個人利用者による迷惑メール対策

倪　　永茂

はじめに

本文でいうメールはEメール（Electronic mail）のことである。IT社会ではメールの使用は衰退の一途を辿りながらもまだ大活躍しているが、近年迷惑メールが大幅に増え、一日の仕事は迷惑メールの駆除からスタートするというほどである。届いたメールのうち、8～9割以上が迷惑メールという日もよくある。

いくら政府や、事業者、関係団体による迷惑メール対策を真面目に取り組んできても、迷惑メールの数が年々増大している現状では、利用者個人が対策を講じるしかない。

筆者の同僚がウイルスメールを不本意に開け、LAN上にウイルスをばら撒いてしまった。その結果、仕事で使うPCがLANから強制的に隔離されるだけでなく、保存データの消去、OSやソフトの再インストール等の作業が強いられ、仕事が数日できなくなった。

迷惑メールが絶滅しない根本的な原因は無論メールの仕組みそのものに重大な欠陥があるからである。そのためか、多くの国ではメールを使わずにSNSのみで情報交換や情報共有するようになった。また、多くの企業では社内の通信手段としてすでにメールから別のものに切り替えた。

ところで、デジタル署名付き暗号メール（S/MIME）という仕組みがだいぶ昔に提案され、実用できる状態になっている。それを普及すれば、迷惑メールへの有効な対策になるが、なかなか利用者が広まらない。

個人利用者は迷惑メールの被害から免れ、時間的ロスやストレスから解放され、ITライフをより楽しいものにするにはどうすればいいか。それを考えるのは本文の目的である。

Ⅰ 迷惑メールの実態

ここでは、メールの仕組みや、迷惑メールの定義や種類、迷惑メールの偽装工作について解説する。迷惑メールへの対策を考える際には、これらの基礎知識を把握しておく必要がある。

1 メールの仕組み

メールとはSMTP（Simple Mail Transfer Protocol）というプロトコルによって規定されるインターネット上のデータ交換の方法であり、インターネットの初期から実装されたサービスのひとつである。メールに関する基本的考え方は、従来の封書やその配達に基づいているので、SMTPを解説する代わりに、従来の封書でわかりやすく説明する。

封書の配送は郵便局同士が都合のよい時間に、連携（中継）によって達成される。封書の封筒には受取人の住所氏名を記入するだけでなく、差出人の住所氏名も書かないといけないが、その差出人の住所氏名について郵便局がいちいち身元確認はしていない。その重大な欠陥がメールにも引き継がれている。なお、住所氏名のことをメールではメールアドレス（以下略してメルアド）という。また、都合のよい時間で中継するので、メールを送出した瞬間に宛先に届くことが多いが、一日経ってやっと届くこともありうる。SNSのようなリアルタイム通信手段とプロトコル上、異なる。

封書では、封筒以外に便箋にも受取人と差出人の氏名を書くことが一般的である。メールとの対応を表1に示す。使用しているメールソフトによって表示されている受取人と差出人はあくまでも便箋に書かれたもので、郵便配達で使われているものと異なることによく注意しよう。なお、メールソフトによって表示されたメールのヘッダー情報も多くは便箋の内容であって、配達に必要な封筒の情報はメール配達完了時に、一部だけヘッ

ダー情報に書き込まれるが、多くは削除されてしまうことにも留意しよう。

表１　封書とメールとの対応関係

封書	メール
封筒に書かれた受取人	Envelope-To（メール配達完了時に削除され、メールソフトでは表示されない）
封筒に書かれた差出人	Envelope-From（メールソフトで表示される Return-Path）
便箋に書かれた受取人	Header-To (メールソフトで表示される To)
便箋に書かれた差出人	Header-From (メールソフトで表示される From)

なお、Envolope-To に関する情報は Received に転記されることもある。

では、ヘッダー情報についてより詳しく確認しよう。ヘッダー情報がとても長く、短縮表示になっているメールソフトがほとんどであるが、迷惑メールの判別には短縮表示は不利になる。図 1 ではあるメールのヘッダー情報を例示した。


