

迷惑メールへの対応の在り方に関する研究会
中間とりまとめ（案）

平成 1 9 年 1 2 月

迷惑メールへの対応の
在り方に関する研究会

目 次

はじめに.....	1
1. 迷惑メール対策の経緯と現状.....	3
(1) これまでの迷惑メール対策への取組.....	3
(2) 最近の迷惑メールの状況.....	13
2. 諸外国の状況.....	21
(1) 最近の迷惑メールの状況.....	21
(2) 各国の規制の動向.....	22
3. 迷惑メール対策の検討の方向性.....	29
(1) 総合的な対応の必要性和法の果たす役割.....	29
(2) 法制度見直しの必要性.....	30
(3) 法制度見直しの視点.....	31
4. 法制度の見直しの在り方.....	32
(1) 巧妙化・悪質化する迷惑メールへの対応の強化.....	32
(2) 現行のオプトアウト方式の見直し.....	39
(3) 法の実効性の強化.....	45
(4) 国際的整合性・連携の強化.....	47
(5) 法制度の見直しに関する評価.....	48
5. 今後の検討事項.....	49

はじめに

我が国において、インターネットは、利用者が平成18年に8,754万人に達するなど社会経済その他あらゆる活動に不可欠な基盤となっている。その中でも、電子メールは、基礎的なコミュニケーションツールとして、社会経済活動や市民生活において必要不可欠な連絡・伝達的手段となっている。若年層をはじめ電子メールのない生活はもはや考えられないという人も多いだろう。

電子メールの利用が飛躍的に増大する一方、これに比例して、受信者の同意を得ず一方的に送信される広告・宣伝等のメール(いわゆる迷惑メール)も依然増加している。現在、全世界的にみても、また、我が国においても、流通する電子メールの7割以上が迷惑メールと推定されており、迷惑メールによる利用者の送受信上の支障や、電子メールサービスを提供する事業者の設備等への負荷は多大なものとなっている。

我が国では、携帯電話宛ての迷惑メールが社会問題化したのを契機に、平成14年、世界的にも先駆的な立法として「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。)が制定された。また、平成17年には同法の改正が行われ、対応が強化された。こうした法整備や電子メールサービスを提供する事業者等による積極的な取組により、我が国における迷惑メール対策は一定の成果を収めている。

しかしながら、現実の世界と比べ、極めて変化の早いインターネットの世界において、迷惑メールは一層の巧妙化・悪質化が進んでおり、最近では、フィッシングメール等のメールも流通するようになっている。我が国における高速・低廉なブロードバンドの急速な発展は、インターネット利用者にとって大きなメリットである一方、迷惑メールの送信者にとっても、迷惑メールの送信を行いやすい環境になっていることも意味する。さらに、外国発の迷惑メールの増加や、諸外国における法整備の進展など、平成14年の特定電子メール法制定時とは事情が変わってきた点もある。

平成17年改正の特定電子メール法附則第7条では、政府は施行後3年以内に法の施行状況について検討を加え、その結果に基づき必要な措置を講ずる旨規定している。こうした点も背景に、迷惑メール対策全般の検討を行う「迷惑メールへの対応の在り方に関する研究会」が平成19年7月より開催され、このたび、特に現行法制の見直しを中心に、中間とりまとめを行うこととした。

迷惑メール対策に特效薬はないが、法制度は取組全般の基盤となるものであり、本中間とりまとめを踏まえ、政府が法制度の見直しを行い、迷惑メール対策を着実に進展させていくことを期待する。

1. 迷惑メール対策の経緯と現状

(1) これまでの迷惑メール対策への取組

特定電子メール法制定及び改正の経緯

迷惑メール問題の発生と特定電子メール法の成立

我が国では、90年代後半から、電子メールの利用が、携帯電話での幅広い利用も含め、急速に普及したが、21世紀に入った平成13年(2001年)春頃から、受信者の同意を得ず一方的に送信される広告・宣伝目的のメールが、携帯電話での利用を中心に大きな問題となった。

このため、総務省において、平成13年11月より、「迷惑メールへの対応の在り方に関する研究会」(第1次研究会)が開催され、迷惑メールの現状の把握、迷惑メール流通の抑制・防止のための方策の検討が行われ、平成14年1月、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まとめられた。

こうした状況の下、平成14年4月、議員立法により特定電子メール法が成立し、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)の内容

受信者にとって、望まない広告・宣伝メールの受信は、(携帯電話等で)それに対し課金が行われる場合もあり、また、受信と削除に時間と手間がかかる、内容が不快など、電子メールの利用に不便が生じ、私的生活領域の侵害にもつながる。

また、電子メールサービスを提供する事業者側では、メールサーバ等の電気通信設備へ負荷が生じることで電子メールの送受信の処理に支障が生じる等、一時に多数の受信者に宛てた大量の広告・宣伝メール等が送信されることにより、電子メールの送受信の処理に支障が生じることとなる。

このような送受信上の支障を防止する必要があることにかんがみ、広告・宣伝メールの送信の適正化の措置等を定めることにより、電子メールの利用についての良好な環境の整備を図り、もって高度情報通信社会の健全な発展に寄与することを目的として制定されたのが特定電子メール法であり、具体的には以下の規律が設けられた。

第一に、同一の送信者から繰り返し、同意のない自己又は他人の営業につ

¹ また、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、同時期に国会で成立し、特定電子メール法と同日に施行された。

き広告又は宣伝の手段としての電子メール（以下、「特定電子メール」という。）を受信し続けることになることを避けるため、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が禁止された（いわゆる「オプトアウト」方式）²。

また、その前提として、受信者が特定電子メールであることを容易に認識できるよう「未承諾広告」を表示することなどの表示義務が課された。

第二に、自動生成プログラムを用いて作成された架空アドレスを含む多数のアドレスにあてて送信が行われた場合には、電気通信設備に過度の負荷が生じるため、架空電子メールアドレス宛の電子メールの送信が禁止された。

第三に、電気通信事業者に対し、電子メールの送受信上の支障を防止する目的の範囲内で、一時に多数の架空電子メールアドレス宛てに電子メールが送信された場合、その電気通信役務を拒否することができることとされた。

その他、送信者が違反行為を行った場合の総務大臣の措置命令や、措置命令に従わない場合の罰金（50万円以下）の規定等についても整備された。

なお、特定電子メール法制定時においても、法の施行後、継続的に法執行の状況等の見直しを図る必要があることが認識されており、附則において、政府は施行後3年以内に法の施行状況について検討を加え、その結果に基づき必要な措置を講ずる旨が規定された。

（図 1：特定電子メールの送信の適正化等に関する法律（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

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）

² これに対して、あらかじめ受信を承諾している者に対して送信を認めるのがオプトイン方式である。英語の opt は「選ぶ、決める」の意であり、opt - in は（活動などに）加入を決める、opt - out は（活動などに）不参加を決める、が本来の意味である。

【参考：電子メールと他の通信手段の違い】

電子メールサービスは、従来の郵便や電話といった通信手段と比べると、送信コストが非常に小さいこと、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、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えることができる。

【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事ができないが、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。

(出典：迷惑メールへの対応の在り方に関する研究会 平成17年7月最終報告書)

特定電子メール法の平成17年改正

特定電子メール法の制定後、携帯電話事業者に寄せられる迷惑メールに関する苦情が相当数減少するなど、特定電子メール法の制定は携帯電話あての迷惑メール対策に一定の効果があったと考えられる。

しかしながら、送信者の情報を意図的に受信者に分からないようにしたメールの送信や、空メールや友人を装ったメールの送信など、送信手法が巧妙化・悪質化といった状況も生じた。このため、平成16年10月から「迷惑メールへの対応の在り方に関する研究会」(第2次研究会)が開催され、迷惑メールへの総合的な対応方策が検討された。

この研究会の中間とりまとめを踏まえ、内閣提出法案として特定電子メール法の改正法案が国会に提出され、平成17年5月に可決・成立、同年11月から施行された。この平成17年改正のポイントは以下のとおりである。

) 送信者情報を偽った送信の禁止及び直罰規定の整備

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の取締りを困難にしているものがあるため、送信者情報を偽って送信することが禁止された。さらに、送信者情報の偽装は、基本的なコミュニケーションの手段としての電子メールに対する社会的信頼を損なう悪質なものであることから、刑事罰の対象とされた。

) 架空アドレスあての送信を禁止する範囲の拡大及び罰則の見直し

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を問わず禁止された。これにより、自動アドレス生成ソフトを用いて、実在のアドレスの確認を行う場合などに、空メールや友人を装ったメールを送信する行為も規制対象に含まれることとなった。

また、上記行為への措置命令の違反者に対する罰則が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られた。

) 特定電子メールの範囲の拡大

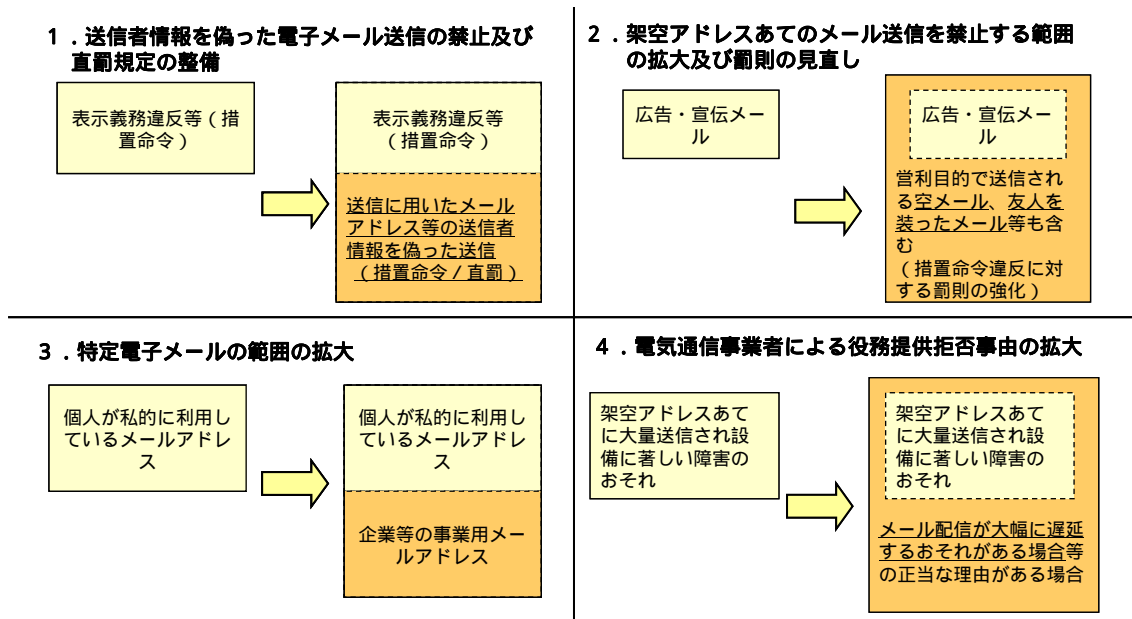
迷惑メールの送信者は、無差別に広告・宣伝メールを送信するため、個人が私的に利用しているメールアドレスのみでなく、企業や事業を営む個人が利用している事業用のメールアドレスに対しても、迷惑メールが送信される。このため、企業や事業を営む個人が利用している事業用のメールアドレスあての電子メールにも規制対象が拡大された。

）電気通信事業者による役務提供拒否事由の拡大

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するなどして自己の設備に著しい障害が発生し役務提供に著しい支障が生じるおそれがある場合のみが規定されていた。改正法では、メール送信が大幅に遅延する可能性があるような場合、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使用が生じるおそれがある場合、その他電子メールの送受信上の支障を防止するため正当な理由があると認められる場合には役務提供を拒否できるとして拒否事由が拡大された。

なお、この平成17年改正においても、法の施行後、継続的に法執行の状況等の見直しを図る必要があることが認識され、附則において、政府は施行後3年以内に法の施行状況について検討を加え、その結果に基づき必要な措置を講ずる旨が規定された。

(図 2 : 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)



平成17年法改正以降の取組

警察による摘発

平成17年法改正により、送信者情報を偽った電子メールの送信が禁止され、これについて直罰規定が設けられたことから、平成18年5月、複数の他人名義や架空のアドレスを使って出会い系サイトの広告メールを送信した疑いで、千葉県警が東京都内の男性会社員を逮捕（裁判の結果、懲役8ヶ月、執行猶予3年の判決が確定）するなど、特定電子メール法第6条違反事件の検挙が行われているが、その件数はこれまでに3件に留まっており、法執行の実効性を高めることが課題となっている。

（図3：警察による摘発状況）

平成18年5月25日	千葉県警が、特定電子メール法第6条に違反した東京都内の男性を逮捕。懲役8月、執行猶予3年が確定。 法人については、罰金80万円が確定。
平成18年8月3日	大阪府警が、特定電子メール法第6条に違反した大阪市内の元会社社長等3名を書類送検。 元社長に罰金100万円、従業員1名に罰金50万が確定。
平成19年1月16日	千葉県警が、特定電子メール法第6条に違反した東京都内の会社社長等4名を逮捕。 2名に懲役8月執行猶予4年。1名に懲役6月、執行猶予5年、 1名に懲役6月、執行猶予3年が確定。

警告メールの送信

また、受信者から、特定電子メール法の登録送信適正化機関である財団法人日本データ通信協会の迷惑メール相談センターに情報提供がなされた電子メールについて、総務省において違法性が確認された場合、総務省が迷惑メールの送信元の電子メールアドレスあてに警告メールを送信しており、平成17年11月の改正法施行後、平成19年9月末までに1,359件の警告メールを送信している。

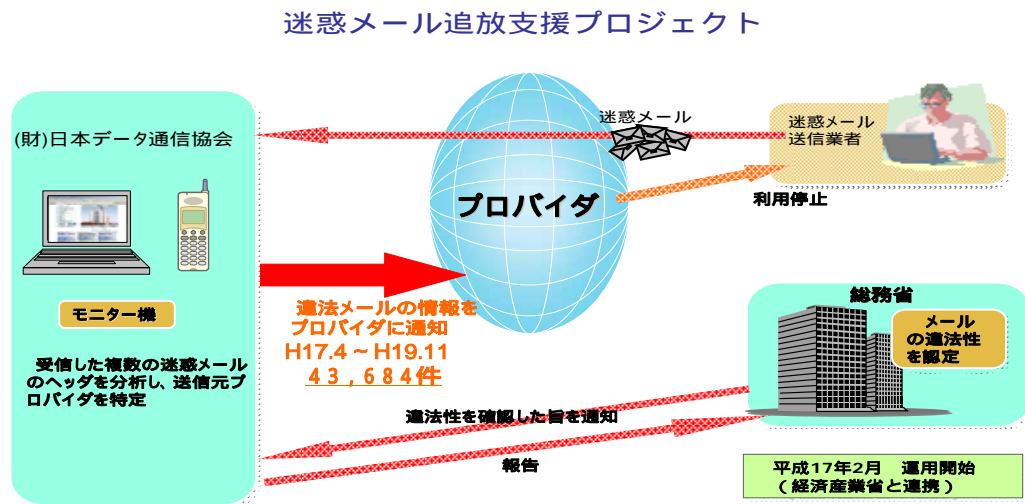
迷惑メール追放支援プロジェクト

平成17年2月より運用が開始された迷惑メール追放支援プロジェクトでは、経済産業省とも連携しつつ、（ ）迷惑メール相談センターに設置しているモニター機を利用し、（ ）当該モニター機が受信した広告・宣伝メール及び一般から寄せられた情報に基づいて迷惑メールの違法性を総務省が確認し、（ ）当該迷惑メールのヘッダ（経路）情報を分析して送信元の電気通信事業者（プロバイダ）を特定し、（ ）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、（ ）契約約款に基づく措置（利用停止、警告

等)を促している。

このプロジェクトに基づき、平成19年11月末までに43,684件の違法メールに関する情報がプロバイダに対して通知され、プロバイダが必要な対応をとっている。

(図4: 迷惑メール追放支援プロジェクトの概要)



電気通信事業者等の取組

電気通信事業者等における取組としては、大量送信の制限や約款に基づく措置、ドメイン指定受信機能やフィルタリングサービスの提供等に加え、迷惑メールの送信の抑止に効果を発揮する Outbound Port 25 Blocking(OP25B)³の導入が進められた。総務省における法的な整理を踏まえ⁴、現在、日本の大手ISPにおいては、概ねOP25Bが導入され、導入したISPにおいて迷惑メール送信の減少に大きな成果を上げている。また、送信ドメイン認証の導入も開始され、迷惑メールに多くみられる送信ドメインを偽った電子メールを技術的に判別することが可能となりつつある。これらの技術的な対策は、迷惑メール対策では有効なものであり、一層の普及が期待される。

