令和２年８月 11 日

令和2年7月期観測資料

1　観測結果概要

令和2年7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 6,071.3 件で、令和2年6月期（以下「前月期」という。）の 8,190.2 件と比較して 2,118.9 件（25.9%）減少しました。また、送信元 IP アドレス [i] 数は、一日当たり 52,782.0 個で、前月期の 53,205.4 個と比較して 423.4 個（0.8%）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 946.2 件で、前月期の 1,076.6 件と比較して 130.5 件（12.1%）減少しました。また、送信元 IP アドレス数は、一日当たり 13,378.6 個で、前月期の 12,770.4 個と比較して 608.2 個（4.8%）増加しました。

DoS 攻撃被害検知件数は、一日当たり 11,185.1 件で、前月期の 12,769.9 件と比較して 1,584.8 件（12.4%）減少しました。また、送信元 IP アドレス数は、一日当たり 478.3 個で、前月期の 392.4 個と比較して 85.9 個（21.9%）増加しました。

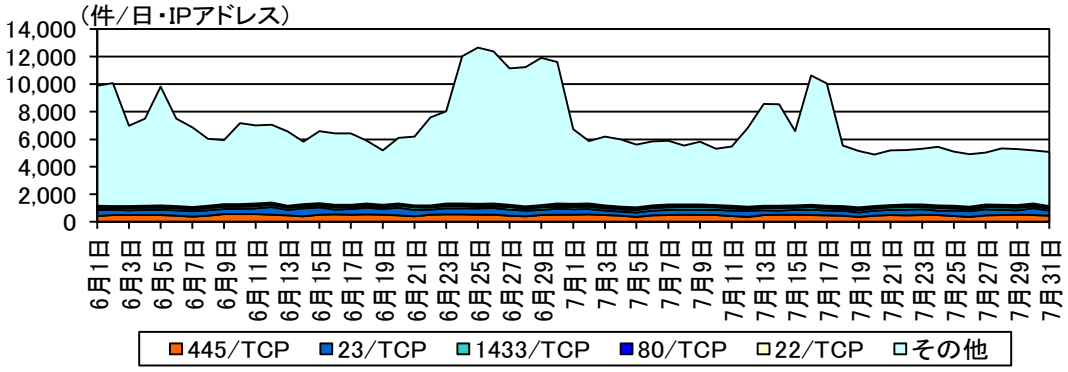

図 1-1　宛先ポート別検知件数の推移

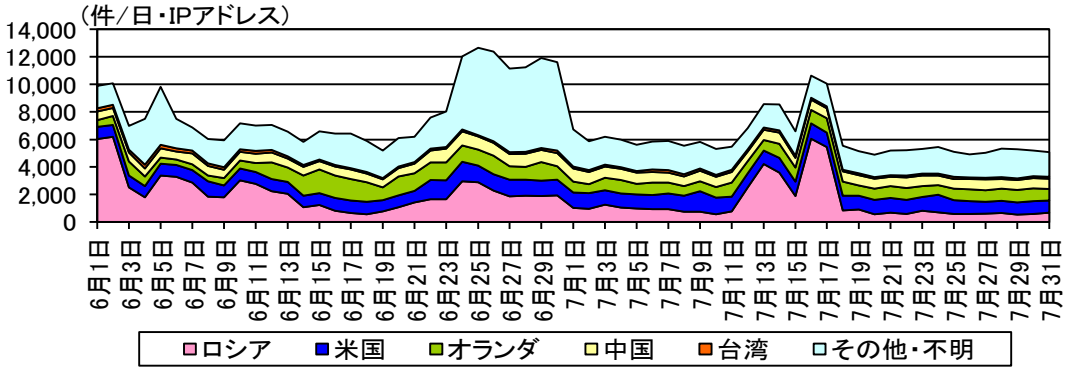

図 1-2　送信元国・地域別検知件数の推移 [ii]

[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。

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

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

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	1 位	445/TCP	466.63 件	－4.4%　（－21.67 件）
2 位	2 位	23/TCP	379.27 件	－13.1%　（－56.93 件）
3 位	3 位	1433/TCP	162.81 件	＋4.2%　（＋6.61 件）
4 位	4 位	80/TCP	97.58 件	＋13.8%　（＋11.80 件）
5 位	5 位	22/TCP	92.70 件	＋16.0%　（＋12.76 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	8/ICMP	70.91 件	＋57.3%　（＋25.84 件）	6 位	9 位
2 位	5555/TCP	48.87 件	＋96.2%　（＋23.96 件）	8 位	17 位
3 位	85/TCP	20.88 件	－[ii]　（＋19.33 件）	19 位	－[ii]
4 位	22/TCP	92.70 件	＋16.0%　（＋12.76 件）	5 位	5 位
5 位	80/TCP	97.58 件	＋13.8%　（＋11.80 件）	4 位	4 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	23/TCP	379.27 件	－13.1%　（－56.93 件）	2 位	2 位
2 位	52869/TCP	36.59 件	－46.8%　（－32.24 件）	13 位	6 位
3 位	445/TCP	466.63 件	－4.4%　（－21.67 件）	1 位	1 位
4 位	8080/TCP	47.64 件	－26.3%　（－16.99 件）	9 位	7 位
5 位	8000/TCP	8.29 件	－65.3%　（－15.64 件）	44 位	20 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。

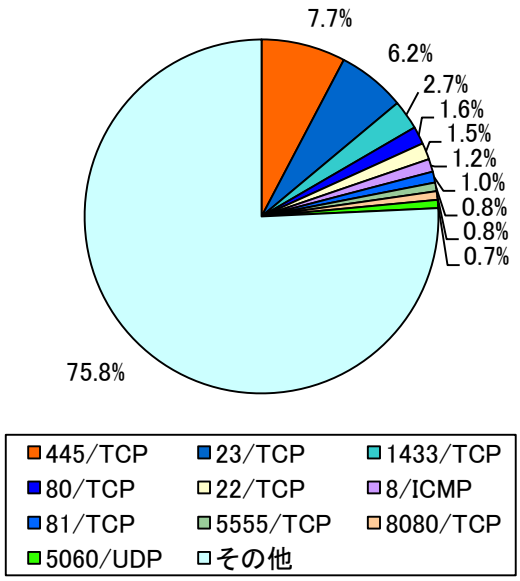

図 3-1　宛先ポート別比率（全て）[i]

