令和２年 10 月 16 日

令和2年9月期観測資料

1　観測結果概要

令和2年9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 6,588.0 件で、令和2年8月期（以下「前月期」という。）の 5,476.5 件と比較して 1,111.5 件（20.3%）増加しました。また、送信元 IP アドレス[i] 数は、一日当たり 56,165.9 個で、前月期の 46,146.9 個と比較して 10,019.1 個（21.7%）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 1,088.1 件で、前月期の 791.1 件と比較して 297.0 件（37.5%）増加しました。また、送信元 IP アドレス数は、一日当たり 10,633.1 個で、前月期の 9,467.3 個と比較して 1,165.8 個（12.3%）増加しました。

DoS 攻撃被害検知件数は、一日当たり27,735.5 件で、前月期の 12,171.8 件と比較して 15,563.6 件（127.9%）増加しました。また、送信元 IP アドレス数は、一日当たり 521.7 個で、前月期の 520.4 個と比較して 1.2 個（0.2%）増加しました。

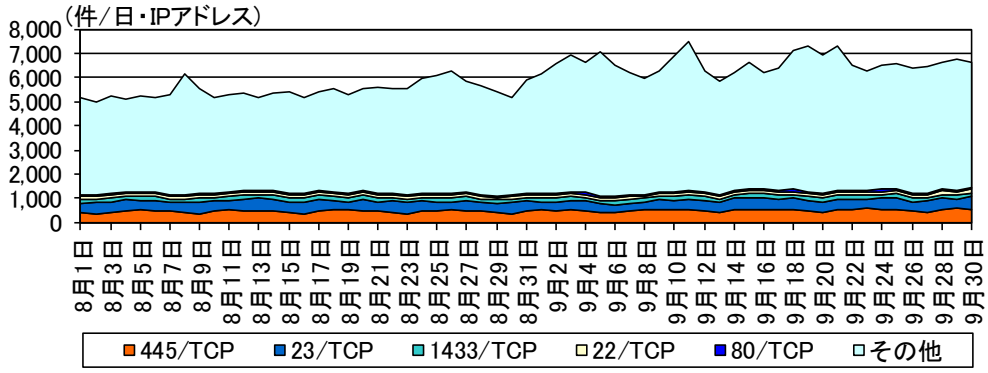

図 1-1　宛先ポート別検知件数の推移

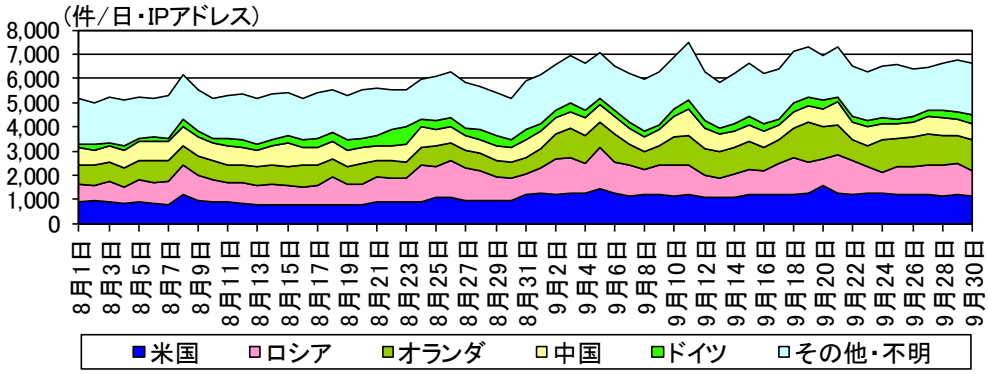

図 1-2　送信元国・地域別検知件数の推移[ii]

[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	514.85 件	＋10.8%　（＋50.05 件）
2 位	2 位	23/TCP	414.32 件	－2.2%　（－9.11 件）
3 位	3 位	1433/TCP	159.20 件	＋1.8%　（＋2.79 件）
4 位	4 位	22/TCP	128.48 件	＋11.7%　（＋13.46 件）
5 位	5 位	80/TCP	72.06 件	＋5.2%　（＋3.54 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	514.85 件	＋10.8%　（＋50.05 件）	1 位	1 位
2 位	8291/TCP	43.49 件	＋73.5%　（＋18.43 件）	10 位	16 位
3 位	22/TCP	128.48 件	＋11.7%　（＋13.46 件）	4 位	4 位
4 位	2323/TCP	23.57 件	＋82.1%　（＋10.63 件）	18 位	28 位
5 位	5060/UDP	49.85 件	＋17.6%　（＋7.46 件）	7 位	10 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	9530/TCP	4.67 件	－89.1%　（－38.33 件）	91 位	9 位
2 位	8/ICMP	44.31 件	－24.7%　（－14.53 件）	9 位	6 位
3 位	23/TCP	414.32 件	－2.2%　（－9.11 件）	2 位	2 位
4 位	6379/TCP	18.03 件	－22.3%　（－5.19 件）	22 位	17 位
5 位	0/TCP	4.56 件	－50.5%　（－4.64 件）	95 位	39 位

[i] 一日・1IP アドレス当たり。

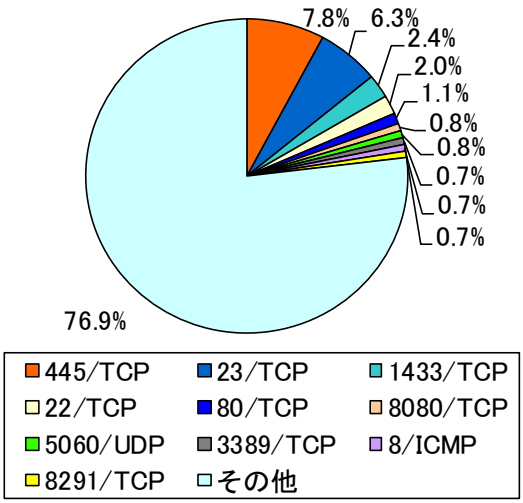

図 3-1　宛先ポート別比率（全て）[i]

