令 和 2年 6月 5日

令和2年4月期観測資料

1　観測結果概要

令和2年4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 5,506.6 件で、令和2年3月期(以下「前月期」という。)と比較して 94.9 件(1.8%)増加しました。また、送信元 IP アドレス[i] 数は、一日当たり 48,028.2 個で、前月期と比較して 4,370.9 個(8.3%)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 928.1 件で、前月期と比較して 223.8 件(31.8%)増加しました。また、送信元 IP アドレス数は、一日当たり 8,152.1 個で、前月期と比較して 39.6 個(0.5%)減少しました。

DoS 攻撃被害検知件数は、一日当たり 29,633.6 件で、前月期と比較して 29,285.4 件(49.7%)減少しました。また、送信元 IP アドレス数は、一日当たり 4,550.2 個で、前月期と比較して 5,961.2 個(56.7%)減少しました。

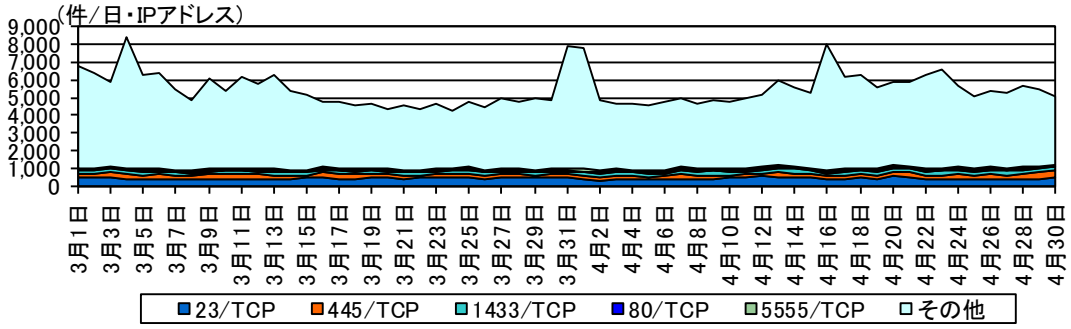

図 1-1　宛先ポート別検知件数の推移

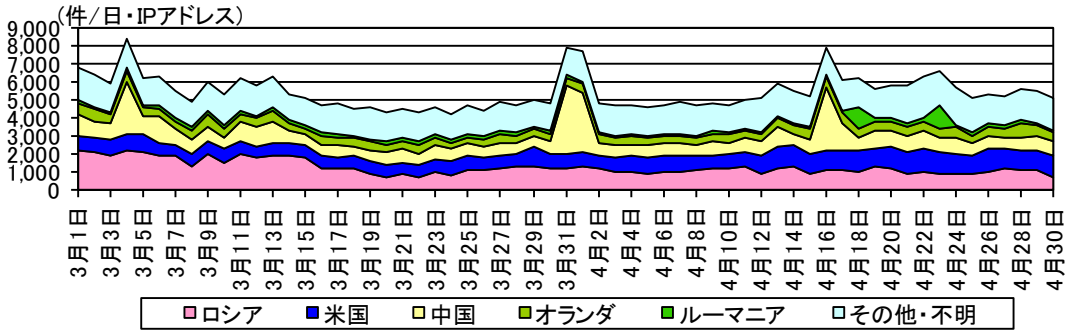

図 1-2　送信元国・地域別検知件数の推移[ii]

[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。

2　センサーにおけるアクセス検知の観測結果

2-1　宛先ポート別アクセス検知件数

表 2-1　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	450.54 件	－1.4%　（－6.54 件）
2 位	2 位	445/TCP	228.91 件	＋2.1%　（＋4.79 件）
3 位	3 位	1433/TCP	195.27 件	＋8.7%　（＋15.63 件）
4 位	4 位	80/TCP	85.52 件	＋10.5%　（＋8.10 件）
5 位	6 位	5555/TCP	79.05 件	＋28.4%　（＋17.49 件）

表 2-2　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	5555/TCP	79.05 件	＋28.4%　（＋17.49 件）	5 位	6 位
2 位	52869/TCP	62.03 件	＋35.9%　（＋16.37 件）	7 位	10 位
3 位	1433/TCP	195.27 件	＋8.7%　（＋15.63 件）	3 位	3 位
4 位	53413/UDP	37.14 件	＋61.3%　（＋14.11 件）	13 位	18 位
5 位	8089/TCP	17.16 件	＋227.7%　（＋11.92 件）	22 位	64 位

表 2-3　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	22079/UDP	検知なし	－　（－16.70 件）	－	28 位
2 位	1723/TCP	5.46 件	－75.0%　（－16.41 件）	63 位	20 位
3 位	37215/TCP	7.61 件	－65.1%　（－14.17 件）	49 位	21 位
4 位	139/TCP	15.93 件	－45.1%　（－13.06 件）	24 位	15 位
5 位	23/TCP	450.54 件	－1.4%　（－6.54 件）	1 位	1 位

[i] 一日・1IP アドレス当たり。

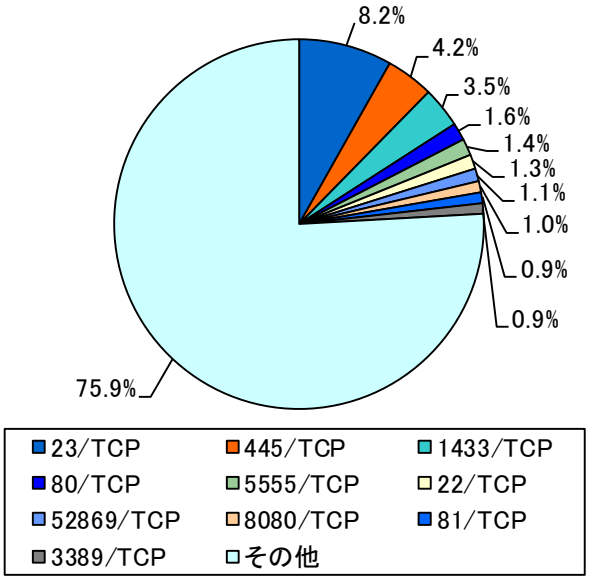

図 2-1　宛先ポート別比率（全て）[i]

