2003-9-1

H．P．Report

第79号

発行責任者 稲崎義明

ハッキングの仕方（1）

これまで、セキュリティとか、暗号の特集などをやってきましたが、今回からの特集は、ハッキングの仕方です。ハッキングがこうだからこうセキュリティをするといった話ではなく、全くハッキングをするための特集です。とはいってもどうなるかはいつもの事ながらわからないのですが。

まずはハッキングの種類からです。

・セキュリティ破壊：サーバやパソコンネットワークを外部から覗けないようにファイアウォール等が設置されていますが、これらを破壊して機能しないようにする。

・セキュリティホールサーチ：必要に応じてファイアウォールに開けられた出入り口やプログラムの穴(セキュリティホール)をサーチして内部ネットワークへ侵入する。

・侵入：ファイアウォールなどを破壊してサーバやパソコンに入り込むこと。

・データ破壊：ハードディスクやリムーバブルディスクに記録されているデータの破壊行為。直接パソコンに侵入する場合もあるが、メールに破壊工作ウィルスを添付して送りつける場合もある。

・データ改竄：サーバやパソコンに侵入してデータを勝手に書き換えてしまう行為。ログオンするときのパスワードを書き換えて、持ち主がアクセスできなくすることもできる。

・データ窃盗：サーバやパソコンに侵入してデータを盗み出す行為。

・データ隠蔽：一見普通のデータのように見えるが、実は犯罪行為などの隠しデータが埋め込まれているなどの手法。例えば画像データに埋め込んで隠れてデータのやり取りを行ったりすることができる。

このようにいろいろなハッキングがありますが、インターネッ上にはいろいろなハッキングのソフトが存在します。また、もともとはデバッグ用だったり、システム保守用であったものがハッキングに使われたりしています。インターネット上にはハッキングのための情報交換するホームページもありますので、必要な情報をそのホームページから入手するのも方法であったりします。

ではまず簡単なハッキングの仕方から。それは、他人のパスワードのハッキングです。ＩＥなどには便利な仕組みがあって、１度入力したユーザＩＤやパスワードを記録しておいて（もちろん記録しないようにもできますが）次から同じページに炉群する場合にパスワードを入力しなくてもすむという便利な仕組みがあります。もちろん、画面表示は「＊＊＊＊」となって、見る事はできないようになってはいるのですが、それを簡単にもとのデータに表示を戻すものがあります。検索すれば簡単に出てくる「ＰａｓｓｗｏｒｄＢｏｍｂｅｒ」や「パスみえ２０００」というソフトがそれで、本当はパスワードを忘れてしまったときに重宝なソフトです。これは、例えば起動した「PasswordBomber」のウィンド内をドラッグして、表示されたパスワードなどの「＊＊＊＊」の部分にドロップするだけで元の表示に戻ってしまいます。仕組みとしては、データとしてはもちろんそのまま入っているパスワードのデータを、表示するときに隠し文字として「＊＊＊＊」として表示しているものを、ただデータの中から探し出して表示しているものです。これを使って他人のパスワードを見るときには、そのパソコン上で操作する必要があります。

（次回に続く）

(情報誌トピックス)

○日経エレクトロニクス　９月１日号
　特集　いまどきのＡＳＩＣは、こう選ぶ
　　→従来のセルベースのＡＳＩＣでは納期が長い上に開発コストが膨大にかかる。だからといってＦＰＧＡでは出来上がったチップ単価が高すぎる。そこで、両方の特徴の中間のマルチスライス方式のＡＳＩＣが注目されてきている。

○日経パソコン　９月１日号
　特集　知らなきゃ損する常識･上級ワザ１００
　　→不便だと思いながら我慢していることが簡単に解消されることがある。特に長く使っていると慣れから来る思い込みでこうした罠に陥りやすい。ＷｉｎｄｏｗｓからＯｕｔｌｏｏｋやＩＥ、Ｗｏｒｄ、Ｅｘｃｅｌなど「ワザ」を１００特集。
　特集　ｅ都市ランキング２００３
　　→毎年行われる情報化の都市ランキングの２００３年度版。ちなみに金沢は１２位、富山が９８位、福井１８６位。町村でトップに富山の福光町、２位に石川の野々市町がランキング。
　特集　仕事の効率が大幅アップ　職場環境改善計画
　　→４，５年前に導入したパソコン、プリンタと現行機種を比較したときの時間短縮、コスト削減の効果は。

○日経バイト　９月号
　特集　コピープロテクトかくあるべし
　　→音楽ＣＤを中心に進んでいるコピープロテクト。不正コピーに対抗する手段ではあるが、強すぎるコピーがユーザに反感をもたらすのも事実。理想のコピープロテクトとはどうあるべきか。
　特集　体感速度を測る
　　→ＣＰＵやメモリが速くなっているけれど実感はそうでもない。パソコンの速度はベンチマークテストで測るのが一般的だが、どこをどうすれば“速くなった”と感じることができるのか。

○日経システム構築　９月号
　特集　個人情報を守る
　　→個人情報漏洩事件が続く中、個人情報保護法が成立し、訴訟ともなれば１件あたりの賠償額は２億円を超える。企業にとって個人情報にどのように向かい合っていかなければならないか。セキュリティを強固なものとする一方、社員教育による意識改革が必要。
　特集　Ｊａｋａｒｔａソフトを使いこなす
　　→業務システムにおいて無償で利用できるＪａｋａｒｔａソフトの利用が広まってきている。サーブレットコンテナのＴｏｍｃａｔやフレームワークのＳｔｒｕｔｓなどは既にデファクトスタンダードともすえる状態になっている。各ソフトの使い粉とのポイントと利用上の注意点は。

○Ｎ＋ＩＮＥＴＷＯＲＫ　１０月号
　特集　インターネットＶＰＮ「要検討」マニュアル

→安価で、高速で、セキュリティを確保できるということで導入が進んでいる「インターネットＶＰＮ」。実際導入する場合に、導入、設計・計画、構築、運用の各段階で検討すべきことにはどういうものがあるか。絶対見落としてはいけないポイントとは。

特集　Ｓｎｏｒｔ２．０活用ガイド

→フリーかつオープンな侵入監視システムであるＳｎｏｒｔ２．０。使えるものなら使ってみたいシステム管理者向けに、概要から導入、シグネチャ作成、ログ解析、チューニングまでの活用法を解説。

○ＡＳＣＩＩ　９月号

特集　ネットワーク再入門

→パケットを中心に、その生成から伝送経路、加工、目的地まで届くところまでを解説し、ミクロ的なパケットとマクロ的なレイヤーを中心にネットワークを再確認する。

特集　オンラインソフトで悩みを解決

→国内サイトで入手できるフリーソフトを中心に、パソコンを使いやすくするためのツールを紹介。

○ＤＯＳ／Ｖｍａｇａｚｉｎｅ　９月１５日号

特集　そこが知りたい自作トラブルＱ＆Ａ

→自作マシンに新しいパーツを入れると落ち込みやすいトラブル。メインパーツから周辺機器、ネットワークに分けて解決する。