

迷惑メール白書 2018



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

迷惑メール白書

2018

迷惑メール対策推進協議会



はじめに

迷惑メール対策推進協議会は、電気通信事業者など迷惑メール対策に関わる関係者が幅広く集まり、関係者間の緊密な連絡を確保し、最新の情報共有、対応策の検討、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に資することを目的に、**2008年11月27日**に発足しました。

迷惑メールは、**2001年**春頃から、主に出会い系サイトの宣伝を中心としたメールが増加し、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りました。このような迷惑メールに対しては、携帯電話事業者やサービスプロバイダなどが、迷惑メールの根絶に向けて機能面での拡充など様々な取組を行っているほか、制度面においても、**2002年**に「特定電子メールの送信の適正化等に関する法律」が制定され、また、同じ年に「特定商取引に関する法律」が改正されました。さらに、**2008年**には、両法の一部改正によりオプトイン規制が導入されるなど、実効性の確保に向けた規制の強化が図られてきました。

当協議会は、迷惑メールの根絶に少しでも貢献できるよう、電子メールの送信者情報が詐称されているかどうか確認できる「送信ドメイン認証技術」の普及啓発を目的とした「送信ドメイン認証技術導入マニュアル」や、迷惑メールの現状や対策などをまとめた「迷惑メール対策ハンドブック」の公表などを行ってきました。

近年の迷惑メールの傾向としては、総数そのものは減少傾向にありますが、新たに、情報を詐取するフィッシングサイトへ誘導する電子メールやウイルスなどのマルウェア感染を目的とする電子メール、さらに最近では、特定の企業をターゲットとしたビジネスメール詐欺（BEC）が社会的な問題となっており、日本を代表する企業が数億円単位のビジネスメール詐欺の被害に遭った事件は記憶に新しいところです。

このような迷惑メールの最新の傾向などを踏まえ、また、当協議会発足**10周年**の節目として、幅広く国民の皆様に迷惑メールの現状などを知っていただくため、「迷惑メール対策ハンドブック」の内容を見直し、名称についても「迷惑メール白書**2018**」としました。

この白書が有効に活用され、迷惑メールの根絶に繋がることを切に期待しております。

2018年11月

迷惑メール対策推進協議会座長

新美 育文



目次

第1章 2017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	2
第2節 悪質化・巧妙化する迷惑メールの動向	3
1 フィッシングメール	3
2 ビジネスメール詐欺（BEC）	4
第3節 迷惑メール対策の動向	6
1 総務省が「DMARC 導入に関する法的な留意点」を発表	6
2 「Stop! 迷惑メールの日」の創設	6
3 Post-M ³ AAWG meetup の開催	7
トピックス：2017年度の迷惑メールに関するできごと	8
トピックス：迷惑メール対策推進協議会 10年の歩み	11

第2章 迷惑メールについて

第1節 電子メールとは	14
1 電子メールなど	14
2 電子メールの仕組み	15
第2節 迷惑メールとは	18
1 迷惑メールの特徴	18
2 迷惑メールの具体例	19
第3節 迷惑メールの動向	23
1 全体的傾向	23
2 国内発の迷惑メールの割合	25
3 迷惑メールの送信国・地域	26
4 迷惑メールの内容	27
5 世界全体の迷惑メール送信国・地域の傾向	28
第4節 迷惑メールの送信方法	29
1 送信先の選定	29
2 送信元の偽装	30
3 サーバーの不正利用	31
4 その他（迷惑メールフィルターの回避）	33
トピックス：SNSの悪用	34



第3章 迷惑メール対策

第1節 制度的な対策	36
1 特定電子メール法	36
トピックス：特定電子メール法の沿革	40
トピックス：現行の特定電子メール法の詳細	42
2 特定商取引法	45
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	46
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	48
3 その他の法律による迷惑メールに関する規制	51
4 海外での対策法制の整備状況	52
第2節 技術的な対策	56
1 概要	56
2 送信側での対策	57
3 受信側での対策	63
トピックス：OP25B（Outbound Port 25 Blocking）	67
トピックス：送信ドメイン認証技術（SPF・DKIM・DMARCなど）	68
第3節 利用者による対策	72
1 迷惑メールを受け取らないための対策	72
2 迷惑メールを受信してしまったときの対策	73
3 自ら同意した広告宣伝メールへの対応	74
4 その他	75
トピックス：通信の秘密とOP25B、送信ドメイン認証技術	79

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	82
1 概要	82
2 主な取組	82
第2節 行政による取組	84
1 特定電子メール法の執行状況	84
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）	84
3 その他の取組	85
第3節 事業者による取組	87
1 携帯電話事業者の取組	87
2 サービスプロバイダの取組	90
3 セキュリティベンダーの取組	93
4 配信サービス事業者の取組	95



第4節 関係組織による取組	98
1 (一財)日本データ通信協会 迷惑メール相談センター	98
2 (一財)日本産業協会 電子商取引モニタリングセンター	100
3 (一財)インターネット協会 迷惑メール対策委員会	102
4 (独)国民生活センター	104
5 フィッシング対策協議会	106
6 (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	108
第5節 国際的な取組	110
1 国際連携の動向	110
2 民間による取組 (M ³ AAWG)	118

参 考 編

第1節 迷惑メールの量・割合の推移	120
第2節 迷惑メール送信国・地域の推移	123
1 国内着の迷惑メール送信国・地域の推移	123
2 世界全体の迷惑メール送信国・地域の推移	130
第3節 迷惑メールの内容の傾向	131
第4節 特定電子メール法の執行状況	132
1 2008年改正までの執行状況(オプトイン規制導入前)	132
2 2008年改正後の執行状況(オプトイン規制導入後)	132
第5節 特定商取引法の執行状況(電子メール広告に関するもの)	135
1 2008年改正までの執行状況(オプトイン規制導入前)	135
2 2008年改正後の執行状況(オプトイン規制導入後)	135
第6節 送信ドメイン認証技術の導入状況	136
第7節 送信ドメイン認証技術の認証結果	139
1 SPFの認証結果の推移(2018年3月まで)	139
2 DKIMの認証結果の推移(2018年3月まで)	141

資 料 編

1 関係法令・窓口等	144
2 迷惑メール対策推進協議会 関係資料	148
3 索引	153

第1章

2017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

2017年度の迷惑メールに関する概況としては、国内着の迷惑メールは減少傾向にあり、その内容も広告・宣伝メールが大半を占めるなど、近年と同様の傾向が続いています。2017年度においても、迷惑メールの内容はますます悪質化・巧妙化しており、ビジネスメール詐欺（Business E-mail Compromise:BEC）により大手企業が多額の金銭を詐取された事件は社会的に大きな注目を集めたところ です。

まず、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、2017年度においても時期によって変動はあるものの減少傾向にあり、2018年3月においては36.7%となっています。なお、世界的な迷惑メールの割合は、2017年において僅かながら増加傾向にあり、2017年11月には55.5%に達しました。

国内着信の迷惑メールの発信元（国）としては、2017年度においても引き続き、日本、米国、中国が多く、2018年3月には、それぞれ約42%、約12%、約11%となっています。

迷惑メールの内容としては、「出会い系」サイトへ誘導する広告宣伝メールが大半を占めていますが、2017年は65.9%となり、2009年の調査開始以来、初めて7割を下回りました。また、副業紹介や情報商材などに関するメールが16.6%となり、2016年と比較して10%以上増加しています。その他にも、情報を詐取するフィッシングサイトへ誘導する、いわゆるフィッシングメールや、企業をターゲットにして、取引先や経営層などを装い、偽のメールを送り金銭を詐取するビジネスメール詐欺（BEC）が社会的に大きな問題となっており、実際に大手企業が多額の金銭を詐取された事件が発生しています。

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など様々な関係者が、2017年度も引き続き「迷惑メールを送信させない・受信しない」ための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。

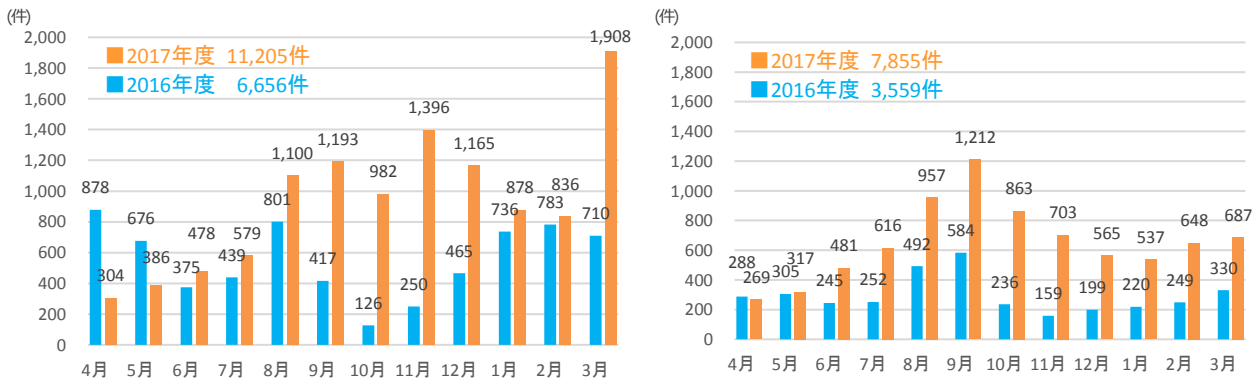


第2節 悪質化・巧妙化する迷惑メールの動向

1 フィッシングメール

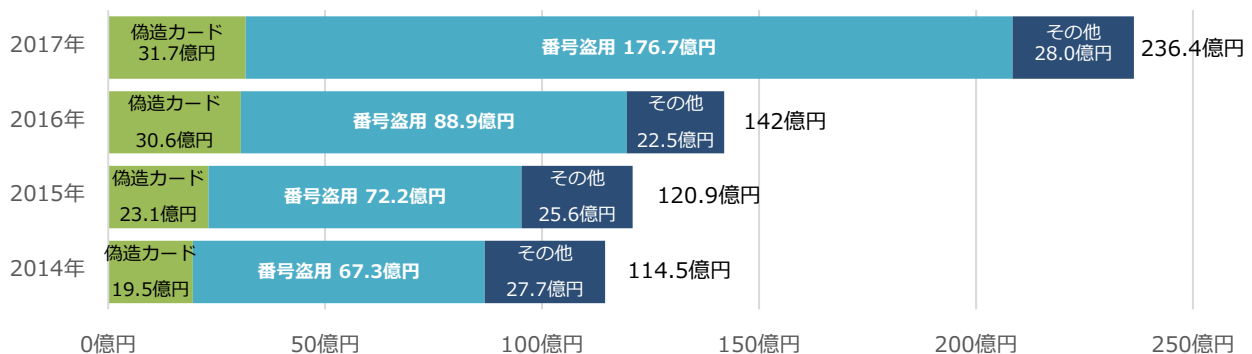
フィッシング対策協議会によれば、2017年度には、フィッシング報告件数は前年度比1.7倍（6,656件→11,205件）と増加し、また、フィッシングサイトのURL件数も前年度比2.2倍（3,559件→7,855件）と増加しています^{注1}。フィッシングメールの内容としては、銀行情報（口座番号、暗証番号など）やクレジットカードの情報を詐取する目的のものに加えて、仮想通貨の情報を詐取する目的のものも確認されています^{注2}。また、（一社）日本クレジット協会によれば、被害額の全てがフィッシングメールを端緒にしたものとは限りませんが、2017年には、クレジットカード不正使用による被害額が前年比1.6倍（142億円→236.4億円）と増加し、14年ぶりに200億円を超えました^{注3}。

図表1-2-1 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

図表1-2-2 クレジットカード不正使用被害の発生状況



出典：（一社）日本クレジット協会「クレジットカード不正使用被害の集計結果について」をもとに、迷惑メール対策推進協議会事務局が編集

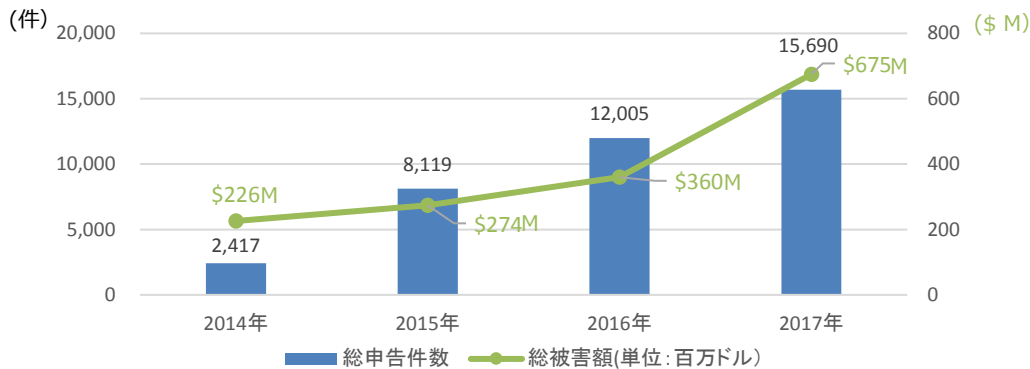
注1 フィッシング対策協議会（フィッシングレポート2018） https://www.antiphishing.jp/report/pdf/phishing_report_2018.pdf
 注2 フィッシング対策協議会（緊急情報等）、トレンドマイクロ社セキュリティブログ（2018年3月19日「仮想通貨を狙うフィッシング詐欺、既に闇市場での「サービス化」も確認」）
 注3 （一社）日本クレジット協会（クレジットカード不正使用被害の集計結果について） <https://www.j-credit.or.jp/download/news20180330b.pdf>



2 ビジネスメール詐欺（BEC）

2017年度は、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）が注目されました。米国のFBIによると^{注4}、2017年のBECによる被害額は、前年比1.8倍（3.6億ドル→6.7億ドル）と増加したほか、日本国内においても、2017年12月には大手航空会社がBECにより3.8億円を詐取されたことが判明し、他の航空会社でも偽のメールが送られてきたことが確認されています^{注5}。

図表1-2-3 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

このようなBECによる被害は、2016年6月にトレンドマイクロ(株)が公表したBECに関する注意喚起^{注6}によると、2013年10月頃から確認されており、これまでのBECの手口を次の5タイプに分けられるとしています。

- ・ 偽の請求書になります
- ・ CEOになります
- ・ アカウントの侵害
- ・ 弁護士になります
- ・ 情報詐取

2017年4月、(独)情報処理推進機構(IPA)は、「ビジネスメール詐欺「BEC」に関する事例と注意喚起」と題するレポート^{注7}を発表し、BECへの注意喚起を行いました。同レポートでは、先のトレンドマイクロ(株)の注意喚起で紹介している5タイプの手口を引用しながら、実際に発生した具体的な事例も紹介しています。例えば、「取引先との請求書の偽装」のケースは、送信者側(攻撃者側)がターゲットとした企業の取引先を装い、請求に関わるやりとりを電子メールなどで行っている際に、送信者側の用意した口座に差し替えた偽の請求書などを送り、振込みをさせるという手口です。この際、送信者側は取引に関わる正規のやりとりをなら

^{注4}2017 Internet Crime Report, https://pdf.ic3.gov/2017_IC3Report.pdf

^{注5} 2017年12月20日 日本経済新聞

^{注6} 2016年6月16日 トレンドマイクロ(株) (多額の損失をもたらすビジネスメール詐欺「BEC」)
<https://www.trendmicro.com/vinfo/jp/threat-encyclopedia/web-attack/3151/billiondollar-scams-the-numbers-behind-business-email-compromise/>

^{注7} 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>



かの方法により事前に取得し、取引や請求に関する情報や、関係している従業員の電子メールアドレスや氏名などを入手している場合があるとしています。

また、IPAは、同レポートにおいてBECへの対策として次の対策を推奨しています。

図表1-2-4 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
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
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
不審と感じた場合の組織内外での情報共有	不審な電子メール情報を適切な部門に報告できる体制の構築が重要であり、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。
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



第3節 迷惑メール対策の動向

1 総務省が「DMARC 導入に関する法的な留意点」を発表

迷惑メール対策技術としては、なりすましメールを検知可能とする送信ドメイン認証技術の普及が進んできましたが、依然として認証に失敗した電子メールのブロックを行うまでには至っておらず、利用者に迷惑メールが届いてしまう状況が続いています。この問題の解決策の一つとして、米国を中心に、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新たな送信ドメイン認証技術 DMARC の導入が進んでおり、米国の国土安全保障省は政府機関に対する全面的な導入指令を 2017 年 10 月に発令しました^{注8}。この指令は法的拘束力を持ち、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。我が国では、総務省が、送信ドメイン認証技術を推進するため、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9}。それによると、DMARC の特徴的な処理^{注10}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。

2 「Stop! 迷惑メールの日」の創設

(一財)日本データ通信協会は、迷惑メールに関する一般利用者のリテラシー向上と防止技術の普及促進に寄与することを目的に、新たに迷惑メール対策の周知強化日として「Stop! 迷惑メールの日」を創設しました。

「Stop! 迷惑メールの日」は、(一財)日本データ通信協会に迷惑メール相談センターが開設された日（7 月 10 日）とし、2017 年 7 月 10 日にその創設記念式典を開催しました。同式典には、迷惑メール対策推進協議会関係者が参加したほか、同協議会事務局の(一財)日本データ通信協会迷惑メール相談センターが所在する巣鴨の当地キャラクター「すがもん」を一日所長に任命し、PR に協力してもらいました。

図表 1-3-1 「Stop! 迷惑メールの日」創設記念式典の様相



^{注8} <https://cyber.dhs.gov/bod/18-01/>

^{注9} http://www.soumu.go.jp/main_content/000495390.pdf

^{注10} 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



3 Post-M³AAWG meetup の開催

2018年3月7日、Post-M³AAWG meetup が開催されました。今回開催された会合では「Japanese Post-M³AAWG」と題し、M³AAWG 議長を始め、セキュリティベンダー、ISP などの関係者が、直前の2月に米国で開催された M³AAWG 会合で議論された内容を踏まえて、電子メールに限らず、情報セキュリティ全般について広く意見交換を行いました。



トピックス：2017年度の迷惑メールに関するできごと

2017年4月3日

IPAが、BECに関する注意喚起を実施し、手口や対策について周知^{注11}。

2017年4月14日

消費者庁が、メールを端緒に、有料動画サイトなどの未納料金の回収を依頼されていると称して金銭を請求する事業者に関する注意喚起を実施^{注12}。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、「本日中に連絡なき場合、法的手続に移行する」旨を記載したメールにより、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。

2017年6月15日

放送大学が、2017年6月4日から同月9日までの間、第三者に大学のメールアドレスを不正に利用され、同大学のメールサーバーから不特定多数のメールアドレスに迷惑メールが74万件以上送信されたと発表。

2017年6月30日

長野県立科町が、2017年6月30日、同町観光商工課のメールアドレスから迷惑メールが大量に送信される事案が発生したと発表。

2017年7月6日

総務省がDMARC導入に関する法的な留意点^{注13}を発表。

(独)国民生活センターが、心当たりのないメール・SMSには反応しないよう注意喚起を実施^{注14}。同センターの報道資料によれば、2014年度以降、迷惑メールに関する相談が増加傾向にあるとのこと。

2017年7月10日

(一財)日本データ通信協会 迷惑メール相談センターは、一般利用者のリテラシー向上と防止技術の普及促進に寄与する活動として、同センターが開設された7月10日を新たに迷惑メール対策の周知強化日「Stop! 迷惑メールの日」とし、その創設記念式典を開催。

2017年8月4日

神奈川県相模原市が、同市と座間市の共催事業「市民大学」のメールアドレスが第三者に不正に使用され、不特定多数にメールが送信される事案が発生したと発表^{注15}。

2017年8月15日

複数の国会議員事務所に中国語の迷惑メールが大量に届いた旨を報道^{注16}。

2017年9月4日

ソフトバンク(株)及びトピラスシステムズ(株)が、二社と愛知県警察本部を加えた三者間で迷惑メール対策に関する覚書を締結したと発表^{注17}。報道資料によると、ソフトバンクのスマートフォン向けに、愛知県警察本部から提供を受けた迷惑電話番号のデータベースをもとに、SMSで届いた不審な電話番号からのメールを検知し、受信時に迷惑メールとして振り分け、警告を表示する迷惑メール対策機能を、2017年9月下旬以降に提供すること。

^{注11} <https://www.ipa.go.jp/security/announce/20170403-bec.html>

^{注12} http://www.caa.go.jp/policies/policy/consumer_policy/information/pdf/consumer_policy_information_170414_0001.pdf

^{注13} http://www.soumu.go.jp/main_content/000495390.pdf

^{注14} http://www.kokusen.go.jp/pdf/n-20170706_1.pdf

^{注15} http://www.city.sagamihara.kanagawa.jp/_res/projects/default_project/_page_/001/006/265/0804_02.pdf

^{注16} 産経新聞

^{注17} https://www.softbank.jp/corp/group/sbm/news/press/2017/20170904_01/ 2018年4月現在、富山県警、岐阜県警が新たに参加し、引き続きサービスを提供中



2017年9月7日

警察庁が「平成29年上半年におけるサイバー空間をめぐる脅威の情勢等について」を発表^{注18}。同レポートによれば、警察庁が連携事業者から報告を受けた2017年上半年における標的型メール攻撃の件数は589件で、2016年下半年よりも1,506件減少したとのこと。

2017年9月26日、29日

(一財)インターネット協会が、9月26日に大阪で、また、同月29日に東京で迷惑メール対策カンファレンスを開催し、関係者間で活発な意見交換を実施。

2017年10月2日～5日

総務省及び(一財)日本データ通信協会が、カナダ(トロント)で開催されたUCENet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。

2017年10月6日、7日

(一財)日本データ通信協会が、情報セキュリティワークショップ in 越後湯沢2017に参加し、同協会から要請を受けた迷惑メール対策推進協議会技術WGの構成員が、電子メールのなりすまし対策について講演。

2017年10月20日、21日

(一財)日本データ通信協会が、くらしフェスタ東京2017に出展し、迷惑メールに関する注意喚起を実施。

2017年11月11日

BECによる犯罪被害が国内で広がり始めたことから、専門家が対面や電話で必ず確認するなど対策を呼びかけた旨を報道^{注19}。

2017年11月14日

消費者庁が、SMSによるアマゾンジャパン(合)などを騙った架空請求に関する注意喚起を実施^{注20}。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。

2017年11月20日

総務省及び消費者庁が、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。)に基づく措置命令を(株)ライトニングに対して実施した旨を発表^{注21}。

2017年12月7日

Googleを装い、ランダムに携帯電話番号を入力するプログラムを用いてSMSを不特定多数へ送り、クレジットカード番号を詐取るフィッシングにより、3,600万円を詐取した者が、警視庁に詐欺容疑で逮捕された旨を報道^{注22}。

2017年12月12日、13日

2017年8月以降、フィッシングが急増し、11月にフィッシング対策協議会へ報告されたフィッシングの件数が前年同月比の5.6倍になったと報道^{注23}。

2017年12月13日

放送大学が、2017年10月27日から11月8日までの間、第三者にメールアカウントを不正利用され、同大学のメールサーバーから不特定多数の電子メールアドレス宛てに迷惑メールが14万件以上送信されたと発表^{注24}。今後、再発防止に向け監視を強化するとともに、サーバー脆弱性検査などの対策を行うとのこと。

注18 https://www.npa.go.jp/publications/statistics/cybersecurity/data/H29_kami_cyber_jousei.pdf

注19 読売新聞

注20 http://www.caa.go.jp/policies/policy/consumer_policy/information/pdf/consumer_policy_information_171114_0001.pdf

注21 http://www.soumu.go.jp/menu_news/s-news/01kiban18_01000032.html

注22 毎日新聞、産経新聞、東京新聞

注23 日本経済新聞、東京新聞

注24 https://www.ouj.ac.jp/hp/o_itiran/2017/pdf/291213.pdf



2017年12月21日

日本航空(株)がBECにより3.8億円を詐取されたとの報道^{注25}。

2017年12月22日

消費者庁が、未納料金为名目で金銭を支払わせようとする、ヤフーを騙ったSMSに関する注意喚起を実施^{注26}。消費者庁の報道資料によれば、「未納料金が発生しており、本日中に連絡なき場合、法的手続に移行する」旨を記載したSMSが出回っており、SMSに記載された電話番号に連絡した場合、支払い方法はコンビニエンスストアでギフトカードを買って、その番号を教示するよう求めるもので、このような相談が消費生活センターなどに寄せられたとのこと。

2017年12月28日

総務省が、特定電子メール法第30条に基づくものとして初めて、迷惑メールに関わる情報を外国執行当局と交換するための協力覚書をカナダ・ラジオテレビ通信委員会との間で締結したと発表^{注27}。

2018年1月26日

IPAが、国内プラント事業者を狙ったウイルス付メールが1年以上継続送信されていると発表^{注28}。

2018年2月28日～3月1日

(一財)日本データ通信協会が、文京区消費生活展(くらしフェスタ2018～情報を活かす私の消費生活～)に出展し、迷惑メールに関する注意喚起を実施。

2018年3月1日

アマゾン、ヤフーを装ったSMSによる架空請求が多発していると報道^{注29}。

2018年3月1日、2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2018に参加し、同協会から要請を受けた迷惑メール対策推進協議会技術WGの構成員が、電子メールのなりすまし対策について講演。

2018年3月7日

M³AAWG 関連で国内初開催となる会合として、Post-M³AAWG meetup が開催され、M³AAWG 議長を始め、関係者が活発な意見交換を実施。

2018年3月13日

総務省及び消費者庁が、特定電子メール法に基づく措置命令を、(株)MOTHER に対して実施した旨を発表^{注30}。

2018年3月22日

警察庁が「平成29年中におけるサイバー空間をめぐる脅威の情勢等について」を発表^{注31}。同レポートによれば、警察庁が連携事業者から報告を受けた2017年下半期における標的型メール攻撃の件数は5,438件で、上半期の589件から急増した。これにより、2017年の年間件数は6,027件になり、引き続き増加しているとのこと。また、同レポートによれば、そのうちの90%がインターネット上に公開されていない電子メールアドレスへの攻撃であり、62%が送信元メールアドレスを偽装していると考えられる電子メールであるとのこと。

2018年3月23日

総務省が、Outlook2016やWindows10に対応した迷惑メール情報提供用プラグインソフトの配布を開始した旨を発表。

注25 読売新聞、毎日新聞、日本経済新聞

注26 http://www.caa.go.jp/notice/caution/phone/pdf/caution_phone_171222_0001.pdf

注27 http://www.soumu.go.jp/menu_news/s-news/01kiban18_01000033.html

注28 <https://www.ipa.go.jp/files/000063812.pdf>

注29 東京新聞

注30 http://www.soumu.go.jp/menu_news/s-news/01kiban18_01000036.html

注31 https://www.npa.go.jp/publications/statistics/cybersecurity/data/H29_cyber_jousei.pdf



トピックス：迷惑メール対策推進協議会 10年の歩み

2008年

○迷惑メール対策推進協議会の設置

2008年の改正特定電子メール法の施行後も迷惑メール対策の関係者間の緊密な連絡を確保し、最新の情報共有、対応方策の検討、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に「迷惑メール対策推進協議会」を設置。

図表1-3-2 第1回総会

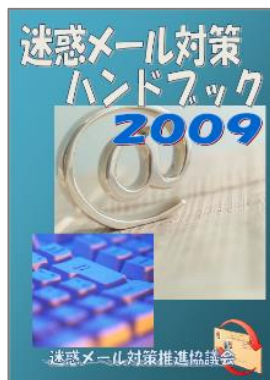


2009年

○迷惑メール対策ハンドブックの公表

迷惑メールの現状や迷惑メールへの対策をまとめた「迷惑メール対策ハンドブック」を公表（2009年以降、年次で同ハンドブックを公表）。

図表1-3-3 迷惑メール対策ハンドブック



○送信ドメイン認証技術 WG の設置

迷惑メールへの技術的な対策として、なりすましメールの検知に有効な「送信ドメイン認証技術」の普及促進を強化していくため、協議会の下に「送信ドメイン認証技術 WG」を設置。

2010年

○送信ドメイン認証技術導入マニュアル第1版の公表

送信ドメイン認証技術の普及促進の強化策として、同技術の導入方法を記した「送信ドメイン認証技術導入マニュアル」を公表。

図表1-3-4 送信ドメイン認証技術導入マニュアル第1版



○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～の公表

協議会やその他の団体などによる、それまでの迷惑メールに対する取組や今後の活動計画を記した「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」を公表（2013年には同プログラムの改訂版を公表）。



2011年

○送信ドメイン認証技術導入マニュアル第2版を公表

送信ドメイン認証技術導入マニュアル第1版に最新の状況の追補などをおこなった、同マニュアル第2版を公表。

○協議会の英文表記の規定

協議会の英語表記を「Anti-Spam mail Promotion Council」とし、その略称表記を「ASPC」と規定。

○「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-」のリーフレット第1版を公表

送信ドメイン認証技術の概要を記したリーフレット「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-」の第1版を公表。

図表1-3-5 電子メールのなりすまし対策



2014年

○LAP10 TOKYO 委員会の設置

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）によるLAP10東京会合が開催された。協議会としてその準備のため「LAP10 Tokyo 委員会」を設置。

図表1-3-6 LAP10 Tokyo 委員会



○技術WGの設置

送信ドメイン認証技術の普及に加え、その他の技術的課題もその目的範囲とするため、「送信ドメイン認証技術WG」を発展的に改組し、「技術WG」を新たに設置。

2017年

○協議会活動貢献者を表彰

新たに迷惑メール対策の周知強化日として「Stop！迷惑メールの日」となった7月10日に、多年にわたり協議会活動に尽力され、大きく貢献された個人を協議会活動貢献者として表彰。

図表1-3-7 協議会活動貢献者の表彰



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きましたが、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32}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・伝達的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

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、数十文字程度の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。ただし、写真や動画などは送受信できません。
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32} 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。



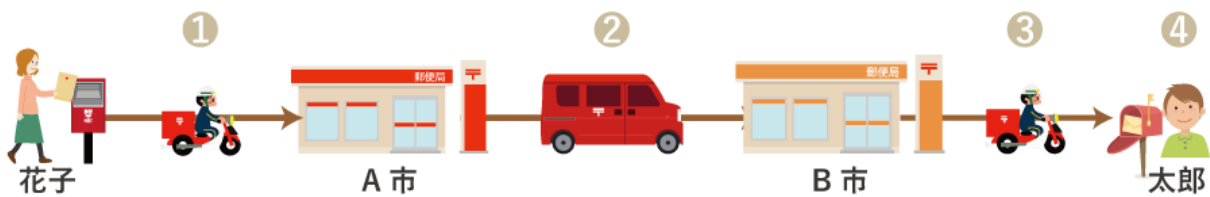
2 電子メールの仕組み

メールソフト^{注33}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。

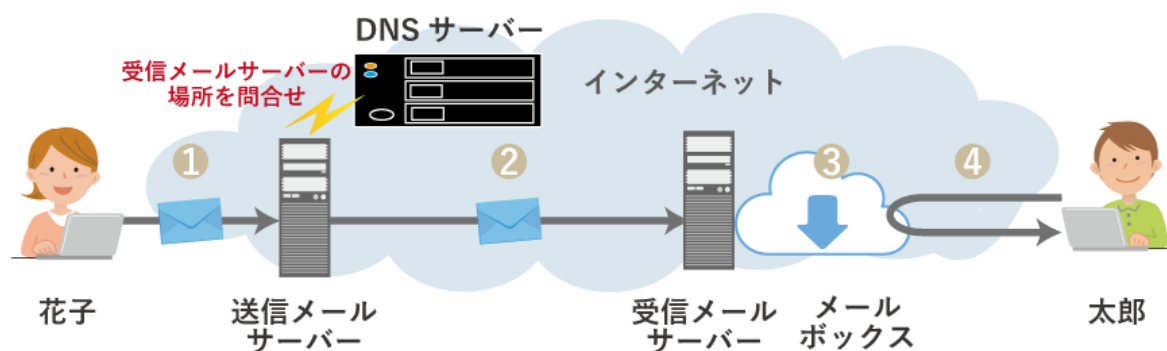
図表 2-1-2 郵便物の配達



- 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

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



^{注33} MUA (Mail User Agent) といひ、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。