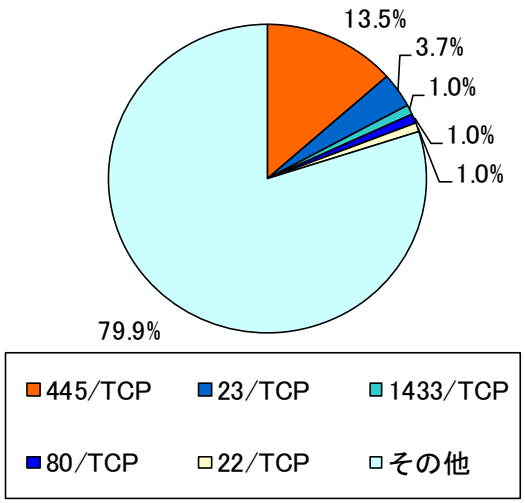

図 3-2　宛先ポート別比率（日本国内）

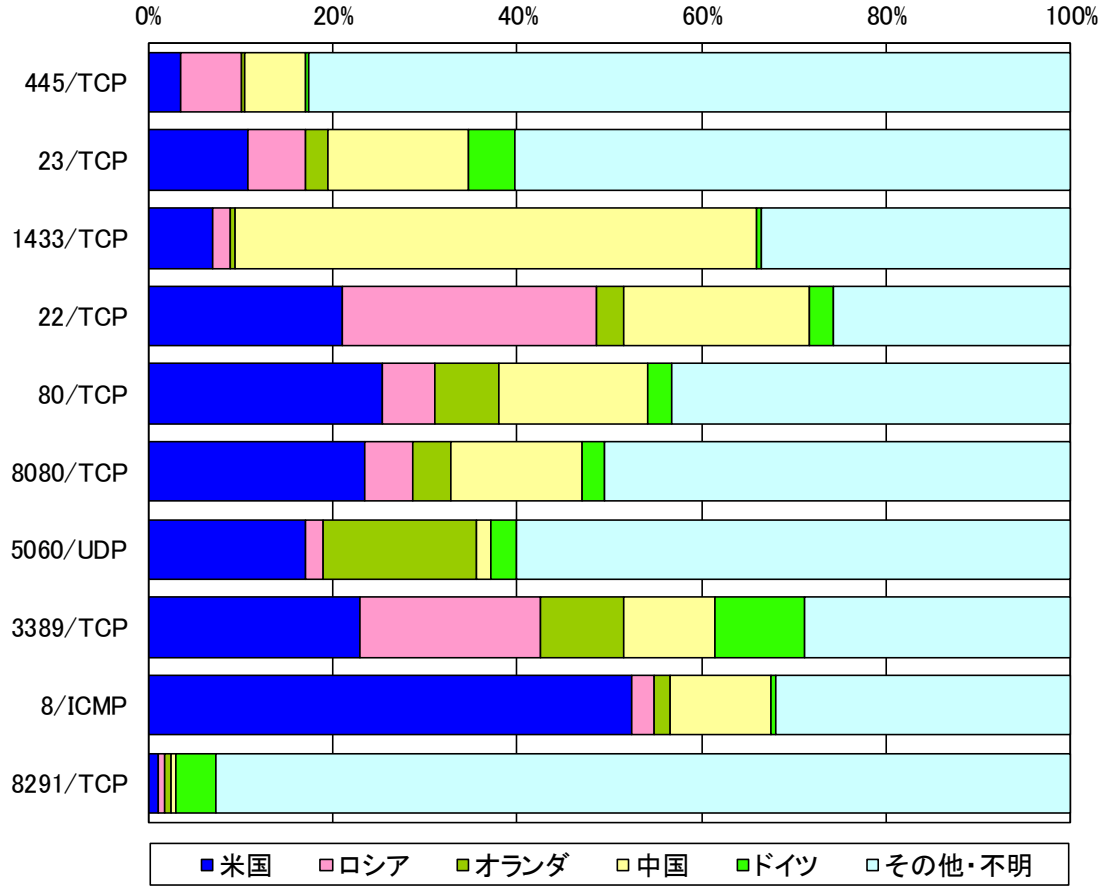

図 3-3　宛先ポート別上位の送信元国・地域別比率

[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。

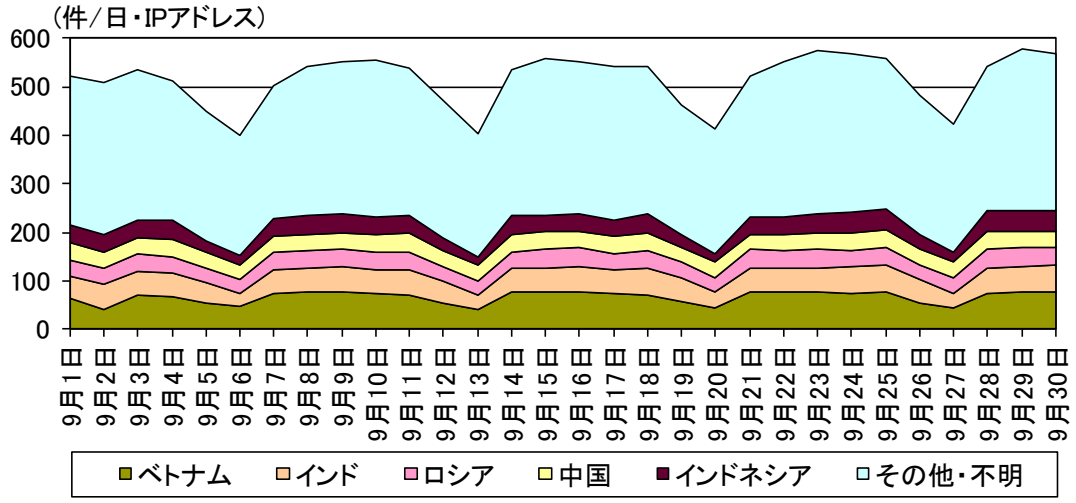

図 3-4　センサーのポート 445/TCP における検知件数の推移

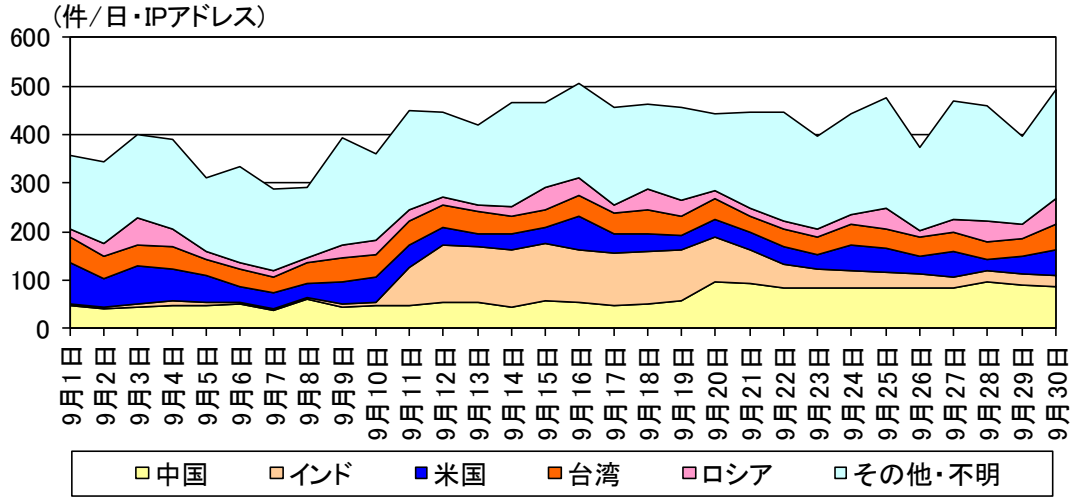

図 3-5　センサーのポート 23/TCP における検知件数の推移

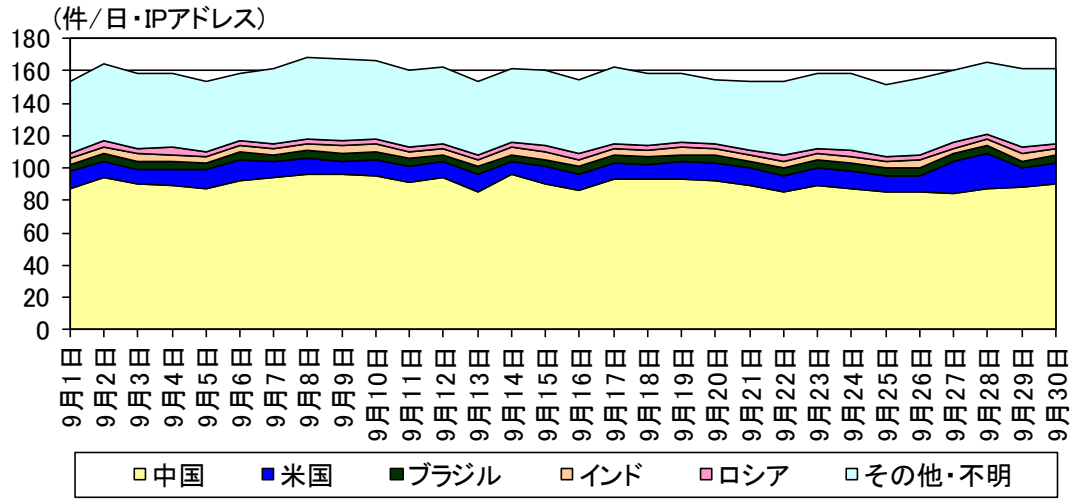

図 3-6　センサーのポート 1433/TCP における検知件数の推移

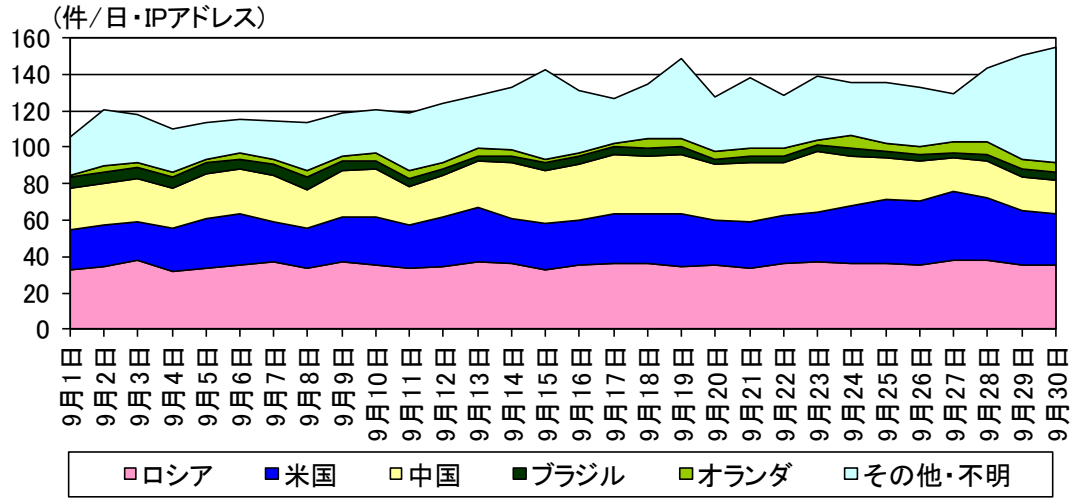

図 3-7　センサーのポート 22/TCP における検知件数の推移

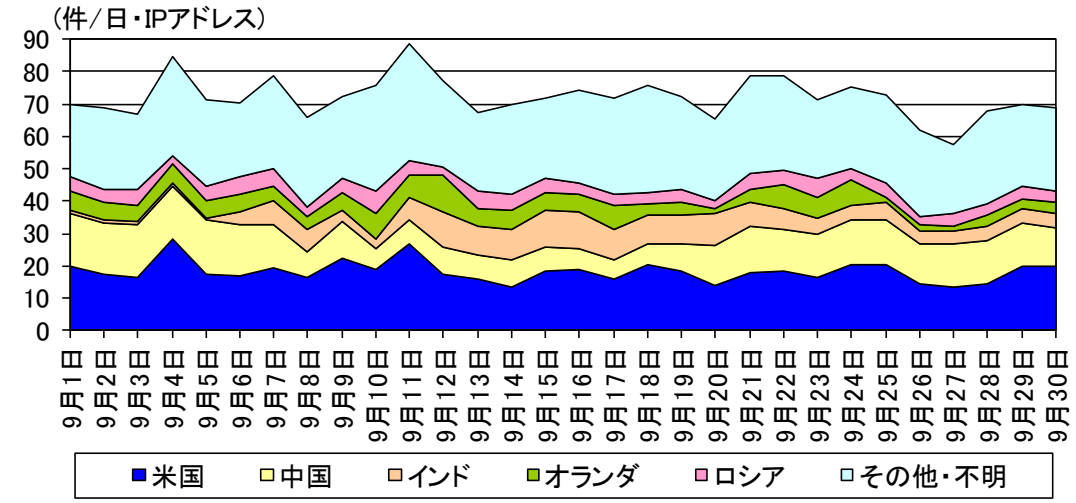

図 3-8　センサーのポート 80/TCP における検知件数の推移

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	2 位	米国	1,227.32 件	＋34.2% （＋312.82 件）
