

迷惑メールへの対応の在り方に関する 研究会

最終報告書（案）

平成 17 年 7 月

迷惑メールへの対応の
在り方に関する研究会

目 次

1 . はじめに	1
2 . 迷惑メール対策の現状	2
(1) 迷惑メールとは	2
(2) 我が国における迷惑メールの実態とこれまでの対策	6
(3) 諸外国における迷惑メールの実態と対策	13
3 . 迷惑メール対策の方向性	20
(0) 総合的な対策の必要性	20
(1) 政府による効果的な法執行	21
(2) 電気通信事業者による自主規制	30
(3) 技術的解決策	35
(4) 利用者支援	39
(5) 国際協調	42
4 . 最後に	44

1. はじめに

我が国におけるインターネットの利用人口は増加を続けている。平成 16 年末におけるインターネット利用人口は 7,948 万人¹、世帯普及率では 86.8%と²、インターネットは生活に欠かせない存在となっており、そのほとんど全ての利用者が電子メールをコミュニケーション手段として利用している。

また、我が国の携帯電話端末については、その多くがインターネットに対応³しており、電子メールはいつでもどこでも誰でもが簡単に利用できるコミュニケーション手段として、深く生活に関わっている。

他方で、受信者の同意を得ず一方的に送信される広告宣伝メール（いわゆる迷惑メール）については、受信者の平穏な生活を害するものとして、以前よりその対策が求められてきたところであり、我が国においても、平成 14 年 7 月に「特定電子メールの送信の適正化等に関する法律」（平成 14 年法律第 26 号。以下「特定電子メール法」という。）が施行されたところである。

しかしながら、近年における送信手法の巧妙化・悪質化により、法律に基づく取締りや電気通信事業者における自主的取組だけでは、迷惑メール問題の解決が難しくなっている。

このような状況を踏まえ、「迷惑メールへの対応の在り方に関する研究会」を平成 16 年 10 月 7 日より開催し、迷惑メール流通の抑制・防止のために必要な対応方策について幅広く検討してきた。

本資料は、研究会における検討結果を報告書として取りまとめたものである。

¹ 平成 17 年版情報通信白書より。

² 平成 16 年「通信利用動向調査」より。

³ 我が国の携帯電話契約数に占める携帯電話インターネットの契約数の割合は、平成 16 年 9 月末現在で、94.1%であり、世界一となっている。（平成 17 年版情報通信白書より。）

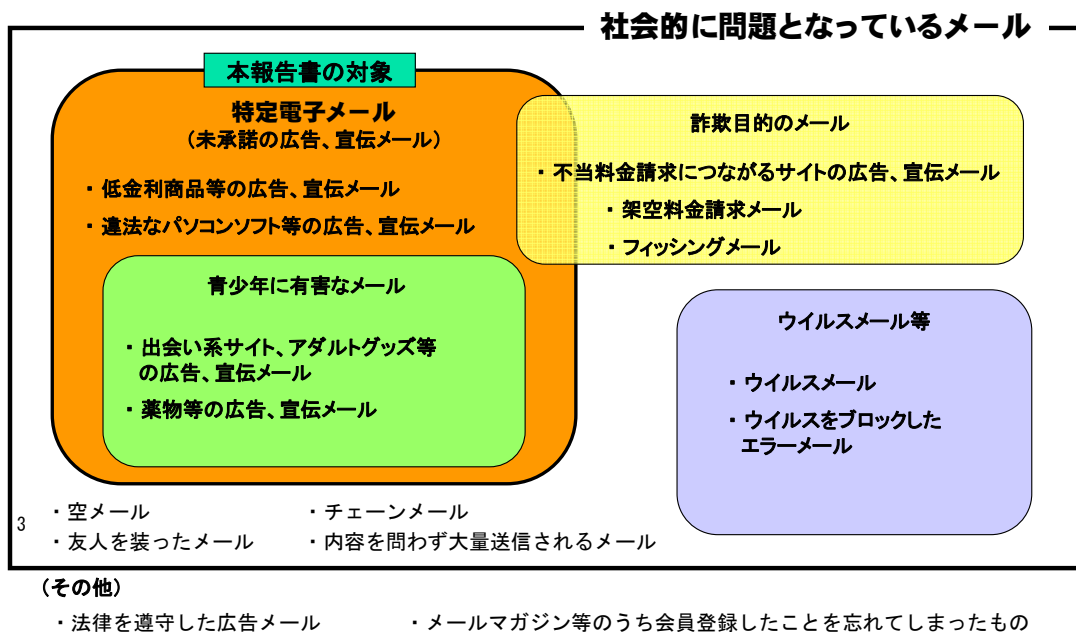
2. 迷惑メールの現状

(1) 迷惑メールとは

① 迷惑メールとは何か

「迷惑メール」という言葉については、人によって意味の相違があり、出会い系サイト等を広告宣伝するメールのほか、架空請求を目的とした電子メール、ウイルスメール、フィッシング¹目的の電子メールなど、社会的に問題となっているメールを含む場合もある。

なお、諸外国では「スパム」(spam)²という言葉が広く用いられている。



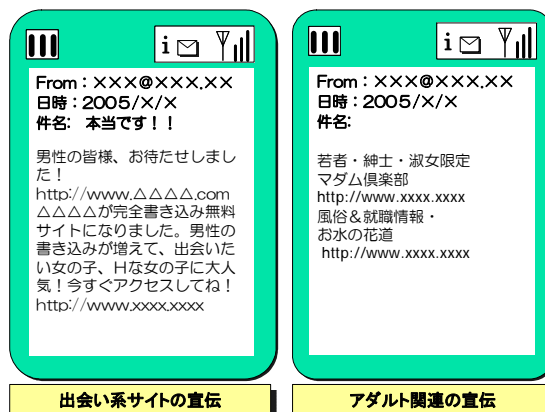
本研究では、これらのメールのうち、特に一方的に送信される広告宣伝メールを「迷惑メール」として議論を行ってきたところであり、本報告書においても、基本的に広告宣伝メールへの対策を扱うこととする（特定電子メール法においても、規制の対象は広告宣伝メールとされている。）。

¹ 金融機関等を装った電子メールによって、偽のウェブサイトを利用者を誘導し、個人情報などを不正に入手する詐欺的な行為。平成16年秋頃から我が国でも事例が確認されるようになってきた。

² 特に英語圏において広く使われている。このほか、「Unsolicited Commercial Email」(UCE。望まれない商業電子メール)という言葉も用いられている。我が国において用いられることのある「spamメール」という言葉は、「spam」や「スパム」とほぼ同じ意味であると考えられる。

³ 空メールや友人を装ったメール、その他エラーによる返信や間違いを装ったメールは、広告宣伝メールではないため基本的に本研究の検討及び特定電子メール法の規制対象外であるが、架空アドレスにあててこれらのメールを送信する行為については、法改正により規制の対象に含まれることとなった(p24参照)。

一方的に送信される広告宣伝メールは、単に不快であるばかりでなく、架空請求や児童買春の契機になっていること、携帯電話等で受け取った場合は受信を望んでいないにもかかわらず課金されてしまうこと、電気通信事業者の設備に障害を与えたり、事業に支障をきたしたりすることなどにより大きな問題となっている。



② 広告宣伝メール以外の社会的に問題になっているメールについて

広告宣伝メール以外の社会的に問題になっているメールについては、以下のようにそれぞれ対策が講じられているところである。

1. 架空請求メール

一方的に広告宣伝メール等を送信し、受信者を出会い系サイト等に誘引し、サイトを訪問した者に対し契約が成立したと称して根拠のない請求（架空請求）をメールで行うものがある。

架空請求により財物を交付させる行為そのものは現在の刑法において詐欺罪等を構成するため、捜査機関による摘発等の対策が講じられている。

なお、架空請求そのものを内容とするメールは広告宣伝メールではなく、特定電子メール法の規律の対象ともならないが、これに先だってサイトに誘引するための広告宣伝メールを一方的に送信する行為については、特定電子メール法による取締りの対象となっている。

2. フィッシングメール

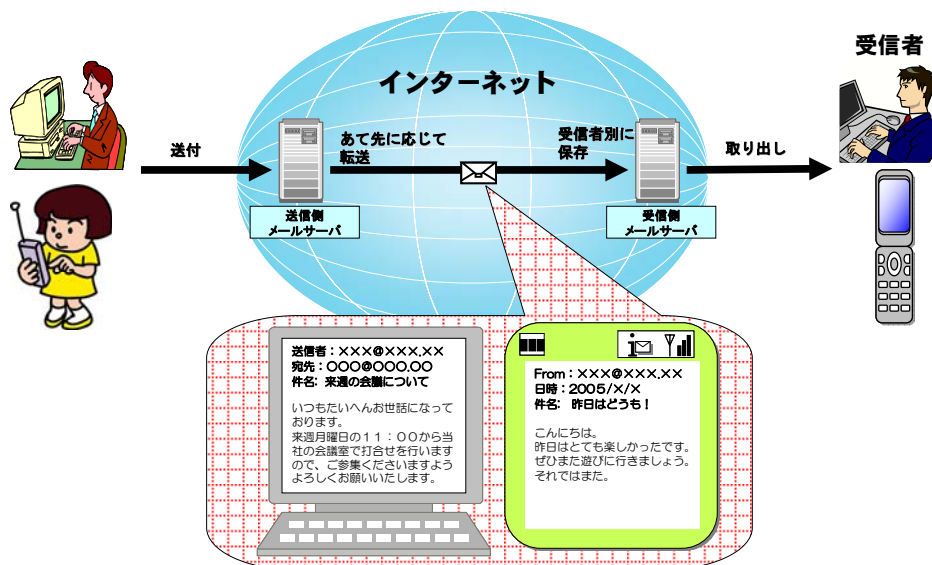
フィッシング詐欺のために送信されるメールについては、総務省において平成 17 年 1 月からインターネット・サービス・プロバイダ（ISP）等を構成員とした「フィッシング対策推進連絡会」を開催し、情報共有を図るとともに、効果的な対策に関する検討を進めているところである。政府全体としても、平成 17 年 2 月に取組を開始したところであり、各省庁においてそれぞれ所管の観点から対策の検討等が進められている一方で、内閣官房が主催する「インターネット上における違法・有害情報等に関する関係省庁連絡会議」（IT 安心会議）において全体の調整が行われている。

3. ウイルスメール

コンピュータウイルスについては、現在国会において審議中の「犯罪の国際化及び組織化並びに情報処理の高度化に対処するための刑法等の一部を改正する法律案」の中に刑法を改正し不正指令電磁的記録作成等の罪を新設する条項が含まれており、この法律案が成立した場合にはウイルスの作成・供用等が直接刑事罰の対象とされることになる。

③電子メールの仕組みについて

電子メールは、その名のとおり郵便のサービスを電子化したものであり、広義には電気通信を用いてメッセージを送受信するさまざまなサービスが含まれ得るが、現在最も一般的なのは、インターネット上のメールサービス（インターネットメール）である。携帯電話で利用される電子メールについても、インターネット接続サービスを利用して、他社の携帯電話やPC等にあてて送信することもできるなど、インターネットメールと同様に利用することが可能となっている⁴。



通常の送受信手順

- 1: 送信者がPCや携帯電話を用いて、ISPのメールサーバ⁵に接続し電子メールを送付する。
- 2: メールサーバがあて先ISPのメールサーバに対し電子メールを転送する。
- 3: あて先ISPのメールサーバは、受け取った電子メールをその設備上にある受信者のメールボックス(郵便箱に相当)に保存する。
- 4: 受信者がメールボックスから電子メールを取り出す(受信完了)。

⁴ 携帯電話では、このほかにショートメッセージサービス(SMS)が利用できるが、これは原則として携帯電話同士で送受信するものであり、インターネットメールとは技術方式等が異なる別のサービスとなっている。

⁵ 電子メールを受け取り、あて先に応じて配送するコンピュータ。

前ページのような仕組みで電子メールサービスが提供されているため、従来の郵便や電話といった通信手段と比べると、①送信コストが非常に小さいこと、②送信に要する作業が自動化でき連続した大量送信が可能であること、③自ら送信設備を設置して自由に送信できることといった特殊性があり、一方的に広告宣伝の内容等を送りつけようとする者にとって非常に有利な通信手段であるということができる。

【電子メールと郵便の違い】

電子メールと郵便は、機能の面で多くが似通っているが、異なる点としては以下のようなものが挙げられる。これらは、いずれも利用者に大きな利便をもたらす要素であり、電子メールの普及を後押しする力となってきたところであるが、近年はこれらの利便性を逆手にとった迷惑メール送信が問題となっていると考えられる。

- ・一通あたりの送信料金が非常に低廉であること。
- ・コンピュータを用いて送信するため、自動的な送信が可能であること。
- ・ブロードバンド接続環境が整っているため、短い時間で大量の送信が可能であること。
- ・郵便では郵便局が集配を行い、利用者は郵便物を差し出すだけであるが、電子メールでは自らメールサーバを設置して直接受信者に向けて送信することが可能であるなど、様々な送信形態をとりうること。

【電子メールと電話の違い】

電子メールは主に文字をやり取りするのに対し、電話は通話の手段として利用されており、リアルタイムでのコミュニケーションの実現を前提としているため、以下のような違いがある。

- ・電話では要件を伝えるために音声を送る必要があるため、送信するデータ量が大きくなるが、電子メールでは文字データのみで足りる。
- ・電話では相手が不在の場合は本来の目的である通話をすることができないが、電子メールでは不在でも通信文を届けることができる。
- ・電話では電話会社に通話を中継してもらう必要があるが、電子メールでは自らメールサーバを設置して直接受信者に向けて送信することが可能である。

(2) 我が国における迷惑メールの実態とこれまでの対策

迷惑メール問題の発生時から現在に至るまでの経緯

我が国においては、平成13年春頃から、主に携帯電話あての出会い系サイトの宣伝を中心とした迷惑メールが増加し、携帯電話事業者に多くの苦情相談が寄せられるようになったほか、出会い系サイトに起因した犯罪も多発するなど社会的に大きな問題となっていた。携帯電話事業者をはじめとする電気通信事業者では、メールアドレス変更機能の提供や契約約款の変更など様々な対策を講じたが、迷惑メール問題の抜本的な解決には至らなかった。

このため、平成13年11月より、総務省において、本研究会と同名の「迷惑メールへの対応の在り方に関する研究会」(座長：堀部 政男 中央大学法学部教授)が開催された。この研究会では、当時の迷惑メールの現状を把握するとともに、迷惑メールの流通を抑制・防止するために必要な方策の検討を実施し、平成14年1月に、迷惑メールの送信自体を規律するための法制的な対応が効果的との提言が行われた。

その後、迷惑メール対策のための法制度を整備するため、平成14年4月に、特定電子メール法が議員立法により成立し、同年7月1日より施行された¹。

特定電子メール法(制定時)の概要

表示義務

特定電子メール(広告メール)の送信にあたり、送信者に次の事項の表示を義務づけ(第3条)
特定電子メールである旨(「未承諾広告」)
送信者の氏名又は名称、住所
送信に用いた電子メールアドレス
受信拒否の通知を受けるための電子メールアドレス 等

オプトアウト²

受信拒否の通知をした者に対する特定電子メールの再送信を禁止(第4条)

その他

- ・自動生成プログラムを用いて作成した架空電子メールアドレスに宛てて、電子メールを送信することを禁止(第5条)
- ・電気通信事業者は、一時に多数の架空電子メールアドレスに宛てた電子メールが送信された場合には、その電気通信役務の提供を拒むことができる(第10条)

罰則

- ・送信者が第3～5条に違反した場合、総務大臣による措置(是正)命令(第6条)
- ・措置命令に従わないときは、50万円以下の罰金(第18条)

