資料　5

迷惑メールに係る対応方策について
（法制度に係る検討事項）

事　　務　　局

1　政府による効果的な法執行①（再掲）

「特定電子メール」等の定義の見直し

- 現在、通常のインターネット経由のメール送信に用いられるＳＭＴＰを利用した電子メールのみが対象とされているが、最近におけるＳＭＳを利用した広告宣伝メールの増加に鑑み、特定電子メールの定義にＳＭＳを含むように措置することが考えられる。
- 送信の対象として、現在は個人に限定（ただし、事業のために利用している場合は対象外）しているが、法人あるいは事業で利用している個人のメールアドレスあての送信についても対象とすることが考えられる。（法第2条関係）

論点

- 各社で様々なサービス内容が存在するＳＭＳの範囲をどのように画定するか。
- ＳＭＳを対象とする場合、表題部が存在しなかったり、文字数等表現能力が限定されていたりすることにより、現在ＳＭＴＰによるメールに課している表示義務を満たすことが困難となる場合があるが、異なる内容の表示義務を設けるべきか。
- 端末間で直接情報の送受信を行い事業者のサーバを経由しない場合、受信回避のための技術的対応が困難ではないか。
- 事業用メールアドレス等に対象を拡大する場合、事業を営む者の間でのメール送受信について、たとえば一定の継続的な取引関係にある場合を除外するか否かなど、具体的にどの範囲までを対象とすべきか。

SMTP：シンプルメールトランスファープロトコル。インターネットで電子メールを送信する際に、一般的に用いられている通信方式。
SMS　：ショートメッセージサービス。携帯電話同士で、短い文字メッセージを電話番号あてに送受信できるサービス。

SMSによる迷惑メールへの対応について

ＳＭＳを特定電子メール法の対象とする場合、以下のような点について、具体的にどのように扱うかを整理する必要がある。

表題部が存在しない、文字数が少ない等の制約

- 表示義務については、受信者に対して情報として提供することが必要な最小限のものについて定められていることから、その一部についてそもそも受信者に提供しなくてもよいこととするのは不適当と考えられる。
- 「未承諾広告※」の表示場所を本文の先頭で可とすることや、送信者の名称や住所等の詳細な情報については、それらの情報が示されている箇所へのリンクを掲載することで足りるものとすることも可能である。

⇒ 表示義務については、原則として現行のＳＭＴＰメールと同様の内容を課すこととするのが可能であり、また適当であると考えられる。

「未承諾広告※」と表記させる趣旨は、フィルタリング処理を行うためだけではなく、受信者が目視により広告宣伝メールであることを認識して内容を見るか否かを判断する機会を与えることを意味しており、一見して広告宣伝メールであることを識別することができるよう、メールの先頭部分に記述すべきものとする必要がある。

ＳＭＴＰを利用したメールとの技術的差異

- 携帯電話の利用者にとっては、受信するメールがＳＭＴＰを採用しているか否かによって大きな差は存在しないが、ＳＭＳの中には、端末間で直接情報の送受信を行うものがあり、現在提供されているようなフィルタリングのサービスを提供することが困難な場合がある。
- その反面、基本的に同一の携帯電話事業者のネットワーク内に送信者も受信者も存在するため、送信者を特定して利用停止等の措置をとることが容易であるという面も存在する。

⇒ 必ずしもＳＭＴＰメールと同一の受信回避の環境が整備できるわけではないが、事後的な対応はむしろ容易に行える面もあるため、大きな障害とはならないと考えられる。

SMTP以外の通信方式を使った主なメールサービス（SMS）一覧（再掲）

○ **各社共通の特徴**
- 受信者の電話番号あてに送信
- 件名がない（ボーダフォンのロングメール等を除く）
- 事業者側で、フィルタリング等を行うことが技術的に困難

	サービス名	文字数	送信料金※	備　考
NTTドコモ	ショートメール	50文字	5円	固定電話、公衆電話等からも送信可
	SMS（FOMA）	70文字	5円	
au	Cメール	50文字	3円	
ボーダフォン	スカイメール	64文字	2円	固定電話、公衆電話等からも送信可
	ロングメール	3,000文字	4円	件名入力可能
	SMS（VGS）	70文字	5円	
TUKA	スカイメール	64文字	5円	固定電話、公衆電話等からも送信可
DDIポケット	ライトメール	45文字	6円	固定電話、公衆電話等からも送信可
	DXメール	1,000文字	10円	固定電話、公衆電話等からも送信可 一部機種のみ件名入力可能
	Pメール	半角20字	6円	固定電話、公衆電話等からも送信可

※「送信料金」は、料金プランにより異なる場合あり

事業用アドレスあての迷惑メールによる被害について

特定電子メール法において、その送信の相手方として「個人」（事業のために電子メールの受信をする場合における個人を除く）のみを対象としているのは、法制定時に、営業の自由や表現の自由への制約を最小限にするという観点から、対象範囲について、もっとも被害が深刻である部分にできるかぎり限定することを意図していたものと思われる。

一方、迷惑メールの送信については、自動的にメールアドレスを生成したり、webサイトから自動的にアドレスを収集したりして大量に送信されることが多いと考えられることから、

- その送信先としては個人が私的に利用しているか否かは意識されていない
- 企業が必要に応じて不特定多数からメールを送信してもらうことを目的として公開している電子メールアドレスについては、公開されているために迷惑メール送信者が宛先として設定することが多い

と想定される。

大量の迷惑メールが企業等が事業に利用しているメールアドレスに送信されることにより、本来業務への支障も生じているのではないかと考えられるが、このような場合には、「電子メール送受信上の支障」（法第１条）が生じていると言うことができるのではないかと考えられる。

特定電子メール法による取り締まりの対象として、事業に利用されている電子メールアドレスを加えることが適当ではないか。

具体的に対象とすべき事業用アドレスあて電子メールの範囲について

事業に利用されているメールアドレスについて取り締まりの対象とする場合、以下のような点について、どのように取り扱うべきかが論点となると考えられる。

論点	考え方
事業に利用していることから広告宣伝を含めた事業に関する電子メールを受信することがそもそも想定されている場合が多い	※一律に広告宣伝メールの送信を規制の対象とする場合、業務に関連してメールを送信する者に対し過度の不便を強いることにならないか
私的な利用ではないため、プライバシーの侵害や平穏な生活の侵害といった問題は生じないのではないか	※企業のドメインあてに大量に送信されることで業務のための電子メール利用に不都合が生じるなど、私的な利用とは別の問題が生じているのではないか

→ たとえば、事業に利用しているメールアドレスに送信されるものについても、受信者の行っている事業と関係のない内容の広告宣伝メールのみを対象とすること、一定の内部関係にあると考えられる場合については対象外とすること、等が考えられる。

（参考）特定商取引法における対象範囲（通信販売の場合）

メールを受信する者について、特に個人に限定してはおらず、事業用アドレスあての電子メールも含まれているが、適用除外として、以下のものを規定している（特定商取引法第２６条）。

- 購入者が営業のために又は営業として締結する契約に係るもの等（第1号）
- 特別の法律に基づき設立された組合等がその構成員に対して販売等を行う場合（第4号）
- 事業者がその従業員に対して販売等を行う場合（第5号）

