令和２年 10 月２日

令和2年8月期観測資料

1　観測結果概要

令和2年8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 5,476.5 件で、令和2年7月期（以下「前月期」という。）の 6,071.3 件と比較して 594.7 件（9.8%）減少しました。また、送信元 IP アドレス[i] 数は、一日当たり 46,146.9 個で、前月期の 52,782.0 個と比較して 6,635.1 個（12.6%）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 791.1 件で、前月期の 946.2 件と比較して 155.0 件（16.4%）減少しました。また、送信元 IP アドレス数は、一日当たり 9,467.3 個で、前月期の 13,378.6 個と比較して 3,911.3 個（29.2%）減少しました。

DoS 攻撃被害検知件数は、一日当たり 12,171.8 件で、前月期の 11,185.1 件と比較して 986.7 件（8.8%）増加しました。また、送信元 IP アドレス数は、一日当たり 520.4 個で、前月期の 478.3 個と比較して 42.1 個（8.8%）増加しました。

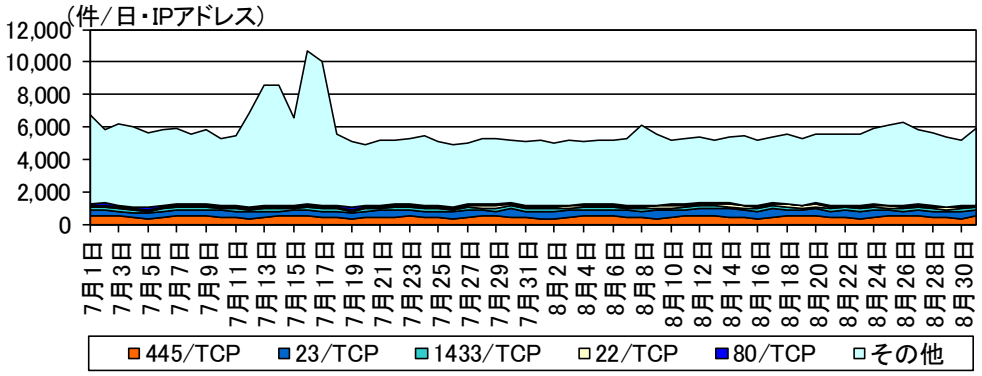

図 1-1　宛先ポート別検知件数の推移

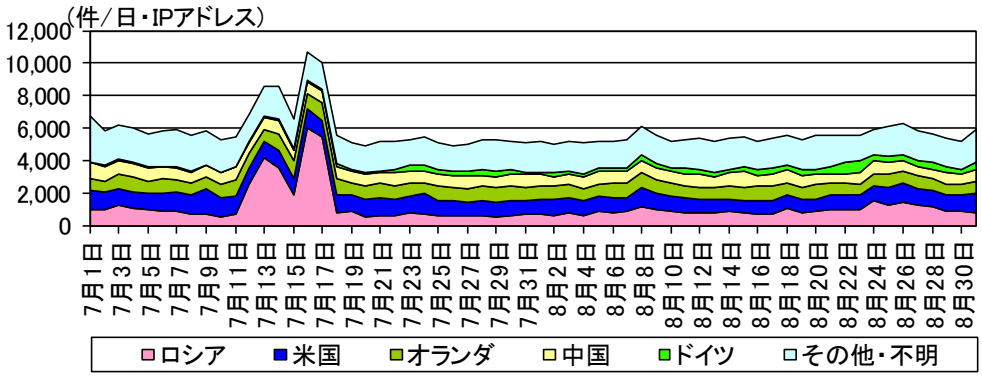

図 1-2　送信元国・地域別検知件数の推移 [ii]

[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	464.80 件	－0.4%　（－1.83 件）
2 位	2 位	23/TCP	423.43 件	＋11.6%　（＋44.16 件）
3 位	3 位	1433/TCP	156.41 件	－3.9%　（－6.41 件）
4 位	5 位	22/TCP	115.03 件	＋24.1%　（＋22.32 件）
5 位	4 位	80/TCP	68.52 件	－29.8%　（－29.06 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	23/TCP	423.43 件	＋11.6%　（＋44.16 件）	2 位	2 位
2 位	9530/TCP	43.00 件	＋759.1%　（＋37.99 件）	9 位	65 位
3 位	22/TCP	115.03 件	＋24.1%　（＋22.32 件）	4 位	5 位
4 位	5038/TCP	15.23 件	＋350.7%　（＋11.85 件）	23 位	－[ii]
5 位	0/TCP	9.20 件	－[ii]　（＋8.72 件）	39 位	－[i]

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	80/TCP	68.52 件	－29.8%　（－29.06 件）	5 位	4 位
2 位	81/TCP	35.46 件	－41.3%　（－24.98 件）	12 位	7 位
3 位	52869/TCP	14.79 件	－59.6%　（－21.80 件）	24 位	13 位
4 位	88/TCP	8.39 件	－70.1%　（－19.65 件）	44 位	17 位
5 位	85/TCP	4.02 件	－80.7%　（－16.86 件）	84 位	19 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。

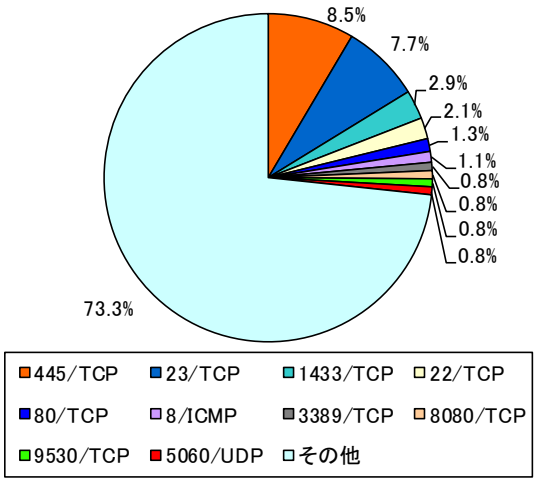

図 3-1　宛先ポート別比率（全て）[i]

