平成 24 年5月 15 日

インターネット観測結果等

(平成 23 年度第4／四半期(1月～3月))

・23/TCP 及び 3389/TCP へのアクセスが増加
・中国の特定 IP アドレスからの SQL Slammer が減少
・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 4／四半期における状況

1-1　23/TCP 及び 3389/TCP へのアクセスが増加

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 275.5 件で、平成 23 年度第3／四半期(以下「前期」という。)と比較して 35.6 件(14.8%)増加した。また、発信元 IP アドレス数は一日当たり 8,526.4 個で、前期と比較して 45.2 個(0.5%)増加した。

アクセス件数の上位5ポートは、445/TCP、1433/TCP、557/UDP、23/TCP、ICMP Echo Request(以下「8/ICMP」という。)の順であった(表 2-1)。平成 23 年度第4／四半期(以下、「今期」という。)は、1月下旬を中心に、韓国、台湾及び中国を発信元とする 23/TCP に対するアクセスが増加した。このポートは TELNET サービスで使用されるもので、不正なアクセスの試みと推測される。2月以降は、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増加した。また、これまでほとんど観測されなかった 557/UDP 及び 42731/UDP に対して、中国を発信元とするアクセスを多数検知している。

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

1-2　中国の特定 IP アドレスの SQL Slammer が減少

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 6.9 件で、前期と比較して 0.5 件(6.4%)減少した。また、発信元 IP アドレス数は一日当たり 265.3 個で、前期と比較して 25.7 個(8.8%)減少した。

前期から継続して、中国の特定 IP アドレスから SQL Slammer を検知しているが、2月頃から減少傾向にあり、3月下旬にはほとんど見られなくなった(図 3-7)。

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 6,436.3 件で、前期と比較して 5,954.2 件(48.1%)減少した。発信元 IP アドレス数は一日当たり 390.5 個で、前期と比較して 158.4 個(68.3%)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 639.9 件(43.0%)増加した。これは、1月から2月にかけて、米国の特定の 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、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が大半を占めていると考えられる。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 アドレス数ともに減少を続けている（表 2-1）。

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、前期と比較して横ばいである。1433/TCP に対するアクセス件数の 86.9%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 92.8%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。

557/UDP は、短期間に多数のアクセスを検知しており、そのほとんどが中国を発信元としている(図 2-6)。

23/TCP に対するアクセスは、1月下旬に韓国、2月に台湾及び中国を発信元とするアクセスが増加した(図 2-7)。このポートは TELNET サービスで使用されるもので、不正なアクセスの試みと推測される。

8/ICMP は、1月中旬及び2月中旬に、日本国内からのアクセス件数の増加が見られた。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。また、3月中旬から下旬にかけて、米国からのアクセス数の増加が見られた。このアクセスは、米国の研究機関が発信元で、特定のネットワークにあるセンサーに対してのみ、一定の時間間隔でのアクセスが観測された。どちらのアクセスについても、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。

Windows リモートデスクトップの探索と考えられる 3389/TCP に対するアクセスは、前期に引き続き今期も増加している(図 2-9)。このポートへのアクセスは、2月２日に発信元 IP アドレス数が増加し、2月３日にピークを迎えた後、3月 19 日までの間、高い水準で推移した。

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	88.33 件	−13.0% （−13.17 件）
2 位	2 位	1433/TCP	45.43 件	＋2.4% （＋1.08 件）
3 位	−	557/UDP	23.79 件	−[2] （＋23.79 件）
4 位	11 位	23/TCP	15.21 件	＋414.9% （＋12.25 件）
5 位	3 位	8/ICMP	13.73 件	＋5.5% （＋0.71 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	557/UDP	23.79 件	−[2] （＋23.79 件）	3 位	−
2 位	23/TCP	15.21 件	＋414.9% （＋12.25 件）	4 位	11 位
3 位	42731/UDP	8.05 件	−[2] （＋8.05 件）	8 位	−
4 位	27209/UDP	3.85 件	−[2] （＋3.85 件）	12 位	−
5 位	3389/TCP	11.62 件	＋41.6% （＋3.41 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	445/TCP	88.33 件	−13.0% （−13.17 件）	1 位	1 位
2 位	80/TCP	5.94 件	−33.9% （−3.04 件）	11 位	4 位
3 位	135/TCP	5.96 件	−23.6% （−1.85 件）	10 位	7 位
4 位	8909/TCP	1.57 件	−51.8% （−1.69 件）	17 位	10 位
5 位	8080/TCP	2.79 件	−24.4% （−0.90 件）	13 位	9 位

[1] 一日・1IP アドレス当たり。
[2] 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。

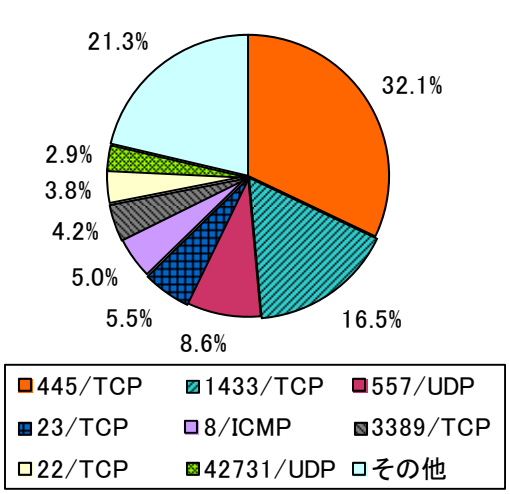

図 2-1　宛先ポート比率(すべて)[1]

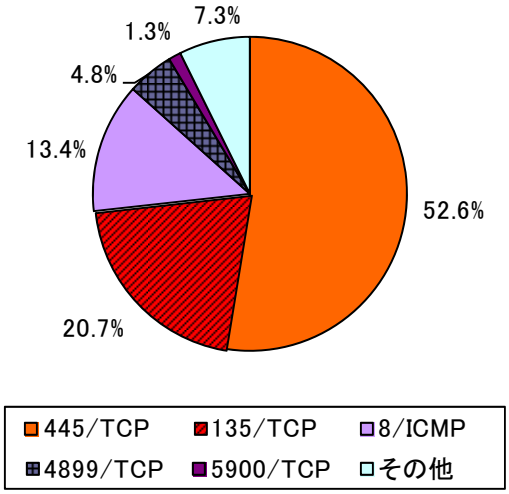

図 2-2　宛先ポート比率(日本国内)[1,2]

