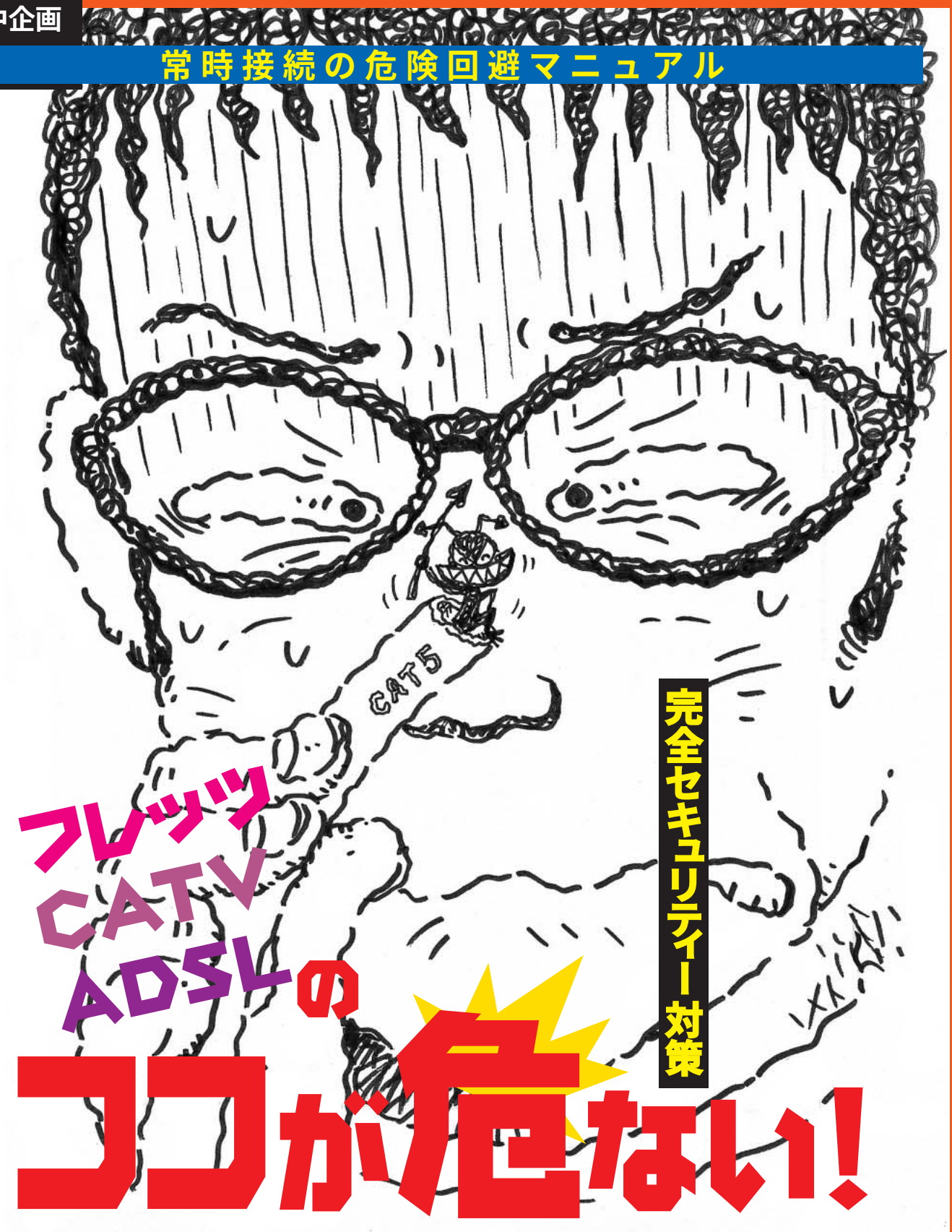


フレッツ CATV ADSLの ココが危ない!

完全セキュリティー対策

フレッツ・ISDNの登場で常時接続サービスはぐっと身近になった。しかし、常時接続の危険な部分、特にセキュリティー面の危険性は意外と知られていない。常時接続時代だからこそ、誰もがセキュリティー対策を押さえておかねばならない。この記事で紹介する簡単な設定をするだけで、あなたの常時接続のセキュリティー対策が強固なものに変わる！「備え」こそが、セキュリティー対策の基本なのだ。

梅垣まさひろ
illustration : Kimoto Hiwako

いつも誰かにねらわれている…
常時接続ウラの裏

常時接続されたコンピュータは常に人の目に触れており、不正侵入や不正使用は密かに行われる。もし、ある日突然コンピュータの調子が悪くなっても、あなたはそれが不正侵入によるものだとは簡単に気が付かないだろう。まずはどこに危険が生じやすいのかポイントをチェックしよう！ そのうえで、次ページからのケーススタディーに進みたい。

常時接続サービスに潜む危険

1 プライバシーを盗み見られる

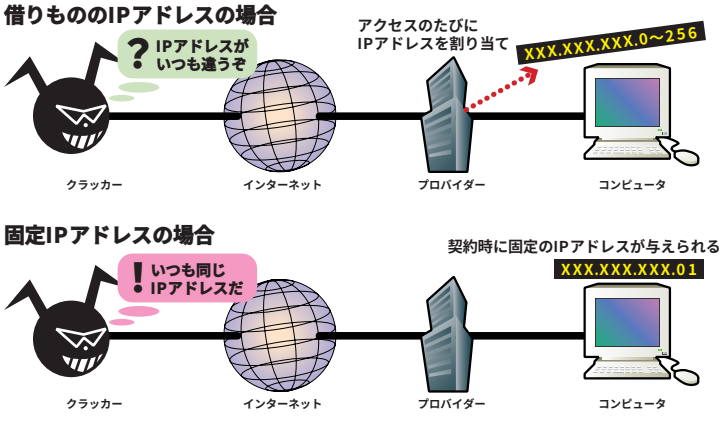
クレジットカード番号などの個人情報をはじめ、コンピュータ上の大事なファイルを盗み見られる。

2 コンピュータを壊される

重要なファイルを壊されるなど、コンピュータやネットワークを使えなくされる。

3 攻撃の「踏み台」にされる

他のサーバーへの攻撃の出撃基地にされ、共犯者にされてしまうことも…。



常時接続は甘くない！

フレッツ・ISDN（以下「フレッツ」）やCATV、ADSLなどの低価格なサービスが登場して、常時接続はぐっと身近になった。しかし常時接続されたコンピュータは、ネットワーク上に存在する他人の目に常にさらされているということを忘れてはならない。ここでまず、常時接続にどんな危険が待ち受けているのかおさらいしておこう。

1つ目は「プライバシーを盗み見られる」危険だ。もちろんダイアルアップでも同様の危険はあるが、常時接続ではより狙われやすくなる。メールのパスワードを盗み見られたり、電話番号やクレジットカードなどの大事な情報を不正な方法で知られたりしてしまうのだ。特に危険なのが、ICQなどのコミュニケーションツールで設定した個人情報を見られるケースだ。

2つ目は、ハードディスクの中身をごっそりと盗まれたり、「コンピュータを破壊」されたりする危険。特に、ネットワークを使ったファイル共有で設定ミスを犯すと、その結末は悲惨なものになる。

