

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17年度第1/四半期)

サイバーフォースセンター(CFC)では、全国の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)による攻撃等の活動の監視を行っている。本レポートは平成17年度第1/四半期の監視状況をとりまとめたものである。

第1/四半期における状況

平成17年度の第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約1,916,000件(前期比-約114,000件)、一方で侵入検知装置におけるアラートの総検知件数は約102,000件(前期比-約23,000件)となった。

- ・ **ファイアウォールに対するアクセス件数：TCP135番、139番ポートが増加傾向**
前期まで減少傾向であった135/TCPに対するアクセスは、今期は増加傾向を示しており、前期から減少傾向にあった139/TCPに対するアクセスも6月5日以降急増している。
- ・ **IDSの検知件数は各攻撃手法共に減少**
各攻撃手法の検知件数がそれぞれ減少しており、総検知件数も約18%減少した。
- ・ **SYNflood攻撃被害観測状況：中華人民共和国からの検知件数が減少**
総検知件数が、前期に比べ約69%減少している。ウェブサーバ(80/TCP)へのSYNflood攻撃の割合が約59%と、依然高い割合を占めている。

主な出来事

表 1 第 1/四半期の主な出来事

4月13日	MS05-016、017、018、019、020、021、022、023 公表 (Microsoft) ¹
4月14日	TCP 実装における ICMP パケットの処理に関する脆弱性 ² W32.Sober.O@mm (別名 W32/Sober.p@MM、WORM_SOBER.S) ウイルス発生
5月3日	³ 、 「Sober ワームの成功はウイルス対策の弱点に起因」 ⁴
5月10日	IPsec に関する脆弱性 ⁵
5月11日	MS05-024 公表 (Microsoft) ⁶ 、 「Windows 2000 のセキュリティパッチが出される」 ⁷
6月15日	MS05-025、026、027、028、029、030、031 公表 (Microsoft) ⁸ : @police 「世界のセキュリティ事情」 ⁹ より

¹ http://www.cyberpolice.go.jp/important/2005/20050413_082928.html

² http://www.cyberpolice.go.jp/important/2005/20050414_195834.html

³ http://www.cyberpolice.go.jp/important/2005/20050503_060919.html

⁴ http://www.cyberpolice.go.jp/international/vulnerability/20050517_230037.html

⁵ http://www.cyberpolice.go.jp/important/2005/20050512_115848.html

⁶ http://www.cyberpolice.go.jp/important/2005/20050511_073501.html

⁷ http://www.cyberpolice.go.jp/international/vulnerability/20050512_220506.html

⁸ http://www.cyberpolice.go.jp/important/2005/20050615_061306.html

⁹ <http://www.cyberpolice.go.jp/international/index.html>

インターネット定点観測 - ファイアウォール / Firewall

第1/四半期における宛先ポート別の日別推移(累積件数の上位5か国)を以下に示す。

135/TCP

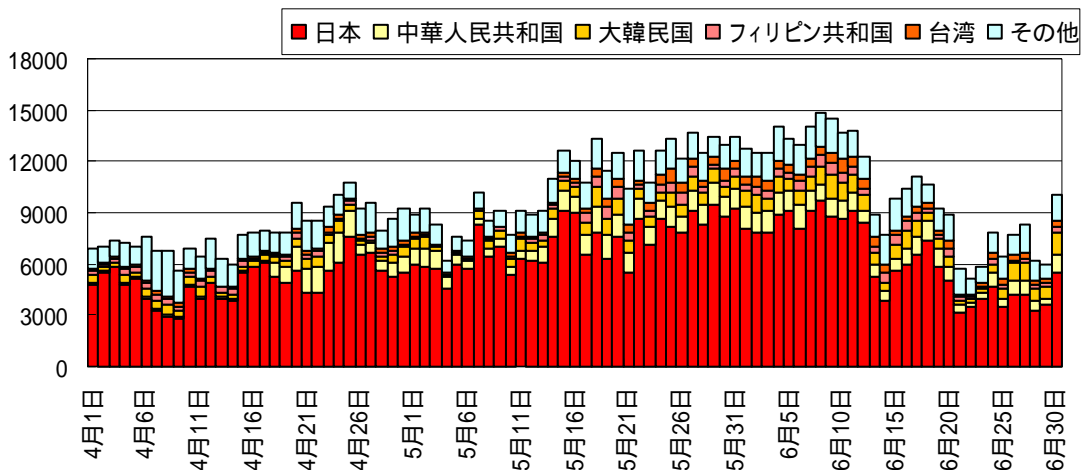


図 1 宛先ポート 135/TCP に対する推移

国内からの 135/TCP に対するアクセス件数が全体の約 64%を占めており、アクセス件数は前期比約 52%増と、前期とは異なり増加傾向が見られる。135/TCP は、平成 15 年 8 月に発生したBlaster を代表とする多くのウイルス及びその亜種が、RPC の脆弱性 (MS03-026、MS03-039) を悪用し感染活動を行うポートである。

