

## パソコンの便利な使い方 第24回

### 光ファイバについて

FTTH ( fiber to the home ) のような光ファイバを利用した通信サービスが身近になってきた。「光ファイバ」というと、銅線に電気信号を流してデータを送る通信よりも速いイメージがある。

光は1秒間に地球を7回半も回るスピードがあるからだろうか。いえいえ、ここでいう速いとは信号が伝わる速度ではなく、データを送る能力のこと。信号が伝わる速度だけを見れば、銅線と光ファイバの差はほとんどありません。しかし、光ファイバを使った通信回線は銅線より、同じ時間ではるかに大量のデータを送ることができる。

#### 減衰もノイズも関係ない

光ファイバの通信では、送信側で電気信号をレーザー光の点滅に置き換える。短時間に多くの情報を伝えるには、この点滅の回数を増やします。つまり、短い時間にどれだけ多く光をオン・オフさせられるかで、データ伝送速度は決まります。ここまでは銅線に電気信号を流してデータを送る場合でも同じです。

両者の違いは、光ファイバの方が点滅させるスピード(周波数)の上限がケタ適いに高いことです。これが光ファイバを使った通信を高速にできる最大の理由です。しかも通信用の光ファイバを使うと、レーザー光は、ほとんど減衰せずに数十 km の距離を伝わります。

銅線を使った通信では、こうは行きません。電気信号には、伝える周波数が高いほど減衰しやすくなる性質があるからです。別の言い方をすると、信号の周波数を高くすればするほど、長い距離を伝えられなくなります。通信距離と信号の周波数がトレードオフの関係になるのです。しかも光ファイバ通信は、途中で電磁波を受けても信号の波形が変化しません。要するにノイズにも強いのです。つまり光ファイバ通信は銅線に電気信号を流して使う通信より、高い周波数の信号を安定して長い距離を送れるわけです。

#### 光ファイバの能力はもっとすごい

このため長距離・大容量通信の世界では、光ファイバ以外は使われていません。大陸間を結ぶ海底ケーブルの通信などでは、1本の光ファイバで、ビットの1000倍にあたるTビット/秒クラスの通信が実用化されています。こうした通信の世界では、もはや銅線の出番はないのです。

銅線を使った通信の高速化は、技術的にほぼ限界に達しています。もうこれ以上、大幅に高速化される可能性はほとんどないのです。例えADSLサービスは1.5メガで始まり、8メガ、12メガ、24メガと高速化されてきました。しかし高速化の恩恵を受けられるのは、ごく限られたユーザーだけだという事実はよく知られています。電話局から数km以上離れると、どの仕様のADSLを使っても、実際の伝送速度はほとんど変わらなくなるのは、その速度が鋼の電話線で伝えられる理論的な限界値に近いからです。しかし光ファイバ通信は、まだまだ限界が見えない状況です。現行の技術は、光ファイバのポテンシャルをぜんぜん使い切っていないのです。

米国のベル研究所が2001年6月に公開した試算によると、理論的には光ファイバ通信で100Tビット/秒までは十分に可能だそうです。しかし現行の技術ではその10分の1の速度でさえも、実験室レベルなのです。ADSLが銅線(電話線)を使った通信の理論限界に迫る技術であることを考えると、現行の光ファイバ通信技術は、10数年前の1200ビット/秒のモデムのようなものと言えるかもしれません。

## パソコンの便利な使い方 第25回

総会で希望のあったウイルスについて数回に分けて掲載します。

### ウイルス対策入門

コンピューターウイルスって何？

「Bugbear (バグベアー)」「Klez (クレズ)」「Redlof (レッドロフ)」「Hybris (ハイブリス)」「Sobig (ソービグ)」「Blaster (プラスター)」 - 。これらが何の名前か分かるだろうか。いずれも2003年に大きな被害を引き起こしたコンピューターウイルスの名称である。

新しいウイルスは次々に生み出される。そのたびに被害が起こり、さまざまなメディアが注意を喚起する。合わせて、ウイルス対策の必要性を説く。それでも被害はなくなる。ウイルス作成者はそれを面白がり、また新種のウイルスが出現する。インターネットが普及して以降、この負の連鎖を断ち切れないうま、ここまで来た。

