令和元年7月 19 日

令和元年6月期観測資料

1　観測結果概要

令和元年6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 3,727.2 件で、令和元年5月期（以下「前期」という。）と比較して 131.3 件（3.7%）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 40,889.0 個で、前期と比較して 181.1 個（0.4%）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 663.4 件で、前期と比較して 354.2 件（34.8%）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 7,659.3 個で、前期と比較して 450.0 個（5.5%）減少しました。

DoS 攻撃被害検知件数は、一日当たり 4,426.8 件で、前期と比較して 16,331.7 件（78.7%）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 253.3 個で、前期と比較して 378.3 個（59.9%）減少しました。

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	574.51 件	＋13.3%	（＋67.34 件）
2 位	2 位	445/TCP	394.39 件	－2.1%	（－8.30 件）
3 位	3 位	22/TCP	83.27 件	＋21.4%	（＋14.66 件）
4 位	4 位	37215/TCP	73.19 件	＋23.3%	（＋13.84 件）
5 位	5 位	80/TCP	53.71 件	＋5.8%	（＋2.95 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	23/TCP	574.51 件	＋13.3%	（＋67.34 件）	1 位	1 位
2 位	5500/TCP	30.47 件	－[ii]	（＋29.86 件）	13 位	－[ii]
3 位	5038/TCP	31.65 件	＋90.0%	（＋14.99 件）	12 位	21 位
4 位	22/TCP	83.27 件	＋21.4%	（＋14.66 件）	3 位	3 位
5 位	37215/TCP	73.19 件	＋23.3%	（＋13.84 件）	4 位	4 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	123/UDP	12.99 件	－51.9%	（－14.00 件）	24 位	13 位
2 位	81/TCP	33.20 件	－20.5%	（－8.54 件）	11 位	7 位
3 位	445/TCP	394.39 件	－2.1%	（－8.30 件）	2 位	2 位
4 位	3389/TCP	37.50 件	－14.7%	（－6.44 件）	10 位	6 位
5 位	65530/TCP	2.59 件	－70.5%	（－6.19 件）	－[iii]	29 位

[i] 一日・1IP アドレス当たり。

[ii] 前期のアクセス件数が僅かなため、前期比及び前期順位は記載していません。

[iii] 今期のアクセス件数が僅かなため、今期順位は記載していません。

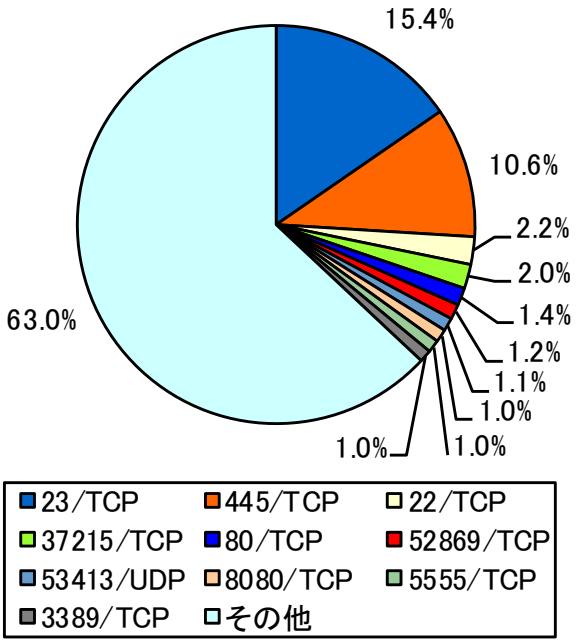


図 2-1　宛先ポート別比率（全て）[i]

