第２章

迷惑メールについて

第1節　電子メールとは

1　電子メールなど

個人や組織の間で交わされる情報は、以前は手紙やハガキ、電話やファックスなどでやりとりされていましたが、近年では電子メールやメッセージアプリなどを利用し、インターネット経由でやりとりすることが増加しています。なかでも電子メールについては、1993 年のインターネットの商用利用の開始以降、次々に誕生した ISP がインターネット接続を開始し、その利用が広がり、1999 年に(株)NTT ドコモの携帯電話で i モード[注 32]が開始されるなど、携帯電話のネットワークからもインターネットへの接続が可能となったことにより、その利用はより身近なものとなりました。また、ブロードバンド化の急速な進展などに伴い、現在では、電子メールは、社会経済活動や市民生活において必要不可欠な連絡・伝達の手段となっています。

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

図表２－１－１　電子メールなどのメッセージ交換サービスの主な種類

電子メール（SMTP）	電子メール（SMTP）とは、SMTP（Simple Mail Transfer Protocol）という通信方式を使用して、電子メールアドレスを宛先にし、インターネットを介してテキストや画像などをやり取りするサービスです。その際、電子メールアドレスは「利用者名@ドメイン名」で表記され、個人を識別する利用者名と、所属する組織やサービスを提供する事業者などをあらわしたドメイン名で構成されます。電子メールは、パソコンなどでメールソフトを利用したり、携帯電話を利用したり、インターネットのブラウザを利用したり（Web メール）、様々な方法で送受信されます。
SMS	SMS とは、Short Message Service の略で、電話番号を宛先にし、携帯電話事業者のネットワークを介して、短いテキストをやり取りするメッセージングサービスです。事業者によって多少呼び名や機能が異なりますが、携帯電話事業者のネットワークを利用して、数十文字程度のメッセージや絵文字を携帯電話同士で送受信することが可能です。ただし、写真や動画などは送受信できません。
SNS	SNS とは、Social Networking Service(Site)の略で、インターネット上で友人を紹介しあい、個人や組織間の交流を支援するサービス（サイト）です。利用者は自身のプロフィールなどを公開できるほか、その SNS 上で友人などのプロフィールなどを閲覧したり、コメントしたり、メッセージを送ったりすることができます。最近では、会社や組織の広報としての利用も増えてきました。

注32 1999 年 2 月に NTT ドコモが携帯電話向けサービスとして開始した、電子メールの送受信や Web ページの閲覧などができるインターネットサービス。

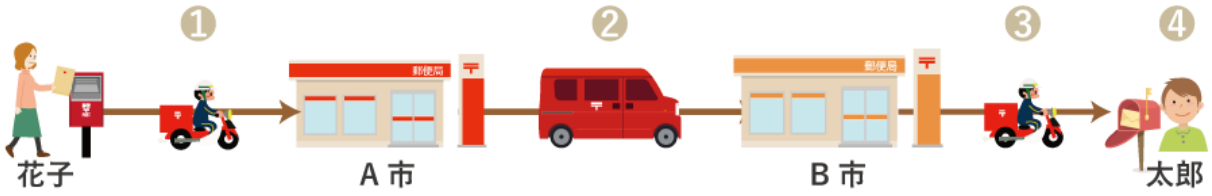
2　電子メールの仕組み

メールソフト[注 33]で文章を書いて「送信」をクリックすると、その文章が相手に届きます。いつも私たちが便利に使っている電子メールですが、そもそもどのような仕組みになっているのでしょうか。SMTP を使った電子メールの送信などの仕組みを郵便の仕組みにたとえながら説明していきます。

（１）　送受信の仕組み

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

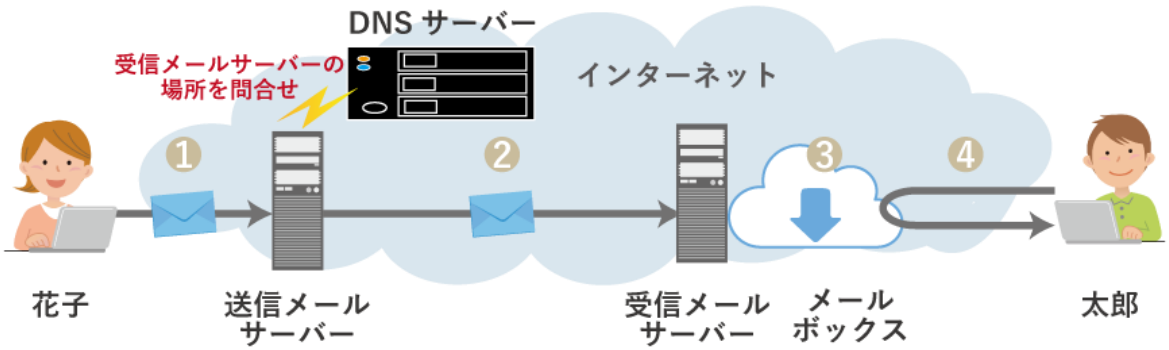
図表２－１－２　郵便物の配達



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

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

図表２－１－３　電子メールの配送



注33 MUA（Mail User Agent）といい、Microsoft Outlook や Mozilla Thunderbird などのメールクライアントソフトウェアを指す。

1. 電子メールが送信メールサーバー[注34]に投稿される（ポストへの投函と最寄りの郵便局への配送に当たります）
2. 投稿された電子メールが、送信メールサーバーから受信メールサーバーに配送される※（最寄りの郵便局から宛先の郵便局への配送に当たります）
3. 受信メールサーバーから、受信者のメールボックスに電子メールが保存される（宛先の郵便局から住所への配達に当たります）
4. 受信者が受信メールサーバーに対して自らの端末への配送要求を行い、電子メールを受信する（ポストの確認・受取りに当たります）[注35]