1　政府による効果的な法執行②（再掲）

架空アドレスあてメール送信を禁止する範囲の見直し

- 現在、架空アドレスあてのメール送信行為について、①自動アドレス生成ソフトウェアの使用により得たアドレスであること、②自己又は他人の営業についての広告又は宣伝の目的であること、が要件とされている。
- 電気通信事業者の設備に与える本来不要な過大な負荷については、大量の宛先不明メールが送信されている限りその送信手法による差異はないことから、この範囲を拡大することが考えられる。（法第5条関係）

論点

- 上記①について、自動アドレス生成ソフトウェアを使用する場合以外のアドレス生成手法としては、どのようなものが考えられるか。
- 上記②について、広告宣伝目的のメール送信以外に、大量に架空アドレスあてにメールを送信する行為としては具体的にどのようなものが考えられるか。
- 架空アドレスあての送信とは異なるが、web上を巡回して自動的にメールアドレスを収集して大量に送信する行為について取り締まりの対象とする必要はないか。

（架空電子メールアドレスによる送信の禁止）
第五条　送信者は、自己又は他人の営業につき広告又は宣伝を行うための手段として電子メールの送信をするときは、電子メールアドレスとして利用することが可能な符号を作成する機能を有するプログラム（電子計算機に対する指令であって一の結果を得ることができるように組み合わされたものをいい、総務省令で定める方法により当該符号を作成するものに限る。）を用いて作成した架空電子メールアドレス（符号であってこれを電子メールアドレスとして利用する者がないものをいう。第十条及び第十六条第一項において同じ。）をその受信をする者の電子メールアドレスとしてはならない。

架空アドレスあての送信に利用される自動アドレス生成ソフトについて

【特徴】

- **インターネット等で販売されており、比較的容易に入手可能。**
- **ランダムな英数字のほか、メールアドレスに使われることが多い単語も組み合わせて、文字数の多いアドレスも作成可能。**
- **ＰＣの処理能力向上により、短時間に膨大な量のアドレスを作成することが可能。**
- **テストメールの送信などにより、生成したアドレスの中から実在するアドレスだけを自動的に抽出することが可能。**

広告、宣伝目的以外の架空アドレスあてメール送信の例

現在、架空アドレスあてにメール送信を行う場合として、自己又は他人の広告又は宣伝を目的とする場合を規定しているが、それ以外に、以下のような場合に架空アドレス宛のメール送信を行うことが想定される。

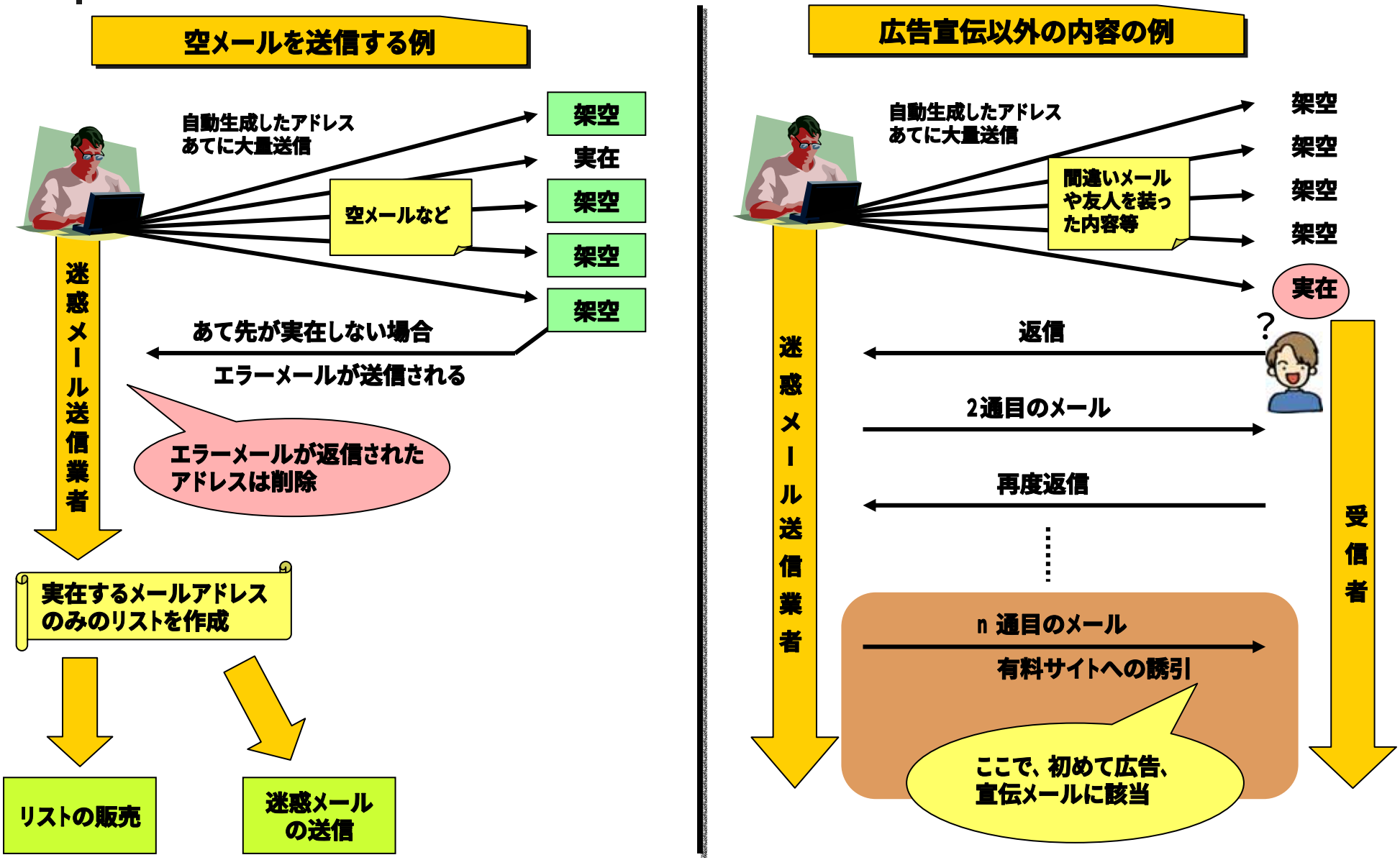
・自動アドレス生成ソフトを使用する際に、ランダムに作成したアドレスリストの中から実在するアドレスを抽出するためにテストメールとしてメールの送信を行い、エラーメール等が帰ってきたものを削除する作業を行う場合。この場合、実際に広告宣伝を内容とするメールを送信する時点では実在するアドレスにのみ送信されていることになる。

・そのメールそのものは広告宣伝目的のメールではないが、受信者からの返信に対して自動的に応答を続けて行き、その課程で営利目的のサイトへの誘引する内容を送信することを目的とするメールを無差別に送信する場合。この場合、架空アドレスあてに送信しているメールは広告宣伝目的と言い難く、（反応があった）実在するアドレスに対してのみ広告宣伝メールを送信していることになる。

