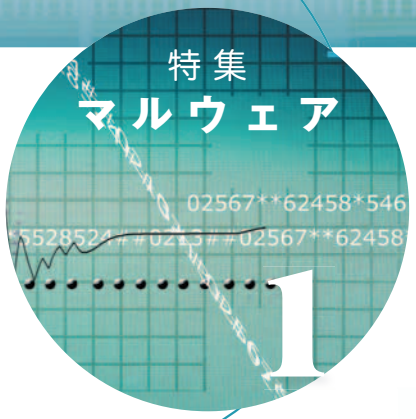
特集
マルウェア



マルウェアって？

井上大介　中尾康二（(独) 情報通信研究機構）

ウイルスからマルウェアへ

最近，新聞報道や Web ニュースなどで「マルウェア」という言葉を目にする機会が増えてきているのではないだろうか？　マルウェアとは英語の Malicious（悪意のある）と Software を組み合わせた混成語であり，ユーザの望まない不正な動作を行うプログラムの総称として，2001 年頃から広く使われるようになった用語である [1]．

それ以前は，このような不正なプログラムをウイルス（広義のウイルス）と呼ぶことが多かったが，20 世紀終盤から 21 世紀初頭にかけてウイルスの多様化が爆発的に進み，その感染形態や機能，目的などによって数多の用語[☆1]が乱立することとなった．また，90 年代の前半まで，ウイルスといえば愉快犯的なものや自己顕示を目的としたものが支配的であり，必ずしも悪意と直結したものではなかったが，90 年代後半以降，その目的は金銭搾取という明確な悪意を有するものへと変貌を遂げていった．このように，多様化・高度化・悪質化する不正なプログラムを統一的に表現する新たな用語が，学術的に，また社会的にも必要とされた結果，マルウェアという言葉が世界規模で認知され定着することとなったと考えられる．

ところで，マルウェアという造語がいつ誰によって発明されたかについては，筆者らの知る限り明らかではないが，現存するセキュリティ関連の文書を遡ると，2001 年 7 月には米国コンピュータセキュリティ緊急対応チーム CERT/CC によって発行された文書 [2] の中で，下記のようにマルウェアという用語が使用されている [1]．

> While we believe that this level of intruder activity is not unusual, additional concern may be warranted in light of a new emerging class of "malware" such as W32/Leaves.

また，学術論文を遡ってみると，1994 年の Spafford[☆2] による論文 [3] の中で，下記のようなマルウェアに関する言及があり，90 年代前半の段階で，すでにマルウェアという造語が存在していたことが窺える．

> If the source of the instructions was an individual who intended that the abnormal behavior occur, then we consider this malicious coding ; authorities have sometimes referred to this code as *malware* and *vandalware*.

マルウェアという造語の発明者はさておき，マルウェアという統一用語が定着したことで，マルウェアに関連した研究分野を指し示す「マルウェア検出」や「マルウェア解析」，さらには「マルウェア対策」といった包括的な用語も生み出されてきた．他の活発な研究分野の例に漏れず，明快な分野名は研究人材を集める求心力の 1 つとなり，その結果，本研究分野における人的資源の創出が進んでいる．また，社会的にもマルウェアという用語は徐々に浸透してきており，本分野の研究成果を社会還元する際のハードルを下げる効果も発揮している．このように，マルウェアという用語の学術的および社会的な存在意義は非常に大きいと言える．

以降の章では，本マルウェア特集を読み進める上で役立つ，マルウェア関連の用語解説を行うとともに，マルウェアの歴史について概観する．

マルウェア関連用語

前章で述べたように，我々はマルウェアという統一用語を獲得したが，それを細分化するための用語には，マルウェアの感染形態や目的，機能など，異なる切り口による分類から生み出されたものが混在しており，さらにそれらの用語について厳密なコンセンサスが形成されているわけではない [4]．そこで本章では，本特集を読み進める上で役立ついくつかの分類に絞って紹介することとする．なお，より詳細な用語解説や体系的な分類については文献 1)，4) を参考のこと．

