コンピュータセキュリティー

藤田和弘*

医用画像情報学会 平成 11 年度春季 (第 126 回) 大会 特別講演
2000 年 2 月 5 日
京都工芸繊維大学

Abstract

不正アクセスやウィルスなどを対象とした狭い意味でのコンピュータセキュリティーではなく、コンピュータが安心して使える状態とはいう観点から、経験などを交えながら、コンピュータセキュリティーについて、考察を行なった。また、不正アクセス禁止法や、セキュリティー関係の情報収集にもふれた。

1 まえがき

ここでは、コンピュータセキュリティーについて考えてみたいと思います。一般に、コンピュータセキュリティーというと、

- 悪意のある人によるアタック
- コンピュータウィルスやワーム

などを連想しますが、ここでは、もう少し広く、コンピュータセキュリティーについて考えてみたいと思います。

私は、特別、コンピュータセキュリティーの専門家ではありませんが、学科の教育用計算機システムの管理者として、少なからず、いろいろな問題に直面してきましたので、その経験を述べたいと思います。また、システム管理者のセキュリティー講座やアタッカー養成講座ではないので、スタックオーバーフローによるセキュリティー上の問題、ICMP Amplifier などのテクニカルな問題は、今回は、省略しました。

2 セキュリティーの高いコンピュータとは

ホームセキュリティーという言葉がありますが、某社の宣伝によると、窓やドアなどからの侵入だけでなく、ガス洩れや火災などについても、警報が鳴り、担当者が駆けつけてくれるようです。この場合のホームセキュリティーというのは、安心して住める家としてのセキュリティーということになると思います。

では、セキュリティーとは何でしょうか。Longman Dictionary of Contemoprary English で、security を引くと、一番目に “the state of being secure”、二番目に “protection against lawbreaking, violence, enemy acts, escape from prison, etc.” となっています。つづいて、secure を引くと、一番目に “safe; protected against danger or risk” とあります。日本語で “セキュリティー” というと、二番目の意味が強いように思いますが、実際は、一番目の意味、つまり “安全” や “安心” という意味が重要であると思います。

そこで、ここではセキュリティーとは、“安心な状態” と考えます。また、セキュリティーの高いコンピュータとは、“安心して使えるコンピュータ” と考えます。つぎに、 “安心して使えるコンピュータ” とは何でしょうかということになります。何も問題がなければ、安心して使えると考えると、安心して使えない理由、障害となるものがあり、それにより、 “安心して使えないコンピュータ” になると考えることができます。以下の章では、その障害となるものについて、見ていくことにします。

3 障害となるもの

コンピュータを安心して使えない、障害となるものには、いろいろなものが考えられます。一番先に思いつくのが、悪意のある人によるアタックですが、ここで、よく考えなくてはいけないのは、本当にそれだけでしょうかということです。まえがきで、ホームセキュリティーのことを書きましたが、窓やドアからの侵入だけでなくガス洩れや火災などにも対応したホームセキュリティーサービスがあります。コンピュータについても、アタック以外のことも考える必要があります。例えば、障害となるものとして、

- 悪意のある人によるアタック

*京都工芸繊維大学工芸学部電子情報工学科 〒 606-8585 京都市左京区松ヶ崎御所街道町 Tel(075)724-7497 Fax(075)724-7400 E-mail: fujita@dj.kit.ac.jp HomePage: http://image.dj.kit.ac.jp/ ~ fujita/

- 悪意のない人による悪影響
- ハードウェア障害
- コンピュータウィルス
- ソフトウェア障害
- 劣悪なコンピュータ環境
- 対外的な信用低下

などがあります。

以下、それぞれについて見ていくことにします。

3.1 悪意のある人によるアタック

悪意をもって、自分のコンピュータ以外のコンピュータにアタックをかける人は、かなりいるようです。狭い意味でのコンピュータセキュリティーは、このような人達から、コンピュータを守ることです。アタックをかける人といっても、愉快犯のように、アタックをかけて楽しんでいるだけという人もいるようです。

