インターネット普及に伴うセキュリティ問題

新美　洋
hniimi@cs.reitaku-u.ac.jp
麗澤大学国際経済学部国際経済学科

概　要

IT（Information Technology）産業は、日進月歩の発展を遂げている。日々、新たな技術が生まれ、それまでのものに取って代わる。そんな情報技術を、国が、企業が、学校が、個人が簡易に利用できる社会が形成された。しかしこの順風満帆に見える新産業にも大きな落とし穴はある。コンピュータやパーソナルコンピュータ（PC）の利用者が増大したということは、ある意味、セキュリティ等に関心のない者の利用も増えたということである。また、インターネットによって情報を得るのが容易になったということは、同時に自分の情報を他人が得る事も容易になったということでもある。本論では、この情報セキュリティの現状を分析し、そこから導き出される危機意識の必要性について、特にパスワードの管理、およびその惰弱性についての見解を示す。
キーワード：セキュリティ、不正アクセス、コンピュータウィルス、パスワード解析

Problems of Information Security Attendant on the Internet

Hiroshi Niimi

Reiteku University

Abstract

IT (Information Technology) industry is making steady advanced. The new technology is developed day-by-day and still changing. Like that information technology made social system that can use easily for nation, firm, school, and personal. Therefore personal computer (PC) had rapid progress, now each family has a computer but recently more person have each computer. But that's new industry must have a big mistake. It's easy to get information that means it's easy to know the self-information by others. This main issue shows the basic knowledge, the present condition about information security. And I would like to discuss about how to need of mind of crisis coursing for it in this paper.
Keywords: security, deny access, computer virus, password cracking

１．はじめに

インターネットは現代の社会・経済を形成するにあたって無くてはならない技術となっている。昨今、インターネットの利用人口の増加は著しく、大多数の人が何らかの形でインターネットを利用した経験があるだろう。

ひと昔前には、一部の人の間でのネットワークの利用であったのに対し、近年では老若男女を問わず、毎日のようにウェブサ

ーフィンや電子メールでの情報交換を行っている。そのあまりの利便性により、使いやすすぎる環境ができてしまったため、利用者はその危険性に対しての意識が低くなってしまっている。この問題意識・危機意識の欠如がさまざまな問題の起因となるのである。

もしもこれが一般ユーザだけでなく、システム及びネットワーク管理者にも言えるような状況があるとしたら、そのような管理下では、セキュリティに関する十分な知識や理解が欠如しているため、外部からの攻撃を受ける対象となり易い。

本論では、まず前半部で、情報セキュリティに関する基本的な知識を紹介・解説する。また後半部で、フリーウェア等で入手可能なツールを用いて、実際に password の惰弱性について考察する。

2. 情報セキュリティとは

2－1. 情報セキュリティの変遷

情報セキュリティは 1990 年代に入り、ようやく本格的にその重要性が認識され始めた分野である。コンピュータが未だ一部の大企業や政府関連機関でしか扱われていなかった 1960 年代から 1970 年代にかけては、セキュリティの問題はあまり注目されていなかった[1]。これは主に、メインフレームとそこにつながる端末というコンピュータの利用形態に起因するといえる。1980 年代に入り、LAN（Local Area Network）接続というネットワークの形成が普及して、ようやく情報セキュリティは問題視され始めた。しかし、セキュリティはその守備範囲も広く、全貌もつかみにくいものであった。この問題を打開するための対応策がセキュリティ評価・認証である。

2－2. セキュリティ評価・認証

セキュリティ評価・認証は個々の対策や技術を深く追求するのではなく、情報システムやそれを構成する機器やソフトウェア（OS を含む）について、セキュリティ機能全般及び目標とするセキュリティレベルを、統一した評価基準に基づいて評価し、その評価過程と結果を認証機関が認証するもので、そのための仕組みがセキュリティ評価認証制度である。

コンピュータ技術の先駆者であるアメリカの政府は、早くからこのセキュリティ問題に着目し、1986 年、いわゆるオレンジブック（Trusted Computer Security Evaluation Criteria / TCSEC）を制定している。これはアメリカ合衆国国防総省が制定しているセキュリティの評価基準である。1983 年に国防総省の標準として作られ、1986 年から主として国防関係システムから運用されてきた。また、欧米の先進主要 5 カ国（ドイツ・イギリス・カナダ・アメリカ・フランス）では、固有のセキュリティ評価基準が確立し、それらを国際統一した Common Criteria Project（CCP）を立ち上げている［2］。我が国でも、政府利用の情報機器のためのセキュリティ評価認証制度を 2001 年度に創設予定である。

2－3. 身近なセキュリティ

もっと身近なところに目を向けてみる。日頃 PC を使用しているわれわれ一般ユーザは、それほどセキュリティに対して気を使っていない。ログオン時のパスワード設定ぐらいである。しかし、実はそこに個人情報・企業情報の漏洩や改ざん・破壊といった危険性が常に孕んでいるのである（これは何も、PC にのみ関係している事ではないのだが、本論では本筋から外れるものであるので触れないでおく）。

現代社会におけるデータの管理は専ら PC に依っている。企業でいうなら顧客情報や在庫管理、スケジュールや人事など、ほとんど全ての企業情報が PC によって管理されている。これらのデータの一部ないし全てが一夜にして破壊されたとしたら、その損害は膨大なものになるだろう。そのような危険性は、できる限り排除していくべきものである。では、どのようにして自分たちの情報を他者から守っていけばいいのだろうか。そこで必要となってくるのが情報セキュリティポリシーである。

3. セキュリティポリシー

情報セキュリティポリシーとは、組織が情報資産に対してどのように取り組み、その構成員がどのように行動すべきかという

「方針」を明文化した「規範」である[3]。

セキュリティポリシーは運営者側の意思を示し、守るべき事項とその優先順位、対象を明確にした最低限の情報保護レベルである。つまり、情報セキュリティにおける組織の規則である。情報セキュリティはまた、CIA を確保・維持していくことである。CIA とは機密性（Confidentiality）、完全性（Integrity）、可用性（Availability）のことをいう。この３つを情報セキュリティの３要素と呼ばれる。

