

制度面以外の提言の方向性（案）

平成23年2月18日
事務局

目 次

- 3 電気通信事業者による自主的な取組み
- 4 広告関係事業者等による自主的な取組み
 - (a) 広告関係事業者による取組み
 - (b) メール配信事業者による取組み
 - (c) アフィリエイト事業者による取組み
- 5 適正な電子メール環境の整備
- 6 技術的対策
 - (a) OP25B(Outbound Port 25 Blocking)
 - (b) 送信ドメイン認証技術
 - (c) その他の技術的対策
- 7 利用者への周知啓発
- 8 国際連携の推進
- 9 総合的対策

3 電気通信事業者等による自主的な取組み

現状

- ・ 電気通信事業者等による自主的な取組として、契約約款に基づく利用停止等の措置を実施
- ・ 利用停止措置を受けた契約者の情報を事業者間で交換し、いわゆる「渡り」を防止
- ・ 今後、スマートフォンの普及が進展することが予想される。
(2010年8月現在、携帯電話販売台数に占めるスマートフォンの構成比は20%超(BCN調査))

論点

- 約款に基づく利用停止等の措置等が行われているが、電気通信事業者が新たに取り得る自主的な取組みとして、どのようなものがあるか。
- 携帯電話各社で検討中のSMSの相互接続に起因して迷惑メールが増加することはないか。
- スマートフォンでの迷惑メール対策は適切に行われているか。

【利用停止等の措置】

■ 電気通信事業者では、契約約款等に基づき、迷惑メールの送信者等に対して、利用停止や契約解除等の措置を実施してきている。また、2005年(平成17年)からは、総務省により、モニター機で受信した迷惑メールについて、国内の送信元のプロバイダに情報提供する「迷惑メール追放支援プロジェクト」が行われている。これらの取組は、迷惑メールの送信者等に対して、直接的な措置を行うものであり、効果が大きいことから、継続して実施していくべきである。

【電気通信事業者間の情報交換】

- ある電気通信事業者から迷惑メールの送信行為を原因として利用停止や契約解除の措置を受けた利用者が、他の電気通信事業者と契約して、引き続き迷惑メールを送信する、いわゆる「渡り」と呼ばれる行為が見られる。
- このため、携帯電話事業者では、2006年(平成18年)より、迷惑メール等の送信行為により利用停止等の措置を受けた加入者に関する契約者名、住所等の情報の交換を実施してきている。この取組は、携帯電話発の迷惑メール対策の一つとして効果が大きいことから、継続して実施していくべきである。
- また、現在、携帯電話事業者各社では、SMS(Short Message Services)の相互接続について検討している。それに伴い、SMSでの迷惑メールが増加するおそれがあることから、SMSにおける迷惑メール等の送信行為による利用停止等を受けた加入者の情報交換についても、相互接続の開始当初より実施することを検討すべきである。

【虚偽登録等への対応】

- インターネット接続や、ドメイン名等の取得の際の契約に関し、その契約者の情報が必ずしも正確でない場合があるという指摘がある。契約者の情報が正確でないと、迷惑メールの送信行為を原因として契約解除を行った場合でも、再度の契約申込みの際の審査が十分にできなかつたり、法執行にあたり支障が発生するおそれがある。
- このため、電気通信事業者等において、本人確認が可能な場合には、その業務に必要な範囲で、本人確認を行う等の取組を実施していくことが望ましい。特に、OP25Bを導入した場合であっても、受信側メールサーバに対し、直接、電子メールの送信が可能な固定IPアドレスの利用者に対しては、電気通信事業者各社において、迷惑メール送信に用いられた場合の対応を適切に行うことが望ましい。

【迷惑メール対策のためのサービスの提供】

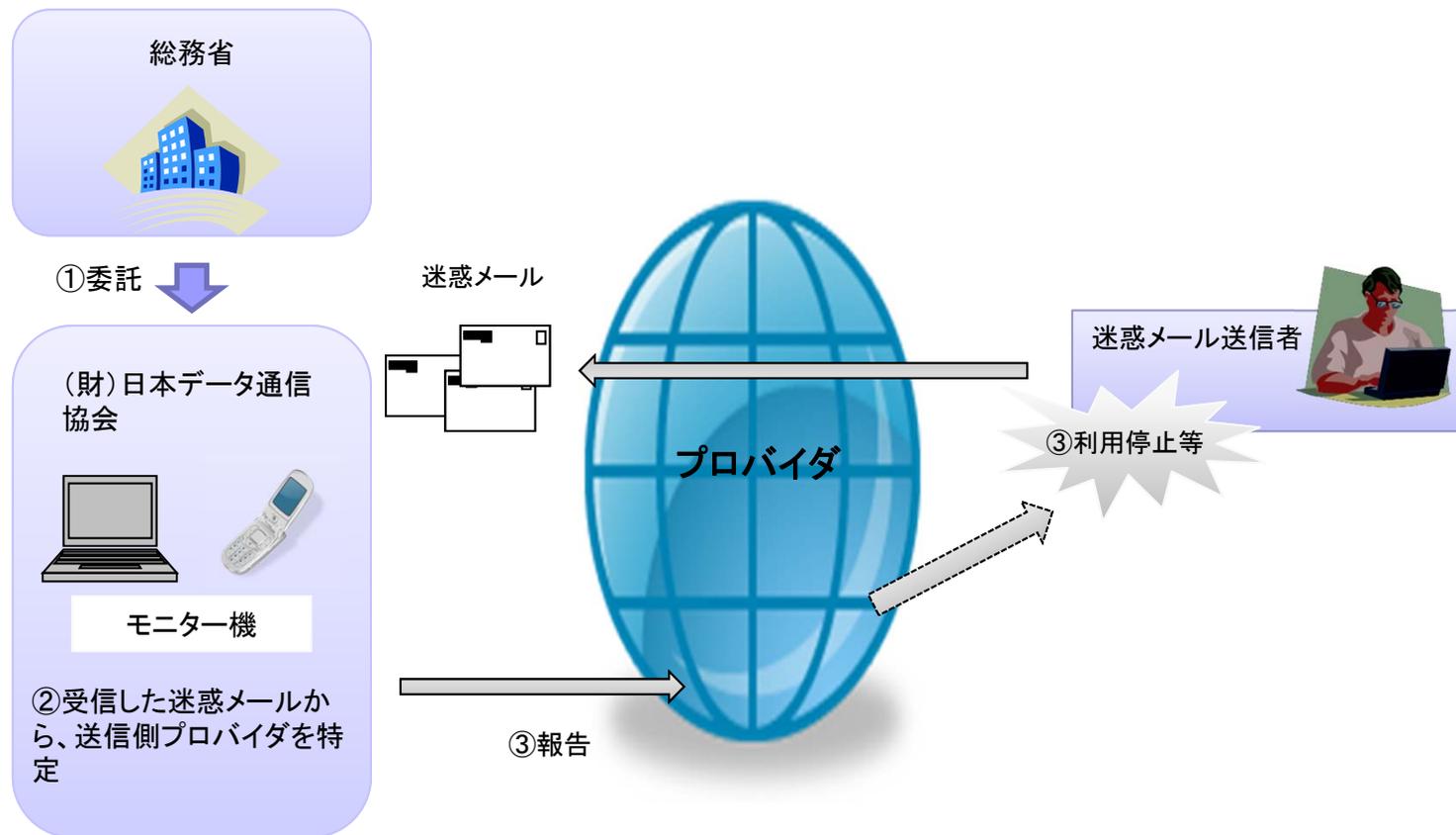
- 電気通信事業者等では、利用者に対して、フィルタリング等の迷惑メール対策のサービスを提供している。これらのサービスを利用することにより、受信者は、迷惑メールを受信しないことや受信した迷惑メールを迷惑メールフォルダに隔離すること等が可能となっている。受信者側の個別の設定により効果的な迷惑メール対策を可能とするものであるため、電気通信事業者等では、引き続き、こうした迷惑メール対策のサービスの提供に努めていくべきである。
- その際、電気通信事業者等が提供する迷惑メール対策のサービスは、多様化・高度化してきていること、電気通信事業者等により名称や設定方法等が異なることなどから、利用にあたっての設定が難しいとの指摘もある。このため、携帯電話事業者をはじめ、電気通信事業者等では、設定方法の周知や、一括して簡単に設定できる機能の提供などの対応をしてきている。
- 引き続き、電気通信事業者等において、サービスの名称や設定方法等について可能な限り統一的な対応をしていくことや設定方法をわかりやすく解説すること等、利用者の利便を向上させ、迷惑メール対策サービスの利用促進のための取組を実施していくことが望ましい。
- また、例えば、迷惑メールの大部分を諸外国発のものが占める中で、利用者の同意を受けて、一定の国・地域から送信される迷惑メールをフィルタするようなサービスを求める意見もあることから、今後も、引き続き、より効果的なサービスの開発を進めていくことが望ましい。

