Distributed via
@police
https://www.npa.go.jp/cyberpolice/

令和２年７月 16 日

令和2年6月期観測資料

1　観測結果概要

令和2年6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 8,190.2 件で、令和2年5月期（以下「前月期」という。）の 6,413.1 件と比較して 1,777.1 件（27.7%）増加しました。また、送信元 IP アドレス [i] 数は、一日当たり 53,205.4 個で、前月期の 53,994.7 個と比較して 789.3 個（1.5%）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 1,076.6 件で、前月期の 972.5 件と比較して 104.1 件（10.7%）増加しました。また、送信元 IP アドレス数は、一日当たり 12,770.4 個で、前月期の 12,527.4 個と比較して 243.0 個（1.9%）増加しました。

DoS 攻撃被害検知件数は、一日当たり 12,769.9 件で、前月期の 49,259.0 件と比較して 36,489.1 件（74.1%）減少しました。また、送信元 IP アドレス数は、一日当たり 392.4 個で、前月期の 6,866.4 個と比較して 6,474.0 個（94.3%）減少しました。

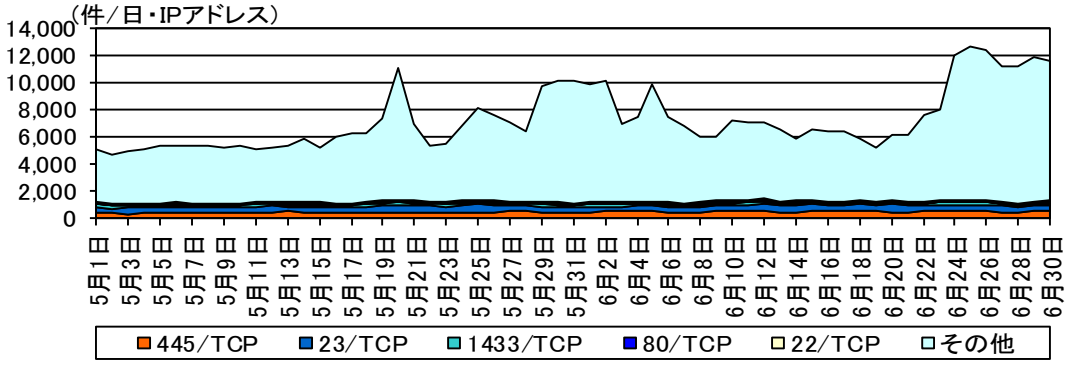

図 1-1　宛先ポート別検知件数の推移

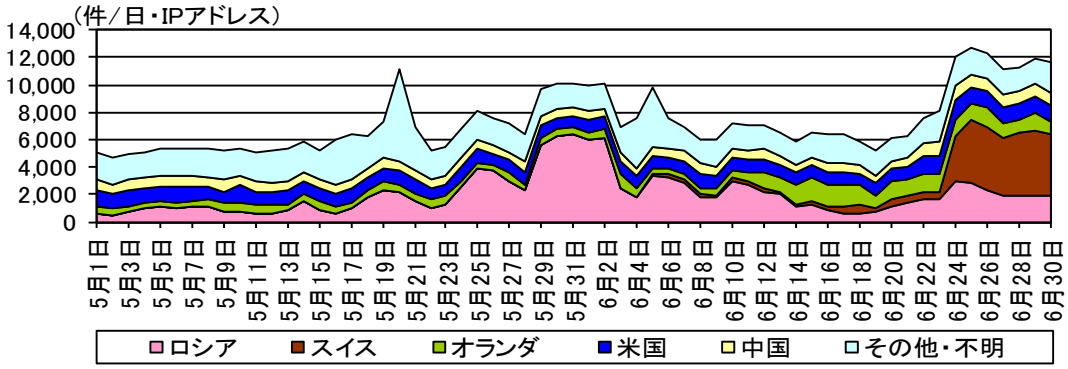

図 1-2　送信元国・地域別検知件数の推移 [ii]

[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。
[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。

Copyright 2020 Cyber Force Center, NPA JAPAN

2　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。

2-1　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。）。

2-2　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 2-1 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 2-1　パケットの分類

章	集計対象	
3　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
5　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

Copyright 2020 Cyber Force Center, NPA JAPAN

2-3　不正侵入等の検知

検知された各シグネチャ は、表 2-2 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 2-2 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-APACHE	Apache の脆弱性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

Copyright 2020 Cyber Force Center, NPA JAPAN

3　センサーにおけるアクセス検知の観測結果

3-1　宛先ポート別アクセス検知件数

表 3-1　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	2 位	445/TCP	488.30 件	＋16.6%　（＋69.53 件）
2 位	1 位	23/TCP	436.20 件	＋1.8%　（＋7.60 件）
3 位	3 位	1433/TCP	156.20 件	－1.4%　（－2.26 件）
4 位	4 位	80/TCP	85.78 件	－2.0%　（－1.78 件）
5 位	5 位	22/TCP	79.94 件	－6.9%　（－5.91 件）

表 3-2　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	445/TCP	488.30 件	＋16.6%　（＋69.53 件）	1 位	2 位
2 位	52869/TCP	68.83 件	＋103.4%　（＋34.99 件）	6 位	15 位
3 位	60001/TCP	21.80 件	＋181.1%　（＋14.04 件）	22 位	53 位
4 位	53/UDP	20.91 件	＋93.0%　（＋10.08 件）	23 位	40 位
5 位	23/TCP	436.20 件	＋1.8%　（＋7.60 件）	2 位	1 位

表 3-3　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	8291/TCP	26.18 件	－44.1%　（－20.68 件）	16 位	9 位
2 位	5555/TCP	24.90 件	－41.3%　（－17.49 件）	17 位	13 位
3 位	81/TCP	48.90 件	－23.2%　（－14.73 件）	8 位	7 位
4 位	37215/TCP	13.31 件	－50.3%　（－13.46 件）	27 位	18 位
5 位	53413/UDP	29.99 件	－29.8%　（－12.74 件）	15 位	12 位