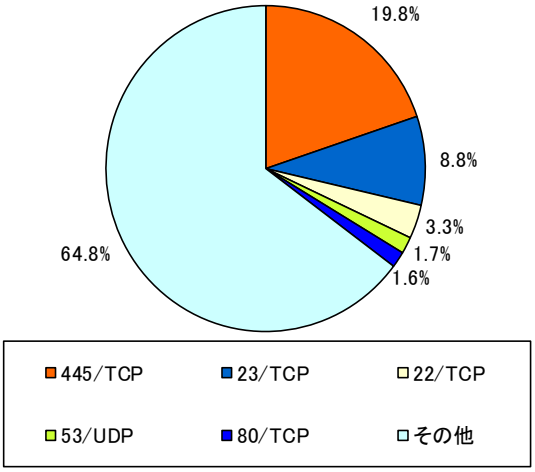

図 3-2　宛先ポート別比率（日本国内）

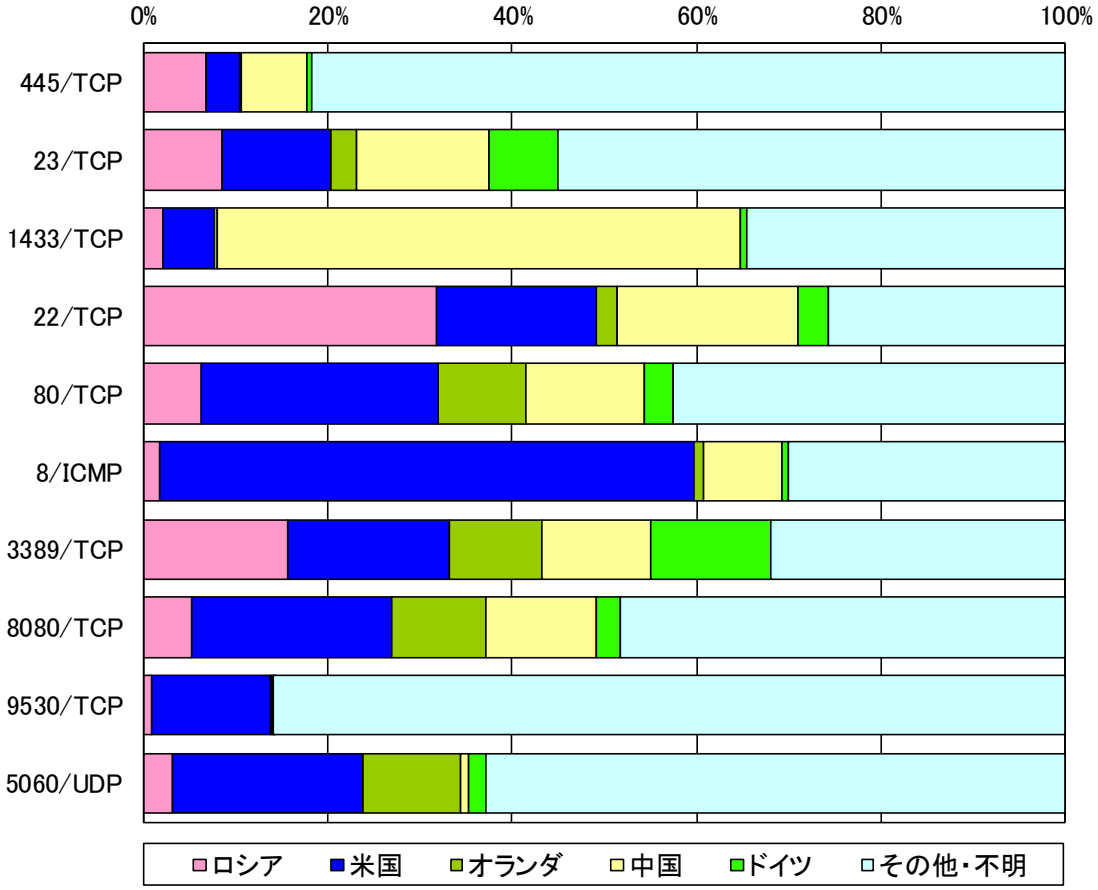

図 3-3　宛先ポート別上位の送信元国・地域別比率

[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。

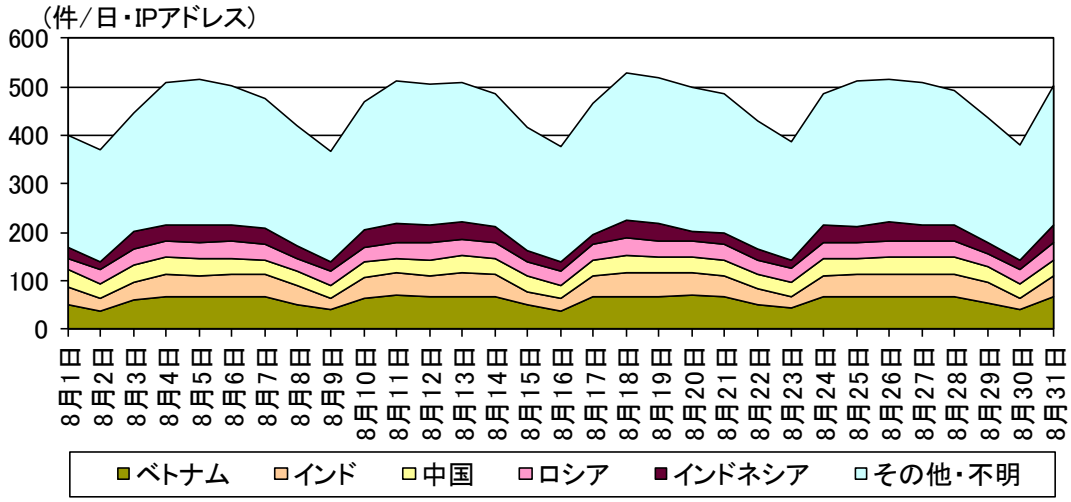

図 3-4　センサーのポート 445/TCP における検知件数の推移

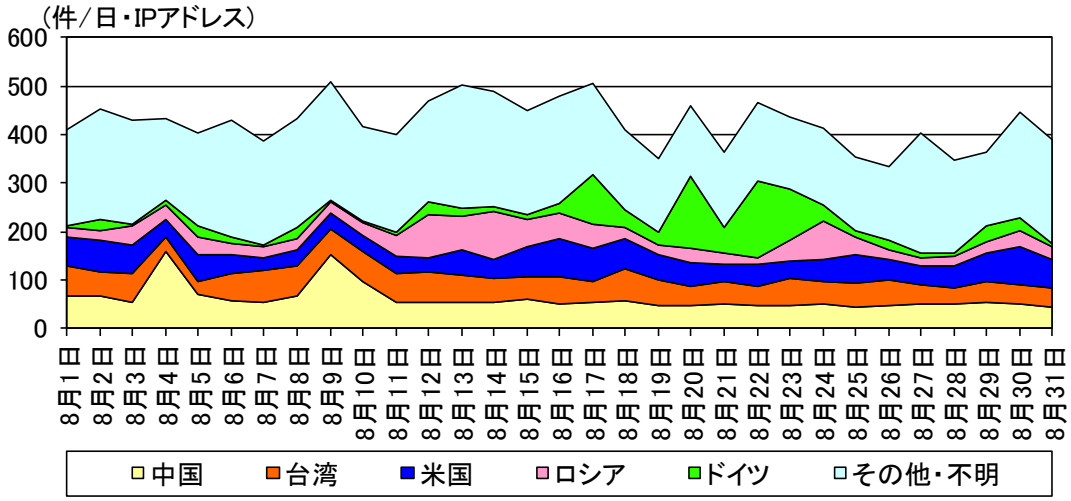

図 3-5　センサーのポート 23/TCP における検知件数の推移

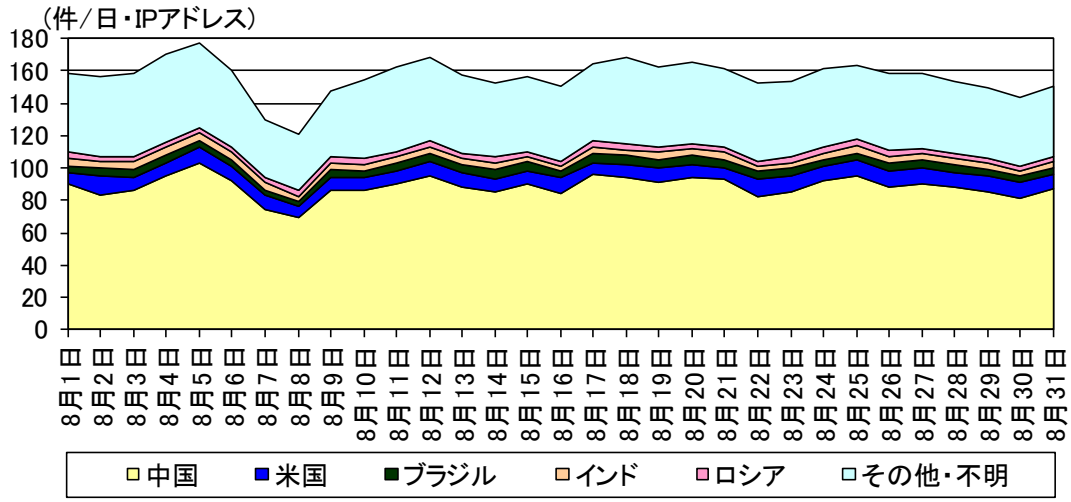

図 3-6　センサーのポート 1433/TCP における検知件数の推移

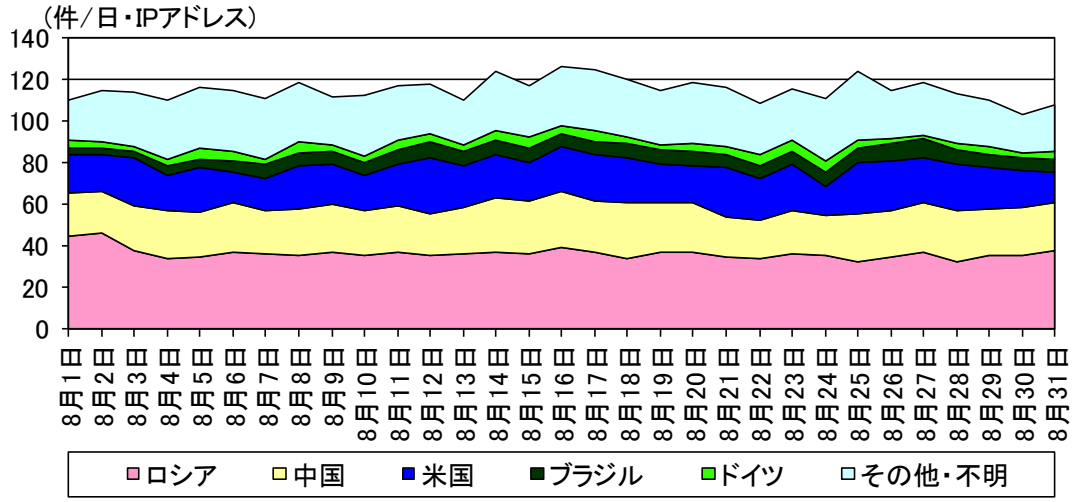

図 3-7　センサーのポート 22/TCP における検知件数の推移

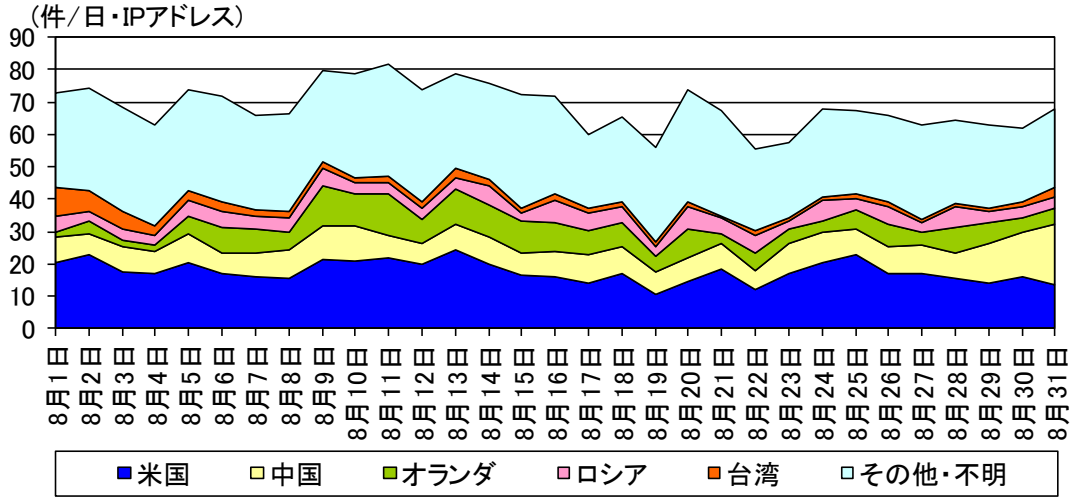

図 3-8　センサーのポート 80/TCP における検知件数の推移

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	953.43 件	－31.5%　（－437.67 件）