【スマートフォンでの迷惑メール対策】

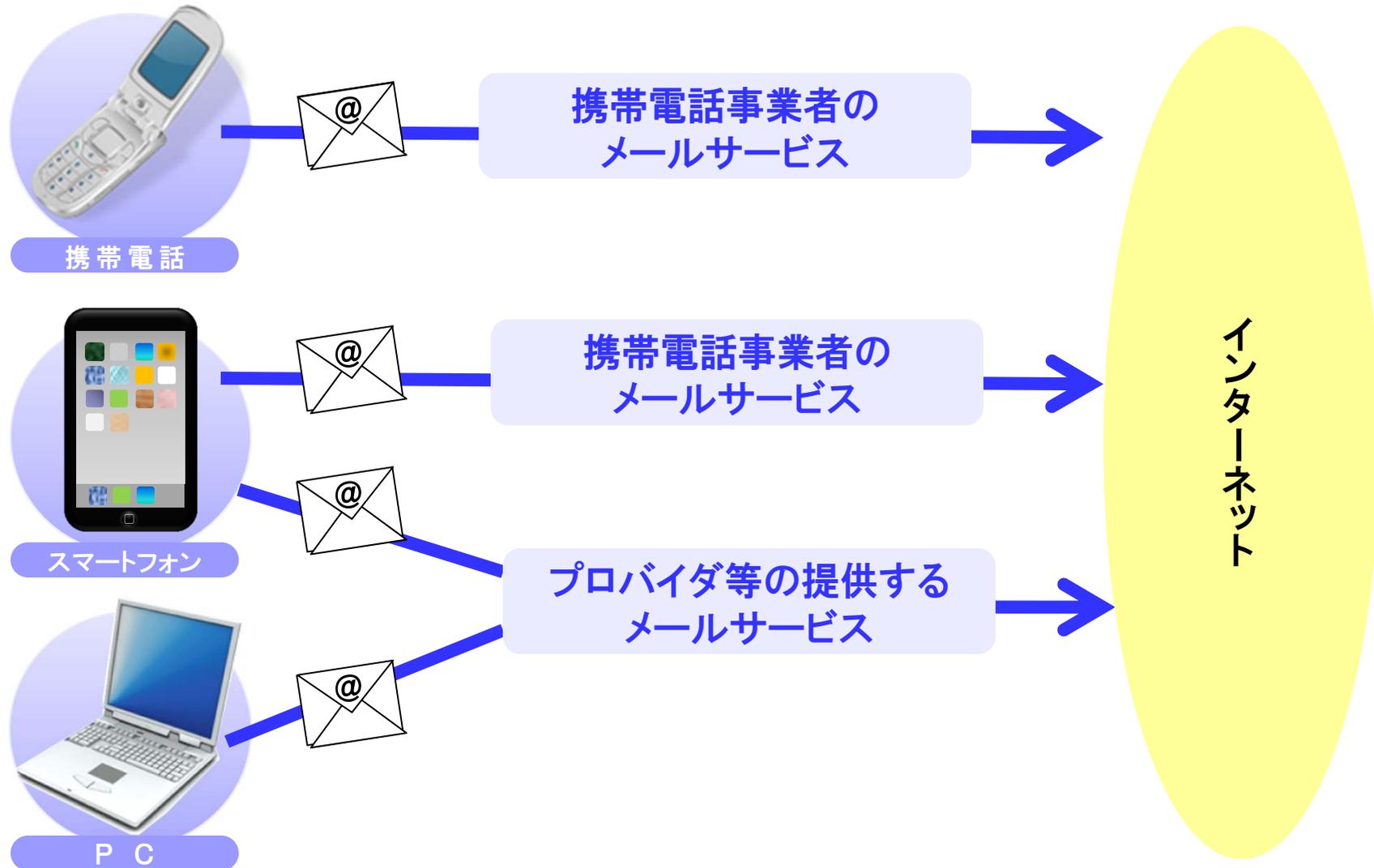
- スマートフォンにおける電子メールサービスをみると、携帯電話事業者が提供する電子メールサービスだけでなく、他の電気通信事業者が提供する電子メールサービスも利用可能となっている。
- 携帯電話事業者各社では、スマートフォン向けの電子メールサービスについても、従来の携帯電話機向けに提供する迷惑メール対策機能とほぼ同様の機能を提供しており、携帯電話事業者が提供する電子メールサービスを利用する場合には、それらの機能を利用することが可能である。一方で、他の電気通信事業者が提供する電子メールサービスを利用する場合には、それらの機能を利用することはできず、当該電子メールサービスの迷惑メール対策機能を利用することとなる。
- 利用者は、スマートフォンを利用するにあたっては、このような状況を理解し、適切に迷惑メール対策機能を利用することが望ましい。また、携帯電話事業者は、利用者に対して、スマートフォンの利用にあたっての迷惑メール対策の観点からの注意点について、適切な周知を行うことが必要である。

迷惑メール追放支援プロジェクト

総務省は、2005年から、プロバイダ及び携帯電話事業者等と連携して、迷惑メール送信回線の利用停止措置等の円滑な実施を促す「迷惑メール追放支援プロジェクト」を実施。



スマートフォンは、携帯電話事業者の電子メールサービスの他、様々な電子メールサービスを使用することが可能。



(※)Wi-Fiによりインターネットに接続するなど携帯電話回線を用いず、携帯電話事業者のメールサービスを用いることができないスマートフォンもある。

スマートフォンと従来の携帯電話との迷惑メール設定機能の相違

【NTTドコモ(迷惑メール設定機能)】

機能名称	概要	spモード	iモード
かんたん設定	迷惑メール設定を簡易な操作で実施	○	○
URL付きメール拒否設定	URL付きメールを拒否	○	○
宛先指定受信	なりすましメールを拒否設定にした場合に、送信元等の電子メールアドレスを指定することで指定したアドレスからのメールの受信が可能	10件	10件
ドメイン・アドレス受信設定	ドメイン及びメールアドレスを指定して受信する	120件	120件
アドレス拒否設定	指定したメールアドレスの受信を拒否する	120件	120件
ドメイン拒否設定	指定したドメインの受信を拒否する	120件	120件
なりすましメール拒否	なりすましのメールの受信を拒否する	○	○
iモード/spモードメール大量送信者からのメール受信制限	1日あたり1台から送信される500通目以降のiモード/spモードメールの受信を拒否する	○	○
未承諾広告※メール拒否	「未承諾広告※」が付いた電子メールの受信を拒否する	○	○

※NTTドコモが提供するメールサービスを利用する場合。

(参考) 同時送信機能

	spモード	iモード
同時送信	100件まで	5件まで

スマートフォンと従来の携帯電話との迷惑メール設定機能の相違

【KDDI(迷惑メール設定機能)】

機能名称	概要	スマートフォン	EZweb
カンタン設定	迷惑メール設定を簡易な操作で実施	○	○
一括指定受信	インターネット、携帯電話各社、PHSからの電子メールを受信するかどうか選択して一括設定する。	○	○
なりすまし規制	なりすましのメールの受信を拒否する	高・中・低	高・中・低
指定拒否リスト設定	指定したドメインやメールアドレスの受信を拒否する	200件	200件
指定受信リスト設定	指定したドメインやメールアドレスの受信を許可する	200件	200件
指定受信リスト設定 (なりすまし転送メール許可)	なりすまし規制を設定した場合に、送信元等の電子メールアドレスを指定することで指定したアドレスからのメールの受信が可能	20件	20件
HTMLメール規制	携帯、PHS以外から送信されるHTML形式のメールの受信を拒否する	○	○
URLリンク規制	URL付きメールを拒否	○	○
拒否通知メール返信設定	メールフィルタで受信をブロックしたメールに対し、拒否通知メールを返信する	○	○
ワンタッチ拒否登録	受信したメールアドレスに含まれるメールアドレスから簡易に指定拒否リストに登録する	○	○

※auが提供するメールサービスを利用する場合。

(参考) 同時送信機能

	スマートフォン	EZweb
同時送信	30件まで	30件まで

スマートフォンと従来の携帯電話との迷惑メール設定機能の相違

【ソフトバンク(迷惑メール設定機能)】

機能名称	概要	スマートフォン S!メール(MMS)	従来の携帯電話 S!メール(MMS)
かんたん設定	各種迷惑メールブロック設定を、一括設定	○	○
なりすましメール	送信元アドレスを携帯電話・PHS事業者のドメインに詐称したメールを拒否	○	○
ともだちメール安心設定	S!電話帳バックアップに登録されたメールアドレスからのEメールを受信	×	○(*1)
未承諾広告メール拒否設定	件名に「未承諾広告※」と表示のあるメールを拒否	○	○
URLリンク付きメール拒否設定	特定URLもしくはすべてのURLを含むメールを拒否	○	○
受信許可・拒否設定	特定のアドレスやドメイン等からのメールを「受信拒否」、「受信許可」または「ケータイ/PHSからのみ受信」を設定	○	○
海外からの拒否設定	海外事業者から電話番号で送られてくるメールを拒否	○	○
迷惑メールフィルター	迷惑メールフィルター機能を利用できる	○	○

※ソフトバンクが提供するメールサービスを利用する場合。

(*1) S!電話帳バックアップに加入していない場合は、当ブロック機能は無効となる。

(参考) 同時送信機能

	スマートフォン S!メール(MMS)	従来の携帯電話 S!メール(MMS)
同時送信	20件まで	20件まで(*2)

(*2) 但し、一部の機種は除く。

スマートフォンと従来の携帯電話との迷惑メール設定機能の相違

【イー・モバイル(迷惑メール設定機能)】

機能名称	概要	スマートフォン EMNET	従来の携帯電話 EMNET
全受信	全ての受信を許可	○	○
指定拒否設定	指定した文字列が送信者のアドレスに部分的に含まれる場合、メールの受信を拒否	20件	20件
メールアドレス指定受信	指定した文字列が送信者のアドレスに部分的に含まれる場合、メールの受信を許可	20件	20件
ドメイン指定受信	既存キャリアのドメインのうち、指定するドメインから送られてくるメールのみを受信	○	○
URLフィルタ拒否	本文中にURLが含まれるメールの受信を拒否	○	○
未承諾広告拒否	件名に「未承諾広告※」を含むメールを拒否	○	○
なりすまし規制	PCから携帯電話・PHSのメールアドレスを用いて、携帯電話・PHSから送信されたかのように装ったメールの受信を拒否	○	○
送信ドメイン認証	送信元のIPアドレスについて、送信元のSPFLコードと合致しないメールを拒否	○	○
拒否通知の送信	メールフィルタ設定で拒否されたメールに対し、拒否したことを相手に通知	○	○

※ イーモバイルが提供するメールサービスを利用する場合。

(参考) 同時送信機能

	スマートフォン EMNET	従来の携帯電話 EMNET
同時送信	10件まで	10件まで

スマートフォンと従来のPHSとの迷惑メール設定機能の相違

【ウィルコム(迷惑メール設定機能)】

機能名称	概要	スマートフォン	従来のPHS
未承諾広告メール拒否	件名に「! 広告!」「未承諾広告※」と表示のあるメールを拒否	○	○
メールアドレス指定受信拒否	指定したメールアドレスの受信を拒否	20件まで	20件まで
メールアドレス指定受信	指定したメールアドレスを受信	20件まで	20件まで
メールアドレス変更	電話機からメールアドレスを変更	○	○

(参考) 同時送信機能

	スマートフォン	従来の携帯電話
同時送信	100件まで	100件まで

※PHS端末の場合、端末側で機種により更に低い制限を設定(直近の機種で最大20件)

4 広告関係事業者等による自主的な取組み (a) 広告関係事業者による取組み

現状

- ・ 広告関係事業者（媒体社、広告会社等）の取組みとして、電子メール広告に関する業界ガイドライン、自主基準等を定め、法の遵守に努めてきている。

論点

- 広告関係事業者の取組みとして、さらにどのようなことが期待されるか。

提言の方向性

【広告関係事業者による取組】

- 電子メールを用いた広告宣伝について、その適正な実施を確保するため、広告主や広告会社等の広告関係事業者や広告関係団体では、これまで、ガイドラインの策定・遵守や、法遵守の宣言の採択、会員社への説明会の実施などの取組を実施してきている。
- 広告関係事業者にとっては、正当なメール広告を行おうとしているにもかかわらず、受信者にとって迷惑メールとなってしまうことは、広告効果との関係からも問題となる。こうしたことから、広告関係事業者や広告関係団体における取組は、特定電子メール法制定前から行われてきており、適正なメール広告の実施に一定の役割を果たしている。
このため、広告関係事業者や広告関係団体において、今後も、引き続き、このような自主的な取組を実施していくことが期待される。