¹ また、同国会において、特定の商品の販売業者等に対し同様の義務を課すことを内容とする「特定商取引に関する法律」の一部改正も行われている。

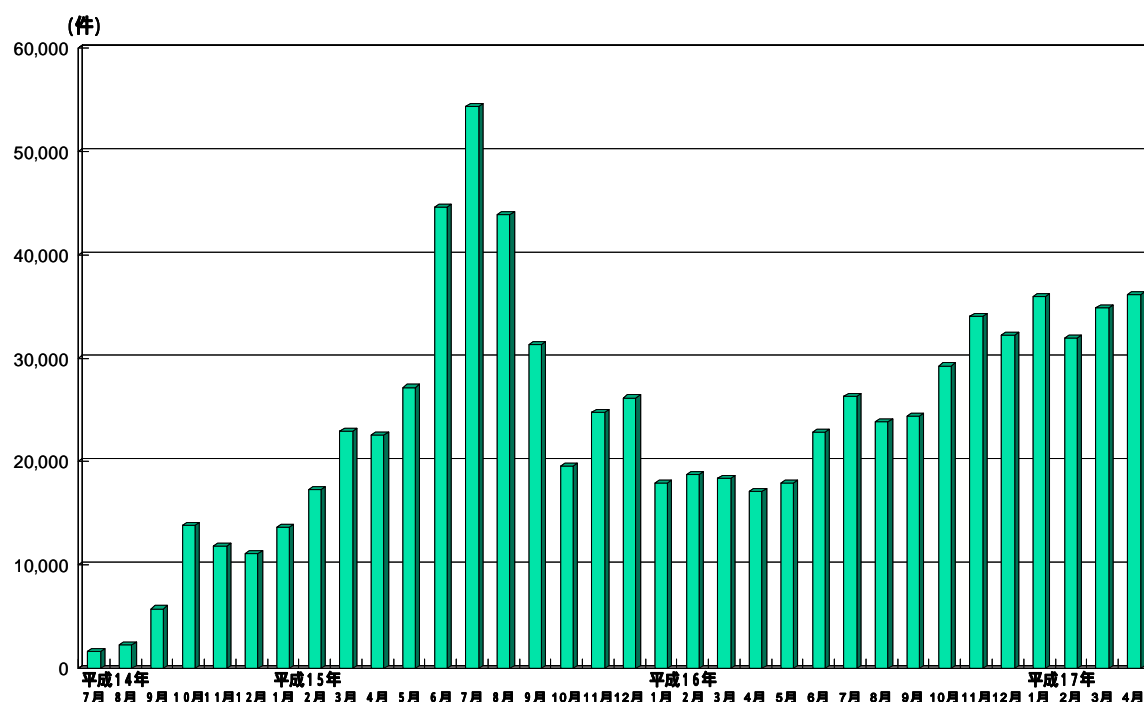
² オプトアウト方式とは、メールの送信者に受信拒否の意思を伝えた場合、以後の送信を認めない方式であり、承諾を得ず送信している広告宣伝メールにそれが広告宣伝メールである旨や受信拒否の連絡方法等の表示義務を課しており、これを満たさない場合は違法となる。これに対し、あらかじめメールの受信を承諾している者に対してのみ送信を認める方式をオプトイン方式という。

特定電子メール法では、受信者からの同意を得ずに広告宣伝メールを送信する場合に「未承諾広告」等の表示義務を課すとともに、受信拒否の通知をした者に対する広告宣伝メールの再送信を禁止しているほか、架空電子メールアドレスに対する広告宣伝メールの送信についても禁止しており、これらの規定に対する違反者には、総務大臣が措置命令を発出できることとしている。

また、同法に基づき、総務大臣に対する申出をしようとする者に対する指導・助言や申出に係る事実関係調査等の業務を行う指定法人として、(財)日本データ通信協会が指定され、同協会内に設置された「迷惑メール相談センター³」において迷惑メール受信者からの申告や相談の受付が開始された。

法施行後、携帯電話事業者等に寄せられる迷惑メールに関する苦情等が相当数減少するなど、一定の効果があったものと考えられるが、表示義務を守らない等の違法な広告宣伝メールに関して、迷惑メール相談センターには、未だに月3万件を超える申告が寄せられている。

迷惑メール相談センターに寄せられた違法メールに関する申告件数の推移

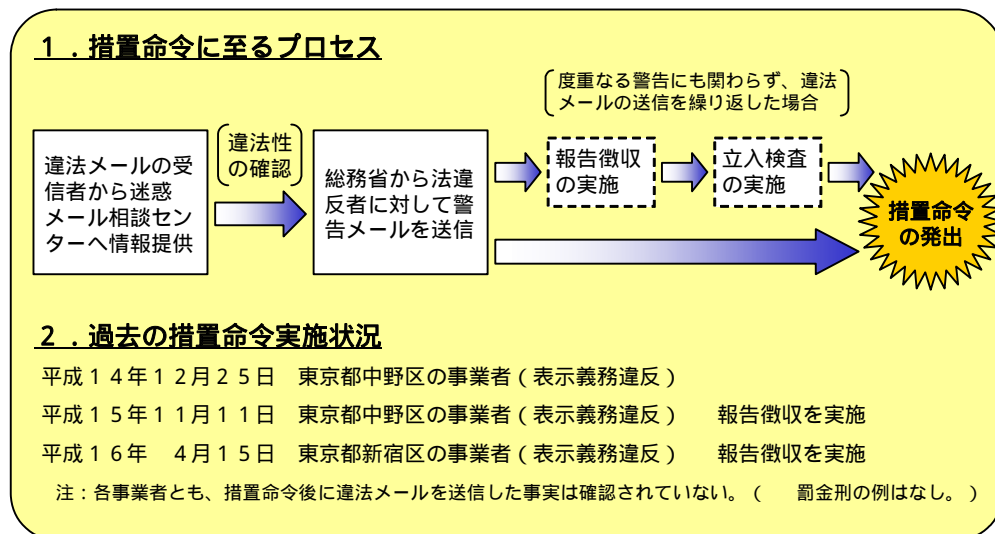


³ <http://www.dekyo.or.jp/>。違法メールに関する申告についても、このサイトからフォームに入力することで可能となっている。

政府によるこれまでの取組

総務省においては、受信者からの申告に基づく警告メールの送信や措置命令の発出など違法送信者に対する特定電子メール法の適切な執行に努めてきたほか、「携帯電話に着信する迷惑メールに対する自衛策」や「迷惑メール送信業者への名義貸し」等について報道発表⁴を行うなど受信者に対する周知啓発も継続的に行ってきた。

特定電子メール法に基づく「措置命令」について



また、「迷惑メール対策推進連絡会」⁵を開催し、携帯電話事業者相互間における迷惑メール対策に関する情報の共有を促進したほか、電気通信事業者が講じる新たな迷惑メール対策について電気通信事業法との関係を整理するなど電気通信事業者における自主規制の促進も行っている。

このほか、OECD（経済協力開発機構）やITU（国際電気通信連合）等の国際機関における迷惑メール対策に関する会議に積極的に参加し、我が国の特徴であるモバイルスパムの状況及びその対策等について説明するとともに、具体的な国際連携策を模索してきている。

⁴ 平成16年1月19日発表「携帯電話等に着信する迷惑メールに対する自衛策について」
http://www.soumu.go.jp/s-news/2004/040119_3.html

平成15年10月7日発表「迷惑メール送信業者への『名義貸し』について」
http://www.soumu.go.jp/s-news/2003/031007_3.html

⁵ 迷惑メール対策の一層の改善に向け、携帯電話・PHS事業者、総務省等関係機関による実質的な意見交換、官民合同施策の検討などを行うため、平成15年11月から開催。

民間によるこれまでの取組

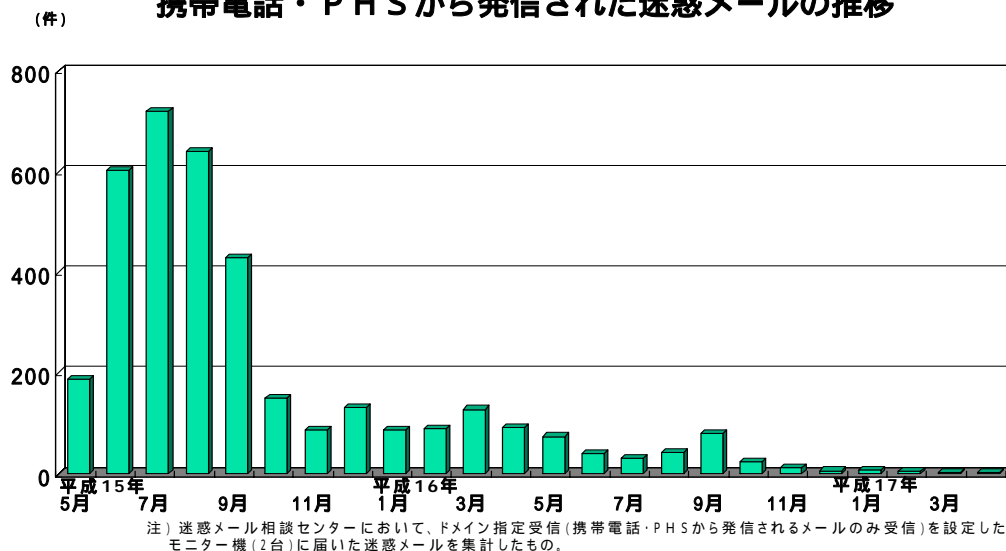
電気通信事業者においても、迷惑メールの受信を回避するために様々なサービスを提供しているところであり、たとえば、受信側における対策として、長いメールアドレスへの変更、特定のドメイン⁶からのメールのみを受信するドメイン指定受信機能の提供、受信者の実際の受信メールの内容に応じて最適なメールの振り分けなどを行う学習型フィルタリングサービスの提供などを行っている。

また、迷惑メールの送信者への対策としては、大量送信者に対するメール送信通数制限措置や利用停止措置（携帯電話事業者において平成17年6月までに、合計65,000回線以上を停止）を行っており、特に携帯電話発の迷惑メール送信に対しては、一定の効果が上がっているところである。

携帯電話発メールの送信通数制限措置

事業者	概要
NTTドコモ	・送信可能通数を1回線1日当たり1,000通未満に制限(平成15年10月20日～) ・送信可能通数を原則として1回線1日当たり200通未満に制限(平成16年1月8日～)
KDDI(au)	・1日1,000通を超えて送信する者(回線)を利用停止に(平成15年9月18日～) ・送信可能通数を1回線1日当たり1,000通未満に制限(平成16年8月23日～)
ボーダフォン	一定の時間内(最大3時間)における送信可能通数を1回線120通未満に制限(上限を超えて送信した場合は、その時点から21時間メール送信不能に)(平成15年12月22日～)

携帯電話・PHSから発信された迷惑メールの推移



⁶ インターネット上で機器を識別するためのアドレス(住所)を表す文字列。例えば、メールアドレスであれば「sample@soumu.go.jp」のうちの@以降の「soumu.go.jp」を、ウェブサイトのアドレスであれば「http://www.soumu.go.jp/」のうちの「www.soumu.go.jp」を指す。

民間団体における会合も数多く開催されており、平成17年3月には、国内の主なISPや携帯電話事業者、ソフトウェア・ハードウェアメーカーなど約30社によってJ E A G (Japan E-mail Anti-Abuse Group) が設立され、技術的な見地から迷惑メール対策の検討を重ねているほか、(社)日本インターネットプロバイダー協会の「行政法律部会」や(財)インターネット協会の「迷惑メール対策委員会」など、迷惑メール対策に関する法的課題や周知啓発策の検討を行うための会合が開催されている。

最近の迷惑メールの特徴

最近の迷惑メールの特徴としては、以前に比べパソコン着の比率が増加傾向にある⁷ことが挙げられ、一部の受信者には極めて大量の迷惑メールが届いている状況にある⁸。

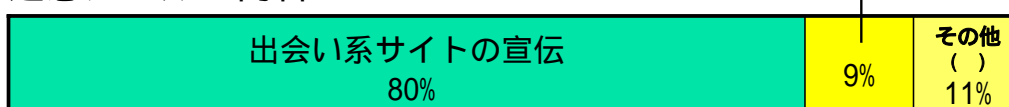
迷惑メールの内容については、出会い系サイトの宣伝がその大部分を占めている点で変化はなく、その他には、アダルト商品や薬品、パソコンソフトの宣伝などがある。

日本における迷惑メールの状況 (特徴)

媒体 (端末)



迷惑メールの内容



薬物、ソフトウェア等

平成16年度上半期に迷惑メール相談センターに寄せられた違反情報提供を分析したもの(サンプル調査)。

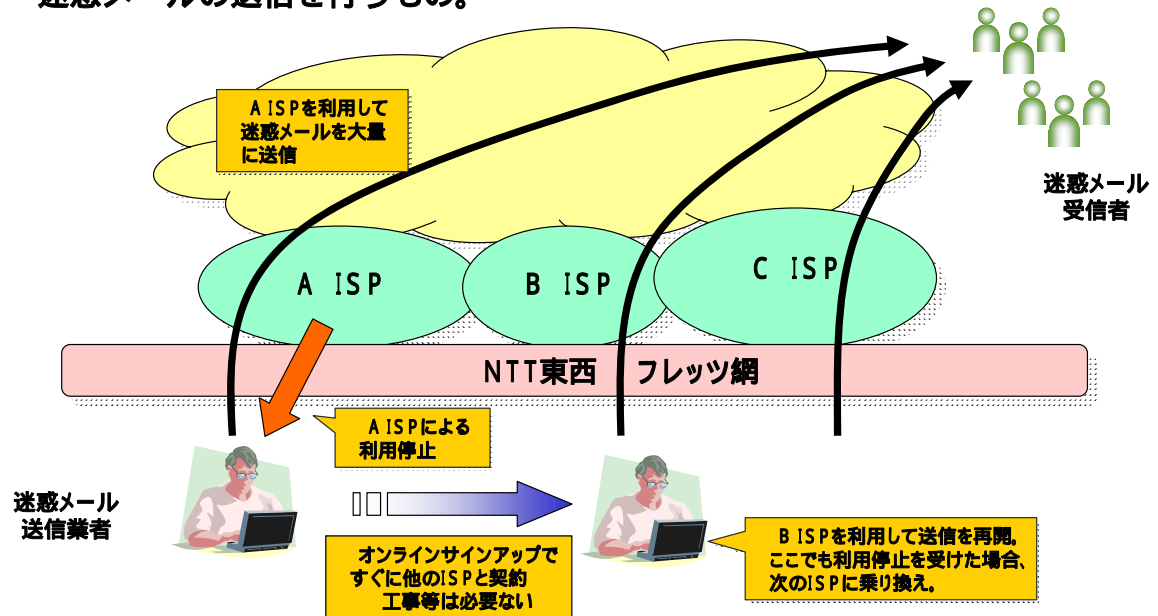
また、迷惑メールの送信手法については巧妙化・悪質化が進んでおり、次ページ以降で紹介するような手法を用いることにより、受信者に対して送信者を特定させないようにして一方的に送信を続けるという行為が行われていると考えられている。

⁷ 平成15年12月に実施したサンプル調査では、携帯着が約90%、PC着が約10%であった。

⁸ 発信側については、平成15年夏をピークに携帯電話発のメールが増加していたが、携帯電話事業者が利用停止等の自主規制を強化したため、最近では携帯電話発の迷惑メールはかなり少なくなっている。(p9のグラフ参照)

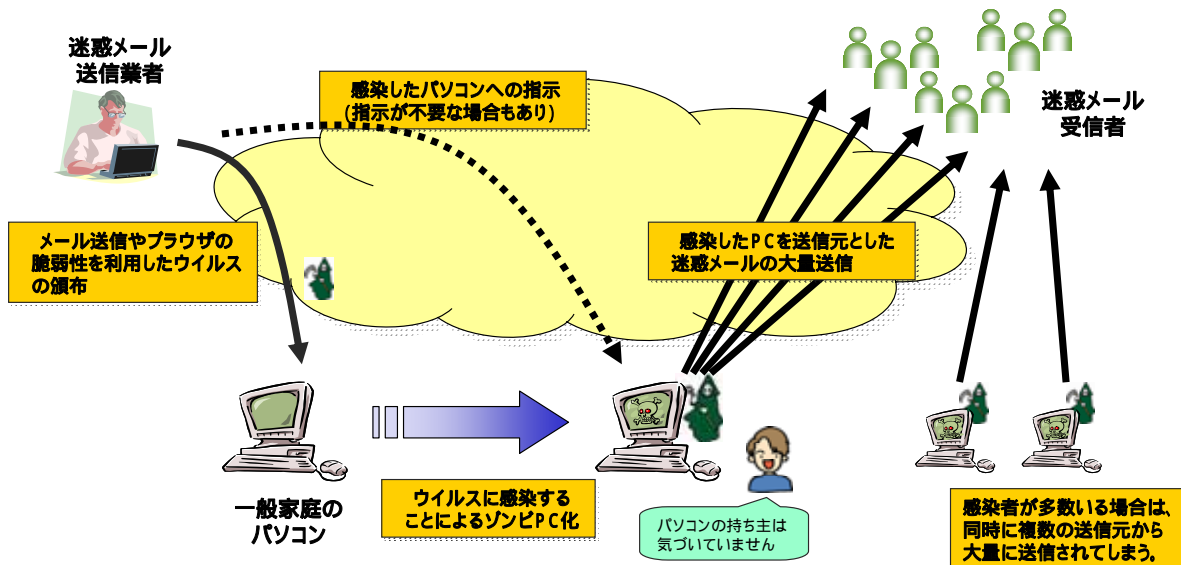
【悪質化・巧妙化した送信手法：「渡り」による送信】

NTT東西のフレッツ網を利用している場合に、あるISPが利用できなくなると、即座に他のISPと契約することにより、間を空けずに継続して迷惑メールの送信を行うもの。



