

# Looming Security Challenges

## 不気味に迫るセキュリティの危機

ゾンビ、トロイの木馬、“ボッツ (bots)”、そしてワーム。人間は何を生み出したのか？

— デビッド・バリー (David Barry) による報告



2004年6月、ロボットすなわち“ボッツ (bots)”とも呼ばれるゾンビと化したPCの大集団がGoogle、Yahoo、その他主要なWebサイトを攻撃。これらのサイトへのアクセスが2時間にわたって遮断された。悪さをしていると思われるボットのネットワーク (ボットネット: botnet) をセキュリティの専門家が特定し、ようやく封鎖してその攻撃を止めたのである。しかし、この攻撃は、USA Today紙が最近「感染力をもったプログラムが波のように次から次へと現れてインターネットを飽和状態にし、ハッカーに乗っ取られていわゆるゾンビと化したPCの数が急増。その数は数百万に達した」と報じたものの1つにすぎなかったのである (usatoday.com 2004年9月8日)。

ゾンビのコンピュータは、まるで1960年代のホラー映画のように、墓場から蘇り住民を恐怖の底に陥れる意

思のない死人のテクニカルバージョンである。2005年、これらのゾンビがサイバースペースで動き出し、私的なネットワークとインターネットの双方に広く拡散し増殖している。ボットネットは、今日のセキュリティの脅威がパワフルで複雑であることを表す典型的な例である。

悪意に満ちた開発者がワーム、ウイルス、あるいはアプリケーションに埋め込まれた攻撃を使って、このような脅威を創り出している。たとえば、ボットネットでは、悪質な開発者はワームおよびWebトラフィックやピア・ツー・ピアの共用ファイルなどアプリケーショントラフィックの中に攻撃を隠すアプリケーション埋め込み型の攻撃を利用して“トロイの木馬 (Trojans)”を埋め込む。トロイの木馬は、ユーザのコンピュータに残される小さな実行プログラムである (本記事のコラム『トロイの木馬: 古い概念の復活』を参照)。疑うことを知らないユーザがインターネットにログオンすると (ケーブルモデムやDSL接続では自動的に行われる)、ボッツはサーバに入り込み“ゾンビマスター (zombie master)”からの指令を待つ。2004年6月に起こった事件と同じように、ハッカーはコンピュータの所有者が知らないうちに数千台のコンピュータにトロイの木馬を埋め込むウイルス攻撃を開始するのである。その後、ゾンビマスターはこれらのアプリケーションを使ってDDoS (Distributed Denial-Of-Service: 分散型サービス拒否) 攻撃の中で特定のサイトをパケットで溢れさせる、あるいは大量のスパムを創り出すのだ (29ページの図を参照)。

シマンテック社によるインターネットの脅威に関する最近のレポートによれば、毎日3万台以上のコンピュータがボットネットに“リクルート (recruited)”されている。「ボットネットは、ネットワークの環境の脅威がどれほど複雑になり、拡散しているかを顕著に表しています」とシ

スコのセキュリティ・テクノロジー・グループの製品マーケティング・マネージャであるスコット・ポープ (Scott Pope) は語る。

「さらに不幸なことに、ハッカーが創り出す攻撃はますます精巧かつ創造的になっており、それにつれて状況はますます悪化し続けているのです」

たとえば、ウイルスやワームを使ってトロイの木馬を送り込むような攻撃テクニックの組み合わせは比較的新しいものであり、ブレンド型攻撃と呼ばれている。ブレンド型攻撃は段階的に起こることもある。つまり、トロイの木馬を持ったウイルスが最初に攻撃してコンピュータ上で安全が確保されていないポートをこじ開け、アクセス制御リスト (ACL: Access Control Lists) を不能にしたり、アンチウイルスソフトウェアを武装解除したりするのだ。そして、その直後に無防備となったシステムに対して、さらに破壊的な最終攻撃を仕掛けてくるのである。