Return-Path: <ek@amazon.co.jp>
X-Original-To: web@cc.uts.ab.jp
Delivered-To: web@cc.uts.ab.jp
Received: from miy.uts.ab.jp (miy.uts.ab.jp [166.22.221.22])
by nan.cc.uts.ab.jp (Postfix) with ESMTP id 936DA180F4B
for <web@cc.uts.ab.jp>; Sun, 30 Oct 2022 13:48:35 +0900 (JST)
Received: from amazon.co.jp ([152.32.228.152]) by miy.uts.ab.jp with ESMTP id cuueaHjrzW5mkInJ for <web@cc.uts.ab.jp>; Sun, 30 Oct 2022 13:48:34 +0900 (JST)
Message-ID: <20221030074834406076@amazon.co.jp>
From: "Amazon.co.jp" <ek@amazon.co.jp>
To: <web@cc.uts.ab.jp>
Subject: Amazon 株式会社から緊急のご連絡
Date: Sun, 30 Oct 2022 07:48:28 +0300
X-mailer: Khlwbuk 0

図１　ある迷惑メールのヘッダー情報

各行の意味をそれぞれつぎに書き出す。

Return-Path: メール差出人のメルアド。Envolope-To の内容のコピーであることがほとんど。

X-Original-To: 本来のメール受取人（Header-To）のメルアド

Delivered-To: 最終的に配達された受取人（Header-To）のメルアド。メールを受け取ったメールサーバによって転送された場合に、X-Original-To と Delivered-To が異なる。

Received: メールサーバを受信側から送信側まで遡った時のリスト、ルートともいう。それぞれの受信時刻や、ドメイン名、IP アドレスが記載される。Envolope-To の情報が書き込まれることが重要。なお、最後の送信メールサーバについて、そのドメイン名が偽装されることが迷惑メールでは多い。たとえば、図 1 のところの IP アドレス 152.32.228.152 は amazon.co.jp ではなく、偽装されたものである。

Message-ID: メールにつけられた識別 ID

From: 差出人（Header-From）のメルアド。迷惑メールでは偽造されることがほとんどである。

To: 受取人（Header-To）のメルアド

Subject: メールの件名

Date: メールの作成日時

X-mailer: 差出人が使用したメールソフト

差出人（Return-Path）の情報や、メールの配達に関わったメールサーバに関する情報（Received）はとくに重要で、迷惑メール対策を考えるうえではその見方を習得することが必要であろう。

2 迷惑メールの定義とその種類

迷惑メールに関する明確な定義はないが、本文では最も広義的な定義、すなわち、「受信者の受け取る意思に反するメール」を迷惑メールとする。

つまり、受信者の同意や了解を得ずに送られたメールや、受け取る拒否をしたにも関わらず送信しつづけるメールを迷惑メールという。また、利用者本人がメールの配達を取りやめたにも関わらず、メールを送りつづけることも迷惑メールにあたると考える。

迷惑メールの種類を大きく分けると、商品やサービス、サイトの宣伝などの「広告宣伝メール（スパムメール）」、お金や個人情報をだまし取ろうとする詐欺目的の「フィッシングメール（詐欺メール）」、ウイルス感染を目的とする「ウイルスメール」、特定の組織や個人の秘密情報や個人情報の取得を狙った「標的型メール」、他人に転送させようとする「デマ・チェーンメール」等がある。

近年、ウイルスメールやデマ・チェーンメールが大幅に減少したが、フィッシングメールが逆に大幅に増え、金銭目的の迷惑メールが氾濫してい

る。図2はフィッシング対策協議会が報告した日本国内のフィッシング情報の届け出件数に関する年半期変化を示したもので、右肩上がりに増加している様子はよくわかる。

図2　国内のフィッシング情報届け出件数
出典 フィシング対策協議会「フィッシングレポート2021」

迷惑メールはなぜ社会問題になったかというと、受信者にとって、迷惑メールによって時間的ロスやストレスをもたらし、場合によっては金銭的、名誉的損失を被ることになるからである。

迷惑メールが多く来ると、その判定、削除に時間がかかり、仕事の効率が下がる。同僚等になりすました悪質なメール（いわゆる標的型メール）に遭遇すると、どのメールに対しても疑心暗鬼になり、仕事どころではなくなる。また、誤ってウイルスメールを開けてしまったら、組織にウィルスをばらまくことになってしまい、その自責の念や後処理に大変なストレスがたまる。周りの理解が足りないと、職場での評判を落とすことになる。詐欺メールを信じてしまったら、金銭的損失につながる。

3 迷惑メールの偽装

迷惑メールは悪質であればあるほど、取締の追跡をかわすため、様々な方法で偽装して送信している。

大規模のメールアドレスを取得するために、名簿業者から購入する、ランダムにメールアドレスを作成する、プログラムを使ってインターネット上に公開しているメールアドレスを自動収集する等のことを行っている。