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

（２）　宛先の仕組み

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

電子メールでも、手紙の場合と同様に、封筒に書かれた宛先や差出人にあたる情報と、便箋に書かれた宛先や差出人にあたる情報があり、いずれも電子メールアドレスが用いられます。手紙の場合の封筒に書かれた情報にあたる情報は「Envelope-To」及び「Envelope-From」[注36]と、便箋に書かれた情報にあたる情報は、「Header-To」及び「Header-From」[注37]といいます。このうち、電子メールの配送に用いられるのは、「Envelope-To」のみであり、他の情報は、配送には用いられず、どのような情報（電子メールアドレス）でも利用が可能です。送信元を偽装したなりすましメールが送信されることがあるのは、このためです[注38]。

なお、郵便の場合と異なり、「Envelope-To」及び「Envelope-From」は、メールサーバー間の通信においてのみ用いられ、受信者に届けられることなく、メールソフトで表示される宛先・差出人は、「Header-To」及び「Header-From」の情報になっています[注39]。

注34 MSA（Message Submission Agent）といい、電子メールを送信する際に接続するメールサーバーを指す。

注35 電子メールを受信するための通信方式として、ユーザーが受信メールサーバーへアクセスして受信した電子メールをパソコンなどに保管する「POP」という方式や、電子メールを受信メールサーバーに置いたまま管理する「IMAP」という方式があります。

注36 電子メールの通信プロトコルである SMTP（Simple Mail Transfer Protocol）の仕様を定めた RFC5321 では、「Envelope-To」、「Envelope-From」は、それぞれ「forward-path」、「reverse-path」とされています。

注37 インターネットメッセージの仕様を定めた RFC5322 では、「Header-To」、「Header-From」は、それぞれ「destination field」、「from field」とされています。

注38 「Envelope-To」以外の情報を自由に記載できることには、メリットもあります。例えば、「Header-To」と「Envelope-To」 が分かれていることにより、他の受信者に電子メールアドレスが見えないように宛先を指定する BCC（「Header-To」には表示されないが、「Envelope-To」には設定されている。）での送信が可能になっています。

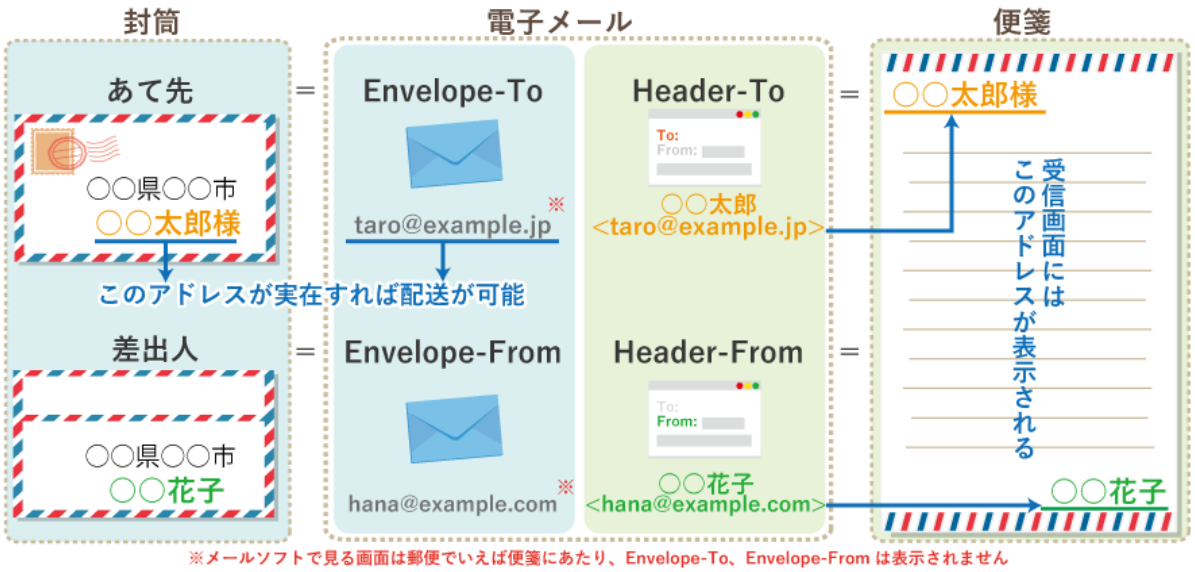
注39 「Envelope-To」および「Envelope-From」を配送上の受信者情報・送信者情報、「Header-To」および「Header-From」をメールヘッダーの受信者情報・送信者情報ということもあります。

以上を、比較表ならびに図式にしてみると次のようになります。

図表２－１－４　郵便と電子メールの比較表

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

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



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

第2節　迷惑メールとは

1　迷惑メールの特徴

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

（1）受信者の意思に反する

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

（2）迷惑な内容が含まれる

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

（3）迷惑な手法で送信する

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

２　迷惑メールの具体例

（１）事前同意のない広告・宣伝メール

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

事前同意のない広告・宣伝メールの例（出会い系のメール）

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

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

I XXXX YOU

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

（２）詐欺メール

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

- フィッシング

  金融機関など一般消費者の認知度の高い企業やブランドを装った電子メール（フィッシングメール）を送り、口座番号、パスワード、クレジットカード番号などの個人情報を詐取する行為です。電子メールの URL から本物と見分けのつかない偽サイトに誘導し、そこで個人情報を入力させる手口が一般的に使われています。

