令和３年２月２日

令和2年 12 月期観測資料

1　観測結果概要

令和2年 12 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 8,770.2 件で、令和2年 11 月期（以下「前月期」という。）の 7,402.7 件と比較して 1,367.6 件（18.5%）増加しました。また、送信元 IP アドレス[i]数は、一日当たり 47,874.0 個で、前月期の 50,815.0 個と比較して 2,941.0 個（5.8%）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 1,107.3 件で、前月期の 1,144.8 件と比較して 37.5 件（3.3%）減少しました。また、送信元 IP アドレス数は、一日当たり 11,197.3 個で、前月期の 10,673.7 個と比較して 523.6 個（4.9%）増加しました。

DoS 攻撃被害検知件数は、一日当たり 15,860.4 件で、前月期の 12,724.0 件と比較して 3,136.4 件（24.6%）増加しました。また、送信元 IP アドレス数は、一日当たり 1,181.2 個で、前月期の 696.4 個と比較して 484.8 個（69.6%）増加しました。

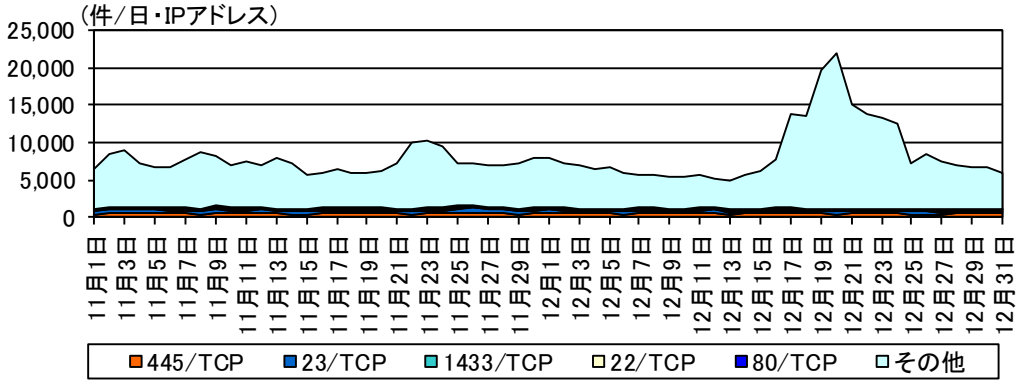

図 1-1　宛先ポート別検知件数の推移

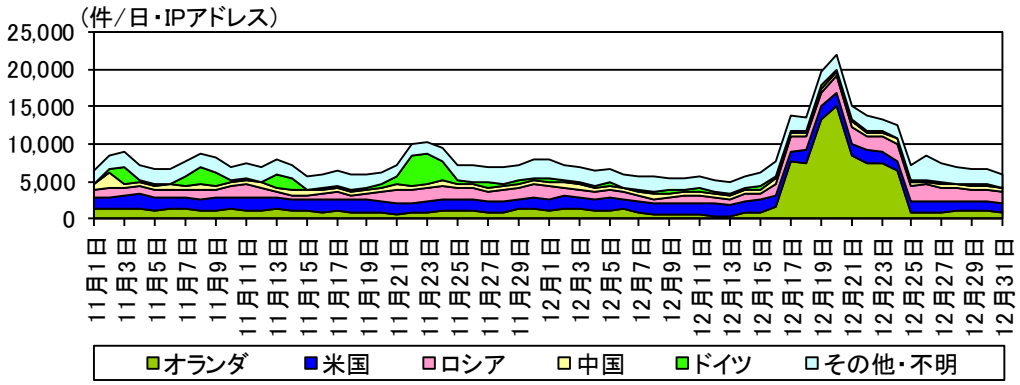

図 1-2　送信元国・地域別検知件数の推移 [ii]

[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	527.67 件	＋0.7%　（＋3.90 件）
2 位	2 位	23/TCP	340.98 件	－21.4%　（－93.01 件）
3 位	3 位	1433/TCP	143.36 件	－6.8%　（－10.54 件）
4 位	4 位	22/TCP	114.41 件	＋3.1%　（＋3.44 件）
5 位	5 位	80/TCP	72.99 件	－14.3%　（－12.18 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	0/TCP	45.08 件	－[ii]　（＋42.93 件）	9 位	－[ii]
2 位	123/UDP	47.57 件	＋41.2%　（＋13.89 件）	7 位	16 位
3 位	26/TCP	18.63 件	＋194.6%　（＋12.31 件）	21 位	56 位
4 位	6379/TCP	31.59 件	＋39.3%　（＋8.92 件）	14 位	20 位
5 位	37215/TCP	11.67 件	＋196.8%　（＋7.74 件）	31 位	－[ii]

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	340.98 件	－21.4%　（－93.01 件）	2 位	2 位
2 位	8/ICMP	30.69 件	－53.1%　（－34.69 件）	16 位	6 位
3 位	500/UDP	13.04 件	－71.9%　（－33.34 件）	29 位	12 位
4 位	52869/TCP	18.51 件	－56.2%　（－23.79 件）	22 位	14 位
5 位	38725/UDP	0.00 件	－100.0%　（－16.75 件）	－[ii]	27 位

[i] 一日・1IP アドレス当たり。

[ii]アクセス件数が僅かなため、前月期比、前月期順位及び今月期順位は記載していません。

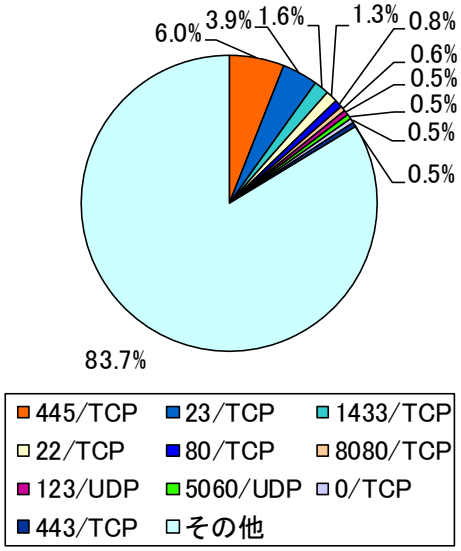

図 3-1　宛先ポート別比率（全て）[i]

