特集

ネットの脅威と防衛技術

その最新手口と対策を一挙公開

最近のネット社会では、さまざまな方法での攻撃行為や詐欺行為など、多くの「脅威」が蔓延している。その手口はますます巧妙化し、もはや一般社会で本能的に脅威から逃れていた人であっても、ネット上では安心できる状況ではなくなってきている。
こうした「脅威」は個人に限らずとも、企業としても重要な問題となっている。自社のサイトを踏み台にされたり、または自社の名前を使って詐欺行為を働かれたりする危険もあるのだ。これこそネット社会における企業の信用問題にまで発展している出来事だ。
犯罪ともいえるこれら「脅威」の手口を知ることが、最も有効な対抗策ともいうことができる。

企画協力：NPO日本ネットワークセキュリティ協会　http://www.jnsa.org/

CONTENTS

Illust:©HIKARI production

Part1 ネットの脅威の現状

愉快犯の時代は終わり、さらに巧妙化し犯罪化する脅威のトレンド

野々下 幸治
株式会社シマンテック 法人営業事業部 エグゼクティブシステムエンジニア

変化を見せるネットの脅威

ここ数年、インターネットの環境の変化とともに、セキュリティーの状況は毎年のように新たな脅威が現れ、その度に新たな対策が必要とされている。

2000年はYahoo!やeBayなどに大規模なDDoSの攻撃が行われ、日本では官公庁のウェブの改ざんが相次ぎ、インターネットのネットワークのセキュリティーに大きな関心が集まった年だった。また、ウイルスとしてはメールによって感染するLoveLetterウイルスが世界中で感染を広げた。

この当時、インターネットに広いバンド幅で常にコンピュータがつながり、また、セキュリティーの甘いマシンが存在するのが大学のネットワークだった。したがって、DDoSの送信元として踏み台に使われたのは大学ネットワークのUNIXのコンピュータで、ウェブの改ざんとともに、サーバーの対策の強化が謳われた。

2001年、CoderedとNimdaの2つのワームが脆弱なサーバーに次々と感染する事件がインターネット上を襲った。この複合型の脅威により、セキュリティー対策にも新たな方法が必要になった。これは従来ウイルス対策とネットワークセキュリティーは別に考えられていたが、サーバーのパッチ対策が大きな問題となるとともに、ファイアーウォール、アンチウイルス、侵入検知などの複数のセキュリティー製品による対策がいわれた。

2003年にはSlammerが十数分で世界中に大規模な感染を引き起こし、米国ではATMのストップなど、生活に関わるシステムにまで影響を及ぼした。また、同じ年の夏にはBlasterとWelcheaが世界中のクライアントPCに感染し、クライアントの脆弱性が大きな脅威として認識された。

2004年の2月ぐらいから、BeagleやMyDoomの大規模なメールにより拡散するワームが大流行し、これとともにインターネットの脅威は大きく変

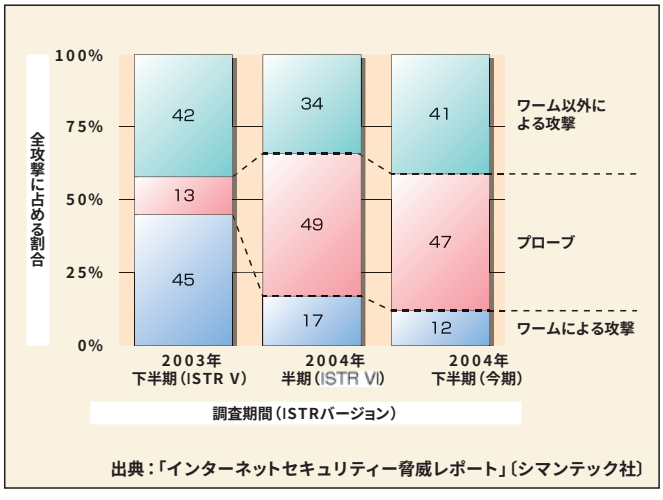


図1 攻撃タイプ

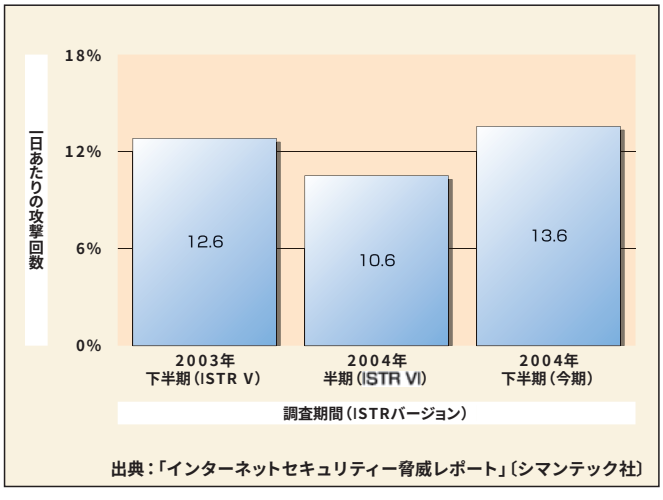


図2 1日当たりの攻撃回数

化してきている。

これまでのワームの作者はどちらかといえば、自身の技術を誇示するための愉快犯的な作者で、ワームの亜種も限られていた。ところが、BeagleやMyDoomに始まる2004年のワームの作者は組織的に行われていて、それを表すかのように次々と亜種が開発されて、拡散している。

たとえば、CodeRedの場合は5つの亜種、Nimdaの場合も2001年9月18日W32.Nimda.Aが発見され、W32.Nimda.Rが2003年6月17日と亜種の種類も出現頻度も非常に低くなっている。一方Beagleは2004年1月18日にW32.Beagle.Aが発見され、2004年4月21日時点でW32.Beagle.BPと短期間の間に多くの亜種が生まれている。

また、それとともにBotnetの拡大、トロイの木馬の増加とブロードバンドの増加に伴って、攻撃の対象が常時接続されて、しかもセキュリティー対策がしっかりしていない家庭のコンピュータとなってきている。また、インターネット上での経済活動が大きくなるに従い、犯罪組織にとってもインターネットが魅力的なものとなってきている。

攻撃数と攻撃タイプ

その変化の状況はシマンテック社が1年に2度発行している「インターネットセキュリティー脅威レポート」の中の統計データからも読むことができる。これはインターネット上の脅威に関する分析情報を6か月ごとにまとめた報告書だ。この報告書には、ネットワーク上の攻撃、既知の脆弱性、悪意のあるコードおよび各種セキュリティーリスクの分析や顕著な傾向が含まれている。実際のその中の具体的な統計データを元に2004年の脅威の状況を具体的に見ていこう。

図1の攻撃タイプのグラフを見てみると、明らかに2004年になって変わっている。2003年まではワームによる攻撃と判断されるものがインターネットの攻撃の半分近くを占めていたのだが、2004年からはその割合が大きく減ってきている。なお、図2に示すように全体的なインターネットの攻撃自体の数は変わっておらず、むしろ増えている。

よって、一見すると、これはワームの活動が減りって人による攻撃が増えてきたかのように見えるが、そうではない。2004年前半に大流行したBeagleやMyDoom、Sobigなどに代表されるマスメールの大きな感染は通常のメール通信として感染を広げるため、ファイアーウォールのログやIDSでは検知できない。最近になって増えているウェブの訪問によるクライアントの脆弱性を利用したワームの感染も通常のHTTP通信として判断されるために検知されない。また、Welchiaに代表されるように感染を効率的に行うために、最初に攻撃対象が脆弱な部分を持っているかどうかをスキャンした後に攻撃を行うものはスキャンニングとして捕らえられる。また、PHPの脆弱性を狙って拡散したSantyワームはインターネット上の検索エンジンを使って直接PHPを利用しているウェブサーバーを攻撃した。このようにランダムに手当たり次第に感染活動をしていた従来と比べ、ワームも感染を効率的に行うようになったり、対象がクライアントやウェブアプリケーションに移ってきたりしているため、結果としてワームの攻撃としての分類がしにくくなってきている。

これは表1の攻撃対象ポートトップ10にも表れており、従来は80番ポートのHTTPサービスが1位だったが、ランク外になっている。これはWelchiaの亜種がWebDAVによる攻撃を2004年6月1日に停止したため、その影響も出ている。

インターネット上の攻撃タイプの数についても従来は上位がほとんどワームによるもので占められていたが、表2の攻撃回数トップ10にはランク外であったSYN Flood攻撃が2位に出てきている。

ウイルス命名の最後のアルファベットが亜種を表す。BPの場合は68番目の亜種となる。ボットの亜種はさらに多く、W32.Spybotの場合、4月24日の時点で、W32.Spybot.OBZまでなっている。

攻撃対象となるシステムに直接感染するような攻撃をランダムに行った場合、対象のシステムが攻撃対象となるサービスを提供していない場合は、TCPの接続のタイムアウトで待たされる。最初にスキャンを行い、対象となるサービスの提供と脆弱性の確認をすることにより、より効果的に感染させることができる。

2004年 下半期順位	ポート	サービス	2004年 下半期 攻撃者の割合	2004年 上半期 攻撃者の割合
1	445 TCP	CIFS (Microsoft File Sharing)	35%	17%
2	135 TCP	DCE-RPC (Remote Microsoft Windows communication)	17%	15%
3	1026 UDP	Various dynamic services	8%	3%
4	4662 TCP	Edonkey (File-sharing)	6%	7%
5	1027 UDP	Various dynamic services	5%	NA
6	6346 TCP	Gnutella (File sharing)	5%	5%
7	139 TCP	SMB (MicrosoftFile Sharing)	4%	NA
8	1025 TCP	Various Backdoors and dynamic services	2%	3%
9	1434 UDP	Microsoft SQL Services	2%	NA
10	25 TCP	SMTP Services	2%	NA

出典：「インターネットセキュリティー脅威レポート」（シマンテック社）

表1　攻撃対象ポートトップ10

2004年下半期順位	2004年上半期順位	内容	2004年下半期割合	2004年上半期割合
1	2	Microsoft SQL Server Resolution Service Stack Overflow Attack	22%	15%
2	(ランク外)	Generic TCP Syn Flood Denial of Service Attack	12%	NA
3	10	Microsoft Windows DCOM RPC Interface Buffer Overrun Attack	7%	1%
4	6	Generic SMTP Malformed Command/Header Attack	5%	2%
5	2	W32.HLLW.Gaobot Attack	4%	4%
6	(ランク外)	Generic Invalid HTTP Version String Attack	4%	NA
7	7	Generic ICMP Flood Attack	3%	2%
8	3	Generic WebDAV/Source Disclosure "Translate: f" HTTP Header Request Attack	2%	4%
9	9	Generic HTTP Directory Traversal Attack	2%	1%
10	(ランク外)	Generic UTF8 Encoding in URL Attack	2%	NA

MS SQL Server Resolution Stack Overflow Attackが3期連続で首位
Generic TCP Syn Flood Denial of Service Attackが新たにランクイン。DoS攻撃の古い手法の復活の可能性。

出典:「インターネットセキュリティー脅威レポート」(シマンテック社)

表2　攻撃回数トップ10

亜種についてはそのウイルスの名前の最後のアルファベットを見るとわかる。たとえば、Spybotにいたっては W32.Spybot.AAA となっており、すでにアルファベット3文字になっている。

また、このSYN Flood攻撃の多くが攻撃元のIPアドレスが偽装されており、シマンテックではボットを使った攻撃ではないかと見ている。特にWindows XPになり、Rowソケットが使えるようになり、IPアドレスの偽装が可能になった。また、一部のネットギャンブルサイトではDDoS攻撃によりギャンブルサイトを使えなくするという金銭の恐喝を受けたりしている。

悪意のあるコードの傾向については、2003年の下半期には報告件数トップ50の悪意のあるコードのうち36%が秘密情報を盗み出すタイプのものだったのに対し、2004年下半期には57%まで増加している。

