

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16年度第3/四半期)

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16年度第3/四半期の監視状況をとりまとめたものである。

第3/四半期における状況

平成16年度の第3/四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アクセス件数は約2,289,000件(前期比-約128,000件)、一方で侵入検知装置におけるアラートの検知件数は約86,000件(前期比+約13,000件)となった。

・ファイアウォールに対するアクセス件数：TCP445番ポートは減少傾向

前期増加した445/TCPに対するアクセスは、減少傾向となっている。

・IDSの総検知件数は増加、国内は減少傾向

中国からのSQL Slammer ワームの検知件数が、11月28日から12月15日にかけて一時的に激増したために、IDSの総検知件数は増加した。しかし、日本を含め、その他の国の検知件数は減少傾向となっている。

・SYN flood 被害観測システム：TCP80番ポートへの攻撃が最多

前期に比べ、総検知数は減少した。しかし、依然としてウェブサーバ(80/TCP)へのSYN flood 攻撃の割合が約75%と最多を記録している。

・SSHを利用した不正侵入行為

SSHに対して行われている活動を把握するために、専用の監視システムを用いて約一ヶ月間観測を行った結果、32件の侵入行為が確認された。

主な出来事

表 1 第 3/四半期の主な出来事

10 月 13 日	MS04-029、030、031 公表 (Microsoft) ¹ 、 MS04-032、033、034、035、036、037、038 公表 (Microsoft) ² 「Microsoft 社が 10 件のセキュリティ勧告を公表、緊急は 7 件」 ³
11 月 10 日	MS04-039 公表 (Microsoft) ⁴
11 月 19 日	Sober.I (別名 WORM_SOBER、I,WORM_SOBER.I) ウイルス発生 ⁵
12 月 2 日	MS04-040 公表 (Microsoft) ⁶
12 月 14 日	Adobe Acrobat/Adobe Reader の脆弱性公表 (Adobe) ⁷
12 月 15 日	MS04-041,042,043,044,045 公表 (Microsoft) ⁸
12 月 15 日	W32.Erkez.D@mm (別名 W32/Zafi.d@MM、WORM_ZAFI.D) ウイルス発生 ⁹

: @police 「世界のセキュリティ事情¹⁰」より

¹ http://www.cyberpolice.go.jp/important/2004/20041013_172034.html

² http://www.cyberpolice.go.jp/important/2004/20041013_172259.html

³ http://www.cyberpolice.go.jp/international/north_america/20041015_043342.html

⁴ http://www.cyberpolice.go.jp/important/2004/20041110_080814.html

⁵ http://www.cyberpolice.go.jp/important/2004/20041119_211444.html

⁶ http://www.cyberpolice.go.jp/important/2004/20041202_065548.html

⁷ http://www.cyberpolice.go.jp/important/2004/20041215_133649.html

⁸ http://www.cyberpolice.go.jp/important/2004/20041215_061355.html

⁹ http://www.cyberpolice.go.jp/important/2004/20041215_113842.html

¹⁰ <http://www.cyberpolice.go.jp/international/>

インターネット定点観測 - ファイアウォール / Firewall

第 3/四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)を以下に示す。

135/TCP

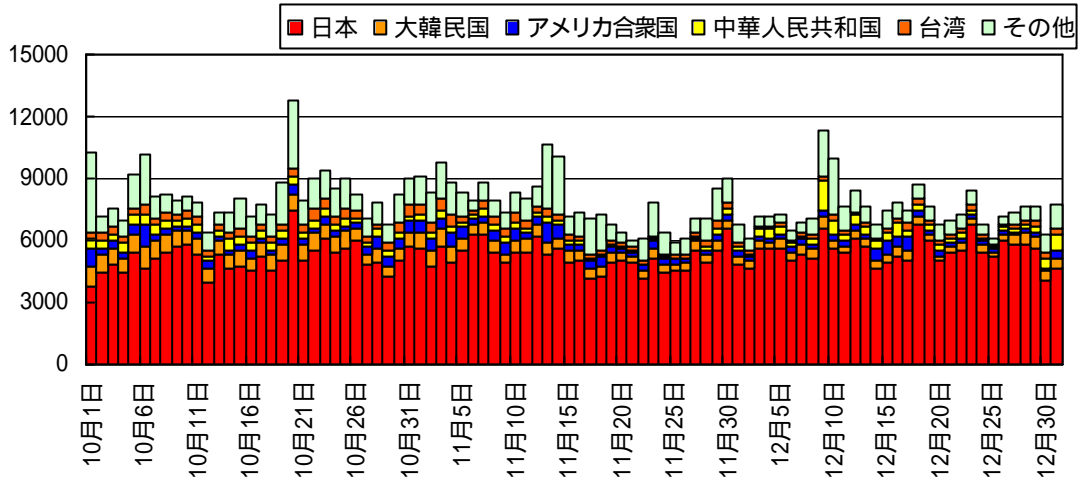


図 1 宛先ポート 135/TCP に対する推移

国内からの 135/TCP に対するアクセス件数が全体の約 6 割半を占めている。135/TCP は、昨年度発生した 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

