迷惑メール対策の有効性に関する分析

宿南達志郎

▶1　はじめに

電子メールはインターネットの重要なアプリケーションの一つであり，電子メールが正常に送受信できることが，今後の情報化社会にとって必要欠くべからざるものである。しかしながら，迷惑メールの受信数はやや減少しているとも言われているが，大幅に改善される目処は立っていない。

迷惑メールの実害については，不要なメールの判定や削除にかかる手間や時間，必要なメールを誤って削除するリスク，メール内容による不快感，絶え間なくかつ大量に送り届けられることによるプライバシーの侵害，ウィルスやスパイウェアによるパソコンの被害，ワンクリック詐欺やフィッシング詐欺などによる被害など様々であり，送信者の手口も巧妙化している。

日本の迷惑メール対策については，携帯電話の迷惑メールが社会問題化するなかで，立法化が行われ，2001年の特定電子メールの送信の適正化等に関する法律（以下，特定電子メール法）の制定と特定商取引法の改正が行われたところである。その後，2005年の特定電子メール法の改正によって，一定の成果が現れてはいるものの，大きな進展はないのが実情である。

世界的な動向を見ると，欧米諸国において迷惑メール対策法が相次いで制定され，とりわけEU25カ国においては，2002年の指令（2002/58/EC）に基づき，商業広告メールの事前承諾制（いわゆるオプトイン）を前提とした法律の整備が行われたところである。また，米国ではパソコン着信の迷惑メールについては，事後拒否制（いわゆるオプトアウト）が採用されているが，携帯電話着信の迷惑メール対策はオプトインを採用している。日本の法制度はすべてオプトアウトであり，世界の趨勢とは異なる結果となってしまった。

更に，迷惑メールによる被害状況の把握や，犯罪者の摘発についても，あまり進んでいるとは言えないのが実態である。摘発が進まないのは，組織的な問題，法制度的な問題，申告プロセスの問題など様々である。

技術的な対策も開発されてはいるが，全てのプロバイダーに導入されないと効果があまり期待できないものも多く，従来の対策に加えて，更に総合的な観点からの検討が必要である。そこで，本論文では，日本及び諸外国で実行中の迷惑メール対策の有効性について，法制度の課題，実行プロセスの課題，技術的な課題等を中心に総合的に論じて

●表2-1　迷惑メール発信上位10カ国

国名	2004年上半期	2005年上半期	2005年下半期
米国	60%	51%	56%
韓国	9%	14%	9%
カナダ	6%	7%	7%
中国	4%	5%	9%
ベルギー	2%	3%	4%
英国	2%	2%	3%
フランス	—	2%	2%
日本	2%	2%	3%
スペイン	—	1%	2%
ブラジル	1%	1%	—

Figure & Table

（出典）Sophos社資料

いきたい。

▶2　迷惑メールの実態

（1）海外における迷惑メールの状況

迷惑メールの絶対量や比率は，様々な調査機関が計測あるいは予測を行っているが，その結果にはかなり幅がある。例えば，米国のMessageLabs社の調査によれば，2004年７月のピーク時には94.5%のメールが迷惑メールであった。その後大幅に低下したが，最近はまた上昇傾向にあり，2005年１月では83%となっている。サンフランシスコのCloudmark社が2006年８月16日に公表したデータによれば，１日に送信された30兆の電子メールのうち，92%が迷惑メールである。Cloudmark社は，世界の50の主要プロバイダーに１億のメールアカウントを保護しているが，そのアカウントに送信されたメッセージを分析したものである。

しかしながら，シマンテック社のデータによれば，最近の迷惑メール比率は，概ね50%で推移しているとされる。しかしながら，ISPやクライアントにおける迷惑メール対策ソフトの効果も反映されたデータであるため，上記のMessageLabsのデータと必ずしも矛盾していない。

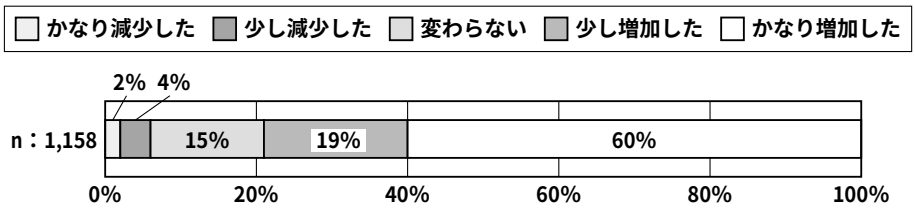
地域別に迷惑メール発信上位地域を見ると，北米，アジア，欧州が上位にいる（**表2-1**参照）。例えば，アジア３国（韓中日）で2004年下半期には15%であったが，2005年下半期には21%に上昇しており，日本は迷惑メールの被害国であると同時に加害国でもある。従って，迷惑メールの受信をうまく拒否する仕組みも重要だが，中韓とも協調して海外に迷惑メールを発信しないような対策も重要である。

（2）日本における迷惑メールの状況

上記の調査結果を見ていると，日本の迷惑メールについてはさほど問題がないように見えるが実はそうではない。最近のアンケート調査などから，迷惑メールの急増が懸念され，実際に，利用者からの苦情申告件数も増加しているからだ。

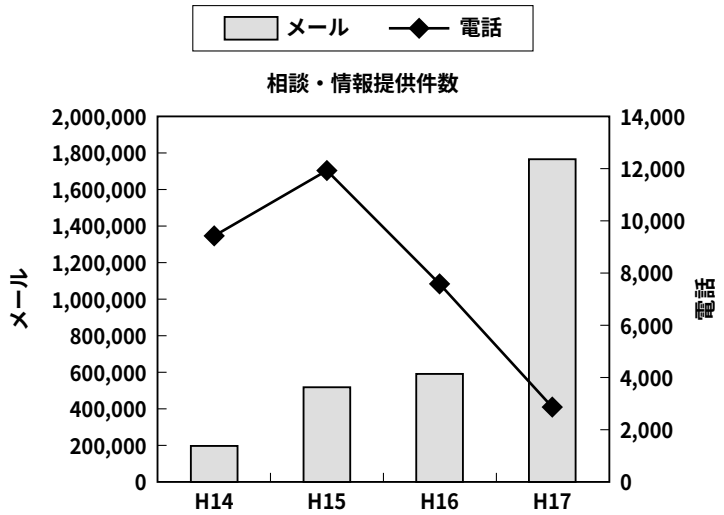
まずは，迷惑メール相談センターによる『平成18年度迷惑メール受信状況についての調査（パソコン版）』（平成18年５月実施）であるが，迷惑メールについて昨年よりかなり増加した利用者の割合が60%と非常に高く，少し増えたを加えるとなんと79%にも及

