平成 24 年8月 31 日

インターネット観測結果等

（平成 24 年度第1／四半期（4月～6月））

・3389/TCP へのアクセスが前期に引き続き増加
・プロキシサーバの探索とみられる「Scan」が増加
・米国を発信元とする 80/TCP からの跳ね返りパケットが増加

1　第 1／四半期における状況

1-1　3389/TCP へのアクセスが前期に引き続き増加

センサーに対するアクセス件数は一日・1IP アドレス当たり 231.1 件で、平成 23 年度第4／四半期（以下「前期」という。）と比較して 44.4 件（16.1%）減少した。また、発信元 IP アドレス数は一日当たり 8,356.5 個で、前期と比較して 169.9 個（2.0%）減少した。

アクセス件数の上位5ポートは、445/TCP、1433/TCP、3389/TCP、ICMP Echo Request（以下「8/ICMP」という。）、22/TCP の順であった（表 2-1）。平成 24 年度第1／四半期（以下「今期」という。）は、Windows リモートデスクトップの探索と考えられる 3389/TCP に対するアクセスが、前期と比較して、36.4%増加しており、昨年度同期と比較すると4倍以上のアクセス件数であった。445/TCP に対するアクセス件数は前期と比較して、一日・1IP アドレス当たり 8.4 件(9.5%)減少したが、他のポートに対するアクセス件数と比較して、依然として多い状態である。TELNET サービスで使用される 23/TCP に対するアクセス件数は、前期に増加していた韓国、台湾及び中国を発信元とするアクセスが減少したため、前期と比較して、一日・1IP アドレス当たり 7.4 件（48.1%）減少した。

アクセス件数の上位5か国は、中国、米国、台湾、日本、ロシアの順であった（表 2-4）。

1-2　プロキシサーバの探索とみられる「Scan」が増加

シグネチャを用いた不正侵入等の検知件数は、一日・1IP アドレス当たり 8.4 件で、前期と比較して 1.5 件（22.1%）増加した。また、発信元 IP アドレス数は一日当たり 315.1 個で、前期と比較して 49.9 個（18.8%）増加した。

発信元国・地域別の検知件数の上位5か国は、中国、米国、ドイツ、インド、ブラジルの順であった。上位5か国すべてにおいて、プロキシサーバの探索とみられる「Scan」の検知件数が増加し、攻撃手法別検知件数全体の 56.8%を占めた(図 3-2)。

1-3　米国を発信元とする 80/TCP からの跳ね返りパケットが増加

DoS 攻撃被害観測状況は、一日当たり 8,806.8 件で、前期と比較して 2,370.4 件（36.8%）増加した。発信元 IP アドレス数は一日当たり 515.7 個で、前期と比較して 125.2 個（32.1%）増加した。

米国からの 80/TCP の跳ね返りパケットは、前期と比較して、一日当たり 541.1 件(25.4%)増加した。これは、4月前半に、特定の IP アドレスから多くの跳ね返りパケットが見られたためである(図 4-3)。

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

445/TCP に対するアクセスは、主に、Windows 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 ワームによるアクセスであると考えられる。このポートに対するアクセスは、前期に引き続き、アクセス件数及び発信元 IP アドレス数ともにやや減少したが、依然として高い水準で推移している(図 2-4)。

1433/TCP は、マイクロソフト社製データベース製品で使用されるポートである。このポートに対するアクセス件数は、前期と比較して 16.8%減少したが、ドイツからのアクセス数は、前期と比較して、約 22 倍に増加した。これは、今期初めから4月中旬頃まで、ある特定の IP アドレスからのアクセスが大量にあったためである(図 2-5)。また、このポートに対するアクセス件数のうち、82.3%は中国からのものであり、89.8%は何らかのツールを使用したスキャン活動と考えられる 6000/TCP を発信元ポートとするアクセスであった。

3389/TCP に対するアクセスは、Windows リモートデスクトップの探索と考えられる。このポートに対するアクセス件数は、前期と比較して、36.4%増加した(表 2-2)。昨年度同期と比較して4倍以上のアクセスがあり、増加傾向にある。このポートに対するアクセスにおいても 1433/TCP に対するアクセスと同様に 6000/TCP を発信元とするアクセスが見られ、その割合は 30.4%であった。

8/ICMP は、日本国内及び米国からのアクセス件数の増加が見られた(図 2-7)。このアクセスは、複数の研究機関や大学を発信元とし、複数のセンサーに対してそれぞれ一定数のアクセスがあった。インターネット上における何らかの調査を行っていたものと考えられる。

22/TCP は、SSH サービスで使用されるポートである。同ポートへのアクセスは、SSH サービスが稼働しているサーバへの侵入を目的とした探索と考えられる。このポートに対するアクセス件数は、前期と比較して 15.0%減少した(表 2-1)。5月下旬及び6月下旬に発信元 IP アドレス数の増加が見られたが、一時的なものであった。英国からのアクセスは前期と比較して、約 2.3 倍に増加したが、これは、6月に特定の IP アドレスから多くのアクセスがあったためである。

表 2-1 宛先ポート別検知件数(今期順位)

今期順位	前期順位	ポート	今期件数[1]	前期比[1]
1 位	1 位	445/TCP	79.96 件	−9.50% （−8.37 件）
2 位	2 位	1433/TCP	37.78 件	−16.8% （−7.65 件）
3 位	6 位	3389/TCP	15.84 件	＋36.4% （＋4.22 件）
4 位	5 位	8/ICMP	14.54 件	＋5.9% （＋0.81 件）
5 位	7 位	22/TCP	8.96 件	−15.0% （−1.59 件）

表 2-2 宛先ポート別検知件数(増加順位)

増加順位	ポート	今期件数[1]	前期比[1]	今期順位	前期順位
1 位	3389/TCP	15.84 件	＋36.4% （＋4.22 件）	3 位	6 位
2 位	8080/TCP	5.03 件	＋80.5% （＋2.24 件）	9 位	13 位
3 位	6666/TCP	1.42 件	＋183.7% （＋0.92 件）	15 位	28 位
4 位	8/ICMP	14.54 件	＋5.9% （＋0.81 件）	4 位	5 位
5 位	210/TCP	0.86 件	＋434.9% （＋0.70 件）	21 位	40 位

表 2-3 宛先ポート別検知件数(減少順位)

減少順位	ポート	今期件数[1]	前期比[1]	今期順位	前期順位
1 位	557/UDP	3.01 件	−87.3% （−20.78 件）	11 位	3 位
2 位	445/TCP	79.96 件	−9.5% （−8.37 件）	1 位	1 位
3 位	42731/UDP	ごく僅か	−100.0% （−8.05 件）	−[2]	8 位
4 位	1433/TCP	37.78 件	−16.8% （−7.65 件）	2 位	2 位
5 位	23/TCP	7.89 件	−48.1% （−7.32 件）	6 位	4 位

[1] 一日・1IP アドレス当たり。

[2] 検知件数がごく僅かであったため、記載していない。

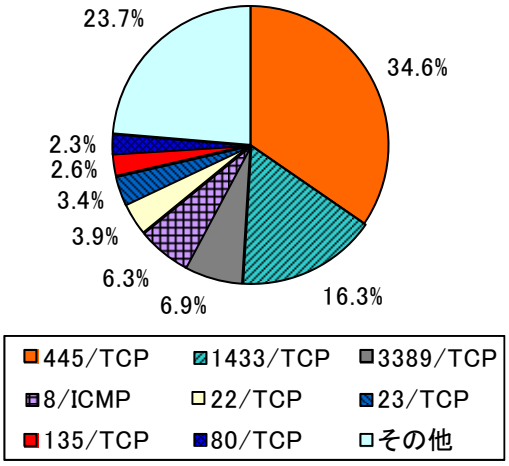

図 2-1　宛先ポート比率(すべて)[1]

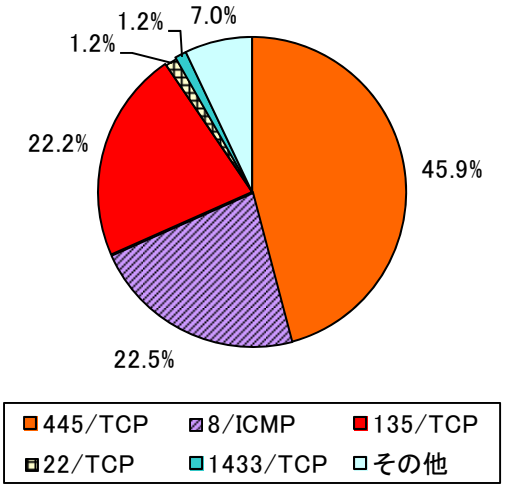

図 2-2　宛先ポート比率(日本国内)[1,2]

