ネットワーク・クラッキングの防御法
—忍び寄るクラッカーへの挑戦—

工学系研究科生体機能システム制御工学専攻
中國 真教*

1 はじめに

ネットワークを経由したコンピュータへの侵入や悪戯は,『ドラマや映画の中の話だ』とか『自分には全く関係のない話だ』と考えても何の問題もないのは一昔前の話です．数ヵ月程前，テレビの深夜番組で一昔前（いやもっと昔？）の刑事ドラマの再放送をしていたのですが，その日のストーリーの内容は,『とある大学病院のネットワークにハッカー[1] が侵入しコンピュータ内に保存されている患者のデータが改竄された恐れがある』という内容でした．筆者は『こんなの今では日常茶飯事だなぁ…』と思いつつ，テレビのスイッチを切り，床に就きました．このようなドラマの中での事件が，インターネットが普及した現在では，あなたの身近なところで多発しているのです．このような被害を受けた人々は，クラッキングへの対策は何も行っていなかったという人が大半を占めています．クラッキングに気付いた時には既に手遅れで大切なデータを失ってしまったというケースもたくさんあるでしょう．あなたのコンピュータもあなたが知らないうちにクラッキングされているかもしれません．被害を受けてしまった後では遅いのです．最近，コンピュータの調子が悪いと感じたことはありませんか？ それは，あなたのコンピュータにもクラッカーの魔の手がのびている証拠かもしれません．

ここでは学内 LAN 等のネットワークに接続されたコンピュータが受ける攻撃（クラッキング）の種類と，その防御法や対策について紹介します．しかし，セキュリティーを考慮して，クラッカーの手口について具体的には触れません．ここでは Windows95 を中心に紹介することになりますが，Windows98，WindowsNT，MacOS のセキュリティーホールについてもほんの少しだけ紹介します．また，攻撃ではありませんが使用する OS に関係無く，ネットワークを利用するユーザにとって不利益（プライバシーの侵害など）となるネットワーク上での個人データの漏洩にも触れることにします．

本題に入る前に，コンピュータを利用するにあたって，

『自分の身は自分で守る』

ということを（できるだけ）心がけてください．組織によっては，その組織のネットワークの出入口に頑丈な厚い壁を築いて攻撃から身を守っているかもしれませんが，それがいつ崩されるかわかりません．確実に身を守ってくれるという保証は一切無いのです．万が一，その壁が崩されたとき，あなたはどうしますか？そのような場合に備えて，あなた自信で『最後の砦』を築くのです．一人一人が『自分の身は自分で守る』という意識を持つことにより，万が一のことがあっても被害を最小限に食い止めることができると思います．

* masanori@ms.saga-u.ac.jp

[1] この場合，ハッカーと呼ぶのは間違いで正確にはクラッカーと呼びます．ハッカーはコンピュータのハードウェア，ソフトウェアおよびネットワークの知識を駆使して技術的好奇心や技術的可能性を追求する人を指します．また，クラッカーは知識や技術を悪用する人を指します．

2　とにかく攻撃から身を守るには

まず，攻撃法について述べる前に，具体的な防御法と対策から述べることにします.『技術的なことはよく分からないが，とにかく自分のコンピュータをさまざまな攻撃から守りたい』という方の為に，この節では具体的な防御法のみ説明します．この節を読み，それを実行するだけで（完璧とは言えませんが）ある程度の攻撃から逃れることができると思います．その防御法と対策は主に以下の 4 つの方法があります.

1. ネットワーク関連のソフトウェアをアップデートする
2. ワクチンソフトを導入する
3. JavaScript を利用したホームページは見ないようにする
4. ハードディスクのバックアップをマメに取る

2.1　ネットワーク関連のソフトウェアをアップデートする

ネットワーク関連のソフトウェアでアップデートを必要とするものは，インターネットプロトコルである TCP/IP のネットワークドライバです．Windows95 の場合，バージョン『4.00.950』,『4.00.950a』がアップデートの対象となります．アップデートのファイル[2] は Microsoft のホームページで無料配布されており，アップデートの方法などの詳細な説明もあります.

Windows98 では今のところ TCP/IP のネットワークドライバをアップデートする必要はないようですが，いつかバグが報告されるかもしれないので Microsoft のホームページを，たまにチェックされることをおすすめします．WindowsNT4.0 では OS 購入時に付属している『サービスパック 3』と呼ばれる CD-ROM の中にパッチが収録されていますが，Microsoft のホームページからも入手可能です.

MacOS では今のところ，ネットワークドライバ自体にバグは発見されていないようですが，ネットワークソフトウェアである Apple Share にバグがある（バージョンは不明）ことが報告されています．勿論，このバグに対するパッチも用意されているようです.