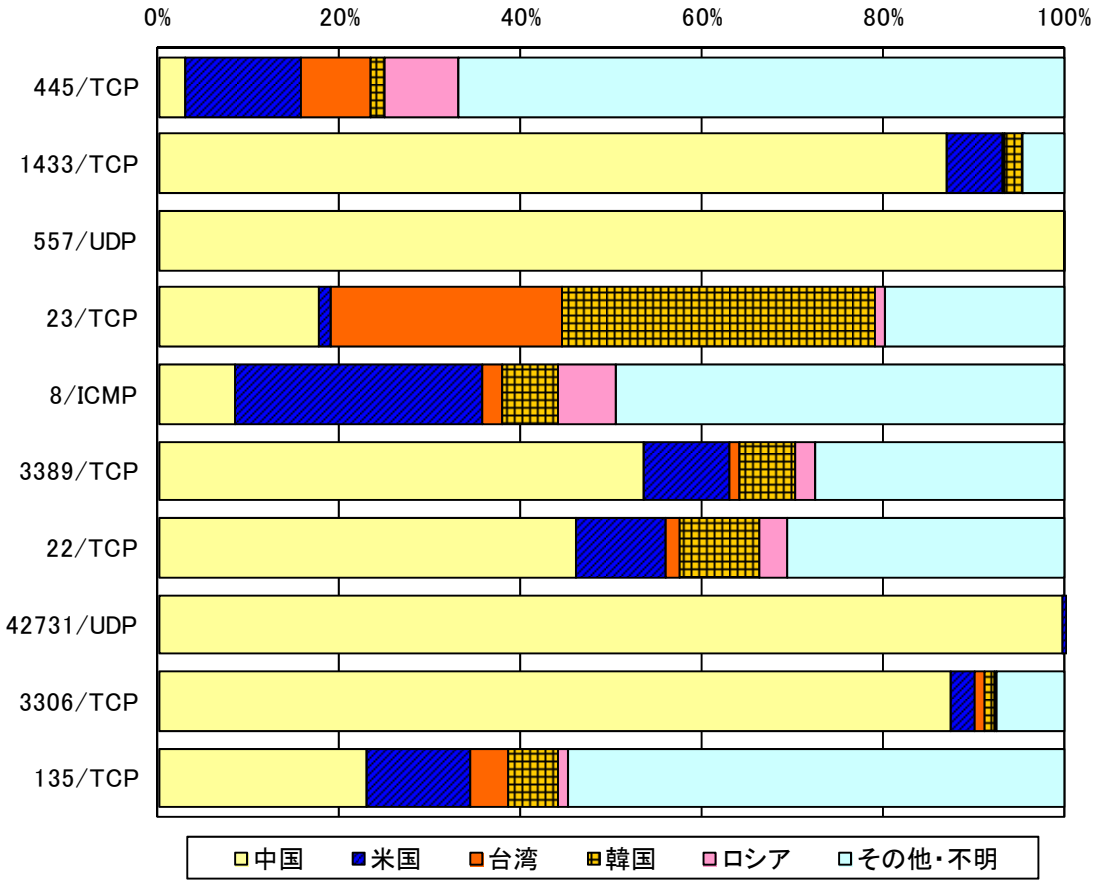

図 2-3　宛先ポート別上位の発信元国・地域別比率

[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。

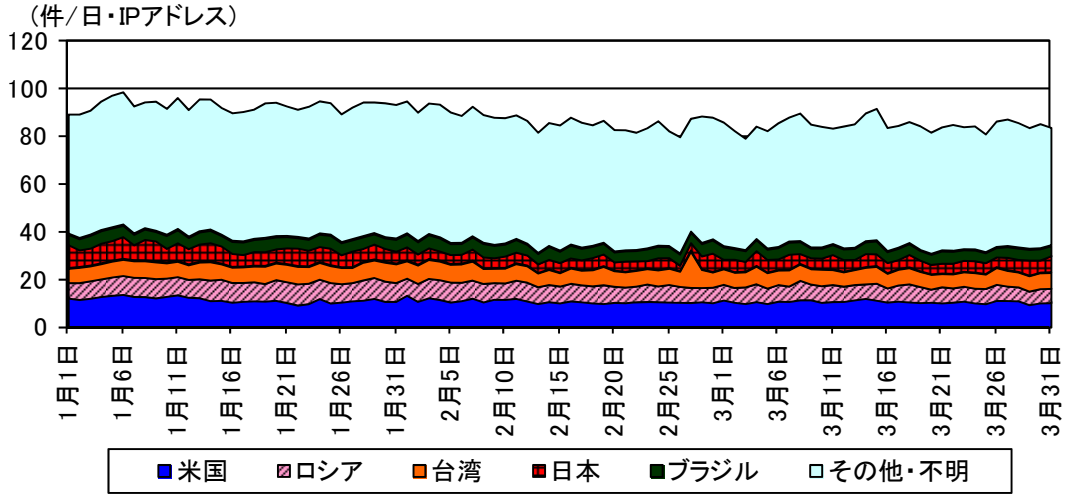

図 2-4　宛先ポート 445/TCP に対するアクセス件数の推移

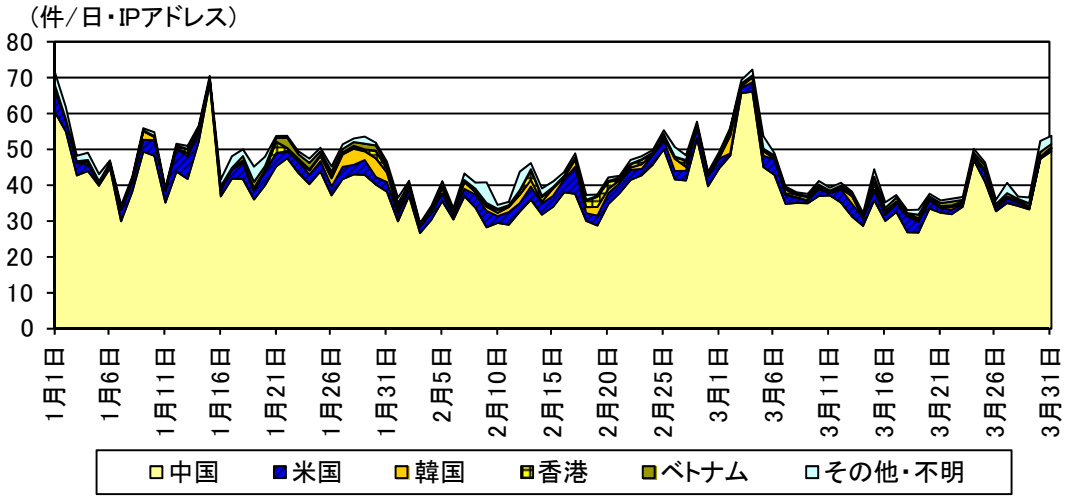

図 2-5　宛先ポート 1433/TCP に対するアクセス件数の推移

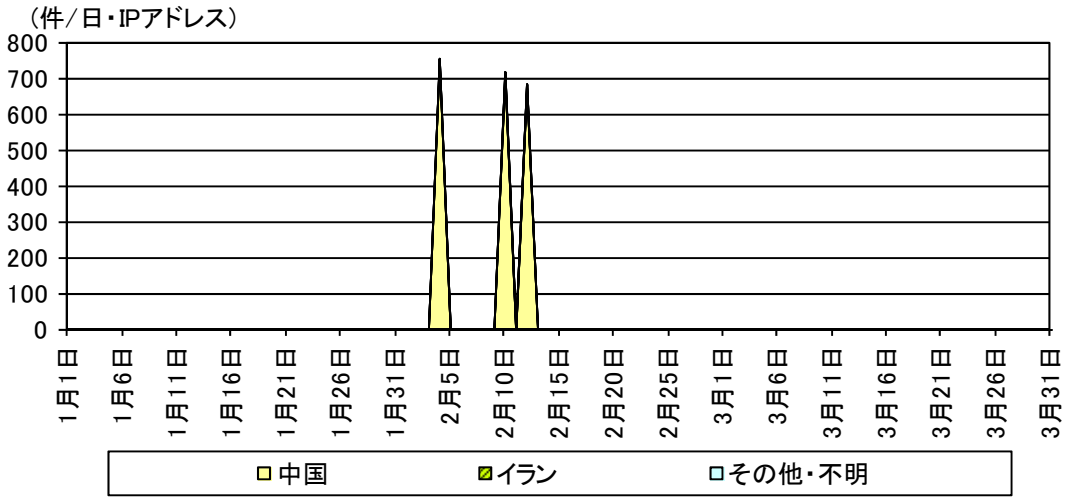

図 2-6　宛先ポート 557/UDP に対するアクセス件数の推移

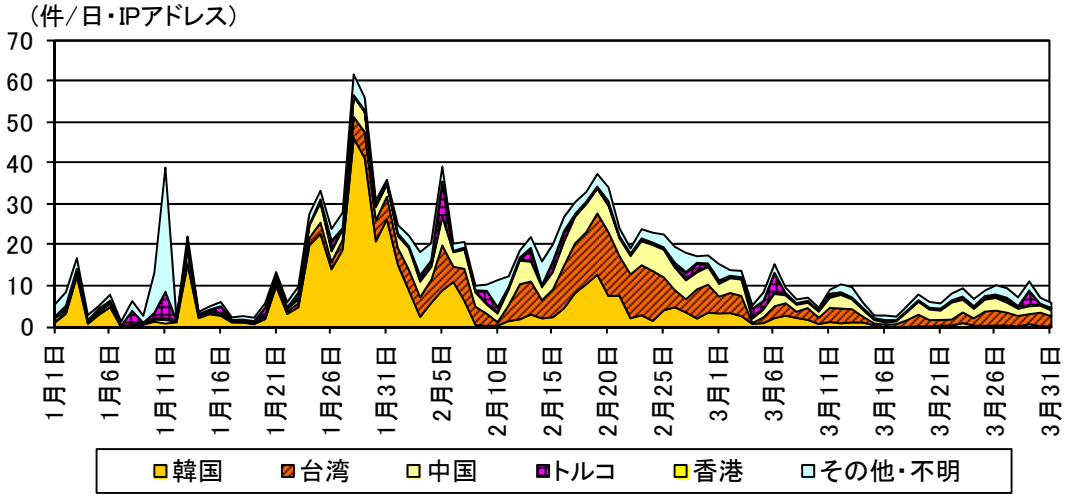

図 2-7　宛先ポート 23/TCP に対するアクセス件数の推移

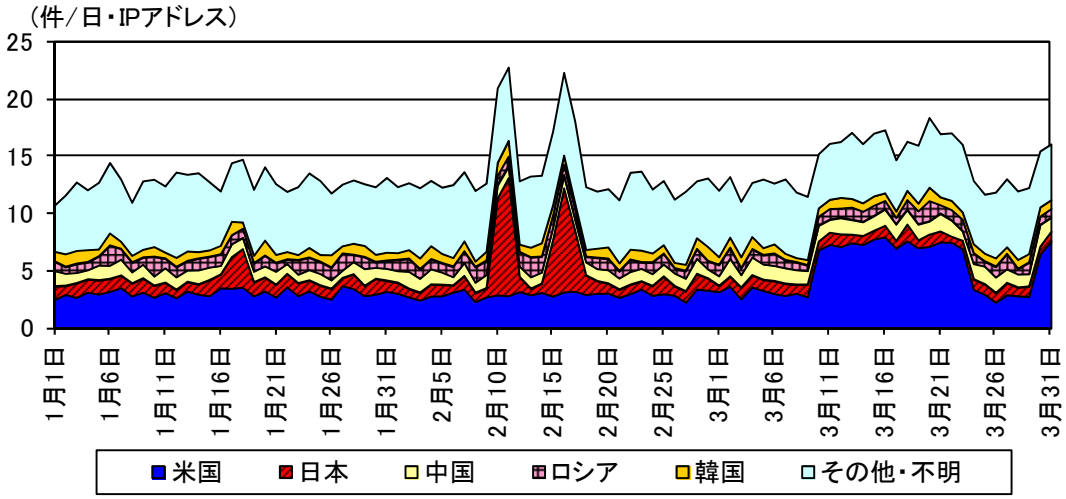

図 2-8　8/ICMP のアクセス件数の推移

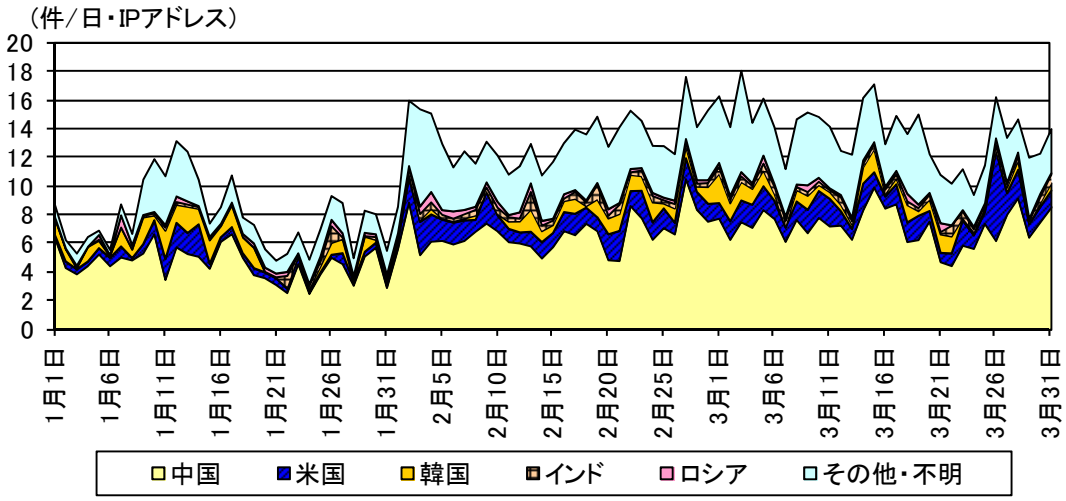

図 2-9　宛先ポート 3389/TCP に対するアクセス件数の推移

2-2　発信元国・地域別

中国からのアクセスは、これまでほとんど見られなかった 557/UDP へのアクセスを短期間に多数観測した（図 2-12）。6000/TCP を発信元とする 1433/TCP へのアクセスは、前期に引き続き増加し、1433/TCP に対するアクセス全体の 93.7%を占めている。

米国からのアクセスは、前期と比較して減少している（図 2-13）。1月８日の急激なアクセスの増加は、53/UDP を発信元ポートとする特定の IP アドレスから多数のアクセスがあったためである。

台湾からは、定常的に 445/TCP へのアクセスを観測しているが、今期は 23/TCP へのアクセスが増加した（図 2-14）。

韓国からは、23/TCP へのアクセス増加を1月下旬に観測した（図 2-15）。2月以降は減少に転じているが、このアクセスが要因となって、今期の発信元国・地域別検知件数の増加順位は2位となっている（表 2-5）。