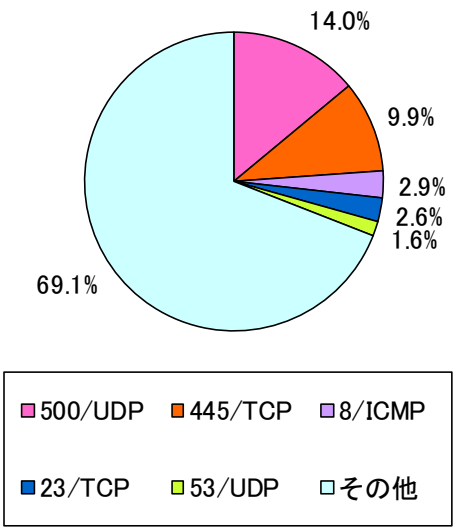

図 3-2　宛先ポート別比率（日本国内）

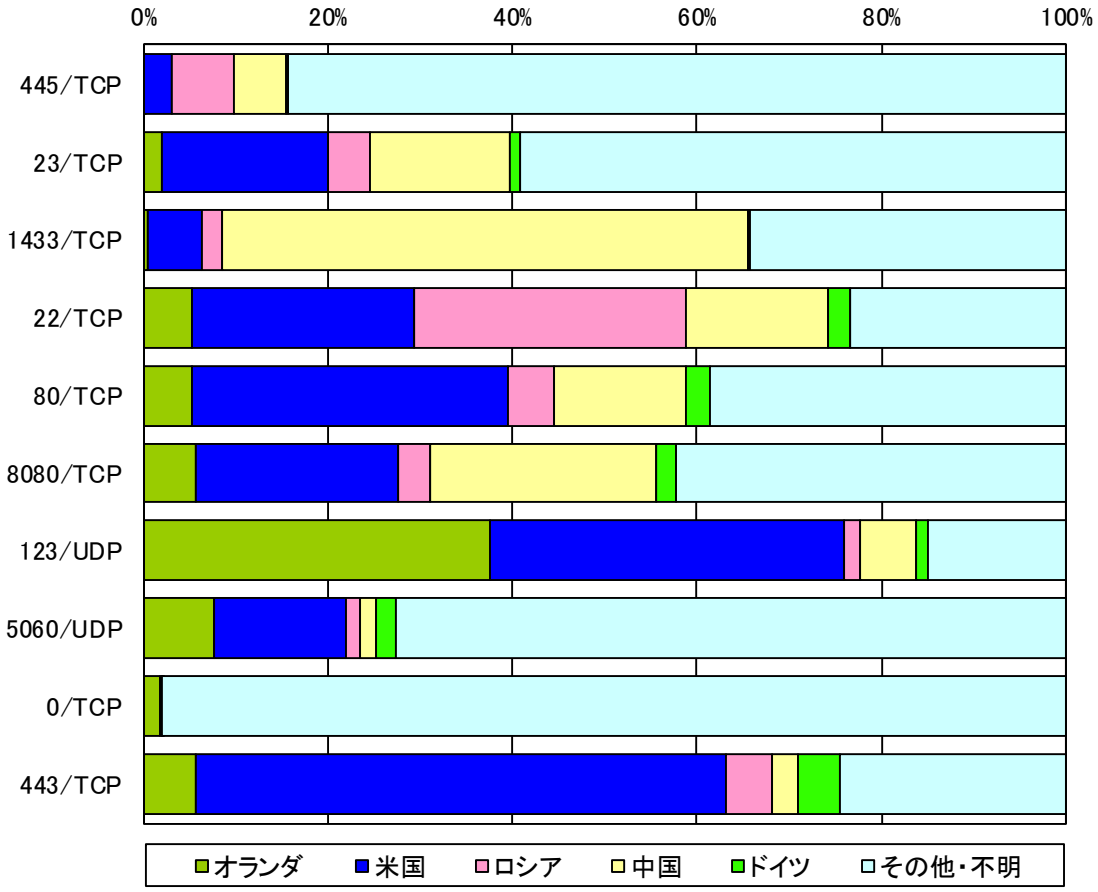

図 3-3　宛先ポート別上位の送信元国・地域別比率

[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。

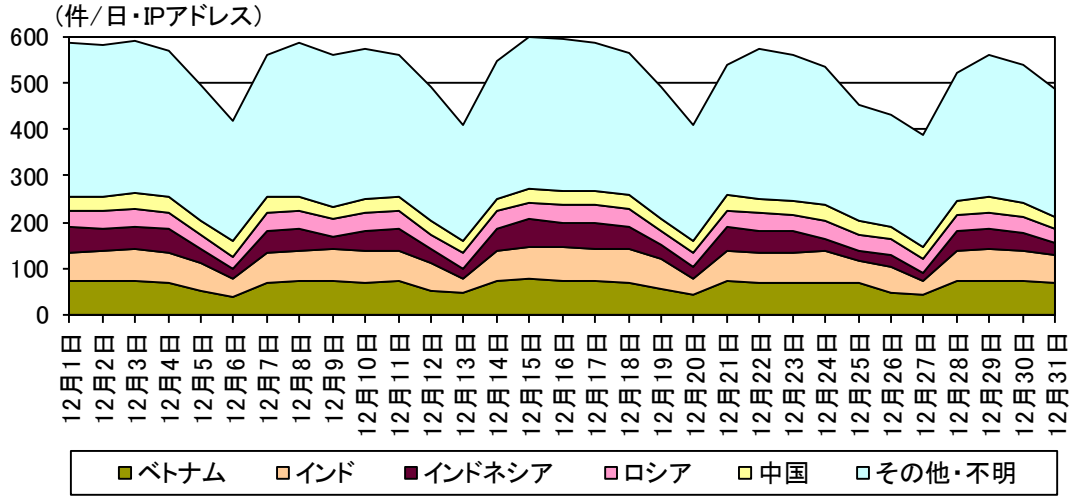

図 3-4　センサーのポート 445/TCP における検知件数の推移

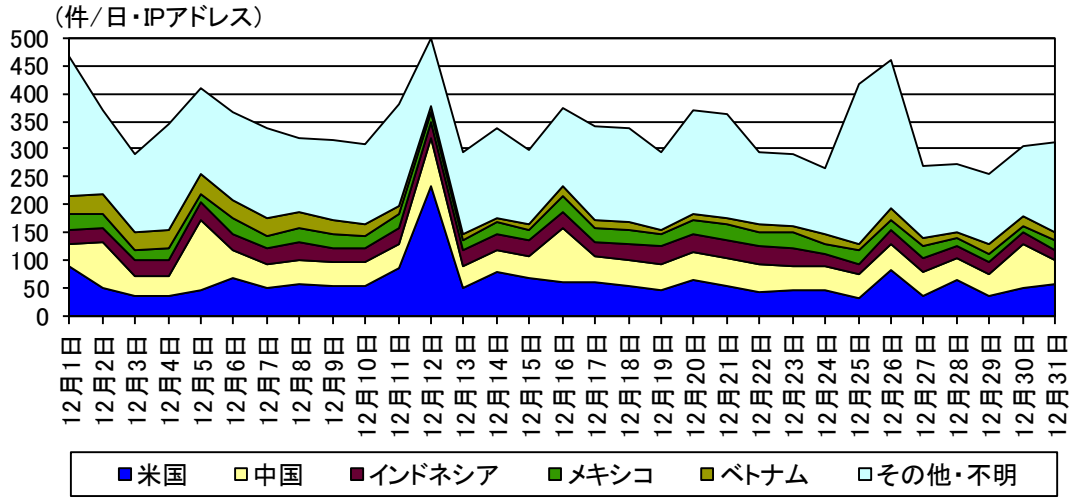

図 3-5　センサーのポート 23/TCP における検知件数の推移

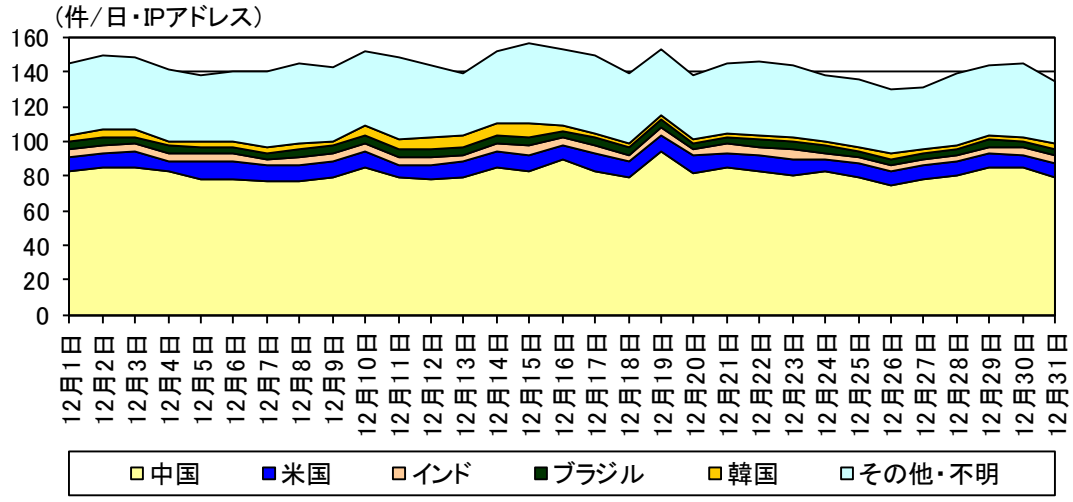

図 3-6　センサーのポート 1433/TCP における検知件数の推移

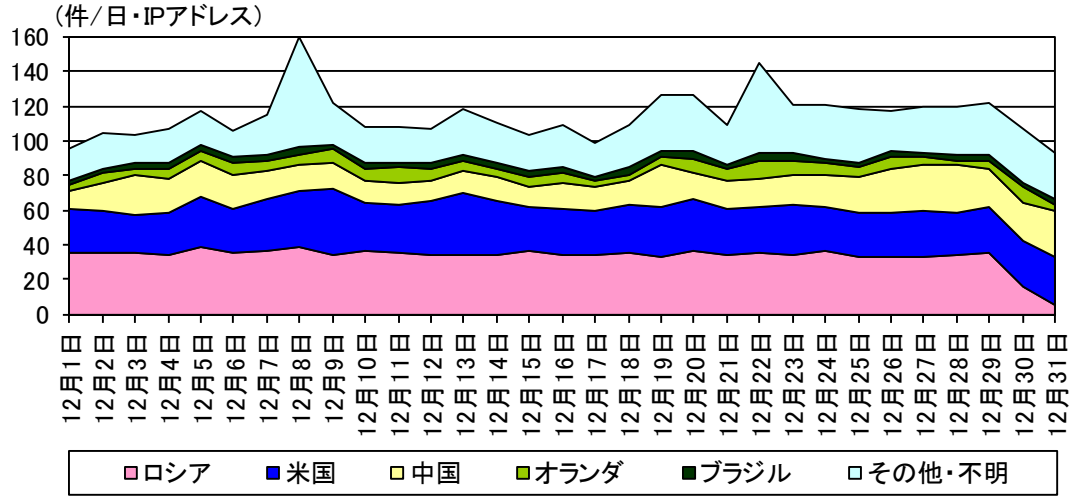