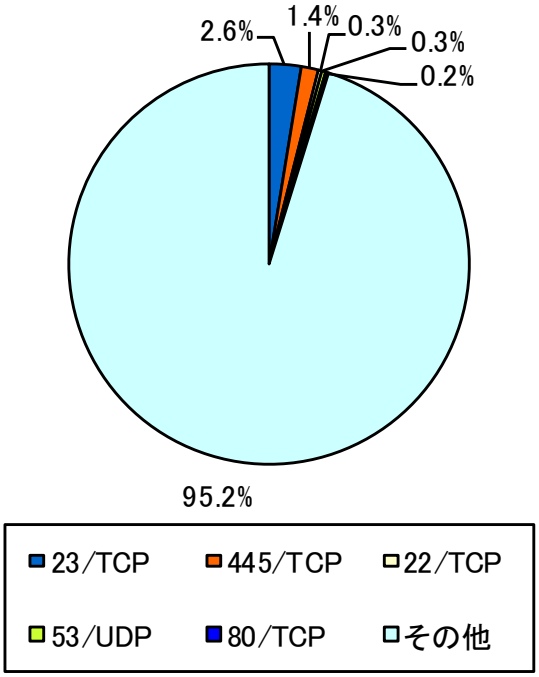


図 2-2　宛先ポート別比率（日本国内）

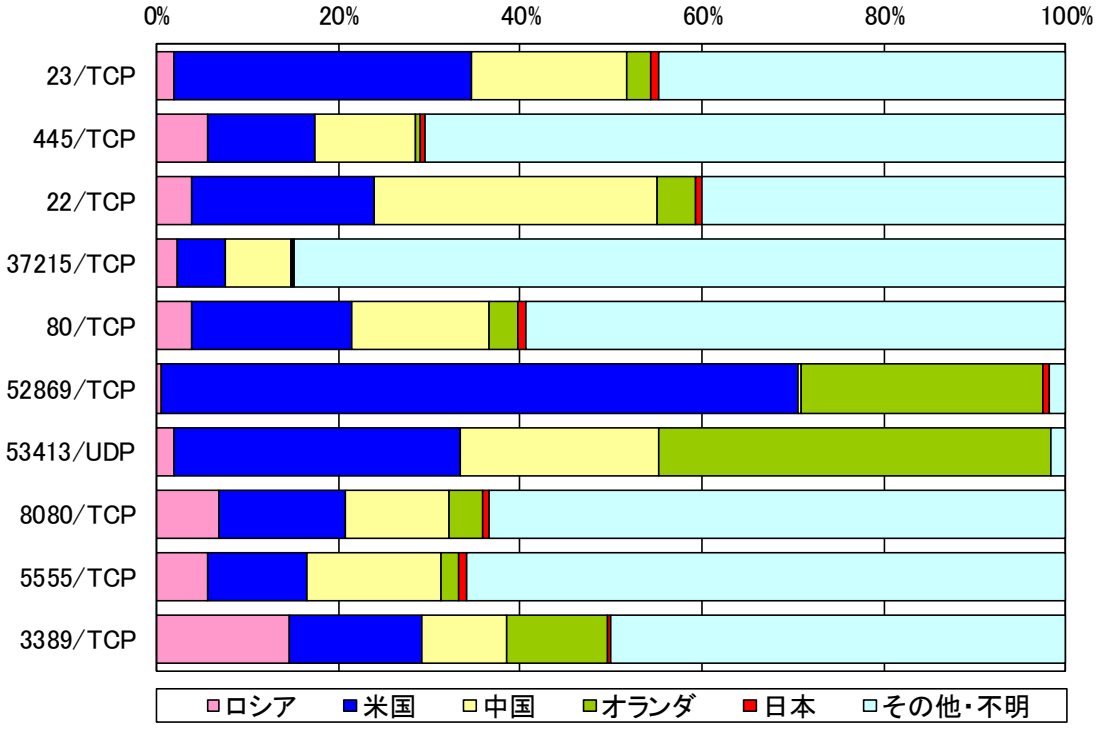


図 2-3　宛先ポート別上位の着信元国・地域別比率 [ii]