また、それと同時にトロイの木馬もトップ50の悪意のあるコードのうちの33%を占め、2003年下半期の15%から倍以上に増えている。この傾向は今年も続いており、4月1日から4月25日までに発見された132のウイルスの内、34がトロイの木馬になっている。たとえば、PWSteal.Bancosは当初ブラジルの銀行をターゲットにキーロギングを行っていたが、4月26日に発見されたPWSteal.Bancos.Tでは日本の銀行も含まれている。実際に海外ではトロイの木馬により、銀行のIDとパスワードを盗まれ、金銭を盗まれた事件が発生している。よって、フィッシングにおいてもこれまでの偽のメールおよび偽のウェブサイトへの注意だけでは対応できなくなっている。

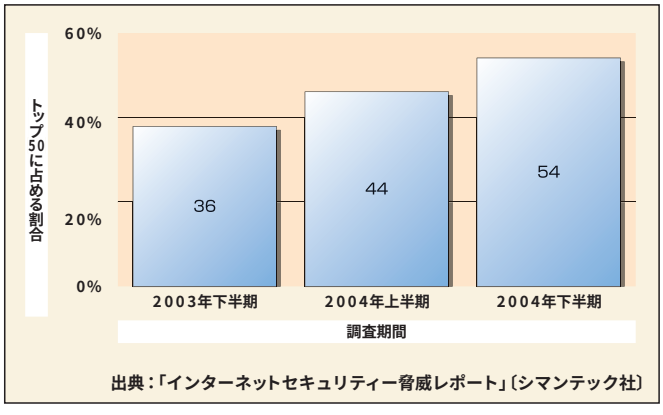
ボットに関してはSpybotにいたっては2004年下半期だけで、4288もの亜種が報告された。特にボットの亜種の多さは顕著だが、他のワームやトロイの木馬でも亜種が多くなっている。これはこれまでのウイルスの傾向と大きく異なっている。このような亜種の多さは1つにはアンチウイルスソフトの対策への対抗措置とも考えられる。

そして、これらのトロイの木馬やボットの感染の元となっているのが、大量のメール送信や、そのメールにつけられるウェブのリンクのクリックによって、システムに侵入している。

ブラウザーの脆弱性

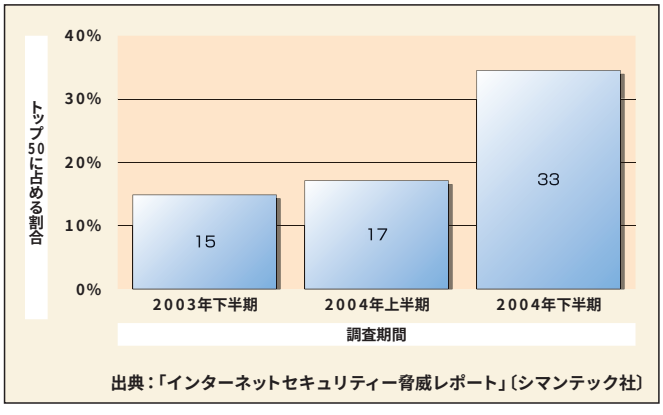
それを裏付けるかのように、図5に示すブラウザーの脆弱性の傾向を見てもわかるように、ブラウザーの脆弱性は増えており、そのブラウザーの脆弱性を使ったワームも増えている。特にIEについてはSP2の提供によって、若干下がったようにも見えるが、深刻度の高い脆弱性の割合に関してはMozila系ブラウザーより高くなっている。

ブラウザーの脆弱性のような受動的な攻撃は攻撃対象を罠に誘い込む必要があり、以前は攻撃



出典:「インターネットセキュリティー脅威レポート」(シマンテック社)

図3　秘密情報をねらう悪意のあるコードの傾向



出典:「インターネットセキュリティー脅威レポート」(シマンテック社)

図4　トロイの木馬の傾向

の効率として非効率であったものが、スパムメールなどの大量メール送信により、効果的に行えるようになってきている。メールの添付ファイルについてはアンチウイルスソフトで駆除されると共に、ユーザーも添付ファイルには気を付ける。しかし、メールに含まれるURLはアンチウイルスソフトを通過し、ユーザーもそれに対しては無防備だ。

そのようなボットやトロイの木馬などの感染対象として狙われるのはブロードバンド先進国だ。表3にボット感染国のトップ10を示しているが、イギリスがトップだ。イギリスは2004年にブロードバンド接続が飛躍的に伸びたために、ボット感染マシンの全世界での割合が非常に高くなっている。

ブロードバンドの発達に伴って、常時接続のコンピュータが増え、それらのコンピュータのボットやトロイの木馬の感染がインターネットの脅威の状況を大きく変えてきている。

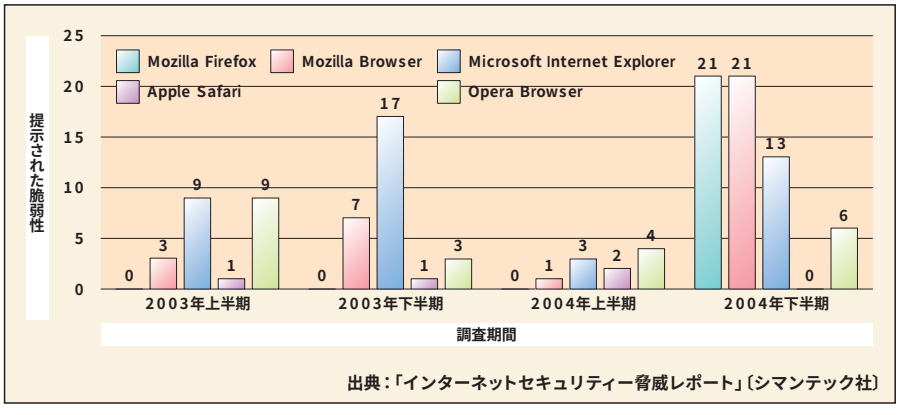
スパムについても、以前は不適切な設定のメールサーバーが狙われていたが、現在ではボットやトロイの木馬に感染したマシンが踏み台に使われるため、いっそうスパムへの対策を難しくしている。また、ボットやトロイの木馬がフィッシングの偽造ウェブサイトに使われたり、直接キーロガーなどでIDやパスワードを盗まれたりし、ユーザーのフィッシング対策も難しくしている。さらにはボットを使ってのDDoSによるウェブサイトへの金銭要求の脅しに使われたりしている。このようにブロードバンドの発達と金銭目的のインターネットの脅威によって、新たな時代を迎えようとしているのかもしれない。

なお、今回引用した「インターネットセキュリティー脅威レポート」の元となっているデータは、シマンテック社が保有するつぎのようなインターネット上の数々の情報源から得られている。

1）Symantec DeepSight™ Threat Management SystemおよびSymantec™ Managed Security Servicesにより、世界180か国以上に約20,000のセンサーを置いてネットワーク上の活動を監視しており、インターネット上の脅威に関するデータは世界でも有数の広範なものである。
2）同社のウイルス対策ソフトを導入している法人および個人のクライアント／サーバ／ゲートウェイシステム1億2000万台から、悪意のあるコードやスパイウェア、アドウェアに関するデータを収集している。
3）シマンテック社には、世界最大級のセキュリティー脆弱性のデータベースがあり、現在2,000社、20,000種類を超える製品について、11,000種以上の脆弱性を記録している。
4）シマンテック社はインターネットの脆弱性についての公表や議論を行う人気フォーラムBugTraqを運営している。
5）Symantec Probe Networkでは、200万件のおとりアカウントを使って世界20か国から電子メールメッセージを集め、スパムやフィッシングの活動をグローバルに監視している。

これら多彩な情報源を元に、シマンテックのアナリスト陣は攻撃や悪意のあるコードの最新動向を把握し、半年に一度インターネット脅威レポートして報告している。レポートの日本語の完全版は下記のURLより入手可能である。

http://www.symantec.co.jp/region/jp/istr/



出典：「インターネットセキュリティー脅威レポート」（シマンテック社）

図5　ブラウザーの脆弱性の傾向

順位	国名	ボット感染マシンの割合
1	イギリス	25.2%
2	アメリカ	24.6%
3	中国	7.8%
4	カナダ	4.9%
5	スペイン	3.8%
6	フランス	3.6%
7	ドイツ	3.5%
8	台湾	3.1%
9	韓国	3.0%
10	日本	2.6%

出典：「インターネットセキュリティー脅威レポート」（シマンテック社）

表3　ボット感染国のデータ

Part 2 個人への脅威

フィッシング
巧みな誘導で個人情報が収集される

河岡 忠広
日本アイ・ビー・エム システムズ・エンジニアリング株式会社
主任IT スペシャリスト

フィッシングとは、インターネットなどのネットワークを利用して個人の情報を盗み出す行為である。英語で「phishing」と書くが、sophisticated と fishing を組み合わせた造語であり、巧みに誘導して個人の情報を釣り上げるという意味である。

手口 Threat

フィッシングの手口としては、銀行やクレジットカード会社、EC サイトなどからのメールを装って、無差別にメールを送信し、メールの受信者に偽のホームページにアクセスするように仕向け、そのページでクレジットカード番号などの個人の情報を入力させて盗みだす行為が一般的である。メールの本文にはたとえば、「キャンペーン期間中につき抽選でプレゼントがもらえます。つきましては当社のサイトにアクセスして申し込んでください」などといった内容で、メールの受信者を誘い出すための偽のウェブサイトへのリンクを掲載し、ユーザーがそのリンクをクリックすると、実在のウェブサイトに見せかけたサイトにつながり、そこで個人の情報を入力させて情報を入手する。

フィッシングを試みる詐欺師（フィッシャー）が聞き出そうとする個人の情報は、クレジットカード番号、ID、パスワード情報、住所、氏名、電話番号などである

フィッシャーは、これらの情報を悪用して現金を引き出したり本人になりすまして不正な売買をしたりすることなどを目的とする。 別の手口としては、表面的には一見本物の EC サイトであるが、実際は入力した個人情報を盗み出すための詐欺サイトであり、ユーザーが合法的なサイトだと信じてユーザー登録し、自分の個人情報を入力することでその情報を不正取得する方法などもある。このようなサイトは、検索エンジンなどで見つかることもあるため、利用者は合法的なサイトだと信じて、被害にあってしまう。

フィッシングはこのようなユーザーをだまして個人の情報を入手するソーシャルエンジニアリング的な手法がメインであるが、別の手法も存在する。 たとえば、メール中のリンクをクリックすると、メーラーのセキュリティーホールをついてパソコンの中にキーロガーをダウンロードし実行させる手口もある。キーロガーにより、ユーザーのキー入力を記録し、フィッシャーはその情報を入手する。

なお、キーロガーのような不正プログラムの配布に使われるサイトは、偽のホームページだけではなく、ブログサイトなどに仕込まれることもある。

こういったユーザーに気づかれないように個人の情報を入手するステルス型の手口も存在する。

ファーミング：キーロガーなどの不正プログラムを仕込んで個人情報の詐取をはかる手口をファーミング（Pharming）と呼ぶこともある。これは、フィッシング（Phshing）が釣り（Fishing）に基づいた造語であるのに対して、農業（Farming）をもじった造語である。フィッシングが偽メールという餌”をまくことに対して、ファーミングでは餌をまかなくても、“種”として不正プログラムを仕込んで個人情報を収穫することから来ている。その他のファーミングの手法としては、OS の hosts ファイルを書き換えて、アドレスバーに入力したウェブサイトとは別のサイトにアクセスさせるものや、DNS（ドメインネームシステム）サーバーのデータを書き換えてユーザーを偽サイトに誘導する“DNS キャッシュポイズニング”などが知られている。

ウェブサイトに誘導しないフィッシングもある。個人情報を入力する HTML フォームを含むメールを送って、直接詐取をはかろうとする方法もある。

対策
Defence

個人の対策としては、第一に、怪しいスパムメールは無視することである。少しでも怪しいリンクはクリックしない、仮にクリックしてしまったとしても個人情報の要求には決して答えないということが重要である。なんらかのリアクションを示すことは今後も同様のスパムメールを受けるリスクが高まる。

第二に、メールが正規のものであるかどうかわからない場合には、その真偽を確かめるべきである。電話やメールなどで確認をとったり、URLを入力して本当のサイトにアクセスしたりして、そのような連絡が本当なのかどうかを確認すべきである。