図 3-7　センサーのポート 22/TCP における検知件数の推移

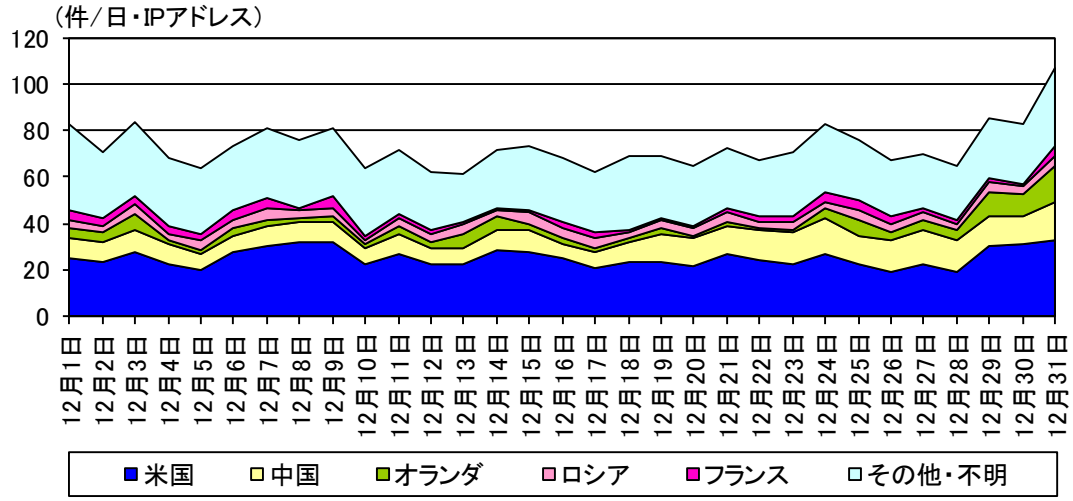

図 3-8　センサーのポート 80/TCP における検知件数の推移

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	3 位	オランダ	3,058.73 件	＋183.9%　（＋1,981.43 件）
2 位	1 位	米国	1,541.42 件	－3.5%　（－56.00 件）
3 位	2 位	ロシア	1,423.10 件	＋16.5%　（＋201.62 件）
4 位	5 位	中国	554.04 件	－14.7%　（－95.19 件）
5 位	4 位	ドイツ	295.34 件	－68.3%　（－635.94 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	オランダ	3,058.73 件	＋183.9%　（＋1,981.43 件）	1 位	3 位
2 位	ロシア	1,423.10 件	＋16.5%　（＋201.62 件）	3 位	2 位
3 位	ブルガリア	130.65 件	＋165.0%　（＋81.36 件）	10 位	20 位
4 位	ウクライナ	131.46 件	＋119.3%　（＋71.52 件）	9 位	15 位
5 位	英国	101.76 件	＋43.0%　（＋30.60 件）	11 位	12 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	ドイツ	295.34 件	－68.3%　（－635.94 件）	5 位	4 位
2 位	中国	554.04 件	－14.7%　（－95.19 件）	4 位	5 位
3 位	日本	72.98 件	－49.2%　（－70.64 件）	12 位	8 位
4 位	米国	1,541.42 件	－3.5%　（－56.00 件）	2 位	1 位
5 位	スイス	19.48 件	－74.1%　（－55.69 件）	29 位	11 位

