令和元年6月 21 日

令和元年5月期観測資料

1　観測結果概要

令和元年5月期（以下「今期」という。）に、インターネットとの接続点に設置したセンサーにおいて検知したアクセス件数は、一日・1IP アドレス当たり 3,595.9 件で、平成 31 年4月期（以下「前期」という。）と比較して 167.9 件（4.9%）増加しました。また、着信元（送信元）IP アドレス数は、一日当たり 41,070.0 個で、前期と比較して 2,467.5 個（5.7%）減少しました。

不正侵入等の行為（以下「不正侵入等」という。）のシグネチャを用いた検知件数は、一日・1IP アドレス当たり 1,017.7 件で、前期と比較して 129.3 件（11.3%）減少しました。また、着信元（送信元）IP アドレス数は、一日当たり 8,109.3 個で、前期と比較して 357.1 個（4.2%）減少しました。

DoS 攻撃被害検知件数は、一日当たり 20,758.5 件で、前期と比較して 5,628.1 件（37.2%）増加しました。また、着信元（送信元）IP アドレス数は、一日当たり 631.6 個で、前期と比較して 291.3 個（85.6%）増加しました。

2　センサーにおけるアクセス検知の観測結果

2-1　宛先ポート別アクセス検知件数

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[i]	前期比[i]
1 位	1 位	23/TCP	507.16 件	－1.4%　（－7.14 件）
2 位	2 位	445/TCP	402.69 件	－1.3%　（－5.30 件）
3 位	4 位	22/TCP	68.62 件	－2.2%　（－1.58 件）
4 位	11 位	37215/TCP	59.35 件	＋90.9%　（＋28.27 件）
5 位	5 位	80/TCP	50.75 件	－2.9%　（－1.52 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[i]	前期比[i]	今期順位	前期順位
1 位	37215/TCP	59.35 件	＋90.9%　（＋28.27 件）	4 位	11 位
2 位	5555/TCP	37.36 件	＋55.4%　（＋13.32 件）	11 位	13 位
3 位	65530/TCP	8.78 件	＋389.3%　（＋6.99 件）	29 位	129 位
4 位	3389/TCP	43.94 件	＋15.6%　（＋5.92 件）	6 位	10 位
5 位	8545/TCP	23.26 件	＋21.7%　（＋4.15 件）	15 位	19 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[i]	前期比[i]	今期順位	前期順位
1 位	52869/TCP	38.40 件	－56.3%　（－49.52 件）	10 位	3 位
2 位	9001/TCP	2.81 件	－87.4%　（－19.41 件）	77 位	14 位
3 位	123/UDP	26.99 件	－29.7%　（－11.42 件）	13 位	9 位
4 位	23/TCP	507.16 件	－1.4%　（－7.14 件）	1 位	1 位
5 位	53/UDP	9.96 件	－34.8%　（－5.32 件）	24 位	23 位

[i] 一日・1IP アドレス当たり。

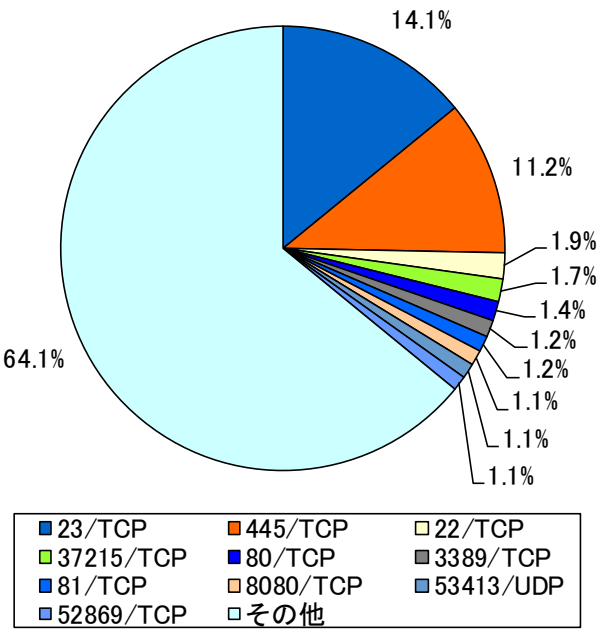

図 2-1　宛先ポート別比率（全て）[i]

