

平成 22 年 7 月 30 日

インターネット観測結果等

(平成 22 年度第 1 / 四半期)

- ・ 53/UDP を発信元とする日本国内からのアクセスが急増
- ・ ファイル共有ソフト BitTorrent の稼働を確認する通信が 5 月以降減少

1 第 1 / 四半期における状況

今期のセンサーに対するアクセス件数は一日・1IP 当たり 533.7 件で、前期と比較して 101.4 件 (23.4%) 増加した。また、発信元 IP アドレス数は一日当たり 12,161.8 個で、前期と比較して 2,118.8 個 (14.8%) 減少した。この IP アドレス数の減少については、宛先ポート別 1 位の 445/TCP にアクセスのあった IP アドレス数がやや減少したことが原因である。

アクセス件数の上位 5 ポートは、445/TCP、ICMP Time Exceeded(以下「11/ICMP」とする。)、1433/TCP、135/TCP、ICMP Echo Request(以下「8/ICMP」とする。)の順であった。今期 2 位の 11/ICMP は、前期の検知件数はごくわずかであったが、今期は一日・1IP 当たり 22.7 件であり、増加が顕著であった。これは、今期増加している 53/UDP を発信元とするアクセスに伴って検知したものであり、詳細については「2-1 宛先ポート別」で述べる。

アクセス件数の上位 5 か国は、日本、中国、米国、ロシア、台湾の順であった。

前期 1 位の中国と、2 位の日本の順位が入れ替わっている。これも上述の 53/UDP を発信元とする日本国内からのアクセスの増加が原因である。

今期のシグネチャを用いた不正侵入等の検知件数は、一日・1IP 当たり 15.2 件で、前期と比較して 5.6 件 (26.9%) 減少した。また、検知した発信元 IP アドレス数は 1 日当たり 1,304.9 個で、前期と比較して 530.0 個 (28.9%) 減少した。これは、ファイル共有ソフト BitTorrent の稼働を確認する通信が 5 月以降減少したことが原因である。

今期の DoS 攻撃被害観測状況における SYN/ACK 及び RST/ACK パケット (DoS 攻撃の一種である SYN flood 攻撃において、発信元 IP アドレスを詐称した攻撃パケットに対する応答パケット) の検知件数は、一日当たり 8,719.0 件 (前期比 + 1,257.6 件、+ 16.9%) であり、発信元 IP アドレス数は一日当たり 149.7 件 (前期比 + 16.4 件、+ 12.3%) であった。米国からは、特定の IRC サーバに対する攻撃によるものと考えられる 6667/TCP を発信元ポートとする跳ね返りパケットを大量に検知しており、この IRC サーバに対する攻撃が頻繁に行われていると考えられる。

2 インターネット定点観測 センサーに対するアクセス

2-1 宛先ポート別

今期、最も特徴的であったのは、6月1日以降に検知している53/UDPを発信元ポートとするアクセス(図2-1、図2-2では「その他」に分類される。)の増加である。^{1,2}

DNSサーバで使用される53/UDPを発信元ポートとして、国内の複数の特定IPアドレスから、大量の回答パケットを継続的に検知している。この目的は不明であるが、何者かが特定の複数の国内DNSサーバに対し、発信元を偽って大量の問い合わせパケットを送信しているものと考えられる。また、一部の問い合わせパケットについては、経路途中で破棄されたことを11/ICMPとして検知している。(図2-4)

今期1位の445/TCPに対するアクセスは、平成20年11月頃から増加し、その後継続して検知している。445/TCPに対するアクセスの多くは、Windowsパソコンにおける特定のサービスの脆弱性(MS08-067)を悪用して感染活動を行うConfickerワームによるものと考えられる。前期と比較してアクセス件数、IPアドレス数はともにやや減少しており、Confickerワームの感染者数は減少傾向にあると考えられる。(図2-5)

今期2位の11/ICMPのアクセスは、上記の特定の国内DNSサーバ宛の通信によるもののほか、5月中旬に米国からの一時的な増加が見られた。これは、特定の1IPアドレスに対する80/TCPへのアクセスを試みようとしたパケットであった。(図2-6)

また、今期増加2位となっている9415/TCPに対するアクセスは、中国の多数のIPアドレスからの6000/TCPを発信元としたものが大半を占めていた。このアクセスは前期3月頃から5月にかけて大幅に増加しており、9415/TCPを使用する公開プロキシサーバを探索しているものと考えられる。³

今期増加3位となっている23/TCPに対するアクセスは、6月に入って急増している。Telnetサービスに対するスキャン行為であると考えられる。

¹ 「53/UDPを発信元ポートとするアクセスの増加について」, <http://www.cyberpolice.go.jp/detect/pdf/20100603.pdf>

² 「53/UDPを発信元ポートとするアクセスの増加について(第2報)」, <http://www.cyberpolice.go.jp/detect/pdf/20100611.pdf>

³ 「9415/TCPに対するアクセスの増加について」, <http://www.cyberpolice.go.jp/detect/pdf/20100615.pdf>

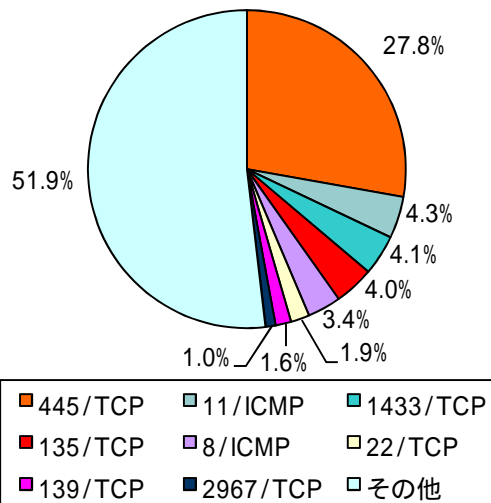


図 2-1 世界の宛先ポート比率¹

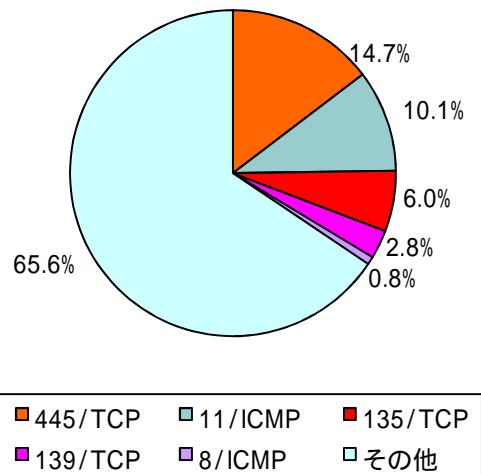


図 2-2 日本の宛先ポート比率¹

表 2-1 宛先ポート別検知件数

今期 順位	前期 順位	ポート	今期件数 (一日・1IP 当たり)	前期比 (一日・1IP 当たり)	増加 順位	減少 順位
1位	1位	445/TCP	148.32 件	- 15.3% (- 26.73 件)		1位
2位	155位	11/ICMP	22.73 件	+ 37,011.3% (+ 22.67 件)	1位	
3位	4位	1433/TCP	21.93 件	+ 11.9% (+ 2.33 件)	4位	
4位	2位	135/TCP	21.59 件	- 30.6% (- 9.53 件)		2位
5位	3位	8/ICMP	18.18 件	- 34.1% (- 9.41 件)		3位
7位	5位	139/TCP	8.46 件	- 45.2% (- 6.98 件)		4位
9位	28位	9415/TCP	5.38 件	+ 467.7% (+ 4.43 件)	2位	
10位	20位	23/TCP	4.90 件	+ 241.9% (+ 3.47 件)	3位	