- ビジネスメール詐欺（BEC）

  取引先などを装い、それになりすました偽のメールを送り、用意した口座などに金銭を振り込ませ詐取する行為です。攻撃者は、担当者がメールで取引を進めている間、不正アクセスしたシステムでやりとりを盗み見ます。金銭の請求段階に入ったところで、取引先になりすましたメールを送信して担当者をだます手口が一般的に使われています。

詐欺メールの例（架空請求のメール）

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

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

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

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

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

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

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

（３）ウイルスメール

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

ウイルスメールの例（当選を装ったメール）

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

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

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

（４）チェーンメール

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

チェーンメールの例（不幸の手紙系、募集系のメール）

＜不幸の手紙系のメール（脅かして転送を促す内容）＞

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

＜募集系のメール（善意の気持ちから転送を促す内容）＞

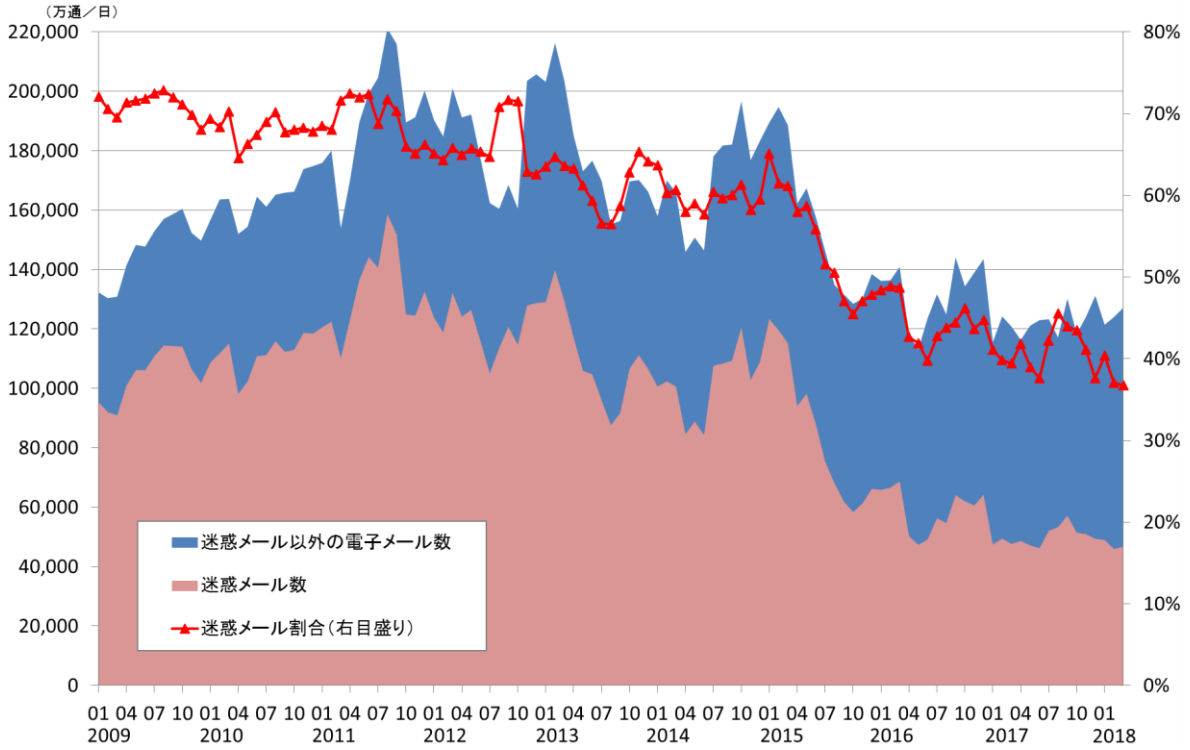
友人の子どもがＲＨマイナスＢ型の血液不足で手術が受けれない状態です！誰かＲＨマイナスＢ型の方いませんか！？
１人の幼い子の命がかかっていて、とても危険な状態だそうです！
最寄りの献血センターで献血できるようなので、是非是非協力おねがいします！
分からないことあればいつでも連絡ください！090********
なかなかない血液みたいで、私だけの人脈だと間に合わないのでおねがいします！

第3節　迷惑メールの動向

1　全体的傾向

日本では、2001 年頃から迷惑メールが社会問題になった後、電気通信事業者などの関係者により、様々な迷惑メール対策が講じられてきました。国内の ISP の取り扱う国内着の電子メールのうち、迷惑メールの占める割合は減少傾向にあり、2012 年までは 70%前後の高い水準にありましたが、それ以降は徐々に減少し、2018 年３月では 40%を切る状況になりました。このように、迷惑メールそのものが減少している上、このうちのかなりの部分は電気通信事業者のフィルターなどで対応されていることから、実際に利用者に届く迷惑メールは減少していることが考えられます。