[i] 一日・1IP アドレス当たり。

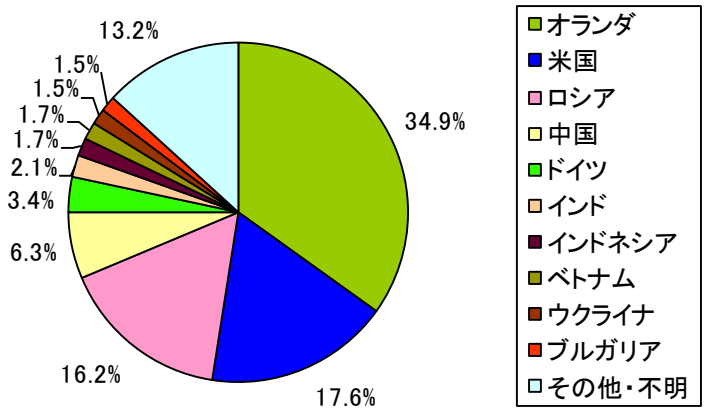

図 3-9　送信元国・地域別比率

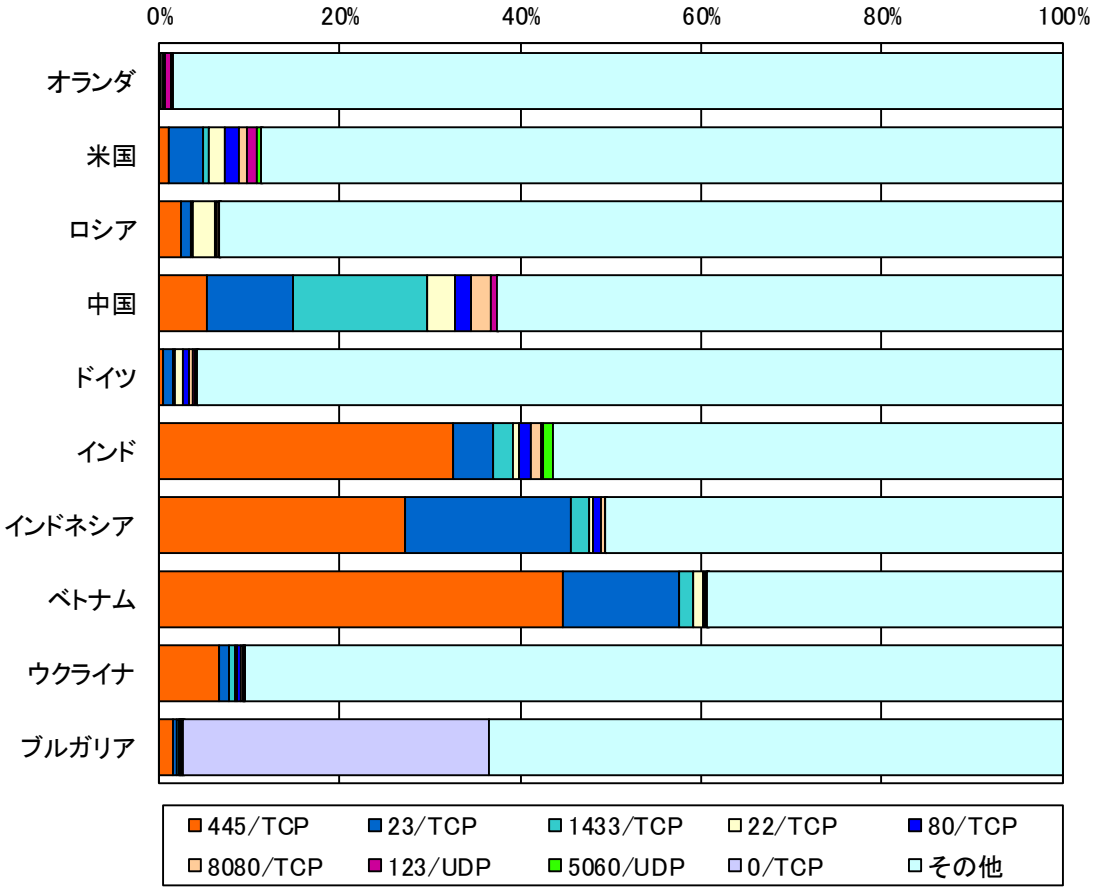

図 3-10　送信元国・地域別上位の宛先ポート別比率

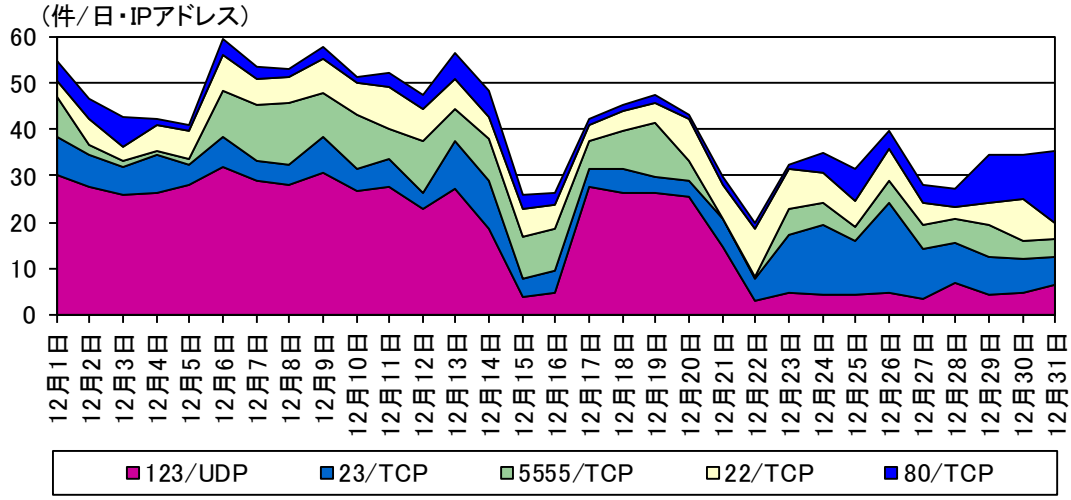

図 3-11　オランダからの上位5ポートの検知件数の推移

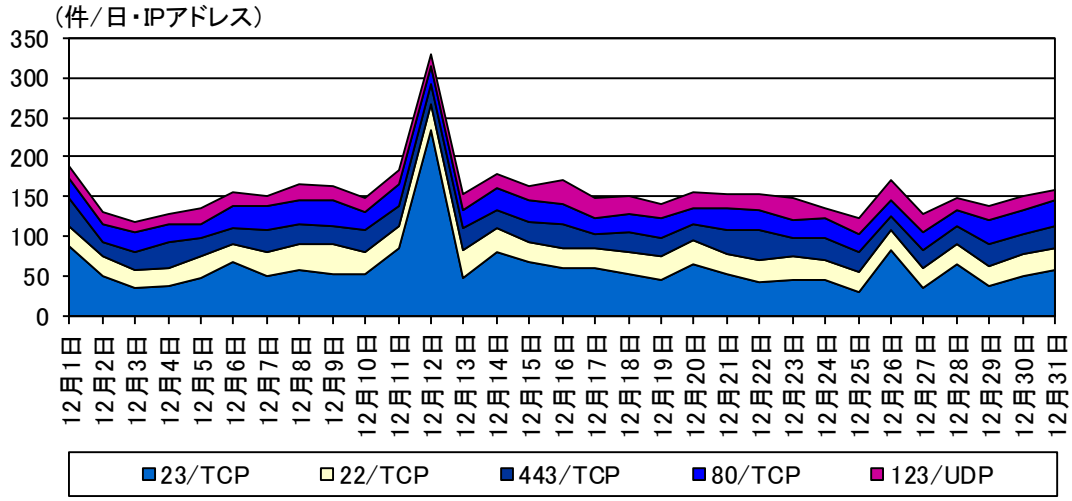

図 3-12　米国からの上位5ポートの検知件数の推移

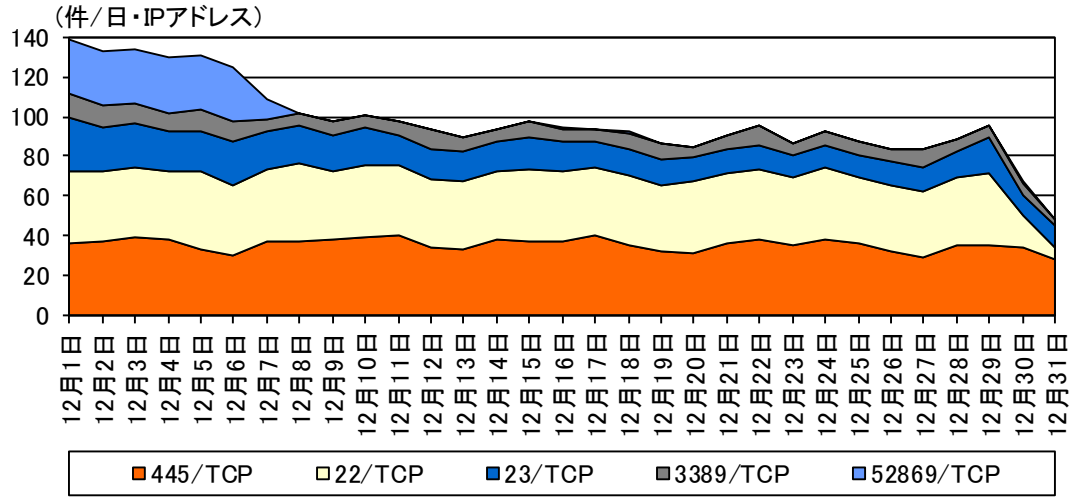

図 3-13　ロシアからの上位5ポートの検知件数の推移

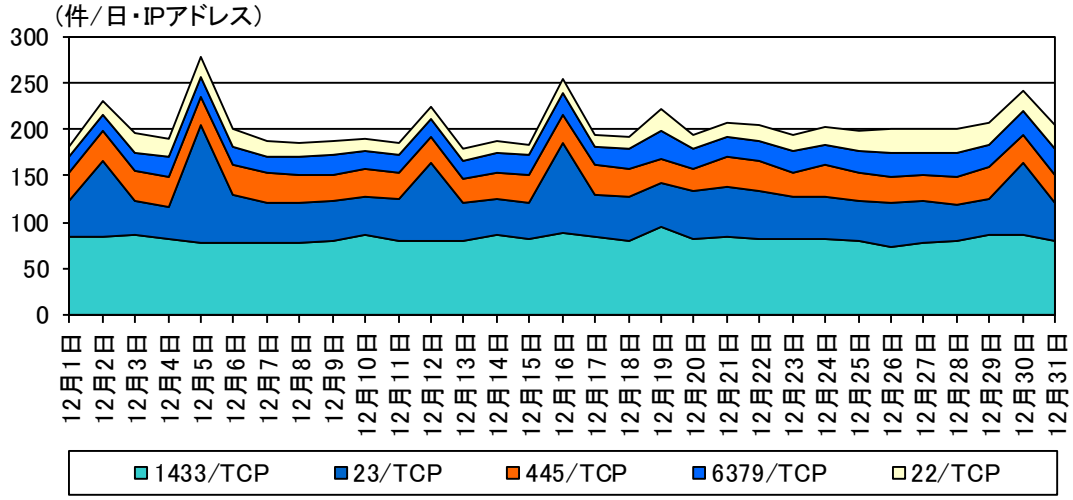

