[特集]

すずきひろのぶ／白橋明弘（P202〜P203、P214〜P215、P220〜P221）／林 毅（P210〜P211）
Photo（本文中）：Nakamura Tohru

スパムメールからファイアーウォール技術まで

最強インターネットディフェンス術

インターネットが生活の一部となり始めた今、

そこには多くのプライバシーが存在するようになった。
楽しさや便利さを得るために、
「影」の部分から身を守る術が求められている。
部屋のドアに鍵をかけるように、
今こそ「最強のディフェンス術」をマスターしたい。

“インターネット”大都会を歩く

巨大都市“インターネット”

私たちは情報時代と呼ばれる時代に生きている。インターネットという世界を覆うネットワークを使うことができる。世界中に散らばる莫大な数のサイトがここに接続されて、世界中に散らばるユーザーが利用している。私たちは地球の裏側に存在しているサイト上の情報を瞬時にアクセスすることが可能だ。同時に、自分のサイトから世界に向けて情報を発信することもできる。

1960年代の頃である。マーシャル・マクルーハンという社会学者は、通信技術によって世界が1つに結ばれ、密に情報を交換し合うような世界を予見した。そして、そのような世界に住む人々が作るコミュニティーを「グローバルビレッジ」と名付けた。いわゆる「地球村」である。

マクルーハンが今から30年以上も前に予見した通信技術によって世界を1つにしてしまう状況は、今日のインターネットそのものだ。しかし、それは「地球村」と言えるのだろうか。

彼の予想は大きく外れた。インターネットによって出現したのは「村」ではなく「大都市」だった。しかも、世界中どこにも存在し得ないような超巨大都市だ。

地域格差≠情報格差

競争をするうえにおいて、同じことをするなら情報をたくさん持っているほうが有利である。実世界でも、情報は大都市に集中する。そして、地域格差が情報格差に結びつく。その結果、大都会に住むほうが競争を有利に進められるようになる。

ところが、インターネットの世界では地理的な問題は関係なくなる。インターネットを使うことで、どこに住んでいようとも情報格差はなくなる。だれもが大都会の住民なのである。これは素晴らしいことであり、インターネットがもたらす可能性の多くがここにあるのだ。

「光」あるところに「影」がある

「インターネットは危険か安全か」
この議論をする前に
インターネットがどんな場所かを考えてみよう。
さまざまな情報にあふれ、世界中の人々が国境を超えて集まる。
実生活にたとえるなら、それはまさに「大都会」である。
都市生活者なら、自分の住んでいる場所が
危険か安全かにかかわらず、
無防備でいることはありえない。
インターネットが悪意の人であふれているなどという
幻想に怯えるのではなく、
そこが都会なのだという自覚を持つことから始めよう。

という

どう暮らすかでセキュリティーレベルも変わる

実生活と同様に、インターネットという大都会にどれだけ深くかかわるかで護身術のレベルも変わる。そこに住むのか、たまに遊びに行くだけなのか、それともそこが職場なのか。この特集では、インターネットの利用形態を初級、中級、上級の3つに分類してそれぞれのユーザーにどんなリスクがあるのか、そしてどんなことに注意すべきなのかを詳しく解説する。まずは、自分がどのレベルにあてはまるかを考えてみよう。

ディフェンス術［初級編］

自宅からダイアルアップでインターネットに接続する。インターネットの利用目的はおもに趣味のための情報収集。いくつかのメーリングリストにも加入し、ソフトウェアもウェブサイトやFTPサイトからダウンロードする。

このようなユーザーなら「スパムメール」と「ウイルス感染」から身を守る方法をマスターしておきたい。その予防は、そして被害を受けてしまったらどうするか。

ディフェンス術［中級編］

インターネットを日常のコミュニケーションの手段としている。趣味よりも仕事での利用が中心。FTPやTELENETで自分のホームページも管理する。プロバイダーのサービスや会社のシステムを利用してメーリングリストの運営も手がける。

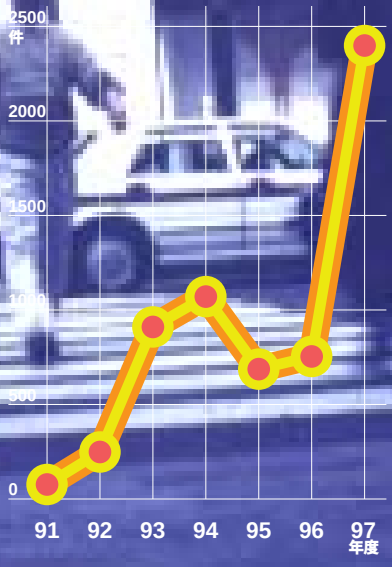
これらのヘビーユーザーはリスクも大きい。通信中のパスワード漏洩も深刻だ。そして、「メールボム」はどうすれば防げるか。「暗号メール」や「署名付きメール」の送受信もマスターしたい。

ディフェンス術［上級編］

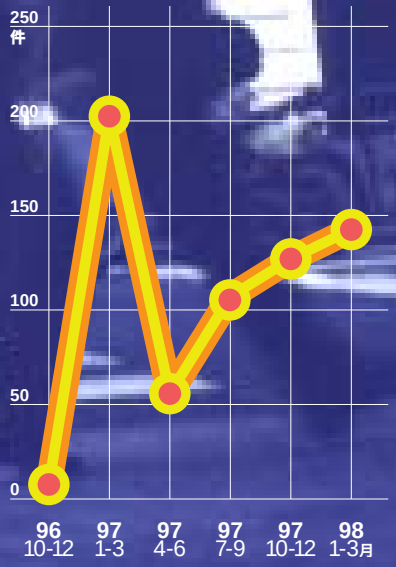
初級、中級と決定的に異なるのは「常時接続」であること。もちろん、DNSやメールサーバーも自ら管理、運営する。

いつでも相手から見える状態にあるだけにリスクは最大だ。「踏み台」として悪用されれば、自分だけでなく第三者に迷惑をかけることになる。人為的なサーバーの設定ミスからソフトウェアのセキュリティーホールまで、注意すべき点は多い。そして、頑強なファイアーウォールを築くには。

コンピュータウイルス被害の届出状況について



JPCERT/CCが受け付けた不正アクセス報告件数の推移



資料提供：IPA（情報処理振興事業協会）

＊ここにあげた件数は、JPCERT/CCが受け付けた報告の件数であり、実際の不正アクセスの発生件数を類推できるような数値ではない

大都会を安全に歩くための知恵

実世界における大都会の生活は、仕事のうえでも生活のうえでも便利にできている。情報、資本、娯楽、ありとあらゆるものがそこに集中している。が、しかし、大都会にはこのような「光」の部分があると同時に「影」の部分がある。大都会で生活するにはそれなりのリスクを覚悟しなければならないのだ。

実際、都市生活者は暗黙のうちにそのリスクを了解している。そして、リスクの中で自分で自分の安全を確保するすべを身に付けている。外出する際には鍵をかける、深夜の繁華街は注意深く歩く、街頭アンケートにむやみに回答しない。当然、見ず知らずの人に自分の住所、氏名、電話番号などを明かしたりはしない。逆説的に言えば、大都会で安全に暮らすための暗黙のルールを知っていて初めて本当の「都市生活者」と言えるのかもしれない。

つまり、「インターネット＝大都会」という事実を認識した瞬間に、そこに存在するリスクから身を守るすべを意識し始めるのは、ごくあたりまえのことなのである。

インターネットに「村」はない

実世界では、そんな危険な大都会の生活に疲れて「村」の生活に戻る者も出てくる。ところが、インターネットは端から端まですべて大都会である。確かに、インターネットの古き良き時代には「村」があったのかも知れない。しかし、今やどこにも「村」は存在しない。

私たちは過去には戻れない。大都会の呪縛からは逃れられないのだ。インターネットを使うのなら、大都会で生活する楽しさと引き替えにリスクを覚悟しなくてはならない。そして、また、どうすれば安全に生活できるかを知らなければならない。「大都会を安全に歩くための知恵」、これが今インターネットを使う者すべてに要求されている。

見せる部分と隠す部分を自分の意思で決める

プライバシーと

インターネットの利用になぜセキュリティーが必要なのか。いったい、何を守るための護身術なのか。この疑問に答えるためには「プライバシー」とは何かを考える必要がある。インターネットが生活に入り込んできた今、自分の持っている情報の中で、どれを公開してどれを隠すかをしっかりと管理することが求められている。

内側へ向かう情報と外側へ向かう情報

考えをまとめる、そして記録として残す。他者とのコミュニケーションを図る。大量の情報の中から知りたいことを検索する。コンピュータで仕事のための販売計画を作成し、勉強のためにレポートを書き、そしてプライベートな日記を付ける。電子メールで取引先に見積書を送付し、友人に季節の挨拶を送り、恋人にラブレターを送る。今日、私たちは公私にわたってコンピュータをメディアとして使っている。

そして、この単なるツールを超えたメディアは内側へ向かう部分と、外側に向かう部分という、相反する2つの方向性を持っている。

コンピュータの中には、机の引出しと同じように人には見られたくないような大切なものが一杯つまっている。いや、もしかすると、それ以上の意味を持っているかもしれない。コンピュータは私たちの知覚や思考を助けるものとなっていて、そこにはあなたの知っていることや考えていることの断片が、情報という形で収まっているところまで進んでいる。

そうなると、自分のコンピュータに入っている、あるいはやりとりしている情報というのは、あなたのプライバシーそのものではないだろうか。そして、これらは「内側」に向かう部分だ。

一方、今日のコンピュータはネットワークで互いに接続され、外部にアクセスする。そして外部からもアクセスされる。自宅や仕事場にあるコンピュータがインターネットという世界を覆うネットワークの一部を構成する1つのサイトとなる。これは「外側」に向かう部分だ。

プライバシーを守るためのセキュリティー

この内側と外側の区分けを自分の判断で明確にしなければならない。そうでなければプライバシーをさらけだすことになるからだ。他人に見られたくない日記、あるいは会社の会計報告書を、誰もが通る道端に置かれたテーブルに出しっぱなしする人はいないだろう。他人が勝手に出入りしたり取り出したりできない所に、しっかりとしまっておくはずだ。これらのことは、ごく普通の人間が持つごく普通の感覚だ。個人のプライバシーを何よりも大切にし、何であれ侵害したりされたりすることに関して嫌悪する人も少なからずいるだろう。

コンピュータの世界では「スタンドアローン」で使用している限りは、見られたくない情報を他人にのぞかれる可能性は非常に低い。ところが、インターネットなどのネットワークに接続した瞬間から問題は深刻になる。まずは、このような事実を認識することから始めよう。そして次の段階は、コンピュータに存在するさまざまな情報（文書だけでなく、設定やログ情報、プロフィールなども含む）の中で、どれが「隠しておきたいもの」か、どれが「公開することで意味があるもの」かをはっきりと区別してみよう。

これから話を進めていくコンピュータセキュリティーとは、ほかでもないこの「プライバシーを守る」ためにある。プライバシーを基本的人権と考えるならば、コンピュータセキュリティーとは基本的人権を守る手段なのかもしれない。

パスワードの選び方から確認しよう

コンピュータセキュリティーという話を進める前に、それ以前の話を確認しなければならない。それは、「正しいパスワードを選択しているか」ということである。もしあなたが簡単なパスワードを使っていたら、これから進める数々のコンピュータセキュリティーに関する知識は何も役に立たない。

パスワードには大文字、小文字、数字、記号を組み合わせておくこと。決して、辞書に載っているような単語や人名、地名などをパスワードに使用してはならない。そのような語句はパスワードを推測するプログラムを使えば、数分から数時間で見破られてしまうからだ。これでは、「ないよりはまし」という程度のことで、パスワード本来の役目を果たしてはいない。

初級編の前に、セキュリティー以前の最低限のルール「正しいパスワードの選び方」をマスターしておこう。

privacy【名】
❶私的自由、私生活、プライバシー、隠退、隠遁（いんとん）、独居、閑居
❷秘密、内密（⇔publicity）

security【名】
❶安全、無事、安全確保
❷安心感
❸（…からの）防衛、防御、防衛［保護］手段
❹警備部［課］、警備会社
❺（借金などに対する）担保（物件）、抵当、借用書、保証人、保証金、敷金

『プログレッシブ英和中辞典第3版』
©小学館1980、1987、1998

セキュリティ

○破られにくいパスワード

aZ$e2Pq3（大文字、小文字、数字、記号を組み合わせている）

×破られやすいパスワード

tanaka（人名を使用）
impress（会社名を使用）
19620817（生年月日を使用）
jaguar（辞書に載っている名詞を使用）

間違った情報に踊らされるな

コンピュータセキュリティーうんぬんと大上段に構えて騒ぐ必要はないのだ。あたりまえのことをあたりまえに行えばいいのである。ここでは、よくほかの雑誌やテレビで騒ぐように、「インターネットは悪意に満ちたコンピュータ犯罪者に溢れた世界だ」と煽る気はまったくない。

ちょうど、それは、都会の雰囲気を味わっただけの者が都会を知らぬ者に対して「都会は怖いところだ」と吹聴するのと同じに見える。確かに、都会は戸締りをせずに夜を過ごせるようなところではない。毎日のように犯罪が発生している。しかし、多くの都市生活者はそれなりに平和に生活している。無意味に騒いだり煽ったりする必要などどこにもないのである。

すべてのダイアルアップユーザーに贈る

ディフェンス術 初級編

こんなユーザーのための護身術

- 自宅からダイアルアップでインターネットに接続
- 利用目的は趣味の情報収集
- メーリングリストに加入している
- ソフトウェアのダウンロードを行う

10 スパムメールを防げ!

事件プロファイル① PROFILE

Tさんと A さんの場合

Tさんは、ある日自分のもとに届いた英文メールを見て驚いた。「GET CASH FAST!!」（手早くお金を稼げる）という表題が付けられたメッセージは、いわゆる「ネズミ講」の勧誘だった。もちろん、あて先にはTさん個人のメールアドレスが使われている。当然、誘いには乗らなかったものの、このメールの差出人がどこで、どうやって自分のメールアドレスを知ったのかがわからず、とても不安な思いをした。

また、Aさんのもとには卑猥な言葉を列挙した「アダルトサイト」の広告メールが送られてくるようになった。メッセージの最後の部分に「このメールを受け取りたくない方はサブジェクトに“unsubscribe”と書いて返送してください」とあったため、即座にこれに従った。ところがこれ以降、さらに多くの広告メールが届くようになってしまった。

ある日突然、見知らぬ相手から送られてくる「スパムメール」。一般のユーザーがなぜこのような事件に巻き込まれるのだろうか。

なぜ事件は起こったのか……

「スパム」メールとは、大量に発信され、受け手の意志を無視して送り付けてくる電子メール版の広告やダイレクトメールのことである。スパムの語源は肉の缶詰であるが、テレビコメディー番組で「スパム、スパム、スパム」と連呼するシーンから転じて、こうした迷惑メールのことを指す呼称となった。

スパムメールの内容は、一般的な商品の宣伝のほか、アダルトサイトの紹介やネズミ講まがいの金もうけビジネスの勧誘などが多い。電子メールはきわめて低コストで大量の相手に送れるという点が悪用されるわけである。スパムメールを出す「SPAMMER」は多くの場合確信犯であって、スパムメールを専門に引き受ける業者が送信を行っている場合も多い。

特に登録などをした覚えがないのに、なにゆえスパムメールが送られてくるのだろうか。それはあなたのメールアドレスが知らないうちに収集されているからである。ウェブサイトで何かの登録をしたデータが転用されたり、ネットニュースへの投稿やウェブページから電子メールアドレスがプログラムによって自動的に収集されたりしている。たとえば、数千万人分の電子メールアドレスのリストとスパムツールのセットが数百ドルという価格で販売されているのが現状である。

スパムメールを受け取るユーザからすれば、内容は不愉快で役に立たないし、そのためにインターネット接続費を余分に払わされるのではたまらない。プロバイダーからしても、メールサーバーやネットワークの回線といった資源をSPAMMERに「ただ乗り」されたうえに、対策や苦情の対応に追われるのでは、踏んだり蹴ったりである。