¹ 当データは、小数点第二位で四捨五入しているため、合計が 100%にならないことがある。

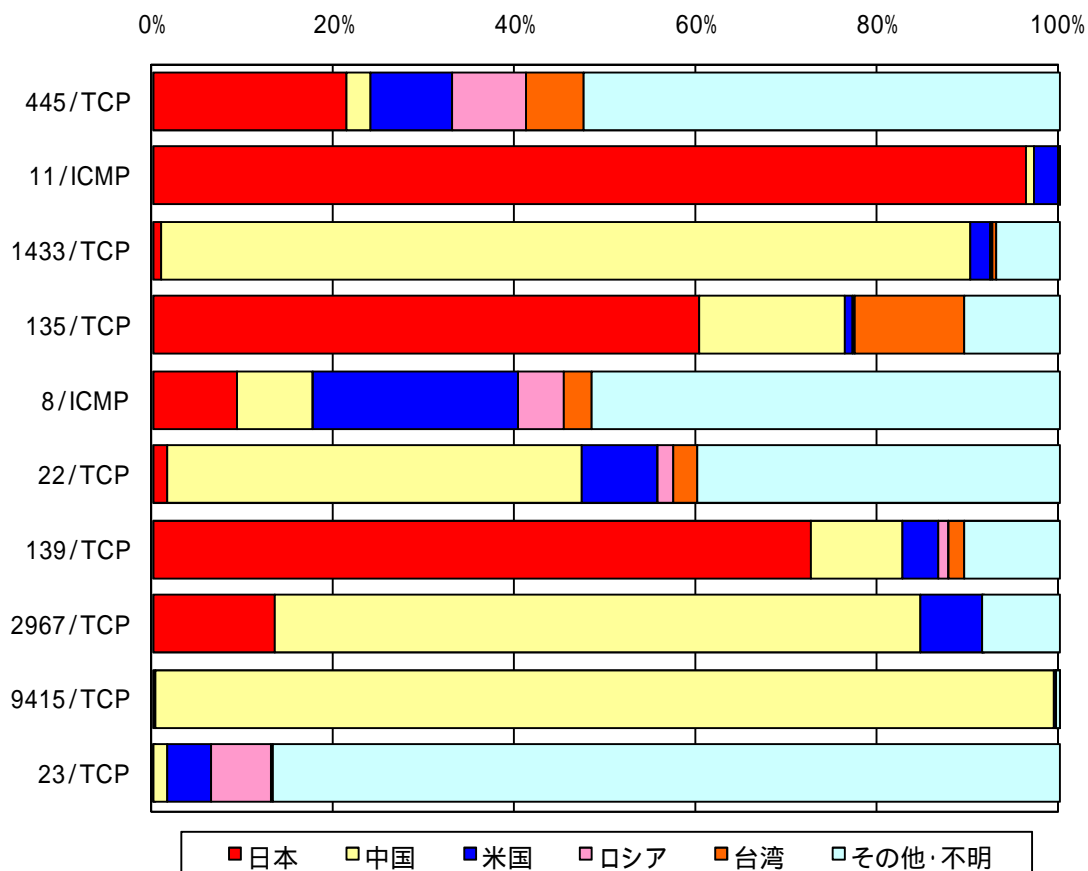


図 2-3 宛先ポートの国・地域別比率

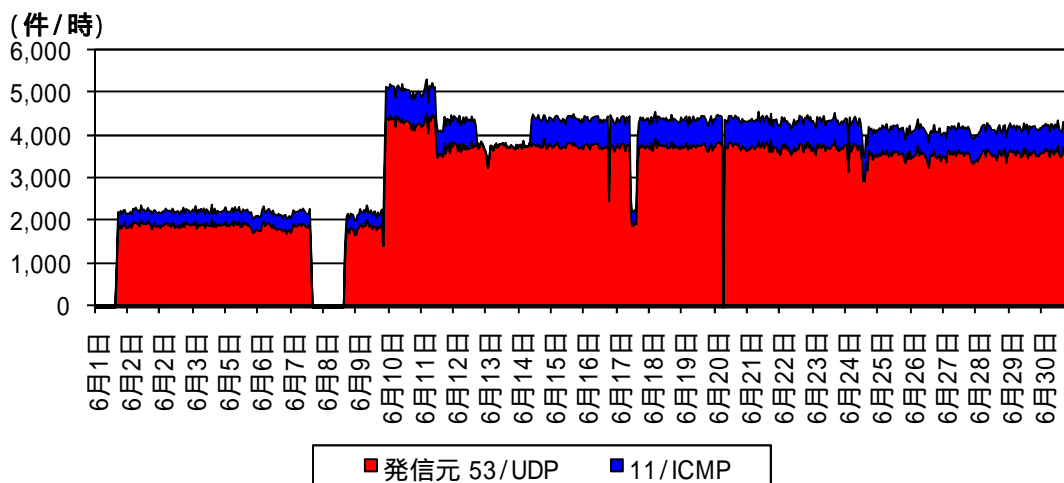


図 2-4 日本国内からの発信元 53/UDP 及び 11/ICMP のアクセスの推移

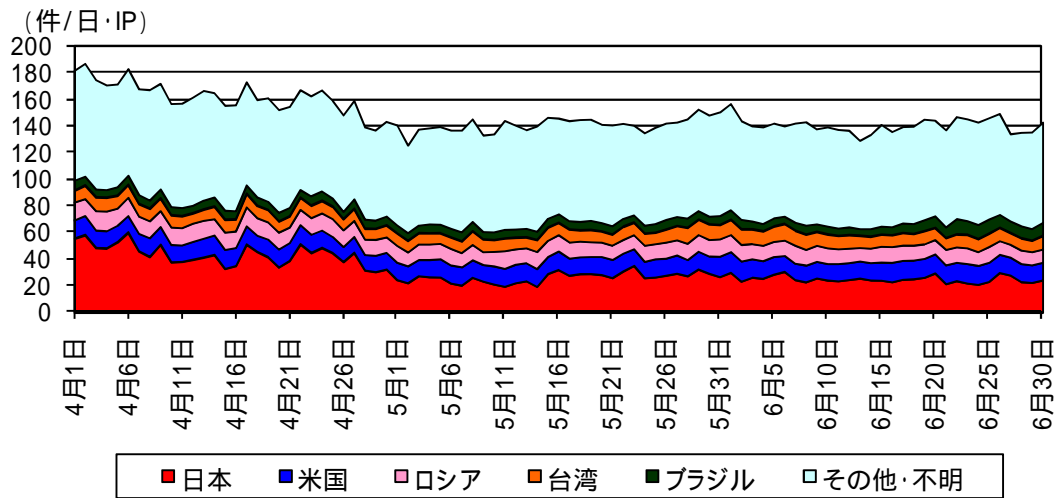


図 2-5 宛先ポート 445/TCP に対するアクセスの推移

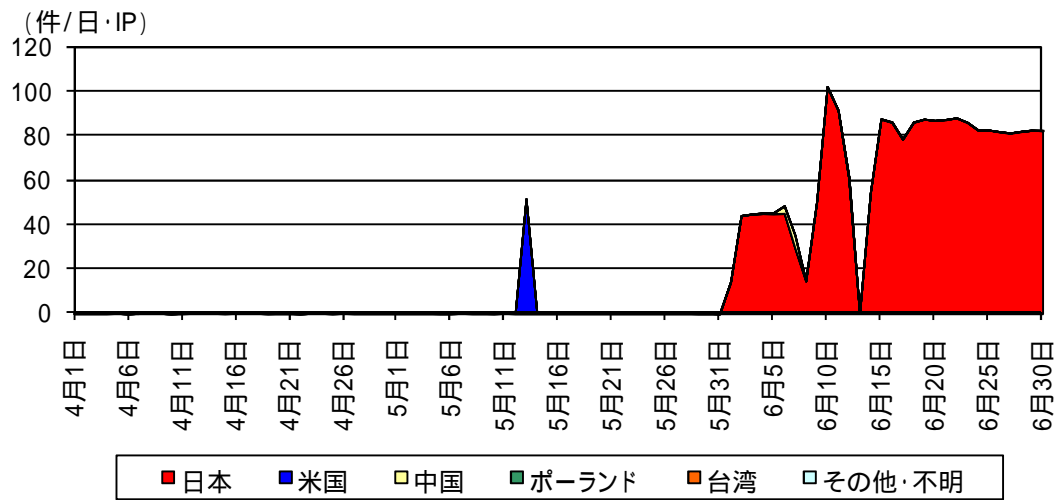