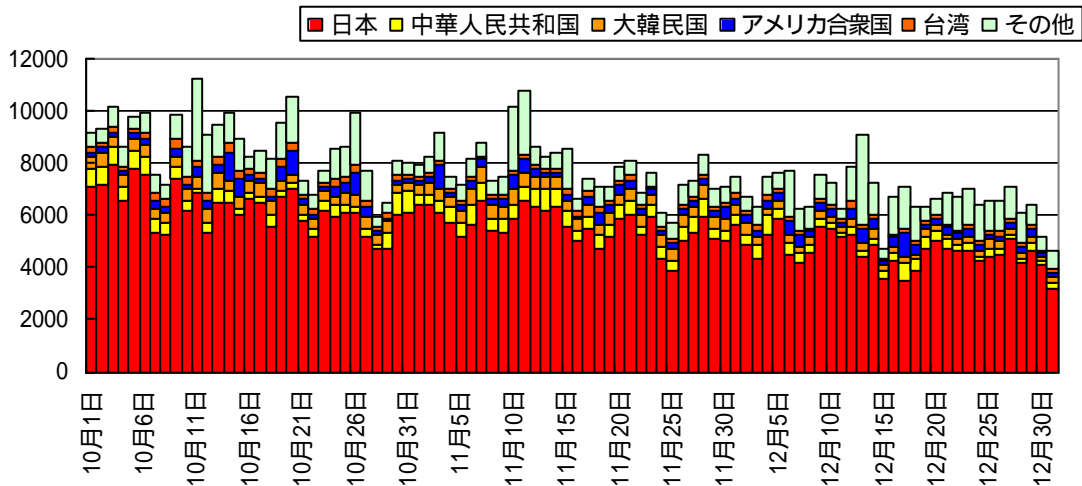


図 2 宛先ポート 445/TCP に対する推移

国内からの 445/TCP に対するアクセス件数が全体の約 7 割を占めている。Microsoft 社が 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、今期に入り徐々に減少してきている。

139/TCP

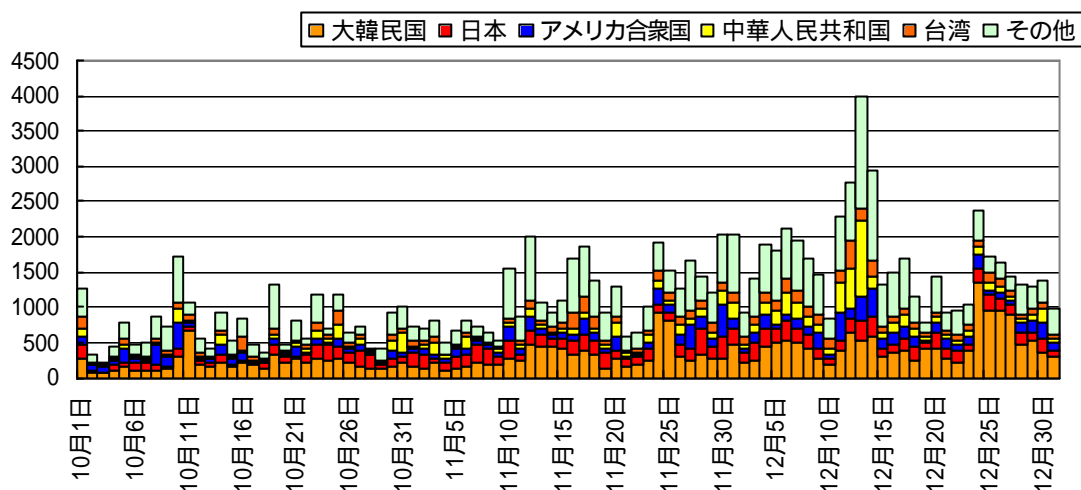


図 3 宛先ポート 139/TCP に対する推移

139/TCP に対するアクセスは様々な国が発信元となっており、増加傾向である。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 系ワームの標的になりやすいポートである。

4899/TCP

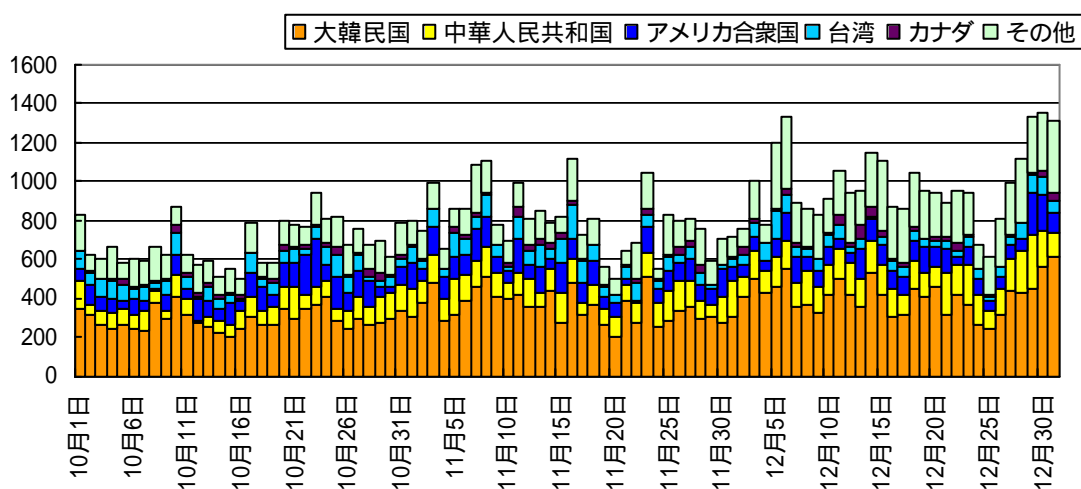


図 4 宛先ポート 4899/TCP に対する推移

大韓民国からの 4899/TCP に対するアクセス件数が全体の約 4 割を占めており、徐々に増加傾向にある。4899/TCP は、Famatech 社の遠隔管理用ソフトウェア「Radmin」で使用するポートであり、同ソフトウェアにおける脆弱性や脆弱な設定を標的としたアクセス及び Gaobot¹¹等のワームの攻撃であると推測される。

