PRINT ISSN 2434-5016
ONLINE ISSN 2434-4982

迷惑メール白書
2019

迷惑メール対策推進協議会
Anti-Spam mail Promotion Council

第１章

２０１８年度の迷惑メールに関する状況

第1節　迷惑メールに関する概況

2018 年度の迷惑メールに関する概況としては、日本国内のインターネットサービスプロバイダ（Internet Service Provider:ISP）が扱う迷惑メールは、2017 年度の減少傾向とは異なり増加傾向にあります。具体的には、国内の ISP が取り扱う国内着の電子メールのうち、迷惑メールの占める割合は 2019 年 3 月時点で約 44%となっており、2017 年度の同時期と比較すると約 7%の増加となっています。また、国内着の迷惑メールの発信元（国）としては、2017 年度は日本、米国、中国がその上位 3 カ国でしたが、2018 年度は中国にかわりブラジルが第 3 位となり、2019 年 3 月の割合は、それぞれ約 36%、約 9%、約 7%となっています。

迷惑メールの内容については、近年と同様に、出会い系および副業や情報商材などを扱ったビジネス系の広告宣伝メールが大半を占める傾向が続いています。具体的には、出会い系サイトへ誘導するメールは、66%となっており、2009 年の調査開始以降初めて 7 割を下回った 2017 年の約 66%と比較して大きな変化はない状況です。また、副業紹介や情報商材などに関するメールは約 15%であり、こちらも昨年と比較して大きな変化はない状況です。その他には、B-CAS カードに関するメールが約 6%、ギャンブルに関するメールが約 4%となっています。

2018 年度に注目された迷惑メールの手口としては、ビジネスメール詐欺（Business E-mail Compromise: BEC）が昨年度から引き続き世界で横行しており、日本においても最高経営責任者（CEO）の名義やメールアドレスを詐称し、日本語によって送金を促すものが初めて確認されたほか、企業や官公庁などの IT や経理などの責任者の約 4 割が詐欺メールを受信した経験があることが分かりました。また、大手宅配事業者を装い SMS をスマートフォンに送りつけ、連絡先など個人情報を抜き取られる被害が多発したほか、「アダルトサイトを閲覧している姿を録画した」とする偽メールを送り、仮想通貨を騙し取られる被害も相次ぎました。

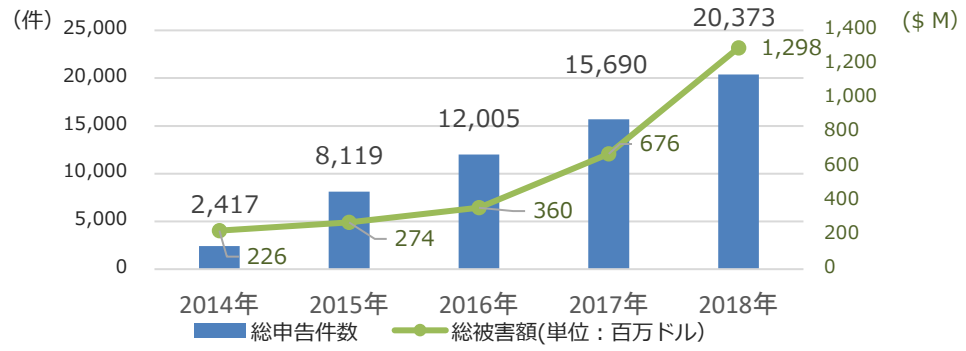
このような迷惑メールに対して、携帯電話事業者やサービスプロバイダーなど様々な関係者が、2018 年度も引き続き迷惑メール対策に取り組んでいます。また、(一財)日本データ通信協会など関係団体による、利用者の意識向上に向けた周知広報も積極的に行われています。

第2節　悪質化･巧妙化する迷惑メールの動向

1　企業等の金銭や情報を狙ったビジネスメール詐欺（BEC）等

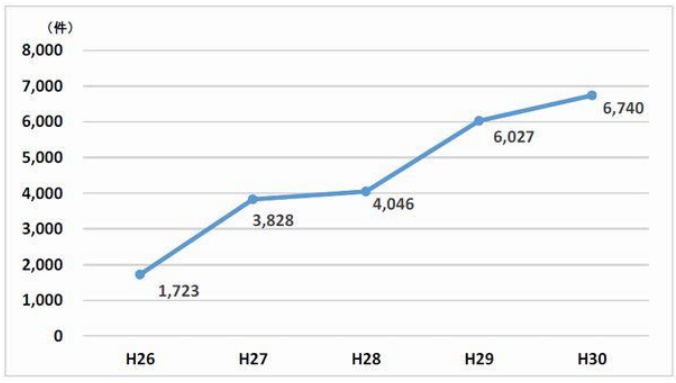
2018 年も引き続き、取引先や経営層などを装い、偽の電子メールを送り金銭を詐取するビジネスメール詐欺（BEC）が多数確認されています。米国の FBI によると、2018 年の BEC による被害額は 12.9 億ドルと、前年比 1.9 倍にまで増加しました。日本においては、（独）情報処理推進機構（IPA）が昨年 7 月に企業からの情報提供により、最高経営責任者（CEO）の名義やメールアドレスを詐称し、日本語によって送金を促す詐欺メールを初めて確認したほか、トレンドマイクロ社の調査によると、企業や官公庁などの IT や経理などの責任者 1030 人のうち、39.4%にあたる 406 人が「振込先の口座が変わった」などの詐欺メールを受信した経験があり、そのうち 22 人は実際に指定の口座に送金を行い、1 億円以上送金したケースもありました。また、日本人が関与した BEC も確認され、米国の農業関連会社から不正に送金させたとして実際に逮捕される事案なども発生しています。さらに、企業を標的にした詐欺メールは BEC だけでなく、不正プログラムを添付して、業務に関連した正当なものであるかのように装った電子メールを送信し、情報を詐取する「標的型メール」も横行しています。警察庁の発表によると、「標的型メール」の攻撃の件数は 2018 年に 6,740 件と近年増加傾向にあり、そのうち、同じ文面や不正プログラムが 10 か所以上に送付された「ばらまき型」攻撃が多数発生し、全体の 90%を占めています。

図表１－２－１　米国の BEC による被害額



出典：米国 FBI「Internet Crime Report」をもとに、迷惑メール対策推進協議会事務局が編集

図表１－２－２　標的型メール攻撃の件数の推移



出典：警察庁「平成 30 年におけるサイバー空間をめぐる脅威の情勢について」

BEC に関しては、2018 年 8 月、（独）情報処理推進機構（IPA）より、2017 年 4 月に公表した「ビジネスメール詐欺「BEC」に関係した事例と注意喚起」[注1]の続報として、あらためて BEC への注意喚起を行っています。同続報では、2015 年から 2018 年 7 月にかけて発生した BEC に関する 17 件の企業からの情報提供のうち、新たな手口や特徴が見られた 5 件の事例を詳しく紹介しています。例えば、2018 年 7 月に発生した「国内企業の CEO を詐称する日本語メールの攻撃」では、日本国内の企業の CEO を詐称し、同企業内の担当者に対して国際送金をさせようとする攻撃が行われましたが、その際、先述のとおり、攻撃者は日本語のメールでやりとりを行っており、日本語によるものが初めて確認されました。また、メールアドレスの詐称も非常に巧妙に行われており、攻撃者は正規のドメインに似通った、偽の「詐称用ドメイン」を新規に取得しただけでなく、この詐称用ドメインの DNS 情報には、SPF レコードも存在しており、SPF 検証も「PASS」する状態でした。この事例では実際の被害は生じませんでしたが、メールアドレスの詐称が非常に巧妙に行われていることから、このようなケースにおいては、日頃からメール受信者がメールアドレスに注意して、ドメイン名が異常であることに気づくことが重要です。

なお、IPA は、同続報において BEC への対策として次の対策を引き続き推奨しています。

図表 1 – 2 – 3　IPA による BEC への対策

対策	内容
取引先との電子メール以外の方法での確認	振込先の口座の変更といった、通常とは異なる対応を求められた場合は、送金を実施する前に、電話や FAX など電子メールとは異なる手段で、取引先に事実を確認すること
社内規定の整備	「メール以外の方法での確認」といった手順を含む、電信送金に関する社内規定を整備することも必要
普段とは異なる電子メールに注意	普段とは異なる言い回しや表現の誤りには注意が必要
不審と感じた場合の組織内外での情報共有	不審なメール情報を適切な部門に報告できる体制が重要であり、それら情報の集約により、組織に対する悪意ある行為を認識し、対策に繋げることが可能。また、取引先との連絡・情報共有も重要
ウイルス・不正アクセス対策	「不審な電子メールの添付ファイルは開かない」など、基本的なウイルス対策の実施のほか、「メールアカウントには複雑なパスワードを設定する」など、不正アクセスへの対策も重要
電子署名の付与	取引先との間で請求書などの重要情報を電子メールで送受信する際、電子署名をつけるなど、なりすましを防止する対策も有効
類似ドメインの調査	定期的に組織に類似のドメインが取得されていないか確認し、必要であれば注意喚起を実施

出典：IPA「ビジネスメール詐欺「BEC」に関する事例と注意喚起」をもとに、迷惑メール対策推進協議会事務局が編集

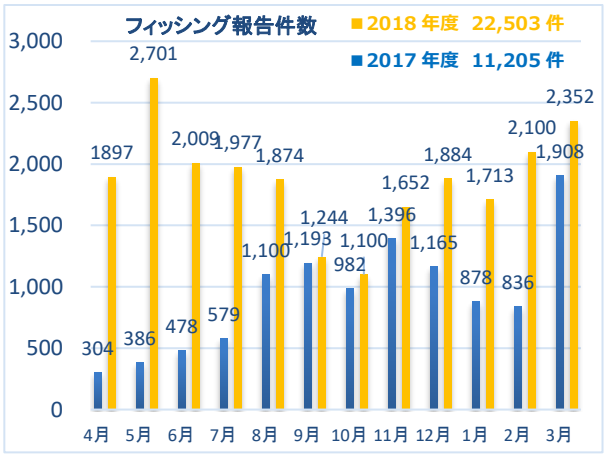
[注1] 2017 年 4 月 3 日 IPA (ビジネスメール詐欺「BEC」に関する事例と注意喚起) https://www.ipa.go.jp/files/000058478.pdf

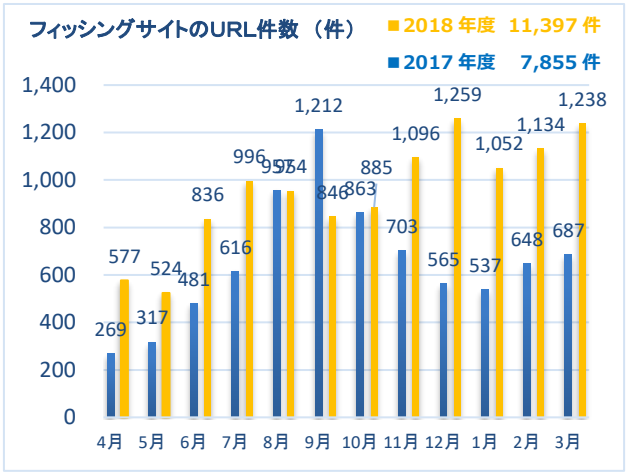
2　個人情報や仮想通貨を狙うフィッシングメール

2018 年に確認された主なフィッシングメールとしては、大手宅配事業者を装った SMS がスマートフォンに送りつけられ、インストールした不正なアプリにより個人情報を詐取された上、そのスマートフォンが、さらに不特定多数の人に同様の偽 SMS を送る送信元として利用される被害が相次ぎました。また、「アダルトサイトを閲覧している姿を録画した」とする偽メールを送りつけて脅し、仮想通貨を詐取する被害も確認されました[注 2]。IPA によると、はじめてこの相談があったのが 2018 年 3 月であり、9 月には 263 件と相談件数が増加しました。さらに、トレンドマイクロ社の調査によると、9 月中に発見されたこの仮想通貨を騙し取る偽メール数は少なくとも 3 万 6 千通に上り、偽メールを信じたとみられる利用者から、攻撃者の仮想通貨口座に通貨が払い込まれている形跡が確認されました。攻撃者は利用者のパソコンを乗っ取ったと思わせることで、偽メールの内容を信じ込ませようと様々な細工を施しており、その一つが、利用者が少なくとも過去に使っていたパスワードを偽メールのタイトルにする手口です。これは本物であった（ある）パスワードなので利用者は動揺するかもしれませんが、すぐ攻撃者の要求に応えるのではなく、まずは公的機関等に相談することが重要です。

2020 年には東京オリンピック・パラリンピックが開催されますが、このような世界的な注目を集めるイベントにおいては、それに関連する官公庁や企業などが攻撃の対象となりやすく、それらになりすました偽メール等が増加する可能性があります。昨年、東京オリンピック・パラリンピックの無料チケットの提供を装った偽メールによる攻撃がネット上で計画されていることが判明しました[注3]。その手口は、無料チケットの提供を装った偽のメールや SMS を不特定多数に送り、本文に記載した不正サイトのアドレスに接続させて情報を盗み取るものとなっており、メールの利用者は一層の注意が必要です。

図表１－２－４　フィッシング情報の報告件数とフィッシングサイトの URL 件数





出典：フィッシング対策協議会「フィッシング報告状況」をもとに、迷惑メール対策推進協議会事務局が編集

注2 フィッシング対策協議会（緊急情報等）、トレンドマイクロ社セキュリティブログ（2018 年 3 月 19 日「仮想通貨を狙うフィッシング詐欺、既に闇市場での「サービス化」も確認」）

注3 読売新聞

第3節　迷惑メール対策の動向（DMARCの普及状況等）

1　DMARC の普及状況

（1）DMARC とは

前節で BEC（ビジネスメール詐欺）やフィッシングメールについてふれましたが、これらのメールは送信者情報を詐称することがほとんどです。これら送信者情報を詐称したなりすましメールの検知を可能とするのが、SPF、DKIM、DMARC といった送信ドメイン認証技術です。詳細な技術の内容は第 3 章で紹介しますのでここでは簡単にふれるだけにしますが、SPF はメールサーバーの IP アドレスを使用して、また、DKIM はメールに付与された電子署名を使用して送信者情報が詐称されていないかどうか検証します。さらに DMARC は、この SPF、DKIM で検証したドメイン名と、メールソフトなどに表示される送信者アドレス（From アドレス）のドメイン名が一致しているかどうかを検証します。さらに、SPF などの認証が失敗した場合のメールの処理方法（ポリシー）を送信側が指定することができ、その認証結果をまとめたレポートを受信側から送信側に送信することを可能にしています。これにより送信側は受信側の認証状況や自組織をなりすますメールの流通状況を把握し、それに対する対策をとることができます。このように、送信者が真正かどうかを、送信側と受信側双方で検証する送信ドメイン認証技術は、世界規模で被害が生じている BEC やフィッシングメールなどに対する対策として非常に有効であると考えられますが、上述の検証の仕組みから、送信ドメイン認証技術がうまく機能するかどうかは、その普及状況が極めて重要になります。

（2）日本における普及状況

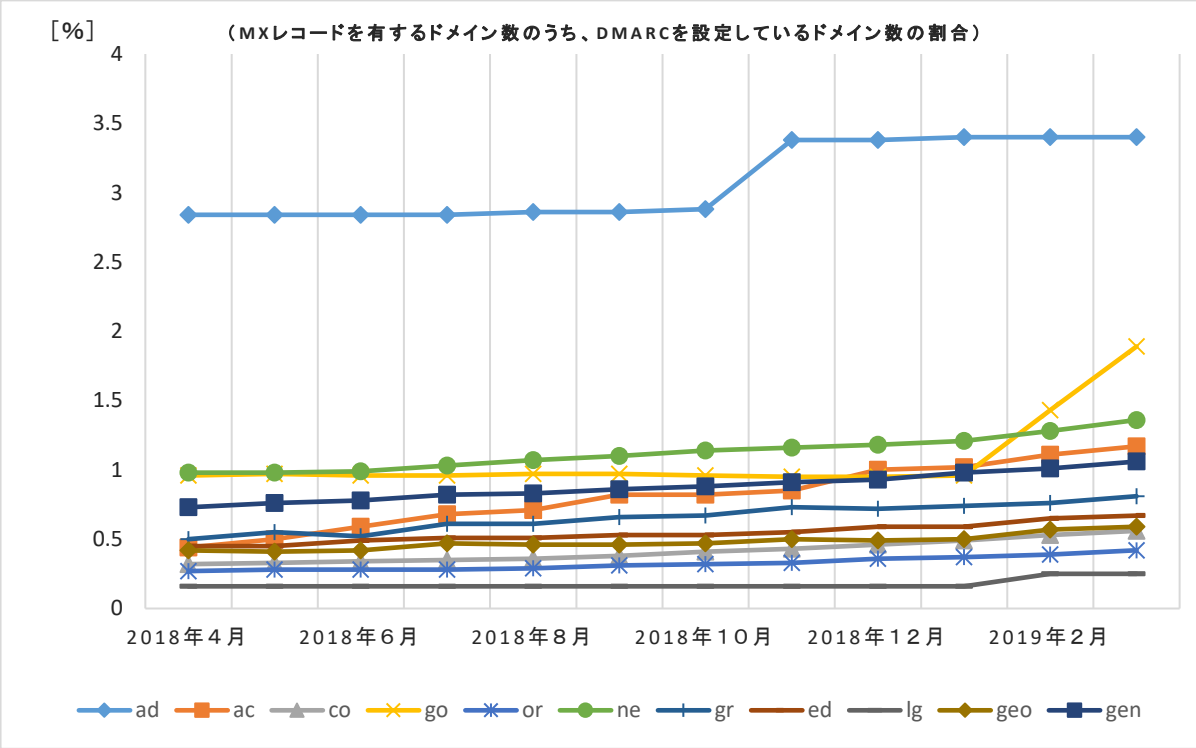
我が国においては、国の行政機関、独立行政法人等が情報セキュリティ対策を実施する際に参照すべき「政府機関等の対策基準策定のためのガイドライン」において、電子メールのなりすまし防止策の一つとして、送信ドメイン認証技術が示されており、各組織が取り扱う情報の特性等を踏まえながら対策を行うことになっています。また、総務省においては、このような送信ドメイン認証技術を普及させるため、2017 年 7 月に DMARC について法的な整理を行い、「DMARC 導入に関する法的な留意点」を発表しました[注4]。それによると、DMARC の特徴的な処理[注5]が、電気通信事業法第 4 条に規定する通信の秘密の侵害に外形的に該当するとしつつも、一定の条件を満たすことで、その違法性が阻却されるとしています。

また、同省においては 2018 年 1 月より、「co.jp」、や「go.jp」といったドメイン毎にその普及状況を調査し、公表しています。そのうち SPF については各ドメインとも普及状況は高く、特に「go.jp」ドメインについては 90%以上の普及率となっています。しかし、DMARC の普及状況は極めて低く、一番高い「ad.jp」ドメインでも 3%程度の普及率であり、「go.jp」ドメインについてはわずか 1 %程度の普及率となっています。

[注4] http://www.soumu.go.jp/main_content/000495390.pdf

[注5] DMARC ポリシーと呼ばれる送信者側が設定したポリシーに基づく処理、DMARC レポートの一種である認証結果レポートの送信

図表１－３－１　ドメイン種別毎のＤＭＡＲＣの設定状況



出典：（一財）日本データ通信協会と（株）日本レジストリサービスとの共同研究

（3）世界における普及状況（米国、英国）

(ア) 米国

2017 年 10 月、米国の政府機関の一つである国土安全保障省は連邦政府機関に対して、DMARC を導入すべき指令を発令しました[注6]。この指令は法的拘束力をもち、30 日以内に DMARC の実装に向けた計画を作成し、3 ヶ月以内にその実装などを政府機関に求めています。また、ポリシーについても 1 年以内に最も厳しい ”reject” に設定するよう求めました。民間企業による調査結果によると、この指令により、発令時に政府ドメインのうち DMARC を導入していたのは約 18%にすぎませんでしたが、 1 年後には実に 85%の政府ドメインに DMARC が導入され、そのうち少なくとも 74%のドメインのポリシーは ”reject” に設定されたとのことです[注7]。同国の民間企業のうち、導入率が 50%を超えているのは、時価総額 10 億ドル以上のテクノロジー企業など一部企業だけといわれている状況の中で、政府機関においてわずか 1 年の間にここまで導入が進んだのは、もちろん一定の強制力をもった指令の存在が一番大きいと考えられます。ただ、導入が進んだ理由としてはそれだけではなく、犯罪者等が政府機関をなりすますことにより起こるフィッシング等の被害に対する、強い危機意識[注8]もその導入が進んだ背景にあったものと考えられます。

注6 国土安全保障省による指令 https://cyber.dhs.gov/bod/18-01/

注7 https://www.agari.com/email-security-blog/dmarc-bod1801/

注8 米国上院議員 Wyden 氏が国土安全保障省に提出した書簡（2017.7.18）
https://www.wyden.senate.gov/imo/media/doc/letter%20to%20DHS%20regarding%20DMARC.pdf

(イ) 英国

2016 年、英国は全ての政府機関に対して同年 10 月までに DMARC の導入を義務付けました。ポリシーについては米国と同じく ”reject” に設定するよう求めています。その導入効果については、英国の歳入関税庁の例が挙げられます。歳入関税庁は、「世界で最もなりすまされたブランドの一つ」といわれ、そのなりすましメールには「還付金のお知らせ」という古典的な手口の件名が付され、受信者の個人情報等を詐取するような仕組みが施されていました。同庁はこれに対応するため DMARC を導入した結果、年間 3 億通ものフィッシングメールを削減したとしています[注9]。その普及率については、最近の民間企業による調査結果によると、調査した 2,000 以上の「gov.uk domains」のうち 28%であり、ポリシーについてはそのうち 53%が「none」と設定しているとのことです[注10]。

2　「情報化促進貢献個人等表彰」の受賞（迷惑メール対策推進協議会）

総務省において、経済社会の情報化の促進に貢献したと認められる個人・企業等（企業、団体、教育機関等）を表彰する「情報化促進貢献個人等表彰」を行っています。迷惑メール対策推進協議会は、2018 年 10 月 1 日に、同表彰の「企業等部門」において、総務大臣賞を受賞しました。これは、迷惑メール対策推進協議会が、「「迷惑メール対策ハンドブック（現 迷惑メール白書）」や「送信ドメイン認証技術導入マニュアル」の発行等により、一般のリテラシー向上や迷惑メール対策技術の導入促進にこれまで 10 年に渡り貢献してきた」ことによるものです。

図表１－３－２　総務大臣賞を受ける迷惑メール対策推進協議会 新美座長

注9 https://hmrcdigital.blog.gov.uk/2016/11/25/combatting-phishing-a-very-big-milestone/

注10 https://www.computerweekly.com/news/252459868/UK-government-organisations-email-security-lagging

3　迷惑メール対策推進協議会 10 周年記念講演

2018 年 11 月 8 日、迷惑メール対策推進協議会 新美座長が、同協議会 10 周年を記念し、「ネット社会は成熟するのか？」と題した講演を行いました。

図表１－３－３　記念講演を行う迷惑メール対策推進協議会 新美座長

トピックス：2018 年度の迷惑メールに関するできごと

2018 年 4 月 3 日

外務省、経済産業省、総務省等の中央省庁の職員延べ 2,000 人余りのメールアドレスが流出し、インターネット上で売買されていることが判明したため、内閣サイバーセキュリティセンターが注意喚起を実施[注 11]。

2018 年 4 月 26 日

ソフトバンク株式会社とトビラシステム株式会社、愛知県警察本部は、ソフトバンクのスマートフォン向けに 2017 年 9 月から提供を開始した、迷惑メールブロック機能の効果を検証した結果、提供開始から 2018 年 3 月末までの約 6 ヶ月間で、約 10 万件の迷惑メールを検知したことが分かったと発表[注 12]。

2018 年 5 月 27 日

インターネットバンキング利用者のＩＤやパスワードを不正に盗み取るウィルス（DreamBot）を添付したメールが、2017 年秋以降大量に送信されていることから、警察庁や（一財）日本サイバー犯罪対策センターが注意喚起を実施[注13]。

2018 年 6 月 6 日

横浜市立大学が、フィッシングによる正規アカウントの乗っ取りにより、3,512 通のメールが外部に無断で転送される事案が発生したと発表[注14]。

2018 年 6 月 8 日

ＬＩＮＥやヤフーなどインターネット関連企業 4 社は、実在する企業などを装ったメールで偽サイトに誘導し、入力させた情報を盗み取る、フィッシング詐欺の被害に遭わないための知識が学べるキャンペーン「サイバー防災訓練」を始め、詐欺の手口を動画などで紹介する特設サイトを開設したと発表[注 15]。

2018 年 6 月 20 日

沖縄県立看護大は、教職員がフィッシングメールの被害に遭い、この教職員宛てのメール 210 件が不正に外部に転送され、学内外の個人情報 330 件が流出したと発表[注16]。

2018 年 6 月 22 日

島根大学は、フィッシングメールにより、5 人の教職員のメール設定が改ざんされた結果、397 通のメールが不正に外部に転送されたほか、1 人の教職員がアカウントを不正に取得され、その教職員になりすました迷惑メールが 2,777 件送信されたと発表[注 17]。

2018 年 6 月 27 日

弘前大学は、フィッシングメールにより、教職員に届いた 3,151 件のメールが不正に転送され、個人情報が漏えいしたと発表[注 18]。

2018 年 6 月 29 日

森永乳業や山崎製パンなど、実在の有名企業を装った「偽キャンペーン」を告知し、住所などの個人情報を入力させようとする迷惑メールが増加していることから、5 月上旬から 6 月下旬にかけ、該当する各社が相次いで注意喚起の文書を発表[注19]。

注11 朝日新聞
注12 https://www.softbank.jp/corp/news/press/sbkk/2018/20180426_01/
注13 読売新聞
注14 https://www.yokohama-cu.ac.jp/news/2018/pr/owabi180607.html
注15 https://linecorp.com/ja/pr/news/ja/2018/2229
注16 http://mono.okinawa-nurs.ac.jp/oshirase/kojinjyoho.html
注17 https://www.shimane-u.ac.jp/docs/2018062200069/
注18 https://www.hirosaki-u.ac.jp/35460.html
注19 https://www.unilever.co.jp/news/press-releases/2018/pay-attention-lipton-consumer-campaign.html
https://www.yamazakipan.co.jp/company/news2/pdf/20180514.pdf

2018 年 6 月 29 日

消費者庁が、アマゾンジャパン(合)などを騙り、ＳＭＳを用いて有料動画等の未納料金の名目で金銭を支払わせようとする架空請求について、注意喚起を実施（2017 年 11 月にも同様の注意喚起を実施）。消費者庁の報道資料によれば、「有料動画の未納料金が発生しており、本日中にご連絡無き場合、法的手続に移行する」などと記載した SMS を送り、SMS に記載された電話番号に連絡してきた者に金銭を請求してくる事業者に関する相談が消費生活センターなどに寄せられたとのこと[注20]。

2018 年 7 月 2 日

実在の仮想通貨交換事業者を騙り、偽メールなどを通じて個人情報を不正に入手する「フィッシング」により、仮想通貨を盗み取ろうとするサイバー攻撃が、国内で本格化していると報道[注21]。

2018 年 7 月 5 日

取引先や上司になりすますビジネスメール詐欺（ＢＥＣ）により、米国の農業関連会社から約 7800 万円を不正に送金させた上、6020 万円を引き出したとして、警視庁は男女 4 人を逮捕したとの報道[注22]。

2018 年 8 月 1 日

佐川急便を装ったＳＭＳをスマートフォンに送りつけ、連絡先など個人情報を抜き取られるだけでなく、そのスマートフォンから不特定多数に同様のＳＭＳを送信するサイバー攻撃が多発しているとの報道。それによると、佐川急便への相談は 7 月に入ってから急増し、ＳＭＳの文例が 20 種類以上あることが確認されたとのこと[注23]。

2018 年 8 月 14 日

トレンドマイクロ社は、取引先や上司になりすまして偽メールを送り、金銭をだまし取る「ビジネスメール詐欺」（BEC）について、企業のＩＴ部門や経理部門の責任者計 1,030 人を対象にしたアンケートの結果を発表した。それによると、39%に当たる 406 人がこの種のメールを受け取ったことがあると回答し、そのうち 22 人が実際に送金手続きを行い、被害額についても 2 人が 1 億円以上を送金していたとのこと[注24]。

2018 年 8 月 27 日

情報処理推進機構（ＩＰＡ）は「ビジネスメール詐欺」（BEC）で、日本語によるものが初めて見つかったと発表[注25]。

2018 年 9 月 4 日

トレンドマイクロ社は、クレジットカードなどの情報を盗むために、電子メールを送りつけて偽サイトを開かせる「フィッシング」詐欺の手口で、偽サイトに誘導された件数が、日本国内で今年上半期（1～6 月）に過去最多の約 290 万件に上るとの調査結果を公表した。傾向としては、アップルやアマゾン、楽天など有名企業のサービスを利用する際に使われるアカウントを盗もうとする攻撃が増加したとのこと[注 26]。

2018 年 9 月 12 日

情報セキュリティ会社サイバーリーズンによると、情報を盗み取るほか、業務を妨害する目的で、社内のパソコンの基本ソフト（ＯＳ）を一斉に起動できなくする新手のサイバー攻撃が国内企業に行われ、一度に数百台のパソコンが使えなくなった企業もあったとのこと[注27]。

2018 年 10 月 1 日

総務省において行った、情報化促進貢献個人等表彰において、「迷惑メール対策推進協議会」が企業等部門の総務大臣賞を受賞[注 28]。

注20 https://www.caa.go.jp/policies/policy/consumer_policy/information/pdf/consumer_policy_information_180629_0001.pdf
注21 産経新聞
注22 日経新聞
注23 産経新聞
注24 https://www.trendmicro.com/ja_jp/about/press-release/2018/pr-20180814-01.html
注25 https://www.ipa.go.jp/security/announce/20170403-bec.html
注26 https://resources.trendmicro.com/jp-docdownload-form-m087-web-20181h-securityroundup.html
注27 読売新聞
注28 http://www.soumu.go.jp/menu_news/s-news/01tsushin10_02000047.html

2018 年 10 月 8 日

総務省および(一財)日本データ通信協会が、米国（ニューヨーク）で開催された M[3]AAWG／UCENet 合同会合に参加し、迷惑メール対策を担当する各国の執行当局と意見交換を実施[注 29]。

2018 年 10 月 16 日

ドメイン専用のオークションサイトに、ＮＨＫ関連団体の旧サイトのドメイン名が出品されており、落札した第三者が本物のサイトを装って悪用する恐れがあるとの報道[注 30]。

2018 年 10 月 23 日

データ分析会社アントゥイットの調査によると、2020 年の東京五輪に便乗し、無料チケットの提供を装った不正メールによるサイバー攻撃がネット上で計画されていたことがわかったとのこと[注31]。

2018 年 10 月 27 日

トレンドマイクロ社の調査によると、アダルトサイトを閲覧している姿を録画した、とする偽メールを送りつけて脅し、仮想通貨をだまし取る手口の詐欺被害が相次ぎ、少なくとも攻撃者側に 46 件の払い込みがあり、計 250 万円分の被害が確認できたとのこと[注 32]。

2018 年 11 月 8 日

2018 年 10 月末に設立を発表した「JPAAWG」（Japan Anti-Abuse Working Group。メールのセキュリティについて情報を交換したり対策を検討したりする業界団体）が、第一回総会を開催[注 33]。

2018 年 11 月 26 日

宅配大手の不在通知を装ったフィッシング詐欺が相次いでいる問題で、iPhone 利用者を標的とした新種のＳＭＳが出回っており、毎月の通話料と合算する「キャリア決済」の認証コードを盗まれ、勝手に「iTunes カード」などを購入される被害が出ているとの報道[注 34]。

2019 年 1 月 22 日

違法薬物の密売や振り込め詐欺などの組織犯罪で、犯罪グループ内のメッセージのやり取りが完全消去されるアプリやメールが相次いで発見されており、最新のデジタルフォレンジック（鑑識技術）でも復元は不可能で、捜査の障壁になっているとの報道[注 35]。

2019 年 2 月 8 日、12 日

自治体 CSIRT 協議会[注36]が開催した平成 30 年度技術講習会（大阪、東京開催：地方公共団体の情報セキュリティ担当者向け）で、迷惑メール対策推進協議会技術 WG の構成員が、DMARC を中心に「送信ドメイン認証技術」について講演。

2019 年 3 月 7 日、8 日

(一財)日本データ通信協会が、サイバーセキュリティシンポジウム道後 2019 [注37]に参加し、展示会場にて、迷惑メール白書 2018 の紹介活動を実施。

2019 年 3 月 28 日

企業のメールアドレスを乗っ取り偽の振込みの指示を行う、いわゆる「ビジネスメール詐欺」（BEC）により、約１億１千万円を詐取したとして、２人の日本人が逮捕されたとの報道[注 38]。

注29 https://www.m3aawg.org/events/44th-general-meeting
注30 朝日新聞
注31 読売新聞
注32 産経新聞
注33 https://meetings.jpaawg.org/
注34 読売新聞
注35 読売新聞
注36 https://www.j-lis.go.jp/spd/security/csirt_kyougikai/about_csirt_kyougikai.html
注37 http://sec-dogo.jp/
注38 朝日新聞

第２章

迷惑メールについて

第1節　電子メールとは

1　電子メールなど

個人や組織の間で交わされる情報は、以前は手紙やハガキ、電話やファックスなどでやりとりされていましたが、近年では電子メールやメッセージアプリなどを利用し、インターネット経由でやりとりすることが増加しています。なかでも電子メールについては、1993 年のインターネットの商用利用の開始以降、次々に誕生した ISP がインターネット接続を開始し、その利用が広がり、1999 年に(株)NTT ドコモの携帯電話で i モード[注39]が開始されるなど、携帯電話のネットワークからもインターネットへの接続が可能となったことにより、その利用はより身近なものとなりました。また、ブロードバンド化の急速な進展などに伴い、現在では、電子メールは、社会経済活動や市民生活において必要不可欠な連絡・伝達の手段となっています。

電子メールには、SMTP（Simple Mail Transfer Protocol）という通信方式を使ったインターネットのメールや、SMS（Short Message Service）と呼ばれる携帯電話の電話番号を用いたメッセージ送信などがあります。また、スマートフォンの普及に伴い、電子メールなどと同様にメッセージの交換ができる SNS（Social Networking Service）の利用も一般的となっています。

図表２－１－１　電子メールなどのメッセージ交換サービスの主な種類

種別	サービスの概要
電子メール（SMTP）	電子メール（SMTP）とは、SMTP（Simple Mail Transfer Protocol）という通信方式を使用して、電子メールアドレスを宛先にし、インターネットを介してテキストや画像などをやり取りするサービスです。その際、電子メールアドレスは「利用者名@ドメイン名」で表記され、個人を識別する利用者名と、所属する組織やサービスを提供する事業者などをあらわしたドメイン名で構成されます。電子メールは、パソコンなどでメールソフトを利用したり、携帯電話を利用したり、インターネットのブラウザを利用したり（Web メール）、様々な方法で送受信されます。
SMS	SMS とは、Short Message Service の略で、電話番号を宛先にし、携帯電話事業者のネットワークを介して、短いテキストをやり取りするメッセージングサービスです。事業者によって多少呼び名や機能が異なりますが、携帯電話事業者のネットワークを利用して、メッセージや絵文字を携帯電話同士で送受信することが可能です。
SNS	SNS とは、Social Networking Service(Site)の略で、インターネット上で友人を紹介しあい、個人や組織間の交流を支援するサービス（サイト）です。利用者は自身のプロフィールなどを公開できるほか、その SNS 上で友人などのプロフィールなどを閲覧したり、コメントしたり、メッセージを送ったりすることができます。最近では、会社や組織の広報としての利用も増えてきました。

[注39] 1999 年 2 月に NTT ドコモが携帯電話向けサービスとして開始した、電子メールの送受信や Web ページの閲覧などができるインターネットサービス。

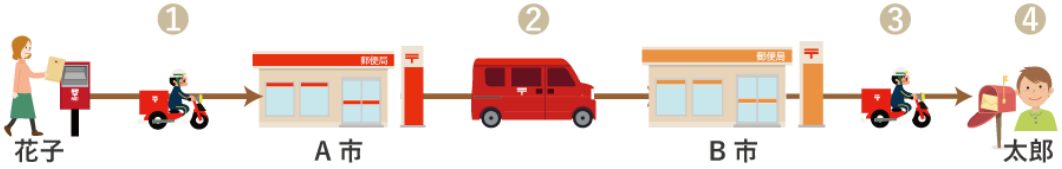
２　電子メールの仕組み

メールソフト[注40]で文章を書いて「送信」をクリックすると、その文章が相手に届きます。いつも私たちが便利に使っている電子メールですが、そもそもどのような仕組みになっているのでしょうか。SMTP を使った電子メールの送信などの仕組みを郵便の仕組みにたとえながら説明していきます。

（１）送受信の仕組み

郵便物が A 市の花子さんから B 市の太郎さんに送られる場合には、以下のように配達されます。

図表２－１－２　郵便物の配達

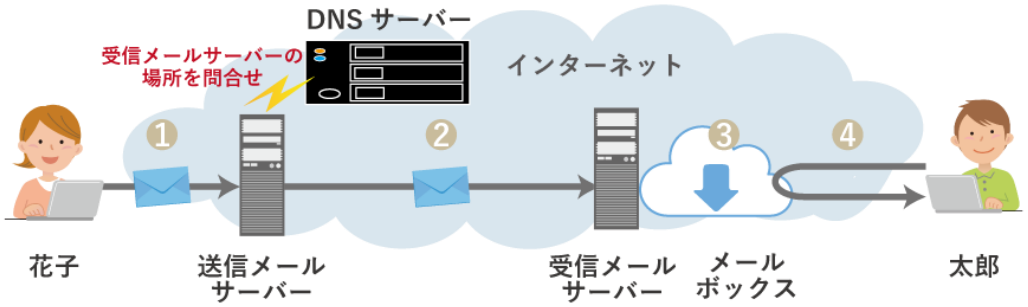


1. ポストに投函された郵便物が A 市の郵便局に配送される
2. A 市の郵便局から B 市の郵便局に配送される
3. B 市の郵便局から太郎さんの住所に配達される
4. 太郎さんがポストから郵便物を受け取る

[注40] MUA（Mail User Agent）といい、Microsoft Outlook や Mozilla Thunderbird などのメールクライアントソフトウェアを指す。

一方、電子メールが花子さんから太郎さんに送られる場合には、以下のように配送されます。

図表２－１－３　電子メールの配送



1. 電子メールが送信メールサーバー[注 41]に投稿される（ポストへの投函と最寄りの郵便局への配送に当たります）
2. 投稿された電子メールが、送信メールサーバーから受信メールサーバーに配送される※（最寄りの郵便局から宛先の郵便局への配送に当たります）
3. 受信メールサーバーから、受信者のメールボックスに電子メールが保存される（宛先の郵便局から住所への配達に当たります）
4. 受信者が受信メールサーバーに対して自らの端末への配送要求を行い、電子メールを受信する（ポストの確認・受取りに当たります）[注 42]

※　郵便の場合は、郵便局が住所を統一的に把握していますが、インターネットの場合は、それぞれのネットワークごとに宛先が管理されているため、DNS サーバー（Domain Name System サーバー）に対して問い合わせを行い、受信側メールサーバーの情報を確認する必要があります。インターネットでは、接続されている機器には、「IP アドレス」という固有の番号が割り当てられ、通信は、相手の機器の IP アドレスを指定することにより行われます。しかし、電子メールの送受信においては、宛先は電子メールアドレスで指定されます。このため、電子メールが投稿された送信メールサーバーは、その電子メールアドレスのドメイン名から、それに対応する受信メールサーバーの IP アドレスを確認する必要があり、この確認は、サーバーの IP アドレスなどが登録された DNS サーバーに問い合わせることで行われます。

（２）宛先の仕組み

郵便では、手紙の場合には、封筒と便箋の両方に宛先や差出人を記載します。このうち、封筒への宛先の記載は必須であり、郵便物は、その住所に対して配送されます。その他は、郵便物の配達には用いられず、どのような情報でも記載が可能です（記載しないことも可能）。

電子メールでも、手紙の場合と同様に、封筒に書かれた宛先や差出人にあたる情報と、便箋に書かれた宛先や差出人にあたる情報があり、いずれも電子メールアドレスが用いられます。手紙の場合の封筒に書かれた情報にあたる情報は「Envelope-To」および「Envelope-From」[注 43]と便箋に書かれた情報にあたる情報は、

注41 MSA（Message Submission Agent）といい、電子メールを送信する際に接続するメールサーバーを指す。

注42 電子メールを受信するための通信方式として、ユーザーが受信メールサーバーへアクセスして受信した電子メールをパソコンなどに保管する「POP」という方式や、電子メールを受信メールサーバーに置いたまま管理する「IMAP」という方式があります。

注43 電子メールの通信プロトコルである SMTP（Simple Mail Transfer Protocol）の仕様を定めた RFC5321 では、「Envelope-To」、「Envelope-From」は、それぞれ「forward-path」、「reverse-path」とされています。