シマンテック社は2004年、「インターネットセキュリティ

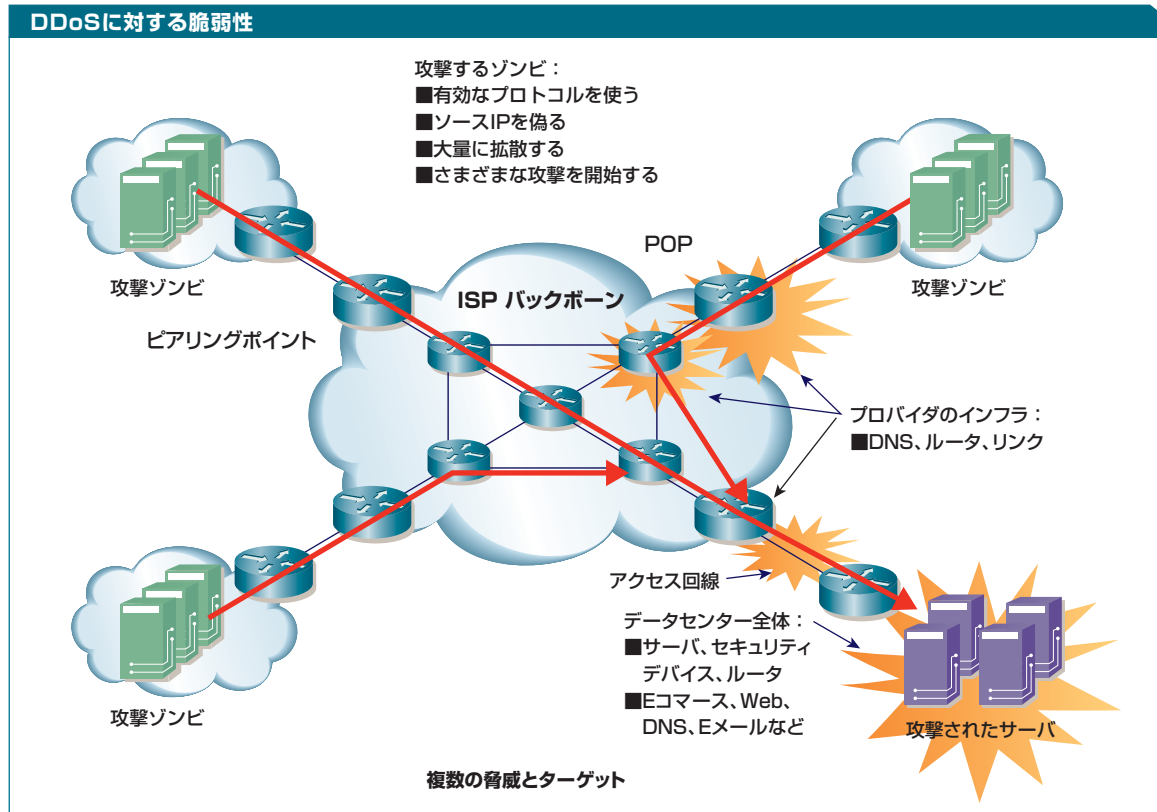
## トロイの木馬：古い概念の復活

ネットワークセキュリティの用語定義にしたがえば、トロイの木馬とは「害のないアプリケーションを装った、破壊的なプログラム」ということになる。ウイルスとは異なり、トロイの木馬は自分自身を複製することではなく、それ自体が破壊的なだけだ。最も狡猾なタイプのトロイの木馬は、コンピュータからウイルスを駆除すると偽って、実際にはウイルスを持ち込むプログラムである。

この言葉は、トロイ戦争にまつわるギリシャ神話「トロイの木馬」に由来している。すなわち、ギリシャ人が和解を装い、トロイへの贈り物として巨大な木馬を贈った逸話だ。トロイ人が木馬を都市の城壁の中へ引きずり込むと、空洞になっていた木馬の腹部に潜んでいたギリシャ兵が這い出して、城門を開け、そこからギリシャ軍がなだれ込んでついにトロイを占領した——というストーリーになぞらえているのである。

出典：[webopedia.com](http://webopedia.com)

の脅威に関するレポート (Internet Security Threat Report) ] ([cisco.com/packet/171\\_5a1](http://cisco.com/packet/171_5a1)) でワーム、ウイルス、トロイの木馬、バックドア、およびブレンド型の脅威の不正コードを分析し、個人データ、特に金融情報やパスワードを盗むために設計された悪質なソフトウェア (malware) が一層増えていることを示唆した。この



**ゾンビの攻撃：**ボットネットは、今日蔓延しているセキュリティの脅威のパワーと複雑さを表す典型的な例である

ようなデータ泥棒が増加している傾向の中で、すべての企業——特にインターネット上で支払いトランザクション処理を行う必要がある銀行やEコマース企業——が未曾有の脆弱性を呈し、危険に晒されているという。