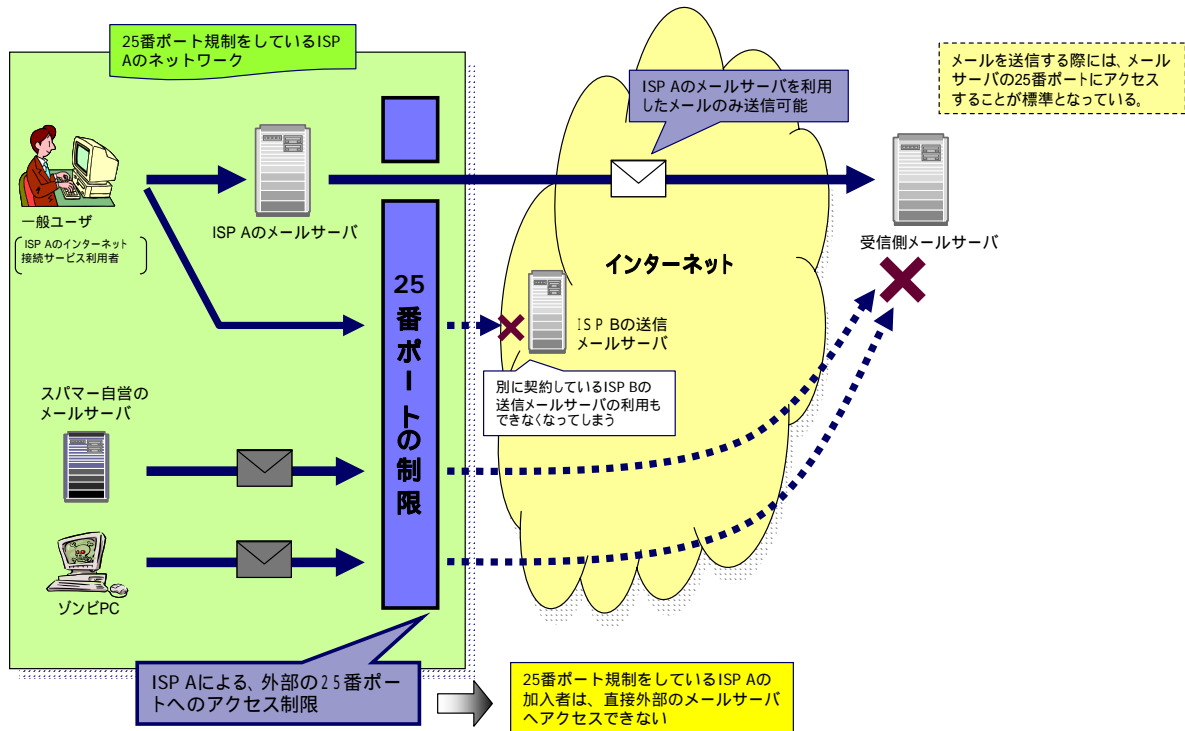
さらに、個別の事業者による取組に加え、平成17年3月に設立されたJEAG(Japan Email Anti-Abuse Group)において技術的な見地から迷惑メール対策の検討が進められている。また、社団法人インターネットプロバイダー

³ OP25Bとは、ISPが、その支配・管理するルータを通過するすべての電子メールの送信元(及びあて先)のIPアドレス及びポート番号を機械的に確認して、当該ISPが提供するメールサーバを経由せず動的IPアドレスから25番ポート(動的IPアドレスからのメールを伝送するために通常使用されるポート)に対して送信した電子メールを割り出し、当該電子メールをブロックする運用をいう。

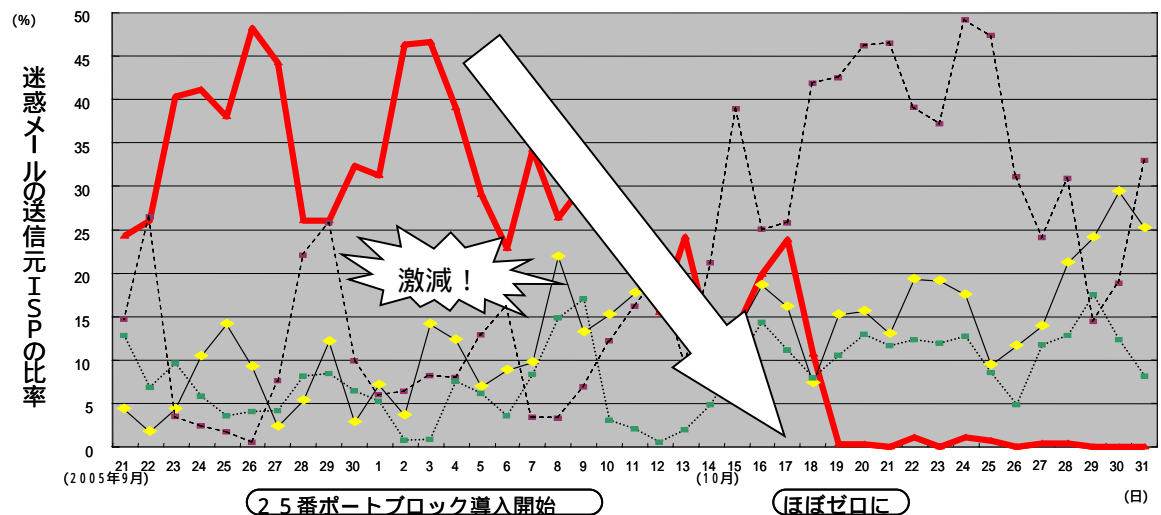
⁴ 総務省ウェブサイト http://www.soumu.go.jp/joho_tsusin/d_syohi/jigyosha.html

協会「行政法律部会」や、財団法人インターネット協会「迷惑メール対策委員会」においても、法的な課題や周知啓発等に関する検討、迷惑メール対策に関する情報交換等が継続的に行われている。

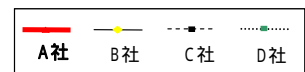
(図 5 : OP25B の仕組み)



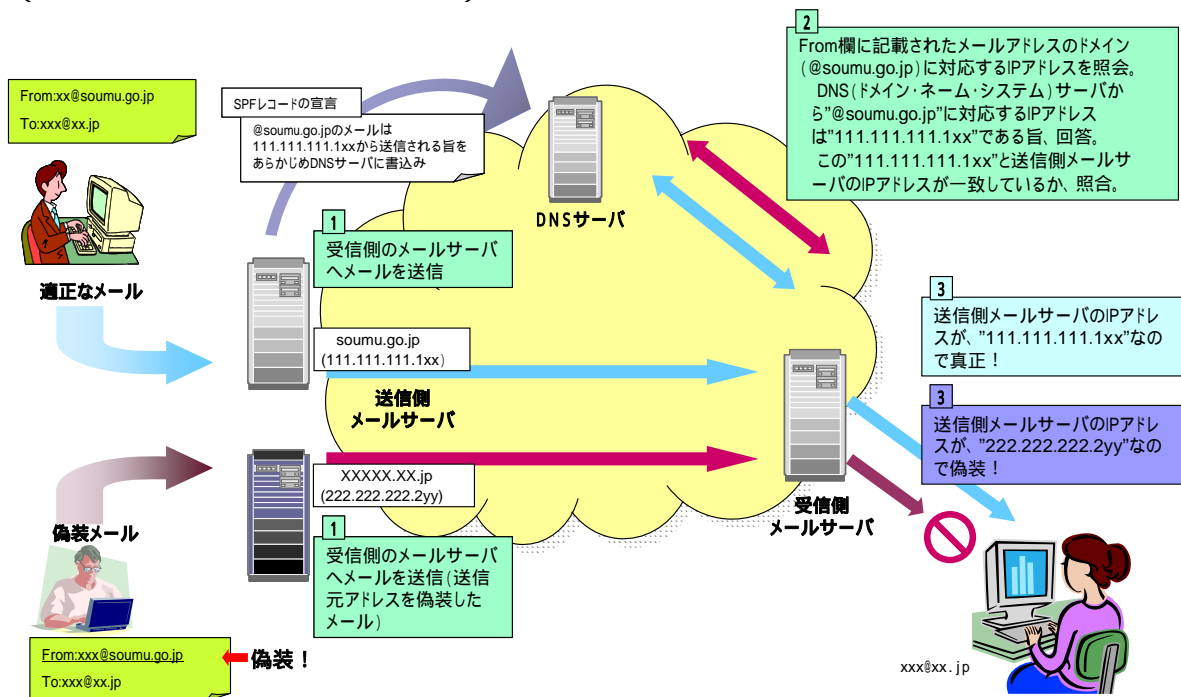
(図 6 : OP25B の効果)



注) (財)日本データ通信協会において、同協会あてに情報提供のあった携帯電話あての迷惑メール(2005年9月21日から10月31日までに受信された約1.3万通)の送信元ISPをヘッダ情報から分析。



(図 7 : 送信ドメイン認証の例)



国際的な連携

迷惑メールは、国際的な問題でもあり、平成16年(2004年)以降、OECDやAPECなど国際機関等においても議論が行われている。総務省は、平成16年に「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)⁵」に合意し、執行機関相互の情報交換等に努めるとともに、平成17年4月にアジア太平洋地域の11機関との間で合意した「スパム対策の協力に関する多国間MoU(覚書)」に基づき、多国間での具体的な協力策について定期的に議論している。また、米国をはじめとする欧米諸国とも個別に連携強化を図っており、二国間定期協議等を通じ、迷惑メール(スパム⁶)対策についての意見交換やMoUの署名などを行っている。

⁵ 2004年11月10日、ロンドンにおいて開催された「スパム対策執行に関するワークショップ」に参加した15カ国19機関が合意した行動計画。国際的なスパム法執行機関相互の意思疎通や協調、官民対話の促進を目的とする。

⁶ 「spam」は主に英語圏で広く用いられている言葉。「SPAM」は米国の食品会社が販売しているハムの缶詰であるが、レストランで料理を注文しようとした客に対しウェイトレスらが「スパム、スパム、スパム・・・」と執拗に連呼し、根負けして客がスパムを注文してしまう英国のTVコメディ番組にちなんで迷惑メールを意味するようになったといわれる。缶詰の「SPAM」と区別して、迷惑メールは小文字で「spam」と表記されることが多い。このほか、「Unsolicited Commercial Email」(UCE。望まれない商業電子メール)、「Unsolicited Bulk Email」(UBE。望まれない大量電子メール)という言葉なども用いられる。

(図 8 : 政府による国際連携の枠組み)

【マルチ (多国間)】

OECD「スパムタスクフォース」(04年7月～)

- ・ 06年4月までに「アンチスパム・ツールキット(包括的スパム対策)」を取りまとめて公表した。

LAP(ロンドンアクションプラン)(04年11月～)

- ・ 年1回の会合及び年最低4回の電話会議等を通じ、法執行の強化をテーマに議論。

スパム対策の協力に関する多国間MoU(覚書) (05年4月～)

- ・ アジア太平洋地域の12機関が締結した覚書に基づき、具体的な協力策等について定期的に議論。

ITU

- ・ 世界規制庁シンポジウム(05年11月)等でスパム対策について定期的に意見交換。

APEC

- ・ 電気通信サブグループ等でスパム対策について定期的に意見交換。

ICPEN(国際消費者保護執行ネットワーク)

- ・ 国境を越える違法な対消費者取引行為を規制するために結成された会合。05年にはスパムの実態調査を行った。

【バイ (二国間)】

日EU定期協議(04年6月～)

- ・ 両者のスパム対策等について意見交換。

日仏定期協議(04年12月～)

- ・ 両国のスパム対策等について意見交換。
(06年5月、パリにて、スパム対策に関する共同声明が署名された。)

日米情報通信政策協議(05年7月～)

- ・ 両国のスパム対策等について意見交換。

日加情報通信政策協議(05年10月～)

- ・ 両国のスパム対策等について意見交換。
(06年10月、オタワにて、スパム対策に関する共同宣言が署名された。)

日豪情報通信政策協議(05年10月～)

- ・ 両国のスパム対策等について意見交換。

日英定期協議(06年7月)

- ・ 両国のスパム対策等について意見交換。
(06年9月、東京にて、スパム対策に関する共同宣言が署名された。)

日独情報通信政策協議(06年9月)

- ・ 両国のスパム対策等について意見交換。
(07年7月、スパム対策に関する共同声明が署名された。)

また、国際的な連携は、政府のみならず、民間部門においても積極的に進められている。迷惑メール対策に関し米国を中心に各国の事業者が集まるMAAWG (Messaging Anti-Abuse Working Group) には、我が国から JEAG が参加し、OP25B 等我が国における技術的対策を紹介するなど、各国における取組について情報交換を行っている。また、財団法人インターネット協会は、日中韓のインターネット協会の間で覚書を締結⁷し、APCAUCE (Asia Pacific Coalition Against Unsolicited Commercial Email) に参加するなど、アジア・太平洋地域の ISP 間のネットワークの形成を模索している。

⁷ <http://www.iajapan.org/mou/mou.html>

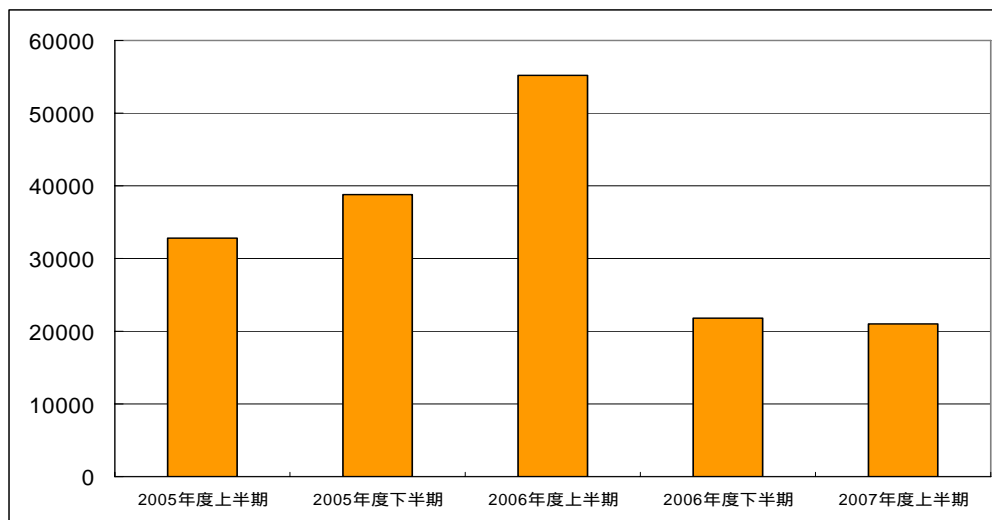
(2) 最近の迷惑メールの状況

全体的な動向

従来 of 取組による一定の成果

受信者のもとに到達する電子メールについては、上記の電気通信事業者等の取組や、利用者側におけるフィルタリングサービスの活用等の結果、携帯電話に着信する迷惑メールの通数は減少するなど、一定の成果が上がっている⁸。

(図9：携帯電話に着信した迷惑メール数の推移)
(通数)



注) 平成17年度上半期～平成19年度上半期に迷惑メール相談センターに設置したモニター機(携帯電話5台)に着信した迷惑メール数の推移

迷惑メールの全体的な傾向

一方、全体として流通する迷惑メールの量は依然として増加⁹しており、PCに着信する迷惑メールの通数も増加傾向にある。

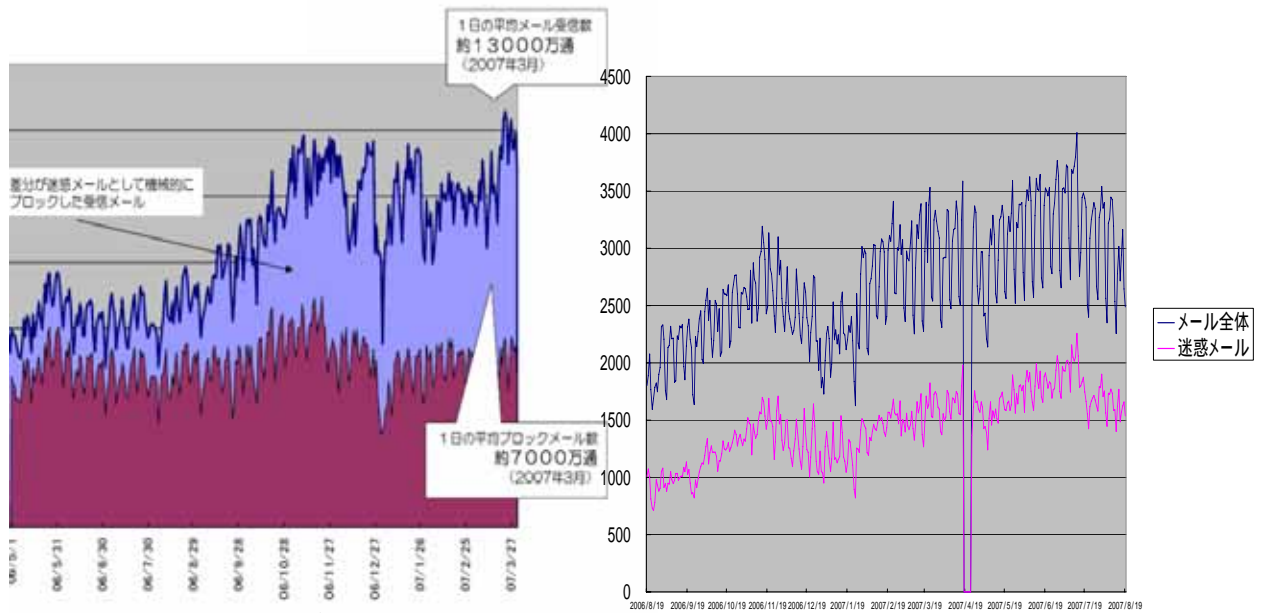
⁸ソフォス社によると、2005年4～9月期において、世界における迷惑メール発信国順位が9位であった日本は、2007年7～9月期においては、25位に低下している(P.21参照)。

⁹ISPのA社においてブロックする迷惑メールの総数も増加傾向にあり、平成19年3月時点のある一日において受信した迷惑メールは7000万通(全受信メール1億3000万通中)にのぼる。さらに、B社における迷惑メールの割合は、平成17年6月以降70%を推移しており、メールトラフィック全体が増加していることから、迷惑メールの総量も増加していることがわかる。

(図 10 : A 社総受信メールにおけるブロックメール数の推移及びB社における迷惑メール数の推移)