表1のように、メールソフトで表示される差出人や受取人はメールの配送に使われているものと異なっていてもメールが届くので、差出人（From）の偽装はよく行われる。

また、メールの本当の差出人がバレないために、踏み台（関係のないPCやサーバ等）を悪用したり、ボットネットを使用したり、契約者情報を偽ってプロバイダと契約したりする偽装工作を行っている。

メールの本文に書かれているリンク（URL）についても偽装工作が行われていることが多い。表示されるURLが実際のものと異なること、誤認されやすい文字（oと0、lと1、mとrn、wとvv、tとf、eとc、半角と全角等）が使用されること等である。

偽装が何重も行われているために取締が難しく、外国にあるサイトからのメール発信になれば、日本の法律を適用することにも限界があるので、野放し状態になっている。

このように、国や企業（組織）が迷惑メール対策を必死で行っていると思われるが、図2のとおり、有効な成果がまだ現れておらず、われわれ利用者個人が自らの力で迷惑メール対策を講じないといけないのが現状である。

Ⅱ 迷惑メール対策

ここでは、われわれ利用者個人が取れる迷惑メール対策について詳しく説明する。迷惑メールに対処するには、最後の砦は自力で自分を守ることである。

1 迷惑メールを受け取らないための対策

迷惑メールを受け取らないこととは、自分の使用しているメールサーバが迷惑メールを受信しない意味である。

迷惑メールに遭わない最強の対策法はメールをそもそも使わないことであるが、仕事している人にとってはメールを使わない選択肢はない。

従って、現実的対策としては仕事用と私用のメールをきちんと分けること、私用のメールはその内容をSNSで済ませるか、そのアドレスは定期的に変えること、仕事用のメールアドレスは安易に公開せず、他人にむやみに教えないことである。

Gmail等の無料メールサービスは迷惑メールにしっかり対処しているし、定期的に（たとえば1年ごと）にアカウントを作り直しても余計なコス

トはかからない。問題はメール内容や交友関係（メール友）がGoogleに知られてしまうリスクをどう評価するかである。

仕事用のメールはそのアドレスを変えることが大変困難なので、名刺交換の範囲等、ふだん気を付けて行動することに心がけよう。

プロバイダーによってはメールの拒否設定ができるところもある。その場合、指定したドメイン（たとえば日本）からのメールしか受信しない、指定したドメインのメール受信を拒否する、見せかけの送信元メールアドレスと実際の送信元が異なるメールを拒否する、URL付メールを拒否することができる。

2 受け取った迷惑メールへの対処法

メールを使う以上、早かれ遅かれ迷惑メールが届く。迷惑メールへの対処法はIT社会のリテラシーだと言われるが、そう簡単なものではない。

2.1 迷惑メールかどうかの判別

送られてきたメールが迷惑メールかどうか、その判別は一目でわかるようにスキルアップしないといけない。英語でメールのやりとりがないのに、英語で書かれた件名を迷惑メールだと判定すればよい。心当たりのないメールも迷惑メールと思ってよい。

件名をクリックし、メールを開けて内容確認する段階でも、迷惑メールかも、とつねに疑う心構えが必要である。URLが本文に書かれてもクリックしない。添付ファイルの保存を慎重に行い、ウイルススキャンを行ってから、やっと対応ソフトを起動させて、ソフトの「ファイルを開く」という機能を使って添付ファイルを開けることにしよう。

添付ファイルをダブルクリックして実行すると、拡張子の偽装によって別のプログラムが起動され、あるいは、添付ファイル自身が実行することになるので、とても危険だと認識すべきである。拡張子の偽装という手法がウイルスメールにとくに多く、細心の注意を払うしかない。

無論、どんなに親しい間柄や重要な仕事に関わるメールの内容であっても、添付された実行ファイル（ファイルの拡張子で実行ファイルであるかどうか確認できることが多い）は絶対に保存してはいけないし、実行させることはもってのほかである。

迷惑メールかどうかの判別は一瞬にしてできないといけないし、集中力が必要なので、なかなか大変である。

なお、迷惑メールではないと判断したメールに対しても、メール本文内のURLをクリックしないこと（アクセスするときにはそのURLをブラウザにコピーして使う）、また、URLの先にIDやパスワードの入力が求められたら、詐欺メールだと強く警戒すべきである。いったん操作を止めて、落ち着いて考えてみよう。少しでもおかしいと思ったら、SNSや電話で相手に確認するなり、一日放置しておくことがいいかもしれない。