「Header-To」および「Header-From」[注44]といいます。このうち、電子メールの配送に用いられるのは、「Envelope-To」のみであり、他の情報は、配送には用いられず、どのような情報（電子メールアドレス）でも利用が可能です。送信元を偽装したなりすましメールが送信されることがあるのは、このためです[注45]。

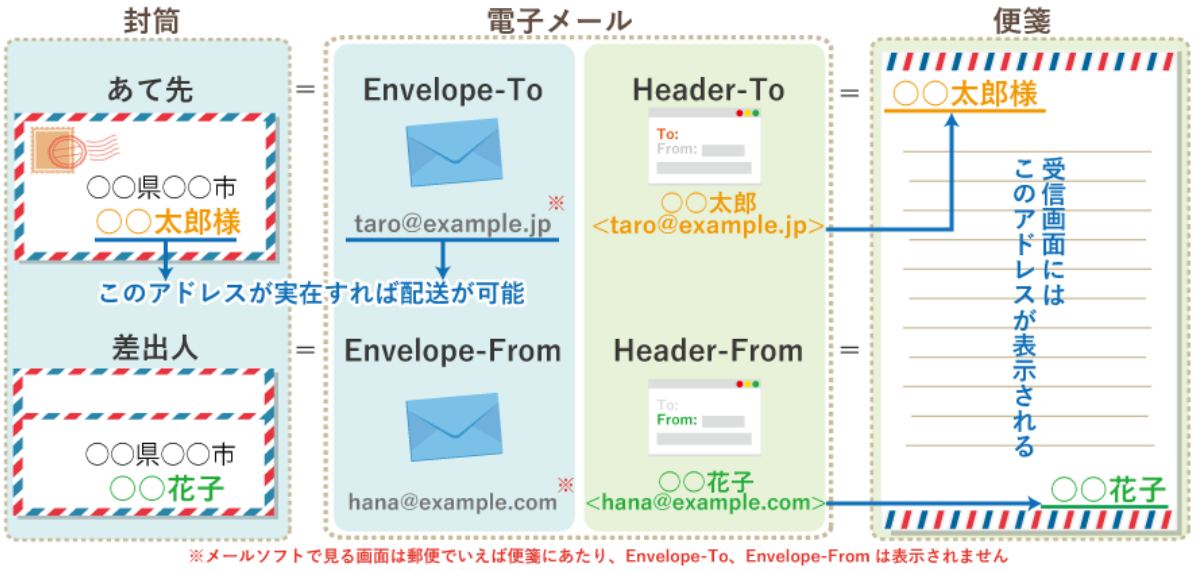
なお、郵便の場合と異なり、「Envelope-To」および「Envelope-From」は、メールサーバー間の通信においてのみ用いられ、受信者に届けられることなく、メールソフトで表示される宛先・差出人は、「Header-To」および「Header-From」の情報になっています[注46]。

以上を、比較表ならびに図式にしてみると次のようになります。

図表２－１－４　郵便と電子メールの比較表

郵便の場合	電子メールの場合
封筒に書かれた宛先	Envelope-To
封筒に書かれた差出人	Envelope-From
便箋（本文）に書かれた宛先	Header-To（受信画面に表示される）
便箋（本文）に書かれた差出人	Header-From（受信画面に表示される）

図表２－１－５　Envelope-To と Envelope-From、Header-To と Header-From



上図の示すように、電子メールの「Header-To」および「Header-From」には、送信者の個人名（○○太郎、○○花子）や法人名などを表す「ディスプレイネーム」を追加することが可能であり、それらは受信者のメールソフト上で表示されます。

注44 インターネットメッセージの仕様を定めた RFC5322 では、「Header-To」、「Header-From」は、それぞれ「destination field」、「from field」とされています。

注45 「Envelope-To」以外の情報を自由に記載できることには、メリットもあります。例えば、「Header-To」と「Envelope-To」 が分かれていることにより、他の受信者に電子メールアドレスが見えないように宛先を指定する BCC（「Header-To」には表示されないが、「Envelope-To」には設定されている。）での送信が可能になっています。

注46 「Envelope-To」および「Envelope-From」を配送上の受信者情報・送信者情報、「Header-To」および「Header-From」をメールヘッダーの受信者情報・送信者情報ということもあります。

第2節　迷惑メールとは

1　迷惑メールの特徴

「迷惑メール」とは何かについては、誰もが一致するような確たる定義はなく、様々な説明が行われていますが、社会的な問題となるような「迷惑」なメールとしては、次のような特徴が見られます。

（1）受信者の意思に反する

- 受信者の同意・承諾を得ずに送信されるもの
- 受信者が送信を拒否しても引き続き送信されるもの
- 受信者の生活や業務に支障を及ぼすような頻度で送信されるもの

（2）迷惑な内容が含まれる

- ウイルスなどのマルウェア感染や不正アプリのインストールを目的とするもの
- 詐欺目的のもの（個人情報を不正に取得する目的のフィッシングメール、ワンクリック詐欺を誘引するメール、架空請求メールなど）
- 有害情報を含むもの（違法な商品の広告・宣伝や、受信者の年齢などを考慮せずに行われる出会い系・アダルト系などの広告・宣伝など）
- 同じ内容を誰かに転送するよう促す目的で送信されるもの（チェーンメール）
- 特定企業を標的に、従業員をだまして不正な送金処理をさせることを目的としたもの（ビジネスメール詐欺（BEC））

（3）迷惑な手法で送信する

- 架空電子メールアドレス（プログラムを用いて自動的に作成された、利用者の存在しないメールアドレス）を宛先に大量に含んで送信されるもの
- 電気通信設備に過大な負担を生じさせるような一時に大量に送信されるもの
- 送信者情報や経路情報（メールが配送されてきた道筋（サーバー）を示す情報）が偽装されているもの（なりすましメール）
- エラーメールの仕組みを悪用して送信されるもの（届けたい宛先を送信者情報として記述することで、送りたい内容をエラーメールとして送信させるもの）

２　迷惑メールの具体例

（１）事前同意のない広告・宣伝メール

受信者の事前同意なく送信される迷惑メールには、様々な内容のものが存在します。その中でも、事前同意なく広告・宣伝メールを送信することは、特定電子メールの送信の適正化等に関する法律（以下、「特定電子メール法」という。）や特定商取引に関する法律（以下、「特定商取引法」という。）の規定により、原則禁止されています。広告・宣伝メールについては、同意があった場合でも、受信者が配信停止を希望したときは、その後の送信はできません。

事前同意のない広告・宣伝メールの例（出会い系のメール）

送信者：XXXXmail@example.com
件名：★*。。。*☆本日限定【1000 円：本会員登録】で案内中の豪華特典併用ゲット☆*。。。*★

★I XXXX YOU★
ぜ｜ん｜ぶ｜
┗┛┗┛┗┛
１｜０｜０｜０｜円｜
┗┛┗┛┗┛┗┛┗┛
現在、全決済で 1000 円本会員登録サービスを行っておりますので【GOLD KING 会員昇格】と本会員登録を同時に 1000 円で行う事が出来ます♪
ポイント購入を１度でも行っていただければ本会員登録完了となり【GOLD KING 会員】に昇格できます♪
▼【GOLD KING 会員】詳細▼
http://＊＊＊＊＊/＊＊＊＊＊/
▼【1000 円】本会員登録ｷｬﾝﾍﾟｰﾝ詳細(無料)▼
http://＊＊＊＊＊/＊＊＊＊＊/
↓各種ポイント購入方法↓
☆ﾋﾞｯﾄｷｬｯｼｭ☆
http://＊＊＊＊＊/*＊＊＊＊＊/
（中略）
▼お問合せ▼
http://＊＊＊＊＊/＊＊＊＊＊/

I XXXX YOU
※

仮に事前同意があったとしても、この例のように、送信者名・住所・連絡先や、配信停止ができることとその通知先がないなど、表示義務を満たさなければ法律違反となります。

（２）詐欺メール

詐欺メールとは、事前に準備された偽サイトへのリンク（有名検索サイトのドメインを入れるなど、不審に思われないように巧妙に記述されています。）を本文中に置き、文面で本物と信じさせることで、その偽サイトにアクセスさせたり、添付されたファイルを介してウイルスに感染させたりするなどして、情報や金銭を詐取することが目的のメールです。詐欺メールの例としては、身に覚えのない架空の有料コンテンツの利用料などを請求するようなものや、「フィッシング」などがあります。

- フィッシング
  - 金融機関など一般消費者の認知度の高い企業やブランドを装った電子メール（フィッシングメール）を送り、口座番号、パスワード、クレジットカード番号などの個人情報を詐取する行為です。電子メールの URL から本物と見分けのつかない偽サイトに誘導し、そこで個人情報を入力させる手口が一般的に使われています。
- ビジネスメール詐欺（BEC）
  - 取引先などを装い、それになりすました偽のメールを送り、用意した口座などに金銭を振り込ませ詐取する行為です。攻撃者は、担当者がメールで取引を進めている間、不正アクセスしたシステムでやりとりを盗み見ます。金銭の請求段階に入ったところで、取引先になりすましたメールを送信して担当者をだます手口が一般的に使われています。

詐欺メールの例（架空請求のメール）

送信者：＊＊＊＊＊service<info@example.com>
件名：アカウント凍結による所有者特定措置行使【(株)＊＊＊＊＊】
――

開示 ID 番号　第＊＊＊＊＊49 号
(＊＊＊＊＊@example.jp)殿

下記、ご確認お願い申し上げます
・情報開示請求概要(プロバイダ責任制限法第 4 条)
開示関係役務提供者
株式会社＊＊＊＊＊デジタルコンテンツ管理部

貴殿(＊＊＊＊＊@example.jp)は＊＊＊＊＊が管理する＊＊＊＊＊【ウェブアプリケーション】(インターネット上における電子商取引に基づいた有料サイトおよび無料期間を設けた月額制サービス)ご登録後、無料期間終了後に正式な解約処理を行わないまま放置をされ現在、利用料金を滞納している状態となっております。

（中略）
＊＊＊＊＊（下記 WEB コンテンツ一覧）に登録をしてない、利用した記憶がない、その他間違いである場合、当窓口にご連絡を頂きましたら、登録情報の確認並びに本人確認を行うことが可能となっております。
（中略）

尚、このままいずれかのご返答が確認できなかった場合は債権回収三次団体への委託処分となります。債権回収三次団体は国からの認可を受け、合法的な強制処分を執行できる機関となります。
1.ご口座及び給与の差押え
2.所有財産(ご自宅、家財、車)の競売処分
3.自宅への訪問及びご自宅のポスト及びドアなどへの督促状の貼り付け
4.ご親族、職場へのご連絡と代理返済の要求を代理人弁護士を通じて法的手続きによる執行と致します。
このような事態にならないよう貴殿の速やかな対応をお願い致します。
（中略）

貴殿の速やかな対応が予期せぬトラブルを防ぎ、これ以上の請求の発生を防ぐ唯一の手段となりますのでご対応の程、お願い申し上げます。
以上
■会社概要およびサービス概要（後略）

（3）ウイルスメール

ウイルスメールとは、攻撃者がウイルスを含んだ添付ファイルを送ったり、ウイルスに感染するリンク先などを送ったりするメールです。添付ファイルを開くことなどによりウイルスに感染すると、感染した PC やスマホから情報が盗まれる、ファイルを暗号化して PC やスマートフォンを利用できないようにされ身代金を要求される、コントロールが奪われて遠隔操作され、迷惑メールの送信に利用されるなどの被害を受けます。

ウイルスメールの例（当選を装ったメール）

送信者：銀行送金担当/○原<＊＊＊＊＊@example.com>
件名：ゲスト様、この度の消費者応援企画での¥300000000 ご当選誠におめでとうございます。
―――

本文の確認
http://＊＊＊example.com/＊＊＊＊＊/＊＊＊＊＊
最初の画面
http://＊＊＊example.com/＊＊＊＊＊/＊＊＊＊＊

サイトへのリンクをクリックすることで、偽サイトへ繋がり、ウイルスに感染する可能性があります。

（4）チェーンメール

チェーンメールとは、そのメールを受け取った人に転送を呼びかけ、それが次々と連鎖していく迷惑メールであり、断ち切らないと自分が加害者になってしまいます。チェーンメールの種類としては不幸の手紙系のもの（転送しないと不幸になる、危害を加えるなどと脅かして転送させるもの）、幸福系のもの（メールを送信すれば幸せになるとして転送させるもの）や、募集系のもの（人の善意を利用して転送させるもの）あるいはバトン系のもの（友だち内でバトンを回させるもの）などがあります。

チェーンメールの例（不幸の手紙系、募集系のメール）

＜不幸の手紙系のメール（脅かして転送を促す内容）＞

これは、最後までとばさずに読んで下さい。でないと、大変な目に合います。
あるところに、●子という人が居ました。●子は、両親が事故で亡くなり、いじめられるようになりました。そして、自殺してしまいました。●子は、まだこの世をさまよっています。
このメールを、8 人以上に送らないと●子があなたのところに、襲いに来ます。何故かはおわかりですね？
もちろん、あなたを裏切り者の親友とみて死の世界に連れて行くか、自分と同じ運命をたどわせるかの辺りでしょう。
8 人以上に送ればあなたを友達とみて襲いに行くことはないでしょう。
世界には三つだけ、本物のチェーンメールがあるって知っていますか？
これはその三大チェーンメールの一つです。本当に危ないです。どのメールよりも危ないです。命が惜しければ、すぐに送って下さい。
いつ襲いに来るかは分かりません。一人でいると危険です。●子は、朝から晩までだって一人になればいつでも来るでしょう。本当に危ないです。気をつけて下さい。
テレビや鏡からもでてくるらしいので、気をつけて下さい。
タイムリミットは、メールがきてから 24 時間後までです。だんだんあなたに死が。たまにフェイントをかけるみたいです。
フェイントは何人かが、かけられたみたいです。例えば、鏡の中を横切ったり、携帯の画像に●子がいたり、テレビに映ったり、寝てたらお腹の上に乗っていたり、誰も居ないのに声がしたり等です。
このメールを送って来た人に送りかえすと、ただ送らないより大変な事が起こります。たまに友達や、家族に化けるみたいなので…あと、知らない着信がくるかも…しかも、自分の知らない着信....。
タイムラインでもオッケーらしい！
これ********で調べたらほんとだったらしいです。

＜募集系のメール（善意の気持ちから転送を促す内容）＞

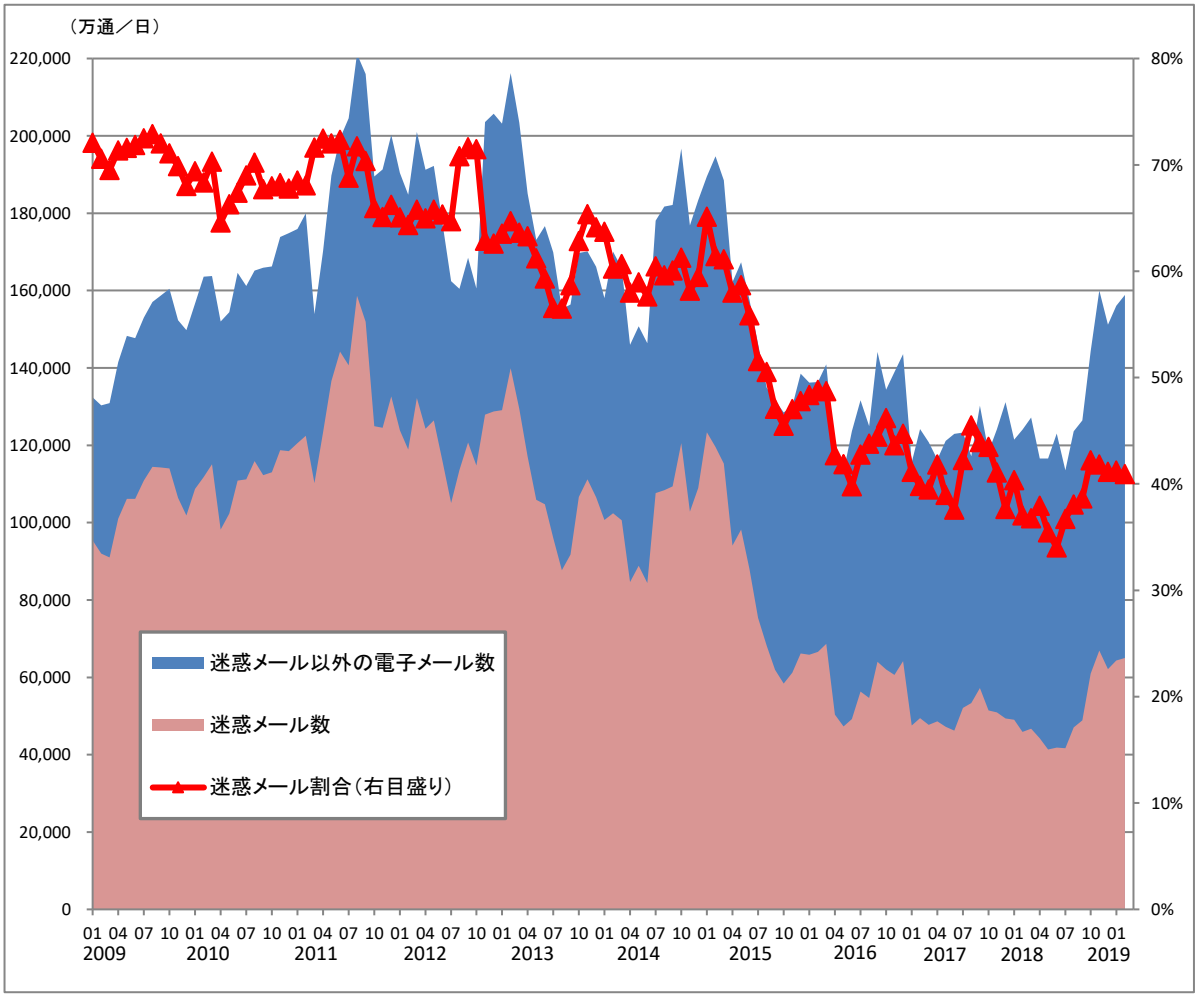
友人の子どもがＲＨマイナスＢ型の血液不足で手術が受けれない状態です！誰かＲＨマイナスＢ型の方いませんか！？
１人の幼い子の命がかかっていて、とても危険な状態だそうです！
最寄りの献血センターで献血できるようなので、是非是非協力おねがいします！
分からないことあればいつでも連絡ください！090********
なかなかない血液みたいで、私だけの人脈だと間に合わないのでおねがいします！

第3節　迷惑メールの動向

1　全体的傾向

日本では、2001 年頃から迷惑メールが社会問題になった後、電気通信事業者などの関係者により、様々な迷惑メール対策が講じられてきました。国内の ISP の取り扱う国内着の電子メールのうち、迷惑メールの占める割合は減少傾向にあり、2012 年までは 70%前後の高い水準にありましたが、それ以降は徐々に減少し、2018 年３月では 40%を切る状況になりました。しかし、2018 年６月以降はそれまでの傾向とは異なり、その割合は増加傾向にあります。このうちのかなりの部分は電気通信事業者のフィルターなどで対応されていることから、実際に利用者に届く迷惑メールはその割合よりも低いと考えられますが、利用者は注意が必要です。

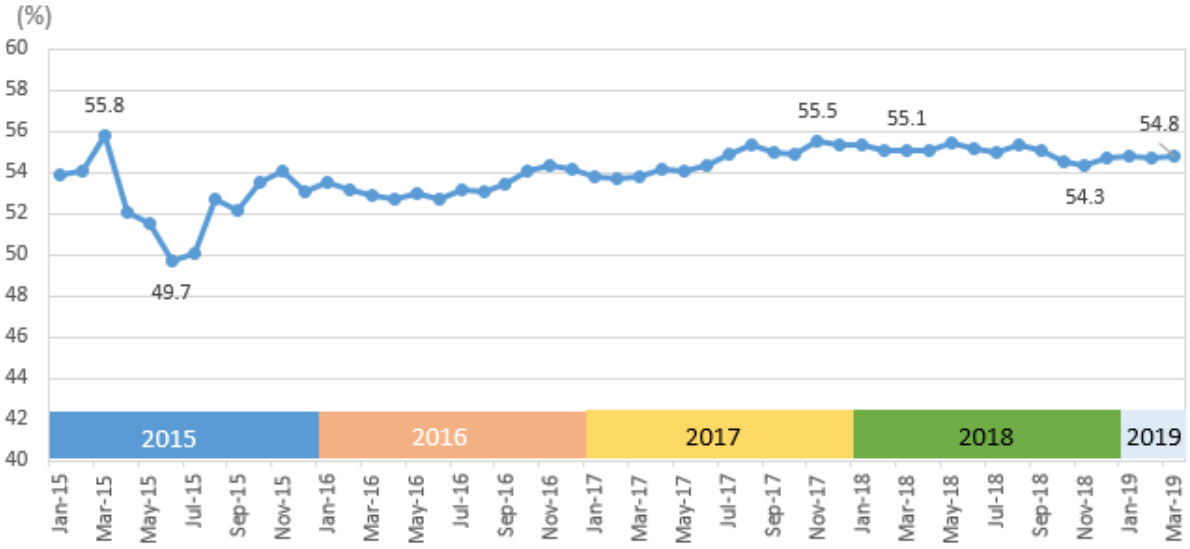
図表２－３－１　国内 ISP における迷惑メール数・割合の推移



出典：総務省「電気通信事業者 10 社の全受信メール数と迷惑メール数の割合（2019 年３月時点）」

また、世界的な迷惑メールの割合は、2015 年の一時期に急減しましたが、その後回復し、2016 年以降はほぼ横ばいの状態が続いています。

図表２－３－２　世界的な迷惑メールの割合



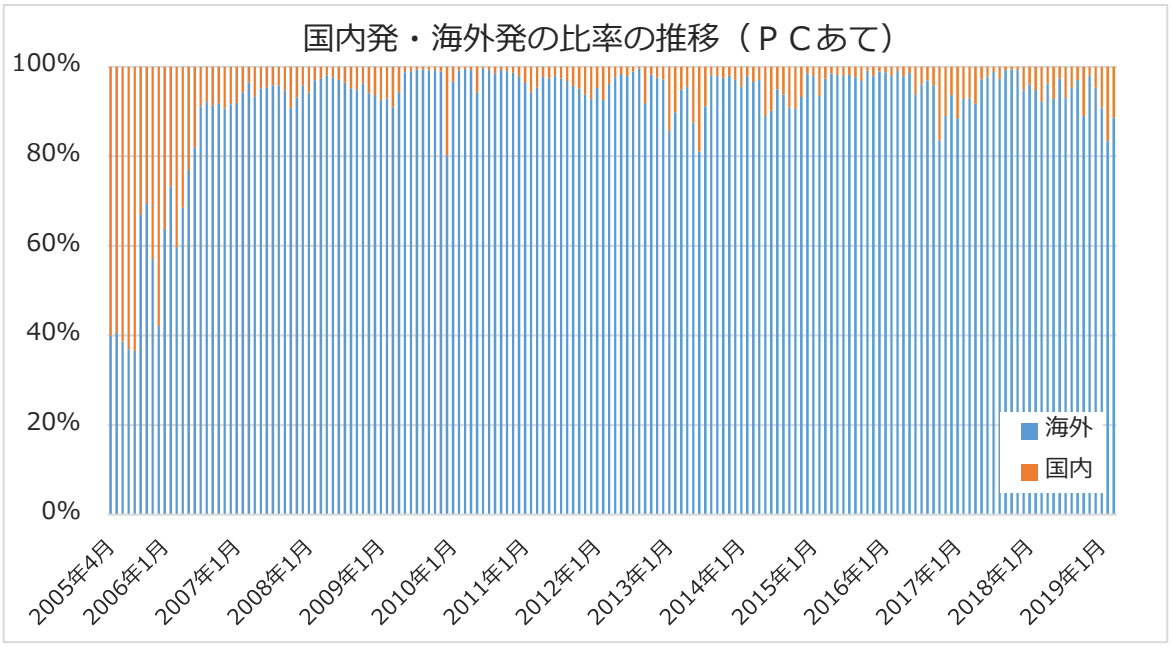
出典：シマンテック「2019 年インターネットセキュリティ最新レポート　セキュリティレスポンスブログ」

２　国内発の迷惑メールの割合

国内着の迷惑メールのうち国内発のものの割合は、PC 宛ての迷惑メールについては減少してきており、その多くを海外発のものが占める一方で、携帯電話宛ての迷惑メールについては依然として高く、その半数程度を国内発のものが占める傾向が続いています。

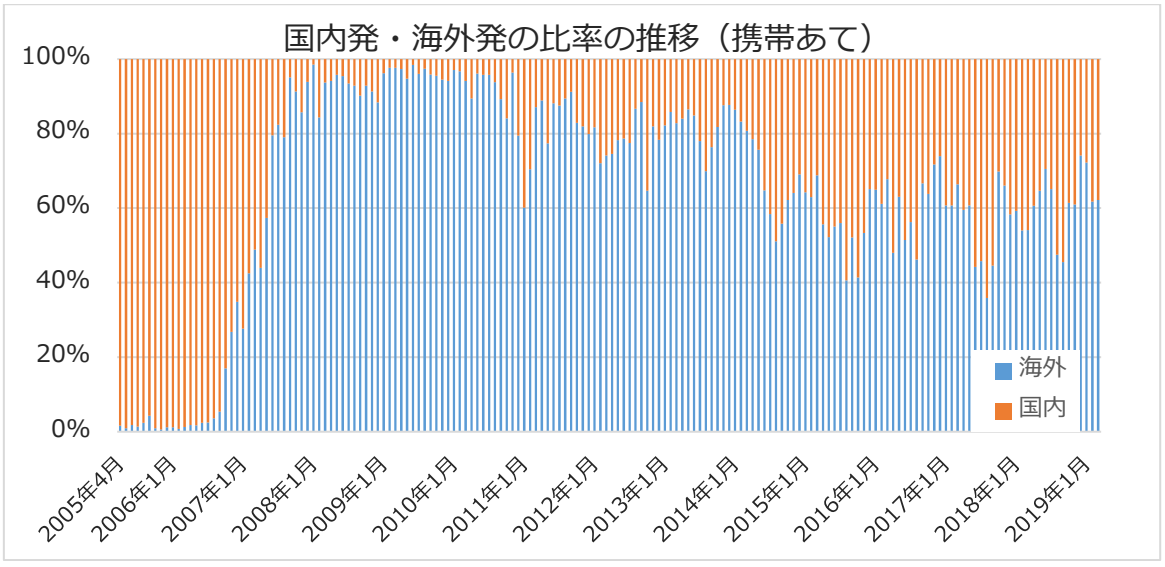
(一財)日本データ通信協会が設置しているモニター機に着信した迷惑メールでは、国内発のものの割合は、PC 宛ての迷惑メールについては 2005 年には 50%を超える時期があったものの、その後は減少し、2006 年以降はそのほとんどが海外発のものとなっています。一方、携帯電話宛ての迷惑メールについては、国内発のものが一時期減少しましたが、2014 年以降は増加傾向にあり、現在では半数程度が国内発のものとなっています。

図表２－３－３　国内発・海外発の比率の推移（PC あて）



出典：（一財）日本データ通信協会迷惑メール相談センター調べ（センターのモニター機で受信した情報を分析したもの）

図表２－３－４　国内発・海外発の比率の推移（携帯あて）

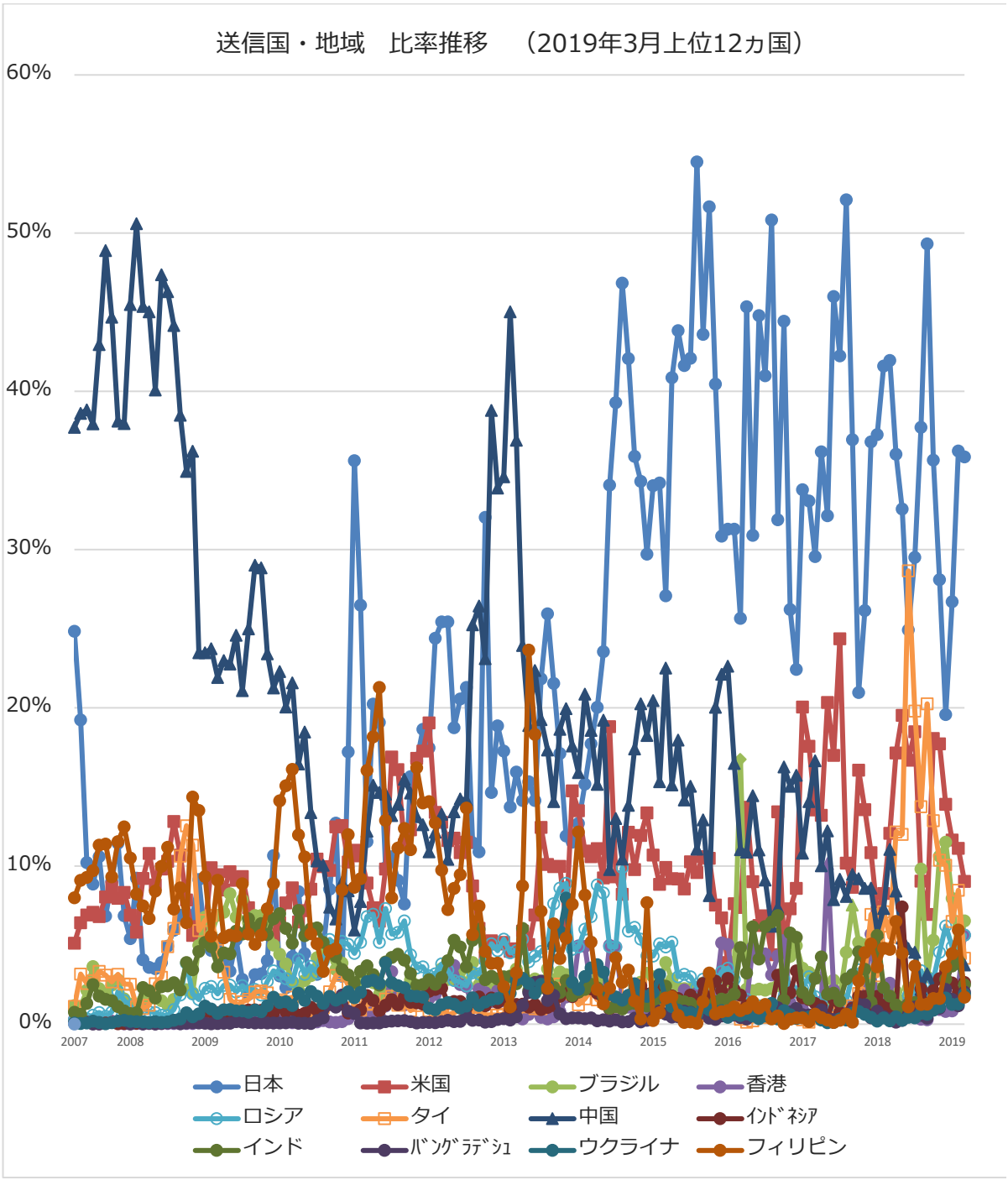


出典：（一財）日本データ通信協会迷惑メール相談センター調べ（センターのモニター機で受信した情報を分析したもの）

3　迷惑メールの送信国・地域

国内着の迷惑メールの送信国・地域としては、2018 年までは日本、米国、中国が上位にある傾向が続いていましたが、2019 年は中国からの送信が減り、ブラジルや香港からの送信が増加しました。特にブラジルからの送信は 2018 年 8 月から増え始め、2019 年 3 月時点においても多くの迷惑メールが送信されています。

図表２－３－５　国内着の迷惑メールの発信国・地域の推移



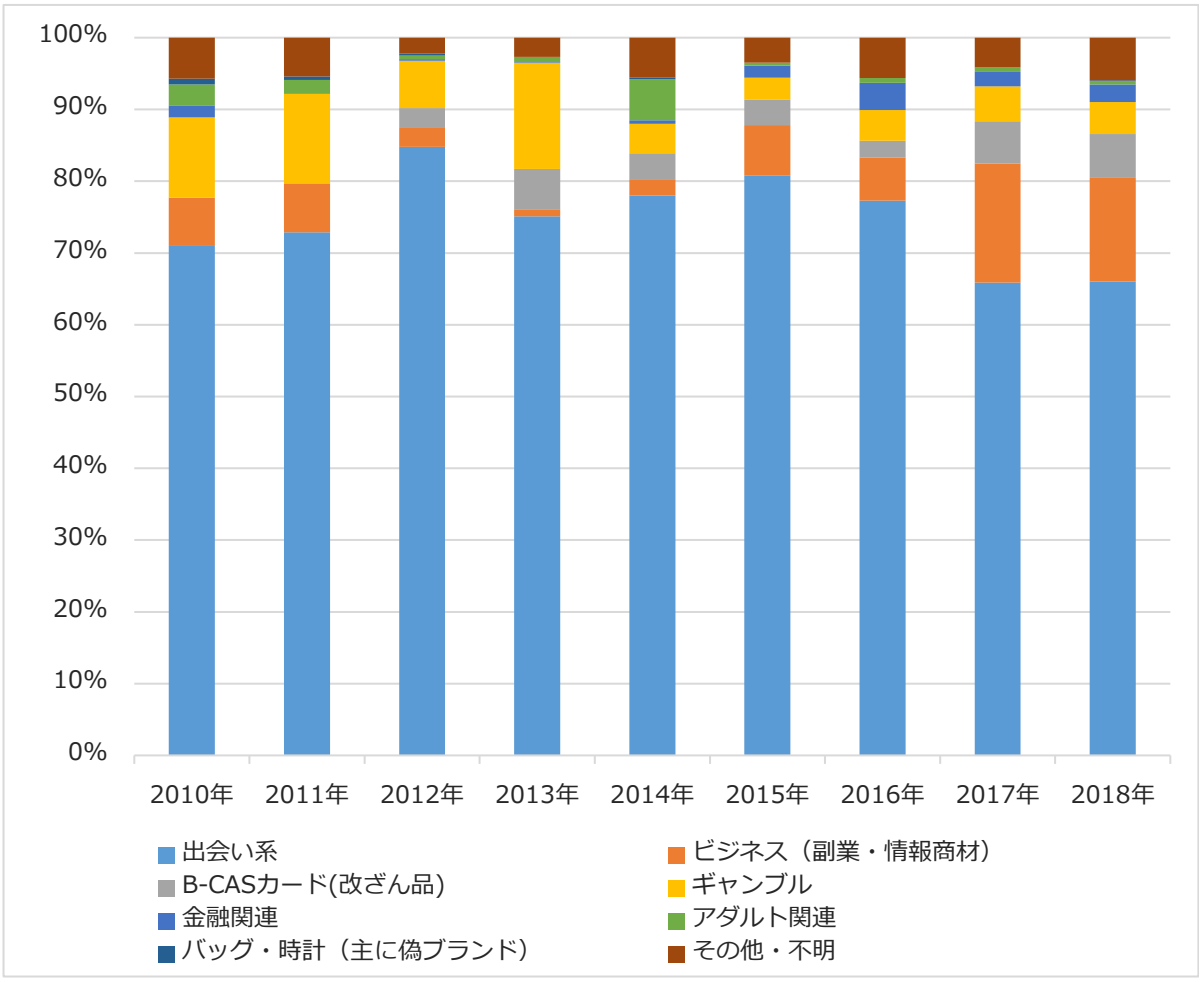
出典：（一財）日本データ通信協会 迷惑メール相談センター調べ（センターのモニター機で受信した情報を分析したもの）

4　迷惑メールの内容

国内着の迷惑メールの内容としては、「出会い系」サイトの広告・宣伝が多くを占める傾向が続いています。

(一財)日本産業協会が設置しているモニター機に着信した迷惑メールの内容としては、「出会い系」サイトの広告・宣伝が 2009 年の調査開始以来ほぼ一貫して 7 割～8 割を占めていましたが、2017 年は 65.9%となり、初めて 7 割を下回りました。2018 年についてもその傾向に変化はなく、66%となっています。その他については、「ギャンブル」に関するものが時期によっては 10%を超える割合になっていますが、2018 年については 4.4%となっています。また、情報商材をはじめとする「ビジネス」に関するものが、2017 年に初めて 10%を超え 16.6%と急増し、2018 年についても 14.4%と 10%を超える状況が続いています。

図表２－３－６　迷惑メールの内容

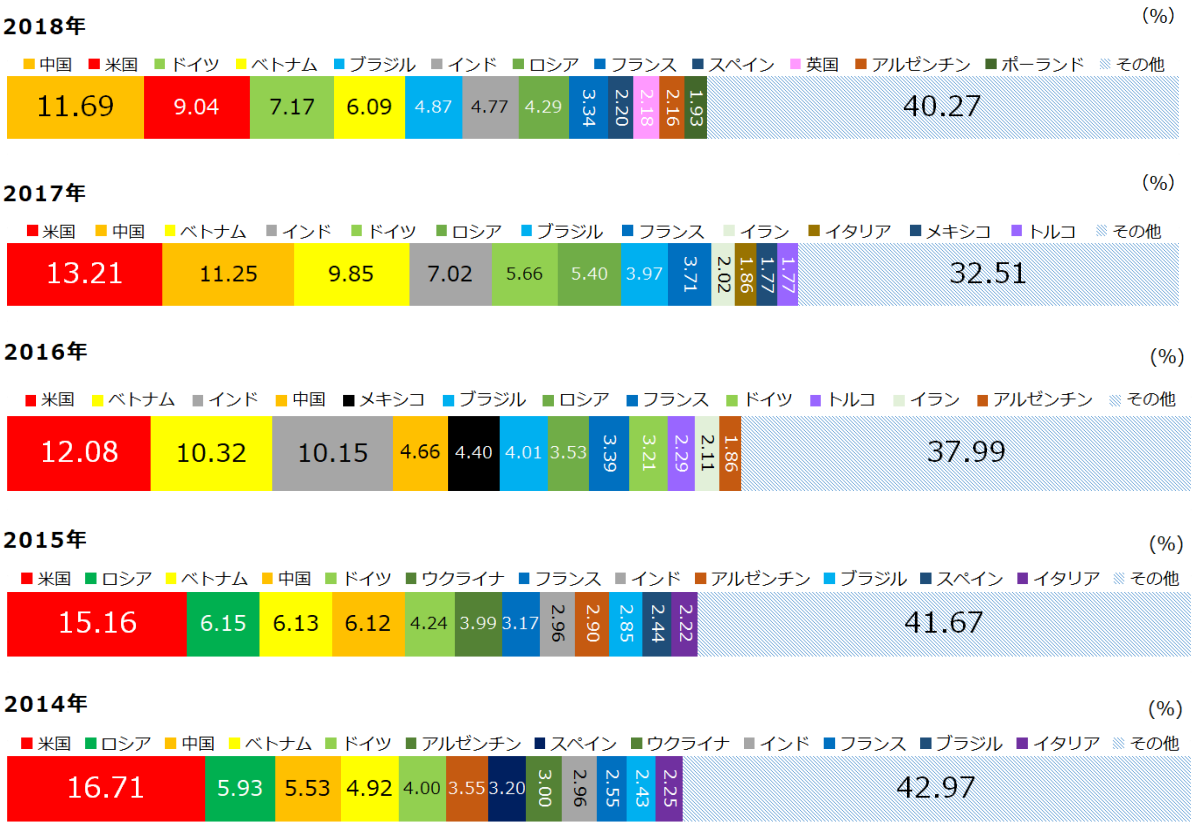


出典：(一財）日本産業協会が設置するモニター機で受信した迷惑メールおよび同協会に消費者からの申立として着信した迷惑メールのうち、日本語のサンプルデータを集計・分析したものを元に、迷惑メール対策推進協議会事務局が作成

5　世界全体の迷惑メール送信国・地域の傾向

世界全体の迷惑メールの送信国をみると、米国が一貫して高い比率を占めています。また、中国が 2017 年は２番目の比率でしたが、2018 年は米国と中国の順番が逆転しました。３項（迷惑メールの送信国・地域）で述べた国内着の迷惑メール送信国・地域の上位である米国、中国が、ここでも高い比率を占めているのがわかります。その他にも、ベトナムが高い比率を占めていることや、2018 年はドイツの占める比率が高くなっていることが判ります。

図表２－３－７　迷惑メール送信国・地域の傾向



出典：(株)カスペルスキー「Sources of Spam by Country」

第4節　迷惑メールの送信方法

迷惑メールを送信する者は、何らかの情報や利益を得るため、様々な方法で迷惑メールを送信します。例えば、個人情報や金銭を詐取しようとする場合は、受信者が疑念を抱かないように、実在する企業や取引先などの本来の送信者になりすます方法で迷惑メールを送信します。ここでは、送信先の選定から、送信元のメールサーバーをどのように確保して送信するかまで、悪質化・巧妙化する迷惑メールの送信方法を説明していきます。

