令和元年6月 21 日

平成 31年3月期観測資料

1　観測結果概要

平成 31 年3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 3,127.8 件で、平成 31 年2月期（以下「前期」という。）と比較して 662.0 件（17.5％）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 47,499.6 個で、前期と比較して 1,721.9 個（3.5%）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 834.1 件で、前期と比較して 108.9 件（11.6%）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 8,805.2 個で、前期と比較して 1,049.1 個（13.5%）増加しました。

DoS 攻撃被害検知件数は、一日当たり 8,849.9 件で、前期と比較して 4,370.4 件（33.1%）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 348.2 個で、前期と比較して 27.6 個（7.3%）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	495.60 件	＋10.9%	（＋48.85 件）
2 位	2 位	445/TCP	432.48 件	＋24.0%	（＋83.63 件）
3 位	6 位	52869/TCP	117.85 件	＋35.9%	（＋31.10 件）
4 位	5 位	22/TCP	78.29 件	－10.9%	（－9.60 件）
5 位	8 位	80/TCP	51.29 件	－13.4%	（－7.90 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	445/TCP	432.48 件	＋24.0%	（＋83.63 件）	2 位	2 位
2 位	23/TCP	495.60 件	＋10.9%	（＋48.85 件）	1 位	1 位
3 位	52869/TCP	117.85 件	＋35.9%	（＋31.10 件）	3 位	6 位
4 位	9527/TCP	15.96 件	－[ii]	（＋15.72 件）	20 位	－[ii]
5 位	5555/TCP	32.94 件	＋23.0%	（＋6.15 件）	10 位	15 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	1433/TCP	15.11 件	－84.2%	（－80.24 件）	21 位	3 位
2 位	123/UDP	38.03 件	－57.9%	（－52.22 件）	8 位	4 位
3 位	8545/TCP	22.71 件	－69.5%	（－51.84 件）	16 位	7 位
4 位	5060/UDP	23.70 件	－38.0%	（－14.51 件）	15 位	11 位
5 位	5038/TCP	16.82 件	－37.1%	（－9.92 件）	19 位	16 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。

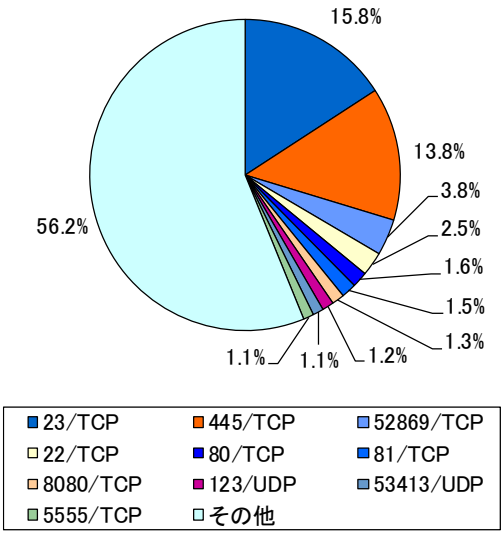

図 2-1　宛先ポート別比率（全て）[i]