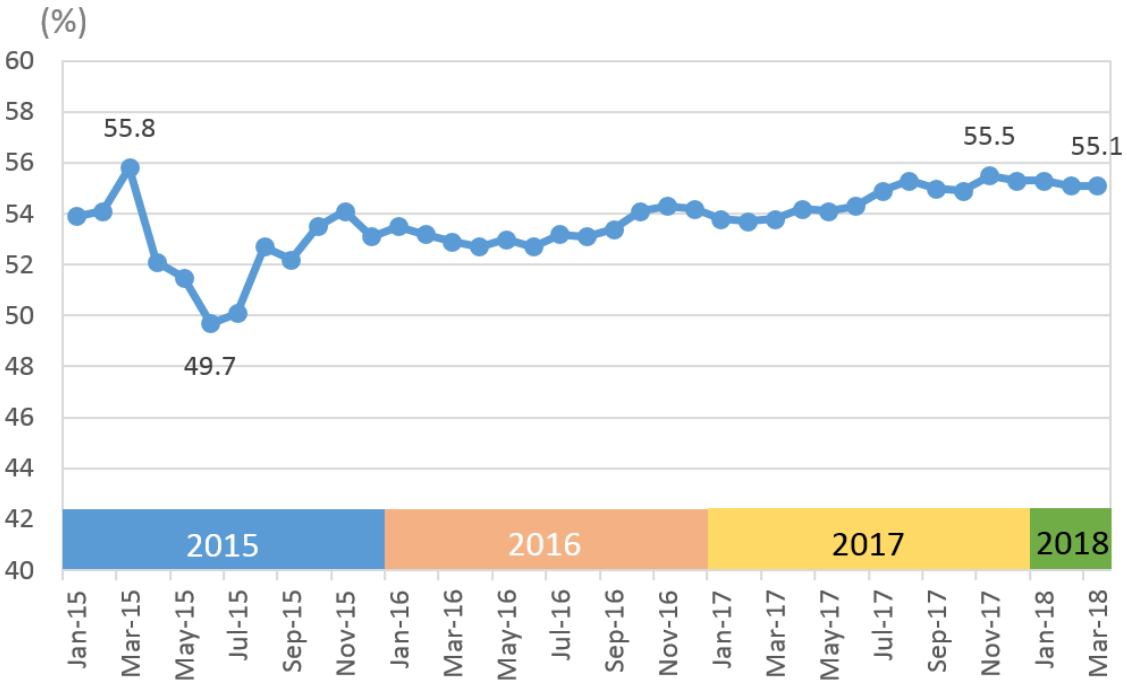
図表２－３－１　国内 ISP における迷惑メール数・割合の推移



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

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

図表２－３－２　世界的な迷惑メールの割合



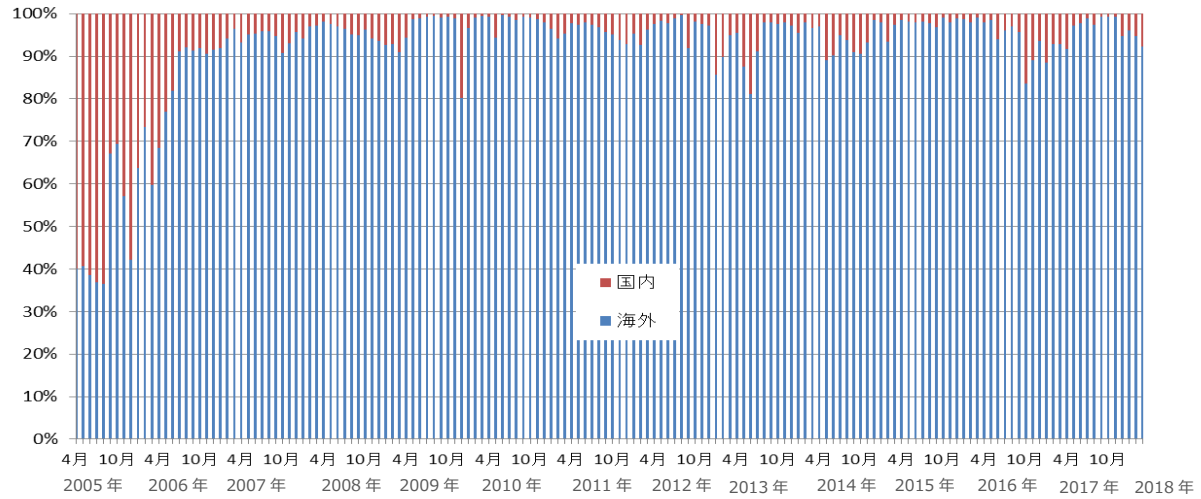
出典：シマンテック「2017 年インターネットセキュリティ最新レポート　セキュリティレスポンスブログ」

