

我が国におけるインターネット治安情勢の分析について (平成20年度第1/四半期)

サイバーフォースセンター(CFC)では、全国にある警察施設のインターネット接続点において、ファイアウォール及び侵入検知装置(Intrusion Detection System:IDS)により攻撃等の活動に対する監視を行っている。本レポートは、平成20年度第1/四半期の監視状況を取りまとめたものである。

■ 第1/四半期における状況

◆ 総括

平成20年度第1/四半期における外部ネットワークからのファイアウォールに対する総アクセス件数は一日・1IP当たり約191.2件(前期比約7.9%増)であり、侵入検知装置におけるアラートの総検知件数は一日・1IP当たり約10.3件(前期比約9.9%増)であった。

1 ファイアウォールに対するアクセス件数：UDP1026番、UDP1027番及びTCP1433番ポートが増加

宛先ポート上位5位までの順位は、135/TCP、ICMP (Echo Request)、1026/UDP、1027/UDP及び1433/TCPの順で前期と同様であるが、1026/UDP、1027/UDP及び1433/TCPに対するアクセス件数が増加した。

国別の上位5か国までの順位は、中国、日本、米国、台湾及び韓国の順であり、中国からのアクセスが前期と比べ一日・1IP当たり約36.1%の大幅な増加となった。

2 IDSの総検知件数：Worm、Scan共に増加

SQL Slammer ワームの検知は、前期と比べ一日・1IP当たり約10.1%の増加となった。同様にScan Proxy attemptも、前期と比べ一日・1IP当たり約9.3%の増加となった。

国別では、中国が依然高い件数で推移している。

3 SYNflood 攻撃被害観測状況：総検知件数のうち、約95.6%は80/TCPへの攻撃

総検知件数は前期と比べ、一日・1IP当たり約83.4%増加した。総検知件数のうち約95.6%がウェブサーバ(80/TCP)への攻撃であった。

国別では、中国及び米国が高い割合を占めており、合わせて全体の約84.8%を占めている。

◆ 第1 / 四半期の主な出来事

4月9日	Flash Player の脆弱性について
4月18日	インターネット治安情勢更新(平成20年3月報を追加)
4月21日	マイクロソフト社のセキュリティ修正プログラムについて (MS08-014, 015, 016, 017) (4/21) 更新
4月22日	脆弱性情報の発表日の修正についてのお知らせ
4月23日	インターネット治安情勢更新(平成19年度第4四半期報を追加)
4月25日	マイクロソフト社のセキュリティ修正プログラムについて (MS08-018, 019, 020, 021, 022, 023, 024, 025) (4/25) 更新
5月1日	@police インターネット定点観測グラフの変更についてのお知らせ
5月13日	インターネット治安情勢更新(平成20年4月報を追加)
5月14日	マイクロソフト社のセキュリティ修正プログラムについて (MS08-026, 027, 028, 029)
6月11日	マイクロソフト社のセキュリティ修正プログラムについて (MS07-063, 064, 065, 066, 067, 068, 069) (6/11) 更新
6月11日	QuickTime の脆弱性について
6月19日	マイクロソフト社のセキュリティ修正プログラムについて (MS06-072, 073, 074, 075, 076, 077, 078) (6/19) 更新
6月20日	インターネット治安情勢更新(平成20年5月報を追加)
6月20日	マイクロソフト社のセキュリティ修正プログラムについて (MS08-030, 031, 032, 033, 034, 035, 036) (6/20) 更新
6月24日	アドビシステムズ社の Adobe Reader と Acrobat のセキュリティ修正プログラムについて
6月25日	マイクロソフト社のセキュリティ修正プログラムについて (MS07-042, 043, 044, 045, 046, 047, 048, 049, 050) (6/25) 更新