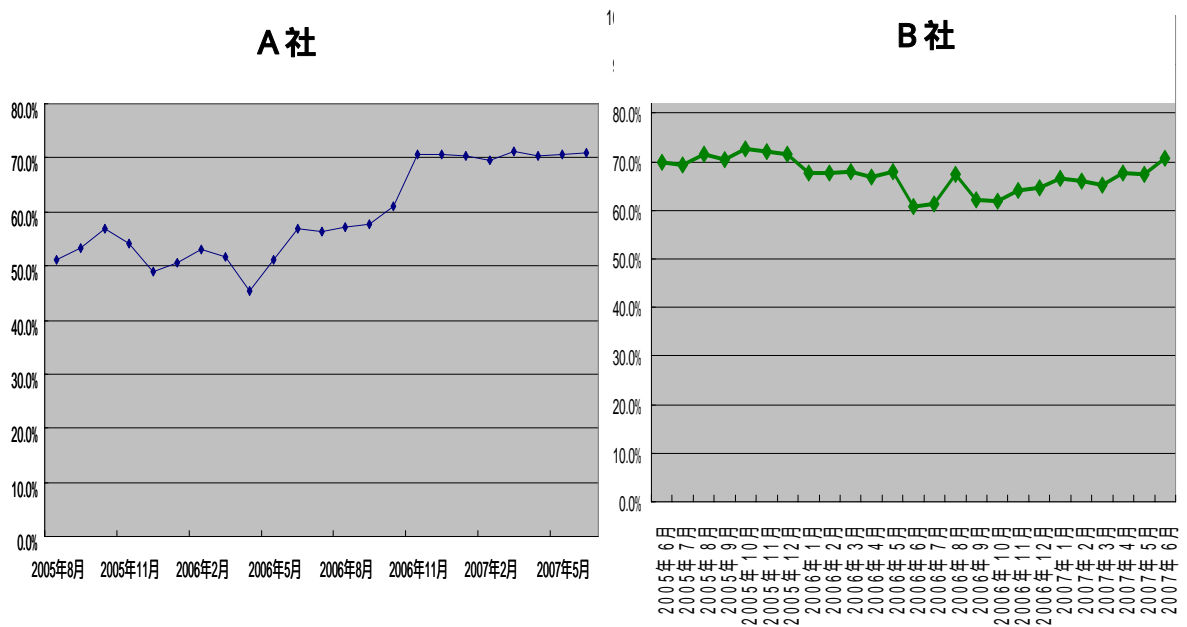
A 社総受信メールにおけるブロックメール数の推移

B 社における迷惑メール数の推移

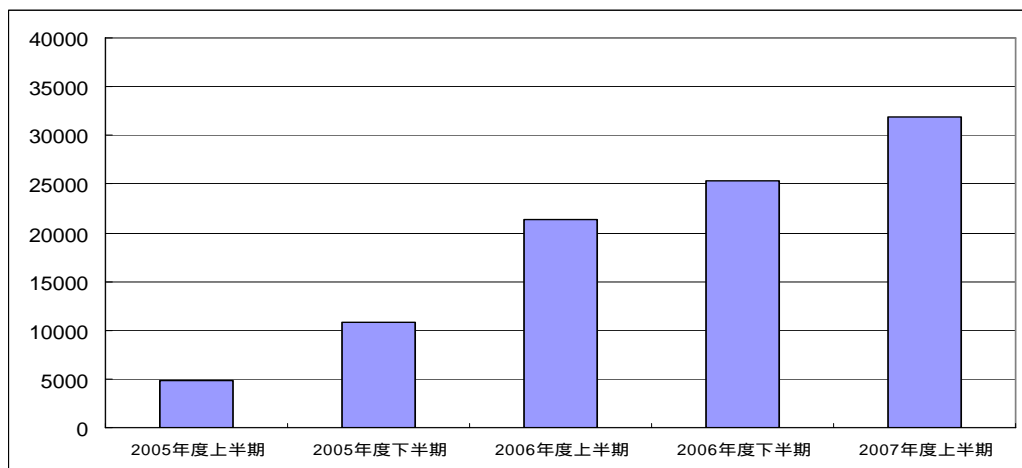


(注) A (注) A 社及びB社は I S P

(図 11 : A 社及びB社における総受信メールに占める迷惑メールの割合)



(図 12 : P C に着信した迷惑メール数の推移)
(通数)



注) 平成 17 年度上半期～平成 19 年度上半期に迷惑メール相談センターに設置したモニター機 (P C 1 台 (9 アカウント)) に着信した迷惑メールを分析したもの

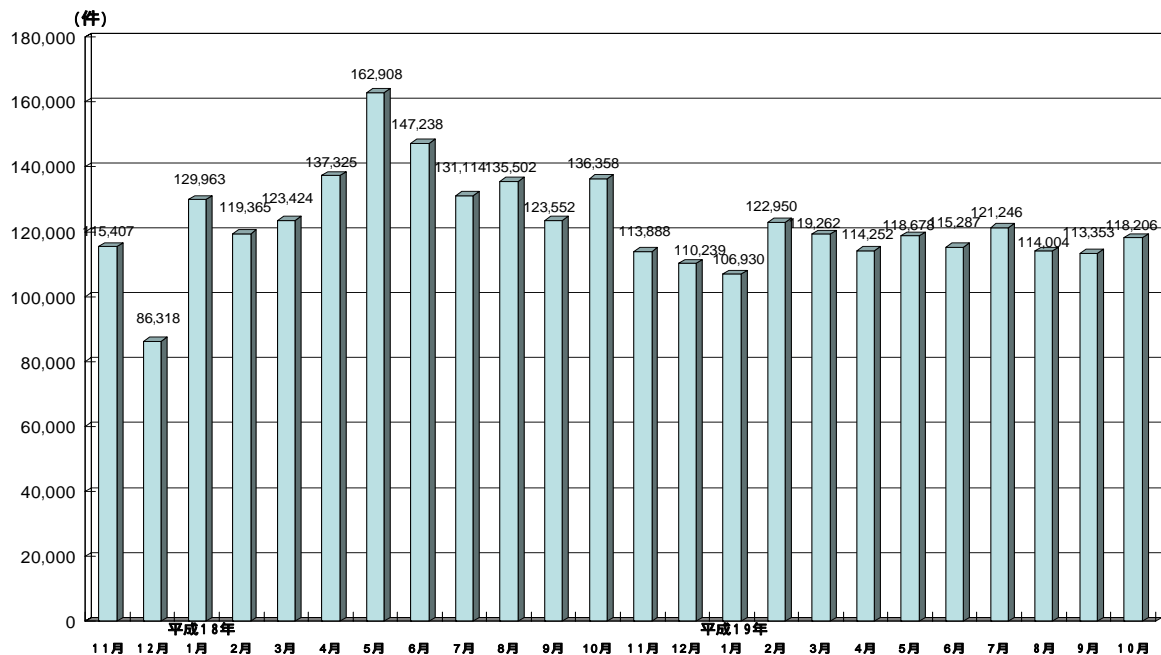
このような迷惑メールの増加により、電気通信事業者等は、迷惑メール対策技術の開発、サーバの増設等の設備構築及び運用、問い合わせ対応のためのサポートセンターの充実等のコスト負担を強いられている。受信者側においてもフィルタリングに対する追加費用や削除等の処理に要する時間と手間が発生するなど、総体として大きな負担となっている³¹。

また、迷惑メール相談センターへ特定電子メール法における表示義務違反として申告された迷惑メールの件数は、平成 17 年の特定電子メール法改正後、一時減少したものの、その後は一月あたり 12 万件程度の高い水準で推移している。

迷惑メール相談センターに寄せられた迷惑メールの内容については、依然として出会い系サイトの宣伝が多く、約 8 割を占めており、これにアダルト広告が続いている。

³¹ 我が国においては、平成 16 年において、迷惑メールにより、約 5000 億円の損失が生じているとの試算結果がある。(Ukai, Y. and T. Takemura, "Spam Mails Impede Economic Growth" The Review of Socionetwork Strategies, Vol.1(1), pp14-22, 2007) また、2006 年に公表された欧州委員会の報告 (COMMUNICATION on Fighting spam , spyware and malicious software (COM(2006) 688 final)) には、2005 年の迷惑メールによる損害は、世界全体で 390 億ユーロ (約 6 兆円) に達するというフェリス・リサーチ社の調査結果が紹介されている。

(図 13：特定電子メール法における表示義務違反として申告された迷惑メール件数の推移)



迷惑メールの巧妙化・悪質化

迷惑メールの全体量が増えていることに加え、最近では、以下のように、迷惑メールが巧妙化・悪質化している。

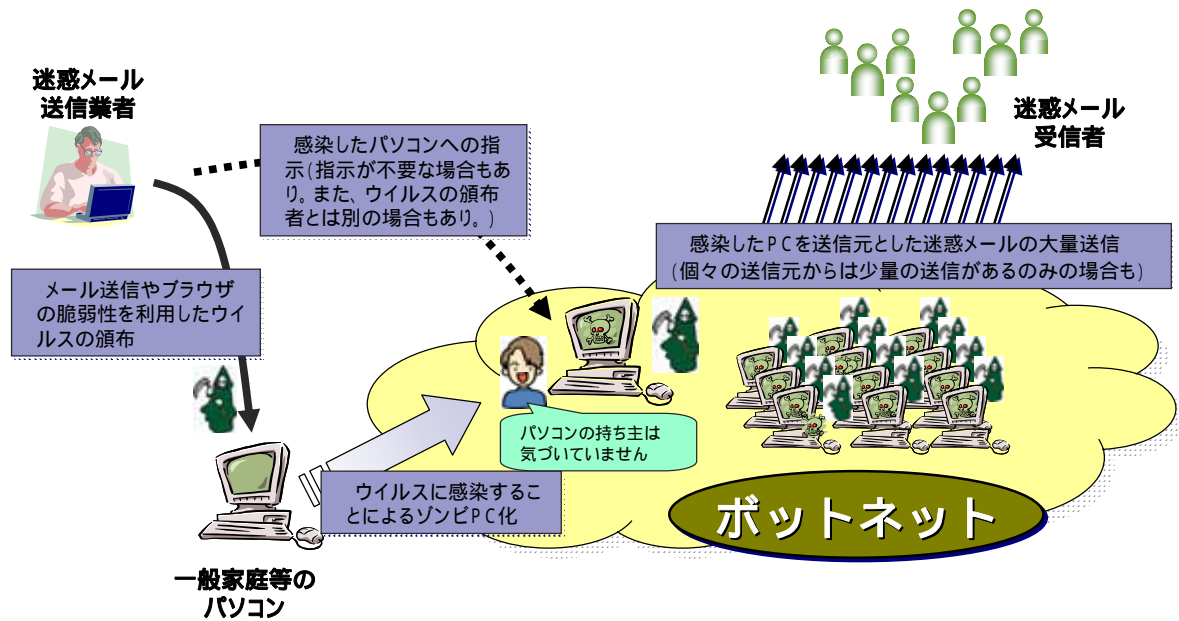
ボットネットを利用して送信される迷惑メール

ボットネットとは、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、外部から操作されるようになったPCにより構成されるネットワークのことである。

平成16年春頃より、ボットネットを利用した迷惑メールの送信が確認されるようになっており、現在では、ボットネットを利用した迷惑メールの送信が極めて増加していると言われる³²。

³²ソフォス社によれば、2007年8月現在において、世界全体の迷惑メールの90%以上がボットから発信されているとのことである。

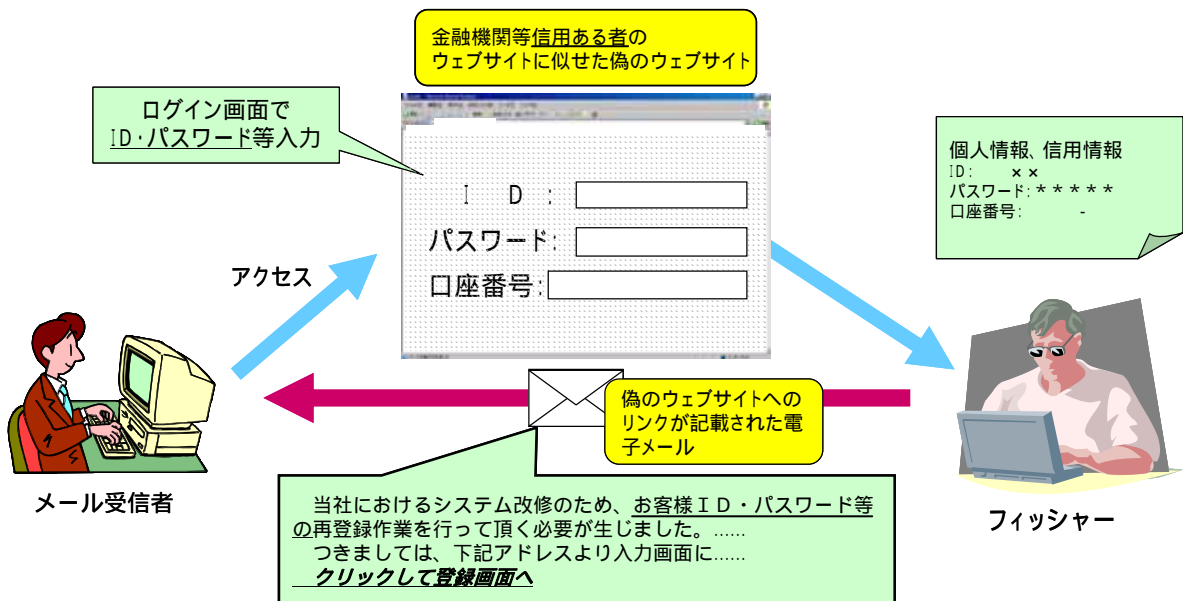
(図 14 : ボットネットを利用して送信される迷惑メール)



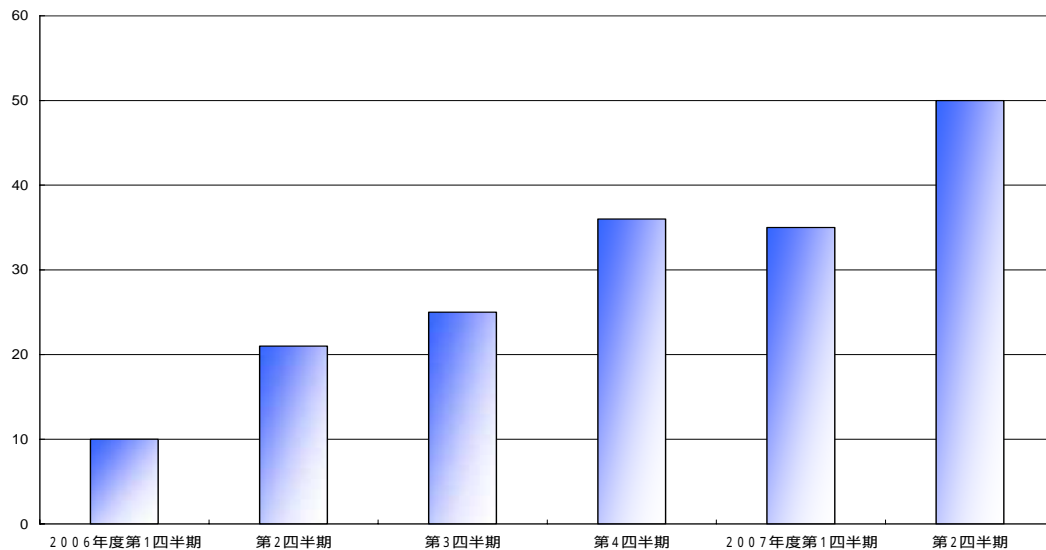
フィッシングメール

フィッシングメールとは、金融機関等信用ある者からのメールを装い、メールの受信者に偽のウェブサイトへアクセスするように仕向け、又はメールの返信を行わせることを通じて、ID・パスワード等を入力させるなどして、それらの情報を不正に入手（フィッシング）するための端緒となるメールである。我が国においては、平成16年秋頃から、クレジット会社や、ISP、銀行等を騙ったフィッシングメールの存在が確認されており、フィッシングメールの件数は増加傾向である。

(図 15 : フィッシングメールについて)



(図 16 : フィッシングメールの件数の推移 (国内))



(出典 : フィッシング対策協議会「月次報告書フィッシング情報届出状況」

<http://www.antiphishing/report/index.html>)

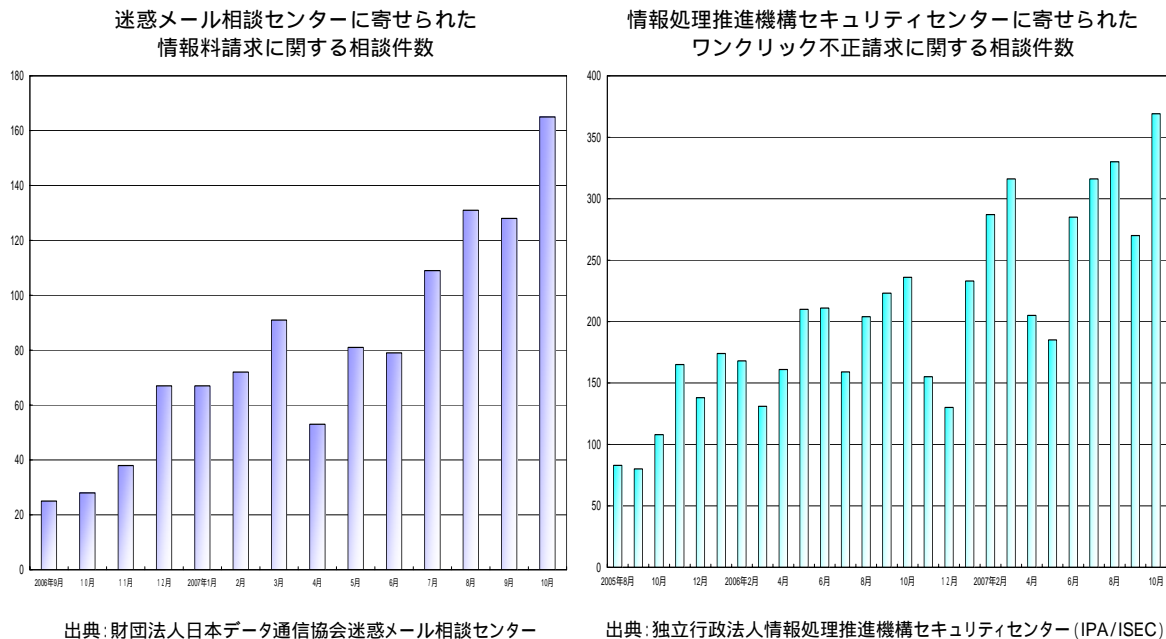
その他

その他、電子メールに表示された URL のクリック・アクセス等により、受信者の意思にかかわらず、登録完了画面等が表示され、利用料金等を請求されるいわゆるワンクリック詐欺を誘引するメールも問題となっている。迷惑メール相談センターや情報処理推進機構セキュリティセンターに対するワンクリック詐欺を誘引するメールに関わる相談件数は増加傾向となっており、検挙件数は依然として高い水準にある³³。

