平成 24 年 11 月 14 日

インターネット観測結果等

（平成 24 年度第2／四半期（7月～9月））

・3389/TCP へのアクセスが前期に引き続き増加
・中国及び韓国を発信元とする SQL Slammer が増加
・80/TCP を発信元とする跳ね返りパケットが減少

1　第2／四半期における状況

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 282.8 件で、平成 24年度第1／四半期（以下「前期」という。）と比較して 51.7 件（22.4%）増加した。また、発信元 IP アドレス数は一日当たり 10,993.9 個で、前期と比較して 2,637.4 個（31.6%）増加した。

宛先ポート別検知件数は、445/TCP が最も多く、次いで 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 2／四半期（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 11.0%増加した（表 2-1）。このアクセスには、ツールによる探索や Morto ワームの感染活動によるアクセスが含まれていると考えられる。

発信元国・地域別検知件数は、中国が最も多く、次いで米国、台湾、日本、韓国の順であった（表 2-4）。

1-2　中国及び韓国を発信元とする SQL Slammer が増加

シグネチャを用いて検知した不正侵入等の行為（以下「不正侵入等」という。）の件数は、一日・1IP アドレス当たり 9.5 件で、前期と比較して 1.2 件（13.8%）増加した。また、発信元 IP アドレス数は一日当たり 363.8 個で、前期と比較して 48.7 個（15.4%）増加した。

「Worm」に分類される SQL Slammer は、7月下旬から 9 月中旬にかけて中国の特定の IP アドレスを発信元とする検知件数が増加した。また、9 月中旬以降は韓国の特定の IP アドレスを発信元とする検知件数が増加した。

1-3　80/TCP を発信元とする跳ね返りパケットが減少

DoS 攻撃被害観測状況は、一日当たり 4,449.3 件で、前期と比較して 4,357.5 件（49.5%）減少した。発信元 IP アドレス数は一日当たり 382.5 個で、前期と比較して 133.2 個（25.8%）減少した。

80/TCP からの跳ね返りパケット検知件数が前期と比較して一日当たり 2,782.3 件(50.9%)減少した。これは、4月に多数検知していた米国を発信元とする特定の IP アドレスからの跳ね返りパケットが見られなくなったことが主な要因である。また、検知件数上位の ICMP Destination Unreachable(以下「3/ICMP」という。)及び ICMP Time Exceeded(以下「11/ICMP」という。)も前期と比較して減少した（表 4-1）。

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 は、Windows ファイル共有等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）。このアクセスは、Windows 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。

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 15.6%増加した。9 月中旬以降、特定の IP アドレスからのアクセスが継続して行われていたことが増加の原因と考えられ、アクセス件数の 85.8%は中国からのものである。また、発信元ポートに偏りが見られ、6000/TCP の割合が 90.2%を占めている。これは、何らかのツールを使用して、マイクロソフト社製データベース製品が稼働しているコンピュータを探索している可能性がある（図 2-5）。

3389/TCP は、Windows リモートデスクトップ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、11.0%増加した。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るため、ツールによる探索であると考えられる。また、Windows リモートデスクトップを使用して感染を拡大する Morto ワームの感染活動によるアクセスも含まれていると考えられる（図 2-6）。

8/ICMP は、ping 等のネットワーク診断で使用されるが、ワームによる感染対象の探索にも悪用されている可能性がある。アクセス件数は、前期と比較して 28.8%減少したが、これは、前期までに多く観測されていた、複数の研究機関や大学からのネットワーク調査と考えられるアクセスが見られなくなったためである（図 2-7）。

22/TCP は、SSH サービス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 4.6%増加した（図 2-8）。この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。

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	76.79 件	−4.0% （−3.17 件）
2 位	2 位	1433/TCP	43.68 件	＋15.6% （＋5.91 件）
3 位	3 位	3389/TCP	17.59 件	＋11.0% （＋1.75 件）
4 位	4 位	8/ICMP	10.36 件	−28.8% （−4.18 件）
5 位	5 位	22/TCP	9.38 件	＋4.6% （＋0.41 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	1433/TCP	43.68 件	＋15.6% （＋5.91 件）	2 位	2 位
2 位	3389/TCP	17.59 件	＋11.0% （＋1.75 件）	3 位	3 位
3 位	2025/UDP	1.33 件	−[2] （＋1.33 件）	20 位	−
4 位	39455/UDP	1.98 件	＋200.4% （＋1.32 件）	15 位	27 位
5 位	23/TCP	9.09 件	＋15.2% （＋1.20 件）	6 位	6 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	8/ICMP	10.36 件	−28.8% （−4.18 件）	4 位	4 位
2 位	445/TCP	76.79 件	−4.0% （−3.17 件）	1 位	1 位
3 位	557/UDP	検知なし	−[3] （−3.01 件）	−	11 位
4 位	80/TCP	4.31 件	−19.9% （−1.07 件）	10 位	8 位
5 位	27507/UDP	検知なし	−[3] （−0.68 件）	−	26 位

[1] 一日・1IP アドレス当たり。
[2] 前期の検知件数がごく僅かであるため、前期比率は記載していない。
[3] 今期の検知件数が 0 件であるため、前期比率は記載していない。

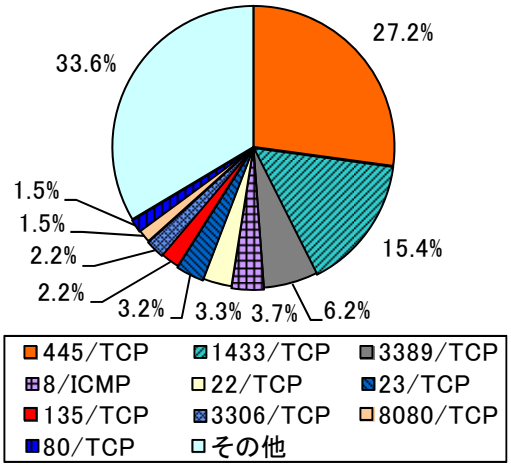

図 2-1　宛先ポート比率(全て)[1]

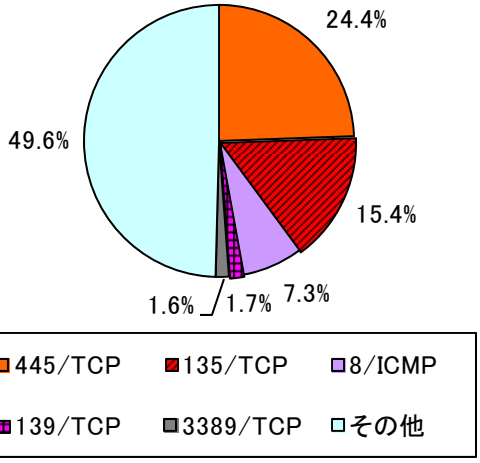

図 2-2　宛先ポート比率(日本国内)[1,2]