図2-1　迷惑メールの増加傾向



（出典）迷惑メール相談センター平成18年度アンケート調査

図2-2　迷惑メールに関する相談等件数



（出典）迷惑メール相談センター資料

ぶ（**図2-1**参照）。

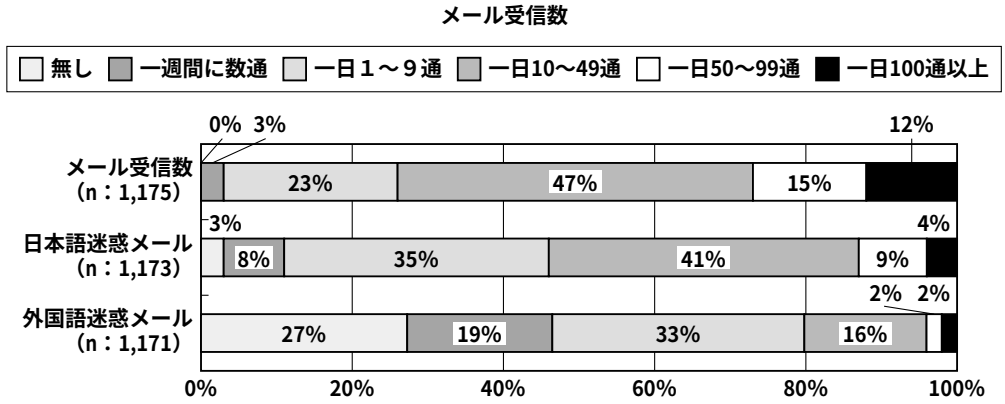
この傾向は，アンケート調査のみならず，迷惑メール相談センターに転送あるいは申告された迷惑メールに関する情報提供数にも示されているのだ。既に，平成17年度は対前年比で約３倍となっているが，更に，平成18年度は平成17年度の２倍にも到達しそうな勢いで伸びているのである（**図2-2**参照）。

量的な増加も問題であるが，利用者は質的な問題にも頭を悩ませている。迷惑メールが不快な理由の上位３項目を見ると，①メールの内容が不快だから，②必要なメールが読みづらくなるから，③詐欺などの犯罪の危険があるから，であり，通数の多さもさることながら，送りつけられるメールの内容に対する苛立ちが示されている。

迷惑メールの受信数は１日10通以上が74%であり，１日50通以上を受信する比率は27%であった。主として日本語の迷惑メールであるが，外国語の迷惑メールもかなり多くなっている。平成17年度の調査では，10通以上は49%に留まっていたので，やはりこの１年で迷惑メールは急増していることが分かる（**図2-3**参照）。

迷惑メールの内容については，出会い系サイトとアダルト系が圧倒的に多く，友達を装ったりエラーメールを装った件名であるものがそれに次いでいる。

図2-3　迷惑メールの受信数と記述言語の内訳



（出典）迷惑メール相談センター平成18年度アンケート調査

▶3　迷惑メール対策の実効性

（1）海外における迷惑メール対策法の現状と課題

（A）米国の迷惑メール対策法

米国では2003年にいわゆるCAN-SPAM法[1]が制定され，受信者の求めていない商業用電子メールに関する規制をしている。正式名称は，許しを得ていないポルノやマーケティング活動を制御する法律であるが，商業電子メールを送る人々のための条件を確立し，スパマーや企業が法律に違反した場合の罰則を規定し，消費者にはメールの送信者は迷惑メールを止めるように依頼する権利を与えている。

CAN-SPAM法は，商業用の電子メール（Commercial Electronic Mail），つまり，商品やサービスの広告や販売促進するためのメッセージの送信についてのものである。既存の取引関係などで既に電子メールの送信について同意が得られていると考えられる場合（transactional or relationship message）には，虚偽の情報や紛らわしいルーティング情報を含まなければ，この法律の適用は免除される。

連邦取引委員会（Federal Trade Commission：FTC）は，全国の消費者を保護する組織であり，この法律の執行を行う権限を与えられている。司法省（Department of Justice：DOJ）は，刑事罰を執行する権限を与えられている。他の連邦政府機関や州の機関は自らの権限の範囲で法律を執行でき，インターネット・サービス・プロバイダー（Internet Service provider：ISP）も違反者を訴えることができる。

一般のPC等からの発信については，善意の商業的な活動の阻害をしないように，オプトアウトが採用され，着信者が拒否の意思表示を行った場合は送信を停止する義務がある。一方，携帯着信の迷惑メールについては，着信者が受信の際の料金を支払わなければいけないことなどを勘案し，オプトインとなっている。

①法律の主要な内容は以下の通りである：

脚注

1．CAN-SPAM法の正式名称は，Controlling the Assault of Non-Solicited Pornography and Marketing Actで，2003年の12月に制定され，2004年１月から施行された。

●虚偽または紛らわしいヘッダー情報を禁止する。電子メールの「From：」欄，「To：」欄，およびルーティング情報は，発信ドメイン名および電子メールアドレスを含めて，送信者を正確に識別できるものでなければならない。
●虚偽の件名表示を禁止する。本文の内容や件名について受信者に誤解を与えてはならない。
●受信者にオプトアウトする権利を与えることが必要である。オプトアウトとは，受信者が将来その送信者からの電子メールメッセージを受け取らないように依頼する仕組みであり，依頼された送信者はその要求通りに行動しなければならない。受信者に対して送信する情報メニューの選択肢を与えることは可能だが，その中には完全に止めるというオプションも必要である。
●送信停止は遅くとも依頼された日から10日以内に行わなければいけない。オプトアウトを要求した受信者の電子メールアドレスを他者に売買や転送することは禁止されている。
●メールは広告であると識別できる明確な符号（ADV：）が付けられなければならない。また，発信者への郵便物送付先の住所を記載する必要がある。また，オプトアウトのための情報が明記されていなければならない。

②FTCによる民事罰の規定

各違反に対しては，最高$11,000までの罰金を適用するが，他の法律に違反している場合には追加の罰金が科せられる場合がある。以下の行為は禁止されている。
●ハーベスティング（harvesting）と呼ばれるが，ホームページ上などに表示された転用禁止のメールアドレスを機械的に収集すること。
●辞書攻撃（dictionary attack）と呼ばれるが，名前やアドレスや数値などを適当に組み合わせて架空の電子メールアドレスを作成すること。
●自動送信を行うためのプログラムを記述し，電子メールを機械的に送ること。
●コンピュータやネットワークに許可なく接続して電子メールを送信すること。例えば，オープンリレーやオープンプロキシを承認なしに利用すること。

③DOJによる刑事罰の規定

DOJは，次の事由により最大５年の投獄を含む刑事罰を求刑することができる。
●別のコンピュータを承認なしで使用し，商業電子メールを送ったこと。
●メッセージについて受信者を欺くか，メッセージの発信者について誤解させるために，多数のメッセージを中継サーバーを経由させたり再送信すること。
●多数の電子メールメッセージのヘッダー情報を偽造し，発信すること。
ここで，多数とは，１日に百通，１ヶ月で千通，１年で１万通以上のことである。
●実際の登録者の情報（ID）を誤魔化すために多数の電子メールアカウントやドメイン名を登録すること。
●実際に商業用に使われている多数のIPアドレスの所有者と偽ること。

（B）米国の法律執行状況

FTCはすでに数百件の発信者を提訴しており数百万ドルの罰金を徴収しているが，全体の迷惑メール規模から考えると必ずしも摘発が進んでいるとは言えない。以下は最近の摘発事例である。

①2005年12月：フロリダ州在住の男性（James McCalla）に対し，２億８千万通を超える違法なメールを原告のCIS社を偽装して送信した罪で，112億ドルの支払いを命じる判

決が出た。

②2006年９月：ミシガンの連邦控訴裁判所は，Daniel Linに対して，１万ドルの罰金と３年間の禁固刑（２年間の執行猶予付きで）を言い渡した。数百万の迷惑メールを送信して，違法なドラッグの輸入や販売を行っていた。この判決の前に，FTCは１万以上の苦情メールをうけて，彼らを摘発し２万ドルの罰金で和解していた。