### 進化するセキュリティの見通し

ネットワークアーキテクチャの変化と脅威の進化によって、新しいセキュリティの挑戦が行われている。その上、ネットワークの境界線への概念そのものも変わりつつある。かつてユーザは数個の入口または出口ポイントからネットワークにアクセスすることができなかった。つまり、一般的には社内ネットワークがインターネットに接続されているポイント経由でのみ、アクセスすることができたのである。そこで、各企業はインターネットの周辺にファイアウォールや侵入検知システム(IDS: Intrusion Detection System)などのセキュリティ層の構築を重ねてきた。

それに対して、今日ではネットワークに入る方法がどんどん増えている。ネットワークの境界線の環境の拡大と分散が進む中で破壊的な脅威を防ぐためには、拡大する新しい入口と出口のポイントのそれぞれにセキュリティを適用しなければならない。それが、セキュリティのアーキテクチャを一層複雑にしているのである。たとえば、VPN(Virtual Private Network)によって、社外から会社のネットワークにリモートアクセスできるようになった。その利用は、わずか2~3年前と比べても大きく広がってきている。少し前まで、企業は社内ですべての特定のコンピュータでVPNソフトウェアを実行することにこだわっていた。それが今ではユーザ自身のPCから、あるいはコピーセンターや他のオフィスからでもVPNを実行することができるのだ。

そのおかげで社内ネットワークへの侵入経路は格段に増え、IT部門にとって頭の痛い問題となっている。すなわち、そのコンピュータはウイルス防御を装備しているか、そのウイルス防御ソフトは最新のものか、コンピュータ内にワームが埋め込まれていないかという問いかけが不可欠なのだ。

セキュリティに関わるもう1つの大きな課題、それはワイヤレスLAN(WLAN)である。たとえば、最寄りの喫茶店の無防備な無線ネットワークを利用しているユーザ

は、同じ無線のサブネットを使っている悪質なPCが、自分のPCにウイルスを送り込んだことに気づかないかもしれない。その後、そのPCが社内ネットワークにつながれるとウイルスは難なくネットワークに侵入してしまう。

同時に出入口ポイント数の増大によって、攻撃に対するネットワークの脆弱性が悪化してくる。それに伴って、脅威そのものも変化しているのである。トロイの木馬やボットネット以上に危険な新しい脅威としてラーク(lurk:潜伏型)があり、その最も厄介な脅威は2つある。つまり、フラッシュの脅威(flash threats)と自己変身型ワーム(self-mutating worm)である。

フラッシュの脅威は、ウイルスやワームが拡散するスピードからそう名づけられた。1999年、「メリッサ(Melissa)」と命名されたウイルスが最も早く登場した。これは当時、最も広く拡散したものの1つであり、ネットワークアソシエーツ(現・マカフィー)社によれば、16時間で世界全体に広まった。また、2003年1月のSlammerウイルスは、よく知られたMicrosoft's SQL Serverの脆弱性を利用して、10分以下の時間で世界中にある脆弱なホストの90%以上に感染を拡大した。来月あるいは来年登場するであろうさらに新しいウイルスは、一層急速な感染力を持つことが予想される。ポーブによれば「新しいタイプのウイルスは60秒以内に数百万台のホストに感染する能力を持っている可能性があります。ですから、我々が作る防衛策は、今までよりはるかに素早く脅威を特定し、対処できるものでなければならない」のである。

もう1つの切迫した脅威、それは自己変身型のワームである。現在のワームは比較的知的レベルが低い。これは、たとえば特定のポートを通じてあるマシンに侵入し、何らかの方法でそのマシンを乗っ取ったらパッパオーバーフローを起こす、あるいはトロイの木馬を埋めこむなど一定の命令に従うようプログラムされているものである。予定された命令に何か邪魔が入った場合、ワームには適応能力がなくそのまま死滅してしまう。しかし、今では悪質な開発者がワームにインテリジェンスやロジックを追加し、特定のタスクを完了できなかった場合には、自ら変身して別種の攻撃に移ることができるようにしている。

「セキュリティのジレンマは、ムーアの法則を逆転させた

ようなものです」とポーブは語る。

「ムーアの法則は18ヵ月ごとにプロセッサのパフォーマンスが倍になり、一方コストは大幅に下がると仮定しています。これに対して、セキュリティは逆の方向へ動いているのです。つまり、ネットワークの安全性が低下すればするほど防衛のためのコストが増大しているのです」