これらの例は、次ページのイメージ図のように、いずれも現在の特定電子メール法第５条の適用対象外であると考えられるが、いずれの場合も、架空のアドレスあてに送信する際に電気通信事業者の設備に本来不要な過度の負荷を与えることとなるため、法第５条の対象範囲にこれらの送信行為が含まれるように措置する必要があるのではないか。

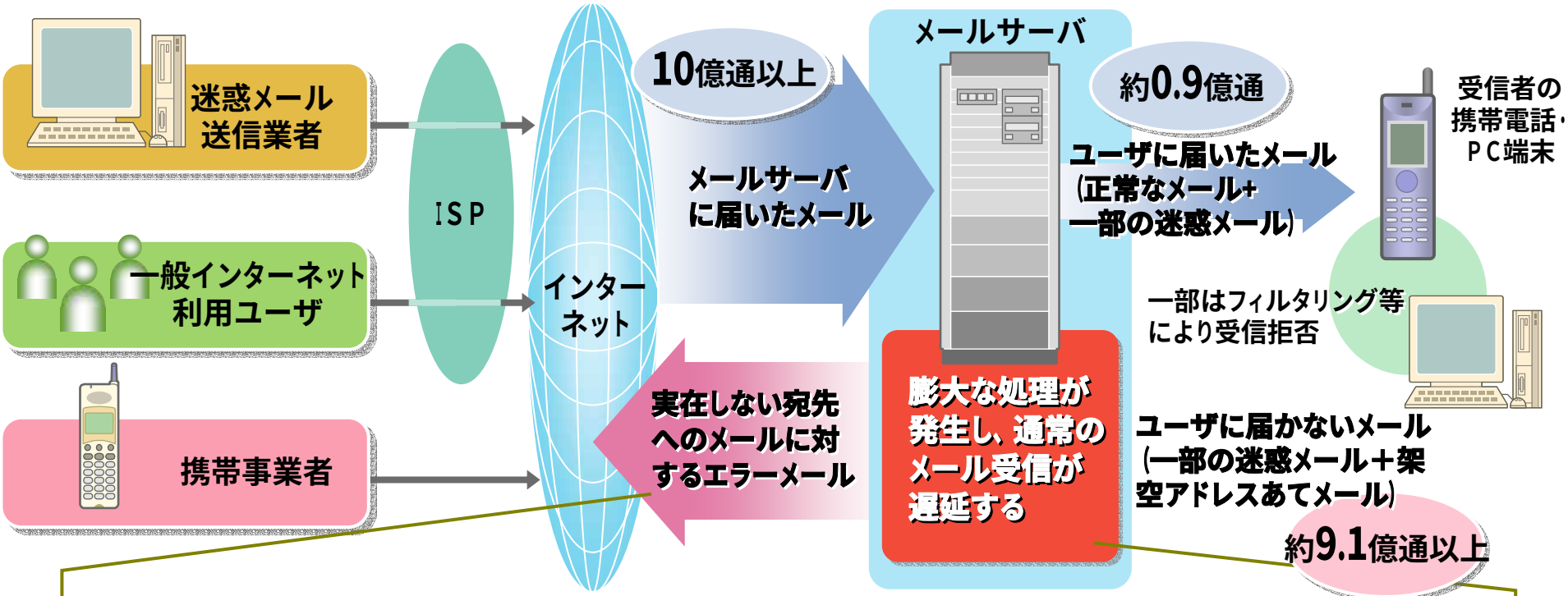
具体的には、法第5条において架空アドレスを宛先としたメールそのものが広告宣伝目的で送信されたものであることという要件を外すことが考えられる。

広告、宣伝目的以外の架空アドレスあてメール送信のイメージ



架空アドレスあてに大量にメールを送信することによる電気通信事業者の設備に対する過剰な負荷について（再掲）

PCから行われる携帯電話やPC端末への架空アドレスあての大量送信が集中した場合、たとえば1日にユーザに届くメールが約1億通程度であるのに対し、ユーザに届かないメールがその10倍もの規模に達する場合もある。



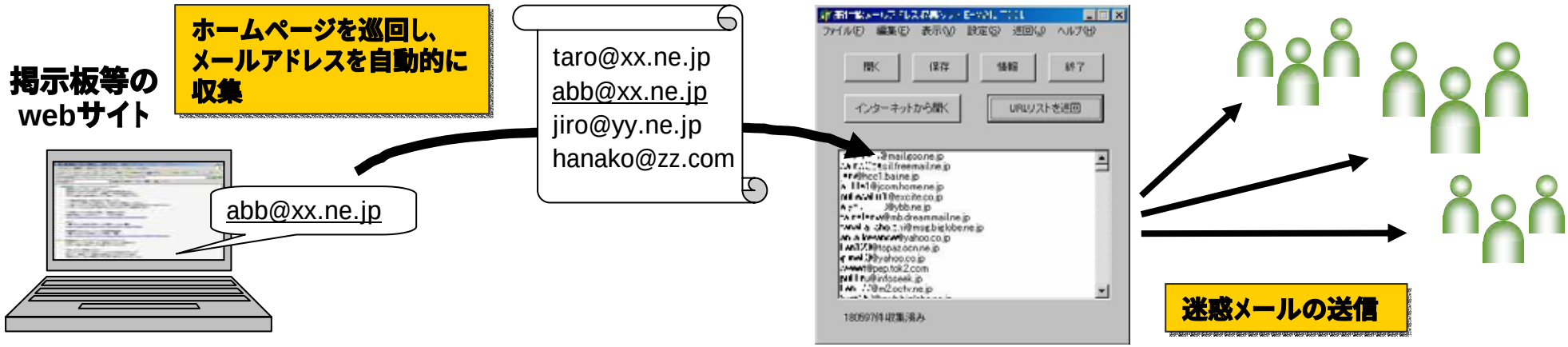
②宛先が実在しないメール等に対してエラーメールを返す場合には、さらに膨大な処理が行われる。
また、送信者の情報を偽ることによりこのエラーメールを利用して無関係な第三者にエラーメールとして迷惑メールを送りつける手法もみられる。

①宛先が実在しない大多数のメールについても処理を行う必要があるため、設備に過大な負荷が生じることになる。
このため、一般ユーザが送信したメールの処理についても遅延してしまう。

本来処理する必要のない大量の架空アドレスあてのメールを処理するために、電気通信事業者においていわば過剰な設備を保有・運用する必要が生じており、業務上も経費上も大きな負担となっている。

自動アドレス収集ソフトについて

ｗｅｂ上に掲載されているメールアドレスを自動的に収集することにより、使用されているメールアドレスのリストを作成可能。



【特徴】

- インターネット等で入手可能。
- １時間あたり、数万件以上収集可能なものも存在。
- アドレスの重複は自動的に削除。
- インターネット上の掲示板のＵＲＬリストも販売しており、巡回対象を絞って高い効率で収集可能。

自動アドレス収集による送信行為の扱いについて

自動アドレス収集による送信

・web上に掲載されているメールアドレス（と思われる）文字列を検索・収集してメールの送信先に設定して送信する行為。
・web上にメールアドレスを公開している利用者に多くの迷惑メールが送信される傾向があると言われることから、迷惑メールの送信手法として広く行われているものと考えられる。