第2章 迷惑メールについて

- ① 電子メールが送信メールサーバー^{注34}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35}

※ 郵便の場合は、郵便局が住所を统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（Domain Name System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」及び「Envelope-From」^{注36}と、便箋に書かれた情報にあたる情報は、「Header-To」及び「Header-From」^{注37}といえます。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38}。

なお、郵便の場合と異なり、「Envelope-To」及び「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」及び「Header-From」の情報になっています^{注39}。

^{注34} 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35} 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36} 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。

^{注37} 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38} 「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39} 「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。

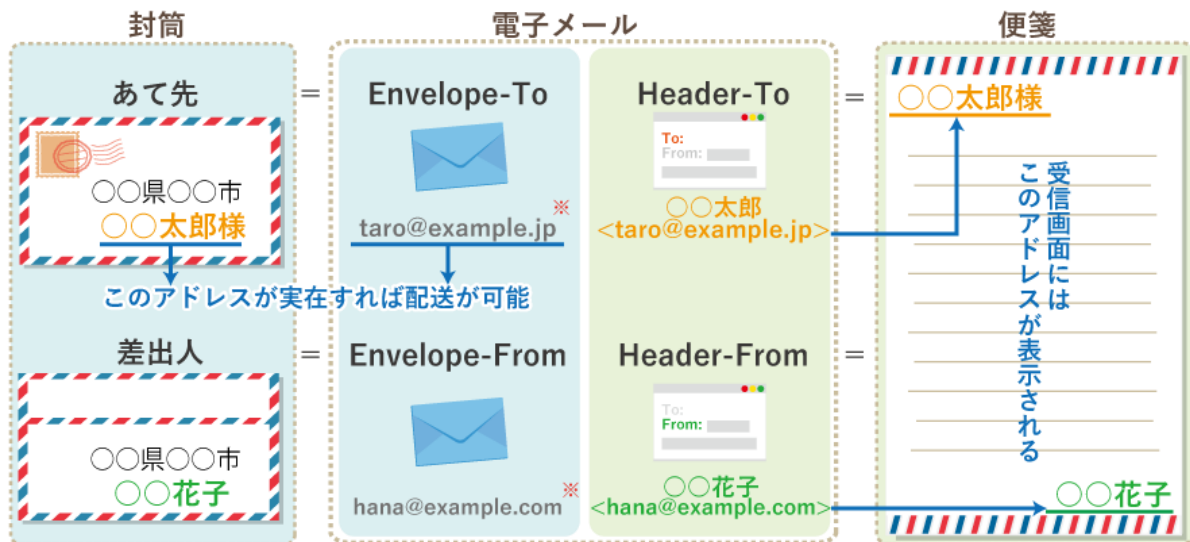


以上を、比較表ならびに図式にしてみると次のようになります。

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」及び「Header-From」には、送信者の個人名（〇〇太郎、〇〇花子）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。



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（個人情報など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、従業員を騙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。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】本会員登録キャンペーン詳細(無料)▼

http://*****/*****/

↓各種ポイント購入方法↓

☆ヒットキャンペーン☆

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。



第2章 迷惑メールについて

● 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/〇原<*****@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、智恵という人が居ました。智恵は、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。智恵は、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智恵があなたのところへ、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。智恵は、朝から晩までだっ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、携帯の画像に知恵がいたり、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クケーらしい！
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られない状態です！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！

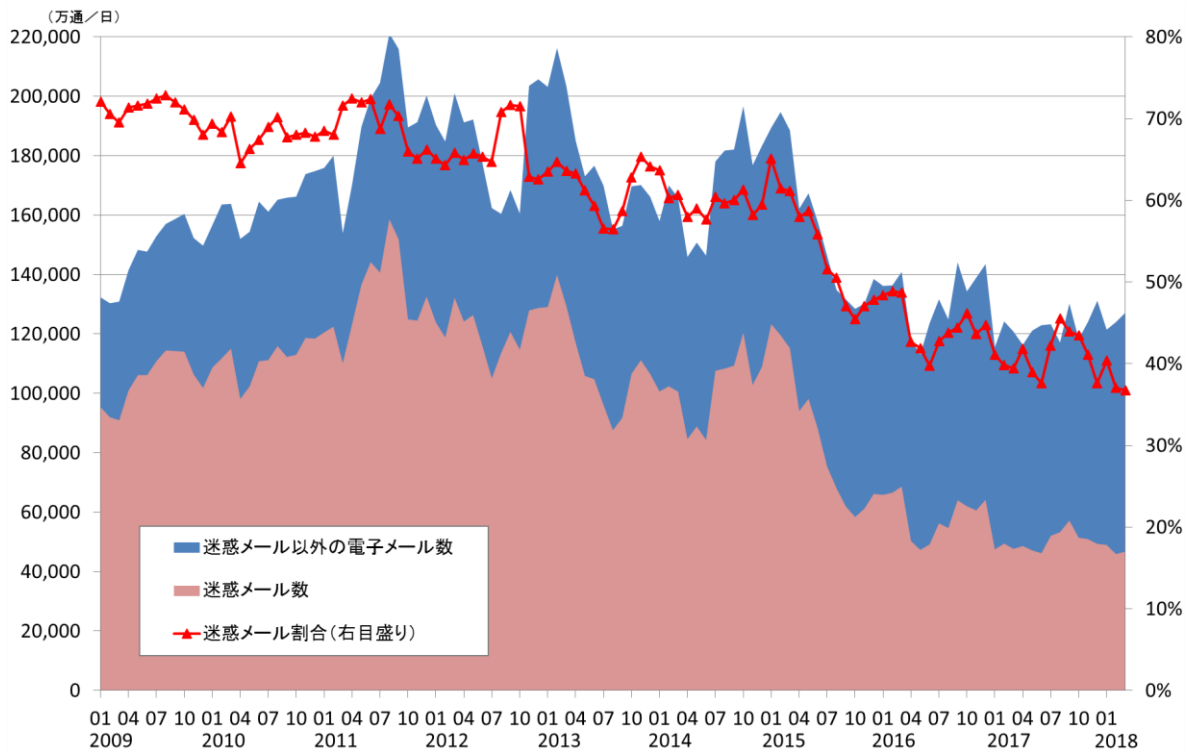


第3節 迷惑メールの動向

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。このように、迷惑メールそのものが減少している上、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減少していることが考えられます。

図表2-3-1 国内ISPにおける迷惑メール数・割合の推移



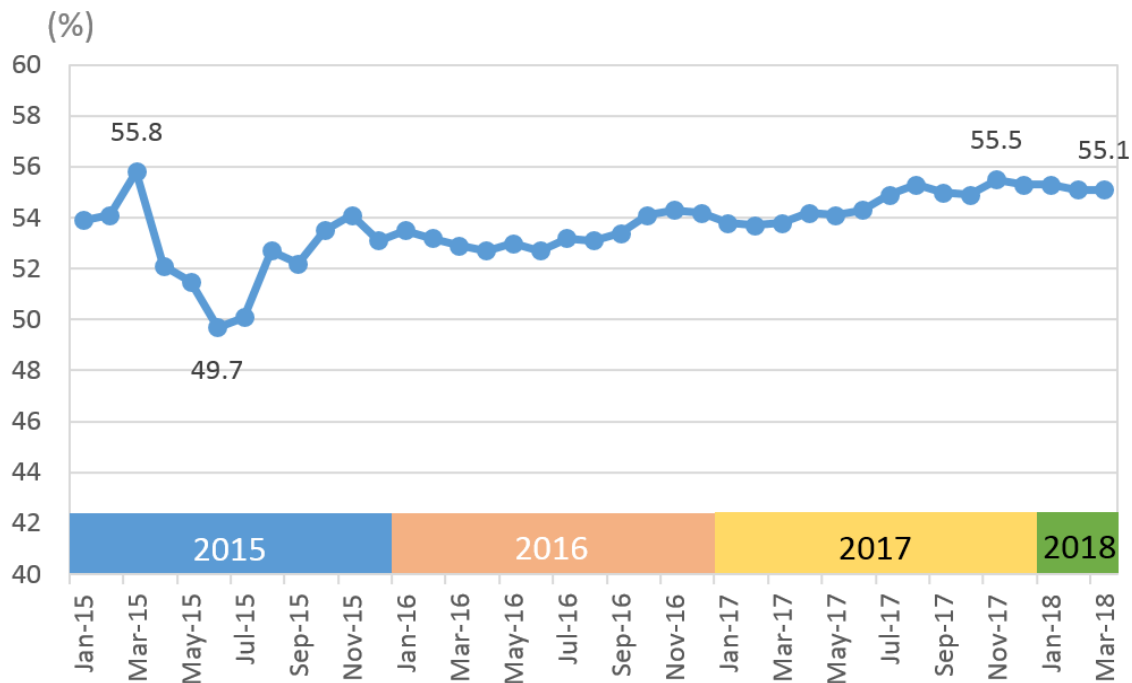
出典：総務省「電気通信事業者10社の全受信メール数と迷惑メール数の割合（2018年3月時点）」



第2章 迷惑メールについて

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「2017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」

第1章

第2章

第3章

第4章

参考編

資料編

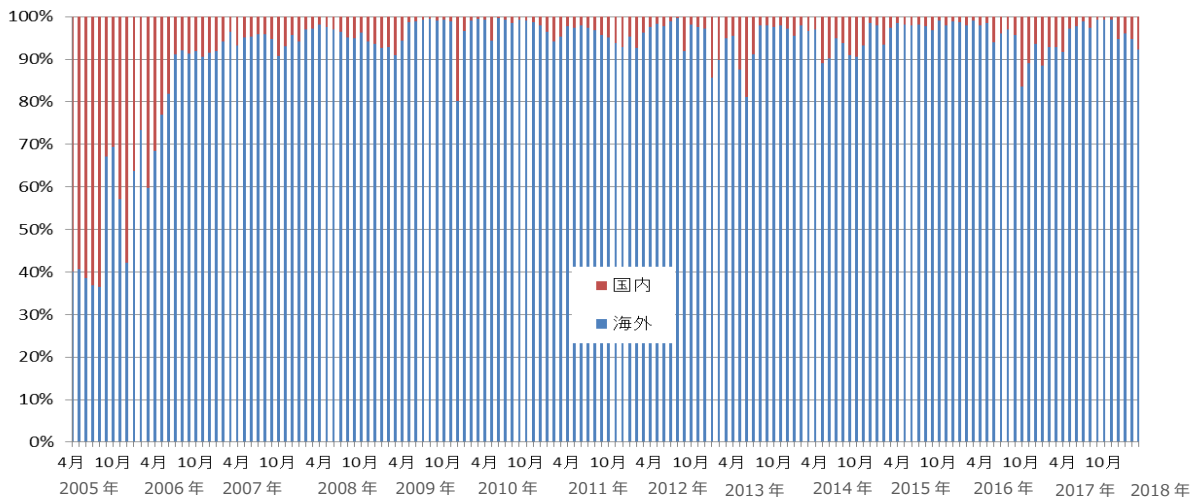


2 国内発の迷惑メールの割合

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。

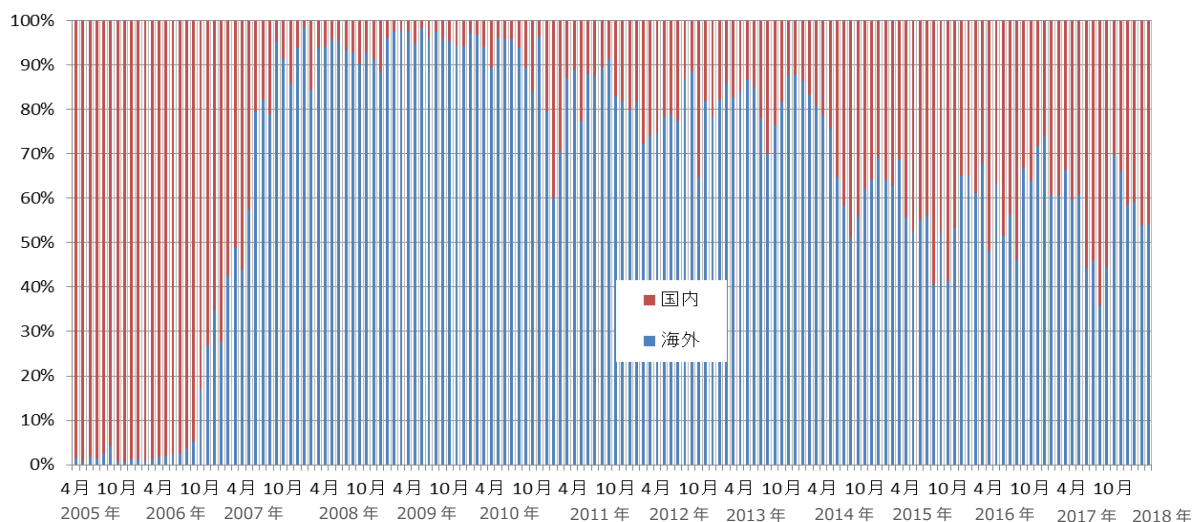
(一財)日本データ通信協会が設置しているモニター機に着信した迷惑メールでは、国内発のもの割合は、PC宛ての迷惑メールについては2005年には50%を超える時期があったものの、その後は減少し、2006年以降はそのほとんどが海外発のものとなっています。一方、携帯電話宛ての迷惑メールについては、国内発のものが一時期減少しましたが、2014年以降は増加傾向にあり、現在では半数程度が国内発のものとなっています。

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）

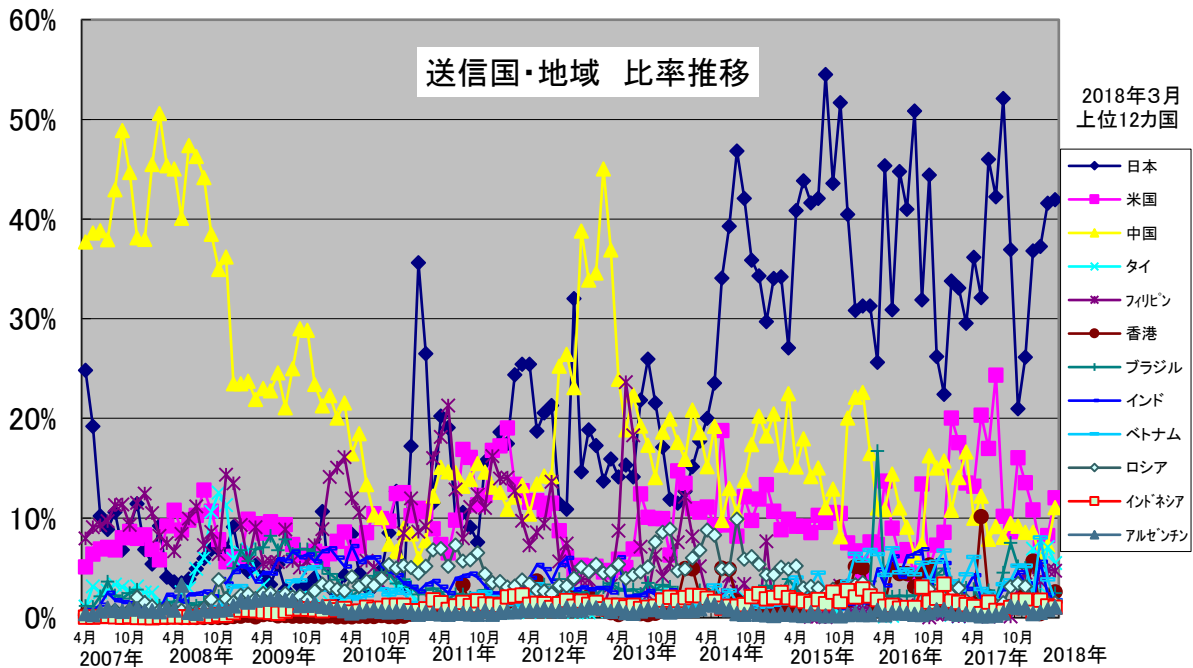


3 迷惑メールの送信国・地域

国内着の迷惑メールの送信国・地域としては、日本、米国、中国が上位にあ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についての送信国・地域としては、時期的な変動はありますが、一貫して日本、米国、中国が多くなっています。その他の国・地域としては、2013年度頃までフィリピンからの発信が多く、時期によっては20%を超えることもありましたが、2017年度には、タイやベトナムからの迷惑メールが増加しました。

図表2-3-5 日本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)

第1章

第2章

第3章

第4章

参考編

資料編

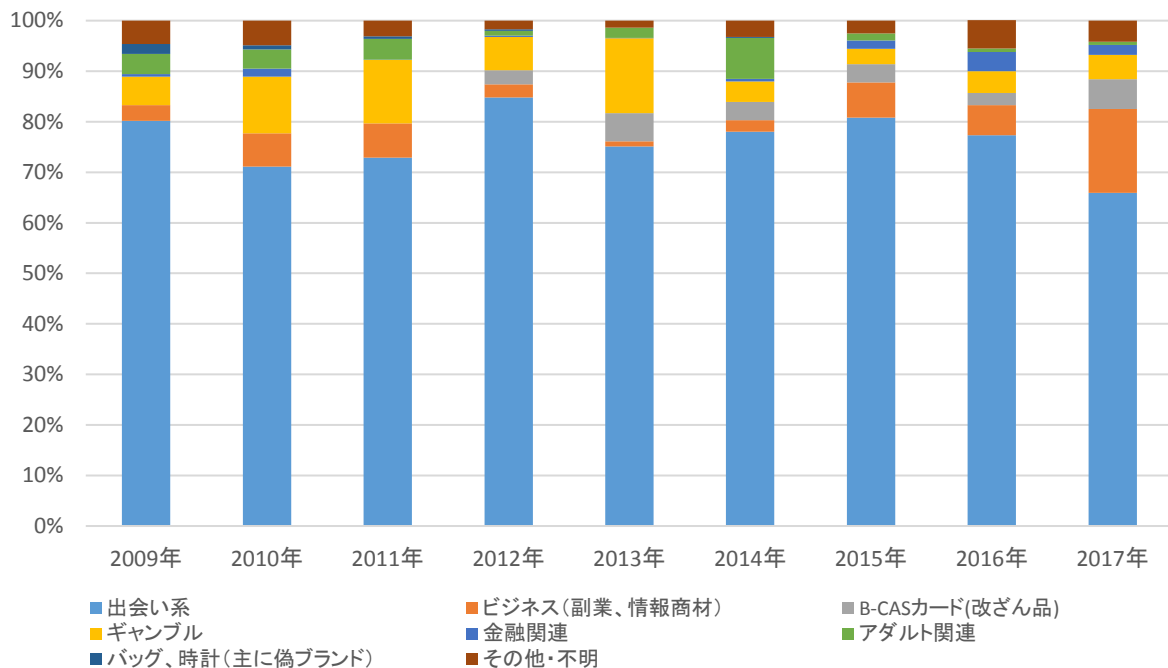


4 迷惑メールの内容

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。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。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%と急増しました。

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及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

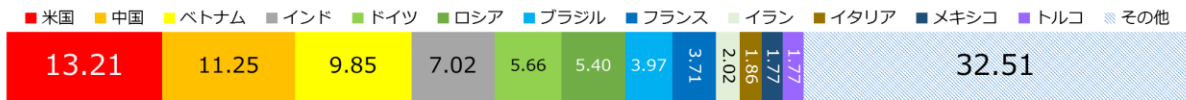


5 世界全体の迷惑メール送信国・地域の傾向

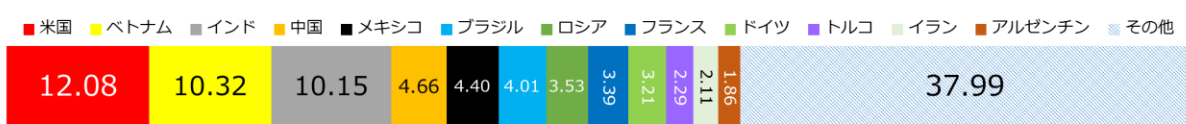
世界全体の迷惑メールの送信国をみると、3でみた国内着の迷惑メール送信国・地域の上位である米国、中国が、ここでも高い比率を占めているのがわかります。その他にも、ベトナム、インド、ロシアといった国からの迷惑メールが多いこともわかります。

図表2-3-7 迷惑メール送信国・地域の傾向

2017年



2016年



2015年



2014年



2013年



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、送信元のメールアドレス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などの方法があります。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用い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 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（ホモグラフィ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）及び（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

<p>From: *****アカウントチーム <support@*****.com></p> <p>To: ***@example.com</p> <p>Subject: ***** アカウントの不審なサインイン</p>	<p>Header</p>
<p>*****セキュリティチームの調べによれば、あなたの**ソフトのプロダクトキーが何者かにコピーされている不審の動きがあります。</p> <p>サインイン情報:</p> <p>Wind**システム: Wind**7</p> <p>IP: 100.10.** **</p> <p>日時: 2018/6/22 (GMT)</p> <p>お客様がこれを実行した場合は、このメールを無視しても問題ありません。</p> <p>お客様がこれを実行した覚えがない場合、悪意のあるユーザーがお客様のプロダクトキーを使っている可能性があります。こちらからはあなたの操作なのかどうか判定できないため、検証作業をするようお願いします。</p> <p>*今すぐ認証* http://*****.com/</p> <p>サービスのご利用ありがとうございます。</p> <p>*****アカウントチーム</p>	<p>Body</p>

(1) 送信元アドレスの偽装

(2) 表示名（ディスプレイネーム）の偽装

(3) ドメイン名の悪用

一見正規ドメインと見間違えるようなドメインを使用

例:

- ✓ m&rn → micro>rnicro
- ✓ w&vw → will>vwill
- ✓ t&f → soft>soff
- ✓ e&c → News>Ncws
- ✓ e&a → store>stora
- ✓ i&l → id>ld
- ✓ l&t → lucky>lucky
- ✓ O&t0 → Opera>Opera

第1章

第2章

第3章

第4章

参考編

資料編



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40}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（ボット）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41}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目立っていることから、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42}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きます（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43}からの送信をブロックする OP25B ^{注44}による対策が行われています。しかし、(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40} 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41} 常に同じ IP アドレスが割り当てられること

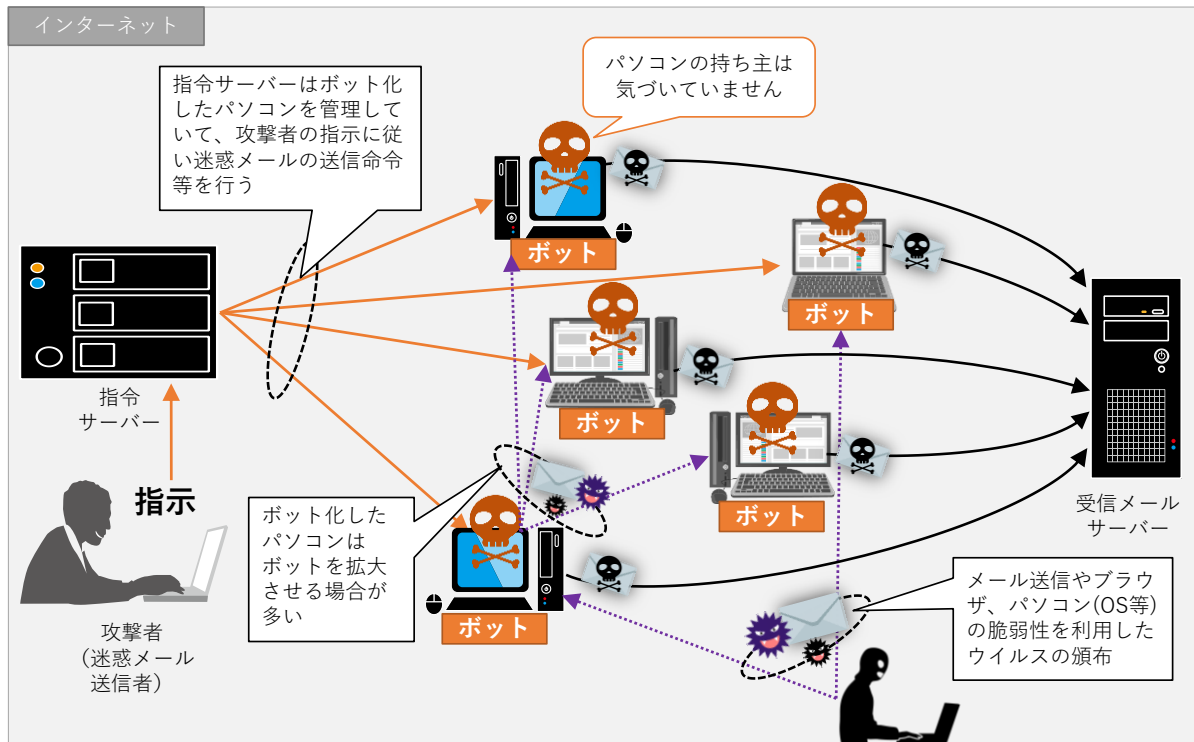
^{注42} 「Malicious Software」（悪意のあるソフトウェア）の略で、様々な脆弱性や情報を利用して攻撃をするソフトウェアの総称

^{注43} 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44} 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、そのような対処が行えないよう、契約者情報を偽って契約を締結することで、送信元の特定が行えないようにしています。

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

電子メールアドレスの 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ドレスを不正に利用して、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ドレス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、電子メールアドレスが不正に利用され、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。


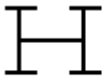




4 その他（迷惑メールフィルターの回避）

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
メール・写メ・プロフ閲覧等も全てが無料!!  円	 な 季節が来た!	 	◆ 専用 メール B O X 【開封無料】



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。

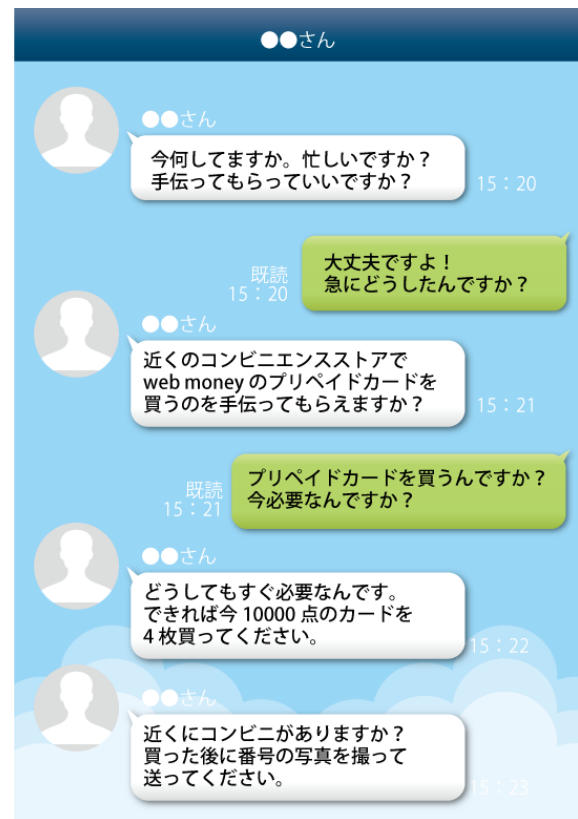
そして、SNSの利用者が増えてくると、知らないアカウントから「悪質サイトへの誘導」などの迷惑メッセージがSNSでも送られるようになりました。電子メール同様、SNSのメッセージを使った詐欺被害やマルウェア感染なども発生しています。

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まりました。

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45}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46} ）、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45 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

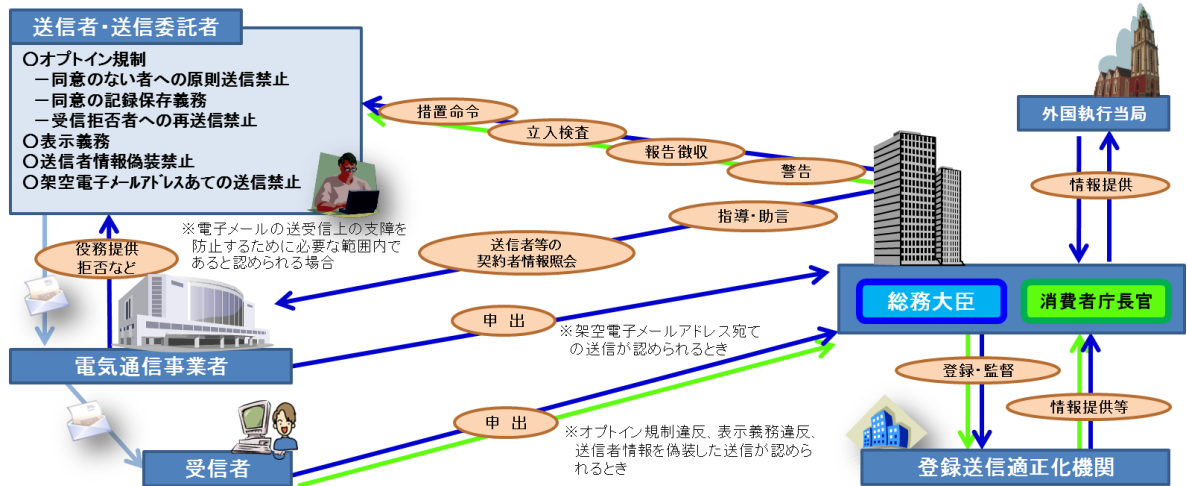
注46 違法行為に対して（行政指導や行政処分を課すことなく）即時に適用される刑事罰を直接罰という。一方、違法行為に対して行政指導や行政処分（例えば、措置命令）後、その指導や処分に違反する行為があった場合に、それを理由に適用される刑事罰を間接罰という。



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

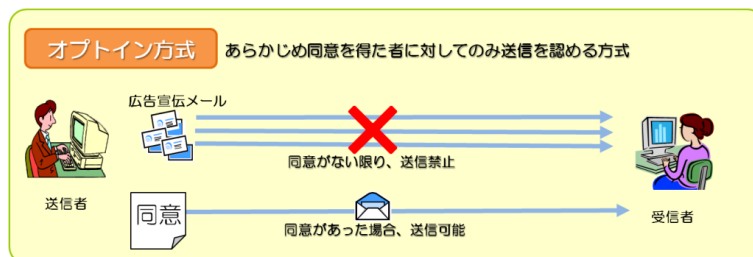


(1) 電子メールの送信者に対する規制

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。

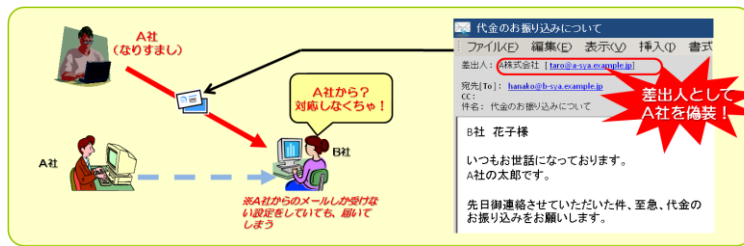
また、迷惑メールの中には、ヘッダーFromを偽って送信し、電子メールの送信元を突き止めにくくしているものがありますが、広告宣伝メールの送信に当たっては、このような、送信者情報の偽装が禁止されています（送信者情報を偽った送信の禁止）。さらに、プログラムを用いて自動的に大量に生成した電子メールアドレス（架空電子メールアドレス）宛てに送信することは、迷惑メールの送信を助長するだけでなく、大量のエラーメールを発生させ、電気通信事業者のメール配送設備に多大な負荷をかけることから、禁止されています。

図表3-1-3 オプトイン方式

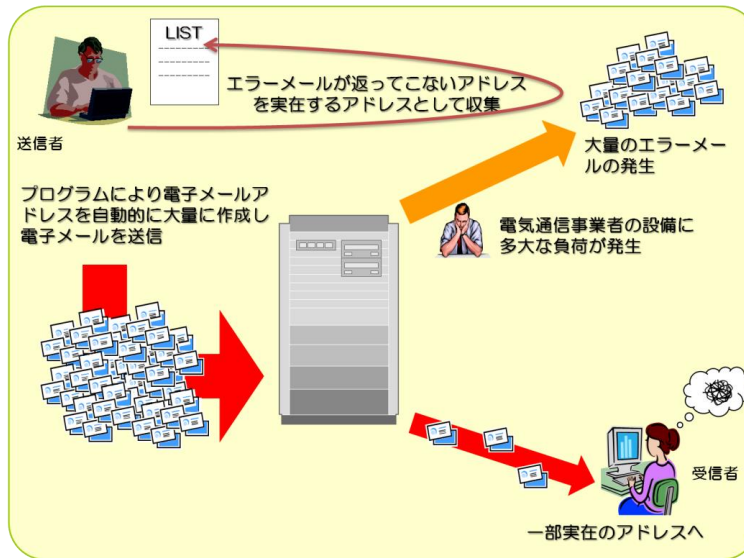




図表3-1-4 送信者情報の偽装の例



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47}、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48}。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49}の観点からも問題が生じます。