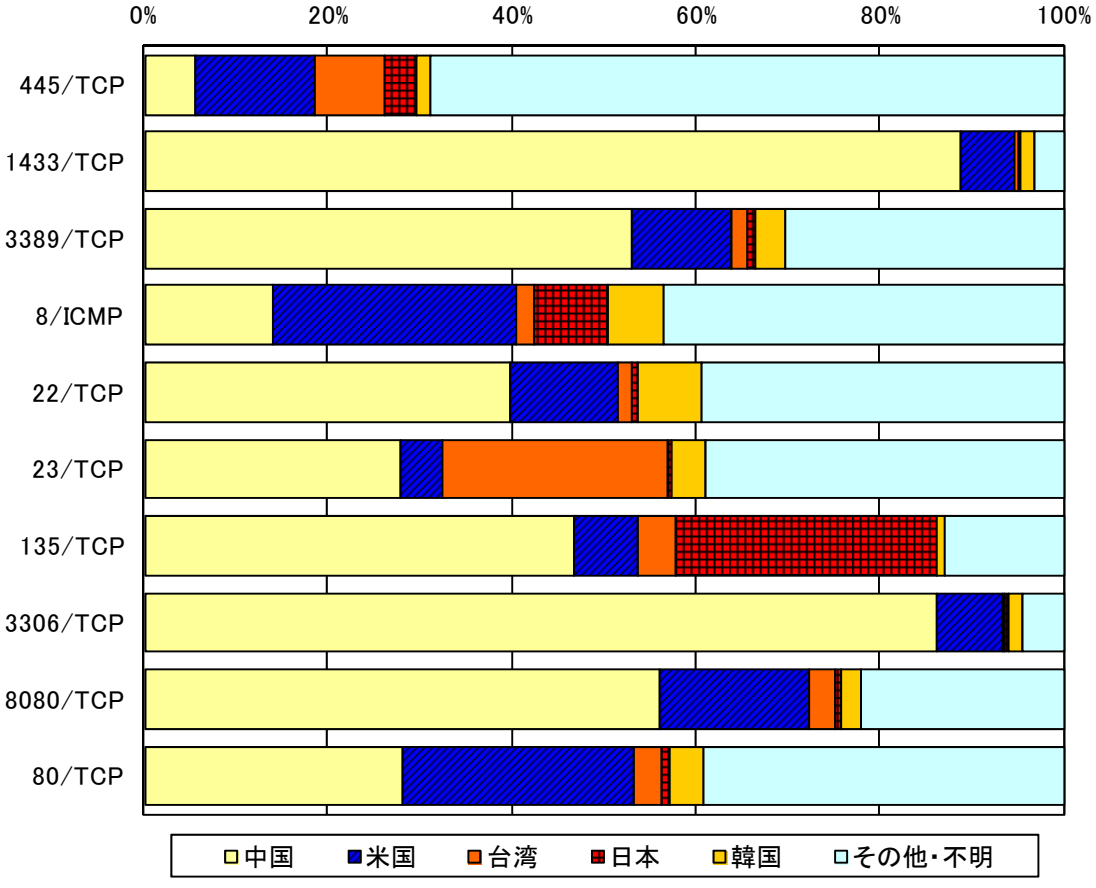

図 2-3　宛先ポート別上位の発信元国・地域別比率

[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。

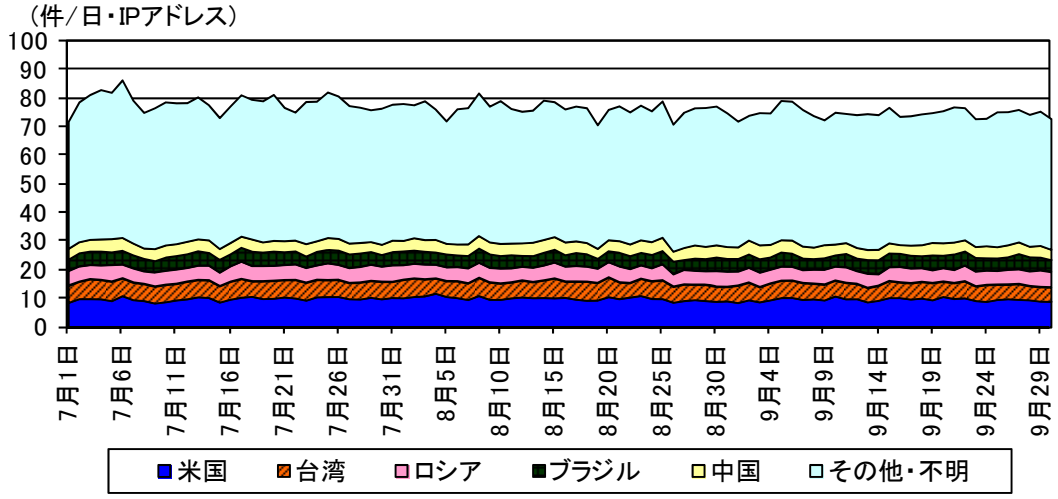

図 2-4　宛先ポート 445/TCP に対するアクセス件数の推移

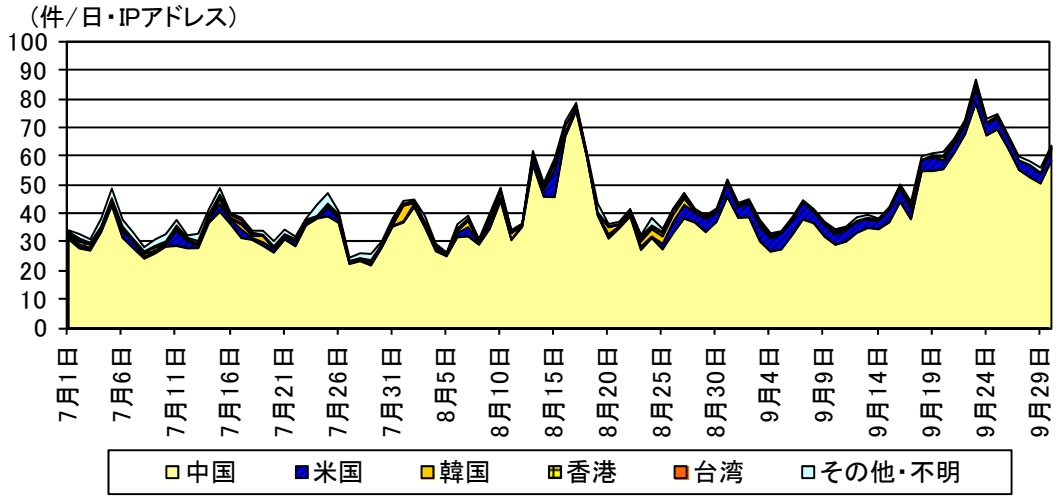

図 2-5　宛先ポート 1433/TCP に対するアクセス件数の推移

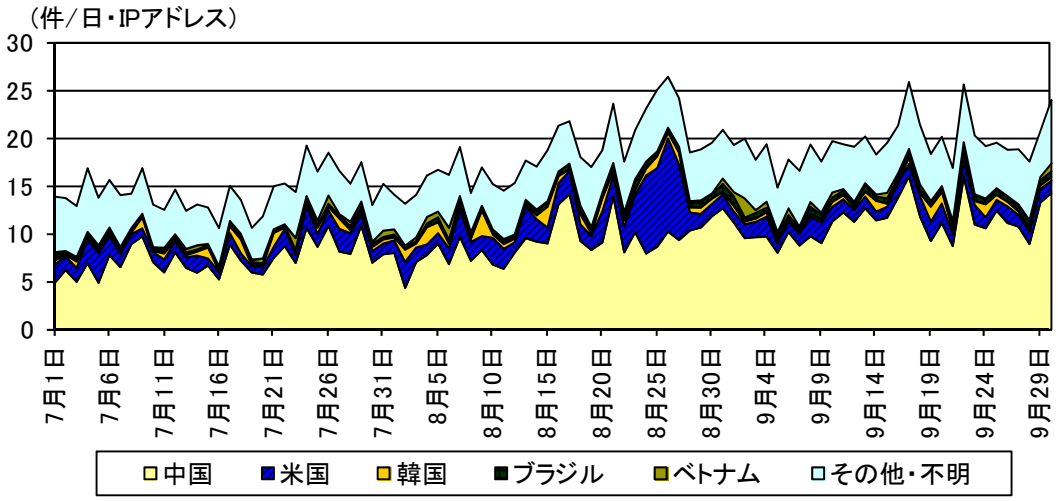

図 2-6　宛先ポート 3389/TCP に対するアクセス件数の推移

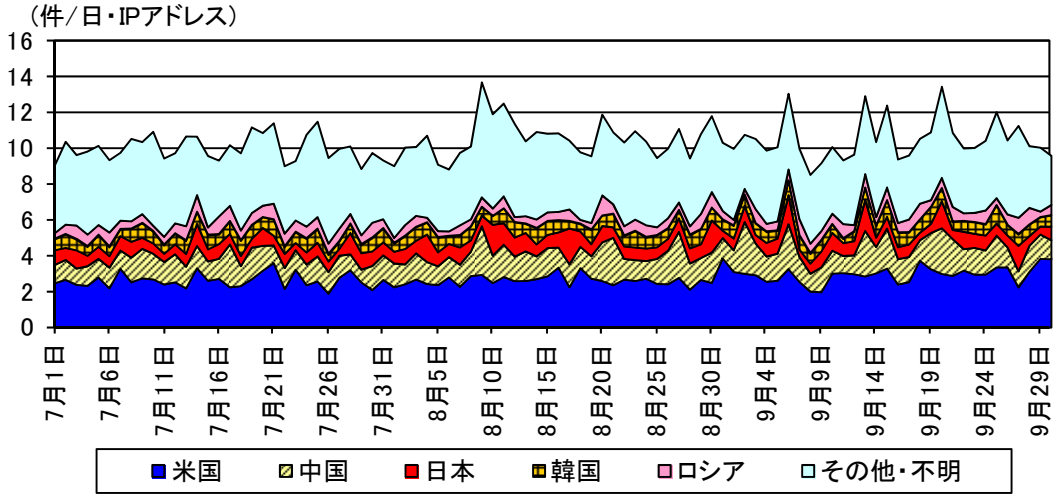

図 2-7　8/ICMP のアクセス件数の推移

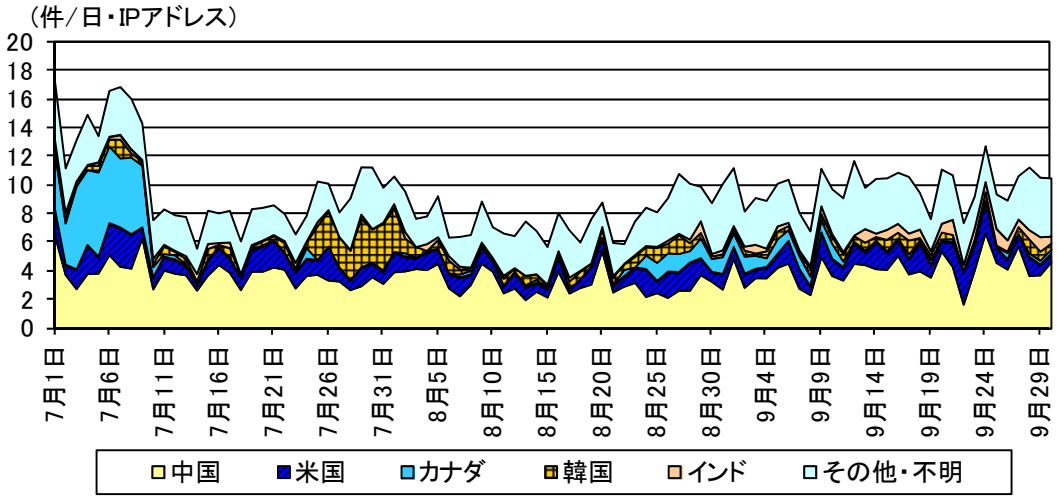

図 2-8　宛先ポート 22/TCP に対するアクセス件数の推移

2-2　発信元国・地域別[1]