③2006年９月：バージニア州の控訴裁判所は，世界で８番目にランクされていた悪名高いスパマーであるJeremy Jaynesに対し2,500ドルの罰金と懲役９年の判決を下した。これは，Virginia州の反迷惑メール法に基づくものであった。

このような成果を踏まえて，FTCは2005年の12月に議会に対して，CAN-SPAM法の有効性についてポジティブな報告を行っている。しかしながら，必ずしも国民的な同意が得られているわけでもない。迷惑メールの比率は下がっているが，絶対量はさほど減少していない。

FTCの評価の客観性を疑わせるデータとしては，MxLogic社の調査レポートなどがあるが，CAN-SPAM法を遵守したメールの比率が激減しているという。昨年の平均では何とか３―４％を保っていたが，2006年７月には0.75%，８月には0.35%，そして９月には0.27%と大幅に下がっっている。また，全メールに対する迷惑メールの比率も７―８月には72%であったが，９月には77.4%に上昇しているとのことだ。

また，この法律が施行される以前は，カリフォルニア州などいくつかの州では，でオプトイン規制が行われており，それらの州にとっては規制が緩まったことになる。更には，迷惑メールの悪質化や国際化に的確な対応を行う必要があり，FTCは新たな法案“US SAFE WEB ACT”を提案したが，成立には至っていない。

（C）EUの迷惑メール対策法とその執行状況

EUでは2002年に加盟各国に対して，自然人についてはオプトイン，法人については原則としてはオプトインだが，オプトアウトを選択しても良いという内容の指令を出した。その指令では，各国が法律を制定するタイムリミットは2003年10月となっていたが，若干遅れた国もあったようである。

①英国：2003年12月に施行された“The Privacy and Electronic Communications（EC Directive）Regulations 2003”によって，地方の裁判所（magistrate's court）では5,000ポンドまでの罰金，陪審の場合は無制限の罰金が科せられることになった。しかしながら，刑事罰は科せられない。

オプトインについては，既に送信者が営業活動などを通じて受信者のメールアドレスを入手しており，既に販売を行っている商品と類似の商品であれば，事前の同意がなくてもメールの送信が可能（ソフトオプトインとも呼ばれる）とされている。この規定については，送信者が恣意的に類似品の拡大解釈を行う可能性があり，反対論もあった。

米国と同様に，電話とFaxの着信拒否リストの設定（“Do-not-call-List”と呼ばれる）は義務付けられているが，メールに関してはそのリストは義務付けられていない。

②イタリア：2003年の迷惑メール規制法により，違反者には３年までの懲役と最高９万ユーロの罰金が科せられる。罰金の水準はEU内では高いレベルである。

③オーストリア：2003年のテレコミュニケーション規制法の改正（第107条）で，事前の同意のない電子メール送付は，広告目的の場合または50以上の受信者に向けられている場合に違法であるとされた。また，広告は商業目的に限定されておらず他国より幅広い概念である。

④オランダ：MessgaeLab社の調査（2005）によれば，先進国における迷惑メール比率の

低さでが，シンガポール，日本などに次いで６位となっている。2005年には41件の捜査を行い，そのうち31件が迷惑メールであった。６社に罰金を課し，金額は2,000ユーロから27,500ユーロであった。他にも21件の警告を発している。そのような努力により，2005年の第４四半期には2004年の第一四半期と比較した迷惑メール減少率は85%という驚異的な減少に結びついた。

（D）オーストラリアの対策法と執行状況

オーストラリアの法規制は最も厳格であると言われている。海外発信の迷惑メールも規制対象であり，罰金も初犯は最大22万豪ドルであるが，再犯であれば最大110万豪ドルまで科すことができる。規制を行っているのはThe Australian Communications and Media Authority（ACMA）である。2006年３月までに，10社に対して警告文書を発出し，５つの企業または個人に対する改善命令を出した。また，13種類の罰金を５社に対して課したほか，以下のような事例がある。

2006年４月には迷惑メール対策法制定以来最初の判決が出た。5,600万通の迷惑メールを送信した罪で2005年４月に起訴されていたスパマーWayne Mansfieldに対してである。

2006年９月には，オランダの規制当局（OPTA）との協力で，医薬品（Viagra）販売用に20億通もの迷惑メールを送信していた犯人の捜査を開始した。

迷惑メールの申告プロセスについては，簡素化するソフトを政府機関が提供しておりSpamMATTERSと呼ばれるメールソフトのAdd-inをインストールしておけば，ボタン一つで迷惑メール申告が可能となっている。約１年半でのWebからの申告が30万件であったのに対し，このメールソフトによる申告は88万件に達したという。

（2）日本における迷惑メール対策法の現状と課題

（A）特定電子メール法

本法律は2001年に迷惑メールが大きな社会問題となっていたことを受けて，議員立法により2002年７月１日に施行された。特定電子メール法は，受信者の同意を得ずに送信される広告宣伝メールを「特定電子メール」と定義し，その送信をする者に対して一定の表示義務を課す等の措置により電子メールの利用環境の整備を図る目的で制定された。

主な内容は，表題部への「未承諾広告※」の表示，受信者が拒否通知を行った場合の再送信禁止，架空アドレスあて送信の禁止，設備への著しい支障などによる電気通信役務の提供の拒否，措置命令や罰則，そして３年以内の見直し規定などであった。

同じ時期に制定された特定商取引法の類似性と差異は**表3-1**の通りであり，公正な取引の観点から消費者保護を目指す特定商取引法と電子メールという通信手段の円滑な提供を目指す特定電子メール法という差はあるが，２つの法律と主管組織が必要なのかどうかは疑問がある。

（B）特定電子メール法の改正

①研究会による見直しの検討

「迷惑メールへの対応の在り方に関する研究会」により，法律施行後の評価と見直しの方向性が議論され，2004年10月の「中間とりまとめ」で法制度見直し案が固まった。

中間とりまとめでは，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であるとされた。

●規制対象の拡大：事業用メールアドレスへの送信，携帯電話のショートメッセージ（SMS），についても特定電子メールの定義に含める。

●表3-1　特定商取引法と特定電子メール法の比較

		特定商取引法	特定電子メール法
法目的		取引の公正及び消費者保護の観点から広告規制	電子メールの送受信上の支障の防止の観点から送信規制
規制対象メール		通信販売等の商業広告メール（指定商品等に限る）	一時に多数送信される広告宣伝メール（SMS等を除く）
規制対象者		販売業者及び役務提供事業者等（広告代行業者は除く）	送信者（委託をした者は除く）
規制内容			
	表示義務（共通事項）	・件名欄に「未承諾広告※」 ・販売業者等のメールアドレス，住所等 ・受信拒否の方法	・件名欄に「未承諾広告※」 ・送信者のメールアドレス，住所等 ・受信拒否の方法
	（個別事項）	・取引条件等	・経路情報
	再送信禁止	○	○
	架空メール対策	—	・架空メールアドレスによる送信禁止 ・電気通信役務の提供の拒否
	Webサイト規制	・虚偽誇大広告の禁止 ・意に反して契約の申込みをさせようとする行為の禁止	—
主務大臣		経済産業大臣及び事業所管大臣	総務大臣

Figure & Table

（出典）総務省資料

●架空アドレスへの送信禁止：広告宣伝以外の内容も対象とする。
●直罰：悪質な送信行為については直接刑事罰を科す。

②法律の改正

改正法の４つのポイントは以下の通りである。（2005年５月13日に成立し，2006年の11月１日に施行）

●特定電子メールの範囲の拡大

導入時には携帯電話へのメールが問題となっていたが，現在ではパソコン向けや事業所向けへの迷惑メールが増大しているため，事業所向けにも対象を拡大するとともに，携帯のSMSも範囲に含める（省令改正により対処する）こととした。