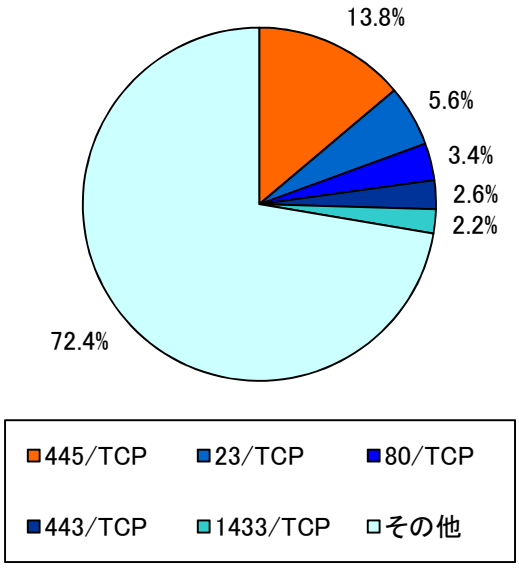

図 3-2　宛先ポート別比率（日本国内）

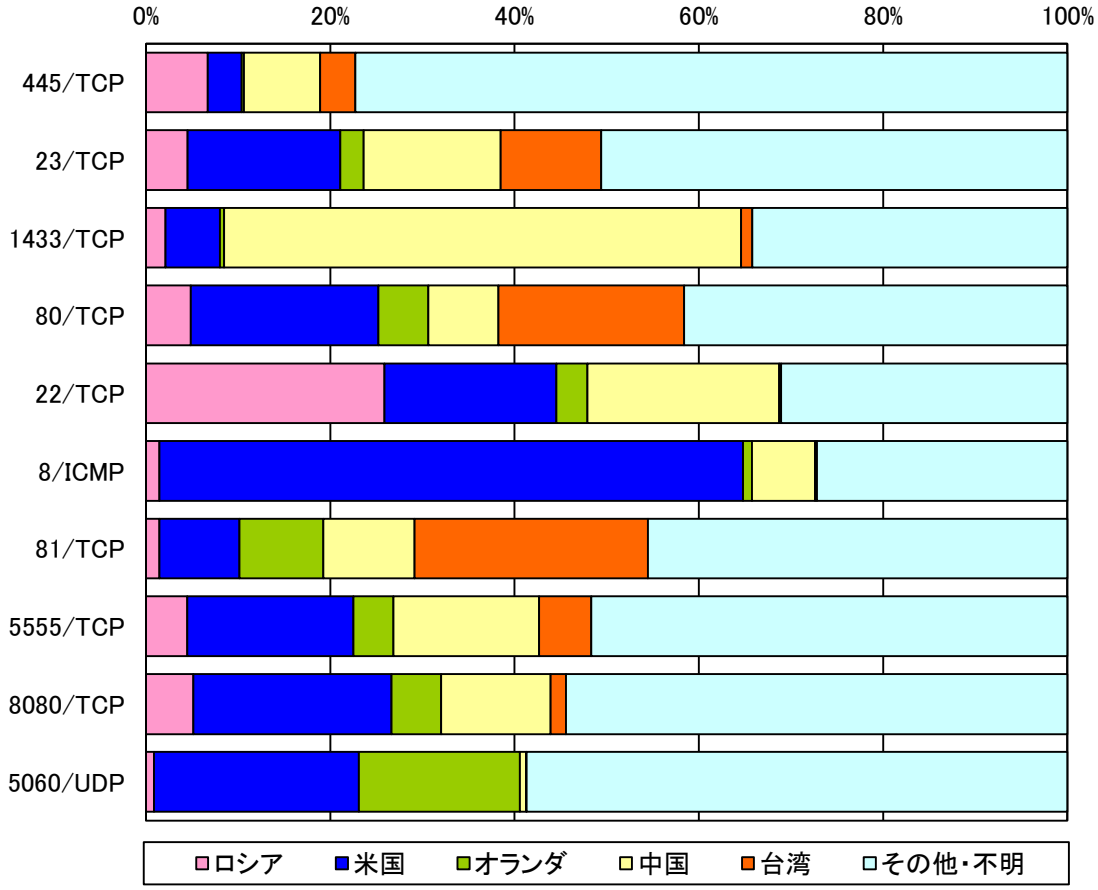

図 3-3　宛先ポート別上位の送信元国・地域別比率

[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。

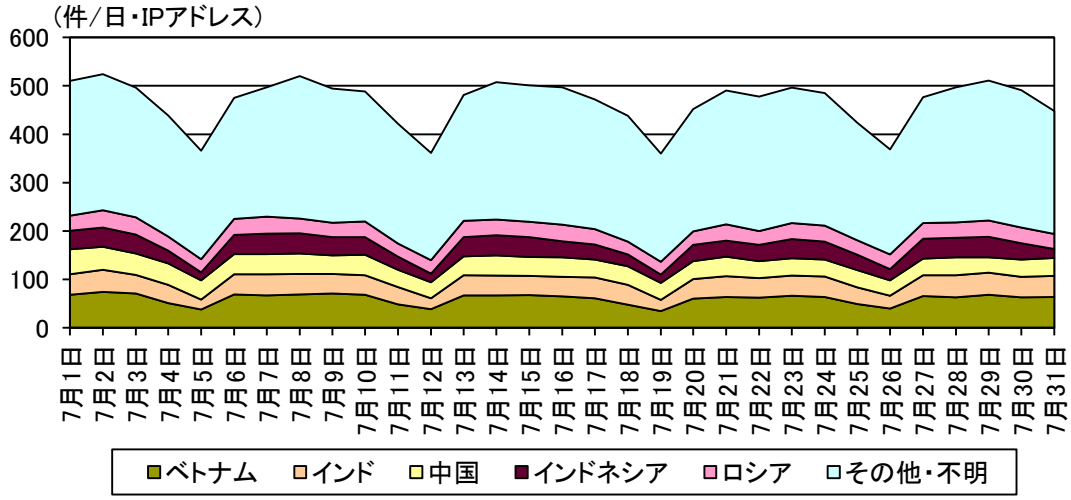

図 3-4　センサーのポート 445/TCP における検知件数の推移

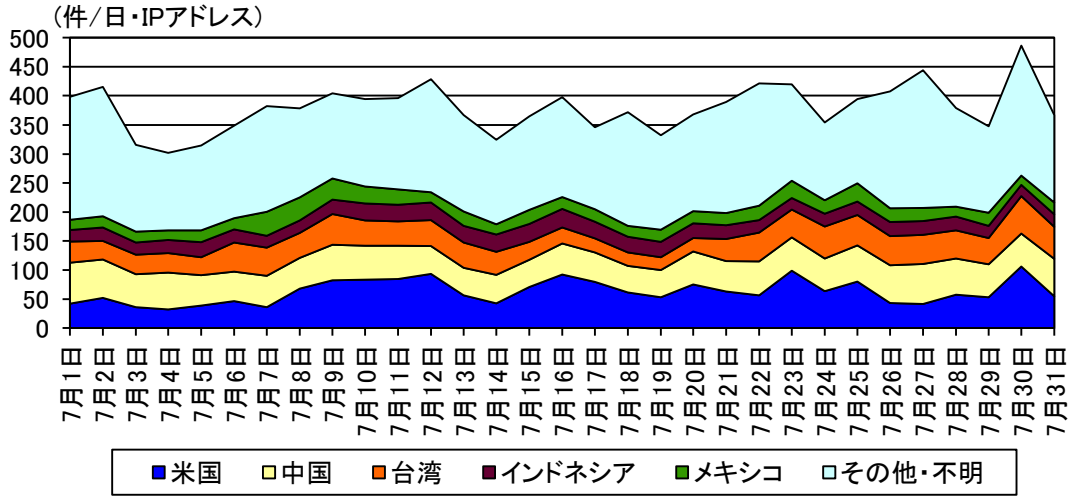

図 3-5　センサーのポート 23/TCP における検知件数の推移

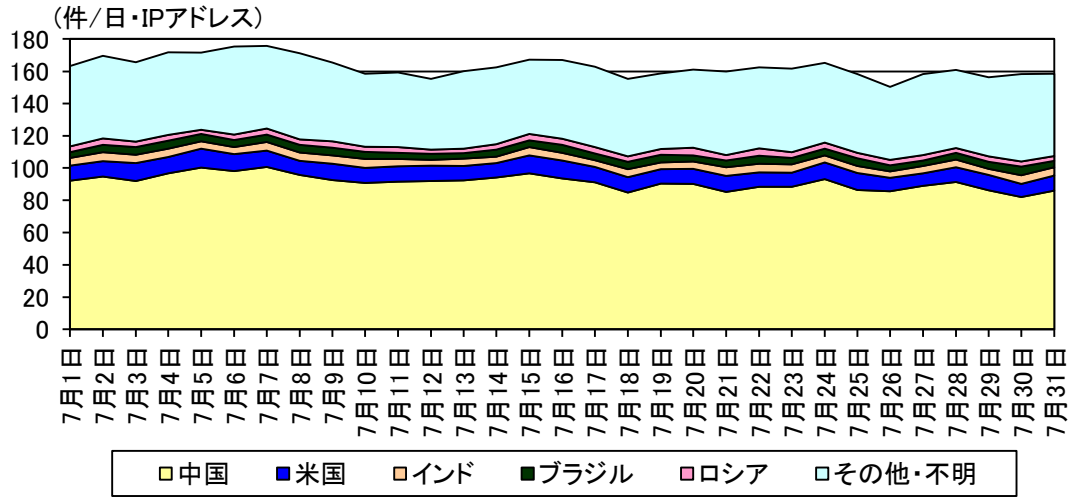

図 3-6　センサーのポート 1433/TCP における検知件数の推移

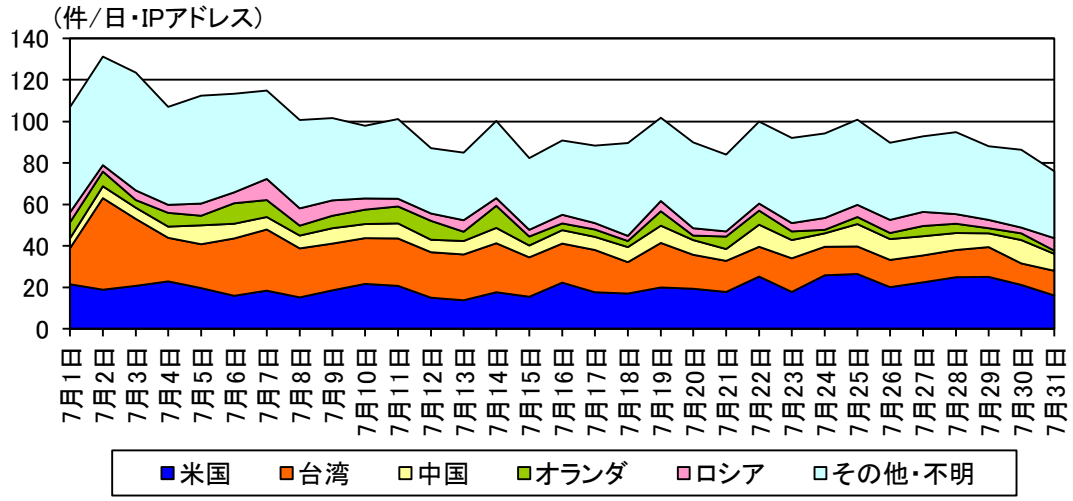

