令和2年 11 月 20 日

令和2年 10 月期観測資料

1　観測結果概要

令和2年 10 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 6,454.4 件で、令和2年9月期(以下「前月期」という。)の 6,588.0 件と比較して 133.6 件(2.0%)減少しました。また、送信元 IP アドレス[i] 数は、一日当たり 56,637.5 個で、前月期の 56,165.9 個と比較して 471.6 個(0.8%)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 1,067.7 件で、前月期の 1,088.1 件と比較して 20.5 件(1.9%)減少しました。また、送信元 IP アドレス数は、一日当たり 10,831.9 個で、前月期の 10,633.1 個と比較して 198.8 個(1.9%)増加しました。

DoS 攻撃被害検知件数は、一日当たり14,695.6 件で、前月期の 27,735.5 件と比較して13,039.9 件(47.0%)減少しました。また、送信元 IP アドレス数は、一日当たり 625.4 個で、前月期の 521.7 個と比較して 103.7 個(19.9%)増加しました。

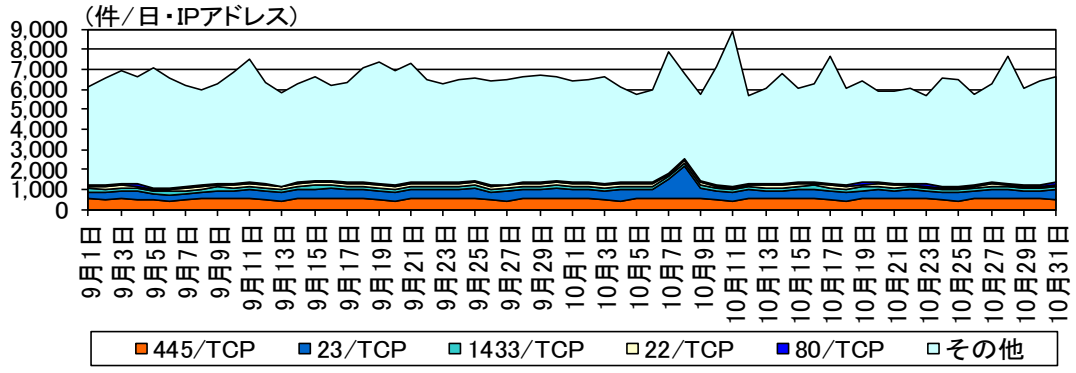

図 1-1　宛先ポート別検知件数の推移

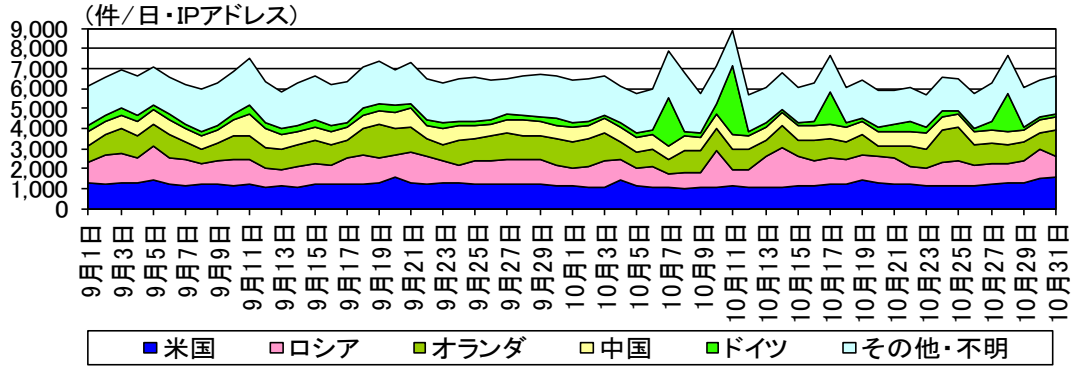

図 1-2　送信元国・地域別検知件数の推移[ii]

[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	519.64 件	＋0.9%　（＋4.79 件）
2 位	2 位	23/TCP	477.79 件	＋15.3%　（＋63.47 件）
3 位	3 位	1433/TCP	155.47 件	－2.3%　（－3.73 件）
4 位	4 位	22/TCP	118.37 件	－7.9%　（－10.11 件）
5 位	5 位	80/TCP	75.41 件	＋4.6%　（＋3.34 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	477.79 件	＋15.3%　（＋63.47 件）	2 位	2 位
2 位	5060/UDP	59.35 件	＋19.1%　（＋9.50 件）	6 位	7 位
3 位	8/ICMP	53.28 件	＋20.2%　（＋8.97 件）	7 位	9 位
4 位	11211/TCP	13.08 件	＋66.3%　（＋5.22 件）	28 位	47 位
5 位	445/TCP	519.64 件	＋0.9%　（＋4.79 件）	1 位	1 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	22/TCP	118.37 件	－7.9%　（－10.11 件）	4 位	4 位
2 位	53413/UDP	17.19 件	－32.5%　（－8.29 件）	21 位	17 位
3 位	5038/TCP	13.12 件	－31.2%　（－5.96 件）	27 位	21 位
4 位	50802/TCP	4.80 件	－54.8%　（－5.82 件）	82 位	35 位
5 位	2323/TCP	18.40 件	－21.9%　（－5.16 件）	19 位	18 位

[i] 一日・1IP アドレス当たり。

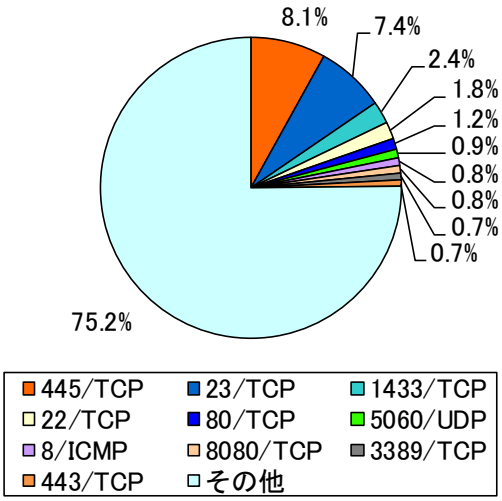

図 3-1　宛先ポート別比率（全て）[i]