[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。

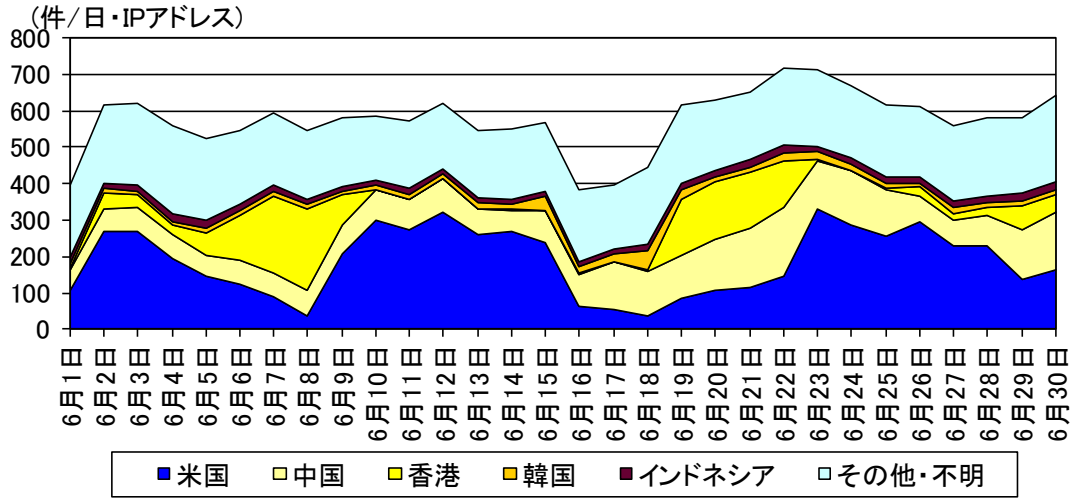


図 2-4　センサーのポート 23/TCP における検知件数の推移

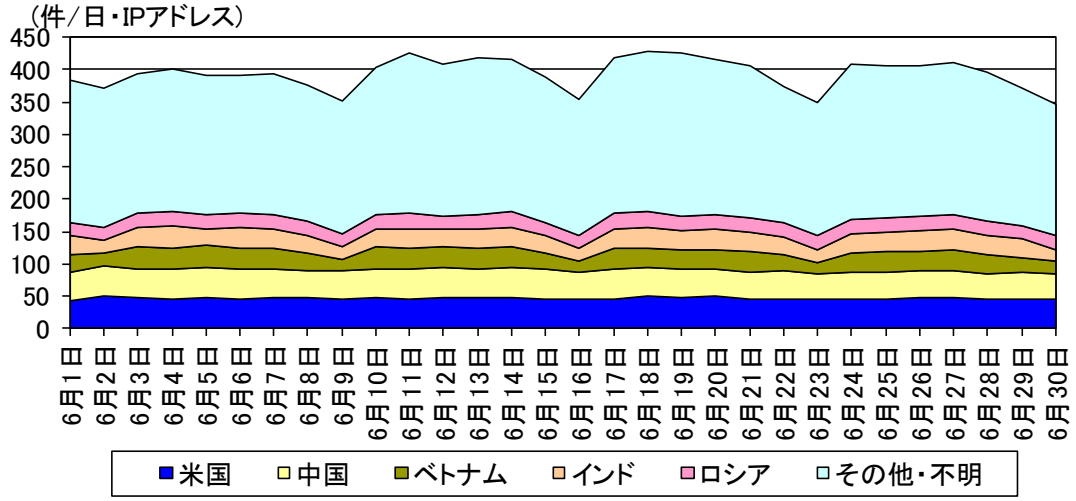


図 2-5　センサーのポート 445/TCP における検知件数の推移

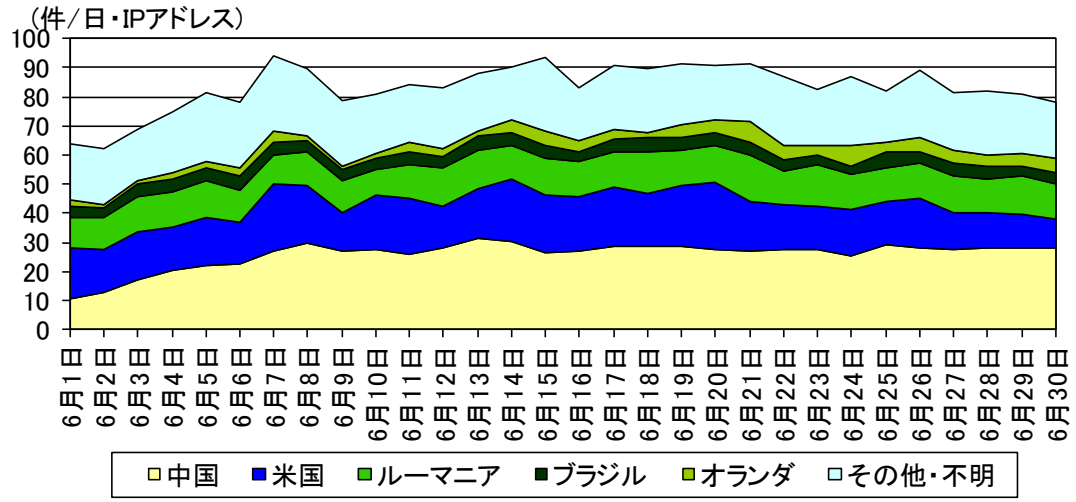


図 2-6　センサーのポート 22/TCP における検知件数の推移

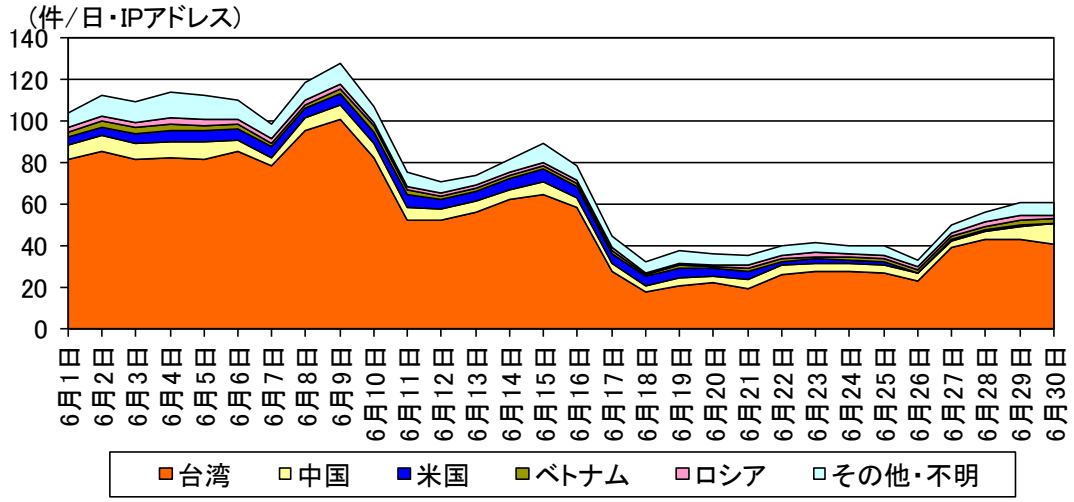


図 2-7　センサーのポート 37215/TCP における検知件数の推移

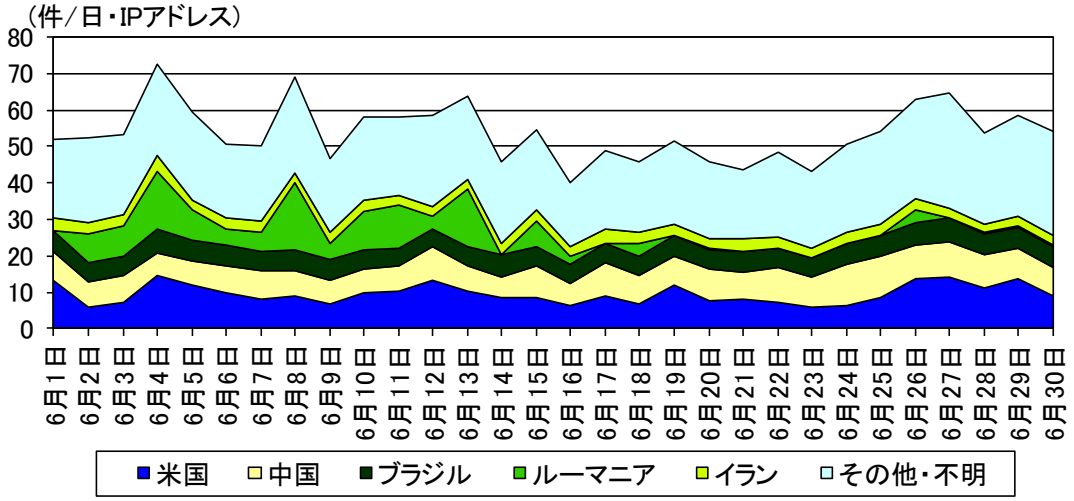


図 2-8　センサーのポート 80/TCP における検知件数の推移

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	774.04 件	＋2.2%	（＋16.45 件）
2 位	2 位	米国	662.63 件	＋3.8%	（＋24.41 件）
3 位	3 位	中国	416.09 件	＋8.7%	（＋33.25 件）
4 位	4 位	オランダ	365.05 件	－3.9%	（－14.96 件）
5 位	11 位	日本	183.18 件	＋144.4%	（＋108.24 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	日本	183.18 件	＋144.4%	（＋108.24 件）	5 位	11 位
2 位	香港	78.10 件	＋109.5%	（＋40.82 件）	9 位	18 位
3 位	中国	416.09 件	＋8.7%	（＋33.25 件）	3 位	3 位
4 位	エストニア	117.21 件	＋37.2%	（＋31.80 件）	6 位	8 位
5 位	米国	662.63 件	＋3.8%	（＋24.41 件）	2 位	2 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	英国	43.32 件	－55.1%	（－53.10 件）	17 位	6 位
2 位	フランス	45.82 件	－45.5%	（－38.31 件）	15 位	9 位
3 位	オランダ	365.05 件	－3.9%	（－14.96 件）	4 位	4 位
4 位	インドネシア	77.12 件	－15.2%	（－13.84 件）	10 位	7 位
5 位	ルーマニア	91.03 件	－13.0%	（－13.62 件）	8 位	5 位

