東京家政学院筑波女子大学紀要第７集　141～145ページ　　2003年

＜研究ノート＞

大学のセキュリティシステム（１）

山野井一夫

Security System of College

Kazuo YAMANOI

１．はじめに

インターネットの利用者は、世界中で６億人、日本では４億４千万人と言われている[1)]。インターネットに接続した場合、よくいわれるのがクラッカー対策とウィルス対策である。一般にウィルスは、電子メールで感染するものが多いが、ワームと呼ばれるプログラムで自ら攻撃するものも現れている。ワームは、自動で複数のコンピュータへ浸入を試み、浸入したら次のコンピュータへと浸入を試みるソフトである。そのほか、Web ブラウザの弱点をついてホームページを閲覧しただけで感染するウィルスまで現れた。さらに、ウィルスとワームの両方の機能を持った複合タイプのウィルスも現れている。Nimda や Code Red と呼ばれているウィルスである[2,3)]。

2001年から本格的なハッキング関連の書籍が本屋に並ぶようになり、インターネットに関連する基礎知識があれば誰もがウィルスやワームを作成することができるようになった。ハッカー・クラッカーのためのホームページも増えて、xprobe やポートスキャンなどのクラッキングツールと呼ばれる道具も簡単にダウンロードできるようになった。

感染したウィルスやワームは、重要文書を外部に送ってしまう、ファイルを消す、他サイトを攻撃するなどが上げられる。本研究では、これらウィルスの特性や浸入、防御に付いてどうしたよいかをまとめた。

２．外部からの侵入や用語

いろいろな用語があるが、これらのキーワードについてまとめた。

（１）ハッカーとクラッカー

コンピュータへの侵入を目的とした人をハッカーと呼び、情報を悪用もしくはファイルを書き換え・削除したり、破壊活動を行う人をクラッカーと多くの人が呼んでいる。明確には、２つの分類をするのは困難とされている。

（２）ウィルスやワームは何でできているか

ウィルスやワームは、プログラムでありコンパイルした機械語、VBS やJavascript、Perl などのスクリプトなどである。

（３）マクロウィルス

マクロとよばれるアプリケーション専用のスクリプトがあり、ワープロや表計算ソフトなどで使われている。これらのマクロの機能に、ファイルの読み書き、ネットワークへの通信機能もしくは外部のプログラムや ActiveX、Java を呼び出せる機能があればウィルス作成の道具となりえる。このマクロを利

用したウィルスをマクロウィルスと呼んでいる。

（4）セキュリティホール

プログラムから発見される不備をセキュリティホールと呼ぶ。セキュリティホールは、特定の文字列を送りつける、大量の情報を送って麻痺させるなどが上げられる。

（5）電子メールでの感染

ウィルスを電子メールの添付ファイルで相手に送り付けて感染させる[4)]。開きたくなるメッセージをつけて送り付けるものもある[5)]。受け取った人は、疑いもせずに電子メールの添付ファイルを開いてしまう。開いた瞬間に、ウィルスは、感染したパソコンの電子メール履歴を見て自分自身を無差別に送付する。ウィルスが送付した電子メールの相手には友人が多く、これが感染を広げる原因にもなっている。友達からウィルスが送られて感染する場合が圧倒的に多い理由である。

ウィルスによっては、添付ファイル名を偽ったり、電子メールの不備をついて自動で感染させるものも多い。花火のプログラムにウィルスを埋め込んで感染に気づかせないもの、感染してもしばらく活動をしないで特定の条件で活動を始めるウィルスもある。

（6）ホームページによる感染

JavaScript などのスクリプトで書かれたウィルスをホームページに付け加えて、閲覧したパソコンに感染する。これは、Web ブラウザや JavaScript の不備をついて行われたものである。そのほか、サイト名に十進数を用いてローカルな Web サーバと思い込ませてウィルスを送り付けるものも現れている。

（7）ファイル形式の偽装

MIME タイプを偽って、パソコンに JPG や MIDI のように思わせて、開くときに実行形式のウィルスとして活動する。OS の不備を突いたもので、代表される例が Nimda である。

