令和２年 ４ 月 28 日

令和2年3月期観測資料

1　観測結果概要

令和2年3月期（以下「今月期」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 5,411.8 件で、令和2年2月期（以下「前月期」という。）と比較して 1,628.7 件（23.1%）減少しました。また、送信元 IP アドレス[i] 数は、一日当たり 52,399.1 個で、前月期と比較して 532.9 個（1.0%）減少しました。

不正侵入等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 704.3 件で、前月期と比較して 191.4 件（21.4%）減少しました。また、送信元 IP アドレス数は、一日当たり 8,191.7 個で、前月期と比較して 364.9 個（4.7%）増加しました。

DoS 攻撃被害検知件数は、一日当たり 58,919.0 件で、前月期と比較して 50,588.2 件（607.2%）増加しました。また、送信元 IP アドレス数は、一日当たり 10,511.5 個で、前月期と比較して 9,422.7 個（865.5%）増加しました。

[i] 観測した IP パケットの IP ヘッダ情報に記録された送信元アドレス（Source Address）の値のこと。

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（今月期順位）

今月期順位	前月期順位	ポート	今月期件数 [i]	前月期比 [i]
1 位	1 位	23/TCP	457.08 件	－13.3%　（－70.21 件）
2 位	2 位	445/TCP	224.13 件	－1.0%　（－2.33 件）
3 位	3 位	1433/TCP	179.64 件	＋1.5%　（＋2.63 件）
4 位	5 位	80/TCP	77.41 件	＋10.8%　（＋7.52 件）
5 位	4 位	22/TCP	65.45 件	－10.8%　（－7.96 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	今月期件数 [i]	前月期比 [i]	今月期順位	前月期順位
1 位	5555/TCP	61.56 件	＋49.2%　（＋20.31 件）	6 位	12 位
2 位	22079/UDP	16.70 件	－ [ii]　（＋16.70 件）	28 位	－ [ii]
3 位	37215/TCP	21.78 件	＋174.4%　（＋13.85 件）	21 位	44 位
4 位	1723/TCP	21.88 件	＋98.1%　（＋10.84 件）	20 位	30 位
5 位	5060/UDP	41.41 件	＋23.7%　（＋7.93 件）	11 位	14 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	今月期件数 [i]	前月期比 [i]	今月期順位	前月期順位
1 位	23/TCP	457.08 件	－13.3%　（－70.21 件）	1 位	1 位
2 位	8545/TCP	40.63 件	－33.8%　（－20.70 件）	13 位	6 位
3 位	8291/TCP	32.55 件	－26.1%　（－11.53 件）	14 位	11 位
4 位	52869/TCP	45.66 件	－19.2%　（－10.83 件）	10 位	7 位
5 位	8728/TCP	6.95 件	－53.7%　（－8.06 件）	53 位	24 位

[i] 一日・1IP アドレス当たり。

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

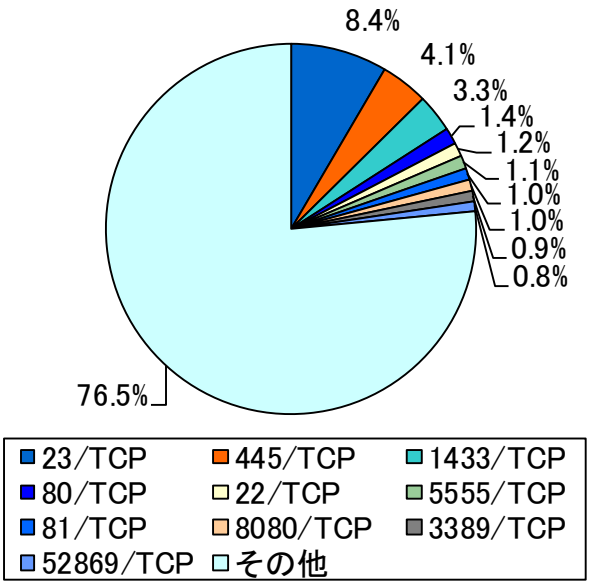

図 2-1　宛先ポート別比率（全て）[i]

