迷惑メールの法的規制

新保史生

▶はじめに

「迷惑メール」（以下，「スパム」という。）とは，受信者の求めによらずに一方的に送信されてくる商用の電子ダイレクトメールのことをいい，電子メールという利便性の高い通信手段の利用と引き替えに，ネットワーク社会に参加する者の多くがその受信を甘受せざるを得ないものとなっている。

とりわけ，携帯電話の電子メールアドレスに対して送信されるスパムの増加は社会問題化しており，移動体通信事業者のメール・サーバについてみれば，日々大量に送信され宛先不明になっているスパムの中に，通常のメールが埋もれてしまっているといっても過言ではない。

しかし，スパムをめぐる議論は，携帯電話宛のスパム問題が深刻になるにつれ，スパムの受信にかかる費用に対する受信者課金の問題ばかりが強調され，その対策に要する通信事業者側の負担について論じられることは少なく，むしろ取扱通信量の増加による事業収益の増加ばかりが批判の対象となるといった図式がある。

実際には，ネットワーク社会の規範たるネチケットを無視したスパムの送信が常態化する中，通信インフラの公共性と確実な回線確保を義務づけられている電気通信事業者は，日々増加し続ける「不必要なトラヒック」にも対応した通信設備の拡充を迫れる一方で，受信者の意思に関係なくスパムの受信を強いられている利用者からも対応を求める要請や苦情が寄せられ，その矛先が，そのような問題を発生させる元凶たるスパムの送信に従事する者（以下，「スパマー」という。）ではなく，移動体通信事業者等に向けられているのが現状である。

将来的なブロードバンド化への移行とともに，これらスパムをめぐる問題もブロードバンド化し続けるとすれば，通信事業者及び利用者の双方にとってスパムの受信が受忍限度を超え，適正な通信環境の維持が困難になる日も遠くはないであろう。

かかる状況に対し，法的側面からスパム規制が必要であると考えられており，米国ではソルキン教授[1]によって，1991年電話消費者保護法によるジャンク・ファックスの規制論との比較によるスパム規制論が提唱されて以降，ネバダ州のスパム規制法制定を端緒に州レベルでの具体的な規制へと動き，一方，わが国では，岡村弁護士によるスパムに関する論考[2]を嚆矢に，法的問題としてのスパム問題が意識されるようになった。

脚注

1．Sorkin, David E., Spam Laws <http://www.spamlaws.com/>. Sorkin, David E.,（1997）*Unsolicited Commercial E-Mail and the Telephone Consumer Protection Act of 1991*, 45 BUFFALO L. REV. 1001.

2．岡村久道（1998）「商用電子ダイレクトメールに対する法的規制（上）（下）」NBL650号・651号。

さらに，我が国においても現実のスパム規制へと向かいつつあり，経済産業省による迷惑メール規制を目的とした特商法改正のための研究会の発足，東京都消費生活対策審議会基本問題部会による都条例の改正による規制へ向けた検討[3]，総務省による迷惑メールへの対応の在り方に関する研究会の発足[4]，そして，民主党が議員立法によるスパム規制法案[5]を提出するなど，法規制へ向けた動きも具体化しつつある。

一方，通信事業者側も，2001年11月９日に，「大量な宛先不明メールの受信ブロック」に係るNTTドコモの契約約款の変更が総務省から認可されたことを受けて，大量の宛先不明メールの受信ブロックを開始している。

さらに，司法の場においても刑事及び民事の両面から具体的な事案が扱われるようになりつつあり，2001年10月３日には，迷惑メールで15万通のエラーメールを発生させたことによってメール転送サービス会社の業務を妨害したとして，スパム送信者が偽計業務妨害罪のかどで逮捕された事案があり，また，携帯電話宛に大量のスパム送信行為を行いNTTドコモの取り扱う通信に支障を及ぼしたとして，当該送信行為の禁止を求めた仮処分申請に対して横浜地裁が業者に対して送信行為の１年間禁止の仮処分決定を行っている[6]。

このように，スパム規制へ向けて動きつつある現在，その具体的な法整備にあたっては，インターネットを利用した電子メールの送受信の特性を理解した上で，規制の対象となるスパムの定義や規制方法を受信者の負担及び通信事業者の負担の両面から検討し，通信手段を利用して行われる広告規制の規制内容の合理性を判断する必要がある。よって，本稿では，EUにおけるスパム規制と，州レベルでスパム規制法を制定し，連邦レベルでも規制法制定への審議が継続している米国の現状を比較法的な視点から検討を行い，スパム規制のあり方について考えたい。

▶ 1　スパムの定義

迷惑メールを表す「スパム」という呼称は，本来はHormel Foods社の缶詰豚肉の商品名であるSPAM（Spiced Pork And Ham）の名称であり，電子メールとは全く関係のないものである。現在のような意味合いで用いられるようになったきっかけは，1969年から74年にかけて放映された英国テレビのバラエティー番組である「モンティー・パイソンズ・フライングサーカス（Monte Python's Flying Circus)」の，1970年６月25日に収録されて同年12月15日に放映された番組内において，料理のメニューのスパムを連呼するジョークが，その後，「くだらない」とか「つまらない」物を指す俗語として用いられるようになったことに端を発する。

そのような意味から，受信者が望んでいないにもかかわらず一方的に送信されてくる電子メールを俗語としてのスパムに準え，現在では，そのようなメールを指す言葉として一般に用いられるようになった。

我が国では，スパムについては一般的に「迷惑メール」と呼ばれることが多いが，その他にも，大量の電子メールの送信について数量的な観点から定義する「バルク・メー

脚注

3．「第17次東京都消費生活対策審議会『社会経済状況の変化に対応した消費生活条例・規則の改正について』基本問題部会中間報告（2001年10月31日)」
<http://www.shouhiseikatu.metro.tokyo.jp/s_hogo/singi/singi6.html>.
4．「迷惑メールへの対応の在り方に関する研究会」の開催（平成13年11月26日）総務省。
5．民主党「商業広告に係る電子メールの適正化等に関する法律案骨子」(2001年11月５日)
<http://www.dpj.or.jp/seisaku/joho/BOX_JH0011.html>.
6．岡村久道（2001）「横浜地裁，NTTドコモの申立でメール広告発信差止の仮処分決定を行う」NBL11月15日号（No.725)。

ル（bulk mail)」，受信者にとって興味のない内容のメールという観点からゴミ扱いという意味で定義される「ジャンク・メール（junk mail)」，受信者の求めによらずに一方的に送信されてくる商用の電子メールと定義される「UCE（Unsolicited commercial E-mail)」，受信者の求めによらない扇情的な電子メールと定義される「Unsolicited Pandering E-mail」，受信者の求めによらずに一方的に大量に送信されてくるメールと定義される「UBE（Unsolicited bulk E-mail)」などの表記がある。

このように，表記方法も種々様々であるスパムは，送信方法，内容，及び数量などからその定義も様々であるが，一般的には，「発信者情報を偽り又は隠蔽し，大量の商用電子ダイレクトメールを執拗に送信する行為[7]」とか，「受信者とは送信以前に関係を有さない送信者が，本人からの依頼なしに大量かつ反復的に送信する商業的な性質を有する電子メール[8]」などと定義されるメールがスパムに該当するものといえる。

よって，スパムに該当するか否かを判断するにあたっては，①商業的な性質を有するものであり，かつ，②受信者の求めによらずに送信されるメールであること，という二つの条件を最低限満たす必要があり，それに付随する要件として，執拗な大量のメールの送信であったり，虚偽の情報を用いて発信元を特定できないような手段での送信など，スパムの送信にあたって行われる発信者情報の隠蔽や誤認を生ずる件名などを含め，それらの総称を「スパム」と称している。

▶ 2　スパム問題の背景

2-1　スパム増加の背景

スパムの増加の背景には，インターネットが新たな効果的なマーケティング手段として認識されるようになったことが大きく影響している。

米国のダイレクト・マーケティング協会（DMA）によると，米国内における1999年度のダイレクト・マーケティング費用は，1760億ドルに達しており，商用通信全体（3089億ドル）の実に57パーセントを占めている。この数字は，2003年には2215億ドルに達すると見込まれている。

さらに，既存の広告媒体への広告の出稿ではなく，通信手段を利用して行われるDMの増加も著しく，とりわけ，電子メールの普及はその傾向をさらに加速させている。その理由としては，①費用面における効果（郵便を利用したDMとは異なり，電子メールは費用がほとんどかからないこと)，②顧客転換率（電子メールが５～15パーセント程度，従来のDMが0.5～２パーセント程度)，及び③顧客反応率（バナー広告と比較して，電子メールを利用した広告に対して消費者が反応する比率が格段に高いこと）の三つの要素が指摘されている[9]。また，いずれの点についても既存の広告媒体よりも顕著な効果が認められることが，通信手段を利用したDMの最大の増加要因となっており，その延長線上に，業界団体の自主規制やネチケット等を無視して一方的に送信される商用電子ダイレクトメールの問題がある。

解　注

7．Commission of the European Communities, Unsolicited Commercial Communications and Data Protection (Internal Market DG - Contract n° ETD/99/B5-3000/E/96) (January 2001) 14.

8．Data Protection Working Party, *Privacy on the Internet - An integrated EU Approach to On-line Data Protection*, Adopted on 21 Nov. 2000, available at: <http://europa.eu.int/comm/internal_market/en/media/dataprot/wpdocs/wp37en.pdf>.

9．Commission of the European Communities, *Unsolicited Commercial Communications and Data Protection* (Jan 2001) 13.

●表１　米国市場における広告費全体に占めるDM費用

（単位：10億米ドル）	ダイレクトマーケティング費用	広告費及びDM費用の合計	総費用におけるDM比率
1994年度			
ダイレクトメール	29.6	29.6	100
テレマーケティング	46.8	76.8	60.9
新聞	12.2	34.4	35.6
雑誌	6.2	11.5	53.7
テレビ	12.9	35.4	36.5
ラジオ	3.8	10.5	36.5
その他のメディア	9.7	20.4	47.5
合計	$121.30	$218.70	55.50%
1999年度			
ダイレクトメール	42.2	42.2	100
テレマーケティング	66.9	110.5	60.5
新聞	17.4	47	37.1
雑誌	8.9	15.9	56.3
テレビ	20.4	51.4	39.6
ラジオ	6.5	15.5	42
その他のメディア	14.2	26.4	53.7
合計	$176.50	$308.90	57.10%

（Commission of the European Communities, *Unsolicited Commercial Communications and Data Protection*, Jan 2001.）

●表２　米国内における双方向メディアを利用したDMの増加

	1994	1998	1999	2000	2004	94-99
合計	$11.00	$742.00	$1,311.00	$2,135.00	$8,614.00	160.20%
事業者間（B to B）	7.5	469.7	824.6	1,338.60	5,418.20	156.00%
対消費者（B to C）	3.5	272.3	486.4	796.4	3,195.80	168.30%

（単位：10億米ドル）
（Commission of the European Communities, *Unsolicited Commercial Communications and Data Protection*, Jan 2001.）

Figure & Table

2-2　スパム被害の内容

スパムによる被害は，スパムを受信する受信者側の負担と，スパムの送受信を取り扱う通信事業者側の負担の両面がある。

受信者の負担としては，携帯電話等の受信者課金によるサービスを利用している者にとっては，本来受信を望んでいないメールに対してもパケット毎に課金されてしまうため，不必要なメールの受信が利用者の通信料金に転嫁されてしまう点が最も深刻な問題である。また，不必要なメールの送受信に要する費用だけでなく，大量に受信しなければならないメールの確認，選別および削除のために時間を費やさざるを得ない。特に，電子メールを受信した時点では，送信者や件名などの限られた情報から，そのメールがスパムなのか自分にとって必要なメールなのかを判断することが困難な場合も多く，必然的に受信したメールを開いて内容を確認する負担を受信者が強いられることになる。

一方，通信事業者側の負担としては，大量のスパムの送受信によって，メールサーバに過度の負担がかかり，結果的に，全体のメールの送受信そのものに支障を来したり，

最悪の場合にはメールの取り扱い量にサーバの処理能力が追い付かないために，サーバがダウンするという事態に陥る可能性すらある。そのため，電子メールサービス等の電気通信役務を提供する通信事業者にとっては，大量のスパムの送受信のために必要な処理能力と容量の確保に多大な負担を強いられるようになっており，スパム以外の通信が遅滞なく行われるような環境を維持するために，膨大な量のスパムの取り扱いにも対応できる設備や管理体制の構築を迫られている。

