令和２年３月 25 日

令和2年2月期観測資料

1　観測結果概要

令和2年2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 7,040.5 件で、令和2年1月期（以下「前月期」という。）と比較して 2,200.3 件（45.5%）増加しました。また、送信元 IP アドレス[i] 数は、一日当たり 52,932.0 個で、前月期と比較して 5,663.6 個（12.0%）増加しました。

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 895.7 件で、前月期と比較して 36.4 件（4.2%）増加しました。また、送信元 IP アドレス数は、一日当たり 7,826.8 個で、前月期と比較して 1,061.7 個（11.9%）減少しました。

DoS 攻撃被害検知件数は、一日当たり 8,330.9 件で、前月期と比較して 1,685.7 件（16.8%）減少しました。また、送信元 IP アドレス数は、一日当たり 1,088.7 個で、前月期と比較して 604.8 個（125.0%）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	527.29 件	＋48.0%　（＋171.02 件）
2 位	2 位	445/TCP	226.45 件	－2.6%　（－6.12 件）
3 位	3 位	1433/TCP	177.01 件	－11.4%　（－22.69 件）
4 位	6 位	22/TCP	73.41 件	＋19.1%　（＋11.79 件）
5 位	4 位	80/TCP	69.90 件	－5.6%　（－4.11 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	23/TCP	527.29 件	＋48.0%　（＋171.02 件）	1 位	1 位
2 位	9530/TCP	19.74 件	－[ii]　（＋19.63 件）	21 位	－[ii]
3 位	8291/TCP	44.08 件	＋43.9%　（＋13.45 件）	11 位	17 位
4 位	22/TCP	73.41 件	＋19.1%　（＋11.79 件）	4 位	6 位
5 位	8728/TCP	15.01 件	＋187.2%　（＋9.78 件）	24 位	55 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	1433/TCP	177.01 件	－11.4%　（－22.69 件）	3 位	3 位
2 位	123/UDP	30.52 件	－38.2%　（－18.88 件）	16 位	9 位
3 位	52869/TCP	56.49 件	－23.4%　（－17.22 件）	7 位	5 位
4 位	1900/UDP	24.49 件	－24.5%　（－7.94 件）	18 位	15 位
5 位	4567/TCP	12.47 件	－36.7%　（－7.24 件）	28 位	21 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。

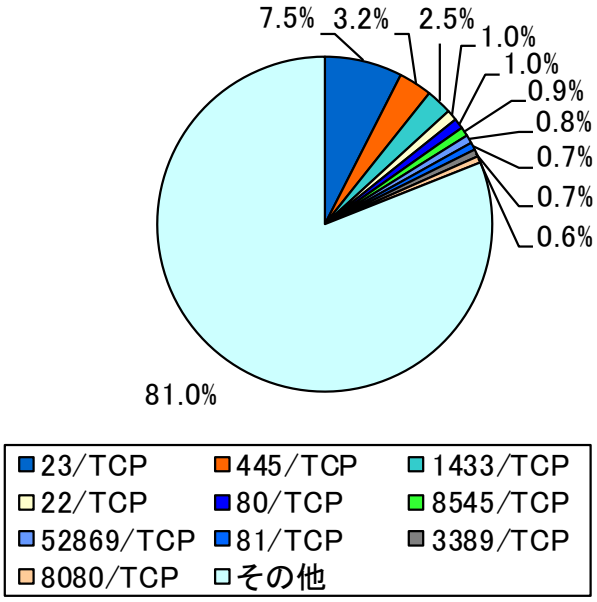

図 2-1　宛先ポート別比率（全て）[i]

