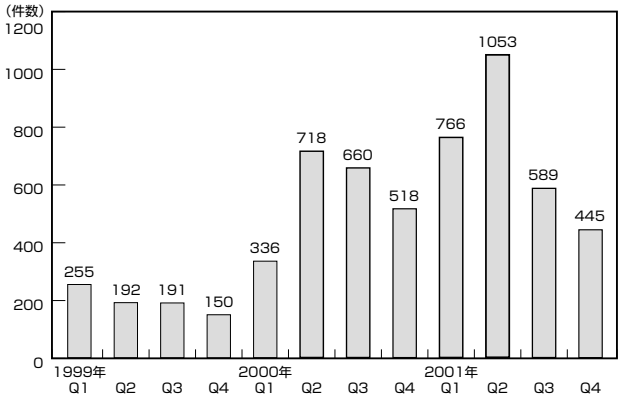
第3章 犯罪/セキュリティー

不正アクセス　コンピュータワームが高度化、さらに悪質に

資料3-3-1 過去3年間のインシデントレポート数推移（JPCERT/CC）



資料3-3-2 2001年度に発行されたセキュリティー勧告などの数

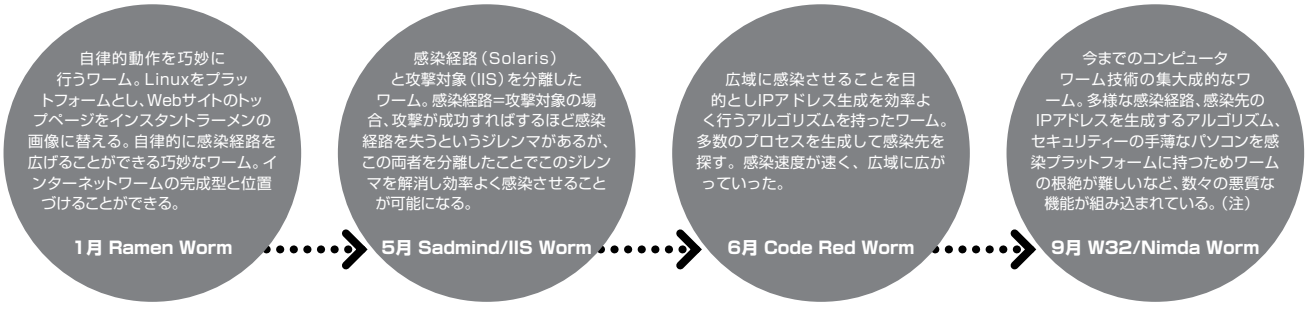
組織	ドキュメント名	数	URL
CERT/CC	セキュリティーアドバイザリー	37	www.cert.org
マイクロソフト	セキュリティービルトイン	60	www.microsoft.com/technet/security/
JPCERT/CC	緊急報告	26	www.jpcert.or.jp

出所　鈴木裕信氏が作成

（注）Q1,Q2,Q3,Q4 ：「四半期」の意味
インシデントとはコンピュータやネットワークのセキュリティーを侵害する、あるいは侵害を試みる人為的な行為で、意図的あるいは偶発的に発生する事象である。侵入を試みないポートスキャンなども含まれる。法律で規定している「不正アクセス」よりも広い概念である。

出所　JPCERT/CC（コンピュータ緊急対応センター）の「活動概要」を元に鈴木裕信氏が作成

資料3-3-3 2001年におけるワームの進化



（注） コンピュータウイルスとワームの違いについて
W32/Nimda Wormはパソコン上でも感染・増殖するため、ウイルスに分類される場合が多い。ウイルスは独立したプログラムではなく、他の実行可能なファイルに寄生する形でのみ機能を発現させることができるものである。ワームは単独で実行可能なプログラムで、自律的に振る舞う。技術的側面からの定義には違いがあり、本来は区別するべきであるが、パソコン上では便宜上、両者は区別されることなくウイルスという1つのカテゴリーに分類されることが多いように思われる。

