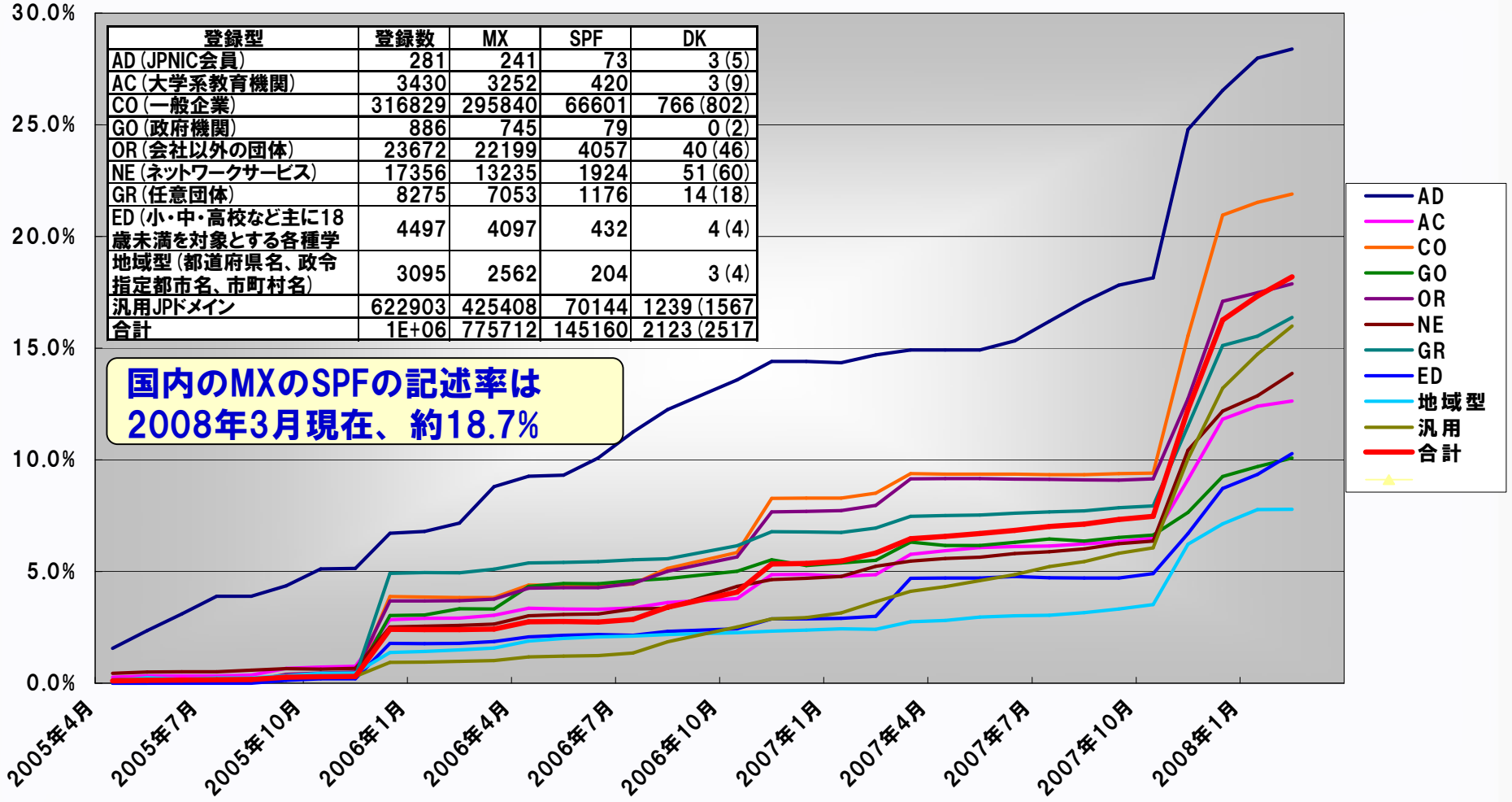


※:本データは、個人が所有する携帯電話一台に送信されたメールを集計したものであり、全体の傾向を表す物ではありません。 （サンプル数:3,123通）

実施すべき技術対策について

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。

登録型	登録数	MX	SPF	DK
AD (JPNIC会員)	281	241	73	3 (5)
AC (大学系教育機関)	3430	3252	420	3 (9)
CO (一般企業)	316829	295840	66601	766 (802)
GO (政府機関)	886	745	79	0 (2)
OR (会社以外の団体)	23672	22199	4057	40 (46)
NE (ネットワークサービス)	17356	13235	1924	51 (60)
GR (任意団体)	8275	7053	1176	14 (18)
ED (小・中・高校など主に18歳未満を対象とする各種学	4497	4097	432	4 (4)
地域型 (都道府県名、政令指定都市名、市町村名)	3095	2562	204	3 (4)
汎用JPドメイン	622903	425408	70144	1239 (1567
合計	1E+06	775712	145160	2123 (2517



国内のMXのSPFの記述率は
2008年3月現在、約18.7%

※: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

送信ドメイン認証導入に向けて

- **送信側はSPFの記述する事を、強く推奨する。**
  - 受信側の対応が進んだ為、送信側で記述するメリットが増えている。
  - ドメインを詐称して送信されるケースが多々見受けられ、自ドメインを守る意味で送信元を明らかにする意味が高くなっている。
  - SPFを記述していても、記述内容が間違っているケースがあるので、記述内容の確認が必要である。（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、等による設定ミスが散見されている。
- **受信側は、SPFの認証を実施し、その結果を積極的に活用する事を推奨する。**
  - 国内のSPFレコードの記述率は18%を超え、認証対象となるメールはそれを遙かに超えた割合を占めており、認証するには十分な条件になりつつある。
  - 認証結果から、送信アドレスを詐称しているか判別可能となる。その結果を利用する事で、アドレス詐称してくるメールの受信を拒否する等の対応が可能となる。