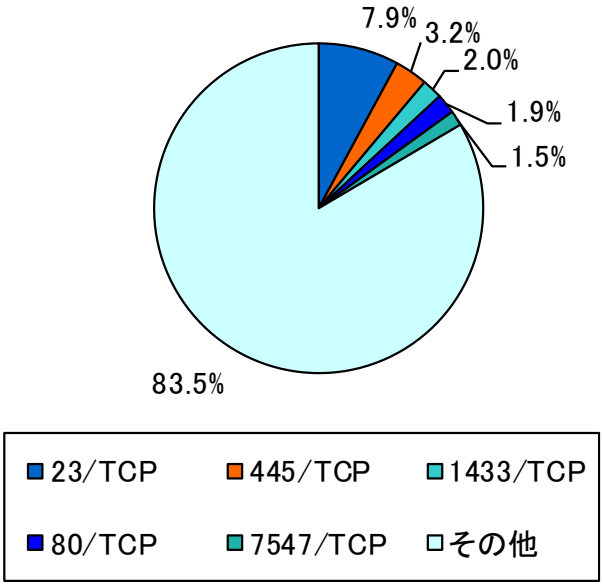

図 2-2　宛先ポート別比率（日本国内）

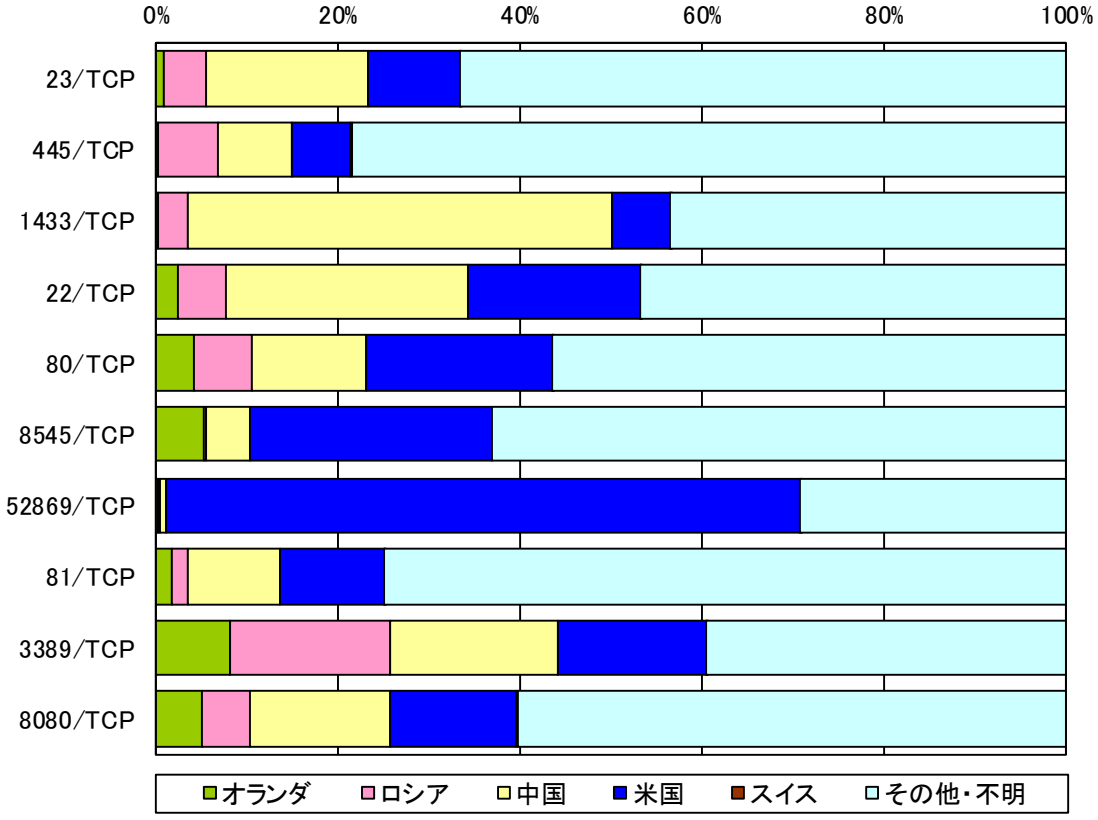

図 2-3　宛先ポート別上位の送信元国・地域別比率 [ii]