³³ 警察庁「平成19年度上半期のサイバー犯罪の検挙状況等について」

(<http://www.npa.go.jp/cyber/statics/index.html>) 参照。ただし、ネットワーク利用犯罪のうち詐欺の検挙件数は、平成18年上半期の733件から平成19年上半期は490件に減少している。

(図 17 : ワンクリック詐欺を誘引するメールに関わる相談件数推移)



法規制の実効性に関する状況

前節でも述べたとおり、平成17年の特定電子メール法改正以降、警察による摘発が3件行われ、総務省による警告も多数実施されている。

しかしながら、財団法人日本データ通信協会に設置したモニター機に受信した広告・宣伝メールのほとんどすべて³⁴は、表示義務違反の状態である。

表示義務違反に関しては、件名に「未承諾広告」の表示を付さないもののほか、送信者の名称や所在地等の情報についても記載されていなかったり、記載されていても虚偽の場合が多く、違法な送信者を特定するのが困難な場合が極めて多い。

さらに、特定電子メール法第4条では、再送信の拒否の通知が、再送信を禁止するための要件となっているが、実態として、この拒否の通知を行うことにより、かえって受信者の望まない広告・宣伝メールを誘発するとの指摘がある (P.40 参照)。

海外発迷惑メールの増加

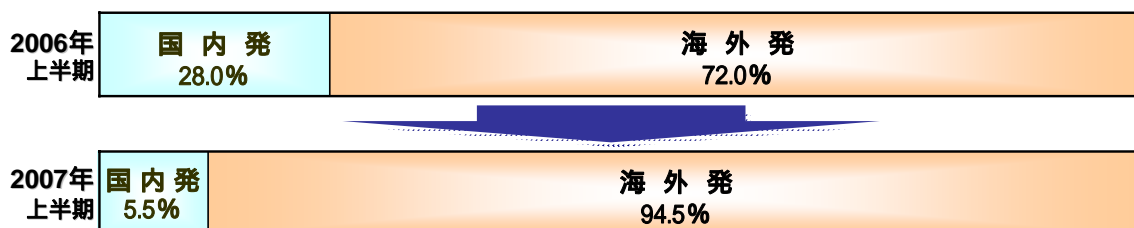
また、最近の傾向として、海外発の迷惑メールは急増していることも挙げられる。例えば、平成19年上半期に迷惑メール相談センターに設置した

³⁴ 平成19年6月～7月にモニター機に受信した迷惑メール(10,844件)を調査した結果、件名欄に「未承諾広告」を付していない広告・宣伝メールは97%であった。また、平成17年11月～12月に実施した同様の調査(4,146件)の結果では99.3%に達していた。

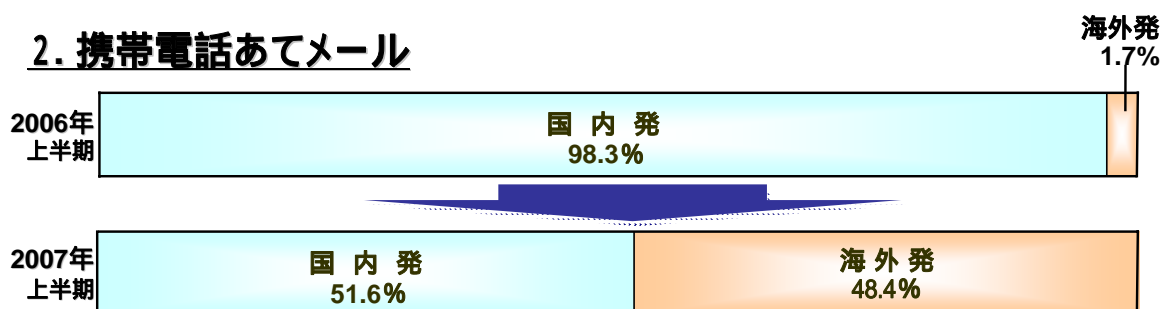
PC のモニター機に着信した迷惑メールの90%以上が海外から発信されていた。その多くは明らかに日本人又は日本に居住する者に対して行われた日本語による迷惑メールの送信であり³⁵、こうした海外発迷惑メールへの対応も課題となっている。

(図 18 : 日本発と外国発の迷惑メールの割合の変化)

1. PCあてメール



2. 携帯電話あてメール



注) 2006年1月～2007年6月に迷惑メール相談センター((財)日本データ通信協会内)に設置したモニター機に着信した迷惑メールを分析したもの

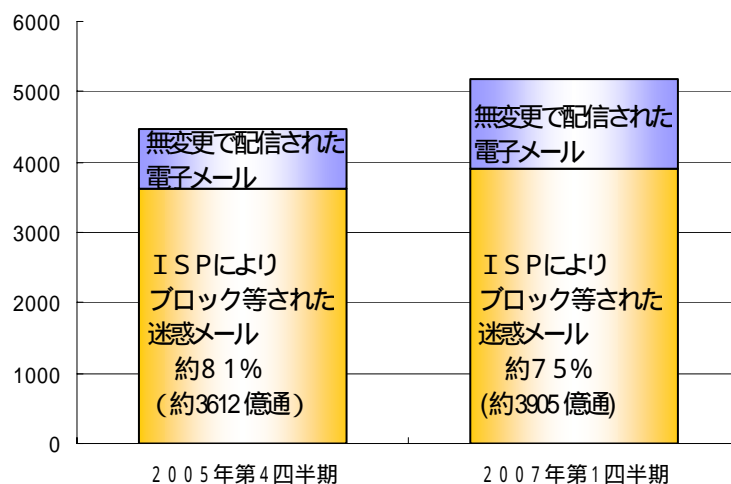
³⁵ 平成18年7月時点においては、迷惑メール相談センターに設置されたモニター機(PC)が受信したメールのうち、約91%が日本語のメールであった。

2. 諸外国の状況

(1) 最近の迷惑メールの状況

世界全体としては、引き続き電子メールのおよそ7割～8割程度が迷惑メール³⁶によって占められているものと推測される。

(図19：世界のメールトラフィックに占める迷惑メールの比率)



出典：MAAWG 公表資料

発信国としては米国、中国、韓国が引き続き上位を占めているが、13位以下の国である「その他」が約34%に達するなど発信国の分散化傾向がみられる。

(図20：世界における迷惑メール発信国(ソフォス社公表資料より³⁷))

	2005年4月～9月	2007年7月～9月
1位	米国 (26.4%)	米国 (28.4%)
2位	韓国 (19.7%)	韓国 (5.2%)
3位	中国 (15.7%)	中国 (4.9%)
4位	フランス (3.5%)	ロシア (4.4%)
5位	ブラジル (2.7%)	ブラジル (3.7%)
6位	カナダ (2.5%)	フランス (3.6%)
7位	台湾 (2.2%)	ドイツ (3.4%)
8位	スペイン (2.2%)	トルコ (3.2%)
9位	日本 (2.0%)	ポーランド (2.7%)
10位	英国 (1.6%)	英国 (2.4%)
11位	パキスタン (1.4%)	ルーマニア (2.3%)
12位	ドイツ (1.2%)	メキシコ (1.9%)
その他	11.7%	33.9%

日本は25位(0.9%)

³⁶ MAAWG 公表資料では、協力ISPにより接続拒否、ブロック又はタグ付けされたメールを「迷惑メール」(abusive email)として集計しているため、受信者にとってはこれらの電子メール以外にも迷惑メールが存在する可能性がある。

³⁷ ソフォス社「スパム送信国ワースト12」

<http://www.sophos.com/pressoffice/news/articles/2007/10/dirtydozooct07.html>

(2) 各国の規制の動向

米国

米国では、2004年1月に施行された CAN-SPAM 法によりオプトアウト方式の規制（携帯電話あてはオプトイン方式）が実施されている。

(図 21 : CAN-SPAM 法の概要)

CAN-SPAM法 (Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003)	
オプトアウト (携帯電話向けはオプトイン)	・商業電子メールについて、受信拒否の要請から10日後以降の当該受信者への送信を禁止
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	・ 偽ヘッダー情報による送信 ・ 欺瞞的表題を付した送信 ・ 受信拒否の通知を受けた後の当該受信者の電子メールアドレス売却、貸与、交換、移転等 ・ 送信元を偽る意図をもって、電子メールを中継又は再伝送するためにコンピュータを利用すること ・ あて先メールアドレスが、電子メール送信のためにメールアドレスを提供しないことを表明しているウェブサイト又はオンラインサービスから自動取得したものであると知りながら違反メールを送信すること ・ あて先メールアドレスが自動生成したものであると知りながら違反メールを送信すること ・ 違反メールを送信するため複数の電子メールアドレスを自動で登録すること ・ 許可なくアクセスしたコンピュータからの違反メール送信又は多数の送信 ・ アイデンティティを著しく偽った情報を使用して5個以上の電子メールアカウント又は2個以上のドメイン名を登録し、そのアカウント又はドメイン名を組み合わせることで多数の商業電子メールを送信すること ・ 5個以上のIPアドレスについてその登録者であると偽ってそのアドレスから多数の商業電子メールを送信すること
制裁措置	・ 行政 (民事) 上の措置として、裁判所による差止命令、FTCによる違反行為停止命令等 ・ 罰則として、最高で5年間の禁固または罰金 (罰金は、違反行為により被告が得た利益若しくは他者が被った損害の2倍の額、個人25万ドル法人50万ドルのうち、高額な方が上限)

CAN-SPAM 法は、携帯電話あてを除きオプトアウト方式を採用してはいるが、我が国の特定電子メール法に比べ、悪質な迷惑メール送信手法を規制するための禁止事項が多く規定されている。この禁止事項の中には、ボットネットを用いた送信に適用可能であると解される規定も含まれている(許可なくアクセスしたコンピュータからの送信)。

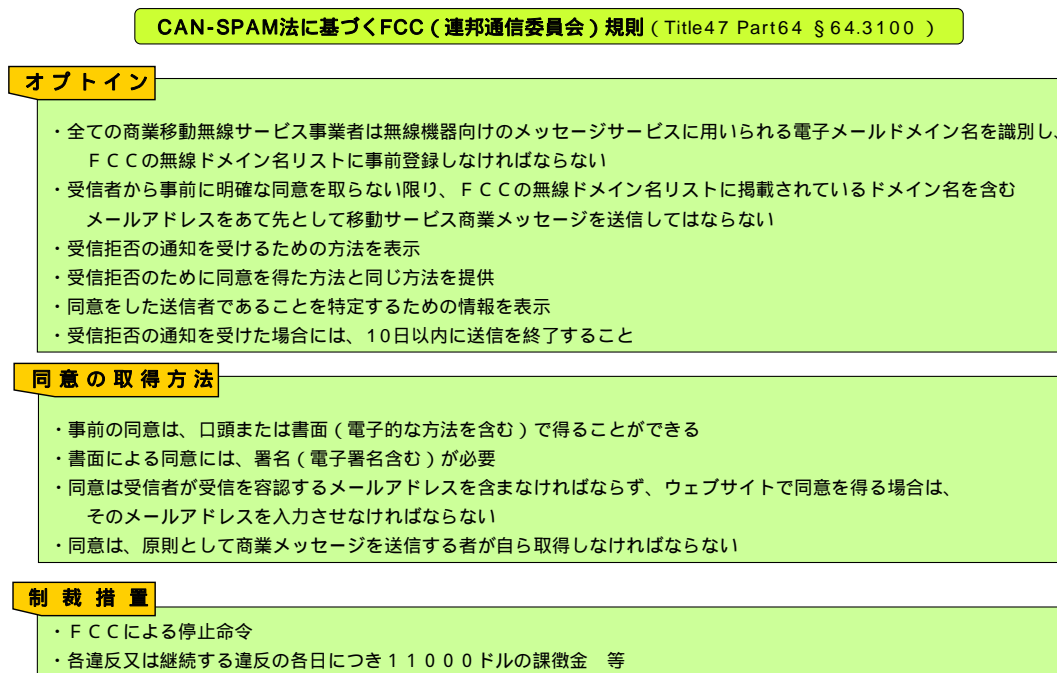
また、受信拒否要請後の電子メールアドレス売却・移転等の禁止、他人のウェブサイトから自動取得したメールアドレスにあてた送信を加重違反とすること等により、原則として受信者の同意を得ずに送信が可能であるとしつつも、不当に取得したメールアドレスあての送信については一定の制限を課す内容となっている。

法執行は、主に FTC(連邦取引委員会)が違反行為停止命令等により実施し、一部については刑事罰規定を適用し司法省による起訴も行われている。また、CAN-SPAM 法のほかに US SAFE WEB 法が2006年12月に成立し、他国の関係機関との情報共有や捜査協力等について FTC の権限が強化されたところである。しかしながら、全体の傾向としては、法遵守率が低下している(200

4年3%、2005年4% 2006年0.45%)とする調査結果³⁸があるほか、発信国として依然として第1位にランキングされている³⁹など、迷惑メールが引き続き問題となっている状況にある。

なお、携帯電話あての商業電子メールについては、FCC（連邦通信委員会）によってオプトイン方式の規制が実施されており、その規則において、オプトアウトの方法及び同意を得た送信者である旨を示さなければならないことや、同意は原則として送信者が自ら取得しなければならない等の詳細なルールが規定されている。

（図 22：FCC 規則の概要）



³⁸ MX Logic社 2007年1月8日公表

³⁹ ソフォス社 2007年7月18日公表

E U

E Uでは、オプトイン方式を規定するプライバシー・電子通信指令(2002/58/EC)が2002年7月に制定され、加盟各国が国内法により当該指令を担保することとされた。

(図23: プライバシー・電子通信指令(2002/58/EC)の概要)

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2002年7月12日の欧州議会及び理事会指令(DIRECTIVE 2002/58/EC)

第13条 望まれない通信

1. DM(ダイレクトマーケティング)を目的とした、人間が介在しない自動通話システム(自動発信機)、ファックス又は電子メールの利用は、加入者の事前の同意がある場合のみ許される。
2. 第1項にかかわらず、自然人又は法人は、指令95/46/EC(個人データ保護指令)に従って製品又はサービスの販売を通して電子メールを送るための詳細情報をその顧客から取得した場合には、当該自然人又は法人が所有する類似製品又はサービスのDM用にそれらの情報を利用できる。ただし、詳細な情報が収集された時点や、顧客がその情報の利用を最初に拒絶しなかった場合には各メッセージが送られるときに、当該利用を無料かつ簡易な方法で拒絶する機会が明確にはっきりと当該顧客に与えられることを条件とする。
3. 加盟国は、第1項及び第2項以外の場合に、加入者の同意なく行われるDMを目的とした通信、又はそれを受け取ることを望まない加入者に向けられたDMを目的とした通信が許されず、無料で拒絶できるように保証しうる適切な措置をとるものとする。いずれのオプションを選択するかは国内法により決定されるものとする。
4. いかなる場合においても、通信を行う発信者の身元を偽り、若しくは隠し、又は受信者が通信の停止を求めめることを連絡できる有効な受取人のアドレスなしに、DMの目的で電子メールを送信してはならない。
5. 本条第1項及び第3項で定められた権利は自然人たる加入者に適用されるものとする。加盟国はまた、EU法及び適用される国内法の枠組みの中で、望まれない通信に関して自然人以外の加入者の正当な権利が十分に保護されることを保証するものとする。

第17条 国内法への移行

1. 2003年10月31日より前に、加盟国はこの指令を遵守するために必要な国内規定を発効させるものとする。(後略)

E Uの制度はオプトイン方式ではあるが、類似の製品・サービスのダイレクトマーケティングを行う場合には改めて同意を取る必要はないとされている。ただし、オプトアウトの機会を示すこと及び送信者の身元を偽らないことは、事前の同意の有無にかかわらず、送信に際し必須とされている。本指令を受けて、英独仏等各国でオプトイン方式の規制が実施されている。

特にオランダは迷惑メールを85%減少させるという成果をあげ⁴⁰、その迷惑メール対策が模範的であるとして、2006年11月に欧州委員会から評価を受けた⁴¹。オランダでは、同意について消費者ではなく事業者⁴²に証明責任が

⁴⁰ ただし、これはオランダ発オランダ着の迷惑メールにおける成果である。また、オランダ着の迷惑メールの大半が海外発であるとの報告もある。

(Stratix Consulting, The size and business case of spam in the Netherlands
http://www.ispo.nl/home/downloads/Business_case_spam_in_NL.pdf)
(2004年12月)

