

迷惑通信に関する電気通信事業者の責務研究会

報告書

2005年5月25日

株式会社NTTドコモ

モバイル社会研究所

概要

本報告書は近年激増している迷惑通信に関して現行の電気通信事業法の下でとりうる対策を整理し、電気通信事業者としてできること、或いはできないことを明らかにし電気通信事業の責務の内容を明確にすることを目的として行われた研究会の報告をするものである。

なお、研究会は2004年9月から2005年2月までに全5回行われた

日時：

第一回 2004年 9月22日

第二回 2004年 10月27日

第三回 2004年 12月1日

第四回 2005年 1月18日

第五回 2005年 2月21日

出席者（敬称略）：

中央大学法科大学院 教授 堀部政男

千葉大学法経学部 教授 多賀谷一照

東京大学法学部 教授 佐伯仁志

中央大学総合政策学部 教授 平野 晋

筑波大学大学院図書館情報メディア研究科 助教授 新保史生

富士通株式会社法務部 法務第一部長 丸橋 透

株式会社情報通信総合研究所 代表取締役社長 藤田 潔

森・濱田松本法律事務所 弁護士 横山経通

森・濱田松本法律事務所 弁護士 岡田 淳

株式会社NTTドコモプロダクト&サービス本部 担当部長 永田英昭

株式会社NTTドコモ法務室 担当部長 二階 信

「迷惑通信に関する電気通信事業者の責務研究会」 報告書

1. 迷惑メールの現状
 - 1-1. 迷惑メール対策の現状
 - 1-2. 携帯電話事業者による迷惑メール対策
 - 1-3. 迷惑メールの送信形態と発信者情報

2. 迷惑メールをめぐる論点
 - 2-1. 迷惑メールと通信の秘密
 - 2-2. 迷惑メールと役務提供義務
 - 2-3. 迷惑メールと媒介者の責任

3. 携帯電話事業者として取りうる対策
 - 3-1. 自社サーバにある情報の調査
 - (1) 受信者（契約者）の苦情・依頼等に基づくヘッダ情報の調査
 - (2) 受信者（契約者）の苦情・依頼等に基づかない通信記録の調査
 - 3-2. 事業者単独で行いうるブロック等
 - (1) 受信者（契約者）の苦情・依頼等に基づく特定送信者・属性メールのブロック
 - (2) 受信者（契約者）の苦情・依頼等に基づかない特定送信者・属性メールのブロック
 - (3) 発信者が自社ユーザである場合の利用停止・契約解除
 - 3-3. 他事業者への情報提供・対応依頼
 - (1) 受信者（契約者）の苦情・依頼等に基づくメール情報の他事業者への提供
 - (2) 受信者（契約者）の苦情・依頼等に基づかないメール情報の他事業者への提供
 - 3-4. 発信者側 ISP による他事業者の情報に基づく対策
 - (1) 他事業者の情報に基づく契約者情報等の調査
 - (2) 他事業者の情報に基づく利用停止・契約拒否

4. 迷惑メール対策の課題
 - 4-1. 総務省研究会で提示されている論点
 - 4-2. 迷惑メール対策における課題

1. 迷惑メールの現状

1-1. 迷惑メール対策の現状

電子メールは、インターネット利用者のほとんどが利用するコミュニケーションツールとして、インターネットの普及とともに、急速に社会に浸透してきた。我が国では、諸外国に先駆けて携帯電話メールが爆発的に普及しており、いつでもどこでも簡単にパーソナルなコミュニケーションを実現する手段として、広く利用されるようになっていいる。その一方で、いわゆる迷惑メールも 2001 年初めから不特定多数の携帯電話宛に送信されはじめており、社会的にも大きな問題となっている。

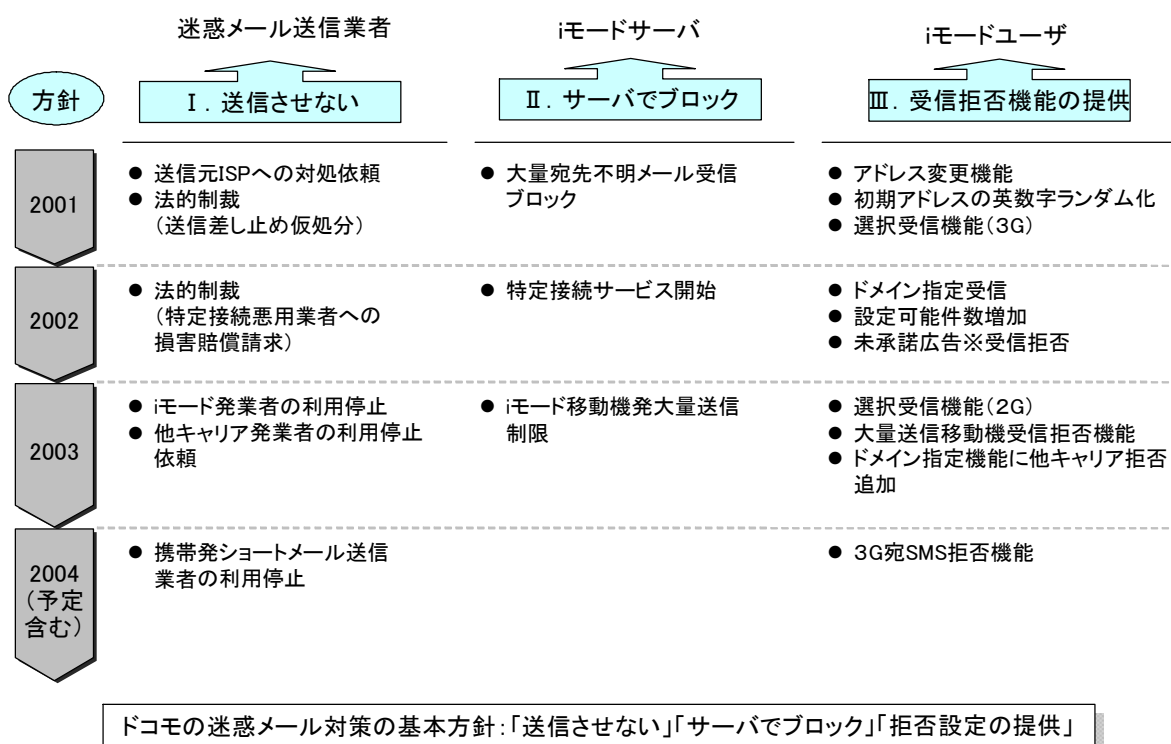
各携帯事業者は受信拒否機能等の技術的対策を講じており、総務省及び経済産業省も検討を行い、2002 年 7 月には迷惑メールに関し一定のルールを定める立法として特定電子メールの送信の適正化等に関する法律（以下「特電法」という。）及び改正特定商取引法が施行されている。しかし、近年、送信行為の巧妙化・悪質化等が進行しており、未だ迷惑メール問題は解決していないという状況が続いている。

1-2. 携帯電話事業者による迷惑メール対策

NTT ドコモでは、迷惑メールを「送信させない」「サーバでブロック」「拒否設定の提供」を柱とした迷惑メール対策を行っており、迷惑メール対策のための費用として平成13年度から平成15年度までの累計で約1,580億円を投じている（図1）。