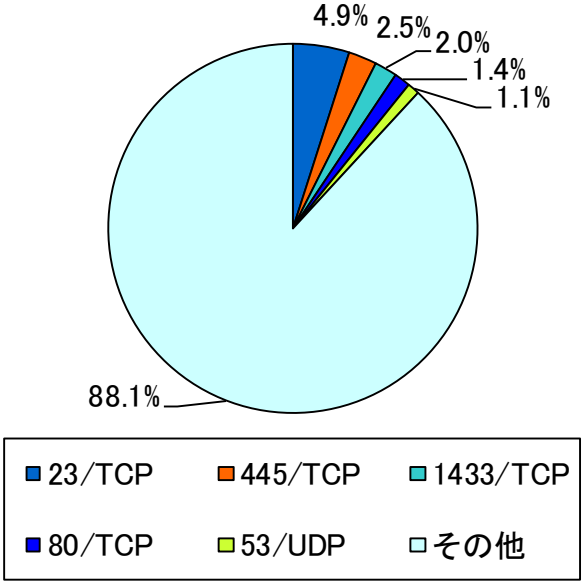

図 2-2　宛先ポート別比率（日本国内）

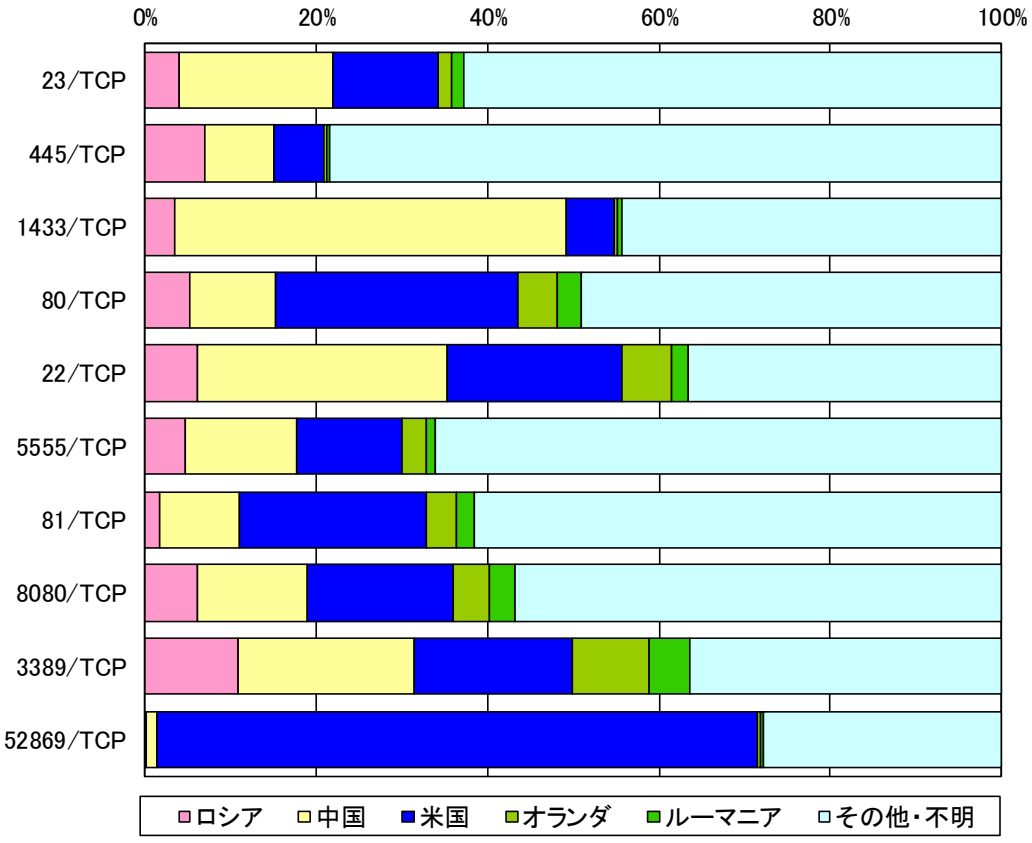

図 2-3　宛先ポート別上位の送信元国・地域別比率 [ii]

[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] 送信元国・地域については、判明した送信元 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。