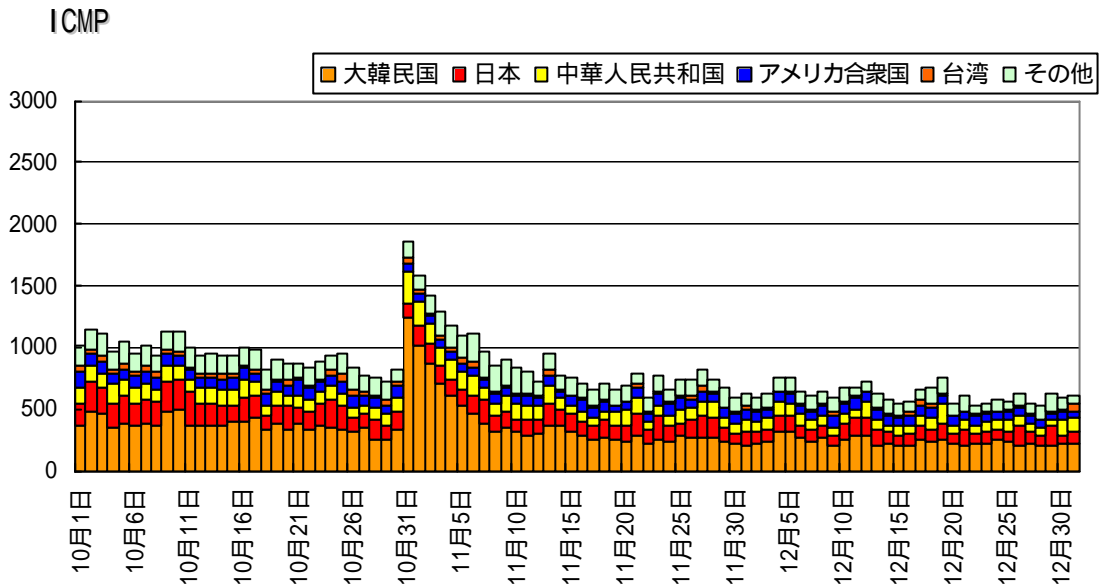


図 5 ICMP の推移

大韓民国からの ICMP のアクセス件数が全体の約 4 割近くを占めている。ICMP のアクセス数は、今年 5 月前半に発生した Sasser.D ワーム以降、徐々に減少していたが、10 月 31 日に韓国からのアクセス数が急増し、その後、再度減少傾向に転じている。アクセス数と共に送信元ホスト数も増加しているため、一時的に韓国国内でワームが発生したことも考えられるが、現時点では原因は不明である。

¹¹ 「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

他ポートのアクセス状況

・ WINS の脆弱性をねらう 42/TCP へのアクセス

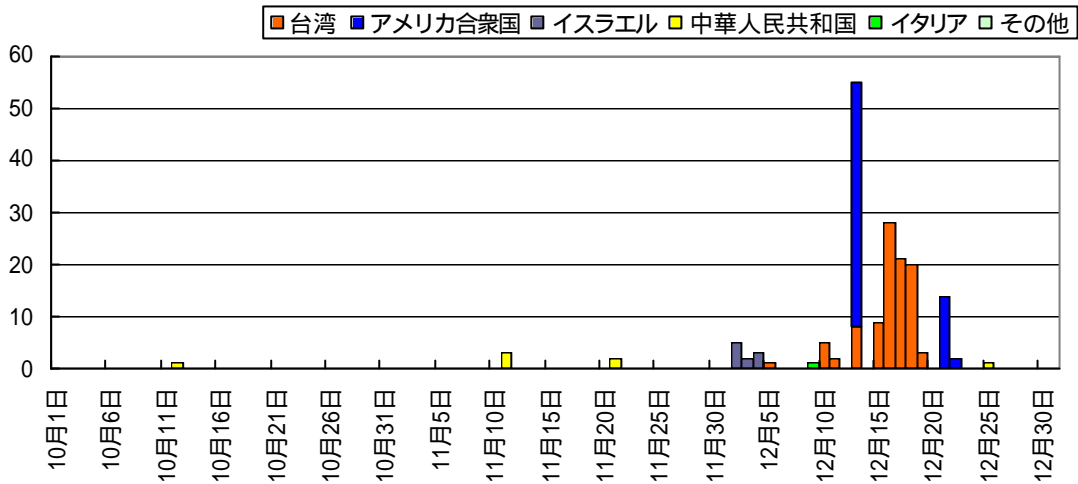


図 6 WINS の脆弱性をねらったと推料される宛先ポート 42/TCP に対する推移

11 月下旬、Microsoft WINS サーバの脆弱性についての情報がインターネット上で公開された。その後、同ポートへのアクセスが見られ、12 月 13 日にはアメリカ合衆国からのアクセスが増加している。同月 15 日には Microsoft 社が、MS04-045 のパッチをリリースしたが、同月 31 日に exploit コードが登場していることから、動向に注視していく必要がある。

