迷惑メール対策ハンドブック 2011

迷惑メール対策推進協議会

目　次

特集
送信ドメイン認証技術の普及促進

【特集】送信ドメイン認証技術の普及促進

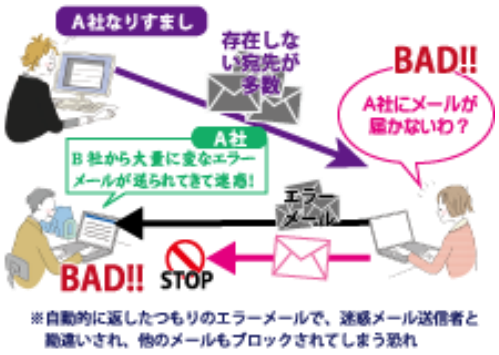
第１節　送信ドメイン認証技術の概要

１　メールの「なりすまし」問題

電子メールは、簡易で便利なコミュニケーションツールとして、広く普及しています。電子メールの通信は、SMTP（シンプル・メール・トランスファー・プロトコル）という通信方式が用いられています。しかし、この通信方式の標準規格は1970年代に策定されたもので、送り手が誰であるのかを確認する仕組みが備わっていません。

そのため、送信者情報のドメインを偽装する、いわゆる「なりすまし」が容易にできてしまい、それによって、近年では、多くの問題が引き起こされています。

図表Ｓ-1　「なりすまし」により発生する問題



(1)フィッシング等に悪用される

有名企業などになりすましたメールにより、メールアドレスやクレジットカード番号、パスワードなどを詐取されるなど、フィッシング等に悪用されるという問題があります。

我が国において、ドメイン名を詐称されることにより信頼性に対する悪影響の大きい、金融機関、自治体などの有名企業等になりすましたメールが送られた事例が、実際に発生しています。

a)金融機関がなりすまされた事例

平成19年（2007年）に日本国内の都市銀行になりすましたメールが送信されました。アカウントが不正アクセスにあったのでアカウントを停止したため、連絡を求める旨の内容で、メール内にURLが記載され、偽のサイトに誘導されるようになっていました。

メールの発信元は、インド、フランス、米国など多数の国にわたり、また、誘導先のサイトも、トルコ、ロシアなど22種類にも及びました。

誘導先サイトが英語だったため、実際に被害があったのかは不明ですが、当該金融機関では、注意喚起をウェブページ等で実施しました。

b)地方公共団体がなりすまされた事例

福島県で、自治体のメールアドレスになりすましたメールが送付された事案がありました。ウィルス感染等を目的としたものと思われます。

同県内の自治体では、自治体のサイトで、なりすましメールについて、注意喚起を行っています。

(2)必要なメールを探しづらい

例えば、大量の迷惑メールが送られることにより、受信者側で必要なメールを探しづらくなる、という問題もあります。なりすまされたメールの場合には、送信元のメールアドレスなどでのフィルタリングをしていても、届いてしまいます。

(3)迷惑メール送信者と勘違いされる

さらに、最近では、なりすまされた迷惑メールにエラーメッセージを返した受信者が、逆に迷惑メールの送信者と勘違いされる、という複雑な問題も出てきています。

SMTP では、宛先不明のメールを受け取った場合には、送信元に対してエラーメッセージを返送することになっています。しかし、送信元がなりすまされている場合には、そのなりすまされた送信元に対してエラーメッセージを返送することになってしまいます。なりすまされた送信者側では、送った覚えのないメールに対するエラーメールが送られてくるため、エラーメールの送信元（標準規格に則ってエラーメールを返送した者）を、迷惑メールの送信者と判断することになってしまいます。

2　送信ドメイン認証技術による解決

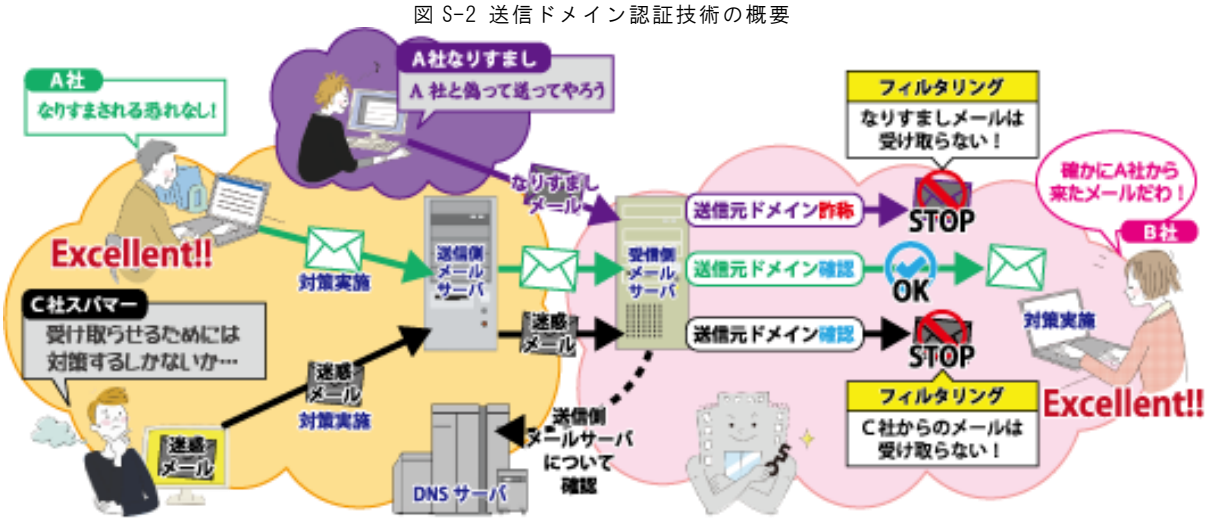
このようななりすましメールの防止策として、「送信ドメイン認証技術」があります。送信ドメイン認証技術とは、受信者が受け取ったメールについて、送信者情報が詐称されているかどうかをドメイン単位で確認可能とする技術で、インターネットの標準規格にもなっています。具体的な方式は、大きく分けて、SPF/Sender ID と DKIM の２つがあり、いずれの方式も、IETF で標準規格化されています。

送信ドメイン認証技術を利用するためには、送信側と受信側の双方で、メールサーバに新たな設定や機能を追加することが必要となります。

しかし、従来の通信方式の標準規格に直接影響を与えることなく下位互換的に導入することができますので、送信側と受信側のどちらからでも導入することができます。また、メールサーバでの対応ですので、個々の利用者が対応するのではなく、メールサーバを管理しているプロバイダや企業などが対応することになります（受信側で、なりすましの確認結果をフィルタリングなどに利用する場合には、利用者による設定が必要となる場合があります）。

なお、送信ドメイン認証技術の詳細については、「第４章　第３節　送信ドメイン認証」をご覧ください。

図 S-2 送信ドメイン認証技術の概要



3　送信ドメイン認証技術を導入する必要性

送信ドメイン認証技術には、なりすましメール対策として、送信側・受信側の双方が対応することが求められています。

(1)送信側

送信側では、なりすましメールにより、顧

客がフィッシング詐欺等の被害に遭うなどの恐れがあり、適切に対応していないと、自ら使用しているドメインについて、顧客の信頼を失う恐れがあります。

将来的には、受信側により、送信ドメイン認証技術に対応し、認証されたメールでなければ、受け取ってもらえないようになる可能性もあります。現に、携帯電話事業者やインターネットサービスプロバイダの中には、送信ドメイン認証技術を用いた受信側のフィルタリングサービスを提供しているところもあり、受信者の設定次第では、そのような事態が生じてきています。

(2)受信側

受信側では、送信ドメイン認証技術に対応した認証を活用することにより、受け取るメールを選別し、より安全な電子メール環境を構築することが可能となります。

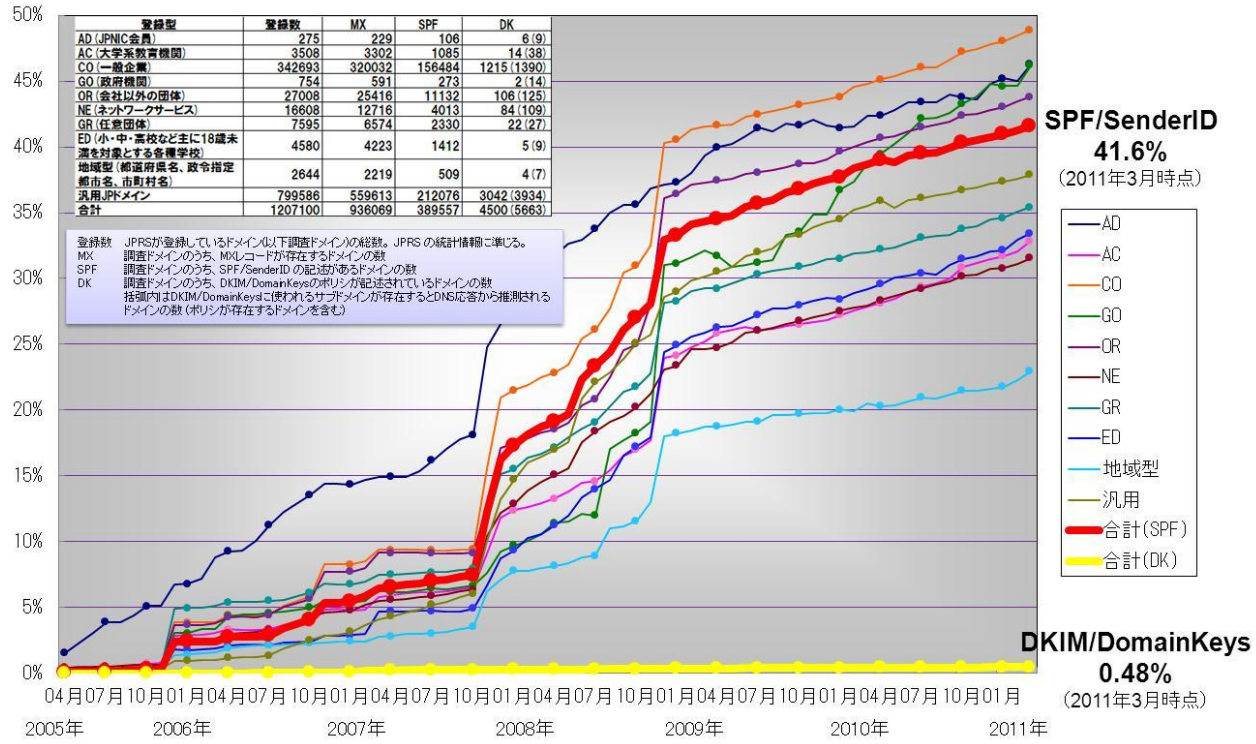
すなわち、第一段階としてなりすましメールを見分けることで、その後のフィルタリング等の処理が、より適切に行えるようになります。

一般の利用者の方も、プロバイダのサービスを利用することにより、対応が可能です（サービスの提供の有無や内容は、プロバイダにより異なります）。

4　送信ドメイン認証技術の普及状況

送信ドメイン認証技術に関して、.jp ドメインでの送信側の導入状況については、WIDE プロジェクト及び JPRS が行っている調査結果によると、ネットワーク方式の送信ドメイン技術である SPF/SenderID は、全体で約 40%のドメインで導入されており、co.jp では、45%超のドメインで導入されているなど、一定の普及が進んできていることがわかります。電子署名方式の送信ドメイン認証技術である DKIM については、現時点で、約 0.5%のドメインで導入されています。

図 S-3　送信ドメイン認証技術の導入状況



登録型	登録数	MX	SPF	DK
AD（JPNIC会員）	275	229	106	6(9)
AC（大学系教育機関）	3508	3302	1085	14(38)
CO（一般企業）	342693	320032	156484	1215(1390)
GO（政府機関）	754	591	273	2(14)
OR（会社以外の団体）	27008	25416	11132	106(125)
NE（ネットワークサービス）	16608	12716	4013	84(109)
GR（任意団体）	7595	6574	2330	22(27)
ED（小・中・高校など主に18歳未満を対象とする各種学校）	4580	4223	1412	5(9)
地域型（都道府県名、政令指定都市名、市町村名）	2644	2219	509	4(7)
汎用JPドメイン	799586	559613	212076	3042(3934)
合計	1207100	936069	389557	4500(5663)

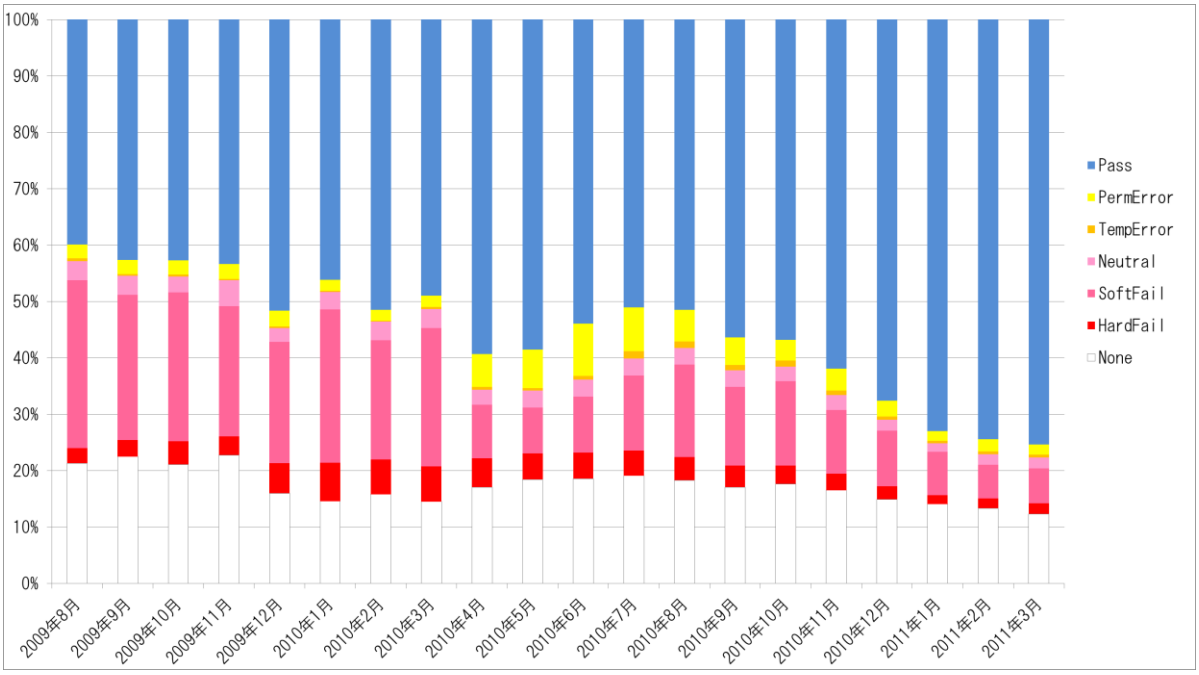
登録数　JPRSが登録しているドメイン以下調査ドメイン）の総数。JPRS の統計情報に準じる。
MX　調査ドメインのうち、MXレコードが存在するドメインの数
SPF　調査ドメインのうち、SPF/SenderID の記述があるドメインの数
DK　調査ドメインのうち、DKIM/DomainKeysのポリシが記述されているドメインの数
括弧内はDKIM/DomainKeysに使われるサブドメインが存在するとDNS応答から推測されるドメインの数（ポリシが存在するドメインを含む）

出典：WIDE プロジェクトが JPRS(Japan Registry Service)との共同研究で行っている調査による

我が国で実際に流通しているメールでの SPF/SenderID への対応状況については、総務省が電気通信事業者の協力により行っている調査結果によると、約 8 割のメールがそれに対応したドメインから送信されてきていることがわかります。そのうち、約半数が正規の送信元から送信されたメールとなっています。

図 S-4 実際に流通している電子メールにおける SPF/Sender ID の対応状況

	2009年					2010年												2011年		
	8月	9月	10月	11月	12月	1月	2月	3月	4月	5月	6月	7月	8月	9月	10月	11月	12月	1月	2月	3月
データ提供者数	4	4	4	4	4	5	5	5	6	6	6	6	6	7	7	7	7	7	7	7
認証結果の割合（①～⑦の各認証結果）／（認証結果総数）（%）																				
① None	21.31%	22.49%	21.11%	22.75%	15.99%	14.57%	15.82%	14.50%	17.07%	18.45%	18.59%	19.05%	18.28%	17.05%	17.63%	16.48%	14.90%	14.10%	13.33%	12.34%
② Neutral	3.34%	3.36%	2.78%	4.55%	2.42%	3.07%	3.27%	3.38%	2.70%	3.04%	3.05%	3.02%	2.97%	2.95%	2.58%	2.62%	1.97%	1.52%	1.85%	1.92%
③ Pass	39.92%	42.61%	42.71%	43.36%	51.64%	46.17%	51.50%	48.99%	59.34%	58.55%	53.90%	50.87%	51.47%	56.38%	56.81%	61.64%	67.61%	72.95%	74.46%	75.35%
④ HardFail	2.69%	2.97%	4.09%	3.35%	5.37%	6.80%	6.13%	6.27%	5.12%	4.65%	4.63%	4.44%	4.10%	3.83%	3.25%	2.89%	2.33%	1.54%	1.75%	1.87%
⑤ SoftFail	29.78%	25.75%	26.46%	23.10%	21.48%	27.26%	21.20%	24.52%	9.47%	8.09%	9.89%	13.22%	16.41%	13.95%	14.97%	11.28%	9.84%	7.70%	5.97%	6.21%
⑥ TempError	0.51%	0.27%	0.37%	0.26%	0.33%	0.21%	0.13%	0.35%	0.51%	0.45%	0.67%	1.33%	1.16%	0.99%	1.09%	0.79%	0.60%	0.40%	0.54%	0.47%
⑦ PermError	2.45%	2.55%	2.49%	2.64%	2.77%	1.91%	1.96%	1.98%	5.79%	6.77%	9.27%	7.69%	5.60%	4.84%	3.67%	3.91%	2.76%	1.79%	2.09%	1.84%



出典：電気通信事業者７社（※）の協力による、総務省とりまとめ
※KDDI 株式会社、NEC ビッグローブ株式会社、株式会社インターネットイニシアティブ、エヌ・ティ・ティ・コミュニケーションズ株式会社、株式会社テクノロジーネットワークス、ニフティ株式会社、ヤフー株式会社

また、多くの電気通信事業者でも、既に送信側での対応が行われており、受信側でもラベリングやフィルタリングの提供が始まっています。

このように、我が国において、送信ドメイン認証技術が比較的早期に一定の普及が進んだのは、政府や電気通信事業者、広告業者等のメール送信者など、様々な関係者による普及のための取り組みが積極的に行われてきた成果です。

しかし、その一方で、送信側については、全ドメインの約６割がいまだSPF/Sender IDに対応していません。前述のように、フィッシング等に悪用される危険性の高い業種であるにもかかわらず、普及率が我が国の全ドメインの普及率（約４割）を下回っている業種も見受けられるところです。

送信ドメイン認証技術は、多くのドメインが対応することにより効果が増していくものであり、送信側として、できるだけ多くのドメイン保有企業が導入することが望まれるものです。特に、ドメイン名を詐称されることにより、信頼性に対する悪影響が大きいと考えられる政府、自治体、金融機関、ショッピングモール等が送信する電子メールに関しては、率先的に対応を推進することが求められており、なりすましメールの撲滅に向けて、関係者による、普及に向けた、さらなる取り組みが求められています。

次節以降では、迷惑メール対策推進協議会をはじめ、関係者による送信ドメイン認証技術の普及に向けた活動について、ご紹介します。

第２節　迷惑メール対策協議会による普及活動

1　『送信ドメイン認証技術 WG』の設置

平成 21 年（2009 年）10 月、迷惑メールへの技術的な対策としての「送信ドメイン認証技術」の普及促進を強化していくため、新たに「送信ドメイン認証技術 WG」が設置されました。

送信ドメイン認証技術の普及促進の具体的な作業を実施してきており、平成 22 年（2010 年）7 月には、送信ドメイン認証の普及により、なりすましメールの撲滅を目指す「なりすましメール撲滅宣言」、メールシステムの運用・管理者の参考となる「送信ドメイン認証導入マニュアル」が作成・公開されました。

平成 22 年（2010 年）夏以降、なりすましメール撲滅宣言に掲げる工程に基づき、電気通信事業者、広告事業者・金融機関・地方公共団体等メール送信を行っている主な会社・組織に対して、説明会やリーフレットの配布による、送信ドメイン認証技術の周知普及を進めています。

図 S-5　迷惑メール対策推進協議会における送信ドメイン認証技術の普及の取り組み

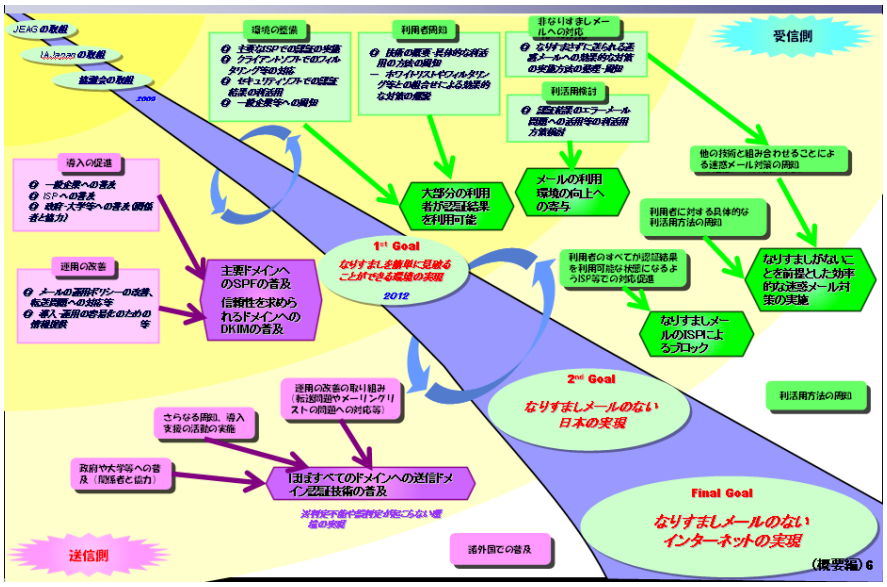
2　『なりすましメール撲滅宣言』の公表

迷惑メールは、送信者情報を詐称して送られてくることが多いことから、詐称を発見することができる送信ドメイン認証技術は、迷惑メール対策として期待されています。しかし、その効果をあげるためには、できるだけ多くのメールサーバで足並みをそろえて導入することが重要です。

このため、本協議会では、この技術を広く普及させ、理想的なメールの利用環境を整備するための工程を明確にするため、平成 22 年（2010 年）7 月、「なりすましメール撲滅プログラム」を作成・公表しました。

本プログラムでは、なりすましメールのない、理想的なメール環境の整備に向けては、関係者が送信ドメイン認証技術に対応し、なりすましメールを検知可能とすることにより、失われかねない電子メールの信頼性を取り戻していくことが期待されるとして、同技術を広く普及させるための工程を明らかにしています。具体的には、第一段階（2012 年度中）では、送信ドメイン認証技術により、受信側で、なりすましを容易に見破ることができる環境の実現を目指す、第二段階では、同技術により、我が国において、ドメイン単位でのなりすましメールがないインターネット環境の実現を目指す、最終段階では、全世界における、ドメイン単位でのなりすましメールがないインターネット環境の実現を目指すという目標を掲げるとともに、それぞれの目標の実現に向けた、送信側・受信側等の取組みを設定しています。

図表 S-6 なりすまし撲滅プログラムの概要



3『送信ドメイン認証技術導入マニュアル』の公表

送信ドメイン認証技術がその効果をあげるためには、導入に当たって、技術の詳細や、メールの利用環境や利用局面に応じて考慮すべきことなど、具体的な導入手順や内容について、正しく理解していただく必要があります。

このため、本協議会では、メールシステムの運用・管理者の方の参考となるよう、送信ドメイン認証技術の概要や、導入時に必要になる手順や内容をまとめた「送信ドメイン認証技術導入マニュアル」を平成 22 年（2010 年）7 月に作成・公表しました。さらに、平成 23 年（2011 年）7 月には改訂版を作成・公表しました。

図表 S-7　送信ドメイン認証技術導入マニュアル

4　企業・団体向け説明会等の実施

我が国の送信側での SPF/Sender ID の対応状況は約 4 割と一定の普及が図られているものの、約 6 割がいまだ SPF/Sender ID に対応しておらず、前述のように、実際にフィッシング等のなりすましの被害が発生している業種でも、送信ドメイン認証技術の普及はあまり進んでいないのが現状です。

そこで、本協議会では、「なりすましメール撲滅プログラム」の第一段階の目標（2012 年度中に、なりすましを容易に見破ることができる環境を実現）に向けて、平成 22 年（2010 年）夏以降、電気通信事業者や広告関係者など、本協議会の主要

な構成員の会員等に対する説明会を精力的に開催し、送信ドメイン認証技術の導入方法や課題への対応方法等について周知を図っています。

さらに、すべてのドメインに対応していただき、なりすましメールによるフィッシング被害などの根絶を図るべく、ドメイン名を詐称されることにより、信頼性に対する悪影響が大きいと考えられる自治体、金融機関等については、率先的に対応を推進していただくことが求められることから、業界団体等にご協力いただき、説明会やリーフレット配布等の活動を続けています。

図 S-8　企業・団体向け説明会等の実施状況

1　協議会関係

主催者等	期日	概要
社団法人日本広告業協会	2010/9/17	・インターネット広告小委員会で説明（約 10 名）
社団法人日本インターネットプロバイダー協会	2010/10/18	・地域 ISP 部会で説明(約 20 名)
一般社団法人モバイル・コンテンツ・フォーラム	2010/12/21	・会員向けセミナーで説明（約 50 名）
財団法人インターネット協会	2011/3/8	・電子メールセキュリティーセミナー in 熊本で紹介
社団法人日本広告業協会	2011/4/20	・　EDI 小委員会で説明（約 10 名）
違法・有害情報相談センター、通信4団体	2011/4/25 2011/4/26 2011/4/28	・事業者向けセミナーで説明 25 日：東京　26 日：名古屋 28 日：大阪

リーフレット配布

主催者等	期日	概要
全国消費者団体連絡会	2011/3/3	団体会合で会員に配布(50 部)
財団法人インターネット協会	2011/5/27	迷惑メール対策カンファレンスで配布(100 部)

2　協議会以外

主催者等	期日	概要
全国銀行協会	2010/11/8	・E コマース検討部会で説明（約 20 名）
社団法人全国地方銀行協会	2010/11/22	・EB関連業務部会で説明（約 20 名）
特別区情報システム勉強会	2011/2/25	・特別区情報システム勉強会で説明（約 30 名）
社団法人生命保険協会	2011/3/4	・情報システム部会で説明（約 50 名）
日本証券業協会	2011/4/5	・証券会社最高情報責任者（CIO）会議で説明（約 20 名）
社団法人日本クレジット協会	2011/7/21	・カード取引対応研究部会にて説明（約 30 名）

リーフレット配布

主催者等	期日	概要
財団法人地方自治情報センター	2011/1/26 ～2/28	・期間に開催された自治体向けセミナーにおいて、配布（330 部）

5　送信ドメイン認証技術の導入状況の調査・周知

前述のとおり、本協議会では、協議会の構成員や自治体、金融機関等の協議会以外の関係業種の業界団体等を通じて、送信ドメイン認証技術の周知・普及を図っていますが、当該業界団体等における進捗管理の参考となるよう、各業界ごとのSPF/Sender ID の導入状況を定期的に調査し、当該業界団体に周知しています。

具体的には、各業界団体等の構成員企業等の MX レコードを有するドメインを抽出し、四半期ごとに、各ドメインの SPF/Sender ID の導入の有無を調査し、各業界団体ごとの導入率等を当該団体にお知らせしています。

図 S-9 SPF/Sender ID の導入状況の業界団体等への周知例

○○協会会員のSPF宣言率

○○会員全体のSPF宣言率は、2011年4月の時点で ○○%（調査数○○○）。
なお、JPドメイン全体のSPF宣言率は、2011年2月の時点で 41.3% 。

	11/4	11/3	11/2	11/1	10/12	10/11	10/10	10/9	10/8	10/7	10/6
○○会員平均	○○%	○○%	○○%	○○%	○○%	○○%	○○%	○○%	○○%	○○%	○○%
CO.JPドメイン平均	-	-	48.5%	48.0%	47.8%	47.5%	47.3%	46.6%	46.0%	46.1%	45.8%
JPドメイン平均	-	-	41.3%	41.0%	40.8%	40.5%	40.3%	39.9%	39.6%	39.5%	39.3%

10/5	10/4	10/3	10/2	10/1	09/12	09/11	09/10	09/9	09/8	09/7	09/6	09/5
○○%	○○%	○○%	○○%	○○%	○○%	○○%	○○%	○○%	○○%	○○%	○○%	○○%
45.4%	45.2%	44.8%	44.5%	43.8%	43.6%	43.4%	43.2%	42.9%	42.7%	42.5%	42.3%	41.7%
38.8%	39.0%	38.7%	38.4%	37.7%	37.5%	37.2%	36.8%	36.6%	36.0%	35.7%	35.5%	34.8%

調査条件等

- 企業は、各団体のHPよりある時点で抽出したものを使用しているため、最新の情報と異なる場合がある
- ドメインは、原則各企業のトップドメインとしているため、実際のメール送信ドメインではない場合がある
- 調査は、DNSのnslookupコマンドで調べているが、手集計のため、誤集計している可能性がある
- 一部企業で、SPFの記述が間違っているものもあったが、フォーマットチェックはしていない
- 宣言済みとしているのは、"-all"、"~all" となっているもの（最新の数値で、1組織がSPFレコードの宣言はしているが、"?all"となっているため、未宣言として集計されている）
- 本データは、機密情報ではありませんが、このデータをこのまま外部に公開はしないで下さい。

第３節　協議会以外の組織による普及活動

1　政府

政府では、セキュリティ対策の年度計画を定める『セキュアジャパン 2008』以降、迷惑メール対策の一環として送信ドメイン認証技術の普及に取り組むことを定めています。

最新版の『情報セキュリティ 2011』では、「内閣官房及び全府省庁は、悪意の第三者が政府機関又は政府機関の職員に成りすまし、一般国民や民間企業等に害を及ぼすことが無いよう、SPF 等の送信ドメイン認証技術の採用等を推進していく」ことを定めており、政府をあげて、SPF 等の送信ドメイン認証技術の導入に積極的に取り組んでいます。

本協議会の調査によると、平成 23 年(2011 年) 4 月 1 日時点で、政府の各府省のドメイン(MX レコードが存在するドメイン)の送信側としての SPF/SenderID 導入率は 92.3%に達しています。また、WIDE プロジェクト及び JPRS が行っている調査結果においても、go.jp ドメインの SPF/SenderID 導入率は、2 年間で 10 ポイント以上の伸びを示しており、『情報セキュリティ 2011』等において、送信ドメイン認証技術の積極導入を図っている効果が顕著に現れてきています。

2　総務省

送信ドメイン認証技術や 25 番ポートブロックといった迷惑メール対策技術は、効果的な迷惑メール対策として実用化が図られてきたところですが、こういった技術の中には、その利用が電気通信事業法に規定されている通信の秘密の保護及び役務提供における差別的取扱いの禁止に抵触するおそれがあるものもあります。そこで、総務省では、こうした迷惑メール対策技術に関して、法的な整理を行い、迷惑メール対策技術の導入を促進しているところです。

具体的には、平成 18（2006 年）年 5 月に、『送信ドメイン認証及び 25 番ポートブロックに関する法的留意点』を作成し、総務省のサイトを通じて、公表しています。

本文書では、「送信ドメイン認証及び 25 番ポートブロックは、効果的迷惑メール対策として導入されているところ。他方、上記技術の利用は、電気通信事業法に規定されている通信の秘密の保護及び役務提供における差別的取扱いの禁止に抵触する。しかしながら、上記技術の利用は、いずれも正当業務行為として、違法性阻却事由が認められることから、その利用は適法なものと認められる。以上のように、上記技術は法的問題点についても整理できることから、ISP による上記技術の導入の促進が図られることが望ましい。」として、電気通信事業者における送信ドメイン認証技術の導入の際の懸念点に対応しています。

3　財団法人インターネット協会

財団法人インターネット協会では、平成 16 年（2004 年）9 月より、ISP、一般企業、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、迷惑メール対策活動を行っており、毎年開催している迷惑メール対策カンファレンスの中で、平成 17 年～19 年（2005 年～2007 年）、平成 21 年～23 年（2009 年～2011 年）に、送信ドメイン認証技術の普及を議題としています。

また、メール管理者等向けに、解説資料を作成し、公表しています。

図表 S-10 迷惑メール対策カンファレンス

4　財団法人地方自治情報センター

財団法人地方自治情報センター(LASDEC)では、地方公共団体の情報セキュリティ対策支援事業を行っており、その一環として、自治体向けのメールマガジン等により、送信ドメイン認証技術の周知啓発を図っています。

5　財団法人日本データ通信協会

財団法人日本データ通信協会では、平成 21 年（2009 年）5 月以降、主要な ISP 等における送信ドメイン認証技術の送信側・受信側の対応状況について調査し、その結果をウェブページで公表してきています。

図 S-11 （財）日本データ通信協会による、ＩＳＰの送信ドメイン認証技術の対応状況の公表

ISPの送信ドメイン認証実装状況		送信時実装※1,2		受信時実装※3			
No.	事業者名	SPF/ SenderID	DKIM/ domainKeys	SPF/ SenderID		DKIM/ domainKeys	
				ラベリング	フィルタリング	ラベリング	フィルタリング
1	KDDI株式会社	☆	—	○	—	—	—
2	KMN株式会社	☆	—	—	—	—	—
3	NECビッグローブ株式会社	☆	—	◎	—	◎	—
4	NTTコミュニケーションズ株式会社	☆	—	○	—	—	—
5	株式会社NTTデータ三洋システム	☆	—	—	—	—	—
6	株式会社NTTぷらら	☆	—	—	—	—	—
7	株式会社STNet	☆	—	○	—	—	—
8	株式会社TOKAI	☆	—	—	—	—	—
9	株式会社アイエフネット	☆	—	○	—	—	—
10	イッツ・コミュニケーションズ株式会社	☆	—	—	—	—	—
11	株式会社インターネットイニシアティブ	☆	☆	◎	☆	◎	—
12	株式会社エヌ・ティ・ティ エムイー	☆	—	—	—	—	—
13	株式会社エヌ・ティ・ティ・ドコモ	☆	—	—	—	—	—
14	おりべネットワーク株式会社	☆	—	—	—	—	—
15	株式会社キャッチネットワーク	☆	—	—	—	—	—
16	株式会社ケイ・オプティコム	☆	—	—	—	—	—
17	株式会社コアラ	☆	—	—	—	—	—
18	シーシーエヌ株式会社	☆	—	—	—	—	—
19	ジェットインターネット株式会社	☆	—	○	☆	—	—
20	ヤフー株式会社 ソフトバンクBB株式会社	☆	☆	○	☆	◎	☆
21	ソフトバンクテレコム株式会社	☆	—	—	—	—	—
22	株式会社つなぐネットコミュニケーションズ	☆	—	—	—	—	—
23	株式会社テクノロジーネットワークス	☆	—	—	—	—	—
24	トナミ運輸株式会社	☆	—	—	—	—	—
25	株式会社ドリーム・トレイン・インターネット	☆	—	—	—	—	—
26	ニフティ株式会社	☆	☆	◎	—	◎	—
27	株式会社ハイネット	☆	—	—	—	—	—
28	株式会社ハイホー	☆	—	—	—	—	—
29	ひまわりネットワーク株式会社	☆	—	—	—	—	—
30	関西マルチメディアサービス株式会社	☆	—	—	—	—	—
31	九州通信ネットワーク株式会社	☆	—	—	—	—	—
32	株式会社 佐遊テレビジョン	☆	—	○	—	—	—
33	三河湾ネットワーク株式会社	☆	—	—	—	—	—
34	知多メディアスネットワーク株式会社	☆	—	—	—	—	—
35	中部ケーブルネットワーク株式会社	☆	—	◎	—	◎	—
36	飯能ケーブルテレビ株式会社	☆	—	—	—	—	—

携帯・PHS事業者		送信時実装※1,2		受信時実装※3	
No.	事業社名	SPF/ SenderID	DKIM/ DomainKeys	SPF/ SenderID	DKIM/ DomainKeys
37	KDDI株式会社	☆	—	◎	—
38	株式会社エヌ・ティ・ティ・ドコモ	☆	—	◎	—
39	ソフトバンクモバイル株式会社	☆	—	—	—
40	株式会社ウィルコム	☆	—	—	—

フリーメール		送信時実装※1,2		受信時実装※3			
No.	事業者名	SPF/ SenderID	DKIM/ domainKeys	SPF/SenderID		DKIM/domainKeys	
				ラベリング	フィルタリング	ラベリング	フィルタリング
41	Google株式会社	☆	☆	◎		◎	
42	NTTレゾナント株式会社	☆	—	○	—	○	—
43	株式会社ライブドア	☆	—	◎	—	—	—
44	Microsoft Corp	☆	—	○	—	—	—
45	ヤフー株式会社	☆	☆	○	☆	◎	☆

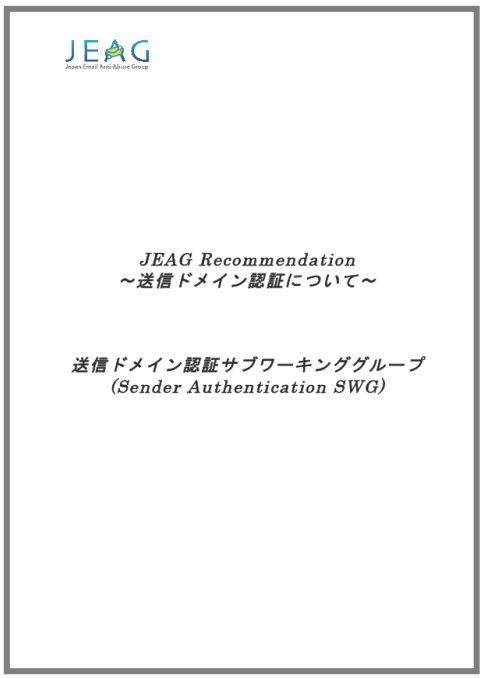
※1 送信時実装はいずれかの方式により実施されている場合に"☆"と表示しています。
※2 送信時SPF実装については、限定子が"-all"、"~all"のものを実装としています。
※3 受信時実装は、ラベリングをAuthentication-Resultsヘッダにしている場合を"◎"、Received-SPFヘッダにしている場合を"○"、フィルタリングサービスについては、いずれかの方式により実施されている場合に"☆"と表示しています。

6　JEAG

JEAG（Japan Email Anti-abuse Group）は、インターネットサービスプロバイダーやベンダーがビジネスの枠を超えて、迷惑メール根絶のための取り組みを行う目的で、平成 17 年（2005 年）3 月に設立され、現在 30 社が加盟しています。

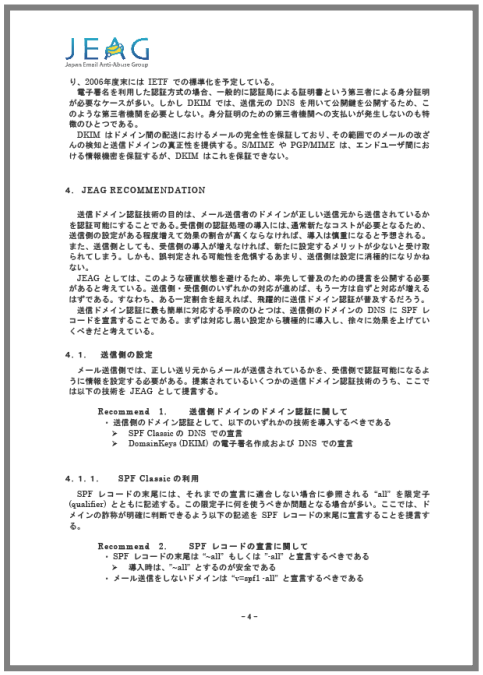
JEAG では、平成 18 年（2006 年）2 月の送信ドメイン認証技術に関するレコメンデーションの作成・発表、各所での講演活動の実施など、送信ドメイン認証技術の普及のための取り組みを実施してきています。

図 S-12 JEAG 送信ドメイン認証技術に関するレコメンデーション


JEAG

JEAG Recommendation
～送信ドメイン認証について～

送信ドメイン認証サブワーキンググループ
(Sender Authentication SWG)


JEAG

り、2006年度末には IETF での標準化を予定している。
電子署名を利用した認証方式の場合、一般的に認証局による証明書という第三者による身分証明が必要なケースが多い。しかし DKIM では、送信元の DNS を用いて公開鍵を公開するため、このような第三者機関を必要としない。身分証明のための第三者機関への支払いが発生しないのも特徴のひとつである。
DKIM はドメイン間の配送におけるメールの完全性を保証しており、その範囲でのメールの改ざんの検知と送信ドメインの真正性を提供する。S/MIME や PGP/MIME は、エンドユーザ間における情報機密を保証するが、DKIM はこれを保証できない。

4. JEAG RECOMMENDATION

送信ドメイン認証技術の目的は、メール送信者のドメインが正しい送信元から送信されているかを認証可能にすることである。受信側の認証処理の導入には、通常新たなコストが必要となるため、送信側の設定がある程度増えて効果の割合が高くならなければ、導入は慎重になると予想される。また、送信側としても、受信側の導入が増えなければ、新たに設定するメリットが少ないと受け取られてしまう。しかも、誤判定される可能性を危惧するあまり、送信側は設定に消極的になりかねない。
JEAG としては、このような硬直状態を避けるため、率先して普及のための提言を公開する必要があると考えている。送信側・受信側のいずれかの対応が進めば、もう一方は自ずと対応が増えるはずである。すなわち、ある一定割合を超えれば、飛躍的に送信ドメイン認証が普及するだろう。
送信ドメイン認証に最も簡単に対応する手段のひとつは、送信側のドメインの DNS に SPF レコードを宣言することである。まずは対応し易い設定から積極的に導入し、徐々に効果を上げていくべきだと考えている。

4.1.　送信側の設定

メール送信側では、正しい送り元からメールが送信されているかを、受信側で認証可能になるように情報を設定する必要がある。提案されているいくつかの送信ドメイン認証技術のうち、ここでは以下の技術を JEAG として提言する。

Recommend 1.　送信側ドメインのドメイン認証に関して
・送信側のドメイン認証として、以下のいずれかの技術を導入するべきである
➢ SPF Classic の DNS での宣言
➢ DomainKeys (DKIM) の電子署名作成および DNS での宣言

4.1.1.　SPF Classic の利用

SPF レコードの末尾には、それまでの宣言に適合しない場合に参照される "all" を限定子 (qualifier) とともに記述する。この限定子に何を使うべきか問題となる場合が多い。ここでは、ドメインの詐称が明確に判断できるよう以下の記述を SPF レコードの末尾に宣言することを提言する。

Recommend 2.　SPF レコードの宣言に関して
・SPF レコードの末尾は "~all" もしくは "-all" と宣言するべきである
➢ 導入時は、"~all" とするのが安全である
・メール送信をしないドメインは "v=spf1 -all" と宣言するべきである

-4-

7　フィッシング対策協議会

フィッシング対策協議会は、平成 17 年（2005 年）4 月に発足され、海外、特に米国を中心として大きな被害を生んでいるフィッシング詐欺に関する事例情報、技術情報の収集及び提供を中心に行うことで、日本国内におけるフィッシング詐欺被害の抑制を目的として活動しています。

同協議会では、平成 20 年（2008 年）9 月に作成された「フィッシング対策ガイドライン」の中で、送信ドメイン認証技術を紹介しているほか、セミナー等で、同技術に関する講演等を行っています。

8　WIDE・JPRS

WIDE プロジェクト及び JPRS では、共同して、平成 17 年（2005 年）4 月以降、我が国のドメインでの送信ドメイン認証技術の送信側の DNS への設定状況を毎月公表してきています。

9 dkim.jp

dkim.jp(Japan DKIM Working Group)は、迷惑メール対策のドメイン認証技術「DKIM」の国内における普及を推進することを目的として、平成 22 年(2010 年)11 月に設立され、現在メンバー 32 社、協力団体/オブザーバ 5 団体が加盟しています。

dkim.jp では、平成 23 年(2011 年)5 月に「送信事業者における DKIM 導入・運用について」のレコメンデーションの発表など DKIM の啓発・普及を推し進めています。

10 電気通信事業者

インターネットサービスプロバイダー、携帯電話事業者等の多くが既に、送信側については、SPF/SenderID に対応しています。また、一部の事業者では、DKIM への対応が始まっています。

受信側では、SPF/SenderID については、フィルタリングサービスを提供しているインターネットサービスプロバイダーはまだ少ないものの、ラベリングへの対応は進んできています。また、携帯電話事業者においては、大手 2 事業者が、フィルタリングサービスを提供しており、なりすましメールの受信拒否に大きな効果をあげています。また、携帯電話事業者による、フィルタリングサー

ビスの開始に伴い、送信側での SPF/Sender ID への　　す。
対応が急速に進んだことが見受けられるところで

図 S-13 携帯電話事業者による送信ドメイン認証技術を用いた迷惑メールフィルター

出典：KDDI ホームページ（http://www.au.kddi.com/service/email/support/meiwaku/email_boshi/filter/narisumashi/index.html）

第 4 節　利用者への周知啓発

1　協議会による周知

迷惑メール対策協議会では、企業・団体等の送信側、一般利用者等の受信側ともに、送信ドメイン認証技術に対する認知度が高くない一方、同技術の導入・活用により、送信側ではフィッシング被害等のなりすまし防止、受信側ではなりすましメールの受信拒否等に大きな効果があげられることから、同技術の周知を積極的に行っています。