■ インターネット定点観測 - ファイアウォール / Firewall

◆ 宛先ポート別比率

全世界及び日本を発信元とする宛先ポート別の比率を以下に示す。

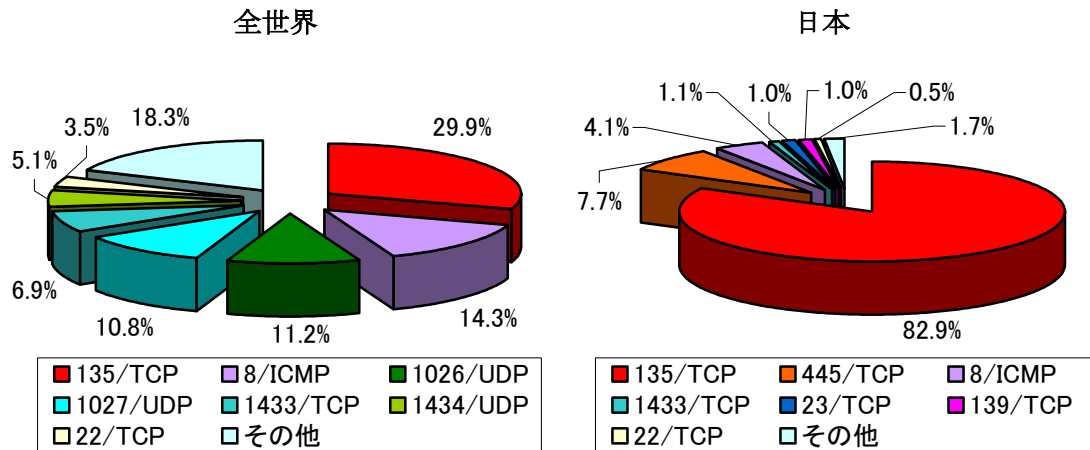


図1 宛先ポート別比率

全世界で見ると、前期と比較して 1026/UDP、1027/UDP 及び 1433/TCP の割合が大幅に増加している。これらは、中国からのアクセスが大半を占めている。

日本国内からのアクセスは、前期と比べ 445/TCP、8/ICMP 及び 1433/TCP の割合が減少したものの、23/TCP の割合は増加した。このポートは TELNET サービスで使用されるものであり、不正なアクセスの試みと推測される。

◆ 宛先ポート別推移

・ 135/TCP

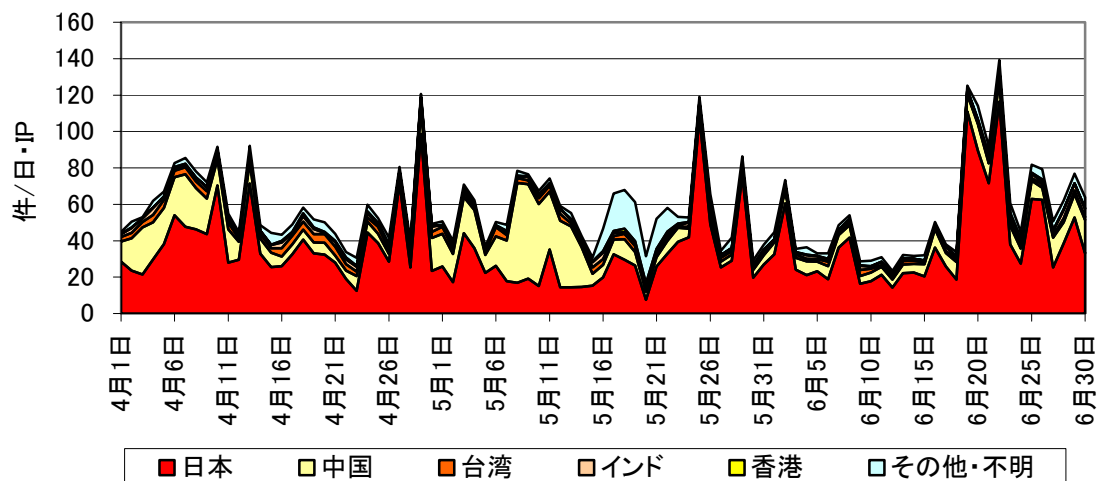


図 2 宛先ポート 135/TCP に対するアクセス件数

135/TCP に対するアクセス件数は前期と比較して一日・1IP 当たり約 5.2%減少している。3位の台湾及び4位のインドからのアクセス件数が減少したことから、全体として減少傾向となった。

135/TCP は、Blaster (平成 15 年 8 月発生) 等のウイルスが、RPC (Remote Procedure Call) の脆弱性 (MS03-026、MS03-039) を突いて感染活動を行う際にも使用される。

・ ICMP (Echo Request) ¹

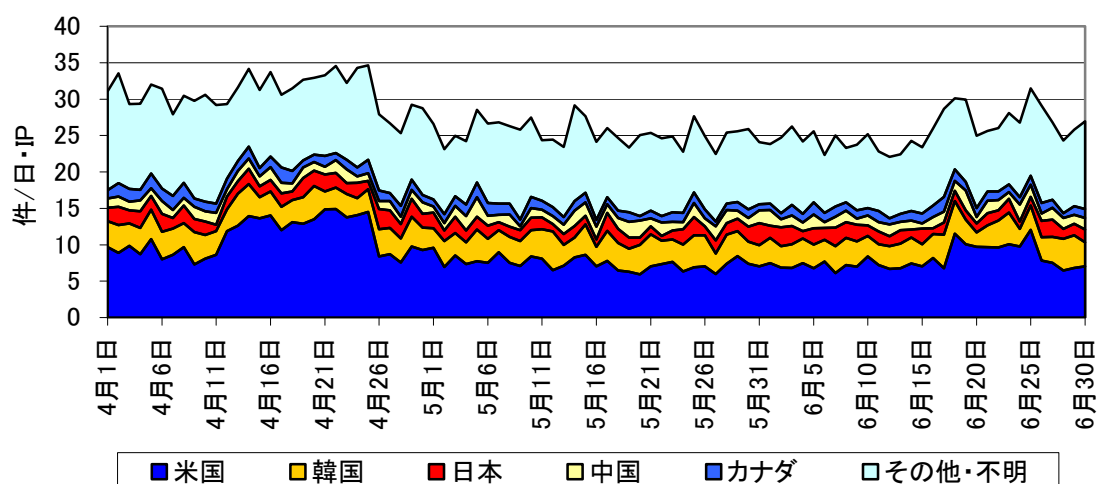


図 3 ICMP(Echo Request)の件数

¹ ICMP に関しては、タイプごとに集計している。

ファイアウォールに到達した ICMP (Echo Request) の件数は、前期と比較して一日・1IP 当たり約 15.6%減少している。上位 5 か国の件数については、いずれも減少している。