☆1 狭義のウイルス，ワーム，トロイの木馬，スパイウェア，アドウェア，ランサムウェア，スケアウェア，ダウンローダ，ドロッパ，ボット，等々．

☆2 Morris ワームの最初の解析者としても知られている．

マルウェアの感染形態に着目した分類

• ウイルス（Virus）

ウイルス（狭義のウイルス）とは，それ単体では動作せず，自分自身を他のファイルやプログラムに寄生させる感染形態のマルウェアを指し，感染対象によって，ブートセクタ感染型とファイル感染型に大別できる．前者は，フロッピーディスクやハードディスクなどのシステム領域を感染対象とし，後者は実行可能ファイルを主な感染対象とする．ウイルスの中には，他のウイルスを感染対象とするものも存在する．

• ワーム（Worm）

ワームとは，狭義のウイルスのように宿主となるファイルやプログラムを必要とせず，単体で動作し自己増殖を行う感染形態のマルウェアを指す．一般に狭義のウイルスに比べ高い感染力を有し，大規模感染を引き起こす傾向にある．ワームの感染手法には，電子メールやリムーバブルメディア（USB メモリ等）を移動媒体とするもの，Windows のファイル共有やメッセージング機能を利用するもの，そして OS やアプリケーションの脆弱性に対する攻撃コード☆3 を用いるもの，などが存在する．

• トロイの木馬（Trojan Horse）

トロイの木馬とは，ギリシャ神話のトロイア戦争で計略に用いられた木馬に倣い，有用なプログラムやファイルを装ってユーザ自身によるシステムへの導入・起動を誘い，実際にはユーザの意図しない不正な動作を行うマルウェアを指す．トロイの木馬はユーザの不注意を利用してシステムへの侵入を果たすため，感染機能を持たないものが多い．

上記以外にも，フィルタドライバ☆4 として実装され，OS のカーネルの深部に潜伏する巧妙な感染形態を持つマルウェアも少なからず存在している．たとえば，マルウェアのファイルやプロセスをアンチウイルスソフトやタスクマネージャに対して隠蔽するルートキット（Rootkit）や，ユーザのキーボード操作を記録・収集するキーロガー（Keylogger）などは，この感染形態を取ることが多い．

マルウェアの目的に着目した分類

• スパイウェア（Spyware）

スパイウェアとは，ユーザの PC 上で個人情報や行動履歴を収集し，特定のサーバなどに送信することを目的としたマルウェアを指す．キーロガーも目的という点ではスパイウェアの一種と考えられる．

• アドウェア（Adware）

アドウェアとは，ユーザに企業広告などを提示することを目的にしたプログラムであり，無害なアドウェアも存在する一方，ユーザの同意なしに広告を頻繁にポップアップしたり，ユーザの意図しない Web サイトに強制誘導したりするものはマルウェアと見なされる．

• ランサムウェア（Ransomware）

ランサムウェアとは，ユーザの PC 上のディレクトリやファイルに対して強制的に暗号化やパスワード付き ZIP 圧縮を行うことで，ユーザのデータを「人質」にし，そのデータの復号や解凍の見返りとして，ユーザから身代金（ransom）を搾取することを目的としたマルウェアである．

• スケアウェア（Scareware）

スケアウェアとは，ユーザに虚偽の情報を提示し不安（scare）を煽ることで，無意味なソフトウェアを販売することを目的としたマルウェアである．典型的な例として，偽のマルウェア感染情報をユーザに提示して Web サイトに誘導し，実際には何の機能も有さないプログラムをアンチウイルスソフトと称して販売しようとするものがある．

マルウェアの機能に着目した分類

• ダウンローダ（Downloader）

ダウンローダとは，それ自身とは別のマルウェアを特定のサイトからダウンロードし，感染 PC にインストールする機能を持ったマルウェアである．最近のマルウェアの多くは感染後にダウンローダを多段に用いることで解析を困難にしたり，定期的にダウンロードを繰り返したりすることで，新しい機能を持ったマルウェアを容易に拡散させることが可能になっている．