3つ目は「踏み台にされる」危険だ。踏み台というのは、他のコンピュータへの不正侵入のための言わば「出撃基地」として勝手に使われてしまうこと。知らない間に侵入されて、いつの間にか犯罪の片棒を担いでいることになってしまう可能性もある。

常時接続の安全性を確保することは、あなた自身に課せられた課題なのである。しかし、何も難しいことはない。この記事で紹介する簡単な設定をするだけで、たいていの危険は避けられるはずだ。

「固定IPアドレス」のリスク

常時接続の危険性を語るうえで注意しなければならないのは「IPアドレスが固定かどうか？」だ。多くの常時接続サービスの場合、コンピュータに割り当てられるIPアドレスが長時間変わらない性質を持つ。ADSLやフレッツのような固定IPアドレスのサービスを利用すると、インターネット上の「グローバルアドレス」（LANなどの閉ざされたネットワーク内だけで使うIPアドレスではなく、インターネット上のすべてのコンピュータに個々に割り当てられるユニークなIPアドレスのこと）を割り当ててもらうことができる。

固定IPアドレスを取得すれば、自分でサーバーの運用や管理ができる。これらは常時接続を使う大きなメリットなのだが、一方で、侵入しようとするクラッカーにとっては好都合なのだ。なぜなら、固定IPアドレスを使っているユーザーの名前やOSがわかれば、クラッカーは攻撃を仕掛けやすくなるからだ。ところが固定IPアドレスでなければ、クラッカーが一度侵入した後で再度侵入しようとしても、ターゲットのIPアドレスが変わっていることがあるために、簡単には侵入できない。

グローバルIPアドレスが与えられるか

サービス名	IPアドレスの種類
フレッツ・ISDN	グローバル
CATVインターネット	グローバル／プライベート
ADSL	グローバル／プライベート
OCNエコノミー	グローバル

利用するサービスが固定IPアドレスでなくても要注意だ。プロバイダーが「IPアドレスは固定ではありません」と謳っている場合でも、実際には長期にわたって同じIPアドレスが割り当てられることも多いからだ。

IPアドレス：インターネットに接続されたコンピュータを識別するために付けられる、基本的に世界で1つしかない番号。IPアドレスにわかりやすい名前を付けたのがホスト名。

ファイルを消された、盗まれた!

「ファイル共有」はとってもデンジャラス!

重要なデータ

ウィンドウズの「ファイル共有」機能には多くの危険が潜む。設定が不十分だと、いとも簡単に他人にファイルを読まれてしまうばかりか、内容を改ざんされたり、ウイルスやトロイの木馬を仕込まれたりする可能性もある。大切なデータはしっかりとガードしよう。

このとき何が起こったのか 原因と対策

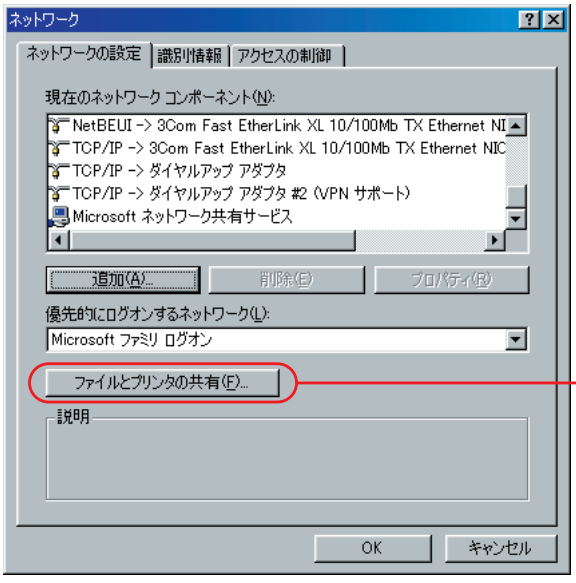
フレッツなどのように、PCにグローバルIPアドレスが割り振られるサービスでファイルを共有するのは危ない。コンピュータのIPアドレスさえわかれば、どこからでもファイルにアクセスできるからだ。ウィンドウズの「ファイル共有」はよく使われる機能だが、この機能を使うときは必ずパスワードを設定しよう。ひどいケースになると、ファイルごとの共有設定が面倒になって、Cドライブ全体をフルアクセスにしている場合もあるのではないだろうか。こうした状態で常時接続サービスを使うのは非常に危険だ。データを盗み見られるだけでなく、大切なファイルを根こそぎ消されたり、改ざんによって知らない間にトロイの木馬プログラムを仕込まれたりする可能性もある。

対策としては、フルアクセスが不要なフォルダーはできるだけ「読み取り」権限のみを与えるようにすること。どうしてもフルアクセスにする必要があるときは、フルアクセス専用のフォルダーを作るといい。もちろん、その中には必要最低限のファイルだけを置くようにし、大事なファイルは他の場所に移動しておく。共有の必要がない期間は、ファイル、プリンターともに共有設定を解除しておこう。いま一度、自分のコンピュータの共有設定をすべてチェックし直す必要があるだろう。

トロイの木馬:コンピュータ犯罪の1つ。他人のコンピュータの中に、不正行為を実行させるためのプログラムを忍ばせておく。そして、外部からそのプログラムを実行させて悪事を働くもの。

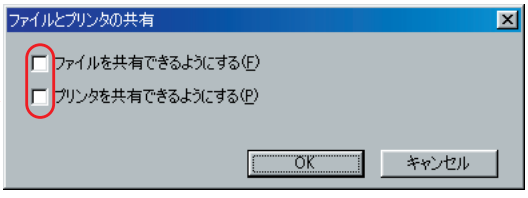
対処方法

共有の設定を確認しよう！

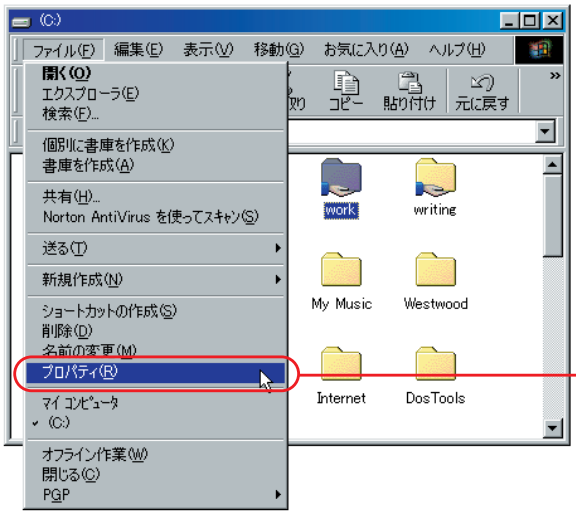


Cドライブのアイコンに手のマークが付いているのは、「共有」していることを意味する。「windows」フォルダーなどの大事なデータが含まれているCドライブをそのまま共有設定するのはやめよう！

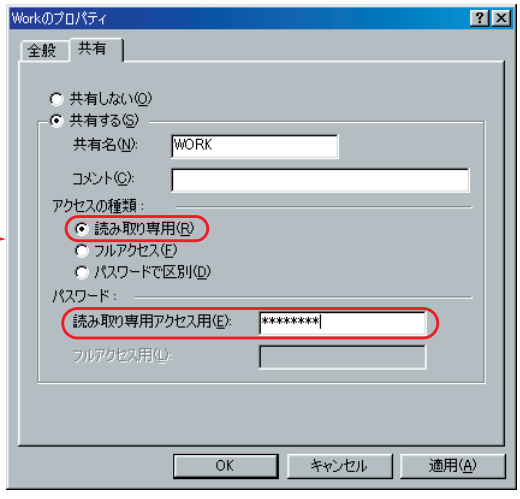
「コントロールパネル」の「ネットワーク」で「ファイルとプリンターの共有」を開き、各項目が有効になっているかどうかを確認。もし、どちらも共有する必要がないのなら、チェックを外しておくこと。