なお、ICMP (Echo Request) は、ネットワークの疎通調査などに利用されている。

・ 1026/UDP

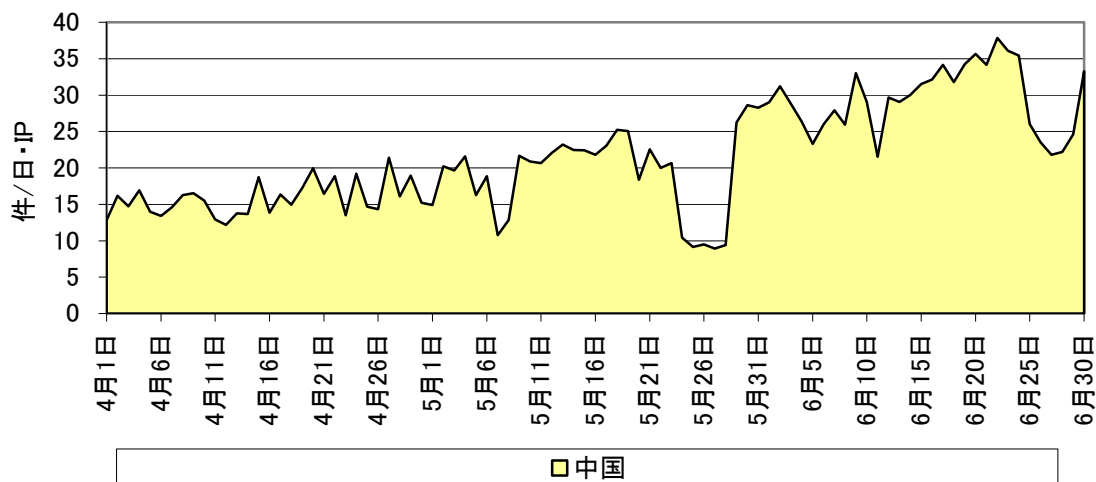


図 4 宛先ポート 1026/UDP に対するアクセス件数

1026/UDP に対するアクセス件数は前期と比較して一日・1IP 当たり約 37.9%増加しており、すべて中国からのアクセスであった。

なお、1026/UDP に対するアクセスの多くは、Windows の Messenger サービスを悪用したスパムである。スパムの内容は、商品の購入を促す広告等を表示させることを目的としたものであった。