出所　鈴木裕信氏が作成

解　説

2001年を一言で表せば「コンピュータワーム進化の年」だった。昨年度は不正アクセスの傾向として「大規模化・自動化・ワームツールキット」の3点を指摘したが、それが現実となった年だった。

2001年1月は、2000年暮れから発生していたRamen Wormが猛威をふるった。5月は感染経路がSolarisで攻撃対象がMicrosoft IISという感染と攻撃が分離されている新しいコンセプトのSadmind/IIS Wormが発生する。

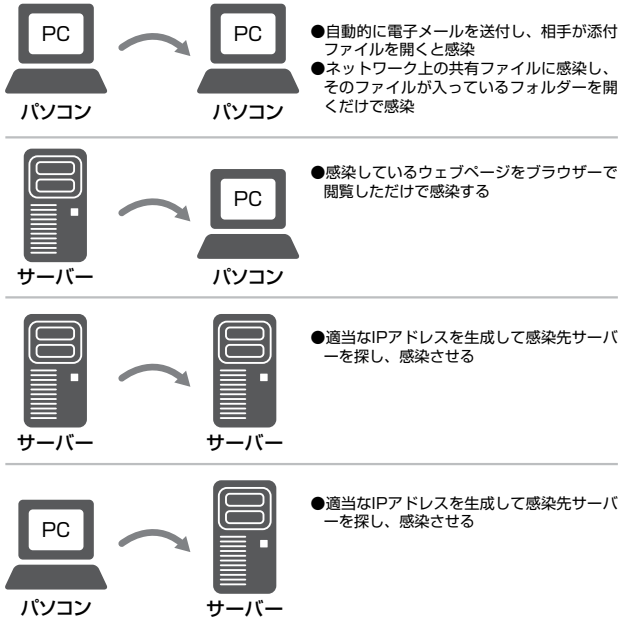
6月はCode Red Wormが発生。これは Microsoft Index Server ISAPI Extensionのバッファーオーバーフローの脆弱性を狙って侵入するワームである。感染したサーバー上で多数のプロセスを生成して攻撃先を探す。また効率の良いIPアドレス生成法を用いて攻撃先IPアドレスを決めるのも特徴だ。そのため感染速度はかつてないほど速く、短時間で世界各地のサーバーに感染していった。Code Red Wormはバッファーオーバーフローフローを引き起こすための異常な長さのデータをhttpポートへ送信するので、その影響は攻撃対象となるサーバーだけでなく、そのような大量の入力を想定していなかったネットワーク機器が誤動作またはハングアップする問題も広く発生した。

9月にはコンピュータワームの中で最も感染能力の高いW32/Nimda Wormが現れた。W32/Nimda Wormは感染経路がかつてないほどの多様な経路を持っている点が最大の特徴である。サーバー間だけではなく、パソコン間でも感染し、その感染したパソコンからサーバーを攻撃・感染させる。そのためインターネットから隔離されているイントラネットのサーバーであっても被害にあう。