最近では、ポートスキャンを行なって、よそのネットワークのコンピュータの弱点を探し回る人が、かなりいます。私が管理する研究室のメイルサーバや、学科の教育用電子計算機システムのメイルサーバなど、DNS に掲載されているコンピュータには、月 1 回程度以上、ポートスキャンの類が、かけられます。つい先日も、国内の某国立大学のあるコンピュータからポートスキャンがかけられました。コンピュータは、ポートとよばれる内線番号のようなもので、サービスの要求を待ち受けていますので、それをスキャンすることで、対象となるコンピュータのサービスのメニューがわかります。そのサービスに対して、アタックを仕掛けるというわけです。家で考えると、「どこに窓があり、鍵はかかっているかなあ。」ということに、近いと思います。もし、他人の家でそんなことをしていたら、普通「どろぼう]と思われて、110 番通報されますよね。

ここでは、実際のアタックの事例の中からひとつ、御紹介したいと思います。「カッコウのたまご」の話などは、テレビや新聞での話で、自分とはほど遠い話だと思っていたころ、学科の教育用電子計算機システムで、不正侵入があり、当時は管理者ではありませんでしたが、非常事態ということで、私が対処致しました。ここで、強調しますが、私は当時システム管理者ではありません。なぜ、強調するかというと、システムに大きなセキュリティーホールがあったからです。

事例 1 不正侵入

学科の教育用電子計算機システムのファイルサーバのハードウェア保守の後、ブートして作業をはじめると、一部のシステム管理用のコマンドが実行できません。そこで、*"ls -l /usr/sbin"* としてみると、システム管理用のコマンドの所有者は、本来 *root* であるはずが、ある一般ユーザとなっています。ここから、探偵ごっこのはじまりです。

探偵ごっこ 1 とりあえず、現状を把握しようとした結果、以下のことがわかりました。

- *NIS* のマスタサーバ上に、*/boo* という、*setuid* のついた中身は*/bin/sh* で、作成日は *1* 月 *27* 日、所有者は *root* のファイルを発見しました。
- 不正侵入者は、何らかの方法で、*root* 権限を得た。
- 次の侵入のために、*/boo* を残した。

トラップ */boo* を使われては困るし、それを使って、今後も悪さをしようとするかもしれないということで、トラップを仕掛けることにしました。

- */boo* の中身を *"whoami; last; netstat -A"* の結果をメイルするように変更。これで、今後、*/boo* を実行すれば、誰が実行して、どこから、コネクションをはっているかがわかります。
- また、タイムスタンプとサイズは変わらないように調整。

探偵ごっこ 2 つぎに、なぜ、不正侵入できたのかを調査することにしました。

- */usr/adm/SYSLOG* を見て、侵入者の痕跡を調査しましたが、*"su root"* での失敗はないし、*root* でのリモートログインの失敗もありません。
- つぎに、*find* で *setuid* のファイルを調査したら、特定のユーザのディレクトリに *hsoak* というファイルを発見しました。そのファイルの作成日は、*/boo* の作成日と同じ *1* 月 *27* 日で、中身は*/sbin/sh* でした。
- つぎに、セキュリティーホールの調査のために、システムのいろいろな設定ファイルを調べました。そして、ファイルサーバの*/etc/exports* に、セキュリティーホールを見つけました。これは、*"*アクセスオプションのない行*"* でした。つまり、任意のコンピュータで *mount* 可能ということです。

推理 では、このセキュリティーホールをどのように使ったのでしょうか。私の推理は以下のようなものです。

1. 侵入者は、ファイルサーバの*/etc/exports* の設定に気づく。
2. 自分のコンピュータで、*mounut* する。

3. 自分のコンピュータのハードディスク上に、*/sbin/sh* を *hsoak* という名前で作成する。
4. *hsaok* に *setuid* をつける。
5. *mount* したディレクトリに、*hsoak* をコピーする。
6. *umount* する。
7. *NIS* のマスタサーバにログインする。
8. *hsoak* を実行し、特権を得る。

