令和元年10月29日

令和元年９月期観測資料

1　観測結果概要

令和元年9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 5,407.1 件で、令和元年8月期（以下「前期」という。）と比較して 830.9 件（18.2%）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 54,269.8 個で、前期と比較して 5,265.5 個（10.7%）増加しました。

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 798.9 件で、前期と比較して 173.1 件（27.7%）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 7,769.0 個で、前期と比較して 161.3 個（2.1%）増加しました。

DoS 攻撃被害検知件数は、一日当たり 2,213.3 件で、前期と比較して 653.2 件（22.8%）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 233.0 個で、前期と比較して 4.2 個（1.8%）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	458.42 件	＋1.2%　（＋5.47 件）
2 位	2 位	445/TCP	402.17 件	＋2.3%　（＋9.21 件）
3 位	3 位	22/TCP	115.95 件	＋8.8%　（＋9.36 件）
4 位	5 位	80/TCP	68.68 件	＋18.5%　（＋10.73 件）
5 位	6 位	8080/TCP	62.23 件	＋7.5%　（＋4.33 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	34567/TCP	41.27 件	＋610.1%　（＋35.46 件）	9 位	45 位
2 位	8000/TCP	18.04 件	＋216.7%　（＋12.34 件）	22 位	46 位
3 位	88/TCP	15.83 件	＋347.8%　（＋12.30 件）	23 位	68 位
4 位	80/TCP	68.68 件	＋18.5%　（＋10.73 件）	4 位	5 位
5 位	22/TCP	115.95 件	＋8.8%　（＋9.36 件）	3 位	3 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	13.31 件	－74.0%　（－37.87 件）	26 位	9 位
2 位	52869/TCP	32.15 件	－53.0%　（－36.28 件）	13 位	4 位
3 位	37215/TCP	8.14 件	－75.3%　（－24.80 件）	39 位	15 位
4 位	53413/UDP	35.32 件	－31.9%　（－16.53 件）	10 位	8 位
5 位	60001/TCP	25.60 件	－30.2%　（－11.10 件）	16 位	12 位

[i] 一日・1IP アドレス当たり。

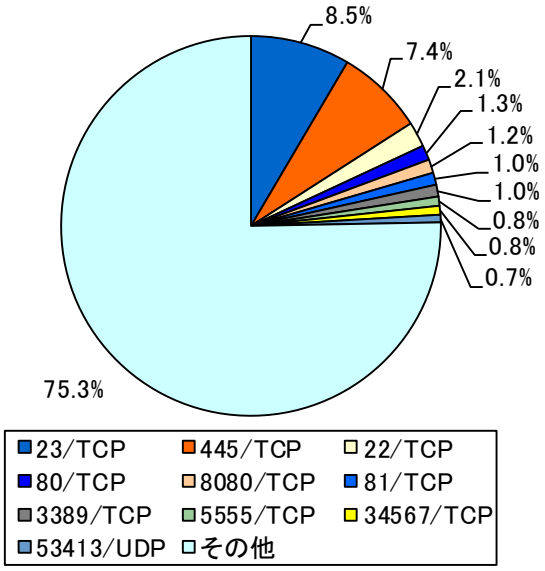

図 2-1　宛先ポート別比率（全て）[i]