図 3-7　センサーのポート 80/TCP における検知件数の推移

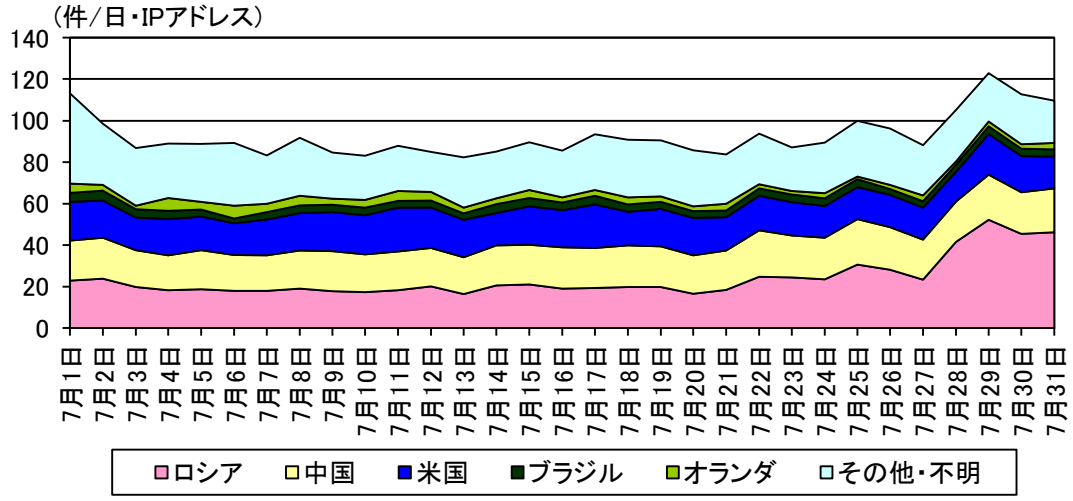

図 3-8　センサーのポート 22/TCP における検知件数の推移

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	1,391.10 件	－37.2%　（－825.17 件）
2 位	4 位	米国	1,048.03 件	＋6.1%　（＋60.01 件）
3 位	3 位	オランダ	862.51 件	－15.3%　（－155.22 件）
4 位	5 位	中国	754.76 件	＋2.8%　（＋20.36 件）
5 位	7 位	台湾	142.01 件	－9.6%　（－15.13 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	米国	1,048.03 件	＋6.1%　（＋60.01 件）	2 位	4 位
2 位	ドイツ	140.84 件	＋50.2%　（＋47.07 件）	6 位	13 位
3 位	中国	754.76 件	＋2.8%　（＋20.36 件）	4 位	5 位
4 位	インドネシア	137.36 件	＋10.7%　（＋13.29 件）	8 位	8 位
5 位	ベトナム	117.44 件	＋11.2%　（＋11.87 件）	9 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	スイス	140.45 件	－88.4%　（－1,072.83 件）	7 位	2 位
2 位	ロシア	1,391.10 件	－37.2%　（－825.17 件）	1 位	1 位
3 位	オランダ	862.51 件	－15.3%　（－155.22 件）	3 位	3 位
4 位	ルーマニア	97.86 件	－53.6%　（－113.09 件）	11 位	6 位
5 位	日本	38.38 件	－59.6%　（－56.71 件）	21 位	12 位