共有の範囲を決めよう！



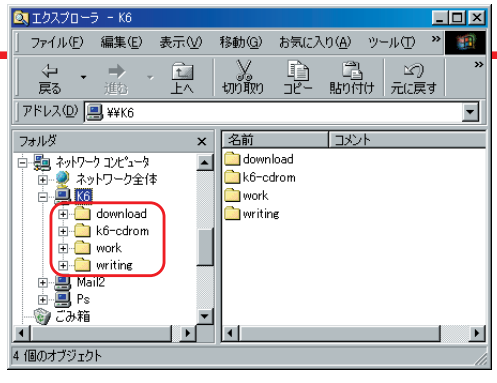
共有が設定されているフォルダー（手のマークが付く）の「プロパティ」を確認する。



書き込み権限を与えると危険が増すので、できれば「読み取り専用」で済ませよう。もちろん、パスワードは簡単に推測できない文字列を選ぶこと。

「ネットワークコンピュータ」から共有設定が確認できる

「ネットワークコンピュータ」に表示される自分自身のコンピュータを開く。ここに表示されているフォルダーには共有設定がなされているということだ。



共有ファイルにほかのコンピュータからアクセスして、共有の設定をチェックしておこう。ほかのコンピュータがなければ、共有を設定したコンピュータ自体で「エクスプローラ」を開いて「ネットワークコンピュータ」をクリックする。共有フォルダーの一覧が表示されるので、確認したうえで前述のように「マイコンピュータ」からフォルダーのプロパティーを確認する。

プライバシーが筒抜け！

ICQで個人情報を盗まれた!

常時接続で威力を発揮するのが、ICQなどのコミュニケーションツールだ。ICQを使えば相手がインターネットに接続しているかどうかがすぐにわかるし、オンラインの友人同士で連絡を取り合ったり、チャットやネットワークゲームを楽しんだりするときの連絡用にも便利。しかし、簡単な設定を誤るだけで、個人情報が流出する危険がある！

このとき何が起こったのか 原因と対策

ICQで友達とのコミュニケーションを楽しんでいるだけだったのに、変なメッセージが届き始めたり、ストーカーまがいの変なメールが届いたりした。そんな怪しい徴候が現れはじめたら要注意だ。ICQが原因で、あなたの個人情報が第三者に漏れてしまっているのかもしれない。とりわけ、女性ユーザーは電話番号や住所などを知られればさらに本格的なストーカー行為へとエスカレートする可能性だってある。

また、ICQでIPアドレスを調べて、前のページで解説したファイル共有の設定ミスを突いてファイルを削除するなどといったイタズラによる事件も報告されている。ICQがセキュリティー面でもプライバシー保護の観点からも弱点になってしまうのだ。

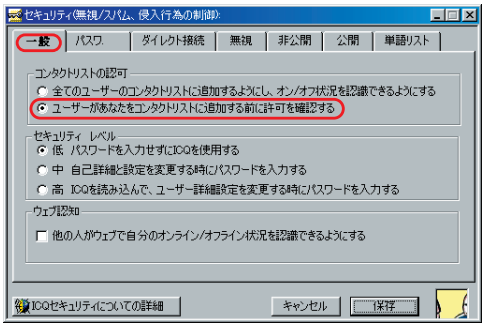
対策としては、ICQの設定を細かく見直すことが必要だ。まず設定に関するポリシーとして憶えてほしいのは「必要最低限の情報を除き個人情報は設定する必要がない」ということだ。ICQには個人情報を設定する義務はないし、電話番号や住所などを空欄にしても問題ない。友人との連絡でも、お互いの「ICQ#」さえわかれば不便はないのだからニックネームや偽名を使っても構わない。ただし、ICQを使っているときは、相手も偽名である可能性があることを忘れないこと。

ICQ（アイ・シー・キュー）：イスラエルのMirabilis社（現在AOL傘下）が開発したインスタントメッセージングソフト。自分のコンタクトリストに載っている相手がオンラインかどうかを調べ、オンラインなら短いメッセージやファイルの送受信ができる。

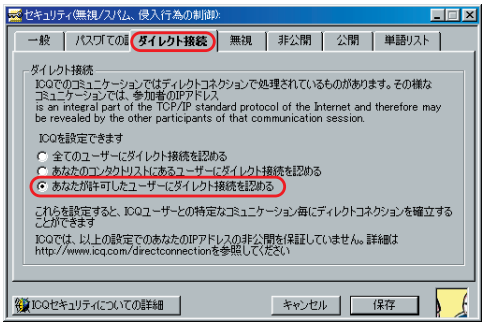
対処方法

アクセス権を設定しよう！

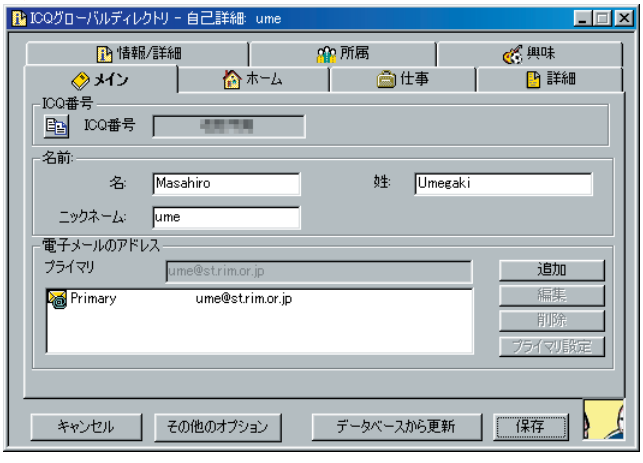
ICQのセキュリティー設定は、ICQメニューの「セキュリティー＆プライバシー」から行う。この設定では「一般」（右画面）と「ダイレクト接続」（右下画面）のタブがポイント。「コンタクトリストの許可」の設定で「ユーザーがあなたをコンタクトリストに追加する前に許可を確認する」を選んでおけば、あなたの許可がないと他人のコンタクトリストに勝手に登録されなくなる。



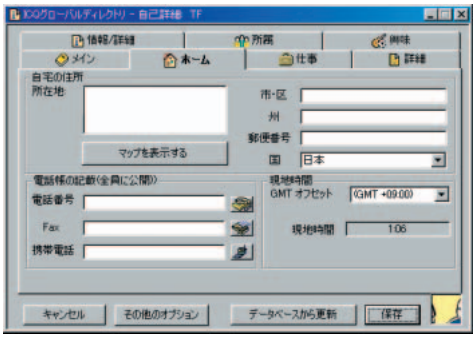
さらに「ダイレクト接続」タブをクリックして、その中で「あなたが許可したユーザーにダイレクト接続を認める」をチェックしておけば、許可したユーザー以外にあなたのPCのIPアドレスを知られることはない。