・ 1027/UDP

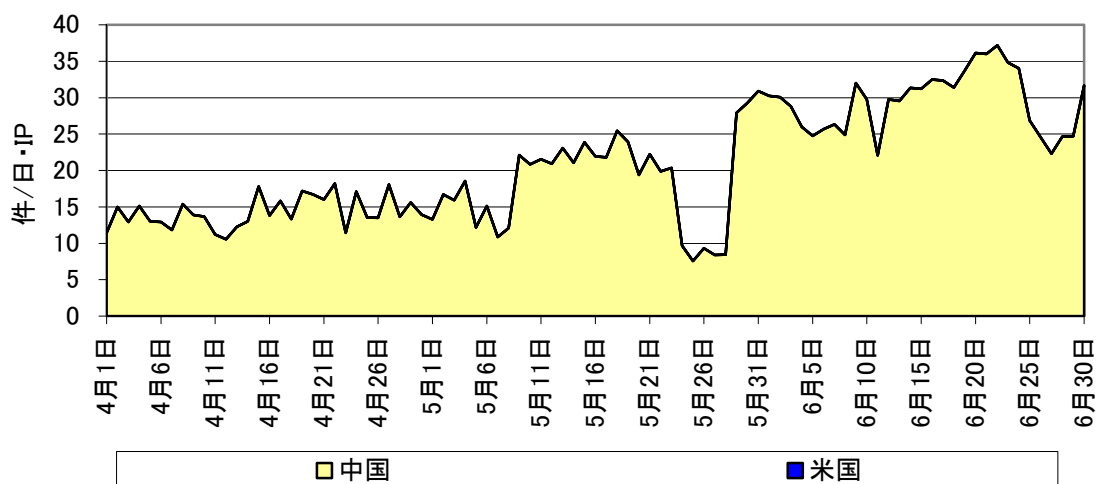


図 5 宛先ポート 1027/UDP に対するアクセス件数

1027/UDP に対するアクセス件数は前期と比較して一日・1IP 当たり約 57.6%増加しており、ほぼすべてのアクセスが中国からであった。

なお、1027/UDP に対するアクセスの多くは、1026/UDP と同様に Windows の Messenger サービスを悪用したスパムである。

・ 1433/TCP

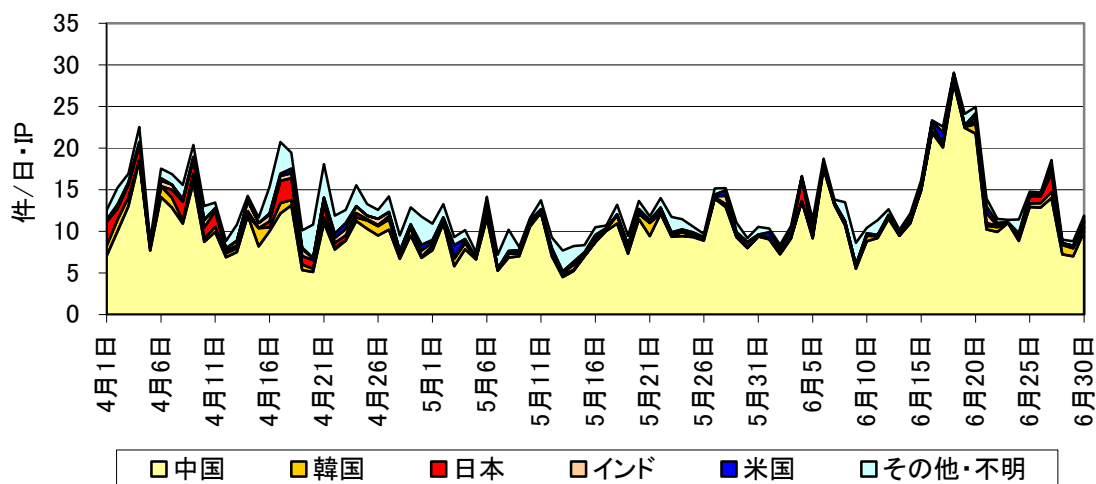


図6 宛先ポート 1433/TCP に対するアクセス件数

1433/TCP に対するアクセス件数は前期と比べ一日・1IP 当たり約 29.4%増加している。これは中国を発信元とするアクセス件数が一日・1IP 当たり約 40.4%増加したことが主な要因である。

なお、1433/TCP は Microsoft SQL Server で使用されるポートであり、このソフトウェアの脆弱性や脆弱なパスワードを狙ったものと推測される。

◆ 発信元（国/地域）別比率

発信元（国/地域）別比率を以下に示す。

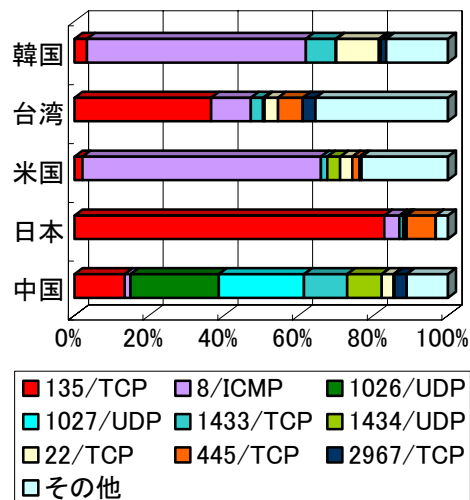
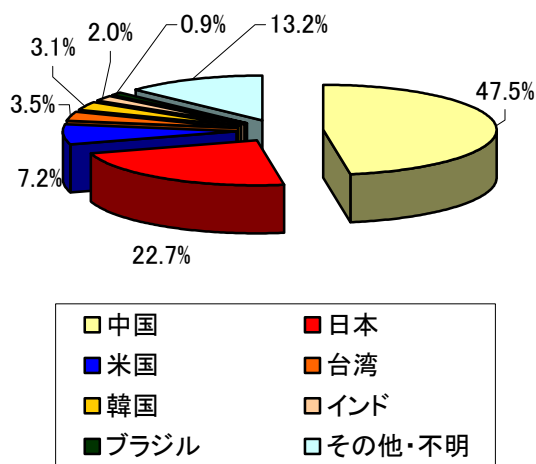