[i] 一日・1IP アドレス当たり。

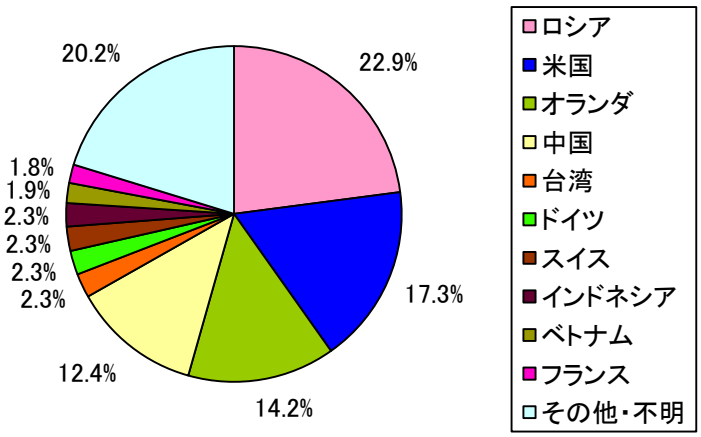

図 3-9　送信元国・地域別比率

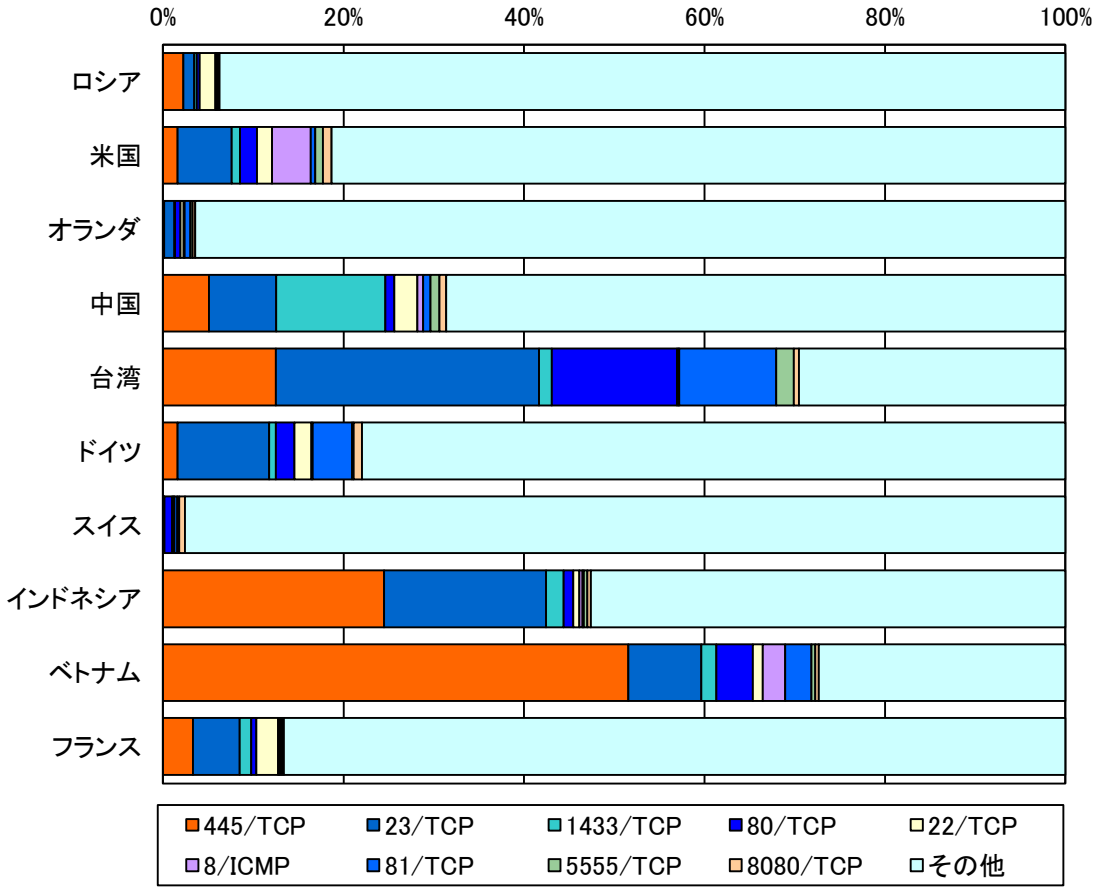

図 3-10　送信元国・地域別上位の宛先ポート別比率

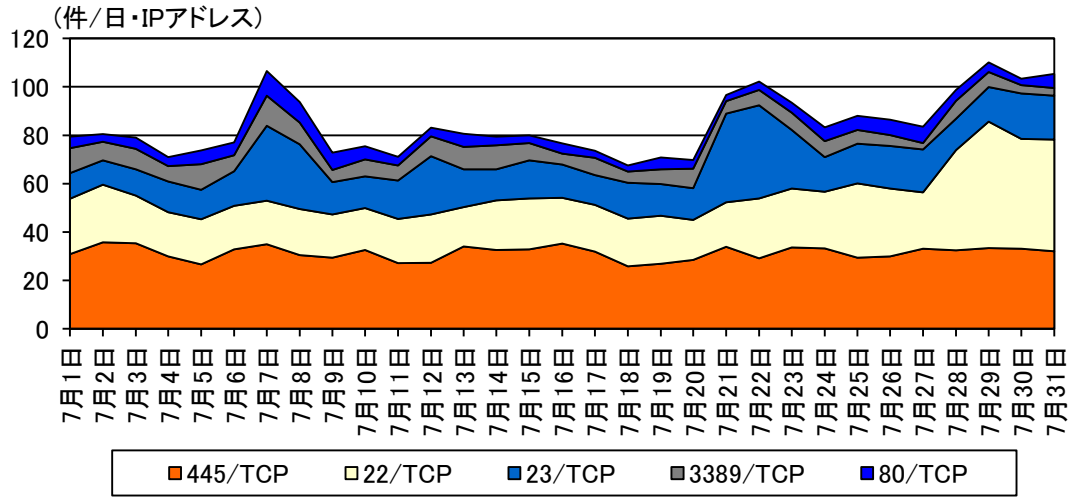

図 3-11　ロシアからの上位5ポートの検知件数の推移

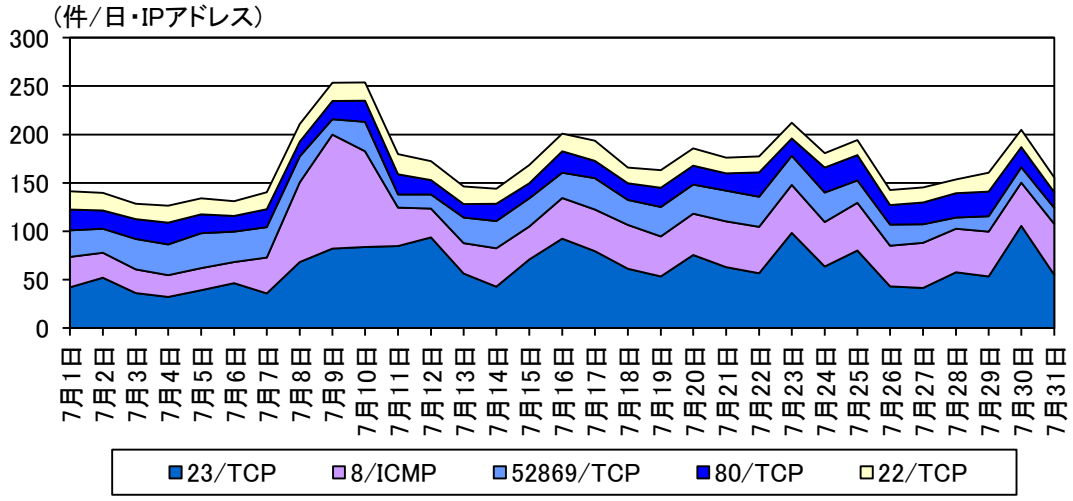

図 3-12　米国からの上位5ポートの検知件数の推移

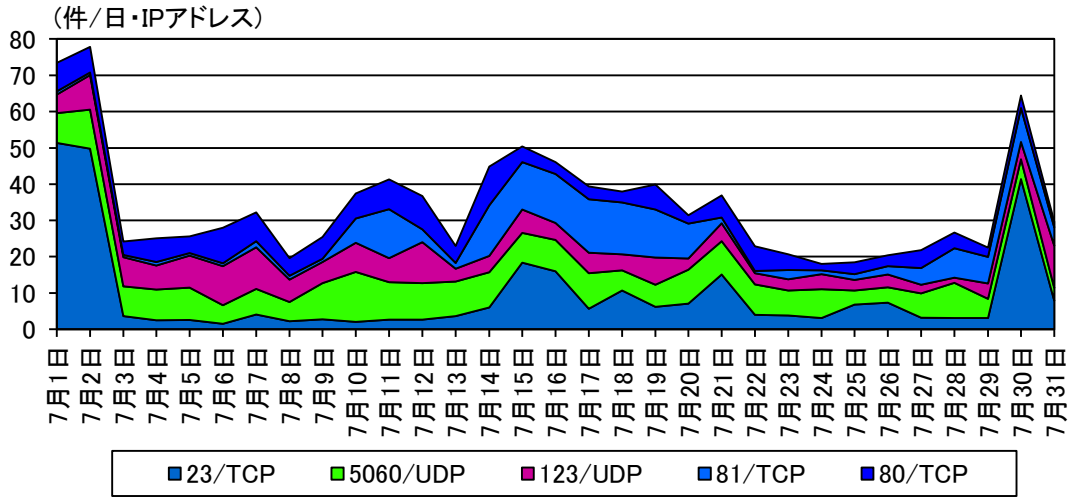

図 3-13　オランダからの上位5ポートの検知件数の推移

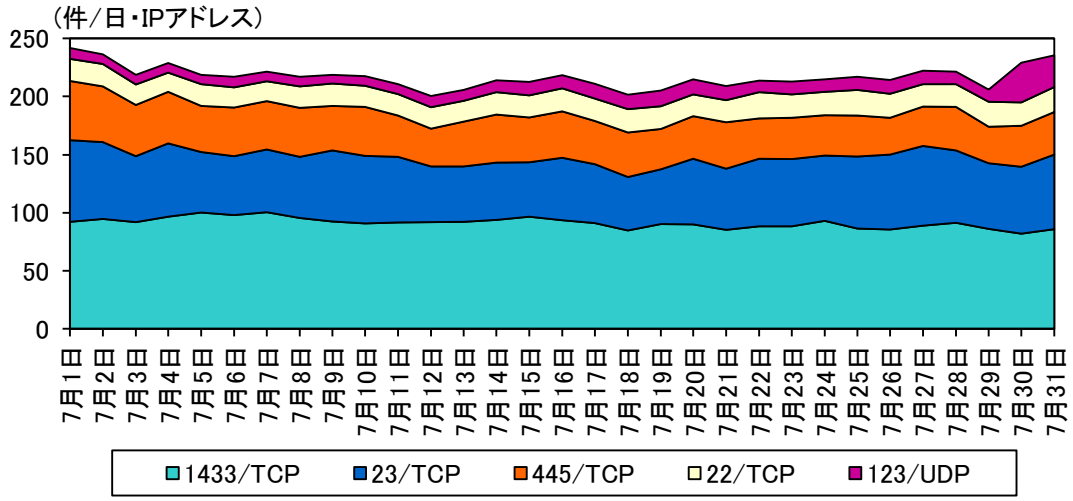