中国からのアクセスは、前期と比較して 46.8%増加した。9月 11 日及び 12 日に 53/UDP を発信元とするアクセスが増加した。このアクセスは、DNS サーバへ名前解決の問い合わせを行った際に返される回答パケットであり、何者かが発信元 IP アドレスを詐称し、DNS サーバへ名前解決の問い合わせを行っていたと考えられる（図 2-11、図 2-12）。

米国からのアクセスは、前期と比較して 5.4%増加した。7月中旬頃から特定の IP アドレスを発信元としたネットワーク調査と考えられるアクセスが継続して行われている。この発信元からは、137/UDP、1900/UDP 等に対するアクセスが広範囲の IP アドレスに対して行われていると考えられる（図 2-13）。

台湾からのアクセスは、前期と比較して 34.5%増加した。9月中旬以降、TELNET で使用される 23/TCP に対するアクセスが増加した（図 2-14、図 2-15）。

日本国内からのアクセスは、前期と比較して 9.5%増加した。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ている（図 2-16、図 2-17）。

韓国からのアクセスは、前期と比較して 77.1%増加した。宛先ポート別で見ると「その他」の割合が増加している。（図 2-18、図 2-19）

今期は、多くの国・地域において、「その他」として分類されるアクセスが増加した。これは、6月下旬以降、主に日本、韓国及び台湾を発信元とする複数の IP アドレスから様々な宛先ポートに対するUDPパケットを観測したためである。これらのUDPパケットの一部には、ファイル共有ソフト「Bit Torrent」で使用される通信と考えられるものを確認しているが、その目的は不明である。また、全てのセンサーで観測されたことから、インターネット上の広範囲の IP アドレスに対して送信されている可能性がある。7月下旬にも、日本、韓国及び台湾のIPアドレスを発信元とする大量のUDPパケットを検知したが、このアクセスは、特定のセンサーへのアクセスであることから、前述のアクセスとの関連は不明である。（図 2-14、図 2-16、図 2-18）

1 発信元国・地域については、当該国・地域に割り当てられた IP アドレスを指している。以降同様の表記。

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	113.68 件	＋46.8% （＋36.25 件）
2 位	2 位	米国	32.68 件	＋5.4% （＋1.69 件）
3 位	3 位	台湾	14.82 件	＋34.5% （＋3.80 件）
4 位	4 位	日本	11.35 件	＋9.5% （＋0.98 件）
5 位	7 位	韓国	10.43 件	＋77.1% （＋4.54 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	中国	113.68 件	＋46.8% （＋36.25 件）	1 位	1 位
2 位	韓国	10.43 件	＋77.1% （＋4.54 件）	5 位	7 位
3 位	台湾	14.82 件	＋34.5% （＋3.80 件）	3 位	3 位
4 位	米国	32.68 件	＋5.4% （＋1.69 件）	2 位	2 位
5 位	ルーマニア	4.54 件	＋35.1% （＋1.18 件）	9 位	11 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	ロシア	8.53 件	－15.7% （－1.59 件）	7 位	5 位
2 位	欧州連合	0.04 件	－97.6% （－1.54 件）	108 位	26 位
3 位	ドイツ	3.32 件	－23.4% （－1.02 件）	11 位	9 位
4 位	チェコ	0.68 件	－37.3% （－0.40 件）	42 位	32 位
5 位	ウクライナ	1.97 件	－13.3% （－0.30 件）	23 位	15 位

[1] 一日・1IP アドレス当たり。

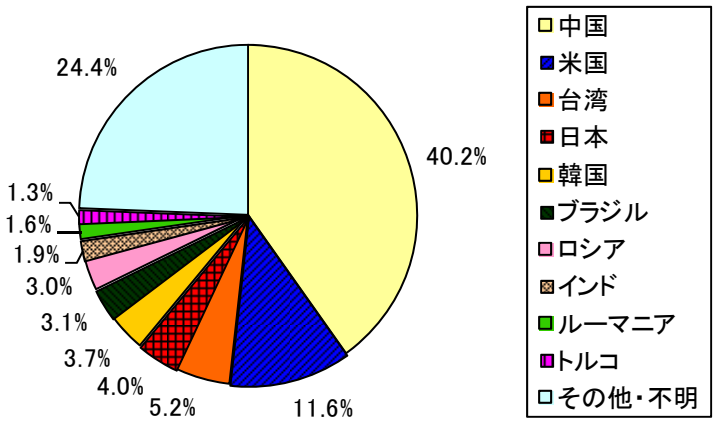

図 2-9　発信元国・地域別比率[1]

