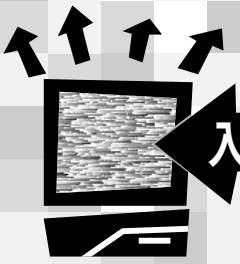


入門者のための FAQ

Frequently Asked Question

このコーナーでは、みなさんから寄せられたインターネットに関する質問や疑問についてお答えしていきます。日頃からわからないなあと思っている疑問、困っていることなどありましたらどんなことでもけっこうですから質問を編集部までお寄せください。宛先はip-faq@impress.co.jpです。電子メールでの回答はできませんのでご了承ください。

「Good Times」というタイトル（Subject）のメールを受け取ったらそれはウィルスだから気をつけてくださいという内容のメールが、メーリングリストで回ってきました。読むとハードディスクが破壊されるそうです。実際に被害にあった人はいるのでしょうか。もし、そういうメールがきたらどうすればいいでしょうか。

（匿名希望）

A. 昨年の冬から、僕が知っているだけでもすでに3回ほど、このウィルスの件であちこちのメーリングリストがパニックになっていましたが、この情報は単なるデマです。ですから、全くあわてることはありません。安心してください。くわしくは、CIAC（Computer Incident Advisory Capability:米国エネルギー省によるコンピュータセキュリティに関する情報の収集・公開を行っている組織）のサーバー（http://ciac.llnl.gov/）を参照するといいでしょう（http://ciac.llnl.gov/ciac/notes/Notes09.shtml）。同様の話に「エボラウィルス」騒動というのもあります（http://ciac.llnl.gov/ciac/notes/Notes10.shtml）。

ところで、今回の騒動がデマだったからといって安心できるのでしょうか？ 嘘つき少年ではありませんが、デマだと思っているうちに、本物のウィルスがやってくるかもしれません。そこで、技術的にこんなことが可能なのかを、ちょっと考えてみたいと思います。

まず、ファイルを消したりシステムを高負荷にして利用できなくしたりするためには、相手のコンピュータ上でファイル操作（ファイルの生成や変更、削除）やプログラムの実行ができることが前提となります。さらに、システムを破壊するためには特権ユーザー（rootや管理者）の権限も必要となってきます。

こうしたことを相手にメールを読ませるだけで実現する手段はあるのでしょうか？ まず、テキストだけのメールの場合には、単にテキストが画面に表示されるだけですから、これだけではまず不可能でしょう。端末のエスケープシーケンスを用いて細工をするという可能性を議論したことがありますが、これも難しいでしょう。問題は、MIME（Multi-purpose Internet Mail Extentions）形式のメールです。MIME形式を用いると、画像ファイルや動画ファイル、音声ファイルなどを添付して、それを相手側で見ることができるようになります。この場合、GhostScriptのファイル操作拡張機能やRichText（MS-Word文書などを添付して送った場合の形式）に含まれるマクロ機能などで前述の操作（ファイル操作やプログラムの実行）ができる可能性があります（.gifファイルのファイル記述領域を用いるとできる可能性があるという報告もある）。

しかし、これらの方法については可能性だけが示唆されただけで、実際にこうした方法を用いてウィルスが送り込まれたという報告は出されていません。MIMEの勧告では、画像表示プログラムやPostScriptインタープリターなど、別プログラムを起動する際には、必ず本当に実行するかをユーザーに問うことを求めています。したがって、知らない人から受けとったメッセージに興味をそそる画像ファイルが格納されているように記述されていたとしても、それを表示しないように設定しておけばいいでしょう。

結局のところ、可能性がないわけではないが、今のところ低いということです。とくに、今回の「Good Times」ウィルスのように、メーラー（受けとったメールを読むためのソフトウェア。MHやVMAILなど）やオペレーティングシステムを特定せず、どんな状況でも感染するようなウィルスを送り込むことはまず不可能だと断言できます。それよりも、NetNewsに流れるバイナリーだけのプログラムを実行するほうがよっぽど危険だということに留意してください。

とはいうものの、メールの読み書きについては、以下の点に注意しておくべきでしょう。

回答者●砂原秀樹
奈良先端科学技術大学院大学
情報科学センター助教授
電気通信大学情報工学科助教授（併任）
WIDEプロジェクト・ボードメンバー。
日本でのインターネット普及のために
研究と後輩の指導に努めている。