ユーザの受信拒否機能（ドメイン指定受信機能）の提供等では大きな効果をあげているが、迷惑メールの大勢を占めるインターネット経由のメールはあまり減少しておらず、現在行われている事業者による対策では限界があるといわざるをえない。

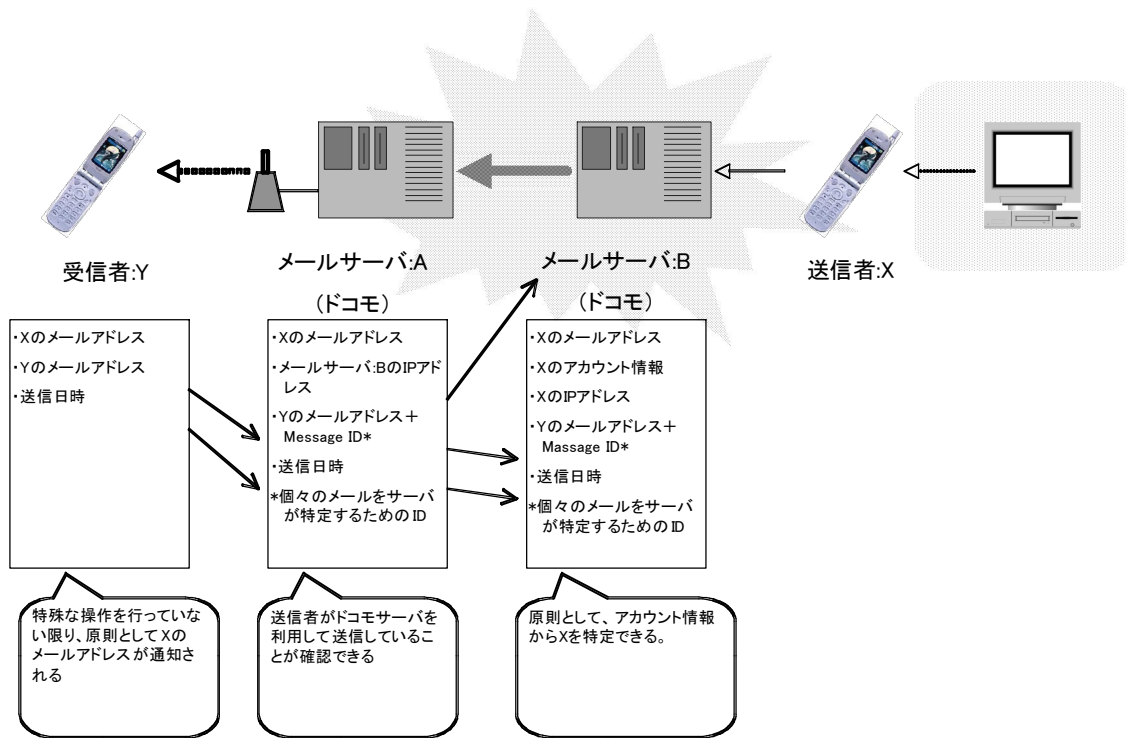
（図1）NTT ドコモの迷惑メール対策の基本方針



1-3. 迷惑メールの送信形態と発信者情報

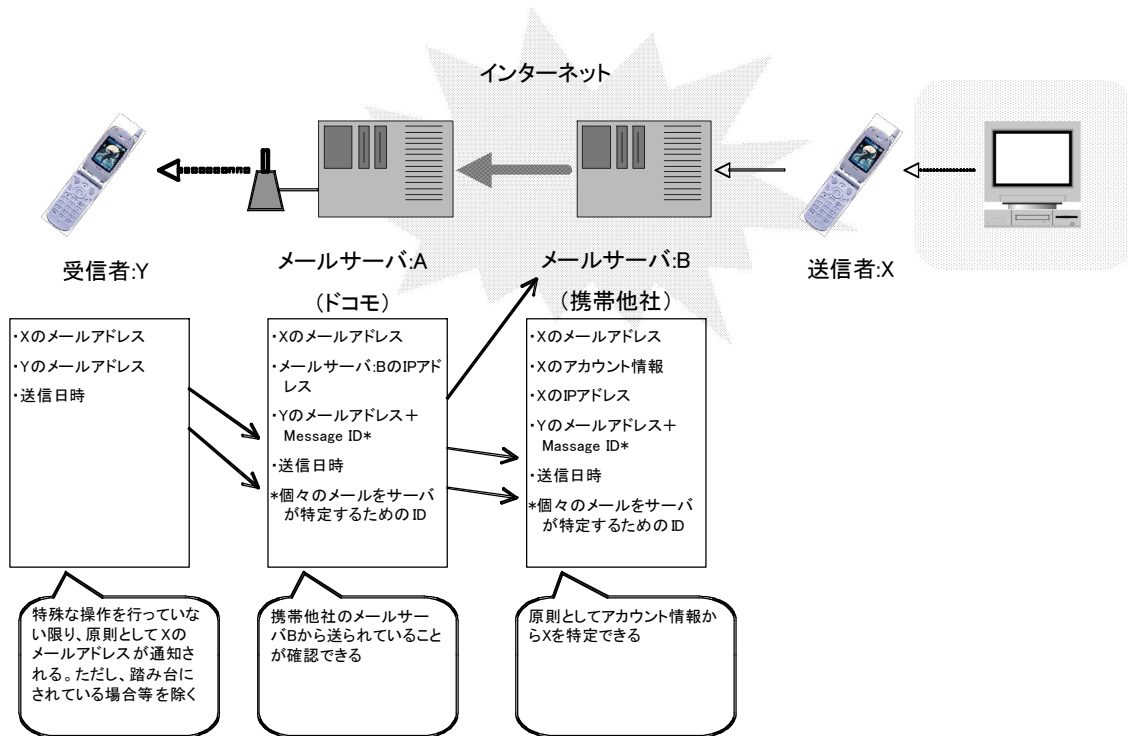
迷惑メールの送信形態としては、大きく①携帯電話から送信されるものと②携帯電話会社以外のISPを経由して送信されるものがある。①の携帯電話から送信されるもののうち、受信者と同一の携帯電話事業者の端末から送信されている場合には、発信者の情報はすべて当該事業者のサーバ上に保有されていることになる（図2）。したがって、これらの情報の調査が許されれば、対策は比較的容易であるといえる。