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。

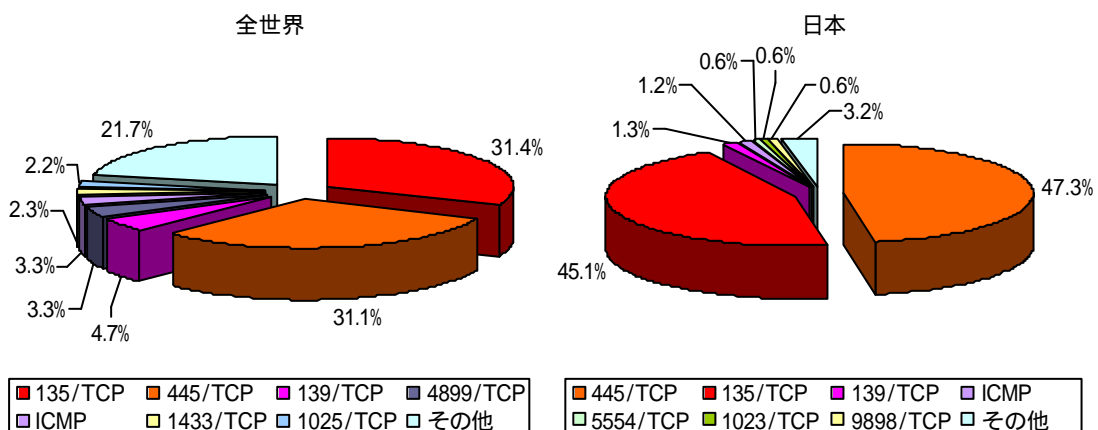


図 7 宛先ポート別比率

全世界で見ると、前期のアクセス総件数と比較して今期は減少傾向にあるものの、依

然として RPC の脆弱性を持つ 135/TCP 及び LSASS の脆弱性を持つ 445/TCP を利用して感染を広げるワーム (Blaster 系ワーム、Sasser 系ワーム、Gaobot 系ワーム) の活動が盛んであると考えられる。

また、前期のアクセス総件数で上位を占めていた Dabber ワームの影響と思われる 5554/TCP 及び 9898/TCP のアクセスは減少したが、再び 1025/TCP のアクセス比率が高くなっており、依然 Gaobot 系ワームの影響が大きいと考えられる。

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 92% を占めている。この原因の一つとして、近隣の IP アドレスを攻撃する割合の高いアルゴリズムを実装している Blaster ワームが考えられており、依然同ワームが蔓延していると考えられる。