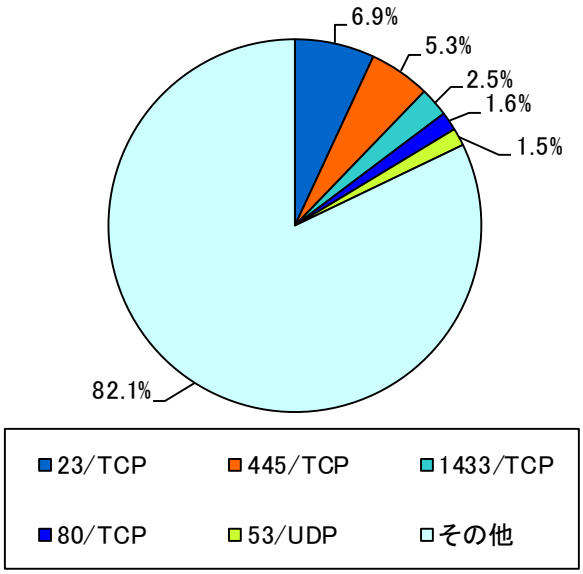

図 2-2　宛先ポート別比率（日本国内）

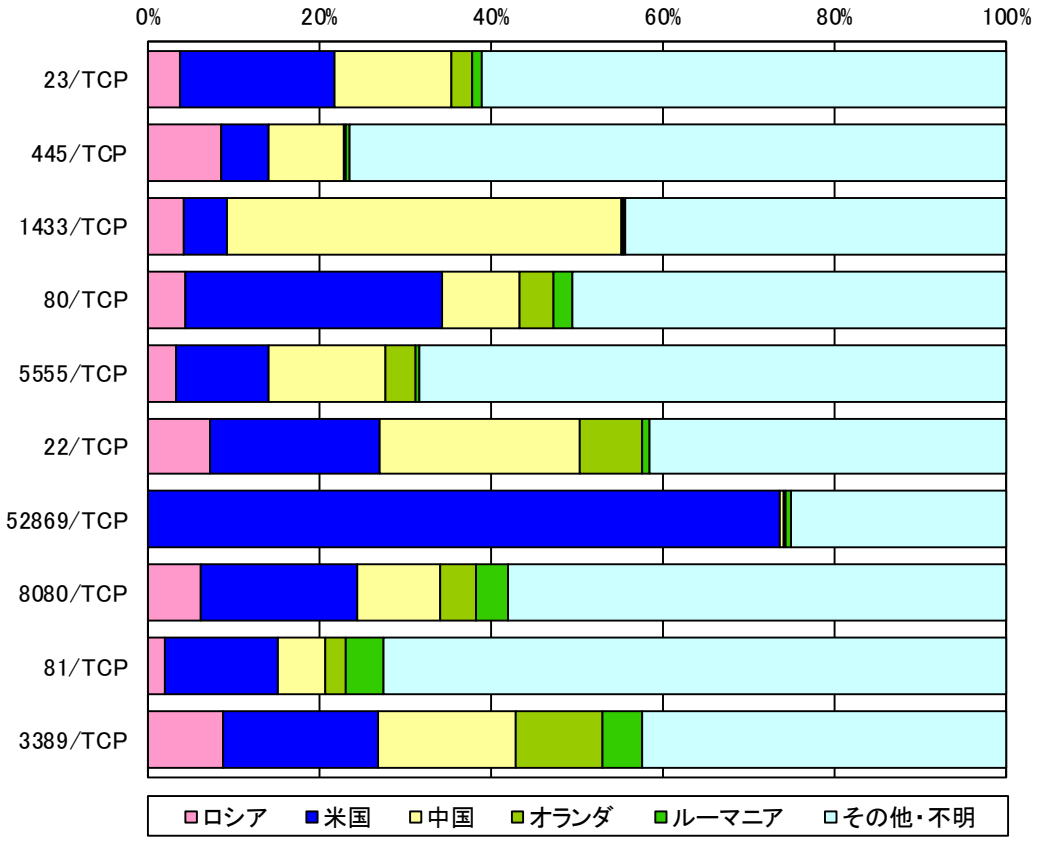

図 2-3　宛先ポート別上位の送信元国・地域別比率

[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。

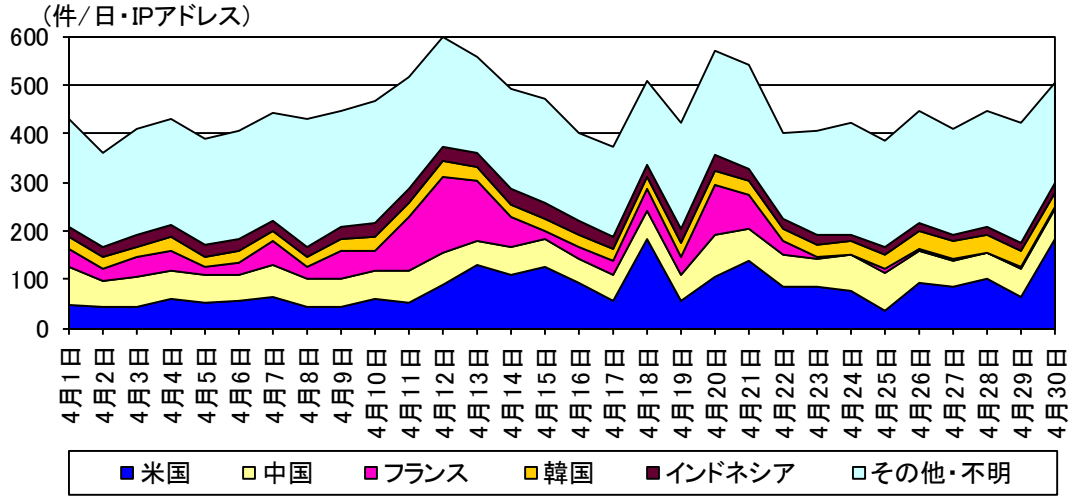

図 2-4　センサーのポート 23/TCP における検知件数の推移

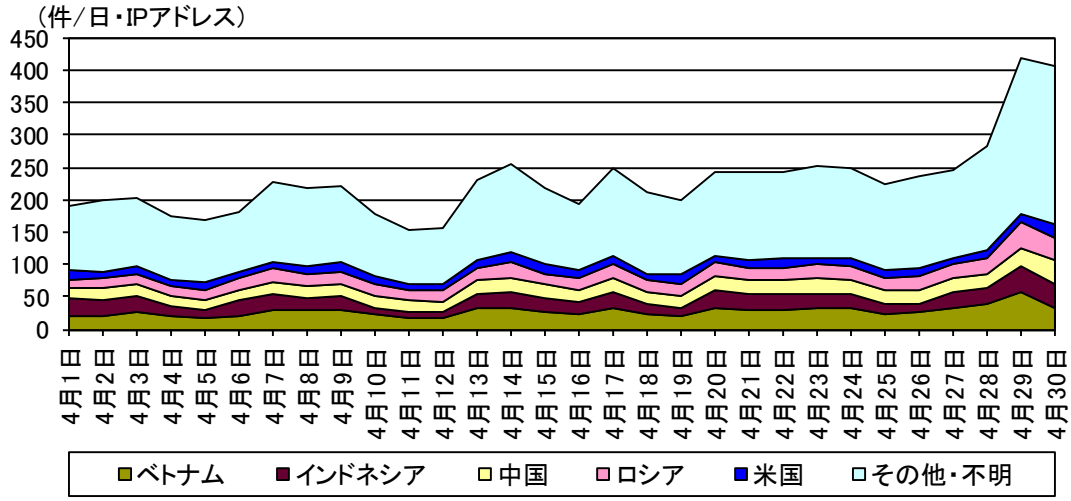

図 2-5　センサーのポート 445/TCP における検知件数の推移

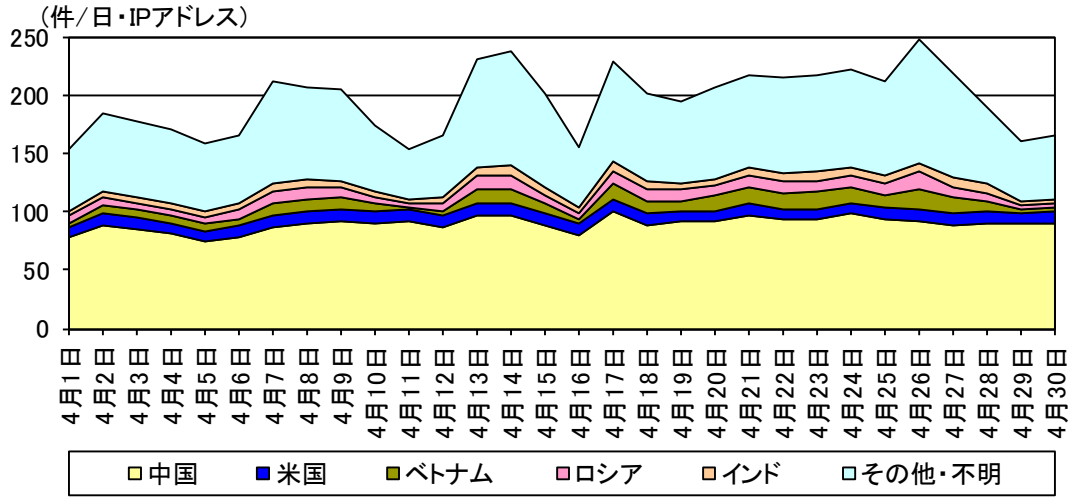

図 2-6　センサーのポート 1433/TCP における検知件数の推移

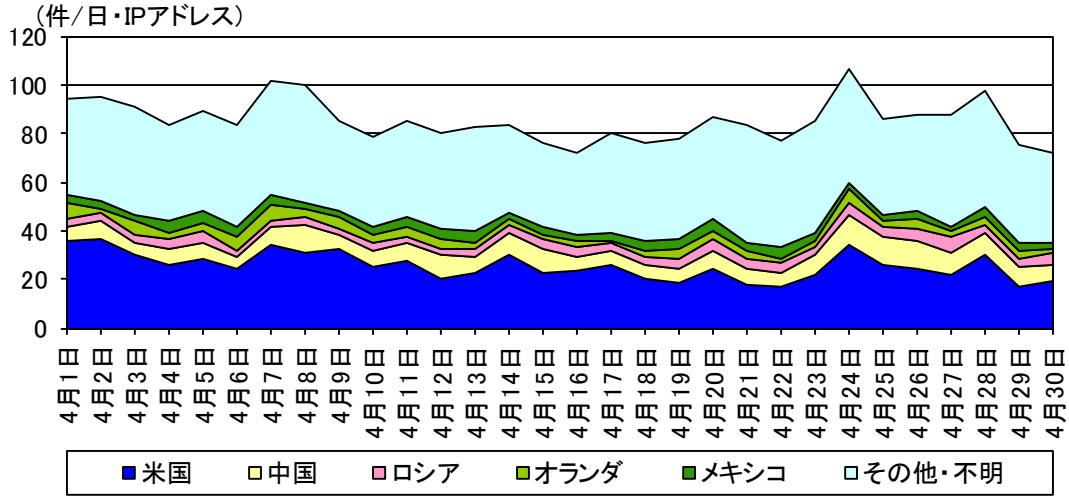

