令和２年６月 23 日

令和2年5月期観測資料

1　観測結果概要

令和2年5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 6,413.1 件で、令和2年4月期（以下「前月期」という。）の 5,506.6 件と比較して 906.5 件（16.5%）増加しました。また、送信元 IP アドレス[i] 数は、一日当たり 53,994.7 個で、前月期の 48,028.2 件と比較して 5,966.5 個（12.4%）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 972.5 件で、前月期の 928.1 件と比較して 44.4 件（4.8%）増加しました。また、送信元 IP アドレス数は、一日当たり 12,527.4 個で、前月期の 8,152.1 個と比較して 4,375.3 個（53.7%）増加しました。

DoS 攻撃被害検知件数は、一日当たり 49,259.0 件で、前月期の 29,633.6 件と比較して 19,625.4 件（66.2%）増加しました。また、送信元 IP アドレス数は、一日当たり 6,866.4 個で、前月期の 4,550.2 個と比較して 2,316.2 個（50.9%）増加しました。

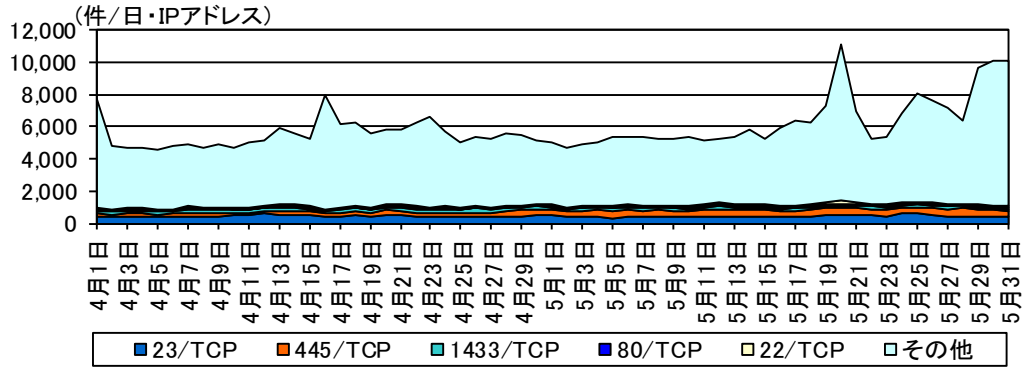

図 1-1　宛先ポート別検知件数の推移

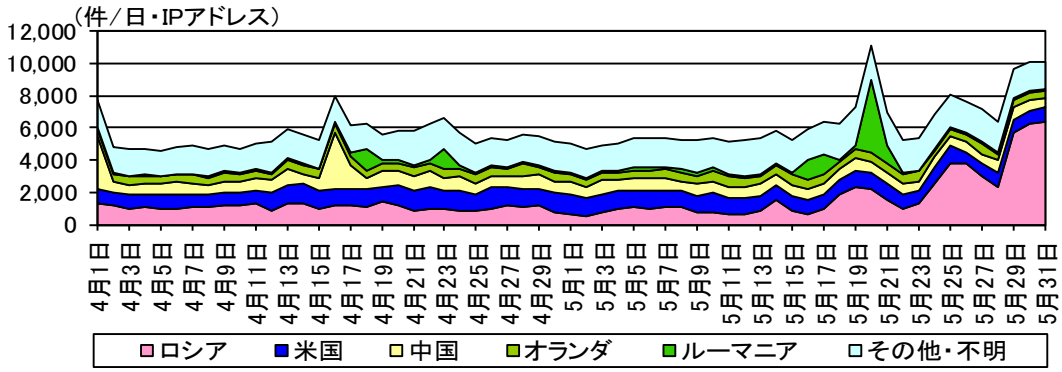

図 1-2　送信元国・地域別検知件数の推移 [ii]

[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が一切接続されていません。

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	23/TCP	428.60 件	－4.9%　（－21.94 件）
2 位	2 位	445/TCP	418.77 件	＋82.9%　（＋189.86 件）
3 位	3 位	1433/TCP	158.47 件	－18.8%　（－36.80 件）
4 位	4 位	80/TCP	87.56 件	＋2.4%　（＋2.05 件）
5 位	6 位	22/TCP	85.85 件	＋22.4%　（＋15.70 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	418.77 件	＋82.9%　（＋189.86 件）	2 位	2 位
2 位	37215/TCP	26.76 件	＋251.6%　（＋19.15 件）	18 位	49 位
3 位	2323/TCP	26.22 件	＋155.3%　（＋15.95 件）	19 位	35 位
4 位	22/TCP	85.85 件	＋22.4%　（＋15.70 件）	5 位	6 位
5 位	123/UDP	39.25 件	＋42.7%　（＋11.75 件）	14 位	16 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	1433/TCP	158.47 件	－18.8%　（－36.80 件）	3 位	3 位
2 位	5555/TCP	42.39 件	－46.4%　（－36.66 件）	13 位	5 位
3 位	52869/TCP	33.83 件	－45.5%　（－28.20 件）	15 位	7 位
4 位	23/TCP	428.60 件	－4.9%　（－21.94 件）	1 位	1 位
5 位	44614/UDP	検知なし	－　（－8.50 件）	－	45 位

[i] 一日・1IP アドレス当たり。

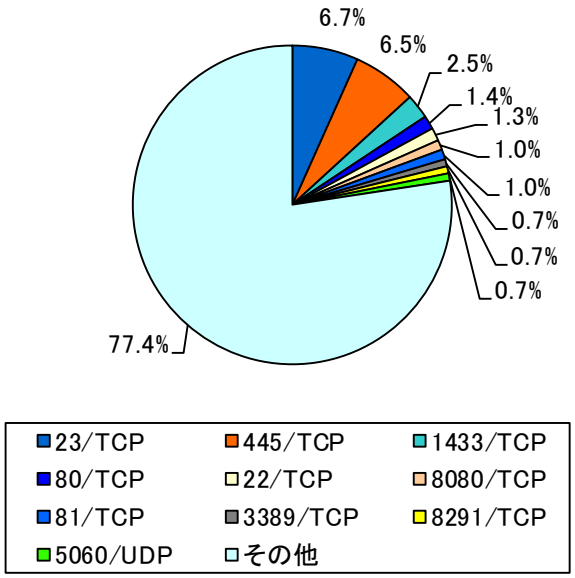

図 3-1　宛先ポート別比率（全て）[i]