図 2-6 11/ICMP のアクセスの推移

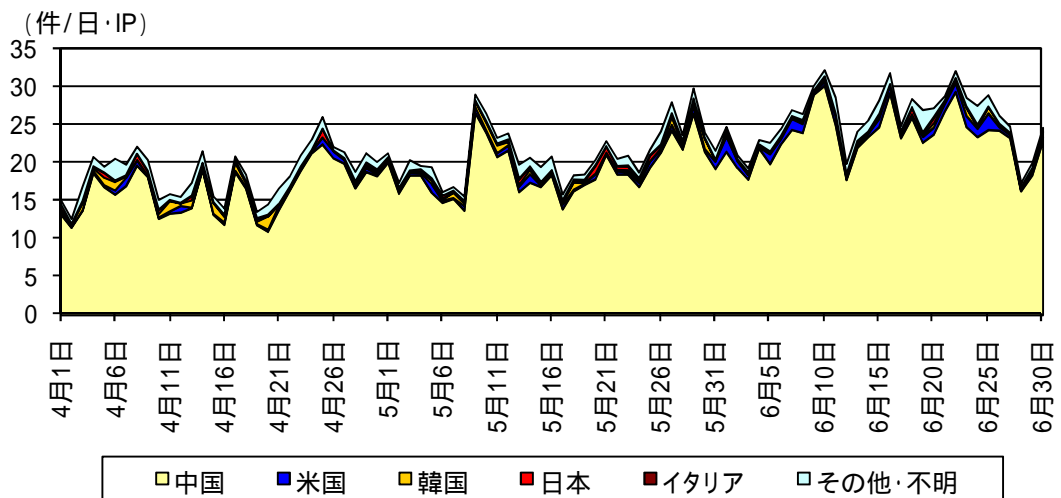


図 2-7 宛先ポート 1433/TCP に対するアクセスの推移

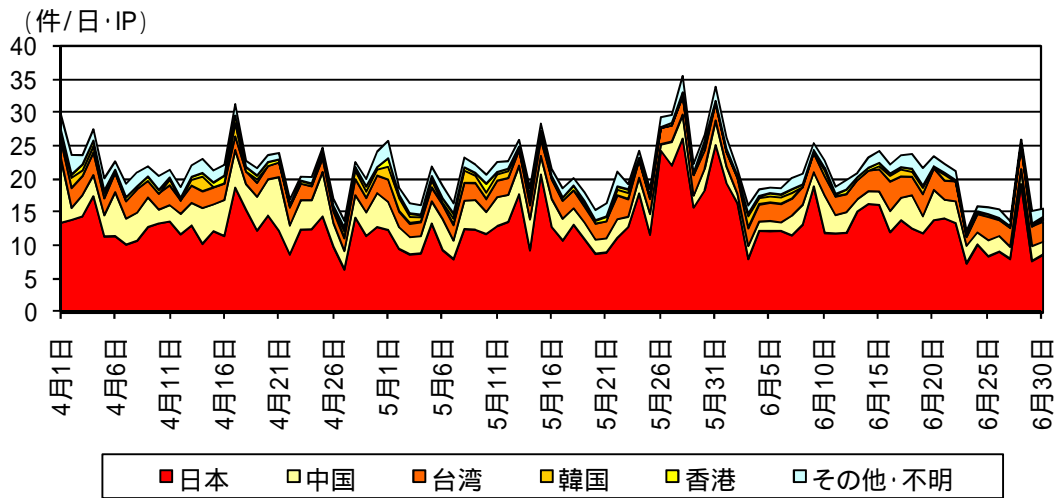


図 2-8 宛先ポート 135/TCP に対するアクセスの推移

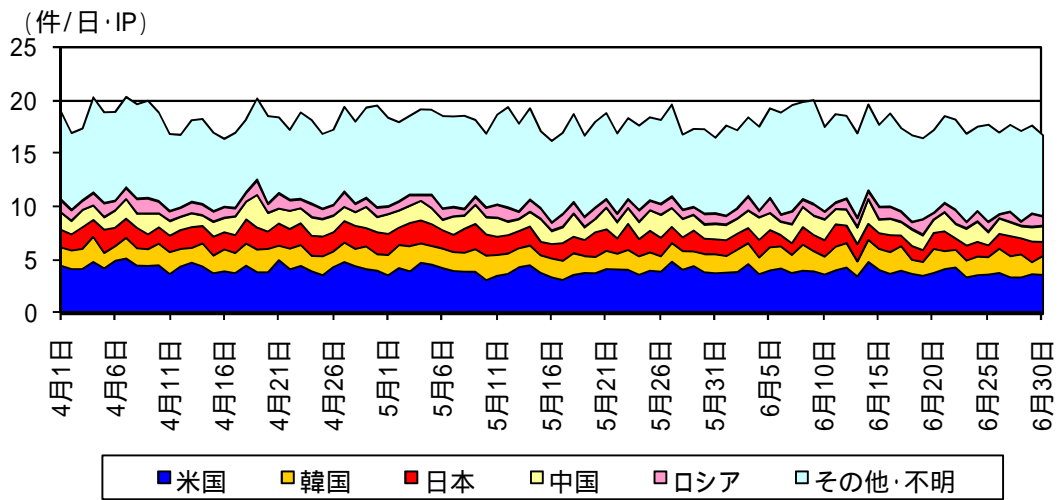


図 2-9 8/ICMP のアクセスの推移

2-2 発信元国・地域別

今期は、日本からのアクセスが大幅に増加しており、前期 1 位の中国との順位が逆転した。それ以外の上位国については、順位の変動はなかった。(図 2-10)