また、メールのメールヘッダーを確認して送信元の詐称がないかどうかをチェックしたり、サイトにアクセスしたりした場合にはアドレスバーを確認し、正規のURLでないかどうかをチェックすることも安易なフィッシングに対しては有効である。クレジットカード番号などをうっかり入力してしまった場合には、カードの利用を停止するなどして、被害にあわないための策を速やかに講じるべきだ。

また、クレジットカードの利用明細や銀行の通帳などを定期的にチェックして、身に覚えのない取引がないかどうかを確認することも重要である。次に、フィッシング対策ツールを導入する方法がある。たとえばフリーのツールであるSpoofStick（http://www.corestreet.com/spoofstick/）は、URLを偽装したサイトに対しても、本当のURLを表示する機能を持つ。このような手段でフィッシング詐欺を未然に察知することが可能となる。

また、前述のキーロガーのような不正プログラムを仕掛けられることがないよう、日頃からセキュリティパッチをこまめに適用しセキュリティーホールを放置しないよう心がけるべきである。最後に、万が一被害にあってしまった場合やフィッシングサイトを発見した場合には、最寄りの警察署か都道府県警察本部のサイバー犯罪相談窓口（フィッシング110番）に相談すべきである。

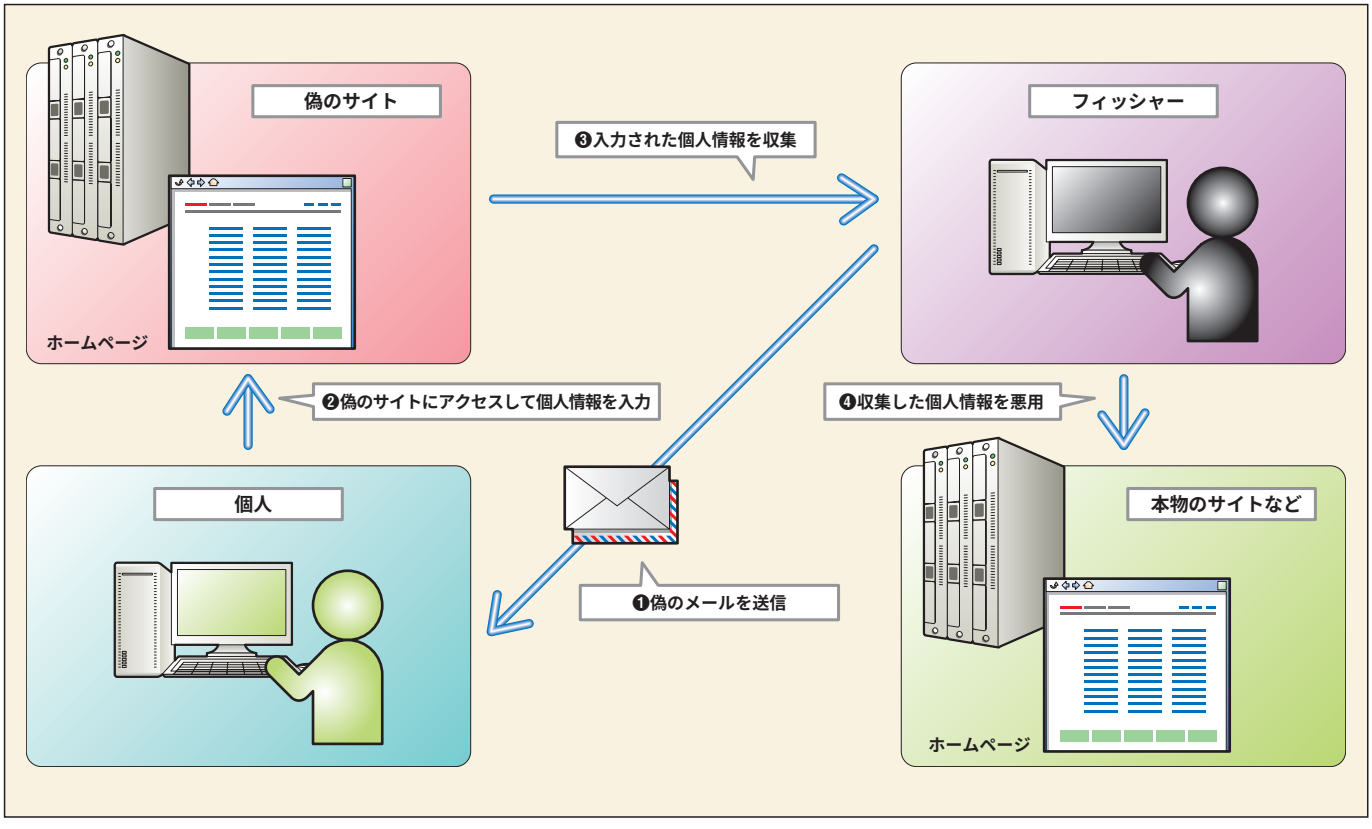


図6　フィッシング詐欺の手口

Part 2 個人への脅威

ウイルス／ワーム 知っているはずなのに、なぜ感染するのか？

二木 真明
住商エレクトロニクス株式会社 ネットワークセキュリティ事業部
副事業部長（技術担当）

**ネットワークが普及する以前から愉快犯的にばらまかれているウイルス、
そしてネットワーク時代になり急速に広まるワーム。
その存在は十分に知られているはずなのにまだまだその被害は大きい。**

ウイルス（コンピュータウイルス）：本来は、コンピュータ上のプログラムやデータファイルに寄生することで、そのプログラムの実行を通じて破壊行為や感染の拡大を行うような寄生型の悪性プログラムのことだが、現在では、ワームなどを含めた悪性プログラム全体の代名詞として使われることのほうが多い。

ワーム：本来の意味でのウイルスのように、なんらかの宿主プログラムに感染するのではなく、コンピュータ内部で独立したプログラムとして行動するタイプの悪性プログラムのこと。最近のメール感染型ウイルスと言われるものの多くが、厳密にはワームと呼ぶべきであるほか、ネットワークを経由して攻撃・侵入するようなもののほとんどはワームと呼ばれるべきものである。

手口 Threat

コンピュータウイルスという言葉はいまでは誰でも知っている。怪しい電子メールに添付されたファイルを開いてはいけないことや、怪しいURLへのリンクをクリックしてはいけないことも多くの人が知っている。にもかかわらず、感染事故が後をたたないのはなぜか。その原因の1つに、インターネット利用者層の急拡大と、ウイルスやワームを作る側がより巧妙になってきていることがある。

電子メールで拡散するタイプのウイルスやワームは、そのほとんどが添付ファイルを開いたり、メールに書かれたURLをクリックしたりしなければ感染しない。一般に少し知識があるユーザーならば躊躇するはずのこうした行為を行わせるために、最近のウイルスは巧妙に細工されている。こうした手口は基本的にフィッシングなどとも共通する。友人からのメールや信頼できる組織からのメールを偽装するために、発信者名やメールアドレスを詐称したり、興味を引きそうな表題や添付ファイル名などを使用したりする。単純なことのようだが、たとえばREADMEのようなファイル名がついているだけで、それをうっかり開いてしまう利用者はかなり増えるはずだ。

また、あたかも自分が出したメールがメールサーバーからエラーで戻ってきた時のエラーメッセージを偽装したようなものも増えている。不思議に思って、ついつい添付ファイルを開いてしまうことを意図したものだ。ウイルスの内容は昔とそれほど大きく変わってはいないが、ユーザーの心理を悪用して感染させるための手法はどんどん巧妙化しているのだ。

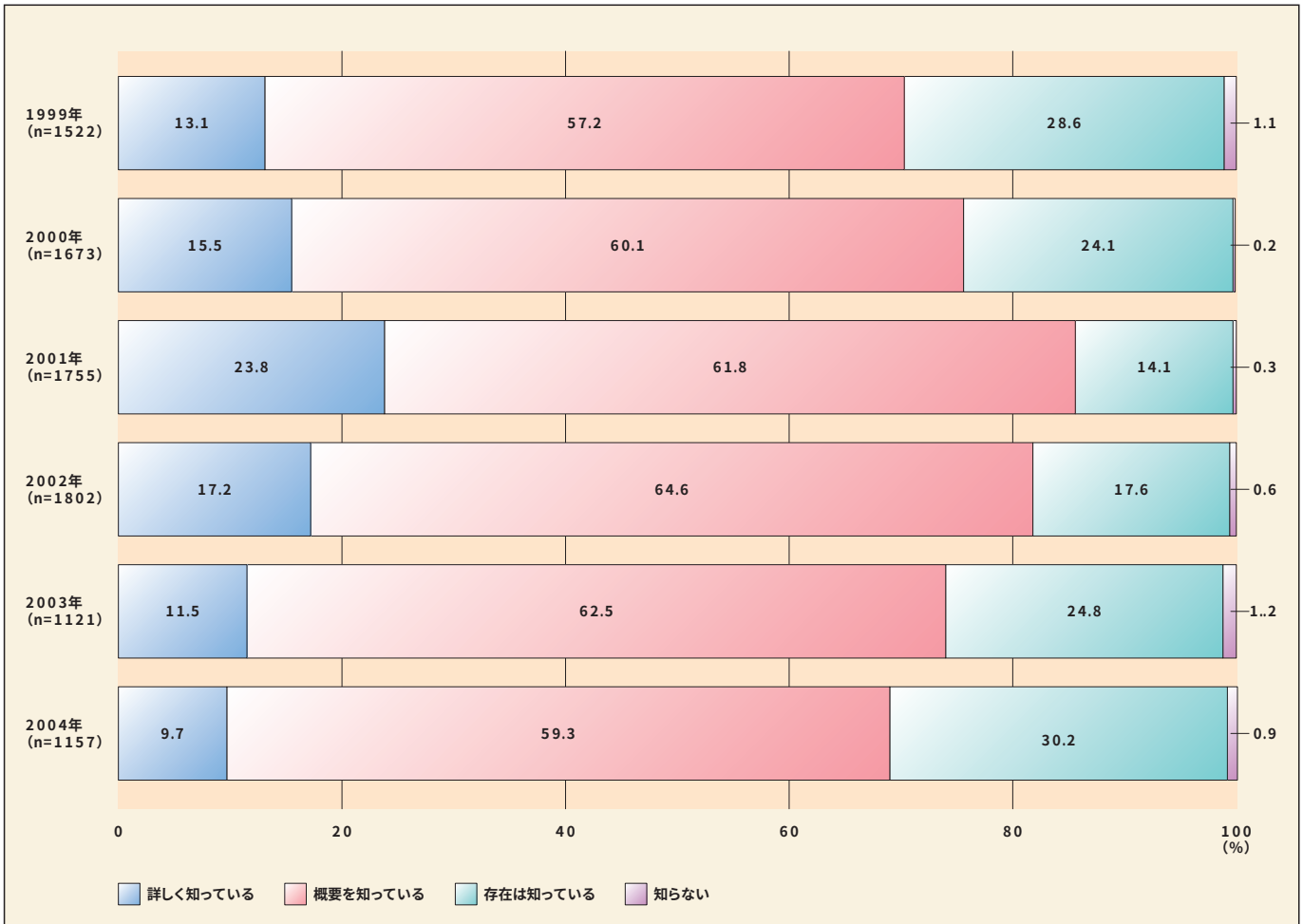
セキュリティーホールを攻撃するタイプのワームもまた脅威だ。たとえば2年前に買ったPCをリカバリーCDで復旧して、そのまま、直接インターネットにつなぐと、セキュリティーパッチをダウンロードする間もなくワームに感染してしまうだろう。インターネットには常にワームの通信が流れているからだ。

ウイルスやワームの作者が狙うのは、どちらかといえばPCやインターネットの利用にまだ不慣れな人たちだ。言葉では知っていても、ウイルス対策ソフトでは防ぎきれないウイルスがあることをきちんと理解していないような層である。急拡大していくインターネット利用を背景にウイルスやワームも増え続ける初心者層（図7参照）を狙ってさらに巧妙なものになっていくに違いない。