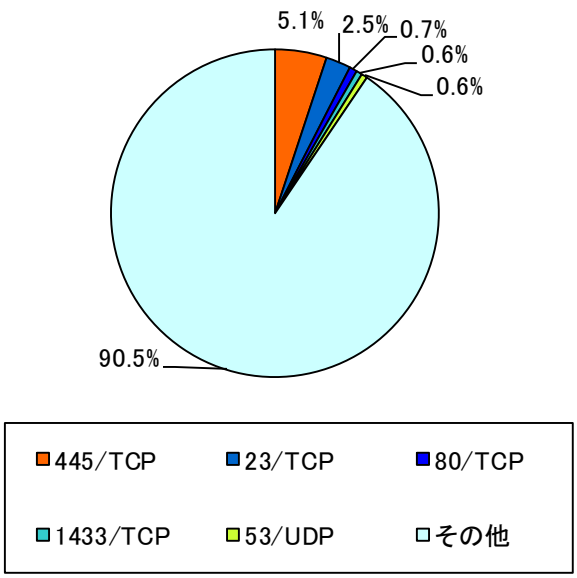

図 3-2　宛先ポート別比率（日本国内）

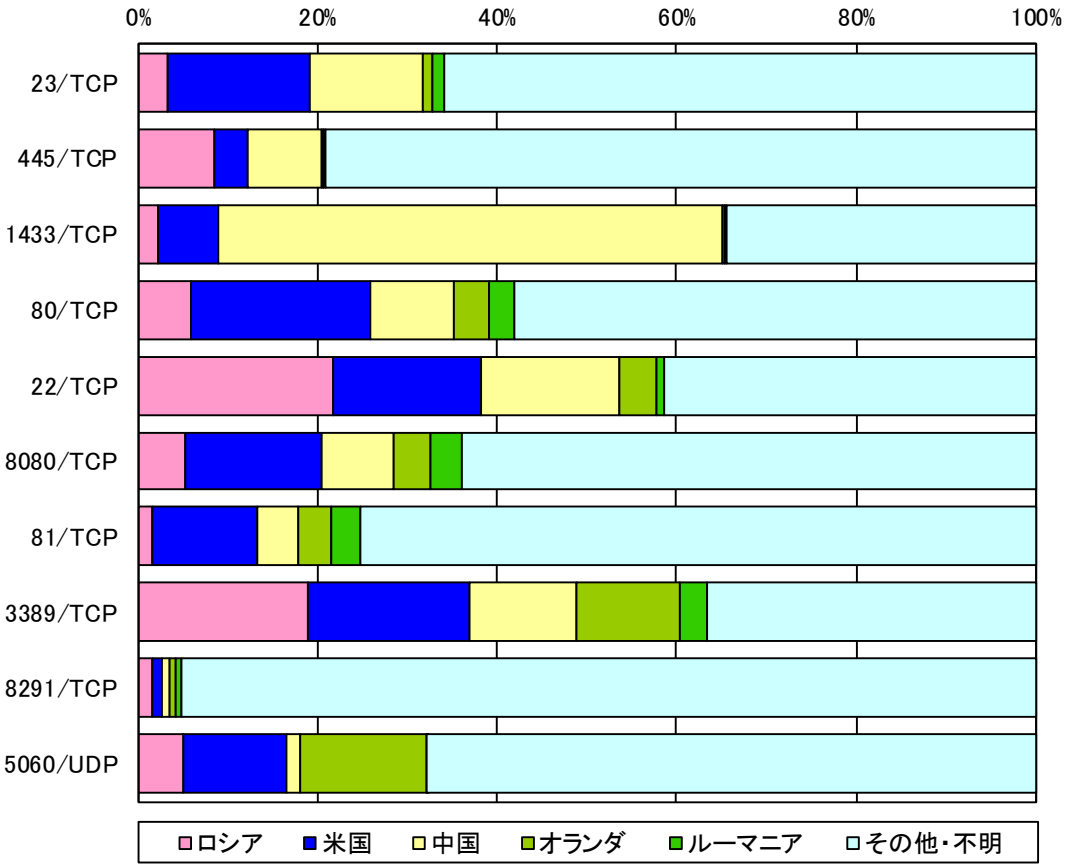

図 3-3　宛先ポート別上位の送信元国・地域別比率

[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。

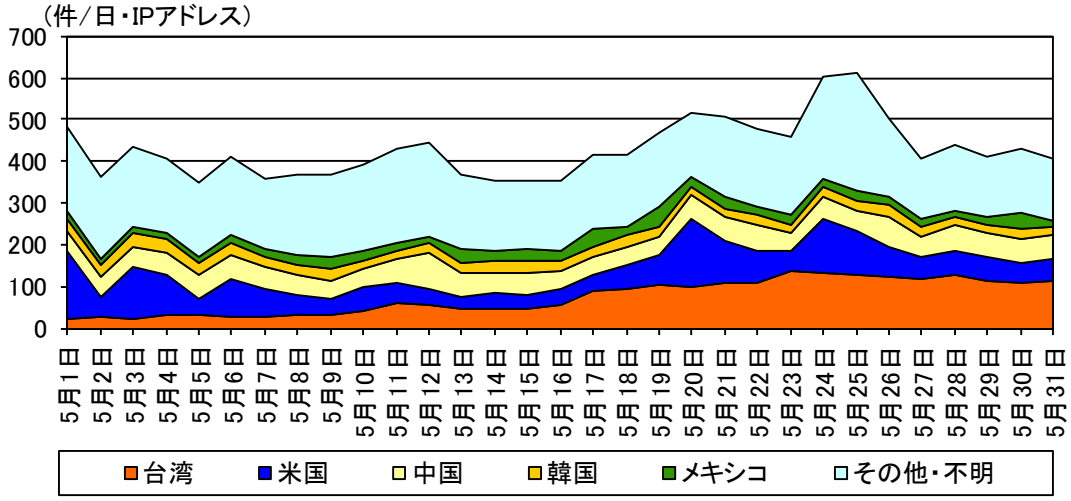

図 3-4　センサーのポート 23/TCP における検知件数の推移

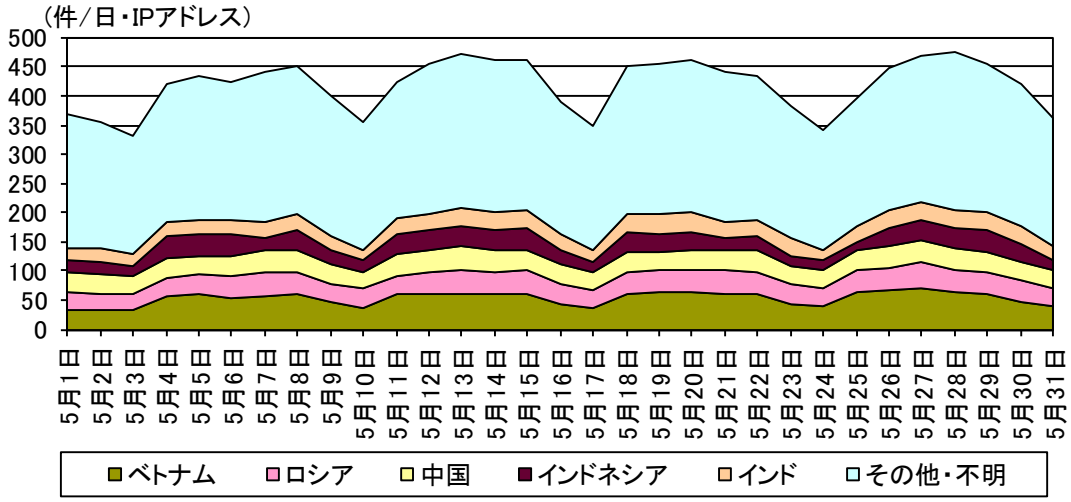

図 3-5　センサーのポート 445/TCP における検知件数の推移

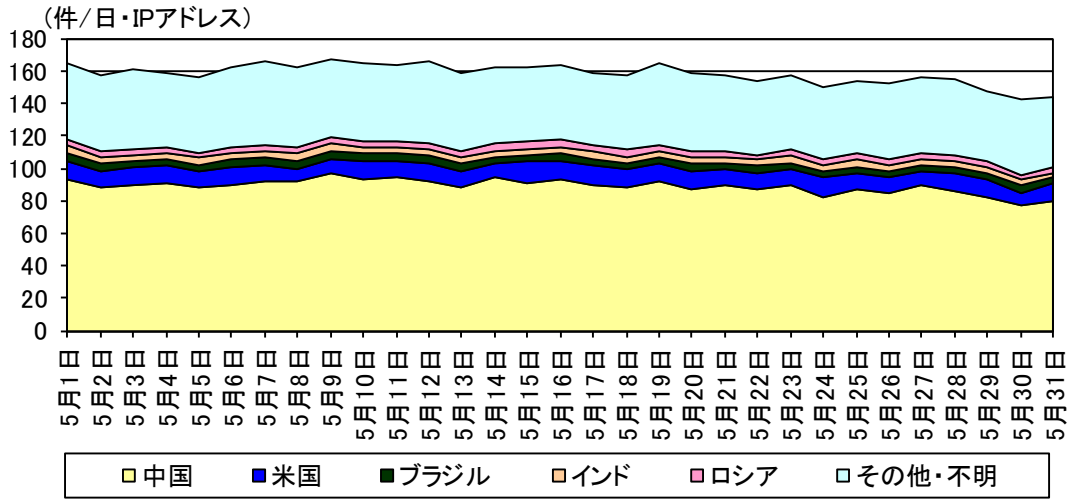

図 3-6　センサーのポート 1433/TCP における検知件数の推移

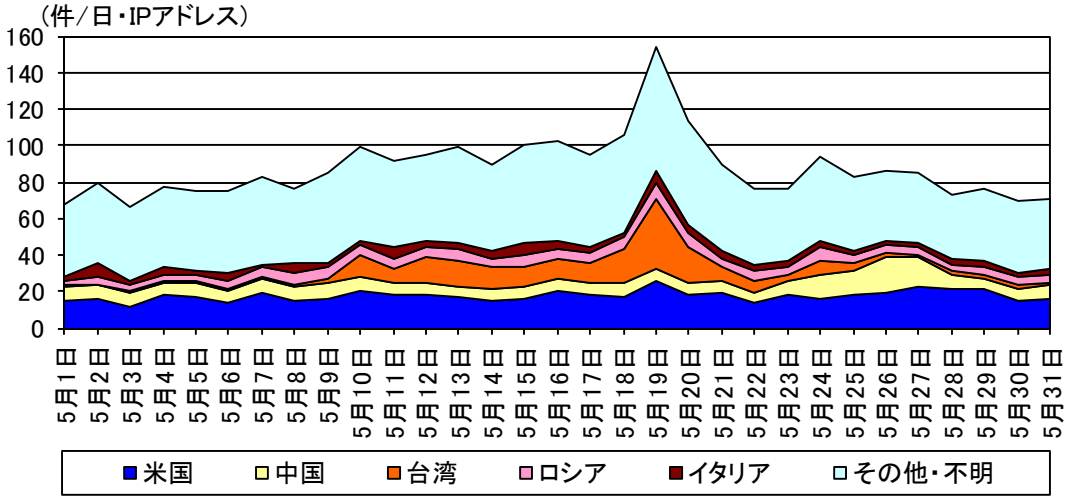