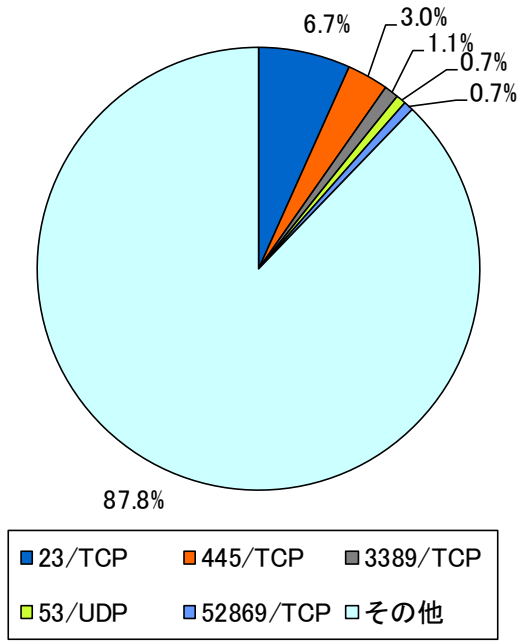

図 2-2　宛先ポート別比率（日本国内）

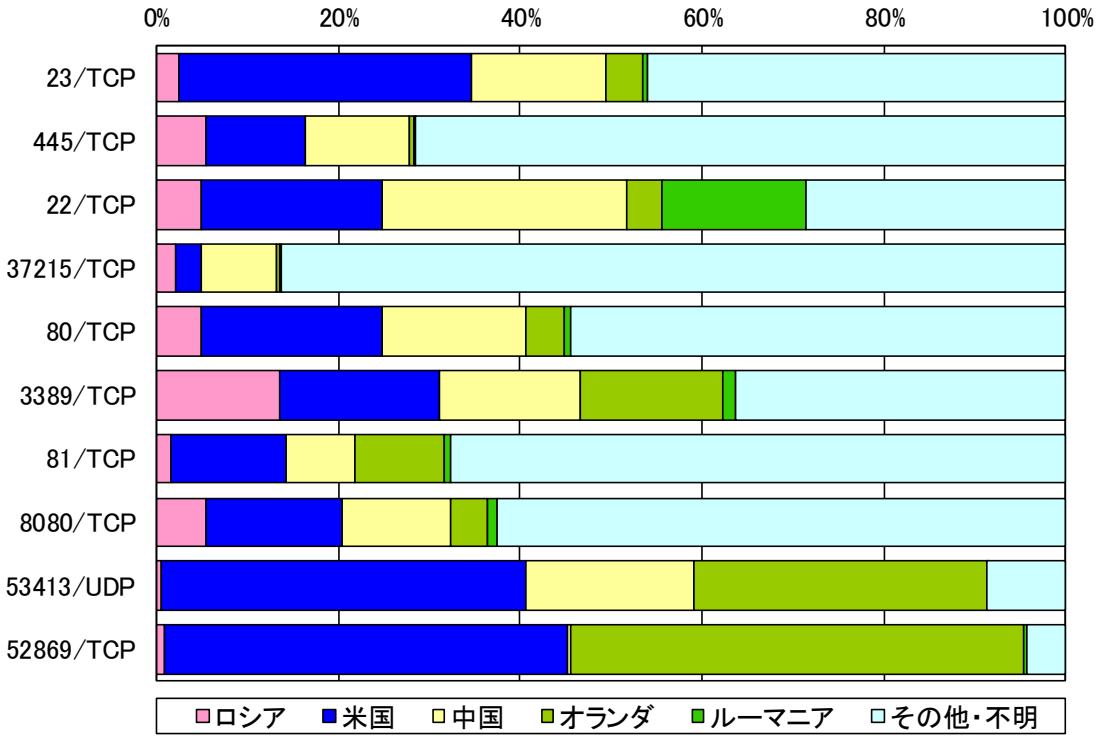

図 2-3　宛先ポート別上位の着信元国・地域別比率 [ii]

[i] 当データは、小数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ります。以降の円グラフも同様です。

[ii] 着信元国・地域については、判明した着信元（送信元）IP アドレスが当該国・地域に割り当てられていることを指しており、踏み台となっているなどにより、送信者の所在と一致していない場合があります。以降も同様の表記です。