⁴¹ 2006年11月27日欧州委員会公表「スパム、スパイウェア及び悪意あるソフトウェアとの闘い: 加盟各国はより良い取組みをすべき(IP/06/1629)」また、欧州委員会は、フィンランドがフィルタリングによって迷惑メールの割合を80%から30%に減少させたことについても成果として言及している。

あるとされているとともに、多くの警告及び罰金(罰金の最高額は45万ユーロ(約7200万円)に達する)を課すなど積極的な法執行が行われていることが特徴である。

(図24: オランダ電気通信法の概要)

オランダ電気通信法(11.7条等)	
オプトイン	<ul style="list-style-type: none"> ・受信者が前もって承諾したことを送信者が証明できるときのみ、商売目的、理想主義的な目的、慈善目的のための望まれない電子メール等を送信できる ・ただし受信者を識別するための情報及び拒否通知するための連絡先を示さなければならない ・製品販売の一環として連絡先を入手した場合に、当該連絡先に類似の製品に係る通信を伝送することは可 ・ただし連絡先の使用について異議申し立てを行う機会を示さなければならない ・自然人に対して送信される電子メール等(電子メール、ファックス、自動通話システム)が対象 ・ただし法人から法人へ送信されるものも対象に含める法案を検討中 ・電子メール等以外の手段の通信についてはオプトアウト
ポットネット、フィッシング	<ul style="list-style-type: none"> ・フィッシングメールは望まれない電子メールに含まれる。 ・マルウェア及びスパイウェアの配布に対しては行政上及び刑事上の規定も存在
制裁措置	<ul style="list-style-type: none"> ・最高45万ユーロ(約7200万円)の罰金
執行状況	<ul style="list-style-type: none"> ・法の執行後スパムを大きく減らすことに成功(欧州委員会公表資料等による) ・2006年末、欧州委員会はオランダのスパム対策が模範的であるとして賞賛。 <ul style="list-style-type: none"> - 執行がOPTA(郵便電気通信庁)により行われていること - OPTAに最高45万ユーロの罰金を適用する権限があること - 紛争が起こった時、証明責任は事業者であり消費者ではないこと等 ・OPTAが多くの警告及び罰金を実施し、3年間で28000件の苦情(うち113件は訴訟に発展)を受領
国際的な対応	<ul style="list-style-type: none"> ・2006年、オーストラリアのスパマーがOPTAの提供した情報により突き止められた

オーストラリア

オーストラリアでは、2003年スパム法(Spam Act of 2003)によりオプトイン方式が採用されている。

(図25: オーストラリア2003年スパム法の概要)

オーストラリア2003年スパム法	
オプトイン	<ul style="list-style-type: none"> ・商業電子メッセージは、受信者の同意がある場合のみ送信できる ・商業電子メッセージには正確な送信者情報を記載しなければならない ・商業電子メッセージは配信停止機能を有しなければならない ・「同意」には、行動(conduct)又はビジネスその他の関係から合理的に推定できる同意が含まれるほか、公開されているメールアドレスについても、同意が推定される場合がある。
禁止事項	<ul style="list-style-type: none"> ・違法メール送信に関連して、アドレス収集ソフトを提供、取得、利用すること ・違法メール送信に関連して、アドレス収集ソフトを利用したアドレス帳製作物の提供、取得、利用を行うこと ・存在しないメールアドレスをあて先として送信すること
ポットネット、フィッシング	<ul style="list-style-type: none"> ・ポットネットから送信される商業電子メッセージもスパム法の対象 ・(単なる送信(send)行為のほか、援助(aid)・教唆(abet)・cause to be sent等の行為も規制) ・フィッシングメールはスパム法の対象であるとともに詐欺行為ともみなされる ・(スパム法では、商業電子メッセージに、不正な利益取得の支援・可能化を目的とする電子メールが含まれる。)
制裁措置	<ul style="list-style-type: none"> ・ACMA(豪通信メディア庁)による正式警告、違反通知、強制執行、禁止命令、起訴 ・民事罰として個人に最大22万豪ドル(約2200万円)、法人に最大110万豪ドル(約1億1000万円)の罰金
国際対応	<ul style="list-style-type: none"> ・送信者、受信者又は受信メールにアクセスするための機器がオーストラリアに所在していれば規制対象 ・2006年にオランダOPTAの提供した情報によりオーストラリアのスパマーが突き止められた例が存在

2003年スパム法は、現在、我が国で問題となっているボットネットを用いた送信、フィッシングメール、海外からの送信、いずれについても明文により対応をしており、現時点で考えうるスパム対策を包括的に盛り込んだ先進的なスパム法制として、我が国でも参考となる点が多い。法執行は通信メディア庁により行われ、刑事罰は規定されていないが、違反者には民事罰として比較的高額の罰金（法人では最高1億1000万円）を課すことが可能であり、実際にも適用されている。また、法執行を助けるため、利用者が電子メールクライアントソフトウェアに拡張機能をインストールすることによりスパムの消去及び通信メディア庁への通報を実施可能とするシステム（Spam MATTERS）が運用されており、2006年5月以来、同システムを通じた通報件数は約2400万件以上に上っている。これらの努力の成果もあり、オーストラリアのスパム発信国順位は法施行時（2004年）の10位から2006年には28位に低下した。

なお、オプトイン方式ではあるが、「同意」については、ビジネス上の関係があれば推定できるとするなど比較的緩やかな規定が置かれている。

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」により、電話あての広告メールはオプトイン方式、それ以外の端末あての広告メールについてはオプトアウト方式が採用されている。

（図 26：韓国情報通信網法の概要）

情報通信網利用促進及び情報保護等に関する法律（情報通信網法）	
オプトアウト、携帯電話あてはオプトイン	<ul style="list-style-type: none"> 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 電話あての広告メールは以下のいずれかの場合を除き受信者の事前同意を得なければならない <ul style="list-style-type: none"> - 取引関係を通じて受信者から直接連絡先を収集して広告メールを送信する場合 - 特定の種類の電話勧誘の場合
表示義務	電子メール：「（広告）」等の文字、氏名、メールアドレス、住所、電話番号、メールアドレス収集元、受信拒否等のための情報 電話（SMS）：氏名、連絡先電話番号、受信拒否のための無料電話番号
禁止事項	<ul style="list-style-type: none"> 受信拒否又は不同意の阻害、メールアドレスの自動作成、並びに送信者の隠匿をする技術的操作 プログラムによるメールアドレス自動収集、収集したメールアドレスの売却、頒布及び利用
ボットネット、フィッシング	<ul style="list-style-type: none"> 正当な権利なく又は権限を濫用してパソコンをボットネットにして遠隔操作できるようにすることは犯罪 ボットネットを通じて送信されるスパムを送信者から直接送信されたものと同様に規制 情報通信網を通じて個人情報収集又は頒布するために他人を騙す行為について規制
制裁措置	<ul style="list-style-type: none"> オプトアウト、オプトイン、表示義務違反の場合：3千万ウォン（約390万円）以下の過料（過怠金） 禁止事項違反の場合：1年以下の懲役又は1千万ウォン（約130万円）以下の罰金
国際的な対応	<ul style="list-style-type: none"> 海外から送信されたとしても、韓国から送信されたとしても、送信者は罰金刑等の罰を受ける（オプトアウト/イン違反及び表示義務違反については「行われた者」にも過料が課される）（広告伝送を委託した者は受託者に対して監督責任を負う）

中国

中国では、2006年3月にインターネット電子メールサービス管理弁法が施行され、法制度による対応が本格的に開始された。当該法は、オプトイン方式を採用するとともに、他人のコンピュータの不正利用（ボットネット等）、ヘッダ情報の隠匿・偽造、メールアドレスの自動収集・自動作成等、悪質な送信手法についても幅広く規制する内容となっている。また、ログの保存及び提出、セキュリティ対策、苦情の処理等、電子メールサービスプロバイダの義務を明文により定めていることも特徴である。

（図 27：中国インターネット電子メールサービス管理弁法の概要）

インターネット電子メールサービス管理弁法（互聯網電子郵件服務管理弁法）	
オプトイン	<ul style="list-style-type: none">・ 受信者の明確な同意を得ずに、商業広告の内容を含む電子メールを送信又は委託送信してはならない・ 受信者が継続的受信を拒否した場合、送信者は送信を停止しなければならない・ 継続受信を拒否する場合の連絡先を提供しなければならない(当該連絡先は30日間有効であることが必要)
表示義務	<ul style="list-style-type: none">・ 商業広告の内容を含む電子メールには、標題情報の前に「広告」又は「AD」を明記しなければならない
禁止事項	<p>（いずれも商業広告の有無にかかわらず電子メール全般が対象）</p> <ul style="list-style-type: none">・ 授権されていない他人のコンピュータを利用した電子メールの送信・ オンライン自動収集・文字数字の任意組合せ等の手段により取得した他人のメールアドレスの販売、共同利用、交換・ オンライン自動収集・文字数字の任意組合せ等の手段により取得した他人のメールアドレスに対する送信・ ヘッダ情報を隠匿又は偽造する行為・ 電気通信条例57条が規定する内容（国家安全危害、わいせつ等）を含む電子メールの制作、複製、公表、発信・ 電子メールを利用した、電気通信条例58条が禁止するセキュリティに危害を与える行為（データ改竄、設備攻撃等）・ 通信の秘密を侵害する行為
制裁措置	<p>（禁止事項の一部については別規定により処罰）</p> <ul style="list-style-type: none">・ 情報産業部又は通信管理局による是正命令、及び1万元（約16万円）以下の罰金。・ 違法所得があった者については3万元（約48万円）以下の罰金。
現在の状況	<ul style="list-style-type: none">・ 中国のスパム発信地に占める比率は06年第1四半期の21.9%から07年第2四半期の8.4%に低下・ 受信メールに占める迷惑メールの比率はやや減少傾向（06年3月63.97% 07年3月58.01%）
その他	<ul style="list-style-type: none">・ 電子メールサービスプロバイダには、メールサーバIPアドレスの事前登録・オープンリレー対策等のセキュリティ措置実施・ログの保存及び必要に応じた提出・苦情の処理等の義務あり

まとめ

以上の各国の規制動向について、迷惑メール対策における課題別に状況をまとめると以下のとおりであり、我が国においても、迷惑メールが法執行面で国際連携を必須とする問題であることを踏まえ、これら諸外国の制度を十分に考慮することが必要と考えられる。

i) オプトイン方式の一般化

EUを始めとして、既に我が国以外の主要国は何らかの形でオプトイン方式を導入している状況にあり、国際的にみてオプトインが一般的な迷惑メール法制となりつつある点に留意する必要がある。

ii) ポットネット等への対応

ポットネットを利用した迷惑メールの送信については、米国、オーストラリア、韓国、中国がスパム法制に位置付けて規律している。また、フィッシングメール等については、既存の法制の解釈・適用により対応している国があるほか、オーストラリアがスパム法に位置付けて規律している。

iii) 国外発メールへの対応

オーストラリアが「オーストラリアン・リンク」という概念を設けて送信者、受信者、電子メールにアクセスするための機器、のいずれかが国内に所在すれば規制対象とするとして明文で定めているほか、米国及び韓国が一般的には国外からの送信であっても規制対象とするなど、迷惑メールが国境を越える問題であることを踏まえた制度が既に整備されている国がある。また、米国では US SAFE WEB 法が 2006 年 12 月に成立し、他国の関係機関との情報共有や捜査協力等について FTC の権限が強化された。また、執行面においても、複数の国の法執行機関が協力して送信者を摘発した例が存在する。

iv) 抑止力のある制裁

スパム法制により一定の成果をあげているとされるオーストラリアやオランダは、高額な金銭的制裁を用いているのが特徴である。米国等その他の国においても我が国に比べ高い制裁金額が規定されている国が比較的多いといえる。

(図 28：諸外国の罰則に関する規定の概要)

(罰金は最大額)

	罰則対象	個人に対する罰則	企業に対する罰則
米国 (CAN - SPAM法)	性的素材表示義務違反、重罪を行うため又は再犯の場合の刑事罰規定違反 許可なくコンピュータにアクセスして送信、20以上の電子メールアドレス又は10以上のドメインを偽って登録、違反メールの大量送信、違反メールにより多額の損害又は多額の利益、組織の指導者等の場合(いずれも刑事罰規定) その他の刑事罰規定違反 (その他、課徴金等の制裁措置が若干あり)	5年以下の拘禁又は 25万ドル(約2900万円)の罰金(注) 3年以下の拘禁又は 25万ドル(約2900万円)の罰金(注)	50万ドル(約5800万円)の罰金 (注) 50万ドル(約5800万円)の罰金 (注)
英国(プライバシー・電子通信規制)	違反行為	5000ポンド(約120万円)の罰金	
ドイツ(テレメディア法)	「冒頭行及び件名欄に送信者及び通信の商業的性格を隠したり、秘密にしてはならない。」に対する違反	5000ユーロ(約800万円)の罰金	
フランス(郵便・電子通信法典)	オプトイン不遵守 個人情報たるメールアドレスの不正収集・不正利用等	1通ごとに750ユーロ(約12万円)の罰金 5年以下の懲役又は30万ユーロ(約4800万円)の罰金	
オランダ(電気通信法)	違反行為	45万ユーロ(約7200万円)の罰金	
オーストラリア (2003年スパム法)	オプトイン、架空アドレスあて送信禁止違反 その他の違反 1日に2回以上の違反 1日に2回以上の違反	2200豪ドル(約22万円)の罰金 1100豪ドル(約11万円)の罰金 4万4千豪ドル(約440万円)の罰金 2万2千豪ドル(約220万円)の罰金	1万1千豪ドル(約110万円)の罰金 5500豪ドル(約55万円)の罰金 22万豪ドル(約2200万円)の罰金 11万豪ドル(約1100万円)の罰金
韓国 (情報通信網利用促進及び情報保護等に関する法律)	オプトイン/アウト違反、表示義務違反 技術的操作禁止違反及び アドレス収集・売却・頒布・利用禁止違反	3000万ウォン(約390万円)の過料 1年以下の懲役又は1000万ウォン(約130万円)の罰金	

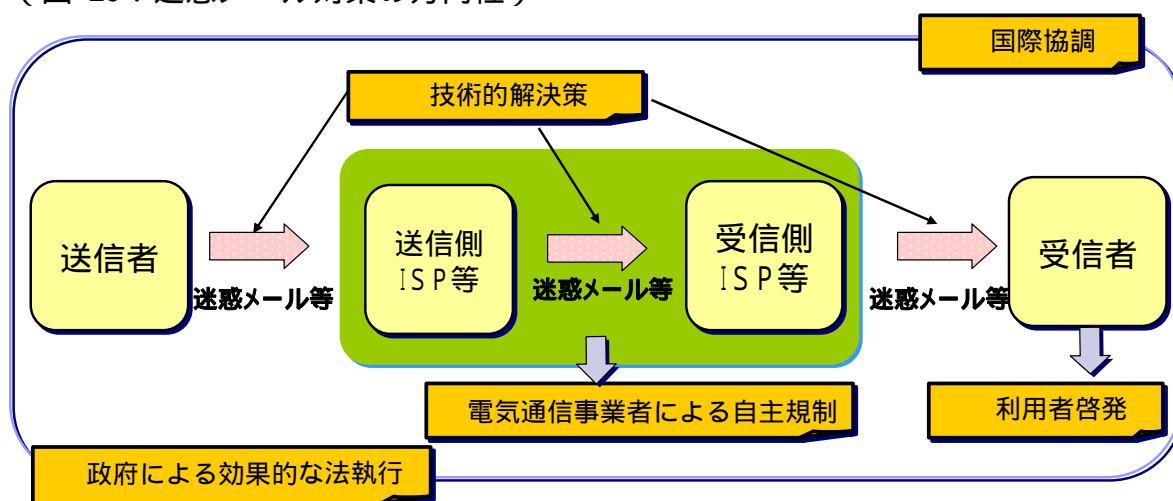
米国(注)：(違反行為により被告が得た利益又は他者が被った損害の2倍の額)の方が高額な場合はその金額が上限となる。
為替レート：1米ドル=115円、1ポンド=220円、1ユーロ=160円、1豪ドル=100円、1ウォン=0.13円 により換算。

3. 迷惑メール対策の検討の方向性

(1) 総合的な対応の必要性と法の果たす役割

迷惑メール対策については、特効薬はなく、多面的な対策をできるところから措置していくことが必要である⁴²。「迷惑メールへの対応の在り方に関する研究会」(第2次研究会)の最終報告(平成17年7月)では、この認識に基づき、政府による効果的な法執行、電気通信事業者による自主規制、技術的解決策、利用者啓発、国際協調、による総合的な対応方策を進めていくべきであるとして、以下(図29)の枠組を提示している。

(図29: 迷惑メール対策の方向性)



この枠組の有効性は現在も変わっておらず、引き続き、この枠組に沿って、総合的な対応方策を進めていくことが必要であると考えられる。

総合的な対応方策を進める上で、法制度は、執行の根拠となるのみならず、違法行為は何か、政府、電気通信事業者の役割は何か、といった対応方策の基本的な枠組を提供する点で重要であり、迷惑メール対策として、中間とりまとめにおいては、まず、法制度の在り方を検討することが必要と考えられる。

⁴² 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。できるところから行動すべき。」との認識で一致している。

(2) 法制度見直しの必要性

迷惑メールが全体として増加し続けており、変化の激しいインターネットの世界の中で、迷惑メールの送信手法等も巧妙化、悪質化してきている現状の下では、総合的な迷惑メール対策を引き続き、充実・強化していく必要があり、総合的な迷惑メール対策の基本的な枠組となる法制度について、現行の法制度で対応が困難な点があれば、見直しを図るべきであると考えられる。