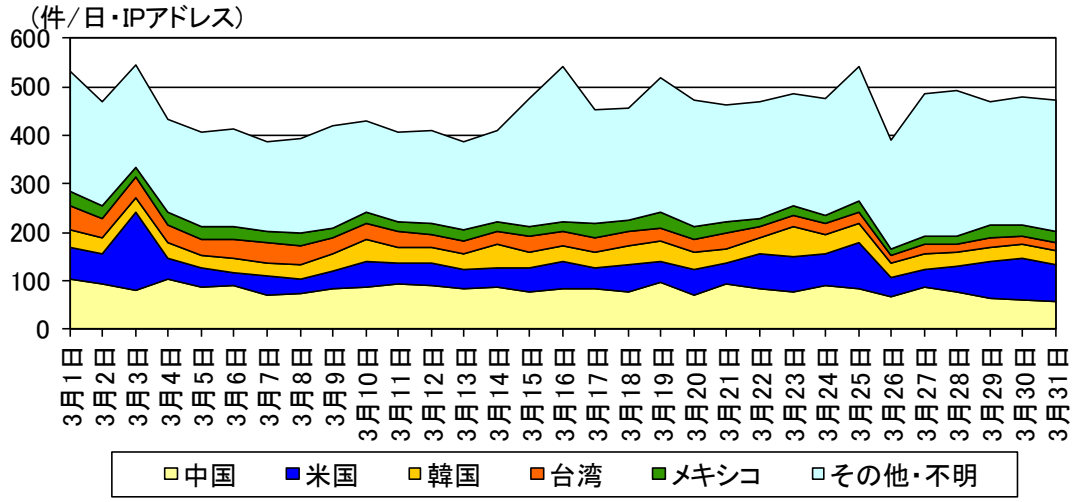

図 2-4　センサーのポート 23/TCP における検知件数の推移

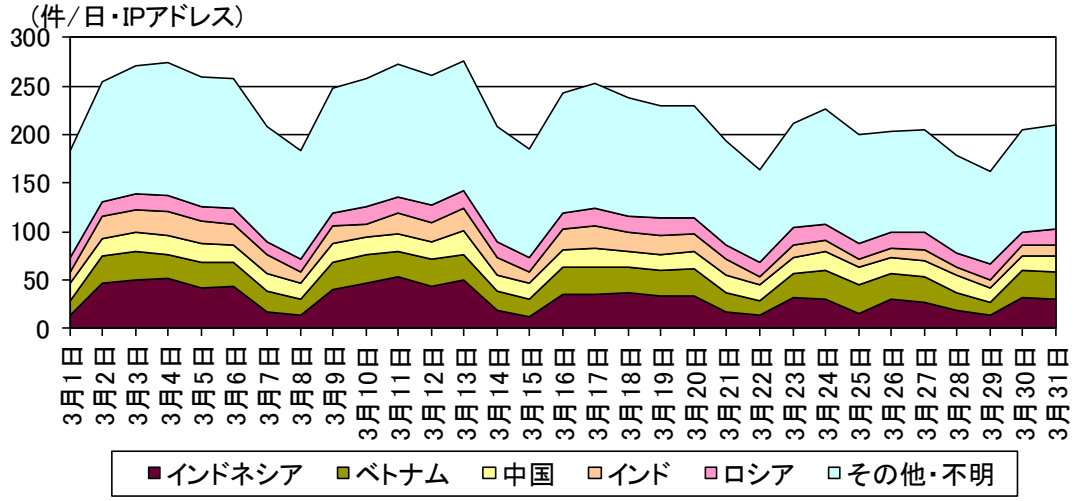

図 2-5　センサーのポート 445/TCP における検知件数の推移

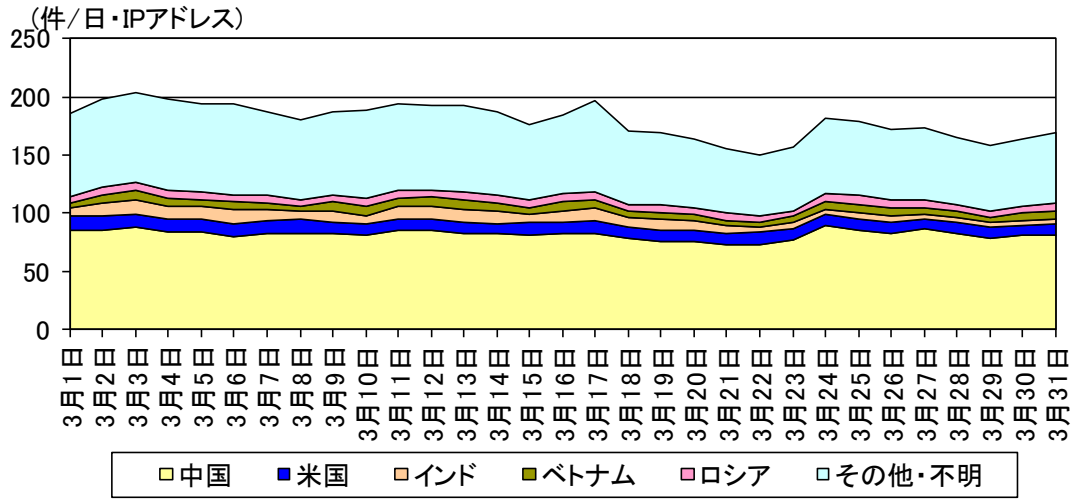

図 2-6　センサーのポート 1433/TCP における検知件数の推移

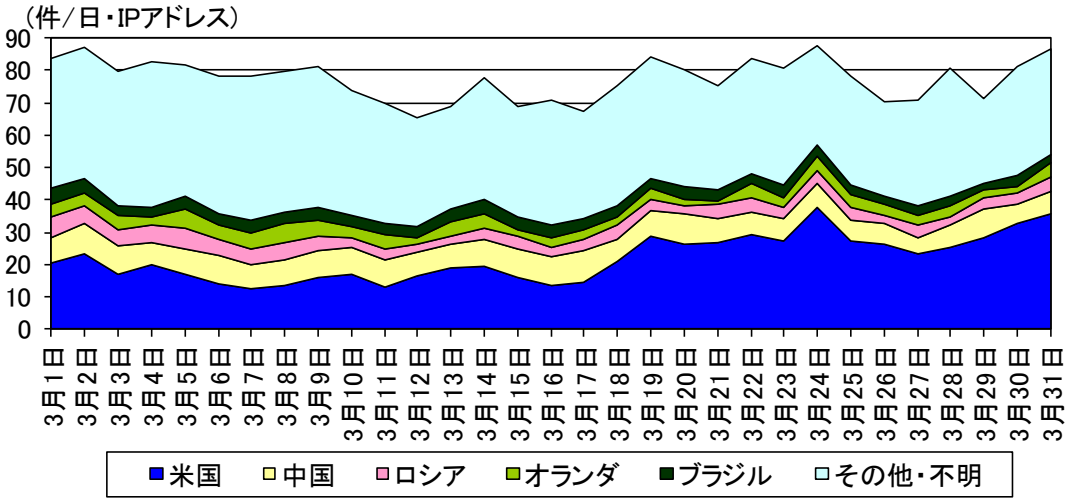

図 2-7　センサーのポート 80/TCP における検知件数の推移

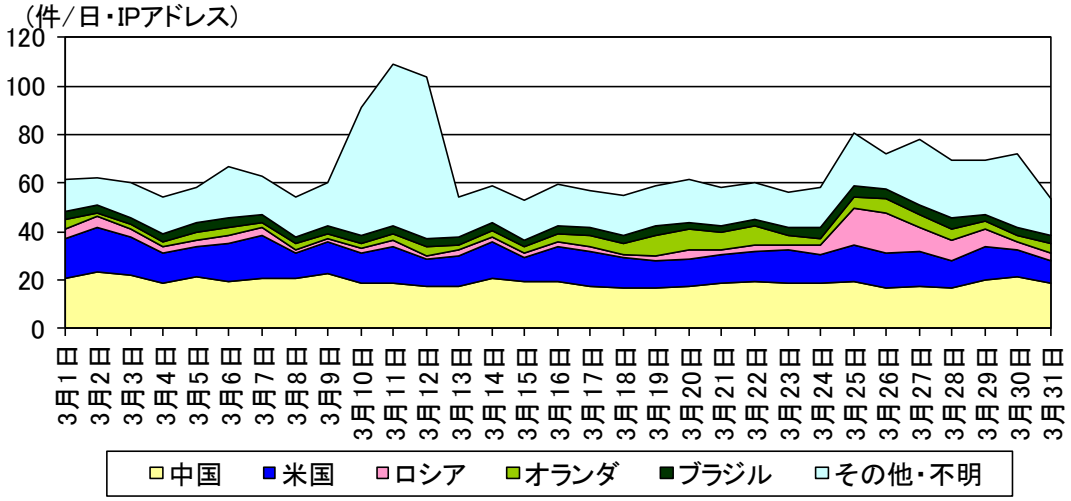

図 2-8　センサーのポート 22/TCP における検知件数の推移

2-2　送信元国・地域別アクセス検知件数

表 2-4　送信元国・地域別検知件数（今月期順位）

今月期順位	前月期順位	国・地域	今月期件数 [i]	前月期比 [i]
1 位	2 位	ロシア	1,496.81 件	＋32.5%　（＋366.89 件）
2 位	3 位	中国	959.39 件	＋10.7%　（＋92.65 件）
3 位	4 位	米国	745.67 件	＋12.6%　（＋83.65 件）
4 位	1 位	オランダ	469.78 件	－80.8%　（－1981.66 件）
5 位	6 位	ルーマニア	171.00 件	－8.7%　（－16.32 件）