図 2-7　センサーのポート 80/TCP における検知件数の推移

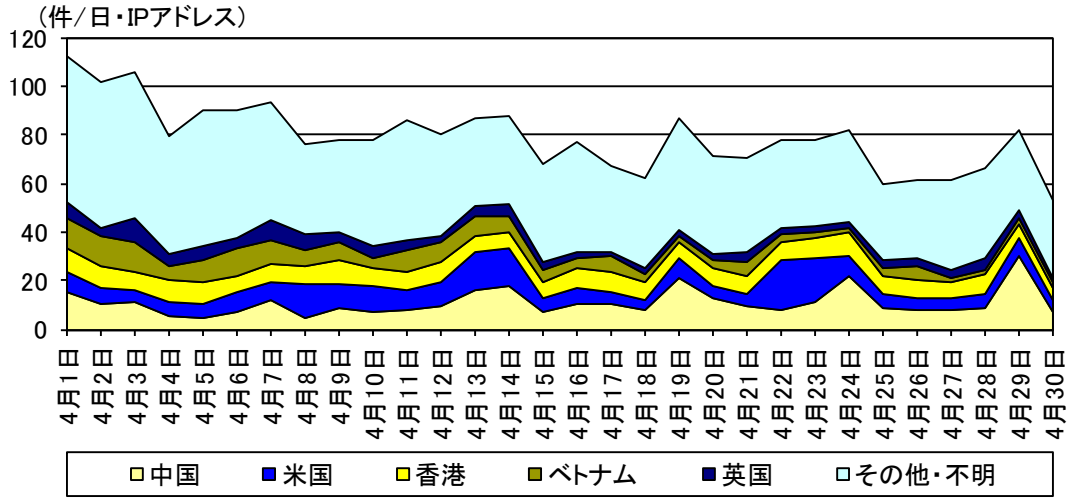

図 2-8　センサーのポート 5555/TCP における検知件数の推移

2-2　送信元国・地域別アクセス検知件数

表 2-4　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	1,092.09 件	－27.0%　（－404.72 件）
2 位	3 位	米国	1,031.17 件	＋38.3%　（＋285.51 件）
3 位	2 位	中国	958.57 件	－0.1%　（－0.82 件）
4 位	4 位	オランダ	489.76 件	＋4.3%　（＋19.99 件）
5 位	5 位	ルーマニア	200.32 件	＋17.1%　（＋29.32 件）

表 2-5　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	1,031.17 件	＋38.3%　（＋285.51 件）	2 位	3 位
2 位	ドイツ	97.04 件	＋122.0%　（＋53.32 件）	9 位	19 位
3 位	ブルガリア	71.58 件	＋86.1%　（＋33.12 件）	12 位	20 位
4 位	ルーマニア	200.32 件	＋17.1%　（＋29.32 件）	5 位	5 位
5 位	フランス	142.08 件	＋22.2%　（＋25.83 件）	7 位	8 位

表 2-6　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	1,092.09 件	－27.0%　（－404.72 件）	1 位	1 位
2 位	エストニア	62.04 件	－28.8%　（－25.13 件）	13 位	10 位
3 位	台湾	57.11 件	－29.1%　（－23.42 件）	16 位	11 位
4 位	スイス	1.08 件	－94.9%　（－19.94 件）	81 位	27 位
5 位	日本	36.36 件	－28.5%　（－14.46 件）	21 位	15 位