1　送信先の選定

迷惑メールの送信者が送信先を選定する際の方法としては、主に大量送信型と標的型の２つがあります。

（１）大量送信型

大量の送信先を確保する方法として、以下があります。

（ア）　名簿業者からメールアドレスのリストを購入する

（イ）　ランダムにメールアドレスを作成して無差別にメールを送信し、反応があったアドレスをリスト化する

（ウ）　懸賞サイトなどの「おとりサイト」を作ってアドレスを登録させる

（エ）　インターネットに公開されているブログ掲示板などから収集する

その他にも、便利なアプリなどを装って不正アプリをインストールさせ、スマートフォン内の電話帳のデータを丸ごと詐取するような方法などもあります。

このような方法で取得した大量のアドレスに送信する手法は、迷惑メールの半数以上を占める「出会い系」サイトなどの広告・宣伝などに多く見られる手法です。

（２）標的型

特定の組織や個人に標的を絞って送信される迷惑メールは、何らかの方法で入手した組織や個人の情報をもとに、実際の業務内容などを詳細に調査、把握した上で、上司や取引先などになりすまして詐欺を行う場合や、ウイルスを含んだ添付ファイルを送り、情報を詐取する場合などに多く見られる手法です。

2　送信元の偽装

送信元を偽装する際の方法としては、送信元アドレスの偽装や、表示名（ディスプレイネーム）の偽装などがあります。

（1）送信元アドレスの偽装

Header-From は、送信者がどのような情報でも記載することが可能なことから、Header-From の電子メールアドレスに他者の電子メールアドレスを用いることにより、なりすましメールを送信する方法です。

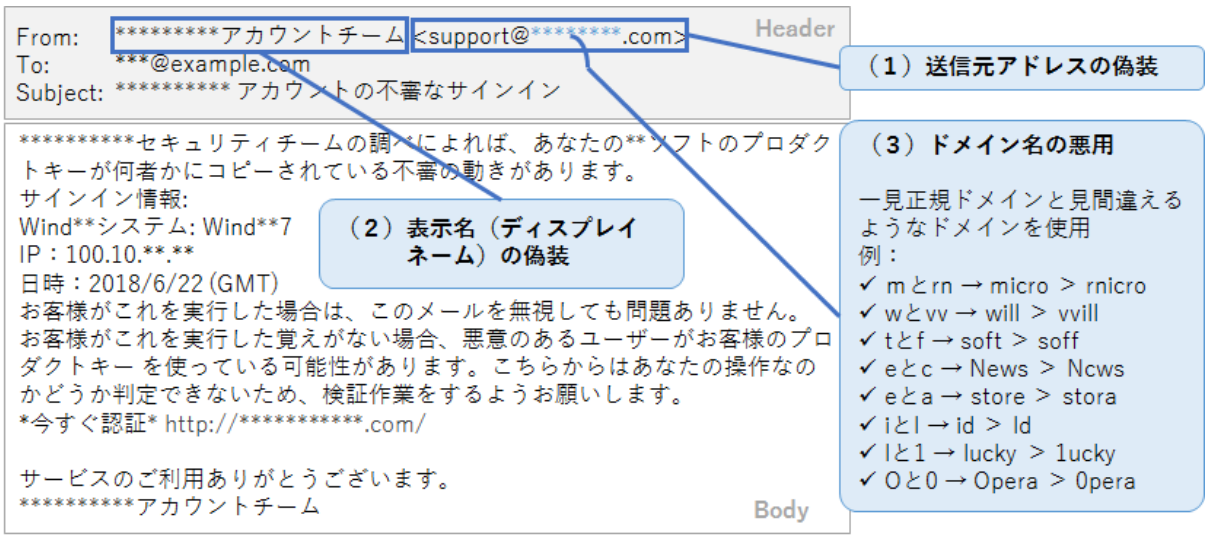
（2）表示名（ディスプレイネーム）の偽装

Header-From のうち、表示名（通常は個人名や法人名など）を偽って記述し、なりすましメールを送信する方法です。偽って記載する表示名には、他者の個人名などのほか、実際の送信元メールアドレスとは違う電子メールアドレスを用いることもあります。

（3）ドメイン名の悪用

本物の送信者のドメイン名と一見しただけでは誤解してしまう可能性のある類似したドメイン名（ホモグラフドメインやカズンドメインなどと呼ばれます）をあらかじめ取得し、なりすましメールを送信する方法です。この方法は、（1）および（2）とは異なり、送信元自体は正規のものですが、なりすまし先から送信されたものと誤解させるものです。

図表２－４－１　送信元の偽装



3　サーバーの不正利用

迷惑メールは、以前は、外部から匿名で利用可能なオープンリレーサーバー[注 47]を利用して送信されることが行われていましたが、不要なメール中継の制限などの不正中継対策が講じられるようになり、そのような方法で迷惑メールを送信することは難しくなっています。一方で、ウイルスに感染した大量のパソコンなどを用いたり、契約者情報を偽って取得した固定 IP アドレス[注 48]を用いたり、ISP の送信メールサーバーを不正に利用したりする事例が注目されていることから、ここではそれらの 3 つの方法について説明します。

（1）ボットネットの利用

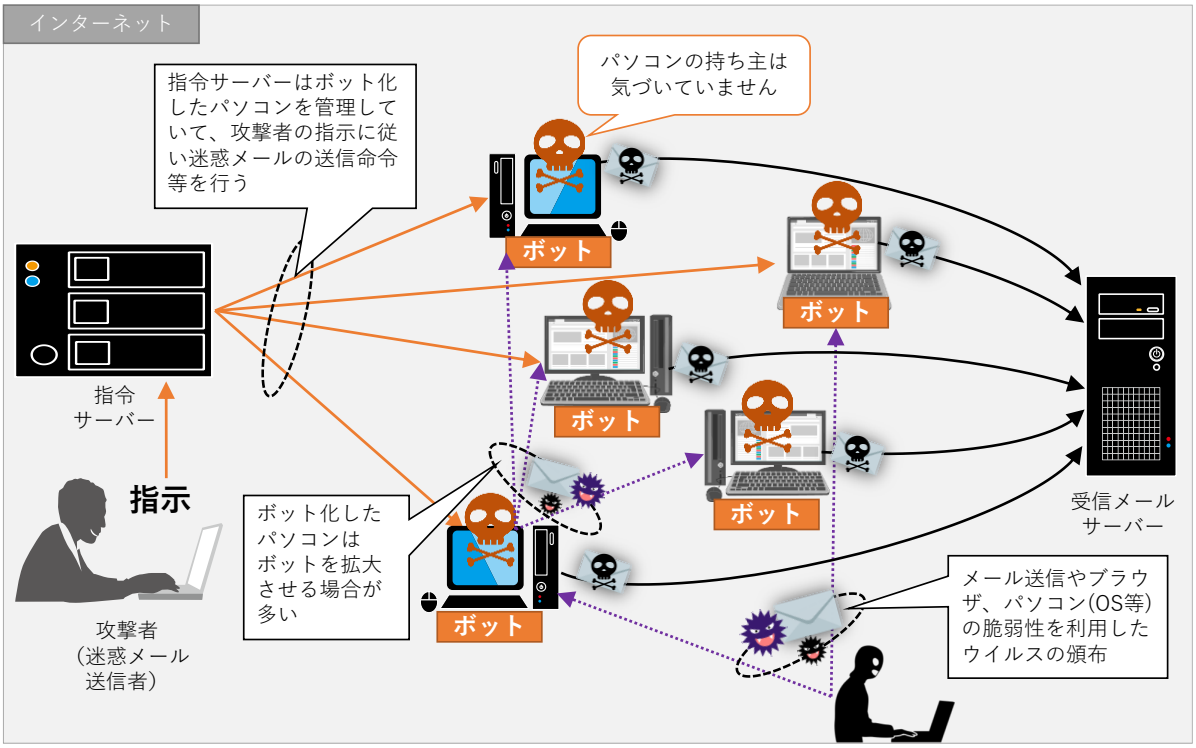
コンピューターウイルスのような悪意のあるソフトウェア（マルウェア[注 49]）を大量の一般の利用者のパソコンに感染させ、このマルウェアに感染したパソコンを外部から操作することによって、迷惑メールの送信などに利用する手法で、2002 年頃から使われるようになっています（マルウェアに感染したパソコンはロボットに擬して「ボット」と、ボットの集合は「ボットネット」と呼ばれています）。

ボットネットを利用した迷惑メールは、同一の送信元(IP アドレス)から少量ずつ送信されること、地理的に大規模に分散した送信元から送信されることなどの特徴があり、従来有効に機能していた迷惑メールの送信元を登録した DNSBL（DNS Black List/DNS Blackhole List）や、特定の送信元からの大量送信を検知して接続を制限する手法（スロットリング）が機能しない場合が出てきました。

ボットネットに対しては、ISP の正規のメールサーバーを介さない、電子メールの動的 IP アドレス[注 50]からの送信をブロックする OP25B [注 51]による対策が行われています。しかし、後述する（3）のようにボットが正規の利用者のパスワードなどを詐取し、その利用者を装って迷惑メールを送信する場合や、まだ OP25B を導入していない海外などの ISP を利用して迷惑メールを送信する場合など、対策には限界があるのが現状です。

注47 外部からのメール送信依頼を受け付け、メールの送信を行うサーバー
注48 常に同じ IP アドレスが割り当てられること
注49 「Malicious Software」（悪意のあるソフトウェア）の略で、様々な脆弱性や情報を利用して攻撃をするソフトウェアの総称
注50 接続のたびに異なる IP アドレスが割り当てられること
注51 第 3 章トピックス「OP25B(Outbound Port 25 Blocking)」（P67）参照

図表２－４－２　ボットネットのイメージ



（２）固定 IP アドレスの不正利用

契約者情報を偽って固定 IP アドレスの使用契約を ISP と締結し、迷惑メールを送信する手法です。固定 IP アドレスを使用した迷惑メールの送信では、ISP との契約が発生することから、送信元が特定可能であり、利用停止などの運用的な対処や法的対処が比較的容易ですが、契約者情報を偽って契約を締結することで、送信元の特定を困難にしています。

このような送信手法に対しては、ISP において契約時の確認を強化することにより対応をしています。しかし、複数の契約を締結することにより、大量の固定 IP アドレスを確保したり、迷惑メールの送信行為が判明して利用停止措置などを受けた場合に、すぐに新たな契約を締結して別の固定 IP アドレスを確保したりして、迷惑メールを送信する者も存在しているのが現状です。

（３）アカウントの不正利用

電子メールアカウントの ID、パスワードなどの情報を何らかの方法で入手し、利用者になりすまして電子メールアカウントを不正に利用して、迷惑メールを送信する手法です。実際に発生した事例においても、使われなくなったメールアカウントを削除し忘れたことや、パスワードが適切に設定されていなかったことなどから、電子メールアカウントが不正に利用され、大量の迷惑メールが送信されました。

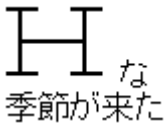
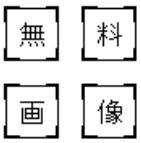
このような送信手法に対しては、利用者において適切な ID やパスワードの管理を行うこと、セキュリティ対策を行うことなどが重要になります。

４　その他（迷惑メールフィルターの回避）

多くの迷惑メールは、なんらかの広告・宣伝行為やホームページへの誘導、ウイルスの流布などが主目的であり、その内容には類似性があります。そこで、よく使われる文字列など迷惑メールの内容を統計的に処理して迷惑メールかどうかを判定する、迷惑メールフィルターが用いられるようになりました。

しかし、最近の迷惑メールは、迷惑メールフィルターを回避するため、ある文字について形状的に似た文字を使ってメッセージを伝える手法や、文字ではなく画像や PDF ファイルによってメッセージを伝える手法などが使われるようになりました。さらに、大量のドメインを取得して送信ごとにメールに掲載するドメインを変えたり、添付した画像データを簡単に同一の画像と判定されないように、個々に変化を持たせたりするなどの手法も用いられるようになってきています。

図表２－４－３　形状的に似た文字を使った例

（１）「0 円」を形状的に表した例	（２）「H」を形状的に表した例	（３）文字の周りを囲い、スペースも入れて 1 つの言葉としての連続性を分断した例	（４）文字の間にスペースを入れて 1 つの言葉としての連続性を分断した例
			

トピックス：SNS の悪用

スマートフォンの普及に伴い LINE、Facebook、Twitter などに代表される SNS（ソーシャルネットワークサービス）が、広く利用されるようになりました。

SNS は、電子メールと同様に 1 対 1 のメッセージ交換ができますが、グループを作ってメッセージを送信することにより、簡単にグループ内でメッセージ共有ができるなど、コミュニケーションツールとして優れた、とても便利なサービスです。

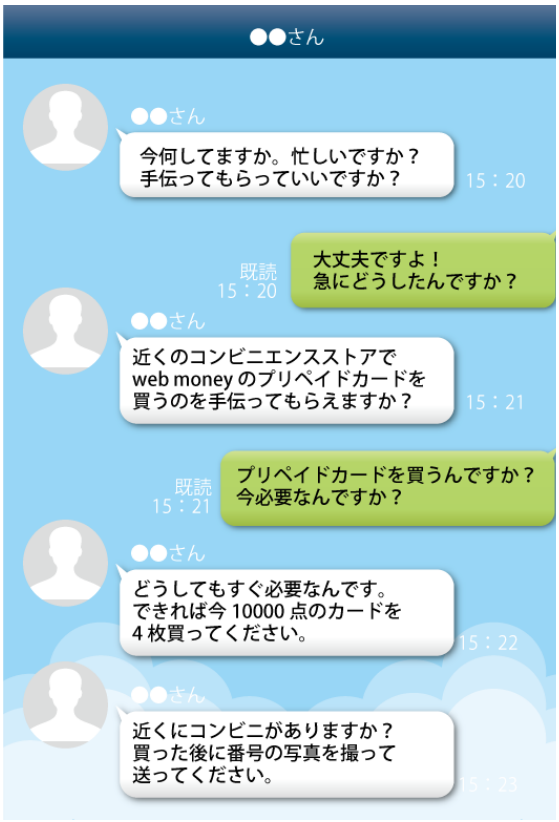
そして、SNS の利用者が増えてくると、知らないアカウントから「悪質サイトへの誘導」などの迷惑メッセージが SNS でも送られるようになりました。電子メール同様、SNS のメッセージを使った詐欺被害やマルウェア感染なども発生しています。

例えば、2014 年頃に知り合いになりすまして、プリペイドカードの金券番号をだまし取る詐欺の手口が広がりました。

その手口は、まず、なりすまし犯が SNS アカウントの ID などの脆弱性をつき、被害者の友人・知人のアカウントを乗っ取ります。その上で、そのアカウントの友人・知人へ「緊急で必要だからプリペイドカードを購入して番号を知らせて」とメッセージを送り、実際に知らせた番号を詐取するというものでした。全く知らない他人なら、怪しんだり、警戒したりしますが、友人・知人の名前で送られてきたメッセージを疑うことはなく、少し不審な内容でも信じて協力してしまったようです。

乗っ取られたアカウントからのメッセージを見破るのは難しいかも知れませんが、もし突然不審な内容のメッセージを受け取ったとしても、SNS でも電子メール同様に、なりすましその他の詐欺の手口があると知っていることで、被害にあう可能性を低くすることができます。

図表２－４－４　アカウント乗っ取り詐欺の手口のイメージ



SNS はインターネット上で様々な人と交流することができるツールですが、安全に利用するために、登録した個人情報や発言を「誰」に「どこまで」公開するかを任意に設定することができます。

また、SNS の中には、このような迷惑メッセージを受け取らないようにするために、あらかじめ見知らぬ人からのメッセージや友人申請を受け取らないように設定することもできます。利用に際しては、このような設定を事前にしておくことが大切です。

第３章

迷惑メール対策

第1節　制度的な対策

携帯電話による電子メールの急速な普及などに伴い、2001 年頃から、迷惑メールが大きな問題[注 52]となりました。このような状況を受け、2002 年に、特定電子メールの送信の適正化等に関する法律（特定電子メール法）が制定されるとともに、特定商取引に関する法律（特定商取引法）が改正され、迷惑メールへの制度的な対応がとられました。以来、複数の改正を経ながら、主にこれら二法によって迷惑メール対策が実施されています。なお、架空請求メールの送信が、刑法に規定する詐欺罪や、その未遂罪に該当する場合があるなど、迷惑メールの送信が、これら二法以外の法律による規制対象となることもあります。

図表３－１－１　特定電子メール法と特定商取引法との比較

項目	特定電子メール法	特定商取引法
目的	電子メールの送受信上の支障の防止の観点から送信を規制	消費者保護と取引の公正の観点から広告を規制
規制対象	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送信する電子メールなど	通信販売などの電子メール広告
規制対象者	送信者及び送信委託者	販売事業者など及び電子メール広告受託事業者
オプトイン規制	あらかじめ同意した者など以外に広告宣伝メールを送信することを禁止、同意を証する記録の保存義務、受信拒否者への再送信禁止、表示義務	あらかじめ承諾した者など以外に電子メール、広告をすることを禁止（直接罰[注 53]）、請求・承諾の保存義務（直接罰）、受信拒否者への電子メール広告の禁止（直接罰）、表示義務（直接罰）
架空電子メールアドレスを宛先とした電子メール	架空電子メールアドレスを宛先とする送信の禁止	（規定なし）
送信者情報を偽装した電子メール	送信者情報を偽った送信の禁止（直接罰）	（規定なし）
電気通信事業者などへの情報提供の求め	総務大臣は、電子メールアドレスなどの契約者情報を保有する電気通信事業者などに対し当該契約者情報の提供を求めることができる。	主務大臣は、電子メールアドレスなどの契約者情報を保有する電気通信事業者などに対し当該契約者情報の提供を求めることができる。
主務大臣	内閣総理大臣及び総務大臣 ※内閣総理大臣の権限は一部を除いて消費者庁長官に委任されている。	内閣総理大臣、経済産業大臣及び事業等所管大臣 ※電子メール広告受託事業者に関する事項については、内閣総理大臣及び経済産業大臣が主務大臣とされている。なお、内閣総理大臣の権限は一部を除いて消費者庁長官に委任され、さらに、消費者庁長官に委任された権限の一部は経済産業局長に委任されている。

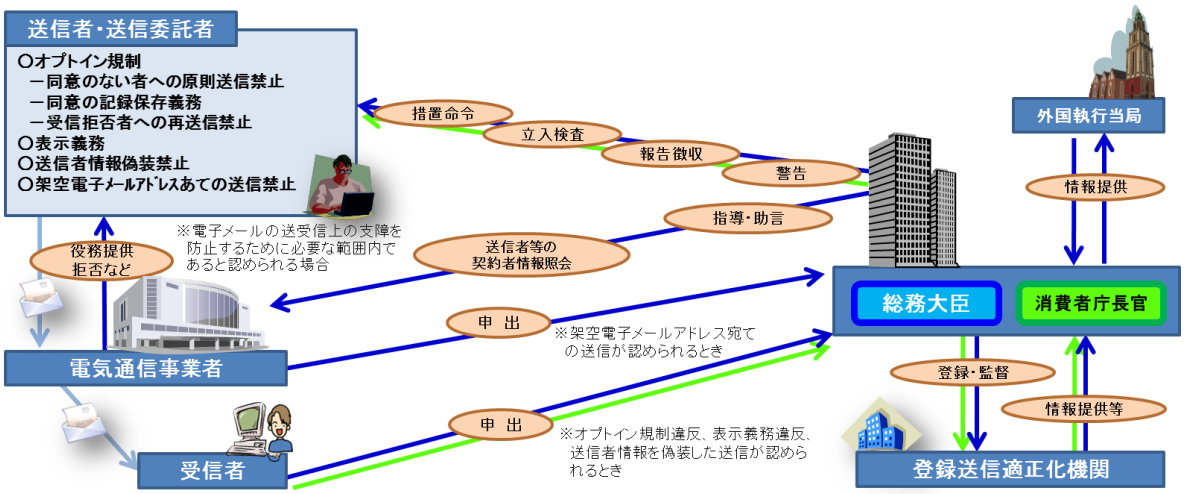
注52 総務省「迷惑メールへの対応の在り方に関する研究会　中間取りまとめ」(2002 年 1 月 24 日)
http://warp.da.ndl.go.jp/info:ndljp/pid/235321/www.soumu.go.jp/s-news/2002/020124_4.html

注53 違法行為に対して（行政指導や行政処分を課すことなく）即時に適用される刑事罰を直接罰という。一方、違法行為に対して行政指導や行政処分（例えば、措置命令）後、その指導や処分に違反する行為があった場合に、それを理由に適用される刑事罰を間接罰という。

１　特定電子メール法

特定電子メール法は、電子メールの送受信上の支障（受信者や電気通信事業者における支障）を防止する観点から、電子メールの送信について規制を行う法律です。規制の対象となる電子メールは、主として、広告宣伝を行うための電子メールであり、そのような電子メールの送信者や送信委託者に対する義務などが規定されています。

図表３－１－２　特定電子メール法の概要

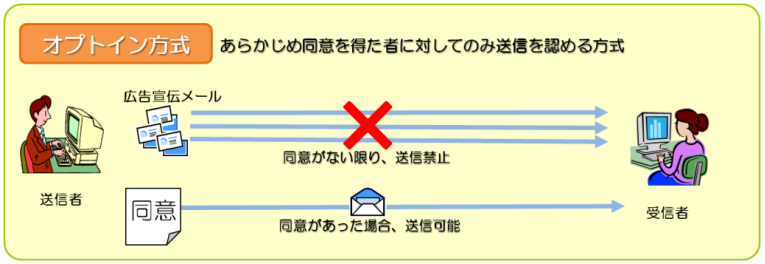


（１）電子メールの送信者に対する規制

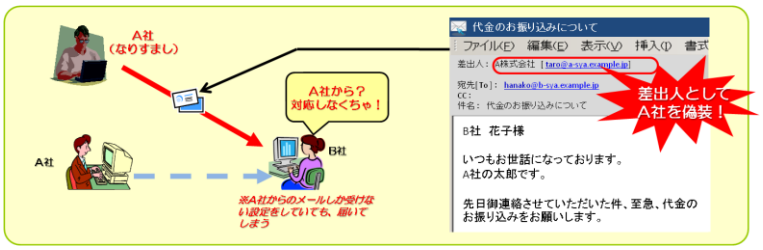
原則として、受信者の同意を得ない広告宣伝メールの送信が禁止されています（オプトイン方式による規制）。同意を得て広告宣伝メールを送信する場合であっても、受信拒否の通知先など一定の事項を電子メールの本文などに表示する義務が課されているほか、受信者から受信拒否の通知を受けた場合に、その受信者への以後の送信が禁止されています。

また、迷惑メールの中には、ヘッダーFrom を偽って送信し、電子メールの送信元を突き止めにくくしているものがありますが、広告宣伝メールの送信に当たっては、このような、送信者情報の偽装が禁止されています（送信者情報を偽った送信の禁止）。さらに、プログラムを用いて自動的に大量に生成した電子メールアドレス（架空電子メールアドレス）宛てに送信することは、迷惑メールの送信を助長するだけでなく、大量のエラーメールを発生させ、電気通信事業者のメール配送設備に多大な負荷をかけることから、禁止されています。

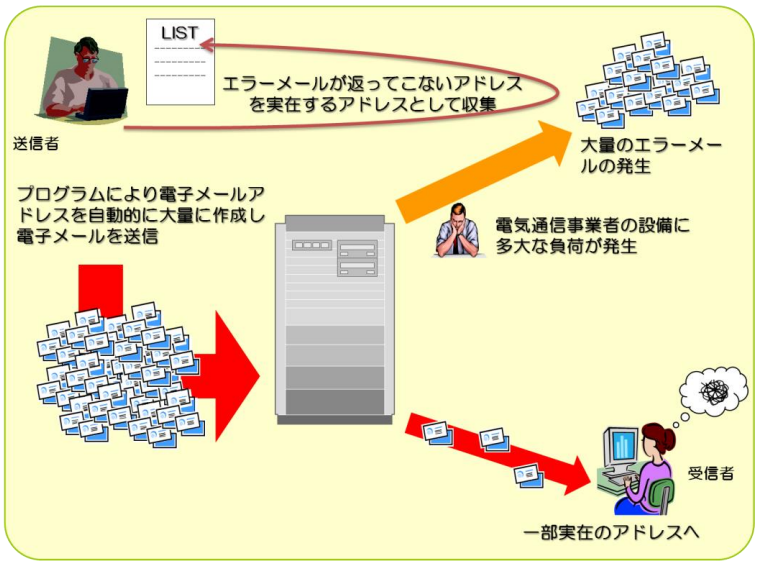
図表３－１－３　オプトイン方式



図表３－１－４　送信者情報の偽装の例



図表３－１－５　架空電子メールアドレス宛の送信



（２）電子メールの送信を委託している者に対する規制

電子メールの送信を委託した者（送信委託者）に対しても一定の規制が課されています。例えば、送信委託者が特定電子メール法に違反する広告宣伝メールの送信に責任を有している場合には、送信委託者が行政処分の対象となることがあります。

（３）電気通信事業者に関する規定

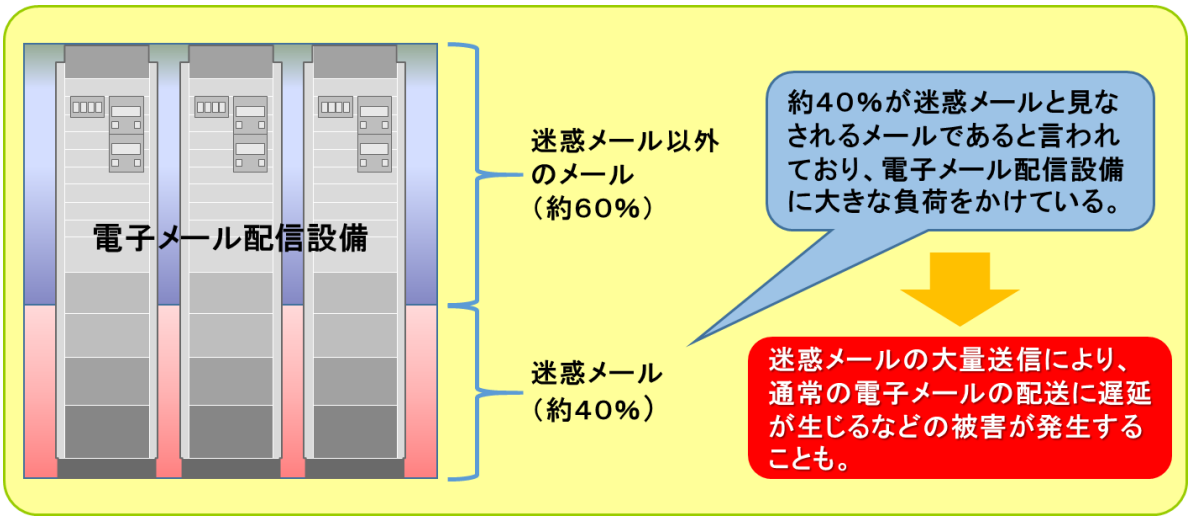
電子メールの大量送信は、電気通信事業者のメール配送設備に負荷を生じさせます。また、これにより、通常の電子メールの配送が遅延するなどの被害が生じることがあります。

総務大臣による認定を受けた電気通信事業者は、電気通信事業法によって、正当な理由のないサービスの提供拒否が禁じられており[注 54]、利用者に対して公平にサービスを提供する義務を負っています[注 55]。また、通信の発信元などに応じて差別的な取扱いを行うことには、通信の秘密[注 56]の観点からも問題が生じ得ます。

注54 電気通信事業法第 121 条
注55 電気通信事業法第６条
注56 電気通信事業法第４条

このため、迷惑メールを送信していると思われる送信者に対しても、電子メールサービスの提供を拒否することは、原則として認められません。しかし、一定の要件に該当する場合には、この限りではなく、特定電子メール法においては、例外的にサービスの提供を拒否することができる場合を規定しています。例えば、大量の迷惑メールによって通常のサービスの提供に支障が出るおそれがある場合には、このような悪質な大量送信者に対してサービスの提供を拒否することができます。

図表３－１－６　電子メールの配送を行う設備への負荷



（４）法の実効性の確保

総務大臣や消費者庁長官は、特定電子メール法違反が疑われる送信者などに対する報告の求め（報告徴収）や立入検査を行うことができ[注 57]、さらに、違反した送信者などには、一定の条件下で、行政処分（措置命令）により、電子メールの送信の方法の改善に関し必要な措置を命ずることができます[注 58]。なお、措置命令に違反した者や送信者情報を偽って特定電子メールを送信した者には刑事罰が科される場合があります[注 59]。また、総務大臣は、電子メールアドレスや IP アドレスなどの契約者情報を保有する電気通信事業者などに対し、迷惑メールの送信者などの契約者情報の照会を行うことができます[注 60]。

（５）国際連携に関する規定

外国から送信される迷惑メールに対応するため、総務省と外国執行当局との連携に関する規定が設けられています[注 61]。

注57 特定電子メール法第 28 条
注58 特定電子メール法第７条
注59 特定電子メール法第 34 条、第 35 条
注60 特定電子メール法第 29 条
注61 特定電子メール法第 30 条

トピックス：特定電子メール法の沿革

（１）法律の制定（2002 年）－オプトアウト方式による規制の導入

携帯電話宛ての迷惑メールが社会問題となったことなどを受けて、2002 年に特定電子メール法が制定されました。

受信者から受信拒否の通知があった場合に広告宣伝メールの送信が原則として禁止される「オプトアウト方式」の規制が導入され、広告宣伝メールの送信に当たっては、標題部に「未承諾広告※」と表示するなどの表示義務が課されました。また、架空電子メールアドレスを宛先とする送信が禁止されたほか、電気通信事業者がサービスの提供を拒否できる場合についての規定が設けられました。

（２）法律の改正（2005 年）－送信者情報を偽った送信の禁止など

迷惑メール送信の悪質化・巧妙化に対応するため、2005 年に法律の改正が行われました。この改正により、送信者情報を偽った送信が禁止され、これに違反した場合は直接罰（１年以下の懲役又は 100 万円以下の罰金）が科されることとされました。また、規制対象が、私用の電子メールアドレスだけでなく、事業用のメールアドレスにも拡大されたほか、広告宣伝メール以外の電子メールについても、架空電子メールアドレス宛ての送信が禁止され、規制範囲が拡大されました。措置命令に違反した場合の罰則も強化されています（50 万円以下の罰金から、１年以下の懲役又は 100 万円以下の罰金に。）。

（３）法律の改正（2008 年）－オプトイン方式による規制の導入など

依然として巧妙化・悪質化する迷惑メールや、外国から送信される迷惑メールに対応するため、2008 年に法律の改正が行われました。この改正により、オプトイン方式による規制が導入されたほか、法の実効性の強化や、外国から送信される迷惑メールへの対策強化が図られています。それぞれの概要は以下のとおりです。

オプトイン方式による規制の導入

- 取引関係にある者への送信など一定の場合を除き、受信者の同意なく広告宣伝メールを送信することが禁止されました。
- 受信者の同意を証する記録の保存が義務づけられました。
- 表示義務がオプトイン方式による規制に対応したものとなりました。

※　改正前は、受信者の承諾を得ることなく送信する広告宣伝メールを特定電子メールと定義し、表示義務や、受信拒否の通知を受けた後の再送信の禁止が課されていました。2008 年改正により、広告宣伝メール全般を特定電子メールと定義し、同意のない送信が原則禁止されるとともに、同意を得ての送信や、同意を得ずに例外的に送信できる場合（取引関係にある者に送信する場合など）についても、表示義務が課され、受信拒否の通知を受けた後の再送信が禁止されるなど、規制の範囲が拡大されました。

法の実効性の強化

- 法人に対する罰金額の上限が 100 万円以下から 3,000 万円以下に引き上げられるなど、罰則が強化されました。
- 総務大臣が、電気通信事業者などに対し、電子メールアドレス、IP アドレス、ドメイン名などの契約者情報の提供を求めることが可能になりました。
- 電子メールの送信を委託した者（送信委託者）に対して措置命令などを行えるようになりました。

外国から送信される迷惑メールへの対応強化

- 総務大臣が、外国の迷惑メール対策法令の執行当局に対して、職務の遂行に有用であると認められる情報を提供できるようになりました。
- 送信委託者（海外に送信を委託した者を含みます。）に対して措置命令などを行えるようになりました。

（４）法律の改正（2009 年）－消費者庁と共同所管に

内閣府の外局として消費者庁が創設されるにあたり、消費者庁が必要な措置を講じることができるよう法律が改正されました。これにより、主務大臣に内閣総理大臣が追加され、その権限を委任された消費者庁長官が、行政処分、報告徴収、職員による立入検査などを行うことが可能となりました。主な改正点は以下のとおりです。

- 特定電子メール法に基づく措置命令を、総務大臣と消費者庁長官が共同で行うこととなりました。ただし、架空電子メールアドレスを宛先とする送信に関する措置命令は、通信ネットワーク環境の整備の観点から行われることから、引き続き、総務大臣が単独で実施することとなりました。
- 総務大臣に加えて、消費者庁長官が、広告宣伝メールなどの送信者又は送信委託者に対し、報告徴収や、職員による立入検査を行うことが可能になりました。
- 特定電子メール法に違反する電子メールを受信した者が、総務大臣だけでなく、消費者庁長官に対しても、適当な措置をとるべきことを申し出ることが可能になりました。
- 特定電子メール法に基づく登録送信適正化機関（特定電子メール法の円滑な執行を支援するための登録機関）の監督などを、総務大臣が内閣総理大臣と共同で行うことになりました。

（５）ガイドラインの改正（2011 年）

特定電子メール法の 2008 年改正法の附則で、政府は施行後 3 年以内に法の施行状況について検討を加え、その結果に基づき、必要な措置を講ずる旨が規定されていることなどを踏まえ、「利用者視点を踏まえた ICT サービスに係る諸問題に関する研究会[注 62]」において、2010 年 9 月から「迷惑メールへの対応の在り方に関する WG」を設置しました。電気通信事業者、消費者団体、学識経験者など、幅広い関係者の参画のもと、今後の迷惑メール対策の在り方について検討を行い、2011 年 7 月、制度面について、現時点では、特定電子メール法の更なる改正が必要な状況ではないが、現行の制度に基づき法執行の強化が必要であることや、法の運用が適切に行われるようにするため、簡便なオプトアウト方法を明記するなど、ガイドラインの改正を検討すべきことなどを提言としてとりまとめました[注 63]。

これを受けて、2011 年 8 月、「特定電子メールの送信等に関するガイドライン」を改正し[注 64]、デフォルトオンで同意を取得する際の注意事項の明記や簡便なオプトアウト方法の推奨などの明記、具体的な画面例の追加などを行いました。

注62 総務省「利用者視点を踏まえた ICT サービスに係る諸問題に関する研究会」
http://www.soumu.go.jp/menu_sosiki/kenkyu/11454.html

注63 総務省「「利用者視点を踏まえた ICT サービスに係る諸問題に関する研究会」、「プロバイダ責任制限法検証に関する提言」および「迷惑メールへの対応の在り方に関する提言」の公表」（2011 年 7 月 21 日）
http://www.soumu.go.jp/menu_news/s-news/01kiban08_01000037.html

注64 総務省「特定電子メールの送信等に関するガイドラインの改正の公表及び改正案に対する意見募集の結果」（2011 年 8 月 31 日）
http://www.soumu.go.jp/menu_news/s-news/01kiban08_01000045.html

トピックス：現行の特定電子メール法の詳細

（1）法律の目的

電子メールの送受信上の支障を防止し、電子メールを利用することによる効用を十分に享受できる環境を整備する観点から、広告宣伝メールの送信についての規制などが行われています。

（2）規制の対象となる電子メール

主として、広告宣伝を目的とする電子メール（SMTP を用いたもののほか、携帯して使用する通信端末機器（携帯電話、スマートフォン、タブレット端末など）同士でメッセージを電話番号により送受信するサービス（例えば、SMS）も含む。）が規制の対象です。

（3）規制などの対象となる者

- 電子メールの送信者及び送信委託者が規制の対象です。また、電気通信事業者に関する規定や、特定電子メール法の執行などに資する業務を行う登録送信適正化機関に関する規定も整備されています。

（4）オプトイン方式による規制（送信者・送信委託者への規制）

- 送信禁止
  取引関係にある者への送信など一定の例外を除いて、受信者の同意を得ることなく広告宣伝メールを送信することが禁止されています。
- 同意を証する記録の保存義務
  広告宣伝メールの送信に当たって、受信者の同意を証する記録を保存することが義務づけられています。
- 再送信禁止
  受信者から、広告宣伝メールの受信を拒否する旨の通知を受けた場合は、その受信者に対する以後の送信が禁止されています。
- 表示義務
  広告宣伝メールの送信に当たって、受信拒否の通知先など一定の事項を表示することが義務づけられています。

（5）送信者情報を偽った送信の禁止（送信者への規制）

送信者情報（メールヘッダーに表示される電子メールアドレスや送信元の IP アドレスなど）を偽って広告宣伝メールを送ることが禁止されています。

（6）架空電子メールアドレス宛ての送信の禁止（送信者への規制）

架空電子メールアドレス宛てに送信することが禁止されています。

（７）電気通信事業者に関する規定

- 電子メールサービスの提供者によるサービスの提供拒否
  電子メールサービスを提供する電気通信事業者は、特定電子メール法に違反する電子メールの大量送信などにより、電子メールサービスの円滑な提供に支障が出るおそれがある場合は、必要な範囲で、そのような電子メールの送信についてサービスの提供を拒否することができます。
- 電気通信事業者による情報の提供・技術の開発
  電気通信事業者は、利用者に対し、広告宣伝メールなどによる電子メールの送受信上の支障を防止するためのサービスの情報提供や、技術の開発・導入に努めることとされています。
- 電気通信事業者の団体に対する指導・助言
  総務大臣は、電気通信事業者の団体に対し、広告宣伝メールなどによる電子メールの送受信上の支障の防止に関して、指導・助言を行うように努めるものとされています。
- 総務大臣による研究開発などの状況の公表
  総務大臣は、広告宣伝メールなどによる電子メールの送受信上の支障の防止に資する技術の研究開発の状況や、電気通信事業者におけるその導入状況を、少なくとも年１回公表することとされています。

（８）総務大臣又は消費者庁長官に対する申出

広告宣伝メールの受信者は、（４）～（６）の規制に違反する送信があると認めるときは、総務大臣又は消費者庁長官に対し、適当な措置をとるべきことを申し出ることができます。また、電子メールサービスを提供する者は、（６）の規制に違反する送信があると認めるときは、総務大臣に対し、必要な措置をとるべきことを申し出ることができます。総務大臣や消費者庁長官は、このような申出があった場合は、必要な調査を行わなければなりません。また、調査結果に基づき必要があると認めるときは、特定電子メール法に基づく措置など適当な措置をとらなければなりません。

（９）登録送信適正化機関

総務大臣や消費者庁長官に対する（８）の申出を円滑に行うことができるようにするなど、特定電子メール法の執行を支援するため、同法には、総務大臣及び内閣総理大臣による登録機関（登録送信適正化機関）に関する規定が設けられており、総務大臣及び内閣総理大臣は、登録送信適正化機関に以下の業務を行わせることができます。

- 総務大臣又は消費者庁長官に対する申出をしようとする者に対する指導・助言
- 申出を受けての調査
- 広告宣伝メールに関する情報収集など

（10）法律違反があった場合の措置など

- 報告徴収、立入検査
  総務大臣又は消費者庁長官は、特定電子メール法の施行のために、広告宣伝メールの送信者又は送信委託者に対し、必要な報告をさせることができるほか、職員による立入検査を行うことができます。報告徴収があった場合に報告をしなかった場合・虚偽の報告をした場合や、立入検査を拒んだ場合は刑事罰の対象となります。
- 行政処分（措置命令）
  総務大臣及び消費者庁長官は、以下の場合において、電子メールの送受信上の支障を防止するため必要があると認めるときは、送信者に対し、行政処分（措置命令）を行うことができます。また、送信委託者が同意の取得を行っている場合など、電子メールの送信について送信委託者に一定の責任がある場合には、送信者に加えて送信委託者に対しても措置命令を行うことができます。なお、措置命令に違反した場合は刑事罰の対象となります。
  - オプトイン方式による規制を遵守していないと認める場合
  - 送信者情報を偽った電子メールの送信をしたと認める場合
  - 架空電子メールアドレスを宛先とする電子メールの送信をしたと認める場合

  ※措置命令は、総務大臣と消費者庁長官が共同で行います（ただし、架空電子メールアドレスを宛先とする送信についての措置命令は、総務大臣が単独で行います。）。

- 刑事罰措置命令に違反した場合や、送信者情報を偽って広告宣伝メールを送信した場合は、刑事罰の対象となります。

図表３－１－７　特定電子メール法の主要な罰則

違反事項	罰則
送信者情報を偽った送信	１年以下の懲役又は 100 万円以下の罰金（法人の場合は行為者を罰するほか、法人に対して 3,000 万円以下の罰金）。 ※行政処分（措置命令）の対象ともなる。
架空電子メールアドレスあての送信（電子メールの送受信上の支障を防止する必要があると総務大臣が認めるとき）	行政処分（措置命令）。 措置命令に従わない場合、１年以下の懲役又は 100 万円以下の罰金（法人の場合は行為者を罰するほか、法人に対して 3,000 万円以下の罰金）。
同意のない者への送信	
受信拒否者への送信	
表示義務違反	
同意を証する記録の保存義務違反	行政処分（措置命令）。 措置命令に従わない場合、100 万円以下の罰金（法人の場合は行為者を罰するほか、法人に対して 100 万円以下の罰金）。
報告徴収を受けた場合の報告の懈怠 立入検査に際しての検査忌避	100 万円以下の罰金