日本国内からのアクセスは、今期減少したが、国別のアクセス数順位はロシアに次いで6位となっている。今期は、リモートコントロールソフトで使用される 4899/TCP 及び 5900/TCP へのアクセスが増加した（図 2-17）。

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	113.86 件	＋46.4% （＋36.07 件）
2 位	2 位	米国	29.61 件	－2.1% （－0.62 件）
3 位	4 位	台湾	13.20 件	＋18.8% （＋2.09 件）
4 位	7 位	韓国	11.75 件	＋65.9% （＋4.66 件）
5 位	5 位	ロシア	11.02 件	＋8.6% （＋0.88 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	113.86 件	＋46.4% （＋36.07 件）	1 位	1 位
2 位	韓国	11.75 件	＋65.9% （＋4.66 件）	4 位	7 位
3 位	台湾	13.20 件	＋18.8% （＋2.09 件）	3 位	4 位
4 位	ロシア	11.02 件	＋8.6% （＋0.88 件）	5 位	5 位
5 位	ルーマニア	3.49 件	＋29.4% （＋0.79 件）	11 位	15 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	日本	10.23 件	－45.5% （－8.55 件）	6 位	3 位
2 位	米国	29.61 件	－2.1% （－0.62 件）	2 位	2 位
3 位	ブラジル	6.66 件	－7.3% （－0.52 件）	7 位	6 位
4 位	インド	4.88 件	－8.4% （－0.45 件）	8 位	8 位
5 位	フィリピン	0.97 件	－19.6% （－0.24 件）	33 位	29 位

[1] 一日・1IP アドレス当たり。

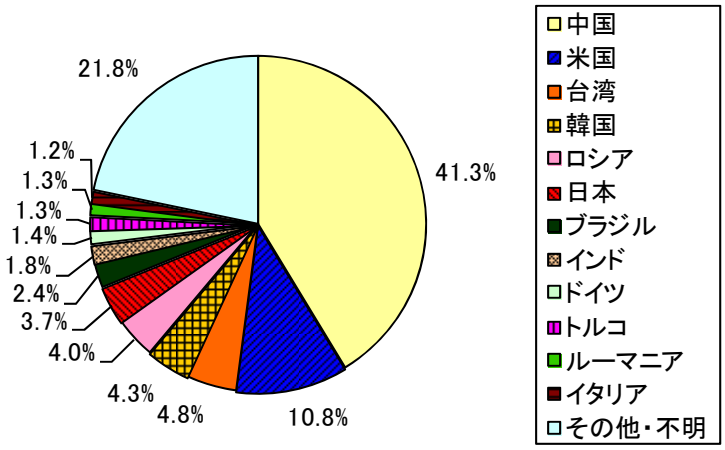

図 2-10　発信元国・地域別比率[1]