[i] 一日・1IP アドレス当たり。

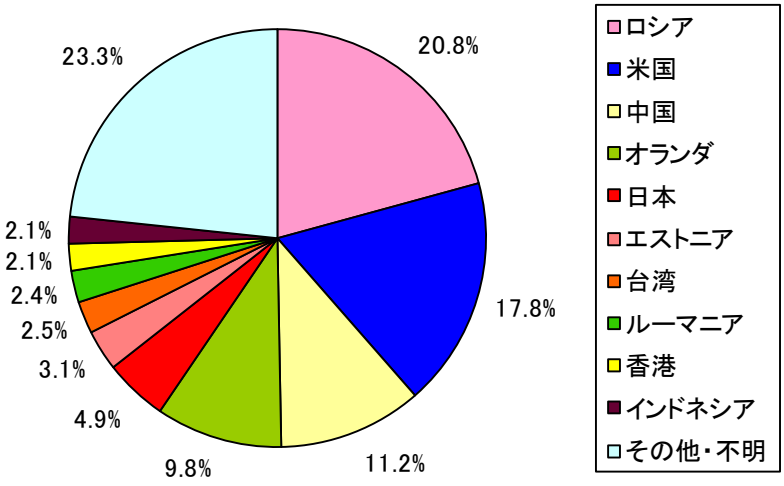


図 2-9　着信元国・地域別比率

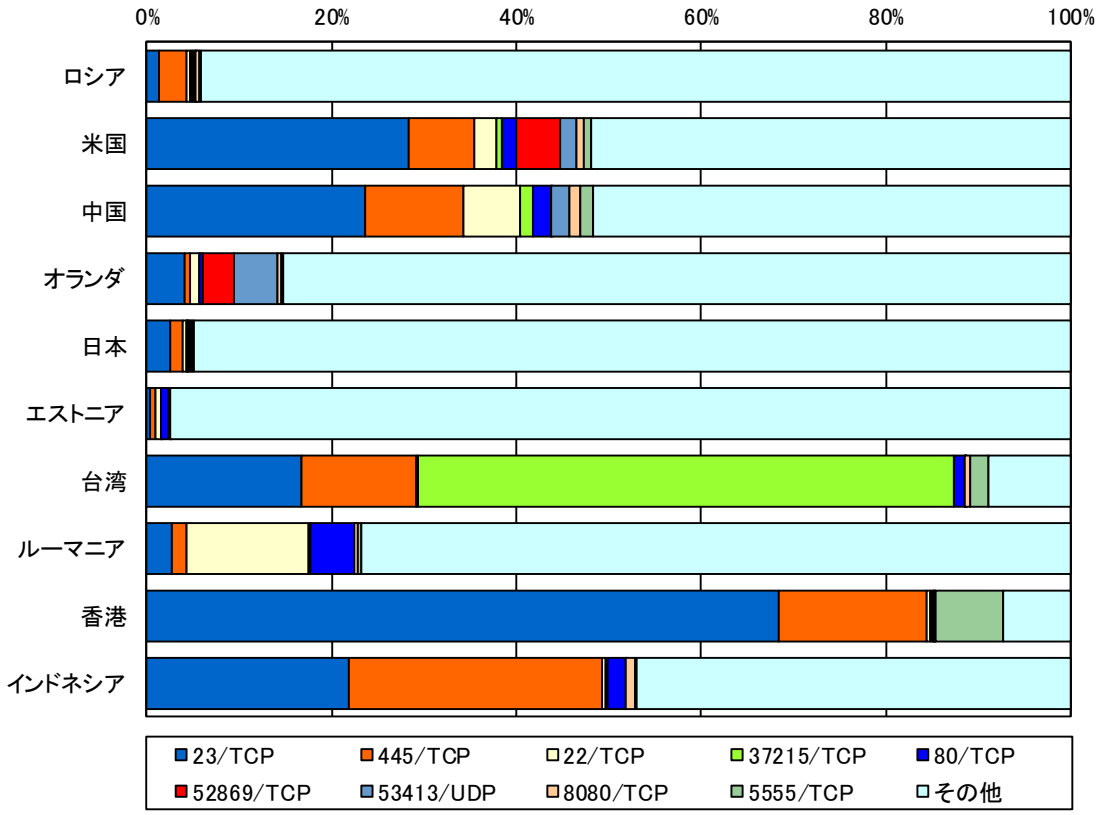


図 2-10　着信元国・地域別上位の宛先ポート別比率

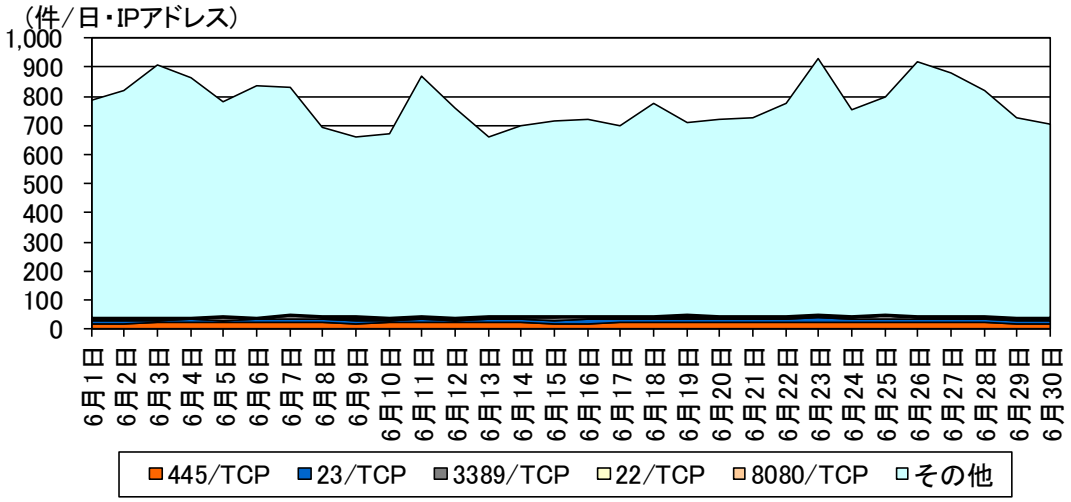


図 2-11　ロシアからの検知件数の推移

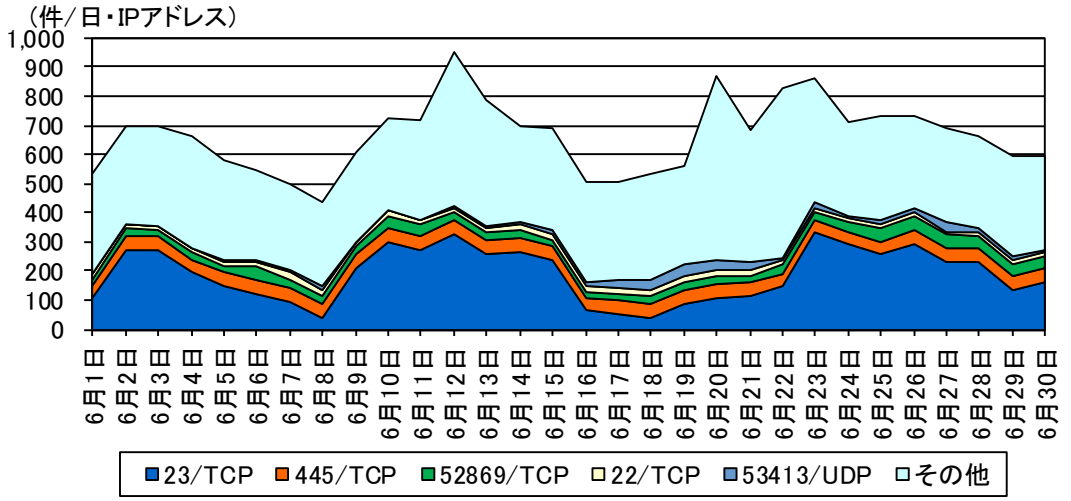


図 2-12　米国からの検知件数の推移

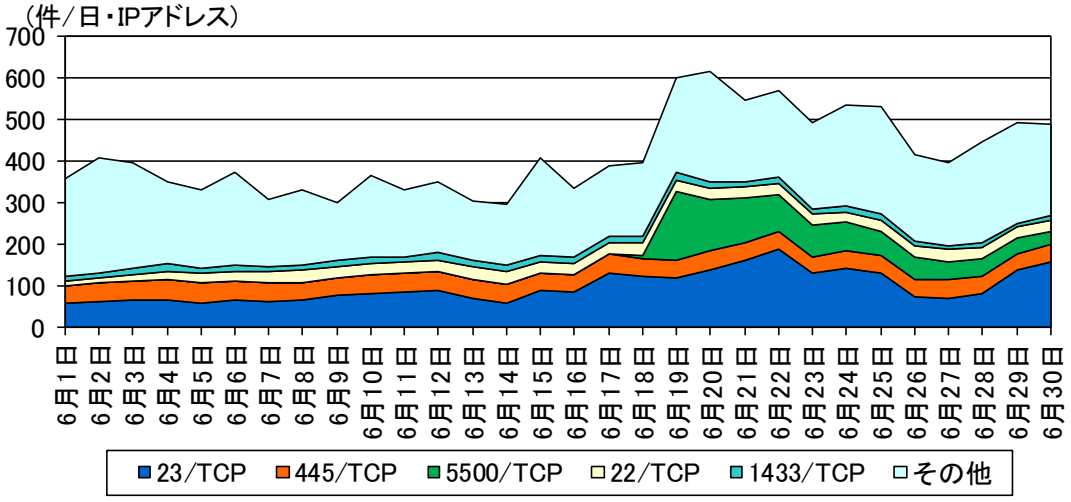


図 2-13　中国からの検知件数の推移

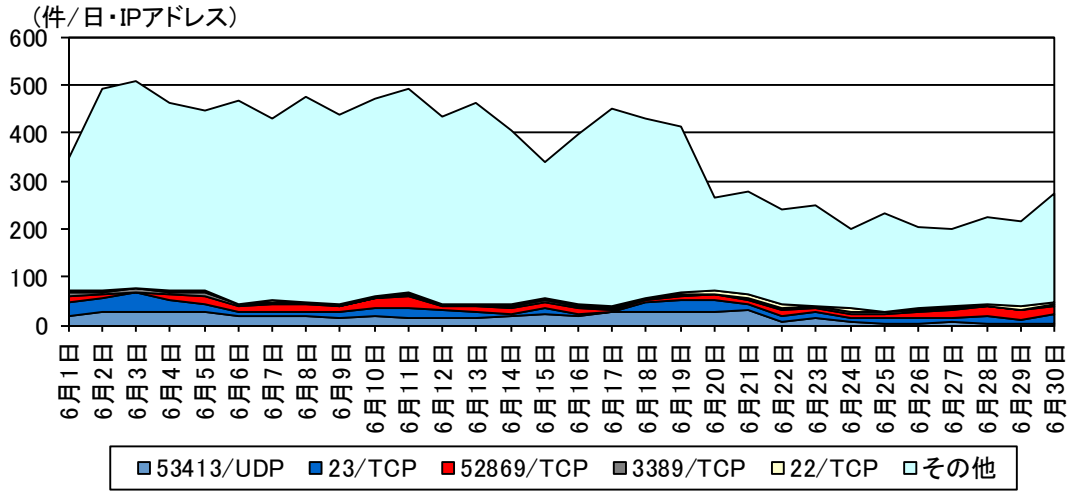