広告関係事業者の迷惑メール対策

	迷惑メール対策
ガイドラインによる対応	<p>■ 「インターネット広告掲載基準ガイドライン」の策定(2000年制定)</p> <p>・ガイドラインにおいて、「日本国憲法及び法律に反するような類の広告は掲載しない」等を記載。 [一般社団法人インターネット広告推進協議会]</p>
	<p>■ 「メール広告の運用ガイドライン」(2001年制定)</p> <p>・ガイドラインにおいて、「配信許諾を徹底する」、「責任の所在を明確にする」、「ユーザーからの配信拒否に対して即時対応を行う」、「迷惑行為を防止する」等を記載。 [一般社団法人インターネット広告推進協議会]</p>
	<p>■ 「メール広告のパーミッション取得のためのガイドライン」(2004年制定)</p> <p>・ガイドラインにおいて、「事前に消費者に利用目的を明示し、個人情報などがどのように取り扱われるかを理解させ、提供の有無を判断する機会を与え、パーミッション取得をしなければならない」「配信にあたっては、広告媒体者名・サービス名称など配信元の所在を明らかにするべきである」等を記載。 [一般社団法人インターネット広告推進協議会]</p>
団体としての法遵守の宣言	<p>■ 「電子メール広告の健全な発展のために ～広告に関わる者として、迷惑行為、違法行為と明確な一線を～」を公表(2003年)</p> <p>・広告に関わる媒体社、広告会社等の活動がユーザーのクレームの対象とならないよう、法の内容を正しく理解し、厳しく自らを律していくことを宣言 [一般社団法人インターネット広告推進協議会]</p>
説明会による法律の理解促進	<p>■ 「特定電子メール法改正」に伴う会員社への説明会の開催(2008年度) [一般社団法人インターネット広告推進協議会]</p> <p>■ 「特定電子メール法改正」に伴う会員社への説明会の開催(2008年度) [(社)日本アドバタイザーズ協会・(社)日本広告業協会]</p>

4 広告関係事業者等による自主的な取組み^(b)メール配信事業者による取組み

現状

- ・ メール配信事業者の取組みとして、オプトイン・オプトアウト機能の提供、配信エラーのメンテナンス機能の提供、送信ドメイン認証技術への対応等を行ってきている。

論点

- ・ メール配信事業者の取組みとして、さらに、どのようなことが期待されるか。

提言の方向性

【メール配信事業者による取組】

- 広告宣伝メールをはじめとする大規模なメールの送信については、そのための設備を専門的に提供するメール配信事業者を利用して行われることが多くなっている。
メール配信事業者では、その設備を迷惑メール送信に用いられないことがないよう、契約前の調査や運用中のモニタリングなどの対策、ダブルオプトイン機能等の標準装備、エラーメールの解析機能の提供、送信ドメイン認証技術への対応などの技術的な対策や特定電子メール法等に関する周知などの取組を実施してきている。
- 大規模なメール送信を行うメール配信事業者による自主的な取組は、迷惑メール対策として有効である。このため、メール配信事業者において、今後も、引き続き、このような取組を実施していくことが期待される。

メール配信事業者の迷惑メール対策

	迷惑メール対策
技術的な対応	<p>■ ダブルオプトイン、オプトアウト機能の標準装備 [エイケアシステムズ(株)、(株)パイプドビッツ]</p>
	<p>■ エラーメール解析エンジンの提供 (※致命的なエラー(ドメイン不明、ユーザ不明、受信拒否)になったアドレスは自動的に配信対象から除外) [エイケアシステムズ(株)、(株)パイプドビッツ]</p>
	<p>■ 送信ドメイン認証技術の導入 [エイケアシステムズ(株)、(株)パイプドビッツ]</p>
	<p>■ Fromアドレス制限(※顧客保有のドメイン以外の使用不可) [エイケア・システムズ(株)]</p>
	<p>■ 文章の自動差込機能 (※あらかじめテンプレート登録する事により、メール本文の末尾に自動的に追加されることにより、特定電子メール法の表示義務に対応) [エイケア・システムズ(株)]</p>
サービスを不適正に利用されないための対応	<p>■ 約款上で、禁止事項を記載 (※同意のない相手への配信の禁止など特定電子メール法に則した禁止事項の記載、問題がある場合に解約される旨の明記) [エイケアシステムズ(株)、(株)パイプドビッツ]</p>
	<p>■ 契約前の調査 (※メール配信の目的、お客様事業内容、Fromに使用するドメインの所有者などの確認) [エイケアシステムズ(株)、(株)パイプドビッツ]</p>
	<p>■ 運用中のモニタリング(※配信されたメール本文のキーワード検査) [エイケア・システムズ(株)]</p>

4 広告関係事業者等による自主的な取組み (c)アフィリエイト事業者による取組み

現状

- ・ アフィリエイト事業者による取組みとして、アフィリエイトターの審査、メールマガジンでの広告配信許可制の導入、ガイドラインによる禁止行為の規定等の対応を行ってきている。

論点

- ・ アフィリエイト事業者の取組みとして、さらに、どのようなことが期待されるか。

提言の方向性

【アフィリエイトサービス提供者による取組】

- 最近では、成果報酬型のインターネット広告であるアフィリエイトサービスが出現し、アフィリエイトターによる広告宣伝メールの送信が行われている。アフィリエイト広告をする媒体を保有するアフィリエイトターの中には、成果報酬を目的に迷惑メールを送信する者や、特定電子メール法による規律を知らずに違反してしまっている者もいるとの指摘もある。

このため、アフィリエイトターとの関係が深いアフィリエイトサービス提供者の団体では、ガイドラインで迷惑行為の禁止を規定したり、アフィリエイトターの審査や強制退会したアフィリエイトターの情報共有等をしたりするなど、迷惑メールの送信が行われないための取組を実施してきている。

- 今後、更にアフィリエイトターが増加していくことも考えられることから、アフィリエイトターによる迷惑メールの送信が行われないようにすることが重要である。このため、アフィリエイトサービス提供者の団体等において、今後も、引き続き、このような迷惑メール対策の取組を実施していくことが期待される。

アフィリエイト団体の迷惑メール対策

	迷惑メール対策
ガイドラインによる対応	<ul style="list-style-type: none"> ■ 「日本アフィリエイト・サービス協会 アフィリエイト・ガイドライン」で迷惑行為の一類型として、「迷惑メールの配信による自身のサイトへの誘導」を盛り込み、その行為を禁止 ■ 「モバイルアフィリエイト事業運用管理体制適合基準」で、アフィリエイトの媒体が法規違反となる場合や法規違反を誘引・助長ほう助等する場合は、利用停止する旨の審査基準を加盟社で作成することを盛り込んでいる
サービスを不適正に利用されないための対応	<ul style="list-style-type: none"> ■ 日本アフィリエイト・サービス協会の加盟社間で、強制退会処分としたアフィリエイトの情報を共有 ■ アフィリエイトの審査(加盟全社で実施) ■ 広告主が認めたアフィリエイトのサイトにのみ出稿させるため、アフィリエイトと広告主との提携の承認制(加盟全社で実施) ■ アフィリエイトによるメールマガジンでの広告配信の許可制(加盟全社で実施)

5 適正な電子メール環境の整備

現状

- ・ 短期間で大量に広告宣伝メールが送信されること等により、メール受信設備に負荷がかかる。

論点

- 広告関係事業者から一度に大量に送信される電子メールは、電気通信事業者への設備負荷が大きいことから、どのように考えるべきか。
- メルマガ等のリスト管理が不十分なことによる問題について、どのように考えるか。

提言の方向性

[毎正時の同時大量送信の改善]

■ メールマガジン等、毎日決まった時間に合わせて(毎正時)、大量に送信される広告宣伝メールがある。そうした電子メールが重畳することにより、電気通信事業者においては、毎正時の電子メール処理量が他の時間帯に比べて甚大となることがあると指摘されている。

このようなメールについては、ほとんどが毎正時に送信する必要がないと思われ、設備の効率的な利用の観点から、送信者側である広告関係事業者等において、大量に広告宣伝メールを送信する場合には、携帯電話向けに深夜に送信することとならないようにする等受信者への配慮をしつつ、1時間から数時間の範囲内で可能な限り均等に送信するなど送信方法を工夫することが期待される。

[リスト管理の適正化]

■ 広告宣伝メールの送信の際に、送信先のメールアドレスの管理が適正に行われていないことにより、宛先不明率が高くなってしまうことがある。そのような場合、大量のエラーメールが発生することになり、電気通信事業者において、受信者側に到達しないメールの処理に係る設備負荷が生じることとなる。

また、場合によっては、その広告宣伝メールの送信者が迷惑メール送信者と勘違いされるおそれもある。このため、広告宣伝メールの送信者側では、宛先不明としてエラーメールやエラーコード応答が戻ってきた送信先については、速やかにリストから除外するなど、送信先のメールアドレスの管理を適正に行うことが期待される。

提言の方向性

[メール転送時の対応]

■ 多くの電気通信事業者では、利用者が受信した電子メールを自動的に別の電子メールアドレスに転送するサービスを提供している。しかし、転送先のメールアドレスが変更されているにもかかわらず転送設定が変更されず、存在しない転送先にメールが送信され続けている場合も多く見られ、電気通信事業者の設備に不要な負荷を生じさせているとの指摘がある。

このため、転送サービスの利用者においては、転送先のメールアドレスを変更した場合等には、速やかに転送設定を変更することが必要である。

■ また、転送サービスの中には、迷惑メールも含め、すべての電子メールをそのまま転送してしまうものもある。そのようなサービスは、不要な電子メールが転送されることになり設備への不要な負荷を生じさせるものであるだけでなく、転送元のサーバが、迷惑メールを転送し続けることにより、転送先から、迷惑メール送信者と勘違いされるおそれもある。このような事態に対応するため、転送サービスの提供にあたって、例えば、利用者の設定により転送設定時にフィルタ機能を利用可能とするなど迷惑メールを転送しないような仕組みを設けること等が考えられる。

[適切なオプトアウトの実施環境の整備]

■ 利用者が自らオプトインをした広告・宣伝メールについて、オプトアウトがしづらいことなどにより、オプトアウトをせずに、受信側の電気通信事業者のサービスを用いてフィルタリングをされ続けるメールの存在が指摘されている。このようなメールについては、設備への負荷となる一方で、受信者によって閲読されないことから、広告・宣伝の効果がまったくないものと考えられ、関係者による改善のための取組についての検討が望まれる。