具体的には、平成 22 年度（2010 年度）においては、送信側企業、一般利用者双方が送信ドメイン認証技術の必要性・仕組み・導入活用方法等について、分かりやすくご理解いただけるよう、リーフレット(「電子メールのなりすまし対策ー送信ドメイン認証技術でなりすましを防ぐー」)を作成し、各種イベント等で配布するとともに、協議会のサイトに掲載しています。

図表 S-14 送信ドメイン認証技術の周知用リーフレット

2　電気通信事業者による周知

前述のように、一部の携帯電話事業者やインターネットサービスプロバイダーでは、送信ドメイン認証技術（SPF/Sender ID）を利用したフィルタリングサービスの提供を開始しています。

電気通信事業者において、迷惑メール対策、なりすましメール対策として、このようなフィルタリングサービスの一層の周知が期待されます。

MEMO

第1章
迷惑メールとは

第１章　迷惑メールとは

第１節　迷惑メールの定義

１　迷惑メールの問題

現在、電子メールは、コミュニケーションツールとして社会経済活動や市民生活において必要不可欠な連絡・伝達の手段となっています。その一方で、電子メールの利用の飛躍的な増大とともに、いわゆる迷惑メールも依然として減少したとはいえない状況であり、利用者の送受信上の支障や、電子メールの伝送サービスを提供する事業者の設備への負荷は過大なものとなっています。

２　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。

まず、「メール」については、「電子メール」であって、郵送される手紙や、ブログへの迷惑コメントなどは含まれません。「電子メール」にも、SMTP（Simple Mail Transfer Protocol。）と呼ばれる通信方式を使ったインターネットのメール（ウェブメールなど通信の一部において SMTP を用いるものもあります。）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様々なものがあります。

また、「迷惑」についても、様々な形の「迷惑」が考えられます。例えば、友人からのメールであっても、時間帯によっては「迷惑」となることもあり得ますが、それは「迷惑メール」の問題とは違います。

社会的な問題となるような「迷惑」なメールとしては、次のような特徴が考えられます。これらの特徴については、通常の電子メールでも当てはまるものもありますが、一般的に「迷惑メール」といわれているものの多くは、これらの特徴の複数が当てはまります。

(1) 同意の有無
- ・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

(2) 内容
- ・ウイルスなどのマルウェア感染を目的とするもの
- ・詐欺目的のもの（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、架空請求メール等）
- ・有害情報を含むもの（違法な商品の広告・宣伝や、受信者の年齢等を考慮せずに行われる出会い系・アダルト系等の広告・宣伝等）
- ・個人情報を不正に取得する目的で送信されるもの
- ・チェーンメール

(3) 送信形態
- ・宛先に架空電子メールアドレス（プログラムによって作成された、利用者の存在しないアドレス）を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
- ・既に利用されていないアドレスが宛先の大部分を占めるように送信されるもの
- ・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
- ・携帯電話を宛先とし時間帯を考慮せず無差別に送信されるもの
- ・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）

(4) その他
- ・アドレスの存在確認等を目的として送信される空メール
- ・送信元アドレスが詐称された送信で、詐称されたアドレス宛に送信されてしまうエラーメール（詐称された送信元に対してエラーメールが大量に到達してしまうもの。）
- ・エラーメールを悪用した送信（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）

３　法律の対象となる「迷惑メール」

我が国では、「迷惑メール」について、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。）及び特定商取引に関する法律（特定商取引法。）による規制が行われています。特定電子メール法・特定商取引法では、それぞれ次のような電子メールを対象としています（２で記載した「迷惑メール」のうち広告・宣伝目的ではないもの等は法規制の対象となっていない一方で、受信者が送信に同意している広告・宣伝メールも法規制の対象になっているなどの違いがありますので、両法の対象となる電子メールについては、正確には、それぞれの法律の規定をご確認下さい。）。

特定電子メール法：営利の主体が受信者の同意等なく送信する広告・宣伝の電子メール（SMTP のほか、SMS も含む。）

特定商取引法：通信販売等で事前の承諾等なく

個人に対して送信する電子メール広告（SMTP のほか、SMS も含む。）

また、例えば、詐欺目的のメールを送信し、受信者から金品をだまし取ると刑法上の詐欺罪に該当するなど、迷惑メールに関して、迷惑メールに特化した規定がある法律以外の法律違反となることもあります。どのような「迷惑メール」が法律違反となるかについては、それぞれの法律により異なります。

４　このハンドブックで扱う迷惑メール

このように、いわゆる「迷惑メール」は様々なものがありますが、このハンドブックでは、特定電子メール法・特定商取引法で禁止される電子メールを中心としつつ、それに限らず、２で述べたような特徴を持ち、一般的に「迷惑」とされ、社会的に問題となっているものも想定して、「迷惑メール」として扱います。

Topics：電子メールの仕組み

1　配送の仕組み

電子メールの送受信の仕組みは、郵便物に似ています。
郵便物がA市の太郎さんからB市の花子さんに送られる場合には、以下のように配達されます。

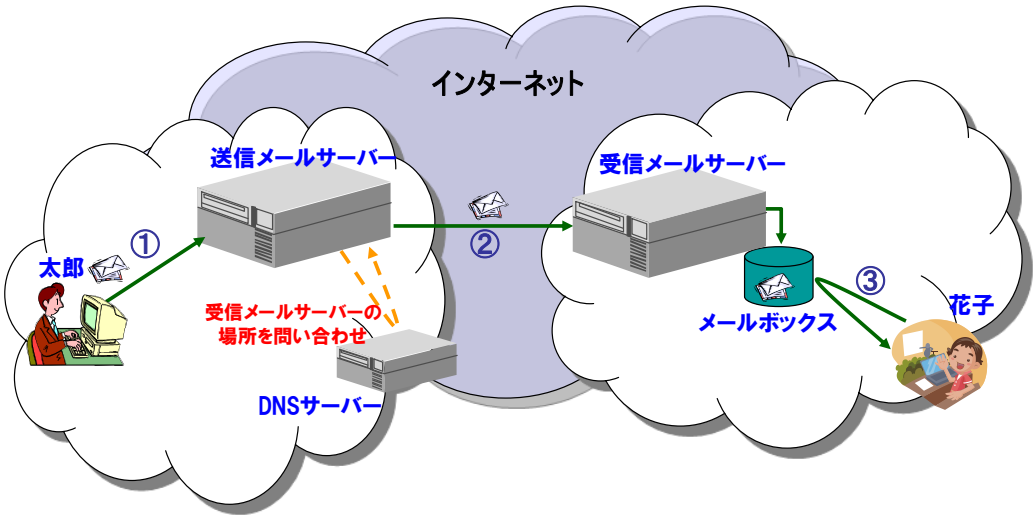
① ポストに投函された郵便物がA市の郵便局（正確には、郵便事業会社の集配センター）に配送される
② A市の郵便局からB市の郵便局に配送される
③ B市の郵便局から花子さんの住所に配達される

図表１：郵便物の配達

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

① 電子メールが送信メールサーバーに投稿される
② 投稿された電子メールが受信メールサーバーに配送され※、受信者のメールボックスに保存される
※　このとき、送信メールサーバーが、あて先の受信メールサーバーがどこにあるかを DNS サーバー（Domain Name System サーバー：それぞれネットワーク管理者が、サーバーの位置情報などを登録しているサーバー）に問い合わせます。郵便の場合は、郵便局が住所を統一的に把握していますが、インターネットの世界では、ネットワークの各部分が独立に管理されており、自らが管理していないネットワーク内に存在するサーバーの位置情報は保有していません。このため、DNS サーバーに対して問い合わせを行う必要があります。
③ 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

図表２：電子メールの配送



2　あて先の仕組み

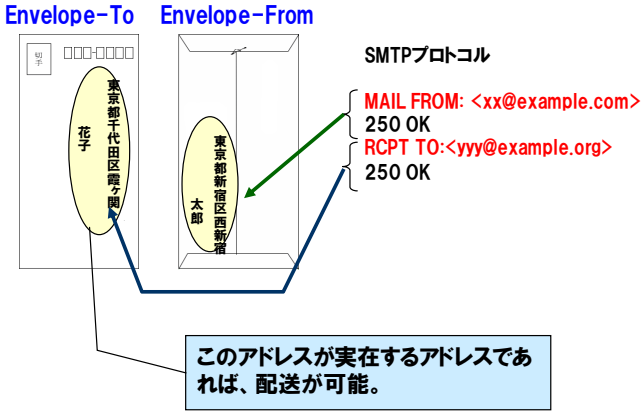
封書の場合に、封筒と便箋にあて先や差出人を書くように、電子メールにおいても、封筒に書かれたあて先や差出人にあたる情報と、便箋に書かれたあて先や差出人にあたる情報があります。

封筒に書かれたあて先にあたる情報を「Envelope-To」と言い、封筒に書かれた差出人にあたる情報を「Envelope-From」と言います（なお、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（RFC について、）では、それぞれ、「forward path」、「reverse path」とされています。）。また、便箋に書かれたあて先にあたる情報を「Header-To」と言い、便箋に書かれた差出人にあたる情報を「Header-From」といいます。

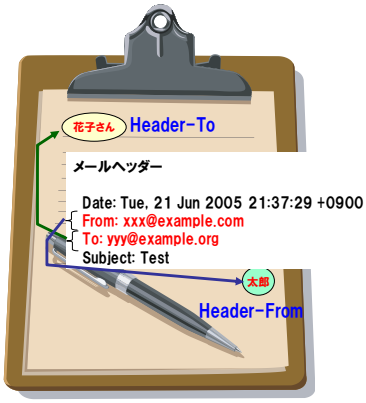
通常は、Header-To や Header-From として記載された電子メールアドレスが受信者のパソコンなどの受信画面に表示されます。Envelope-To や Envelope-From は、メールサーバ間の通信において用いられるものであり、郵便の場合と違って、受信者に届けられることはなく、通常は、送信者が目にすることもありません。

なお、この両者の違いは、送信ドメイン認証技術で重要になりますので、第４章の用語解説「配送上の送信者情報とメールヘッダー上の送信者情報」で、より詳しく解説します。

図表３：**Envelope-To** と **Envelope-From**



図表４：**Header-To** と **Header-From**



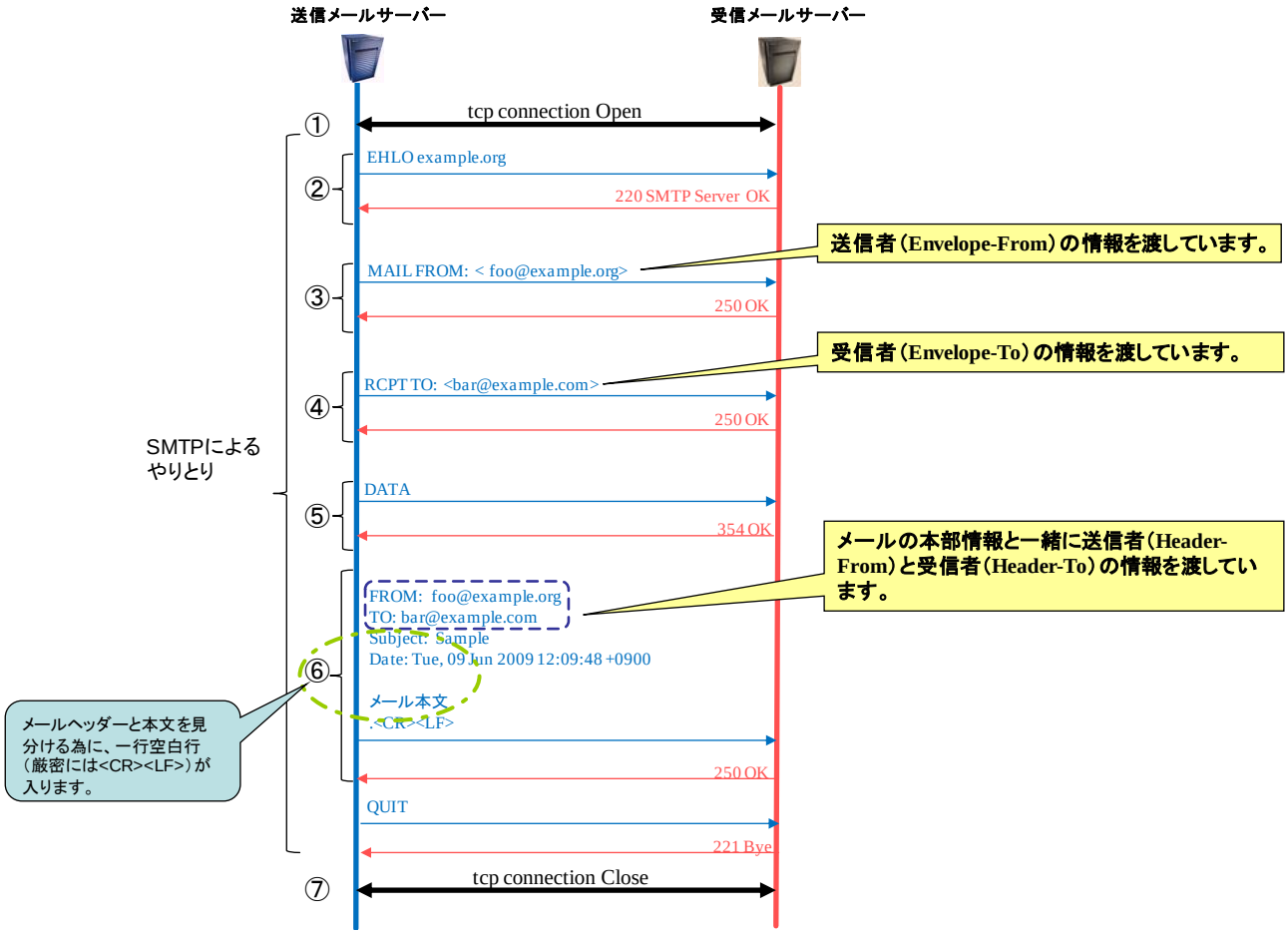
郵便物は、封筒に書かれた住所が実在するものであれば、誰から投函されたものであっても、また、便箋に書かれた情報がどんなものであっても、あて先に配達されます。電子メールについてもこの点は同じであり、Envelope-To が実在する電子メールアドレスであれば、通常は、その電子メールアドレスに配送されます。Header-To と Envelope-To、Header-From と Envelope-From には、それぞれ同じ電子メールアドレスが記載されるのが一般的ですが、BCC での送信やメールマガジンの配信など、そうではない場合もあります。さらに、Header-From と Envelope-From などの情報を偽って記述することも可能です。悪質な送信者によって、差出人を偽装した迷惑メールが送信されることがあるのはこのためです。

3　電子メール送受信のプロトコル

送信メールサーバーと受信メールサーバーの間での通信は、以下のような決まり（プロトコル）で行われています。

①送信メールサーバーと受信メールサーバーの間で、電子メールの通信を行うための接続が確立されます。
②インターネットで用いられる通信プロトコルのうち、電子メールの配送に用いられる SMTP による通信が開始されます。②から⑥までの過程が、SMTP による通信です。）
③送信メールサーバーから、送信者についての情報として、「Envelope-From」に記述された情報が受信メールサーバーに渡されます。
④送信メールサーバーから、受信者についての情報として、「Envelope-To」に記述された情報が受信メールサーバーに渡されます。複数の宛先に送信を行う場合は、このやりとりを繰り返すことになります。
⑤送信メールサーバーから受信メールサーバーに対し、次に送る内容が、Header に記述された情報やメール本文であることを伝えています。
⑥送信メールサーバーから、Header に記述された情報やメール本文を受信メールサーバーに渡しています。受信者が見ることができるのは、このときに渡される情報です。
⑦送信メールサーバーと受信メールサーバーの間での通信が終了します。

図表５：送信メールサーバーと受信メールサーバーの間での通信



第２節　迷惑メールの歴史

１　散発的な広告・宣伝メール

迷惑メールの歴史は古く、世界最初の迷惑メールは、Digital Equipment Corporation（DEC）（現HP）が、昭和53年(1978年)5月3日に製品発表会の案内を送信したものと言われており、インターネットの商用利用が可能となった平成5年（1993年）以前から、受信者による同意を得ないで送られる広告・宣伝メールがありました。また、パソコン通信でも、同様の広告・宣伝メールの送信が行われていました。

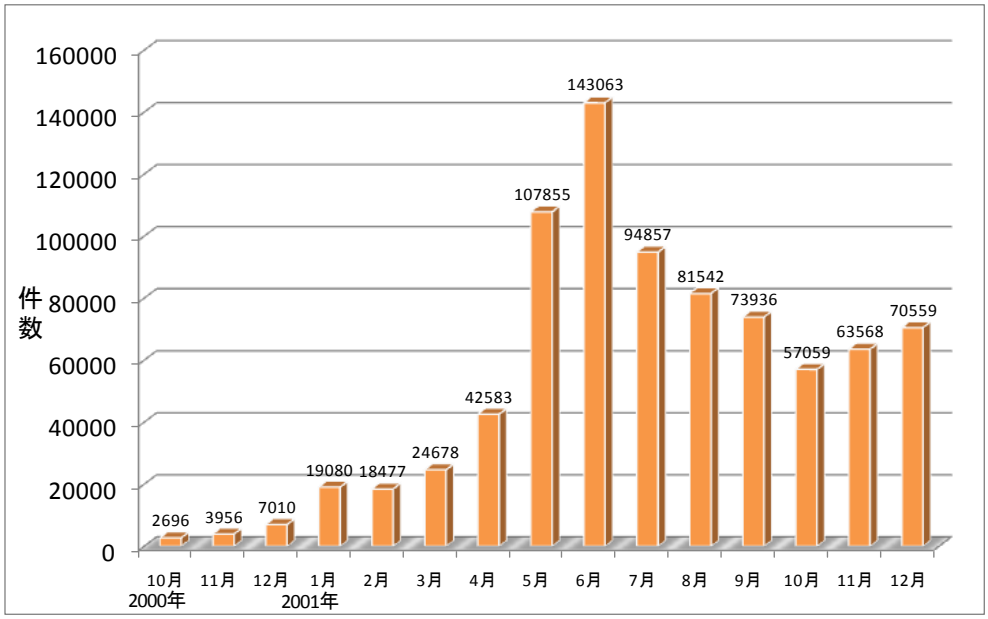
しかし、ブロードバンドが普及する以前は、通信速度が遅かったことやメール送信にも一定のコストがかかったこともあり、社会問題となるほど大量に送信され、問題となることはありませんでした。

２　迷惑メールの増加

平成12年（2000年）頃からADSL（Asymmetric Digital Subscriber Line）の利用が拡大したことに伴い、我が国における通信回線のブロードバンド化が進むとともに、パソコンのオペレーティングシステム（OS）が高度化し、誰もが容易にインターネットを利用できる環境が整いました。それに伴い、手軽に大量の電子メールを送信できるようになりました。また、携帯の世界では、平成11年（1999年）にインターネット接続可能なパケット通信サービス（NTTドコモによるｉモード）が開始され、その後、各社から同様のサービスが提供されるようになり、携帯電話による電子メールがより身近なものになりました。

その結果、広告・宣伝の手段として迷惑メールが大量に送信されるようになり、特に、平成13年（2001年）春頃から、携帯電話宛の迷惑メールが社会問題化しました。具体的には、機械的に作成したランダムな電子メールアドレスに宛てて広告・宣伝メールが大量に送信されることにより正常なメールに大幅な遅延が生じたり、パケット定額制が提供されていなかったため、迷惑メールの受信にも上限がなくパケット代がかかったり、昼夜の時間を問わずに広告・宣伝メールが送信されてきたりしました。

図表１－１：携帯電話利用者からの苦情・相談件数の月例推移



携帯電話・PHSを利用した電子メールサービスを提供する関連６グループ（ＮＴＴドコモ、ＫＤＤＩ株式会社、ジェイフォン株式会社、アステル、ツーカー、ＤＤＩポケット）についての集計（なお、数値については、集計当時のものであり、会社によっては、その後異なる集計基準の数値を公表しているところもある）

出典：総務省第１次迷惑メール研究会中間とりまとめ（平成14年（2002年）１月）

3　国内発から海外発へ

このような状況に対応し、我が国では、世界に先駆けて、平成 14 年（2002 年）7 月に、迷惑メール対策のための法律が整備されました（特定電子メール法及び特定商取引法）。また、携帯電話事業者やサービスプロバイダーにより、様々な迷惑メール対策のための措置が実施されました。

その結果、平成 18 年（2006 年）頃には、我が国着の迷惑メールのうち、国内発のものの割合は減少し、大部分は海外から送信されるようになりました。特に、海外から送信される迷惑メールは、ウイルス感染した個人のパソコン（ボット）を利用して送信されるものが多いと言われています。

Topics：迷惑メールに関する裁判例

迷惑メールについての裁判例としては、次のようなものがあります。

(1)ニフティサーブ・スパムメール送信差止め事件（浦和地決 H11.3.9）判例タイムズ 1023 号 272 頁

【事案の概要】
パソコン通信のニフティサーブ（当時）の不特定多数の会員に対し、わいせつビデオ販売を内容とする電子メールを継続的に送信した者に対し、ニフティサーブを運営していたニフティ株式会社が、同社が有する権利（社会的信用を維持する権利・メールサービス提供のためにサーバーを常に良好な状態に保つ権利）を理由に、同社会員に対する当該電子メールの送信の差止めの仮処分を申し立てた事案。
【決定の概要】
認容（ニフティサーブの会員に対し、わいせつビデオ販売を内容とする電子メールの送信をしてはならない。）。

(2)NTT ドコモ仮処分事件（横浜地決 H13.10.29）判例時報 1765 号 18 頁

【事案の概要】
NTT ドコモの i モードアドレス（当時は、「電話番号@docomo.ne.jp」であった）宛てに、ランダムな数字を当てはめる方法で、大量・継続的に、いわゆる出会い系サイトの広告・宣伝メールを送信した者に対し、NTT ドコモが、電気通信設備への所有権侵害（機能障害）を理由に、送信行為の差止めの仮処分を申し立てた事案。
【決定の概要】
認容（決定送達の日から 1 年間、ランダムな数字を当てはめる等の方法で、存在しない多数の電子メールアドレス宛に、営利目的の電子メールを送信する等して、電気通信設備の機能の低下・停止をもたらす行為をしてはならない。）。

(3)NTT ドコモ損害賠償請求事件（東京地判 H15.3.25）判例時報 1831 号 132 頁

【事案の概要】
「特定接続サービス（迷惑メールを防止するための一定の措置を採り、一定の利用料を支払うことを条件に、専用の接続口から円滑かつ確実に i モード利用者宛に電子メール送信を可能とするサービス）」を利用し、契約の条件に違反して、大量の宛先不明メールの送信をした者に対し、NTT ドコモが、債務不履行として、電気通信設備の使用料相当額（宛先不明により請求できなかった通信料）等 656 万 7,020 円の損害賠償請求を行った事案。
【判決の概要】
認容。

第2章
迷惑メールの現状

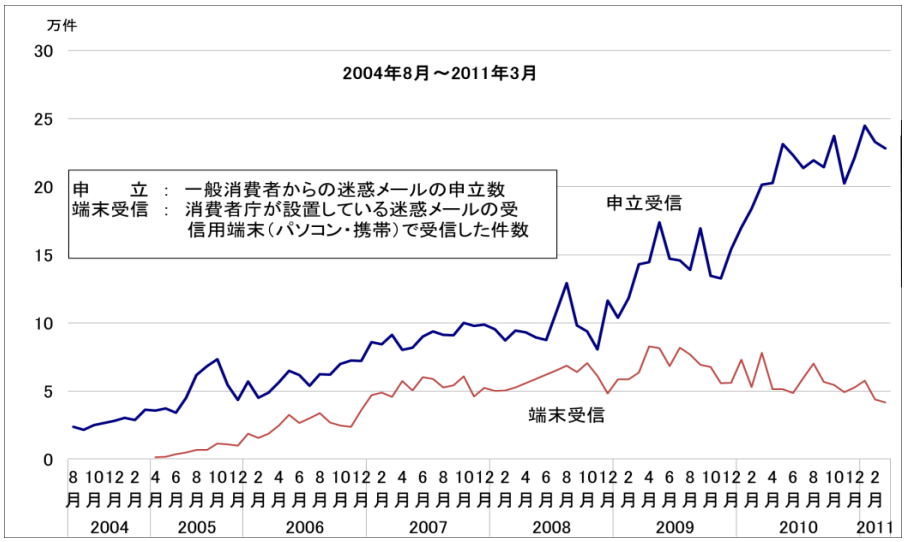
第２章　迷惑メールの現状

第１節　量的傾向

１　全体的傾向

我が国では、迷惑メールが社会問題になった後、様々な関係者により、様々な迷惑メール対策が講じられてきています。しかし、依然として、全体的に見ると、迷惑メールの数量が減少したとはいえない状況にあります。迷惑メールとして一般消費者からの申立てがあった数や、モニター機での受信数などを見ても、時期的変動はあるものの、現在に至るまで、依然として、高水準にあることがわかります。

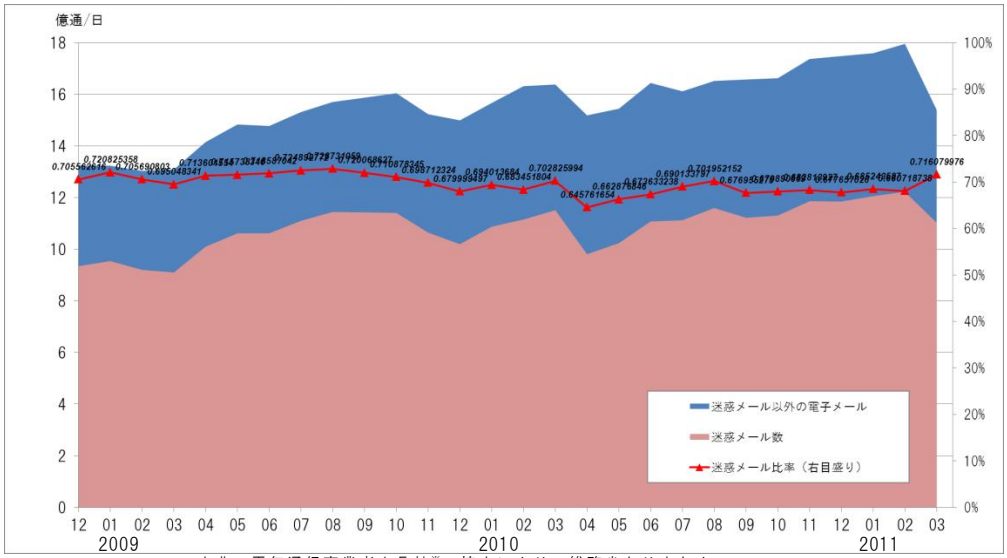
図表２－１：迷惑メールに係る申立数等



出典：消費者庁調べ

また、国内のインターネットサービスプロバイダー（Internet Service Provider：ISP）の取り扱う電子メールのうち迷惑メールの占める割合は、７割を超える状況となっています。このうちのかなりの部分は電気通信事業者のフィルター等で対応され、利用者には届いていません。しかし、利用者に届かないものも含め、迷惑メールが全メールの過半数を占め、ネットワークに対する負荷が非常に大きくなっていることが分かります。

図表２－２：国内 **ISP** における迷惑メール数・割合の推移

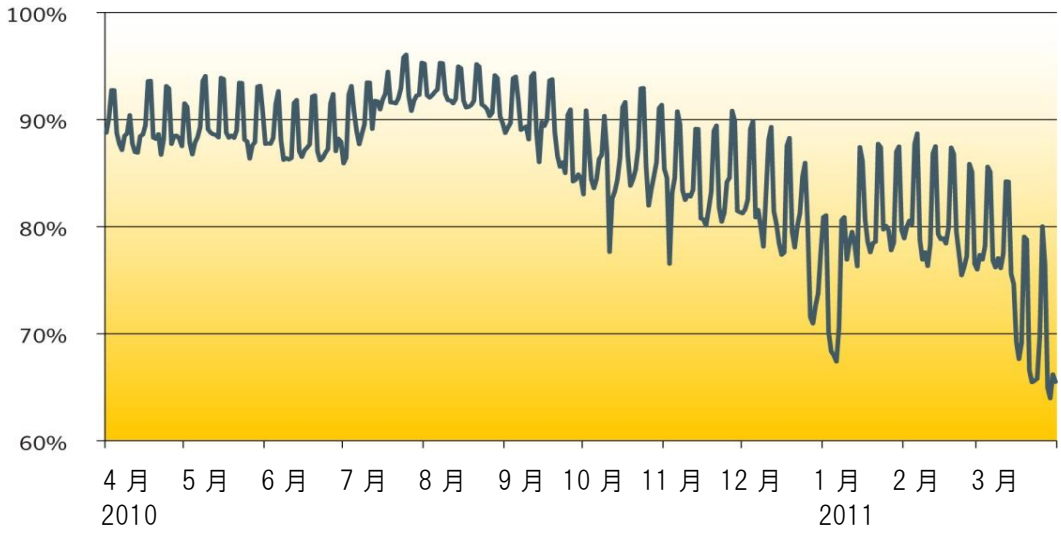


出典：電気通信事業者１５社※の協力により、総務省とりまとめ

※ KDDI 株式会社、NEC ビッグローブ株式会社、株式会社ＮＴＴぷらら、イー・モバイル株式会社、株式会社インターネットイニシアティブ、株式会社ウィルコム、エヌ・ティ・ティ・コミュニケーションズ株式会社、関西マルチメディアサービス株式会社、株式会社ケイ・オプティコム、ソネットエンタテインメント株式会社、ソフトバンクテレコム株式会社、ソフトバンクモバイル株式会社、株式会社テクノロジーネットワークス、ニフティ株式会社、ヤフー株式会社

なお、海外における迷惑メールの割合は、2010年前半まで 90%という高い水準で推移していましたが、年末年始と今年３月に大幅に低下しております。これは迷惑メールを大量に送信していたRustock と呼ばれるボットネットが活動を停止したためと思われます。3 月は 70%台で推移しています。しかしながら、依然として高い割合で推移している事実には変わりありません。

図表２－３：海外における迷惑メールの割合

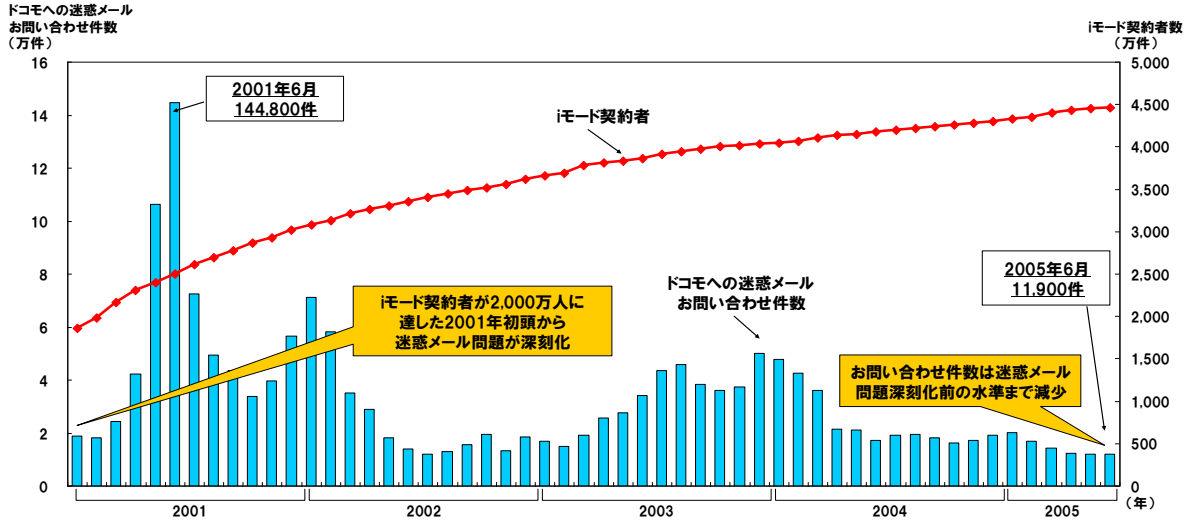


出典：シマンテック　スパム＆フィッシングマンスリーレポート　2011 年 4 月（株式会社シマンテック）より

２　携帯電話宛ての迷惑メール

その一方で、携帯電話の利用者からの問合せ件数が減少してきているなど、利用者から見た携帯電話宛の迷惑メールについては、これまでの携帯電話事業者の取り組みや、利用者側におけるフィルタリングサービスの活用等の結果として、一定の成果が上がってきているものと考えられます。

図表２－４：携帯電話会社への問合せ件数の推移



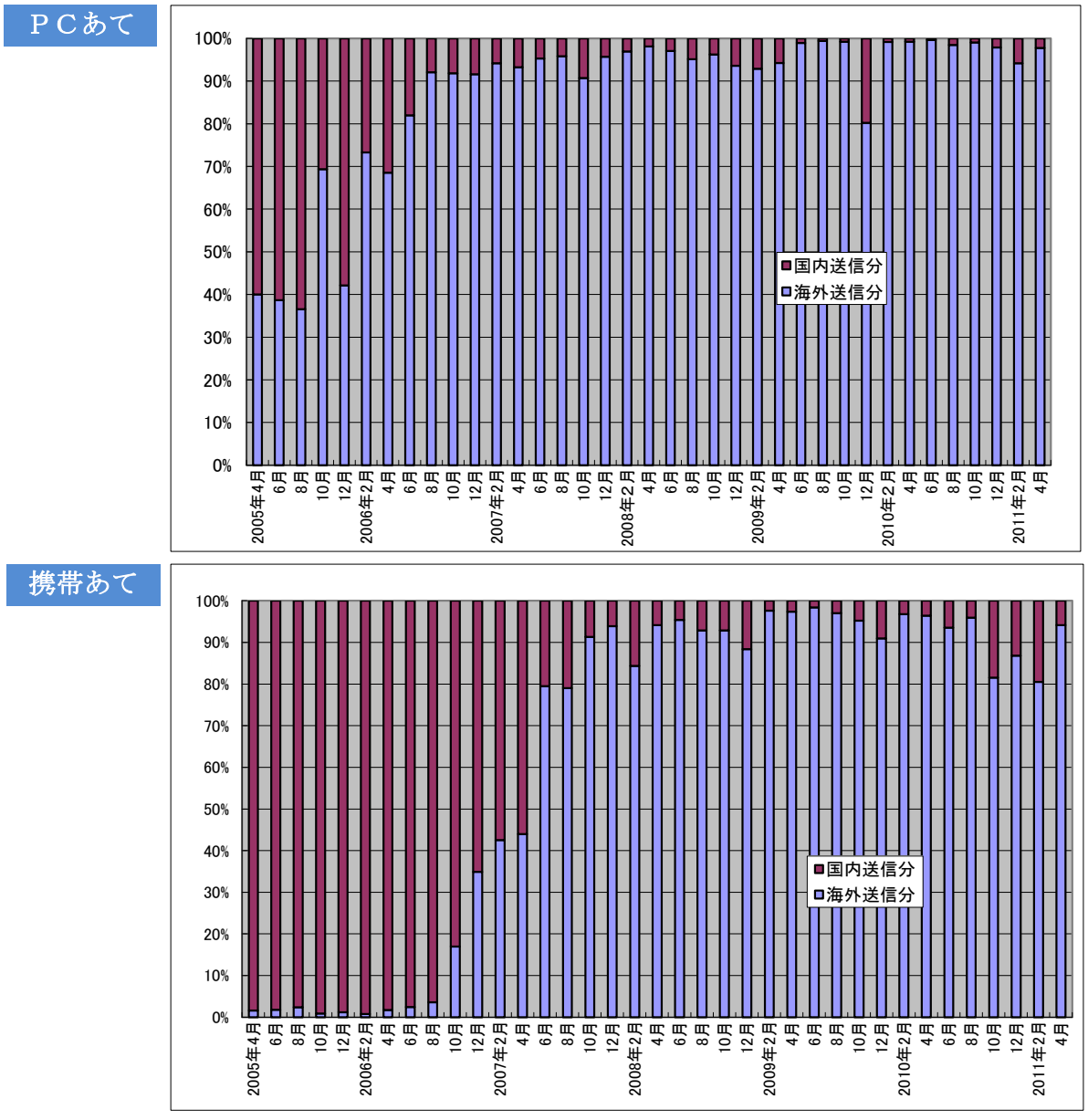
出典： NTT ドコモレポート No.29（2005/8/8）より
http://www.nttdocomo.co.jp/binary/pdf/info/news_release/report/050808.pdf

3　国内発の迷惑メール

また、パソコン宛て、携帯電話宛てともに、国内着の迷惑メールについては、国内発のものの占める割合は減少しており、最近では、9 割以上が海外発のものとなっているという統計もあります。

これは、我が国では、行政による法執行や電気通信事業者による技術的な対策など、関係者による対策が一定の成果を上げてきていることも一因と考えられます。

図表２－５：国内発・海外発の比率の推移



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

Topics：迷惑メールによる影響

1　迷惑メールが日本経済に及ぼす影響

迷惑メールが日本経済に及ぼす影響については、平成 20 年（2008 年）3 月に、財団法人日本データ通信協会が主催した「迷惑メールの経済的影響・調査研究会」（座長：鵜飼康東関西大学ソシオネットワーク戦略研究センター長）で調査が行われました。

この調査では、迷惑メールが日本経済に及ぼす影響について、(a)生産面への被害、(b)ISP 等における対策と投資、(c)事業所・行政機関等における対策と投資、(d)消費者における対策と投資の 4 つに分けて分析されています。なお、消費者への被害として、迷惑メールの削除等に伴う時間的損失、コンピューターウィルス等への感染等の多様な影響が想定されますが、この調査では、その被害額は含まれていません（定量的推計の対象外とされています。）。

調査結果では、我が国における迷惑メールによる経済的な被害額は年間約 7,300 億円（a）、また、迷惑メールへの対策額は年間約 970 億円（b～d の合計）にものぼるとされています。

図表 1 ：迷惑メールによる日本経済への影響額

経済的な被害額		約 7,300 億円
（a） 生産面への被害	迷惑メールによる直接的な影響として、「労働時間損失による経済的損失（GDP への影響）」を金額換算して推計。前年にアンケートを実施し、各産業における迷惑メール受信比率、迷惑メール受信数、迷惑メール処理時間を導出した上で、直近で利用可能な GDP を基に、生産関数を用いて生産面への被害を付加価値で計測推計。	約 7,300 億円
対策額		約 970 億円
（b） ISP 等における対策・投資	迷惑メール対策のためのメールサービス、ヘルプデスク運用担当者の負荷増大、ホスティングサービスの無償提供などを推計。	約 319 億円
（c） 事業所・行政機関等における対策・投資	情報システム担当者による迷惑メール対応コスト、迷惑メール対策ソフトウェアのライセンス費用などを推計。	約 518 億円
（d） 消費者における対策・投資	迷惑メール対策のためのソフトウェア費用を推計。	約 132 億円

※　消費者への被害としては、迷惑メールの削除等に伴う時間的損失、コンピューターウィルス等への感染等の多様な影響が想定されるが、それらの消費者被害の定量的推計は今回の調査の対象外

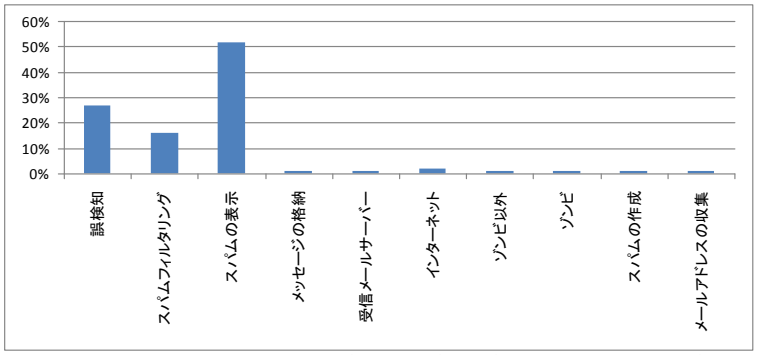
2　迷惑メールが環境に及ぼす影響

迷惑メールによるエネルギー消費量についての試算結果が、平成 21 年（2009 年）4 月に、米国マカフィー社により公表されました。

その結果によると、迷惑メールによる年間のエネルギー消費量は、世界全体では 330 億 KWh で、米国の 240 万世帯が消費する電気量に相当し、310 万台の自家用車が約 75 億リットルのガソリンを消費した場合と同等の温室効果ガス（GHG）排出量になるものとされています。また、迷惑メール 1 件あたりの GHG 排出量は平均 0.3g の CO2 であり、車で 1m 進んだ場合の排出量に相当するとされています。年間全体では、地球を 160 万周した場合と同じ排出量になるものとされています。

迷惑メールの GHG 排出量について要素ごとにみると、その大半（約 80%）は、迷惑メールの表示と削除、誤検知（誤って迷惑メールと認知された電子メールの検索）にかかる電力消費に起因しているものとされています。

図表 2 ：スパムメッセージ 1 件当たりの **GHG** 排出量の比率



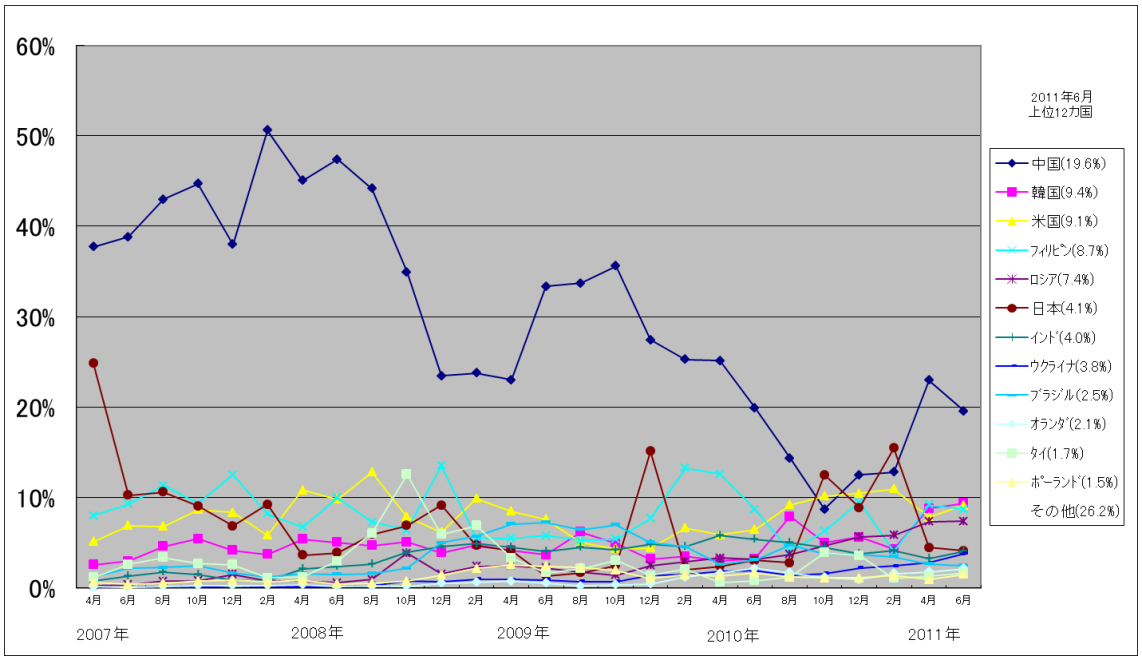
出典：「スパムメールと二酸化炭素排出量」（平成 21 年（2009 年）4 月米国マカフィー社公表）より

第２節　発信国の特徴

１　国内着の迷惑メールでの傾向

第１節でみたとおり、日本着の迷惑メールの大部分は海外発になっています。発信国では、突出して割合の高かった中国の比率が平成 20 年(2008 年）後半より急激に減少しましたが、平成 22 年（2010 年）10 月以降再び増加傾向にあります。従来から発信国上位に位置するフィリピン、アメリカ、韓国に加え、ロシア発の迷惑メールの割合も増加してきており発信国の分散が進んでいると考えられます。

図表２－６：日本着の迷惑メールの発信国の推移

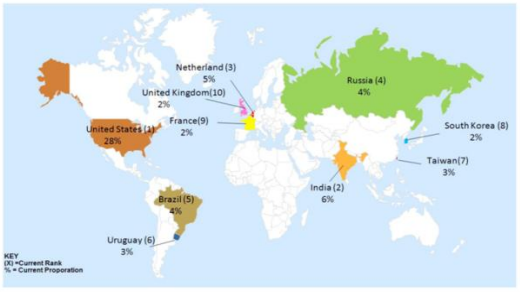


出典：日本データ通信協会迷惑メール相談センター調べ（相談センターのモニター機で受信した情報を分析したもの）

２　世界全体での傾向

日本着のものに限らず、世界全体の迷惑メールの発信国をみると、アメリカ発の迷惑メールの割合が非常に高くなっていることが分かります。また、インド、オランダ、ロシアなどが上位になっています。

図表２－７：世界全体での迷惑メールの発信国の推移



国名	2011年3月	2011年2月	変化(%)
アメリカ	28%	28%	変化なし
インド	6%	5%	+1
オランダ	5%	5%	変化なし
ロシア	4%	4%	変化なし
ブラジル	4%	4%	変化なし
ロシア	3%	3%	変化なし
台湾	3%	情報なし	
韓国	2%	情報なし	
フランス	2%	2%	変化なし
イギリス	2%	3%	-1