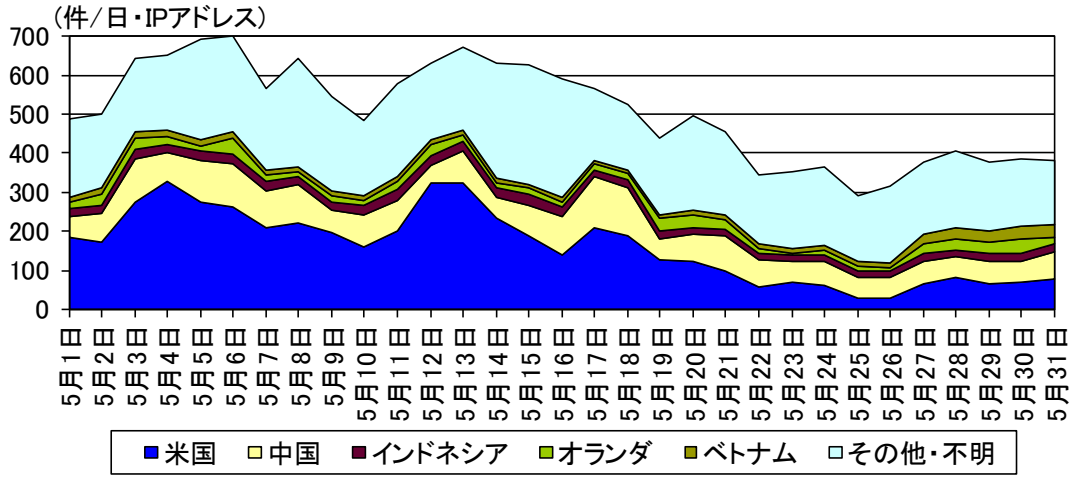

図 2-4　センサーのポート 23/TCP における検知件数の推移

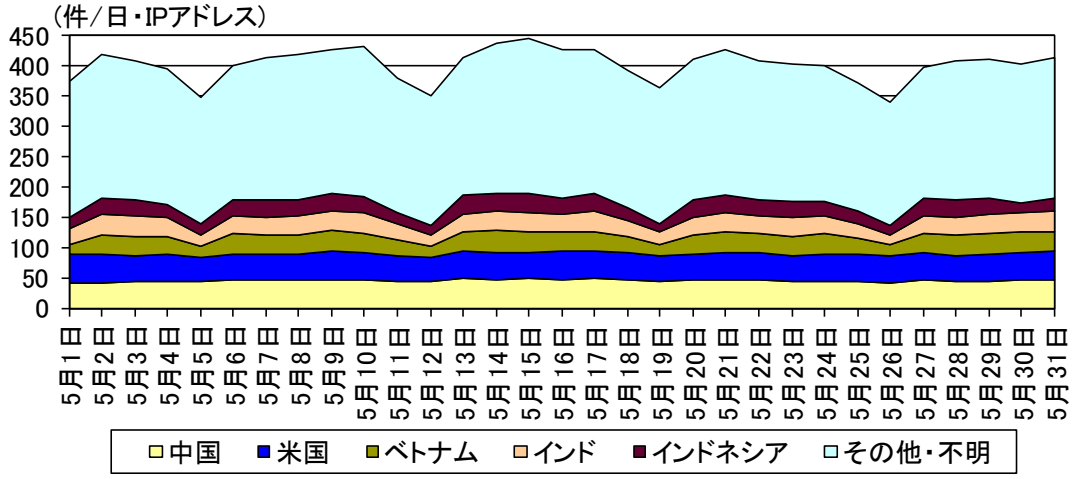

図 2-5　センサーのポート 445/TCP における検知件数の推移

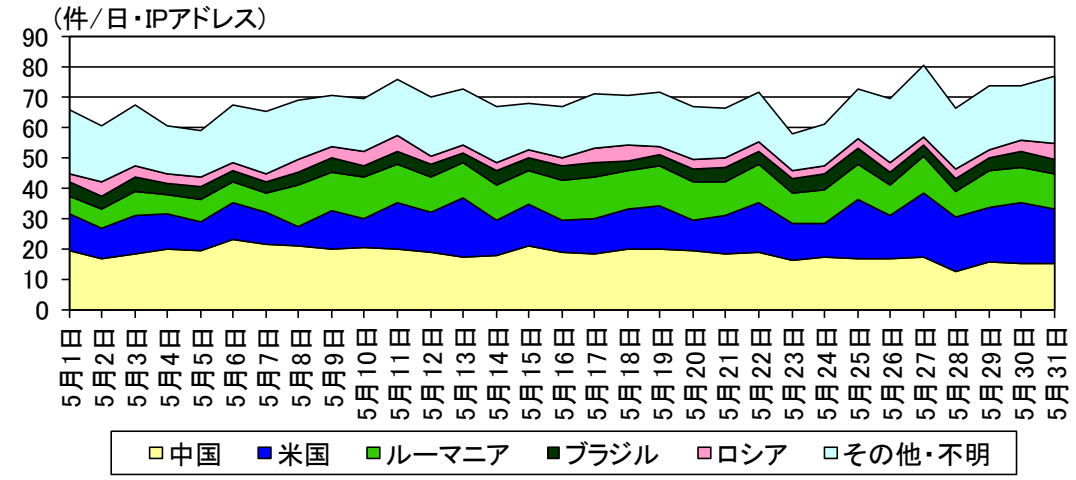

図 2-6　センサーのポート 22/TCP における検知件数の推移

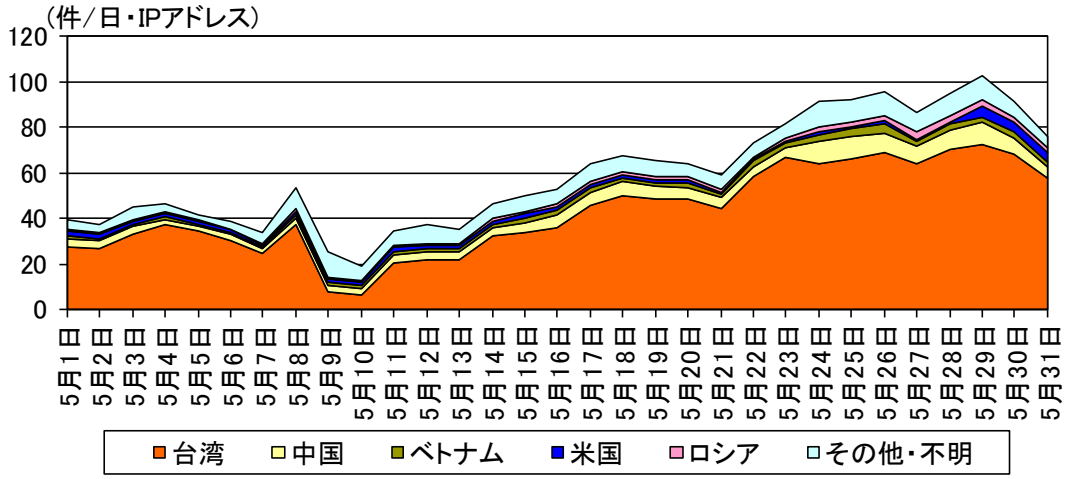

図 2-7　センサーのポート 37215/TCP における検知件数の推移

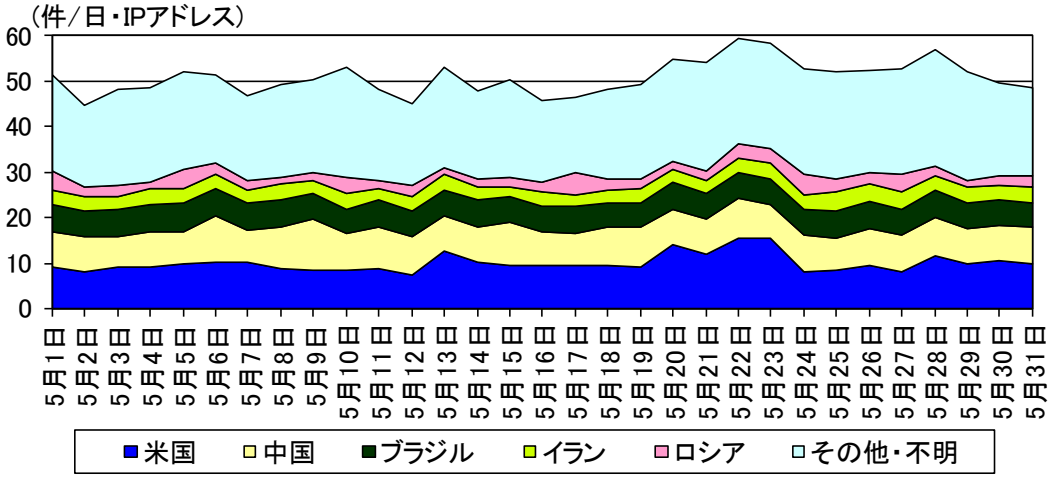

図 2-8　センサーのポート 80/TCP における検知件数の推移

2-2　着信元国・地域別アクセス検知件数

表 2-4　着信元国・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 [i]	前期比 [i]
1 位	1 位	ロシア	757.59 件	－13.6%　（－119.56 件）
2 位	2 位	米国	638.22 件	＋2.3%　（＋14.30 件）
3 位	3 位	中国	382.84 件	＋3.9%　（＋14.33 件）
4 位	4 位	オランダ	380.01 件	＋38.9%　（＋106.33 件）
5 位	5 位	ルーマニア	104.65 件	＋5.0%　（＋4.96 件）

表 2-5　着信元国・地域別検知件数（増加順位）

増加順位	国・地域	今期件数 [i]	前期比 [i]	今期順位	前期順位
1 位	オランダ	380.01 件	＋38.9%　（＋106.33 件）	4 位	4 位
2 位	英国	96.43 件	＋154.2%　（＋58.50 件）	6 位	18 位
3 位	フランス	84.13 件	＋111.0%　（＋44.26 件）	9 位	16 位
4 位	ウクライナ	37.06 件	＋194.1%　（＋24.46 件）	19 位	31 位
5 位	ドイツ	45.91 件	＋109.2%　（＋23.97 件）	15 位	22 位