しかし，いわゆるスパムに類似するメールの送受信をめぐる問題は，パソコン通信の時代から存在していたものである。パソコン通信の場合は，登録者のIDが固定長の英数字からなる番号であったことから，英数字を一文字ずつ変えるなどしてメールを送信することによって現在でいうところのスパムに類似するメールの送信が行われていた。

これと同様の手法を用いて送信される電子メールが，移動体通信の普及に伴い増加し，11桁に固定された携帯電話の番号を，パソコン通信のときと同様に一つずつ番号を変えさえすれば，@（アットマーク）以下のドメインが同一の携帯電話のメールアドレスに対しては，事前にメールアドレスを取得せずに大量の電子メールの送信が可能である。

よって，スパムの増加をもたらした要因として，これらに共通する特徴にみられるように，固定長の連続する数字等から構成される番号が利用者に割り振られていることがあげられる。そのため，電話番号からなる初期設定のアドレスの変更を行うのが一般的となっているが，スパムウェア（後述）を用いてランダムに文字や数字等の組み合わせを生成し，無断生成した電子メールアドレス宛に大量の電子メールを送信する方法が用いられることが多い。よって初期設定の電話番号を用いないメールアドレスに変更したとしても，一過的にスパムの受信を回避する効果はあるものの実質的な効果が薄いのが現状である。

▶ 3　欧州におけるスパム規制

3-1　「オプト・イン方式」への傾斜

欧州におけるスパム規制は，個人情報保護との関連において論じられることが多い。そのため，商用電子ダイレクトメールを送信することを目的として電子メールアドレスを取得する事業者については，他の個人情報データベース等を構築する事業者同様に，個人情報保護に関する監督機関等への登録が義務づけられていることが多い。

そのような背景から，電子メールアドレスも含む個人情報の不正な取り扱いに関しては，監督機関による厳格な行政処分が実施されてきている。また，当該アドレスの取得時点における情報主体の同意要件が個人情報保護の観点から重視されており，「EUの個人データ保護指令第29条に基づく作業部会による検討[10]」においても，「欧州委員会の報告書[11]」においても，情報主体の同意要件を明確にする手段として，電子メールの配信を事前に同意した者に対してのみ行う「オプト・イン方式」の導入に関する議論が中心となっている。

その一方で，各加盟国における足並みは必ずしも一致しておらず，それぞれの国内措置においては，「オプト・アウト方式」と「オプト・イン方式」が対立している。

脚注

10. Data Protection Working *Party, Privacy on the Internet - An integrated EU Approach to On-line Data Protection*, Adopted on 21 Nov. 2000, available at: <http://europa.eu.int/comm/internal_market/en/media/dataprot/wpdocs/wp37en.pdf>.

11. Commission of the European Communities, Unsolicited Commercial Communications and Data Protection (Internal Market DG - Contract n° ETD/99/B5-3000/E/96) (January 2001).

3-2　EUの各指令とスパム規制

EUにおけるスパム規制は，EUの各指令において規制方針が一定範囲においてある程度具体化されている。

「EUの個人データ保護指令[12]」の第６条，７条，10条，及び14条は，個人データの適正な取得及び利用並びに正当な目的における処理を求めており，スパムを送信する際に取得及び利用される電子メール・アドレスの取り扱いにあたっては，これらの規定を根拠に定められた各加盟国の国内法に基づく適正な取り扱いを行うことが求められている。

「電気通信分野における個人データ保護指令[13]」の第12条は，通信手段を利用したダイレクト・マーケティングについて規定しており，同条に基づく対応としては，「人的操作が介在しない自動呼び出し装置（自動発呼装置）又はファクシミリ（FAX）を用いたダイレクト・マーケティングは，加入者が事前に同意している場合にのみ実施できる。」との規定に電子メールも含めて解釈することによってスパムを規制しようというものである。

「消費者保護指令（通信販売指令）[14]」の第10条は，特定通信手段の利用禁止について定めており，①人的操作が介在しない自動発呼システム（自動呼出装置），又は②ファクシミリを利用して勧誘を行う場合には，消費者の事前の同意を得なければならないと第１項において規定している。また，第２項では，「加盟国は，第１項の定める通信手段以外の手段であって，消費者から明示的な異議の申立がない個人の通信を可能にすることを目的とした通信を保障しなければならない。」と規定しており，ここにいう，「第１項の定める通信手段以外の手段」には，当然のことながら電子メールも含まれるものと解されている。

「電子商取引指令[15]」の第７条は，受信者の求めによらない商用通信について定めており，第１項では，「共同体の法令に定められている要件に加え，受信者の求めによらない電子メールを用いた商用通信を認める加盟国は，受信者が受信した時点において，国内において事業を営むサービスプロバイダの発する当該商用通信を，明確かつ明示的に識別できるように保障しなければならない。」と規定し，第２項では，「指令97/7/EC及び指令97/66/ECに関わらず，加盟国は，電子メールを用いて受信者の求めによらない商用通信の送信を行うサービスプロバイダが，定期的に意見を聴取し，当該商用通信の受信を望まない自然人が自ら登録を行うことができるオプトアウトの登録を尊重することを保障するための基準を策定しなければならない。」と規定し，商用電子メールにその旨を示す識別徴表を示すことと，オプト・アウト方式による受信停止措置について定めることを要求している。

脚注

12. Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, 395L0046, Official Journal L 281, 23/11/1995 p. 0031 - 0050.
13. Directive 97/66/EC of the European Parliament and of the Council of 15 December 1997 concerning the processing of personal data and the protection of privacy in the telecommunications sector, 397L0066, Official Journal L 024, 30/01/1998 p. 0001 - 0008.
14. Directive 97/7/EC of the European Parliament and of the Council of 20 May 1997 on the protection of consumers in respect of distance contracts -Statement by the Council and the Parliament re Article 6(1)- Statement by the Commission re Article 3(1), first indent,Official Journal L 144, 04/06/1997 p. 0019 - 0027 <http://europa.eu.int/eur-lex/en/lif/dat/1997/en_397L0007.html>.1997年５月20日制定。加盟国の履行期限は2000年５月21日。
15. Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce'), Official Journal L 178 , 17/07/2000 p. 0001 - 0016 <http://europa.eu.int/eur-lex/en/lif/dat/2000/en_300L0031.html>. 2000年６月８日制定。加盟国の履行期限は2002年１月17日。

3-3 「オプト・イン方式」による規制法の整備

「オプト・イン方式」によるスパム規制に関する議論が活発な欧州では，既に，EU加盟４カ国及びEEC加盟１カ国において，人的操作が介在しない手段を用いて行われるダイレクト・マーケティング技術を利用し，受信者の求めによらない商用通信を行う際に受信者の事前同意を義務づける法律が制定されている[16]。また，ドイツにおいても同様の方式を採用した法律案が提出されている。

１）法整備の状況

a）イタリア

「電気通信分野におけるプライバシー保護令[17]」が1998年５月13日に制定され，自動発呼システムを利用して受信者の求めによらない広告を発信する際に，受信者の事前の同意を得ることが義務づけられ，電子メールもその対象に含まれている。

また，個人情報保護の観点からも，1996年12月31日に「個人データ処理に係る個人及び法人の保護に関する法律[18]」が制定され2000年５月８日に施行されている[19]。

電子メールも含む個人情報の適正な取り扱いに関する具体的な手続きについては，「個人データ保護法第33条第３項に基づく個人データ保護監督機関の組織及び運用に関する規則を定める大統領令[20]」，「公的部門の取り扱う機微な個人情報処理令[21]」，「歴史，統計，及び科学研究目的での個人データ処理令[22]」，「医療分野における個人データの機密保持令[23]」，「個人データの処理に係るセキュリティの最低基準に関する大統領令[24]」等に定められている。

b）オーストリア

1999年８月に施行された電気通信規制法（1997年法律第100号）第101条において，「加入者の事前の同意なしに広告目的での発呼（テレファックスの送信を含む）を行ってはならない。」と規定され，電子メールについても，同条において，「大量又は広告目的で電子メールの送信を行うにあたっては，受信者の事前の同意を得ることを要す。」と規定されており，商用目的で自動発呼システム，ファックス，又は大量の電子メールの送信を行うにあたっては，ダイレクト・マーケティングの対象者の事前の同意を得ることが義務づけられている。

当該規定に違反した場合には，同法第104条により，50万オーストリアシリング（３万６千336ユーロ）以下の罰金が科される。

16. *See* Commission of the European Communities, Unsolicited Commercial Communications and Data Protection (Internal Market DG - Contract n° ETD/99/B5-3000/E/96) (January 2001).
17. Legislative decree No. 171 of 13.05.98 Provisions applying to the protection of privacy in the telecommunications sector, implementing EC Directive 97/66, of the European Parliament and of the Council, and to journalistic activities.
18. Protection of individuals and other subjects with regard to the processing of personal data Act no. 675 of 31.12.1996. 本法の条文は，<http://www.garanteprivacy.it/>に掲載されている。
19. *See* Patrick Del Duca, *The Maturation of Italy's Response to European Community Law: Electric and Telecommunication Sector Institutional Innovations*, 23 FORDHAM INT'L L.J. 536 (2000).
20. Decree by the President of the Republic No. 501 of 31.03.98 Rules on organizazion and operation of the office of the Garante [Supervisory Authority] for the Protection of Personal Data pursuant to Article 33(3)of Act no. 675 of 31.12.96.
21. Legislative decree No. 135 of 11.05.99 [As amended by legislative decrees no. 281 and no. 282 of 30.07.99] Provisions Supplementing Act no. 675 of 31.12.96,on the Processing of Sensitive Data by Public Bodies.
22. Legislative decree no. 281 of 30.07.99 Provisions concerning the processing of personal data for historical, statistics and scientific research purposes.
23. Legislative decree No. 282 of 30.07.99 "Provisions for ensuring confidentiality of personal data in the health care sector" .
24. Presidential decree No. 318 of 28.07.99 Regulations including provisions for laying down the minimum security measures applying to the processing of personal data in pursuance of Article 15(2) of Act no. 675 of 31.12.96.

c）デンマーク

マーケティング法（法律第418号）が，2000年５月31日に制定されている。本法では，受信者が望まないマーケティング目的での電子メール，自動発呼システム，又はファックスの利用について明示的に規定し，受信者の事前の同意を得ることを義務づけている。

d）フィンランド

電気通信分野における個人データの保護に関する法律（1999年法律第565号）が，1999年４月22日が制定されている。

電気通信及びダイレクト・マーケティングについて定めている同法第21条は，ダイレクト・マーケティング目的で，自動発呼システム又はファックスを利用する際に，受信者の事前同意を得ることを義務づけている。

電子メール等，同条に定められている手段以外の方法を利用したダイレクト・マーケティングについては，当該手段の機能及びセキュリティ等の検討を行った上で，事前の同意要件を義務づけるかどうか決定する権限は大臣に与えられている。

なお，大臣に付与された当該権限を行使し，2000年度末までに，電子メールを利用したマーケティングに対して，「オプト・イン」要件を課す決定がなされている。さらに，2000年10月には，フィンランドのダイレクト・マーケティング連盟が，オプト・イン方式に基づく電子メールを利用したダイレクト・マーケティングを実施する際の行動規範を策定している。

e）ドイツ

前述の電子商取引指令を履行するための法律案において，オプト・イン方式による商用通信の規制へ向けた法律案が提出されている。

f）ノルウェー

2001年３月１日に施行されたノルウェーのマーケティング活動規制法の第2b条は，「特定通信手段の利用の規制」に関し，「電子メール，携帯電話向けテキスト・メッセージング・サービス，ファクシミリ，又は自動発呼装置を，個人的な通信手段として消費者が利用している電気通信に対し，受信者の事前の同意を得ずにダイレクト・マーケティング事業に従事することを目的として使用することを禁ずる。」と定めている。

これにより，電子メール等を利用したダイレクト・マーケティング活動を行うにあたっては，受信者の同意を得ることが義務づけられている。

▶ 4　米国における連邦レベルのスパム規制法案

4-1　スパム規制への試み

米国のスパム規制は，電話勧誘販売，訪問販売，及び郵便物等によるダイレクトメール問題の延長線上の問題として，インターネットの普及に伴い規制論が高まってきた問題である。

例えば，電子メール同様，通信回線を経由して文字が送信される形態をとっているものとしてファクシミリが一般的に普及しているが，ファクシミリを利用したダイレクト・マーケティングについては，1991年の電話消費者保護法により，ファクシミリを使用して受信者の求めによらない広告の送信を行うことが禁止されている[25]。さらに，同法では，自動電話ダイアル・システム（ATDS[26]）や人工又は事前録音音声（APV[27]）を使

