2002-4-1

H. P. Report

第45号

発行責任者 稲崎義明

セキュリティと暗号（2）

まず無線ＬＡＮのセキュリティについてです。セキュリティというより「無線ＬＡＮは盗聴されるものと思え」という内容です。前回も書きましたが、無線であるため有線と違ってどうしても漏れてしまいます。そのため盗聴する場合はパケット収集機をネットワークに物理的に接続する必要もなく、電波が屋外に届けば無線ＬＡＮの設置してある施設内に入る必要もありません。通信しているデータを収集するツールは既に有償／無償を問わず存在しています。例えば無線ＬＡＮのパケットを見ることで不具合の原因や不正な使用を突き止めようとするツールであっても、暗号化されていないパケットの場合メールのユーザＩＤ、パスワードやメールの本文まで見ることができます。これは暗号化されていない場合ですが、無線ＬＡＮが標準で備える暗号化機構ＷＥＰ(Wired Equivalent Privacy)であれば問題はないのでしょうか。ツールによっては鍵データを知れば復号化できますが、普通１０４ビットの鍵データを使っているため、２の１０４乗の組み合わせがあり鍵データを総当りで試すことは現実的ではありません。ここでＷＥＰの暗号化の仕組みですが、送信する前に次のような計算を行っています。まずＷＥＰには鍵データがあり、通信しあう端末とアクセスポイントには同じ鍵データが登録されています。この鍵データには４０ビットと１０４ビットがあり、この鍵データと暗号化するとき初期化ベクトル（ＩＶ：２４ビットのデータで送信するたびに作られる。このデータと鍵データを合わせて６４または１２８ビットとなる。）を連結して、米ＲＳＡ Ｄａｔａ Ｓｅｃｕｒｉｔｙ社の開発したＲＣ４と呼ばれる関数に代入され、ランダムな長いデータ列が作られます。このランダムなデータ列と送信しようとするメッセージデータ(実際のデータとチェックサム)との排他的論理輪（ＸＯＲ）をとったものが暗号化されたデータとなり、これに暗号鍵に連結されたＩＶを連結したものが実際に送信されています。受け取ったほうはどうするかといえば、データにはＩＶが付いて送られてきますので、このデータと鍵データをＲＣ４に代入することによって作られるランダムなデータと、送られてきたデータの排他的論理和をとることによって複合化することができます。このように作られたＷＥＰによる暗号化ですが、鍵データが分かれば復号することができるわけですから、鍵データを割り出したり、暗号化パケットを取り出すツールがインターネット上では無償で配布され、これを利用することによって数時間パケットを集めることによって解読することができてしまいます。実際どうやるかですが、パケットデータを収集することによって同じＩＶで暗号化したデータを集めることができます（ＩＶは毎回変わるといっても２４ビットですからそのうちに同じ物が出てきます）。同じＩＶの付いたデータの排他的論理和をとるとその結果は送られた元データの排他的論理輪になり、どちらかのデータの内容が判明すればもう一方も分かってしまいます。データの中には容易に推測することのできるデータもあるため、もう一方も分かってしまいます。また、盗聴しようとするほうがメールを送信し、そのときに使われたＩＶの付いたデータを待ち伏せる方法もあります。このようにＷＥＰの暗号だけでは安全と言い切ることはできません。無線ＬＡＮカードによってはＩＶを電源投入時にリセットし、パケットを送るたびに１ずつ増やすようなプログラムになっているものもありますし、そうでなくても５Ｍｂｐｓで通信を断続的に行うことによって半日でＩＶを使い切ってしまいます。そのため、無線ＬＡＮの規格を決めたＩＥＥＥでも現在暗号機構の強化をはかっています。

（次回へ続く）

(情報誌トピックス)

○日経エレクトロニクス　3月２５日号
　特集　アナログは怖くない
　　→デジタル化が進んでいる中、ネットワーク、マルチメディアなどもすべて外部とのインターフェースはアナログ信号で、アナログ回路は複雑かつ大規模になってきている。しかし、アナログ半導体技術の進歩が加速し、アナログ回路の複雑なノウハウはチップの中に入っていく。
　解説　ＩＰモビリティがケータイ網と無線ＬＡＮ網をシームレスに
　　→有線のＩＰネットワークと移動体通信の垣根がなくなるかもしれない。中核となるのがＩＰモビリティと呼ばれる技術で、携帯電話をＩＰ化し、無線ＬＡＮと接続することによって移動体通信は通信方式を意識することなく使えることになる。

