2002-4-15

H．P．Report

第46号

発行責任者　稲崎義明

セキュリティと暗号（3）

無線ＬＡＮはどうやっても盗聴されるものと思えと前回書きました。では有線ＬＡＮでスイッチングＨＵＢを入れたらどうでしょうか。

まずスイッチングＨＵＢですが。その前に、ＬＡＮに接続されるネットワーク機器にはＭＡＣアドレス(48ビット：24ビットはベンター固有、24ビットは連番)という固有のアドレスがつけられています。ＩＰアドレスは付け替えることができますが、ＭＡＣアドレスは固有で、接続された機器を識別することができます。では、ＨＵＢですが。これまでのＨＵＢはリピータＨＵＢと呼ばれ、1台のマシンからのパケットは、接続されたすべてのポートに転送出力されます。それに対してスイッチングＨＵＢは、ＨＵＢ内にＭＡＣアドレスの管理テーブルを持ち、1台のマシンからのパケットはどの機器のＭＡＣアドレスに対するものかを管理テーブルで判断し、その機器が接続されたポートにのみ、そのパケットを転送し、出力するようになっています。どのＭＡＣアドレスに対するものかの情報が管理テーブルにない場合は、すべてのポートにパケットを流し、それに対する返答を受け取ることによって、管理テーブルに新しいデータとして付け加えられます。つまり、スイッチングＨＵＢを利用すれば、送信側の機器と受信側の機器だけが結ばれることになり、他のマシンからは盗聴することができなくなっているはずです。

その前に、ＬＡＮによる通信の方法ですが。各端末はＡＲＰキャシュというＩＰアドレスとＭＡＣアドレスの対応表を参照しながら通信を行います。パケットを送る場合、その中に該当するものがあれば、そのＭＡＣアドレスに対して送りますし、もしなければ、ＡＲＰプロトコルを使って全端末に対してＭＡＣアドレスの問い合わせを行います。つまりＩＰアドレスを指定してこの端末のＭＡＣアドレスは何かというパケット(ＡＲＰ要求)を全端末に(ブロードキャストで)送信します。該当する端末は、ＭＡＣアドレスとＩＰアドレスのセットを、問い合わせ元に(ユニキャストで)送信し回答します。問い合わせ元は、受け取ったＭＡＣアドレスとＩＰアドレスのセットをＭＡＣアドレス対応表に登録し、送ろうとしていたパケットを送信します。このままでは盗聴できる状態ではありません。しかし、この対応表のＡＲＰキャシュは通信をしていなければ数十秒で消えてしまいます（何せキャシュですから）。

スイッチングＨＵＢをターゲットとした盗聴の方法の１つに、ＭｉＭというものがあります。ＡからＢへ通信しようとした場合、Ａからネットワークに対してＢのＭＡＣアドレスを見つけるためのＡＲＰ要求のパケットを出します。このとき盗聴しようとする端末Ｘは、本来返答しなければならない端末Ｂからの返答より先に自分のＭＡＣアドレスをＡに返します。するとＡのＡＲＰキャシュには、端末ＸのＭＡＣアドレスが登録されます。本来のＢからの回答はＸが受け取るため、その後の交信は、ＡからＸにまず入り、ＸからＢにあらためて送信されるため、本来交信しているＡとＢは気づかない内にデータが盗聴されることになります。この方法は同じスイッチングＨＵＢに接続されている必要はなく、同じサブネットであれば盗聴することができます。他にもスイッチングＨＵＢのＭＡＣ管理テーブルをあふれさせるなどいくつもの方法があります。

このようにスイッチングＨＵＢを使っていてもところが、それでも盗聴することができます。これらの方法は同じネットワークに盗聴する端末を設置する必要があるため、最大の対策は不審者の入室を制限することが上げられます。　　（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８日号
特集　ブロードバンドを塗り替える、それがＯＦＤＭ
→無線ＬＡＮ、ＤＳＬなど高速通信に使われているＯＦＤＭ(デジタル変調)。スタートはデジタル放送に使用するぐらいであったが、ユビキタスネットを実現するほとんどの通信手段として使用されている。次は移動体通信で、下りで100Ｍｂｐｓを目指す。

○日経パソコン　４月１５日号
特集　ＷｉｎｄｏｗｓＸＰの心得
→Ｗｉｎｄｏｗｓ２０００の高い安定性を引き継いだＷｉｎｄｏｗｓＸＰ。ハングアップでいらだつことは少なくなったが、見た目が大きく変わったため操作に戸惑う。こんなＸＰを使いこなすための心得３７個の紹介。
特集　ＰＣインターフェースの基本
→いろいろな端子(インターフェース)があるパソコン。以前はシリアルインターフェース、プリンタインターフェースなどが中心だったが、今はマルチメディア関連などいろいろある。使い方を知って戸惑わないように紹介。

○日経オープンシステム　４月号
特集　仕様変更に打ち勝つ
→開発期間短縮、アイデア取り込み、ビジネス変化への対応などそれでなくても決めることが難しい仕様に対して、「つくりながら決めたい」という要求が増えてきている。決めるべき仕様とそうでないものを見極め、変更を前提とした開発手法とはどのようなものか。

○日経ネットビジネス　４月１０日号
特集　集客アップ達人の決め手
→どのように集客するか。「知りたい」「欲しい」「安い」「楽しい」「お得だ」「人に教えよう」などの集客の「行動原理」。もっとも大事なのは客の心を知ること。達人のノウハウに迫る。
特集　ＢｔｏＣへの新トレンド“家族向けビジネス”に勝機あり
→子供のインターネット利用が増えている。ネットビジネス事業者は子供がいつでもどこでもインターネットを見ているという状況を前提にしなければならない。子供の存在を忘れていると大切なビジネスチャンスを逃す可能性がある。

○ＤＯＳ／Ｖｍａｇａｚｉｎｅ　５月１日号
特集　ＣＰＵアクセル全開
→ＣＰＵの性能とは何かをもう一度問い直す。性能を評価するものとしてのベンチマークについてもそのＯＳやアプリケーションソフトによって大きくその値は変化する。もう一度現在の最新ＣＰＵのアーキテクチャーの解説から始めて再評価する。
特集　比類なきＬｉｎｕｘデスクトップ環境
→ＬｉｎｕｘはサーバようＯＳ中心からデスクトップ環境へと進化を遂げている。ＧＵＩ環境から各種Ｏｆｆｉｃｅ互換やその他各種アプリケー

ションの紹介まで。付録ＣＤ－ＲＯＭにＬｉｎｕｘもあり、すぐに使える。

企画　ドきれいＭＰＥＧ－４録画

→オンラインで動画配信するためのものと考えられがちなＭＥＰＧ－４。しかし取り込み方によっては十分きれいな画像を取り込むことが出来る。どうすればきれいに画像が残せるか。