図 3-14　中国からの上位5ポートの検知件数の推移

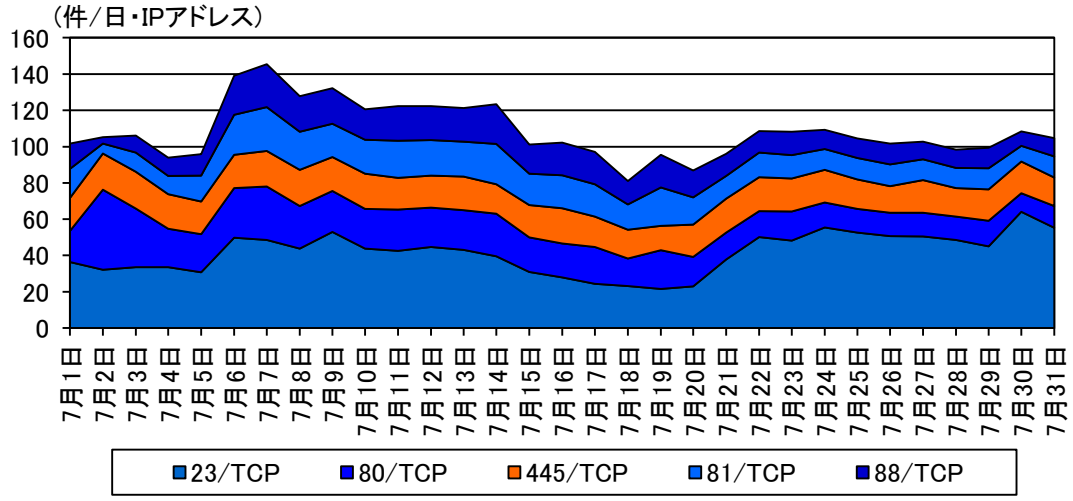

図 3-15　台湾からの上位5ポートの検知件数の推移

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	2 位	INDICATOR-SCAN	305.61 件	−9.8%　（−33.34 件）		2 位
2 位	1 位	Microsoft Windows Terminal server	240.49 件	−30.3%　（−104.56 件）		1 位
3 位	3 位	SMBv1	150.60 件	＋5.3%　（＋7.56 件）	3 位	
4 位	5 位	OS-WINDOWS	52.54 件	＋26.0%　（＋10.84 件）	1 位	
5 位	6 位	SERVER-APACHE	45.71 件	＋22.7%　（＋8.44 件）	2 位	