[i] 一日・1IP アドレス当たり。

Copyright 2020 Cyber Force Center, NPA JAPAN

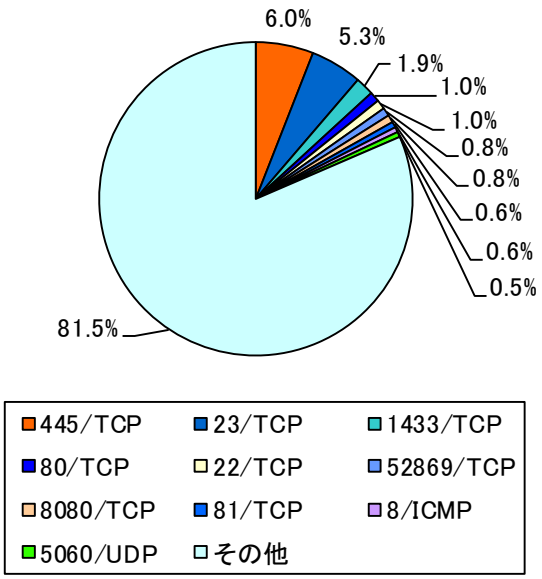

図 3-1　宛先ポート別比率（全て）[i]

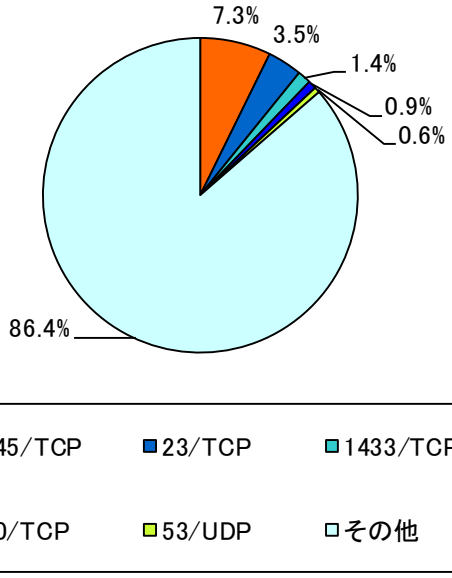

図 3-2　宛先ポート別比率（日本国内）

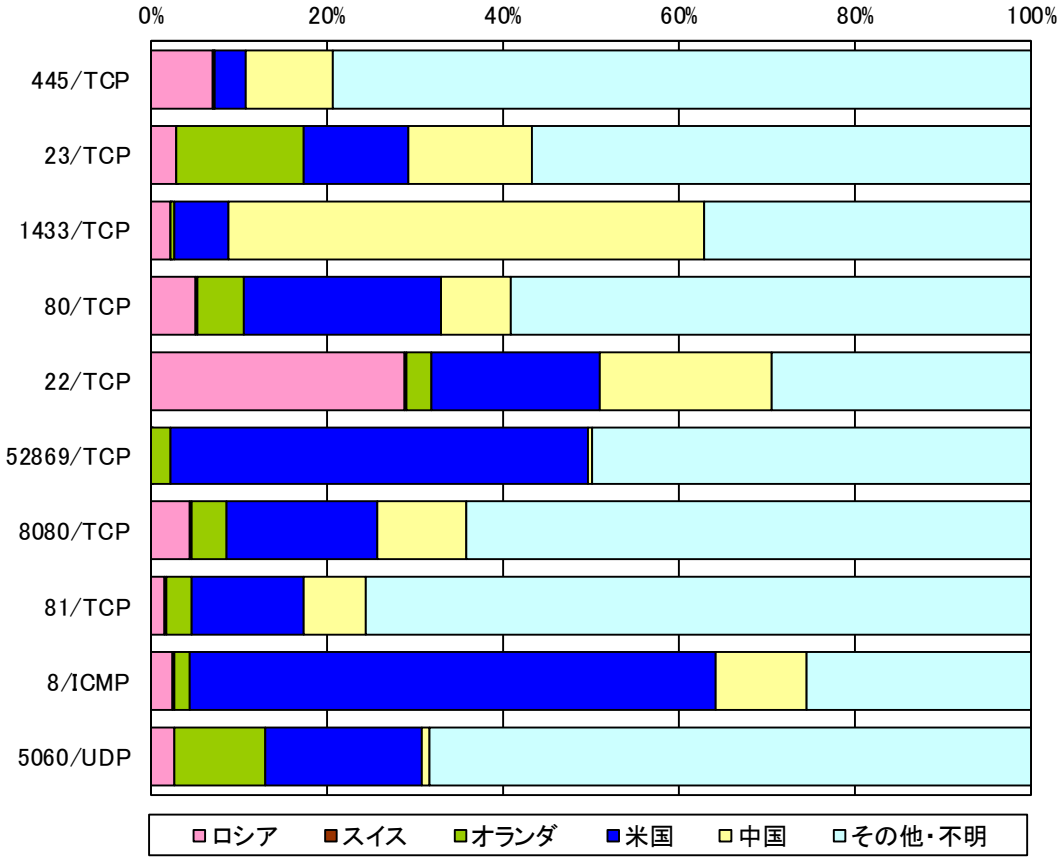

図 3-3　宛先ポート別上位の送信元国・地域別比率

[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。

Copyright 2020 Cyber Force Center, NPA JAPAN

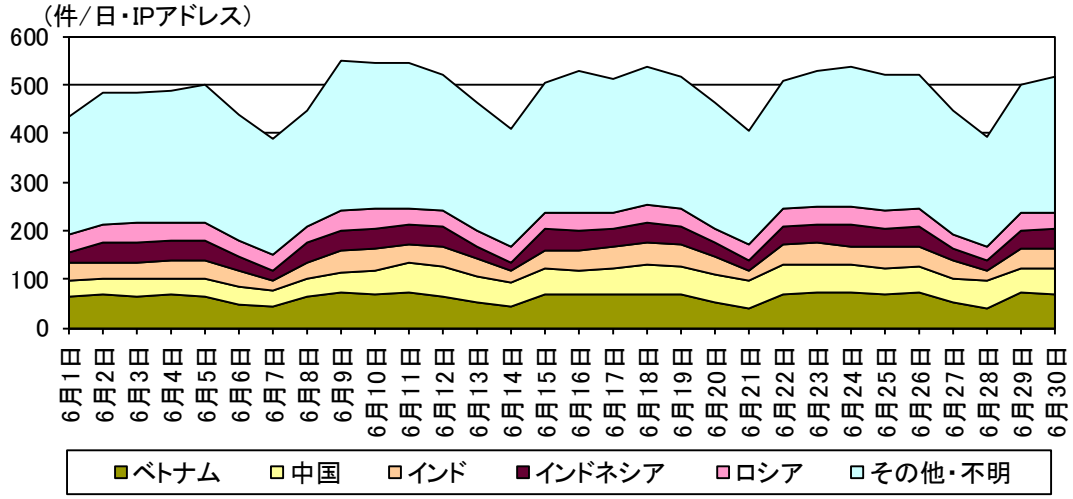

図 3-4　センサーのポート 445/TCP における検知件数の推移

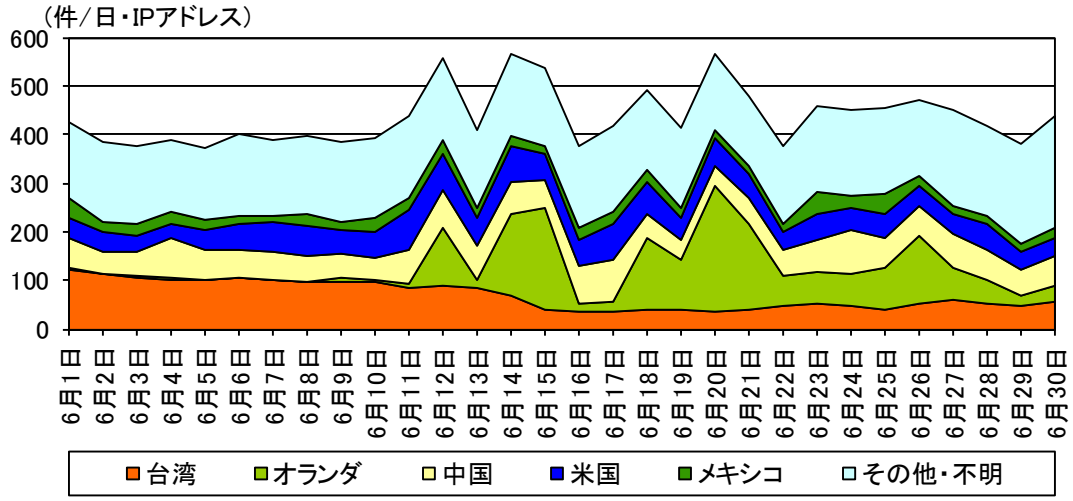

図 3-5　センサーのポート 23/TCP における検知件数の推移

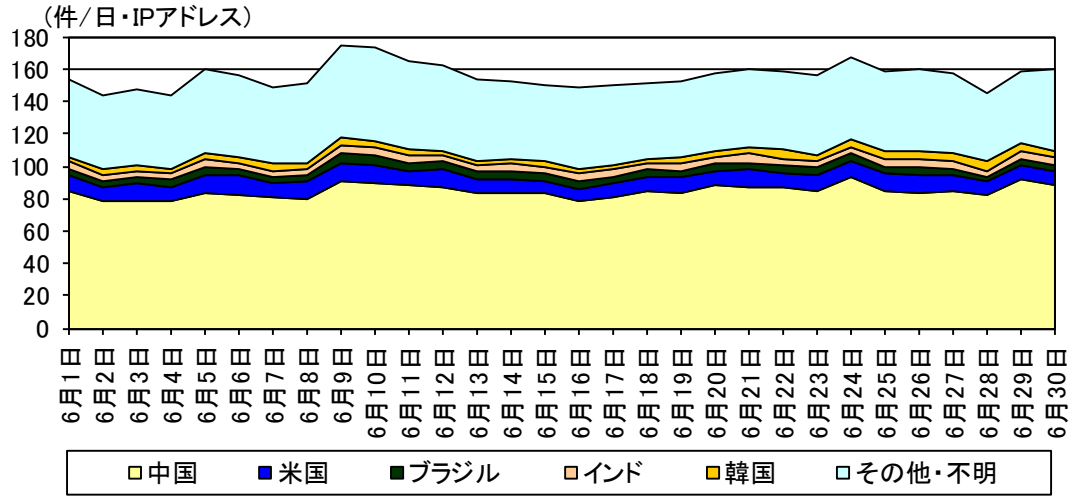

図 3-6　センサーのポート 1433/TCP における検知件数の推移