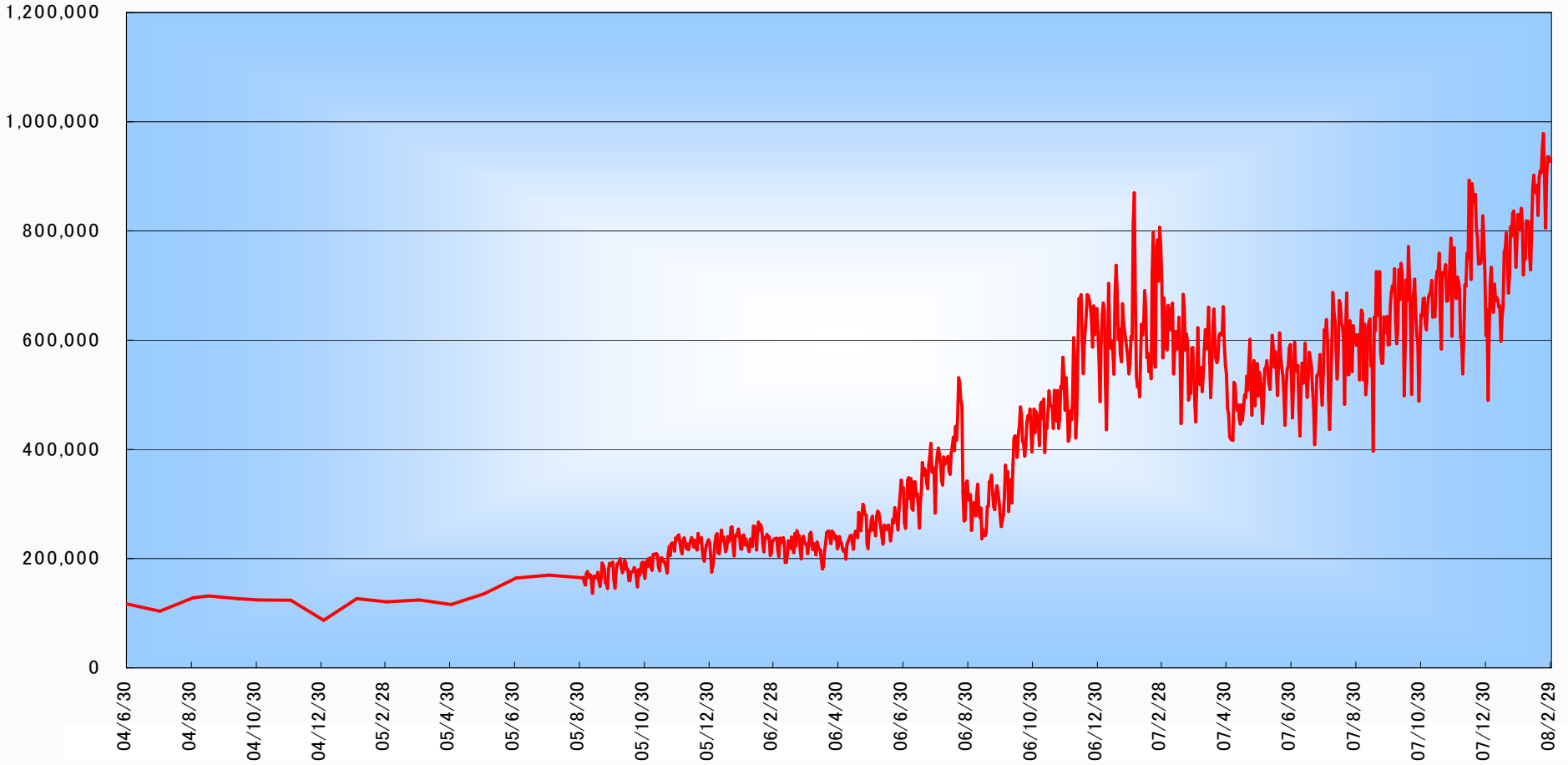
海外発迷惑メール

インターネットには国境がない為、迷惑メールは日本国内のみならず、広く海外から送信されてきている状況である。

特にOP25Bの導入が進んでからは、海外発の迷惑メールは増加の一途を辿っている。

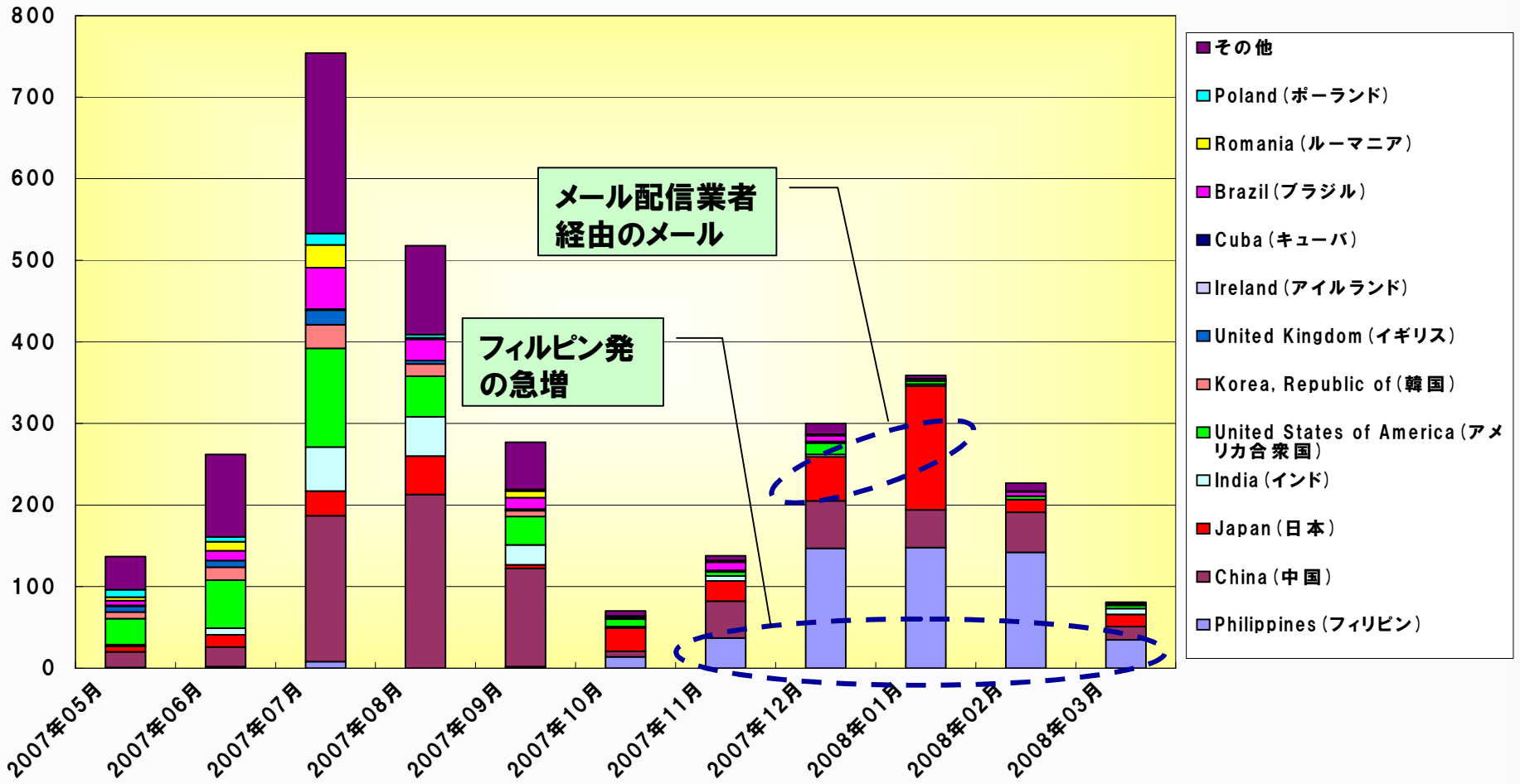
ユニークIP数推移

メールの送信元(IP数)は、2004年当時は10数万IP/日であったものが、最近では日当たり100万に届く勢いである。この増えている要因の大半が海外送信のIPであり、この結果からも海外発の迷惑メールが増えていると推測出来る。



送信国状況について

2007年5月1日～2008年3月9日の調査データを下記に示す。受信データからその多くが、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：3,123通）

海外発の迷惑メール対策について

海外発の迷惑メール対策については、各国の事情もあり即効性のある対策は存在しないが、継続的な対策は検討していく必要がある。

- **日本における迷惑メール対策の成功事例を各種WGでインプットし続ける。**
  - Outbound Port 25 Blockingの成功事例を海外に発信する。
    （その国の事情により、すぐに出来るものではないが、日本での成功事例は一つの参考事例としてインプットし続ける必要がある）
