第 1 章

電子メール

これだけは押さえておきたい メールのセキュリティ

1

メールを送るときのコツ

送信したのにメールが届かない?
メールはテキスト形式が常識!
HTML形式メールでは嫌われる?

電子メールを送信するとき、自分がどんな形式を使っているのかご存知だろうか？　たいていはHTML形式かテキスト形式のいずれかを利用しているはず。

HTML（HyperText Markup Language）というのは、ホームページを作成するときに使用されるページ記述言語のこと。だから、メールを作成する際にHTML形式を利用すれば、ホームページと同様のビジュアル表現を行うことができる。具体的には、使用する文字のサイズやフォントの種類、飾り、配置などを細かく指定したり、図形や写真、アニメーション等を文章中に貼り込むことなどが可能になる。

これに対し、テキスト形式では文字情報しか送信できない。文字のサイズやフォントの種類も選ぶことはできないが、データ容量が小さくて、すべての電子メールソフトで利用できるという利点がある。携帯電話やPDA（携帯情報端末）にメールを送るときも、テキスト形式であれば通常なら受信可能だ。

●HTMLメールでのトラブル

HTML形式でメールを送ると、こんなトラブルも……。

子育ても一段落したことから、仕事を再開しようと、思い切って自分専用のパソコンを購入することにした元翻訳者。自分

専用は初めてだが、それまで夫のパソコンを借りて友人とメールをやり取りしたり、オンラインショッピングを楽しんでいたので特に操作に悩むことはなかった。早速、仕事仲間にメールを送ってみたが、いくら待っても返信が来ない。そこで、電話で問い合わせたところ、メールは届いていないという。何度、送り直しても結果は同じ。そこで、夫のPDAと娘の携帯電話にもメールを送ってみたが、メールは着信したものの、文面が読めないという。

これはメールがHTML形式だったことがトラブルの原因だった。HTML形式のメールは容量が大きいので、ウイルスメールを警戒した受信メールの容量制限にひっかかってしまったから。HTML形式はウイルス感染の恐れもあって嫌われているから通常のメールには使用しないほうが賢明。

●HTML形式は便利だが……

以前は、多くの電子メールソフトがHTML形式をサポートしておらず、通信環境も貧弱で、容量の大きなデータを送るのに時間がかかったので、メールといえばテキスト形式が当たり前だった。しかし、最近では、代表的な電子メールソフトがデフォルト（既定）でHTML形式を採用。ネットワークのブロードバンド化も進展し、テキスト形式に比べてデータ容量の大きいHTML形式のメールでもストレスなく利用できるようになったため、利用者が次第に増えてきている。機能面でも、デジカメが急速に普及している現在、文中に簡単に画像を貼り込め、様々なデザイン処理を施すことができるHTML形式は、時代のニーズにマッチした電子メールのスタイルといえるだろう。

しかし、HTML形式のメールは、いいことばかりというわけではない。ホームページと同様の表現が可能になるということは、不正なスクリプト（イベント駆動型プログラム）を埋め込むことも可能なのである。ここでいう不正なスクリプトとは、ホームページにアクセスしたユーザーに被害を与える目的で作成されたプログラムのこと。これが埋め込まれたホームページを表示させると、パソコンのシステムを勝手に改変して起動できなくなったり、コンピュータウイルスに感染させられてしまう恐れがある。

●メールを読んだだけでウイルスに感染

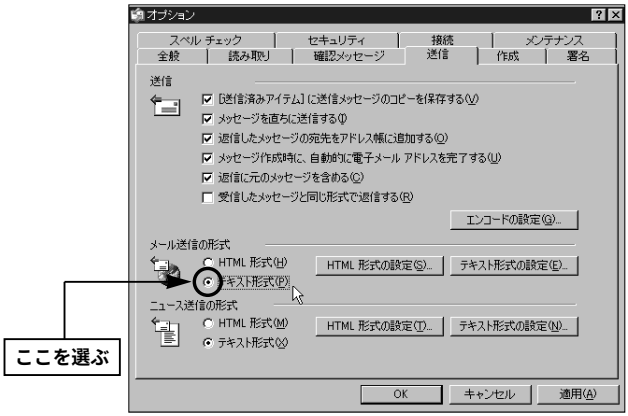
添付ファイルを開かなくても、メール本文をプレビューしただけでスクリプトが自動実行されるという仕組みを利用したウイルスも多いため、HTML形式で送られてきたメールを警戒する人は少なくない。セキュリティ意識の高い人だと、HTML形式のメールはプレビューしない設定にしていることもある。