Copyright 2020 Cyber Force Center, NPA JAPAN

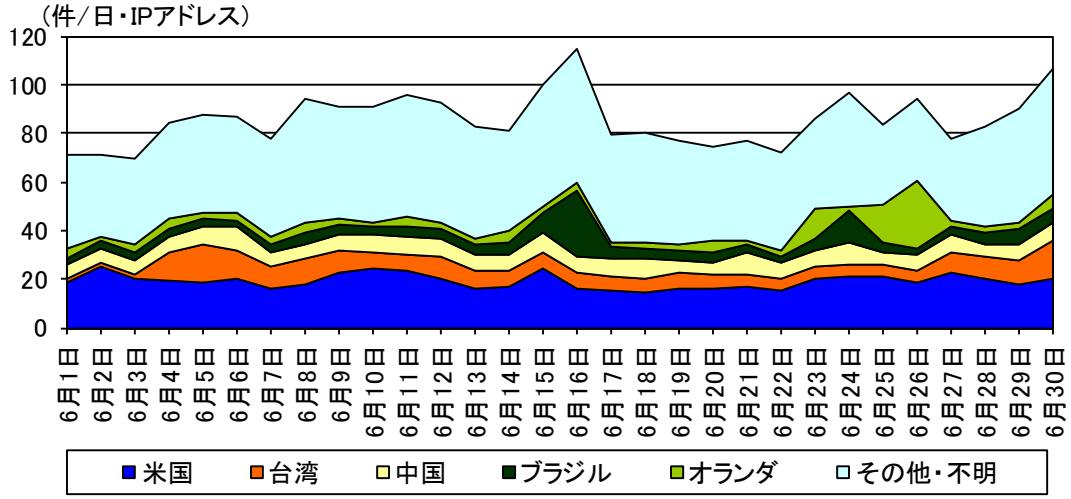

図 3-7　センサーのポート 80/TCP における検知件数の推移

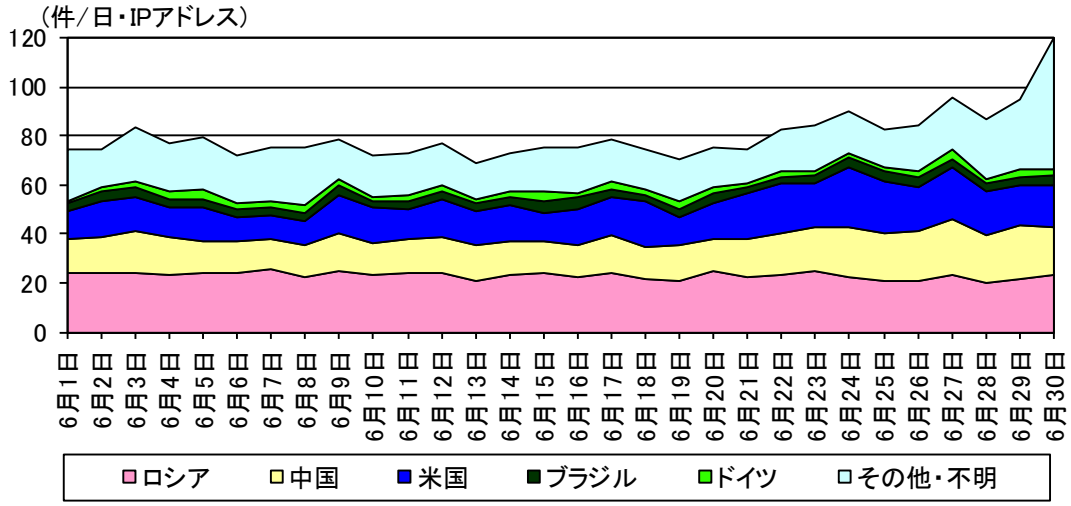

図 3-8　センサーのポート 22/TCP における検知件数の推移

Copyright 2020 Cyber Force Center, NPA JAPAN

3-2 送信元国・地域別アクセス検知件数

表 3-4　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	1 位	ロシア	2,216.27 件	＋17.1%　（＋323.83 件）
2 位	53 位	スイス	1,213.28 件	ー [ii]　（＋1,209.42 件）
3 位	4 位	オランダ	1,017.73 件	＋97.6%　（＋502.61 件）
4 位	2 位	米国	988.02 件	＋1.3%　（＋12.36 件）
5 位	3 位	中国	734.40 件	＋5.3%　（＋37.09 件）

表 3-5　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	スイス	1,213.28 件	ー [ii]　（＋1,209.42 件）	2 位	53 位
2 位	オランダ	1,017.73 件	＋97.6%　（＋502.61 件）	3 位	4 位
3 位	ロシア	2,216.27 件	＋17.1%　（＋323.83 件）	1 位	1 位
4 位	中国	734.40 件	＋5.3%　（＋37.09 件）	5 位	3 位
5 位	インドネシア	124.07 件	＋13.0%　（＋14.29 件）	8 位	9 位

表 3-6　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	ルーマニア	210.95 件	ー43.7%　（ー163.66 件）	6 位	5 位
2 位	ウクライナ	100.81 件	ー40.2%　（ー67.72 件）	11 位	7 位
3 位	台湾	157.14 件	ー16.2%　（ー30.34 件）	7 位	6 位
4 位	ラトビア	14.14 件	ー60.1%　（ー21.26 件）	35 位	23 位
5 位	イタリア	24.87 件	ー35.0%　（ー13.41 件）	26 位	22 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。