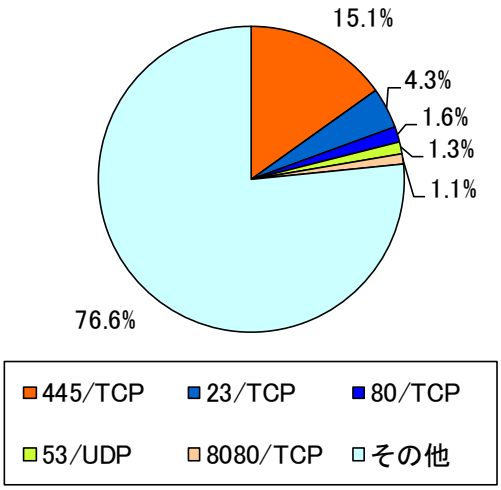

図 3-2　宛先ポート別比率（日本国内）

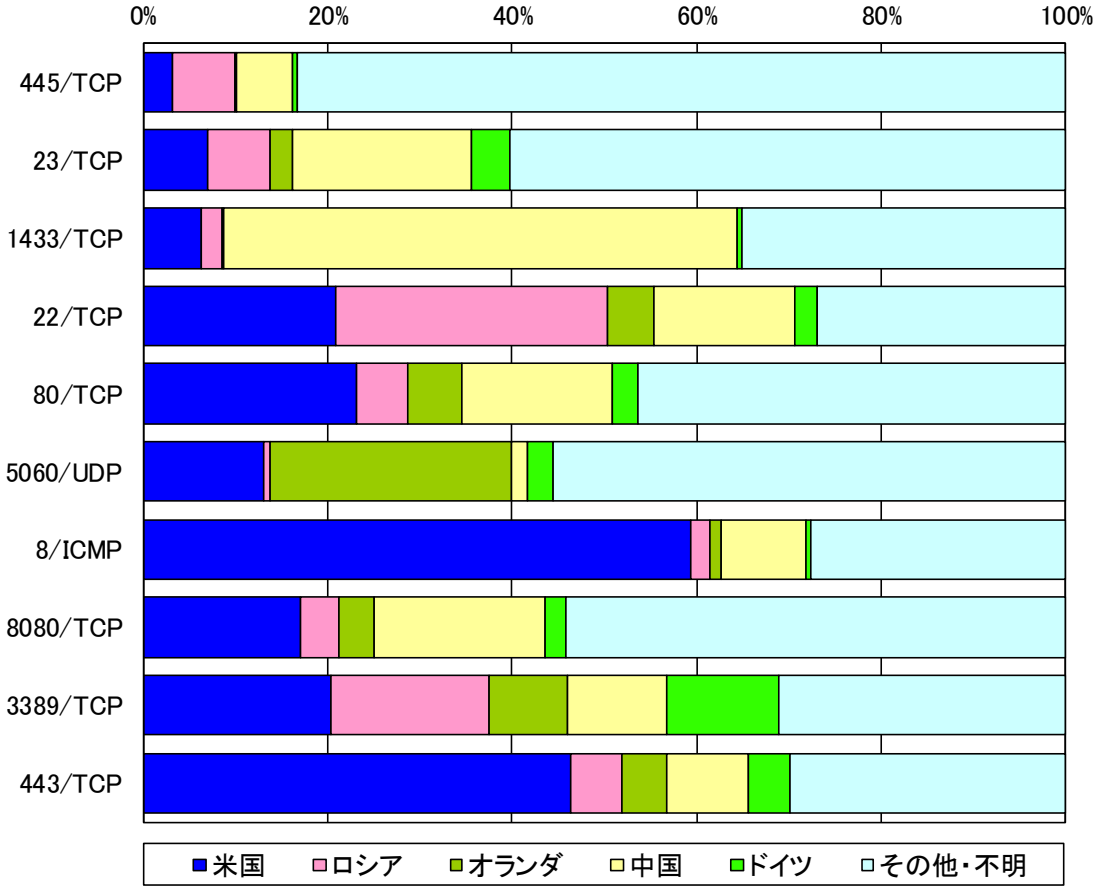

図 3-3　宛先ポート別上位の送信元国・地域別比率

[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。

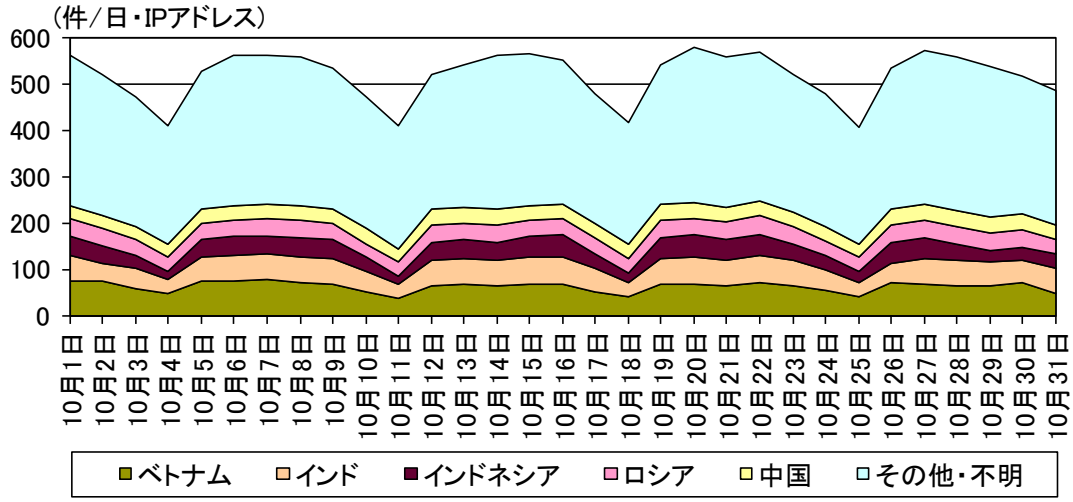

図 3-4　センサーのポート 445/TCP における検知件数の推移

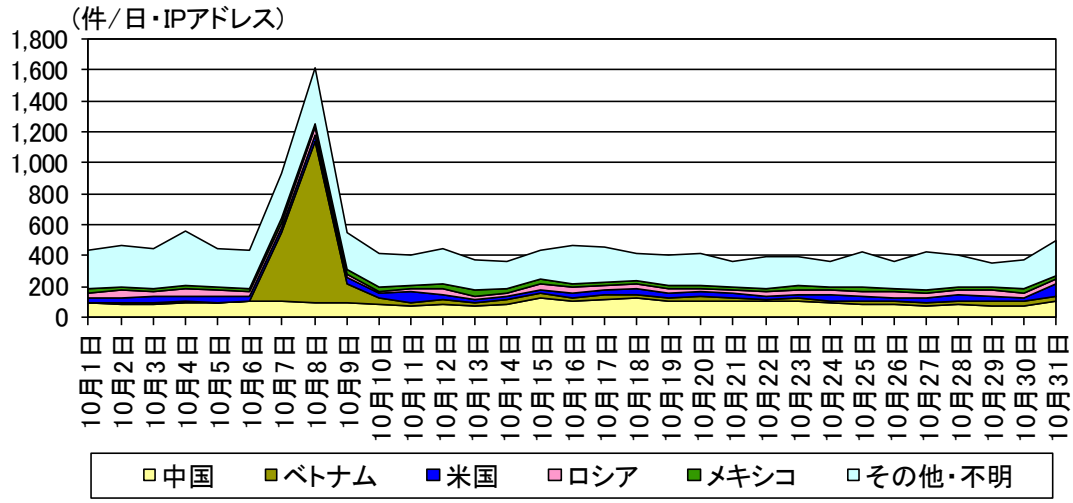

図 3-5　センサーのポート 23/TCP における検知件数の推移

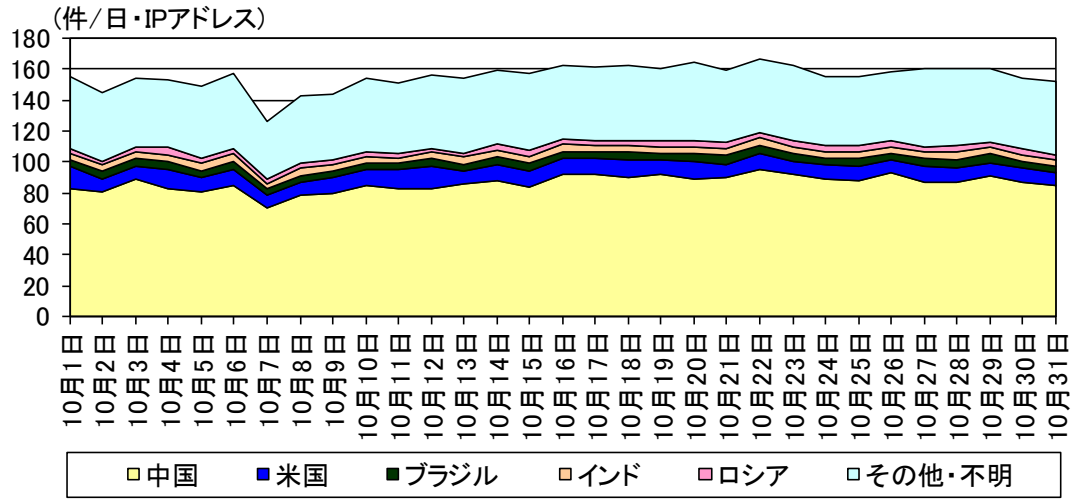

図 3-6　センサーのポート 1433/TCP における検知件数の推移

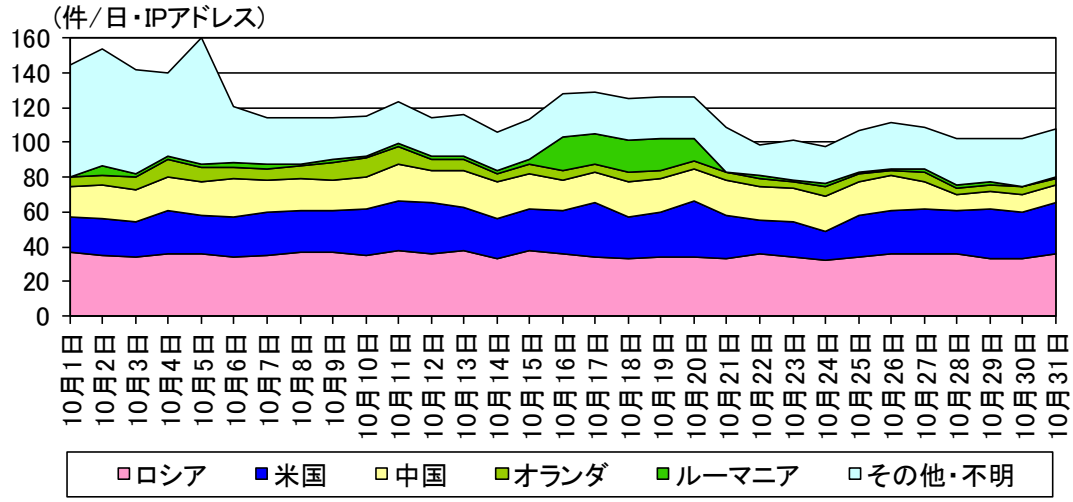