[i] 一日・1IP アドレス当たり。

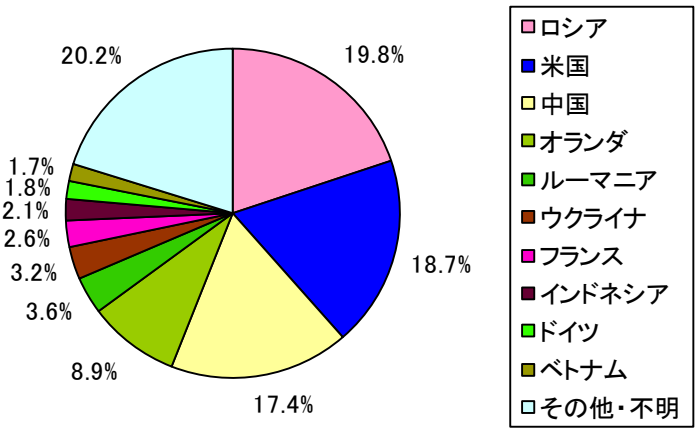

図 2-9　送信元国・地域別比率

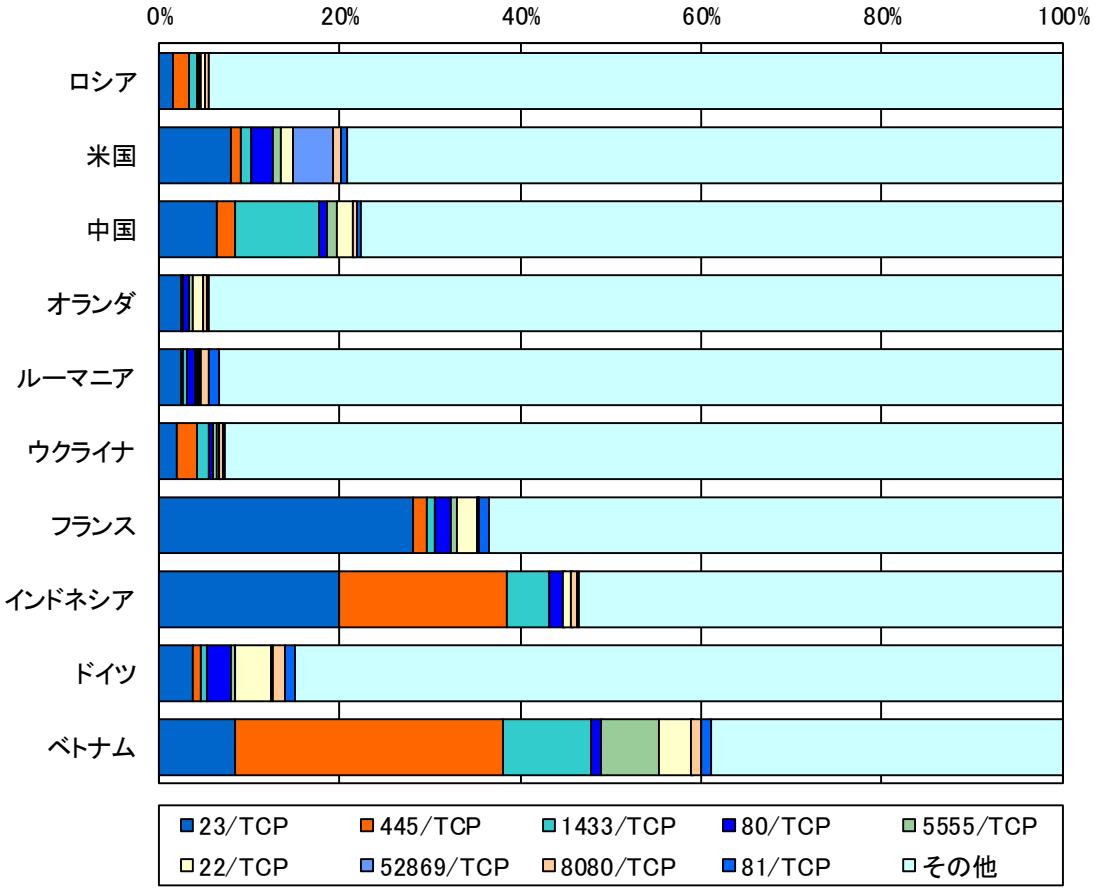

図 2-10　送信元国・地域別上位の宛先ポート別比率

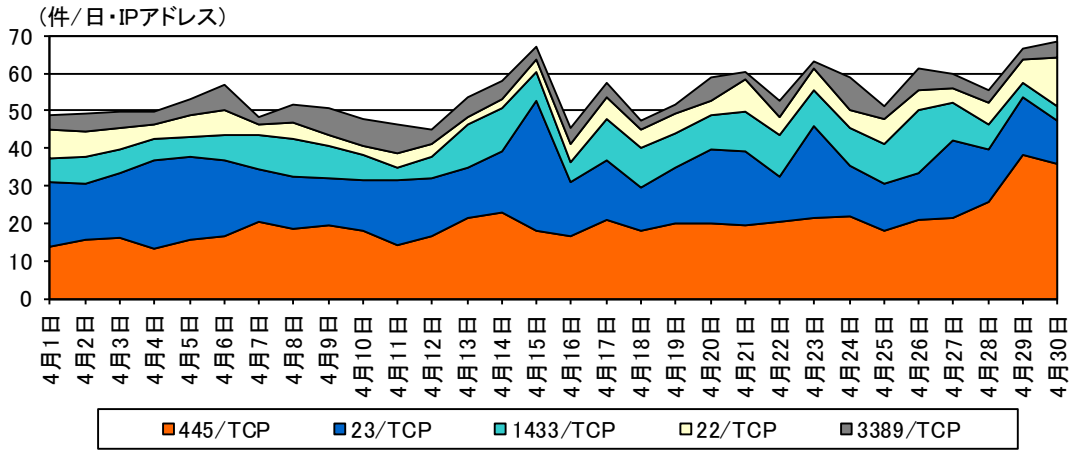

図 2-11　ロシアからの上位5ポートの検知件数の推移

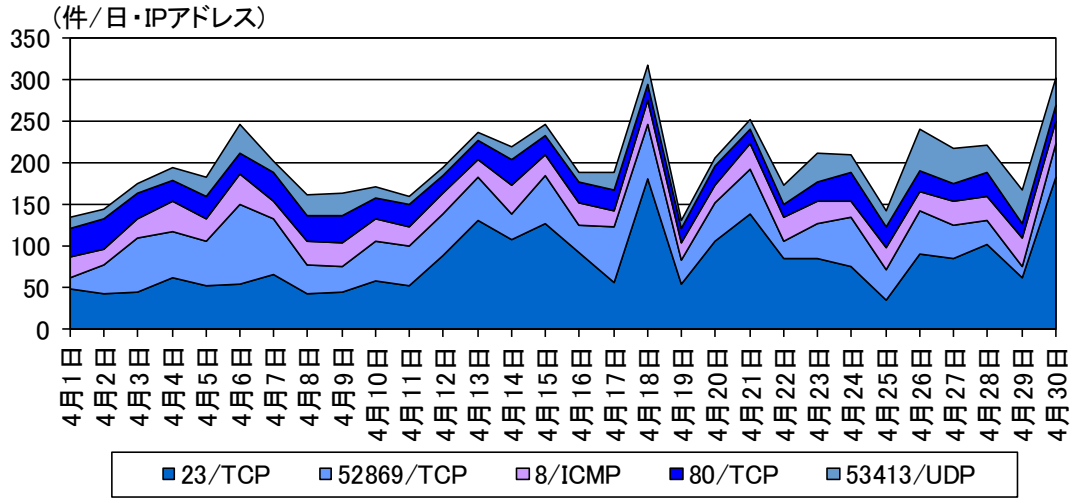

図 2-12　米国からの上位5ポートの検知件数の推移

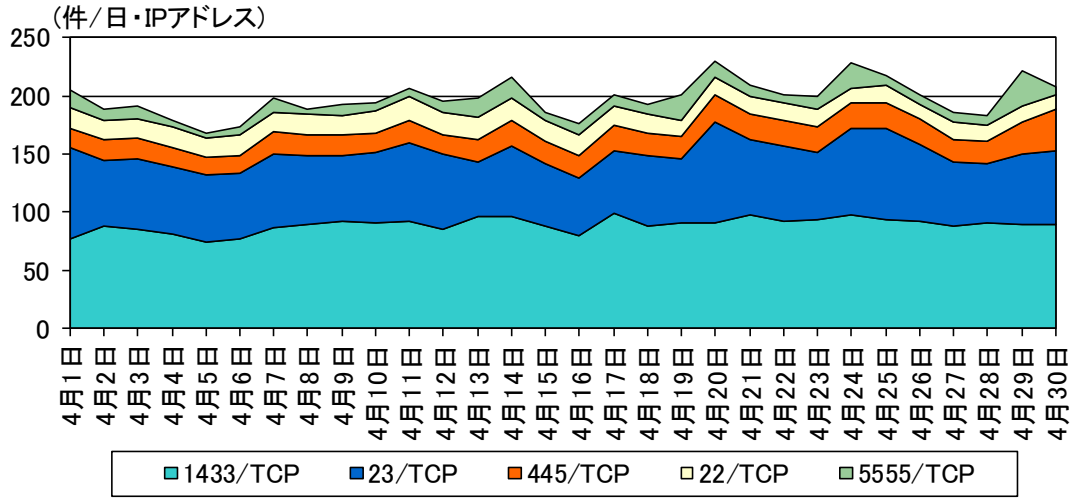

図 2-13　中国からの上位5ポートの検知件数の推移

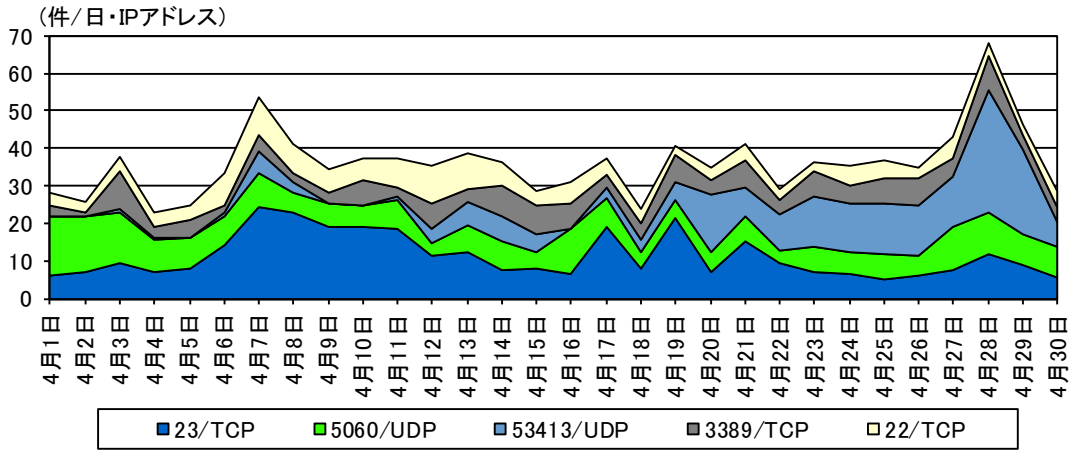

図 2-14　オランダからの上位5ポートの検知件数の推移