以上、実際の不正侵入の事例を紹介しましたが、この侵入者は単なる愉快犯で、特別、悪いことはしてなかったようです。

つぎに、別の不正侵入について、紹介します。これは、あるメイルサーバの事例で、私は直接携わっていなかったのですが、話を聞いて、興味があったので、システムのログを調べた例です。

事例 2 不正侵入

1. あるユーザが、「メイルが読めない」と管理者に連絡。
2. ログを調べると、そのユーザはドイツからログインしたことがあることになっている。
3. しかし、そのユーザは、その時期、確かに日本に居たし、リモートでドイツのコンピュータにログインしてから、ログインするということもしていない。
4. どうも、そのユーザのパスワードが破られた可能性がある。
5. そこで、とりあえず、メイルサーバに、学内からしかログインできないようなアクセス制限をかけた。
6. また、ドイツから例のユーザで、ログインしようとして、失敗。
7. 数分後には、学内の他学科のウェブサーバから、例のユーザでログインを試みる。
8. 今度は、特定のコンピュータからしか、ログインできないようにアクセス制限をかける。
9. いたちごっこ終了。

つぎに、紹介する事例は、とてもホットな不正アクセスの事例で、セキュリティーホールの内側から、学生用のクライアント PC に対して、学生がアタックをしかけたというものです。

事例 3 1. *SE* さんが全ての *PC* で、*Solaris* のパッチあて作業を行なっていたら、*root* で *login* できないものがあった。
2. */etc/shadow* の日付を調べると、日付が新しい。
3. とりあえず、*root* のパスワードを元に戻し、誰が不正アクセスを行なったか調べました。
4. 特定の学生が、特定の授業中に、特定のツールでセキュリティホールを利用して、不正アクセスをしていたことが判明。
5. 授業の担当教官が、面接をし、事実を確認。

これら、三つの事例は、アタックであり、セキュリティーホールなどを利用して、不正侵入を行なった事例です。これらに対しては、技術的な解決をはかることが、まず、第一です。その技術力のない人は、技術力のある人にお願いをするしかないというものです。このようなアタックを退けるためには、技術をもって、制限をかけるしかないと思います。

しかしながら、どうしてもセキュリティーホールは残るでしょうし、ファイアウォールの内側から攻撃されるとどうしようもありません。利用者のモラルの向上も必要となります。

3.2 悪意のない人による悪影響

悪意のある人によるアタックに対する対策は、技術的に大変かもしれませんが、悪意のない人達によるトラブルは、人間関係的にとても困ります。

つぎに、紹介するのは、PC-UNIX がはやりだしたころ、悪意のないユーザによる全学的な LAN のトラブルの事例です。

事例 4 学内 LAN のインターネット接続ダウン

1. 学外への接続が断たれた。
2. 当初、専用線のダウンかと思ったが、*traceroute* で調べると、学外へ行くはずのパケットが、特定の建物に行く。
3. その建物のルータの経路情報を調べると、インターネット向けの経路が特定のコンピュータになっていました。
4. その建物で、スニファーというパケット解析装置で、パケットを解析すると、特定のコンピュータが、*RIP* をいう経路制御プロトコルで、「インターネットへのゲイトウェイは、私です。」と公言している。
5. そのコンピュータのところへ行き、まず、管理者と話をして、そのコンピュータを *LAN* から切り離し、プロセスの状態を見ると、*"routed -g -s"* が動作していた。これは、上記の「インターネットへのゲイトウェイは、私です。」と *RIP* で公言する設定です。