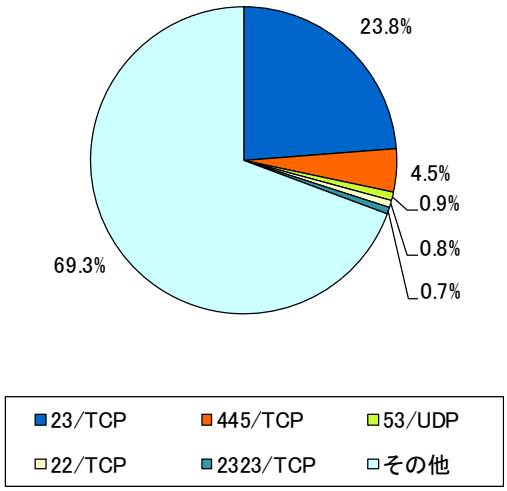

図 2-2　宛先ポート別比率（日本国内）

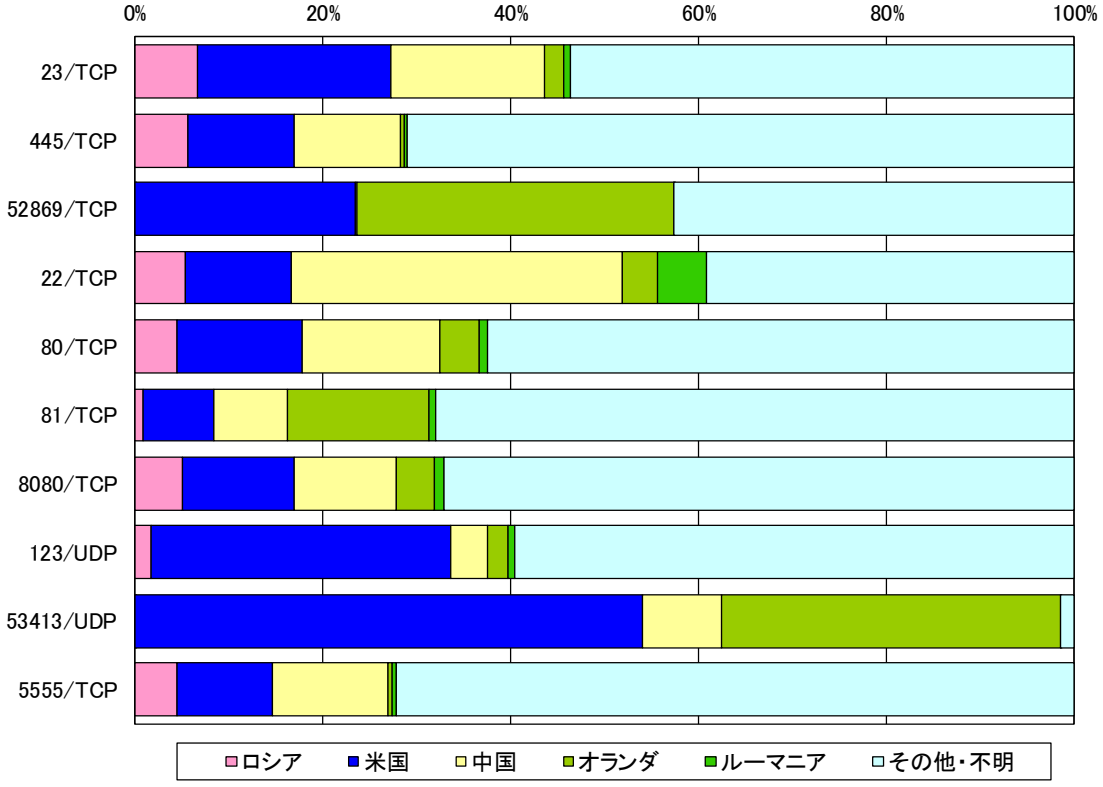

図 2-3　宛先ポート別上位の着信元国・地域別比率 [ii]