出典：シマンテック　スパム＆フィッシングマンスリーレポート　2011 年 4 月（株式会社シマンテック）より

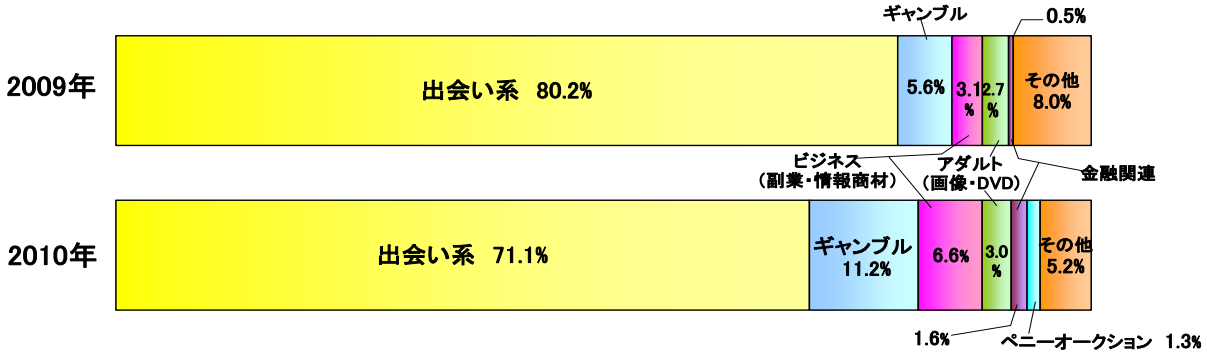
第３節　内容の特徴

１　国内着の迷惑メールでの傾向

我が国の迷惑メールは、いわゆる「出会い系」サイトの広告宣伝が大半を占めていましたが、最近は「ギャンブル」や「ビジネス」が増加傾向にあります。これらは「初心者でも高収入」「在宅ワーク」といった広告文句で、競馬情報や情報商材の販売サイトに誘引しています。

また、最近消費者トラブルが急増した「ペニーオークション」の広告も１.３%を占めています。

図表２－８：国内着の迷惑メールの内容



（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分析したもの　（2009年 34,203件、2010年 37,143件）

出典：（財）日本産業協会　電子商取引モニタリングセンター　8月一斉調査

２　世界全体での傾向

世界全体での迷惑メールでは、その内容は、日本着の迷惑メールとはかなり異なったものとなっています。もっとも多いのが「インターネット」で、これは、インターネットやコンピューター関連の製品・サービスを広告するものです。また、製品・サービスの広告である「各種製品」、懸賞等の「娯楽」や投資関係の「金融」という順になっています。

図表２－９：世界全体の迷惑メールの内容

カテゴリ名	2011年3月	2011年2月	変化（%）
アダルト	<1%	<1%	変化なし
金融	7%	5%	+2
フィッシング	4%	4%	変化なし
医療	4%	6%	-2
インターネット	52%	50%	+2
娯楽	10%	8%	+2
ナイジェリア(419)スパム	8%	11%	-3
政治	<1%	<1%	変化なし
各種製品	12%	12%	変化なし
詐欺	2%	3%	-1

- **インターネット(Internet)メール攻撃**は、インターネットやコンピュータ関連の製品やサービスを提供する（または広告する）ものです。例: ウェブホスティング、ウェブデザイン、スパムウェア
- **医療(Health)メール攻撃**は、健康と医療関連の製品やサービスを提供する（または広告する）ものです。例: 医薬品、治療法、ハーブ療法
- **娯楽(Leisure)メール攻撃**は、懸賞、当選、格安の各種娯楽を提供する（または広告する）ものです。例: 観光旅行、オンラインカジノ
- **各種製品(Products)メール攻撃**は、一般の製品やサービスを提供する（または広告する）ものです。例: 機器、調査サービス、衣料品、化粧品
- **金融(Financial)メール攻撃**は、金銭、株式やその他の「儲け話」を騙って提供するものです。例: 投資、クレジットレポート、不動産、ローン
- **詐欺(Scams)メール攻撃**は、詐欺的と判断できる、または意図的にだまそうとしている、または送信者の詐欺行為に利用されたことがあるものを言います。
- **フィッシング(Fraud)メール攻撃**は、有名企業から来たメールを装っているが、実態は違うというものです。この種のメールはブランドになりすます商標詐称(brand spoofing)やフィッシング(phishing)と呼ばれ、ユーザーをだましてメールアドレス、財務情報、パスワードといった個人情報を送信させようとするものが大半です。例: 口座情報、クレジットカード利用確認、利用明細
- **ナイジェリアスパム（419スパム）メール攻撃**は、ナイジェリア刑法第419条が詐欺に対する罰則を規定していることに由来する命名ですが、宝くじの当選や、引退した政府高官からや死亡した富豪の遺産によって大金を受け取る権利がある旨を告げるスパム電子メールを指します。これは、「前払い金詐欺」と呼ばれることもあります。
- **政治(Political)メール攻撃**は、候補者や選挙戦について広告する、政党や運動への献金を募る、政治家や選挙戦に関する商品を提供する、などを行なうものです。例: 政治関連のブログ
- **アダルト(Adult)メール攻撃**は、18歳以上の成人を対象とする製品やサービスを含み（または紹介し）、攻撃的なものや不適切な内容のものが多く見られます。例: ポルノ、個人広告、出会い系

出典：シマンテック　スパム＆フィッシングマンスリーレポート　2011年４月（株式会社シマンテック）より

Topics うっかりクリックに注意！

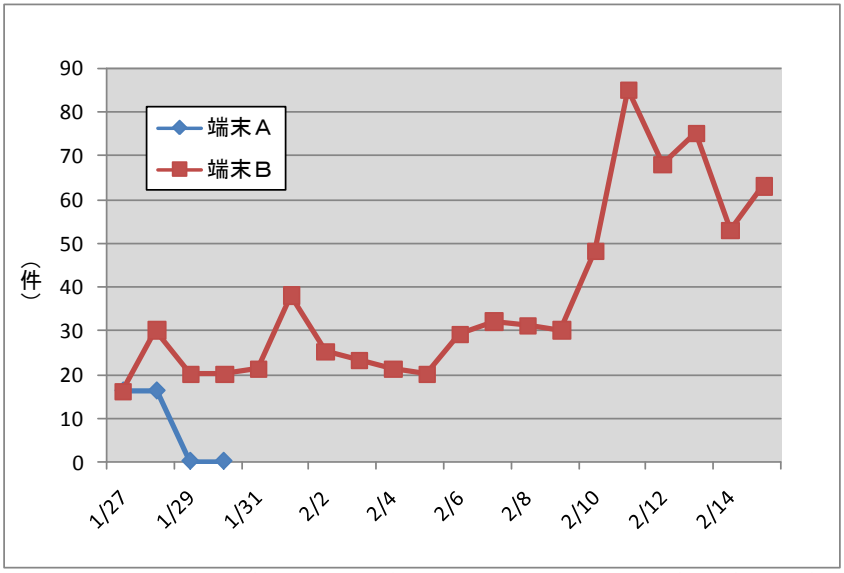
迷惑メールに含まれる URL は、クリックしないように注意する必要があります。

下のグラフは、同一のサイトからメールを受信した 2 台の端末の受信件数の比較です。端末 B のみメールの URL にアクセスしたところ、メール件数は急激に増加し、2 月中旬からは、身に覚えのない請求メールを毎日受信するようになりました。一方、何もクリックしていない端末 A は 4 日ほどで受信が停止しました。

このようにオプトインを装ったサイトは、不当な請求を行う場合もあります。URL をクリックしただけで、どの受信者がアクセスしたか特定できるため、むやみにクリックすることは危険です。

なお、メールによっては、開くだけでウィルスに感染したりする場合もありますので、クリックしなければ安全という訳ではありませんので、注意が必要です。

図表：迷惑メール内の **URL** をクリックしたあとの経過



出典：「迷惑メール送信リポート」（日本産業協会電子商取引モニタリングセンター平成 21 年（2009 年）2 月公表）による

Topics：迷惑メールの例

1　我が国での迷惑メールの例

我が国の迷惑メールで圧倒的に多いいわゆる出会い系サイトに関する広告宣伝の電子メールには、様々なものがありますが、その一例は、次のようなものです。

【出会い系サイトの広告宣伝の例】

【○×○×】
〝ミナミん[るんるん][るんるん]〟さんからメールが届きました。
http://www.****.jp/user.app?cmd=message&memberID=****&password=****&toID=****&resID=****
△この URL を開いてください。

【タイトル】
好意を持ってくれたら活発に動きます(^-^)！

【本文】
あまり人前で目立とうとするタイプではないので、控えめな性格だと思います。でも、恋愛経験が停止状態では何も始まらないので…
MEI さんに私の止まってる時間をスタートさせて欲しいなって思ってます(^-^)☆
時間あるようなら、少しお話ししませんか？早く仲良くなって普通にデートとかしたいですね！

【SNS 会員向けを装った広告宣伝の例】

GUEST 様へ
●●様[写真付き]から新着メールが届いています

▼タイトル▼
《手付金 100 万》を今日中に先払いします。

↓続きを読む↓
http://www.xxlove-▲▲▲.jp/
└有名な SNS サイト名

[PR]
★大歓声特典★　K^/8^J^]A,]=!!この上ない特典を！A,]=お見逃しなく!!　※18 禁

××Love

また、次のような物品販売などに関する迷惑メールも、最近少しずつ目立つようになってきています。

【模造ブランド品販売に関する広告宣伝の例】

他では手に入らない、最高品質の○○○○のレプリカが、大量入荷！
http://********.net/

正規代理店に紛れていたことで世界を驚かせた、
あの最高品質のブランドのレプリカが大量に入荷しました！
http://*******.net/

【高額副業情報に関する広告宣伝メールの例】

【件名】
日給 5 万円以上！高収入副業情報！
【本文】
□高収入副業情報□
日給 5 万円以上！
勤務地は全国から選べます
http://*******.com/
↑詳細はこちらから♪
18 歳以上なら OK！
初心者大歓迎！
週 1 回 1 時間でも OK！
簡単な作業です
http://********.com/
↑詳細はこちらから♪

次の例は、受信者の恐怖心や興味をあおり転送させようとする「チェーンメール」です。

【チェーンメールの例】【本文】

HAPPYMAIL★☆
「人を好きって気持ちは簡単には消せなくてすぐに誰かを好きになるのも無理なんだ。」このメールを７人以上の友達に送った後、送信箱をみてください(-^ ○^-)そしてあなたの生年月日を入力するとあなたの将来の大切な人の名前がでるんです(_<)
このメールは現在人気の雑誌でも公開されています(^0^)本当に当たるので是非みなさんやってみてください o(^-^)o
※本当に７人以上に送信しないと見れません(_<)
７人に送信しないと見れません(_<)
７人に送信したあと、このページを見れば名前が書いてあります★
http://www.****.****/*.cgi?********/

【原子力発電所事故の例】【本文】

小学校生徒の父兄の友達情報です。原発で働いている人だということです。第一原発１号機爆発の後、上った放射線の雲が風に流され北に向かい 13 日現在、仙台上空に達したかもしれません。さらに北に向かう可能性があるとのこと。家の中で窓は開けずになるべく外には出ないで、出るとして も肌の露出を避け、マスクに濡らしたタオルなどあてて短時間にして下さい。しばらくは注意。運良く来なければいいですが、正式発表はとにかく遅れて来るので注意するに越したことはないと思います。特に小さいお子さんがいる人、注意してあげて下さい。このメールをお知り合いの方にも出来るだけ配って下さい。何もないことを祈るばかりです。念のため、お知らせします。雨が降れば汚染されている可能性もあります。

出典：日本データ通信協会迷惑メール相談センター提供資料より

2　海外での迷惑メールの例

【時事問題やニュースを件名に利用した例】

昨年、大規模な地震、サッカーのワールドカップ、自動車のリコール、メキシコ湾原油流出事故等が関心を集めましたが、このような実際のニュースや出来事に加え、スパマーは人々の関心を引くために偽のニュースや出来事を件名に利用する傾向が強く、これは今度も続くと予想されます。

出典：シマンテック　スパム＆フィッシングマンスリーレポート　2010 年 12 月（株式会社シマンテック）より

【有名なソーシャルネットワーキングサイトを詐称するフィッシングの例】

海外では、フィッシングサイトへ誘導するメールの比率が多くなっています。メールの送り主または依頼主が個人情報や金銭を詐取するために送信されており、受信者が何らかのアクションを起こすと次の例のようなサイトに誘導されます。この種のメールは、誘導したサイトが正規サイトに見えるよう巧妙に工夫しており、悪質な例では日本語で書かれたフィッシングサイトへ誘導するメールも確認されています。

このフィッシングは、人気テレビ番組をオンラインで視聴できる Web アプリケーションを提供すると謳ったもので、人気テレビ番組を巧妙に利用し、ユーザーの隙を突いて個人情報を引き出そうする手口を用いています。

出典：シマンテック　スパム＆フィッシングマンスリーレポート　2011 年 2 月（株式会社シマンテック）より

この例に限らず、フィッシャーたちはワナをさらに巧妙にしてエンドユーザーを誘い込める確率を高くしようと画策しています。ワナとして利用されるのは、大部分がポルノなどのアダルトコンテンツであることが確認されています。上記事例の場合、フィッシングサイト自体にポルノは使われていませんでしたが、攻撃の手口はやはり、テレビ番組に出演している特定の有名人のアダルトビデオを見られるというユーザーの期待を利用するものでした。

第４節　送信手法の特徴

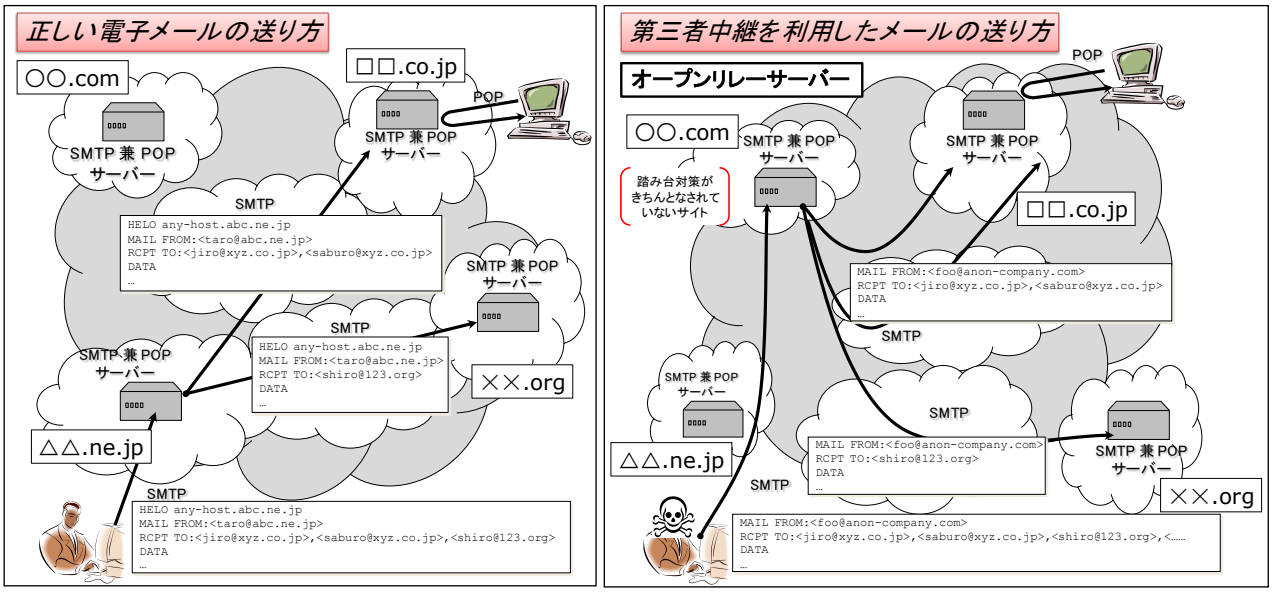
迷惑メールは、そのほとんどが、広告・宣伝やフィッシング、詐欺など、営利を目的として送信されています。そのため、できる限り受信者に到達させるために、手法の巧妙化・悪質化が進んできています。

１　送信者情報などの偽装

迷惑メール送信者の多くは、自身の身元を隠して迷惑メールを送信するために、様々な手法を用いています。

例えば、メールサーバーの設定が不十分なことによりどこからでもメール送信を受け付けてしまう「オープンリレー」と呼ばれるメールサーバーを利用することで、直接自分が使っているネットワーク（インターネットへの接続に使っているプロバイダー等）を特定しづらくする手法や、自らとは無関係のメールアドレスを発信元として表示されるようにすることでメールアドレスから送信者を特定しづらくする手法が、古くから用いられてきました。こういった行為に対処するため、迷惑メールの送信元（IP アドレス）を登録したブラックリスト（後述の DNSBL（DNS Black List / DNS Blackhole List））や、送信元のアドレスに含まれるドメイン名の実在性を確認する手法、正当なメールサーバーから送信されてきているか否かを確認する手法（後述の送信ドメイン認証技術）などによる対応が、主として受信側のプロバイダー等によって行われてきました。

図表２－１０：送信者情報などの偽装



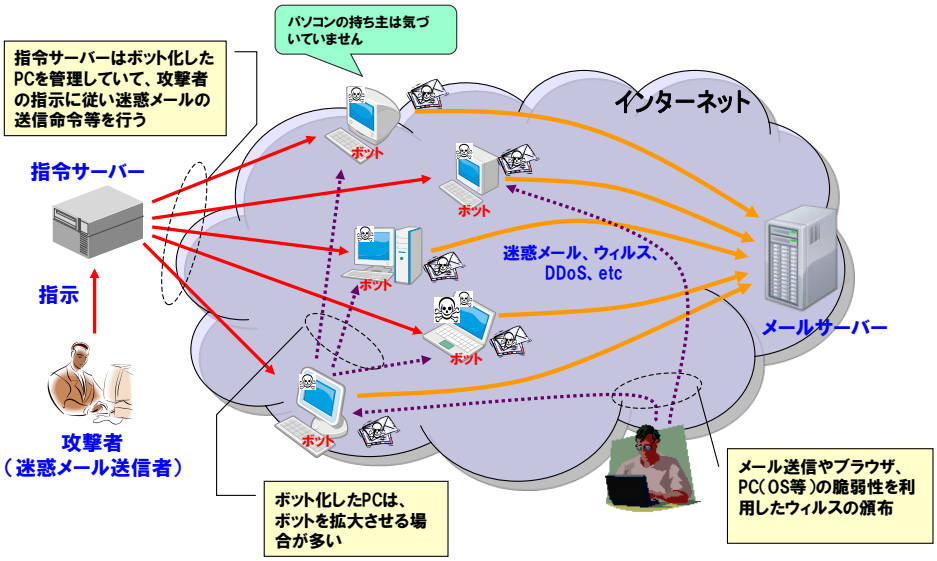
２　ボットネット

平成 14 年（2002 年）頃から、新たな迷惑メールの送信手法が出てきました。コンピューターウィルスのような悪意のあるソフトウェア（マルウェア）を一般ユーザーの PC に大量に感染させ、マルウェアに感染した PC（ロボットに擬して「ボット」と呼ばれています。）を外部ネットワークから操作することによって、迷惑メール送信などに利用する手法が使われるようになっています（こうしたボットの集合は「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という特徴があります。そのため、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（これらの手法の概要については、第４章第１節を参照。）。

ボットネットからの迷惑メールに対しては、インターネット接続に利用する動的 IP アドレスからの直接メール送信ができないように送信側のプロバイダー等で制限する手法（OP25B（Outbound Port 25 Blocking））が有効です（詳細については、第４章第２節参照。）。

図表２－１１：ボットネットのイメージ



３　固定 IP アドレスを用いた送信

日本国内では、後述のとおり、OP25B が普及したことにより、動的 IP アドレスから直接迷惑メールを送信しづらくなったことから、迷惑メールを送信しようとする者は、ISP と固定 IP の使用契約（固定 IP の払出しの契約）を締結し、迷惑メールを送信するようになってきました。

この手法では、ISP との契約が発生することから、本来であれば送信元が特定可能なはずですが、契約者情報を偽って複数の契約を締結することで、大量の固定 IP アドレスを確保し、迷惑メールの送信を行っているという実態があります（第４章第２節参照。なお、「固定 IP アドレス」、「動的 IP アドレス」については、同節の用語解説参照。）。

また、迷惑メールの送信行為が判明し、契約する ISP から利用停止措置など受けると、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、迷惑メール送信を繰り返す迷惑メール送信者も存在します。

固定 IP アドレスを用いた迷惑メールの送信を防ぐためには、それらの違反者に対する法執行が効果的です。そのために、利用者において、受信した迷惑メールに関する情報を関係機関に提供するとともに、プロバイダー等が行政機関に対して、法律に基づき、それらの固定 IP アドレスの契約者情報を提供することにより、法執行の強化を図っていくことが有効と考えられます。一方で、契約時の契約者情報の確認が十分に行われていないと、これらの有効な措置を講じることが難しくなること、前述のとおり、利用停止等を受けても新たに契約を締結して迷惑メールの送信行為を繰り返す送信も存在することから、プロバイダー等において、契約を締結する際に契約者情報が真正であることを確認し、水際で防止していくことが重要です。

４　迷惑メールフィルターの回避

多くの迷惑メールは、なんらかの販売・宣伝行為やホームページへの誘導、ウィルスの配布などが主目的であり、その内容がほとんど同じであるという特徴があります。そこで、よく使われる文字列など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手法が用いられるようになりました。この手法は、一般的に、迷惑メールフィルターと呼ばれています。

しかし、迷惑メールフィルターによる迷惑メールとの判定を回避するため、最近の迷惑メールでは、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、用いられる画像データは、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２－１２：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！	┌┐ ┌┐ ┌┐ ┌┐ ｜無｜ ｜料｜ ｜画｜ ｜像｜ └┘ └┘ └┘ └┘	◆ 専 用 メ ー ル Ｂ Ｏ Ｘ 【開封無料】

Topics：ボット対策の取り組み（サイバークリーンセンター）

【サイバークリーンセンターとは】

サイバークリーンセンターは、インターネットにおける脅威となっているボットの特徴を解析するとともに、ユーザーのコンピューターからボットを駆除するために必要な情報をユーザーに提供する活動を行っています。また、ISP（インターネットサービスプロバイダー）の協力によって、ボットに感染しているユーザーに対し、ボットの駆除や再感染防止を促すプロジェクトの中核を担っています。

平成 18 年（2006 年）12 月から総務省･経済産業省共同で行われてきたこの取り組みは、平成 23 年（2011 年）度以降は取り組みの一部が民間を中心に運営される予定であり、現在準備が進められています。

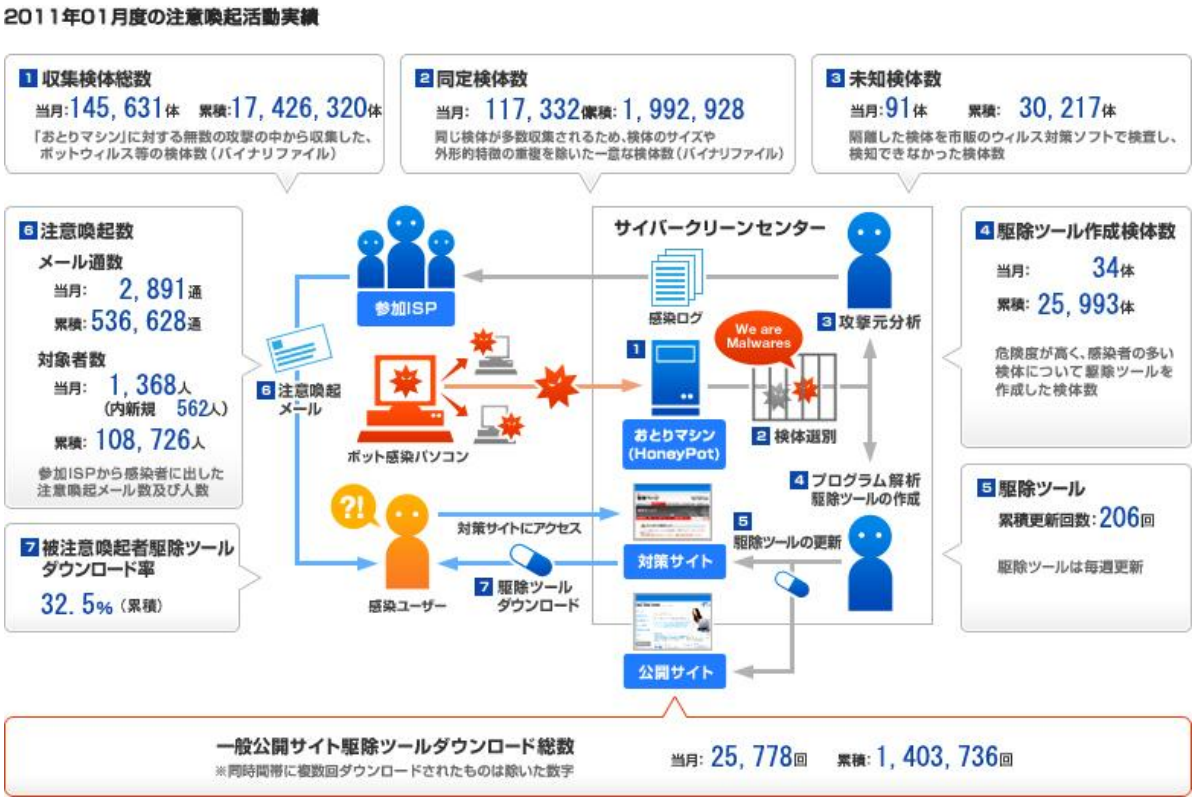
【サイバークリーンセンターの目的】

近年、インターネット上で感染拡大している不正プログラムの一種「ボット」には非常に多くの亜種が存在し、従来のコンピューターウィルスの駆除手法による対応が困難となってきています。また、ボットによる攻撃・感染活動は限定的かつ水面下で実施されることから、ユーザー自身が攻撃や感染の事実を把握できないという深刻な状況になっています。

このような状況において、安全なインターネット環境を実現するためには、ボットの攻撃・感染活動を効率的かつ安全に把握し、感染ユーザーに対策手法を提示することでボットの駆除を促す活動が必要であると考えられます。

サイバークリーンセンターでは、関係機関および ISP、ボット対策情報作成者、セキュリティベンダーが有機的に連携した統合基盤を構築し、この基盤を利用した活動を継続することを目的としています。

図表：サイバークリーンセンターの活動実績



出典：Cyber Clean Center（サイバークリーンセンター）（https://www.ccc.go.jp/）より

Topics：ボットネットの切断

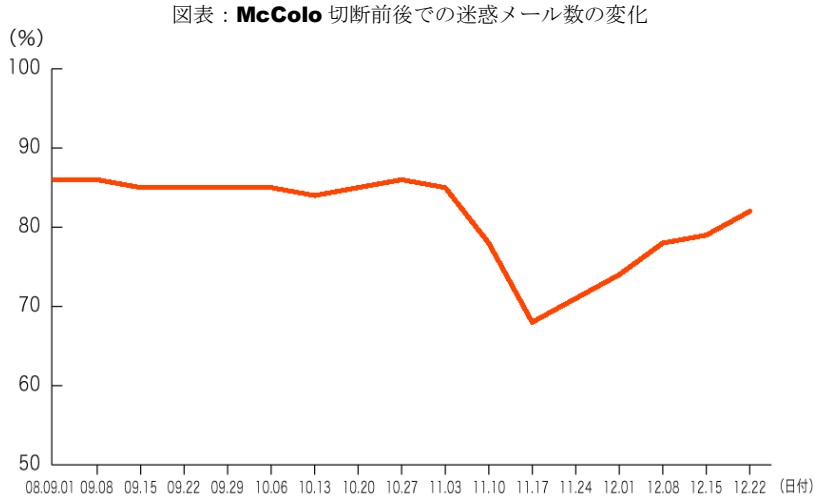
現在の迷惑メールの多くがボットネットから送信されていることから、迷惑メールの送信を減らすため、これらボットネットの動きを止めることが重要です。ボットネットの活動を抑止する方法の一つとして OP25B がありますが、ボットへの外部からの操作を抑制することができれば、より効果的です。

ボットは、主に IRC（Internet Relay Chat）などの既存の通信手法を利用し、外部から迷惑メール送信などの指令を受けます。これら指令を送っているボットの管理元は、C&C（Command and Control）サーバーやハーダー（Herder，元々は羊飼いの意味）と呼ばれます。これら操作元からの指令がボットに届かないように対応したことで、迷惑メールが劇的に減少した事例がありました。

1　McColo の切断

2008 年 11 月 11 日(米国時間)、米国カリフォルニア州のウェブホスティングの事業を行っている McColo 社のネットワークが遮断されました。ワシントンポスト紙の記者は、これは McColo 社にインターネット接続を提供している大手 ISP2 社によるものと報じています。McColo 社の顧客には、最も評判の悪いサイバー犯罪組織が含まれており、そういった情報を集めて大手 ISP に報告した結果、McColo 社のインターネット接続が遮断されたとのことです。このネットワーク遮断により、McColo 社のサーバーによって運営されていた数百万のボットへの指令が届かなくなりました。ボットへの指令が届かなくなったことにより、迷惑メール送信などの活動が働かなくなり、結果として迷惑メールの送信量が劇的に減少しました。幾つかのセキュリティベンダーの調査では，これにより迷惑メール（スパム）の送信量が半分から 1/3 程度にまで減少したとの報告がなされています。

図表：**McColo** 切断前後での迷惑メール数の変化



出典：Internet Infrastructure Review vol.2　Feb.2009（株式会社インターネットイニシアティブ）より

この McColo 社のネットワーク遮断という出来事により、幾つかの事柄が明らかになりました。一つは、迷惑メールの大部分は、やはりボットネットにより送信されている、ということです。迷惑メールの送信を減らすためには、このボットネットに対する対策が必要不可欠といえます。もう一つは、現状のボットネットはごく限られた管理サーバーによって運営されている、ということです。残念なことに、McColo 社のネットワーク遮断は現在も回復していないにもかかわらず、遮断の数週間後には迷惑メールの送信量が回復基調になり、今年に入ってからほぼ以前の水準に戻っているとの調査結果も出ています。このことから、新たなボットネットの管理サーバーが復活していることが推測できますし、また管理サーバーによる垂直的な指令構成ではなく Peer-to-Peer 技術を使った新しいタイプのボットネットが出現しているとの報告もあります。

2　Rustock の切断

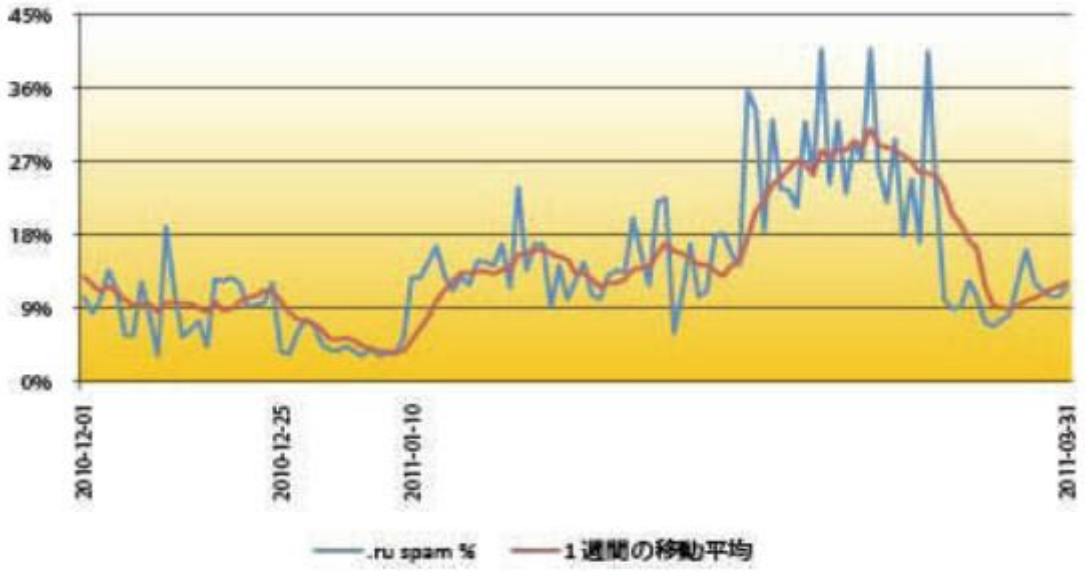
2011 年 3 月 16 日(米国時間)、歴史上最大と言われていたボットネット「Rustock」が遮断されました。米国政府と Microsoft 社との連携により実行されたもので、シマンテック社がスパム流通量の大幅減を報告しています。世界全体のスパム量は、Rustock 遮断後、遮断前に比べて 24.7 パーセント減少し、翌 17 日には、さらに 11.9 パーセント減少、1 週間前と比較すると 40.4% 減になっているとのことです。

図表 1　Rustock 遮断によるめスパム流通量の変化

出典：シマンテック　スパム＆フィッシングマンスリーレポート　2011 年 4 月（株式会社シマンテック）より

この事例も迷惑メールの大部分がボットネットから送信されていることを裏付けています。また、Rustock が世界的に活動していることから、スパム発信が増えているロシアでも利用されていたことを窺わせる調査結果が、シマンテック社より報告されています。Rustock は 2010 年末にも休眠状態の期間があったといわれており、この時期と 2011 年 3 月 16 日の遮断後に.ru ドメイン（ロシア）のスパムが減少しているというものです。

図表 2　.ru ドメインのスパム流通量



出典：シマンテック　スパム＆フィッシングマンスリーレポート　2011 年 4 月（株式会社シマンテック）より

第3章
制度的な対策

第３章　制度的な対策

第１節　法令による制度的な対策

携帯電話による電子メールの急速な普及などに伴い、平成 13 年（2001 年）頃から、迷惑メールが大きな問題となりました。このような状況を受け、平成 14 年（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。

また、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：迷惑メール規制に関する特定電子メール法と特定商取引法との比較

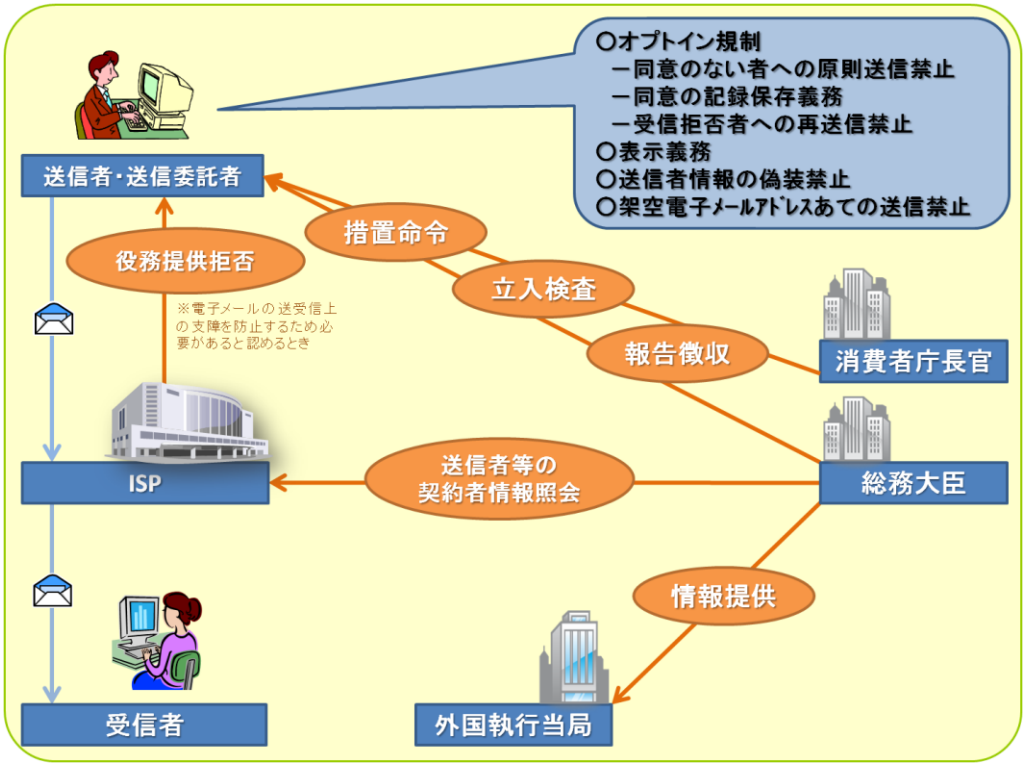
特定電子メール法		特定商取引法
電子メールの送受信上の支障の防止の観点から送信を規制	目的	消費者保護と取引の公正の観点から広告を規制
自己又は他人の営業につき広告又は宣伝を行うための手段として送信する電子メールなど	規制対象	通信販売等の電子メール広告
送信者及び送信委託者	規制対象者	販売事業者及び電子メール広告受託事業者
・あらかじめ同意した者等以外に広告宣伝メールを送信することを禁止 ・同意を証する記録の保存義務 ・受信拒否者への再送信禁止 ・表示義務	オプトイン規制	・あらかじめ承諾した者等以外に電子メール広告をすることを禁止（直罰） ・請求・承諾の保存義務（直罰） ・受信拒否者への電子メール広告の禁止（直罰） ・表示義務（直罰）
・架空電子メールアドレスを宛先とする送信の禁止	架空電子メールアドレスを宛先とした電子メール対象	―
・送信者情報を偽った送信の禁止（直罰）	送信者情報を偽装した電子メール対策	―
総務大臣は、電子メールアドレス等の契約者情報を保有する ISP 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。	電気通信事業者等への情報提供の求め	主務大臣は、電子メールアドレス等の契約者情報を保有する ISP 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・
総務大臣及び内閣総理大臣	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

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３－２：特定電子メール法の概要



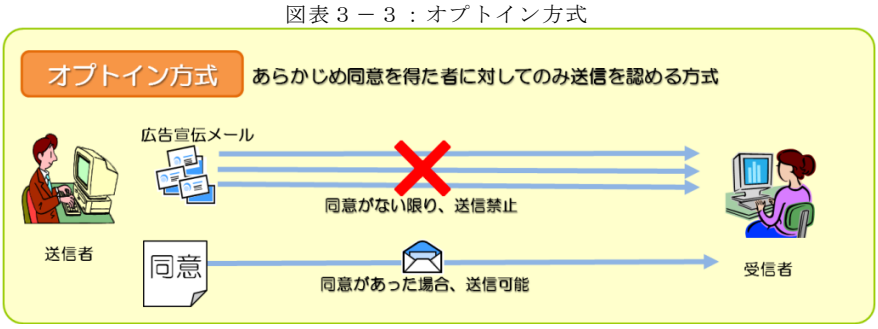
(1)電子メールの送信者に対する規制

まず、受信者の同意を得ない広告宣伝メールの送信が原則として禁止されています(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、From 欄に表示される差出人アドレスなどを偽って送信し、メールの発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(送信者情報の偽装についての詳細は、第２章第４節１を参照)。

さらに、プログラムを用いて自動的に大量のアドレスを生成し、それらのアドレスをあて先として送信することで、実在する電子メールアドレスを収集する手法についても、迷惑メールの送信を助長するだけでなく、電気通信事業者の設備に多大な負担をかけることから、禁止されています。

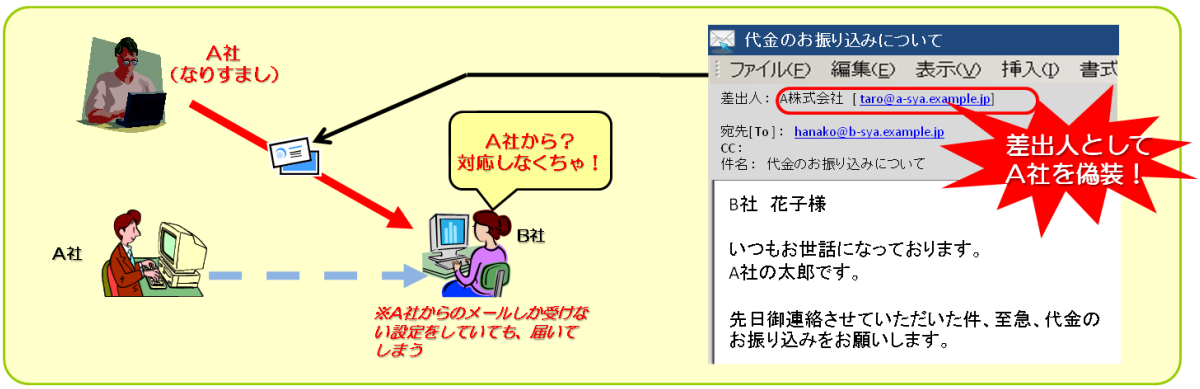
図表３－３：オプトイン方式



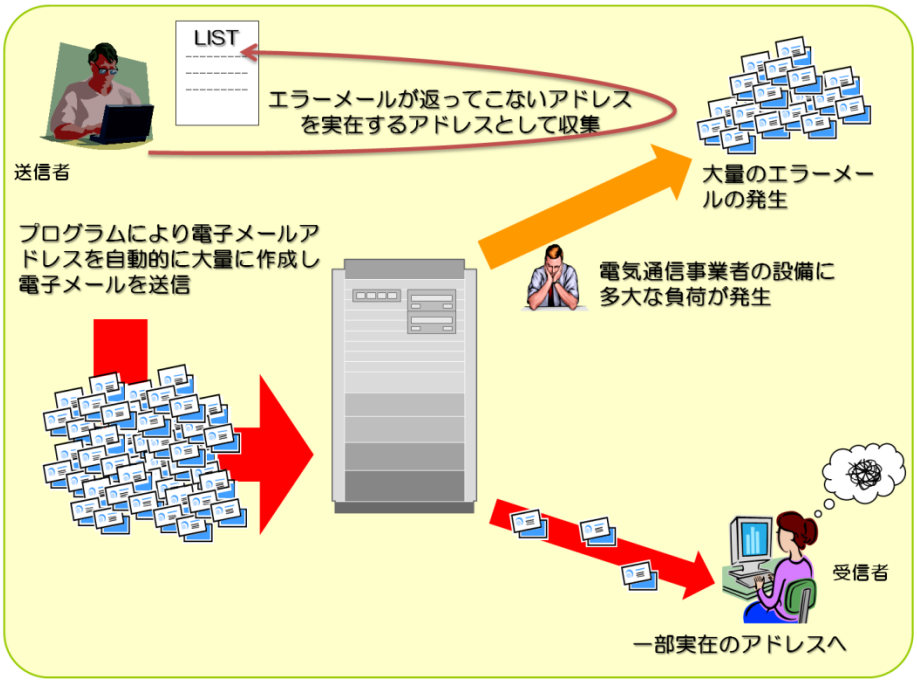
(2)電子メールの送信を委託している者に対する規制

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、送信委託者が違法な広告宣伝メールの送信に責任を有していた場合には、送信委託者が行政処分の対象となることがあります。

図表３－４：送信者情報の偽装の例



図表３－５：架空電子メールアドレスあての送信



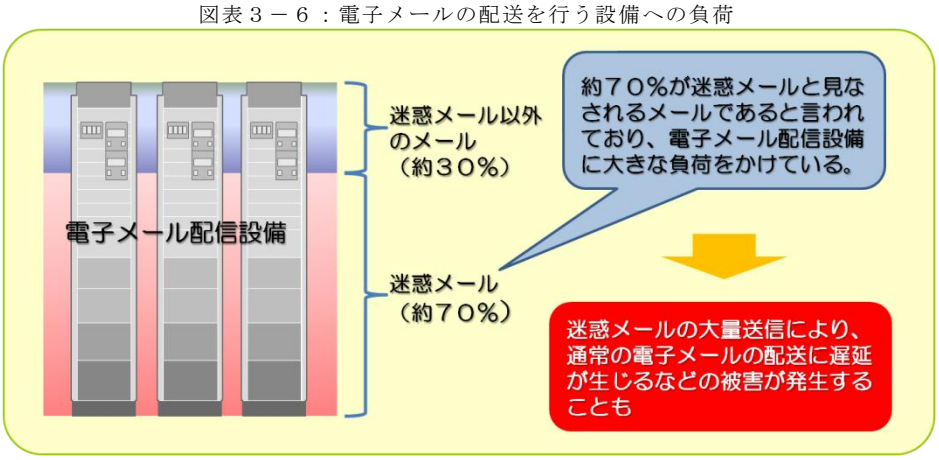
(3)電気通信事業者に関する規定

電子メールの大量送信は、電気通信事業者の設置する電子メールの配送設備に負荷を生じさせます。これによって、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、法律によって、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、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。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、通信の秘密の観点からも問題が生じ得ます。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、サービスの提供拒否が、緊急避難や正当業務行為に該当する場合には、この限りではありません。特定電子メール法においては、このような、例外的にサービス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電子メールサービスの提供を拒否することができます。

図表３－６：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

法律違反者に対しては、総務大臣と消費者庁長官が共同で行政処分（措置命令）を行えます（ただし、架空電子メールアドレスをあて先とする送信に関する措置命令は、総務大臣が単独で行います。）。また、違反内容によっては、直接に刑事罰が科されるものもあります。

このほか、総務大臣や消費者庁長官が、法律違反が疑われる送信者などに対し、報告徴収や職員による立入検査を実施できます。プロバイダーなどに対しては、総務大臣が、迷惑メール送信者等の契約者情報の照会を行うことができます。

(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、総務省と外国当局との連携に関する規定が設けられています。

特定電子メール法の沿革

(1)法律の制定（平成 14 年（2002 年））－オプトアウト方式による規制の導入

携帯電話あての迷惑メールが社会問題となったことなどを受けて、平成 14 年（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あて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)法律の平成 17 年（2005 年）改正－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、平成 17 年（2005 年）に法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、違反の場合は直接刑事罰（１年以下の懲役または 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、私用のアドレスだけでなく、事業用のアドレスにも拡大されたほか、広告宣伝メール以外のメールについても、架空電子メールアドレスあての送信が禁止され、規制範囲が拡大されました。措置命令に違反した場合の罰則も強化されています（50 万円以下の罰金から、１年以下の懲役または 100 万円以下の罰金に）。