■ 簡便なオプトアウト方法の提供については、制度上也求められており、まずは、広告・宣伝をする事業者において、そのような手段の提供が必要である。その上で、信頼できる一定の広告関係事業者等に対して、受信側の電気通信事業者が受信者からの依頼を受けてオプトアウトの意思を伝達する取組を、広告関係事業者等と電気通信事業者の両者が協力して実施のための検討することが考えられる。

6 技術的対策 (a)OP25B(Outbound Port 25 Blocking)

現状

- ・ JEAGによるレコメンデーションの公表等の取組の結果、我が国の主要ISPで導入が進展。
(※中小のISPでは導入していないところもある。)

論点

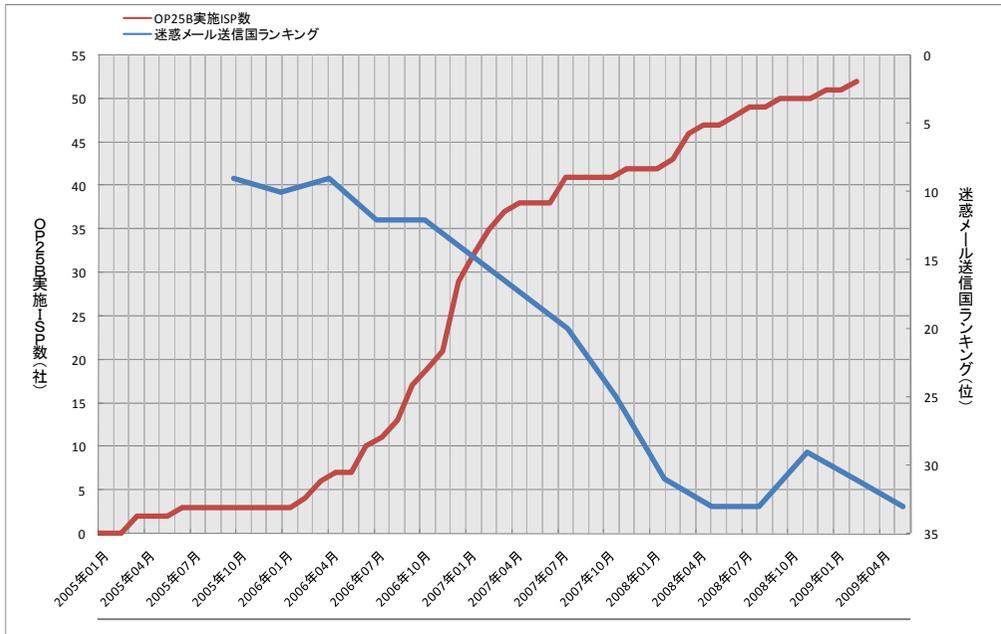
- 国内ISPでのさらなる導入を図るために、どのような取組をすべきか。
- OP25Bを導入していても迷惑メールが送信される場合への対応についてどう考えるか。
(例えば、送信者認証をID・パスワードを用いている場合に、ID・パスワードを破られることにより、迷惑メールが送信される。)

提言の方向性

[OP25Bの更なる普及促進]

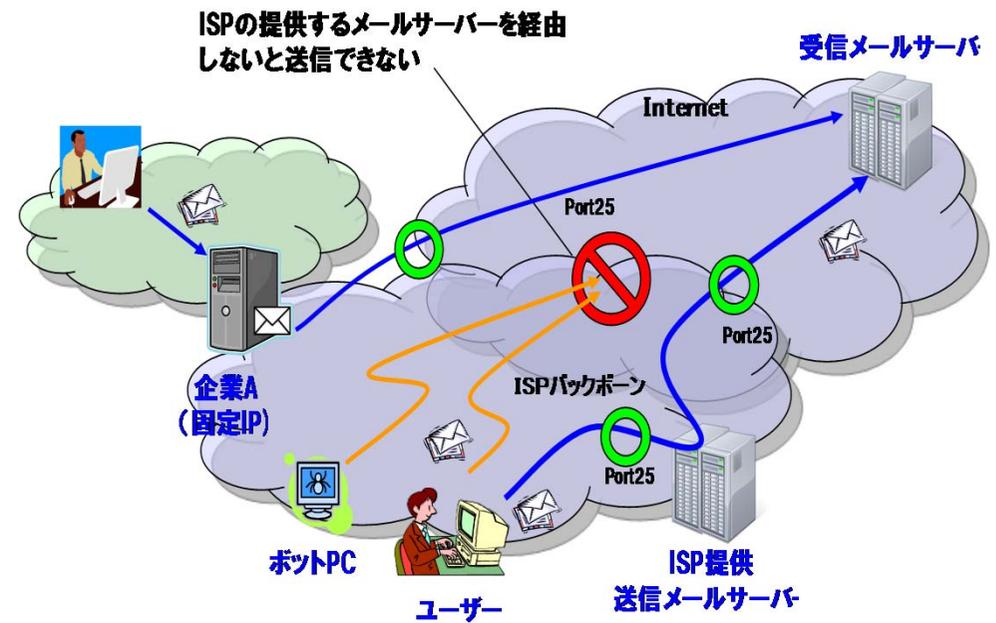
- OP25Bは、我が国の大手電気通信事業者での普及が進み、ボットネットを利用した迷惑メールなど動的IPアドレスによる迷惑メールの削減に大きな効果を上げている。
- しかし、OP25Bは、大手電気通信事業者での導入は進んだものの、中小規模の電気通信事業者ではそれほど導入が進んでいないとの指摘もある。中小規模の電気通信事業者によるOP25Bの導入が進めば、国内発の迷惑メールの送信を更に減少させることができるため、今後、未導入の電気通信事業者においては、OP25Bを導入していくことが求められる。また、その導入を促進していくため、必要に応じて、事業者団体等の関係者による注意喚起等の取組を行うことが望ましい。
- また、OP25Bを既に導入している電気通信事業者でも、全てのサービスについてはOP25Bを実施しておらず、結果として、未対応の部分から迷惑メールが送信されていることがあるとの指摘がある。電気通信事業者では、OP25Bに未対応のサービスがあった場合には、当該部分についてもOP25Bに対応するよう早急に改修することが望ましい。
- これらの点に関連し、現在、(財)日本データ通信協会により、電気通信事業者におけるOP25Bの導入時期に関する状況が公表されているが、関係の事業者団体も協力し、回線別(ブロードバンド、ナローバンド、モバイルデータ通信等)の導入状況など、より詳細な事項についての調査・公表が行われることが望まれる。
- なお、OP25Bを実施していても、利用者のパスワードを推測されたり、利用者側でウィルスに感染しパスワードを盗まれたりすること等により、電気通信事業者のメールサーバへのアクセスの際の認証を破られて、迷惑メールが送信されてしまう問題も起きているとの指摘がある。
- そのようなことにならないよう、電気通信事業者では、認証に一定回数失敗した場合にはアカウントを一時的に停止する仕組みや、安易なパスワードが設定できないようにする仕組みの導入等厳格な送信者認証を実施するための対策を行うことが望まれる。また、利用者は、推測されにくいパスワードの設定やウィルス対策ソフトウェアの利用等を行うことが望まれる。

OP25Bの導入状況と日本のスパム送信国ランキング



出典: (財)日本データ通信協会資料及びソフォス社資料より作成

OP25Bの概要



6 技術的対策 (b)送信ドメイン認証技術

現状

- ・ 送信ドメイン認証技術のうち、SPFの送信側導入率は4割、DKIM送信側の導入率は0.5%程度。

論点

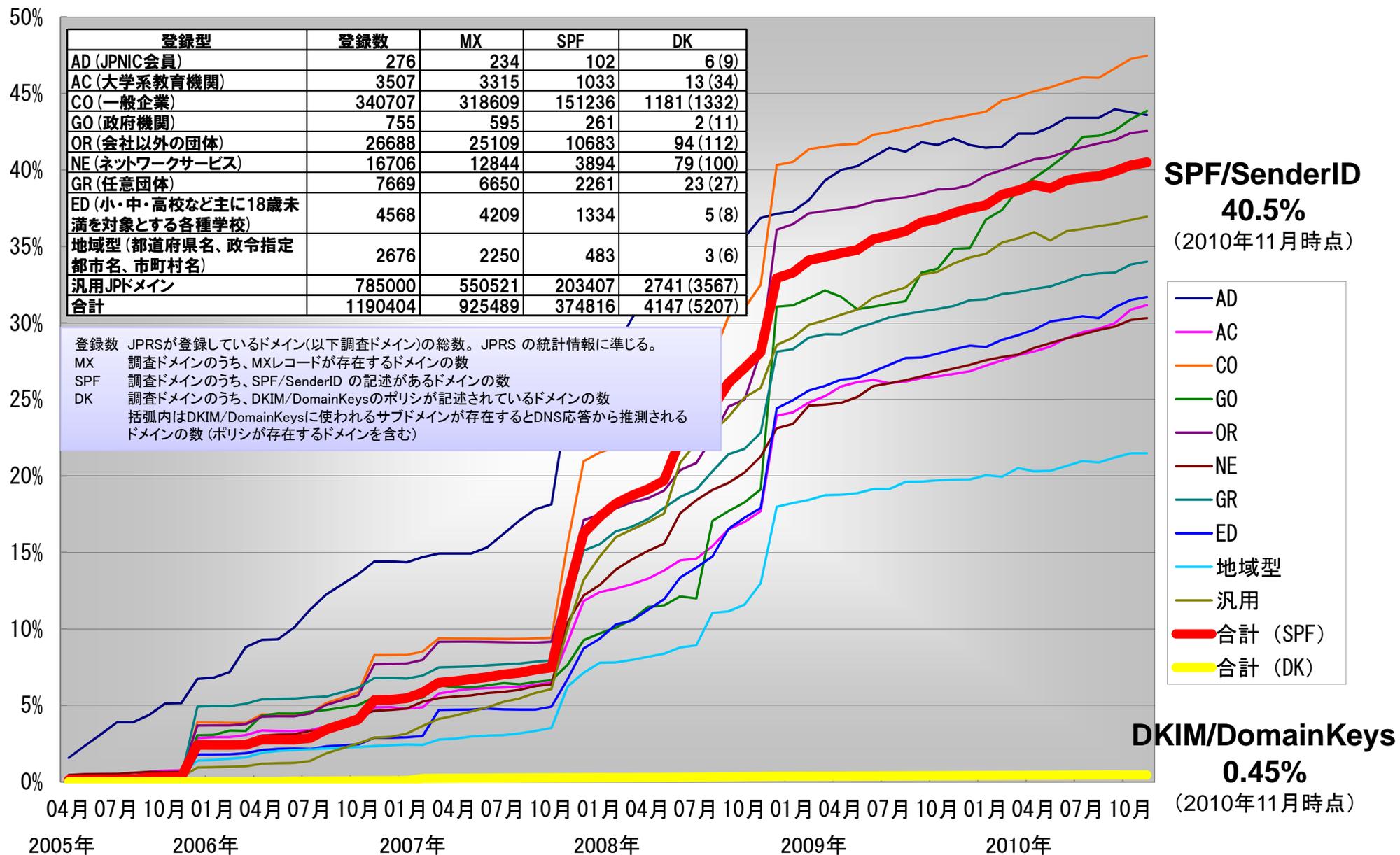
- SPFの送信側導入率を上げるため、ドメイン保有企業に対して、どのような取組をすべきか。
- 国内ISPでのさらなる導入を図るために、どのような取組をすべきか。
- なりすまさずに送られてくる迷惑メールへの対策について、どのように考えるか。

