2003-11-15

H．P．Ｒｅｐｏｒｔ

第84号

発行責任者　稲崎義明

ハッキングの仕方（６）

今回は、IPを利用したハッキングのいろいろです。まず、IPですが、これまでのインターネットへの接続のように、電話線を接続してダイヤルアップでインターネットを使っていたのであれは、毎回違うIPアドレスがプロバイダから割り付けられるためあまり問題ではなかったのです。しかし、時代はブロードバンド、常時接続の時代です。IPアドレスは１度割り振られるとそのまま変わらないという状態になってきています。これがどれだけ危ないものか。そこで登場するのが「Back Oriffice」です。このソフトは、相手のIPアドレスを指定することによってパソコンが遠隔操作することができるようになります。使い方としては、「Back Oriffice」の遠隔操作が可能になるようにウィルスを進入させるところから始まります。このウィルスは、メールの添付ファイルで送り込めばすみます。ここで大事なのがIPアドレスですが、上にも書いたとおり、これまでのインターネットのように毎回IPが換わるのならば問題なかったのですが、常時接続というのはIPが変わりませんから、もしこのIPを知ることができれば、その後は相手に進入し放題ということになります。では、この大事なIPをどのように知るかということです。１つの方法として「ICQ」を利用する方法があります。ICQはインターネットコミュニケーションツールの１つで、オンラインのもの同士でリアルタイムにメッセージ交換することができるものです。ICQを使うときにはまずICQサーバに自分のIPを登録し、IDが発行されます。次からはICQサーバに接続することによってIDとIPを送信され、現在オンラインになったことが会員のパソコンに表示され、メッセージ交換することができるようになります。もちろんそれぞれのパソコンにはIDしか送られないのですが、ここで登場するのが「ICQ KILLER」と総称されるICQのIPをサーチするソフトです。ICQを利用してIPアドレスを調べることができればあとは進入し放題ということになります。

パソコンの玄関にはポートと呼ばれるいくつもの通り道があります。たとえばインターネットをする場合には８０番、メールは２５番がそのポートとなっています。通常その他のポートは閉じられていて侵入できないようになっているはずです。Back Orifficeの場合もメールで送り込んだウィルスがこのポートを内側から開けることによって進入できるようになります。で、まず相手のポートのどこのポートが開いているかを調べるものに「NMAP」があります。このNMAPはもともと管理者用のツールで、これを悪用しようとするわけですが、ただ、進入感知ソフトを入れておくと、アタックがありましたという具合に検知されます。

さて、Back Oriffeceに戻りますが、ターゲットに送り込むウィルスですが、通常EXEファイルが送り込まれ、間違って起動するとWindowsのシステムファイルを書き換え、誰でも侵入できるようにしてしまい、自分自身を消去するようになっています。つまり証拠隠滅です。こうなってしまったら、自覚症状が無いまま進入し放題状態となってしまいます。もし、これまで変なメールの添付EXEファイルを起動してしまって、でも何の変化も無かったってことがあれば、もしかしたら進入し放題の状態になっているかもしれません。Back Oriffeceで入ることができれば、あとはやり放題で、HDの中をのぞいたり、書き換えたりするばかりでなく、メールのログファイルを覗いたりすることもできます。しかも、もう最期だなと思えば、Windowsの大切なファイル、たとえばWin.comを破壊することによって、相手のパソコンを二度と起動できなくすることもできます。

（次回に続く）

(情報誌トピックス)

○日経エレクトロニクス　１１月１０日号

特集　実験室を出る燃料電池

→これまで各社で研究されてきた燃料電池がその普及に向けて動きが活発化してきている。さまざまなものから生成できる水素を原料に、水しか排出しない燃料電池は、小型化でパソコンに組み込まれたり、燃料電池自動車、家庭の電力供給など、現実のものになりつつあるが、オゾン層の可能性が出てきたり、まだ克服しなければならない項目は数多い。

解説　これからのクルマの性能はエレクトロニクスが決める

→第３７回東京モーターショーから。今回のショーで目立っていたものは、無線通信や生体認証船さ、走行や操舵を制御するエレクトロニクス、燃料電池車など。

○日経パソコン　１１月１０日号

特集　失敗の研究

→失敗は成功の元とは言うが、できれば失敗はしたくない。そこで、人様の失敗談を聞こうという特集。どんな失敗をしてどうしたら防げたのか。失敗の内容を見ると、簡単なことも多いが、なかなか対処できないものばかり。

特集　企業の情報化実態調査

→アンケートによる実態調査。ＯＳはＷｉｎＸｐへの以降は今後で、Ｏｆｆｉｃｅ２００３への関心は低い。パソコンの導入はリプレースが中心で、価格重視。セキュリティ対策は、中小企業での遅れが目立つ。ＶｏＩＰ電話の導入は１２％が導入で、通信コストの低減に効果あり。など。

○N＋ＩNETWORK　1月号

特集　セキュリティ指向、Ｗｅｂアプリ開発

→Ｗｅｂアプリケーションがビジネスツールとして普及しているが、セキュリティ意識に欠けているために問題も発生している。Ｗｅｂアプリケーションはなぜ脆弱なのかから、ＩＤ、パスワードによる構築のポイントと、開発工程へのセキュリティ指向の導入を解説。

特集　３つの視点で見るリモート管理のポイント

→ネットワークによる遠距離からのリモートによる管理／監視についての検討項目を「ネットワーク」、「セキュリティ」、「ストレージ」の３つに分けてその管理のポイントを解説。

○ＤＯＳ／Ｖｍａｇａｚｉｎｅ　１２月１日号

特集　最新Ｐ４チップセット実力ランキング

→ＦＢＳ８００MHｚに対応したＰｅｎｔｉｕｍ４向けチップセットにはＩｎｔｅｌの８７５Ｐ／８６５シリーズがあるが、ここにきてサードパーティからのチップセットの発表が続いている。それぞれのチップセットの実力は、そのランキングを解説。

特集　進化形ＯＳの解剖学

→家電的な使い方のできる「ＷｉｎｄｏｗｓＸＰＭｅｄｉａＣｅｎｔｅｒＥｄｉｔｉｏｎ２００４」、６４ｂｉｔＣＰＵ対応の「ＷｉｎｄｏｗｓＸＰ６４－ｂｉｔＦｏｒＥｘｔｅｎｄｅｄＳｙｓｔｅｍｓ」、次世代Ｏ

Ｓ「Ｌｏｎｇｈｏｒｎ」、Ｗｉｎｄｏｗｓに似たユーザインターフェースを持つ「Ｔｏｒｂｏｌｉｎｕｘ１０Ｄｅｓｋｔｏｐ」など各種の新ＯＳが登場している。最新ＯＳについて詳しく解説。