イギリスにあるコンピュータセキュリティ専門の調査会社mi2g社(mi2g.org)も、この予測を支持している。敵意を持ったネットワークセキュリティへの攻撃による経済的損失は、2004年には世界全体で1570億ドルから1920億に上るだろうとmi2g社は報告している。

### 新しい脅威との戦い

現在のセキュリティ防衛の典型的な形態は、ネットワークの個々のセグメント全体にわたり、既存のテクノロジーを逐次的に追加していくというものである。ここにはアクセスを遮断し、アプリケーション検査を行うファイアウォールやACL、さらに非常にきめ細かいトラフィック検査の実行によって、既知の脅威を識別する侵入防止システム(IPS: Intrusion Protection System)、盗聴に対抗する暗号化ソフトウェア、ワームやDoS攻撃を検知する異常検知、およびウイルスと戦うアンチウイルスソフトウェアが含まれている。今日のセキュリティテクノロジーの多くは、特定の機能を遂行するために開発されたものであり、ネットワークに脅威となる環境全体の状況はほとんど考慮されていないというも事実だ。また、各テクニックの能力の間に“セキュリティのギャップ(security gaps)”が存在するために、これらのテクノロジーを単独で使っても新種の攻撃を阻止するための効果が期待できないだけでなく、ユーザがネットワークにアクセスする方法を変化させてしまうことにもなる。

さまざまな技術を組み合わせてネットワークを破壊するブレンド型のように、脅威はますます複雑になっている。そこで、攻撃を阻止して、ネットワークの活動とアプリケーションに対するコントロールを改善するには、セキュリティテクノロジーも相互に協調して動作しなければならない。

残念ながら、多くの企業では長年にわたって個別の問題に直面するたびに、その都度デバイスやソフトウェアを追加し続けてきた。それが逆に、深刻なセキュリ

ティの問題を抱える結果を招いてしまったのである。つまり、整合性がとれないまま、アンチウイルスやファイアウォール、VPN、および侵入防止策がバラバラに林立するという状況を生んでしまったのである。

短期的なニーズにとらわれ、近視眼的な対処を施している間に、個々に独立して作動する多くのシステムの林立という、さらに大きな問題を生み出してしまったのだ。しかし、実際には進化した脅威が登場すればするほど、セキュリティは包括的なものになるべきであり、ますます高度化する脅威の検知にはセキュリティテクノロジーが協調して防衛に当たらなければならない——それがポーブをはじめとする多くの人々の確信である。

「パズルのピースをつなぎ合わせて、従来のネットワークセキュリティシステムにあるギャップを埋めることができる、そんなデバイスに対するニーズが高まっています」とポーブは説明する。

「現在、脅威を正しく分類できない、あるいは組織的で適正な対応がとれない、さらに悪いことには、最終的に脅威そのものを見失ってしまうことによって非常に大きな問題が起こっているのです」

### 変化する世界に適応できるセキュリティ

このような混沌状態を、明解で管理可能なセキュリティポリシーに変えることが非常に重要だ。それが、将来のネットワークセキュリティシステムがコンバージェンスと統合に焦点を絞らなければならない理由なのである。ネットワークセキュリティでは、事前に対策を講じるアプローチが不可欠である。これは、できるだけ早く、その攻撃が標的としたホストから遠いうちに、正体を正確に見極めて阻止すること、そしてそれを実行するのに必要なセキュリティアーキテクチャを簡素化するという考え方である。数多くのセキュリティ機能を、適応力を持った1つのデバイスまたはシステムに統合することで、その複合的な機能が協力して防衛に当たり(サイロ型ではなく)さらに広範な攻撃を阻止し、また展開しなければならない多種多様なデバイスの数を大幅に減らすことができる。その結果、セキュリティの設計と管理が簡素化されるのである。