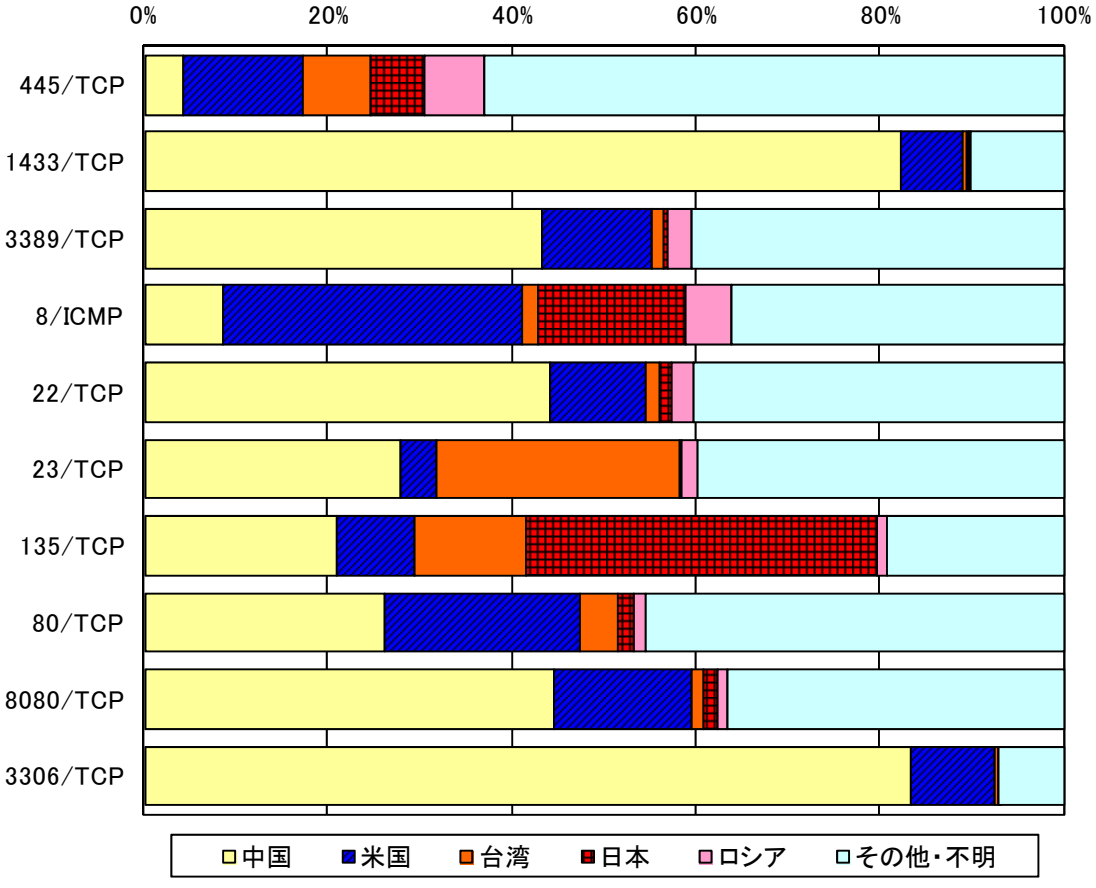

図 2-3　宛先ポート別上位の発信元国・地域別比率

[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。
[2] 発信元国・地域が日本国内からのアクセスのみ集計した。