[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。

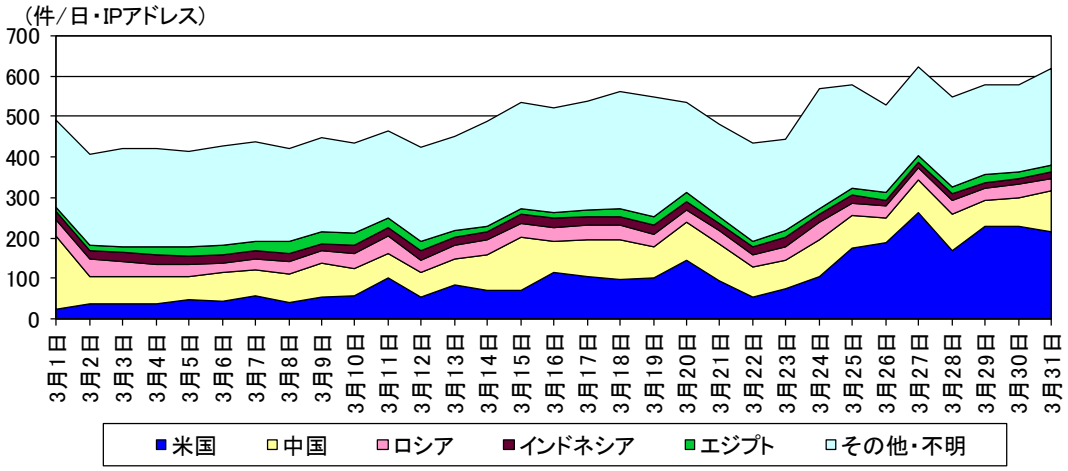

図 2-4　センサーのポート 23/TCP における検知件数の推移

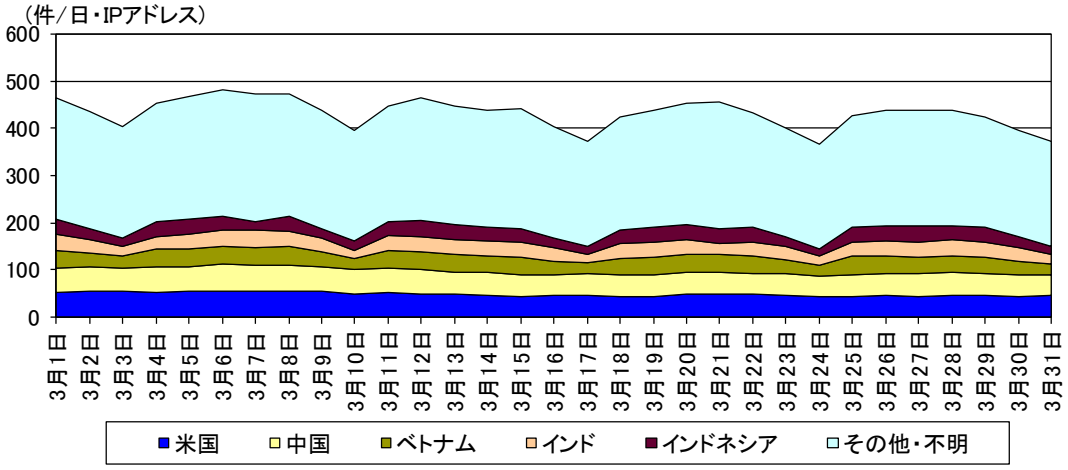

図 2-5　センサーのポート 445/TCP における検知件数の推移

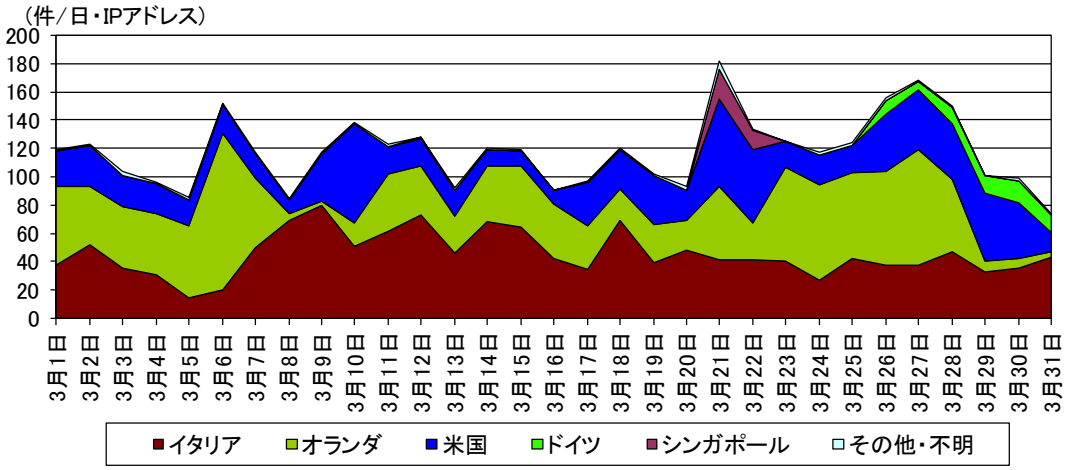

図 2-6　センサーのポート 52869/TCP における検知件数の推移

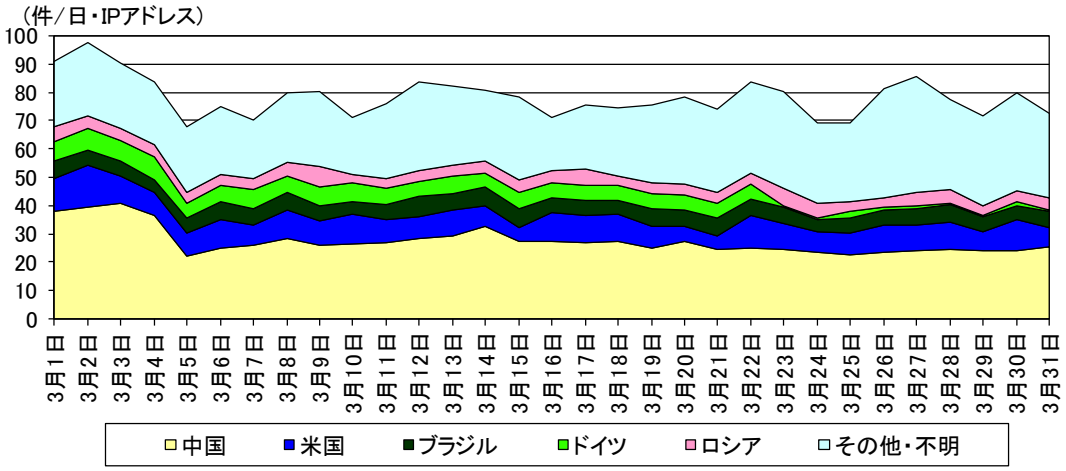

図 2-7　センサーのポート 22/TCP における検知件数の推移

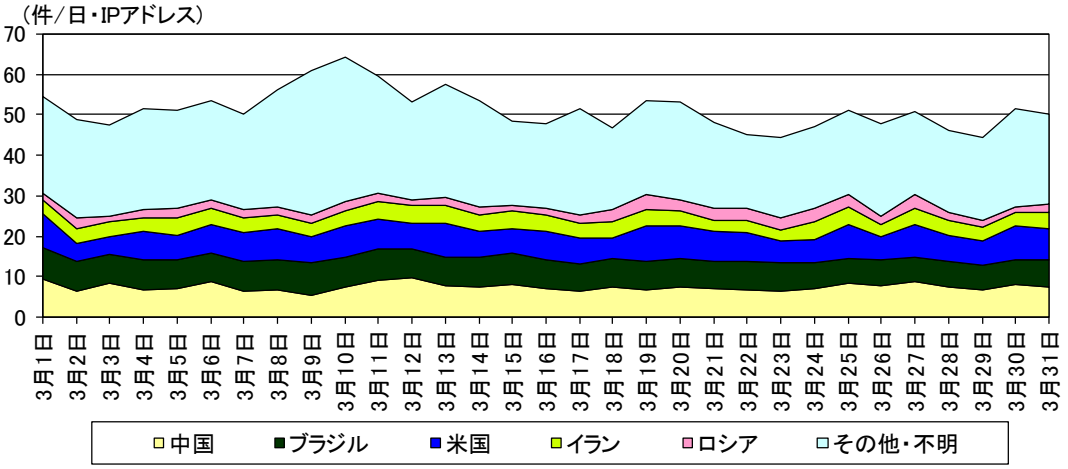

図 2-8　センサーのポート 80/TCP における検知件数の推移

2-2　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	622.58 件	－27.1%　（－231.23 件）
2 位	2 位	米国	538.47 件	＋1.7%　（＋9.16 件）
3 位	3 位	中国	378.84 件	－9.5%　（－39.73 件）
4 位	5 位	オランダ	200.71 件	＋28.8%　（＋44.85 件）
5 位	13 位	ルーマニア	126.49 件	＋80.7%　（＋56.47 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	ルーマニア	126.49 件	＋80.7%　（＋56.47 件）	5 位	13 位
2 位	オランダ	200.71 件	＋28.8%　（＋44.85 件）	4 位	5 位
3 位	イタリア	95.96 件	＋31.6%　（＋23.04 件）	6 位	12 位
4 位	南アフリカ	44.94 件	＋55.7%　（＋16.08 件）	15 位	23 位
5 位	エジプト	26.23 件	＋98.5%　（＋13.02 件）	24 位	31 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	622.58 件	－27.1%　（－231.23 件）	1 位	1 位
2 位	リトアニア	30.50 件	－87.9%　（－221.65 件）	19 位	4 位
3 位	パナマ	7.20 件	－91.8%　（－80.62 件）	39 位	9 位
4 位	ブルガリア	11.69 件	－86.1%　（－72.55 件）	31 位	10 位
5 位	韓国	56.36 件	－48.7%　（－53.45 件）	13 位	6 位