対策
Defence

技術的な意味では根本的な対策はいまのところないといってもいい。最低限の対策はいい尽くされたことだが、ウイルス対策ソフトの導入と常に最新のパターンファイルに更新を行っておくこと。これだけで、まったく新種のウイルスを除いて感染する危険はほとんどなくなる。また、ワーム対策として、こまめにセキュリティーパッチ（修正プログラム）を導入することや、インターネットに直接接続するPCにはパーソナルファイアーウォールなどの防御ソフトウェアを必ず導入しておくことなども重要だ。家庭で使うならば、ブロードバンドルータなどを使って接続し、そのファイアウォール機能などを使うことでインターネットからのワーム感染は防止できる。それでも残る新種ウイルスやワーム感染リスクへの対策は、先に述べたようなウイルス作者の手口を知ることで、それにひっかからないユーザーを増やしていくことしかない。たとえば、完全にウイルスフリーなOSでもできない限りは、こうしたユーザーとウイルス作者との競争はいつまでも続いていくだろう。

未知ウイルスと対策ソフト：最近のウイルス対策ソフトウェアの多くが、未知ウイルスに対応するなんらかの機能を持っている。かなり高い確率でまったく新種のウイルスをパターンファイル更新なしで検知できるのだが、決して確実ではない点は注意が必要だ。見落としや誤認の可能性とともに、ウイルス作者が対策ソフトウェアを入手し、検知できないことを確認することができる点にも留意する必要があるだろう。



2001年を境に、意外にも詳しく知っている人の比率は減少している。
これは利用者の全体数の増加に啓蒙が追いついていない結果とも考えられる。
出典：国内におけるコンピュータウイルス被害状況調査報告書
（http://www.ipa.go.jp/security/fy16/reports/virus-survey/documents/2004_virus_domestic.pdf）

図7　IPA国内・海外におけるコンピュータウイルス被害状況調査（2004年）

Part 2 個人への脅威

スパイウェア／トロイの木馬 知らない間に情報が盗聴されている

渡部 章
株式会社アークン

スパイウェア（Spyware）とトロイの木馬（Trojan horse）は、
分類する観点によってさまざまな定義が存在するため厳密な区別は難しい。
共通点は、利用者の知らない間に侵入し、ユーザーの意図しない被害を及ぼすプログラムであることだ。
異なる点は、侵入と発病の仕方である。

ウイルス対策ベンダー各社の名称：
TROJ_DELF.RM（トレンドマイクロ）
Trojan.Jasbom（シマンテック）
JS/Exploit-MhtRedir.gen および PWS-Lineage!chm（マカフィ）

Trojan/Downloder（ダウンローダー）／Trojan/Dropper（ドロッパー）：特定のサイトへ接続して、ハッキングツールやウイルス等の不正プログラムがダウンロードされる。ダウンロードが完了すると、そのプログラムを実行させ、パソコンにインストールする。それにより、マシンを乗っ取る。

手口 Threat

トロイの木馬は、一見、普通のプログラムのよう見え、無害だと思って実行すると破壊やいたずら、情報漏えいなどの被害を及ぼすプログラムである。侵入経路としては、第三者から手渡しされたり、第三者によって故意にインストールされたり、メール添付で侵入したり、ウイルスやワームによって組み込まれたり、ウェブ閲覧中にスクリプトによってインストールされるなどがある。

一方、スパイウェアの特徴は、上記の侵入方法の他に、オンラインソフトやフリーソフトウェアをインストールする際に利用者の気がつかない間にインストールされ、利用者の許可なくシステム情報やインターネット履歴などの個人情報を外部に送信することである。収集した情報はマーケティング会社などに売買される場合もある。

スパイウェアもトロイの木馬も被害を与える悪意あるプログラムという意味では、広義にコンピュータウイルスとして扱われる場合がある。しかし、狭義のウイルスは、ある特定のプログラムファイルや起動プログラムに埋め込まれて、その宿主プログラムを利用して動作、感染するのに対して、スパイウェアやトロイの木馬は独立したプログラムであり、他への感染（自己複製）機能を持たないところが異なる。

5月11日、【価格.com】が不正アクセスによってウェブサイトのプログラムが改ざんされ、その結果、サイトの閲覧者がトロイの木馬を組み込まれるなどの被害にあい、サイトはセキュリティ対策を施すために一時閉鎖を余儀なくされた。

判明しているウイルスは「trojandownloader.small.AAO」と「PSW.Delf.FZ」（NOD32 アンチウイルスでの名称）の2種類であるという。これは、オンラインゲームの「リネージュ」にログオンすると、そのキー入力やアプリケーションメモリを記録して、アカウント情報を盗み出して外部に送信するトロイの木馬である。

今回の被害では、その手口が2段階になっており、ダウンローダーまたはドロッパーと呼ばれる侵入方法に特徴がある。まず、何者かがサイトに不正アクセスしてトロイの木馬をインストールした。次にユーザーがそのウェブサイトにアクセスするとトロイの木馬がダウンロードされて感染するのだ。

対策
Defence

メールの受信時や、ウェブの閲覧時にスパイウェアやトロイの木馬が侵入・発病しないようにするためには、先ず、メールソフトやインターネットエクスプローラのセキュリティー設定でスクリプトが不用意に動作しないようにしておくことが肝心である。

しかし、それでもセキュリティー設定を潜り抜けて知らない間に侵入してくるものが多い。最近ではアンチウイルスソフトでも検出ができるようになってきたが、暗号化していたり、他のプログラムとパッケージ化されていたりする場合には、従来のシグネチャ方式だけでは侵入を完全に防止することはできない。

また、アンチウイルスソフトは、ウイルスを駆除する構造となっているため、スパイウェアやトロイの木馬を安全にかつ確実に駆除することができないケースが多い。スパイウェアやトロイの木馬は、他のプログラムの機能の一部としてインストールされている場合が多く、不用意に構成ファイルの一部だけを削除すると他のアプリケーションが動作しなくなる場合があるからだ。その点、スパイウェア対策ソフトであれば、駆除した後に何か問題があれば元に戻せる機能をも有しているので安心だ。

企業では、サーバーを保護するためにホスト型侵入検知システムが利用でき、ネットワークの侵入経路で検出するためにはファイアーウォールやネットワーク型侵入検知システムが有効である。

ウイルスの届出機関であるIPAでも、ウイルスばかりでなく、スパイウェア（キーロガー等）や不正プログラム（バックドア等）などが多数出回っていると発表している。

また、誤ってメールの添付ファイルやホームページ上からスパイウェアや不正プログラムを取り込まないよう、Windows Updateなどでシステムのセキュリティホールを解消した上で、以下の対策をするように呼びかけている。

1. スパイウェア対策ソフトの活用（パソコンショップ等で入手可能）
2. 不審なWebサイトへのアクセスを避ける
3. ブラウザのセキュリティレベルを高く設定する

IPA（独立行政法人情報処理推進機構）：http://www.ipa.go.jp/security/isg/virus.html

主なスパイウェアの構造
Trojan/StartPage（スタートページ）：レジストリを改変することにより、ブラウザ（Internet Explorer）の起動時に表示されるスタートページを不正なWeb サイトに変更する。
Trojan/Websearch（ウェブサーチ）：ブラウザの設定を改変し、URLリクエストをリダイレクト（意図しないページを表示）する。これにより、特定の検索サイトにアクセスすると、意図しないページが表示される。
Trojan/PWSteal（パスワードスティール）：侵入したパソコン上から、パスワードやシステム情報を収集し、特定のメールアドレスにそれらの情報を送信する。
Trojan/IRC（インターネットリレーチャット）：IRCサーバーを通じて、ユーザーのシステムへアクセスする。接続に成功すると、そのターゲットのシステム情報などを盗み出したり、ファイルを削除したりするなどの操作がリモートから可能となる。

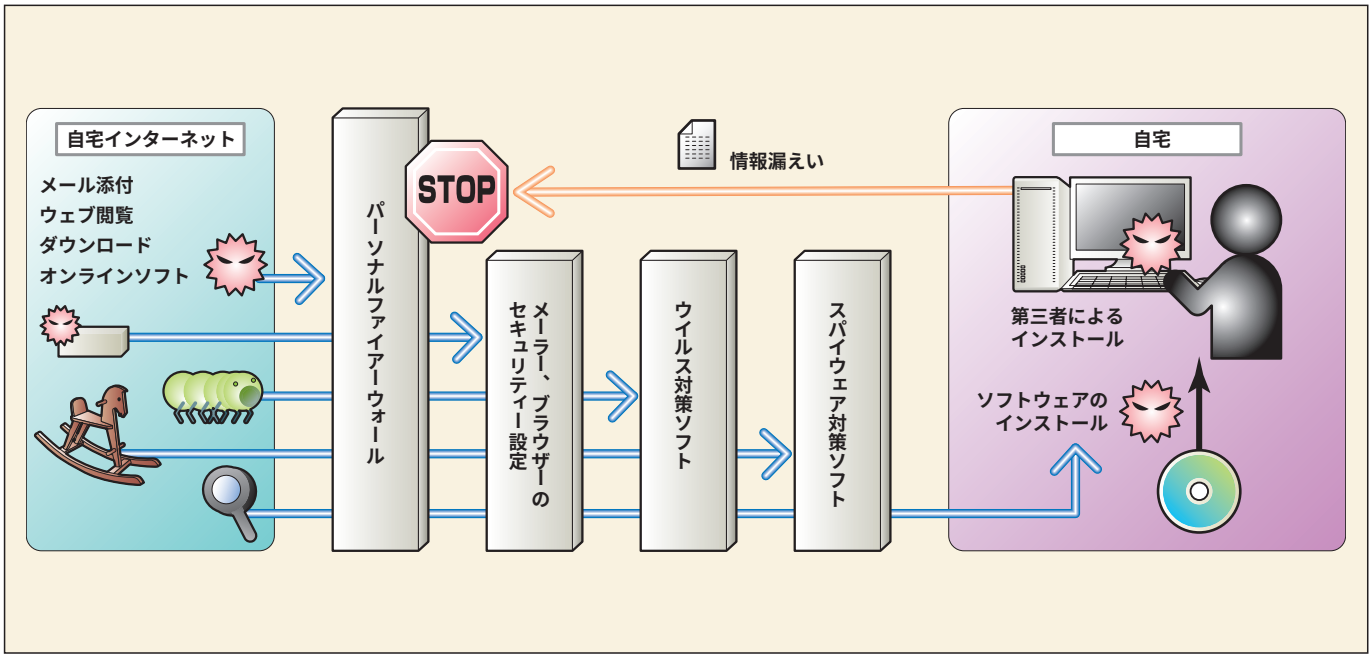


図8　スパイウェアとトロイの木馬の侵入と対策

Part 2 個人への脅威

ケータイに対する脅威 PCだけではない組み込みデバイスでの脅威

大津留 史郎
日本アイ・ビー・エム システムズ・エンジニアリング株式会社
ICP アドバイザリー IT アーキテクト

ネットワークの脅威にさらされているのはPCだけではない。
すでに8,000万台が普及している携帯電話も例外ではない。
これまで携帯電話での脅威が話題になることはあまりなかったが、これからは重要な社会問題化することは間違いない。

すでにNECはLinuxをベースにした携帯電話端末を発売している。近い将来、PCと同様にウイルスやクラッキングツールなどが出回る可能性が高いと考えられる。

ネットワーク経由以外の脅威として、持ち主が置き忘れた携帯電話に対して暗証番号の解析を行い、電話帳やメールなどの保管されている個人情報を抜き取るといった脅威も考えられる。PC上で動作する解析ツールもインターネット上で出回っており、こういったツールを使えば数分間で暗証番号解析ができてしまうケースもあるようである。また、特定の機種については、携帯電話開発者が使用するデバッグモードに入る操作についての情報も存在している。これが携帯電話に対する脅威となり得るかどうかは不明だが、デバッグモードから携帯についているカメラのシャッター音を消すということが可能であれば、携帯電話がいたずらのツールとして悪用される危険性がある。

手口 Threat

現在、携帯電話は高機能化が進められており、それに伴って様々な脅威が発生してきている。

ネットワーク経由で入ってくる脅威としては、スパム／フィッシングメールやウイルス／ワームのようにPCと同様に考えられるものと、Bluetooth通信を悪用した電話機の乗っ取りやXHTML（携帯電話向けのホームページを記述する言語）の悪用による不正操作のように携帯電話独特の特性を持ったものとがある。