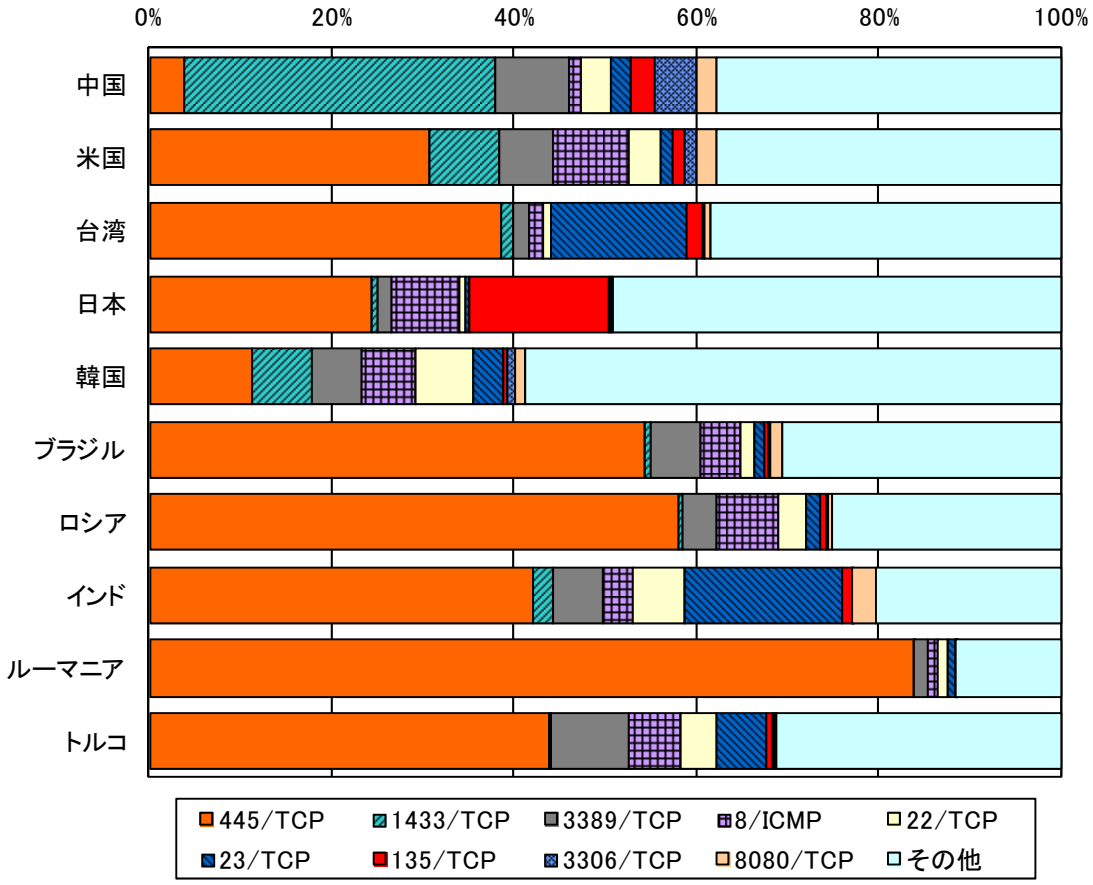

図 2-10　発信元国・地域別上位の宛先ポート別比率

[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。

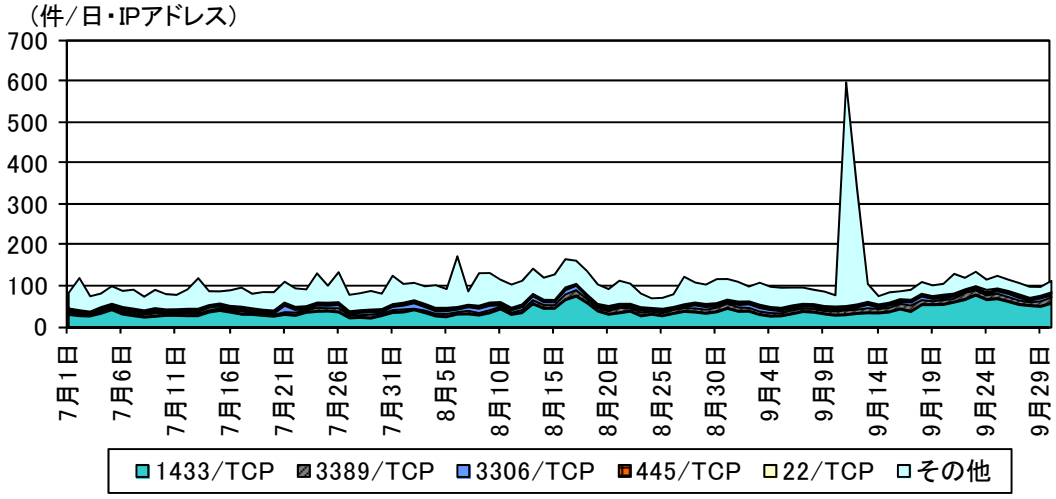

図 2-11　中国からのアクセス件数の推移

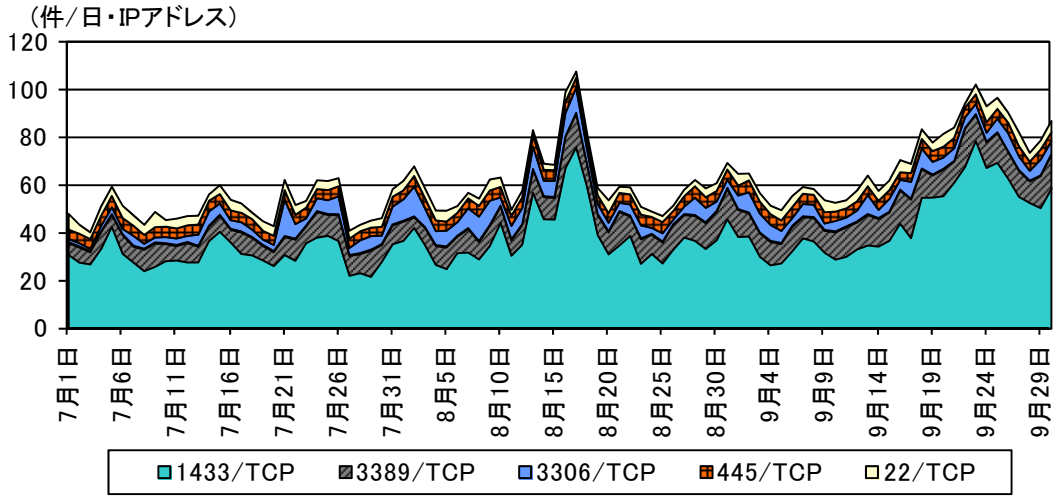

図 2-12　中国からのアクセス件数の推移（「その他」を除いたもの）

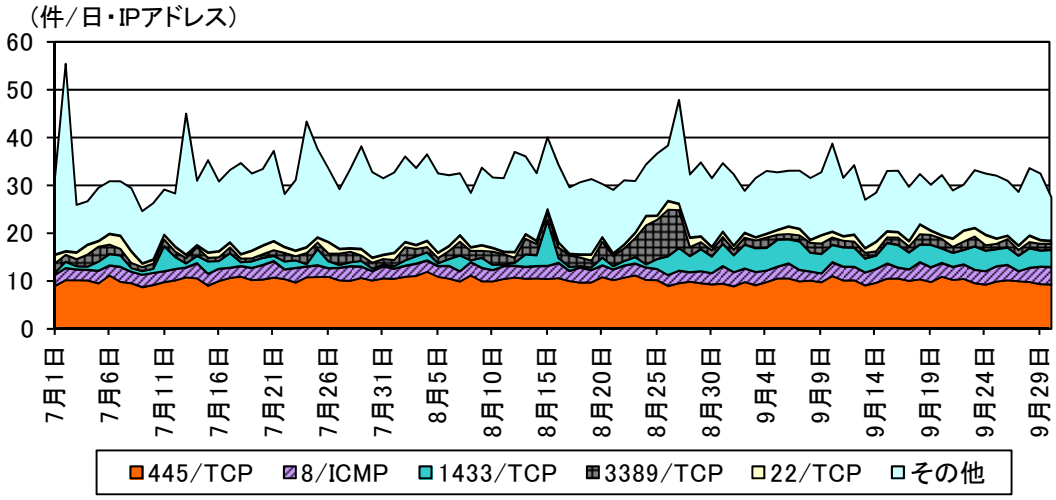

図 2-13　米国からのアクセス件数の推移

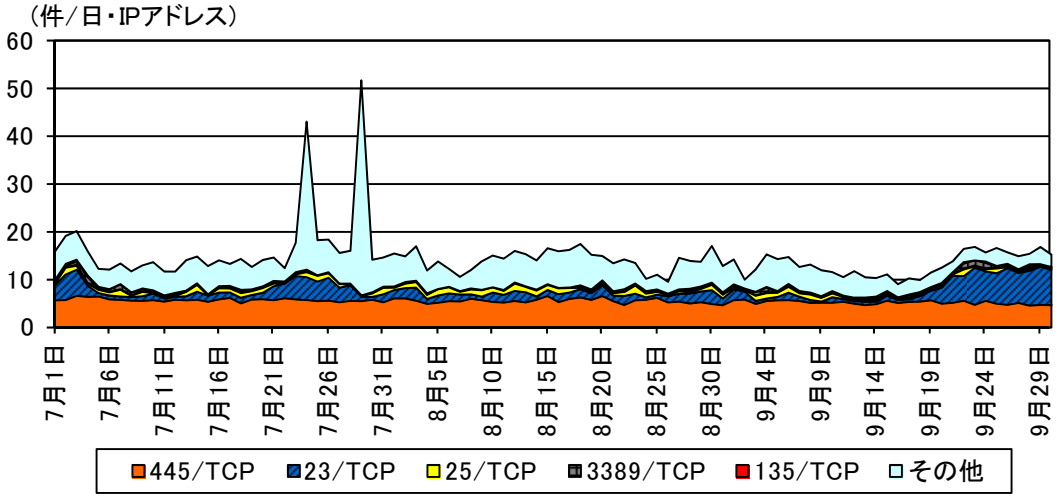

図 2-14　台湾からのアクセス件数の推移

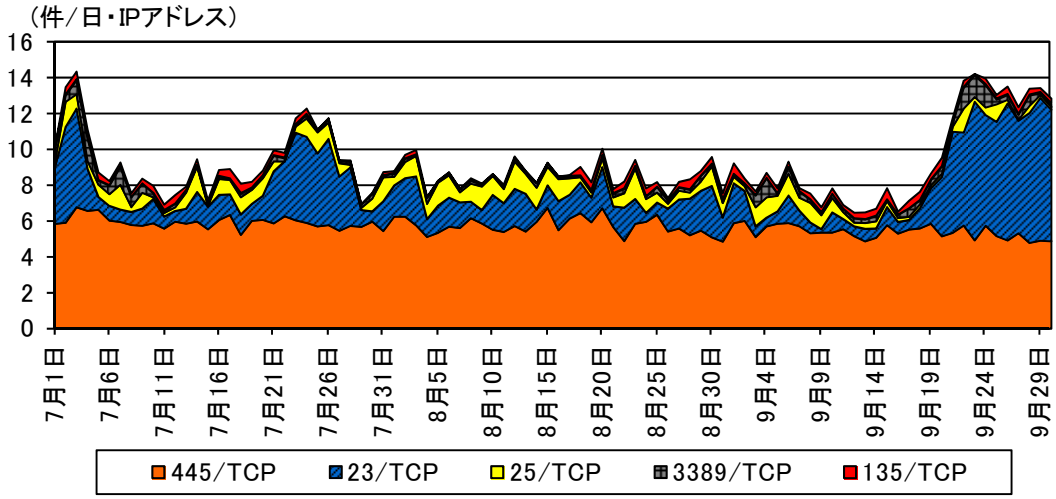

図 2-15　台湾からのアクセス件数の推移（「その他」を除いたもの）

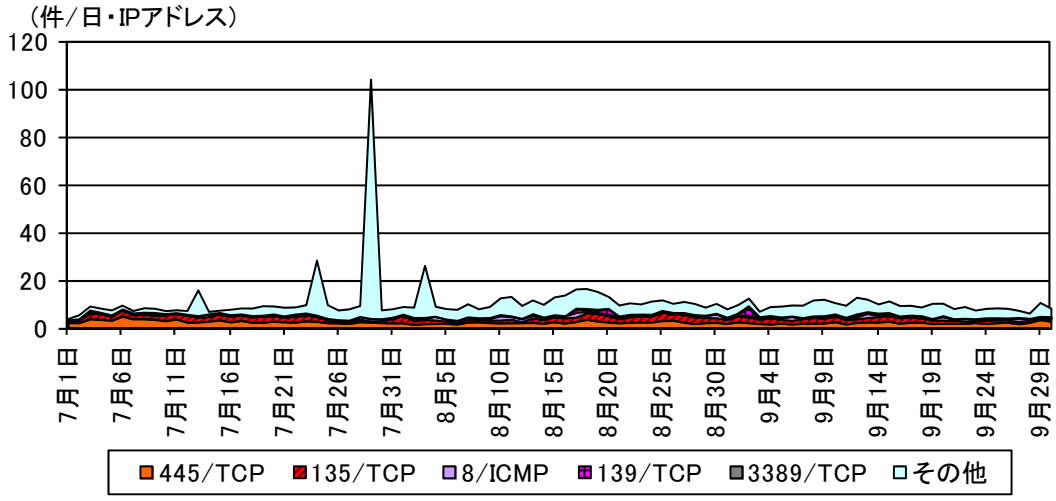

図 2-16　日本からのアクセス件数の推移

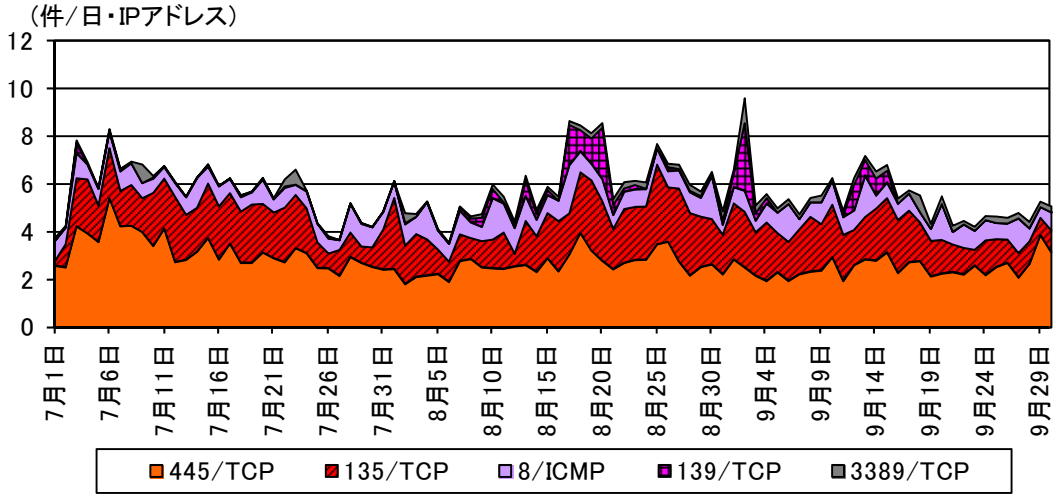

図 2-17　日本からのアクセス件数の推移（「その他」を除いたもの）

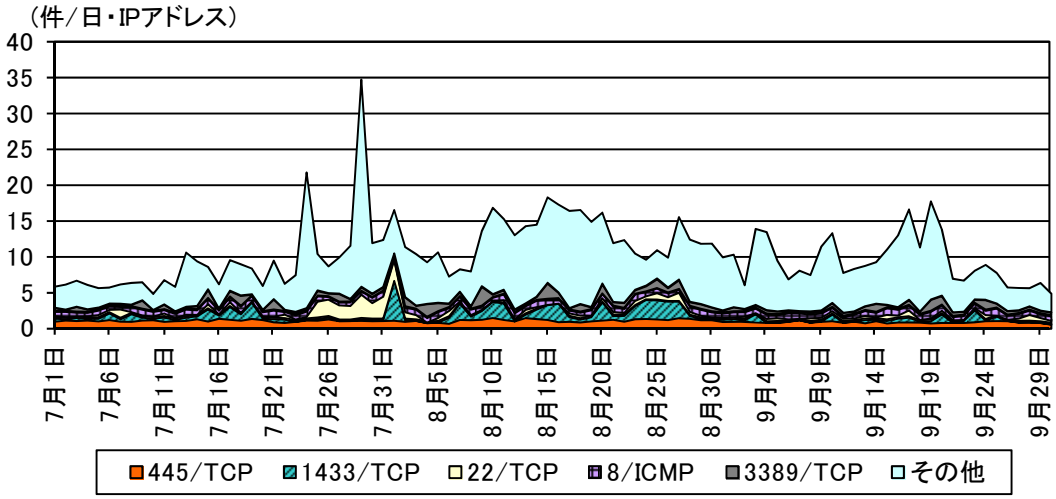

図 2-18　韓国からのアクセス件数の推移

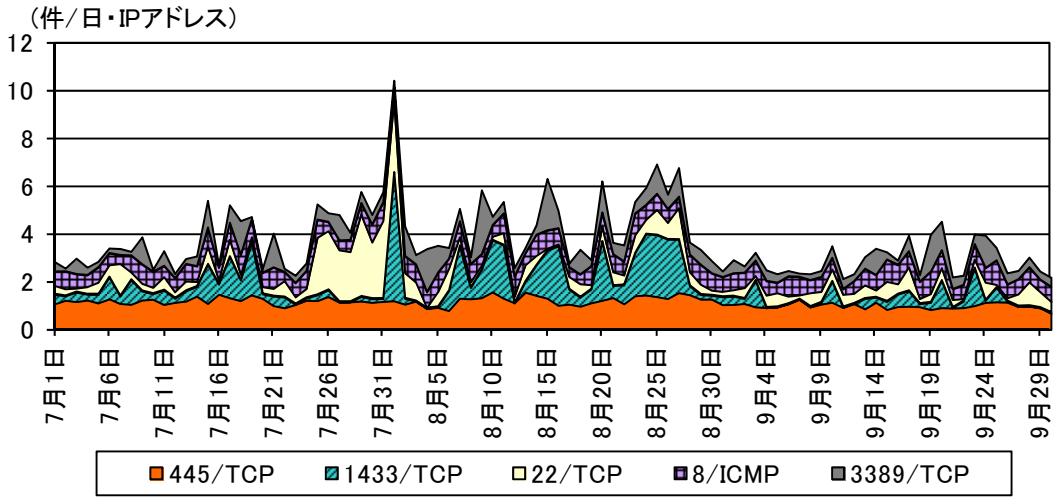

図 2-19　韓国からのアクセス件数の推移（「その他」を除いたもの）

3　インターネット定点観測 ―不正侵入等の検知

3-1　攻撃手法別

