3. 特集：猛威を振るうコンピュータウィルス

情報通信ユニット　山崎　哲也

3.1 はじめに

7月から8月にかけて「サーカム(SirCam)」、「コードレッド(CodeRed / CodeRed II)」という二つの**ウィルス**①が猛威を振るった。いずれも感染力が高く、症状(感染による被害)も重いという、悪質なものである。

ウィルス、**ワーム**、**トロイの木馬**①など悪意のあるプログラムは年々その手口が巧妙になり、またインターネットの普及により感染速度が大きくなったことなどから、被害が深刻化している。

ここでは、上記二つのウィルスを中心に最近のコンピュータウィルスの動向を紹介する。

3.2 ウィルスの概要

3.2.1 SirCam

(1)特徴

SirCamは電子メールの添付ファイルを通じて感染するウィルス/ワームで、7月17日に出現した。添付ファイルを開くことで、PCに感染し、以下のような活動を行う。

MS Outlook/Outlook Expressのアドレス帳、および「インターネットテンポラリファイル」フォルダのファイルにあるメールアドレスに対して、「マイドキュメント」フォルダからランダムに選んだドキュメントファイルや画像ファイルに自分自身を追加して添付ファイルとしたメールを送りつける。メールの題名は添付ファイルの題名、本文は英語またはスペイン語である。メール送信はワーム自身が行うため、正規のメールソフトに記録が残らず、ユーザが感染に気づきにくい。

10月16日に一定の確率でCドライブのすべてのファイルを消去する。

起動時に一定の確率でハードディスクの未使用スペースを埋めてしまう

SirCam は作者のプログラムミスから Windows NT/2000 では動作しない。また、大手企業や一部プロバイダーでは、これまでの教訓から、サーバの段階でウィルス除去を行うなどの対策が進んだため、2000年5月の「Love Letter(別名 I love you)」ウィルスほどは急速な拡散は起こっていない。それでも個人ユーザを中心に感染が広がっていると見られる。日本のウィルス監視を行っている情報処理振興事業協会には7月 21 日から 8 月 20 日までに累計 1441 件の届出(内感染22%)が寄せられており、8 月は単独ウィルスの月間届出件数としてこれまでの最高(1257 件)を記録した。

(2)実際の被害

前述のようにこのウィルスはPC内のファイルをランダムに選んで送るため、個人や企業の情報が漏出してしまう。FBI やウクライナ政府の公式文書が流出するなどの被害もでている。日本でも長野や滋賀などの県庁のコンピュータが感染する被害がでている。米国のIT調査会社 Computer Economics 社は、8 月末までに全世界で 230 万台以上に感染し、ウィルス除去費用やその間に失われた生産能力をあわせた被害金額は 10 億ドルに上ると推測している。

3.2.2 Code Red / Code Red II

Code Red は、Microsoft Windows NT/2000 に感染するワームで、IIS(Internet Information Sarver)というサーバ用プログラムのセキュリティホール(ある動作をしたときにセキュリティチェックが行えなくなるなどのセキュリティ上の問題点)を利用して感染する。

7 月 13 日に拡散を始めたと考えられており、7 月 19 日には 9 時間で 25 万台以上に感染したと推定されている。Microsoft は全世界で 600 万台に感染の危険性があると推定している。

感染した CodeRed は時間、日付によって以下のような動作を行う。

- 感染 2 時間後から 10 時間:クライアントのウェブページアクセスに対して「Welcome to http ://www.worm.com! Hacked by Chinese!」という表示を返す。
- 毎月 1～19 日:ランダムに生成される IP アドレスのコンピュータに対し感染攻撃を仕掛ける。
- 毎月 20～27 日:米国ホワイトハウスのウェブサイトに **DdoS**②攻撃を仕掛ける。
- 毎月 28～月末:休眠期間となり、活動を停止する。

ホワイトハウスは7月19日にウェブサイトのIPアドレスを変更してDDoS攻撃を避けている。

Code Redは8月1日から再度活動を始め、再び被害が広がった。また、7月19日前後にVer.2と呼ばれる変種が、8月4日にはCode Red IIという、より危険度が大きい新種が発見されている。