2 位	2 位	米国	914.50 件	－12.7%　（－133.53 件）
3 位	3 位	オランダ	780.49 件	－9.5%　（－82.02 件）
4 位	4 位	中国	710.12 件	－5.9%　（－44.64 件）
5 位	6 位	ドイツ	322.20 件	＋128.8%　（＋181.36 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	ドイツ	322.20 件	＋128.8%　（＋181.36 件）	5 位	6 位
2 位	パナマ	97.94 件	＋425.5%　（＋79.30 件）	11 位	32 位
3 位	インド	101.07 件	＋49.1%　（＋33.27 件）	9 位	14 位
4 位	ブルガリア	55.88 件	＋56.4%　（＋20.14 件）	17 位	22 位
5 位	ルーマニア	109.52 件	＋11.9%　（＋11.66 件）	8 位	11 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	ロシア	953.43 件	－31.5%　（－437.67 件）	1 位	1 位
2 位	米国	914.50 件	－12.7%　（－133.53 件）	2 位	2 位
3 位	スイス	45.35 件	－67.7%　（－95.10 件）	20 位	7 位
4 位	オランダ	780.49 件	－9.5%　（－82.02 件）	3 位	3 位
5 位	中国	710.12 件	－5.9%　（－44.64 件）	4 位	4 位