そういうわけで、SPAMMER対ユーザーやプロバイダーなど反スパム団体の熱い闘いは、インターネット上にとまどまらず、スパムを禁止する法案が米国連邦議会に提案されるまでに広がりを見せる状況になっている。

メールアドレスを不用意に露出させるな

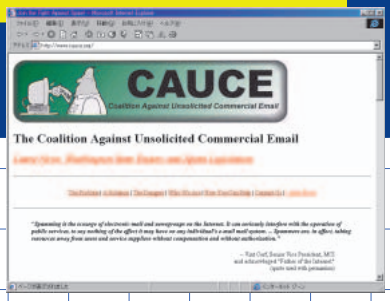
スパムメールを受けとらないで済ますにはどうしたらいいのだろうか。残念ながら、今のところこれが決め手という対策はない。まず、できるだけ電子メールアドレスを不用意に露出しないことで、スパムのリストに登録されないようにする方法が考えられる。この対策は確かに有効であるが、いわばスパム対策のためにインターネットの利用を控えるようにということであり、やや本末転倒と言わざるを得ない。

次に、スパムメールを送ってきた相手にリストから削除してくれるように伝える、あるいはメールを送らないように抗議するのはどうか。これが実はかなり危ない方法なのである。まず、このような返信を送ると「確実にメールを読んでいる相手」として認識され、最悪の場合には一層多くのスパムメールを送られる可能性がある。

次に、メールのヘッダーの「From:」に書かれているアドレスは簡単に偽造が可能な点に注意しなくてはならない。内容的に返信メールが返ってこなくてもかまわないスパムメールなら、でたらめのFrom:アドレスが書かれている場合も少なくない。

また、ある組織に対する嫌がらせを目的として、その名前とアドレスをかたって、読んだ人の怒りをかうような内容のスパムメールを送り付けるという事件も起こっている。それを受け取った人たちから多数の抗議のメールがその組織に送られ、この結果その組織のメールサーバーがパンクしたり、対応処理に追われたりする事態になる。これは立派な業務妨害行為であるが、この場合には善意の第三者が知らずして犯人に利用されてしまうわけである。

反スパム団体「CAUCE」のホームページ
URL http: / / www. cauce. org/



スパムについてのさまざまな情報が得られるCaramia Creationsの「SPAM Information Page」
URL http: / / caramia. g- net. org/ spam/

偽造ヘッダーを見破れ

ちょっとした注意を払えば、偽造ヘッダーを見分けらる場合もある。SMTPによるメール配送では、メールサーバーでメールが中継されるたびに「Received:」ヘッダーが付加される。パソコン用電子メールソフトではReceived:ヘッダーは非表示の場合が多いが、大抵「全ヘッダー表示」や「詳細ヘッダー表示」といったオプションで調べることができる。このRecevied:ヘッダーをたどると、多くの場合メールが最初に発信されたサーバーまではたどれるのである。

たとえば、著名な会社からのメールを装っているのに、Received:ヘッダーを調べるとプロバイダーからのダイアルアップ接続としか思えない「ppp73.provider.net」のようなアドレスが発信元であれば、偽造メールであると判断できる。

このように、インターネットメールの仕組みを理解していることがスパムに対抗する手立てになり得る。本特集がそのための助けとなれば幸いである。

スパムメールと偽造ヘッダーの例（アドレスと本文は架空のもの）
「From:」が企業ドメインになっているのに、最初の「Recived:」を見ると「ppp73.provider.net」とプロバイダーからのダイアルアップ接続によって送信されたことがわかる。

```
Received: from mail.○○○○.co.jp (proxy3.○○○○.co.jp [210.XXX.XX.129])
        by po.○○○○.co.jp (8.8.8/8.8.8) with ESMTP id EAA12819
        for target@○○○○.co.jp; Wed, 15 Apr 1998 04:09:31 +0900 (JST)
Received: from relay.■■■■.com (relay.■■■■.com [202.XXX.XX.65])
        by mail.○○○○.co.jp (8.8.8/8.8.8) with ESMTP id EAA05161
        for target@○○○○.co.jp; Wed, 15 Apr 1998 04:07:29 +0900 (JST)
Received: from big-business.com (ppp73.provider.net [192.XXX.XX.73])
        by relay.■■■■.com (8.8.5/8.8.5) with ESMTP id EAA19123
        for target@○○○○.co.jp; Tue, 14 Apr 1998 10:25:15 -0400 (EDT)
To: all@public.com
From: sales@big-business.com
Subject: The Hottest XXX Adult Accounts FREE
Message-ID: <19943672.886214@relay.■■■■.com>
Date: 14 Apr 1998 10:25:12 -0400

This is a ONE time mailing, if you do not wish to receive future mailings,
simply DO NOT reply and you will be taken off from the mailling list. We
apologize if you have already receieved this mailing. Due to numerous
demands we are pleased to announce the location of our new Web Page !!

Limited FREE Offer !!
Spectacular XXX Accounts Today!!
The Best in Quality and Entertainment!
The Purest and Finest Adult Content Anywhere !!
Ages 18+ Only Please.
```

20 ウイルスの感染を防げ!

事件プロファイル❷ PROFILE

Eさんの場合

Eさんの会社では、通常の業務連絡はほとんど電子メールで行っている。簡単なメッセージはもちろん、ワードやエクセルで作成した文書もメールに添付してやり取りする。ある日、取引先にエクセルで作成した見積書を送信したEさんは、取引先の担当者から送られてきた返事に驚いた。なんと、「あなたの送ってくれたエクセルファイルはウイルスに感染している」と書かれていたのだ。たった今自分が作成したばかりのエクセルファイルになぜウイルスが感染したのか。いくら考えても原因がわからない。自社のネットワーク管理者が調査を行ったところ、Eさんだけでなく、彼の会社のほとんどのコンピュータがウイルスに感染していたことが判明した。

最近話題の「マクロウイルス」である。実行ファイルだけにウイルスが感染するという常識はもう通用しない。メールに添付された単なるワープロ文書も危険なのだ。

なぜ事件は起こったのか……

今日では、どのユーザーにとってもコンピュータウイルス（Computer Virus）という単語は身近な言葉になっているだろう。また、多くの人はすでにウイルスチェッカーソフトを使っていることだろう。もしかすると、何割かはもうウイルスの被害にあっているかもしれない。

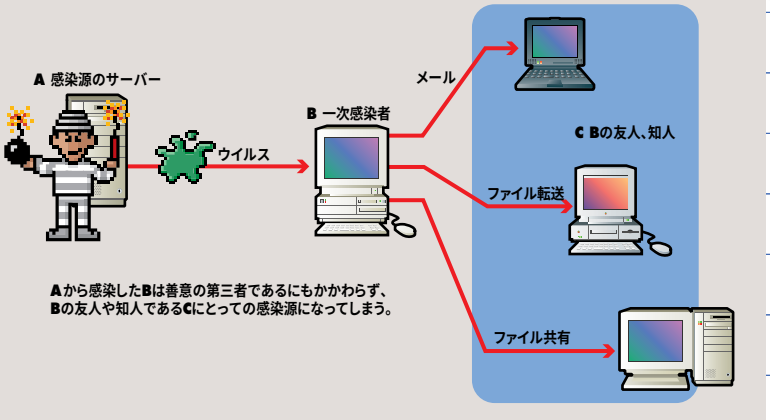
ほかのソフトウェアに寄生し、そして、感染していくようなメカニズムを持ったコードがウイルスである。1983年にフレッド・コーエンという研究者によって、「ウイルス」という命名がなされた。コーエンは、ウイルスは簡単に作成でき、簡単に隠せて、そして発見して駆除する前に広く感染するという危険性を示した。ウイルスが世間に広がっていることが認められたのは1987年だ。パキスタン生まれの「Brainウイルス」が世界最初の一般に感染したウイルスだとされている（ちなみにこの名前は、ウイルスに感染したフロッピーディスクがパキスタンにあるBrain Computerというコンピュータショップから出荷されていたことに起因する）。

ウイルスの構造自体は、はさほど複雑ではない。少し詳しい知識があれば誰にでも作れる程度のものである。したがって、1987年以降、数々のウイルスが登場してきた。また、1つのウイルスに対して一部を変更した亜流のウイルスも数多く存在する。ウイルス感染がこれだけ流行するのは、パソコンのオペレーティングシステム自体、ウイルスが感染、繁殖しやすいメカニズムを持っているからである。

ウイルス感染ルートベスト4

①電子メールの添付ファイル
②外部から持ちこまれた各種メディア
③ネットワークからダウンロードしたソフトウェア
④LAN環境での共有ファイル

ウイルスの広がり～感染者は次の感染源となる



“アウトブレイク（爆発的感染）を防げ!”

ウイルスの怖さは、感染源が明確でないまま、急速に感染が広がることにある。ほかの不正アクセスのように、悪意のある誰かが直接関与するわけではない。たとえば、あなたのマシンが感染したとき、その直接の感染源は友人や仕事仲間といった、善意の第三者からである場合がほとんどなのだ。

ウイルスを避けるための基本として、「怪しいサイトからアプリケーションを取ってこない」といったことが挙げられる。しかし、この教えを厳密に守っていても、自分の周りの誰かが破っていれば、その人経由で感染する可能性がある。

心構えだけではどうしようもなく、ウイルスチェッカーを使って防御することがどうしても必要になる。しかも、ウイルスは作るのが簡単で、新種が次々と現れる。したがって、ウイルスチェッカーは常に最新のものにアップデートしなければ、十分に役目を果たせない（次ページを参照）。

インターネットの流行以前は、フロッピーディスクでのプログラムやデータのやり取りによって感染が発生していた。インターネット時代は、これに代わって電子メールの添付ファイルやFTPでのファイル転送などが感染の原因となっている。

最近流行のマクロウイルスは、「マイクロソフトワード」などのマクロ部分に感染する。まるでワープロ文書に感染するように見える。昔のように「実行ファイルに気を付ければOK」とはいかない。

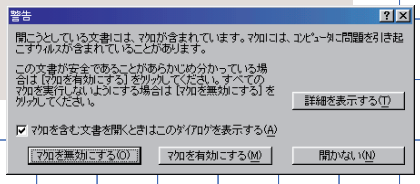
感染してしまった環境では、ワードのようなアプリケーションで新しく文書ファイルをオープンするたびに、次々と別の文書ファイルに感染していく。汚染された文書ファイルが電子メールで送られ、受け取り先で開かれると自動的にウイルスの入っているマクロが実行され、感染してしまう。

ワードが持つマクロ機能は非常にウイルスが繁殖、感染しやすいメカニズムを持っている。知らぬ間に感染しないように、自動的にマクロ実行をさせない設定にしておくなど、今まで以上に細心の注意が必要だ。

ウイルス検出アドインツールの入手

マクロウイルスに関しては、マイクロソフトもさまざまな対応を行っている。ワード97、98とエクセル97には、すでにウイルス対策機能が標準装備されている。これらのバージョンでは文書にマクロが含まれている場合、その旨をユーザーに知らせたうえでマクロを実行するかどうか、また文書を開くかどうかを選べるようになった（下図）。
これ以前のバージョンを使っている人は、必ず下記のURLから「ウイルス検出アドインツール」をダウンロードしてセットアップしよう。

マイクロソフト Security Information
URL http: / / www. microsoft. com/ japan/ Security/



1998年度（1月～3月）IPAに被害届が出された主なウィルスとその特徴

ウイルス名	件数	感染した機種	感染と発病
エクセルマクロ／Laroux	296	PC/AT、98、マック	マクロウイルス。感染したエクセルファイルを開くと、「XLSTART」フォルダーに「PERSONAL.XLS」という名のファイルを作成。これに「laroux」という名でウイルスのマクロを登録する。発病はしない。
ワードマクロ／Cap	189	PC/AT、98、マック	マクロウイルス。毎月20日以降の11時以降にワードが起動されると発病。ステータスバーに「Reading menu... Please wait!」のメッセージを表示。さらに、Cドライブの「WINDOWS」、「WINWORD」、「WINWORD6」以外のフォルダーにあるファイルをすべて消去する。日本語版のワードでは感染も発病もしない。
アンチシーモス	15	PC/AT	常駐型。ブートセクターに感染。このウイルスに感染したディスクからコンピュータを起動すると暴走する。
フォーム	13	PC/AT	常駐型。ハードディスクやフロッピーディスクのブートセクターに感染。毎月24日にシステムスピーカーからクリック音が出るようになる。
カスケード	8	PC/AT、98	常駐型。拡張子が「COM」ファイルに感染。システムの日付が1988年10月から12月になると画面 に表示された文字が滝のように流れる。
ヤンキードゥードル	7	PC/AT、98	常駐型。拡張子が「EXE」、「COM」のファイルに感染。17時になると 「Yankee Doodle」（アルプスー万尺）が流れる。
ワードマクロ／Concept	5	PC/AT	マクロウイルス。感染した回数をメッセージボックスに表示。ワードのテンプレートに「AAZAO」、「AAZFS」、「FileSaveAs」、「PayLoad」が追加される。日本語版のワードでは感染も発病もしない。
ベイジン	4	PC/AT	常駐型。ディスクのブートセクターに感染。発病はしないが、ディスクの内容を破壊することがある。
バリティブート	3	PC/AT	常駐型。ブートセクターに感染。キー入力をカウントし、これがシステムの時計と一致した際に画面表示を壊してハングアップする。
ワードマクロ／Wazzu	3	PC/AT	マクロウイルス。文書を開くたびに5分の1の確率で3回ランダムに文書内の単語の位置を入れ替えたり、4分の1の確率で「Wazzu」という文字をランダムな位置に挿入したりする。日本語版のワードでは感染も発病もしない。
ワードマクロ／Niknat	3	PC/AT	マクロウイルス。ワードの「FILE」メニューの「TEMPLATE」と「TOOLS」メニューの「MACRO」が消えてしまう。発病すると「Windows Protection Error　OK」というメッセージを表示。
ステルスブート	3	FDのみ	常駐型。ディスクのブートセクターに感染。
リッパー	3	PC/AT	常駐型。ディスクのブートセクターに感染。ウイルスが常駐している状態でディスクに書き込みを行うと、書き込んだデータが破壊され、プログラムが暴走することがある。
インベーダー	3	98	常駐型。「COMMAND.COM」以外の拡張子が「COM」、「EXE」のファイルに感染。一定時間が経過すると音楽を流す。

ウイルス対策ソフトを使ってみよう

ウイルス対策ソフトと言えば、かつてはユーザーが自分で定期的に起動しなければならないものだった。現在のウィルス対策ソフトは、ファイルを操作した瞬間にチェックを行う機能や、データファイルを自動的に更新する機能を持つものが主流になり、ユーザーがチェックを忘れてもウイルスを防いでくれるようになった。単純にハードディスクをスキャンするだけでなく、ソフトに「常駐して防ぐ」、「データを更新する」機能があるかどうか調べ、そうした機能を活用することが重要だ。

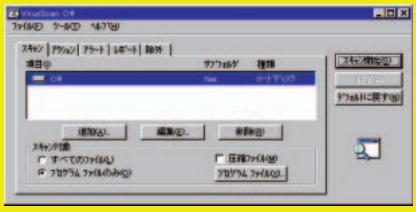
ここでは、ネットワークアソシエイツ社のウイルス対策ソフト「VirusScan」を紹介しよう。本誌付属CD-ROMにも試用版が収録されている。