○日経パソコン　４月１日号
　特集　パソコンの“心得”
　　→パソコンを使う上でデータの消失、機器やソフトの動作不良などの不具合も付き物。どうしてトラブルが発生するのか、どう回避・解決すればいいかなどのパソコンと付き合う“心得”は。

○日経バイト　４月号
　特集　知って得する先端技術用語２５
　　→コンピュータ業界は日進月歩で休むことなく新しい技術が生まれ、用語が生まれている。現時点の先端技術用語(スレッド・レベル・パラレリズム、波長ルーティングなど)を２５ピックアップして解説。
　ﾚﾎﾟｰﾄ　Ｙａｈｏｏ！ＢＢ網にセキュリティ上の大問題、他社網は大丈夫か
　　→同一局社内に接続された漏洩問題は解決したが、Ｙａｈｏｏ！ＢＢにはまだ問題が多い。Ｗｉｎｄｏｗｓでフォルダを共有設定にすると、他のパソコンからネットワークコンピュータを開くだけで見えてしまうなど。Ｙａｈｏｏ！ＢＢ側は解決策を提示せず、野放しになっている。

○日経ネットビジネス　３月２５日号
　特集　ブロードバンド対応サイト構築ノウハウ
　　→ネットワークがブロードバンドが中心となってきている。これまでのような６４ｋを前提としていたサイトが、ブロードバンドに対応したサイトになりつつある。読ませるより見せるサイトの構築方法を先進ユーザから学ぶ。
　ﾚﾎﾟｰﾄ　チャンスか、それとも無駄遣いか？「電子政府」が動き出す
　　→電子政府の推進基盤ｅ－Ｊａｐａｎ２００２プログラム。各省庁でいろいろな施策が盛り込まれているが、大きなメリットを生み出すが実際はどうなるか。

○Ｎ＋Ｉ　ＭＡＧＡＺＩＮＥ　４月号
　特集　階層化で改革する社内ネットワークシステム
　　→社内ネットワークをどう管理するか。管理安いネットワークする方法の１つが階層化管理。ＶＬＡＮを導入し、ネットワークの一元管理化と例や3スイッチによる統合管理を組み合わせた運用手法を解説。

特集　ネットワークストレージ徹底理解
→増加を続けるデジタル情報資産、業務の中核に浸透しているネットワーク。これまでのデータストレージ環境を変革するものとして注目されているのがネットワークストレージ。代表的なＮＡＳ(Ｎｅｔｗｏｒｋ　Ａｔｔａｃｈｅｄ　Ｓｔｏｒａｇｅ:ストレージをネットワーク経由で提供することに機能を特化したサーバ)／ＳＡＮ(Ｓｔｏｒａｇｅ　Ａｒｅａ　Ｎｅｔｗｏｒｋ：複数のサーバでストレージを共有するために構成されたストレージ専用ネットワーク)の特徴と次世代のテクノロジーを紹介。
特集　入門／ＩＰ－ＶＰＮ
→通信の安全を守るＶＰＮ、その仕組みから導入までを解説。

○ＡＳＣＩＩ　４月号
特集　ストレージ最新技術と製品選び
→ハードディスクの容量が１６０ＧＢを越え、２．５インチＨＤＤも５４００回転モデルが登場した。ストレージ関連でネットワークストレージから大容量光ディスクまでの最新情報。
特集　ブロードバンドルータを使い倒せ！
→ブロードバンドルータの仕組みと各製品の比較。使い方によってどのようなルータを選べばよいか。

○ＤＯＳ／Ｖｍａｇａｚｉｎｅ　４月１５日号
特集　悦楽のＰＣ自作全書
→自分だけの超プレミアムＰＣをつくるには。自作ＰＣの基礎から応用までの幅広い情報。