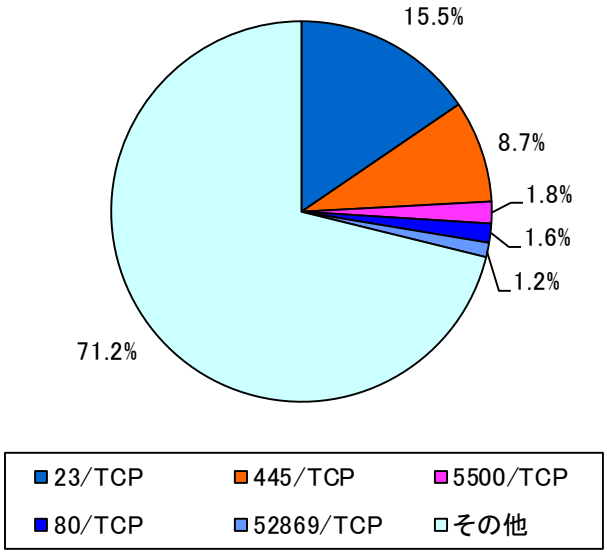

図 2-2　宛先ポート別比率（日本国内）

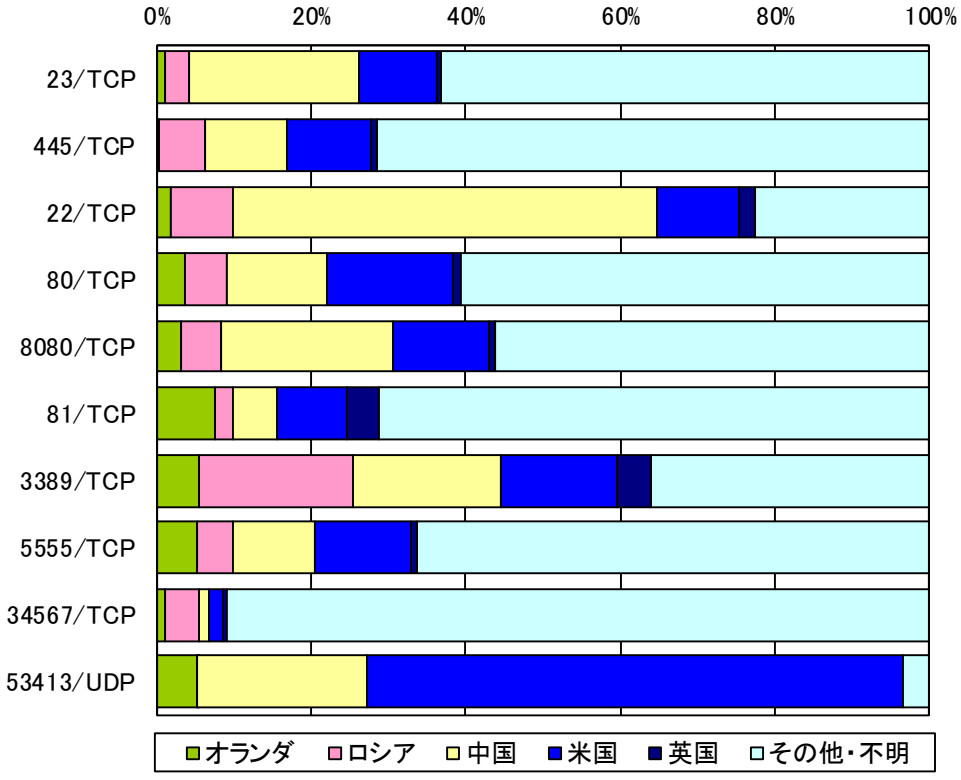

図 2-3　宛先ポート別上位の着信元国・地域別比率 [ii]