[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。

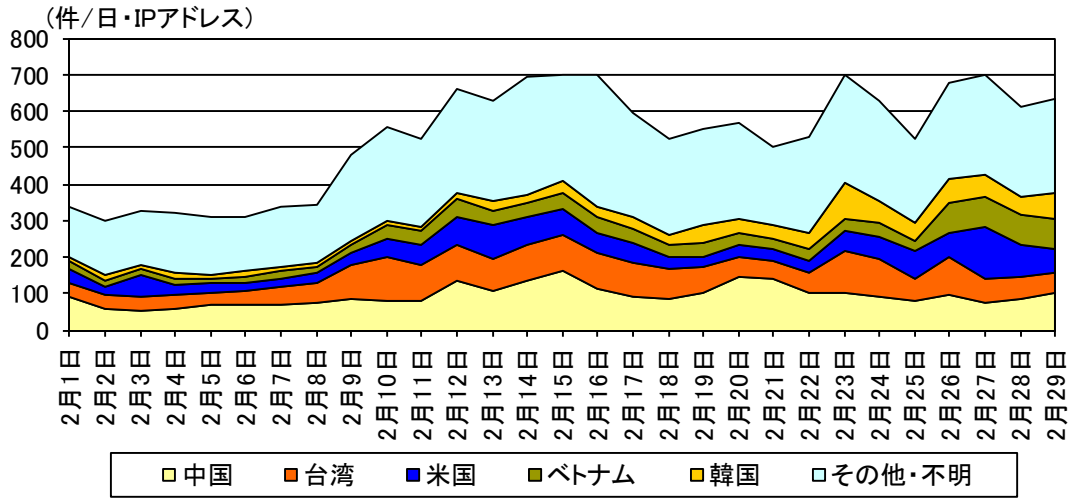

図 2-4　センサーのポート 23/TCP における検知件数の推移

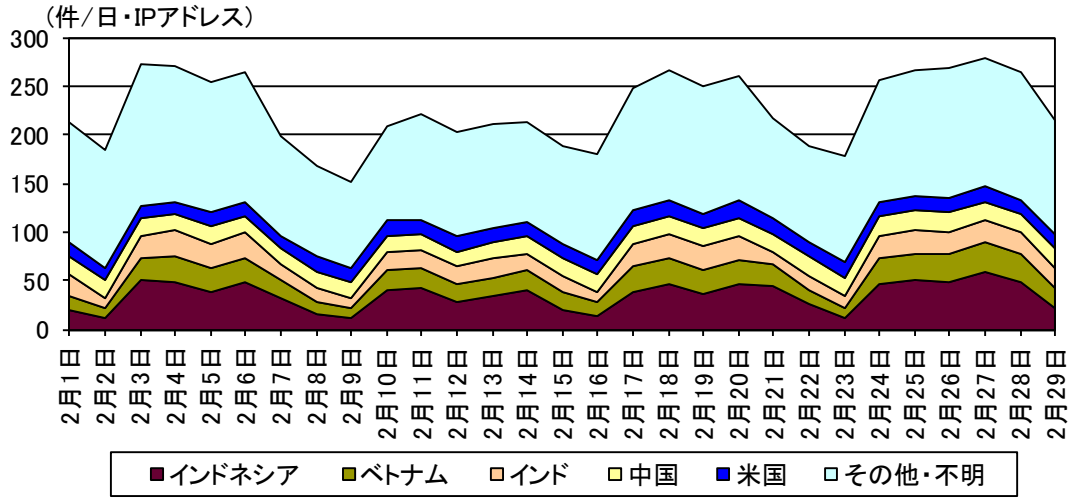

図 2-5　センサーのポート 445/TCP における検知件数の推移

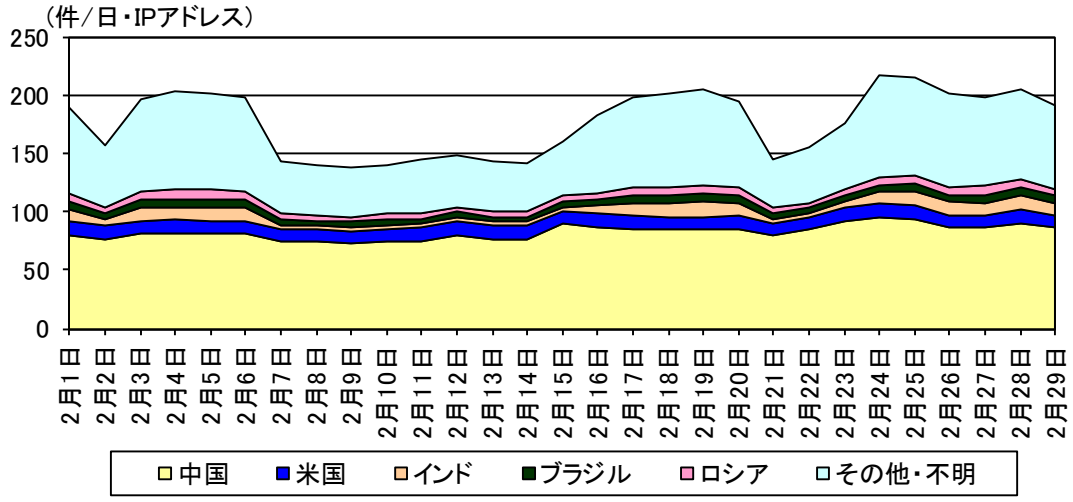

図 2-6　センサーのポート 1433/TCP における検知件数の推移

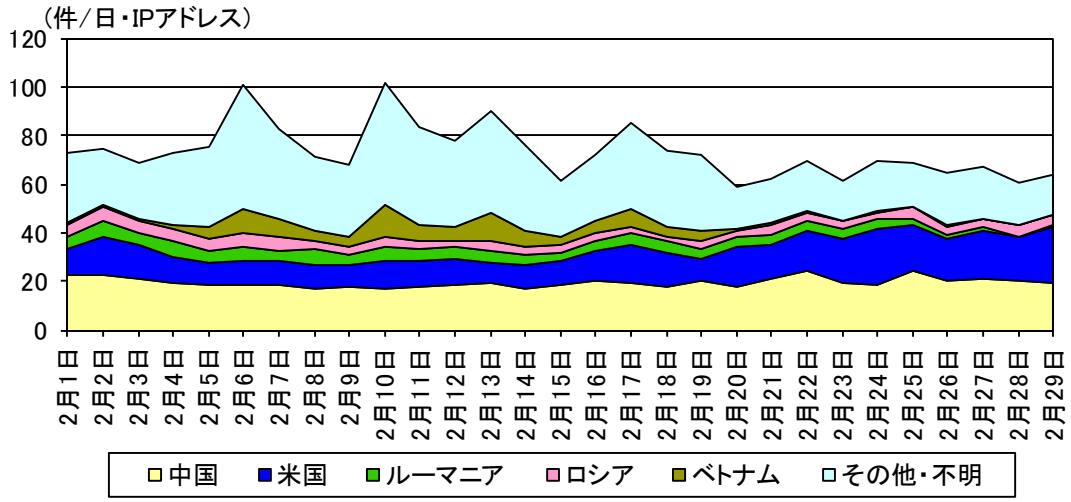

図 2-7　センサーのポート 22/TCP における検知件数の推移

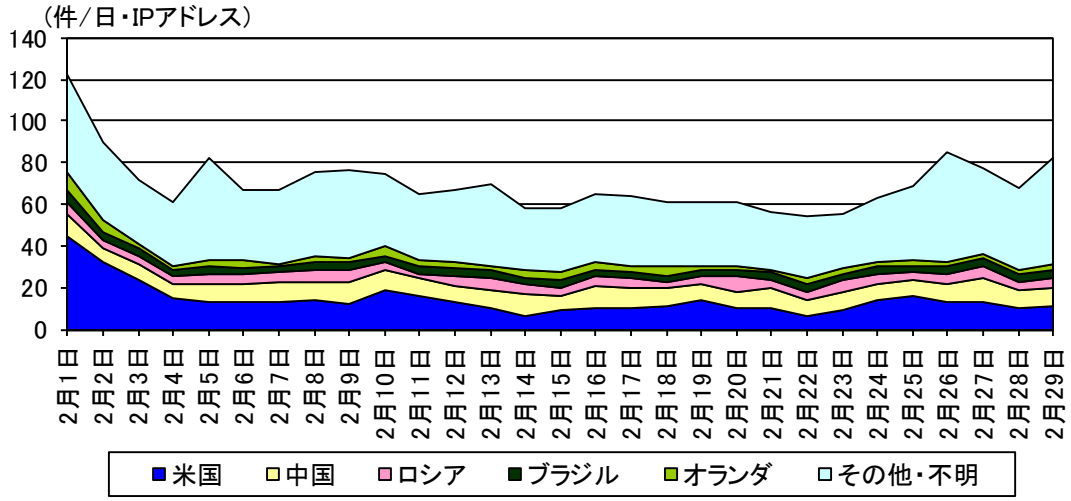

図 2-8　センサーのポート 80/TCP における検知件数の推移

2-2　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	3 位	オランダ	2,451.44 件	＋291.4%　（＋1,825.12 件）
2 位	1 位	ロシア	1,129.91 件	－14.6%　（－192.42 件）
3 位	2 位	中国	866.74 件	＋2.0%　（＋17.29 件）
4 位	4 位	米国	662.02 件	＋21.3%　（＋116.31 件）
5 位	43 位	スイス	225.14 件	－[ii]　（＋220.30 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	オランダ	2,451.44 件	＋291.4%　（＋1,825.12 件）	1 位	3 位
2 位	スイス	225.14 件	－[ii]　（＋220.30 件）	5 位	43 位
3 位	米国	662.02 件	＋21.3%　（＋116.31 件）	4 位	4 位
4 位	ルーマニア	187.32 件	＋39.0%　（＋52.58 件）	6 位	5 位
5 位	台湾	105.86 件	＋78.2%　（＋46.46 件）	9 位	12 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	ロシア	1,129.91 件	－14.6%　（－192.42 件）	2 位	1 位
2 位	ウクライナ	85.44 件	－23.8%　（－26.67 件）	12 位	7 位
3 位	英国	46.91 件	－15.2%　（－8.40 件）	18 位	13 位
4 位	イタリア	31.01 件	－9.8%　（－3.38 件）	23 位	20 位
5 位	メキシコ	40.71 件	－7.5%　（－3.32 件）	19 位	17 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、前月期比は記載していません。