●架空アドレスあて送信禁止範囲の拡大，及び措置命令違反の罰則引上げ

架空アドレスあての送信については，知人を装う，エラーメールを装う，空メールを送信するなどの手口が増えており，送受信設備への負荷は目的に関わらずかかって来るため，自己又は他人の営業のため多数のメールを送る行為を全て禁止した。また，罰則についても，これまでの50万円から100万円以下または１年の懲役に引き上げる。

●送信者情報を偽って広告宣伝メールを送信する行為に対して直罰を導入

第三者のアドレスや存在しないアドレスなど真のアドレスと異なる偽装が増加したため，送信者情報を偽って広告宣伝メールを送信することを禁止した。送信情報とは，電子メールアドレスとIPアドレスである。違反した者には１年以下の懲役または100万円以下の罰金という刑事罰を直接科すことができる。従って，警察等が直接捜査を行えることから，裁判所から令状を取得することによって通信履歴の閲覧が可能となる。送信者を特定できる可能性が高まると期待されている。

●電気通信事業者による迷惑メール送信者に対する役務提供拒否事由の拡大

旧法では，メールサーバーの停止などの場合にのみ役務の提供が拒否できるとしていたが，電子メールの送受信が大幅に遅延する場合なども正当な理由に加えられた。

（3）日本における迷惑メール法制の有効性

（A）スパマーの高度化に対する対応

2002年の迷惑メール法制定後一時は迷惑メール数が減少したが近年は再び増加傾向を示している。現在の迷惑メールの送信者の約４割はボットと呼ばれるゾンビ化した多数のPCからの送信であると言われており，送信したPCをコントロールするスパマーを発見するのが困難になっていることも原因の一つである。

（B）オプトアウト方式の限界

オプトアウトかオプトインかについては法律制定時も様々な意見があったが，早期の法律制定を優先してオプトアウト方式を採用した。今回の改正時にも同様な議論があったが，有効性が不明確であること等によりオプトインの導入は見送られた。

しかしながら，オプトアウトの場合には，受信者が拒否登録をするための膨大な作業時間が必要となる。また，仮に拒否通知を行ったとしても，「生きたアドレス」として他社に売買される恐れがあり，根本的な対策とはならない。

（C）迷惑メールの規制対象が限定的

規制対象となるのは，「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」であり，送信者が「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」（２条２号）に限定されているため，知人からのメールを偽装した場合には，対象外となってしまう恐れがある。

更に，架空請求（ワンクリック詐欺）やフィッシング詐欺のためのメールが増加しているが，これらについても本法の対象外となっている。

（D）スパマーの摘発件数が少ない

2002年の法律施行後に総務省から措置命令が出たのはわずかに３回である。いずれも，その件名欄に「未承諾広告※」と正しく記載せず，また「＜送信者＞」の表示及び送信者の氏名又は名称の表示を行っていないなど，特定電子メール法第３条に定める表示義務に違反によるものだ。メールの内容は出会い系であった。

１件目は，2003.11.11で，中野区の事業者に対し，2002年８月から2003年９月の間の送信について。２件目は，2004.4.26で，新宿区のエス・アイ・エス・ワールド社に対し，2003年７月から2004年２月までの間の送信について，３件目は，大阪市北区のコスモメディアサービス社で，2005年４月から６月の間の送信に対してであった。罰金も50万円以下であり，効果についてはやや疑問がある。

一方，経済産業省も特定商取引法違反で行政処分を行った事例が３件（５社）ある。

１件目は，2003年10月７日に，杉並区のリメイン社と中野区のアクセス・コントロール社に対し，特定商取引法第11条違反として，是正の指示が行われた。違反内容は，：①表題部への「未承諾広告※」の不表示，「未 承 諾 広 告 ※」「未承諾広告※」，「※未詳諾広告※」等の不適切な表示。②メール本文中への消費者から受信拒否を受けるための電子メールアドレスの不表示③メール本文中での事業者名不表示であった。

２件目は，2005年６月における，３ヶ月の業務停止命令を含む是正指示であった。(有)エス・ケー・アイ及び(有)アジアン・オアシスという，出会い系サイト・アダルト画像サイト事業者２社に対して，表示義務違反での処分である。

３件目は，2006年３月31日に，出会い系サイト運営事業者（荒居利栄）に対する１か月の業務停止命令を発したものである。表示義務違反と虚偽広告の違反であった。

このほか，平成15年度だけでも2,800件の警告メールが送られているが，送信者の特定が難しいことなどから，行政処分を行ったのはわずかに２件である。通信販売の新たな課題に関する研究会が平成17年１月に発表した「迷惑メール対策の今後の方向性について」においても，行政の役割としてISPや携帯電話事業者と連携し迷惑メール送信者のサービス利用停止等を推進すべきである，と述べるに留まっている。

総務省も経済産業省も，登録適正化機関などからの情報に基づき，発信者への警告やISPへの情報提供は行っているが，犯人が懲役刑となった例は未だない。ISPの利用停止はあくまで約款レベルの自主規制であり，迷惑メールに対する抑止効果は限定的だと考えられる。

（E）迷惑メール追放支援プロジェクト

経済産業省は総務省等と連携して2005年２月から「迷惑メール追放支援プロジェクト」を開始した。経済産業省が特定商取引法違反を認定してISPに情報提供した件数は1,278件（６月10日現在）に達している。ISP迷が惑メールの送信者を利用停止にしたり，ウェブサイトを削除したりするための支援が可能となった。また，金融機関に対しても不正預金口座として凍結を促す狙いもある。

▶４　迷惑メール対策技術の進歩と今後の課題

ここではISPの迷惑メール対策の技術動向とスパマーの手口などについて述べていきたい。

（1）送信者認証

迷惑メールの原因の一つは送信者詐欺（なりすまし，スプーフィングとも呼ばれる）である。現在のSMTPプロトコルでは，指定した宛先に届けることが最優先され，送信者に関する情報のチェックは完全ではない。

このことに対する対策としては，IPアドレスによるドメイン認証と電子署名による認証の２つの方式の標準化が行われている。IPアドレスによるドメイン認証は，ホストのIPアドレス情報を公開するSender-IDと呼ばれる方式の検討が進められてきたが，規格化作業は頓挫している。もう一つの方式は公開鍵を利用した電子署名による認証である。

IPアドレス方式は，メーリングリストサーバー等でのヘッダーや本文の書き換えに強く，電子署名は転送等に強いという特徴がある。Japan Email Anti-Abuse Group（JEAG）では，この技術を積極的に普及させるため，SPF（Sender Policy Framework）と，DKIM（Domain Keys Identified Mail）の２つの方式のいずれかを導入することを提案を行っている。

（2）アウトバウンド・ポート・25番ブロッキング（以下OP25B）の導入効果

迷惑メール送信者は，契約先のISPのメールサーバーを経由させずに，動的IPアドレスを割り当てられた自前で設置したサーバーから直接送信するのが一般的である（Biglobeの場合は，送信された迷惑メールの約９割）。この時にポート番号25を利用するが，そこからの送信を制限する方法がOP25Bである。この機能を導入するためには，一般のメール利用者は，メールソフトの設定変更（ポート番号を587に変更）をしなければいけない。