提言の方向性

[送信ドメイン認証技術の普及促進]

- 送信ドメイン認証技術は、多くのドメインが対応することにより効果が増していくものであり、送信側として、できるだけ多くのドメイン保有企業が導入することが望まれるものである。特にドメイン名を詐称されることにより、信頼性に対する悪影響が大きいと考えられる政府、自治体、金融機関、ショッピングモール等が送信する電子メールに関しては、率先的に対応を推進することが求められる。
- また、メール配信事業者は、その設備が、多くのドメインを送信元とするメールの送信に用いられていることから、送信ドメイン認証技術に対応するとともに、そのサービスの利用者に対する積極的な導入の働きかけをすることが期待される。
- さらに、送信ドメイン認証技術は、メールサーバ段階で実装されるものであり、利用者個人のみで対策することはできないものであることから、電気通信事業者には、少なくとも、受信側での認証及び認証結果のメールヘッダへの表示の実施が求められる。
- 送信ドメイン認証技術の導入促進のため、迷惑メール対策推進協議会による「送信ドメイン認証技術導入マニュアル」の作成・公表や周知活動、JEAGによる技術的な検討やレコメンデーションの公表、(財)インターネット協会による解説資料の公表やカンファレンスの実施等の取組が行われてきている。
- 送信ドメイン認証技術の普及にあたっては、実装にあたって整理すべき技術的な課題や利用者への普及のための課題など様々な課題も考えられることから、引き続き、関係者による積極的な取組が期待される。

送信ドメイン認証技術の導入状況



6 技術的対策 (c)その他の技術的対策

現状

- ・ 迷惑メールの技術的対策として、OP25B、送信ドメイン認証技術の他、送信通数制限、フィルタリング等がある。

論点

- OP25B、送信ドメイン認証技術の他、積極的に進めて行くべき技術的な対策として、どのようなものがあるか。

提言の方向性

[その他の技術的対策]

- 迷惑メール受信防止のための技術については、電気通信事業者やセキュリティベンダ等から、フィルタリングサービスやフィルタリングソフトウェアが提供されている。利用者は、フィルタリングサービス等を利用することにより、迷惑メールを受信しないことが可能となるため、電気通信事業者等の関係者により、より利用者が利用しやすい形で提供されることが望ましい。
- また、流通している電子メールの約7割が迷惑メールという状況の中では、電気通信事業者の設備に対する負荷軽減の観点からも、迷惑メールを送信させないための対策が重要であり、引き続き、電気通信事業者等の関係者において、その他の技術的対策の導入を促進していくべきである。

[IPv6対応]

- 現在のインターネットのプロトコルであるIPv4(Internet Protocol version 4)のアドレス枯渇に伴い、今後、その後継プロトコルであるIPv6(Internet Protocol version 6)への移行が行われる。IPv6移行後も基本的にはIPv4での技術的対策は継続して行われることが望まれる。
- この点について、OP25Bや送信ドメイン認証技術などの技術は大きな影響は受けないが、BL(ブラックリスト)などの技術では影響が生じることが指摘されている。IPv4の枯渇が間近に迫ってきている中で、関係者により、IPv6への移行に伴う対応について、速やかに課題等を整理することが望まれる。
また、IPv6に対応した新たな技術的対策の開発・導入も期待される。

迷惑メール送信・受信防止のための主な技術

【迷惑メール送信防止のための主な技術】

技術名	技術の概要
1. 送信数制限	同一アカウントからの送信量を制御する方法
2. 送信トラフィック制御	一定期間内に送信されるメールの通数をIPアドレスで制御する方法
3. 送信者認証(SMTP-AUTH)	送信側のISPで、自社メールサーバからの送信時に、IDとパスワードによる認証を行う方法
4. OP25B (Outbound Port25 Blocking)	ISPのメールサーバを経由しない動的IPアドレス(インターネットに接続される度に割り当てられるIPアドレス)からのメール送信を遮断する方法

【迷惑メール受信防止のための主な技術】

技術名	技術の概要
1. キーワード(ブラックワード)判定	メールのヘッダ及び本文中の特定のキーワードに合致するものを迷惑メールと判定する方法
2. 送信元情報参照による判定	メールの送信元情報を参照し、迷惑メールであるかを判定する方法
ブラックリスト	迷惑メール送信元として知られるIPアドレスをまとめたリストからのメールを、迷惑メールと判定する方法
送信ドメイン認証	自社のメールドメインから正しく発信されたメールであることを示す情報をDNSを利用して表明することにより、メール受信側で送信者情報が詐称されているかどうかを判断する方法
3. 内容参照による判定	主にメールの内容を検査し、流通する迷惑メールから分析した情報に基づいて迷惑メールかどうかを判定する方法
4. 受信トラフィック制御	特定の送信元から一時的に大量受信した場合や、存在しないあて先を多く含むメールを受信した場合等、迷惑メールの送信元である可能性が高い送信元からのメール受信に際し、トラフィック量を制御する方法

携帯3社における簡易設定機能の比較

○:自動的にON ×:自動的にOFF -:簡易設定機能での設定変更なし or 機能の提供なし

	au		docomo			Softbank		
名称	カンタン設定		かんたん設定			かんたん設定		
設定名	「携帯、PHS、PCメールを受信」	「携帯、PHSメールを受信」	「キッズオスメ」	「受信拒否強」	「受信拒否弱」	「きつずオスメ」	「推奨ブロック」	「ケータイ/PHS設定」
指定受信 (ホワイトリスト優先受信)	—	—	-	-	-	○	○	○
なりすまし対策	○	○	○	○	○	○	○	○
ドメイン認証	SPF/SenderID で判定	—	-	-	送信メールのFromアドレスのドメインについてDNSの応答を確認し、実在するドメインか判定し、実在する場合のみ受信。	-	-	-
あて先指定受信	×	×	-	-	-	-	-	-
一括設定(PCメール拒否)	×	○	○	×	×	○	×	○
一括設定(海外からのメール拒否)	—	—	-	-	-	○	×	×
URL付きメール受信拒否	×	×	-	-	-	○	×	×
特定URL付きメール受信拒否	—	—	○	○	○	×	○	○
HTMLメール受信拒否	×	×	-	-	-	-	-	-
大量送信メールの受信制限	—	—	-	-	-	-	-	-
未承諾広告※メールの受信拒否	×	×	-	-	-	○	○	○
迷惑メール コンテンツフィルタ	—	—	-	-	-	○	○	○

用語説明

指定受信・拒否
メールアドレス・ドメイン・電話番号など、任意の受信・拒否リストを設定できる機能。
一括設定
携帯電話、PHSやPCからのメールなど、送信元の種類によって、一括で受信・拒否が設定出来る機能。
ドメイン認証
一般ISPからの送信メールを、ドメイン詐称されていないか確認してくれる、なりすまし対策のパソコン版。迷惑メールは、身元を詐称して送ることが多いので非常に有効です。ただし、詐称される正規のISPのドメインがSPF登録していることが条件です。
なりすまし対策
パソコンから送信しているのに、携帯・PHS会社のメールアドレスになりすましたメールを拒否する機能。ただし、一般ISPのドメインになりすましたメールは見抜けないので、その場合はドメイン認証をすることで対処できます。
あて先指定受信
パソコンから転送設定していて、従来は「なりすまし」と判定され届かなかったメールについて、転送元のメールアドレスを登録することで受信出来るようになる「なりすまし対策」「ドメイン認証」の救済機能。
URL付きメール受信拒否
URL(http://www~~/ など)リンクが含まれるメールを拒否する機能。
特定URL付きメール受信拒否
出会い系・アダルト系・違法行為・グロテスクなど、有害な特定のURLリンクのあるメールを拒否する機能。迷惑メールにはこのようなURLリンクが含まれることが多いので非常に有効です。
HTMLメール受信拒否
HTML形式で送られるメールを拒否する機能。HTMLメールの多い英文スパムに有効です。
大量送信メールの受信制限
1日あたり、1台の携帯電話から大量に送信される迷惑メールを、500通目以降から受信拒否の設定が出来ます。
未承諾広告※メールの受信拒否
件名に「未承諾広告※」と記載のあるメールを拒否する機能。
受信許可リスト拡張版
ネットワークにアドレス帳を補完するサービスを利用し、登録されたメールアドレスを優先的に受信する機能。

7 利用者への周知啓発

現状

- ・ 行政機関、(財)日本データ通信協会、ISP、携帯電話事業者、各種団体等が迷惑メール対策に関し、Web、パンフレットでの周知活動を実施。

論点

- 利用者側での迷惑メール対策が、より適切に行われるよう、利用者への周知を強化するため、どのようなことが考えられるか。

提言の方向性

- 総務省が実施した「平成21年通信利用動向調査」によれば、PC利用者の約5割が迷惑メール対策を行っていないと回答し、また、携帯電話利用者の約3割が迷惑メール対策を行っていないと回答している。

[周知啓発の方法]

- こうしたことから、利用者側での対策を促すため、利用者に対する迷惑メール対策に関する一層の周知啓発を図る必要がある、引き続き、総務省・消費者庁、電気通信事業者等の迷惑メール対策の関係者が行っているパンフレット、HP等での周知啓発を行っていくことが必要である。