表 2-6　着信元国・地域別検知件数（減少順位）

減少順位	国・地域	今期件数 [i]	前期比 [i]	今期順位	前期順位
1 位	ロシア	757.59 件	－13.6%　（－119.56 件）	1 位	1 位
2 位	イタリア	24.82 件	－56.3%　（－32.01 件）	22 位	13 位
3 位	南アフリカ	28.04 件	－33.6%　（－14.20 件）	20 位	15 位
4 位	韓国	47.72 件	－18.5%　（－10.84 件）	14 位	10 位
5 位	エジプト	18.87 件	－32.0%　（－8.87 件）	25 位	20 位

[i] 一日・1IP アドレス当たり。

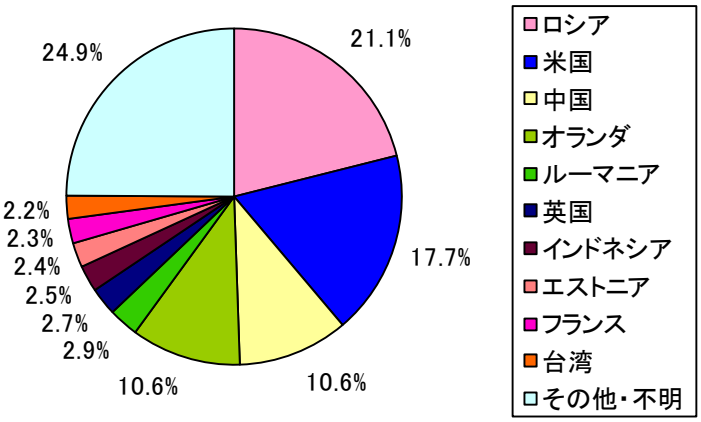

図 2-9　着信元国・地域別比率

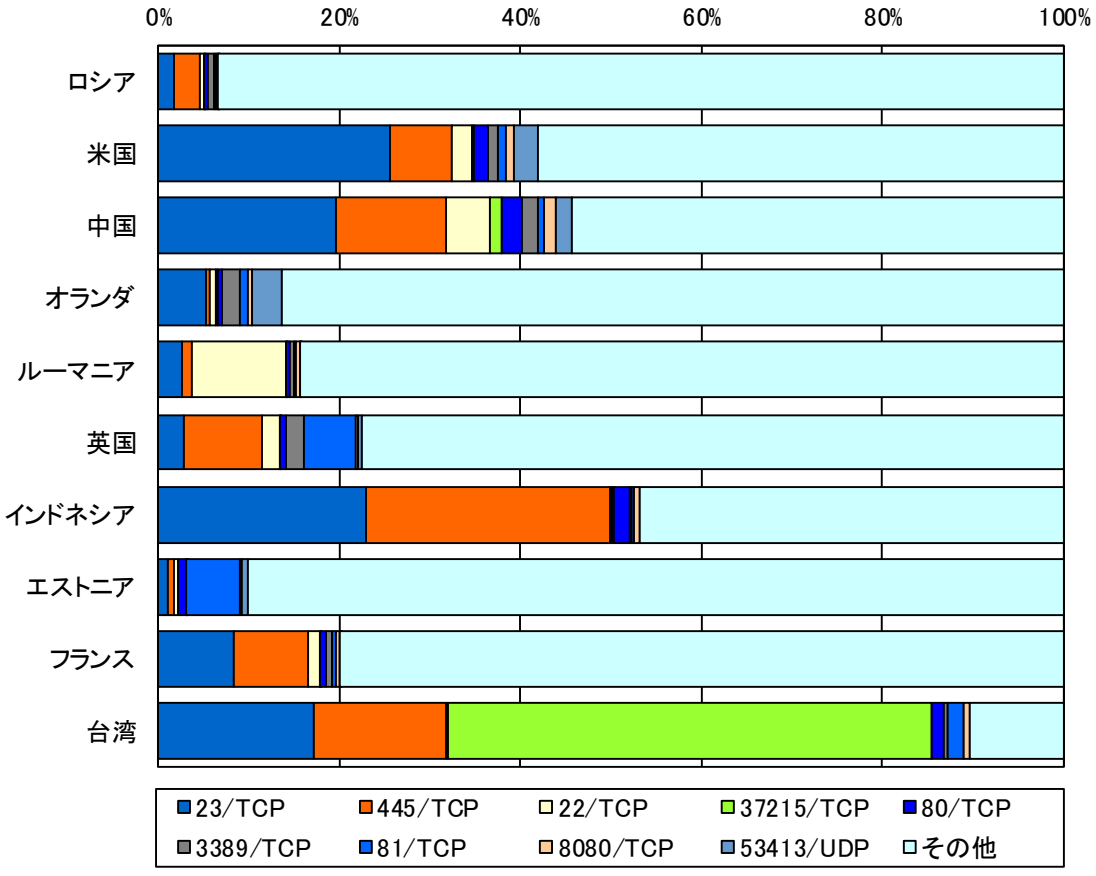

図 2-10　着信元国・地域別上位の宛先ポート別比率

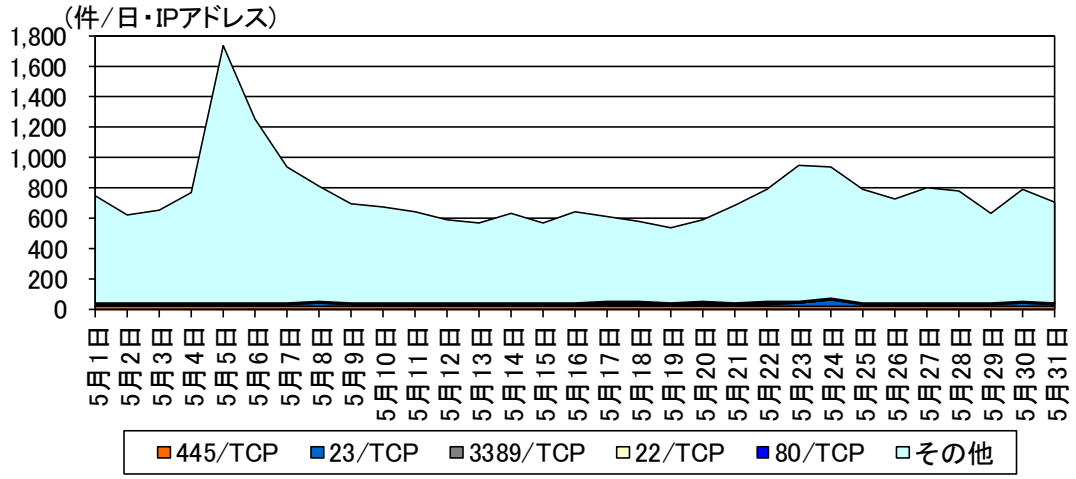

図 2-11　ロシアからの検知件数の推移

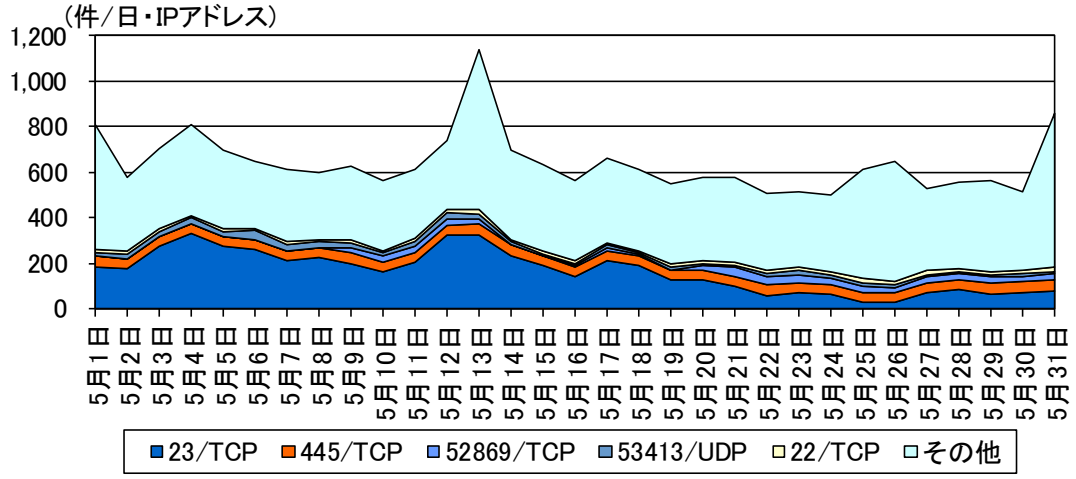

図 2-12　米国からの検知件数の推移