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

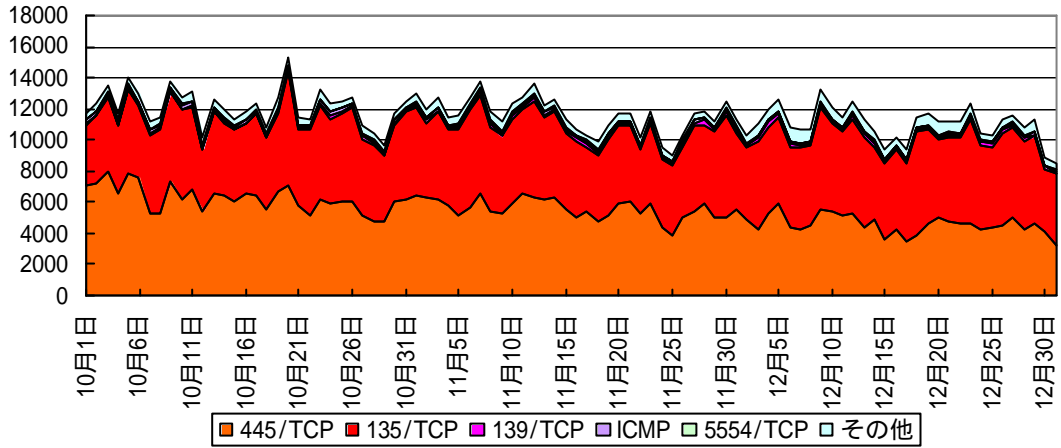


図 8 発信元の国/地域別のアクセス件数（日本）

・大韓民国

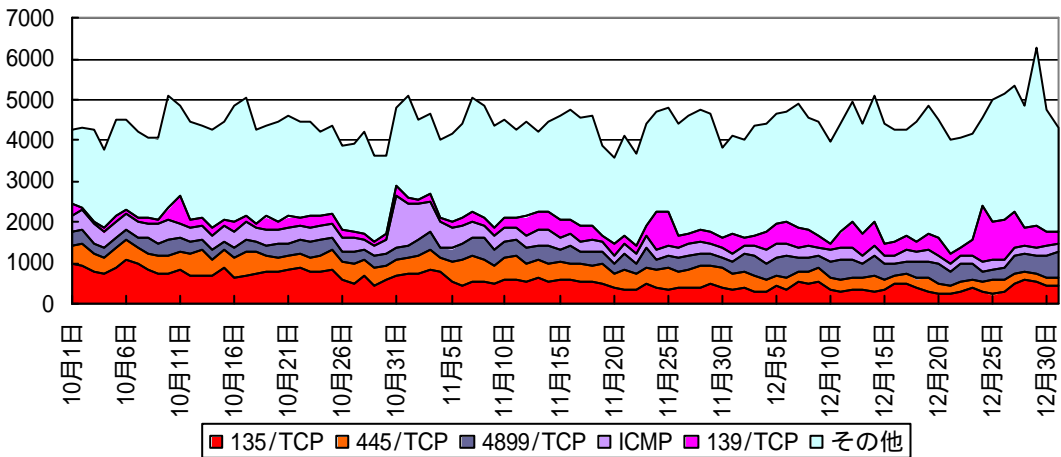


図 9 発信元の国/地域別のアクセス件数（大韓民国）

・ 中華人民共和国

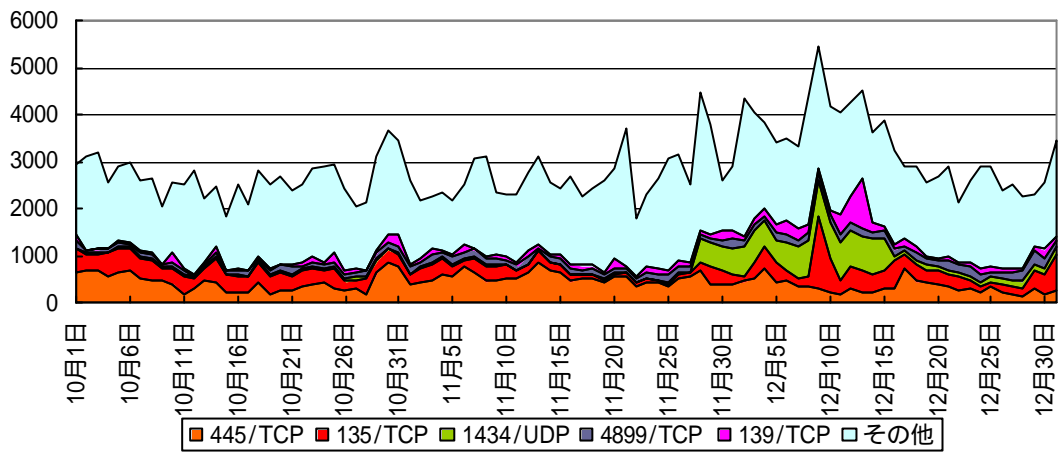


図 10 発信元の国/地域別のアクセス件数 (中華人民共和国)

・ アメリカ合衆国

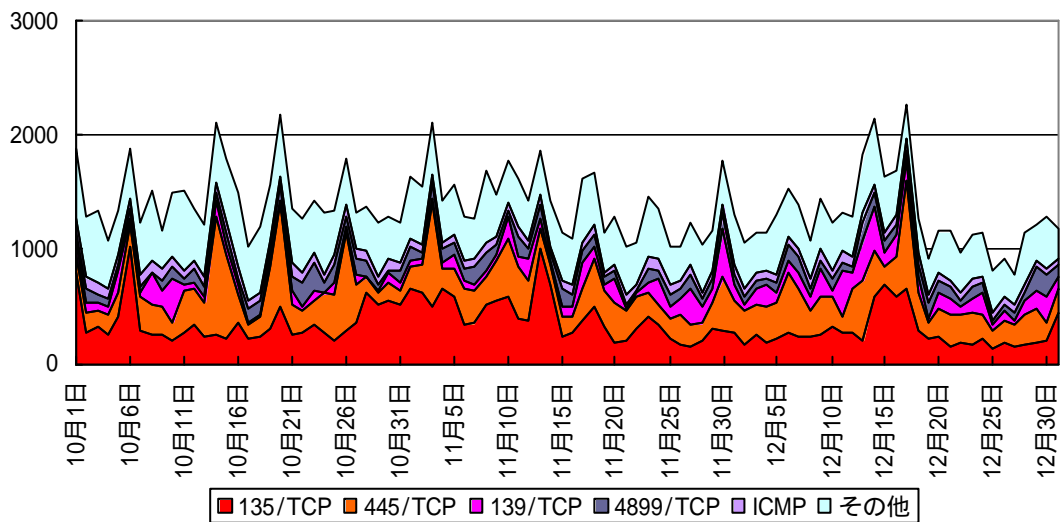


図 11 発信元の国/地域別のアクセス件数 (アメリカ合衆国)

・台湾

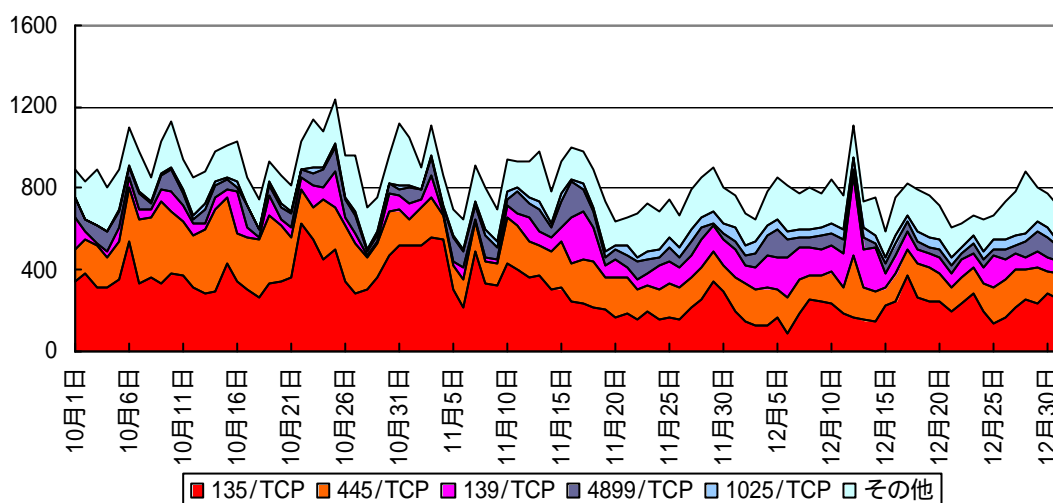


図 12 発信元の国/地域別のアクセス件数（台湾）

日本及び台湾の上位を占めるポートは、前期とあまり変化はない。また、アクセス件数も減少傾向である。

大韓民国は、その他のポートに占める割合が高く、その内訳は 7 月上旬から増加した Dabber.B が感染活動に利用する 1023/TCP、5554/TCP、9898/TCP に対するアクセスが大半を占める。

中華人民共和国は、11 月 28 日から 12 月 15 日にかけて 1434/TCP が急激に増加しているが、後述する IDS の統計からも分かるとおり、一時的に SQL Slammer ワームが蔓延したことが原因と考えられる。