445/TCP

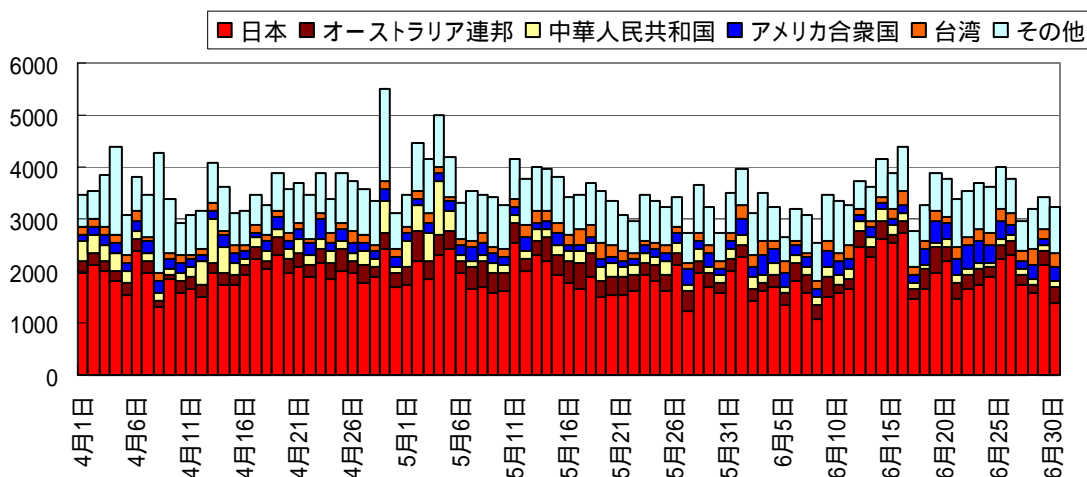


図 2 宛先ポート 445/TCP に対する推移

国内からの 445/TCP に対するアクセス件数が全体の約 53%を占めている。

Microsoft 社が平成 16 年 4 月に公表した LSASS の脆弱性 (MS04-011) を悪用するワームが多数発生したことにより、445/TCP に対するアクセスは年間を通して高い件数で推移していた。しかし、アクセス件数は前期比約 37%減となり、今期も前期と同様に減少傾向が見られる。

1433/TCP

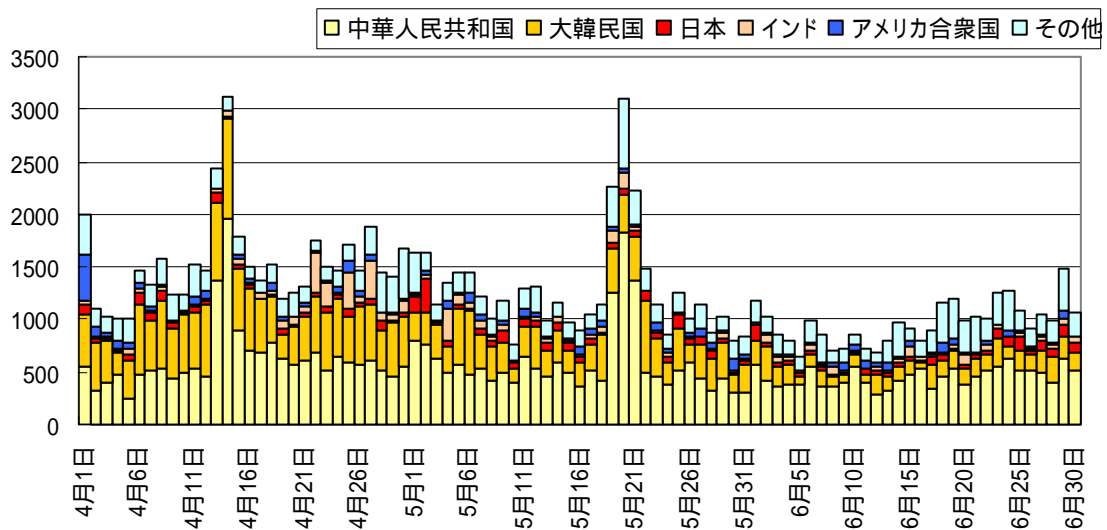


図 3 宛先ポート 1433/TCP に対する推移

前期では累積件数で第 4 位であった 1433/TCP に対するアクセス件数が、今期では 139/TCP を抜いて第 3 位となったが、これは 139/TCP に対するアクセス件数が減少したためであり、アクセス件数は前期比約 3%増と微増であった。

中華人民共和国からの 1433/TCP に対するアクセス件数が全体の約 44%を占めており、次いで大韓民国からが約 27%を占めている。1433/TCP は、Microsoft SQL Server がデフォルトの設定で使用するポートであり、脆弱なパスワード設定を標的としたアクセス及び、bot 系ワームの攻撃であると推測される。