図 3-7　センサーのポート 22/TCP における検知件数の推移

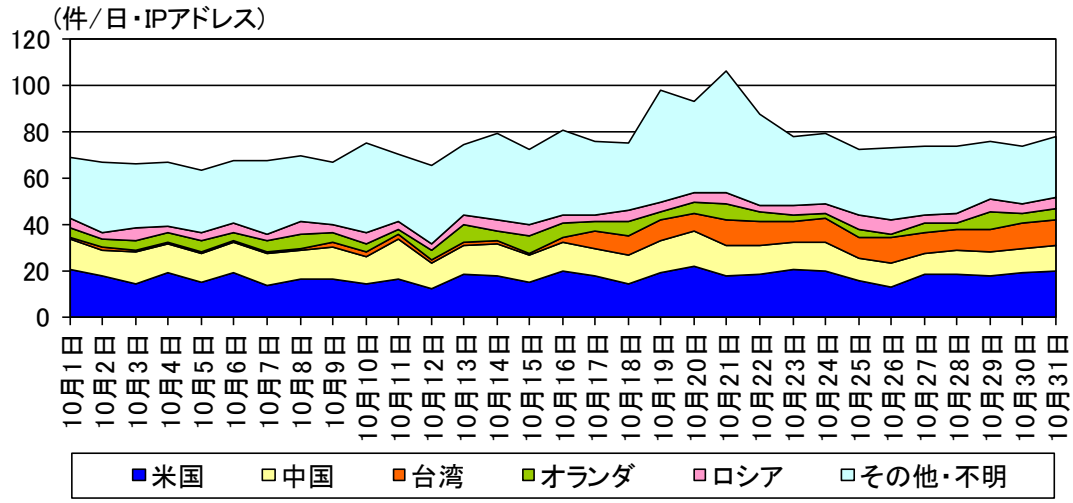

図 3-8　センサーのポート 80/TCP における検知件数の推移

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	1 位	米国	1,182.63 件	－3.6%　（－44.69 件）
2 位	2 位	ロシア	1,139.59 件	－5.4%　（－64.48 件）
3 位	3 位	オランダ	1,022.02 件	－8.2%　（－91.56 件）
4 位	4 位	中国	692.62 件	－4.3%　（－31.17 件）
5 位	5 位	ドイツ	513.07 件	＋82.9%　（＋232.50 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	513.07 件	＋82.9%　（＋232.50 件）	5 位	5 位
2 位	ベトナム	168.94 件	＋68.9%　（＋68.90 件）	6 位	9 位
3 位	ルーマニア	90.59 件	＋11.2%　（＋9.10 件）	10 位	12 位
4 位	ブルガリア	141.43 件	＋5.9%　（＋7.84 件）	8 位	8 位
5 位	イスラエル	9.44 件	＋97.6%　（＋4.66 件）	40 位	50 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	オランダ	1,022.02 件	－8.2%　（－91.56 件）	3 位	3 位
2 位	インド	157.55 件	－36.5%　（－90.71 件）	7 位	6 位
3 位	ロシア	1,139.59 件	－5.4%　（－64.48 件）	2 位	2 位
4 位	米国	1,182.63 件	－3.6%　（－44.69 件）	1 位	1 位
5 位	中国	692.62 件	－4.3%　（－31.17 件）	4 位	4 位