注47 電気通信事業法第121条

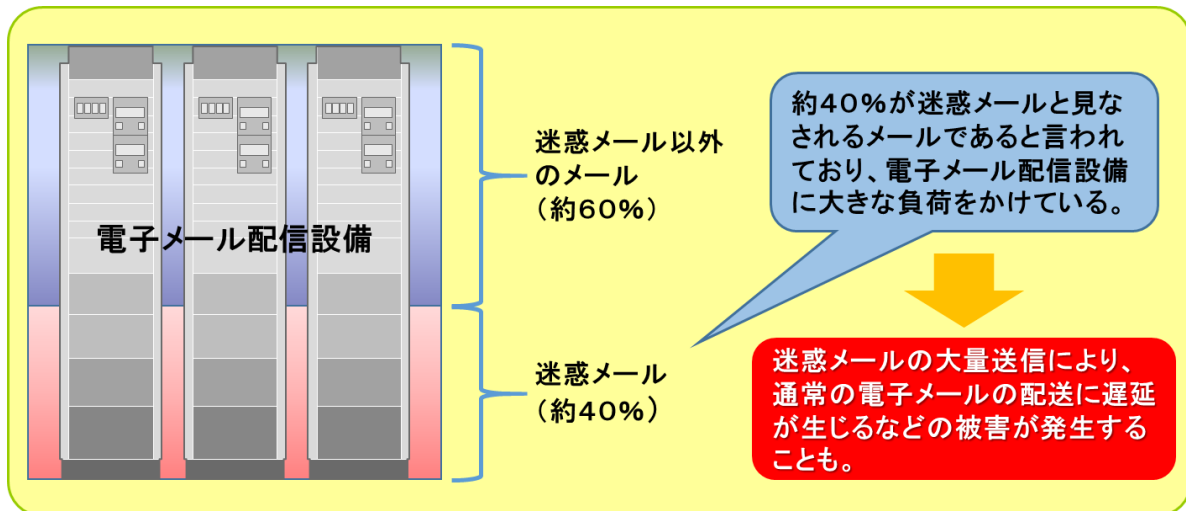
注48 電気通信事業法第6条

注49 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50}、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51}。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52}。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53}。

(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54}。

^{注50} 特定電子メール法第28条

^{注51} 特定電子メール法第7条

^{注52} 特定電子メール法第34条、第35条

^{注53} 特定電子メール法第29条

^{注54} 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

携帯電話宛での迷惑メールが社会問題となったことなどをを受けて、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での送信が禁止され、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55}」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56}。

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57}、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55} 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56} 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57} 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。
- 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。
- 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。

(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	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）。
同意を証する記録の保存義務違反	
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58}消費者庁長官に委任されています。

^{注58} 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

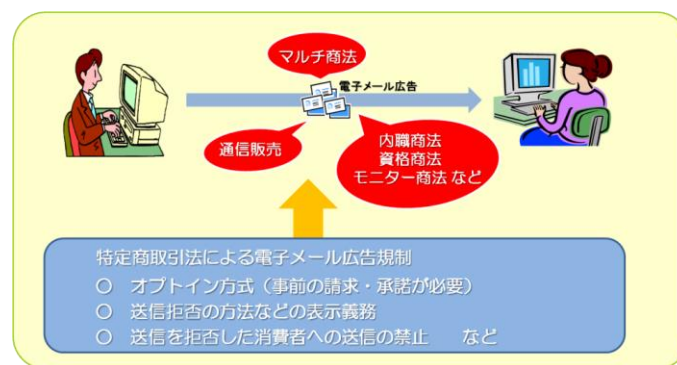
特定商取引法においては、通信販売、連鎖販売取引（いわゆるマルチ商法）、業務提供誘引販売取引（いわゆる内職商法、資格商法、モニター商法など）の形態で消費者と取引をする場合において、事業者が、取引の対象となる商品や役務などについて電子メールにより広告をする場合には、オプトイン方式による規制が課されます。すなわち、事業者が消費者に対してこれらの電子メール広告を行うに当たっては、原則として消費者による事前の請求又は承諾が必要です。また、請求・承諾を得て電子メール広告を行う場合であっても、電子メール広告の送信を拒否する方法など一定の事項を表示する義務が課されているほか、電子メール広告の送信を拒否した消費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

- 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59}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60}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61}。

^{注59} 特定商取引法第14条、第15条など

^{注60} 特定商取引法第66条第1項

^{注61} 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、ファクシミリ広告を請求等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) 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一定の事項を表示することが義務づけられています。
- (エ) 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。
- (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た詳細な事項は、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に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に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62}。

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

(画面例)

容易に認識できる例

注文確認

注文内容を確認し、注文を確定して下さい。
下記の注文内容が正しいことを確認してください。
〔注文を確定する〕ボタンをクリックするまで、実際の注文は行われません。

お届け先 変更
 経済 太郎
 〒100-xxxx
 東京都千代田区霞が関x-x-x

支払方法 変更
 △△カード xxx-xxx
 有効期限: 07/2020

注文明細 変更

商品	単価	数量	小計
商品 (1)	1,000円	1個	1,000円
		送料	200円
		消費税	96円
		合計	1,296円

発送方法: 宅配便 変更

今後、当社からのお知らせ（商品についての広告メール）を受け取ることを希望します。（希望しない方はチェックを外して下さい。）

[TOPに戻る](#) (注文は確定されません)



デフォルト・オン方式

送信 (注文) ボタンに近接して記載

デフォルト・オンの表示について、画面の中で消費者が認識しやすいように明記（例：全体が白色系の画面であれば、赤字で明記するなど）

(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62 消費者庁「特定商取引法ガイド」<http://www.no-trouble.go.jp/pdf/20120401ra05.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 3-1-1-1 電子メールの送信に関わる法規制（特定電子メール法及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63} ）	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64} ）	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 ウィルス作成・提供・保管等		
ウィルス作成・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
ウィルスの取得・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65}	1 年以下の懲役又は 50 万円以下の罰金

^{注63} 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64} 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65} 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66}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67}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68}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69}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が課しています。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70}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71}及びプライバシー・電子通信規則^{注72}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66} 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67} Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003

^{注68} Rules and Regulations Implementing the Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003

^{注69} Telephone Consumer Protection Act of 1991

^{注70} 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71} Data Protection Act 1998

^{注72} 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73}及びテレメディア法^{注74}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75}及び消費法典^{注76}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77}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78}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79}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80}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73} Gesetz gegen den unlauteren Wettbewerb

^{注74} Telemediengesetz

^{注75} Code des postes et des communications électroniques

^{注76} Code de la consommation

^{注77} 互联网电子邮件服务管理办法





^{注78} 通信短信息服务管理规定

^{注79} 정보통신망 이용촉진 및 정보보호 등에 관한 법률

^{注80} Spam Act 2003



図表3-1-12 海外での

	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)

第1章

第2章

第3章


第4章

参考編

資料編



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	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1章

第2章

第3章

第4章

参考編

資料編



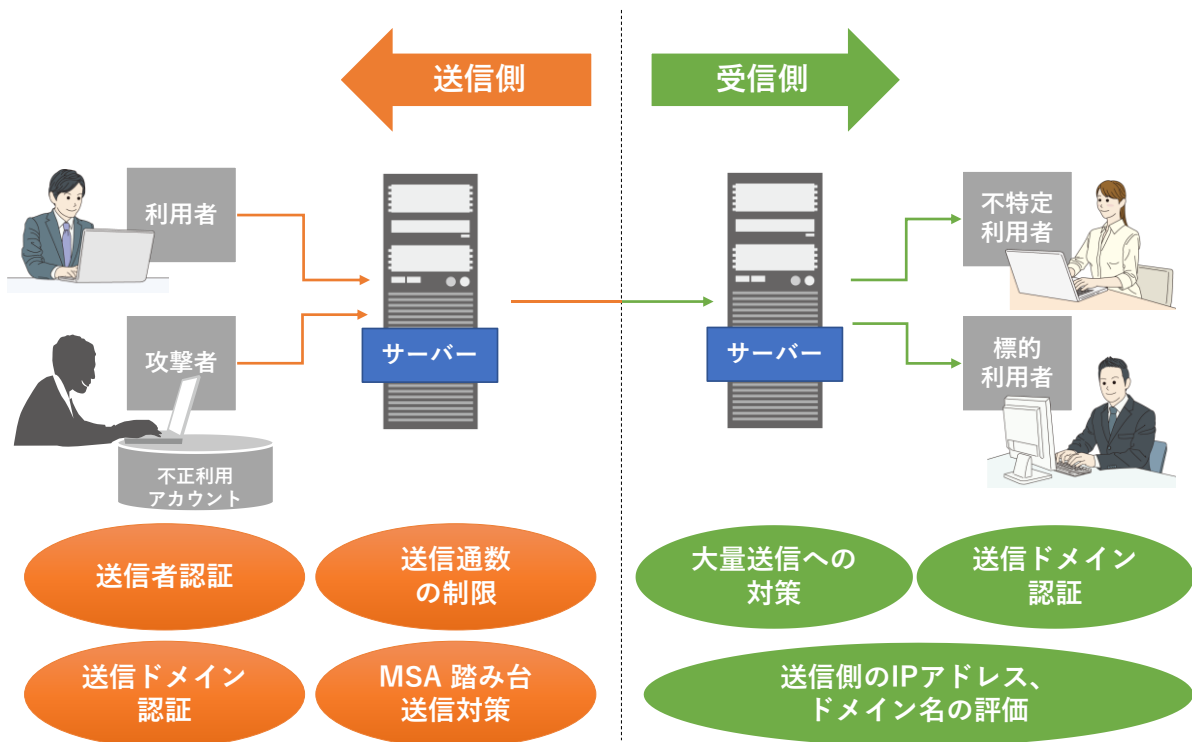
第2節 技術的な対策

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



第1章

第2章

第3章

第4章

参考編

資料編



2 送信側での対策

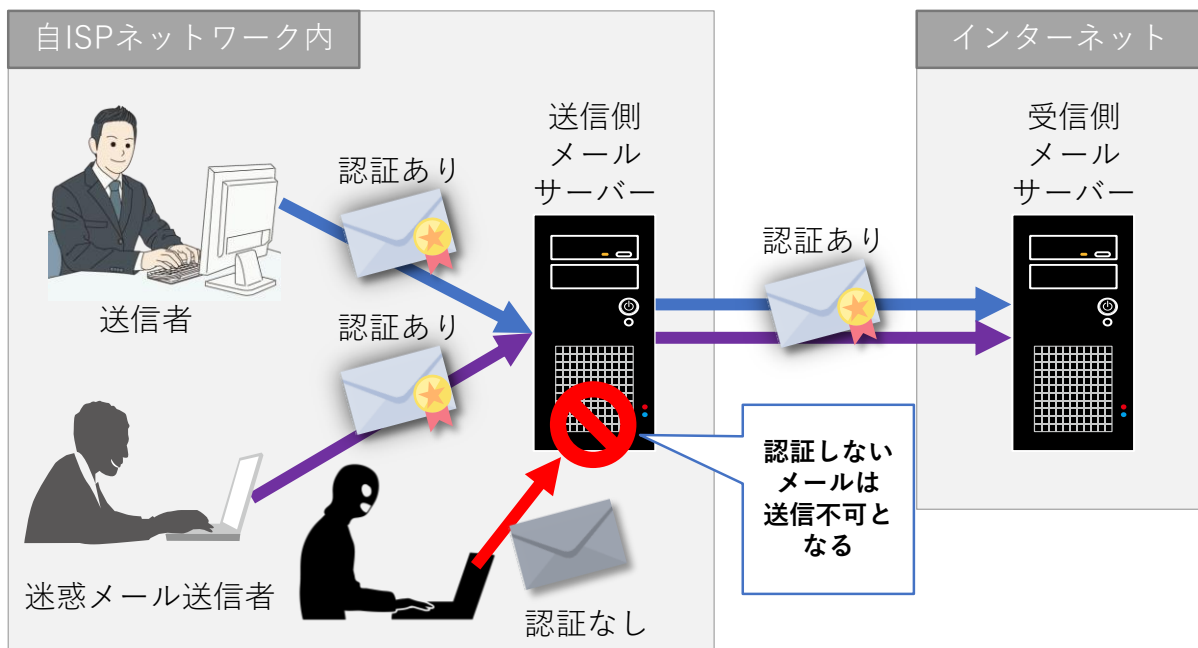
固定 IP アドレス^{注81}を取得して送信する方法は、契約者情報の確認を適切に実施していれば送信元を特定できることから、利用停止などの運用的な対処や法的対処が比較的容易です。一方、ASP^{注82}や共用ホスティングサービス^{注83}の送信メールサーバーは、該当のサービスを契約している不特定多数の利用者を前提にしているため、その中に紛れ込んだ迷惑メールの送信を制限することは容易ではありません。そのため、効果があると思われる技術的な対策を組み合わせることで対応が行われています。

(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84}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及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ようになります。

図表3-2-2 送信者認証 (SMTP-AUTH)を用いた対策



注81 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82 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83 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、複数の利用者が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84 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。



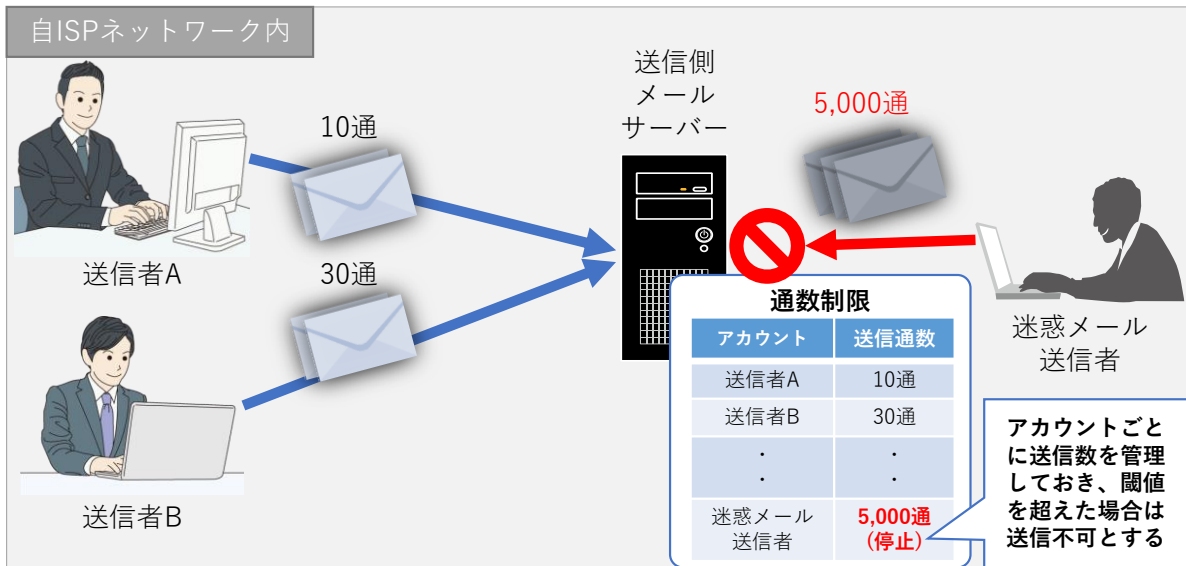
(2) 電子メールの通数を制限する方法

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85}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ー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85} 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ドレス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ます、「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ドレスからの電子メールが送信できないことに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。

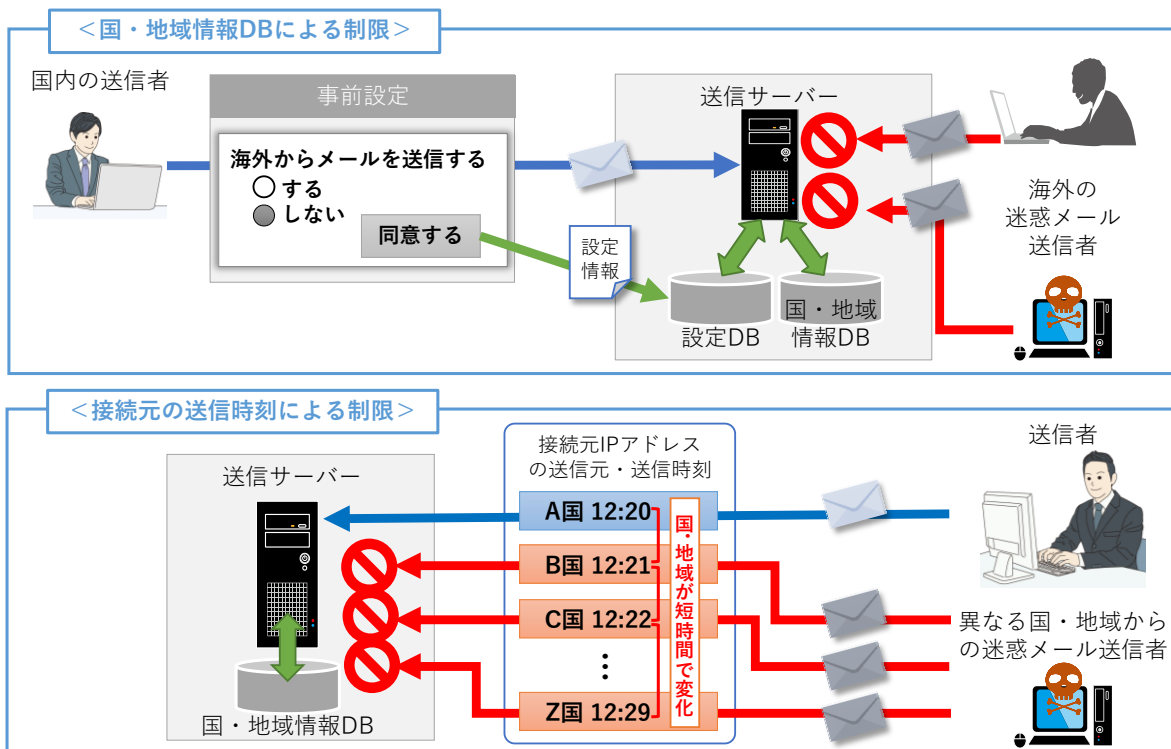
(ア) 接続元情報による制限

送信側で、それぞれの電子メールアドレスがどの接続元 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ドレス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ドレス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、そのメールアドレス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



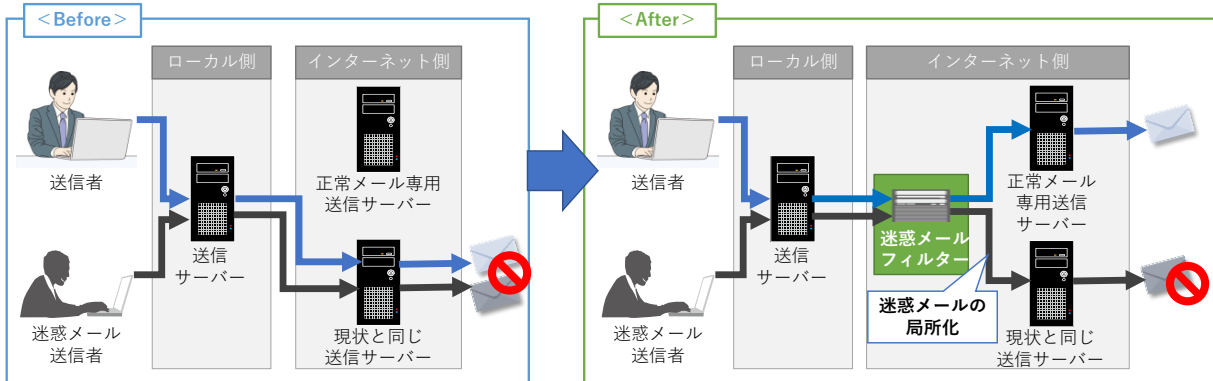


第3章 迷惑メール対策

(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ドレス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ドレス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。

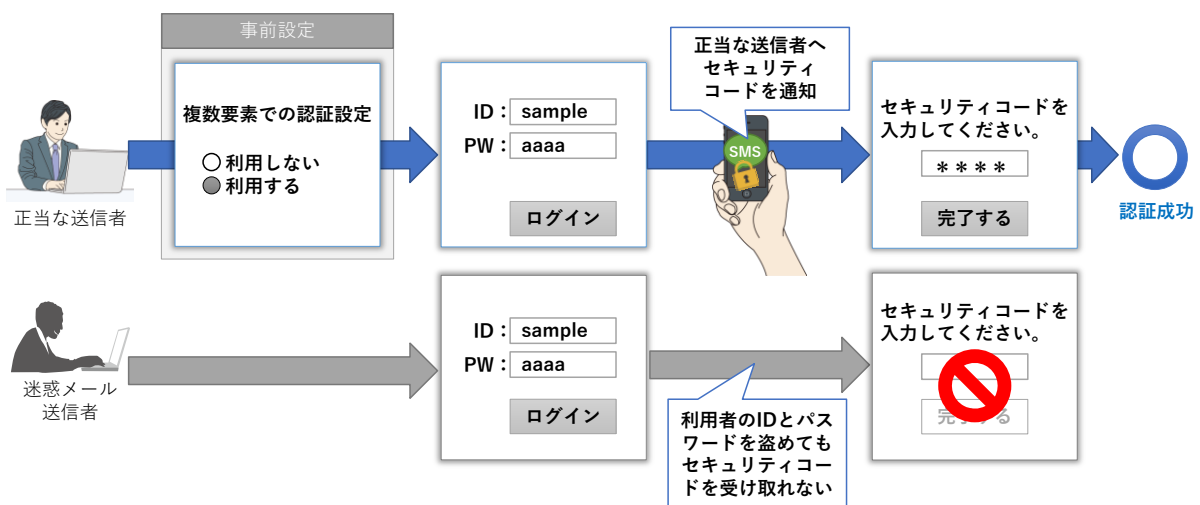
図表 3-2-5 送信メールサーバーの分離対策



(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86}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



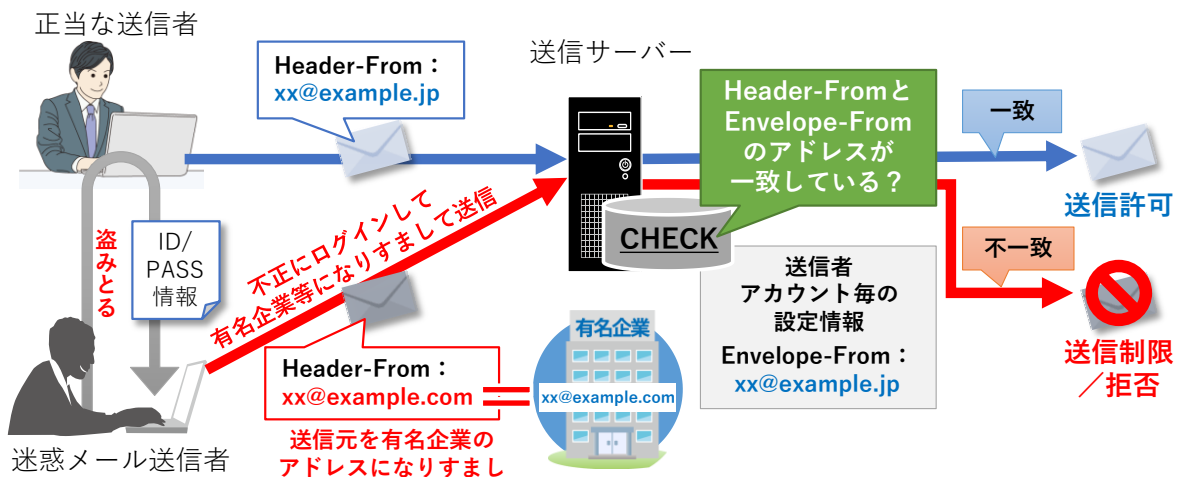
注86 一時的にしか使えないパスワードを通知し、その入力を求める認証のこと。



(工) 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。

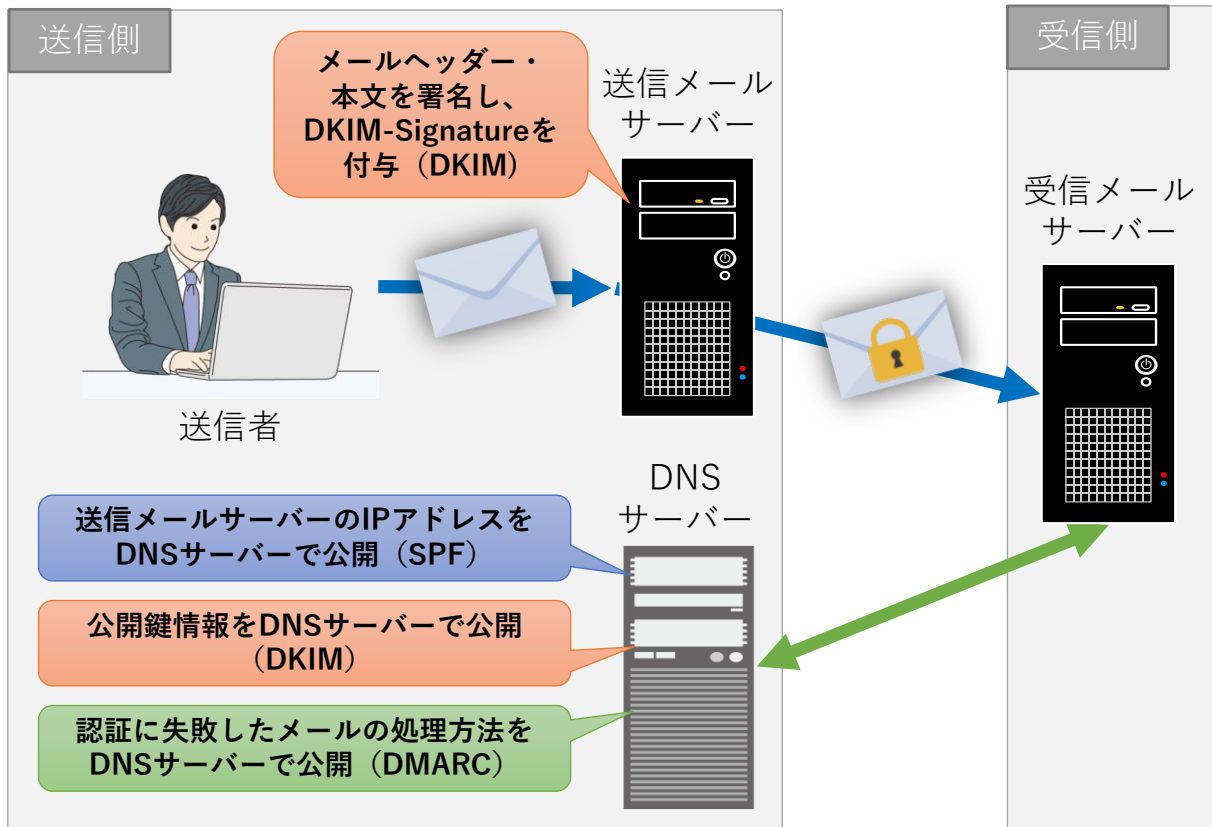
送信ドメイン認証技術とは、受信側が、電子メールを送信した側のドメイン名の正当性を確認することができる技術で、送信側での設定と受信側での検証とにより対応するものです。

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87}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87} 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88}」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88}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4版）」https://www.jaipa.or.jp/other/mtcs/guideline_v4.pdf



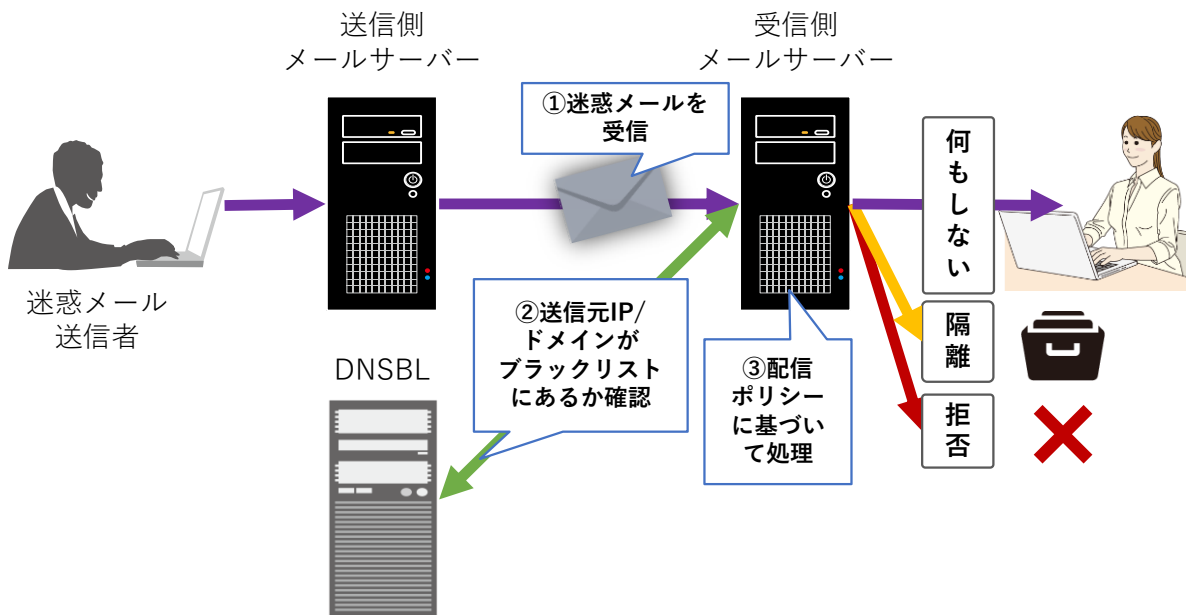
(3) IPアドレスやドメイン名のレピュテーション

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89}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90}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89 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。

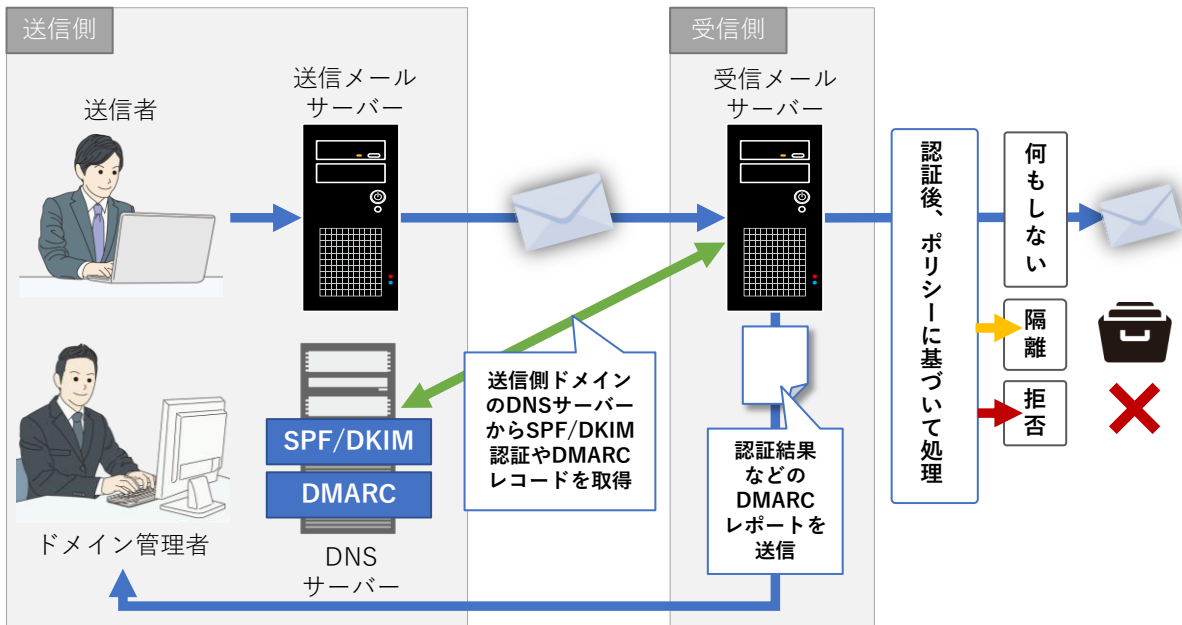
注90 元になる情報量が十分あり、かつ、著しく恣意的な情報を使わないなどの配慮がなされたレピュテーションのこと。