[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。

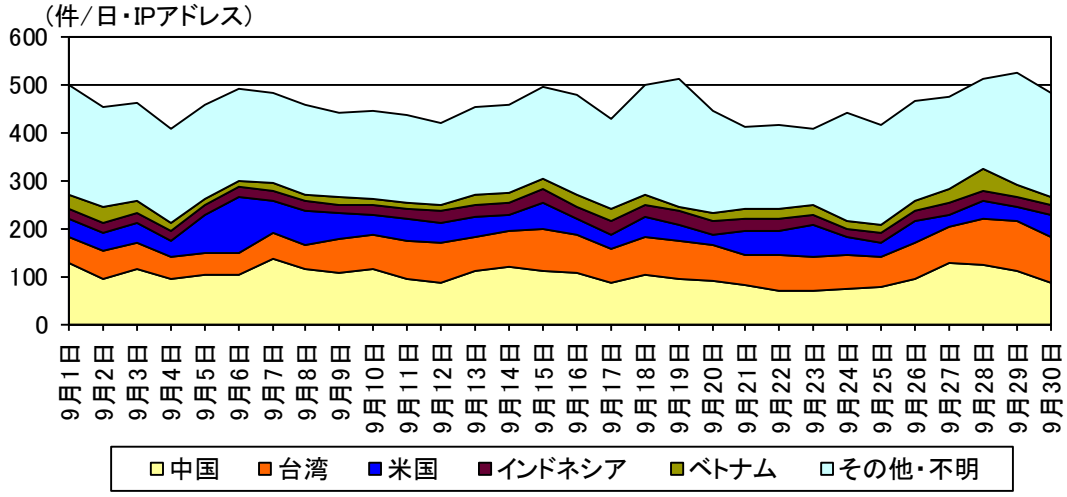

図 2-4　センサーのポート 23/TCP における検知件数の推移

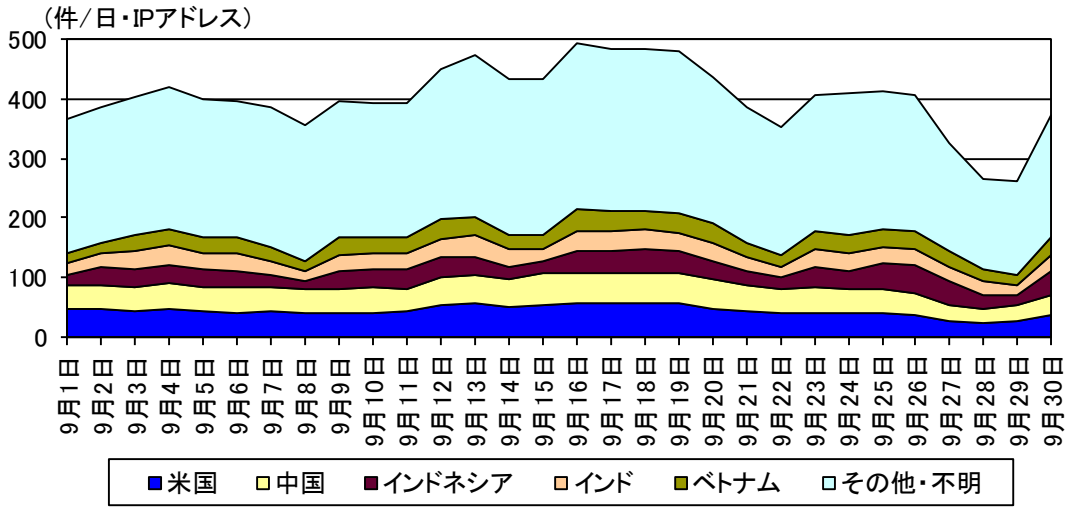

図 2-5　センサーのポート 445/TCP における検知件数の推移

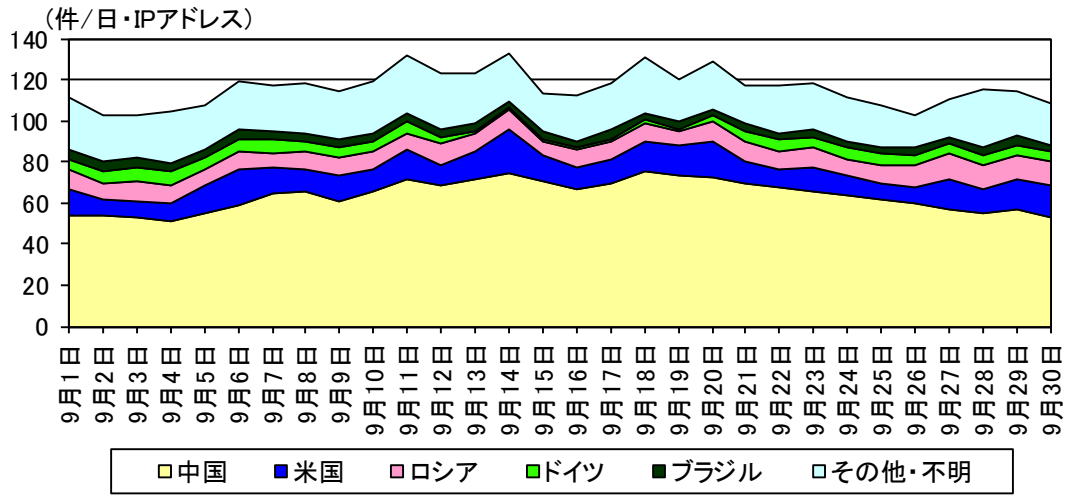

図 2-6　センサーのポート 22/TCP における検知件数の推移

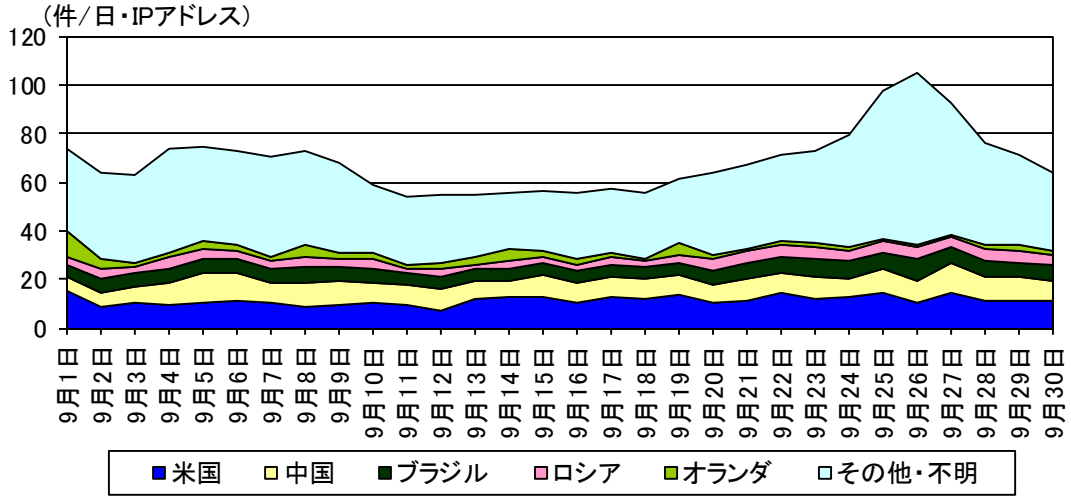

図 2-7　センサーのポート 80/TCP における検知件数の推移

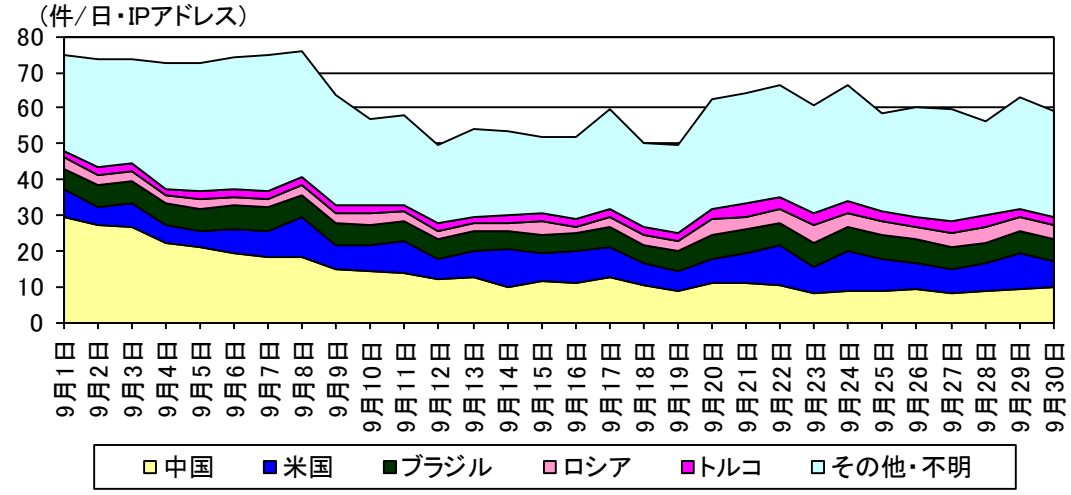

図 2-8　センサーのポート 8080/TCP における検知件数の推移

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	オランダ	1,602.74 件	＋54.3%　（＋564.25 件）
2 位	2 位	ロシア	820.05 件	＋1.6%　（＋13.16 件）
3 位	4 位	中国	591.94 件	＋15.2%　（＋78.09 件）
4 位	3 位	米国	553.43 件	－7.3%　（－43.75 件）
5 位	5 位	英国	170.03 件	＋36.4%　（＋45.40 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	1,602.74 件	＋54.3%　（＋564.25 件）	1 位	1 位
2 位	中国	591.94 件	＋15.2%　（＋78.09 件）	3 位	4 位
3 位	英国	170.03 件	＋36.4%　（＋45.40 件）	5 位	5 位
4 位	スイス	48.55 件	－ [ii]　（＋44.85 件）	16 位	－ [v]
5 位	スペイン	126.88 件	＋32.7%　（＋31.23 件）	6 位	11 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	米国	553.43 件	－7.3%　（－43.75 件）	4 位	3 位
2 位	韓国	54.46 件	－33.0%　（－26.79 件）	14 位	12 位
3 位	台湾	109.30 件	－5.9%　（－6.90 件）	10 位	8 位
4 位	香港	27.69 件	－11.5%　（－3.59 件）	23 位	18 位
5 位	ドイツ	26.88 件	－11.6%　（－3.52 件）	25 位	19 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。