CIA の３要素を、実際の場面に適用するために具体化すると、大きく物理的セキュリティと論理的セキュリティに分ける事ができる。

物理的セキュリティは、建物や設備などの物理的な対応で主に災害や侵入などへの対策である。

論理的セキュリティは、さらに、「人的セキュリティ」、「管理的セキュリティ」、「システム的セキュリティ」の３つに分かれる。

人的セキュリティとは、労務管理・セキュリティ啓蒙・カウンセリングなどに区分される。管理的セキュリティは、組織・物財・運用・業務を管理する事である。そして、システム的管理とは、パスワードの設定・ファイアウォール・暗号化・アクセス制御などを管理する事である。これらは、図１のように区分することができ、セキュリティポリシーは人的・管理的セキュリティの領域で活用される。

現在、安全対策を講じなければならない情報資産は膨大な量である。また、その情報資産のどれから対策を講じていけばよいのかという、優先順位を明確化しなければならない。データベースによる情報資産の一括管理は利便性を向上させたが、情報漏洩によるリスクの拡大にもつながった。利便性とセキュリティ対策のバランスをとることは組織において非常に重要になってきている。

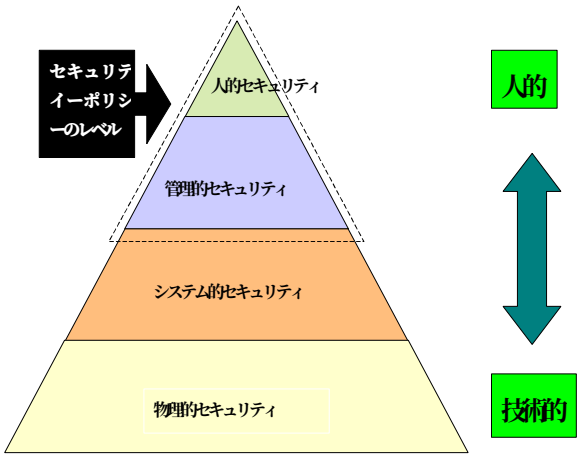

図１　セキュリティポリシーの区分

情報資産を管理する上での最大のネックは、それを扱う人間の知識不足・関心のなさにある。こういったマイナス要因は、ひいてはさまざまな不正の原因ともなる。教育・訓練プログラム、管理体制の確立がこれらの解決の鍵となるだろう。

最も重要なのはルールの明確化である。組織内でのこうした問題を防止、統制していくためにセキュリティポリシーは必要となってくるのである。

４．セキュリティホール

セキュリティホールとは、招かれざる者、いわゆる攻撃者がシステムに不正にアクセスするのを可能にしてしまうハードウェア、ソフトウェアおよびポリシーの弱点のことである。また、本論では設定ミスから派生する弱点もセキュリティホールであると定義する。そのような弱点を放置しておくと、それが攻撃のきっかけとなって、多大な被害を受ける場合もある。ルーター、クライアント／サーバソフトウェア、オペレーティングシステム、ファイアウォール等、幅広い範囲のネットワークツール、機器等に影響を与える。

こういったセキュリティホールがいつ発見されたのか、そして、それに対してどのような措置を取るべきか、管理者は常に敏感に反応しなければならない。そこで必要となってくるのが、セキュリティプロダクツである。セキュリティポリシーを設定した次の段階として、その指標に基づいてセキュリティプロダクツを選択し、設定していかなければならない。

５．セキュリティホールの発見（SATAN）

セキュリティホールをそのままにして、何の処置もとらないとセキュリティホール

を悪意のある人間に発見されたときに容易に攻撃を受ける危険性がある。

SATAN（Security Network Tool for Administrators）は、システム全体、さらにはネットワーク全体をスキャンする強力なツールで、よくある、しかも重大なセキュリティホールを見つけだすことができる。

SATAN は、移植性が高く、マウスによる直感的なインターフェイスを持つ。セキュリティホールのデータベースを持ち、それを元にセキュリティホールを発見する。言い換えれば、自分のマシンを攻撃し、セキュリティホールを検出するのである。それにより、外部からの攻撃者が狙うような潜在的侵入経路を探す。管理者は、発見された弱点を修正することでセキュリティ強化を実施することが可能となる。

SATAN はセキュリティ監査者、ネットワーク管理者、システム管理者向けのツールではあるが、諸刃の剣的性質を持っているので、入手したユーザは悪用することも可能となってしまう。SATAN はシステムの弱点は発見するが、実際システムに侵入し、被害を与えるようなことはしない。しかしながら、この強力なツールを用いればたやすく弱点を探し当てることができ、攻撃者はそれを悪用し、攻撃をしかけることができてしまうのである。

SATAN を公表することで、そのような不誠実なユーザも取得可能になってしまうのは果たして良いのだろうか、という問題も出てくるのだが、そのことについてあるクラッカーは、次のように述べている［5］。

「セキュリティ情報とツールの配布を制限しようとすると、一層状況が悪くなるだけだということは歴史が物語っている。いくら制限したところで、コンピュータ世界の“歓迎されない”人々はどうやっても手に入れるだろうし、反対に情報を合法的に求める人々まで拒否される。アクセスを制限すると、独断による不公平な排除が行われるから、制限したとしても、攻撃者はどこかで入手するであろう。また、制限があるが故に、セキュリティ強化のために利用する人々が取得できなくなる恐れが出てしまう。このような善にも悪にも成り得る強力なツールの使用に際しては、十分な理解と注意をもってして取り掛からねばならない。」

こうした状況を考慮し、実際にセキュリティホールをカバーして、不正アクセスやコンピュータウィルスから身を守るためには、さまざまなセキュリティプロダクツが必要となってくる。