スパムメールとは無差別に送信される広告メールのようなユーザーが受信を望まないメールの総称であり、携帯電話ユーザーはスパムメール受信によりパケット通話料の無駄な出費を強いられたり、携帯電話キャリアのネットワークが本来は不要なスパムメールにより浪費されたりするといった影響がある。

フィッシングメールとはオンラインバンキングやウェブサイトからの正規なメールのように装って、暗証番号、パスワード、個人情報を詐取する詐欺メールのことである。ウイルス／ワームについてはここで解説する必要はないと思われるが、携帯電話の高機能化に伴って携帯電話に感染するウイルス／ワームが徐々に出回り始めていることを述べておきたい。今年の3月にはBluetooth通信を経路として感染するCaribeまたはCabirと呼ばれるウイルスが日本に上陸したことが伝えられている。

XHTMLの悪用による不正操作としては、PhoneTo（電話をかける）、MailTo（メールを送信する）が埋め込まれたリンクを携帯向けのホームページやメールに表示しておき、ユーザーにリンクをクリックさせることにより、ユーザーに気づかれることなく電話をかけさせたりメールを送信させたりすることが挙げられる。実際に2000年6月から7月にかけてPhoneToを悪用してユーザーに気づかれずに110番に電話をかけさせるいたずらメールが出回り、一時110番の電話がかかりにくくなったという事件が発生している。

Bluetooth経由による携帯電話の乗っ取りには、携帯電話のIDをコピーしてクローン携帯電話を作るスナーフ攻撃、認証済みコンピュータになり

すまして携帯電話にアクセスするバックドア攻撃、携帯電話のATコマンドセットを乗っ取るブルーバグ攻撃、Bluetooth認証にメッセージを挿入するブルージャッキング攻撃といった攻撃が行えることが知られている。こういった攻撃により第三者の携帯電話をBluetooth経由で乗っ取り、携帯電話に保存された個人情報や電話帳データを盗み取るという事件が実際に発生している。

また、携帯電話はノートパソコン以上に持ち運びが容易であることから、ネットワーク経由ではなくユーザーが置き忘れた直接アクセスする事による脅威も存在する。ツール悪用による携帯電話パスワードの解析がその代表例である。

対策
Defence

これらの脅威に対抗する対策としては以下のようなものが考えられる。

まず、スパム／フィッシングメールについては、アドレス取得目的の宛先不明メールをブロックするなど各携帯電話キャリアが自身のネットワーク内で実施している対策があるほか、ユーザーに対して提供している迷惑メール防止サービスがある。フィッシングメールは人をだます詐欺行為であるため、携帯電話キャリアが注意を呼びかけているが、ユーザー側でも最近の手口を知って用心をする必要がある。

ウイルス／ワームについて、現在のところは携帯電話に感染するウイルスの事例も少なく各携帯電話キャリアが対策を検討している段階であるが、近い将来携帯電話にアンチウイルスを導入してパターンファイルを定期的に更新するといったPCのウイルス対策と同様の対策が必要になってくると考えられる。実際、カスペルスキーというロシアのウイルス対策製品ベンダーが今年の6月にSymbian OSの携帯電話向けのウイルス対策製品を発売する事が伝えられている。

XHTMLの悪用による不正操作対策としては、ユーザーの側で怪しいリンクはクリックしないというPC上のメールやインターネットブラウザーを使うときと同じ注意が必要である。この脅威はフィッシングメール同様人を騙す行為であるため技術での完全な対策は難しく、どうしてもユーザー側での用心が必要になってくる。

Bluetooth通信の悪用対策については、携帯電話の設定によりBluetooth通信を無効にしておく必要がある。海外メーカーの携帯電話にはBluetooth以外にも無線LANやActive Syncが搭載されているものもあり、これらの通信インターフェイスについても同様である。これは携帯電話の機種によっては不可能な場合もあるだろうが、視野を広げて考えると不要なサービスを停止したり、セキュリティパッチを定期的に適用したりするサーバーのハードニングと同様の対策であることが言える。

携帯電話における脅威と対策について記述してきたが、総じて言えることは高機能化に伴い、携帯電話でもPCと同様の対策が必要になりつつあるということと、高機能な携帯電話を使用するユーザーの自己責任としての注意も必要であるということである。この2点は携帯電話のヘビーユーザーにぜひお伝えしたい。

個人に対する脅威以外に、携帯電話サイトを運営している企業に対する脅威も考えられる。携帯電話が高機能化してPCと同様の機能を持つようになり、かつ携帯電話キャリア内の通信がIP化されたとすると、携帯電話キャリアのネットワークはインターネットと同様に信頼できないネットワークとなる可能性がある。このような状況では携帯電話サイトもインターネット向けのサイトと同様に、基盤やウェブアプリケーションの脆弱性を自らチェックし、発見された脆弱性については早急に対策を施すといった運用が必要になる。現段階からインターネットサイトと同様のペネトレーションテストを行うのも1つの有効な予防策となると考えられる。

脅威	対策
スパム／フィッシングメール	携帯キャリアでのメールフィルタリング
	迷惑メール防止サービスの利用
	ユーザー側の注意
ウィルス／ワーム　(近い将来発生する脅威)	アンチウィルスソフトの導入
	パターンファイルの定期更新
XHTMLの悪用による不正操作	ユーザー側の注意
Bluetooth(その他)通信悪用による乗っ取り	不要な通信の無効化

表4　ケータイに対する脅威の手口とその対策

Part 3 企業に対する脅威

ブランドスプーフィング 企業のブランドを失墜させる危険

河岡 忠広
日本アイ・ビー・エム　システムズ・エンジニアリング株式会社
主任IT スペシャリスト

フィッシングは個人が引っかからないようにすればよいというものではない。
自社のブランドがフィッシングに利用されることは、企業の信頼性を失墜させることにもつながる。
自社のブランドがフィッシングに利用されないように、組織として防衛し、
そして万が一利用されてしまった場合の速やかな対処が要求される。

Anti-Phishing Working Group の“Phishing Activity Trends Report March,2005”によると、2005年3月中では、フィッシングにハイジャックされた商標の数は78にのぼる。なお、フィッシングサイトのオンライン上での活動時間は平均5.8日である。

手口 Threat

フィッシャーは、さまざまな手を尽くしてメールやウェブサイトを本物に見せかけようとするが、よくある手口として、本当の企業と酷似したURLやメールアドレスを使用する方法がある。

たとえば、正規のサイトである、http://www.impress.co.jp/を http://www.impres.co.jp/としても、ほとんど見分けがつかない。

他の手口としては、たとえば、クレジットカードのVISAをかたるフィッシングが今年の4月に報告されているが、その偽サイトではアドレスバーのURL情報を http://www.visa.co.jp/verified/と偽装して表示する。このようなアドレスバーの偽装はJavaScriptを悪用することで可能となる。

また、アドレスバーを非表示にする方法もある。接続先が偽のURLであっても非表示にしてしまえば、それを判別することは困難である。

フィッシングは主に米国での被害が多かったが、去年に入り日本語でのメールやウェブサイトを使っ

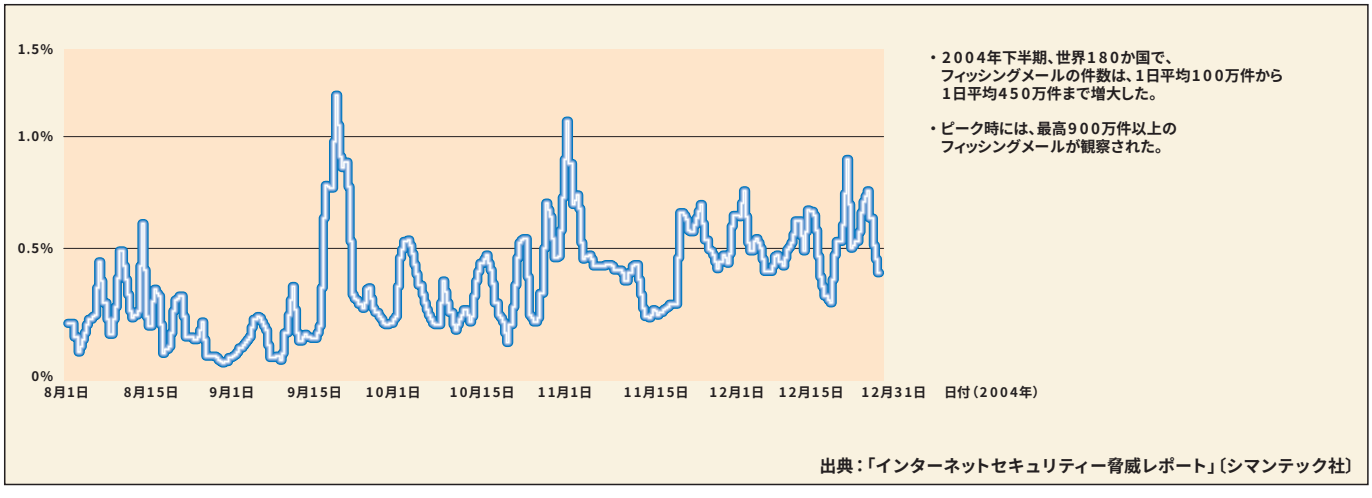


図10　フィッシングメールの件数

たフィッシングが報告されている。たとえば、前述のVISA、UFJ銀行、JCBなどをかたったフィッシングが発見されており、今後は日本でも米国同様フィッシングが増加する傾向にある。

このようなフィッシング行為は個人の被害だけでなく企業のブランドイメージも傷付ける行為である。企業側でのフィッシング対策が重要になってくる。

対策
Defence

企業の対策としては、まずユーザーにとって、偽装メールや偽装サイトでないことを識別しやすい仕組み作りを心がけるべきである。

たとえば、メールを送る場合であれば、メールの本文に「山田太郎 様」といったユーザー本人の名前を入れることで、フィッシャーにとって偽装しづらいメールを送ることが可能となる。また、メールに通し番号を付けたり、デジタル署名を付けたりすることも有効な手段である。

つぎに、ウェブサイトでの対策としては、アドレスバーを表示することで、ユーザーにアクセスしているURLを判別できるようにすべきである。さらに、ユーザーは自分の取引情報をいつでも自由に参照できるようにすべきであろう。これにより、ユーザーはフィッシング詐欺にあっていないかどうかの確認を速やかに行うことができる。

また、SSLサーバー証明書を導入し、暗号通信を実現し盗聴を防ぐとともにアクセス先のURLとサーバー証明書に記載されるURLを比較できるようにし、ユーザーに正しいURLにアクセスしているかどうかを確認できるようにすべきだ。

さらに、フィッシングサイト情報配信ソフトを利用する方法もある。これをユーザー側に導入することで、あらかじめ登録されたフィッシングサイトにアクセスしたときにはユーザーに警告を発することが可能となる。

万が一、自分の企業をかたる偽サイトが発見された場合には、ユーザーに対して速やかに注意を呼びかけるべきである。ウェブサイトやメールでの通知などの手段で周知させ、被害を最小限に抑えることが求められる。