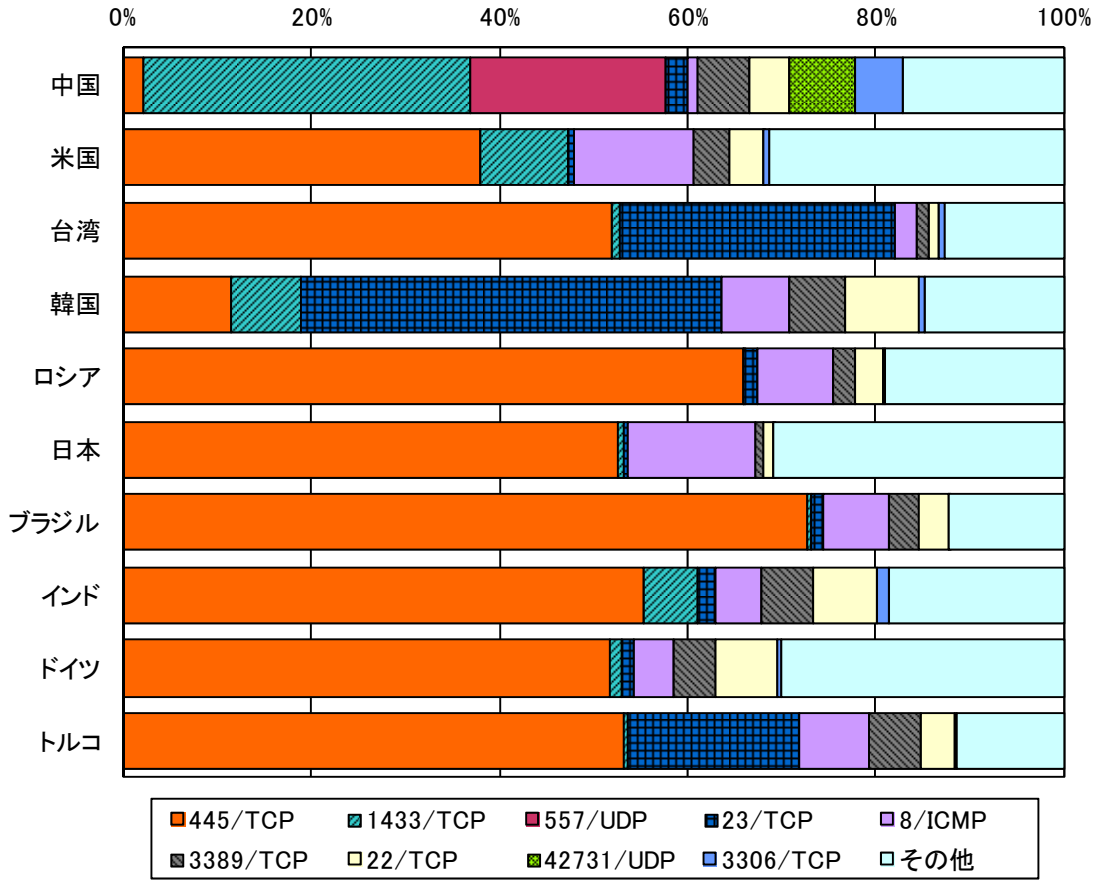

図 2-11　発信元国・地域別上位の宛先ポート別比率

[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。

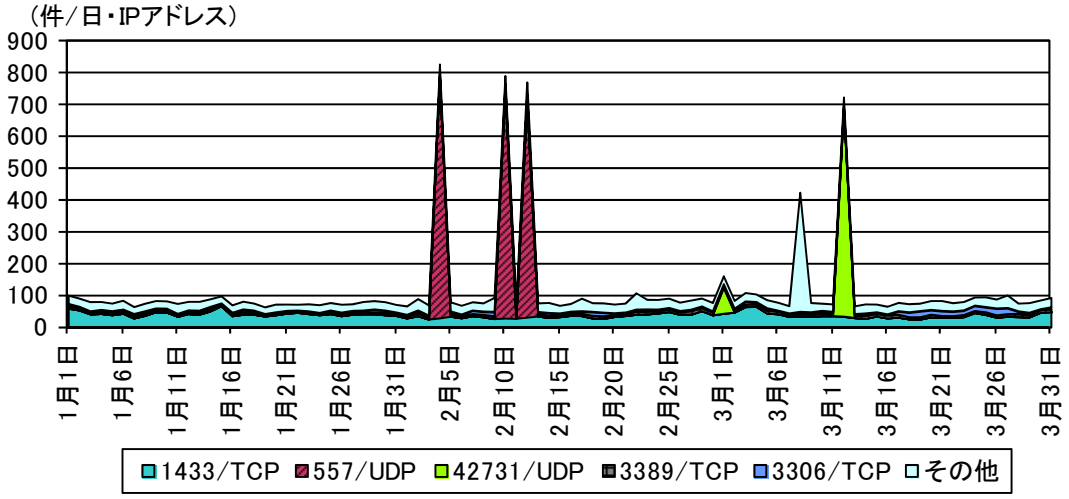

図 2-12　中国からのアクセス件数の推移

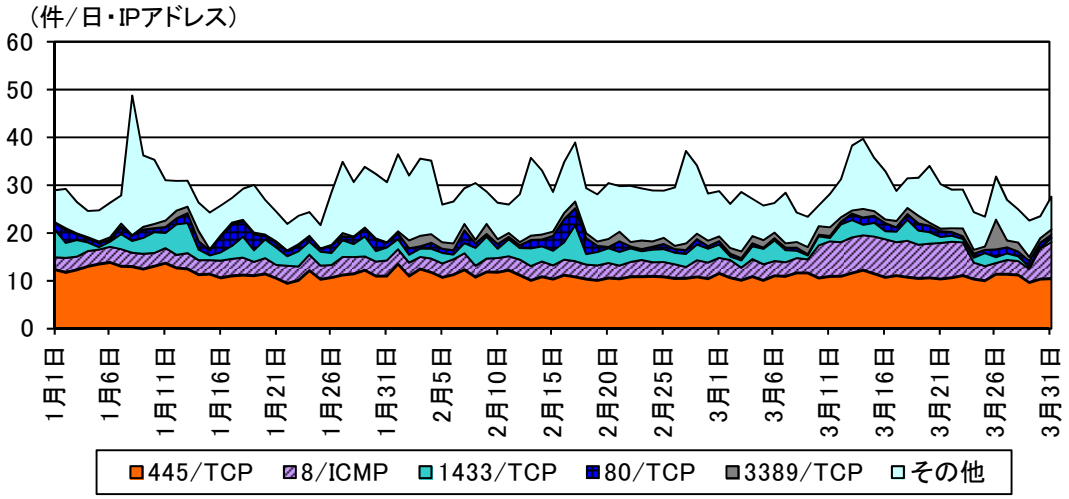

図 2-13　米国からのアクセス件数の推移

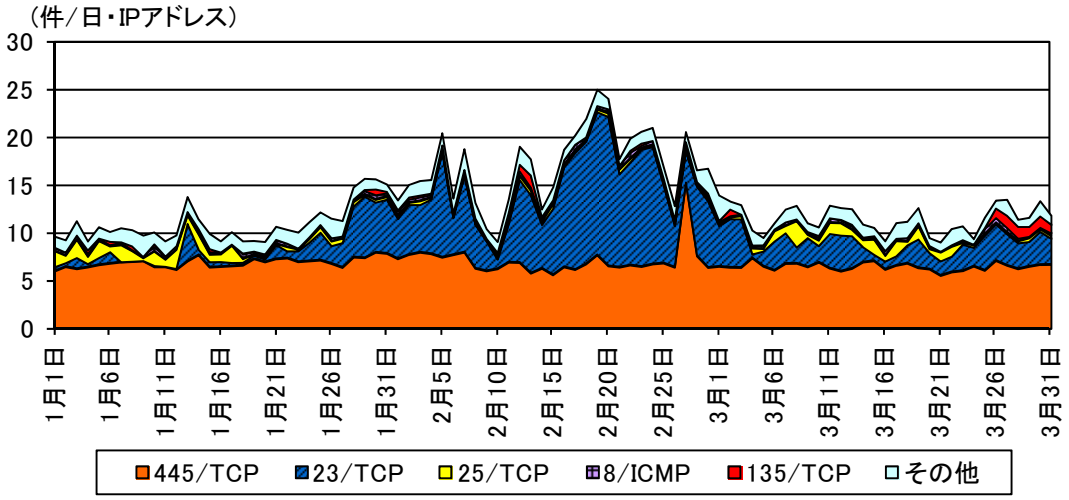

図 2-14　台湾からのアクセス件数の推移

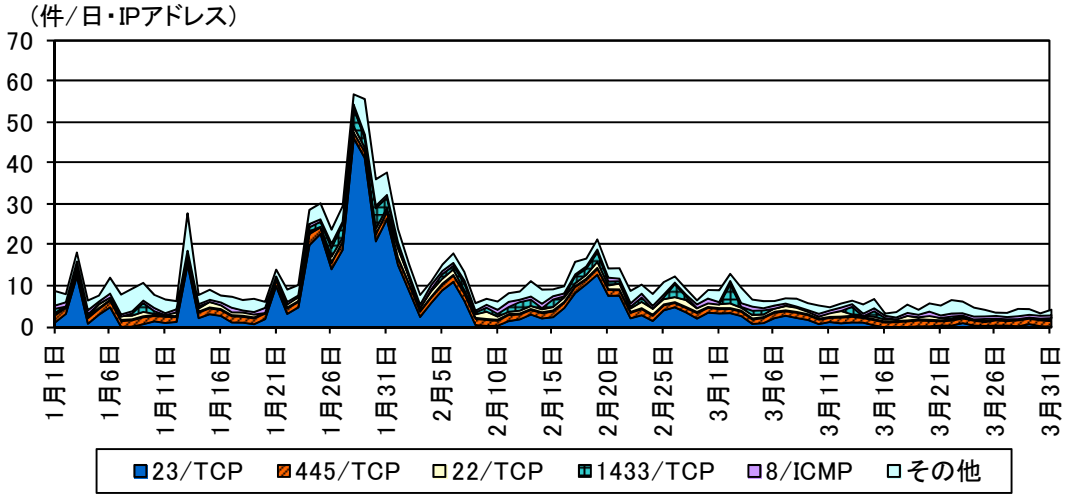

図 2-15　韓国からのアクセス件数の推移

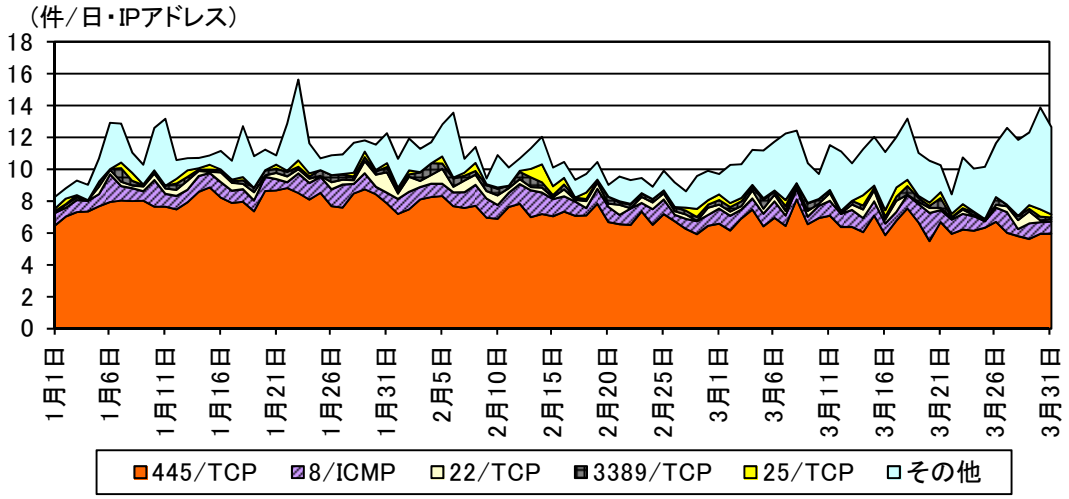

図 2-16　ロシアからのアクセス件数の推移

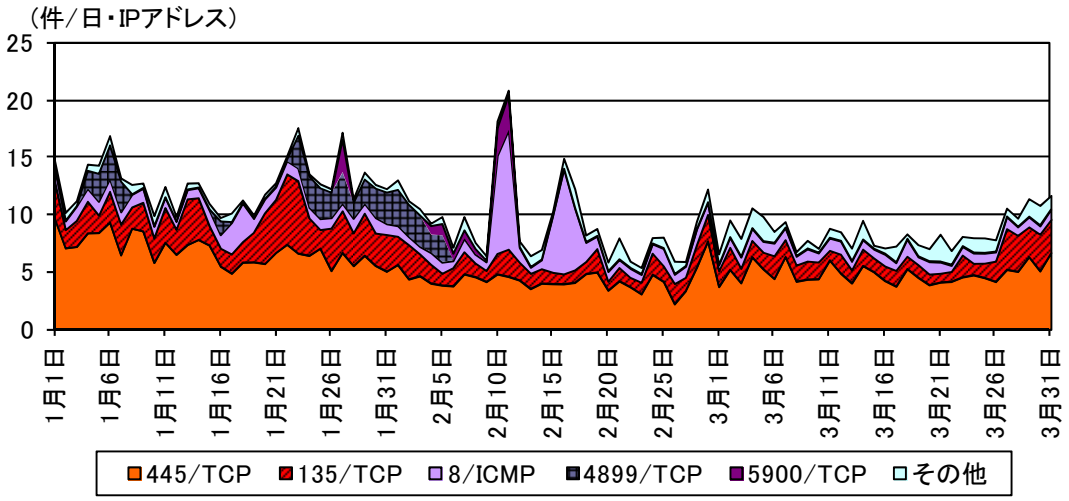

図 2-17　日本国内からのアクセス件数の推移

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 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 2.3 件で、前期と比較して 0.7 件(23.8%)減少した(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 96.1%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、これまで多数検知していた台湾からの通信が減少傾向にある。

「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)。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 0.4 件で、前期と比較して 0.1 件(29.7%)減少しているが、ドイツからの検知件数は、一日・1IP アドレス当たり 0.1 件で、前期と比較して 0.1 件(97.9%)増加した。

「Worm」の検知件数は、一日・1IP アドレス当たり 1.8 件で、前期と比較して 0.1 件(6.5%)増加した(表 3-1)。中国の特定 IP アドレスから SQL Slammer を検知しているが、2月頃から減少傾向にあり、3月下旬にはほとんど見られなくなった。

「Scan(P2P)」の検知件数は、一日・1IP アドレス当たり 0.4 件で、前期と比較してほぼ横ばいであった(表 3-1)。韓国からのファイル共有ソフト BitTorrent の稼働を確認する通信が、1月から2月上旬まで一時的に増加したが、その後、大きな変化は見られない。

「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 0.1 件(245.9%)増加した(表 3-1)。これは、米国、フランスやドイツ等を発信元とする DNS 情報の調査をする通信が、2月中旬から3月上旬の間に一時的に増加したためである。