（図2）迷惑メールと発信者情報（ドコモのメールサーバを利用している場合）



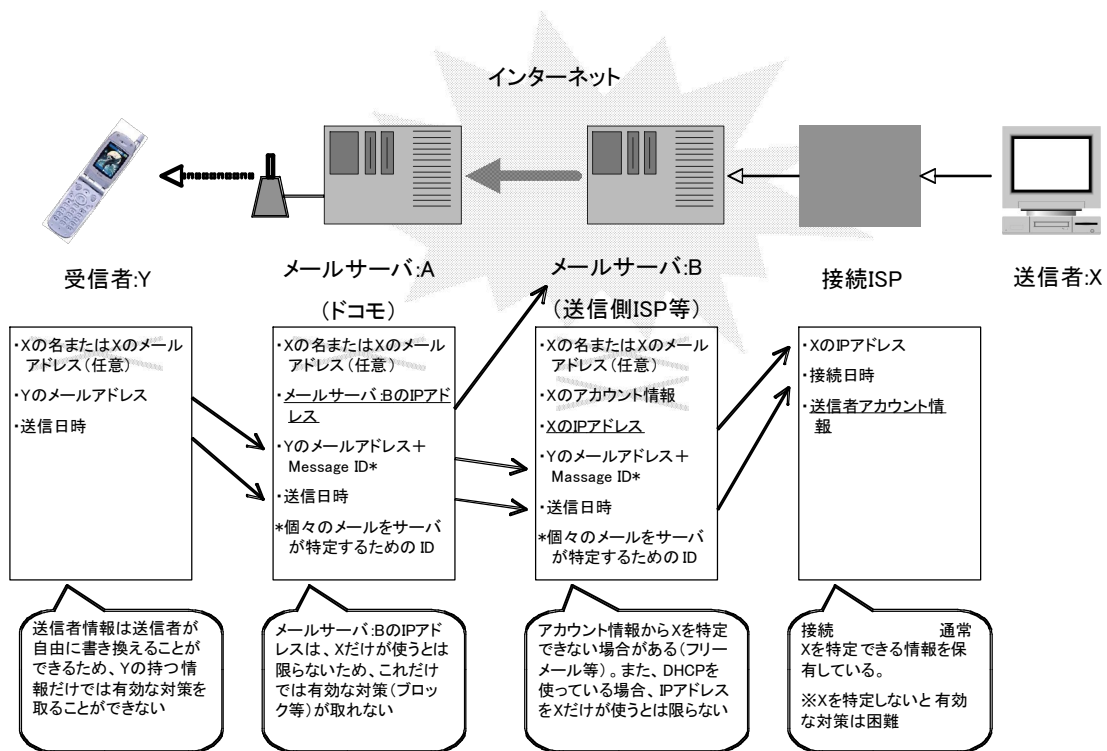
②の受信者とは異なる携帯電話事業者からメールが送られている場合でも、基本的に携帯電話から送られてくるメールはアカウントが特定できる場合が多いため、比較的ブロック等の対策が容易である（図3）。

(図 3) 迷惑メールと発信者情報 (携帯他社のメールサーバを利用している場合)



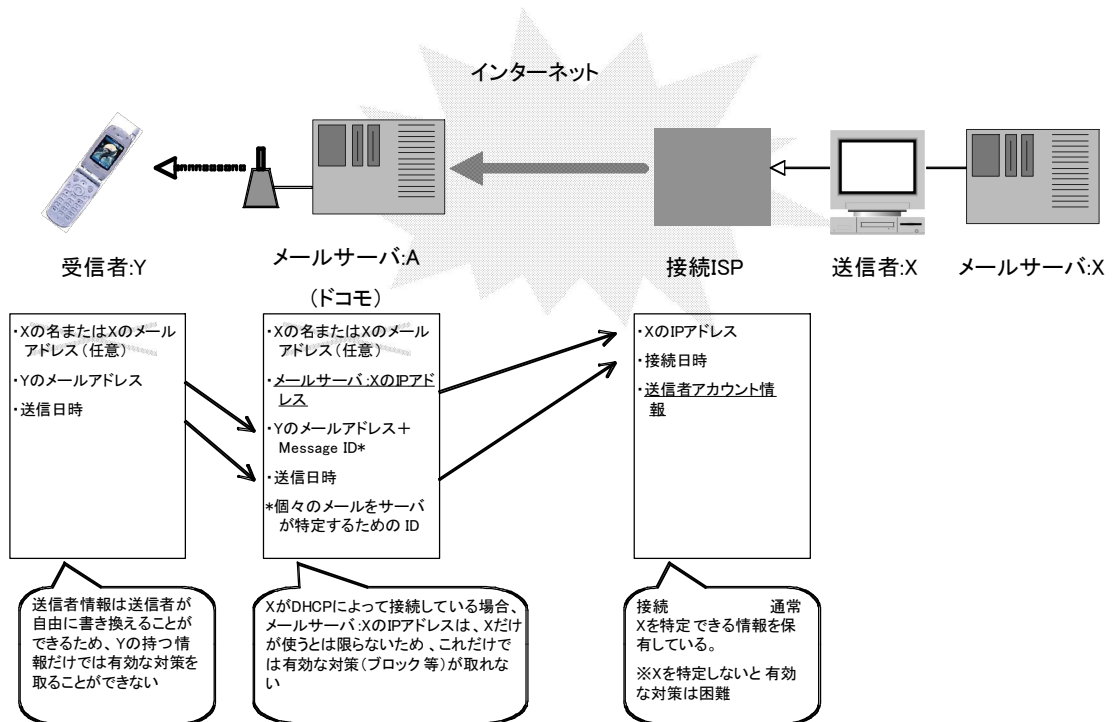
しかし、携帯電話会社以外の ISP 等のメールサーバを経由して送られてくるメールについては、メールのヘッダ情報に記載されている発信者情報は基本的に発信者が自由に書き換えることができるため、当該発信者から送信されたメールを有効にブロックすることが困難である。また、メールを送信する際に利用されたメールサーバの IP アドレスはヘッダ情報として受信者側に送信されるが、この IP アドレスはあくまでメールサーバの IP アドレスであって当該メールの送信を誰が行ったかを特定するためには、そのメールサーバを保有する ISP 等が通信記録等を調査しなければならない (図 4)。したがって、受信側だけでは有効な対策を行うことが難しい。

(図 4) 迷惑メールと発信者情報 (外部のメールサーバを利用している場合)



また、送信者がいわゆる「自前サーバ」を設置してメールを送信している場合には、当該送信者が利用している IP アドレスを受信側で知ることができるため、当該 IP アドレスからのメール送信をブロックする等の対策が考えられる。しかし、当該メールサーバにインターネット接続を提供している ISP が、動的 IP アドレスを付与している場合には、その IP アドレスが常に当該サーバに付与されるとは限らない (図 5)。したがって、この場合もメール送信時の IP アドレスをもとに当該 IP アドレスから送信されるメールをブロックするという方法は、必ずしも有効な対策にはならない。

(図5) 迷惑メールと発信者情報 (自前のメールサーバを利用している場合)



2. 迷惑メールをめぐる論点

2-1. 迷惑メールと通信の秘密・検閲

電子メールは一般に通信であると考えられているため、事業者が迷惑メールへの対応策を考えるにあたっては、通信の秘密との関係を検討する必要がある。我が国では憲法 21 条 2 項及び電気通信事業法 4 条において「通信の秘密」の保護が規定されており、特に電気通信事業法では「通信の秘密」の侵害は処罰の対象にもなっている。また、通信内容の検査・改変を行うことは、憲法 21 条 2 項及び電気通信事業法 3 条が禁止する検閲との関係からも問題となる可能性がある。