- 電気通信事業者などへの情報提供の求め
  総務大臣は、特定電子メール法の施行のために、電気通信事業者などに対し、電子メールアドレス、IP アドレス、ドメイン名などの契約者情報の提供を求めることができます。これにより得られた情報は、迷惑メール送信者の特定に役立てられます。
- 外国執行当局への情報提供
  総務大臣は、外国の迷惑メール対策法令の執行当局に対して、職務の遂行に有用であると認める情報を提供できます。例えば、外国からの迷惑メールの送信において、当該国の執行当局に対して、送信者についての情報提供を行い、措置を要請できる場合もあります。

（11）省令・ガイドライン

特定電子メール法の運用に当たっての詳細な事項は、以下の省令によって定められています。

- 特定電子メールの送信の適正化等に関する法律施行規則
  オプトイン方式による規制の例外、同意を証する記録として保存すべき事項・保存すべき期間、表示が義務づけられる事項の詳細などが規定されています。
- 特定電子メールの送信の適正化等に関する法律第二条第一号の通信方式を定める省令
  特定電子メール法の規律の対象となる電子メールの通信方式が規定されています。
- 特定電子メールの送信等に関するガイドライン
  法律及び施行規則の解釈を明確化するとともに、広告宣伝メールの送信に当たって推奨される事項を示すため、「特定電子メールの送信等に関するガイドライン」が定められています。

（12）主務大臣

内閣総理大臣、総務大臣が、主務大臣とされています。なお、内閣総理大臣の権限は、一部を除いて[注 65]消費者庁長官に委任されています。

[注65] 特定電子メールの送信の適正化等に関する法律第三十一条第一項の規定により消費者庁長官に委任されない権限を定める政令

２　特定商取引法

特定商取引法は、消費者保護と取引の公正の観点から、取引の形態などの規制を行う法律であり、通信販売などに係る電子メール広告も規制の対象とされています。

電子メール広告を送信する事業者などに対する規制

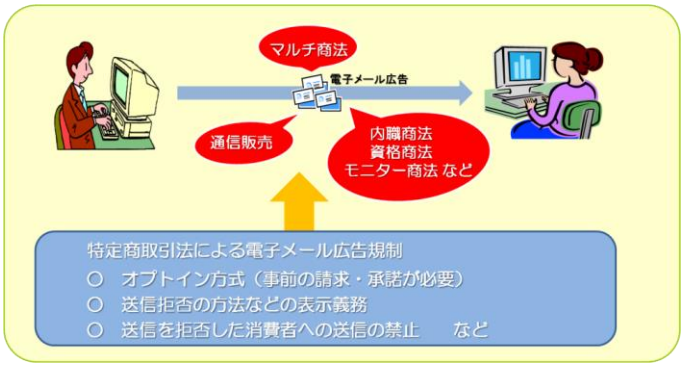
特定商取引法においては、通信販売、連鎖販売取引（いわゆるマルチ商法）、業務提供誘引販売取引（いわゆる内職商法、資格商法、モニター商法など）の形態で消費者と取引をする場合において、事業者が、取引の対象となる商品や役務などについて電子メールにより広告をする場合には、オプトイン方式による規制が課されます。すなわち、事業者が消費者に対してこれらの電子メール広告を行うに当たっては、原則として消費者による事前の請求又は承諾が必要です。また、請求・承諾を得て電子メール広告を行う場合であっても、電子メール広告の送信を拒否する方法など一定の事項を表示する義務が課されているほか、電子メール広告の送信を拒否した消費者への送信が禁止されています。

電子メール広告に関する業務を受託している者に対する規制

販売業者などから電子メール広告に関する以下の業務を一括して受託している場合には、販売業者などに課されている義務が受託事業者に課されます。

- 消費者から電子メール広告送付についての請求を受け、又は承諾を得る業務
- 消費者からの請求や承諾の記録を作成し、保存する業務
- 送信する電子メール広告に、消費者が受信拒否の意思を表示するための方法や連絡先などを表示する業務

図表３－１－８　特定商取引法による電子メール広告の規制



法の実効性の確保

法律違反者については、主務大臣による行政処分（指示又は業務停止命令等）の対象となる[注66]ほか、刑事罰の対象となります。また、主務大臣は、法律違反が疑われる販売業者等に対して報告徴収や立入検査等を実施できる[注67]ほか販売業者等と取引をする者（電気通信事業者等）に対して報告徴収等を行うことができます[注68]。

注66 特定商取引法第 14 条、第 15 条など
注67 特定商取引法第 66 条第１項
注68 特定商取引法第 66 条第３項

トピックス：特定商取引法による電子メール広告規制の沿革

（1）特定商取引法施行規則の改正（2002 年）－表示義務の導入

通信販売業者等が電子メール広告を送る際に、従来表示が義務づけられていた事項に加えて、表題部に「！広告！」と表示するなどの義務が課されました。

（2）法律の改正（2002 年）－オプトアウト方式による規制の導入

迷惑メールに対して十分な対応を行うため、消費者から電子メール広告の受取拒否があった場合に、その消費者に対する再度の電子メール広告の送信が禁止されることとなりました。あわせて、消費者が通信販売業者などに対して電子メール広告を拒否する方法を表示することが義務づけられました。また、施行規則の改正により、請求又は承諾を得ずに電子メール広告を送る場合には、表題部に「未承諾広告※」と表示することが義務づけられました。

（3）法律の改正（2008 年）－オプトイン方式による規制の導入など

2002 年の法律の改正以降も、迷惑な電子メール広告に関する苦情の件数は増加しており、表示義務違反や誇大広告のみならず、消費者が望まない取引に気づかずに誘引されるという問題が生じていました。この状況に有効に対処し、消費者が望まない取引に気づかずに誘引されることを防止するため、2008 年 6 月に法律が改正され、オプトイン方式による規制が導入されました（同年 12 月 1 日施行）。改正の概要は以下のとおりです。

オプトイン方式による規制の導入

- 通信販売事業者等が消費者からの請求又は承諾を得ずに電子メール広告を送ることが原則として禁止されました。消費者から電子メール広告を受けない旨の意思表示を受けたときは、その消費者に対する以後の送信が禁止されています。
- 消費者からの請求や承諾を証する記録の保存が義務づけられました。
- 表示義務がオプトイン方式による規制に対応したものとなりました。
  以下の行為を行った販売業者等に対し、行政処分（指示）を行うことができる旨規定されました。
  - 消費者に分かりにくい形で、電子メール広告を行うことについての請求・承諾を得ようとする行為
  - オプトイン方式の規制に違反している者に、以下の業務を一括して委託する行為
    - 消費者から電子メール広告送付についての請求や承諾を得る業務
    - 消費者からの請求や承諾の記録を作成し、保存する業務
    - 送信する電子メール広告に、消費者が受信拒否の意思を表示するための方法や連絡先などを表示する業務

規制対象となる電子メール広告の範囲の拡大

- 連鎖販売取引（マルチ商法）、業務提供誘引販売取引（内職商法など）に係る電子メール広告の送信についても、オプトイン方式による規制が導入されました。
- 請求・承諾のない電子メール広告の送信が原則禁止されるとともに、請求・承諾を得ての送信や、請求・承諾を得ずに例外的に送信できる場合についても、表示義務や受信拒否の通知を受けた後の再送信の禁止などが課されることとなり、規制の範囲が拡大されました。

法の実効性の強化

- 以下の業務を一括して受託している事業者に対して、オプトイン方式による規制が適用されることとされました。
  - 消費者から電子メール広告送付についての請求や承諾を得る業務
  - 消費者からの請求や承諾の記録を作成し、保存する業務
  - 送信する電子メール広告に、消費者が受信拒否の意思を表示するための方法や連絡先などを表示する業務
- 主務大臣が、電子メールアドレス、IP アドレス、ドメイン名などの契約者情報を保有する電気通信事業者などに対して、契約者情報の提供を求めることが可能となりました。
- 主務大臣が、販売業者等と取引する者に対し、販売業者等の業務や財産に関して参考となるべき報告や資料の提出を命ずることができるようになりました。
- オプトイン方式による規制への違反者に対して直接罰が科されるなど、罰則が強化されました。

（４）法律の改正（2009 年 9 月）－消費者庁と共同所管に

内閣府の外局として消費者庁が創設されるにあたり、電子メール広告に関し、消費者庁が必要な措置を講じることができるよう法律が改正されました。これにより、電子メール広告規制に係る事項の主務大臣に内閣総理大臣が追加され、その権限を委任された消費者庁長官及び経済産業局長が、行政処分、報告徴収、職員による立入検査、プロバイダ等への契約者情報の照会、販売業者等と取引する者への報告命令などを行うことが可能となりました。

（５）法律の改正（2009 年 12 月）－インターネット取引等の規制を強化

これまでの指定商品・指定役務制が廃止され、訪問販売・通信販売等では原則すべての商品・役務が規制対象となりました。

（６）法律の改正（2017 年 12 月）－規制範囲の拡大等

訪問販売・通信販売等においては、指定権利制度を見直し、株式・社債等を加えて特定権利が規制対象となりました。また、通信販売においては、ファクシミリ広告の請求等をしていない消費者に対するファクシミリ広告の提供を禁止する規制が導入されました。

トピックス：現行の特定商取引法による電子メール広告規制の詳細

（１）法律の目的

特定商取引（訪問販売、通信販売、電話勧誘販売、連鎖販売取引、特定継続的役務提供、業務提供誘引販売取引、訪問購入）を公正にし、及び購入者等が受けることのある損害の防止を図ることにより、購入者等の利益を保護し、あわせて商品等の流通及び役務の提供を適正かつ円滑にし、もって国民経済の健全な発展に寄与することを目的としています。

（２）規制の対象となる「電子メール広告」

通信販売、連鎖販売取引（いわゆるマルチ商法）、業務提供誘引販売取引（いわゆる内職商法、資格商法、モニター商法など）の形態で消費者と取引をする場合において、事業者が、取引の対象となる商品や役務などについて電子メールにより広告をする場合が規制の対象です。

（３）規制の対象となる者

消費者と契約を締結しようとする販売業者等のほか、販売業者等から、電子メールに関する以下の業務を一括して受託している電子メール広告受託事業者等も規制の対象です。

(ア) 消費者から電子メール広告の送付についての請求や承諾を得る業務

(イ) 消費者からの請求や承諾の記録を作成し、保存する業務

(ウ) 送信する電子メール広告に、消費者が受信拒否の意志を表示するための方法や連絡先などを表示する業務

（４）オプトイン方式による規制

(ア) 送信禁止
消費者からあらかじめ請求や承諾を得ていない限り、電子メール広告を送ることは、原則的に禁止されています。

(イ) 再送信禁止
電子メール広告の送信を拒否した消費者に対しては、それ以後、電子メール広告を送ることが禁止されています。

(ウ) 請求や承諾の保存義務
電子メール広告を送信することについて消費者からの請求や承諾を受けた場合は、その記録を保存することが義務づけられています。

(エ) 表示義務
販売業者等が送信する電子メール広告には、電子メール広告を拒否する方法などの一定の事項を表示することが義務付けられています。

(オ) その他
以下の行為も禁止されています。

- いわゆる「ワンクリック詐欺」（販売業者等が消費者から申込みを受ける場合に、パソコンの操作等が契約の申込みとなることを、消費者が容易に認識できるように表示しない行為）。
- 消費者に分かりにくい形で、電子メール広告を行うことについての請求・承諾を得ようとする行為。
- オプトイン方式の規制に違反している者に、（３）の(ア)から(ウ)の業務を一括して委託する行為。

（５）法律違反があった場合の措置など

(ア) 刑事罰
請求・承諾のない者への電子メール広告の送信、受信拒否者に対する電子メール広告の送信、請求・承諾があった旨の記録の保存義務違反などの場合は、刑事罰の対象となります。

(イ) 行政処分（指示又は業務停止命令等）
主務大臣は、以下の場合において、消費者の利益が害されるおそれがあると認めるときは、販売業者等に対して行政処分（指示又は業務停止命令等）を行うことができます。指示又は業務停止命令等に違反した場合は刑事罰の対象となります。

- 請求や承諾をしていない消費者に電子メール広告を送信した場合
- 電子メール広告の提供を拒否した消費者に電子メール広告を送信した場合
- 請求や承諾の記録を作成・保存しなかった場合や、虚偽の記録を作成・保存した場合
- （４）(オ)に掲げる行為を行った場合

(ウ) 報告徴収、立入検査
主務大臣は、特定商取引法の施行のために、販売業者等に対し、報告や物件の提出を命ずることができるほか、職員による立入検査を行うことができます。報告徴収を受けた場合に報告をしなかった場合・虚偽の報告をした場合や、立入検査を拒んだ場合は刑事罰の対象となります。

(エ) 販売業者等と取引する者への報告命令
主務大臣は、特定商取引法の施行のために、販売業者等と取引する者に対し、販売業者等の業務や財産に関して参考となるべき報告や資料の提出を命ずることができます。例えば、販売業者等と取引をする銀行に対し、口座番号を手がかりに、販売業者等の住所などの契約者情報の提出を命ずることが可能です。

(オ) 電気通信事業者などへの情報提供の求め
主務大臣は、特定商取引法の施行のために、電気通信事業者などに対し、電子メールアドレス、IP アドレス、ドメイン名などの契約者情報の提供を求めることができます。

(カ) 主な罰則
主な罰則をまとめて図表３－１－９に記します。

図表３－１－９　特定商取引法の主な罰則

違反事項	罰則
請求・承諾のない者への電子メール広告の送信	100 万円以下の罰金
拒否者に対する電子メール広告の送信	
請求・承諾があった旨の記録の保存義務違反	
請求・承諾のない者や拒否者へ送信された電子メール広告における誇大広告や表示義務違反	１年以下の懲役又は 200 万円以下の罰金 （又はこれらの併科）
業務停止命令等違反	３年以下の懲役又は 300 万円以下の罰金 （法人の場合は３億円以下の罰金）
指示違反	６月以下の懲役又は 100 万円以下の罰金 （又はこれらの併科）

（６）省令・ガイドライン

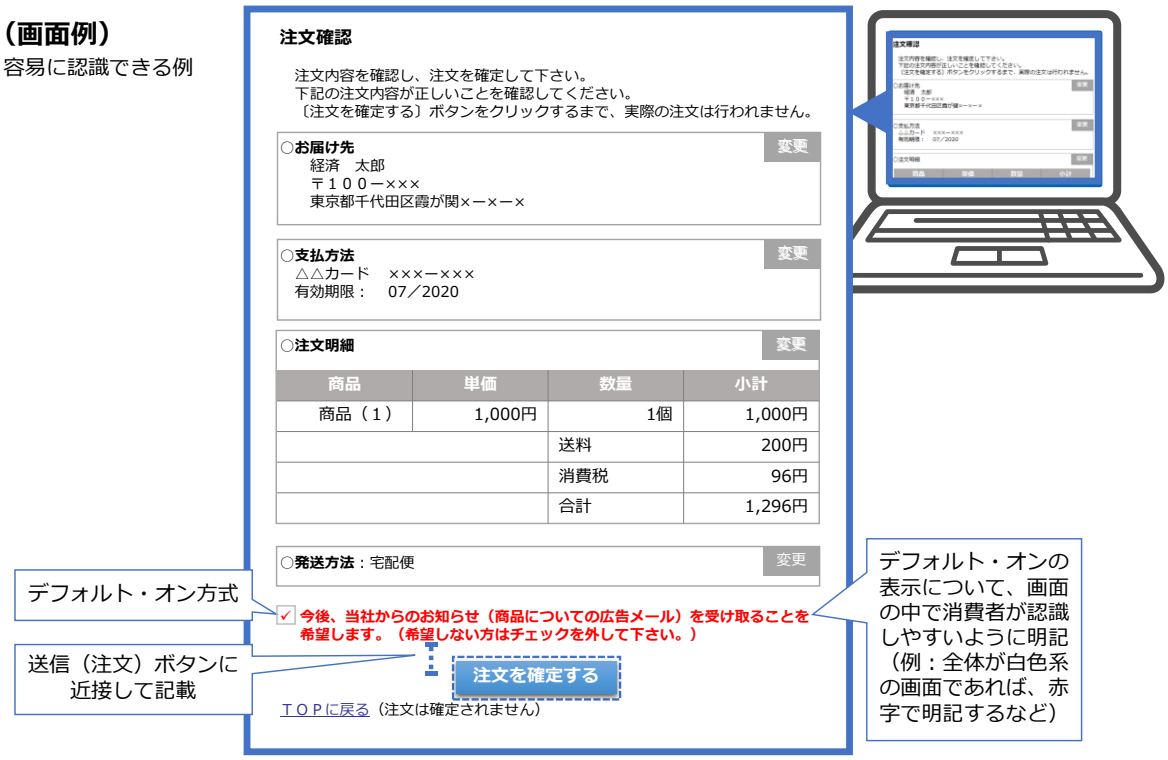
特定商取引に関する法律施行規則

特定商取引法の運用に当たっての詳細な事項は、特定商取引に関する法律施行規則に定められています。具体的には、オプトイン方式による規制の適用が除外される場合、請求・承諾があったことを証する記録として保存すべき事項・保存すべき期間、表示が義務づけられる事項の詳細などが規定されています。

電子メール広告をすることの承諾・請求の取得等に係る「容易に認識できるよう表示していないこと」に係るガイドライン

特定商取引法においては、消費者に分かりにくいやり方で電子メール広告を受けることについての承諾・請求を行わせようとする行為が、行政処分の対象とされていますが、どのようなケースが行政処分の対象となり得るかを明確化するため、「電子メール広告をすることの承諾・請求の取得等に係る『容易に認識できるよう表示していないこと』に係るガイドライン」が定められています[注69]。

図表３－１－１０　消費者が商品を購入したショッピングサイトなどにおける承諾の取り方



（７）主務大臣

内閣総理大臣、経済産業大臣及び事業等所管大臣が、主務大臣とされています。また、電子メール広告受託事業者に関する事項については、内閣総理大臣及び経済産業大臣が主務大臣とされています。なお、内閣総理大臣の権限は、一部を除いて消費者庁長官に委任されており、消費者庁長官に委任された権限の一部は、経済産業局長に委任されています。

注69 消費者庁「特定商取引法ガイド」http://www.no-trouble.go.jp/pdf/20190410ra03.pdf

３　その他の法律による迷惑メールに関する規制

迷惑メールに関しては、特定電子メール法や特定商取引法による電子メールに特化した規制のほか、電子メールの内容などによっては、刑法などによる法規制の対象にもなります。

例えば、架空請求メールを送信し、現金の振り込みなどを行わせた場合は、刑法第 246 条の詐欺罪が成立する可能性があります。

図表３－１－１１　電子メールの送信に関わる法規制（特定電子メール法および特定商取引法を除く）

規制されている電子メールの送信	根拠法	罰則
1　名誉毀損、侮辱、脅迫		
人の名誉を毀損する多数の者への電子メールの送信の禁止	刑法第 230 条（名誉毀損）	3 年以下の懲役若しくは禁錮又は 50 万円以下の罰金
他人を侮辱する多数の者への電子メールの送信の禁止	刑法第 231 条（侮辱）	拘留又は科料
他人を脅迫する電子メールの送信の禁止	刑法第 222 条（脅迫）	2 年以下の懲役又は 30 万円以下の罰金
2　風説の流布、業務妨害（信用毀損、株価操作など）		
虚偽の風説の流布等により、信用を毀損し、又は業務を妨害する電子メールの送信の禁止	刑法第 233 条（信用毀損及び業務妨害）	3 年以下の懲役又は 50 万円以下の罰金
有価証券等の相場の変動を図る目的をもって、風説を流布する電子メールの送信の禁止	金融商品取引法第 158 条、第 197 条第 1 項第 5 号	10 年以下の懲役若しくは 1,000 万円以下の罰金又はその併科
3　わいせつ物頒布、児童ポルノ提供など		
わいせつ画像データを含む電子メールの送信の禁止	刑法第 175 条（わいせつ物頒布等[注70]）	2 年以下の懲役若しくは 250 万円以下の罰金若しくは科料又は懲役及び罰金の併科
人に児童買春をするように勧誘する電子メールの送信の禁止	児童ポルノ処罰法第 6 条第 1 項	5 年以下の懲役若しくは 500 万円以下の罰金又はその併科
児童ポルノの画像等を含む電子メールの送信の禁止	児童ポルノ処罰法第 7 条第 2 項	3 年以下の懲役又は 300 万円以下の罰金
4　著作権の侵害		
著作物の無断配信等著作権を侵害する電子メールの送信の禁止	著作権法第 119 条第 2 項	5 年以下の懲役若しくは 500 万円以下の罰金又はその併科
5　ネズミ講への勧誘		
業として、ネズミ講に加入することを勧誘する電子メールの送信の禁止	無限連鎖講防止法第 6 条	1 年以下の懲役又は 30 万円以下の罰金
ネズミ講に加入することを勧誘する電子メールの送信の禁止	無限連鎖講防止法第 7 条	20 万円以下の罰金
6　詐欺		
架空請求等の詐欺行為の実行の着手となる電子メールの送信の禁止	刑法第 246 条（詐欺[注71]）	10 年以下の懲役
7　個別分野における広告		
（例）医薬品等の虚偽又は誇大広告、承認前の医薬品等の広告を行う電子メールの送信の禁止	医薬品医療機器等法第 66 条第 1 項、第 68 条、第 85 条	2 年以下の懲役若しくは 200 万円以下の罰金又はこれらの併科
8　ウイルス作成・提供・保管等		
ウイルス作成・提供・供用の禁止	刑法第 168 条の 2（不正指令電磁的記録作成等）	3 年以下の懲役又は 50 万円以下の罰金
ウイルスの取得・保管の禁止	刑法第 168 条の 3（不正指令電磁的記録取得等）	2 年以下の懲役又は 30 万円以下の罰金
9　フィッシングメール		
フィッシングメールの送信の禁止	不正アクセス行為の禁止等に関する法律第 7 条第 2 号、第 12 条第 4 号[注72]	1 年以下の懲役又は 50 万円以下の罰金

注70　2011 年 6 月に公布された「情報処理の高度化等に対処するための刑法等の一部を改正する法律」により、電子メールを含む「電気通信の送信によりわいせつな電磁的記録その他の記録を頒布した」行為などを処罰する規定が挿入された。

注71　財物の交付又は財産的利益の移転がなされていない場合は、詐欺未遂。

注72　2012 年 3 月に公布された「不正アクセス行為の禁止等に関する法律の一部を改正する法律」により新たに設けられた。

4　海外での対策法制の整備状況

（1）米国

規制対象の電子メールは、パソコン向け商用電子メール、携帯電話向け商用電子メール、自動ダイヤリングシステム[注73]を用いて送信される SMS に大別され、それぞれ規制内容が異なります。パソコン向け商用電子メールは CAN-SPAM 法[注74]によりオプトアウト方式で規制しています。携帯電話向け商用電子メールは CAN-SPAM 法実施規則[注75]によりオプトイン方式で規制しています。自動ダイヤリングシステムによって送信される SMS は TCPA 法[注76]によりオプトイン方式で規制しています。いずれの場合も表示義務を課しています。違反者に対する制裁処置として、行政処分（停止命令）、自由刑及び罰金刑が設けられています。

（2）カナダ

規制対象の電子メールは商用電子メール（SMS を含む）とされ、CASL 法[注77]によりオプトイン方式でこれを規制し、表示義務を課しています。違反者に対する制裁処置として、行政処分（過料）及び罰金刑が設けられています。

（3）英国

規制対象の電子メールはダイレクトマーケティング目的の電子メール（SMS を含む）とされ、データ保護法[注78]及びプライバシー・電子通信規則[注79]によりオプトイン方式でこれを規制しています。違反者に対する制裁処置として罰金刑が設けられています。

注73 自動ダイヤリングシステム（automatic telephone dialing system）とは、下記の機能を有する機器をいう。
無作為または連続の番号発生機を使用して被呼者の電話番号を蓄積または産出する機能、当該電話番号をダイヤルする機能

注74 Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003

注75 Rules and Regulations Implementing the Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003

注76 Telephone Consumer Protection Act of 1991

注77 An Act to promote the efficiency and adaptability of the Canadian economy by regulating certain activities that discourage reliance on electronic means of carrying out commercial activities, and to amend the Canadian Radio-television and Telecommunications Commission Act, the Competition Act, the Personal Information Protection and Electronic Documents Act and the Telecommunications Act S.C. 2010

注78 Data Protection Act 1998

注79 The Privacy and Electronic Communications (EC Directive) Regulations 2003

（４）ドイツ

規制対象の電子メールは商用電子メールとされ、不正競争防止法[注80]及びテレメディア法[注81]によりオプトイン方式でこれを規制し、表示義務を課しています。違反者に対する制裁処置として、行政処分（中止命令、過料）が設けられています。

（５）フランス

規制対象の電子メールはダイレクトマーケティング目的の電子メール（SMS を含む）とされ、郵便・電子通信法典[注82]及び消費法典[注83]によりオプトイン方式でこれを規制し、表示義務を課しています。違反者に対する制裁処置として、罰金刑が設けられています。

（６）中国

規制対象の電子メールは商用電子メールと商用 SMS に大別され、それぞれ規制内容が異なります。商用電子メールはインターネット電子メールサービス管理弁法[注84]によりオプトイン方式で規制し、表示義務を課しています。違反者に対する制裁処置として、行政処分（改善命令）、罰金刑が設けられています。一方、商用 SMS は通信ショートメッセージサービス管理規定[注85]によりオプトイン方式で規制しています。違反者に対する制裁処置として、行政処分（過料）が設けられています。

（７）韓国

規制対象の電子メールは、営利目的の広告電子メール（SMS を含む）とされ、情報通信網利用促進及び情報保護などに関する法律[注86]によりオプトイン方式で規制し、表示義務を課しています。違反者に対する制裁処置として、行政処分（過料）、懲役刑及び罰金刑が設けられています。

（８）オーストラリア

規制対象の電子メールは商用電子メール（SMS を含む）とされ、スパム法[注87]によりオプトイン方式でこれを規制し、表示義務を課しています。違反者に対する制裁処置として、行政処分（警告、違反通知、法的拘束力を有する約束）及び罰金刑が設けられています。

注80 Gesetz gegen den unlauteren Wettbewerb
注81 Telemediengesetz
注82 Code des postes et des communications électroniques
注83 Code de la consommation
注84 互联网电子邮件服务管理办法
注85 通信短信息服务管理规定
注86 정보통신망 이용촉진 및 정보보호 등에 관한 법률
注87 Spam Act 2003

図表３－１－１２（1）海外での対策法制の整備状況一覧

	米国			カナダ	英国	ドイツ
所管機関	連邦取引委員会（FTC）	連邦通信委員会（FCC）		カナダ・ラジオテレビ通信委員会（CRTC）	・通信庁（Ofcom） ・情報コミッショナーズオフィス（ICO）	通信ネットワーク庁（BNetzA）
規制対象の電子メール	パソコン向け商用電子メール	携帯電話向け商用電子メール	自動ダイヤリングシステムによって送信される SMS	商用電子メール（SMS を含む）	ダイレクトマーケティング目的の電子メール（SMS を含む）	商用電子メール
迷惑メール規制法令	CAN-SPAM 法	CAN-SPAM 法 実施規則	TCPA 法	CASL 法	・データ保護法 ・プライバシー・電子通信規則	・不正競争防止法 ・テレメディア法
送信に関わる規制	オプトアウト方式（受信拒否の意思表示がなされた者への送信を停止する）	オプトイン方式（同意を得た者にのみ送信する）	オプトイン方式（同意を得た者にのみ送信する）	オプトイン方式（同意を得た者にのみ送信する）	オプトイン方式（同意を得た者にのみ送信する）	オプトイン方式（同意を得た者にのみ送信する）
表示義務	・送信者名・受信者に誤解を与えないない件名・広告メールである旨 ・オプトアウトが可能である旨 ・オプトアウトの通知を受け付ける電子メールアドレス又はオプトアウトの方法 ・送信者の住所 ・性的内容を含む場合はその旨	・オプトアウトが可能である旨 ・オプトアウトの通知を受け付ける電子メールアドレス又はオプトアウトの方法 ・受信者が送信者がオプトインした者であることを合理的に判断できる情報	・オプトアウトが可能である旨 ・オプトアウトの通知を受け付ける電話番号 ・テレマーケティングを行う者又は送信者の身元、電話番号及び住所	・送信者を特定するための情報 ・送信者の連絡先	・送信者名 ・オプトアウトの通知を受け付ける電子メールアドレス	・送信者の情報 ・商用電子メールであること
違反者への制裁処置	・行政処分（停止命令） ・刑事罰（自由刑、罰金刑）	・行政処分（停止命令） ・刑事罰（自由刑、罰金刑）	・行政処分（停止命令） ・刑事罰（自由刑、罰金刑）	・行政処分（過料） ・刑事罰（罰金刑）	・刑事罰（罰金刑）	・行政処分（中止命令、過料）

図表３－１－１２（２）海外での対策法制の整備状況一覧

フランス	中国		韓国	オーストラリア	（参考）日本	
国家個人情報保護機関（CNIL）	工業・情報化部（MIIT）		放送通信委員会（KCC）	オーストラリア通信メディア庁（ACMA）	総務省 消費者庁	経済産業省 消費者庁
ダイレクトマーケティング目的の電子メール（SMS を含む）	商用電子メール	商用 SMS	営利目的の広告電子メール（SMS を含む）	商用電子メール（SMS を含む）	広告宣伝メール	電子メール広告
・郵便・電子通信法典 ・消費法典	インターネット電子メールサービス管理弁法	商用 SMS は通信ショートメッセージサービス管理規定	情報通信網利用促進及び情報保護等に関する法律	スパム法	特定電子メール法	特定商取引法
オプトイン方式（同意を得た者にのみ送信する）	オプトイン方式（同意を得た者にのみ送信する）	オプトイン方式（同意を得た者にのみ送信する）	オプトイン方式（同意を得た者にのみ送信する）	オプトイン方式（同意を得た者にのみ送信する）	オプトイン方式（同意を得た者にのみ送信する）	オプトイン方式（同意を得た者にのみ送信する）
・商用電子メールであること ・商用電子メールの送信を委託した者が存在する場合は、委託した者 ・オプトアウトが可能である旨	・広告である旨	（不明）	・広告である旨 ・送信者名 ・送信者の電子メールアドレス、電話番号及び住所 ・オプトアウトが可能である旨及びその方法	・送信者名 ・送信者の連絡先 ・オプトアウトが可能である旨 ・オプトアウトの通知を受け付ける電子メールアドレス	・送信者などの名称 ・オプトアウトが可能である旨 ・オプトアウトの通知を受け付ける電子メールアドレス又はURL ・送信者などの住所苦情・問い合わせなどを受け付けることが可能な電話番号、電子メールアドレス、URL	・オプトアウトが可能である旨 ・オプトアウトの通知を受け付ける電子メールアドレス又はURL
・刑事罰（罰金刑）	・行政処分（改善命令） ・刑事罰（罰金刑）	・刑事罰（罰金刑）	・行政処分（過料） ・刑事罰（懲役刑及び罰金刑）	・行政処分（警告、違反、通知、法的、拘束力を有する約束） ・刑事罰（罰金刑）	・行政処分（措置命令） ・刑事罰（懲役刑、罰金刑）	・行政処分（指示、業務停止命令） ・刑事罰（懲役刑、罰金刑）

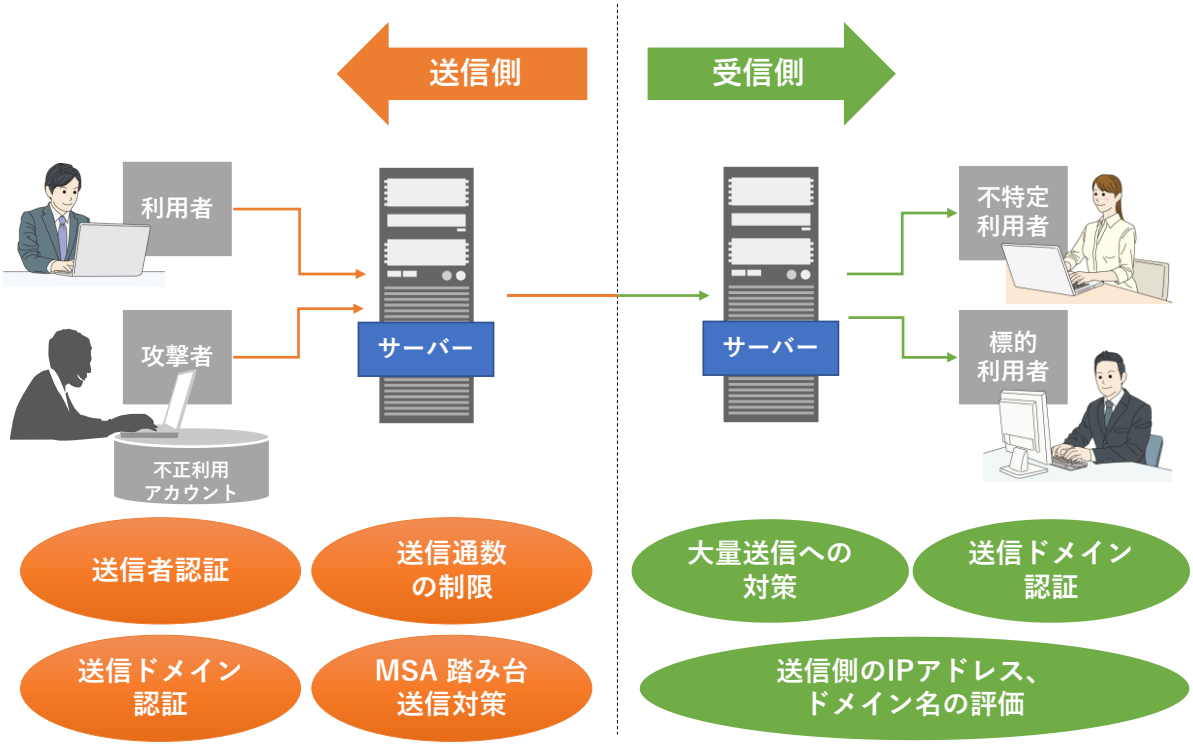
第2節　技術的な対策

1　概要

迷惑メールの送信方法の悪質化・巧妙化に対応して、技術的な対策についても、その高度化・精緻化が進んでいます。迷惑メールへの技術的な対策として、送信側で迷惑メールを送信させないようにすること、受信側で迷惑メールを受信しないようにすることの二つの視点があり、いずれか一方だけでは十分な対策にはならないため、双方において適切な技術的な対策を組み合わせることで、より高い効果を得ることができます。

本節では、迷惑メールへの技術的な対策の代表例について、送信側・受信側に分けて説明します。

図表３－２－１　主な技術的な対策の概要



２　送信側での対策

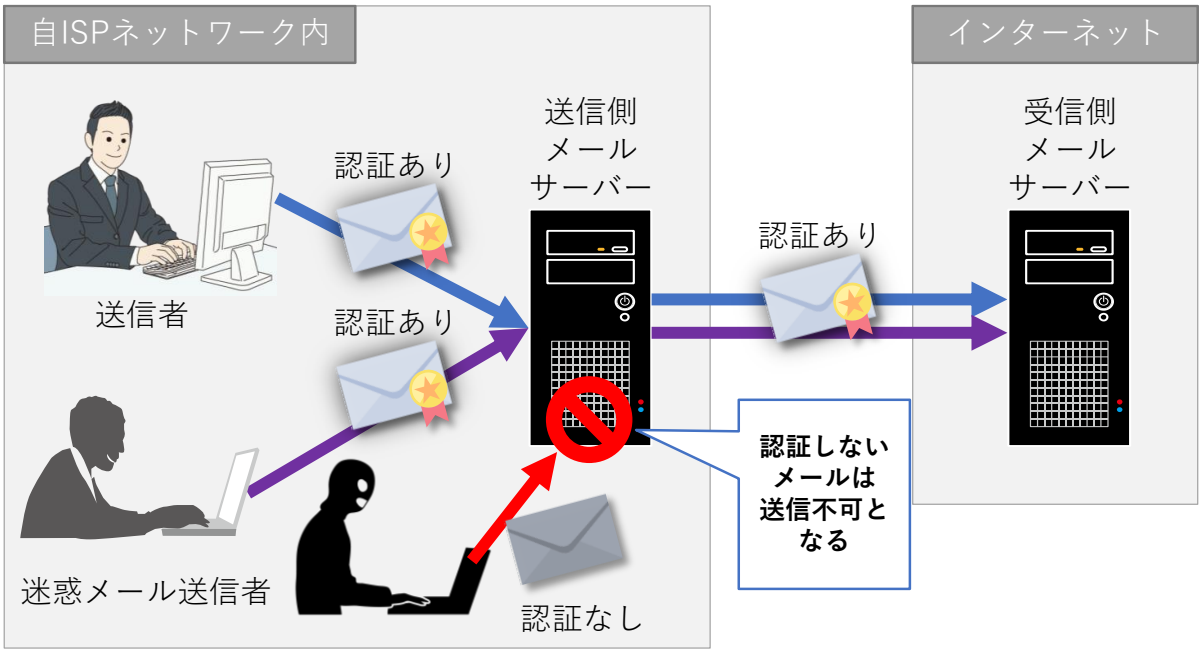
固定 IP アドレス[注 88]を取得して送信する方法は、契約者情報の確認を適切に実施していれば送信元を特定できることから、利用停止などの運用的な対処や法的対処が比較的容易です。一方、ASP[注 89]や共用ホスティングサービス[注 90]の送信メールサーバーは、該当のサービスを契約している不特定多数の利用者を前提にしているため、その中に紛れ込んだ迷惑メールの送信を制限することは容易ではありません。そのため、効果があると思われる技術的な対策を組み合わせて対応が行われています。

（１）送信者認証

電子メールの送信に用いられる通信方式である SMTP には、送信者を確認（認証）する機能が設けられていません。そのため、従来のメールサービスでは、ISP のネットワーク内であれば、電子メールの送信時に送信者の認証を必要としないものが存在しており、迷惑メールの送信に悪用されることになりました。これに対応するための技術的な対策として用いられる機能が、送信者認証を用いた電子メールの送信制限です。

送信者認証とは、送信側 ISP において自社の送信メールサーバーから電子メールを送信しようとするユーザーを認証することをいい、その代表的な方法として、SMTP に認証機能を設けた SMTP-AUTH[注 91]が挙げられます。SMTP-AUTH では、送信メールサーバーにおいて送信者をアカウントおよびパスワードにより認証し、認証に成功した者からのメールのみを送信可能とするものです。迷惑メールが送信された場合には、送信者の特定が容易になり、迷惑メールの送信抑止につながることになります。

図表３－２－２　送信者認証（SMTP-AUTH)を用いた対策



注88 再接続しても IP アドレスが変わることのない IP アドレスのこと。

注89 Application Service Provider の略称で、ネットワーク経由でソフトウェアやソフトウェア稼働環境を提供する事業者のこと。

注90 ホスティングサービスとは、事業者が管理するサーバーを顧客に貸与するサービスのことで、複数の利用者でサーバーを共用するホスティングサービスを共用ホスティングサービスという。

注91 SMTP Authentication の略称で、SMTP 認証という。SMTP-AUTH は、1999 年に RFC2554（https://tools.ietf.org/html/rfc2554）で規定された後、2007 年に RFC4954（https://tools.ietf.org/html/rfc4954）によって更新された。

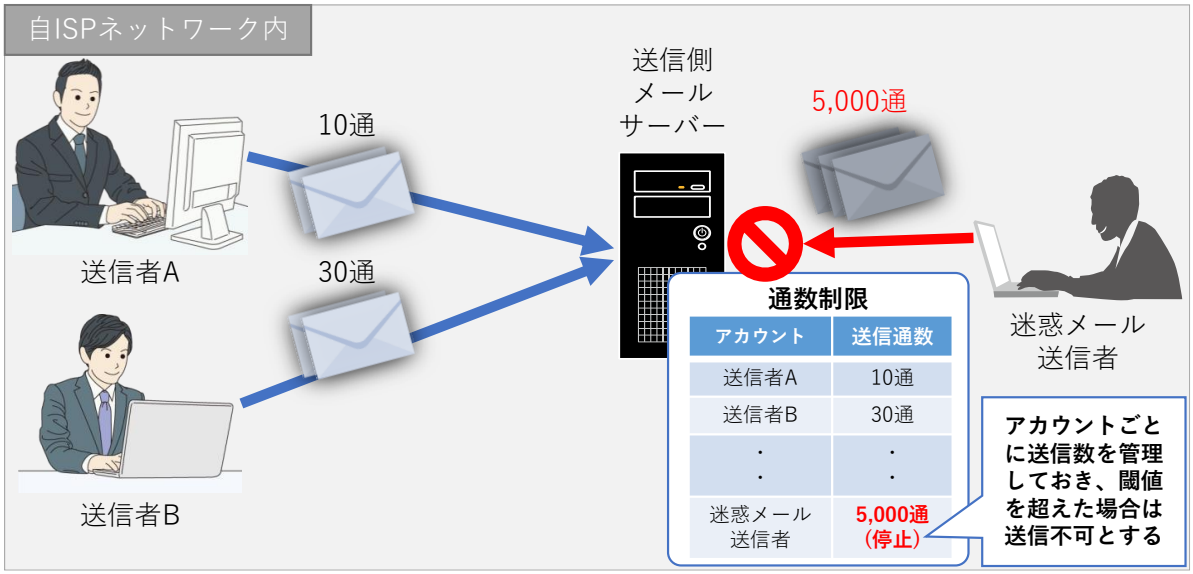
（2）電子メールの通数を制限する方法

迷惑メールは、一時に大量送信されることがあり、そのような送信手法に対応するための技術的な対策として、1 つの電子メールアカウントや IP アドレスから一定期間に送信可能な電子メールの通数を制限する仕組みがあります。なお、CIDR [注 92]単位や IP アドレスの地域情報を用いたグループを単位にして制限することも可能です。