先に述べた、迷惑メールとその対策の現状や諸外国の迷惑メール対策の進展を踏まえると、現行の法制度に関しては、以下の点で対応が困難な点があると考えられる。

第一に、ポットネットの利用、フィッシングメール等の送信など、迷惑メール送信の巧妙化・悪質化が進む中で、現行法上違法といえるかが微妙な形態のものが出現してきている。

第二に、現行法の実効性は十分ではない。法執行機関が必要な措置等を行おうとする場合でも、現行法の制度的な限界から十分な措置ができない場合が多い。

第三に、諸外国でも迷惑メール法制の整備が進み、迷惑メール法制の国際的な調和も必要となっており、また、外国発の迷惑メール等国境を越えて送受信される迷惑メールが増加している状況の中で、現行法は、必ずしもこの点を前提とした制度とはなっていない。

こうした点を踏まえると、現行の特定電子メール法は一定の見直しが必要と考えられる。

(3) 法制度見直しの視点

法制度の見直しにあたっては、具体的には、以下の3つの観点から、特定電子メール法の見直しを行うべきと考えられる。

巧妙化・悪質化する迷惑メールへの対応の強化

ポットネットの利用、フィッシングメールその他現行法の適用を回避する巧妙化・悪質化した電子メールへの対策を総合的に講じていく上で、対策が必要な電子メールについて、法制度上、違法であることを明確化することが必要であると考えられる。

法の実効性の強化

より効果的な迷惑メール対策を行っていく上で、法の実効性の強化が必要であり、下記の実現に資するように制度を構築すべきと考えられる。第一に、迷惑メールの送信者にとって、迷惑メール送信のコスト、リスクがより高くなる制度が必要であると考えられる。第二に、迷惑メールの受信者にとって、迷惑メール受信の防止のコスト、リスクがより低くなる制度が必要であると考えられる。第三に、電子メールサービスを提供する事業者にとって、自主的な対策を行いやすくなる制度が必要であると考えられる。そして、法の執行機関にとって、法執行のための措置が円滑かつ機動的にとりやすくなる制度が必要であると考えられる。

国際的整合性・連携の強化

インターネットは国際的なネットワークであり、特に最近、外国発の迷惑メール等国境を越えて送受信される迷惑メールが増加していることから、我が国が国際的な迷惑メール対策の抜け穴とならないよう国際的整合性を一層向上させ、各国との連携の強化に資する制度とすべきと考えられる。

4. 法制度の見直しの在り方

3(3) 法制度の見直しの視点に基づき、具体的に法制度の見直しを検討すべき点としては以下の点が挙げられる。

(1) 巧妙化・悪質化する迷惑メールへの対応の強化

現行の法規制の適用範囲と問題点

現行の法規制の適用範囲

電子メールの送信に関しては、特定電子メール法等により電子メールに特化した規制が行われているものに加え、下の図 30 にあるとおり、その内容や行為の態様により、現行のメディア横断的な法規制の対象とされている。

(図 30：電子メールの送信に関する法規制について)

(1) 電子メールの送信についての規制

規制されている電子メールの送信	根拠法	罰則
受信者が再送信の拒否の通知を行った場合の広告・宣伝メールの送信の禁止 (特定商取引法上の指定商品・指定役務について上記の送信の禁止)	特定電子メール法第4条、第7条、第32条 特定商取引法第12条の3等	措置命令。違反した場合、1年以下の懲役又は100万円以下の罰金 指示。違反した場合、100万円以下の罰金 業務停止命令。違反した場合、2年以下の懲役又は300万円以下の罰金(併科あり)
営業のための架空電子メールアドレス宛の多数の者への電子メールの送信の禁止	特定電子メール法第5条、第7条、第32条	措置命令。違反した場合、1年以下の懲役又は100万円以下の罰金
送信者情報を偽った広告・宣伝メールの送信の禁止	特定電子メール法第6条、第32条	1年以下の懲役又は100万円以下の罰金(1)

(1) 措置命令もあり。

(2) メディア横断的な法規制(電子メールの送信に関わるもの)

規制されている電子メールの送信	根拠法	罰則
名誉毀損、侮辱、脅迫 人の名誉を毀損する多数の者への電子メールの送信の禁止 他人を侮辱する多数の者への電子メールの送信の禁止 他人を脅迫する電子メールの送信の禁止	刑法第230条(名誉棄損) 刑法第231条(侮辱) 刑法第222条(脅迫)	3年以下の懲役若しくは禁錮又は50万円以下の罰金 拘留又は科料 2年以下の懲役又は30万円以下の罰金
風説の流布、業務妨害(信用毀損、株価操作等) 風説の流布等により、信用を毀損し、又は業務を妨害する電子メールの送信の禁止 有価証券等の相場の変動を図る目的をもって、風説を流布する電子メールの送信を禁止	刑法第233条(信用毀損及び業務妨害) 金融商品取引法第158条、第197条	3年以下の懲役又は50万円以下の罰金 5年以下の懲役又は100万円以下の罰金
わいせつ物頒布、児童ポルノ提供等 わいせつ画像データを含む電子メールの送信の禁止 人を児童との性交等の相手方となるように誘引する電子メールの送信の禁止 人に児童買春をするように勧誘する電子メールの送信の禁止 児童ポルノの画像等を含む電子メールの送信の禁止	刑法第175条(わいせつ物頒布等(2)) 出会い系サイト規制法第6条、第16条 児童ポルノ処罰法第6条第1項 児童ポルノ処罰法第7条第1項	2年以下の懲役又は250万円以下の罰金若しくは科料 100万円以下の罰金 5年以下の懲役又は500万円以下の罰金 3年以下の懲役又は300万円以下の罰金
著作権の侵害 著作物の無断配信等著作権を侵害する電子メールの送信の禁止	著作権法第119条	5年以下の懲役又は500万円以下の罰金
ネズミ講への勧誘 業として、ネズミ講に加入することを勧誘する電子メールの送信の禁止 ネズミ講に加入することを勧誘する電子メールの送信の禁止	ねずみ講防止法第6条 ねずみ講防止法第7条	1年以下の懲役又は30万円以下の罰金 20万円以下の罰金
詐欺 架空請求等の詐欺行為の実行の着手となる電子メールの送信の禁止	刑法第246条(詐欺(3))	10年以下の懲役
個別分野における広告 (例)医薬品等の虚偽又は誇大広告、承認前の医薬品等の広告を行う電子メールの送信の禁止	薬事法第66条第1項、第68条、第85条	2年以下の懲役又は200万円以下の罰金又はこれを併科
ウィルスの頒布 ウィルスを添付した電子メールの送信の禁止	刑法第168条の2(不正指令電磁的記録供用(4))	3年以下の懲役又は50万円以下の罰金

(2) 現行の刑法第175条の適用についての判例(横浜地川崎支判平成7年7月14日)あり。また、この行為を条文中明確化するための改正法案が平成16年に国会に提出されたが現時点で未成立。(3) 財物の交付がなされていない場合は詐欺未遂。(4) 改正法案が平成16年に国会に提出されたが現時点で未成立。

例えば、客観的に見て恐怖を感じるような内容のメールを送信した場合、刑法第222条の脅迫罪が成立する可能性があり、2年以下の懲役又は30万円以下の罰金を科されることとなる。

また、有価証券の相場の変動を図る目的を持って、風説を流布する電子メールを送信した場合、金融商品取引法第158条に違反する可能性があり、5年以下の懲役又は100万円以下の罰金を科されることとなる。

ネズミ講への加入を勧誘するもので、「無限連鎖講（ねずみ講）の防止に関する法律」第7条に該当する場合、20万円以下の罰金が科されることとなる。

医薬品や、化粧品、医療機器等について、その効能、効果又は性能に関して、虚偽又は誇大な記事を広告する電子メールを送信した場合、承認前の医薬品等について、その効能を広告する電子メールを送信した場合、それぞれ薬事法第66条、第68条に違反する可能性があり、違反した場合は2年以下の懲役若しくは200万円以下の罰金又はその併科に処されることとなる。

現行の法規制の問題点

このように、現行法においても、問題となる電子メールの送信は、かなりの部分が規制の対象とされている。しかし、最近では、ボットネットの利用やフィッシングメール等の送信など、現行法の規制対象となっている電子メールの送信と比較してもより悪質であると考えられるものがあり、これらについて法規制が十分であるかという点も含め、対応策の検討が求められている。

(図31：現在問題となっており法規制を含め対応策を検討すべき電子メール)

問題となっている電子メールの送信	備考
電子メールの種類が問題となるもの フィッシングメール等の送信	-
電子メールの送信の手法が問題となるもの ボットネットを利用した迷惑メールの送信 外国からの迷惑メールの送信	ボットネットを利用する者が送信者に該当する場合は、特定電子メール法第4条～第6条が適用。 送信地の外国で違法とされている場合等は、外国法の適用の可能性あり。

(注) この他、広告・宣伝メールの送信に関する現行のオプトアウト規制の実効性が問題となっている。

ボットネットを利用して送信される迷惑メールへの規制の考え方

ボットネットを利用して迷惑メールを送信させる行為については、概念上、2つのフェーズに分けることが可能である。すなわち、ウイルスに感染させ、第3者のPCをボット化させる行為（第1フェーズ）と、ボットネットを利用して迷惑メールを送信させる行為（第2フェーズ）である。

ボットネットを利用して送信される迷惑メールに対する法規制の範囲

このうち、前者（第1フェーズ）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」に不正指令電磁的記録作成・供用等に関する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、3年以下の懲役又は50万円以下の罰金が科されることとなる。

他方、後者（第2フェーズ）については、ボット化したPC（ゾンビPCと呼ばれる。）を踏み台として迷惑メールを送信する場合（図35（右）パターン1）には、送信者情報を偽装するためにゾンビPCに迷惑メールを送信又は送信指示を行っており、現行の特定電子メール法第6条において禁止されている「送信者情報を偽った送信」に該当しうるものであり、直接刑事罰（1年以下の懲役又は100万円以下の罰金）の対象となる。

現行法では想定されていない送信形態に対する法規制の考え方

一方、ボットネットに関しては、ボットネットを構築した者が自らのビジネスのために利用していると言われており、ボットの制御手法等の技術革新や、ウイルス作成者とボットネットの指令者、迷惑メールを受信させようとする者等の役割分担の細分化が進み、ボットネットの利用形態は複雑化していると考えられている。

例えば、ゾンビPC自らがボットネット指令者のPCにアクセスし、次に外部サーバへアクセスし、迷惑メールに関する情報を取得した上で、ゾンビPC自身が迷惑メールを送信するケースもあり（図35（右）パターン2）このような場合、ボットネット指令者や、迷惑メールを受信させようとする者への規制は、現行の特定電子メール法では想定されていない。

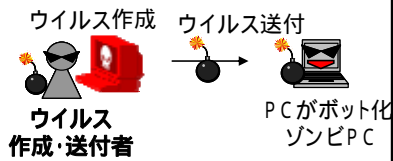
しかし、迷惑メールを送信するという悪質性については、現行法で対象となる送信形態と同様であることから、このような形態のボットネット指令や迷惑メールを受信させようとする行為についても、特定電子メール法等現行法の適用の在り方を含め、規制の方法を検討すべきと考えられる。

なお、迷惑メール送信に利用されるか否かにかかわらず、ボットネットの存在自体が問題であるとの指摘もあり、ボットネットそのものの駆逐に向け

た取組も行っていく必要があると考えられる。

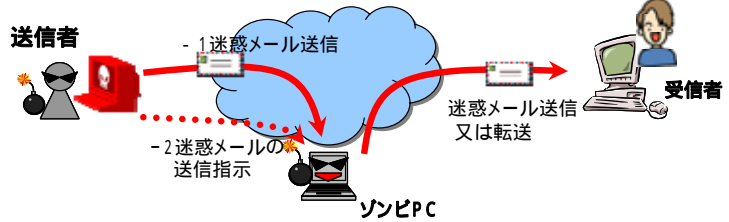
(図 35 : ボットネットを利用した迷惑メール送信に関する規制について)

フェーズ1(ウイルス作成~ボット化)

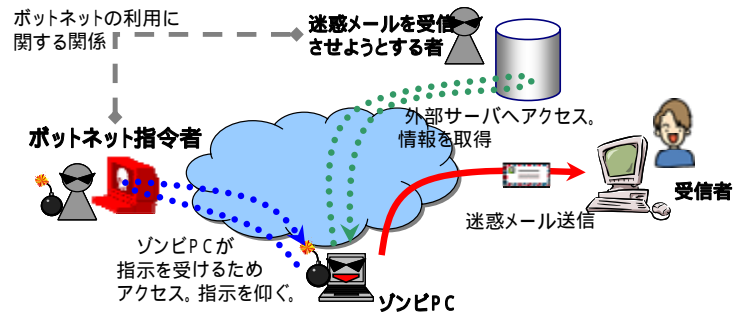


フェーズ2(迷惑メールの送信)

パターン1:ゾンビPCを踏み台として、迷惑メールを送信するケース



パターン2:ゾンビPCがボットネット指令者のPCにアクセスし、次に外部のサーバ等にアクセスし、迷惑メールの情報を取得した上で、迷惑メールを送信するケース

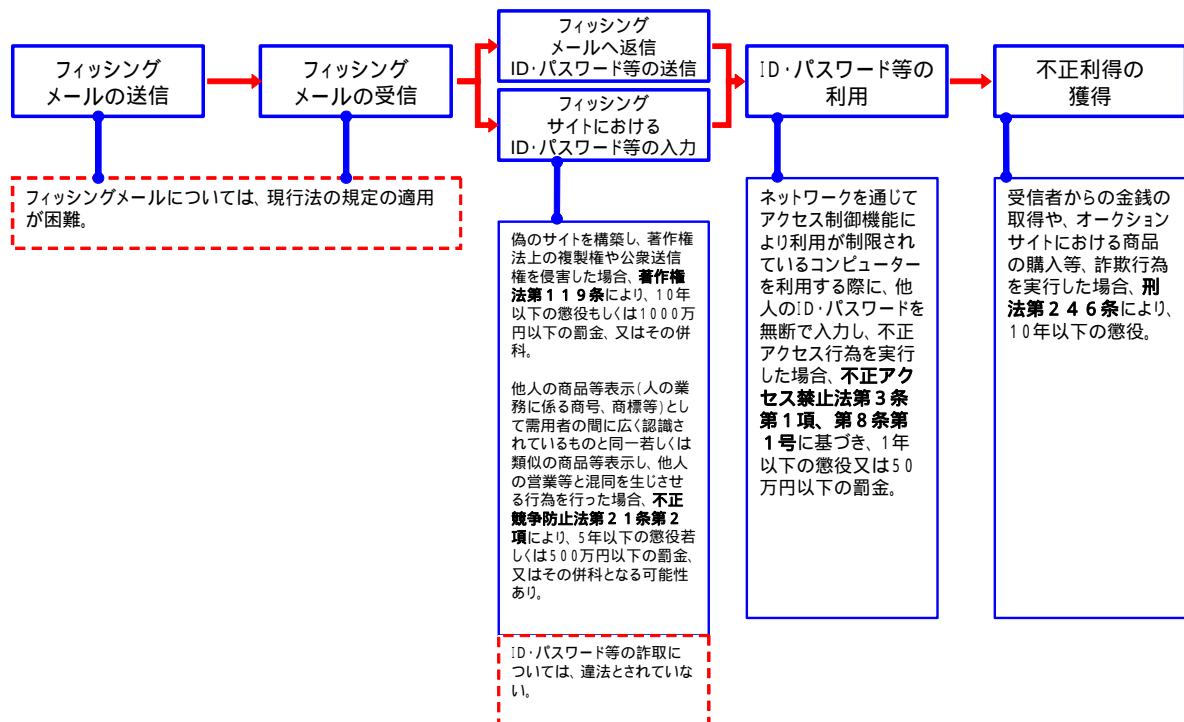


フィッシングメール等に対する規制の考え方

フィッシングメールの送信から被害の発生までの段階について

フィッシングメールの送信から、受信者等に金銭の搾取等の被害が発生するまでのフローと現行法の適用関係を示すと図 32 のようになる。

(図 32 : フィッシングメールに関する法規制について)



具体的には、フィッシングメールの送信から被害の発生までには、フィッシングメールの送信、フィッシングメールの受信、フィッシングメールに対し、ID・パスワード等を入れて返信、又は、フィッシングサイトにおいて ID・パスワード等を入力、ID・パスワード等の利用、不正利得の獲得、という 5 段階に分けて考えることができる。

このうち、については、受信者から金銭ないし財産的利益を取得し、又はオークションサイトにおいて商品を購入する等の場合には詐欺等となりうるものであり、詐欺に該当する場合は刑法第 246 条により 10 年以下の懲役が科される。また、の段階で、偽のサイトを構築し、著作権法の複製権等を侵害した場合、著作権法第 119 条が適用されうるものであり、10 年以下の懲役若しくは 1000 万円以下の罰金、又はその併科となる。

フィッシングメールに対する法規制の考え方

フィッシングメールの送信に対しては、現行法上の規定は極めて適用されにくい。フィッシングメールの流通は、営業活動で電子メールの送信を行う場合の信頼性確保や、インターネット上での取引に必要なものとなっているID・パスワード等の情報に関する電子メールでの利用の信頼性を著しく損ない、電子メールの円滑な利用に支障を及ぼすものであり、高度情報通信社会の健全な発展を阻害するものである。