6. そのコンピュータを *LAN* から切り離して、数分後、インターネット接続は復旧しました。

7. *"routed -g -s"* により、建物間のルータの経路情報が、書き換えられて、インターネット接続がダウンすることとなったと思われます。

8. 理由を説明して、設定を私の指示にしたがって変更してもらって、一件落着です。

これと全く同様の事件が、計 3 回発生しました。どの事例も、UNIX のことを知らない方が、PC-UNIX を導入しての失敗のようでした。ご本人には、悪意はなく、どのような事態となったかも理解できないようでした。数時間におよぶ対処で、こちらは疲れていたのですが、文句を言うこともできず、やり場がありませんでした。

つぎは、X 端末を学科の教育用計算機で使っていたころのことです。

事例 5 ホストの IP アドレス

X 端末の設定に、 *"Host IP Address"* という項目があり、*X* 端末の *IP* アドレスを入力するのですが、年輩の教官の方の中には、ホストというと大型計算機を想像し、サーバの *IP* アドレスを入力した方がいました。これにより、ネットワークは大混乱です。スニファーというネットワーク解析装置を利用して、事態を把握し、サーバの *IP* アドレスをつけた教官のところに行き、設定を変更して、トラブル解消です。

年輩の教官に文句も言えず、研究室へ帰ってきました。

つぎは、10BASE-5 で建屋内の基幹 LAN を構築し、研究室がそれらを利用していたころの話です。

事例 6 ある建屋の基幹 LAN を利用した NFS でのネットワーク性能の著しい低下

1. ある建屋で *LAN* が使えないという連絡を受ける。

2. スニファーというネットワーク解析装置を使って調べると、確かにパケットは異常に多く、ネットワークはオーバーロードの状態です。

3. しかしながら、よく調べてみると、特定の数台のコンピュータ間の通信がほとんどです。

4. それらのコンピュータの管理者に事情を聞くと、ファイルサーバとクライアントとのことです。また、ブリッジなどを利用していないとのことです。

5. *NFS* のパラメータチューニングによる再送の抑制方法を教えて、予備のブリッジをその研究室のネットワークと、基幹 *LAN* の間に設置して、トラブル解消です。

この研究室は、X-Window の "make world" はできるけれど、ブリッジは知らないは、NFS のパラメータチューニングは知らないはという、プライドの高い困った人達でした。

以上、複数の事例を見てきましたが、どれもこれも、悪意のない人達によるトラブルです。しかも、建屋レベル、学科レベルや全学レベルのトラブルになったものもあります。これらについては、ユーザ各自がスキルアップしていただくしかありません。このような方々が多いと、ネットワークを安心して利用できなくなります。

3.3 ハードウェア障害

コンピュータを安心して利用するには、コンピュータ自体に、トラブルがないことが重要です。コンピュータ自体のトラブルの一つとして、ハードウェア障害があります。現在、みなさんが利用しているコンピュータというとパソコンが多いと思いますが、ここ数年でパソコンが壊れたという経験をお持ちの方は、かなり少ないのではないでしょうか。たとえ、壊れたとしてもハードディスクの故障がほとんどであると思います。ハードウェアのうち、記憶媒体以外は、かなり安心できるようになってきたのではないかと思いますしかしながら、コンピュータの中でもっとも大事なのは、いろいろな情報を格納する記憶媒体です。それが、故障するということは、依然、安心してコンピュータを使えない要因のひとつとなります。そういう意味では、WindowsCE のようなハードディスクを持たないコンピュータは、安心して使えます。

これに対処するには、バックアップしかありません。

3.4 コンピュータウィルス

コンピュータセキュリティーというとアタックとならんで、よく取り上げられるのが、コンピュータウィルスです。実際に、コンピュータウィルスで出会うのは、

メイルの添付ファイルについてくるマクロウィルス Excel の文書に寄生するラルーや、Mellisa など

ダウンロードしたファイルなどに寄生しているトロイの木馬 不用意にダウンロードしたファイルを実行して、その中のウィルスに感染する。

が多いのではないでしょうか。しかしながら、これらのウィルスを雑誌以外では全く見聞きしたことがないという幸せな方も多いはずです。これは、自分の所属する組織やソサイエティのコンピュータ文化に依存するようです。私も、大学内でこのようなウィルスの話は、ほとんど見聞きしませんが、非常勤講師で出講している大学では、ラルーなどのウィルスが蔓延しています。授業中に、たまに、受講生