Copyright 2020 Cyber Force Center, NPA JAPAN

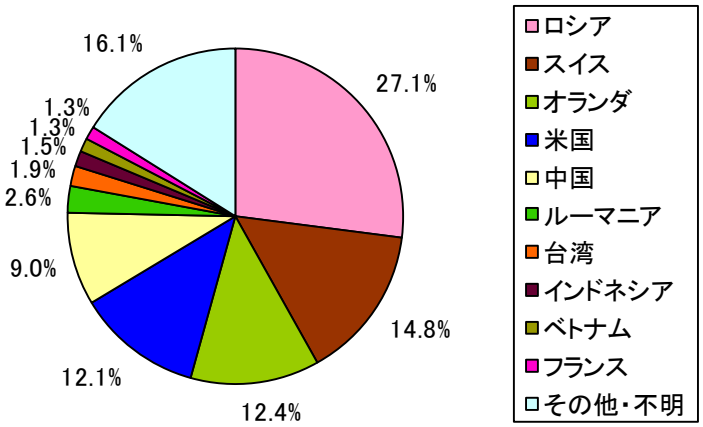

図 3-9　送信元国・地域別比率

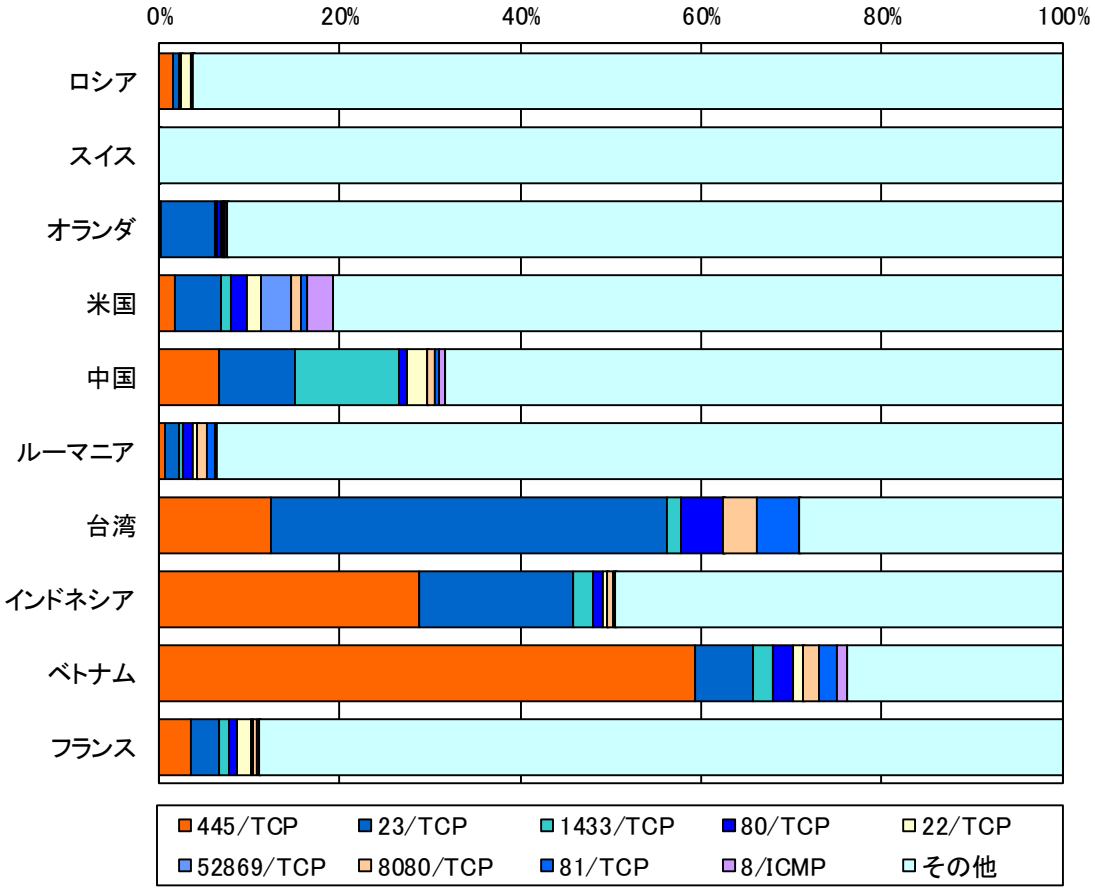

図 3-10　送信元国・地域別上位の宛先ポート別比率

Copyright 2020 Cyber Force Center, NPA JAPAN

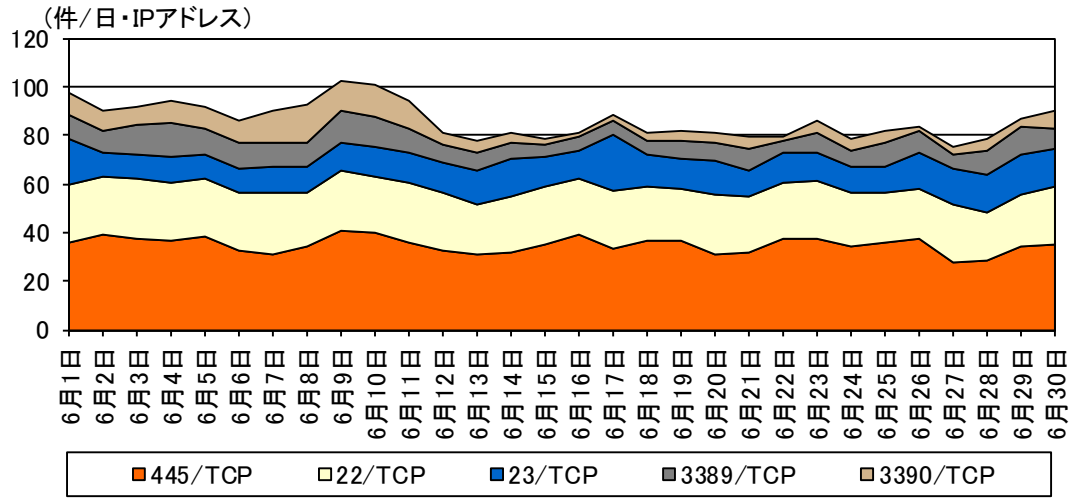

図 3-11　ロシアからの上位5ポートの検知件数の推移

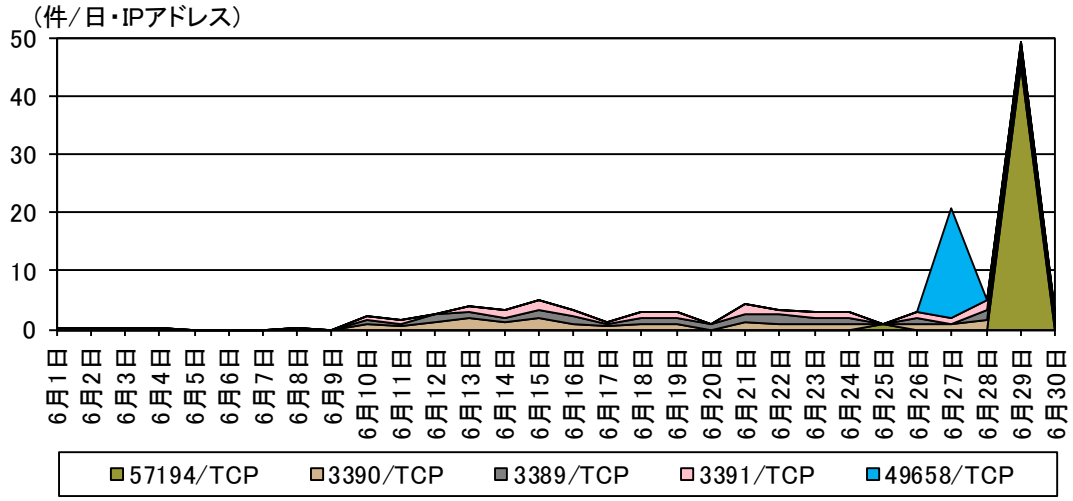

図 3-12　スイスからの上位5ポートの検知件数の推移

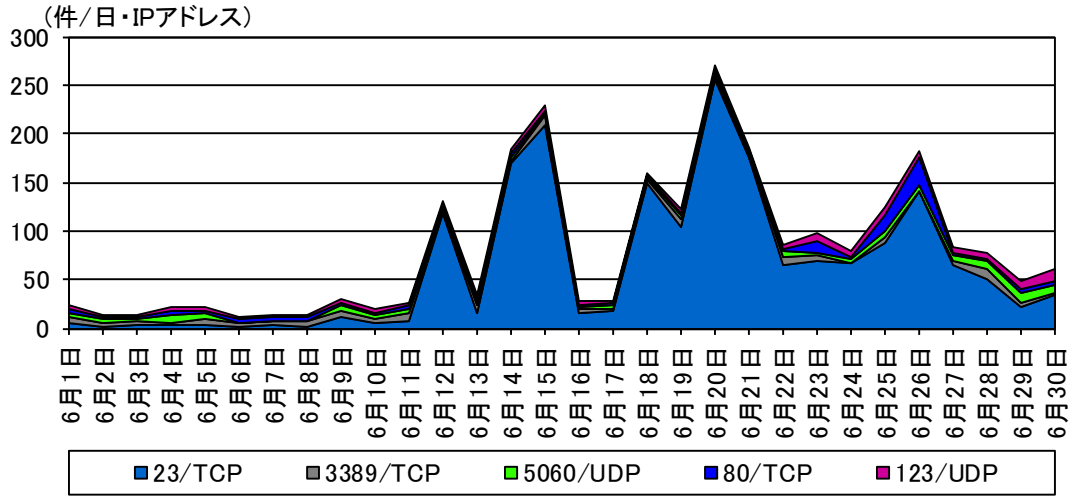

図 3-13　オランダからの上位5ポートの検知件数の推移

Copyright 2020 Cyber Force Center, NPA JAPAN