139/TCP

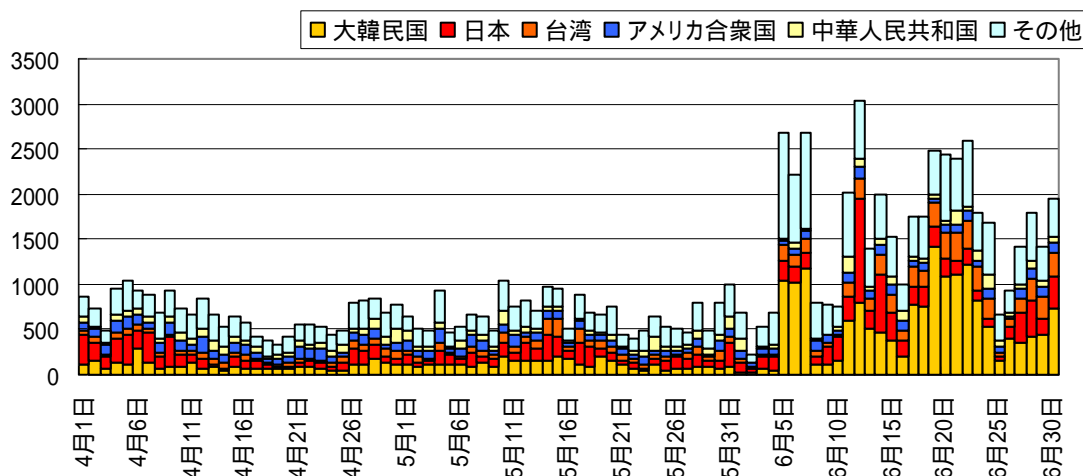


図 4 宛先ポート 139/TCP に対する推移

139/TCP に対するアクセスは、2月下旬以降に減少したまま推移しており、アクセス件数は前期比約 22%減と大幅に減少している。しかし、6月5日にアクセス件数が増加し、それ以降、以前以上の水準で推移しており、今後の動向に注意が必要である。Windows のネットワーク共有サービスを提供する 139/TCP は、同様なサービスを提供する 135/TCP や 445/TCP と共に bot 系ワーム¹⁰の標的になりやすいポートである。

ICMP

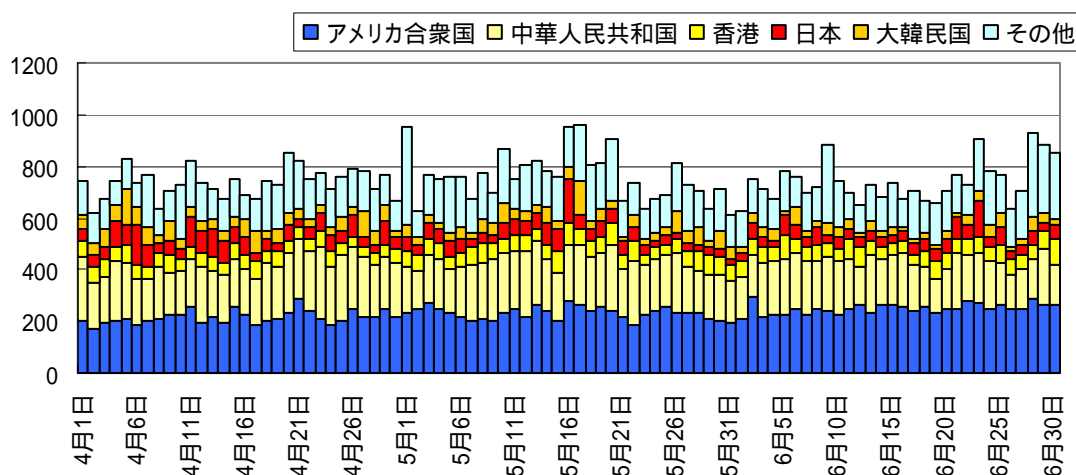


図 5 ICMP の推移

¹⁰ 「複数の脆弱性を悪用する Gaobot ワームについて」
http://www.cyberpolice.go.jp/detect/pdf/report_gaobot.pdf
 「ボットネット(botnet)に注意」
http://www.cyberpolice.go.jp/detect/pdf/H170127_botnet.pdf

前期では累積件数で第 6 位であった ICMP によるアクセス件数が、今期では 4899/TCP を抜いて第 5 位となったが、これは 4899/TCP に対するアクセス件数が前期比 29%減と大幅に減少したためであり、ICMP は前期比約 8%増と微増であった。今期は、ICMP、4899/TCP 共に、アクセス件数が急増した期間もなく、1 日あたり約 700 件のまま推移した。

他ポートのアクセス状況

- VERITAS Backup Exec の脆弱性を狙う 10000/TCP へのアクセス

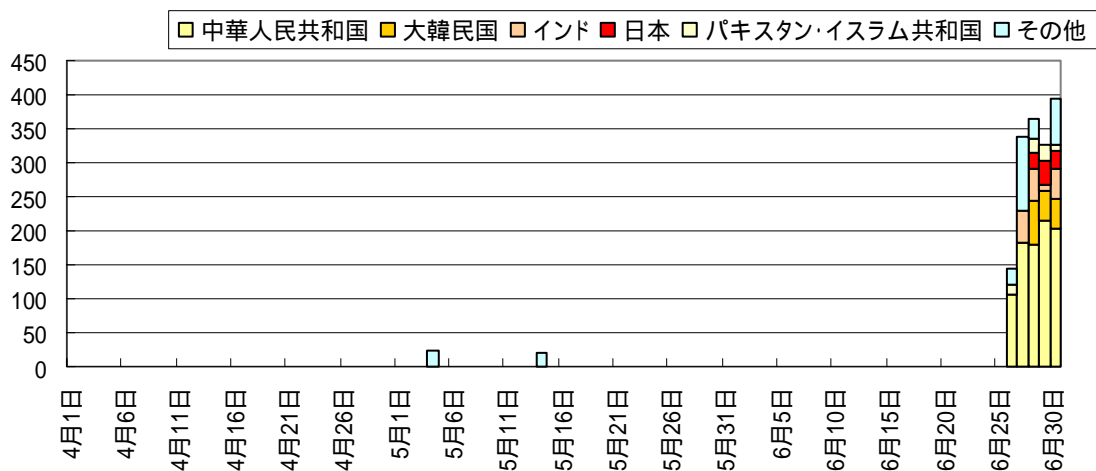


図 6 宛先ポート 10000/TCP に対する推移

6月26日以降、10000/TCP に対するアクセスが急増した。これは、日本時間6月23日に発表された、米国 Veritas Software 社のバックアップソフトウェア「VERITAS Backup Exec」の脆弱性を狙ったものと思料される。既に修正プログラムは提供されているが、修正プログラムが適用できない場合は、10000/TCP をフィルタリングするなどの措置が必要である。