[i] 一日・1IP アドレス当たり。

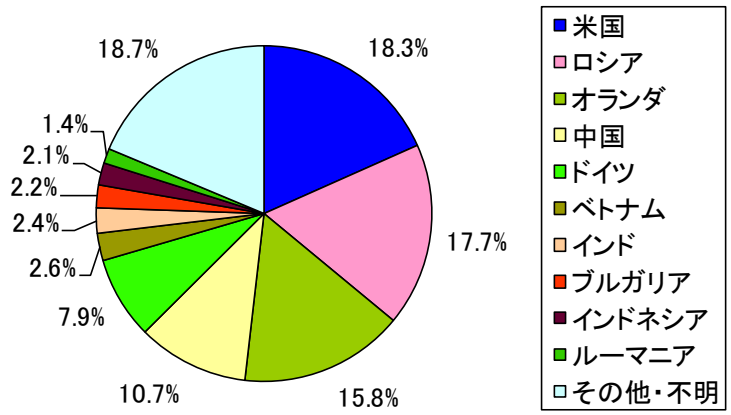

図 3-9　送信元国・地域別比率

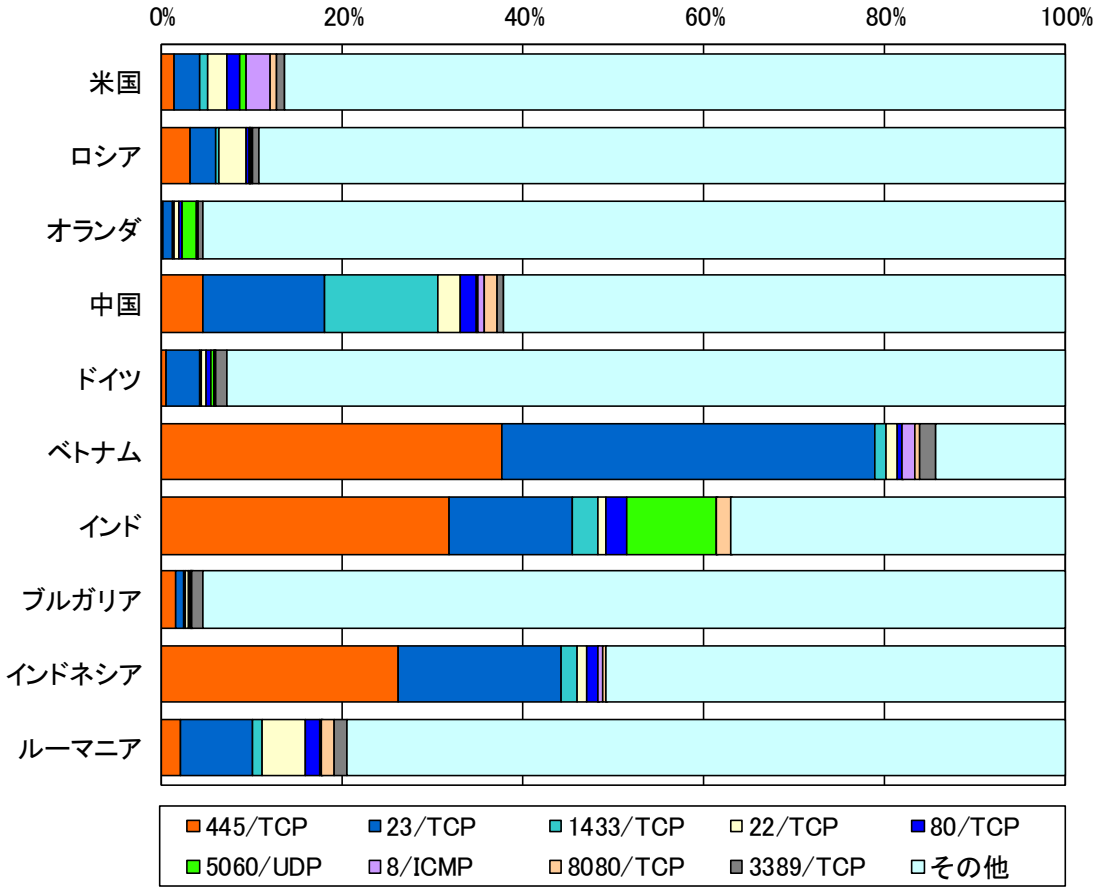

図 3-10　送信元国・地域別上位の宛先ポート別比率

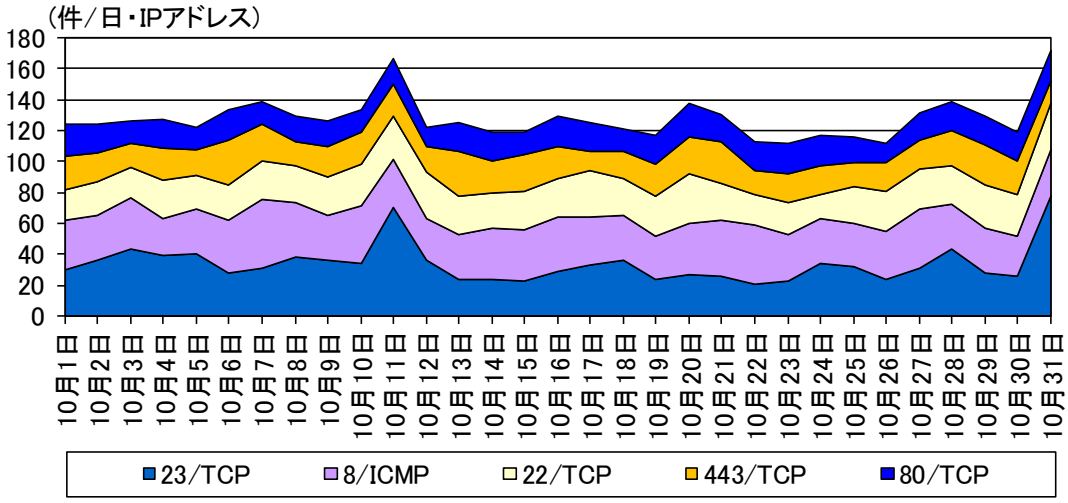

図 3-11　米国からの上位5ポートの検知件数の推移

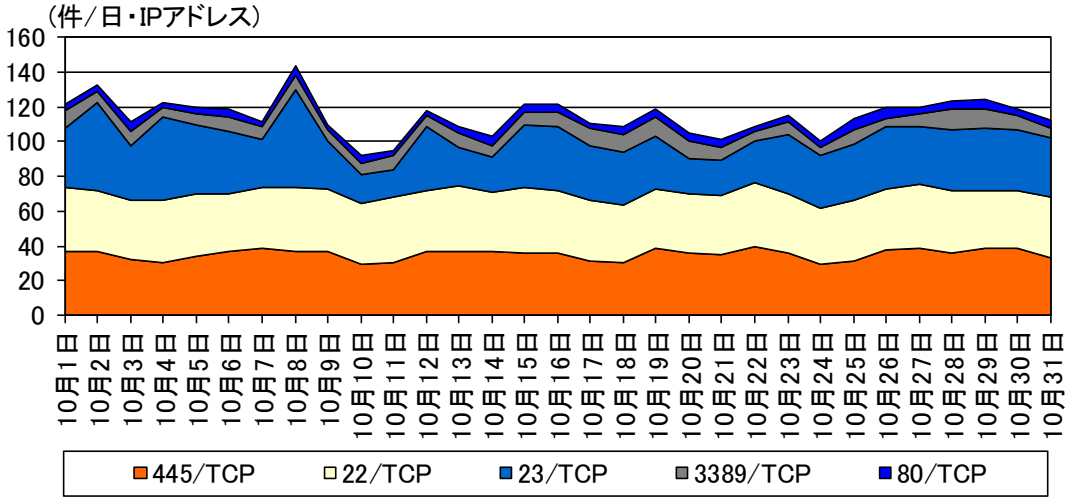

図 3-12　ロシアからの上位5ポートの検知件数の推移

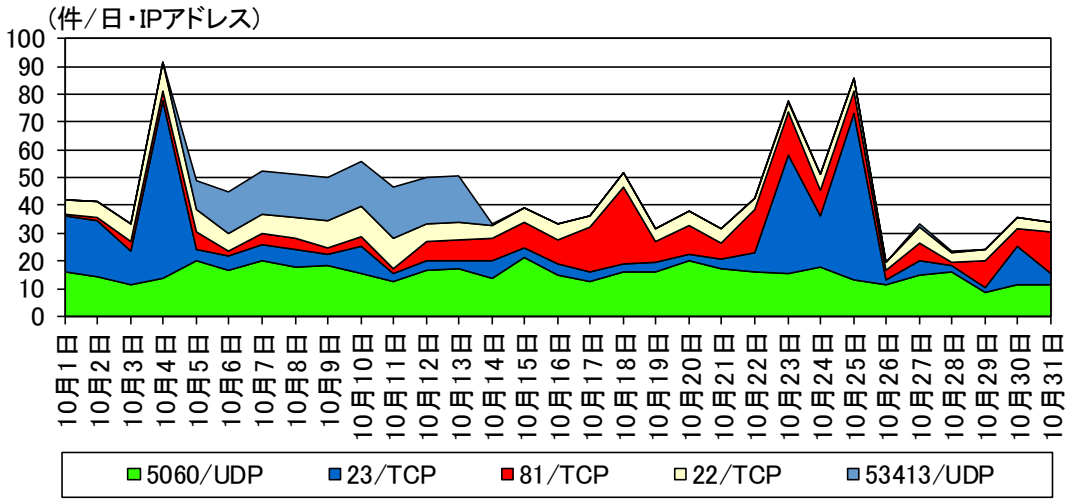

図 3-13　オランダからの上位5ポートの検知件数の推移

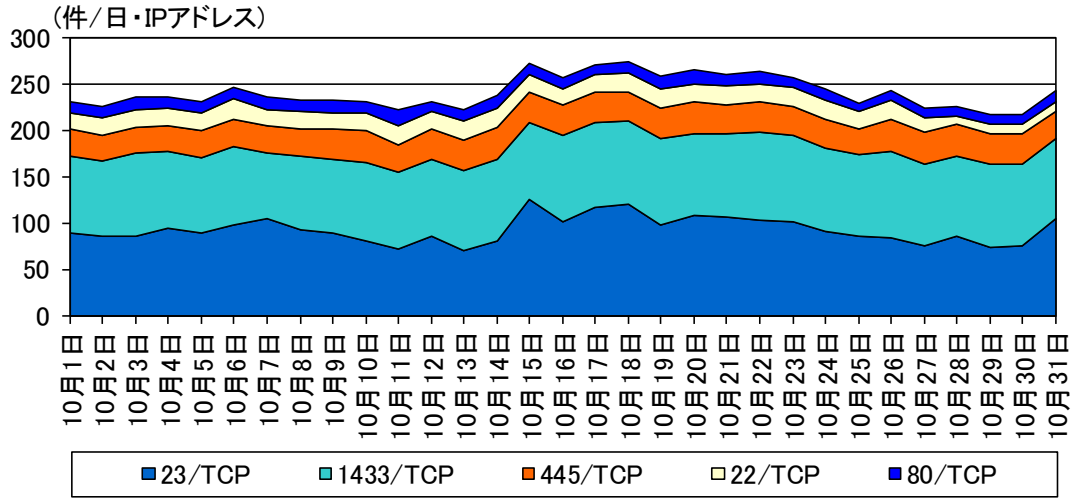