怖さを知るべし

そもそもウイルスとは何なのか。一言で表現すれば、「被害を起こすことを目的に、意図的に作られた悪意あるプログラム」である。悪意のプログラムは、挙動や特徴によって「ウイルス」「ワーム」「トロイの木馬」などと呼称を区別する場合もあるが、「ウイルス = 悪意のプログラム」と考えて間違いはない。では、ウイルス被害を避けるために何をしなければならないのか。第一歩はウイルスの怖さを知り、「対策は不可欠」と認識することである。数あるウイルスの一つひとつ理解する必要はない。ウイルスがこれまでに引き起こした主な被害を知るだけで十分である。例えば、「ハードディスクを破壊する」「システムを起動不能にす為」などの被害は、多くのユーザーが致命的と感じるはずである。仮に「パソコンが壊されても修理すればいいじゃないか」と考えていたとしても、他人から非難を浴びるのはいやなはずだ。他のシステムに無差別攻撃を仕掛けたり、ウイルスメールをばらまくウイルスは数多く存在する。このようなウイルスに感染すると、他人からの苦情が相次ぎ、謝罪を要求される可能性がある。最悪の場合、損害賠償を請求されることも考えられる。

プライバシーが漏れる

ウイルスがもたらす怖い被害例を もう1つ示そう。それは実名とともに、あなたのプライバシー情報やパソコン上での行動が白日のもとにさらされるかもしれないということだ。これは、ファイルを持ち出すウイルスに感染することで起こり得る。ウイルスが盗んだファイルが契約書や会社の書類だった場合、高い確率であなたの実名や会社名などがばれる。同時に、チャットやメッセージャーでの会話履歴などを持ち出されると、人に知られたくない日ごろの行動や友人との会話が実名とともに、だれかの手に渡る。つまり、ウイルスによってネット上の人物と実在の人物がマッチングされ、それが他人 - に知れ渡ってしまうのだ。加えて、このタイプのウイルスに感染すると、クレジットカード情報やユーザーID / パスワード情報を記録したファイルまで盗まれるかもしれない。この脅威は、2004年3月に流行した「Antinny」というウイルスによって再認識させられた。このウイルスはファイル交換ソフト「Winny」を使って感染を広げる。感染すると、Windowsのデスクトップ上のファイルや、パソコンに登録しているユーザー名 / 組織名などをアップロードフォルダー（他のWinnyユーザーがダウンロードできる場所）にコピーする。デスクトップ上に、チャットなどへの書き込み内容、パスワードやクレジット情報を書き留めたファイルを置いたままにしているユーザーは意外と多い。Antinnyが、ある男性のデスクトップ上にあった女性との“いけない会話”を持ち出したと一時話題になったのだ。加えて、Antinnyはファイル交換ソフトがウイルス

をまん延させる危険性も再認識させた。3月29日には、京都府警が捜査関係書類をインターネット上に流出したと発表。ファイル交換ソフト上のウイルスが原因の公算が高い。ウイルスはメールだけでなく、さまざまな経路からやって来ることも知っておきたい。

今、最も恐れられているウイルスは何か。それは、インターネットにつないだとたん感染するタイプのウイルスである。代表は2003年夏に猛威を振るったBlaster。Windowsのソフトウェア的な欠陥（セキュリティホール）を突いて感染を広げる。ラックの新井悠コンピュータセキュリティ研究所グループリーダーによると、「最もまん延していた時期、インターネット上でBlasterの攻撃を30秒に1回の割合で検知した」と言う。ウイルス自らがセキュリティホールを探して無差別攻撃を繰り返すため、感染速度が非常に速く、ネットワークに高い負荷がかかる。結果、各所で“渋滞”が起こり、インターネットが使い物にならなくなってしまう。特に、企業に及ぼす影響は大きい。Blasterのようなウイルスが社内に侵入すると、社内システムがすぐにパンクする。例えば、日本郵政公社は2003年夏、侵入した“一匹”のWelchi（ウェルチ）というBlasterに似たウイルスが原因で約4000台のパソコンが感染。数日間、システムの停止を余儀なくされた。このタイプのウイルスがまん延する原因はセキュリティホールの放置。ちょっとした油断が取り返しのつかない事態を引き起こすことを知ってほしい。いまやウイルスは、セキュリティホールを突くタイプが主流である。ネットにつなぐだけで感染するタイプのほかに、Webにアクセスしただけで感染するウイルスや、受け取ったメールを開かなくても感染するウイルスが存在する。Webアクセスで感染するウイルスは、2002年に出現したRedlof、2001年秋に猛威を振るったNimda（ニムダ）が有名。どちらもInternet Explorer（IE）が抱えるセキュリティホールを突く。セキュリティホールを抱えたままのIEを使って、ウイルスに侵されたWebサーバーをアクセスすると感染した。Redlofはスクリプトで書かれたウイルス。HTML形式のメール経由でも感染した。対して、Nimdaはサーバーとクライアントの区別なく、すべてのWindowsに感染。電子メール、共有フォルダー、バックドア経由など複数の感染経路を持ち、当時は「史上最悪のウイルス」と呼ばれた。相変わらず、メールで送られてくるウイルスは多い。メールに添付されるウイルスの場合、多くはユーザーが添付ファイルを実行しない限り感染しない。このため、ユーザーに添付ファイルを実行させる“だまし”のテクニックを盛り込んでいることがほとんどである。