[i] 一日・1IP アドレス当たり。

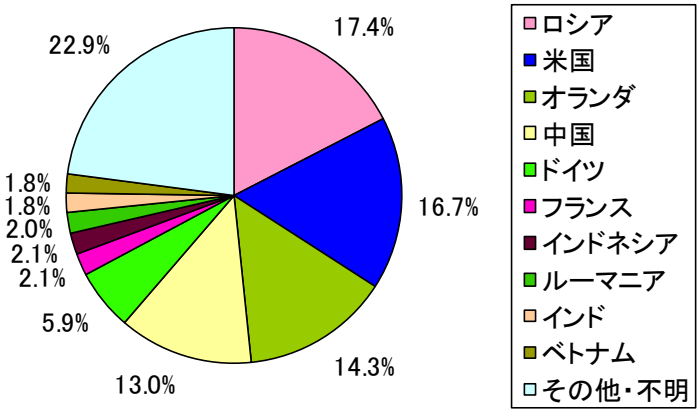

図 3-9　送信元国・地域別比率

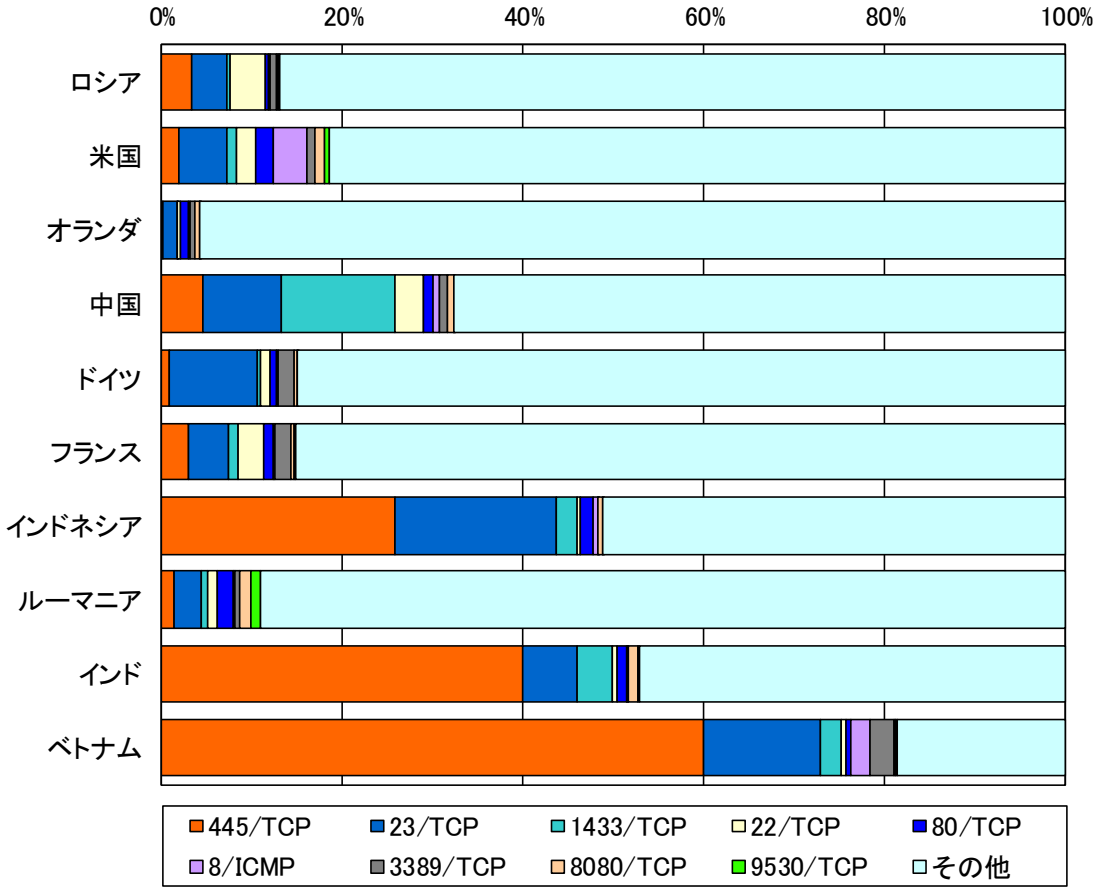

図 3-10　送信元国・地域別上位の宛先ポート別比率

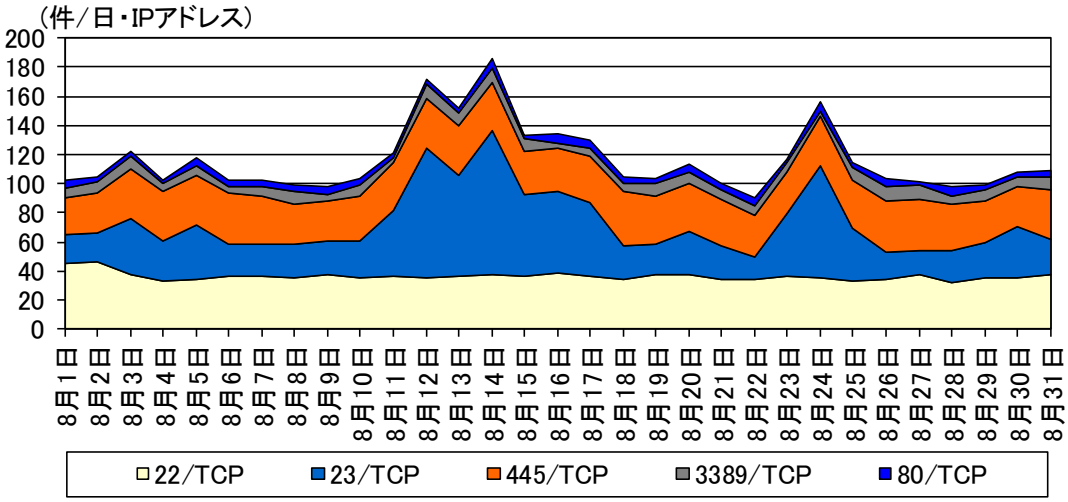

図 3-11　ロシアからの上位5ポートの検知件数の推移

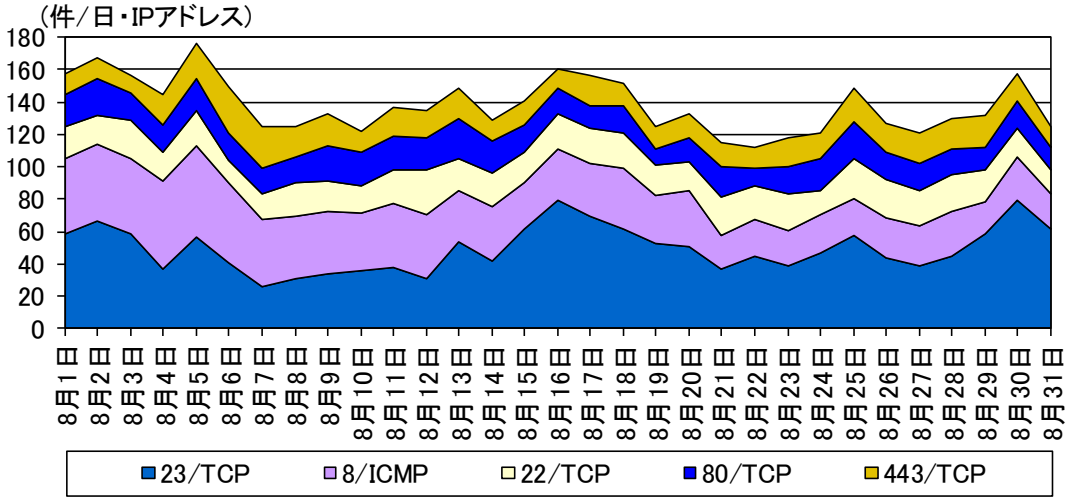

図 3-12　米国からの上位5ポートの検知件数の推移

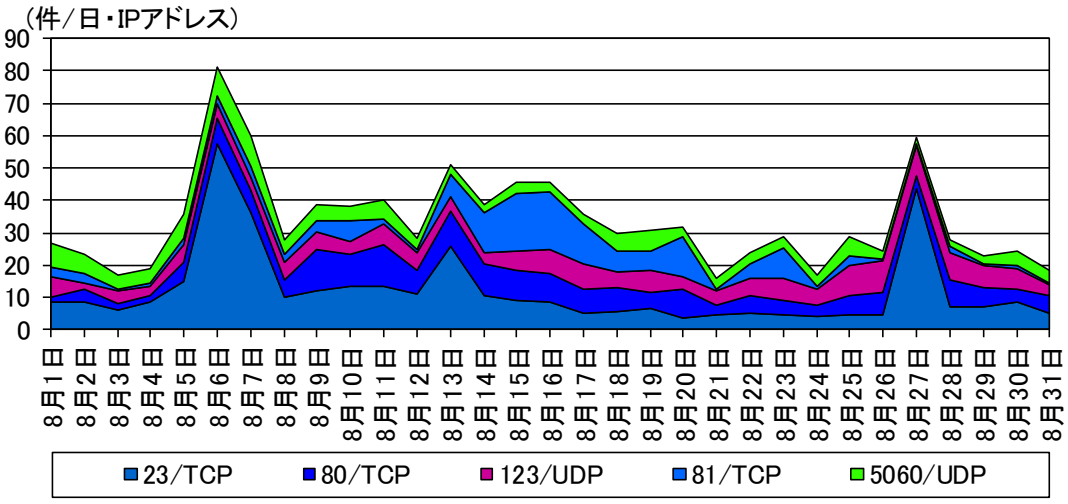

図 3-13　オランダからの上位5ポートの検知件数の推移

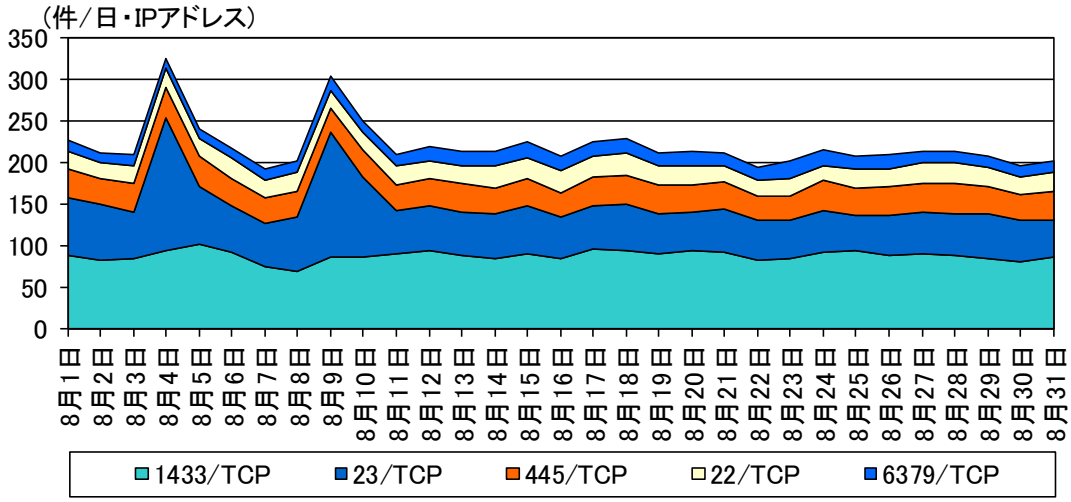

