



JSOC Quarterly Security Report

2003 年 1 月 ~ 2003 年 3 月

rev.1.0

2003 年 5 月 12 日

**Japan
Security
Operation
Center**

目次

| | |
|--------------------------|----|
| 総評 | 3 |
| 1. はじめに..... | 4 |
| 2 . 統計分析 | 5 |
| 2.1 イベント発生件数の遷移..... | 5 |
| 2.2 イベントレベル..... | 6 |
| 2.3 攻撃発信国 | 7 |
| 2.4 イベント別分析 | 8 |
| 3. ワームの動向..... | 10 |
| 3.1 SLAMMER ワーム..... | 10 |
| 3.2 DELODER ワーム | 11 |
| 3.3 NIMDA ワーム..... | 12 |
| 3.4 CODERED ワーム..... | 13 |
| 4. アナリストの視点..... | 14 |
| 4.1 注意が必要なセキュリティホール..... | 14 |
| 4.2 イベントとの関連性..... | 15 |

総評

この四半期における最大のトピックは、やはりマスコミにも大きく報道された Slammer ワームの出現かと思えます。Slammer ワームは感染対象のシステムの破壊や、情報漏洩、ホームページの改竄など、直接的な被害を与える挙動はしませんが、さらなる感染活動を行うための大量のパケットを生成することによって、帯域に負荷を与え、事実上ネットワークを利用不能にさせる被害を与えました。これは、Slammer ワームが利用する攻撃が udp の通信を利用するものであったことが関係しています。Nimda や CodeRed 等、これまでのワームでは、主に tcp の通信を利用するものであったため、攻撃を行う前に、攻撃先のホストとのネゴシエーションの通信が必要となり、udp と比較してパケットの大量発生が起りにくいという特徴がありました。Slammer ワームによる韓国の被害状況は、udp を対象とするワームの脅威が露呈した事象だと言えます。udp を利用するアプリケーションとしては、tcp ほど数は多くないものの、DNS 等必要不可欠なものもあり、問題点の早急な対策には一層の注意が必要かと思われます。また、udp のもうひとつの特徴として、パケット偽造の容易性が挙げられます。Slammer ワーム自体はパケットを偽造して発信元を偽ったりしませんが、パケット偽造を行う亜種の出現も考えられます。3月の CodeRed.F の出現に見られるように、ワームの亜種については今後も発生する可能性があります。

ワームに関しては、既知のワームやその亜種だけでなく、新種のワームの出現も危惧されるどころです。3月は、IIS（正確には IIS を含むいくつかの Windows アプリケーションが利用するモジュール）や sendmail といった広く利用されているアプリケーションに新たな脆弱性が発見されました。今までのワーム出現の傾向としては、問題が報告されて、半年から 1 年後にその問題を利用するワームが出現しています。しかし、問題が報告されてからすぐにワームが出現してもおかしくない状況です。特に利用頻度の高いアプリケーションの問題は狙われやすく、大きな影響を与えます。利用頻度の高いアプリケーションに限ったことではありませんが、敏速な対策を行うことが重要です。また、ワームに感染したノート PC 等を内部ネットワークに接続してしまい、組織内にワームを持ち込んでしまうケースが相変わらず多く見受けられますので、機器の管理や運用ルールにも注意が必要です。

ワーム以外のトピックとしては、3月後半にイラク戦争が始まったことにより、サイバー空間においても動きがありました。主にホームページの改竄を行う事件が多方面で発生しましたが、いわゆるサイバーテロと呼ばれるような深刻な問題は発生していません。ホームページ改竄に利用された脆弱性は、IIS や Apache 等の問題で比較的古いものでした。つまり、問題の対策をせずに放置したサーバが被害を受けたこととなります。今までに報告された脆弱性に限らず、今後報告されるであろう脆弱性の情報にも注視し、対策を講じることを強く推奨いたします。

1. はじめに

本資料は、下記対象期間内に JSOC において検知したイベントの分析結果、および脅威情報との関連性を分析し、まとめたものです。

対象期間

2003 年 1 月 1 日 ~ 2003 年 3 月 31 日

本資料の目的は、分析結果により日本国内での社会的情勢や IT 技術の動向、および国際的な政治的イベントやテロリズムを含む脅威情報などの海外情報と、国内における不正アクセスとの関係を関連付けることが挙げられます。ネットワークセキュリティにおける不正アクセスと脅威情報の橋渡しの役割に位置付けることにより、今後の情報危機管理対策に役立てることが期待できます。