図 3-7　センサーのポート 80/TCP における検知件数の推移

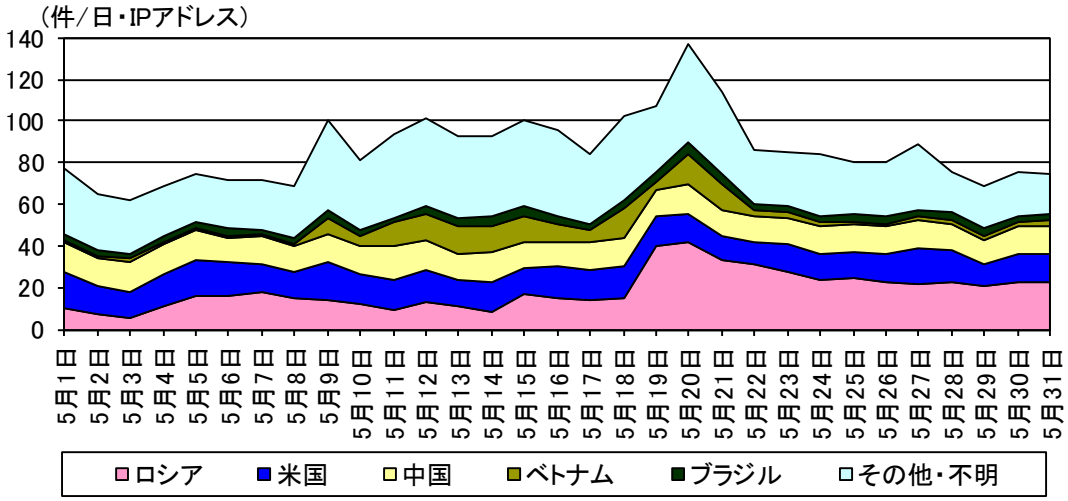

図 3-8　センサーのポート 22/TCP における検知件数の推移

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	1,892.44 件	＋73.3%　（＋800.35 件）
2 位	3 位	米国	975.66 件	－5.4%　（－55.51 件）
3 位	2 位	中国	697.31 件	－27.3%　（－261.26 件）
4 位	4 位	オランダ	515.12 件	＋5.2%　（＋25.36 件）
5 位	5 位	ルーマニア	374.61 件	＋87.0%　（＋174.29 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	ロシア	1,892.44 件	＋73.3%　（＋800.35 件）	1 位	1 位
2 位	ルーマニア	374.61 件	＋87.0%　（＋174.29 件）	5 位	5 位
3 位	台湾	187.47 件	＋228.3%　（＋130.37 件）	6 位	16 位
4 位	日本	91.69 件	＋152.2%　（＋55.33 件）	11 位	21 位
5 位	ベトナム	118.82 件	＋27.4%　（＋25.59 件）	8 位	10 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	中国	697.31 件	－27.3%　（－261.26 件）	3 位	3 位
2 位	米国	975.66 件	－5.4%　（－55.51 件）	2 位	2 位
3 位	フランス	98.36 件	－30.8%　（－43.72 件）	10 位	7 位
4 位	ブルガリア	47.94 件	－33.0%　（－23.64 件）	20 位	12 位
5 位	カナダ	61.08 件	－23.0%　（－18.20 件）	16 位	11 位