図 3-14　中国からの上位5ポートの検知件数の推移

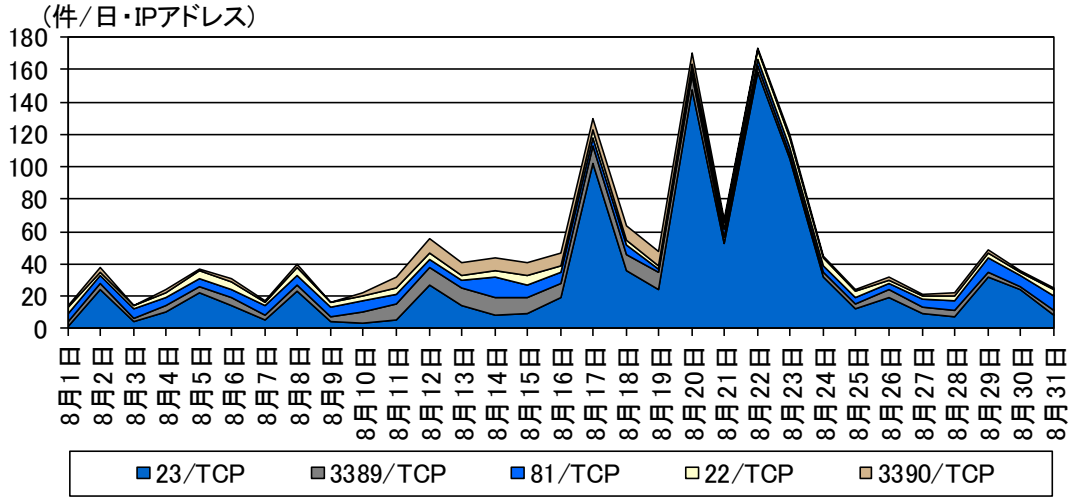

図 3-15　ドイツからの上位5ポートの検知件数の推移

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	1 位	INDICATOR-SCAN	274.69 件	−10.1 %　（−30.92 件）		2 位
2 位	2 位	Microsoft Windows Terminal server	234.39 件	−2.5%　（−6.10 件）		
3 位	3 位	SMBv1	122.49 件	−18.7%　（−28.11 件）		3 位
4 位	6 位	ICMP	29.12 件	−7.2%　（−2.26 件）		
5 位	5 位	SERVER-APACHE	26.16 件	−42.8%　（−19.55 件）		4 位