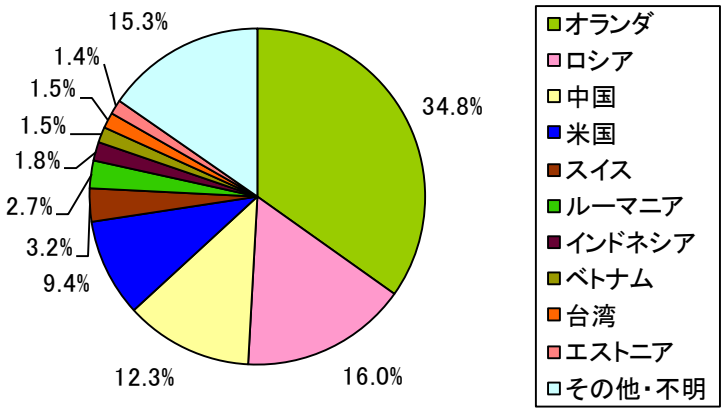

図 2-9　送信元国・地域別比率

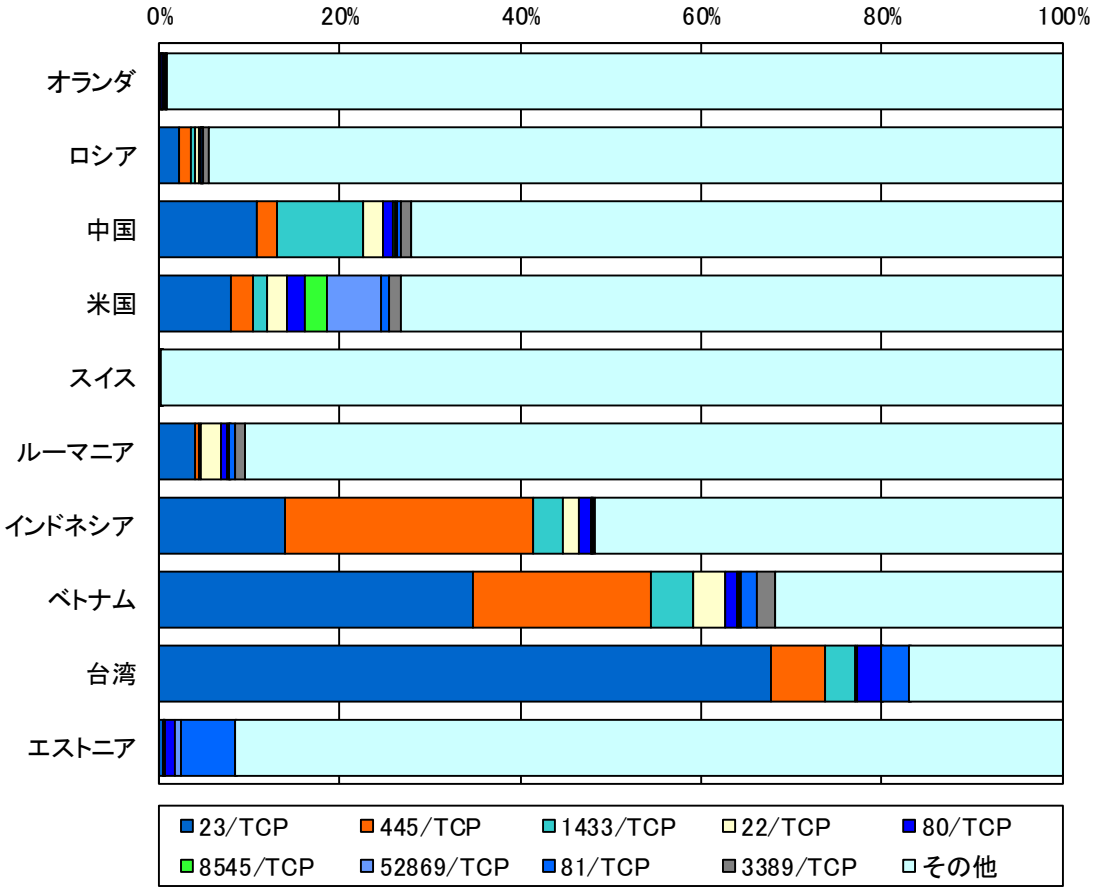

図 2-10　送信元国・地域別上位の宛先ポート別比率

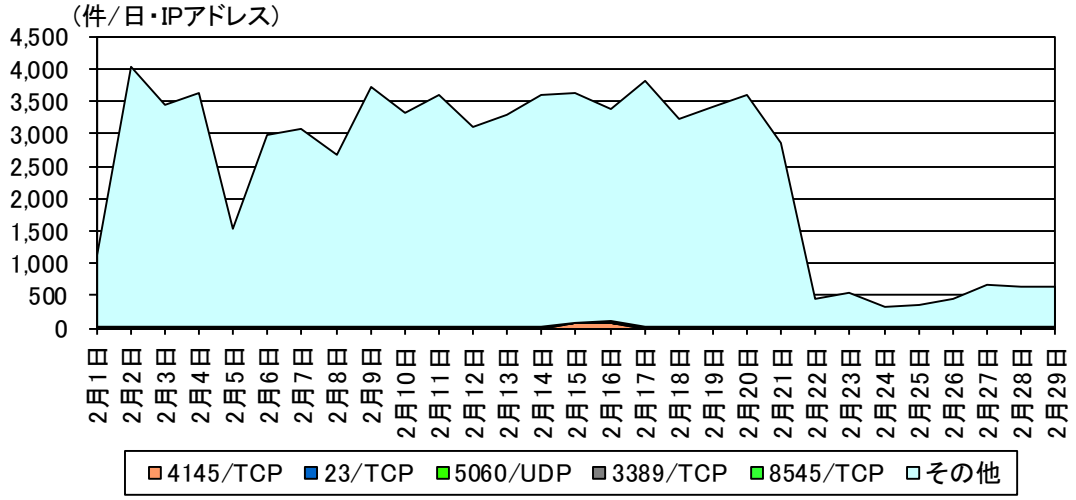

図 2-11　オランダからの検知件数の推移

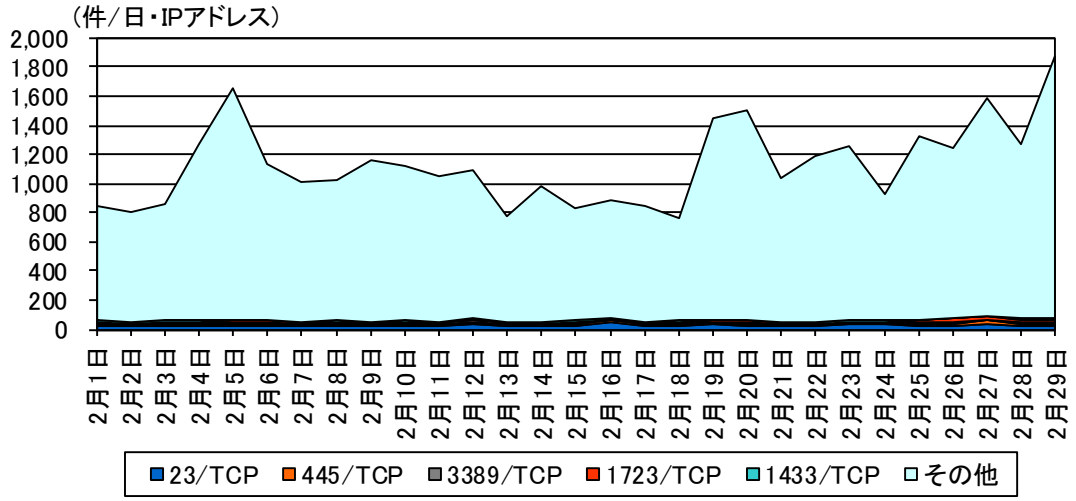

図 2-12　ロシアからの検知件数の推移

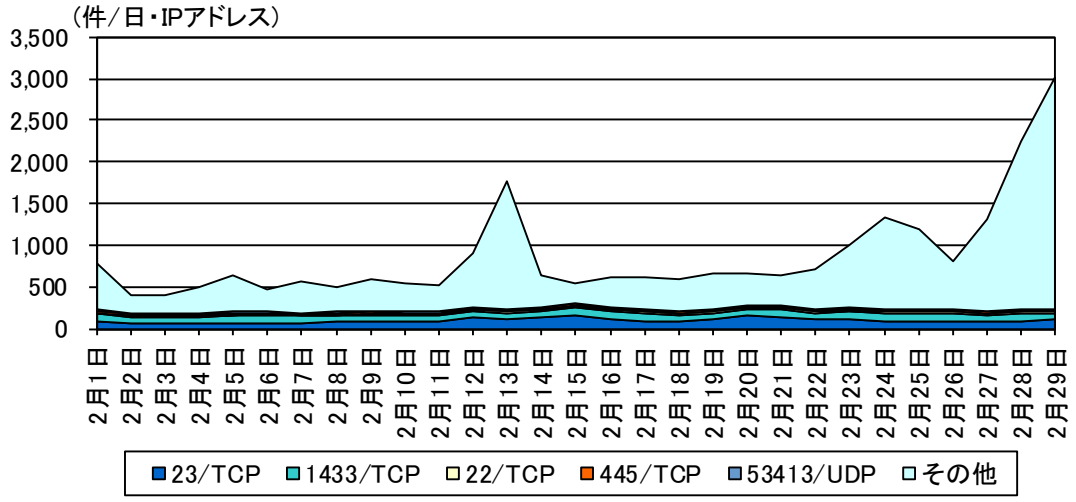

図 2-13　中国からの検知件数の推移

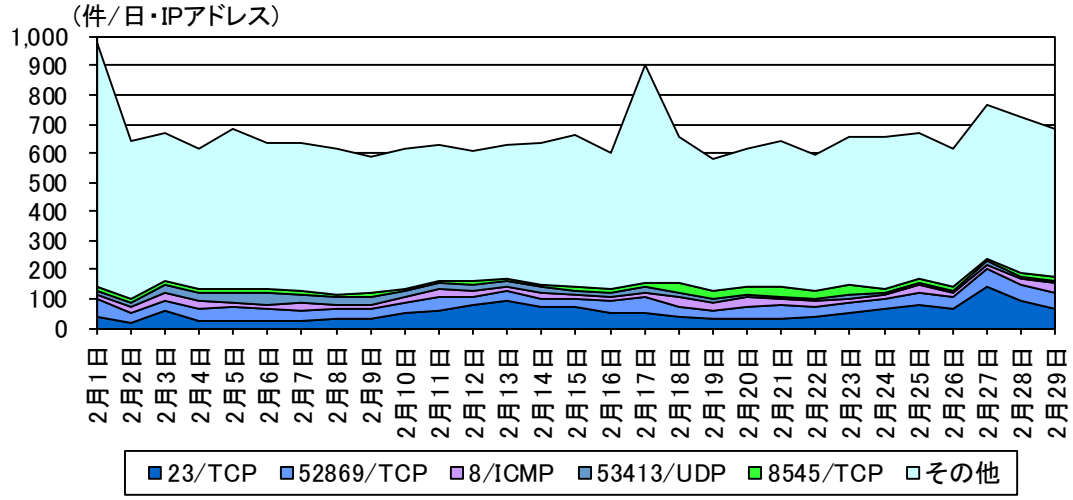

図 2-14　米国からの検知件数の推移