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。

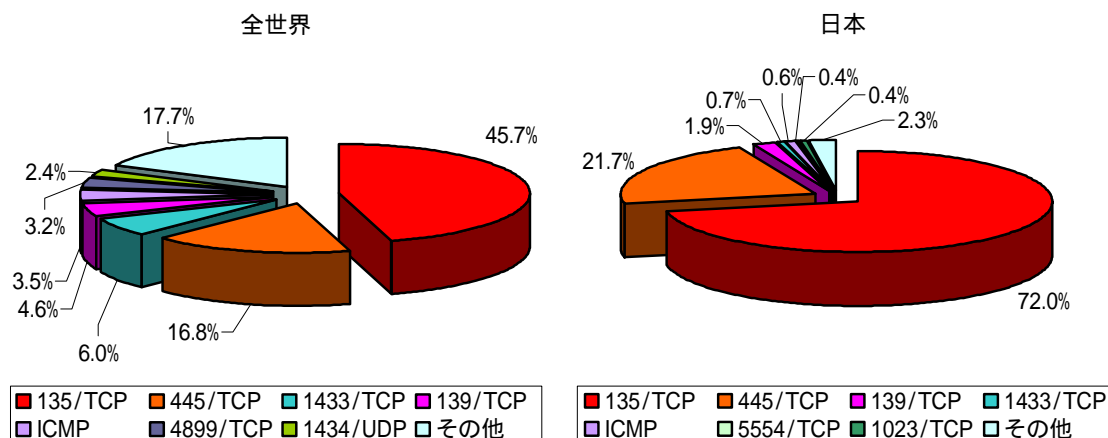


図 7 宛先ポート別比率

全世界で見ると、前期まで減少傾向にあった 135/TCP が増加しており、135/TCP 及び 445/TCP の合計で約 63%を占めている。依然として RPC の脆弱性に関連する 135/TCP 及び LSASS の脆弱性に関連する 445/TCP を利用して感染を広げるワームの活動が盛んであると考えられる。

一方で、日本を発信元とするアクセス状況は、135/TCP 及び 445/TCP の合計で約 94%を占めており、これは全世界での割合の約 63%を大きく上回る。

発信国/地域別推移(上位5か国)

発信元の国/地域別のアクセス件数の推移を以下に示す。

・日本

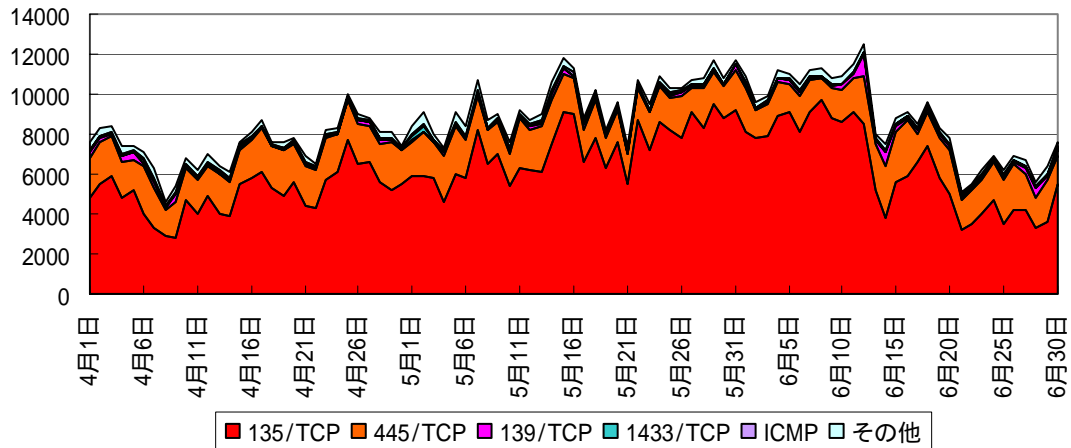


図 8 発信元の国/地域別のアクセス件数(日本)