ある事業者が携帯電話着信向けのメールに対して，2005年10月１日から18日にかけてOP25Bを導入したところ，対策を講じた事業者からの発信はゼロになっており，非常に効果があることが示されている。

しかしながら，この方法も万能ではない。OP25Bにより自らのネットワーク内にいる

動的IPアドレスからの発信はブロックできるが，他のISP内の動的IPアドレス利用のスパマーからの発信はブロックできない。

そこで，OP25Bが完全導入されるまでのつなぎとして，一部のISPで導入が始まったのがIP25B（Inbound Port 25 Blocking）と呼ばれる技術である。他のISPが管理する動的IPアドレスを個別に問い合わせする必要があり，海外のISPからの協力を得られるかどうかが課題だ。

また，既にスパマーはOP25B対策を取り始めているようである。ボットに対して，ISPのメールサーバーを経由させるように指示を出し，小刻みな送信を行うことによりISP側が一般のメール送信との識別を行うことを困難にするやり方である。

（3）スパムゾンビの拡大とその対策

迷惑メール業者が，他のPCにスパイウェアやウィルスなどを送り込み，自らが遠隔操作して迷惑メールを送らせることができる状態のPCをゾンビと呼ぶ。利用者がゾンビ化していることを気づかない場合も多く，ISPへの対策強化と利用者教育が課題となっている。すでに100万台以上がこのネットワーク（ボットネットと呼ばれる）に組み込まれていると言われており，捜査当局も送信元の洗い出しに躍起となっている。

また，構築したボットネットを貸し出す犯罪者も現れ，DeepSight社の調査によれば，15万台クラスのボットネットの使用料がわずか300ドル程度であることが分かっている。ボットに感染するPCの多さはブロードバンドの普及率などに関連があると考えられるため，利用者環境におけるファイアーウォールソフトの導入などの対策も必要である。

次の**表4-1**にあるように，迷惑メールの送信数の多い国とボット感染数には相関関係があるようだ。2006年５月には，韓国で16,000のボットネットを操り，133カ国に向けて毎日1,800万通の迷惑メールを送信し続けた男が逮捕された。韓国発信の迷惑メールは世界の１割を占めており米国，中国に次ぐ世界で３番目の迷惑メール大国である。

（4）トラフィックシェーピング

トラフィックシェーピングとは，発信元のIPが既知の迷惑メール発信源として特定された場合に，どの接続を許可，拒否，抑制するかを選択的に決定する方法を言う。この方法はメールサーバーより上位のフィルタリングであるため，大量のトラフィックをさばくISPや大企業にメリットがある。

●表4-1　ボット感染したコンピュータの割合ワースト10カ国

	国名	ボット感染PCの割合 2005年７―12月（上半期）
2（1）	英国	22%（32%）
1（2）	米国	26%（19%）
3	中国	9%（ 7%）
6（4）	カナダ	4%（ 5%）
4（5）	フランス	4%（ 4%）
5（6）	韓国	4%（ 4%）
9（7）	ドイツ	3%（ 4%）
10（8）	日本	2%（ 3%）
8（9）	スペイン	3%（ 3%）
7（10）	台湾	3%（ 2%）

（出典）シマンテック「インターネットセキュリティレポート（2005年）」

Figure & Table

（5）ブロッキング，スロットリング

ゾンビは一時拒否エラー（tempfailng）を返すと再送してこないという特性があり，再送を行ってきたものだけを受信する「お馴染みさん方式」が有効であることが確認されている。同様な方式として，セッション中に得られる差出人，受取人，IPアドレスの３情報を検査するグレイリスティングという手法もある。

また，迷惑メールは高速大量配信を行うためにタイムアウトの時間が短いという特徴があり，これを利用した対策としてセッションの応答を10―15秒遅らせるスロットリングという手法もある。

（6）フィルタリング

様々なフィルタリング技術が開発されているが，それぞれ一長一短があり，ISPにより提供機能が異なっている。

●送信者アドレス，件名等によるフィルタリング

メールアドレスやキーワードなどを設定してフィルタリングを行う方法である。ソフトによっては，指定するアドレス数の制限などがある。

●送信元情報によるフィルタリング（Source Blocking）

外部機関の提供するブラックリストによるフィルタリングや，信用度（レピュテーション）データによるフィルタリングなどがある。

●本文を参照したフィルタリング（Content Blocking）

受信者が迷惑メールと判定したデータに基づき統計学的に判定するベイジアンフィルター，受信者が登録したキーワードによるキーワードフィルタリング，ヘッダーや本文を解析しそのスコアによる判定を行うヒューリスティクフィルタリングなどがある。

▶５　今後の迷惑メール対策のあり方

諸外国の迷惑メール規制をまとめると**表5-1**のようになるが，やはり大きな違いはオプトアウトかオプトインの差である。EUの25カ国は自然人についてはオプトインで統一されているが，法人については加盟各国の裁量に任されている。法人については，自然人と区別する必要はないとするドイツなどと，法人は自然人とは取引関係などが異なるので区別してオプトアウトにするイギリスなどと，商業的なメール以外でも規制の対象とする（但しオプトアウト）オランダなどといくつかの方針の差が見られる。

また，米国においては，携帯電話着信については，オプトアウトを採用している。すなわち，全ての迷惑メール対策がオプトアウトなのが，日本の法規制特徴であるが，その効果については特定電子メール法の導入時から疑問の声が上がっていたのである。

（1）オプトインの導入に向けて

このような状況であるので，オプトアウトの有効性や，オプトインの導入のメリットなどを検討してみたい。まずはオプトアウトの有効性について考えてみる。

（A）オプトアウトは本当に可能なのか？

ここで，実際に受信した迷惑メールに対し，オプトアウトの意思表示を行う実験を試みた。必須であるはずの「未承諾広告※」の表示もない，ある１日分の迷惑メール（37通）についてである。知人や情報提供を装ったタイトルがつけられており，会社の名前や電話番号は本文中にもなく，拒否通知アドレスが記載されているのは９通であった。また，見かけ上は別の発信者を装っているが，広告宣伝の対象となるリンク先や拒否通

●表5-1　諸外国における迷惑メール規制の比較

	パソコンへの発着		携帯着信
	自然人	法人	
EU	オプトイン	原則はオプトイン （国によってはオプトアウトを選択可）	オプトイン
米国	オプトアウト	オプトアウト	オプトイン
日本	オプトアウト	オプトアウト	オプトアウト

（出典）各種資料より筆者作成

Figure & Table

知のメールアドレスが同一であるものも多かった。

記載された拒否通知アドレスに対して拒否の意思表示を行ったが，送信される迷惑メールの数は，減るどころかかなり増加した。では，スパマーの行動パターンを推測してみよう。まず，拒否通知が到着した場合には，次の送信時に別の送信者名とメールアドレスを使用すれば，「拒否通知後の再送信禁止」に違反しているという訴えから逃れることが可能である。また，拒否通知を行ったことにより，スパマーは，そのアドレスへのメールがISPやメールソフトのフィルターで排除されていないと解釈する。そうすると，同じスパマーが配信している他の別の迷惑メールの送信リストにアドレスを追加するか，該当のメールアドレスを有効性の確認済みのものとして転売することが考えられる。

このように，一度スパマーのターゲットになると，その後の受信メールを減らすのはほとんど不可能である。従って，オプトアウトという制度は実効性がほとんどないものと言える。このことは，迷惑メールセンターや消費生活センターでは既に常識化しており，善良な企業であると確認できる場合を除き，迷惑メールに対してオプトアウトすることは止めるように指導しているのである。