2　国内発の迷惑メールの割合

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

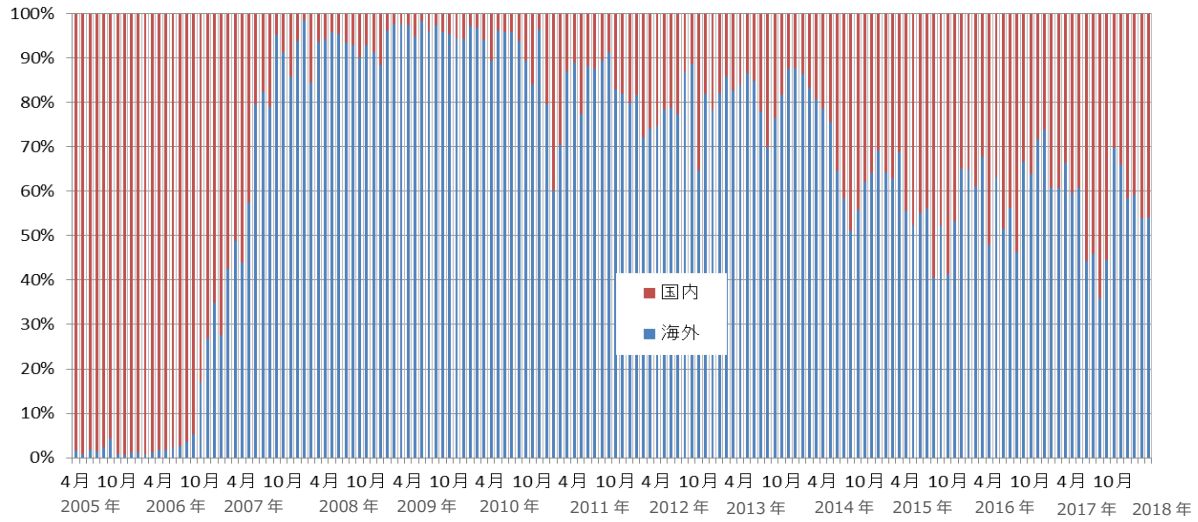
(一財)日本データ通信協会が設置しているモニター機に着信した迷惑メールでは、国内発のものの割合は、PC 宛ての迷惑メールについては 2005 年には 50%を超える時期があったものの、その後は減少し、2006 年以降はそのほとんどが海外発のものとなっています。一方、携帯電話宛ての迷惑メールについては、国内発のものが一時期減少しましたが、2014 年以降は増加傾向にあり、現在では半数程度が国内発のものとなっています。

図表２－３－３　国内発・海外発の比率の推移（PC あて）



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

図表２－３－４　国内発・海外発の比率の推移（携帯あて）



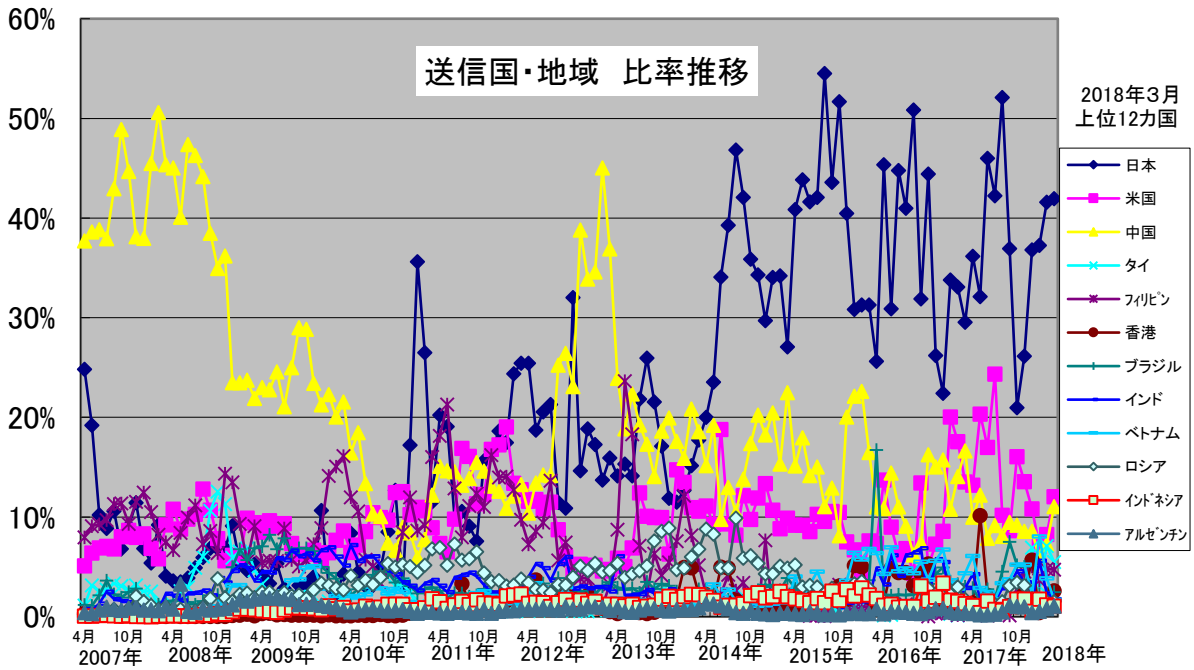
出典：（一財）日本データ通信協会迷惑メール相談センター調べ（センターのモニター機で受信した情報を分析したもの）

3　迷惑メールの送信国・地域

国内着の迷惑メールの送信国・地域としては、日本、米国、中国が上位にある傾向が続いています。

(一財)日本データ通信協会が設置しているモニター機に着信した迷惑メールについての送信国・地域としては、時期的な変動はありますが、一貫して日本、米国、中国が多くなっています。その他の国・地域としては、2013 年度頃までフィリピンからの発信が多く、時期によっては 20%を超えることもありました。また、2017 年度には、タイやベトナムからの迷惑メールが増加しました。