電子メールアカウント単位での制限は、送信者認証を実施していないと迷惑メールの送信者が特定できないため、実施できません。IP アドレス単位での制限は、送信者認証を実施していない場合でも実施可能ですが、IP アドレスを再利用している場合や同一の IP アドレスを複数のユーザ―で利用している場合には、制限すべきユーザー以外の者からの電子メールの送信が制限されてしまうおそれがありますので、注意が必要です。

携帯電話から送信される迷惑メールが増加した当時には、携帯電話事業者では、電子メールの通数を制限する仕組みを導入して、対策を実施していました。

図表３－２－３　電子メールの通数を制限する対策



注92 Classless Inter-Domain Routing の略称で、有限な IP アドレスの有効利用に資する仕組み。クラス分類とは関係なく IP アドレスの割り当てと、グループ化したアドレスブロックによる経路情報の集約により、柔軟な運用が可能。

（３）MSA 踏み台送信への対策

第三者が正当なユーザーの電子メールアカウントを不正に用いて送信メールサーバー（MSA）に接続して迷惑メールを送信する場合があり、「MSA 踏み台送信」と呼ばれています。MSA 踏み台送信は、送信側での技術的な対策である送信者認証による検知や電子メールの通数の制限による送信の予防を行うことができない場合があります。一方で、受信側での技術的な対策として、踏み台にされた送信メールサーバー（MSA）がブラックリストに登録されると、当該送信メールサーバーを共用する正当な電子メールアカウントからの電子メールが送信できないこととなってしまうという問題もあります。そこで、MSA 踏み台送信に対しては、送信側での技術的な対策として、次のような対策が取られています。

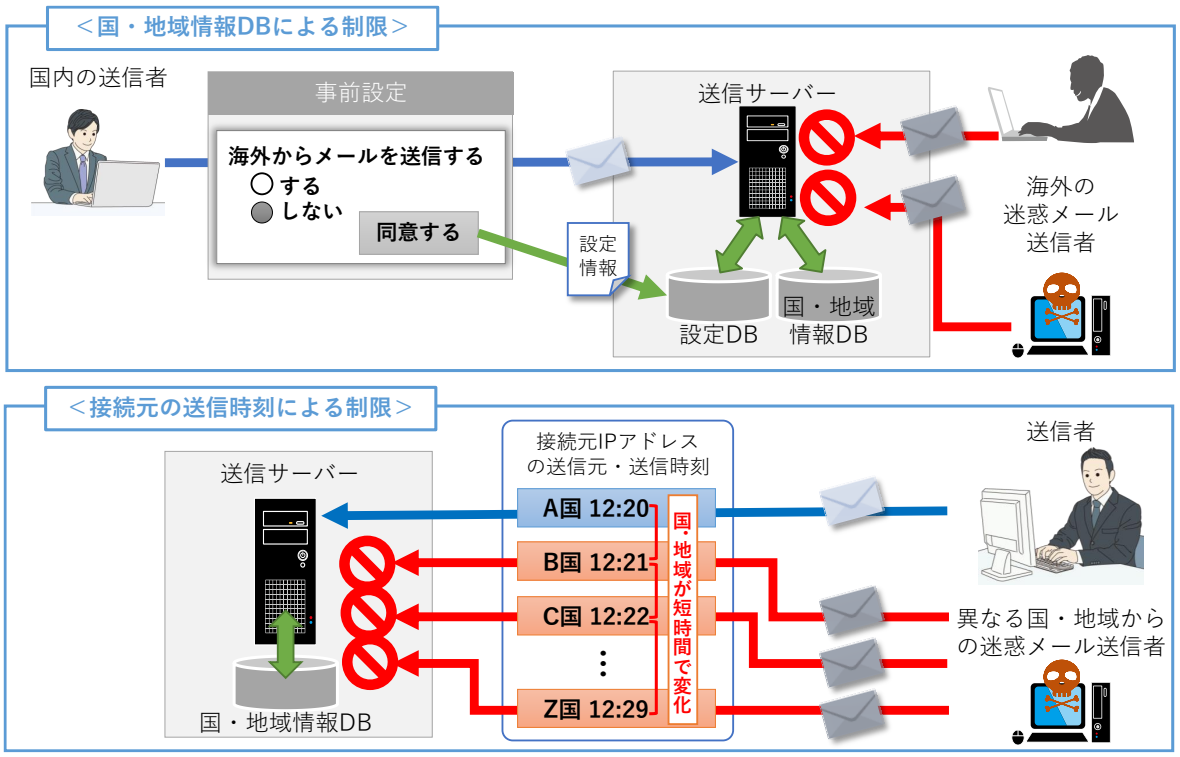
(ア) 接続元情報による制限

送信側で、それぞれの電子メールアカウントがどの接続元 IP アドレスを利用して電子メールを送信しているかを把握することにより、迷惑メールであるかを判断して、その送信を制限する方法です。

この方法の１つとして、接続元の IP アドレスを、IP アドレスの国別のデータベースと比較することにより海外からの電子メールの送信を制限する方法があります。あらかじめ利用者からの申込みを受けることにより、このようなサービスが提供されています。利用者の多くは海外から電子メールを送信することはありませんので、有効な対策になります。

また、別の方法として、同一の電子メールアカウントで送信元情報が短時間で変化することを検知し、迷惑メールの送信を制限する方法があります。不正取得した電子メールアカウントを利用した迷惑メールの送信では、多くの場合は異なる接続元 IP アドレスからメールが送信されていることから、接続元 IP アドレスの国・地域情報の変化を見極めて、これらが短時間で変化している場合は、それを検知し、そのメールアカウントに関わる電子メールの送信を制限する対策が行われます。

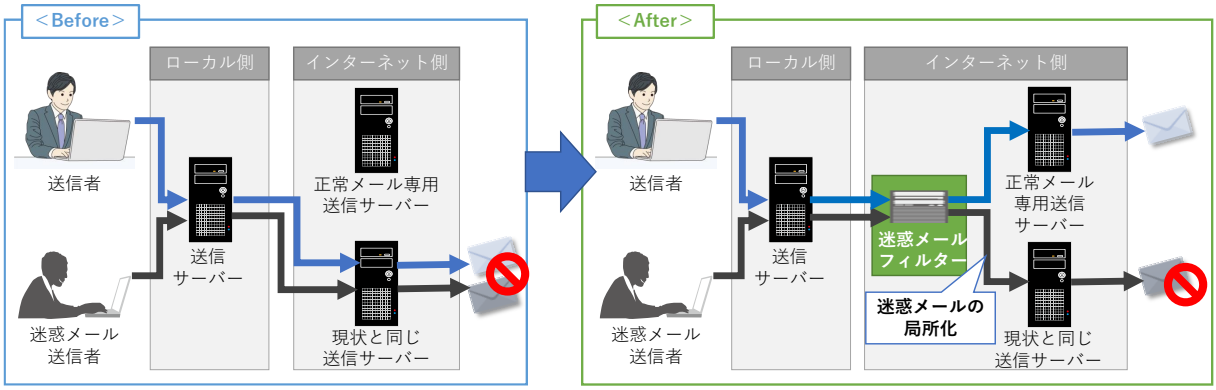
図表３－２－４　接続元情報による制限



(イ) 送信メールサーバーの分離

送信メールサーバーに投稿された電子メールをメールヘッダーや本文を元に迷惑メールとそうでないメールに分類し、それぞれ異なる IP アドレスを持つ別々の送信メールサーバー（MSA）から受信メールサーバーに宛てて送信する方法です。これにより、受信側での技術的な対策として行われる送信メールサーバー MSA のブラックリスト登録による影響を局所化して、不正利用されている電子メールアカウントから迷惑メールが送信されることを防ぐとともに一方、そうでない電子メールアカウントからの通常の電子メールの送信は妨げないようにすることができます。

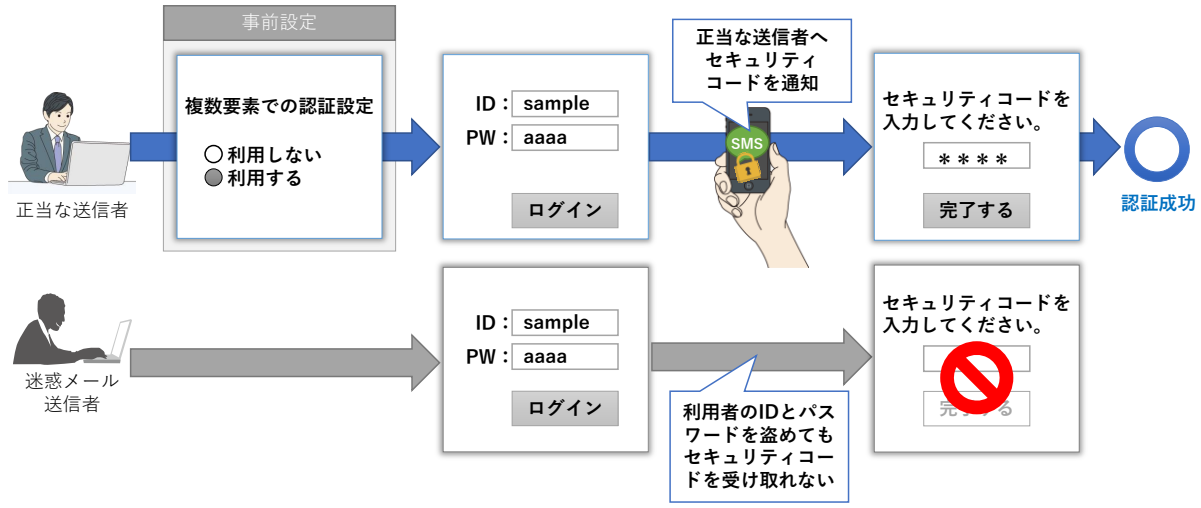
図表３－２－５　送信メールサーバーの分離対策



(ウ) 複数要素での認証

送信者認証に加えてワンタイムパスワードによる認証[注 93]などの複数要素での認証を設けることで、MSA への不正な接続の難易度を高め、迷惑メールの送信を制限する方法です。不正に入手したパスワードなどで MSA に不正に接続して電子メールが送信されると送信者認証に成功するため、迷惑メールを送信することができます。そこで、当対策により MSA への不正な接続の難易度を高めることで、迷惑メールの送信を制限することができます。

図表３－２－６　複数要素での認証

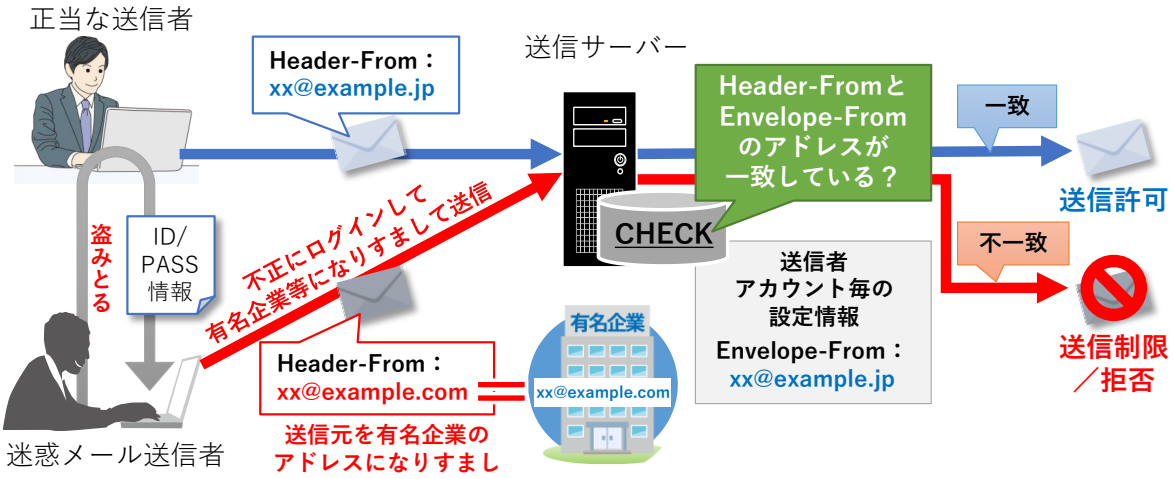


注93 一時的にしか使えないパスワードを通知し、その入力を求める認証のこと。

(エ) 送信者情報の不一致による制限

電子メールの送信にあたり、送信者認証を実施し、送信された電子メールのメールヘッダーの送信者情報（ヘッダーFrom（Header-From）の電子メールアドレス）が、送信者認証に係る電子メールアカウントに付与された電子メールアドレス（通常配送上の送信者情報（Envelope-From）としても用いられる。）と一致するかを確認することで、迷惑メールであるかを判断して、制限する方法です。この方法では、メールヘッダーの電子メールアドレスと配送上の送信者情報とが必ず一致することになるため、送信者認証に成功した電子メールアカウントを用いて、有名企業等別の送信者になりすますような送信元を偽装した電子メールによる問題への対策として有効です。

図表３－２－７　送信者情報の不一致による制限



（４）送信ドメイン認証

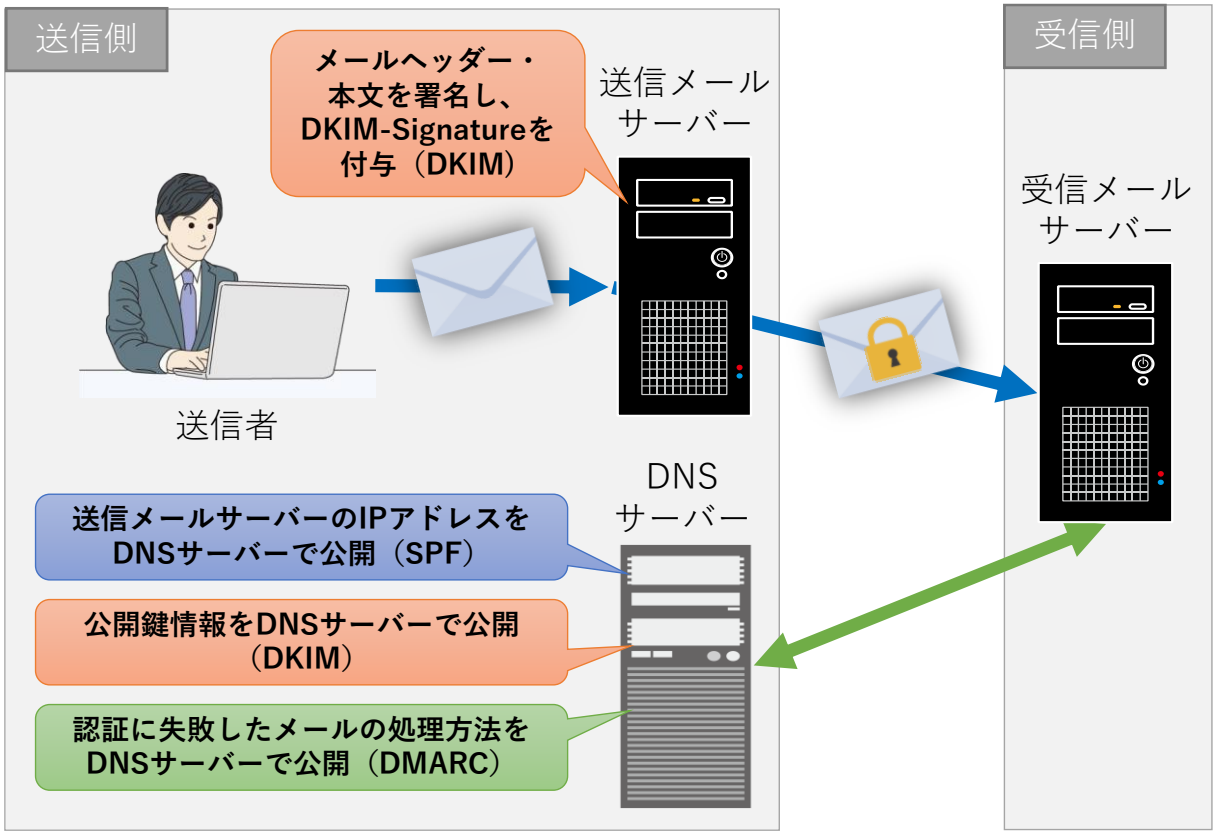
迷惑メールのうち、送信者情報を偽装するなりすましメールへの対応に有効なものとして、送信ドメイン認証技術があります。

送信ドメイン認証技術とは、受信側が、電子メールを送信した側のドメイン名の正当性を確認することができる技術で、送信側での設定と受信側での検証とにより対応するものです。

送信ドメイン認証技術には、送信者情報の違いや認証の仕組みの違いによって複数のものがあります。具体的には、送信メールサーバーの IP アドレスを元に認証する技術（SPF）と、送信メールサーバーで作成した電子署名[注 94]を元に認証する技術（DKIM）があります。さらに、それら認証の結果を元にして、認証に失敗した電子メールの取扱いを送信側で宣言することなどを可能とする技術（DMARC）もあります。

注94 電子署名とは、電磁的記録に記録された情報について作成者を示す目的で行われる暗号化などの措置で、改変が行われていないかどうか確認することができる。

図表３－２－８　送信ドメイン認証（送信側）



(ア) SPF の設定

送信側では、送信者情報である電子メールアドレスのドメイン名の DNS 上に、ドメイン名、当該ドメイン名を用いる電子メールアドレスが用いる送信メールサーバーの IP アドレスなどの情報と、それらに該当した場合の認証結果を記号で示したものを記述することで設定します。

(イ) DKIM の設定

送信側では、電子メールの送信時に 1 通ずつ電子署名を作成し、メールヘッダーに関連情報と合わせて追記して送信するとともに、送信者情報である電子メールアドレスのドメイン名の DNS 上で、電子署名の検証に用いる公開鍵などを公開します。なお、電子署名は、電子メールの本文及びヘッダーから作成した要約データ（ハッシュデータ）を、秘密鍵を用いて符号化することによって作成します。

(ウ) DMARC の設定

送信側では、送信者情報である電子メールアドレスのドメイン名の DNS 上に、認証に失敗した電子メールの取扱い（DMARC ポリシー）を宣言します。また、DMARC には、認証結果のレポートを電子メールで受け取ることができる仕組みがあり、送信側では、レポートの送付先や送付頻度などを設定します。

３　受信側での対策

受信側のメールサーバーでは、様々な方法で送信される迷惑メールの特徴に対して多様な対策をとる必要があります。単位時間や IP アドレスごとの通数に閾値を設けて大量に送信される迷惑メールを防ぐ方法、ドメイン名をなりすました迷惑メールを検知する送信ドメイン認証を利用した方法、迷惑メールに関する利用者の苦情やフィードバックを利用した IP アドレスやドメイン名のレピュテーションを用いる方法などがあります。

（１）大量に送信される迷惑メールへの対策

特定のメールサーバーに対して電子メールを一時に大量送信することで、過負荷になった受信側のメールサーバーを機能不全に陥らせることがあります。このような攻撃をメールボム攻撃といい、サイバー攻撃の一つの方法です。インターネットの安定的な運用の観点から、サイバー攻撃への対処方法が「電気通信事業者におけるサイバー攻撃等への対処と通信の秘密に関するガイドライン[注 95]」として策定されています。大量の通信は、受信側の設備を安定的に運用する妨げになるため、単位時間当たりに受信できる通数を超える場合や、特定の送信元（IP アドレスや CIDR)による大量の通信を確認できる場合は、流量の制限を設けることができます。

（２）送信者情報や電子メールの内容から判断する方法

送信者情報や送信された電子メールの内容を元に、受信側で行う技術的な対策には、いくつかのものがあります。

まず、受信メールサーバーで受信する電子メールについて、受信メールサーバーで受信時に、差出人アドレスなどの送信者情報を基に迷惑メールか否かを判断し、破棄や振分けなどの処理をする方法があります。この方法については、受信メールサーバーではなく、いったん受信メールサーバーで受信した後に判断・処理をすることもあります。

また、送信者情報ではなく、電子メールの内容から迷惑メールと判断、破棄や振分けなどの処理をする方法もあります。例えば、本文や件名に含まれる特定のキーワードや添付ファイルに含まれる特定の情報から迷惑メールと判断します。

注95 インターネットの安定的な運用に関する協議会「電気通信事業者におけるサイバー攻撃等への対処と通信の秘密に関するガイドライン（第５版）」https://www.jaipa.or.jp/other/mtcs/guideline_v5.pdf

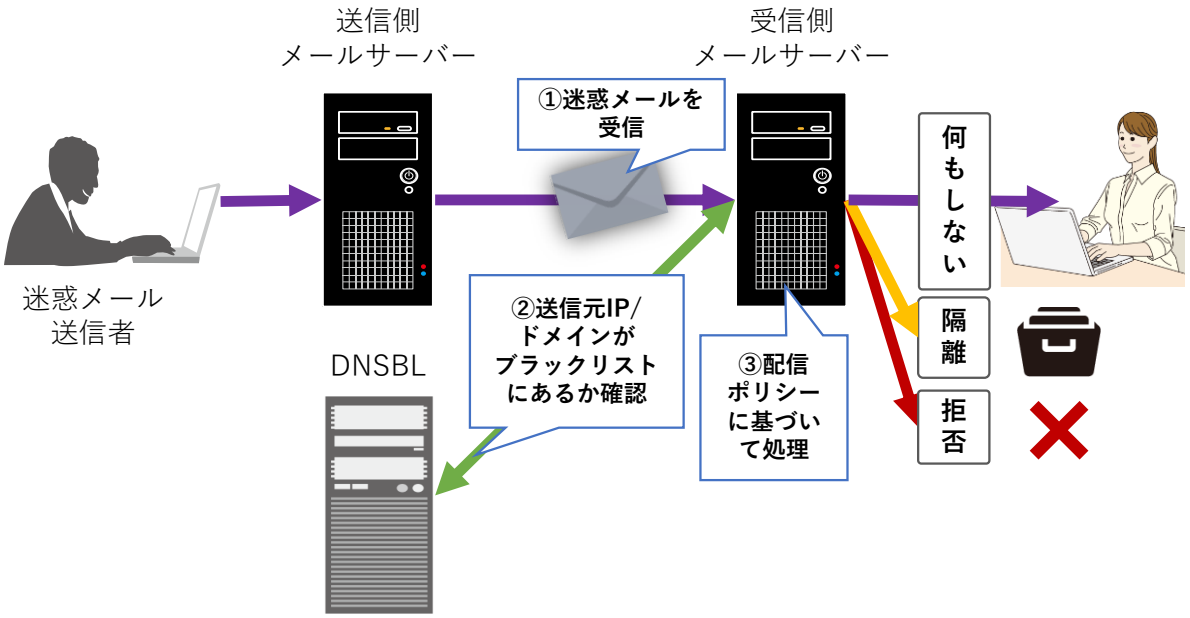
（3）IP アドレスやドメイン名のレピュテーション

受信メールサーバーで、迷惑メールの送信に用いられた送信メールサーバーの IP アドレスを収集し、その IP アドレスから配送される電子メールを受信拒否する方法があります。例えば、DNSBL [注 96]と呼ばれるブラックリスト方式の対策が挙げられます。

受信拒否をするのではなく、該当する送信メールサーバーから受信する電子メールについて、流量の制限を設けることもできます。

また、過去に迷惑メールの送信に用いられた送信メールサーバーだけでなく、客観性のあるレピュテーション [注 97]を用いて、流量の制限や受信拒否を行う送信メールサーバーを決める方法もあります。この方法では、最近出てきている正当なドメイン名に似せたドメイン名や知名度の高いブランド名を含んだ長いドメイン名を取得して利用者をだます方法にも有効です。ただし、レピュテーションを用いた対策を行う場合には、利用者ごとに同意を得て適用している場合を除き、恣意的なものにならないような配慮が必要です。

図表３－２－９　ブラックリストによる対応



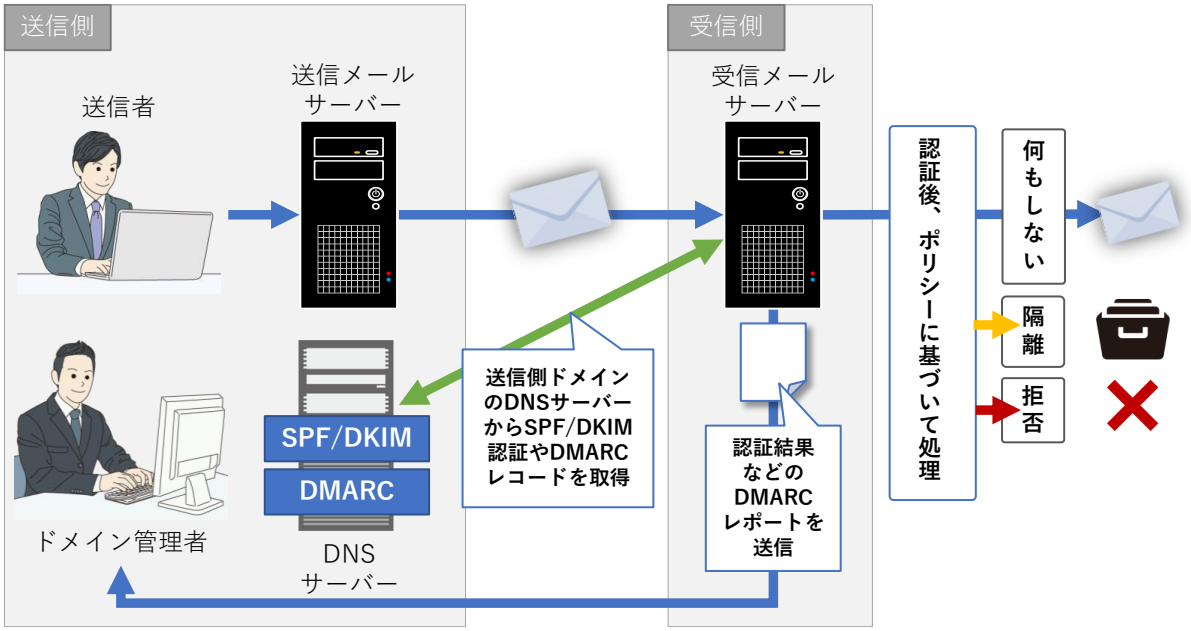
注96 DNS Black（Blackhole とも言う）List。迷惑メール送信元の IP アドレス情報をインターネット上で共有するシステム。受信側メールサーバーでは、DNSBL を利用して送信元の IP アドレス情報によりメールをフィルタリングする。

注97 元になる情報量が十分あり、かつ、著しく恣意的な情報を使わないなどの配慮がなされたレピュテーションのこと。

（４）送信ドメイン認証

送信者情報を偽装するなりすましメールへの対応には、送信側での技術的な対策で説明したとおり、送信ドメイン認証技術が有効であり、送信側で SPF、DKIM、DMARC の設定がなされている場合に、受信側では受信メールサーバーで認証を行い、その結果を次のような様々な方法で利用することができます。

図表３－２－１０　送信ドメイン認証（受信側）



(ア) 認証結果のラベリングおよびフィルタリング

受信メールサーバーで、配送する電子メールのメールヘッダーに、認証結果を示した情報（Authentication-Results ヘッダー[注 98]）を付加して記録（ラベリング）することができます。この記録を用いることで、ISP やメールクライアントソフト（MUA）により、認証に成功したメールを優先して表示することや、認証に失敗したメールを迷惑メールフォルダーなどに振り分けることが可能となります。

(イ) DMARC ポリシーに従った処理

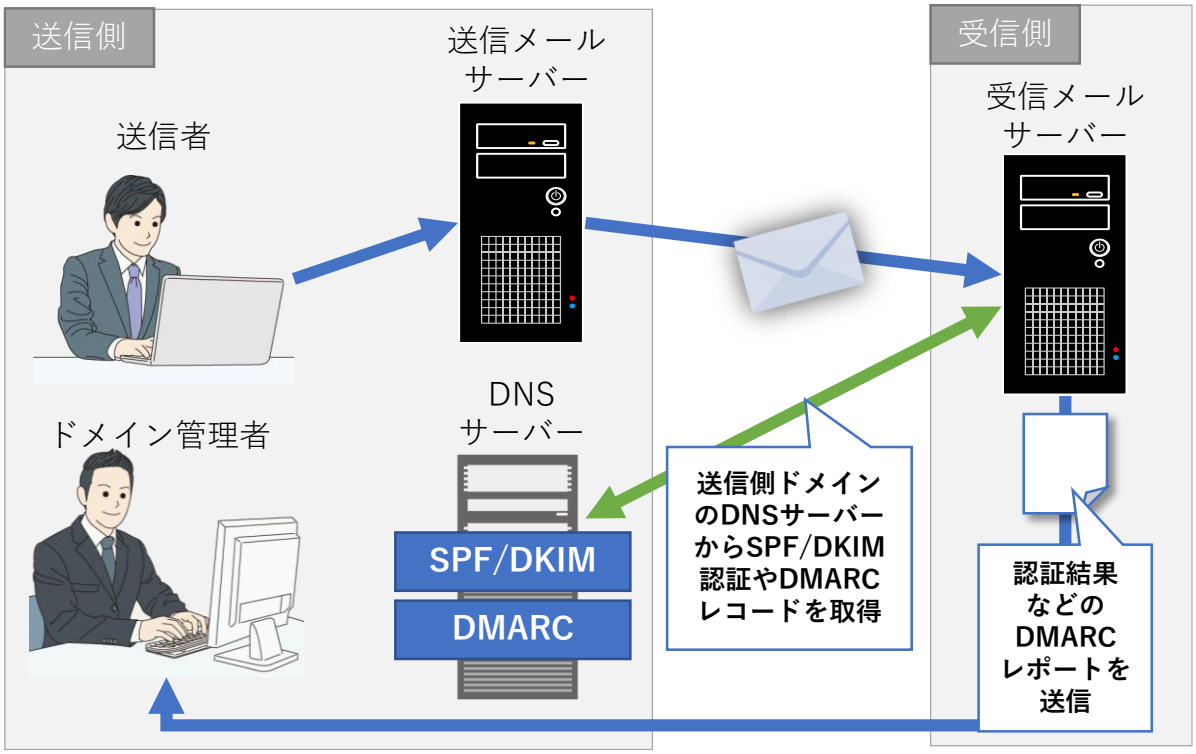
送信側で DMARC ポリシーが設定されている場合には、受信メールサーバーで、認証結果とその DMARC ポリシーに基づいてなりすましメールの処理ができます。海外の一部では、既に DMARC ポリシーに基づいてなりすましメールを排除すること（受信メールサーバーで、認証に失敗した電子メールの受信を拒否すること）に成功しています。

注98 RFC7601 で規定

(ウ) DMARC レポートの送信

送信側で認証結果のレポートを受け取る設定をしている場合には、受信側では、送信側が指定した送付先（管理者）宛てに認証結果のレポートを送付することが重要です。レポートを分析することにより、送信側の管理者は、送信ドメイン認証の運用が適切であるかを判断できます。海外の一部の ISP のようにレポートを送信する受信メールサーバーが増えていくことで、DMARC の普及が進み、受信メールサーバーでの対策も効果的となることが期待されます。

図表３－２－１１　DMARC レポートの送信



(エ) ARC による認証結果の保存

電子メールの利用においては、ユーザーの指定する宛先に転送したり、メーリングリストとして複数の宛先に再配送したりする場合があります。これらの場合には、SPF や DKIM による認証が失敗し、DMARC による認証も失敗することがあります。このため、現在、ARC（Authenticated Received Chain）という転送や再配送に際して認証結果を保存する仕組みが検討されています。その標準化および導入が進んだ場合には、送信ドメイン認証による認証結果の精度向上が図られることが期待されます。

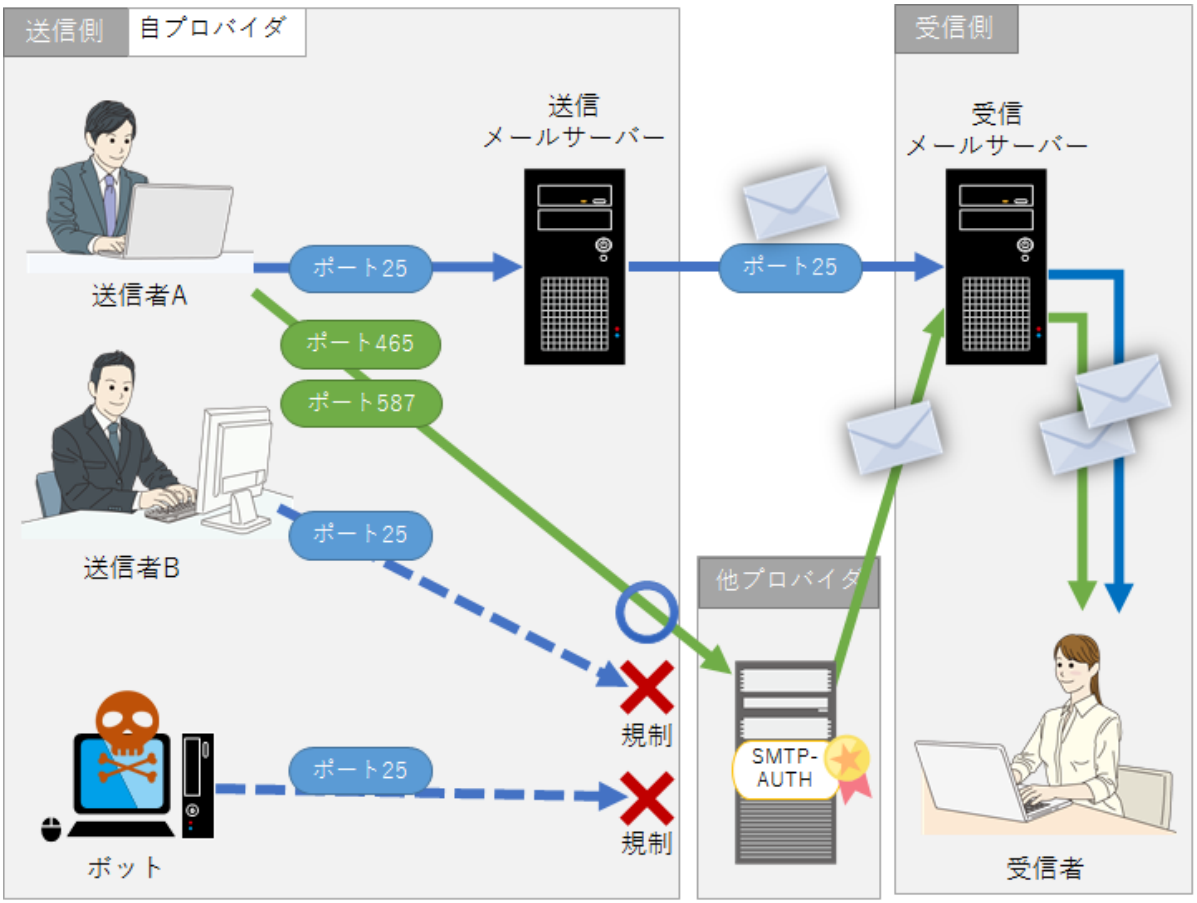
トピックス：OP25B（Outbound Port 25 Blocking）

迷惑メール送信者は ISP の迷惑メール対策を回避するため、契約先の ISP のメールサーバーを使わず、自ら設定するメールサーバーやボットネットを利用して電子メールを直接送信することがあります。このとき利用される IP アドレスは、安価で利用者を特定しにくい動的 IP アドレスであることが多い傾向にあります。そこで、ISP のメールサーバーを利用せず、動的 IP アドレスを割り振られた送信者から電子メールを直接送信することを阻止する技術が OP25B です。

電子メールの送信は受信側メールサーバーの 25 番ポートに向けて行われます。OP25B は、動的 IP アドレスを持つ機器からこの 25 番ポートに向けた通信を遮断することで、迷惑メールの送信を防ぎます。なお、OP25B を実施すると、正当な利用者の通信（例えば、外出先で Wi-Fi 環境から電子メールを送信する場合）も遮断してしまう場合があるため、多くの ISP では、25 番ポートとは別に、SMTP-AUTH が必須の 465 番ポートや 587 番ポートを提供することで、正当な利用者の通信を遮断することを防いでいます。

国内では、2005 年に初めて OP25B が導入され、(一財)日本データ通信協会の調査[注 99]によれば、2011 年第４四半期から導入が広がりました。しかし、サービスを制限すること（例えば、通信を抑止することなど）についての考え方の違いなどから、世界的にみれば OP25B はまだあまり普及していません。日本国内だけではなく、海外の ISP における OP25B の早急な導入が期待されております。

図表３－２－１２　OP25B の概要



注99 (一財)日本データ通信協会迷惑メール相談センター「各プロバイダ（ISP）、CATV(ケーブルテレビ）、モバイル事業者における OP25B 実施状況」https://www.dekyo.or.jp/soudan/contents/taisaku/i2.html

トピックス：送信ドメイン認証技術（SPF・DKIM・DMARC など）

なりすましメール対策の一つとして、送信ドメイン認証は、2003 年頃から検討され始め、現在では SPF、DKIM および DMARC が標準的な技術とされています。

図表３－２－１３　SPF・DKIM・DMARC の比較

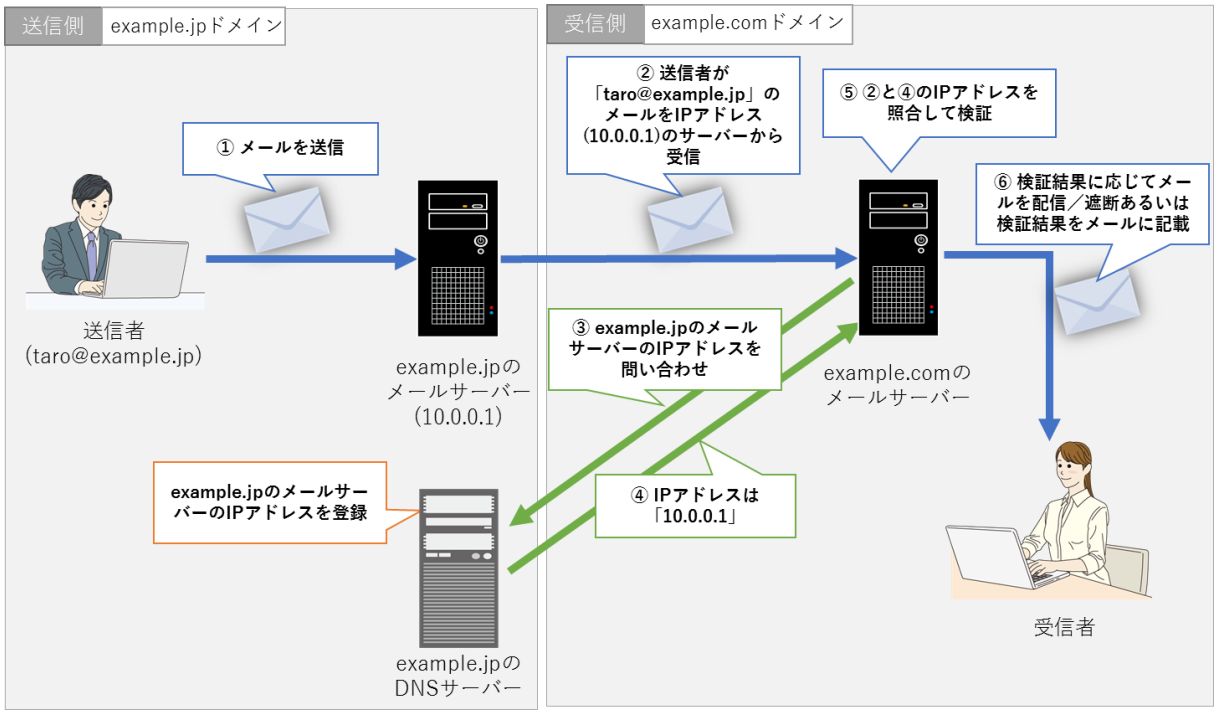
	SPF	DKIM	DMARC
特徴	送信元をネットワーク的に判断 (送信元の IP アドレスにより確認)	送信時に電子署名を電子メールに付加(電子署名の検証により判断)	SPF、DKIM の認証結果を利用 （送信側で DMARC ポリシーを設定、認証結果などのレポート機能）
導入コスト	送信側はほぼ皆無（DNS の記述のみで 1 通づつの処理は不要） 受信側では一定の処理が必要	送信側は総体的に高め (1 通ずつ署名作成・付加が必要) 受信側では一定の処理が必要	既に SPF、DKIM を導入していれば送信側はほぼ皆無（DNS への記述のみ） 受信側では一定の処理が必要
長所	送信側の導入の容易さ 普及が進んでいる	電子メール本文の改ざんも検知 電子メールの配送経路に影響されない	送信側の導入の容易さ 認証失敗時のふるまいを DMARC ポリシーで指定可能
短所	電子メール転送時に認証に失敗する場合がある	配送経路上で電子メールの内容が変更されると認証失敗 第三者署名では DMARC 認証に失敗する場合がある（DNS 設定の工夫で回避できる場合がある）	SPF と DKIM 双方が認証に失敗する場合には、DMARC の認証にも失敗する