このように，オプトアウト制度を維持するということは，悪意のある配信者に対抗する手段を受信者が持ち得ない状態を黙認することになる。オプトインのメリットは，少なくとも受信者が送信者の反応に関わらず迷惑メールの着信拒否権を獲得できる点である。また，苦情受付機関の事務処理も，基本的に申告があった時点で違法の疑いが強いため，シンプルになり，申告数も大幅に増加して実態把握が容易になるメリットもある。

（B）オプトイン導入にむけて

EU25カ国を初めとして，オーストラリア，スイスなど世界の主要国では，オプトインが採用されている。また，米国でも携帯電話着信の迷惑メール規制には，CAN-SPAM法に基づいてオプトアウトが採用されている。カナダでは迷惑メール対策法という独立した法律はないが，2005年のTask Force Reportでオプトインの提案がなされている。

オプトアウトのメリットは，営業の自由を保証できるという点にある。郵便によるDMやポストへの投げ込み広告などは自由であり，それらとのバランスを取るためには電子メールも拒否されるまでは送信する自由を維持することが望ましいという考え方である。

一方，オプトインのメリットは，商業広告の受け取りについて，受信者が事前に自らの希望を反映できることである。善良な企業であれば，可能な限り，その広告を見たがっている受信者にターゲットを絞って送りたいというのが普通であり，それが営業の自由を奪うとは考えにくいからである。

迷惑メールが，郵送されるDMや個別配達される投げ込み広告と異なるのは，量と質の差である。量が多いのは，迷惑メールはその送信コストの安さに注目し，0.001%でも販売等ができれば儲かると言われているのだが，確率を無視してひたすら入手したアドレスにメールを毎日送り続けるビジネスモデルだからである。

しかも，インターネットのメールアドレスのみに基づいて情報を送信するので，ほとんど個人の属性や好みに関係ない一方的な押し売りや押し付けである。日本語の迷惑メールはアダルト系，出会い系が大多数で，見出しを読むだけでも恥ずかしくなったり不快になる。英語の迷惑メールは医薬品やソフトウェアの安売りなどが多いが，意味不明の文字の羅列だけの愉快犯的メールもある。

いずれも，特定電子メール法に定められた発信者情報（メールアドレス，会社名，住所など）を記載していない違法メールで，「無料で交際相手を紹介」とか「相手は社長なので報酬を支払う」など現実離れした虚偽の内容のメールがほとんどである。つまり，善良な企業はそのような迷惑メールと一線を画したいので，顧客の希望を聞いてから（つまりオプトイン）でないと，情報提供や広告のメールは配信しないのが通常である。中小企業を育成するためにオプトアウトが必要だという意見も聞くが，普通の中小企業はホームページに来訪したお客を中心に情報提供を行ったり，メールマガジンへの広告などで営業を行っている。どこから入手したか分からないような，不特定多数のメールアドレスへの一斉送信を行っている事例はほとんどないだろう。

総務省が2006年の７月に「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」へのパブリックコメントを実施したが，その中でもオプトインの導入意見が数多く出されていた。オプトアウトを維持すべきという意見はわずかに３件であったが，オプトインを導入すべきという意見は38件あった。それらのコメントに対する総務省からの反論は，FTCの議会へのレポートで「英国でオプトインが導入されたが，迷惑メールが減少したという結果は出ていない」という主張などを根拠にしていた。また，大きな制度変更になるので，効果があるかどうかを確認したいとも述べられていた。

しかしながら，オプトインが導入されてから日が浅いが，オランダでは大幅に迷惑メールが減少していること，FCCの担当者へのヒアリングでも，元々CAN-SPAM法に基づいて携帯はオプトインにしたのだが，その政策を採用したことは正しかったと考える，と述べていた。

経済産業省とも意見調整をしなければならない大きな制度変更にはなるが，遅くとも改正法施行後３年以内の見直し時期である2008年には，オプトインへの見直しを前向きに検討するべきである。ちなみに，EUの2002年の指令18条において，国内法の整備の期限である2003年の10月から３年以内に，この指令の導入後の状況についてEU議会への報告が義務付けられている。国内法の整備が若干遅れていたので，現時点での報告時期は明らかではないが，2007年にもその報告が提出されるであろう。

（2）法の執行の迅速化について

次に法律違反の取り締まりの実態と改善について検討する。

（A）執行状況と課題

日本でのスパマー対策の執行件数は，ほとんどが民間（ISP）が契約約款に基づいて行っているものである。総務省と経済産業省が改善命令を発したのはわずかに４―５件であり，しかも罰則が１ヶ月の業務停止などという軽微なものであった。これでは，迷惑メール行為に対する抑止力にはならない。

日本における執行上の課題はいくつか考えられる。まずは，情報不足である。実際に

迷惑メールがどの程度送受信されているか，スパマーが何社（何名）いるのか，あるいはスパマーが利用している電子メールアドレスがいくつあるか，というような基本的なデータが公表されていない。迷惑メールセンターに転送される迷惑メールの件数は2005年度には前年の３倍以上の約180万件に達しており，2006年度はそれをはるかに上回る勢いであるが，実際に業務改善や刑事告発された件数は非常に少ない。

海外では，迷惑メールボックスが設置されており，転送されてメールが大量に蓄積され誰でも検索できるデータベールとなっている。日本でも，このようなデータベースを公開すれば，現在は迷惑メールの申告を行っていない数多くの被害者も声を上げやすくなる。摘発を行うためには，発信者の情報も必須だが，どのスパマーから摘発するかの優先順位付けには，受信通数や被害者数も重要である。

申告数を増やす工夫を行っているのがオーストラリアである。これまでは，メールのヘッダー情報などを複雑な操作を行ってウェブの申告フォーマットに貼り付けるなど，申告にはパソコン操作に関する技術力と時間が必要であった。その問題を解決するために，メールソフトのアドイン（SpamMATTERSと呼ばれるソフト）を導入し，利用者が使っているメールソフトに組み込んで，ボタン一つでフォルダーごと苦情申告センターのサーバーに送信できるようにした。このソフトは2004年の12月から試行的に導入され，その後の申告件数が88万件に急増するなど好評であったため，2006年５月からは本格実施されたものである。このソフトを日本語対応することが可能となれば，情報収集の大きな武器になることは間違いないだろう。

スパマーの住所等を特定するための情報が重要であるが，現在のプロバイダー責任制限法では，顧客の個人情報を提供する義務はないことから，捜査がなかなか進まないのである。これに対応するためには，特定電子メール法を改正し，スパマーを捜査する場合にはISPの協力を義務付けるようにすべきであろう。これについては，宗田（2004-b）もISPからの情報提供を提言しているが，オプトインや申告のワンタッチ化に加えてスパマーに関する捜査が迅速に行えるような改正を検討すべきだと考えられる。

（B）犯罪者と通信の秘密

摘発がスムーズに行えない理由として，プロバイダーからの情報開示が不十分であることが指摘されている。これについては，仮に迷惑メールの発信者に関する情報が収集できても，プロバイダーが該当する契約者に関する情報を提供しづらい点がネックになっていると言われている。例えば，プロバイダー責任制限法第４条２項では，「開示の請求を受けたときは，・・・開示するかどうかについて当該発信者の意見を聴かなければいけない」と規定されている。

まず，ここでも対象となっているのは，有償の契約を締結している発信者であるが，プロバイダーの義務は意見の聴取のみであり，発信者の情報開示への強制力は全くない。スパマーが情報開示に応じる可能性は皆無に近いので，意思の確認により拒否権がより強まることになってしまう。

