2002-3-15

H．P．Report

第44号

発行責任者　稲崎義明

セキュリティと暗号（1）

いろいろなものがネットワークに接続され、あらゆる情報がネットワークを通じてやり取りされています。普通に使っている上では気にもしないでいることが問題であるセキュリティと、情報を保護するために良く用いられる暗号について解説できればと思います。

まずセキュリティの必要性です。インターネットを利用しているといろいろなサイトがあり、商品の購入やものの売買などが良く行われています。また、銀行の口座振替や残高照会などが行え、いろいろな個人情報がネットワーク上を流れています。このようなサイトを利用する場合に良く用いられるのが、ユーザＩＤとパスワードです。しかし、世間にはいろいろなツールがあるもので、本来は試験用のものなので、ネットワーク上を流れるパケットを収集するというパケットキャプチャツールというものがフリーソフトでありますが、このソフトを使うとネットワーク上を流れるパケットをのぞき見ることができます。そうすると暗号化されていないユーザＩＤやパスワードを読み取ることができます。いわばネットワーク盗聴です。このようなネットワーク盗聴の脅威は、近頃の常時接続環境や無線ＬＡＮの普及と共に変化してきています。代表例としては、拡大を続けている「Ｙａｈｏｏ！ＢＢ」のＡＤＳＬサービスにおいておきたもので、ＡＤＳＬサービスは、サービス会社が利用者の電話回線が収納されている電話局にＡＤＳＬ接続用機器を設置する必要があるのですが、同じ電話局内に収納されたユーザ間で、他人のパケットを前期のようなツールを使って覗き見れたというのがありました。この場合は、ユーザＩＤやパスワードばかりでなく、メールの中身まで見れたようですが、現在は対応済みということです。また、無線ＬＡＮの利用についてですが、有線のＬＡＮと違ってどうしても無線は外に漏れてしまいます。近くへ無線ＬＡＮカードを装着したノートパソコンを持っていけば、暗号化されていないパケットであれば簡単にユーザＩＤやパスワードを盗むことができます。確かに無線ＬＡＮには、「ＷＥＰ」という規格化された暗号化機構を利用することができますが、どうしても通信速度が遅くなってしまうため利用しないユーザも多く、この場合でもセキュリティに対する考え方が問題になっています。また、特殊な盗聴として電磁波盗聴があります。これは、パソコンからもれ出る電磁波をキャッチして、そこからユーザＩＤとパスワードを盗み出そうとするもので、高精度な盗聴器が必要となりますが、今後大きな脅威となる可能性があります。いろいろな盗聴の方法がありますが、その前に必要なものがセキュリティに対する正しい知識となります。何気なく使えるものにどれほどのセキュリティが必要なのか。ネットワーク利用者がどれほどセキュリティが必要なものかを理解しているかです。暗号を使うと遅くなるから使わないなどは、閉ざされた小さなネットワークを利用するのであれば問題ないでしょうが、現代のネットワークはどのように接続されているかわかりません。自分の前にあるパソコンがインターネットを通じて世界につながっているという意識をもつことがまず重要です。セキュリティは関係ないと思っているようでは、どういった脅威にさらされるのかわからない今後では問題になります。知らないうちにユーザパスワードが盗まれ、３ヵ月後に請求書だけが送られてくるといったこともありえます。そのための基礎知識になればと考え、無線ＬＡＮの脅威や、簡単にできるセキュリティ対応機器の落とし穴から暗号化の仕組みなどについて解説できればと考えています。

（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１１日号

特集　ネット危機対策、まずは足元から

→携帯型情報機器(ＰＤＡ)やネットワーク家電などいろいろなものがネットワークに接続されるようになってきているが、個人に迫るネットの脅威に対して安心を売る時代になってきている。各社はセキュリティに走っている。

解説　産声をあげる無線の革命児「Ｕｌｔｒａ　Ｗｉｄｅｂａｎｄ」

→無線ＬＡＮが注目されているが、低消費電力で数百ｋｂｐｓの伝送速度をもつUWBで、これまでは軍事目的で利用されていた周波数帯を利用するもので、今後製品開発が進む。

○日経パソコン　３月１８日号

特集　自作パソコン徹底ガイド

→パーツの選び方からソフトウェアのインストールまでの自作パソコンの特集。

特集　デジカメ画像百年保存の心得

→カメラの主流になりそうなデジカメ。実際印刷したものはどのぐらい持つのか。ＣＤ-Ｒにした場合の保存方法のコツは。注意しないと持ちそうなＣＤ-Ｒも使えなくなってしまう。

○日経オープンシステム　３月号

特集　クライアント管理の３大課題を克服する

→今年６月にＷｉｎＮＴとＷｉｎ９８のプリインストール版の出荷が終わる。そのうちにサポートもなくなる。バージョンアップ、セキュリティ対策、ライセンス管理のクライアントを管理する場合の３大課題をどう克服するか。それぞれに分けてその方法を解説。

活用　広域ＬＡＮ

→イーサネットの技術を使って、遠隔地にある拠点間でＬＡＮと同じような通信のできるＷＡＮサービス。アクセス回線部とバックボーンの事業者が異なるため適切な監視や障害対策が必要だが、高価なＷＡＮ機器を必要としないため費用が押えられる。広域ＬＡＮは拠点から通信事業者のアクセスポイントに接続するだけで、サービス網に接続された全拠点と通信ができる。

○日経ネットビジネス　３月１０日号

特集　ネットでよみがえれ！日本の中小企業

→３分の１が消えるといわれる日本の中小企業の中で、ネットを利用して一品物へのすばやい対応、ネットで連結した仮想企業化など生き残る道を探している。

ﾚﾎﾟｰﾄ　「ホットスポット」がやってきた！！

→街角でインターネットにアクセスできるサービス「ホットスポット」が今春商用化が始まる。駅や喫茶店に無線ＬＡＮのアクセスポイントを設置し、そこでＰＤＡやパソコンを持っているとインターネットが使える。セキュリティや課金など課題もあるがＮＴＴコミュニケーションズは４月にもサービスを始める。

○ＤＯＳ／Ｖｍａｇａｚｉｎｅ　４月１日号

特集　ＧｅＦｏｒｃｅ４進化の証明

→新しいビデオチップＧｅＦｏｒｃｅ４が登場した。エントリーからハイスペックまでのファミリーは現在最高レベルにあるが、その内部テクノロジーやテストを通じて進化のポイントを探る。

特集　５４Ｍｂｐｓ高速ＬＡＮの実力

→現在の５倍の能力をもつＩＥＥＥ８０２．１１ａの規格。ようやく商品化が始まったが、多少高価なのが難ではあるが、スピードの魅力はいっぱい。現在の製品群を紹介。