• ドロッパ（Dropper）

ドロッパとは，マルウェアを内包した状態で流通し，

☆3 マルウェアが感染対象の OS やアプリケーションの脆弱性を攻撃し，管理者権限を奪取するための命令列を攻撃コード（Exploit Code）と呼ぶ．攻撃コードの多くはバッファオーバフローと呼ばれる手法によって，アクセス権を持たないシステム上で任意の命令を実行させることを可能にしている．この攻撃コードに含まれる任意の命令部分をシェルコード（Shellcode）と呼ぶ．シェルコードという用語は，攻撃コードによって攻撃が成功した後，システムを制御するためにシェル（/bin/sh）を立ち上げることが多いことに由来しているが，原理的にはシェルコードにシェルの起動以外の命令が入ることもあり得る．

☆4 OS のカーネル内で，（アプリケーションに近い）上位のデバイスドライバと（ハードウェアに近い）下位のデバイスドライバ間の入出力をインターセプトし，機能の拡張や置き換えを行うデバイスドライバ．アンチウイルスソフトにもしばしば用いられる．

ユーザの PC 上で実行されると，暗黙のうちにマルウェアをインストール(ドロップ)する機能を持ったマルウェアである．ドロッパの中には Microsoft Word などの文書ファイルになりすまし，実行されると実際の文書を表示すると同時にマルウェアをインストールするという巧妙なものも存在する．

その他の分類

• ボット(Bot)

ボット☆5 とはロボットの短縮語であり，指令者☆6 からの遠隔操作によって，多岐にわたる活動，目的，機能を実現するマルウェアである．ボットに感染した PC はボットネットと呼ばれる一種のオーバレイネットワークを形成する．ボットネットは小規模なものでは数百，大規模なものでは数十万もの感染 PC 群によって成り立っている．指令者は，指令サーバ☆7 (IRC☆8 サーバや HTTP サーバ) 経由でボットネットに制御命令を同報し，その結果，多数のボットが命令に従って一斉動作を行う．今日，ボットネットはスパムメールの大量送信や，DDoS 攻撃☆9，大規模な感染活動などさまざまなセキュリティインシデントの源泉となっている．

マルウェアの歴史

本章では，マルウェアの歴史を概観する．表 -1 は，年ごとに出現した主要なマルウェアを示している．紙面の都合上，マルウェア名から感染対象のアーキテクチャ(W32 など)や亜種の区別(Sobig.a, Sobig.b)などは省略し，極力新種として発見された日付順に記載している．もちろん，この年表に載っていないマルウェアも多数存在することに留意されたい．

1970 年代〜 1980 年代中盤：発見の時代

聞き慣れた科学技術用語は SF 小説に由来していた，ということはままあることだが，ウイルスとワームという用語も実は 70 年代の SF 小説が基となっている．

ウイルスは米国の SF 作家 David Gerrold の 1972 年の作品「When HARLIE Was One」☆10 の中で登場する．同作では，ウイルスに対抗するためのワクチンという名のプログラムも登場する．一方，ワームは英国の SF 作家 John Brunner の 1975 年の作品「The Shockwave Rider」☆11 の中でテープワーム（tapeworm）という自己増殖機能を持ったプログラムとして登場する．

ところで，自己増殖するプログラムという概念が示されたのは，それら SF 小説より遥か以前であり，1949 年の John von Neumann による自己増殖オートマトン理論にまで遡る．Neumann は，2 次元のセル・オートマトンの中で自己複製を行うプログラムを定義し，それが無限に自己複製を繰り返すことを証明した．

実際のネットワーク上で自己増殖するプログラムが作成されたのは 1971 年であり，BBN 社の Bob Thomas がインターネットの原型である ARPANET に放ったプログラム Creeper が世界初☆12 のワームと言われている．Creeper は自分自身のコピーをリモートシステム上に生成し，"I'M THE CREEPER : CATCH ME IF YOU CAN" というメッセージを表示するプログラムであった．これに対し，Reaper というワクチンプログラムが作られ，Creeper は駆逐された．ちなみに，Reaper は Creeper とまったく同じ感染機能を有していた．

1980 年にはゼロックス・パロアルト研究所(PARC)の John F. Shoch と Jon A. Hupp が，ワームを用いた分散コンピューティングの実験を行った．このワームはネットワークを探索し，アイドル中のマシンを見つけると，それをネットワークブートさせ，その際に自分自身を送り込んで計算力を借りるという機能を持っていた．しかしながらある夜，PARC のイーサネット上にテストのため置かれていたワームが暴走を始め，PARC の相当数のマシンがクラッシュするという事態が起こった．幸いにも，万が一を想定してワームに組み込まれていた緊急停止機能によって，ワームは次の日には駆除された．

