インターネット大学SOIで学ぶデジタルリテラシー

【村井純教授のインターネット基礎講座】

ダイジェスト

第5回：コンピューターウイルスと不正アクセス対策

日常でインターネットを使っていても、技術の基本はよくわからない、ホントの意味を知っておきたいというみなさんに、テクノロジーとしてのインターネットがどのような原理や仕組みで動いているかを正しく理解していただくことを目的に、インターネット大学SOIの「インターネット概論」の授業の一部をダイジェストとして紹介しています。今回は不正アクセスなどの具体的な方法を見ていき、対策について考えましょう。

URL http://www.soi.wide.ad.jp/class/20020002/

村井純 むらい・じゅん

慶應義塾大学環境情報学部教授。日本のインターネット第一号となったWIDEプロジェクトを設立。インターネットでの日本語の取り扱い方の取り決めの開発、IAB委員、インターネット協会（ISOC）理事など国際的なインターネット組織の役員を歴任するなど、インターネットの技術と社会の発展に尽力している。

今回の授業はこちらを参照
SOI「インターネット概論」（第8回「コンピューターウイルスと不正アクセス対策」）へ
URL http://www.soi.wide.ad.jp/class/20020002/slides/08/

◎増加するコンピューターウイルス

コンピューターウイルスが発生したときに、その届け出を受け付けて、対策をする組織がいくつかあります。ISEC（インフォメーションテクノロジー・セキュリティーセンター）とか、カーネギーメロン大学の中のCERT（コンピューターエマージェンシーレスポンスチーム）とか、その日本版のJPCERTなどが有名ですね。こういった一般的な組織のほかにトレンドマイクロなどのウイルス対策ソフトの会社があり、ウイルス警報を出したり、新しいウイルス定義ファイルを配布したりしています。一方ではコンピューターウイルスをまいた人を罰する法律の整備なども進んでいます。日本でも2000年2月に「不正アクセス行為の禁止等に関する法律」が施行され、最近はウイルスの報告件数も増えています（図1）。もっとも発表される数字は届け出ベースなので、必ずしもウイルス被害の規模に対応しているわけではありません。

◎不正アクセスとパスワード

セキュリティーというとウイルスに注目が集まりがちですが、前回も述べたように、セキュリティーとはネットワークに繋がっている状態だから必要な全般的な用心なのです。「繋がっている状態だから鍵をかけなくてはいけない」と言いだされたのが、SFC（慶應義塾大学湘南藤沢キャンパス）ができた頃の話でした。当時はSFCでも

インターネット上の大学SOI

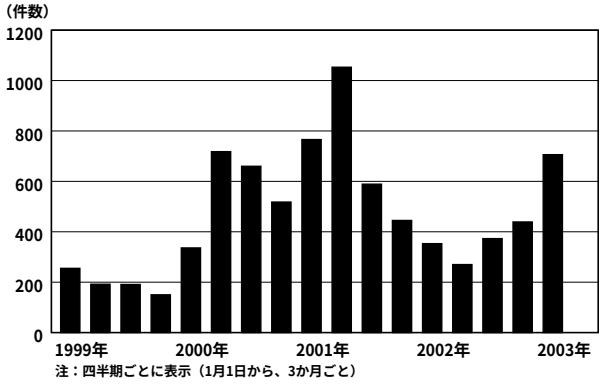
この連載の内容はSOI（School of Internet）でストリーミング映像によって公開しています。 URL http://www.soi.wide.ad.jp/

SOIとは、世界中の学ぶ意欲を持つ人々にインターネットを基盤とした高等教育と研究機会を提供することを目的として1997年に開始したインターネット大学です。
希望者はインターネットから入学を登録し、学生認証を受けることができます。詳細はホームページをご覧ください。

レッスン1

ウイルスと不正アクセスの動向

図1　インシデントの被害届け出状況



注：四半期ごとに表示（1月1日から、3か月ごと）

出典：JPCERT/CC

（注）インシデントとはコンピューターやネットワークのセキュリティーを侵害する、あるいは被害を与えようと試みる人為的な行為。法律で既定している「不正アクセス」よりも広い概念。

図2　攻撃手法の多様化・複雑化

- 自動化
- 高度な攻撃プログラム
- パスワード推測
- 既知セキュリティーホールの悪用
- サービス妨害攻撃
- パケット盗聴
- プロトコルの脆弱性への攻撃