2 位	1 位	ロシア	1,204.07 件	＋26.3% （＋250.64 件）
3 位	3 位	オランダ	1,113.58 件	＋42.7% （＋333.09 件）
4 位	4 位	中国	723.80 件	＋1.9% （＋13.67 件）
5 位	5 位	ドイツ	280.57 件	－12.9% （－41.63 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	1,113.58 件	＋42.7% （＋333.09 件）	3 位	3 位
2 位	米国	1,227.32 件	＋34.2% （＋312.82 件）	1 位	2 位
3 位	ロシア	1,204.07 件	＋26.3% （＋250.64 件）	2 位	1 位
4 位	インド	248.26 件	＋145.6% （＋147.18 件）	6 位	9 位
5 位	ブルガリア	133.59 件	＋139.1% （＋77.71 件）	8 位	17 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	パナマ	25.80 件	－73.7% （－72.14 件）	28 位	11 位
2 位	ドイツ	280.57 件	－12.9% （－41.63 件）	5 位	5 位
3 位	フランス	75.06 件	－35.0% （－40.43 件）	13 位	6 位
4 位	エストニア	14.38 件	－71.3% （－35.77 件）	36 位	19 位
5 位	ルーマニア	81.49 件	－25.6% （－28.03 件）	12 位	8 位