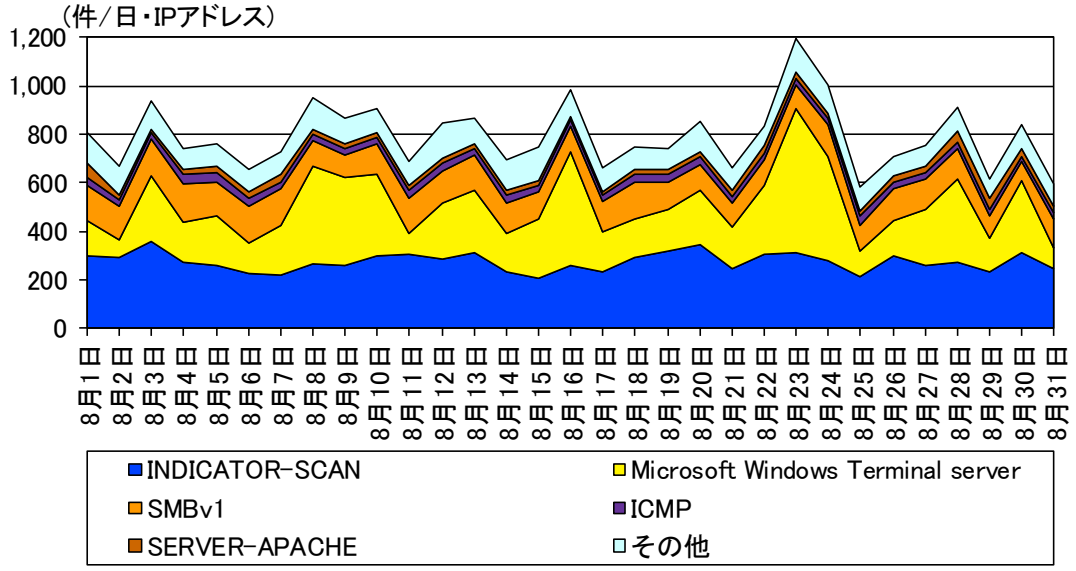

図 4-1　不正侵入等の攻撃手法別検知件数の推移

[i] 一日・1IP アドレス当たり。

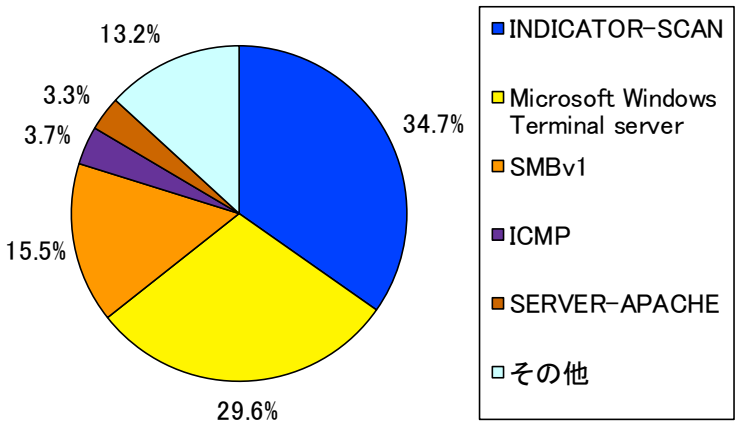

図 4-2 不正侵入等の攻撃手法別検知比率

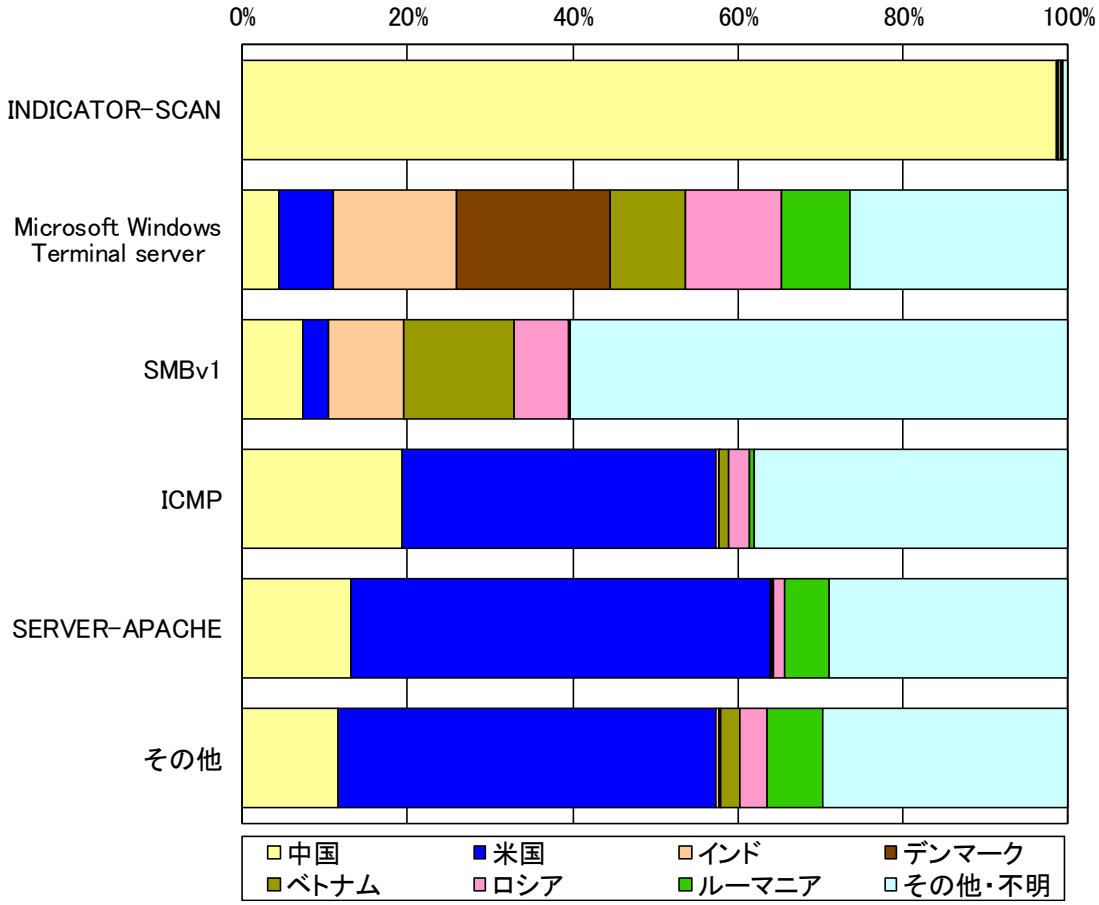

図 4-3 不正侵入等の攻撃手法の国・地域別検知比率

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	311.54 件	－9.6% （－33.15 件）
2 位	2 位	米国	91.78 件	－55.2% （－113.29 件）
3 位	7 位	インド	46.83 件	＋120.1% （＋25.55 件）
4 位	99 位	デンマーク	43.73 件	－ [ii] （＋43.62 件）
5 位	6 位	ベトナム	41.34 件	＋32.3% （＋10.09 件）