（8）ワームによる感染

主にサーバのセキュリィティホールをついて侵入する。たとえば、Web サーバにバッファオーバーランと呼ばれる大量の情報を贈りつけてサーバを乗っ取ってしまう。現在は、ブロードバンド接続とよばれる常時接続のパソコンもサーバと同様に感染が増えている。常時接続のパソコンは、一般にサーバよりセキュリティが甘いので侵入しやすい。使っている人の意識も甘いので常時接続のパソコンを狙った感染は後を絶たない。

（9）ハッキングの道具

ping と呼ばれるネットワークの接続を調べる道具を使って侵入する相手を探すものが多い。Ping には OS ごとに応答のメッセージが異なるものが多く、OS を特定できるツールも登場している。そのほか、パソコンで使われているポートを調べるポートスキャンと呼ばれるツールもある。

(10) VPN による感染

VPN で構築すれば、外部に個人情報が流れないと勘違いしやすいが時と場合による。家庭のパソコン VPN を動かして学校のシステムに繋ぐということは、学校のファイヤーウォールに穴を開けることになる。VPN を動かしているパソコンが感染した場合、ウィルスは容易にネットワークに侵入することができる。ワクチンソフトが入っていないパソコンでの VPN 接続は、非常に危険である。

(11) クロスサイトスクリプティング(XSS)[6)]

悪意のあるホームページを閲覧したときに、スクリプトをクライアント経由で掲示板などに貼り付け、それを見たクライアントがクッキーなどの個人情報を関係ないところに送ってしまう巧みな方法である。

(12) バックドア

ファイヤーウォールがあっても、内部ネットワークに侵入を手助けするバックドアと呼ばれるプログラムを何らかの形で動かされる場合がある。バックドアにより外部とのトン

ネルが作られて、ハッカーの侵入を容易にしてしまう。ハッカーによる侵入を防ぐ大きな問題がバックドアである。

3．セキュリティホール

セキュリティ対策の基本は、セキュリティホールと呼ばれるプログラムやサービスの問題点を修復することにある。メーカからパッチが出ており、定期的にパッチ（Windows Update を含む）を当てる。多くのウィルスやワームによる攻撃は、これらパッチを当てることで防げる。このパッチでしか解決できない、クロスサイトスクリプティングには特に有効である。

パッチの情報は、セキュリティ関係のメールニュースで把握する。CERT、Microsoft、ワクチンソフト会社が出しているニュースは、本学でも有効な情報入手先となっている。

4．ワクチンソフト

幾つかのワクチンソフトとよばれるものが出ている。ワクチンソフトは、ウィルスやワームを撃退するのには有効な手段である。サーバを対象にした製品、パソコンを対象にした製品、電子メールやプロキシーサーバを対象にした製品があり、本学でも取り入れている。電子メールとプロキシーサーバを対象にした製品を入れ、電子メールでのウィルスの駆除、ホームページ閲覧でのウィルス駆除を行っている。さらに製造メーカを変えて、ファイルサーバにワクチンソフトを入れて攻撃に備えている。サーバとクライアントで別会社のワクチンソフトを入れるのもウィルス対策として安全性が向上する。

ワクチンソフトは、利用者が誤ってウィルスを実行しても防御してくれる。ウィルス付き電子メールは、友達から来る場合が多く、引っかかりやすい。これらを完全に防ぐには、ワクチンソフトしかない。

ワクチンソフトの問題点は、ウィルスが出現してからワクチンパターンが完成、かつパターンがワクチンソフトに組み込まれるまでの数時間について、ウィルスに対して無意味であるということだ。流行するウィルスの多くは、感染速度が速くワクチンパターンが間に合わなかった場合が多い。ワクチンソフトだけに頼るのは危険であるということである。

5．ファイヤーウォール

インターネットに接続するときにファイヤーウォールは必要である。ファイヤーウォールは、外からの要求には応えずに内側から外への要求のみに対応するので、ハッカーの侵入はほとんど不可能と考えられる。しかし、Web サーバを置いて情報発信を行う場合や電子メールシステムを外部から見る場合に、外部からアクセスできないのでは利便性が欠ける。そこで考えられたが DMZ である。ファイヤーウォールで守る２つ目のネットワーク DMZ を用意して、この DMZ に Web サーバや電子メールサーバを置く。もし、サーバの不具合で DMZ のコンピュータに侵入されても内部ネットワークにハッカーは侵入できない。