本資料の内容は、JSOC で監視を行っている全監視対象ネットワークおよびホストから得たデータを基に全体の不正アクセスの傾向を導きだし、様々な角度から比較評価したものです。この資料は日本国内におけるインターネット事情と関係したものではありません。

JSOC Analysis Team

2 . 統計分析

2.1 イベント発生件数の遷移

分析対象期間（2003/1/1～2003/3/31）のイベント発生件数は77,291件です。

イベント発生件数とは、JSOCが監視するセンサー（ファイアウォールやIDS）が検出したログをJSOCアナリストが解析し、誤報（フォールスポジティブ）を排除した件数です。

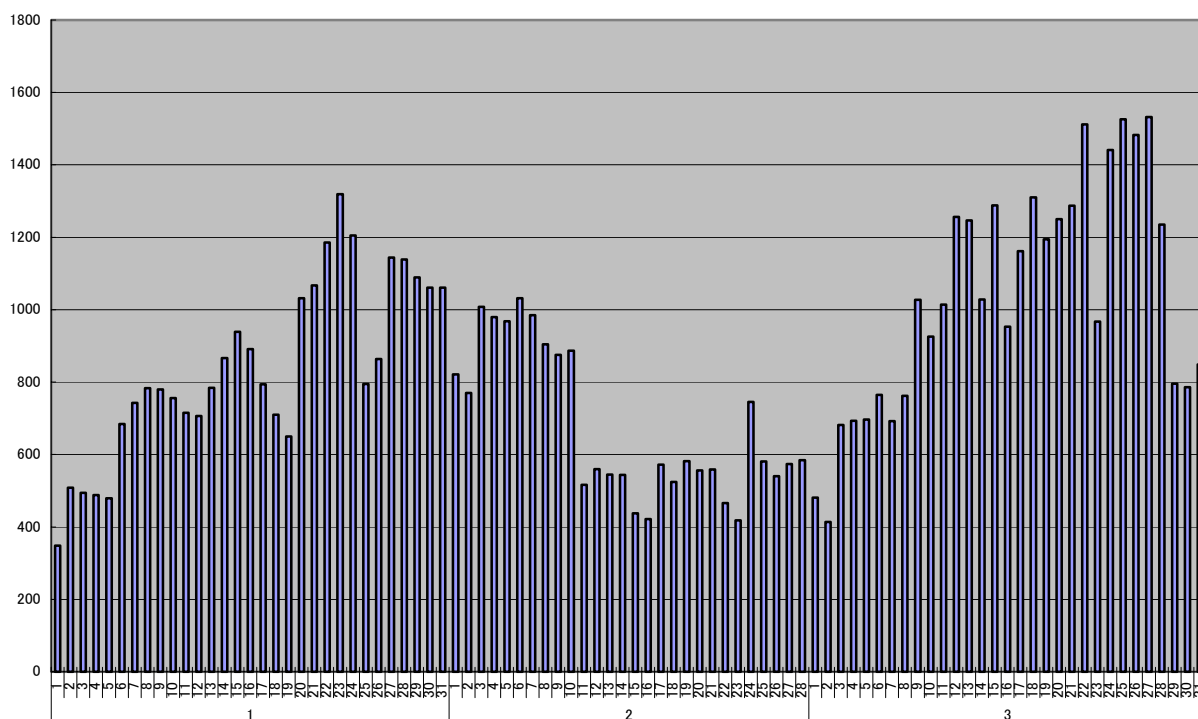


図 1 イベント発生件数の推移

1月は月初から月末に掛けて徐々にイベント件数が増加しています。2月は比較的に少ない件数で推移しているものの、3月は増加の一途をたどっています。イベントの大半が攻撃の予備調査（ポートスキャンやプローブなど）や、ワームによるものでした。1月にはSlammerワーム、3月にはCodeRedワームの亜種が発生したことに起因しています。