図表２－３－５　日本着の迷惑メールの発信国・地域の推移



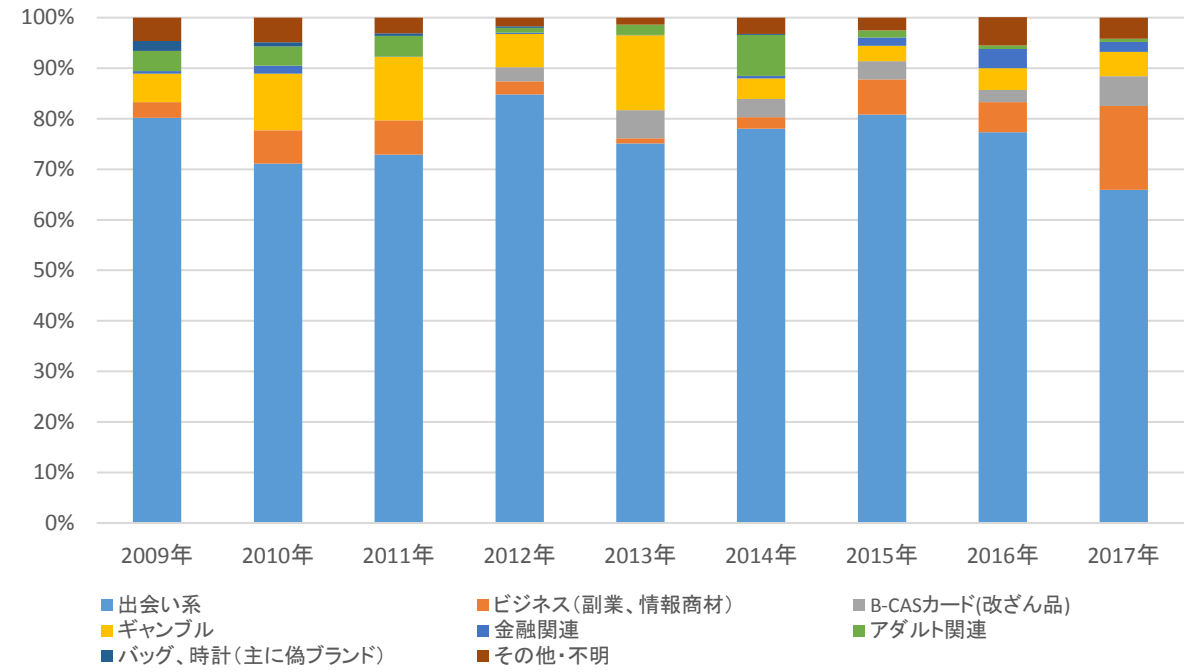
出典：（一財）日本データ通信協会 迷惑メール相談センター調べ（センターのモニター機で受信した情報を分析したもの）

4　迷惑メールの内容

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

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

図表２－３－６　迷惑メールの内容

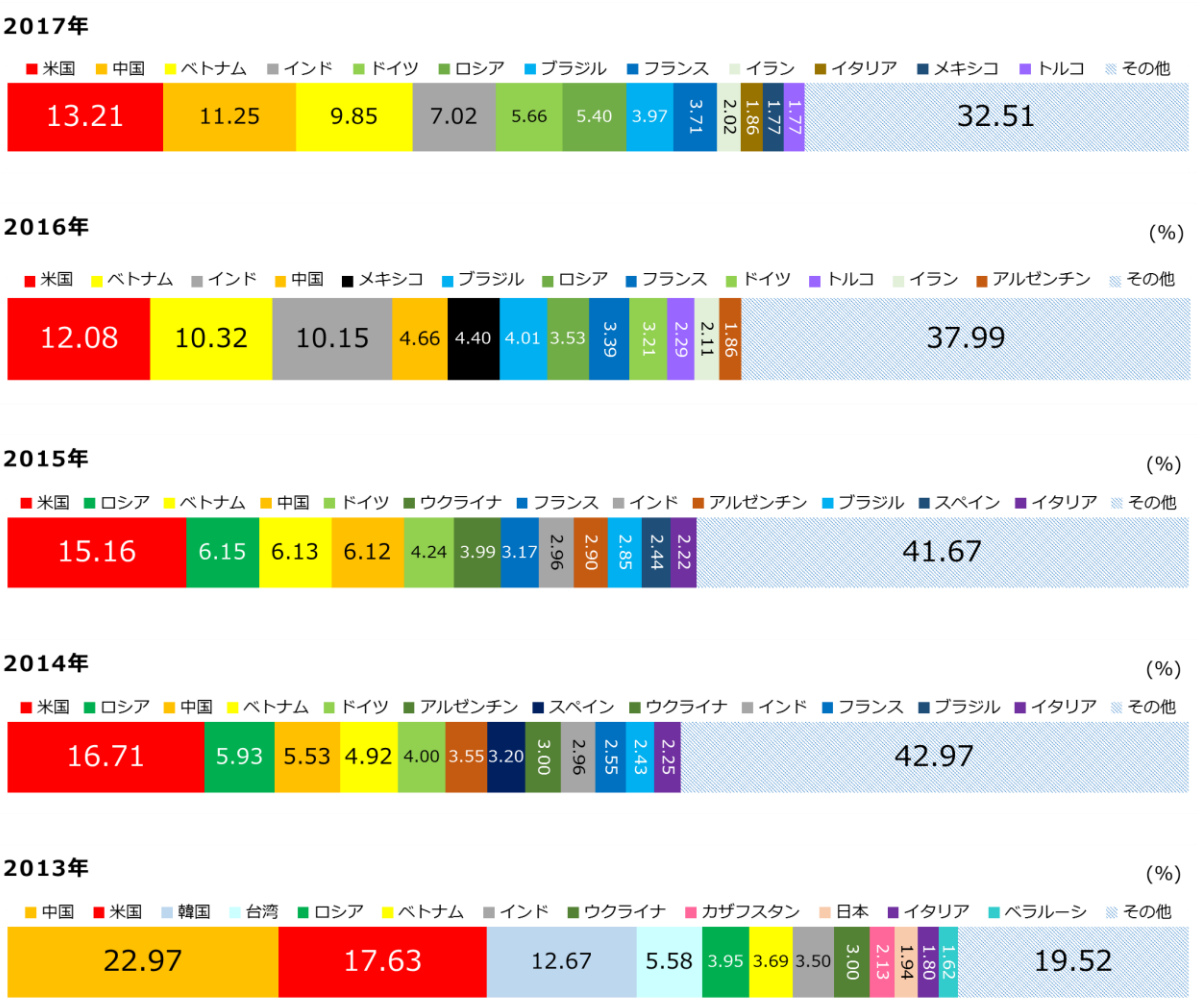


出典：(一財）日本産業協会が設置するモニター機で受信した迷惑メール及び同協会に消費者からの申立として着信した迷惑メールのうち、日本語のサンプルデータを集計・分析したものを元に、迷惑メール対策推進協議会事務局が作成