1982 年には当時高校生であった Richard Skrenta が，同級生を驚かせる目的で世界初のウイルス Elk Cloner を作成した．Elk Cloner は Apple II のフロッピーディスクのブートセクタに感染するウイルスであり，感染したマシンは 50 回の起動ごとに次のような詩を表示した．

> Elk Cloner : The program with a personality
> It will get on all your disks
> It will infiltrate your chips
> Yes it's Cloner!
> It will stick to you like glue
> It will modify ram too
> Send in the Cloner!

☆5 ボットは一般的には任意の機能を自動実行するプログラムを意味し，したがって検索エンジンの巡回用ボットなど，マルウェアではないボットも存在する [4]．
☆6 複数のボットを一斉に操ることからハーダー（Herder：羊飼い）とも呼ばれる．
☆7 Command and Control サーバ，あるいは C&C サーバと呼ばれることもある．
☆8 Internet Relay Chat
☆9 Distributed Denial of Service 攻撃(分散型サービス不能攻撃)．
☆10 邦題：H・A・R・L・I・E
☆11 邦題：衝撃波を乗り切れ
☆12 世界初のワームや世界初のウイルスについては諸説ある．

Year	Malware
1970	
1971	Creeper (1st worm)
1972	# The term “virus” first appeared in a SF novel “When HARLIE Was One”.
1973	
1974	
1975	# The term “worm” first appeared in a SF novel “The Shockwave Rider”.
1976	
1977	
1978	
1979	
1980	Xerox PARC Worm
1981	
1982	Elk Cloner (1st virus)
1983	
1984	# Cohen defined virus in his paper “Computer Viruses - Theory and Experiments”.
1985	
1986	Brain (1st IBM PC virus), PC-Write (1st Trojan horse), Virdem
1987	Cascade, Jerusalem, Lehigh, Christmas Tree, MacMag
1988	Byte Bandit, Stoned, Scores, Morris Worm
1989	AIDS (1st ransomware), Yankee Doodle, WANK
1990	1260 (1st polymorphic virus), Form, Whale
1991	Tequila, Michelangelo, Anti-Telefonica, Eliza
1992	Peach (1st anti-antivirus programs), Win.Vir_1_4 (1st Windows virus)
1993	PMBS
1994	Good Times (1st hoax)
1995	Concept (1st macro virus)
1996	Laroux, Staog (1st Linux m.w.)
1997	ShareFun, Homer, Esperanto
1998	Accessiv, StrangeBrew (1st Java m.w.), Chernobyl
1999	Happy99, Tristate, Melissa, ExploreZip, BubbleBoy, Babylonia
2000	Loveletter, Resume, MTX, Hybris
2001	Anna Kournikova, BadTrans, CodeRed I, Sircam, CodeRed II, Nimda, Klez
2002	LFM-926 (1st Flash m.w.), Chick, Fbound, Shakira, Bugbear
2003	Sobig, SQLSlammer, Deloder, Sdbot, Mimail, Antinny, MSBlaster, Welchia, Agobot, Swen, Sober
2004	Bagle, MyDoom, Doomjuice, Netsky, WildJP, Witty, Sasser, Wallon, Bobax, Rbot, Cabir (1st Symbian m.w.), Amus, Upchan , Revcuss, Lunii, Minuka, Vundo
2005	Bropia, Locknut, BankAsh, Banbra, Anicmoo, Commwarrior, Pgpcoder, Zotob, Gargafx, Peerload, Cardblock, PSPBrick (1st PSP m.w), DSBrick (1st Nintendo DS m.w.), Dasher
2006	Kaiten, Leap (1st Mac OS X m.w.), Redbrowser, Cxover, Exponny, Mdropper, Flexispy, Spaceflash, Stration, Mocbot, Fujacks, Allaple
2007	Storm Worm, Pirlames, Zlob, Srizbi (1st full-kernel m.w.), Silly, Pidief
2008	Mebroot, Infomeiti, Conficker
2009	Virux, Yxes, Gumbler, Induc
2010	Zimuse