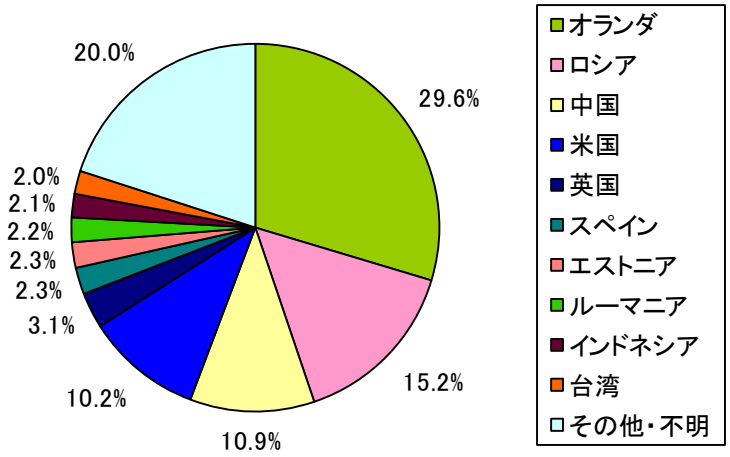

図 2-9　着信元国・地域別比率

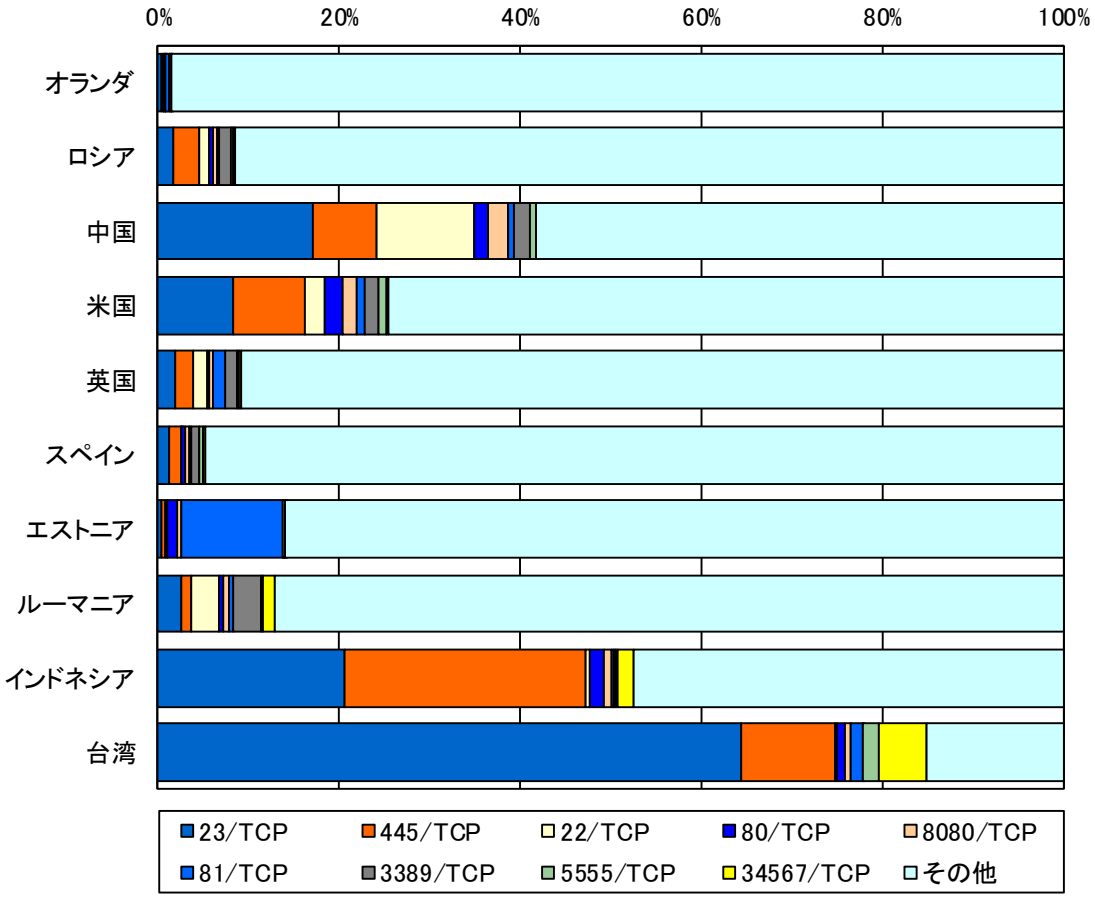

図 2-10　着信元国・地域別上位の宛先ポート別比率

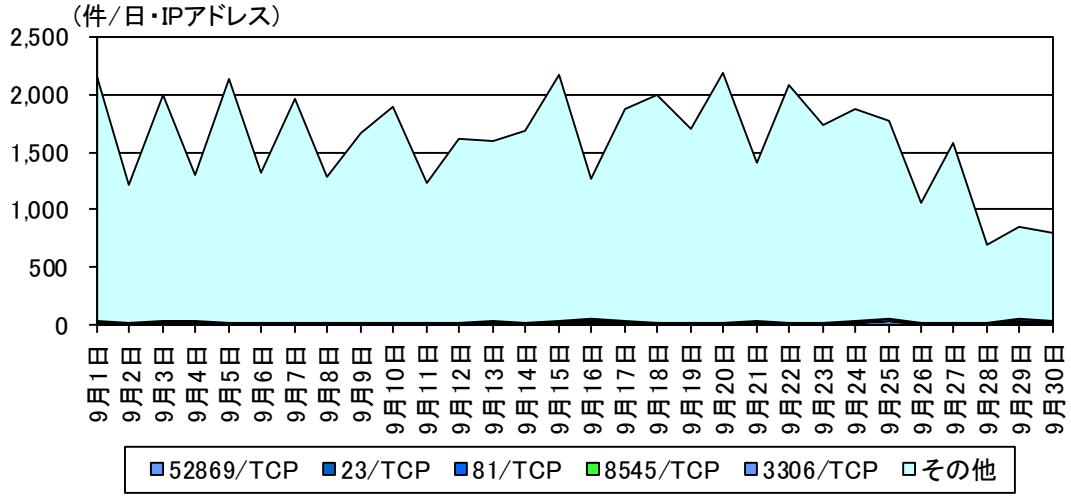

図 2-11　オランダからの検知件数の推移

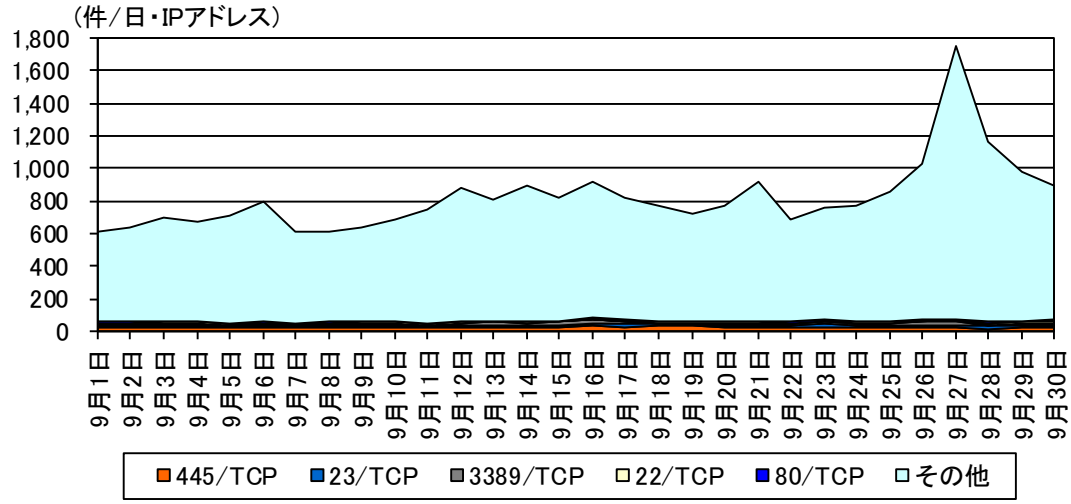

図 2-12　ロシアからの検知件数の推移

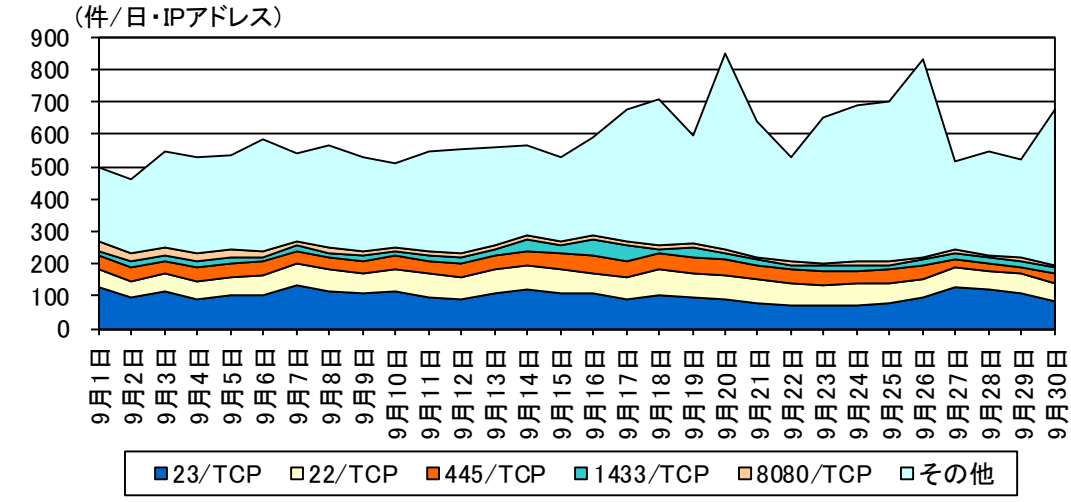

図 2-13　中国からの検知件数の推移

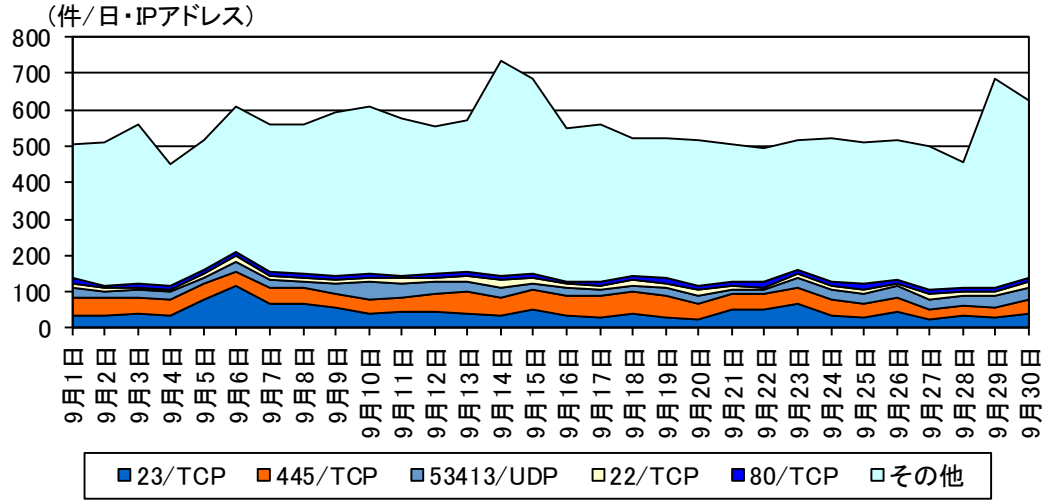