[i] 一日・1IP アドレス当たり。

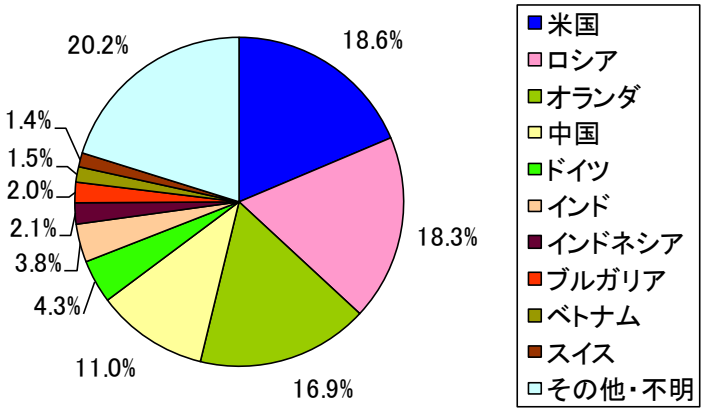

図 3-9　送信元国・地域別比率

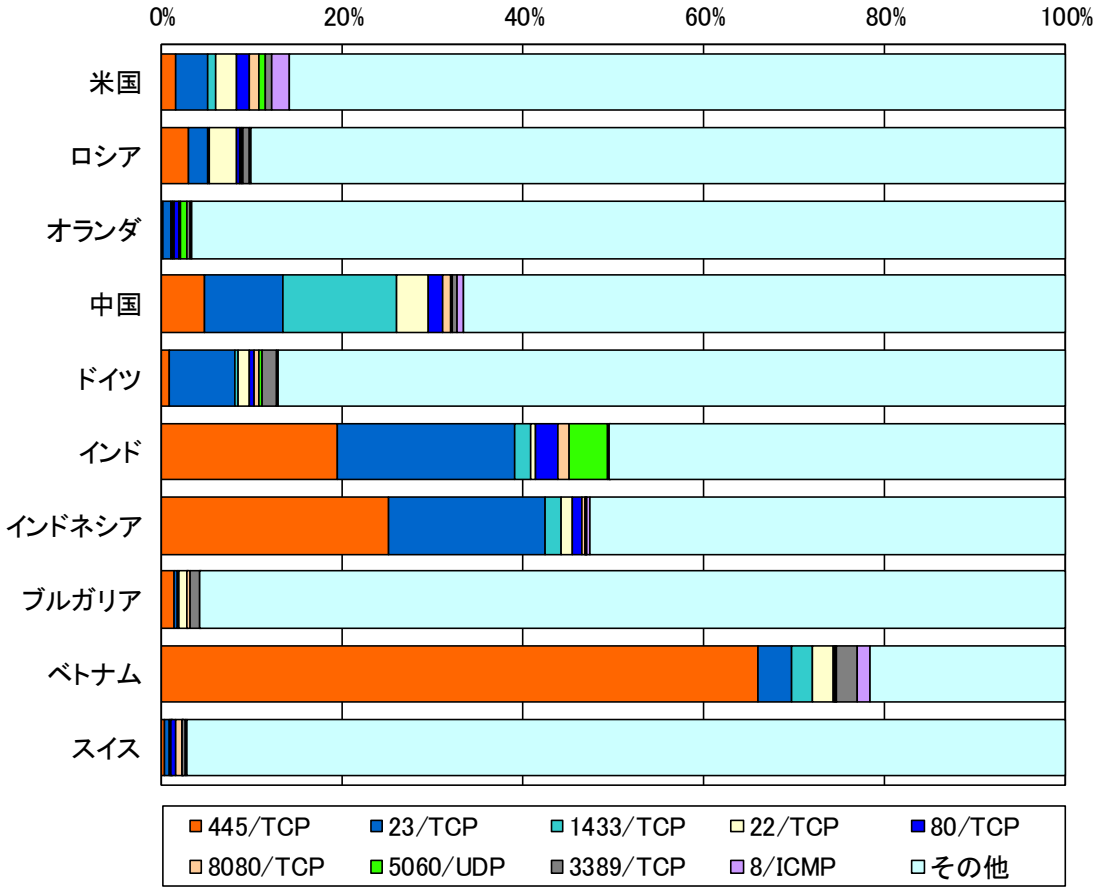

図 3-10　送信元国・地域別上位の宛先ポート別比率

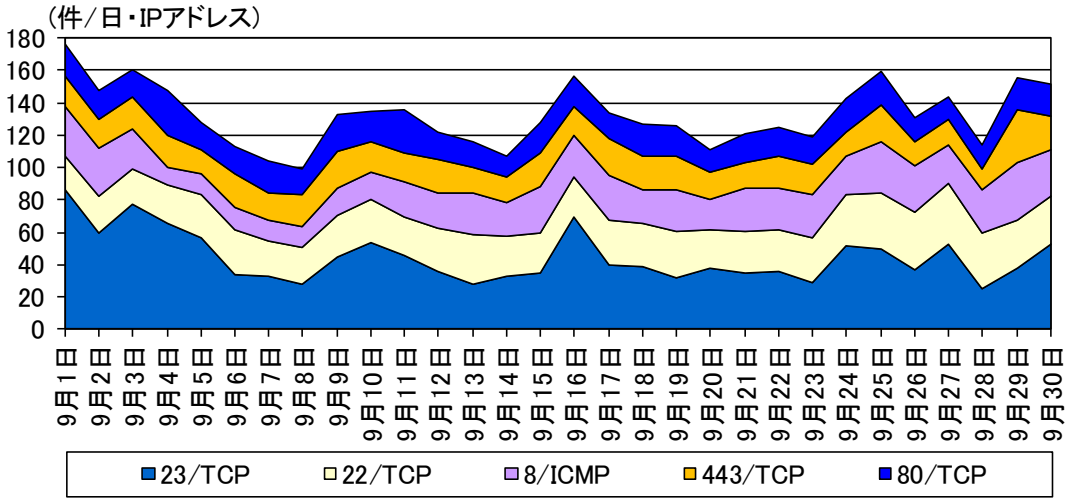

図 3-11　米国からの上位5ポートの検知件数の推移

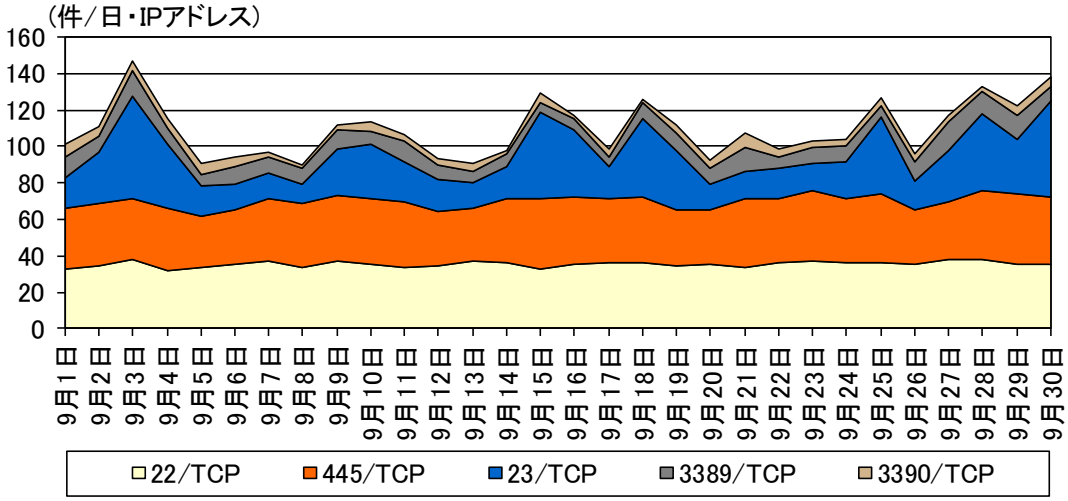

図 3-12　ロシアからの上位5ポートの検知件数の推移

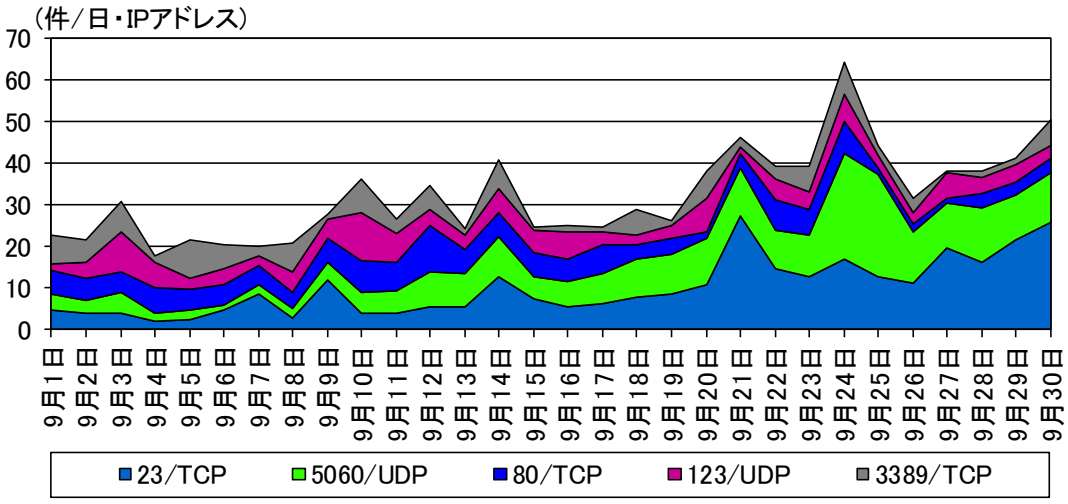

図 3-13　オランダからの上位5ポートの検知件数の推移

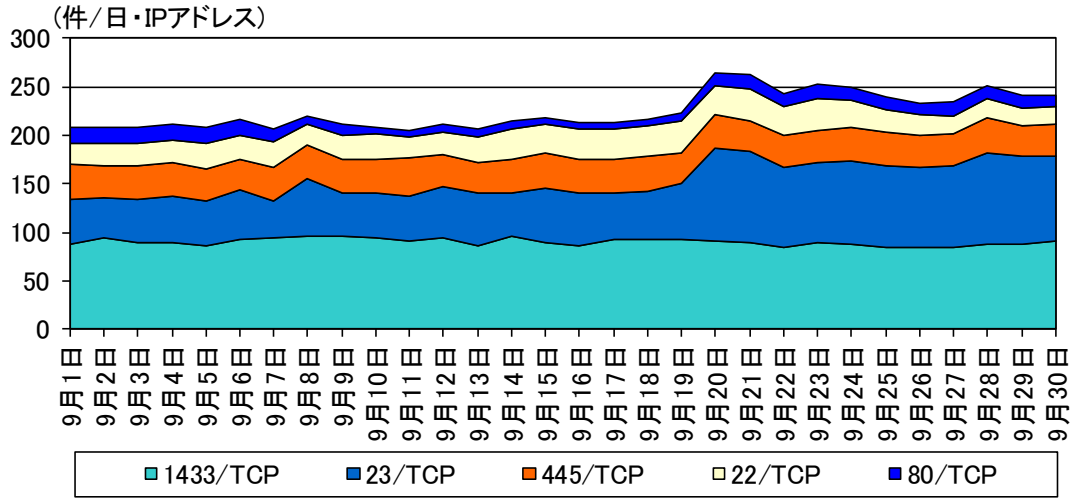