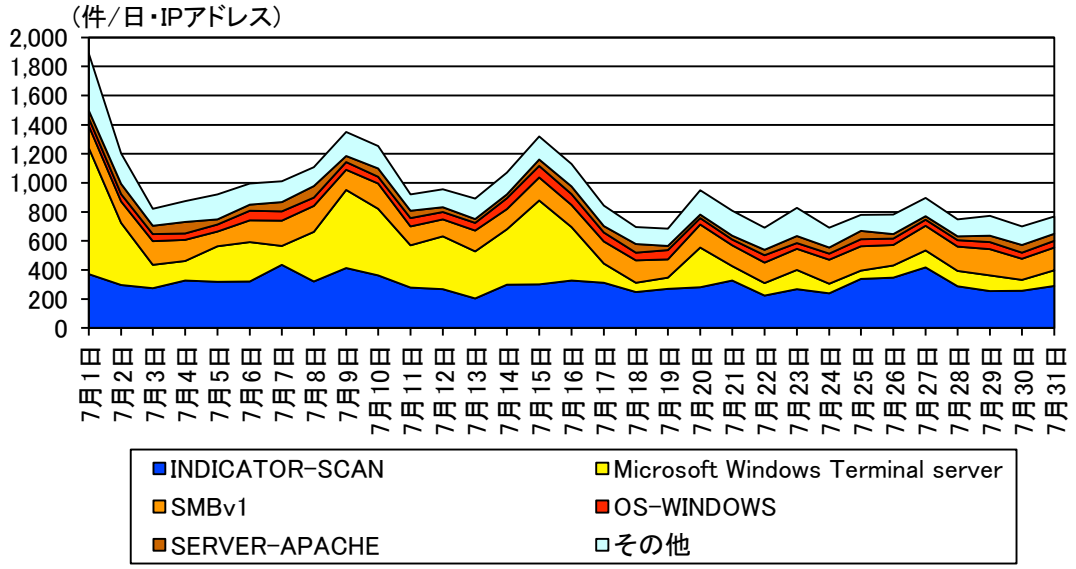

図 4-1　不正侵入等の攻撃手法別検知件数の推移

[i] 一日・1IP アドレス当たり。

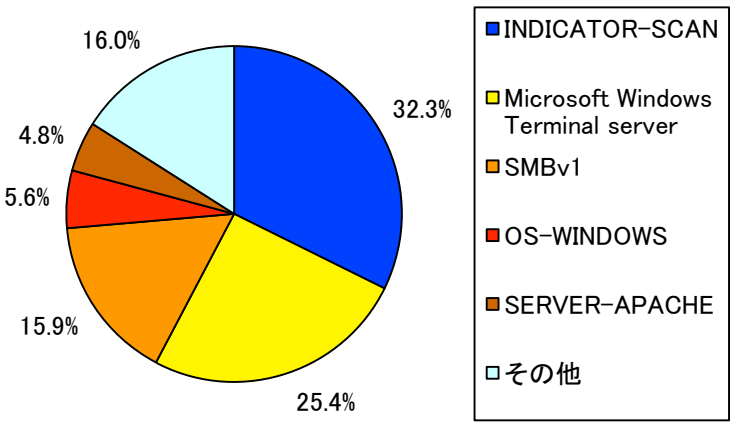

図 4-2 不正侵入等の攻撃手法別検知比率

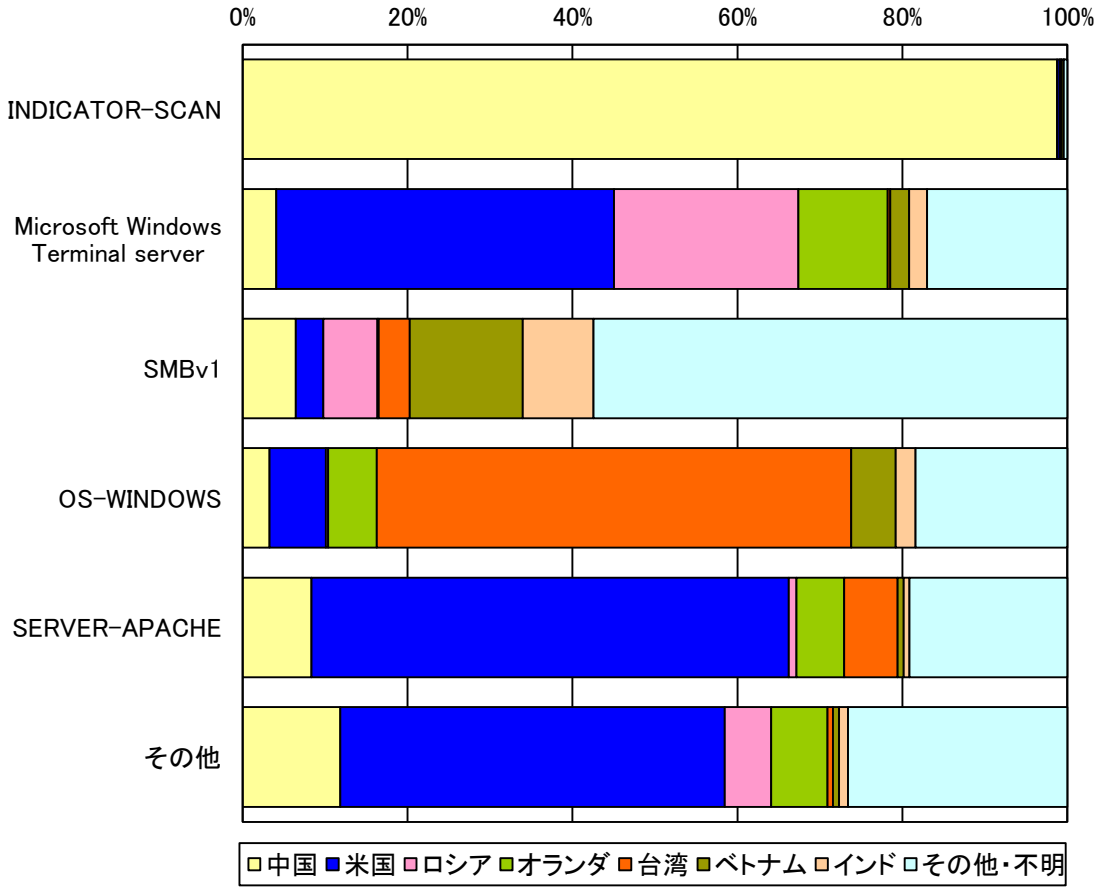

図 4-3 不正侵入等の攻撃手法の国・地域別検知比率

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	344.70 件	－26.1% （－121.72 件）
2 位	2 位	米国	205.07 件	＋52.5% （＋70.57 件）
3 位	3 位	ロシア	73.23 件	－18.9% （－17.09 件）
4 位	9 位	オランダ	42.55 件	＋127.0% （＋23.81 件）
5 位	6 位	台湾	40.57 件	＋81.8% （＋18.26 件）