公開する情報を決めよう！



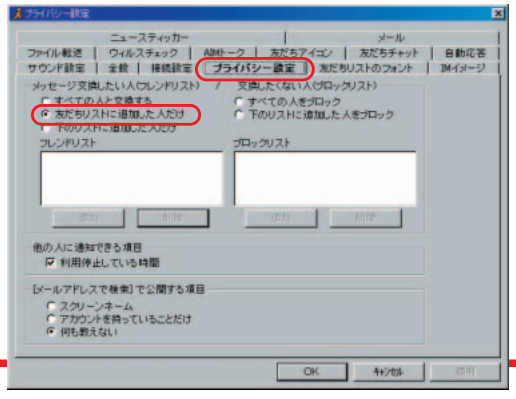
名前やメールアドレスを知られたくなければ正直に書く必要はない。プライバシー保護の観点から、ここでは設定を空欄にしておくほうが好ましい。見ず知らずの友達を見つけるツールとしてICQを使う場合も、最低限の情報だけを設定するようにしよう。とくに女性は注意して設定したい（右下は住所などを設定する画面）。



AOLメッセンジャーのプライバシー設定方法

ICQ以外のソフトを使うときも、原則として最低限の項目のみを設定するようにし、限られた人以外のメッセージを受け付けないようにしよう。AOL Instant Messengerの場合は「My AIM」メニューの「プロフィールの編集」で公開プロフィールを確認するとともに、「オプションの編集」メニューの「環境設定」→「プライバシー設定」でメッセージ交換する人を限定したほうがよい。

AOL Instant Messengerのプライバシー設定画面。



なぜかネットワークが使えない?!

DoS攻撃で操作不能にされた!

「あれ、なんか最近通信速度が遅いような気が…」。そう感じたら、DoS（Denial of Service、サービス停止）攻撃を疑う必要があるかもしれない。他人のコンピュータに不正なパケットを大量に送り込み、相手のネットワークを使えなくするのがDoS攻撃だ。個人ユーザーの常時接続環境ではDoS攻撃は一般的ではないが、比較的簡単にいたずらできることから、今後は嫌がらせや興味本位で実行する輩が間違いなく増加するだろう。

このとき何が起こったのか 原因と対策

注意深くネットワークの状態をウオッチしていないと、DoS攻撃を受けていても気が付かないのがこの問題の厄介なところだ。攻撃には、面白半分に攻撃ツールを実行したり、OSのセキュリティーホールを突いて侵入を試みたりするケースがある。特に後者では、DoS攻撃が侵入や攻撃、破壊などにつながっていくため、注意して対策する必要がある。OSのセキュリティーホールをねらわれた場合は、ハードディスクが急にフルになったり、OSがハングアップさせられたりするなど深刻な事態につながるため要注意だ。

この種の攻撃への対処のもっとも大事な点は、OSのセキュリティー対策だ。ウィンドウズなら「スタートメニュー」の「Windows Update」機能を使って常にセキュリティー対応のアップデートを行うようにし、メールソフトやブラウザーなどOS以外のアプリケーションも適宜アップグレードを行う必要がある。また、LinuxなどのUNIX系のOSで使われるネットワークツールやサーバーソフトは、セキュリティー上の問題点が広く知れわたるものだ。その情報をもとに攻撃専用のツールも作られるので、サーバーとして使っていないコンピュータでも十分に注意を払っておこう。また、非常に有効な対策の1つが、次ページで解説する「ルーターの導入」だ。

DoS攻撃（ディー・オー・エス攻撃）：DoSとは「Denial of Service」の略で、悪意を持つ何者かが第三者のコンピュータを利用して、標的にしたコンピュータに対して大量のパケットデータを一斉に送るもの。処理能力を上回る量のデータを受信したサーバーは、通常のサービスを行うことができなくなる。

対処方法

TAをルーターに替えればDoS攻撃も防げる！

サーバーをDoS攻撃から守るのはなかなか難しい。米国でヤフーなどが攻撃されてサーバーを使用不能にされていることなどは事件としても報道され、知っている人も多いだろう。だが、常時接続をウェブを見たりメールを読み書きしたりするだけに使っているコンピュータであれば、簡単に対処することができる。それは「NAT機能を持ったルーターを使うこと」だ。

NAT（Network Address Translation）とは、インターネットで使用する正式なグローバルIPアドレスを、家庭内LANなど内部ネットワーク用のローカルIPアドレスに変換してくれる機能ことだ。ローカルアドレスを持つコンピュータには外部からアクセスできないので、NATを使えば、外部からは（グローバルIPアドレスを持つ）ルーターまでしか侵入できなくなるわけだ。またTAやCATVモデムなどとコンピュータを直結している場合には、コンピュータにグローバルIPアドレスが割り振られてしまい、外部から見られてしまう。そんなときはルーターを使って家の中のコンピュータにローカルIPアドレスを振るようにすれば、外からはルーターまでしか見えなくなる。こうしてルーターをファイアーウォールの代わりに使うことができる仕組みだ。