6．セキュリティプロダクツ

セキュリティプロダクツは、大きく分けて 3 種類の働きを持つものに分類される。

まず、データの紛失やコンピュータウィルスに感染した際の対策を主とするもの。例えば、バックアップ装置や無停電電源装置、ウィルス駆除ソフトなどである。次に、情報の信憑性を確保するためのもの。パスワードや指紋・声紋などの本人と認証するためのもの。そして、情報の出入口を監視するためのもの。ファイアウォールやプロキシサーバなどである（図２）。これら様々なプロダクツをその場の状況に合わせて取捨選択していくことが必要となってくる。

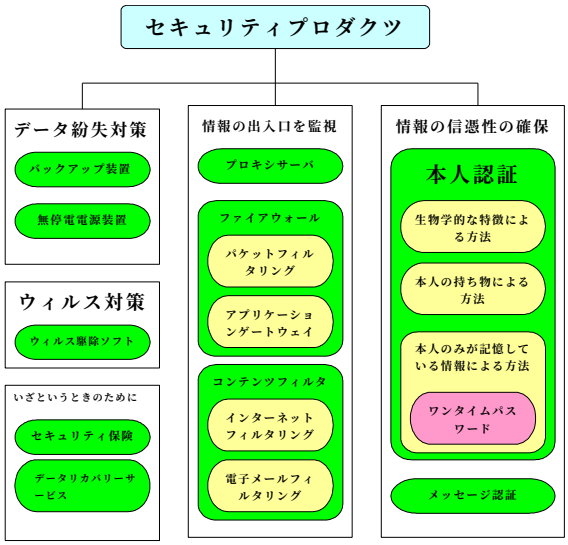

図２　セキュリティプロダクツ一覧

6－1．コンテンツフィルタ

コンテンツフィルタとは、学校や企業などで、外部から内部へ、または内部から外部への情報のやり取りをフィルタリングして、セキュリティポリシーに反する情報を出入口で制御するための仕組みである。コンテンツフィルタは、外部からの情報をコントロールするための「インターネットフ

ィルタリングソフト」と、内部からの情報をコントロールするための「電子メールフィルタリングソフト」がある。

インターネットフィルタリングソフトとは、学校や企業などの組織において、内部ネットワークからインターネットへの接続を監視、記録、報告、管理することによって、教育上好ましくない情報や業務に関係ない情報へのアクセスを規制し、教育環境、作業効率の悪化を防ぐためのソフトウェアである。代表的なものとして「WebSENSE」(Websense 社[1])や、「SonicWALL」(SonicWALL 社[2])などがある。

また、電子メールフィルタリングソフトとは、内部からの機密情報の漏洩を監視・防止するために、電子メールの内容をチェックし、指定したキーワードを含むメールの社外送信を防止したり、特定タイプの添付ファイル付メールの社外送信を防止するほか、指定したキーワードを含むメールの流れの監視や、内容の業務度・使用度の評価等も可能である。

これにより、機密情報の漏洩の防止、誹謗中傷用語を含むメールの制限、組織内での電子情報活用のモラルの向上、メールの悪質な利用の阻止が可能となる。住友金属システム開発[3]の「メールガーディアン」が代表的である。

6－2. ファイアウォール

インターネットのような外部ネットワークと LAN のようなプライベートな内部ネットワークの間に設置し、両者のネットワークユーザからの通信要求を監視し、不正な侵入を防ぐシステムがファイアウォールである。主にパケットフィルタリング方式とアプリケーションゲートウェイ方式がある。

パケットフィルタリング方式とはパケットのヘッダにある発信元アドレス情報や宛先アドレス情報、ポート番号などに基づいてフィルタリングを行い、不必要なトラフィックを制限する方式である。例えば、外部からの HTTP リクエストは受け付けるが、FTP や TELNET、FINGER のようなセキュリティ上問題になるアクセスは遮断する、といった使い方が可能である。

また、アプリケーションゲートウェイ方式は、通信を中継するプロキシ・プログラムを使用することで、組織内ネットワークをインターネットから切り離しつつ、特定のアプリケーションに対するアクセスだけを仲介するという方式である。

いずれにしても、組織内ネットワークとインターネットの間に位置し、特定の通信を通過させたり遮断することで、セキュリティを保持するという考え方に基づいている。しかし、旧来のゲートウェイ型ファイアウォールではセキュリティを守りきれなくなってきているという認識が強まっている[4]。理由としては、一台のファイアウォールで、複雑に連携された複数のシステムを守るということが原理的に困難であること、ゲートウェイ型ではインターネット側からの不正アクセスは防止できても、内部からの不正アクセスは防止できないからである。

コンピュータ犯罪の、特に企業で起こるものの多くは組織内・社内から発生しているのである[3]。こういった現状の問題に対応する方法として登場したのがホスト・ベース型ファイアウォールである。

これはセキュリティ的な保護対象となるコンピュータそのものにファイアウォールを組み込んでしまうというもので、セキュリティポリシーをコンピュータ単位で設定することが可能になる。ただし、全ての管理下の PC に導入するということは、それぞれの PC ごとに設定をする必要がある点で問題もある。

これらを従来のゲートウェイ型との併用すれば、より高いレベルのセキュリティを保持することができると考えられる。

6－3. パスワード認証

パスワード認証は、一般ユーザにとっては簡易で身近なセキュリティと言えるだろう。パスワードはアリババの「ひらけゴマ」や「山」と言ったら「川」と言うように昔から使われており、セキュリティの基本と言える。クレジットカード等の暗証番号など、現代でも日常的に使われているが、あまりに身近にあるため、その重要性、利便性

[1] http://www.websense.com/
[2] http://www.sonicwall.com/
[3] http://www.nsc.ssd.co.jp/security/

を忘れがちになってしまう。

パスワードの管理はすなわち自分に関わる全ての情報の管理であることをユーザは今一度認識しなければならない[4]。

パスワードを設定する際の留意点として次のようなものが挙げられる。

- 辞書に載っている言葉を使わない。例えば、SECRET、PASSWORD、LOVE、COMPUTER などといった言葉は避ける。
- 自分に関係ある語を使わない。家族の名前や自宅の電話番号、生年月日、趣味に関連した語などがこれにあたる。
- 自分で覚えられないようなパスワードはつけない。
- ８文字以下のパスワードはつけない。
- 大文字と小文字を混在させ、一文字以上の数字や特殊文字を入れる。
- 複数の ID を持っている場合は、それぞれ異なるパスワードをつける。
- パスワードを入力する際には後ろから見られないように注意する。
- 他人に決して漏らさない。
- ファイルに記述しておいたり、電子メールで送ったりしない。