【悪質化・巧妙化した送信手法：「ゾンビPC⁹(スパムゾンビ)」による送信】

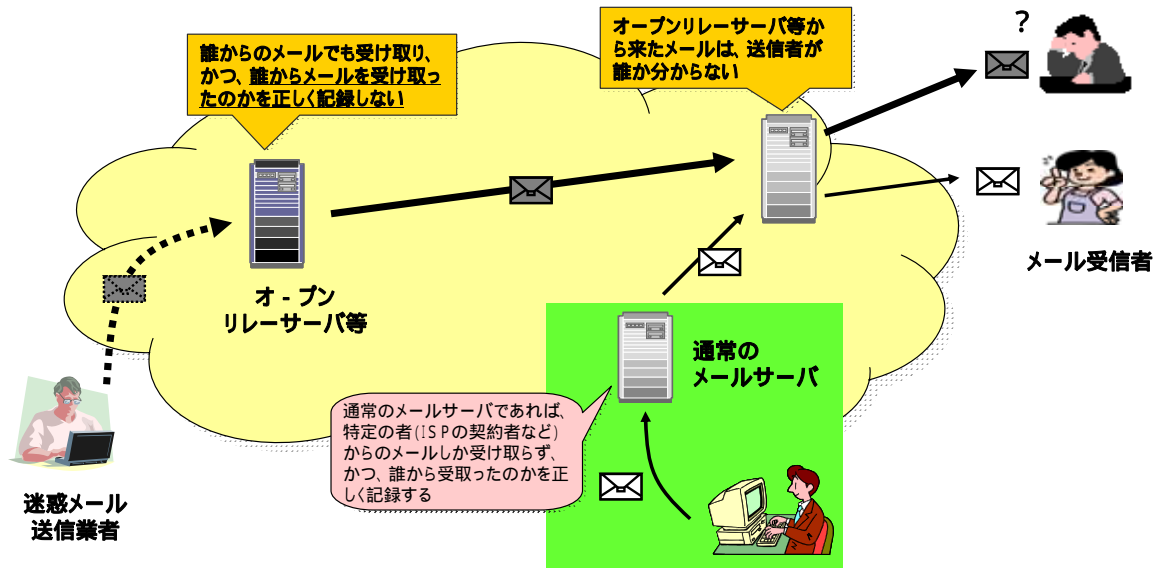
第三者のPCに不正侵入したりウイルスに感染させたりすることにより、そのPCを迷惑メールを送信するために利用するもの。



⁹ 最近では、ゾンビPCのことをボット（ボットネット）と呼ぶこともある。

【悪質化・巧妙化した送信手法 : 「オープンリレーサーバ等」を経由した送信】

電子メール送信の経路情報を正しく記録しない設定がされているサーバ（オープンリレーサーバ等）を経由することにより、送信者の情報を受信者に分からないようにするもの。



【悪質化・巧妙化した送信手法 : 「自動アドレス収集」による送信】

web上に情報が掲載されているメールアドレスを自動的に収集することにより、迷惑メールを送信する。



友人との間のみ等、メールを日常やりとりする特定の相手方との間でのみメールアドレスを伝えている場合に比べ、自己の電子メールアドレスをweb上等に公開し、広く電子メールによるやりとりを可能としている場合に特に迷惑メールの受信件数が多くなっているのではないかとされているが、上記のような手法により迷惑メール送信者の送信先リストに掲載されてしまっている可能性がある。

(3) 諸外国における迷惑メールの実態と対策

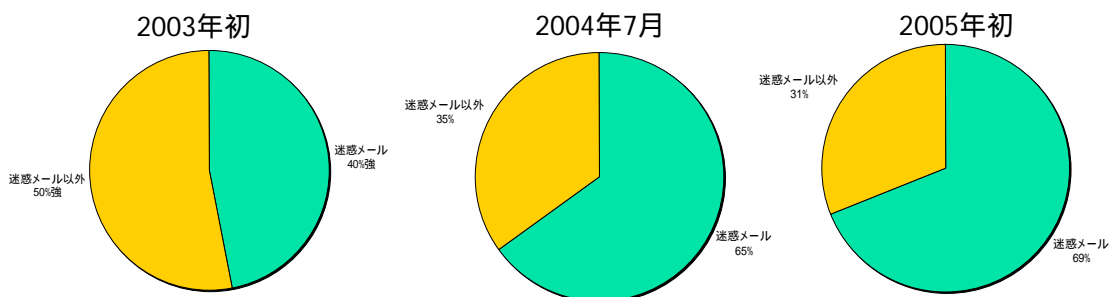
諸外国における迷惑メールの現状

迷惑メールの問題は、我が国においてのみならず諸外国でも問題となっており、迷惑メール対策は世界的な課題となっている。

1. 世界の迷惑メールの割合

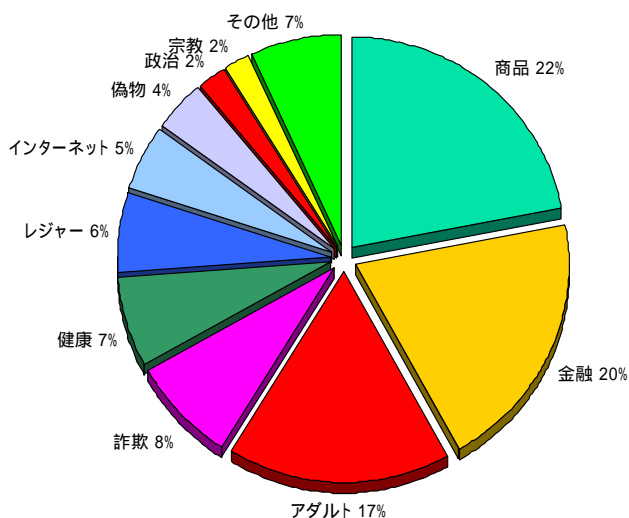
世界全体での迷惑メールの状況を示すものとしては、Symantec 社によれば、全電子メールに占める迷惑メールの割合が徐々に上昇していることを示しており、2003 年初め頃には 40%強であったものが 2004 年 7 月には 65% 程度となり、2005 年に入って 69%に達したとしている。

世界における全電子メールに占める迷惑メールの割合



また、Message Labs 社によれば、世界中の迷惑メールの比率は 2003 年通年では約 40%だったものが 2004 年通年では約 73%に上昇したとし、送信手法として家庭のユーザが迷惑メール送信のための踏み台にされているとしている。

なお、迷惑メールの内容としては、商品の宣伝が 22%、金融関係の宣伝が 20%、アダルト関係が 17%となっており、出会い系サイト等のアダルト関係の宣伝がほとんどを占める我が国における状況とは異なっている (Symantec 社調査)。

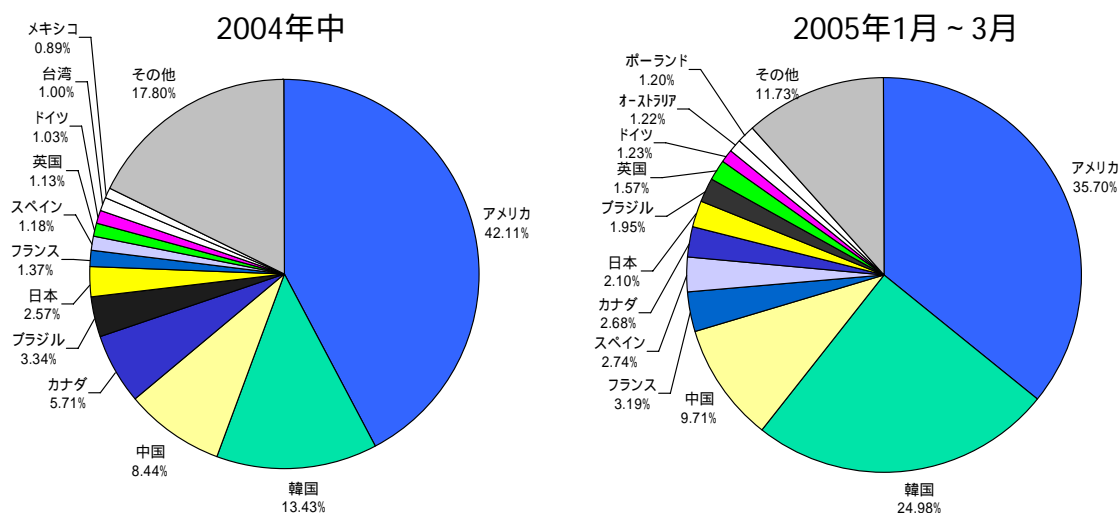


2. 世界の迷惑メールの発信元

諸外国における迷惑メールの状況について、Sophos 社が発信元の国別の統計¹を公表しており、2004 年 1 年間の統計として第 1 位が米国で約 42%、第 2 位が韓国で約 13%、第 3 位が中国（香港含む）で約 8.4%と、米国から発信されるものが最も多いという結果になっている（我が国は第 6 位で約 2.6%）が、それに続く国として韓国や中国の割合が増加しており、2005 年 1 月から 3 月の統計では、第 1 位が米国である点には変わりはないが約 36%に減少し、韓国及び中国がそれぞれ約 25%及び約 10%と上昇している（我が国は第 7 位で約 2.1%）。

また、Sophos 社は、迷惑メールの 40%以上がゾンビ PC から送信されているのではないかとしている。

迷惑メール発信国の推移



3. 諸外国と日本の違い

諸外国では電子メールの利用は PC を利用するのが一般的であり、携帯電話での電子メールの利用はそれほど普及していないため、迷惑メールの被害も PC への着信が中心となっている。

欧米、特に米国では携帯電話端末を電子メール端末として利用すること自体がそれほど多くなく、韓国では携帯電話での電子メール利用も相当程度普及しているが、いわゆる SMS の利用がほとんどであり、我が国のようにインターネット上で利用する電子メールと相互に送受信することが可能な形態での利用が一般的となっているわけではない。

¹ 世界各地に配置したハニーポット(おとりのメールアドレス)で受信したメールを分析したもの。

諸外国における迷惑メール対策法の整備・運用状況

1. 米国

米国では、2004年1月にCAN-SPAM法²が施行されている。この法律では、我が国における特定電子メール法と同様、基本的にオプトアウト方式を採用しており、広告宣伝メールの送信について電子メールの内容が広告又は勧誘である旨の表示や、受信拒否の通知が可能である旨及びその連絡先メールアドレスの表示を義務づけるとともに、受信者から受信拒否の通知を受けた以降は再度の送信を禁止している。

拒否者への再送信禁止以外の禁止事項としては、不正にアクセスしたコンピュータから送信すること、送信元を隠蔽するために送信を中継させること、ヘッダ情報を改ざんして送信すること、他人のウェブサイトから自動取得したアドレスへ送信すること、自動生成したアドレスへ送信することなどがある。

米国スパム対策法の概要

表示義務

- ・ 広告又は勧誘である旨
- ・ 受信拒否を行う機会がある旨及び受信拒否を要請を受けるための電子メールアドレス
- ・ 送信者の住所
- ・ 性的素材を含む場合は、その旨の警告ラベル 等

禁止事項

- ・ 不正にアクセスしたコンピュータからの送信（いわゆるゾンビPCによる送信など）
- ・ 送信元を隠蔽するために送信を中継させる行為（いわゆるオープンリレーサーバを利用した送信など）
- ・ ヘッダ情報を改竄した送信
- ・ 受信拒否の要請から10日後以降の当該受信者への送信の禁止
- ・ 他人のウェブサイトから自動取得したアドレス及び自動生成したアドレスを使用した送信の禁止 等

罰則

- ・ 最高で5年間の懲役または罰金（損害賠償額の上限は600万ドル）

なお、CAN-SPAM法の規定はPCに着信する電子メールを対象としたものであり、その執行はFTC（連邦取引委員会）が行っているが、携帯電話に着信する電子メールについてはFCC（連邦通信委員会）が執行することとされ、その具体的規制内容をFCCの規則（FCCルール）で定めるべき旨が同法において規定されている。

この規定を受けて、FCCでは2004年8月12日にFCCルールを策定し、携帯電話に着信する電子メールについてはオプトイン方式を採用し、事前に明確な同意を得なければ広告宣伝メールを送信してはならないこととした。

² Controlling the Assault of Non-Specified Pornography and Marketing Act of 2003.

米国 F C C 携帯端末向けスパム規制の概要

オプトイン

- ・受信者から、事前に明確な同意を取らない限り、移動サービスを介した商業メッセージの送信は禁止。
- ・受信拒否の通知を受けるための方法（無料かつ30日間は有効である必要あり）を表示。
- ・同意をした送信者であることを特定するための情報を表示。
- ・受信拒否の通知を受けた場合には、10日以内に送信を終了すること。

ドメインリスト

- ・移動サービス提供事業者は、移動サービス用ドメイン名を F C C に登録、F C C はリストを公表。
- ・リスト掲載期間が 30 日を超えたドメインあてに商用メッセージを送信することが禁止される。
- ・新たなドメインの利用 30 日前に登録、6 ヶ月以上使用しないドメインを削除。

同意の取得方法

- ・事前の同意は、口頭または書面（電子的な方法を含む）で得ることができる。
- ・書面による同意には、署名（電子署名含む）が必要。
- ・ウェブサイトで同意を得る場合は、受信者が受信を容認するメールアドレスを入力させなければならない。
- ・同意は、商業メッセージを送信する者が自ら取得しなければならない。

適用除外

- ・SMS 及び企業と顧客間の取引メールは対象外（SMS については、既存の迷惑電話取り締まりの対象となる）
- ・PC 着メールを携帯電話に転送する（ように受信者が設定している）場合は対象外

米国政府は、CAN-SPAM 法の執行のために F T C がスパム送信事業者の取締りを行っているほか、司法省の実施するスパム制圧作戦（Operation Slam Spam）³による摘発も実施されている。

また、民間のプロバイダ等においても、CAN-SPAM 法に違反するスパム送信者に対し損害賠償請求等の訴訟を積極的に提起している。

米国における CAN-SPAM 法執行の状況

時期	概要
2004 年 3 月	Microsoft 社、AOL 社、Earthlink 社、Yahoo 社が、大手スパム業者を含む数百人のメール送信者に対し、差出人アドレスの詐称や受信拒否手続の欠如等の CAN-SPAM 法違反があるととして、各地の連邦裁判所で計 6 件の訴訟を提起。
2004 年 8 月	FBI(連邦捜査局)が、ポルノサイトを宣伝するメールをいわゆる「ウォードライビング」(無防備な無線 LAN のアクセスポイントを求めて、郊外を車で探し回る方法)の手法で車上のパソコンから不正アクセスを行うなど、CAN-SPAM 法に違反して大量に送信した容疑者を逮捕。
2004 年 12 月	Microsoft 社が、アダルトメールを迷惑メール送信業者に対し不正侵入したコンピュータを経由して送信し、送信停止の方法も記載せず CAN-SPAM 法に違反しているとして 7 件の訴訟を提起。
2005 年 1 月	テキサス州検察が、住宅ローンや保険商品の売り込みを行うメールを CAN-SPAM 法に違反して大量送信していた迷惑メール送信業者を摘発。
2005 年 1 月	F T C が、ポルノサイトに勧誘するメールを CAN-SPAM 法に違反して送信していた複数の事業者を提訴し、連邦裁判所が業務停止を命令。
2005 年 4 月	F T C 及びカリフォルニア州検察が、住宅ローン等の売り込みを行うメールを CAN-SPAM 法に違反して送信していた事業者を提訴し、連邦裁判所がメール送信を停止するよう命令。

³ 官民合同で実施しているサイバー犯罪一掃作戦 (Operation Web Snare) 中のスパム対策に特化したプロジェクト。F T C や民間団体等が協力している。

2. 英国

英国を含むEU諸国では、2002年7月12日に「電子通信分野における個人データ処理及びプライバシー保護に関する指令」がEU議会で決定され、勧誘のための電子メールの利用は、相手方の事前同意がある場合に限られるというオプトイン方式の採用と、発信者の身元を偽ったり隠したりすること、受信者が送信停止を求めるための確実な連絡先を示さずに送信することの禁止について、加盟国において国内法の整備を行うこととされた。

英国では、これを受け、2003年9月18日に「2003年プライバシー及び電子通信(EU指令)規則」を策定し、上記EU指令の内容に沿った国内法整備を行い、2003年12月11日から施行している。

英国スパム対策法の概要

オプトイン

- ・ 次の場合を除き、マーケティング目的での一方的な電子メールの送信は禁止
メール送信について受信者が同意した場合
製品販売の過程で、受信者に関する連絡情報を取得した場合であって、類似製品のみに関するメールを送信する場合(拒否できる手段を提供する必要あり。)
- ・ 個人に対して送られる電子メール、SMSが対象

禁止事項

- ・ 送信者の身元を偽装、秘匿すること
- ・ 送信停止を要求するための有効なアドレスを提供しないこと

罰則

- ・ 違反者には最大5000ポンド(約93万円)の罰金

3. オーストラリア

オーストラリアでは、2004年4月10日に「Spam Act 2003」が施行されている。EU諸国と同様にオプトイン方式を採用しているほか、メールアドレスの自動収集ソフトの使用・販売等や自動的に作成したアドレスあての送信を禁止している。

オーストラリアスパム対策法の概要

オプトイン

- ・ 望まれない商業メールの送信禁止(受信者が同意した場合のみ送信可能)
- ・ 電子メール、ショートメッセージサービス、インスタントメッセージが対象
- ・ オーストラリア発の全メール及び、海外発オーストラリア着のメールも対象