ネットワークアソシエイツ社
URL http: / / www. nai. com/ japan/

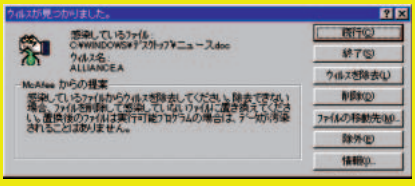
ディフェンス術 初級編

ウィンドウズ95の場合

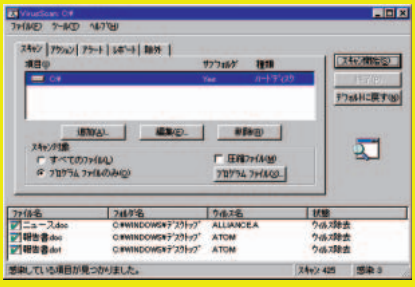
●ハードディスクをチェックしよう



インストールが完了したら、まずスタートメニューからVirusScanを起動しよう。「スキャン開始」ボタンを押すと、ウイルスチェックが始まる。

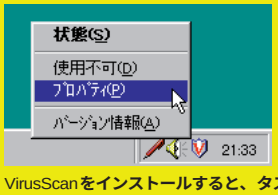


ウイルスが発見されたら、「ウィルスを除去」ボタンでファイルの修復を試みるか、「削除」ボタンでファイルを削除してしまおう。

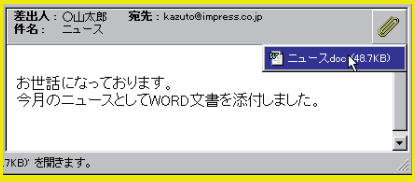


ウイルスチェックが完了した。スタートメニューから「VirusScanコンソール」を選べば、スケジュール機能を使ってウイルスチェックを行うこともできる。

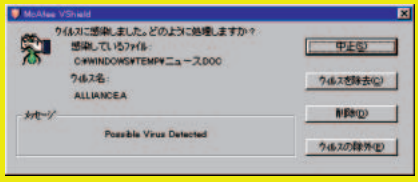
●常駐プログラムで完全ガード



VirusScanをインストールすると、タスクバーに盾の形のアイコンが現れる。これが常駐プログラムだ。右クリックで「プロパティ」を選べば、さまざまな設定ができる。

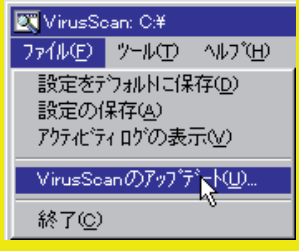


最近は電子メールにワードやエクセルのファイルが添付されることが多くなった。アウトルックエクスプレスを使えば、簡単に添付ファイルが開けてしまう。

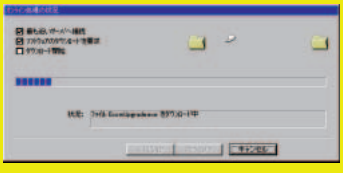


VirusScanの常駐プログラムが動いているので、ファイルを開いた瞬間にウイルスがチェックされる。「ウィルスの除去」ボタンで駆除しよう。このほかに、ファイルをコピーしたり解凍した瞬間にもチェックが行われる。

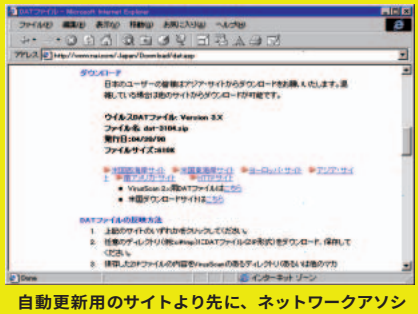
●ウイルスデータの自動更新



VirusScanを購入してユーザー登録をすれば、自動的にウイルスデータを更新する機能が使える。「ファイル」メニューから「VirusScanのアップデート」を選ぶ。



インターネット経由でネットワークアソシエイツ社のサイトに接続する。必要なファイルが自動的にダウンロードされ、更新される。



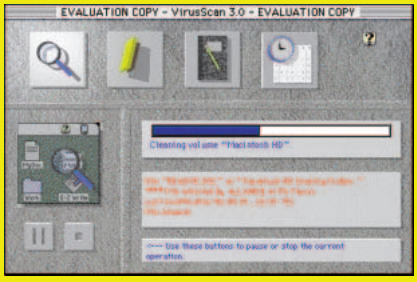
自動更新用のサイトより先に、ネットワークアソシエーツ社のホームページに最新のデータファイルがアップロードされていることがある。つねに最新の情報をチェックするようにしよう。

試用版のインストール
Trial→Win→Vscan

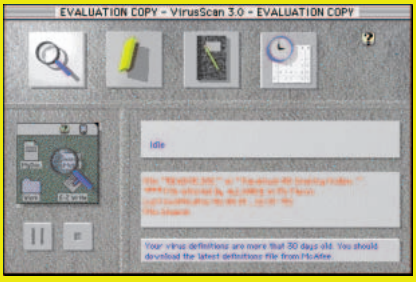
Lhasaなどの解凍ソフトを使って「v95i310e.zip」を適当なフォルダーに解凍し、「Setup.exe」を起動しよう。

マッキントッシュの場合

●ドラッグアンドドロップでウイルスチェック

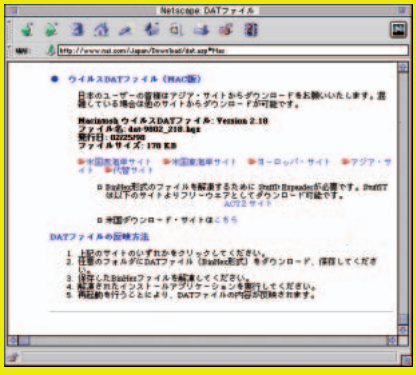


インストールが完了したら、デスクトップにできたVirusScanのアイコンに、ハードディスクのアイコンをドロップしよう。ハードディスク全体がチェックされ、ウイルスが見つかると自動的に駆除される。



アプリケーションが起動する際にもウイルスがチェックされる。ウイルスが含まれるワード文書を開こうとすると、自動的に駆除される。ウィンドウズ版と違い、ファイルのコピーや解凍の際にはチェックされない。

●ウイルスデータを更新しよう



マッキントッシュ版のVirusScanには、自動的にウイルスデータを更新する機能はない。ネットワークアソシエイツ社のホームページからファイルをダウンロードする。解凍してできたインストーラーを起動すれば簡単にデータが更新できる。

試用版のインストール
Trial→Mac→VirusScan

「VirusScan 3.0.1 Eval Installer」がインストーラーだ。アイコンをダブルクリックすれば、インストールされる。英語版なので注意してほしい。

注　意

本誌付属CD-ROMに収録したVirusScan試用版の試用期間は30日間です。30日を超えて使い続けるには、製品版を購入する必要があります。また、試用版にはユーザーサポートはありません。

正しい知識を持てばウイルスは怖くない

－IPAウイルス対策室に聞く－

「最近の傾向としてマクロウイルスが非常に増えています」とIPAセキュリティセンターコンピュータウイルス対策室の木谷氏は言う。IPA（情報処理振興事業協会）は通産省の外郭団体で、最近の高度ネットワーク化に伴い、コンピュータウイルス対策や不正アクセス対策のためのセキュリティセンターを設けている。

木谷氏の言葉にあるように、現在のウイルス被害のほとんどはマクロウイルスによるものだ。IPAの調査によると、1996年の調査では全体の10パーセントにも満たなかったマクロウイルスの被害が、1997年では全体の約65パーセントまで増えている。しかも被害件数は3倍以上に増えている。

木谷氏によれば、被害の原因は「電子メールに添付されて送られてきたウイルスに感染しているファイルを開いて感染するケースがほとんど」とのこと。まさに昨今のオフィスや家庭のネットワーク化によって生まれている被害だといえる。

また、最近ではウイルス検出ソフトやワクチンといったソフトが知られているが、これらのツールに関しての正しい知識が少ないのも原因の1つのようだ。「せっかくウイルス検出ソフトをコンピュータにインストールしていても、最新のアップデートファイルをインストールされない方が多く、新しいウイルスに対抗できずに感染するケースも多い」と木谷氏は語る。これは、ワクチンなどのソフトをインストールすることによって安心してしまうユーザーの落とし穴ともいえるだろう。アップデートファイルを更新するのは、ユーザーの努力に尽きるが、被害を防ぐ手だては現状ではこれ以外にない。

「正しい知識を持てば、ウイルスは怖いものではないし、十分に対処できる。しかし軽く見てもらうのは問題がある。ワクチンソフトの使い方を理解して、日々新しいものを使うってこそウイルスの被害を食い止めることができる」と木谷氏から力強いアドバイスをいただいた。

“（ウイルスについての）電話での相談も受け付けています。”とIPAの活動について語るIPAウイルス対策室の木谷文雄氏。

●IPAコンピュータセキュリティ対策
URL http: / / www. ipa. go. jp/ SECURITY/ index- j. html
●IPAコンピュータウイルス110番
TEL：03- 3433- 4844

使いこなしている人ほど落とし穴におちいる

ディフェンス術 中級編

こんなユーザーのための護身術

- 自宅からダイアルアップでインターネットに接続
- 社内で電子メールを使っている
- TELNETを使っている
- インターネットから社内の電子メールを取り込んでいる
- 自分でメーリングリストを管理している

10 暗号メールをマスターせよ!

事件プロファイル❸ PROFILE

Kさんと Yさんの場合

Kさんは友達とのコミュニケーションにも電子メールを使っている。友達同士で電子メールをやり取りしているということもあり、電子メールの内容はプライベートなことについて書くことが多い。

ある日、Kさん宛てに見知らぬメールアドレスから電子メールが送られてきた。その電子メールを見てKさんは驚いた。自分が友達とやり取りしていたメールの内容がすべて書かれていたのだ。電子メールの内容がどこから漏れたのかまったく見当がつかない。契約しているプロバイダーに問い合わせても明確な回答を得られなかった。

またYさんの会社のあるサーバーがクラッカーによって乗っ取られた。しばらくするとあるウェブサイトにYさんが過去にやり取りしたメールが掲示されていた。どうやらサイト乗っ取りを行ったクラッカーの犯行のようだが、もう取り返しがつかない。

こんなことがあっても不正行為からプライバシーを守る手だてはなかったのだろうか。

なぜ事件は起こったのか……

自分の発信した電子メールが相手に届くまでには、いくつものネットワークと電子メールの中継ホストを経由している。

電子メールは書かれている内容がまったく隠されていない「はがき」のようなものだ。ネットワーク上を流れる電子メールは経由しているどこかのネットワークあるいはホストの上で、管理者権限さえ持っていれば簡単に見ることができてしまう。悪意に満ちた電子メール盗聴も簡単に仕掛けられるのだ。

またシステムが不調になると、配送されなかった電子メールが山のようにたまってしまう。システム管理者は配送されなかった電子メールを1つ1つ見て、どこに何が送られなかったかをチェックしながら、システムが正しく動くようにメンテナンスをしなければならないときもある。

もしインターネットサービスプロバイダーだけを経由して電子メールが配信されるなら、少しは安心だろう。なぜならプロバイダーには電気通信事業法が適用されるので、ユーザーの通信に対する守秘義務がある。つまり内容を漏らしたり悪用したりするようなことがあれば、法律により罰せられるのだ。

ところが、大学や企業のシステム管理者にとって電子メールのシステム管理は、やりたくもない厄介な仕事が回ってきただけかもしれない。専任の管理者がいるのはまだいいが、いったい誰が管理しているのかわからないようなところも多い。そんな誰だかわからない人に電子メールの中身を見られるというのは非常に不安だ。

さらに、これは考えたくないことだが、もしメールシステムの管理者がストーカーのように悪意を持った人間だったらどうなるだろう。電子メールが経由するネットワークのシステム管理に携わるすべての人間が責任感や良心を持っているとは限らない。

最悪のケースとしては、サイトがクラッカーに乗っ取られ、かつそれを管理者がまったく気付かない場合だ。クラッカーはいくらでも他人のメールを盗み読みできる。まさかと思われるかもしれないが、管理能力に欠ける管理者も世の中にはいるのだ。

どこの誰だかわからない人間を信用してはならない。自分のプライバシーは自分で守らない限り保証されないことを心に留めておこう。

電子メールが盗み読みされる3つのケース

1. 自分が登録しているメールホストのシステム管理者による盗み読み
2. 電子メール中継地点のメールホストのシステム管理者による盗み読み
3. メールホストのあるサイトを乗っ取ったクラッカーによる盗み読み

暗号メールで対処しろ!

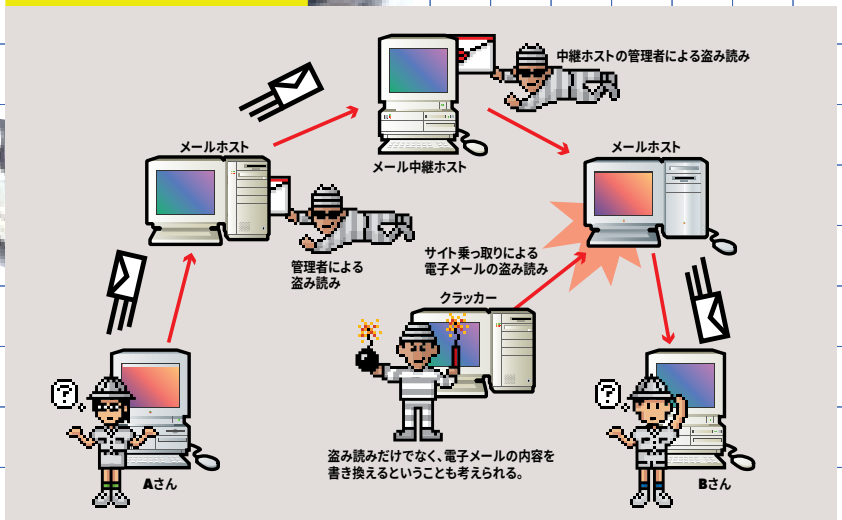
電子メールははがきであると説明したが、電子メールを封筒に入れたかのように読めなくしてしまえば、他人に読まれる可能性はなくなる。これを実現するのが暗号技術だ。

インターネットのようにネットワーク経由で暗号をやり取りする場合は、暗号化する鍵と復号化する鍵が異なる公開鍵暗号法を用いた暗号方式が広く使われている。この暗号方式を使って電子メールを暗号化すれば、特定の相手しかその内容を読むことができない。

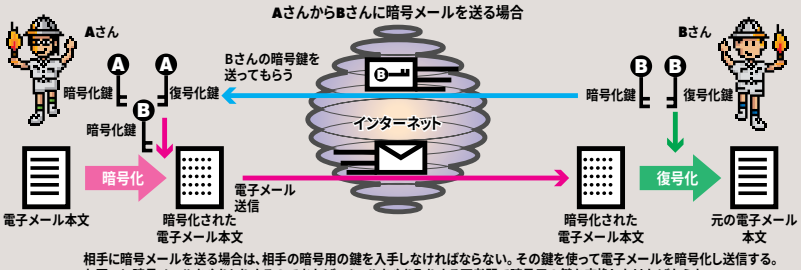
ただし、公開鍵暗号方式の中にもいくつかの方式があり、電子メールの送信者と受信者の両方で同じ暗号方式を使わなければならない。また、暗号化された電子メールを復号するための鍵が他人に盗まれないように管理する必要もある。

暗号メールはまだまだ一般に普及したとはいえないが、今後セキュリティーの意識が高まるとともに急速に普及することだろう。

電子メールの盗み読み



暗号メールのしくみ



相手に暗号メールを送る場合は、相手の暗号用の鍵を入手しなければならない。その鍵を使って電子メールを暗号化し送信する。お互いに暗号メールをやりとりするのであれば、メールをやり取りする両者間で暗号用の鍵を交換しなければならない。

主な暗号ツールと暗号メールソフト

暗号技術	解　説	対応製品
PGP	米ネットワークアソシエイツ社の汎用暗号ツール。米国版と国際版がある。	汎用ツールなので製品を選ばない。プラグインに対応電子メール製品はアウトルック（マイクロソフト）、Eudora Pro（クニリサーチ）など
S/MIME	RSA社が提唱している電子メールなどの暗号手順で、対応製品が多い。	魔法便（NTTエレクトロニクス）、Secure Messenger（アスキーサムシンググッド）、アウトルックエクスプレス（マイクロソフト）、メッセンジャー（ネットスケープ）など
FEAL	NTTが開発したFEAL（128）を使用。	Feal for Eudora Pro（NTTアドバンステクノロジ）

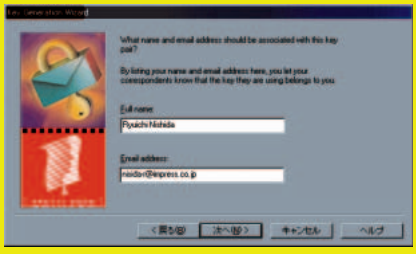
PGP5.5iを使おう!