図 3-14　中国からの上位5ポートの検知件数の推移

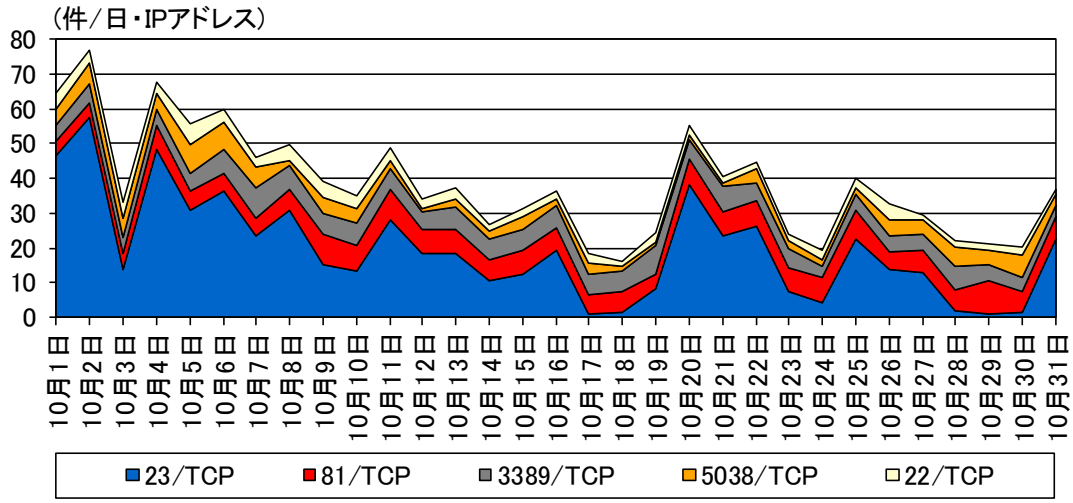

図 3-15　ドイツからの上位5ポートの検知件数の推移

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	1 位	Microsoft Windows Terminal server	345.98 件	−16.2%　（−66.74 件）		1 位
2 位	2 位	INDICATOR-SCAN	334.29 件	＋13.1%　（＋38.76 件）	1 位	
3 位	3 位	SMBv1	156.75 件	＋13.9%　（＋19.16 件）	2 位	
4 位	4 位	Remote Desktop	56.63 件	−3.5%　（−2.04 件）		
5 位	5 位	SERVER-APACHE	50.81 件	−3.6%　（−1.92 件）		