とにかく、焦って冷静さを失うことが禁物である。

2.2 広告宣伝メールへの対策

ほとんどの人は広告宣言メール（スパムメール）に興味がないのに、毎日大量に送られてくる。国内サイトからの配信であれば、政府の対策によって、配信しないように設定を変えられることが多い。たとえば、楽天（www.rakuten.co.jp）では、会員ページにログインし、「楽天からのメールマガジンの確認・停止」という項目を開き、たくさんの配信メール（図3）を止めることができる。

ただし、海外サイト等、日本の法律が適用しないところからのスパムメールについては止めることができないところもある。信用のおけないサイトの利用や登録はしないように心掛けよう。

図3 楽天の配信メールを止める

2.3 メールフィルタリングの活用

メールフィルタリングとは、事前に設定した条件に基づいて受信したメールの一部や、学習機能に基づき、迷惑メールとして指定されたメールを削除したり、あるいは隔離したりする仕組みのことである。

設定方法はメールソフトごとに異なるが、ここでは Mozilla Thunderbird 最新バージョン 102.4.1 を例として取り上げ、主につぎの 3 つの手順でフィルターリング設定を行う。

・迷惑メールの学習フィルタを有効（図 4）
・迷惑メールの移動先フォルダの設定（図 5）
・共通の迷惑メール設定（図 6）

図 4　Thunderbird では学習フィルタを有効

図 4 は学習フィルタを有効にしたところである。同時に、個人用アドレス帳や記録用アドレス帳に書かれたメルアドの相手からのメールにも迷惑メールにしない設定をしたが、偽装メールに弱い。

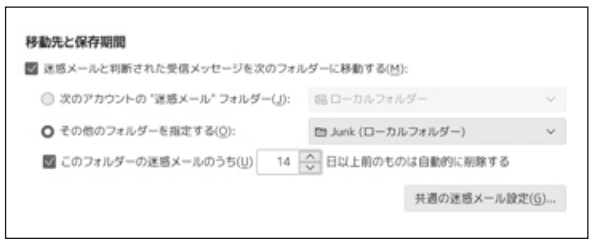

図 5　迷惑メールの移動先フォルダ

図 5 は図 4 と同じ設定画面の下部に、迷惑メールの移動先（隔離先）と保管期間を設定したところである。さらに、図 5 の右下に表示される、共通の迷惑メール設定については図 6 のように行う。

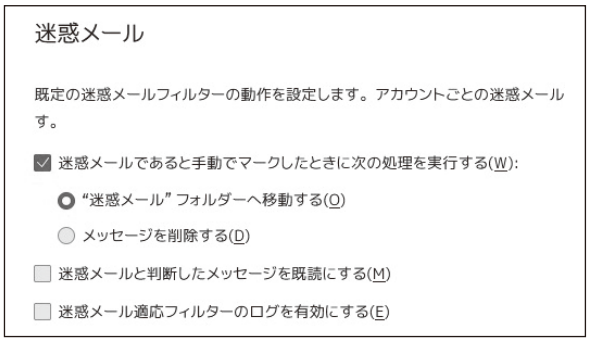

図 6　共通の迷惑メール設定

設定が終わったら、個々の受信したメールに対して、迷惑メールかどうかを判断し、迷惑メールと認定した場合には、マウスの右クリックで「マーク」→「迷惑メールとしてマーク」を選べば、迷惑メールとして隔離される。そして、学習機能により、発信元（差出人）が同一のメールはその後、すべて迷惑メールとして処理される。

学習がある程度進むと、多くの迷惑メールが隔離され、目にした迷惑が大幅に減少することを実感できる。

それでも、いままで受信したことのなかった差出人からの迷惑メールは入ってくるし、迷惑メールが進化するので、油断してはいけない。

3 損害を被った場合の対策

銀行口座の番号や暗証番号を入力してしまったり、クレジットカード番号等を知らせてしまったりした場合は、まず銀行やクレジットカード会社のコールセンターに連絡すること、つぎに、居住地区の都道府県警察サイバー犯罪相談窓口に連絡すること、心身的余裕があれば、国民生活センター、または消費生活センターに連絡したり、フィッシング対策協議会へ情報提供することを行おう。

アカウントの ID やパスワードを知らせてしまった場合は、それらのパスワードを即座に変更する。アカウントを作成しなおせるサイトでは ID をさらに変更することでより安心する。