特に、(財)日本データ通信協会迷惑メール相談センターが公開している迷惑メール対策HPは、PCや携帯電話別の具体的な迷惑メール対策方法や、技術的対策の解説、子供向け解説ページ等、利用者が行うべき迷惑メール対策についておおよそ理解できる構成となっている。また、(財)インターネット協会が公開している迷惑メール対策のHPでは、電子メールソフトウェアでの迷惑メールフィルタ設定方法を詳細に紹介している。こうしたHPを迷惑メール対策関係者が幅広く利用者向けに周知することにより、利用者のリテラシー向上策の一環とすることが考えられる。

- 一方で、利用者側での迷惑メール対策が進んでいない理由についての分析は十分に行われてきていないことから、総務省等において、詳細な調査・分析を行い、それを活かして適切な周知啓発を図るべきである。

[周知啓発の内容]

- (独)国民生活センターの相談事例からは、迷惑メールを受けて個人情報相手が相手方に伝わっているのではないかと不安になったり、消費者トラブルに巻き込まれるなどの問題が依然として発生していることがうかがえる。これは、利用者側でできる迷惑メール対策の知識が十分に理解されていないことにも一因があると推察される。周知啓発にあたっては、その内容として、迷惑メールを受信しないための対策、迷惑メールを受信してしまった場合の対策及び自ら同意した広告宣伝メールへの対応について、迷惑メール対策関係者が改めて積極的に周知することが必要である。

- 迷惑メールを受け取らないための対策としては、①メールアドレスを安易に公表しない、②不用意に同意しない、③推測されにくいアドレスを使うの三原則が重要である。迷惑メールを受け取ってしまった場合の対策としては、①開かない(怪しい電子メールは開封しない)、②クリックしない(怪しい電子メールに記載されたURLをクリックしない)、③入力しない(安易に個人情報を入力しない)の三原則が重要である。また、自ら同意した広告宣伝メールへの対応としては、①自分で申し込んだメールが不要になったらきちんとオプトアウトする、②メールアドレスを変更したら自分で申し込んだ広告宣伝メールの発行者にきちんと通知する、③ID、パスワードが送信者から付与されている場合は忘れないようにする の三原則が重要である。

[迷惑メール受信者のための相談窓口]

- 迷惑メールに悩む受信者が、迷惑メールに対する適切な対処を行い、無用なトラブルに巻き込まれないようにするためには、有用な助言を与えることのできる相談窓口の役割は重要である。総務省の委託事業として、迷惑メール相談センターにおいて、相談窓口が開設され、年間約5千件の相談を受けており、今後も、その重要性は変わらないことから、引き続き、相談窓口が開設される必要がある。
- また、(独)国民生活センターや各地の消費生活センターといった消費者相談窓口にも、迷惑メール受信者からの相談が寄せられることがあるため、迷惑メール受信者自身が適切な対処を行うことができるよう、関係者間で必要な情報交換等を行っていくことが期待される。

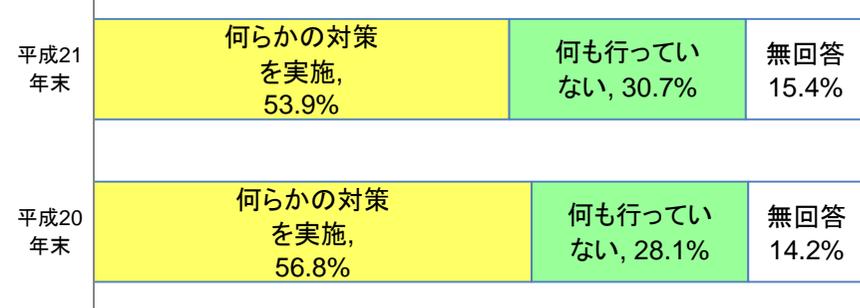
利用者における迷惑メール対策の実施状況

パソコンでの迷惑メール対策を行っていない利用者が約5割、携帯電話での迷惑メール対策を行っていない利用者が約3割となっており、迷惑メール対策があまり実施されていない。

①パソコン

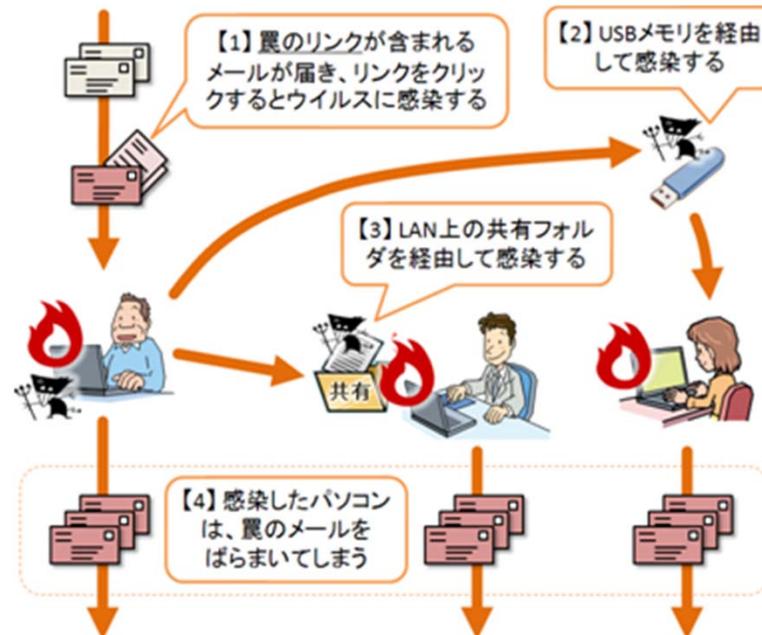


②携帯電話(PHS, PDAを含む)



出典:平成21年通信利用動向調査(総務省)

迷惑メールをはじめとした様々な経路で感染させようとするウィルスの仕組み



迷惑メール対策関係者による主な普及啓発活動

	主な普及啓発活動
総務省・消費者庁	<ul style="list-style-type: none"> ・HPによる特定電子メール法、技術的対策、電気通信事業者における自主的取組の推進等の周知 ・パンフレットによる特定電子メール法の解説
(財)日本データ通信協会 迷惑メール相談センター	<ul style="list-style-type: none"> ・HPによる迷惑メール対策の周知 ・パンフレットによる特定電子メール法の解説、利用者向け迷惑メール対策方法の解説 ・迷惑メールに関する調査研究活動と成果公表 ・電話相談 等
(財)インターネット協会 迷惑メール対策委員会	<ul style="list-style-type: none"> ・HPによる迷惑メール対策の周知 ・迷惑メール対策カンファレンスの開催 ・地方セミナーの開催
各ISP事業者	<ul style="list-style-type: none"> ・HP、パンフレットによる自社の迷惑メール対策サービスの周知 ・子供向け安全教室の開催 ・迷惑メール申告窓口の設置
各携帯電話事業者	<ul style="list-style-type: none"> ・HP、パンフレットによる自社の迷惑メール対策サービスの周知 ・子供向け安全教室の開催 ・迷惑メール申告窓口の設置
消費者団体	<ul style="list-style-type: none"> ・HPによる迷惑メールに関する相談事例等を紹介 ・通報窓口の紹介、消費者相談

8 国際連携の推進

現状

- ・ 多国間連携(ロンドンアクションプラン、ソウル・メルボルンMOU)、二国間連携(カナダ、英国、フランス、ドイツと共同声明等)を実施。
- ・ 中国、香港、台湾、ブラジルと送信元IPアドレスを交換。
- ・ JEAG、(財)インターネット協会において、APCAUSE(アジア太平洋地域の民間の迷惑メール対策団体)と連携し、情報交換等を実施。
- ・ また、JEAGにおいて、MAAWG(国際的な民間の迷惑メール対策団体)と連携し、情報交換等を実施。

論点

- 海外発の迷惑メールが増加してきており、諸外国との連携・協調を一層行っていくべきではないか。
- 諸外国からボットによる電子メール送信が見られることから、ボット対策に有効なOP25B等の海外普及を図るべきではないか。

提言の方向性

[日本の成功事例の紹介]

- 国際連携にあたっては、それぞれの国のベストプラクティスを共有していくことが有益である。我が国は、総合的な対策を実施することにより、自国発の迷惑メールを低い水準に押さえてきていることから、その成功事例について諸外国に紹介し、諸外国における対応を促進していくことが望ましい。
- 具体的には、特定電子メール法の概要やその執行状況など、我が国における制度的な対応をはじめとする迷惑メール対策の概要について、総務省において、簡潔な英語での情報をまとめ、ウェブページで公表していくこと等が期待される。
- また、我が国で大きな効果をあげたOP25Bについて、官民の関係者が協力し、英文による導入のための解説資料等を準備し、それを関係者のウェブページ等で公表するとともに、各種の多国間連携の場や二国間連携の場で、積極的に我が国の成功事例として紹介していくこと等により、その普及を促進していくことが期待される。
- さらに、総務省及び経済産業省が連携して実施してきたサイバークリーンセンター(CCC)によるボットウィルスを撲滅する取組について、約3年半の試行により、諸外国に比べ、非常に低いボット感染率を達成するという効果を上げている。これについては、ドイツが、CCCを参考に、2010年(平成22年)9月から同様の取組を開始しているなど、諸外国でも評価されている。総務省では、CCCの取組を、積極的に諸外国に紹介していくことにより、諸外国において同様の取組の実施を促進していくことが望ましい。

[多国間連携]

- 国際連携について、政府では、「国際的スパム執行協力に関するロンドン行動計画(LAP(London Action Plan))」や「ソウル・メルボルン スパム対策の協力に関する多国間MoU」に参加するなど、執行機関相互の多国間連携の枠組みにより、情報交換等の取組を実施してきた。総務省では、引き続き、これらの国際連携の枠組みを活用し、諸外国の迷惑メール執行機関の間で情報交換を行うとともに、国境を越える迷惑メールについて、重点的な執行を呼びかけていくことが望ましい。
- 政府以外の機関においては、JEAG(Japan Email Anti-Abuse Group)においてMAAWG(Messaging Anti-Abuse Working Group)と連携し、迷惑メール対策に関する情報交換等を行っている。また、JEAG及び(財)インターネット協会では、APCAUCE(Asia Pacific Coalition Against Unsolicited Commercial Email)と連携し、アジア太平洋地域における民間レベルでの国際連携活動を行っている。
こうした活動については、引き続き積極的に関与し、技術的対策の動向の把握や、我が国の成功事例の紹介等を行っていくことが望ましい。
- また、関係団体に所属する者のみが国際的な活動を行うだけでなく、各電気通信事業者等においても、国際的な会合等に参加する場合や、諸外国の電気通信事業者との協力関係がある場合に迷惑メール対策に関する情報交換を行うことや、諸外国の電気通信事業者と共同して迷惑メール対策を推進していくことなどが期待される。

[二国間連携]