図 3-14　中国からの上位5ポートの検知件数の推移

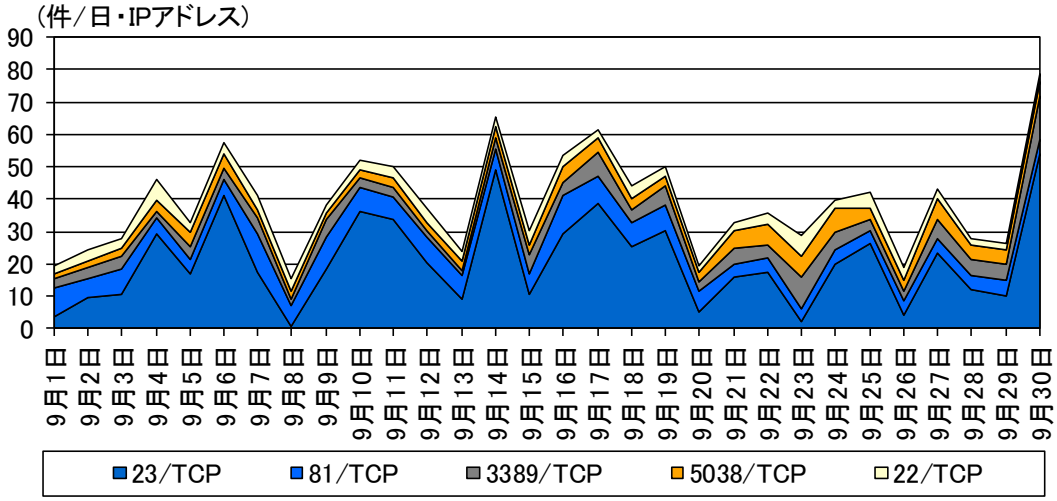

図 3-15　ドイツからの上位5ポートの検知件数の推移

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	2 位	Microsoft Windows Terminal server	412.72 件	＋76.1%　（＋178.33 件）	1 位	
2 位	1 位	INDICATOR-SCAN	295.52 件	＋7.6%　（＋20.83 件）	4 位	
3 位	3 位	SMBv1	137.59 件	＋12.3%　（＋15.10 件）	5 位	
4 位	12 位	Remote Desktop	58.67 件	― [ii]　（＋52.11 件）	2 位	
5 位	5 位	SERVER-APACHE	52.73 件	＋101.6%　（＋26.57 件）	3 位	