Code Red IIはウェブページの改竄は行わず、サーバ内にバックドアツール(ハッカーが進入するための裏口)を残し、サーバをハッカーが自由にコントロールできるようにする。また、感染攻撃に使われるIPアドレスがCode Redより広い範囲で生成されるようになっており、感染範囲が広がる危険性がある。

個人用PCであっても、IISがインストールしてあればこのワームに感染する。また、実際には感染しなくとも、感染攻撃によるネットワークの負荷増大や、一部のルーター、モデムが不調を起こすなど二次的な被害も発生する。

(2)実際の被害

前述のようにホワイトハウスのウェブサイトがアドレス変更を行った。また、米Federal ExpressやMicrosoftの無料メールサービスHotmailをはじめとして、多くのウェブサイトが感染やネットワーク負荷増大により閉鎖や業務支障などの被害を受けた。また、韓国や中国でも8月に入って被害が発生している。国内でも東京メタリック通信のネットワークが、このワームが原因と見られる通信障害を起こしている。情報処理振興事業協会は8月6日の段階で国内では数千台に感染していると推定している。Computer Economics社は、8月末までにCode Red全体で100万台以上が感染し、被害金額は26億ドルに上ると推定している。

3.3 最近のウィルスのトレンド

今回のSirCamとCode Redは最近のウィルスの特徴をよく示している。

SirCamのようなファイル感染型のウィルスは、ファイルがメールなどで送られ、それが開かれない限り感染しない。そのため、SirCamは自分自身でメールを送りつける機能を持つことで感染経路を急速に増やした。

また、感染したPCのアドレス帳を利用することで、知り合いからのメールと思わせる、メール、添付ファイルの題名をランダムにすることでウィルスであることを気づきにくくするなど、心理的なトリックを使用している。Love Letterウィルスをはじめ、最近はこのようなウィルスが多くみられる。

一方、添付ファイルを開かなくても感染する、メール本文がウィルスとなったものも発見されている(VBS. Happy Timeなど)。また、正確にはウィルスではないが、ホームページを開いただけで感染し、パソコンをクラッシュさせる悪質なプログラムも発生している(国内で8月18日に発生した)。このような感染速度を増加させる傾向以外に、新しく普及したIM(インスタントメッセージ)サービスや携帯情報機器を媒介としたウィルスの増加も懸念されている。

一方、Code Redではウェブ改竄とDDoS攻撃のためにウィルスが利用されている。これらは政治的デモンストレーションとして用いられることが多く、今回もホワイトハウスのウェブサイトが標的となった。また、Code Red IIのようにハッキングツールを残すことで、情報の不正取得を行おうとするウィルスも増加している。これらの特徴は従来のウィルス作家には見られなかった点で、ウィルス作家の性格が変わりつつある傾向と見られる。

3.4 ウィルス防止の動向

SirCamは、メールに添付されたファイルを開かなければ感染しない。また、各アンチウィルスソフトメーカーは発見直後に対応した**ウィルス定義ファイル**[3]を出しており、これが十分広まっていれば感染を防げたはずである。一方、Code Redが感染に利用したセキュリティホールは、6月19日に発見され、サーバが乗っ取られる危険性が高いとする警告と、対応するパッチ(欠陥を補正するための追加ソフト)がMicrosoftより公開されていた。また7月はじめにはこのセキュリティホールを利用してサーバに侵入するプログラムがインターネット上で流されており(その後削除された)、危険性は予想されていた。すべての該当するコンピュータにパッチが当たっていれば問題が無かったはずである。

しかし、実際にはいずれのウィルスも広く感染し、大きな被害をもたらした。その理由として以下のことが考えられる。

個人ユーザを中心にウィルスの危険性やアンチウィルスソフト更新の必要性を十分理解していない人が多い。

企業においてセキュリティ対策の重要性が十分理解されておらず、セキュリティ対策が徹底されていない。特にSOHOなどでは、十分な技術を持つ、専属のシステム管理者がいないところも多い。