表示義務

- ・ 受信者が送信者と連絡をとるために必要な正確な情報
- ・ 今後メールを受け取らないようにするための方法

禁止事項

- ・ メールアドレスの自動収集ソフトの使用及び当該ソフトを用いて作成したアドレスリストの使用禁止

罰則

- ・ 違反者には最大約22万豪ドル(約1760万円)の罰金
(再犯の場合、最大約110万豪ドル(約8800万円の罰金))

4. 韓国

韓国では、「情報通信網利用促進及び情報保護等に関する法律」(Act on Promotion of Information and Communications Network Utilization and Information Protection, etc.)の中で迷惑メール対策を法制化しており、2002年12月に本格的な法整備を行っている。

原則としてオプトアウト方式を採用しているほか、ヘッダの改ざんなどの受信拒否から逃れるための技術的操作を行うことやメールアドレス自動作成プログラムを用いることの禁止、ウェブサイトから管理者に無断でメールアドレスを収集することなどを禁止している。

また、携帯電話でのメールについて、オプトイン方式を採用している。

韓国スパム対策法の概要

オプトアウト

- ・ 受信者の明確な拒否に反して広告メールを送ることを禁止
- ・ 電子メール、電話、FAX、ショートメッセージサービス、大統領令で定めるその他メディアが対象
違反者には3000万ウォン(約300万円)の罰金

表示義務

- ・ タイトル先頭に(韓国語で)「広告」または「アダルト広告」、末尾に「@」と表記
- ・ 本文に発信者の連絡先及び受信拒否の明確な方法を明記
違反者には3000万ウォン(約300万円)の罰金

禁止事項

- ・ 未成年者(19才以下)に対する卑猥な内容、暴力的な内容を含む広告メールの送信の禁止
- ・ ヘッダの改ざんなど、受信拒否から逃れるためのあらゆる技術的操作の禁止
- ・ メールアドレスおよび電話番号の自動生成プログラムの使用禁止
- ・ ウェブサイトから管理者に無断でメールアドレスを収集すること及びメールアドレスリストの販売の禁止
違反者には2年以下の禁固または1000万ウォン(約100万円)の罰金

(参考) 諸外国の迷惑メール対策法と特定電子メール法の比較

	米国 (平成16年1月施行)	英国 (平成15年12月施行)	オーストラリア (平成16年4月施行)	韓国 (平成14年12月本格施行)	日本 ⁴ (平成14年施行時 改正後)
規制対象					
事業用アドレス あての送信		×			×
表示義務					
送信者の情報					
受信拒否方法					
禁止行為					
架空アドレス あて送信		×			
送信者の情報を 隠蔽する特殊な 手法での送信		×	×		×
罰則	5年以下の懲役刑 罰金刑	罰金刑	罰金刑	2年以下の禁固刑 罰金刑	間接罰のみ 直罰も追加
電気通信事業者 の役務提供拒否	-	-	-		(一部拡大)

⁴ 今般の法改正により矢印右側のように制度が改められることになる(p21以降参照)。

国際的な迷惑メール対策の進展状況

また、各国における法制度の整備に加えて、平成16年以降、OECD、ITU、APEC（アジア太平洋経済協力）といった国際機関等において、迷惑メールに関する議論が活発に行われてきている。

OECD（経済協力開発機構）

- 平成16年 2月 第1回「スパムに関するワークショップ」（ブリュッセル）
・スパムが世界規模で問題となっていること、多面的な対策が必要であることの認識を共有
7月 「スパムタスクフォース」設置（10月に第1回、翌年3月に第2回会合が開催）
・各種ワークショップとメンバー限定用電子掲示板を通じて議論
・法令、技術等多面的（包括的）なスパム対策の取りまとめが目的
9月 第2回「スパムに関するワークショップ」（釜山）
・第1回会合で議論された対策の具体的方策を議論
10月 「スパム対策執行に関するワークショップ」（ロンドン）
・米・英・豪を中心に、執行面に焦点を当てて議論

ITU（国際電気通信連合）

- 平成16年 7月 WSIS（世界情報サミット） スパム対策に関するテーマ会合
・スパムが世界規模で問題となっていること、多面的な対策が必要であることの認識を共有
・豪・韓、米・英・豪を先例としたMoU（覚書）の締結等による国際協調の必要性を確認
12月 「規制機関による国際シンポジウム」
・各国規制機関によるスパム対策に関するシンポジウムを開催
平成17年11月 第2回WSISチュニス会合
・スパム対策が、インターネットガバナンスと並んで主要議題となる予定

APEC（アジア太平洋経済協力）

- 平成16年 2月 電子商取引ステアリンググループ会合（ECSG）
・スパムが主要議題となり、情報交換、各国対策の取りまとめ、他機関との連携推進を合意
9月 電気通信・情報ワーキンググループ会合（TEL）
・セキュリティの一環として、スパム対策を議論

特に、平成16年10月にロンドンで開催された「スパム対策執行に関するワークショップ」では、「国際的スパム執行協力に関するロンドン行動計画」（London Action Plan: LAP）が合意され、定期的な電話会議を開催しつつ、各国における迷惑メールの特徴等に関する世界規模の調査（International Internet Sweep）や、世界各国のISPに対してスパムゾンビに関する注意喚起レターを発出する取組（Operation Spam Zombies）を行っている。

「Operation Spam Zombies」について

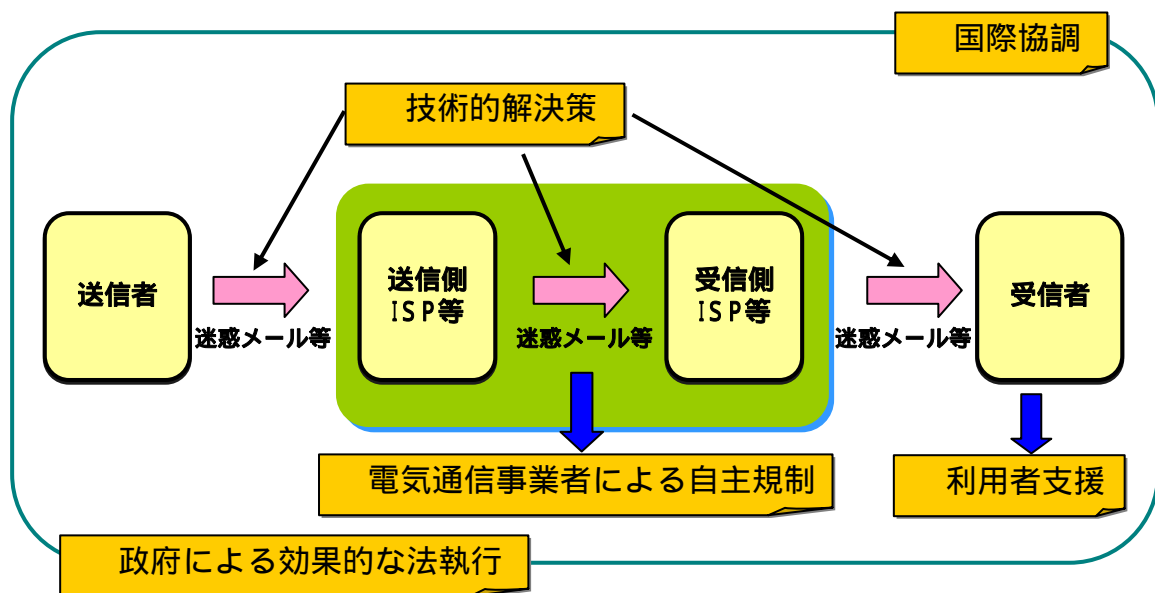
全世界のISPに対し、スパムゾンビの脅威・対策等に言及した注意喚起レター（メール）を発出するもの
25ヶ国34政府機関（今後増加する予定）を代表して、米国FTCが実施（日本からは総務省及び経済産業省が参加）
平成17年5月24日（火）から順次実施
平成16年10月に世界各国のスパム対策法執行機関等が合意した「ロンドン・アクション・プラン（LAP）」に基づく取組
対策として、25番ポートブロック、流量制限規制、感染防止方法等に関するユーザへのアドバイス、等を列挙
（一部の対策については、実施に当たり電気通信事業法との関係を整理する必要）
今後、スパムゾンビへの感染が疑われるIPアドレスの管理者への個別の注意喚起レターが発出される予定

3. 迷惑メール対策の方向性

(0) 総合的な対策の必要性

迷惑メールによる被害が減少していない現状を踏まえると、何らかの対策を講じる必要があることは明らかであるが、前章で述べたように、迷惑メールの送信手法は巧妙化、悪質化してきており、措置命令等政府による法執行のみで迷惑メールを撲滅することや、フィルタリング等の技術的対策のみで迷惑メールを撲滅することは困難である。

したがって、本研究会では、政府による法執行の強化等特定の部分のみに着目して迷惑メール対策を行うのではなく、他の部分において可能な取組との連携を踏まえ、総合的な対応方策を検討する必要があるとの認識に基づき検討を行ってきた¹。



検討の過程で、平成 16 年 12 月 24 日には、中間とりまとめとして特に法制度に係る論点²について検討結果を示したところであるが、それ以降に技術的解決策や利用者支援、国際協調についての論点を含めて検討した結果としての迷惑メール対策の方向性を、次ページ以降でそれぞれ掲げていくこととする。

¹ このような考え方は諸外国でも共通しており、2004年2月に開催されたOECDスパムワークショップにおいても、「スパム対策は“No silver bullet”(特効薬はない)であり、多面的な対応が不可欠。できることから行動すべき」との認識で一致している。

² 本文図の「政府による効果的な法執行」のうち法制度の見直しに係る部分及び「電気通信事業者による自主規制」のうち特定電子メール法に基づく電気通信事業者による役務提供拒否。

(1) 政府による効果的な法執行

①特定電子メール法改正の概要

本研究会の中間とりまとめとして法制度の見直しの方向性について提言を公表した後、総務省において特定電子メール法の改正案について検討が行われ、平成17年3月11日に第162回国会に「特定電子メールの送信の適正化等に関する法律の一部を改正する法律案」が提出された。

この法案は、国会での審議の結果、原案のとおり衆議院・参議院とも全会一致で可決・成立し、5月20日に公布された¹。施行日は公布の日から起算して6月を超えない範囲内において政令で定める日とされており(同法附則第1条)、平成17年秋頃までに施行される見込みとなっている。

本研究会の中間とりまとめ(平成16年12月24日公表)の概要

近年、迷惑メールの送信が巧妙化・悪質化していることを踏まえ、規制対象範囲の見直しや違反者への取り締まりの強化を図ることが必要として、法制度の見直しについて以下の基本的方向性を提示。

1. 特定電子メールの定義の見直し

企業や事業を営む個人が利用している事業用メールアドレスに対する送信を行う場合や、携帯電話同士で短い文字メッセージを電話番号あてに送受信するSMS(ショートメッセージサービス)による広告宣伝メールの送信についても、特定電子メール法の対象に追加することが適当。

2. 架空アドレスあて送信禁止の範囲拡大

現在法第5条において禁止されている架空アドレスあてのメール送信は、広告宣伝メールを送信する場合であるが、その他の内容のメールを送信する場合についても、対象範囲に含まれるように見直すことが適当。

3. 悪質な違反行為に対する直罰化

現在、違反行為に対しては、総務大臣の措置命令がまず行われることとなっているが、重大な法益侵害をもたらすおそれのある悪質な送信行為については、送信者に直接刑事罰を科すことも検討することが適当。

4. ISP等による役務提供拒否の範囲の明確化

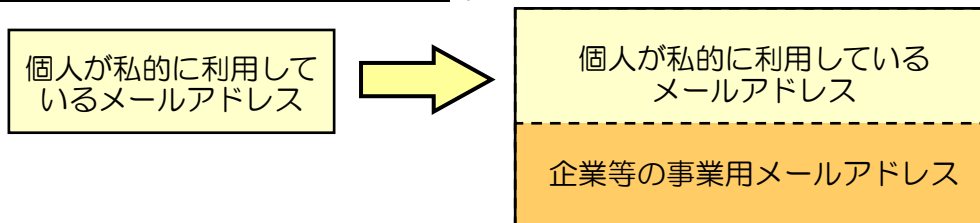
法第10条において規定されている場合以外にも、電気通信事業者が役務提供を拒否することに正当な理由が認められる事例があるため、正当性のあると考えられる事例の整理を進める必要がある。

改正法の概要は次のとおりであり、本研究会の中間とりまとめにおける提言が盛り込まれたものとなっている。

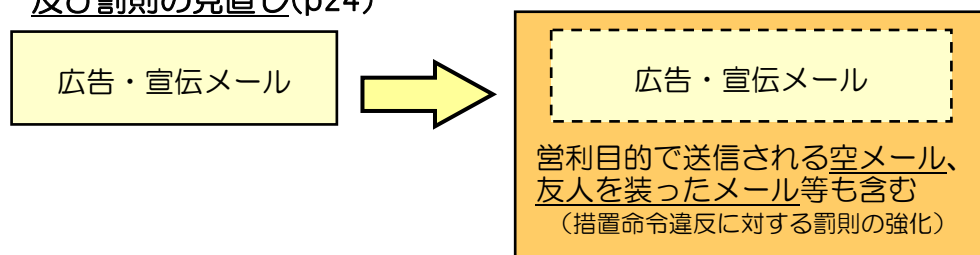
¹ 平成17年法律第46号。

特定電子メールの送信の適正化等に関する法律の一部を改正する法律の概要²

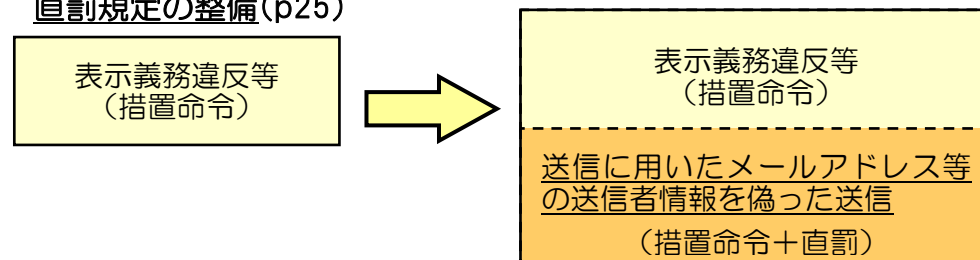
1. 特定電子メールの範囲の拡大(p23)



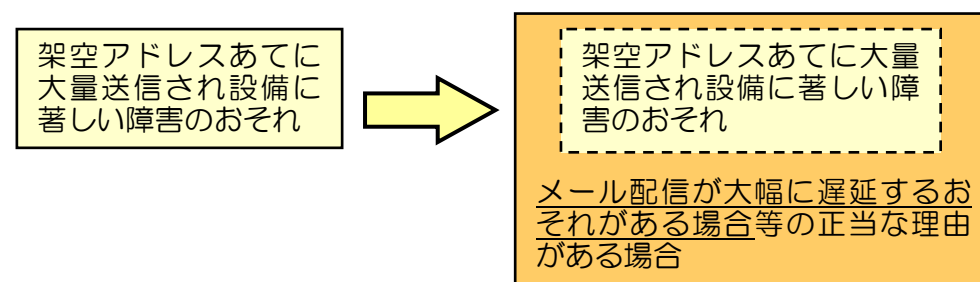
2. 架空アドレスあてのメール送信を禁止する範囲の拡大及び罰則の見直し(p24)



3. 送信者情報を偽った電子メール送信の禁止及び直罰規定の整備(p25)



4. 電気通信事業者による役務提供拒否事由の拡大(p26)



² このほか、総務大臣に対する申出をしようとする者に対する指導・助言や申出に係る事実関係調査等の業務(特定電子メール送信適正化業務)について、これまで総務大臣が指定した公益法人(指定法人)が行うこととしていたものを、総務大臣の登録を受けた者(登録機関)が行うこととする制度に変更する改正も行われている。