また，この項の義務は無償の利用者の場合には適用されないので，スパマーが活用している無料の電子メールアカウントにおいては，発信者の意見を聴く必要はない。しかしながら，無料アカウントの場合は登録されている情報が不十分であったり虚偽であったりするのがほとんどであり，住所などの個人属性については，捜査情報としては必ずしも効果的ではない可能性がある。電子メールの送受信に関する情報については，摘発を行ったり裁判所での係争時には重要な情報であるが，通信の秘密に該当するため，捜査令状等がなければ開示されないところがネックになっている。

送信者名を詐称して送られてくる迷惑メールの発信元を，IPアドレスを用いて突き止め，スパマーの契約を開場するまでの一連の手続きにおいても，各ステップで通信の秘密との兼ね合いを考慮していく必要があるという。また，契約解除を行う際にも本当に正しい相手なのかを誰が担保するのかも課題だ。

（C）犯罪摘発のためのデータベース化

発信者の特徴やメール送信の頻度などをデータベース化することが重要である。既に民間の迷惑メール対策機関や研究所では，おとりのPCなどを活用してスパマーの出現場所，時間，頻度，送信するメールのタイプなどを詳細にチェックして，迷惑メール対策ソフトの開発などに活用している。日本でも国家レベルで迷惑メール対策データベースの構築や技術開発に取り組む必要がある。

日本は迷惑メールに関して被害国であるという認識が主流であると思われるが，日本は迷惑メール発信国のトップ10に常にランクインしており，比率は上昇中であるので加害国であるという認識がまず重要である。また，Spamhaus社の悪質スパマーの本拠地のある国別ランキングでは，米国の1998名，中国の318名に次いで，第３位（242名）とされており，発信者の情報や被害状況を早急に把握し，対策を立案すべきであろう。

その他にも，迷惑メール発信が多い理由が考えられるが，日本のサーバーを経由した送信が多い（発信者は海外にいる），日本のPCの多数がゾンビウィルスに感染し海外等から制御を受けている，などの理由が考えられる。

日本のサーバー経由で送信されている場合には，海外に居ながら無料の.jpアカウントを利用する，オープンリレーやオープンプロキシを使う，などが考えられる。無料アカウントの利用者についての管理は困難であろうから，オープンリレーやオープンプロキシを保有している企業や個人をリストアップし，必要であれば改善のための指導や助言を行う方法がある。

日本のゾンビPC対策は，NEC（BIGLOBE）が既に始めているが，ウィルスやスパイウェアの駆除などをISPがサポートするのも一つである。インターネットユーザの2〜2.5%がボットに感染しているといわれており，BIGLOBEでもボット感染者による大量メール送信が急増している。ボット感染の疑いのある利用者に対して，BIGLOBEカスタマーサポートから案内を行い，駆除の方法などについて対策が完了するまでサポートすることを2006年５月29日に発表した。

また，マイクロソフトのレポートによれば，悪意のあるソフトウェアを削除するツールにより，15ヶ月で570万台のコンピュータから1,600万個のマルウェアが削除された。特に多かったのは，３種類のボット（Rbot，SdbotおよびGaobot）であり，は上位５位までに含まれているが，670万個が削除された。

2006年12月には，総務省と経済産業省の共同運営組織である「サイバークリーンセンター」が開設され，本格的にボット対策に乗り出し始めた。更に，これらのゾンビPCを操っているスパマーの存在を突き止めることも必要だ。

（D）迷惑メールの対象の明確化及び拡大

迷惑メールの発信者が摘発される基準が不明確であり，米国のようにある時間内の送信通数を超えた場合など，総務省や経済産業省や警察庁が捜査を開始するトリガーを明確に示す必要もあろう。例えば，オーストリアのように，50通を超える送信は迷惑メール規制の対象とするなど，迷惑メールの範囲を拡大する案も考えられる。迷惑や不快感を感じるのは，希望しない広告宣伝メールのみでなく，文字を並べただけのメールも不

快であるし，友達を偽装するメールも迷惑である。スパマーは法律の裏をかいてくるので柔軟な対応が必要になる。

オプトインに変更を行うならあまり関係がなくなるが，送信者の同一性について，もう少し幅広くして犯罪者の摘発を可能とすべきであろう。例えば，同じ拒否通知アドレスを共用している発信者については，同一グループあるいは同一人物とみなして調査や捜査を行う仕組みが望ましいと考えられる。

▶6　おわりに

以上のように，迷惑メール対策は世界的な課題であり，一朝一夕には解決しない課題である。ここで，2006年11月27日にEUが発表した迷惑メール等に関する通知[2]（communication）について触れておきたい。この通知で述べられているように，迷惑メール対策については，問題の把握（awareness），規制や技術的対策，協力関係，そして法の執行の４つの柱がある。とりわけ重要なのは，国際的な協力関係と法の執行であろう。

国際的な協力関係については，OECDなどの国際機関や，地域内の協定や，様々な二国間協定が結ばれており，一定の進展は見られているものの，具体的な成果が現れているのはごくわずかの事例にしか過ぎない。発信者（加害者）と受信者（被害者）とは先進国では表裏一体となっており，今後とも情報共有から捜査協力に至るまで幅広い協力関係の強化が必要であろう。

また，同じ声明で述べられているのは，法の執行の問題である。日本にも当てはまるが，迷惑メールなどと戦うという強い意思や公約（commitment）や，国内の様々な機関の責任体制の明確化や，執行機関への適切な資源配分などが執行力をアップさせるはずである。

最後になるが，EUでは各国の執行状況を睨みながら，2007年に向けた法制度の見直しを検討することを宣言しており，日本においてもその状況も踏まえながら，迷惑メール対策を早急に再検討すべきと考える。

●参考文献

Cloudmark “ Cloudmark Reports up to 92% of Email is Spam; Processing 3B Messages per Day ”, August 16, 2006. http://www.cloudmark.com/press/releases/?release=2006-08-16-03
Commission of the European Communities “ On unsolicited commercial communications or ‘ spam ’”, COM（2004）28 final, 22.01.2004.
Commission of the European Communities “ On fighting spam, spyware and malicious software ”, COM（2006）688 Final, 15.11.2006.
EU “ DIRECTIVE 2002/58/EC（Directive on privacy and electronic communications）”, 31.7.2002.
Frieder Laura, and Zittman Jonathan “ Spam Works：Evidence from Stock Touts and Corresponding Market Activity ”, July 27, 2006.
飯田耕一郎『プロバイダー責任制限法解説』三省堂，2002年.
JEAG OP25B SWG「Outbound Port25 Blocking についてのJEAG recommendation」，2006.2.23
JEAG Sender Authentication SWG「送信ドメイン認証についてのJEAG recommendation」，2006.2.23
経済産業省「迷惑メール事業者に対する１か月の業務停止命令」2006年３月31日.