事業者が行う迷惑メール対策との関係では、(1) 迷惑メールを送っている者に関する情報（発信者情報）を調査することが許されるか、(2) 特定の特徴を持ったメールの送信や受信をブロックするためにメールに関する情報（メール属性）を調査することが許されるか、という点が問題となる。

(1) 発信者情報の調査

「通信の秘密」として保護される対象の範囲は、伝統的には「(ア) 電話、電報、その他の業務における通信の内容（ここでいう「業務」とは、業としてなされる、電気通信設備を用いて他人の通信を媒介し、その他電気通信設備を他人の通信の用に供する行為を指す）、(イ) (ア)に係る通信の発信者及び着信者の番号・氏名・住所、並びに発着信日時、(ウ) 特定の通信の存在の有無、特定人にかかる通信回数・通話時間など、(エ) 上記(ア)から(ウ)までの事項を実質的に推知せしめるもの¹」とされている。

メールのヘッダ情報やメールサーバの通信記録に含まれる発信者に関する情報は「通信の当事者の居所、氏名、発信電話番号・受信電話番号、通信回数、通信年月日など通信の意味内容をなすものではないが、通信そのものの構成要素であり、これらの事項を知られることによって通信の意味内容が推知されるような事項」に該当すると考えられ、これを「知ろうとする意思を持って、積極的に知ること（知得）」は通信の秘密の侵害にあたるとするのが、従来の通説の立場である²。

発信者情報が通信の秘密であるとしても、通信当事者である受信者の承諾がある場合に発信者情報を調査することは違法性が阻却されるとも考えられるが、「相手方にとっては通信当事者間限りで秘密とすべき通信もありうることから、一方の通信当事者の承

¹内閣法制局一発第 24 号「通信の秘密について」（昭和 38 年 12 月 9 日）

²藤田潔「電気通信とプライバシー」ジュリスト増刊『情報公開・個人情報保護』有斐閣、1994 年、225 頁

諾では、違法性が阻却されない場合がある（例えば、発信者の逆探知は、無限定で認められるものではない。）と考えられてきた³。

ただし、このような見解は、音声電話サービスを対象に、発信電話番号が着信者に通知されないシステムを前提としたものである。当時想定されていなかったような通信の形態における秘密の保護を考える場合は、メディアの特徴に即した検討が必要であるとも考えられる。通信の発展により、「公然性を有する通信」とも呼ぶべき新たな通信の形態が生まれていることは既に1990年代前半から指摘されており、このような通信における情報発信に対して通信の秘密をどのように考えるべきかが議論されている⁴。サービスの多様化に対応して通信の秘密概念は相対化しており、従来のような通信と新たにあらわれた私信性を持たない通信を区別して、通信の秘密を前者に限定することでより実質的に保護することができるとする見解もある⁵。発信者情報であるから無条件に通信の秘密として保護されると考えるべきではなく、発信者が自己に関する情報の秘匿に関する合理的な期待を持ちうるかどうかによって判断すべきであるという考え方もありうると考えられる。

現在、不特定の者に対して送信される「特定電気通信」については、プロバイダ責任制限法が発信者情報開示請求権の規定を設けている。しかし、電子メール等の1対1の通信については、「多数の者に宛てて同時に送信される形態での電子メールの送信であっても1対1の通信が多数集合したものにすぎない」ことから「特定電気通信」には含まれないとするのが総務省の立場である⁶。しかし、通信の秘密の例外として特定電気通信に関して発信者情報開示請求権が認められるのは、「それにより誰もが容易に発信をすることが可能であり（発信の容易性）、ひとたび被害が拡大すると容易に拡大し（被害の拡大性）、匿名で発信された場合には被害の回復が困難である（被害回復の困難性）などの特質をもつため⁷」であるならば、大量に送信される電子メールも同様の性格を

³電気通信法制研究会『逐条解説電気通信事業法』（第一法規、1987）24頁

⁴堀部政男「マルチメディア時代の放送の自由・通信の自由」根岸毅=堀部政男編『放送・通信新時代の制度デザイン 各国の理念と実態』（日本評論社、1994）28頁、堀部政男「電子情報とネットワークの社会的・法的課題」郵政省電気通信局監修=電子ネットワーク利用に関する調査研究会（座長：堀部政男）編『高度情報通信社会 日本の岐路 安全なネットワーク 危険なネットワーク』（第一法規、1996）6頁・40頁、郵政省電気通信局監修=電気通信における利用環境整備に関する研究会（座長：堀部政男）編『インターネットと消費者保護 インターネット時代における電気通信利用環境の整備に向けて』（クリエイト・クルーズ、1997）55頁以下

⁵多賀谷一照『行政とマルチメディアの法理論』（弘文堂、1995）192頁以下

⁶総務省電気通信利用環境整備室著=社団法人テレコムサービス協会編著『プロバイダ責任制限法-逐条解説とガイドライン-』（第一法規、2002）7頁

⁷大村真一=大須賀寛之=田中 普「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の概要」NBL No. 730（2002）28頁

持つと言える。このような考え方から、事案によっては、不特定多数に送信される電子メールも特定電気通信にあたるか解する余地があるとする見解もある⁸。

なお、実際に存在しないメールアドレスに向けた架空アドレス宛メールは、そもそも通信が有効に成立する可能性がないため通信の秘密の保護の対象ではないとも考えられる。電気通信事業法2条において電気通信事業を定義する際に、除外する通信の形態として「放送」をあえてあげていないのは、放送は「視聴者が不特定かつ多数で必ずしもこれを受信していることを要せず、法律上は受信者を通信相手として観念していない」ことも理由であるとされている⁹。このような考え方に立てば、宛先の存在しないメールは電気通信でないと考え得る可能性がある。しかし、有効に到達するメールだけを通信の秘密保護の対象とすると考えると、通常の利用においてメールアドレスを誤記したために未達になったメールも保護されないおそれもあり妥当ではないかもしれない。したがって、存在しないアドレス宛のメールであってもメールアドレスの誤記のような場合には、通信の秘密の対象として保護されるべきとも考えられる。しかし、一度に大量送信されており、かなりの割合で存在しないアドレスに向けたメールが含まれているなど、誤記でないことが外形から明確な場合には、通信の秘密の対象とはならないとする余地もあると考えられる。

(2) メール属性情報

まず、受信者から迷惑メールに関する苦情や対策要請等があった場合に、メールの属性情報（特定のメールアドレス・ドメイン・IPアドレス、「未承諾広告※」等の特定の文字列を含む、ウィルスのおそれがある等）を事業者が調査することによって通信の秘密を侵害しないかが問題となる。少なくとも、通信の当事者である受信者から提供を受けた情報を事業者が受け取ることは、事業者による通信の秘密の侵害にはあたらないと考えられる。したがって、受信者からの提供情報を確認する等の場合には通信の秘密を侵害することにはならない¹⁰。

一方、特定の受信者からの依頼・苦情等がない場合に、事業者がメールの属性を調査することは、原則として通信の秘密侵害や検閲との関係からも問題となる可能性があり、特に違法性阻却事由が認められる場合でなければ許されないと考えられる。