- 政府では、迷惑メール対策に関し、フランス、イギリス、カナダ等の執行当局との間で共同声明を締結するなど、二国間連携も進めてきている。今後、既に迷惑メール対策に関する協力文書を締結している外国執行当局との間で、より一層の執行面での協力関係の構築を図るべきである。
- 総務省では、日本への迷惑メール発信の多い外国執行当局との間での連携強化をしていくことが必要である。特に、現在、特定電子メール法第30条に基づく情報交換が進展していないことから、特定電子メール法に相当する法令を執行する外国当局との間で、その取組を積極的に進め、迷惑メール発信国における措置を促進することが重要である。
- また、総務省では、委託業務を通じて、迷惑メールの送信元IPアドレスの交換を中国、ブラジル等と実施している。この取組については、既に交換を実施している国・地域との間での交換した情報の一層の有効活用の促進や、対象国の拡大などにより、さらに強化していくことが必要である。

【多国間連携】

迷惑メール対策に特化した枠組み

○ ロンドンアクションプラン(LAP: London Action Plan)

- ・主要国の迷惑メール対策執行当局が参加し、執行当局間の意思疎通や連携、官民対話の促進などを目的として2004年11月に合意された行動計画であり、以後、同計画に基づき、継続的に活動。総務省から、定期的な電話会議や、物理的会合に参加。
- ・2010年10月に開催された会合に出席し、日本の迷惑メールの取組について説明・意見交換を実施

○ ソウル-メルボルン スпам対策の協力に関する多国間Mou

- ・アジア太平洋地域の迷惑メール対策執行当局が参加し、迷惑メールの削減のための協力を推進するために2005年4月に合意されたMou(覚書)であり、以後、同覚書に基づき、各国の法制や、執行当局の取組について、情報交換を行うとともに、加盟機関間における執行協力に関する議論を行っている。総務省から、定期的な電話会議や、物理的会合に参加。2008年3月には東京で会合を開催。

○ 国際電気通信連合 (ITU: International Telecommunication Union)

- ・電気通信分野に関する国際連合の専門機関。電気通信技術の標準化を扱うITU-Tにおいて、迷惑メール対策について議論。
- ・2009年4月に開催された世界電気通信政策フォーラムの成果文書において、迷惑メール送信者や技術的対策に関する情報交換の推進を合意。

○ 経済協力開発機構(OECD)

- ・2004年2月「スパムに関するワークショップ」を開催し、迷惑メールに対する多面的な方策の枠組みについて検討。
- ・2006年4月に迷惑メール対策の枠組みをまとめた「アンチスパム・ツールキット」を取りまとめ公表。

○ アジア太平洋経済協力(APEC)

- ・電気通信サブグループ等で迷惑メール対策について定期的に意見交換を実施。

○ アジア・太平洋電気通信共同体(APT)

- ・アジア・太平洋地域の電気通信の開発促進、地域電気通信網の整備・拡充を目的とする国際機関。
- ・2009年5月に開催された政策・規制フォーラムにおいて迷惑メール対策について議論。

○ 日ASEAN情報セキュリティ政策会議

- ・アジア地域におけるセキュアなビジネス環境の整備、安心・安全なICT利用環境の構築に向けた地域的対応を目的として、2008年6月に設置が合意された高級事務レベル会合。
- ・2009年2月に開催された第1回会合の成果文書において、迷惑メール等サイバー脅威への対応における連携の強化について合意。
- ・2010年3月にバンコクにて開催された第2回会合で、日・ASEANの協力事項を定めた「連携枠組み」に一致。

国際機関などを通じた取組

【二国間連携】

北米

- 米国
 - ・個別協議のほか、日米情報通信政策協議や日米規制改革イニシアティブにおいて、迷惑メール対策について意見交換。
- カナダ
 - ・2006年10月に迷惑メール対策に関し合意(共同声明)。日加情報通信政策協議等で迷惑メール対策について意見交換。

欧州

- EU
 - ・日EU定期協議(直近は2008年3月に開催)等で迷惑メール対策について意見交換。
- 英国
 - ・2006年9月に迷惑メール対策に関し合意(共同宣言)。日英定期協議等(直近は2008年1月開催)で迷惑メール対策について意見交換。
- フランス
 - ・2006年5月に迷惑メール対策に関し合意(共同声明)。日仏定期協議(直近は2010年11月開催)等で迷惑メール対策について意見交換。
- ドイツ
 - ・2007年7月に迷惑メール対策に関し合意(共同声明)。日独情報通信政策協議(直近は2006年9月開催)等で迷惑メール対策について意見交換。

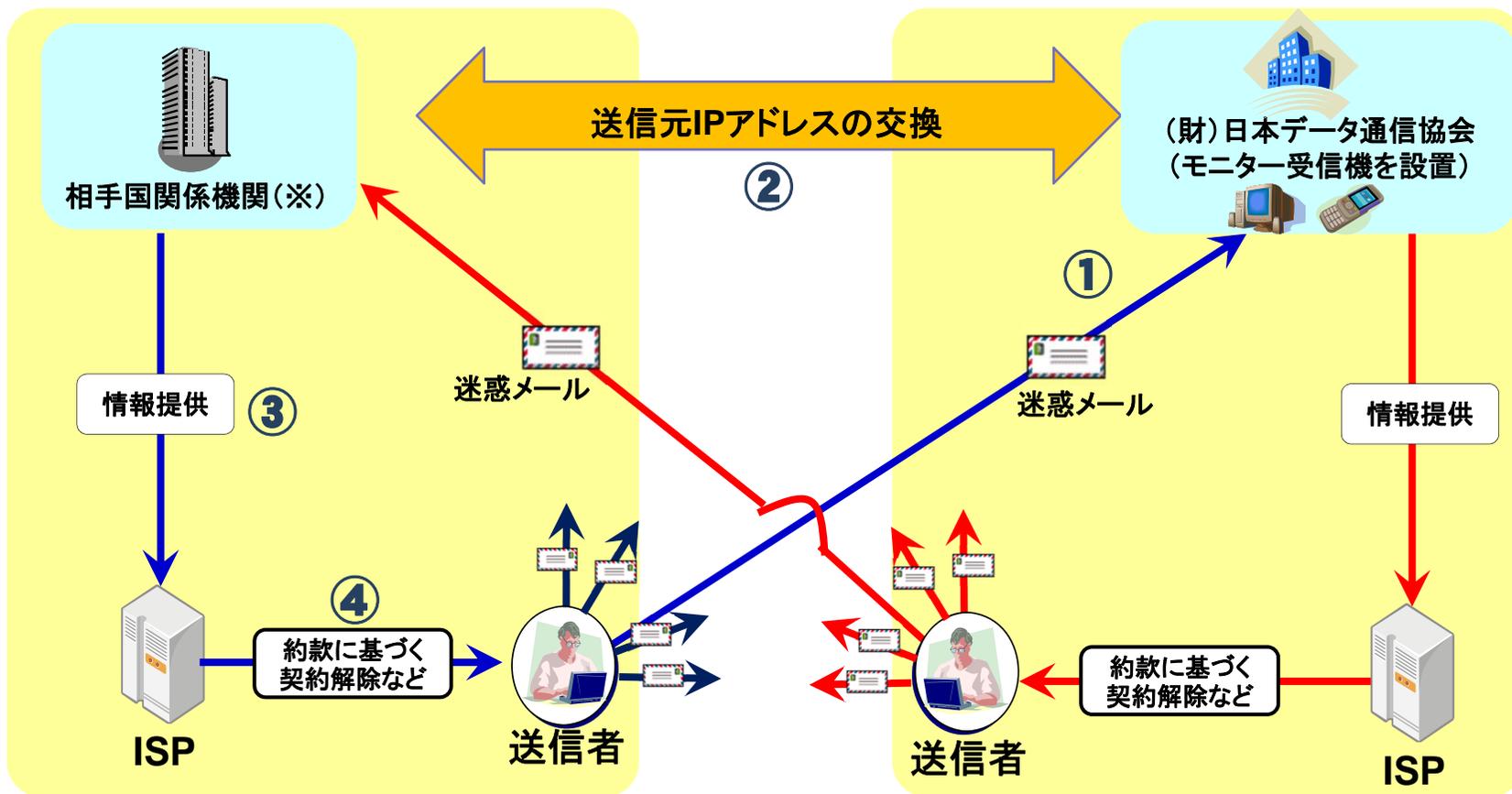
南米

- ブラジル
 - ・2010年5月に第1回ブラジル－ジャパン アンチスパムワークショップを開催し、迷惑メール対策について意見交換。

アジア・オセアニア

- オーストラリア
 - ・日豪情報通信政策協議等で迷惑メール対策について意見交換。
- 中国
 - ・2009年3月に迷惑メール対策に関する意見交換
 - ・2009年5月にICT協力に関する文書を締結。
 - ・2009年8月に日中ICT競争政策・規制制度セミナーでの迷惑メール対策に関する意見交換。
- 韓国
 - ・2009年5月に放送及び電気通信分野における協力に関する日本国総務省と大韓民国放送通信委員会との覚書き締結。
 - ・2010年4月に迷惑メール対策に関する意見交換。