(3)法律の平成 20 年（2008 年）改正－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、平成 20 年（2008 年）に更なる法改正が行われました。この改正により、a)オプトイン方式による規制が導入されたほか、b)法の実行性の強化や、c)外国から発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。

a)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。法改正により、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。

b)法の実効性の強化

・法人に対する罰金額が 100 万円以下から 3000 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 ISP 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。
・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。

c)外国から発信される迷惑メールへの対応強化

・総務大臣が、迷惑メール対策を行う外国執行当局に対し、その職務に必要な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（上述）。

(4)法律の平成 21 年（2009 年）改正－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、消費者庁が広告宣伝メールなどの送信に関して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。主要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あて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また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)平成 23 年（2011 年）見直しの検討

「特定電子メールの送信の適正化等に関する法律」の 2008 年（平成 20 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等を踏まえ、「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」において、2010 年（平成 22 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、学識経験者等、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（平成 23 年）7 月、提言をとりまとめました。

提言では、制度面について、現時点では、特定電子メール法のさら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等を提言しています。

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、ショートメッセージサービス（SMS）を含みます。）が規制の対象です。

(3)規制等の対象となる者

電子メールの送信者およ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）

a)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。

b)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。

c)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。

d)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（From 欄に表示されるメールアドレスや発信元の 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あての送信の禁止（送信者への規制）

プログラムによって自動的に作成された電子メールアドレスであって利用者がいないもの（架空電子メールアドレス）をあて先として電子メールを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

a)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。

b)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。

c)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。

d)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)総務大臣また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、総務大臣また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へ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、総務大臣および内閣総理大臣による登録機関（登録送信適正化機関）についての規定が置かれています。総務大臣および内閣総理大臣は、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。

・総務大臣また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
・広告宣伝メールなど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

a)刑事罰

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(図表参照)。

b)行政処分（措置命令）

総務大臣および消費者庁長官は、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。

✔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あて先とする電子メールの送信をしたと認める場合

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。

措置命令に違反した場合は刑事罰の対象となります（図表参照)。

※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あて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。)。

c)報告徴収・立入検査

総務大臣または消費者庁長官は、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

また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実施できます。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（図表参照）。

図表：特定電子メール法の主要な罰則など

違反事項	罰則など
送信者情報を偽った送信	1年以下の懲役または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3000万円以下の罰金）。 ※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年以下の懲役または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3000万円以下の罰金）。
同意のない者への送信	
受信拒否者への送信	
表示義務違反	
同意を称する記録の保存義務違反	行政処分（措置命令）。措置命令に従わない場合、100万円以下の罰金（法人の場合は行為者を罰するほか、法人に対して100万円以下の罰金）。
報告徴収を受けた場合の報告の懈怠 立入検査に際しての検査忌避	100万円以下の罰金

d) プロバイダー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、プロバイダーなどに対し、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。

e) 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。

a) 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。

b) 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通信方式が規定されています。

また、法律およ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。

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。

(1)「電子メール広告」を送信する事業者などに対する規制

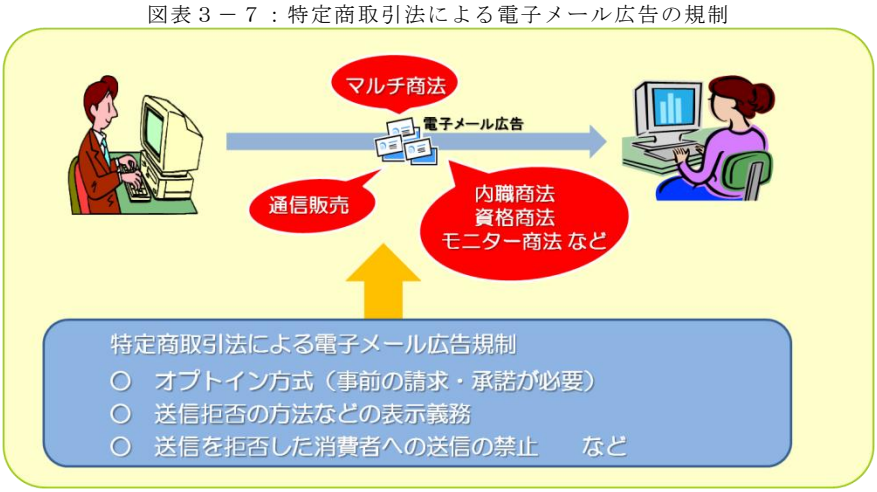
特定商取引法においては、通信販売、連鎖販売取引（いわゆるマルチ商法）、業務提供誘引販売取引（いわゆる内職商法、資格商法、モニター商法など）の形態で消費者と取引をする場合において、事業者が、取引の対象となる商品や役務などについて電子メールにより広告をする場合には、オプトイン方式による規制が課されます。すなわち、事業者が消費者に対してこれらの電子メール広告を行うに当たっては、消費者による事前の請求または承諾が必要です。また、請求・承諾を得て電子メール広告を行う場合であっても、電子メール広告の送信を拒否する方法など一定の事項を表示する義務が課されているほか、電子メール広告の送信を拒否した消費者への送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

(2)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

販売業者等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、販売業者等に課されている義務が受託事業者に課されます。

a)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
b)消費者からの請求や承諾の記録を作成し、保存する業務
c)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３－７：特定商取引法による電子メール広告の規制



(3)法の実効性の確保

法律違反者に対しては、直接刑事罰が科されるほか、主務大臣が行政処分（指示または業務停止命令）を行うことができます。また、主務大臣は、法律違反が疑われる販売業者等に対し、報告徴収や職員による立入検査を実施できます。プロバイダーなどに対しては、主務大臣が、迷惑メール送信者等の契約者情報の照会を行うことができます。さらに、販売業者等と取引をする者に対する者に対しては、主務大臣が、報告や書類の提出などを命じることができます。

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（平成 14 年（2002 年）2 月）－表示義務の導入

通信販売業者等が電子メールにより商業広告を送る際に、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（平成 14 年（2002 年）4 月）－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。併せて、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、請求また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（平成 20 年（2008 年）12 月）－オプトイン方式による規制の導入など

平成 14 年（2002 年）の法改正以降も、迷惑広告メール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、平成 20 年（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。

a)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また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（特定商取引法施行規則で定められています。）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

イ）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

ロ）消費者からの請求や承諾の記録を作成し、保存する業務

ハ）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

b)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。

c)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。

イ）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

ロ）消費者からの請求や承諾の記録を作成し、保存する業務

ハ）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や IP アドレスなどの契約者情報を保有する ISP 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刑事罰が科されるなど、罰則が強化されました。

(4)法律の改正（平成 21 年(2009 年)9 月）ー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および経済産業局長が、行政処分、報告徴収、職員による立入検査、プロバイダー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（平成 21 年(2009 年)12 月）ー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。

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）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。

a)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
b)消費者からの請求や承諾の記録を作成し、保存する業務
c)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

a)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。

b)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。

c)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。

d)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。

e)その他
以下の行為（特定商取引法施行規則で定められています。）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、上記(3)a)～c)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

a)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(図表参照)。

b)行政処分（指示または業務停止命令）

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（指示または業務停止命令）を行うことができます。指示または業務停止命令に違反した場合は刑事罰の対象となります（図表参照)。

✔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
✔上記(4)e)「その他」に掲げる行為を行った場合

c)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（図表参照)。

d)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（上記ａに該当する場合を除く）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。

e)プロバイダー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、プロバイダーなどに対し、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。

f)主要な罰則など

図表１：主な罰則について

違反行為	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）
業務停止命令違反	２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	100 万円以下の罰金

※主務大臣について

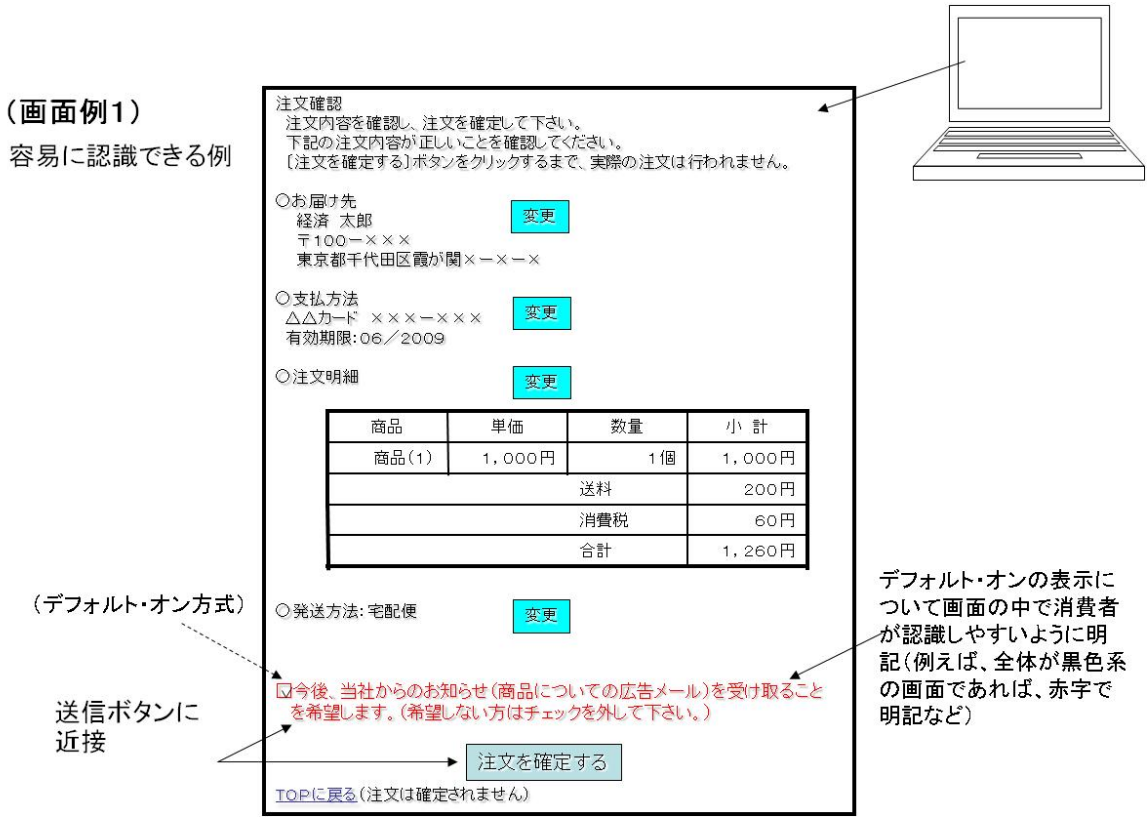
内閣総理大臣、経済産業大臣および事業等所管大臣が、主務大臣とされています。また、電子メール広告受託事業者に関する事項については、内閣総理大臣および経済産業大臣が主務大臣とされています。なお、内閣総理大臣の権限は、一部を除いて消費者庁長官に委任されており、消費者庁長官に委任された権限の一部は、経済産業局長に委任されています。

(6)省令・ガイドライン

特定商取引法の運用に当たっての詳細な事項は、省令（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。

また、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、ガイドラインが策定されています（『電子メール広告をすることの承諾・請求の取得等に係る「容易に認識できるよう表示していないこと」に係るガイドライン』）。

図表２：消費者が商品を購入したショッピングサイト等における承諾の取り方について



3　その他の法律

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に加えて、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、架空請求を行うメールを送信し、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。また、医薬品や、化粧品、医療機器等について、その効能、効果又は性能に関して、虚偽又は誇大な記事を広告する電子メールを送信した場合には、薬事法第 66 条に違反する可能性があり、承認前の医薬品等について、その効能を広告する電子メールを送信した場合には、同法第 68 条に違反する可能性があります。

図表３－８：電子メールの送信に関わる法規制

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、株価操作等）		
○　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 1000 万円以下の罰金又はその併科
3　わいせつ物頒布、児童ポルノ提供等		
○　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（※１））	2 年以下の懲役若しくは 250 万円以下の罰金若しくは科料又は懲役及び罰金の併科
○　人に児童買春をするように勧誘する電子メールの送信の禁止	児童ポルノ処罰法第 6 条第 1 項	5 年以下の懲役若しくは 500 万円以下の罰金又はその併科
○　児童ポルノの画像等を含む電子メールの送信の禁止	児童ポルノ処罰法第 7 条第 1 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（※２））	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	薬事法第 66 条第 1 項、第 68 条、第 85 条	2 年以下の懲役若しくは 200 万円以下の罰金又はこれらの併科
8　ウイルス作成・提供・保管等		
○　ウイルス作成・提供・供用の禁止	刑法第 168 条の 2（不正指令電磁的記録作成等）（※３）	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）（※３）	2 年以下の懲役又は 30 万円以下の罰金

※１：　平成 23 年 6 月の「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」行為等を処罰する規定が挿入された。
※２：財物の交付または財産的利益の移転がなされていない場合は、詐欺未遂。
※３：平成 23 年 6 月の「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」により新たに設けられた。

第２節　迷惑メール関連法の執行状況

１　特定電子メール法の執行状況

(1)平成 20 年（2008 年）改正までの執行状況（オプトイン規制導入前）

平成 20 年（2008 年）改正までのオプトアウト規制の下で、総務大臣による措置命令が 6 件、警察による摘発が 4 件行われています。オプトアウト規制時には、6 件全てが表示義務違反が絡んでおり、措置命令件数は年間平均約 0.94 件でした。

図表３－９：総務大臣による措置命令

処分年月	事業者名	法違反の内容
平成 14 年（2002 年）12 月	東京都中野区の事業者（名称非公表） （出会い系サイトの広告・宣伝）	表示義務違反 再送信禁止義務違反
平成 15 年（2003 年）11 月	東京都中野区の事業者（名称非公表） （出会い系サイトの広告・宣伝）	表示義務違反
平成 16 年（2004 年）4 月	（株）エス・アイ・エス・ワールド （出会い系サイトの広告・宣伝）	表示義務違反
平成 17 年（2005 年）9 月	（有）コスモメディアサービス （出会い系サイトの広告・宣伝）	表示義務違反
平成 20 年（2008 年）2 月	（株）ビューティースタイル （美容商品等の広告・宣伝）	表示義務違反
平成 20 年（2008 年）6 月	（株）Botolo （出会い系サイトの広告宣伝）	表示義務違反

図表３－１０：警察による摘発

摘発年月	概要	判決内容
平成 18 年（2006 年）5 月	千葉県警が東京都内の男性を逮捕	懲役 8 ヶ月、執行猶予 3 年。法人については罰金 80 万円。
平成 18 年（2006 年）8 月	大阪府警が大阪市内の元会社社長等を書類送検	元社長に罰金 100 万円、従業員 1 名に罰金 50 万円。
平成 19 年（2007 年）1 月	千葉県警が東京都内の会社社長等を逮捕	2 名に懲役 8 月執行猶予 4 年。 1 名に懲役 6 月、執行猶予 5 年。 1 名に懲役 6 月、執行猶予 3 年。
平成 20 年（2008 年）2 月	警視庁が東京都内の男性を逮捕	懲役 6 月、執行猶予 3 年。

※送信者情報を偽って広告宣伝メールを送信したことによる直接刑事罰

(2)平成 20 年（2008 年）改正後の執行状況（オプトイン規制導入後）

平成 20 年（2008 年）改正後のオプトイン規制の下で、総務大臣及び消費者庁長官（平成 21 年（2009 年）8 月以前は総務大臣）による措置命令は、平成 23 年（2011 年）7 月までに、20 件行われています。また、警察による摘発が 1 件行われています。オプトイン規制後は、措置命令が年間平均約 7.49 件とオプトアウト規制時の約 7 倍になっています。

図表３－１１：総務大臣及び消費者庁長官による措置命令（オプトイン規制導入後）（※）

処分年月	事業者名	違反事項
平成 21 年（2009 年）4 月	個人事業者 （出会い系サイトの広告・宣伝）	受信者の同意を得ずに送信
平成 21 年（2009 年）6 月	（株）HolyAce （美容商品等の広告・宣伝）	受信者の同意を得ずに送信 表示義務違反
平成 21 年（2009 年）10 月	(株)EIGHT （出会い系サイトの広告・宣伝）	受信者の同意を得ずに送信 表示義務違反
平成 21 年（2009 年）10 月	(株)アルファクト （出会い系サイトの広告・宣伝）	受信者の同意を得ずに送信
平成 21 年（2009 年）12 月	(株)エレクトリックオペレーション （出会い系サイトの広告・宣伝）	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
平成 22 年　（2010 年）3 月	個人事業者 （出会い系サイトの広告・宣伝）	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
平成 22 年（2010 年）4 月	(株)スパイラルネット （出会い系サイトの広告・宣伝）	受信者の同意を得ずに送信

平成 22 年（2010 年）4 月	(株)広告研究所 （出会い系サイトの広告・宣伝）	受信者の同意を得ずに送信
平成 22 年（2010 年）8 月	(株)アンビション （出会い系サイトの広告・宣伝）	受信者の同意を得ずに送信 表示義務違反
平成 22 年（2010 年）12 月	(株)ＩＴＳ （他者サイトの広告・宣伝）	受信者の同意を得ずに送信
平成 23 年（2011 年）1 月	(株)エース （出会い系サイト及び他者サイトの広告・宣伝）	受信者の同意を得ずに送信 表示義務違反
平成 23 年（2011 年）3 月	(株)フレンディア （出会い系サイトの広告・宣伝）	受信者の同意を得ずに送信
平成 23 年（2011 年）3 月	(株)エルベール （出会い系サイトの広告・宣伝）	受信者の同意を得ずに送信
平成 23 年（2011 年）4 月	(株)シックスエストレラ （出会い系サイトの広告・宣伝）	受信者の同意を得ずに送信
平成 23 年（2011 年）5 月	(株)ノブロ （出会い系サイトの広告・宣伝）	受信者の同意を得ずに送信 表示義務違反
平成 23 年（2011 年）6 月	個人事業者 （出会い系サイトの広告・宣伝）	受信者の同意を得ずに送信 表示義務違反
平成 23 年（2011 年）6 月	(株)ＦＩＮＥ （出会い系サイトの広告・宣伝）	受信者の同意を得ずに送信 表示義務違反
平成 23 年（2011 年）6 月	(株)Ｂｒｅｅｚｅ （出会い系サイトの広告・宣伝）	受信者の同意を得ずに送信 表示義務違反
平成 23 年（2011 年）6 月	(株)next media （出会い系サイトの広告・宣伝）	受信者の同意を得ずに送信 表示義務違反
平成 23 年（2011 年）7 月	(株)Cyber Factory （出会い系サイトの広告・宣伝）	受信者の同意を得ずに送信 表示義務違反

※　平成 21 年（2009 年）8 月以前は総務大臣による措置命令

図表３－１２：警察による摘発

摘発年月	概要	判決内容
平成 23 年（2011 年）1 月	京都府警・山梨県警が東京都内の男女計 7 人を逮捕	法人(1 社)について罰金 700 万円。 1 名に懲役 10 ケ月、執行猶予 3 年。 2 名に懲役 8 ケ月、執行猶予 3 年。 4 名に罰金 30～50 万円（略式起訴）。

※送信者情報を偽って広告宣伝メールを送信したことによる直接刑事罰

2　特定商取引に関する法律の執行状況（電子メール広告に関するもの）

(1)平成 20 年（2008 年）改正までの執行状況（オプトイン規制導入前）

平成 20 年（2008 年）改正までのオプトアウト規制の下で、電子メール広告に関する特定商取引法による　　行政処分は 8 件行われています。

図表３－１３：特定商取引法に基づく行政処分

処分年月	業者名	処分内容	法違反の内容
平成 15 年（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。
平成 15 年（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。
平成 17 年（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
平成 17 年（2005 年）6 月	（有）エス・ケー・アイ	業務停止命令 3 ヶ月及び指示	表示義務違反および顧客の意に反する申し込み（ワンクリック）
平成 18 年（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
平成 19 年（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、誇大広告および顧客の意に反する申し込み
平成 19 年（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、誇大広告および顧客の意に反する申し込み
平成 20 年（2008 年）5 月	（有）メディアテクノロジー	指示	誇大広告

(2)平成 20 年（2008 年）改正後の執行状況（オプトイン規制導入後）

平成 20 年（2008 年）改正後のオプトイン規制の下で、未承諾電子メール広告に関する特定商取引法による行政処分（指示）は平成 23 年（2011 年）5 月末までに、7 件行われています。また、警察による摘発が 2 件行われています。

図表３－１４：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	業者名	処分内容	法違反の内容
平成 21 年（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
平成 21 年（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
平成 21 年（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
平成 21 年（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
平成 22 年（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
平成 22 年（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
平成 22 年（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

図表３－１５：警察による摘発

摘発年月	概要	判決内容
平成 22 年(2010 年)10 月	千葉県警が千葉県内の男計 3 人を逮捕	1 名に罰金 30 万円
平成 23 年(2011 年)4 月	埼玉県警が埼玉県内の男計２人を逮捕	2 名に罰金 50 万円
平成 23 年(2011 年)5 月	警視庁が東京都内の男計 3 人を逮捕	法人に罰金 30 万円 1 名に罰金 30 万円 ２名に罰金 20 万円

※事前に受信者の同意を得ずに、広告宣伝メールを送信したことによる直接刑事罰

MEMO

第4章
技術的な対策

第４章　技術的な対策

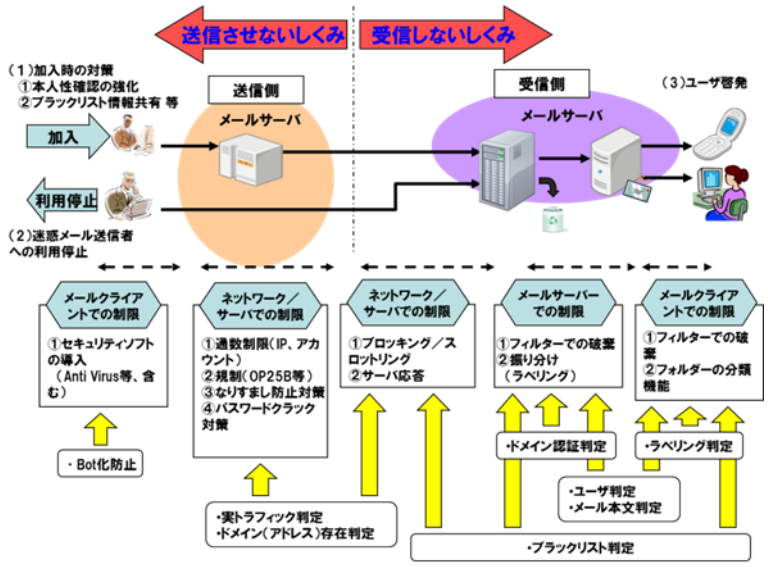
第１節　概要

迷惑メールに対しては、様々な技術的な対策が図られてきています。第２章でみた送信手法の悪質化・巧妙化に対応して、迷惑メールに対する技術的な対策も、高度化・精緻化が進んできています。本節では、迷惑メールに対する技術的な対策の概要について記述し、次節以下で、迷惑メール送信防止対策、受信防止対策、それらの対策の中で特に推奨される対策として、OP25B、送信ドメイン認証について記述します。

１　技術的な対策の概要

迷惑メールに対する技術的な対策は、送信側での迷惑メールを送信させない仕組みと、受信側での迷惑メールを受信しない仕組みの２つに大きく分けられます。実際の対策は、これらを適切に組み合わせることで、より効果が高められます。

図表４－１：技術的な対策の概要



(1)　送信させない仕組み

迷惑メールを送信させないための技術的な対策としては、１つのメールアカウントや IP アドレスからの一定時間に送信可能なメールの通数を制限する手法や、一定の方法によるメールの送信を制限する手法（例えば、第４節で説明する OP25B）などがあります。

また、迷惑メールの多くが BOT 化したパソコンから送信されている状況から、ユーザーにおける対策として、パソコンにセキュリティ対策を導入し、かつ、定期的に監査することも有効な対策となります。

特に、各種迷惑メール対策が施されたことで、不特定多数のユーザーが利用する ISP/ASP のメールサーバー等を経由して迷惑メール送信する方法が散見され始めています。

代表的な迷惑メール送信防止対策について、第２節で概説します。

(2)　受信しない仕組み

迷惑メールを受信しないための技術的な対策としては、受信側のメールサーバーの前段階で止める方法（ネットワーク／サーバーでの制限）と、受信したメールの内容から判断して処理する方法とに分けられます。受信したメールの内容から処理する方法には、メールサーバー上で特定領域に隔離したり受取拒否したりする方法(「メールサーバーでの制限」)と、受信者のメールクライアントで処理する方法(「メールクライアントでの制限」)があります。

これらの制御にあたっては、何が迷惑メールであるのかを判定する仕組みが重要となります。その判定の仕組みとしては、大量に送信されていることなど実トラヒックを元に判定する方法、送信元のドメインが実在するかにより判定する方法、事前に登録された迷惑メールの送信元のリスト（ブラックリスト）により判定する方法、ユーザーの設定したルールにより判定する方法などがあります。

迷惑メールの送信手法が悪質化・巧妙化する中で、それのみで決定的な処方箋的な対策は存在しないことから、複数の対策を組み合わせて対応することが必要となります。なお、提供するサービスによっては、通信の秘密等の法令により無条件で一律に設定できないものも存在するため、ISP 等が導入する場合には、十分な考慮が必要となります。

比較的効果が高いと想定される迷惑メール受信防止対策について、第３節で概説します。

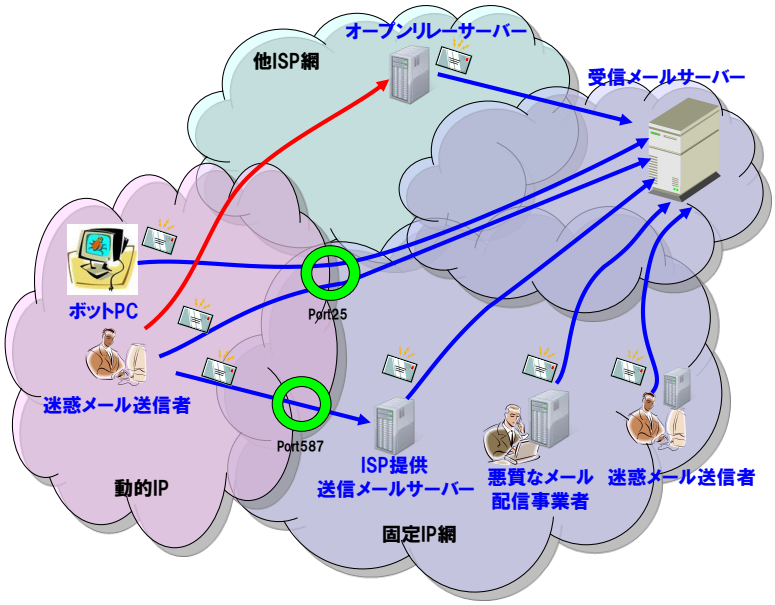
第２節　迷惑メール送信防止対策

迷惑メールの送信方法としては、動的 IP アドレスから直接送信する方法、固定 IP アドレスを取得して直接又はメールサーバーを立ち上げて送信する方法、ISP/ASP や共用ホスティングサービスの MSA を踏み台にして送信する方法、悪質なメール配信業者のメール配信サービスを利用する方法、オープンリレー（他のメールサーバーから別のメールサーバーに宛てたメールの中継が可能となっているメールサーバーで、直接の送信元を隠蔽するために利用されることも多い）可能なサーバーを経由して送信する手法などがあります。

このうち、動的 IP アドレスから直接送信する方法は、日本国内では OP25B が広く普及したことから、ほぼ制限されつつあります。また、固定 IP アドレスを取得して送信する方法や悪質なメール配信業者を利用する方法は、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しやすいといえます。また、オープンリレー可能なメールサーバーを経由して送信する方法は、従来はセキュリティに問題があるサーバーを乗っ取り、該当のサーバーを経由して送信する方法が主流でした。しかし、最近では海外にサーバーを構築し、そのサーバーを日本国内から利用して送信する方法が増えているといわれています。この方法を防止するには海外との連携が不可欠となります。

また、不特定多数のユーザーが利用する ISP/ASP や共用ホスティングサービスの MSA 経由で送信する方法で送信される迷惑メールでは、全体の通常のメールに紛れることで迷惑メールの判断が困難となることや、逆に迷惑メール送信元と受信側から判断されて通常のメールも巻き込まれて受信ブロックされることなどの問題が出てきます。このようなことから、送信側の迷惑メール対策としては、ISP/ASP が提供する MSA 経由の迷惑メール送信方法に対する対策も非常に重要となっています。

図表４－２　迷惑メールの送信経路



１　MSA の踏み台対策について

ISP/ASP や共用ホスティングサービスの MSA は該当のサービスに契約している不特定多数のユーザーの利用を前提にしていることから、その MSA を踏み台にした迷惑メールの送信を簡単に抑止する方法は存在しません。したがって、実際には、効果があると思われる方法をいくつか組み合わせて対策が行われています。

(1)　送信者認証を用いたメール送信制限

送信者認証を用いたメール送信制限とは、メールの送信時に送信者認証（SMTP AUTH）を実装し、認証に成功した者のみメールを送信可能とする方法です。これにより、万が一迷惑メールが送信されても、ISP/ASP や共用ホスティングサービスの提供者が送信者を特定しやすくなり、抑止することが可能となります。

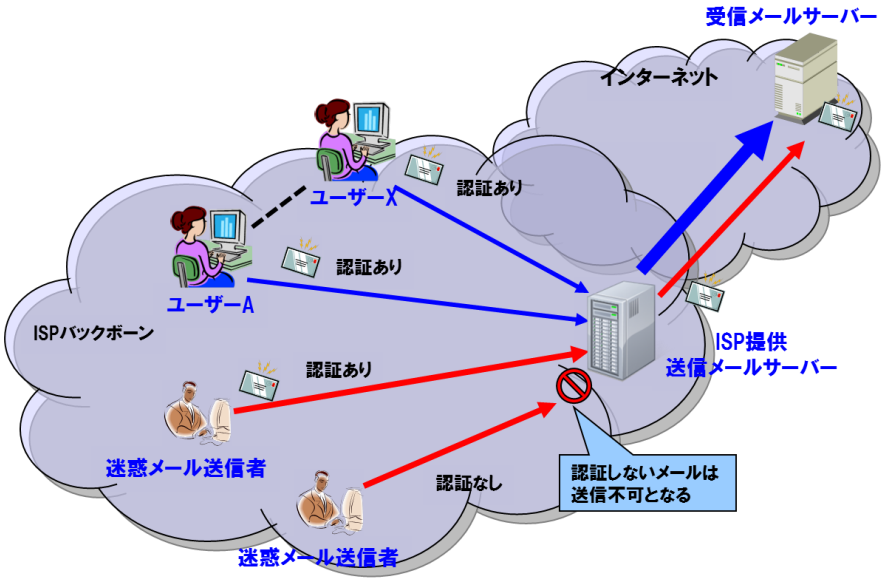
従来のメールサービスでは、(自 ISP のネットワーク内であれば）メール送信時にユーザーの認証を必要としないものが存在していました。その結果、該当の ISP に契約さえすれば、誰もが自由にメールを送信することが可能であり、迷惑メール

送信者がMSAを経由して迷惑メールを送信されても、誰がそのメールを送信したのかの特定できませんでした。これに対応するための対策が、送信者認証を用いたメール送信制限です。

送信者認証を導入するためには、ISP/ASP での対応のみならず、ユーザーのメールソフトの設定の変更も必要となるため、関係者が協力していくことが必要になります。この点については、最近のメールクライアントの多くはデフォルト設定が送信者認証を使用するとなっており、設定画面にて数カ所変更するだけで送信者認証の利用が可能となるため、利用に関する障壁はほとんどなくなってきています。

なお、送信者認証を行っても、自らのアカウントからかまわず迷惑メールを送信する送信者も存在するため、この対策のみならず、後述の対策も併せて行うことが必要になります。

図表４－３　**MSA** を踏み台にした迷惑メール送信対策



(2)　送信宛先数（通数）制限

送信宛先数（通数）制限とは、１つのメールアカウントや IP アドレスからの一定時間に送信可能なメールの通数を制限する方法です。この方法は、携帯発の迷惑メールが増えた際に、携帯キャリア各社が導入して効果を得たという実績があります。

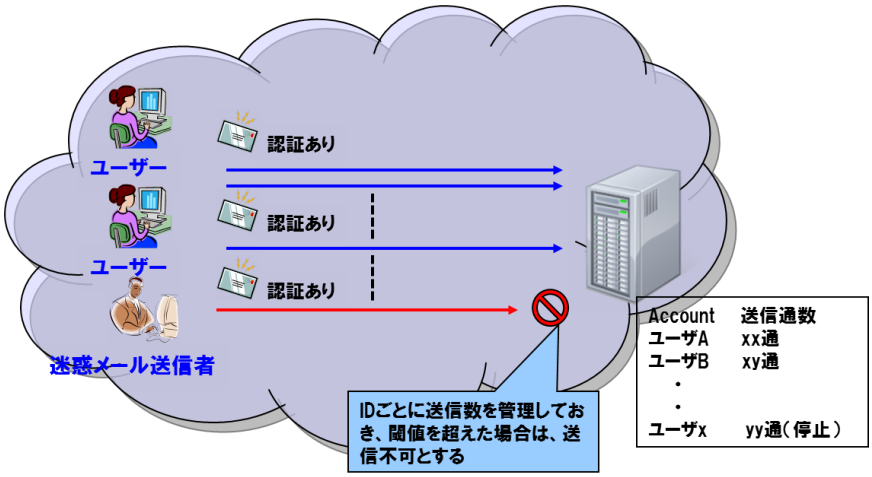
前述の送信者認証を用いて送信者を特定してメール送信制限をしても、自らのアカウントからかまわず迷惑メール送信されると、該当のアカウントを利用停止等するまでは迷惑メールを送信し続けることが可能となってしまうため、更なる対策として有効なのが、送信宛先数制限です。

送信宛先数制限は、その設定によっては、一般ユーザーの利用に影響を及ぼすおそれもあります。このため、導入する ISP/ASP では、そのような影響が出ないように、サービスごとの特徴を理解して設定することになります。特に、法人ユーザーが利用する共用ホスティングサーバーでは、該当のサーバーを利用して広告メール等を送信している場合があるため、利用目的を定めて制限する等の工夫も必要になります。また、宛先数のカウント方法は、時間単位、日単位、月単位などが考えられますが、これもサービスごとの特徴を理解して決めることが重要となります。

アカウント単位で行う送信宛先数制限では、送信者認証を行ったアカウントごとにいくつの宛先にメールを送信したかの管理を行い、設定した閾値を超えた場合に、該当のアカウントからメールを送信させないという仕組みになります。

また、送信者認証を実施しておらず、送信ユーザーを特定できない場合には、IP アドレス単位でメールを送信させないようにする方法もあります。この方法では、IP アドレスの再利用や同一 IP に複数ユーザーが利用している場合には、他のユーザーが送信したメールが巻き込まれてブロックされる可能性があるため、実施に際してアクセス形態を十分考慮することが必要となるものです。

図表４－４　送信宛先通数制限



(3)　詐称送信制限

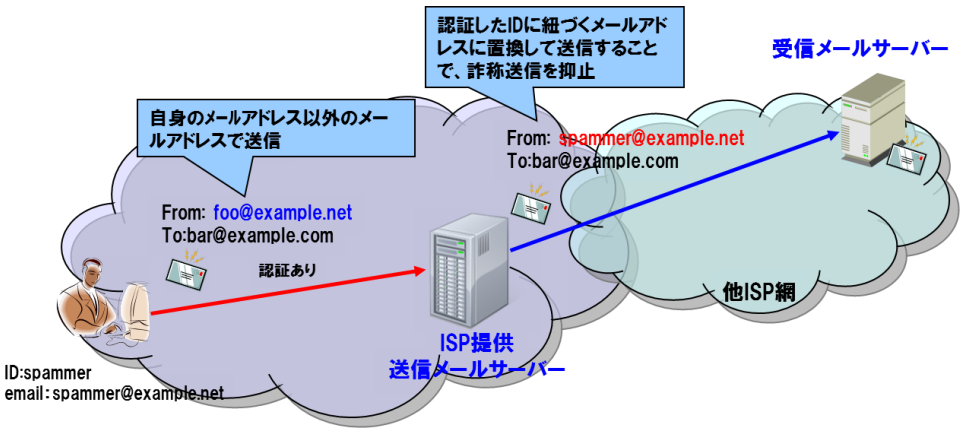
詐称送信制限とは、前述の送信者認証を実装し、かつ、送信時に認証した ID と送信者のアドレスを照合して異なる場合には、送信を許可しない、メールアドレスを書き換える等の対応をすることにより、詐称を防止する方法です。

メールを送信する際に、善悪は問わず送信者アドレスを詐称することが可能な場合が多く存在します。メールアドレスを詐称して送信された場合には、そのメールの送信者を特定しづらくなります。これに対して、この方法により対応することが可能です。

一般のユーザーはメールアドレスを詐称して送信する必要はなく、また、後述の送信ドメイン認証技術が普及しつつある現状を考えると、詐称したドメインのメールが送信されることは、送信側のドメインのレピュテーションを低下させるおそれもあることから、送信側の ISP/ASP では、この方法を導入することが望まれます。既に、一部のサービスでは、認証した ID 以外のメールアドレスからメールの送信ができない機能が提供されています。

なお、この方法が採用できない場合でも、ISP/ASP では、メールアドレスを詐称しているメールと詐称されていないメールを、別サーバーや別 IP に分けて送信することで、詐称していないメールのレピュテーションの低下を防ぐ効果を出すことが可能です。

図表４－５　アドレス変換送信



２　パスワード漏洩防止対策

１では、MSA を経由した迷惑メールを防止する方法を説明しました。そのような対策が実施されている場合に、MSA を経由してメールを送信するためには、正規の ID/パスワードが必要となります。したがって、迷惑メール送信者が ID/パスワードを入手することを抑止する方法による対策も重要です。

ID/パスワードの入手方法としては、正規にサービスに契約する方法があります。これに対しては、

加入時の審査を厳格にする、迷惑メール送信を確認した場合には利用停止にする等の運用的な対策があります。

また、PC をマルウェア等に感染させ ID/パスワードを抜き取る方法もあります。マルウェア対策としては、PC にセキュリティソフトを導入する等の対策が有効であるため、ユーザーがセキュリティ対策の意識を高めることが重要であり、関係者によるユーザーへの啓発が必要です。

さらに、メールサーバー等にパスワードクラックを行って ID/パスワードを入手する方法があります。パスワードクラックに対しては、サーバーの管理者が、クラックされていることを検知し、そのアクセスを抑止する等の技術的対策を行うことが必要となります。

なお、多くのメールサービスは、メールアドレスやメールアドレスのローカルパートを ID としている場合が多く、この場合には容易に ID が推測でき、他の認証サービスと比較すると、セキュリティレベルが低くなります。関係者は、そのような問題があることを認識しておくことが重要です。

＜以上の部分と、以下の(1)～(3)の説明部分との関係が若干わかりづらいような気がします。この最後のところで、「以下、○○について説明します。」的な記述ができないでしょうか。＞

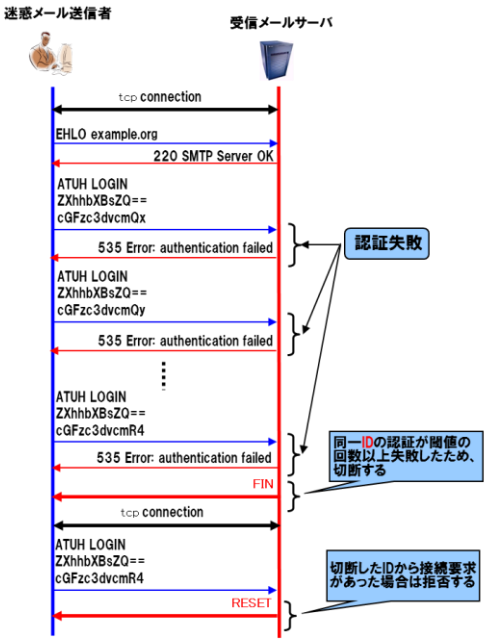
(1)　アカウントロック機能

アカウントロック機能とは、メール送受信時に入力するパスワードをあらかじめ設定していた回数を超過して失敗した場合に、該当のアカウントを一時的に利用禁止にする方法です。また、アカウントロックした際にアラームを出力することで、監視者がアタックを検知可能となる場合もあります。

パスワードクラックの代表的な方法としては、該当の ID に対してパスワードをランダムに変えて認証が成功するまでアクセスを行い取得する方法（ブルートフォースアタック等）があります。ブルートフォースアタック等に対しては、このアカウントロック機能等の対策が有効です。

ただし、Web メールのように認証時に毎回 ID/パスワードを入力するようなサービスではユーザー自身が誤って複数回パスワードを間違えることが想定されます。さらには、愉快犯が意図的に ID をロックさせるために攻撃をすることなども想定されます。したがって、導入にあたっては、ロックする際の認証失敗回数を適切に選定したり、一定時間過ぎたらロックを自動的に解除する機能を実装したりすることなどが必要となります。なお、ISP では、自動的に解除する機能を具備しない場合には、ロックしたユーザーからの問合せが増えるため、場合によっては運用負荷が増える可能性があることから、アカウントロック機能を実装する場合は、自動解除機能を具備することが望ましいものと考えられます。

図表４－６　アカウントロック機能



ID:exampleに対して、Passwordをpassword1、password2・・・と変えてパスワードクラックした例
（なお、この例では、認証方式は、AUTH LOGIN形式としている。）

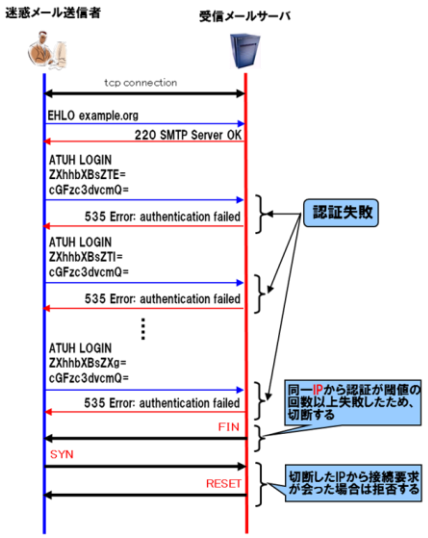
(2)　IP ブロック機能

IP ブロック機能とは、同一の IP アドレスからの認証がある一定回数以上失敗した場合に、該当の IP からの接続を拒否する機能です。

ユーザーがパスワードを設定する場合に、安易な設定が散見されるという報告もあります。そのため、ブルートフォースアタック等では、1 つの ID については数回ずつのアクセスとして、多数の ID に攻撃してくるケースがあります。この方法を行うと、前述のアカウントロック機能は効果がなくなり、繰り返し攻撃することでパスワードを取得されてしまう可能性が高くなります。したがって、さらなる対策として、この IP ブロック機能が有効となります。

同一の IP からある単位時間に多数の ID にアクセスすることは通常はありえないため、複数の ID に対して認証を失敗した場合には、該当の IP アドレスからのアクセスをブロックすることが有効です。また、存在しない複数の ID に対して接続要求することも通常はありえないため、このようなアクセスが行われた場合には、該当の IP アドレスからのアクセスをブロックすることも有効です。

図表４－７　**IP** アドレスブロック機能



IDを:example1、example2・・・と変えて、パスワードクラックした例
（なお、この例では、認証方式は、AUTH LOGIN形式としている）

(3)　その他の対策

ブルートフォースアタック等を行うためには、攻撃するための ID を入手する必要があります。多くのメールサービスでは、メールアドレスを元に ID を提供していることが多いため、そのサービスを理解すれば、存在しそうなメールアドレスから容易に ID を特定できます。これに対しては、ID をメールアドレスに紐付かないものにする方法が有効です。この場合には、併せて、存在しない ID で一定回数以上アクセスして来た場合に、前述の IP ブロック機能を動作させることで、その効果をさらに高めることが可能です。

また、パスワードを長くすることや英数字記号を組み合わせたパスワードにすることで、パスワードがマッチする可能性が低くなりブルートフォースアタック等の成功率は格段に下がるといわれています。したがって、ユーザーが、長いパスワードや英数字記号を組み合わせたパスワードなど強固なパスワードを設定することが重要です。また、ISP 等側で、パスワードの最低長を定め、短いパスワードを取得できないようにすることや、パスワード取得の際に、英数字記号を１文字ずつ必須とすることも有効です。また、すでに導入済みのシステムで容易に変更できない場合でも、ユーザーに対して、パスワード設定に関する注意喚起をすること（例えば、パスワード設定画面に注意事項を出す等）である程度の効果が期待できます。

３　転送メール対策

ISP/ASP のメールサービスを始め、多くのメールサービスが、メールをあらかじめ設定したメールアドレスに転送する機能を具備しています。

しかし、メール転送は受信したメールを転送するため、転送するメールの正当性を判断していないケースがほとんどといえます。

したがって、メール転送設定しているユーザーが多数の迷惑メールを受信した場合には、迷惑メールそのものが転送されることとなり、転送しているメールサーバー自身が迷惑メール送信者になる可能性が出てきます。このため、メール転送を行う場合にも、迷惑メール対策を施すことが望まれます。