用した電話の発呼行為も禁止されており，自動的に複数回に渡って宣伝目的の電話を掛ける行為も禁止されている。

なお，スパムについては，規制の必要性が唱えられながらも，現時点において連邦レベルでそれを規制する法律の制定には至っていない。

4-2　第105回議会に提出されたスパム規制法律案

スパム規制を目的として提出された最初の法律案は，1997年５月21日にマコウスキ（Frank Murkowski）上院議員が提案した「受信者の求めによらない商用電子メール選択法案[28]」である。本法案は，スパムの本文中に，送信者の住所及び電話番号の記載や，商用メールであることを示すヘッダを表示することを義務づけるものである。さらに，ISP側に対しては，ヘッダに商用メールであることが表示されているメールを，ユーザの要請によって排除するように設定することを義務づけている。

続いて，同年５月22日には，スミス（Christopher Smith）下院議員によって「ネチズン保護法案[29]」が提出された。本法案は，1934年の通信法を改正し[30]，ファクシミリによるダイレクトメールの禁止を電子メールにも拡大することによってスパムを全面的に禁止することを試みたものである。また，受信者側が自発的な意思に基づいて，メールの送信を希望する申し込みを行っていることを要件として定め，さらに，電子メールの本文に送信者を識別する情報を表記することを義務づけようとするものである。

さらに，翌月６月11日には，トリチェリ（Bob Torricelli）上院議員によって「電子メールボックス保護法案[31]」が提出された。本法案は，電子商取引及び電子通信を促進し，消費者及びISPの設備を介して，他人が大量のスパムを送信する際に，コンピュータ設備の悪用から消費者及びISPを保護することを目的とするものである。また，スパムの送信を実行する者に対して，受信拒否者リストの作成を義務付け，スパムの受信拒否を表明した者に対してはスパムを送信してはならないとしている。

これらの法案は，スパム規制への議論の端緒とはなったものの，いずれも制定には至らなかった[32]。

4-3　第106回議会に提出されたスパム規制法律案

第106回議会に入ってからもスパムをめぐる議論は活発に行われ，議会にも多数の法律案が提出された。その背景には，廃案となったスパム規制法案を提出した議員が，新たな法案を議会に提出することにより，再度スパム規制の実現へ向けて活発な活動を継続したことが影響している。

第106回議会では，1999年３月25日に提出された「電子メール受信箱のプライバシー法案[33]」を端緒として，第105回議会において提出された法案数以上の法案が提出されることになる。

この法案では，①商用電子メールの本文に正確な返信先情報を表記すること，②ヘッダの偽造禁止，③「削除」要求の尊重，等について定めている。また，本法案によるス

脚注

25. 47 U.S.C. § 227(b)(1)(C)（1994 suppl.4）.
26. Id. § 227(b)(1)(A),(D).
27. Id. § 227(b)(1)(B).
28. Unsolicited Commercial Electronic Mail Choice Act of 1997, S.771,105th Cong.（1997）.
29. Netizens Protection Act of 1997, H.R.1748,105th Cong.（1997）.
30. 47 U.S.C. § 227（1994 suppl.4）.
31. Electronic Mailbox Protection Act of 1997, S.875,105th Cong.（1997）.
32. その他，成立に至らなかった法案として，「1998年の電子メール利用者保護法案（E-Mail User Protection Act of 1998, H.R.4124, 105th Cong.（1998）.）」。
33. Inbox Privacy Act of 1999, S.759, 106th Cong.（1999）.

パム規制の特色としては，ドメイン名の保持者が，商用電子ダイレクトメールの受信を拒否する意思を表示することができるようにしている。

その一方で，スパムの包括的な規制を回避するために，ISPに対して商用電子メールの一部又は全てを受信することを希望している利用者リストの作成を求めている。さらに，ISPが提供しているスパムのフィルタリングを目的としたサービスを「オプト・アウト」することができるようにしなければならないとした。しかし，そのような設定を可能にするために，ISP側が経済的な負担又は労力を要したとしても，利用料金の増額によって負担を利用者に転嫁することを禁じ，ISPが，法律に基づいて設定を実施しない場合には，本法律の適用を受けることができないとした。

1999年５月24日には，グリーン（Gene Green）下院議員により，「電子メール利用者保護法案[34]」が提出されている。本法案は，送信者情報を偽って大量の受信者の求めによらない電子ダイレクトメールを送信する行為を禁ずることを目的としている。

つまり，大量の受信者の求めによらない電子メールを送信する行為自体は違法とはならないが，そのようなメールを送信する際に，虚偽の送信者情報を用いて送信した場合に違法となる。また，受信者が，大量の受信者の求めによらない電子メールの送信の一切の受信を拒否しているにもかかわらず，そのようなメールを送信することは禁止されている。

違反者に対しては，１通あたり50ドル又は違反行為の継続期間中は１日あたり１万ドル以下の罰金が科される。

個人の受信者が被害を被った場合には，現実的損害，１通あたり50ドルの損害賠償及び合理的な弁護士費用並びに原状回復に要した費用を請求することができるとしている。

一方，ISPに対しては，本法に基づいて民事訴訟を提起することを認め，現実的損害及び１通あたり50ドル又は違反行為の継続期間中は１日あたり１万ドル以下の損害賠償，並びに合理的な弁護士費用及び原状回復に要した費用を請求することができるとしている。

また，個人の受信者及びISPの両者とも，スパムの送信差止を請求することができ，エクイティ上の救済又は宣言的救済を求めることができる。

さらに，受信者が受信拒否を表明した後に，電子メールアドレスを偽造又はスパムを送信した場合には，罰金又は１年以内の禁固刑に処せられる。また，連邦取引委員会法に基づき，不公正又は欺瞞的取引行為として摘発される。

1999年６月10日には，ミラー（Gary Miller）下院議員によって「スパム封じ込め法案[35]」が提出されている。本法律案は，ISPの方針に反して，商用電子メールを送信することを目的として電子メール・サービス・プロバイダの装置を使用することを禁止し，インターネットのドメイン名の無断使用を禁ずることを目的としたものである。

規制の内容は，①商用電子ダイレクトメールを許容しない意思表明をしているISPの方針に反したスパム送信者に対して，訴訟を提起する権利を付与，②商用電子ダイレクトメールに対する方針を，ウェブ上又は自らが管理するメール・サーバ上で公表することを可能とする体制を提供，③商用電子ダイレクトメールを送信する際に，他者の保有するドメイン名を無断で利用する行為を処罰する規定の創設といった規定を置いている。

本法案においては，ISPの保有する設備及び顧客の保護を図ることにより，スパムの規制を行うという規制態様をとっている。つまり，スパムを一律に規制の対象とするのではなく，ISPが予めスパムの取り扱いに対する方針を表明することにより，ISPの方針に

脚注

34. E-Mail User Protection Act, H.R.1910, 106th Cong.（1999）.

35. Can Spam Act, H.R.2162, 106th Cong.（1999）.

反する商用電子ダイレクトメールを排除する権限を付与しているのである。また，その方針に反して，スパムの送信を行った者に対して，メッセージ１通あたり50ドル，１日最高２万5000ドルの損害賠償を請求することも認めている。

1999年10月20日には，ウィルソン（Heather Wilson）及びグリーン（Gene Green）下院議員により，「受信者の求めによらない電子メール法案[36]」が提出されている。これは，1934年の通信法を改正し，受信者の求めによらない商用メールの受信を望まない人物に対して当該メールを発信する行為を禁止する法律案である。

本法による規制の内容は，本人の代理又は子供の代わりに，連邦通信委員会に対して，受信者の求めによらない商用電子メール（Unsolicited Commercial Electronic Mail），受信者の求めによらない扇情的な電子メール（Unsolicited Pandering E-Mail），又はその両者の受信を望まない意思を表明することを認めている。

商用電子メール又は扇情的な電子メールの本文には，受信者が，今後一切そのような通信を受信しない意思を表明することができるように，電子メールの返信先アドレスを明示しなければ送信することができないとしている。

また，連邦通信委員会に対しては，①当該ファイルの最新リストを保持及び維持し，②当該リストの請求費用も含めて，合理的な期間及び条件の下で入手を可能にすることを義務づけている。なお，リストの作成目的は，氏名及び電子メールアドレスが30日以上掲載されている個人に対して，商用電子メール又は扇情的な電子メールを送信する行為を禁止することにある。また，当該リストの目的外での利用も禁じられている。

スパム規制への試みは，直接的に商用電子ダイレクトメールの規制を図る法案だけでなく，消費者保護の観点から規制を試みている法案もある。

例えば，1999年３月24日に，ワイデン（Wyden）上院議員が提出した「電話勧誘販売詐欺及び高齢者保護法案[37]」は，インターネットを利用した詐欺を含め，電話勧誘販売詐欺から一般市民，特に高齢者を保護し，電話勧誘販売詐欺に対して高齢者が身を守る能力を向上させるための教育活動を認めることを目的とするものである[38]。

本法案は，電話勧誘販売詐欺の実行手段として，インターネット通信も対象に含める規定を盛り込み，連邦取引委員会に対しては，販売の促進，広告の提供又は商品若しくはサービスの販売をインターネットを介して行う際に，受信者の求めによらない商用電子メールの送信等も含めて，欺瞞的な行為によって行った場合に適用する権限の明確化を図っている。

第106回議会においても，いずれの法律案についても成立には至らなかった。

4-4　第107回議会に提出されているスパム規制法律案

スパム規制をめぐる法案は，現在の第107回議会においても多数提出されている。以下，提出法案を概観すると，2001年１月３日には，共和党のグリーン下院議員によって「受信者の求めによらない商用電子メール法案[39]」が提出されている。

この法案では，受信者が望まない商用の電子メールのメッセージを，合衆国内において保護の対象となっているコンピュータに対し，当該メッセージに含まれているドメイン名若しくは送信者識別情報が虚偽又は不正確であることを知りながら，故意に送信する行

脚注

36. Unsolicited Electronic Mail Act of 1999, H.R.3113, 106th Cong.（1999）.
37. Telemarketing Fraud and Seniors Protection Act, S.699, 106th Cong.（1999）.
38. 1999年２月４日に，ヴェーガン（Weygand）下院議員が提出した「高齢者対象詐欺に対する保護法案（Protection Against Scams on Seniors Act, H.R.612, 106th Cong.（1999）.）」も，同様の規制内容となっている。
39. Unsolicited Commercial Electronic Mail Act of 2001, H.R.95, 107th Cong.（2001）, H.R.718, 107th Cong.（2001）.

為を処罰の対象としている。

また，そのようなメッセージを送信する者は，受信者がそれ以降メッセージの受信を希望しない意思を表明することができるように，当該メッセージに正確な電子メールアドレスを明確に認識できるような状態で記載しなければならないとしている。

さらに，受信者が望まない商用の電子メールに関する方針を通知及び一般に認識可能な状態にし，受信者が当該メッセージを受信しない選択を行う機会を提供するなど，定められた要件に反して当該メッセージの送信に及んだ場合は処罰の対象となる。

なお，連邦取引委員会は，本法律に基づいて違反者に対して当該メッセージの将来的な送信を禁止し，受信者及びISPの氏名並びに電子メールアドレスを，送信者がすべてのメーリングリストから削除するよう命ずることができる。

受信者又はISPに対しては，本法律に定められた要件に反して電子メールを送信した者に対し，訴訟を提起する権利が与えられている。

また，同様の法律案として，連邦刑法典の改正によって，①誤認を生ずるインターネットのドメイン名又は他人の識別情報であることを認識しながら，保護されたコンピュータに対して受信者が望まない大量の電子メール・メッセージを故意及び許可なく送信すること，②当該電子メールの送信経路に関する情報を隠蔽することを目的として作成されたコンピュータ・プログラムの販売又は頒布することを禁止することを目的とした法律案[40]が提出されている。

その他，連邦刑法典の改正によって，電子メールのヘッダに表示される送信経路情報を，実質的に又は意図的に虚偽若しくは誤認を生ずる情報を用いて，受信者の求めによらない商用の電子メール・メッセージの送信に及ぶ行為に対して科料又は禁固に処すことを目的とした法律案[41]が提出されている。本法案では識別情報，オプト・アウトの手段，及び実社会における所在地を，受信者の求めによらない商用電子メールの本文中に記載することを要求し，違反行為に対する執行権限を，①連邦取引委員会，②指定政府機関，及び③合衆国政府に付与することを定め，インターネット接続に係る通信役務を提供しているISPに対し，本法の禁ずる違反行為によって被った損害賠償を請求する権利を付与している。

なお，移動体通信に限定した規制を試みるものとして，受信者が求めていない広告を送信することを目的として一般に公開されていない移動体通信のメッセージ・システムを利用する行為を禁止することを目的とした法律案[42]なども提出されている。

▶ 5　州法による規制

5-1　州レベルでのスパム規制

連邦レベルでは，スパム規制を目的として多くの法律案が提出されながらも，いずれも成立には至っていない一方で，州レベルでは，既に18の州においてスパム規制法が制定されている。

しかし，州レベルのスパム規制法は，連邦レベルでの法整備が実現していないという現状から，やむなく州毎に規制を行っているがゆえに，各州における規制内容の整合性が大きな問題となっている。

脚注

40. Anti-Spamming Act of 2001, H.R.1017, 107th Cong.（2001）.
41. CAN SPAM Act of 2001, S.630, 107th Cong.（2001）H.R.2162, 106th Cong.（2000）.
42. Wireless Telephone Spam Protection Act, H.R.113, 107th Cong.（2001）.