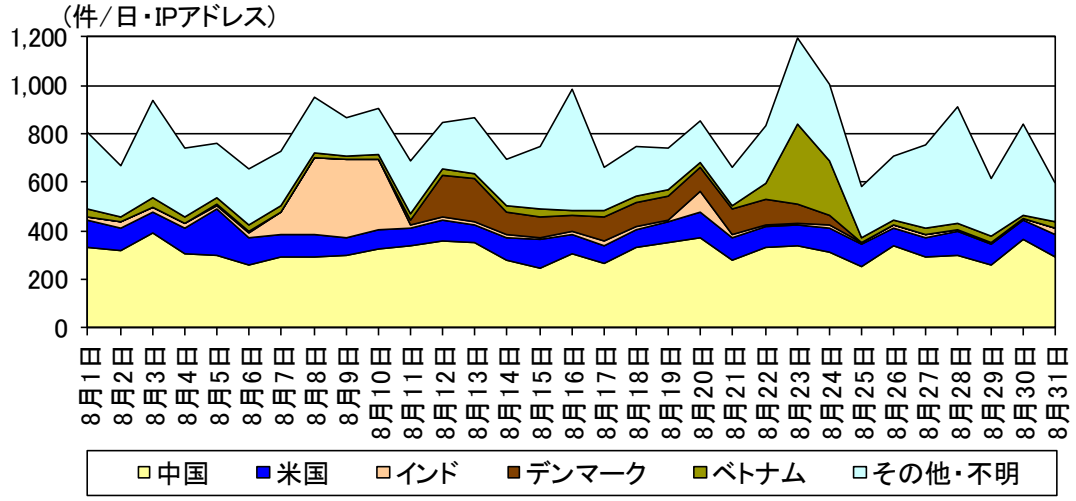

図 4-4 不正侵入等の送信元国・地域別検知件数の推移

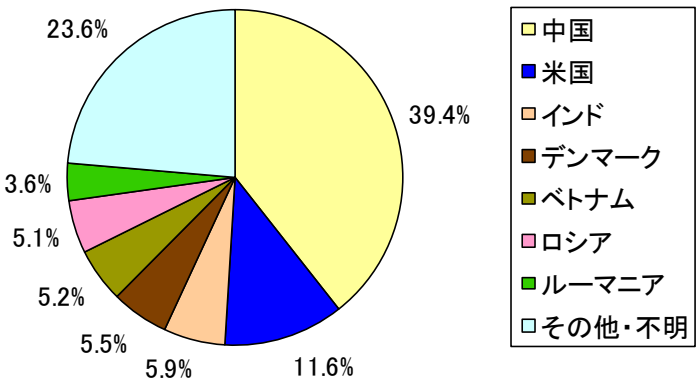

図 4-5 不正侵入等の送信元国・地域別検知比率

[i] 一日・1IP アドレス当たり。

[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。