制度上取り締まることとする場合の問題点

web上からの特定の文字列の検索・収集行為そのものは、公開されている情報の検索等を行っているにすぎないため、それ自体を特に禁止すべきということはできない。

問題となりうるのは、少なくとも、メールアドレスを掲載している側がそのアドレスあてにメールを送られることを望んでいない場合（発言者のメールアドレスを掲載する方針で運営されている掲示板等に書き込みを行うことにより、明示的にメールの送信を望んでいるわけではないがアドレスが公開される場合など）に限定されると考えられる。

この問題は、メールアドレスに限らず、web上に掲載されている個人の情報について、その扱いを適正にすべきという問題であり、広告宣伝メールの送信とメールアドレスとの関係についてのみ制度上禁止する等の扱いをすることは適当ではないのではないか。

なお、架空アドレスあての送信と異なり、以下のような事情があることも勘案すべきと思われる。
①通常は実在するアドレスあてにメールを送信することとなるため、電気通信事業者が必ずしも不要なメールの処理を強いられるわけではないこと
②広告宣伝メールの送信については、適正な表示義務を定めるとともに受信拒否の意思表示があった以降の送信を禁止することとしており、送信自体を違法な行為と位置づけているわけではないこと

1　政府による効果的な法執行③（再掲）

悪質な違反行為の直罰化

- 現在、特定電子メール法に違反する行為を行った場合には総務大臣の措置命令がまず行われることとなっており、その命令に反してさらに違反行為を行った者に対してはじめて刑事罰を科すものとしているが、迷惑メール送信行為の巧妙化・悪質化や、それに伴う送信者の特定の困難さから、措置命令の発出そのものが困難である。
- 現行制度に違反するような行為など、迷惑メールの送信に関して特に違法性の高い行為であると考えられるものについて、総務大臣の措置命令を経ずに直接刑事罰を科すことができるよう措置することが考えられる。

（第3条～第6条、罰則規定関係）

論点

- 直接刑事罰の対象となる禁止行為として、禁止範囲の限定性・明確性が要求されるため、現行規定における禁止対象行為の書きぶりに比較して特に悪質な行為に限定する必要があるが、具体的にはどのような行為が想定されるか。
- 刑事罰をもって取り締まるべき高度の違法性や被害の深刻性がどの程度あるか。
- 偽計業務妨害罪（刑法第２３３条）や電子計算機損壊等業務妨害罪（刑法第２３４条の２）等、既存の刑事罰の対象行為との合理的な整理が可能か。

特定電子メールの送信に係る違法行為と直罰化について

現在の禁止行為

表示義務違反（第３条）

「未承諾広告※」等の表示

拒否者への再送信（第４条）

受信拒否の意思表示をした者への再度の送信

架空アドレスへの送信（第５条）

実在しない架空のアドレスを自動生成して送信

上記の各条の違反者のうち特に悪質な者

送信者情報を意図的に改竄する等の悪質な送信行為

受信者に送信者の情報を得させないようにすることを目的として特殊な送信手法により送信

直罰化の考え方

- 本来は、法にしたがった表示内容等により特定電子メールを送信し、また受信拒否の通知をきちんと取り扱うといった送信者による適正な電子メールの送信が行われるように促すことが目的。
- そのため、一般的には、過失による表示内容の欠如や受信拒否の意思表示に対し誠実な対応をとらないことについて、総務大臣の措置命令により改善を図ることが適当と考えられる。

→ 現在の禁止行為を一律に直罰化するのは厳しくなりすぎて不適当ではないか。

- 通常の電子メール送信の際には行われることが全く想定されないような、特に悪質な送信行為を意図的に行っているものであると考えられる。
- 架空アドレスへの送信や送信者情報の改竄といった行為には適正な方法といった概念は通常想定できず、過失により実行してしまうということも考えにくいことから、総務大臣の措置命令を前置せずに刑事罰を科すべき事例も多いのではないか。