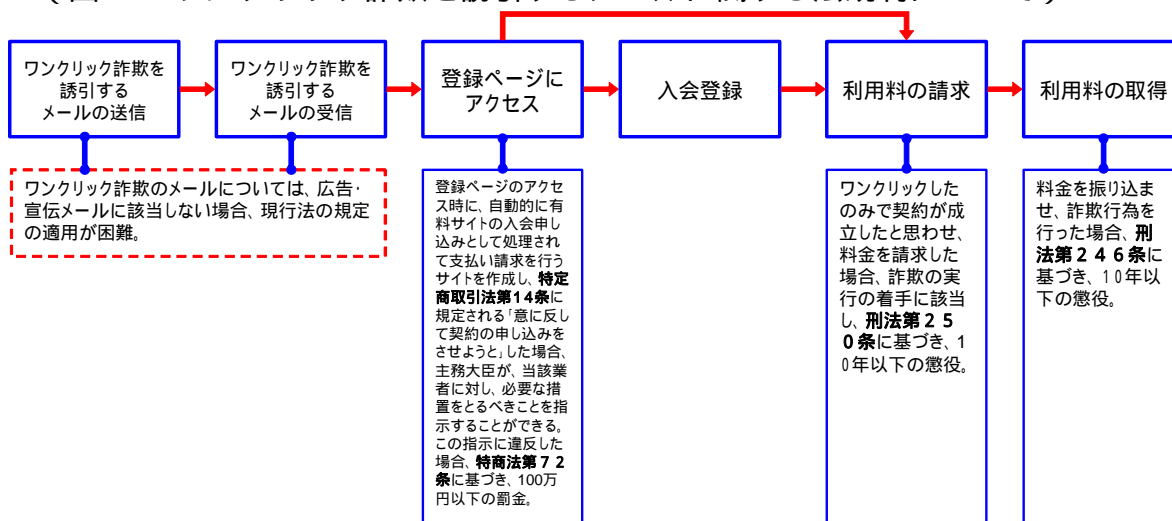
さらに、受信者等の被害の発生に関しては、フィッシングサイトの構築というよりはフィッシングメールの送信が被害発生 of 主要な契機となっており、また、被害の発生がフィッシングメールの送信から連続した行為により極めて短時間で発生するケースが多いため、被害が発生した場合の回復が困難である。

こうしたことから、フィッシングメールの送信についても規制を行う必要があると考えられる。この場合、フィッシングメールは、受信者に望まれない電子メールの大量送信という点で、同意のない広告・宣伝メールの大量送信と同様の性格をもつこと、電子メール以外の方法を契機として、フィッシングサイトへの誘引を図るケースは極めて少ないことから、電子メールを規律する特定電子メール法の改正による対応も視野に入れ、検討していくことが適当と考えられる。

ワンクリック詐欺を誘引するメールに対する法規制の考え方

ワンクリック詐欺を誘引するメールの送信から、受信者等に金銭の搾取等の被害が発生するまでのフローと現行法の適用関係を示すと図33のようになる。

(図33：ワンクリック詐欺を誘引するメールに関する法規制について)



ワンクリック詐欺を誘引するメールの流通は、インターネット上での営業活動に必要不可欠なものとなっているウェブサイトとリンクした電子メールの送受信に関する信頼性を著しく損ない、電子メールの円滑な流通に支障を及ぼすものであり、高度情報通信社会の健全な発展を阻害するものである。

ただし、ワンクリック詐欺を誘引するメールの規制の検討に当たっては、フィッシングメールへの規制の検討の場合と比較して、以下の点に留意する必要がある。

第一に、ワンクリック詐欺を誘引するメールは広告・宣伝メールに該当するものも少なからずあり、その場合は現行の特定電子メール法が適用される。

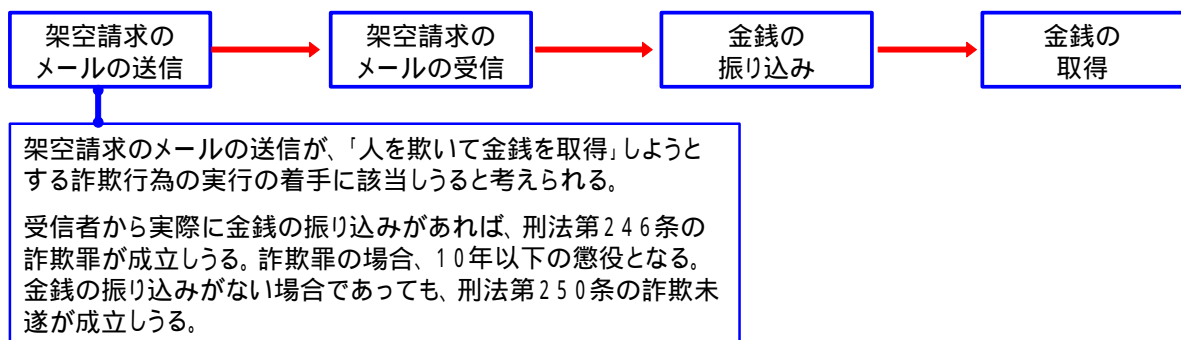
第二に、フィッシングメールが金融機関等信用ある者からのメールを装うのに対し、ワンクリック詐欺を誘引するメールでは、登録用ウェブサイト等への誘導を目的とするため、必ずしも他者からのメールを装うものではない。

しかしながら、ワンクリック詐欺を誘引するメールは、受信者に望まれない電子メールの大量送信という点は、同意のない広告・宣伝メールの大量送信と同様の性格を有している点もあり、特定電子メール法で規制する必要があるかどうかについては、さらに政府において検討すべきである。

架空請求メールに関する法規制の考え方

架空請求メールについては、メールの送信自体が「人を欺いて金銭を取得」しようとする詐欺行為の実行の着手に対応すると考えられるため、受信者からの実際に金銭の振り込みがあれば、刑法第246条の詐欺罪が成立しうる。また、金銭の振り込みがない場合であっても、刑法第250条の詐欺未遂が成立しうると考えられる。このため、新たな規制を設ける必要は少ないと考えられるが、受信者に望まれない電子メールの大量送信という点は、同意のない広告・宣伝メールの大量送信と同様の性格を有している点もあり、この点は留意すべきである。

(図 34：架空請求のメールに関する法規制について)



(2) 現行のオプトアウト方式の見直し

現行のオプトアウト方式については、「迷惑メールへの対応の在り方に関する研究会」(第2次研究会)においても議論があり、平成16年12月の同研究会中間とりまとめにおいては、「迷惑メール対策については、国際的な整合性・協調体制も重要であることから、オプトイン方式の採用国における取り締まりの効果を注視するとともに、我が国でオプトイン方式を採用した場合において電子メールを利用した正当な営業活動にどの程度の影響が生じるか等についても考慮しながら、迷惑メール対策の実効性を確保するためにオプトイン方式の採用の是非について継続的に検討することが必要であると考えられる。」とされた。

したがって、本研究会においても、第2次研究会以降の状況を踏まえた上で、現行のオプトアウト方式の見直し及びオプトイン方式の採用の是非について検討する必要があると考えられる。

現行法の趣旨と施行後の状況

現行法の趣旨

現行のオプトアウト方式は、電子メールというメディアの特性を利用して大量に送信される広告・宣伝メールに対し、広告・宣伝メールの送信の基準を受信者側の拒否の有無とした上で、送信者側に拒否の有無を事前に確認することによる送信者側への負担の大きさや、「未承諾広告」の表示がある広告・宣伝メールに対するフィルタリング処理等の技術的手段への期待から、一度広告・宣伝メールを受信した者から拒否の通知を受けた場合の再送信を禁止することとしたものである。

現行法施行後の状況

しかしながら制度導入後、正当な営業活動の一環として広告・宣伝メールが送信される場合に関しては、受信者側の意識や広告宣伝効果等から、オプトイン的な運用が大勢⁴³となっている一方、技術的手段に関しては、技術的にブロックされると、そもそも広告・宣伝としての意味をなさないとの点から、前提となる表示義務がほとんど守られず、法執行の問題とも相俟って想定された効果を発揮できていないという結果が生じている。

⁴³ 総務省の依頼に基づき、平成19年9月にモバイル・コンテンツ・フォーラムが実施したアンケートによると、広告・宣伝メールを送信する際、事前に受信者の同意を得ていない事業者は1割であった。また、インターネット広告推進協議会等では、自主的なガイドラインの策定を行うなどの対応を進めている。

また、迷惑メールの総量は増加しており、電子メールの送受信上の支障の解消という特定電子メール法の目的は達成されてはいない。

さらに、オプトアウト方式は、受信者からの拒否の通知が前提になるが、拒否の通知がかえって受信者が望まない広告・宣伝メールの送信を招くとの指摘があり、制度が円滑に機能していない。

(図 36 : 再送信拒否通知後の迷惑メールの推移について)

・オプトアウトの問題点として挙げられている送信者に受信拒否の通知をすることがかえって迷惑メールを招くという点について。

2007年8月に(財)日本データ通信協会が実施したWebアンケートにおいて、「今後の受信を希望しない旨の通知を行った後、かえって広告や宣伝を内容とするメールが増えたと感じるか。」と質問したところ、「増えた」と感じている人は45%。

オプトアウトを行った結果、5ヶ月間のうちに、8150通の迷惑メールを受信したとの研究結果。(出典:社団法人情報処理学会研究報告 2005年5月13日 中京大学長谷川明生氏他)

広告メールを受け取らない旨を通知したにもかかわらず広告メールの送信が止まらない、あるいは、当該通知をした結果かえって広告メールが増えてしまったとして、一般の消費者から寄せられた情報提供件数は、2006年度で1866件。

(出典:産業構造審議会特定商取引小委員会第7回会合配布資料)

受信者側の意識としては、95%が広告・宣伝メールを一切受け取りたくないか、送信してくることを同意したもの以外は受け取りたくないという調査結果もあり、そうした点にも留意する必要があると考えられる⁴⁴。

法規制の見直しの考え方

こうした状況の下において、少なくとも受信者側の拒否が推定できるような場合には、本来の立法趣旨の観点から、現行のオプトアウト方式の見直しを行い、オプトイン的な考え方を導入することが適当ではないかと考えられる。

⁴⁴ (財)日本データ通信協会は、2007年8月に電子メール利用者にWebアンケートを実施しており、「今後、広告・宣伝等のメールの受信を希望するか」という問に対して、このような回答結果となった。

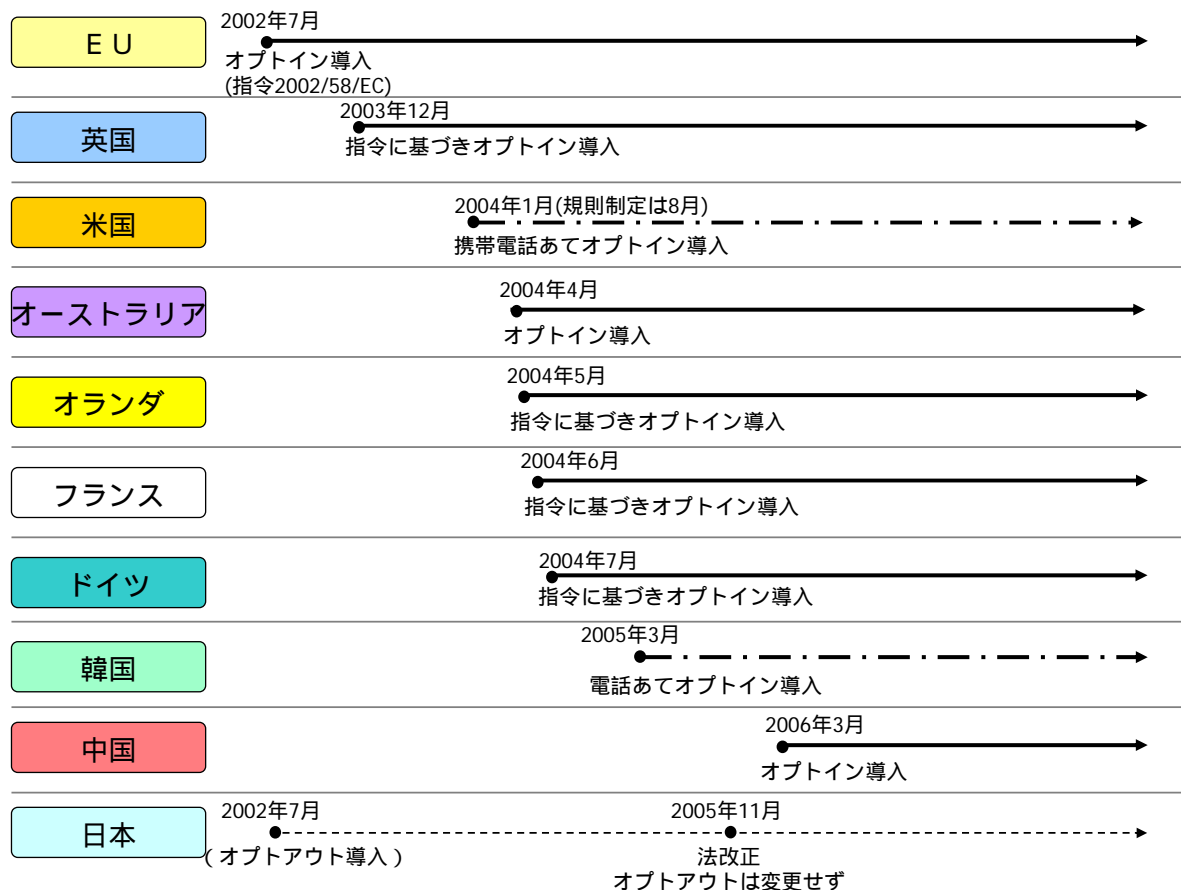
国際的整合性の向上の必要性

特定電子メール法制定時とその後の国際的状況

平成14年(2002年)の制定時においては、特定電子メール法は、迷惑メール対策として世界的にも先駆的な立法であったが、その後、各国で迷惑メール対策の立法が進み、我が国より、迷惑メール対策が強化されている国が多くなっている。

特に、広告・宣伝メールの送信の規制に関しては、主要国では、何らかのオプトイン方式を採用する国が多数となってきている。

(図37: 諸外国におけるオプトイン導入状況)



国際的整合性の向上のための法規制の見直しの考え方

インターネットは国際的なネットワークであり、特に最近、外国発のメール等国境を越えて送受信される迷惑メールが増加していることから、国際的な連携の強化が急務であり、その前提として、我が国が国際的な迷惑メール対策の抜け穴とならないよう、制度的な国際的整合性を向上させることが必要と考えられる。こうした観点からもオプトイン的な考え方を導入することが適当ではないかと考えられる。

営業活動との関係

現行のオプトアウト方式の見直しに当たっては、営業活動における電子メール送信の現状を踏まえ、正当な営業活動の一環として電子メールを送信しようとする者にとって過剰な負担となる方式を避け、規制目的とバランスのとれたものとするべきと考えられる⁴⁵。したがって、仮にオプトイン的な考え方を導入する場合でも、オプトイン的な考え方は必要な範囲で導入することが適当と考えられる。

例えば、現行のオプトアウト方式では取引関係のある者は規制の対象外とされており、こうした点に留意する必要がある。また、企業間（B to B）で広告・宣伝メールを送信する場合についてもオプトイン的な考え方が必要かどうかについてはさらに検討する必要がある。

さらに、オプトイン的な考え方の導入に当たっては、同意の取得の方法や範囲等を定めるべきか、定める場合どの程度のレベルを求めるのかといった点も営業活動と大きく関わってくる点であり、制度の移行に当たっての留意点等と併せ、同意を必要とする趣旨も勘案しつつ、営業活動における電子メール送信の現状を踏まえ、引き続き検討していくべきと考えられる。

見直しの方向性

広告・宣伝メールの送信には、送信先の電子メールアドレスを取得し、その取得した電子メールアドレスを利用して行う必要があるが、この電子メールアドレスの取得の状況により、規制の必要性が変わってくるものと考えられ、具体的には、電子メールアドレスの取得の方法により、

- i) 受信者から直接提供された電子メールアドレスを利用する場合、
- ii) 送信者が（架空も含め）作成した電子メールアドレスを利用する場合
- iii) 送信者が、ウェブサイト上の電子メールアドレスを検索ソフトにより収集（ハーベスティングという。）する等、自らが収集して利用する場合
- iv) 第三者から提供された電子メールアドレスを利用する場合

の4通りに分けて検討することが適当と考えられる。

⁴⁵ 広告・宣伝メールの送信は、営利的言論としての保護を考える必要があり、その規制に関しては「最も制限的でない他の選びうる手段」(least restrictive alternative)である必要があると考えられる。また、米国の判例では、営利的言論の法理として、セントラル・ハドソン基準と呼ばれる基準が示されている（セントラル・ハドソン基準とは、まず、営利的言論が表現の自由保障規定の範囲内に入るためには、それが少なくとも合法的な活動であり、人を欺くようなものであってはならない、次に、そういう合法的活動に関し正確に公衆に情報を与える表現について、主張される公権力側の規制利益が実質的であるか否かが問われる。以上の二つの要件が充足される場合、右規制が規制利益を直接に促進するものか、また、その利益を達成するのに必要以上に広範でないものか否かが、判定されなければならない、との基準とされる。芦部信喜著「憲法学 III 人権各論（1）増補版（2003）」参照）

このうち、i)の受信者から直接提供された電子メールアドレスを利用する場合は、受信者にとって送信者が既知であり、オプトイン方式をとる国でも一定の例外をとっている場合がある。

ii)の送信者が(架空も含め)作成した電子メールアドレスを利用する場合には、迷惑メールの大量送信と送受信上の支障が起りやすく、我が国(現行特定電子メール法第5条)を含め、既に各国が規制を行っている⁴⁶。

iii)の送信者が、ハーベスティングする等、自ら送信先の電子メールアドレスを収集して利用する場合には、オプトイン方式の国においては、送信前に同意を得ることが必要であり、オプトアウト方式の国でも我が国以外の国では、ハーベスティングに関し、何らかの規制を加えている場合が多い。ウェブサイトの巡回により大量の電子メールアドレスの収集ができる現状では、ハーベスティングにより収集された電子メールアドレスを利用して送信する場合も、迷惑メールの大量送信と送受信上の支障が起りやすいと考えられる。