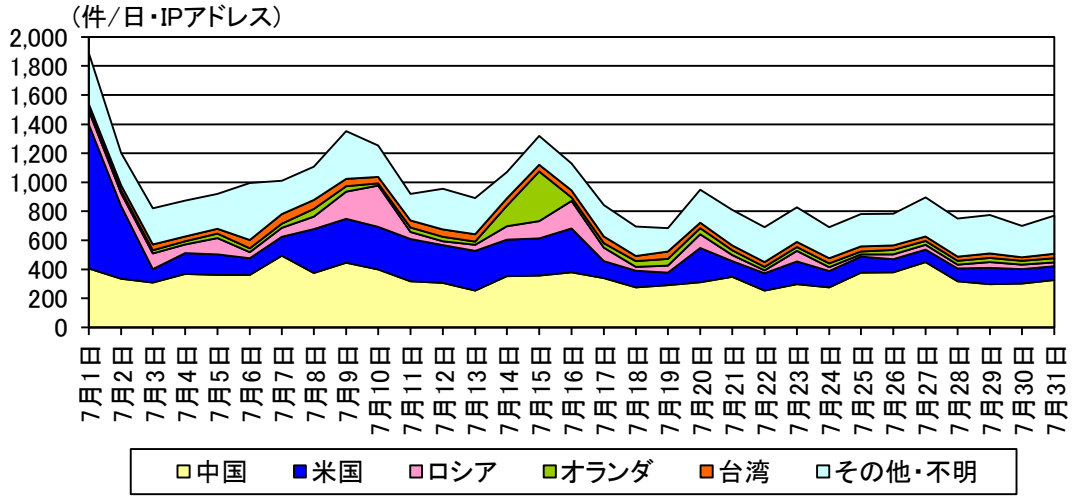

図 4-4 不正侵入等の送信元国・地域別検知件数の推移

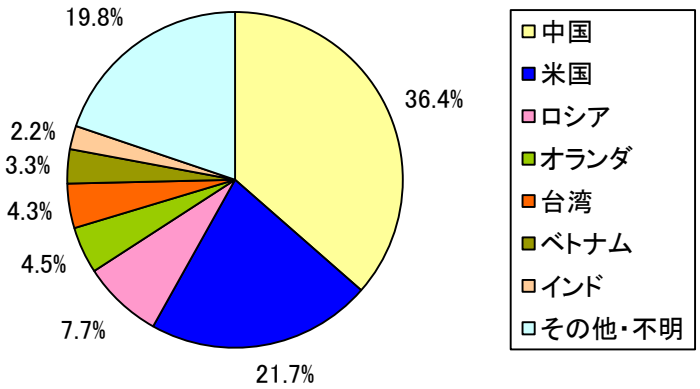

図 4-5 不正侵入等の送信元国・地域別検知比率

[i] 一日・1IP アドレス当たり。

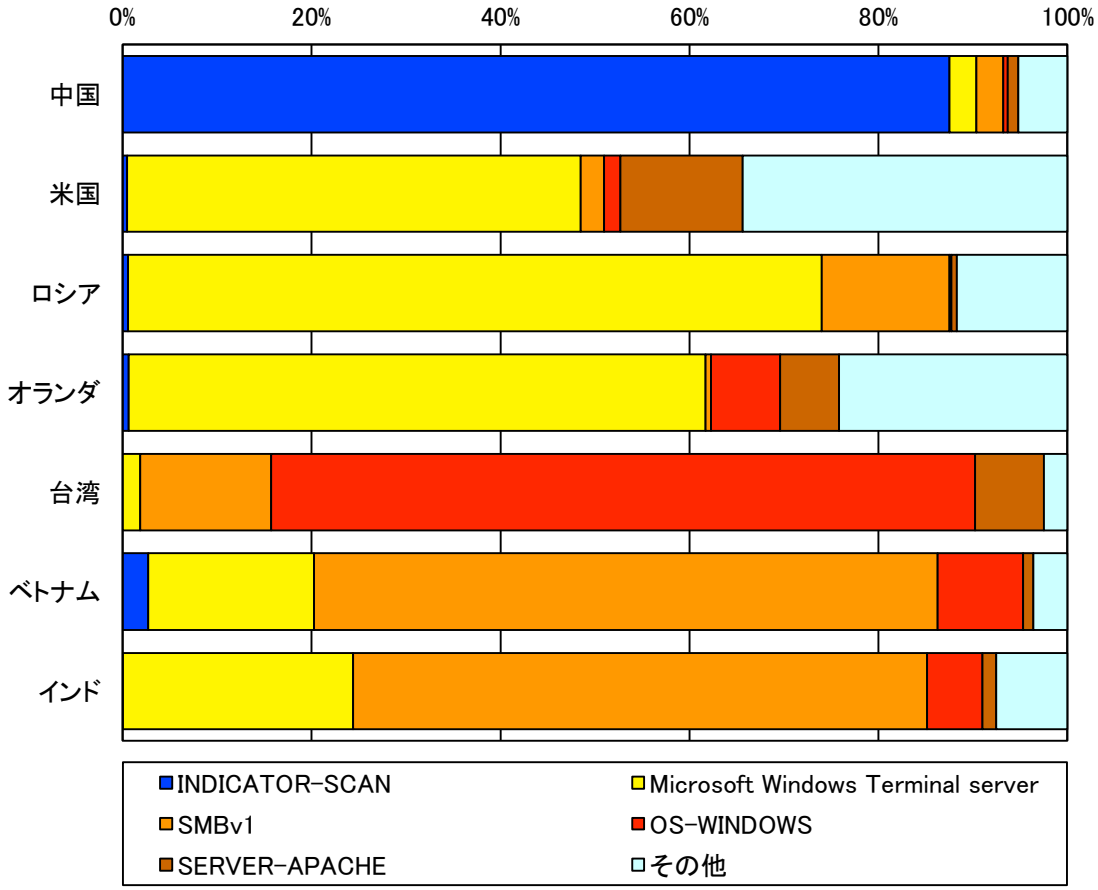

図 4-6 不正侵入等の送信元国・地域別上位の攻撃手法別検知比率

5　DoS 攻撃被害の観測結果

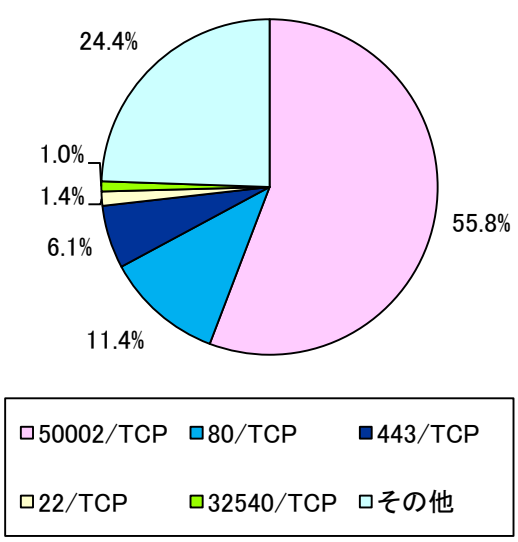

図 5-1　跳ね返りパケット送信元ポート別比率

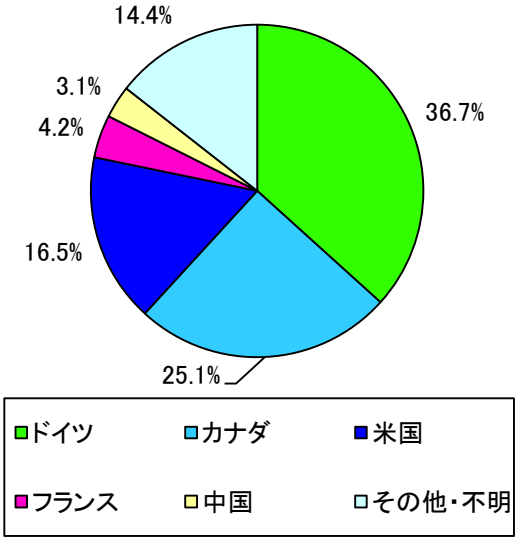

図 5-2　跳ね返りパケット送信元国・地域別比率