2.2　ワクチンソフトを導入する

ワクチンソフトとはコンピュータウィルスの退治や感染防止を行うソフトウェアです．ワクチンソフトには製品化されているソフトウェアもありますが，それほど高価なものではないので，ワクチンソフトウェアを購入しコンピュータにインストールしておくことをおすすめします．ワクチンソフトとそのメーカーのホームページの URL を以下にいくつか紹介しておきます.

ウィルスバスター 98 （トレンドマイクロ社）

URL　`http://www.trendmicro.co.jp/`

Norton AntiVirus （シマンテック社）

URL　`http://www.symantec.com/region/jp/`

VirusScan （ネットワークアソシエイツ社）

URL　`http://www.nai.com/japan/`

[2] 詳細は `http://www.microsoft.com/japan/win95/modules/pcat.htm` を御覧下さい.

2.3 JavaScript を利用したホームページは見ないようにする

JavaScript を利用したホームページを見ないようにするというのは非現実的なので，JavaScript を安全に楽しむ方法を紹介します．それは，

- WEB ブラウザのキャッシュサイズを 0 バイトにする
- 使用する WEB ブラウザのバージョンは最新のものにする

などの方法です．これらの 2 つの方法を併用すれば JavaScript を利用した攻撃を受ける可能性は低くなるでしょう．勿論，WEB ブラウザのオプションで JavaScript や ActiveX コントロールなどの機能を無効にしておく方法が一番良いのですが，これでは JavaScript で作られた楽しいページも JavaScript を動かせないためにつまらないページになってしまい，この方法も現実的ではありません．

2.4 ハードディスクのバックアップをマメに取る

攻撃を受けたことによりコンピュータのデータが破壊された場合でも，バックアップを取っておくことによってある程度のデータは復旧可能です．また，攻撃されることによりデータを失うのではなく，単にハードディスクの故障によるデータの喪失にも有効なので月に 1 回くらいのペースでバックアップを取ることをおすすめします．但し，コンピュータがウィルスに感染していた場合，感染したデータまでバックアップを取ってしまうことになり非常に危険ですので，バックアップを取ったデータの中にウィルスが含まれていないかをワクチンソフトのウィルスチェッカーで確認しておく必要があります．

3 これらの防御法はどのような攻撃に対して有効なのか？

前節で述べた防御法はどのような攻撃に対して有効であるのかをこの節で説明します．前節の防御法に関係する攻撃は主に以下の 4 つの攻撃です．

- サービス不能攻撃
- コンピュータウィルスの散布
- JavaScript による地雷攻撃
- メール爆弾

3.1 サービス不能攻撃

サービス不能攻撃は，主にコンピュータにインストールされているネットワークドライバのバグやネットワークに関連したサービスを行っているソフトウェアのバグを利用した攻撃です．これは前節の 2.1 で紹介した『ネットワーク関連のソフトウェアをアップデートする』方法で攻撃を防御できます．Windows がインストールされたコンピュータが攻撃を受けたときの症例の一つとして,『攻撃を受けた直後にそのコンピュータの画面がシステムエラー時の青い画面に切り替わる』という現象があります．また，システムエラー時の青い画面にはならず,『見かけ上，正常に動作

しているように見えるが，実は，そのコンピュータのネットワーク機能が麻痺し，ネットワークからのデータの送受信ができなくなる』という症状もあります．

稼働しているコンピュータを学内 LAN に繋いでいる間は，常にそのような危険にさらされています．コンピュータの操作を行っていないのに突然青い画面になった場合は特に注意して下さい．

ところで，このような攻撃を受けたときの被害は Windows や Macintosh に限らず，症状が軽い場合はコンピュータを再起動することによって元の状態に戻すことができますが[3] ，最悪の場合はコンピュータ内のデータが破壊され，コンピュータが起動しなくなることもあります．

前節で述べたとおり，Windows95 の『4.00.950』,『4.00950a』というバージョンでのバグであると報告されていますが，バグが修正されているはずのバージョン『4.00.950b』がインストールされたコンピュータを実験的に攻撃してみたところ，その攻撃を受けたコンピュータは見事にシステムエラーを起こしました[4] ．

Windows98 に関しては，手元にその OS がインストールされたマシンがなかったので実験は行なっていません[5] ．

3.2 コンピュータウィルスの散布

動物がウィルス（病原菌）に感染するようにコンピュータもウィルスに感染することがあります．コンピュータウィルスには，ある日時になるとディスプレイにメッセージを表示するようなジョーク的なウィルスから，ハードディスク内の全てのデータを消去してしまうような凶悪なウィルス，また，ユーザの手を借りずに自己増殖するウィルスなど様々なウィルスが存在します．このような攻撃には前節の 2.2 の防御法である『ワクチンソフトの導入』を行なうことによって防御できます．

