

## セキュリティと暗号 (4)

無線LAN、スイッチングHUBに対する盗聴を説明してみましたが、今回はそれとは全く別の盗聴方法です。これまではネットワークを通過する情報を盗聴する方法でしたが、今度はパソコンなどの電子機器から漏れ出る電磁波を捉えて、その中にある情報を盗み出す方法です。この方法はTEMPESTと呼ばれる方法で、微弱な電波を受信して行うため相手に気づかれずに盗聴することがたできます。

まず、電子機器のどこから電磁波が漏れているかといえば、簡単に言えばいろいろなところから漏れています。電磁波は導体に電流が流れていれば発生するわけですから、例えば、本体とキーボードやマウス、ディスプレイなどの接続ケーブルはもちろんのこと、電源ケーブルや各種インタフェースのコネクタや本体自体からも漏れています。ディスプレイケーブルからの電磁波を解析すればパソコン画面を表示することができますし、キーボードケーブルからはキー入力されたデータを盗聴することができます。漏れ出す電磁波のうち再生しやすいのはシリアル伝送の信号で、LANケーブルやUSB機器への信号は盗聴再現しやすいものです。それに対して、プリンタとの接続などに使うパラレル信号は、同時に複数の信号を取り扱うために再生が難しいように思われますが、例えばプリンタの場合実際に打ち出すときなどは内部でシリアルに変更していることがあり、この部分で発生する電磁波を拾えば再生することができます。複数のパソコンがある場合でも、内部の周波数が小数点以下数桁のレベルで異なるため、微妙に調整することによって特定のパソコンのデータを再生することができます。

では実際にどのようにして盗聴するのでしょうか。パソコンから発生する電磁波を受信する方法は、アンテナを使うのが一般的で、指向性の高いアンテナを目的のパソコンに向けることによって建物の外からでも受信することができます。他にアンテナがなくても受信することができます。建物の梁や水道管など導電性の素材できているものから電磁波を拾うことができます。梁や水道管は建物の中に張り巡らされているため、建物内で発生した電磁波を受信・伝播します。また、部分的に建物の外に露出している部分にリード線をつなげば、簡単に電磁波を拾い出すことができます。

ただ、このような電磁波による盗聴については、ネットワークの盗聴に比べて敷居の高い方法のため安心できる面があります。盗聴するための機器が高価(数千万といわれる)であるため、よほど強い動機があり、資金が豊富でないとできない方法で、いたずら半分では手を出すことができません。また、もともとメーカーのパソコンはVCCIという団体があり、機器から漏洩する電磁波の許容値や測定法に関する規定値をクリアしています。買ったパソコンにハードディスクやオプションボードを増設することによって、この規定値を越えた電磁波が漏れ出す可能性が高くなります。さらに、電磁波が漏れるケーブルに対策をすることもあげられます。被覆材に電磁波を遮断する素材を使ったり、コネクタ部分にフィルム上のフィルタを使うなどの方法があります。

確かに電磁波による盗聴は、その費用がかかたりすることからあまり神経質になる必要はないのですが、電磁波対策は、パソコンから発生する電磁波で周辺機器やラジオなどの受信機に影響を与えないようにするものにもなることから、別の意味で対策することは必要です。特にビジネス用は漏れ出る電磁波は多くなっていることがありますから。

(次回へ続く)

(情報誌トピックス)

○日経エレクトロニクス 4月22日号

特集 もう、プリント基板じゃない

→ユビキタス時代に向かって、機器の小型化にはプリント基板の技術が欠かせない。基板は部品を取り込み、部品は回路を取り込んできて、部品と基板の境界線がぼやけてきているが、日本メーカーの強さはこの技術にある。

解説 「心臓部は買えばいい」それがケータイを戦国時代に

→携帯電話機分野で世界標準が登場しようとしている。携帯が高機能、多機能化することによって、CPUを搭載し、OSを搭載するようになってきている。これまで独自仕様が売りであったものが、標準ができることによって参入の障壁が低くなり、新規参入、新機能部品への参入が始まる。

○日経パソコン 4月29日号

特集 CD-Rの心得

→記録できるDVDが登場しても、最もユーザが利用しているのはCD-R。最近の動向から、データ記録、音楽CD作成、ハードディスクのバックアップなどCD-Rの使いこなし技術の再確認。

特集 調べる・予約する 特選Webサイト

→調べる、予約するときに便利なWebサイトはどこか。予約サイト、地図情報サイト、買い物情報サイトなど。

○日経バイト 5月号

特集 熱との格闘

→CPUが高性能になるにしたがって熱が問題となってきている。昔のCPUはよっぽど熱くなったとしても、ちょっと触れない程度であったが、今は放熱フィンが付き、ファンが付いている。サーバも含めて小型、薄型の要求に応えるため、熱との格闘が日々行われている。

特集 IEを捨てるという選択

→IEは絶対的なトップシェアを持っているが、数々のセキュリティホールが見つかり、ここにきてIE離れの動きが見られるようになってきている。対抗馬となる可能性のあるMozillaとOperaの実力を探る。

○日経ネットビジネス 4月25日号

特集 ビジネスの死命を制する「ネットの法」と向き合え

→ネットビジネスに関連する法整備が急ピッチで進んでいる。古物営業法、個人情報保護法、放送法など、トラブルを回避するために法の整備は必要だが、過度の法規制からビジネスを守るためにも法整備への積極的な関与が不可欠になってきている。

特集 迷惑メールに埋もれない方法

→携帯電話の電子メールビジネスで、マーケティングができなくなってきている。迷惑メールの中に埋もれさせない方法はあるか。ユーザにストレスを与えない方法は。

○N+I MAGAZINE 5月号

特集 広域Ethernetのメリットを拠点間ネットワークに活かせ！！

→LANレベルで発展してきたEthernetをWANの領域まで拡大し、WAN-LAN巻をシームレスにつなぎ利用できるようにしたものが広域イーサネット。広域イーサネットのメリットを正しく認識し、サービス選択のポイント、その信頼性を正しく認識する。

特集 技術者が必ず知っておくべきネットワーク法律知識と対処法

→ネットワークを構築する上で、知らなかったでは済まされない法律がいろいろある。その重要性を知り、ネットワークを構築する上で知らなければならない、法律のチェックポイントを知る。

○ASCII 5月号

特集 ブロードバンド速度ベスト100！ 無線LAN/ホットスポット完全ガイド

→どこのブロードバンドが速いのか。ADSL、CATV、FTTHのそれぞれでのベスト100を公開。一方、街中で無線LANの使えるホットスポットはどこにあるのか。使い心地はどうか。また、家庭での無線LANの使い心地は。

○DOS/V magazine 5月15日号

特集 FSB533MHz時代 パワーユーザの選択

→インテルはCPUとチップセット間のバスクロックを533MHzに引き上げたPentium4を出荷した。新たな時代ではあるが、チップセットからメモリの速度がまだ十分に速くなっているわけではなく、広帯域に対応して周辺チップの登場待ち。

特集 激速HDD快適テクニック

→現在のHDDの標準は、100MB/secのデータ転送能力を持つUltraATA/100。さらに高速な133も登場しているが、今HDDを選択(自作、増設などで)するための各種情報。

特集 “プロの目”で作るDV編集講座

→ビデオの編集をこれからしようとする人に、DV編集のコツを紹介。長続きしない人に対してもちょっとしたコツで再チャレンジを。