（鈴木裕信　ソフトウェアコンサルタント）

脆弱性をもつパソコンやサーバーを確実に攻撃

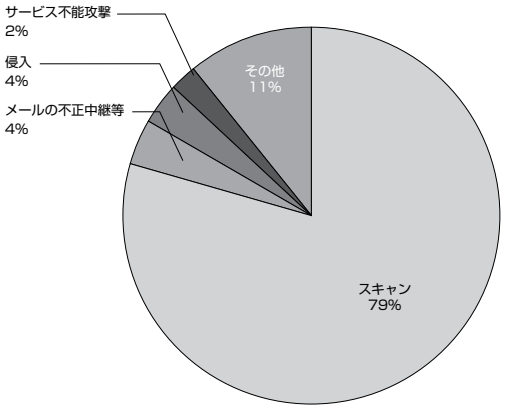
資料3-3-4　W32/Nimda Wormの感染経路



※攻撃に使うサーバーやパソコンの脆弱性は、すでに広く知られているものである。この傾向はW32/Nimda Wormに限らず、他のワームも同様である。

出所　鈴木裕信氏が作成

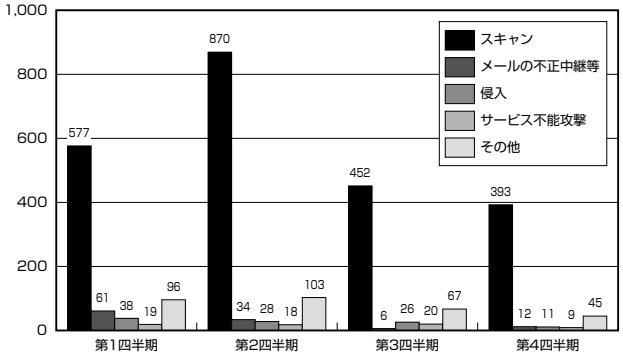
資料3-3-5　2001年インシデント報告発生状況（年間の内訳）



（注）2001年にJPCERT/CCが受け付けたインシデント報告
グラフからもわかるように脆弱性へのスキャンは高い頻度で発生している。インターネットに接続されているマシンは常にスキャンを受けていると考えた方が良い。スキャン先IPアドレスは自動的に生成されるので脆弱性を持つサイトがインターネットからアクセス可能であれば発見されるのは時間の問題だといえる。

出所　JPCERT/CC（コンピュータ緊急対応センター）の「活動概要」を元に鈴木裕信氏が作成

資料3-3-6　2001年インシデント報告発生状況（四半期ごとの推移）



出所　JPCERT/CC（コンピュータ緊急対応センター）の「活動概要」を元に鈴木裕信氏が作成

（本文注1）JPCERT/CCでは毎週セキュリティー関連情報をメールで届けるサービス（無料）を行っている。詳しくはwww.jpcert.or.jpのウェブサイトを参照のこと。

解　説

W32/Nimda Wormは攻撃先を探すためのIPアドレス生成方法がエレガントな設計になっている点が特徴的である。IPアドレス全体の利用空間は虫食い的であり、そこをランダムに探していては効率が悪い。そこで感染したマシンのIPアドレスが含まれるIPアドレスブロックを集中的に走査する。このような形で同じ組織内、同じISP内、あるいは同じNIC組織が管理しているIPアドレスブロックを探査するため、ヒット確率が高くなる。この特性はイントラネット内での感染であっても同様で、そのイントラネット内サーバーを集中的に攻撃することになる。

これはグローバル地域にも当てはまる。たとえばAPNICが管理するIPアドレスブロックに属する日本、中国、韓国、香港などは同じグループにある。そのためブロードバンド先進国である韓国での爆発的なW32/Nimda Worm感染の影響が、日本も含むアジア圏全体に影響を与えることとなった。W32/Nimda Wormがアジア圏内で猛威をふるう一方で、同圏内の国々でインシデント対応の協調体制がなかったことは大きな問題として残った。

W32/Nimda Wormはインターネット上に存在する膨大な数のパソコン上でも感染するので、サーバー管理者だけではなく一般ユーザーによる対策も必要となる。そのため効果的な駆除は非常に困難といえ、現在でもウェブサーバーのログを見れば、多数の攻撃跡が観察できる。

サーバーなどの脆弱性に対するメインテナンスを怠ると、その脆弱性を狙ったワームが発生すれば、確実に餌食になってしまう。管理者はこまめなセキュリティー情報の収集（注1）と、頻繁なシステムのメインテナンスが必須である。

（鈴木裕信　ソフトウェアコンサルタント）

［インターネット白書ARCHIVES］ご利用上の注意

このファイルは、株式会社インプレスR&Dが1996年～2012年までに発行したインターネットの年鑑『インターネット白書』の誌面をPDF化し、「インターネット白書ARCHIVES」として以下のウェブサイトで公開しているものです。

http://IWParchives.jp/

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、データ、URL、名称など）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・図の作成者、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掲載されていない場合があります。
- このファイルの内容を改変したり、商用目的として再利用したり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される際は、出典として媒体名および年号、該当ページ番号、発行元（株式会社インプレスR&D）などの情報をご明記ください。
- オリジナルの発行時点では、株式会社インプレスR&D（初期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。

お問い合わせ先 | 株式会社インプレスR&D | ✉ iwp-info@impress.co.jp