また、最近ではワンタイムパスワードと呼ばれる技術がある。これは使い捨て（一回きり）のパスワードを使うことによって、パスワードの漏洩による被害や、ブルートフォースアタック[5]等を防止する技術である。

７．コンピュータ犯罪

ではこういったセキュリティの準備、セキュリティホールの認識をしておかないとどのような被害に遭うのだろうか。攻撃者はセキュリティホールをついてさまざまな攻撃を加えてきたり、コンピュータウィルスによる社会的な混乱を引き起こす。

もっとも恐ろしいことは、攻撃者は世界中におり、いつ、どこから自分たちのネットワークが攻撃されるのか全く予想がつかないことにある。これらの脅威から身を守るには、その犯罪の手口を熟知しておくことが必要不可欠となってくる。

7－1．コンピュータ不正アクセス

コンピュータ犯罪の代表的なものとしてコンピュータ不正アクセスがある。不正アクセスというと幅の広い言葉になるが、現状に即していえば、以下が挙げられる。

- 盗聴
  通信内容を通信者の許可無くして傍受することである。誰でもその気になれば、容易に盗聴ができてしまうのが現状である。例えば、電子メールを盗聴する場合、具体的には以下のような手口で盗聴してくる。

  ① 何らかの方法で管理者権限を取得し、盗聴対象者のメールボックスから電子メールを取り出す。
  ② 盗聴対象者のメールボックスが置かれたサーバ（メールサーバ）から、盗聴者のサーバへ電子メールのコピーを転送する。
  ③ 盗聴対象者のメールボックスが置かれたサーバの回線に「ネットワークプロトコルアナライザ」を接続し、電子メールの「パケット」を取り出した上で復元する。
  ④ ③と同じ作業を NTT など電気通信事業者の回線で行う。

つまり、電子メールの盗聴は、サーバが置かれている企業やプロバイダーなどに出向かなくても可能なのである。盗聴はその他のより深刻な犯罪を引き起こすことになる。

- 侵入
  アクセス権限を持たない第三者が何らかの方法でシステムへのアクセスを可能とし、システムが本来の意図とは異なった形態で利用されてしまう事を指す。

---

[4] IPA のパスワード設定の HP
http://www.ipa.go.jp/security/ciadr/cm01.html#user

[5] 固有の辞書を用い、総当り方式でパスワード解析を行うクラックの一種。

- なりすまし
  物理的に侵入された第三者がそのPC の所持者本人もしくはそれに準じた人物になりすまして電子メールでの誹謗中傷やWebページにおける猥褻物の掲載などを行うことである。
- 改ざん
  情報が第三者によって不正に書き換えられることである。Web ページやデータやシステムを改ざんされ、記録情報の完全性が守られないのである。これはネットワークの伝送経路が盗聴や改ざんがされやすいシステム構造であることに起因している。
- 破壊
  第三者が、通信システム、コンピュータシステムのデータを故意に消去又は破壊が行われることである。また、後で述べるコンピュータウィルス感染などの外的要因による破壊が増加している。
- ポートスキャン
  IP アドレスの範囲を指定し、その範囲で開放されているサービスポートを探す不正アクセス。最近では、Windows 上で動作するものもあり、簡単に実行できる。これ自体では大きな影響がないこともあるが、スキャンにより発見されたサービスから、侵入を受ける可能性がある。
- Dos 攻撃（Denial of Service）
  対象となるサーバに大量のパケットを送信することにより、他のサービスの運用を困難に、あるいは停止させてしまう攻撃方法。特定の IP アドレスからのパケットを受信しないように設定する事で防御できる。しかし最近では Distributed Dos と呼ばれる送信先の IP アドレスを次々と変えるシステムによって防御策を無効にしてしまうシステムが開発され、問題になっている。

もっと厳密にいえば、「システムを利用する者が、その者に与えられた権限によって許された行為以外の行為を、ネットワークを介して意図的に行うこと」である。

具体的なコンピュータ不正アクセスの例として、某大学での不正アクセスログを集計して、図 3 にまとめた。

Tcp_Wrapper を用いると、特定のサービス（telnet、ftp 等）に対して、特定のホストやネットワークからのアクセスを制御することが可能となる。Tcp_Wrapper では、許可されないアクセスがあった場合に、管理者あてにそれをメールで通知することができる。図 3 は、この機能を用いて、管理者当てに届いた警告メールから、不正アクセスの件数および、どこから不正アクセスが行われたかについて、送信元ホストのドメイン名と IP アドレスを元に分類したものである。

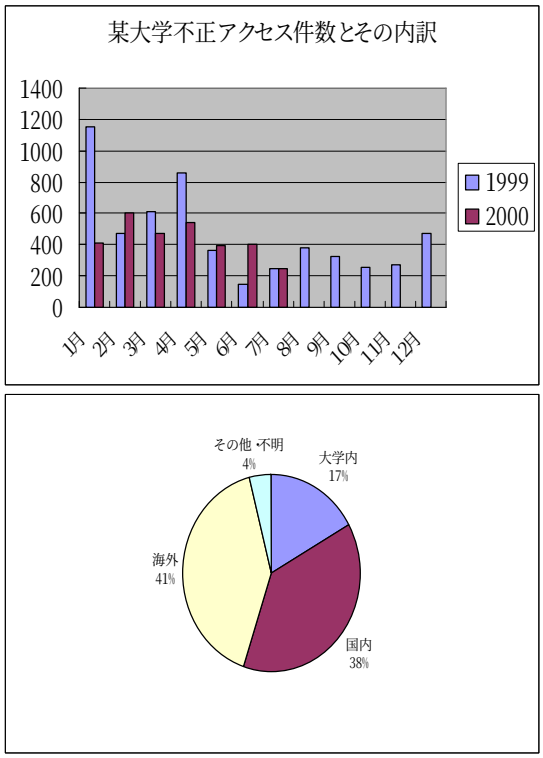

図３　某大学の不正アクセスログ件数とその内訳

この大学の不正アクセスは 1999 年の一年間で、5,000 件を超えている。また、内訳を見ると、国内、海外を問わず不正アクセスを受けている様子がうかがえる。これは、インターネットにより世界が一つの窓口から繋がっている現代においては、逆に世界のどこからでも不正アクセスを受ける可能性があるということが顕著に示されている例である。学内からの不正アクセスもあるが、これは、教室やダイヤルアップ接