・中華人民共和国

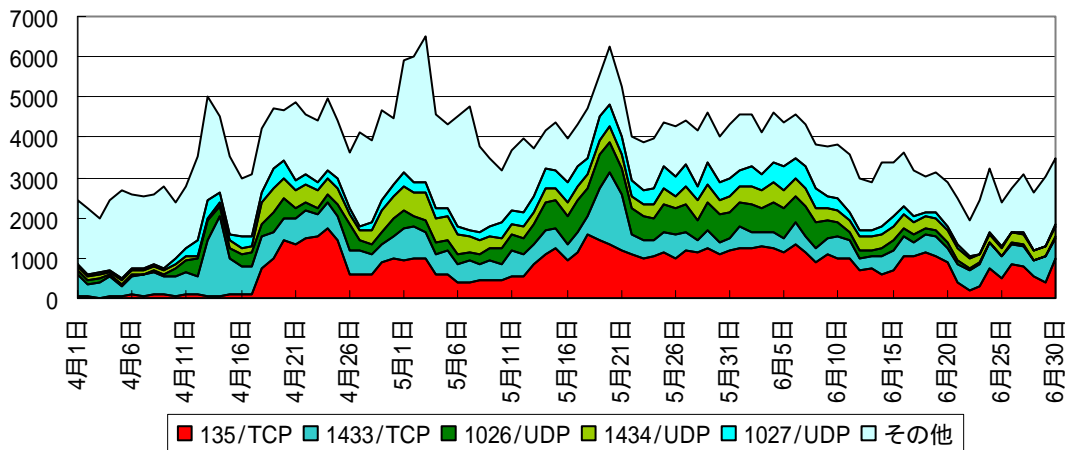


図 9 発信元の国/地域別のアクセス件数(中華人民共和国)