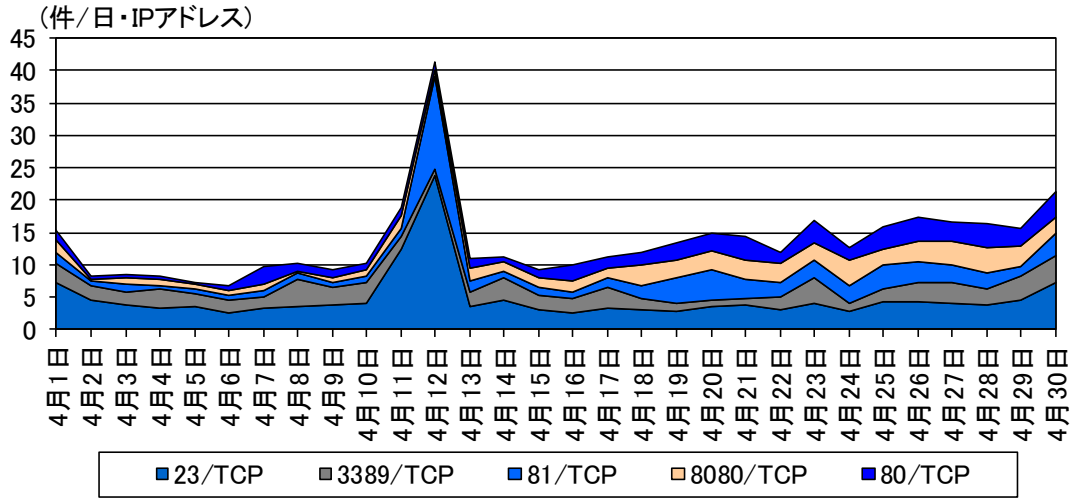

図 2-15　ルーマニアからの上位5ポートの検知件数の推移

3　不正侵入等の観測結果

3-1　攻撃手法別アクセス検知件数

表 3-1　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	Microsoft Windows Terminal server	325.08 件	＋93.1%　（＋156.78 件）	1 位	
2 位	1 位	INDICATOR-SCAN	238.97 件	－8.3%　（－21.72 件）		1 位
3 位	3 位	SMBv1	101.64 件	－4.5%　（－4.78 件）		2 位
4 位	12 位	Remote Desktop	98.98 件	－ [ii]　（＋91.57 件）	2 位	
5 位	4 位	ICMP	30.89 件	＋15.0%　（＋4.02 件）	5 位	