続などから、許可されていないホストへのアクセスがあったことを示している。また、この組織では、学外からの POP アクセスを認めていないが、これを知らずに外部のプロバイダー等から POP アクセスを試みたことなどから不正アクセスとみなされているケースもある。

この集計では、tcp_wrapper を組み込んだシステムからの不正アクセスログしか検出できない。場合によっては、そういったものを組み込んでいないシステムも存在するわけで、全体としての不正アクセスの件数はさらに大きいであろうことは想像に難くない。

また最近、日本の Web サイトが Distributed DoS 攻撃の踏み台として利用される可能性があるということを、JPCERT/CC がホームページやメーリングリスト（ML）を通じて呼びかけている。JPCERT/CC の ML の購読方法は第 9 章の CERT 説明のところで詳しく紹介するのでそちらを参照していただきたい。

いずれにせよ、こうした不正アクセスは日常的に発生しているという事実を認識する必要があると思われる。

7－2. コンピュータウィルス

コンピュータウィルスの基本的な機能は、自己伝染機能、潜伏機能、発病機能の 3 つがある。この中のどれか 1 つの機能を持っているものをウィルスと呼ぶ。

- 自己伝染機能
  自分自身を自動的に複製する機能のことである。これはバックグランドで実行され、感染したコンピュータに接続しているすべてのドライブに対してウィルスを複製する。
- 潜伏機能
  ウィルスが発病するまで、正常な状態であるかのように振舞う機能である。この機能を利用してウィルスはコンピュータ内部で大量に増殖する。
- 発病機能
  コンピュータに実害を与える機能である。ウィルスに組み込まれたプログラムによって様々な症状が出る。

ここでいくつかの、実際に世界中で蔓延したコンピュータウィルスを紹介する［3］。

- Melissa
  「Word」の文書ファイルに感染し、「Outlook」のアドレス帳から上位 50 人にメールの形でウィルスを送りつける。
- CHI
  毎月 26 日になるとハードディスクを初期化し、パソコンを破壊する。
- VBS/NewLove
  LoveLetter ウィルスの変種で「Outlook」を利用して全アドレスに自身を送付する大量メール送信型。ただし、メールの件名と添付ファイル名は固定せず、送信されるごとに変更される。現在使用している以外のファイルを全てワーム自身のウィルスコードで上書きしてしまうため、ファイルが使用不可能になるという悪質な発病を持っている。
- Timofonica
  ロシアのコンピュータウィルス対策ソフト会社カスルスキ研究所が発見した携帯電話を対象にスパムメールを送りつけるウィルス。
- VBS/Stages
  メールに添付された SHS ファイルを実行する事によって感染・発病する。2000 年 6 月に発見され、猛威を振るった。

この他にも、「トロイの木馬」（コンピュータ内部に潜み、内部情報を盗み出すプログラム）や「ワーム」（感染はしないが、ネットワークを介して広がるプログラム）、ファイル感染型ウィルスが複合化し、感染力や破壊力が強化した新種のウィルスも登場し被害が悪化している。

なお、最近の状況として、Melissa ウィルスや VBS/Loveletter ウィルスのように、電子メールを経由したウィルス感染が大きな問題となっている。

MicroSoft 社製の「Outlook」や「Outlook Express」は、OS とともに無料で提供されるメールツールであるため、これを利用しているユーザは多い。上記のウィルスは、Outlook のアドレス帳に登録されたアドレスに対して、ウィルス付メールを自動送信するという機能を持つ。ウィルスは、添付

ファイルの形式で送付される。Subject には、本文とは関係のない件名が付くので、受信者（特に初心者）はそれに気づかない。受信者は、そのメールが友人や知人から来ているということもあり、安易に添付ファイルを開いてしまう。それでウィルスに感染してしまうわけである。感染すると、さらにその人のアドレス帳を元にメール送信が行われるので、被害は甚大となる。

もはや、コンピュータウィルスによる脅威は一般ユーザの身近に存在していると言える。ウィルスの被害に遭わないためには次のような点に注意する必要がある。

- 最新のワクチンソフトを使い、ウィルス検査を行う。
- 万一のウィルス被害に備えるため、データのバックアップを行う。
- ウィルスの兆候を見逃さないようにして[6]、ウィルス感染の可能性が考えられる場合、ウィルス検査を行う。
- 電子メールの添付ファイルはウィルス検査後に開く。
- ウィルスが感染している可能性があるファイルを扱うときはマクロ機能の自動実行は行わない。
- 外部から持ち込まれたフロッピーディスクおよびダウンロードしたファイルはウィルス検査後使用する。
- コンピュータの共同利用時の管理を徹底する。

実際に感染するまでは誰もが、「まさか自分がコンピュータウィルスの被害者になる訳がない」という意識がある。クラッカーであれば、自分のターゲットとしたサーバーのみを攻略し、一般のユーザにはほとんど被害は及ばないだろう。しかし、コンピュータウィルスは違う。コンピュータウィルスのターゲットは稼動している PC 全てなのである。コンピュータウィルスには人間的な感情はなく、感染のプロセスにおいてミスはない。私たちは常にこのコンピュータウィルスに狙われているということを自覚すべきである。さらに問題となるのは、ウィルスによって自分が単に被害者となるだけではなく「加害者」となってしまう可能性もあるわけである[7]。