・大韓民国

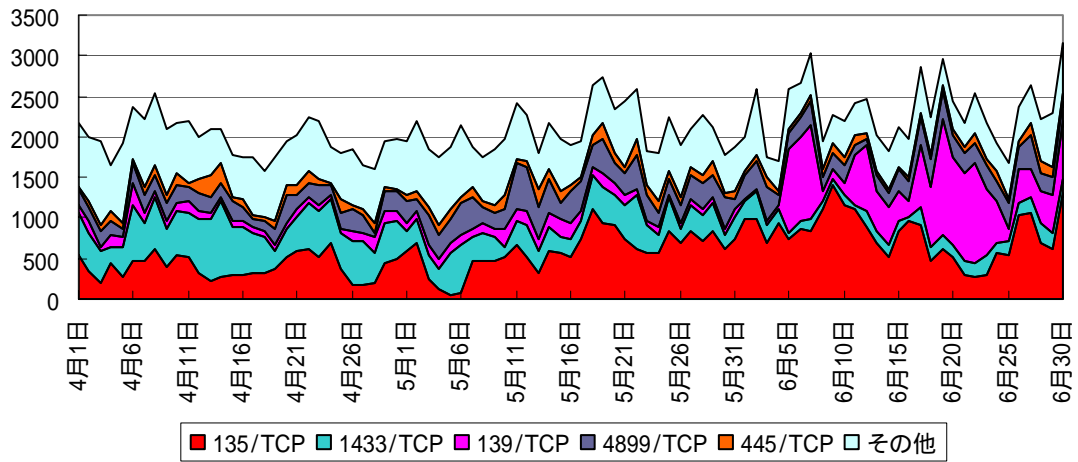


図 10 発信元の国/地域別のアクセス件数（大韓民国）

・アメリカ合衆国

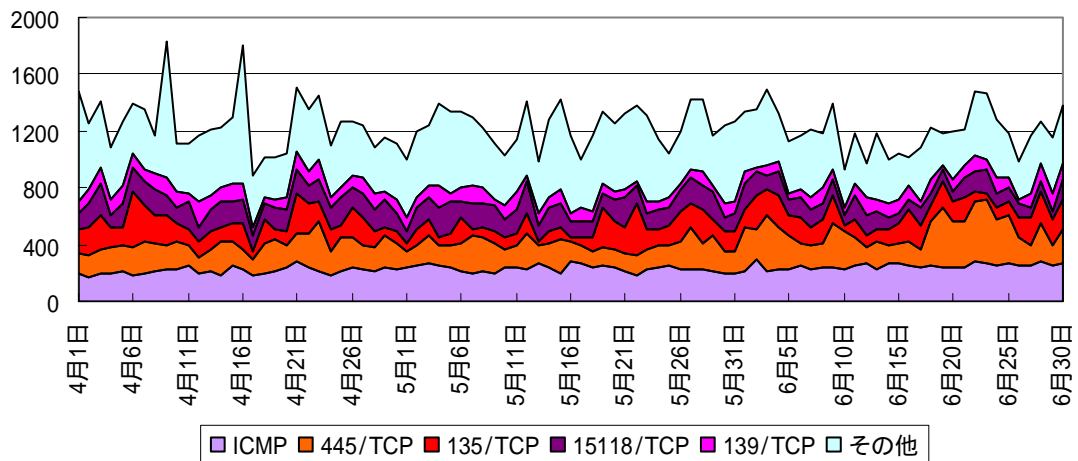


図 11 発信元の国/地域別のアクセス件数（アメリカ合衆国）

・台湾

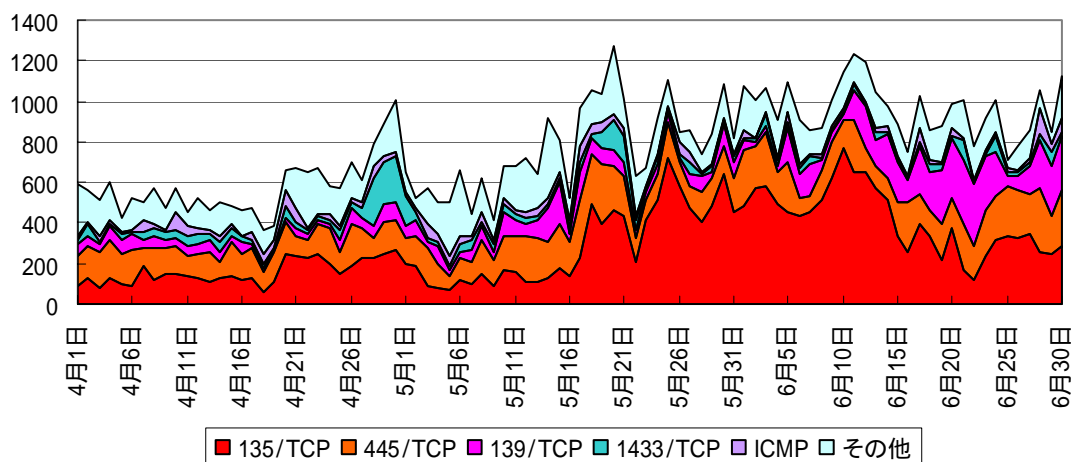


図 12 発信元の国/地域別のアクセス件数（台湾）

日本の上位を占めるポートは、1位の135/TCPが約72%と大部分を占め、2位の445/TCPと合わせると約94%を占めている。前期に比べ、135/TCPが増加したものの445/TCPが減少したため、アクセス件数は前期比約1%増と変化はなかった。

中華人民共和国は、前期に増加傾向にあった445/TCPへのアクセス件数は少なく、4月18日頃から増加した135/TCPが1位となっている。また、4月10日頃から6月21日頃まで1026/UDP及び1027/UDPへのアクセス件数が増加していたが、これはWindowsのメッセージサービスを利用したスパム広告によるものと思われる。

大韓民国は、1433/TCPに対するアクセス件数は減少傾向にあるが、135/TCPは増加傾向にある。また、6月5日以降に139/TCPが断続的に急増しており、全体的にもやや増加傾向にある。

アメリカ合衆国は、前期に増加したICMPがそのまま推移しており、期間を通じてアクセス件数が急増したポートは見られなかった。

台湾は5月17日頃から135/TCPへのアクセス件数が急増しており、135/TCPが減少し始めた6月11日頃からは139/TCP及び445/TCPが増加しており、期間の後半は高いアクセス件数のまま推移した。

国/地域別比率

発信元の国/地域別比率を以下に示す。

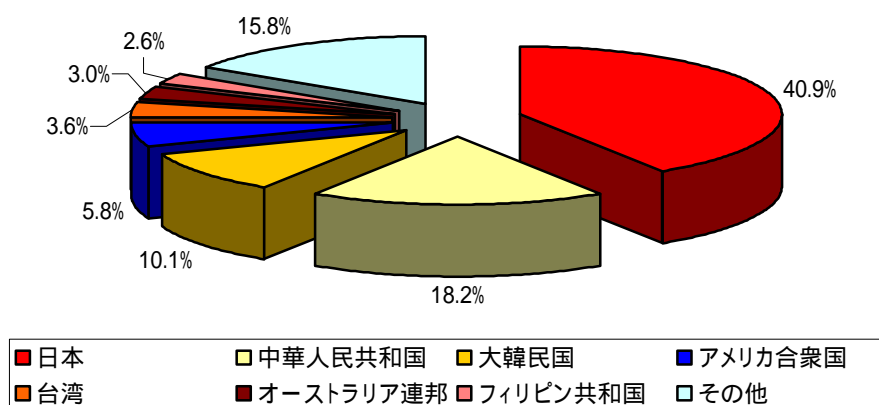


図 13 発信元の国/地域別比率

発信元の国及び地域の順位は、上位 5 ヶ国は前期と同様であり、1 位の日本と 2 位の中華人民共和国については、全体に占める割合もほぼ変化はなかった。3 位の大韓民国と 4 位のアメリカ合衆国は前期よりも減少しており、5 位の台湾はやや増加した。

上位 3 ヶ国からのアクセス件数が全体の約 69%であり、前期の約 73%と比べて減少しているが、これは 3 位の大韓民国からのアクセス件数が減少したためである。