全員にウィルスチェックをかけさせるのですが、数人はウィルスに感染しています。ラルーぐらいならば、風邪と思って、それほど気にしなくてもすみますが、風邪をひいていない受講生ばかりということがない程度に、ラルーには誰か感染しています。

ウィルスにかからないためには、とりあえず、

- 不用意にメイルの添付ファイルを開かない
- 不用意にダウンロードして、プログラムをインストールしない
- 必ず、ウィルスチェックソフトを使う。

しかないと思います。

また、自分が (発病していない) キャリアになっているかもしれませんので、他人にメイルで添付ファイルを送る時は、必ず、ウィルスチェックソフトを使うようにしてください。そうでないと、ウィルスをひろげるのに、一役かってしまいますし、後で、人間関係がこじれるもととなります。

結核と同じで、軽視しているとひどめに会うことも、将来ありえますので、ご注意下さい。

また、最近は、ActiveX のスクリプトを利用したウィルスも報告されています。メイルの本体や HomePage 中のスクリプトに、ウィルスを入れておくことにより、悪いことをしようというものです。これまでは、「メイルの添付ファイルを不用意に開かない。」ということで、ウィルスの感染を防止できたのですが、それだけでなく、Windows 系では、ActiveX を有効にした状態で、不用意にメイルを見ない、不用意に Web ページを見ないというのも、加える必要がでてきました。

3.5 ソフトウェア障害

某社の OS のように、使っているとダウンすることがよくある OS というのは、安心して使えるコンピュータの OS としては、ふさわしくありません。何かの作業をコンピュータ上で行なっていた際に、いつダウンするかわからないアプリケーションや OS を使っていたのでは、精神衛生上よくありません。

また、たびたび、パッチを適用しないとセキュリティーやバグを解消できない OS も、困ったものです。

3.6 劣悪なコンピュータ環境

コンピュータの環境は決して、いいものでないところが多いように思います。しっかりとした電源設備や空調設備が必要なことは、もちろんです。ここでは、これまでに、私が遭遇したことがらについて、紹介します。

ボイラーによる電源電圧の低下 学科の教育用計算機システムで大きなサーバを導入したことがありましたが、そのサーバは三相電源を必要としました。通常、三相電源は、モータなどの動力系に使用するものです。ところで、そのサーバは、冬になると 9 時ごろと、13 時ごろにしばしば、ダウンしました。最初は気づかなかったのですが、スチーム暖房のボイラーが始動する時刻と、ダウンする時刻がほぼ一致します。そこで、そのサーバの提供業者さんにお願いして、三相電源にラインモニターを設置して頂き、電源電圧の変動を記録しました。そうすると、やはりボイラーの始動が原因で、電圧低下が起こっていることがわかりました。

瞬間的な電圧低下 瞬間的な電圧の低下により、計算機がダウンすることがあります。これは、負荷の問題などにより起こるようです。大きな電流を必要とする機械などを始動する際に、一瞬電圧が低下します。普段私が使用しているコンピュータに設置してある UPS は、時々、一瞬バッテリーモードに切り替わっています。

水洩れ 信じられない話ですが、新築の建物の 3 階の計算機室で、天井から水洩れして大変なことになったことがあります。ちなみにその建物は、5 階建てですが、計算機室の上は、ベランダとなっています。

瞬間的な停電で止まる空調設備 瞬間的な停電は、夏に時々起こります。その際、注意しなくてはいけないのが、高い空調能力が要らないからと家庭用のエアコンなどで、計算機室などを空調している場合です。家庭用のエアコンのほとんどは、瞬間的な停電の後、自動的に運転の再開は行ないません。したがって、ほっておくと冷却できないまま、計算機のガマン大会となってしまいます。