[i] 一日・1IP アドレス当たり。

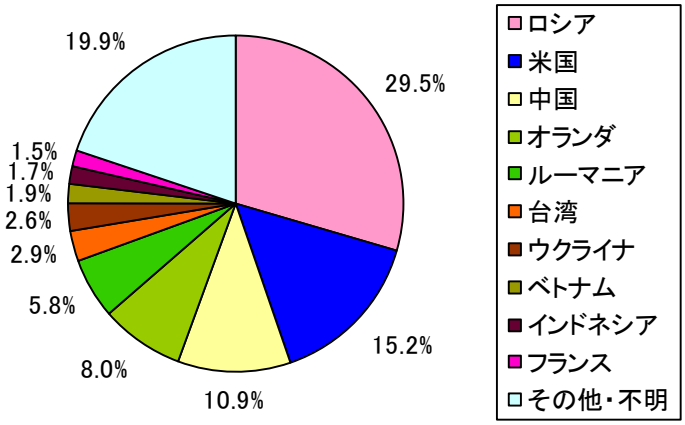

図 3-9　送信元国・地域別比率

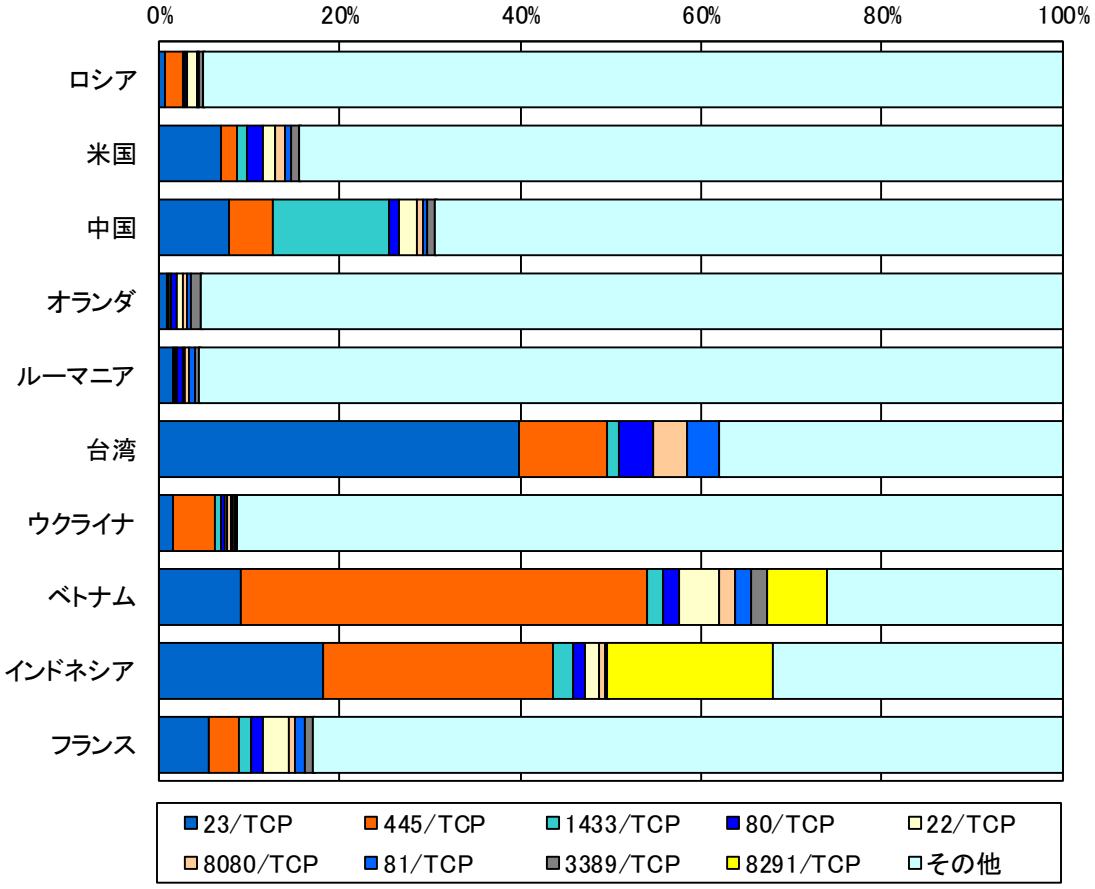

図 3-10　送信元国・地域別上位の宛先ポート別比率

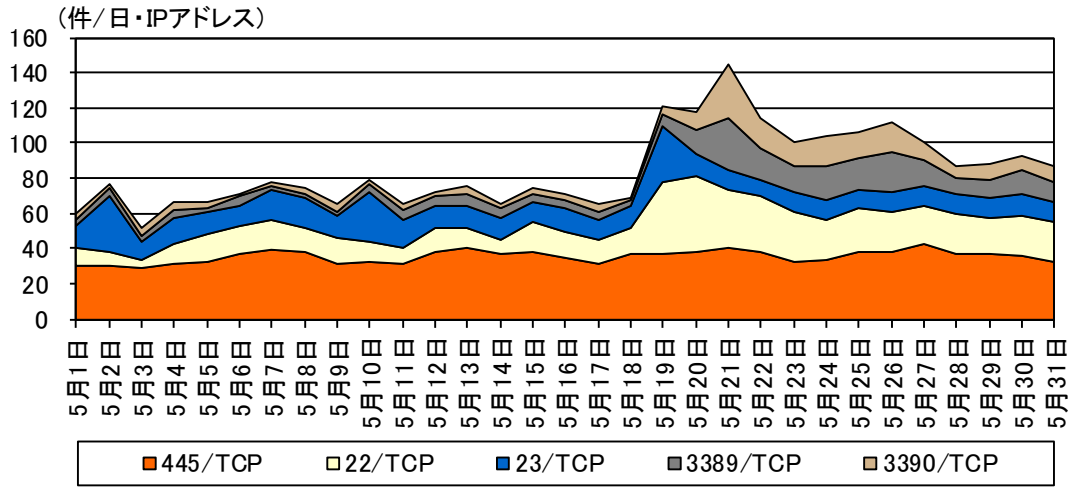

図 3-11　ロシアからの上位5ポートの検知件数の推移

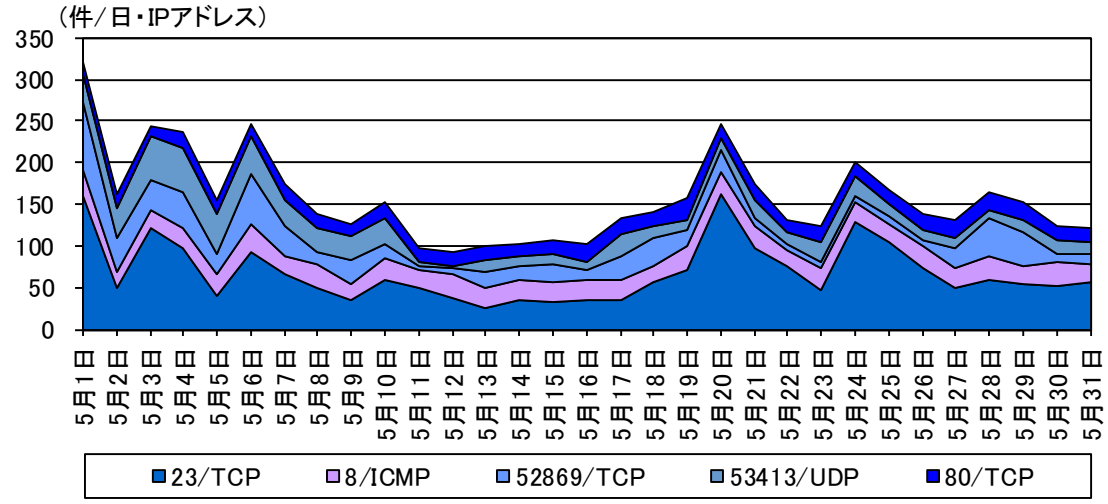

図 3-12　米国からの上位5ポートの検知件数の推移

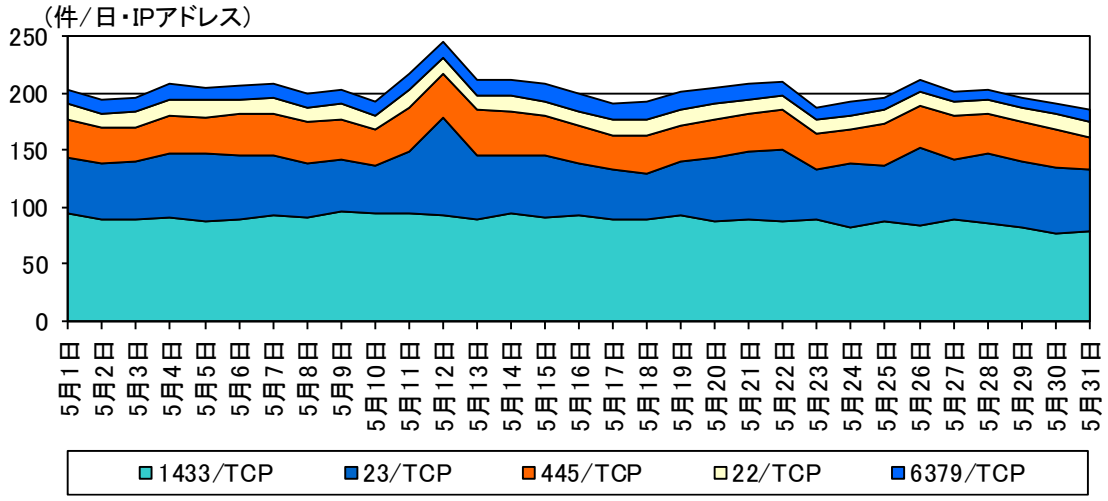

図 3-13　中国からの上位5ポートの検知件数の推移

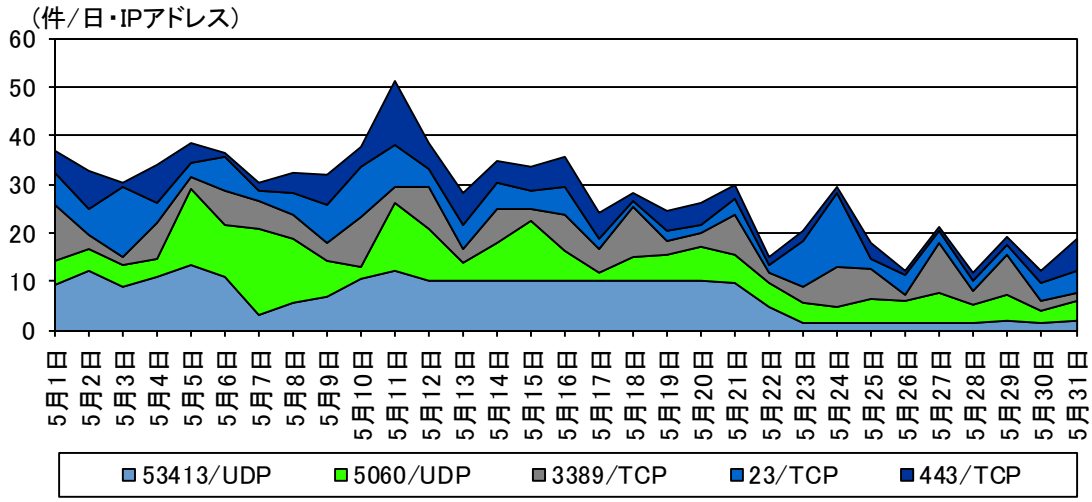