(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及びフィルタリング

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91}) 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。

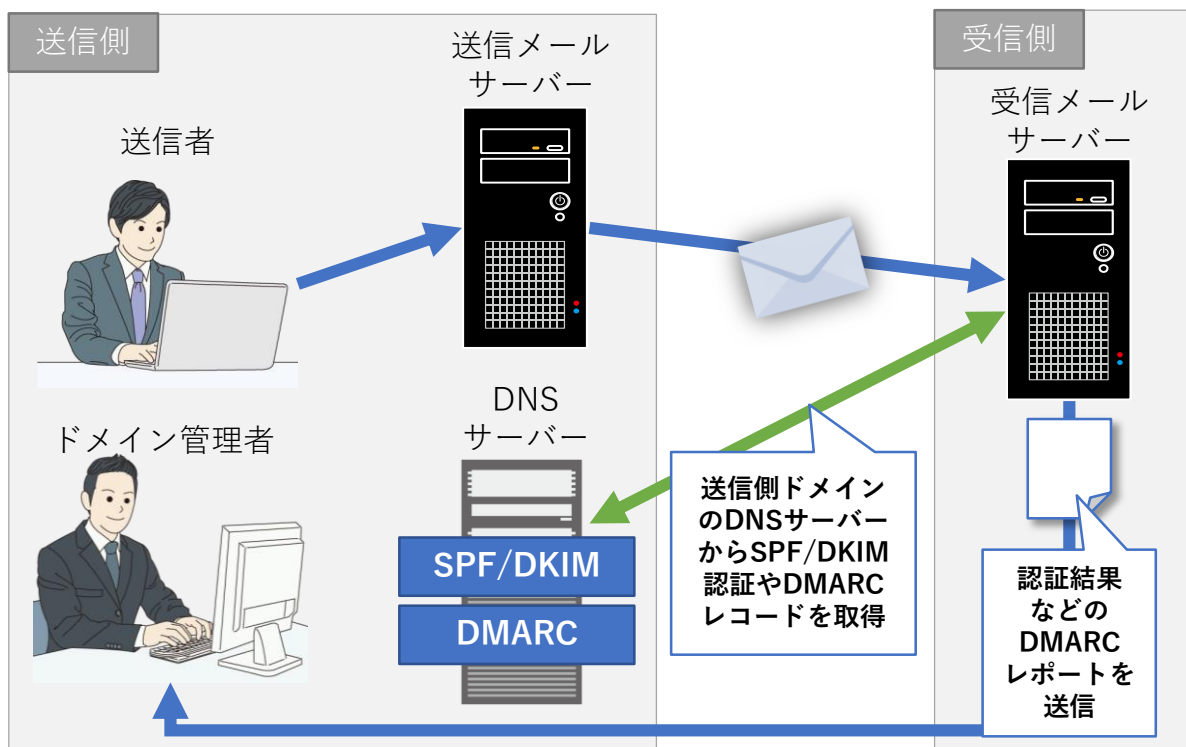
注91 RFC7001 で規定



(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。その標準化及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。



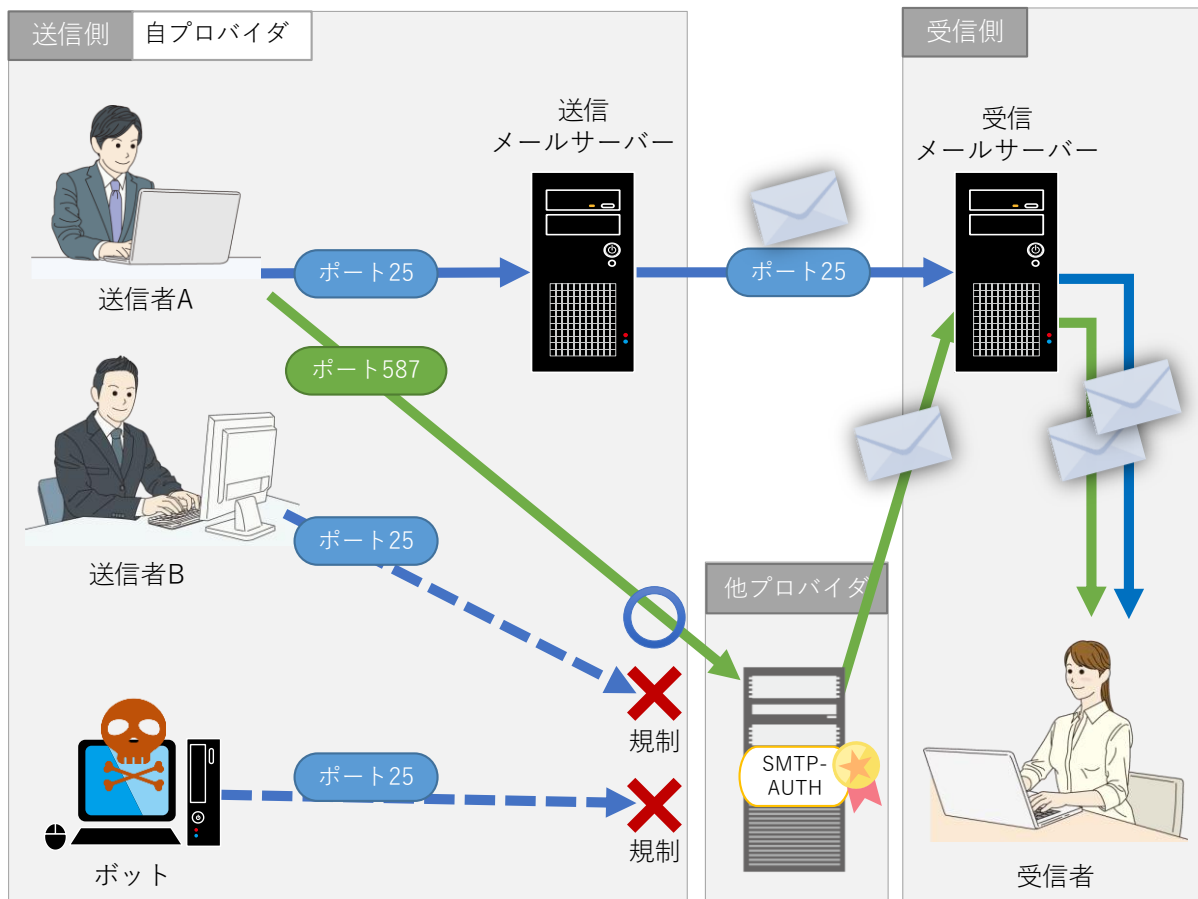
トピックス : OP25B (Outbound Port 25 Blocking)

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92}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92 (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 及び 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

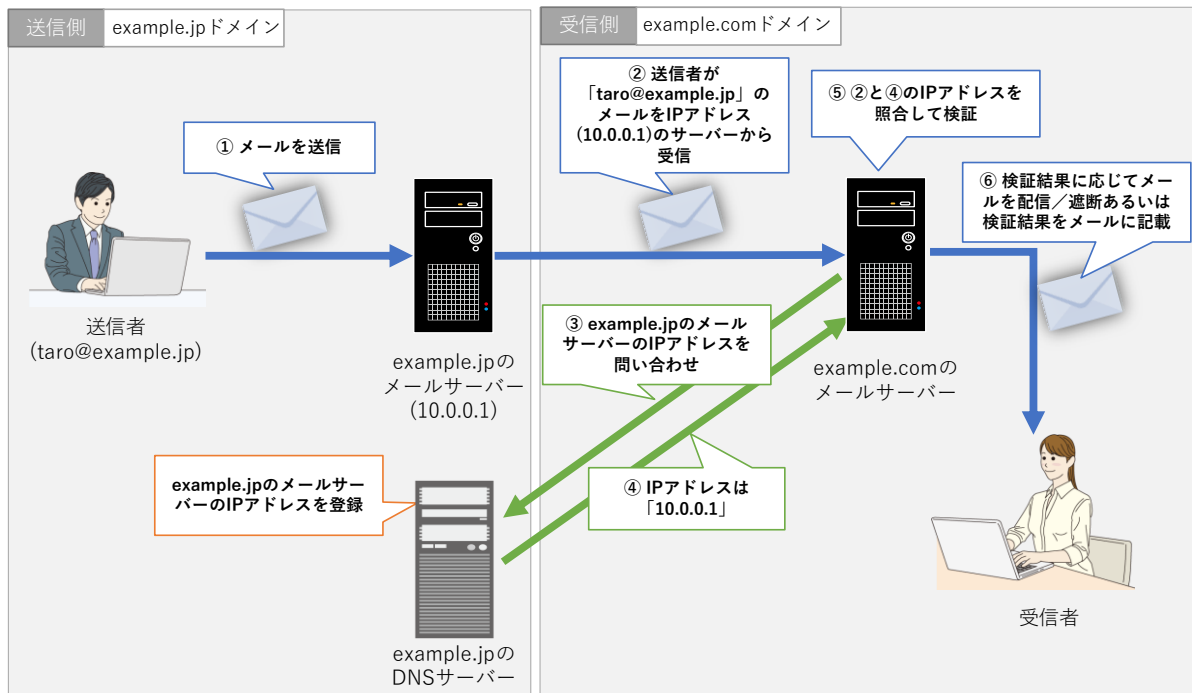


(1) SPF (Sender Policy Framework)

SPF は、RFC7208^{注93}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94})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達など。) 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93 <https://tools.ietf.org/html/rfc7208>

注94 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。

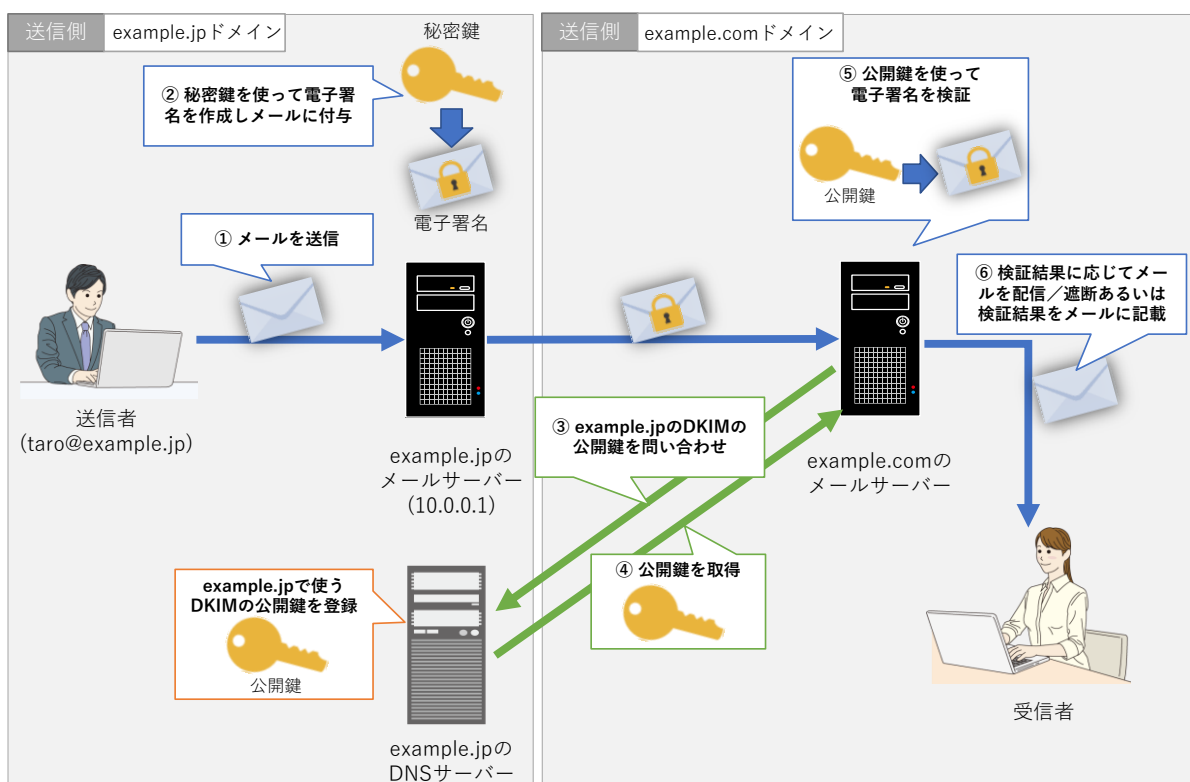


(2) DKIM (DomainKeys Identified Mail)

DKIM は、STD76^{注95}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96}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97}）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の認証及び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、なりすましが無いものと判断します。

注95 <https://tools.ietf.org/html/std76>

注96 <https://tools.ietf.org/html/rfc7489>

注97 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。



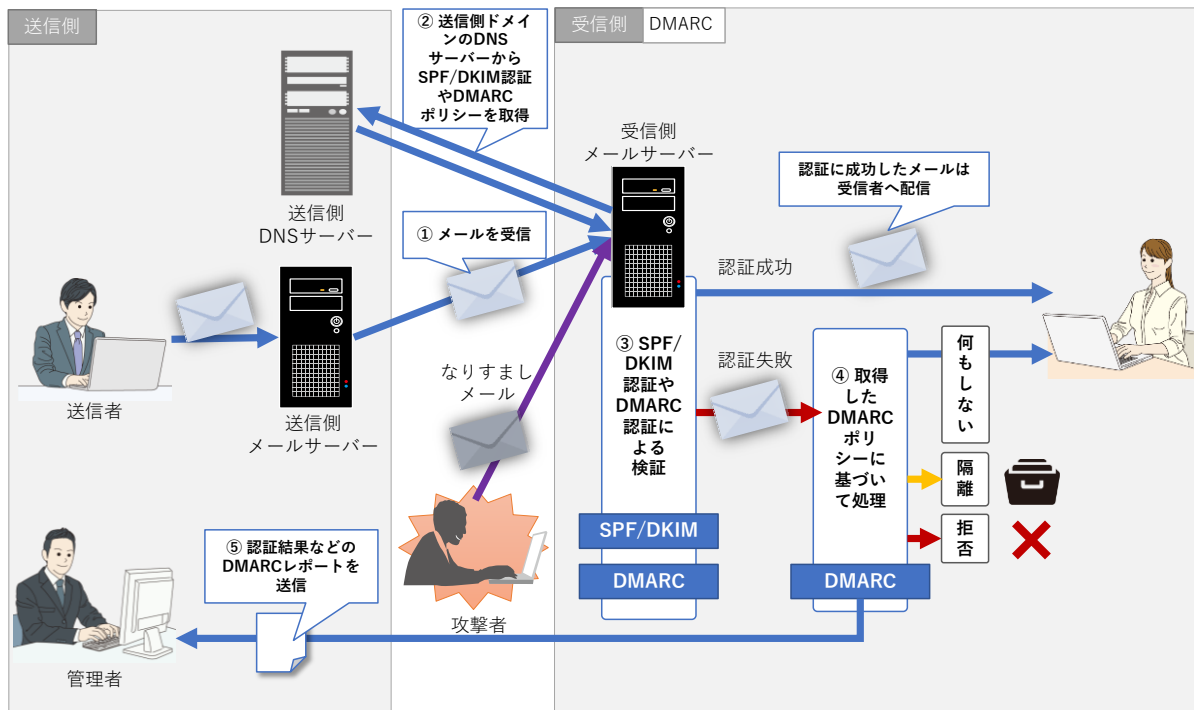
なお、SPF の認証と DKIM の認証をどのように用いるか（一方のみを用いるなど）については、送信者側で、送信者情報である電子メールアドレスのドメインの DNS 上で宣言することにより設定します。

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ト機能です。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、再配達された場合など 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、再配達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、再配達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、再配達された場合でも 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、注意する必要があります。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、事業者を確認の上、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98}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へ誘導し、そこで巧妙に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98} (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するのですが、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99}、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や(一財)日本産業協会内にある電子商取引モニタリングセンターで法律違反と思われる迷惑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。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なるためです。

^{注99} (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電子メールアドレスを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、気づかぬうちに、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 番ポートを利用する

利用している ISP などが 587 番ポートでの接続を提供しているときには、587 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 関連組織や携帯電話事業者

関連組織	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100} 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101} 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102} 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103} 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104} 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	<ul style="list-style-type: none"> ・(独)国民生活センターのウェブサイト^{注105}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

注100 <https://www.dekyo.or.jp/soudan/aspc/report.html#auth>

注101 http://www.soumu.go.jp/main_sosiki/joho_tsusin/kyouiku_joho-ka/jireishu.html

注102 http://www.soumu.go.jp/main_sosiki/joho_tsusin/d_faq/index.html

注103 https://www.dekyo.or.jp/soudan/data/info/gmeiwaku_book.pdf

注104 <https://www.dekyo.or.jp/soudan/data/chain/chainbook.pdf>

注105 <http://www.kokusen.go.jp/mimamori/index.html>



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		「スマホ・タブレットまるわかりBOOK」 迷惑メール対策を含む利用者向けの冊子	・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106} からダウンロード
		「iPhone・iPad まるわかりBOOK」 迷惑メール対策を含む利用者向けの冊子	・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107} からダウンロード
KDDI(株)		「設定&サービスガイドブック (Android 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108} からダウンロード

注106 <https://www.nttdocomo.co.jp/support/utilization/maruwakari/index.html>

注107 https://www.nttdocomo.co.jp/iphone/support/startup_guide/

注108 https://cdn.softbank.jp/corp/set/data/csr/responsibility/safety/rule/pdf/smartphone_guidebook.pdf



図表3-3-2 関連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

関連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109} 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又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110} を通じた情報提供も可能
(一財)日本産業協会 電子商取引モニタリングセンター	spam-in@nissankyo.jp	左記の電子メールアドレスへ特定商取引法に違反していると思われる電子メールを転送することにより情報提供が可能 また、ウェブフォーム ^{注111} を通じた情報提供も可能
(株)NTT ドコモ	imode-meiwaku@nttdocomo.co.jp	iモードに対応した携帯電話又はスマートフォンの場合、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）
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112} 又はウェブフォーム ^{注113} 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109 <http://plugin.antispam.soumu.go.jp/>注110 https://www.dekyo.or.jp/bingo/mail_ihan_meiwakuform/index.html注111 <https://www.nissankyo.or.jp/spam/form-a.html>
<https://www.nissankyo.or.jp/spam/form-b.html>

注112 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113 <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) OP25B 及び送信ドメイン認証技術と通信の秘密の関係

OP25B 及び送信ドメイン認証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 114}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。

^{注114} 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
1
章

第
2
章

第
3
章

第
4
章

参
考
編

資
料
編

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。

2018年4月現在、協議会の構成員は57名で、幹事会の構成員は36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年目の本年より、体裁を改めた「迷惑メール白書」（本書）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。



2017年度の協議会の主な活動内容は、迷惑メールに関する一般利用者のリテラシー向上と防止技術の普及促進への寄与を目的に行った「Stop! 迷惑メールの日」の創設など、以下のような取組を行っています。

- 「Stop! 迷惑メールの日」の創設（2017年7月10日）
- 情報セキュリティワークショップ in 湯沢 2017 への参加（2017年10月6、7日）
- 迷惑メール対策推進協議会第10回総会の開催（2017年11月8日）
- サイバーセキュリティシンポジウム道後 2018 への参加（2018年3月1、2日）
- 技術WGの開催（2017年5月19日、6月30日、8月25日、10月13日、12月8日、2018年1月19日、3月16日）

図表4-1-1 迷惑メール対策推進協議会第10回総会（2017年11月8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、2018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5.79件と、オプトアウト方式による規制時の約6倍になっています。

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、2018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115}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	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		ブラックワード	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、認証自社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。
ブラックワード	送信者アドレス、件名等を組み合わせることで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「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その導入の状況」（2017年6月30日）の概要より抜粋

http://www.soumu.go.jp/menu_news/s-news/01kiban18_01000029.html

^{注115} 2009年以降に公表した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

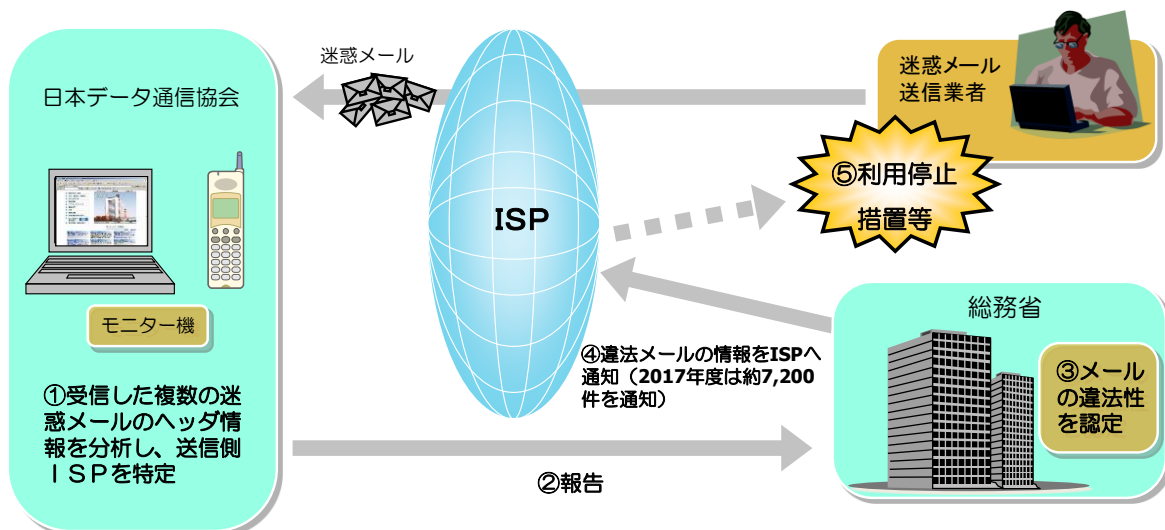
総務省及び消費者庁は、民間事業者による自主的な迷惑メール対策を促す「迷惑メール追放支援プロジェクト」を2005年から実施しています（2009年に消費者庁発足する以前は、総務省及び経済産業省が実施）。

特定電子メール法の観点からは、モニター機で受信した電子メールのうち、同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、2017年度は約7,100件の通知を実施しました。

また、特定商取引法の観点からは、モニター機や消費者からの情報提供により電子メール広告の情報を収集した電子メールのうち、同法違反が確認された電子メールに関する情報をホスティングISPなどに通知することで、契約約款などに基づく利用停止措置などを促しております。あわせて、不当請求を行っている事例から悪質事業者の口座情報がわかった場合には、消費者庁から金融庁に対し、口座情報の提供も行っています。

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1章

第2章

第3章

第4章

参考編

資料編



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1億6千万件を超え^{注116}、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117}。

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116} (一社)電気通信事業者協会「事業者別契約数」
<http://www.tca.or.jp/database/index.html>

^{注117} 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118}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119}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120}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118} ・(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)「迷惑メールでお困りのとき」
<https://www.softbank.jp/mobile/support/antispam/>

^{注119} ・(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/>

・ソフトバンク(株)「考えよう、ケータイ ～情報モラル授業プログラム～」(ソフトバンク(株)がNPO法人企業教育研究会と協力して実施するもの) <https://ace-npo.org/info/kangaeyou/index.html>

^{注120} ・(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)「メール送受信の際の注意」
<https://www.softbank.jp/mobile/support/antispam/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121}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業者間で交換する取組を行っており^{注122}、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123}。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121} 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122} (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」

<http://www.tca.or.jp/mobile/sms-mail.html>

^{注123} (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）

http://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ゲートウェイ的に提供する、いわゆるクラウド型のサービスプロバイダも増えています。

サービスプロバイダにおける迷惑メール対策としては、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ことで、利用者に届けないようにするため、送信ドメイン認証技術などを用いた迷惑メール判定サービスなどを提供しています。また、サービスプロバイダでは、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に参加し、迷惑メールに関する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、M³AAWG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 といった標準化組織の議論にも参加しています。

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側と送信側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

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を迷惑メールか否かの判断に利用する迷惑メールフィルターを提供しており、フィルターの提供元が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ます。

送信ドメイン認証と認証結果に基づく処理

迷惑メールか正当な電子メールかの判断などに利用することができるよう、SPF や DKIM に加えて DMARC を併用した認証を行い、認証結果に基づくヘッダーへの認証結果の記述やフィルタリングなどの処理を行ったり、認証結果を踏まえたドメイン名の評価（ドメイン名のレピュテーション）を行ったりしています。なお、図表 4-2-1（85 ページ）のとおり、送信ドメイン認証を送信側に導入しているサービスプロバイダは多い一方、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

電子メールの受信時に、迷惑メールフィルターを導入したり、送信ドメイン認証を実施したりしていた場合でも、その結果が受信者に適切に示されないようであれば、対策としての意味がありません。不要な迷惑メールは参照できないようにすべきであり、判断が難しい電子メールや利用者が受信を望む場合には、適切に結果を参照



できるようすべきです。そのため、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、送信側としても適切に最新技術に対応することで、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)

サービスプロバイダは SMTP-AUTH を導入しており、その認証結果を一定期間保存することで、電子メールアカウントの認証情報を不正利用され MSA 踏み台送信などが行われた場合に、一時的な利用停止、パスワード変更などの対応を行っています。また、短い間で大量に電子メールが送信されていないか、短時間に地理的に離れた送信元から電子メールが送信されていないかなど、電子メールアカウントが不正利用されていないかどうかの監視を常に行っています。

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 (85 ページ) 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。



利用停止などの取組

サービスプロバイダでは、利用者の同意を得ながら電子メールの送信元を制限することや、迷惑メールに関するレポート（フィードバックループ^{注124}）から不正利用されている利用者を特定し、一時利用停止するなどの取組も行っています。なお、認証情報を窃取され、不正利用されたために利用停止措置を受けた利用者には、パスワードを適切なものに変更するなどのアドバイスをしています。

また、サービスプロバイダでは、自社のメールサーバーから迷惑メールが送信される場合には、WHOIS^{注125}などにより送信元のメールサーバーのIPアドレスの管理元と判断され、ブラックリストに登録されるおそれもありますので、迷惑メールの送信が行われたというフィードバックループや、適切なブラックリスト運営者などからの問い合わせがあった場合には、利用停止なども含めた対応をしています。

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。

^{注124} メールを受信者が送信者（サービスプロバイダ）に対して迷惑メールの苦情などの情報を伝える仕組みのこと。

^{注125} ドメイン名やIPアドレスの運用者などに関する情報を誰でも参照可能とする公開データベースのこと。



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及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が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术の開発と取組

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126}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、新技术の紹介、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126} 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。



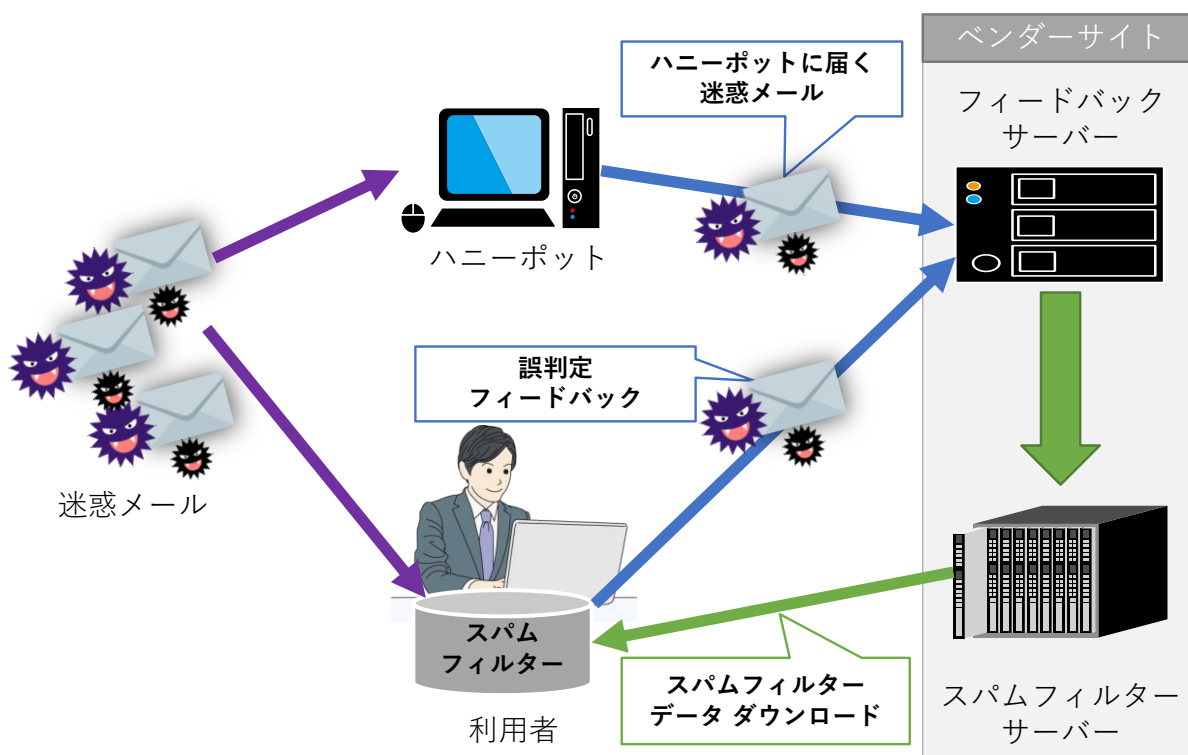
第4章 迷惑メール対策の取組

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パイフィッシング（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



第1章

第2章

第3章

第4章

参考編

資料編



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み

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及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及び送信目的・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2017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(2,624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43万件)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1,664万件)。

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、総務省及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7,200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。



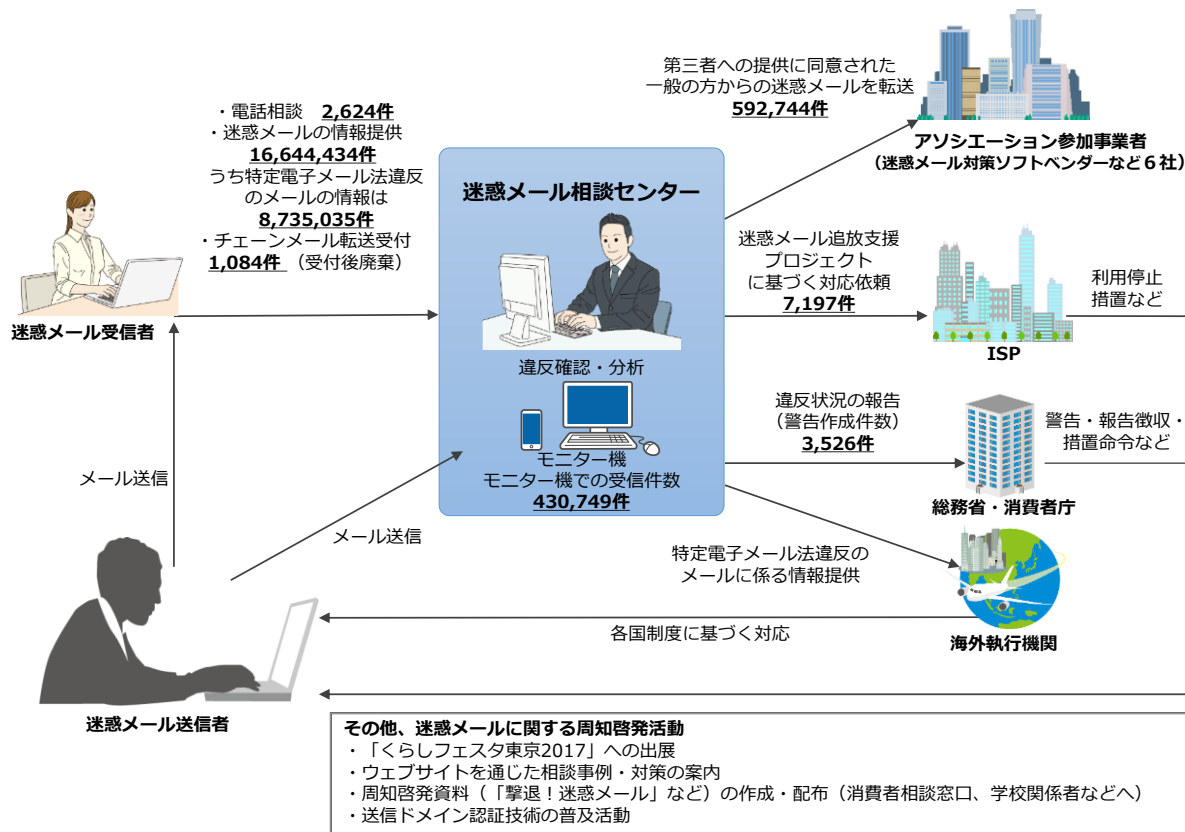
セキュリティベンダーなどへの情報提供

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59万件）^{注127}。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としています。