5　世界全体の迷惑メール送信国・地域の傾向

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

図表２－３－７　迷惑メール送信国・地域の傾向



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

第4節　迷惑メールの送信方法

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

1　送信先の選定

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

（1）大量送信型

大量の送信先を確保する方法として、以下があります。

（ア）　名簿業者からメールアドレスのリストを購入する

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

（ウ）　懸賞サイトなどの「おとりサイト」を作ってアドレスを登録させる

（エ）　インターネットに公開されているブログ掲示板などから収集するなどの方法があります。その他にも、便利なアプリなどを装って不正アプリをインストールさせ、スマートフォン内の電話帳のデータを丸ごと詐取するような方法などもあります。

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

（2）標的型

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

２　送信元の偽装

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

（１）送信元アドレスの偽装

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

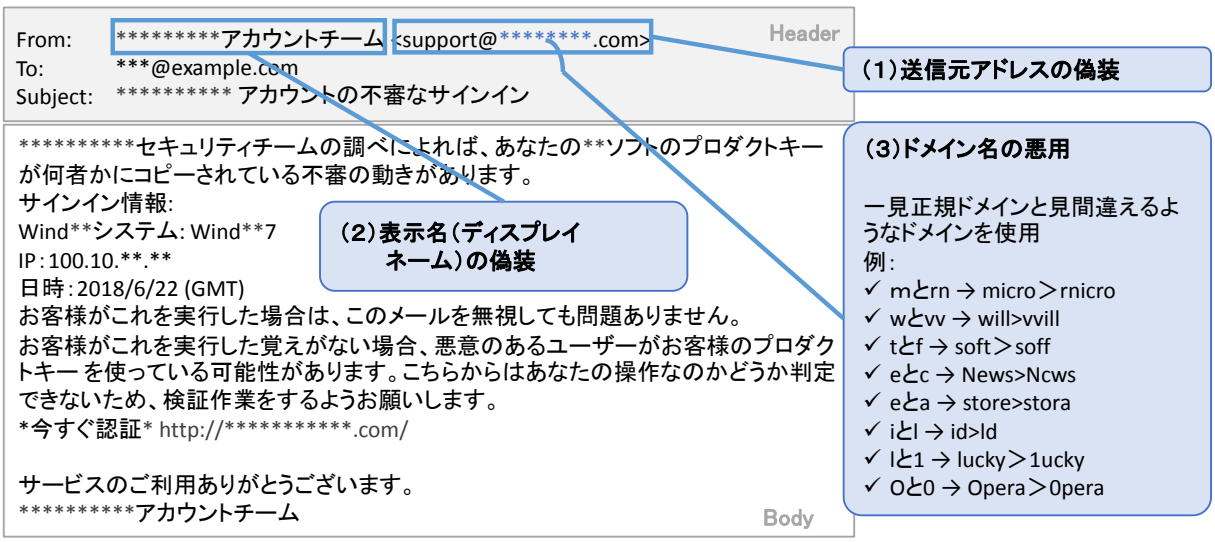
（２）表示名（ディスプレイネーム）の偽装

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

（３）ドメイン名の悪用

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

図表２－４－１　送信元の偽装



3　サーバーの不正利用

迷惑メールは、以前は、外部から匿名で利用可能なオープンリレーサーバー[注40]を利用して送信されることが行われていましたが、不要なメール中継の制限などの不正中継対策が講じられるようになり、そのような方法で迷惑メールを送信することは難しくなっています。一方で、ウイルス（ボット）に感染した大量のパソコンなどを用いたり、契約者情報を偽って取得した固定 IP アドレス[注41]を用いたり、ISP の送信メールサーバーを不正に利用したりする事例が注目されていることから、ここではそれらの３つの方法について説明します。