2.2 イベントレベル

イベントレベル説明

Information :

悪意のある通信の可能性を含んでいるが、日常的な通信である可能性が著しく高い場合、または不審な通信であるが、ファイアウォールによりドロップされた通信を指します。例として、インスタントメッセージなどがあります。

Warning :

大抵の場合は、ポートスキャンやプローブなどのような意図的な通信を指し、監視対象ホストの情報が漏洩した可能性がある場合です。また、Critical に昇格する可能性を含んだ不審な通信に関しても使用される場合があります。

Critical :

特定のシステムへの不正侵入が成功した可能性が著しく高い場合です。ワームの感染なども含まれます。

Emergency :

不正侵入事実が確認された場合です。または、監視対象ホストから外部（インターネット）へ致命的な攻撃を検知した場合に適用されます。

表 1 発生イベントレベル数

| イベントレベル | 2003年1月 | 2003年2月 | 2003年3月 |
|-------------|---------|---------|---------|
| Information | 22764 | 16173 | 28365 |
| Warning | 3282 | 2746 | 3853 |
| Critical | 30 | 36 | 36 |
| Emergency | 4 | 1 | 1 |
| 総計 | 26080 | 18956 | 32255 |

Information レベルおよび Warning レベルの件数は多いですが、Critical レベルや Emergency レベルも毎月 40 件弱発生しています。この四半期には、IIS（正確には IIS を含むいくつかの Windows アプリケーションが利用するモジュール）や sendmail といった広く利用されているアプリケーションに新たな脆弱性が発見されましたが、これらの脆弱性を悪用する攻撃は JSOC において数件検出されましたが、被害を受ける事態には至っていません。Critical レベルや Emergency レベルのイベントは、3 ヶ月で 108 件発生していますが、このうちの 57 件は内部の人間が誤ってノート PC などでワームを持ち込んでしまったケースです。ワーム持ち込みのケース以外では、ほとんどが古い脆弱性を悪用されたケースであり、依然、対策が行われていないサイトが見受けられました。対策を行わないと実際に被害を受けるということが示されています。被害を受ける前に敏速に対策を講じるよう、細心の注意が必要です。