アメリカ合衆国の上位を占めるポートは、前期とあまり変化はない。135/TCP が突発的に増加しているが、原因は不明である。

国/地域別比率

発信元の国/地域別比率を以下に示す。

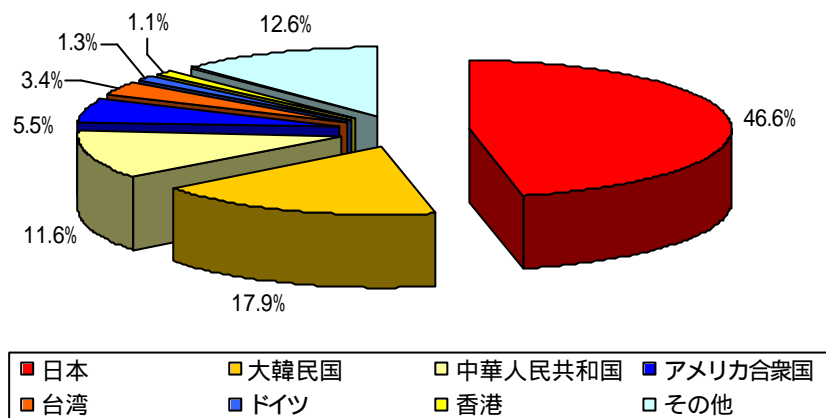


図 13 発信元の国/地域別比率

発信元の国及び地域の順位は、前期と比較して、アメリカ合衆国の 4 位以上の変化は見られない。

上位 2 か国以外のアクセス件数はいずれも減少しており、中華人民共和国、アメリカ合衆国、台湾からのアクセス件数は、それぞれ前期比約 22%、約 25%、約 11%の減となっている。

日本からのアクセス件数は減少傾向を示しているが、検知比率としては前期比約 10%増となっている。

発信元の上位第 3 か国は、日本、大韓民国、中華人民共和国の順であり、これらのアクセス件数が、全体の約 7 割半を占める。

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。

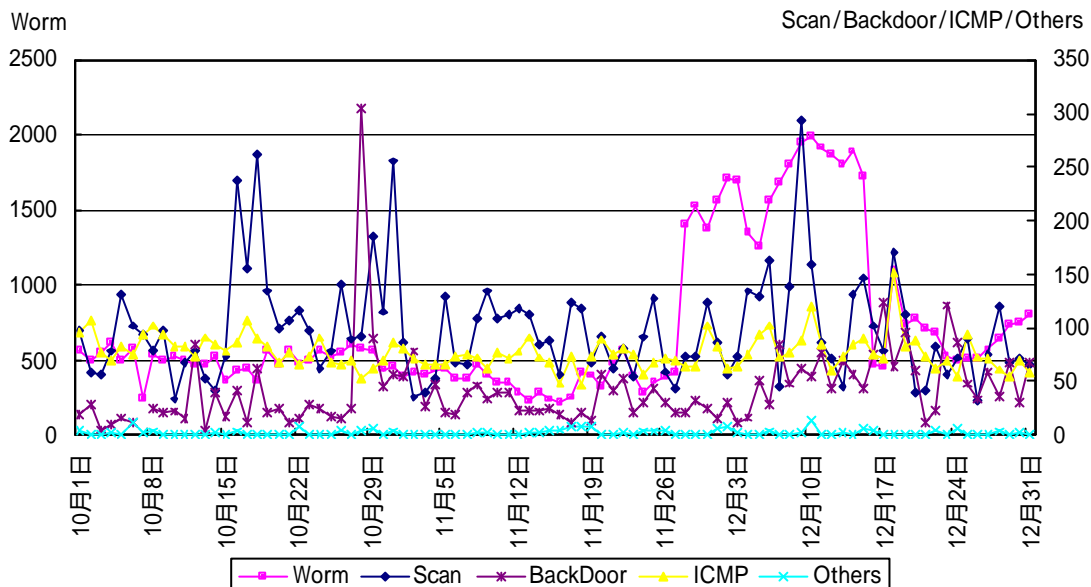


図 14 攻撃手法別の検知件数推移

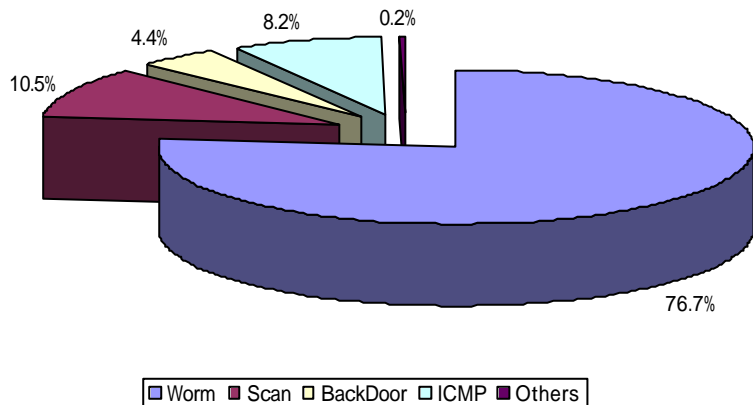


図 15 攻撃手法別の検知件数比率

「Worm」(SQL Slammer ワーム)が11月28日から12月15日にかけて増加しており、検知件数は、前期比約28%増となっている。

また、「BackDoor」も、約64%増加しており、その増加の大半はトロイの木馬の一種を検知する「SubSeven v2.2 probe」によるものである。同シグネチャの検知件数は「BackDoor」の約94%を占めており、前期比約100%の増加となっている。

その他の検知件数は減少しているため、「Worm」と「BackDoor」の攻撃手法別の検知件数比率が、前期に比べ70.6%から76.7%、3.1%から4.4%とそれぞれ増加している。