今期 1 位の日本国内からのアクセスのうち、11/ICMP が 10.1%、53/UDP を発信元とするアクセス(図 2-12 では「その他」に含まれる。) が 64.5%を占め、全体の 74.6%が 53/UDP を発信元とするアクセス増加に関するものとなっていた。これらのアクセスは「2-1 宛先ポート別」で述べたとおり、何者かが、特定の複数の国内 DNS サーバに対して、発信元を偽った大量の問い合わせ要求を送信しているものと考えられる。(図 2-12)

今期 2 位の中国からのアクセスは、9415/TCP の大幅な増加が見られた。中国の動画共有サイトにおいて配布されているソフトウェアに、このポートを利用して、外部からも利用可能なプロキシサーバとしてコンピュータを動作させるものがあることを確認している。今回のアクセスは、このようなプロキシサーバを探索するものである可能性が考えられる。¹ また、4 月下旬に、特定の IP アドレスの 6532/TCP からの跳ね返りパケット(図 2-13 では「その他」に分類される。)が見られた。これはオンラインゲームで使用されているポートとみられる。中国のオンラインゲームサービスへの攻撃とみられる跳ね返りパケットは、今期に限らず以前から検知している。(図 2-13)

今期 3 位の米国は、5 月 13 日に一時的に 11/ICMP のアクセスが急増した。これは何者かが、発信元を偽って、特定の IP アドレスの 80/TCP へのアクセスを試みたパケットが、経路中で破棄された事を伝えるものであった。同時期に、同じ IP アドレスからの 80/TCP の跳ね返りパケットを検知しており、この IP アドレスを持つウェブサーバに対して DoS 攻撃があったと推測される。また、4 月上旬から5月上旬まで検知があった 23632/UDP のアクセスは、ファイル共有ソフト BitTorrent の稼働を確認する通信であった。(図 2-14)

今期 4 位のロシアは、4 月後半に、図 2-15 の「その他」に分類されるアクセスが増加した。これは複数の UDP ポートへのアクセスであり、BitTorrent の稼働を確認する通信であった。(図 2-15)

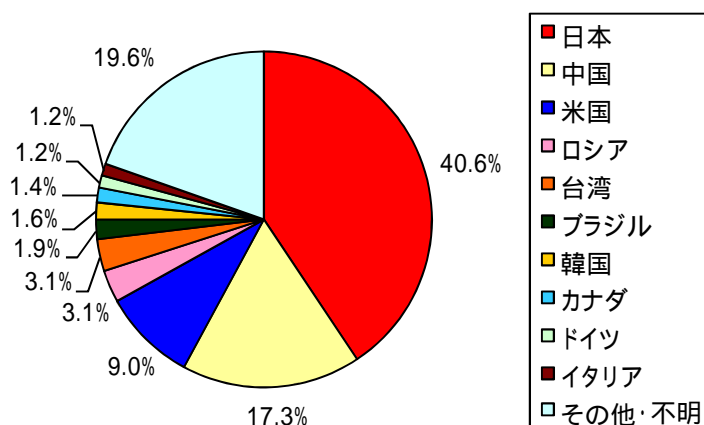


図 2-10 発信元国・地域別比率²

¹ 「9415/TCP に対するアクセスの増加について」, <http://www.cyberpolice.go.jp/detect/pdf/20100615.pdf>

² 当データは、小数点第二位で四捨五入しているため、合計が 100%にならないことがある。

表 2-2 発信元国・地域別検知件数

今期 順位	前期 順位	国・地域	今期件数 (一日・1IP 当たり)	前期比 (一日・1IP 当たり)	増加 順位	減少 順位
1位	2位	日本	216.89 件	+ 158.9% (+ 133.10 件)	1位	
2位	1位	中国	92.14 件	- 10.9% (- 11.32 件)		1位
3位	3位	米国	48.11 件	+ 23.9% (+ 9.27 件)	2位	
4位	4位	ロシア	16.68 件	- 18.7% (- 3.84 件)		3位
5位	5位	台湾	16.33 件	- 9.4% (- 1.70 件)		4位
6位	6位	ブラジル	10.07 件	- 30.8% (- 4.48 件)		2位
11位	14位	英国	5.62 件	+ 13.4% (+ 0.66 件)	4位	
18位	15位	オーストラリア	3.06 件	- 35.6% (- 1.69 件)		5位
31位	43位	パキスタン	1.74 件	+ 41.2% (+ 0.51 件)	5位	
40位	68位	ペルー	1.31 件	+ 228.9% (+ 0.91 件)	3位	