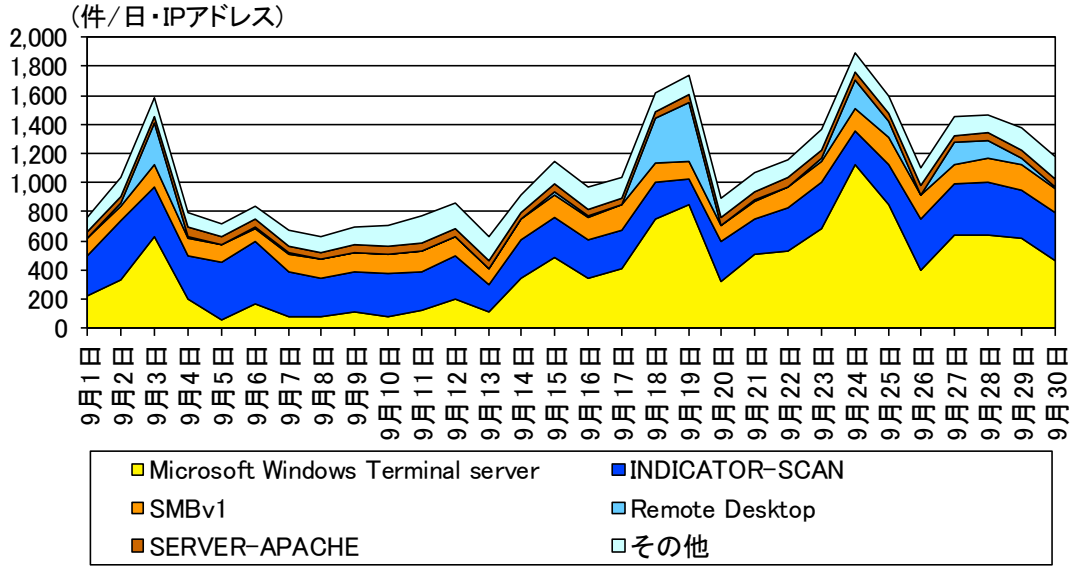

図 4-1　不正侵入等の攻撃手法別検知件数の推移

[i] 一日・1IP アドレス当たり。

[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。

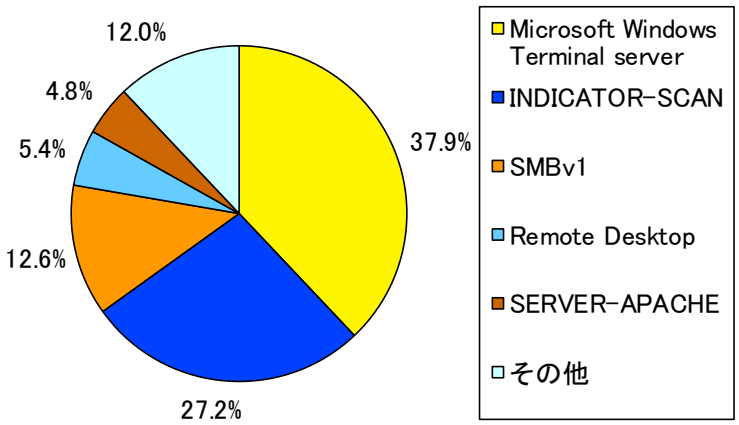

図 4-2 不正侵入等の攻撃手法別検知比率

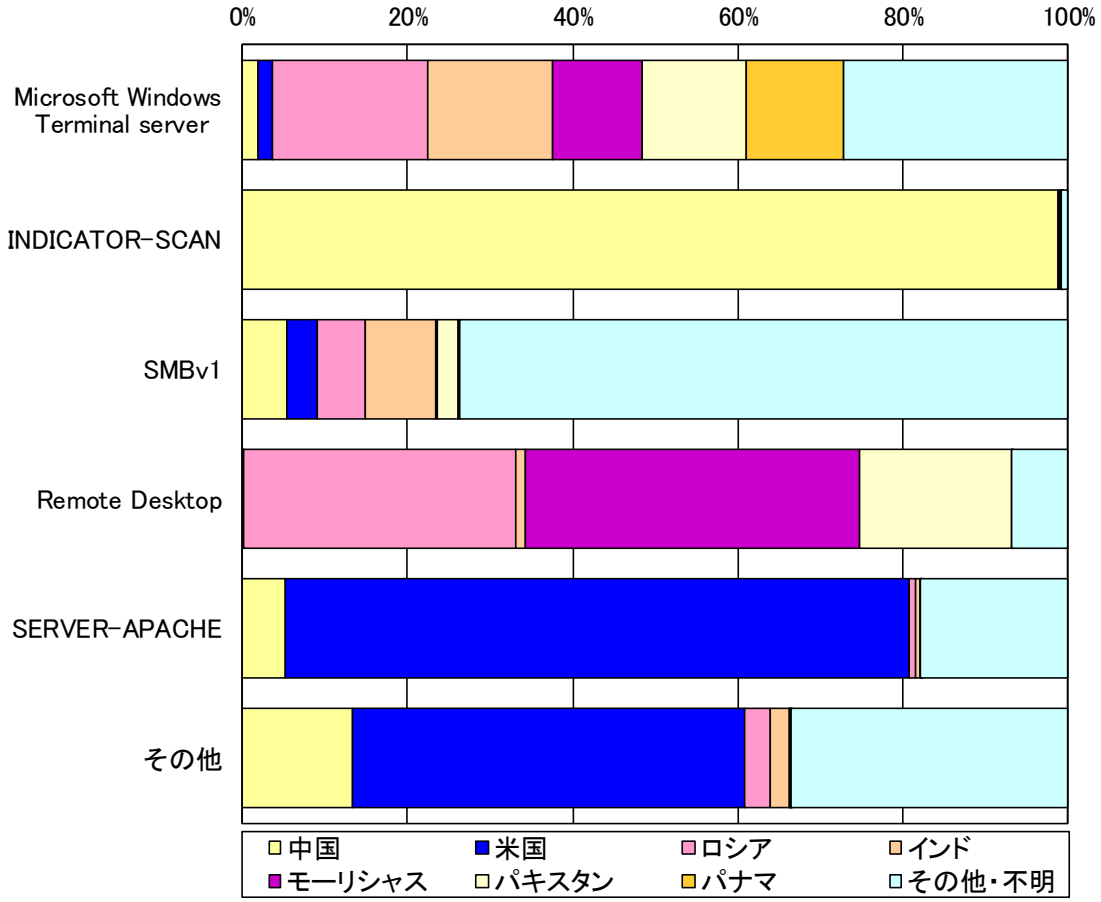

図 4-3 不正侵入等の攻撃手法の国・地域別検知比率

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	328.27 件	＋5.4% （＋16.73 件）
2 位	2 位	米国	114.29 件	＋24.5% （＋22.51 件）
3 位	6 位	ロシア	109.86 件	＋171.8% （＋69.44 件）
4 位	3 位	インド	78.34 件	＋67.3% （＋31.50 件）
5 位	－ [ii]	モーリシャス	68.72 件	－ [ii] （＋68.58 件）