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	2.25 件	−23.8%　(−0.70 件)		1 位
2 位	2 位	VoIP	2.16 件	−0.4%　(−0.01 件)		2 位
3 位	3 位	Worm	1.84 件	+6.5%　(+0.11 件)	1 位	
4 位	4 位	Scan(P2P)	0.44 件	+4.0%　(+0.02 件)	3 位	
5 位	5 位	DNS	0.15 件	+245.9%　(+0.10 件)	2 位	

[1] 一日・1IP アドレス当たり。

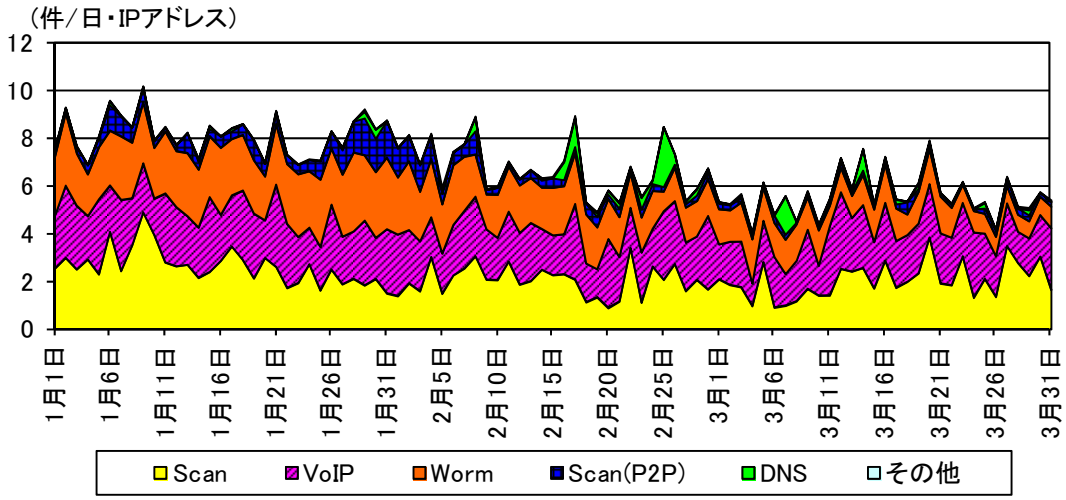

図 3-1　シグネチャを用いた不正侵入等の攻撃手法別検知件数の推移

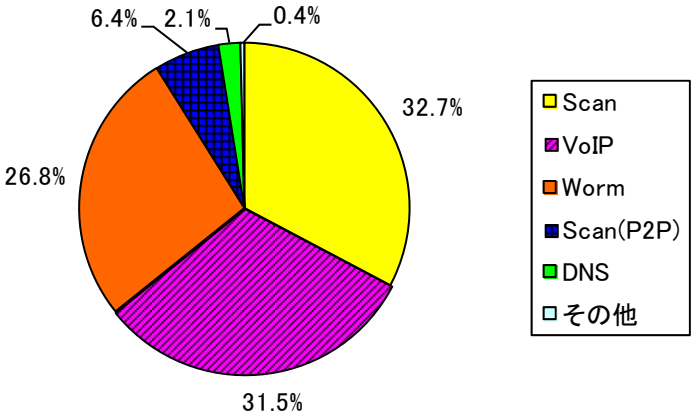

図 3-2　シグネチャを用いた不正侵入等の攻撃手法別検知比率[1]

[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。

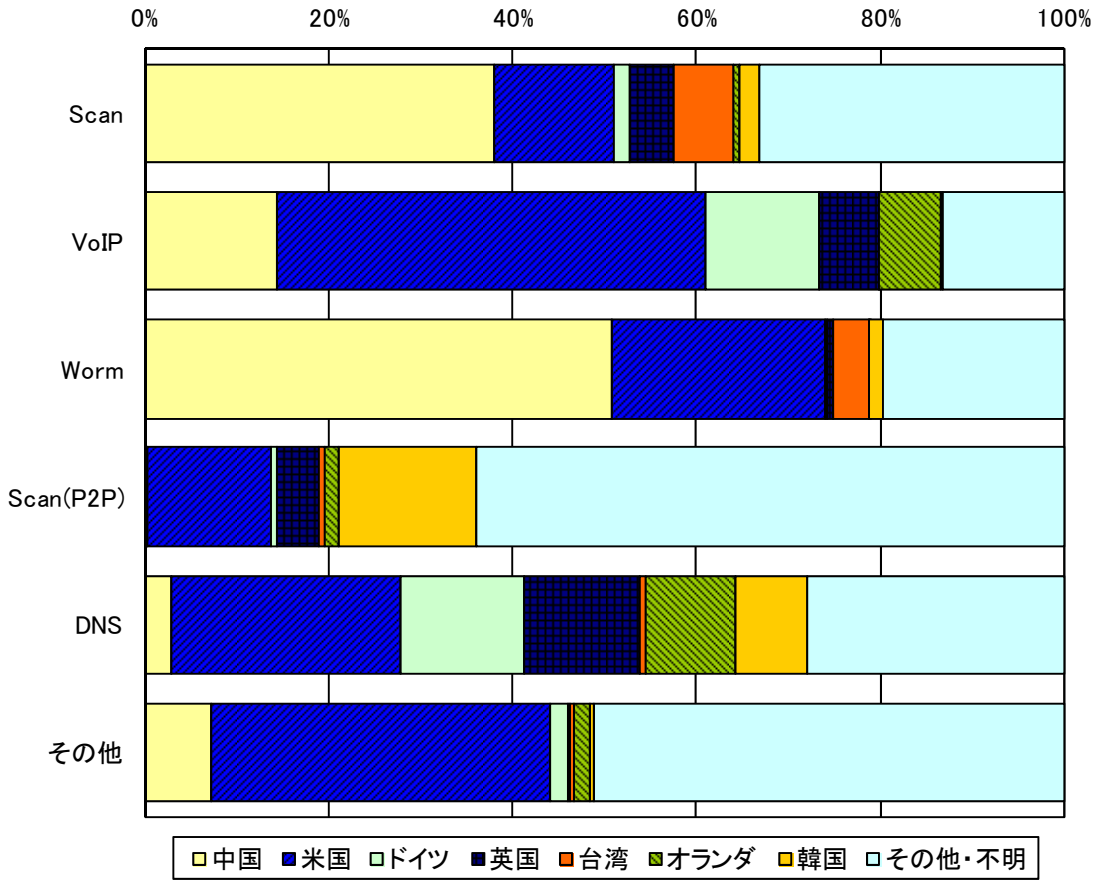

図 3-3 シグネチャを用いた不正侵入等の攻撃手法の国・地域別検知比率

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、英国、台湾の順であった。

中国を発信元とする検知件数は、一日・1IP アドレス当たり 2.1 件で、前期と比較して 0.1 件(3.7%)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、「Worm」の検知件数が、前期と比較して 0.3 件(36.6%)増加しており、最も多く検知しているが、2月頃から減少傾向となり、3月下旬にはほとんど見られなくなった。

前期5位から今期3位に検知件数が増加しているドイツは、「VoIP」の検知件数が、前期と比較して、一日・1IP アドレス当たり 0.1 件(97.9%)増加した。また、2月中旬には、特定の IP アドレスから、DNS 情報の調査をする通信を検知した。

今期4位の英国は、「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 0.1 件(460.1%)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、1月から2月中旬までは多く見られたが、それ以降は減少傾向である。

今期5位の台湾は、「Scan」の検知件数が前期と比較して、0.5 件(78.4%)減少した。前期から継続して3月上旬まではプロキシサーバを探索する通信を検知していたが、それ以降はほとんど見られなくなった。