→ 直接刑事罰を科すことができるように措置することが必要ではないか。

警察による捜査と総務省による行政処分の比較

警察による捜査の場合

【被害者】

迷惑メールの受信

告訴

【警察】

違法性の確認

令状の取得により迷惑メール送信時の通信履歴をたどっていくことが可能

ＩＳＰ等のメールサーバ

迷惑メール送信者を摘発

総務省による行政処分の場合

違法メールの受信者から迷惑メール相談センターへ情報提供

違法性の確認

法違反者に対して警告メールを送信

報告徴収の実施

立入検査の実施

措置命令の発出

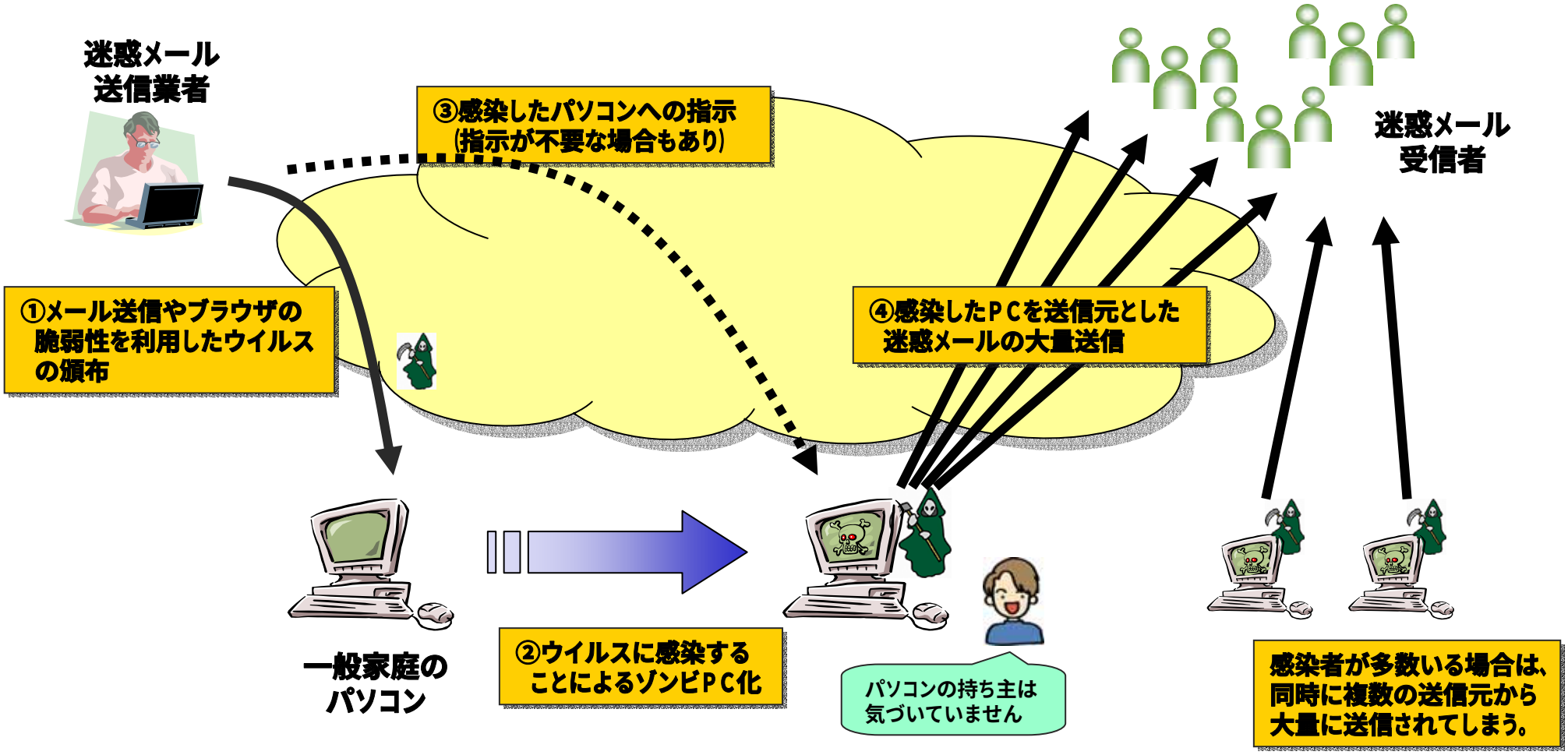
措置命令に違反した場合、罰金刑となる

迷惑メール等に記載された情報から送信者が特定できる場合に限り可能

迷惑メールに記載された情報から送信者が特定できない場合は、処分が困難

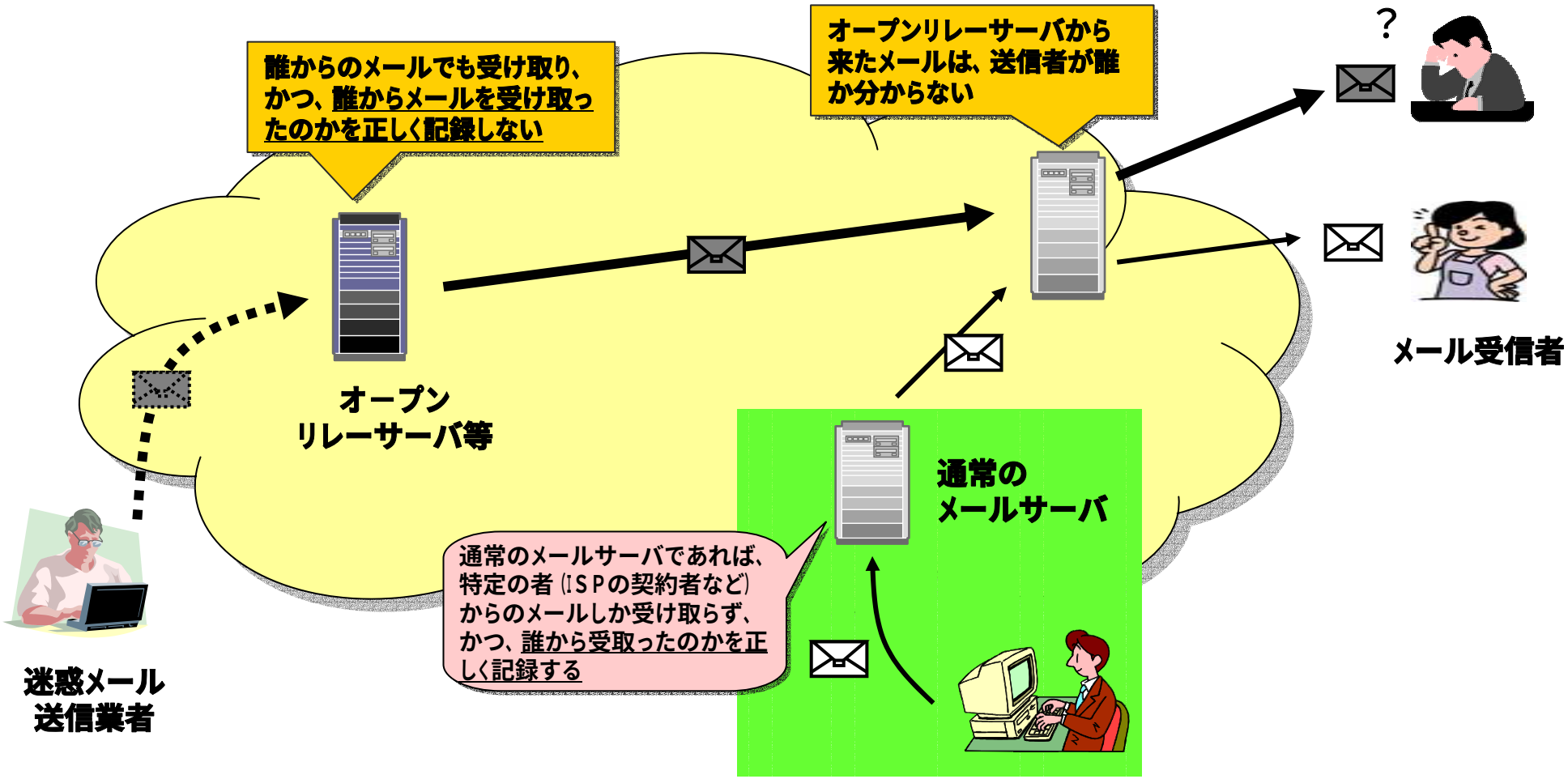
いわゆるスパムゾンビ（ゾンビＰＣ）による送信（再掲）

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



オープンリレーサーバの利用等不正中継による送信（再掲）

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



諸外国における送信者情報を意図的に改竄するための悪質な送信行為に関する禁止規定

行為類型	米国	英国	豪国	韓国
①送信者が、ヘッダー情報等を改竄して送信する行為 **〔送信者情報を意図的に改竄する行為〕**	・電子メールのヘッダー情報を偽って又は虚偽の電子メールアドレス、ドメイン名を用いて実質的に誤解させるようにして送信すること	・送信者の身元を偽装または隠蔽して電子メールを送信（送信の教唆）すること	なし	・送信者が受信拒否を回避するための技術的操作を行うこと
②送信者が、特殊な送信経路をとって送信する行為 **〔オープンリレーサーバ等を利用した不正な中継〕**	・電子メールを意図的に他のコンピュータを経由させて、送信に使用したコンピュータが正確に識別できないようにして送信すること	なし		
③他者のコンピュータを不正に使用して送信する行為 **〔いわゆるスパムゾンビ(ゾンビＰＣ)等による送信〕**	・他のコンピュータに不正アクセスし、そのコンピュータを送信元として送信すること、又はそのコンピュータ自身が送信元となっていなくてもそのコンピュータを使用して電子メールを送信すること			なし
④送信者以外の第三者が送信の中継や再送信をする行為	・実際の送信の開始元である送信者について受信者又はインターネット接続サービス事業者を欺いたり誤解させたりするために、電子メールを中継又は再送信すること			

注）上記のような行為類型について、個別に禁止規定をおいていると考えられるものを示したため、実際に上記行為を行った場合に当該国において違法とされる場合を網羅しているものではない。
（英国については送信者情報の改竄のみを、韓国については送信者情報の改竄及び不正な中継を対象としているとして取り扱った。）