⁸飯田耕一郎編著『プロバイダ責任制限法解説』（三省堂、2002）34頁以下

⁹電気通信法制研究会『逐条解説電気通信事業法』（第一法規、1987）15頁

¹⁰電気通信法制研究会『逐条解説電気通信事業法』（第一法規、1987）24頁

2-2. 迷惑メールと役務提供義務

電気通信事業法は、認定電気通信事業者である携帯電話事業者に対して、正当な理由がない場合の役務提供拒否を禁じている（121条）。そこで、迷惑メールの受信をブロックすることが、この役務提供義務に違反しないかが問題となる。

まず、受信者からの依頼に基づいて特定の属性を有するメールをブロックすることについては、受信者には、特定の属性（特定のメールアドレス・ドメイン・IPアドレス、「未承諾広告※」等の特定の文字列を含む、ウィルスのおそれがある等）を有するメールを受信しない権利が認められると考えられる。したがって、少なくとも受信者に代わって事業者がこれをブロックするサービスを提供することは、提供義務違反にならないと考えられる。

次に、特定の受信者からの依頼・苦情等はないが問題のあるメールが送信されていることを事業者が認識した場合に、当該メールを受信者に配信することを拒むことができるかが問題となる。例えば、架空アドレス宛大量送信メール、コンピュータ・ウィルス添付メール等が送られている場合がこれにあたり、これらの行為が行われていることが役務提供を拒む正当な理由に該当するかを検討する必要がある。

従来の第一種電気通信事業者に課せられた役務提供義務（電気通信事業法旧34条）の例外が認められる「正当な理由」としては、「例えば、天災、地変、事故等により電気通信設備に故障を生じ役務提供が不能の場合、役務を契約約款に違反する条件で受けようとする者または料金滞納者に対する場合、正常な企業努力にもかかわらず、需要に対して速やかに応ずることのできない場合等」が想定されており、通信の属性が拒否事由になることはあまり想定されていなかった。特電法10条では、大量の架空アドレス向けメールについて一定の役務提供拒否を認めているが、特電法10条に該当する場合は、あくまで事業者が役務提供を拒否できる場合を例示したに過ぎず¹¹、同規定の定める「自己の電気通信設備の機能に著しい障害を生ずることにより電子メールの利用者に対する電気通信役務の提供に著しい支障を生ずるおそれがあると認められる」場合にあらなくても役務提供を拒否しうる場合はあり得るであろう。

なお、指定電気通信役務を提供する電気通信事業者の提供義務（25条）違反は罰則の対象となっている（178条）のに対して、認定電気通信事業者の役務提供義務違反については総務大臣による措置命令が出されるにとどまる（121条2項）ことから、指定電気通信役務を提供する電気通信事業者と比較すると、認定電気通信事業者のほうが役務提供を拒否しうる「正当な理由」は広く認められるとも考えられる。

¹¹総務省『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』（平成16年12月24日）27頁

2-3. 迷惑メールと媒介者の責任

迷惑メールの送信者に法的責任が問われる場合に、その通信を媒介した事業者にも法的責任が問われる可能性がないかが問題となる。送信者の責任としては、大きく刑事責任（詐欺罪、脅迫罪、恐喝罪、業務妨害罪、出資法違反、貸金業法違反等）が問われる場合と、受信者や事業者に対する不法行為責任が問われる場合が考えられる。

まず、刑事責任については、事業者が故意に積極的にこれらの行為を助長したというような場合でなければ問われる可能性はほとんどなく、あまり現実的な場面ではないと考えられる。

次に、送信者の行為によって損害が発生している場合に、事業者が民事上の責任を負わないかが問題となる。従来、電気通信事業者は、通信の秘密を守る義務を課されている反面として、電気通信役務を利用してなされた行為に対しては、責任を負わないと理解されてきた。

そもそも、不法行為は故意または過失に基づく人の行為によって生ずる（過失責任の原則）ものであり、その結果発生する責任は行為者本人が自ら負う（自己責任の原則）のを原則としている（民法709条）¹²。しかし、人の積極的な行動（作為）によってではなく、人がある行動を取らなかったこと（不作為）によって損害が発生することもある。このような場合、作為義務が存在し作為義務違反が違法であれば不法行為となるとされている。作為義務が認められ不作為の不法行為が認められる根拠は、「法令、契約、慣習ないし条理である¹³」といわれている。つまり、法令や契約によって明示的に示されていなくても、「私法秩序の一部をなすものとして法による強制を要請される慣習もしくは条理に基づく義務」があればこれに違反することは不法行為となりうる。ただし、本来的に不作為でいることは許されているのであり、不作為に対する責任を問うためには十分な根拠が必要であると考えられる。

ところで、事業者と受信者との間には契約関係があるため、不法行為責任だけでなく債務不履行責任も生じる可能性がある。債務不履行責任について判例で広く承認されている義務として安全配慮義務¹⁴があるが、これは当事者間に何らかの契約がある場合の不作為不法行為における作為義務と「多少のずれはあるにせよ、ほとんど重なり合う概念である¹⁵」とされる。事業者にこのような行為を防止する契約上の義務があるにもか

¹²加藤一郎『不法行為』（有斐閣、増補版、1974）62頁

¹³四宮和夫『不法行為』（青林書院、1987）292頁

¹⁴「ある法律関係にもとづいて特別な社会的接触の関係に入った当事者間に、その法律関係の付随義務として、相手方の生命及び健康等を危険から保護するような配慮をすべき義務（最判昭和50年2月25日民集2929巻2号143頁）」

¹⁵四宮和夫『不法行為』（青林書院、1987）663頁

かわらずこれを怠ったために損害が生じた場合には、債務不履行責任も問われることになる（民法 415 条）。

以上のように、第三者の行為について責任を問われるのは、立法による特別の定めがない限り、作為義務違反または安全配慮義務違反が認められる場合に限られると解すべきであろう。

なお、特定電気通信については、プロバイダ責任制限法によって、次のような場合以外はプロバイダが免責されることが定められている（プロバイダ責任制限法 3 条 1 項）。

1 当該関係役務提供者が当該特定電気通信による情報の流通によって他人の権利が侵害されていることを知っていたとき。

2 当該関係役務提供者が、当該特定電気通信による情報の流通を知っていた場合であって、当該特定電気通信による情報の流通によって他人の権利が侵害されていることを知ることができたと認めるに足りる相当の事由があるとき。

また、プロバイダ責任制限法成立以前に第三者の通信を利用した情報発信に関する媒介者責任が争われた例としては、パソコン通信におけるフォーラム（掲示板）管理者のフォーラム上での発言に対する責任について、「名誉毀損等の発言の存在を具体的に知ったと認められる場合に必要な措置を取るべき条理上の作為義務」があるとした判決がある¹⁶。