6．その他の対策

（1）電子メールで html メールは使わない

電子メールで感染する場合、高度な html のやり取りができるメールソフトからの感染である。インターネットでは、まだ html メールは主流ではない。本学では、感染の可能性が高いということを考え、html に対応していない電子メールソフトを利用している。

（2）パソコンは、復元ツールで戻す

本学では学生が利用するパソコンは、データをすべてファイルサーバに保存している。パソコンは、学生が共同で利用するために復元ツールと呼ばれるものを入れて、電源を入れなおすと初期設定に戻るようにしている。インターネットから安易にソフトがインストールされたり、パソコンの設定が変更されても復旧できる。WindowsXP ではセキュリィティ設定ができるが、そのために動かないソフトも多くある。そのため、本学では学生用パソコンは、セキュリィティをソフトが利用できるレベル（admin）まで低くしてある。

（3）制限された Web サーバ

本来の Web サーバは、外部からホームページを閲覧するためのものである。この目的だけに考えれば、Web サーバにセキュリィティ制限をかけて運用することは、ハッキング対策として有効である。もし、Web サーバを外部から乗っ取られても外部にアクセスできない、内部のディスクに書き込めないようにすれば被害を最小限に食い止められる。

（4）ルーティングを絶つ

パソコンの多くは、DNS サーバ、電子メールサーバ、Proxy サーバが使えればインターネットを利用できる。パソコンには、ゲートウェイアドレスと呼ばれるインターネットへの出口を設定するがローカルなネットワークで３つのサーバが使えれば、設定しなくても事が足りてしまう。ゲートウェイアドレスがなければインターネットに直接アクセスできないのでバックドアを仕掛けられても侵入を防ぐ手助けになる。

（5）メッセージサービスの禁止

あるバックドアは、ハッカーとの連絡にメッセージサービスを使う。ICQ では、ID の利用者が接続されているかどうかを確認でき、ファイルの転送も可能である。特定のサービスをとめてしまうのも有効な手段である。（1）のルーティングを絶てば、バックドアはメッセージサービスを使えなくなる。

（6）Proxy サーバで特定のアクセスを禁止

WebDAV などの特定のプロキシーサーバで中継しないようにしておくことは、対策として有効である。

（7）ルータで icmp を止めるのも有効

icmp もインターネットでの１つの通信手段である。この icmp を使ってバックドアを作ることも可能である。また、Code Red のように icmp で攻撃するサーバを探しているワームもある。攻撃されにくくするための１つの方法が icmp をルータもしくはファイヤーウォールで止めてしまうことである。

7．巨大なイントラネットは、インターネットと同様

全国規模の某イントラネットにウィルスが入って蔓延してしまった原因がこれである。インターネットとの間にはファイヤーウォールやワクチンソフトを置いても、イントラネット内での対策がほとんどなかったために生じてしまった。イントラネット内でもファイルサーバを中心にウィルス対策は必要である。

8．まとめ

新しいウィルスやワームは、毎月数個現れます。その手口は、電子メール、ホームページ閲覧、直接攻撃するワームなどです。管理者のネットワーク対策として、次の項目が重要と考える。

（1）DMZ 付きファイヤーウォールでアクセスを分ける

（2）電子メール、プロキシー、ファイルサーバ、パソコンにワクチンソフトを導入する

（3）Windows Update などで最新の不具合に

すばやく対応する

（4）icmp を絶つようにする

（5）必要がなければパソコンのゲートウェイアドレスにルータの IP を書かない

（6）ファイルは、一括ファイルサーバで管理するように徹底する

（7）cert、Microsoft，コンピュータメーカ、ワクチン会社から無料で出されている最新ニュースには目を通す。

（8）届いてしまった最新ウィルスのファイルをためらわずに開いて実行してしまう。これを防ぐには、ワクチンソフトは有効であるが完璧ではない。今のところ徹底した学内の教育を行う。

参考文献

1）インターネット人口
http://www.nua.com/surveys/how_many_online/index.html

2）Nimda 情報
http://www.cert.org/advisories/CA-2001-26.html

3）Code Red 情報
http://www.cert.org/advisories/CA-2001-19.html

4）http://www.cert.org/incident_notes/IN-2002-01.html

5）http://www.cert.org/advisories/CA-2001-03.html

6）クロスサイトスクリプティング
http://www.ipa.go.jp/security/ciadr/20011023css.html