クリックを誘う魅力的な件名や添付ファイル名にするのは当たり前。多くは、プログラムでありながら、テキストや画像ファイルに見せかける工夫も施している。なかには、マイクロソフトなどの有名企業を装って実行を促したり、セキュリティの警告メールを装うものもある。多くは英語メールだが、件名が日本語のウイルスも存在する。ここ2~3年で増えたのが、メールの送り主を偽るウイルス。ウイルスを送った本当のユーザーを特定できず、ウイルスに無防備なユーザーが“飼育”しているウイルスを駆除することが難しくなる。Klezや、2004年2月に出現したNetsky（ネツスカイ）などがこの機能を備える。感染したユーザーの保持するアドレス帳を取り出し、その中にあるアドレスから送ったメールであるかのように装う。

日経パソコンより

## パソコンの便利な使い方 第26回

### ウイルス対策入門第2回

ウイルスから身を守るために何をすべきなのか。遵守すべき対策は大きく3つある。

1つは、ウイルス対策ソフトを導入すること。これは基本中の基本。

2つめは、セキュリティホールをこまめにふさぐこと。最近の主流は、ホールを突き、感染を広

げるウイルス。対策ソフトをインストールしても、ウイルスを 100%の確率で防げるわけではない。最後の対策は、パソコンをインターネット上で「野ざらし」にしないこと。「野ざらし」とは、第三者がインターネット経由で簡単にアクセスできる状態を指す。インターネット上の機器に対して、無差別に攻撃を仕掛けるウイルスは数多い。野ざらしの状態だと、この無差別攻撃のえじきになる危険性がある。加えて「メールの添付ファイルを安易に開かない」という心がけも大切。メールに添付されるウイルスは相変わらず多い。上記の対策を講じても、少しでも怪しいと思える添付ファイルは開かない方がよい。

では、それぞれの対策方法について説明していこう。まずは対策ソフトの導入・活用について。現在、数多くの対策ソフトが販売されている。製品によって機能差はあるが、ウイルス検知に関してはどれも問題はない。指示通りにインストールすれば、パソコン上に常駐してウイルスを監視する。対策ソフトがパソコンにプリインストールされている場合は、パソコンに付属するマニュアルの「ウイルス対策」などの項目を読んで正しくセットアップしよう。

対策ソフトを利用するうえで注意すべき点は2つ。1つは定義ファイルを最新に保つこと。対策ソフトは、ウイルスに関する情報を記述した定義ファイルを使ってウイルスを検知する。新種のウイルスは次々に出現し、定義ファイルも毎週のように更新される。定義ファイルが古いと、対策ソフトを動かしていてもウイルスの侵入を見逃す危険性が高まってしまう。

一般に、定義ファイルは対策ソフトをインストールした際に最新のものに更新され、初期設定の状態でもその後も自動更新される。ただ、新種のウイルスが出現したときなどは、バージョンを手動で確認した方が無難。定義ファイルが自動更新されるまでに、新種のウイルスが侵入する危険性もある。

もう1つは、対策ソフトに有効期限が存在すると知っておくこと。対策ソフトの価格には、1~2年間の定義ファイルの更新料が含まれている。この期間を過ぎると、定義ファイルを更新できなくなり、新種のウイルスを検知できない。有効期限が近づくと、対策ソフトのほとんどがそれを知らせてくれる。