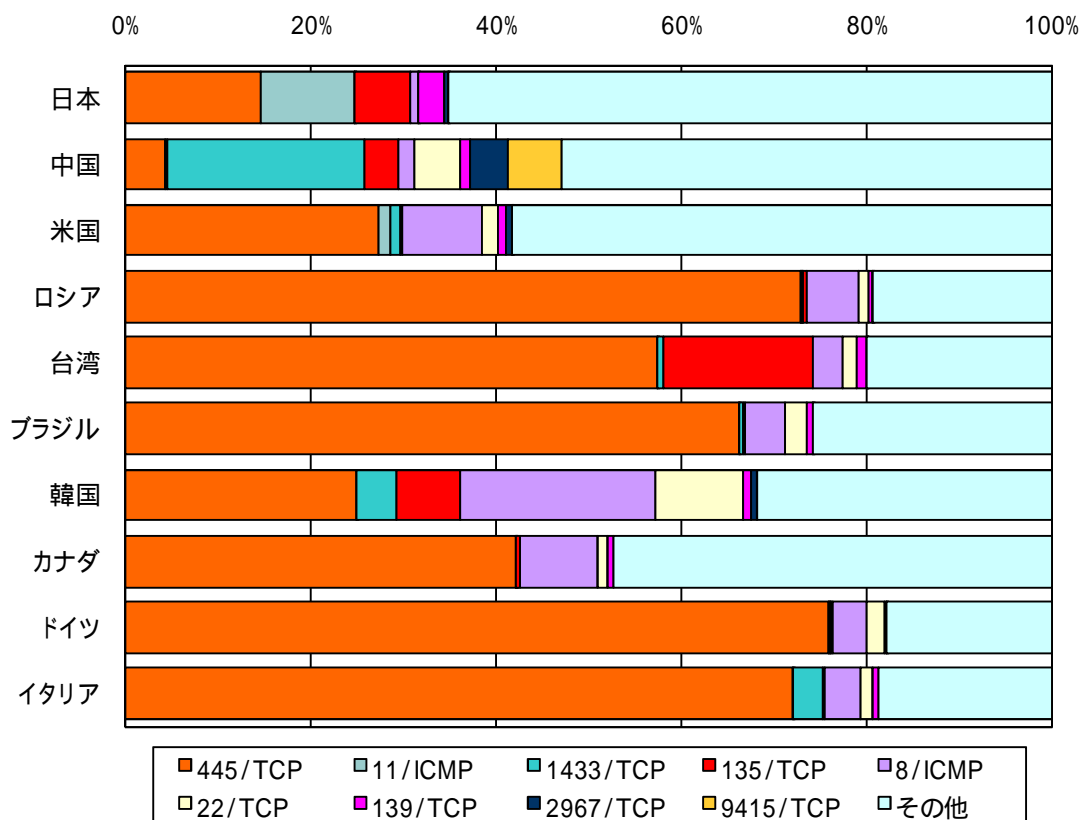


図 2-11 発信元国・地域別上位のポート別比率

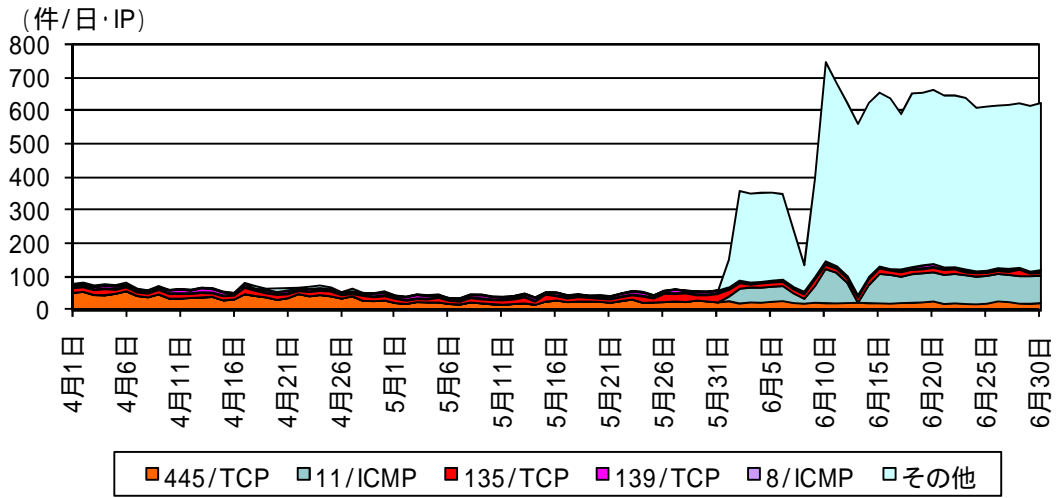


図 2-12 日本からのアクセスの推移

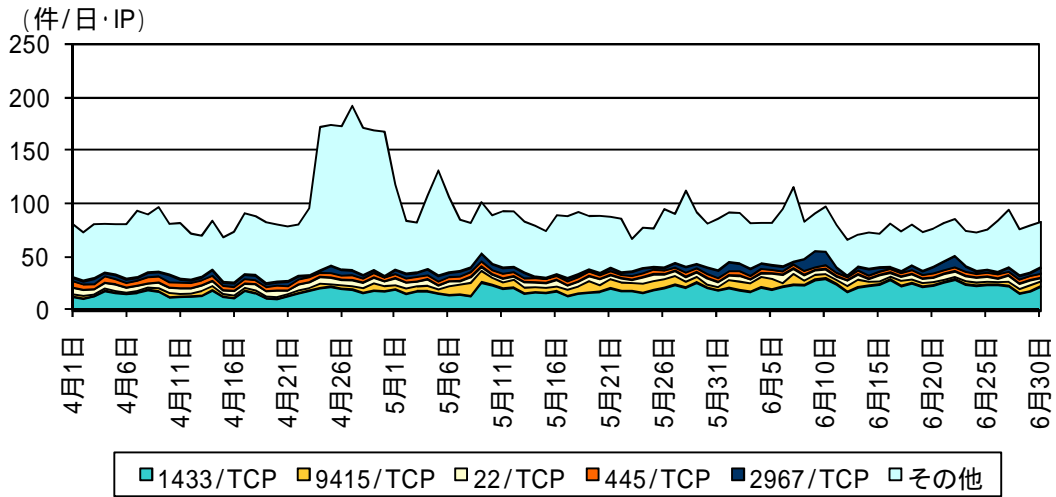


図 2-13 中国からのアクセスの推移

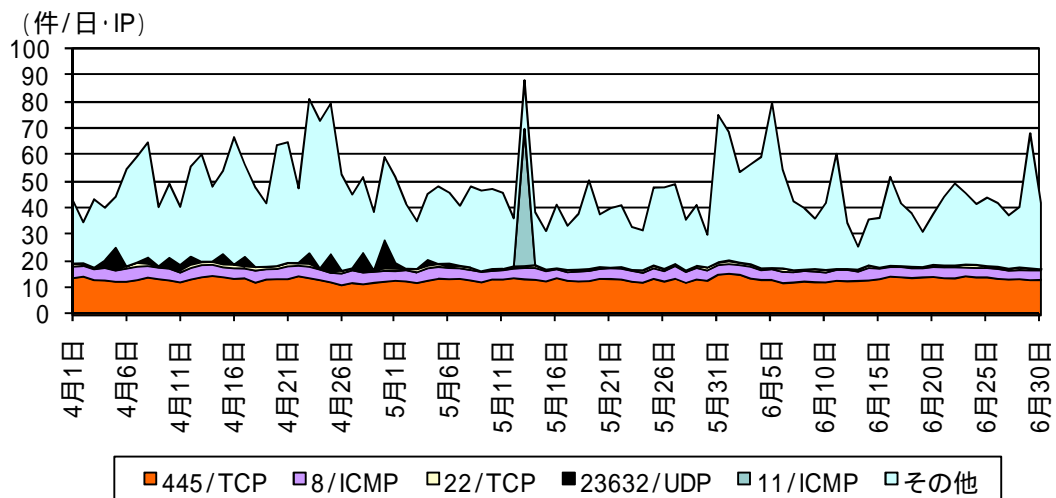


図 2-14 米国からのアクセスの推移

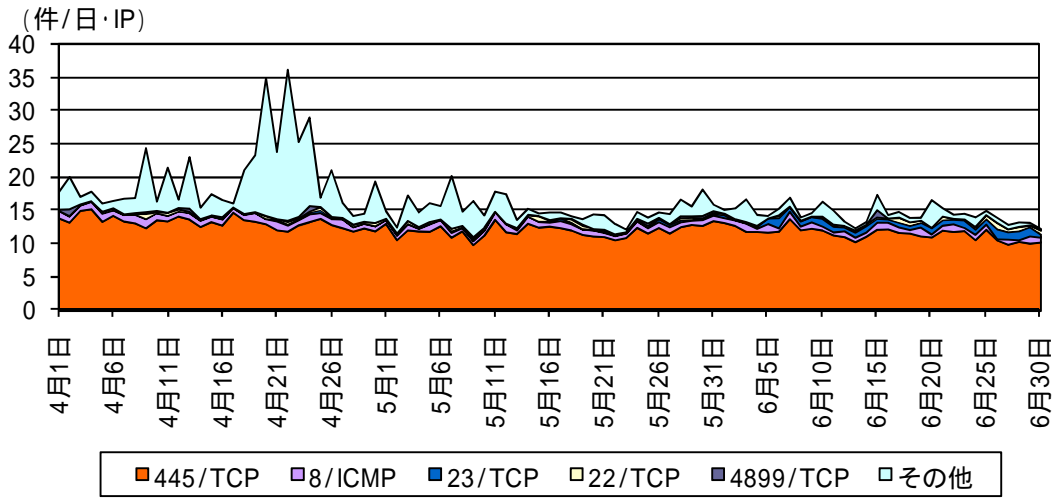


図 2-15 ロシアからのアクセスの推移

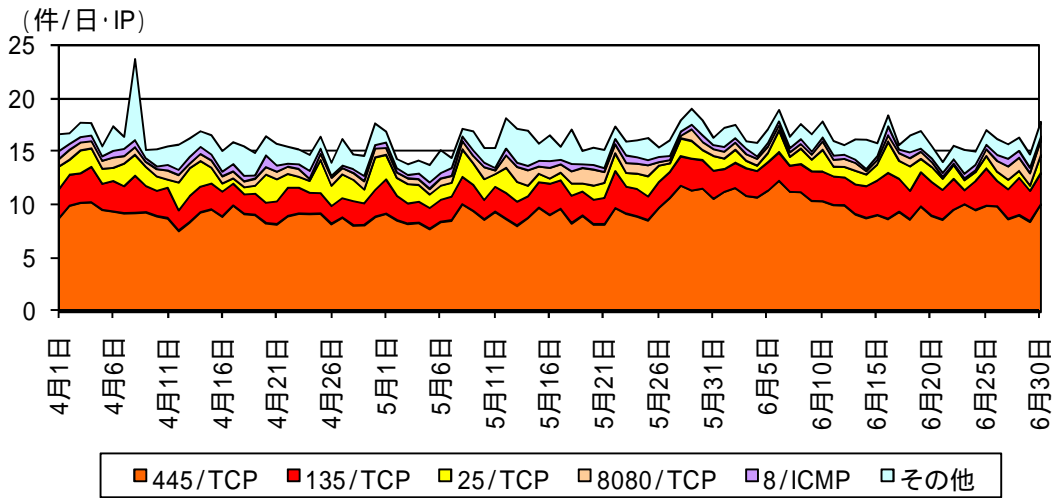


図 2-16 台湾からのアクセスの推移

3 インターネット定点観測 シグネチャを用いた不正侵入等の検知

3-1 攻撃手法別

今期のシグネチャを用いた不正侵入等の検知件数は、攻撃手法別では前期同様「Scan(P2P)」、「Worm」、「Scan」の順であり、この3分類で全体の97.6%を占めている。(図3-2)

「Scan(P2P)」は、前期に引き続いてすべてBitTorrentの稼働を確認する通信である。前期2月上旬から急激に増加し、4月中旬から下旬にかけてピークを迎え、6月には一日・1IP当たり2.4件になっている。ピーク時の検知件数は、一日・1IP当たり46.4件である。

「Worm」の検知件数は、一日・1IP当たり4.0件で、前期と比較して0.9件(17.8%)減少した。(表3-1) 「Worm」として検知したものの大部分はSQL Slammer及びNachiであり、SQL Slammerの検知件数は、前期と比較してやや減少していた。Nachiは、前期から引き続き緩やかな減少傾向にある。