図 2-14　米国からの検知件数の推移

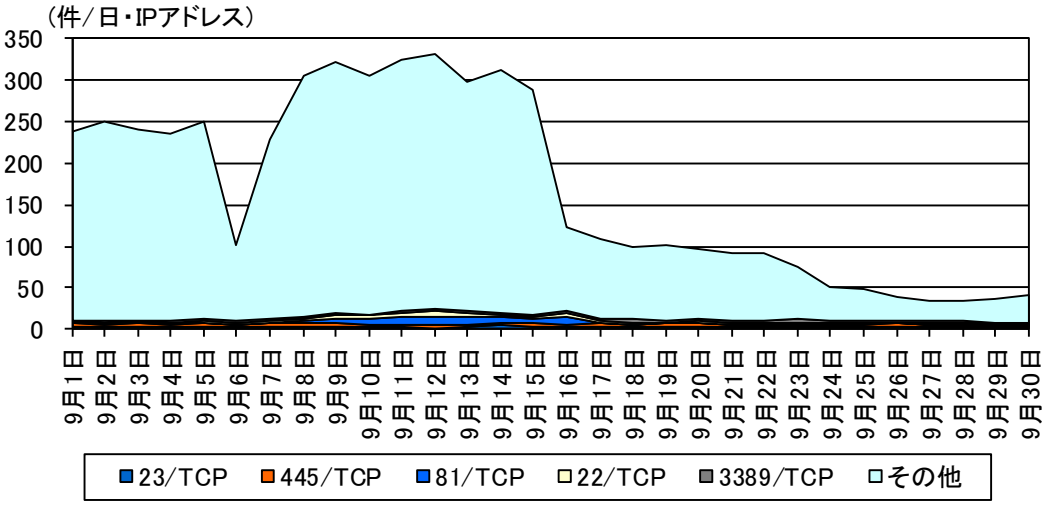

図 2-15　英国からの検知件数の推移

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	243.22 件	＋26.5%　（＋50.99 件）	2 位	
2 位	2 位	Microsoft Windows Terminal server	227.59 件	＋43.0%　（＋68.46 件）	1 位	
3 位	3 位	SMBv1	170.54 件	＋29.6%　（＋38.92 件）	3 位	
4 位	4 位	VOIP	40.76 件	＋23.5%　（＋7.76 件）	5 位	
5 位	5 位	ICMP	24.03 件	－10.8%　（－2.90 件）		2 位