(1)　フィルタリング転送

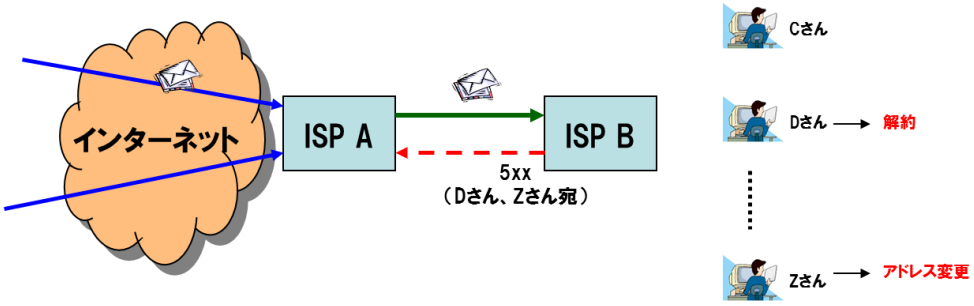
メール転送設定をしているユーザーが多数の迷惑メールを受信した場合には、転送メールにも多数の迷惑メールが含まれることとなり、結果として、転送サーバー自身が迷惑メール送信サーバーとみなされ、転送先で受信拒否される場合があります。この場合は、転送しているユーザーだけではなく、該当の転送先と同じドメインに転送している他のユーザーのメールも巻き込まれてブロックされる可能性があります。

この問題を回避するためには、ユーザーが、メール転送サービスを利用する場合には、迷惑メールフィルター等で迷惑メールでないと判別したメールのみを転送する等の回避策が考えられます。また、ISP/ASP で、メール転送サービスを提供する際に、そのような機能を提供したり、その機能の利用を必須としたりすることが考えられます。

(2)　転送設定解除機能

転送先のメールアドレスを変更・解約等した場合には、ユーザーは、転送設定の変更・解除を行う必要があります。この設定の変更・解除を忘れると存在しないアドレスに転送し続けることになります。

図表４－８：転送先アドレス変更との問題



- **ISP A から ISP B にメール転送を実施しているユーザが解約やアドレス変更をした場合、ISP Aで行っている転送設定を変更する必要がある。**
- **この変更を行わない場合には、ISP A で受信したメールは、それ以後も ISP B に転送し続けられるが、ISP B では存在しないユーザであるため、5xxのエラー応答を実施する。**
- **解約やアドレス変更をしたユーザが少なければ、存在しない宛先のメールはわずかな通数にとどまるが、 ISP B で解約やアドレス変更したユーザが増えると、存在しない宛先へのメールも徐々に増加し、その結果、場合によっては ISP B で受信拒否をされることとなる。受信拒否をされると、他の転送メールも拒否されることとなり、メールの遅延につながる。**

存在しないメールアドレスへのメール送信が少ない場合はさほど問題にはなりませんが、これが増え続けると、受信側では存在しないあて先に多数のメールを送信してくるために規制することがあります。特に、メール転送用のサーバーを個別に準備している場合には、本問題が発生しやすくなります。

また、該当のユーザーが元のメールをサーバーに残さずに転送する設定を行っていた場合には、該当ユーザーに送信されたメールは、転送元ではなく送信元にエラーメールと返信されることとなり、ユーザーは転送に失敗しているメールがあることを認識できず、転送設定の変更・解除を忘れていることに気づかない可能性もあります。

さらには、転送に失敗したことで、送信者に返信されたエラーメールは、送信者が実際に送信した宛先のメールアドレスではなく、見知らぬメールアドレスへの送信に失敗したというものになることから、送信者はエラーメールを受信して困惑する可能性もあります。

これらの問題に対する技術的な解決方法として、転送元のメールサーバーで、ある一定回数以上転送が失敗した場合は、転送機能を解除する機能が考えられます。

(3)　転送アドレス書き換え機能

メールを転送する際は、多くのメールサーバーでは転送元のメールアドレスをそのまま用いて転送しています。

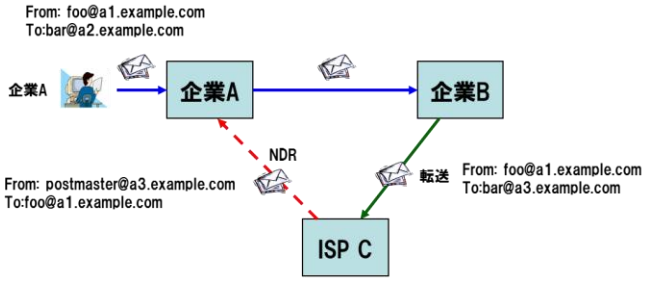
また、メールサーバーでは、存在しないメールアドレスにメールを送信された場合にエラーメールを返します。このエラーメールは、通信上の応答でエラーが返った場合は転送元が、転送先で一旦受信した後にメールアドレスの存在を判断した場合は転送先で、返すこととなります。

前者の場合には、転送元で転送に失敗したことが判断可能となり、前述の転送設定解除機能で対応することができます。一方、後者の場合には、転送元では転送に失敗したことが判断できずに、存在しないメールアドレスにメールを転送し続けることになります。

これに加え、転送元では送信元のメールアドレ

スを用いてメール転送することとなるため、転送先のサーバーが、後述する送信ドメイン認証技術を導入していた場合には、認証が失敗するという問題も発生します。もし、転送先で送信ドメイン認証技術による認証に失敗したメールを拒否するような機能を具備していた場合には、転送したメールは届かなくなります。

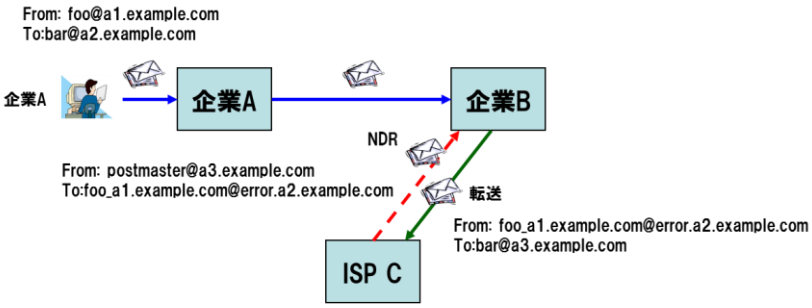
図表４－９：転送失敗時のエラーメール送信先の問題



- 企業A の“foo@a1.example.com”から、企業B の“bar@a2.example.com”にメールを送信。
- 企業B の “bar@a2.example.com” は、ISP C の “bar@a3.example.com” にメール転送設定をしているので、該当のアドレスにメールが転送される。このときの送信アドレスは、企業A の “foo@a1.example.com” になる。
- ISP C で、何らか理由で “bar@a3.example.com” 宛てに転送されたメールを受信できなかった場合には、ISP C から “foo@a1.example.com” 宛に “bar@a3.example.com” にメールが送信できなかった旨のエラーメールが送信される。
- 企業A の “foo@a1.example.com” は、企業B の “bar@a2.example.com” は、受信したメールを、ISP C の “bar@a3.example.com” のアドレスに転送していたことを知ることになる。
- エラーメールは、ISP C から 企業 A に送信されるため、企業B では、存在しない宛先へメールを送信(転送)しているという事実を知ることができない。

これらの問題を解決する方法として、メール転送する際に、メールの送信元アドレスを、転送元のメールアドレス等で書き換えて送信する方法があります。これにより、転送に失敗したことをメールの転送をする側で管理可能となり、前述の転送設定解除機能で転送設定を外すことなどの対応が可能になります。

図表４－１０：転送アドレス書き換えによる、転送失敗の検知対策



- 企業A の “foo@a1.example.com” から、企業B の “bar@a2.example.com” にメールを送信。
- 企業B の “bar@a2.example.com” は、ISP C の “bar@a3.example.com” にメール転送設定をしているので、該当のアドレスにメールが転送される。このときの送信アドレスを、企業B で管理するドメインに書き換える。なお、この際に、どのアドレスからのメールを転送したかを分けるように規則性を持たせることで、送信失敗時の管理が容易になる。
- ISP C で、何らか理由で “bar@a3.example.com” 宛てに転送されたメールを受信できなかった場合には、ISP C から、企業B で書き換えを行ったアドレスにエラーメールが送信される。
- 企業B では、どのユーザのメールが転送に失敗したかの管理が可能となり、継続的に転送に失敗した場合などに、該当の転送設定を解除すること等により、不要なメール転送を防ぐことが可能となる。

第３節　迷惑メール受信防止対策

迷惑メールの送信方法は巧妙化しており、受信側で一つの対策で防ぐことはほぼ不可能となりつつあります。したがって、複数の受信防止対策を組み合わせて対応することが有効となります。

１　実際のトラヒックを元にしたネットワークレベルの制限

特定の送信元から大量に送信される迷惑メールは、受信側のメールサーバーの負担も大きく、通常のメール受信にも影響を与えることが多いため、受信側のメールサーバーで、実際のトラヒックを元にして、大量送信を検知し、極端な接続要求を行う送信元のメールサーバーからの接続を制限する手法が採られています。この手法は、ネットワークレベルでの制限として行われるものであり、接続をブロックするという意味で「ブロッキング」と呼ばれるものと、接続を絞るものをという意味で「スロットリング」と呼ばれますものがあります。例えば、特定の送信元（IP アドレス）から同時に多数の接続を要求する場合や、短時間に接続要求を頻繁に繰り返す場合、存在しないあて先に多数のメールを送信して来る場合などには、この機能が有効になります。

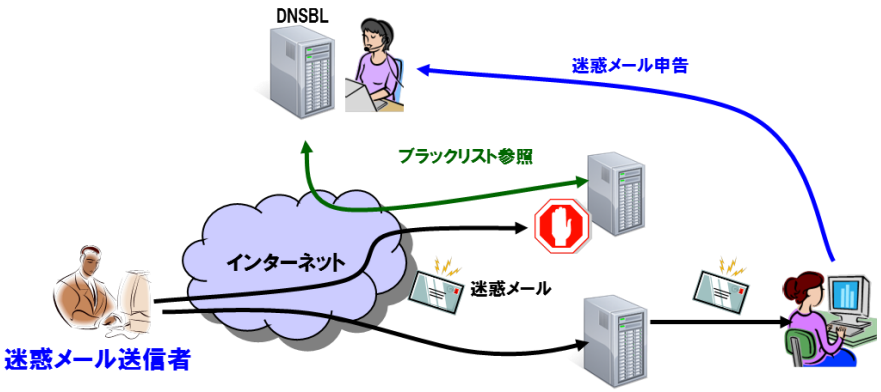
ただし、ISP/ASP のサーバーを踏み台にして大量に送信された場合に本機能を実行すると、正常のメールも巻き込まれて拒否されるという問題（お隣さん問題）がありますので、実際に機能させる場合には注意が必要なものです。また、この手法については、特定の IP アドレスからの大量送信がある場合には有効ですが、通常１台のＰＣからは大量送信を行わないボットネットを利用した迷惑メールの送信への対応が困難であるという問題があります。なお、そのような送信手法にも非常に有効な技術として、第 2 節で述べる OP25B があります。

また、ブロッキング等されないために、1 つの IP から送信するメールの量を制限し、送信元の IP 数を増やして迷惑メールが送信される場合があります。この場合も、この方法による迷惑メールへの対応が困難となります。ただし、送信元のメールアドレスやドメインが同じ場合には、該当のメールアドレスやドメイン単位でブロッキングやスロットリングすることで対応が可能です。この方法は、IP アドレス単位の対策と異なり、ISP/ASP のサーバーを踏み台にされても、（前述の送信宛先規制がされていれば）正常なメールは影響を受けないという利点もあります。

２ブラックリスト

頻繁に迷惑メールの送信を繰り返す送信元に対応するための対策として、迷惑メールの送信元の IP アドレスや、オープンリレー設定になっているメールサーバーの IP アドレスを収集し、その情報を受信の拒否や迷惑メールの判定基準の一部として利用する手法があります。この手法は、DNSBL(DNS Block List / DNS Blackhole List)と呼ばれています。

図表４－１１：ブラックリストによる対応の概念



ブラックリストによる対策には様々なものがあり、ネットワークレベルでの制限、メールサーバーでの制限、メーラーでの制限などそれぞれの段階で使用することが可能です。ブラックリストの多くは、迷惑メールの送信元の IP アドレス等を収集し、ドメイン名の名前解決などに広く使われて実績のある DNS の仕組みなどを利用して受信側のメールサーバー側へ提供されています。これにより、受信側のメールサーバーで最新の情報をリアルタイムに確認できるようになっています。ブラックリストに含まれる送信元からのメールについては、受信側のメールサーバーで、受信の拒否（ネットワークレベルでの制限）やフィルターでの破棄（メールサーバーでの制限）のための判定

基準の一部として利用することができます。

しかし、この DNSBL については、登録基準や解除方法が不明瞭なものがあるなどの問題が指摘されています。DNSBL に一旦登録されてしまうと、登録された IP アドレスからの電子メールは、DNSBL を利用している受信メールサーバーに全く届かなくなってしまう場合があります。また、ボットネットを利用して送信される迷惑メールは、DNSBL に登録されていない送信元（IP アドレス）からの送信であることも多く、この手法では対応できない場合があるという問題もあります。この問題に対しては、ボットネットなどに使われる動的 IP アドレスの範囲を収集しようという動きもあります。

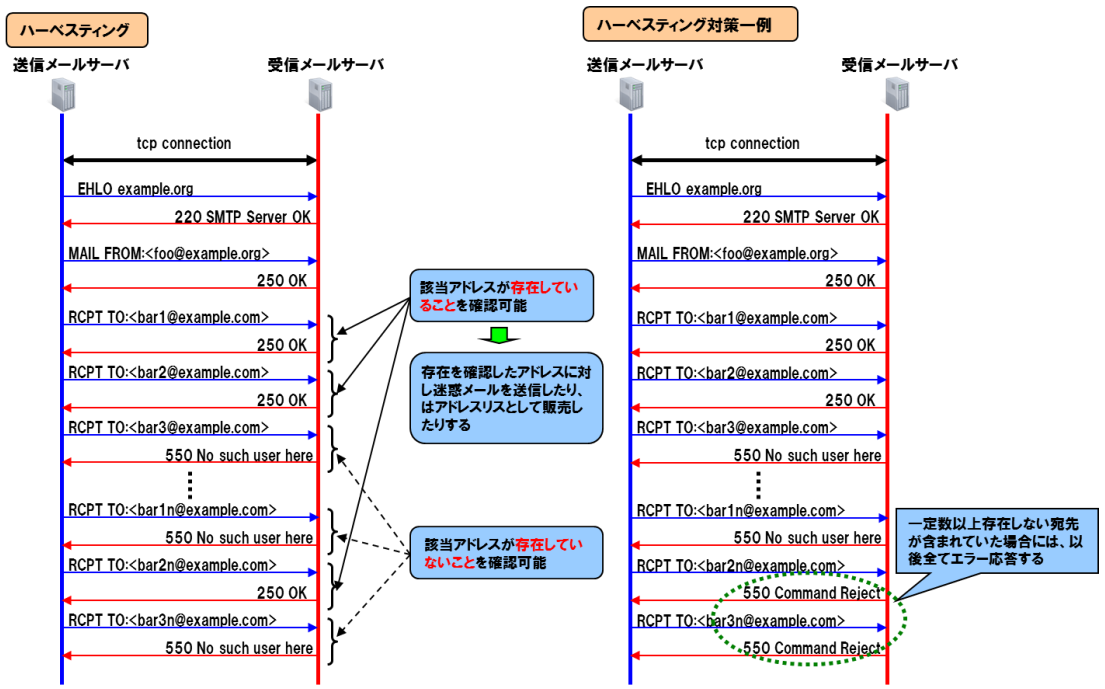
このように、DNSBL の利用は、受信側メールサーバー等において、ネットワークレベルで受信を拒否できるため、受信側の負担を小さくできるという利点があります。その一方で、誤って登録された場合の弊害は、登録された送信側だけでなく、必要なメールが受け取れなくなってしまう受信側にも及びます。DNSBL を参照する機能は、受信側で用いる迷惑メール対策製品の機能の一部として含まれることもあるため、判定基準の内容については注意が必要です。

さらに、IPv4 アドレスの枯渇により、IP アドレスの再利用が頻繁に行われているため、新たにメールを送信しようとした時点ですでに DNSBL に登録されていてメールが送信できないという問題も出てきています。したがって、解除の更新が頻繁に行われない DNSBL を使用する際は、より注意が必要となります。

３　ドメイン（アドレス）の実在確認

メール配送時には、メール本文以外にも幾つかの情報がやりとりされています。メールの届け先である受信者のメールアドレスは、メール本文のヘッダーに指定されているものではなく，別途メール配送時に個別指定することになっています（第１章の topics「電子メールの仕組み」を参照。）。受信側メールサーバーからは、宛先のメールアドレスが実在しない場合には、その旨を送信側メールサーバーに応答する（エラー応答する）ことになります。この仕組みを悪用すれば、メール配送時の宛先の指定で、宛先となるメールアドレスを大量に指定することにより、それらのメールアドレスが実在するかどうかを確認することができます。メールアドレスを収集する（harvest）という意味でハーベスティングとも呼ばれています。

図表４－１２：ハーベスティング



このような行為に対しては、宛先や送信元のドメイン（アドレス）の実在性を判定することにより、受信メールサーバーで行うことができるいくつかの対策があります。

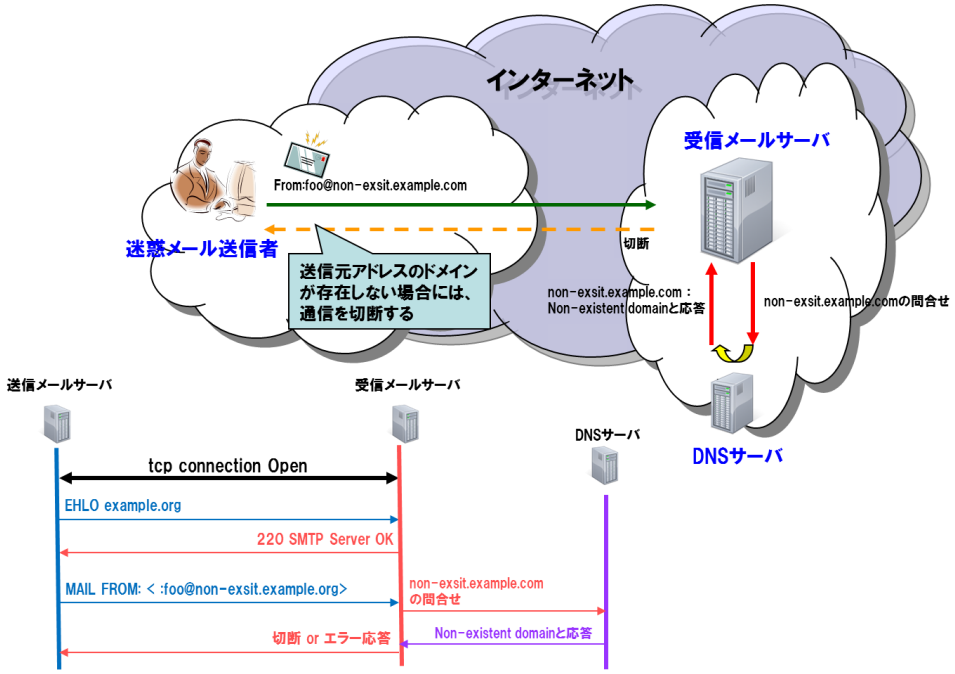
まず、指定された宛先メールアドレスが複数の場合であって、それらのうちに一定数以上存在しないものが含まれるときには、そこで処理を止め、メールを受信者に配送せずに、送信メールサーバ

ーに対してエラーを応答するという手法があります。

また、宛先メールアドレスが実在しない場合でも、そのアドレスが存在しないことを示すエラーの応答を送信メールサーバーに返さないことにより、アドレスの存否の確認ができないようにする、という手法もあります。しかし、受信メールサーバーが送信メールサーバーからのメール配送時にエラーを返さずにいったんメールを受け取ってしまった場合に、その後宛先不明などで配送できないことが分かれば、エラーメールを返す必要があります。このことにより別の問題が発生しますが、このエラーメールの問題については、別途詳しく述べます（第５節の topics「エラーメール問題の仕組み」を参照）。

さらに、メール配送時に指定する送信元のメールアドレスの実在性を確認する手法もあります。具体的には、送信者情報を偽装して送信される迷惑メールに対応するため、送信元のメールアドレスに含まれるドメインの実在性を確認し、ドメインが存在しないことが分かった場合には、メール本文の受信をせずに、送信メールサーバーにエラーの応答を返すものです。なお、この手法では、実在するドメインを用いた送信元のメールアドレスの偽装には対応できませんが、そのような場合を含めて、送信元のドメインの偽装にさらに有効な技術として、第５節で述べる送信ドメイン認証技術があります。

図表４－１３：送信元ドメインの確認の例



４　フィルタリング

受信したメールが迷惑メールかどうかについて、メールのヘッダー情報（タイトルや送信者情報、日付や配送経路など）や本文の内容、添付ファイルなどの情報などから判定し、該当するメールを破棄したり振分けしたりする手法があります。この手法が、メール内容によるフィルタリングです。

(1)　利用者設定のフィルタリング

この手法の一つとして、利用者が受信したくない送信者のメールアドレスなどを登録することによるフィルタリングがあります。様々なプロバイダ等において、指定拒否機能等として提供されています。しかし、迷惑メールの送信者は送信元を頻繁に変えることが多いことなどから、利用者がそのすべてに事前に対応することは困難であることも指摘されています。

利用者設定のフィルタリングには、利用者が受信許可したメールアドレスなどからのメールのみを受信する許可型のフィルタリングもあります。許可型のフィルタリングは、後述の送信ドメイン認証技術と組み合わせることで、迷惑メールを完全に遮断することができるようになります。しかし、この方法では、事前に許可したメールアドレス等以外からのメールが受信できなくなってしまうという問題があります。

(2)　受信メールサーバーでのフィルタリング（迷惑メールフィルター）

利用者の設定により判断をするのではなく、セキュリティベンダー等が提供するソフトウェア等を用いて判断をする、より高度なフィルタリング

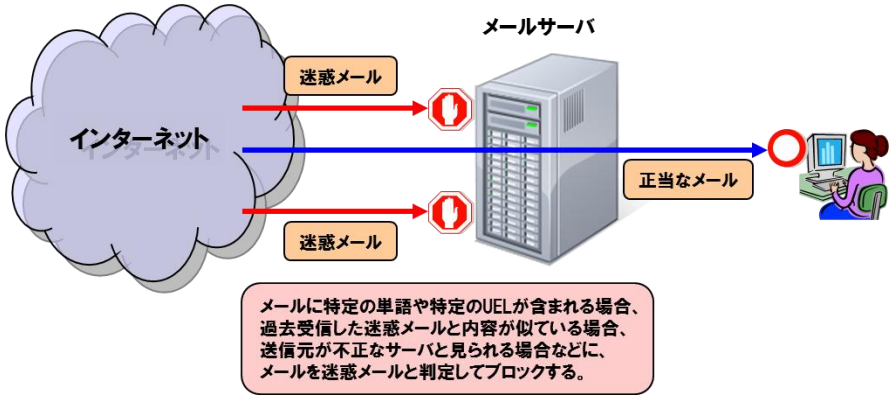
の手法があります。
　例えば、メールのヘッダーや本文に含まれている様々な情報の中から迷惑メールに典型的な特徴や経路情報（メールが配送されてきた道筋（サーバー）を示す情報）の矛盾などをスコア化し、一定基準を超えるかどうかで迷惑メールを判定する手法があります。また、メール本文から、迷惑メールや通常のメールで使われる単語や語句の出現頻度などをそれぞれ自動的に学習したり、迷惑メールに典型的に用いられる文字列（誘導先の URL 情報など）を自動的に学習したりして、確率的に迷惑メールらしさを判定する手法もあります。しかし、次のような手段により、フィルターの判定が回避されることもあります。確率的手法により迷惑メールを判断するソフトウェアは、オープンソースで提供されることが多く、迷惑メールの送信側が事前にその判定手法を解析できるため、判定を回避させる新たな手段を検討できることも要因となっているようです。

・視覚的に形が似ている文字（例えば数字の 0 とアルファベットの O など）を代わりに利用すること
・一般的なニュース記事などを添付することで単語の出現頻度を混乱させること（通常のメールで用いられる単語の頻度が上がる）
・文字列を画像として添付すること

　最近新しい技術として、多くの迷惑メールから、あらかじめ迷惑メール特有の特徴を抽出し、受信したメールと比較を行うことで迷惑メールを判定する手法が用いられています。迷惑メール特有の特徴（シグニチャー）を抽出してデータベース化することから、シグニチャーフィルターと呼ばれます。メール本体のどの部分を特徴として取り出すか、それらをデータとしてどのように表現するか、更新をどの程度頻繁に行うかがフィルターの性能に大きく影響します。
　なお、迷惑メールフィルターは、メールの特徴で迷惑メールと判断するため、正常なメールも迷惑メールと判定してしまう（誤判定：False Positive）おそれがあります。したがって、ユーザーは、フィルタリングサービスの利用の際には、それを十分に認識することが必要です。また、プロバイダ等は、サービスを提供する場合には、誤判定する可能性があることを十分周知するとともに、ユーザーが必ず受信したいメールを受信することを可能とするために、ホワイトアドレス機能を具備することが必要となります。

(3)　フィルターの判定結果の利用方法
　迷惑メールフィルターの判定結果は、メールのヘッダー部分に迷惑メールと識別できるような文字列（例えば、[meiwaku]という文字列）を記録したり（ラベリング）、迷惑メールと判定されたメールを通常のメール保管領域外（例えば、隔離領域や迷惑メールフォルダー）に隔離したり（フィルタリング）して利用されます。メールヘッダーに判定結果が記録される場合には、受信者のメールソフトウェアが提供する機能を用いることにより、迷惑メールと判断されたメールを自動的に特定のフォルダーに振り分けるように設定することなどによって、受信者のメールの選り分けの手間を軽減することもできます。
　しかし、迷惑メールと判定されたメールを受信することとなり、そのための設備が必要となるため、迷惑メールと判定されたメールの保存期間を短くして設備数を削減する等の対応が取られています。また、迷惑メールと判定されたメールは全て破棄し、破棄されたメールのレポートを利用者に送信する対応もあります。迷惑メールの流量は日々増加しており、迷惑メールを受信するための設備という本来不要な投資が増えることとなるため、結果の取扱いについては考慮が必要となります。

図表４－１４：受信メールサーバーでのフィルタリング



第４節　OP25B（Outbound Port25 Blocking）

1　概要

(1)　動的 IP アドレスからの直接送信

インターネットへの接続するためには ISP と契約を行い接続することになります。接続する際には、接続する都度 ISP から割り当てられる（動的に割り当てられる）IP アドレス（動的 IP アドレス）を用いる場合と、固定的に割り当てられている IP アドレス（固定 IP アドレス）を用いる場合があります。ISP がユーザーに提供するインターネット接続サービスでは、通常、IP アドレスが動的に割り当てられますので、一般の個人のユーザーの多くは、動的 IP アドレスを用いています。迷惑メールの送信に際しては、インターネットが広く普及し、安価で容易に高速インターネットに接続可能になったことで、動的 IP アドレスを用いることが多くなっています(「動的 IP アドレス」と「固定 IP アドレス」については、用語解説参照。)。

また、ISP を用いてインターネットに接続しているユーザーは、通常、メールを送信する際には、インターネット接続に用いる ISP のメールサーバーを用いています。しかし、現在の迷惑メールの多くは、このようなメールサーバーを用いずに、直接外部のメールサーバー（受信側メールサーバー）に宛てて送信されています。

このような傾向は、迷惑メールに対する対策を採りづらくするために行われるものです。動的 IP アドレスの多くは、接続するたびに割り当てられる IP アドレスが変更されるため、受信側では誰が迷惑メールを送信しているのかを特定することが困難になるからです。また、接続に用いる ISP（迷惑メール送信者と契約している ISP）のメールサーバー（投稿用メールサーバー）を経由せずに、受信側メールサーバーに直接に送信を行うことにより、接続に用いる ISP からも、送信行為を把握することが困難になるものです。

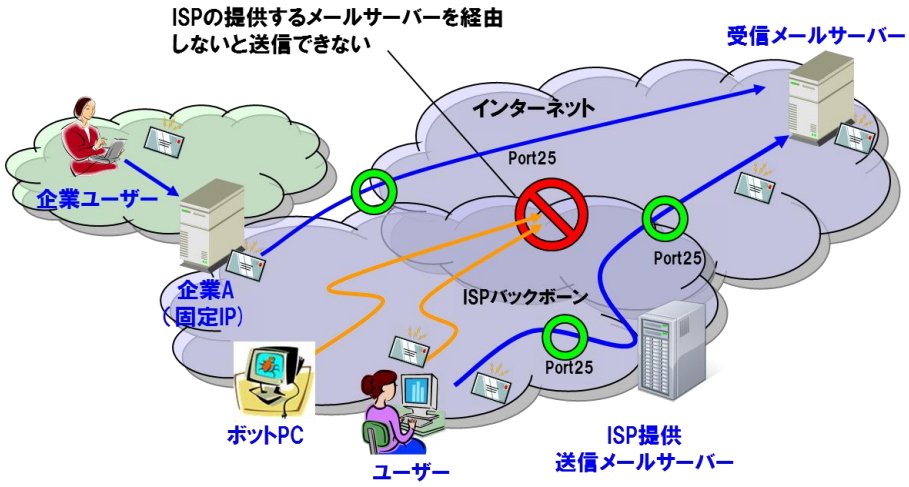
また、ボットネットを利用した迷惑メールの送信が増加しているのも、一つの要因と考えられます。ボットの多くは、一般ユーザーが使用する PC であり、それらの多くには動的 IP アドレスが割り当てられています。ボットネットを利用した送信では、ISP のメールサーバー（投稿用メールサーバー）を用いず、受信側メールサーバーに直接送信されることが多いという特徴があります。

このような迷惑メールの送信手法に対する有効な対策として、OP25B という技術があります。

(2)　OP25B の概要

OP25B は、発信元 IP アドレスが動的 IP アドレスである場合に、外部に向けた通信のうち、当該 ISP が設置するメールサーバー（投稿用メールサーバー）を用いずに、受信側メールサーバーの 25 番ポート（Destination Port 25：メールの通信であることを識別するために用いられる番号）に向けて行われるものを送信側の ISP で遮断する方法です。送信側の ISP で OP25B が実施されている場合には、受信側メールサーバーに直接送信される動的 IP アドレスを発信元とする迷惑メールを完全に遮断することができます。

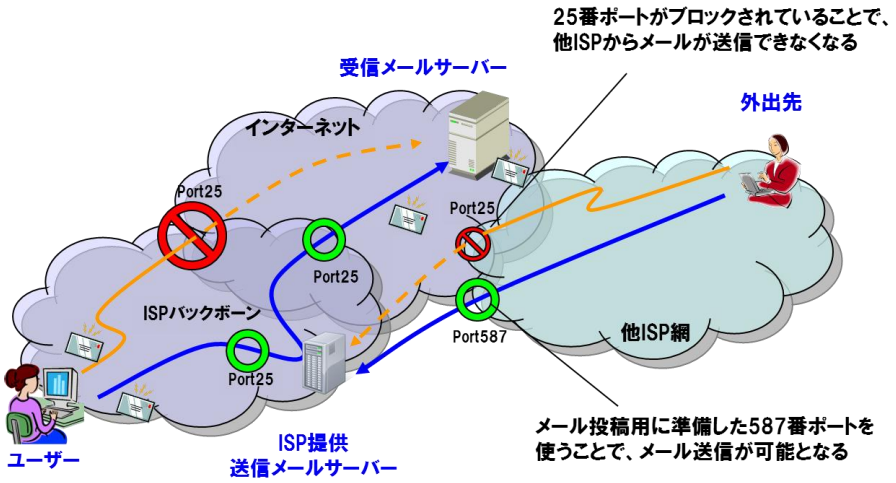
図表４－１５：**OP25B** の概要



なお、OP25B を実施した場合には、動的 IP アドレスを割り当てられている送信者が、インターネット接続を提供している ISP 以外の ISP のメールサーバーからメールが送信できなくなるという問題があります。例えば、外出先でインターネットに接続して、いつも用いている ISP のメールサーバー（投稿用メールサーバー）からメールを送信しようとした場合に、インターネットへの接続を提供する ISP が自分の契約している ISP ではなく、かつ、接続を提供する ISP で OP25B を実施していると、投稿用メールサーバーに接続できなくなります。

この問題を解決するために、多くの ISP では、25 番ポートとは別に、送信者の認証をして用いられるメール投稿用のポートを準備し、提供しています。さらに、第 2 節で説明した、送信者認証を用いたメール送信制限、送信宛先数制限、詐称送信制限を実施する事で、迷惑メールの送信をさらに抑制出来る事になります。

図表４－１６：**587** 番ポート（**Submission Port**）



用語解説

1　メールアドレスとドメイン

１ メールアドレスとドメイン

メールアドレスは、foo@example.com というように表現されます。ここで、@の左側の部分（foo）は、手紙でいえば名前にあたるもので、ローカルパートと呼ばれます。また、@の右側の部分（example.com）は、手紙でいえば住所にあたるもので、ドメインと呼ばれます。

2　動的 IP アドレスと固定 IP アドレス

IP アドレスは、インターネットで通信を行う際に、通信を行うそれぞれの機器を判別するための番号です。ICANN(The Internet Corporation for Assigned Names and Numbers）という組織を中心として、世界的に管理が行われ、使用権限の割当てが行われています。

この IP アドレスのうち、インターネットに接続する都度、契約した ISP から自動的に接続した機器に設定されるものを動的 IP アドレスと呼びます。動的 IP アドレスは、その ISP が使用権限を有する（所有する）IP アドレスの中から割り振られるため、接続する都度異なる IP アドレスが付与されることが多いものです。個人の利用者のインターネット接続では、動的 IP アドレスが用いられるのが一般的です。

これに対して、固定 IP アドレスとは、契約した ISP から契約者がインターネットへの接続用に用いるものとして使用権限を与えられている（払い出される）IP アドレスです。契約者は、払い出されたアドレスを、インターネットに接続するために用いる機器に登録します。インターネットで提供しているサービス（例えば、インターネットでのウェブページなど）では、IP アドレスが変わると突然接続できなくなるという問題が発生することや、アドレスの管理が煩雑になることから、固定 IP アドレスが使われるのが一般的です。

動的 IP アドレスでは、同じ IP アドレスであっても、時間の経過により、別の者が用いるようになっていることも多いため、接続元の IP アドレスが分かったとしても、実際に誰が使っているか判りづらいという問題があります。一方、固定 IP アドレスでは、ISP がその IP アドレスを払い出した契約者が自明のため、誰が使っているかを特定しやすくなっています。

3　ポート番号（25 番ポートと 587 番ポート）

ポート番号とは、データ通信を行う際に、通信の種類（例えば、メールなのか、ウェブなのか等）を特定するための番号です。このポート番号は、0 から 65535 まで（216 個）あり、このうち 0 から 1023 まで（210 個）の番号は、よく使われる番号として、Internet Assigned Numbers Authority（IANA)という機関で統一的に定義されています。

例えば、メールのプロトコルである SMTP では 25 番ポートを使うことが、IANA で定義されています。メールを送信する際に 25 番ポートで接続を要求すると、接続先のメールサーバーでは、この接続がメール送信の要求であると判断して、メールのやりとりのための応答を返します。

なお、メールでは、ユーザーがメールクライアントを使ってメールの送信をする際も、メールサーバー同士が通信をする際も、同じ SMTP プロトコルで通信をするため、すべて 25 番ポートを使うのが一般的でしたが、最近では、ユーザーがメールを送信（投稿）する際には、587 番ポートを使うことが推奨されています。この 587 番ポートは、Submission Port と呼ばれ、IANA により、メールを投稿するためのポートとして定義されています。

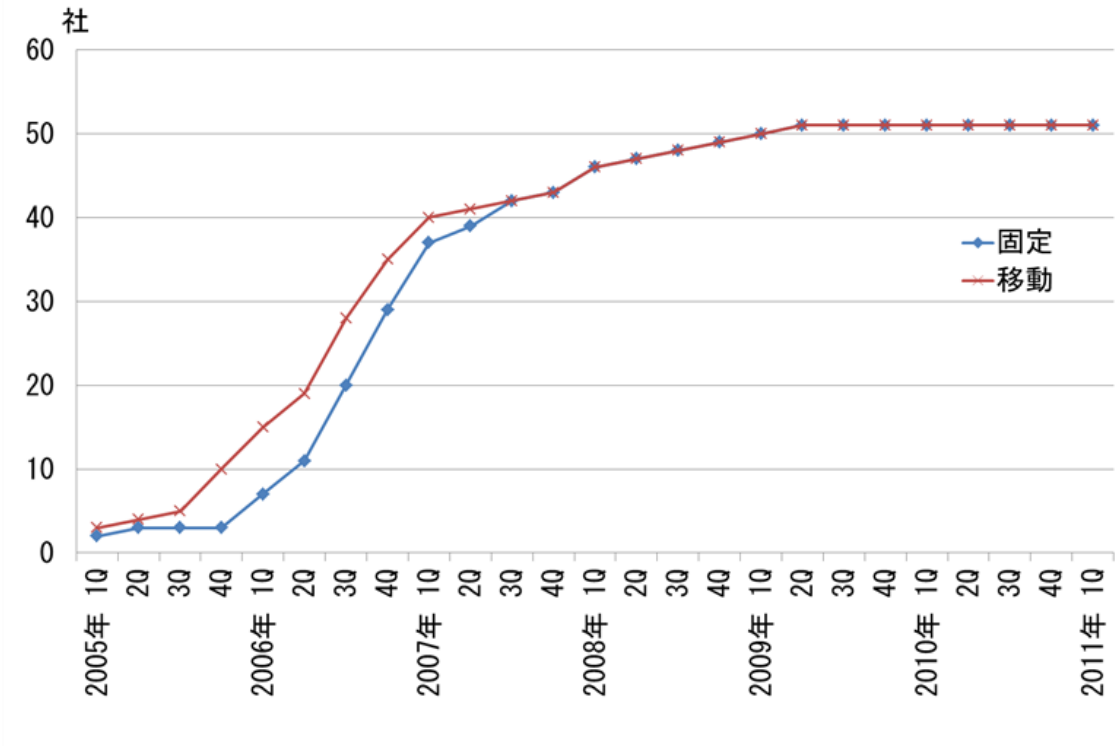
2　導入の状況

OP25B は、元々は米国の一部の ISP で採用されていた技術です。我が国では、平成 17 年（2005 年）に最初に導入され、平成 23 年(2011 年)3 月時点で 52 社の ISP で導入されています。国内の大手 ISP の大部分が OP25B を採用しており、迷惑メール対策としては最も成功した事例の一つとなっています。

OP25B については、JEAG（Japan Email Anti-Abuse Group）による OP25B 導入に際しての技術的留意点をまとめた Recommendation の発表、各種講演における効果の説明などの活動や、総務省による OP25B の導入に関する法的な整理の公開が、その普及を後押ししました。

図表４－１７：**OP25B** の導入状況

導入ＩＳＰ数



3　OP25B 導入後の課題

日本国内では多くの ISP が OP25B を導入して効果を上げてきましたが、まだいくつかの課題が残っています。

(1)OP25B 未実施の ISP 等

OP25B を実施していない一部の ISP からは、未だに迷惑メールが送信されている状況にあります。また、OP25B を実施済みの ISP でも、すべての接続に対しては実施されていない場合があり、これら未実施のポイントが迷惑メール送信者に狙われていることも確認されています。日本国内発の迷惑メール削減のためには、OP25B 未実施の ISP は OP25B の導入を、未実施ポイントのある ISP は OP25B の完全実施をすることが不可欠です。

海外等で迷惑メールをブロックする際に、迷惑メールの受信を受けて該当の IP アドレスを含む IP アドレスレンジで行う場合があります。この際に、迷惑メールを送信した ISP のアドレスレンジが拒否されるのであれば当事者同士の問題ですが、より大きな IP アドレスレンジでブロックすることで、当該の ISP 以外のアドレスが拒否される恐れもあります。したがって、迷惑メールの送信を見過ごすことは、他社のメールトラフィックに対しても影響を及ぼすことありますので、OP25B 実施にあたっては、自社の都合のみならず他社への影響も考慮して実施の可否を検討することが望まれます。

(2)海外への普及

日本では、大手 ISP を中心に、迷惑メールを送信させないことが迷惑メールを減少させることと考え、OP25B の導入が広がりました。しかし、残念なことに、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。海外発の迷惑メ

ールが増加していることを考えると、日本国内だけではなく、海外の ISP における OP25B の早急な導入が望まれており、このための国際連携の取り組みの強化が必要となっています。

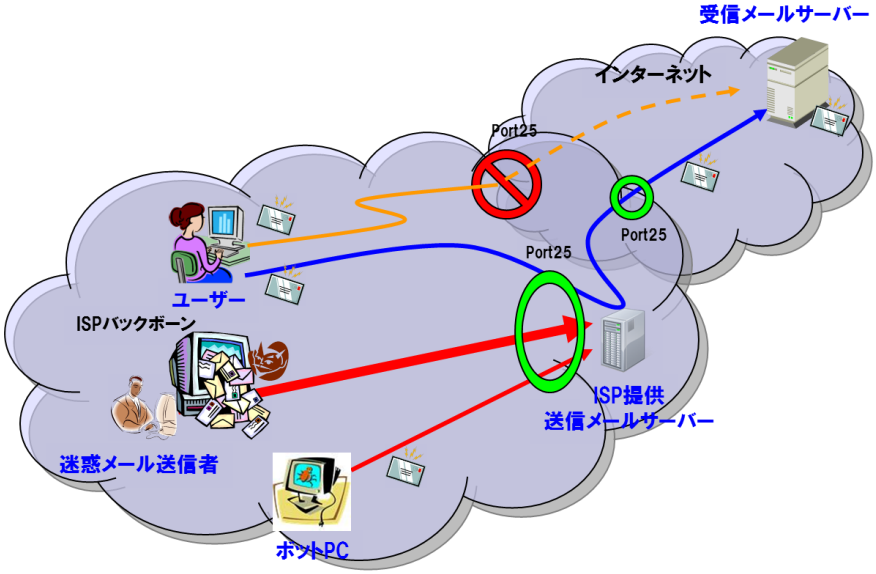
(3)ISP 内のメールへの対応

OP25B を採用している場合でも、自 ISP 内で終始するメールの送信に対して OP25B を実施している（自 ISP の動的 IP アドレスからの自 ISP の受信用メールサーバーへのメールの直接送信への OP25B を実施している）ISP はほとんどありません。

自 ISP 内で終始するメールの送信について OP25B を実施していないと、迷惑メール送信者が、自ら契約している ISP の提供している受信メールサーバーに対して迷惑メールの送信が可能になってしまいます。

このような事態を防ぐためには、自 ISP 内で終始するメールの送信に対しても OP25B を実施し、自 ISP のユーザーが送信するメールは、すべて、送信者認証を実施した 587 番ポートを用いることが、最も効果的な対策です。

図表４－１８：**ISP** 内のメールへの対応



(4)利用者への周知等

OP25B の実施にあたっては、メール送信にあたって、25 番ポートではなく、587 番ポートを用いるようにメールソフトを設定することについての利用者に対する周知が課題となります。

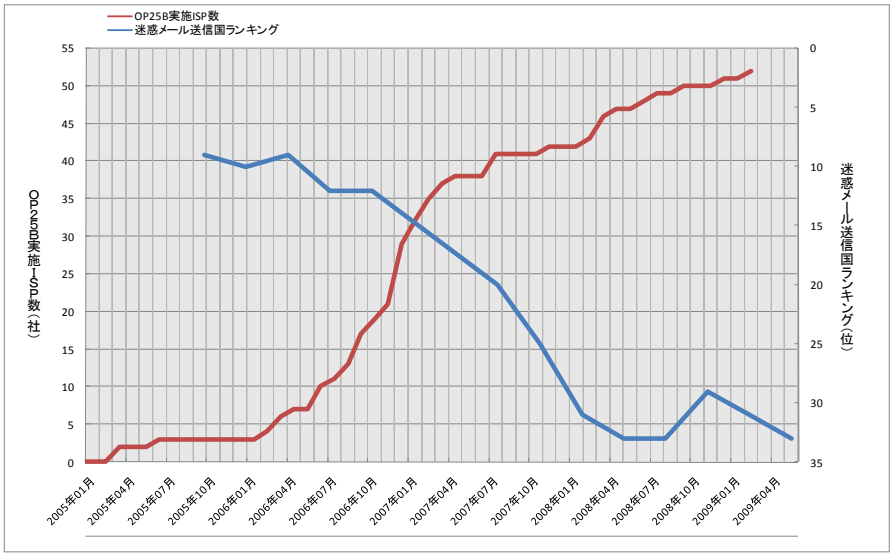
すなわち、既にメールを使っている利用者は、メールソフトの設定の変更が必要となります。また、現在、メールソフトの初期設定が未だに 25 番ポートとなっているものがあるため、新たにメールを使い始める利用者も、設定変更を行う必要があります。メールソフトの初期設定自体を変えていくことも、今後の課題です。このため、ISP における利用者への周知のための取り組みは当然のこととして、メールソフトメーカーや各種ガイドの作成者等とも協力し、多方面で利用者への周知のための取り組みを実施していく必要があります。

Topics： OP25B の効果

OP25B の日本国内での最初の採用は、平成 17 年（2005 年）1 月に、ぷららネットワークス（現株式会社 NTT ぷらら）が、ボーダフォン（現ソフトバンクモバイル）の有する携帯電話アドレスに向けた送信について実施したものです。その後、日本では、平成 18 年（2006 年）6 月頃から OP25B を導入する ISP が増加しました。下図にあるとおり、導入する ISP の増加に呼応する形で迷惑メール送信国ランキング（ソフォス社公開）における日本の順位が顕著に下がっていることが確認できます（平成 17 年（2005 年）9 月時点で全体の 9 位であったものが、最近では 30 位前後まで下がっています。）。