「Scan」の検知件数は、一日・1IP当たり3.1件で、前期と比較して-0.2件(-4.8%)と大きな変化はなかった。(表3-1) 「Scan」として検知したものの96.9%は前期と同様にプロキシサーバを探索する通信であり、継続的に検知している。この通信は、攻撃のための踏み台となるプロキシサーバを探索していると考えられる。

表3-1 シグネチャを用いた不正侵入等の攻撃手法別検知件数

今期 順位	前期 順位	攻撃手法	今期件数 (一日・1IP 当たり)	前期比 (一日・1IP 当たり)	増加 順位	減少 順位
1位	1位	Scan(P2P)	7.64件	-38.1% (-4.70件)		1位
2位	2位	Worm	4.04件	-17.8% (-0.87件)		2位
3位	3位	Scan	3.12件	-4.8% (-0.16件)		3位

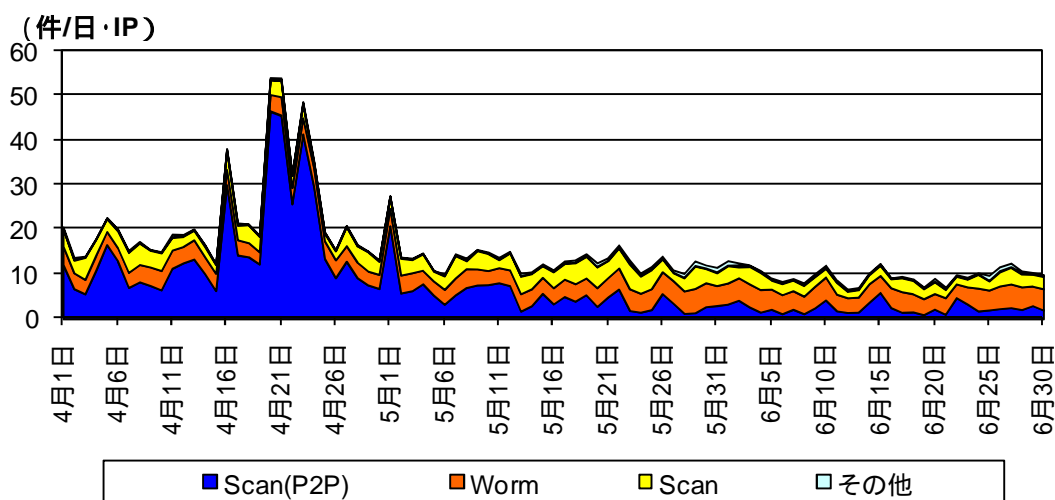


図3-1 シグネチャを用いた不正侵入等の攻撃手法別検知推移

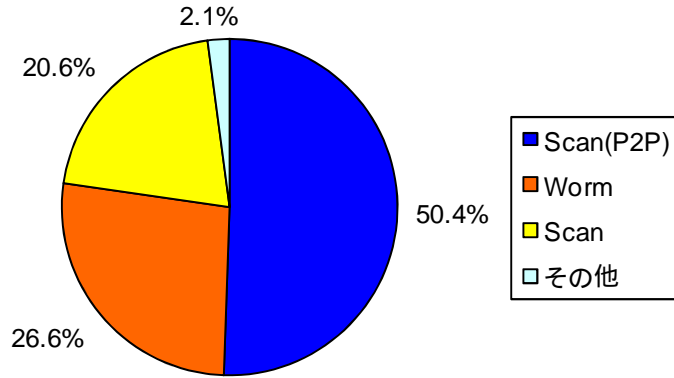


図 3-2 シグネチャを用いた不正侵入等の攻撃手法別検知比率¹

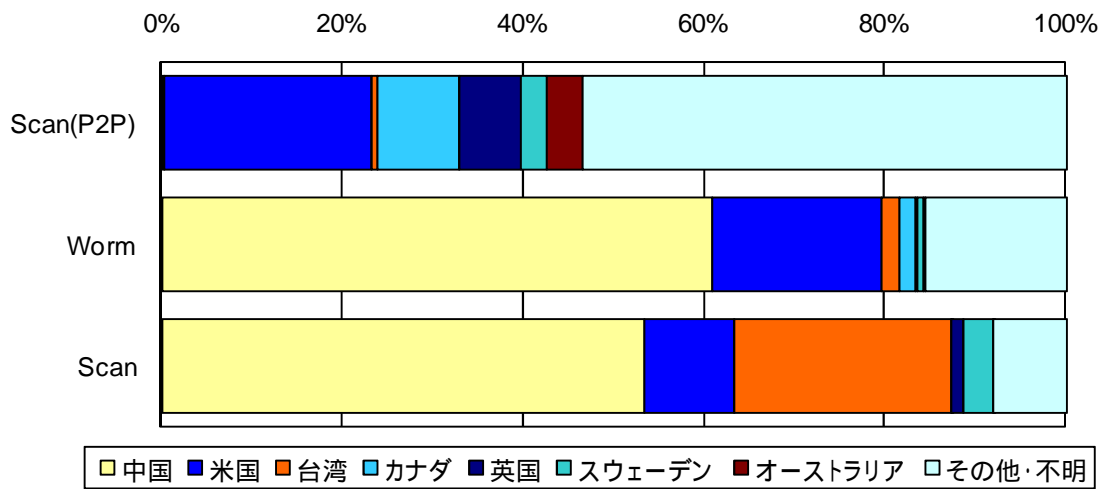


図 3-3 シグネチャを用いた不正侵入等の攻撃手法の国・地域別検知比率

¹ 当データは、小数点第二位で四捨五入しているため、合計が 100%にならないことがある。

3-2 発信元国・地域別

発信元国・地域別の検知件数は、中国、米国、台湾、カナダ、英国の順である。(表 3-2)