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



注127 (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)日本産業協会 電子商取引モニタリングセンター

(1) 概要

(一財)日本産業協会の電子商取引モニタリングセンターでは、2001年にインターネット通信販売のモニタリング事業を開始し、2002年には消費者からの情報提供窓口を設置して迷惑メールの調査も開始しました。

現在は、2005年に経済産業省が発表した「迷惑メール追放支援プロジェクト」に基づく調査に加え、危険ドラッグ販売サイトや外貨決済を利用する出会い系サイトの調査、また、スマートフォンの普及に伴い利用が急増しているアプリストアの調査や、インターネットオークション、テレビ通販などの調査を実施しています。なお、センターでは、消費生活アドバイザー有資格者の調査員が、当事業を通じて、電子商取引の円滑な推進と消費者被害の防止のための監視を行っています。

(2) 主な活動内容（括弧内の数値は2017年度の実績）

迷惑メールの収集

センターに設置したモニター機で迷惑メールを収集（約380万件）するとともに、センターのウェブサイトを通じ消費者から特定商取引法に違反すると思われる電子メール（迷惑メール）の情報提供を受け付けています（約270万件）。

迷惑メールの分析

収集した迷惑メールについて、その広告元であるウェブサイトの運営者の調査を行い、特定商取引法違反の有無の分析を行っています。

また、モニター機で受信した迷惑メールについては、送信元ISP、発信国の分析を行っています。

関係機関への情報提供

特定商取引法違反と判断された電子メール・広告サイトについては、違反内容及び事業者情報などの詳細を消費者庁へ報告しています（49,851件）。

さらに、我が国の消費者に向けた中国発の広告メールの急増を受け、2007年より、消費者庁を通じて中国の関連機関（中国インターネット協会（ISP））へ情報を提供しています。

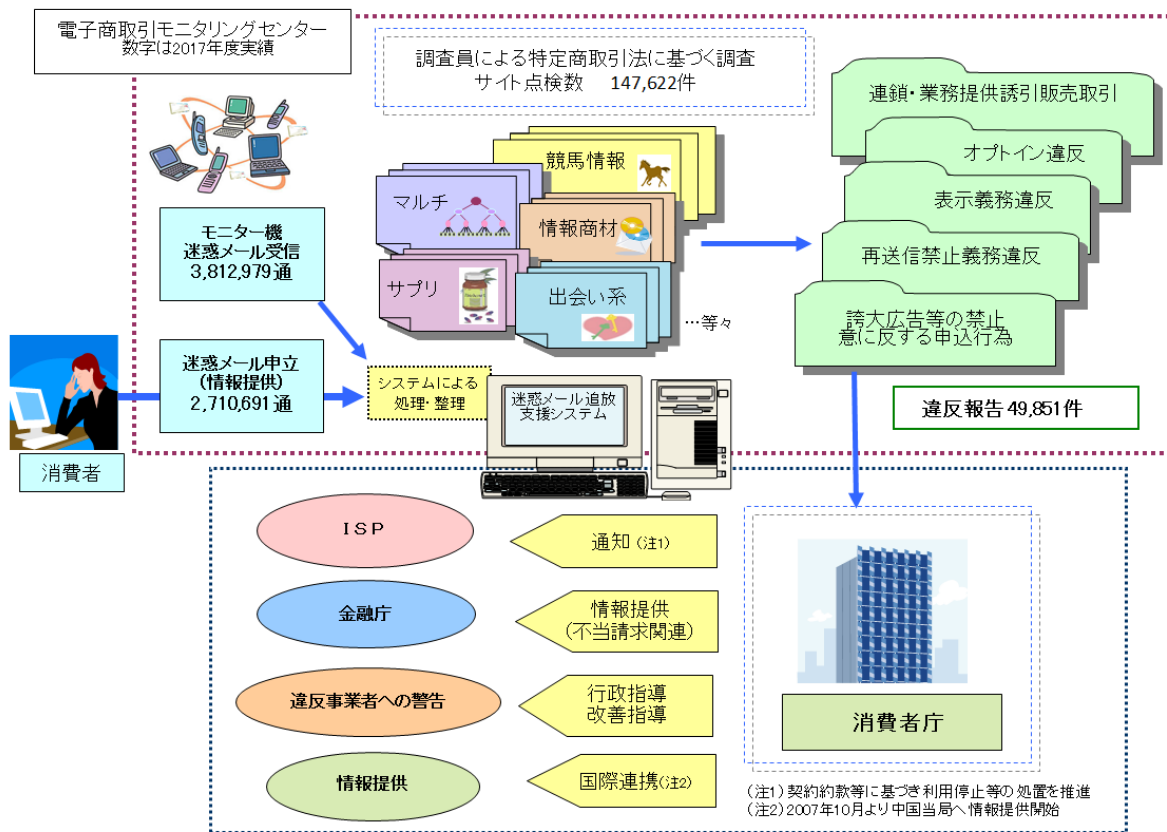
一般消費者への啓発

情報提供された電子メールを分析し、最新の迷惑メールの動向や悪質サイトの仕組みをセンターのウェブサイト^{注128}で公表し、一般消費者への注意喚起を行っています。

^{注128}(一財)日本産業協会「迷惑メール調査最前線！」<http://www.nissankyo.or.jp/mail/index/index.html>



図表4-4-2 電子商取引モニタリングセンター活動模様



第1章

第2章

第3章

第4章

参考編

資料編



3 (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の第10回会合(LAP10 TOKYO)と併催し、さらに、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129}を東京と大阪で合同開催したことで、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。

図表4-4-3 第17回迷惑メール対策カンファレンス(東京)の様子



^{注129} 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



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130}」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131}」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132}など、迷惑メール対策及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130} (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」

http://salt.iajapan.org/wpmu/anti_spam/

^{注131} なりすまし対策のポータルサイト ナリタイ

<https://www.naritai.jp/>

^{注132} DMARC.orgのウェブサイト

<https://dmarc.org/>



4 (独)国民生活センター

(1) 概要

(独)国民生活センターは、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1,200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・立案及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年度に4万5,000件を超える相談が寄せられたことから、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133}。

その際、消費者へのアドバイスとして、心当たりのない不審なメールが届いた場合は、開かずには削除することが前提となること、心当たりのない不審なメールなどに決して反応しないことに加え、事前に迷惑メールに関するトラブル防止のための対策をするよう呼びかけました。さらに、迷惑メールをきっかけにした架空請求や出会

^{注133} 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



い系サイトなどに関するトラブルも生じていることから、これらのトラブルに巻き込まれた場合には、すぐに最寄りの消費生活センターなどに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」

お住まいの地域の市区町村や都道府県の消費生活センターなどをご案内する全国共通の3桁の電話番号です。

図表4-4-4 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 402100502918】

平成29年7月6日
独立行政法人国民生活センター

**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！—**

全国の消費生活センター等には、携帯電話やパソコン等に届く電子メールやSMS（ショートメッセージサービス）等のうち、いわゆる「迷惑メール」が関連した相談が寄せられており、2014年度以降増加しています。その内容は、「迷惑メールが1日に何十通も送られてくる」といった迷惑メールの受信に関するトラブルのほか、「有料サイトの米納料金を請求するSMSが届き、支払ってしまった」、「お金がもらえるという当選メールが届き、受け取るための費用を支払ったが入金されない」という迷惑メールをきっかけに他のトラブルになってしまったもの等がみられます。

そこで、最新の相談事例やアドバイスをまとめ、消費者に情報提供します。

1. P10-NETにおける相談件数
迷惑メールに関する相談件数は、2012年度から2013年度にいったん減少しましたが、2014年度以降、増加傾向にあります（図1）。また、契約当事者¹の年代をみると、2012年度以降、60歳以上の割合が年々高まっています。

図1. 相談件数の推移

年度	相談件数	60歳以上の割合
2012年度	25,125	28.2%
2013年度	24,294	28.2%
2014年度	34,203	33.2%
2015年度	42,980	41.5%
2016年度	45,176	45.5%

1 P10-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、2017年5月31日までの集計数。消費生活センター等からの経由相談は含まれていない。なお、2016年度の相談件数（2016年5月31日までの集計数）は2,306件。
2 本資料内では、「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）と「特定徴収料に関する

図表4-4-5 メールマガジンによる注意喚起

見守り新鮮情報

申し込んだ覚えはないのに、数億円当選したとのメールがスマートフォンに**何度も届く**ので、本当に当選したかかもしれないと思い**返信**した。当選金を受け取るには**登録料1万円**がかかると言われ、**指示されるままに**プリペイド型電子マネーのギフト券をコンビニで購入して、番号を写真に撮って**送信**した。その後も**手数料等の名目で請求**があり、合計で**5万円**ほど支払ってしまった。返金してほしい。(60歳代 男性)

「数億円当選した」はずが5万円の支払いに迷惑メールは無視

ひとこと助言

- 「有料サイトの料金が未納」「当選したのでお金がもらえる」などの心当たりのないメールやSMS（ショートメッセージサービス）が届いても、絶対に開かず、すぐに削除してください。
- 安易に連絡をしてしまうと、金銭を要求されたり、個人情報を開き出されたりする危険があります。メールの内容には反応しないようにしましょう。
- 不安を感じたときや困ったときは、早め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

迷惑メールは無視

※本資料は、消費者ホットライン188による注意喚起です。



5 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。

2018年3月末現在、協議会には正会員38社と賛助会員29社、他に、リサーチパートナー5名とオブザーバー7団体、関連団体10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

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、一般消費者に対して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（一社）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、セキュリティ対策事業者などに、フィッシングサイトの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

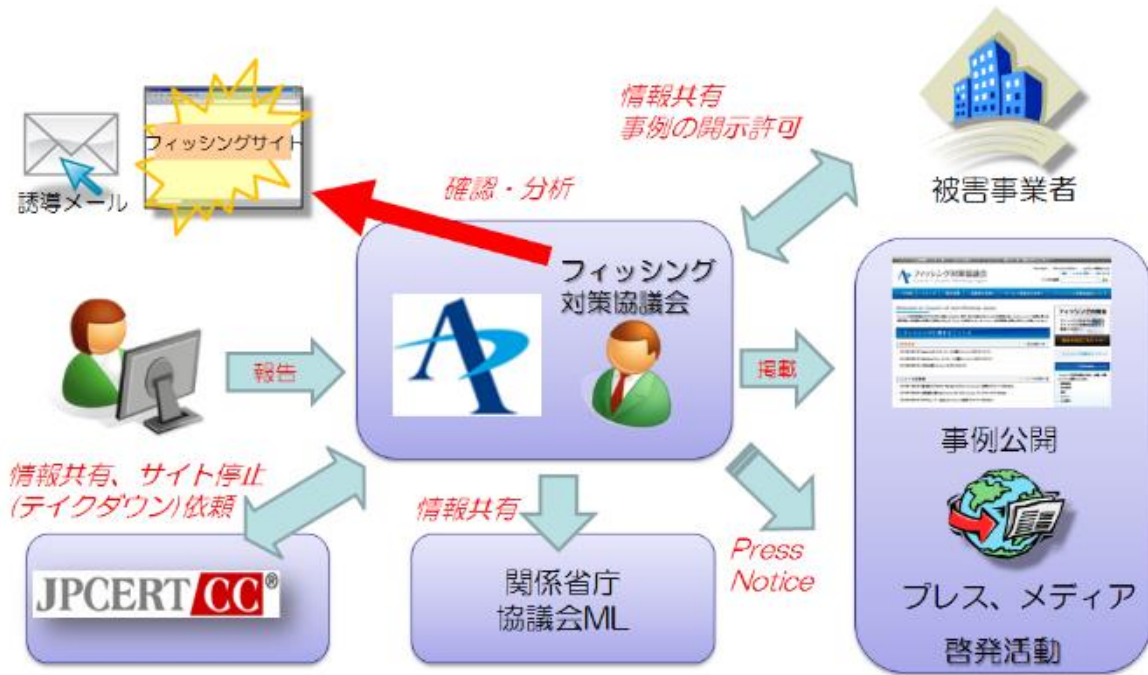
協議会内には、正会員が参加することができるワーキンググループ（以下、WG）があります。現在、ガイドライン策定WG、STOP. THINK. CONNECT.（STC）普及啓発WG、証明書普及促進WGの3つのWGがあり、フィッシング詐欺対策に資するガイドラインの策定や啓発イベントの開催を主導しています。2017年6月、ガイドラインWGが策定した「フィッシング対策ガイドライン2017年度版」を協議会ウェブサイトで公開しています。また、2018年2月、STC普及啓発WGがサイバーセキュリティ啓発イベント「カードゲームで学ぶセキュリティ」を主催しました。

セミナー及び勉強会の開催

協議会では、会員や一般の方々に対して、年に数回、セミナー及び勉強会を企画しています。2017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、複数回のセミナー及び勉強会を開催しました。



図表4-4-6 フィッシング対策協議会の活動イメージ



第1章

第2章

第3章

第4章

参考編

資料編

**(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、モノなどの実在性及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。

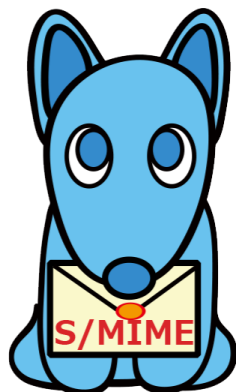
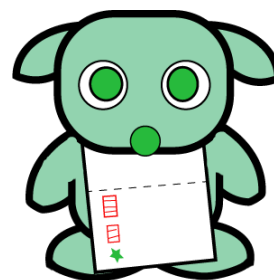
(2) 主な活動内容**迷惑メール対策技術の普及啓発**

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と一見難しそうなりすましメール対策技術に、それぞれのゆるキャラを作成し、親しみを持たせています。

図表4-4-7 S/MIME、DKIM、DMARCのゆるキャラのイメージ

エスマいぬ
(S/MIME)ディーキいぬ
(DKIM)ディーマーくんくん
(DMARC)



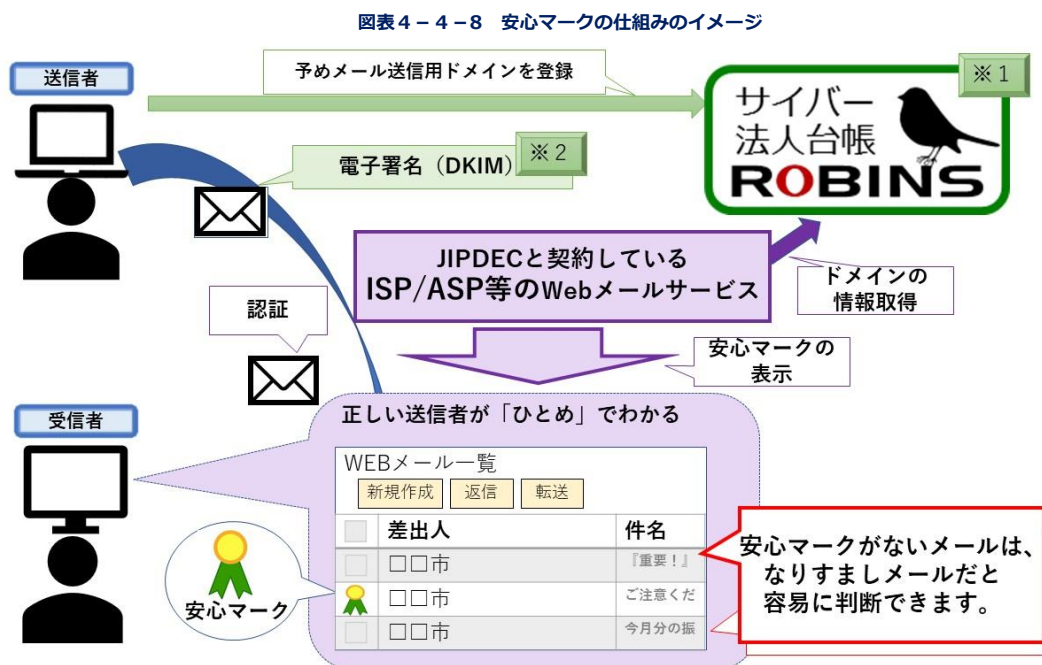
安心マークの普及

「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 M³AAWG (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。



※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



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、未承諾通信対策執行ネットワーク（UCENet : Unsolicited Communications Enforcement Network^{注134}）に名称を変更しています。

^{注134} UCENet ウェブサイト <https://www.ucenet.org/>



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）

<p>国際電気通信連合（ITU）</p> <ul style="list-style-type: none"> ✓ 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
<p>経済協力開発機構（OECD）</p> <ul style="list-style-type: none"> ✓ 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
<p>アジア太平洋経済協力（APEC）</p> <ul style="list-style-type: none"> ✓ 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
<p>アジア・太平洋電気通信共同体（APT）</p> <ul style="list-style-type: none"> ✓ 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月及び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
<p>日ASEAN情報セキュリティ政策会議</p> <ul style="list-style-type: none"> ✓ 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

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）

<p>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）））</p> <ul style="list-style-type: none"> ✓ 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 ✓ 2011年10月に開催された第7回会合では、日本のスパム対策の取組、法執行の強化などを説明 ✓ 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
<p>APCAUCE（Asia Pacific Coalition Against Unsolicited Commercial Email）</p> <ul style="list-style-type: none"> ✓ アジア・太平洋地域での迷惑メール対策関連の民間交流団体 ✓ 迷惑メールの現状、技術的対策・法的対策の状況などについて情報交換

最新の動向（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が



第4章 迷惑メール対策の取組

らスパム対策の取組状況に関する説明及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。

（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が確認されました^{注135}。

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136}。

（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137}。

注135 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136 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137 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



(2) 二国間などでの取組

共同声明など

総務省及び経済産業省が、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138}。

迷惑メール送信元情報の交換

2018年1月より、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139}。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：日米協カインシアティブ」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。

(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及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、特定電子メール法第30条に基づくものとして初めて2018年1月から情報交換が開始されました。

(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140}。

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。

^{注138} 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139} 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

^{注140} 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



第4章 迷惑メール対策の取組

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141}。同年2月、我が国で開催された第1回日印合同作業部会参加のため来日したインド通信IT省委員との間で、日本側から迷惑メール対策を含むサイバーセキュリティ協力を提案し、「迷惑メール対策連携プロジェクト」に大筋合意^{注142}、同年3月のドバイでの2国間会談において同プロジェクトの推進を確認しました。その後、(一財)日本データ通信協会がインドコンピューター緊急対応チーム(CERT-In)を訪問し、迷惑メール対策に関する具体的な手法などについて意見交換を行いました。それらを受けて、2014年12月に我が国で開催した第2回日印合同作業部会において、「迷惑メール対策日・印連携プロジェクト」を実施することを決定しました^{注143}。

2015年6月のLAP第11回会合の際、インド電気通信庁との間で迷惑メール対策に関する意見交換を行いました。また、同年11月に我が国で開催した第3回日印合同作業部会^{注144}、2017年6月に我が国で開催した第4回同部会においても、同様の意見交換をインド側と行いました^{注145}。

(エ) ベトナム

2010年10月、総務省及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146}、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147}。

(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148}。

注141 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142 総務省「第1回日印合同作業部会の開催結果」(2014年2月13日)

http://www.soumu.go.jp/menu_news/s-news/01tsushin09_02000025.html

注143 総務省「第2回日印合同作業部会の開催結果」(2014年12月4日)

http://www.soumu.go.jp/menu_news/s-news/01tsushin09_02000031.html

注144 総務省「第3回日印合同作業部会の開催結果」(2015年11月10日)

http://www.soumu.go.jp/menu_news/s-news/01tsushin09_02000042.html

注145 総務省「第4回日印合同作業部会の開催結果」(2017年7月29日)

http://www.soumu.go.jp/menu_news/s-news/01tsushin09_02000060.html

注146 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147 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148 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



(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149}。

(ク) 香港

2015年6月のLAP第11回会合の際、総務省及び(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及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、意見交換を行ったほか、2017年10月のUCENet第13回会合の際、NCC及びTTCとの間で、迷惑メール対策の現状及び今後の取組について意見交換を行いました。

(コ) 韓国

2009年5月、総務省及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150}。

2015年6月、LAP第11回会合の際に、総務省は、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及び今後の取組について意見交換を行いました。

2016年10月、総務省は、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ったほか、2017年10月のUCENet第13回会合の際、KISAとの間で、迷惑メール対策の現状及び今後の取組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151}。









^{注149} 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

^{注150} 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151} 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

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）

第1章

第2章

第3章

第4章

参考編

資料編



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局 (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おこなっています。

(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、メンバー間での協動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が、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。近年は、training session を設けたり、UCENet との joint meeting を開催したりしています。いずれも M³AAWG メンバーとゲストだけが参加できる会合ですが、それでも毎回 25~30 カ国から 300~500 名が参加する大規模なイベントとなっています。General Meeting では、実際のメール運用者や技術開発者、セキュリティの研究者などが参加し、その時点のホットな話題や対策技術などについて情報交換や対策についての議論などを行っています。こうした議論などで得られた知見などは、ベストプラクティスとして文書にまとめられ、ウェブサイト^{注 152}でも一般に公開されています。対策技術については、初期の頃から OP25B、SPF、DKIM の効果や普及状況などが共有されてきました。また、実務者ならではの課題や提案なども議論されており、特に DMARC は M³AAWG メンバーを中心に仕様が検討され、その後 IETF で標準化の検討が行われました。現在でも ARC や BIMi といった、新しい電子メールに関連する技術の検討が行われていますが、その大部分が M³AAWG を中心に検討されているものです。技術的な内容以外にも、各国の法規制に関する情報交換や、最近では欧州における一般データ保護規則 (GDPR (General Data Protection Regulation)) の施行による影響など、幅広い議論が行われています。このように、General Meeting は実際の運用者や技術仕様を作成している当事者らと直接議論できる貴重な場となっています。また、こうした機会が、新しい技術を生み出したり、背景を知ることでより普及が促進されたりするなどの効果をもたらしています。いまや M³AAWG は、国際的な迷惑メール対策組織として、ますますその役割が重要となってきています。

^{注152} <https://www.m3aawg.org/published-documents>

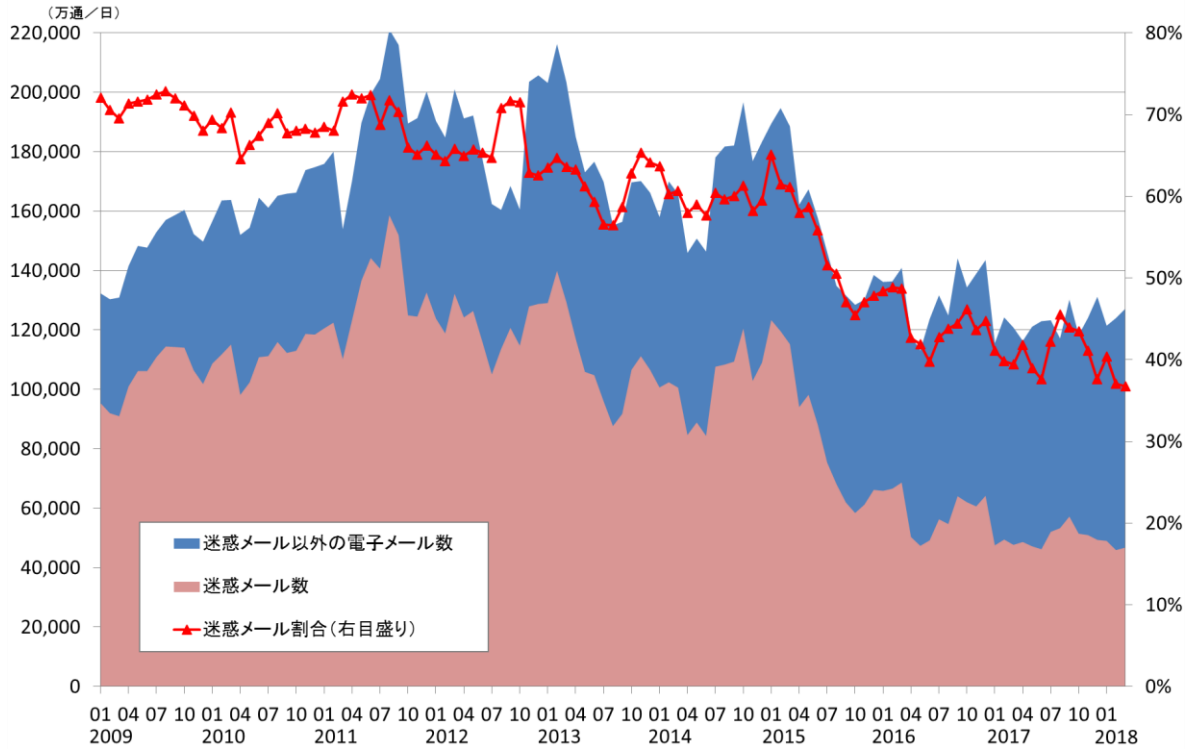
参考編



第1節 迷惑メールの量・割合の推移

第2章第3節に記した図表2-3-1を再掲し、その具体的な数値を以下に記します。

図表S-1-1 迷惑メールの量・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（2018年3月時点）」

2008年度（2009年1月以降のみ）

	4月	5月	6月	7月	8月	9月	10月	11月	12月	1月	2月	3月
電子メール総数（万通/日）	-	-	-	-	-	-	-	-	-	132,349	130,399	130,915
迷惑メール数（万通/日）	-	-	-	-	-	-	-	-	-	95,401	91,993	90,992
迷惑メール割合（%）	-	-	-	-	-	-	-	-	-	72.08	70.57	69.50
アカウント数（万アカウント）	-	-	-	-	-	-	-	-	-	8,487	8,643	8,792
フィルター利用者数（万アカウント）	-	-	-	-	-	-	-	-	-	3,974	4,133	4,269

2009年度

	4月	5月	6月	7月	8月	9月	10月	11月	12月	1月	2月	3月
電子メール総数（万通/日）	141,506	148,308	147,737	153,129	157,041	158,704	160,434	152,307	149,914	156,645	163,160	163,795
迷惑メール数（万通/日）	100,979	106,150	106,162	111,002	114,440	114,278	114,049	106,419	101,942	108,714	111,512	115,119
迷惑メール割合（%）	71.36	71.57	71.86	72.49	72.87	72.01	71.09	69.87	68.00	69.40	68.35	70.28
アカウント数（万アカウント）	8,764	8,833	8,799	8,827	8,865	8,892	8,874	9,041	8,972	8,916	8,879	8,942
フィルター利用者数（万アカウント）	4,245	4,299	4,268	4,290	4,317	4,346	4,331	4,501	4,606	4,397	4,350	4,402



2010 年度

	4月	5月	6月	7月	8月	9月	10月	11月	12月	1月	2月	3月
電子メール総数 (万通/日)	151,857	154,417	164,390	161,161	165,188	165,734	166,233	173,686	174,810	175,922	179,543	153,910
迷惑メール数 (万通/日)	98,063	102,360	110,739	111,223	115,954	112,195	113,020	118,596	118,461	120,550	122,218	110,212
迷惑メール割合 (%)	64.58	66.29	67.36	69.01	70.20	67.70	67.99	68.28	67.77	68.52	68.07	71.61
アカウント数 (万アカウント)	8,958	9,033	8,988	9,026	9,055	9,085	9,145	9,172	9,207	9,301	9,281	9,417
フィルター利用者数 (万アカウント)	4,389	4,453	4,430	4,474	4,498	4,382	4,454	4,479	4,504	4,532	4,517	4,632

2011 年度

	4月	5月	6月	7月	8月	9月	10月	11月	12月	1月	2月	3月
電子メール総数 (万通/日)	170,106	189,717	199,247	204,530	221,163	215,849	189,519	191,175	200,261	190,390	184,606	201,040
迷惑メール数 (万通/日)	123,283	136,618	144,175	140,664	158,654	151,864	124,950	124,407	132,573	123,885	118,807	131,116
迷惑メール割合 (%)	72.47	72.01	72.36	68.77	71.74	70.36	65.93	65.07	66.22	65.07	64.36	65.22
アカウント数 (万アカウント)	9,395	9,488	9,506	9,524	9,553	9,511	9,145	9,660	9,693	9,752	9,758	9,891
フィルター利用者数 (万アカウント)	4,607	4,685	4,671	4,682	4,703	4,669	4,770	4,746	4,812	4,869	4,844	4,979

2012 年度

	4月	5月	6月	7月	8月	9月	10月	11月	12月	1月	2月	3月
電子メール総数 (万通/日)	191,112	191,975	161,967	162,409	160,450	168,380	160,529	203,453	205,716	203,191	215,994	203,453
迷惑メール数 (万通/日)	124,171	126,296	117,912	105,070	113,627	120,699	114,735	127,855	128,778	129,083	139,692	129,437
迷惑メール割合 (%)	64.97	65.79	72.80	64.69	70.82	71.66	71.47	62.84	62.60	63.53	64.67	63.62
アカウント数 (万アカウント)	9,616	9,674	9,717	9,737	9,734	9,284	9,809	9,817	9,874	9,930	9,891	10,026
フィルター利用者数 (万アカウント)	4,948	5,000	4,993	5,012	4,912	5,066	5,079	5,064	5,117	5,154	6,581	6,787

2013 年度

	4月	5月	6月	7月	8月	9月	10月	11月	12月	1月	2月	3月
電子メール総数 (万通/日)	184,987	173,083	176,563	169,887	155,219	156,402	169,712	170,153	166,175	158,135	169,922	165,819
迷惑メール数 (万通/日)	117,025	105,907	104,711	96,045	87,646	91,758	106,622	111,196	106,560	100,787	102,304	100,600
迷惑メール割合 (%)	63.26	61.19	59.31	56.53	56.47	58.67	62.83	65.35	64.13	63.74	60.21	60.67
アカウント数 (万アカウント)	10,022	10,101	10,043	10,052	10,070	10,090	10,117	10,113	10,125	10,141	10,101	10,322
フィルター利用者数 (万アカウント)	6,830	6,929	6,998	6,949	7,086	7,249	7,296	7,308	7,362	7,410	7,367	7,571

2014 年度

	4月	5月	6月	7月	8月	9月	10月	11月	12月	1月	2月	3月
電子メール総数 (万通/日)	145,983	150,784	146,431	178,097	181,755	182,126	196,617	176,840	183,333	189,466	194,702	188,545
迷惑メール数 (万通/日)	84,669	88,905	84,384	107,673	108,357	109,399	120,445	102,854	109,001	123,355	119,590	115,221
迷惑メール割合 (%)	58.00	58.96	57.63	60.46	59.62	60.07	61.26	58.16	59.46	65.11	61.42	61.11
アカウント数 (万アカウント)	10,251	10,233	10,507	12,029	12,068	12,081	12,105	12,072	12,135	12,238	12,212	12,315
フィルター利用者数 (万アカウント)	7,519	7,536	7,821	9,363	9,428	9,464	9,519	9,503	9,561	9,681	9,652	9,771