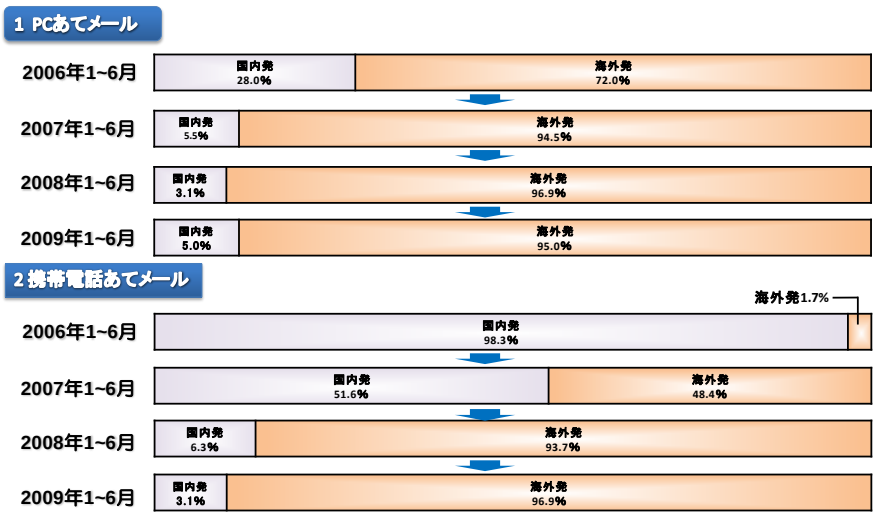
また、日本着の迷惑メールのうち国内発の迷惑メールの割合が減っているというデータもあり（日本データ通信協会迷惑メール相談センターの調査データ）、その効果が確認できます。

図表１：国内の導入状況と日本のスパム送信国ランキング



出典：日本データ通信協会迷惑メール相談センター資料及びソフォス社資料より作成

図表２：スパムメールの国内・国外の割合



出典：日本データ通信協会迷惑メール相談センター

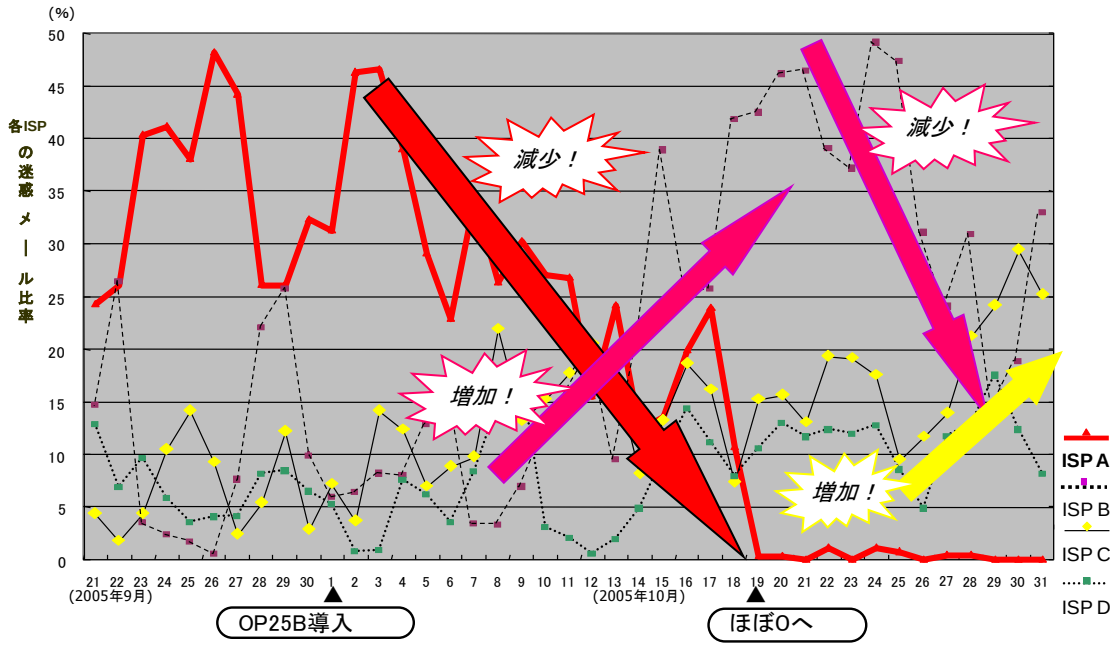
日本での OP25B は、普及の初期段階には、大手 ISP で順次導入が進みました。これは、OP25B を導入した ISP からの迷惑メールの送信が難しくなり、迷惑メールの送信者が OP25B を実施していない他の ISP に移って迷惑メールの送信を継続することになり、その結果、その ISP でも OP25B が導入される、という形で、普及が進んだものです。

実際のデータでも、この状況を確認することができます。下の図は、平成 17 年（2005 年）10 月前後に日本データ通信協会で受信した国内発の迷惑メールのうち、発信元の ISP ごとの比率を表したものです。

a) 当初、迷惑メールの発信元として比率が高かった ISP A で、10 月上旬に OP25B が導入されました。
b) その直後から、ISP A の比率が減少し、10 月下旬にはほぼゼロになっています。
c) 一方で、それと入れ替わる形で、ISP B の比率が 10 月中旬から増加しています。
d) ISP B で、10 月下旬に OP25B が導入されました。
e) その直後から、ISP A の比率が減少しています（図では、ゼロまで減っていませんが、こののち、ほぼゼロになっています。）。
f) それと入れ替わる形で、ISP B の比率が 10 月中旬から増加しています。

このような普及の経緯を見ても、迷惑メールに対する技術的対策としての OP25B の有効性がわかります。

図表３：**OP25B** の導入と迷惑メール比率の推移



出典：日本データ通信協会迷惑メール相談センター

第５節 送信ドメイン認証技術

１　概要

(1)送信者情報の詐称がもたらす被害

迷惑メールの一部は、メールの送信者を特定しづらくするために、メールの送信者情報を詐称しています。もともとメール配送の仕組みには、送信者情報を確認する機能が備わっておらず、全く関係のないメールアドレスを送信者情報として指定しても、多くの場合、問題なくメール受信者に届いてしまいます。それにより、送信者を特定しづらくする、フィッシング詐欺に悪用する等、様々な問題を引き起こすこととなり、それにより、送信者を特定しづらくする、フィッシング詐欺に悪用する等、様々な問題を引き起こすこととなります。

迷惑メールの送信手法に対する有効な対策の基盤技術として、「送信ドメイン認証技術」という技術があります。

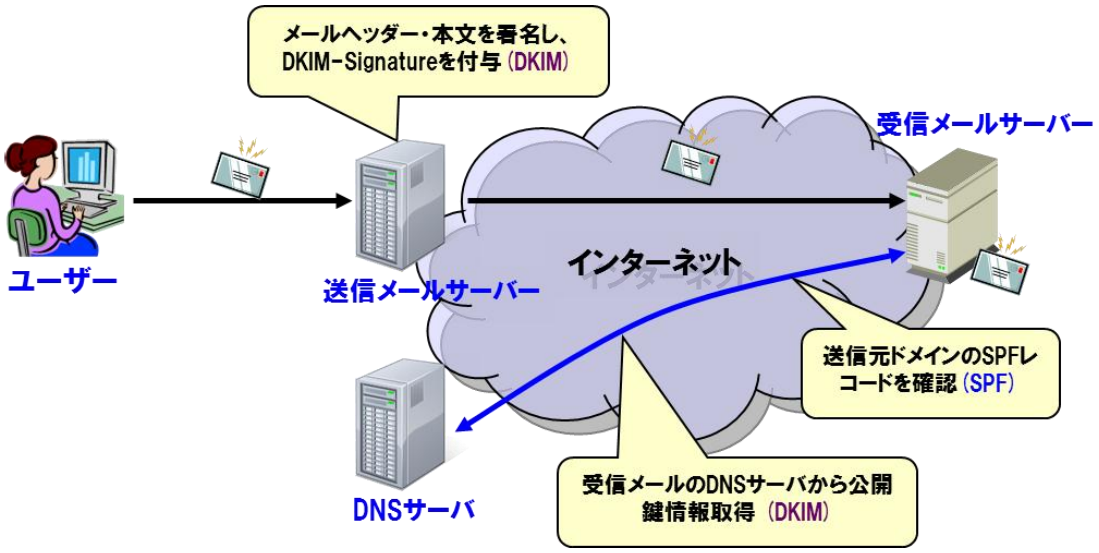
(2)送信ドメイン認証技術の概要

送信ドメイン認証技術は、既存のメール配送の仕組みを変えることなく、送信者情報が詐称されているかどうかを受信側で確認可能とする技術です。

メール配送における送信者情報は複数存在しており、それぞれ利用する送信者情報の違いや認証の仕組み自体の違いから複数の送信ドメイン認証技術が規格として提案されています。認証の仕組みとして分類すると、ネットワーク的にメールの送信元である IP アドレスを元に認証する技術（ネットワークベースの送信ドメイン認証技術）と、特定の送信者でなければ作成できない電子署名を利用する技術（電子署名ベースの送信ドメイン認証技術）に分けられます。

この送信ドメイン認証技術は、送信側メールサーバーと受信側メールサーバーの双方での対応が必要ですが、導入したドメインから順次利用することが可能なものです。

図表４－１９：送信ドメイン認証技術の概要



(3)認証結果の利用

受信側のメールサーバーでは、受信したメールが送信に用いられたドメインから正規に送信されたものであるかどうかを認証することになります。その認証結果は、受信側メールサーバーで、配送されるメールのヘッダー部分に記録したり（「ラベリング」といいます。）、認証されなかったメールを通常のメール保管領域外に隔離したり破棄したり（「フィルタリング」といいます。）することで利用されます。

ISP によっては、既に、認証結果のヘッダー部分への記録の実施や、認証結果に基づく振分けサービスの提供などを行っています。また、メールのヘッダー部分に記録された認証結果を元に自動振分け処理を設定できるメールクライアントソフトウェア（MUA: Mail User Agent）もあります。利用者は、契約している ISP のサービスを確認した上で、以上のいずれかの方法で認証結果を活用することにより、認証されたメールだけを優先して閲覧したり、認証に失敗したメールの処理を後回ししたりして、メール処理の手間を軽減させていくことが可能になります。

また、認証結果と認証するドメイン名を組み合わせてフィルター処理をしたり、何かあった場合に認証された送信側に苦情等を伝える仕組み（フィードバックループ。topics を参照。）など、送信ドメイン認証技術を利用したさらなるメール疎通の仕組み

なども検討されています。
　なお、送信ドメイン認証技術を用いた認証結果のメールのヘッダー部分への記録形式については、標準規格として提案されています（RFC5451）。今後、認証結果のメールのヘッダー部分への記録を実施する ISP が増加するとともに、そのヘッダー部分の認証結果の記録を用いた振分け処理を自動で行う機能を有する MUA が増えることが期待されます。

(4)ネットワークベースの送信ドメイン認証技術
　ネットワークベースの送信ドメイン認証技術は、受信されたメールの送信元 IP アドレスが、そのメールの送信者情報のメールアドレスのドメイン名部分の管理者が宣言した IP アドレスと一致しているかどうかにより、送信ドメインの認証を行う仕組みです。
　送信側では、送信者情報であるメールアドレスのドメイン名について、それを管理している DNS 上にメールの送信元の情報を記述します。これを、SPF レコードといいます。SPF レコードには、テキスト形式でメールの送信元であるホスト名や 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ます（詳細は、Topics ： SPF レコードの具体例）。
　受信側では、メール受信時に、送信元の IP アドレスと送信者情報を利用して認証します。まず、送信者情報からドメイン名を抽出し、そのドメイン名から DNS の仕組みを利用して、SPF レコードを取得します。SPF レコードを先頭から解釈し、送信元の IP アドレスがどこに含まれるかを調べます。SPF レコードの該当部分にある記号に従い、認証結果が決まります。
　ネットワークベースの技術には、SPF と Sender ID の二つの技術があります。Sender ID は、SPF の上位互換的な仕様になっていますので、認証時に参照する SPF レコードは、SPF と Sender ID の両方で共通に利用することができます。
　SPF と Sender ID の違いは、取り出す送信者情報にあります。SPF は配送上のメールアドレス（一般に envelope sender）を利用するのに対して、Sender ID はメールのヘッダー部分に記述される送信者のメールアドレスを利用することができます。
　なお、ネットワークベースの技術では、メール転送などメールの配送経路が元々のメール送信者と異なる場合には、認証に失敗することがあるという問題があります。この問題とその解決方策については、３(2)で詳述します。

図表４－２０：**SPF/Sender ID** と **DKIM**

SPF/Sender ID		DKIM
Sender Policy Framework (RFC4408) Sender ID Framework (RFC4406,4407)	名称	DomainKeys Identified Mail (RFC4871,5672)
送信元をネットワーク的に判断	特徴	送信時に電子署名をメールに付加
送信側はほぼ皆無（DNS の記述のみで、１通ずつの送信時の処理は不要） 受信側では一定の処理が必要（１通ずつの確認が必要） （ライセンス料は不要）	コスト	送信側は、相対的に高め（１通ずつ署名付加が必要） 受信側でも、一定の処理が必要（１通ずつ検証が必要） （ライセンス料は不要）
送信側導入の容易さ（特にコスト面） 普及が進展（co.jp では既に 40%超）	長所	メール本文の改ざんも検知
メール転送時に認証失敗となる（ホワイトリスト等での対応が必要）	短所	メールヘッダ等を変更する一部のメーリングリストで認証失敗となる（メーリングリストシステム側での再署名が必要）

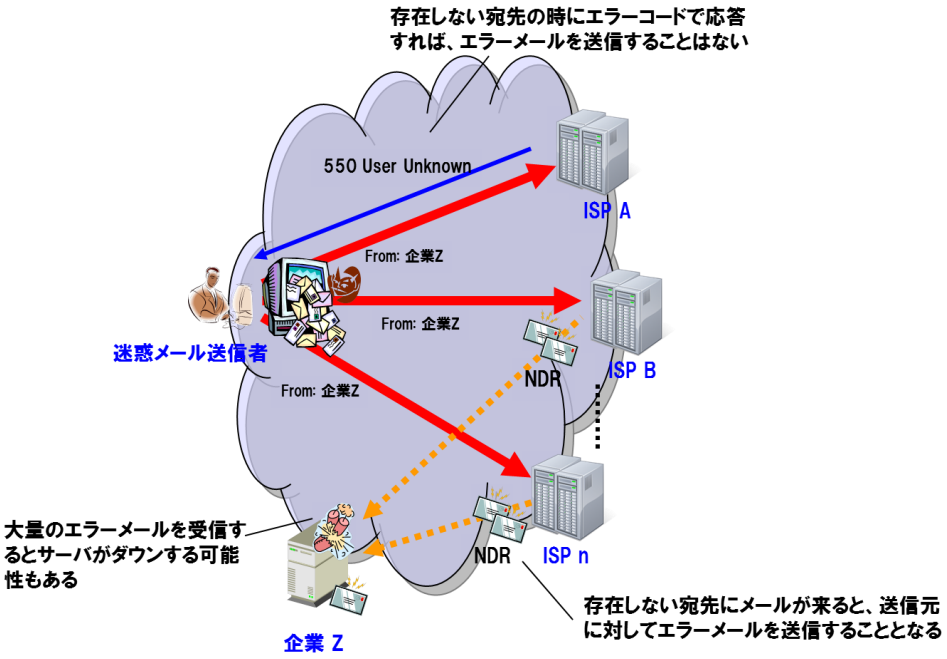
(5)電子署名ベースの送信ドメイン認証技術
　電子署名技術を利用する技術は、公開鍵暗号技術を使い、秘密鍵を持っている者だけが符号化できるデータをメールヘッダーに付加することにより、署名者が特定できるようにする仕組みです。
　電子署名技術を利用する技術には、DKIM（Domain Keys Identified Mail） があります。
　送信側メールサーバーでは、メールの送信時に 1 通づつ電子署名を作成し、メールのヘッダー部分に関連の情報とともに追加して送信します。なお、電子署名は、メールの本文及びヘッダー情報から作られる要約データ（ハッシュデータ）を秘密鍵を使って符号化することによって作られます。
　受信側では、メールヘッダーからこの電子署名情報を含む関連の情報を取得し、そこに含まれている DNS の関連情報から、DNS の仕組みを利用して公開鍵情報を取得します。次に送信側と同様に、メール本文とヘッダーから要約データを作成します。その上で、DNS から取得した公開鍵を用いてメールヘッダーに記述された電子署名を復号し、作成した要約データ（ハッシュデータ）と比較することで検証します（両者が一致すれば、認証されたことになります。）。
　なお、DKIM では、メール転送などメールの配送経路が元々のメール送信者と異なる場合でも、電子署名が崩れないかぎり認証が正しくできること、送信者の認証以外にもメール本文の改竄も検知できることなどの利点があります。

Topics:エラーメール問題の仕組み

メール配送の仕組みでは、一旦受け取ったメールについて、宛先が間違っていたりして最終的な宛先に配送できない場合には、配送できない旨を示した警告メール(エラーメール：配達不能通知（Non-Delivery Report））を元々の送信者に返すことが決められています（RFC5321)。

無差別的に大量送信されることの多い迷惑メールは、宛先が実在しているかどうかにかかわらず送信されてくることも多いという特色があります。この場合に、メールを受信する途中で、存在しない宛先のものであることが判明した場合には、エラーコードを返すことで処理を終了することができます（図表４－３での受信メールサーバーでの応答参照。)。しかし、一旦メールを受け取った後、存在しない宛先に来たメールであることが判明した場合には、送信元に対してエラーメールを返すことになり、大量の宛先不明であることを伝達するためのエラーメールが発生することになります。迷惑メールの多くは、送信者情報を偽装しているため、これら大量のエラーメールが、送信者情報の偽装に使われたメールアドレスに宛てて送信されてしまいます。

図表：エラーメールの流れ



このように、迷惑メールの問題は、不要なメールが単に大量に送信されるメール受信側だけの問題だけではなく、送信者情報が簡単に詐称できてしまうことにより、直接関係のない第三者をも巻き込む広範囲な問題となっています。さらに、身に覚えのないエラーメールが届く場合に、そのエラーメールが迷惑であるとして、そのメールの送信元を（迷惑メールの発信元として）ブラックリストに登録してしまうと、その送信元からその後に送られてくる通常のメールまで届かなくなってしまいます。しかし、エラーメールの送信側は、迷惑メールのターゲットになったに過ぎません。エラーメールも、メール配送の規格に従った通常どおりの処理をしているだけで、悪意を持って送信しているわけではありません。

この問題は、送信者情報が詐称できてしまうことと、その送信者情報が詐称されているかどうかを受信側で判断できないことによって発生してしまっている問題といえます。

用語解説

１　電子署名

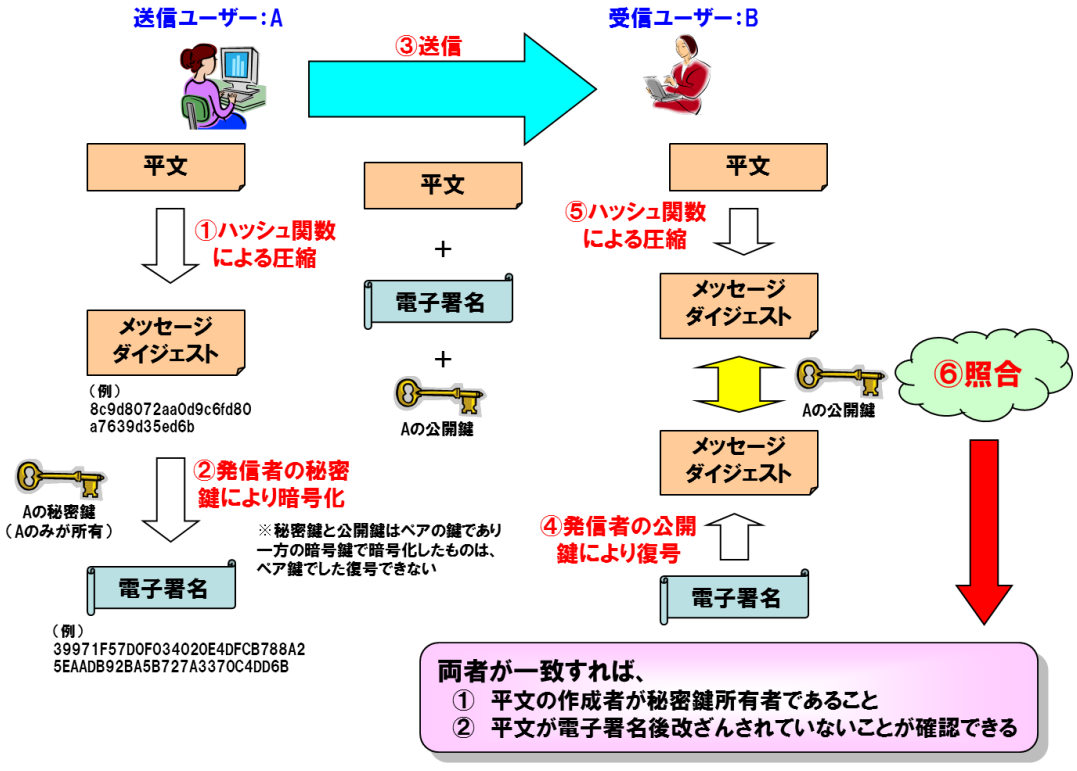
電子署名は、公開鍵暗号技術とハッシュ関数を利用して、データ作成者のなりすましやデータが改ざんされていないことを検証するために利用されます。

ハッシュ関数は一方向関数とも呼ばれ、あるデータから要約データを生成する関数です。対象とするデータから生成された要約データをハッシュ値と呼び、ハッシュ値は元のデータ長に関わり無く固定長の短いデータであり、また、ハッシュ値からは元のデータを推測することが事実上困難であるという特徴があります。変更が加えられたデータから生成されたハッシュ値は、元のハッシュ値とは異なるものになりますので、データの改ざんも検知することができます。

公開鍵暗号技術は、秘密鍵（private key）と公開鍵（public key）という二つの鍵を利用します。秘密鍵で変換されたデータは、それと対となる公開鍵を用いて復号することができます。公開鍵だけでは、元のデータを推測することは一般にはできませんので、正しく復号できたデータは秘密鍵で変換されたものであることになります。

電子署名では，署名対象となるデータのハッシュ値は署名側と検証側の双方が生成できますので、そのハッシュ値を秘密鍵で変換した署名データを公開鍵で復号し比較することにより、秘密鍵によって変換されたデータか、署名対象のデータが改ざんされていないかを確かめることができます。秘密鍵が署名者によって正しく管理されているとすれば、その署名データを作成したのは秘密鍵の管理者であることが確認できます。

図表：電子署名のイメージ



2　配送上の送信者情報とメールヘッダー上の送信者情報

現在のメールシステムでは、送信者を示す情報として、配送上の送信者情報とメールそのもののヘッダー部分に記述されるメールヘッダー上の送信者情報の二種類あり、それぞれ利用目的が異なります。その概要は、第１章の Topics「電子メールの仕組み」（２）あて先の仕組みで解説したとおりですが、ネットワークベースの送信ドメイン認証技術の２方式での取扱いが異なることになっていますので、ここではもう少し詳しく解説します。

メール配送上の送信者情報は、メール配送のための SMTP（Simple Mail Transfer Protocol, RFC5321）の MAIL コマンドで指定されるメールの送信者情報であり、reverse-path と呼ばれます。reverse-path は、その名前のとおり配送時のエラーの報告先などに利用されます。メール配送上の送信者ということで、envelope sender や envelope from などとも呼ばれることもあります。

メール受信者がメールクライアントソフトウェア（MUA: Mail User Agent）を利用した場合に表示される送信者情報としては、一般に、メールヘッダーの "From:" ヘッダーに示されている情報が使われます。メールの送信者を示すヘッダー情報としては，"From:"ヘッダーのほかに、 "Sender:" ヘッダーや "Reply-To:" ヘッダーなどがあります。"Sender:" ヘッダーは、実際のメール本文の作成者と送信者が異なる場合などに、メール本文の作成者をそのまま "From:" ヘッダーに記述するのに対し、実際の送信者を表すために使われます。"Reply-To:" ヘッダーは、そのメールへの返信時に宛先として指定して欲しいメールアドレスを記述します。なお、この "Reply-To:" ヘッダーが存在しない場合には、通常は "From:" ヘッダーに指定されたメールアドレスが返信先として利用されます。

整理すると、配送上の送信者情報（reverse-path） は、受信メールサーバーがエラーなどの報告先として利用する情報であり、メールヘッダー上の送信者情報（"From:"ヘッダー等）は、メールクライアントソフトウェア（MUA）がメールの閲覧者に送信者を伝えるとともに、返信メールを作成する場合の宛先に利用するための情報、ということになります。

Topics：送信ドメイン認証での記載例

1　SPF レコードの具体例

DNS では、ドメイン名に関連した各種情報を格納することができます。格納されるデータの種類に応じて、「資源レコード型」が定義されることになっています。SPF レコードは、新たに定義された資源レコード型の一つですが、これまでの DNS サーバーでも利用できるように TXT 資源レコードに SPF レコードの情報を格納することもできます。
以下に TXT 資源レコードに設定された SPF レコードの設定例を示します。

```
example.com.      TXT "v=spf1 +ip4:192.0.2.0/24 -all"
```

これは、"example.com" というドメインを用いて送信されるメールに関するものです。
先頭（左側）の "v=spf1" は SPF のバージョン情報を示します。SPF では、"v=spf1"、Sender ID では、" spf2.0" となります。なお、Sender ID は、SPF の上位互換的な仕様になっていますので、"v=spf1"の SPF レコードでも認証できるようになっています。
"+" や "-" は、その記号に続いて記載されたメールの出口についての認証結果を示すものです。"-" は "fail"（認証失敗）を、"~"は "softfail"（認証失敗の可能性あり）を、 "+" は "pass"（認証成功）を表します。
正規のメールの出口（設定例では、 "ip4:192.0.2.0/24" ）の前には、"+"をつけます。なお、認証結果を示す記号を省略した場合は、"+" が付いているものとして扱われます。
最後（右側）の "all" は、それまで指定された出口以外のすべてのメールの出口を示すものです。ドメインの管理元であるメールの送信者は、正規のメールの出口以外から送信された場合の認証結果を "all" の前の記号によって指定することになります。通常の場合には、"-all" 又は "~all"のいずれかの記述をします。上の設定例では、"-all" と記述していますので、正規のメールサーバー以外から送信されたメールは、すべて "fail"（認証失敗）として扱うことを示しています。

2　DKIM でのヘッダーの記載例

DKIM では、メール送信時に "DKIM-Signature" ヘッダーをメールに追加します。これは電子署名データとそれに関連した情報が含まれます。
"DKIM-Signature" ヘッダーの例は、次のとおりです。

```
DKIM-Signature: v=1; a=rsa-sha256; s=brisbane; d=example.com;
  c=simple/simple; q=dns/txt; i=joe@football.example.com;
  h=Received:From:To:Subject:Date:Message-ID;
  bh=2jUSOH9NhtVGCQWNr9BrIAPreKQjO6Sn7XIkfJVOzv8=;
  b=AuUoFEfDxTDkHILXSZEpZj79LICEps6eda7W3deTVFOk4yAUoqOB
    4nujc7YopdG5dWLSdNg6xNAZpOPr+kHxt1IrE+NahM6L/LbvaHut
    KVdkLLkpVaVVQPzeRDI009SO2Il5Lu7rDNH6mZckBdrIx0orEtZV
    4bmp/YzhwvcubU4=;
```

署名情報は ";" で区切られた "tag=value" で表されるタグ形式でパラメーターが指定されます。各タグの意味と用途は、あらかじめ RFC によって定義されています。
署名検証に使われるハッシュ関数と公開鍵暗号技術は "a=" タグで示されます。上記の例では、"rsa-sha256" が指定されており、これはハッシュ関数に SHA-256 という関数を、暗号アルゴリズムとして RSA というアルゴリズムを利用することを示しています。
ヘッダー以外のメール本文のハッシュ値は、 "bh=" タグで示されます。ヘッダーのハッシュ値を秘密鍵で変換した署名情報は "b=" タグで示されます。これらのデータは、実際に計算された数値をさらに base64 方式によって文字列に変換したものが記述されます。
そのほかのタグでは、署名するドメインの情報や、署名対象にするヘッダー情報などが記述されます。

2　課題

(1)利用する送信ドメイン認証技術

前述のとおり、送信ドメイン認証技術には複数の方式が存在しています。それぞれの方式は共存可能ですので、すべての技術を送信側と受信側の双方で導入することもできます。しかし、導入ポイントによってはメールサーバーに新たな機能追加が必要なものもありますし、新たな機能追加によってメールサーバーの負荷も増加することから設備増強が必要になる場合もあります。

a)SPF/Sender ID の利用

比較的簡単に導入できる部分は、ネットワークベースの SPF/Sender ID の送信側への導入です。これは、メール送信に使われるドメインに対して、SPF レコードを設定することによって導入できます。送信側のメールサーバーに変更が無い限り、一度設定した SPF レコードはそのまま継続して利用できます。

メール受信時の送信ドメイン認証を行うためには、既存のメールサーバーへの機能追加が必要になります。ネットワークベースの送信ドメイン認証技術では、送信元の IP アドレスが認証に必要ですので、最初にメールを受信するメールサーバーに認証処理を追加導入することになります。

b)DKIM の利用

電子署名技術を利用する DKIM の場合は、メールの送信時に電子署名を作成し DKIM ヘッダーをメールに追加する機能の追加が必要になります。また、セキュリティの観点から、電子署名を作成するために必要な秘密鍵と、検証のための公開鍵を定期的に更新していく作業も必要になります。このため、SPF に比べて送信側の導入コストが高く、まだ導入の割合が低いという状況になっています。

DKIM の受信側もネットワークベースと同様に、認証を行うためには新たな機能追加が必要になります。DKIM の場合は、メール本体だけあれば検証ができるので、受信してから最終的に受信者のメールボックスに保管されるまでの間でメールが改変されないのであれば、受信者の MUA でも検証は可能です。

c)普及の方向性

現在の日本での普及率を考慮すれば、普及の進んでいる SPF について、受信側で実効性のある活用を可能としていくために、送信側での SPF レコードの設定は必須の段階にあると考えられます。各組織でのメールシステムの管理者と DNS の管理者は、管理しているドメインに対して、まず SPF レコードを宣言すべきです。メールサービスの運用者は、これだけ SPF レコードの宣言率が高い状況なのですから、ネットワークベースの受信側の認証を行うべきです。

DKIM については、メール受信者からの苦情が正当なものであるかを判断するための仕組み（フィードバックループ。Topics 参照。）ツールとして利用できますので、大量のメールを送信する送信事業者などに導入の利点があると考えられます。ARF (Abuse Reporting Format) の規格化など、フィードバックループの環境が整備されるに従い、普及が進んでいく可能性があります。

(2)ネットワークベースの転送問題

ネットワークベースの送信ドメイン認証技術(SPF/Sender ID) では、ドメイン認証を行う直前のメールサーバーの IP アドレスを利用します。そのため、メール転送を行うことにより直前のメールサーバーと、転送されてもそのまま利用される送信者情報に不一致が生じてしまう、という問題が起こります。

本問題の解決方法としては、２つの方法が存在します。

一つは、第２節で説明した転送アドレスを書き換える方法です。転送時に、転送元のメールアドレスやドメインで送信元を書き換えて送信すれば、受信側では転送元のドメインで認証することとなりますので、転送元のドメインが SPF/Sender ID に対応していれば認証可能となります。しかし、受信したメールをすべて受信時のメールアドレスに書き換えて転送すると、転送先で宛先不明になったエラーメールも転送してしまうことになり、転送元と転送先でループが発生する可能性があります。そのため、転送時に書き換えるメールアドレスは、受信時のメールアドレスとは別のメールアドレスを利用し、そのメールアドレス宛に受信したメールは単純に転送しない、といった処理が必要になります。

もう一つの方法は、転送元のメールアドレスをホワイトリストに入れて送信ドメイン認証をせず、又はその結果を利用しないで受信するという手法です。一般に、メールの転送元と転送先はそのメールアドレスの管理者（利用者）が同一であることが多いため、メール転送によって認証が失敗する場合は、管理者（利用者）自身で把握できているはずです。この管理者（利用者）が、メール受信時に特定の送信元からのメールをホワイトリストに入れることにより認証結果の影響を受けないという特別扱いができれば、この問題は回避することができます。送信ドメイン認証技術によるフィルターを提供している多くの ISP では、本機能を具備していますので、管理者（利用者）は、送信ドメイン認証技術の利用にあたっては、そのような機能も併せて活用することが考えられます。

(3)電子署名ベースにおける認証されないメールの取扱い問題

電子署名ベースの送信ドメイン認証技術(DKIM)では、DKIM シグネチャが付与されていない場合には、その認証結果は、シグネチャが存在しないということになります。あるドメインでメールを送信する際に、全てのメールに DKIM シグネチャが付与されていれば問題ありませんが、付与されていない場合があると、シグネチャがないメールに問題があるか否かを判断できないということになります。

本問題を解決するために、DKIM シグネチャが付与されていない場合の振る舞いを定義した、DKIM Autohr Domain Signing Practice (DKIM ADSP) という技術があります。本技術を用いると、DKIM シグネチャが付与さ

れていないメールの正当性を定義することが可能になり、DKIM の実用性がより高くなります。しかし、メールの配送経路によっては容易に使えない等の問題をかかえており、今後の改善が期待されているものです。

(4)普及に向けて

メールの送信者情報を詐称できてしまうことにより、様々な問題が発生しており、それらは迷惑メールの増大とともにメール利用者に大きな負担を与えています。また、迷惑メールの割合が通常のコミュニケーションに利用されるメールの量を超えている現在、行き過ぎた対策によって本来届くべきメールにまで悪影響を与えるような状況も発生しかねません。本来受け取るべきメールを受信側で正しく区別できるようにするために、送信側と受信側の双方での送信ドメイン認証技術の普及をより進めていく必要があります。

Topics: フィードバックループ

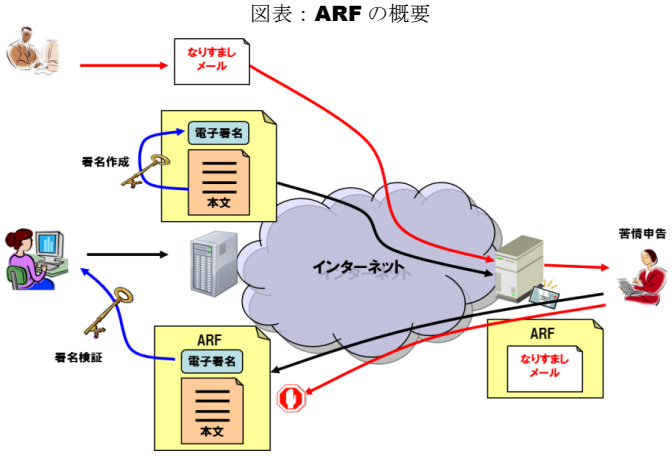
メールシステムにおける「フィードバックループ」とは、メールの受信者が送信者に対して迷惑メールの苦情等の情報を伝える仕組みのことをいいます。メールの送信者（メールの配信事業者などが該当します。）は、フィードバックループにより、自社のサービスをより向上させることができるようになります。例えば、もう送信を必要としない宛先を識別して宛先リストを整理することや、送信間隔や頻度の調整、苦情の多かった送信内容を識別できるなど、メール受信者に快適なサービスの提供に貢献することができます。

フィードバックループで情報を受け取る送信者（配信事業者）にとっては、受け取る情報の形式が統一されていることが望まれます。苦情等の情報の送り元が、実際に送った送信先リストに含まれているかどうか、苦情等の対象となったメールがどれなのか、苦情等の種類が何であるかなどが簡単に抽出できるようになっていれば、より迅速に対応することが可能になるからです。また、苦情等を連絡する側としても、連絡先ごとにそれぞれ異なった手段での連絡を求められるより、同じような手段や形式が決められていれば便利なはずです。

現在、フィードバックループをメールで通知することを前提に、対象のメールそのものを、電子メールでファイルを添付する場合などに一般的に用いられている MIME（Multipurpose Internet Mail Extension） 形式で取り込む ARF(Abuse Reporting Format）と呼ばれる方式の標準化作業が行われています。MIME のそれぞれのパートとして、内容の説明やフィードバックの種別を指定し、対象としているメールそのものなども取り込みます。フィードバックの種別には、迷惑メールを示す ″spam″ や詐称やフィッシングの場合を示す ″fraud″、オプトアウト を示す″opt-out″ などが示されています。

フィードバックループに ARF を利用することで、送信者（配信事業者）は送信したメール本文が得られることになり、自身が実際に送信したものであるかどうかを判断することができます。また、送信者（配信事業者）がメール配送時にそれぞれのメールに DKIM の署名を付加している場合には、フィードバックとして戻ってきたメールの署名部分を確認することで、より厳密に自身が実際に送信したものであるかどうかを確認できます。

図表：**ARF** の概要



既に米国などでは、大手のメールサービス提供事業者（ISP や ASP など）がこのフィードバックループの仕組みを導入し始めています。これらのメールサービス事業者は、事前に登録された配信事業者へメール受信者からの苦情を伝えるなどの仕組みを運用しています。

これまで、日本では、メールの送信者情報を詐称できてしまうことにより、送られてきたメールがいわゆる迷惑メールなのか、自分が送信を同意した正規の広告宣伝メールなのかの判断が難しいという問題がありました。そのため、迷惑なメールに対してやみくもに苦情を連絡することは、逆に相手に実在するメールアドレスを通知してしまうことになるのであまり推奨されてきませんでした。送信ドメイン認証技術を利用することにより、連絡しても問題がない正規の送信者かどうかの判断がしやすくなり、さらにフィードバックループを普及させることにより、メール配信事業者とそれを受け取るメール受信者双方にとって、快適なメール環境を実現することが可能となります。

フィードバックループ以外の方法としては、ユーザーが設定した迷惑メールフィルターで受信拒否をした際に、SMTP セッションで 5xx のエラーを返し、該当のメールを受信する意思がないことを伝えることも可能です。ただし、5xx エラーを返す事由として受信拒否以外である可能性も高いため、一回のエラーで受信する意思がないと判断することは問題となる可能性があり、複数回失敗した場合に一時的に送信を止めるなどの工夫が必要となります。

第5章
関係者による自主的な取り組み

第５章　関係者による自主的な取り組み

第１節　携帯電話事業者の取り組み

我が国における携帯電話の契約数は１億回線を超え、普及率は実に日本全人口の８割を超えるレベルに達しています。その中で、携帯電話によるインターネットの利用者は約９割近くに及び、メールやコンテンツなどにより、世界に先駆けて日本独特の新しいコミュニケーション文化が創造されてきました。

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すが、負の側面も問題となってきました。特に迷惑メールは、平成 13 年（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

(1) メールアドレス変更機能

初期の段階では、携帯電話のメールアドレスが電話番号と同一だった携帯電話事業者もあり、迷惑メール送信者が容易にアドレスを推測することが可能でした。そこで、メールアドレスの変更機能を提供し、迷惑メール送信者に類推されづらいメールアドレスへの変更が推奨されています。メールアドレスの変更は、友人や購読しているメールマガジンの発行元など関係者への周知の手間はかかりますが、それ自体が有効な迷惑メール対策といえます。

(2) 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、携帯電話事業者各社では、利用者の意思で特定のドメインやアドレスから送信されるメールのみを受信する機能（指定受信機能）や、それらの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。

代表的な受信拒否機能として、携帯電話のドメインになりすまして送信されるメールを拒否する機能や、受信者が指定したアドレスからのみメールを受信する指定受信機能などがあり、迷惑メール対策として大きな効果をあげています。その他にも、各社から様々なメール受信機能が提供されています。

なお、携帯電話になりすましたメール送信の抑止を目的として、携帯電話事業者各社では、送信ドメイン認証の SPF レコードが記述されています。

近年スマートフォンが急速に普及しつつありますが、これら受信機能については同様に利用可能となっています。

(3) 利用者への啓発

以上のような迷惑メール対策の利用方法等について、携帯電話事業者各社では、契約後の確認通知書や請求書同封物、店頭配布ツール、ホームページなどを通じて、長期間に渡り継続的な啓発を実施しています。また、各社では、それに加えて、新聞、雑誌等の各種媒体で迷惑メール対策機能の紹介を行っているほか、ショップ店頭でも、適切な迷惑メール対策の設定を行うことができるよう、利用者に対する補助を実施しています。

さらに、携帯電話事業者各社では、ケータイ安全教室を開催し、小中高等学校の生徒に加え保護者･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。

(4) 送信者への啓発

携帯電話事業者各社では、存在しない宛先へのメール送信や短時間での大量メール送信を控えること、また宛先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、送信者がメール送信にあたって注意すべき点をホームページを通じて周知し、適切な方法でのメール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メール送信を行った ISP/ASP 等からのメールの受信が一時的に相手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。

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

(1) 送信通数制限

迷惑メールが社会問題化していく中で、平成 15 年（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、携帯電話事業者各社により、自社の契約者が迷惑メール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数を制限する措置（送信通数制限）が導入されました。これによって、携帯電話から送信される迷惑メールが抑制されました。

(2)利用停止措置

携帯電話事業者各社では、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、迷惑メール送信が確認された契約者に関して利用停止等の積極的な対処を実施しています。

また、平成18年（2006年）3月1日以降、迷惑メール送信を行い利用停止となった利用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り組みが行われています。

さらに、平成18年(2006年)4月1日以降、携帯電話不正利用防止法（用語集参照）に基づき、架空名義や名義貸しでの契約を防ぐために、厳格な契約者の本人確認が行われています。具体的には、新規の申込みや名義の変更に際して、契約者本人であることが確認できる書類の原本により契約者本人であることを確認しています。

第２節　サービスプロバイダーの取り組み

サービスプロバイダーには、インターネット接続とともにメールサービスを同時に提供することの多いISP と、メールサービスだけを提供するホスティングサービスやフリーメールサービス（用語集参照）などの提供者である ESP（Email Service Provider）などがあります。

サービスプロバイダーは、メールの受信側だけではなく、メールの送信側としての立場もありますので、それぞれの立場での取り組みについて紹介します。

１　送信側での取り組み

提供するサービスが、迷惑メールの送信に利用されることがあるため、サービスプロバイダーでは、迷惑メールを送信させないための取り組みを実施してきています。

(1)OP25B の実施

迷惑メールの送信者が、サービスプロバイダーの提供するインターネット接続回線を利用して、直接受信メールサーバーへ大量に迷惑メールを送信するケースがあります。この場合、第４章で述べた OP25B などの技術的な対策によって、動的 IP アドレスから送信される迷惑メールを防止できるようになりました。

(2)利用停止等の取り組み

しかし、近年は OP25B の対象外である固定 IP アドレスを契約して送信するケースも多くみられるようになりました。また、直接受信メールサーバーへ送信するのではなく、サービスプロバイダーが提供するメールサービスを踏み台にして送信する手法も、従来から行われています。

サービスプロバイダーの多くは、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、これらの利用方法はサービスの不正利用として、迷惑メールの送信が確認された利用者に対して、利用停止や契約の解除を行っています。また、こういった迷惑メール送信者が、契約を解除されても再度契約し迷惑メールを送信し続けることを防止するため、契約者情報に基づいた事前確認を行うなど、虚偽の情報で契約しようとしていないかをチェックするプロバイダーもあります。

(3)利用者への啓発

多くのサービスプロバイダーでは、こうした不正利用に自社のサービスが使われることを防ぐため、また不正利用された場合に契約解除を行いやすくするために、サービスの提供条件を約款として記述し、あらかじめ同意を得ています。不正利用とされる行為の具体的な内容として、サービスプロバイダーによっては具体的な事例を示し、法律違反となる行為のほか、自社や他社の設備に著しく悪影響を与えるような行為などを禁止しています。

また、サービスプロバイダーによっては、不正利用が行われたことを利用者が簡単に報告できるように、ウェブによる問合せフォームを用意するなどの取り組みを行っています。

２　受信側での取り組み

大量に送られる迷惑メールは、サービスプロバイダーの受信メールサーバーに過大な負荷を与えることになり、これにより正規のメールが受信できない、配送遅延が発生するなどの問題が発生します。さらに、本来不要である迷惑メールを格納することによるメールを保管する設備（ストレージ）の不足は、より深刻な問題となっています。顧客の大事なメールを保管するために、サービスプロバイダーが利用しているストレージは、費用をかけて耐障害性が高められた高価なものですが、増加し続ける迷惑メールによって大部分が無駄に消費されているのです。

(1)迷惑メールフィルターの提供

多くのサービスプロバイダーでは、迷惑メールの混入を防ぐため、迷惑メールフィルタ（第４章第１節５参照）を提供しています。

サービスプロバイダー各社では、ネットワークレベルのフィルターやメール内容によるフィルターなど、様々な迷惑メールフィルタを提供しています。メールは社会にとって重要なコミュニケーション基盤となっているため、こういった悪質なメール配送要求によって、通常のメール配送に支障が出ることは、防がれなければなりません。安定したサービス提供の維持のため、サービスプロバイダーはこうした設備保護的な対策を今後も継続していく必要があります。

(2)送信ドメイン認証の利用

幾つかのサービスプロバイダーでは、メール受信時に送信ドメイン認証を実施しています。送信ドメイン認証により、メールが正当なドメインから送信されているかどうかを確認できるため、これらの情報をうまく利用すれば、正しいメールの受信に役立てることができます。