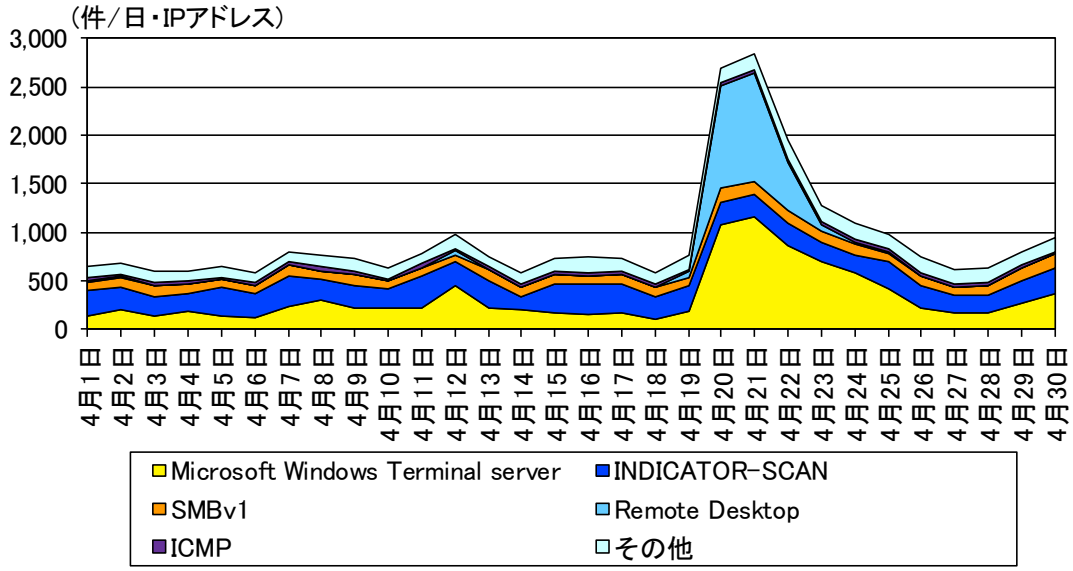

図 3-1　不正侵入等の攻撃手法別検知件数の推移

[i] 一日・1IP アドレス当たり。

[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。

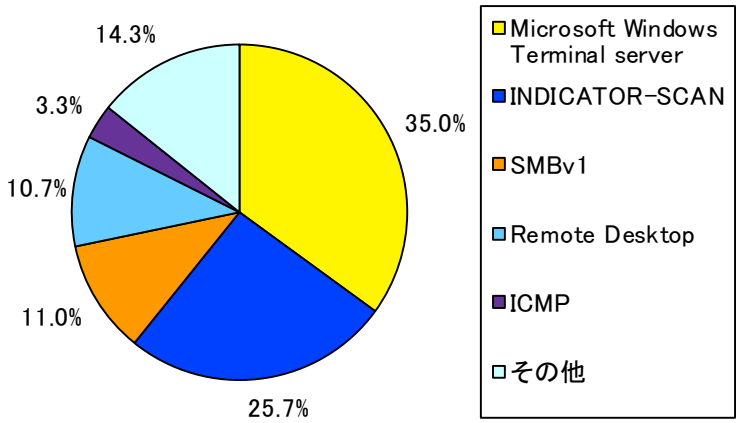

図 3-2 不正侵入等の攻撃手法別検知比率

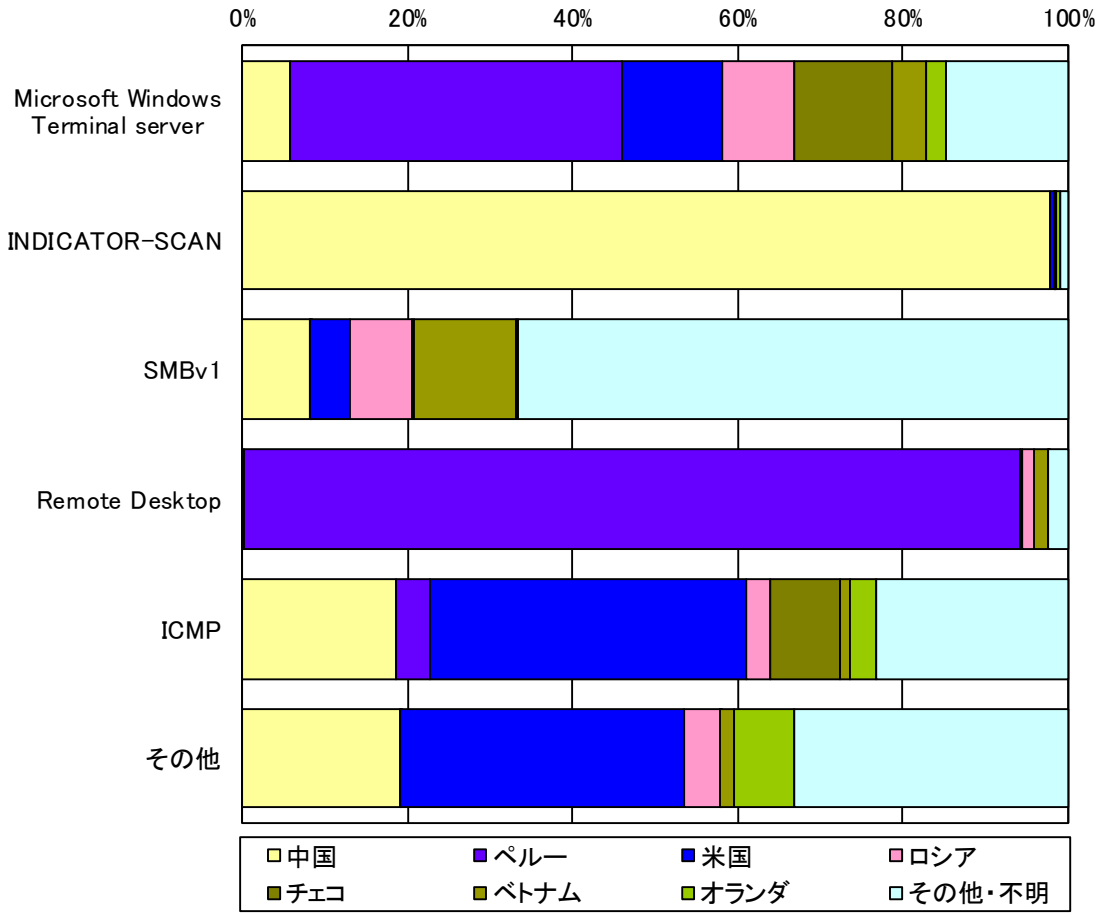

図 3-3 不正侵入等の攻撃手法の国・地域別検知比率

3-2 送信元国・地域別アクセス検知件数

表 3-2 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	291.93 件	－7.5% （－23.81 件）
2 位	63 位	ペルー	225.62 件	－ [ii] （＋225.41 件）
3 位	2 位	米国	102.82 件	＋14.4% （＋12.92 件）
4 位	3 位	ロシア	44.64 件	－46.9% （－39.39 件）
5 位	24 位	チェコ	41.53 件	－ [ii] （＋38.46 件）