図 7 発信元（国/地域）別比率

国/地域別で見ると、前期と比較して中国からのアクセス件数が大幅に増加した。8/ICMP は、上位 5 か国でいずれも減少となった。

◆ 発信元（国/地域）別推移

・ 中国

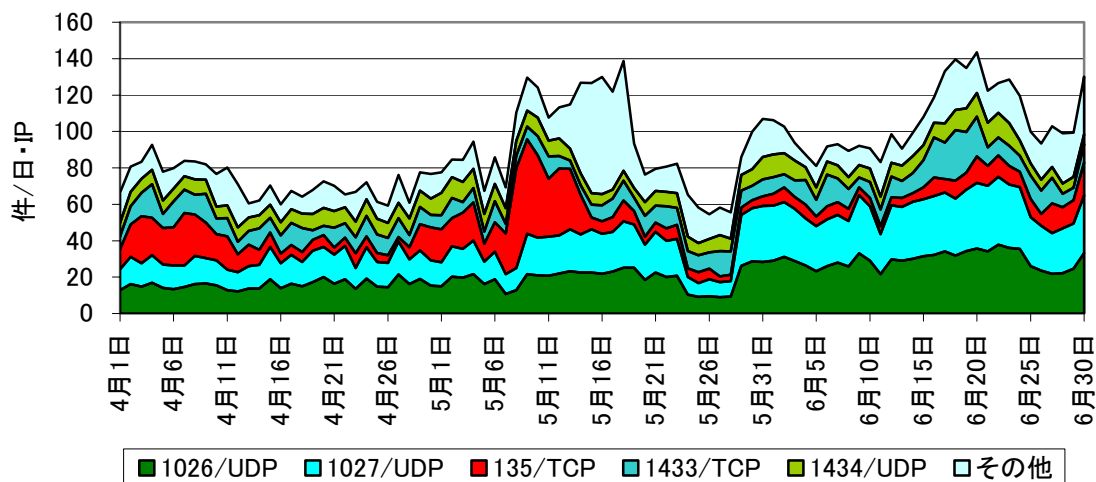


図8 中国からのアクセス件数

中国からのアクセス件数は前期と比べ一日・1IP 当たり約 36.1%増加している。中国からのアクセスのうち 1 位、2 位である 1026/UDP と 1027/UDP は、前期と比べ一日・1IP 当たり約 44.6%、57.6%の増加となった。また、1433/TCP も前期と比べ一日・1IP 当たり約 40.4%の増加となった。

1026/UDP 及び 1027/UDP に対するアクセス件数の増加は 2007 年 11 月 30 日以降から続いており、調査の結果、その多くが Windows の Messenger サービスを悪用したスパムである。スパムの内容は、商品の購入を促す広告等を表示させることを目的としたものであった。

・ 日本

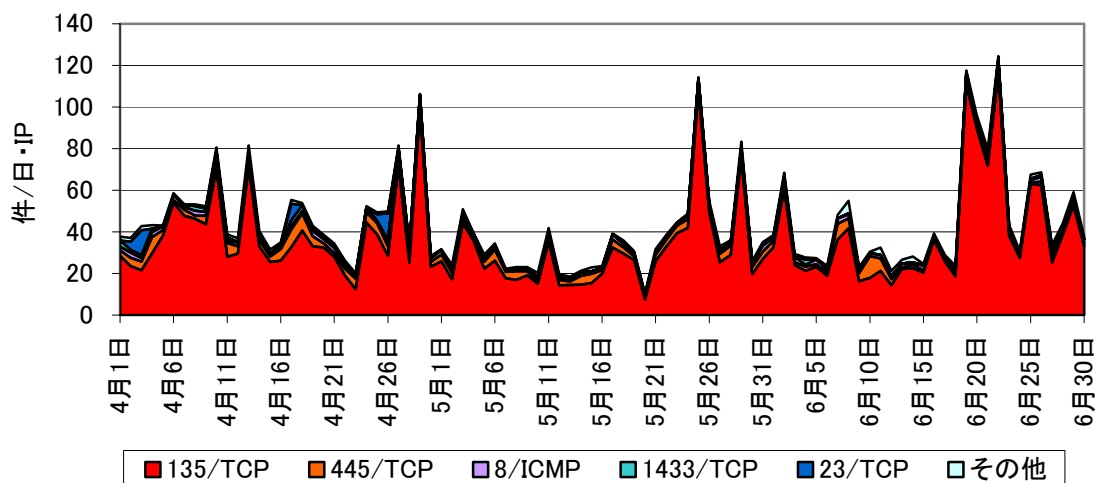


図9 日本国内からのアクセス件数

日本国内からのアクセス件数は前期と比べ一日・1IP 当たり約 3.0%減少している。445/TCP、8/ICMP 及び 1433/TCP は減少となり、23/TCP が前期と比較して一日・1IP 当たり約 87.3%の大幅増となった。このポートは TELNET サービスで使用されるものであり、不正なアクセスの試みと推測される。