表 2-5　送信元国・地域別検知件数（増加順位）

増加順位	国・地域	今月期件数 [i]	前月期比 [i]	今月期順位	前月期順位
1 位	ロシア	1,496.81 件	＋32.5%　（＋366.89 件）	1 位	2 位
2 位	中国	959.39 件	＋10.7%　（＋92.65 件）	2 位	3 位
3 位	米国	745.67 件	＋12.6%　（＋83.65 件）	3 位	4 位
4 位	ウクライナ	151.21 件	＋77.0%　（＋65.76 件）	6 位	12 位
5 位	フランス	116.26 件	＋34.1%　（＋29.59 件）	8 位	11 位

表 2-6　送信元国・地域別検知件数（減少順位）

減少順位	国・地域	今月期件数 [i]	前月期比 [i]	今月期順位	前月期順位
1 位	オランダ	469.78 件	－80.8%　（－1981.66 件）	4 位	1 位
2 位	スイス	21.01 件	－90.7%　（－204.13 件）	27 位	5 位
3 位	台湾	80.53 件	－23.9%　（－25.33 件）	11 位	9 位
4 位	ルーマニア	171.00 件	－8.7%　（－16.32 件）	5 位	6 位
5 位	ベトナム	91.16 件	－14.5%　（－15.46 件）	9 位	8 位