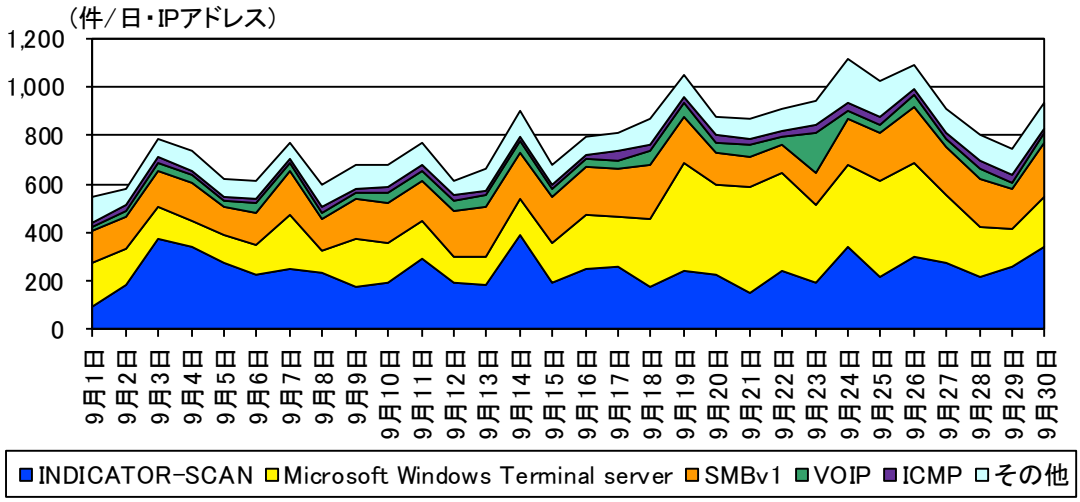

図 3-1　不正侵入等の攻撃手法別検知件数の推移

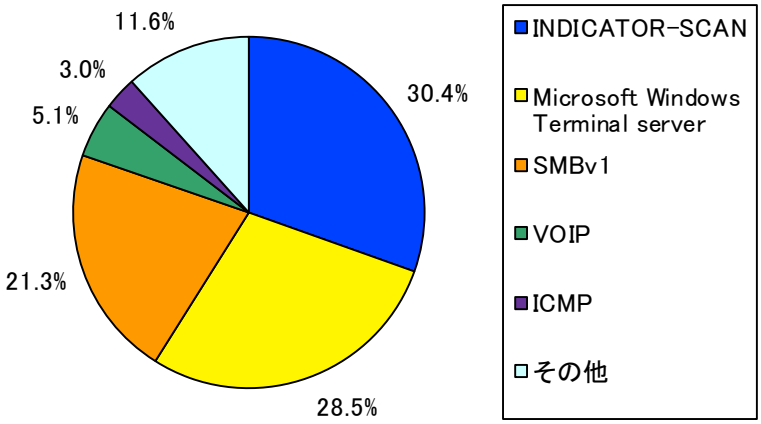

図 3-2　不正侵入等の攻撃手法別検知比率

[i] 一日・1IP アドレス当たり。

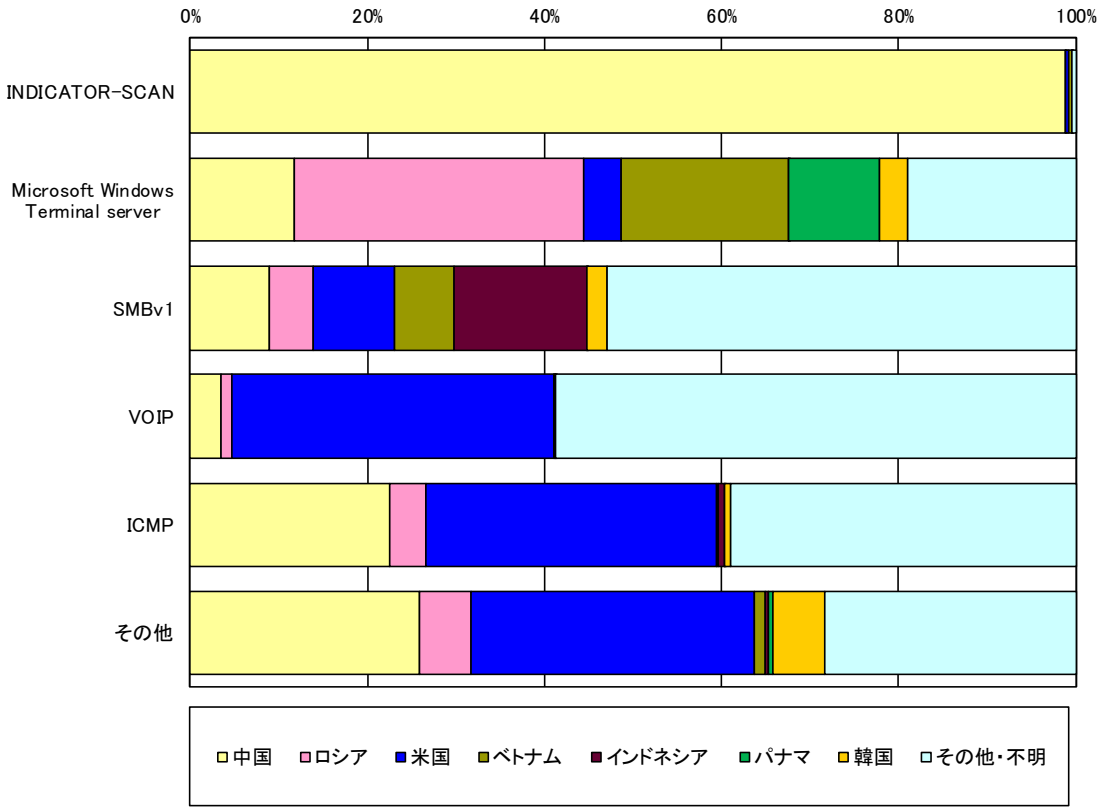

図 3-3 不正侵入等の攻撃手法の国・地域別検知比率

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	313.15 件	＋29.0% （＋70.36 件）
2 位	2 位	ロシア	90.09 件	＋9.9% （＋8.10 件）
3 位	3 位	米国	77.92 件	＋29.0% （＋17.54 件）
4 位	10 位	ベトナム	56.65 件	＋413.8% （＋45.62 件）
5 位	6 位	インドネシア	26.04 件	＋91.7% （＋12.46 件）