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。

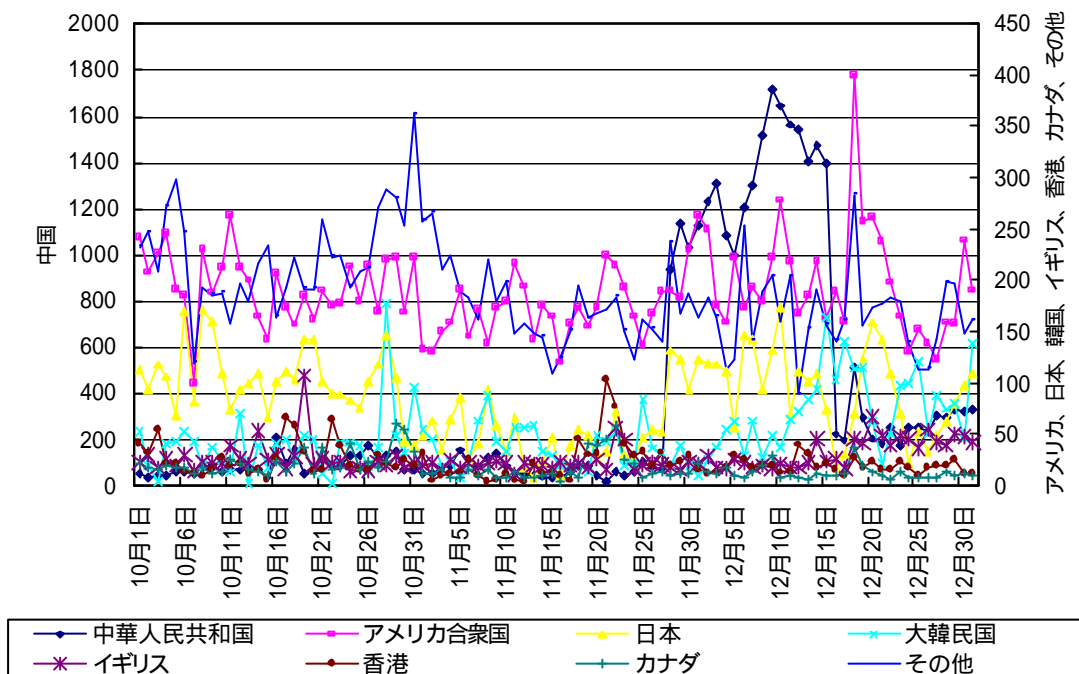


図 16 発信国/地域別の検知件数推移

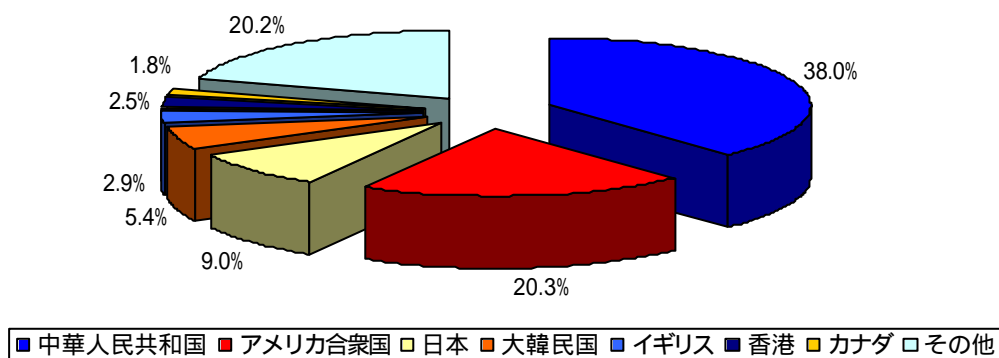


図 17 発信国/地域別の検知件数比率

11月28日から12月15日にかけて増加した「SQL Slammer ワーム」の影響により、中華人民共和国からの検知件数が最も多くなっており、前期比400%の増加となっている。また、前期第7位であった韓国も200%増加し、検知件数第4位となっている。

これまで検知件数の最も多かったアメリカ合衆国が、前期比約30%減となったのをはじめ、その他の国は全体的に減少傾向である。国内からの検知件数も、前期比約30%減となっている。

SYN flood 被害観測システムについて

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インターネットの定点観測を行っており、これを利用して SYN/ACK パケットの観測を行っている。

今期の検知比率を図 18 に示す。

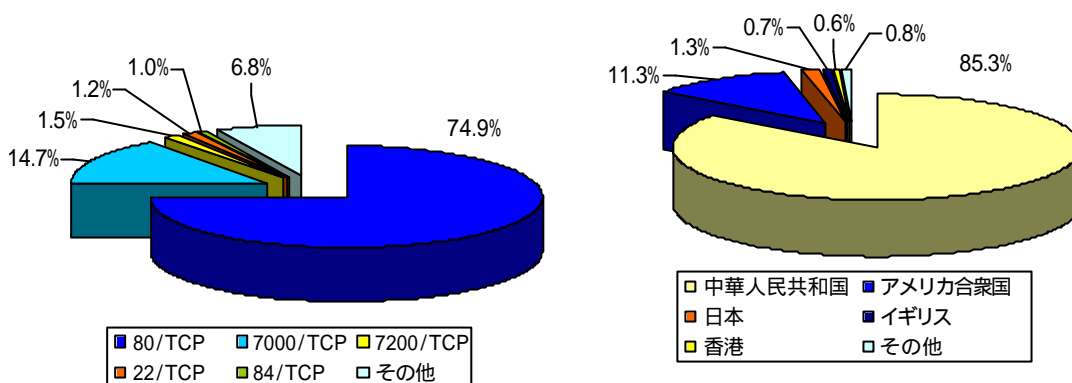


図 18 平成 16 年度第 3/四半期における SYN/ACK パケットの検知比率

検知総件数は、前期に比べ約 58%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 85%から 75%と減少しているが、依然として最多である。SYN flood 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 パケットが約 85%と大多数を占める。

また、アメリカ合衆国を発信元とするパケットも多く検知している。中華人民共和国・アメリカ合衆国の二国については、定常的に検知しており、この二国に対する SYN flood 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、11 月中旬に特定個人サーバ等からのパケット、12 月中旬に国内企業からのパケットを検知している。(図 19) このことから、これらのサーバが SYN flood 攻撃の被害を受けたものと推定される。