なお、指定法人の業務と登録機関の業務の内容には大きな変更はない。

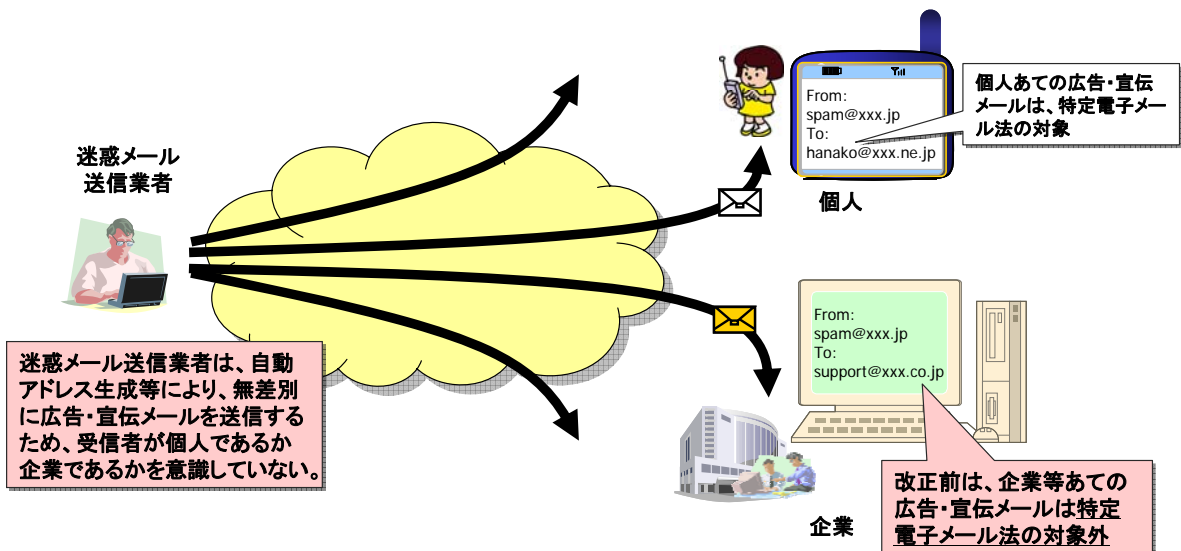
1. 特定電子メールの範囲の拡大（改正後の第2条第2号）

「特定電子メール」の定義を拡大し、個人が私的に利用しているメールアドレスあての送信のみが規制の対象だったものを、企業等が利用しているメールアドレス（事業用メールアドレス）にも規制対象を拡大した。

これにより、個人事業主や会社の従業員等にあてて送信される広告宣伝メールについても、特定電子メール法の規制が及ぶこととなった。

企業等が利用する事業用メールアドレスに対する送信について

迷惑メールの送信者は無差別に広告宣伝メールを送信しているため、現在特定電子メール法の対象となっている、個人が私的に利用する電子メールアドレス以外にも、企業や事業を営む個人が利用している事業用メールアドレスに対しても同じように送信している。



(定義)

第二条 この法律において、次の各号に掲げる用語の意義は、当該各号に定めるところによる。

二 特定電子メール 次に掲げる者以外の者に対し、電子メールの送信をする者(営利を目的とする団体及び営業を営む場合における個人に限る。以下「送信者」という。)が自己又は他人の営業につき広告又は宣伝を行うための手段として送信をする電子メールをいう。

イ あらかじめ、その送信をするように求める旨又は送信することに同意する旨をその送信者に対し通知した者(当該通知の後、その送信をしないように求める旨を当該送信者に対し通知した者を除く。)

ロ その広告又は宣伝に係る営業を営む者と取引関係にある者

ハ その他政令で定める者

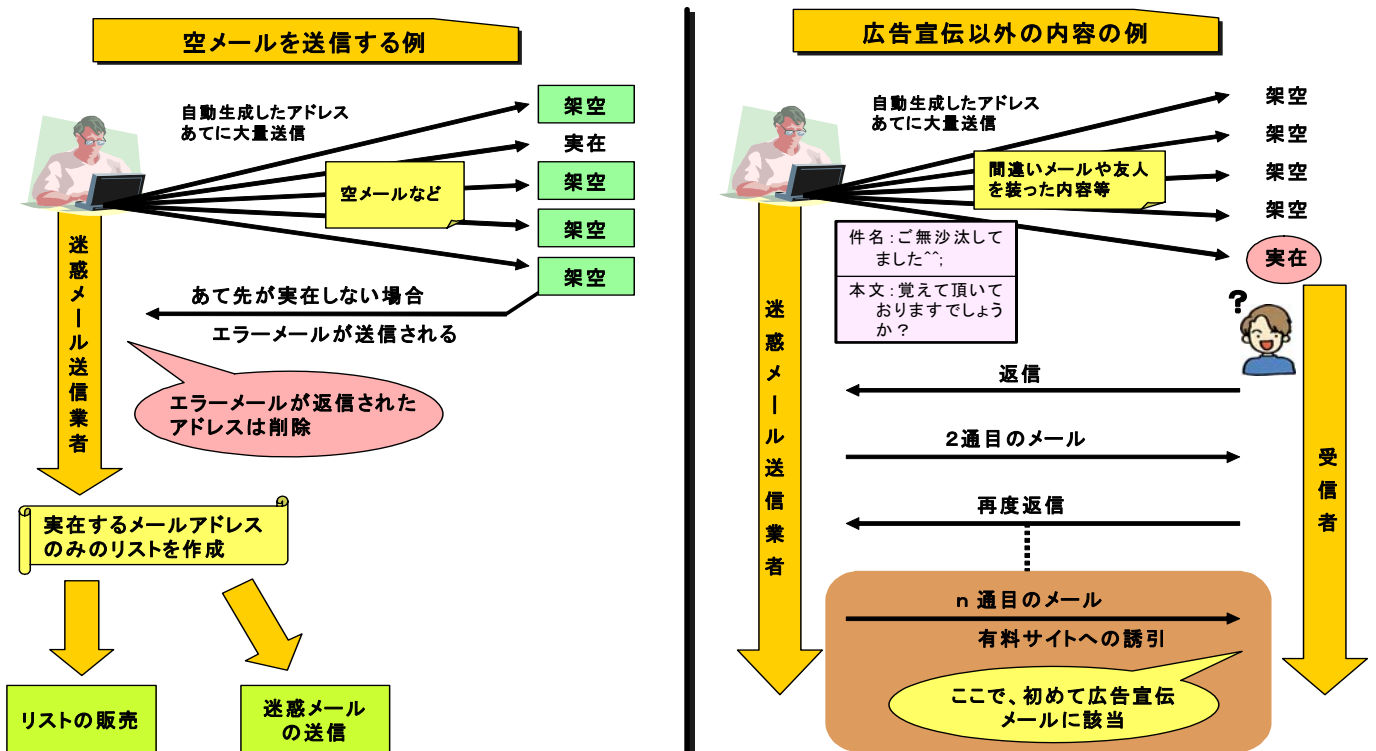
※ハの政令は未制定。

2. 架空アドレスあて送信禁止の範囲拡大及び罰則の見直し（改正後の第5条）

架空アドレスあて送信の禁止について、広告・宣伝を内容とする電子メールのみが対象となっていたものを、営利目的で送信されるメールであれば内容に関わらず禁止することとして、空メールや友人を装ったメールなどについても対象に含まれるようにした。

また、上記行為に対する措置命令違反者に対する罰則を50万円以下の罰金から、1年以下の懲役又は100万円以下の罰金に引き上げている。

改正前の第5条の規制の対象となっていない 広告、宣伝目的以外の架空アドレスあてメール送信のイメージ



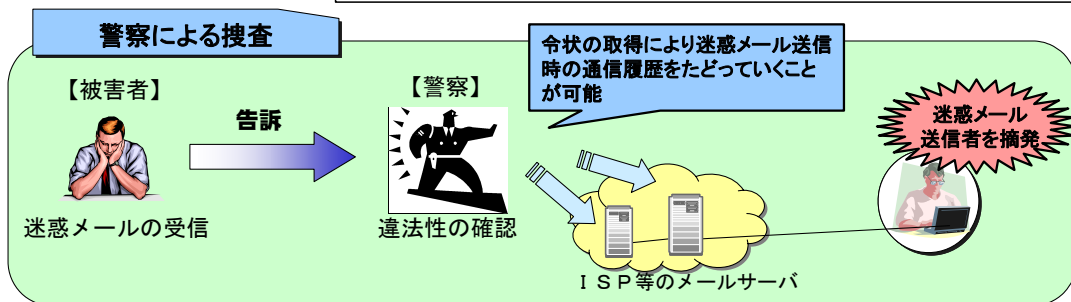
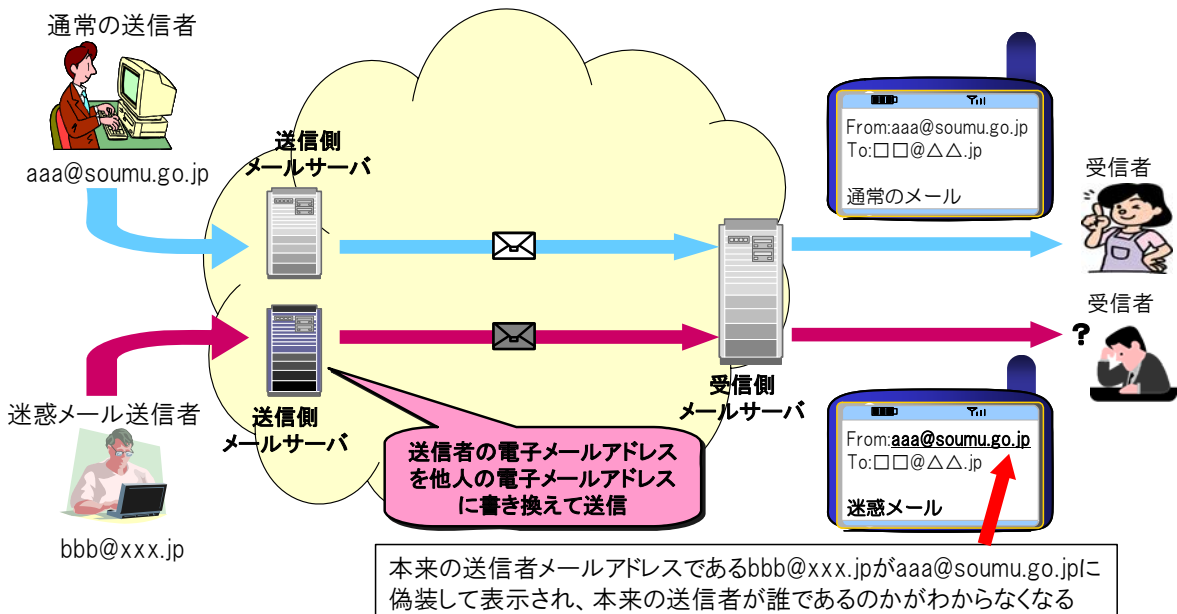
(架空電子メールアドレスによる送信の禁止)
 第五条 送信者は、自己又は他人の営業のために多数の電子メールの送信をする目的で、架空電子メールアドレスをそのあて先とする電子メールの送信をしてはならない。

[架空電子メールアドレスの定義(第2条第4号)]
 次のいずれにも該当する電子メールアドレスをいう。
 イ 多数の電子メールアドレスを自動的に作成する機能を有するプログラム(電子計算機に対する指令であって、一の結果を得ることができるように組み合わせられたものをいう。)を用いて作成したものであること。
 ロ 現に電子メールアドレスとして利用する者がいないものであること。

3. 送信者情報を偽った送信の禁止及び直罰規定の整備（改正後の第6条）

最近における悪質な迷惑メールの送信手法として、メールアドレスの改ざんや他人のPCを踏み台にして送信するなどの方法により送信者の情報を偽って送信し、受信者による対応や政府による取締りを困難にしているものがほとんどであることが挙げられる。

これを踏まえ、広告宣伝メールを送信する際に、from 欄のメールアドレスの詐称など、送信者情報を偽って送信することを禁止した。改正前の特定電子メール法では、法違反者に対しては、総務大臣の措置命令をまず行い、これに違反した場合にはじめて刑事罰の対象としていたが、改正により、送信者の情報を偽って送信する行為については、直接刑事罰（1年以下の懲役又は100万円以下の罰金）を科すこともできるようにした。

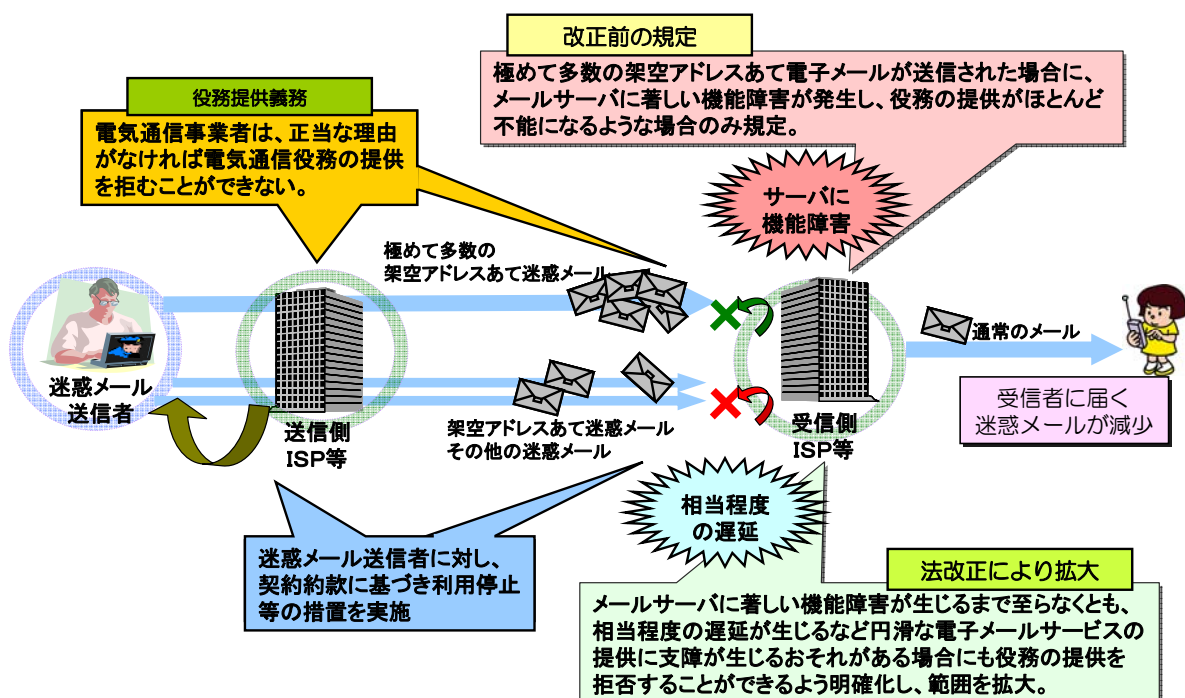


（送信者情報を偽った送信の禁止）
 第六条 送信者は、自己又は他人の営業につき広告又は宣伝を行うための手段として、電子メールの送受信のために用いられる情報のうち送信者に関するものであって次に掲げるもの（以下「送信者情報」という。）を偽って電子メールの送信をしてはならない。
 一 当該電子メールの送信に用いた電子メールアドレス
 二 当該電子メールの送信に用いた電気通信設備（電気通信事業法第二条第二号に規定する電気通信設備をいう。）を識別するための文字、番号、記号その他の符号

4. 電気通信事業者による役務提供拒否事由の拡大（改正後の第11条）

電気通信事業者は、電気通信事業法第6条により不当な差別的取扱いが禁止されており、同法第121条等により認定電気通信事業者等に役務提供義務が課せられている。

改正前の特定電子メール法では、電気通信事業者が役務提供を拒否できる場合として、メールサーバがダウンして事業者の設備に著しい障害が発生するなど、厳しい条件を満たした場合のみを規定していたが、メール送信が大幅に遅延する可能性があるような場合など、正当な理由があると認められる場合についても含まれるように範囲を拡大した（p30参照）。



なお、オプトイン方式の導入については、今般の改正では見送られているが、本研究会の中間とりまとめにおいても当面はオプトアウト方式を維持するのが適当としつつ³、オプトイン方式の採用国における取締りの効果等を注視しながら今後も導入の是非について継続的に検討する必要があると提言しているところである。

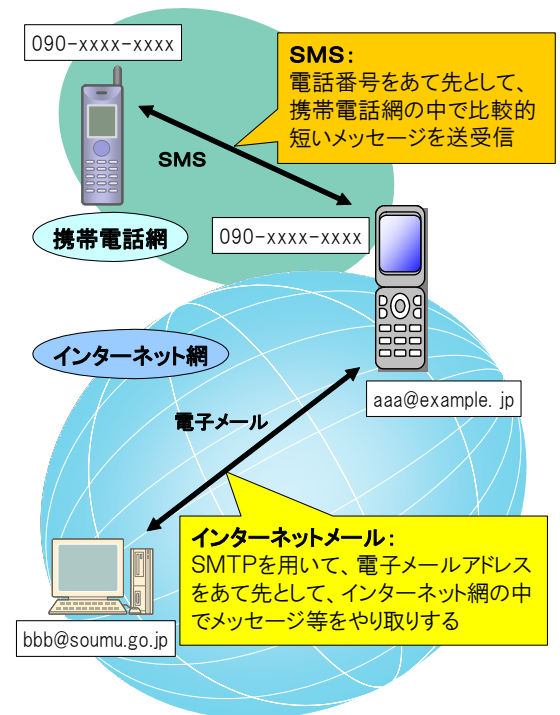
³ 中間とりまとめにおいては、現在の迷惑メールの大きな問題点は、送信行為の巧妙化・悪質化により、違法送信者に対する行政による取締りや電気通信事業者による対応が困難となっている点にあり、オプトイン方式を採用したとしてもこの点には変わりがないと結論付けられている。

②ショートメッセージサービス（SMS）への対応

携帯電話同士で短い文字メッセージを電話番号により送受信する「ショートメッセージサービス」（SMS）は、改正前の特定電子メール法における「特定電子メール」の定義に含まれていない⁴ため、本研究会の中間とりまとめにおいて特定電子メールの定義に含めることが適当と提言したところである。