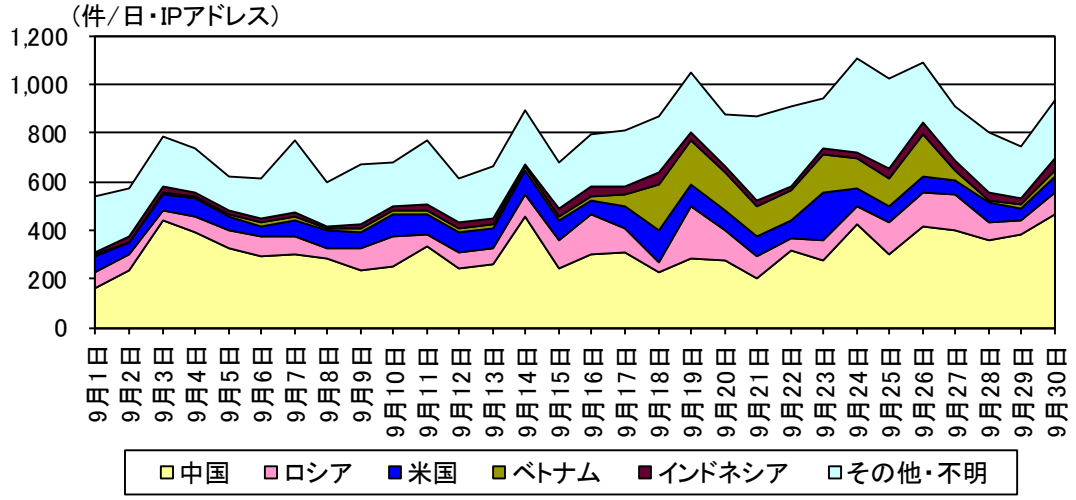

図 3-4 不正侵入等の着信元国・地域別検知件数の推移

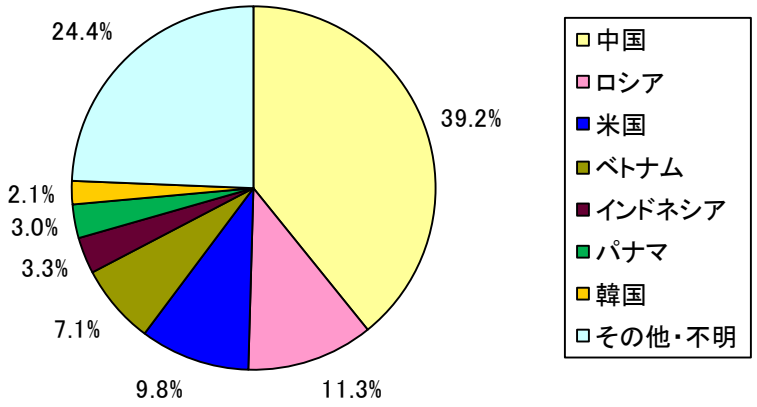

図 3-5 不正侵入等の着信元国・地域別検知比率

[i] 一日・1IP アドレス当たり。

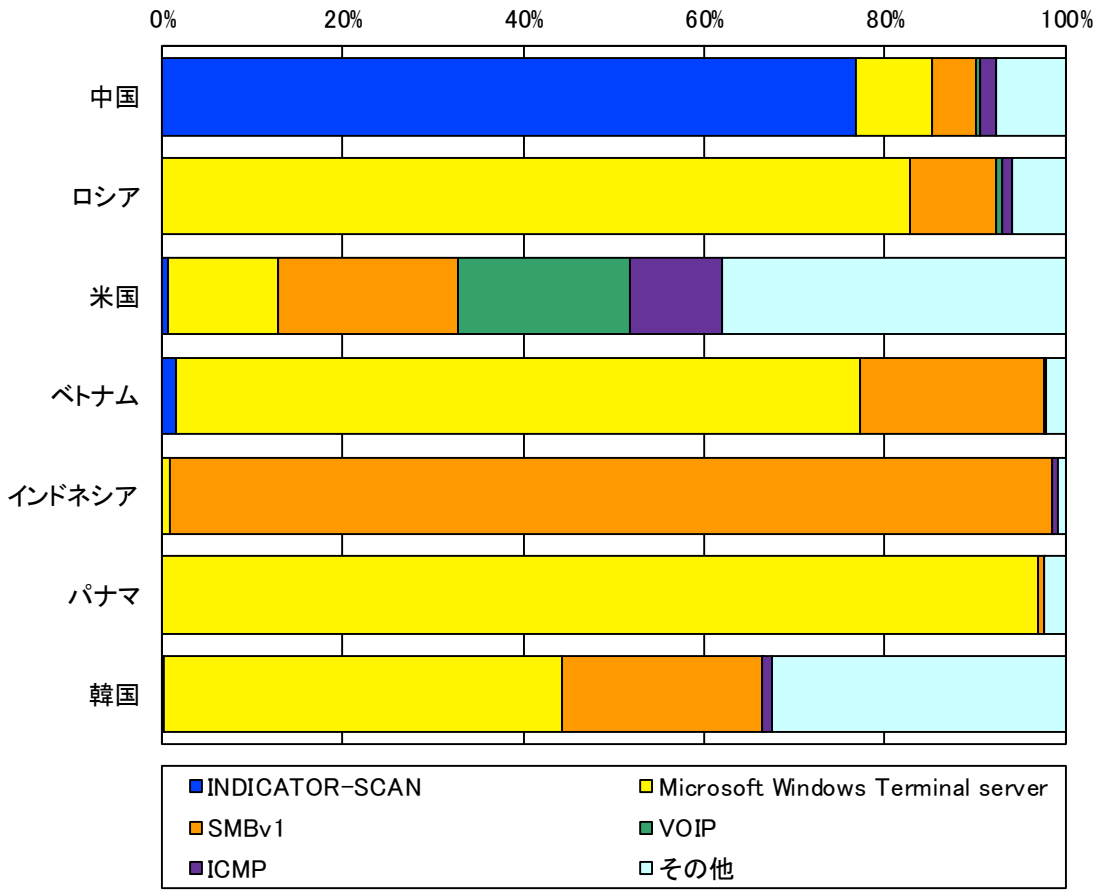

図 3-6　不正侵入等の着信元国・地域別上位の攻撃手法別検知比率

4　DoS 攻撃被害の観測結果

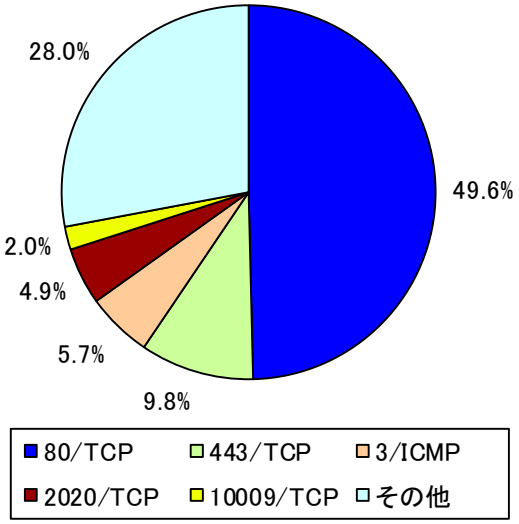

図 4-1　跳ね返りパケット着信元ポート別比率

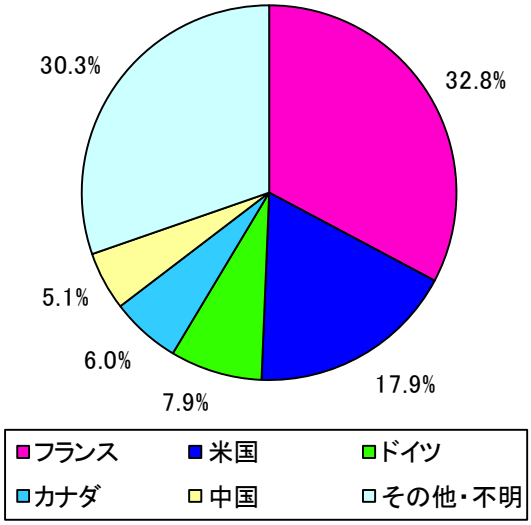

図 4-2　跳ね返りパケット着信元国・地域別比率

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