表 -1　マルウェア年表

1984年，Fred Cohenは論文"Computer Viruses - Theory and Experiments"を発表し，その中で初めて（コンピュータ）ウイルスという用語を定義し，それがもたらすであろう脅威を予見するとともに，対策の困難さについて言及している．

このように，1970年代から1980年代中盤にかけては，ウイルスやワームが計算機やネットワーク上で実在し得ることや，そのポテンシャルが認識され始めた「発見の時代」であったと言える．

1980年代中盤～1990年代中盤：実験的試行の時代

1980年代中盤から1990年代中盤にかけては，マルウェアの多種多様な機能が開発され，さらにそれらが実世界で試される「実験的試行の時代」であった．

1986年，パキスタンのFarooq Alvi兄弟によって，IBM PCに感染する初のウイルスBrainが作成された．このウイルスは彼らが経営するBrain社のソフトウェアを違法コピーしたPCに感染し，下記のようにウイルス駆除のためにBrain社にコンタクトを求めるメッセージを表示するものであった．その結果，米国や英国からの電話がBrain社に殺到することとなった．

> Welcome to the Dungeon ©1986 Basit * Amjad (pvt) Ltd.
> BRAIN COMPUTER SERVICES 730 NIZAM BLOCK
> ALLAMA IQBAL TOWN LAHORE-PAKISTAN
> PHONE: 430791,443248,280530. Beware of this
> VIRUS.... Contact us for vaccination...

同年には初のトロイの木馬PC-Writeも登場している．PC-Writeは同名の文書編集ソフトになりすまし，実行されるとファイル・アロケーション・テーブル（FAT）を破壊し，ハードディスクをフォーマットするものであった．

1988年には，sendmail，fingerd，rsh/rexecなどの複数の脆弱性とパスワードクラックを悪用したMorrisワームがインターネット上で拡散し，6,000台あまりのUNIXマシンに感染したと言われている．これは当時のインターネットの約10%にあたるとされ，これを契機に米国ではCERT/CCが設立される運びとなった．

1990年以降，Virus Exchange BBSと呼ばれるウイルス情報交換のための掲示板が立ち上がり，また，MtE☆13，VCL☆14，PS-MPC☆15に代表されるマルウェア作成ツールが次々と登場する[1]など，マルウェア作成の技術的ハードルが下がり，実験的なマルウェアが数多登場することとなる．さらに，感染のたびに異なる鍵で自己暗号化を行うポリモーフィック（Polymorphic）型ウイルスや，アンチウイルス無効化機能など，マルウェアの基礎技術がこの時代に数多く開発・試行されている．

1990年代中盤～現在：悪用の時代

1990年代中盤以降，マルウェアはいよいよ「悪用の時代」に突入する．

マクロウイルスの台頭

1995年，Conceptと呼ばれるウイルスが発見される．このウイルスはMicrosoft Wordのマクロ機能（アプリケーションの機能を自動実行する機能）を利用して感染するマクロウイルスの先駆けであった．Concept自体はユーザに実害を与える機能は有していなかったものの，これ以降，多数のマクロウイルスが出現することになる．

1999年に出現したマクロウイルスMelissaはユーザが感染したWordファイルを開くと，Wordの標準テンプレート（NORMAL.DOT）に感染する．そして，それ以降に開くすべてのWordファイルにも感染する．さらに，感染PC上のOutlookのアドレス帳に登録された最大50個のメールアドレスに向けて，感染したWordファイルが添付された電子メールを送信することで拡散する．Melissaの感染台数は数十万台に上ったと推定されている．

ワームの大規模感染

2000年代前半には，WindowsやWindowsサーバの脆弱性を狙う攻撃コードを用いたワームの大規模感染が次々と発生した．

2001年7月に出現したワームCodeRed Iは，Windows NT/2000上で動作するサーバソフトウェアであるIIS☆16の脆弱性を攻撃するHTTP要求を，インターネット上に無作為に送出し，1日で30万台を超えるWebサーバへの感染を引き起こすとともに，世界中のネットワークを逼迫させた．