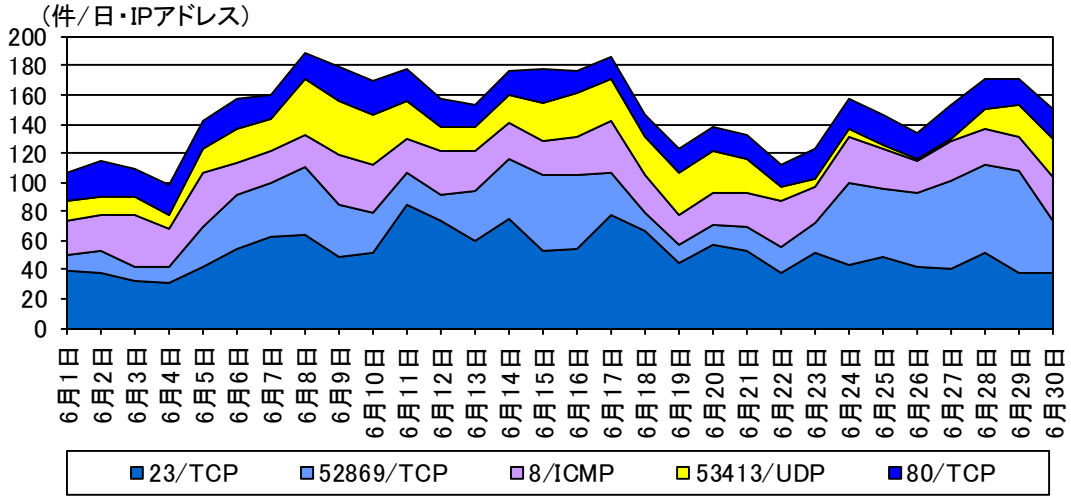

図 3-14　米国からの上位5ポートの検知件数の推移

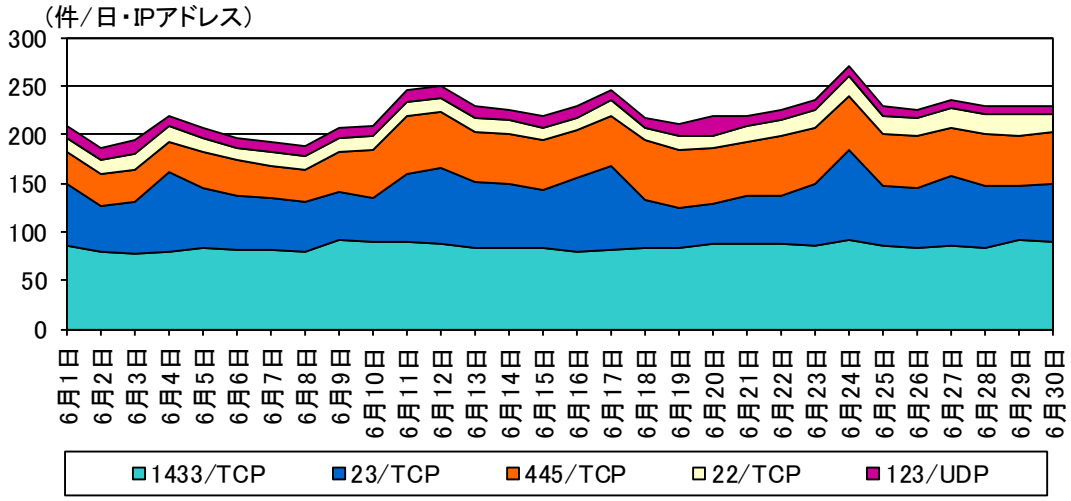

図 3-15　中国からの上位5ポートの検知件数の推移

Copyright 2020 Cyber Force Center, NPA JAPAN

4　不正侵入等の観測結果

4-1　攻撃手法別アクセス検知件数

表 4-1　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	345.05 件	＋12.8%　（＋39.02 件）	1 位	
2 位	2 位	INDICATOR-SCAN	338.95 件	＋12.6%　（＋37.86 件）	2 位	
3 位	3 位	SMBv1	143.04 件	＋4.5%　（＋6.21 件）		
4 位	7 位	Remote Desktop	46.60 件	＋164.5%　（＋28.98 件）	3 位	
5 位	5 位	OS-WINDOWS	41.69 件	＋28.7%　（＋9.30 件）	4 位	