図 2-14　オランダからの検知件数の推移

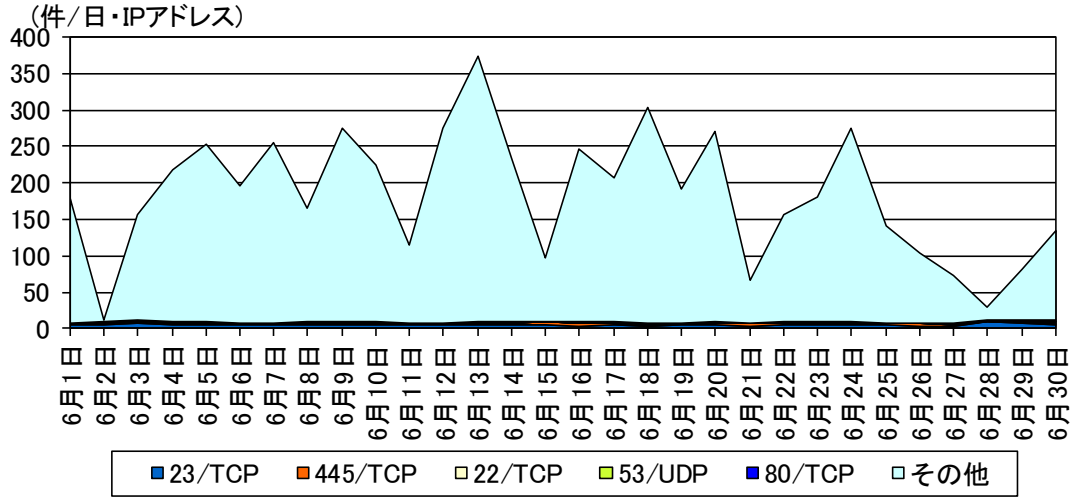


図 2-15　日本からの検知件数の推移

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	236.26 件	−36.4%　（−135.43 件）		1 位
2 位	2 位	Microsoft Windows Terminal server	180.71 件	−35.9%　（−101.10 件）		2 位
3 位	3 位	SMBv1	125.19 件	−11.6%　（−16.50 件）		4 位
4 位	5 位	VOIP	33.03 件	＋4.3%　（＋1.36 件）	4 位	
5 位	6 位	ICMP	18.07 件	−15.5%　（−3.32 件）		