電子メールを暗号化してやり取りするのにいくつものツールがあるが、ここではユーザーも多く汎用的に使え、しかも無料の暗号ソフトである「PGP」を取り上げる。PGPのインターフェースは以前はコマンド形式となっていたが、5.X以降のバージョンではGUIになり操作面の向上が図られた。また、プラグイン対応の電子メールソフトであれば簡単に暗号メールを送ることができるが、ここではどんな電子メールソフトでも使えるように、一般的な方法での注意点を解説しよう。

PGPの入手先
Win95、NT版 PGP5. 5. 3i
URL ftp: / / ftp. jp. pgpi. com/ pub/ pgp/ 5. 5/ win95nt/ pgp553i- win95nt. exe
MAC版 PGP5. 5. 3i
URL ftp: / / ftp. jp. pgpi. com/ pub/ pgp/ 5. 5/ mac/ pgp553iC8. sit. bin

❶鍵生成の注意点

鍵の生成はウィンドウズ版もマッキントッシュ版もほぼ同じだ。選択式になっているところは、初期値のままにしておけばいい。

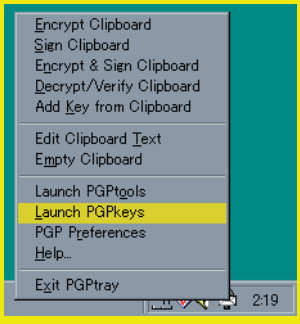


「Full Name」と「Email address」には電子メールソフトの設定と同じ内容を入力する。

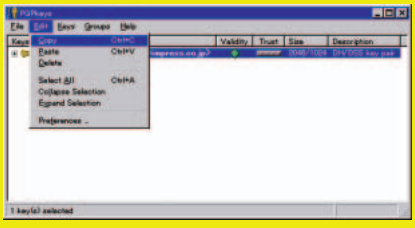
鍵タイプは「D-H/DSS」でいいが、PGP 2.6.Xを使っている人とやり取りするには別途RSAの鍵を作っておくといいだろう。

❷公開鍵を相手に送ろう

暗号メールをやり取りするためには、やり取りする二者間で互いの公開鍵を交換しなければならない。そのために公開鍵を送る必要がある。手順としては、自分の鍵をテキスト形式で取り出し、電子メールで送ればいい。



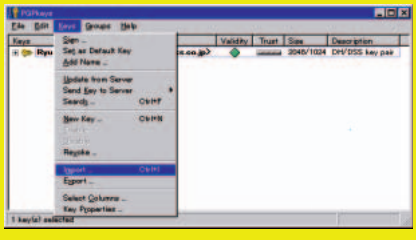
画面右下にある「PGPtray」から「Launch PGPkeys」を選び、「PGPkey」ウィンドウを開く（マッキントッシュの場合はメニューバーのPGPメニューから「PGPKeys...」を選ぶ）。



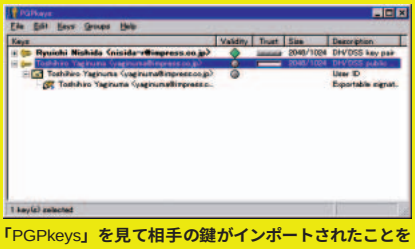
自分の公開鍵を取り出して電子メールで送るには、「PGPKeys」ウィンドウから自分の鍵を選んでコピーし、電子メールソフトの本文欄にペーストして送信する。

❸相手の公開鍵を登録しよう

相手の公開鍵を電子メールで送ってもらったら、その鍵をキーリングという鍵を保管しておく場所に登録しておく必要がある。手順としては、相手から送られてきた公開鍵入りのメール本文全体をテキストファイルとして保存し、「PGPKeys」を使ってキーリングに登録すればいい。



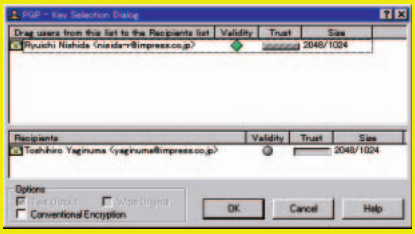
「PGPkeys」の「Keys」メニューから「Import...」を選び、ファイル選択画面ですでに保存してある（鍵データの入った）テキストファイルを選んで「Import」ボタンを押せば完了だ。



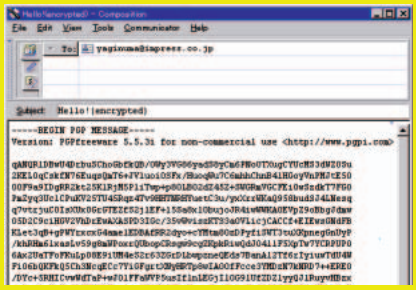
「PGPkeys」を見て相手の鍵がインポートされたことを確認しよう。

❹暗号化したメールを送信しよう

相手の公開鍵を入手したならば、その鍵を使ってメール本文を暗号化して送ればいい。まずは普段どおりの手順で電子メール本文を書いたあと、本文全体を選択してコピーする。あとはPGPを使ってコピーした内容を暗号化し、電子メール本文に貼り付けて送るだけだ。



本文全体を選択してコピーした内容を暗号化するには、「PGPtray」の「Encrypt Clipboard」を選び、「KeySelecting」ダイアログが出てきたら送信相手の鍵をダブルクリックしてウィンドウの上半分から下半分へ移動する。最後にOKボタンを押せばいい。

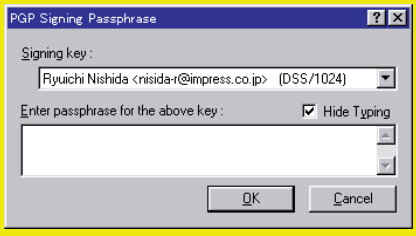


書きかけのメールに暗号化したものを貼り付けると暗号化されたテキストが表れる。あとはそのまま送信する。

❺暗号化されたメールを読もう

最後に送られてきた暗号メールの復号の仕方を解説しおく。まず送られてきた暗号メールの本文をテキストファイルとして保存しておく。このときウィンドウズ版を使っているならば、拡張子「asc」を付けておこう。あとは、作成したファイルを相手の公開鍵を使って復号化するだけだ。PGPが復号したテキストファイルを自動的に作ってくれる。

テキストファイルとして保存した暗号メールの本文（ここではenc.txt.asc）を選択し、ウィンドウズ95の場合はダブルクリックする。マッキントッシュの場合はPGPメニューから「Decrypt/Verify」を選ぶ。



ポップアップしてきたウィンドウには、鍵生成時に設定したパスフレーズを入力すればいい（すると復号化されたテキストファイルが作成される）。

PGP最新情報

米国版と国際版

PGPには商用PGPとフリーソフトPGPがあり、それぞれに対して米国内版と国際版（PGPi）が存在する。米国内版も国際版も基本的には同じものである。

ではなぜ2つのバージョンがあるのか。米国内版は米国の法律によって暗号の輸出が規制されいるので、PGPを米国から海外に持ち出せない。そこで、PGPのソースコードを出版物として海外に持ち出し、OCRを使ってそのソースコードを読み込んでファイルに戻している。このソースコードファイルをコンパイルしたものが国際版PGPである。ソースコードを米国から海外に持ち出せる理由は、出版物にしてしまえば、その著作物は米国憲法で保障された出版言論の自由により守られるからである。よって通常のユーザーが入手できるのは国際版PGPということになる。

PGPの暗号手順は本年中にOpenPGPという形でRFCになる予定がある。これが実現するとPGPのデータ交換のための明確な規格が決まるため、この規格に合ったPGP互換ソフトウェアが出てくる可能性が高い。

日本の状況

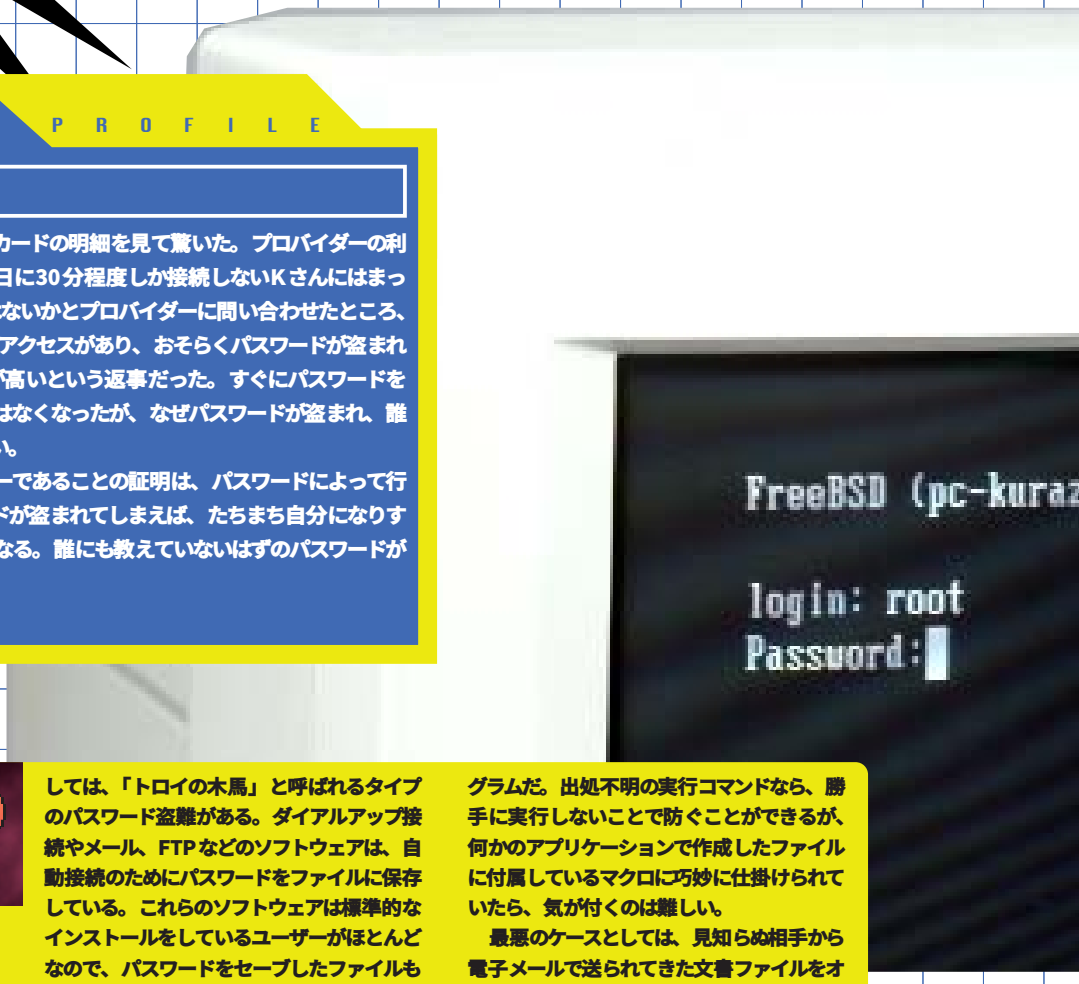
現在PGP 5.0i以降の日本語対応は、複数のボランティアの手により進行中である。ウィンドウズ、マッキントッシュ、UNIXという複数のプラットフォームで使えるように作業が進んでいる。3月から始まったばかりで全体の進捗の整理はできていないが、おそらく6、7月ぐらいには日本語に対応したPGPが国際版開発チームに渡されることだろう。

PGPの公開鍵を交換するためのサーバーが世界各地にあり、各々のサーバー間で鍵を交換している。日本でも94年4月から国内のサーバーが鍵の交換に参加している。ちなみにサーバー管理者はこの記事の筆者の一人、すずきひろのぶ氏である。

昨年末から今年にかけて世界中のPGPユーザーが激増し、すずき氏の管理するサーバーがパンクした。そのため現在は一時的に中断しており、高負荷でも耐えられるようなサーバー環境を構築している最中である。新しいサーバーの公開は5月末ぐらいになる予定。「このサーバーは劇的にネットワーク環境が良くなるので、ぜひ期待していただきたい」とすずき氏は話してくれた。

●すずき氏が管理する新しいPGPサーバー
URL http://pgp.nic.ad.jp
●国際商用版
URL http://www.pgpeurope.com
●国際フリー版
URL http://www.pgpi.com

4 パスワードの漏洩を防げ!



事件プロファイル④ PROFILE

Kさんの場合

Kさんは、ある日とどいたクレジットカードの明細を見て驚いた。プロバイダーの利用料が1万円を超えているのだ。1日に30分程度しか接続しないKさんにはまったく身に覚えがない。何かの間違いではないかとプロバイダーに問い合わせたところ、利用記録上ではたしかにKさんのIDでのアクセスがあり、おそらくパスワードが盗まれて何者かに利用されてしまった可能性が高いという返事だった。すぐにパスワードを変更してもらい、その後はそうしたことはなくなったが、なぜパスワードが盗まれ、誰に利用されたのかはいまもってわからない。

インターネットでは自分が正規ユーザーであることの証明は、パスワードによって行われている。しかし、ひとたびパスワードが盗まれてしまえば、たちまち自分になりすました他人の利用を許してしまうことになる。誰にも教えていないはずのパスワードがなぜ他人に使われてしまうのだろうか。

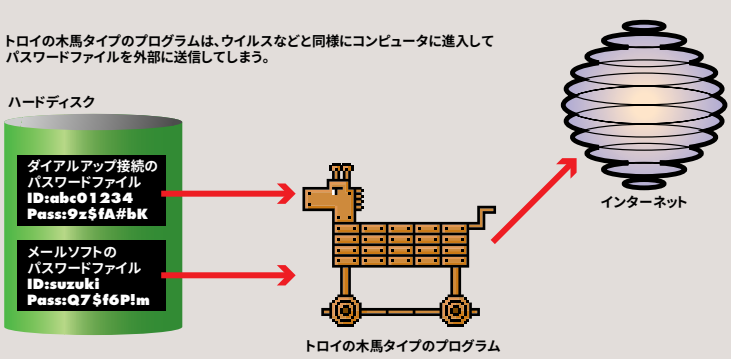
なぜ事件は起こったのか……

常識的なシステムでは、パスワードはファイルの中に暗号化された形で入っている。したがって、もしパスワードファイルが盗まれても、暗号の解読には数週間から数か月はかかるので、その間は大丈夫だろう。しかし、人名や英単語などのいわゆる「弱い」パスワードだった場合には、ありとあらゆる単語をしらみ潰しに試すタイプのクラックソフトによって、数分から数時間でパスワードは破られてしまう。「クラックするための辞書はどうやって用意するのか」などと考えるだけ無駄だ。国語辞典、英語辞典、百科事典などがCD-ROM化されて売られている。そこから大量の単語を抜き出せばよい。

たとえどんなに頑強なパスワードを使っていても、パスワード自体を盗まれたらおしまいだ。心がけ程度では防御しきれないものとしては、「トロイの木馬」と呼ばれるタイプのパスワード盗難がある。ダイアルアップ接続やメール、FTPなどのソフトウェアは、自動接続のためにパスワードをファイルに保存している。これらのソフトウェアは標準的なインストールをしているユーザーがほとんどなので、パスワードをセーブしたファイルもおおよそ似たような場所にある。こうしたファイルを自動的に取り出してどこかへ送ってしまうのが、「トロイの木馬」タイプのプログラムだ。出処不明の実行コマンドなら、勝手に実行しないことで防ぐことができるが、何かのアプリケーションで作成したファイルに付属しているマクロに巧妙に仕掛けられていたら、気が付くのは難しい。