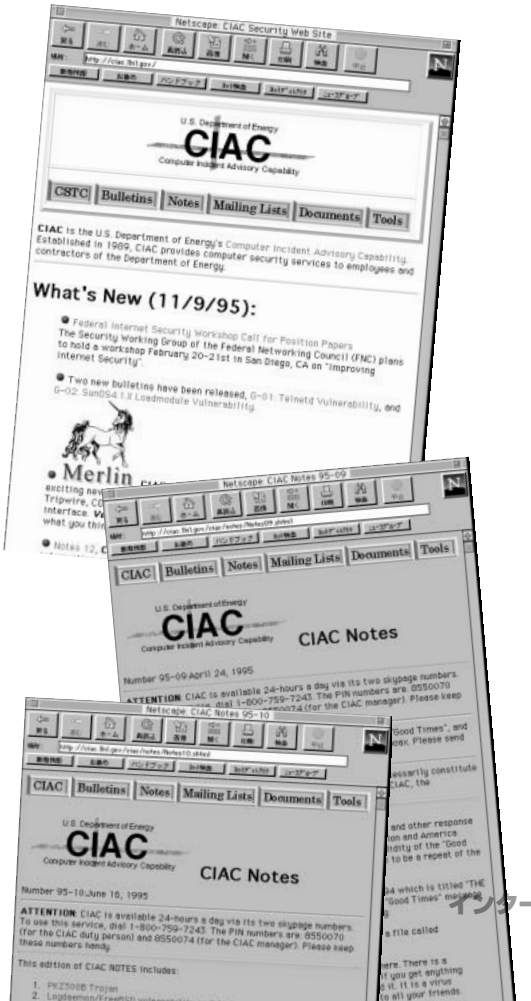
❶特権ユーザー（root）でメールを読み書きしない特権ユーザー宛のメールは、実際に管理を行うユーザーまたはユーザーのグループに転送し、そこで読み書きするようにしましょう。このかぎりにおいて、特権ユーザーの権限が不用意に他人にわたることはなくなるはずです。

❷MIMEメッセージの表示は注意深く、たとえ楽しそうな画像でも、知らない人から送られたメールに含まれるものは表示しないようにするべきです。また、画像表示プログラムなどを起動する際に、確認の問い合わせをせずにいきなり実行するようなメーラーはすぐに利用を停止するべきです。また、送られてきたメッセージにプログラムが含まれているような場合においても、これを自動起動するような設定やメーラーの利用はやめるべきです。

ともかく、インターネットにこれだけ情報が氾濫するようになると、デマもたくさん出回るようになってきます。デマに惑わされないだけの知識を身につけていないと、情報にふり回されるだけになってしまいます。

通常、こうしたセキュリティに関する情報は、「どのシステム（オペレーティングシステムやアプリケーション）でどういうことをしたときに発生するから注意するように」と記述されています。ですから、今回のように単にパニックを煽るようなメッセージは疑ってみるべきでしょう。非常に有名なMorris Wormでさえ、BSD UNIXで動作するSunとVAXだけにしか侵入できなかったのですから。

最後に、「Good Times」ウィルスは、世界中のインターネット利用者がパニックを起こして電子メールを大量に発送したこと、つまり、チェーンメーン（いわゆる不幸の手紙のようなこと）的能力が、最もウィルスらしいものであったという感想を誰かが述べていました。そういう意味では、「GoodTimes」ウィルスは成功だったのかもしれませんね。



先日インターネットを始めたばかりです。プロバイダーはベッコアメに加入しました。ぼちぼちネットスケープであちこちを見て回ったりしています。さて、電子メールで不都合が生じていて、どうしたら解決するのか悩んでいます。アメリカの友人のところへメールが送れないのです。ところが、同じ宛先にニフティサーブからはメールが送れます。また、アメリカの友人からメールを受け取ることは可能で、ほかのところへメールを送ることもできます。結局、どこともやりとりができるのですが、アメリカにいる友人に送信することだけができないのです。ニフティサーブからメールが送れるのですから、もちろんアドレスは正しいはずです。どうしたら解決するのでしょうか。よい解決策があったら教えてください。

（古野慎二さん）

A. 基本的に、インターネットはすべての場所との接続性を確保することが最も重要な目標となっています。とくにプロバイダーはインターネットへの接続性を提供することで収益をあげているわけですから、これは至上命題であるわけです。したがって、どのプロバイダーを利用しても原則としてインターネット上のすべてのコンピュータに到達可能となっているはずです。どこのネットワークを利用しているからつないであげないといった意地悪（意図的な設定）はありえません（少なくともそう信じたい）。当然、ファイアウォールの問題などで、組織内のコンピュータに他の組織から直接アクセスできないといったことは起こることですが、今回の質問のようにメールが届かないということはないでしょう。