[i] 一日・1IP アドレス当たり。

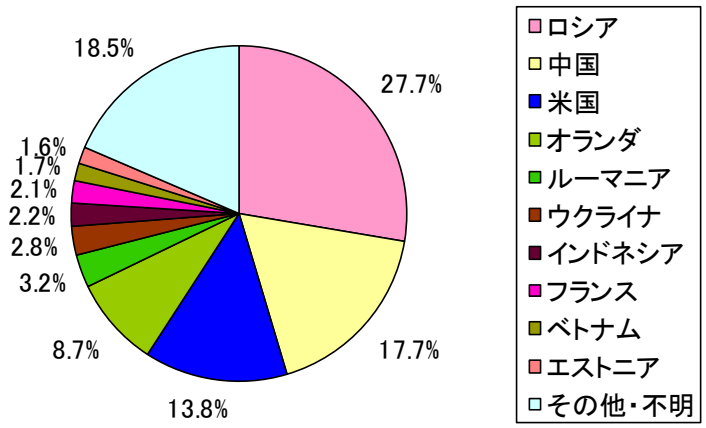

図 2-9　送信元国・地域別比率

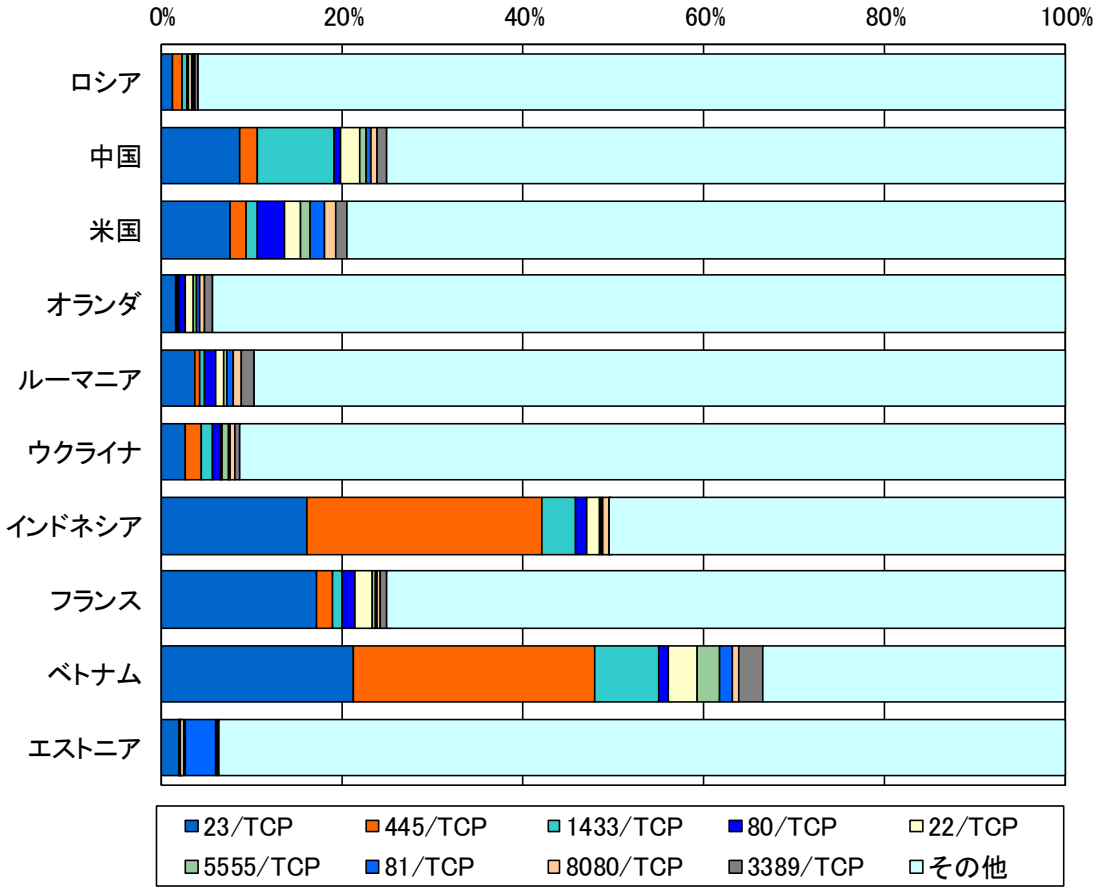

図 2-10　送信元国・地域別上位の宛先ポート別比率

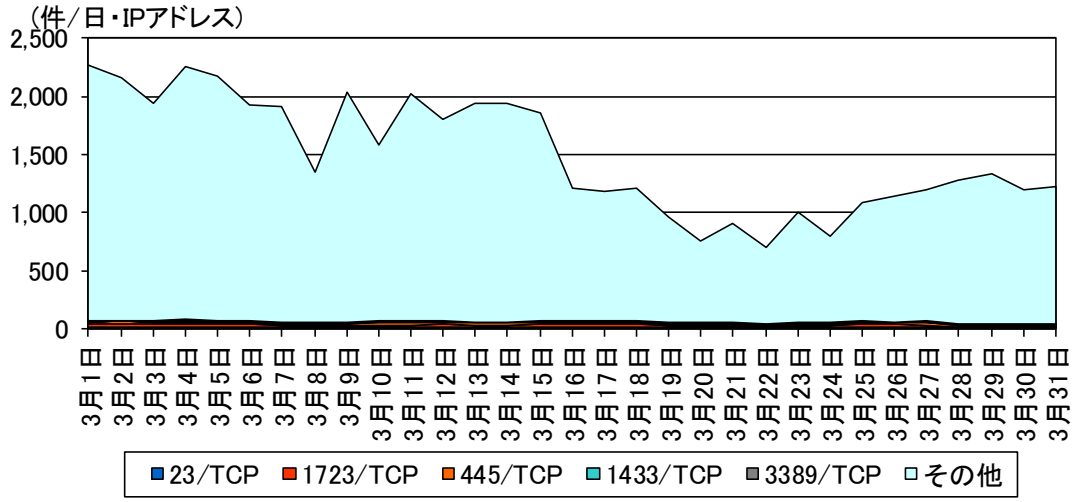

図 2-11　ロシアからの検知件数の推移

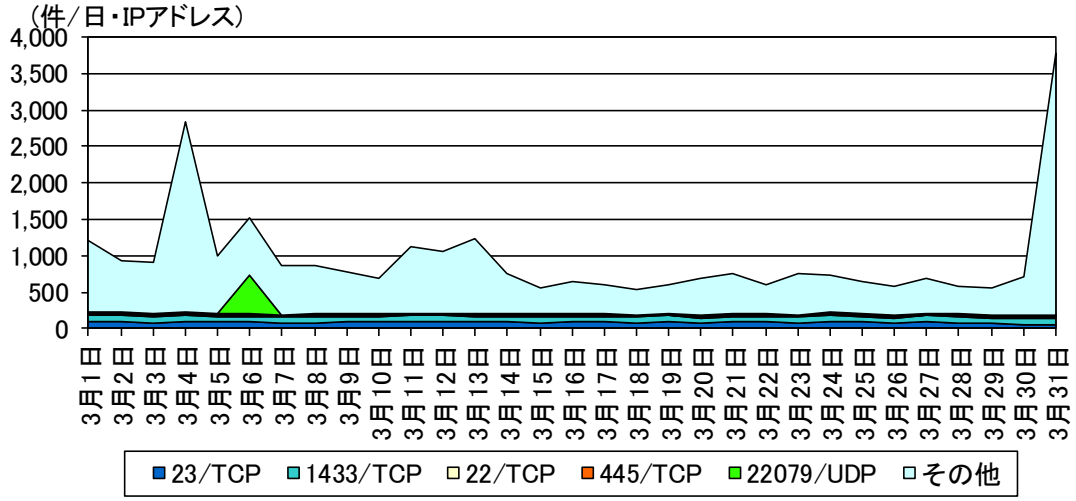

図 2-12　中国からの検知件数の推移

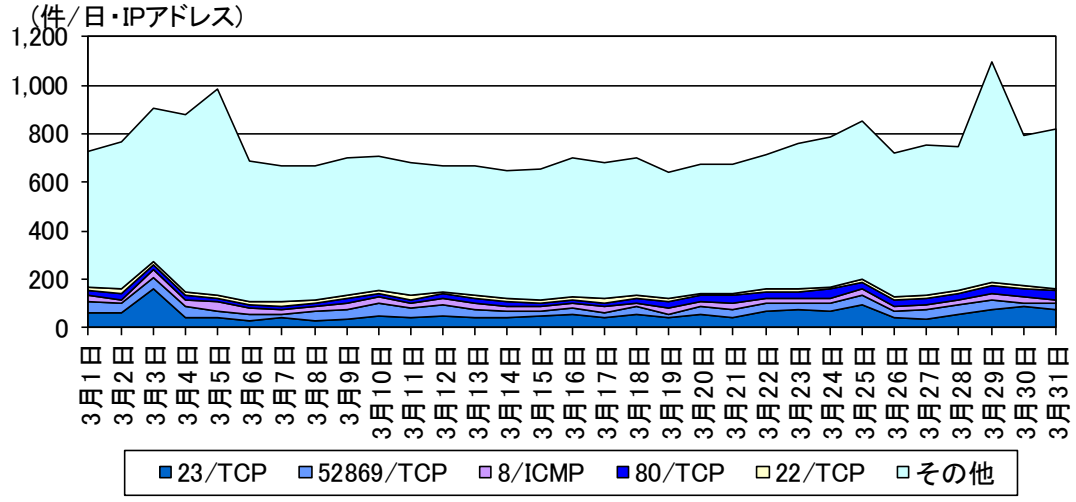

図 2-13　米国からの検知件数の推移

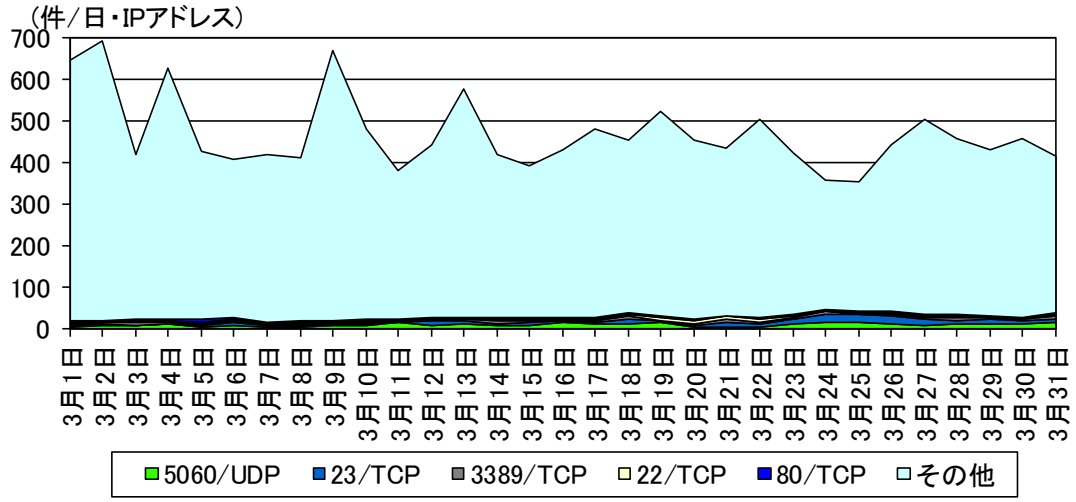

図 2-14　オランダからの検知件数の推移