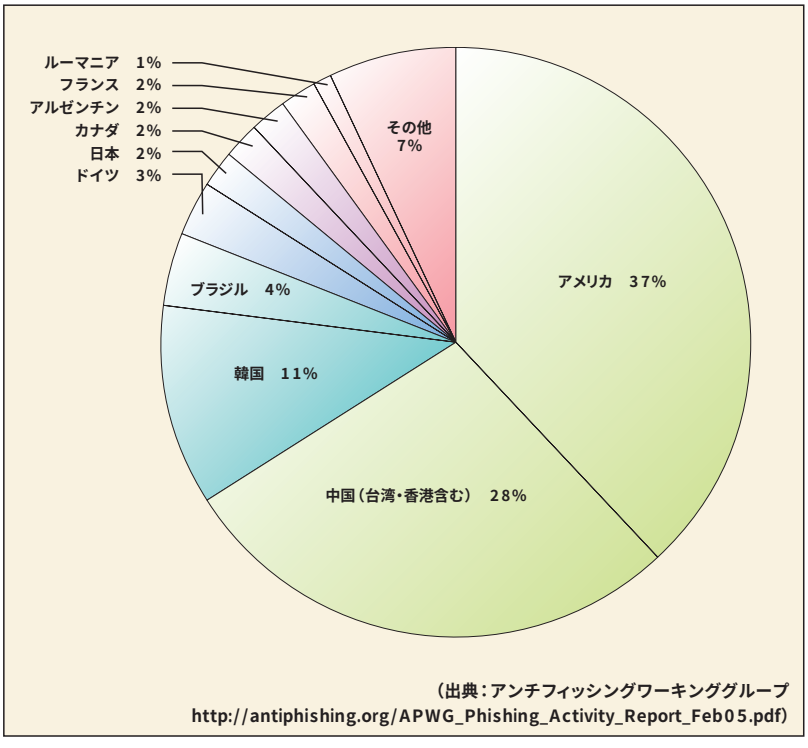
仮に、個人情報がフィッシャーに入手されてしまった場合でも、サイトにログインする際の認証方式を強化することで、そのサイトでの悪用を阻止することが可能となる。フィッシャーが本人に成りすまそうとしても認証機能で防御できるからである。ID、パスワードの他に、乱数カードなどを併用することで認証の強度は大きく向上する。

別のアプローチとしては、イーバンク銀行のように、ユーザーが普段利用しているプロバイダー（IPアドレス）を指定することで、フィッシャーが別のプロバイダー経由でログインしようとしても受け付けないようにする方法などもある。

最後に、フィッシングから顧客や会社を守るだけではなく、社員を守るという観点も考慮していくべきであろう。社員への偽装メールの受信や偽装サイトへのアクセスを防止する対策としては、URLフィルタリングやアンチウイルス、アンチスパム製品を利用する方法などが考えられる。

メールのデジタル署名の方式としてS/MIMEがある。Outlook ExpressなどのS/MIME対応メーラーを利用することで、デジタル署名からメールの送信者を特定できる。

認証には様々な方式があり、パスワード方式の他に、乱数カードを併用する方式や、ワンタイムパスワードやデジタル証明書を利用した方式などがある。それぞれで認証の強度が異なるが、セキュリティ上のリスクとコストやユーザーの利便性の観点から適切な対策を選定する必要がある。



（出典：アンチフィッシングワーキンググループ
http://antiphishing.org/APWG_Phishing_Activity_Report_Feb05.pdf）

図11　フィッシングサイトの国別の割合

Part 3 企業に対する脅威

DoS攻撃 サーバーが機能不全に陥れられる

渡部 章
株式会社アークン

DoS攻撃は、Denial of Service Attackの略で、サービス拒否攻撃、サービス妨害攻撃、
または、サービス不能攻撃などと訳されているインターネット経由での攻撃手法である。
標的システムの処理能力を上回る大量のデータや不正パケットを送りつけることで
ネットワークに負荷をかけサービスを遅延させたり、
システムそのものを停止させたりすることでコンピュータやネットワークを利用できない状態にする。

IPAによる「コンピュータウイルス・不正アクセスの届出状況について」：http://www.ipa.go.jp/security/txt/2005/05outline.html

SSH（Secure Shell）：主にUNIXコンピュータで利用される。ネットワークを介して別のコンピュータにログインしたり、遠隔地のマシンのコマンドを実行したりするときに通信を暗号化して一連の操作を安全に行えるようにするためのソフトウェア。

手口 Threat

攻撃者はインターネットサーバーによって提供されているサービス（WWW、FTP、DNS、メールなど）を標的とし、TCP/IPプロトコルやOSなどに内在する脆弱性を悪用した攻撃がある。これらの攻撃はインターネットで比較的簡単に入手可能なDoS攻撃ツールを利用して行われることが多い。

主な攻撃手法には、大量のデータを送信してネットワークの帯域を渋滞させサービスを妨害する攻撃、TCP/IPプロトコルを悪用して標的に負荷をかけてサービスを妨害する攻撃、サーバー上のアプリケーションの脆弱性を悪用してサービスを妨害する攻撃などがある。

DDoS攻撃は、Distributed Denial of Service Attackの略で、分散型サービス拒否攻撃、分散型サービス妨害攻撃、分散型サービス不能攻撃などと訳されているDoS攻撃の発展形である。DoS攻撃が1台のマシンから行うのに対して、DDoS攻撃は、事前に準備した複数のマシンから特定のシステムに対して一斉にDoS攻撃を仕掛けるため、その威力はより大きなものとなる。

DDoS攻撃は、ほとんどの場合、ツールを利用する。攻撃者は、事前にインターネットに接続されている複数の第三者のマシンに侵入し、攻撃用のプログラムを仕掛けておく。そして、遠隔でそのマシンに指令を出して特定マシンを一斉攻撃するのだ。その攻撃用プログラムのことをゾンビ、または、エージェント、最近ではボットと呼んでいる。また、複数のボットで構成された攻撃ネットワークのことをボットネットと呼んでいる。最近の傾向として、これらボットは、ウイルスやワームの感染力を利用して無差別にばら撒かれてDDoS攻撃のために利用されている。

IPAによる「コンピュータウイルス・不正アクセスの届出状況について」によると、最近、SSHで使用するポートへの不正なアクセスが多発しているため、サーバーが多数ダウンしているという。これはSSHの処理コードがパケットを適切な処理できないというセキュリティホールを狙われたDoS攻撃である。このセキュリティホールを狙われた場合、

DoS攻撃以外に、遠隔から第三者が任意のコードを実行できたり、脆弱なシステムの場合、管理者権限を取得されたりする可能性もあるという。

対策
Defence

DoSやDDoS攻撃への基本的な対策は、ルーター、OS、サーバーアプリケーションなどに対してセキュリティーパッチを適用して攻撃の対象となる脆弱性をなくすことである。

次にOSやルーターにあるパケットフィルタリング機能やファイアーウォールによって不審なアクセスを拒否することが有効である。また、攻撃によるネットワーク負荷の増加に対応するために、ネットワーク帯域を広げたり、帯域制御をしたり、負荷分散装置（ロードバランサー）を導入するなどの防衛策も有効だ。

従来、DDoS攻撃に狙われたら最後、完全な対策はないと言われてきた。しかし近年では、さまざまな防止技術が開発され（図2参照）、それらの技術を複合的に実装した製品が商品化されている。

また、自社がDDoS攻撃の踏み台とならないために、システム管理者は自社のマシンが不明なブロードキャストをしないようにルーターなどの設定をしたり、ウイルス対策ソフトやスパイウェア対策ソフトを利用したりしてボットなどの仕掛けられたプログラムを常時発見できる体制をとることが重要だ。

実際の攻撃別の対策は以下になる。たとえば、Smurf攻撃は、大量のICMPパケットを発生させるものである（図9 参照）。不幸にもSmurf攻撃の標的になったり、中継者にされた場合は、OSでICMPパケットに応答しないように設定したり、他のネットワークから送信されてくる IP ブロードキャストを拒否するようにルーターを設定することで阻止できる。しかし、ルーターとISP間のネットワークの混雑は回避できないので、この攻撃を止めるようにISPに相談したり、攻撃の中継者に連絡して、前述のOSやルーターへの対策をとったりするように連絡するべきである。

また、自身のネットワークが攻撃源にならないためには、内部から外部へのパケットで「始点アドレスが自身のネットワークではないもの」は送信しないようにルーターなどでフィルタリングすることである。

また、フラッディング攻撃（図9 参照）など特定のサイト、特定ポートへの大量パケットを送信するタイプの攻撃に関しては、同様にルーターなどによるフィルタリングで対処できるが、完全に防止できない場合もあるので、アクセス元へ連絡して対応を取るように依頼しなければならない。

ロードバランサー：負荷分散装置ともいう。外部ネットワークからの要求を一元的に管理し、同一目的の複数のサーバーに対して、負荷の比較的小さいものを使うようにすることで、ネットワーク全体の可用性を向上させるための装置。

ICMP（Internet Control Message Protocol）：IPのエラーを制御するためのプロトコル。TCP/IPで接続されたコンピュータやネットワーク機器間で、互いの状態を確認するためにpingやtracerouteなどのコマンドで使われている。

IPブロードキャスト：ネットワーク内で、不特定多数のホストに向かって同報通信すること。簡単に利用でき便利であるが、無関係なホストに対しても無用な負荷を強要する場合がある。

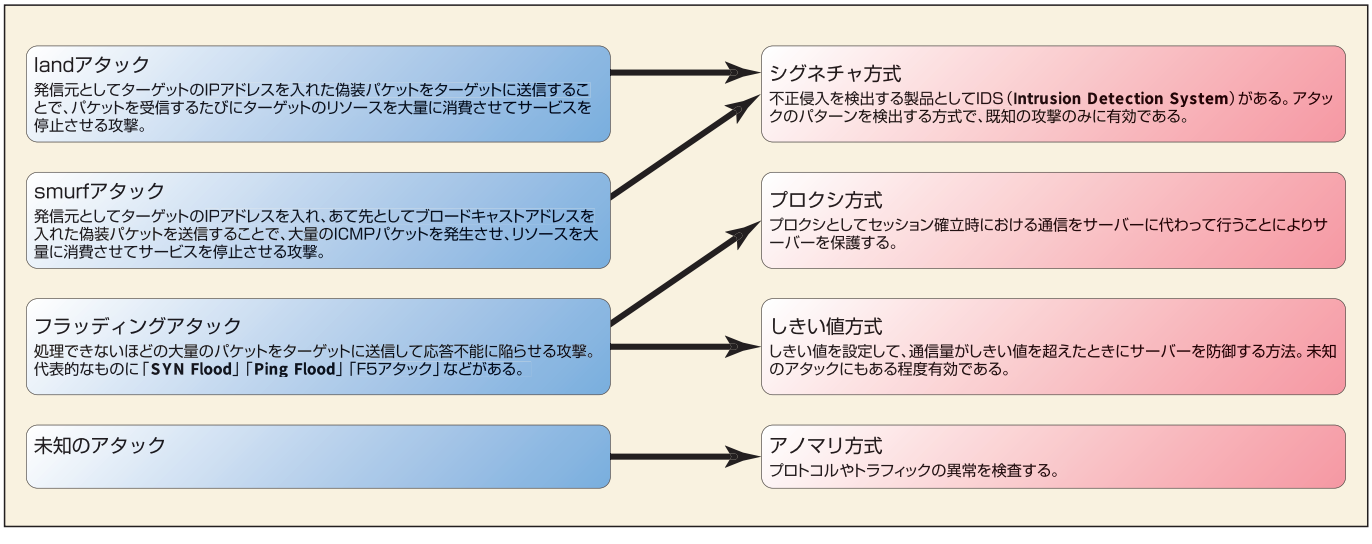


図9　主要な攻撃と防御装置の関係

Part 3 企業に対する脅威

ウイルス／ワーム 企業ウイルス感染、知られざる副作用の深刻度

二木 真明
住商エレクトロニクス株式会社 ネットワークセキュリティ事業部
副事業部長（技術担当）

企業へのウイルス対策の導入は、かなり進んでいるとはいえ、昨年度の中小企業中心の調査（IPA）では、9割以上のPCへの導入が終わっている民間企業は、まだ63.7％にとどまっている。
一方、ウイルス感染を経験した企業は、同じ調査で40％以上あり、企業にとってウイルス感染のリスクは少なからず残っている状況だ。特に、決定的な対策がない新種のウイルスについては、すべての企業で感染の危険がある。

ウイルス／ワームによる情報漏えい：電子メール感染型ウイルス・ワームによるメールアドレス漏洩の副作用は本文に書いたが、より直接的に情報漏えいに加担するようなものも存在しうる。ウイルスやワームであるが、いわゆるスパイウエア、トロイの木馬といったものと同様の機能を自分自身が持つものや、感染後、特定の悪意あるサイトから、スパイウエアなどをダウンロードし、インストールするドロッパーと呼ばれるようなものも多く存在する。また、幸いにも今のところ大きな流行の報告はないが、たとえば、PC内にあるファイルを無作為に添付して外部に送信してしまうような機能をウイルスに付加することは、技術的に見てそれほど困難ではない。情報漏えいに敏感な世相を逆手に取ったようなウイルスが出現しないとも限らないので、注意するにこしたことはないだろう。