しかし、インターネットはベストエフォート（Best Effort: 最善努力）式のネットワークであり、「できるだけがんばるけど失敗

したら許してね」という方針の元に運用されています。コンピュータの故障などなんらかの要因でうまく届かない場合が発生するかもしれないというわけです。システムのメンテナンスなどの理由でたまたま届かないということもありますから、1度や2度届かないからといって、全然届かないというのはあまり良いことではなく、しばらく時間をおいて（たとえば1日2日たってから）再度試してみるべきでしょう。

ところで、今回の質問はたぶん何度も試みた結果だと思いますが、いかがでしょうか？ そうだとすると、インターネットのどこかの設定に問題があるようです（とくにベッコアメの設定とは限りません）。したがって、自分が利用しているプロバイダーと連絡を取り合いながら問題に対処していかなければならないわけです。

しかし、こうしたときに、単に「メールが届かない」だけでは、問題への対処のしようがありません。少なくとも、どういう症状なのかを正しく伝えることを覚えていただきたいと思います。たとえばメールの場合には、原則としてエラーが発生するとどういった問題でエラーしたのかを電子メールで送り返してきます（図1参照）。したがって、まずはどういうメッセージが返ってきたのかを正しくプロバイダーの技術者に伝えるようにしてください。

最近、電子メールにかぎらず、「うまくつながらないんだけど、どうして？」とか、「WWWが使えないけどなぜ？」といった質問をよく受けるようになりましたが、大抵の場合、必要な情報がないために、「それでは答えようがないよ」と言わざるをえないことが多いのです。細かいことがわからなくてもいいですから、エラーメッセージなど発生している問題の症状を的確に伝える技術を身につけるようにしてください。それが問題解決への近道でもあります。

```
Received: from localhost by mailgate.aist-nara.ac.jp (8.6.10+2.5Wb1/2.8Wb/NAIST-1.6[gate])
          id QAA09066; Mon, 13 Nov 1995 16:47:28 +0900
Date: Mon, 13 Nov 1995 16:47:28 +0900
From: Mail Delivery Subsystem <MAILER-DAEMON>
Subject: Returned mail: User unknown
Message-Id: <199511130747.QAA09066@mailgate.aist-nara.ac.jp>
To: <suna@is.aist-nara.ac.jp>

The original message was received at Mon, 13 Nov 1995 16:47:12 +0900
from alpha401.aist-nara.ac.jp [163.221.216.49]

   ----- The following addresses had delivery problems -----
<who@cs.uec.ac.jp>  (unrecoverable error)

   ----- Transcript of session follows -----
... while talking to uecgw.cs.uec.ac.jp.:
>>> RCPT To:<who@cs.uec.ac.jp>
<<< 550 <who@cs.uec.ac.jp>... User unknown
550 <who@cs.uec.ac.jp>... User unknown

   ----- Original message follows -----
Received: from alpha401.aist-nara.ac.jp by mailgate.aist-nara.ac.jp (8.6.10+2.5Wb1/2.8Wb/NAIST-
1.6[gate])
          id QAA09060; Mon, 13 Nov 1995 16:47:12 +0900
Return-Path: <suna@is.aist-nara.ac.jp>
Received: by alpha401.aist-nara.ac.jp (5.67+1.6W[kuis-17]/2.8Wb/NAIST-1.3[is])
          id AA12551; Mon, 13 Nov 95 16:47:07 GMT+0900
Date: Mon, 13 Nov 95 16:47:07 GMT+0900
From: suna@is.aist-nara.ac.jp
Message-Id: <9511130747.AA12551@alpha401.aist-nara.ac.jp>
Apparently-To: who@cs.uec.ac.jp

this is test
```

図1　エラーメッセージの例

最近、会社でマッキントッシュを使用して某商用プロバイダーにダイアルアップIP接続を始めました。普段は、イーサネットを通じて社内のLANに接続しています。ここで、MacTCPをPPPに切り変えて、商用プロバイダーに接続し、マッキントッシュのセレクターをみると、しっかりとAppleTalkでつながっているのに気がつきました。もしかして、外部と社内はつながっている？現在、ダイアルアップIP接続には、ファイアウォールなどのセキュリティは考慮していませんが、ダイアルアップIP接続をターゲットとした侵入などは、問題になっていないのでしょうか？ なお、NCSATelnetを使用している場合、FTPを有効にすると、外部からファイルを盗まれる危険があると思います。