2015 年度

	4月	5月	6月	7月	8月	9月	10月	11月	12月	1月	2月	3月
電子メール総数 (万通/日)	162,198	167,342	157,660	146,227	134,872	131,656	128,501	130,194	138,511	136,186	136,389	140,912
迷惑メール数 (万通/日)	94,058	98,211	88,060	75,063	67,946	61,802	58,155	61,059	66,200	65,858	66,608	68,658
迷惑メール割合 (%)	57.99	58.69	55.85	51.33	50.38	46.94	45.26	46.90	47.79	48.36	48.84	48.72
アカウント数 (万アカウント)	12,267	12,288	12,286	12,378	12,355	12,366	12,331	12,324	12,316	12,329	12,331	12,451
フィルター利用者数 (万アカウント)	9,723	9,754	9,740	9,839	9,827	9,845	9,827	9,831	9,835	9,875	9,871	10,002

2016 年度

	4月	5月	6月	7月	8月	9月	10月	11月	12月	1月	2月	3月
電子メール総数 (万通/日)	117,935	113,111	123,648	131,677	124,919	144,100	134,337	138,934	143,532	115,566	124,228	120,803
迷惑メール数 (万通/日)	50,336	47,336	49,184	56,295	54,688	64,036	62,037	60,627	64,189	47,520	49,456	47,674
迷惑メール割合 (%)	42.68	41.85	39.78	42.75	43.78	44.44	46.18	43.64	44.72	41.12	39.81	39.46
アカウント数 (万アカウント)	12,401	12,384	12,388	12,345	12,329	12,367	12,363	12,336	12,372	12,356	12,305	12,422
フィルター利用者数 (万アカウント)	9,957	9,950	9,973	9,981	9,976	10,003	10,015	9,995	10,038	10,029	9,984	10,089

2017 年度

	4月	5月	6月	7月	8月	9月	10月	11月	12月	1月	2月	3月
電子メール総数 (万通/日)	116,340	121,116	122,974	123,287	117,178	130,246	118,311	124,100	131,179	121,448	124,020	127,164
迷惑メール数 (万通/日)	48,637	47,188	46,213	52,067	53,311	57,210	51,432	50,977	49,362	49,008	45,920	46,747
迷惑メール割合 (%)	41.81	38.96	37.58	42.23	45.50	43.92	43.47	41.08	37.63	40.35	37.03	36.76
アカウント数 (万アカウント)	12,401	12,406	12,354	12,395	12,378	12,393	12,378	12,351	12,390	12,418	12,350	12,477
フィルター利用者数 (万アカウント)	10,084	10,118	10,120	10,168	10,163	10,186	10,195	10,168	10,215	10,241	10,184	10,299

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（2018 年 3 月時点）」

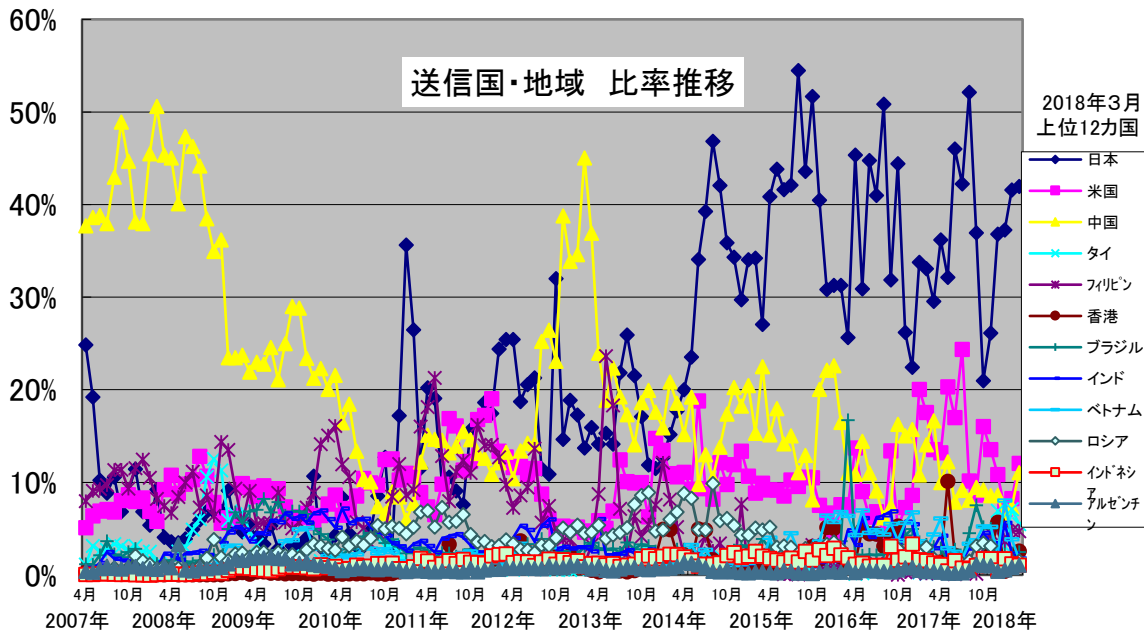


第2節 迷惑メール送信国・地域の推移

1 国内着の迷惑メール送信国・地域の推移

第2章第3節に記しました図表2-3-5を再掲し、その具体的な数値を以下に記します。

図表S-2-1 迷惑メール送信国・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）

2007年度

	4月	5月	6月	7月	8月	9月	10月	11月	12月	1月	2月	3月
日本	24.84%	19.23%	10.22%	8.86%	10.59%	6.83%	9.05%	11.44%	6.85%	5.40%	9.23%	4.07%
米国	5.12%	6.41%	6.90%	7.08%	6.80%	8.04%	8.67%	7.96%	8.33%	6.89%	5.82%	9.21%
中国	37.72%	38.60%	38.83%	37.95%	42.96%	48.90%	44.69%	38.12%	37.97%	45.48%	50.60%	45.36%
タイ	1.13%	3.16%	2.58%	2.74%	3.34%	3.10%	2.68%	3.14%	2.54%	2.52%	1.11%	1.00%
フィリピン	7.98%	9.09%	9.28%	9.71%	11.32%	11.38%	9.32%	11.54%	12.48%	10.51%	8.22%	7.47%
香港	0.31%	0.21%	0.22%	0.17%	0.16%	0.06%	0.20%	0.11%	0.03%	0.06%	0.03%	0.05%
ブラジル	1.18%	1.09%	2.15%	3.64%	2.25%	1.94%	2.47%	2.81%	1.60%	1.26%	1.21%	1.52%
インド	0.76%	0.62%	1.31%	2.50%	1.77%	1.57%	1.49%	1.10%	0.84%	0.66%	0.72%	2.31%
ベトナム	0.07%	0.06%	0.10%	0.09%	0.05%	0.08%	0.10%	0.13%	0.22%	0.18%	0.09%	0.16%
ロシア	0.26%	0.16%	0.35%	0.57%	0.75%	0.49%	0.78%	2.05%	1.50%	1.14%	0.74%	1.01%
インドネシア	0.07%	0.08%	0.13%	0.15%	0.09%	0.08%	0.12%	0.03%	0.04%	0.01%	0.05%	0.10%
アルゼンチン	0.41%	0.31%	0.69%	0.98%	0.73%	0.65%	0.88%	0.94%	0.63%	0.71%	0.62%	1.00%



2008 年度

	4月	5月	6月	7月	8月	9月	10月	11月	12月	1月	2月	3月
日本	3.59%	3.50%	3.90%	4.92%	5.93%	6.88%	6.86%	6.88%	9.14%	5.42%	4.65%	5.28%
米国	10.79%	8.80%	9.81%	10.29%	12.82%	10.68%	7.85%	5.61%	6.18%	6.05%	9.89%	9.46%
中国	45.03%	40.09%	47.37%	46.30%	44.17%	38.49%	34.94%	36.21%	23.47%	23.48%	23.74%	21.91%
タイ	1.19%	2.56%	2.95%	4.90%	6.05%	10.62%	12.55%	11.32%	5.91%	6.56%	6.87%	4.66%
フィリピン	6.69%	8.42%	9.97%	11.18%	7.28%	8.61%	6.41%	14.36%	13.50%	9.33%	5.57%	9.09%
香港	0.10%	0.04%	0.04%	0.04%	0.04%	0.04%	0.04%	0.05%	0.13%	0.18%	0.26%	0.10%
ブラジル	1.60%	1.67%	1.48%	1.21%	1.58%	2.14%	2.17%	1.99%	4.99%	6.77%	5.68%	6.88%
インド	2.11%	1.65%	2.36%	2.42%	2.62%	2.16%	3.90%	3.44%	4.60%	5.18%	4.89%	3.63%
ベトナム	0.78%	0.63%	0.47%	0.19%	0.60%	1.05%	1.06%	1.72%	3.15%	3.18%	1.75%	1.85%
ロシア	0.78%	0.73%	0.57%	0.54%	0.92%	1.83%	3.84%	1.91%	1.56%	2.26%	2.39%	1.91%
インドネシア	0.10%	0.11%	0.07%	0.11%	0.23%	0.17%	0.32%	0.25%	0.53%	0.77%	0.78%	0.71%
アルゼンチン	0.79%	3.29%	0.56%	0.44%	0.81%	0.69%	0.79%	0.83%	1.20%	1.72%	1.58%	1.78%

2009 年度

	4月	5月	6月	7月	8月	9月	10月	11月	12月	1月	2月	3月
日本	22.99%	22.77%	24.58%	21.09%	24.99%	29.02%	28.84%	23.41%	21.25%	22.29%	20.04%	21.57%
米国	8.48%	9.64%	9.09%	9.34%	7.37%	6.27%	6.26%	6.67%	5.63%	6.43%	7.66%	8.62%
中国	5.46%	5.63%	5.58%	8.87%	5.69%	5.04%	5.63%	7.29%	8.90%	14.12%	15.07%	16.11%
タイ	0.72%	0.66%	0.70%	0.49%	0.49%	0.62%	0.85%	0.80%	0.59%	0.78%	0.80%	0.50%
フィリピン	4.15%	4.81%	3.32%	5.07%	5.96%	5.49%	5.07%	3.75%	3.88%	4.25%	3.52%	2.98%
香港	4.10%	3.35%	5.34%	2.83%	1.90%	3.14%	3.19%	4.02%	10.66%	3.04%	2.31%	4.28%
ブラジル	4.51%	4.45%	5.89%	5.69%	6.66%	6.07%	6.36%	5.66%	6.67%	6.99%	6.05%	5.13%
インド	7.07%	8.24%	6.77%	7.87%	6.42%	6.87%	6.87%	6.59%	5.01%	4.41%	3.82%	2.69%
ベトナム	1.20%	1.06%	1.38%	1.52%	0.96%	1.08%	1.06%	1.14%	1.12%	1.20%	1.18%	1.31%
ロシア	2.04%	1.86%	2.25%	2.06%	2.06%	1.30%	1.06%	1.43%	1.13%	1.03%	1.23%	1.06%
インドネシア	1.03%	1.04%	1.26%	1.00%	1.10%	1.07%	0.88%	0.97%	0.70%	0.80%	1.22%	1.47%
アルゼンチン	1.02%	1.00%	1.48%	1.67%	1.90%	1.63%	1.37%	1.42%	1.17%	1.36%	2.22%	2.34%

第 1 章

第 2 章

第 3 章

第 4 章

参考編

資料編



2010 年度

	4月	5月	6月	7月	8月	9月	10月	11月	12月	1月	2月	3月
日本	8.38%	4.46%	3.09%	3.14%	4.82%	8.52%	12.71%	3.03%	17.21%	35.63%	26.49%	11.53%
米国	6.46%	7.18%	8.53%	10.43%	9.96%	9.72%	12.47%	12.56%	10.25%	10.99%	10.64%	8.93%
中国	16.45%	18.47%	13.37%	10.32%	10.04%	7.39%	6.65%	8.98%	8.43%	5.95%	7.76%	12.20%
タイ	0.44%	0.47%	0.62%	0.81%	1.03%	2.04%	3.08%	3.23%	2.45%	1.07%	0.89%	1.24%
フィリピン	11.97%	10.57%	5.71%	5.09%	3.34%	4.59%	4.77%	8.48%	11.98%	8.64%	9.19%	16.03%
香港	0.09%	0.15%	0.14%	0.14%	0.23%	0.14%	0.11%	0.16%	0.34%	0.78%	0.48%	0.82%
ブラジル	2.16%	2.75%	3.07%	4.19%	4.57%	4.45%	3.45%	3.86%	3.06%	2.36%	2.79%	2.96%
インド	7.18%	5.60%	6.03%	6.08%	5.18%	4.65%	4.27%	3.46%	3.11%	2.63%	3.34%	3.70%
ベトナム	2.09%	1.93%	2.24%	3.01%	2.85%	2.36%	2.81%	2.50%	1.49%	0.97%	1.04%	1.34%
ロシア	4.10%	3.16%	3.65%	3.24%	3.96%	5.35%	4.97%	5.25%	5.05%	4.47%	5.17%	6.81%
インドネシア	0.56%	0.69%	1.07%	0.88%	0.97%	1.25%	1.25%	1.26%	0.70%	0.70%	0.90%	1.80%
アルゼンチン	0.49%	0.60%	0.70%	0.82%	0.64%	0.60%	0.64%	0.71%	0.56%	0.37%	0.54%	0.46%

2011 年度

	4月	5月	6月	7月	8月	9月	10月	11月	12月	1月	2月	3月
日本	20.23%	19.09%	9.89%	10.58%	9.09%	7.60%	15.64%	16.63%	18.64%	17.47%	24.40%	25.44%
米国	7.36%	6.52%	9.81%	16.89%	16.10%	11.35%	12.29%	16.80%	17.26%	19.05%	13.38%	12.76%
中国	15.11%	14.65%	14.55%	13.19%	13.89%	15.48%	14.61%	13.12%	12.60%	10.89%	12.13%	13.28%
タイ	1.29%	1.10%	1.59%	1.76%	1.19%	1.36%	0.86%	1.17%	1.37%	0.86%	0.55%	0.93%
フィリピン	18.15%	21.29%	12.87%	7.98%	11.13%	12.36%	11.03%	16.21%	13.99%	14.07%	12.73%	9.74%
香港	0.68%	0.51%	1.15%	3.31%	1.25%	1.21%	1.31%	1.91%	1.79%	1.62%	1.87%	2.93%
ブラジル	2.62%	1.88%	2.37%	2.34%	2.01%	2.14%	2.79%	2.33%	2.49%	2.82%	2.65%	3.51%
インド	3.13%	2.47%	3.93%	4.22%	4.42%	4.04%	3.19%	2.44%	2.50%	2.81%	2.53%	2.95%
ベトナム	1.55%	0.84%	1.32%	1.44%	1.49%	2.37%	2.56%	2.10%	1.91%	1.84%	1.37%	1.28%
ロシア	6.96%	5.17%	7.31%	5.69%	5.80%	6.53%	4.39%	3.55%	3.62%	3.07%	3.18%	3.80%
インドネシア	1.51%	0.82%	1.19%	1.53%	1.22%	1.70%	1.39%	1.35%	1.26%	2.08%	2.19%	2.29%
アルゼンチン	0.39%	0.35%	0.46%	0.45%	0.39%	0.35%	0.71%	0.35%	0.53%	0.61%	0.61%	0.78%



2012 年度

	4月	5月	6月	7月	8月	9月	10月	11月	12月	1月	2月	3月
日本	25.44%	18.74%	20.56%	21.29%	11.47%	10.89%	32.03%	14.65%	18.87%	17.27%	13.72%	15.94%
米国	11.61%	11.77%	10.84%	11.51%	8.73%	6.05%	4.20%	5.27%	5.07%	5.17%	4.61%	4.76%
中国	10.41%	13.42%	14.24%	14.17%	25.24%	26.43%	23.10%	38.80%	33.88%	34.60%	45.03%	36.91%
タイ	0.58%	0.73%	0.85%	0.62%	1.06%	0.77%	0.59%	0.59%	0.56%	0.64%	0.91%	1.04%
フィリピン	7.25%	8.59%	9.45%	13.66%	5.67%	7.45%	4.60%	3.85%	3.87%	2.36%	1.09%	3.25%
香港	3.11%	3.70%	2.50%	2.37%	1.02%	2.22%	2.00%	1.43%	2.12%	1.46%	0.86%	0.53%
ブラジル	2.83%	2.82%	3.36%	2.52%	3.89%	2.49%	1.86%	2.61%	2.10%	2.20%	3.05%	3.48%
インド	4.01%	5.31%	4.88%	3.63%	5.31%	6.01%	2.82%	3.04%	2.86%	3.00%	3.01%	2.56%
ベトナム	2.53%	3.38%	2.89%	1.33%	1.94%	2.99%	1.65%	1.60%	1.40%	1.62%	1.41%	1.35%
ロシア	3.40%	2.77%	2.68%	2.42%	3.25%	3.18%	3.99%	5.08%	4.64%	5.38%	4.51%	4.64%
インドネシア	1.35%	1.44%	1.43%	1.03%	1.43%	1.72%	1.16%	1.66%	1.36%	1.55%	0.91%	1.25%
アルゼンチン	0.73%	0.74%	0.90%	0.73%	0.67%	1.01%	0.78%	0.79%	1.05%	1.00%	0.97%	0.64%

2013 年度

	4月	5月	6月	7月	8月	9月	10月	11月	12月	1月	2月	3月
日本	14.13%	15.32%	14.14%	21.84%	25.94%	21.54%	17.12%	11.89%	11.51%	12.69%	15.17%	17.73%
米国	5.88%	5.04%	6.90%	12.43%	10.10%	9.95%	9.97%	6.30%	14.75%	13.49%	10.95%	10.60%
中国	23.94%	18.87%	22.35%	19.25%	17.33%	14.08%	18.64%	19.94%	17.59%	15.90%	20.86%	18.57%
タイ	1.14%	1.09%	0.98%	0.98%	1.24%	1.26%	2.53%	2.30%	1.89%	1.23%	1.61%	2.15%
フィリピン	8.73%	23.64%	18.31%	7.14%	2.27%	6.34%	4.15%	5.45%	7.58%	12.15%	8.16%	5.18%
香港	0.33%	0.61%	0.89%	0.43%	0.34%	0.47%	0.78%	1.73%	1.85%	4.95%	4.92%	2.25%
ブラジル	2.91%	2.70%	2.85%	2.41%	3.51%	2.81%	3.31%	3.13%	2.55%	1.93%	2.10%	2.76%
インド	6.06%	2.12%	2.23%	2.30%	2.69%	2.33%	2.00%	2.75%	1.80%	2.05%	2.20%	2.52%
ベトナム	1.84%	1.67%	1.02%	1.01%	1.67%	1.28%	1.18%	2.00%	0.97%	0.97%	1.13%	1.03%
ロシア	5.38%	3.95%	4.31%	4.60%	5.10%	7.62%	8.59%	8.90%	4.73%	4.88%	6.00%	6.79%
インドネシア	1.26%	1.08%	1.24%	0.92%	1.06%	1.17%	1.75%	2.07%	1.74%	2.03%	2.25%	2.22%
アルゼンチン	0.91%	0.52%	0.44%	0.66%	0.83%	0.84%	0.66%	0.58%	0.73%	0.70%	0.75%	0.91%

第 1 章

第 2 章

第 3 章

第 4 章

参 考 編

資 料 編



2014 年度

	4月	5月	6月	7月	8月	9月	10月	11月	12月	1月	2月	3月
日本	20.03%	23.54%	34.07%	39.29%	46.84%	42.08%	35.89%	34.32%	29.71%	34.04%	34.21%	27.07%
米国	11.10%	9.25%	18.80%	9.32%	8.20%	12.13%	9.77%	11.92%	13.36%	10.69%	8.83%	9.91%
中国	15.16%	19.21%	9.77%	12.99%	10.43%	13.82%	17.39%	20.25%	18.24%	20.46%	15.32%	22.50%
タイ	1.53%	1.44%	1.28%	1.10%	1.43%	2.08%	1.81%	2.51%	1.31%	1.19%	1.10%	1.35%
フィリピン	2.19%	1.28%	2.28%	4.20%	2.63%	3.42%	1.47%	0.34%	7.68%	0.23%	0.72%	1.66%
香港	2.22%	1.50%	4.98%	4.88%	1.63%	1.08%	1.09%	0.68%	0.86%	1.01%	1.65%	1.20%
ブラジル	2.75%	2.34%	1.58%	1.69%	1.29%	1.62%	2.36%	2.66%	3.21%	2.99%	2.67%	3.90%
インド	2.30%	1.77%	1.00%	1.11%	0.96%	1.26%	1.31%	1.67%	1.15%	1.28%	1.67%	2.41%
ベトナム	1.64%	3.26%	2.03%	2.73%	1.56%	1.09%	1.55%	1.08%	1.15%	1.32%	2.65%	1.44%
ロシア	8.80%	8.30%	4.91%	4.88%	9.90%	5.88%	6.13%	5.37%	4.31%	4.30%	5.09%	4.87%
インドネシア	1.97%	1.63%	0.96%	1.17%	1.16%	1.31%	2.11%	2.41%	1.90%	2.04%	2.54%	2.04%
アルゼンチン	1.33%	1.27%	1.09%	0.80%	0.41%	0.34%	0.61%	0.36%	0.28%	0.22%	0.35%	0.35%

2015 年度

	4月	5月	6月	7月	8月	9月	10月	11月	12月	1月	2月	3月
日本	40.87%	43.83%	41.63%	42.09%	54.50%	43.60%	51.67%	40.46%	30.85%	31.29%	31.29%	25.64%
米国	9.19%	9.19%	8.54%	10.27%	9.58%	10.59%	10.49%	7.52%	6.71%	3.89%	7.61%	7.37%
中国	15.12%	17.96%	14.17%	15.03%	11.06%	12.92%	8.12%	20.03%	22.13%	22.62%	16.48%	11.02%
タイ	1.08%	1.14%	1.19%	1.17%	0.63%	0.86%	0.52%	1.36%	1.01%	0.99%	1.06%	0.32%
フィリピン	1.73%	0.55%	0.10%	0.14%	0.06%	1.42%	3.23%	0.65%	0.79%	0.86%	1.10%	0.85%
香港	0.81%	1.08%	2.17%	1.62%	1.97%	2.00%	3.07%	1.73%	5.14%	5.03%	1.97%	1.10%
ブラジル	2.83%	2.28%	2.25%	2.21%	1.58%	2.61%	1.97%	2.27%	3.31%	2.75%	3.66%	16.72%
インド	1.49%	1.49%	1.41%	1.32%	1.08%	1.32%	0.97%	1.43%	1.59%	1.56%	1.90%	4.85%
ベトナム	4.05%	1.79%	3.25%	4.52%	2.64%	2.76%	2.66%	3.63%	6.41%	5.75%	6.82%	6.40%
ロシア	5.19%	3.00%	3.15%	2.99%	2.34%	2.85%	2.78%	2.64%	3.32%	3.54%	2.83%	1.83%
インドネシア	1.79%	1.63%	1.42%	1.84%	1.42%	2.57%	1.63%	2.72%	2.11%	2.89%	2.17%	1.85%
アルゼンチン	0.28%	0.23%	0.51%	0.40%	0.21%	0.26%	0.18%	0.32%	0.44%	0.34%	0.32%	0.78%



2016年度

	4月	5月	6月	7月	8月	9月	10月	11月	12月	1月	2月	3月
日本	45.39%	30.90%	44.78%	40.99%	50.84%	31.89%	44.43%	26.22%	22.43%	33.79%	33.07%	29.59%
米国	13.71%	9.01%	6.24%	6.84%	4.39%	13.42%	5.04%	7.29%	8.59%	20.05%	17.56%	13.54%
中国	10.87%	14.44%	11.02%	9.10%	6.19%	7.38%	16.26%	15.04%	15.74%	10.80%	14.07%	16.66%
タイ	0.13%	0.21%	0.45%	0.43%	0.44%	0.53%	0.53%	0.71%	0.62%	0.29%	0.12%	0.36%
フィリピン	1.01%	1.41%	1.03%	1.25%	0.33%	0.52%	0.03%	0.32%	0.40%	0.39%	0.16%	0.64%
香港	1.42%	4.86%	4.45%	4.44%	3.11%	4.33%	5.29%	1.35%	0.88%	0.94%	0.57%	0.60%
ブラジル	2.22%	2.11%	2.21%	2.15%	2.24%	2.43%	3.30%	4.29%	4.96%	3.54%	3.27%	3.02%
インド	3.23%	6.16%	4.11%	6.18%	6.46%	6.86%	1.52%	5.77%	5.50%	2.00%	1.61%	2.89%
ベトナム	4.32%	6.98%	4.56%	4.87%	4.39%	5.53%	3.72%	5.63%	6.76%	3.68%	2.82%	4.38%
ロシア	1.57%	1.20%	1.16%	0.67%	0.94%	1.05%	2.84%	2.29%	2.04%	2.26%	2.99%	1.74%
インドネシア	1.16%	1.27%	0.98%	1.04%	1.03%	3.09%	1.57%	1.97%	3.36%	1.67%	1.56%	1.32%
アルゼンチン	0.28%	0.52%	0.49%	0.46%	0.37%	0.33%	0.53%	0.80%	0.84%	0.50%	0.37%	0.43%

2017年度

	4月	5月	6月	7月	8月	9月	10月	11月	12月	1月	2月	3月
日本	36.18%	32.13%	46.00%	42.24%	52.12%	36.94%	20.97%	26.15%	36.80%	37.26%	41.60%	41.99%
米国	13.20%	20.33%	16.99%	24.36%	10.17%	8.65%	16.05%	13.55%	10.84%	7.07%	8.27%	12.06%
中国	10.00%	12.22%	7.87%	9.17%	8.08%	9.47%	9.19%	8.58%	8.59%	5.82%	7.31%	11.05%
タイ	0.39%	0.40%	0.44%	0.86%	0.62%	1.15%	1.94%	3.25%	6.94%	3.06%	7.11%	5.49%
フィリピン	0.41%	0.27%	0.12%	0.25%	0.64%	0.12%	2.73%	4.52%	5.06%	3.63%	4.80%	4.73%
香港	1.40%	10.14%	2.15%	0.55%	1.14%	1.11%	0.98%	2.35%	5.70%	0.41%	0.85%	2.59%
ブラジル	2.90%	1.55%	2.78%	1.80%	4.54%	7.52%	5.17%	5.01%	2.43%	2.24%	2.33%	2.48%
インド	4.26%	1.90%	1.96%	1.47%	2.86%	3.12%	4.57%	3.47%	1.40%	5.61%	2.33%	1.78%
ベトナム	6.12%	2.88%	2.49%	1.77%	3.39%	3.76%	5.25%	5.23%	2.23%	8.06%	3.85%	1.72%
ロシア	1.22%	1.06%	0.78%	1.23%	1.50%	3.13%	3.44%	3.14%	1.83%	0.92%	1.53%	1.52%
インドネシア	1.12%	0.43%	1.56%	0.74%	0.65%	1.03%	1.75%	1.76%	0.54%	1.76%	1.19%	1.07%
アルゼンチン	0.32%	0.21%	0.21%	0.25%	0.49%	1.17%	1.04%	0.99%	0.42%	0.56%	0.82%	1.06%

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S-2-2 迷惑メール送信上位12か国の推移（各年3月時点）

迷惑メール送信国・地域の推移（各年3月時点での送信国・地域上位12か国の推移）

順位	2008年 3月	2009年 3月	2010年 3月	2011年 3月	2012年 3月	2013年 3月	2014年 3月	2015年 3月	2016年 3月	2017年 3月	2018年 3月
1	中国	中国	中国	フィリピン	日本	中国	中国	日本	日本	日本	日本
	45.36%	21.91%	21.57%	16.03%	25.44%	36.91%	18.57%	27.07%	25.64%	29.55%	41.95%
2	米国	米国	フィリピン	中国	中国	日本	日本	中国	ブラジル	中国	米国
	9.21%	9.46%	16.11%	12.20%	13.28%	15.94%	17.73%	22.50%	16.72%	16.66%	12.06%
3	フィリピン	フィリピン	米国	日本	米国	米国	米国	米国	中国	米国	中国
	7.47%	9.09%	8.62%	11.53%	12.76%	4.76%	10.60%	9.91%	11.02%	13.54%	11.05%
4	台湾	ブラジル	インド	米国	フィリピン	ロシア	ロシア	ロシア	米国	ベトナム	ロシア
	6.82%	6.88%	5.13%	8.93%	9.74%	4.64%	6.79%	4.87%	7.37%	4.38%	5.49%
5	韓国	日本	日本	ロシア	ロシア	ブラジル	フィリピン	ブラジル	ベトナム	ブラジル	フィリピン
	4.10%	5.28%	4.28%	6.81%	3.80%	3.48%	5.18%	3.90%	6.40%	3.02%	4.73%
6	日本	韓国	韓国	韓国	ブラジル	フィリピン	カナダ	インド	インド	インド	香港
	4.07%	5.20%	2.98%	5.18%	3.51%	3.25%	3.55%	2.41%	4.85%	2.89%	2.59%
7	インド	ロシア	ブラジル	インド	韓国	カナダ	ブラジル	ベトナム	韓国	シンガポール	ブラジル
	2.31%	4.66%	2.69%	3.70%	3.06%	3.08%	2.76%	2.04%	2.01%	2.80%	2.48%
8	ブラジル	インド	ロシア	台湾	インド	カナダ	インド	韓国	ベトナム	オーストラリア	インド
	1.52%	3.63%	2.69%	3.04%	2.95%	2.81%	2.52%	2.03%	1.85%	2.46%	1.78%
9	イタリア	インド	ベトナム	ブラジル	香港	インド	香港	フィリピン	ロシア	ロシア	ベトナム
	1.34%	2.12%	2.64%	2.96%	2.93%	2.56%	2.25%	1.66%	1.83%	1.74%	1.72%
10	スペイン	ロシア	英国	カナダ	ロシア	ブラジル	ベトナム	カナダ	イタリア	韓国	ロシア
	1.33%	2.03%	2.34%	2.69%	2.36%	1.88%	2.22%	1.57%	1.40%	1.49%	1.52%
11	フランス	ロシア	ロシア	ベトナム	ベトナム	韓国	ロシア	ベトナム	香港	ベトナム	ベトナム
	1.32%	1.91%	1.71%	1.80%	2.29%	1.72%	2.15%	1.44%	1.10%	1.32%	1.07%
12	英国	ベトナム	ロシア	ベトナム	台湾	ベトナム	韓国	ロシア	イタリア	英国	アルゼンチン
	1.32%	1.85%	1.55%	1.34%	1.57%	1.35%	1.94%	1.35%	0.99%	1.23%	1.06%

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）



2 世界全体の迷惑メール送信国・地域の推移

迷惑メール送信国・地域の順位は毎年変動します。近年は米国、中国、ベトナム、インドなどの国々が上位を占めています。

図表S-2-3 各年の迷惑メール送信国・地域上位20か国・地域の推移

順位	2013年	2014年	2015年	2016年	2017年
1	中国 23%	米国 16.7%	米国 15.2%	米国 12.1%	米国 13.2%
2	米国 17.6%	ロシア 5.9%	ロシア 6.2%	ベトナム 10.3%	中国 11.3
3	韓国 12.7%	中国 5.5%	ベトナム 6.1%	インド 10.2%	ベトナム 9.9%
4	台湾 5.6%	ベトナム 4.9%	中国 6.1%	中国 4.7%	インド 7.0%
5	ロシア 4.0%	ドイツ 4.0%	ドイツ 4.2%	メキシコ 4.4%	ドイツ 5.7%
6	ベトナム 3.7%	アルゼンチン 3.6%	ウクライナ 4.0%	ブラジル 4.0%	ロシア 5.4%
7	インド 3.5%	スペイン 3.2%	フランス 3.2%	ロシア 3.5%	ブラジル 4.0%
8	ウクライナ 3.0%	ウクライナ 3.0%	インド 3.0%	フランス 3.4%	フランス 3.7%
9	カザフスタン 2.1%	インド 3.0%	アルゼンチン 2.9%	ドイツ 3.2%	イラン 2.0%
10	日本 1.9%	フランス 2.6%	ブラジル 2.9%	トルコ 2.3%	イタリア 1.9%
11	イタリア 1.8%	ブラジル 2.4%	スペイン 2.4%	イラン 2.1%	メキシコ 1.8%
12	ベラルーシ 1.6%	イタリア 2.3%	イタリア 2.2%	アルゼンチン 1.9%	トルコ 1.8%
13	ルーマニア 1.3%	韓国 2.2%	英国 2.2%	インドネシア 1.8%	アルゼンチン 1.6%
14	カナダ 1.3%	台湾 2.0%	トルコ 2.0%	コロンビア 1.5%	英国 1.6%
15	ドイツ 1.2%	英国 1.7%	メキシコ 1.9%	スペイン 1.5%	オランダ 1.5%
16	ブラジル 1.1%	メキシコ 1.7%	韓国 1.8%	パキスタン 1.3%	スペイン 1.5%
17	ポーランド 1.0%	イラン 1.7%	日本 1.8%	イタリア 1.2%	インドネシア 1.4%
18	ブルガリア 0.9%	日本 1.5%	シンガポール 1.6%	ポーランド 1.1%	コロンビア 1.2%
19	英国 0.7%	コロンビア 1.4%	オランダ 1.5%	英国 1.1%	パキスタン 1.1%
20	スペイン 0.6%	トルコ 1.4%	ルーマニア 1.5%	シンガポール 1.1%	ウクライナ 1.1%