（１）SPF（Sender Policy Framework）

SPF は、RFC7208[注100]で規定された、ネットワーク方式で電子メールのなりすましを判断することができる技術です。具体的には、送信側で、送信者情報である電子メールアドレスのドメインの DNS 上に、当該ドメイン名を用いる電子メールアドレスが用いる送信メールサーバーの IP アドレスなどの情報と、それらに該当した場合の認証結果を記号で示したものを記述し（SPF レコード）、受信メールサーバーで、受信する電子メールの電子メールアドレスのドメインの DNS を確認し、送信メールサーバーの IP アドレスが、当該 DNS で記述された IP アドレスと一致しているかを確認することにより、送信ドメインの認証を行う仕組みです。SPF で用いられる送信者情報は、配送上の送信者情報(Envelope-From、RFC5321.From[注101])です。また、SPF レコードの末尾には、認証結果を記号（-all、+all など）で指定でき、「-all」は送信者を詐称したメールと判断して認証失敗（fail）として扱うものであり、「+all」は正当な送信者から送信されたメールと判断して認証成功（pass）として扱うものです。

SPF の長所としては、送信側での導入コストがほぼ皆無であるなど、送信側での導入の容易さが挙げられます。一方、短所としては、自動転送（ユーザーの指定する宛先への転送や、メーリングリストでの複数の宛先への再配送など。）により、電子メールの送信メールサーバーが、元々の送信者が送信に使用したメールサーバーと異なる場合には、認証に失敗することがあるということが挙げられます。

図表３－２－１４　SPF の仕組み



[注100] https://tools.ietf.org/html/rfc7208

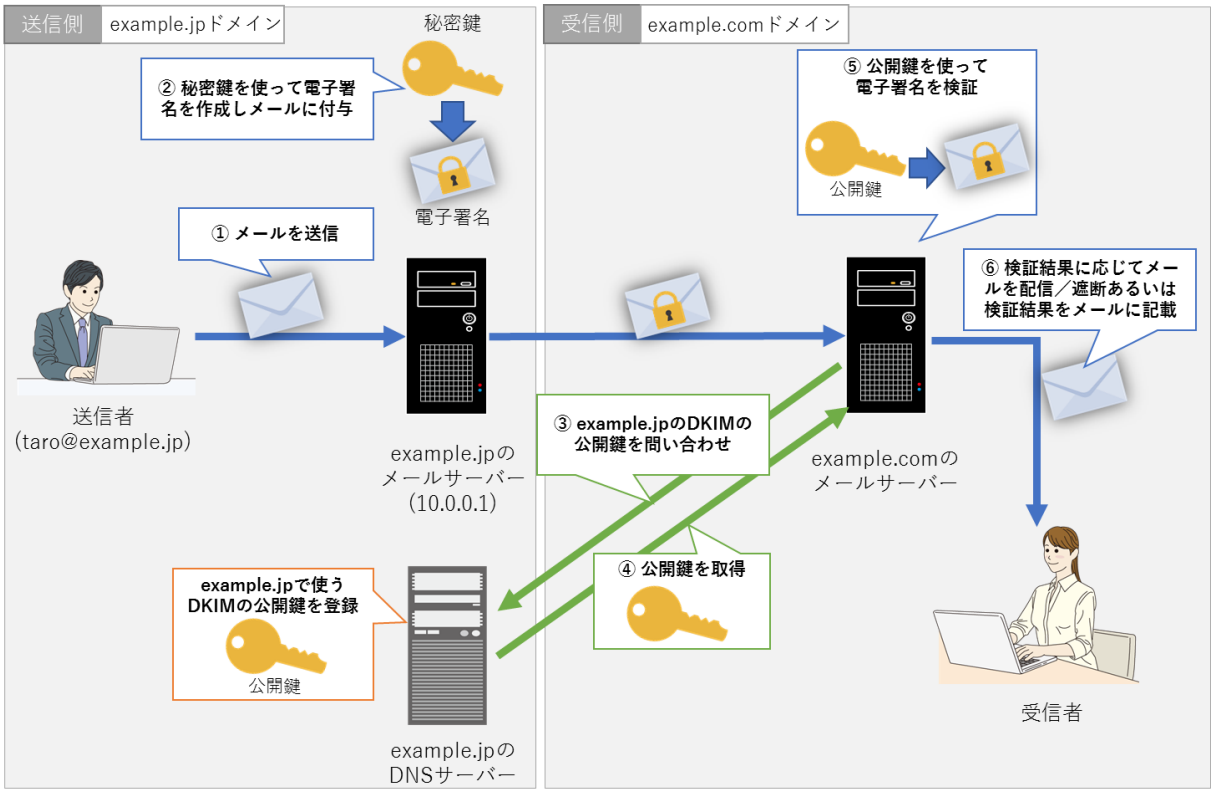
[注101] Envelope-From と同義。SMTP 上で伝達される送信者情報を指し、SMTP を規定した RFC5321 に由来する。

（２）DKIM（DomainKeys Identified Mail）

DKIM は、STD76[注102]で規定された、電子署名（公開鍵暗号技術）を利用して電子メールのなりすましを判断することができる技術です。具体的には、送信メールサーバーで、電子メールの送信時に、送信メールサーバーのみが保有する秘密鍵を用いて１通ずつ電子署名を作成し、メールヘッダーに関連情報とともに追記して送信するとともに、送信者情報である電子メールアドレスのドメインの DNS 上で、電子署名の検証に用いる公開鍵などを公開し、受信メールサーバーで、受信する電子メールの電子メールアドレスのドメインの DNS から公開鍵を入手して電子署名を検証することにより、送信ドメインの認証を行う仕組みです。

DKIM の長所としては、電子メールの配送経路によらない認証のため、ネットワーク方式の SPF とは異なり、自動転送などの場合でも正しく認証ができることと、送信ドメインの認証以外にも電子メールの本文の改ざんも検知できることなどが挙げられます。一方、短所としては、電子メールの送信ドメインが正しい場合でも、メーリングリストのように電子メールの本文などを変更するサーバーを経由したときは、認証に失敗することが挙げられます。

図表３－２－１５　DKIM の仕組み



（３）DMARC（Domain-based Message Authentication, Reporting & Conformance）

DMARC は、RFC7489[注103]で規定された、SPF や DKIM の認証結果を元にした技術で、大きく３点の特徴があるものです。一点目は、メールヘッダー上の送信者情報（ヘッダーFrom、RFC5322.from[注104]）について、電子メールのなりすましを判断することができることです。具体的には、DMARC では、SPF の認証および DKIM の認証に成功した配送上の送信者情報（Envelope-From、RFC5321.from）とメールヘッダーの送信者情報（ヘッダーFrom、RFC5322.from）とが一致した場合に、なりすましがないものと判断します。なお、SPF の認証と DKIM の認証をどのように用いるか（一方のみを用いるなど）については、送信者側で、送信者情報である電子メールアドレスのドメインの DNS 上で宣言することにより設定します。

注102 https://tools.ietf.org/html/std76

注103 https://tools.ietf.org/html/rfc7489

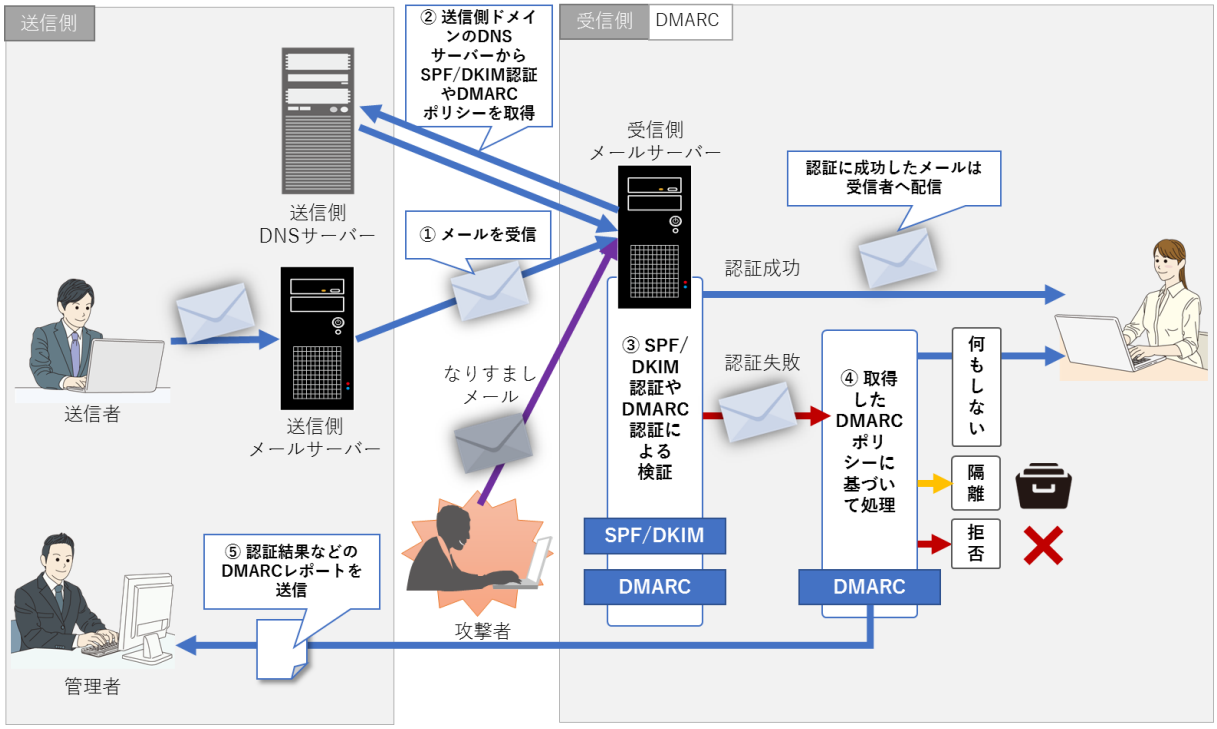
注104 ヘッダーFrom と同義。メールヘッダー上の送信者情報を指し、メッセージ形式を規定した RFC5322 に由来する。

二点目は、送信側が、認証に失敗した電子メール（なりすましメール）の処理方法を指定することができることです。具体的には、送信側は、認証に失敗した場合に、「何もしない（処理方法を指定しない）」、「隔離する」、「受信拒否する」の３つの処理方法を送信者情報である電子メールアドレスのドメインの DNS 上で指定し、受信メールサーバーでは、それを参照して取扱いを決定することができます。

三点目は、認証結果についてのレポートを送信側が電子メールで受け取るレポーティング機能です。具体的には、送信側では、送信者情報である電子メールアドレスのドメインの DNS 上で、レポートの送付先や送付頻度などを設定し、受信メールサーバーでは、それを参照して、指定された送付先（管理者）宛てに、認証結果のレポートを送付します。レポートには、一定期間における認証結果を記した「集約レポート」や認証に失敗した電子メールの情報を記した「失敗レポート」があります。送信側では、レポートを解析することで、自ドメイン名を詐称した電子メールの状況の把握や、適切な DMARC ポリシーの設定に活用することができます。

DMARC の長所としては、SPF と DKIM 双方の長所を生かした認証ができること、送信側の導入の容易さが挙げられます。一方、短所としては、再配送された場合など SPF と DKIM がともに認証に失敗するような場合には、DMARC の認証も失敗してしまうことが挙げられます。

図表３－２－１６　DMARC の仕組み



（４）その他（ARC：Authenticated Received Chain）

送信ドメイン認証技術は、再配送された電子メールについては正しく認証できない場合があるため、再配送された電子メールでも正しく認証できるようにするために考えられた技術が ARC です。ARC では、電子署名の技術を利用し、再配送された場合でも Authentication-Results ヘッダーを辿れるようにすることで、認証の結果を確認することができます。現在、ARC は標準化の検討が進められているところであり、今後、ARC と送信ドメイン認証技術が併用されることで、電子メールのなりすましがより確実に判断可能となることが期待されます。

第3節　利用者による対策

迷惑メール対策は、関係組織により、様々な取組が行われてきています。しかし、迷惑メール送信者はそれらの対策を潜り抜けて利用者まで迷惑メールを届けようとしていますので、利用者においても迷惑メール対策を講じることが肝要となります。本節では利用者が取ることが望ましい対策や注意すべき点について、簡単にお示しします。なお、詳細については、関連組織が作成した冊子などにまとめられていますので、そちらをご覧ください。

1　迷惑メールを受け取らないための対策

（1）電子メールアドレスを安易に公表しない

電子メールアドレスを不必要に公開しないようにしましょう。ホームページや掲示板で公開した電子メールアドレスを迷惑メール送信者が収集している場合があるので、電子メールアドレスを不必要に公開すると、迷惑メールが増加する可能性があります。特に、電子メールアドレスの収集を目的とした懸賞サイトや占いサイトなどもあるため、注意することが必要です。また、プロフィールサイトなどで、初期設定のまま利用すると、電子メールアドレスが公開される場合もあるため、注意しましょう。

（2）推測されにくい数字や記号を使った複雑で長い電子メールアドレスを使う

数字や記号を組み合わせた複雑で長い電子メールアドレスを用いましょう。迷惑メール送信者は、架空電子メールアドレスを作成し、無差別にメールを送信している場合があります。単純な電子メールアドレスの場合には、その送信先に含まれてしまう可能性が高くなります。このため、複雑で長い電子メールアドレスを用いることが有効です。

（3）不用意に同意しない

運営者が誰かもよく知らないウェブサイトを利用して、当該ウェブサイトなどの中に記載されている「今後、当サイトや関連サイトから広告宣伝メールを送信する」旨の表記に、同意をして、電子メールアドレスなどを運営者に通知すると、必要もない広告宣伝メールが大量に送信されてくることにつながることがあります。広告宣伝メールの送信に同意をする際には、十分注意した上で同意をすることを心がけましょう。

（４）携帯電話事業者や ISP などの迷惑メール対策サービスを利用する

携帯電話事業者や ISP などの提供するフィルタリングなどの迷惑メール対策サービスを利用しましょう。具体的な内容や利用条件などは、事業者により異なるため、事業者に確認の上、利用することをお勧めします。また、技術的な対策としての OP25B や送信ドメイン認証技術の事業者での導入状況については、(一財)日本データ通信協会のウェブサイト[注 105]でもご確認いただけます。

（５）セキュリティソフト、メールソフトの迷惑メール対策機能を利用する

セキュリティソフトやメールソフトの迷惑メール対策機能を利用しましょう。お使いのセキュリティソフトやメールソフトには、独自の迷惑メール対策機能を持っているものもあるため、そのような機能を利用することも有効です。

２　迷惑メールを受信してしまったときの対策

（１）開かない

受信した迷惑メールは、開かないようにしましょう。電子メールを開くだけでウイルスに感染することもありますので、電子メールを自動的に開くプレビュー機能は停止しておくようにしましょう。また、HTML メールでは、電子メールを開くだけでウェブへの接続が行われ、電子メールを閲覧したことなどの情報が送信者側へ伝わってしまうこともありますので、HTML メールを自動的に開くプレビュー機能を停止しておくことも重要です。

（２）クリックしない

迷惑メールに記載された URL やハイパーリンクの文字列からは、ウェブサイトへアクセスしないようにしましょう。ウェブサイトへアクセス後、高額な料金を請求する迷惑メールを受信するようになったケースがあります。また、アクセスすることで、受信した電子メールに記載した URL やハイパーリンクの文字列からウェブサイト閲覧したことなどの情報が送信者側へ伝わってしまい、その電子メールアドレスで受信する迷惑メールが増える可能性もあります。

（３）個人情報は入力しない

個人情報は入力しないようにしましょう。言葉巧みに電子メールの本文からウェブサイトに誘導し、そこで巧妙に口座番号、パスワード、クレジットカード番号などの個人情報を入力させるフィッシングと呼ばれる手口もあります。

注105 (一財)日本データ通信協会迷惑メール相談センター「各プロバイダ（ISP）、CATV(ケーブルテレビ）、モバイル事業者における OP25B 実施状況」https://www.dekyo.or.jp/soudan/contents/taisaku/i2.html

（4）心当たりのない電子メールには返信しない

送信者に心当たりのない電子メールには、返信しないようにしましょう。そのような電子メールの中にある連絡先に返信すると、反応した受信者として管理され、より多くの迷惑メールが届くようになる可能性がありますので、注意しましょう。

（5）チェーンメールは転送しない

チェーンメールは、転送しないようにしましょう。チェーンメールでは、善悪様々な内容により、メールを転送させようとしますが、転送することで、あなたから転送されたチェーンメールの受信者に不快な思いをさせてしまうことにもなりかねません。チェーンメールを転送しなかったら不幸なことが起きるのではなど不安な場合には、(一財)日本データ通信協会内にある迷惑メール相談センターではチェーンメール転送先アドレスを設けているので[注106]、そちらに転送してください。

（6）関連組織に情報提供する

迷惑メール相談センターで法律違反と思われる広告宣伝メールに関する情報提供を受け付けており、提供された情報は迷惑メール対策に活用されます。

3　自ら同意した広告宣伝メールへの対応

（1）オプトアウトを確実に実施する

受信不要になったメールマガジンなどについては、フィルタリングなどによって受信拒否設定をするのではなく、登録の解除（オプトアウト）を行いましょう。フィルタリングなどによって受信拒否設定をした場合には、送信側では、その電子メールが利用者にとって不要であることを認識できず、受け取られることのない電子メールが延々と送信され続けることになり、電気通信事業者のメール配送設備に余計な負荷がかかることになるためです。

（2）電子メールアドレスの変更を広告宣伝メール発行者にきちんと通知する

電子メールアドレスを変更したら、変更した電子メールアドレスを広告宣伝メールの送信者に通知しましょう。通知をしないと必要な広告宣伝メールが届かなくなるだけでなく、存在しない電子メールアドレス宛てに広告宣伝メールが延々と送信され続けることになり、電気通信事業者のメール配送設備に余計な負荷がかかることになるためです。

注106　(一財)日本データ通信協会迷惑メール相談センター「撃退！チェーンメール」P5 チェーンメールの転送先
https://www.dekyo.or.jp/soudan/chain/tensou.html#add

（3）ID、パスワードが送信者から付与されている場合は忘れないようにする

広告宣伝メールの送信に同意後、第三者が、正当な受信者が登録した受信用の電子メールアドレスを変更することやオプトアウトすることなどを防止するため、送信者から、ID、パスワードが付与されることがあります。この ID、パスワードは、受信用の電子メールアドレスの変更、オプトアウトなどに必要となるため、忘れないようにしましょう。

4　その他

（1）ウイルスに感染しないようにする

ウイルスに感染すると、気づかないうちに、自分のパソコンやスマートフォンから迷惑メールの送信が行われてしまうこともあります。セキュリティ上の脆弱性を修正し、ウイルスに感染しないようにするため、セキュリティソフトの利用、オペレーティングシステムなどのソフトウェアのアップデートを実施するとともに、信頼できないソフトウェアは利用しないことなどに注意しましょう。

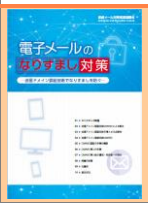
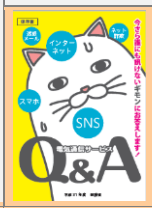
なお、セキュリティソフトは、未知の問題に対しては効果がありません。効果を過信して、危険なウェブサイトにアクセスしたり、添付ファイルをむやみに開いたりしないようにしましょう。また、セキュリティソフトも定期的にアップデートするよう心がけましょう。

（2）電子メールの送信に 587 番ポート（または 465 番ポート）を利用する

利用している ISP などが 587 番ポート（または 465 番ポート）での接続を提供しているときには、587 番ポート（または 465 番ポート）を利用するようにしましょう。インターネットへの接続のために利用している ISP 以外の ISP などから 25 番ポートを用いて電子メールを送る場合に、OP25B が実施され、結果的に送信できない場合があります。

インターネットへの接続のために利用している ISP のウェブサイトなどで対応方法を確認し、587 番ポート（または 465 番ポート）を利用するようにメールソフトの設定の変更などを行いましょう。

図表３－３－１　関係組織が発行している利用者向けの冊子など

関係組織	概要		入手方法
迷惑メール対策推進協議会		「電子メールのなりすまし対策」 DMARC などの送信ドメイン認証技術を紹介する冊子	迷惑メール対策推進協議会のウェブサイト[注107]からダウンロード
総務省		「インターネットトラブル事例集」 迷惑メールを含むインターネットトラブルの実例を挙げ、その予防法と対処法を紹介する冊子	総務省のウェブサイト[注108]からダウンロード
		「電気通信サービス Q&A」 迷惑メール対策を含む電気通信サービスを Q&A 方式で紹介する冊子	総務省のウェブサイト[注109]からダウンロード
(一財)日本データ通信協会迷惑メール相談センター		「撃退！迷惑メール」 迷惑メール対策全般を紹介する冊子	(一財)日本データ通信協会のウェブサイト[注110]からダウンロード
		「撃退！チェーンメール」 チェーンメール対策に特化して紹介する冊子	(一財)日本データ通信協会のウェブサイト[注111]からダウンロード
(独)国民生活センター		「見守り情報」 迷惑メールによるものを含む様々な悪質商法に関する情報を記したメールマガジン、リーフレット	・(独)国民生活センターのウェブサイト[注112]でメールマガジンに登録 ・リーフレットは同ウェブサイトからダウンロード
内閣サイバーセキュリティセンター（NISC）		「インターネットの安全・安心ハンドブック」 身近な話題からサイバーセキュリティに関する基本的な知識を紹介	内閣府サイバーセキュリティセンターのウェブサイト[注113]からダウンロード

注107 https://www.dekyo.or.jp/soudan/aspc/report.html#auth
注108 http://www.soumu.go.jp/main_sosiki/joho_tsusin/kyouiku_joho-ka/jireishu.html
注109 http://www.soumu.go.jp/main_sosiki/joho_tsusin/d_faq/index.html
注110 https://www.dekyo.or.jp/soudan/data/info/gmeiwaku_book.pdf
注111 https://www.dekyo.or.jp/soudan/data/chain/chainbook.pdf
注112 http://www.kokusen.go.jp/mimamori/index.html
注113 https://www.nisc.go.jp/security-site/handbook/index.html

図表３－３－２　携帯電話事業者が発行している利用者向けの冊子など

携帯電話事業者	概要		入手方法
(株)NTT ドコモ		「サービスカタログ＆基本設定ガイド（スマートフォン・タブレット・Android 用）」 迷惑メール対策を含む利用者向け冊子	・ドコモショップなどの店頭で配布 ・NTT ドコモのウェブサイト[注 114]からダウンロード
		「サービスカタログ＆基本設定ガイド（iPhone・iPad・iOS 用）」 迷惑メール対策を含む利用者向け冊子	・ドコモショップなどの店頭で配布 ・NTT ドコモのウェブサイト[注 115]からダウンロード
KDDI(株)		「設定＆サービスガイドブック（Andoroid 搭載端末向け）」 迷惑メール対策を含む利用者向けの冊子	au ショップなどの店頭で配布
		「設定＆サービスガイドブック（iPhone・iPad 向け）」 迷惑メール対策を含む利用者向けのリーフレット	
ソフトバンク(株)		「お子さまがスマートフォンを安全に楽しく使うために!!」 迷惑メール対策を含む利用者（特に保護者）向けの冊子	・ソフトバンクの講座にて配布 ・ソフトバンクのウェブサイト[注 116]からダウンロード

注114 https://www.nttdocomo.co.jp/support/utilization/maruwakari/index.html
注115 https://www.nttdocomo.co.jp/iphone/support/startup_guide/
注116 https://cdn.softbank.jp/corp/set/data/csr/responsibility/safety/rule/pdf/smartphone_guidebook.pdf

図表３－３－３　関係組織や携帯電話事業者が用意している迷惑メール情報提供先

関係組織や携帯電話事業者	迷惑メール情報提供先	備考
総務省	ウェブサイト[注117]から迷惑メール情報提供用プラグインソフトをダウンロードし、メールソフトに設定することで、情報提供が可能となる	プラグインソフトを設定可能なメールソフトの詳細はウェブサイトを参照のこと
(一財)日本データ通信協会 迷惑メール相談センター	meiwaku@dekyo.or.jp	左記の電子メールアドレスへ特定電子メール法に違反していると思われる電子メールを転送または添付形式により情報提供することが可能 また、ウェブフォーム[注118]を通じた情報提供も可能
(株)NTT ドコモ	imode-meiwaku@nttdocomo.co.jp	sp モード、i モードに対応したスマートフォンまたは携帯電話の場合（iPhone、iPad 除く）、受信した電子メールの表示画面のサブメニューなどから、迷惑メールの情報提供先アドレスへ直接転送可能 （SMS も同様　※スマートフォンでは+メッセージを利用）
KDDI(株)	au-meiwaku@kddi.com	Android 搭載スマートフォンの場合、au メールアプリより「迷惑メール報告機能」を利用し、受信した迷惑メールを迷惑メールの情報提供先アドレスへ直接転送可能 SMS は電話[注119]またはウェブフォーム[注120]により情報提供可能
ソフトバンク(株)	a@b.c（ソフトバンクの携帯電話からの情報提供用） stop@meiwaku.softbank.co.jp （ソフトバンクの携帯電話以外で、ソフトバンクの携帯電話からの迷惑メールを受信した場合）	iPhone 以外の Android 搭載スマートフォン、携帯電話の場合、受信した電子メール表示画面のサブメニューなどから、［迷惑メール申告］機能を利用し、受信した迷惑メールを迷惑メールの情報提供先アドレスへ直接転送可能（SMS も同様）

注117 http://plugin.antispam.soumu.go.jp/
注118 https://www.dekyo.or.jp/bingo/mail_ihan_meiwakuform/index.html
注119 迷惑メール受付センター（電話番号 0077-7089）（受付時間 平日 9:00～17:00）
注120 https://www.au.com/support/service/mobile/trouble/mail/common/report/

トピックス：通信の秘密と OP25B、送信ドメイン認証技術

（１）通信の秘密とは

日本国憲法第 21 条第２項では、通信の秘密を保障し、これを侵害することを禁じています。その趣旨を受け、電気通信事業法では、第４条で通信の秘密の侵害を禁じ、第 179 条でこれを侵害した場合の罰則を設けています。

> 日本国憲法（抜粋）
> 第 21 条　（略）
> ２　検閲は、これをしてはならない。通信の秘密は、これを侵してはならない。

> 電気通信事業法（抜粋）
> 第４条　電気通信事業者の取扱中に係る通信の秘密は、侵してはならない。
> ２　（略）
> 第 179 条　電気通信事業者の取扱中に係る通信（第 164 条第３項に規定する通信を含む。）の秘密を侵した者は、二年以下の懲役又は百万円以下の罰金に処する。
> ２・３　（略）

なお、通信の秘密に属する事項には、個別の通信に係る通信内容のほか、個別の通信に係る通信当事者の住所、氏名、発信場所、通信日時などの構成要素を含むとされ、さらに、通信の秘密を侵害する行為として、知得、窃用、漏えいが挙げられています。ただし、通信当事者の同意を得ることなく通信の秘密を侵害した場合であっても、違法性阻却事由がある場合には、例外的にこれを侵害することが許容されます。

（２）送信ドメイン認証技術等と通信の秘密の関係

送信ドメイン認証技術等と通信の秘密の関係について、総務省では次のとおり整理しています。なお、詳細は総務省のウェブサイト[注 121]をご参照ください。

OP25B と通信の秘密

通信当事者の同意なく OP25B を運用することは通信の秘密を侵害する行為に該当しますが、電気通信事業者の提供するメールサーバーを経由しない動的 IP アドレスからの大量送信が行われていることなどが認められる場合には正当業務行為と認められ、違法性が阻却されると考えることが可能と整理されています。

送信ドメイン認証技術と通信の秘密

通信当事者の同意なく送信ドメイン認証を行うことは通信の秘密を侵害する行為に該当するとしつつも、大量送信される迷惑メールにより生じるサービスの遅延などの電子メールの送受信上の支障のおそれを減少させるために実施する場合、送信ドメイン認証は正当業務行為と認められ、違法性が阻却されると考えることが可能と整理されています。

また、DMARC による処理は通信の秘密を侵害する行為に該当するとしつつも、利用者が随時、任意に設定変更できる等の条件を満たす場合は、約款等による包括同意に基づいて提供する場合であっても、利用者の有効な同意を取得したものと考えることが可能と整理されています。

注121 総務省「送信ドメイン認証技術等の導入に関する法的解釈について」
http://www.soumu.go.jp/main_sosiki/joho_tsusin/d_syohi/m_mail/legal.html

第４章

迷惑メール対策の取組

第1節　迷惑メール対策推進協議会の取組

1　概要

迷惑メール対策推進協議会（座長：新美育文明治大学名誉教授）は、迷惑メール対策の関係者間の緊密な連携を確保し、最新の情報共有、対策方針の検討、対外的な情報提供などを行うことにより、効果的な迷惑メール対策の推進を図ることを目的として、2008 年 11 月 27 日に発足しました。協議会には、実務的な問題に関わる情報共有、対策の検討などを目的とする幹事会、送信ドメイン認証技術の普及促進の強化を目的とする技術 WG（2009 年 10 月に設置され、2014 年 9 月までは送信ドメイン認証技術 WG）が設置されています。

2019 年 6 月現在、協議会の構成員は 55 名で、幹事会の構成員は 33 名となっています。

2　主な取組

協議会では、2008 年 11 月 27 日に開催された第 1 回総会において、迷惑メールの追放に向けた決意と具体的に講ずるべき措置などをまとめた「迷惑メール追放宣言」を採択しました。また、2011 年 10 月 7 日に開催された第 3 回総会において、「なりすましメール撲滅プログラム～送信ドメイン認証技術普及工程表～」を作成し、公表しています（2013 年には同プログラムの改訂版を公表）。

2009 年以降、幹事会を中心として「迷惑メール対策ハンドブック」を毎年作成しており、10 年目の 2018 年よりハンドブックの体裁等を改め、「迷惑メール白書」として作成しています。

技術 WG では、2009 年に「送信ドメイン認証技術導入マニュアル」を作成する（2011 年第 2 版作成）とともに、2011 年にリーフレット「電子メールのなりすまし対策－送信ドメイン認証技術でなりすましを防ぐ－」を作成する（2012 年第 2 版、2017 年第 3 版、2018 年第 4 版）など迷惑メール対策技術の普及の検討などを行ってきています。

2018 年度の協議会の活動内容としては、「迷惑メール白書 2018」を活用した迷惑メール防止技術の普及促進など、主に以下のような取組を行いました。

- 技術 WG の開催（2018 年 4 月、5 月、6 月、8 月、12 月、2019 年 1 月）
- 迷惑メール対策推進協議会第 11 回総会の開催（2018 年 7 月 10 日）
- 協議会として総務大臣より平成 30 年度の「情報化促進貢献個人等表彰」を受賞（2018 年 10 月）
- 「迷惑メール白書 2018」発行（2018 年 11 月）
  （全国の公立図書館や大学・高等専門学校などの図書館へ約 2,000 部を寄贈、全国の消費生活センターへの紹介活動など）
- 協議会 10 周年記念講演会開催（2018 年 11 月 8 日）
- 地方公共団体情報システム機構（J-LIS）主催の自治体 CSIRT 協議会技術講習会で送信ドメイン認証技術を講演（2019 年 2 月））

図表４－１－１　迷惑メール対策推進協議会第 11 回総会（2018 年 7 月 10 日開催）

第2節　行政による取組

1　特定電子メール法の執行状況

（1）2008 年改正までの執行状況（オプトアウト方式による規制）

特定電子メール法の 2008 年改正までのオプトアウト方式による規制の下で、総務大臣による行政処分（措置命令）が 6 件、警察による摘発が 4 件行われています。なお、同規制の下での措置命令の件数は年間平均 0.94 件でした。

（2）2008 年改正後の執行状況（オプトイン方式による規制）

特定電子メール法の 2008 年改正後のオプトイン方式による規制の下で、総務大臣及び消費者庁長官（2009 年 8 月以前は総務大臣）による措置命令は、2019 年 3 月末までに 54 件行われています。また、警察による摘発が 5 件行われており、2014 年 9 月には特定電子メール法第 7 条に基づく措置命令違反として初めての摘発が行われています。同規制の導入後は、措置命令の件数が年間平均 5.23 件と、オプトアウト方式による規制時の約 6 倍となっています。

2　特定商取引法の執行状況（電子メール広告に関するもの）

（1）2008 年改正までの執行状況（オプトアウト方式による規制）

特定商取引法の 2008 年改正までのオプトアウト方式による規制の下で、電子メール広告に関する行政処分が 8 件行われています。

（2）2008 年改正後の執行状況（オプトイン方式による規制）

特定商取引法の 2008 年改正後のオプトイン方式による規制の下で、未承諾電子メール広告に関する行政処分（指示）は、2019 年 3 月末までに 9 件行われています。

3　その他の取組

（１）特定電子メール法第 13 条に基づく研究開発等の状況の公表

総務省では、特定電子メール法第 13 条に基づき、毎年１回、「特定電子メール等による電子メールの送受信上の支障の防止に資する技術の研究開発及び電子メール通信役務を提供する電気通信事業者による導入の状況」と題し、移動系電気通信事業者及び固定系電気通信事業者の主な迷惑メール送受信防止対策（送信通数制限、送信ドメイン認証技術、OP25B など）の事業者ごとの提供状況を公表[注 122]しております。

図表４－２－１　固定系電気通信事業者の主な迷惑メール送受信防止対策の提供状況

事業者	主な送信防止対策		主な受信防止対策									
			送信ドメイン認証						メールの内容による判定			大量受信制限
			SPF/SenderID		DKIM/Domainkeys		DMARC					
	送信ドメイン認証	OP25B	ラベリング	フィルタリング	ラベリング	フィルタリング	ラベリング	フィルタリング	ﾌﾞﾗｯｸﾜｰﾄﾞ	メール容量	迷惑メールフィルタ	
D社	○	○	○	○	○	○	○	○	○	○	○	○
E社	○	○	○	○	○	○	○	○	○	○	○	○
F社	○	○	○	－	－	－	－	－	○	－	○	－
G社	○	○	－	－	－	－	－	－	○	○	○	－
H社	○	○	－	－	－	－	－	－	○	－	○	－
I社	○	○	－	－	－	－	－	－	○	－	－	－
J社	○	○	○	○	○	－	－	－	○	－	○	－
K社	○	○	○	－	○	－	－	－	○	○	○	－
L社	○	○	○	○	－	－	－	－	○	－	○	－
M社	○	○	○	－	○	－	－	－	○	○	○	○
N社	○	○	○	－	○	－	○	－	○	－	○	－
O社	○	○	○	－	○	－	○	－	○	○	○	－
P社	○	○	－	－	－	－	－	－	○	○	○	－
Q社	○	○	○	○	○	○	－	－	○	－	○	○
R社	○	○	－	－	－	－	－	－	○	－	○	－
S社	○	○	－	－	－	－	－	－	○	－	○	－

用語	内容
【主な送信防止対策】	
送信ドメイン認証（送信側）	自社のメールドメインから発信されるメールについて、メール受信側のサーバに対し、同社のサーバから送信されたメールであることを確認する手段を提供する。ドメイン詐称を防ぐ SPF、アドレス詐称を防ぐ SenderID とメールの電子署名を利用する DKIM がある。また、SPF と DKIM を認証を利用して統一的に処理する DMARC がある。
OP25B	ISP が自社のネットワークの動的 IP から相手方電子メールサーバの 25 番ポートに電子メールを送信することをブロック方法。
【主な受信防止対策】	
送信ドメイン認証（受信側）	受信したメールについてドメインが詐称されていないか送信側のサーバに問い合わせて確認する。ネットワークベースの SPF/SenderID と、電子署名を利用する DKIM がある。また、SPF と DKIM を認証を利用して統一的に処理する DMARC がある。
ブラックワード	送信者アドレス、件名等を組み合わせて受信拒否条件を設定できる。
メール容量	受信メールのサイズによる受信拒否設定ができる。
迷惑メールフィルタ	主にメールの内容を検査し、流通する迷惑メールから分析した情報に基づいて迷惑メールかどうかを判定し、受信拒否できる。
大量受信制限	大量の宛先不明のメール送信を行うサーバに対し、受信拒否等を行う。

出典：総務省「迷惑メール対策技術の開発及び導入状況についての公表」平成 29 年版の概要から抜粋

注122 公表資料は下記の総務省ウェブサイトの「迷惑メール対策技術の開発及び導入状況についての公表」のリンク先を参照のこと。
http://www.soumu.go.jp/main_sosiki/joho_tsusin/d_syohi/m_mail.html

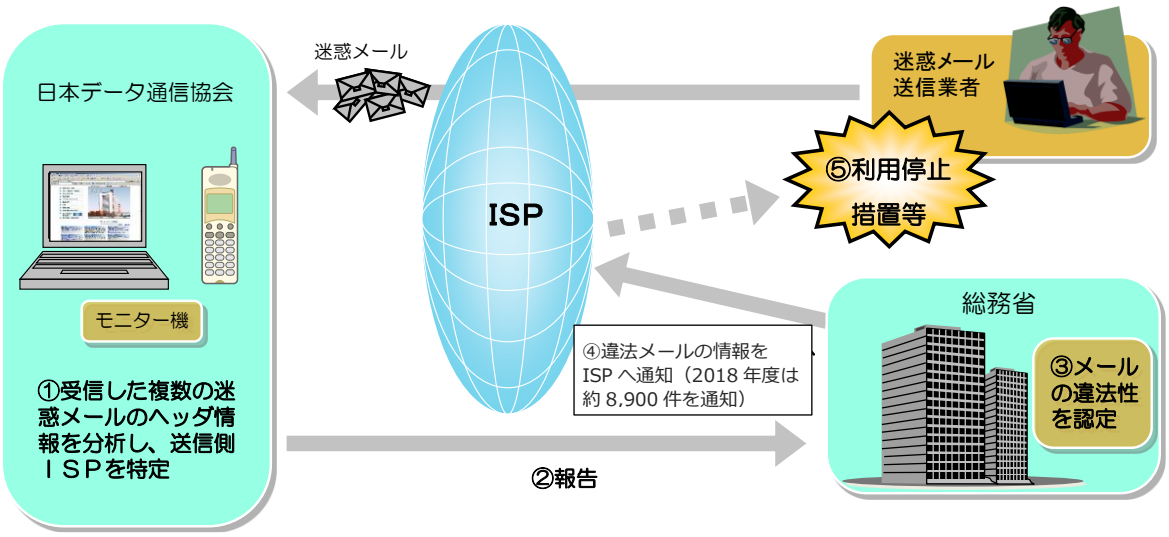
（２）迷惑メール追放支援プロジェクト

総務省および消費者庁は、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」を 2005 年から実施しています（2009 年に消費者庁発足する以前は、総務省および経済産業省が実施）。

（一財）日本データ通信協会が運用するモニター機で受信した電子メールのうち、特定電子メール法違反が確認された電子メールに関する情報を ISP に通知することで、契約約款などに基づく利用停止措置などを促しており、2018 年度は約 8,900 件の通知を実施しました。

図表４－２－２　総務省による迷惑メール追放支援プロジェクトの概要（特定電子メール法関係）

・2005年より、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」を開始。
・特定電子メール法に違反して送信されたメール（いわゆる迷惑メール）に関する情報をISPに通知することにより、迷惑メール送信者の利用停止措置等の円滑な実施を促す。



第3節　事業者による取組

1　携帯電話事業者の取組

我が国における携帯電話の契約数は１億７千万件を超え[注123]、普及率は全人口の 100%を超えるレベル（一人が複数台の携帯電話を持つケースがある）に達しており、インターネット利用者の 59.7%がスマートフォンによりそれを利用している状況にあります[注124]。

しかし、携帯電話のメールサービスは、いつも身近にある便利なコミュニケーションツールである反面、負の側面も問題となってきました。特に迷惑メールは、2001 年春頃から増加し、多くの苦情・相談が寄せられるようになったほか、利用者が金銭的な被害を受けるなど社会的に大きな問題となってきました。

携帯電話事業者では、携帯電話発・携帯電話着の迷惑メールの根絶を図ることを目的とし、以下のような、迷惑メールを「送信させない、受信させない」ための対策を実施しています。