・ 米国

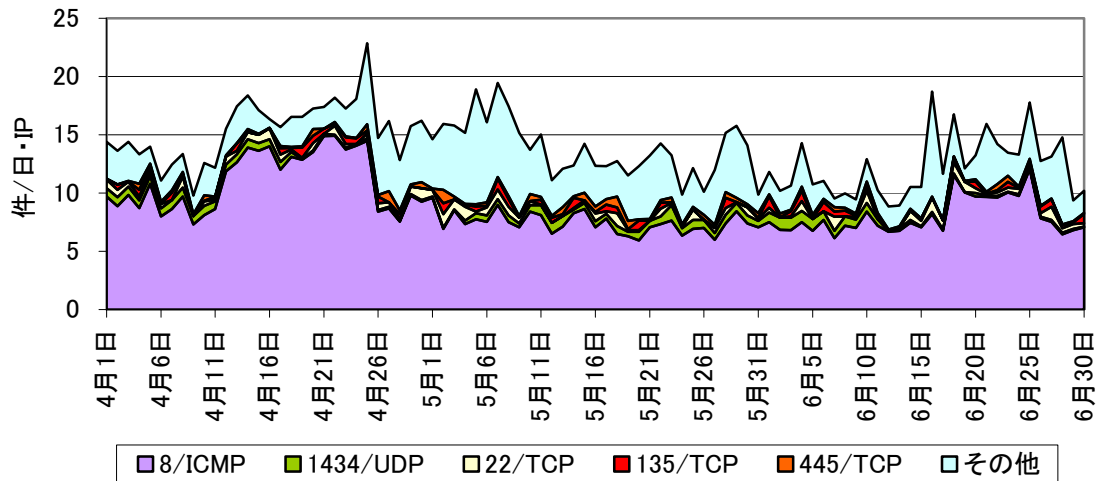


図 10 米国からのアクセス件数

米国からのアクセス件数は前期と比べ一日・1IP 当たり約 11.1%減少している。これは、アクセス件数の大部分を占めていた 8/ICMP が前期と比べ一日・1IP 当たり約 12.1%減少したことが主な要因である。1434/UDP も前期と比べ一日・1IP 当たり約 33.9%減少した。

・ 台湾

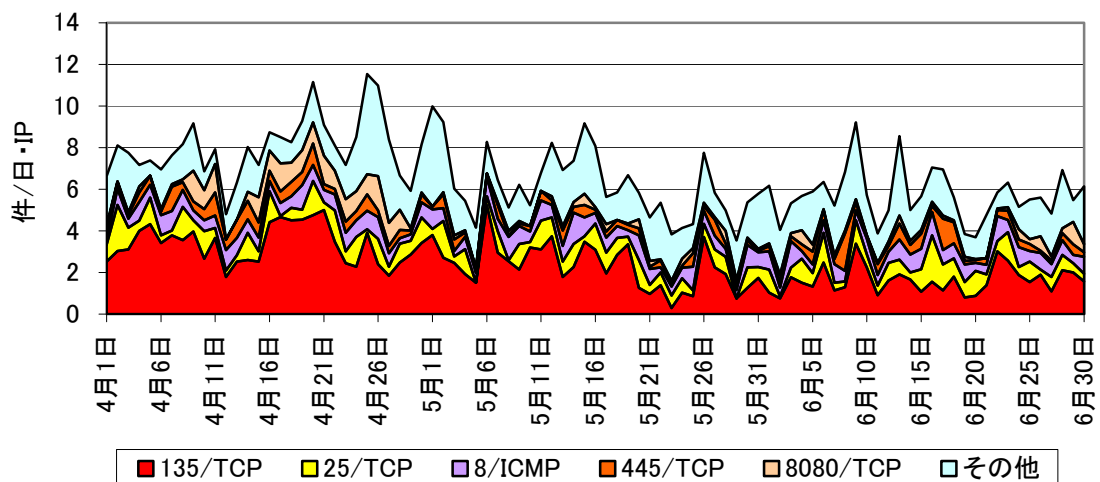


図 11 台湾からのアクセス件数

台湾からのアクセス件数は前期と比べ一日・1IP 当たり約 22.6%減少している。8080/TCP は一日・1IP 当たり約 36.5%増加したが、その他の上位ポートへのアクセス件数は減少した。

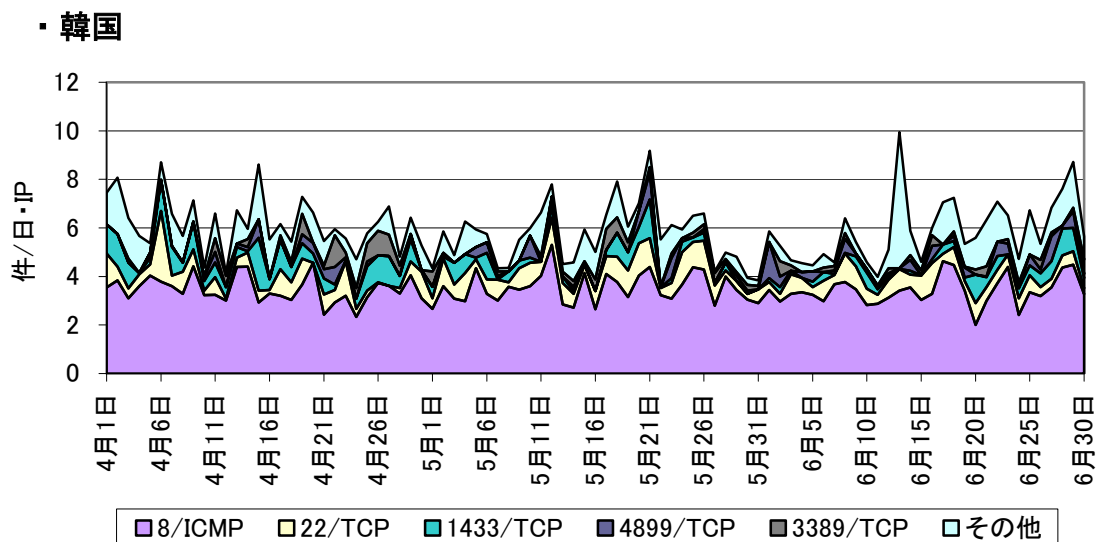


図 12 韓国からのアクセス件数

韓国からのアクセス件数は前期と比べ一日・1IP 当たり約 11.6%減少している。しかし、22/TCP の件数は、前期と比較して一日・1IP 当たり約 14.7%増加し、3389/TCP の件数も一日・1IP 当たり約 38.2%増加した。これらのポートは遠隔地からコマンド操作などを行う際に利用される。