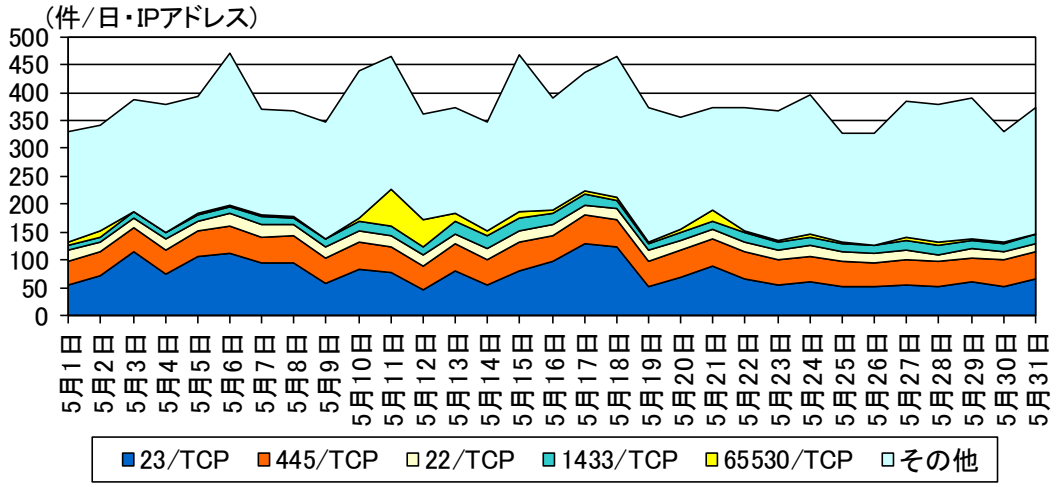

図 2-13　中国からの検知件数の推移

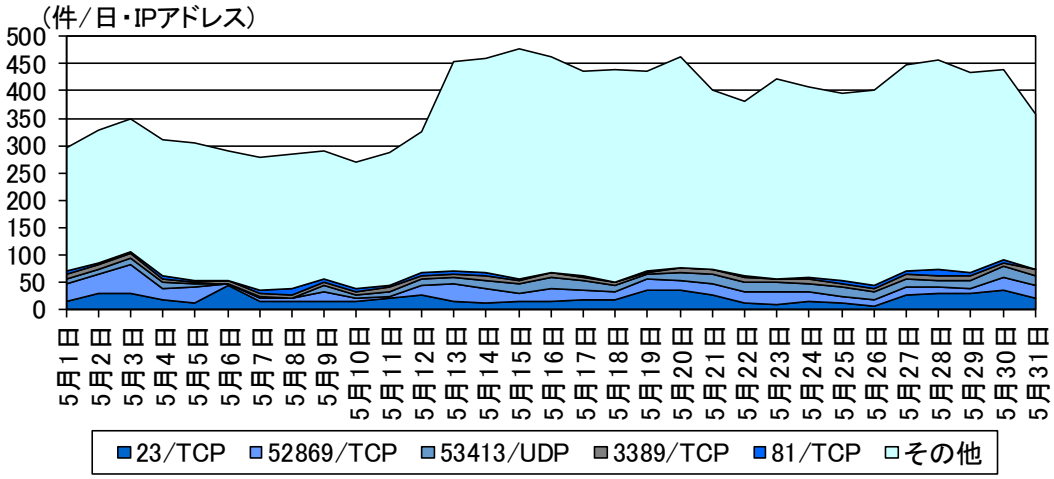

図 2-14　オランダからの検知件数の推移

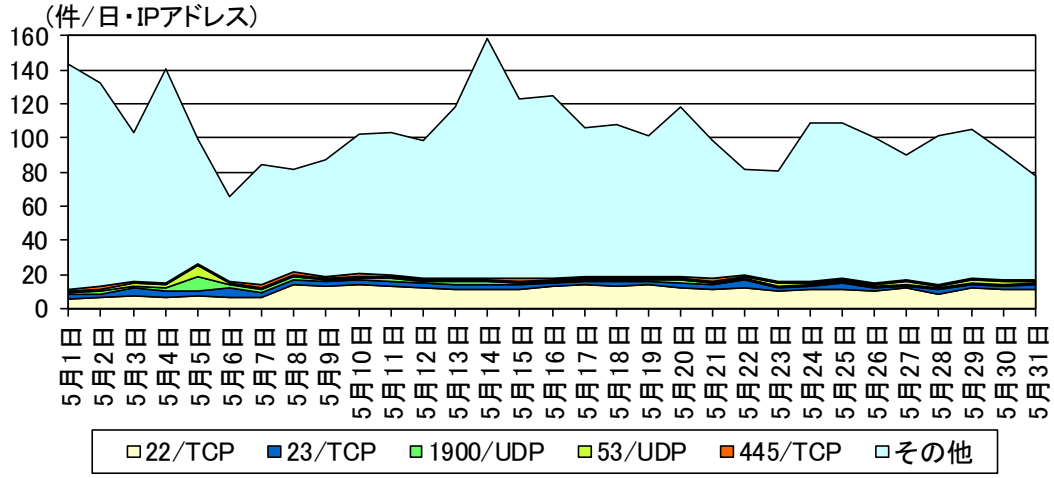

図 2-15　ルーマニアからの検知件数の推移

3　不正侵入等の観測結果

3-1　攻撃手法別アクセス検知件数

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 [i]	前期比 [i]	増加順位	減少順位
1 位	1 位	INDICATOR-SCAN	371.69 件	−20.2%　（−94.29 件）		1 位
2 位	2 位	Microsoft Windows Terminal server	281.82 件	−2.7%　（−7.71 件）		4 位
3 位	3 位	SMBv1	141.69 件	−9.9%　（−15.65 件）		2 位
4 位	4 位	Remote Desktop	97.86 件	−8.6%　（−9.20 件）		3 位
5 位	5 位	VOIP	31.67 件	+5.4%　（+1.62 件）	3 位	