前述の通り、電子メールは基本的には特定電気通信に該当しないとされているが、これは 1 対 1 の通信であるため事業者の関与度合いが低いことも考慮されていることを考えれば、電子メールを提供する事業者の責任が特定電気通信役務を提供するプロバイダの責任より広く解されることはありえない。電報を使った脅迫について電話会社の責任が争われた事例でも、電話会社が電報の内容によってその配達を差し止める義務があるとする、「必然的に全ての通信内容の事前審査に通じるものであり、人が通信を利用して社会的生活を営むに際し、通信の内容が逐一吟味されるものとする、これら通信による情報伝達の萎縮効果をもたらし、自由な表現活動ないし情報の流通が阻害されることになる」として、裁判所は電話会社の責任を否定している¹⁷。

この判決でも触れられているように、事業者に通信内容に関する責任を認める場合には、事業者は通信の内容についてある程度の関与をすることを余儀なくされるため、従来の通信の秘密に関する考え方を維持することは困難となる。事業者の責任を考える際には、通信の秘密として保護すべき範囲に関する考え方も、当然に再検討される必要があると考えられる。

¹⁶東京高判平成 13 年 9 月 5 日判タ 1088 号 94 頁

¹⁷大阪地判平成 16 年 7 月 7 日判タ 1169 号 258 頁

3. 携帯電話事業者として取りうる対策

3-1. 自社サーバにある情報の調査

(1) 受信者（契約者）の苦情・依頼等に基づくヘッダ情報の調査

論点：事業者が、受信者からの苦情等に基づき、その受信者に送られてきた迷惑メールの発信メールアドレスや IP アドレス等に関する情報を調査することは通信の秘密の侵害にならないか。

インターネットにおいて発信メールアドレスや IP アドレス等に関する情報は、メールのヘッダ情報として通常受信者に送信されるものであり、携帯メールでは技術的な仕様によって送信されるヘッダ情報が制限されているものがあるに過ぎない。受信者が自ら受信したヘッダ情報を事業者に提供することは、通信の秘密の侵害にならないことは疑いがない。本来受信者に送信されるべきヘッダ情報が事業者の設備にとどまっている場合に、事業者の設備に保有されているヘッダ情報を受信者の承諾を得て確認することは、実質的には受信者が事業者に情報を提供することと同様に評価できる。したがって、事業者が受信者の依頼に基づいて受信メールの発信メールアドレスや IP アドレス等に関する情報を調査しても、基本的には通信の秘密の侵害にはならないと考えられる。

(2) 受信者（契約者）の苦情・依頼等に基づかない通信記録の調査

論点：事業者が、特定の属性を有するメール（架空アドレス宛大量送信メール、コンピュータ・ウイルス添付メール、特電法上の表示義務違反メール、架空請求等悪質なメール）について受信者からの苦情等に基づかずにそのメールに関する通信記録を調査することは、通信の秘密の侵害または検閲にあたらぬか。

架空アドレス向けメールのように受信者がそもそも存在しないメールによって被害が生じている場合には、事業者が受信者からの苦情・依頼等に基づかずに対応を行うことになる。この場合、発信メールアドレスや IP アドレス等に関する情報を得るためには、事業者が保有する通信記録を調査する必要がある。通信記録に関して「電気通信事業における個人情報保護に関するガイドライン（平成 16 年 8 月 31 日総務省告示第 695 号）の解説（以下「総務省ガイドライン解説」という。）」では、「発信者を探知するための通信履歴の解析は、目的外利用であるばかりでなく通信の秘密の侵害となることから、違法性阻却事由がある場合でなければ行うことはできないと解される」という見解を示している。この立場にたてば、どのような場合に事業者による発信メールアドレスや IP アドレス等に関する情報の調査について違法性が阻却されるかが問題となる。

違法性阻却事由が認められる場合として総務省ガイドライン解説では、「インターネットのホームページ等の公然性を有する通信において、違法・有害情報が掲載され、その発信者に警告を行わないと自己のサービス提供に支障を生じる場合(自己のサービスドメインからの通信がアクセス制限される場合等)に、自己が保有する通信履歴などから発信者を探知すること」を例示しており、公然性を有する通信について自社の事業運営に支障が生じる場合を念頭に置いている。

上記のような場合以外にも、例えば、特電法 10 条に該当し事業者が役務提供を拒むことができるような場合には、当然に当該メールの発信メールアドレスや IP アドレス等に関する情報の調査が許されるであろう。しかし、この規定は「自己の電気通信設備の機能に著しい障害を生ずることにより電子メールの利用者に対する電気通信役務の提供に著しい支障を生ずるおそれがあると認められるとき」とかなり限定的であり、このような状況に至らなくとも、ネットワークの保全のためにヘッダ情報の調査が許される場合もありうると考えられる。どのような場合に違法性が阻却されうるかについて個々の事業者による判断に委ねるよりは、客観的な基準を設けることが望ましい。

サーバに直接顕著な負担をかける架空アドレス宛の大量メールは、メールの内容を調査しなくても外形的にある程度判断をすることができるうえ、そもそも通信の秘密の保護対象となるか否かにも疑義があり、少なくとも違法性阻却の余地はあると考えられる。しかし、特電法における表示義務違反(未承諾広告であるにもかかわらず「未承諾広告※」の表示がないもの)や架空請求等の悪質なメールを調査するためには、特定の文字列等を含む電子メールを抽出する等メールの内容の調査を伴うことが想定されるため、通信の秘密の侵害に該当するおそれがある。メールの属性を確認するためにその内容について調査を行うことは検閲の観点から問題とされる可能性もあり、事業者の正当な業務行為として違法性が阻却されるものといえるか疑いがある。これらのメールに対する対策は、受信者からの依頼(苦情)を端緒として行わざるをえないと考えられる。

3-2. 事業者単独で行いうる対策

(1) 受信者（契約者）の苦情・依頼等に基づく特定発信者・属性メールのブロック

論点：受信者の苦情・依頼等に基づき、特定の属性（特定のメールアドレス・ドメイン・IP アドレス、「未承諾広告※」等の特定の文字列を含む、ウィルスのおそれがある等）を有するメールをブロックすることは、提供義務違反にあたらぬか。

受信者の発意により、特定の属性（特定のメールアドレス・ドメイン・IP アドレス、「未承諾広告※」等の特定の文字列を含む、ウィルスのおそれがある等）を有するメールをブロックすることは、受信者に当然認められるべき受信拒否の権利行使を実現するに過ぎず、このようなサービスを提供することは提供義務違反にならないと考えられる。

受信者に送信されるメールについて上記のような属性があるかどうかを判別することは、機械的なフィルタリングソフトによって行うことができ、事業者を含めて当該通信に関する情報を知得する者がいない（迷惑電話おことわりサービス類似の）仕組みで実現することが可能である。少なくとも、外形から明らかに判別できる属性を有するメールをブロックするサービスがこのような仕組みで行われる限りにおいては、通信の秘密の侵害にはならないと考えられる。ただし、これらのサービスの提供は基本的には契約者の選択に委ねられるべきであり、事業者がサービスを提供する際に特定の属性メールについてブロックすることを初期設定（デフォルト）とするためには、ブロックの方法等について約款や利用規約等に規定した上で実施することが必要であると考えられる。