図１　州のスパム規制法

法　律	制　定	施　行	主な規制内容										罰　則
			オプトアウト	削除要求の尊重	虚偽送信者アドレスの禁止	第三者のドメイン使用禁止	送信経路情報の偽造	送信識別情報の明示	誤認を生ずる件名の禁止	ラベリング	事前の関与又は同意	ISPポリシー	
ワシントン州	Wash. Rev. Code 19.190（WEST Supp. 2000）	1998年３月	1998年６月11日。H.B. 1037（Wash. 1999）により改正。			●	●	●		●			消費者保護法で規定
ネバダ州	Nev. Rev. Stat. 41.705-.735（1998）	1997年７月	1998年７月１日	●	●	●			●			●		
カリフォルニア州	Cal. Bus. & Prof. Code 17538.4（1999）, 17538.45（Deering Supp. 2000）	1998年９月	1999年１月１日	●	●		●				●	●	●	５千ドル以上１万ドル以内の罰金及び深刻な事例に対しては禁錮（電子メール及びファックスの両者に適用）
ウェストバージニア州	W. Va. Code 46a-6G-1 et seq.（Michie 1999）	1999年３月	1999年６月11日			●	●	●	●	●			●	
テネシー州	Tenn. Code Ann. 47-18-2501, -2502（WEST, 1999 Rdg. Sess.）	1999年６月	1999年６月17日	●	●				●		●		●	
アイオワ州	Iowa Code 714E.1（WEST Supp.2000）	1999年５月	1999年７月１日	●	●	●	●	●	●			●		迷惑メールの定義（1000通以上のメール）
オクラホマ州	Okla. Stat. Tit. 15, 776.1 et seq., Tit. 74, 5060.52（WEST Supp.2000）	1999年６月	1999年７月１日			●	●	●						メール１通あたり10ドル以上１日あたり最大２万５千ドルの罰金
バージニア州	Va. Code Ann. 8.01-328.1, 18.2-152.2, -152.4, -152.12（Michie Supp. 2000）	2000年４月	2000年７月１日	●	●				●				●	メール１通あたり10ドル以上１日あたり最大２万５千ドルの罰金
デラウェア州	Del. Code Ann. tit. 11, 936-941（WEST, 1999 First Spec. Sess.）	1999年７月	1999年７月２日	●	●			●				●		
ロードアイランド州	R.I. Gen. Laws 6-47（1999）	1999年６月	1999年７月８日	●	●	●	●	●				●	●	メール１通あたり10ドル以上100ドル以下で１日あたり最大２万５千ドルの罰金
	R.I. Gen. Laws 11-52-1, -6, -4.1（1999）	1999年６月	1999年10月１日											
ルイジアナ州	La. Rev. Stat. 14:73.1(5), (8), (12), (13), 14:73.6（WEST Supp. 2000）	1999年７月	1999年８月15日			●	●	●					●	メール１通あたり10ドル以上500ドル以下の罰金
コネチカット州	1999 Conn. Acts 99-160（Reg. Sess.）	1999年６月	1999年10月１日。Conn. Gen. Stat. 52-59(b)により廃止											一般制定法によって各種違法行為（ハッキング，ウィルスの頒布等）が処罰の対象になっている
	Conn. Gen. Stat. 42 et seq., 52-59(b)(1999)		1999年10月１日			●	●	●			●		●	2500ドル以上の罰金
ノースカロライナ州	N.C. Gen. Stat. 1-75.4, 14-453, 14-458, 1-539.2a（1999）	1999年６月	1999年12月１日			●		●					●	メール１通あたり10ドル以上１日あたり最大２万５千ドルの罰金
イリノイ州	815 Ill. Comp. Stat. 511/1 et seq.（Supp. 2000）	1999年７月	2000年１月１日				●	●		●				メール１通あたり10ドル以上１日あたり最大２万５千ドルの罰金
コロラド州	Colo. Rev. Stat. Ann. 6-2.5-103（WEST, 2000 2d Reg.Sess.）	2000年５月	2000年６月３日	●	●	●	●	●			●			
アイダホ州	Idaho Code 48-603E（Michie Supp. 2000）	2000年4月	2000年7月1日	●	●	●	●	●	●					メール１通あたり100ドル以上1000ドル以下の罰金
ペンシルバニア州	18 Pa.C.S. 5903（2001）	2000年６月	2000年８月12日			●				●				虚偽送信者情報を用いて送信に従事した場合，メール１通あたり100ドル以上500ドル以下の罰金，又は90日以内の禁錮
ミズーリ州	2000 Mo. Legis Serv. 407.1310（WEST）	2000年６月	2000年８月28日	●		●		●				●		

Commission of the European Communities, Unsolicited Commercial Communications and Data Protection, Jan 2001 ; David E. Sorkin, Spam Laws<http://www.spamlaws.com/> ; Scot M. Graydon, Much Ado About Spam: Unsolicited Advertising, The Internet, And You, 32 St. Mary's L. J. 77(2000) ; Max P. Ochoa, Case Note: Legislative Note: Recent State Laws Regulating Unsolicited Electronic Mail, 16 Computer & High Tech. L.J. 459（2000）等に基づき作成。

Figure & Table

とりわけ，スパムの規制方法は，各州毎に大きく異なっており，スパム規制を主たる目的とした法律と，消費者保護の観点からスパム規制を試みる法律が混在しているのが現状である。

5-2　スパム規制法

①ネバダ州

州レベルのスパム規制が具体化したのは，ネバダ州において「1997年電子メール法」が制定されてからである。同法は，1997年７月１日に制定され，1998年７月１日に施行されている[43]。

ネバダ州のスパム規制法では，商用電子ダイレクトメールを送信又は送信されるようにした者は，受信者が受信した電子メール１件あたり，10ドルの損害賠償，弁護士報酬，及び訴訟費用の賠償責任を負うものとされている。

②ワシントン州

続いて，ワシントン州においても，スパム規制法が1998年３月25日に制定され，同年６月11日に施行されている[44]。

ワシントン州のスパム規制法は，ネバダ州法の後に制定されてはいるが，施行はネバダ州法よりも約１ヶ月早いため，州レベルのスパム規制法の中では同法が最初に施行されたものである。

同法は，「何人も，商用の電子メール・メッセージを，ワシントン州内に設置されているコンピュータから，又はワシントン州民の保有する電子メールアドレスであることを認識若しくは認識していることに合理性が認められながら，当該アドレス宛に送信してはならない。」とした上で，「⑷第三者に無断でインターネットのドメイン名を使用すること，発信元を特定する情報を偽ること」，及び，「⑹誤認を生ずる件名表示の禁止」について定めている。

違反者は，受信者に対して500ドル又は現実の損害のうち，賠償金額の大きい方の額を賠償しなければならないと定められ，双方向コンピュータ・サービス提供者が被った損害に対しては，1000ドル又は現実の損害のうち，賠償金額の大きい方の額を賠償しなければならないとしている。

また，ISPがスパムをブロックする措置については，「⑴双方向コンピュータ・サービス提供者が，当該事業者の提供するサービスを利用して送信される商用の電子メールが，本条に違反し又は違反していると信ずるに足る相当な理由がある場合には，その受信又は送信を，自発的に停止（block）することができる。」とし，さらに，「⑵双方向コンピュータ・サービス提供者が，当該事業者の提供するサービスを利用して送信される商用の電子メールが，本条に違反し又は違反していると信ずるに足る相当な理由がある場合には，その受信又は送信を停止するために自発的に講じた措置に対しては責任を負わない。」と定めることにより，ISPがスパムを遮断するために講じた措置によって責任を問われないようにしている。

脚注

43. Nevada Acts 1997 ch. 341, Senate Bill 13（codified as amended at NEV. REV. STAT., §S 41.705-41.735.）<http://www.leg.state.nv.us/97bills/SB/SB13_EN.HTM>.夏井高人教授による邦訳を参照のこと<http://www.isc.meiji.ac.jp/~sumwel_h/doc/code/act-1998-NRS41.htm>.
44. An Act Relating to Electronic Mail, 1998 Wash. Laws ch. 149, House Bill 2752.,（codified as amended at WASH. REV. CODE, tit.19.ch.19.190.）<http://www.jmls.edu/cyber/statutes/email/wah2752b.html>.夏井高人教授による邦訳を参照のこと<http://www.isc.meiji.ac.jp/~sumwel_h/doc/code/act-1998-RCW19.htm>。なお，同法の解説は，Miller, Steven（1999）, *Washington's "Spam Killing" Statute: Does It Slaughter Privacy In The Process?*, 74 WASH. L. REV. 453.

③カリフォルニア州

カリフォルニア州においては，スパム規制を目的とした三つの法律が制定されている[45]。

⒜ ボーウェン法（Bowen Bill：迷惑ファックス規制法の改正法）[46]

同法は1998年９月26日に制定され，カリフォルニア州において，不動産，商品，サービス又は信用枠の拡大等において，賃貸，販売，譲渡等の促進を目的として，受信者の求めによらない広告をファクシミリ若しくはファクシミリの送信を実行，又は電子メール若しくは電子メールの送信を実行する事業に従事することを禁止した。

また，①スパムの件名表示を「ADV:」から始めなければならないこと，②無料の電話番号又は電子メールアドレスを本文中に記載することにより，受信者がスパムの送信停止の意思を表示することができるようにする措置を義務づけた。

違反者には，５千ドル以上１万ドル以内の罰金及び深刻な事例に対しては禁錮となっているが，ISPや受信者が，同法に基づいてスパマーに対して訴訟を提起することはできない。

なお，同法は，2000年６月２日に合衆国憲法第１条の定める未発動の通商条項に違反するため違憲であるとの判決が下されている。

⒝ 刑法典第502条（カリフォルニア州包括的コンピュータ・データ・アクセス及び詐欺に関する法律）

スパム規制を目的とした刑法改正により，第三者のドメイン名を用いてスパムを送信することを禁止し，１台又は複数のコンピュータに損害を与えた場合には刑事処分の対象となる。同法に違反した場合は，１万ドル以内の罰金又は３年以内の禁錮刑に処せられるとしている[47]。

同時に，同法に基づく損害賠償請求訴訟を提起することができる。特に，無断で自らが保有するドメイン名が冒用されてスパムの送信を行う際に利用された場合，正規のドメイン保持者は，スパマーに損害賠償を求めることができる。

⒞ ミラー法（Miller Bill：営業及び職業倫理法第17538.45条[48]）

ミラー法では，ISPに自社が運営するネットワークを利用してスパムの送信を行った者を訴える権利を付与している。

同法に基づき，自社の提供するネットワークを利用してスパムの送信に従事した場合，又は自社の提供するサービスに加入している者に対してスパムを送信した場合に，電子メール・サービス提供者が当該スパムの送信者を訴えることができる。

本法の特徴は，自社の提供するサービスに加入している者が実行するスパムの送信行為だけでなく，外部から自社のサービス加入者に対してスパムを送信する者に対しても，訴訟を提起することができる点にある。

賠償請求額は，スパム１通あたり50ドル（１日最大２万５千ドル以内）又は現実の損害となっている。

④ウェストバージニア州

1999年３月13日には，ウェストバージニア州において「電子メール保護法[49]」が成立し

脚注

45. カリフォルニア州法の解説については，Bartels, David T.（1999）, *Review Of Selected 1998 California Legislation: Business Associations And Professions: Canning Spam: California Bans Unsolicited Commercial E-Mail*, 30 MCGEORGE L. REV. 420.
46. An act to amend Section 17538.4 of the Business and Professions Code, relating to advertising, Assembly Bill 1676（1998）（codified as amended at CAL. BUS.& PROF. CODE §§17538.4, 17538.45.）.
47. Assembly Bill 1629（1998）（codified as amended at CAL. PENAL CODE, §502）.
48. CAL. BUS.& PROF. CODE 17538.45（West Supp. 2000）.

