2003-12-15

H．P．Report

第86号

発行責任者　稲崎義明

ハッキングの仕方（８）

今回まずは、Ｐｉｎｇによる攻撃です。Ｐｉｎｇはよくご存知のこととは思いますが、データの送受信の速度が測定できるもので、他のパソコンにテスト用のデータを送って、そのパソコンからどの程度の時間で戻ってくるかがｐｉｎｇの時間として測定されるものです。ではどうやって攻撃をするかですが、ｐｉｎｇの場合に送信するテストデータを普通なら数ｋＢのものに対して膨大なデータを送ってしまうのです。しかし、普通のｐｉｎｇを利用するとそのまま送り返されてしまうので、身元がばれてしまいます。それで使うツールが「ＳｉｎＦｌｏｏｄ」です。別に送受信の速度測定をするわけではないので、偽のアドレスを指定すると、攻撃されたほうは普通のｐｉｎｇと思い込んで一生懸命送り返そうとするわけです。

では、ちょっと違う方向から。今度は企業スパイのテクニックです。何がハッキングだと思われるかもしれませんが、このごろの企業スパイも何らかの方法によって社内のコンピュータに侵入しなければならないのです。必要なシステム情報を正規ユーザから得る方法をソーシャルエンジニアリングといますが、その前にまず、パスワードの保管場所について。ある調査で、代表的なものは目盛らずに記憶しているが６０％、パスワード用のメモ帳に記録しているが１３％、ＰＣの中に保管しているが９％、付箋紙などでディスプレイに貼り付けているが６％という結果があります。ではどうするかというと、まず何らかの作業員を装って会社内に入ります。従業員が少なければ見つかるでしょうが、よく工場から来客が有ったり、掃除や蛍光灯の交換、電気の点検などで入ってくる人についてはそれほど注意を配ったりしません。そこで、ディスプレイの付箋紙チェックしたり、パスワードを入力するときの動きを見てどこにメモが有るのかをみて、後から探したりしてパスワードを見つけます。後は、システムを管理している会社に企業側の管理責任者を装ったり、管理システム会社からシステムの以上のためにパスワードを一時的に同じ物に変えさせたりいろいろな方法がこれまでとられたりしています。また、ショルダーハッキングという方法があります。もちろん肩越しにパスワードを打ち込んでいる瞬間を覗き込んでみてしまう方法ですが、この場合、会社内というよりも大学などで他人のＩＤパスワードで相手の情報の改ざんに使われたりします。

企業スパイのテクニックとして、トラッシングという方法があります。とラッシュはゴミ箱で、ごみ箱荒らしのことです。ごみ箱にどのようなデータがあるのかと思われるかもしれませんが、実際ごみ箱のごみは誰の目にも触れず直接焼却ということは有りません（自分で焼却炉の中に投入するのでなければ）。トラッシングで利用される代表的なごみとしては、従業員の名前や名刺、パスワードに関するメモ、コンピュータやシステムの取扱説明書、明細書やレシートなど個人情報に関するもの、名簿や社員リスト、社員配置表、内線電話一覧などがあります。又、ＦＤやＨＤＤなども注意して捨てなければいろいろな情報が入っていたりします。簡単にミスコピーだからといって捨てたり、個数や金額が入っていないからといって見積もりの構成表をそのまま捨てたり裏紙やメモとして利用することは問題があります。

さて、大分ハッキングについて書いてきました。中にはそのままでハッキングしたり、他人のパソコンを使えなくするものも含まれたりします。しかし、実際のハッキングはもちろんこれ以上のもので、十分に注意し、対処しなければ大変なことになってしまいます。中途半端な気もしますが・・・　　（連載終了）

(情報誌トピックス)

○日経エレクトロニクス　１２月８日号

特集　蓄電革命

→これまでの２次電池は、充電するのにある程度時間が必要で、３００回程度という寿命もあったが、この常識を覆す蓄電技術がまもなく登場する。それは大容量キャパシタ。つまりコンデンサ。これまで瞬間的な電源供給は可能だったものがＮｉ水素２次電池程度のエネルギー密度を持ち、機器に組み込まれれば、瞬間(１分程度)充電が可能で、充電回数も数万回以上と無限に近い。

解説　モバイル機器をテレビに　小型パネルも美しさを競う

→モバイル機器の画面も、これまで表示できればよかったものがＡＶ機能への対応で、ＦＳ方式、液晶、有機ＥＬなど美しさの映像表示能力を競っている。

○日経パソコン　１２月８／２２日号

特集　気になるオールインワン機器のうまみを探る

→カラーコピーができるインクジェット複合機、ＤＶカメラなみの画質で動画が取れる「動画デジカメ」、すべてのメディアに読み書きできる「全規格対応ＤＶＤドライブ」などいろいろあるオールインワン機器。これまでは中途半端と見られていたこれらのものも十分な機能を持っている。現状はどうか。

特集　出先の「情報遮断」克服計画

→職場から出るとメールやネットが一切使えない「情報遮断」環境。安価に取り組める携帯活用術から、パソコンによる出先でのネット接続までを紹介。

○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　１月１日号

特集　頑固者のこだわり自作　五輪書

→自作ＰＣのこだわりについて、高性能ＰＣ、完全水冷ＰＣ、ゲーム専用小型ＰＣ、超小型ＰＣ、ちょっとこだわったＰＣに分けてその内容を説明。

特集　電源選びの黄金律

→パソコンの電源をどう選べばよいのか。あまり気にしなかった電源について、正しい選び方から実機の騒音レベルと電気特性の評価を行い、電源を見直してみる。

特集　快楽マウス大全

→いまどきのマウスは、安いものから高いものまでいろいろある。流行のワイヤレスマウス、わいヤードマウス、オプティカルマウスにモバイル用マウスなど。形も超小型からエルゴノミクスデザインのものまで。どれがいいのか、実際使って見なけりゃやっぱりわからない？