不正侵入等の検知件数は、攻撃手法別では「Scan」が最も多く、次いで「VoIP」、「Worm」、「DNS」、「Scan(P2P)」の順であり、この5分類で全体の 99.6%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 4.7 件で、前期と比較して横ばいであった(表 3-1)。「Scan」として検知したもののうち 87.7%は、プロキシサーバを探索する通信である。この通信は、攻撃のための踏み台として利用可能なプロキシサーバを探索しているものと考えられる。発信元国・地域別で見ると、前期に引き続き、中国からの通信が約半数を占めている(図 3-3)。

「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 2.3 件で、前期と比較して横ばいであった(表 3-1)。発信元国・地域別で見ると、米国からの通信が約半数を占めている(図 3-3)。

「Worm」の検知件数は、一日・1IP アドレス当たり 1.4 件で、前期と比較して 0.6 件(74.9%)増加した(表 3-1)。「Worm」として検知したものの大部分は、SQL Slammer 及び Nachi であった。SQL Slammer は、7月下旬から9月中旬にかけて中国の特定の IP アドレスを発信元とするアクセスが増加した。また、9月中旬からは韓国の特定の IP アドレスを発信元とするアクセスが増加した(図 3-4)。

「DNS」の検知件数は、一日・1IP アドレス当たり 0.9 件で、前期と比較して 0.7 件(438.6%)増加した(表 3-1)。これは、7月下旬から8月下旬にかけて、オランダの複数 IP アドレスを発信元とする通信が増加したためである。この通信は、DNS 要求を使用したネットワーク調査が目的と考えられる。

「Scan(P2P)」の検知件数は、一日・1IP アドレス当たり 0.4 件で、前期と比較して横ばいであった(表 3-1)。前期、全体の 22.5%を占めたロシアからの通信は、今期も全体の 14.6%を占め、検知件数が1位となったものの、減少した(図 3-3)。