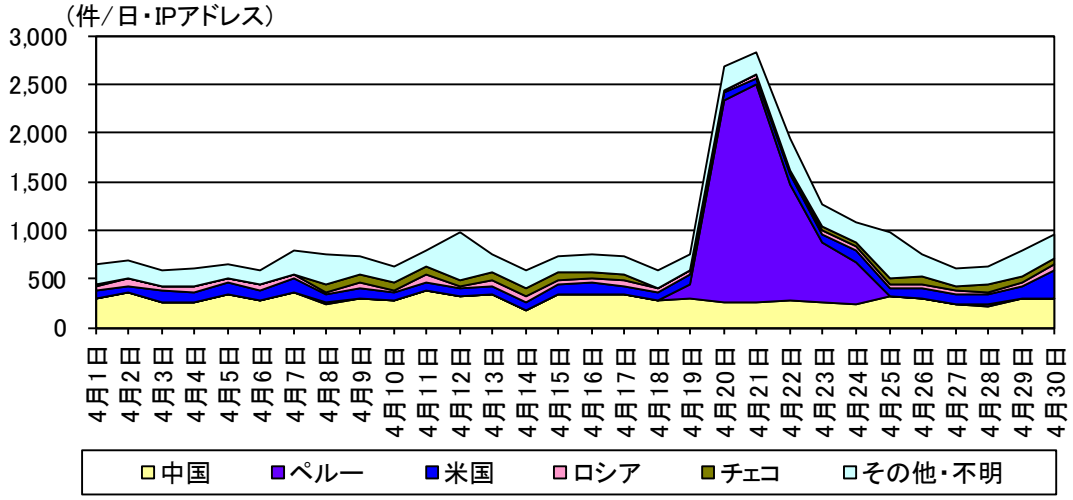

図 3-4 不正侵入等の送信元国・地域別検知件数の推移

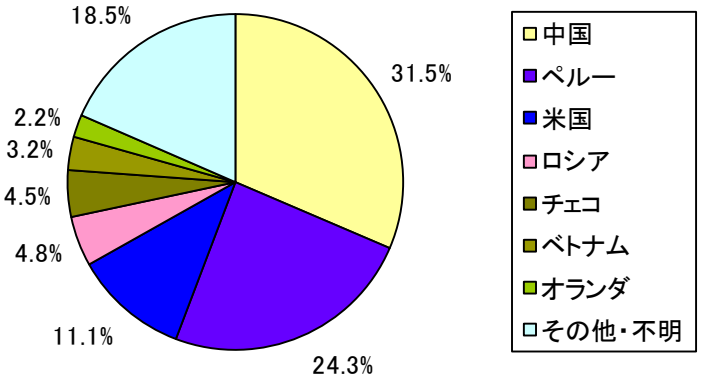

図 3-5 不正侵入等の送信元国・地域別検知比率

[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。

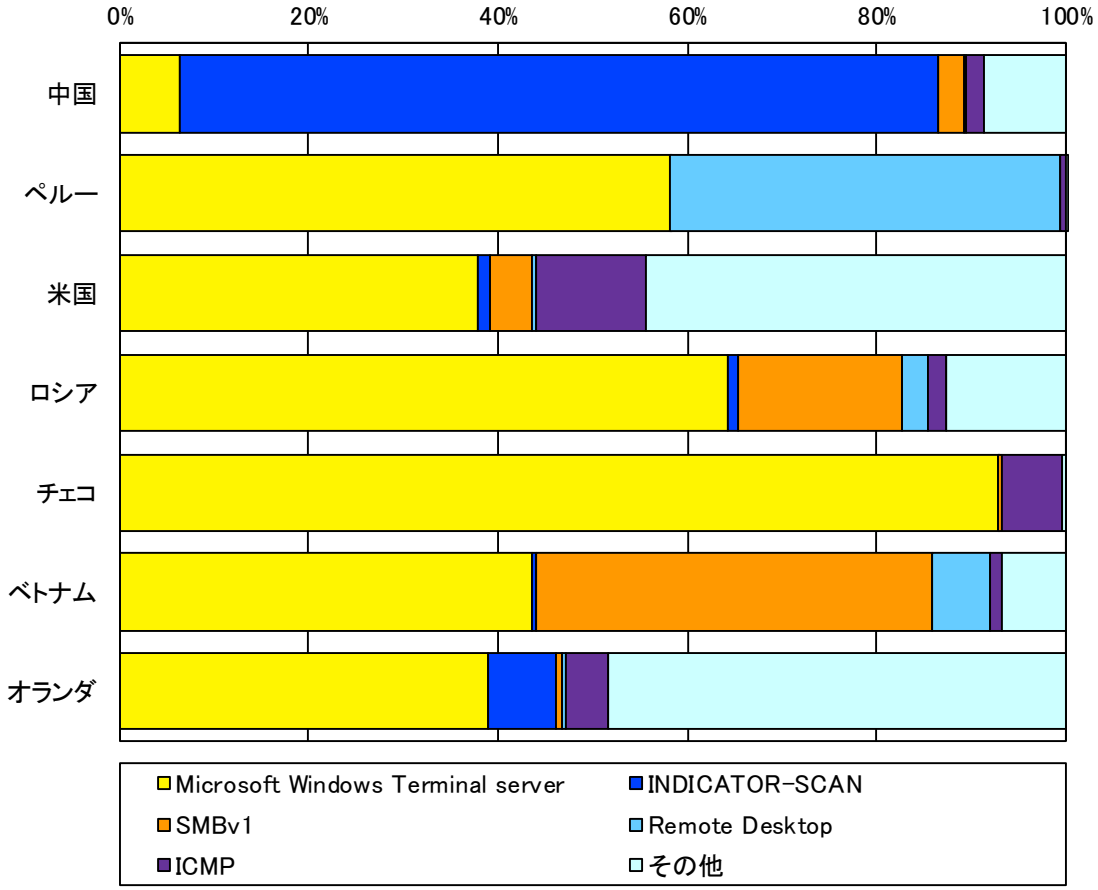

図 3-6 不正侵入等の送信元国・地域別上位の攻撃手法別検知比率

4　DoS 攻撃被害の観測結果

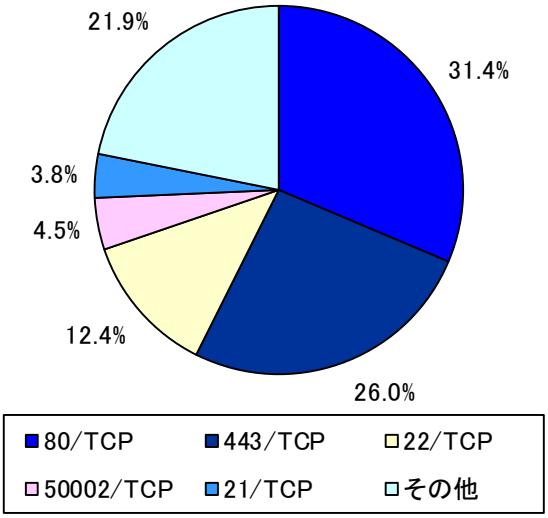

図 4-1　跳ね返りパケット送信元ポート別比率

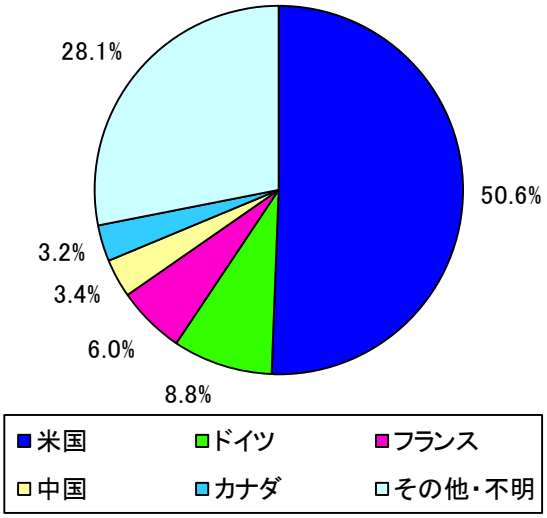

図 4-2　跳ね返りパケット送信元国・地域別比率

5　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。

5-1　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。）。

5-2　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 5-1 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 5-1　パケットの分類

章	集計対象	
2 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
4 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

5-3　不正侵入等の検知

検知された各シグネチャ は、表 5-2 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 5-2 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-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