刑法等の他の法律により禁止されている行為の例

刑法第２３３条（偽計業務妨害）

・偽計を用いて、他人の業務を妨害する行為に対し、３年以下の懲役又は５０万円以下の罰金。

・迷惑メールの送信については、電気通信事業者の役務提供に障害が発生することを認識した上で、大量の電子メールの送信を行うこと等によりその業務を妨害したような場合などに、この規定の適用可能性がある。

刑法第２３４条の２（電子計算機損壊等業務妨害）

・業務用コンピュータまたはその記録を損壊したり、コンピュータに虚偽の情報・指令を与えること等により使用目的に沿わない動作等をさせて業務を妨害する行為に対し、５年以下の懲役又は１００万円以下の罰金。

・迷惑メールの送信については、電気通信事業者の役務提供に障害が発生することを認識した上で、メール送信に際しての何らかの技術的操作によりメールサーバに本来の目的以外の動作等をさせて、その業務を妨害したような場合などに、この規定の適用可能性がある。

不正アクセス禁止法第３条（不正アクセス行為の禁止）

・ＩＤやパスワードによって利用権限を識別するアクセス制御機能を有するコンピュータに対し、ネットワークを介して他人のＩＤやパスワードを入力したりセキュリティホールを突く情報等を入力したりして利用する行為に対し、１年以下の懲役又は５０万円以下の罰金。

・迷惑メールの送信については、アクセス制御をしている他人のコンピュータを上記のような手段により不正に利用して送信を行う場合などに、この規定の適用可能性がある。

（参考）その他の禁止規定

広告宣伝メールの送信以外の広義の迷惑なメールの送信にあたり関連すると思われる規定としては、昭和６２年にコンピュータ犯罪への対応のための刑法改正により新設された以下の処罰規定があるが、電子メールの送信行為そのものについて適用されることはあまり想定されない。

刑法第234条の2については、前ページで既述。

刑法第１６１条の２（電磁的記録不正作出及び供用）

・人の事務処理を誤らせる目的で、その事務処理に用いる権利、義務、事実証明に関する電磁的記録を不正に作成する行為に対し、５年以下の懲役又は５０万円以下の罰金（使用する行為も同様）。

刑法第２４６条の２（電子計算機使用詐欺）

・人のコンピュータに虚偽の情報・不正な指令を与えて財産に関する虚偽の記録を作成したり、虚偽の記録を処理させたりすることにより不法に利益を得ること等の行為に対し、１０年以下の懲役。

なお、電気通信事業法においては、直接電気通信事業者の電気通信役務の提供を妨害する行為について罰則規定が置かれているが、電子メールの送信は電気通信役務の利用行為であり、この規定に抵触することはあまり想定されない。

電気通信事業法第１８０条第１項

・みだりに事業用電気通信設備を操作して電気通信役務の提供を妨害する行為に対し、２年以下の懲役又は５０万円以下の罰金。

犯罪の国際化及び組織化並びに情報処理の高度化に対処するための刑法等の一部を改正する法律案について

２００１年１１月に欧州評議会（Council of Europe）で採択された「サイバー犯罪条約」の国内法制化を目的として刑法及び関連する法律を改正するために、先の通常国会（第１５９回国会）に提出されたものであり、現在衆議院法務委員会で審査中となっている。
今後、成立した際には、公布の日から２０日以内に施行されることとなっている。

不正指令電磁的記録作成等の罪（刑法第１６８条の２の追加）

・コンピュータ・ウイルスの作成、供用等の罪を新設している。
・迷惑メールの送信の方法として、他人のコンピュータにウイルスを感染させて電子メールを勝手に送信する行為（いわゆるゾンビＰＣを作り上げる行為をウイルスの頒布によって行う場合）については、同法により刑法に追加される「不正指令電磁的記録作成罪」等の構成要件である「人が電子計算機を使用するに際してその意図に沿うべき動作をさせず、又はその意図に反する動作をさせるべき不正な指令を与える電磁的記録の作成、提供又は実行」に該当し、刑事罰の対象となるものと考えられる。

第１６８条の２　人の電子計算機における実行の用に供する目的で、次に掲げる電磁的記録その他の記録を作成し、又は提供した者は、３年以下の懲役又は５０万円以下の罰金に処する。
一　人が電子計算機を使用するに際してその意図に沿うべき動作をさせず、又はその意図に反する動作をさせるべき不正な指令を与える電磁的記録
二　前号に掲げるもののほか、同号の不正な指令を記述した電磁的記録その他の記録
２　前項第一号に掲げる電磁的記録を人の計算機における実行の用に供した者も、同項と同様とする。
３　前項の罪の未遂は、罰する。

米国司法省によるスパムの取締強化
～スパム制圧作戦（Operation Slam Spam）について～

米国司法省発表資料、新聞報道等により作成

背　景

・司法省による過去最大規模の合同法執行作戦であるサイバー犯罪一掃作戦（Operation Web Snare）中のスパムに特化したプロジェクトである。

・スパム問題は、軽犯罪の積み重ねで、犠牲者が明確でない場合も多く、従来、取り締まりは困難であったが、CAN-SPAM法制定後もスパムの量が増え続け、また、スパムが別の犯罪（個人情報盗用やクレジットカード詐欺）へつながる事例も増えたため、取り締まりを強化することとなった。

・サイバー犯罪一掃作戦は、ネット詐欺の告発や、関連犯罪防止を行うもので、今年6月1日から現在までで、約160の事件の捜査を行っている。米国連邦捜査局（FBI）、ネット犯罪苦情処理センター（Internet Crime Complaint Center）、ソフトウェア企業、マーケティング企業、州政府等の協力体制で行われている。

体　制

・司法当局と産業界の初めての官民合同プロジェクトである。執行面ではFTC（米国連邦取引委員会）が協力し、資金面ではダイレクトマーケティング協会（Direct Marketing Association）が全面的に協力している。

内　容

・スパマーの送信手法の分析と犯罪手法の調査の2チームに分かれて行われており、事案の発見とその調査のほか、調査手法の開発や、捜査官・分析官の訓練も行われている。

・司法当局の収集した情報と、スパマーを調査し訴訟を行っている私企業の情報を元に、名前が判明したスパマーのデータベースを構築して分析に役立てている。

・サイバー犯罪一掃作戦の捜査には、このプロジェクトで進められた調査結果が活用されている。

海外における取り締まり状況
（米国連邦政府によるＣＡＮ-ＳＰＡＭ法に基づく違法業者の摘発事例等）

米国の状況①：ＦＴＣによる摘発

・2004年4月29日、FTCは大量の偽のダイエットパッチを売り込む詐欺メールを送信していたスパム業者2社の摘発を発表。
・Phoenix Avatar社に対してはFTCの要請で米連邦地裁判事が違法スパムの送信停止を命じ、資産の凍結・責任者の逮捕を行った。
・オーストラリア及びニュージーランドを拠点とするGlobal Web Promotions社に対しても、以後の違法なメール送信及び製品の出荷を差し止める仮処分の申請を行った。この摘発には、オーストラリア及びニュージーランドの政府当局の協力があった。
・2業者に共通する送信手法として、ヘッダー情報の送信元メールアドレス等（reply-to:及びfrom:）を無関係な第３者になりすまして送信しており、その第三者に配信不能メールが大量に届き正常な利用ができなくなったとしている。