ている。同法は，ウェストバージニア州民が保有する電子メールアドレスであることを認識していながら，①第三者のドメイン名を無断で使用又は商用電子メールの発信元を偽り，②虚偽又は誤解を招く情報を件名に表示し，③送信日時，送信者，及び返信先を明示せずに，又は④明らかに性的な表現を表示して，大量の電子メールを送信する行為を禁止している。

⑤アイオワ州

1999年５月26日には，アイオワ州でスパムを規制する法律[50]が成立し，同年７月１日に施行されている。アイオワ州法は，返信先アドレスに無断で第三者の名前を使用すること，及び虚偽の電子メールの発信元を特定する情報を表示又は表示せずに送信すること，当該電子メールの受信拒否の依頼先メールアドレスを表示することを求めるなどの規制を行っている。

⑥オクラホマ州

1999年６月８日には，オクラホマ州でスパムを規制する法律[51]が成立し，同年７月１日に施行されている。オクラホマ州法は，①電子メールの発信元を特定する情報を偽って表示，②発信元を特定できる情報の非表示，③他人に損害を与えることを目的として虚偽，悪意的，又は誤解を招く情報を表示して，電子メールを送信する行為に対して，500ドル以下の罰金を科すとしている。

⑦テネシー州

1999年６月17日には，テネシー州で電子的な手段を用いた受信者の求めによらない広告の規制に関する法律[52]が成立している。同法は，受信者の求めによらない電子メール広告の規制について定めており，ファクシミリ又は電子メールを用いて受信者の求めによらない広告を送信する際には，そのようなファクシミリ又は電子メールの受信を拒否する意思を表示するために用いることができる通話料が無料の電話番号又は電子メールアドレスの表示を義務づけている。

⑧コネチカット州

1999年６月23日には，コネチカット州でコンピュータの不正使用を禁ずる法律[53]が制定され，1999年10月１日に施行されている。同法は，大量の電子メールを送信する際に，虚偽の電子メールの発信元情報又は送信パスを偽造する行為が禁止している。また，虚偽の電子メールの送信者又は送信経路を作成することを主な目的とするソフトウェアの頒布又は販売，譲渡若しくは頒布目的での所持を禁止している。

⑨デラウェア州

1999年６月23日には，デラウェア州においてスパムを規制する法律[54]が成立し，同年７月２日に施行されている。デラウェア州法は，許可なく大量の電子メールを故意に送信

脚注

49. Acts 1999, chapter 119, House Bill 2627, W. VA. CODE, ch. 46A. WEST VIRGINIA CONSUMER CREDIT AND PROTECTION ACT, art.6G. ELECTRONIC MAIL PROTECTION ACT .
50. House File 448（1999）(codified as amended at IOWA CODE ch. 714D).
51. OKLA. LAWS 1999, ch. 337, House Bill 1410（1999）.(codified as amended at OKLA. STAT., tit. 15. § 776.)
52. Public Acts 1999, Chapter No. 475（HB 530/SB 690）.(codified as amended at TENN. CODE ANN., tit. 47, ch. 18).
53. An Act Prohibiting Unauthorized Use of a Computer and Other Computer Offenses, Conn. Pub. Acts No. 99-160（1999）.
54. Public Act 135, House Bill No. 242（1999）.(codified as amended at DEL. CODE, tit. 11, § 931, §§937 & 938).

する行為を禁止し，虚偽の返信先情報を作成することを主な目的としたソフトの頒布又は販売，譲渡若しくは頒布目的での所持を禁止している。このような規制は，他州にも見られる規制内容であるが，デラウェア州のスパム規制法は，スパムを受信した時点において，送信先アドレスのコンピュータ・システムの利用者がデラウェア州内に在住している場合，デラウェア州外から送信された電子メールも適用の対象としている点に特徴がある。

⑩ノースカロライナ州

1999年６月25日には，ノースカロライナ州でスパムを規制する法律[55]が成立し，同年12月１日に施行されている。ノースカロライナ州法は，コンピュータ又はコンピュータ・ネットワークの使用における禁止事項として，受信者を欺くことを目的として虚偽の発信元情報を用いて大量の商用電子メールを送信する行為を禁止している。

なお，本法の規制対象となる「受信者の求めによらない商用電子メール」の定義として，「『受信者の求めによらない』とは，商業的又は個人的な関係を有する受信者に対するものではなく，受信者の送信要求又は明示的な同意に基づく送信に該当しない行為をいう。[56]」と定義され，規制対象となる「商用電子メール」とは，「その内容が商用広告で電子的に送受信されるメッセージであって，商品又はサービスを受信者に販売若しくはリースし，商業的な利益を得ることを主たる目的とするものをいう。」と定義されている。

⑪ロードアイランド州

ロードアイランド州では，1999年７月３日及び同月８日にスパムを規制する法律[57]が制定され，両法とも同年10月１日に施行されている。ロードアイランド州法は，州内に設置されているコンピュータを利用して商用電子メールを送信する行為，又はロードアイランド州民が保有する電子メールアドレスであることを認識しているアドレス宛に送信を行う場合には，通話料が無料の電話番号を表示又は受信者の求めによらない電子メールを受信した者が，受信を拒否する意思を表明することができる返信先アドレスを表示しなければならないとされている。

⑫ルイジアナ州

1999年７月９日には，ルイジアナ州において刑法改正によりスパムの規制に関する規定[58]が設けられ，同年８月15日に施行されている。ルイジアナ州法では，電子メールの送受信役務を提供しているISPの方針に反して，大量の受信者の求めによらない電子メールを送信することを目的として，ISPのコンピュータ，コンピュータ・ネットワーク，又はコンピュータ・サービスを使用することを禁止している。また，虚偽の送信者情報によって大量の受信者の求めによらない電子メールを送信することを目的として，無断でコンピュータ又はコンピュータ・ネットワークを使用することも禁止している。

⑬イリノイ州

イリノイ州では，1999年２月22日に，「イリノイ州電子メール法案[59]」及び「ファクシ

脚注

55. Session Laws 1999-212, Senate Bill No. 288.（codified as amended at N. C. GEN. STAT., §§14-453, 458.).
56. N.C. Gen. Stat. 14-453(10)（1993).
57. 1999 Pub. Laws ch. 479, House Bill 5641（codified as amended at R. I. GEN. LAWS, tit. 6, ch. 47.), 1999 Pub. Laws ch. 421, House Bill 5644（codified as amended at R. I. GEN. LAWS, tit 11, ch 52.).
58. Act 1180, House Bill 2228（1999）（codified as amended at LA. REV. STAT., tit. 14, §§73.1, 73.6）

ミリ及び電子メール商勧誘法案[60]」が議会に提出され，1999年７月22日に，「イリノイ州電子メール法[61]」が制定され2000年１月１日に施行されている。

イリノイ州電子メール法は，許可なく第三者のドメイン名を使用若しくは虚偽の電子メールの発信元を表示又は虚偽若しくは誤解を招く件名によって，電子メール広告を送信する行為を禁止している。また，電子メール送受信役務提供者以外の者が，スパムの受信によって現実の損害を被った場合には，損害の原因となった電子メール１通又は全てのメールあたり最低10ドル又は１日あたり２万千ドルの損害賠償及び弁護士費用を請求することができる。しかし，スパムの送信時に単に利用されたにすぎない電子メールの送受信役務を提供するISPに対しては訴訟を提起することはできないとされている。

一方，ISPが，スパムに起因する現実の損害を被った場合にも，メール１通又は全てのメールあたり最低10ドル，又は１日２万５千ドルの損害賠償及び弁護士費用を，スパムの送信を行った個人若しくは団体に対して請求することができる。

⑭バージニア州

バージニア州では，1999年４月12日に，スパムを規制するために民事訴訟に関する州法の改正を行い[62]，さらに，2000年４月８日には，大量の受信者の求めによらない電子メールを送信することを目的として，送信者情報を偽って電子メールを送信する行為を禁止することを目的としたコンピュータ犯罪に関する州法の改正を行い[63]，2000年７月１日に施行されている[64]。

⑮アイダホ州

2000年４月17日には，アイダホ州で「消費者保護法[65]」が成立し2000年７月１日に施行されている。本法は，不公正な大量の電子メール広告による宣伝行為に関する規制について定め，双方向のコンピュータ・サービスを，大量の電子メール広告の送信を行う目的で使用する者は，受信者が当該メールの受信拒否を示すメールを送信することができるように，電子メール広告内に電子メールアドレスを明確に識別できるように表示しなければならないと定めている。

また，①返信先アドレス欄内において，第三者の許可を得ずに第三者の氏名を偽って使用すること，②電子メールの発信先を特定する情報を偽ること，③送信先を特定する情報が含まれていない場合，③大量の電子メール送信者に対して，広告メールの受信拒否依頼を送信してから５営業日を経過した後に送信又は転送を行うことを目的として，双方向のコンピュータ・サービスを使用することも禁止している。

⑯ミズーリ州

2000年５月12日には，ミズーリ州において，電気通信を利用した商取引行為の規制に関する州法の改正が行われ，改正条項は，2000年８月28日に施行されている。

脚注

59. An Act in relation to electronic mail, Illinois Electronic Mail Act, House Bill No. 2616.
60. An Act concerning electronic communications and amending the Consumer Fraud and Deceptive Business Practices Act, Facsimile and Electronic Mail Commercial Solicitation Act, House Bill No. 2718.
61. Illinois Electronic Mail Act, PUB. ACT 91-233（1999）.
62. Virginia Acts 1999, ch. 886, 904, & 905（codified as amended at VA. CODE, tit. 8.01., ch. 9, §8.01-328.1）
63. Virginia Acts 2000, ch. 627（House Bill 526）（VA CODE, tit.18.2., ch.5., art7.1., §18.2-152.2, 18.2-152.4, & 18.2-152.12（1999））.
64. バージニア州法の解説は，Amaditz, Kenneth C.（1999）, *Canning "Spam" In Virginia: Model Legislation To Control Junk E-Mail,* 4 VA. J.L. & TECH. 4.
65. Consumer Protection Act, § 48-603E. Unfair Bulk Electronic Mail Advertisement Practices,（House Bill 505）（codified as amended at IDAHO CODE, tit.48., ch.6）

ミズーリ州法におけるスパム規制は，広告を内容とする電子メールを送信するにあたって，受信者がオプト・アウトすることができる方法を，電子メールのメッセージに記載することを義務づけ，記載内容として，無料の電話番号又は送信者の正確な返信先アドレスを表示することを義務づけている。

⑰コロラド州

2000年５月11日には，コロラド州において，「コロラド州迷惑電子メール法」が制定され，同年６月３日に施行されている。

同法の成立までには，スパム規制を目指して1997年１月30日に「迷惑な電子通信も含む欺瞞的な商行為の規制に関する法案[66]」が提出されたものの，商用電子メール広告の規制は見送られたという背景がある。当時は，スパムを直接規制することが結果的にできず，1997年４月24日にファクシミリを利用した商用広告を規制する法律が制定されている[67]。

しかし，この法律は，あくまでファクシミリを利用した商用通信を規制するものであることから，実質的にはスパム規制には有効な手段を提供することができなかったため，2000年５月にスパムを直接規制可能な法律が制定された。

同法において規制の対象となる「受信者の求めによらない商用電子メール・メッセージ（第6-2.5-102条⑸において定義）」とは，商品若しくはサービスを販売又はリースの促進を目的として，受信者の明示的な許可なしに送信される電子メール・メッセージをいうと定義されている。

同法の規制内容は，①実際の発信元を表示させずに行う送信行為，②転送情報又はその他の送信経路に関する情報を偽った送信行為，③第三者のインターネットのアドレス又はドメイン名を無断で使用すること，④電子メールの件名に「ADV:（文字の順序は，A，D，及びVの順とし，これらの文字の後にコロンを表示させること）」の４文字を表示させずに送信すること，⑤送信者の電子メール・アドレスのリストから受信者が費用を掛けずに容易に送信を停止する措置を取ることができるようにせずに送信する行為に対し，民事罰を科すというものである。

⑱ペンシルバニア州

2000年８月12日には，ペンシルバニア州において，猥褻及び性的な情報並びに当該行為の処罰に関する刑法の規定を改正することにより，電子通信を用いて性的な情報を頒布する行為の規制の一環としてスパム規制を目的とした法律が制定されている。

同法では，電子通信を用いて行われる広告の件名に，「ADV-ADULT」という文言を表示させることを義務づけている。また，虚偽送信者情報を用いて送信に従事した場合，メール１通あたり100ドル以上500ドル以下の罰金，又は90日以内の禁錮を科すとしている。

⑲その他の州の法律案

州レベルのスパム規制法は，連邦レベルの法案同様に，議会に提出されて直ちに制定に至っているわけではない。また，法案の提出時点では，スパム規制を目的としたもの

脚注

66. A Bill for An Act Concerning Deceptive Trade Practices Involving Unsolicited Electronic Communications, House Bill 1284.