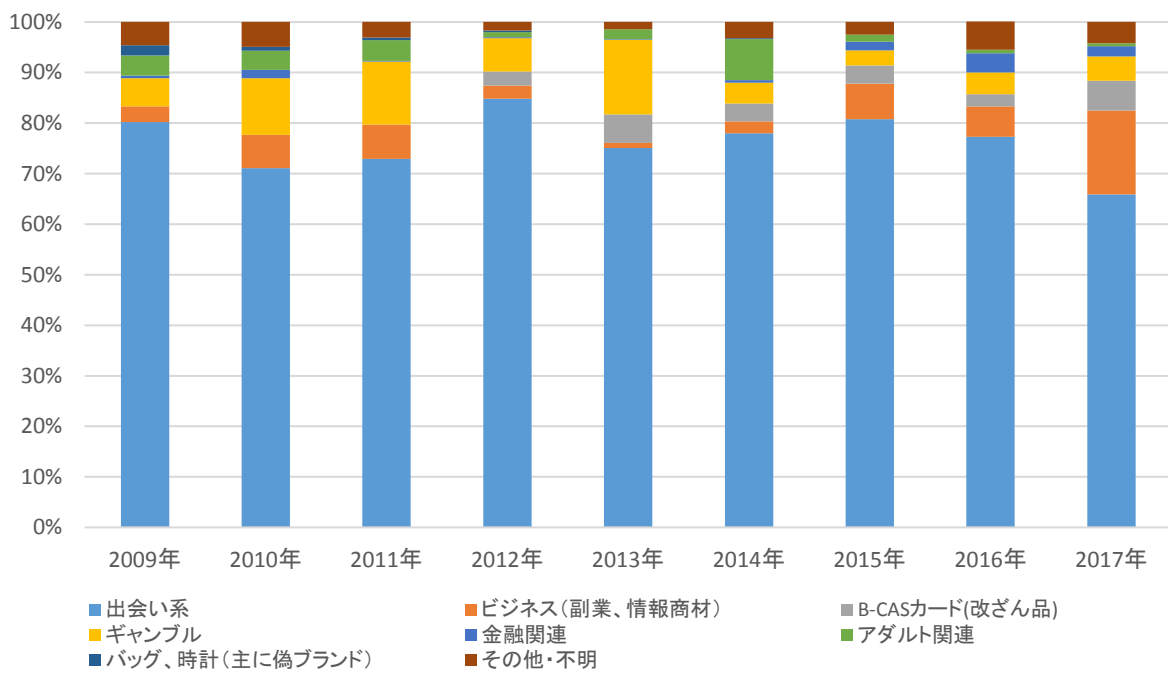
出典：カスペルスキー（株）のスパム発信国リスト Sources of spam by country を元に迷惑メール対策推進協議会が作成



第3節 迷惑メールの内容の傾向

「第2章 第3節4 迷惑メールの内容」において「出会い系」サイトの広告宣伝が調査開始以来、初めて7割を下回った一方、情報商材をはじめとする「ビジネス」が大幅に増加した旨の説明をしました。以下に2009年以降の内容別比率を記します。

図表S-3-1 迷惑メールの内容の傾向



迷惑メールの内容	2009年	2010年	2011年	2012年	2013年	2014年	2015年	2016年	2017年
出会い系	80.2%	71.1%	72.9%	84.8%	75.1%	78.0%	80.8%	77.3%	65.9%
ビジネス (副業、情報商材)	3.1%	6.6%	6.8%	2.6%	1.0%	2.3%	7.0%	6.0%	16.6%
B-CASカード(改ざん品)	0.0%	0.0%	0.0%	2.8%	5.6%	3.6%	3.6%	2.4%	5.9%
ギャンブル	5.6%	11.2%	12.5%	6.6%	14.8%	4.1%	3.0%	4.3%	4.8%
金融関連	0.5%	1.6%	0.1%	0.2%	0.1%	0.5%	1.7%	3.8%	2.0%
アダルト関連	4.0%	3.8%	4.1%	1.0%	2.0%	8.1%	1.4%	0.7%	0.6%
バッグ、時計(主に偽ブランド)	2.0%	0.8%	0.5%	0.3%	0.0%	0.2%	0.0%	0.0%	0.0%
その他・不明	4.6%	4.9%	3.1%	1.7%	1.4%	3.2%	2.5%	5.6%	4.2%

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及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



第4節 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（オプトイン規制導入前）

図表S-4-1 2008年改正までの総務大臣による措置命令

処分年月	対象者名	法違反の内容
2002年12月	東京都中野区の事業者（名称非公表）	表示義務違反 再送信禁止義務違反
2003年11月	東京都中野区の事業者（名称非公表）	表示義務違反
2004年4月	(株)エス・アイ・エス・ワールド	表示義務違反
2005年9月	(有)コスモメディアサービス	表示義務違反
2008年2月	(株)ビューティースタイル	表示義務違反
2008年6月	(株)Botolo	表示義務違反

図表S-4-2 2008年改正までの警察による摘発

摘発年月	概要
2006年5月	千葉県警が東京都内の男性を逮捕
2006年8月	大阪府警が大阪市内の元会社社長などを書類送検
2007年1月	千葉県警が東京都内の会社社長などを逮捕

2 2008年改正後の執行状況（オプトイン規制導入後）

図表S-4-1 2008年改正後の総務大臣及び消費者庁長官による行政処分（措置命令）（オプトイン規制導入後）

処分年月	対象者名	法違反の内容
2009年4月	個人事業者	受信者の同意を得ずに送信
2009年6月	(株)HolyAce	受信者の同意を得ずに送信 表示義務違反
2009年10月	(株)EIGHT	受信者の同意を得ずに送信 表示義務違反
2009年10月	(株)アルファクト	受信者の同意を得ずに送信
2009年12月	(株)エレクトリックオペレーション	受信者の同意を得ずに送信 記録保存義務違反 表示義務違反
2010年3月	個人事業者	受信者の同意を得ずに送信 記録保存義務違反 表示義務違反
2010年4月	(株)スパイラルネット	受信者の同意を得ずに送信
2010年4月	(株)広告研究所	受信者の同意を得ずに送信
2010年8月	(株)アンビション	受信者の同意を得ずに送信 表示義務違反
2010年12月	(株)ITS	受信者の同意を得ずに送信
2011年1月	(株)エース	受信者の同意を得ずに送信 表示義務違反



処分年月	対象者名	法違反の内容
2011年3月	(株)フレンディア	受信者の同意を得ずに送信
2011年3月	(株)エルベール	受信者の同意を得ずに送信
2011年4月	(株)シックスエストレラ	受信者の同意を得ずに送信
2011年5月	(株)ノプロ	受信者の同意を得ずに送信 表示義務違反
2011年6月	個人事業者	受信者の同意を得ずに送信 表示義務違反
2011年6月	(株)FINE	受信者の同意を得ずに送信 表示義務違反
2011年6月	(株)Breeze	受信者の同意を得ずに送信 表示義務違反
2011年6月	(株)next media	受信者の同意を得ずに送信 表示義務違反
2011年7月	(株)Cyber Factory	受信者の同意を得ずに送信 表示義務違反
2011年10月	(有)ライズ	受信者の同意を得ずに送信
2011年12月	(合)ウィンラック	受信者の同意を得ずに送信 表示義務違反
2012年3月	(株)ソル	受信者の同意を得ずに送信 表示義務違反
2012年5月	(株)ライズ(旧社名(株)SEO)	受信者の同意を得ずに送信
2012年6月	(有)カリスト	受信者の同意を得ずに送信
2012年7月	(株)アイエイコミュニケーションズ	受信者の同意を得ずに送信 表示義務違反
2012年8月	(株)ポアソルチ	受信者の同意を得ずに送信 表示義務違反
2013年2月	(株)シグナル	受信者の同意を得ずに送信 表示義務違反
2013年2月	(株)vivid	受信者の同意を得ずに送信 記録保存義務違反、表示義務違反
2013年3月	(有)ナビール	受信者の同意を得ずに送信 表示義務違反
2013年3月	(株)福田	受信者の同意を得ずに送信
2013年5月	(株)Capsule	受信者の同意を得ずに送信
2013年9月	(株)アップスタート	受信者の同意を得ずに送信
2013年9月	(株)アレグレ	受信者の同意を得ずに送信 表示義務違反
2013年11月	(株)GNT	受信者の同意を得ずに送信 表示義務違反
2013年12月	(株)INFLUENCE	受信者の同意を得ずに送信 表示義務違反
2013年12月	(株)Neptune	受信者の同意を得ずに送信 表示義務違反
2014年2月	(株)SANS	受信者の同意を得ずに送信 記録保存義務違反 表示義務違反
2014年5月	(株)ミネルバ	受信者の同意を得ずに送信 記録保存義務違反
2014年6月	(株)Peace	受信者の同意を得ずに送信 記録保存義務違反



処分年月	対象者名	法違反の内容
2014年11月	(株)インペリアル	受信者の同意を得ずに送信 記録保存義務違反 表示義務違反
2014年12月	(株)440	受信者の同意を得ずに送信
2015年2月	(合)ネクスト	受信者の同意を得ずに送信 記録保存義務違反 表示義務違反
2015年2月	(株)メテオ	受信者の同意を得ずに送信 表示義務違反
2015年2月	(株)アイコミュニケーション	受信者の同意を得ずに送信 記録保存義務違反 表示義務違反
2015年5月	(株)ヒカリメディア	受信者の同意を得ずに送信
2015年5月	(株)Ties	受信者の同意を得ずに送信 記録保存義務違反 表示義務違反
2015年6月	(株)トライデント	受信者の同意を得ずに送信 記録保存義務違反 表示義務違反
2015年9月	(株)フィーズ	受信者の同意を得ずに送信 表示義務違反
2015年9月	(株)エムパワー	受信者の同意を得ずに送信 表示義務違反
2015年9月	(合)エース	受信者の同意を得ずに送信 記録保存義務違反 表示義務違反
2015年10月	(株)スタイラス	受信者の同意を得ずに送信 表示義務違反
2017年11月	(株)ライトニング	受信者の同意を得ずに送信 記録保存義務違反 表示義務違反
2018年3月	(株)MOTHER	受信者の同意を得ずに送信 記録保存義務違反 表示義務違反

※2009年8月以前は総務大臣による措置命令

図表S-4-2 2008年改正後の警察による摘発（特定電子メール法第5条（送信者情報偽装）違反関連）

摘発年月	概要
2011年1月	京都府警・山梨県警が東京都内の男女計7名を逮捕
2013年7月	千葉県警が東京都内などの6名を逮捕

図表S-4-3 2008年改正後の警察による摘発（特定電子メール法第7条（措置命令）違反関連）

摘発年月	概要
2014年9月	警視庁が東京都内の男1人を逮捕
2014年10月	警視庁・北海道警が千葉県内などの男3人を書類送検

図表S-4-4 2008年改正後の警察による摘発（特定電子メール法第28条（報告徴収）違反関連）

摘発年月	概要
2015年4月	警視庁が東京都内の法人（1社）及び男1人を書類送検



第5節 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(オプトイン規制導入前)

図表S-5-1 2008年改正までの特定商取引法に基づく行政処分(オプトイン規制導入前)

処分年月	対象者名	処分内容	法違反の内容
2003年10月	(有)アクセス・コントロール	指示	法律に義務づけられている表示事項の欠落や不適切な表示を行っていた
2003年10月	(株)リメイン	指示	法律に義務づけられている表示事項の欠落や不適切な表示を行っていた
2005年6月	(有)アジアン・オアシス	業務停止命令 3ヶ月	表示義務違反
2005年6月	(有)エス・ケー・アイ	業務停止命令 3ヶ月及び指示	表示義務違反及び顧客の意に反する申し込み (ワンクリック)
2006年3月	個人事業者	業務停止命令 1ヶ月	広告表示義務違反及び虚偽広告
2007年3月	(有)アイニティプランニング	業務停止命令 6ヶ月	表示義務違反、誇大広告及び顧客の意に反する 申し込み
2007年3月	(株)フィットウェブ	業務停止命令 3ヶ月	表示義務違反、誇大広告及び顧客の意に反する 申し込み
2008年5月	(有)メディアテクノロジー	指示	誇大広告

2 2008年改正後の執行状況(オプトイン規制導入後)

図表S-5-2 2008年改正後の特定商取引法に基づく行政処分(オプトイン規制導入後)

処分年月	対象者名	処分内容	法違反の内容
2009年2月	(株)クロノス	指示	受信者の請求承諾を得ずに電子メール広告を送信
2009年3月	(合)HAiGHA(メイヤ)	指示	受信者の請求承諾を得ずに電子メール広告を送信
2009年5月	(有)リーテックシステムズ	指示	受信者の請求承諾を得ずに電子メール広告を送信
2009年8月	ニュートラルインターネットリサーチ(株)	指示	受信者の請求承諾を得ずに電子メール広告を送信
2010年8月	(合)S・T企画	指示	受信者の請求承諾を得ずに電子メール広告を送信
2010年8月	(合)パルク	指示	受信者の請求承諾を得ずに電子メール広告を送信
2010年10月	(株)BEAR	指示	受信者の請求承諾を得ずに電子メール広告を送信
2011年8月	(株)ジョイントツ	指示	受信者の請求承諾を得ずに電子メール広告を送信
2011年9月	(株)アクオリティ	指示	受信者の請求承諾を得ずに電子メール広告を送信



第6節 送信ドメイン認証技術の導入状況

総務省の業務委託先である（一財）日本データ通信協会が（株）日本レジストリサービス（以下「JPRS」といいます。）と共同研究契約を締結し、2018年1月から、JPドメイン名における送信ドメイン認証技術の設定状況の調査を開始しましたので、その調査結果（JPドメインにおける全体の普及状況およびドメイン種別毎）を以下に記します。

JPドメイン全体

図表S-6-1 送信ドメイン認証技術の導入状況（全体）

年	月	[a] 全ドメイン名数 ※括弧内はMXレコードを有するドメイン名数	[b] 全ドメイン名の中でのSPF設定数はMXレコードを有するドメイン名の中でのSPF設定数	[c] 全ドメイン名の中でのDMARC設定数 ※括弧内はMXレコードを有するドメイン名の中でのDMARC設定数	DMARCポリシーの設定状況 ※括弧内はMXレコードを有するドメイン名の中でのDMARC設定しているドメイン数				DMARCレポートの宛先の設定状況 ※括弧内はMXレコードを有するドメイン名の中でのDMARC設定しているドメイン数			
					[d] p=reject としているドメイン名数	[e] p=quarantine としているドメイン名数	[f] p=none としているドメイン名数	[g] DMARCポリシーとして、reject、quarantine及びnone以外のものを記述（誤記）しているドメイン名数	[h] uaタグ及びrufタグを共に設定していないドメイン名数	[i] uaタグのみを設定しているドメイン名数	[j] rufタグのみを設定しているドメイン名数	[k] uaタグ及びrufタグを共に設定しているドメイン名数
2018	1	1,471,348 (1,203,711)	699,672 (684,561)	7,835 (6,919)	1,298 (590)	246 (229)	6,279 (6,088)	12 (12)	2,629 (2,561)	1,213 (820)	24 (24)	3,969 (3,514)
	2	1,476,865 (1,205,702)	705,520 (690,288)	7,999 (7,061)	1,338 (618)	255 (237)	6,394 (6,194)	12 (12)	2,731 (2,662)	1,237 (842)	25 (25)	4,006 (3,522)
	3	1,481,735 (1,209,274)	708,764 (693,720)	8,173 (6,988)	1,361 (628)	261 (244)	6,538 (6,103)	13 (13)	2,820 (2,749)	1,276 (881)	25 (25)	4,052 (3,333)

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

JPドメイン種別毎

図表S-6-2 送信ドメイン認証技術の導入状況（種別毎）

ad.jp

年	月	[a]	[b]	[c]	[d]	[e]	[f]	[g]	[h]	[i]	[j]	[k]
2018	1	252 (212)	142 (140)	6 (6)	0 (0)	0 (0)	6 (6)	0 (0)	2 (2)	2 (2)	0 (0)	2 (2)
	2	252 (211)	143 (141)	6 (6)	0 (0)	0 (0)	6 (6)	0 (0)	2 (2)	2 (2)	0 (0)	2 (2)
	3	252 (211)	142 (140)	6 (6)	0 (0)	0 (0)	6 (6)	0 (0)	2 (2)	2 (2)	0 (0)	2 (2)



ac.jp

年	月	[a]	[b]	[c]	[d]	[e]	[f]	[g]	[h]	[i]	[j]	[k]
2018	1	3,596 (3,367)	2,111 (2,086)	11 (10)	1 (0)	1 (1)	9 (9)	0 (0)	5 (4)	5 (5)	0 (0)	1 (1)
	2	3,602 (3,371)	2,124 (2,100)	12 (11)	1 (0)	1 (1)	10 (10)	0 (0)	6 (5)	5 (5)	0 (0)	1 (1)
	3	3,614 (3,383)	2,143 (2,120)	14 (13)	1 (0)	1 (1)	12 (12)	0 (0)	6 (6)	7 (7)	0 (0)	1 (1)

co.jp

年	月	[a]	[b]	[c]	[d]	[e]	[f]	[g]	[h]	[i]	[j]	[k]
2018	1	403,955 (380,239)	254,292 (252,961)	1,121 (1,089)	71 (48)	50 (49)	993 (985)	7 (7)	715 (711)	229 (220)	6 (6)	171 (152)
	2	405,300 (381,261)	255,581 (254,253)	1,175 (1,140)	77 (53)	55 (54)	1,036 (1,026)	7 (7)	746 (742)	238 (228)	7 (7)	184 (163)
	3	406,453 (382,449)	256,930 (255,613)	1,210 (1,172)	78 (52)	61 (60)	1,064 (1,053)	7 (7)	757 (753)	248 (237)	7 (7)	198 (175)

go.jp

年	月	[a]	[b]	[c]	[d]	[e]	[f]	[g]	[h]	[i]	[j]	[k]
2018	1	582 (428)	492 (395)	1 (1)	0 (0)	0 (0)	1 (1)	0 (0)	0 (0)	1 (1)	0 (0)	0 (0)
	2	579 (427)	495 (395)	1 (1)	0 (0)	0 (0)	1 (1)	0 (0)	0 (0)	1 (1)	0 (0)	0 (0)
	3	581 (423)	491 (391)	3 (3)	0 (0)	0 (0)	3 (3)	0 (0)	0 (0)	2 (2)	0 (0)	1 (0)

or.jp

年	月	[a]	[b]	[c]	[d]	[e]	[f]	[g]	[h]	[i]	[j]	[k]
2018	1	35,146 (33,012)	21,233 (21,043)	72 (71)	2 (1)	7 (7)	63 (63)	0 (0)	38 (37)	15 (15)	0 (0)	19 (19)
	2	35,293 (33,154)	21,372 (21,183)	77 (76)	2 (1)	7 (7)	68 (68)	0 (0)	42 (41)	15 (15)	0 (0)	20 (20)
	3	35,425 (33,286)	21,491 (21,304)	85 (84)	2 (1)	7 (7)	76 (76)	0 (0)	47 (46)	15 (15)	0 (0)	23 (23)

ne.jp

年	月	[a]	[b]	[c]	[d]	[e]	[f]	[g]	[h]	[i]	[j]	[k]
2018	1	13,044 (13,044)	5,721 (5,590)	102 (99)	3 (3)	6 (6)	93 (90)	0 (0)	70 (68)	26 (25)	0 (0)	6 (6)
	2	13,037 (10,605)	5,728 (5,601)	103 (100)	3 (3)	6 (6)	94 (91)	0 (0)	71 (69)	25 (24)	0 (0)	7 (7)
	3	13,008 (10,583)	5,728 (5,602)	105 (102)	3 (3)	6 (6)	96 (93)	0 (0)	71 (69)	27 (26)	0 (0)	7 (7)

gr.jp

年	月	[a]	[b]	[c]	[d]	[e]	[f]	[g]	[h]	[i]	[j]	[k]
2018	1	6,112 (5,438)	2,935 (2,884)	27 (27)	1 (1)	1 (1)	25 (25)	0 (0)	19 (19)	5 (5)	0 (0)	3 (3)
	2	6,100 (5,424)	2,940 (2,884)	25 (25)	1 (1)	1 (1)	23 (23)	0 (0)	19 (19)	4 (4)	0 (0)	2 (2)
	3	6,093 (5,425)	2,944 (2,892)	27 (27)	1 (1)	1 (1)	25 (25)	0 (0)	19 (19)	5 (5)	0 (0)	3 (3)



ed.jp

年	月	[a]	[b]	[c]	[d]	[e]	[f]	[g]	[h]	[i]	[j]	[k]
2018	1	5,230 (4,852)	2,889 (2,854)	21 (21)	0 (0)	0 (0)	21 (21)	0 (0)	16 (16)	2 (2)	0 (0)	3 (3)
	2	5,243 (4,857)	2,904 (2,867)	21 (21)	0 (0)	0 (0)	21 (21)	0 (0)	16 (16)	2 (2)	0 (0)	3 (3)
	3	5,267 (4,864)	2,931 (2,898)	21 (21)	0 (0)	0 (0)	21 (21)	0 (0)	16 (16)	2 (2)	0 (0)	3 (3)

lg.jp

年	月	[a]	[b]	[c]	[d]	[e]	[f]	[g]	[h]	[i]	[j]	[k]
2018	1	1,652 (1,216)	937 (921)	2 (2)	0 (0)	1 (1)	1 (1)	0 (0)	0 (0)	2 (2)	0 (0)	0 (0)
	2	1,654 (1,217)	939 (922)	2 (2)	0 (0)	1 (1)	1 (1)	0 (0)	0 (0)	2 (2)	0 (0)	0 (0)
	3	1,656 (1,220)	943 (930)	2 (2)	0 (0)	1 (1)	1 (1)	0 (0)	0 (0)	2 (2)	0 (0)	0 (0)

地域型・都道府県型

年	月	[a]	[b]	[c]	[d]	[e]	[f]	[g]	[h]	[i]	[j]	[k]
2018	1	13,414 (7,530)	4,183 (3,959)	150 (28)	124 (2)	2 (2)	24 (24)	0 (0)	18 (18)	129 (7)	0 (0)	3 (3)
	2	13,317 (7,564)	4,244 (4,018)	148 (26)	124 (2)	2 (2)	22 (22)	0 (0)	17 (17)	128 (6)	0 (0)	3 (3)
	3	13,319 (7,593)	4,114 (3,905)	153 (31)	124 (2)	2 (2)	27 (27)	0 (0)	18 (18)	132 (10)	0 (0)	3 (3)

汎用

年	月	[a]	[b]	[c]	[d]	[e]	[f]	[g]	[h]	[i]	[j]	[k]
2018	1	988,365 (756,800)	404,737 (391,728)	6,322 (5,565)	1,096 (535)	178 (162)	5,043 (4,863)	5 (5)	1,746 (1,686)	797 (536)	18 (18)	3,761 (3,325)
	2	992,488 (757,611)	409,050 (395,924)	6,429 (5,653)	1,130 (558)	182 (165)	5,112 (4,925)	5 (5)	1,812 (1,751)	815 (553)	18 (18)	3,784 (3,331)
	3	996,067 (759,837)	410,907 (397,925)	6,547 (5,527)	1,152 (569)	182 (166)	5,207 (4,786)	6 (5)	1,884 (1,821)	834 (573)	18 (18)	3,811 (3,115)

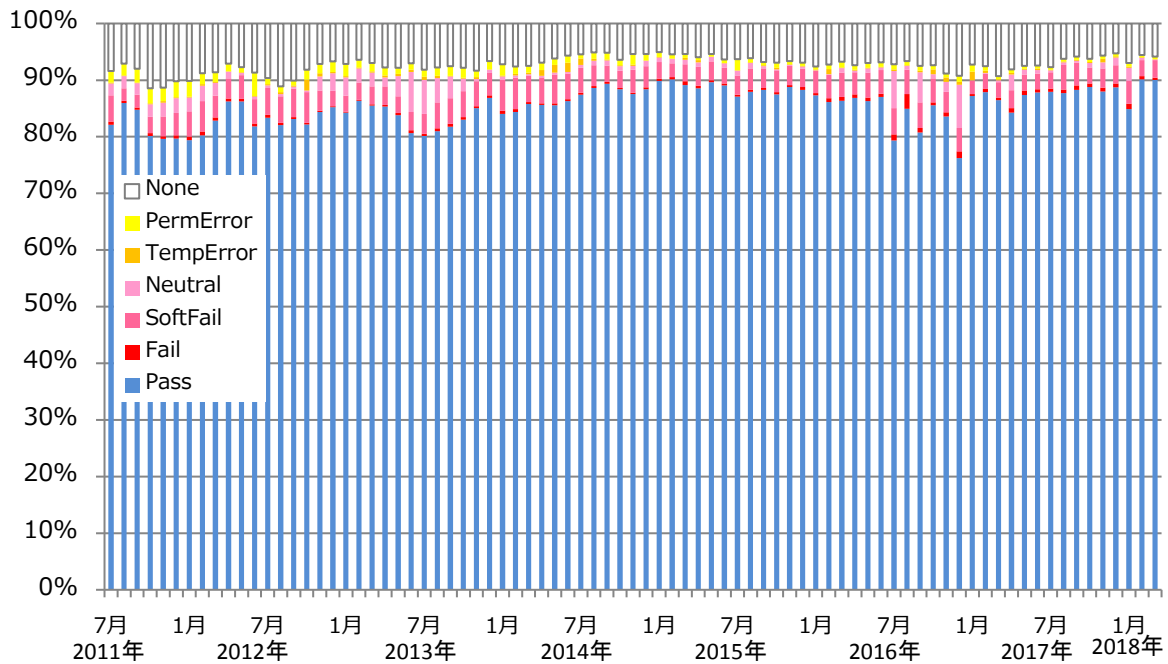
出典：（一財）日本データ通信協会と（株）日本レジストリサービスとの共同研究



第7節 送信ドメイン認証技術の認証結果

1 SPFの認証結果の推移（2018年3月まで）

図表S-7-1 SPFの認証結果の推移



出典：電気通信事業者7社の協力により総務省がとりまとめ

2011年度（2011年7月以降のみ）

	4月	5月	6月	7月	8月	9月	10月	11月	12月	1月	2月	3月
None	-	-	-	8.41%	7.11%	7.99%	11.46%	11.35%	10.22%	10.16%	8.80%	8.59%
PermError	-	-	-	2.01%	2.05%	2.42%	2.65%	2.36%	2.83%	2.76%	1.89%	1.72%
TempError	-	-	-	0.15%	0.12%	0.12%	0.13%	0.27%	0.12%	0.15%	0.28%	0.16%
Neutral	-	-	-	2.12%	2.14%	2.06%	2.24%	2.40%	2.63%	2.47%	2.70%	2.26%
SoftFail	-	-	-	4.64%	2.22%	2.24%	2.88%	3.52%	3.93%	4.42%	5.40%	3.86%
Fail	-	-	-	0.56%	0.37%	0.38%	0.49%	0.44%	0.60%	0.62%	0.67%	0.57%
Pass				82.11%	85.98%	84.78%	80.15%	79.64%	79.66%	79.42%	80.25%	82.84%

2012年度

	4月	5月	6月	7月	8月	9月	10月	11月	12月	1月	2月	3月
None	7.06%	7.70%	8.64%	9.62%	11.13%	10.07%	8.15%	7.12%	6.71%	7.13%	6.39%	6.96%
PermError	1.38%	0.93%	4.16%	1.07%	1.01%	0.88%	1.77%	1.65%	1.85%	2.15%	1.36%	1.48%
TempError	0.08%	0.10%	0.12%	0.26%	0.33%	0.23%	1.92%	0.58%	0.21%	0.23%	0.18%	0.22%
Neutral	1.16%	0.37%	0.43%	0.44%	0.39%	0.33%	0.31%	2.47%	3.14%	3.22%	2.47%	2.45%
SoftFail	3.59%	4.19%	4.31%	4.76%	4.68%	5.01%	5.38%	3.56%	2.69%	2.84%	3.05%	3.16%
Fail	0.51%	0.47%	0.50%	0.49%	0.43%	0.34%	0.28%	0.22%	0.16%	0.19%	0.19%	0.21%
Pass	86.23%	86.23%	81.84%	83.37%	82.04%	83.14%	82.20%	84.39%	85.23%	84.24%	86.36%	85.52%



2013 年度

	4月	5月	6月	7月	8月	9月	10月	11月	12月	1月	2月	3月
None	7.79%	7.84%	7.04%	8.18%	7.76%	7.53%	7.82%	8.31%	6.66%	7.18%	7.58%	7.47%
PermError	1.37%	1.03%	1.13%	1.20%	1.48%	1.69%	1.74%	1.18%	1.44%	1.97%	1.29%	1.17%
TempError	0.36%	0.43%	0.40%	0.58%	0.38%	0.13%	0.16%	0.30%	0.09%	0.19%	0.33%	0.31%
Neutral	1.59%	3.56%	7.08%	6.01%	4.29%	3.85%	2.20%	0.38%	0.55%	0.64%	0.39%	0.21%
SoftFail	3.26%	2.92%	3.21%	3.52%	4.58%	4.49%	4.58%	4.43%	3.96%	5.44%	5.52%	4.69%
Fail	0.27%	0.38%	0.49%	0.39%	0.52%	0.51%	0.46%	0.33%	0.42%	0.55%	0.52%	0.36%
Pass	85.35%	83.83%	80.66%	80.11%	80.99%	81.78%	83.04%	85.08%	86.88%	84.04%	84.37%	85.78%

2014 年度

	4月	5月	6月	7月	8月	9月	10月	11月	12月	1月	2月	3月
None	6.92%	6.21%	5.69%	5.42%	5.10%	5.16%	6.40%	5.40%	5.39%	5.07%	5.47%	5.41%
PermError	1.28%	1.11%	1.25%	0.76%	1.13%	1.18%	0.96%	1.87%	1.11%	0.80%	0.70%	0.68%
TempError	1.00%	1.35%	1.64%	1.11%	0.37%	0.19%	0.18%	0.18%	0.10%	0.12%	0.06%	0.30%
Neutral	0.33%	0.36%	0.28%	0.51%	0.78%	0.90%	0.78%	0.70%	0.93%	0.78%	0.83%	0.84%
SoftFail	4.54%	5.05%	4.51%	4.44%	3.66%	2.91%	3.05%	4.08%	3.74%	2.96%	2.43%	2.95%
Fail	0.28%	0.33%	0.30%	0.32%	0.34%	0.30%	0.25%	0.24%	0.32%	0.42%	0.39%	0.70%
Pass	85.63%	85.59%	86.32%	87.43%	88.62%	89.37%	88.37%	87.52%	88.40%	89.84%	90.12%	89.13%