一般に、ファイアウォールはかなりシンプルなデバイスだが、レイヤ3およびレイヤ4の情報とセッションの状態

に基づいてパケットを遮断したり、通過させたりするのに効果的だと考えられてきた。これは、ある程度のアプリケーション検査機能を提供することができるが、ある種のテクノロジーのような詳細な検査を実施できるわけではない。IPSデバイスは、パケットの中身をさらに深く見て、そのデータが会社のポリシーに適合しているか否かを見極める。そのおかげで、従来のファイアウォールがやり残した部分を補完することができるのである。しかし、IPSデバイスにはネットワークセキュリティ管理者が必要としている広範な緩和策とファイアウォールのレジリエンスに欠けている。そこで、ファイアウォールとIPSデバイスを組み合わせると、単独で機能させた時よりもはるかに効果が高まる。たとえば、IPSデバイスはファイアウォールが見逃してしまう可能性があるアプリケーションに埋め込まれた攻撃を捕えることができる。一方、IPSデバイスはファイアウォールのような攻撃に対する適切な取り締り行動ができない。そこで、ネットワークセキュリティ管理者はファイアウォールとIPSの能力を統合することによって、IPSの検査のインテリジェンスをすべて備えながら、ファイアウォールの緩和対策とレジリエンスも手に行うことができるのである。

IPSデバイスは、その他ネットワークトラフィックに対する非常にきめの細かい観点を持っているが、それはシグネチャベースである。つまり、前もって何を見張るのかを知らせるアップデートを受け取っていないと制約を受けるのだ。シグネチャのアップデートには24時間から48時間かかることがあり、そうなるともしかしたら明日受けるかも知れないフラッシュの脅威には効果を発揮できなくなる。ここで、ダイナミックに発生を阻止するアップデートを備えたネットワークのアンチウイルスソフトウェアの出番である。アンチウイルスソフトウェアは極めて迅速にアップデートすることができ、インフラを通じてすべてのエンドポイントに情報を流すことができる。そこで、このインフラがIPSおよびファイアウォールと合体すれば、企業は個々の単独パワー以上のものを得ることができるのである。つまり、セキュリティの脅威に対処する防衛システムができ、迅速に情報をアップデートし、ワームやウイルスを識別するためにパケットを詳細に分析する手段を得ると同時に、そのようなパケットのネットワークへの侵入を阻止するファイアウォ

ールの機能とレジリエントの高いソリューションも実現されることになるのだ。

このような体系的なアプローチは、受身的なモードで別個のサイロ型テクノロジーとして作用し、検知方法も限定的かつ静的なセキュリティを変革する。つまり、脅威の環境に適応して協調しながら、脅威に対して先制的に防御するセキュリティへと変身させてくれるのだ。

ポーブによれば、このようなシステムは検知の改善、イベント分類精度の大幅な向上、運用コストの削減、管理の合理化、そして最先端のセキュリティテクノロジーが開発されると同時に統合するサービスの拡張能力という数多くのメリットを提供してくれる。ここで最も重要なポイントは、このような統合されたシステムはどのようなカテゴリでもQoS(Quality of Security)で妥協することがなく、むしろ個々の持つ力を相互補完するよう組み合わせ、より堅固で組織的な防衛を実現することである。

#### レジリエンス(耐障害性・障害回復力):

レジリエンスとは、障害を未然に予測して、システム障害に至る致命的なエラーを回避するとともに、万一障害に陥った場合でも早急にシステムを復帰させることができる能力を指している。

#### 詳しい情報

- シスコのセキュリティとVPNの情報(Cisco Security and VPN Information): [cisco.com/jp/go/security](http://cisco.com/jp/go/security)
- シスコの自己防衛型ネットワーク(Cisco Self-Defending Networks): [cisco.com/japanese/warp/public/3/jp/event/offer/powernow/security/](http://cisco.com/japanese/warp/public/3/jp/event/offer/powernow/security/)
- シスコの侵入防止アラートセンター(Cisco Intrusion Prevention Alert Center): [cisco.com/go/ipsalert](http://cisco.com/go/ipsalert)
- SANS Instituteのインターネットストームセンター(SANS Institute Internet Storm Center): [isc.sans.org](http://isc.sans.org)
- eSecurityプラネットオンライン(eSecurity Planet Online): [esecurityplanet.com](http://esecurityplanet.com)
- SecurityTracker: [securitytracker.com](http://securitytracker.com)
- 「ハッカーはあなたのPCを使ってスパムをばら撒いたり泥棒をしたりしていませんか? (Are hackers using your PC to spew spam and steal?)」(USA Today紙 2004年9月): [usatoday.com/tech/news/computersecurity/2004-09-08-zombieuser\\_x.htm](http://usatoday.com/tech/news/computersecurity/2004-09-08-zombieuser_x.htm)
- 「作成者のための泥棒するコード(Code that steals for its creators)」(NetworkWorld-Fusion.com 2004年3月): [nwfusion.com/weblogs/security/004453.html](http://nwfusion.com/weblogs/security/004453.html)