次のセキュリティホール対策に話を移す。これは WindowsUpdate をこまめに行うしかない。深刻なホールが発見された場合に、Windows 2000 や P が自動的に通知するメッセージを見逃さないほか、WindowsUpdate を定期的に手動実行する習慣を身に付けたい。

ホールを狙うウイルスの代表は 2003 年夏に猛威を振るった Blaster ( プラスター )。プラスターも、対策ソフトで検知・駆除できた。しかし、プラスターはインターネット上のパソコンに対して無差別攻撃を繰り返したため、ホールを抱えたままの Windows の場合、駆除しても次から次へとプラスターに感染した。

そもそも、プラスターのような感染能力の高いウイルスだと、定義ファイルが完成する前に広範囲にまん延する危険性が高い。定義ファイルは、新種のウイルスが確認されてから作られる。対策ソフトは、感染能力の高いウイルスに対して、どうしても無力化してしまうのだ。

多くの場合、ホールをふさいでおけば、ウイルスの無差別攻撃は防げる。しかし、システムをリカバリーしたことで、ふさいだはずのホールを再び開けてしまうことがある。未公開のホールを攻撃するウイルスが出現する可能性もある。

このために、パソコンを野ざらしにしない対策が必要になる。方法は大きく 2 つ。1つはルーターを設置して、パソコンにプライベートな IP アドレスを割り当てること。もう1つはパーソナルファイアウォールを使用することである。どちらの対策を採るかは、ユーザーの環境に合わせて決めればよい。

プライベートアドレスとは、企業内や家庭などの閉じた領域で使うアドレス。「10.0.0.0~

10.255.255.255」「172.16.0.0~172.31.255.255」「192.168.0.0~192.168.255.255」の範囲を指し、このアドレスのパソコンはインターネット上の機器と直接アクセスできない。インターネットとアクセスするにはルーターを介する。ADSL ユーザーなら、ADSL モデムとパソコンを直結するのではなく、間にルーターを挟み込む。そしてルーターが備える、インターネット用の IP アドレス（グローバルアドレス）とプライベートアドレスを変換する機能を有効にする。すると自分から始めた Web アクセスなどの通信は問題なく通るが、外部からパソコンに対する通信は届かない。これにより、ウイルスの無差別攻撃から逃れられる。

変換機能には「NAT (NetworkAddressTranslation)」と呼ばれるものや「NAPT (Network Address Port Translation)」がある。NAT はグローバルとプライベートアドレスを 1 対 1 で変換する機能。ネットに同時凍結する端末の台数だけグローバルアドレスが必要になる。対して、NAPT (IP マスカレードとも呼ぶ) は 1 個のグローバルアドレスで複数端末をカバーする仕組みである。

ノートパソコンが危ない

ただ、外出先ではルーターを介することが難しい。こういった場合は、パーソナルファイアウォールを利用する。パーソナルファイアウォールがウイルスの無差別攻撃を遮断してくれる。最近では、多くの対策ソフトがパーソナルファイアウォール機能を標準で備えている。対策ソフトをインストールすれば、パーソナルファイアウォール機能も自動的に有効になる。

パーソナルファイアウォール利用の注意点は 1 つ。複数台のパソコンをつないで LAN を構築している場合、パーソナルファイアウォールを使っていると、ファイルサーバー上の共有フォルダーやネットワーク上のプリンターにアクセスできなくなる可能性がある。パーソナルファイアウォールを正しく設定すれば問題を回避できるが、LAN ユーザーはルーターを用いる方が無難。LAN にもつなぐし、持ち運ぶこともあるノートパソコンは、外に持ち出すときだけパーソナルファイアウォールを有効にしたい。ここ 1~2 年、外出先でウイルスに感染し、それを持ち帰って被害を広げるケースが増えている。ノートパソコンのウイルス対策には十分に注意を払いたい。

(日経パソコンより)

## パソコンの便利な使い方 第 27 回

インターネットから資料を印刷する場合、右端が切れた場合の処理。(会員の方からの質問)

web ページの印刷で右端が切れてしまった場合は、以下の対策を順に試してください。

1. まず IE の「ファイルメニュー」から「ページ設定」で余白を減らす。
2. プリンタードライバーの「プロパティ」などで拡大・縮小を設定する。
3. 最後に、用紙を横にする手もある。