手口 Threat

最近の電子メール大量送付型ウイルスは、感染すると大量の電子メールをばらまくため、これに付随したいくつかの問題を企業にもたらす。これらのウイルスのほとんどが、電子メール送信者名やメールアドレスを詐称するが、本当の発信元はメールヘッダーやメールサーバーのログから容易に見つけることができるため、受信者がウイルス感染を引き起こした会社をつきとめることは簡単だ。ウイルス感染の発覚、それだけならば、企業としての体面の問題だけともいえるのだろうが、より重要な問題がそこに隠れていることは意外と認識されていない。

この種のウイルスは、PC内に保存されているメールアドレスをさまざまな形で探し出し、悪用する。それらのアドレスにウイルス付きのメールを送るだけでなく、メールの発信者を偽装するために使うことも一般的だ。宛て先に使われるだけならば、その本人にウイルスが届くという被害のみなのだが、発信者として使われることで、第三者にそのメールアドレスがわたってしまうことになる。氏名、所属が特定できるようなメールアドレスの場合、一種の個人情報漏洩となりうるので注意が必要だ。

また、先に述べたように、メールヘッダー上の配送経路記録やメールサーバーのログから真の送信者を企業のレベルで特定することもできるから、当然そうしたメールアドレスをその企業のだれかが保有していたと推測できる。それが取引先のメールアドレスだったりすると、取引関係などが漏洩することにもなりかねない。

実際に、ある企業内で大量感染が発生して、取引先などへ大量のウイルス付きメールが送られた際、受け取り側のメールサーバーで、すべてのログを集計してみると、感染元の会社のおおまかな取引関係がわかってしまったというような事例もあるので事は重大である。

企業での感染発生には、こうしたリスクをともなうということもきちんと認識されるべきだろう。

対策
Defence

万一のウイルス感染発生時に外部に情報を漏洩させないための対策として有効なものに、ファイアーウォールによるメール送信規制がある。企業ユーザーがメールを送信する場合、各PCからその企業のメールサーバーに対してメールを送り、メールサーバーが相手方に配信する形が一般的だ。したがって、通常は外部に対するメール送信はメールサーバーからしか発生しない。

一方、ウイルスの多くはクライアントPCから直接インターネットにメールを送信する。この特性を利用して、内部から外部へのメール送信をメールサーバーからのみに限定するような規制をファイアーウォールで実施することで、ウイルス感染時の外部へのメールによる情報流出を防ぐことができる。簡単な対策で効果が大きいので是非実施して欲しい。

いまでは、ほとんどの企業がウイルス対策を導入しているし、ファイアーウォールの導入、脆弱性対策なども常識となっているのだが、それでもウイルスやワームの感染は100％防ぐことは難しい。ウイルスやワームの世代交代が加速していることや、感染速度の圧倒的な向上がその背景にある。

こうした状況を考えるならば、これからの対策は、万一の感染に備えたものでなくてはならないだろう。

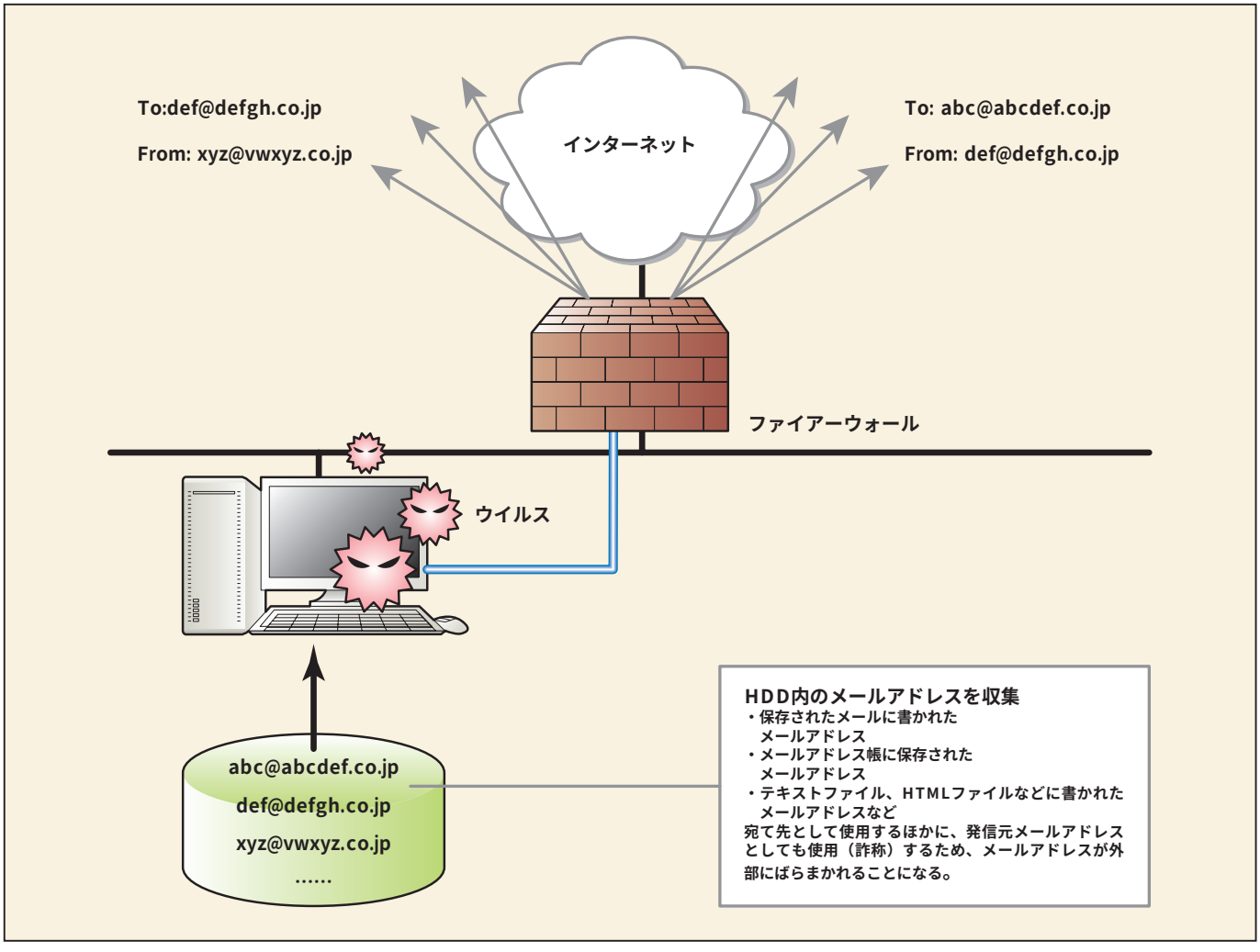


図12　ウイルスによるメールアドレス漏洩

Column

スパムもDoSも根本にあるのは『発信者の詐称』

安藤 一憲
株式会社IRIコミュニケーションズ

スパムやDoSなどを始め、多くの「脅威」を作り出す根本にあるのは「発信者の詐称」という特性である。
インターネットが性善説で運用されていた時代には問題とならなかったこの特性がいまや脅威の根本になっている。
それを回避するためにいくつかの取り組みも開始されている。

そのメールは誰が送信したのか？

スパムの問題は結局のところメールというシステムの送信コストの安さと発信者の詐称のしやすさが仇となって拡大し続けている。たとえば、一般のユーザーの手元にどこからかメールが1通届いたときに、そのユーザーはメールの文面から誰が本当の発信者であるのかを知ることができるのであろうか？発信者がデジタルシグネチャで署名して、それが受け手の側で検証されれば文面の改変がないことを含めて発信者がその人であることが保証されるケースはあるかも知れない。だが実際にどれだけの人がそれを意識してメールを使っているだろうか？

一般ユーザーよりもう少しメール配送に近いところにいるメールサーバー管理者は送受信記録を見れば、そのメールがどの送信元サーバーから送信されてきたものかを知ることができる。一般に送受信記録にはDNSを逆引きした相手サーバーのFQDN（Full Qualified Domain Name）が記録されているが、そのFQDNが詐称されていなかったという過去の事実を検証するのは非常に難しい。

送受信記録には送信元サーバーのIPアドレスも記録されているに違いない。だが経路情報が詐称されている場合はそのIPアドレスさえ信用できるかどうか疑わしい。では、経路情報の詐称に対して十分な対策は打たれているのか？

スパムの問題を題材に芋づる式に問題を挙げてみたが、出てくる問題を眺めると、スパムの問題は氷山の一角でしかないことがわかる。どんな対策が進められているのがユーザーから丸見えになっている分、まだ問題がどこにあるのかを説明しやすいのが救いである。スパムの問題は、いまそこにある危険を示しているのだ。

スパムがはびこり、送信者がなかなか検挙されない裏側には各レイヤー、各アプリケーションでの発信者の詐称の問題が根本にある。逆に言えば、スパムを送信する者は、発信者を詐称する技術を駆使しているのだ。したがって、これらの問題の根源を攻める対策は、発信者の詐称をいかに防ぐかという1点にテーマを絞ることになる。

メールが社内で安全に活用されるための必要十分条件

社員同士のメールのやり取りであっても、そのメールを誰が送信したのか判別が難しいケースがある。たとえば、出張しているスタッフが滞在中のホテルのインターネット接続サービスなどを経由して社内に向けてメールを送ってくるケースである。この場合、どこかにユーザー認証を入れれば問題は解決するが、最もメールに近いところで誰がそのメールを発信しているのか認証する枠組はSMTP AUTHである。認証の結果が社内のメールサーバーの送受信記録に残るので、結果として全てのメールが誰のユーザー権限で送信されたかを確実に記録することが可能になる。

ちなみに従来ISPで用いられてきた技術であるPOP before SMTPはそのIPアドレスからPOPをしたのがそのユーザーであることは検証できるかもしれないが、そのIPアドレスからSMTPでメールを送りつけて来たのが誰かは検証しない。現在の状況は「本当にそれでいいのか？」というレベルの話になっているのである。

メールがビジネスに安全に利用されるための必要十分条件

多くの場合、ビジネスというのは個人対個人ではなく会社対お客さんのやり取りであるに違いない。そこでメールに必要とされる最低限の信頼性とは何だろうか？全てのメールに「○○株式会社の△

△さんがこのメールを発信しました」という情報が本当に必要なのだろうか？必要十分という視点で考えると「このメールは○○株式会社から発信しました」ということを保証できれば十分ではなかろうか？たとえば企業から製品ユーザーへの案内と、発信者をその企業に偽装したスパムを区別できることがその必要十分条件であろう。

こうした視点をもとにメールがその組織から発信されたことを検証するしくみがいくつか提案されている。それが、SPF、Sender-ID、DomainKeysといった、送信ドメイン認証と呼ばれる技術である。これらに共通する特徴は、自ドメインの正規のメール送信サーバーの情報をDNSを利用して広報することである。

広報する情報は正規のメールサーバーのアドレスであったり、FQDNであったり、そのメールサーバーが持っている公開鍵だったりする。正規の送信サーバーの情報を広報することで、受信側では正規のサーバー以外から発信元を詐称して送られてくるスパムを識別することができるようになる。

送信ドメイン認証はいかにしてスパムを防ぐか？

昨今、スパムはボットネットと呼ばれる数十万台規模の乗っ取られたマシンの集団から送信されてくる。送信ドメイン認証が普及すると、ボットネットからスパムを送信して相手に受け取ってもらうには、偽装した発信元ドメインのDNSサーバーに正規のメール送信サーバーとして乗っ取った数十万台のマシンの情報を登録するという離れ技を達成しなければならなくなる。つまり、ボットネットという究極の発信者の詐称インフラを封じ込めるには送信ドメイン認証がどこまで普及するかが鍵になる。結果的に送信ドメイン認証は、スパムを送信するにも自ドメインの正規の送信サーバーから送らざるを得ない状況を作り出す。

残る問題点

現状の多くのISPのダイアルアップ接続には、契約しさえすれば実質的にスパム送信を阻む仕組みはない。一方でユーザーの意図しないボットネットの活動を完全に封じ込めるにはISPのIPアドレスブロックから正規の送信サーバーを介さずに外へメールを送信する動きを封じなければならない。そこで国内のISPがおそるおそる始めているのがOutbound Port 25 blockingである。