2.3 攻撃発信国

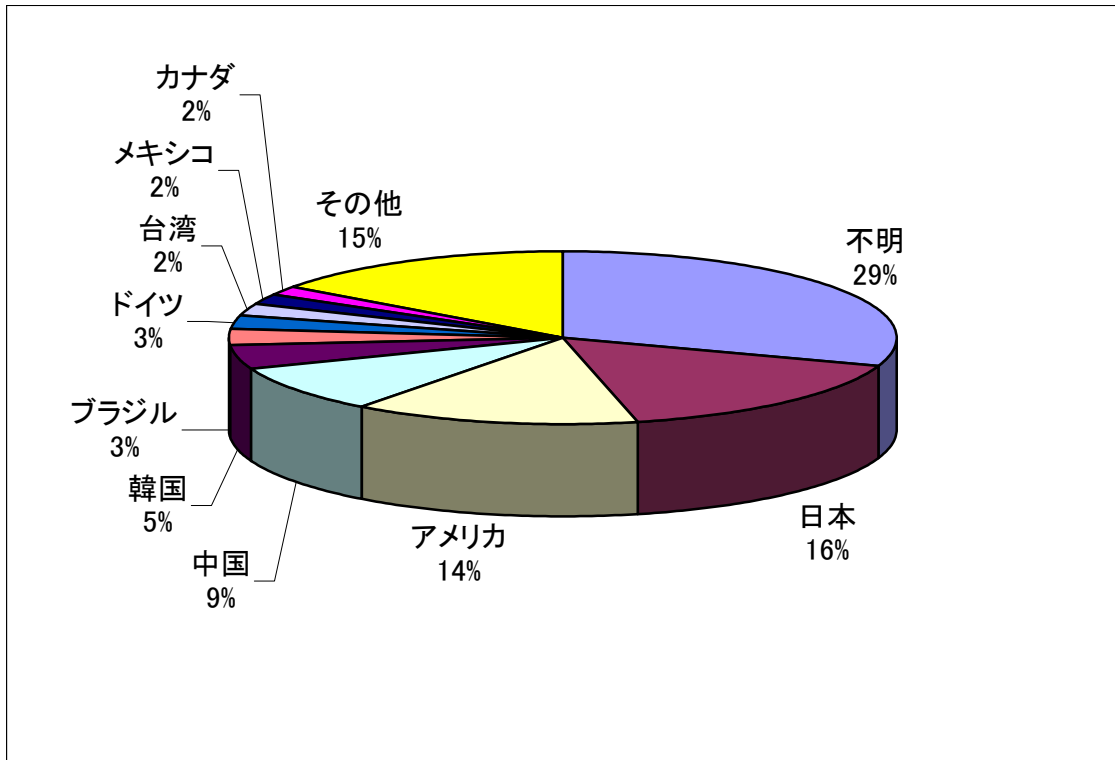


図 2 攻撃発信国の分布

上の図は JSOC で検出された攻撃のソース IP アドレスを元に、攻撃元を国別で集計し、各国の分布をグラフ化したものです。不明を除いてトップが日本、続いて米国、中国、韓国となっています。過去の統計と比較すると、中国、韓国からの攻撃の比率が減少しているのですが、上位 4 カ国に変化はありません。攻撃が行われる場合、踏み台を利用するなどのケースが考えられ、実際の攻撃発信国を正確に表すものではありません。

2.4 イベント別分析

表 2 発生イベント Top 10 (カッコ内はイベントが検出されるワーム)

| | 攻撃名称 | ログ件数 |
|----|--|------------|
| 1 | Horizontal Scan (各種ワーム) | 19,899,158 |
| 2 | MS-SQL:REG-STACK (Slammer ワーム) | 297,482 |
| 3 | TCP-SWEEP | 286,507 |
| 4 | HTTP_Windows_Executable (Nimda ワーム等) | 255,044 |
| 5 | Vertical scan | 207,903 |
| 6 | TCP-FLAGS | 113,355 |
| 7 | MS-SQL Control Overflow (Slammer ワーム) | 56,264 |
| 8 | HTTP_IIS_URL_Decoding (Nimda ワーム、CodeRed ワーム等) | 50,929 |
| 9 | HTTP_IIS_UTF8_Evasion (Nimda ワーム、CodeRed ワーム等) | 35,595 |
| 10 | IIS:IDA-ISAPI-OVERFLOW (CodeRed ワーム) | 35,363 |

上の表は JSOC で検出された攻撃のトップ 10 です。そのほとんどが、Slammer や Nimda, CodeRed 等のワームによって検出される攻撃です。ワームは不特定多数のターゲットホストに対して、短期間に大量の攻撃を行うため、必然的に検出件数の上位に位置付けられます。