（１）ボットネットの利用

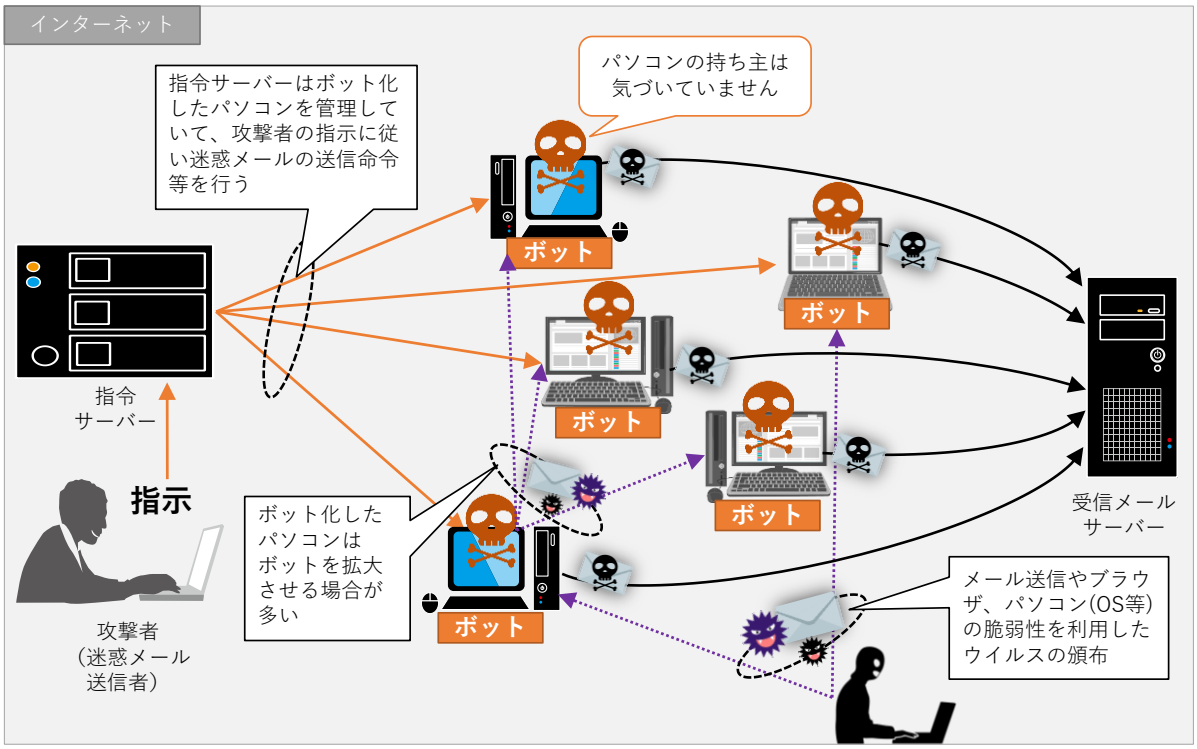
コンピューターウイルスのような悪意のあるソフトウェア（マルウェア）[注42]を大量の一般の利用者のパソコンに感染させ、このマルウェアに感染したパソコンを外部から操作することによって、迷惑メールの送信などに利用する手法で、2002 年頃から使われるようになっています（マルウェアに感染したパソコンはロボットに擬して「ボット」と、ボットの集合は「ボットネット」と呼ばれています）。

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

ボットネットに対しては、ISP の正規のメールサーバーを介さない、電子メールの動的 IP アドレス[注43]からの送信をブロックする OP25B[注44]による対策が行われています。しかし、（３）のようにボットが正規の利用者のパスワードなどを詐取し、その利用者を装って迷惑メールを送信する場合や、まだ OP25B を導入していない海外などの ISP を利用して迷惑メールを送信する場合など、対策には限界があるのが現状です。

注40 外部からのメール送信依頼を受け付け、メールの送信を行うサーバー
注41 常に同じ IP アドレスが割り当てられること
注42 「Malicious Software」（悪意のあるソフトウェア）の略で、様々な脆弱性や情報を利用して攻撃をするソフトウェアの総称
注43 接続のたびに異なる IP アドレスが割り当てられること
注44 第３章トピックス「OP25B(Outbound Port 25 Blocking)」（P67）参照

図表２－４－２　ボットネットのイメージ



（２）固定 IP アドレスの不正利用

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

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

（３）アカウントの不正利用

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

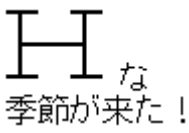
このような送信手法に対しては、利用者において適切な ID やパスワードの管理を行うこと、セキュリティ対策を行うことなどが重要になります。

４　その他（迷惑メールフィルターの回避）

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

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

図表２－４－３　形状的に似た文字を使った例

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

トピックス：SNSの悪用

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

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

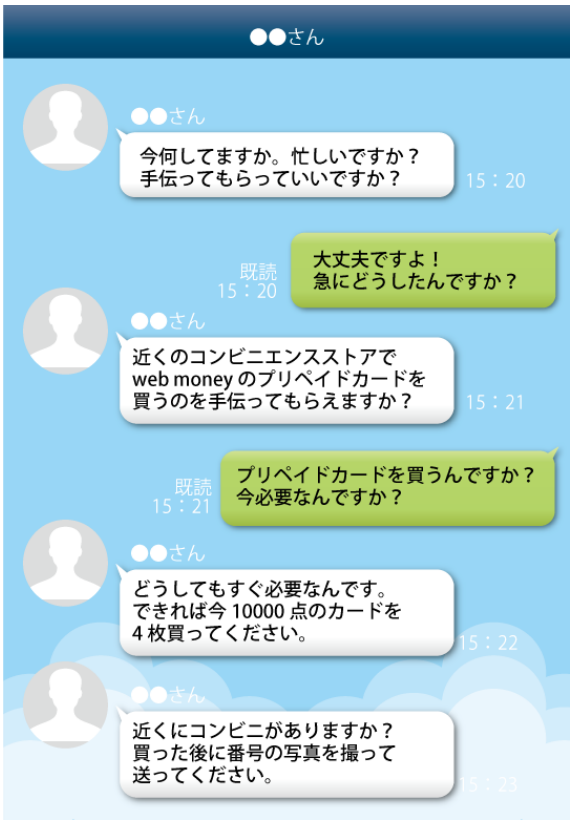
そして、SNSの利用者が増えてくると、知らないアカウントから「悪質サイトへの誘導」などの迷惑メッセージがSNSでも送られるようになりました。電子メール同様、SNSのメッセージを使った詐欺被害やマルウェア感染なども発生しています。

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

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

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

図表２－４－４　アカウント乗っ取り詐欺の手口のイメージ



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

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