ウィルスの被害に遭わないために利用する、代表的なアンチウィルスソフトをいくつか紹介する。

- Norton Anti Virus
  Norton Anti Virus は日本でもウィルスバスターと人気を二分するほどのソフトではあるが世界的に見ても McAfee とともにポピュラーなアンチウィルスソフトである。リリースしている SYMANTC 社[8]は大手の多国籍企業でコンピュータウィルスをいち早く検知するために SARC という専門機関を世界各地に配置しており、24時間体制で活動している。最新版は Norton Anti Virus 2000 である。
- ウィルスバスター2000
  現在、日本で最も広く使用されているソフトである。Trend Micro 社[9]が販売している。“ウィルスバスター”は日本のみで使用されている名前であり、諸外国で売られる場合は”Pc-Cillin”という名前で販売されている。
- 鉄壁（VirusScan）
  鉄壁というアンチウィルスソフトはここ最近で急に出てきたソフトのように思われがちであるが、ネットワークアソシエイツ社[10]の“MacAfee ウィルススキャン”の日本版専用の名前である。よってソフト自体は“MacAfee”とまったく変わらない。

8. 情報セキュリティ対策

今まで述べてきた経緯から、情報セキュリティ関係者は、常に最新の情報を収集し、既存の攻撃に対して有効な防御策を講じなければならない。それでは具体的にどのようにしてセキュリティ犯罪から身を守るのだろうか。

システム管理者は、まずその組織に適合

[6] コンピュータの動作が日常と違うなど。

[7] Outlook の事例など。ウィルス感染すると、そこからメールが発信される。

[8] http://www.symantec.com/

[9] http://www.trendmicro.co.jp/

[10] http://www.nai.com/japan/

したセキュリティポリシーを設定し、規則を作り、それに見合ったセキュリティプロダクツを導入して、セキュリティホールに対して敏感にならなければならない。また、運用していくにあたって不正アクセスやコンピュータウィルスから受ける被害の予防と被害にあった場合の復旧対策を常日頃から講じてなければならない。そして一般ユーザに対して、インターネットを利用する際の危険性に対しての危機感を認識させることも重要な役割である。

また、一般ユーザ側もコンピュータを利用する上での必要な常識を正しく理解し、何が安全で、何が危険かを察知する事が不可欠である。また、日頃からバックアップをとるなどして、安全対策を管理者に任せきりするのではなく、ユーザ自らセキュリティ対策を講じて、それに伴った知識、技術を身に付けていかなければならない。

どんなに優れたセキュリティ製品を導入しても、利用者が十分な知識と技術を持っていなければうまく機能しない。一人一人が「自覚」と「責任」をもち、「知識」を深めることが情報セキュリティ対策の基本となっていくのである。その上で必要なファイアウォールやアンチウィルスソフトを装備し、パスワードやその他のデータ管理に常に注意を払うことがこれからのユーザの義務となっていく。

こうした不正アクセスやコンピュータウィルスに対して、コンピュータセキュリティに取り組んでいる機関を利用することも、セキュリティ対策の有効な手段だといえる。

次章に、セキュリティに関連した組織について概要しておく。

9. 様々な機関の対応

9－1. JPCERT/CC

インターネットでセキュリティ問題が発生した時に支援する機関として、海外のCERT（Computer Emergency Response Team）を元に日本で組織されたのが、JPCERT/CC[11]である。JPCERT/CC は、インターネットを介して発生する各種のコンピュータセキュリティインシデントに際して、システム運用管理の視点からコーディネーションを行っている組織である。セキュリティ対策の参考となる情報をホームページや ML 等で提供している。

JPCERT/CC の ML には、誰でも簡単な手続きで参加する事ができる。具体的には、“subscribe announce”という内容をメールの本文に書き（サブジェクト行は無視される）、「majordomo@jpcert.or.jp」宛に送信すると完了である。図 4 はその ML の一例である

To: announce@list.jpcert.or.jp
Subject: Attention in your Web site
Date: Fri, 23 Feb 2001 15:39:21 +0900
From: JPCERT/CC <info@jpcert.or.jp>
Sender: announce-errors@list.jpcert.or.jp

-----BEGIN PGP SIGNED MESSAGE-----

<<< 注意喚起 >>>

JPCERT/CC
2001.2.23

多くの組織におかれましては、Web ページの改ざんを目的とした不正なアクセスが、日本国内のサイトを目標として集中的に行われていることをご認識されていることと思います。各組織におかれましては、引き続き、不正アクセス
発生の予防にご配慮くださいますようお願い申し上げます。

(ご参考) 情報処理振興事業協会 緊急警告
http://www.ipa.go.jp/security/ciadr/webjack_a.html

Web サーバを運用しているホストは、インターネット上の他のホストからアクセスでき、かつ、ホスト名を類推しやすい (あるいは公開している) ため、攻撃を受ける可能性が最も高いホストの一つです。
現在、実用的に使われているソフトウェアはどれも複雑で大規模なものになっているため、未知のセキュリティホールが含まれる可能性はどのシステムであっても否定できません。また、対策が明らかになっている既知のセキュリティホールであっても、対策が広く実施されていない間はやはり脅威となります。この ような状況では、
・常にセキュリティ関連の情報収集を行なう。
・セキュリティホールが利用されるまえに、パッチの適用やバージョンアップ
を行なう。
・本当に必要なネットワークサービスだけを運用し、必要がないネットワーク
サービスは停止する。
などの対応を推奨いたします。
各サイトにおかれましては、緊急時の連絡体制につき再確認頂くと共に、いま一度、セキュリティ対策の実施状況をご確認なさることをお勧めします。また、不審なアクセスの監視を継続されることをお勧めします。

==========

コンピュータ緊急対応センター (JPCERT/CC)
TEL: 03-5575-7762　FAX: 03-5575-7764
http://www.jpcert.or.jp/