表 3-1　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	4.69 件	－1.6%　(－0.07 件)		2 位
2 位	2 位	VoIP	2.27 件	＋1.1%　(＋0.03 件)	4 位	
3 位	3 位	Worm	1.35 件	＋74.9%　(＋0.58 件)	2 位	
4 位	5 位	DNS	0.85 件	＋438.6%　(＋0.70 件)	1 位	
5 位	4 位	Scan(P2P)	0.35 件	＋8.7%　(＋0.03 件)	3 位	

[1] 一日・1IP アドレス当たり。

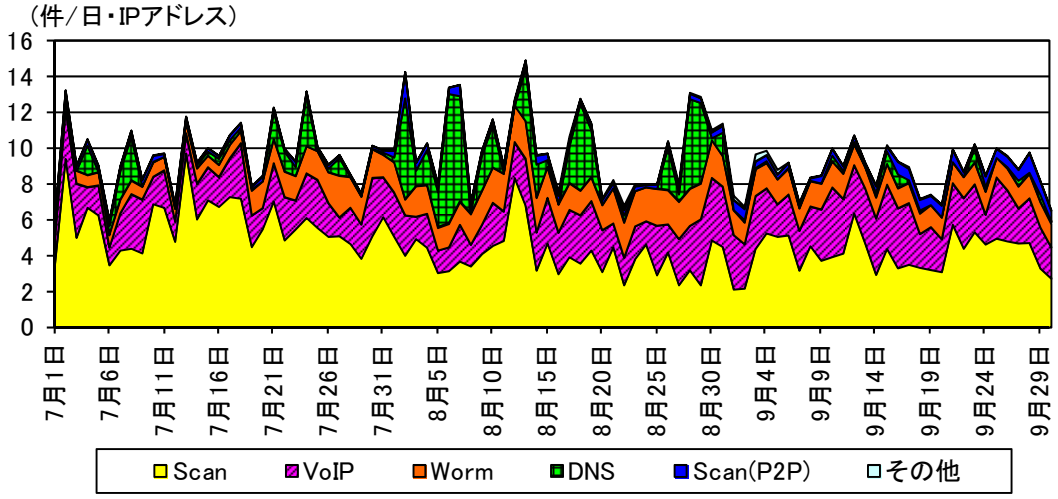

図 3-1　不正侵入等の攻撃手法別検知件数の推移

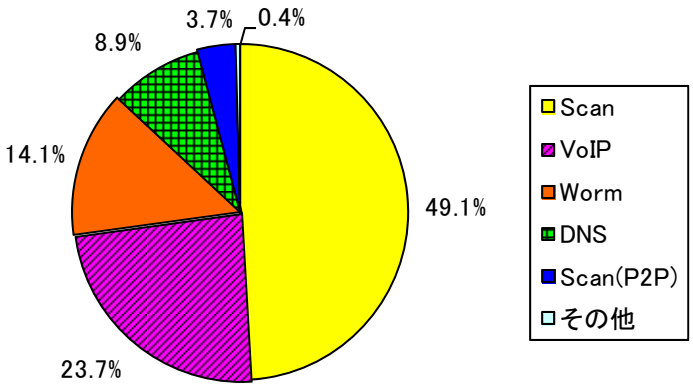

図 3-2　不正侵入等の攻撃手法別検知比率[1]

[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。

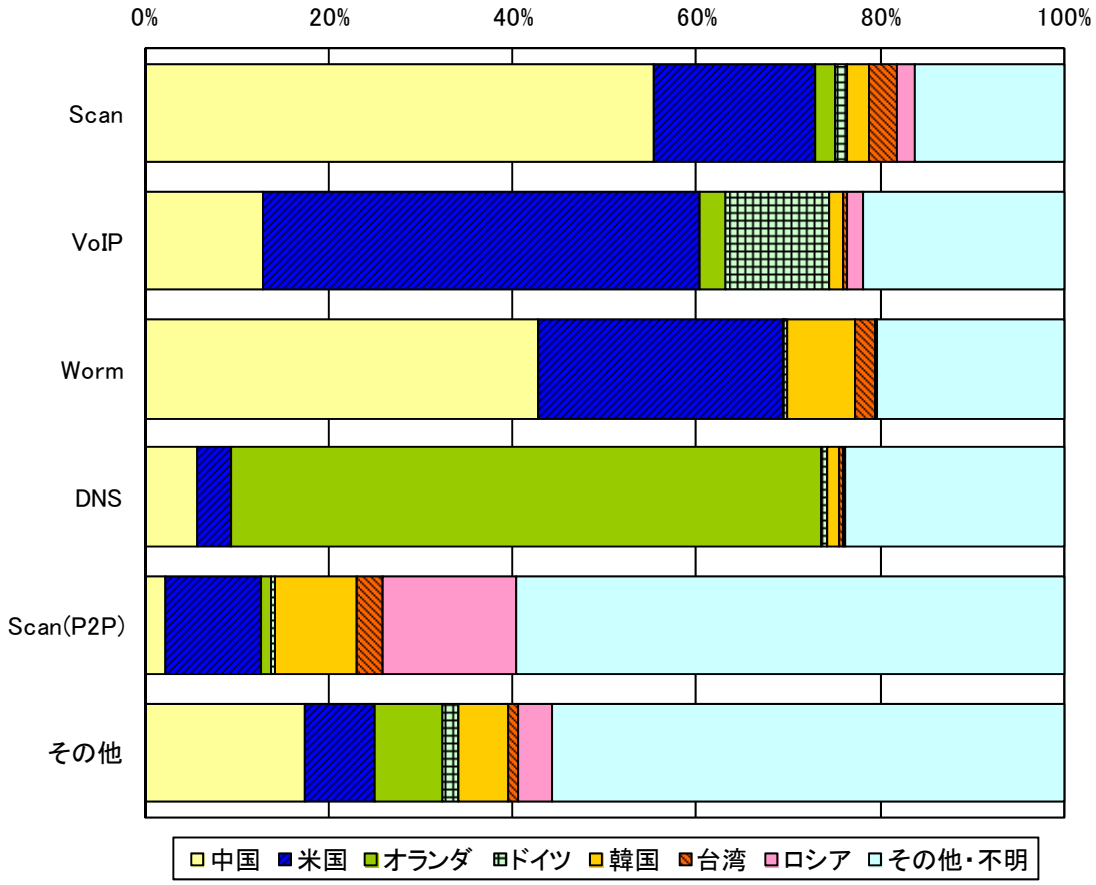

図 3-3　不正侵入等の攻撃手法の国・地域別検知比率

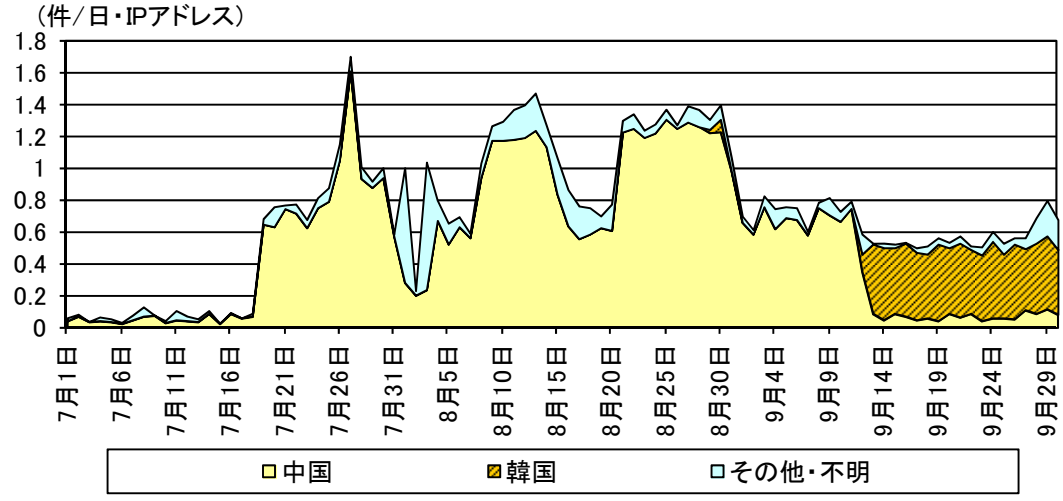

図 3-4　SQL Slammer の検知件数の推移

3-2　発信元国・地域別

発信元国・地域別検知件数は、中国が最も多く、次いで、米国、オランダ、ドイツ、韓国の順であった(図 3-6)。

中国を発信元とする検知件数は、一日・1IP アドレス当たり 3.5 件で、前期と比較して 0.9 件(35.4%)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、一日・1IP アドレス当たり 2.6 件で、前期と比較して 0.4 件(16.3%)増加しており、最も多く検知している。また、「Worm」の検知件数は、一日・1IP アドレス当たり 0.6 件で、前期と比較して 0.5 件(526.5%)増加した。これは、SQL Slammer の検知件数が一時的に増加したためである。