図 3-14　中国からの上位5ポートの検知件数の推移

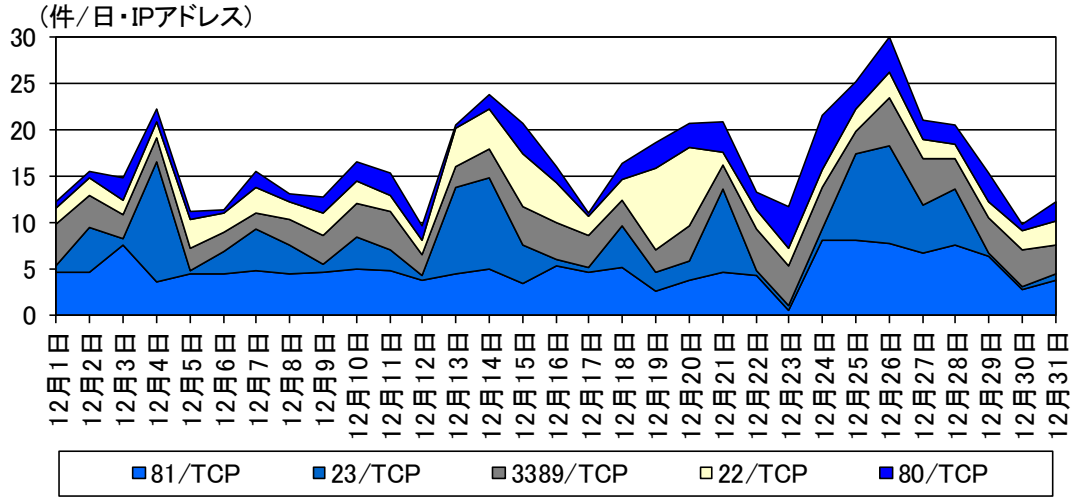

図 3-15　ドイツからの上位5ポートの検知件数の推移

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	569.65 件	＋4.8%　（＋25.92 件）	1 位	
2 位	2 位	Microsoft Windows Terminal server	186.92 件	－27.8%　（－71.89 件）		1 位
3 位	3 位	SMBv1	166.75 件	＋10.6%　（＋15.96 件）	2 位	
4 位	4 位	SERVER-APACHE	47.06 件	＋1.4%　（＋0.64 件）		
5 位	5 位	ICMP	25.54 件	－12.1%　（－3.53 件）		4 位