2001年9月にはNimdaと呼ばれるワームが出現した．NimdaはCodeRedと同様，IISの脆弱性を攻撃すると同時に，CodeRed II（CodeRed Iの亜種）が作成したバックドア☆17経由での侵入，電子メールの添付ファイル，Windowsのファイル共有など複数の感染経路を持っていた．さらに，NimdaはInternet Explorerの脆弱性に対する攻撃手法も備えており，Nimdaが埋め込まれたWebサイトを閲覧したPCが大量感染した．

2003年1月にはMicrosoft SQL ServerおよびMSDE☆18を標的としたSQLSlammerと呼ばれるワームが発生し

☆13 Mutation Engine
☆14 Virus Creation Laboratory
☆15 Phalcon/Skism Mass Produced Code Generator
☆16 Internet Information Server

た．このワームはデータサイズが 376 Byte と非常に小さく，1 つの UDP パケットに収まるサイズであったため，インターネット上で高速に拡散し，わずか 10 分間で 75,000 台の SQL サーバに感染したと推定されている．このワームによる膨大なトラフィックは各国に影響を及ぼし，特に韓国ではインターネットが数時間にわたりアクセス不能となった．

2003 年 8 月には，Windows のリモート・プロシージャ・コール（RPC）の脆弱性を狙うワーム MSBlaster が出現し，過去最大規模の感染（後の Microsoft の発表では最低でも 800 万台）を引き起こした．MSBlaster は 2003 年 8 月 16 日に Windows Update サイトに DDoS 攻撃を開始するようプログラムされていたが，Microsoft が DNS から攻撃対象（windowsupdate.com）のエントリを一時的に削除することによって攻撃は無効化された☆19．なお，この直後に出現したワーム Welchia は，MSBlaster と同じ脆弱性を利用して拡散し，感染後に MSBlaster の駆除と Windows Update を行う機能を有していた．

2000 年代序盤から中盤にかけては，上述のワームのほかにも，Sobig や MyDoom，NetSky，Sasser など大規模感染を引き起こすマルウェアが多数出現した．また，P2P ファイル共有ソフト Winny を介して拡散するマルウェア Antinny は，数々の情報漏えいの引き金となった．

ボットネットの登場

2004 年頃から，マルウェアに感染している PC 群が同期して活動する様子が世界中で観測され始めた．マルウェアの革新技術「ボットネット」の登場である．ボットネットは前述の通り，ボットと呼ばれるマルウェアに感染したホストの集合体である．初期のボット（Sdbot，Agobot，Rbot など）は感染形態としてはワームであり，リモートからの脆弱性攻撃や，Windows ファイル共有などを利用して拡散し，感染後は特定の IRC サーバに接続して指令者からの制御命令を待ち受ける．指令者は原理的には任意の命令を膨大な数のボットに一斉に行わせることが可能であり，このボットネットを利用した数々の不正行為（ほぼすべてが金銭目的）が，日々発生するようになった．たとえば，スパムメールの 9 割近くがボットネットから送信されているという調査結果もあり，そのスパムメールがユーザをフィッシング☆20 サイトやマルウェア感染サイトへと誘導し続けている．ボットの詳細については，本特集の“ボット対策プロジェクト「サイバークリーンセンター」からみた国内のマルウェア対策”を参考のこと．

ポストボットネット

ボットネットの登場以降，マルウェアは急速に高度化・巧妙化していった．2000 年代後半のマルウェアの多くは，検出を避けるため静かに潜伏を続ける戦略を取り，MSBlaster のような大規模感染を引き起こすものは姿を消した（と，多くのセキュリティ専門家が考えていた）．また，フィッシングや SQL インジェクション☆21，標的型攻撃☆22 など，金銭的価値の高い個人情報を狙った攻撃も目立つようになってきた．

ところが，2008 年 11 月，多くの専門家の予想を覆し Conficker と呼ばれるマルウェアが出現した．Conficker は MSBlaster を上回る大規模感染（Arbor Networks 社による調査報告では 2009 年 2 月の段階で約 1,200 万台）を引き起こし，その勢いは 2010 年現在も衰えていない．Conficker は過去のワームが備えていたさまざまな機能を集大成したかのようなマルウェアであり，それに加えて USB メモリ経由の感染や，時間をシードとした動的なランデブーポイント（指令サーバの URL）の決定，さらには感染 PC 間での P2P ネットワークの自律的確立など，これまでにないさまざまな機能を備えている．