また、電源設備で注意すべきことについて、まとめておきます。

- グランドを接続する。
- ホットとコールドをチェックする。通常、コンセントの左側は穴が縦に長く、コールド側です。ときどき、逆に電気工事してあるところがありますので、チェックが必要です。
- 電気容量に気をつけて、過剰な負荷を接続しない。より線の OA タップからのタコ足配線は、もってのほかです。

3.7 対外的な信用低下

現在、コンピュータでネットワークに接続されていないものは、非常に少数で、ほとんどのコンピュータはネット

ワーク、そして、インターネットに接続されていると思います。そのような状況では、対外的に問題を起こさないということも、重要となります。つまり、

- メイルのリレーに使われていない
- 他の組織のアタックの踏台として使われていない
- ウィルスつきのメイルを送っていない

などです。さもないと、某大学のように政府系のホームページの書き換えの踏台にされて、有名になってしまいますし、メイルのリレーのブラックリストに載ってしまうというのも困ります。

4 セキュリティーツール

セキュリティーツールという言葉を聞いたことがあるでしょうか。セキュリティーをチェックするために、システム管理者が使うツールです。しかしながら、これは悪用することももちろんできます。ここでは、狭い意味でのセキュリティーツールを紹介します。

ツール 1 ポートスキャナー

内線番号に相当するポートというコンピュータのサービスのメニューを調べるためのツールです。例えば、*nmap* というツールがあります。これは、*TurboLinux Ver4.2* にも標準で含まれています。特に、特別なことはありません。特定のコンピュータのポートを調べたい時は、*"nmap IP アドレス"* とするだけです。図 *1*に、*WindowsNT4.0 WorkStation* をインストールしたコンピュータへの適用例、図 *2*に、*TurboLinux Ver4.2* をインストールしたコンピュータへの適用例を示します。それぞれ、開いているポート番号が、わかります。例えば、図 *1*では、ポート *139* が開いていますので、*Windows* 系のファイルサービスである *SMB* サービスを提供していることがわかります。また、図 *2*では、ポート *79* の *finger*、ポート *21* の *ftp* とポート *23* の *telnet* が開いていますので、*"finger @xxx.xxx.xxx.xxx"* でユーザ情報が得られれば、*ftp* や *telnet* をトライすることが可能かもしれません。これ以外にも、*LAN* 全体に対して、適用することもできますが、ここでは、省略します。

ポートスキャナーを利用して、開いているポートを確認し、不必要なものは閉じてしまうことが大事です。そうしないと、悪意をもった人からは、サービスが丸見えとなり、アタックのヒントを得ることができます。

ツール 2 パスワードクラッカー

ほとんどのコンピュータは、ユーザ名とパスワードによりユーザ認証を行なっています。つまり、ユーザ名とパスワードさえ一致すれば、他人になりすますことが可能となります。他人のユーザ名を使って何かを行なえば、不正アクセス行為ということになり、不正アクセス禁止法にふれることになります。しかしながら、このような不正アクセス行為を行なおうとする人がかなりいます。

そこで、パスワードクラッカーというツールがあります。これは、パスワードファイルを解析し、安易なパスワードを推測して、教えてくれます。*UNIX* の場合、*/etc/shadow(*シャドウ化されていないと、*/etc/passwd)* に、ユーザ名と暗号化されたパスワードがあります。システム管理者と言えども、ユーザのパスワードを直接見ることはできないようになっています。システム管理者としては、安易なパスワードをつけたユーザになりすまして、不正アクセスが行なわれるのを阻止するために、パスワードクラッカーを使って、安易なパスワードをつけているユーザに警告を行ないます。

