2003-12-1

H. P. Report

第85号

発行責任者 稲崎義明

ハッキングの仕方（7）

今回は、ＩＰアドレスがわからなくてもハッキングする方法からです。確かに、攻撃対象のＩＰアドレスがわかれば攻撃しやすいことは確かですが、別にＩＰアドレスがわからなくてもハッキングすることはできます。それは、攻撃対象の「コンピュータネーム」を使う方法です。コンピュータネームは、ネットワークの指定をする場合につける識別情報で、「コンピュータ名」、「ワークグループ」、「コンピュータの説明」と指定するあれです。あまり意識もしないで設定しているかもしれませんが、ネットワーク上で資源共有を行う場合などには、このコンピュータ名を使って指定することになっています。それとたちが悪いことに、ＩＰアドレスは、ダイヤルアップであれば接続するたびにアドレスが変わってしまいますが、コンピュータ名の場合、パソコンに固有の指定であるために、そう定期的に変更するものではありません。１度コンピュータ名を知られて、進入できるようになってしまえば、あとはそのままとうことになってしまいます。では、どうやってこのコンピュータ名を知るかということですが、ホームページでいろいろなことができるように、「ＣＧＩ」などでプログラムを組み込んであるページも多くあります。そのページにアクセスすれば、割と簡単に相手の「コンピュータ名」を知ることができます。ＣＧＩでプログラムを作ったことがある人であればわかると思うのですが、アクセスしてきたパソコンのアドレスは簡単に残すことができるのです。普通は、この機能を使ってアクセスログを残したりするために使う（誰がいつアクセスしてきたか、どのページを見ていったかなど）のですが、同じようにしてアクセスログを専門に残すこともできます。ホームページにアクセスする場合には、そのホームページの入り口へいって、「何とかホームページさん、私は、何とかというものですが、中を見せてください」といって入っているわけです。会社ではよくこの機能を使って、どこのパソコンがどこのホームページを見ているかといったアクセス記録をとっています。会社のパソコンであれば、プライバシーの問題にもなりません(ついでに、会社の場合、メールの中身をチェックすることもプライバシーの問題にはなりません)。確かに、ＩＰがアドレスで住所に該当するものであって、コンピュータ名が名前に該当するものですから、ＩＰのように世界でただ1つというわけには行かないので、そう簡単に「誰」ということを突き止められるわけではないのですが、プロバイダをめぐることなどによって、突き止めることはできます。

ついでに侵入した痕跡を消去する方法ですが、サーバがｕｎｉｘである場合、ｕｔｍｐ(現在ログインしているユーザの情報)、ｗｔｍｐ（ログイン履歴）、ｌａｓｔｌｏｇ(各ユーザの最終ログイン履歴)の３つのログファイルを削除します。これらは、ある程度ｕｎｉｘの知識が必要ですが、「ｚａｐ」という自動でログファイルを削除してくれるソフトもあります。このソフトは、「ｐａｃｋｅｔｓｔｏｒｍ」などのサイトにアクセスすることによって簡単に入手することができ、進入したサイトにあわせたものをｔｅｌｎｅｔなどで送り込み実行させることによって、簡単に痕跡を消し去ることができます。ＮＴＯＭａｘというサーバのバッファオーバフローをテストするもの、GFILANgauardNetworkSecurityScannerというサーバのセキュリティホールをチェックしてくれるもの、N-Stealthという高機能なHTTPスキャナーなどがあります。特にN-Stealthは、ファイアーウォールのセキュリティホールを見つけ出すこともできます。

（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２４日号
特集　ＨＤＴＶの次は究極のテレビ
→地上波デジタル放送の開始でハイビジョン放送が本格化するが、業界はその次に開発の主体は移っている。映像伝送を前提としない操作千２００００本の超高精細映像は、映画業界から２０１０年には家庭へやってくる。
解説　データ伝送に悪影響を与えず完全に電力を送る技術
「ＰｏｗｅｒｏｖｅｒＥｔｈｅｒｎｅｔ」の全貌
→1本のＥｔｈｅｒｎｅｔケーブルでデータと電力(４８Ｖ１５．４W)を送るための標準規格ＩＥＥＥ８０２．３ａｆが登場する。直流送電の安全に伴い、データ伝送に悪影響を及ぼさない工夫が必要となる。

○日経パソコン　１１月２４日号
特集　もしやまさかのウィルス対策
→ウィルスは会社のパソコンだけが感染するものではない。自覚無く家庭のパソコンでウィルスをばら撒いている感染者が後をたたない。「これって感染？」という問い合わせに回答し、感染しているかの判断実例から、感染したらどうするか、感染しないためのウィルス対策へと順に解説する。
特集　どっちがお得？
→買い物するとき、消耗品、通信費、電気代など、どっちがお得か迷ったときの判断を解説。

○日経バイト　１２月号
特集　Ｗｉｎｄｏｗｓセキュリティの深層
→８月に有名なウィルスである「Ｂｌａｓｔｅｒ」が登場した。これまでは、メールの添付ファイルをあけなければ大体は大丈夫ということであったのが、ネットワークにつないでいるだけで感染の危険があるなど新しいフェーズに突入した感がある。セキュリティ情報に気を配りながら、適宜ｕｐｄａｔｅを行いながらの生活が始まる。現在の状況を改めて確認し、今後の対応方法を探る。
LAB　ノートパソコンの総合性能
→カタログスペックや店頭ではわからないノートパソコンの発熱と騒音。この２つに注目してノートパソコンの性能を測る。

○日経システム構築　１２月号
特集　ＳＥ再生
→組織や体制の不備を原因の1つとしてＳＥの士気の低下が目に付く。開発期間の短縮とコスト削減がその流れに追い討ちをかけている。ＳＥの士気を向上させるにはどうすればいいか。今後のＳＥのあるべき姿を探る。
特集　ＩＰ電話は導入すべきか
→末端の電話機までをＩＰ化するＩＰ電話。どの企業でも導入すればコスト削減となるかは、その企業の電話の使用状況によっても異なる。これまで以上の品質と信頼性の確保も考えたうえで、思い切った工夫と思

いっきりが必要。

○ＡＳＣＩＩ　１２月号
特集　無線ＬＡＮまるわかり
→これからの無線ＬＡＮから基礎技術解説、構築・利用術の実例解説まで。５４Ｍｂｐｓの高速化や、弱いとされたセキュリティ強化策、対応アプリケーションまで。

○ＤＯＳ／Ｖｍａｇａｚｉｎｅ　１２月１５日号
特集　ＰＣパーツ大選考会
→この冬のボーナスで自作のために買いたいパーツを、ＣＰＵ、マザーボードなどに分けて総チェック。