グローバルアドレスを持つルーターは外部から見えるため、ルーターに対する攻撃は避けようがない。しかし、ローカルアドレスを持つ自分のコンピュータだけは確実に守れる。

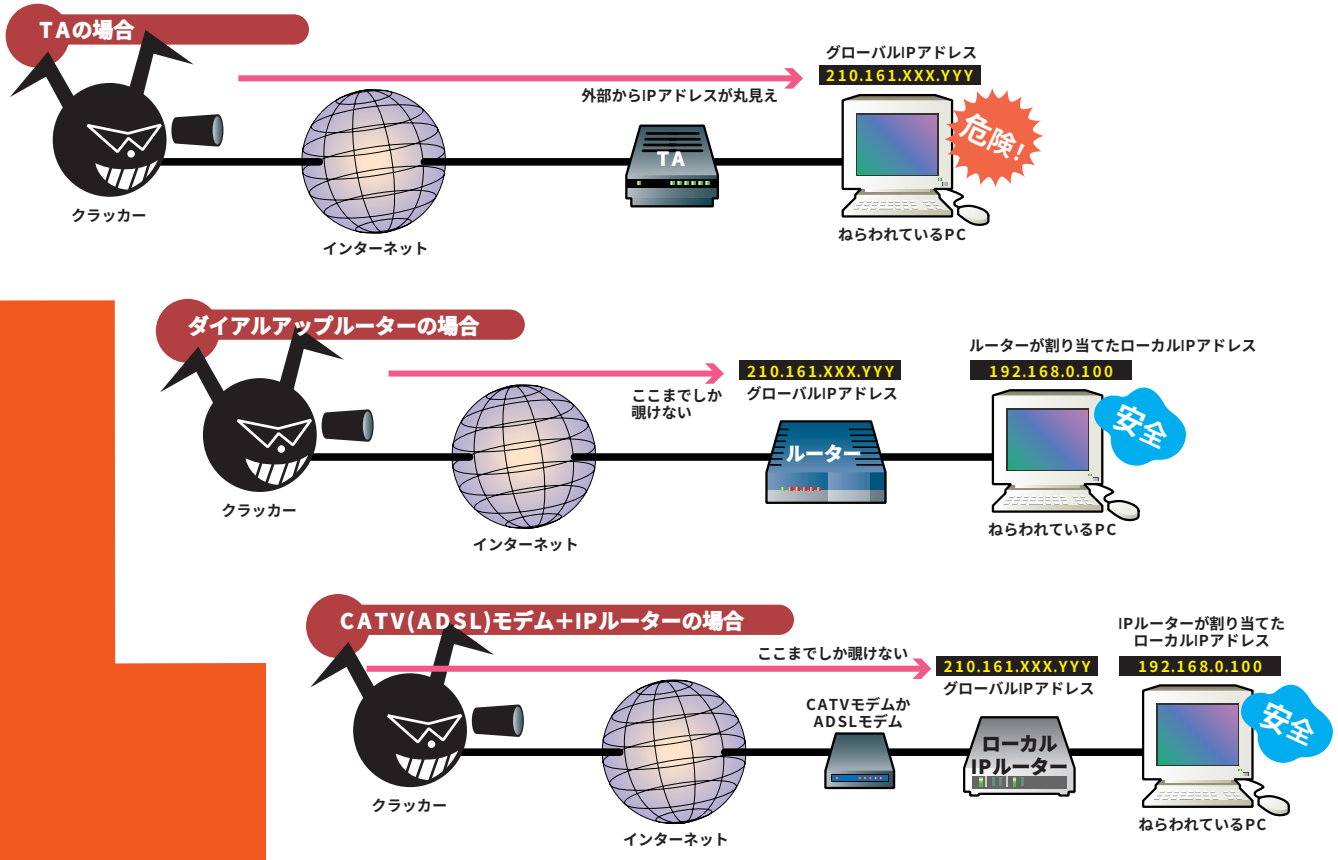
安価なIPルーターは絶対おすすめだ！

NetGenesis CAT（マイクロ総合研究所）

NetGenesis CAT は、常時接続環境向けのローカルIPルーターだ。パケットフィルタリングなども備え、低価格で安心して使える製品。CATVやADSLユーザーにおすすめだ。本誌301ページに製品のレビューを掲載（26,800円）。

	複数のPCで同時に使える	接続切断が完全自動化	セキュリティー	機器が安価
ルーター	○（ハブ付き）	○	○	△
TA	×	△	×	○

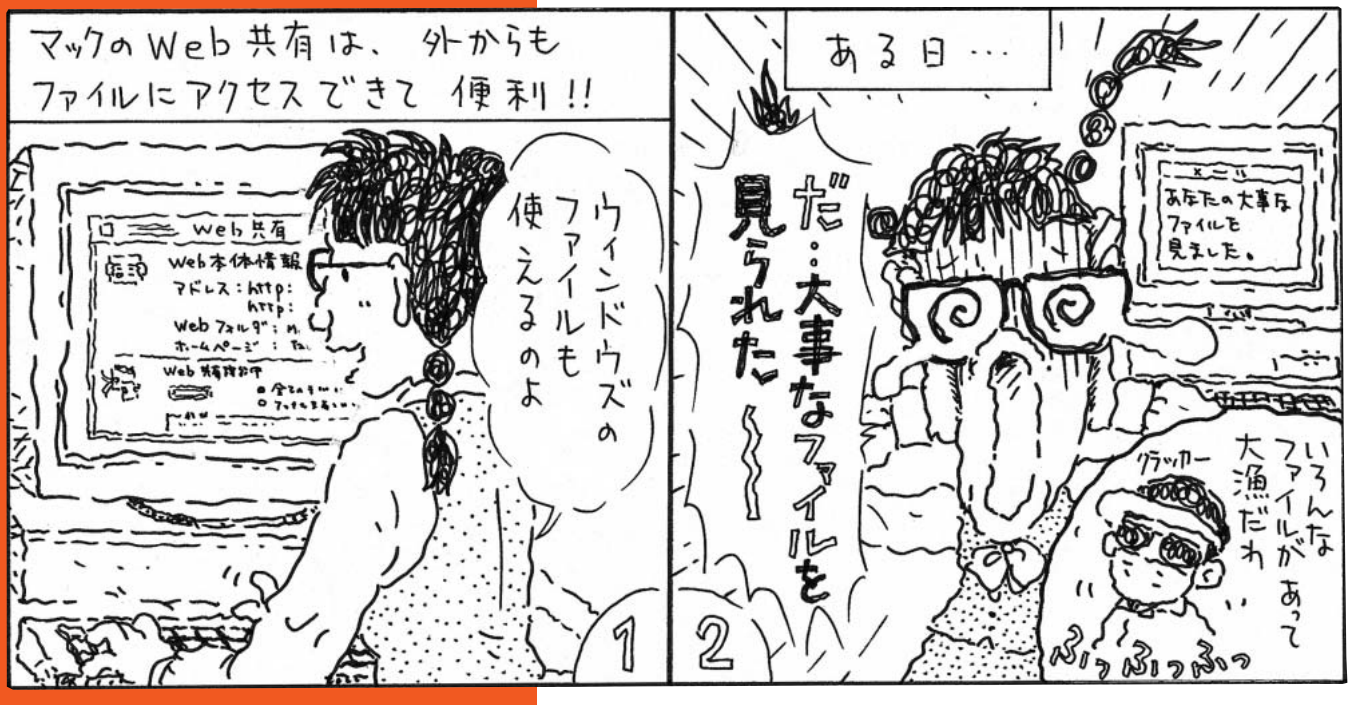
外部からはグローバルIPアドレスまでしか見えない！



大事なファイルが
盗み見された!

MacOSの「ウェブ共有」でファイルが丸見えに!

MacOSの「ウェブ共有」は、ウィンドウズマシンとも手軽にファイル共有できる便利な機能だ。だが、設定を誤ると世界中にファイルを公開することになってしまうぞ!



原因と対策

このとき何が起こったのか

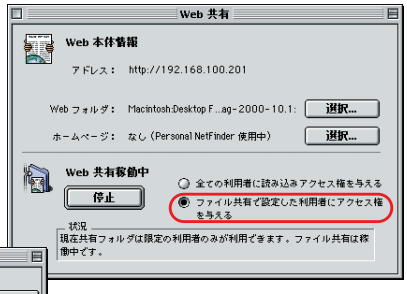
MacOSの「ウェブ共有」は、マッキントッシュのファイルをウィンドウズマシンとの間で共有できる便利な機能だ。しかし、ウィンドウズのファイル共有と同様に、使い方を誤るとファイルに誰でもアクセスできてしまう。ただしウィンドウズの場合と異なり、標準のウェブ共有ではファイルの削除や改ざんができないが、それでも大事なファイルを盗み見られる危険は残る。ウェブの仕組みを使った共有機能なので、不正にファイルにアクセスする側は、何の苦もなくファイルを盗み見ることができてしまうのだ。

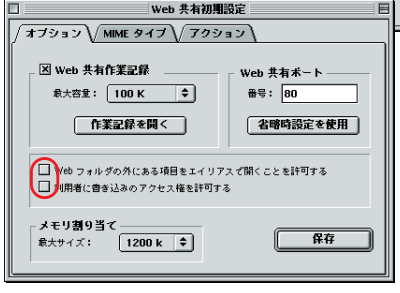
一番の対処方法は、ウェブ共有を使わないことだ。AppleTalkを使った通常のファイル共有だけでネットワークを組んだほうが安全だ。その場合もPC MACLAN Xjump などのソフトをウィンドウズ側で動かせば、ウィンドウズからもファイル共有機能を使うことができる。どうしてもウェブ共有が使いたければ、AppleTalkのファイル共有の設定を行い、ウェブ共有でもそのログインユーザー名とパスワードを使うように設定するといいだろう。