図 3-14　オランダからの上位5ポートの検知件数の推移

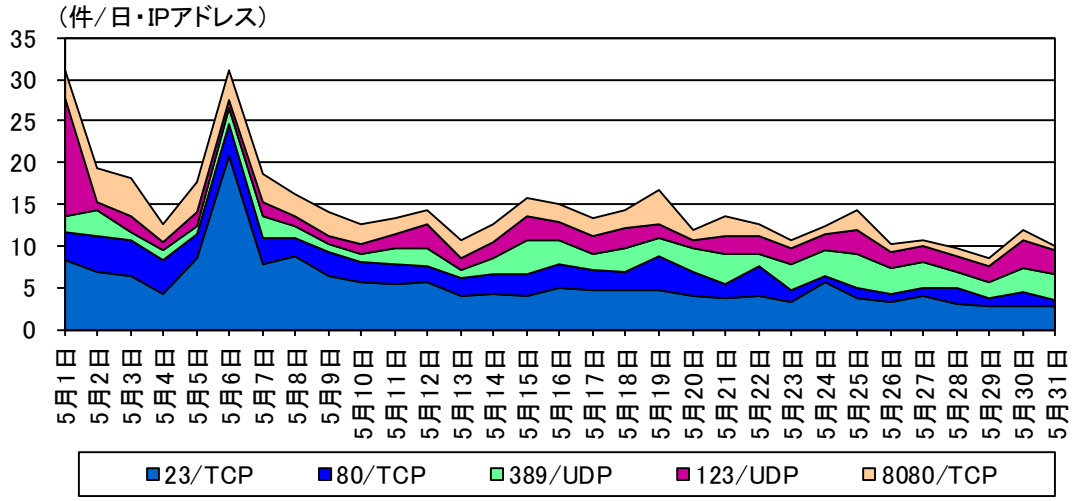

図 3-15　ルーマニアからの上位5ポートの検知件数の推移

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	Microsoft Windows Terminal server	306.03 件	−5.9%　（−19.05 件）		2 位
2 位	2 位	INDICATOR-SCAN	301.09 件	＋26.0%　（＋62.12 件）	1 位	
3 位	3 位	SMBv1	136.83 件	＋34.6%　（＋35.19 件）	2 位	
4 位	6 位	SERVER-APACHE	44.68 件	＋73.5%　（＋18.93 件）	3 位	
5 位	8 位	OS-WINDOWS	32.39 件	＋92.1%　（＋15.53 件）	4 位	