3.2.1 ウィルスの感染経路とその種類

コンピュータウィルスの主な感染経路（感染方法）は以下の 2 つです．

- 電子メールにウィルスを添付してメールを送信する
- ウィルスを『便利なフリーソフトウェア』と称して配布する

このような経路（方法）であなたのコンピュータへウィルスが近づいて来ます．ウィルスは単に受け取るだけでは感染しませんが，受け取ったものを開いたり実行したりすることによって感染します．また，その種類は機械語で作られたもの，Microsoft Word や Microsoft Excel のマクロ形式で作られたものなどがあります．機械語で書かれたウィルスの動作や繁殖は OS（プラットフォーム）の種類に依存するので Windows で動くウィルスは Macintosh には感染せず，またその逆もありません．しかし，MS Word や MS Excel のマクロウィルスは Word や Excel が動くコンピュータであれば OS に関係なくウィルスが感染します．また，以前は機械語で作成されたウィルスが主流でしたが，現在では Excel や Word のマクロウィルスが増加しているそうです．

[3] 再起動ではなく，一度，コンピュータの電源を切ってから改めて電源を投入しなければならない場合もあります．

[4] その後，調べてみて分かったのですが，Windows95 の最終バージョンでもその攻撃によってコンピュータはダウンするそうです．

[5] 自分のコンピュータで是非，実験してほしいという方をお待ちしております．

3.2.2　ウィルス感染の防止策と検査

ウィルス感染を未然に防ぐには，まず，知らない人から送られてきたメールにプログラムやマクロが含まれていても，それを開いたり実行したりしないようにすることです．それによってウィルスの感染を防止できます．また，シェアウェア，フリーウェア・サイトからダウンロードしたソフトウェアや，雑誌の付録のソフトウェアの実行も充分注意してください．古川先生の記事でも書かれているように，ネットワークに関連したソフトウェアであれば，他人に迷惑をかける可能性がさらに高くなります．もし，他人に迷惑をかけた場合，あなたは責任を取れますか？ 責任が取れないのであれば，無闇にシェアウェアやフリーウェアを使わないようにしましょう．どうしてもファイルの中身を開きたい，または実行したい場合は，開く前にワクチンソフトを用いてウィルスの有無を確認し，そのファイルの中にウィルスが含まれていないかどうかだけでも調べてください．

3.2.3　ウィルスに感染してしまったら（ウィルスに感染したかなと感じたら）

運悪くウィルスに感染した場合は，そのコンピュータが接続されているネットワークの管理者に相談することをおすすめします．感染した（または，感染したかもしれない）場合は，組織内のユーザに注意を喚起する必要がありますが，パニックを引き起こす可能性がありますので感染に関するアナウンスの方法やアナウンスを流すか流さないかは，その組織の管理者の判断にお任せしてください．また，被害が出た場合，その被害の範囲や症状などの詳細な状況を情報処理振興事業協会（IPA）に連絡してください．

情報処理振興事業協会の URL は

`http://www.ipa.go.jp/SECURITY/index-j.html`

です．また，このページにはウィルスについての詳しい情報が掲載されており，ウィルス対策をまとめたガイダンスもありますので，是非，御覧下さい．

3.2.4　ワクチンソフト利用時の注意

ワクチンソフトは，全てのウィルスに対して効果があるわけではありません．既に知られているウィルスにのみ効果を発揮するのです．すなわち，そのワクチンソフトがリリースされた後に発生した新種のウィルスには対応できないのです．したがって，ワクチンソフトの利用の際に注意すべきことは，ワクチンソフトが保持するウィルスに関するデータを常に最新のものにしておくことです．ウィルスに関する最新情報は，各社のワクチンソフトのサポートページに掲載されていますので，新種ウィルスが発生していないかを，たまにチェックしてみてください．

3.2.5　デマウィルスについて

デマウィルスとは，その名の通り『デマゴギー』の『ウィルス』ですが，実在しないウィルスに対する注意を電子メールなどを利用して呼びかけるのが特徴です．これは不幸の手紙の一種であり，デマ情報を世間に広めたいということが主な目的です．このようなデマウィルスはかなり多いという報告があります．昨年，学内の一部でウィルスに関する情報が流れましたが，その情報はデマウィルスでした．ウィルスの情報をもらい，その情報を他の人に流す時には，その情報がデマかどうかを WWW の検索エンジン等を利用して調べ，デマウィルスでないかどうかを確

認してから情報を流してください．また，デマウィルスについてもう一つ注意しなければならないことがあります．それは，ファイルが添付されたデマウィルス情報のメールを受け取った場合です．デマウィルス情報に紛れて本物のウィルスが添付されている可能性があります．とにかくこのようなメールを受け取った場合は，メール本体と一緒に速やかに削除してください．