ここでは、*UNIX* のパスワードクラッカーとして、有名な *Crack* の適用例を紹介します。学科の教育用計算機システムのパスワードファイルを解析すると、全ユーザ *2394* 人中、*crack* により推測できたパスワードは、*145* となりました。この解析の中で、興味のあった事例を以下に紹介します。

システム構築業者の安易なパスワード

学科の教育用計算機システムは、賃貸借物品で、システム構築は通常、システムインテグレータなどに行なって頂いています。ところで、このシステム構築業者がシステム構築をする上で、ユーザ登録しているのですが、このパスワードがとても安易です。複数の *SE* さんがいっしょに作業するために、忘れにくいパスワードにしているのでしょうが、会社名であったり、安易な英単語であったりと、ひどいものです。パスワードのつけ方で、システム構築業者のレベルがわかってしまいます。

学生の安易なパスワード

学生さんには、パスワードは重要なものであり、忘れたりしないようにと授業で指導されている影響かどうかはわかりませんが、忘れることのない学生番号にしている学生、名前そのものや、ユーザ名 *(*姓のローマ字 *+*英数字 *+*名のローマ字の一文字目 *)*、彼女の名前*?*、一般的な英単語の学生さんが結構います。また、それらの前や後ろに、数字を一桁加えている人も結構います。この数字を一桁加えたぐらいは、*Crack* で容易に推測できます。

教職員の安易なパスワード

学生さんが安易なパスワードをつけるのは、ある程度しかたないかもしれませんが、教職員が安易なパスワードをつけるのは、困りものです。教職員の安易なパスワードは、地名、名前、自動車の名前 *(*日本の自

```
xxxxxxxxxxx[5]% nmap xxx.xxx.xxx.xxx

Starting nmap V. 2.08 by Fyodor (fyodor@dhp.com, www.insecure.org/nmap/)
Unable to find nmap-services!  Resorting to /etc/services
Interesting ports on  (xxx.xxx.xxx.xxx):
Port    State       Protocol  Service
135     open        tcp        unknown
139     open        tcp        netbios-ssn

Nmap run completed -- 1 IP address (1 host up) scanned in 0 seconds
```

図 1: nmap の WindowsNT WorkStation への適用例

動車は英語名が多い?)、連続なアルファベット数文字、研究上の用語などです。忘れないようにと年輩の方が、安易なパスワードをつけるのはある程度わかりますが、若い方にも、安易なパスワードをつける方がいます。

ちょっと凝っているが推測されてしまうパスワード

ちょっと凝ったパスワードでも、結構推測されてしまいます。例えば、英単語の一部の *oo* を *00* に変更したものなどです。

5 不正アクセス禁止法

ハイテク犯罪対策として、ようやく、法律面で前進があり、不正アクセス行為の禁止等に関する法律[1]が、平成 11 年 8 月 6 日国会において可決・成立し、8 月 13 日に公布されました。施行は、一部を除き、平成 12 年 2 月 13 日からとなっています。内容は、

- 不正アクセス行為の禁止、処罰
- 不正アクセス行為を助長する行為の禁止、処罰
- アクセス管理者による防御措置
- 都道府県公安委員会による援助等

となっていて、不正アクセス行為に対する罰則は、一年以下の懲役又は五十万円以下の罰金、また、不正アクセス行為を助長する行為に対する罰則は、三十万円以下の罰金となっています。未だ、施行となっていませんし、もちろん、これに関する判例もありませんが、今後、注目すべき法律だと思います。

また、コンピュータに対するアタックを含めたハイテク犯罪の防止のためには、技術はもとより法律だけでなく、モラルということも重要だと思います。普段生活する上で、いろいろなやってはいけないことは、単に法律で禁じられているからではなく、モラルの問題として、やっていはいけないと子供の時からの成長過程で、身についてきているのだと思います。

[1]警察庁のホームページ http://www.npa.go.jp/police_j.htm/

6 セキュリティー関係の情報収集

セキュリティー関係のことを含めコンピュータ関係で、"keep current" でいるためには、情報収集に努める必要があります。ここでは情報収集のお役に立ちそうなことがらについて、紹介します。