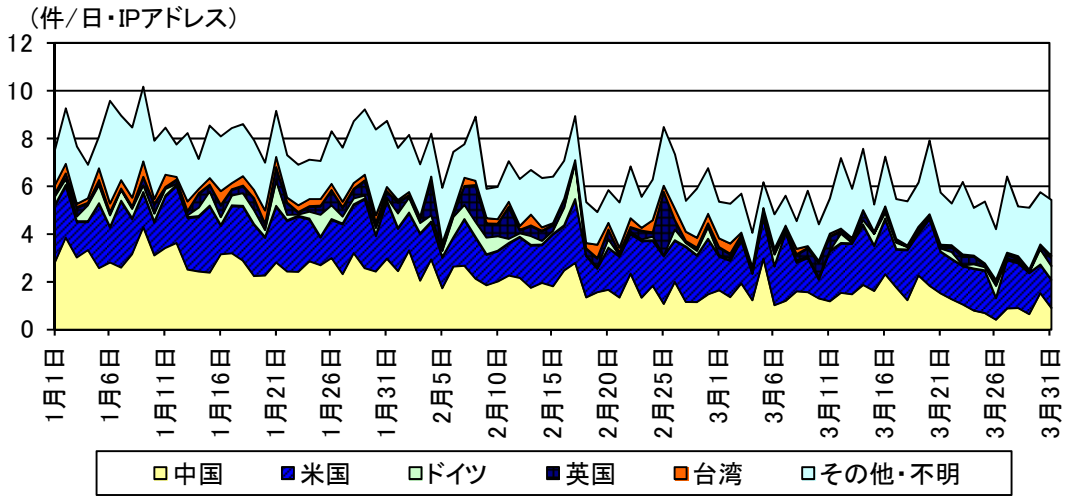

図 3-4　シグネチャを用いた不正侵入等の発信元国・地域別検知件数の推移

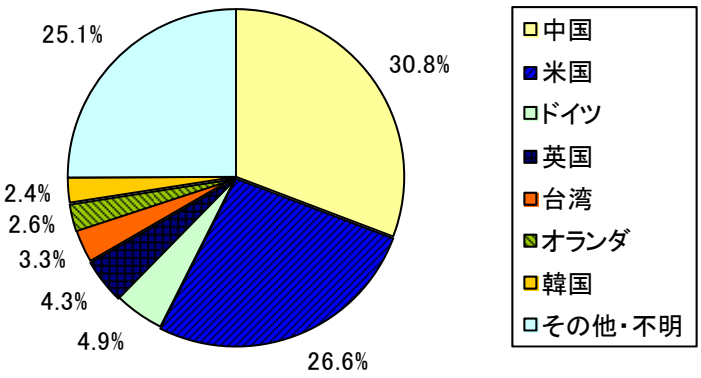

図 3-5 シグネチャを用いた不正侵入等の発信元国・地域別検知比率[1]

[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)

今期順位	前期順位	国・地域	今期件数[1]	前期比[1]
1 位	2 位	中国	2.11 件	＋3.7% （＋0.08 件）
2 位	1 位	米国	1.83 件	－11.6% （－0.24 件）
3 位	5 位	ドイツ	0.34 件	＋69.4% （＋0.14 件）
4 位	8 位	英国	0.30 件	＋88.9% （＋0.14 件）
5 位	3 位	台湾	0.23 件	－70.4% （－0.54 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	英国	0.30 件	＋88.9% （＋0.14 件）	4 位	8 位
2 位	ドイツ	0.34 件	＋69.4% （＋0.14 件）	3 位	5 位
3 位	中国	2.11 件	＋3.7% （＋0.08 件）	1 位	2 位
4 位	香港	0.09 件	＋90.7% （＋0.04 件）	14 位	16 位
5 位	オランダ	0.18 件	＋27.8% （＋0.04 件）	6 位	10 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	0.23 件	－70.4% （－0.54 件）	5 位	3 位
2 位	米国	1.83 件	－11.6% （－0.24 件）	2 位	1 位
3 位	欧州連合	0.13 件	－27.1% （－0.05 件）	10 位	6 位
4 位	韓国	0.16 件	－21.0% （－0.04 件）	7 位	4 位
5 位	ブラジル	0.10 件	－29.1% （－0.04 件）	13 位	11 位