■ インターネット定点観測 — 不正侵入検知システム / IDS

◆ 攻撃手法別の推移と比率

攻撃手法別における検知件数の推移（一日・1IP 当たり）と比率を以下に示す。

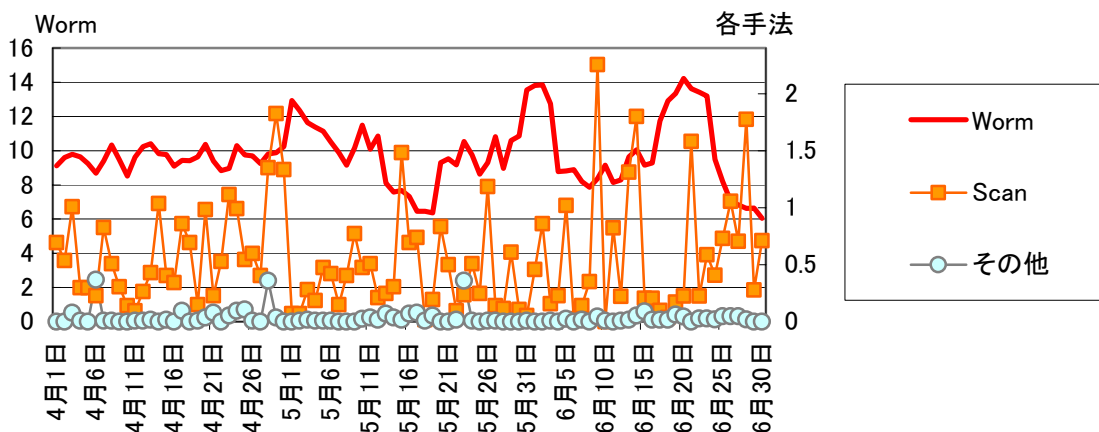


図 13 攻撃手法別の検知件数推移

「Worm」(SQL Slammer ワーム)は前期に比べ一日・1IP 当たり約 10.1%増加し、「Scan」(Proxy attempt) も、一日・1IP 当たり約 9.3%の増加となった。