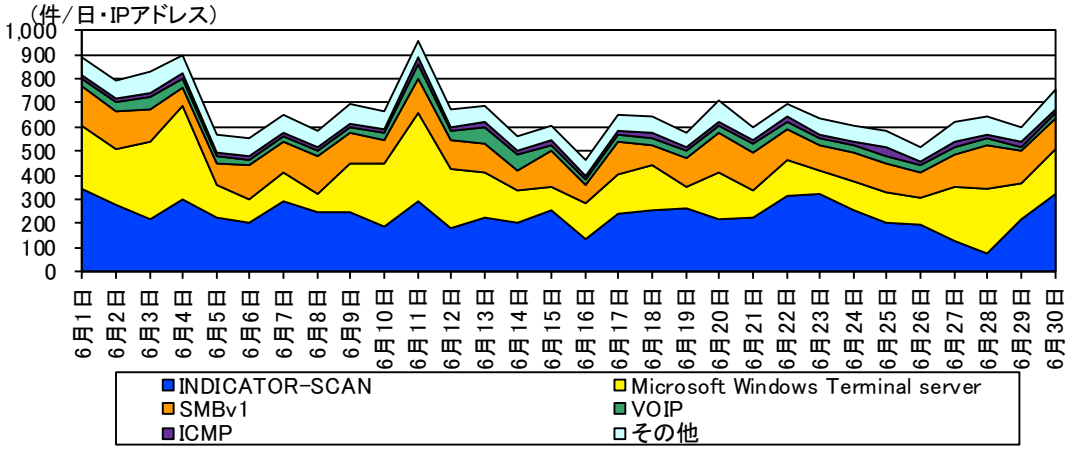


図 3-1　不正侵入等の攻撃手法別検知件数の推移

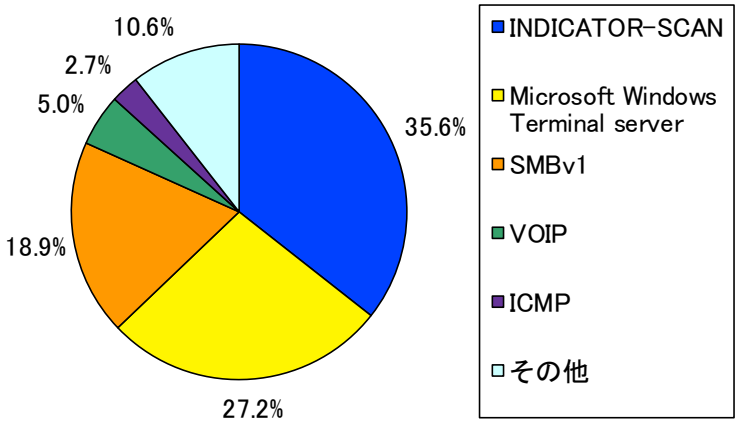


図 3-2　不正侵入等の攻撃手法別検知比率

[i] 一日・1IP アドレス当たり。

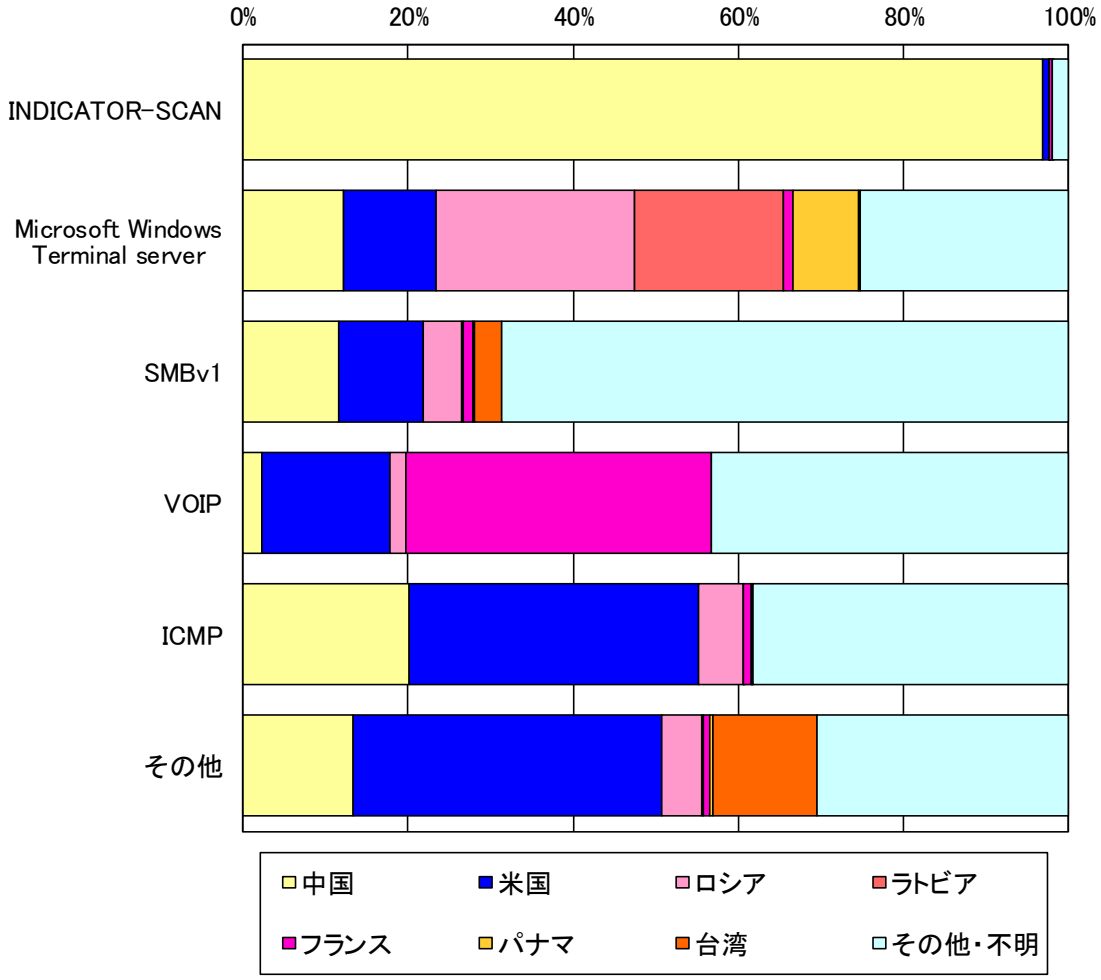


図 3-3　不正侵入等の攻撃手法の国・地域別検知比率

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	279.50 件	−33.0%	（−137.37 件）
2 位	3 位	米国	72.43 件	＋24.7%	（＋14.37 件）
3 位	2 位	ロシア	54.49 件	−78.8%	（−202.94 件）
4 位	4 位	ラトビア	32.52 件	−19.4%	（−7.82 件）
5 位	16 位	フランス	17.72 件	＋153.7%	（＋10.74 件）

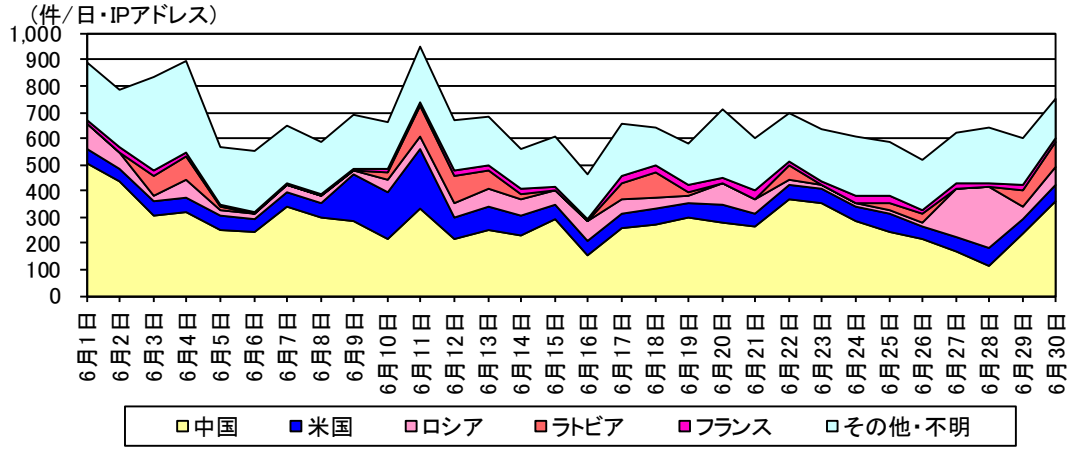
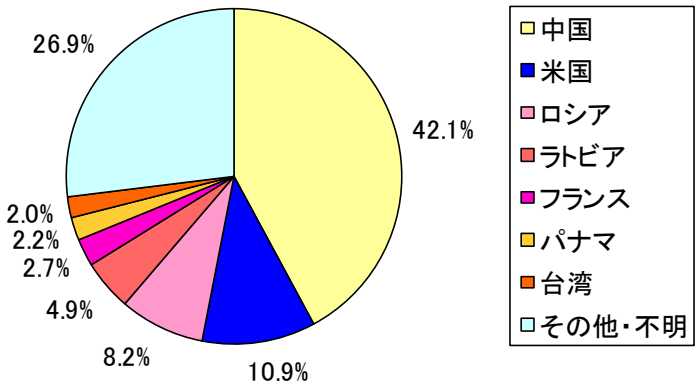