(財)日本データ通信協会において、中国、台湾、香港、ブラジルとの送信元IPアドレスの交換を実施。



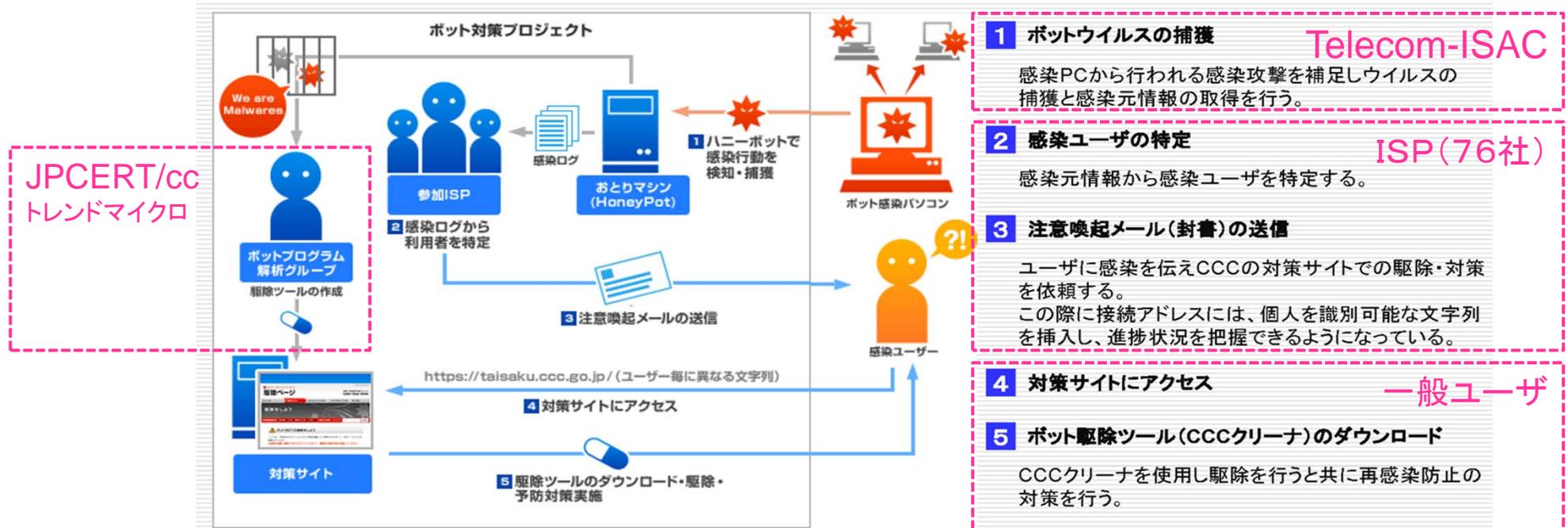
- ① (財)日本データ通信協会のモニター受信機で迷惑メールを受信
- ② 提供された迷惑メールの送信元IPアドレスを分析し、中国発の場合は、送信元IPアドレスを中国インターネット協会 (ISC) に提供
- ③ 送信元のISPにIPアドレスを提供
- ④ 送信元ISPにおいて、送信者との契約解除などの措置

※ 2010年8月現在、中国：中国インターネット協会 (ISC)、台湾：国家通信放送委員会 (NCC)、香港：電気通信管理局 (OFTA)、ブラジル：CERT.brとの間で交換を実施。

ボットウイルス駆除対策プロジェクト①(サイバークリーンセンター(CCC)の概要)

- ◆ 総務省・経産省の連携の下、セキュリティ関係機関のオールジャパン体制として「サイバークリーンセンター(CCC)」を構築し、ボットウイルスを撲滅する取組み
- ◆ 2006～2010年度の5カ年計画
- ◆ ISPのセキュリティ共同組織である「Telecom-ISAC Japan」(会長:伊藤泰彦 KDDI顧問)が中心的な役割を遂行
- ◆ 約3年半の試行により、世界トップクラスの低ボット感染率を実現。国際的にも高い評価

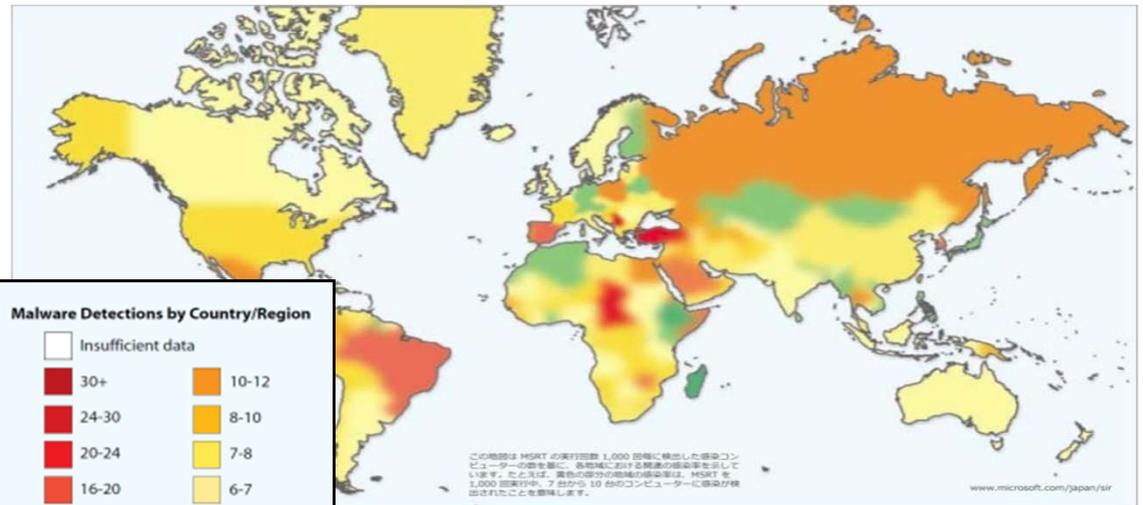
インターネット上のボットウイルス活動を観測し、ボット感染PCを探索。感染ユーザーにボット駆除を勧奨



ウイルス感染者を減らし、世界トップクラスの低ボット感染率を実現

- これまでの取組みにより、ボット感染率は、2005年の約2～2.5% (40～50万ユーザ) から、2008年には約1% (30万ユーザ) に低下
- 在日米国商工会議所 (ACCCJ) も、CCCの取組みにより日本が先進国で最も低いボット感染率を達成しているとの評価 (インターネット・エコノミー白書、2009年10月)

	2007年6月	2010年6月
CCCが収集したボットの数	51 万個	15万個
注意喚起メール	7,697人	3,808人



国別に見たマルウェアの感染率
(マイクロソフトセキュリティインテリジェンスレポート、2009年上期)

【当初3年間の運用実績】

- 新種ボットウイルスの発見: 1日平均25種類
⇒ 駆除ツールを作成、市販のウイルス対策ソフトにも反映
- 注意喚起メール(発見された感染PC): 1日平均438通
⇒ ISP(76社)が、感染者に通知しウイルス駆除を勧奨
- 感染者はCCCのサイトにアクセスし、ウイルス駆除等を実施
CCCサイトへのアクセス: 1日平均 12,722件
駆除ツールのダウンロード: 1日平均 1,110回

※ 収集したウイルスのうち約16%が未知の新種ウイルス(市販のウイルス対策ソフトで検知できないもの)

独でも日本のサイバークリーンセンター(CCC)を参考に同様の取り組みを2010年9月15日から開始。

- 独のスパム送信は世界ワースト4位(2009年BSI調べ。日本はワーストでほぼ最下位)。
- 連邦内務省(BMI)傘下の連邦情報セキュリティ庁(BSI)が、ワースト10位から脱出するため当該プロジェクトを2010年9月開始。

9 総合的対策

現状

- ・ 2008年に、迷惑メール対策の関係者間の緊密な連絡を確保し、最新の情報共有、対応方策の検討、対外的な情報提供などを行うため、迷惑メール対策推進協議会が設立された。

論点

- 迷惑メール対策推進協議会の取組みとして、さらに、どのようなものが期待されるか。

提言の方向性

[今後の総合的な迷惑メール対策]

■ 迷惑メール対策については、以上のような対策を、引き続き、総合的に実施していくことが必要である。すなわち、①政府による効果的な法執行、②電気通信事業者による自主的な取組、③広告関係事業者等による自主的な取組、④技術的対策、⑤利用者への周知啓発、⑥国際連携の推進のそれぞれの取組を有機的に連携させつつ進めていくことが望ましい。

また、可能な限り一時的な大量送信や不要な広告宣伝メールの送信等を減少させ、電気通信事業者の設備への過度の負荷を無くすことにより、適正な電子メール利用環境を実現することが望ましい。このため、「適正な電子メール環境の整備に向けた取組」も総合的な迷惑メール対策として進めていくべきである。

[迷惑メール対策推進協議会]

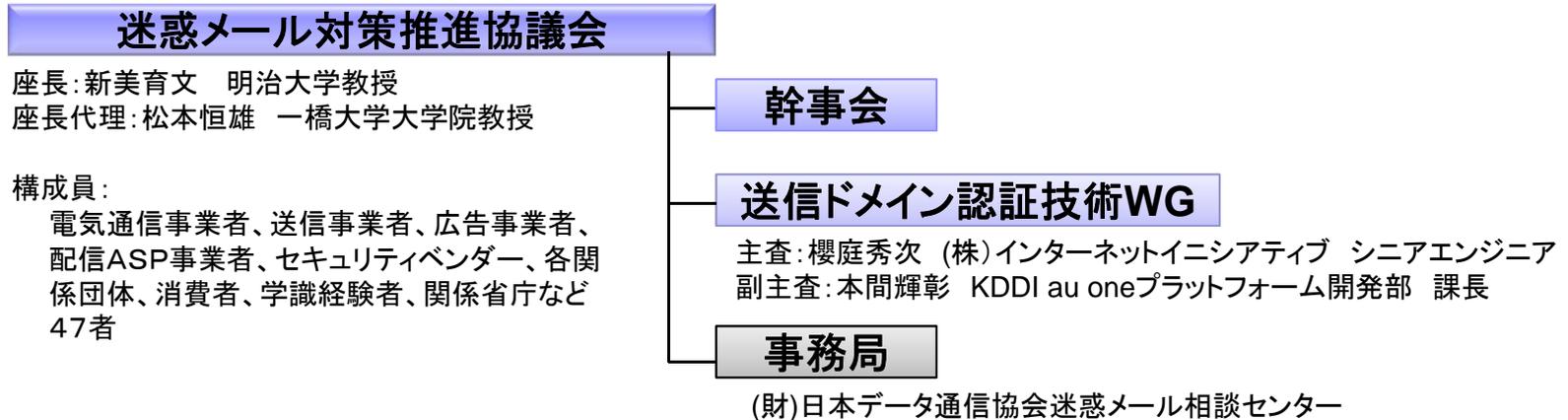
■ 電気通信事業者、広告関係事業者、消費者団体、学識経験者、関係省庁等の迷惑メール対策に関する幅広い関係者が集まり、緊密な連絡を確保し、最新の情報共有、対応方策の検討、対外的な情報提供を行うことを目的として、2008年(平成20年)に、「迷惑メール対策推進協議会」が設立された。

同協議会では、これまで、「迷惑メール追放宣言」の採択(2008年(平成20年)11月)、「迷惑メール対策ハンドブック」の作成・公表(2009年(平成21年)10月・2010年(平成22年)7月)、「送信ドメイン認証技術導入マニュアル」及び「なりすましメール撲滅プログラム」の作成・公表(2010年(平成22年)7月)などの取組を行ってきた。

■ 関係者による取組を有機的に連携させ、迷惑メールに対する総合的に対策を行っていくにあたり、幅広い関係者が集まった迷惑メール対策推進協議会の役割は、今後とも重要であり、一層の活動の充実が期待される。

- ◆ 迷惑メール撲滅を目指す産官学関係者の集まり
- ◆ 2008年11月27日設立
- ◆ 緊密な連絡を確保し、最新情報共有、対応方策検討、対外的情報提供を実施

■ 体制



■ 活動経緯