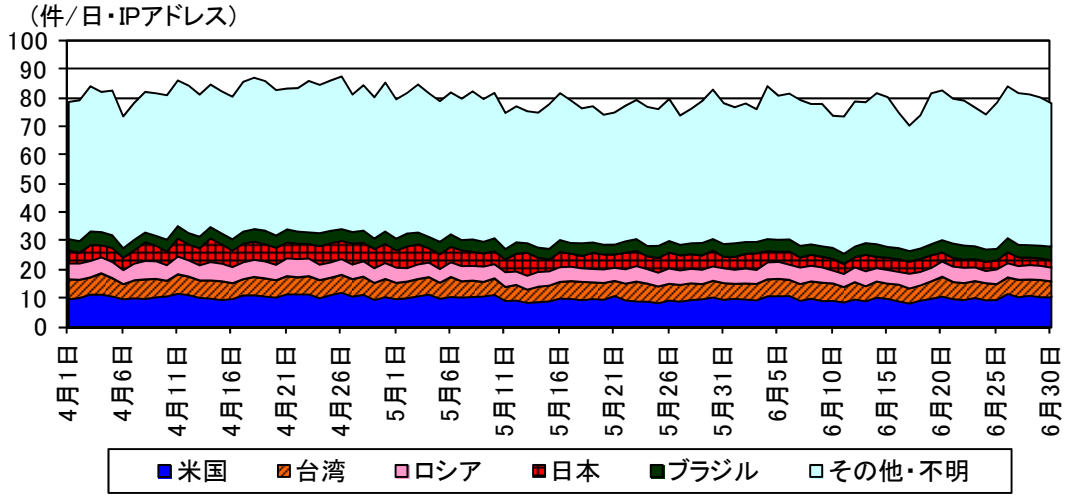

図 2-4　宛先ポート 445/TCP に対するアクセス件数の推移

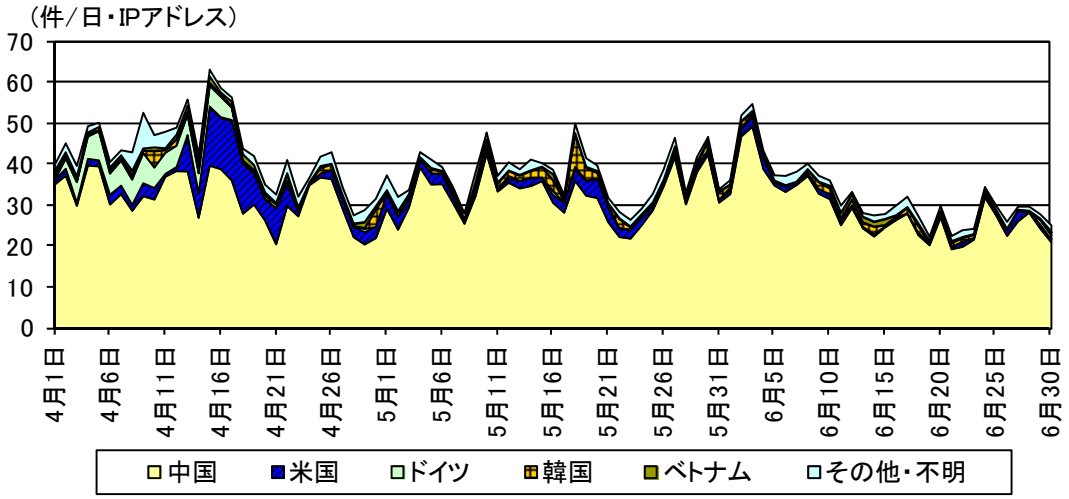

図 2-5　宛先ポート 1433/TCP に対するアクセス件数の推移

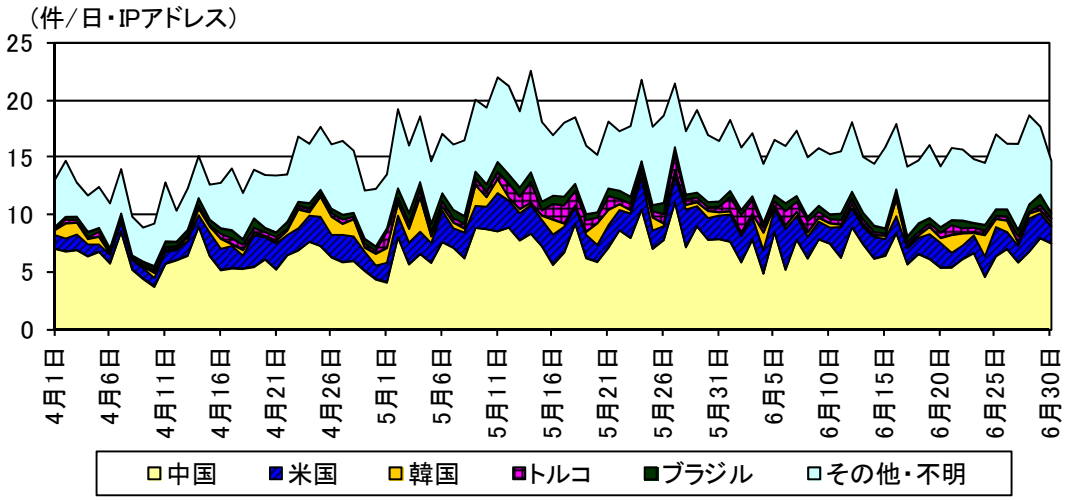

図 2-6　宛先ポート 3389/TCP に対するアクセス件数の推移

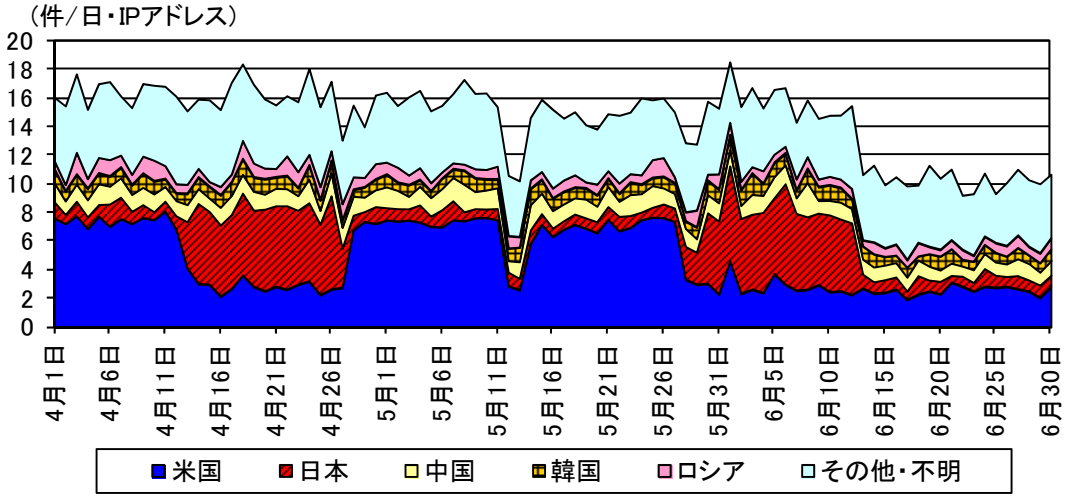

図 2-7　8/ICMP のアクセス件数の推移

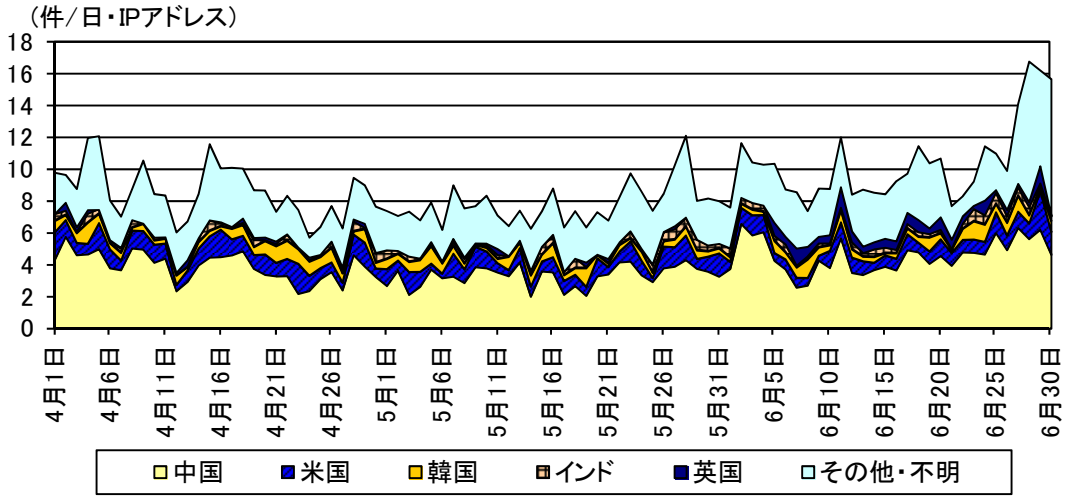

図 2-8　宛先ポート 22/TCP に対するアクセス件数の推移

2-2　発信元国・地域別

今期は、中国からのアクセス件数が減少した。前期に多数見られた 557/UDP 及び 42731/UDP へのアクセス件数が、大幅に減少したことが要因である。また、6000/TCP を発信元とする 1433/TCP へのアクセスは、一日・1IP アドレス当たり、28.3 件で、中国全体の 36.5%を占めているが、前期と比較すると、8.7 件（23.5%）減少した。

米国からのアクセス件数は、4月及び5月に、8/ICMP の増加が見られた。これは、複数の研究機関や大学からのアクセスであった。また、6月下旬のアクセス件数の増加は、特定のIPアドレスから15338/TCP及び15888/TCPを発信元とするアクセスが見られたためであるが、その目的は不明である。

台湾からは、前期に引き続き、445/TCP へのアクセスを多数観測しており、23/TCP へのアクセスが 445/TCP に次いで多い。また、135/TCP へのアクセス件数がやや増加した。

日本国内からのアクセスは、前期に引き続き、445/TCP 及び 135/TCP へのアクセスの割合が多数を占めた。また、4月中旬及び6月上旬に 8/ICMP の増加が見られた。これは、特定の研究機関からのアクセスによるものであった。

ロシアからのアクセス件数は、前期末から4月中旬までの間と5月中旬から6月初旬の間に、多数のUDPポートに対するアクセスが増加した（図2-15）。これは、通信内容の特徴から、特定のファイル共有ソフトによるアクセスの可能性がある。

表 2-4 発信元国・地域別検知件数(今期順位)

今期順位	前期順位	国・地域	今期件数[1]	前期比[1]
1 位	1 位	中国	77.43 件	−32.0% （−36.44 件）
2 位	2 位	米国	30.99 件	＋4.7% （＋1.38 件）
3 位	3 位	台湾	11.02 件	−16.5% （−2.18 件）
4 位	6 位	日本	10.37 件	＋1.4% （＋0.14 件）
5 位	5 位	ロシア	10.13 件	−8.1% （−0.89 件）

表 2-5 発信元国・地域別検知件数(増加順位)

増加順位	国・地域	今期件数[1]	前期比[1]	今期順位	前期順位
1 位	米国	30.99 件	＋4.7% （＋1.38 件）	2 位	2 位
2 位	ブラジル	7.49 件	＋12.4% （＋0.83 件）	6 位	7 位
3 位	インド	5.44 件	＋11.5% （＋0.56 件）	8 位	8 位
4 位	イラン	1.85 件	＋28.1% （＋0.41 件）	24 位	26 位
5 位	ドイツ	4.34 件	＋9.9% （＋0.39 件）	9 位	9 位

表 2-6 発信元国・地域別検知件数(減少順位)

減少順位	国・地域	今期件数[1]	前期比[1]	今期順位	前期順位
1 位	中国	77.43 件	−32.0% （−36.44 件）	1 位	1 位
2 位	韓国	5.89 件	−49.9% （−5.86 件）	7 位	4 位
3 位	台湾	11.02 件	−16.5% （−2.18 件）	3 位	3 位
4 位	欧州連合	1.58 件	−41.8% （−1.13 件）	26 位	14 位
5 位	ロシア	10.13 件	−8.1% （−0.89 件）	5 位	5 位