ネットワークはそれほど整備されていなかったので、あまりセキュリティーに注意を払ってはいませんでした。

SFCでみんなにアカウントを配付したのは1990年になってからで、当時はやはりセキュリティーについての意識は低く、パスワードを設定してくれない人もいました。インターネットは地球全体をおおっているのでパスワードをかけないと、そこからほころびが発生して個別のネットワークも安全を保てないという話をして、パスワード利用に努めました。現在のSFCではパスワードを定期的に変更するよう義務付けているので、みなさんの中にも「同一のパスワードを長く使い過ぎだよ」というメールをもらった人がいるかもしれません。

なぜ、パスワードの定期的な変更が必要かといえば、パスワードを破ることで、ネットワークへの侵入を図る人がいるからです。キーサーチといって、パスワードを探していくプログラムがあって、アタックする人はそういうソフトウェアを使っています。たとえば、どうせSFCの学生なんて日本語をしゃべるだろうから、日本語の辞書を1冊スキャンすればパスワードがわかるはずだと考えるわけですね。

◎破られないパスワードとは

パスワードを破ろうと思ったら、まずその人のことを徹底的に調べるわけです。誕生日の4桁の数字は銀行などの暗証番号に使われているし、乗っている自動車のナンバープレートの数字4桁とか、自宅の電話番号の下4桁とか、このあたりは4桁の数字だとヒット率が高いですね。それから学生だと、自分の名前や所属しているサークルの名前、あるいはその年齢層の人に人気のあるアイドルの名前や、TV番組の名前などを順番にスキャンしていくと結構ヒットする。こうしたものをコンピューターのデータベースでやっていくとパスワードがわかるという研究論文を読んだ記憶があります。

いまははるかにレベルが上がっていて、世界中のウェブサイトから単語を拾ってきて辞書にしてサーチするという手法がありますから、当然かな漢字変換の元の辞書などからも探られます。ドイツからは明らかにかな漢字変換の辞書を使ってアタックしている例があります。だから、辞書に載っているような単語は駄目なのです。

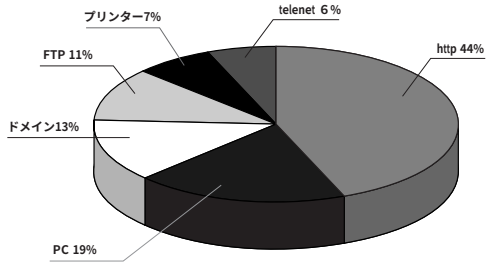
このあたりから、絶対破られないパスワードの作り方みたいな話も出てきました。よく数字もまぜなさいとか、記号も1つ入れてください、それが1つはいるだけでかなり難しくなってアタックから守られますみたいなことがいわれます。

とにかくパスワードを推測して入ってくるのが一番プリミティブな方法です。だから、パスワードはわかりづらいものを定期的に変えること、そして人目につきやすいところにはそのパスワードをさらさないということは、基本的なネットワークリテラシーです。こうしたケースでは被害者というのはコンピューターであって、そこに自動的にパスワードを推測して入ってくるわけですが、パスワードがわからなくてもコンピューターにはいろいろな穴があるため入ることはできるのです（図2）。