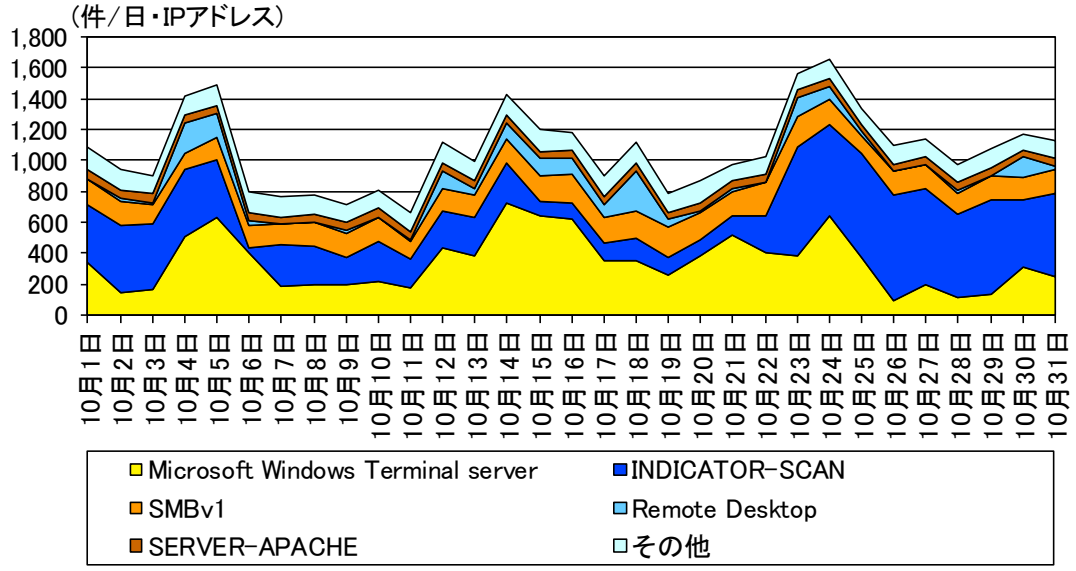

図 4-1　不正侵入等の攻撃手法別検知件数の推移

[i] 一日・1IP アドレス当たり。

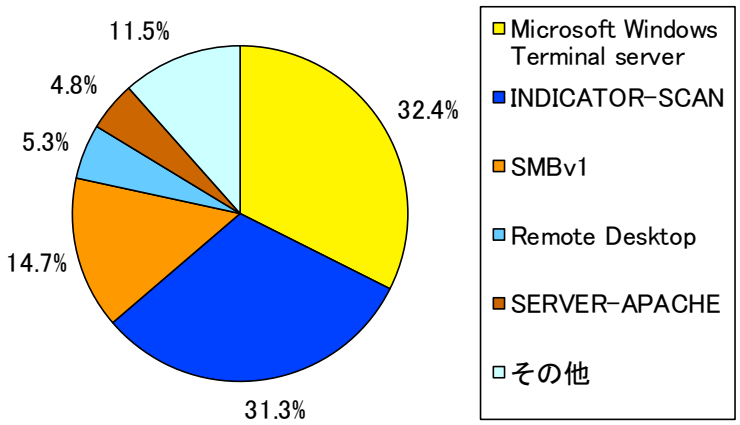

図 4-2 不正侵入等の攻撃手法別検知比率

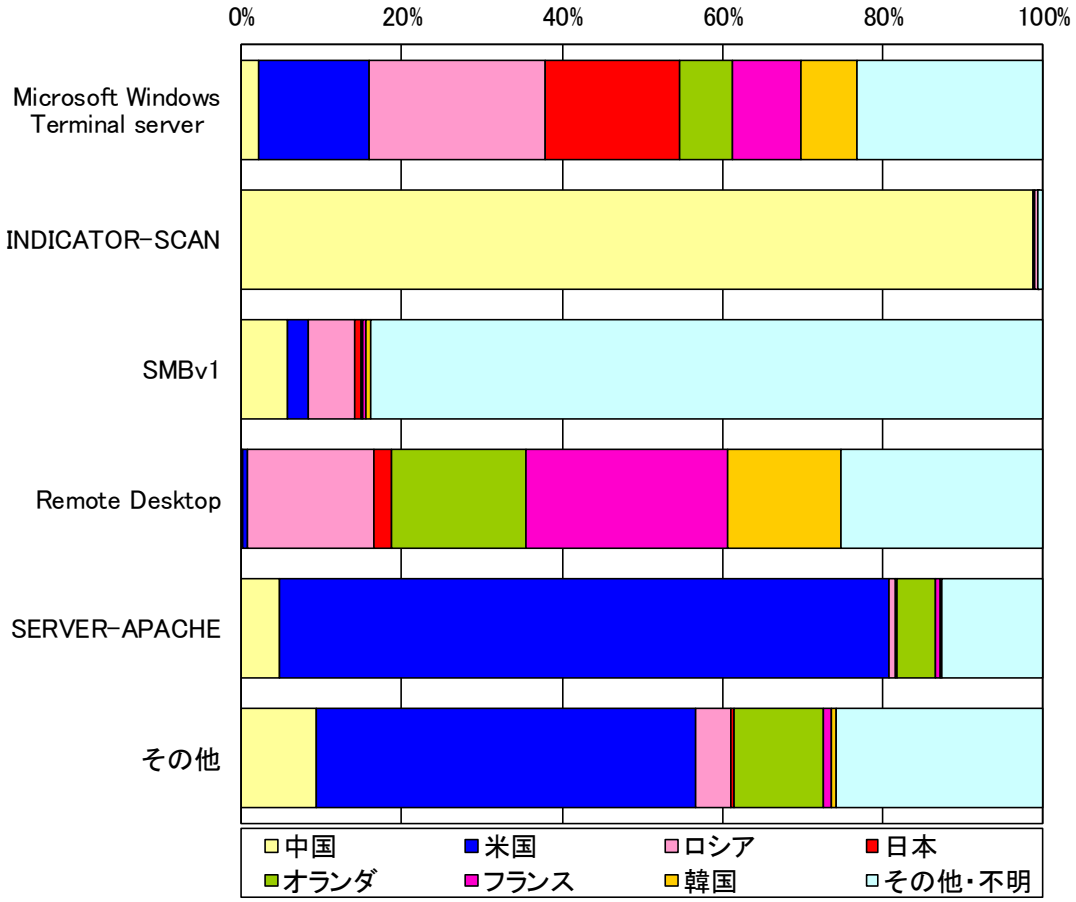

図 4-3 不正侵入等の攻撃手法の送信元国・地域別検知比率

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	360.66 件	＋9.9% （＋32.39 件）
2 位	2 位	米国	149.32 件	＋30.6% （＋35.03 件）
3 位	3 位	ロシア	101.38 件	－7.7% （－8.48 件）
4 位	20 位	日本	60.90 件	－ [ii] （＋55.15 件）
5 位	13 位	オランダ	49.18 件	＋358.9% （＋38.46 件）