[1] 一日・1IP アドレス当たり。

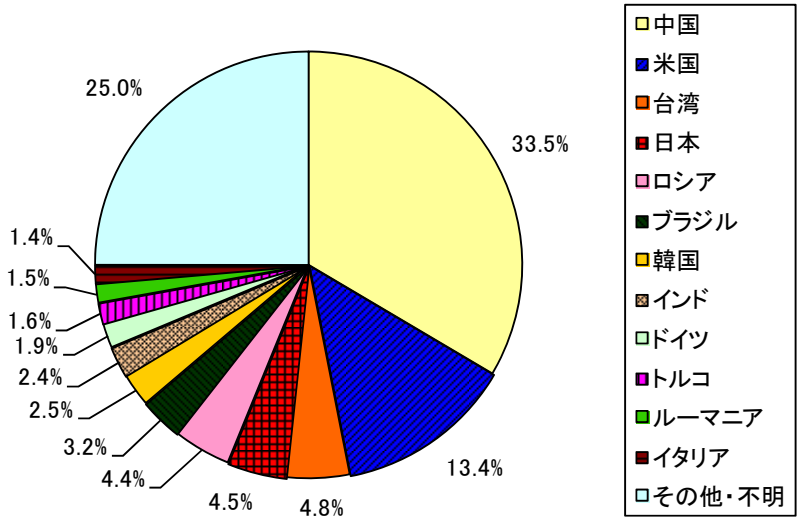

図 2-9　発信元国・地域別比率[1]