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

攻撃手法別の検知件数の推移(日別)と比率を以下に示す。

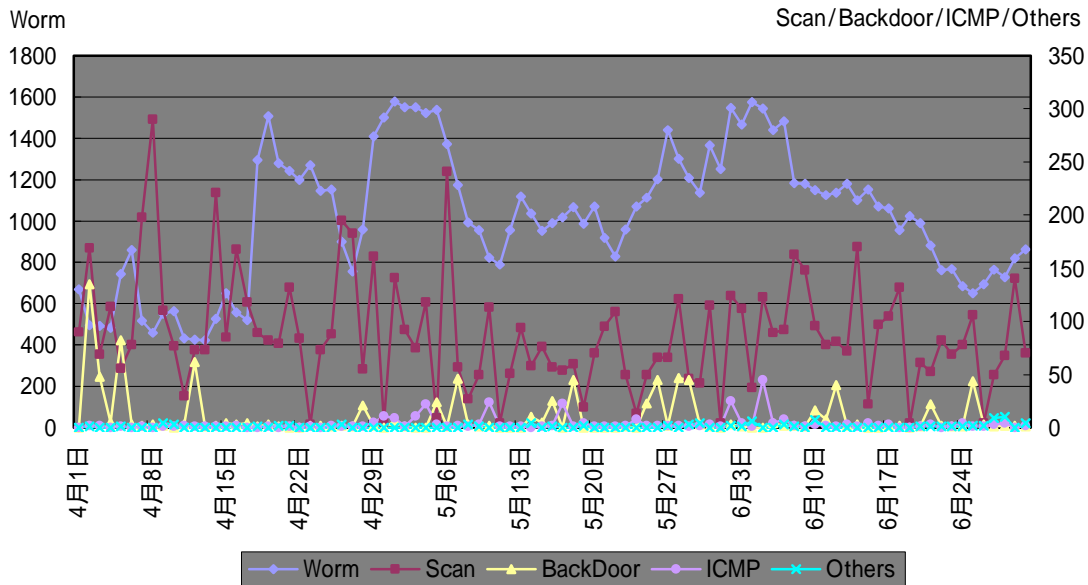


図 14 攻撃手法別の検知件数推移

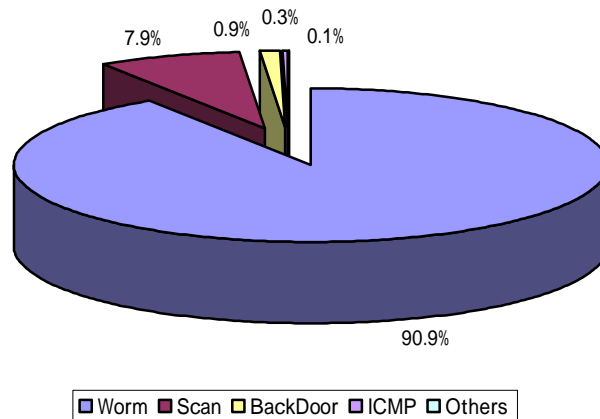


図 15 攻撃手法別の検知件数比率

前期末には減少していた「Worm」(SQL Slammer ワーム)が4月18日頃から増加しているが、前期には1日あたり2,000件前後検知していた期間があったため、検知件数は前期比約14%減となっている。