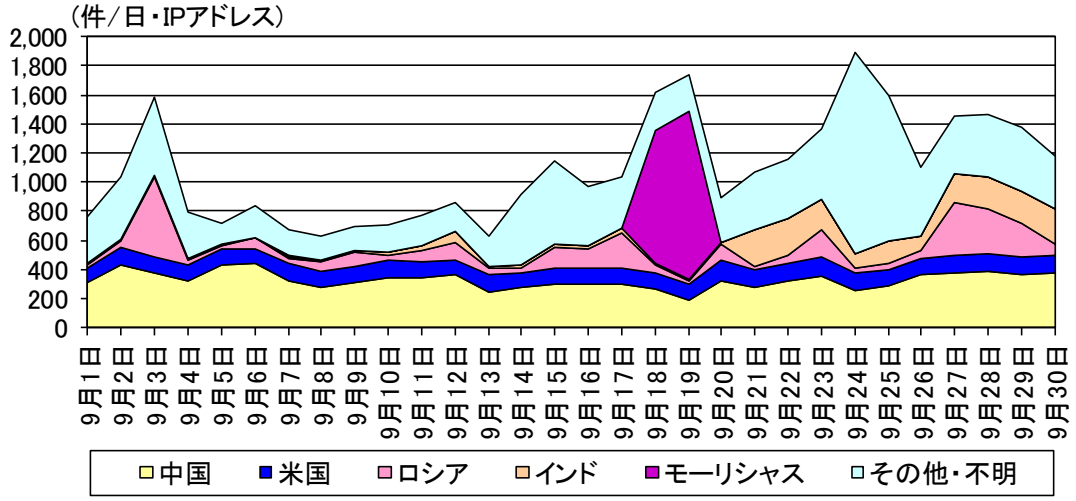

図 4-4 不正侵入等の送信元国・地域別検知件数の推移

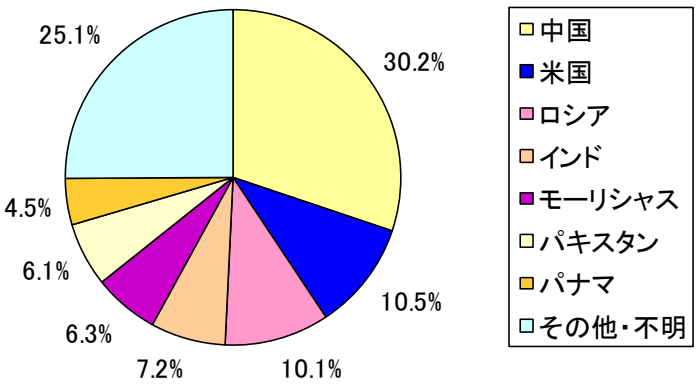

図 4-5 不正侵入等の送信元国・地域別検知比率

[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、前月期比及び前月期順位は記載していません。