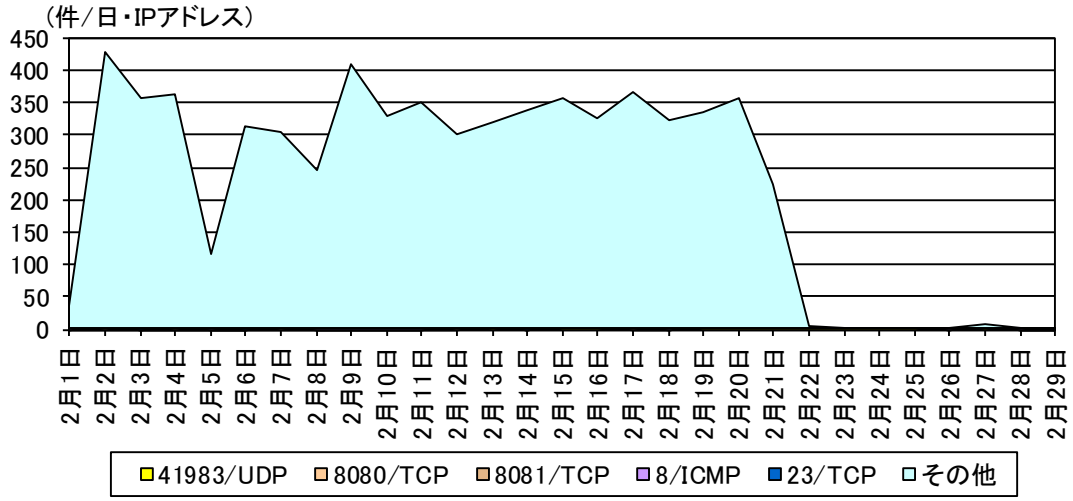

図 2-15　スイスからの検知件数の推移

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	Microsoft Windows Terminal server	331.73 件	＋3.8%　（＋12.26 件）	2 位	
2 位	2 位	INDICATOR-SCAN	255.52 件	－5.5%　（－14.76 件）		1 位
3 位	3 位	SMBv1	105.99 件	－3.8%　（－4.19 件）		3 位
4 位	7 位	Remote Desktop	45.72 件	＋211.7%　（＋31.05 件）	1 位	
5 位	5 位	ICMP	24.72 件	＋4.1%　（＋0.97 件）		