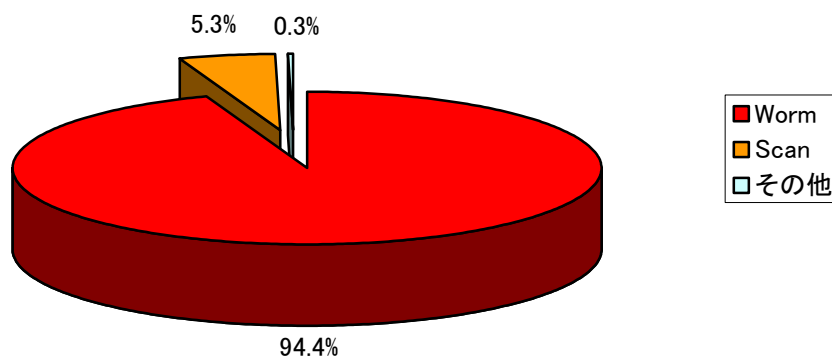


図 14 攻撃手法別の検知件数比率

◆ 発信元（国/地域）別の推移と比率

発信元（国/地域）別における検知件数の推移（一日・1IP 当たり）と比率を以下に示す。

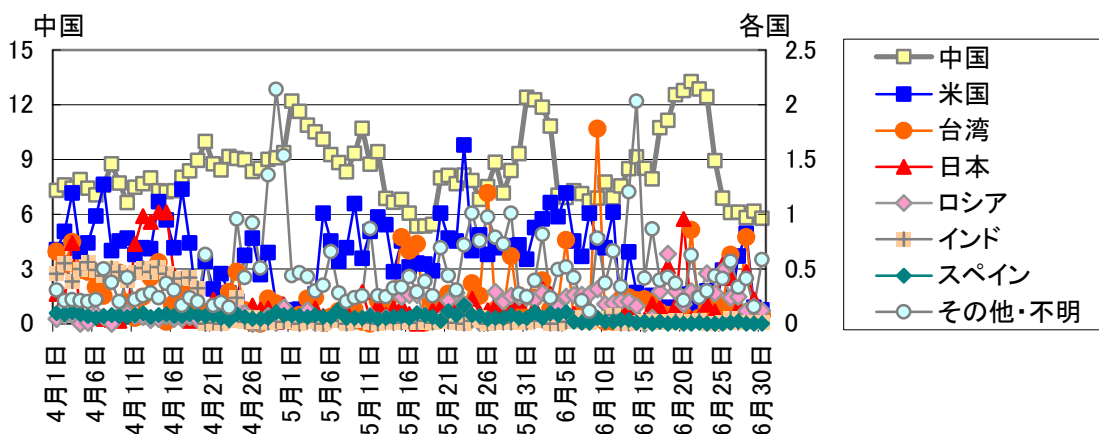


図 15 発信元（国/地域）別の検知件数推移

中国は一日・1IP 当たり約 19.2%の増加となり、依然高い件数で推移している。前期 3 位であったインドは一日・1IP 当たり約 73.8%減少した。

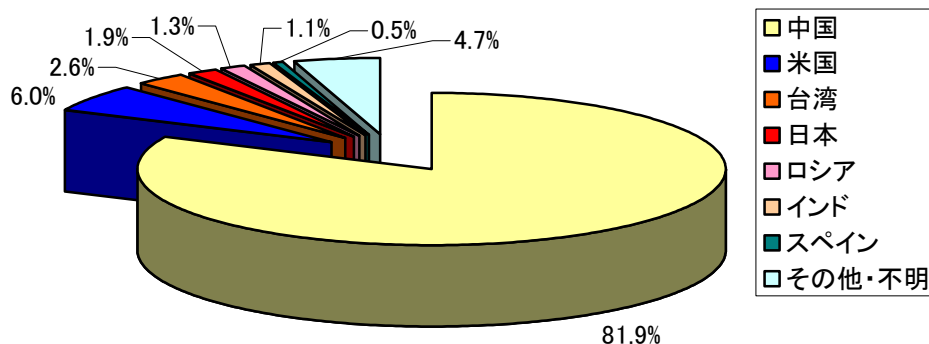


図 16 発信元（国/地域）別の検知件数比率

中国は検知件数の増加に伴い、発信元（国/地域）別の検知件数比率が前期に比べ約 6.4% 増加している。米国は「Worm」（SQL Slammer ワーム）が減少したため、発信元（国/地域）別の検知件数比率が前期に比べ約 2.4%減少した。

■ SYNflood 攻撃被害観測状況について

警察庁では、全国の警察組織に設置したファイアウォールを利用して SYNflood 攻撃の兆候について観測を行っている。このうち、SYN/ACK パケットの分析結果を以下に示す。

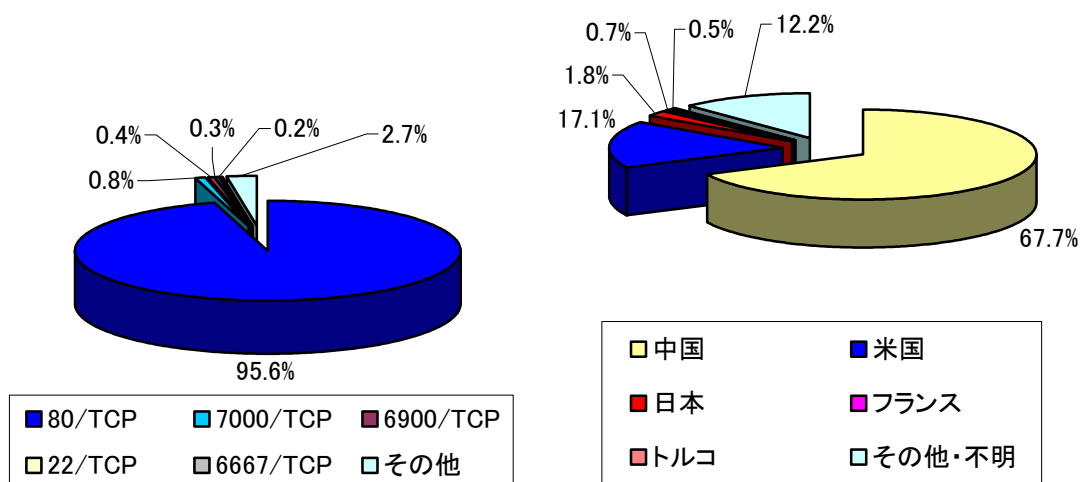


図 17 SYN/ACK パケット検知比率

総検知件数は一日・1IP 当たり約 16.2 件で、前期と比べ約 83.4%増加している。これは、中国の件数が一日・1IP 当たり約 67.5%増加したことが大きな要因となっている。

発信元ポートを 80/TCP とする SYN/ACK パケットの検知比率は、前期が約 77.0%であるのに対して、今期は約 95.6%と大幅に増加した。国別では、中国及び米国を合わせた割合が全体の約 84.6%を占めた。

日本国内を発信元とする SYN/ACK パケットの検知件数は一日・1IP 当たり約 0.3 件で、前期と比べ約 5 倍増加した。これは、検知件数の大半を占める 80/TCP が大幅に増加したことが影響している。