[i] 一日・1IP アドレス当たり。

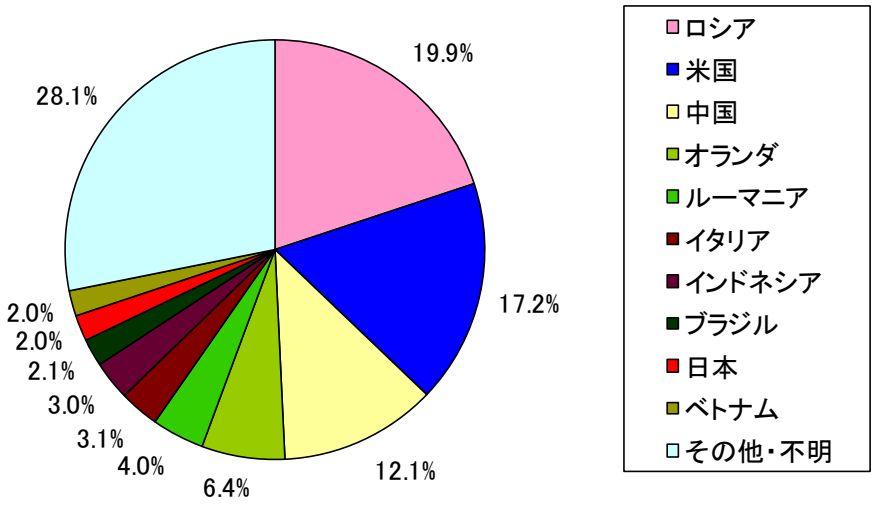

図 2-9　着信元国・地域別比率

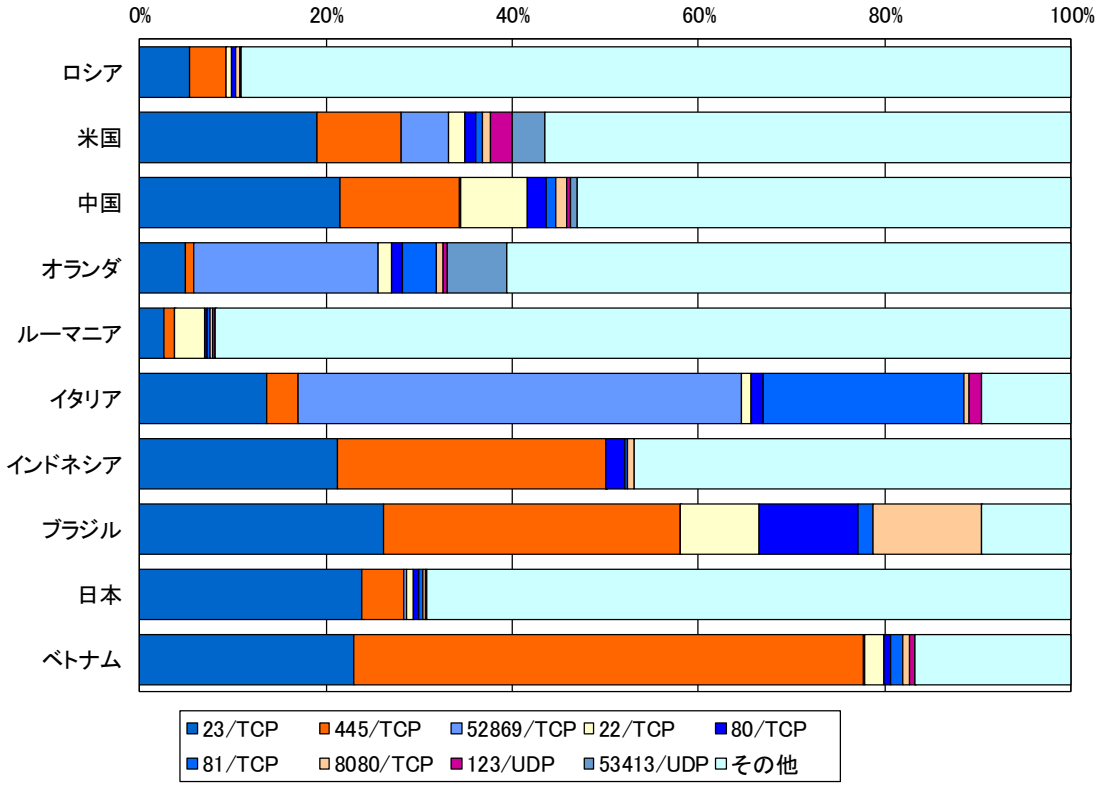

図 2-10　着信元国・地域別上位の宛先ポート別比率

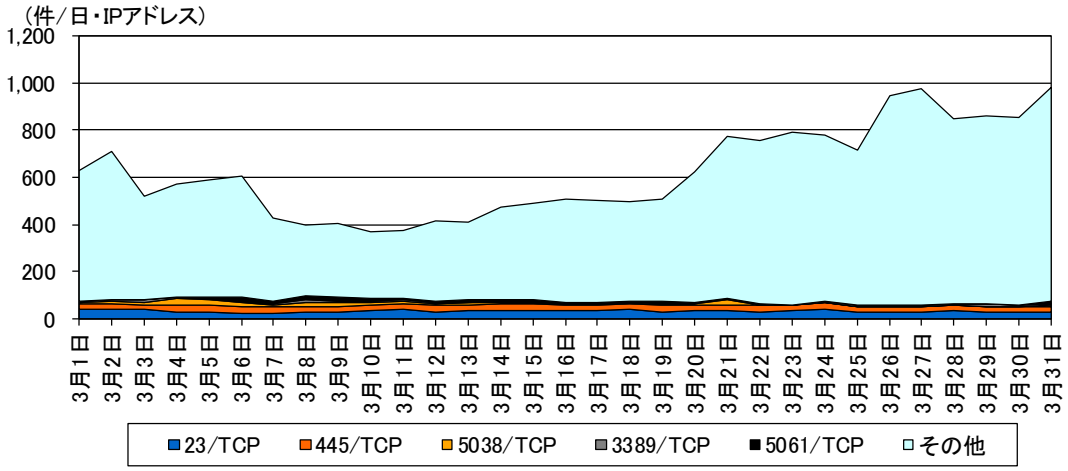

図 2-11　ロシアからの検知件数の推移

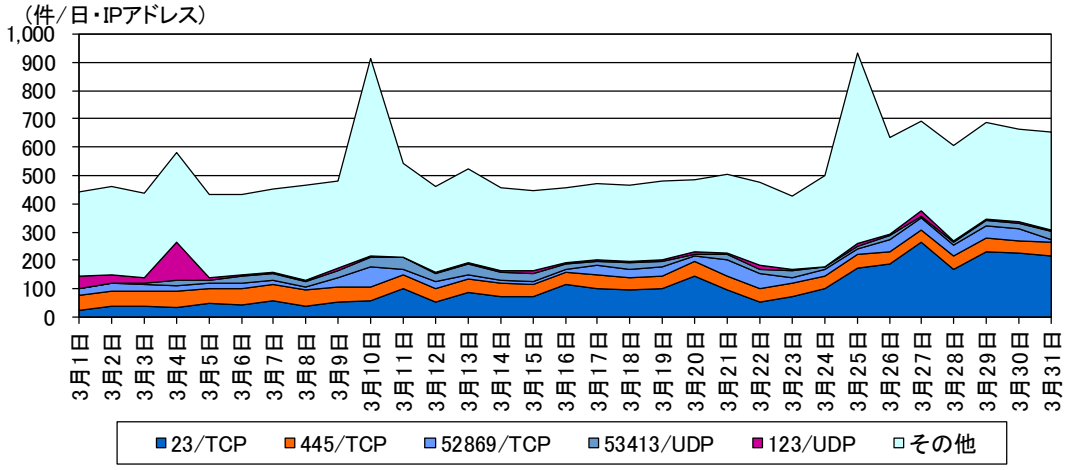

図 2-12　米国からの検知件数の推移

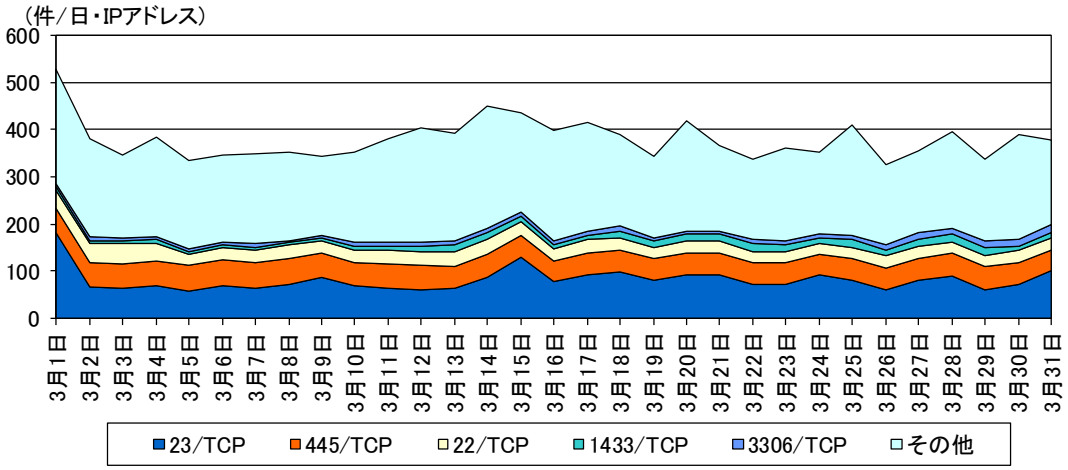

図 2-13　中国からの検知件数の推移

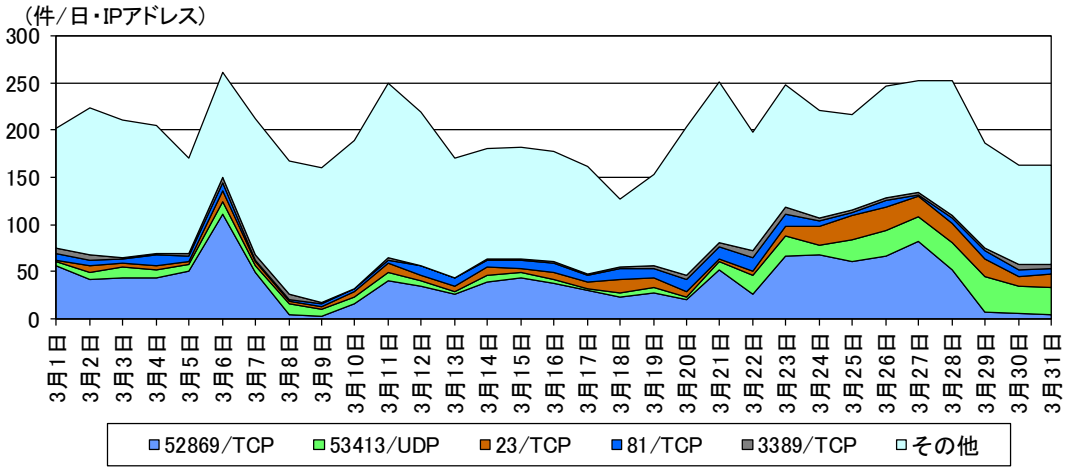