67. COLO. REV. STAT. §1. 6-1-105(1).

であっても，スパムを対象とした規制内容では議会を通過させることができないとして，結果的に他の通信手段を利用した迷惑通信の規制という形で法整備を行った例もある。

そのため，法案が提出されながら，成立に至っていない州も多い。

ケンタッキー州では，商用電子メールであることが明確に区別できるようにし，発信元を明確に識別できる情報及び削除請求の方法を本文に示すことを義務づける法案[68]が，1998年１月６日に提出され，同年３月11日にも，同様の規制内容の法案[69]が提出されているが，結果的に成立には至らなかった。

その他，テキサス州[70]，ニュージャージー州[71]，ニューハンプシャー州[72]，ニューヨーク州[73]，マサチューセッツ州[74]，メリーランド州[75]等においてもスパムの規制又は禁止について定めた法律案が提出されるなど，スパム規制を目的とした新法の制定や現行法の改正による規制強化を予定している州も多い。

5-3　消費者保護の一環としてのスパム規制

消費者保護の観点からスパムを規制することを目的として制定された法律においては，電子メールの送信にあたって適切な件名を用いることや，ヘッダの表示内容から送信者を識別できるようにすることを送信者の遵守事項として定めている場合が多い。つまり，これらの法律の特色は，消費者保護の一環として，消費者へのマーケティング活動の規制を行うことによって，その規制目的が結果的にスパム規制に寄与するものとなっている。

このような規制方法は，スパムのみならず，消費者に直接電話をすることによってマーケティングを行うテレマーケティングや，郵便等を利用したダイレクトメールの発送，新聞やテレビ等のマスメディアを利用した広告など，従来から行われてきた様々なダイレクト・マーケティングの規制に対しても行われてきたものである。

とりわけ，テレマーケティングが，数多く用いられているマーケティング手法の中でも，長年に渡って用いられる頻度が高い理由としては，ダイレクトメールやマスメディアでの広告と比べ，電話を利用することによって消費者との双方向のコミュニケーションが可能であることから，商品等への興味を喚起し易く，同時に消費者の反応も即時的に把握できることから，顧客転換率が他の媒体に比べて高いことがあげられる。

テレマーケティングには，消費者からの商品の注文や問い合わせを受けて受動的に行われる「インバウンド・テレマーケティング」と，業者側から消費者に対して電話を掛けるなどして能動的に行われる「アウトバウンド・テレマーケティング」の二種類の形態がある。さらに，アウトバウンド・テレマーケティングには，商品等の直接販売を目的として行われる「セールス・コール」と，将来的なマーケティング活動に利用することを目的とした顧客リストの作成や維持管理のために行われる「データベース・コール」

脚注

68. An Act relating to consumer protection, H.B. 41（1998）.
69. An Act relating to unwanted electronic mail and facsimile transmissions; relating to computer crimes; and providing for an effective date, H.B. 491（1998）.
70. An Act relating to unsolicited electronic mail; providing civil penalties, H.B. 1773（1999）.
71. An Act concerning commercial telephone 1and electronic mail1 solicitations and supplementing P.L.1960, c.69（C.56:8-1 et seq.）, Assembly, No. 295（1998）. An Act concerning unsolicited advertisements by electronic mail and supplementing chapter 170 of Title 2A of the Revised Statutes,Assembly, No. 513（1998）.
72. An Act restricting unsolicited commercial electronic mail, H.B.1633（1998）.
73. An Act to amend the general business law, in relation to requiring disclosures in connection with unsolicited electronic mail advertisements and requiring the affirmative consent of a consumer to use any electronic identifying information, S.B.2534（1997）. A.B. 06805.
74. An Act Relative to Unsolicited Electronic Mail, H.B.4581（1997）.
75. An Act concerning Consumer Protection - Unsolicited Electronic Mail Transmissions, H.B.1114（1998）

がある。

しかし，テレマーケティングを利用する事業者が増えるにつれ，商用の電話が個人の私生活の平穏を侵す機会も増大し，夕食の団らん時にテレマーケティングの電話を受けるなど，受信者が望まない時間帯に電話を受信する機会が増えつつあることなどが社会的に問題となった。そこで，米国では，受信者の求めによらない勧誘電話を一方的に掛けることが，逆に事業者のイメージに悪影響を及ぼすと考えられるようになり，受信拒否者リスト（do-not-call lists）の作成を行う事業者も現れてきた。さらに，1998年にフロリダ州が，受信拒否者リストの作成を目的とした法律を制定したのを嚆矢とし，2001年に入ってからは，テキサス州，コロラド州，ミズーリ州，イリノイ州，インディアナ州，ルイジアナ州，及びワイオミング州において相次いで受信拒否者リストに関する法律が制定された。

受信拒否者リストの仕組みは，当該リストへの掲載を希望する消費者がリストへの掲載を州に請求し，当該リストを州が事業者に貸し出すという仕組みをとっている。リストへの掲載については，年間10ドル程度の掲載料を徴収している州もあり，事業者側への当該リストの貸出についても，既に法律を制定しているすべての州で年間500ドルから800ドルの貸出料を事業者から徴収している。なお，違反者に対しては，違反通話１件あたり１万ドルから２万５千ドル以内の罰金が科される。

▶ 6　スパム規制のあり方

6-1　自主的な取り組み

欧州の一部諸国や米国の一部の州においては，既にスパムを規制するための法整備が行われているものの，国レベルでスパム規制を直接の目的とした法律を制定している国は，ほとんどないのが実状である。

しかし，日常的に大量のスパムが送信されているのは厳然たる事実であり，法規制の遅れによって問題への対処を今後も放置することが適切であるとは考えられない。

また，大量のスパムを取り扱わなければならない通信事業者にとっては，スパム対策は喫緊の課題となっている。

そのため，スパムを取り扱わざるを得ない通信事業者は，加入者をスパムから守るための対策と，外部からスパムの流入をブロックするための対策の両面から，①利用規約によるスパムの送信禁止，②スパマーに対する訴訟の提起，③スパムのブロック措置等の方策を講じてきた。また，ユーザ側にも，スパムのフィルタリングや受信拒否などの選択が提供され，携帯電話向けのメール・ウォール・サービス[76]なども注目されてはいるが，それらの措置を回避する方法で送信されてくるスパムには実質的には効果がない。

通信事業者がサービスを提供するにあたっては，スパムの送信行為も禁止行為に含めた附合契約を定める事業者が増えつつある。これによって，実際にスパムを送信する際には複数のISPを経由しなければならないことから，経由するISPすべての利用規約に適合する方法でメールを送信することが求められることになる。同様の措置は，既にISP毎に送受信可能文字数やメールボックスの容量などに関する規約で用いられている。しかし，そもそもスパムの送信は利用規約に従わないで行われるのが通例であることから効果は望めないであろう。

脚注

76. The Brightmail Anti-Spam Solution（last visited Nov. 24 2001）
<http://www.brightmail.com/products_antispam.html>.

そこで，現実的な対処方法として，スパムをブロックする措置を講ずる事業者も増えており，その方法としては，不正中継ホスト（サーバ）からのメールをブロックする方法が一般的に用いられている。

通常，スパムの送信は，いわゆる踏み台サーバ等，第三者中継を許すサーバを介して実行される。そこで，そのようなサーバのIPアドレスの一覧を，RBL（Realtime Blackhole List）としてデータベース化することによってスパムをブロックする方法が用いられている。

しかし，RBLに登録されているIPアドレスは，逆にスパムの送信に利用することができるサーバを示すことにもなることから，IPアドレスの一覧をすべて公開するのではなく，管理者からの個別の問い合わせに応じて，そのIPアドレスが不正中継サーバに該当するか否かを通知するという仕組みを取っている。

そのような仕組みを提供している組織として，Mail Abuse Prevention System LLC（MAPS）[77]や，Open Relay DataBase（ORDB）[78]などがある。

しかし，MAPSやORDBのRBLの利用によって，スパムの受信量を減らす一定の効果が認められる一方で，一度リストに登録されてしまうと，当該リストからの削除後もキャッシュにデータが登録されているIPからのメールはすべてブロックされてしまうことや，そもそも，私企業がRBLを管理することの是非などが問題になっている。

なお，上記のような措置をISPが講じた場合，通信の秘密の保障や検閲の禁止との関係で責任を問われる可能性もあることから，事業者側の免責について法律で定める必要がある。

現に，スパム規制法を制定している全ての州が，通信事業者の免責に関する規定を置いており，その内容は，①通信事業者の提供するサービスを利用してスパムが送信された場合の免責，及び②スパムのブロック等の措置を講じた場合の責任を免除することを目的とした場合の免責に大別できる。

なお，自主的な取り組みの範疇に含まれる活動として，実社会におけるDM同様に，受信を希望しない者への配信を停止する「電子メール・プレファレンス・サービス: e-MPS（Electronic Mail Preference Service）[79]」が，米国ダイレクト・マーケティング協会（DMA）[80]から提供されている。

さらに，スパムに対する社会的な反感に呼応して，反スパムを目的とした活動を行っている団体として，「CAUCE[81]」，「EuroCAUCE[82]」，「CAUBE[83]」などがある。

6-2　スパム規制を目的とした法律の整備

通信事業者や利用者による自主的なスパム対策は，それらの措置を回避する方法でスパムを送信する事業者や，法的制裁を回避することを前提にスパムの送信に従事している泡沫事業者などには何の効果もない。

よって，電子メール利用者が一方的にスパムを受信せざるを得ない状況が厳に存在していること，ならびに，受信拒否のための措置を講じても実効性が低く，スパマーのネットワーク利用倫理意識も極めて低い現状からすると，スパム規制を目的とした立法措置を

脚注

77. Mail Abuse Prevention System LLC <http://mail-abuse.org>.
78. Open Relay Database <http://www.ordb.org>.
79. The DMA's e-Mail Preference Service <http://www.e-mps.org>/
80. The Direct Marketing Association <http://www.the-dma.org>.
81. The Coalition Against Unsolicited Commercial Email<http://www.cauce.org>.
82. The European Coalition Against Unsolicited Commercial Email<http://www.euro.cauce.org/en/index.html>.
83. Coalition Against Unsolicited Bulk Email, Australia <http://www.caube.org.au/>.

講ずる以外に実効性あるスパム問題の解決の方途はない。

しかし，実際の規制にあたっては，電子メールの送受信の仕組みが実社会の領域概念を超越した上で成り立っているものであるがゆえに，規制の範囲や対象を限定することが困難であることから，米国の連邦レベルでの法制化の試みにも見られるように，現実の立法化にあたっては問題が山積している。

現に，米国の州レベルの規制は州によって規制内容が異なっており，EUの加盟国毎の規制も同様である。しかし，スパムの流通は，州境や国境といった実社会における領域とは関係なく流通するものである。よって，州レベルや加盟国毎に規制内容が異なると，規制の実効性の問題のみならず，スパムには該当しない商用の電子メールを送信する者にとっては，発信時に受信者に適用されるスパム規制に適合した方法でメールを送信するために，受信者の所在を明確に把握することが必要となるが，異なる規制すべてに対応した方法で電子メールを送信することは極めて困難である。

そのため，規制内容が異なる法律が複数制定されると，スパム規制を目的とした法律すべての要件に適合した送信を行うことが求められることから，「スパムの送信に従事する意欲を減退させる（daunting challenge）[84]」ことになると考えられていたが，実際には，零細のスパム送信者に対する萎縮効果としては効果を発揮しているものの，適法な送信を行っている一般の事業者の送信に対する萎縮効果のほうが大きいものと思われる。

a）正確な送信者識別情報の表示

スパムを規制するにあたっては，送信者を特定することができなければ，いかなる規制も無意味となる。なぜなら，送信者が識別できないメールに対して受信者が何らかの意思表示をしようとしても宛先不明のメールを再度受信することになるにすぎない。

よって，商用電子ダイレクトメールを送信するにあたっては，正確な返信先アドレスが表示されていることが最低限必要となる。なお，米国の州法では，無料の問い合わせ電話番号の表示が義務づけられている州もあるが，この場合，合衆国の国内では無料であっても，海外からは国際通話料金が掛かることから，同様に，国内の事業者であっても海外の窓口の問い合わせ電話番号を表示するなどした場合，この要件の効力については疑問が残る。

実際の措置内容については，事業者の窓口が異なるだけで担当者毎にアドレスや送信者名が異なるのが一般的であることから，送信者名の特定を求めることは現実的ではなく，送信事業者の正確なドメイン名の表示義務や，第三者のドメイン名の冒用を禁止するなどの措置が有効であろう。

なお，米国の州法では，第三者ドメインの無断使用によるスパムの送信行為を刑事処分の対象にしている州もあり，虚偽の返信先アドレスを用いてスパムを送信したスパマーが訴えられた事例も既にある[85]。

また，悪質なスパムには，虚偽の送信者識別情報が表示されているだけでなく，その発信元や送信経路も特定できないようにしているものも多い。これらの情報は，通常はヘッダに表示されるが，ヘッダを偽造するなどして送信者を識別できないように措置してある場合，受信者はスパムに対する一切の対抗手段がないのに等しい。そのため，ワシントン州法のように，ヘッダの偽造について規制している州もある。

脚注

84. Ochoa, Max P.（2000）CASE NOTE: Legislative Note: *Recent State Laws Regulating Unsolicited Electronic Mail*, 16 COMPUTER & HIGH TECH. L.J. 459, 465.