この場合、送信者がハーベスティングにより収集された電子メールアドレスを利用した送信行為をしているのかどうかの確認を行うことは執行上、極めて困難であり、オプトイン的な考え方を導入することが考えられる。

iv)の第三者から提供された電子メールアドレスを利用する場合には、第三者が電子メールアドレスの提供と広告・宣伝メールの送信に関し同意を取得している場合は比較的問題が少ないが⁴⁷、受信者の同意なく第三者から提供された電子メールアドレスを利用して、広告・宣伝メールを送信する場合は問題が多いと考えられる⁴⁸。

この点、オプトイン方式の国では、送信前に同意を取得することが必要になる。また、米国(オプトアウト方式)では、受信拒否の通知を受けた電子メールアドレスの第三者提供の禁止を行っている。ただし、この場合と同じく、同意なく第三者から提供された電子メールアドレスを利用して送信行為をしているのかどうかの確認を行うことが執行上、極めて困難であるため、

⁴⁶ オプトイン方式の国では、明文の禁止規定はない場合が多いが、架空アドレスあてに送信する場合に、事前の同意を取得するのは不可能であり、実質的に行為が禁止されていると考えられる。

⁴⁷ ただし、同意の取得が非常に包括的な場合等は問題のある場合もあると考えられる。

⁴⁸ また、この問題に関しては、個人情報保護法の考え方が準用できるのではないかとの指摘もあるが、個人情報保護法では、個人データの第三者提供は、原則、本人の同意が要件であり、利用目的に第三者提供が明示されていない場合には、利用目的による制限の違反にも該当する。

オプトイン的な考え方を導入して、送信前に事前の同意を求める制度を導入することが考えられる。

一方、第三者が受信者の同意を取得している場合には、比較的問題は少ないが、受信者にとって同意と認識できるような方法で同意取得がなされていない場合には問題が残ると考えられる。

オプトイン的な考え方の導入に当たっては、以上の点を参考に検討を進めることが適当ではないかと考えられる。

なお、オプトイン的な考え方を導入する場合、事前の同意を取得して広告・宣伝メールを送信する場合でも、基本的に、受信者が拒否の意思表示をした場合には、以後の広告・宣伝メールの送信は禁止されることが適当⁴⁹と考えられ、これに必要な仕組みも併せて整備することが必要と考えられる。

また、法の実効性強化という点に関しては、オプトイン的な考え方の導入のみで達成されるものではなく、その他の対策と相俟って効果を発揮するものである点に留意する必要がある⁵⁰。

⁴⁹ オプトイン方式の国では、通常こうした方式となっている。

⁵⁰ ソフォス社の資料（P. 21 参照）によると、迷惑メール発信国の1位米国、2位韓国が共にPCにてオプトアウト方式の国である一方、オプトイン方式の国でも必ずしも迷惑メール発信国の順位が低下していない場合もある。また、MessageLabs社の調査（MessageLabs Intelligence: September 2007）では、オプトアウト方式の国と比べ、オプトイン方式の国において迷惑メールの比率が必ずしも低くはなっていない。

(3) 法の実効性の強化

効果的な迷惑メール対策を行っていくためには、法の実効性の強化が必要である。現行のオプトアウト方式の見直し以外に、法の実効性の強化に資する制度として以下の方向が考えられる。

送信者にとって迷惑メール送信のコストやリスクが高くなる制度

現行法の規定が適用されず抜け穴となっている部分について可能な限り措置を行った上で、迷惑メールに対する措置命令や罰則の適用を増加させられるような制度とする必要があると考えられる。また、迷惑メールの送信に対する制裁の強化については、諸外国で我が国より重い制裁が効果を上げていられる例もあり、我が国の法制度全体との整合性の確保を図りつつ、検討する必要があると考えられる。また、法違反者への捜査や検挙の方法についても、参考にできる事例がないかを引き続き調査する必要がある。

迷惑メールの受信者にとって、迷惑メール受信の防止のコストやリスクがより低くなる制度

迷惑メール防止のための技術的措置が一層容易に利用できるように制度を見直すべき点があれば、見直しを行うべきではないかと考えられる。

電子メールサービスを提供する事業者にとって、自主的な対策を行いやすくなる制度

電子メールサービスを提供する事業者は、フィルタリングサービスの提供や、OP25B や送信ドメイン認証技術等の迷惑メールの送信を防止するための技術の導入、約款等に基づく利用停止等の対策を講じている。法制度とこれらの事業者による対策が有機的に連携することにより効果的な迷惑メール対策となるような制度としていくべきである。

法の執行機関にとって、法執行のための措置が円滑かつ機動的にとりやすくなる制度

法執行の円滑化のため、契約者情報等の入手に関し電気通信事業者等の関係者から協力を得ることができることとするなど、より法執行を円滑にするような制度としていくべきである。

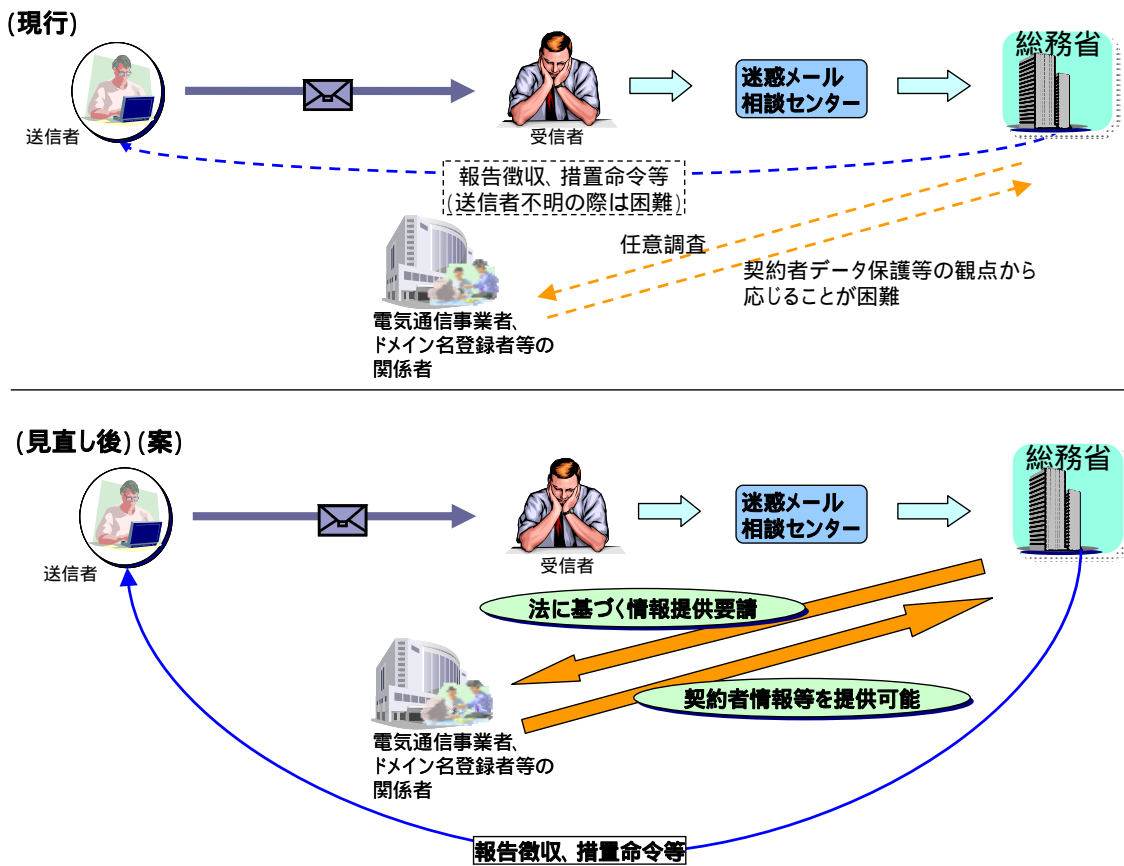
また、措置命令等に関し、より機動的に実施できるような仕組み(例えば、送信者の住所氏名が不明の場合にでも対応できるような制度)があれば、導入すべきであると考えられる。いずれにせよ、送信者の実態が把握しにくいため従来の行政処分の手法がそのまま適用しにくいという電子メールの特性

をかんがみ、制度の体系を検討する必要がある。

さらに、法執行機関の間での情報交換など連携の強化も図るべきであると
考えられる。

その他、迷惑メールの送信に関しては、受信者からの同意の取得や具体的
な送信の指示について、送信を依頼する者が行っている場合もあり、迷惑メ
ールの送信に関わる者全体に対し関係機関による有効な執行が可能となるよ
うな制度としていくべきと考えられる。

(図 38：法の実効性強化の例)



(4) 国際的整合性・連携の強化

近年、我が国で受信する迷惑メールに関しては海外発のものが急増し、国内で受信される迷惑メールの多くが海外発となっている。こうした状況の下において、海外発の迷惑メールに関しても、何らかの措置を講じていくことが必要となっている。

国際的な連携については、前記のとおり、今まで迷惑メールへの対応策に関する情報交換が政府、民間レベルで行われてきた(P.11 参照)。今後は、更に準備の整った国との間で、迷惑メールの発信アドレス等の送信者情報を交換し、迷惑メールの送信者に対する必要な措置を送信国側で行っていくことが妥当と考えられる。

国際的な連携を強化し、こうした措置を講じていく上で、我が国として必要なのは、

)我が国の法制度において、海外発の迷惑メールに関して規制の適用を検討すること⁵¹

)我が国において、迷惑メールの送信国側に迷惑メールの送信者情報の提供等を行うための体制を整備すること

)送信者情報の交換等を行うことについて、外国の迷惑メール対策の主管庁と調整し、相互主義の観点から、我が国から送信され外国で受信される迷惑メールに関しても、相手国側から送信者情報の提供等があった場合には、我が国の主管庁側で措置をとれるような体制を整備すること

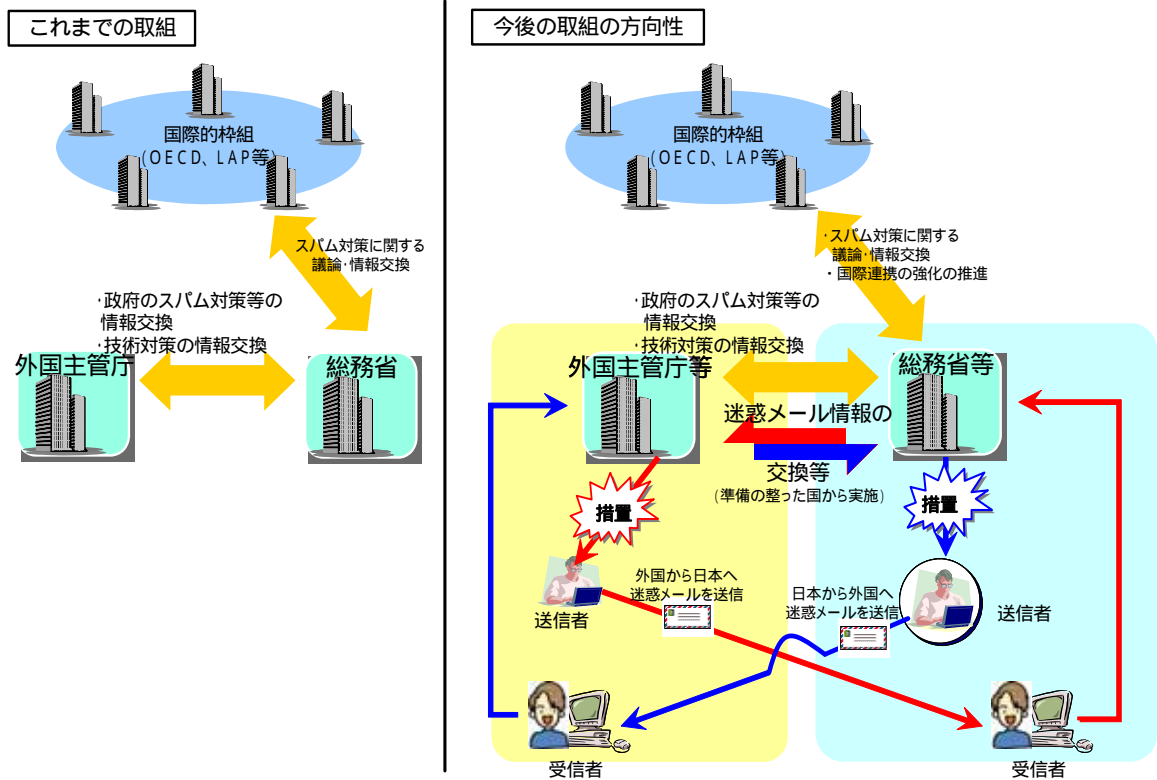
の三点と考えられ、これらの点に対応可能な法制度の見直しを行うことが必要であると考えられる。

また、この取組においては、迷惑メール対策を行う法執行機関同士の連携に加え、民間レベルでの連携も重要であり、官民を問わず迷惑メール対策の国際会議等に我が国からも積極的に参加するなどの取組を進めていく必要があると考えられる。

なお、国際連携の強化を図る上では、相互主義の観点から、我が国発外国宛の迷惑メールの送信に関しても法的な措置を行っていくことが必要であることから、そうした措置の前提となる我が国の法制度についても国際的整合性を向上させ、主要国で違法化されている迷惑メールに対し、できるだけ対応を可能としていくことが望ましい。

⁵¹現行の特定電子メール法では、違法行為の要件を送信行為としていることから、送信行為自体が外国で行われる場合には、特定電子メール法は適用にならないと解される。

(図 39 : 今後の国際連携の方向性)



(5) 法制度の見直しに関する評価

法制度の見直しにあたっては、想定される効果などについて評価を行い、その結果を公表することを通じて、法制度の質の向上を図るとともに、利害関係者のみならず、広く国民の理解を得ることが重要である。そのため、法制度の見直しにより、どのような効果があるのかなどについて、明らかにする必要がある。

5. 今後の検討事項

本研究会においては、迷惑メールへの総合的な対応方策のうち、主に法制度に係る論点について先行的に検討し、その在り方について、本中間とりまとめで提示した。

今後は、その他の検討項目、すなわち、電気通信事業者等が約款等に基づく措置や OP25B・送信ドメイン認証等の技術的解決策の導入を一層進めていく上で、その在り方や課題、フィルタリングサービスの活用の推奨等の利用者への啓発の在り方、民間レベル及び政府レベルでの国際連携の強化の在り方や課題等について引き続き検討を行うことが必要と考えられる。特に、海外発の迷惑メールが急増している現状を踏まえると、国際連携は重要な課題であり、重層的な取組が求められていると考えられる。

また、制度の在り方に関しては、オプトアウト方式の見直しに伴い、受信者の同意の取得が、広告・宣伝メールの円滑な流通にとって、一層重要になってくると考えられることから、同意の取得の在り方等について、引き続き議論を行っていく必要があると考えられる。

法制度の見直しが行われた場合、確実に成果を挙げるため、想定される効果を明らかにするなど評価の在り方についても検討していく必要があると考えられる。

迷惑メールに対する多面的な対策を有機的に結びつけて効果的な方策とし、迷惑メールの流通を抑制・防止できるよう、本研究会として、更に検討を進めていくことが必要と考えている。

「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

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）については、これまでも「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）の厳正な執行や迷惑メール対策技術の積極的な導入などの対策の強化に努めているところだが、一方で、迷惑メール送信者の送信手法が技術革新により巧妙化・悪質化し、新たな手法が出現しており、また、最近は海外から送信される迷惑メールが増大している。このため、現行の迷惑メール対策全般について検証を行うとともに、今後の対策の方向性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) 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 開催期間

本会の開催期間は、平成19年7月から平成20年夏頃を目途とする。

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
- 阿佐美 弘恭 (株)エヌ・ティ・ティ・ドコモ コンテンツ&カスタマ部長
- 五十嵐 善夫 ソフトバンクモバイル(株) 業務執行役員
- 井口 尚志 独立行政法人国民生活センター 相談調査部長
- 井上 恵悟 (社)日本ケーブルテレビ連盟 理事・事務局長
- 岡村 久道 弁護士
- 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
- 坂田 紳一郎 (社)電気通信事業者協会 専務理事
- 佐久間 修 大阪大学大学院 高等司法研究科教授
- 高瀬 哲哉 エヌ・ティ・ティ・コミュニケーションズ(株) ブロードバンド
IP事業部長
- 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
- 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
- 長谷部 恭男 東京大学大学院 法学政治学研究科教授
- 林 一司 ニフティ(株) 技術理事 IT統括本部長
- 別所 直哉 ヤフー(株) 最高コンプライアンス責任者兼法務部長
- 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
- 吉満 雅文 KDDI(株) コンシューマ技術統括本部 プラットフォーム開
発本部長
- (オブザーバ)若林 成嘉 (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	主な議題
第1回	平成19年7月24日	・迷惑メール対策の現状と対応策の検討の方向性について
第2回	平成19年8月22日	・迷惑メールの現状と対策について ・諸外国の迷惑メールに対する規制について ・法制度の在り方についての論点（案）
第3回	平成19年9月27日	・営業活動における電子メールの送信について ・法制度の在り方について
第4回	平成19年10月16日	・中間とりまとめ案について