  - これまでも、MAAWGでの発表、KISA（韓国情報保護振興院)との意見交換、等を実施。

- **総務省、経済産業省が取り組んでいる国際連携の強化への期待。**
  - ISPが個別に対応するには非現実的であり、国家レベルでの連携強化に期待したい。
  - 国の施策にISPとしても、出来る限り協力していく事が重要である。

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。

海外のメール配信業者の取り組み

- 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。
  - Obtain Clear and Conspicuous Consent
    - ➔同意の取り方について
  - Enable Clear, Conspicuous, and Easy to Use Unsubscription Options
    - ➔解除方法について
  - Enhancing Sender Accountability and Messaging Reputation
    - ➔送り主の責任強化とメール送信に関するレピュテーションについて
  - Managing Delivery Errors and List Maintenance
    - ➔配信エラーとリストメンテナンスについて
  - Mitigating and Resolving Messaging Disruption Issues
    - ➔メッセージ配信時の負荷軽減について

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

まとめ

実施すべき技術対策について

- OP25Bは完全実施に向けて進めるべきである。
  - OP25B未実施の接続先からの迷惑メールは増えつつあると想定している為、未実施のポイントについての積極的導入を推奨する。
  - OP25Bの実施を海外についても継続して訴求していく必要がある。出来ない場合は、代替えの対策を実施する必要がある。（海外ISPの一部では、トラフィックをねじ曲げて、ISPでモニタしている所も存在しているらしい。）
- 送信ドメイン認証は積極的に対応して行く事が望ましい。
  - 受信側の対応が進んだ事もあり、SPFの宣言率は18.2%伸びており、メールを送るドメインについては、SPFレコードを記述する事が望ましい。
  - 新しい法令では、宛先を詐称して送信する事が禁じられているので、送信ドメイン認証の活用し、受信ブロック等に役立てられる可能性がある。
- 海外の政府、事業者等に対して、日本の成功事例（特にOP25B）をインプットして行く必要がある。また、迷惑メール送信者の情報交換を出来る基盤整備が必要である。
- （配信業者経由の迷惑メール関しては、今後法令化される法律による対応に加え、メール配信業者での管理に期待したい。）