（１）迷惑メールの被害者を減少させるための対策

メールアドレス変更機能

迷惑メールの受信対策の一つとして、迷惑メールの送信者に容易に推測されにくい電子メールアドレス（文字数の多い電子メールアドレス）を使用することが挙げられます。そこで、携帯電話事業者では、利用者が任意の電子メールアドレスへ変更することのできる機能を提供しており、万一、迷惑メールの送信者に「送信した電子メールが届く電子メールアドレス」として特定されたとしても、利用者の判断により、電子メールアドレスを変更できるようにしています。

なお、現在では、電子メールアドレスを変更できることは当たり前ですが、携帯電話による電子メールサービスが登場した初期の頃には、携帯電話の電子メールアドレスを電話番号と同一のものとする携帯電話事業者があり、迷惑メールの送信者が容易に電子メールアドレスを推測することが可能でした。

受信機能の拡充

利用者に届いてしまう迷惑メールを、携帯電話事業者側で一律に制限することは困難であるため、携帯電話事業者では、利用者の意思で特定のドメイン名や特定の電子メールアドレスから送信される電子メールのみを受信する機能（指定受信機能）や、それら電子メールの受信を拒否する機能（指定拒否機能）を提供しています。また、その他の代表的な受信拒否機能として、携帯電話のドメイン名になりすまして送信される電子メールを拒否する機能や、迷惑メールの特徴を学習して自動で受信拒否または受信フォルダーを振り分けるフィルター機能などがあり、迷惑メール対策として大きな効果をあげています。

注123 (一社)電気通信事業者協会「事業者別契約数」
https://www.tca.or.jp/database/index.html

注124 総務省「平成 29 年通信利用動向調査の結果」（2018 年６月 22 日）
http://www.soumu.go.jp/johotsusintokei/statistics/data/180525_1.pdf

利用者への啓発

携帯電話事業者では、迷惑メール対策サービスの利用方法などについて、契約後の確認通知書や請求書同封物、店頭配布ツール、ウェブサイト[注125]などを通じて、長期間に渡り継続的な啓発を実施しています。さらに、新聞、雑誌など各種媒体を用いた迷惑メール対策サービスの紹介、携帯電話販売店における適切な迷惑メール対策の設定の補助のほか、スマホ・ケータイ安全教室など[注126]を開催し、小中高等学校の生徒、保護者、教員向けに携帯電話を使う際のマナーやトラブルへの対処方法の啓発を行っています。

送信者への啓発

携帯電話事業者では、存在しない宛先への送信や短時間での大量の送信を控えること、また、宛先となる電子メールアドレスのスクリーニング（宛先リストに存在しないアドレスが含まれないようにすること）の励行など、送信者が電子メールの送信にあたって注意すべき点をウェブサイト[注127]を通じて周知し、適切な方法での送信を要請しています。これは、送信方法が適切でない場合には、設備保護の観点から該当の電子メールの送信を行ったISPやASPなどからの電子メールが一時的に届かなくなることもあるので、そのような事態を減らすために、送信者への啓発を行っているものです。

注125 ・(株)NTTドコモ「迷惑メールでお困りの方へ」
https://www.nttdocomo.co.jp/info/spam_mail/index.html
・KDDI(株)「迷惑メールフィルター設定（@au.com／@ezweb.ne.jp）」
https://www.au.com/support/service/mobile/trouble/mail/email/filter/
・ソフトバンク(株)「迷惑メールの対策」
https://www.softbank.jp/mobile/support/mail/antispam/

注126 ・(株)NTTドコモ「スマホ・ケータイ安全教室」
https://www.nttdocomo.co.jp/corporate/csr/safety/educational/
・KDDI(株)「スマホ・ケータイ安全教室」
http://www.kddi.com/corporate/csr/lesson/
・「考えよう、ケータイ 情報モラル教育を行う全国の先生方、保護者の方を支援します」
https://ace-npo.org/info/kangaeyou/index.html

注127 ・(株)NTTドコモ「同報メールを大量に送信されるお客様へ」
https://www.nttdocomo.co.jp/service/imode_mail/notice/mass_send/
・KDDI(株)「メール送信時のお願い」
https://www.au.com/mobile/service/attention/request/
・ソフトバンク(株)「メールを送受信する際の注意事項」
https://www.softbank.jp/mobile/support/mail/antispam/howto/wrestle/

（２）自社の契約者が迷惑メールの送信者にならないための対策

送信通数制限

迷惑メールが社会問題化していく中で、2003 年頃から携帯電話から発信される迷惑メールが顕著化しました。このような状況に対応するために、携帯電話事業者は、自社の契約者が迷惑メールの送信者とならないよう、一定期間に送信できる電子メールの通数を制限する措置（送信通数制限）を導入しました。これにより、携帯電話から送信される迷惑メールが抑制されました。

利用停止措置と迷惑メールに関する情報交換

携帯電話事業者では、自社の契約者から送信された迷惑メールに関する申告窓口を設け、迷惑メールの送信が確認された契約者に対して利用停止措置を実施しています。

2006 年３月１日からは、迷惑メールの送信により利用停止措置の対象となった契約者の情報を携帯電話事業者間で交換することで、携帯電話事業者を行き来して迷惑メールを送信する行為を未然に防ぐ取組が行われています。

さらに、2006 年４月１日からは、携帯音声通信事業者による契約者等の本人確認等及び携帯音声通信役務の不正な利用の防止に関する法律（携帯電話不正利用防止法）[注 128]に基づき、契約時や契約名義変更時に、契約者や譲受人などを公的証明書により本人確認することで、迷惑メールの送信に使用される可能性のある架空名義や名義貸しによる契約や名義変更を防いでいます。

2011 年７月 13 日からは、迷惑メールのうち SMS に関する申告情報を携帯電話事者間で交換する取組を行っており[注 129]、2016 年 10 月１日からは、SMS に限らず迷惑メールに関する申告情報も交換する取組を行っています[注 130]。これにより、迷惑メールの送信が確認された自社の契約者に対し、契約約款に基づく利用停止措置などを容易に講じることができるようにしています。

注128 総務省「携帯電話の犯罪利用の防止」
http://www.soumu.go.jp/main_sosiki/joho_tsusin/d_syohi/050526_1.html

注129 (一社)電気通信事業者協会「迷惑ＳＭＳに関する申告情報の取扱いについて」
https://www.tca.or.jp/mobile/sms-mail.html

注130 (一社)電気通信事業者協会「迷惑Ｅメールに関する申告情報の取扱いについて」（2016 年９月７日）
https://www.tca.or.jp/press_release/2016/0907_755.html

2　サービスプロバイダの取組

企業や個人に対して、電子メールの送受信機能を提供する電気通信事業者を、ここではサービスプロバイダと呼びます。近年は、ウェブブラウザ上で電子メールの送受信を行うウェブメールや、インターネットとの電子メールの送受信時に特定の機能を提供するゲートウェイ型サービス、メールの送受信も含めて全ての機能をクラウド上で提供するクラウド型のサービスなど、様々な形態のプロバイダーがあります。

サービスプロバイダにおける迷惑メール対策は、広告宣伝メール、フィッシングメール、ウイルス付メールなどの迷惑メールを、受信時に判断するフィルタリング機能を提供することが一般的となっています。また、近年では取引先等を詐称して金銭的被害を及ぼすビジネスメール詐欺（BEC [注131]）や、利用サービスを詐称して個人情報の搾取や金銭的被害につながるフィッシングなど、なりすましメールによる被害が増えています。こうした課題に対処するため、送信ドメイン認証技術を導入するなどの取組も行われています。

サービスプロバイダは、こうした新しい技術や各社の迷惑メールの状況について、迷惑メール対策推進協議会や（一財）インターネット協会の迷惑メール対策委員会などの業界団体に参加し、情報共有や対策方法について議論しています。また、国内だけでなく、海外においても、M^{3}AAWG [注132]などに参加し、会合で議論されている世界的な迷惑メールに関する新たな取組みや技術の紹介、普及に努めています。さらに 迷惑メール対策に関連する新しい技術については、IETF [注133]といった標準化組織の議論に参加するなど、グローバルにおいても様々な課題に取組んでいます。

なお、提供するサービスは、各サービスプロバイダによって異なるため、ここでは代表的な取組を受信時の対策と送信時の対策に分けて紹介します。

（1）電子メール受信側の対策

サービスプロバイダの多くは、受信側の対策として、適切に最新の対策技術を導入し、電子メールの利用者を悪質な迷惑メールから防ぐ努力をしています。

迷惑メールフィルターの提供

迷惑メールフィルターは、送信者情報や電子メールの内容、送信側の IP アドレスやドメイン名などから、迷惑メールか否かの判断をします。こうした迷惑メールフィルターの提供元は、日々様々な迷惑メールに関する情報を収集し、判断基準となるデータをいち早く提供することで、迷惑メールの受信を防ぐことができるようになっています。

迷惑メールと判断されたメールのフィルタリングの方法には、通常のメール受信領域以外の、いわゆるゴミ箱フォルダーといった別の領域に保存する方法や、受信前の隔離領域に保存し、メール受信者に配送をするかどうかを判断してもらう隔離方法、そもそもメールを受け取らないために、受信時にエラーコードを応答する方法など、様々あります。

[注131] BEC: Business Email Compromise

[注132] M^{3}AAWG: Messaging, Malware and Mobile Anti-Abuse Working Group

[注133] IETF: Internet Engineering Task Force

送信ドメイン認証と認証結果に基づく処理

送信ドメイン認証は、受信するメールの送信者情報の中のドメイン名が、正しい送信者から送られてきたかを確認する技術です。対象とする送信者情報や認証の仕組みの違いによって、SPF と DKIM の二つの技術があり、それらの認証結果を利用して、認証が失敗したメールを送信側のポリシー (処理方法) にしたがった処理が可能な DMARC へと発展してきました。

サービスプロバイダの中には、メール受信時に DMARC 認証を行い、認証結果を規格にしたがった形式でヘッダーに保存し、メール受信者に提示する機能を提供しています。さらに、こうした認証結果からキーワードフィルタなどを利用して認証が失敗したメールを隔離したり、DMARC のポリシーに従った処理 (フィルター) を実行する機能を提供しています。

しかしながら、図表４－２－１（P.85 の再掲）に示すとおり、ほとんどのサービスプロバイダが送信側に送信ドメイン認証を導入しているのに対し、受信側に導入しているサービスプロバイダは少ないのが実状です。

利用者への啓発

サービスプロバイダは、既存の利用者に新たに迷惑メールフィルターを導入したり、新たな迷惑メール対策機能を導入する際には、原則として利用者の同意を得る必要があります。こうした対策機能は、メール利用者を守る目的からサービスプロバイダは、なるべく多くの利用者に同意してもらえるよう、また適切に設定してもらうよう、導入する機能を利用者に適切に説明したり、それによる効果を正しく伝える努力が必要です。

このため、サービスプロバイダでは、ウェブメール上で視覚的に判断できるように表示したり、認証している場合に利用マニュアルなどで説明したりするなどにより、利用者に対する情報提供を行っています。

（２）電子メールの送信側の対策

電子メールの受信側の対策が強化されるに従い、電子メールが届きにくい状況も発生しています。サービスプロバイダの多くは、送信側としても迷惑メールなど不要なメール送信を検知する仕組みを導入したり、最新の技術に対応していくことで、利用者の電子メールが正しく届けられるように努力しています。

送信者認証（SMTP-AUTH）と踏み台利用対策

サービスプロバイダの多くは、送信者認証を導入しており、その認証結果とメール送信履歴を一定期間保存しています。これらの情報を利用し、送信者認証のための ID やパスワードを搾取されて送信メールサーバーが悪用 (踏み台利用)された場合に、利用された ID を一時的に利用停止したり、パスワード変更するなどの対策を行なっています。

利用者の ID とパスワードの不正利用を防ぐために、海外からのメール送信をあらかじめ禁止できる機能を提供しているサービスプロバイダもあります。利用者にこの機能を ON にしてもらうことで、海外からの踏み台利用を抑制することができます。

送信ドメイン認証

送信する電子メールを受信側に正しく判断してもらうために、サービスプロバイダの多くは、送信側としての送信ドメイン認証技術を導入しています。

具体的には、SPF や DMARC を導入している場合には、利用する送信側のドメイン名に対して SPF レコードと DMARC レコードを DNS サーバーに設定しています。DKIM を導入している場合には、送信メールサーバーに DKIM 署名追加機能を導入し、送信される電子メール１通ずつに電子署名を行っています。

また、送信ドメイン認証技術を導入した後も、受信側で常に正しく認証されるよう、メールシステムの変更時の設定情報の変更や、電子署名に用いる暗号鍵の定期的な交換などを行っています。DMARC による送信ドメイン認証が受信側での判断に適切に用いられるためには、送信される電子メールの送信者情報が適切に設定されている必要があるため、電子メールの投稿を受け付ける際に、不適切な送信者情報が設定されていないかを確認し、不正なドメインを利用している場合には受付を拒否する取組をしているサービスプロバイダもあります。

OP25B の実施

図表４―２―１（P.85 の再掲）のとおり、サービスプロバイダの多くは OP25B を導入することで、迷惑メールの送信を防いでいます。また、OP25B の導入にあわせて、メール投稿用サーバーでは 587 番ポート（または 465 番ポート）によるメール投稿ができるように設定するとともに、メールソフトウェア（MUA など）で適切な設定ができるように、利用者への周知を行っています。

図表４－２－１（再掲）　固定系電気通信事業者の主な迷惑メール送受信防止対策の提供状況

事業者	主な送信防止対策		主な受信防止対策									
	送信ドメイン認証	OP25B	送信ドメイン認証						メールの内容による判定			大量受信制限
			SPF/SenderID		DKIM/Domainkeys		DMARC		ﾌﾞﾗｯｸﾜｰﾄﾞ	ﾒｰﾙ容量	迷惑ﾒｰﾙﾌｨﾙﾀ	
			ラベリング	フィルタリング	ラベリング	フィルタリング	ラベリング	フィルタリング				
D社	○	○	○	○	○	○	○	○	○	○	○	○
E社	○	○	○	○	○	○	○	○	○	○	○	○
F社	○	○	○	－	－	－	－	－	○	－	○	－
G社	○	○	－	－	－	－	－	－	○	○	○	－
H社	○	○	－	－	－	－	－	－	○	－	○	－
I社	○	○	－	－	－	－	－	－	○	－	－	－
J社	○	○	○	○	○	－	－	－	○	－	○	－
K社	○	○	○	－	○	－	－	－	○	○	○	－
L社	○	○	○	○	－	－	－	－	○	－	○	－
M社	○	○	○	－	○	－	－	－	○	○	○	○
N社	○	○	○	－	○	－	○	－	○	－	○	－
O社	○	○	○	－	○	－	○	－	○	○	○	－
P社	○	○	－	－	－	－	－	－	○	○	○	－
Q社	○	○	○	○	○	○	－	－	○	－	○	○
R社	○	○	－	－	－	－	－	－	○	－	○	－
S社	○	○	－	－	－	－	－	－	○	－	○	－

用語	内容
【主な送信防止対策】	
送信ドメイン認証（送信側）	自社のメールドメインから発信されるメールについて、メール受信側のサーバに対し、同社のサーバから送信されたメールであることを確認する手段を提供する。ドメイン詐称を防ぐ SPF、アドレス詐称を防ぐ SenderID とメールの電子署名を利用する DKIM がある。また、SPF と DKIM を認証を利用して統一的に処理する DMARC がある。
OP25B	ISP が自社のネットワークの動的 IP から相手方電子メールサーバの 25 番ポートに電子メールを送信することをブロック方法。
【主な受信防止対策】	
送信ドメイン認証（受信側）	受信したメールについてドメインが詐称されていないか送信側のサーバに問い合わせて確認する。ネットワークベースの SPF/SenderID と、電子署名を利用する DKIM がある。また、SPF と DKIM を認証を利用して統一的に処理する DMARC がある。
ブラックワード	送信者アドレス、件名等を組み合わせて受信拒否条件を設定できる。
メール容量	受信メールのサイズによる受信拒否設定ができる。
迷惑メールフィルタ	主にメールの内容を検査し、流通する迷惑メールから分析した情報に基づいて迷惑メールかどうかを判定し、受信拒否できる。
大量受信制限	大量の宛先不明のメール送信を行うサーバに対し、受信拒否等を行う。

出典：総務省「迷惑メール対策技術の開発及び導入状況についての公表」平成 29 年版の概要から抜粋

利用停止などの取組

サービスプロバイダの送信メールサーバーは、電子メール利用者で共有して利用されています。そのため、一部の利用者が何らかの理由により迷惑メールの送信が続いた場合、多くの受信メールサーバーで、その送信メールサーバーからの受け取りが拒否されるようになります。これにより、ごく一部のメール利用者が原因で、多くのメール利用者がメール送信できなくなってしまいます。

迷惑メールが送信される理由としては、メール利用者が意図的に迷惑メールを送信する場合と、マルウェアなどに感染しボット化することで、外部の C&C サーバーなどからの指示によって送信する場合、前述したように利用者の ID とパスワードを搾取する場合など、いくつかのケースがあります。いずれにしても、利用者の同意に基づきこうした行為を検知した時点で当該利用者を一時的に利用停止することで送信を止め、利用契約を解除したり、PC でウイルスチェックしてもらったり、パスワードを変更してもらうなど、恒久的な改善のための措置を実施します。

サービスプロバイダが送信メールサーバーの不正利用を見つけるためには、短時間でのメール大量送信を検知したり、メールの投稿元を IP アドレスなどから調査し、短時間で極端に地理的に離れた場所から利用していないかを調べるなどの方法があります。また、ブラックリストに登録されていないか、メールの受信側から拒否されていないかを調べる方法もあります。さらに、迷惑メール送信に関するレポート（フィードバックループ）から不正利用されている利用者を特定する方法もあります。なお、以上いずれも利用者の同意に基づく必要があります。

利用者への啓発

サービスプロバイダでは、迷惑メールの送信などの不正利用を検知できる仕組みを用意する場合もあり、そうした対策を実施していることを利用者に周知・啓発しています。

3　セキュリティベンダーの取組

迷惑メール対策製品を開発、販売するセキュリティベンダーにおいては、迷惑メール数の減少および迷惑メールにより発生する被害の縮小を目的として、迷惑メール対策製品のサポート活動をはじめ、国内においては迷惑メール対策推進協議会やフィッシング対策協議会、また海外では M³AAWG などの迷惑メール対策について議論する場における活動などを行っています。

（1）迷惑メールの状況レポートの作成

セキュリティベンダーは、製品開発や迷惑メール対策フィルターで利用するデータの作成のために収集した情報をもとに、迷惑メールの流量・内容の傾向や被害の状況などをレポートとしてまとめ、定期的に公開しています。これらには、刻々と変化する迷惑メールの内容や送信方法など、迷惑メール対策に役立てることのできる情報が含まれています。

また、より迅速に迷惑メール関連情報を提供するため、ウェブサイト上で最新の情報を逐次報告しているセキュリティベンダーや、迷惑メールを送信しているメールサーバーや送信する可能性のあるメールサーバーの情報について、自社のウェブサイトや DNS サーバーなどで公開し、利用者が自由に参照・利用できるようにしているセキュリティベンダーもあります。

（2）迷惑メール対策の新技術の開発と取組

セキュリティベンダーの多くは、SPF、DKIM、DMARC などの送信ドメイン認証技術の開発や標準化などを行っている IETF [注134]に参加し、各種技術の開発や標準化を進めています。これらの技術は、迷惑メール対策に役立つことから、セキュリティベンダーが提供する製品に積極的に導入されています。

また、セキュリティベンダーは、IETF における標準化活動以外にも、M³AAWG などの迷惑メール対策を行う組織の活動に参加し、新技術の紹介、迷惑メール対策についての利用者からの要望のヒアリング、セキュリティベンダーの枠を超えた協調などを行っています。

（3）迷惑メール対策製品の性能向上

セキュリティベンダーが提供する製品・サービスにおいては、迷惑メールの検出性能向上が図られています。特に日本語の迷惑メールへの対策については、従来行われてきた特定の単語を検知する方法ではなく、数値データをパターン認識する方法など言語に依存しない検出技術が開発されており、実際に我が国で流通している迷惑メールの収集・解析を通じ、検出技術の性能向上が図られています。最近の傾向としては、迷惑メールであるか否かの判断にあたって、単一の迷惑メール検知技術に依るのではなく、複数の検知技術を用い、総合的に判断するものや、迷惑メールをリアルタイムで収集・分析し、その分析結果をもとに検知を行うものが多くみられます。

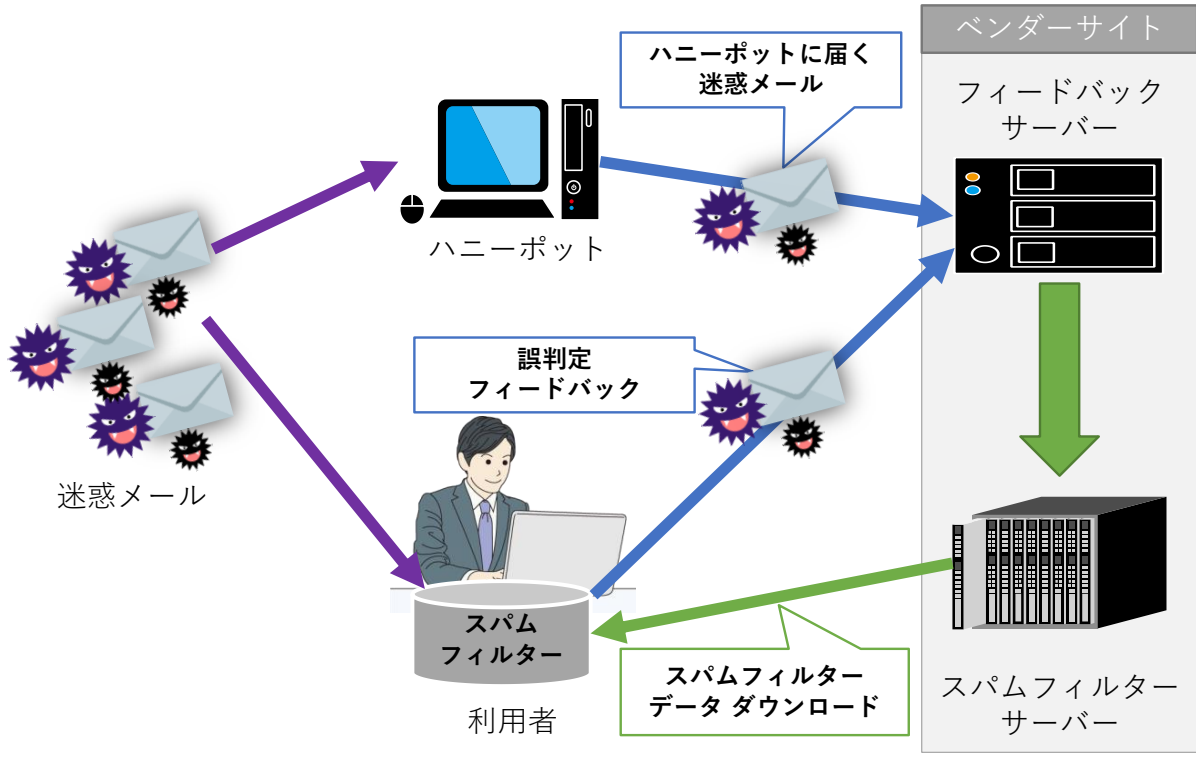
[注134] Internet Engineering Task Force の略称で、インターネット技術の標準化を推進する任意団体。

企業向けとしてはビジネスメール詐欺（BEC）など特に金銭を目的とした詐欺への対応やスピアフィッシング（特定の個人や企業を狙ったフィッシングのこと）などの一般に向けられた迷惑メールに対応するための機能を強化し、提供しているセキュリティベンダーもあります。

（４）迷惑メールのフィードバック窓口

実際に流通している迷惑メールを収集し、その分析結果を利用して迷惑メールの検出を実施している製品を提供しているセキュリティベンダーでは、迷惑メールのフィードバック窓口を設け、利用者からの、当該製品では検知できなかった新種の迷惑メールについての情報提供を受け付けています。迷惑メールの情報提供を簡単に行えるようプラグインツールを提供しているセキュリティベンダーもあります。各ベンダーはそれらのデータを分析し、迷惑メールの検出精度の向上に役立てています。

図表４－３－１　フィードバックを受けた迷惑メールの検出精度向上



4　配信サービス事業者の取組

（1）メール配信サービス事業者の取組

メール配信サービス事業者は、メールマーケティングを行う者など（電子メールの送信者）に対して、メール配信のシステムなどを提供しています。各社では、それぞれのサービス提供にあたって、迷惑行為に対する対応方針を定め、その内容をホームページに掲載するなどして、サービスが迷惑メールの送信に利用されないようにするとともに、より適切に電子メールの配信が行われるようにするなど、迷惑メール対策の取組みを実施しています。

契約時の確認

メール配信サービスが悪用され、迷惑メールの送信に用いられることがないようにするために、契約時に、申込み企業が実在するかどうかの確認やその企業の事業内容などの確認、送信側のドメイン名の登録確認（申込み企業がそのドメイン名を使う権限を有しているかどうかの確認）などを行っているメール配信サービス事業者があります。

また、特定電子メール法や特定商取引法上の表示義務など関係法令に反した運用が行われないようにするため、送信するメールの内容の確認やコンサルタントによる導入支援を行っているメール配信サービス事業者もあります。

送信リスト適正化のための機能の提供

メールマーケティングなどで電子メールの送付先のリストが適正に管理されていないと、アドレス変更などにより使われなくなった電子メールアドレスが残っていることもあります。そのような場合には、配信された電子メールが受信者に到達しない配信エラーになります。配信エラーを大量に含んだ電子メールの配信は、受信事業者の負担になるとともに受信制限の対象となる場合もあるため、配信エラー率を低下させるための取組が求められます。

個々のメール配信サービス事業者では、配信エラー率を低下させ、不要な電子メールの送受信を削減するために、エラーメール（配信エラーの際に受信側のメールサーバーから返送されてくるエラーの通知の電子メール）の分析・配信停止機能を提供するとともに、配信エラー率の高い送信者に対する送信リストの適正化の啓発や、一定以上のエラーメールが送信された場合の送信者への改善要請などの措置を行っています。

また、電子メールの受信者から迷惑メールであるとのフィードバックがあった場合や List-Unsubscribe による退会要求があった場合に自動で退会処理を行う機能を提供しています。

迷惑メールが送信された場合の対応

契約時の確認などにもかかわらず、メール配信サービスを利用して迷惑メールの送信が行われてしまうような事態に対応するため、大手のほとんどのメール配信サービス事業者では、迷惑メールの送信行為は契約約款上の禁止行為に該当することとして規定し、遵守状況を定期的に調査しています。また、迷惑メールの送信が確認された場合には、送信者への警告、利用停止、契約解除などの措置を実施しています。

技術的な対応

大手のほとんどのメール配信サービス事業者では、迷惑メールに対する技術的な対策の一つである送信ドメイン認証に関し、サービスを利用するメールマーケティングなどを行う事業者などが容易に設定できるように、SPF や DKIM、DMARC に関する設定方法の周知や設定内容の無料確認を実施しています。

また、送信ドメイン認証が正しく設定されていないため「なりすましメール」と誤解されることのないよう、メール配信用の操作画面上で送信ドメイン認証の設定状況を自動的に判断して、適切でない場合には警告を表示し、正しく設定されている状態でのみメール配信ができる安全装置のようなチェック機能や、送信に用いるドメインの運用をメール配信サービス事業者に委任することで、利用者にとって複雑な送信ドメイン認証の対応を容易にする機能などを提供している事業者もあります。

さらに、事前に申請されていない From アドレスからの送信の制限や、不適切な内容を含む電子メールが送信されていないかの確認などを行っているメール配信サービス事業者もあります。

その他の措置

2008 年に特定電子メール法および特定商取引法が改正され、オプトイン規制が導入されたことを受けて、ダブルオプトイン機能（通知などがなされた電子メールアドレスに対し広告・宣伝内容を含まない確認の電子メールを送付し、当該電子メールに対して返信などの受信者本人の操作があって初めてその後の特定電子メールについての同意を確定する機能のこと）、オプトインの記録保存機能などを提供しているメール配信サービス事業者もあります。

（2）SMS 配信サービス事業者の取組

SMS 配信サービスとは、携帯電話事業者のネットワーク内で配信が完結する個人間の SMS の配信と異なり、企業から個人向けに SMS を配信するサービス（A2P：Application to Peer）であり、企業から SMS の配信を受け付けて、携帯電話にメッセージを届けるサービスです。SMS の配信経路は、携帯電話事業者と直接国内網で接続している「国内 SMS 配信」と海外網経由の「国際 SMS 配信」の 2 経路があり、SMS 配信サービス事業者は、国内 SMS 配信サービス事業者と国際 SMS 配信サービス事業者に分類されます。

国内 SMS 配信サービス事業者は、それぞれのサービス提供にあたって、迷惑行為に対する対応方針を定め、事前審査を行うなどをして、サービスが迷惑 SMS の送信に利用されないようにするとともに、より適切な SMS 配信が行われるようにするなど、迷惑 SMS 対策の取組を実施しています。

契約時の確認

国内 SMS 配信サービス事業者は、SMS 配信サービスが悪用され、迷惑 SMS の送信に用いられることがないようにするために、契約時に、申込み企業が実在するかどうかの確認やその企業の事業内容などの確認および送信目的・用途などの事前確認を行っています。

迷惑 SMS が送信された場合の対応

契約時の確認などにもかかわらず、SMS 配信サービスを利用して迷惑 SMS の送信が行われてしまうような事態に対応するため、ほとんどの国内 SMS 配信サービス事業者では、迷惑 SMS の送信行為は契約約款上の禁止行為に該当することとして規定しています。迷惑 SMS の送信が確認された場合には、送信者への警告、利用停止、契約解除などの措置を実施しています。

技術的な対応

国内 SMS 配信サービス事業者は、迷惑 SMS が発生しないように、送信元企業の電話番号などを、SMS 送信時の発信元番号として登録し、送信しております。これにより、他者によるなりすましを防止するとともに、迷惑 SMS が発生した場合の送信者特定に寄与しています。

また、国内 SMS 配信サービス事業者は、原則としてアルファベットを送信者情報とした SMS 配信を許可しておりません。これは、海外から配信される SMS では、送信元情報を電話番号に限らず、任意のアルファベットを送信者情報とすることが可能であり、第三者を装った SMS の送信が容易であるためです。

第4節　関係組織による取組

1　(一財)日本データ通信協会　迷惑メール相談センター

（1）概要

(一財)日本データ通信協会では、2002 年 7 月に、迷惑メール相談センターを設置しました。センターでは、現在までに、以下の業務を通じて、電子メールの快適な利用環境作りに取り組んでいます。

（2）主な活動内容（括弧内の数値は 2018 年度の実績）

迷惑メールに関する電話相談受付

迷惑メールを受信して困っている方や、トラブルに巻き込まれそうになっている方などからの相談を電話で受け付け、対処方法や適切な相談窓口を案内しています（3,088 件）。なお、最近では、広告宣伝メールに関する相談以外では、架空請求に関する相談が多く寄せられています。

迷惑メールの収集

センターで設置したモニター機により迷惑メールを収集（約 69 万件）するとともに、迷惑メールを受信した方から特定電子メール法に違反していると思われる電子メールの提供を受け付けることでも収集しています（約 1,756 万件）。

迷惑メールの分析

収集した迷惑メールについて、その内容などを確認し、特定電子メール法違反の有無、送信元 ISP（モニター機で受信する直前のサーバーを管理する ISP）、発信国などの分析を行っています。分析結果は、総務省および消費者庁へ報告し、両省庁による特定電子メール法の執行に活用されています。

関係機関への情報提供

（ア）迷惑メール追放支援プロジェクトへの協力

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」に協力し、収集した迷惑メールのうち特定電子メール法違反に当たる電子メールに関する情報を、総務省との連名で、送信元 ISP に通知し（約 8,900 件）、送信者への警告や利用停止措置などの契約約款に基づく措置を促しています。

（イ）外国執行機関への情報提供

特定電子メール法違反の電子メールのうち、カナダから送信されたものについては、法第 30 条に基づき、総務省を通じて迷惑メール対策にあたるカナダの執行機関へ情報提供を行うことで、当該国の制度に基づく送信者への対応を促しています。

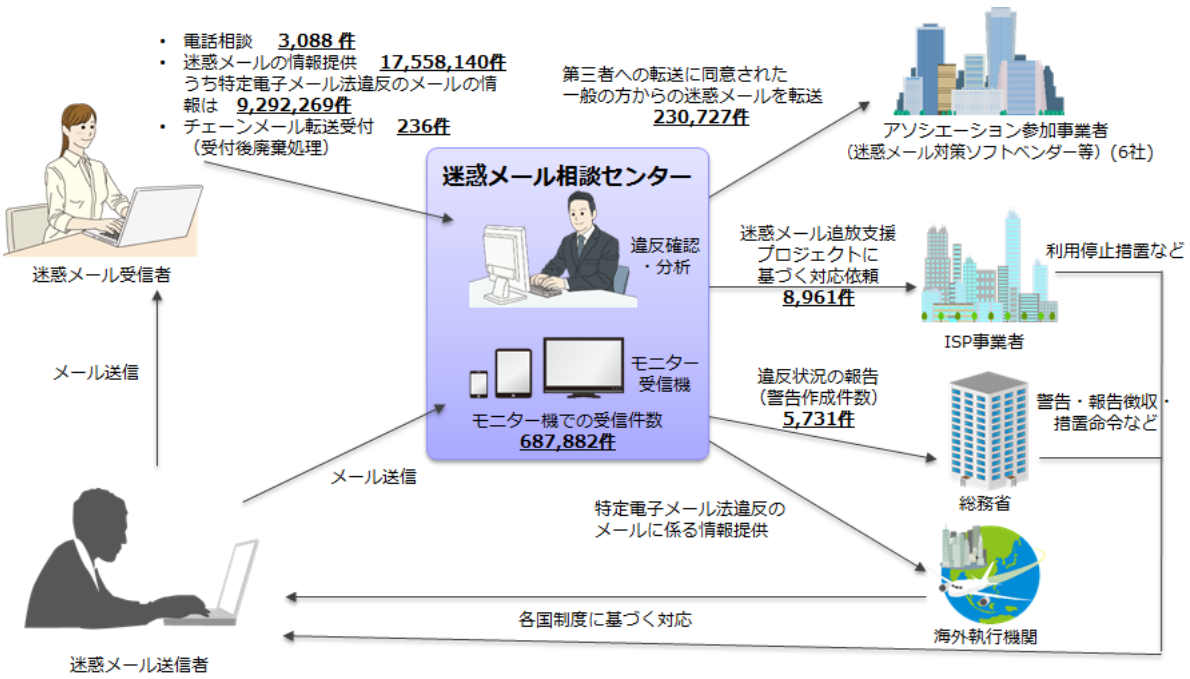
セキュリティベンダーなどへの情報提供

2008 年 1 月に迷惑メール情報共有アソシエーションを設立し、協力者から提供された迷惑メールをセキュリティベンダーをはじめとするアソシエーション参加事業者に提供しています（約 23 万件）[注 135]。このアソシエーションでは、アソシエーション参加事業者への情報提供に同意した方から提供された迷惑メールを参加事業者に提供することで、迷惑メール対策製品の開発などに役立てることを目的にしています。

一般消費者への周知・啓発

迷惑メール対策の周知・啓発活動として、センターのウェブサイトにおいて、迷惑メール対策の紹介、調査研究成果の公表などを行っています。また、迷惑メール対策やチェーンメール対策などについての各種パンフレットの作成・配布を行っています。

図表４－４－１　迷惑メール相談センター活動模様



その他、迷惑メール対策に関する周知啓発活動

・「くらしフェスタ東京2018」等への出展
・ホームページを通じた相談事例、対策の案内
・周知啓発資料（「撃退！迷惑メール「撃退！チェーンメール」」）の作成、配布（消費者相談窓口、学校関係者などへ）

[注135] (一財)日本データ通信協会「迷惑メール情報共有アソシエーション」
https://www.dekyo.or.jp/soudan/contents/sinfo/index.html

２　(一財)インターネット協会　迷惑メール対策委員会

（１）概要

(一財)インターネット協会では、2004 年から、ISP などメールサービスに関わる事業者、学識経験者を含むメンバーにより迷惑メール対策委員会を構成し、様々な活動を行っています。委員会は、2011 年度に一定の成果が得られたことを理由に活動を休止しましたが、2013 年度から新たな迷惑メール対策技術の普及が必要と判断し、活動を再開しているところです。

（２）主な活動内容

定例会合を通じた情報共有など

月一回程度の定例会合を開催し、DMARC をはじめとするとする迷惑メール対策技術などの普及状況や設定状況に関する情報共有、迷惑メール対策カンファレンスの企画検討、その他の迷惑メール対策に関わる各種イベントやメールサービスの状況などの情報共有を行っています。

迷惑メール対策カンファレンスの開催

委員会が継続して取り組んでいる代表的なイベントとして迷惑メール対策カンファレンスがあり、カンファレンスでは、様々な立場の方が参加し、情報共有や活発な議論が行われているところです。カンファレンスは、2014 年には迷惑メール対策を行う各国の執行機関などによる会合である LAP (現 UCENet [注136]) の第 10 回会合 (LAP10 TOKYO) と併催し、2015 年からは、複数のセキュリティ関連イベントを集中的に開催する「Security Week」において、ESC [注 137]を東京と大阪で合同開催し、2018 年は国際的なセキュリティ対策団体である M^{3}AAWG [注138]の日本の地域ワーキンググループ JPAAWG [注139]の立ち上げイベントと併催したことで、参加者の層がより幅広くなり、迷惑メール対策の周知・啓発活動に役立てられています。

注136 Unsolicited Communications Enforcement Network
注137 Email Security Conference の略称で、(株)ナノオプト・メディアが主催し、主に電子メールに関するセキュリティを取り扱うイベント
注138 Messaging, Malware and Mobile Anti-Abuse Working Group
注139 Japan Anti-Abuse Working Group

図表４－４－２　第 18 回迷惑メール対策カンファレンス（東京）の様子

有害情報対策ポータルサイト迷惑メール対策

迷惑メール対策に関わる様々な情報を提供する「有害情報対策ポータルサイト迷惑メール対策編[注 140]」を運営しています。DMARC の技術規格である RFC7489、メール配信事業者・ISP およびメールボックスプロバイダー・ブロックリストのベストプラクティス (M³AAWG の技術文書) の翻訳、ドイツのインターネット産業団体である eco が公表しているドイツ法における DMARC 準拠に関する報告の翻訳（英日対訳）をポータルサイトへ掲載しています。

また、(一財)インターネット協会も作成に協力した「なりすまし対策のポータルサイト　ナリタイ[注141]」のリンク情報などについても掲載しています。

国際連携

電子メールを健全化していくためには、グローバルでの連携が欠かせません。今後も、M³AAWG や DMARC を推進する組織である DMARC.org [注 142]など、迷惑メール対策および対策技術に関係する組織と様々な形で連携して活動していきたいと考えています。

注140 (一財)インターネット協会「有害情報対策ポータルサイト　－迷惑メール対策編－」
http://salt.iajapan.org/wpmu/anti_spam/
注141 なりすまし対策のポータルサイト　ナリタイ　https://www.naritai.jp/
注142 DMARC.org のウェブサイト　https://dmarc.org/

3　(独)国民生活センター

（１）概要

(独)国民生活センター（以下、「センター」という）は、1970 年 10 月に特殊法人国民生活センターとして発足し、その後「独立行政法人 国民生活センター法」に基づき、2003 年 10 月に独立行政法人に移行しました。

センターでは、「消費者基本法」に基づき、関係省庁や全国の消費生活センターなどと連携して、消費者問題における中核的機関としての役割を果たすため、消費生活に関する情報を収集し、消費者被害の未然防止・拡大防止に役立てています。また、消費生活センターなどが行う相談業務を支援するとともに、裁判外紛争解決手続（ADR）を実施しています。さらに、苦情相談解決を図る商品テストや、広く問題点を情報提供するための商品群のテスト、地方自治体の消費者行政担当職員・消費生活相談員などを対象とした研修、生活問題に関する調査研究を実施し、様々なメディアを介して消費者への情報提供を積極的に行うなど、一人一人の消費者が安全かつ安心な生活を送れるよう努めています。

（２）主な活動内容

PIO-NET（パイオネット：全国消費生活情報ネットワークシステム）

近年の消費者を取り巻く社会環境は、サービスの多様化や情報化、グローバル化などの進展により大きく変化しています。それに伴い、消費生活をめぐる問題も多様化・複雑化しています。

センターでは今後ますます、多様化・複雑化する消費者被害に迅速に対処するため、全国の消費生活センターなど（約 1,250 箇所）とオンラインネットワークで結び、消費生活に関する相談情報を蓄積する PIO-NET（パイオネット：全国消費生活情報ネットワークシステム）と呼ばれるデータベースを運営しています。収集された情報は、行政機関による消費者被害の未然防止・拡大防止のための法執行への活用、国や地方公共団体の消費者政策の企画・立案および国民への情報提供、地方公共団体の消費生活相談業務に対する支援などに活用されています。

迷惑メールに関する消費者への注意喚起

全国の消費生活センターなどには、年間約 90 万件もの様々な消費生活相談が寄せられていますが、その中には希望していないのに携帯電話やパソコンなどに届く迷惑メールなどに関する相談が多数みられます。

特に 2014 年度以降、迷惑メールに関する相談件数が増加し、2016 年度は約 4 万 5,000 件、2017 年度は約 5 万 4,000 件と増加しましたが、2018 年度は約 3 万 7,000 件に減少しています（2019 年 3 月時点）。

なお、センターでは 2017 年 7 月 6 日に迷惑メールに関する最新の相談事例やアドバイスをまとめ、消費者に注意を呼びかけました[注 143]。

[注143] 国民生活センター「心当たりのないメール・SMS には反応しないで！ –“迷惑メール”に誘導されてトラブルに！？ –」（2017 年 7 月 6 日）　http://www.kokusen.go.jp/news/data/n-20170706_1.html

また、電子メール・ＳＭＳ（ショートメッセージサービス）の他、ハガキ、封書、電話といった様々な通信手段で消費者のもとに届く架空請求に関する相談は、2016 年度は約８万件でしたが、2017 年度に急増し、2018 年度（2019 年３月時点）は 20 万件以上の相談が寄せられたことから、センターでは 2019 年４月 11 日に架空請求に関する最新の相談事例やアドバイスをまとめ、消費者に注意を呼びかけました[注144]。

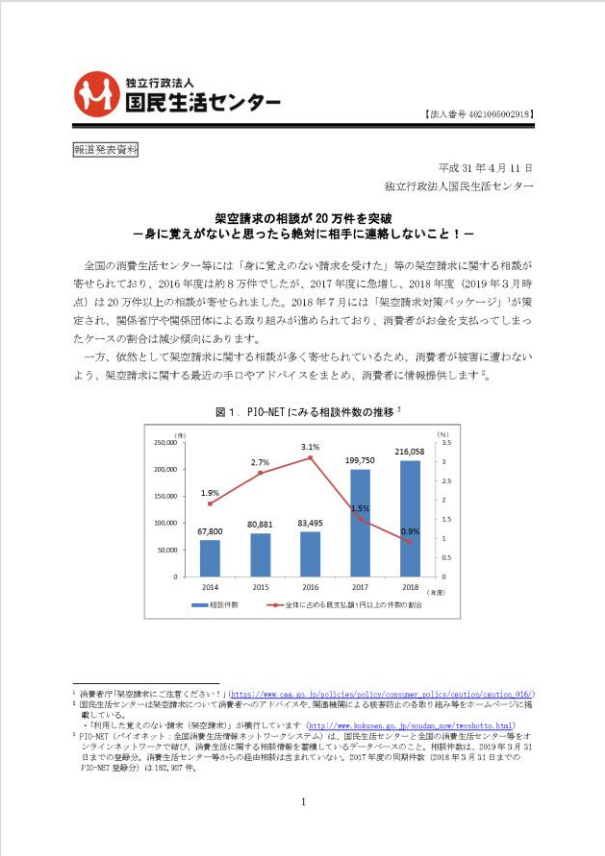
その際、消費者へのアドバイスとして、身に覚えがなければ絶対に連絡しないよう呼びかけました。あわせて、架空請求か判断がつかず不安に思ったり、執拗な請求等のトラブルにあった場合には、すぐに消費生活センターや警察へ相談をするよう注意喚起を行いました。

※消費者ホットライン：「188（いやや！）番」

最寄りの市町村や都道府県の消費生活センター等をご案内する全国共通の３桁の電話番号です。

※警察相談専用電話：＃9110

図表４－４－３　報道機関向けの公表資料



独立行政法人
国民生活センター
【法人番号 4021005002918】

報道発表資料

平成 31 年４月 11 日
独立行政法人国民生活センター

架空請求の相談が 20 万件を突破
－身に覚えがないと思ったら絶対に相手に連絡しないこと！－

全国の消費生活センター等には「身に覚えのない請求を受けた」等の架空請求に関する相談が寄せられており、2016 年度は約８万件でしたが、2017 年度に急増し、2018 年度（2019 年３月時点）は 20 万件以上の相談が寄せられました。2018 年７月には「架空請求対策パッケージ」[1]が策定され、関係省庁や関係団体による取り組みが進められており、消費者がお金を支払ってしまったケースの割合は減少傾向にあります。

一方、依然として架空請求に関する相談が多く寄せられているため、消費者が被害に遭わないよう、架空請求に関する最近の手口やアドバイスをまとめ、消費者に情報提供します[2]。

図１．PIO-NET にみる相談件数の推移[3]

[1] 消費者庁「架空請求にご注意ください！」（https://www.caa.go.jp/policies/policy/consumer_policy/caution/caution_016/）
[2] 国民生活センターは架空請求について消費者へのアドバイスや、関連機関による被害防止の各取り組み等をホームページに掲載している。
・「利用した覚えのない請求（架空請求）」が構行しています（http://www.kokusen.go.jp/soudan_now/twoshotto.html）
[3] PIO-NET（パイオネット：全国消費生活情報ネットワークシステム）は、国民生活センターと全国の消費生活センター等をオンラインネットワークで結び、消費生活に関する相談情報を蓄積しているデータベースのこと。相談件数は、2019 年３月 31 日までの登録分。消費生活センター等からの経由相談は含まれていない。2017 年度の同期件数（2018 年３月 31 日までの PIO-NET 登録分）は 182,967 件。

1

図表４－４－４　メールマガジンによる注意喚起

見守り新鮮情報

事例1　「消費料金に関する訴訟最終告知のお知らせ」と書かれたハガキが届き、電話をしたら、弁護士を名乗る者を紹介され、指示に従いコンビニで支払い番号を伝えて取り下げ料10万円を支払った。（60歳代　女性）

事例2　大手通販会社の名前でSMSが届き、身に覚えがなかったが、連絡しないと法的措置を取るとあったので電話をしたら、未納サイト料金を請求された。19万円、さらに50万円分のプリペイドカードを購入し、番号を伝えて支払った。（60歳代　男性）

架空請求
心当たりのない請求は無視!