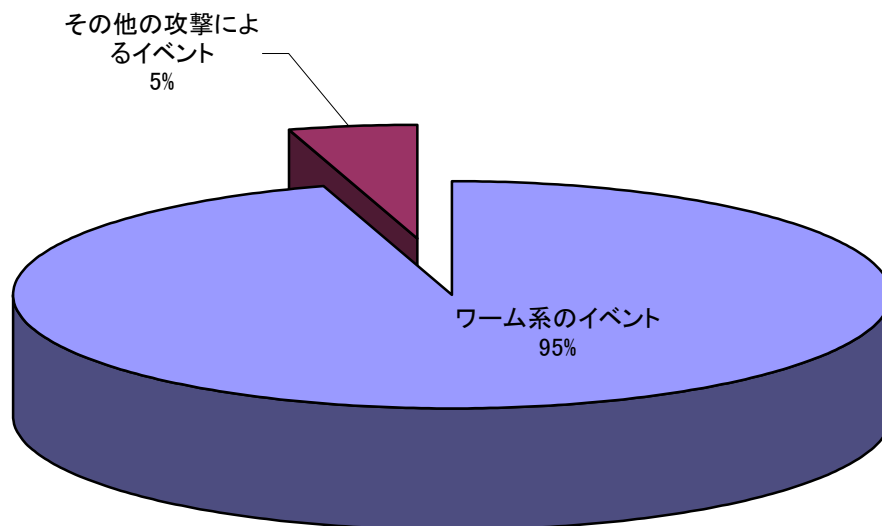


図 3 ワーム系のイベント比率

検出された攻撃のうち、ワームによって発生するものを除いてみると、以下のようなトップ 10 となります。

表 3 ワームを除く発生イベント Top 10

| | 攻撃名称 | ログ件数 |
|----|--------------------------|---------|
| 1 | TCP-SWEEP | 286,507 |
| 2 | Vertical scan | 207,903 |
| 3 | TCP-FLAGS | 113,355 |
| 4 | WEB:FORMMAIL | 27,558 |
| 5 | TCP_Service_Sweep | 20,204 |
| 6 | PortMapper (RPC) Probe | 19,629 |
| 7 | PORT-ZERO | 13,662 |
| 8 | SSH:X2-TESSO-CRC32-OFLOW | 12,871 |
| 9 | NetBus10 Probe | 6,878 |
| 10 | traceroute | 5,882 |

ワームを除いた攻撃のトップ 10 では、そのほとんどが予備調査（ポートスキャンやプローブなど）のイベントです。予備調査以外では、SSH サーバの CRC32 バッファオーバーフロー攻撃や formmail CGI へのアクセス等が検出されています。formmail は Web 経由でのメール送信を行う CGI である formmail に関するイベントが検出されています。これは、formmail を利用した SPAM メールを送信（第三者中継）を行おうとしているものであり、第三者中継目的で formmail CGI の存在を確認するものが最近増えてきています。メール第三者中継の対策は SMTP サーバだけが注目されがちですが、CGI にも注意が必要です。

3. ワームの動向

この四半期には Slammer や Deloder など、いくつかのワームが猛威を振るい、話題となりました。また、依然 Nimda や CodeRed 等に感染するホストも存在しています。ここでは代表的なワームの攻撃件数を、JSOC 監視対象のホスト 1 台に対する日別の平均件数で算出し、その推移をグラフ化しています。