脚　注

２．EU委員会が2006年11月15日に採決したCOM（2006）688finalと呼ばれる通知文書で，タイトルは “ On fighting spam, spyware and malicious sodtware ”（迷惑メール，スパイウェア，そして悪意あるソフトウェアとの戦いについて）である。EUの指令2002/58/ECには３年以内の議会への報告義務項が含まれており，この通知文書はそれを意識して来年にも現在の指令や各国の法律や執行体制などについての見直しや強化を検討すると宣言している。

経済産業省「迷惑メール事業者に対する初の業務停止命令及びワンクリックの不当請求に対する是正指示について」2005年６月15日.
経済産業省「違法な迷惑メールで出会い系サイトの利用を勧誘した事業者２社に特定商取引法による初めての行政処分」2003年10月９日.
経済産業省商務情報政策局消費経済部消費経済政策課編『特定商取引に関する法律の解説：平成16年版』経済産業調査会，2004年11月.
経済産業省産業構造審議会消費経済部会消費者取引小委員会「電子メールによる一方的な商業広告の送りつけ問題に関する対応について（提言）」2002年１月29日.
経済産業省　通信販売の新たな課題に関する研究会報告書「迷惑メール対策の今後の方向性について」　2006年１月24日.
経済産業省　消費経済対策課「『迷惑メール追放支援プロジェクト』の実施状況について」2005年６月14日.
迷惑メール相談センター「平成18年度迷惑メールの受信状況調査」2006年10月13日.
http://www.dekyo.or.jp/soudan/enquete/top-enquete.html
MessageLabs “ Intelligence Reports ” November 2006.
http://www.messagelabs.com/publishedcontent/publish/threat_watch_dotcom_en/intelligence_reports/DA_114080.chp.html
MessageLabs “ Increased Spam Levels Fuelled Through Aggressive Botnet Activities ” November 2, 2006.
http://www.messagelabs.com/publishedcontent/publish/about_us_dotcom_en/news___events/press_releases/DA_173829.html
Microsoft「Windows 悪意のあるソフトウェアの削除ツール：これまでの成果と悪意のあるソフトウェアの傾向」2006年７月６日.
MX Logic “ MX Logic Reports Spam Accounts for 61 Percent of Email in April; "Malcryption" and Ransomware Emerge as Threats ”, May 3, 2006.
http://www.mxlogic.com/news_events/press_releases/release.cfm?id=123&year=2006
NTTドコモ「迷惑メール撲滅に向けた取り組みと現状について」NTTドコモレポート　No.29，2005年８月８日.
http://www.johotsusintokei.soumu.go.jp/whitepaper/ja/cover/index.html
日本電気「BIGLOBEがボットによる迷惑メール対策を実施」2006年５月29日.
http://www.nec.co.jp/press/ja/0605/2901.html
OECD “ Background Paper For The OECD Workshop On Spam, DSTI/ICCP（2003）10/Final ”, 22 Jan 2004.
OECD “ Report of The OECD Task Force on Spam：Anti-Spam Toolkit of Recommended Policies And Measures, DSTI/CP/ICCP/SPAM（2005）3/FINAL ”, 19-April-2006.
大磯一「特定電子メール法改正の概要と迷惑メール対策の取組み」L&T　No.29，民事法研究会，2005年10月.
Onafhankelijke Post en Telecommunicatie Autoriteit（OPTA）“ Annual Report 2004 ” May 2005.
Onafhankelijke Post en Telecommunicatie Autoriteit（OPTA）“ Annual Report 2005 ” May 2006.
新保史生「迷惑メールの法的規制」『メディア・コミュニケーション』，慶應義塾大学メディア・コミュニケーション研究所，第52号，pp59-89，2002年.
Sophos “ Man investigated for sending two billion Viagra spam email ” 12 September 2006.
Sophos “ First spammer found guilty under Australian Spam Act ”, 12 April 2006.
Sophos “ CAN-SPAM Act can do better, Sophos reports ”, 16 December 2005.
宗田貴行『迷惑メール規制法概説』レクシスネクシス・ジャパン，2006年.
宗田貴行「迷惑メール規制の課題―EUにおける近時の展開を参考にして―」『奈良法学会雑誌』第17巻１・２号，pp1-61，2004年９月.
総務省「情報通信白書平成18年版」，2006年７月.
総務省「迷惑メールの在り方に関する研究会―中間とりまとめ」，2002年１月24日.
総務省「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」，2005年７月22日.
総務省「『特定電子メールの送信の適正化等に関する法律』違反者に対する措置命令の実施」2003年11月13日.
総務省「『特定電子メールの送信の適正化等に関する法律』違反者に対する措置命令の実施」2004年４月16日.
総務省「『特定電子メールの送信の適正化等に関する法律』違反者に対する措置命令の実施」2005年９月27日.
総務省「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案に対する意見募集の結果」，2002年６月20日.
総務省「『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』に寄せられた意見及びそれに対する研究会の考え方」，2005年７月22日.
総務省「総務省の迷惑メール対策 ～改正特電法と送信者情報交換～」第２回迷惑メールカンファレンスにおける発表資料，2005年12月７日. http://www.iajapan.org/anti_spam/event/2005/conf1207/pdf/3-2.pdf
総務省「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」2004年１月19日.
総務省「特定電気通信役務提供者の損害賠償責任の制限 及び発信者情報の開示に関する法律 ―逐条解説―」2002年５月.
http://www.soumu.go.jp/joho_tsusin/chikujyokaisetu.pdf
総務省「特定電子メール等による電子メールの送受信上の支障の防止に資する技術の研究開発及び電子メールに係る役務を提供する電気通信事業者によるその導入の状況」2006年11月14日.
総務省総合基盤局「携帯電話等に関する迷惑メール対策」，2001年２月25日.
Spamhause “ 200 Known Spam Operations responsible for 80% of your spam. ”

http://www.spamhaus.org/rokso/index.lasso
Spamhause “ September brings four powerful legal setbacks to the world's Spammers ”, October 6, 2006.
http://www.spamhaus.org/news.lasso?article=610
Spam Task Force “ Stopping Spam Creating a Stronger, Safer Internet, Report of the Task Force on Spam ”, Canada, May 2005.
http://e-com.ic.gc.ca/epic/internet/inecic-ceac.nsf/en/h_gv00317e.html
シマンテック「インターネットセキュリティ脅威レポート」2005年９月.
シマンテック「インターネットセキュリティ脅威レポート」2006年２月.
Technology News Daily “ Spam Hit Highest Level, MX Logic Reports ”, November 1, 2006.
http://www.technologynewsdaily.com/node/5045
The Parliament of Australia “ Spam Act of 2003, An Act about spam, and for related purposes ”, December 2003.
http://www.comlaw.gov.au/comlaw/Legislation/Act1.nsf/0/1160D31116822BC1CA256F720010C588/$file/1292003.pdf
The Australian Communications and Media Authority（ACMA）.
http://www.acma.gov.au/ACMAINTER.1507598:STANDARD::pc=PC_2008
The Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003（CAN-SPAM Act）, 15 U.S.C. §7701-7713.
「特集 spamメールの現状と対策の動向」情報処理　46巻７号，情報処理学会，2005年.
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（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（平成14年法律第26号）.
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（平成14年６月21日　総務省令第66号）.
U.S. Federal Trade Commission “ The US SAFE WEB Act：protecting Consumers from Spam, Spyware, and Fraud ”, A Report To Congress, June 2005.
U.S. Federal Trade Commission “ Effectiveness and Enforcement of the CAN-SPAM Act ”, A Report To Congress, December 2005.
U.S. Federal Communications Commission “ Notice of Proposed Rulemaking and Further Notice of Proposed Rulemaking ” FCC 04-52, adopted March 11, 2004.
U.S. Federal Communications Commission “ CAN-SPAM Implementation Order ” FCC 04-194, adopted August 12, 2004.

（宿南達志郎　慶應義塾大学メディア・コミュニケーション研究所教授）