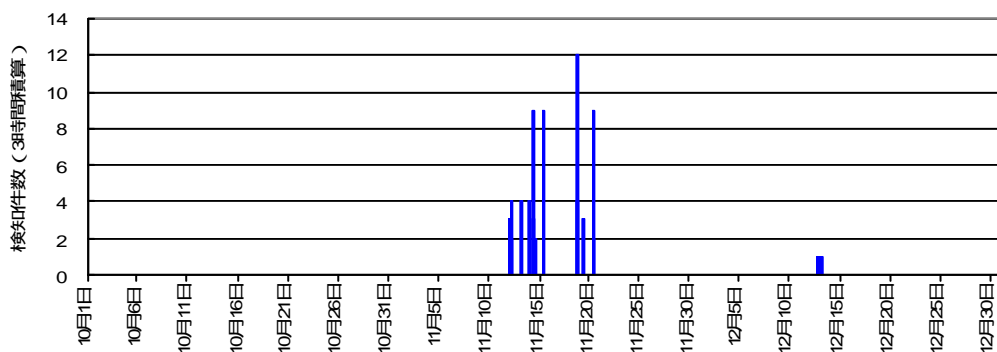


図 19 日本を発信元とする 80/TCP からの、3 時間毎の検知件数

SSH を利用した不正侵入行為

本年7月中旬以降、SSH¹²に対するアクセスをファイアウォールにて多数検知しており、本年度第2/四半期（7月から9月の間）の検知件数が約8,000件であったのに対して、第3/四半期（10月から12月の間）には約13,000件と約1.5倍に増加している。

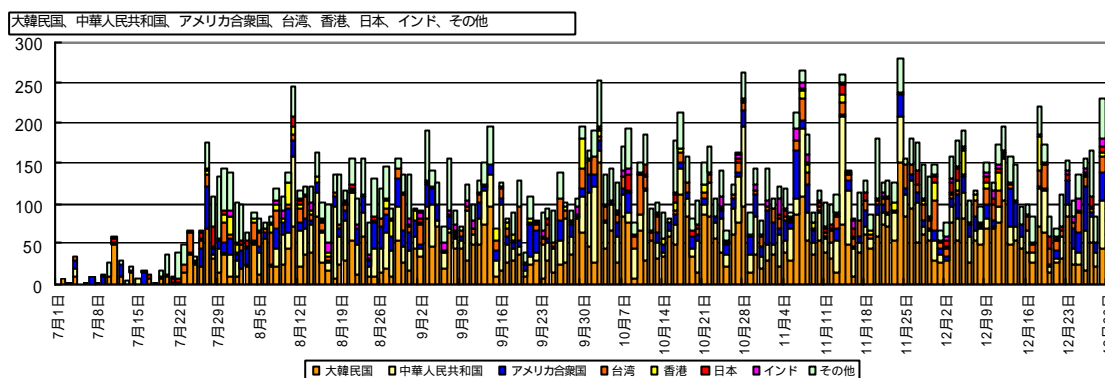


図 20 SSH (22/TCP) の検知状況(7月～12月)

不正侵入行為観測結果

SSH に対して行われている活動を把握するために、専用の監視システムを用いて観測を行った。以下の内容は、10月1日から31日までの一か月の観測結果に基づく不正侵入行為の実態及びその対策についてである。¹³

・攻撃されたアカウント

最も攻撃されたアカウントは、Unix系OSの管理者アカウントである「root」であり、全体の約4割を占める。また、サーバアプリケーション等で作成されるアカウントも確認された。試行されたパスワードとしては、アカウントと同一のものや、単に「password」といった安易なものが観測されている。

・侵入状況

今回の観測では、あらかじめアカウントとして「test」、「user」、「admin」の3つを作成し、パスワードは辞書攻撃を容易にするためにアカウントと同じものとした。実際に観測システムへ侵入した回数は32回であった。

・侵入後に実行したコマンド

観測システムへ侵入後に入力されたコマンドとしては、「wget」、「ftp」、「lynx」、「curl」といったファイル転送に用いられるコマンドが数多く占めており、外部からのツール類

¹² SSH (Secure SHell) は主に UNIX 系コンピュータで使用されるサービスであり、22/TCP ポートを使用する。

¹³ SSH を利用した不正侵入行為

http://www.cyberpolice.go.jp/detect/pdf/ssh_monitor.pdf

のダウンロードを目的とする行為が観測された。また、「cat」、「uname」、「w」、「ps」、「cd」など UNIX 系 OS の標準的なコマンドも実行されている。全般的な傾向として、侵入者の多くは、簡単に観測システム内の状況を確認した後、各種ツール類のダウンロードを試みている。¹⁴

対策

今回の事象は、アプリケーション・OS の脆弱性や欠陥を突くものではないことから、対策としては以下のことを再確認することで攻撃を防ぐことが可能である。

- (1) SSH サービスを使用していない場合は、サービスを停止する。
- (2) root によるログインを許可しない。(telnet では root ログインが不可であるのに対して、SSH では root ログインをデフォルトで許可している場合が多い。)
- (3) 安易なパスワードを設定しない。(サーバアプリケーション等が作成するアカウントを含むすべてのユーザに徹底する。)

その他、SSH 接続を許可する発信元 IP アドレスを限定することや、パスワード以外に証明書を用いた認証を行うなど、利用環境に応じて様々な対策が存在する。

¹⁴ 今回の観測環境では、侵入者はコンピュータを一般利用者の権限で自由に操作できるが、外部ネットワークに対するアクセスはファイアウォールで制限した。