DoS攻撃が可能な理由

さて、今度は少し視野を広げてDoS攻撃の問題に目を向けてみよう。メールにもDoS攻撃はあり、問題を捉えるために変更するのはプロトコルあるいはポート番号の限定を外す操作だけだ。実際、ボットネットはDDoS攻撃にも使える。これはボットネット自体が発信者の詐称機能を備えているからである。一般にネットワークで何か悪いことを試みる人間の共通点はそこにあるようだ。

DoSで詐称されるのはIPパケットの送信元アドレスだったりするだろう。DoS攻撃を伝えるニュース記事を見ると「上流のISPに協力を依頼して」等の記述が目につく。これはパケットを中継している上位ISPのルーターで調査しないとどこからそのパケットが飛んできたのかわからないからである。最近はルーター間で自動的にパケットどこから来たのかを追跡して入口でブロックするシステムも出てきているようである。

帯域を埋めるに至らない攻撃の場合は、サーバーやルーターで発信元アドレスを指定してパケットを破棄することは可能だろう。だが、発信元が詐称でき、次々に変えて攻撃してくるとなると対策はそう容易ではなくなるのである。

DoSに見る発信者の詐称技術

DoSも本当に悪質になると嘘の経路情報を流してできた経路からパケットを流し込むという手法が取られるようだ。この手のDoS攻撃を解明するためには、その経路情報がどこから発信されたかをも検証しなければならないだろう。「発信元を検証する仕組みが必要」という観点では経路情報についても問題は同じと見ることができる。

むすび

DoSをやるような連中はほぼ100％が愉快犯と言ってよいだろう。これは経済的理由をもって継続的にスパムを送信する者とは少し傾向が違うかも知れない。

だが問題の根源をたどって行くと、すべて「発信元の詐称」という1つの問題に集約されそうである。そもそも発信元の詐称が容易なのは、インターネット自体が性善説に基づいて作られてきたからなのだが、それを悪用する人間がごく少数発生しているが故に、システムを変更して対処せざるを得ない状況になってきている。そもそも、インターネットはプロトコルの単純さとその性善説を前提としたオープンさ…たとえば匿名性…によって急激に拡大してきたように思う。

なんとか修正を最低限にしてインターネットならではの良さを失わないようにしたいというのがインターネットを支えてきたベテラン技術者たちの本音ではないだろうか。その何よりの証拠は、必要以上に発信者を特定せずに詐称を防ごうという努力が継続されていることである。

Part 4 脅威の分類と対策の考え方

心理を突いた巧妙な手口にだまされるな

安田 直義(ディアイティ)
NPO 日本ネットワークセキュリティ協会 主席研究員

インターネットは、社会基盤として好むと好まざるとを問わず、生活や仕事の中に取り込まれてきている。新たな問題点が次々に明らかになってきてもいるが、利便性とのバランスを取ることも重要である。インターネットがいろいろな犯罪につながる手段として使われ、手軽に、かつ安価に利用できるので、実際に犯罪を行うきっかけを作ってしまっている面は確かにあるだろう。しかし、悪い面ばかり見るのではなく、良い面をさらに活かし、悪い面を使わないようにして行くリテラシー教育やコモンセンスを作ることが大切であろう。

日本におけるインシデントについては、警察庁からも資料が公開されている。
「不正アクセス行為対策等の実態調査」
http://www.npa.go.jp/cyber/research/h16/countermeasures.pdf
「アクセス制御機能に関する技術の研究開発の状況等に関する調査」
http://www.npa.go.jp/cyber/research/h16/research.pdf
次ページの JNSA の報告書も参考にされたい。

脅威の種類

インターネットの脅威には、複合的なものが増えてきているが、大きく分けると次のように分類できる。

❶技術的な脆弱性やよくある設定不備を突いてくるタイプ
❷人間の勘違いや心の隙間を突く心理的なタイプ

技術的な脅威には技術で立ち向かうしかない。実装や設定の不備を指摘されたら、技術者が技術的な面から対応策をとる必要がある。運用や手続きで回避しようというのは付け焼刃でしかない。今回の特集では、スパイウェア、ウイルス、ワームなどがそれである。それに対して、心理的な脅威は技術では解決することが難しい。ソーシャルエンジニアリングなどといわれたこともあるが、最近のフィッシングや架空請求もこの類である。騙しのテクニックであり、詐欺などの犯罪に容易に結びついてしまう。特に最近は詐欺を専門に職業としている集団がインターネットに出てきているようである。今までも電話や郵便などを使った詐欺被害が広がっているが、インターネットではずっと安いコストで効果が得られる可能性がある。100 万件のアドレスに架空請求メールを送ったとして、0.1 %の 1,000 人が 5 万円を振り込んだとすると、5,000 万円の収入となるのである。

何が問題なのか

インターネットで使っている TCP/IP というプロトコル(通信規約)は、1973 年に米国国防総省で開発が始められてから 30 年以上の年月がたっている。その間、基本的な修正はあまりないが、コンピュータのハードウェアや OS は劇的な変化を遂げている。1953 年に制定されたテレビの NTSC 方式はさらに先輩格ではあるが、通信プロトコルがいかに寿命の長いものであるかが窺える。インターネットとして商用サービスが行われるようになり、使われ方も受け取られ方も大きく変化してきていることが、問題の大きな原因となっている。DDoS 攻撃やスパムメールなどは現在の技術標準では完全に制御することが難しいが、TCP/IP プロトコルの手直しで対策が取れるようになるかもしれないし、アプリケーションレベルの上位プロトコルの再検討を行うこともできるだろう。

たとえば、メールで一番うれしい機能を考えてみよう。今のインターネットメールは一度発信してしまうと、取り消しができないという特徴がある。皆さんも一度や二度、メールの送り間違えをしたことがないだろうか。研究者や仕掛けを理解している人たちが使っている分には謝ればすんでいたが、だんだん仕事など業務で使うようになってくると、社外秘のデータや相手に見せたくない情報を間違えて送ってしまったときの対応に困ることがある。郵便だと差し出したあとでも、宛名の間違い

や、内容の入れ違いに気付いたら、集配局で宛名変更や取戻し請求ができる。これは郵便業務がひとつの事業として存在しているので可能なのであるが、インターネットメールでは送り手と受け手が直接データのやり取りをするように設計されているので、今まではできないということで了解されてきた。しかし、そろそろ人間の誤りをフォローする観点から、問題を解決できるような標準を考えてもいい時期なのかもしれない。少なくとも技術と運用的な観点からの共通認識を持ちたいところである。

今インターネットの脅威で一番大きな割合を占めているのがマイクロソフト社のWindowsをOSに使っているパソコンであろうが、これもWindows NT以降マルチユーザーをサポートしていて、最近売られているパソコンはほとんど全てがWindows XPを搭載している。一昔前のUNIX以上のOS環境を使えるのであるが、残念なことにほとんどのユーザーがAdministratorという管理者権限でご自分のユーザー設定をされていると思われる。せっかくユーザー権限コントロールができるはずなのに、実際には使われていないのである。理由はソフトウェアのインストールや実行に際して管理者権限が必要になった際に、使い方が面倒になってしまうからだと思われる。多くのソフトウェアの実行環境に影響を与えるので、なかなかうまく移行できないだろうことは理解できるが、この解決方法を探ることができれば、現在の問題の半分以上は解決できると思われる。

通信の暗号化や、ICカード、生体認証などをはじめとする認証技術に期待する向きもあるが、これらも万全ではない。一番大切なのは、守りたい情報の価値を評価することである。その結果、問題が起こったときの影響が大きいものは、それなりのコストをかけた体制で守り、影響が少なければ少ないなりに見合ったコストをかけ、最終的には保険でまかなうという考え方は、今までの経験の延長線上に沿ったものだろう。

心理を突いた脅威への対応

今後は、人間を直接ターゲットとした心理的な脅威が増えてくるように感じている。オレオレ詐欺や振り込め詐欺などが新聞テレビを賑わせているが、フィッシングやワンクリック詐欺なども同根の問題であり、特にインターネットに特有な現象というわけではない。郵便や電話やインターネットが使えて、相手の話す言語でコミュニケーションができれば、後は悪意のある動機があれば実行できてしまう。最近の架空請求に関係しているようなサイトを見ていると、かなりインターネットのアプリケーションに詳しい人間が関わっているように見える。証拠や手口がコンピュータの中にあり見えにくいことから、一般の人には郵便や電話よりわかり難さが高いのだろう。これも相手の思う壺だ。

特に最近の現象を見ていると、愉快犯というよりも、職業として詐欺を行っている節が見られる。それも個人営業ではなく、会社組織のような構造を持っていて、利益追求をしているようである。相手は本気でお金を巻き上げようとしているのである。お客さんを探すためにインターネットなどの最新技術も十分活用しているのが実態である。インターネットで詐欺をすることが目的というよりは、インターネットという手段が利用できることにより、より簡単に目的が達成できることに目を付けられたと考えたほうがよいのだろう。いずれにしても被害を受ける側から見たら大きな差はないのだが、市民としての注意事項として心しておかなければならないことに変わりはない。この意味でもいわゆる情報リテラシー教育は重要だ。

今までの伝統的な道具を使った騙しの手口に対抗するには、やはり手口をみんなが知っていて自分が同じ状況に出会ったときに、あわてず冷静に対処できることが最善であった。インターネットでもやはり同じであろう。相手は人間であることを意識し、心理作戦に乗らず相手の罠にはまらないようにしなければならない。インターネットやITだからと技術に頼り切るのではなく、人間の知恵を働かせる必要がある。

『技術だけでは問題は解決できない。しかし技術の裏づけがない施策は役に立たない。』という知見は重要だろう。技術的な進歩とそれを租借し社会システムに組み込むための管理とか運用の問題は、シーソーのように順繰りに問題点が表れてくる。今はマネージメント系の確立がテーマになっているが、そろそろ次世代の技術が議論されなければならない時期だろう。

JNSA教育部会スキルマップ作成WGが、情報セキュリティに関するスキルを16に大分類し、各々に関して専門家としての初学者を対象とした教科書を執筆している。
「情報セキュリティプロフェッショナル総合教科書」
http://www.shuwasystem.co.jp/cgi-bin/detail.cgi?isbn=4-7980-0880-X

［インターネットマガジン　バックナンバーアーカイブ］ ご利用上の注意

このPDFファイルは、株式会社インプレスR&D（株式会社インプレスから分割）が1994年～2006年まで発行した月刊誌『インターネットマガジン』の誌面をPDF化し、「インターネットマガジン　バックナンバーアーカイブ」として以下のウェブサイト「All-in-One INTERNET magazine 2.0」で公開しているものです。

http://i.impressRD.jp/bn

このファイルをご利用いただくにあたり、下記の注意事項を必ずお読みください。

- 記載されている内容（技術解説、URL、団体・企業名、商品名、価格、プレゼント募集、アンケートなど）は発行当時のものです。
- 収録されている内容は著作権法上の保護を受けています。著作権はそれぞれの記事の著作者（執筆者、写真の撮影者、イラストの作成者、編集部など）が保持しています。
- 著作者から許諾が得られなかった著作物は収録されていない場合があります。
- このファイルやその内容を改変したり、商用を目的として再利用することはできません。あくまで個人や企業の非商用利用での閲覧、複製、送信に限られます。
- 収録されている内容を何らかの媒体に引用としてご利用する際は、出典として媒体名および月号、該当ページ番号、発行元（株式会社インプレスR&D）、コピーライトなどの情報をご明記ください。
- オリジナルの雑誌の発行時点では、株式会社インプレス R&D（当時は株式会社インプレス）と著作権者は内容が正確なものであるように最大限に努めましたが、すべての情報が完全に正確であることは保証できません。このファイルの内容に起因する直接的および間接的な損害に対して、一切の責任を負いません。お客様個人の責任においてご利用ください。

このファイルに関するお問い合わせ先
株式会社インプレスR&D
All-in-One INTERNET magazine 編集部
im-info@impress.co.jp