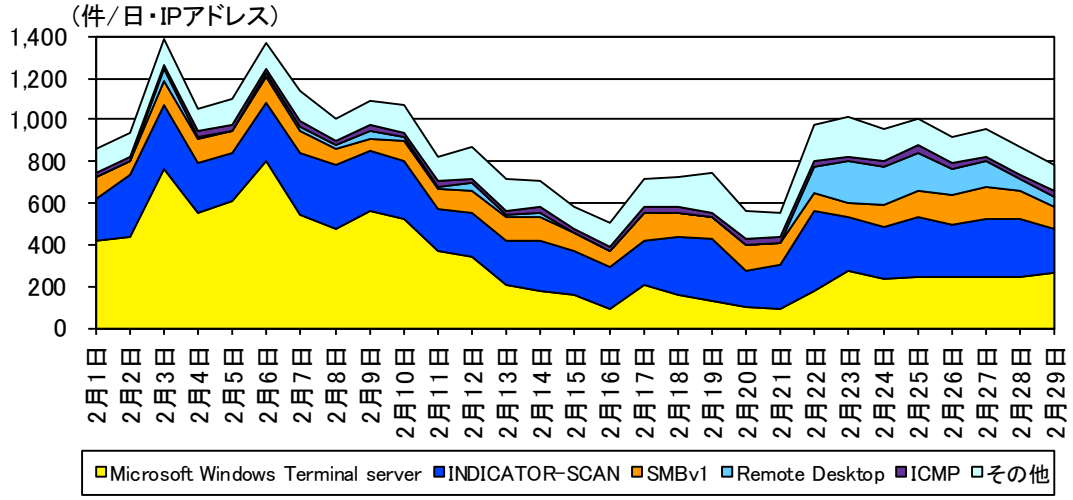

図 3-1　不正侵入等の攻撃手法別検知件数の推移

[i] 一日・1IP アドレス当たり。

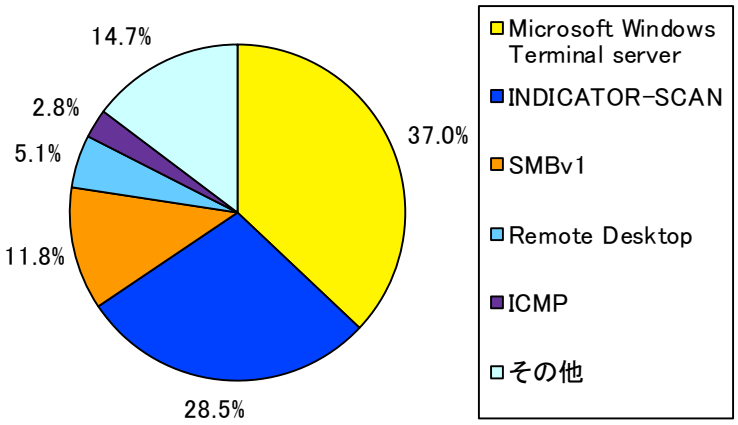

図 3-2 不正侵入等の攻撃手法別検知比率

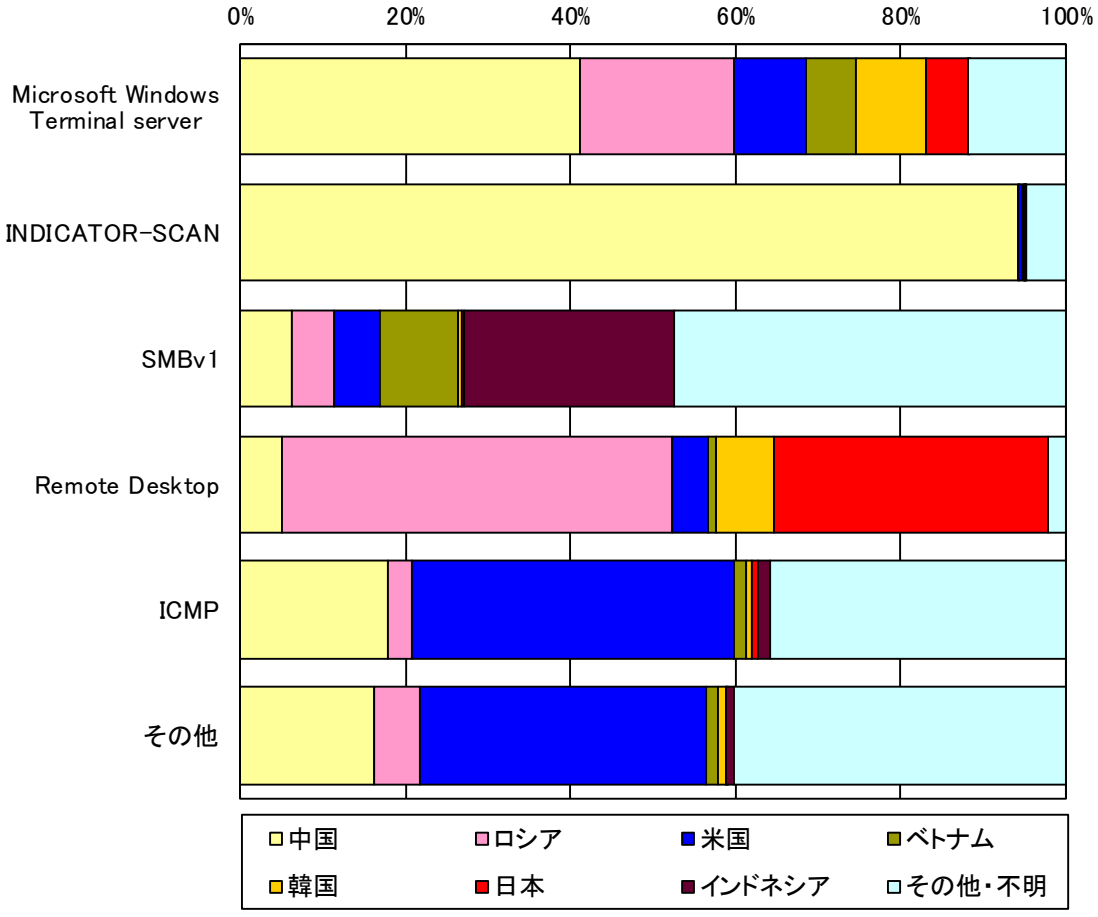

図 3-3 不正侵入等の攻撃手法の国・地域別検知比率

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	411.93 件	＋23.2% （＋77.50 件）
2 位	3 位	ロシア	97.78 件	＋8.9% （＋7.98 件）
3 位	2 位	米国	92.47 件	－14.5% （－15.62 件）
4 位	5 位	ベトナム	33.75 件	－7.6% （－2.79 件）
5 位	27 位	韓国	33.46 件	＋962.7% （＋30.31 件）