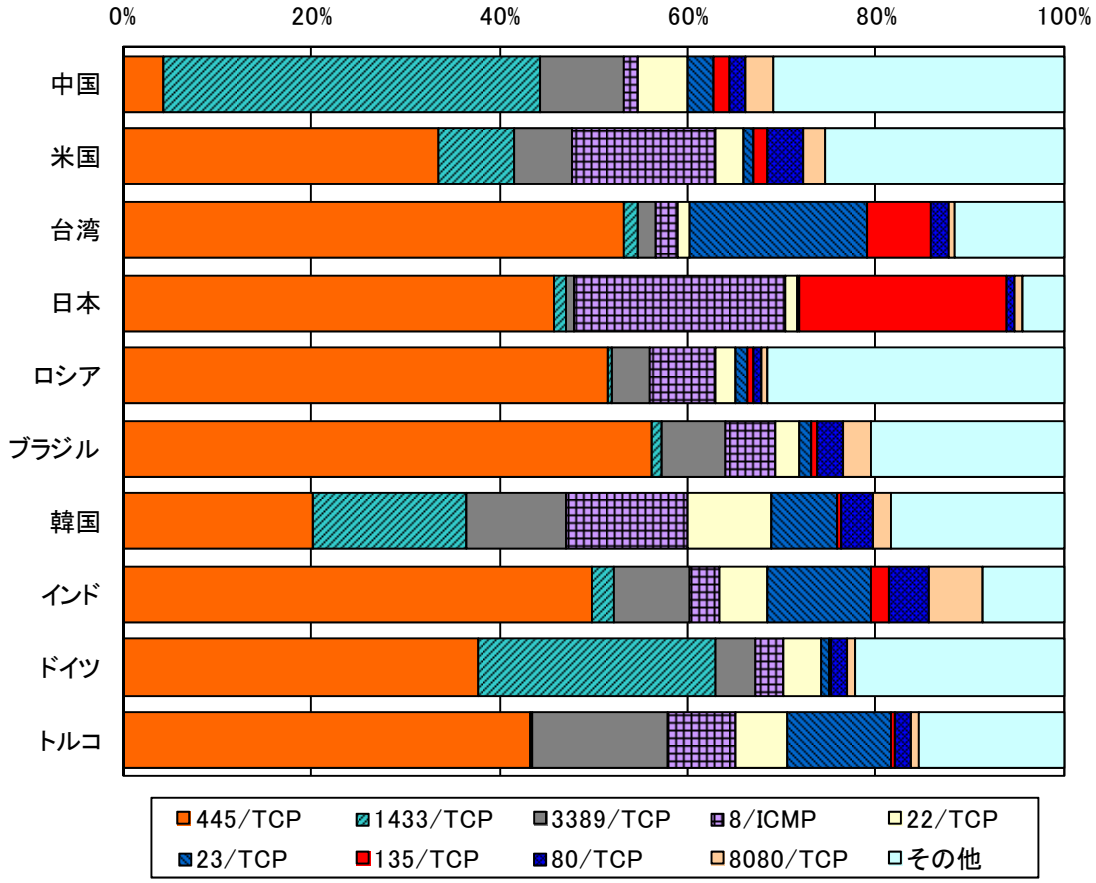

図 2-10　発信元国・地域別上位の宛先ポート別比率

[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。

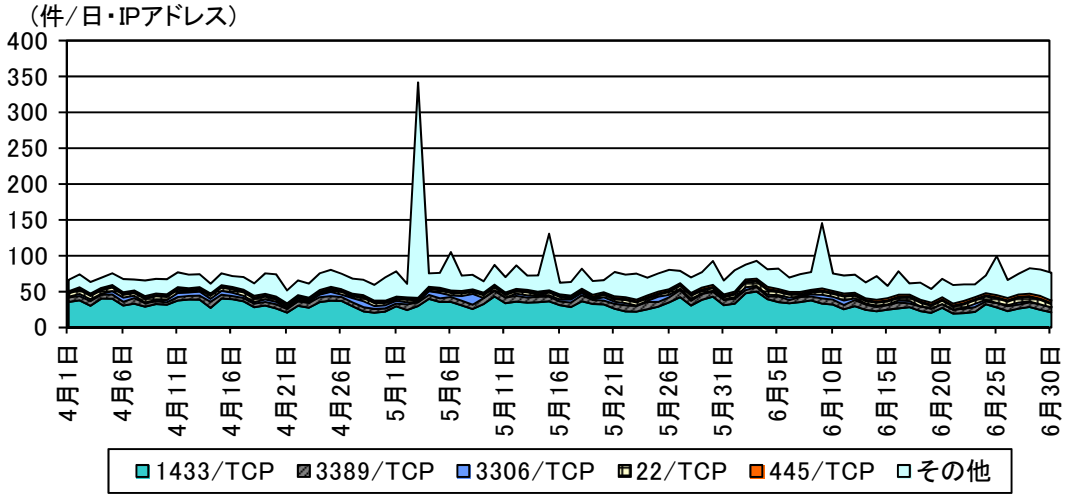

図 2-11　中国からのアクセス件数の推移

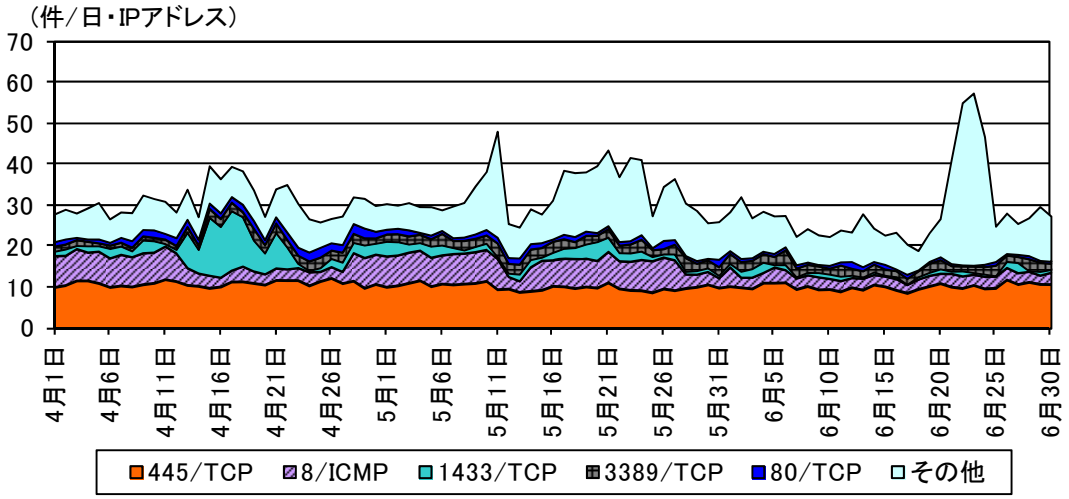

図 2-12　米国からのアクセス件数の推移

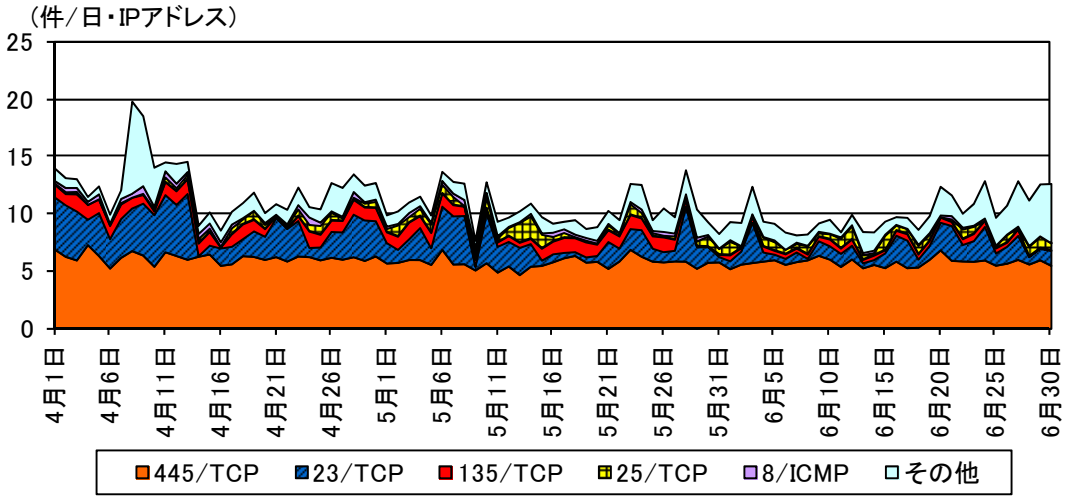

図 2-13　台湾からのアクセス件数の推移

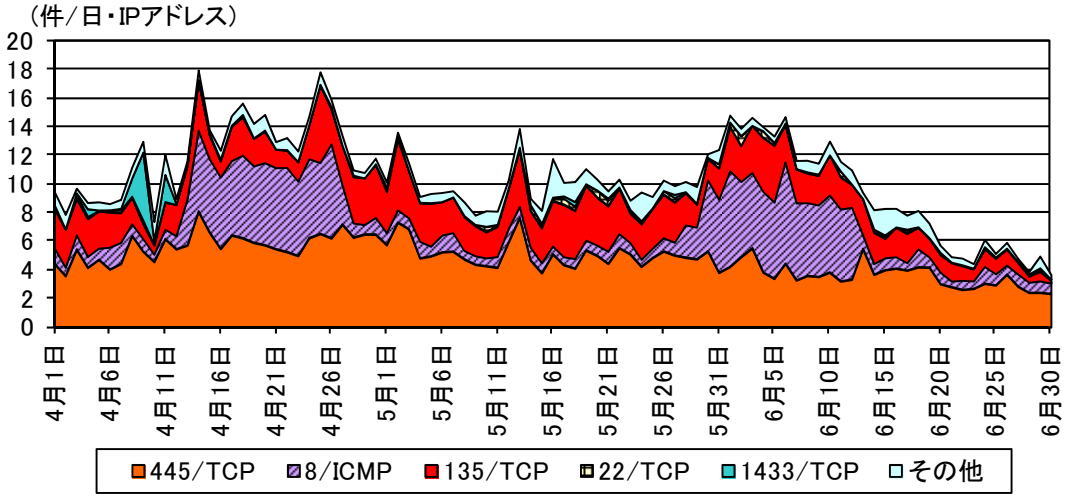

図 2-14　日本からのアクセス件数の推移

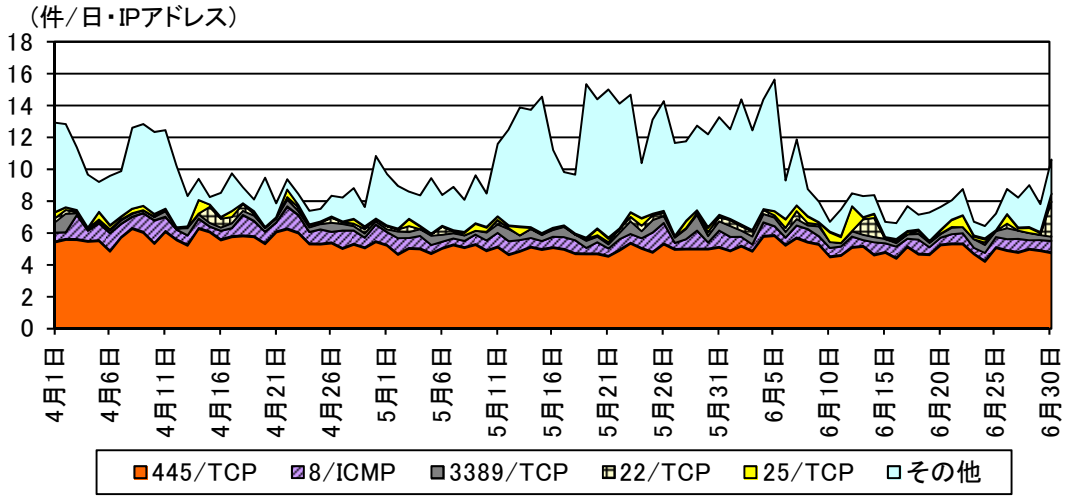

図 2-15　ロシアからのアクセス件数の推移

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

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「Scan」、「VoIP」、「Worm」、「Scan(P2P)」、「DNS」の順であり、この5分類で全体の 98.5%を占めている(図 3-2)。

「Scan」の検知件数は、一日・1IP アドレス当たり 4.8 件で、前期と比較して 2.5 件(111.7%)増加した(表 3-1)。「Scan」として検出したものは、プロキシサーバを探索する通信が全体の 97.7%を占めている。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ものと考えられ、中国からの通信が約半数となっており、増加傾向にある。

「VoIP」は、VoIP/SIP 機器を探索する通信であり、検知件数は一日・1IP アドレス当たり 2.2 件で、前期と比較して横ばいであった(表 3-1)。

「Worm」の検知件数は、一日・1IP アドレス当たり 0.8 件で、前期と比較して 1.1 件(58.2%)減少した(表 3-1)。発信元国・地域別で見ると、中国からの検知件数が一日・1IP アドレス当たり 0.1 件で、前期と比較して 0.8 件(90.2%)減少した。

「Scan(P2P)」の検知件数は、一日・1IP アドレス当たり 0.3 件で、前期と比較して 0.1 件(26.1%)減少した(表 3-1)。ロシアからの通信が 22.5%を占めた(図 3-4)ほか、ポーランドを発信元とする通信が4月下旬に一時的に増加した。

「DNS」 の検知件数は、一日・1IP アドレス当たり 0.2 件で、前期と比較して横ばいであった(表 3-1)。英国、オランダ及び米国からの通信が全体の 86.1%となっており、これら3カ国からの通信は、5月下旬から6月下旬の間に一時的に増加したものである。

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[1]	前期比[1]	増加順位	減少順位
1 位	1 位	Scan	4.76 件	＋111.7%　(＋2.51 件)	1 位	
2 位	2 位	VoIP	2.24 件	＋3.5%　(＋0.08 件)	3 位	
3 位	3 位	Worm	0.77 件	－58.2%　(－1.07 件)		1 位
4 位	4 位	Scan(P2P)	0.32 件	－26.1%　(－0.11 件)		2 位
5 位	5 位	DNS	0.16 件	＋7.4%　(＋0.01 件)	4 位	