3.1 Slammer ワーム

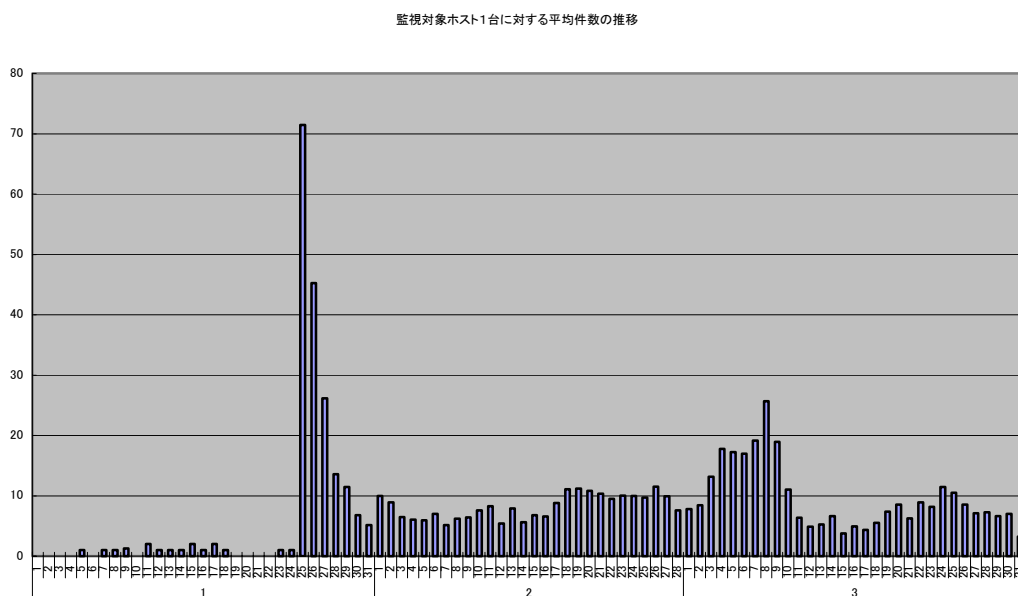


図 4 Slammer ワームの推移

このグラフは Slammer ワームが攻撃を行う 1434/udp へのアクセス件数を、ファイアウォールのログから集計したものです。件数の全てが Slammer ワームによるものではありませんが、Slammer ワーム発生以降、顕著に件数が増加されていることもあり、大半がワームと考えてよいかと思えます。マスコミにも大きく報道された 1 月 25 日の事象をピークに、件数は減少しているものの、依然、感染しているホストが存在していることがわかります。Slammer ワームは、これまでのワームとは異なり、ファイルに感染せず、メモリのみに感染することから、感染してもマシンを再起動すると活動はしません。それにもかかわらず、いまだに感染ホストからのアクセスが検出されています。Slammer ワームはネットワークに高負荷を与えることから、管理者が異変には気付いているものの、ワームによるものと認識していなかったり、ワームに感染したノート PC の内部ネットワークへの持込などがあるのではと思われます。

3.2 Deloder ワーム

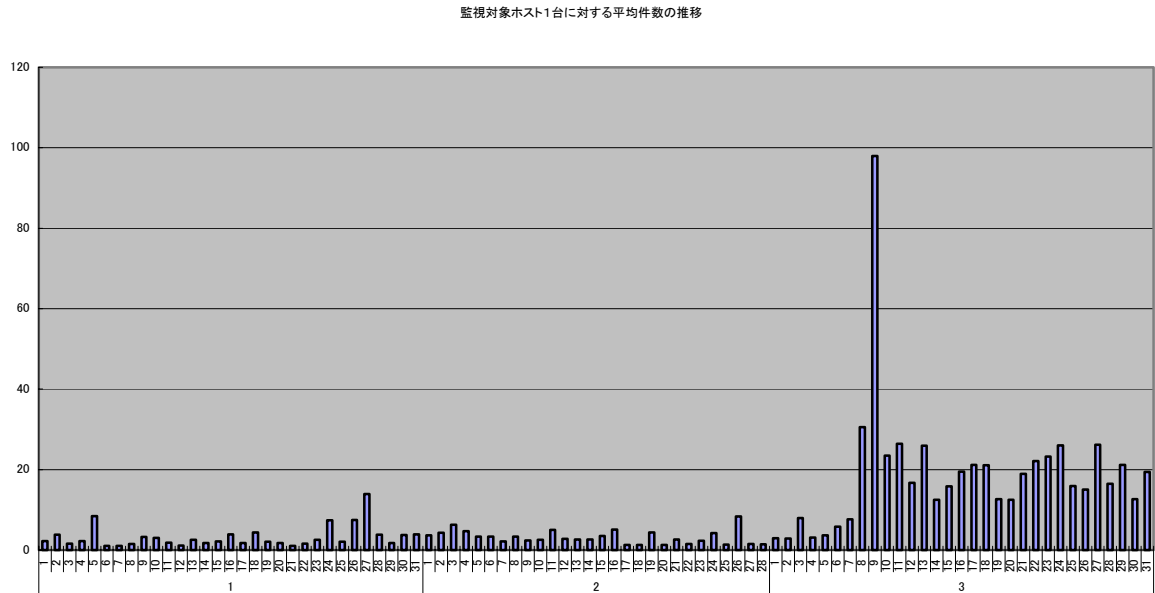


図 5 Deloder ワームの推移

このグラフは Deloder ワームが攻撃を行う 445/tcp へのアクセス件数を、ファイアウォールのログから集計したものです。445/tcp は Microsoft Windows の共有資源へのアクセスの際に利用されるポートです。Deloder ワームは、感染経路として Windows の共有資源を利用します。445/tcp へのアクセスは 3 月 10 日頃から極端に増加していることが見て取れます。これは Deloder ワームの影響です。当初、Deloder ワームは、445/tcp という通常ファイアウォールで阻止される通信を感染経路として利用するため、インターネットではあまり蔓延しないであろうという見解がされていましたが、実際に感染しているホストが見受けられます。おそらく、ブロードバンド環境の普及で、ファイアウォールを設置していない個人の Windows マシンが感染しているのではと想像できます。