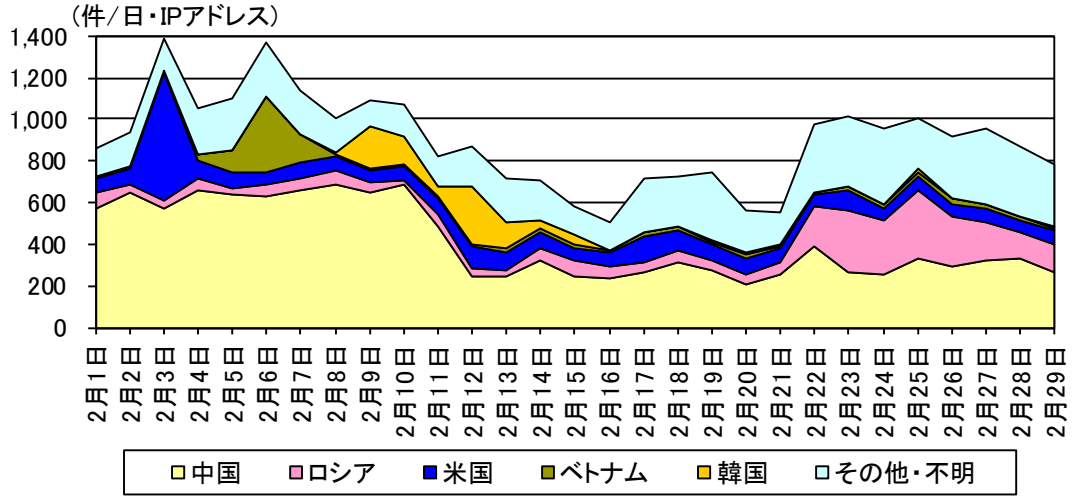

図 3-4 不正侵入等の送信元国・地域別検知件数の推移

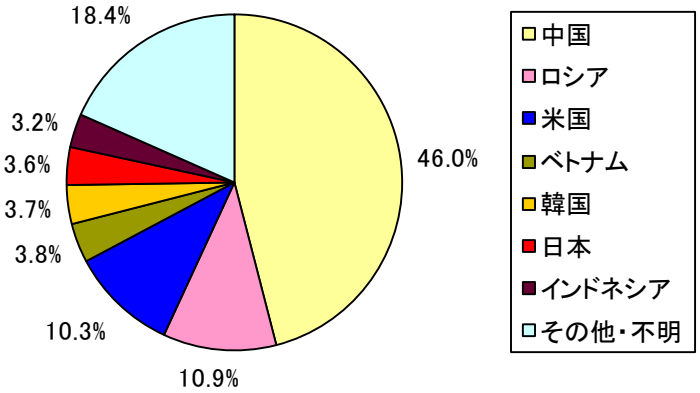

図 3-5 不正侵入等の送信元国・地域別検知比率

[i] 一日・1IP アドレス当たり。

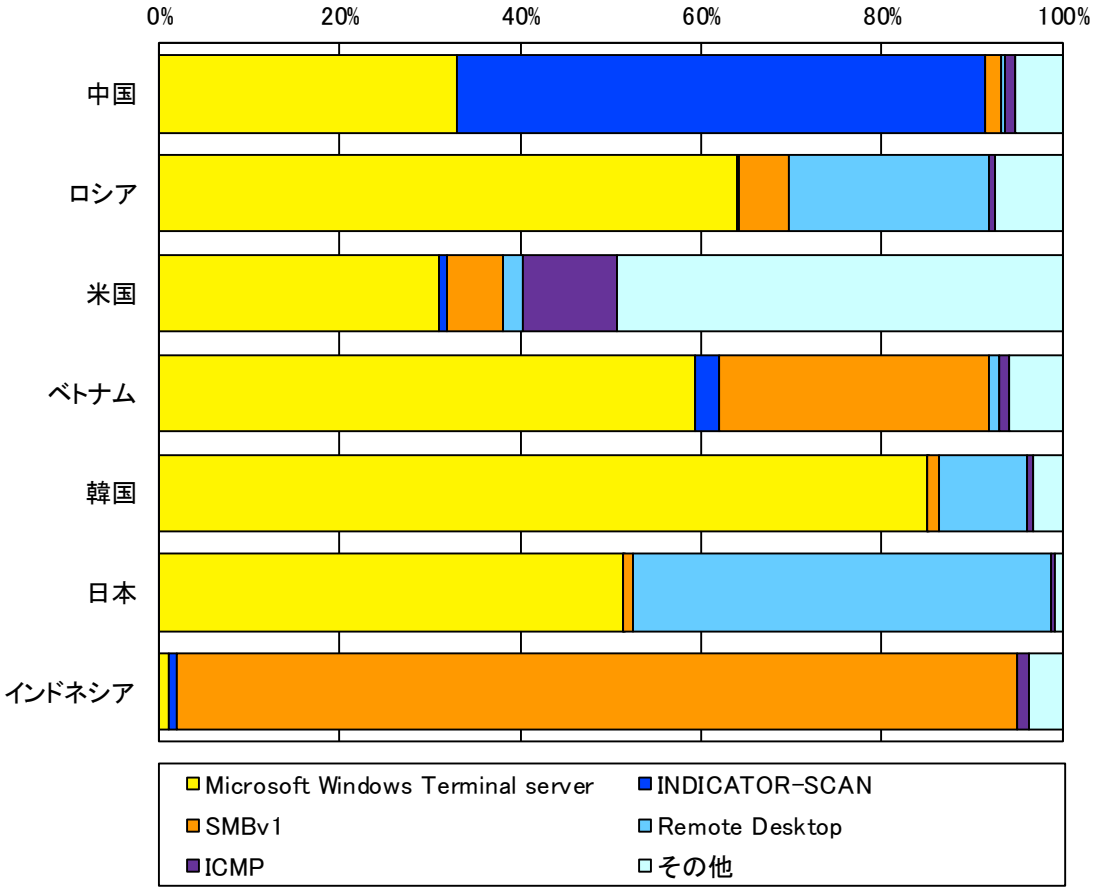

図 3-6 不正侵入等の送信元国・地域別上位の攻撃手法別検知比率

4　DoS 攻撃被害の観測結果

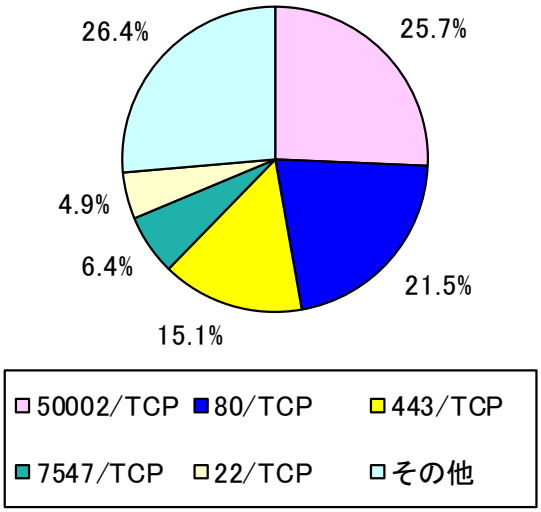

図 4-1　跳ね返りパケット送信元ポート別比率

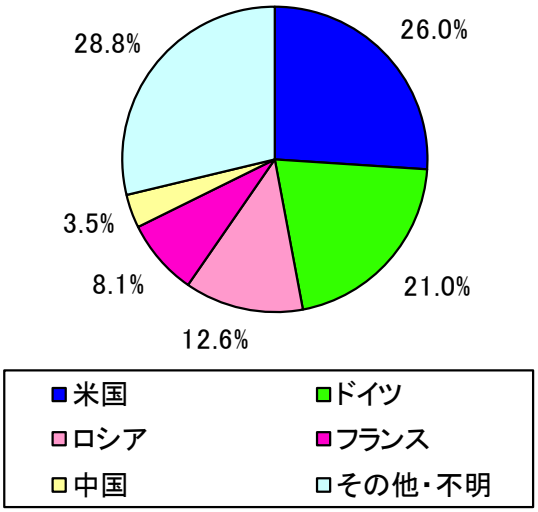

図 4-2　跳ね返りパケット送信元国・地域別比率

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