さらに，2009 年 5 月頃から，大小さまざまな Web サイトの改ざんと，それらの Web サイトを閲覧した PC のマルウェア感染が報じられ始めた．これは Gumblar 攻撃と呼ばれる新種の攻撃手法によるものである．Gumblar 攻撃では，改ざんされた Web サイトの閲覧によるマルウェア感染，感染 PC 上からの FTP アカウント情報の取得，FTP アカウント情報を用いた Web サイト改ざん，という巧妙なサイクルを繰り返すことで感染を拡大している．Gumblar 攻撃の詳細は本特集の“マルウェアと戦う技術　「Web からの脅威」とマルウェア検出・防御技術”を参考のこと．

☆17 感染 PC をリモートから操作するため，マルウェアによって作成された LISTEN ポート．
☆18 Microsoft SQL Server Desktop Engine
☆19 MSBlaster は windowsupdate.com だけを攻撃対象としており，そのリダイレクト先である windowsupdate.microsoft.com を攻撃対象に含めていなかったため，Windows Update は機能し続けることができた．
☆20 オンラインバンクやゲームサイトなど，正規の Web サイトを装ったサイトを立ち上げ，ユーザから ID・パスワードやクレジットカード番号などを搾取する不正行為．
☆21 Web アプリケーションに想定外の SQL 文を実行させて，バックエンドのデータベースを不正に操作し，Web の改ざんや個人情報の搾取を行う攻撃手法．
☆22 特定の個人や組織に的を絞って，巧妙に作り込まれた文面のマルウェア付きメールを送信する攻撃手法．本特集の“コラム：標的型メールがやってきた”を参考のこと．

マルウェアとの戦い

本稿では，マルウェアという用語が定着してきた経緯とその意義，マルウェア関連用語の紹介，そしてマルウェアの歴史について概観した．マルウェアの歴史は裏を返すとマルウェアとの戦いの歴史でもある．本特集の以降の記事では，マルウェアとの戦いの現場や，マルウェアと戦うための最新技術の数々が紹介されているので，ぜひそちらを参考とされたい．

謝辞　本原稿の執筆にあたり，有益な助言をいただいた日立製作所 寺田真敏氏，東海大学 菊池浩明教授に感謝の意を表する．

参考文献

1）瀬戸洋一 他編著：情報セキュリティ概論，日本工業出版，ISBN：978-4819019170 (2007).
2）CERT/CC : W32/Leaves : Exploitation of Previously Installed SubSeven Trojan Horses, CERT Incident Note IN-2001-07 (2001). http://www.cert.org/incident_notes/IN-2001-07.html
3）Spafford, E. H. : Computer Viruses as Artificial Life, MIT Press, Volume 1, Issue 3 pp.249-26 (1994).
4）NIST : Guide to Malware Incident Prevention and Handling, NIST Special Publication 800-83 (2005). http://csrc.nist.gov/publications/nistpubs/800-83/SP800-83.pdf

（平成 22 年 2 月 1 日受付）

井上大介
dai@nict.go.jp
横浜国立大学大学院で情報セキュリティを学んだ後，2003 年に通信総合研究所（現 情報通信研究機構）に入所．新世代モバイル研究開発プロジェクトでのセキュリティ研究を経て，2006 年よりインシデント分析センター nicter の研究開発に従事．2002 年暗号と情報セキュリティシンポジウム論文賞，2009 年科学技術分野の文部科学大臣表彰（科学技術賞）等を受賞．博士（工学）．

中尾康二（正会員）
ko-nakao@nict.go.jp
1979 年早稲田大学卒業後，国際電信電話（株）に入社．KDD 研究所を経て，現在 KDDI（株）情報セキュリティフェロー，および（独）情報通信研究機構（NICT）情報通信セキュリティ研究センターインシデント対策グループリーダー兼務．ネットワークおよびシステムを中心とした情報セキュリティ技術にかかわる技術開発に従事．2002 年より早稲田大学非常勤講師．本会研究賞，経済産業省大臣賞，総務省局長表彰，文部科学大臣賞等を受賞．電子情報通信学会会員．