3.3 Nimda ワーム

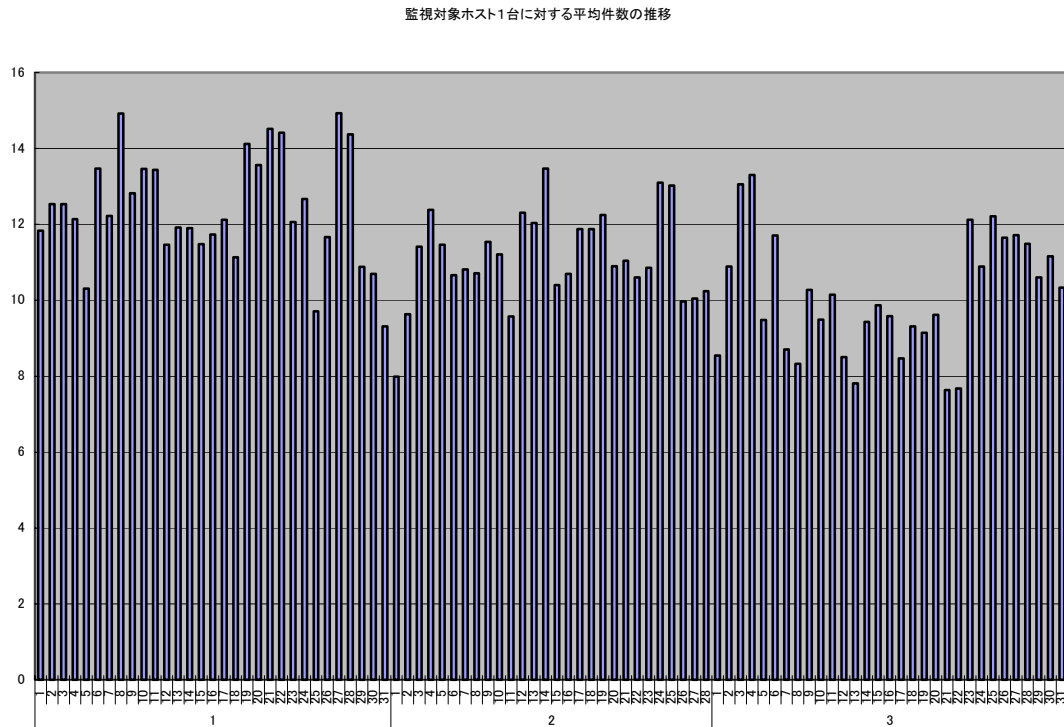


図 6 Nimda ワームの推移

このグラフは IDS によって Nimda ワームと検出された件数を集計したものです。ワーム発生から年月が経っているにも関わらず、いまだに多くのホストが感染しているのがわかります。Nimda ワームについては、一向に衰える傾向も無く、この攻撃は既に日常的な通信となっています。