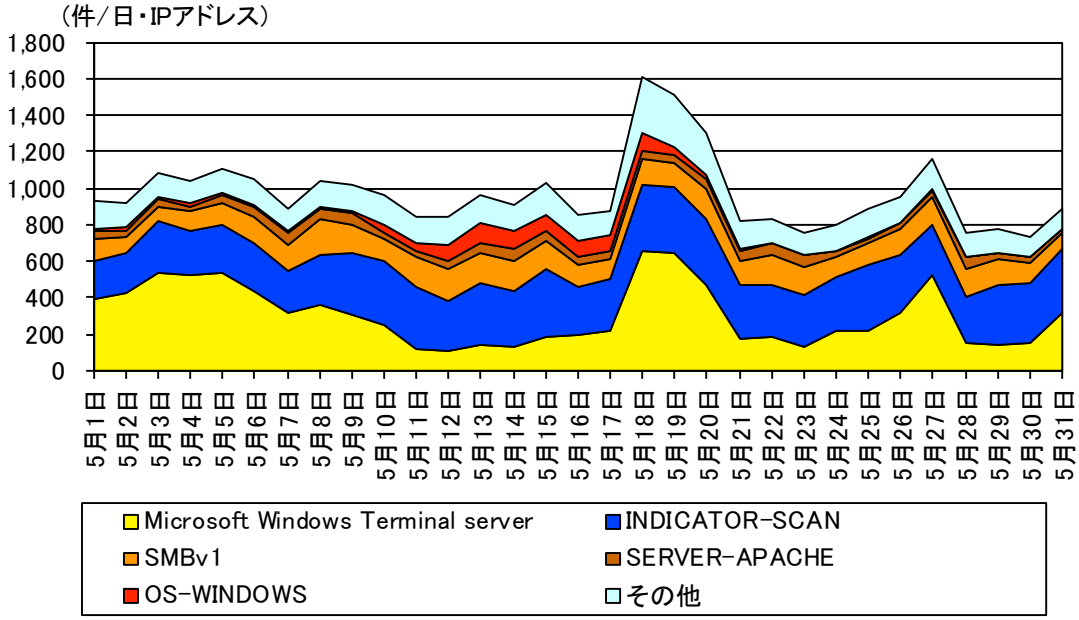

図 4-1　不正侵入等の攻撃手法別検知件数の推移

[i] 一日・1IP アドレス当たり。

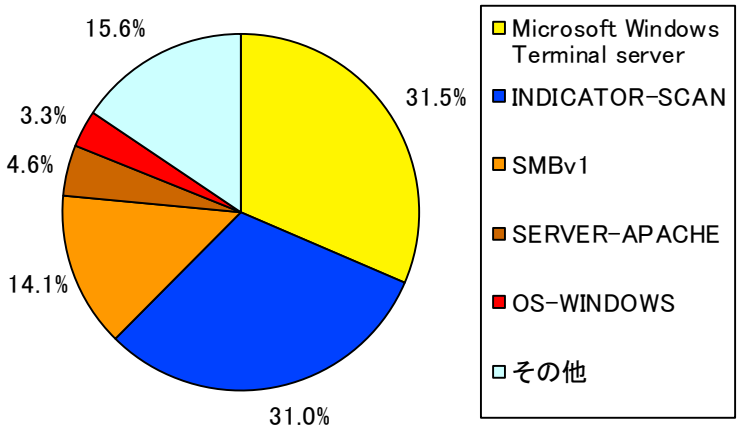

図 4-2 不正侵入等の攻撃手法別検知比率

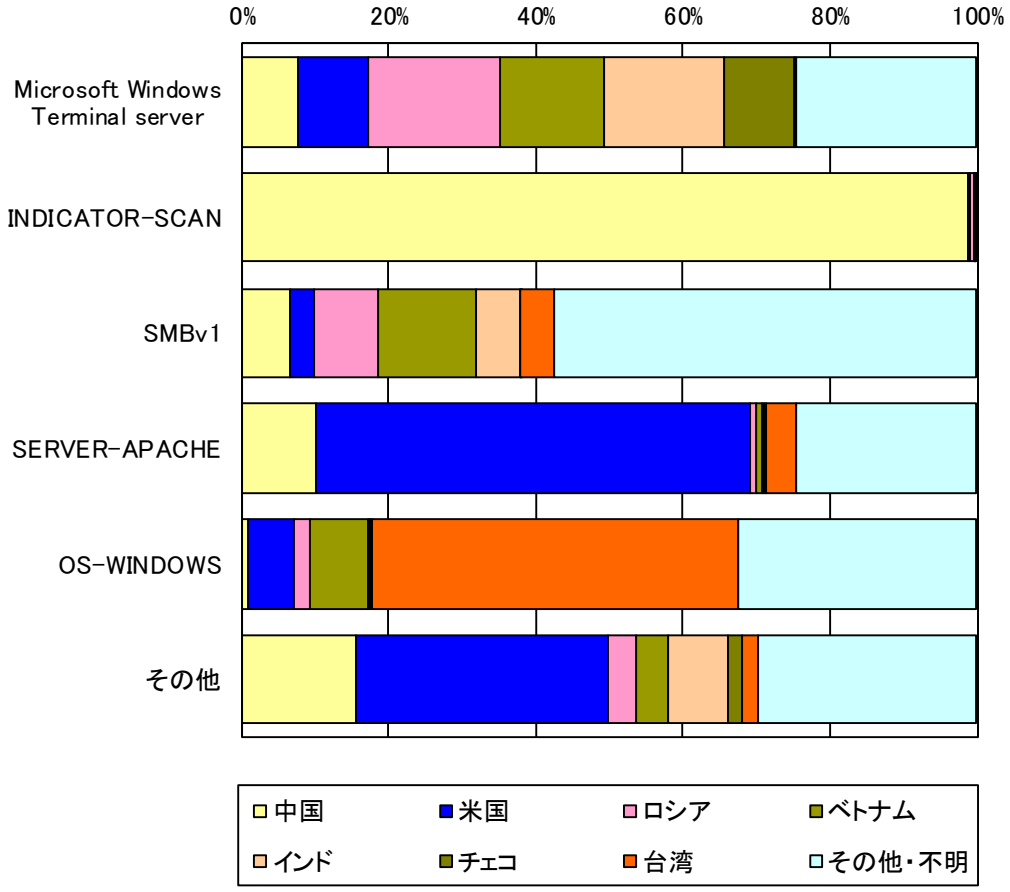

図 4-3 不正侵入等の攻撃手法の国・地域別検知比率

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	358.15 件	＋22.7% （＋66.22 件）
2 位	3 位	米国	114.38 件	＋11.2% （＋11.56 件）
3 位	4 位	ロシア	75.80 件	＋69.8% （＋31.15 件）
4 位	6 位	ベトナム	71.08 件	＋137.3% （＋41.13 件）
5 位	10 位	インド	70.62 件	＋340.8% （＋54.60 件）