2015 年度

	4月	5月	6月	7月	8月	9月	10月	11月	12月	1月	2月	3月
None	5.97%	5.39%	6.33%	6.29%	6.14%	6.81%	6.89%	6.65%	6.94%	7.58%	7.26%	6.77%
PermError	0.50%	0.43%	0.62%	1.98%	0.71%	0.58%	0.93%	0.53%	0.53%	0.50%	0.77%	0.97%
TempError	0.40%	0.11%	0.08%	0.06%	0.10%	0.16%	0.26%	0.13%	0.11%	0.18%	0.91%	0.11%
Neutral	0.77%	0.74%	0.82%	0.83%	1.01%	0.37%	0.19%	0.15%	0.39%	0.11%	0.13%	0.82%
SoftFail	3.37%	3.34%	2.73%	3.40%	3.68%	3.45%	3.84%	3.43%	3.27%	3.90%	4.13%	4.27%
Fail	0.42%	0.35%	0.33%	0.35%	0.42%	0.36%	0.39%	0.33%	0.47%	0.42%	0.69%	0.72%
Pass	88.58%	89.64%	89.09%	87.08%	87.93%	88.26%	87.50%	88.78%	88.29%	87.31%	86.10%	86.33%

2016 年度

	4月	5月	6月	7月	8月	9月	10月	11月	12月	1月	2月	3月
None	7.34%	6.95%	6.88%	7.20%	6.64%	7.48%	7.35%	8.84%	9.26%	7.24%	7.52%	9.28%
PermError	0.84%	0.88%	0.78%	0.92%	0.71%	0.87%	0.77%	0.70%	1.03%	1.28%	0.82%	0.60%
TempError	0.14%	0.11%	0.11%	0.28%	0.13%	0.26%	0.84%	0.76%	0.52%	1.51%	0.36%	0.13%
Neutral	0.28%	0.72%	0.47%	6.56%	0.69%	5.30%	0.72%	1.74%	7.64%	0.06%	0.12%	0.37%
SoftFail	3.93%	4.41%	4.18%	4.62%	4.30%	4.56%	4.26%	3.62%	4.15%	2.39%	2.73%	2.71%
Fail	0.61%	0.65%	0.61%	1.06%	2.61%	0.79%	0.51%	0.74%	1.15%	0.35%	0.56%	0.47%
Pass	86.85%	86.28%	87.01%	79.37%	84.92%	80.74%	85.54%	83.60%	76.26%	87.18%	87.90%	86.45%

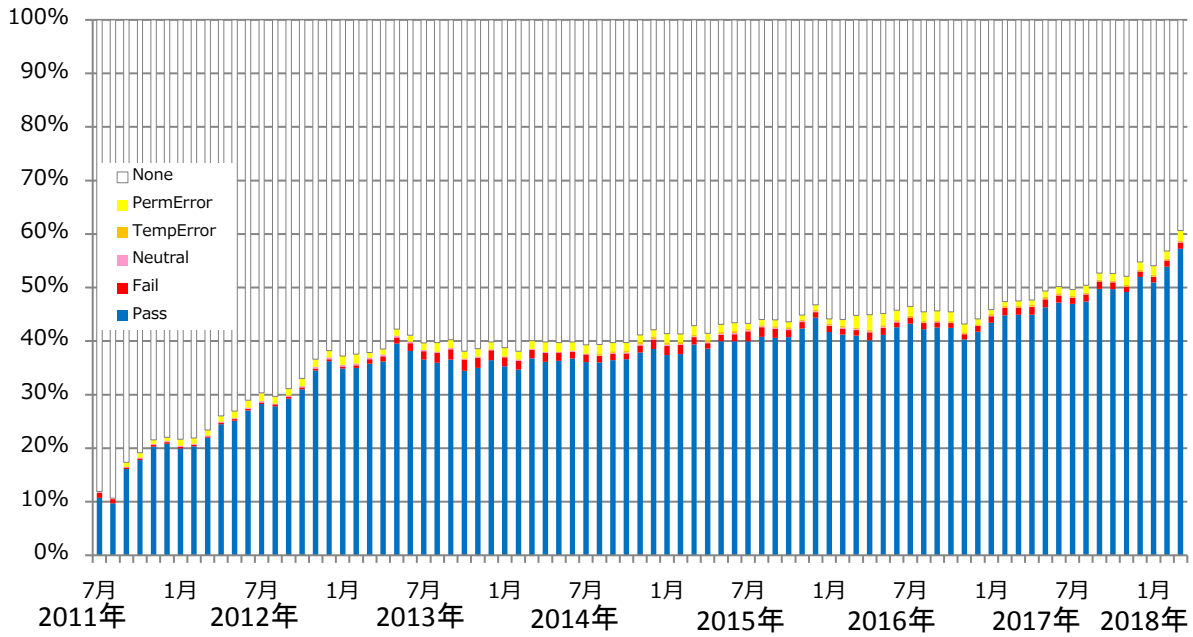
2017 年度

	4月	5月	6月	7月	8月	9月	10月	11月	12月	1月	2月	3月
None	8.09%	7.48%	7.45%	7.70%	6.26%	5.86%	6.24%	5.69%	5.26%	6.95%	5.54%	5.83%
PermError	0.67%	0.48%	0.49%	0.46%	0.43%	0.55%	0.59%	0.57%	0.52%	0.67%	0.43%	0.45%
TempError	0.27%	0.18%	0.29%	0.10%	0.15%	0.17%	0.16%	0.61%	0.25%	0.18%	0.09%	0.05%
Neutral	2.76%	0.89%	0.60%	0.34%	0.48%	0.31%	0.79%	1.06%	1.35%	2.35%	0.44%	0.16%
SoftFail	3.16%	2.78%	2.75%	2.88%	4.37%	4.06%	2.84%	3.38%	3.22%	3.98%	2.81%	3.06%
Fail	0.82%	0.81%	0.60%	0.56%	0.63%	0.76%	0.62%	0.70%	0.65%	1.01%	0.53%	0.40%
Pass	84.24%	87.37%	87.82%	87.95%	87.68%	88.29%	88.76%	88.00%	88.75%	84.86%	90.17%	90.05%



2 DKIM の認証結果の推移 (2018年3月まで)

図表 S-7-2 DKIM の認証結果の推移



出典：電気通信事業者4社の協力により総務省がとりまとめ

2011年度 (2011年7月以降のみ)

	4月	5月	6月	7月	8月	9月	10月	11月	12月	1月	2月	3月
None	-	-	-	88.08%	89.30%	82.64%	80.86%	78.47%	77.97%	78.34%	78.10%	76.61%
PermError	-	-	-	0.08%	0.06%	0.85%	0.88%	0.72%	0.67%	1.21%	1.07%	0.96%
TempError	-	-	-	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.03%
Neutral	-	-	-	0.18%	0.13%	0.13%	0.18%	0.19%	0.22%	0.21%	0.17%	0.16%
Fail	-	-	-	0.96%	0.81%	0.29%	0.32%	0.32%	0.32%	0.27%	0.30%	0.25%
Pass	-	-	-	10.70%	9.70%	16.10%	17.76%	20.30%	20.83%	19.97%	20.36%	21.97%

2012年度

	4月	5月	6月	7月	8月	9月	10月	11月	12月	1月	2月	3月
None	73.95%	73.09%	71.06%	69.64%	70.29%	68.90%	66.98%	63.38%	61.77%	62.81%	62.42%	62.14%
PermError	1.06%	1.23%	1.34%	1.53%	1.32%	1.27%	1.40%	1.41%	1.26%	1.64%	1.75%	0.97%
TempError	0.04%	0.04%	0.02%	0.05%	0.03%	0.04%	0.03%	0.02%	0.01%	0.01%	0.01%	0.01%
Neutral	0.16%	0.19%	0.21%	0.23%	0.19%	0.20%	0.22%	0.29%	0.32%	0.30%	0.35%	0.24%
Fail	0.29%	0.29%	0.29%	0.30%	0.32%	0.34%	0.37%	0.37%	0.35%	0.38%	0.45%	0.84%
Pass	24.50%	25.16%	27.07%	28.25%	27.89%	29.25%	30.99%	34.53%	36.29%	34.86%	35.02%	35.80%



2013年度

	4月	5月	6月	7月	8月	9月	10月	11月	12月	1月	2月	3月
None	61.49%	57.76%	58.87%	60.31%	60.26%	59.74%	61.91%	61.42%	60.16%	61.22%	61.87%	59.92%
PermError	1.00%	1.21%	1.25%	1.30%	1.68%	1.50%	1.31%	1.43%	1.38%	1.60%	1.54%	1.56%
TempError	0.02%	0.01%	0.01%	0.01%	0.00%	0.01%	0.02%	0.07%	0.01%	0.00%	0.01%	0.00%
Neutral	0.32%	0.31%	0.24%	0.23%	0.21%	0.25%	0.19%	0.20%	0.17%	0.22%	0.28%	0.16%
Fail	0.98%	1.18%	1.48%	1.61%	1.89%	1.95%	2.07%	1.91%	1.83%	1.63%	1.60%	1.57%
Pass	36.19%	39.52%	38.15%	36.53%	35.95%	36.55%	34.49%	34.98%	36.45%	35.33%	34.71%	36.79%

2014年度

	4月	5月	6月	7月	8月	9月	10月	11月	12月	1月	2月	3月
None	60.17%	60.28%	60.16%	60.71%	60.65%	60.29%	60.29%	58.85%	57.87%	58.61%	58.63%	57.10%
PermError	1.85%	1.65%	1.63%	1.59%	1.65%	1.57%	1.47%	1.32%	1.29%	1.65%	1.51%	1.66%
TempError	0.01%	0.05%	0.06%	0.09%	0.41%	0.38%	0.39%	0.46%	0.43%	0.45%	0.42%	0.39%
Neutral	0.13%	0.13%	0.13%	0.10%	0.08%	0.09%	0.15%	0.16%	0.17%	0.13%	0.11%	0.10%
Fail	1.71%	1.60%	1.29%	1.40%	1.19%	1.21%	1.12%	1.32%	1.67%	1.74%	1.74%	1.41%
Pass	36.14%	36.29%	36.73%	36.11%	36.02%	36.45%	36.59%	37.89%	38.56%	37.41%	37.59%	39.35%

2015年度

	4月	5月	6月	7月	8月	9月	10月	11月	12月	1月	2月	3月
None	58.52%	56.84%	56.56%	56.66%	55.94%	56.02%	56.36%	55.10%	53.21%	55.83%	55.99%	55.21%
PermError	1.34%	1.43%	1.57%	1.05%	1.11%	1.23%	1.03%	0.84%	0.91%	0.83%	1.14%	2.23%
TempError	0.42%	0.40%	0.38%	0.32%	0.22%	0.26%	0.35%	0.30%	0.34%	0.35%	0.33%	0.32%
Neutral	0.12%	0.15%	0.19%	0.18%	0.16%	0.17%	0.17%	0.19%	0.16%	0.15%	0.16%	0.16%
Fail	1.01%	1.23%	1.35%	1.85%	1.78%	1.67%	1.34%	1.20%	1.02%	1.12%	1.16%	1.06%
Pass	38.60%	39.95%	39.96%	39.94%	40.80%	40.65%	40.75%	42.37%	44.37%	41.71%	41.23%	41.03%

2016年度

	4月	5月	6月	7月	8月	9月	10月	11月	12月	1月	2月	3月
None	55.09%	54.81%	54.21%	53.49%	54.54%	54.35%	54.51%	56.81%	55.84%	54.08%	52.60%	52.47%
PermError	2.77%	2.24%	1.85%	1.76%	1.73%	1.79%	1.74%	1.55%	1.00%	0.88%	0.79%	0.87%
TempError	0.35%	0.34%	0.33%	0.33%	0.32%	0.33%	0.34%	0.31%	0.31%	0.35%	0.37%	0.35%
Neutral	0.15%	0.14%	0.11%	0.03%	0.03%	0.03%	0.03%	0.03%	0.03%	0.04%	0.04%	0.04%
Fail	1.46%	1.30%	0.88%	1.11%	1.14%	0.96%	0.89%	0.96%	1.04%	1.22%	1.40%	1.31%
Pass	40.18%	41.18%	42.62%	43.28%	42.24%	42.54%	42.49%	40.34%	41.78%	43.43%	44.80%	44.95%

2017年度

	4月	5月	6月	7月	8月	9月	10月	11月	12月	1月	2月	3月
None	52.31%	50.65%	49.84%	50.35%	49.59%	47.28%	47.37%	47.89%	45.18%	45.95%	43.18%	39.33%
PermError	0.88%	1.06%	1.22%	1.17%	1.35%	1.25%	1.29%	1.63%	1.50%	1.67%	1.41%	1.89%
TempError	0.39%	0.47%	0.38%	0.33%	0.31%	0.31%	0.32%	0.31%	0.31%	0.33%	0.32%	0.29%
Neutral	0.03%	0.03%	0.03%	0.03%	0.03%	0.03%	0.03%	0.04%	0.04%	0.04%	0.05%	0.09%
Fail	1.44%	1.48%	1.32%	1.17%	1.35%	1.34%	1.29%	0.94%	1.02%	1.03%	1.14%	1.15%
Pass	44.94%	46.31%	47.22%	46.95%	47.36%	49.79%	49.69%	49.20%	51.96%	50.98%	53.89%	57.26%

資料編



1 関係法令・窓口等

(1) 関係資料

関連法令

特定電子メールの送信の適正化等に関する法律等：特定電子メール、同法施行規則の条文、ガイドライン

総務省：http://www.soumu.go.jp/main_sosiki/joho_tsusin/d_syohi/m_mail.html

消費者庁：http://www.caa.go.jp/policies/policy/consumer_transaction/specifed_email/

特定商取引に関する法律等：同法施行規則の条文、ガイドライン

<http://www.no-trouble.go.jp/>

利用者向け資料

撃退！迷惑メール：迷惑メール対策やスマートフォン利用時の注意点をまとめた冊子

https://www.dekyo.or.jp/soudan/data/info/gmeiwaku_book.pdf

撃退！チェーンメール：チェーンメール対策や注意点をまとめた冊子

<https://www.dekyo.or.jp/soudan/chain/image/chainbook.pdf>

技術的な対策

迷惑メール対策技術の開発及び導入状況：特定電子メール法に基づき、電気通信事業者における迷惑メール対策技術の開発及び導入状況を毎年1回作成・公表（総務省作成）

http://www.soumu.go.jp/menu_news/s-news/01kiban18_01000029.html

有害情報対策ポータルサイト：迷惑メール対策編－迷惑メール対策に関する情報を随時整理し、公表（インターネット協会迷惑メール対策委員会作成）

http://salt.iajapan.org/wpmu/anti_spam/

送信ドメイン認証及び OP25B に関する法的解釈：送信ドメイン認証及び OP25B に関して、一般的ケースにおける法的解釈を整理したもの（総務省作成）

http://www.soumu.go.jp/main_sosiki/joho_tsusin/d_syohi/m_mail/legal.html



(2) 関係組織・相談窓口

関連組織

名称	URL
総務省	http://www.soumu.go.jp/main_sosiki/joho_tsusin/d_syohi/m_mail.html
消費者庁	http://www.caa.go.jp/policies/policy/consumer_transaction/ http://www.no-trouble.go.jp/
(独) 国民生活センター	http://www.kokusen.go.jp/
(一財) 日本データ通信協会 「迷惑メール相談センター」	https://www.dekyo.or.jp/soudan/
(一財) 日本産業協会	http://www.nissankyo.or.jp/
(一財) インターネット協会 「迷惑メール対策委員会」	http://www.iajapan.org/anti_spam/
フィッシング対策協議会	https://www.antiphishing.jp/
(一財) マルチメディア振興センター 「e-ネットキャラバン」	https://www.e-netcaravan.jp/
(一社) セーフアインターネット協会 「インターネット・ホットラインセンター」	http://www.internethotline.jp/
違法・有害情報相談センター	https://www.ihaho.jp/
UCENet (旧名称: (LAP))	https://www.ucenet.org/ 迷惑通信 (迷惑メールを含む) 対策法執行機関を中心とした国際的な会合
M ³ AAWG	https://www.m3aawg.org/ 迷惑メールを含めた、インターネット上のウイルスや DoS 攻撃などに対処するために通信関連企業が集まったグループ



相談窓口

名称	詳細
総務省 「電気通信消費者相談センター」	03-5253-5900 平日 9:30~12:00、13:00~17:00 http://www.soumu.go.jp/main_sosiki/joho_tsusin/d_syohi/syohi/syohi_soudan.htm 電気通信サービス(電話、電子メール)を利用している際のトラブルなどについての相談
消費者庁・全国消費生活センター 「消費者ホットライン」	全国统一番号 188 (局番なし) IP 電話など一部の電話不可 お近くの消費生活センターや消費生活相談窓口を案内
(一財) 日本データ通信協会 「迷惑メール相談センター」	03-5974-0068 平日 10:00~12:00、13:00~17:00(年末年始を除く) 広告・宣伝メールに関する相談
(一財) 日本産業協会 「電子商取引モニタリングセンター」	03-3256-3344 平日 10:00~17:00(年末年始を除く) http://www.nissankyo.or.jp/ 特定商取引法関連を中心に消費生活相談や特定商取引法の「申出制度」についての問い合わせ。消費者の他、企業・団体の方からの相談も可能
(独) 情報処理推進機構:IPA 「情報セキュリティ安心相談窓口」	03-5978-7509 平日 10:00~10~17:00(年末年始を除く) https://www.ipa.go.jp/security/anshin/ ウイルスや不正アクセスに関する技術的な相談に対してアドバイスを提供する窓口。メール相談も可能
法務省人権擁護局 「常設人権相談所」	みんなの人権 110 番 0570-003-110 平日 8:30~17:15 子どもの人権 110 番 0120-007-110 平日 8:30~17:15 女性の人権ホットライン 0570-070-810 平日 8:30~17:15 http://www.moj.go.jp/JINKEN/ 差別、いじめ、嫌がらせなど人権に関する相談
文部科学省 「24 時間子供 SOS ダイヤル」	0120-0-78310 年中無休、24 時間 http://www.mext.go.jp/ijime/ 子供たちが全国どこからでも、夜間・休日を含めて、いじめの相談をすることができるよう、全都道府県及び指定都市教育委員会で実施。
日本司法支援センター 「法テラス」	0570-078-374(PHS 可) 平日 9:00~21:00 土曜 9:00~17:00 IP 電話からは 03-6745-5600 http://www.houterasu.or.jp/ 問い合わせ内容に応じて法制度や関係機関の相談窓口を紹介



名称	詳細
docomo ドコモインフォメーションセンター	ドコモの携帯電話から 151 一般電話などから 0120-800-000 9:00～20:00(年中無休) https://www.nttdocomo.co.jp/
au 総合案内	au の携帯電話から 157 au 以外の携帯電話、一般電話から 0077-7-111 9:00～20:00(年中無休) https://www.au.com/ 音声ガイダンスは 24 時間利用可能
au iPhone テクニカルサポート	0077-7066 (携帯電話・PHS 可) 上記番号が利用できない場合 0120-345-516 平日 9:00～19:00 土日祝 9:00～17:00 iPhone・iPad の操作方法・各種設定方法・サービス全般の問い合わせ窓口
SoftBank 総合案内	ソフトバンク携帯電話から 157 一般電話などから 0800-919-0157 9:00～20:00(年中無休) https://www.softbank.jp/mobile/
SoftBank スマートフォンテクニカルサポートセンター	ソフトバンク携帯電話から 151 一般電話などから 0800-1700-151 平日 9:00～19:00 土日祝 9:00～17:00 紛失などによる回線停止、各種変更手続、操作、故障についての問い合わせ窓口
SoftBank iPhone テクニカルサポートセンター	ソフトバンク携帯電話から 151 一般電話などから 0800-2223-151 平日 9:00～19:00 土日祝 9:00～17:00 紛失などによる回線停止、各種変更手続、アドレス設定、故障についての問い合わせ窓口
SoftBank iPad テクニカルサポートセンター	携帯電話/一般電話から 0800-2223-152 平日 9:00～19:00 土日祝 9:00～17:00 iPad 利用者向けの問い合わせ窓口



2 迷惑メール対策推進協議会 関係資料

(1) 迷惑メール対策推進協議会設置要綱

1 目的

いわゆる迷惑メール問題については、これまで幅広い関係者による様々な対策が進められてきたところであるが、送信手法が巧妙化・悪質化し、また、海外からの迷惑メールの送信が増大している中で、迷惑メール対策に関わる関係者が連携し、効果的な対策の実施に取り組んでいくことが強く求められている。このため、電子メールの利用環境の一層の改善に向け、関係者間の緊密な連絡を確保し、最新の情報共有、対応方策の検討、対外的な情報提供などを行うことにより、関係者による効果的な迷惑メール対策の推進に資することを目的として、「迷惑メール対策推進協議会」（以下「協議会」という。）を設置する。

2 構成

1. 協議会は、別紙に掲げる構成員をもって構成する。
2. 協議会に、座長及び座長代理を置く。座長は協議会を招集し、主宰する。座長代理は、座長を補佐し、座長不在のときは、座長に代わり、その職務を遂行する。
3. 座長は構成員の互選により選任する。座長代理は、座長が指名する。
4. 構成員以外の者であって協議会に参加しようとするものは、構成員の過半数の了解を得て、構成員となることができる。

3 運営

1. 迷惑メール対策に関わる実務的な問題に関わる情報共有、対策の検討などを行うため、協議会に、構成員の一部（構成員が指名する者を含む。）からなる幹事会を置く。幹事会の詳細については、別に定める。
2. 協議会は、必要に応じて、ワーキンググループ等を設置することができる。
3. 協議会は、必要に応じて、外部の関係者の出席を求め、その意見を聞くことができる。
4. その他協議会の運営に関しては、座長が定めるところによる。

4 事務局

協議会の事務運営は、関係者の協力を得て、一般財団法人日本データ通信協会迷惑メール相談センターが行う。



(2) 迷惑メール追放宣言

我が国では、携帯電話やインターネットの発展・普及に伴い、新たなコミュニケーション文化としての電子メールが広く国民に定着してきている。その一方で、いわゆる迷惑メールにより、望まない情報の着信による受信者への支障、大量のあて先不明の電子メールの処理に伴う電気通信ネットワークへの支障、正当なメールマーケティングを行う事業者への支障などがあり、さらにフィッシングやワンクリック詐欺等に結びつくこともあるなど、様々な支障が生じている。

この迷惑メールに対しては、平成14年(2002年)の「特定電子メールの送信の適正化等に関する法律」の制定及び「特定商取引に関する法律」の改正などによる制度的な対応が行われており、また、本年には、両法の一部改正により、いわゆるオプトイン規制が導入されるなど、実効性の効果に向けた規制の強化が図られてきているところである。

また、迷惑メール対策については、このような制度的な方策のみならず、技術的な対策、電気通信事業者による自主的な措置、利用者への周知啓発・相談体制の充実、国際連携の推進など、関係者による総合的対策が必要とされるものである。

このような中で、迷惑メール対策に関わる関係者が広く集まり、本日、「迷惑メール対策推進協議会」を設置することとした。ここに集まった関係者は、それぞれの立場から自ら必要な措置を精力的に講じていくとともに、積極的に関係者への周知・広報活動を行うなど、継続的な取組を行うことにより、我が国からの迷惑メールの追放を図っていくことを宣言する。

2008年11月27日
迷惑メール対策推進協議会

関係者が講ずべき取組の例

電気通信事業者

- ・ OP25B など、迷惑メールを送信させないための技術の開発・導入、外国の電気通信事業者への普及促進
- ・ 迷惑メールフィルターなど、受信者側で利用可能な迷惑メール対策のためのサービス提供
- ・ 迷惑メールに関する関係者への周知

広告関係者

- ・ 適正な同意の取得など、健全性を確保したメールマーケティングの実施
- ・ 迷惑メールに関する関係者への周知

配信事業者

- ・ 広告・宣伝メールの適切な配信
- ・ 迷惑メールに関する関係者への周知

セキュリティベンダー等

- ・ 効果的なフィルタリングソフト等の提供
- ・ 迷惑メールに関する関係者への周知



消費者団体等

- ・ 利用者側で行える迷惑メールへの対応策についての消費者に対する周知

行政機関等

- ・ 法の迅速かつ適正な執行
- ・ 迷惑メールに関する関係者への周知
- ・ 迷惑メールに関する情報収集、受信者からの相談受付の適切な実施
- ・ 迷惑メール対策に関わる外国執行当局との連携の推進

その他関係者

- ・ 送信ドメイン認証の活用など
- ・ 迷惑メールに関する関係者への周知



(3) 迷惑メール対策推進協議会構成員構成員

役職	氏名	組織名
	有木 節二	(一社) 電気通信事業者協会 専務理事
	石田 幸枝	(公社) 全国消費生活相談員協会 理事 消費者団体訴訟室長 I T研究会代表
	伊藤 彰浩	(株) アクリート 代表取締役社長
	岩本 新一	シナジーマーケティング (株) 管理部 部長
	大泰司 章	(財) 日本情報経済社会推進協会 インターネットトラストセンター 企画室長
	大濱 健志	警察庁 生活安全局情報技術犯罪対策課長
	大村 真一	総務省 総合通信基盤局 電気通信事業部 消費者行政第二課長
	岡村 久道	弁護士 京都大学大学院医学研究科講師
	興津 智章	トライコーン (株) 取締役
	片山 建	日本マイクロソフト (株) 法務・政策企画統括本部 政策企画本部 次長
	勝野 正博	(一社) 日本インタラクティブ広告協会 専務理事
	鎌野 篤	(株) 朝日ネット 執行役員 システム部 部長
	川口 真理	(一財) 日本産業協会 電子商取引モニタリング センター長
	河内 亜起	PayPal Pte. Ltd. 東京支店 ビジネスインフォメーションセキュリティオフィサー
	菊地 吾朗	(株) シマンテック セールスエンジニアリング本部長
	岸川 徳幸	ビッグロープ (株) サービス事業ライン技術主幹
	岸原 孝昌	(一社) モバイル・コンテンツ・フォーラム 専務理事
	北崎 恵凡	(一財) インターネット協会 迷惑メール対策委員会 副委員長
	木村 孝	ニフティ (株) 人事総務部総務グループ シニアエキスパート
	工藤 潤一	エヌ・ティ・ティ・コミュニケーションズ (株) アプリケーション&コンテンツサービス部長
	後藤 晋一	(株) サパナ 取締役社長
	小林 秀行	シスコシステムズ (合) セキュリティ事業コンサルティング システムズエンジニア
	齋藤 雅弘	弁護士
	佐久間 修	名古屋学院大学 法学部 教授
座長代理	櫻庭 秀次	(株) インターネットイニシアティブ ネットワーク本部アプリケーションサービス部 担当部長
	佐藤 朋哉	消費者庁 取引対策課長
	沢田 登志子	(一社) E Cネットワーク 理事
	椎山 浩二	ソフォス (株) セールスエンジニアリング部 セールスエンジニア
	島野 公志	ソフトバンク (株) I C Tイノベーション本部モバイルE S統括部 担当部長
	末政 延浩	(株) TwoFive 代表取締役



役職	氏名	組織名
	鈴木 信裕	(株) パイブドピッツ 執行役員 CTO
	砂田 浩行	(株) 日本総合研究所 開発推進部門セキュリティ統括室長
	関 聡司	楽天(株) 執行役員 渉外室長
	高橋 哲也	日本ブルーポイント(株) テクニカルサービス ディレクター
	立石 聡明	(一社) 日本インターネットプロバイダー協会 副会長兼専務理事
	玉木 祐介	(独) 国民生活センター 相談情報部 相談第2課 主査
	築嶋 健輔	KDDI(株) 技術統括本部 プラットフォーム開発本部 サービスアプリケーション開発1部 部長
	津山 史生	ソニーネットワークコミュニケーションズ(株) 執行役員 SVP
	土井 隆	(株) ディー・エヌ・エー 渉外統括本部渉外部 シニアマネージャー
	永江 禎	(一社) 日本広告業協会 法務委員会 委員長
	永田 勝美	(株) NTTぷらら 取締役 技術本部長
	長田 三紀	全国地域婦人団体連絡協議会 事務局長
	中本 純子	(一社) 全国消費者団体連絡会 政策スタッフ
座長	新美 育文	明治大学 法学部教授
	野村 維左夫	(株) クオリア クラウドサービス開発本部 本部長
	萩原 健太	トレンドマイクロ(株) TrendMicro Security Incident Response Team チーム統括責任者
	橋本 勇人	チーターデジタル(株) 代表取締役社長
	長谷部 恭男	早稲田大学 法学学術院 法務研究科(法科大学院) 教授
	畠 良	ヤフー(株) コーポレートインテリジェンス本部リーダー
	畠山 昌録	EASY SOLUTIONS JAPAN(合) 営業部 日本事業開発マネージャー
	林 博史	(公社) 日本アドタイザーズ協会 Web広告研究会事務局オフィスマネージャー
	藤木 愛	アイマトリックス(株) マーケティング部
	堀内 浩規	(一社) 日本ケーブルテレビ連盟 理事 兼 通信制度部長
	松田 和男	(一財) 日本データ通信協会 迷惑メール相談センター所長
	明神 浩	(一社) テレコムサービス協会 企画部長
	山本 健太郎	(一社) JPCERT コーディネーションセンター エンタープライズサポートグループ情報セキュリティアナリスト
	山本 正明	(株) NTTドコモ プラットフォームビジネス推進部 担当部長

2018年7月10日現在(50音順・敬称略)



3 索引

A～Z

BEC	8
IP アドレス	16
固定 IP アドレス.....	31,32
動的 IP アドレス.....	31,67,79
LAP/UCENet	9,12,110,115,145
M³AAWG	10,93,103,118
OP25B	67
OP25B と通信の秘密.....	79
RFC	
RFC2554.....	57
RFC4954.....	57
RFC5321、5322.....	16,36,69,70
RFC7001.....	65
RFC7208.....	69
RFC7489.....	70,103
SMS	8,14,52,78,89,97
SMS 配信サービス事業者.....	97
海外での SMS 規制.....	52
SNS	14,34

ア～ワ

ウイルス	18,29,73,75
ウイルス作成・提供・使用の禁止.....	51
ウイルス対策.....	5
オプトイン	36,40,52,84
オプトアウト	40,46,52,74,84
架空請求、不当請求	18,20,36,86,98,104
送信ドメイン認証技術	68
DKIM.....	71
DKIM の設定.....	62

DKIM の認証結果.....	141
DMARC.....	70
DMARC の設定.....	62
DMARC の認証結果.....	65,68,71
DMARC ポリシー.....	62,65,68,71,136
DMARC 導入に関する法的な留意点.....	6,8,112
SPF.....	69
SPF の設定.....	62
SPF の認証結果.....	69,90,139
SPF,DKIM,DMARC の比較.....	68
送信ドメイン認証技術と通信の秘密.....	79
送信ドメイン認証技術の認証結果.....	139
チェーンメール	21,74,76,144
特定商取引法	45
特定商取引法による電子メール広告規制.....	46,48
特定商取引法の執行状況.....	84,135
特定電子メール法	37
特定電子メール法の沿革.....	40
特定電子メール法の詳細.....	42
特定電子メール法の執行状況.....	83,132
特定電子メール法と特定商取引法との比較.....	36
海外での対策法制の整備状況.....	52
フィッシング	20
フィッシング対策協議会.....	106
フィッシングメール.....	3,18,51,90,106
不正利用	
IP アドレスの不正利用.....	32
アカウントの不正利用.....	32
サーバーの不正利用.....	31
ボット	31,67
マルウェア	18,31,34,109,118
迷惑メールフィルター	33,90,149

迷惑メール白書 2018

2018年11月 初版発行

PRINT ISSN 2434-5016 / ONLINE ISSN 2434-4982

編集・発行 **迷惑メール対策推進協議会**

事務局

一般財団法人 日本データ通信協会 迷惑メール相談センター

〒170-8585 東京都豊島区巣鴨 2-11-1 巣鴨室町ビル 7階

TEL: 03-5907-5371

MAIL: q-meiwaku-mail-kyogikai@dekyo.or.jp

URL: <https://www.dekyo.or.jp/soudan/aspc/>

印刷 一般財団法人 日本データ通信協会

本書の全部又は一部の複写、複製及び磁気又は光記録媒体への入力等は、著作権法上での例外を除き禁じられています。
これらの許諾については当事務局までご照会ください。