特定電子メールの対象に含まれることになる電子メールの通信方式の種類については総務省令に委任されており、法改正にあわせて総務省令を改正することが予定されている。

なお、本研究会が中間とりまとめにおいてSMSを特定電子メールの対象に含めるに当たり提言した内容は以下のとおりである。



- ・SMSでは原則として件名欄（表題部）が存在せず、送信可能な文字数が数十文字程度のものもあるなど、表現能力が限定されているが、特定電子メールの表示義務は受信者に対し情報として提供することが必要な最小限のものについて定めていることを踏まえ、義務を免除するのではなく表示方法に可能な範囲で柔軟性を持たせることで対応すべきこと。
- ・SMS以外の通信方式を採用している電子メールサービスについても、その普及状況、利用の実態、技術方式の特徴等を踏まえ、広告宣伝メールの送信への利用が顕著となった場合には個別に検討を行うべきこと。

○特定電子メールの送信の適正化等に関する法律 （定義）

第二条 この法律において、次の各号に掲げる用語の意義は、当該各号に定めるところによる。

- 一 電子メール 特定の者に対し通信文その他の情報をその使用する通信端末機器（入出力装置を含む。次条において同じ。）の映像面に表示されるようにすることにより伝達するための電気通信（電気通信事業法（昭和五十九年法律第八十六号）第二条第一号に規定する電気通信をいう。）であつて、総務省令で定める通信方式を用いるものをいう。

○特定電子メールの送信の適正化等に関する法律施行規則 （通信方式）

第一条 特定電子メールの送信の適正化等に関する法律（以下「法」という。）第二条第一号の総務省令で定める通信方式は、シンプルメールトランスファープロトコルとする。

⁴ 特定電子メールの定義に含まれる電子メールの通信方式として、現在はシンプルメールトランスファープロトコルのみが規定されているが、SMSではこの通信方式は用いられておらず、各社独自の技術方式等が用いられている。

SMSでは、その通信方式の違いからインターネットメールに比べてフィルタリングが困難であるという特徴があるが、基本的に同一の携帯電話事業者のネットワーク内に送信者が存在することが明らかであることから、送信者を特定して行政による取締りや携帯電話事業者による利用停止等の措置を迅速に行うことによりSMSを用いて迷惑メールを送信する者への対策を効果的に実施することが期待される。

S M T P 以外の通信方式を使った主なメールサービス（SMS）一覧

	サービス名	文字数	送信料金※	備考
NTTドコモ	ショートメール	50文字	5円	固定電話、公衆電話等からも送信可
	SMS (FOMA)	70文字	5円	一部海外携帯にも送信可
KDDI(au)	Cメール	50文字	3円	
ボーダフォン	スカイメール	64文字	2円	固定電話、公衆電話等からも送信可
	ロングメール	3,000文字	4円	件名入力可能
	SMS (VGS)	70文字	5円	一部海外携帯にも送信可
TUKA	スカイメッセージ	64(192)文字	5円	固定電話、公衆電話等からも送信可
ウィルコム	DXメール	1,000文字	10円	件名入力可能
	ライトメール	45文字	6円	
	Pメール	半角20文字	6円	

※送信料金は料金プラン等によって異なる場合あり。

③改正法の効果的な執行に向けた課題

今回の特定電子メール法改正によって、送信者情報を偽った広告宣伝メールの送信に対する直罰規定の導入などの取締りの強化が行われることになるが、改正法の施行にあたっては、その効果的な執行が確保されることが必要不可欠である。

特に、以下の点については、改正法の効果的な執行のため十分な検討及びその実施が必要であると考えられる。

1. 迷惑メール相談センター

(財)日本データ通信協会に設置された迷惑メール相談センターについては、これまでも、パンフレットやホームページ等を通じて周知啓発に努めてきているが、取締り内容の強化や新たに登録機関に移行すること等を踏まえ、更なる認知度向上を目指して効果的な周知啓発を行う必要がある。

また、特定商取引法に基づき迷惑メール対策の業務を行っている(財)日本産業協会との連携を強化する必要がある。

さらに、違反行為に対する直罰が導入されると、センターに寄せられた送信者の情報が警察による捜査に活用されることも想定されるため、総務省のみならず警察との連携も視野に入れる必要がある。

総務省においても、センターで収集した情報に基づき、ある事業者が先行して実施し効果の大きいことが判明した迷惑メール対策について、他事業者も採用するように促すなど、センターの情報を積極的に活用することも有効である。

2. 関係省庁との連携強化

総務省は、迷惑メール対策を一層効果的に行うためパンフレットの共同作成や「迷惑メール追放支援プロジェクト」(p33 参照)等を通じて、特定商取引法を所管する経済産業省と連携してきたところであるが、送信手法の巧妙化・多様化や架空請求等詐欺行為の入口にメールが利用されている現状を踏まえると、今後、この連携はより一層重要なものになるほか、他省庁との連携も必要になってくるものと考えられる。

また、送信者情報を偽った広告宣伝メールの送信に対しては、警察が捜査を行うことも可能となるため、その適切な執行に当たっては、改正法施行後、総務省と警察が十分に連携を取っていくことが必要不可欠であり、両者の具体的な協力体制を確立していく必要がある。

3. 諸外国における迷惑メール対策との整合性確保

迷惑メールは、日本国内から発信されるものだけでなく、米国や韓国、中国など外国から発信されるものも多く、取締りを有効に行うためには、このような国境を越えて送信される迷惑メールについて、諸外国との連携を強化していくことが必要である⁵。

したがって、今後とも、諸外国の法規制の実態等を的確に把握し、必要に応じて我が国の法制度に反映させるとともに、諸外国への働きかけ等を行っていくことが求められる。

⁵ 外国から送信される迷惑メールについては、送信国において取締りが行われることが必要である。なお、日本国内から発信して外国のサーバを経由して日本国内に着信するものについては、特定電子メール法の規制が及ぶ。

(2) 電気通信事業者による自主規制

① 電気通信役務の提供の拒否

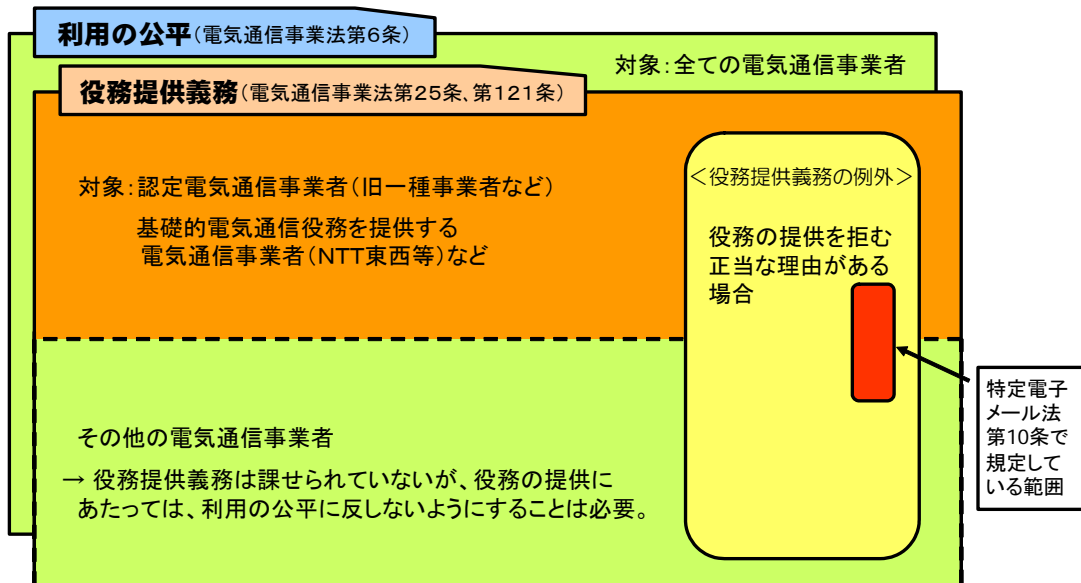
1. 改正前の規定

電気通信事業者に対しては、電気通信の利用者が公平にかつ確実に電気通信サービスが利用できるよう、電気通信事業法において、利用の公平（第6条）や役務提供義務¹（第121条等）の規定が設けられ、正当な理由がなければ電気通信役務の提供を拒むことができず、また、不当な差別的取扱いをしてはならないという義務が課されている。

これらの規定を前提として、改正前の特定電子メール法第10条²では、迷惑メールが送信される場合において電気通信事業者が電気通信役務の提供を拒否することに正当な理由がある場合の事例として、以下のように規定されている。

- ・ 一時に多数の電子メールを架空アドレスあてに送信した場合であって、
- ・ 自己の電気通信設備の機能に著しい障害を生ずることにより電気通信役務の提供に著しい支障を生ずるおそれがある場合に、
- ・ その送信をした電子メールについて拒否することができる。

改正前の特定電子メール法第10条と利用の公平及び役務提供義務の関係



¹ 役務提供義務の規定が適用されるのは、電気通信事業者のうち電気通信事業法第120条に規定する認定電気通信事業者や基礎的電気通信役務を提供する電気通信事業者に限られる。

² 今回の法改正により一部改正され第11条に移動することになる。

- 改正前の規定では、このように限定的な書きぶりとなっていることから、
- ・ 架空アドレスあてに送信された場合以外は一切対象とならない
 - ・ 役務提供に生じる支障が自己のメールサーバの著しい障害発生を理由とするものに限定されている
 - ・ 利用停止や契約解除のような措置は対象とならない

など、電気通信事業者が積極的に対応するために活用することが困難である場合が多くなっている（実際には、電気通信事業者は、約款に基づき本条によらない役務提供拒否を行っているが、電気通信事業法上の責任や契約者からの賠償請求などの法的リスクがあり、これを低減する必要性が指摘されていた）。

また、改正前の第 10 条で規定されているのは役務の提供を拒否することが正当と考えられる場合の一例であり、それ以外の事例における正当性の有無については個別具体的に判断することになるが、その他の場合には役務提供拒否がそもそも認められないのではないかという誤解も生じていた。

そのため、今回の法改正により範囲を拡大し、これまでよりも広い範囲において役務提供拒否が認められることを明らかにしている。

2. 法改正による拡大

具体的には、以下のような事例について対象範囲が拡大されたことになる。

なお、これらは法改正で拡大された部分に関して個別の要件ごとに具体例を記述したものであり、役務提供拒否につき正当な理由が認められるには全体として要件を満たさなければならないことに留意する必要がある。

【対象となる電子メールの範囲の拡大】

① 架空アドレスあての送信でなくとも、メールの大量送信により電子メールサービスの円滑な提供に支障を生じる場合も対象に含まれる。

- ・ 実在するアドレスへの大量送信の場合であっても、「その他電子メールの送受信上の支障を防止するため電子メール通信役務の提供を拒むことについて正当な理由があると認められるとき」に該当すれば役務の提供を拒否できる。

【メールサーバの機能障害要件の撤廃】

② メール処理に通常に比べて非常に時間がかかり、円滑な電子メールサービスの提供に支障が生じるおそれがあれば、対象に含まれる。

- ・ 具体的にどの程度の遅延を指すのかは、その電気通信事業者の設備やサービスの規模により変動するため一概には言えないが、送信したメールが通常より大きく遅れて届くような場合には対象となりうる。なお、この点については、た

例えば携帯電話の場合にはより即時性が求められるなど、個別具体的な事例において判断することが必要である。

③ 自社のネットワークから大量送信が行われたことにより他社のメールサービスに支障が生じ、相互にメールの送受信ができなくなることで自社のサービスに支障が生じるおそれがある場合も、対象に含まれる。

・受信した側だけでなく、送信側のISP等においてもその送信が行われることにより結果として自社の円滑な役務の提供に支障が生じるおそれがあるような場合である。

【役務提供拒否の内容の拡大】

④ 送信者に対し、その回線の利用を停止したり契約を解除したりすることも対象に含まれる。

・一律に拒否できるかは当該支障を防止するために必要な範囲内かどうかの個別具体的な判断が必要。

⑤ メールが遅延等を引き起こす原因となった送信者以外の者に対して役務の提供を拒否することも、円滑な役務の提供に支障を生じるおそれがあれば対象に含まれる。

・ある送信者の大量送信等により電子メールサービスの円滑な提供に支障が生じている場合に、第三者が別に大量送信を行うような場合である。

また、上記以外にも、今後における役務提供拒否の事例を積み重ねていくことで、できる限り電気通信事業者が適切に拒否の是非を判断することができるようにしていくことが重要である。

〔改正後の第十一条〕

（電気通信役務の提供の拒否）

第十一条 電気通信事業者は、一時に多数の架空電子メールアドレスをそのあて先とする電子メールの送信がされた場合において自己の電子メール通信役務の円滑な提供に支障を生ずるおそれがあると認められるとき、その他電子メールの送受信上の支障を防止するため電子メール通信役務の提供を拒むことについて正当な理由があると認められる場合には、当該支障を防止するために必要な範囲内において、当該支障を生じさせるおそれのある電子メールの送信をする者に対し、電子メール通信役務の提供を拒むことができる。

〔改正前の第十条〕

（電気通信役務の提供の拒否）

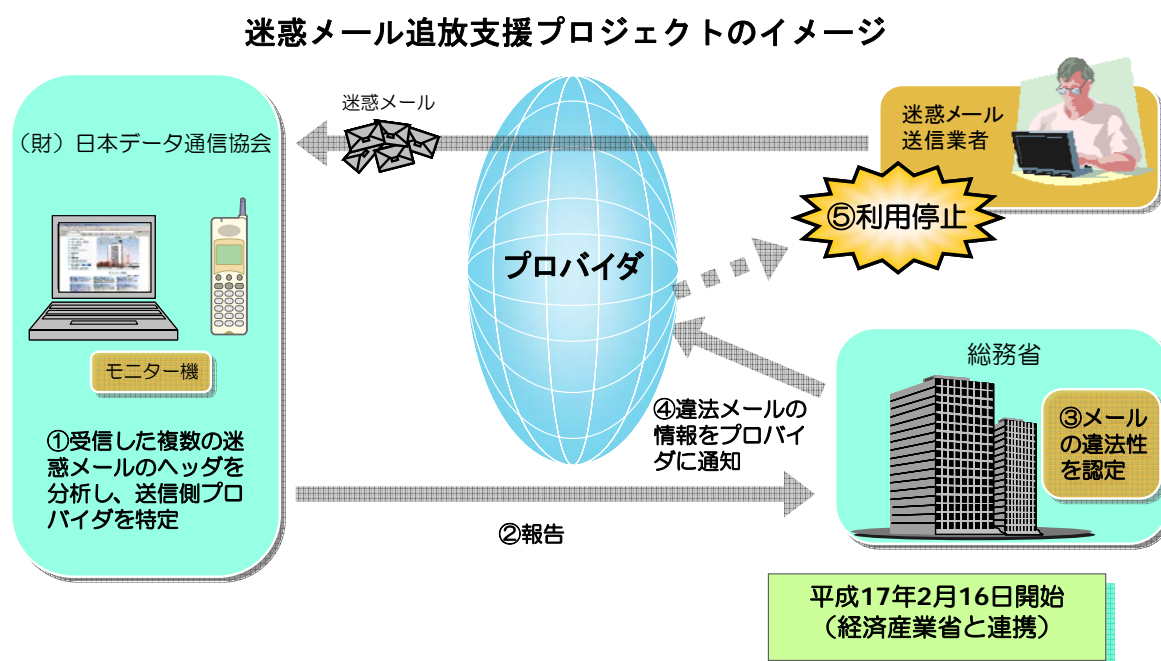
第十条 電気通信事業者（電気通信事業法第二条第五号に規定する電気通信事業者をいう。）は、一時に多数の架空電子メールアドレスをその受信をする者の電子メールアドレスとして電子メールの送信がされた場合において、自己の電気通信設備（同法第二条第二号に規定する電気通信設備をいう。）の機能に著しい障害を生ずることにより電子メールの利用者に対する電気通信役務（同条第三号に規定する電気通信役務をいう。以下この条において同じ。）の提供に著しい支障を生ずるおそれがあると認められるときは、当該架空電子メールアドレスに係る電子メールの送信をした者に対し、その送信をした電子メールにつき、電気通信役務の提供を拒むことができる。

②迷惑メール追放支援プロジェクト

平成15年夏以降、各携帯電話事業者が迷惑メール送信回線の利用停止を積極的に行ったことにより、携帯電話発の迷惑メールが激減したことは前述のとおりであるが、契約約款に基づく「迷惑メール送信回線の利用停止」は、即効性の高い迷惑メール対策の1つであると考えられる。

ISP各社においても、迷惑メール送信回線の利用停止措置が講じられているが、苦情申告の受付体制、事業規模等の違いから、各社間で対応に温度差が見られるのが実状である。

そこで、特定電子メール法を所管する総務省として、(財)データ通信協会に設置したモニター機で受信した迷惑メールの違法性を確認し、当該メールに関する情報を送信元プロバイダに通知することにより、迷惑メール送信回線の利用停止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」を平成17年2月16日から開始した。