以上試してみてください。

## パソコンの便利な使い方 第 28 回

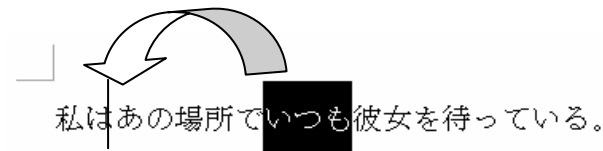
Word で文字を簡単に移動させる方法

Word で入力した文書の一部、あるいは文字列を移動させたい場合、

1. 文字列を選択して「切り取り」「貼り付け」を実行する方法。
2. 文字列を選択して、これをマウスでドラッグし目的の位置でドロップする方法。

しかし Word ならではの、もっと簡単な方法がある。それは、移動させたい文字列を選択した後、

目的の場所で「Ctrl」を押しながら右クリックする。これで文字列が移動できてしまう。

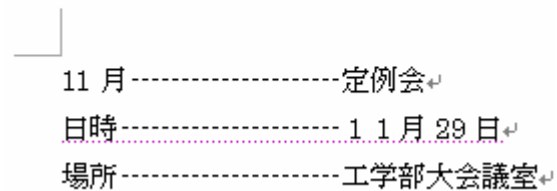
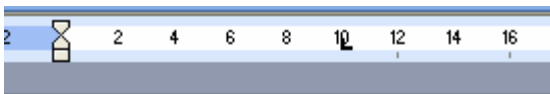


私はいつもあの場所で彼女を待っている。

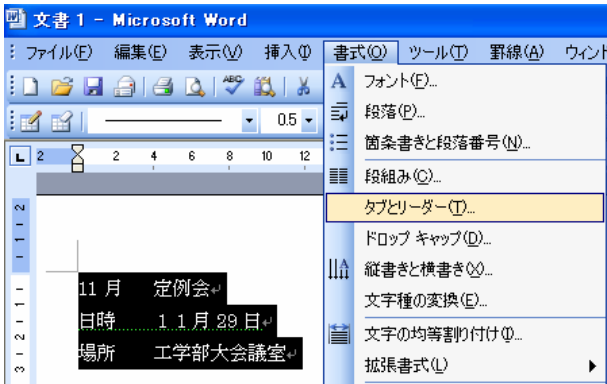
となって移動できている。

## パソコンの便利な使い方 第29回

項目間を伸縮自在の点線で



上図のように対応する項目を点線でつなくテクニック。

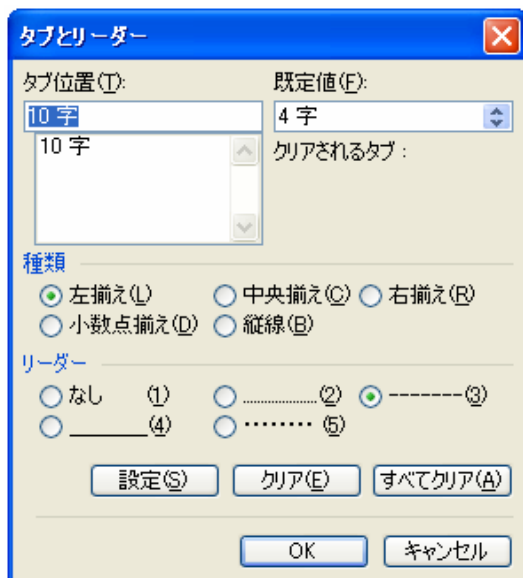


「11月」と入力したら「Tab」キーを1回押してスペースを空け、そのあとに「定例会」と入力する。同じように日時、場所の項目も入力する。

これらの項目を範囲指定して、「書式」メニューの「タブとリーダー」を選択。

二つ目の項目をそろえる位置を、10文字目にしたいのなら「10」と入力し、「種類」を左そろえにし、項目

をつなく線の種類を選ぶ。後は「設定」を押して「OK」を押せばいい。文字数が変わっても点線は伸縮して先頭がそろろう。



## パソコンの便利な使い方 第30回

「@」マークで文字を寝かせる

Word では、「@」マークを入力することで、文章中の一部の文字や記号を簡単に横に寝かせることができる。たとえば下図のように「転ぶ」という字を寝かせるには、通常通り入力してからこれを選択。「MS 明朝」などのフォントの種類が表示の前に、半角で「@」と入力すればいい。ちなみに下図の「」マークも@で「」を寝かせたもの。なお一字だけ寝かせたいときには「縦中横」機能を使っても同様の結果が得られる。