「Scan」及び「ICMP」についても、それぞれ約14%減、15%減と、同程度減少している。

「BackDoor」については、大韓民国からの検知が減少したため、約67%減と大幅に減少している。

発信国/地域別推移

発信国/地域別の検知件数の推移(日別)と比率を以下に示す。

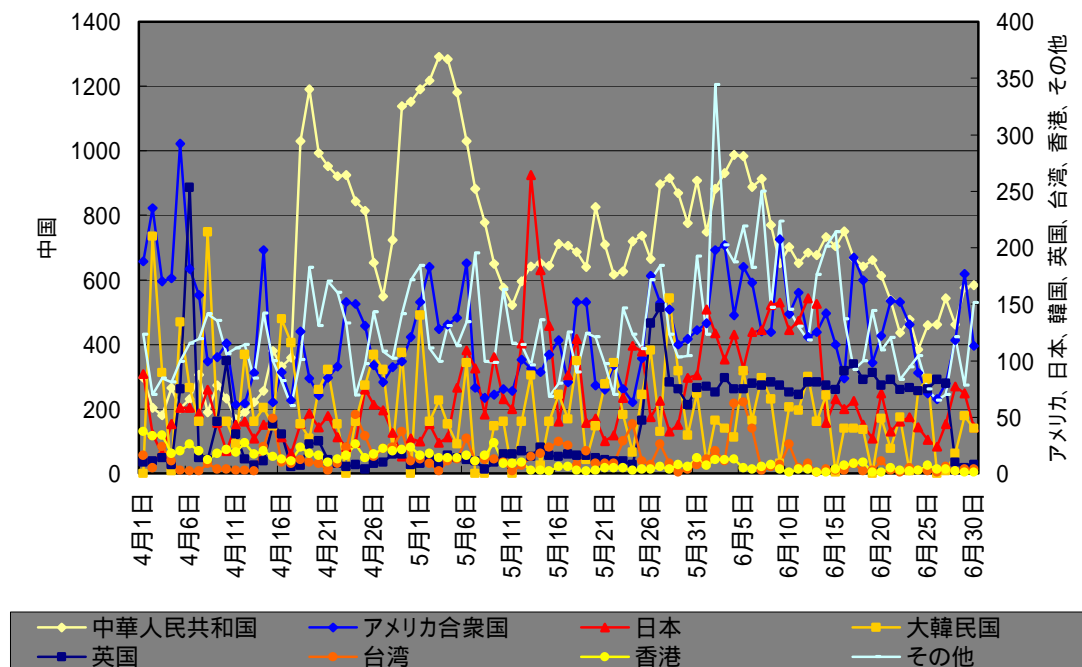


図 16 発信国/地域別の検知件数推移

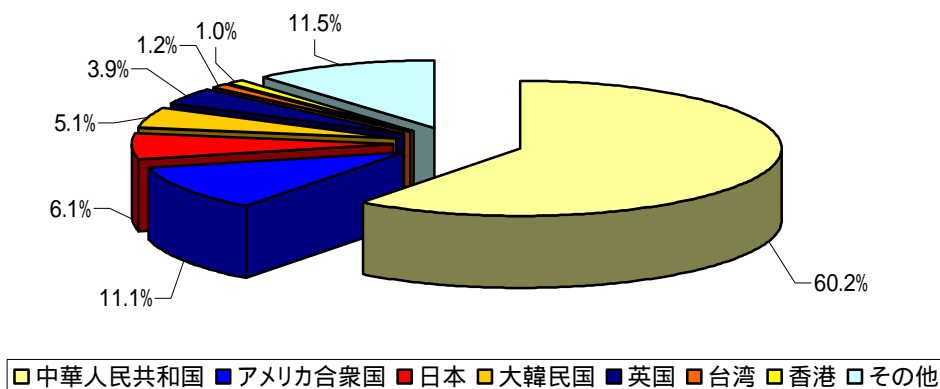


図 17 発信国/地域別の検知件数比率

検知件数の多い「SQL Slammer ワーム」の影響により、前期に引き続き、中華人民共和国からの検知件数が最も多くなっている。上位4ヶ国については、順位も比率も前期とほぼ同じとなっており、5,6,7位についても順位の入替えはあったものの、前期からあまり変化は見られなかった。

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 攻撃被害の観測を行っている。このうち、SYN/ACK パケットの分析結果を以下に示す。

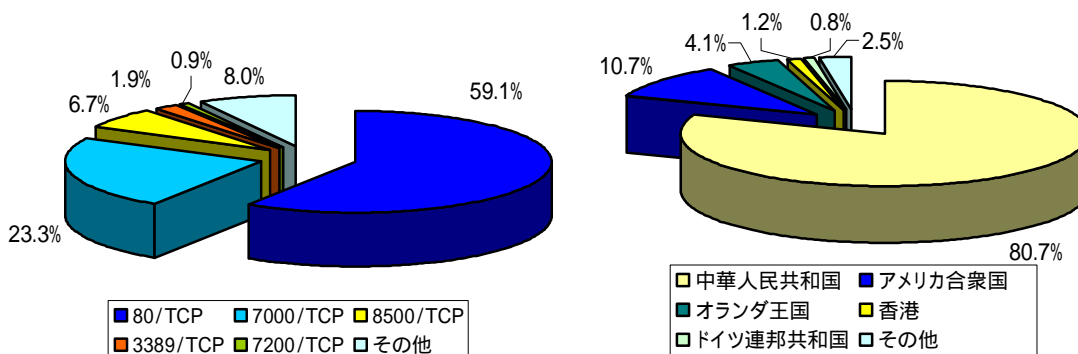


図 18 平成 17 年度第 1/四半期における SYN/ACK パケット検知比率

総検知件数は、前期に比べ約 69%減少している。

80/TCP からの SYN/ACK パケットの検知比率は前期の約 71%から約 59%と減少しているが、依然として最多である。このことから、SYNflood 攻撃が主にウェブサーバに対して行われていることが推測される。

国/地域別では、中華人民共和国を発信元とする SYN/ACK パケットが前期比約 74%減と減少したものの、全体の約 81%と圧倒的多数を占めている。

中華人民共和国・アメリカ合衆国の 2 か国については、SYN/ACK パケットを定常的に検知しており、この 2 か国に対する SYNflood 攻撃が常態化していると推測される。

日本を発信元とする SYN/ACK パケットは、件数は少ないものの、分散型サービス不能 (DDoS) 攻撃を受けていたと報道された期間において、国内の企業が運営するオンラインゲームのサーバからの SYN/ACK パケットを検知しており、これらの観測結果からも SYNflood 攻撃の被害を受けたものと推測される。

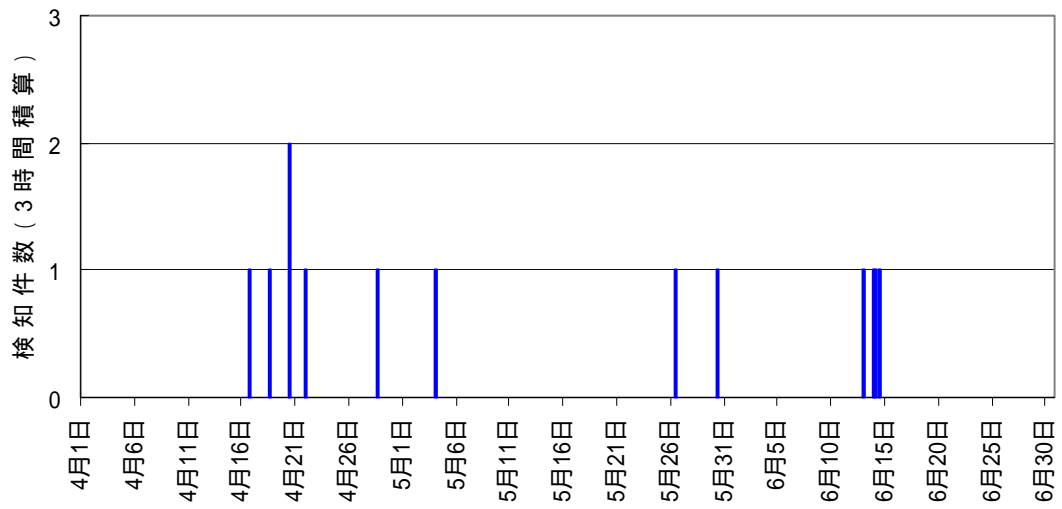


図 19 日本を発信元とする 3 時間毎の SYN/ACK パケット検知件数