セキュリティホールに関する警告は毎週のように出されるため、システム管理者がすべてに対応しきれない

(Microsoft のホームページには最近1年間に IIS 関連のセキュリティ情報だけでも 25 件が掲載されている)。

インターネット上では比較的早い時期に警告が発せられるが、一般的なメディアに情報が流れるのは被害が広がってからである(主要新聞で SirCam の記事がでたのは7月 24 日　毎日新聞夕刊、Code Red については 7 月 31 日　朝日新聞夕刊である)。

ウィルスの作者が逮捕されることも最近は増えているが、ウィルスの発生には追いついていない。特に最近はインターネットなどからツールが入手でき、比較的簡単にウィルスが作成できるような環境になっているため、元を絶つことは非常に困難であろう。

従来から企業向けにはセキュリティ対策サービス会社があったが、最近、ウィルス拡散を防ぐ方法として、メール感染型ウィルスの検出をインターネット接続業者のサーバにおいて行うサービスが始まっている。日本では 7 月に岡山の NDS 社が、8 月から大手接続業者の Nifty がこのサービスを始めた。また、アンチウィルスソフトメーカの Symantec と IBM は、「Digital Immune System」と呼ばれるシステムを共同開発した。新種ウィルスの第一感染に反応し，これに対応したウィルス定義とソフトウェアを，すべての顧客に即座に配布するというものである。また、ウィルス定義のない新種ウィルスを検出するための研究も行われているが、実用化には時間がかかるであろう。

今後、ブロードバンドの普及、家電製品のネット接続など、ますますコンピュータが家庭に普及することを考えると、ウィルスの被害を少しでも低減するためには、最終的には個人における防御が重要となるであろう。そのためには、基本的なウィルス対策を広める一層の努力が求められる。教育機関でのIT教育においても、基本的なウィルス対策教育が十分行われることが必要であろう。また、少なくとも危険度の高いウィルスについては、テレビや新聞といった一般メディアでの注意の喚起が少しでも早く行われることが期待される。

※ZDNN、Nikkei Biz 等のネットニュース、情報処理振興事業協会セキュリティセンター、アンチウィルスソフトメーカ、CERT(カーネギーメロン大コンピュータ緊急チーム)、NIPC(米国家インフラ保護センター)等のホームページを参考にした。

用語説明

①ウィルス、ワーム、トロイの木馬

コンピュータに何らかの害を与えるプログラム全体が一般的にウィルスと呼ばれるが、狭義のウィルスとは、1)別のファイルに寄生する形を取り、これを実行すると感染する、2)感染すると自己の複製を他のファイル、コンピュータに作成する、3)一定の潜伏期間、またはトリガーによって何らかの症状を発現する、の特徴を持つプログラムを指す。

これに対しワームは、1)他のファイルに寄生しない、独立したプログラムである、2)自分で感染先を探し、感染する能力を持つ、と言う点が異なる。

トロイの木馬は、一見正常なプログラムであるが、裏でユーザが意図しない何らかの活動を行うプログラムを指す。感染行動を行うとは限らない点でウィルスやワームとは異なる。最近はこれらの特徴を併せ持つものが多く、SirCam も機関によってワーム、トロイの木馬両方に分類されている。

②DDoS (Distributed Denial of Service Attacks;分散サービス拒否攻撃)

サービス拒否攻撃(DoS)とは目標のウェブサイトに対して同時に多数のアクセスをかけることで、サーバやネットワークを過負荷に陥らせ、サイトのサービスを停止させる攻撃である。DDoS はこの攻撃を複数の地点から行うことで、特にハッキングなどで無関係のコンピュータを多数乗っ取り、攻撃に参加させることを指す。

③ウィルス定義ファイル

ウィルスのプログラムに特徴的なパターンを定義するデータで、アンチウィルスソフトはこのパターンを用いてウィルスの検出を行う。パターンはウィルスによって異なるため、常時更新していないと新しいウィルスに対して無力となる。