容易に推測された他のアカウントのパスワードについても、すべてを変えることが望ましい。

何よりも大事なことは失敗から学び、2 度とひっかからないようにすることである。

4 デジタル署名暗号付きメール（S/MIME）の利用

S/MIME（Secure / Multipurpose Internet Mail Extensions）とは、「メール本文の暗号化」「メール差出人（Header-From）の認証」「メール本文の改ざん検知」という 3 つの機能を兼ね備えた、メールのセキュリティを向上する暗号化方式のひとつである。

S/MIME を使うには、送信者と受信者側との両方が S/MIME に対応するメールソフトを使用する必要があるが、代表的なメールソフト Mozilla Thunderbird や Microsoft Outlook 等がすでに対応済である。

S/MIME を使えば、差出人の偽装ができなくなるだけでなく、メールの内容が盗聴されたり、内容が書き換えられたりすることがなくなる。その結果、標的型メールの根絶や、他の迷惑メールの撲滅に大きな前進となる。これまで、政府も S/MIME の普及・促進を図ろうとしたが、「コストがかかること、手間がかかること、プライバシー保護の視点から、秘匿暗号と認証・署名暗号の両立が難しい」（辻井、2021）等の課題により、なかなか普及しない。

もうひとつ普及しない原因を付け加えるとすれば、IT 大手によるメール内容の把握や、反テロという名の国家による監視にも S/MIME は都合が悪いからであろう。

仕事用のメルアドでは組織の指示や許可がない限り、S/MIME を使うことは難しいが、私用のメルアドであれば、メール友と共に無料の証明書を入手して、S/MIME を利用することができる。公的な証明書ではないにしても、個人同士であれば、迷惑メール対策としてとても有効であろう。S/MIME 以外のメールについては、基本的にすべて迷惑メールとして取り扱うことにすればよいので、メールの処理にかける時間と労力が激減するはずである。

導入のしかたに関しては基本的に図 7 に示した手順を踏む。まずは民間認証局に申請し、無料で証明書を発行してもらう。つぎに、相手であるメール友に取得した証明書をメールを通して送り届ける。その際に、SNS や電話等で相手に直接、確かに自分が証明書を送ったことを明確に伝えることにしよう。

図 7　個人利用者の S/MIME 導入手順

出典　NTT エレクトロニクス株式会社サイト

あとは従来のメールとほぼ同様なやり方で互いにメールのやりとりをすればよい。第三者によるメール差出人の偽造や、メール内容の書き換えはアラームとして表示されるので、一目で気づく。

終わりに

本文は利用者個人の立場から、迷惑メールに関する基礎知識や、複数の迷惑メール対策を考えた。

詐欺電話と違い、メールは電子データなので、個人の対応には限界がある。それでも、受け取ったメールをつねに疑う心構えを持ち、緊急な要件や大事な要件については落ち着いて冷静に考え、相手がいる場合には SNS や電話で確認してから行動しよう。メールは一日経って届くこともあるので、一日置いてから行動しても遅くないはずである。

S/MIME を積極的に普及させることがひとつの改善策になるが、いままでの SMTP を利用する限り、迷惑メールにまつわる攻防戦はこれからも続く。迷惑メールはますます巧妙化・複雑化になっていくからである。

参考文献

大角祐介（2021）『正しく怖がるフィッシング詐欺』オーム社

田中潔（2007）「迷惑メールの現状と対策」岡山商大論叢 43 (2) 1-24。

辻井重男（2021）『フェイクとの闘い 暗号学者が見た大戦からコロナ禍まで』コトニ社。

那須靖弘（2007）「迷惑メールの現状と対策」甲子園大学紀要 35、105-109。

迷惑メール対策推進協議会（2018）『迷惑メール白書 2018』迷惑メール対策推進協議会
迷惑メール対策推進協議会（2021）『迷惑メール白書 2021』迷惑メール対策推進協議会
フィッシング対策協議会（2021）「フィッシングレポート 2021」（https://www.antiphishing.jp/report/phishing_report_2021.pdf、2022.10.20 アクセス）

Anti-spam Measures by Individual Users

NI Yongmao

Abstract

No matter how many serious efforts have been made by the government, companies, and related organizations to combat spam emails, the number of them is increasing year by year, and individual users have no choice but to take measures to combat this problem.

In this article, we explain how email works, how to recognize header information, and sum up the definition and types of spam. Furthermore, their disguise is also mentioned.

And we explain in detail how we, as individual users, can counteract spam. These include measures to avoid receiving them, how to deal with them received, how to determine whether or not it is spam, measures against advertising and promotional email, use of email filtering, and S/MIME.

（2022 年 11 月 1 日受理）