米国の状況②：ＦＢＩのサイバー犯罪一掃作戦による摘発

・2004年8月9日、無防備な無線LANのアクセスポイントを求めて、郊外を車で探し回る、いわゆる「ウォー・ドライビング」を行ない、車上のパソコンから不正アクセスを行い、ポルノサイトを宣伝する商業電子メールを大量に送信したとして、NicholasTombrosを逮捕した。同容疑者は、9月28日に容疑を認めた。
・サイバー犯罪一掃作戦の一環としてロサンゼルスにおいてＦＢＩが捜査を進めていたもの。
・ＦＢＩによると、12月6日に同容疑者に対し、3年以下の懲役刑判決が言い渡される予定。
・判決が下されれば、CAN-SPAM法の元で有罪判決が下される初のケースとなる。

そのほか、韓国においても規制法施行直後に集中的に取り締まりを行い、受信拒否の連絡方法を提供しなかった事業者や発信元アドレスを隠蔽して送信した事業者を摘発している。

1　政府による効果的な法執行④（再掲）

オプトイン方式の採用

- 欧州指令においてオプトイン方式を採用した結果、英国をはじめとする欧州諸国においてはオプトイン方式が採用されている。また、オーストラリアにおいてもオプトイン方式が採用されている。
- 米国では基本的にオプトアウト方式を採用しているが、本年8月に公表されたＦＣＣルールにおいては、携帯電話あてに送信される商業広告メールに関してオプトイン方式が採用されている。
- 我が国においても、制度の枠組みを変更してオプトイン方式を採用することが考えられる。

論点

- オプトイン方式を採用する場合、オプトアウト方式を採用している現行制度の全面的な変更を意味することとなるが、オプトイン方式が取り締まりの枠組みとして明確に優れているという論拠があるか。
- オプトイン方式においては、受信者の同意の有無がもっぱら合法・違法のメルクマールとなるが、現在でも見られるように送信者が受信者の同意を得ていると主張している場合には結局違法性の認定が困難なのではないか。

オプトアウト方式：メールの送信者に受信拒否の意思を伝えた場合、以後の送信を認めない方式
オプトイン方式　：あらかじめメールの受信を承諾している者に対してのみ送信を認める方式

オプトイン方式の効果について

・オプトイン方式を採用している国としては、イギリス・オーストラリアがあり、原則としてオプトアウト方式であるが一部オプトイン方式を採用している国としては、アメリカ・韓国がある。
※アメリカについては、携帯端末あての電子メールについてのみオプトイン方式（ＦＣＣが担当）、韓国については法律上はオプトアウト方式であるが携帯電話事業者の約款上でオプトイン方式を採用している（法制化については今後検討）。

・諸外国においては、迷惑メール規制に係る法制度が施行されてからまだ日が浅く、制度導入による効果についても公式に発表されているものはなく、民間のセキュリティサービス提供会社等による調査結果がいくつか発表されている程度である。

・そのため、現時点では取り締まりの制度的枠組みとして、オプトアウト方式とオプトイン方式のいずれが有効かについては明確な結論がない状況。

継続的にオプトイン方式採用国での効果を注視するとともに、当面は現行のオプトアウト方式による取り締まりを着実に行うこととするのが適当ではないか。

（参考）米国ＦＴＣによる英国のオプトイン方式の効果についての言及
※ＰＣあて電子メールについての執行機関

・英国は、欧州共同体データ保護指令に準拠して2003年12月にオプトイン方式を導入した。国際電子メールフィルタリング会社であるブライトメール社（現シマンテック社）の提供する統計によると、このオプトイン方式は、スパムの量に対して効果があったとは言えない……ブライトメール社によると、2003年12月にオプトインが導入された際、54.9%がスパムだったが、2004年4月には受信メールの60.1%がスパムだった。このデータから、オプトイン方式は英国民が受け取ったスパムの量を減少させたと言うことはできない。
（2004年6月15日付けの「Do-Not-Email登録簿に関する報告書」（第１回資料３ｐ35参照）より）

オプトイン方式を採用している国における規制の内容について

・受信者からの事前の同意がない場合の商業電子メールの送信を禁止。
・同意の取得方法、同意の判断基準について具体的な定めが置かれているが、各国で多少のばらつきがある。
・送信の際には、受信拒否の方法を示さなければならない。受信拒否の意思表示を受けたら送信してはならない。

アメリカ（携帯電話あて）

同意の取得　・口頭による同意の取得、又は書面（電子的な方法を含む）による取得。署名（電子署名含む）が必要。ウェブサイトで同意を得る場合は、受信者が受信を容認するメールアドレスを入力させなければならない。
表示義務　・受信拒否の方法（無料かつ30日間は有効である必要あり）
・受信者が送信者と連絡を取るために必要な情報（同意をした送信者であることを特定するための情報）

イギリス

同意の取得　・受信者の明示的な同意を得た場合
・商品購入やサービス契約の交渉の過程で、受信者の電子メールアドレスを取得した場合
表示義務　・受信拒否の方法（通信費以外は無料で提供）
・受信者が送信者と連絡を取るために必要な情報

オーストラリア

同意の取得　・受信者の明示的な同意（送信行為、送信内容に問題がないという直接的意思表示）をえた場合
・商品購入やサービスの契約時にメールアドレスを取得した等、その後の情報提供を期待していると合理的に判断できる場合
・業務に関連する電子メールアドレスを公開し、業務関連の広告メールの受信を明確に拒否していない場合
表示義務　・受信拒否の方法（電子メールやウェブへのリンク等）
・受信者が送信者と連絡を取るために必要な情報

韓国（携帯電話あて）

・受信者の事前の同意なく広告を送信した場合には、通信事業者が送信者の携帯端末のサービスを停止することで対応。
・具体的な同意の取得や、同意を得た後の送信の際の表示義務に関しての詳細は不明。