図 2-14 オランダからの検知件数の推移

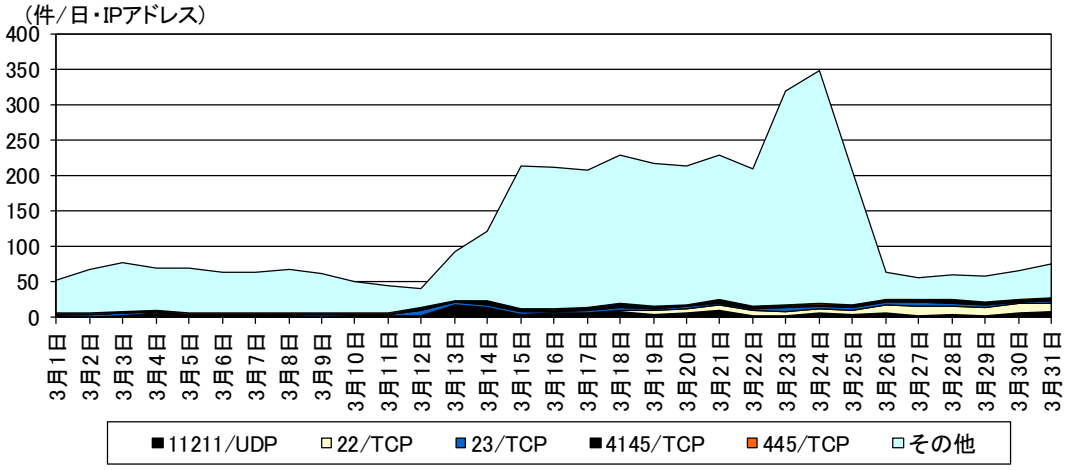

図 2-15 ルーマニアからの検知件数の推移

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	429.90 件	＋29.2%　（＋97.07 件）	1 位	
2 位	3 位	SMBv1	170.47 件	＋9.2%　（＋14.40 件）	2 位	
3 位	2 位	Microsoft Windows Terminal server	119.20 件	－56.6%　（－155.23 件）		1 位
4 位	5 位	VOIP	23.35 件	－39.9%　（－15.52 件）		3 位
5 位	6 位	ICMP	20.89 件	＋1.3%　（＋0.28 件）		