図 4　JPCERT/CC の ML の一例

9－2. 情報処理振興事業協会（IPA）

IPA （Information-Technology Promotion Agency, Japan）は、コンピュータウィルスとコンピュータ不正アクセスの被害に関する日本で唯一の公的機関である。1970 年に「情報処理の促進に関する法律」に基づき、特別認可法人として設立した[12]。ウィルス被害の届出受理、被害の実態調査、被害届出情報の公表といった事業を続ける一方、民間の研究機関や大学等と連携しながらウィルス対策に取り組んでいる。

例えば、コンピュータウィルスの感染による被害について報告している。被害届件数は図 5 のとおりだが、2000 年 10 月までの件数は、1998 年と 1999 年の合計とほぼ同じである（5,000 件を超える）。この 3 年

[11] http://www.jpcert.or.jp/

[12] http://www.ipa.go.jp/

間の数字から計算すると 2001 年には、8,000 件以上の被害届がくることになる。もちろん計算上での話ではあるが、これは驚くべき数字といえるだろう。しかもこの数字は氷山の一角に過ぎず、実際にはこの十倍から数十倍の被害が出ていると予測される。感染経路としては電子メールが全体の約 70%を締めているのが現状である。

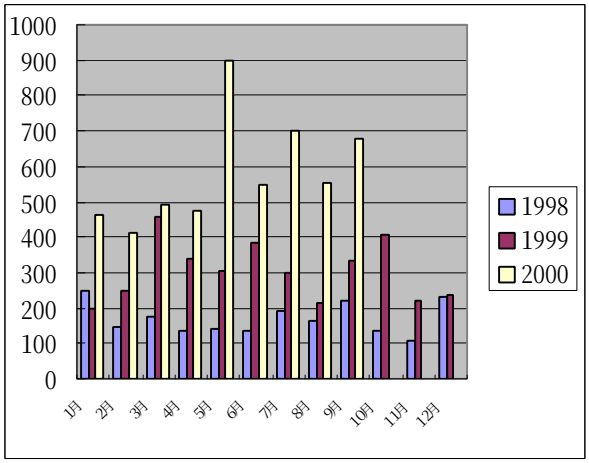

図 5　IPA に報告されたウィルス被害報告

１０．　パスワード解析

これまで、情報セキュリティに関する基礎的な知識の紹介をしてきたが、ここでは実際にフリーウェアやシェアウェア、書籍に付属している CD-ROM で入手できるパスワード解析ツールとそれを実際に動作させた様子についてまとめた。

10－1. 黒木葉子

現在、学校や企業などの組織単位での LAN 接続が増加している。OS に Windows9x を使い、ネットワーク共有サービスを利用している組織は多いのではないだろうか。

図 6 は「黒木葉子」というパスワード解析ツールのウィンドウ画面である。このソフトウェアは書籍[5]に付属する CD-ROM に収録されている。

インストールすると、図 6 の画面が出てくる。そこの「単一ホストのチェック」をチェックし、その下にあるエディットボックスに検索したいホストを指定する。そして「Go!」ボタンを押すだけで対象ホストの共有状態をチェックできる。

対象ホストが Windows9x でありかつネットワーク共有サービスによるディレクトリ共有が行なわれている場合、その共有リソースが次々と表示される。その中で弱いパスワード（簡単なパスワード）が設定されている、もしくは、パスワードが設定されていない共有リソースに対して、結果表示用リストボックスの“ Password ”欄にそのパスワードが表示され、パスワードが設定されていない場合は、「(None)」が表示される。

特定のネットワークをスキャンしたい場合は、「複数ホストのチェック」をチェックし、その下のエディットボックスに「開始 IP アドレス」と「終了 IP アドレス」を入力する。後は単一ホストのチェックと同様である。

このようにして、パスワードは簡単に解析できてしまう。他のホストへのアクセス用パスワードは同一に設定されている場合もあると思われる。注意が必要である。

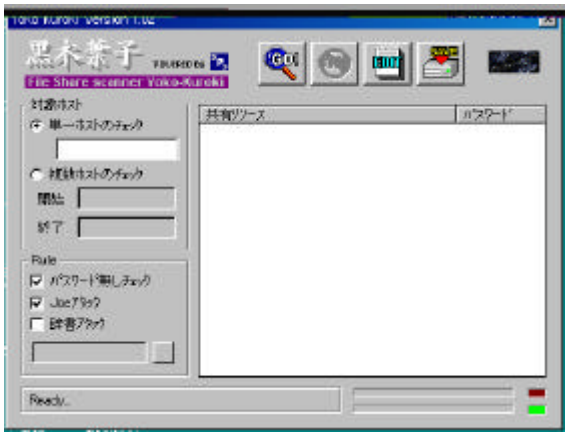

図 6　Password 解析ツール「黒木葉子」

10－2.「Revelation」

また、Snad Boy Software［10］で配布されている、直訳すると「暴露」という名前のアプリケーション“ Revelation ”は、パスワード文字復元化ツールである。

自宅や会社の PC において、ダイヤルアップ接続の際のパスワードを「パスワードの保存」にチェックを入れて保存しているような場合、このツールを使うと簡単にパスワードを盗まれてしまう。

パスワードを保存している場合、パスワード部分は、「*（アスタリスク）」によって表示されている。Revelation は、例えば、現在利用しているマシン環境をコンピュータの買い替えなどによって「別のマシンに移植したいといった場合に、パスワードを忘れてしまった」というユーザのために、そのアスタリスクを読めるようにしてしまうアプリケーションである。

使い方は非常に簡単である。まず Snad Boy Software 社のホームページ[13]からこのツールをダウンロードする。ファイルを解凍したら即座に使用できる。インストールが終了して起動してみると図 7 のような画面が立ち上がる。そして画面上にある「丸に十字」のマークをドラッグしてパスワードの場所まで持っていくだけで Revelation の Password というエリアにアスタリスク化されていたパスワードが表示される。