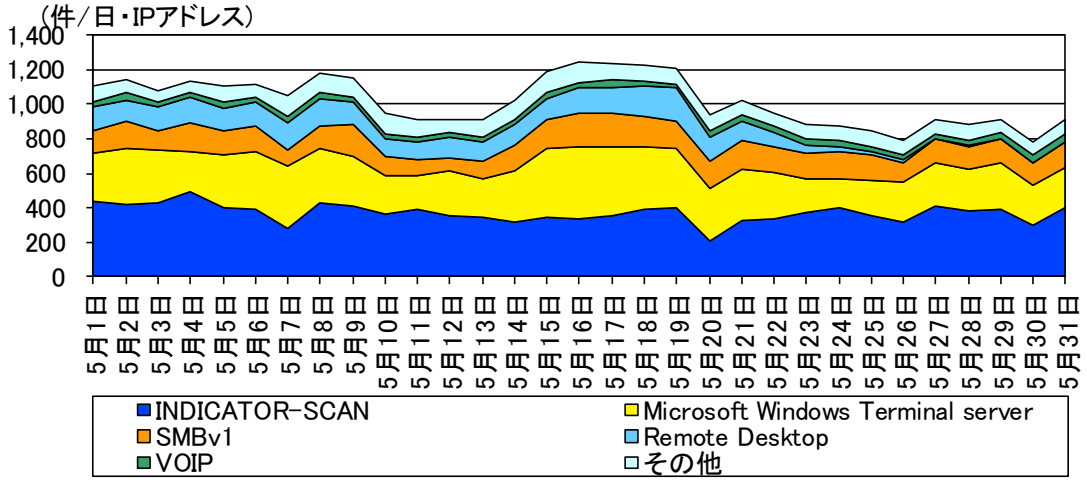

図 3-1　不正侵入等の攻撃手法別検知件数の推移

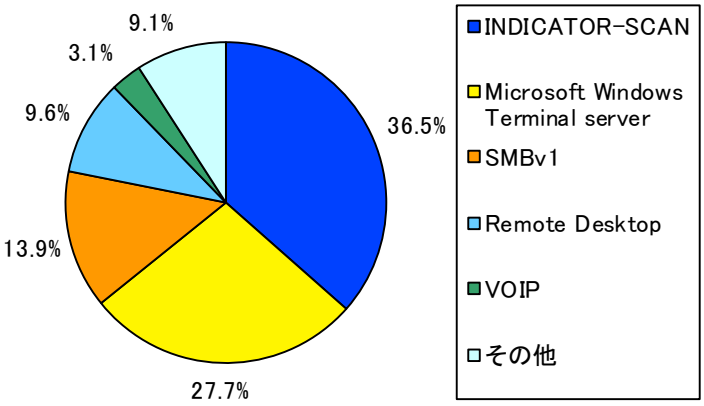

図 3-2　不正侵入等の攻撃手法別検知比率

[i] 一日・1IP アドレス当たり。

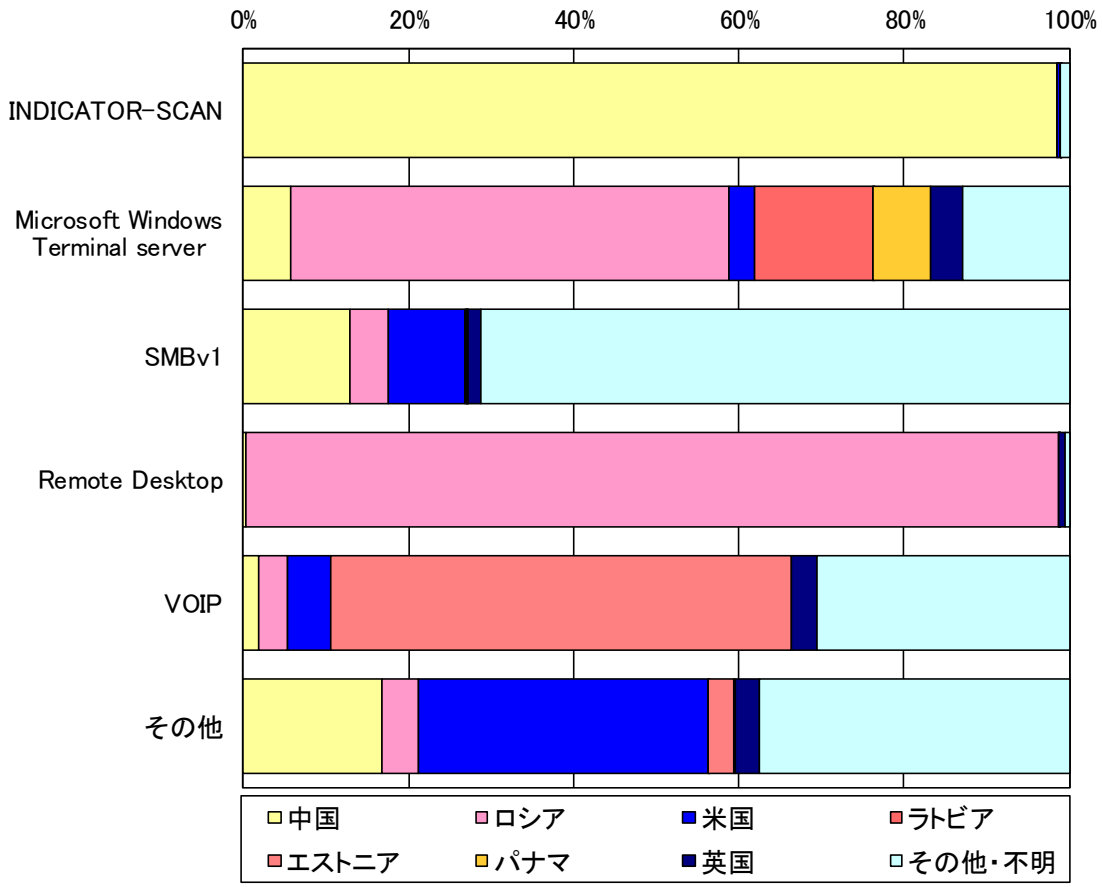

図 3-3　不正侵入等の攻撃手法の国・地域別検知比率

3-2 着信元国・地域別アクセス検知件数

表 3-2 不正侵入等の着信元国・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 [i]	前期比 [i]
1 位	1 位	中国	416.87 件	－18.7% （－95.70 件）
2 位	2 位	ロシア	257.43 件	＋9.0% （＋21.35 件）
3 位	3 位	米国	58.07 件	－12.6% （－8.38 件）
4 位	4 位	ラトビア	40.34 件	＋0.8% （＋0.33 件）
5 位	6 位	エストニア	20.67 件	＋0.0% （＋0.00 件）