普段、コンピュータ関係全般についての情報収集には、コンピュータ関係の技術雑誌をひとつ決めて読むというのが、とりあえず大事です。コンピュータ関係の雑誌は、月刊が多いので、日頃の情報収集には、Home Page を利用するのが、便利です。以下に、私が日頃見ている Home Page を示します。

- BizTech (http://biztech.nikkeibp.co.jp/)
- ZDNet (http://www.zdnet.co.jp/)

セキュリティー関係の情報は、以下の Home Page を見るのがいいと思います。

- JPCERT (http://www.jpcert.or.jp/)
- 情報処理振興事業協会 (IPA) セキュリティセンター (http://www.ipa.go.jp/SECURITY/)

7 サイトの情報検索と連絡

アタックやポートスキャンを受けた際に、相手の IP アドレスはわかるが、それがどこのサイトであるかわからないとい

```
xxxxxxxxxxx[6]% nmap xxx.xxx.xxx.xxx

Starting nmap V. 2.08 by Fyodor (fyodor@dhp.com, www.insecure.org/nmap/)
Unable to find nmap-services!  Resorting to /etc/services
Interesting ports on xxx.dj.kit.ac.jp (xxx.xxx.xxx.xxx):
Port    State       Protocol  Service
21      open        tcp       ftp
22      open        tcp       unknown
23      open        tcp       telnet
79      open        tcp       finger
111     open        tcp       sunrpc
113     open        tcp       auth
513     open        tcp       login
514     open        tcp       shell
515     open        tcp       printer
901     open        tcp       swat
22273   open        tcp       wnn6

Nmap run completed -- 1 IP address (1 host up) scanned in 1 second
```

図 2: nmap の TurbLinux への適用例

うことが、しばしばあります。この場合は、JPNIC の Whois Gateway(http://www.nic.ad.jp/jp/db/whois/) で IP アドレスで検索してサイトの組織名や、その運用責任者、技術連絡担当者がわかります。

つぎに、そのサイトへの連絡ですが、これについては、JPCERT のドキュメント (http://www.jpcert.or.jp/tech/99-0001/) が参考になります。

8 むすび

“コンピュータを安心して使える” というのが、コンピュータセキュリティーであるという定義のもとに、障害となるものについて、考察を行ないました。そこでは、単に、不正アクセスやウィルスのみが障害となるのではなく、悪意のない人による悪影響、ハードウェア障害、ソフトウェア障害、劣悪なコンピュータ環境、対外的な信用低下などがあることを述べました。そのようないろいろな障害が起こらないようにするには、コンピュータを使う人達全員が、モラルとある程度の技術をもつ必要があります。大学などで教えているコンピュータリテラシーの中に、このようなモラルと技術を採り入れる必要があると思っています。コンピュータリテラシーと称して、メイル、ホームページのブラウズ、Word や Excel の使い方のみを教えている大学が、多々あります。

また、何か起こった際に、InfraGard がいいように、Incident Responce Plan が必要です。

また、不正アクセスに関して、法律と情報収集についても述べました。

最後に参考までに、コンピュータ犯罪に関するシンポジウムと、セキュリティーの書籍を紹介します。

- “コンピュータ犯罪に関する白浜シンポジウム”,http://www.kansa.org/
- Anonymous: “クラッキング対策ファイナルガイド”, 翔泳社

“コンピュータ犯罪に関する白浜シンポジウム” は、2000 年開催のシンポジウムで、第 4 回となります。私は、第 2,3 回シンポジウムに参加しました。昨年、このシンポジウムに参加した友人の高校の先生は、「これまで、他人事だと思っていたが、勉強すべきだとわかった。」と話していました。ぜひ、一度、白浜の温泉につかりながら、コンピュータ犯罪に対して、思索する時間をとられることをお勧め致します。