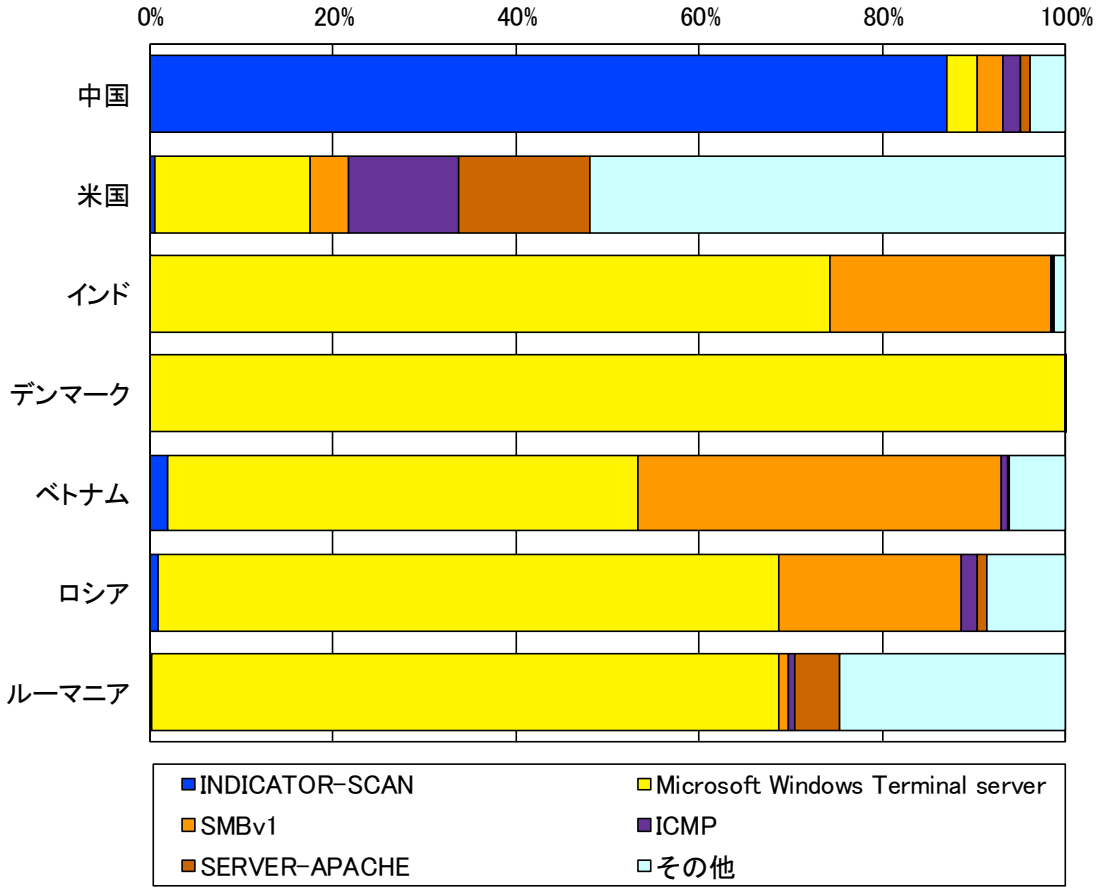

図 4-6 不正侵入等の送信元国・地域別上位の攻撃手法別検知比率

5　DoS 攻撃被害の観測結果

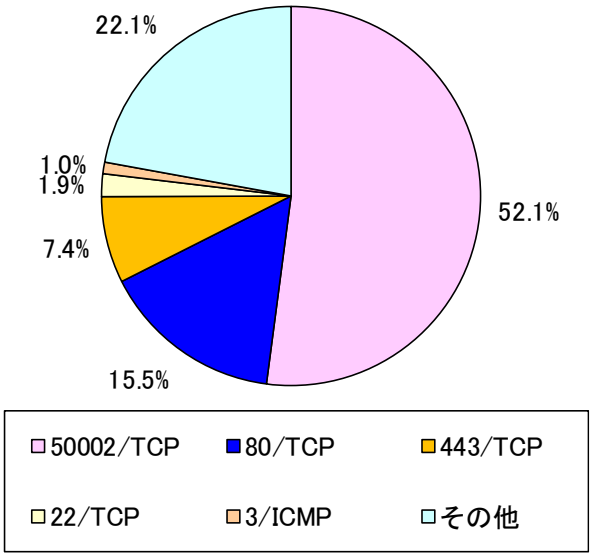

図 5-1　跳ね返りパケット送信元ポート別比率

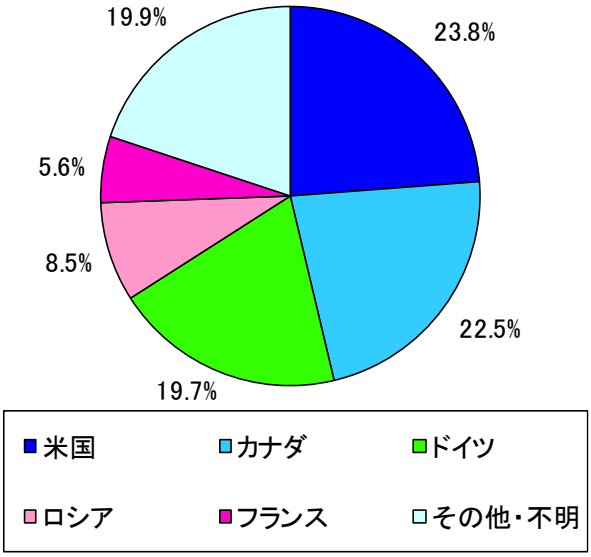

図 5-2　跳ね返りパケット送信元国・地域別比率