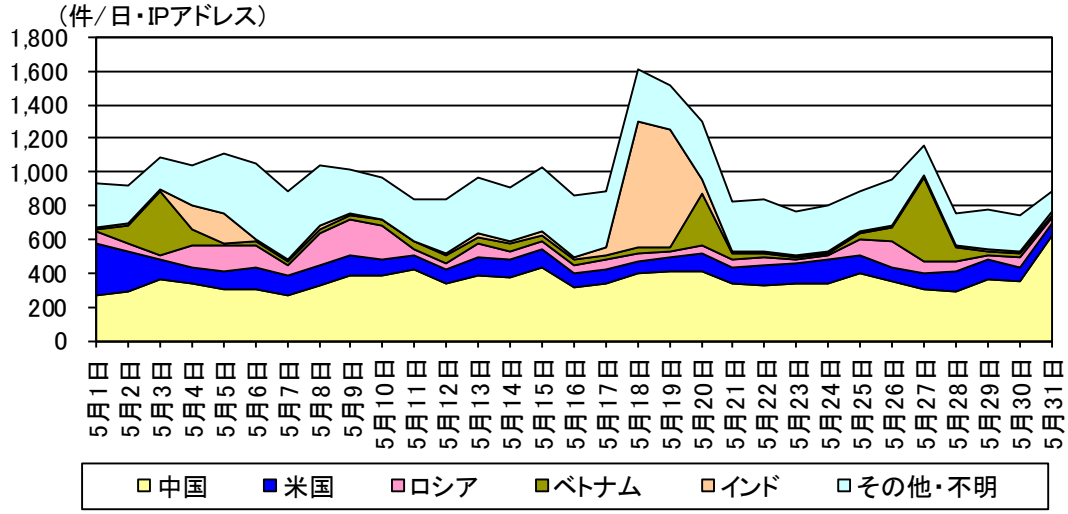

図 4-4 不正侵入等の送信元国・地域別検知件数の推移

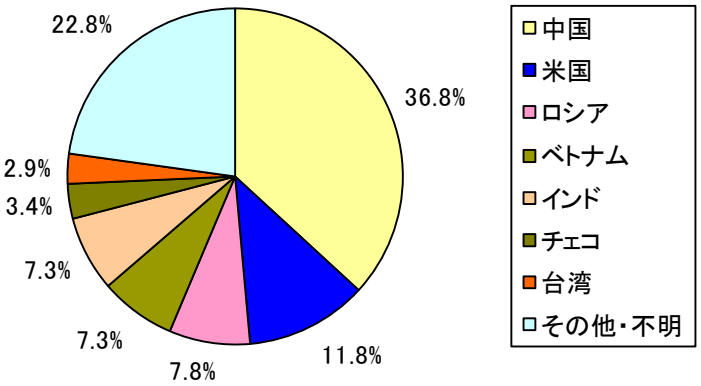

図 4-5 不正侵入等の送信元国・地域別検知比率

[i] 一日・1IP アドレス当たり。

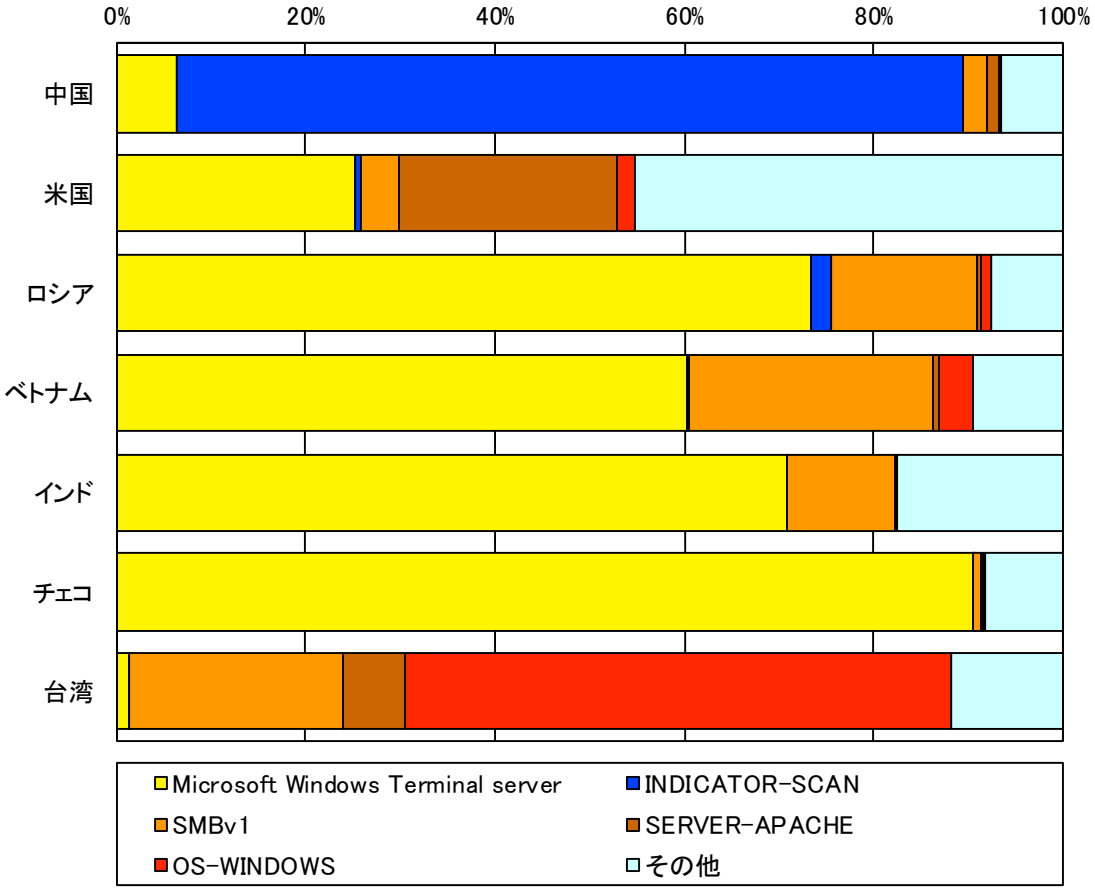

図 4-6 不正侵入等の送信元国・地域別上位の攻撃手法別検知比率

5　DoS 攻撃被害の観測結果

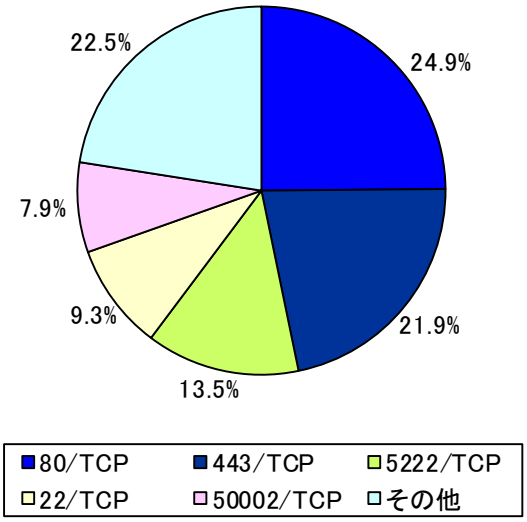

図 5-1　跳ね返りパケット送信元ポート別比率

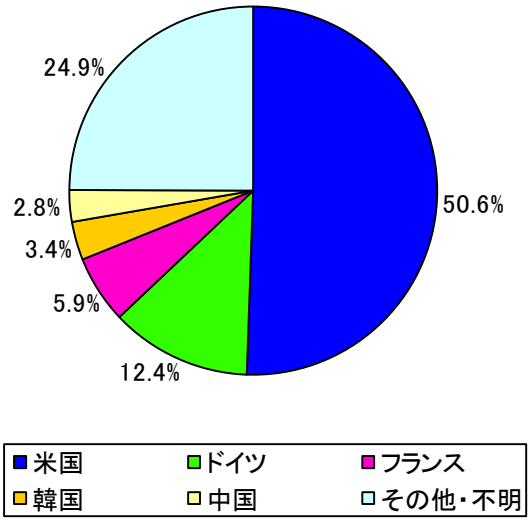

図 5-2　跳ね返りパケット送信元国・地域別比率