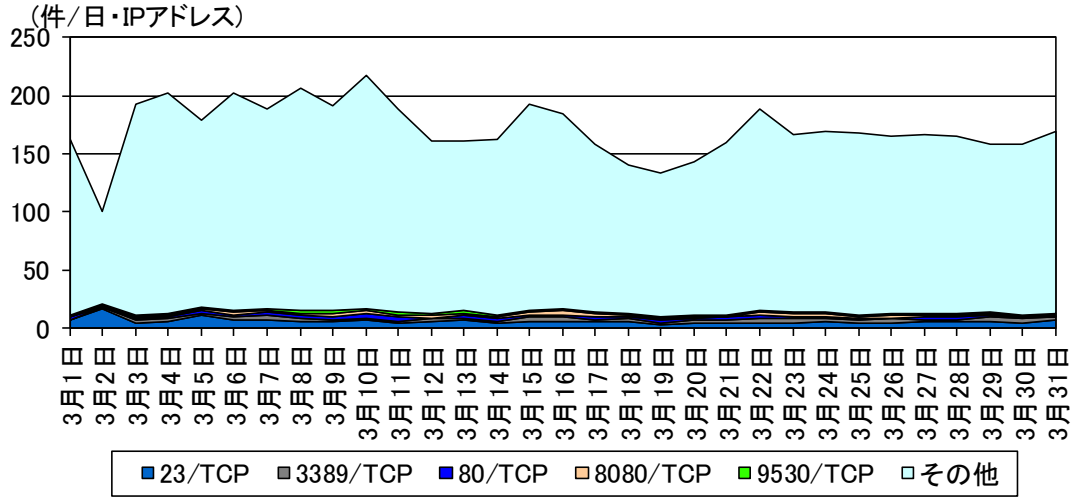

図 2-15　ルーマニアからの検知件数の推移

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

今月期順位	前月期順位	攻撃手法	今月期件数 [i]	前月期比 [i]	増加順位	減少順位
1 位	1 位	INDICATOR-SCAN	260.69 件	＋2.0%　（＋5.17 件）	2 位	
2 位	2 位	Microsoft Windows Terminal server	168.31 件	－49.3%　（－163.42 件）		1 位
3 位	3 位	SMBv1	106.42 件	＋0.4%　（＋0.43 件）		
4 位	7 位	ICMP	26.87 件	＋8.7%　（＋2.15 件）	5 位	
5 位	5 位	OS-WINDOWS	19.50 件	＋3.9%　（＋0.73 件）		