3.4 CodeRed ワーム

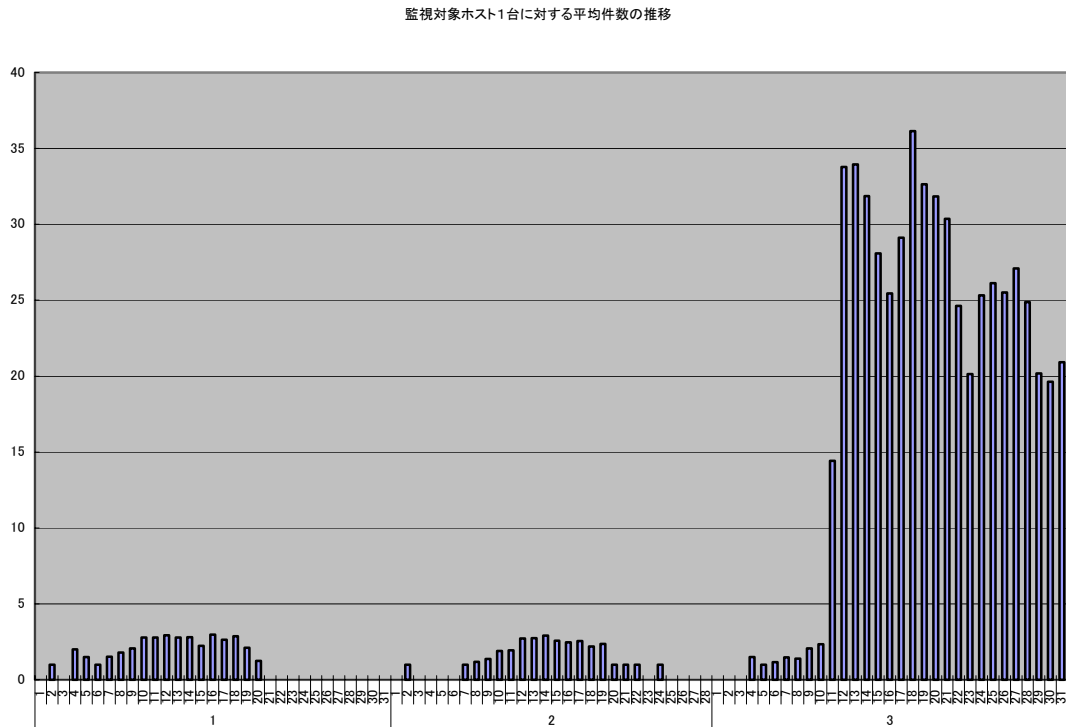


図 7 CodeRed ワームの推移

このグラフは IDS によって CodeRed ワームと検出された件数を集計したものです。CodeRed ワームについては、前述の Nimda ワームと比較しても件数が少ないことがわかります。しかし、3月11日を境に急激に件数が増加していることがわかります。これは、CodeRed II の亜種である CodeRed.F が発生したためです。CodeRed II は、感染先のシステム日付の年の部分をチェックしており、寿命がありました。そのため、衰退の一途をたどっていましたが、亜種の出現によって、新たに感染するホストが増えています。これは、いまだに脆弱性の対策を行っていないホストが多数存在することを物語っています。CodeRed.F と CodeRed II との違いは、日付チェックの部分のみです。

4. アナリストの視点

4.1 注意が必要なセキュリティホール

3月には、IIS（正確には IIS を含むいくつかの Windows アプリケーションが利用するモジュール）や sendmail といった広く利用されているアプリケーションに新たな脆弱性が発見されました。利用頻度の高いアプリケーションの問題ということから、これらの問題を利用するワームの出現も懸念されます。

前者の IIS に関する問題については、いくつかの Windows アプリケーションが共有して利用するダイナミックリンクライブラリである ntdll.dll に存在する問題です。いくつかのセキュリティ勧告では、この問題を IIS の問題として取り上げていますが、他のアプリケーションでも影響を受ける問題ですので、注意が必要です。IIS の使用に関わらず Windows のホストに対しては至急セキュリティパッチを適用することを推奨します。尚、この脆弱性を悪用する攻撃ツールも出回っていますが、現在のところ、日本語版の Windows 環境に対して影響を与えるものは確認されていません。

関連情報

http://www.lac.co.jp/security/intelligence/SNSSpiffy/New_Attack_Vectors_and_a_Vulnerability_Dissection_of_MS03-007.html

後者の sendmail の問題については、立て続けに 2 件の問題が発見されています。先に報告された問題を対策しても、2 件目に報告された問題は解決しませんので注意が必要です。この問題を攻撃するツールも出回っています。出回っているツールは特定のプラットフォームをターゲットとするものですが、別のプラットフォーム用に改造することは、さほど困難ではないため、一層の注意が必要です。sendmail を利用しているホストに対しては、バージョンアップやセキュリティパッチを適用するなど、早急な対策を行うことを推奨します。

関連情報

http://www.lac.co.jp/security/intelligence/CERT/CA-2003_07.html

http://www.lac.co.jp/security/intelligence/CERT/CA-2003_12.html

4.2 イベントとの関連性

JSOC では、前述した脆弱性についてのシグネチャも含め、IDS ベンダなどのセキュリティベンダのシグネチャリリースを待たずに、JSOC 独自のシグネチャをいち早く作成することにより、監視対象サイトへの対策をとりました。前述の脆弱性に対する攻撃については、IDS で数多く検出されています。しかし、それらの検出結果をアナリストが解析したところ、ほとんどが誤検知（フォールス・ポジティブ）であることがわかっています。現在のところ、誤検知ではなく実際の攻撃を検出したケースは数件ありますが、これによる被害（侵入など）は発生していません。