今期2位の米国は、「VoIP」の検知件数が、一日・1IP アドレス当たり 1.1 件で、前期と比較して 0.1 件(12.1%)増加した。また、「Scan」の検知件数も、一日・1IP アドレス当たり 0.8 件で、前期と比較して 0.2 件(22.4%)増加し、この二つの攻撃手法で検知件数全体の 81.5%を占めた。

今期3位のオランダは、「DNS」の検知件数が、一日・1IP アドレス当たり 0.5 件で、前期と比較して増加した。これは、7月 下旬から8月 下旬にかけて一時的に増加したためで、検知件数全体の 76.3%を占めた。

今期5位の韓国は、「Worm」の検知件数が、一日・1IP アドレス当たり 0.1 件で、前期と比較して増加した。これは、SQL Slammer が9月 中旬から増加したためである。

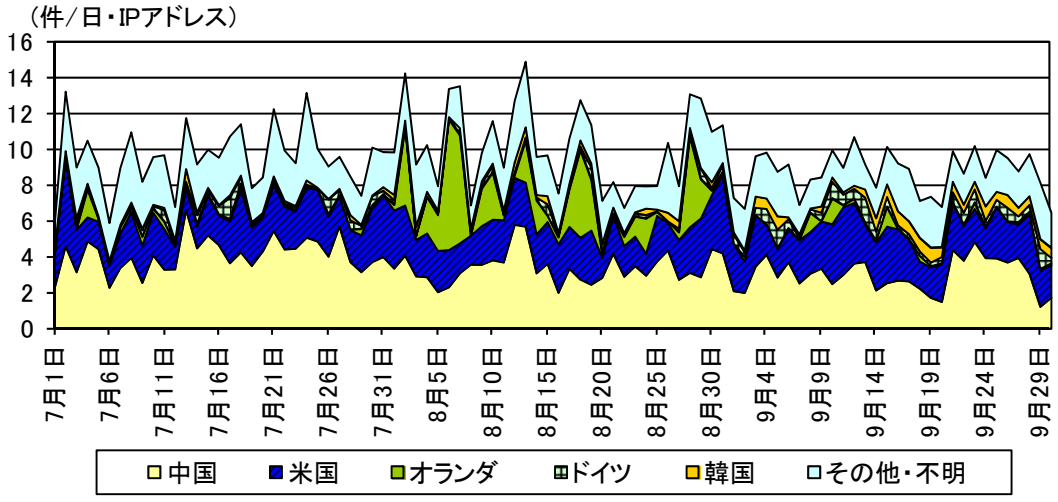

図 3-5　不正侵入等の発信元国・地域別検知件数の推移

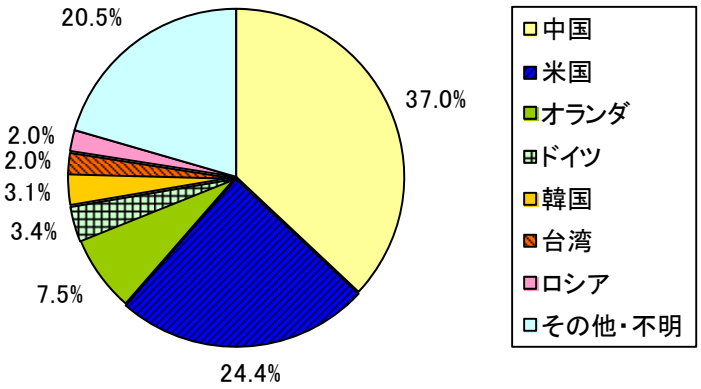

図 3-6　不正侵入等の発信元国・地域別検知比率[1]

[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 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	3.53 件	＋35.4% （＋0.92 件）
2 位	2 位	米国	2.33 件	＋12.0% （＋0.25 件）
3 位	6 位	オランダ	0.72 件	＋251.2% （＋0.51 件）
4 位	3 位	ドイツ	0.32 件	－8.3% （－0.03 件）
5 位	7 位	韓国	0.30 件	＋52.8% （＋0.10 件）

表 3-3 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	3.53 件	＋35.4% （＋0.92 件）	1 位	1 位
2 位	オランダ	0.72 件	＋251.2% （＋0.51 件）	3 位	6 位
3 位	米国	2.33 件	＋12.0% （＋0.25 件）	2 位	2 位
4 位	韓国	0.30 件	＋52.8% （＋0.10 件）	5 位	7 位
5 位	台湾	0.20 件	＋102.3% （＋0.10 件）	6 位	12 位

表 3-4 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	インド	0.13 件	－57.3% （－0.18 件）	10 位	4 位
2 位	ブラジル	0.12 件	－43.6% （－0.09 件）	12 位	5 位
3 位	欧州連合	0.00 件	－97.1% （－0.06 件）	79 位	20 位
4 位	英国	0.14 件	－27.7% （－0.05 件）	9 位	8 位
5 位	トルコ	0.03 件	－54.0% （－0.04 件）	25 位	16 位

[1] 一日・1IP アドレス当たり。

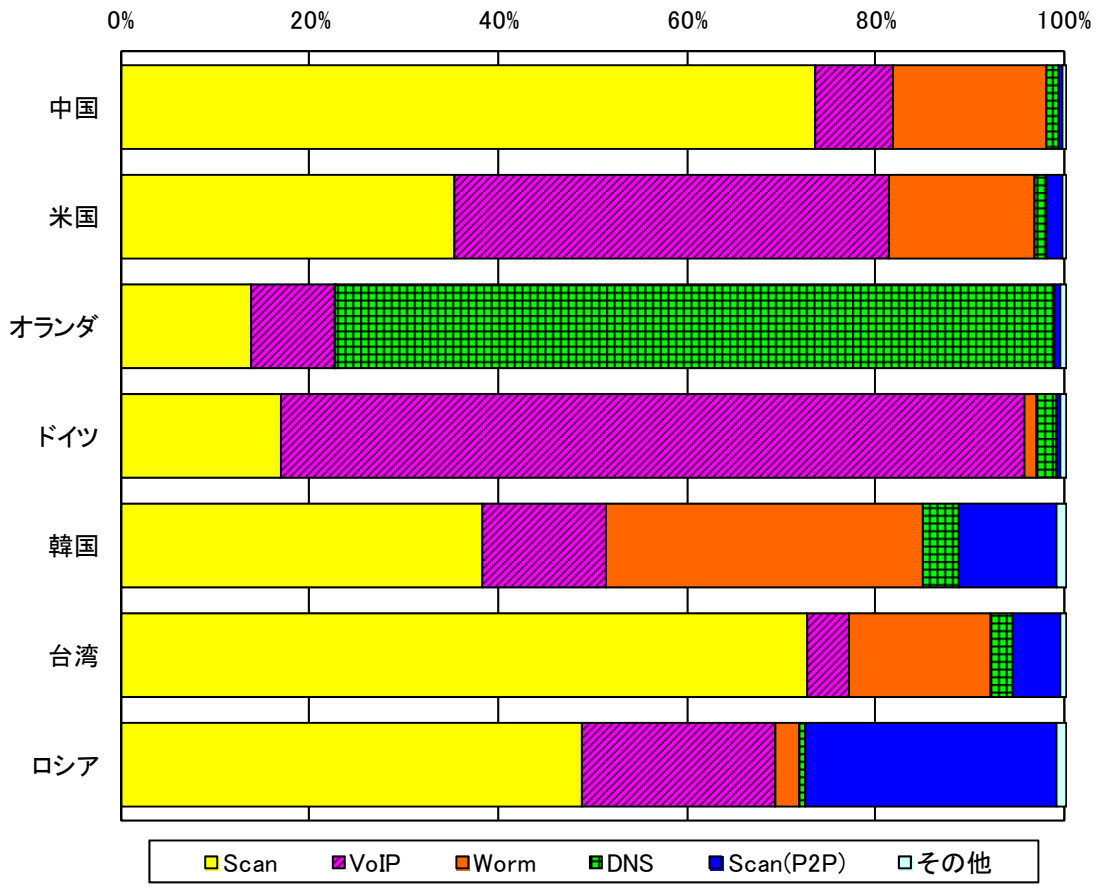

図 3-7　不正侵入等の発信元国・地域別上位の攻撃手法別検知比率

4　インターネット定点観測 ― DoS 攻撃被害観測状況

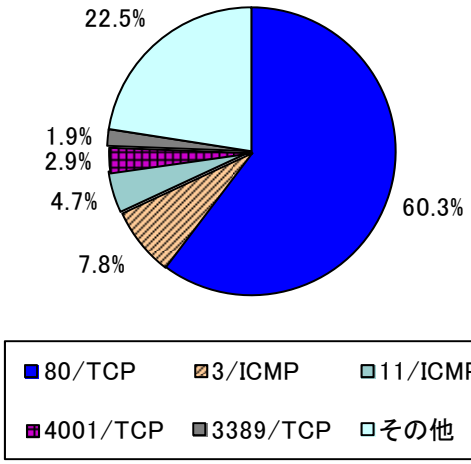

図 4-1　跳ね返りパケット発信元ポート別比率 [1]