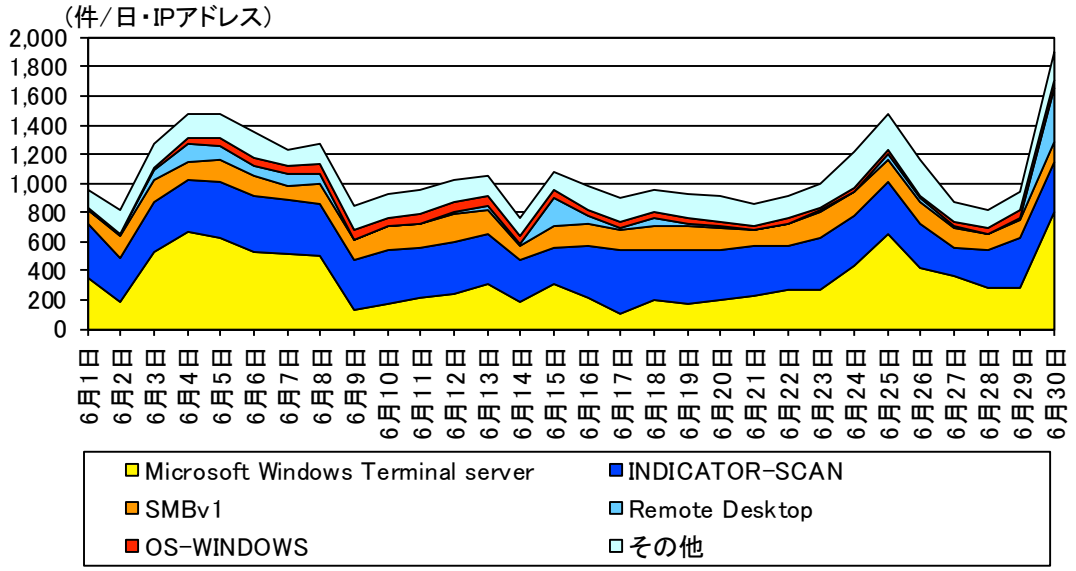

図 4-1　不正侵入等の攻撃手法別検知件数の推移

[i] 一日・1IP アドレス当たり。

Copyright 2020 Cyber Force Center, NPA JAPAN

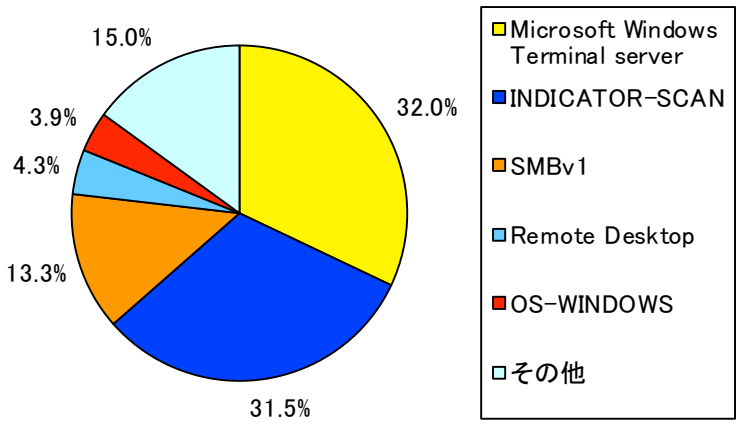

図 4-2 不正侵入等の攻撃手法別検知比率

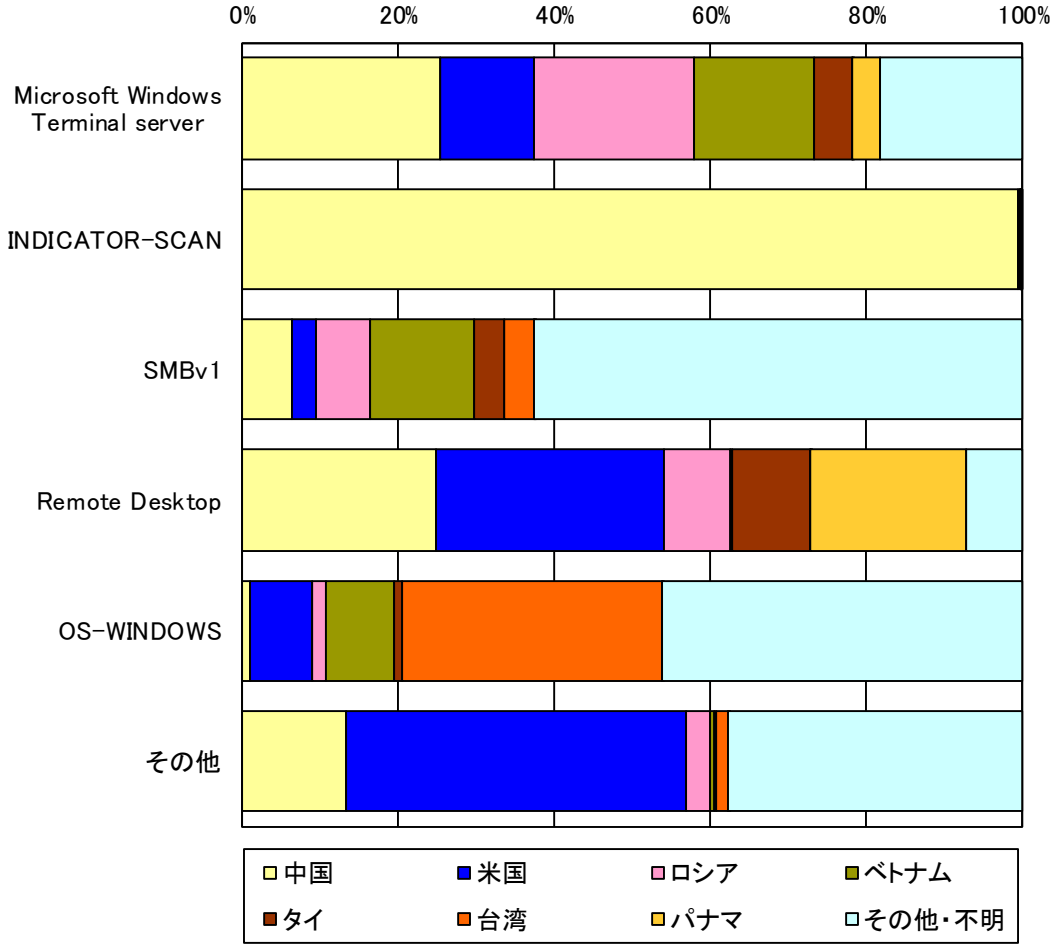

図 4-3 不正侵入等の攻撃手法の国・地域別検知比率

Copyright 2020 Cyber Force Center, NPA JAPAN

4-2 送信元国・地域別アクセス検知件数

表 4-2 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	466.41 件	＋30.2% （＋108.26 件）
2 位	2 位	米国	134.50 件	＋17.6% （＋20.12 件）
3 位	3 位	ロシア	90.32 件	＋19.2% （＋14.52 件）
4 位	4 位	ベトナム	77.11 件	＋8.5% （＋6.03 件）
5 位	16 位	タイ	27.14 件	＋311.6% （＋20.55 件）