Xjump www.dit.co.jp/maclan/

対処方法

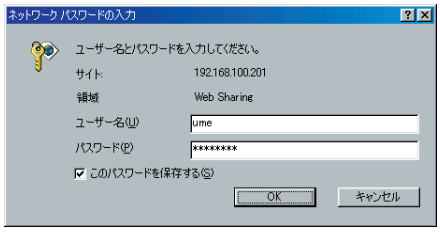
必ず「ファイル共有で設定した利用者にアクセス権を与える」を選ぶこと。すべての利用者にアクセス権を与える場合は、公開されたWWWサーバーとして運用するときだけと考えるべきだ。





Web共有のメニュー「編集」→「Web共有初期設定」で、「エイリアスで開く」や「書き込み権限」にチェックがないこと確認する。

ほかのコンピュータからブラウザーを使ってマッキントッシュのWeb共有を開こうとすると、ユーザー名とパスワードの入力ダイアログが表示される。



AppleTalk（アップルトーク）：米アップル・コンピュータ社が開発したネットワーク用のプロトコル群。

他人にマシンを勝手に使われた

Linuxマシンを踏み台にされた!

某有名企業から「警告」と称するメールが届いた。「あなたが当社のサーバーに不正侵入した形跡がある」との内容…。どうなってるの？　誰かに「踏み台」にされたのだ！

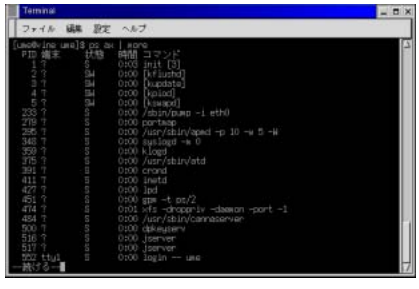
このとき何が起こったのか 原因と対策

常時接続環境でLinuxなどのUNIX系OSを使う場合、ウィンドウズ98やマッキントッシュなどのクライアント専用のOSよりも用心する必要がある。というのもUNIX系のOSでは、コンピュータに侵入されて正規のユーザーになりすましたり、rootパスワードをクラッキングしてコンピュータ全体の権限を掌握されたりする危険性があるからだ。自分のコンピュータが踏み台にされて、他のコンピュータへの攻撃の拠点になってしまうと、ネットワーク犯罪の一味と見なされることも考えられる。

このような事態を防ぐためには、自分のコンピュータでどのようなアプリケーションやサービスが動作しているかなどを細かくチェックして、セキュリティーを高める努力を怠らないようにしよう。サーバーとして使っていないコンピュータであっても、動作しているサービスや空いているポートを把握して、tcpwrapperなどのセキュリティーツールを用いて万全の監視体制を敷くべきだ。

対処方法 動作中のデーモンやサービスを把握する

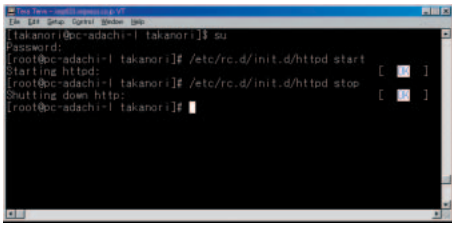
この例のように、コンソールでps axコマンドを実行し、動作中のすべてのデーモンをチェックする。もし、そのデーモンが何をするためのものかわからなければ、manページなどで調べておこう。



/etc/inetd.conf

```
#ftp     stream  tcp  nowait  root  /usr/sbin/tcpd  in.ftpd -l -a
#telnet  stream  tcp  nowait  root  /usr/sbin/tcpd  in.telnetd
```

/etc/inetd.confファイルを見ると、どんなポートが開いているかがわかる。不要なサービスが起動しないように、必要に応じてコメントアウトしておこう。特に、shell、login、ftpなどはねらわれやすいので、使わないならコメントアウトする。inetd.confを編集したら「kill -HUP inetdのPID」を実行すること。



Linuxでのサービスの起動と停止。rootになって右の画面のようにコマンドラインを実行すると、外部からでもサービスを起動したり停止したりできる（ここではhttpdを起動／停止させてみた）。

UNIX（ユニックス）：1969年に米AT＆Tベル研究所で開発されたマルチタスク、マルチユーザ使用のOS。特にインターネットに接続されている多くのサーバーでUNIXが使われており、UNIXを前提とした仕組みや作法がインターネットに色濃く反映されている。

ここまでやれば言うことなし！ セキュリティー設定TIPS その1〜6連発！

常時接続で知っておくべき設定と対策を紹介しよう。これらのTIPSを用いれば、常時接続の安全性がいっそう高まる。自分に関係するものは必ず実行するように心がけよう。

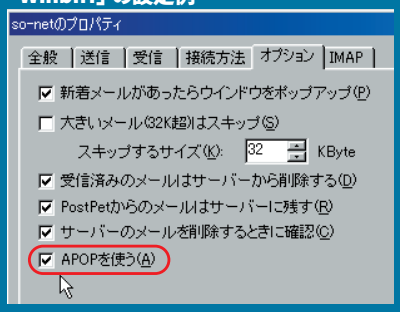
その1 メールのパスワードはAPOPで守れ!!

メールを受信するときに使われるPOPプロトコルには、実は危険な落とし穴がある。と言うのも、通常使われているPOPプロトコルではメールのパスワードを平文（暗号化されない文字列）で送信しているからだ。常時接続の環境では、異なるプロバイダーのメールサーバーにアクセスして送受信するケースが増えるだろう。通過するネットワークが増えるので、盗聴される危険性も増えてしまう。また、メール送受信の頻度も増すので、それだけ危険度は増すわけだ。こうした危険を回避するため、常時接続ではパスワードを暗号化して扱う「APOP」を利用するのがおすすめだ。メールソフトとプロバイダーがAPOPに対応している必要があるので、下の2つの表を参照されたい。

APOP対応の主なプロバイダー

@nifty	Jump www.nifty.com
PSインターネットサービス	Jump www.psn.ne.jp
So-net	Jump www.so-net.ne.jp
OCNダイヤルアクセス	Jump www.ocn.ne.jp

「Winbiff」の設定例



APOPに対応した主なメールソフト

ウィンドウズ	Becky! 1.21以降 AL-Mail32 1.01以降 Winbiff 2.05PL1以降 Eudora PRO 2.1.2J以降
マッキントッシュ	Eudora PRO 2.1.4-J以降 クラリスメール 1.1以降 Outlook Express 4.5/5.0