具体的には、①(財)日本データ通信協会に設置しているモニター機を利用し、②当該モニター機が受信した同一送信者からのものと考えられる広告・宣伝メールの違法性を総務省が確認し、③携帯電話事業者等から得られるヘッダ情報を分析して送信元プロバイダを特定し、④当該プロバイダに違法メールに関する情報提供を行うことにより、⑤契約約款に基づく措置(利用停止、警告等)を促す、というものであり、特定商取引法を所管する経済産業省と連携して行われている。

本施策は、行政が民間事業者の自主規制の円滑な実施を促進する取組として、その実効性に大きな期待が持たれるところであるが、その具体的な運用方法等については、ISPからのヒアリング等を通じ、随時必要な見直しを検討すべきである。

なお、民間事業者による自主規制については、電気通信事業法の規定（通信の秘密の保護、不当な差別的取扱いの禁止等）との整合性を確保しつつ進める必要があることから、所管の総務省と十分連携しつつ、対策を検討・実施することが不可欠である。

③迷惑メール送信者情報の交換

「迷惑メール送信者情報の交換」については、複数の携帯電話事業者・ISP間を渡り歩いて迷惑メールを送信する行為を防止する上で有効と考えられるが、その実施に当たっては、電気通信事業法（通信の秘密の保護、不当な差別的取扱いの禁止等）並びに「個人情報の保護に関する法律」（個人情報保護法）及び「電気通信事業における個人情報保護に関するガイドライン」の規定との整合性を確保する必要があることから、現在、「電気通信事業分野におけるプライバシー情報に関する懇談会」において、検討が進められている。前述のとおり、迷惑メール対策は、既存法等との整合性を確保しつつ検討・実施する必要があることから、同懇談会における検討結果を踏まえ、可能な対策を講じていくことが期待される。

(3) 技術的解決策

送信ドメイン認証技術

現在の迷惑メールは、発信元をでたらめなメールアドレスとしたり、他人のPC等を踏み台として利用したりするなど適切でない方法で発信されることが多くなっているが、この対応策として、メールの発信元の情報を確認する「送信ドメイン認証技術」が米国を中心に導入されつつあり、我が国でも、平成17年春から一部ISPにおいて導入が始まっている。

この技術は、メールを送信できなくするものではなく、メールを受け取る側での対応に関する技術であり、メールの発信者情報から得られる発信元情報（サーバの情報等）を、受信側で確認できる認証の枠組みである。この技術により、「送信元が追跡・特定可能なメール」と確認できたもののみ受け取るなどの対応が可能となる。

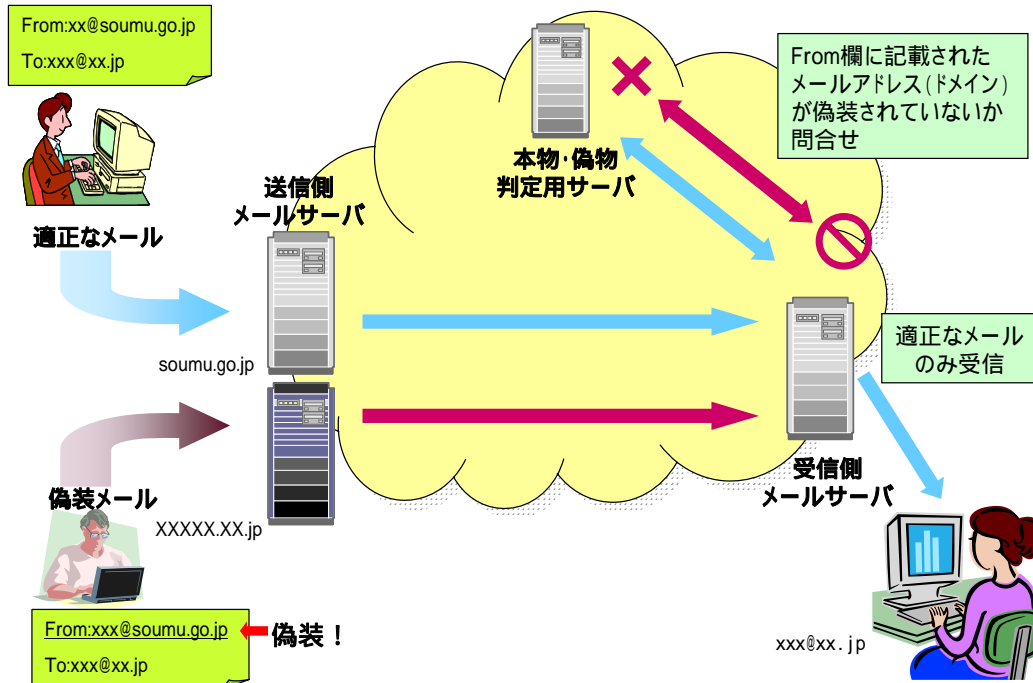
現在、複数種類の送信ドメイン認証技術が提案・実装されているが、主なものとしては、SPF（Sender Policy Framework）/ Sender ID と Domain Keys の2種類がある。前者は、DNS（ドメインネームシステム）サーバにより「メールをインターネットに送信するサーバの情報」を確認する方法であり、米国マイクロソフト社等を中心に検討が進められてきた技術である（次ページ上図）。後者は、DNSサーバを用いて「メール自体の認証」をドメイン単位で行うもので、米国ヤフー社により提唱された技術である（次ページ下図）。これらは、それぞれに独立した技術であり、対立するものではなく、組み合わせで利用することも可能である。

送信ドメイン認証技術は、「送信ドメインが正当なメールサーバから送信されている」ことが確認できる環境の確立を目指すもので、これによってすべてが解決するものではなく、フィルタリングなど他の技術と組み合わせることで効果を発揮することになる。

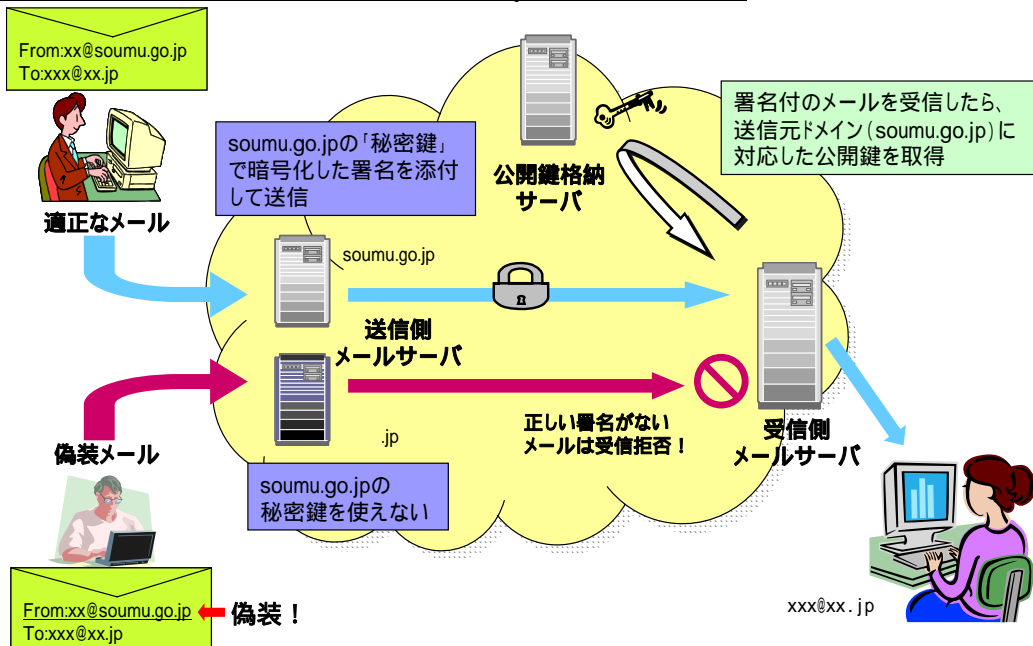
なお、送信ドメイン認証技術には、メーリングリスト利用時や転送の際に認証が失敗する場合があるなど、更なる改善が必要とされている。また、企業等で実際に利用されているメールシステムは多様な形態で利用されているため、メールシステム全体の見直しを要する場合があるなど、有用な導入の手引き等の作成・共有が望まれる。

我が国では、昨今、J E A G (p10 参照) 等の場を通じ、送信ドメイン認証技術の有効性や課題、導入手順等に関する議論が活発化しているが、同技術は単独で実施しても効果が上がらないことから、世界各国における導入状況等も踏まえつつ、他業界との連携も図りながら、業界全体の課題として取組を進めていくことが必要である。

【送信ドメイン認証技術 : S P F /Sender ID のイメージ】



【送信ドメイン認証技術 : Domain Keys のイメージ】

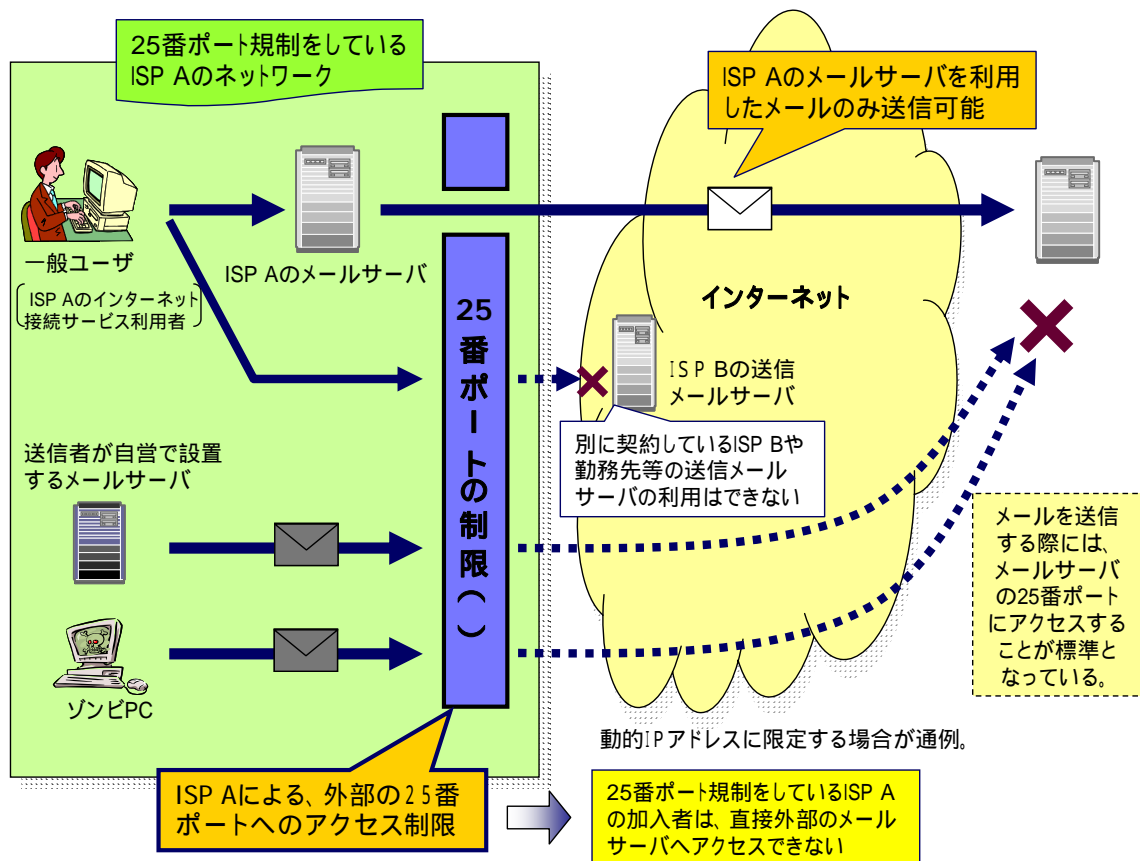


送信ドメイン認証技術以外にも、信頼できる機関において公開されている送信者に関する証明書によって送信者個人の電子署名を検証し、受信側において信頼できる送信者であることを判定できる技術 (S/MIME 等) も効果があると考えられる

その他の新たな技術的解決策

送信ドメイン認証技術のほか、あるISPが提供するメールサーバを経由せず、動的IPアドレス¹を割り当てられた自営で設置するメールサーバ等から直接外部に送信(最近の迷惑メール送信者がよく利用する形態)されるメールを遮断する「25番ポートブロック」や、IPアドレスの信頼度を評価し、その評価に応じてメールをフィルタリングする「レピュテーション」など、新たな技術的解決策が登場し、その有効性や課題、導入手順等について議論が進められており、その進展が期待される。

25番ポートブロックのイメージ



【主な効果】

- ・送信者が自営で設置したサーバからのspamを遮断し、ISPのメールサーバ経由のメールのみを通すことが可能(spam発生の場合の検知が容易)
- ・ゾンビPCのケースにも同様の効果がある

【主な課題】

- ・2次ISP(上位ISPから回線の提供を受けてサービスを提供している下位ISP)への対応が困難
- ・サブミッションポート(25番ポートの代替として使われるメール送信用ポート)への誘導を行うにしても、ISP及びユーザにおける費用負担・設定変更等が必要
- ・メールサーバを自営で設置して運用しているユーザの利用が制限される場合がある

¹ 一定時間ごとに変更されるなど1つに固定されていないIPアドレス。通常のインターネット接続サービスは動的IPアドレスを割り振る形態となっている。

フィルタリング

他方、受信者側で迷惑メールをブロック等する「フィルタリング」も、昨今、高機能化・普及が進んでおり、より精度が高く、効果的なフィルタリングソフト・サービスが開発・提供されることが強く期待される。

主要ISPによる最近の迷惑メールフィルタリングサービス

事業者	概要
ニフティ	ベイズ理論を応用し、迷惑メールを振り分ける際にメールの特徴を覚え、以後に送られてくる同様の迷惑メールに対して、自動的に迷惑メールと判断し、迷惑メールフォルダに自動振り分けする「学習型フィルター」機能を会員向けに提供（平成16年1月～）
IIJ	ベイジアンフィルタやヒューリスティックフィルタなど複数のフィルタリングエンジンからなる解析エンジンにより迷惑メールの解析を行うことにより「迷惑メール度」として点数化し、受信者が点数に従って振り分けることを可能とするサービス（平成16年10月～）
NEC (BIGLOBE)	全世界120万人のモニターから収集した情報をもとに、メールのヘッダを解析して迷惑メールかどうかを判定し、迷惑メールの場合、件名に「spam」と表示させるサービス（平成17年3月から試行サービス開始、5月から本格サービス開始）
ぷらら	Bフレッツ、ADSL回線の利用者宛の迷惑メールを、サーバ側で学習型フィルタによって自動的に判定し、迷惑メールと判定されたメールは専用のフォルダ（ジャンクボックス）に振り分けるサービス（平成17年4月（ADSLは5月から）から試行サービス開始）
NTTコミュニケーションズ (OCN)	全世界120万人のモニターから収集した情報をもとに、メールのヘッダを解析して迷惑メールかどうかを判定し、迷惑メールの場合、件名に「SPAM!!」又は「MEIWAKU!!」と表示させるサービス（平成17年6月、ビジネス利用者からサービス開始）

なお、これまでに紹介してきたISPによる送信ドメイン認証の採用、25番ポートブロック、フィルタリングサービスなどの提供に当たっては、利用者の適切な同意を得るなど、電気通信事業法の規定（通信の秘密の保護、不当な差別的取扱いの禁止等）との整合性を確保しつつ進める必要があることから、同法を所管する総務省と十分連携して進めることが不可欠である。

(4) 利用者支援

利用者側で可能な対策の重要性

迷惑メール対策としては、行政による法執行や電気通信事業者による自主規制により迷惑メールが送信されにくい環境を整えるほか、電子メールの利用者の側において送信された迷惑メールの受信を回避するための対策を講じることが重要である。

現在、携帯電話サービスでもドメイン指定受信機能等のフィルタリングサービスが提供され、PCではISPにより提供されるフィルタリングサービスのほか、利用者がPCに導入するセキュリティ対策ソフトウェアに迷惑メール対策機能が含まれたりするなど、相当程度の対策を講じることが可能となっている。

(参考) 電気通信事業者が、利用者に対し迷惑メールの受信を回避するために提供しているフィルタリングサービスの例

携帯電話事業者が提供しているもの	ISPが提供しているもの
<ul style="list-style-type: none">・「未承諾広告」フィルタリングサービス・アドレス(ドメイン)指定受信・拒否機能・携帯発になりすましたPC発メールを拒否する機能・選択受信機能(送信者と件名のみ先に受信可能)・本文に URL リンクを含むメールの受信を拒否する機能	<ul style="list-style-type: none">・「未承諾広告」フィルタリングサービス・複数のキーワード(from アドレス、宛先、件名、メール容量等)によるフィルタリング機能・迷惑メールのパターンを学習・解析し、迷惑メールと判断したメールを自動的に分類する機能(ベイジアンフィルタ)