中国を発信元とするもののうち 57.3%が SQL Slammer ワームの検知であるが、一日・1IP 当たり 2.4 件で、前期と比較して 0.6 件(18.6%)減少した。

米国を発信元とする検知件数は、一日・1IP 当たり 2.9 件で、前期と比較して 0.4 件(12.4%)減少した。また、米国、カナダ、英国、スウェーデン、オーストラリアなど多数の国を発信元とするものの大部分が「Scan(P2P)」の検知であった。これらの地域からは、ファイル共有ソフト BitTorrent の稼働を確認する通信を多く検知している。

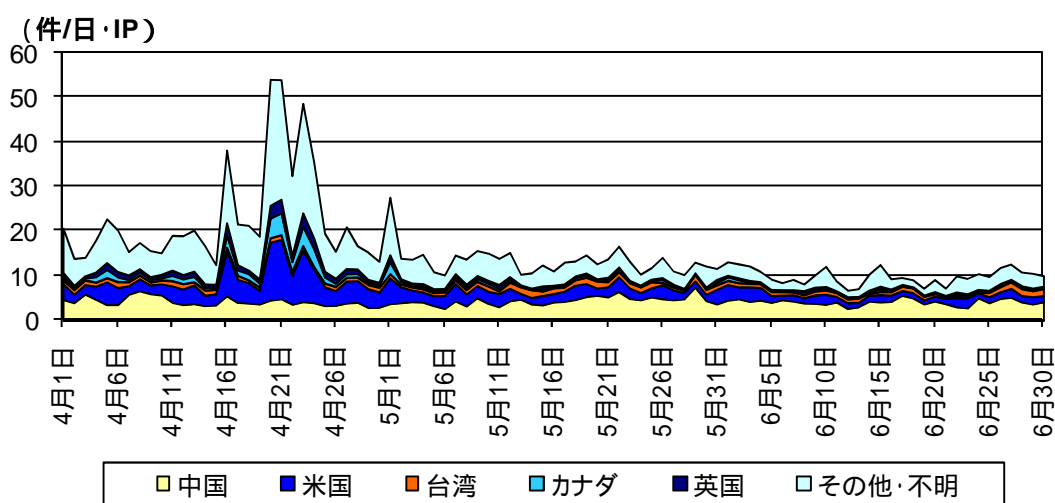


図 3-4 シグネチャを用いた不正侵入等の発信元国・地域別検知推移

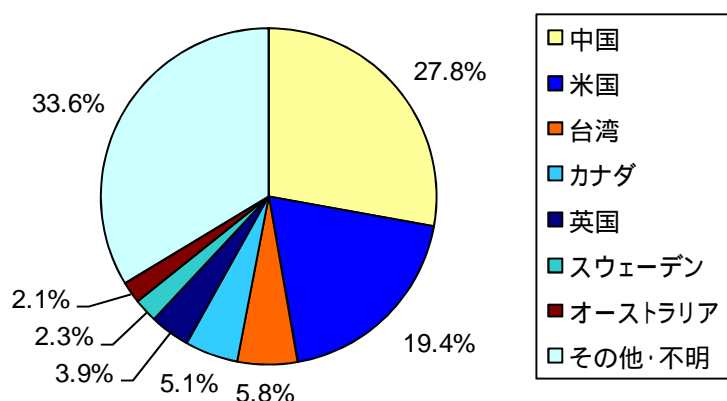


図 3-5 シグネチャを用いた不正侵入等の発信元国・地域別検知比率¹

¹ 当データは、小数点第二位で四捨五入しているため、合計が 100%にならないことがある。

表 3-2 シグネチャを用いた不正侵入等の発信元国・地域別検知件数

今期 順位	前期 順位	国・地域	今期件数 (一日・1IP 当たり)	前期比 (一日・1IP 当たり)	増加 順位	減少 順位
1位	1位	中国	4.22件	- 19.1% (- 1.00件)		1位
2位	2位	米国	2.94件	- 12.4% (- 0.42件)		2位
3位	4位	台湾	0.88件	- 5.6% (- 0.05件)		
4位	3位	カナダ	0.78件	- 23.3% (- 0.24件)		
5位	5位	英国	0.59件	- 29.9% (- 0.25件)		5位
8位	18位	韓国	0.28件	+ 3.6% (+ 0.01件)	2位	
19位	10位	ポルトガル	0.15件	- 65.1% (- 0.27件)		3位
20位	11位	フランス	0.14件	- 64.8% (- 0.25件)		4位
23位	42位	アルゼンチン	0.12件	+ 76.6% (+ 0.05件)	1位	
24位	31位	香港	0.12件	+ 9.2% (+ 0.01件)	3位	