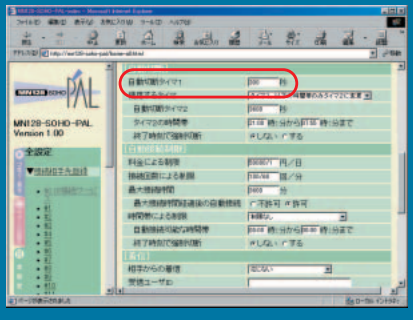
その2 telnetは危ない！sshを使え！

常時接続環境では、telnetを使うケースも増える。自宅でLinuxなどのUNIX系OSでサーバーを立ち上げている場合はもちろんだが、会社のサーバーに接続してちょっとした作業をするといったことも増えるはずで、そんなときtelnetは本当に便利だ。しかし、telnetではパスワードを含むすべての通信内容が平文で流れてしまう。そこで、暗号化機能を持つ「ssh」を使うようにしよう。ウィンドウズ環境では、定番telnetソフトの「TeraTerm」でsshアドインが利用できるし、マッキントッシュでは「NiftyTelnet」や「BetterTelnet」がsshに対応している。ただし日本語化されたBetterTelnetにはssh機能がないため、現状では日本語を通すのが難しい。

ssh対応ソフトと入手先URL

TeraTerm	Jump www.forest.impress.co.jp/library/terat.html
TTSSH	Jump www.zip.com.au/~roca/ttssh.html
BetterTelnet	Jump www.cstone.net/~rbraun/mac/telnet/
BetterTelnetJ	Jump www.netlaputa.ne.jp/~yoshida/
NiftyTelnet	Jump andrew2.andrew.cmu.edu/dist/niftytelnet.html

その3 常時接続でもマメに切断するべし！



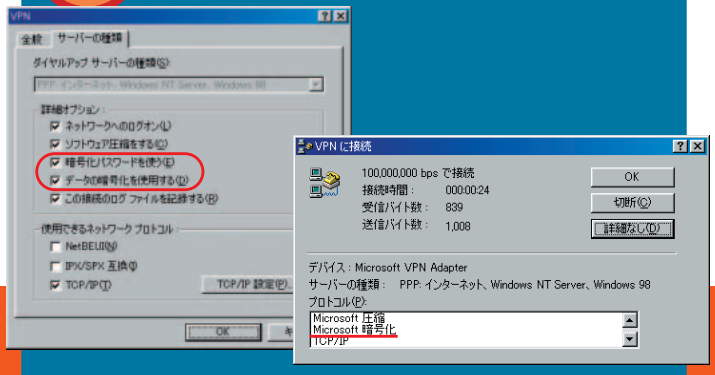
MN128 SOHO PALでは「接続先設定」で自動切断タイマーが使える。筆者は、5分間（300秒）何もなければ自動切断されるように設定した。

常時接続の記事で「切断」をすすめる逆説的なこの見出しは、皆さんを驚かせたかもしれない。通常、常時接続はつなぎっ放しがあたりまえだと考えがちだが、セキュリティー面で言えば「切断」こそが最善策であることに疑いの余地はない。

あなたのコンピュータにねらいが定められている場合は別だが、たいていのクラッカーはめったやたらと弱そうなところを探し回っている。そういう輩から見付けられないようにするためには、切断して息を潜めるのが有効な方法だ。フレッツならダイアルアップルーターを使って一定時間で回線を切断するように設定し、またCATVやADSLの場合も、使わないときはマメにコンピュータの電源を落としたり、レジュームしたりするようにしよう。

SSH（エス・エス・エイチ／Secure SHell）：ネットワーク上の通信内容を暗号化するプロトコル。通常のTELNETやFTPといったプロトコルでは、パスワードが暗号化されないままネットワーク上に流れてしまう、といった危険性がある。

その4 VPNの暗号化は忘れるな！



常時接続では、ダイアルアップと違って「接続先」が限定される。つまり、常時接続用に契約したプロバイダーだけに接続することになるということだ。これまでのように、会社に直接ダイアルアップしたり、いつもと違うプロバイダーにつないだりといったことは常時接続環境では難しくなる。

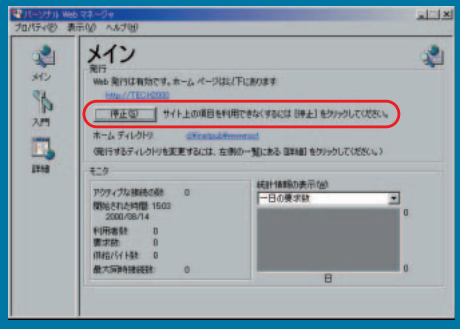
そんなときに便利なのがVPN（仮想プライベートネットワーク）だ。ウィンドウズにはPPTPを使ったVPNの機能があるので、プロバイダー経由でオフィスのコンピュータに接続できるようになる。当然、オフィスなどにある接続先のコンピュータがVPNサービスを使えるようにしておく必要がある。

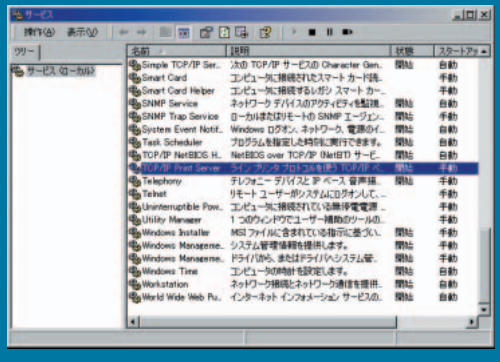
ここで気になるのがVPNの安全性だ。会社の業務にかかわる情報が流れるときなどは、とくに心配だ。ここでも盗聴やパスワードのクラッキングには十分な対策が必要だ。VPNを使うときはオプションをチェックして、必ず暗号化を有効にしておきたい。クライアント側のVPNの設定を怠ると、パスワードや通信の内容がそのまま平文で流れてしまうからだ！

その5 ウィンドウズNT/2000では不要なサービスを削除せよ！

ウィンドウズ2000をプレインストールしたマシンも増えたので、普段から使っている人も多いだろう。こんな人は注意しなければいけない。なぜなら、ウィンドウズ2000にはNTと同様にサーバー機能が盛り込まれているからだ。そのため、ここで気をつけたいのが使わない不要なサービスだ。WWWサーバーやftp、gopherなどの普通なら使わないサービスが動作していると危険は確実に増すのだ。

まずは普段から動作中のサービスをチェックして、使っていないものは「コントロールパネル」から削除しておこう。





その6 万全を期すなら、市販のファイアーウォールを導入すべし！

ビジネスなどの用途では、ルーターが持つパケットフィルターだけは機能的に不安が残る。やはり、JavaやActiveXを監視するなど豊富な機能を持ち、さまざまな攻撃から守ってくれる専用のファイアーウォールが安心だ。フレッツで利用するのなら、シスコのSOHO向けISDNルーター「CISCO 811/813」Jump01にファイアーウォールやVPNのオプションを導入する方法が安価でおすすめだ。これ1台だけで、ルーターとファイアーウォールの機能をすべてまかなえる。また、オールインワンの低価格ファイアーウォール製品も増えている。たとえば、SonicWALL SOHO/10 Jump02は導入時14万円、年間保守料24,000円で使える安価なファイアーウォールである。インストールも簡単なので、CATVやADSLで運用するSOHOクラスでセキュリティーを確保するにはピッタリの製品だ。

Jump01 www.cisco.com/jp/
Jump02 www.smisoft.ssd.co.jp/product/ss/

VPN（ブイ・ピー・エヌ／Virtual Private Network）：公衆網をあたかも専用網のように利用できるサービス。インターネット上で、認証や暗号化などのセキュリティー技術を使って、仮想のプライベートネットワークを作るもの。

セキュリティー対策ソフトで完全防御!

専用ソフトならここまでできる!

ここまでは、設定の変更などでセキュリティーが強化できる方法を紹介してきたが、最後にソフトウェアによる対策を紹介したい。セキュリティー対策専用の製品だけあって、その機能の充実ぶりには目を見張るものがある。ここではおすすめの製品をピックアップして紹介する。

おすすめ製品!