[1] 一日・1IP アドレス当たり。

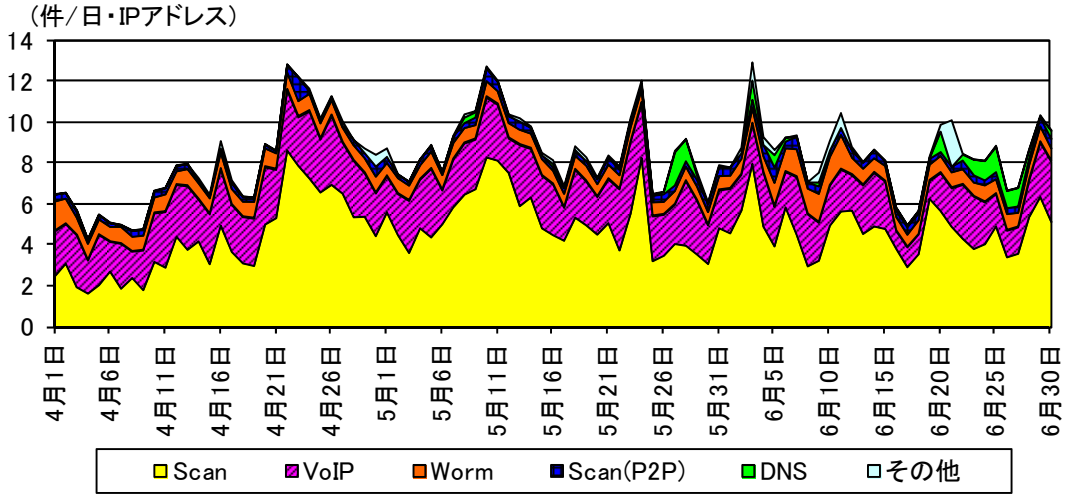

図 3-1　シグネチャを用いた不正侵入等の攻撃手法別検知件数の推移

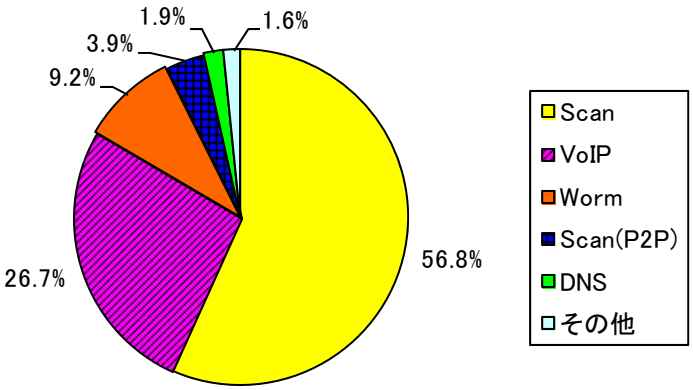

図 3-2　シグネチャを用いた不正侵入等の攻撃手法別検知比率[1]

[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。

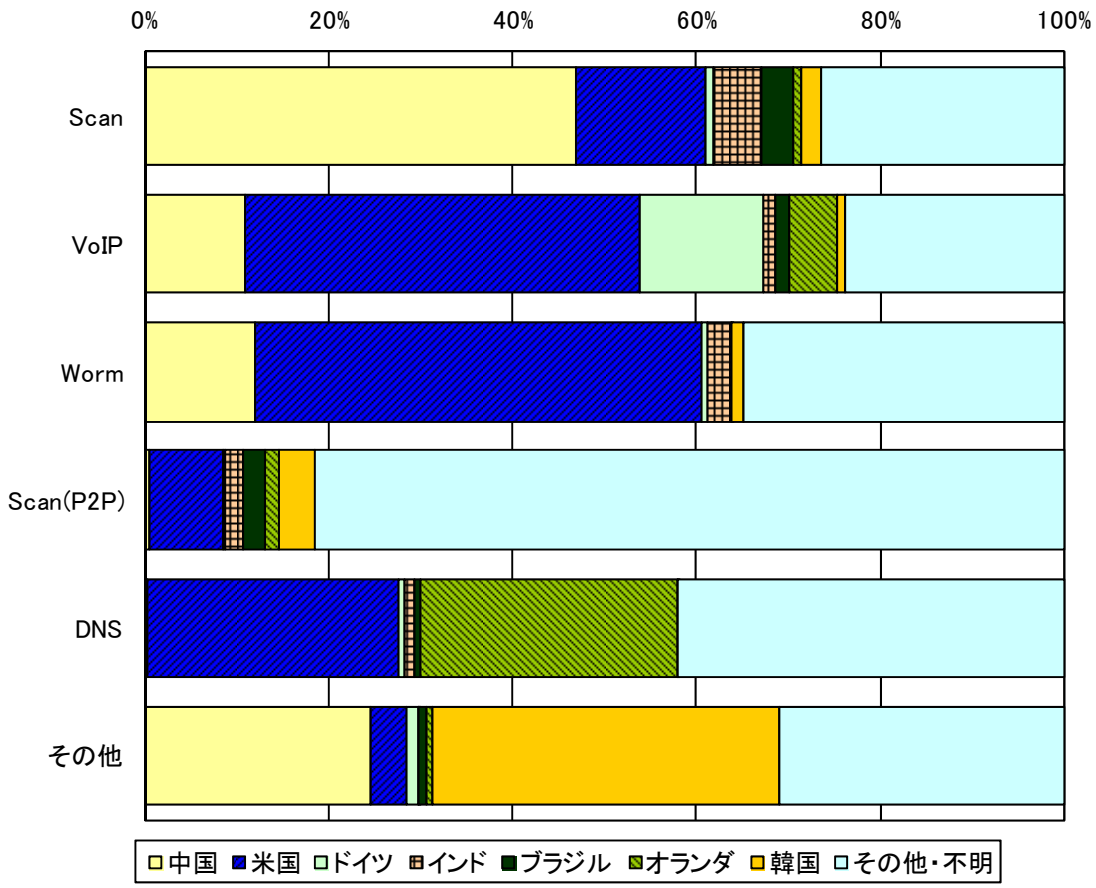

図 3-3　シグネチャを用いた不正侵入等の攻撃手法の国・地域別検知比率

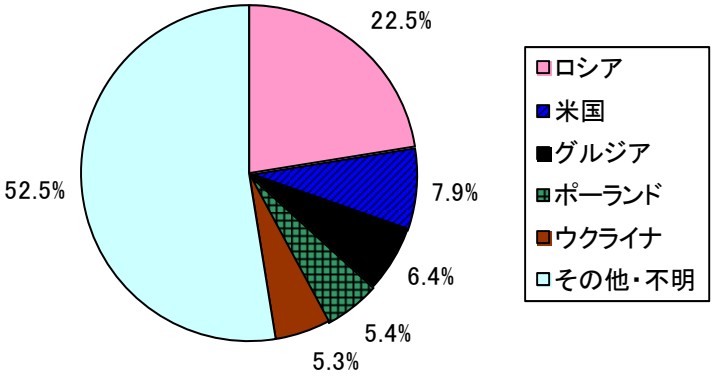

図 3-4　シグネチャ「Scan(P2P)」の国・地域別検知比率[1]

[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。

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、ドイツ、インド、ブラジルの順であった。

中国を発信元とする検知件数は、一日・1IP アドレス当たり 2.6 件で、前期と比較して 0.5 件(23.4%)増加した(表 3-2)。中国からのアクセスを攻撃手法別で見ると、「Scan」の検知件数が、前期と比較して 1.4 件(160.8%)増加しており、最も多く検知している。また、「Worm」の検知件数が、前期と比較して 0.8 件(90.2%)減少している。

今期2位の米国は、「Scan」の検知件数が、前期と比較して、一日・1IP アドレス当たり 0.4 件(131.7%)増加した。「VoIP」の検知件数については、前期と比較して横ばいであるが、全体の 42.8%と高い割合を占めた。

今期4位のインドは、「Scan」の検知件数が増加しており、前期と比較して、一日・1IP アドレス当たり 0.2 件(316.7%)増加した。その多くは、プロキシサーバの探索とみられる通信であり、6月上旬に一時的に増加したものである。

今期5位のブラジルは、「Scan」の検知件数が前期と比較して、0.1 件(105.0%)増加した。4月中旬に増加し、その後増減を繰り返しながら徐々に減少傾向にある。