また、ウイルスメールを警戒して、メール受信設定で、データ容量を制限している人もいる。容量が大きくなりがちなHTML形式のメールは、これにひっかかって受信されない場合もある。そのため、文字だけで十分なビジネス用途のメールなどは、テキスト形式を使用したほうが無難。テキスト形式でも、画像などを添付することができるし、文字や記号を組み合わせた顔文字で感情表現をすることもできるので、特に困ることはないはずだ。

【鉄則】 **メール送信の基本は、テキスト形式である**

注【メールをテキスト形式に設定するには】

メールをテキスト形式にするには、メール作成の設定を変更するか、メール作成時にテキスト形式を選択する。例えばOutlook Express6の場合、常にテキスト形式のメールを利用するのであれば、プルダウンメニューの「ツール」から「オプション」の「送信」を開き、メール送信の形式で「テキスト形式」を選択。相手によってHTML形式とテキスト形式を使い分けたければ、新規メッセージ作成時に、プルダウンメニューの「書式」から「テキスト形式」を選択する。設定方法は電子メールソフトによって異なるので、詳しくは使用説明書を参照のこと。



2

他人が勝手にメールを送らないようにするには

メールで勝手に就職内定を辞退されてしまった。
送信していないのに……。
ネットでは顔が見えないから、なりすまされる。

厳しい就職環境を勝ち抜いて念願の内定を取り付けた女子大生。ところが内定通知後、会社からはなんの連絡もなく、正式な採用通知も届かないという事態に。不審に思った彼女が会社の人事部に問い合わせてみると、「あなたから内定辞退のメールをいただいたので、すでに採用は取り消してある」というではないか。

●なんと友達が犯人!

もちろん、彼女は内定辞退のメールなど出した覚えはない。人事担当者にそのことを説明し、なんとか採用してもらいたいと懇願する彼女だったが、「すでに、代わりの人に採用通知を送ってしまっているので無理だ」と断られてしまった。

どうしても納得がいかず、警察に相談したところ、驚くべき事実が判明した。サークル仲間の男子学生が、彼女のＩＤとパスワードを使って大学のコンピュータに不正アクセスし、彼女になりすまして内定辞退のメールを送信していたのだ。

彼は不正アクセス禁止法違反で逮捕されたが……。

ここで紹介したストーリーは、2001年12月に現実に発生した事件をもとに創作したもので、大筋は事実に沿っている。この事件から得られる教訓は、親しい友人といえども、ＩＤやパス

ワードを知られてはならないということだ。

●覚えやすいパスワードは危険

多くの人はＩＤやパスワードを決めるとき、自分や家族の誕生日、電話番号、住所、趣味などをヒントにすることが多い。友人や知人の場合、これらの情報を得ることはたやすいので、ＩＤやパスワードを推測することができてしまうというわけだ。そのため、周囲の人に知られる可能性のある文字列をＩＤやパスワードに使うことは、避けたほうがいい。

だが、ＩＤやパスワードを、推測が困難な自分と関連のない複雑な文字列にしてしまうと、覚えにくい。かといってメモしておくと、誰かに盗み見られる恐れがあるのでかえって危険だ。

1997年に政府が制定した「情報システム安全対策指針」にも、パスワードを設定する際に注意すべきポイントとして、短いものや単純なもの、辞書に載っている単語、家族の名前、生年月日、本人に関する情報、過去に使ったものなど、推測が容易な文字列を使わないことが推奨されている。定期的にパスワードを変更することや、機密性を高め、メモを残さないことなども重要だ。