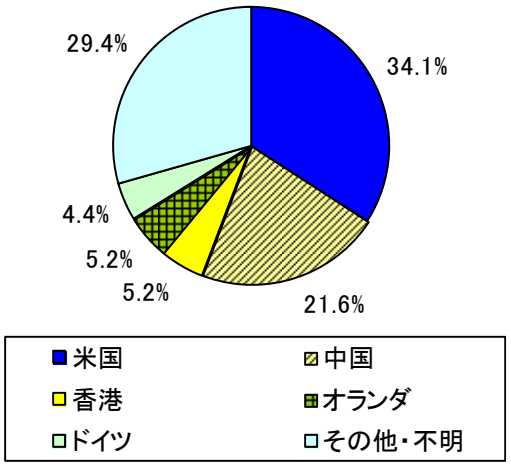

図 4-2　跳ね返りパケット発信元国・地域別比率 [1]

DoS 攻撃被害観測状況は、一日当たり 4,449.3 件で、前期と比較して 4,357.5 件（49.5%）減少した。発信元 IP アドレス数は一日当たり 382.5 個で、前期と比較して 133.2 個（25.8%）減少した。検知件数の上位は、前期に引き続き 80/TCP からの跳ね返りパケット、3/ICMP 及び 11/ICMP であるが、いずれも前期と比較して減少している(表 4-1)。

80/TCPを発信元とする跳ね返りパケット検知件数は全体の 60.3%を占め(図 4-1)、一日当たり 2,683.3 件で、前期と比較して一日当たり 2,782.3 件（50.9%）減少した。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いるが、前期と比較して一日当たり 1,818.7 件(68.1%)減少した(表 4-2)。これは、4月上旬から下旬に見られた米国の特定の IP アドレスを発信元とする跳ね返りパケットが今期見られなくなったことが主な要因である。香港からの跳ね返りパケットは、一日当たり 221.5 件で、前期と比較して 192.0 件（652.0%）増加した。これは、7月上旬、下旬及び8月下旬に特定のネットワーク上の IP アドレスからの跳ね返りパケットを集中して検知したためである。

今期5位となった、Windowsリモートデスクトップで使用される3389/TCPを発信元とする跳ね返りパケットの検知件数は、一日当たり 82.6 件で、前期と比較して 6.9 件(9.1%)増加した(表 4-1)。発信元国・地域別で見ると、前期と同様、韓国からのパケットを最も多く検知しているが、9月以降検知件数は減少している(図 4-4)。米国からのパケットは一日当たり 25.2 件で、前期と比較して 14.2 件（128.8%）増加した(表 4-3)。これは、7月下旬から8月下旬に特定の IP アドレスからの跳ね返りパケットを検知したためである。

[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　跳ね返りパケットのポート別検知件数（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	80/TCP	2,683.3 件	−50.9%	（−2,782.3 件）
2 位	2 位	3/ICMP	345.7 件	−69.1%	（−772.9 件）
3 位	3 位	11/ICMP	207.5 件	−47.1%	（−184.7 件）
4 位	1138 位	4001/TCP	127.4 件	−[2]	（＋127.4 件）
5 位	8 位	3389/TCP	82.6 件	＋9.1%	（＋6.9 件）

表 4-2　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	850.5 件	−68.1%	（−1,818.7 件）
2 位	2 位	中国	568.2 件	−54.4%	（−677.2 件）
3 位	18 位	香港	221.5 件	＋652.0%	（＋192.0 件）
4 位	5 位	オランダ	170.4 件	＋6.1%	（＋9.8 件）
5 位	9 位	シンガポール	92.8 件	＋9.6%	（＋8.2 件）

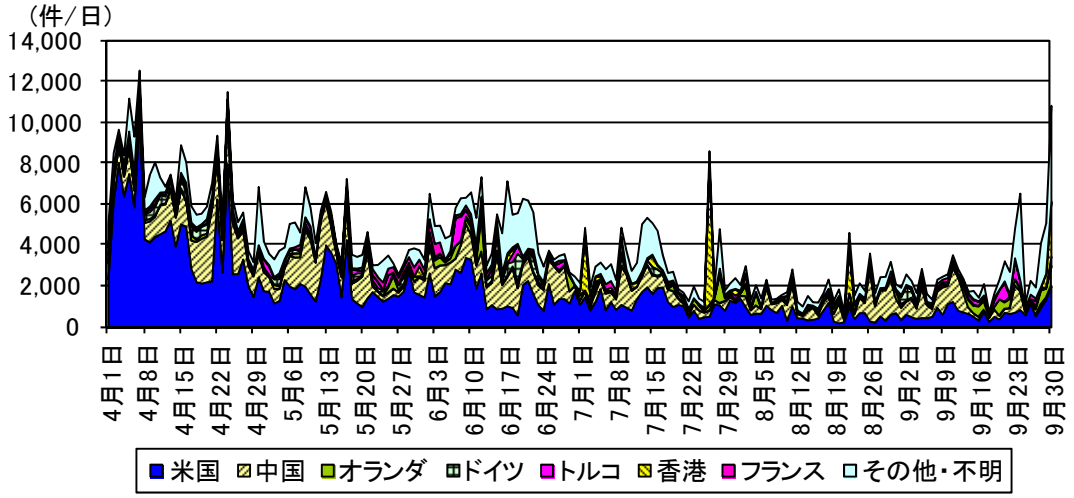

図 4-3　発信元ポート 80/TCP からの跳ね返りパケットの推移(H24/4/1～9/30)

[1] 一日当たり。
[2] 前期の検知件数がごく僅かであるため、前期比率は記載していない

表 4-3　3389/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	韓国	36.6 件	－25.1%	（－12.3 件）
2 位	3 位	米国	25.2 件	＋128.8%	（＋14.2 件）
3 位	2 位	中国	12.8 件	＋15.6%	（＋1.7 件）
4 位	13 位	トルコ	6.3 件	－[2]	（＋6.3 件）
5 位	－	台湾	0.4 件	－[3]	（＋0.4 件）

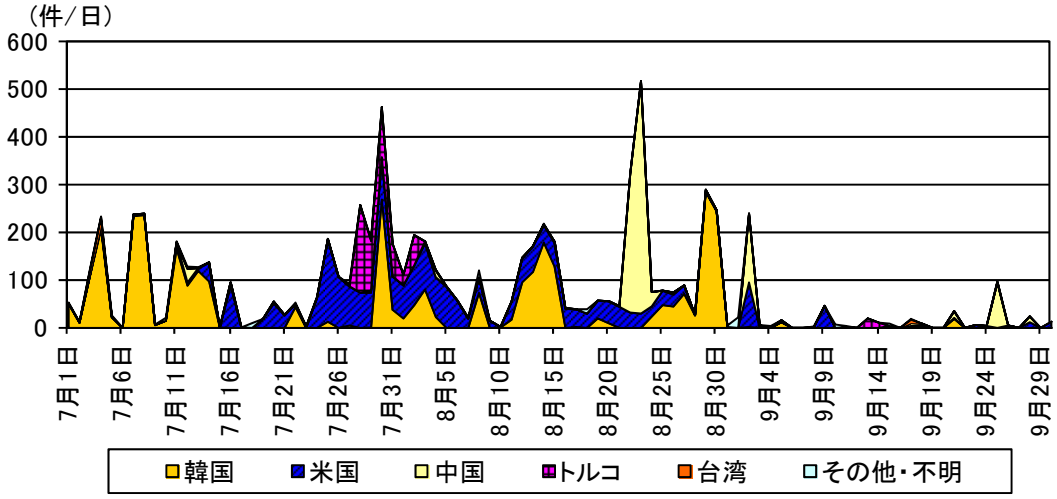

図 4-4　発信元ポート 3389/TCP からの跳ね返りパケットの推移

[1] 一日当たり。
[2] 前期の検知件数が僅かであるため、前期比率は記載していない。
[3] 前期の検知件数が 0 件であるため、前期比率は記載していない。

5　@police　（Topics）掲載事項

@police において、平成 24 年 7 月から 9 月までの第2／四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	7 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 (MS12-043,044,045,046,047,048,049,050,051)
重要	8 月 15 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 (MS12-052,053,054,055,056,057,058,059,060)
重要	8 月 15 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	8 月 15 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	8 月 22 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
●	8 月 31 日	インターネット治安情勢更新(平成 24 年度第 1 四半期報を追加)
重要	9 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(MS12-061,062)
重要	9 月 22 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(MS12-063)

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 11/ICMP 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　不正侵入等の検知

各センサーには、平成 24 年9月 30 日現在、3,136 種類のシグネチャが登録されている。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 VoIP 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