最悪のケースとしては、見知らぬ相手から電子メールで送られてきた文書ファイルをオープンした瞬間にマクロが実行されてパスワードが盗まれる危険性が考えられる。

トロイの木馬タイプのプログラム



危機的な状況を招くネットワーク盗聴

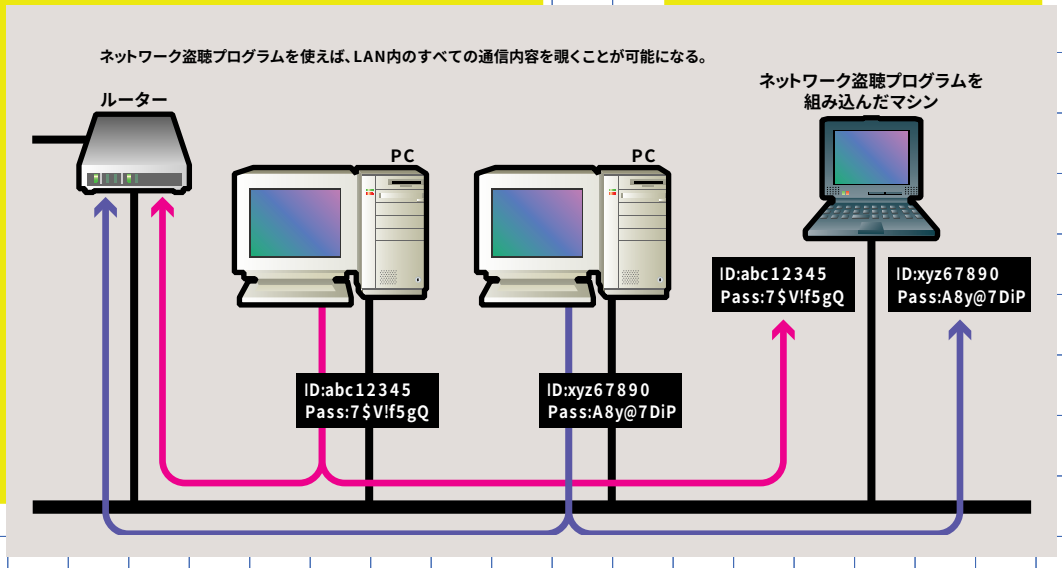
ネットワーク盗聴によるパスワード盗みはもっと深刻だ。LAN（イーサネットなど）に用いられるプロトコルは、流れているデータには誰でもアクセスできるメカニズムを持っている。そこに流れているデータはまる見えなのである。一度ネットワーク盗聴が可能になれば、リモートマシンへのログインに使われるパスワードは全部わかってしまう。ネットワーク盗聴はそんなに難しい技術ではない。ネットワークの障害を監視するためにLANを流れているデータをチェックするソフトウェアが昔からあるので、それを改造すればLAN上に流れるパスワードを盗むプログラムが簡単に作れてしまう。盗聴下においては、無防備にTELNETでも使って電子モールで買い物をしているなら、アカウント、パスワード、クレジットカード番号などすべての情報が盗まれると思ったほうがいい。

とくに厄介なのが内部犯行だ。ネットワーク盗聴のプログラムを搭載したノートパソコンをLANに接続しておけば、24時間365日、誰にも知られずにパスワードが盗み放題となる。

多くの大学や企業では、空いているネットワークポートに何が接続されてるかなど気にかけていない。実に危険な状態である。

外部からインターネットを経由して攻撃される場合には、ネットワーク内のセキュリティーの極めて弱いマシンが乗っ取られ、そのマシン上でネットワーク盗聴プログラムが実行されることによって盗聴が行われる。これは、内部犯行から比べるといくつもの壁を乗り越える必要があるので手間がかかるが、乗っ取られるマシンは後を絶たない。1台でも管理の甘いマシンが存在したならば、ネットワークに接続しているすべてのマシンが危険になることを十分に理解してほしい。

LAN内ネットワーク盗聴のしくみ



パスワードをネットワークに流さない

パスワードの漏洩を防ぐためには、まずは正しいパスワードを付けることが肝心だ。人名や単語などの簡単なパスワードでは、クラックソフトによって簡単に破られてしまうことを肝に銘じておこう。さらに気を付けなければいけないのが、パスワードの盗用を目的とした「トロイの木馬」タイプのプログラムだ。これはウイルス対策と同様で、不用意に正体不明のプログラムを実行しないことが肝心だ。

しかし、ネットワーク盗聴に対してはこうした心構えだけでは防ぎようがない。どのサイトが盗聴されているかは、外部からはわからないからだ。対策としては、なるべく外部のネットワークからはパスワードを送信しないということになる。メールの送受信やホームページの更新をFTPで行う場合には、ほかのプロバイダーなどから不用意に行うのは避けたほうが賢明だ。特にPOP3やTELNETといったプロトコルはパスワードを暗号化せずにネットワークに流してしまうため、盗聴の可能性がある環境ではたいへん危険なプロトコルだといえる。

たとえ盗聴を受けたとしても大丈夫なように、パスワードを暗号化して送信する拡張をほどこしたプロトコルを使用する方法もある。APOPはPOP3の拡張で、パスワードを暗号化して送信するプロトコルだ。対応しているメールソフト【右表】も多く、外部からメールを読む場合には、可能な限りAPOPを利用したい。ただし、サーバー側でもAPOPに対応していなくては使えないので注意が必要だ。また、TELNETに暗号化をほどこしたプロトコルとしては、SSH（Secure Shell）があるが、これもサーバーとクライアントの両方で対応する必要がある。

APOPに対応している主なメールソフト

Windows	AL-Mail32
	Becky! Internet Mail
	Eudora Pro
	WinBiff
	電信八号
Macintosh	Eudora Pro
	クラリスメール

SSHのホームページ

URL http: / / www. cs. hut. fi/ ssh/

5 メールボムを防げ!

ディフェンス術 中級編

事件プロファイル⑤ PROFILE

B社とMさんの場合

ある朝、B社のネットワーク管理者は数千通にものぼる意味不明のメールがメールボックスにあふれているのを発見した。その内容は「これ以上むだなメールを送ってくるのは絶対にやめてほしい」、「スパムメールには断固抗議する」といったものだった。当然ながら、B社がスパムメールを送った事実はない。それなのに、なぜ何千通という抗議のメールが殺到するのか。その日はもちろん、それから数日にわたって同様のメールは送られ続けた。

1日に数通のメールをやり取りするだけのMさんは、不可解な現象に悩まされていた。いつのまにか、膨大な量のメールが送られてくるようになったからだ。プロバイダーに接続してメールを読もうとしたころ、30分たっても1時間たってもダウンロードが終わらない。なんと、その日に送られてきたメールの数は2,000通を超えていた。メッセージを見たところ、どうやら何かのメーリングリストのようだった。Mさんは知らないうちに、20以上のメーリングリストに加入させられていたのだ。

ある日突然襲ってくる「E-mail爆撃」。この悪質な攻撃を防ぐ手立てはあるのだろうか。

なぜ事件は起こったのか……

「E-mail爆撃」(E-mail Bombing)は、スパムのように一応は内容を読んでもらうことが目的なのではなく、特定の相手に大量のメールを送り付けて、嫌がらせやメールサービスを利用不能にすることを目的とした悪質な攻撃である。

E-mail爆撃を行う方法には以下のようなバリエーションがある。

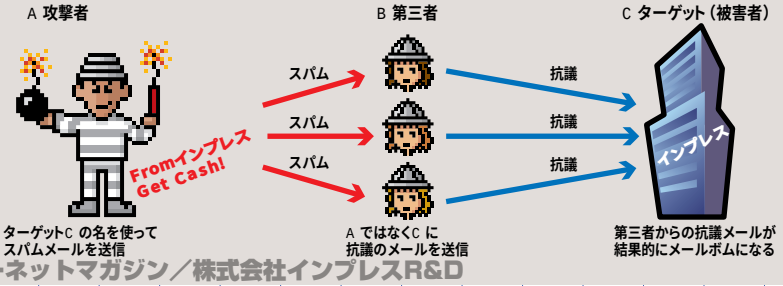
【直接攻撃】ターゲットに直接メールを送りつける爆撃。ただしメールの発信は、発信元をたどられないように不正侵入したサーバーに仕掛けたプログラムによって行われることが多い。この攻撃を受けた場合はプロバイダーの技術窓口に相談して、応急措置としてサーバーやルーターなどで当該サイトからのメールを受け取らないようにフィルタリングをしてもらうとともに、送信元サイトの管理者に連絡をして対策を依頼する必要がある。

【スパム利用攻撃】「初級編」で取り上げたように、ターゲットの名前をかたる悪質なスパムメールをばらまき、それに対する抗議のメールを集中させることによって、E-mail爆撃状態を引き起こす第三者利用攻撃。これを防ぐには、1人1人のユーザーが惑わされないよう注意するしかない。

【メーリングリスト悪用攻撃】多数のメーリングリストにターゲットとなる犠牲者のメールアドレスを勝手に登録してしまう方法。ある日突然、登録した覚えのないリストからのメールが大量に配信されることになる。この攻撃を受けてしまったら、プロバイダーの技術担当に相談して可能であればサーバーで当該メーリングリストからのメールをフィルタリングしてもらうなどの応急措置をしてもらい、そのあとで各メーリングリストの登録を1つ1つ解除していくしかない。

なお、E-mail爆撃を受けた場合、メールの内容を確認して状況を把握する以前に、メールスプールがあふれてしまったり、いつまでたってもメールの取り込みが完了しなかったりといった利用不能状態に陥る場合が多い。このような場合は、プロバイダーあるいはサイトの管理者に事情を話して、サーバー上にあるメールの内容を調べてもらうとよい。

スパムメールを利用した悪質なメールボム



メーリングリストの運用はここに注意

前ページの【メーリングリスト悪用攻撃】に見られるように、残念ながら近年ではメーリングリストがいろいろな形で悪意の第三者に利用されるケースが目立ってきている。メーリングリストの運営者は、こうした濫用行為を許さないように、メーリングリストの設定や運用に十分注意をしなければならない。以下にいくつかの防止策を紹介する。

●メーリングリストに広告宣伝のメールを投げ込む。

登録者（メンバー）のみが投稿できるようにすること（いわゆるクローズドなリスト）によって防止効果がある。

●メーリングリストのメンバー一覧を入手して不正な目的に利用する。

ある特定の分野に関心を持つ人のアドレスはダイレクトメールの宛先として価値が高い。これを防ぐためには、メンバー一覧リストを勝手に取得できないようにする。

●勝手にメーリングリストに第三者を登録してしまう

前述のようにE-mail爆撃に利用される。これを防ぐには登録を確認付きオプションにする（リスト1）。そうすると、登録（subscribe）のリクエストを送ると、登録しようとしているアドレス宛に確認（confirm）のメールが送られる。これにしかるべく返信をしないと登録は行われない（リスト2）。通常、確認のメールに含まれている毎回異なるキーを送り返す仕組みになっているので、攻撃者がこの返事までを偽装して送ることは困難である。

昨年前半、某大手プロバイダーのメーリングリストサービスが、それまでの公開型から閉鎖型（メンバーのみが投稿できる。メンバーのリストはメンバーみが取得できる。登録リクエストは一度管理人に送られて自動では登録されない）に変更されたのは、メーリングリストへのスパムメールの爆撃がきっかけだと言われている。昨年後半に多くのメーリングリストの登録が確認要求型に変更されたのも、E-mail爆撃対策のためである。一般の利用者にとってみれば、このようなセキュリティー強化は面倒と感じられるかもしれないが、悪用されたときの影響を考えれば、必要な予防対策であると言える。

【リスト1】メールボム対策を考慮したメーリングリストサーバー「fml」の設定例

```
      <<< makefml --- FML Configuration Interface --- >>>

 === TOP MENU ===

 Mailing List Addresses      FOR POST
 ip-security@〜.co.jp        FOR COMMAND       ip-security-ctl@〜.co.jp
  ____________

  0    END
  1    POLICY OF ACCESS (WHO CAN POST AND USE COMMANDS)

       [POST]
         PERMIT_POST_FROM             members_only ⇐メンバーからの投稿のみ許可
         WHEN POST FROM NOT MEMBER    reject       ⇐非メンバーからの投稿は拒否

       [COMMAND]
         PERMIT_COMMAND_FROMmembers_only ⇐メンバーからのコマンドのみ許可
         WHEN COMMAND FROM NOT MEMBERauto_regist ⇐非メンバーはsubscribeのみ可

  2    POLICY OF AUTO REGISTRATION

       AUTO_REGISTRATION_TYPE         confirmation ⇐subscribeには確認メールを送る

  3    COMMAND ADDRESS
             address for command          ip-security-ctl@〜.co.jp

  4    REMOTE_ADMINISTRATION              no

                  AUTH_TYPE               crypt

  5    SUBJECT_TAG_TYPE
  6    OPTION
  ************************************************************
  Which section? (0-6) [0]
```

【リスト2】「確認要求型」登録システムから送られてくるfml登録の確認メール

```
From: ip-security-admin@〜.co.jp
Date: Thu, 30 Apr 98 14:41:03 +0900
Reply-To: ip-security-ctl@〜.co.jp
Subject: Subscribe confirmation request (ip-security ML)
To: user@〜.co.jp
X-MLServer: fml [fml 2.1]

To confirm your subscribe request for ip-security@〜.co.jp,
please send the following phrase to ip-security-ctl@〜.co.jp

confirm 199804301441680071372 Akihiro Shirahashi


--ip-security@〜.co.jp, Be Seeing You!

Confirmation（登録の確認）について

このメーリングリスト（ip-security@〜.co.jp）では自動登録を行ないません。まず最初に

          subscribe あなたの名前（注意: Email Address ではなくあなたの名前）
          例：subscribe Keizo Kurazono

のようなリクエストを送ってもらいます。この最初の登録リクエストに対して次のような行（この数字↓はあくまでも例です）を含む

          confirm 84682771 Ken’ichi Fukamachi

このメーリングリストに登録をしてもよいかを確認するメールを返します。これは「勝手にメーリングリストへ登録されてしまう」などのいたずらへの予防策です。

あなたがこのメーリングリストへの参加確認のメールを受けとったなら、

          confirm パスワード（数字） あなたの名前

“この行だけ”を含むメールをもう一度登録用のアドレス

          ip-security-ctl@〜.co.jp

へ送信して下さい。そうするとあなたの確認が得られたとみなし、サーバーはあなたを登録します。

＊＊＊注意＊＊＊
もし、

          confirm パスワード（数字）あなたの名前

のメールをなくしてしまったとか、わからなくなってきたので最初からやりなおしたいという場合は、“最初から”、つまり

          subscribe Keizo Kurazono

を送ることからやり直して下さい。

************************************************************
If you have any questions or problems,
   please make a contact with ip-security-admin@〜.co.jp
************************************************************
```

常時接続ならばさらに危険は増す

ディフェンス術 上級編

こんなユーザーのための護身術

- インターネットに常時接続している
- DNSやメールサーバーを管理している
- ファイアーウォールを構築したい

6 サーバーの設定を徹底せよ!