●パスワードのコツ

他人から推測が困難なパスワードを作成する方法としては、基本となる文字列を、自分だけしかわからないルールを使って変換するのが効果的とされる。パスワードを定期的に変更する際にも、どのように変化させていくかをルール化しておくと、継続的な運用が容易になる。

また、文字列以外のパスワードが利用可能であれば、指紋認

証やサイン認証、認証機能を有したUSBキーなどを使用することも考えられる。

【鉄則】 **パスワードに誕生日、住所、電話番号は使わない。当然、メモにも残さない**

注【ＩＤとパスワード】

ＩＤとは「Identification」の略で、利用者を識別するための記号・文字列等のことを指す。個人を特定する必要があるときにはＩＤを利用するのだ。しかし、ＩＤだけでは他人になりすまされてしまう恐れがある。そこで利用されるのがパスワード。パスワードはＩＤと対にして登録しておく記号や文字列で、ＩＤとパスワードが正しければ本人であることを認証することになる。

ネットショッピングなどでＩＤとパスワードを入力すると、以下のような画面になるはず。

ＩＤ　ＡＢＣ１２３

パスワード　＊＊＊＊＊＊

ＩＤは打ち込んだときに表示されるが、パスワードは＊＊＊＊＊＊と伏せた表示となる。

3

企業のなりすましメールには注意

クレジット会社からの請求書が……。
親切な警告情報メールに、
うっかり個人情報を送信してしまった。

ある日ショッピングサイトから「当店は５月10日に、あなた様のクレジットカード情報を使ったご注文を受け付けました。しかし、当店の不正対策部門では、この注文に疑念を持っています。たいへんお手数ではありますが、同部門が開設したページにアクセスし、正しい情報を入力した上で、今回の注文の確認、もしくは取り消しの手続きを行ってください」という電子メールが届いた。そこで、慌てて指定されたページにアクセスし、住所・氏名・電話番号やクレジットカード番号、有効期限などを入力し、注文の取り消しを行った。これで一安心のはずだったのだが、数カ月後にクレジットカード会社から限度額いっぱい使われている請求書が届いてしまった。

●大手企業を名乗ったなりすまし

これは、電子商取引関連サイトになりすました詐欺メールによる被害の一例。米国ではすでに、大きな問題になっている。

2003年６月には、家電販売チェーン大手「Best Buy」の不正対策部門を名乗る者が、世界中の利用者に向けてクレジットカード番号の盗難を警告する内容のメールを発信。同部門が開設したように見せかけた偽ページへのアクセスを促し、社会保障番号などの重要な個人情報を入力フォームを用いて不正に収集していたという。

著名なオンラインオークション事業者である「eBay」の子会社で、決済サービスを手がける「PayPal」でも、顧客の口座番号やパスワードを不正収集しようとする詐欺メールが近年横行している。

その一例を挙げると、「他人になりすました不正取引が増加しています。そのため、当社では不審なアカウントについて、当社が保有する顧客情報と完全に一致することを確認させていただいています。これが証明されませんと、当社のサービスをご利用いただけなくなります。お手数ですが、このページにアクセスして、お客様情報確認のための手続きをお願いいたします」というようなものだ。この偽ページでは、「クレジットカード番号」「銀行口座番号」「ATM暗証番号」などの入力が求められるという。

●日本でも起きているなりすまし詐欺

詐欺メールの手口は一段と巧妙化してきており、だまされやすいので注意が必要だ。

日本とて例外ではない。2003年４月には、日本企業が運営するドメイン登録サービスの利用者に対し、ドメインの契約更新に関わる料金の支払いを催促する詐欺メール（英文）が送られていることが判明。これも、顧客のクレジットカード情報の取得を目的とした詐欺メールだった。

【鉄則】 **たとえ警告メールでも個人情報はうかつに送らない**