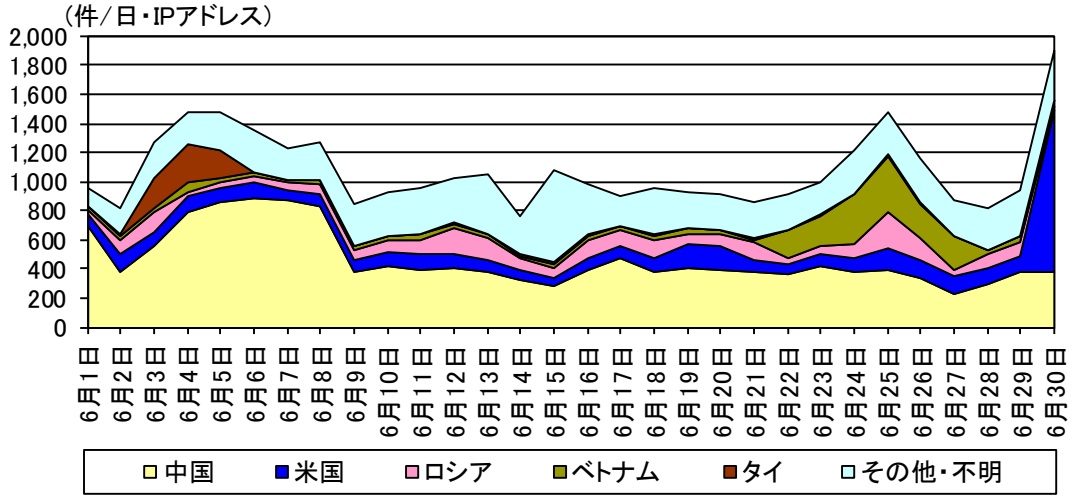

図 4-4 不正侵入等の送信元国・地域別検知件数の推移

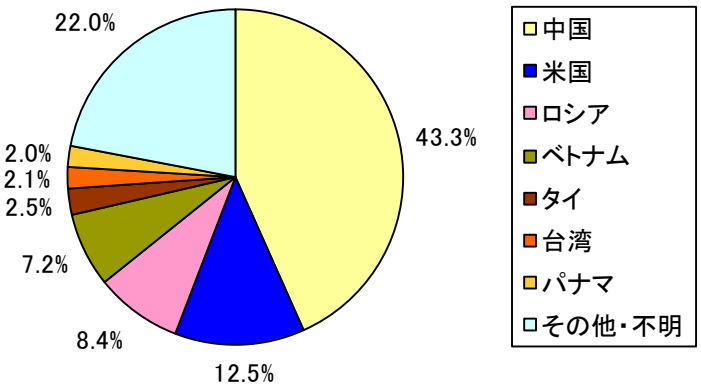

図 4-5 不正侵入等の送信元国・地域別検知比率

[i] 一日・1IP アドレス当たり。

Copyright 2020 Cyber Force Center, NPA JAPAN

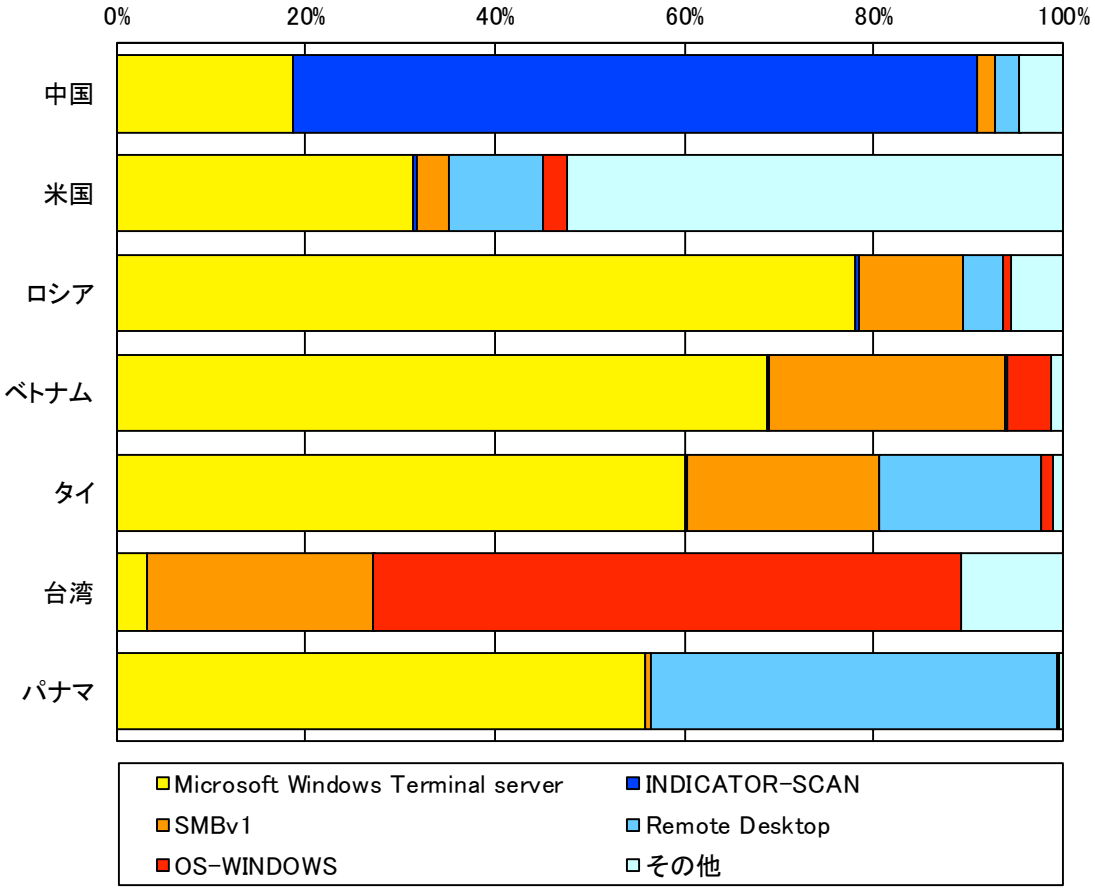

図 4-6 不正侵入等の送信元国・地域別上位の攻撃手法別検知比率

Copyright 2020 Cyber Force Center, NPA JAPAN

5　DoS 攻撃被害の観測結果

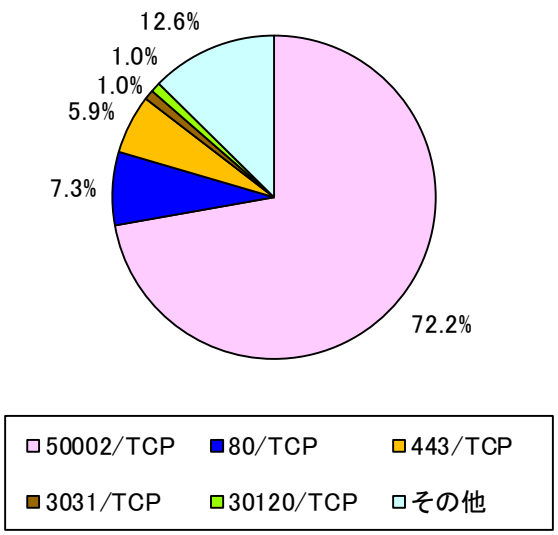

図 5-1　跳ね返りパケット送信元ポート別比率

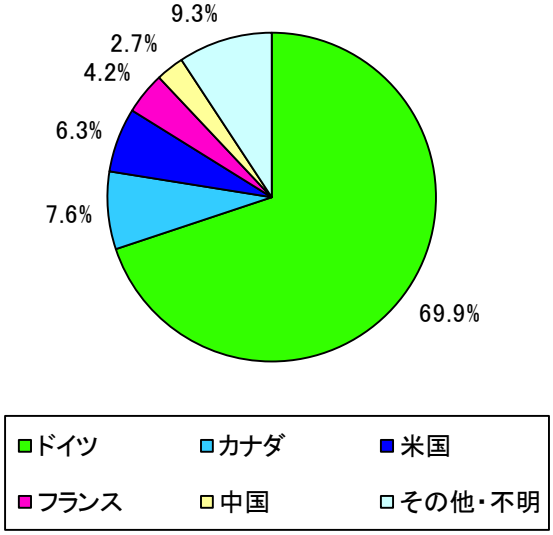

図 5-2　跳ね返りパケット送信元国・地域別比率

Copyright 2020 Cyber Force Center, NPA JAPAN