3.3 JavaScript による地雷攻撃

JavaScript による地雷攻撃[6] とは，ホームページ上に仕掛けられた地雷（ボタンなど）をホームページの閲覧者に押させることにより，JavaScript で巧妙に作られたプログラムや WEB ブラウザのバグを利用した JavaScript のプログラムが実行され，閲覧者のコンピュータを攻撃します．これは前節の 2.3 で紹介した『WEB ブラウザのキャッシュサイズを 0 バイトにする』や『使用する WEB ブラウザのバージョンを最新のものにする』などの対処により，ある程度の防御を行うことができます．もし，防御する為の設定をしていない WEB ブラウザからその地雷（ボタン）を押してしまうと，最悪の場合，あなたのコンピュータのデータは破壊され，そのコンピュータは起動できなくなるでしょう．この地雷の攻撃は様々な OS に対応している可能性があるので，OS の種類に限らず WEB ブラウザを利用する場合には充分注意してください．このような地雷を避けるためには，やはり，怪しい雰囲気のホームページは閲覧しないようにする方が良いでしょう．

3.4 メール爆弾

メール爆弾とは無意味な内容のメールをターゲットとするメールアドレスに大量に送りつけ，相手のメール格納領域をオーバフローさせ，メールの送受信を不能にしてしまうものです．その被害を受けたコンピュータは OS によってはメールの送受信のみならず，それ以外のアプリケーションの利用も不能にしてしまうことがあります．メール爆弾への対策は特に無く，受信したそれらのメールがメール爆弾かどうかの判断（ワクチンソフトによりウィルス検査を行うようなコンピュータによる自動診断）は困難です．運悪く，メール爆弾を受信してしまった場合は，メール爆弾の全てを受信した後に手動でそれらのメールを一通ずつ削除してください．

4 ネットワーク上での個人データの漏洩

ここではユーザにとって不利益（プライバシーの侵害など）となる個人データの漏洩について簡単に述べます．

4.1 パケット盗聴

パケットとはネットワーク上に流れるデータのことであり，そのデータを盗むことをパケット盗聴と呼んでいます．パケット盗聴には，パスワードは勿論，電子メールの内容などネットワーク上に流れるデータであれば，そのデータを暗号化しない限りほとんど全てのデータの盗聴が可能です[7]．実は，このようなパケット盗聴が可能であるソフトウェアは市販されています．しかし，このようなソフトウェアの本来の利用目的はパケットの盗聴ではなくパケットの監視に使われる

[6] 一般的にこのような名前が付けられているかどうか分かりませんが勝手に名付けました．
[7] データを暗号化してもその暗号を解かれてしまうと，結局は盗聴されることになるのですが…

もので，特に，電子メールの内容を監視するソフトウェアは，企業などで社内情報の社外への漏洩防止のために使われています．このようなソフトウェアを利用することにより簡単にパケット盗聴ができます．

4.2 個人データの漏洩

氏名，性別，生年月日，住所等の個人データの漏洩は主にホームページ上の通信販売で品物購入の申込みの時に入力したデータを何者かが盗聴するというケースが多いと思います．また，インターネット上の通販ではクレジットカードによる支払いを受け付ける業者が多いので，クレジットカードの番号までも盗聴されるケースが多いようです．それ以外の個人データの漏洩は，やはりJavaScriptで作られたプログラムをホームページ上に置き，それをホームページの閲覧者に実行させることにより個人のコンピュータの中からデータを盗み出す方法があります．

4.3 漏洩への対策

このような漏洩への対策は，パケット盗聴に関しては『暗号化ソフトウェア[8] を使い，入力するデータを暗号化して送信する』，JavaScriptへの対策に関しては前にも述べましたが『使用するWEBブラウザのバージョンは最新のものにする』,『WEBブラウザのオプションでJavaScriptやActiveXコントロールなどの機能を無効にしておく』,『WEBブラウザのキャッシュサイズを0バイトにする』などの方法を取らなければなりません．しかし，暗号化したデータを送受信する方法は，お互いが暗号化ソフトウェアを持っているという条件を満たす必要があります．全てのホームページが暗号化に対応しているわけではありませんので，まだまだ，インターネットの通信販売などの利用も安心できないでしょう．

5 おわりに

ここで紹介してきた攻撃はあくまで一例に過ぎずません．もっと様々な攻撃方法があり，ちょっとした盲点を突いて攻撃をされる可能性も充分にあります．とりあえず，ここで紹介した防御法を実行しておけば，よほど運が悪くない限りは大惨事には至らないと思います．これらの防御法を実行して全く抵抗できず，効果が無かった場合でも慌てないでください．そのときに最大の効果を発揮する対策はデータのバックアップです．これだけは欠かさずに行なってください．

[8] 電子メールではPGP（Pretty Good Privacy），WWWではSSL（Secure Sockets Layer）という技術です．