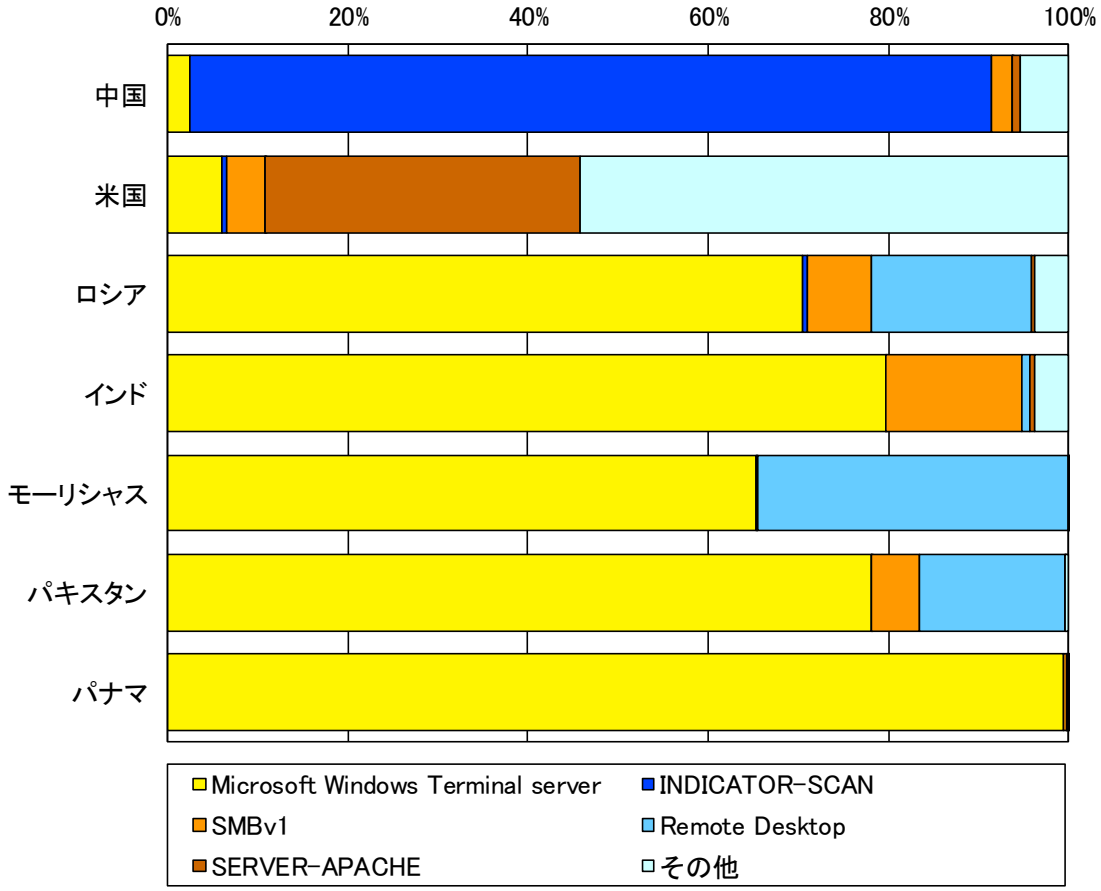

図 4-6 不正侵入等の送信元国・地域別上位の攻撃手法別検知比率

5　DoS 攻撃被害の観測結果

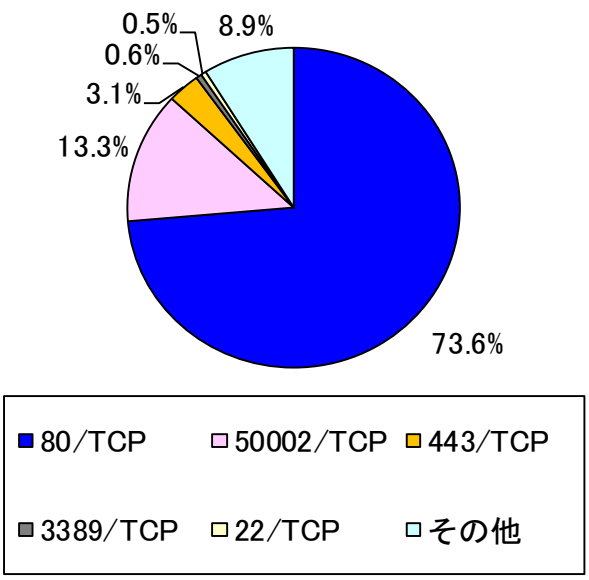

図 5-1　跳ね返りパケット送信元ポート別比率

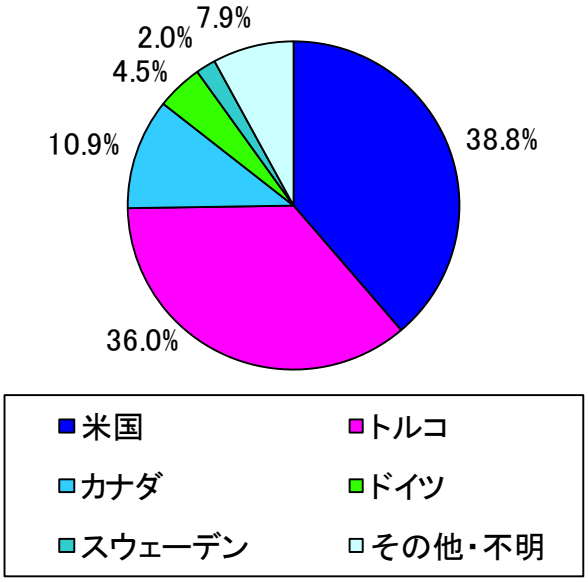

図 5-2　跳ね返りパケット送信元国・地域別比率