85. 判決では，消費者詐欺に関する法律に基づく損害賠償と，スパマーに対する差止命令を認めた。People v. Lipsitz, 663 N.Y.S.2d 468（Sup. Ct. 1997）.

b）受信者意思の尊重

スパムの問題で受信者を最も悩ませている問題は，将来的に同様のメールの受信を拒否する意思を送信者に伝えても，受信者の意思を無視してスパムの送信が継続されることが多い点にある。

そこで，受信者の意思を尊重する手段として，受信を希望する者にのみ配信を行う「オプト・イン方式」と，受信後に配信停止を希望した者への将来的な送信を停止する「オプト・アウト方式」がある。なお，どちらの方式を用いるにしても，その前提として，受信者に対して配信停止の方法の明示が法律で定められている必要がある。

米国ではオプト・アウト方式による規制論が趨勢を占め，EUではオプト・イン方式による規制が議論される機会が多い。両者の規制方針が異なるのは，個人情報保護に対する方針の違いによるところが大きいと思われる。

前者は，個人情報の不正な利用についてはプライバシー侵害として結果不法に至った場合にのみ責任が問われ，個別立法も個人情報の自由な利用を前提に分野毎の規制を行っているにすぎない。

一方，後者は，「個人データ保護」の観点から，個人情報の適正な取得，管理，及び利用を求め，電子メールアドレス等も含め本人の同意に基づく取得・利用を前提とした制度になっている。つまり，個人情報保護制度の違いが，そのまま「オプト・アウト」と「オプト・イン」の相違という図式として表れているといえよう。

よって，米国では，オプト・イン方式による送信規制は，送信者側の営業の自由を過度に侵害するものとして違憲であるとの主張が多いことから，結果的にオプト・アウト方式による規制が妥当であるとの方針をとっている。

そのような背景から，どちらの方式を選択すべきかが問題となっているが，オプト・アウト方式が，あくまで，同一送信者からのスパムの再受信の拒否という形態による限り，一度はスパムの受信を甘受しなければならないことや，送信毎に送信者が変幻するスパマーに対してはオプト・アウトの意味をなさないことから，実効性あるスパム規制を望む場合，オプト・イン方式による規制が妥当である。

オプト・イン方式の場合，最近では，①チェックボックスによる選択確認と，②確認メッセージの自動送信の二段階を経て，受信者へのメール送信が開始される「二重オプト・イン方式」を採用するものが多い。

特に，メールマガジンの普及に見られるように，受信者が「希望するとき，希望する情報を，希望した人だけに」送信する方式が定着しつつあり，このような方法を用いることによって，受信者の趣味嗜好に応じた商用電子ダイレクト・メールを送信することが可能になることから，結果的には，事業者側にとっても，消費者のニーズに適合したダイレクト・メールの送信を促進することが可能になる。

しかし，そのような規制を内容とする法律は，営業の自由に対する過度の制約にあたるとか，営利的表現の自由を侵害するものであるといった観点から違憲の疑いを指摘する見解も予想されるが，この点に関しては後述する。

c）誤認を生ずる件名表示の禁止

電子メールの送受信を行う際に用いられるアプリケーション（メーラー）には，定期的に受信を予定しているメールを，予め個別のフォルダに移動したり既読状態にするなどの振り分け設定を行うことができる機能が備わっている。つまり，メーリングリストに参加したり，メールマガジンを購読するなど，定期的に大量の電子メールを受信する場合でも，事前に，各メールの扱いについて一定のルールを設定しておけば，不定期に

受信する重要なメールを見落とすといった不測の事態を回避することが可能である。

ところが，受信者の振り分け設定を回避し，受信者にとって必要なメールであると誤認を生ずるような件名を表示してスパムが送信されてくることが多い。これは，スパムに限らず，コンピュータ・ウィルスやデマ・メールなどの送信にあたって用いられる常套手段である。つまり，そのようなメールであることを件名から判別できたり，件名がない正体不明のメールについては，受信者が警戒するのは当然であることから，受信したメールに対して警戒感や違和感を感じさせないようにするために，誤認を生ずる件名を表示するのである。

例えば，単に「御礼」とか「ご連絡」といった件名が表示されているメールに対して違和感を感じる人はいないであろうし，年末に，「忘年会のお知らせ」といったメールを受信すれば，大方の人が何の警戒心も抱かずにメールを開くのではないだろうか。

この問題については，カリフォルニア州法のように，スパムの件名の冒頭部分に，広告を意味する「ADV」又は未成年者禁止の広告を意味する「ADV:ADLT」という文言を件名の冒頭に表示させることにより，他のメールと識別できるように措置することを定めている法律がある。その他，テネシー州及びロードアイランド州にも同様の規定がある。

d）個人情報保護の観点からの規制

実際にスパムを送信するにあたっては，対象となる電子メールを取得又は作成する必要がある。電子メールのアドレスは，インターネット上の電子メール利用者の識別徴表であることから個人情報にあたることは明らかであり，個人情報保護の観点からは，電子メールアドレスの適正な取得が求められる。

ところが，実際には，電子メール・アドレスの取得時点における利用目的の明確化や本人の同意等がとられることは少ない。特に，ウェブ上に公開されている電子メールアドレスを，ウェブのmailtoタグを読み込むようなアプリケーション（ロボット）を用いて，地引き網的にメールアドレスを収集するような場合には，本人の同意以前の問題である。

さらに，取得の際の目的明確化や本人の同意に係る問題は，あくまで，電子メールアドレスを直接又は間接的に取得することを前提としているが，実際に，携帯電話等に送信されているスパムは，電子メールを「取得」して送信しているのではなく，ランダムに「作成」して送信しているに過ぎない。

これは，取得したメールアドレス宛に，本人の同意なしにメールを送信しているのと同様であり，個人情報保護の観点からすると，個人情報の不正な利用にあたるといえる。

電子メールアドレスの取得から利用に至るまでの一連の過程については，個人情報保護を目的とした法律による規制の対象として一般に考えられているが，スパム問題の根本的な原因は，受信者と何の関わり合いも持たない事業者が，受信者の意思に関わらず電子メール・アドレスを無断で利用してスパムを送りつけてくることにあることから，この点からしても個人情報保護の面からの規制が重要な意味を持つといえよう。

e）スパムの送信を目的としたアプリケーションの規制

大量のスパムを送信するためには，アプリケーション（スパムウェア: Spamware[86]）が必要となる。その際に用いられるものを大きく二つに分類すると，ウェブサイト

脚注

86. 2001年11月30日現在，328のスパムウェア販売事業者が稼働している<http://www.sengir.demon.co.uk/live_sites.html>.

図２　個人データ保護に関する法律と情報主体の求めによらない通信に関する諸外国の規定

	オーストリア	チェコ共和国	デンマーク	フランス	ドイツ	ギリシア	ハンガリー	アイルランド	イタリア	オランダ	スペイン	スウェーデン	イギリス	オーストラリア	日本	ニュージーランド	カナダ	アメリカ
個人データ保護に関する法律の制定状況	●	●	●	●	●	●	●	●	●	●	●	●	●	●		●	●	
個人データ保護に関する法律案の提出状況															●	●		
個人情報の取得																		
個人情報の取得時における情報主体への事前の告知内																		
氏名及び事業者の所在に関する情報	●	●	●	●	●	●	●	●	●	●	●	●	●	●*3	●			●
事業者内における個人情報管理者						●			●			●			●			
個人情報の提供を拒否する権利		●		●	●	●	●	●	●		●	●			●			●
個人情報の取得目的		●	●	●		●	●	●	●	●	●	●	●		●		●	●
提供先の名称													●					
個人情報へのアクセス権限を有する者の特定，第三者提供の有無	●				●	●		●	●				●	●*4				
個人情報の管理方法及び保存期間					●													
匿名化の有無及びその時期	●	●	●		●		●				●							●
個人情報へのアクセス，修正，削除，又は利用停止に関する情報主体の権利		●		●		●	●	●	●			●		●*5	●			
個人情報の再取得の有無	●		●		●		●	●	●	●	●		●					
一般事項としての個人情報を取得する際の同意確認の																		
口頭による同意	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●*6	●
書面による同意																	●*7	
同意の形態																		
黙示の同意	●	●*1						●						●				●
明示的な同意				●		●	●		●				●		●			
情報主体への告知	●		●							●								
曖昧ではない同意		●																
特定の機微な個人情報を取得する際に必要な同意確認の方法																		
口頭による同意	●	●	●	●	●		●	●		●		●	●	●	●	●	●*8	●
書面による同意						●			●		●						●*9	
同意の形態																		
黙示の同意	●	●*2						●										●*10
明示的な同意				●			●				●		●	●	●			
情報主体への告知	●		●							●	●							
曖昧ではない同意		●																
特定の機微な個人情報に該当する情報																		
人種，政治的信条	●	●	●	●	●	●	●	●	●		●	●	●	●	●			
思想信条	●		●	●	●	●	●		●		●	●		●	●			
信仰	●	●	●	●	●	●	●	●	●		●	●	●	●	●			
労働組合や業界団体への加入事実	●	●	●	●	●	●		●	●		●	●	●	●	●			
道徳観				●	●	●	●		●		●				●			
性的嗜好	●	●	●	●	●	●	●	●	●		●	●	●	●	●			
犯罪経歴		●	●	●	●	●	●	●			●	●	●	●	●	●		
健康状態	●	●	●	●	●	●	●	●	●		●	●	●	●	●		●	
収入							●										●	
ウェブサイト上へプライバシー・ポリシーを掲載する際の法定記載事項の存在									●*11		●		●	●*12				

Figure & Table

	オーストリア	チェコ共和国	デンマーク	フランス	ドイツ	ギリシア	ハンガリー	アイルランド	イタリア	オランダ	スペイン	スウェーデン	イギリス	オーストラリア	日本	ニュージーランド	カナダ	アメリカ
個人情報の管理，利用，及び提供																		
情報主体の求めに応じて氏名と住所を個人識別情報と分離しなければならない期間に関する定め	●	●*13			●	●*14	●			●	●	●				●		
遅滞なく実施	●				不明	不明	●									不明		
２ヶ月以内に実施					不明	不明					●	●				不明		
６ヶ月以内に実施		●*15	●		不明	不明				●						不明		
個人情報の第三者提供の規制	●	●	●*16		●	●	●*17	●	●	●	●	●	●	●	●	●	●	
一定の条件に基づき第三者提供を認容															●			
安全基準に基づき第三者提供を認容													●					
提供先の第三者の個人情報保護措置が必要	●	●			●	●		●*18	●*19	●*20	●*21	●	●*22	●*23	●		●	
一定の条件に基づき第三者提供を認容															●		●	
第三者提供にあたっては情報主体の同意が必要	●	●			●		●	●		●*24	●	●			●		●	●
一般要求事項としての同意要件	●	●	●*25				●	●	●		●	●	●*26	●*27			●	●
特定要求事項としての同意要件	●		●				●							●	●		●	●
第三者（特にクライアント）への個人情報の提供が可能な場合																		
苦情に対するフォローアップ目的	●					●		●	●		●	●	●	●*29	●	●	●	
住所の更新目的	●					●		●	●		●	●	●	●*30	●	●	●	
情報主体への告知が行われている場合								●*31	●									
情報主体の同意がある場合	●								●		●	●	●			●	●	
情報主体の求めによらない通信																		
情報主体の求めによらない通信に関する規制の対象																		
固定電話	○		◎*32		○	○		○		○		○*34	○	○		○	○	○
携帯電話	○		◎*33		○	○		○		○		○*35	○	○		○	○	○
ファクシミリ	○				○	○		○				○*36	○	○		○	○	○
電子メール	○				○	○		○				○*37		○		○		○
情報主体の求めによらない通信を行う上で必要な事前同意を得るための手段																		
固定電話	○		○		○	○		○		○						不明		○
携帯電話	○		○		○	○		○		○						不明		
ファクシミリ	○				○	○		○					○			不明		○
電子メール	○				○	○		○								不明		○
情報主体の求めによらない通信を行う上でオプト・アウト・リストの確認が必要な通信手段																		
固定電話			○			○		○		○			○	○		○	○	○
携帯電話			○			○		○		○			○	○		○	○	○
ファクシミリ						○		○					○	○		○	○	○
電子メール						○		○						○		○		○
その他						○*38												
市場調査を目的として個人情報を取得する場合の措置																		
自動発呼システム又は無作為電話聞き取り調査（RDD）の実施要件																		
情報主体からの事前の書面による同意			○															
事前録音による発呼システムの使用禁止													○				○	○
発呼時間帯の制限																	○	
初回調査の時点で再調査の実施に関する許諾確認	○		○	○	○		○	○		○	○	○	○					