ひとこと助言

●架空請求の請求手段は、電話、ハガキ、メール、SMS（ショートメッセージサービス）など様々です。
●実在の事業者名をかたって本物と思わせたり、法的措置を取るなどと記載をしたり、消費者の不安をあおるケースも見られます。
●架空請求は消費者の情報を完全に特定して送られているわけではありません。連絡してしまうと個人情報が知られ、その情報を元にさらに金銭を要求される可能性があります。未納料金を請求されても心当たりがなければ決して相手に連絡してはいけません。
●不安に思ったら、すぐにお住まいの自治体の消費生活センター等にご相談ください（消費者ホットライン 188）。

見守るくん

本文イラスト：黒崎 玄

見守り新鮮情報　第310号（2018年6月12日）発行：独立行政法人国民生活センター

注144 国民生活センター「架空請求の相談が 20 万件を突破－身に覚えがないと思ったら絶対に相手に連絡しないこと！－」（2019 年４月 11 日）http://www.kokusen.go.jp/news/data/n-20190411_2.html

４　フィッシング対策協議会

（１）概要

2005 年 4 月に発足したフィッシング対策協議会は、国内におけるフィッシング詐欺被害を抑制することを目的に各種活動を行っています。

2019 年 3 月末現在、協議会には正会員 52 社と賛助会員 24 社、他に、リサーチパートナー6 名とオブザーバー7 団体、関連団体 14 団体が参加しています。

（２）主な活動内容

フィッシングメールやフィッシングサイトに関する注意喚起や情報提供

フィッシング対策協議会では、会員や一般消費者などからフィッシングメールやフィッシングサイトの報告を受け、誤ってフィッシングサイトへアクセスしないように注意喚起を行っています。また、フィッシングサイトの停止を目的に、調整機関である一般社団法人 JPCERT コーディネーションセンター（JPCERT/CC）や関係組織にフィッシングサイトを報告しています。さらに、JPCERT/CC と連携し、セキュリティ対策事業者等にフィッシング URL を共有し、検知・ブロック機能のベースとなる情報として活用してもらうなどの対策も進めています。

ワーキンググループ活動

フィッシング対策協議会には、正会員が参加することができるワーキンググループ（以下、WG）があります。現在、技術・制度検討策定 WG、STOP. THINK. CONNECT.（STC）普及啓発 WG、証明書普及促進 WG、認証方法調査・推進 WG の 4 つの WG があり、フィッシング詐欺対策に資するガイドラインの更新、啓発イベントの開催、啓発ドキュメントの策定等の活動を主導しています。2018 年 6 月、技術・制度検討 WG（旧称：ガイドライン策定 WG）が策定した「フィッシング対策ガイドライン 2018 年度版」を協議会ウェブサイトで公開しました。また、2019 年 2 月から 3 月にかけて、協議会の STC 普及啓発 WG と日本クレジットカード協会とが協業し、サイバー犯罪被害防止啓発を目的としたポスターキャンペーンを実施しました。さらに、証明書普及啓発 WG では、SSL サーバー証明書の各ブラウザでの表示の違いや、DV・OV・EV の各サーバー証明書の具体的なユースケースなどを協議会ウェブサイトで公開し、適宜更新しています。

図表４－４－５　サイバー犯罪被害防止啓発キャンペーンのポスター

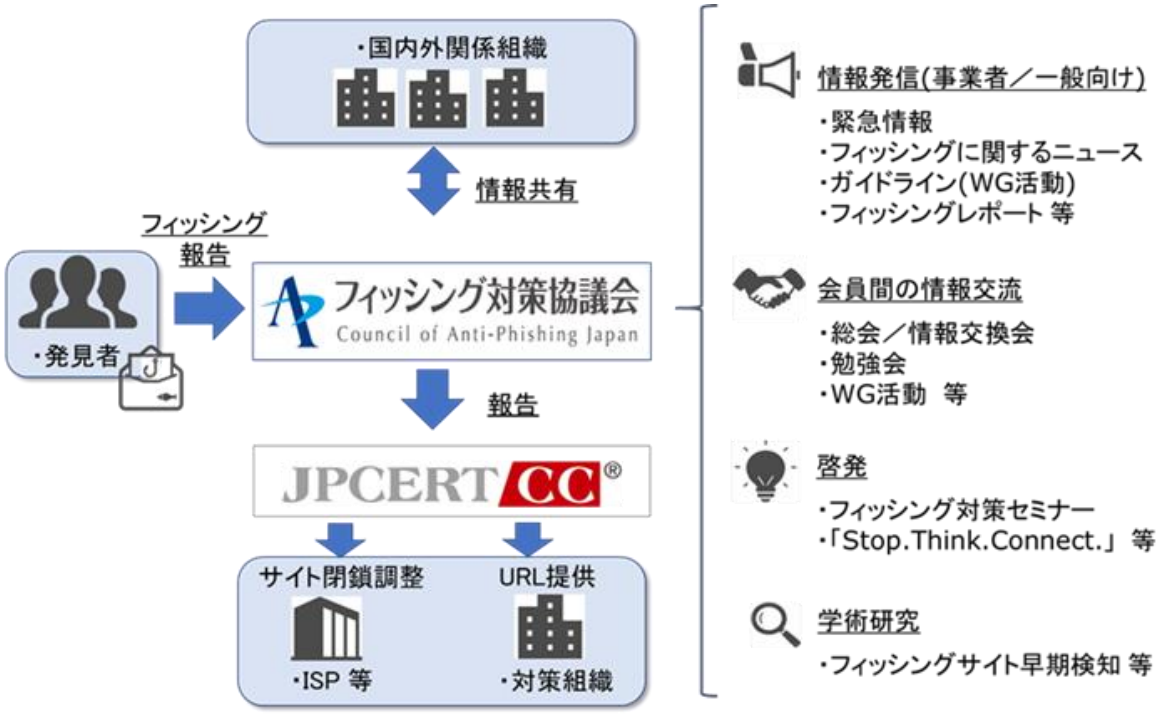
セミナーおよび勉強会の開催

フィッシング対策協議会では、会員や一般の方々に対して、年に数回、セミナーおよび勉強会を企画しています。2018 年は、事業者側のフィッシング詐欺対策促進を図るべく、有識者を講師に招き、複数回のセミナーおよび勉強会を開催しました。

学術研究プロジェクトの実施

フィッシング対策協議会では、2017 年 10 月から長崎県立大学と連携し、産学共同研究プロジェクトとして「フィッシングサイトの早期発見に関する研究」 を行っています。攻撃者がフィッシングサイトを準備する際のドメイン登録の手法に着目し、フィッシングサイトが公開される前に検知する手法の研究です。2018 年 3 月、情報処理学会第 80 回全国大会において、研究経過を発表しました。

図表４－４－６　フィッシング対策協議会の活動イメージ



5　（一財）日本情報経済社会推進協会（JIPDEC）　インターネットトラストセンター

（１）概要

JIPDEC は 1967 年よりわが国の情報化推進の一翼を担い、技術的・制度的課題の解決に向けた様々な活動を展開しています。特に、安心・安全な情報利活用環境の構築を図るため、プライバシーマーク制度の運用、「サイバー法人台帳 ROBINS」や「JCAN 証明書」、「JCAN トラステッド・サービス登録」などのインターネットトラスト事業、オープンデータや個人情報の取り扱いなど情報の保護と活用に関する調査研究・政策提言などを行っています。インターネットトラストセンターはインターネット空間上で、個人、法人、モノなどの実在性およびそれらの属性などを証明する仕組みを提供することにより、インターネットの信頼性の確保に取り組んでいます。

（２）主な活動内容

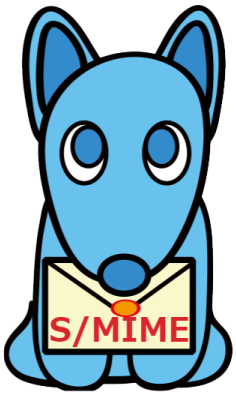
迷惑メール対策技術の普及啓発

各種後援イベントなどで啓発チラシを配布したり、イベントや研修などで講演をしたり、各種コラムや誌面にて、迷惑メール対策について紹介しています。

主なイベント（各種セキュリティイベント、自治体職員向け研修など）

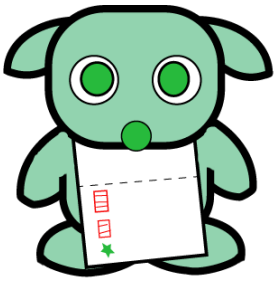
S/MIME、DKIM、DMARC と一見難しそうななりすましメール対策技術に、それぞれのマスコットキャラクターを作成し、親しみを持たせています。

図表４－４－７　S/MIME、DKIM、DMARC のマスコットキャラクターのイメージ



エスマいぬ
（S/MIME）

ディーキぃぬ
（DKIM）



ディーマーくんくん
（DMARC）

※エスマいぬ、ディーキぃぬは JIPDEC の登録商標®です。

安心マークの普及

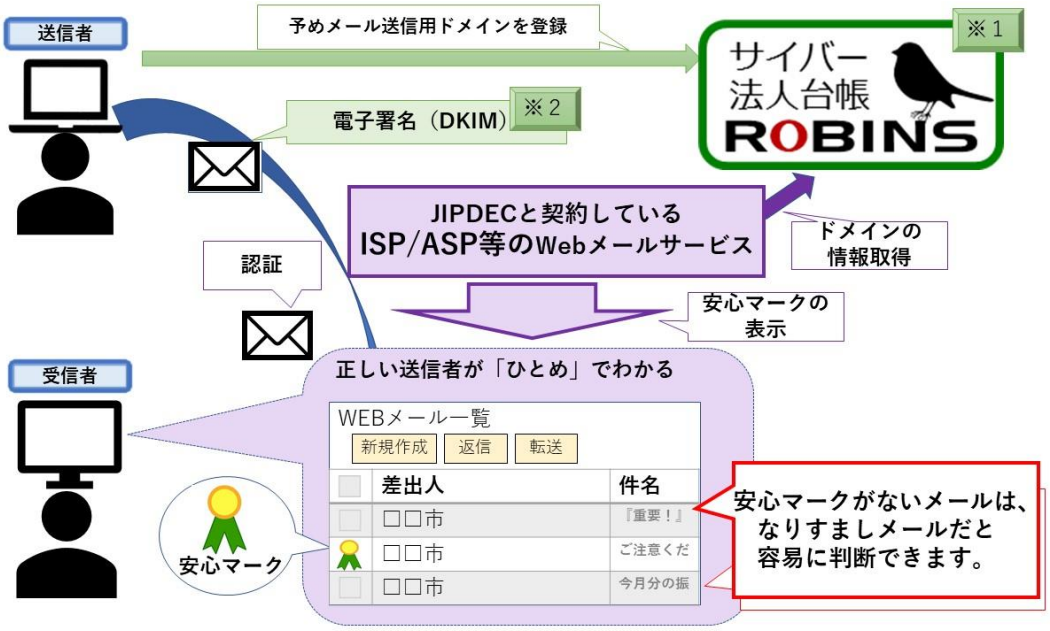
「安心マーク」はなりすましメールでないことを一目で判別できる仕組みです。メール送信者としての金融機関、地方自治体などで広がるとともに、受信者のメールの画面に「安心マーク」を表示させるメールサービスの数も徐々に増えています。

JIPDEC は、安心マークを国際的に普及させる観点から、マルウェア、スパム、DDoS などのサイバー脅威への対策に取り組む国際的なフォーラムである M^{3}AAWG（Messaging, Malware and Mobile Anti-Abuse Working Group）の会合にも研究員を派遣しているところです。

安心マークの仕組み

「安心マーク」登録者が送信した電子メールを安心マーク対応の受信環境で受信する際に、送信ドメイン認証の仕組みを利用して JIPDEC の提供する「サイバー法人台帳 ROBINS」の情報と照合し、合致した場合に受信者の画面に「安心マーク」が表示されます。

図表４－４－８　安心マークの仕組みのイメージ



※１　JIPDEC が運営する真正性の高い企業情報データベース

※２　電子署名を利用した送信ドメイン認証技術

6　JPAAWG

（１）概要

JPAAWG（Japan Anti-Abuse Working Group）は、国際的なセキュリティ対策組織である M³AAWG (Messaging, Malware and Mobile Anti-Abuse Working Group) と連携した日本のメッセージングを中心としたセキュリティ対策組織として 2018 年に発足しました。

今後、インターネット上の様々な脅威について、その対策を議論し、関係者の間で情報共有していくことが予定されており、また、M³AAWG だけではなく、国内における同様な目的を持つ組織とも連携し、活動していくことが予定されています。

（２）主な活動内容

1st General Meeting

JPAAWG は、2018 年 11 月 8 日に 1st General Meeting を開催しました。これは、(一財)インターネット協会の第 18 回迷惑メール対策カンファレンスの併催イベントとして実施されました。JPAAWG としては初めてのイベントでしたが、400 名を超える参加者を迎え、活発な議論も行われました。このイベントでは、産学官および国内外それぞれの分野から多彩な講演者を迎え、迷惑メール対策にとどまらない、IoT やモバイル、SNS などについても取り上げられました。

また、直前に行われた M³AAWG 44th General Meeting の様子なども紹介されました。

国際連携活動

2019 年 2 月の APRICOT 2019（Asia Pacific Regional Internet Conference on Operational Technologies） では、M³AAWG と一緒に、JPAAWG および、日本での迷惑メール対策の活動について講演しました。M³AAWG および JPAAWG では、アジア地域においても同様の活動を広げていくことで、LAC-AAWG[注145]や AFR-AAWG[注146]とも連携し、より幅広い地域をカバーし、課題共有や各種対策を進めていくことが期待されます。

今後について

今後、JPAAWG は組織づくりとともに、メンバーを中心した具体的な課題共有やそれらの対策について議論を行い、上記と同様のイベントの開催や各種資料の公開などにより、広くその活動を公開していくことが予定されています。

[注145] M³AAWG の中南米における下部組織

[注146] M³AAWG のアフリカにおける下部組織

図表４－４－９　1st General Meeting の様子

第5節　国際的な取組

1　国際連携の動向

（1）多国間での取組

国際機関を通じた連携

国際電気通信連合（ITU：International Telecommunication Union）、経済協力開発機構（OECD：Organisation for Economic Co-operation and Development）、アジア太平洋経済協力（APEC: Asia-Pacific Economic Cooperation）などの国際機関において、迷惑メール対策に関わる技術的方策、制度的方策、国際連携枠組みなどについての議論が行われています。

迷惑メール対策に特化した連携枠組み

我が国は、迷惑メール対策を行う各国の執行当局などが、2004 年に「国際的スパム執行協力に関するロンドン行動計画（LAP：London Action Plan）に合意し、以後、定期的に相互の情報交換などを行っている場に参加しています。2014 年 10 月には、アジア地域で初めて LAP の第 10 回会合（LAP10 TOKYO）が東京で開催され、我が国はホスト国として事務局を務め、アジア諸国の迷惑メール対策強化について議論が行われました。さらに、2016 年９月には、LAP は、その活動内容に合わせて、未承諾通信執行ネットワーク（UCENet：Unsolicited Communications Enforcement Network [注 147]）に名称を変更しています。

図表４－５－１　多国間での連携の状況

国際機関などを通じた取組
国際電気通信連合（ITU） **・電気通信標準化部門（ITU-T）などにおいて、スパム対策について議論** **・2009 年４月に開催された世界電気通信政策フォーラムの成果文書においてスパム送信者や技術的対策に関する情報交換の推進を合意** **・ITU-T SG17 の 2011 年９月会合で、日本の迷惑メール対策に関する寄書が提出され、補足文書として発行**
経済協力開発機構（OECD） **・2006 年４月に、迷惑メール対策の枠組みをまとめた「アンチスパム・ツールキット」を公表し、2011 年 10 月にレビューを行い、その後も連携強化に向けた取組を推進**
アジア太平洋経済協力（APEC） **・電気通信サブグループなどにおいて、迷惑メール対策について定期的に意見交換を実施**
アジア・太平洋電気通信共同体（APT） **・1979 年にアジア・太平洋地域の電気通信の開発促進・地域電気通信網の整備・拡充を目的として設立** **加盟国数は 38 カ国（2018 年現在）** **・2015 年５月に開催された第６回サイバーセキュリティフォーラムにおいて、スパム対策について議論** **・2016 年 11 月および 2017 年 11 月にサイバーセキュリティ研修が日本で行われ、我が国の迷惑メール対策を講義**
日 ASEAN 情報セキュリティ政策会議 **・アジア地域におけるセキュアなビジネス環境の整備、安心・安全な ICT 利用環境の構築に向けた地域的対応を目的として、2008 年６月に設置が合意された高級事務レベル会合** **・2011 年３月に東京で開催された第３回会合で、安心・安全な ICT 環境構築のため、引き続き国際的な連携を強化していくことを確認**

注147 UCENet ウェブサイト　https://www.ucenet.org/

図表４－５－２　多国間での連携の状況（迷惑メール対策に特化した枠組）

未承諾通信執行ネットワーク（UCENet（旧名称　国際的スパム執行協力に関するロンドン行動計画（LAP）））
✓ 2004 年から関連情報の共有、官民対話の促進などの目的に合意した各国執行当局間で、定期的に情報交換を実施。米国、カナダ、英国、中国、韓国、日本、オーストラリアなど 27 カ国の迷惑メール対策執行当局、11 カ国の民間機関が参加
✓ 総務省から、定期的な会合等に参加
✓ 2013 年４月に開催された不定期の春期会合では、日本における法執行上の課題などについて紹介
✓ 2013 年 10 月に開催された第９回会合では、参加各国のスパム対策状況を常時情報共有できるように Anti-Spam Index を作成することを確認
✓ 2014 年 10 月東京で第 10 回会合が開催され、最先端技術の取組の相互理解の促進などが盛り込まれた東京宣言を採択
✓ 2015 年 10 月ダブリンで第 11 回会合が開催され、国際機関・警察との協力のあり方などの議論を実施
✓ 2016 年９月に活動内容に合わせて、名称を未承諾通信執行ネットワーク（UCENet）へ変更
✓ 2016 年 10 月パリで第 12 回会合が開催され、情報収集、法執行、情報交換、研修を柱とする次期３カ年活動計画を採択
✓ 2017 年 10 月トロントで第 13 回会合が開催され、各国から迷惑メールの取締りなどの法執行状況について報告。また、同会合において、総務省からは送信ドメイン認証技術（DMARC）に係る法的整理について紹介
✓ 2018 年 10 月ニューヨークで第 14 回会合が開催され、日本における法執行の現状や DMARC の普及状況について説明

最近の動向（2010 年以降）

（ア）UCENet

2014 年 10 月、東京で第 10 回会合（LAP10 TOKYO）が開催され、我が国のほかシンガポール、インドネシア、中国、香港、台湾、韓国などアジアからも多数の国・地域が参加し、各迷惑メール対策機関からスパム対策の取組状況に関する説明および情報交換が行われました。同会合において、総務省から提案した Anti-Spam Library（各国の関係機関が相互に参照可能な迷惑メール対策に関するポータルサイト）の構築を含む、迷惑メール対策の取組強化などを内容とする東京宣言が全会一致で採択されました。

2015 年６月、アイルランド・ダブリンで第 11 回会合が開催され、欧米地域から多数の官民の参加者を得て、今後の LAP での議論の方向性や更なる国際連携の強化の在り方などについても議論が行われました。2016 年 10 月、フランス・パリで第 12 回会合が開催され、カナダ、英国、南アフリカ、オーストラリアなどの各迷惑メール対策機関から迷惑メールの取締りなどの法執行状況の報告が行われたほか、今後３年間の活動計画とその進め方などについて議論が行われました。2017 年 10 月、カナダ・トロントで第 13 回会合が開催され、米国、カナダ、英国、南アフリカ、シンガポール、韓国などの各迷惑メール対策機関から迷惑メールの取締りなどの法執行状況の報告が行われました。また、同会合において、総務省からは送信ドメイン認証技術（DMARC）に関わる法的整理（2017 年７月公表）について紹介しました。

2018 年 10 月、米国・ニューヨークで第 14 回会合が開催され、米国、カナダ、英国、韓国などの各迷惑メール対策機関から迷惑メールの取締りなどの法執行状況の報告が行われました。総務省からも、法執行状況のほか、DMARC の普及状況について報告しました。

（イ）ASEAN

2013 年 12 月に開催された「日・ASEAN 特別首脳会議」において「日・ASEAN 友好協力に関するビジョン・ステートメント実施計画」が採択され、「日・ASEAN サイバーセキュリティ協力に関する閣僚政策会

議」の共同閣僚声明に基づき、「日・ASEAN 情報セキュリティ政策会議」の下、スパム対策に関する情報交換を含めサイバーセキュリティ分野の協力を強化することを確認しました[注 148]。

2014 年 10 月には東京で第 7 回となる政策会議が開催され、日・ASEAN における重要インフラ防護に関するガイドラインの策定など、日・ASEAN の国際的な連携を更に強化していくことで合意されました[注 149]。

（ウ）EU

2013 年 12 月、「日 EU・ICT セキュリティワークショップ」において、スパム対策を含む双方の更なる協力深化が確認されました。また、同月に開催された「日 EU・ICT 政策対話」においては、スパム対策を含む ICT 分野に関する幅広い意見交換が行われました[注 150]。

（２）二国間などでの取組

共同声明など

総務省および経済産業省が、カナダ、英国、フランス、ドイツとの間で、迷惑メール対策における連携について、個別に共同声明や共同宣言を策定しています。また、我が国とスイスとの間で結ばれた経済連携協定（EPA：Economic Partnership Agreement）の協力条項において、迷惑メール対策における連携が言及されています[注 151]。

迷惑メール送信元情報の交換

2018 年 1 月から、総務省は、特定電子メール法第 30 条に基づき、カナダ・ラジオテレビ通信委員会（CRTC）との間で迷惑メール送信元情報の交換を行っています[注 152]。交換された情報は、我が国においては、特定電子メール法に違反する電子メールの送信者への措置に活用されます。

最近の動向

（ア）米国

2012 年 4 月に開催された日米首脳会談において成果文書が公表され、「ファクトシート：日米協力イニシアティブ」の中で、「インターネットエコノミーに関する政策協力対話は、インターネットのオープン性、（中略）、迷惑メールの削減に関し焦点を当てる」との文言が盛り込まれました。また、同年 10 月に開催された「インターネットエコノミーに関する日米政策協力対話局長級会合」の場や 2013 年 4 月の総務副大臣の連邦取引委員会訪問の際に、スパム対策に関する意見交換を実施しました。

注148 外務省「日・ASEAN 特別首脳会議（概要）」（2013 年 12 月 14 日）
https://www.mofa.go.jp/mofaj/area/page3_000594.html

注149 総務省「第 7 回　日・ASEAN 情報セキュリティ政策会議の結果」（2014 年 10 月 8 日）
http://www.soumu.go.jp/menu_news/s-news/01ryutsu03_02000084.html

注150 総務省「日 EU・ICT セキュリティワークショップ（第 2 回）及び日 EU・ICT 政策対話（第 20 回）の結果」（2013 年 12 月 10 日）
http://www.soumu.go.jp/menu_news/s-news/01tsushin06_02000055.html

注151 外務省「日・スイス経済連携協定の発効及び第 1 回合同委員会の開催」（2009 年 9 月 1 日）
https://www.mofa.go.jp/mofaj/gaiko/fta/j_swit/godo_0909.html

注152 総務省「カナダ・ラジオテレビ通信委員会との迷惑メールに係る情報交換に関する協力覚書の締結」（2017 年 12 月 28 日）
http://www.soumu.go.jp/menu_news/s-news/01kiban18_01000033.html

（イ）カナダ

2017 年 10 月の UCENet 第 13 回会合の際に、総務省は、カナダ・ラジオテレビ通信委員会（CRTC）との間で、迷惑メール対策の現状および今後の取組について意見交換を行い、同年 12 月、迷惑メール送信元情報の交換に関する覚書を締結し、2018 年 1 月から、特定電子メール法第 30 条に基づく情報交換を開始しました。

（ウ）インド

2011 年 2 月、日・インド両政府は、迷惑メール対策を含む「日本国とインド共和国との間の包括的経済連携協定（日・インド包括的経済連携協定）」に署名しました[注 153]。

2013 年 2 月のインド通信 IT 省審議官の来日時、同年 4 月の通信 IT 兼海運担当閣外大臣の来日時に、総務省において、迷惑メールの現状などに関し意見交換を行いました。

2014 年 1 月の総務副大臣のインド訪問時に、インド通信 IT 大臣と会談し、迷惑メール対策が含まれる「包括的な日印 ICT 協力枠組み」に合意し、署名しました[注 154]。

（エ）ベトナム

2010 年 10 月、総務省およびベトナム情報通信省は「情報通信分野における協力に関するベトナム情報通信省との覚書」を締結し[注 155]、2012 年 4 月には、ベトナム情報通信副大臣が来日し、迷惑メール対策を含む「日本における ICT 政策」について説明し、意見交換を実施しました。

2013 年 1 月、ベトナム情報通信省などのサイバーセキュリティチームが来日した際、総務省において、迷惑メールの現状などに関する意見交換を行いました。

（オ）マレーシア

2014 年 5 月、総務大臣政務官がマレーシアの通信・マルチメディア副大臣と会談し、迷惑メール対策を含む ICT 分野での協力に関し意見交換を行いました[注 156]。

（カ）シンガポール

2014 年 6 月、総務省とシンガポール情報通信開発庁は「シンガポール ICT 政策対話」を開催し、迷惑メール対策を含む ICT 分野での協力関係強化について意見交換を行いました[注 157]。

（キ）モンゴル

2015 年 2 月、日・モンゴル両政府は、迷惑メール対策を含む「経済上の連携に関する日本国とモンゴル国との協定（日・モンゴル経済連携協定）」に署名しました[注 158]。

注153 外務省「日本国とインド共和国との間の包括的経済連携協定の署名」（2011 年 2 月 15 日）
https://www.mofa.go.jp/mofaj/press/release/23/2/0215_01.html

注154 総務省「上川総務副大臣のウズベキスタン共和国及びインド共和国への訪問結果」（2014 年 1 月 20 日）
http://www.soumu.go.jp/menu_news/s-news/01tsushin09_02000023.html

注155 総務省「情報通信分野における協力に関するベトナム情報通信省との覚書の署名」（2010 年 9 月 28 日）
http://www.soumu.go.jp/menu_news/s-news/35104.html

注156 総務省「藤川総務大臣政務官のマレーシアへの訪問結果」（2014 年 5 月 7 日）
http://www.soumu.go.jp/menu_news/s-news/01tsushin09_02000026.html

注157 総務省「第 3 回　日・シンガポール ICT 政策対話の結果」（2014 年 6 月 20 日）
http://www.soumu.go.jp/menu_news/s-news/01tsushin09_02000027.html

注158 外務省「経済上の連携に関する日本国とモンゴル国との間の協定の署名」（2015 年 2 月 10 日）
経済上の連携に関する日本国とモンゴル国との間の協定の署名

（ク）香港

2015 年 6 月の LAP 第 11 回会合の際、総務省および(一財)日本データ通信協会は、通信事務管理局事務室（OFCA）との間で、迷惑メール対策の現状および今後の取組について意見交換を実施したほか、2016 年 10 月の UCENet 第 12 回会合や 2017 年 10 月の UCENet 第 13 回会合においても、OFCA との間で同様の意見交換を行いました。

（ケ）台湾

2016 年 10 月の UCENet 第 12 回会合の際、(一財)日本データ通信協会は、通信放送委員会（NCC）、財団法人電気通信技術センター（TTC）と会談を行い、台湾が新たに開発する迷惑メールの分析処理システムについて、意見交換を行いました。2017 年 10 月の UCENet 第 13 回会合時にも、台湾の迷惑メール分析処理システムに係る意見交換を行ったほか、2018 年 10 月の UCENet 第 14 回会合時には、台湾における迷惑メール関連法律制定に向けた進捗について確認しました。

（コ）韓国

2009 年 5 月、総務省および韓国放送通信委員会は、「情報通信分野における協力に関する韓国放送通信委員会との覚書」を締結しました[注 159]。

2015 年 6 月、LAP 第 11 回会合の際に、総務省および(一財)日本データ通信協会は、韓国インターネット振興院（KISA）との間で、迷惑メール対策の現状および今後の取組について意見交換を行いました。

2016 年 11 月、総務省および(一財)日本データ通信協会は、KISA の担当者が来日した際に、迷惑メール対策に関わる執行体制や、それぞれが抱える課題などについて意見交換を行いました。それ以降も、2017 年 10 月の UCENet 第 13 回会合時に、迷惑メール対策の現状および今後の取組について意見交換を行ったほか、2018 年 10 月の UCENet 第 14 回会合時には、KISA から提供される日本発韓国着スパムメールデータの活用状況の説明、韓国における犯罪捜査と司法送致の体制などを確認しました。その他、2018 年 11 月の KISA の(一財)日本データ通信協会訪問時に、双方の業務実態などについて意見交換を行いました。

（サ）オーストラリア

2014 年 7 月、日・オーストラリア両政府は、迷惑メール対策を含む「経済上の連携に関する日本国とオーストラリアとの間の協定（日・オーストラリア経済連携協定）」に署名しました[注 160]。

注159 総務省「情報通信分野における協力に関する韓国放送通信委員会との覚書の署名」（2009 年 5 月 11 日）
http://www.soumu.go.jp/menu_news/s-news/02tsushin06_000016.html

注160 外務省「経済上の連携に関する日本国とオーストラリアとの間の協定の署名」（2014 年 7 月 8 日）
https://www.mofa.go.jp/mofaj/press/release/press4_001040.html

図表４－５－３　二国間などでの主な取組１

国、地域	連携の形態	連携の主体	
		日本側	相手側
米国	日米首脳会談に関わる成果文書（ファクトシート）の公表（2012 年４月）	政府	政府
カナダ	共同声明（2006 年 10 月）	総務省 経済産業省	カナダ産業省
	迷惑メール送信元情報の交換に関する覚書の締結（2017 年 12 月）	総務省	カナダ・ラジオテレビ通信委員会（CRTC）
	迷惑メール送信元情報の交換（2018 年１月～）	総務省	カナダ・ラジオテレビ通信委員会（CRTC）
ブラジル	迷惑メールに関する情報の交換（2010 年１月～）	（一財）日本データ通信協会 （一社）JPCERT コーディネーションセンター	ブラジルコンピューター緊急対応チーム（CERT.br）
英国	共同宣言（2006 年９月）	総務省 経済産業省	貿易産業省（DTI）
フランス	共同声明（2006 年５月）	総務省 経済産業省	経済財政産業省
ドイツ	共同声明（2007 年７月）	総務省 経済産業省	連邦経済技術省
スイス	日・スイス経済連携協定への署名（2009 年９月）	政府	政府
インド	日・インド包括的経済連携協定（2011 年２月）	政府	政府
	日印 ICT 協力枠組みに合意（2014 年１月）	総務省	通信 IT 省
ベトナム	情報通信分野における協力に関するベトナム情報通信省との覚書の締結（2010 年９月）	総務省	情報通信省
	迷惑メールに関する情報の交換（2013 年１月～）	（一財）日本データ通信協会	ベトナムコンピューター緊急対応チーム（VNCERT）

図表４－５－４　二国間などでの主な取組２

国、地域	連携の形態	連携の主体	
		日本側	相手側
中国 	迷惑メールに関する情報の交換（2007 年 12 月～）	（一財）日本データ通信協会 （一財）日本産業協会	中国インターネット協会（ISC）
	ICT 協力に関する文書を締結（2009 年５月）	総務省	工業情報化部（MIIT）
モンゴル 	日・モンゴル経済連携協定（2014 年７月）	政府	政府
香港 	迷惑メールに関する情報の交換（2007 年 12 月～）	（一財）日本データ通信協会	通信事務管理局事務室（OFCA）
台湾 	迷惑メールに関する情報の交換（2008 年５月～）	（一財）日本データ通信協会	通信放送委員会（NCC）
韓国 	情報通信分野における協力に関する韓国放送通信委員会との覚書の締結（2009 年５月）	総務省	韓国放送通信委員会（KCC）
	迷惑メールに関する情報の交換（2011 年５月～）	（一財）日本データ通信協会	韓国インターネット振興院（KISA）
オーストラリア 	日・オーストラリア経済連携協定の署名(2014 年７月)	政府	政府

2　民間による取組（M³AAWG）

（1）概要

世界的な迷惑メールの増加を背景に、国際的な電気通信事業者やISPなど19社は、2004年1月にMAAWG（Messaging Anti-Abuse Working Group）を創設しました。現在は、メッセージング以外に、マルウェア（Malware）、モバイル（Mobile）を加えたM³AAWG（Messaging, Malware and Mobile Anti-Abuse Working Group）として、200以上のメンバー組織で構成されています。参加メンバーの多くは、北米と欧州を拠点とする、電気通信事業者やISP、各種ベンダーですが、我が国からも創設時から参加しているメンバーがいます。また、メール業界の識者らが、シニアテクニカルアドバイザーとして参加しており、IETFなどの関係団体との相互連携的な活動も行っています。

（2）主な活動内容

M³AAWGでは、検討分野ごとに委員会（Committee）があり、各委員会のチェアを中心として、それぞれの分野で課題を検討しています。例えば、技術的な内容を検討するTechnical Committeeや、メンバー間での協調的な活動について議論するCollaboration Committee、各国の執行当局や国際機関との連携的な活動をするPublic Policy Committeeなどは、創設時から活動している委員会です。現在では、より多くの分野に関するCommitteeやSIG（Special Interest Group）が作られ、活発な議論が行われています。

M³AAWGでは、毎年3回、北米西海岸、欧州、北米東海岸でGeneral Meetingを開催しています。いずれもM³AAWGメンバーと招待されたゲストのみが参加できる閉じた会合ですが、毎回30カ国程度から500名前後が参加する規模となっています。近年は、欧米以外の地域のとの連携を高める目的で、南米カリブ地区でLAC-AAWG[注161]が、日本でJPAAWG[注162]が立ち上がりました。また、各国の執行当局などが集まるUCENet[注163]との合同会合も開催されています。

General Meetingでは、メール運用当事者や開発技術者、セキュリティ研究者などが参加し、その時点でのホットな話題や対策技術について議論や情報交換を行っています。例えば、OP25BやSPF、DKIMといった対策技術の普及に大きな影響を与え、最近でもDMARCやARCについては、M³AAWGメンバーが中心となって仕様を検討、相互接続テストを行うなどの検証作業を行いました。これらはその後IETFで標準化作業に入るなど、技術の標準化活動にも大きな貢献をしています。M³AAWGで検討してきた内容は、ベストプラクティスとして文書にまとめられ、公開[注164]されています。この中の幾つかの文書は、有志によって日本語に翻訳されており、まとめて参照[注165]できるようになっています。

技術的な内容以外にも、各国の法規制に関連する内容なども議論されています。最近では欧州における一般データ保護規制（GDPR）の施行による影響、例えばWHOISで提供される情報が制限される問題などについて、大きな関心となりました。

注161 https://www.m3aawg.org/published-documents
注162 JPAAWG: Japan Anti-Abuse Working Group
注163 UCENet: Unsolicited Communicvations Enforcement Network
注164 https://www.m3aawg.org/published-documents
注165 https://www.m3aawg.org/japanese