レッスン2

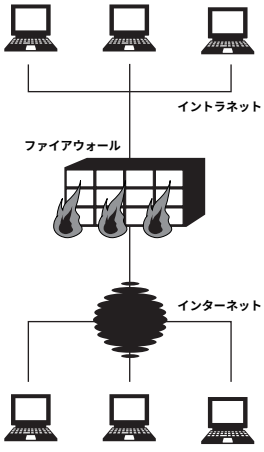
ポートスキャンとファイアウォール

図3　ポートスキャンが狙うサービス



出典：JPCERT/CC
（注）JPCERTに報告が来たものなので、世の中の状況を必ずしも反映しているとは限りません。

図4　ファイアウォールの仕組み



ネットワークを囲い込む
- アクセス制限
- 内向き/外向きのパケットフィルタリング
- ネットワークに管理者のポリシーを反映

最近のファイアウォール
- コンテンツフィルタリング
- ウイルスゲートウェイ
- VPNのエンドポイント

◎深夜に響くオフィスの電話

たとえば、電話のモデムが入り口としては危ないという話がありました。会社のネットワークはぎちぎちにセキュリティーがかかっていて、家から会社のシステムに入れないから帰って仕事ができないので、エンジニアが自分の内線の電話にモデムをくっつけて、帰宅後そのモデムから入っていくという仕事の仕方をけっこうしていた時期があったのです。最近そんな仕事の仕方をしたら首が飛びますね。この場合、大会社の電話番号を端からかけてモデムが出たところから侵入してしまえば後は楽勝です。夜中に警備員が回っていると、暗い事務所のなかで、端から電話が鳴ってはすぐに切れるのだそうです。いったん入ってしまえばなんでもできるので被害を受けるケースがけっこう多かったわけです。

◎サービスを提供するための穴を探す

ポートスキャン（図3）というソフトがあります。サーバーのなかではいろいろなサービスが、リクエストがきたら動き出そうと待ち構えています。それを端からスキャンしてうまく反応する入口からコンピューターに侵入しようとするときに使われます。サーバーになるUNIXなどのコンピューターを買ってきて立ち上げると、最初にいろんなサービスができるように動き出します。セットアップするほうも全部知っているわけではないので、たとえばメールなどの必要なサービスだけを使っています。それ以外のサービスは、よくわからないものが自動的に動き出しているのを放っておくと、そこを狙って侵入してくるケースがあります。

ポートスキャンはそのサーバーがどんなサービスをネットワークに対して提供しているのかを調べて、そのなかできちんと管理されていないサービスを見つけて、そこからセキュリティーホールを経由して入って悪いことをするわけです。入ったあとにスーパーユーザー、アドミニストレーターなどの強い権限を手に入れて、入ってしまえばセキュリティーのシステムは、外側にくらべると内側には全然甘いので、いろんなことができる。次々と侵入を続けるというわけです。

◎ファイアウォールの役割

こういった侵入に対抗するためにファイアウォール（図4）があります。防火壁ですね。ネットワークの一部に見張りを立てて、中のコンピューターに必要じゃないと思われるデータを通さない、一種のフィルターをかけるわけです。ファイアウォールというのはネットワークをこういうふうに使おうと決めて、壁を作って、必要な部分にだけ穴を開けているようなものですから、新しいサービスにアクセスしようとするとはねられてしまう。したがって、何かを新しく始めようとすると、ファイアウォールに新たな穴をあけてもらわなければならないわけです。よくインターネットの新しいサービスには「このサービスがうまく動かない場合は、ファイアウォールの有無を確かめてください」といった表示がありますが、インスタントメッセンジャーなどの複合化サービスでは、ファイアウォールがあるとその先に行けないものはいくつもあります。

レッスン3

自分を信じてもらうための仕組み

図5　SSHの仕組み

- SSH（Secure SHell）
- アプリケーション層の暗号化ツール
  - 暗号化通信路を構築
- 公開鍵暗号方式
  - 接続先が増えれば増えるほど管理する鍵も増える
- TCP Portをフォワードする機能

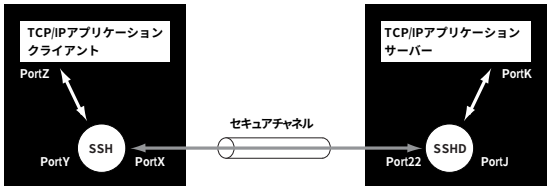
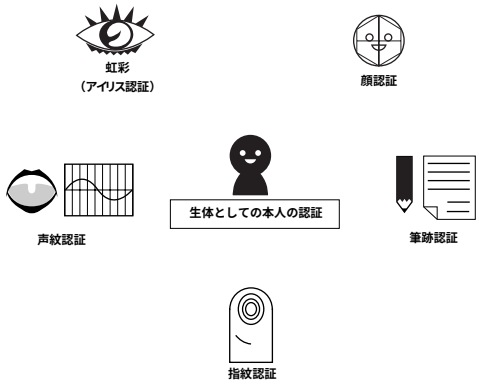


図6　バイオ認証のいろいろ



◎SSHはアプリケーションのパイプ

前回の講義（2003年6月号）と重複する部分がありますが、アタックが来たときにこのコンピューターをいかに守れるかがセキュリティーです。そのためのさまざまな技術があります。