このツールは Internet Explorer などに記憶されているアクセス認証のパスワードも読むことができてしまう。

このようなツールが簡易にしかも無料で誰でも入手できてしまうのが現状である。使い方も簡単で、専門的な知識が要らないだけでなく、ファイルサイズが小さいため、フロッピーディスクに入れて持ち運ぶことも可能である。つまり、対象となる PC に直接的に触れる機会さえあれば、そのマシンの中に存在するパスワードをすべて手に入れることができてしまう。

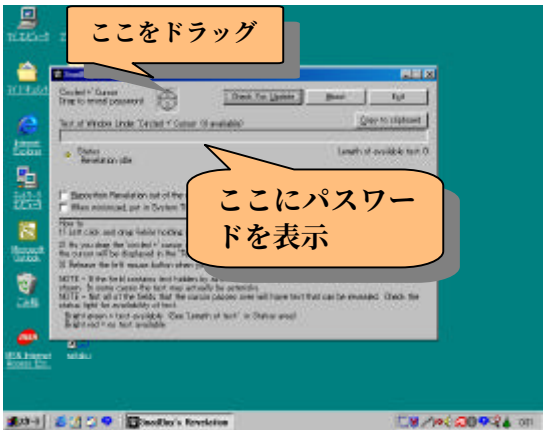

図 7　Snad Boy Software の「Revelation」

[13] http://www.snadboy.co.jp/

いわゆるハッキング行為というのは何もネットワーク上だけに限った話ではない。いくらファイアウォールやアンチウィルスソフトを駆使して外面を覆ったとしても、物理的な方法で直接 PC 本体に触れられてしまうような環境ではセキュリティの意味を成さないといえる。

１１．　まとめ

本研究では、不正アクセス行為が予想以上に頻繁に行われ、多少の知識があれば何かしらのツールを用いて、いとも簡単に、かつ短時間で不正行為を成功する事を知り得た。それに対し、自サイトを防御する管理者は膨大な知識をもってして、より完全なるセキュリティ対策を講じなくてはならない。

インターネットの普及により、攻撃者はより多くのターゲットを得て、そしてユーザはより多くの危険にさらされる事態になっている。ユーザの多くは、インターネットの利便性の部分だけに注目してしまいがちだが、利便性は往々にして危険性を伴うものである。一般ユーザはセキュリティの問題を管理者任せにせずに、自分自身で危険性を把握し、できる範囲のセキュリティ対策をするべきであると、私は考える。

一般ユーザが問題意識を持つと同時に、システム及びネットワーク管理者はさらなる努力を要求されるだろう。管理者はユーザが安心してネットワークを利用できる環境作りをするため、本論で記したような不正アクセス事例を把握し、また日頃からのシステムチェックを怠らないようにすべきである。

前述したパスワード解析ツールは、善意で使用すれば弱点・欠点の発見そして、安全性の確認が可能になり、セキュリティ対策の手助けになる。しかし、一度悪用されれば、セキュリティ上の弱点をついた攻撃が可能になったり、盗聴できたりするのである。同じツールでもそれを扱う人間の気持ちひとつで防御手段にも攻撃手段にもなる。安全と危険は表裏一体なのである。

このように監査ツール等、ツールを用いる時は、十分な知識と理解、注意の上、使用しなくてはいけない。

著者は前述したいくつかのツールを実際に使用してみたが、その結果に多大な脅威を覚えた。コストがほとんどかからずにツールが手に入り、それほどの技術も知識も必要としない簡易な方法で、第三者のパスワードを覗いてみることができるのである。

現在のセキュリティシステムは、外から入ってくる侵入者に対してはある程度効果的に機能する。しかし、一度内部に入られてしまうとその惰弱性を露出してしまう結果になる。前述の Revelation も黒木葉子も持ち運べるサイズのツールである。第三者の PC に触れる機会さえあれば、その組織内で繋がれている全てのユーザのパスワードを解析できてしまう可能性を秘めている。

特に、我が国のセキュリティ意識が低いということが、日本の各サイトが Dos 攻撃の踏み台として標的になっていること[14]からも容易に推測できる。深刻な問題が発生する可能性はどこにでもある。そして、それはもしかしたら、自サイトのセキュリティの甘さが引き金となるかもしれない。そのような事にならぬよう、管理者は問題意識を高め、情報収集し、適切な情報で適切な対処をとる必要があるだろう。また、それが義務であると言っても過言ではない。

加えて、一般ユーザにも自らのセキュリティに対しての知識を深め、自衛のための手段を講じていかなければならない。

１２. 引用・参考文献

[1] ウィリアム・スターリン著　森田進訳：インターネットセキュリティのすべて，日経 BP 社（1997）.

[2] Common Criteria ホームページ：http://csrc.nist.gov/cc/

[3] セキュリティ研究会：インターネットセキュリティがわかる，技術評論社（2000）.

[4] 日経コミュニケーション、日経 NETWORK、日経インターネット、日経オープンシステム特別企画別冊, e-Security Magazine 2001, 日経 BP 社（2001）.

[5] Mad：コンピュータ悪のマニュアル 2000 第 1 巻，(株)データハウス（2000）.

[6] 情報処理振興事業協会（IPA）ホームページ http://www.ipa.go.jp/security/virus/top-j.html

[7] 白橋明弘：インターネットセキュリティ概論 http://www2.netone.co.jp/pressclip/pre008_01.html

[8] JPCERT/CC ホームページ http://www.jpcert.ne.jp/

[9] ToolZ・ArchiveZ：様々な TOOL の紹介 http://www.net-web.co.jp/ipusiron/toolz.htm

[10] Snad Boy Software：パスワード文字復元化ツール「Revelation」のダウンロードサイト(フリーウェア) http://www.snadboy.co.jp

[11] 熊谷誠治：インターネット・セキュリティのしくみ, 日経 BP 社(1999).

[12] 中村達：コンピュータウィルス不正アクセス対策マニュアル，プレジデント社（1998）.

[13] Karanjit Siyan・Ph.D.Chris Hare 著、高辻秀興訳、大塚秀治・牧野晋ほか監修：インターネットファイアウォール，アスキー（1996）.

[14] 図 4 警告文参照のこと