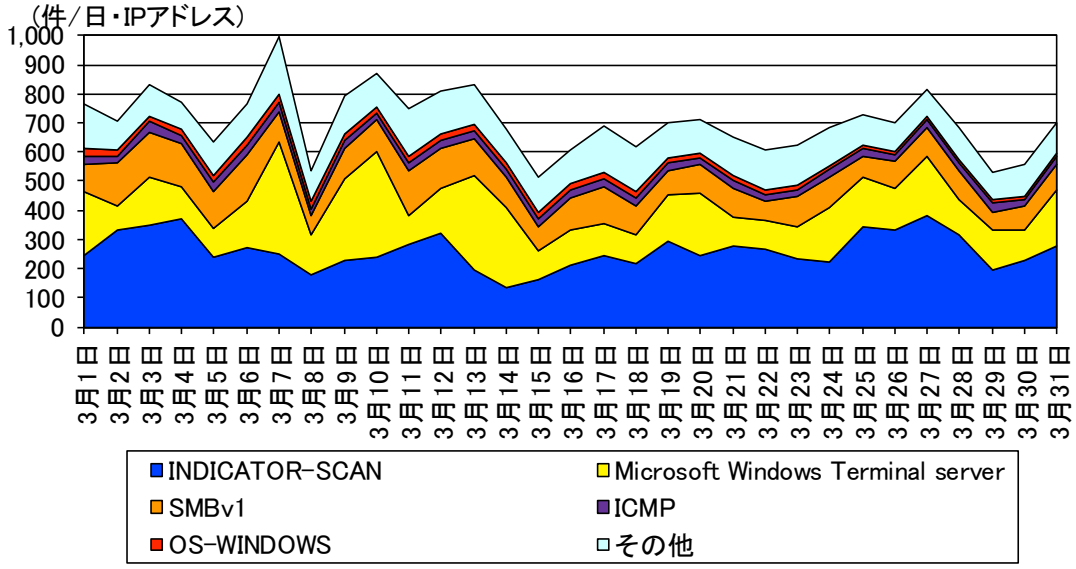

図 3-1　不正侵入等の攻撃手法別検知件数の推移

[i] 一日・1IP アドレス当たり。

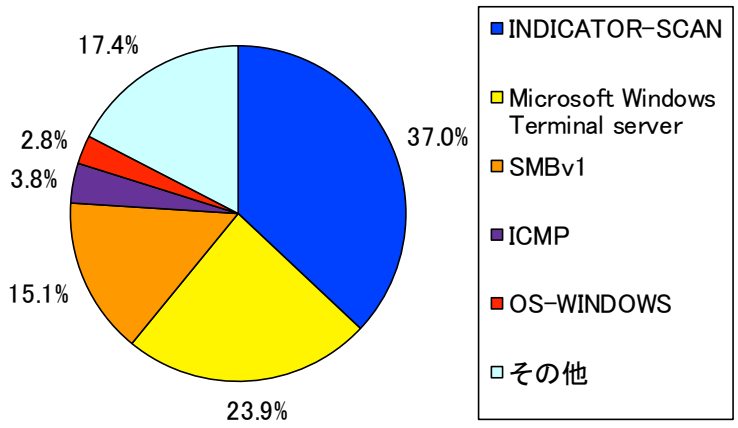

図 3-2 不正侵入等の攻撃手法別検知比率

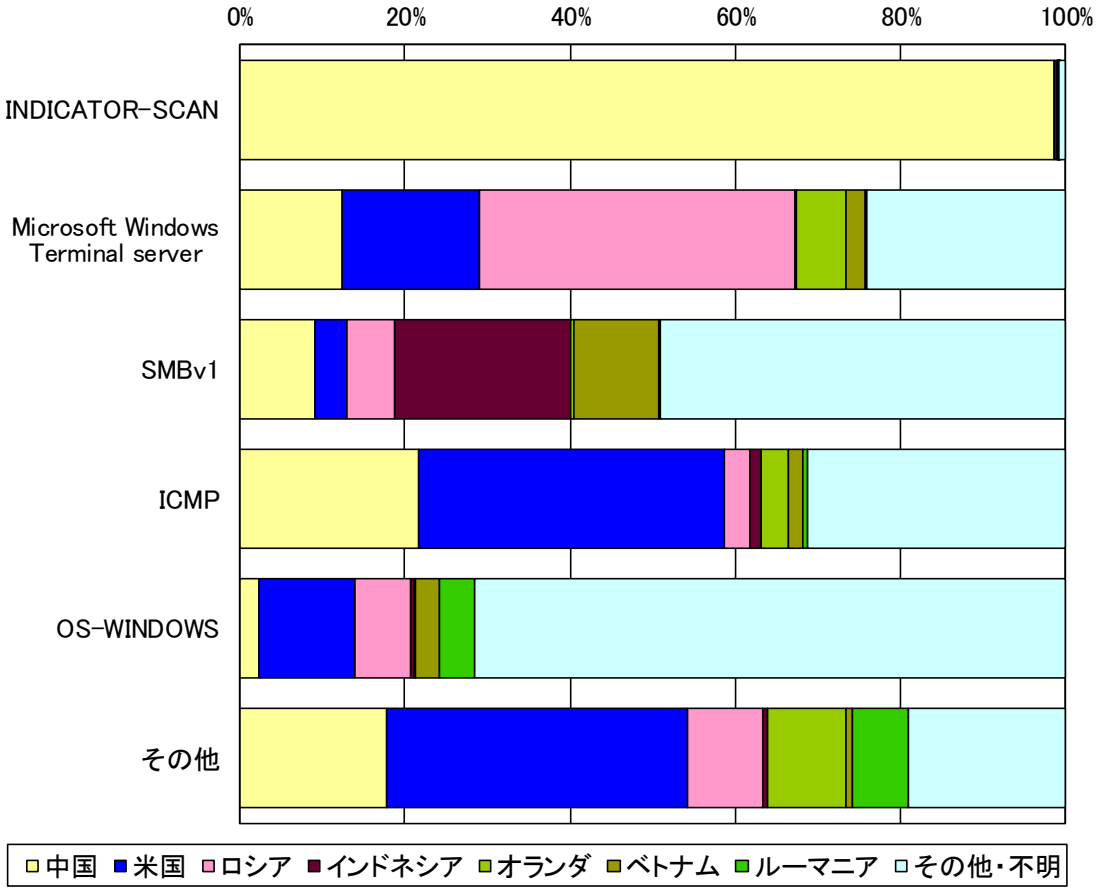

図 3-3 不正侵入等の攻撃手法の国・地域別検知比率

3-2 送信元国・地域別アクセス検知件数

表 3-2 不正侵入等の送信元国・地域別検知件数（今月期順位）

今月期順位	前月期順位	国・地域	今月期件数 [i]	前月期比 [i]
1 位	1 位	中国	315.74 件	－23.4% （－96.19 件）
2 位	3 位	米国	89.89 件	－2.8% （－2.58 件）
3 位	2 位	ロシア	84.03 件	－14.1% （－13.75 件）
4 位	7 位	インドネシア	24.13 件	－16.5% （－4.75 件）
5 位	10 位	オランダ	23.21 件	＋84.9% （＋10.66 件）