事件プロファイル6 PROFILE

Oさんの場合

社内ネットワークの管理者であるOさんのもとに一通の抗議メールが届いた。メールの内容は「あなたの会社のマシンから、当社に対して不正侵入が目的と思われるアクセスが続いている。早急に対処していただきたい」というものだった。

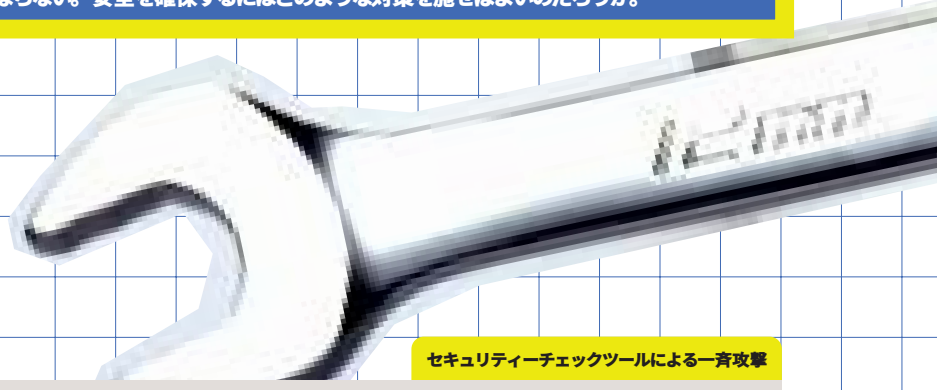
指摘を受けたマシンを見てみると、ディスクの内容が消去されていて、システムすら起動しない状態になっていた。各種の記録ファイルを調査した結果、海外から何者かに侵入されてOさんの会社のマシンが乗っ取られた痕跡が見つかった。乗っ取られたマシンには重要なファイルがあるわけでもなく、またOさんの会社自体も小規模な会社であり、狙われるような理由も思い当たらない。犯人の目的は、Oさんの会社自体ではなく、そのマシンを乗っ取ったうえで、他の会社のマシンを攻撃することにあったようだ。

常時接続環境では、便利さと引き換えにさらにセキュリティーに気を配らなくてはならない。安全を確保するにはどのような対策を施せばよいのだろうか。

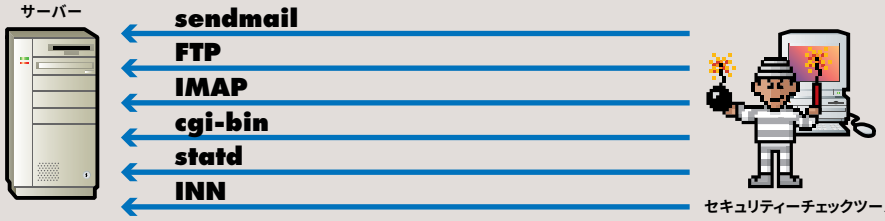
なぜ事件は起こったのか……

「企業や大学ならわかるが、なぜ何の関係もない自分のサーバーまで見つけられ、狙われるのか?」と疑問に思う人もいるだろう。理由は簡単だ。クラッカーはインターネット上に存在するすべてのサーバーに対してスキャンをかけているからだ。時間はかかるが、技術的にはそんなに難しいことではない。

クラッカーは、見つけたサーバーに対して、セキュリティーチェックツールによる検査をしかけてみる。セキュリティーチェックツールは、本来は自分のサーバーの弱点を見つけるものである。ネットワークから簡単に入手できるものも複数存在していて、管理者にとっては便利なツールだ。しかし、少し工夫すれば相手の弱点を見つけるのにも使えてしまう。



セキュリティーチェックツールによる一斉攻撃



ディフェンス術 上級編

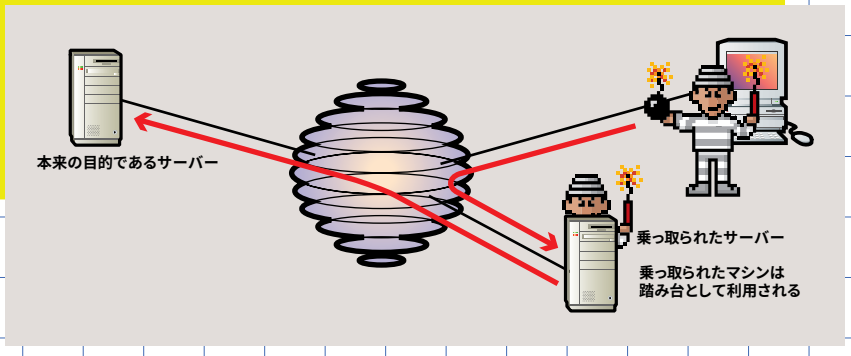
あなたのサーバーも狙われている

SOHO環境で運用しているようなサーバーは、ほとんどの場合、クラッカーはそのサーバー自体には興味がない。しかし、いったんクラックに成功すれば、そこを踏み台にしてさらに他のサーバーをアタックすることができる。相手から逆探知されるような兆候があれば、踏み台にしたサーバーのディスクをまるごと消してしまえば証拠も残らない。クラッカーにとっては、こうしたサーバーがもっとも役に立つものなのだ。

インターネットへの常時接続は、小規模なオフィスや家庭でもできるようになった。ほんの数年前までは、研究所や先端的な一部の企業でしか得られなかった環境である。いまでは回線や機材は格段に安くなり、構築も簡単になっている。とはいえ、セキュリティーに関する部分は、常時接続である限り企業も研究所も、そして家庭であっても、基本的な部分では同じことが求められる。

これは、自動車の安全運転の考え方に似ている。路上で運転するドライバーすべてに、安全運転をするための基本的な技量、知識、経験が求められる。運転している自動車の値段やサイズの違いなどは関係ない。インターネットセキュリティーでも同じである。インターネットという公共の道路に出て運転するならば、誰もが安全運転を心がけなければならない。

乗っ取ったマシンを踏み台にしたアタック



ソフトウェアの脆弱性

脆弱性とは、簡単に言えばバグのことである。バグのないソフトウェアは存在しない。セキュリティーに関するバグが発見されたら、一刻も早く新しいソフトウェアに入れ換えることが肝心だ。

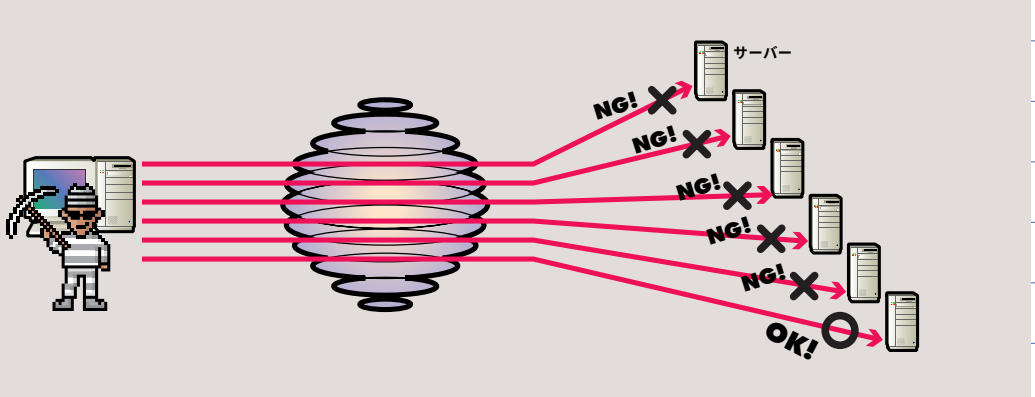
「下手な鉄砲も数打ちゃあたる」式に、古くから知られている脆弱性に対するアタックを手当たり次第に試していく乱暴なクラック方法がある。ほとんどのサーバーには無効なアタックを延々と繰り返す、何も考えていない頭の悪い方法に見えるかもしれない。ところが、現実問題として管理状態の悪いサイトは全体の割合からいけば、ほんの僅かではあるにしろ存在している。インターネットに接続されているサイト数がそもそも多いので、時代遅れのクラック方法でも何台かは踏み台が手に入る。

たとえば、古いバージョンのhttpdに付属しているcgi-bin/phfなどは、もう十分に古典に入っている有名な脆弱性だ。にもかかわらず、これが原因でクラックされるサイトが後を絶たない。また古いバージョンのIMAPへの攻撃も同様である。特にIMAPは、インストールしていることすら忘れている管理者がいるから厄介だ。

FTPも頭痛の種だ。昔から、管理者の設定ミスでよく問題を起こす。ディレクトリーの読み書きの設定が甘いと、ファイルの不正中継に使われる。たとえば、大切なデータ画像がいつのまにかポルノ画像に置き換えられることになる。FTP自体に対する設定ミスが最悪で、この場合、システムへの侵入を許す危険性すらある。

無防備なサーバーをインターネットに接続してしまえば、セキュリティーのトラブルを起こすのは時間の問題である。それは一度も路上を走ったことのないドライバーが、いきなり都内に乗り入れたようなものだ。しかし、都内での運転を（そして、インターネットを）恐れる必要はない。きちんと安全運転を覚えたうえで、注意して運転しさえすればいいだけの話なのだ。

手当たり次第のアタック方法



サーバーソフトの設定ミスを防ごう

ディフェンス術 上級編

サーバーソフトの設定を間違えると、自分のサイトだけではなく、他のサイトにも被害を及ぼすことになりかねない。このページでは、狙われやすい設定ミスやセキュリティホールとその対処方法を紹介する。

ただし、これで万全というわけではない。たとえ正しく設定していたとしても、新しいセキュリティホールはいまでも発見され続けている。最新情報については、JPCERT/CCのホームページやメーリングリストなどを参照してほしい。

JPCERT/ CC（コンピュータ緊急対応センター）
URL http://www.jpcert.or.jp/

IMAPサーバー編

❶概要

IMAPサーバーは、メールをやり取りするためのプログラムだ。University of Washingtonから配布された古いIMAPサーバーには脆弱性がある。また、このプログラムに影響を受けた他のIMAPサーバやPOPサーバーも同様な脆弱性を持っている。この脆弱性が狙われると、不正なプログラムを送り込まれ、それをroot権限で実行されてしまう。また、root権限が不正に入手され、システムに侵入される危険性もある。

IMAPサーバーの脆弱性へのアタックについての勧告は、CERT/CCからは97年4月に、日本のJPCERT/CCからは97年9月に出されている。IMAPに関する情報の詳細は、次のURLを参照してほしい。
URL http://www.jpcert.or.jp/info/97-0004/

【注意】自分ではインストールしていないつもりでも、デフォルトでインストールされている可能性があるので、必ずチェックすること。

❷バージョン

University of Washingtonから配布されたIMAPサーバープログラムのうち、以下のバージョンのものには問題が含まれている。

imapd V10.165以前
ipop2d 2.3（32）以前
ipop3d 3.3（27）以前

これらは、古いバージョンのBSD/OS、RedHat Linux、Slackware Linux、AIXなどにも含まれていた。各ベンダーに関しての情報は、次のURLを参照してほしい。
URL ftp://info.cert.org/pub/cert_advisories/CA-97.09.imap_pop

❸対処法

IMAPが必要なければ、サービスを止めればよい。/etc/inetd.confの中で、【リスト1】の部分をコメントアウトまたは削除する。

IMAPを使う場合には、最新のバージョンに変更する必要がある。最新情報に関しては次のURLを参照してほしい。
URL http://www.washington.edu/imap/server-security.html

【リスト1】/etc/inetd.conf

```
pop2  stream tcp    nowait root   /usr/sbin/tcpdin.pop2d
pop3  stream tcp    nowait root   /usr/sbin/tcpdin.pop3d
imap2 stream tcp    nowait root   /usr/sbin/tcpdimapd
```

statd編

❶概要

statdは、NFSを制御するデーモンプログラムで、各種のUNIXに搭載されている。IMAPの問題と同じように、脆弱性を狙って不正なプログラムを送り込まれ、それをrootで実行されてしまう。このセキュリティーホールを利用してroot権限を不正に入手すれば、システムに侵入される危険性がある。

statdサーバーの脆弱性へのアタックについての勧告は、CERT/CCからは97年12月に、日本のJPCERT/CCからは98年2月に出されている。statdに関しての情報の詳細は、次のURLを参照してほしい。
URL http://www.jpcert.or.jp/info/98-0001/

❷バージョン

SunOS、Digital UNIX、AIX、IRIXなどの古いバージョンのstatdは、この脆弱性を持っている。各ベンダーに関しての詳しい情報は、以下のURLを参照してほしい。
URL ftp://info.cert.org/pub/cert_advisories/CA-97.26.statd
URL ftp://info.cert.org/pub/cert_summaries/CS-98.01

❸対処法

NFSを使用しないのなら、/etc/inetd.confの中で、【リスト2】の行をコメントアウトまたは削除する。
NFSを使用する場合には、statdを最新のバージョンにする。各OSのベンダーに問い合わせていただきたい。

【リスト2】/etc/inetd.conf

```
rstatd/1-3  dgram  rpc/udp  wait  root  /usr/sbin/tcpd  rpc.rstatd
```

FTPサーバー編

❶概要

FTPは脆弱性のみならず、設定ミスでもいろいろな被害を受ける可能性がある。

・システムへの侵入
・海賊ソフトやポルノ画像ファイルなどの不正中継
・ファイルの削除、改ざん（上書き）

❷バージョン

匿名FTPサーバーとして広く用いられているwu-ftpdには、2.4.2以前のバージョンに脆弱性が存在することが広く知られている。もし使用しているwu-ftpdのバージョンが2.4.2以前のものなら、すぐに最新のバージョンに入れ換えよう。

URL http://www.academ.com/academ/wu-ftpd/release.html

また、その他のFTPサーバーに関しては、次のURLを参照してほしい。

URL ftp://info.cert.org/pub/cert_advisories/CA-97.27.FTP_bounce

❸対処法

外部から匿名（anonymous）でのFTPアクセスが必要ないときは、/etc/ftpusersにftpのエントリーを必ず追加する。

```
# mv /etc/ftpusers /etc/ftpusers.old
# cp /etc/ftpusers.old /etc/ftpusers
# echo ftp >> /etc/ftpusers
```

匿名アクセスを許可する場合には、以下のような手順を行う。

①ftpのホームディレクトリーをftp以外のユーザーの所有とする。

```
# cd ~ftp（/var/ftpの場合もある）
# chown -R nobody .
```

②~ftp/etcディレクトリー内のgroupとpasswdの所有者をrootにする。内容は【リスト3】、【リスト4】のようなダミーのものに変更する。

```
# cd ~ftp/etc
# chown root group passwd
```

【注意】/etc/groupや/etc/passwdを~ftp/etcにコピーしてはならない。また、ユーザーIDとグループIDは既存のものと重複してはならない。

③ファイルとディレクトリーを、他者の書き込みができないようにする。

```
# cd ~ftp
# chmod -R o-w *
```

また、incomingのような、外部ユーザーからの書き込みディレクトリーが欲しい場合は、以下の手順で行う。

①incomingを第三者が読めないようにする。

```
# chmod 721 incoming
```

②その下に、パスワードに匹敵するようなランダムな名前のディレクトリーを作成し、同様に第三者は読めないようにする（例として挙げたディレクトリー名とは違うものを使用すること）。

```
# cd incoming
# mkdir 64a42c6b
# chown nobody 64a42c6b
# chgrp wheel  64a42c6b
# chmod 721 64a42c6b
```

③64a42c6bのディレクトリー名を関係者のみに通知する。不要になったら、早急にディレクトリーは削除しよう。また、長期間同じディレクトリー名では使用せず、適当な頻度で別名にすることが必要だ。また、パーミッションを間違えたファイルや、ftpの所有で書かれたファイルがないかを定期的にチェックしておこう。

```
# find ~ftp/ -perm +2 -print
# find ~ftp/ -uid【ftpのユーザーID】-print
```

ftpのユーザーIDは、/etc/passwdを参照して正しいユーザーID番号を引数に与えること。

【リスト3】~ftp/etc/passwd

```
im9804:*:32766:666:Internet Magazine 98 Apr::
im9803:*:32765:666:Internet Magazine 98 Mar::
```

【リスト4】~ftp/etc/group

```
inet_m:*:666:
```

ネットワークのプロに聞くセキュリティー対策

－IIJ編－

「私どものお客様以外からのアクセスというのは、常に検出されています」IIJのファイアーウォールのログには、たしかにさまざまなアクセスの記録が残っていた。「もちろんそうした行為に対しては備えていなければいけません。しかし、それはインターネットにつながっている以上は当然のことであると考えています」と語る口調には、技術力に裏付けられた同社の自信が感じられた。

こうしたアクセスは、そのすべてが不正アクセスと呼べるものではない。相手が悪意を持っているかどうかを確認しない限りは、本当のところはわからないというのが実状だ。

このファイアーウォールはIIJの社内ネットワーク用のもので、プロバイダーサービスとして提供しているサービスホストには適用されていない。「すべての条件を満たすようなセキュリティー対策というのはありえません。目的に合わない手法を無理に用いると、排除したいものを排除できない危険は残りますし、逆に必要な通信に悪影響を及ぼすこともあります」というのが理由だ。

「また、セキュリティー対策を用いるだけでセキュリティーが万全というわけではありません。インターネットの弱点や危険性、そして限界までをも見通した上で対応することが必要です」というコメントはセキュリティーという難しい問題に対する同社の真摯な姿勢が伺える。

今回の取材では具体的なセキュリティー対策の話まで到達することはなかった。また、取材条件として提示されたのは「人物を特定するような表現は避けてほしい」ということだった。すべてを隠すことがセキュリティー対策だということを今回の取材を通して感じた。

IIJのファイヤーウォールのログにも、さまざまなアクセスの痕跡が残っていた。

7 メールサーバーの不正使用を防げ!