[1] 一日・1IP アドレス当たり。

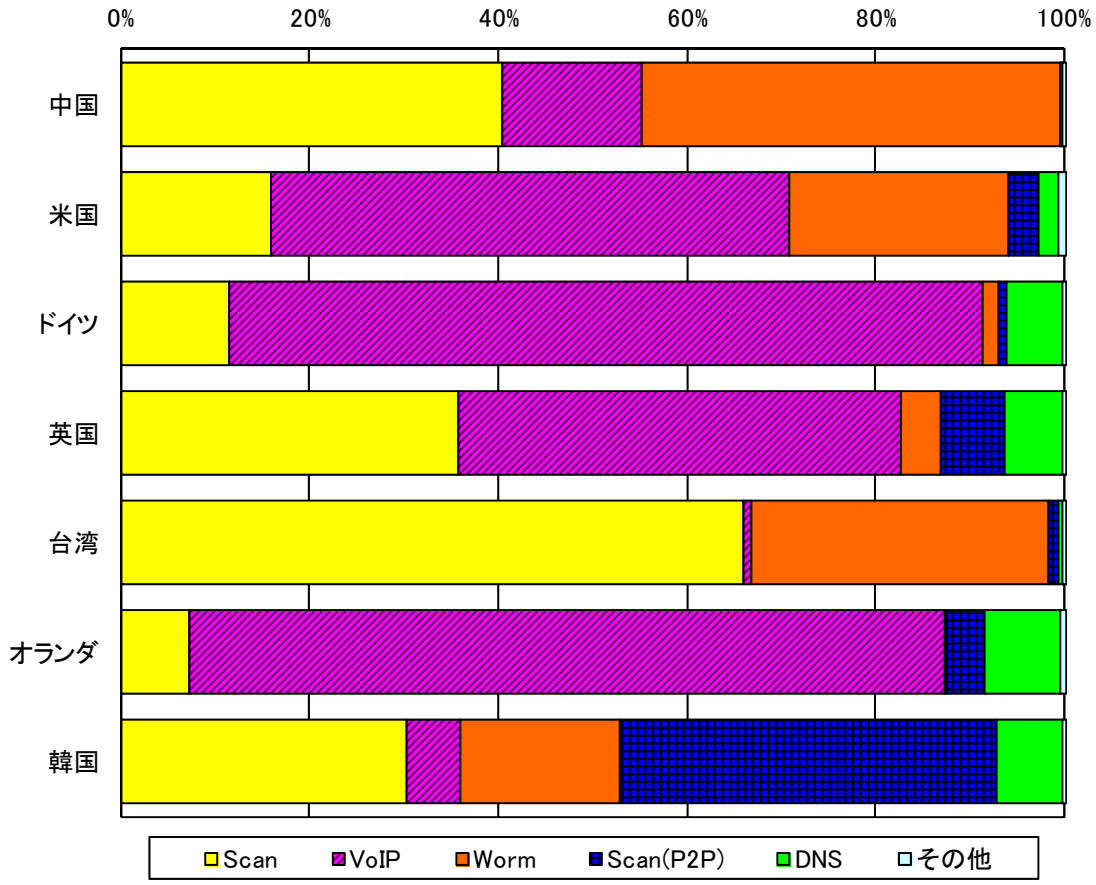

図 3-6　シグネチャを用いた不正侵入等の発信元国・地域別上位の攻撃手法別検知比率

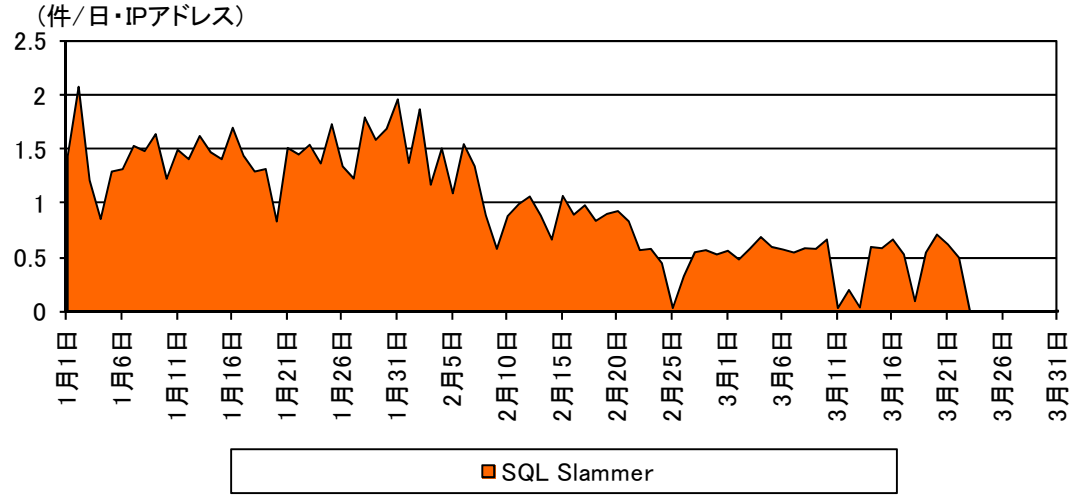

図 3-7　中国からの SQL Slammer の検知状況

4　インターネット定点観測 ― DoS 攻撃被害観測状況

4-1　DoS 攻撃被害観測状況

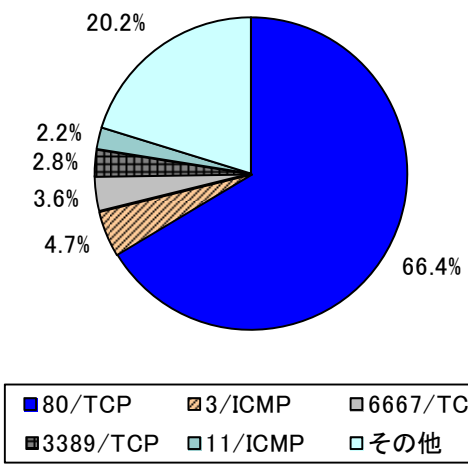

図 4-1　跳ね返りパケット発信元ポート別比率 [1]

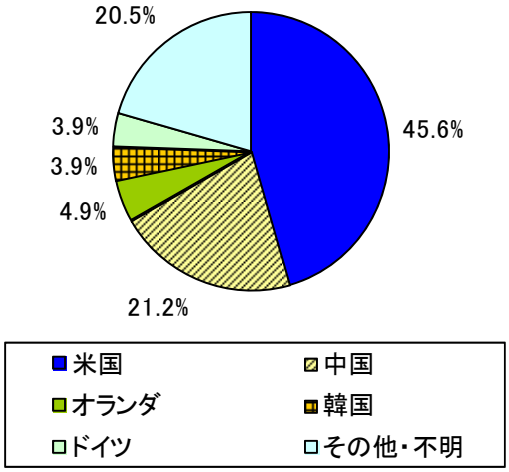

図 4-2　跳ね返りパケット発信元国・地域別比率 [1]

DoS 攻撃被害観測状況は、一日当たり 6,436.3 件で、前期と比較して 5,954.2 件（48.1%）減少した。発信元 IP アドレス数は一日当たり 390.5 個で、前期と比較して 158.4 個（68.3%）増加した。

80/TCPを発信元とする跳ね返りパケットを多数検知し、これが全体の 66.4%を占めていた(図 4-1)。検知件数は、一日当たり 4,275.7 件で、前期と比較して一日当たり 3,113.9 件（42.1%）減少した。

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 639.9 件(43.0%)増加した(表 4-1)。これは、1月から2月にかけて、米国の特定の 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)。一方、中国からの 80/TCP の跳ね返りパケットは、前期と比較して、一日当たり 3,658.0 件(78.3%)減少した。これは、前期に特定の IP アドレスから多くの跳ね返りパケットを観測しており、今期は、これらの跳ね返りパケットが見られなかったことが原因である。

今期2位の ICMP Destination Unreacheable（以下「3/ICMP」という。）は、サーバに到達不能な攻撃パケットに対する応答パケットであり、一日当たり 303.8 件で、前期と比較して一日当たり 124.5 件(69.4%)増加した。この 3/ICMP は、80/TCP や 53/UDP に対するものが多く見られ、ウェブサーバや DNS サーバに対する攻撃の跳ね返りパケットであると考えられる。

国際ハッカー集団「アノニマス」を名乗る者が、3月 31 日にルート DNS サーバに対して DoS 攻撃を行うことを予告したと報じられた。この攻撃予告との関連は不明であるが、3月下旬、複数のルート DNS サーバを発信元とした 53/UDP の跳ね返りパケットを9件検知した。これは何者かが発信元を偽り、名前解決の問い合わせを行ったことにより到達したパケットである可能性がある。

[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　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	2 位	米国	2,128.0 件	＋43.0%　（＋639.9 件）
2 位	1 位	中国	1,014.3 件	－78.3%　（－3658.0 件）
3 位	8 位	オランダ	219.3 件	＋172.0%　（＋138.7 件）
4 位	14 位	ドイツ	157.7 件	＋745.7%　（＋139.0 件）
5 位	3 位	ロシア	126.0 件	－66.9%　（－254.9 件）

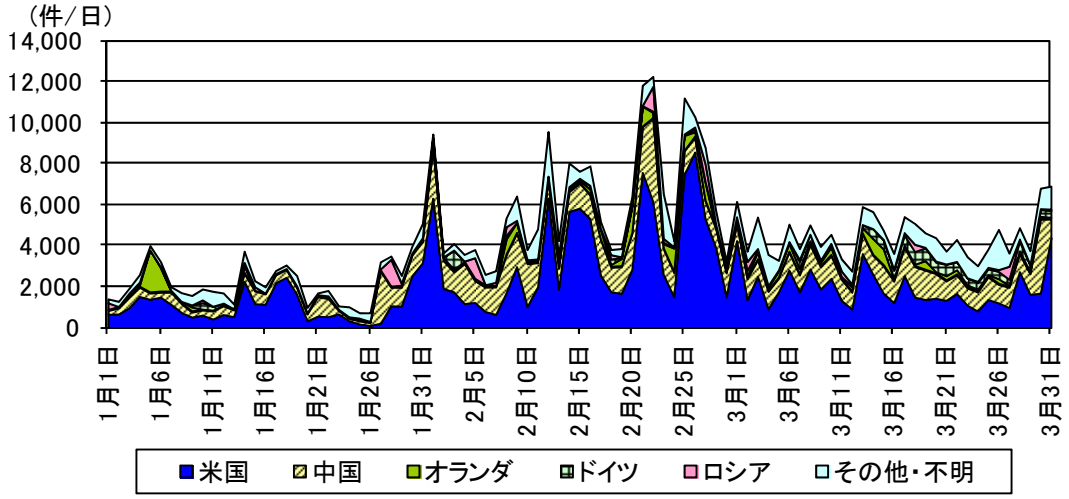

図 4-3　発信元ポート 80/TCP からの跳ね返りパケットの推移

[1] 一日・1IP アドレス当たり。

5　@police（Topics）掲載事項

@police において、平成24年1月から3月までの第4／四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	1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(MS12-001,002,003,004,005,006,007)
重要	1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	2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(MS12-008,009,010,011,012,013,014,015,016)
重要	2月16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	3月6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	3月14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(MS12-017,018,019,020,021,022)
重要	3月29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
●	3月29日	インターネット治安情勢更新(平成23年報を追加)

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

DoS 攻撃被害観測システムで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、ICMP Destination Unreachable 及び ICMP Time Exceeded（以下それぞれ「0/ICMP」、「3/ICMP」及び「11/ICMP」という。）も含め、より多くの攻撃手法での DoS 攻撃被害の観測に対応させた。

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
4-1　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3月 31 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