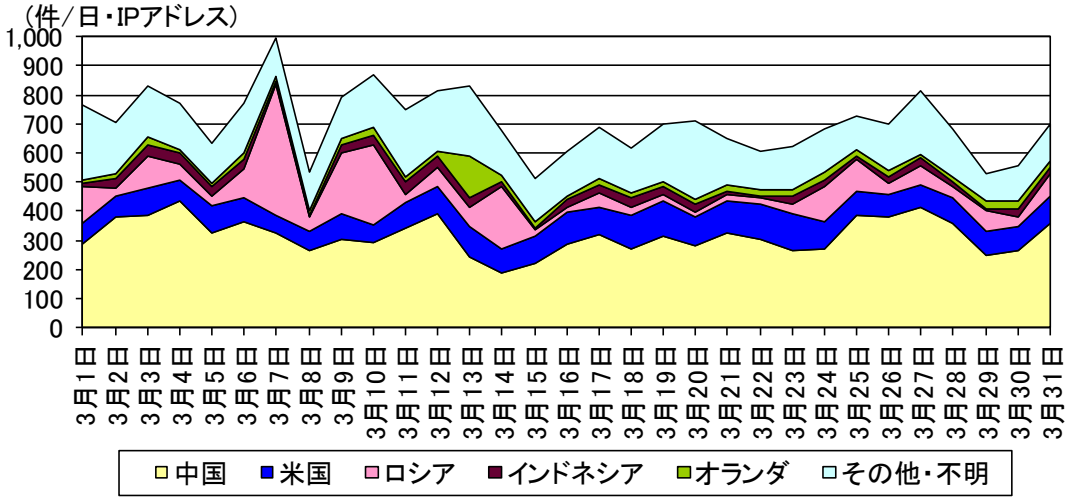

図 3-4 不正侵入等の送信元国・地域別検知件数の推移

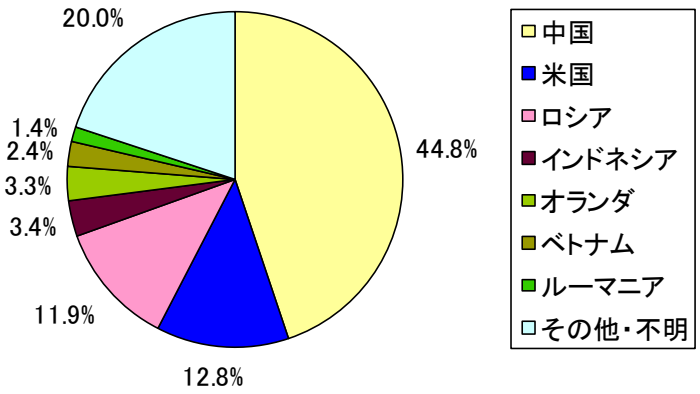

図 3-5 不正侵入等の送信元国・地域別検知比率

[i] 一日・1IP アドレス当たり。

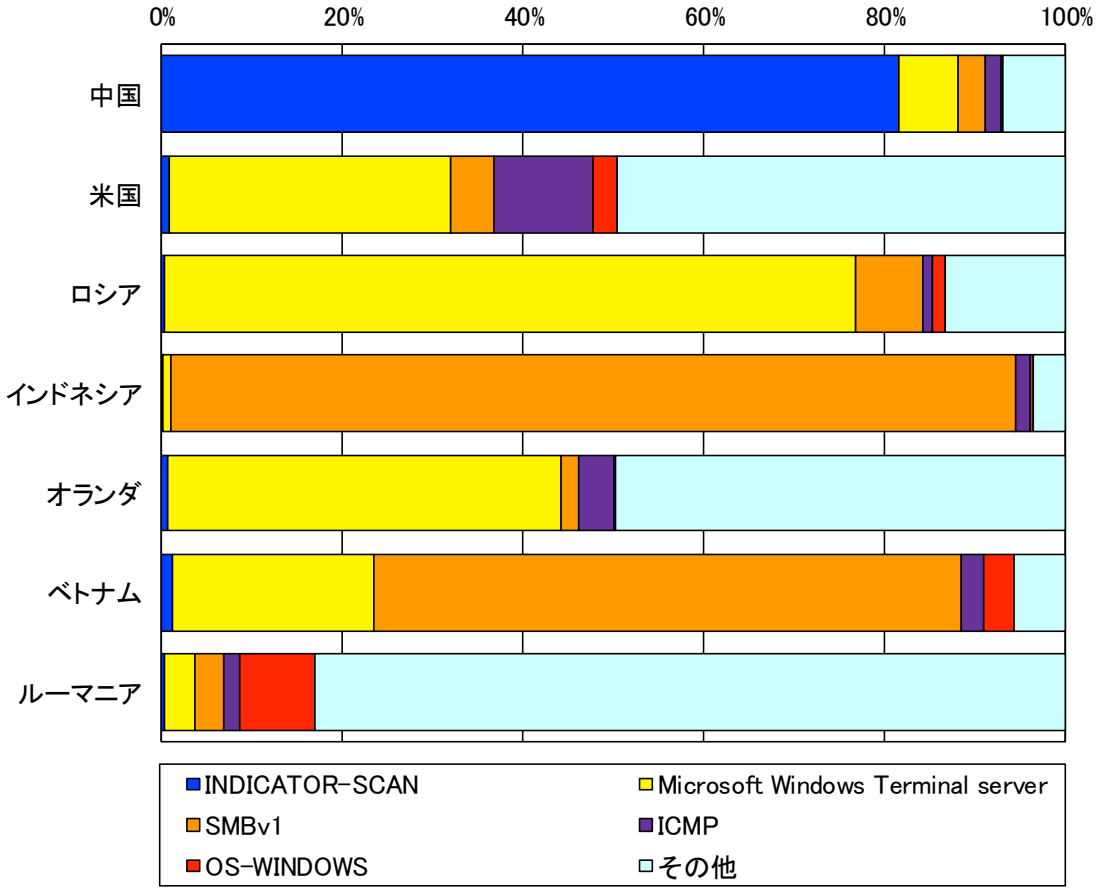

図 3-6 不正侵入等の送信元国・地域別上位の攻撃手法別検知比率

4　DoS 攻撃被害の観測結果

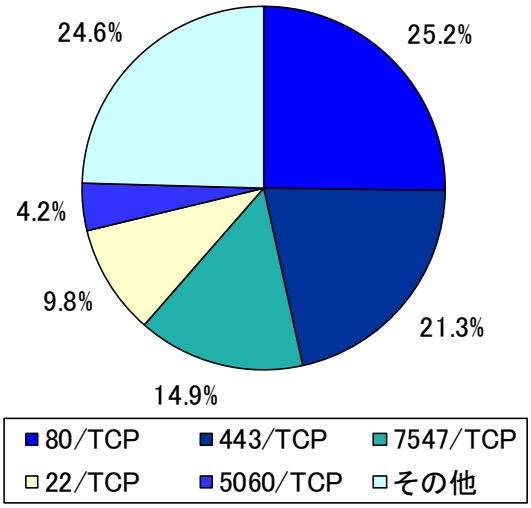

図 4-1　跳ね返りパケット送信元ポート別比率

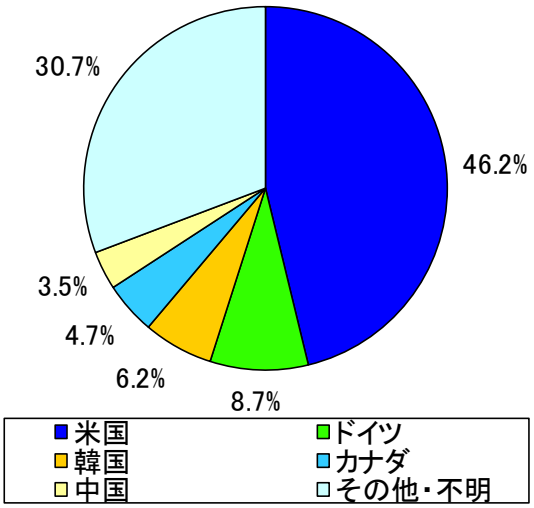

図 4-2　跳ね返りパケット送信元国・地域別比率

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