*1，*2 同意の証明が必要	*22　データ保護法の定める範囲内においてセキュリティのレベルがデータ管理者（Data Controller）と同程度の場合
*3，*4，*5　事前又は取得時点	*23　契約の範囲内での実施を要請
*6，*7，*8，*9　情報の種類によって異なる	*24　明示的な同意が必要
*10　インターネットで取得する場合には，明示的な同意，オプト・イン，及び本人への告知に基づく同意が必要	*25　書面による同意が必要
*11　個人情報を対象とする場合	*26　再委託は不可
*12　ウェブ・サイト上で個人情報の取得を行う場合，サイト管理者は，取得目的等，情報主体に取得時点に提示しなければならない情報を提供する必要がある	*27　取得目的の範囲内にある場合
*13　自主規制	*28　書面による同意が必要
*14　調査種別によって異なる	*29，*30　取得目的の範囲内にある場合
*15　自主規制	*31　受領者の氏名等の情報を情報主体に告知することが必要
*16　公的記録へのアクセスを含む	*32,*33　ランダムに自動的に発呼するシステムの使用にあたっては特別の許可が必要
*17　書面による同意が必要	*34，*35，*36，*37　本人の求めによらない通信が法律上原則禁止
*18　個人識別情報の提供は不可	*38　ダイレクトマーケティングを目的とするオプト・アウト・リストを政府機関が管理／当該リストのマーケティング・リサーチ目的での利用はマーケティング･リサーチ協会の決定事項
*19　情報主体への告知と同意が必要	○　ダイレクトマーケティングに適用
*20　統計目的での利用に制限	◎　ダイレクトマーケティング及びマーケティングリサーチに適用
*21　非営利目的での利用及びセキュリティの確保について書面による保証が必要	
ESOMAR, LEGISLATION ON DATA PROTECTION AND UNSOLICITED CONTACTS, G.R.A.N. Meeting 23 SEPTEMBER 2001に基づき作成。	

Figure & Table

（mailtoタグ）上の電子メールアドレスやニュースグループやMLに登録されているアドレスを収集したり，ランダムに文字列を組み合わせて電子メールを送信するために用いられる，「①プル型ツール」と，大量の電子メールの送信（バルク・メールの送信）や特定のメールサーバ又はISPを経由せずに大量の電子メールの送信に用いられる，「②プッシュ型ツール」に分類することができる[87]。

実際に，コネチカット州，デラウェア州，バージニア州法のように，スパムの送信にあたって送信経路等の情報を偽造することを可能にするソフトウェアの規制を目指している法律もある。

例えば，バージニア州法では，「何人も，以下に掲げるソフトウェアを，故意に販売，提供若しくは頒布すること，又は販売，提供若しくは頒布することを目的として所持することを禁ずる。」とし，規制対象となるソフトについて，「１．電子メールの送信に係る情報又は送信経路に係る情報の偽造を助長若しくは可能にすることを主たる目的として設計若しくは製造されるソフトウェア，２．特定の商業目的において用いられることが明らかな利用又は電子メールの送信に係る情報若しくは送信経路に係る情報の偽造を助長若しくは可能にすること以外の目的で用いられるソフトウェア，３．当該人物が市場に出すソフトウェア，又は電子メールの送信に係る情報若しくは送信経路に係る情報

脚注

87. *See* Commission of the European Communities, Unsolicited Commercial Communications and Data Protection（Internal Market DG - Contract n ° ETD/99/B5-3000/E/96）（January 2001）31-33.

の偽造を助長若しくは可能にすることを目的として用いる知識を有している人物と協力して行うその他の活動[88]」と規定している。

しかし，このようなアプリケーション規制については，「コンピュータのソース・コードは，コンピュータのプログラミングに係る情報及びアイディアの交換手段であることに疑いの余地はないことから，修正第１条による保護の対象と判断することができる[89]」との判断が下されていることからすると，アプリケーション規制については，憲法上の表現の自由の保障との関連で問題となる可能性がある[90]。

▶ 7　おわりに：スパム規制法の合憲性

スパム規制を目的とした法律を制定するにあたっては，規制の対象となるスパムの定義から，規制の内容に至るまで解決しなければならない問題が非常に多い。とりわけ，電子メールという通信手段を介して行われる広告の規制を主たる内容とする立法であることから，「営利的表現」の制約と「営業の自由」の制約が憲法上許容されるものであるかどうかが問題となる。

この点につき，米国の判例理論を参考に検討を試みるならば，既に学説及び判例の双方からスパム規制を目的とした法律の違憲審査に関する議論がなされており，その内容は，合衆国憲法第１条の通商条項の問題と，修正第１条の表現の自由の問題の二つに大別できる。

合衆国憲法第１条第８節第３号の通商条項の観点からは，州のスパム規制法の制定当初から，その合憲性に疑問を呈する学説が公表されている[91]。また，判例においても，ワシントン州[92]及びカリフォルニア州[93]の両州において，州のスパム規制法が通商条項違反にあたることから違憲であるとの判決が下されている。なお，その後，ワシントン州法については合憲判決が下されている。

ワシントン州スパム規制法合憲判決は，オレゴン州在住の被告人が，インターネットを活用して収益をあげる方法に関する本のマーケティングを目的として，受信者の求めによらない商用電子メール（UCE）又はスパムを，10万通から100万通インターネットで送信した事案であり，同州において，虚偽又は誤認を生ずる情報を当該商用電子メールの件名に表示させた行為が，スパム規制法（Wash. Rev. Code § 19.190.020(1)(b)）及び，消費者保護法（Wash. Rev. Code ch. 19.86）に違反する行為にあたるとして起訴されたというものである。

控訴審は，同法の規定は州際間通商に対して過度の負担となることから違憲であると判決したが，州最高裁は原判決を破棄し，同法は，ワシントン州民に対して直接送信される欺瞞的なUCE又は同州内に設置されているコンピュータからそのようなメールの送

解注

88. Va. Code Ann. 18.2-152.4(b)（1999).
89. Junger v. Daley, 209 F.3d 481, FED App. 0117P（6th Cir.2000).
90. スパムウェアの規制の問題については，Ochoa, Max P.（2000）CASE NOTE: Legislative Note: *Recent State Laws Regulating Unsolicited Electronic Mail*, 16 COMPUTER & HIGH TECH. L.J. 459, 468.
91. *See, e.g.*, Blake, Christopher S.W.（1998）Note, *Destination Unknown: Does the Internet's Lack of Physical Situs Preclude State and Federal Attempts to Regulate It?*, 46 CLEV. ST. L. REV. 129, 157, Burk, Dan L.（1996）*Federalism in Cyberspace*, 28 CONN. L. REV. 1095, 1132, Bassinger, Kenneth D.（1998）Note, *Dormant Commerce Clause Limits on State Regulation of the Internet: The Transportation Analogy*, 32 GA. L. REV. 889, 912.
92. State v. Heckel, 143 Wn.2d 824, 24 P.3d 404（June 7, 2001).本件の評釈として，平野晋（2001）「State of Washington v. Heckel ～迷惑メール規制州法が合憲であると判断された最新判例～」国際商事法務Vol.29, No.7, 896～7頁。
93. Ferguson v. Friendfinder, Inc., No. 307309（Cal. Super. June 2, 2000).本件の評釈として，平野晋（2001）「Ferguson v. Friendfinder事件 ～「迷惑メール」規制州法と州際通商条項との関係～」国際商事法務Vol.29, No.6, 774～5頁。

信に及ぶ行為だけを規制しているに過ぎないとして合憲であるとし，その後，連邦最高裁も上訴を棄却した(94)。

控訴審が違憲判決の根拠とした合衆国憲法の定める通商条項とは，州際通商を規制する法律を州レベルで制定することを禁ずる規定であるが，判例では，「未整備又は未発動の通商条項は，州際通商に対する差別的な扱い若しくは不当な負担を課すような州の課税又は規制を行うこと，及び国内市場の自由な通商を妨げる行為を禁止するものである。(95)」と解釈されている。

なお，当該条項は，州によるすべての州際通商に係る規制を阻止するものではなく，あくまで，連邦議会に排他的な規制権限があると考えられる領域についてのみ効力を発するものである。

よって，州最高裁によるスパム規制法の合憲判断は，インターネットが州際通商手段に該当することから連邦議会に規制権限があるため州法による規制は違憲と判断した下級審の判断に対し，同州内の住民に対して送信されるスパム又は同州内のコンピュータからの送信行為に対してのみ適用されるものであることから，州際通商に対して不当な負担を課す規制とはいえないとの判断に基づいている。

一方，修正第１条の保障する表現の自由の観点からは，営利的表現に対する規制に関する指摘(96)がなされているが，判例においては，スパム規制法について修正第１条の点から問題点を指摘したものはない。

なお，営利的表現については，憲法の保障する表現の自由の対象には含まれないと考えられてきたものの，現在においては，表現の自由の保護が認められていることは周知の通りであり，営利的な表現に対する規制の合憲性については，「ハドソン・テスト(97)」に基づいて審査がなされている。

この基準は，(a)合法的な商業活動に関する表現が真実であって欺瞞的なものではないこと，(b)違法な活動を促進する営利的な表現ではないこと，のいずれかに該当する営利的表現に対する規制については，その規制が，(c)表現活動を規制する上で十分に正当なものであること，(d)営利的な表現に対する過度の制約にあたらないこと，という二つの要件を満たしていることが要求されるというものである(98)。

我が国においてもスパム規制を目的とした法整備を行うにあたって，営利的表現の制約が問題になるとすれば，ハドソン・テストを参考にすることによって解決が可能であるといえよう。

また，営業の自由に対する規制についても，スパム規制の目的は，受信者の求めによらずに発信者情報を偽るなどして送信される商用電子ダイレクト・メールを規制することにあり，受信者の求めによってのみ商用電子ダイレクト・メールの送信を許可するオプト・イン方式に基づく規制を採用したとしても，電子メールを利用した一切の営業活動を禁止するものではないことから当該規制に対する厳格審査が妥当であるとは言えないであろう。よって，スパムに対する規制が，ネットワーク社会において重要な通信手段として位置づけられる電子メールの利用環境の適正化という目的達成のために必要かつ合理的な範

脚注

94. Heckel v. Washington, 2001 U.S. LEXIS 10036; 70 U.S.L.W. 3315 (October 29, 2001).
95. General Motors Corp. v. Tracy, 519 U.S. 278, 287 (1997).
96. Marcus, Joshua A. (1998) Note, *Commercial Speech on the Internet: Spam and the First Amendment*, 16 CARDOZO ARTS & ENT. L.J. 245.
97. Central Hudson Gas & Electric Corporation v. Public Service Commission, 447 U.S. 557, 100 S.Ct. 2343 (1980).
98.「ハドソン・テスト」については，*see* ROTUNDA, RONALD D. & NOWAK, JOHN E. (1995) CONSTITUTIONAL LAW, 5TH ED.1087-88, LOCKHART, KAMISAR, CHOPER, SHIFFRIN & FALLON (1996) CONSTITUTIONAL RIGHTS AND LIBERTIES , 8TH ED., 729-33.

囲にとどまるものである限り，公共性の高い通信の円滑な運営を著しく阻害する営利的表現行為に対して行う規制は受信者の意思を尊重するために必要な措置であって，営業の自由に対する不合理な制約にはあたらないことから，憲法適合性の面からもオプト・イン方式によるスパム規制を肯定できるものと思われる。

（2001年11月30日脱稿）

（新保史生　明治大学法学部講師）