(2) 受信者（契約者）の苦情・依頼等に基づかない特定発信者・属性メールのブロック

論点：事業者が、特定の属性（特定のメールアドレス・ドメイン・IP アドレス、特定の文字列を含む、ウィルスのおそれがある等）を有するメールを受信者の苦情等に基づかずにブロックすることは、提供義務違反にあたらぬか。

当該メールの受信が事業者の設備に負担をかけるなど、事業者がサービスを提供する上で必要な範囲であれば、特定発信者・特定属性メールのブロックを事業者自らの判断で行うことも許されると考えられる。

(3) 発信者が自社ユーザである場合の利用停止・契約解除

論点：発信者が、自社の契約者である場合、架空アドレス宛大量送信メール、コンピュータ・ウィルス添付メール、特電法上の表示義務違反メール等の送信を理由に利用停止や契約解除を行うことは、提供義務違反にあたらぬか。

電気通信事業法は、認定電気通信事業者である携帯電話事業者に対して、正当な理由がない場合の役務提供拒否を禁じている（121条）。そこで、架空アドレス宛大量送信メール、コンピュータ・ウィルス添付メール、特電法上の表示義務違反メール等の送信が、役務提供を拒む正当な理由に該当するかが問題となる。

これらの行為は社会的に悪質な行為であり、電子メールについては、多くの事業者がこのような行為を約款・利用規約において禁止している。このような社会的に受容されうる明示的な禁止規定が存在する場合には、このような規定に違反する行為を行ったものに対して利用停止や契約解除等の措置をとっても役務提供義務違反にはならないと考えられる。ただし、契約者の権利利益を不当に害さないよう留意する必要がある。受信者・事業者の被侵害利益も考量させてバランスのある検討を行う視点が重要であろう。また、どのような禁止事項を約款に定めることができるかは通信の形態によっても異なってくると考えられる。

3-3. 他事業者への情報提供・対応依頼

(1) 受信者（契約者）の苦情・依頼等に基づくメール情報の他事業者への提供

論点：受信者からの苦情等に基づきヘッダ情報から発信者が利用している ISP 等を調査し、メールに関する情報（発信メールアドレスや IP アドレス等に関する情報と苦情の内容）を当該 ISP 等に提供することは、通信の秘密の侵害にあたらぬか。

受信者から提供された発信メールアドレスや IP アドレス等に関する情報は通信の秘密に該当しないため、受信側 ISP がこれを受信者の希望に基づいて送信側 ISP 等に提供することも、通信の秘密の侵害にはならないと考えられる。ただし、受信側 ISP がこれらの情報から発信者が利用している発信側 ISP 等を調査することが、通信の秘密の侵害にならないかは別途問題となる。

この場合の IP アドレス等の情報は通信の一方当事者から適法に提供されたものである。一方、当該 IP アドレスをどの ISP が管理しているかということは一般に公開されている。したがって、受信者から提供された IP アドレス等の情報を公開情報と照合して発信側 ISP がどの事業者であるかを調査することは、通信の意味内容を推知されるような事項を新たに知得することにはあたらないと考えられる。したがって、これらの情報から発信者が利用している発信側 ISP 等を調査することは、通信の秘密の侵害にあたらない。

(2) 受信者（契約者）の苦情・依頼等に基づかないメール情報の他事業者への提供

論点：事業者が、発信メールアドレスや IP アドレス等に関する情報から発信者が利用している ISP 等を受信者の苦情等に基づかずに調査し、メールに関する情報（発信メールアドレスや IP アドレス等に関する情報と問題の内容）を当該 ISP 等に提供することは、通信の秘密の侵害にあたらぬか。

事業者が保有する発信メールアドレスや IP アドレス等に関する情報は、受信者から調査の依頼があるなどの特別な事情がなければ、事業者が保有する通信記録の一部と考えるべきであろう。総務省ガイドラインでは、「通信履歴は、通信の秘密として保護されるので、裁判官の発付した令状に従う場合等、違法性阻却事由がある場合を除き、外部提供は行わないこととする」という指針が示されており、電子メールに関連して、「電子計算機損壊等業務妨害罪（刑法 第 234 条の 2）に該当するような大量の無差別のダイレクト・メールが送りつけられ、自社のネットワークやサービスが脅威にさらされており、自己または他人の権利を防衛するため必要やむを得ないと認められる場合には、発信元の電気通信事業者に通信履歴（発信者の IP アドレス及びタイム・スタンプ等）を提

供すること」が許容される例として示されており、かなり限定的な場面が想定されている。

しかし、迷惑メールの増加に歯止めがかからない現状を考えると、特定の犯罪行為が行われていることが明確な場合や自社ネットワークが脅威にさらされている場合に限られず、社会的に重要な法益が侵害されているような場合等にも、違法性阻却を認めるべきであると考えられる。現在、不払い者情報の取扱いについては、総務省ガイドラインで事業者間の共有に関する指針が示され一定の場合に認められている（27 条）が、迷惑メールに関してもある程度明確な指針が示されることが望ましい。

なお、発信メールアドレスや IP アドレス等に関する情報から発信者が利用している ISP 等を調査する行為は、当該 IP アドレスをどの ISP が管理しているかということは一般に公開されている情報であり、その情報と照合を行うことは通信の意味内容を推知されるような事項を新たに知得することにはあたらないと考えられるため、通信の秘密の侵害にあたらないと考えられる。

3-4. 発信者側 ISP 等による他事業者の情報に基づく対策

(1) 他事業者の情報に基づく契約者情報等の調査

論点：他の事業者から提供されたメール情報に基づいて、当該メールを送信した契約者等の情報を調査することは、通信の秘密の侵害にあたらぬか。

受信側事業者から提供されたメール情報をもとに、当該メールを送信した契約者等の情報を調査するためには、発信者側 ISP 等が保有する通信記録とメール情報を照合する必要がある場合が多い。このような照合作業は、通説の立場では、「通信そのものの構成要素であり、これらの事項を知られることによって通信の意味内容が推知されるような事項」を「知ろうとする意思を持って、積極的に知ること（知得）」にあたり、原則として通信の秘密の侵害に該当すると考えられる。したがって、どのような場合に違法性阻却が認められるかが問題となる。

前述の通り、総務省ガイドライン解説では自社の事業運営に支障が生じる場合を念頭に置いた記述がなされており、発信者側 ISP がこのような状況におかれることは必ずしも多くない。しかし、迷惑メールの増加に歯止めがかからない現状を考えると、受信者側 ISP の事業運営に支障を生じるおそれがある場合や社会的に重要な法益が侵害されているような場合にも違法性阻却を認めるべきであると考えられる。

なお、発信側 ISP が当該メールを送信した契約者に対して固定の IP アドレスを付与しており、当該 IP アドレスから送信されたメールについての情報が提供されたような場合には、固定的に付与される IP アドレスは電話番号等と同様の顧客情報に属するものであり通信の秘密に該当しないと考えられる。

(2) 他事業者の情報に基づく利用停止・契約拒否

論点：発信者が、自社の契約者である場合、架空アドレス宛大量送信メール、コンピュータ・ウィルス添付メール、特電法上の表示義務違反メール等の送信を理由に利用停止や契約解除を行うことは、提供義務違反にあたらぬか。