利用者への周知方法等の工夫の必要性

しかしながら、フィルタリングには特定の文字列にのみ反応する単純なものから、巧妙な迷惑メールを必要なメールと区別するために高度で複雑な設定が要求されるものまで多岐にわたっており、利用者にとって「どの対策を講じればどのような効果がどの程度期待できるのか」がわかりにくくなっているのも事実である。

また、現在の携帯電話はほぼ全てメールの機能を有しており、PCでのメール利用とあわせると非常に高い普及率となっており、メールの送受信の仕組みを理解している層のみが利用しているわけではなく、子供や中高年層を含めて広く利用されている状況にあり、対策の周知にあたっては、実際の利用者にとってその内容が理解されるようにすることが必要と考えられる。

利用者の意識改革の必要性

また、電子メールを利用するにあたり、一方的に迷惑なメールが送信される場合があること、原則として電気通信事業者はメールの内容に関知できず、送信者から送られたものがそのまま届いているに過ぎないといった通信の特質があることを理解した上で、電子メールを利用するに際しての基本的なルールを踏まえて利用することが重要である。

なお、利用者が前もって踏まえておくことが望ましい事項として、(財)インターネット協会がインターネットの利用方法を含めた電子メール利用一般に関するマナーを作成している¹ほか、セキュリティ対策を行うシマンテック社においても一般利用者に向けてスパム被害に合わないためのヒント集²を作成している。

迷惑メール対策として可能な事項を把握する必要性

なお、利用者への周知を行うに当たっては、迷惑メール対策におけるそれぞれの果たせる役割を踏まえて行うことが適当と考えられる。

たとえば、電気通信事業者は、メールの送信者と受信者の間で通信の媒介等を行う者であり、その取扱中の通信の秘密は侵されてはならず(電気通信事業法第4条)、通信当事者である送信者と受信者の間の通信の秘密を、電気通信事業者が通信当事者の同意無く知得等することは原則として許されない³。

そのため、送信されるメールの内容に応じて受信回避等をするために電気通信事業者が果たすことのできる役割としては、受信者が自ら回避する対策を講

¹ 「インターネットにおけるルール&マナー公式テキスト」において、以下のような内容を紹介している。

- ・一方的に送りつけられる広告メールや勧誘メールは無視する
- ・身に覚えのないインターネット利用料などを請求するメールが届いた場合、払う必要はないこと
- ・不快なメールに返信する必要がある場合は、すぐに返事を出さず、じっくり考え直してから出すこと
- ・メールによる嫌がらせを受けた場合、自分だけで対処せず家族や友人と相談して対策を考えること
- ・掲示板などにメールアドレスを公開すると迷惑メールが増える原因になること

² 「スパムメール対策 10 のヒント」として、以下のような内容を紹介している。

- ・疑わしいメールに返信しないこと
- ・登録の覚えがないメール等を受け取った場合、配信停止申し込み用のリンクをクリックしないこと
- ・クレジット・カード情報やほかの個人情報を、安全でない Web サイトで入力しないこと
- ・安全な Web サイトでも、入力する前にプライバシー保護に関する記述を確認すること
- ・チャットルーム、インスタントメッセージ、掲示板等で自分のメールアドレスを送信・公開しないこと
- ・メールアドレスを推測されにくいものにする

³ そのため、迷惑メールが送信されてきた場合にも、その送信者の契約者情報などを電気通信事業者が受信者に提供することはできない。また、通信当事者の同意無く「迷惑な」内容のメールを送信されないように措置することも、個別の通信の内容を電気通信事業者が確認しなければならないためにとることができない。

じるためのバックアップを行うことが基本となると考えられる。

具体的な利用者側での対策の促進策

利用者の支援については、以上のことを踏まえ、法執行の主体として送信者の摘発等の取締りを行う政府、送信者に対する利用停止等の措置を行う電気通信事業者が、消費者団体等と協力して利用者が自ら対策を講じることのできるよう継続的に取り組んでいくことが必要と考えられる。具体的な促進策としては、以下のようなものが考えられる。

1. フィルタリングサービスの活用

フィルタリングは、利用者における迷惑メール対策として有効と考えられるが、その設定方法等を十分に理解していない、機能が複雑である等の理由から、十分に活用されていない場合もある。

そこで、たとえば、電気通信事業者がフィルタリングサービスを提供するに当たっては、同意⁴の取得方法を含め、未成年者・高齢者といった利用者の特性に応じたきめ細やかな対応を行うことなどが望まれる。

2. 電気通信事業者と消費者団体等の連携による周知

効果的な周知を行うためには、メールの仕組み等の技術的な内容をわかりやすく伝達する必要があるが、一般利用者にわかりやすいよう簡易な表現にすると技術的な正確性が損なわれ、不正確な表現になるおそれがあることから、利用者支援活動を行う消費者団体等と電気通信事業者等の連携を図ることが重要である。

たとえば、消費者団体や電気通信事業者団体等が連携し、一般利用者や、実際に利用者と接する相談員等に対し、電子メールの基本的な仕組みやフィルタリングの設定方法などに関するアドバイスを行う講習会等を開催することなどが考えられる。

⁴ フィルタリングサービスの提供に当たっては、利用者の意思が反映されないまま電気通信事業者がメールの配信を拒むことのないよう、利用者の適切な同意を得ることが必要である。

(5) 国際協調

政府間の国際協調

総務省は、平成 17 年 4 月下旬、アジア太平洋地域の 11 機関との間で、「スパム対策の協力に関する多国間 M o U (覚書)」に合意した。前述のとおり、中国及び韓国は世界の中でも米国に次ぐ迷惑メールの発信国となっていること、また我が国においても中国や韓国からの迷惑メールが届いていること等を踏まえ、今後、アジア地域の国々との一層の協調が必要と考えられる。

「スパム対策の協力に関する多国間 M o U (覚書)」の概要

締結機関

豪通信庁 (ACA)、韓国情報セキュリティ庁 (KISA)、中国インターネットソサエティ等、アジア太平洋諸国 10 カ国 / 地域から 12 機関が創立メンバーとして参加

日本で初めて締結されたスパム対策 M O U (日本からは、総務省及び経済産業省が参加)

目的

- ・締結国から発信されるスパム、及び締結国民が受信するスパムをできる限り減少させる
- ・締結国の法令に準拠し、相互利益に資する範囲で、スパムに関する緊密な協力と情報の交換を推進する

協力範囲

- ・反スパム規制の確立と執行のための政策と戦略に関する情報の交換
- ・スパム問題に対する技術的、教育的解決策に関する情報の交換
- ・規制政策の効果的利用と執行のサポートに関する戦略と情報の交換
- ・他国 / 地域に関する情報の交換
- ・協力形態としては、情報交換チャネルの確立、相互派遣・訪問、産業界と政府との連携の奨励、をとる

その他

- ・協力に関して責任を負う代表者を指名する
- ・その他、国内法や国際的取り決めの範囲内で活動を行う旨、法改正を行った場合の連絡、秘密情報の取扱い、紛争の解決、協力期間 (原則 5 年間) 等について規定

「スパム対策の協力に関する多国間 M o U (覚書)」調印機関

国名・地域	機関名
日本	総務省 (MIC) 経済産業省 (METI)
オーストラリア	通信庁 (ACA)
韓国	情報セキュリティ庁 (KISA)
中国	インターネットソサエティ (ISC)
香港	貿易工業情報科学技術局 (CITB)
台湾	コンピュータ危機応答チーム / コーディネーションセンター (TAIWAN-CERT)
フィリピン	国家コンピュータセンター (NCC) コンピュータ危機応答チーム (PH-CERT)
マレーシア	通信マルチメディア委員会 (MCMC)
タイ王国	情報通信技術省 (MICT)
ニュージーランド	経済開発省 (MED)

他方、世界最大級の迷惑メール送信国である米国をはじめとする欧米諸国との一層の連携強化も必要と考えられる。

迷惑メールは低コストで国境を越えて送信することが可能なため、送信者は、技術的規制などにより送信が困難になった場合には、まだ対策が不十分な国からの送信に切り替えることが予想される。

このため、諸外国との情報交換を積極的に行い、新たな迷惑メール対策について迅速に国内での導入を検討することが必要であるほか、(インターネットの普及に比べ)迷惑メール対策が遅れている国に対しては、効果的な対策や技術開発動向を情報提供するなどして、迷惑メール送信者に狙われないように支援することも効果的と考えられる。

国際連携の推進に関する最近の動き

平成16年12月8日	<u>日仏定期協議</u> 仏のスパムの85%が英語、7%が仏語。 平成16年6月に反スパム規定を含むデジタル経済法が成立。
平成17年2月10日	<u>日伊定期協議</u> 伊では、携帯あてのスパム(ただしSMS)が最近増加。 フィルタリングは通信の秘密との関係で認められてない。
2月24日	<u>「国際的反スパム協力に関する共同声明」</u> (ASEM第4回電子商取引に関する会合(ロンドン)) 欧州25ヶ国、アジア13ヶ国の計38ヶ国が反スパム対策に共同で取り組むことに合意。
3月9日	<u>OECDスパムタスクフォース第2回会合</u> 「アンチスパム・ツールキット」関係資料(各国の規制、国際協力に関する取組、民間事業者の自主規制等)について議論。
4月下旬	<u>「スパム対策の協力に関する多国間MOU」合意</u> 豪・韓MOU(2003年10月)をアジア10か国/地域12機関に拡大して締結。 規制・執行や技術的解決策等に関する情報交換、相互訪問等を盛り込む。
5月3~4日	<u>ASEAN通信規制庁アンチスパムワークショップ</u> アジア地域における国際連携の重要性を確認。

民間における国際協調

迷惑メール対策に関する国際協調は、政府のみならず、民間部門においても重要である。この点、(財)インターネット協会は、オーストラリアのインターネット産業協会(IIA)とMOUを締結する方向で検討を進めている。また、世界各国の運用技術者から成るMAAWG¹において、技術的な迷惑メール対策が議論されており、我が国からもIIJが参加している。

今後とも、国際的な迷惑メール対策を推進するに当たり、官民がそれぞれのレベル、論点で議論を重ねるとともに、官民相互の連携を一層緊密にすることが求められる。

¹ Messaging Anti-Abuse Working Group。 2003年12月発足。

4．最後に

迷惑メール対策の方向性について 5 つの論点を掲げて示してきたが、迷惑メールの問題は送信手法の変化等の動きが激しく、これらの対策は、いずれも対策を講じてそれで足りるというものではなく、今後とも不断の見直しが必要となるものである。

これは、新たな迷惑メールの送信手法が登場することにより、それまでの法制度や電気通信事業者及び利用者が実施している対策の有効性が損なわれ、電子メールの利用環境が悪化することが考えられるためである。

法制度については、平成 17 年 5 月に成立した「特定電子メールの送信の適正化等に関する法律の一部を改正する法律」の附則において、施行後 3 年以内の見直しを行う旨が規定されており、今回の改正にとどまらず、法制度の見直しを今後も継続的に行っていく方針が示されている¹。

なお、迷惑メールの送信手法の変化は 3 年経過を待たずに急激に起きる場合も想定されるため、弾力的な対応をとることが求められる。

電気通信事業者による自主規制や、技術的解決策、利用者の周知啓発、国際協調といった対策についても、新たな迷惑メールの送信手法に対応するための見直しが不可欠である。

総合的な迷惑メール対策の効果的な実施及び適切な見直しに向けては、それぞれの対策を実施する主体の相互連携が必要である。政府内での省庁間連携をはじめ、諸外国政府との国際連携、民間における国内外の連携や官民間の連携を積極的に進めていく必要があると考えられる。

¹ 政府は、この法律の施行後 3 年以内に、電気通信に係る技術の水準その他の事情を勘案しつつ、この法律の施行の状況について検討を加え、その結果に基づいて必要な措置を講ずるものとする(附則第 7 条)。

「迷惑メールへの対応の在り方に関する研究会」開催要綱

1 目的

携帯電話等を中心とした、受信者の同意を得ず一方的に送信される広告・宣伝目的の電子メール（いわゆる迷惑メール）について、近年における送信行為の巧妙化・悪質化等を踏まえ、各国で行われている法整備等との国際的な整合性に配慮しつつ、「特定電子メールの送信の適正化等に関する法律」（平成 14 年法律第 26 号）に基づく取締り及び電気通信事業者における受信回避のための取組等に関し、迷惑メール流通の抑制・防止のために必要な対応方策について幅広く検討を行うことを目的とする。

2 名称

本会は、「迷惑メールへの対応の在り方に関する研究会」と称する。

3 検討事項

- (1) 法施行後の迷惑メールの状況の変化
- (2) 諸外国の法制度の整備等の状況
- (3) 法制度の在り方、電気通信事業者の取組の在り方、利用者への周知啓発等の対応方策の検討

4 構成及び運営

- (1) 本会は、総務省総合通信基盤局長の研究会として開催する。
- (2) 本会の構成員は、別紙のとおりとする。
- (3) 本会には、座長及び座長代理を置く。
- (4) 座長は、研究会構成員の互選により定めることとし、座長代理は座長が指名する。
- (5) 座長代理は、座長を補佐し、座長不在のときは、座長に代わって本会を招集し、主宰する。
- (6) 本会は、必要があるときは、外部の関係者の出席を求め、意見を聞くことができる。
- (7) その他、本会の運営に必要な事項は、座長が定めるところによる。

5 本会の開催期間

本会の開催期間は、平成 16 年 10 月から平成 17 年 3 月末を目途とする。

6 庶務

本会の庶務は、総務省総合通信基盤局電気通信事業部消費者行政課がこれを行うものとする。

「迷惑メールへの対応の在り方に関する研究会」構成員

(敬称略、五十音順)

座長	新 美 育 文	明治大学 法学部教授
座長代理	松 本 恒 雄	一橋大学大学院 法学研究科教授
	五十嵐 善 夫	ボーダフォン(株) 法務・渉外本部 常務執行役 法務・渉外本部長
	岡 村 久 道	弁護士
	加 藤 雄 一	ニフティ(株)常務取締役インターネットビジネス本部長
	岸 原 孝 昌	モバイル・コンテンツ・フォーラム 事務局長
	桑 子 博 行	(社)テレコムサービス協会 サービス倫理委員会委員長
	西 郷 英 敏	NTTコミュニケーションズ(株)ブロードバンドIP事業部 事業部長
	佐 伯 仁 志	東京大学大学院 法学政治学研究科教授
	高 橋 徹	(財)インターネット協会 副理事長
	長 田 三 紀	東京都地域婦人団体連盟 事務局次長
	奈 良 谷 弘	KDDI(株) マーケティング本部長
	野 口 尚 志	(社)日本インターネットプロバイダー協会 理事 行政法律部会 副部会長
	比 留 川 実	(社)電気通信事業者協会 専務理事
	別 所 直 哉	ヤフー(株) 法務部長
	三 膳 孝 通	(株)インターネットイニシアティブ 取締役戦略企画部長
	山 川 隆	(株)NTTドコモ モバイル社会研究所 副所長
	好 光 陽 子	国民生活センター相談調査部調査役
(オブザーバ)	児 島 久 和	(財)日本データ通信協会 迷惑メール相談センター 所長

「迷惑メールへの対応の在り方に関する研究会」審議経過

会合	開催日	議題
第1回	平成16年10月7日	<ul style="list-style-type: none"> ・迷惑メール対策の現状について ・迷惑メール対策に係る対応方策の検討について（論点整理）
第2回	平成16年10月22日	<ul style="list-style-type: none"> ・構成員からの発表 KDDI株式会社、ニフティ株式会社 ・検討の範囲について ・法制度に係る検討事項について（個別論点に係る検討）
第3回	平成16年11月10日	<ul style="list-style-type: none"> ・中間とりまとめ素案について
	平成16年11月15日 ～平成16年12月10日	<ul style="list-style-type: none"> ・中間とりまとめ案についてのパブリックコメント募集
第4回	平成16年12月20日	<ul style="list-style-type: none"> ・中間とりまとめ案について
第5回	平成17年2月9日	<ul style="list-style-type: none"> ・携帯電話事業者による最近の迷惑メール対策について ・「迷惑メール追放支援プロジェクト」について ・「国際的スパム執行協力に関するロンドン行動計画」について ・「フィッシング対策推進連絡会」について ・構成員からの発表 (株)インターネットイニシアティブ
第6回	平成17年4月6日	<ul style="list-style-type: none"> ・「特定電子メールの送信の適正化等に関する法律の一部を改正する法律案」について ・ISP等による迷惑メール対策について ・国際連携の推進状況等について ・構成員からの発表 (社)日本インターネットプロバイダー協会 (株)インターネットイニシアティブ
第7回	平成17年5月26日	<ul style="list-style-type: none"> ・構成員からの発表 (財)インターネット協会、東京都地域婦人団体連盟 ・国際連携の推進状況について ・最終報告書骨子(案)について
第8回	平成17年6月15日	<ul style="list-style-type: none"> ・最終報告書素案について
	平成17年6月17日 ～平成17年7月8日	<ul style="list-style-type: none"> ・最終報告書案についてのパブリックコメント募集
第9回	平成17年7月15日	<ul style="list-style-type: none"> ・最終報告書案について