

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。

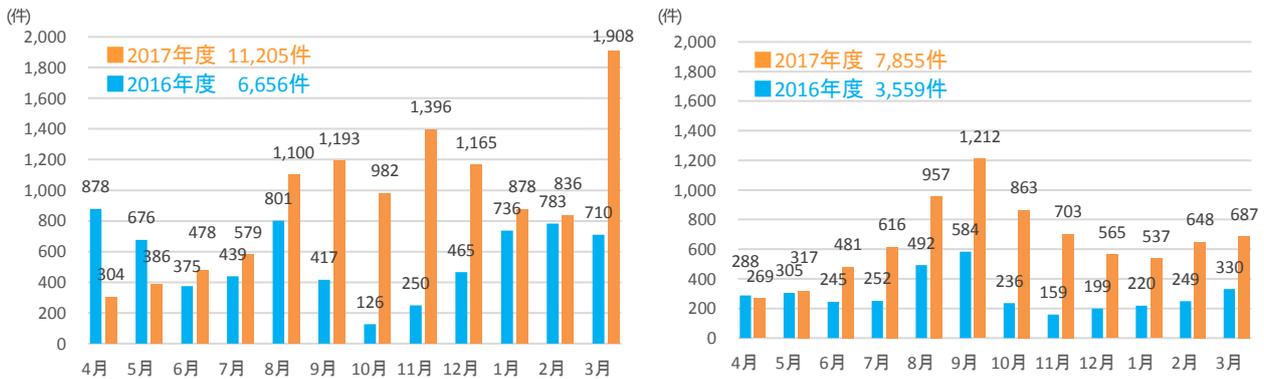


第2節 悪質化・巧妙化する迷惑メールの動向

1 フィッシングメール

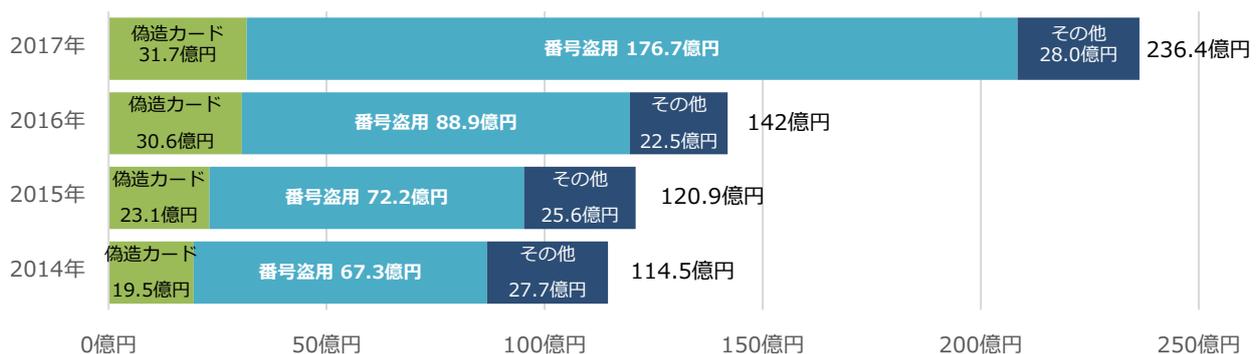
フィッシング対策協議会によれば、2017年度には、フィッシング報告件数は前年度比1.7倍（6,656件→11,205件）と増加し、また、フィッシングサイトのURL件数も前年度比2.2倍（3,559件→7,855件）と増加しています^{注1}。フィッシングメールの内容としては、銀行情報（口座番号、暗証番号など）やクレジットカードの情報を詐取する目的のものに加えて、仮想通貨の情報を詐取する目的のものも確認されています^{注2}。また、（一社）日本クレジット協会によれば、被害額の全てがフィッシングメールを端緒にしたものとは限りませんが、2017年には、クレジットカード不正使用による被害額が前年比1.6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

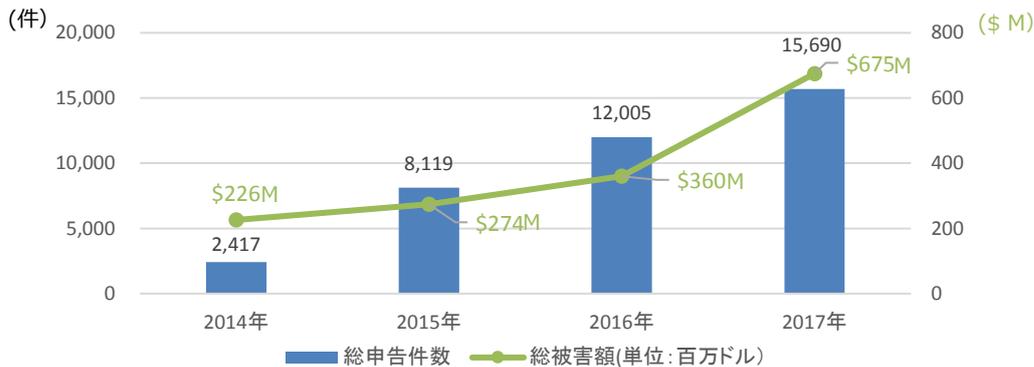
注1 フィッシング対策協議会（フィッシングレポート2018） https://www.antiphishing.jp/report/pdf/phishing_report_2018.pdf
 注2 フィッシング対策協議会（緊急情報等）、トレンドマイクロ社セキュリティブログ（2018年3月19日「仮想通貨を狙うフィッシング詐欺、既に闇市場での「サービス化」も確認」）
 注3 （一社）日本クレジット協会（クレジットカード不正使用被害の集計結果について） <https://www.j-credit.or.jp/download/news20180330b.pdf>



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んら

^{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