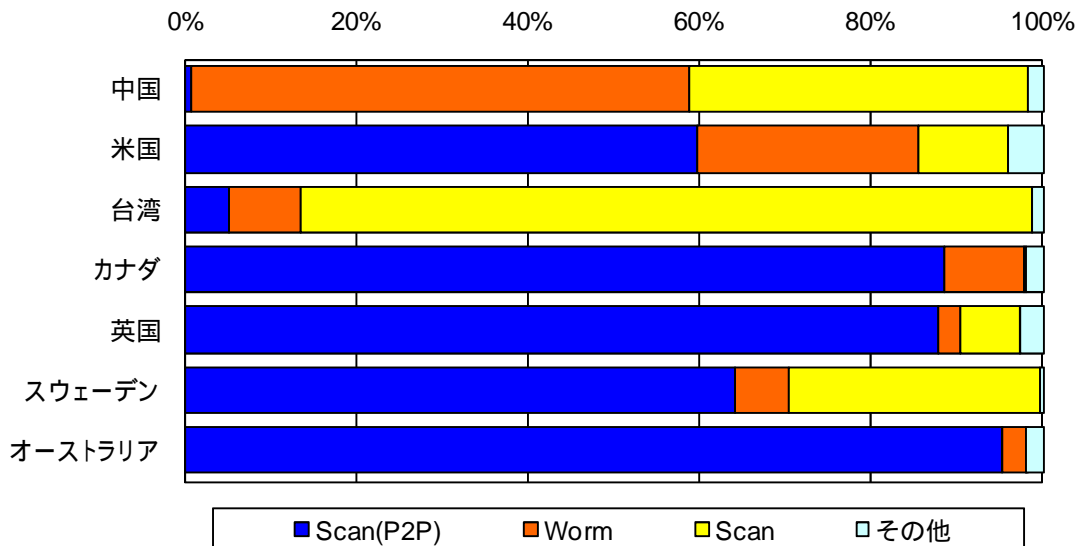


図 3-6 シグネチャを用いた不正侵入等の発信元国・地域別上位のシグネチャ別検知比率

4 インターネット定点観測 DoS 攻撃被害観測状況

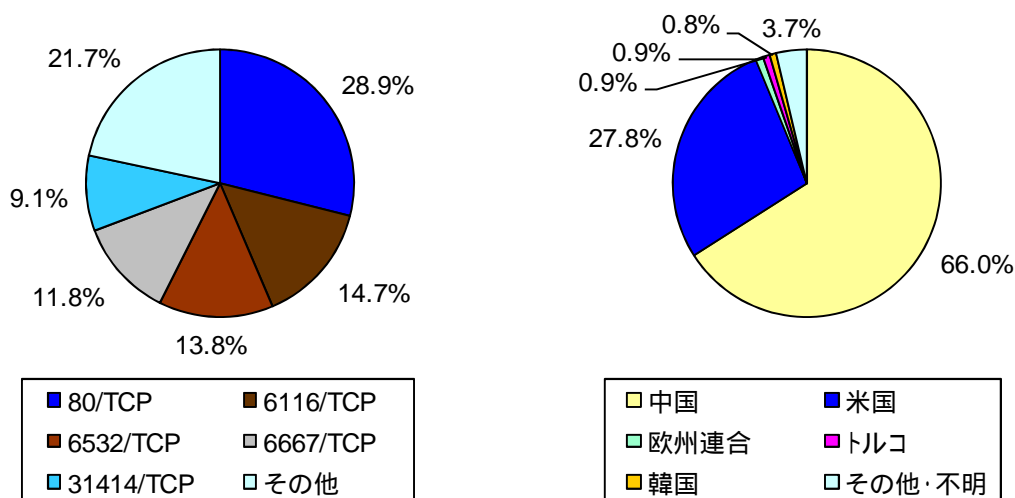


図 4-1 跳ね返りパケット発信元ポート比率¹ 図 4-2 跳ね返りパケット発信元国・地域別比率¹

今期の SYN/ACK 及び RST/ACK パケットの総検知件数は、一日当たり 8,719.0 件(前期比 + 1,257.6 件、+ 16.9%)であり、発信元 IP アドレス数は一日当たり 149.7 件(前期比 + 16.4 件、+ 12.3%)であった。

今期に検知した跳ね返りパケットのうち、6116/TCP、6532/TCP、31414/TCP を発信元ポートとするパケットは、すべて中国を発信元とするものであった。これ以外にも様々な発信元ポートからの同様の跳ね返りパケットを以前から検知している。これらの発信元ポートはオンラインゲームで使用するポートであり、中国国内のオンラインゲームサービスの妨害を目的とした攻撃が行われていると考えられる。

80/TCP を発信元とする跳ね返りパケットは、米国及び中国を発信元とするもので全体の 85.3%を占めている。パケット数は前期と比較して一日当たり 681.61 件(37.1%)増加しており、ウェブサーバに対する攻撃が頻繁に行われていると考えられる。

6667/TCP を発信元とする跳ね返りパケットは、前期と比較して一日当たり 945.36 件(1,091.6%)増加している。米国の特定の IP アドレスを発信元とするパケットが全体の 94.9%を占めており、この IP アドレスを発信元とするパケットは 3 月下旬頃から 7 月 1 日にかけて断続的に検知している。これは、特定の IRC サーバへの攻撃が 3 か月以上にわたって行われているものと考えられる。

韓国を発信元とする跳ね返りパケットは、全体の 91.4%が 80/TCP を発信元ポートとするパケットであった。6 月 9 日に韓国国家代表ポータルサイトに対する DoS 攻撃が行われたことも報じられているが²、警察庁では跳ね返りパケットを検知していない。

日本国内を発信元とする跳ね返りパケットは、一日当たり 5.4 件で、前期と比較して 8.7 件(61.7%)

¹ 当データは、小数点第二位で四捨五入しているため、合計が 100%にならないことがある。

² <http://japanese.yonhapnews.co.kr/society/2010/06/10/0800000000AJP20100610001800882.HTML>

減少している。また、80/TCP パケットが全体の 67.7%を占めている。

5 @police (Topics)掲載事項

@police において、平成 22 年 4 月から 6 月までの第 1 / 四半期に掲載した主なものは、次のとおりである。

分類	日付	掲載事項
【重要】	4月13日	ジャストシステム社ワープロソフトー太郎の脆弱性について
【重要】	4月14日	アドビシステムズ社の Adobe Reader および Adobe Acrobat のセキュリティ修正プログラムについて
【重要】	4月17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 (MS10-019,020,021,022,023,024,025,026,027,028,029)(4/17)更新
●	4月28日	「ガンブラー攻撃」に使用される URL の変化について
●	5月12日	インターネット治安情勢更新(平成 21 年度第 4 四半期報を追加)
【重要】	5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 (MS10-030,031)(5/21)更新
【重要】	6月1日	ジャストシステム社ワープロソフトー太郎の脆弱性について
●	6月3日	53/UDP を発信元ポートとするアクセスの増加について
【重要】	6月11日	アドビシステムズ社の Adobe Flash Player のセキュリティ修正プログラムについて
●	6月11日	53/UDP を発信元ポートとするアクセスの増加について(第2報)
【重要】	6月12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 (MS10-032,033,034,035,036,037,038,039,040,041)(6/12)更新
●	6月15日	9415/TCP に対するアクセスの増加について
【重要】	6月30日	アドビシステムズ社の Adobe Reader および Adobe Acrobat のセキュリティ修正プログラムについて

6 集計方法

6-1 センサーに対するアクセス

TCP 及び UDP はポートごとに集計し、以下ではスラッシュの前にポート番号を付けて表す。(例 135/TCP は TCP の 135 番ポートを表す。) ICMP パケットについては、タイプごとに集計し、以下ではスラッシュの前にタイプ番号を付けて表す。(例 8/ICMP は ICMP Echo Request を表す。)

6-2 シグネチャを用いた不正侵入等の検知

各センサーには、平成 22 年 6 月 30 日現在、シグネチャは 3,035 種類が登録されている。検知された各シグネチャは、表 6-1 に示す分類に従って集計している。

また、各センサーには、サーバ等の攻撃対象となる可能性のある機器を一切接続していない。そのため、セッションの確立を必要としない UDP を利用する Worm や Scan 系の検知が、大きな割合を占めている。

表 6-1 グラフに表示される分類と代表的なシグネチャ

分類	代表的なシグネチャ
Worm	SQL Slammer, Nachi, Conficker P2P
Scan	Proxy port probe, Port scan, TCP ACK ping
Scan (P2P)	BitTorrent DHT peer-to-peer, BitTorrent probe
UDP spam	MSRPC Popup Message
DoS	Windows Trin00 DDoS, ICMP Echo Reply without Echo
DNS	DNS request made for all records, DNS port probe, DNS dot query detected
Others	Traceroute, ISAKMP Vendor ID, SIP message detected