事件プロファイル5 PROFILE

プロバイダーA社の場合

ある日、インターネットサービスプロバイダーA社のメールサーバー管理者あてに、送信不能を告げるエラーメールが大量に届いた。さらに同じ日、A社からスパムメールを送られたという苦情が殺到した。もちろん、A社がスパムメールを送った事実はまったくない。不審に思ったメールサーバー管理者がサーバーのログやメールキューを確認したところ、なんと該当サイトあてではない怪しげなログとメールデータが多数発見された。そして、このメールデータこそ苦情のもととなったスパムメールだったのだ。この事件を起こした巧妙なSPAMMERは、差出人を偽るためにプロバイダーA社のメールサーバーを経由地点にしてスパムメールを送っていた。送信不能のエラーメールも、この処理にともなうCPUの負荷が原因であった。「不正な第三者リレー」と呼ばれるこの不正行為は、どのような盲点をついているのだろうか。

なぜ事件は起こったのか……

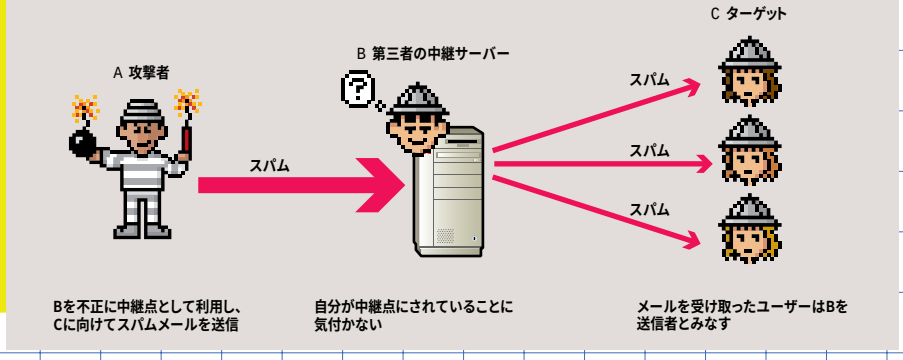
常時接続の環境でメールサーバーを運用している場合は、管理者はスパムメールやE-mail爆撃の中継点としてサーバーを悪用されないように十分注意する必要がある。

多量のメールを配送する場合、最も時間を要するのは、宛先ドメインのDNSを引いてメール送るべきサーバーを決定し、SMTPの接続を張って配送を行うところである。SPAMMERはこれをスピードアップするために、第三者のメールサーバーを勝手に中継に利用する。なるべく高速な回線に接続している適当なメールサーバーを見つけ、SMTPで接続して宛先メールアドレスを列挙してメールを送り込む。メールの本体は1回だけ送ればよい。そのサーバーとのSMTPの接続はこれで完了し、次は同じことを別のサーバーに対して繰り返し、並列配送で効率を上げる。一方中継に利用されたサーバーはSPAMMERのためにせっせとメール配送をさせられる羽目になる。

また、第三者のサーバーでの中継には、スパム発信源に対するトレースへの目くらましや、フィルタリングを逃れる意味もある。特に古いsendmailの設定では「Received:」ヘッダーに十分な中継情報を記録しないものもあって、そういうサーバーの存在はSPAMMERにとっては好都合この上ない。sendmailに代表されるメールサーバーの設定では、伝統的に悪意の利用者は想定しておらず、外から入ってきて外に出ていくようなメール中継も許してきたのが、SPAMMERにつけ込む余地を与えてしまった。

こうした「不正な第三者リレー」に利用されると、資源を無断で使用されてスパムの被害拡大の片棒をかつがされるのみならず、被害サイトからの抗議に対応しなければならなかったり、放置すればスパムサイトとしてブラックリストに登録されてしまってメールの送受信を拒否されたりするなどの副次的な被害に遭う場合もある。

こうした情勢を受けて、今日ではインターネットに直接に接続するメールサーバーでは、不正な中継を意図したメールは配送しないように設定することが強く推奨されている。



「sendmail」の設定が不正行為を防ぐ

「不正な第三者リレー」にメールサーバーを利用されるのを防ぐには、外部からのSMTPの接続に対しては、宛て先アドレス（SMTPの“RCPT TO”で指定されるアドレス）に自ドメイン（とオフサイトのバックアップメールサーバーを引き受けているドメイン）以外のものが書かれているメールは受け取らないように設定すればよい。

sendmailの場合はVer.8.7以前はソースコードを書き直す必要があったが、Ver.8.8以降では「check_rcpt」などのルールセットを利用して「sendmail.cf」のカスタマイズだけでこれを実現できる（リスト1）。

たとえばWIDEプロジェクトで配布しているsendmail設定ツール「CF」（①）を利用すれば、「MAIL_RELAY_RESTRICTION」オプションを設定したうえで、自サイトのIPアドレスまたはドメイン名を指定するだけでよいし、現在β版のsendmail Ver.8.9ではデフォルトの設定がリレー禁止に変更されるなど、スパム対策機能が強化されている。

この他のUNIXでのメールサーバーの設定法は②に詳しいし、ウィンドウズNTなどでの商用のメールサーバーソフトウェアの情報は③にまとめられているので、参考にしてほしい。

①WIDEプロジェクト「配布ソフトウェア」のページ。ここでCFを入手できる。
URL http: / / www. wide. ad. jp/ software/
②ayamura.orgの「ANTI-RELAY」
URL http: / / www. ayamura. org/ mail/ anti_relay. html
③MAPSの「How Can I Fix the Problem?」
URL http: / / maps. vix. com/ tsi/ ar- fix. html

sendmailはバージョンが上がるごとにセキュリティーが強化される。このホームページから最新情報を入手して常に最新版を使うように心がけよう。

「sendmail」のホームページ
URL http: / / www. sendmail. org

リスト1:「不正な第三者リレー」を防ぐrulesetの例

```
C{LocalIP} 210.XXXXXXXXX
C{MyDomain} ----.co.jp

Scheck_rcpt
R$+                     $: $(dequote "" $&{client_addr}$) $| $1
R0 $| $*                $@ ok           no client addr, directly invoked
R$={LocalIP}$* $| $*    $@ ok           from local
R$* $| $*               $: $>3 $2       apply ruleset 3
R$*<@$*$={MyDomain}.>$* $@ ok
R$*<@$+>$*              $#error $@ 5.7.1 $: "550 We cannot relay your mail"
```

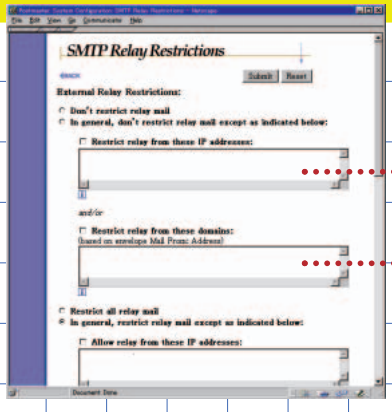
IPアドレスやドメイン名でフィルタリングする

自サイト宛てに送られてくるスパムメールの受取りを拒否するには、スパム発信源のIPアドレスやドメイン名でのフィルタリングを行うことになる。こうした機能は、やはりsendmailの設定により可能なほか、多くのメールサーバーにも備わっており、スパム被害を受けたあとに拒否リストに追加するのなら難しくはない（右図）。より徹底するならば、反スパム団体などが提供しているブラックリストを利用することもできるが、その場合はスパムでないメールまで過剰にフィルタリングしてしまう可能性があることに気を付ける必要がある。

また、SMTPの発信元アドレスにでたらめなアドレスを書いてくるメールを拒否するために、そのドメイン名をDNSでひけない（すなわちエラーメールが正しく返せない）場合は受け取らないという方法もあるが、これも送信元のサーバーやDNSの設定が不適切なだけのメールまで受け取れなくしてしまう可能性がある。実際に最近、某大手プロバイダーがこの種の設定をスパム対策のために導入したところ、ユーザーへの説明が不十分だったこともあって、いろいろ混乱をひき起こすというトラブルがあった。

複数のプロバイダーに加入していてPPP接続先とメールサーバーの所在が異なったり、大学のLANなどからプロバイダーのメールサーバーを利用する場合にも注意が必要である。POPでのメール取り込みはできても、SMTPサーバーの設定を通常のままにしておくと、不正なメール中継と見なされてメールが送れない場合がある。もちろん、接続場所に応じてメールソフトのSMTPサーバーの設定を切り替えればよいのであるが、いちいち面倒な話ではある。この問題に対して、ウィンドウズ用のWinbiffのように割り当てられたIPアドレスによって設定を切り替える機能を持つメールクライアントが現れたり、一部のプロバイダーではPOPでログインしたあと一定時間だけはそのIPアドレスからのSTMPを受け付けるようにしたりするなどの対応策も試みられている。

「Post.Office」の「SMTP Relay Rejections」設定画面
スパムメール送信者のフィルタリングは、上図のAとBに送信者のIPアドレスやドメイン名を登録すればいい。
Post.Officeの入手先（10アカウントまで無料）
URL http: / / www. software. com/



80 ファイアーウォールを構築せよ!

事件プロファイル❹ PROFILE

Sさんの場合

Sさんは自分の家でコンピュータ関連の仕事をしている。取引先とのやり取りにはインターネットを使うことがほとんどなので、OCNを引いてインターネットに常時接続している。またSさんは仕事がら個人にしては多くのマシンを所有しており、そのすべてがインターネットにつながっている。

ある日、Sさんのマシンの1台が調子がおかしいのに気が付いた。調べてみると、そのマシンが外部から不正なアクセスを受けていることがわかった。マシンの数が多いため、マシンそれぞれのセキュリティーについてはあまり考慮していなかったことが原因のようだ。起こってしまってからでは取り返しがつかないが、マシン1台1台のセキュリティーを強化するのも非常に手間がかかる。では、こんなSOHOユーザーにとってもっと簡単にセキュリティーを強化する方法はないのだろうか。

なぜ事件は起こったのか……

インターネットに常時接続しているならば、絶えず誰かに外部からネットワークに侵入される危険があると考えていい。なにも対策をほどこさないと、クラッカーは内部のネットワーク上のコンピュータに自由にアクセスできる。そうなれば、クラッカーはありとあらゆる手口を使ってシステムの不備を探せる。しかも、ゆっくりと時間もかけられる。これではクラッカーにシステムをアタックして下さいと言わんばかりだ。

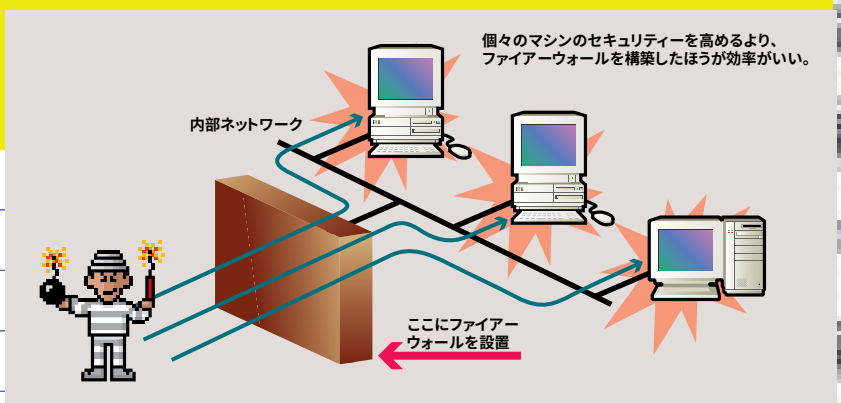
これを一手に解決してくれるのが、ファイアーウォールだ。ファイアーウォールという言葉についてはすでに多くの人が「保護するネットワークとインターネットの間に作られるアクセス制御のための仕組みで、外部からの攻撃や侵入を防ぐため“防火壁”（ファイアーウォール）と呼ばれる」という知識を持っている。

しかし、それ以上には踏み込んでくれないようだ。「ファイアーウォールは大企業のような本格的なネットワークを持っているところでしか必要ない」と考えているかもしれない。また「SOHO環境では、企業のように資源もコストもかけられない」と考えているかもしれない。

そんなに難しく考えることはない。たとえばルーターを使い、プロトコルの種類によってIPパケットをフィルタリングするだけでも立派なファイアーウォールの役目を果たす。外部からTELNETやrloginが使えないようにIPパケットをフィルタリングしていれば、侵入を試みるクラッカーはどのマシンにもログインできない。

またファイアーウォールを作らずに、個々のマシンに対して複雑なセキュリティーの設定を行うほうが実際には面倒だ。ファイアーウォールを作ったほうが管理対象が限定されて問題が局所化する。システム管理者にとって逆に楽になる可能性が大きいのだ。日常の管理にいちいち手間をかけられないSOHO環境だからこそファイアーウォールが必要なのだ。

ファイアーウォールの必要性



ファイアーウォールのセキュリティーポリシーを知ろう

インターネットとのやり取りを行うルーターを使ってIPパケットをフィルタリングすることが、ファイアーウォールの構築の第一歩であり、重要なポイントだ。

『パケットフィルタリング』は、大企業のような環境よりSOHO環境にとって非常に有利で効果的なのだ。というのは、一般にSOHO環境では内部から外部へのアクセスがほとんどで、外部から内部へのアクセスは少ない。また、誰が何のためにネットワークを使うかがはっきりわかっている。したがって、さまざまなユーザーのニーズを同時に満たさなければならない大企業よりもフィルタリングの機能を有効に使える。

しかも最近ではSOHO用ルーターであっても非常に性能が良く、パケットフィルタリングぐらいは簡単に設定できる。

ルーターを使ったパケットフィルタリングの基本的姿勢は「外からは何も通さない」である。まずは「何も通さない」から始めて、どうしても使わなければならない必要最小限のパケットだけを通すのがポイントだ。

販売しているルーターの初期状態は当然ながら「すべてを通す」設定になっている。せっかくのルーターの機能も宝の持ち腐れというだけではなく、外部から無条件のアクセスを許すという非常に危険な状態でもある。

さらに一歩踏み込んで『内部からのパケットのフィルタリング』も考慮しておきたい。

クラッカーに内部から外部へ情報を自動的に持ち出す「トロイの木馬」のようなものを仕掛けられることもある。もし内部から外部への接続が制限されていれば、これを防げるかもしれない。そうすればさらに安全性が増すだろう。

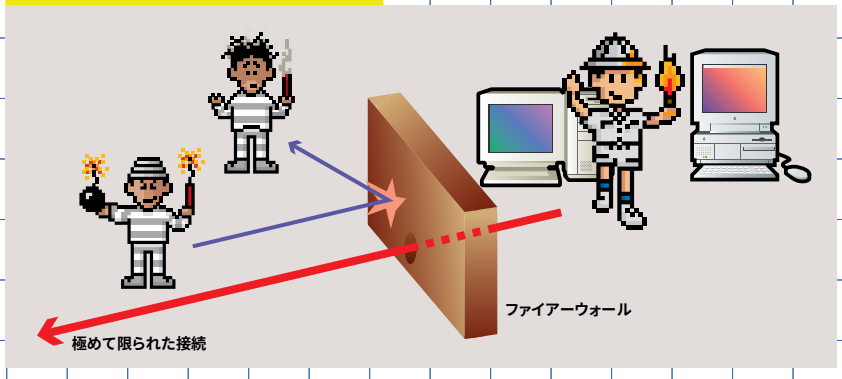
どうしても外部から内部ネットワークのコンピュータと通信する必要があるならば、『要塞ホスト』を設置したい。

要塞ホストは、簡単に言えばインターネットからHTTPやFTP、SMTPなどで直接アクセスされるサーバーのことだ。つまり、最も危険にさらされるホストであり、とりわけ堅牢に構築しなければならない。

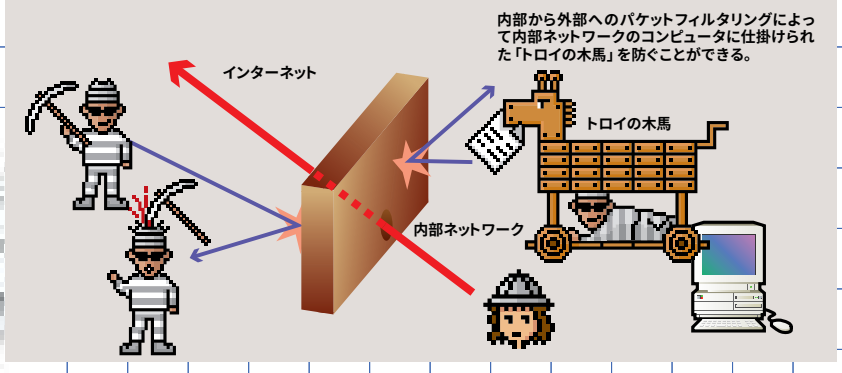
要塞ホストにユーザーアカウントを作成する場合はユーザーの権限を厳しく制限しなければならない。なぜなら、クラッカーから攻撃を受けた際にクラッカー自身が直接侵入できなくても、サーバーソフトウェアの脆弱性を突かれてパスワードファイルが盗まれるといった危険性があるからだ。要塞ホストのセキュリティー管理は十分な注意が必要だ。