そのためには、送信側の送信ドメイン認証の導入割合を高めることが必要ですが、既にサービスプロバイダーや一般企業などを中心に送信側の導入率は増加傾向にあるため、サービスプロバイダーにおいても送信側と受信側双方で簡単に利用できるような環境作りを今後進めて行くことが望まれます。

(3)利用者への啓発

近年、メールを利用して偽装サイトへ誘導し、個人情報や金銭などを搾取するフィッシング詐欺の被害が報告されるようになりました。また、メールを通じてウイルスなどのマルウェアに感染するなどの事例も多く発生するようになっています。利用者がこうした被害にあわないようにするため、多くのサービスプロバイダーでは、安全にインターネットを利用するための手引きや、セキュリティベンダーのウイルス情報へ容易にアクセスできるリンク情報などをウェブに掲載することなどによる利用者啓発の取り組みを行っています。

特に、不正プログラムを誤って実行してしまうことにより、利用者の PC が感染し、外部から遠隔操作されて、内部情報を搾取されたり、ボットネットの一部として外部への不正攻撃に悪用されたりするなどの手口が深刻な問題となっています。現在、多くのサービスプロバイダーが CCC（第 2 章の topics 参照）の活動に参加し、感染者へ注意警告を行うなどの活動をしています。

また、迷惑メールの増加とともに、サービスプロバイダーに対する問合せも増えてきました。サービスプロバイダーの中には、これらの問合せに対応するため、迷惑メールの概要やその特徴などを説明し、ヘッダー情報の閲覧方法や、それらの情報から実際の送信者が誰であるかを確認するための手法の解説などを行っているものもあります。また、迷惑メールへの対策として、迷惑メールフィルターの利用を推奨したり、迷惑メールフィルターの設定方法などの説明を行っているサービスプロバイダーもあります。

第３節　セキュリティベンダーの取り組み

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

また、より迅速に迷惑メール関連情報を提供するため、Web 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ホストや送信する可能性のあるホストの情報について、自社の Web サイトや DNS サーバーなどで公開し、一般ユーザーが自由に参照・利用できるようにしているセキュリティベンダーもあります。

２　迷惑メール対策の新技術の開発と取り組み

セキュリティベンダーの多くは、SPF、Sender ID、DKIM 等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（Internet Engineering Task Force（用語集参照））に属し、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、各社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各社は、IETF における標準化活動以外にも、MAAWG や、JEAG などの迷惑メール対策を行う組織の活動に参加し、新技術の紹介、迷惑メール対策についてのユーザーからの要望のヒアリング、ベンダー間を超えた協調などを行っています。

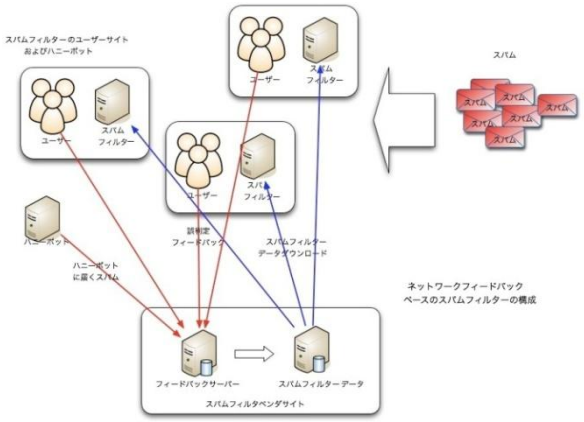
３　迷惑メール対策製品の性能向上

セキュリティベンダー各社が提供する製品・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、実際に日本で流通している迷惑メールの収集･解析を通じ、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のみに依るのではなく、複数の検知技術を総合的に用いるものや、実際に送信されている迷惑メールのデータをリアルタイムで収集して特徴を分析し、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。

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。各社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５－１：フィードバックを受けた迷惑メールの検出精度向上



第４節　配信サービス事業者の取り組み

配信サービス事業者（用語集参照）は、メールマーケティングを行う者など（メール送信者）に対して、メール配信のシステム等を提供しています。各社では、それぞれのサービス提供にあたって、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、より適切なメール配信が行われるようにするなど、迷惑メール対策の取り組みを実施しています。

１　契約時の確認

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

２　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等のメールの送付先のリストが適正に管理されていないと、アドレス変更等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ことになります（配信エラー）。配信エラーにより、本来不要なメールが送受信されることになりますので、配信エラー率を低下させるための取り組みが求められます。

個々の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等の措置を行っています。

３　迷惑メールが送信された場合の対応

契約時の確認等にもかかわらず、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、大手のほとんどの配信サービス事業者では、迷惑メールの送信行為は約款上の禁止行為に該当することとして規定し、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、契約解除等の措置を実施しています。

４　技術的な対応

大手のほとんどの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等を行う事業者等が容易に設定できるように、SPF レコードに関する設定方法の周知や設定内容の無料確認、DKIM に対応したメール送信機能の提供等の対応を行っています。

また、システム的な対応として、事前に申請されていないアドレスからの送信の制限や、不適切な内容を含むメールが送信されていないかの確認等を行っている配信サービス事業者もあります。

５　その他の措置

迷惑メール関係の法改正において、オプトイン規制が導入されたことに対応し、ダブルオプトイン機能（用語集参照）、オプトインの記録保存機能等を提供している配信サービス事業者もあります。

第6章
国際的な取り組み

第６章　国際的な取り組み

第１章で見たとおり、我が国に着信する迷惑メールの９割超が外国から送信されており、諸外国との連携が不可欠となっています。我が国では、総務省、消費者庁による国際連携のほか、民間部門においても積極的な連携が進められています。

１　多国間での取り組み

(1)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: Organization 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、迷惑メール対策に係る技術的方策、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。

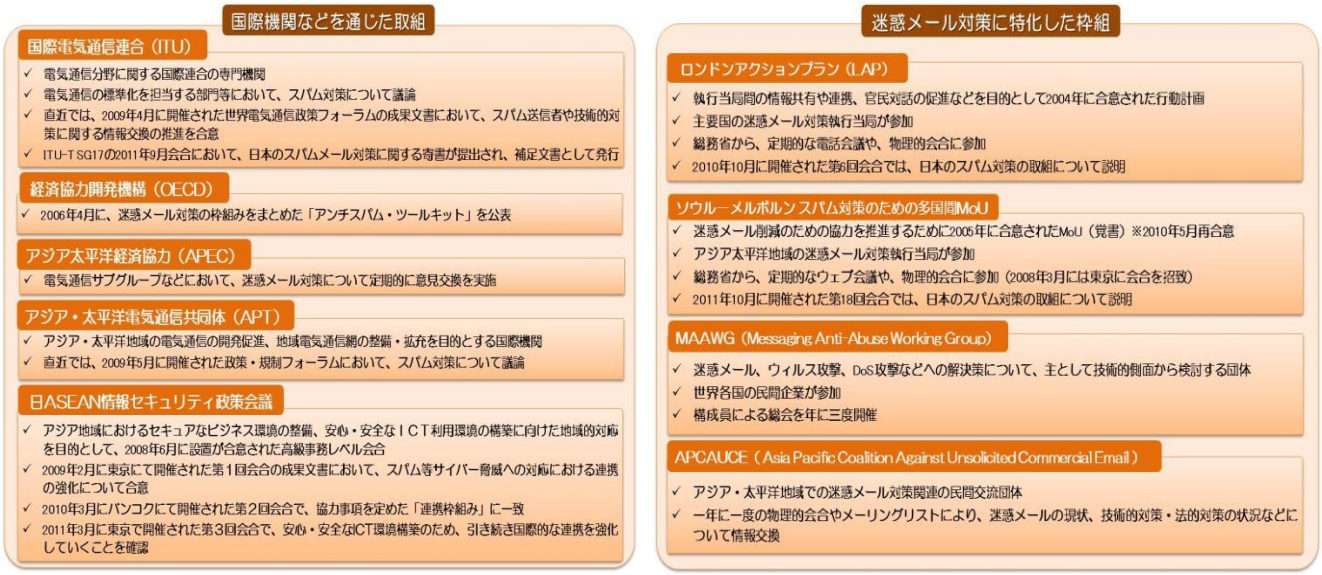
(2)迷惑メール対策に特化した連携枠組み

迷惑メール対策を行う執行当局などが、平成16年（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（London Action Plan :LAP)」に合意し、以後、定期的に執行機関相互の情報交換などが行っています。さらに、アジア太平洋地域の執行当局間の協力枠組として、平成17年（2005年）４月に、「スパム対策の協力に関する多国間 MoU（覚書：Memorandum of Understanding)」が合意され、平成22年(2010年)４月に当該MoUが新たに見直され再締結されるなど、引き続きこの場においても、定期的な情報交換などを行っています。

また、米国を中心とした世界各国の民間事業者が、MAAWG（Messaging Anti-Abuse Working Group）を組織し、迷惑メール、ウイルス攻撃、DoS攻撃などへの解決策について、主として技術的側面から検討を行っています。会合は高頻度で開かれており、構成員による総会が年に三度開催されています。

このほか、アジア・太平洋地域での連携枠組みとして、(財)インターネット協会が、APCAUCE（Asia Pacific Coalition Against Unsolicited Commercial Email）に参加しています。APCAUCEは、各国における迷惑メールの現状や、技術的対策や法的対策の状況などの情報交換を行う民間交流の場です。メーリングリストが運用され、年に一度、顔合わせのミーティングも開催されています。

図表６－１：多国間での連携の状況



2　二国間等での取り組み

(1) 共同声明など

総務省および経済産業省が、フランス、イギリス、カナダ、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、日本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。

(2) 送信者情報の交換

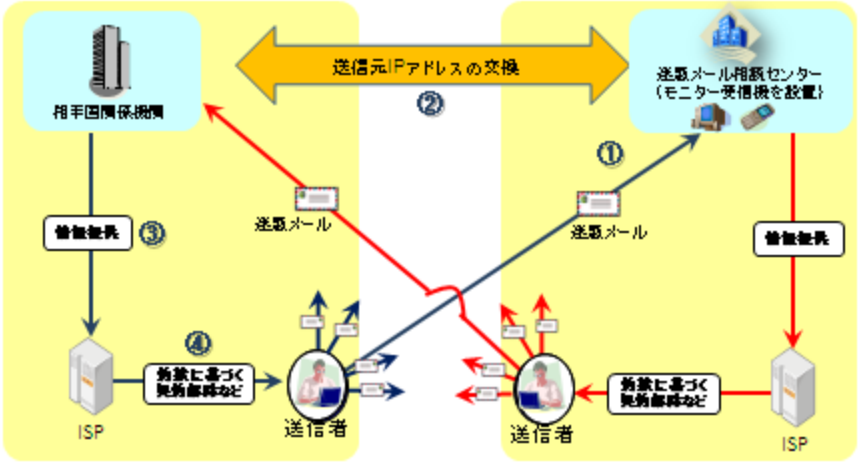
消費者庁（(財) 日本産業協会）および（財）日本データ通信協会迷惑メール相談センターが、中国インターネット協会（ISC）との間で迷惑メールの発信元 IP アドレスの交換を行っています。交換された発信元情報は、両国の ISP による、迷惑メール送信者への措置に役立てられています。

（財）日本データ通信協会は、香港電気通信管理局(OFTA)および台湾通信放送委員会(NCC)との間でも、同様の取り組みを行っており、さらに、平成 22 年 1 月からは、ブラジル(CERT.br)との間においても、同様の取り組みを開始しました。

図表６－２：二国間等での連携の状況

国／地域	連携の形態	連携の主体	
		日本側	先方
フランス	共同声明(2006.5)	総務省・経済産業省	経済財政産業省
英国	共同宣言(2006.9)	総務省・経済産業省	貿易産業省
カナダ	共同声明(2006.10)	総務省・経済産業省	産業省
ドイツ	共同声明(2007.7)	総務省・経済産業省	連邦経済技術省
中国	送信元IPアドレスの交換・ISPへの通知（2007.12～）	(財)日本データ通信協会 (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（2009.5）	総務省	工業情報化部(MIIT)
香港	送信元IPアドレスの交換・ISPへの通知（2007.12～）	(財)日本データ通信協会	電気通信監理局(OFTA)
台湾	送信元IPアドレスの交換・ISPへの通知（2008.5～）	(財)日本データ通信協会	通信放送委員会(NCC)
スイス	経済連携協定(EPA)における協力条項(2009.9)	政府	政府
韓国	ICT協力に関する文書を締結(2009.5)	総務省	放送通信委員会(KCC)
	送信元IPアドレスの交換・ISPへの通知（2011.5～）	(財)日本データ通信協会	韓国情報保護振興院(KISA)
ブラジル	発信元IPアドレスの交換（2010.1～）	(財)日本データ通信協会 一般社団法人JPCERTコーディネーションセンター	CERT. br
ベトナム	ICT分野における協力関係に関するMOUの締結(2010. 9)	総務省	情報通信省
インド	日印経済連携協定における協力条項（2011.2）	政府	政府

図表６－３：相手国との送信元 **IP** アドレスの交換



①迷惑メール相談センターのモニター受信機で迷惑メールを受信
②提供された迷惑メールの送信元IPアドレスを分析し、送信元IPアドレスを相手国関係機関に提供
③送信元のISPにIPアドレスを提供
④送信元ISPにおいて、送信者との契約解除などの措置

3　最近の国際連携の動向

(1)多国間での取り組み

a)日 ASEAN 情報セキュリティ政策会議(平成 23 年（2011 年）3 月)

日 ASEAN 情報セキュリティ政策会議は、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な対応を目的として、平成 20 年（2008 年）6 月に設置が合意された会議です。平成 21 年（2009 年）2 月に東京にて開催された第 1 回会合の成果文書において、スパムを含むサイバー脅威への対応における、日 ASEAN での連携の強化について合意され、平成 22 年(2010 年)3 月にバンコクにて開催された第 2 回会合で、情報セキュリティに関する日・ASEAN の協力事項を定めた「連携枠組み」に一致しました。また、平成 23 年(2011 年)3 月に日本で開催された第 3 回会合で、安心・安全な ICT 環境構築のため、日･ASEAN で引き続き国際的な連携を強化していくことを確認しました。

b) London Action Plan（平成 22 年（2010 年 10 月）

オーストラリアで第 6 回会合が開催され、カナダ、ニュージーランド、ドイツ、台湾、マレーシア、日本等各国のスパムメール対策機関からスパム対策の取組状況に関する説明及び情報交換が行われました。

(2)二国間での取り組み

a) ベトナム

平成 22 年（2010 年）9 月、ベトナム情報通信大臣が来日し、総務大臣との間で ICT 分野における協力関係に関する MOU を締結しました。同文書において、迷惑メール対策における連携について確認されています。

b) 韓国

平成 23 年（2011 年）5 月から、韓国 KISA（情報保護振興院）との間で、迷惑メールの発信元 IP アドレスを交換し、国内 ISP へ通報することを行っています。

C) インド

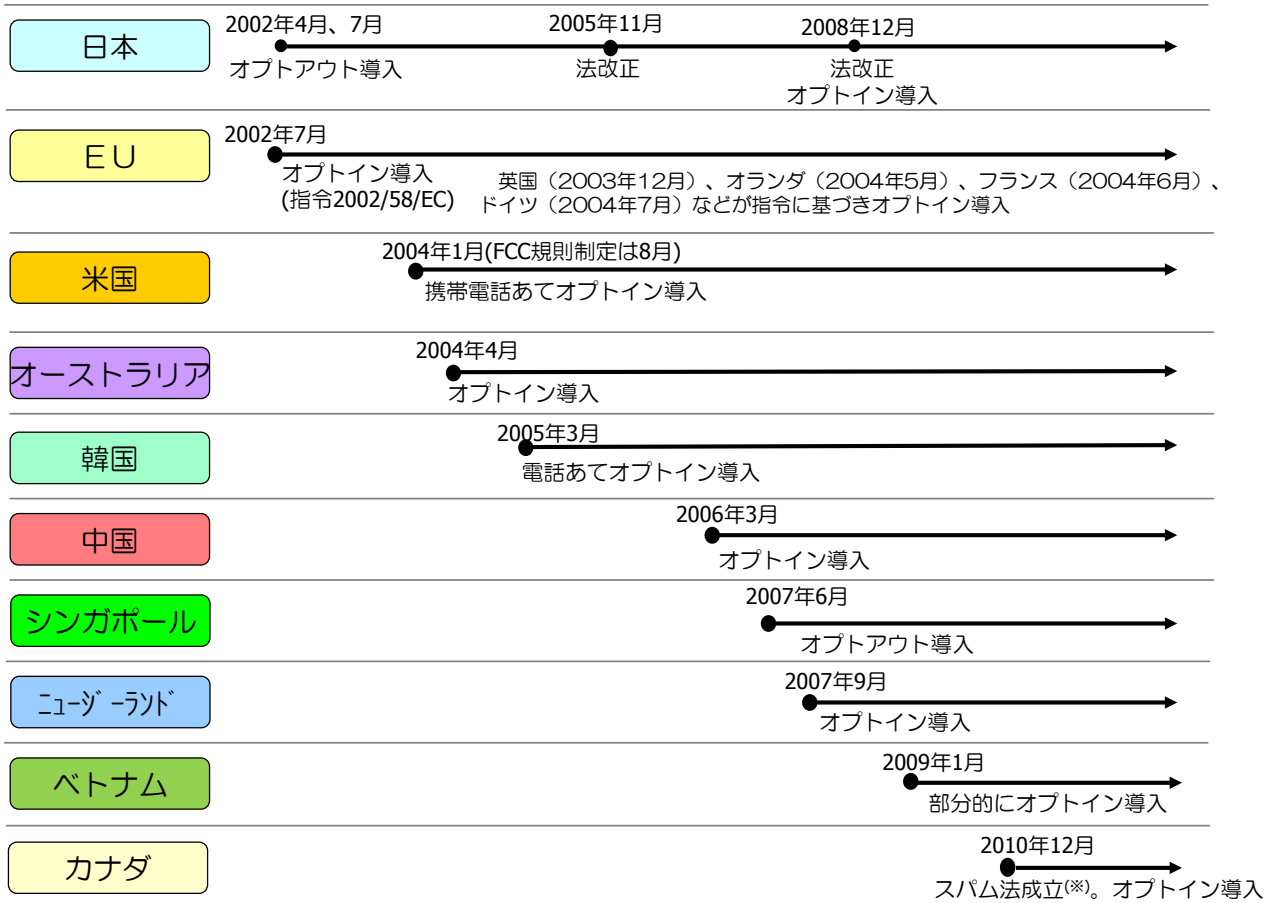
平成 23 年（2011 年）2 月、日印経済連携協定が締結され、電気通信サービス附属書において、迷惑メール対策法令や迷惑メール対策に関するベストプラクティスの情報交換を行うこととされています。

Topics:海外での迷惑メール対策法制の整備状況

平成 14 年（2002 年）に、特定商取引法および特定電子メール法により、我が国においてオプトイン規制が導入された時点では、迷惑メールへの法規制は世界的にも先駆的なものでした。その後、EU 指令によりオプトイン規制が導入されたことを受け、欧州各国でオプトイン方式による法規制が進みました。米国では、連邦法（CAN-SPAM 法）によりオプトアウト規制が課されたほか、FCC（連邦通信委員会）規則により、携帯電話をあて先としたものについてはオプトイン規制が課されました。また、オーストラリア、ニュージーランド、アジア諸国においても、オプトイン規制を中心とした立法がなされています。

平成 22 年(2010 年)12 月には、カナダでオプトイン規制を中心とした法律が成立しました。（施行時期は未定です（23 年（2011 年）5 月現在））

図表：主要国における迷惑メール対策法制の整備状況



※ 正式名称は、「商業活動を行う電子的手段への信頼性を失わせる特定の行為を規制することにより、カナダ経済の効率及び順応性を高め、カナダ・ラジオテレビ通信委員会法、競争法、個人情報保護法及び電子文書法並びに電気通信法を修正する法律」。施行時期は未定(23年5月現在)。

第7章
迷惑メール対策に係る組織等における取り組み

第７章　迷惑メール対策に係る組織等における取り組み

第１節　迷惑メール対策推進協議会

１　概要

平成 20 年（2008 年）11 月 27 日に、迷惑メール対策に関する関係者が幅広く集まり、「迷惑メール対策推進協議会」（座長：新美育文明治大学教授）を設立しました。本協議会では、迷惑メール対策に関する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を目的としています。

平成 23 年（2011 年）３月現在、協議会構成員は 47 名（実務的な問題に係る情報共有、対策の検討等を目的として設置された幹事会の構成員は 27 名）となっています。

２　主な活動内容

平成 20 年（2008 年）11 月 27 日に開催された第１回会合で、迷惑メールの追放に向けた決意と具体的に講ずるべき措置等をまとめた「迷惑メール追放宣言」を採択しました。

平成 21 年(2009)年には、幹事会の活動を中心として、送信ドメイン認証技術など効果的な迷惑メール対策技術の普及や、迷惑メール対策ハンドブックの策定による啓発活動などを進めました。

また、平成 22 年(2010 年)7 月には、迷惑メール対策ハンドブックに最新動向を反映して改版するとともに、送信ドメイン認証技術導入行程を明確にし、導入のためのマニュアルを作成し公開しました。その後、企業・団体等への説明会を実施するなど普及活動を進めています。

さらに、平成 23 年(2011 年)8 月には、これらの活動を踏まえ、迷惑メール対策ハンドブックに送信ドメイン認証技術普及促進の特集を組むとともに、よりわかりやすいハンドブック、マニュアルに改版しております。

図表７－１：第 3 回迷惑メール推進協議会の様子

第２節　(財)日本データ通信協会　迷惑メール相談センター

１　概要

財団法人日本データ通信協会では、平成 14 年（2002 年）7 月に、迷惑メール相談センターを設置しました。迷惑メール相談センターでは、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（数値は平成 22 年度（2010 年度）の実績）

(1)迷惑メール受信者からの電話相談

迷惑メールを受信して困っている者や、トラブルに巻き込まれそうになっている者などからの相談を電話で受け付け、対処方法をアドバイスしたり、適切な相談窓口を案内したりしています。なお、最近では、架空請求に関する相談が多くなっており、ウィルスメールなどに関する相談も寄せられています。

(2)迷惑メールの収集

迷惑メール相談センターに設置したモニター機（パソコン・携帯電話）で迷惑メールを収集しています（約 46 万件）。また、センターのホームページで、迷惑メールの受信者から迷惑メールに関する情報提供を受け付けています（約 720 万件）。

(3)特定電子メール法違反等の調査・分析

収集した迷惑メールについて、その内容等を確認し、特定電子メール法に関する違反の有無の分析を行っています。

また、収集した迷惑メールについて、発信元 ISP や発信国等の分析を行っています。

(4)関係機関への情報提供

収集・分析した結果、特定電子メール法に違反すると判断された電子メールについては、総務省に違反内容等についての情報提供を行っています。

また、発信国が日本であるものについては、総務省・経済産業省が平成 17 年（2005 年）1 月に発表した「迷惑メール追放支援プロジェクト」の一環として、総務省とともに、送信元 ISP に情報提供を行い、約款に基づく措置を促しています。

発信国が外国であるもののうち、中国、香港、台湾、ブラジル発のものについては、それらの国の関連機関へ情報提供を行い、送信者に対する対応の依頼をしています(中国及び香港には平成 19 年（2007 年）12 月から、台湾には平成 20 年（2008 年）5 月から、ブラジルには平成 22 年(2010 年)1 月から情報提供を実施しています。)。

(5)セキュリティベンダー等への情報提供

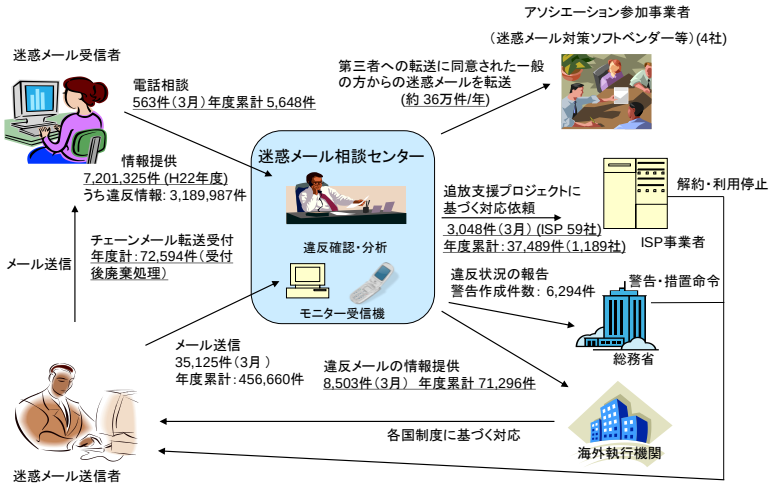
平成 20 年(2008 年)1 月に迷惑メール情報共有アソシエーションを設立し、迷惑メール情報を参加事業者に提供しています（約 36 万件）。このアソシエーションでは、情報提供に同意された方から、迷惑メールをヘッダー情報を含んだ形で収集し、セキュリティベンダーなどの参加事業者に提供することで、迷惑メールのフィルタリング製品の開発等に役立てることを目的にしています。

(6)利用者等への周知・啓発

迷惑メール対策の周知・啓発活動として、迷惑メール相談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、迷惑メールに関するアンケート調査の実施・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７－２：迷惑メール相談センター活動模様



第３節（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

財団法人日本産業協会の電子商取引モニタリングセンターでは、平成 13 年（2001 年）8 月にインターネット通信販売のモニタリング事業を開始、平成 14 年（2002 年）2 月には消費者からの情報提供窓口を設置し、迷惑メール調査についても開始しました。現在は、平成 17 年（2005 年）1 月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、インターネットオークション、テレビ通販等の調査を実施しています。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（数値は平成 22 年度（2010 年度）の実績）

(1)迷惑メールの収集

センターに設置したモニター機（パソコン・携帯電話）で迷惑メールを収集しています（約 64 万件）。また、当センターのホームページより消費者からの情報提供を受け付けています（約 270 万件）。

(2) 特定商取引法違反等の調査・分析

収集した迷惑メールについて、その広告元であるサイト事業者の調査を行い、特定商取引法に関する違反の有無を判定しています。

また、モニター機で受信した迷惑メールについては、発信元 ISP や発信国を分析しています。

(3) 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等の詳細を消費者庁へ報告しています。

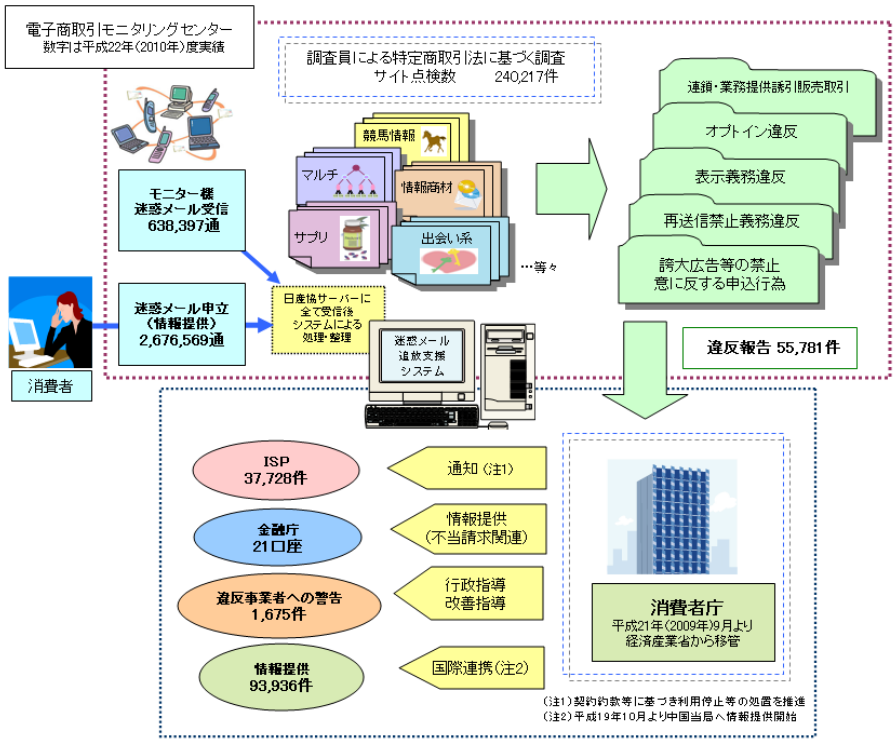
その情報をもとに、消費者庁より事業者へ是正を求めるとともに、「迷惑メール追放支援プロジェクト」の一環として、消費者庁から取引関係のある ISP に通知を行うことで、事業者への利用停止等の措置を促進することが可能となっています。また、同様に不当請求を行っている悪質事業者の口座については、消費者庁から金融庁への情報提供を行っています。

さらに、日本の消費者に向けた中国発の広告メールの急増を受け、平成 19 年（2007 年）10 月より、消費者庁を通じて中国の関連機関への情報提供を開始しています。

(4) 一般消費者への啓発

情報提供されたメールを分析し、最新の迷惑メールの動向やサイトの仕組みについてホームページで公表し、注意喚起を行っています。

図表７－３：電子商取引モニタリングセンター活動模様



第４節　（財）インターネット協会　迷惑メール対策委員会

１　概要

財団法人インターネット協会では、平成 16 年（2004 年）9 月より、ISP、一般企業、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、迷惑メール対策活動を行ってきています。同委員会は、26 名の委員からなり、オブザーバーとして、総務省、経済産業省および消費者庁も参加しています（平成 23 年（2011 年）4 月現在）。

２　主な活動内容

(1)委員会ミーティング

委員会では、月一回の定例の会合を開催しています。この会合では、迷惑メール関連の最新情報の交換と、カンファレンスやセミナー、ポータルサイトにおける情報提供活動などに関して議論を行っています。

(2)迷惑メール対策カンファレンス

委員会では、年１～２回、主にメール管理者を対象とした「迷惑メール対策カンファレンス」を開催しています。来場者数は 300 人規模となっています。カンファレンスでは、他団体と連携した技術情報提供や、総務省・経済産業省からの法令情報など、迷惑メール全般に関する最新情報を提供しています。また、カンファレンスで用いた資料は、ウェブページで公開しています。

(3)地方セミナー

委員会では、年２回程度、地方セミナーを実施しています。地方セミナーでは、主に迷惑メール対策カンファレンスの内容をコンパクトにまとめて情報伝達を図っています。平成 22 年度には、7 月に松山で開催し約 100 人が来場しました。また、3 月には熊本で開催し約 60 人が来場しました。熊本ではフィッシングに関する話題も取り上げました。

(4)迷惑メール対策情報ポータルサイト

委員会のウェブページでは、技術情報の観点から、関連する URL の翻訳や送信ドメイン認証技術関連解説、メールサーバー運用に関する情報などを提供しています。また、法改正の際の解説記事や迷惑メール対策関連情報へのリンクなどを掲載し、適宜更新しています。

(5)国際連携

委員会では、主にアジア・パシフィックを中心とする民間の国際連携活動を行っています。APCAUCE(Asia Pacific Coalition Against Unsolicited Commercial Email)会合のスポンサー支援も行っています。

図表７－４：迷惑メール対策カンファレンスの模様

第５節　JEAG　(Japan Email Anti-abuse Group)

１　概要

日本のメール市場は、高速インターネットやインターネットに対応した携帯電話の普及とともに世界的にも有数の規模に拡大している中で、迷惑メールの存在は設備に支障を及ぼすだけではなく、ユーザに対する直接的な損害を与えるなど、通信サービスの存在基盤を危うくするほどの脅威となってきています。

このような中、各社において迷惑メール対策の取り組みが進められてきましたが、迷惑メールの問題は、サービスプロバイダーやベンダーが、それぞれ単独で実施するだけでは解決できない問題となってきました。このため、メールに携わる業界全体として取り組む問題であるとの認識が醸成されてきました。米国ではMAAWG（Messaging Anti-Abuse Working Group）が設立され、サービスプロバイダーやベンダーがビジネスの枠を超えて、迷惑メール根絶のための取り組みを始めていたことを参考とし、日本においても、同じ目的の団体の設立が急務であると考え、技術的な見地から通信事業者やソフトウェア・ハードウェアメーカー等が連携して具体的な対策を実施・検討する団体として、平成17年（2005年）3月に、JEAGが設立されました。現在30社が加盟しており、オブザーバーとして、総務省、経済産業省、日本データ通信協会も参加しています。

２　主な活動内容

(1)JEAG Recommendation（リコメンデーション）の作成

JEAG設立当初に、迷惑メール撲滅における重要な３つの検討課題「携帯迷惑メールの撲滅」、「Outbound Port 25 Blocking（OP25B）の導入」、「送信ドメイン認証技術の導入」について、それぞれサブワーキンググループを作り検討しました。迷惑メール対策を検討する事業者をはじめメールサーバを運営する管理者に今後の参考としていただくため、導入時の課題に対する検討結果や導入後の成果を、３つのリコメンデーション（「携帯Recommendation」、「Outbound Port 25 Blocking Recommendation」、「送信ドメイン認証Recommendation」）としてまとめ、平成18年（2006年）2月に公開しました（JEAGホームページで公開）。

(2)講演活動（普及活動）について

JEAGでの検討結果は、リコメンデーションとして発表していますが、その成果等を広く普及することを目的に総務省主催の研究会をはじめとした各種研究会や迷惑メールに対するカンファレンス等での報告や講演を実施しています。特に、インターネット協会主催の迷惑メールカンファレンスや、CMPテクノロジー主催のESC（Email Security Expo & Conference）では、毎年JEAGとして発表しています。

図表７－５：**JEAG**設立時の会合模様

(3)国際連携について

JEAG では、JEAG 設立の動機となった国際的な迷惑メール対策団体である MAAWG とは、相互協力の関係を構築しています。近年の MAAWG の総会は、メンバーだけの限定会合となっていますが、MAAWG メンバーではない JEAG メンバーも、これら相互協力の一環として、積極的に MAAWG 会合に参加して発表を行い、日本の迷惑メール状況や取り組みなどを報告しています。

JEAG は、アジアパシフィックの迷惑メールに関する連携の場である APCAUCE の会合でも、日本での OP25B や送信ドメイン認証技術などの取り組みを積極的に紹介し、他国での導入の働きかけも行っています。

JEAG は、これらの国際組織以外にも、迷惑メールを減らし、正しいメールを受け取れるような環境を目指して、他の多くの国際会議にも参加し、技術的な対策や日本での事例などを紹介しています。

(4)その他

平成 20 年度「情報通信月間」において、迷惑メール対策に関する活動、特に提言書の作成とその普及促進により日本から発信される迷惑メールの大幅な削減を実現できたことが評価され、総務大臣表彰を団体として受賞しています。

第8章
今後の取り組み

第８章　今後の取り組み

前章までにみたように、迷惑メールについては、電気通信事業者、配信サービス事業者、広告関係者その他様々な関係者が、その撲滅に向けて、制度的な対策、技術的な対策、自主的な取り組み、国際連携のための取り組みなど様々な取り組みを行ってきています。しかし、迷惑メール対策のための取り組みが強化されるのに対応して、迷惑メールの送信手法も巧妙化・悪質化してきており、依然として、その問題が解決されたと言えません。

このため、今後も、関係者が協力し、引き続き、次のような措置を有機的に連携させ、総合的な迷惑メール対策を推進していくことにより、我が国からの迷惑メールの追放に向けた取り組みを強化していくことが必要とされています。最終的には、全世界からの迷惑メールの追放を目指して、国際連携の強化をはじめとする取り組みを一層進めていく必要があります。

１　制度的な対策

(1) 特定電子メール法・特定商取引法をはじめとした関係法律の適切な執行
(2) 必要に応じた制度の見直しの検討　等

２　技術的な対策

(1) フィルタリング、OP25B や送信ドメイン認証などの対策の開発・導入の促進
(2) セキュリティベンダーによる効果的な迷惑メール対策製品等の提供　等

３　国際連携の強化

(1) 迷惑メール対策を行う諸外国の行政機関や関連組織との連携の強化
(2) 諸外国の電気通信事業者との連携の強化

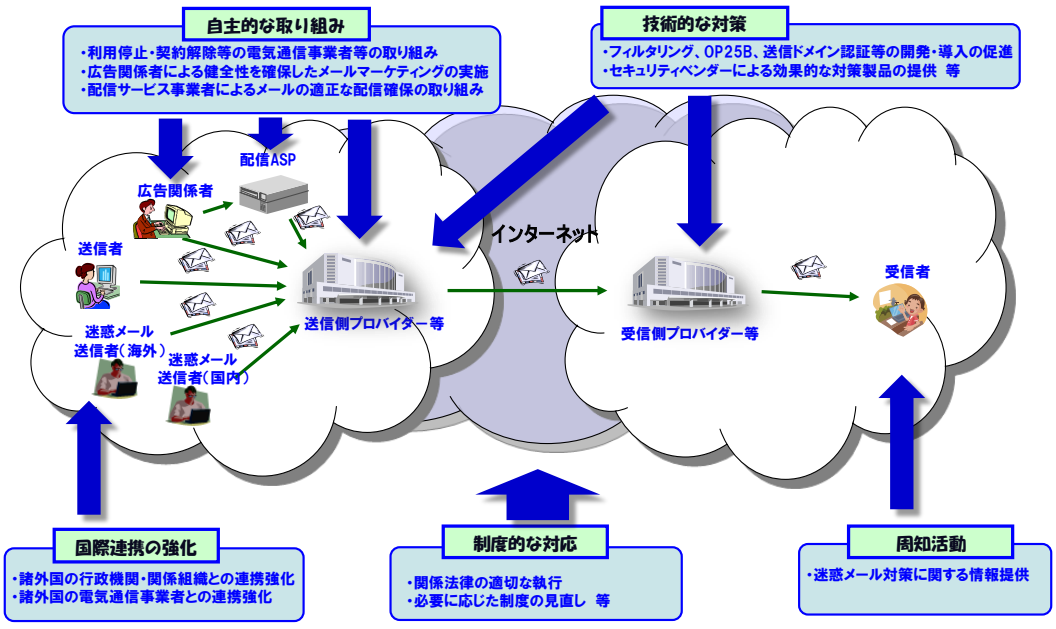
４　自主的な取り組み

(1) 契約約款に基づいた迷惑メール送信者の利用停止や契約解除などの電気通信事業者等による自主的な取り組み
(2) 利用者からの適正な同意の取得など、広告関係者による健全性を確保したメールマーケティングの実施
(3) 配信サービス事業者によるメールの適切な配信確保のための取り組み

５　周知活動

利用者をはじめとした関係者に対する迷惑メール対策に関する情報提供

図表８－１：総合的な迷惑メール対策の実施



MEMO

参考1
利用者が注意すべきこと

（参考１）　利用者が注意すべきこと

迷惑メールについては、行政機関や携帯電話事業者、サービスプロバイダー等、関係組織その他の関係者により、様々な取り組みが行われてきています。ここでは、迷惑メールに対して、利用者が行える対策や利用者が注意すべき点について、ポイントを簡単にお示しします。なお、迷惑メール対策のために利用者が注意すべき点については、様々な関係者によりパンフレットやウェブサイト等にまとめられていますので、詳細については、それぞれのパンフレット等をご覧ください。

１　迷惑メールを受け取らないための対策

(1)アドレスを安易に公表しない

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。ホームページ上や掲示板で公開した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りますので、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、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等もあるため、注意することが必要です。また、プロフィールサイトなどで、初期設定のまま利用すると、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メールアドレスを用いましょう。迷惑メール送信者は、プログラムなどでメールアドレスとして使用できる文字列を作成し、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等を利用して、当該ウェブサイト等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、よくわからないまま同意をして、メールアドレス等を開設者に通知すると、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)携帯電話事業者やサービスプロバイダー等の対策サービスを利用する

携帯電話事業者やサービスプロバイダー等の提供するフィルタリング等のサービスを活用しましょう。携帯電話事業者や多くのサービスプロバイダー等で、迷惑メールフィルターサービスが提供されています。具体的な内容や利用の条件等は、携帯電話事業者やサービスプロバイダー等により異なっているため、利用している携帯電話事業者やサービスプロバイダー等に確認してください。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携帯電話事業者やサービスプロバイダー等の導入状況については、（財）日本データ通信協会のウェブページでもご確認いただけます。

(5)セキュリティソフト等の機能を利用する

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も活用しましょう。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、そのような機能を活用することも有効です。

２　迷惑メールを受け取ってしまったときの対策

(1)開かない

受け取った迷惑メールは、開かないようにしましょう。メールを開くだけでウィルス感染することもありますので、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、メールを開くだけでウェブアクセスが行われ、メールを閲覧したことなどの情報が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

URL 等は、クリックしないようにしましょう。迷惑メールに記載された URL に不用意にアクセスしたら、後日、高額な使用料を請求するメールが届くようになったケースもあります。また、URL にアクセスすることで、メールを閲覧したことなどの情報が伝わってしまい、そのメールアドレスに宛てて、さらに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。迷惑メールからウェブページ等に誘導し、そこで巧妙に個人情報を入力させる手口も出てきていますので、注意しましょう。

(4)送信者が不明なメールには返信しない

身に覚えのないメールには、返信しないようにしましょう。そのようなメールの中にある連絡先に返信すると、「実在するメールアドレス」

のリストに登録され、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、善悪さまざまな内容により、メールを転送させようとしますが、チェーンメールを転送しなくても何も起こりません。逆に、友達に転送することにより、相手にいやな思いをさせてしまうことにもなりかねません。どうしても不安な場合には、財団法人日本データ通信協会で転送先アドレスを提供しているので、その転送先アドレスを使いましょう。

(6)関連組織に情報提供する

迷惑メール対策に生かすために、受け取った迷惑メールに関する情報を提供しましょう。日本データ通信協会迷惑メール相談センターや日本産業協会電子商取引モニタリングセンターで法律違反の迷惑メールに関する情報提供を受け付けています。また、携帯電話事業者各社でも、専用の連絡先を設けて、迷惑メールに関する情報提供を受け付けています。

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、きちんと、登録の解除(オプトアウト)を行いましょう。フィルタリングなどによって受信拒否設定をした場合には、送信側では、そのメールが利用者にとって不要であることがわからず、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、送受信側のプロバイダー等で無用な処理が必要になり、余計な設備負荷がかかることになるためです。

(2) 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

メールアドレスを変更したら、広告宣伝メールの発行者にも変更したメールアドレスを通知しましょう。

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、存在しないメールアドレス宛の広告宣伝メールが延々と送信され続けることになり、プロバイダー等に余計な設備負荷がかかることにもなります。

(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をすると、広告宣伝メールの受信のために登録しているメールアドレスを第三者が受信者になりすまして変更することや広告宣伝メールの送信を解除すること等を防止するため、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、メールアドレスの変更、オプトアウト等に必要となるので、忘れないようにしましょう。

3　迷惑メールの送信者にならないようにするための対策

○ウィルス感染しないようにする

ウィルス感染すると、気づかないうちに、自分の PC から迷惑メール送信が行われてしまうこともあります(ボット)。ウィルス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等のソフトウェアのアップデートの実施(セキュリティ上の脆弱性を修正してくれます。)するとともに、信頼できないソフトウェアを使用しないことなどに注意しましょう。

また、ボットネットに感染しているかの確認・駆除は、サイバークリーンセンター(https://www.ccc.go.jp/)で提供されていますので、必要に応じ、利用しましょう。

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の更新データを定期的に導入するよう心がけましょう。

4　その他の対応

○　メール送信に 587 番ポートを利用する

利用しているサービスプロバイダー等が 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サービスプロバイダー等以外のサービスプロバイダー等から電子メールを送る場合に、OP25B が実施されていると、メール送信に 25 番ポートが利用されているとメールの送信ができないことがあります(一部のサービスでは 25 番ポートへのアクセスが完全に遮断されている場合もあります。)。

インターネットへの接続のために利用しているサービスプロバイダー等のウェブページ等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。

資料名	概要	入手方法
撃退！迷惑メール （最新版 2011 年 1 月）	受信者が気をつけることをまとめた冊子 （日本データ通信協会作成）	日本データ通信協会のウェブページからダウンロード可能
撃退！チェーンメール （最新版 2011 年 1 月）	チェーンメール対策をまとめたパンフレット （日本データ通信協会作成）	日本データ通信協会のウェブページからダウンロード可能
あんしん BOOK （最新版 2011 年 5 月）	迷惑メール対策も含む利用者向けのリーフレット （NTT ドコモ作成）	店頭で配布
au の安心サービス （最新版 2010 年 11 月）	迷惑メール対策も含む利用者向けのリーフレット （KDDI 作成）	店頭で配布
ケータイ安心 BOOK （最新版 2011 年 3 月）	迷惑メール対策も含む利用者向けのリーフレット （ソフトバンクモバイル作成）	店頭で配布

MEMO

参考2
メール送信側が注意すべきこと

（参考２）　メール送信側が注意すべきこと

迷惑メール送信者は、迷惑メールが届けられるように、送信手法を悪質化、巧妙化してきており、それに対応して、受信側でも様々な技術的な対策が図られてきています。

そのような迷惑メールではありませんが、メールを利用しているサービス提供者の中で、メールサーバーやメールアドレス等の管理が行き届いておらず、結果として、大量に送信されるメールや、存在しないあて先を多く含むメールなど、迷惑メールよりも負荷の高いメール等の送信が行われている場合が存在しています。その結果、設備保護の観点で受信側が実施する規制条件に該当して、メールが受信拒否されたり、遅延したりする等の問題が発生しています。

ここでは、これらの問題の発生を防ぐために、主としてメールの送信側として最低限考慮すべき点についてお示ししますので、メールシステムの開発や運用･管理に関わる方は、是非とも参考にしてください。