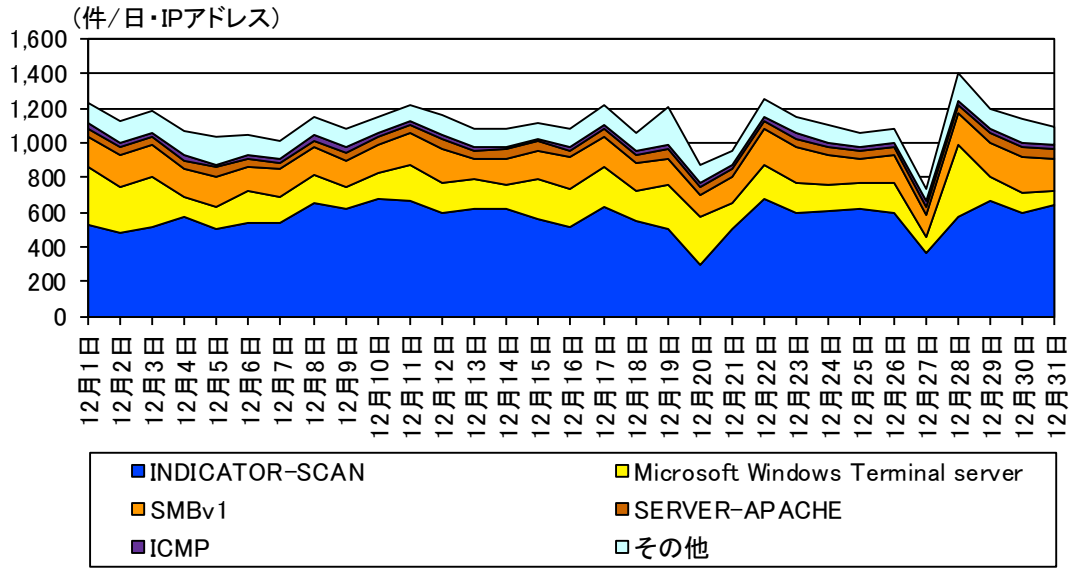

図 4-1　不正侵入等の攻撃手法別検知件数の推移

[i] 一日・1IP アドレス当たり。

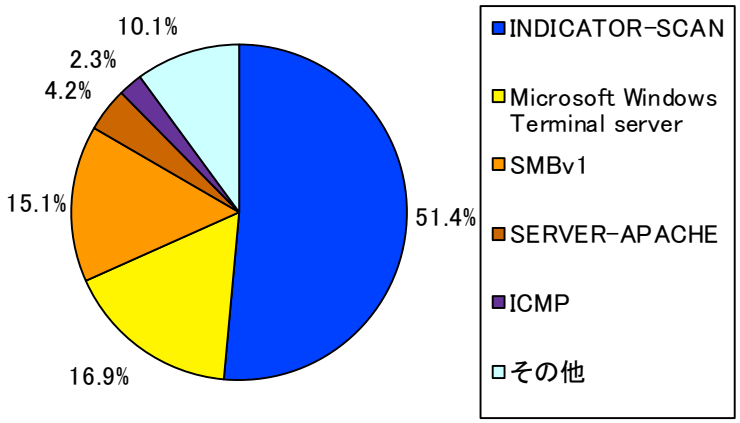

図 4-2 不正侵入等の攻撃手法別検知比率

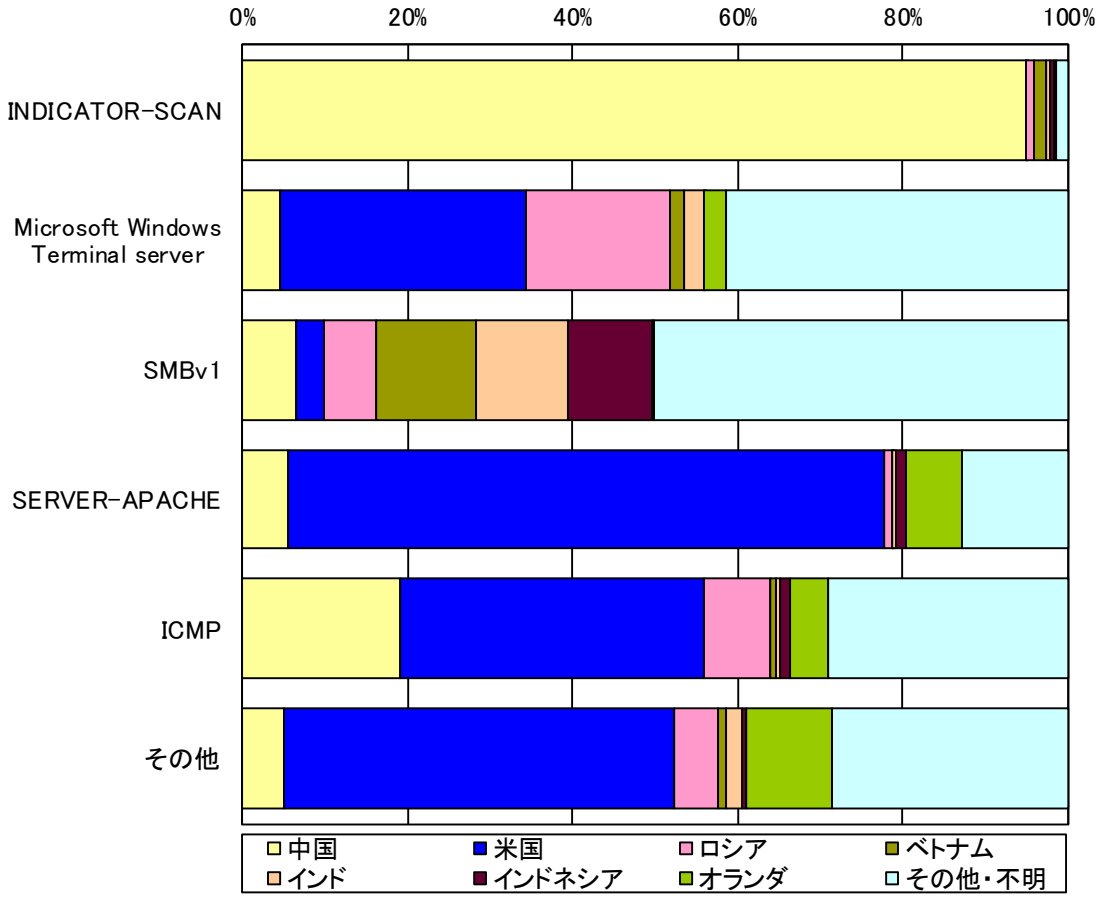

図 4-3 不正侵入等の攻撃手法の送信元国・地域別検知比率

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	572.95 件	＋0.6% （＋3.42 件）
2 位	2 位	米国	158.51 件	＋24.6% （＋31.33 件）
3 位	3 位	ロシア	57.26 件	－24.1% （－18.14 件）
4 位	6 位	ベトナム	32.90 件	－2.0% （－0.66 件）
5 位	8 位	インド	27.76 件	＋26.8% （＋5.87 件）