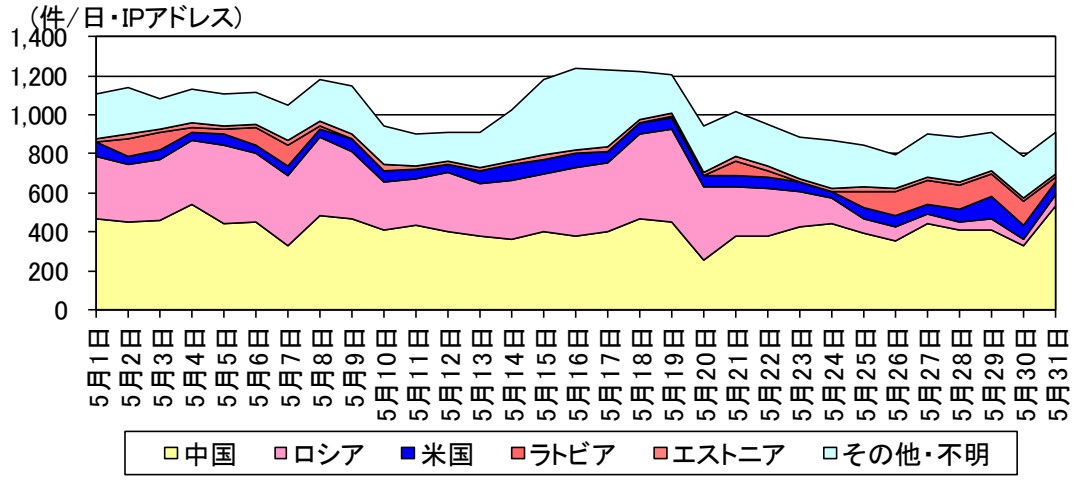

図 3-4 不正侵入等の着信元国・地域別検知件数の推移

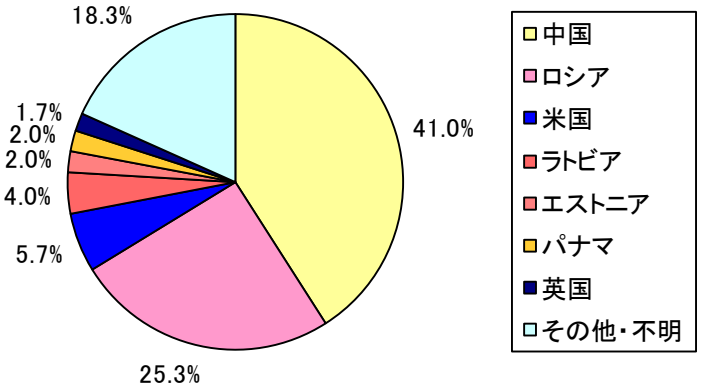

図 3-5 不正侵入等の着信元国・地域別検知比率

[i] 一日・1IP アドレス当たり。

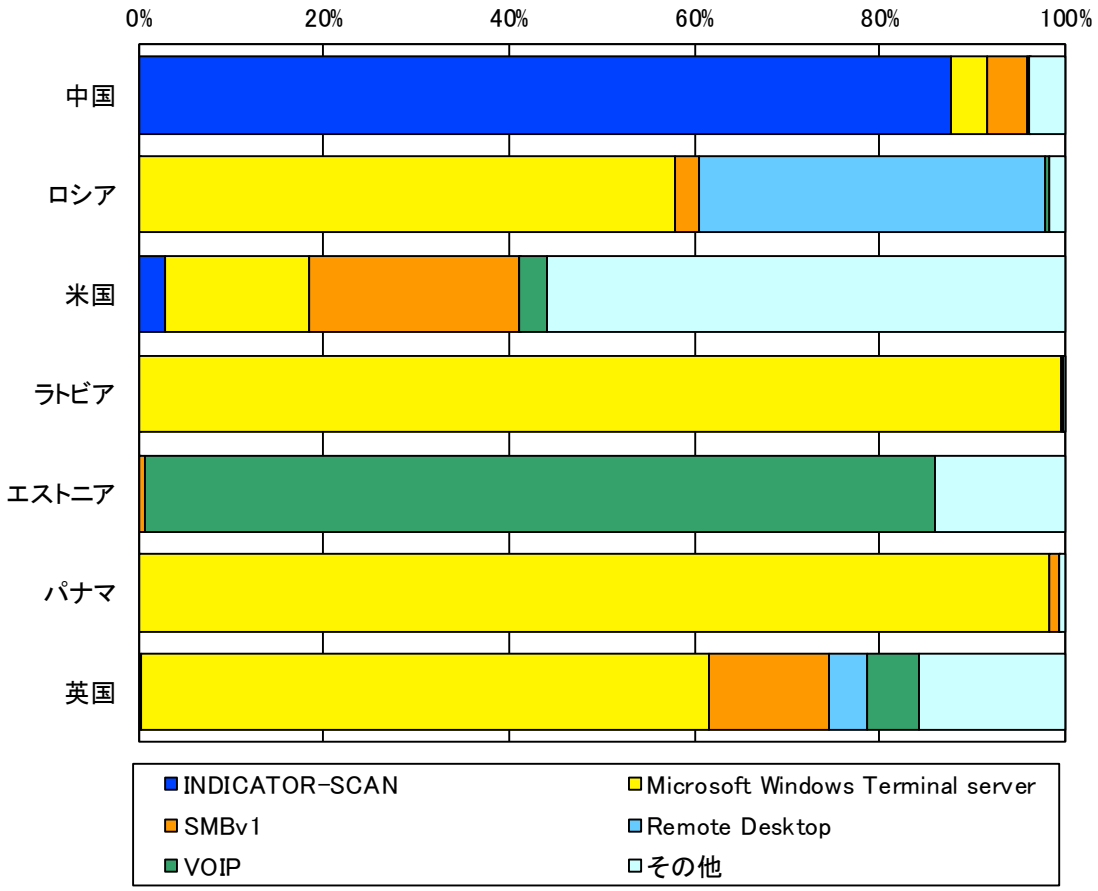

図 3-6 不正侵入等の着信元国・地域別上位の攻撃手法別検知比率

4　DoS 攻撃被害の観測結果

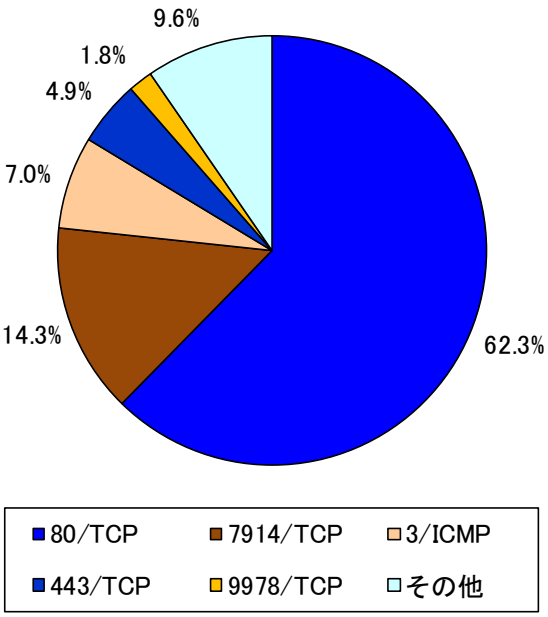

図 4-1　跳ね返りパケット着信元ポート別比率

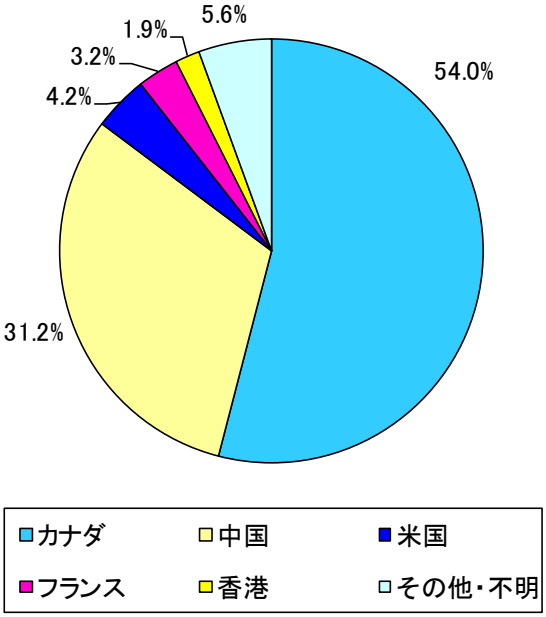

図 4-2　跳ね返りパケット着信元国・地域別比率

5　観測方法等

警察庁では、インターネット接続点に設置したセンサーにおいて検知したアクセス情報等を集約・分析した結果を観測結果として公表しています。その方法については、次のとおりです。

5-1　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ます（例「135/TCP」は TCP の 135 番ポートを表します。）。 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ます（例 「8/ICMP」は ICMP Echo Request を表します。）。

5-2　パケットの分類