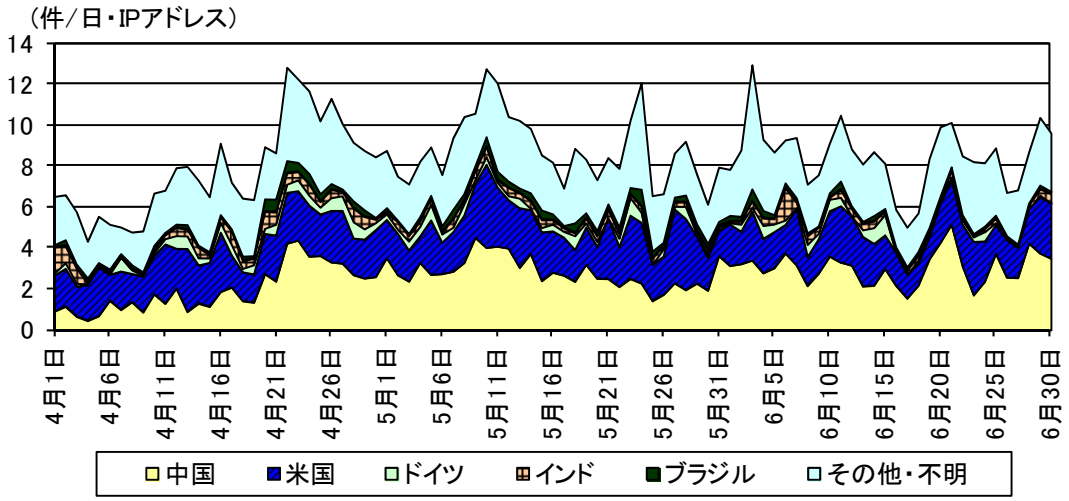

図 3-5　シグネチャを用いた不正侵入等の発信元国・地域別検知件数の推移

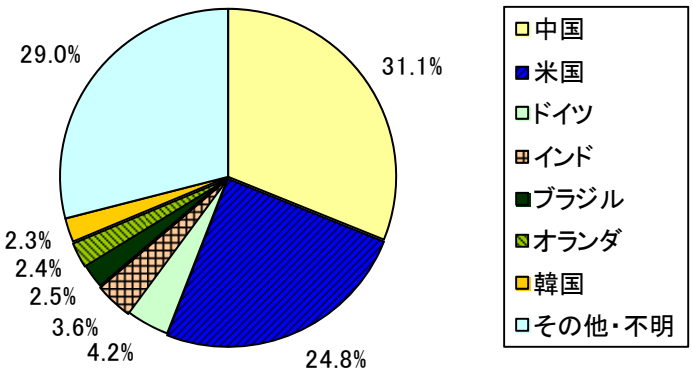

図 3-6 シグネチャを用いた不正侵入等の発信元国・地域別検知比率[1]

[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)

今期順位	前期順位	国・地域	今期件数[1]	前期比[1]
1 位	1 位	中国	2.61 件	＋23.4% （＋0.49 件）
2 位	2 位	米国	2.08 件	＋13.7% （＋0.25 件）
3 位	3 位	ドイツ	0.35 件	＋5.3% （＋0.02 件）
4 位	11 位	インド	0.31 件	＋197.3% （＋0.20 件）
5 位	13 位	ブラジル	0.21 件	＋119.3% （＋0.11 件）

表 3-3 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(増加順位)

増加順位	国・地域	今期件数[1]	前期比[1]	今期順位	前期順位
1 位	中国	2.61 件	＋23.4% （＋0.49 件）	1 位	1 位
2 位	米国	2.08 件	＋13.7% （＋0.25 件）	2 位	2 位
3 位	インド	0.31 件	＋197.3% （＋0.20 件）	4 位	11 位
4 位	ブラジル	0.21 件	＋119.3% （＋0.11 件）	5 位	13 位
5 位	トルコ	0.07 件	＋609.7% （＋0.06 件）	16 位	45 位

表 3-4 シグネチャを用いた不正侵入等の発信元国・地域別検知件数(減少順位)

減少順位	国・地域	今期件数[1]	前期比[1]	今期順位	前期順位
1 位	台湾	0.10 件	－57.4% （－0.13 件）	12 位	5 位
2 位	英国	0.19 件	－36.6% （－0.11 件）	8 位	4 位
3 位	欧州連合	0.06 件	－52.4% （－0.07 件）	20 位	10 位
4 位	香港	0.05 件	－43.2% （－0.04 件）	23 位	14 位
5 位	ウクライナ	0.08 件	－16.4% （－0.02 件）	14 位	12 位

[1] 一日・1IP アドレス当たり。

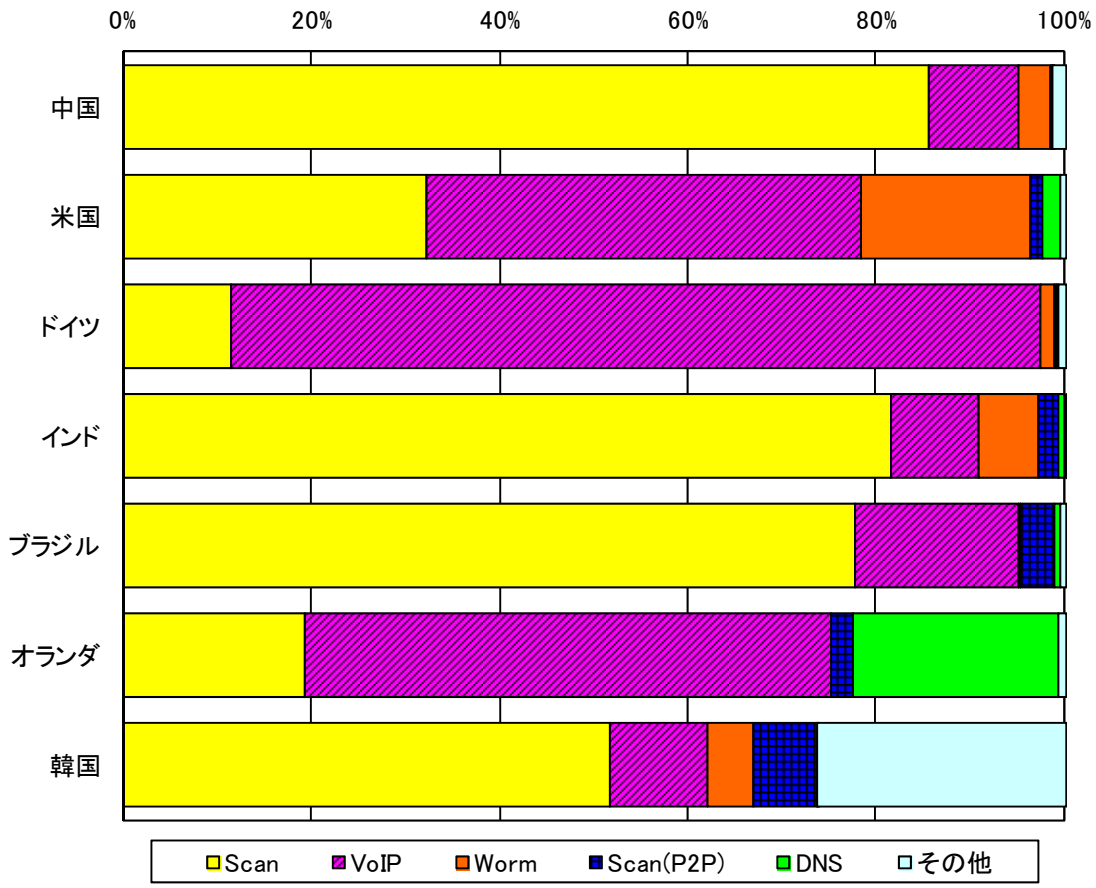

図 3-7　シグネチャを用いた不正侵入等の発信元国・地域別上位の攻撃手法別検知比率

4　インターネット定点観測 ― DoS 攻撃被害観測状況

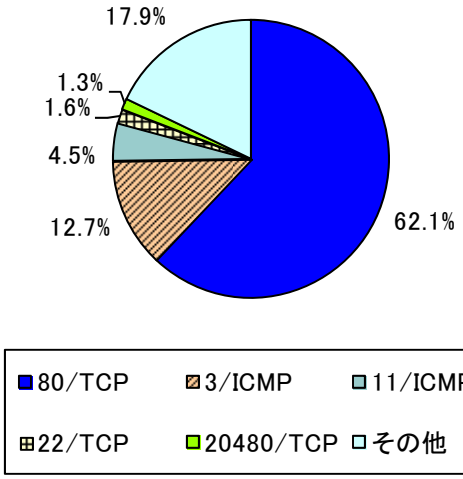

図 4-1　跳ね返りパケット発信元ポート別比率 [1]

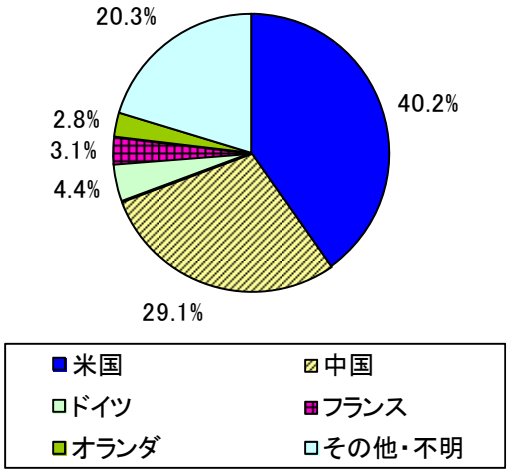

図 4-2　跳ね返りパケット発信元国・地域別比率 [1]