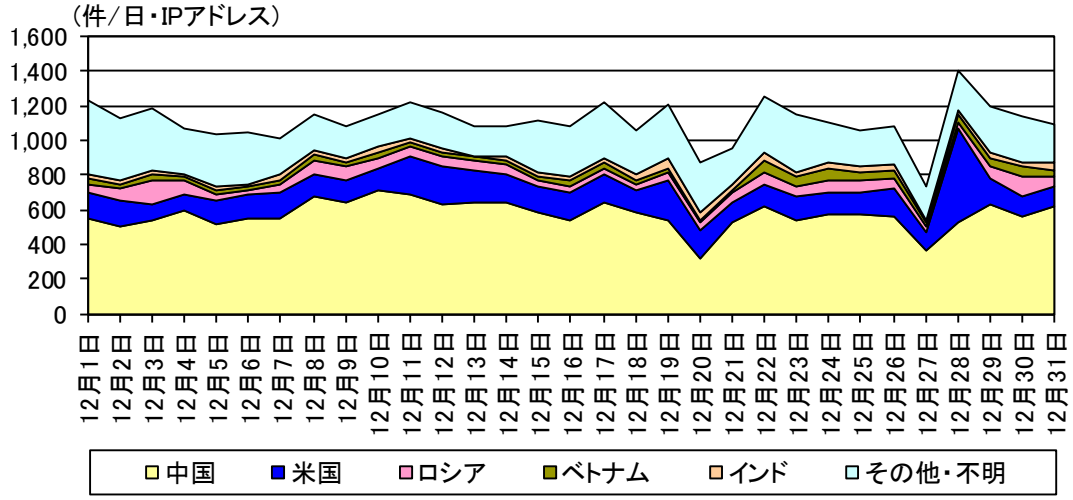

図 4-4 不正侵入等の送信元国・地域別検知件数の推移

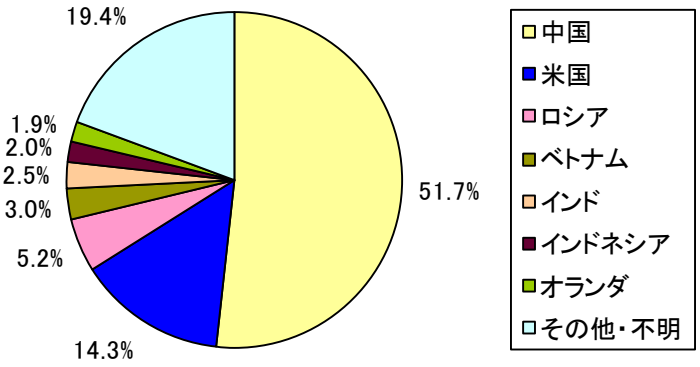

図 4-5 不正侵入等の送信元国・地域別検知比率

[i] 一日・1IP アドレス当たり。

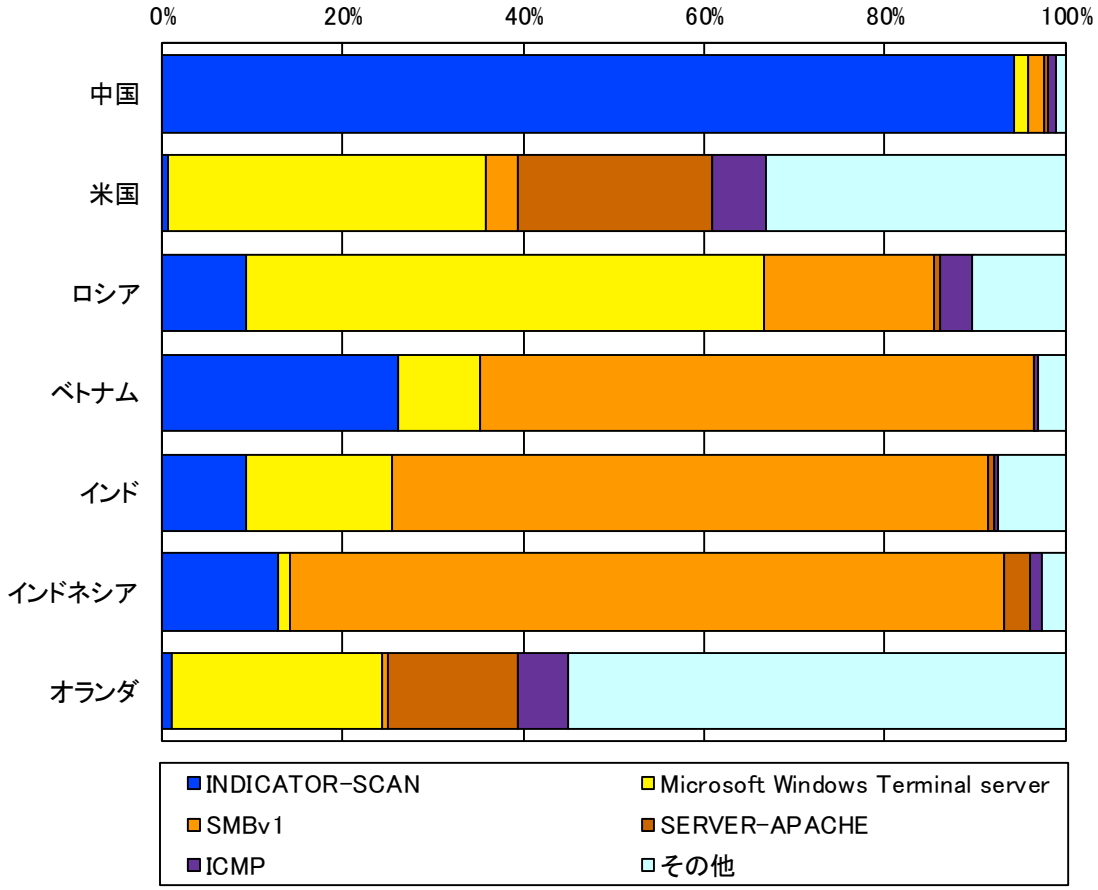

図 4-6 不正侵入等の送信元国・地域別上位の攻撃手法別検知比率

5　DoS 攻撃被害の観測結果

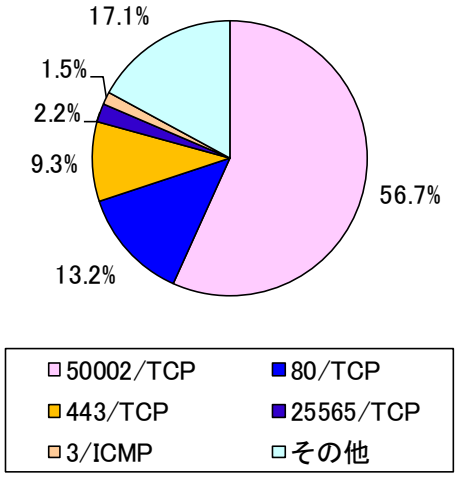

図 5-1　跳ね返りパケット送信元ポート別比率

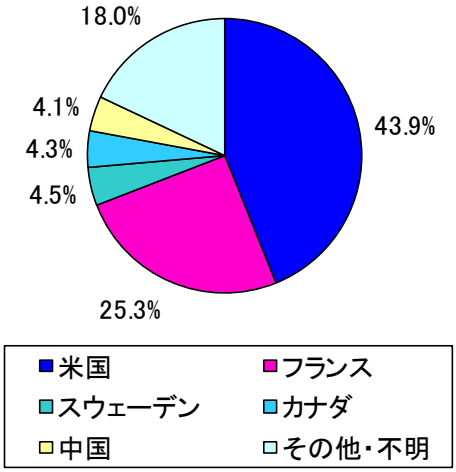

図 5-2　跳ね返りパケット送信元国・地域別比率