（小杉正志さん）

A. これは、自分が利用しているマッキントッシュを経由して社内に侵入されないかということを心配しておられるのですよね。ここで問題となるのは、あなたが利用しているマックが中継をしているのかどうかということです。ここには2つ障

害があって、まずはマック自身が中継を行うように設定されているのかどうかが問題となります。さらに、インターネットはIP、AppleTalkはAppleTalkプロトコルにしたがってネットワークが動いています。したがって、インターネットの世界から社内のAppleTalkのネットワークが、あるいは、その逆が見えるようになるためには、これら2つのプロトコルの間でのプロトコル変換という作業をMacが行なうようになっている必要があります。

僕が知りうるかぎり、通常の状態でマックがIPとAppleTalkの中継を行うことはありません。したがって、あなたが利用しているマックは単に2つのネットワークに接続されたコンピュータという状態にすぎません。したがって、現状でとくに心配することはないでしょう。ただし、インターネットから一旦あなたのマックに入り（たとえばTELNETしてくる）、さらに社内ネットワークに侵入するという経路が考えられますが、通常の設定ではあなたのマックにTELNETしてくるようなことはできませんから、これについても心配することはないでしょう。

なお、小杉さんの質問にあるNCSATelnetでの問題はご指摘のとおり危険ですので、設定しないようにしておくことをお勧めします。

A. 公開されていることと、それを利用して良いか否かということは、独立の問題ですから注意してください。以前にも書いたとおり、PGPの日本での利用は今のところグレイな状況のままです。RSAの技術は輸入規制が緩和されても、PGPに関して結論は出ていません。PGPにかぎらずどんなものでもそうですが、最終的には自分自身の責任で利用するか否かを決めなくてはなりません。つまり、サーバーで公開している人たちは自分たちの責任で、それを公開しているわけですし、それを利用する人は、各自の責任で利用することを決めているわけです。

したがって、現状としてグレイな部分はありますが、それを認識したうえで自分の判断で利用するか否かを決めていただきたいと思います。

11月号にPGPについてのFAQがありましたが、現在下記のように公開されています。やはり、いけないのでしょうか？もし、OKが出ているのなら、再度掲載をお願いいたします。たとえば、http://www.y-min.or.jp/Activity/PGP.htmlから手繰っていくとPGPの使い方とPGPのプログラムが入手できます。
（佐々木光夫さん）

ところで、今回は2つのネットワークの間に立つコンピュータがマックでしたので特別なことをしていないかぎり、気にすることはなかったのですが（これはウィンドウズなどでも同様です）、UNIXマシンによる接続などでは標準の設定で中継ができるようになっていますので注意が必要です。もし、社内ネットワークに接続されたUNIXマシンからダイアルアップ接続サービスを利用してインターネットを利用する場合には、必ず中継を行わないように設定をしなければなりません。これは、カーネル内のipforwarding（ip_forwardingの場合もある）という変数に0を設定すればよく、オブジェクトにパッチをあてたりソースコードで変更したりして設定をすることになります。詳しい方法はシステムによって異なりますので、オペレーティングシステムのマニュアルなどを参照してください。

［インターネットマガジン　バックナンバーアーカイブ］ ご利用上の注意

このPDFファイルは、株式会社インプレスR&D（株式会社インプレスから分割）が1994年～2006年まで発行した月刊誌『インターネットマガジン』の誌面をPDF化し、「インターネットマガジン　バックナンバーアーカイブ」として以下のウェブサイト「All-in-One INTERNET magazine 2.0」で公開しているものです。

http://i.impressRD.jp/bn

このファイルをご利用いただくにあたり、下記の注意事項を必ずお読みください。

- 記載されている内容（技術解説、URL、団体・企業名、商品名、価格、プレゼント募集、アンケートなど）は発行当時のものです。
- 収録されている内容は著作権法上の保護を受けています。著作権はそれぞれの記事の著作者（執筆者、写真の撮影者、イラストの作成者、編集部など）が保持しています。
- 著作者から許諾が得られなかった著作物は収録されていない場合があります。
- このファイルやその内容を改変したり、商用を目的として再利用することはできません。あくまで個人や企業の非商用利用での閲覧、複製、送信に限られます。
- 収録されている内容を何らかの媒体に引用としてご利用する際は、出典として媒体名および月号、該当ページ番号、発行元（株式会社インプレスR&D）、コピーライトなどの情報をご明記ください。
- オリジナルの雑誌の発行時点では、株式会社インプレス R&D（当時は株式会社インプレス）と著作権者は内容が正確なものであるように最大限に努めましたが、すべての情報が完全に正確であることは保証できません。このファイルの内容に起因する直接的および間接的な損害に対して、一切の責任を負いません。お客様個人の責任においてご利用ください。

このファイルに関するお問い合わせ先
株式会社インプレスR&D
All-in-One INTERNET magazine 編集部
im-info@impress.co.jp