クレジットカード番号などの漏洩も防げる!

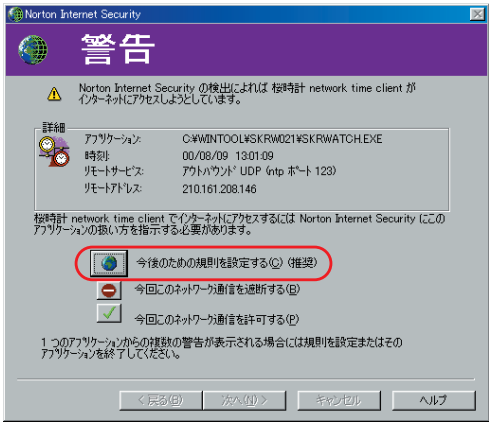
ノートン・インターネットセキュリティ

シマンテック(10月上旬発売)
標準価格　9,800円(消費税別)
動作環境　ウィンドウズ95/98/NTワークステーション4.0/2000プロフェッショナル
Jump www.symantec.com/region/jp/

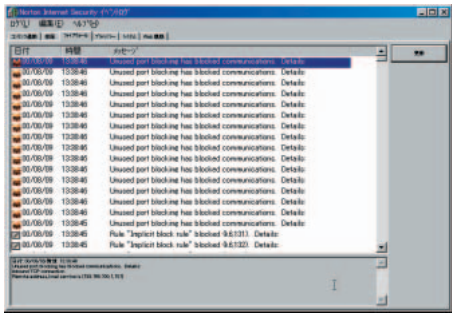
ここがスゴイ!

1 インストール直後からファイアーウォールが動き出す!

インストール後に再起動したら表示されたのが下の画面だ。見ると「桜時計」からのアクセスが遮断されたことがわかる。すでにファイアーウォール機能が動作し始めたのだ。これからも使うソフトの場合は、「今後のための規則を設定する」でアクセスの設定をしておこう。



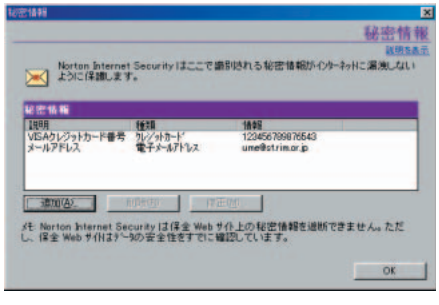
2 外部からのアクセスをすべて検出できる!



ほかのコンピュータからポートスキャン(接続ポートに1つずつアタックをかけていく攻撃)を行った。アクセスを受けたコンピュータには、画面のようなログが残される。バナー広告の遮断やウェブへのアクセス履歴なども、すべてこのログに記録されている!

3 「秘密情報」を設定すればプライバシー保護も万全!

クレジットカード番号などが外部に送信されないように、「秘密情報」でプライバシーの保護を設定しておこう。名前、電話番号、クレジットカード番号などを設定しておけば、それらの情報が送信される際に確認のダイアログが表示される。



4 バナー広告の遮断で不要なコンテンツは受信しない

「広告遮断機能」を使えば、バナー広告だけでなくActiveXやJavaアプレットを遮断することができる。インターネットへのアクセスをすべて監視しているので、不要なアクセスや怪しいプログラムもシャットアウトできる。

シマンテックの「ノートン・インターネットセキュリティ」(NIS) は、個人情報の漏洩を防ぐプライバシー保護機能、侵入や攻撃を防ぐファイアーウォール機能に従来の「ノートン・アンチウィルス」よるウイルス対策機能やバナー広告カット機能などを統合したセキュリティー対策ソフトだ。常時接続環境でグローバルIPアドレスを与えられたウィンドウズマシンには必須のセキュリティーが簡単に使えるソフトだと言える。

大きな特徴は、パーソナル向け製品としてプライバシー保護機能を充実させている点だ。あらかじめ登録しておいた名前や電話番号、クレジットカード番号などのプライバシー情報が、知らない間にインターネットに流されることを防げる。また、Cookieによるプライバシーの侵害も未然に防ぐことも可能だ。なお、ファイアーウォール機能だけを搭載した「ノートン・パーソナルファイアウォール」(標準価格:6,800円)もある。

おすすめ製品！

ウイルスバスター2001

トレンドマイクロ

標準価格　8,500円

動作環境　ウィンドウズ95/98/98SE/NTワークステーション4.0 SP5以上/2000プロフェッショナル（ウィンドウズMe対応予定）

Jump www.trendmicro.co.jp

「ウイルスバスター」の最新バージョンは、新たにパーソナルファイアーウォールなどのセキュリティー機能が搭載され、ウイルスばかりでなく、プライバシー保護やクラッキングへの対処までトータルにサポートできるソフトになった！

ここがスゴイ！

1 ウイルス検索とファイアーウォールが合体

メイン（アドバンストモード）画面がこれ。従来のウイルス検索機能とともに、今回からは非常に使いやすいパーソナルファイアーウォール機能が搭載された。

2 プライバシーの保護も設定次第で万全に！

パケットフィルター、Java、ActiveXなどをブロックするWebTrap、アクセスしたくないURLを登録するURLフィルターなどの機能を設定できる。

おすすめ製品！

BlackICE

東洋テクニカ

標準価格　6,500円

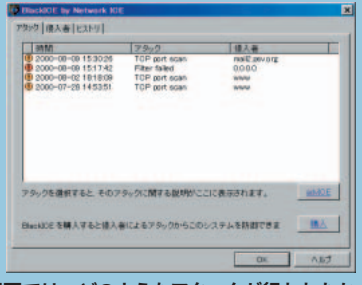
動作環境　ウィンドウズ95/98/NTワークステーション4.0/NTサーバー4.0

Jump www.toyo.co.jp
※試用版のダウンロード、オンライン購入が可能

「BlackICE defender」はウィンドウズへの不正侵入を検出して、防御するためのソフトウェアだ。このソフトを使えば、コンピュータに不正なアクセスがあったとき、どんな対処が必要かを教えてくれる。ちょっとマニアックなセキュリティーツールだ

ここがスゴイ！

1 アタックの履歴も逐一確認できる



この画面では、どのようなアタックが行われたかを確認できる。アタックへの対処は、「advICE」（アドバイス）ボタンを押すと表示される。

2 DoS攻撃も検出できるネットワークトラフィック

この「ヒストリ」画面を見れば、過去のネットワークのトラフィックやアタックの統計が表示され、危険性が示される。

最後に 常時接続時代の心構え

今回の記事では、「セキュリティーをキチンと確保しとかないと怖いぞ！」とあえて強調した。実社会では、誰でも出かけるとき、夜眠る前には玄関に鍵をかけるものだ。それと同じ習慣をインターネットでもやるべきだと言っているに過ぎない。確かに面倒くさいかもしれないが、今のところ、ここで説明した数々の対策を組み合わせるしか方法がないのだ。

もちろんコツはある。もっとも効果的なのはルーターを使うことだ。フレッツではISDNダイアルアップルーターを、CATVやADSLなどの場合はローカルIPルーターを使いNATで守られたプライベートネットワークを作るのだ。最低限のセキュリティーを確保するなら、パーソナルセキュリティー対策ツールが有効だ。「備えあれば憂いなし」、インターネットもこの言葉が金言なのだ。

［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