図 3-4 不正侵入等の着信元国・地域別検知件数の推移



[i]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。

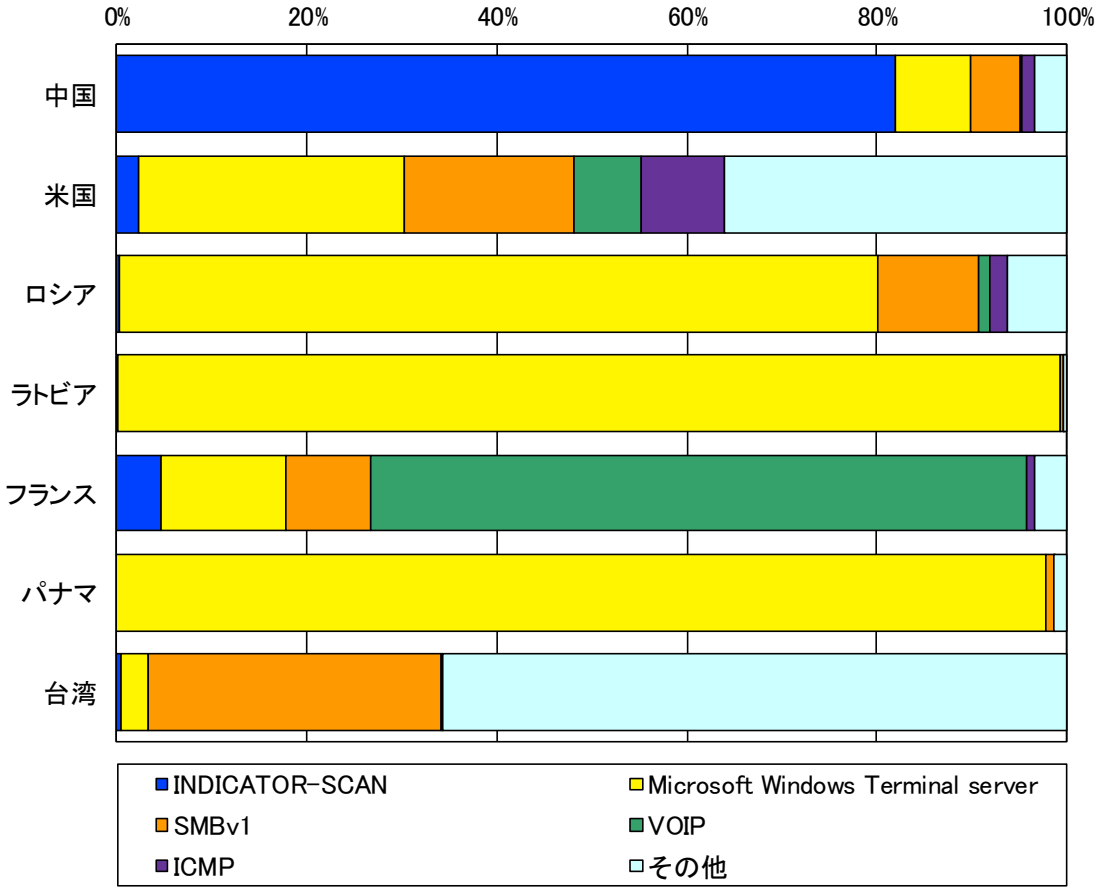


図 3-6　不正侵入等の着信元国・地域別上位の攻撃手法別検知比率

4　DoS 攻撃被害の観測結果

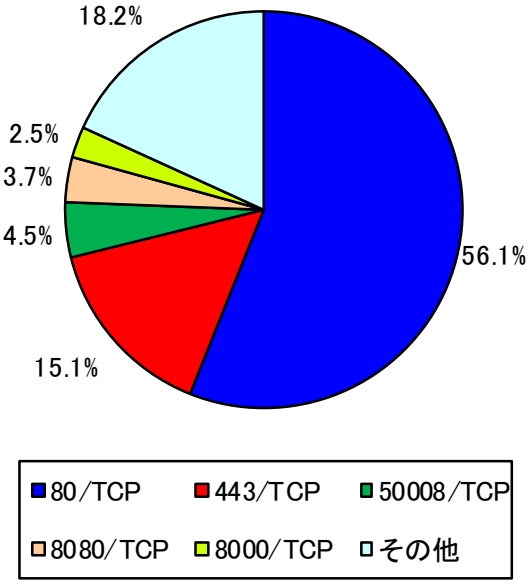


図 4-1　跳ね返りパケット着信元ポート別比率

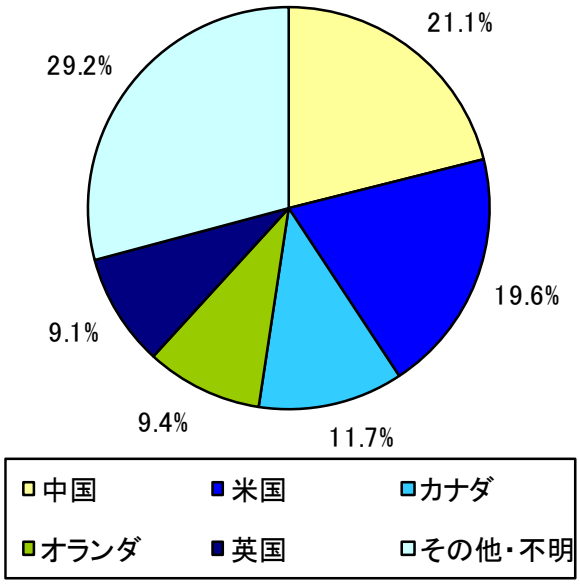


図 4-2　跳ね返りパケット着信元国・地域別比率

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