電気通信事業法は、認定電気通信事業者である携帯電話事業者に対して、正当な理由がない場合の役務提供拒否を禁じている（121 条）。また、認定電気通信事業者でなくとも、契約者に対して正当な理由なく利用停止や契約解除を行うことは、債務不履行責任を問われる可能性がある。そこで、これらのメールの送信行為が役務提供を拒む正当な理由に該当するかが問題となる。

これらの行為は、社会的に悪質な行為であり、電子メールについては、多くの事業者がこのような行為を約款・利用規約において禁止している。このような社会的に受容

されうる明示的な禁止規定が存在する場合には、このような規定に違反する行為を行ったものに対して利用停止や契約解除等の措置をとっても、提供義務違反にはならないと考えられる。ただし、契約者の権利利益を不当に害さないよう留意する必要がある。受信者・事業者の被侵害利益も考量させてバランスのある検討を行う視点が重要であろう。また、どのような禁止事項を約款に定めることができるかは、通信の形態によっても異なってくると考えられる。

4. 迷惑メール対策の課題

4-1. 総務省研究会で提示されている論点

総務省では、迷惑メールに関する問題が根本的な解決に至っていない現状にかんがみ、「迷惑メールへの対応の在り方に関する研究会」を平成16年10月に設置して検討を進めている。12月24日には中間とりまとめが公表されているが、次のような検討の柱が示されている。

1. 政府による効果的な法執行
2. 電気通信事業者による自主規制
3. 技術的解決策
4. 利用者啓発
5. 国際協調

このうち、「1. 政府による効果的な法執行」に関しては、「SMS(ショートメッセージサービス)による広告宣伝メールの送信に対する規制」、「事業用メールアドレスに対する送信に対する規制」、「広告以外の架空アドレスあてメール送信の禁止」、「違反者への直接刑事罰の導入」について積極的な見解が示されている。また、「2. 電気通信事業者による自主規制」に関しては、特電法10条において規定されている電気通信事業者が役務提供を拒否できる事例は、「実際に電気通信事業者が役務の提供を拒否することについて正当性があると考えられる場合のうち一部の例示であり、これ以外にも正当事由の認められる場合は多く存在する」として、正当事由の認められる場合を明確化する必要性について示唆している。取り締まりの強化や電気通信事業者が役務提供拒否の範囲について積極的な検討を進めることが示されており、一定の効果が期待できる。

また、総務省では迷惑メール対策の一環として2月上旬から、民間事業者による自主的な迷惑メール対策を促す「迷惑メール追放支援プロジェクト」の試行を開始しており、4月上旬から本格運用の開始を予定している。具体的には次のような手順で行うこととされている¹⁸。

- (1) 財団法人日本データ通信協会に設置しているモニター機を利用し、
- (2) 当該モニター機が受信した同一送信者からのものと考えられる広告・宣伝メールの違法性を総務省が確認し、

¹⁸ http://www.soumu.go.jp/s-news/2005/050127_1.html

- (3) 携帯電話事業者等から得られるヘッダ（経路）情報を分析して送信元プロバイダを特定し、
- (4) 当該プロバイダに違法メールに関する情報提供を行うことにより、
- (5) 契約約款に基づく措置（利用停止、警告等）を促す。

4-2. 迷惑メール対策における課題

「3. 携帯電話事業者として取りうる対策」で検討をしたように、事業者が迷惑メール対策を行おうとする場合には、次のような点が特に問題となる。

(1) 受信者（契約者）の苦情・依頼等に基づく対策

受信側事業者が、受信者から情報の提供を受けてメールに関する情報を調査すること、特定の属性を有するメールをブロックすること、受信側事業者が発信側事業者に当該メールに関する情報（発信メールアドレスやPアドレスに関する情報と苦情等の内容）を提供すること、については基本的に問題がないと考えられる。しかし、情報の提供を受けた発信側事業者がこれらの情報を自社の通信記録と照合して発信者に関する情報を調査することが通信の秘密との関係から問題となるかどうかは必ずしも明確ではない。

(2) 受信者（契約者）の苦情・依頼等に基づかない対策

受信側事業者が自社のサーバに大量送信されたメール等に対して自主的に対策を行う場合には、当該メールに対する調査が通信の秘密との関係から問題となりうる。また、どのような場合に受信側事業者がメールブロック等の対策を取ることが許されるのか（提供義務違反にならないか）は、必ずしも明確ではない。受信側事業者が発信側事業者に当該メールに関する情報（発信メールアドレスやIPアドレスに関する情報と苦情等の内容）を提供すること、情報の提供を受けた発信側事業者がこれらの情報を自社の通信記録と照合して発信者に関する情報を調査することも通信の秘密との関係から問題となりうる。

しかし、特に受信者から一定の申し出がある場合に当該メールに関する調査を行うことは、基本的に許されると考えるべきである。総務省の「迷惑メール追放支援プロジェクト」においては、総務省が特電法上の表示義務違反にあたる迷惑メールに関する違法性を確認して発信側事業者当該メールに関する情報を提供することになっているが、発信側事業者が対策を行うにあたってはその情報と自社の通信記録を照合することが不可欠な場合が多い。少なくとも特電法違反等が明らかであり業務に支障を生じるおそれがあるメールに関しては、当該メールに関する情報を調査することの違法性が阻却され、通信の秘密の侵害にはならないと考えられる。

また、特に架空アドレス宛の大量送信メールに関しては、受信者からの苦情・依頼が

ない場合でも事業者としての対策が必要な場合がある。このような場合に正当な理由なく事業者間で個別のメールに関する情報を共有することは、通信の秘密との関係から問題となる可能性が高いと考えられる。どのような場合に事業者による発信者情報の調査や事業者間での情報共有が許されるかについては、各事業者の判断にゆだねるのではなく、共通の基準が示されることが望ましいといえる。

これら事業者による対策が可能な範囲が明確化された上で、特電法等における禁止事項を実効のあるものに見直していく必要がある。総務省研究会の中間とりまとめにおいても新たな禁止事項の拡充が検討されているが、悪質化・巧妙化の進む迷惑メールの現状に対応するための検討が常に必要であると考えられる。

以上のような理由から、本研究会としては迷惑メール対策のあり方に関する当面の課題として、次の3つの提言を行いたい。

1. 事業者による法令違反メールに関する情報の調査

上記のように、特電法違反等が明らかであり発信者側または受信者側事業者の業務に支障を生じるおそれがあるメールに関しては、発信側事業者が当該メールに関する情報を自社の通信記録との照合等により調査することは通信の秘密侵害に該当しないと考えるべきである。

2. 事業者間で情報共有を行いうる範囲の明確化

事業者間で正当な理由なく個別のメールに関する情報を共有することは、通信の秘密との関係から問題となる可能性がある。どのような場合に事業者による発信者情報の調査や事業者間での情報共有が許されるかについては、電気通信事業法および特電法との関係から明確な基準が示されるべきである。

3. 違法性を認定しうる禁止事項の拡充

新たな禁止事項の拡充については、悪質化・巧妙化の進む迷惑メールの現状に対応するために検討を継続して行うべきである。