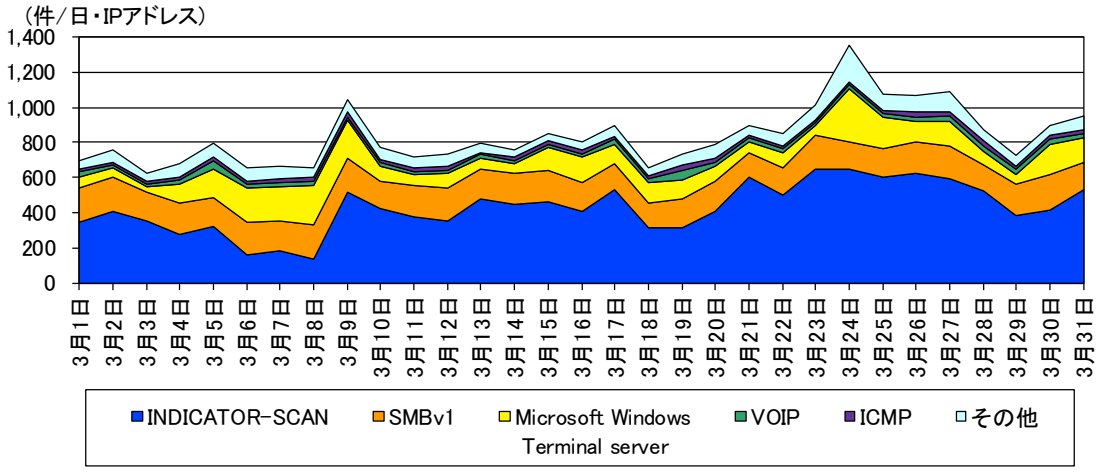

図 3-1　不正侵入等の攻撃手法別検知件数の推移

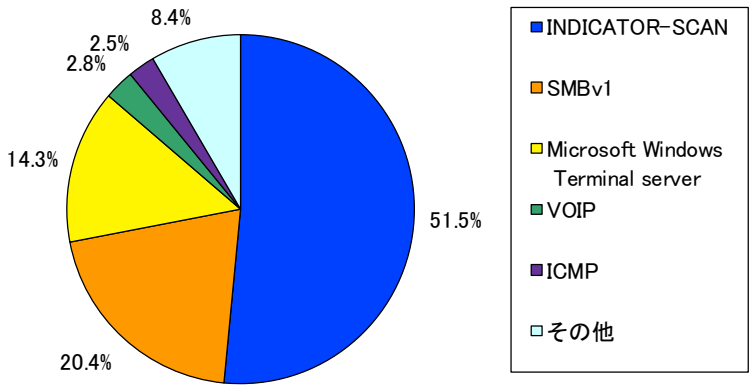

図 3-2　不正侵入等の攻撃手法別検知比率

[i] 一日・1IP アドレス当たり。

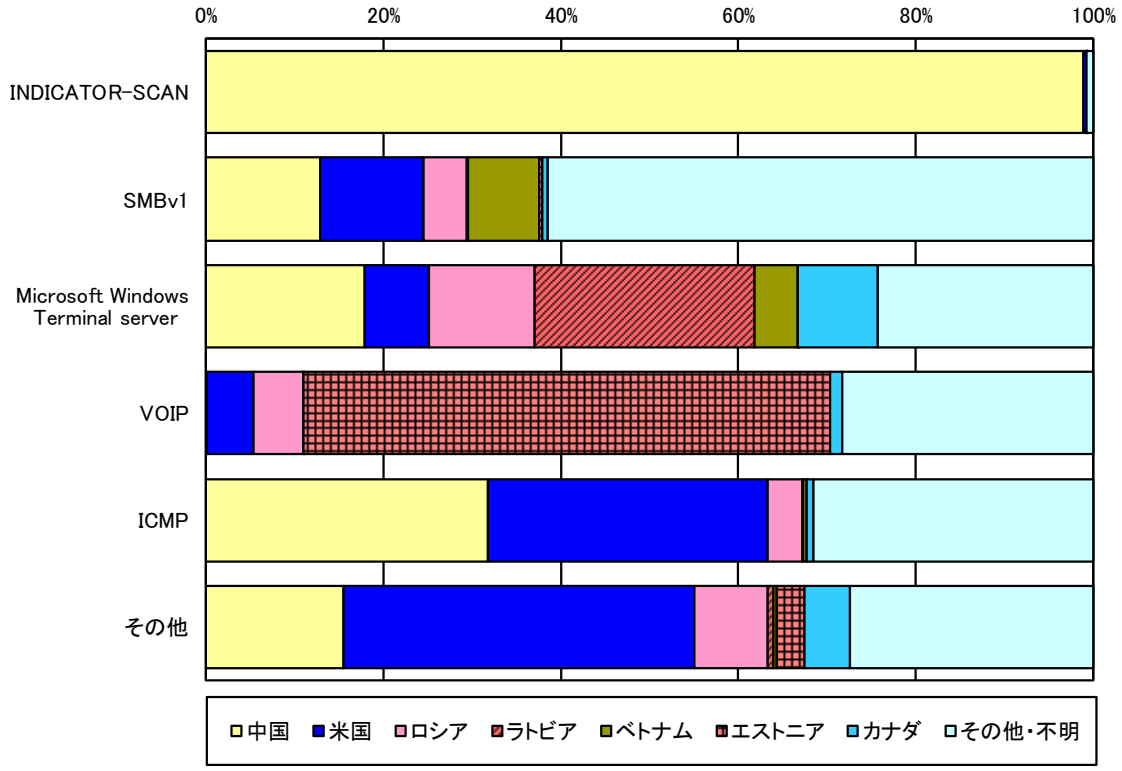

図 3-3 不正侵入等の攻撃手法の国・地域別検知比率

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	485.93 件	＋20.9% （＋84.11 件）
2 位	4 位	米国	65.46 件	＋19.8% （＋10.80 件）
3 位	2 位	ロシア	30.67 件	－82.3% （－143.02 件）
4 位	3 位	ラトビア	30.14 件	－61.5% （－48.13 件）
5 位	8 位	ベトナム	20.24 件	＋49.2% （＋6.67 件）