このほかにもファイアーウォールの作り方はたくさんあるが、まずは「何も通さない」から始めてみるのがいいだろう。

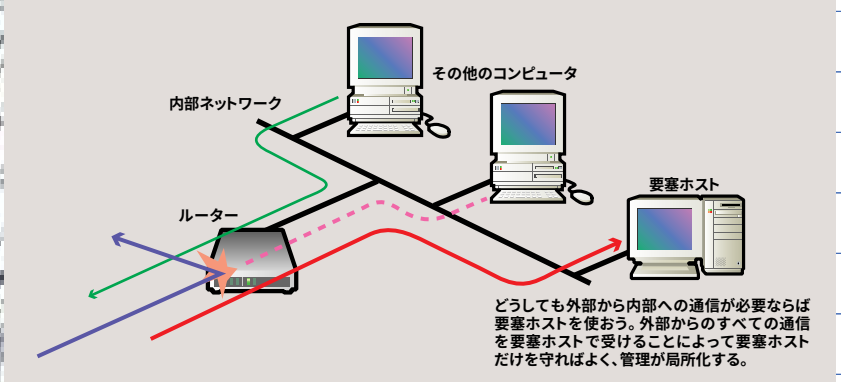
外からは何も通さないパケットフィルタリング



内部から外部へのパケットフィルタリング



要塞ホストを使ったファイアーウォール



ファイアーウォールを作ろう

前述のとおり、SOHO環境でセキュリティーを高める方法はファイアーウォールを作ることが最も手っ取り早いことがおわかりいただけただろう。そこでここではパケットフィルタリングを使ったファイアーウォールの作り方を解説しよう。また機器としては低コストでパケットフィルタリングを実現するPC-UNIX（Linux）とSOHO用ルーター（MN128-SOHO）を取り上げる。

PC-UNIX（Linux）編

安くて安心できるファイアーウォールを作るには、FreeBSDやLinuxといったPC-UNIXをプラットフォームとすることをおすすめする。

PC-UNIXを使ったファイアーウォールのためのハードウェアスペックは控え目だ。SOHO環境なので、せいぜい128Kbpsのネットワークスピードで発生する負荷に耐えられれば十分なので、ちょっと前のペンティアム75MHzマシンでOKだ。i486/100MHzだとしても十分である。ハードディスクも500Mバイト程度あればいい。ただし、メモリーは32Mバイト程度はほしい。といっても、最近のパソコンのメモリー搭載量から見れば、平均的なメモリーサイズだろう。

ここではLinuxを例に取ろう。デュアルホームホストというパケットフィルタリングを行うホスト上にWWWサーバーやメールサーバーを動かすタイプのファイアーウォールを作る手順である。もちろん、ネットワークカードが2枚必要になる。

Linuxにパケットフィルタリングの機能を設定し、このファイアーウォール上にsendmail、httpd、ftpdなど外部とアクセスするサーバー類を用意すれば、デュアルホームホストとなる。

なお同じLinuxでも、Debian、Slackware、ReadHatなどディストリビューションによって設定が少しずつ違うが、誌面が限られているので、大まかな手順だけ説明する。特にLinuxはドキュメントが豊富なので、参考になるものを探すのは楽だろう。

カーネルのコンフィグレーションおよび再コンパイルに関しては、/usr/doc/faq以下に入っている各種ドキュメントが非常に役に立つ。

❶/etc/inetd.confから不必要なデーモンを削除する

これは基本中の基本である。netstat、sysat、tftp、bootp、fingerはコメントアウトして起動させないようにする。pop、imap、rpc、rstatdなども不必要ならコメントアウトしておく。余計なものが動けば、現在は安全であっても、将来ソフトウェアの脆弱性を突いて攻撃される可能性が増えることになる。

inetd.confのエントリーの先頭に“#”を入れてコメントアウトする。

/etc/inetd.conf

```
#finger  stream tcp nowait nobody /usr/sbin/tcpd  in.fingerd -w
#systat  stream tcp nowait nobody /usr/sbin/tcpd  /bin/ps -auwwx
#netstat stream tcp nowait root   /usr/sbin/tcpd  /bin/netstat -a
```

❷カーネルの再コンパイル

カーネルをファイアーウォールとして使えるように再構築する。/usr/src/linuxの下でコンフィグレーションを行う。

```
% make config

*
* Networking options
*
Network firewalls (CONFIG_FIREWALL) [N/y/?] y ←マシンをファイアーウォールの設定にするか
IP: forwarding/gatewaying (CONFIG_IP_FORWARD) [N/y/?] y ←IPパケットをフォワードをするか
IP: firewalling (CONFIG_IP_FIREWALL) [N/y/?] (NEW) y ←IPのファイアーウォールを行なうか
```

❸2枚目のネットワークカードをインストールする

ネットワークカードがPCIバス対応のものであればプラグアンドプレイで「eth1」インターフェイスとして自動的に認識される。

/etc/rc.d/rc.inet1というファイルでeth1のためにifconfigとrouteの設定を行う。

既存側（内部ネットワーク）はすでに設定されているものと仮定しよう。ここでは新しいカード側（外部ネットワーク）の設定を行う。新しいカード側には次のようなIPアドレスが振られているとする。

/etc/rc.d/rc.inet1

```
/sbin/ifconfig eth1 192.XXX.XXX.0   \
          broadcast 192.XXX.XXX.255 \
            netmask 255.255.255.0

/sbin/route add -net 192.XXX.XXX.0  \
              netmask 255.255.255.0 \
              eth1
```

← 新しいネットワークカード（eth1）に対し、IPアドレス、ブロードキャストアドレス、ネットマスクを設定

← 新しいネットワークカード側のルーティングを設定

ディフェンス術 上級編

❹IP パケットフィルタリングの設定

PFWADM コマンドを使ってIP のパケットフィルタリングを設定する。ブート時に設定されるように/etc/rc.d/rc.inet2 といったファイルで呼び出されるようにする。
/etc/rc.d/rc.ipfwadmというファイルを作り、そのファイルにこれから説明するipfwadmの記述をする。まずは何もフォワードさせないように設定する。

/ etc/ rc. d/ rc. inet2

```
if [ -f /etc/rc.d/rc.ipfwadm ]; then
        echo -n "ipfwadm"
        /etc/rc.d/rc.ipfwadm
fi
```

/ etc/ rc. d/ rc. ipfwadm

```
#!/bin/sh
# @ IP forwarding rule file.
/sbin/ipfwadm -F -p deny
/sbin/ipfwadm -F -f
/sbin/ipfwadm -I -f
/sbin/ipfwadm -O -f
```

Ⓐ

❶限られたもののみ通過を許す。
内部からhttpのアクセスを許す例
（内部ネットワークは192.218.XXX.0/24）

Ⓐの部分に追加

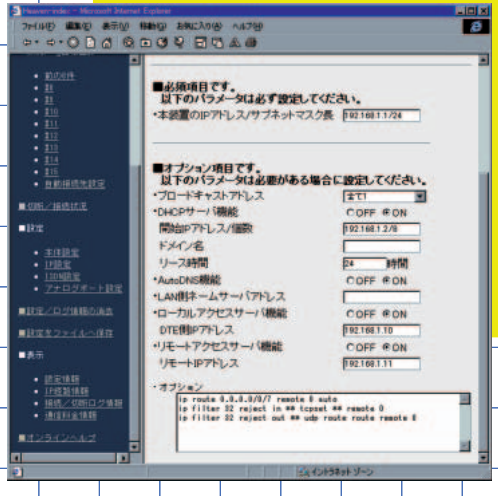
```
/sbin/ipfwadm -F -a accept -b \
    -P tp -S 192.218.XXX.* 80 \
    -D 0.0.0.0/0 1024:65535
```

❷通過パケットのログを取る
（外部から内部へのパケットを記録）。
ipfwadm関連ログ
/proc/net/ip_acct：IPアカウントに関するログ
/proc/net/ip_input：外から内に入ってきたIPのログ
/proc/net/ip_output：内から外に出ていったIPのログ
/proc/net/ip_forward：IPフォワーディングのログ

Ⓐの部分に追加

```
/sbin/ipfwadm -A -f
/sbin/ipfwadm -A -i -S 0.0.0.0/0 \
               -D 192.218.XXX.0/24
```

MN128-SOHO編



MN128-SOHOのような安価なルーターでもパケットフィルタリングの設定はできる。

設定方法はMN128-SOHOのウェブ設定画面の「設定」→「IP設定」→「オプション項目」で行う。

MN128-SOHOをOCNなど常時接続用の設定にしておくと、自動的に外部からのTCPのパケットをフィルタリングする設定になっているので、最初のうちは初期設定のままでも十分だろう。

必要に応じてIPパケットの通過を許可する。詳しい設定方法についてはMN128-SOHOのマニュアルを参照してほしい。

```
IP filter 31 reject in * * tcpset * * remote 0
❹外部からのTCPセッションを禁止する

IP filter 32 reject out * * udp route route remote 0
❹内部のルート情報を流さない（OCN用）
```

被害の報告がセキュリティー向上につながる

コンピュータ緊急対応センター
URL http: / / www. jpcert. or. jp/
連絡先
info@jpcert. or. jp

コンピュータ緊急対応センター

コンピュータへの不正アクセスを受けてしまったらどうするか。まずは、JPCERT/CC（コンピュータ緊急対応センター）に届け出をしてほしい。

JPCERT/CCは不正アクセス問題を専門に取り扱う機関だ。活動内容として不正アクセスの技術的な対応とセキュリティー技術の啓発を行っている。本誌連載記事もその活動の一環だ。

なぜJPCERT/CCに情報を提供するのか。それには2つの意味がある。まずは、被害を受けてしまった場合の技術的なアドバイスを提示してもらえるのだ。これによって不正アクセスの再発は防止できるだろう。

もう1つの理由は、情報を提供することで全体のセキュリティーが向上することだ。提供した情報によって第三者が同じような不正アクセスから守られるかもしれないのだ。

JPCERT/CCでは「有名なサイトだからという理由はなく、どこも等しく狙われる可能性があります。インターネットに国境はなく日本のサイトでも踏台にされる可能性は高い。もし踏台サイトとして侵入されたら自分だけで解決せずに、自分のサイトにアタックしてきたところ、自分のサイトからアタックされたところに連絡し、さらにJPCERT/CCへ連絡してほしい」と協力をお願いしている。

なお、JPCERT/CCでは、法的な問題（犯人特定や証拠などの調査）や民事的な問題（損害賠償などが絡む問題）、個別のシステムコンサルティングについては質問を受け付けていないので注意して欲しい。

被害を受けてしまったら……

「セキュリティーに万全はない」。
悲観的な言葉のようにも聞こえるが、実際はそうではない。
今まで解説したセキュリティー方法をもってしても、
不幸にも被害にあってしまうこともあるだろう。
だからこそ、不正行為によって被害を受けた場合の
対処方法を考えておくのだ。
これこそ、前向きな考え方であり、
本当のセキュリティー対策と言えるだろう。

不正アクセスに対するアドバイス

1. JPCERT/CCのメーリングリストへの登録（最新のセキュリティー情報の入手）
2. 定期的な運用状況のチェック（クラッカーの巧妙な手口によっては不正アクセスの検出は困難）
3. 不正アクセスに関する情報提供（日本のインターネット全体のセキュリティーの向上）

損害保険による解決もある

東京海上火災保険に聞く

東京海上火災保険がこの1月に「ネットワーク総合保険」の発売を開始した。この保険は、不正アクセスやウイルスによる被害に対して保険をかけられる契約内容となっている。契約は基本的にオーダーメードで「お客様がリスクだと感じているところを考慮して設計できる」（東京海上火災保険桑原氏）としている。

不正アクセスやウイルスによる被害は発生の確率が高く、一般的にはリスクの高い保険だという。そのため東京海上では独自のリスク評価シートを用意し、この評価シートのチェック項目の内容を考え合わせながら保険の条件などを決めて契約することになる。「各ユーザーが何も対策を講じずに、保険に頼るというのは避けたい。不正行為に対する対策や管理体制が整っているかをチェックしてもらい、対策が甘ければ対応してもらったり、保険料に反映させたりするようにしている」（桑原氏）としている。また、チェック項目を用意することで一種のコンサルティングをするような形で保険の契約に至るようだ。

いずれにせよ、セキュリティーに前向きな姿勢が求められているのは間違いない。

「リスク評価シートの結果があまりにひどいとお断りするケースがあります」（東京海上火災保険桑原茂雄氏）と厳しい意見も出された。

ニューウェーブ、さらなる発展

そして「セキュリティー」の時代がきた。

インターネットブームの裏側

インターネット自体の歴史は古いが、一般的なユーザーにまで普及したのはごく最近である。今日のインターネットの普及は、CERNで作ったWWWが広まった1991年〜1992年以降だといっていい。それ以降、インターネットに接続したサイトが急速に増え始める。この増加のおかげでさまざまなコストが下がり、接続サイトはさらに爆発的に増えた。

その間、セキュリティーに関しての問題は置き去りにされてきた。インターネットブームの波に乗り、加速度的に利用が増えた背景には低コストで利用できたという側面がある。しかし、低コスト実現のために最初に切り捨てられるのはセキュリティーである。なぜなら、セキュリティーは何も生産せず、コストを増すだけだからである。

インターネットブームを盛り上げる中では、マイナスイメージであるセキュリティー関連の話題を避けてきたような雰囲気がある。本来は当然のこととして知るべき知識であったにもかかわらずだ。意識、無意識にかかわらず、せっかく盛り上がりつつあるインターネットブームに水を差すのを恐れて排除していたのかもしれない。

セキュリティーというのは、応用技術の最たるものである。あまりにも激しいインターネットの膨張のために、セキュリティー技術に対して十分な情報提供や技術提供のチャンスがなかったという面もある。新規参入者にとっては、当面なんとか動かすことに精一杯でセキュリティーまで手が回らなかったという側面もある。

このように数々の要因が重なって、今日のインターネットセキュリティーを取り巻く複雑な状況に至っている。実際のクラッカーの手口といっても、非常に初歩的なものがほとんどである。しかし、ずさんな管理のサイトが数多く存在し、そこが攻撃対象となっているのが現実だ。

進化にともなう「リスク」

根本的な問題は、このインターネット分野というのが技術的にも最先端分野で、かつ一般市場にも急速に発展拡張している特殊な分野であるということである。

ついこのあいだまで研究室レベルだった技術が、あっというまに商品化されて一般市場に出てくる。あるいは研究室レベルの技術であるにもかかわらず、公開されればすぐに飛びつくような状況だ。ほかの分野の製品なら、本来はそこまでに何段階かの評価する時間があってはじめて一般に公開されるものがインターネットの世界では一足飛びに出て来てしまう。見切り発車的に多くの人が飛びつく状況なのだ。そこには今まで以上に多くのリスクが存在するのは当然である。

これらのリスクは「悪いコト」なのだろうか？ 必ずしも「悪いコト」とは言えない。そのリスクを自分で受け止める責任さえ持てば、今世紀最大の技術革新ともいえるこのスリリングな激流の中に飛び込むことができるのだ。

これからも新しい魅力的なソフトウェアが次々に現れるだろう。しかし、バグのないソフトウェアなどこの世に存在しない。たぶん、それらのソフトウェアにも脆弱性があるだろう。また、設定を間違えれば悲惨な目にあうかもしれない。どこまでいってもイタチごっこを繰り返すことだろう。しかし、リスクを理解したうえで正しいセキュリティーに対する意識と感覚を持てば（そして手を抜かなければ）、何も恐れることなどないのだ。

時代の最先端に飛び込む愉しみと、それゆえのリスクを自分で引き受けること。これこそがインターネットの醍醐味なのだ。

［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