DoS 攻撃被害観測状況は、一日当たり 8,806.8 件で、前期と比較して 2,370.4 件(36.8%)増加した。発信元 IP アドレス数は一日当たり 515.7 個で、前期と比較して 125.2 個(32.1%)増加した。

前期に引き続き 80/TCPを発信元とする跳ね返りパケットを多数検知しており、全体の 62.1%を占めた(図 4-1)。検知件数は、一日当たり 5,465.6 件で、前期と比較して一日当たり 1,189.9 件(27.8%)増加した。前期と同様に米国からの跳ね返りパケットを最も多く検知しており、前期と比較して、一日当たり 541.1 件(25.4%)増加した(表 4-1)。これは、4月上旬から中旬にかけて、特定の IP アドレスから多くの跳ね返りパケットが見られたためである(図 4-3)。また、中国からの 80/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 231.2 件(22.8%)増加した。これは、中国から4月と6月に、それぞれ異なる IP アドレスからの跳ね返りパケットを毎日一定の件数を検知する状況が続いたためである。

今期2位の ICMP Destination Unreachable(以下「3/ICMP」という。)の検知件数は、一日当たり 1,118.6 件で、前期と比較して 814.8 件(268.2%)増加した。これは、6月上旬に中国を発信元とする多数の IP アドレスからの跳ね返りパケットを一時的に検知したためであり、中国の何らかのサーバに対して攻撃が行われていた可能性がある(図 4-4)。

[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 4-1　80/TCP からの跳ね返りパケットの発信元国・地域別検知件数（今期順位）

今期順位	前期順位	国・地域	今期件数[1]	前期比[1]	
1 位	1 位	米国	2,669.2 件	＋25.4%	（＋541.1 件）
2 位	2 位	中国	1,245.4 件	＋22.8%	（＋231.2 件）
3 位	4 位	ドイツ	244.8 件	＋55.3%	（＋87.1 件）
4 位	6 位	トルコ	173.0 件	＋98.8%	（＋86.0 件）
5 位	3 位	オランダ	160.6 件	－26.8%	（－58.7 件）

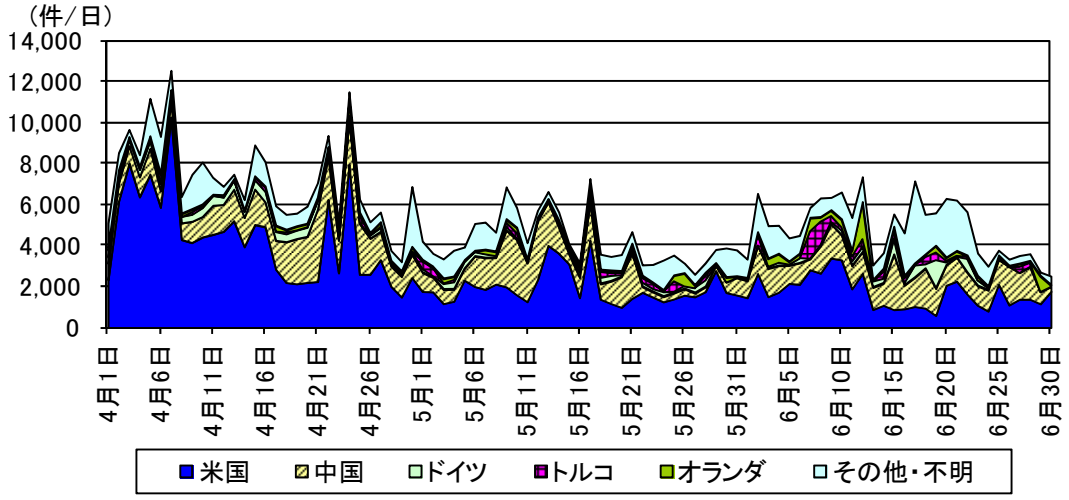

図 4-3　発信元ポート 80/TCP からの跳ね返りパケットの推移

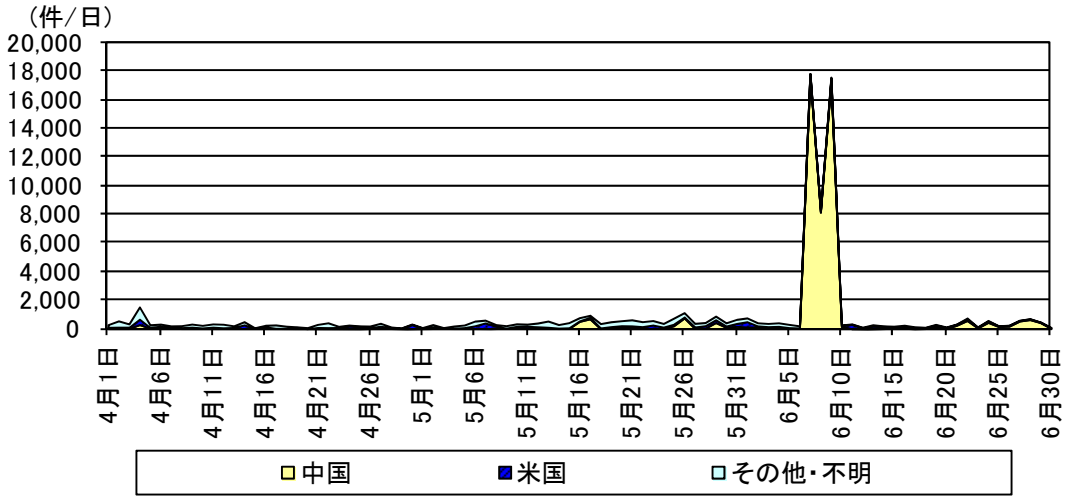

図 4-4　 3/ICMP のアクセス件数の推移

[1] 一日当たり。

5　@police　（Topics）掲載事項

@police において、平成24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(MS12-023,024,025,026,027,028)
重要	4月11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24日	ジャストシステム社製品の脆弱性について
重要	5月5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
重要	5月9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(MS12-029,030,031,032,033,034,035)
●	5月15日	インターネット治安情勢更新(平成23年度第4四半期報を追加)
重要	6月9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
重要	6月13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(MS12-036,037,038,039,040,041,042)

凡例

重要　：　セキュリティ対策上の重要事項

●　：　セキュリティ対策上の参考事項

6　集計方法

警察庁では、インターネット定点観測システムにより、全国のインターネット接続点におけるアクセス情報等を観測・分析している。各観測結果の集計については、次のとおり行った。

6-1　パケットの表記

TCP 及び UDP はポートごとに集計し、スラッシュの前にポート番号を付けて表している。（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、スラッシュの前にタイプ番号を付けて表している。（例 「8/ICMP」は ICMP Echo Request を表す。）

6-2　パケットの分類

インターネット定点観測システムが検知したパケットの分類は、表 6-1 に示す分類に従って集計している。DoS 攻撃被害観測システムでは、集計対象とするパケットとして、SYN/ACK 及び RST/ACK パケットに加えて、ICMP Echo Reply（以下、「0/ICMP」という。）、3/ICMP 及び ICMP Time Exceeded（以下、「11/ICMP」という。）を集計対象としている。

表 6-1　パケットの分類

章	集計対象	
2　インターネット定点観測 ― センサーに対するアクセス	センサーに対するアクセス	● TCP SYN パケット ● UDP による問い合わせパケット等 ● 8/ICMP
	目的が不明なパケット	● その他
4　インターネット定点観測 ― DoS 攻撃被害観測状況	SYN flood 攻撃による跳ね返りパケット	● TCP SYN/ACK ● TCP RST/ACK
	PING flood 攻撃による跳ね返りパケット	● 0/ICMP
	各種の flood 攻撃による跳ね返りパケット	● 3/ICMP ● 11/ICMP

6-3　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 24 年6月 30 日現在、シグネチャは 3,131 種類が登録されている。検知された各シグネチャは、表 6-2 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 6-2　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
VoIP	SIP message detected, SIP long host name detected
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
ICMP	ICMP time stamp request
Others	Traceroute, ISAKMP Vendor ID