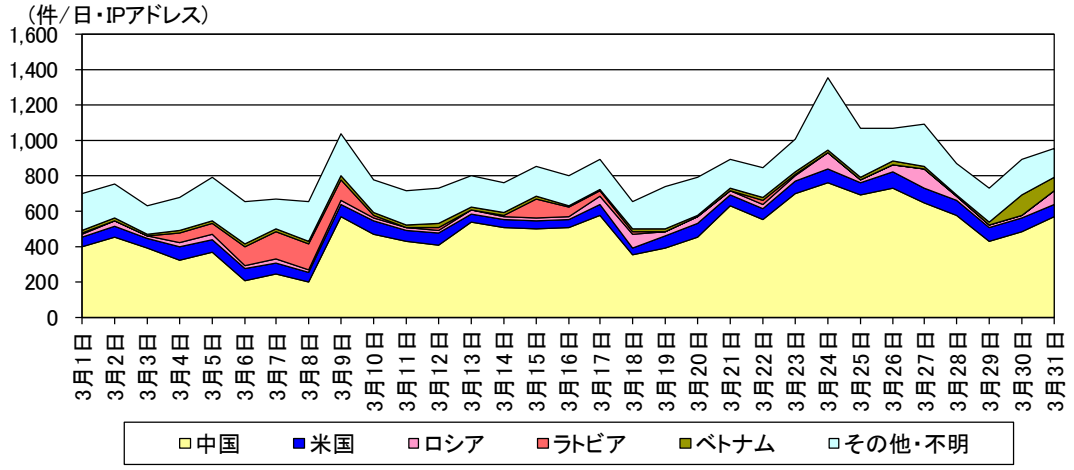

図 3-4 不正侵入等の着信元国・地域別検知件数の推移

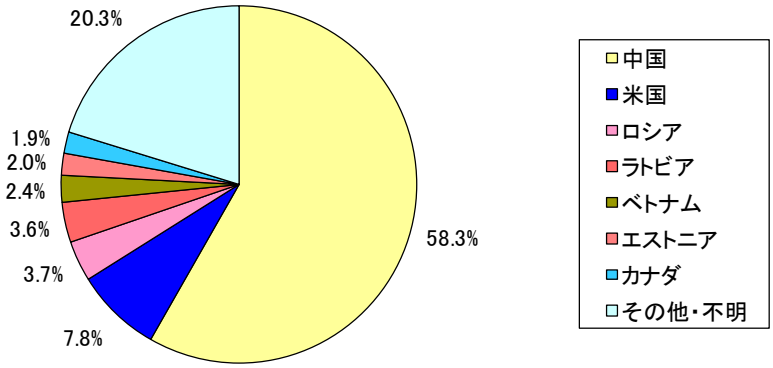

図 3-5 不正侵入等の着信元国・地域別検知比率

[i] 一日・1IP アドレス当たり。

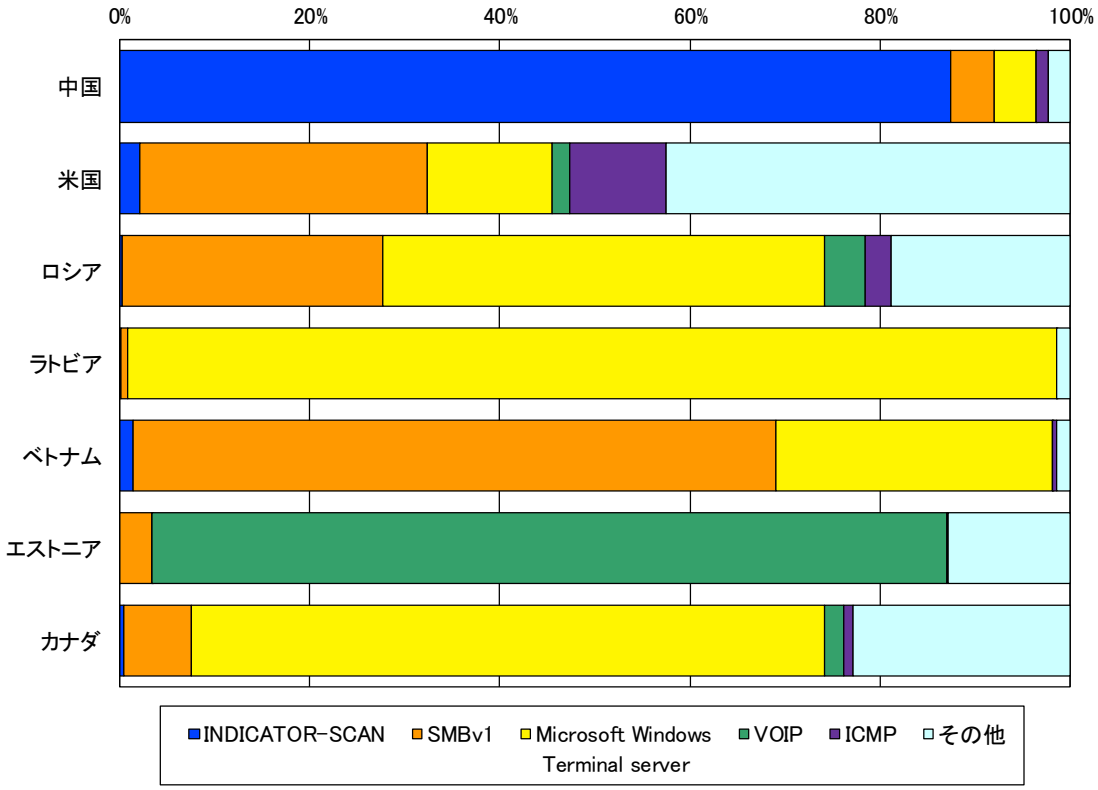

図 3-6 不正侵入等の着信元国・地域別上位の攻撃手法別検知比率

4　DoS 攻撃被害の観測結果

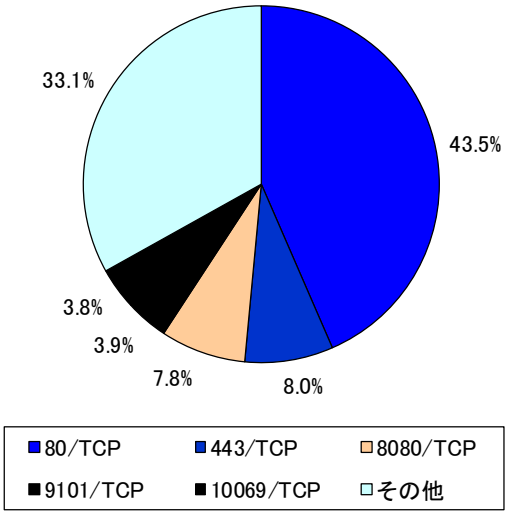

図 4-1　跳ね返りパケット着信元ポート別比率

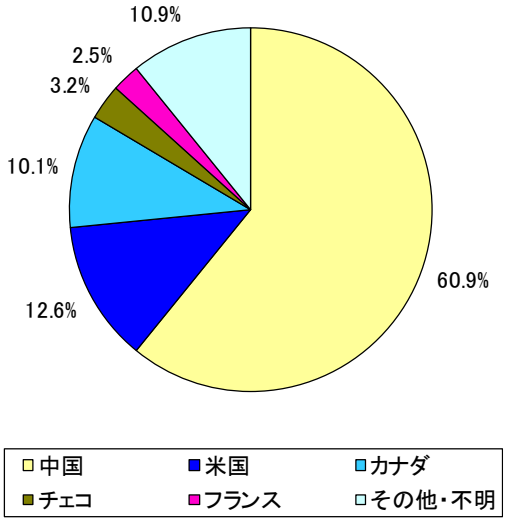

図 4-2　跳ね返りパケット着信元国・地域別比率

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