１　「お隣さん問題」と「Backscatter 問題」

(1) 共用サーバーを利用した迷惑メール送信による「お隣さん問題」

ISP や ASP の提供するメールシステムや共用ホスティングサーバは、不特定多数のユーザーにより利用されています。これらのメールサーバーからは、比較的多量のメールが送信され、かつ一般ユーザーに宛てたメールが送信される場合が多いため、これに紛れて、それらのメールサーバーを利用として迷惑メールを送信する者も存在しています。

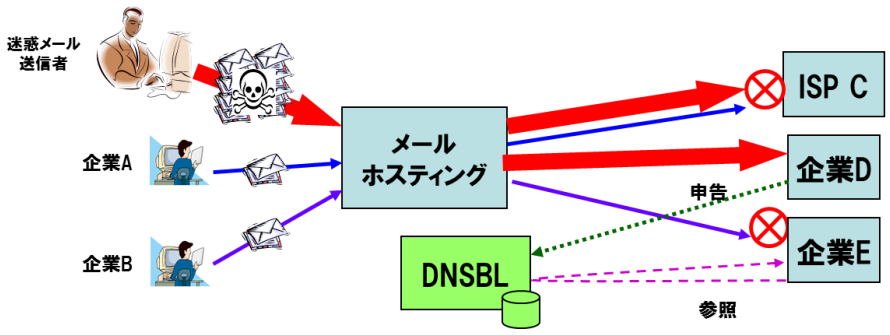
それらのメールサーバーを利用して迷惑メールが送信された場合に、迷惑メールを受け取ったユーザーが、該当の送信元（メールサーバー）から迷惑メールが送信されたと認識し、該当の送信元の情報（IP アドレスなど）をブラックリストを提供している企業へ通知し、それがブラックリストに登録されることがあります。もし、受信側で、そのブラックリストを利用してメール受信ブロックをするシステムが存在した場合には、該当の送信元からのメールの受信が制限されることになります。

また、ブラックリストを利用していない場合でも、短時間に大量の送信や、存在しないあて先を多く含むメールの送信が行われたときには、設備保護の観点から、受信側で一時的に受信を制限する場合があり、この場合も、該当の送信元からメールの受信が拒否されることになります。

このような形で受信側でのメールの受信の制限が行われる場合には、受信制限の原因となった迷惑メールだけではなく、該当の送信元（メールサーバー）から送信される通常のメールも巻き込まれて受信制限されることになり、同じ送信元を利用している多くのユーザーのメールに多大な影響が出ることになります。

このような問題は、同じ送信元を利用している（同居している）ユーザーの影響を受けることから、「お隣さん問題」と呼ばれます。

図表１　お隣さん問題



- ISP C では、メールホスティングからの大量の迷惑メールを受信したため、該当のサーバーからのメールの受信拒否を実施。その結果、メールホスティングを使っている企業A のメールも受信拒否される結果となる。
- 企業D では、メールホスティングから大量の迷惑メールを受信したため、DNSBL（ブラックリスト）管理会社に申告を実施し、メールホスティングが迷惑メール送信元として登録される。
- 企業Eでは、DNSBLの情報を使って受信拒否をしていたため、メールホスティングからのメールの受信拒否をしたことにより、メールホスティングを利用している企業B からのメール受信が拒否される結果となる。

(2) アドレス詐称メールによる「Backscatter 問題」

存在しないあて先にメールが送信された場合には、一般的には、送信元に「該当のあて先が存在しませんでした」という内容のエラーメールが送信されます。

このエラーメールには、2つの送信方法があり、どちらを使わなくてはいけないというルールはありません。

第1は、メール送信時に受信側からエラー応答を受信した送信側のサーバーが、エラーメールを作成して送信するものです。第2は、受信側でメールをいったん受信した後に該当のユーザーが存在しない等の理由でメール保存先がない場合に、受信側でエラーメールを作成して送信するものです。この第2のケースはメールサーバーがユーザー情報を保持していなかったり、ハーベスティング対策等が必要だったりするために、すべてのメールを一旦受信する等している場合に多く発生します。

ここで送信したメールアドレスが詐称されていた場合には、エラーメールはこの詐称されたアドレスにあてて送信されることとなります。

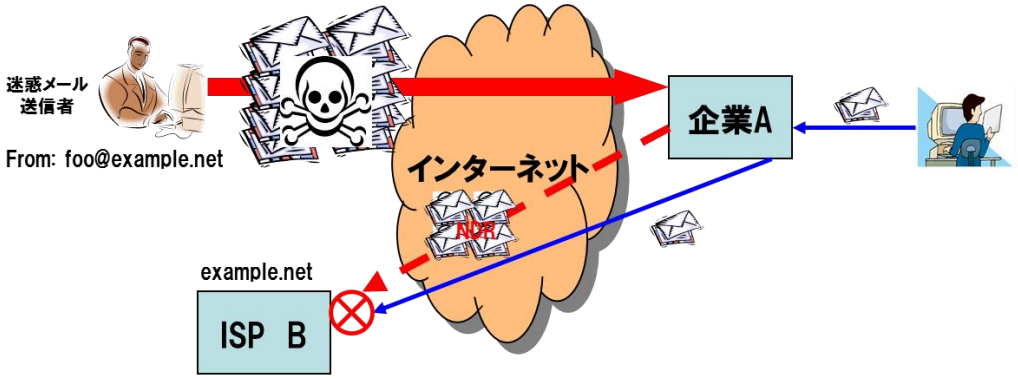
送信側でエラーメールを送信している場合には、送信側が管理しているドメイン以外のアドレスを使っていた場合には、エラーメールのあて先が詐称された存在しないアドレスである可能性があるということは認識できますが、受信側でエラーメールを送信している場合には、送信ドメイン認証技術などを用いない限り、そのことを検知することは通常できません。

エラーメールが大量に送信された場合や、エラーメールの送信先となった詐称されたアドレスが存在しないアドレスだった場合には、エラーメールの受信側では、このエラーメール送信元からのメールを一時的に受信制限することがあります。

このように受信側での制限が行われた場合には、該当の送信元から送信される通常のメールも巻き込まれて受信が制限されることになります。

この問題はメールが拡散して制限されるということから、「Backscatter 問題」と呼ばれます。

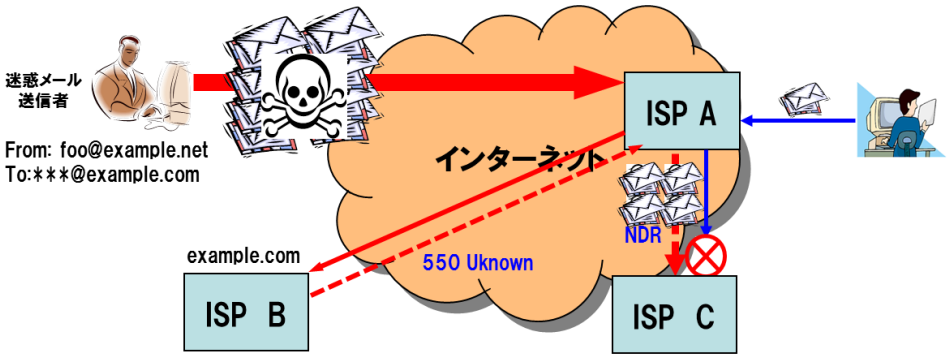
図表2　Backscatter 問題



- 迷惑メール送信者は、ISP B のメールアドレスを詐称して、企業A に迷惑メールを送信する。
- 企業A では、受信した迷惑メール中で存在しないアドレスに送信されたメールに対して、ISP B にエラーメール（NDR）を送信する。
- ISP B では、企業Aから大量のエラーメールを受信したため、設備保護の観点で企業A から送信されるメールの受信拒否を実施することにより、受信拒否されている間に、企業A から ISP B に送信したメールも受信拒否され、メールの遅延が発生する結果となる。

また、「Backscatter 問題」の変化版として、MSA を踏み台にして送信する場合もあります。

図表３　MSA を踏み台にした Backscatter 問題



- **迷惑メール送信者は 、ISP C のメールアドレスを詐称して、ISP A の MSA を踏み台にして、ISP B に迷惑メールを送信。**
- **ISP B では、存在しない宛先へのメールに対して、550 User Unknown としてエラー応答を返すため、それを受けて、ISP A では、ISP C に対して、エラーメール(NDR)を送信。**
- **ISP C では、ISP A から大量のメール(存在しない宛先が多く含む場合もある)を受信したことに対して、設備保護の観点で、ISP A から送信されるメールの受信拒否を実施。**
- **受信拒否がされている間に、ISP A から ISP C に送信したメールも受信拒否され、メールの遅延が発生。**

(3) 「お隣さん問題」や「Backscatter 問題」対策

これらの問題に対して、いくつかの技術的な対策が存在します。

「お隣さん問題」では、送信者認証を導入した上で、1 ユーザーあたりの単位時間のメール送信通数を制限し、送信できるメールの通数を制限することで、受信側で受信制限されにくくすることが可能です。

「Backscatter 問題」では、詐称されたドメインについて送信側として送信ドメイン認証技術を導入し、受信側で送信ドメイン認証技術の認証を実施することで、詐称されたメールであるかどうかを判断し、詐称されたアドレスから存在しないアドレスに送信された場合には、エラーメールを返信せずに破棄するという対応が可能になります。

また、存在しないあて先へメールが送信された場合には、SMTP セッションでエラー応答を返すことで、受信側でエラーメールを返さないようにすることも可能です。

その他にも、送信側で送信者認証を導入し、送信する際に認証したアカウントのアドレスを自動的に送信アドレスとして付与することで、アドレスを詐称した送信をできなくするという対応も可能です。

また、MSA を踏み台にされた「Backscatter 問題」に対しては、自ドメイン以外のメールの送信を禁止することでも対応可能です。さらに、第４章･第２節で説明した詐称送信制限機能を用いることで、本問題の発生を防ぐことができます。

しかし、これらの対策をするには、新規にその機能を導入する必要があり、費用がかかることのほか、導入までの時間がかかることや、ユーザーへの周知が必要なことなどいくつかの課題が発生します。

したがって、これらに代わる対策として、日々のログを分析し、問題が発生した場合には速やかに検知して、運用で対応する方法が考えられます。ただし、不特定多数のユーザーが収容されているシステムから送信されるメールのあて先は非常に種類が多く、集計するにも何らか基準が必要となります。ここでは調査の一例として次のような方法について説明します。

受信側で規制されるのは、通常は大量に送信される場合や存在しないあて先が多く含むメールが送信される場合になりますので、送信先の IP ごとに送信通数（あて先数）と存在しない宛先の数、送信元の IP アドレスの集計を行います。ここで、ある送信先 IP に対して、通

数が多い、存在しないあて先へのメールが多い、ある送信元 IP からのメール送信数が多い等に該当した場合は、受信側で規制される可能性があるメールを送信していると考えることができます。これらを組み合わせて分析することで、規制されるメールが送信されていたか否かを判断できるようになります。

これらを継続的に行うことで、受信側に規制される（規制される可能性がある）メールを送信していたかの判断が可能になり、必要に応じて該当の送信元を規制することで、外部へのメールの送信の抑止が可能になります。

メール送信が遅延する理由は、結果として受信側で制限されている場合でも、その理由は送信側の問題である場合も多くありますので、送信側はまず送り方に問題がないか調査することも重要になります。送信側で問題発生の原因がわかれば、該当の送信者に注意等を行うことで問題回避も可能になり、よりよいメール疎通環境を築くことができます。

2　アドレス未管理による問題

(1) 登録アドレスの変更・解除漏れによる問題

広告宣伝メールにおけるユーザーのアドレス管理は関係者の取り組みによりかなり厳格になってきていますが、一部の広告メールや緊急時の連絡に使われる防災系のメールや災害時に用いられる安否確認メール等では、依然として、アドレス管理の必要性が十分認知されておらず、適切な管理がされていない場合があります。

これらの問題は、前述に説明した問題と同様、受信者がアドレス変更や削除した場合に、設定を随時変更する必要がありますが、その変更を怠ることで徐々に存在しないあて先が多いメールを送信することになり、場合によっては受信側で制限されてメールが遅延するおそれがあります。

防災メールであっても、通信の秘密からその内容を見て特別な対応することは不可能であるため、送信側ではこのような問題が発生しないように対処しておかないと、万一の場合に、大事なメールが届かないという事象が発生しかねません。

本問題は、メーリングリストでも同様に発生するおそれがあります。メーリングリストのアドレス管理は、多くの場合には、登録したユーザーが自ら行うことになりますが、登録していることを忘れたり、変更方法がわからなかったりして、アドレス変更や削除があっても、そのまま放置されるケースがあります。この状態で送信されたメールは送信不可となり、その結果、送信失敗の通知がメーリングリスト管理者に送信されます。ここで、管理者がメンテナンスを行えば問題が肥大化することはありませんが、管理者が放置し続けた場合には、存在しないアドレスへのメールの送信が続くことになります。複数のメーリングリストを管理しているサーバーでは、このような送信先が重畳することにより、多数の存在しないあて先にメールを送信することとなってしまうおそれがさらに高くなります。

(2) アドレス管理方法について

前述のとおり、本来はそのサービスの利用者が変更する必要がありますが、一部の利用者はその変更を行わないという事実があります。したがって、サービス提供側が自主的に管理をする必要が出てきます。

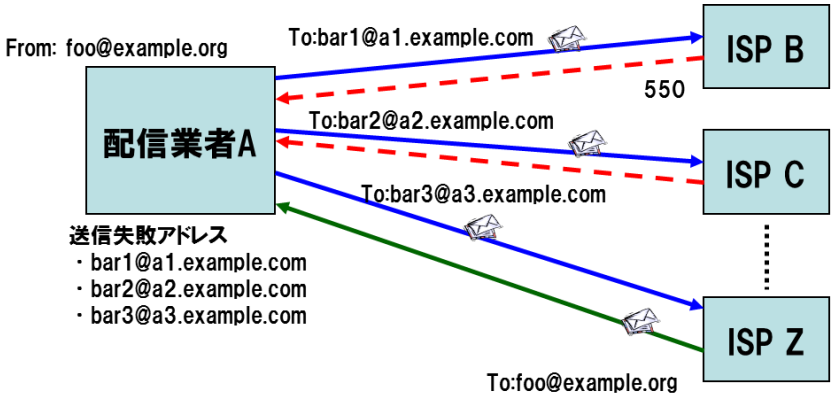
多くのメールサーバーは、RFC5321 で定義されているように、SMTP セッションの中で 550 のエラー応答を返しますので、メール送信時に 550 エラーになった送信先のアドレスを抽出しておきます。

また、一部のメールサーバーでは、一旦受信した後、エラーメールを返信する場合がありますので、受信したエラーメールから、存在しないものとされた送信先のアドレスを抽出しておきます。なお、エラーメールは、その送信元により形式がまちまちであるため、どのようなエラーメールのパターンがあるかを考慮して対応することが必要です。

このように抽出したアドレスに対して、アドレス管理簿から削除したり、一時的に送信を停止したりするようにして、次回配信からは送信しないようにすることで、存在しないあて先へ送信メールを抑止することが可能となります。

なお、何回の送信失敗でこの対応をするかは、そのサービス仕様（配信間隔等）に加えて送信先の仕様も考慮して決めることが望ましいものです。なぜならば、送信できない理由の一つに、一時的にメールアカウントが利用停止になっていたり、メール BOX がいっぱいで受信できなかったりする場合等があるからです。

図表４　アドレス管理方法



- ISP A、ISP B に送信した際に、550応答が返ってきたアドレスを抽出する。
- ISP Z から送ってきたエラーメールから、送信に失敗したアドレスを抽出する。
- 上記2つの方法で抽出したアドレスは、存在しないアドレスのため、管理しているアドレスリストから削除等を行う。
- これらの行為を都度実施し、存在しないアドレスにはメールを送信しないようにする。

また、メールの配信間隔が非常に長いシステムでは、その間に送信先アドレスが変更や削除されているものが含まれる可能性が高くなるため、定期的にアドレスの存在を確認するメールを送るなどの工夫も必要になってきます。また、メールアドレスを再利用している場合は、その間に別のユーザーのアドレスに変更されている可能性もあり、こうなると契約していないユーザーあてにメールを送信してしまうという問題も出てきます。

存在しないアドレスにあてて送信されるメールは、送信側・受信側のどちらからみても無駄なメールであることから、できる限り対処することが望まれます。

さらに、いくつかのメールサービスでは、メールアドレスの再利用を行う場合があります。正しくアドレスのメンテナンスが行われていないと、該当のアドレスについてメールサービスの解約・変更がされ、存在しないアドレスになった後、一定期間後に、別のユーザーにより再利用された際に、身に覚えのないメールを受信することになります。したがって、送信不可となったアドレスに対しては、速やかにメール送信を停止することが重要です。

3　時間バーストメールによる重畳問題

(1) 時間集中のメール

いわゆるメルマガなど、多くの受信者に対して、情報や広告などを提供するためのメールが非常に増えています。

これらのメールについて、いくつかの配信元では、決まった時間に送信を行う場合があります。この決まった時間に送信されるメールの特徴として、毎時 0 分にメールの送信を開始し、極短時間に送り続けるというものが多々見受けられます。

このようなメールの送信方法は、ある特定の送信元が行うのであれば、設備に与える負荷はそれほど大きくありませんが、同様の方法で送信する送信元が多数存在することで、通数が重畳され、受信側からみると、極短時間にバースト的に大量のメールが送信されることとなります。このようなメールを受信した場合には、受信側では設備保護の観点から受信制限をせざる得なくなる場合がありますが、送信元が多岐に渡っていると、1 つの送信元から送信されるメールは多量とはならないため、特定の送信元のメールを制限することができず、結果として、メール全体の受信数を制限せざるを得なくなります。この場合には、受信側で総量規制をすることとなり、すべての送信元からのメールが制限される可能性が出てきます。万が一、総量制限された場合は、このようなメールを送信していない送信元でも送信失敗となる可能性があり、もし送信失敗となった場合には、最低でも送信側のメール再送のタイミングの時間分だけ、遅延が発生することとなります。

また、携帯メールでは、メールを受信したことを携帯側に通知し自動受信するため、受信負荷に加えてメールの受信要求の負荷も同時間に

重畳されることとなり、サーバー負荷はさらに大きくなります。また、受信したメールがある特定地域に集中した場合には、該当の地域で一斉にメールの受信の要求が行われ、無線容量が不足して、受信要求が失敗するという事象が発生する場合もあります。

(2) 受信側を考慮した送信方法

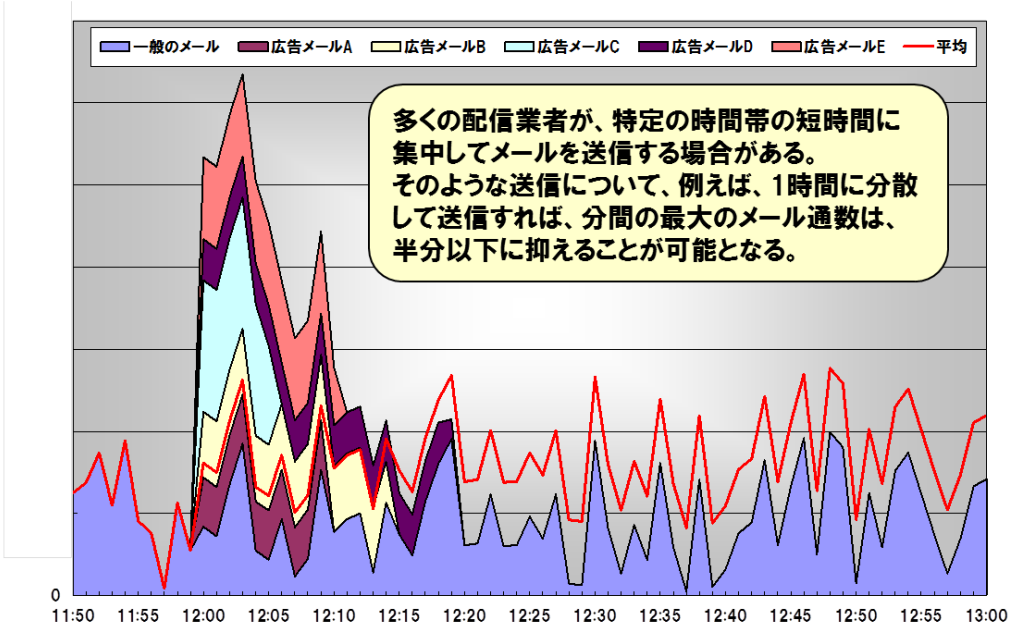
送信側が同様の考えを持ってメールを送信することで、メールがある特定時間に集中し、結果として受信側の処理能力を超えて、メールの受信が制限される事象を招くことは、受信側のみならず送信側にとってもいいことではありません。

したがって、広告メールを送信する際は、より多くの時間をかけて、広く薄く送信することが大事になります。例えば、1 万通のメールを 1 分で送った場合と、日勤帯 8 時間で送った場合では秒間当たりの通数は明らかです。したがって、メールを送信しても迷惑にならない時間帯で広く薄く送信するのが最良になります。

また、企業等から依頼を受けてメールを送信する配信事業者では、依頼する企業等に対して、短時間に集中してメールを送信するのは受信側に取って望ましくなく、結果として送信したいメールが送信できなくなる事象の発生しかねないことを啓発することが重要となります。

送信側が受信側の状況を理解し、かつ、周りにいる他の送信者の状況も考慮することが、良好なメール流通環境を築きあげるという認識を持つことが大事です。

図表 5　メール重畳の問題



参考3
用語集

（参考３）　用語集

インターネット	IP プロトコルを用いて全世界のコンピューターネットワークを相互接続したもの。分散管理されている。
（コンピューター）ウィルス	他人のコンピューターに様々な経路で侵入して動作するプログラム。感染したコンピューターは、システム破壊、データ改ざん、情報漏洩、他のコンピューターへの攻撃などに悪用される。
エラーメール	宛先不明や、メールサイズが大きすぎるなどメールを宛先に配送できない場合、送信元へエラーが発生したことを通知するメール。エラーメールの送信先には、送信者情報を用いる。
エンベロープ	メールサーバー間でやり取りする実際の送信元や宛先を示す通信データ。メールヘッダーの From や To とは異なっている場合がある。
オプトイン	事前に同意を取得するということ。事前に同意した者にのみ広告・宣伝メールを送ることができる。未承諾の者には原則、広告・宣伝メールを送ることはできない。
オプトアウト	事後に同意を拒否するということ。事前に同意なく広告・宣伝メールを送り、受信拒否をした者にのみ今後広告・宣伝メールを送らない方式。
オープンリレー	誰でも使用できる状態の SMTP サーバーのこと。認証なしに誰でも使用できるため、迷惑メール送信者により踏み台にされ送信者の特定を難しくする。また、一般の PC もウィルスに感染するなどして同様の状態になることもある。
架空請求	サイト利用料や事故の慰謝料などと称して、実体のない請求によって金銭を詐取する詐欺行為。
携帯電話不正利用防止法	振り込め詐欺などに代表される架空請求に携帯電話が使用されることが多く、その対処のために携帯電話契約時に本人確認などを義務付けた法律。
経路情報	電子メールは、メールサーバーで中継される際に、どのメールサーバーをいつ経由したかという情報をメールヘッダーに記録する。この経路情報は郵便の消印のようなものであるが、詐称することも可能。
公開鍵暗号技術	公開鍵と秘密鍵という 2 つの鍵を用いて、データの暗号化・復号化を行う暗号方式。迷惑メール対策技術の中では、送信ドメイン認証技術の一つである DKIM において利用される。
スロットリング	1 つの IP アドレスからのセッションの接続数を制限することにより、電子メールの流量を制限する方法。
送信者情報	電子メールの送信者の情報。エンベロープ From（メールヘッダーには Return-path として記録される）がメールサーバー間で使用される送信者情報となる。
ダブルオプトイン	オプトインの際のなりすましや誤入力防止のため、Web から入力されたメールアドレスに対して、登録用 URL などを送信し、利用者本人の再確認を行う手法。
チェーンメール	このメールを「誰かに回して」や「○○人に転送するように」などと書かれているメール。送らないと、幽霊や呪いなどで恐怖心をあおることもある。チェーン（鎖）のようにメールの転送がつながっていくことからこのように呼ばれている。
電子署名	本人確認や、偽造・改ざんの防止に用いる電子的な署名。
電子メール	コンピューターや携帯電話でメッセージをやり取りする文やデータ。
SMTP（エスエムティーピー）	Simple Mail Transfer Protocol の略。インターネットで電子メールを転送するための通信プロトコル。RFC5321、RFC5322。
POP（ポップ）	Post Office Protocol の略。メールサーバーから電子メールを取り出すときに使用される通信プロトコル。RFC1939。
IMAP（アイマップ）	Internet Message Access Protocol の略。メールサーバー上に保存されている電子メールに直接アクセスすることができる通信プロトコル。RFC3501。
MSA（エムエスエー）	Message Submission Agent の略。MUA から発信されたメールを受け取るサーバー。MTA と同義で使用することもあるが MSA は、SMTP Auth や POP before SMTP などの認証機能や不完全なメールヘッダーの修正を行う機能を提供する。

エムティーエー ＭＴＡ	Mail Transfer Agent の略。電子メールをクライアントーサーバー間・サーバーーサーバー間で転送するサーバー。
エムユーエー ＭＵＡ	Mail User Agent の略。いわゆるメールクライアントであり、電子メールを使用するもののユーザーインターフェイスとなる。例えば Microsoft Outlook や Mozilla Thunderbird などである。
エムエックス ＭＸレコード	Mail eXchange レコードの略。DNS サーバーに定義された受信メールサーバーのホスト情報など
電子メールアドレス	電子メールの送信先や送信元を表すもの。ローカルパート（氏名」）＠ドメインパート（手紙で言う「住所」）で表わされる。
特定電子メール法	電子メールの送受信にかかる良好な環境を整備するために制定された法律。インターネットや電子メールの送受信の環境整備の観点から規定。
特定商取引法	特定の商品の取引に関する販売のルールを定めた法律。電子メールによる広告・宣伝の方法についても通信販売の観点から規定。
ドメイン	インターネット上に存在するコンピューターやネットワークを識別する名前。重複しないように ICANN と言う国際組織により一元管理されている。
送信ドメイン認証	メール送信元のドメインの DNS に問い合わせることにより、そのメールが確かにメール送信元として記されたメールサーバーから送信されたものであるか確認する機能。送信ドメイン認証技術を利用することにより、送信元の詐称を防ぐことができる。電子メールが普通の手紙に勝っている 1 例である。
エスピーエフ ＳＰＦ	Sender Policy Framework の略。送信ドメイン認証技術の一つ。エンベロープ情報の From メールアドレスのドメイン名をチェックし、当該 DNS に確認を行い送信元情報の真偽を確認する。RFC4408。
センダーアイディー SenderID	送信ドメイン認証技術の一つ。SPF と同様のチェックに加え、Resent-sender: → Resent-from: → Sender: → From: 順序でヘッダー情報の送信ドメインをチェックし、当該 DNS に確認を行い送信元情報の真偽を確認する。RFC4406。
ディーキム DKIM	DomainKeys と IIM を合わせた電子署名の技術。送信元が付した電子署名により送信元情報の真偽及び電子メールの本文の改変を検知することができる。RFC4871, 5672。
ハーベスティング	メールサーバーがエラー情報を返す機能を悪用し、機械的に作成した大量のメールアドレスをメールサーバーに送り、実際に利用されているメールアドレスを確認する手法。ハーベスティングに対抗するためにメールサーバーは、エラーが大量に発生する通信を遮断したりしている。
配信サービス事業者	電子メールの配送を代行する事業者。多くの電子メールを短時間に同時配信できるなどのサービスを提供する。
バウンスメール	「エラーメール」を参照。
表示義務	特定電子メール法や特定商取引法に規定されている。広告・宣伝メールを送る際にメール本文やメールに記載した URL などから転送で表示しなければならない事項がある。
フィッシング	銀行やクレジットカードなどの金融機関やオンラインサービスを提供する事業者からのメールを装ってカード番号や暗証番号、パスワードなどを不正に入手するサイトへ誘導する。
フィルタリング	迷惑メールの特徴や送信元情報などをあらかじめデータ化して、受信メールと照らし合わせ機械的に判断し、迷惑メールと判断したメールを専用フォルダに格納したり削除したりする機能。
シグネチャーフィルター	あらかじめ多くの迷惑メールから取得した特徴を「シグネチャー」として記録し、それらの「シグネチャー」と届いたメールと比較して迷惑メールか判定する手法。（Signature Filter）
ヒューリスティックフィルター	メールヘッダーや本文から迷惑メールの特徴をスコア化し、スコアが一定条件になった場合に迷惑メールと判定する手法。例えば、迷惑メールに多く含まれるワードや送信に使用したメールクライアントがない場合にスコアが上がる。（Heuristic Filter）
ベイジアンフィルター	メール受信者が迷惑メールを判定した判断基準を自己学習し、統計学的に迷惑メールと判定する手法（Bayesian Filter）

フリーメール	電子メールサービスは、基本的に ISP や企業内で対価を払って有償で提供されるが、無料サービスとして提供されている場合もある。フリーメールからのメールには、Web メールの表示画面の周囲やメール本文の前後に広告・宣伝が入るものもある。
ボット	コンピューターがウィルスに感染することにより他人に遠隔操作されてしまう状態にあること。ロボット(robot)のように外部から操作させられることから、ボット（bot）やゾンビ PC（Zombie PC）とも呼ばれる
ボットネット	インターネットに接続されているボットによるネットワーク。指令者の特定が難しく犯罪に使用されやすい。迷惑メールもボットネットからの送信が非常に多いといわれている。
ポート	IP 上の TCP や UDP のサービス番号。アプリケーション毎に割り当てられる。電子メールでは SMTP に 25 番、POP に 110 番、投稿ポートに 587 番などが割り当てられている。
ホスティングサービス	レンタルサーバーともいわれる。インターネット・データセンターに設置されたサーバーを間借りできるサービス。サーバーの設置、管理にかかる人員やコストを外部委託により削減できる場合がある。
ホワイトリスト	自分の知っているメールアドレスや IP アドレスをリスト化しているデータベース。自身や ISP などで登録するため、ほぼ確実に安全なアドレスのリストなる。通常、ホワイトリストに登録すると各種フィルターはかからない。
マルウェア	不正ソフトウェアともいい悪意を持って作成されたソフトウェアの総称。
メールサーバー	電子メールをインターネット上で送受信するサービスを提供する。手紙で言う郵便局のような存在。
メールヘッダー	電子メールの制御情報データを記述してある部分。宛先、送信元、題名などの他に、発信されたメールサーバーや中継されたメールサーバーなどの経路情報も記述されている。
迷惑メール追放支援プロジェクト	総務省、経済産業省、ISP などが協力して迷惑メールの発信元となっている国内 ISP に対して、迷惑メール情報を送り、ISP の約款に基づく利用停止処置などの対応を促すプロジェクト。
ラベリング	プロバイダーの迷惑メール対策ソフトなどが受信したメールのヘッダー・件名や本文などに何かしらの情報を記述すること。例えば迷惑メールである可能性が高いメールの場合、件名に[meiwaku]と記述したりできる。
ＡＲＦ（エーアールエフ）	Abuse Reporting Format の略。メールの送信元に迷惑メール報告されていることやオプトインが無いことをフィードバックするための規格。
APCAUCE（エーピーコース）	The Asia Pacific Coalition Against Unsolicited Commercial Email の略。迷惑メール対策をアジア太平洋地域において連携していく活動。
DKIM（ディーキム）	「送信ドメイン認証」を参照。
ＤＮＳ（ディーエヌエス）	Domain Name System の略。ドメイン名と IP アドレスを対応付けるデータベースシステム。インターネット上のコンピューターにアクセスするためには IP アドレスを知らなければならないが、直接数字入力するのは実用的ではないので、名前を用いてアクセスする方法が考案された。
DoS攻撃（ドス）	Denial of Service 攻撃の略。サーバーに対して処理能力を超える負荷をかけることで、サーバーのサービス提供をできなくする攻撃のこと。
ＩＥＴＦ（アイイーティーエフ）	The Internet Engineering Task Force の略。インターネット上で利用される技術の標準化を行う組織。策定された標準仕様は、RFC（Request For Comment）として発行している。
IMAP（アイマップ）	「電子メール」を参照。
ＩＰアドレス（アイピー）	インターネット上で個別の端末を判別するための番号。
ＩＰ２５Ｂ（アイピーニーゴービー）	Inbound Port 25 Blocking の略。受信側のメールサーバーが動的 IP アドレスから 25 番ポートを使用して送信してくる電子メールをブロックする。
ＩＲＣ（アイアールシー）	Internet Relay Chat の略。サーバーを介し、クライアントークライアント間での文章のやり取りを行う仕組み。IRC のサーバーはネットワークを組んでおり、クライアントがどれかのサーバーに接続すると、他のサーバーに接続されているクライアントと通信が可能になる。サーバーをリレーするので

	Internet Relay Chat と呼ぶ。
アイエスピー ＩＳＰ	Internet Service Provider の略。インターネットに接続するサービスの提供を行う企業や団体をいう。
ジーグ JEAG	Japan Email Anti-Abuse Group の略。日本の通信関連企業が集まった迷惑メール対策の技術検討を行うグループ。
ラップ LAP	London Action Plan の略。2004 年 10 月にロンドンで開催された迷惑メール対策の会議の後に開始した迷惑メール対策のための国際協力実施計画。
マーグ MAAWG	Messaging Anti-Abuse Working Group の略。迷惑メールを含めた、インターネット上のウィルスや 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。
マイム MIME	Multipurpose Internet Mail Extension の略。従来、US-ASCII 文字（英数字＋半角記号文字）しか扱えなかったメールを、これを拡張してその他の文字や画像などを扱えるようにした規格。
エムエスエー ＭＳＡ	「電子メール」を参照。
エムユーエー ＭＵＡ	「電子メール」を参照。
エムティーエー ＭＴＡ	「電子メール」を参照。
オーピーニージービー ＯＰ２５Ｂ	Outbound Port 25 Blocking の略。ISP が自社のネットワークの動的 IP から 25 番ポートを利用して他の電子メールサーバーに電子メールを送信することをブロックする。
ピアツーピア Ｐ２Ｐ	Peer to Peer の略。サーバークライアントで構成される一般的なネットワークとは異なり、中央で処理するサーバーがなく、クライアントクライアント間のみで通信する形態をいう。
ポップ POP	「電子メール」を参照。
ポップ ビフォア エスエムティーピー POP before ＳＭＴＰ	メールを受信するために使用する POP の認証を利用し、POP の認証後の一定時間に同じ IP アドレスからの SMTP によるメールの送信を許可する仕様。ただし、POP の認証元は保証できるが、SMTP の処理を保証しているわけではない。
ディーエヌエスビーエル ＤＮＳＢＬ	DNS Black(Blackhole とも) List の略。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からは、DNS を利用して、情報を利用する。
アールエフシー ＲＦＣ	Request for Comments の略。IETF で策定されたインターネット上の技術の仕様書。例えば SMTP は RFC 5321 として策定されている。
センダーアイディー SenderID	「送信ドメイン認証」を参照。
エスエムエス ＳＭＳ	Short Message Service の略。携帯電話や PHS で短文を送受信するサービス。電話番号だけで送信可能。
エスエムティーピー ＳＭＴＰ	「電子メール」を参照。
エスエムティーピー オウス ＳＭＴＰ Auth	SMTP Authentication の略。郵便のポストと同じで誰でも電子メールを送付することができる SMTP に認証機能を加えた仕様。
エスピーエフ ＳＰＦ	「送信ドメイン認証」を参照。
ユーアールエル ＵＲＬ	Uniform Resource Locator の略。インターネット上の Web ページなどを特定するための文字列。http://www.dekyo.or.jp/soudan/anti_spam/index.html などで表わされる。

参考4
関連資料

（参考４）　関連資料

1　関連組織

組織名	URL
総務省	http://www.soumu.go.jp/main_sosiki/joho_tsusin/d_syohi/m_mail.html
経済産業省	http://www.meti.go.jp/policy/economy/consumer/consumer/tokutei/index.html http://www.no-trouble.jp/#1200000
消費者庁	http://www.caa.go.jp/representation/
財団法人日本データ通信協会 迷惑メール相談センター	http://www.dekyo.or.jp/soudan/
財団法人日本産業協会 電子商取引モニタリングセンター	http://www.nissankyo.or.jp/e-commerce/
財団法人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/
JEAG (Japan Email Anti-abuse Group)	http://jeag.jp/

2　関連資料

資料	概要	入手方法
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	特定電子メール法･同法施行規則の条文、ガイドライン	総務省ウェブページで入手可能（http://www.soumu.go.jp/main_sosiki/joho_tsusin/d_syohi/m_mail.html） 消費者庁ウェブページで入手可能（http://www.caa.go.jp/representation/index.html）
特定電子メールの送信の適正化等に関する法律のポイント	特定電子メール法の平成 20 年改正の概要をまとめたパンフレット（総務省・日本データ通信協会作成）	総務省ウェブページで入手可能（http://www.soumu.go.jp/main_sosiki/joho_tsusin/d_syohi/m_mail.html#ordinance） 消費者庁ウェブページで入手可能（http://www.caa.go.jp/representation/pdf/091214premiums_1.pdf） 日本データ通信協会ウェブページで入手可能（http://www.dekyo.or.jp/soudan/houritupoint/index.html）
特定商取引に関する法律等	特定商取引法・同法施行規則の条文、ガイドライン	経済産業省ウェブページで入手可能（http://www.meti.go.jp/policy/economy/consumer/consumer/tokutei/jyoubun/index.html） 消費生活安心ガイドのウェブページで入手可能（http://www.no-trouble.jp/#1400000）

利用者向け資料		
撃退！迷惑メール	受信者が気をつけることをまとめた冊子 （日本データ通信協会作成）	日本データ通信協会ウェブページで入手可能 （http://www.dekyo.or.jp/soudan/taisaku/）
撃退！チェーンメール	チェーンメール対策をまとめパンフレット （日本データ通信協会作成）	日本データ通信協会ウェブページで入手可能 （http://www.dekyo.or.jp/soudan/chain/）
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・公表されているもの （総務省作成）	総務省ウェブページで入手可能 （http://www.soumu.go.jp/main_sosiki/joho_tsusin/d_syohi/m_mail.html#technical）
携帯電話宛て迷惑メール対策についての JEAG recommendation	携帯電話宛の迷惑メールへの技術的な対策についての勧告 （JEAG 作成）	JEAG ウェブページで入手可能 （http://jeag.jp/swg/wireless/index.html）
Outbound Port25 Blocking についての JEAG recommendation	OP25B についての勧告 （JEAG 作成）	JEAG ウェブページで入手可能 （http://jeag.jp/swg/op25b/index.html）
送信ドメイン認証についての JEAG recommendation	送信ドメイン認証についての勧告 （JEAG 作成）	JEAG ウェブページで入手可能 （http://jeag.jp/swg/senderauth/index.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）	インターネット協会ウェブページで入手可能 （http://www.iajapan.org/anti_spam/portal/）
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２５番ポートブロックに関して、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）	総務省ウェブページで入手可能 （http://www.soumu.go.jp/main_sosiki/joho_tsusin/d_syohi/jigyosha.html）
国際連携		
ロンドン行動計画		総務省ウェブページで入手可能 （http://www.soumu.go.jp/main_sosiki/joho_tsusin/d_syohi/m_mail.html#international）
スパム対策の協力に関するソウル・メルボルン多国間 MoU	総務省・経済産業省が締結 （平成 17 年（2005 年）4 月 27 日）	
反スパム政策・戦略分野における日仏間の協力に関する共同声明	日仏の共同声明 （総務省・経済産業省が平成 18 年（2006 年）5 月 5 日に締結）	
商業用電子メール政策の協調に関する日英共同宣言	日英の共同声明 （総務省・経済産業省が平成 18 年（2006 年）9 月 13 日に締結）	
反スパム政策・戦略分野における日加間の協力に関する共同声明	日加の共同声明 （総務省・経済産業省が平成 18 年（2006 年）10 月 3 日に締結）	
迷惑メール対策に関するドイツ連邦経済技術省との共同声明	日独の共同声明 （総務省・経済産業省が平成 19 年（2007 年）7 月 31 日に締結）	

参考資料

1　迷惑メール対策推進協議会設置要綱

「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）　迷惑メール対策に係る実務的な問題に係る情報共有、対策の検討等を行うため、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、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

迷惑メール追放宣言

我が国では、インターネットや携帯電話の発展・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負担、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障碍、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生じている。さらに、迷惑メールが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、電子メールというコミュニケーション手段の信頼性が脅かされる状況となっている。

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始められた。本年には、両法の改正により、いわゆるオプトイン規制が導入されるなど、実効性の向上に向けた規制の強化が図られている。

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あわせて必要とされる。

本日、迷惑メール対策に関わる関係者が広く集まり、「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

関係者が講ずるべき取組の例

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に関する情報提供
・迷惑メール対策に関する関係者への情報提供

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
・迷惑メール対策に関する関係者への情報提供

配信事業者
・広告・宣伝メールの適切な配信
・迷惑メール対策に関する関係者への情報提供

セキュリティベンダー等
・効果的な迷惑メール対策製品等の提供
・迷惑メール対策に関する関係者への情報提供

消費者団体等
・利用者側で行える迷惑メール対策についての消費者に対する情報提供

行政機関等
・法の迅速かつ適正な執行
・迷惑メール対策に関する関係者への情報提供
・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
・迷惑メール対策に係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
・迷惑メール対策に関する関係者への情報提供

3　迷惑メール対策推進協議会構成員

2011 年 8 月 1 日現在

有田　道生	エイケア・システムズ株式会社　代表取締役
石田　幸枝	社団法人全国消費生活相談員協会　ＩＴ研究会代表
井上　統之	ＫＤＤＩ株式会社　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部　部長
浦川　有希	独立行政法人国民生活センター　相談部調査役補佐
大野　謙一	アイマトリックス株式会社　カスタマーリレーション第二営業部　部長
岡村　久道	弁護士　国立情報学研究所客員教授
奥山八州夫	社団法人電気通信事業者協会　専務理事
岸原　孝昌	一般社団法人モバイル・コンテンツ・フォーラム　常務理事
桑子　博行	社団法人テレコムサービス協会　サービス倫理委員会委員長
斎藤　雅弘	弁護士
佐久間　修	大阪大学大学院　高等司法研究科教授
櫻庭　秀次	株式会社インターネットイニシアティブ　サービス本部 アプリケーションサービス部シニアエンジニア
沢田登志子	一般社団法人ＥＣネットワーク　理事
四方　光	警察庁　生活安全局情報技術犯罪対策課長
島野　公志	ソフトバンクモバイル株式会社　プロダクト・マーケティング本部 エンタープライズ・サポート統括部長
末政　延浩	センドメール株式会社　代表取締役社長
鈴木　信也	総務省　総合通信基盤局電気通信事業部消費者行政課長
須山　勇	イー・アクセス株式会社　総務本部　本部長
関　聡司	楽天株式会社　執行役員　広報渉外室　室長
竹岡　敏行	一般社団法人インターネット広告推進協議会　常務理事兼事務局長
立石　聡明	社団法人日本インターネットプロバイダー協会　専務理事兼副会長
田中　隆代	全国消費者団体連絡会　事務局
谷井　等	シナジーマーケティング株式会社　代表取締役社長
築島幸三郎	社団法人日本ケーブルテレビ連盟　理事・事務局長
永江　禎	社団法人日本広告業協会　法務委員長
長田　三紀	特定非営利活動法人東京都地域婦人団体連盟　事務局次長
新美　育文	明治大学　法学部教授
長谷部恭男	東京大学大学院　法学政治学研究科教授
畑野　浩朗	消費者庁　取引対策課長
花戸　俊介	トライコーン株式会社　代表取締役
早貸　淳子	一般社団法人ＪＰＣＥＲＴコーディネーションセンター　常務理事
林　一司	ニフティ株式会社　執行役員
林　博史	社団法人日本アドバタイザーズ協会 Ｗｅｂ広告研究会事務局オフィスマネージャー
原　隆一	エヌ・ティ・ティ・コミュニケーションズ株式会社取締役 ネットワークサービス部長
春田　真	株式会社ディー・エヌ・エー　常務取締役 総合企画部長
樋口　貴章	財団法人インターネット協会　迷惑メール対策委員会委員長
平野　祐司	ソフォス株式会社　マーケティング部　部長
深井雄一郎	株式会社パイプドビッツ　取締役副社長兼ＣＯＯ（最高執行責任者）
藤生　昌也	シスコシステムズ合同会社　プロダクトマーケティング　プロダクトマネージャ
藤本　恭史	マイクロソフト株式会社　コンシューマー＆オンラインマーケティング統括本部 コンシューマーWindows 本部 本部長兼ウィンドウズライブ本部 本部長
別所　直哉	ヤフー株式会社 CCO（チーフ・コンプライアンス・オフィサー）兼法務本部長
逸見　久雄	財団法人日本産業協会 事務局長・電子商取引モニタリングセンター センター長
松本　恒雄	一橋大学大学院　法科大学院長・法学研究科教授
村上　智	株式会社シマンテック　システムエンジニアリング本部　本部長
村松　茂	財団法人日本データ通信協会　迷惑メール相談センター所長
柳澤　隆治	株式会社エヌ・ティ・ティ・ドコモ スマートコミュニケーションサービス部　担当部長

索 引

索　引

迷惑メール対策ハンドブック 2011

2011 年 8 月発行

企画・著作・制作　　迷惑メール対策推進協議会

（事務局）

（財）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

URL　　http://www.dekyo.or.jp/soudan/

TEL：03-5907-5371