SSH（SecureSHell）という用語はよく目にすると思います。SSHというのはアプリケーション層で公開鍵暗号を使ってチャネルが暗号化されます。この暗号化された安全なパイプを使って電子メールやTELNETなどの通信を行えば、盗み見られてもわからない。これで初めて、パスワードを流しても大丈夫になります。だから、こうした仕組みがないところでパスワードを流すと誰かに見られていると思った方がいいですね。いまウェブなどで「セキュアなチャネルにしますか」という聞かれ方をしますが、ここで「ノー」と応えたら、入力されるパスワードなどは見られていると考えた方がいいわけで、こうしたところで、決してクレジットカード番号などを言わないようにしましょう。

◎認証技術のさまざまな形

認証技術にはいろんな方法がありますが、「ぼくは村井純だよ」といったときに本当かどうかを証明するのは難しい。

本人を特定できるというのは、たとえばICカードを持っていてそれでないと自分の部屋に入れないとなればそれが証明になるという考え方もある。しかし、部屋を開けといてよと誰かにこのカードを渡したとたんに、誰でも自分になりすませます。

本当に本人じゃないとダメとなったら、バイオ認証が必要になってきます（図6）。指紋や虹彩、筆跡などですね。

バイオ認証は、指紋やサインをスキャナーで読んで登録してあるデータと比較するわけですが、どちらの認証でも100パーセント一致したら、こいつは悪人だからすぐに逮捕しろというアラートが出ます。指紋を読んだ場合、まったく違っていたら嘘つきと言ってはねるけれど、逆に、毎回絶対に誤差が生じるはずなので、ぴったり一致したら何か偽造データとしか思えない。この間のゾーンを認証するという仕組みです。

ぼくの知り合いの筆跡認証の技術の会社では、入退室管理に自社技術を採用しました。うまく作動していたのですが、そのうち社員達がサインではなく、花や丸や四角などを組み合わせ、本人だけにさっと書けるマークを登録して使うようになりました。筆跡認証技術も応用は広そうですね。

入り口だけでなく、ネット一般についても自分が誰だよという仕組みはあるが、それを誰が証明するか、その証明書をどう信頼するかの仕組みが必要になります。

そのための証明書のネットワーク作りが始まっています。この証明書は我々の生活ではどういったところに根拠があるかと言うと、印鑑証明とか住民票や戸籍とかですね。こういった証明を電子証明に作り替えようとしているのが電子政府の一部なんです。それに加えて、大学や友達や会社などが証明してくれる必要があります。実社会で必要なCA（サーティフィケート・オーソリティー）の程度はいろいろです。それを電子的に再構築する試みが進んでいます。

［インターネットマガジン　バックナンバーアーカイブ］ ご利用上の注意

このPDFファイルは、株式会社インプレスR&D（株式会社インプレスから分割）が1994年～2006年まで発行した月刊誌『インターネットマガジン』の誌面をPDF化し、「インターネットマガジン　バックナンバーアーカイブ」として以下のウェブサイト「All-in-One INTERNET magazine 2.0」で公開しているものです。

http://i.impressRD.jp/bn

このファイルをご利用いただくにあたり、下記の注意事項を必ずお読みください。

- 記載されている内容（技術解説、URL、団体・企業名、商品名、価格、プレゼント募集、アンケートなど）は発行当時のものです。
- 収録されている内容は著作権法上の保護を受けています。著作権はそれぞれの記事の著作者（執筆者、写真の撮影者、イラストの作成者、編集部など）が保持しています。
- 著作者から許諾が得られなかった著作物は収録されていない場合があります。
- このファイルやその内容を改変したり、商用を目的として再利用することはできません。あくまで個人や企業の非商用利用での閲覧、複製、送信に限られます。
- 収録されている内容を何らかの媒体に引用としてご利用する際は、出典として媒体名および月号、該当ページ番号、発行元（株式会社インプレスR&D）、コピーライトなどの情報をご明記ください。
- オリジナルの雑誌の発行時点では、株式会社インプレス R&D（当時は株式会社インプレス）と著作権者は内容が正確なものであるように最大限に努めましたが、すべての情報が完全に正確であることは保証できません。このファイルの内容に起因する直接的および間接的な損害に対して、一切の責任を負いません。お客様個人の責任においてご利用ください。

このファイルに関するお問い合わせ先
株式会社インプレスR&D
All-in-One INTERNET magazine 編集部
im-info@impress.co.jp