2004-10-1

混沌とした中から

第5号
発行責任者　稲崎義明

ＩＴ情報社会の進歩の中で（４）

ではネットワークはどうなっているのでしょうか。この分野でも進歩は急激なものがあります。今から２４年位前に登場したのがパソコンで、それから２年ぐらい（自分でやっていなかったのではっきりした時期は適当ですが）して始まったのがパソコン通信です。そのころのサービスはメールであったり、掲示板であったりしましたが、通信回線は１２００ｂｐｓや２４００ｂｐｓのモデム接続で、電話の受話器に直接装置をつけて通信したりしたものです。それから１０年ほどして会社に入り始めたのがＬＡＮで、会社のパソコンがネットワークでつながり始め、一般にはインターネットが徐々に使われ始めました。そのインターネットも最初はモデムでの接続で、２４００ｂｐｓ程度であったものが、ＩＳＤＮ回線の利用により６４ｋｂｐｓとなり、アナログ回線も５４ｋｂｐｓとなって、ＡＤＳＬの登場で1M、10M、50Ｍｂｐｓ、最後に光ファイバーで１００Ｍｂｐｓとなっています。一方携帯電話やＰＨＳを利用したネットワークも通信速度アップと定額制が登場しています。そうしているうちに言葉ばかりが話題になっているのが「ユビキタス」です。

ユビキタスは、いつでもどこでもということで、ユビキタスコンピューティング、ユビキタスネットワークというと、いつでもどこでもネットワーク（インターネットだけでなく）に接続でき、必要（？）となったときに情報を入手できるということのようです。携帯電話でメールやインターネットに接続することを考えられるでしょうが、実際のユビキタスネットワークはもう少し違うもののようです。というのは、情報を受けるものは携帯やモバイルコンピュータには限らず、たとえば車であったり、今後登場するかもしれない電子化された機器が組み込まれていれば、鞄でもカードでもよくなるわけで、能動的にデータが必要になったときにデータを受け取るだけでなく、勝手に外部と通信して情報を入手するようになることも考えられます。便利といえば便利なのかもしれません。知らないところへ行ってもその土地の地図や情報がすでに手元にあるわけですから。知らないうちに自分の趣向に合わせた商品情報が送られてきたり、お買い得情報が送られてきたり。しかし、この場合自分の位置情報がどこかで入手されているわけです。ご存知のとおり、携帯電話は定期的に自分の位置を近くのアンテナと交信することによって携帯電話会社に知らせています。そのため通話していなくても電波を発信しているわけで、これがペースメーカなどに影響を与えているわけですが。携帯電話やユビキタス機器を持ち運ぶことによって、誰がどこにいるかが自分以外の誰かに知られてしまっているということになります。この究極が、人間の体にＩＣチップを埋め込んでしまおうとする動きですが。

ＩＴの発達によっていろいろ便利なことになってきています。しかし、この動きは技術者からの発想で進んでいってしまっています。こんな技術を使えばこんなに便利になる、そのためにもっと小さくしよう、こんなものを開発しよう、こんなにたくさんの情報が提供できるなど。誰も制限をかけなければ、便利だけを考えてしまえば大変な事になる可能性があります。法整備が遅れているのは他の分野も同じことですが、あまりに便利さの裏側についての記事がないのが気になるところです。変なたとえですが、世界大戦が終わってまだ６０年しかたっていません。世界中の国が善人で構成されているわけがありませんし、人々を先導しようとする人が出てこないとも、野望の持った人が出てこないとも考えられないのです。実際この世界は混沌としているように思います。　　（連載終了）

(今週の情報誌から)

○日経パソコン　９月２７日号

特集　ＳＰ２トラブル回避の虎の巻

→鳴り物入りで登場したＷｉｎｄｏｗｓＸＰのＳＰ２。セキュリティは強化されているが、Ｗｉｎｄｏｗｓが起動しなくなる場合や、アプリケーションが動かなくなったりする。簡単にＳＰ２が出たからといって簡単な気持ちでインストールしてはいけない。バックアップを取って、表示されるメッセージをよく読む必要もある。実際導入するにはもう少し上起用を確認したほうがいいようだ。

○日経システム構築　１０月号

特集　迷惑メールと戦う

→迷惑メールには特効薬がない。大量のメールが送られてきて、大事なメールが埋もれたり、サーバダウンにもつながることがある。国内ではそれほど問題となっていないが、米国では全メールの６５％以上を迷惑メールが占めている。一方日本は１日１通以上の迷惑メールを受け取るユーザは２４．５％と少ないが、２．４％のユーザは２０通以上のメールを受け取っている。対策の基本は、迷惑メールを判別するフィルタリングがある。他に方法としては、ブラックリスト、特定文字列の有無、シグネチャ（迷惑メールの本文をハッシュ化したシグネチャを作り受信したメールと比較する方法）、ヒューリスティック分析（メールを分析しスパムらしさのスコアを算出する方法）などがある。他にもあるが、．ｃｏｍドメインを持っている企業やメールアドレスがホームページに公開されている個人に多いが、地道な対策の積み上げが必要になる。

○Ｎ＋Ｉ　Ｎｅｔｗｏｒｋ　Ｇｕｉｄｅ　１１月号

特集　最新Ｐ２Ｐ　その仕組みと企業防衛策

→Ｐ２Ｐソフトはネットワークを使ったファイル交換ソフトで、企業セキュリティ管理者の知識やノウハウが少なく対策は決して十分とはいえない。知識としてＰ２Ｐソフトの利用実態と危険性を把握する必要がある。Ｐ２Ｐソフトとしては、問題になったＷｉｎｎｙから、Ｐｏｒｔ０、ＳｏｆｔＥｔｈｅｒ、ＨＴＴＰトンネルなどがあるが、ファイアウォールがあっても制限することができず、企業の機密情報がネット上に漏洩する場合もある。島、このＰ２Ｐの仕組みを知り、その対策を考える。

○ＮＥＴＷＯＲＫ　ＷＯＲＬＤ　１１月号

緊急企画　フィッシングに備えよ

→インターネット専用講座に不正アクセスの痕跡が姉などといったメールで偽のＨＰに誘導し、クレジットカード番号やＩＤ、パスワードを入力させるオンライン詐欺を「フィッシング」というが、日本に上陸し始めている。来たメールを無視するだけだと本当の重要なメールさえも無視してしまう。手口も巧妙となり対策に追われている。