2　電気通信事業者による自主規制①（再掲）

役務の提供を拒否できる範囲の見直し

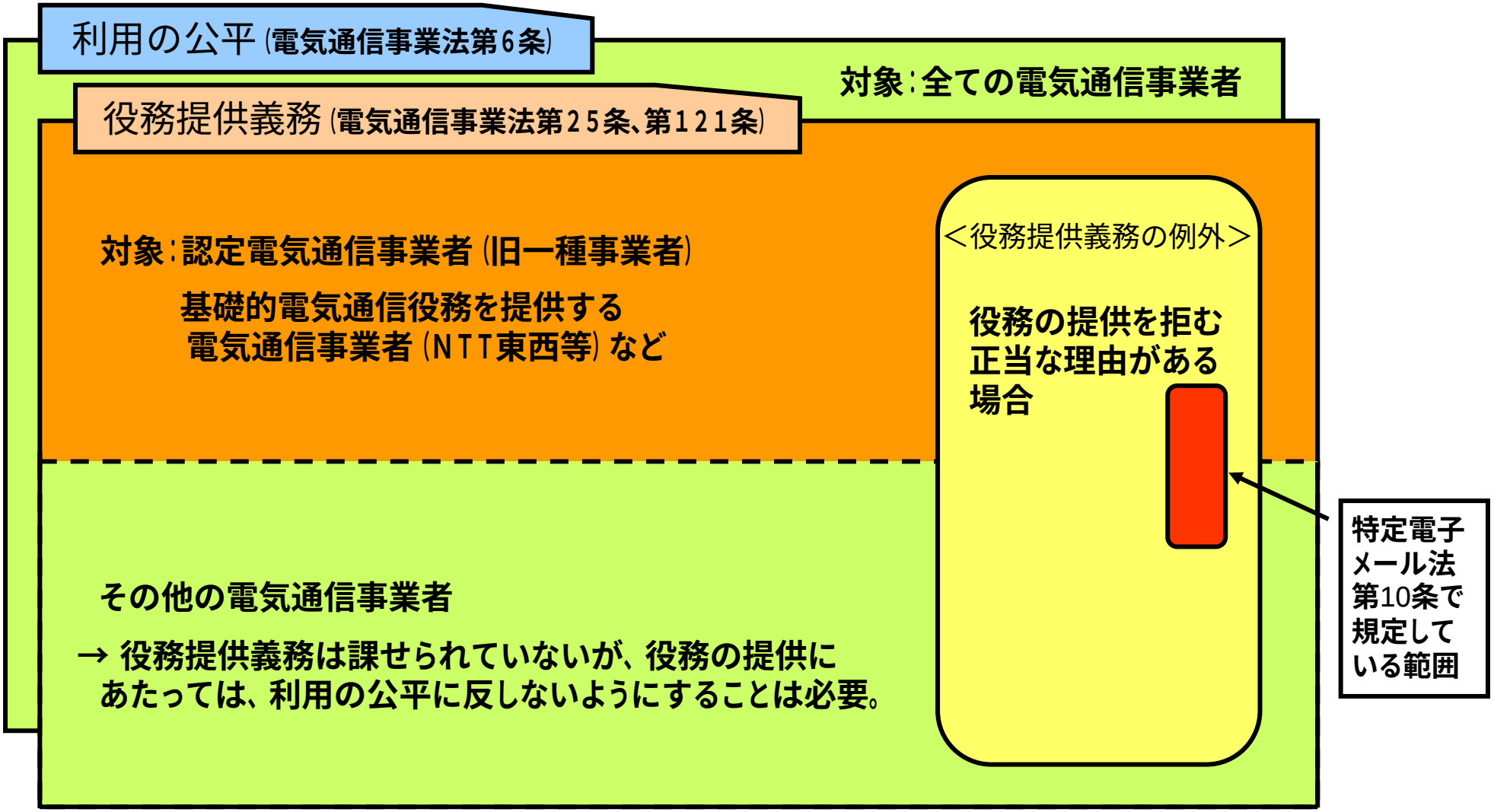
- 現在、電気通信事業者が迷惑メールの送信について役務提供拒否することの正当性を規定しているのは、①電気通信設備に著しい障害を生じ、電気通信役務の提供に著しい支障を生ずるおそれがある場合について、②架空アドレスあてに送信した電子メールについての役務提供を拒否する場合、に限定されている。
- 迷惑メールが送信されることで電気通信事業者の設備に過大な負担がかかること等により役務提供拒否が正当化される事由は、必ずしも上記に限定されないと考えられることから、対象範囲を見直すことが考えられる。（法第１０条関係）

論点

- もともと電気通信事業法における役務提供義務の例外となる正当な拒否事由の一例として規定しているという性格のものであることから、明らかに役務提供を拒否することに正当性があると考えられる場合のみが対象となり、むやみに範囲を拡大することは不適当ではないか。
- 上記のほか、役務の提供を拒否した場合に拒否された送信者との間における紛争を防止するために、プロバイダ責任制限法のように電気通信事業者の損害賠償責任を限定するような措置は考えられないか。

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

特定電子メール法第10条と役務提供義務及び利用の公平の関係



特定電子メール法第10条に規定されている電気通信役務の提供の拒否ができる場合について

	法律上の要件	具体的な態様
①送信されている電子メール	一時に多数の架空電子メールアドレスをその受信をする者の電子メールアドレスとして電子メールの送信がなされた場合	・多数の電子メールが送信されており、その宛先が架空電子メールアドレスとなっている場合 ・メールの通数に関わらず、宛先欄に多数の架空電子メールアドレスが記載されている場合
②電気通信事業者への影響の程度	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	・電気通信事業者のメールサーバに過大な負荷がかかり、稼働不能となった場合（メールサービスが停止した場合等） ・機能停止には至らずとも、その処理速度が著しく低下している場合（メールの配信が大幅に遅延して受信者に届く場合等）
③役務提供を拒否する相手方	当該架空電子メールアドレスに係る電子メールの送信をした者	①の電子メールを送信した者
④役務提供を拒否する電気通信役務	その送信をした電子メールについて	①の電子メール

役務提供義務の例外を法律で規定していることから非常に限定的な書きぶりとなっており、たとえば以下のような場合であっても厳密にはこの規定には該当しないこととなる。

・送信者が広告宣伝メール以外の通常のメールを送信している場合や、広告宣伝メールのうち架空アドレスを含まない状態で送信されているメールが存在する場合など。
・送信されているメールの総量がそれほど多くなく、架空アドレスあてに送信しているがメールサーバが支障なく処理できる場合

には、本条を根拠として役務提供を拒否することはできず、一般原則に戻ることになる。
すなわち、電気通信事業法の役務提供義務の例外となる正当な理由があるか否かを個別に判断してその可否を判定することになる。

電気通信役務の提供を拒否することが正当と考えられる他の場合について

現在の法第１０条で規定されている場合以外であって、電気通信事業者が電気通信役務の提供を拒否することの妥当性が高いと考えられるものとしては、以下のようなものが挙げられる。

架空アドレスあての送信や大量送信を行っている者が送信している電子メール全体

- 架空アドレスあての送信や、実在するアドレスあての送信であっても極めて大量の電子メールを送信している者からの送信については、そもそもその送信者から送信される電子メールを処理することについて過度の負荷を電気通信事業者の設備に与えることになると考えられる。
- 個々のメールの内容等にかかわらず、同一の送信者からのメール送信について拒否することが正当と考えられる条件としてはどのようなものがあるか。

架空アドレスあてに送信されてはいるが、メールサーバが支障なく処理することができる場合

- 架空アドレスあての送信を多数行ってはいるが、電気通信事業者のメールサーバの処理能力に比べて支障を生じさせるほどの通数ではない場合が考えられる。
- 架空アドレスあての電子メールについては受信者へ届けることができないため、配信不能の処理を行うこととなり、無駄な処理を強いられることにはなるが、その処理を行うことに特段の支障がない場合についての妥当性はどのように判断されるか。

直罰化の検討に値するような特に悪質な送信行為を行っている者の送信する電子メール

- 送信者の情報を意図的に改竄するような特に悪質な送信行為を行っている場合などに直接刑事罰を科すこととする場合に、そのような行為を行う者の送信する送信者情報を改竄した電子メールについて役務提供を拒否する場合などが考えられる。

法律に規定する場合には、まぎれの生じない厳格な範囲に限定せざるを得ないことを踏まえつつ、上記のような事例を含め、個別具体的な事例について整理することが妥当ではないか。