センサーにおいて検知したパケットの分類は、表 5-1 に示す分類に従って集計しています。DoS 攻撃被害観測では、SYN/ACK 及び RST/ACK パケットに加えて、ICMP Echo Reply（以下「0/ICMP」という。）、ICMP Destination Unreachable（以下「3/ICMP」という。）及び ICMP Time Exceeded（以下「11/ICMP」という。）を集計対象としています。

表 5-1　パケットの分類

章	集計対象	
2 センサーにおけるアクセス検知の観測結果	センサーにおいて検知したアクセス	● 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 DoS 攻撃被害の観測結果	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

5-3　不正侵入等の検知

検知された各シグネチャ は、表 5-2 に示す分類に従って集約・分析しています。また、各センサーには、攻撃対象となる可能性のあるサーバ等の機器は一切接続していません。

表 5-2 シグネチャによる検知の分類

分類	説明
ICMP	ICMP パケットの検知
INDICATOR-SCAN	インターネット上の各種サービスに対するスキャン活動等の検知
Microsoft Windows Terminal server	Windows ターミナルサービスに対するスキャン活動等の検知
OS-WINDOWS	Windows OS のサービスに対する攻撃の検知
Remote Desktop	リモートデスクトップサービスに対する攻撃の検知
SERVER-WEBAPP	ウェブアプリケーションに対する攻撃の検知
SMBv1	SMBv1 に対するスキャン活動等の検知
SNMP	SNMP に対するスキャン活動等の検知
SSLv3	SSLv3 に対するスキャン活動等の検知
VOIP	VOIP に対するスキャン活動等の検知
Others	上記の分類に含まれないもの