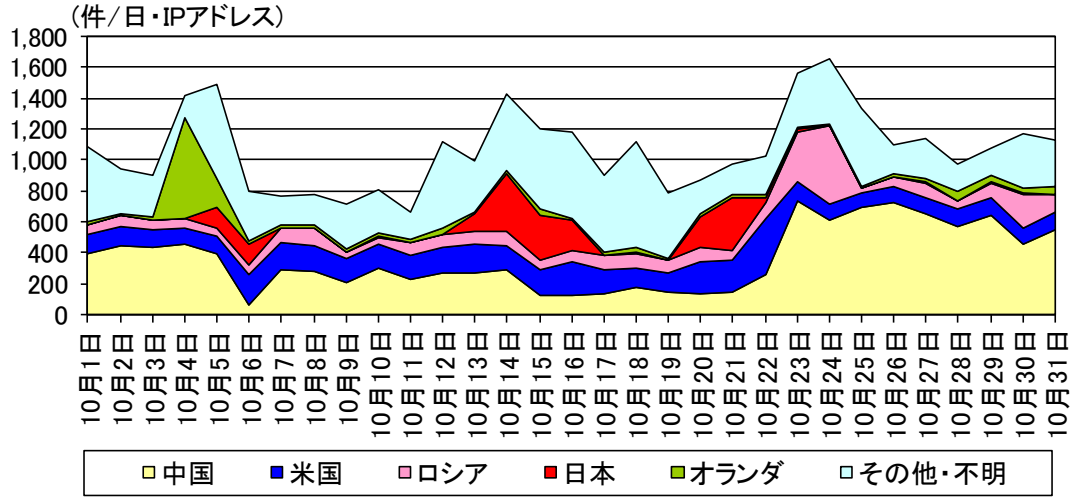

図 4-4 不正侵入等の送信元国・地域別検知件数の推移

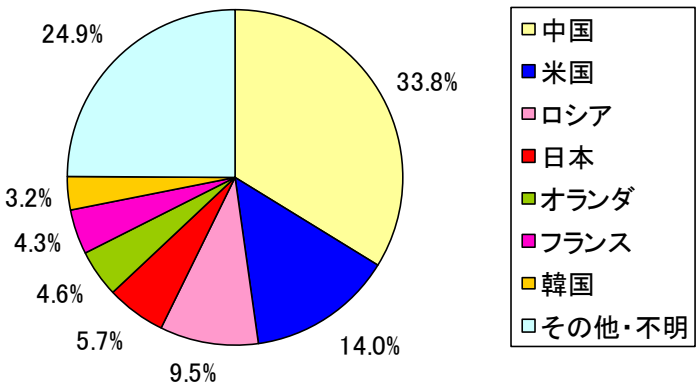

図 4-5 不正侵入等の送信元国・地域別検知比率

[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。

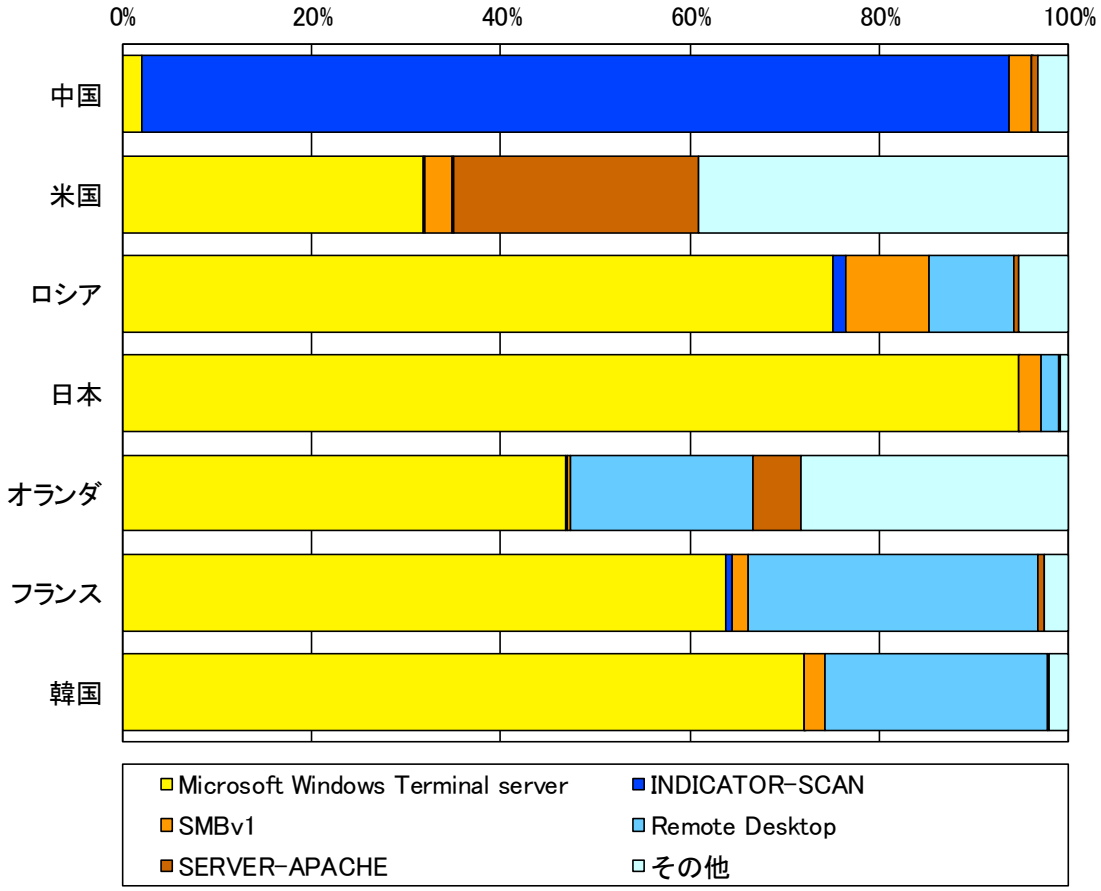

図 4-6 不正侵入等の送信元国・地域別上位の攻撃手法別検知比率

5　DoS 攻撃被害の観測結果

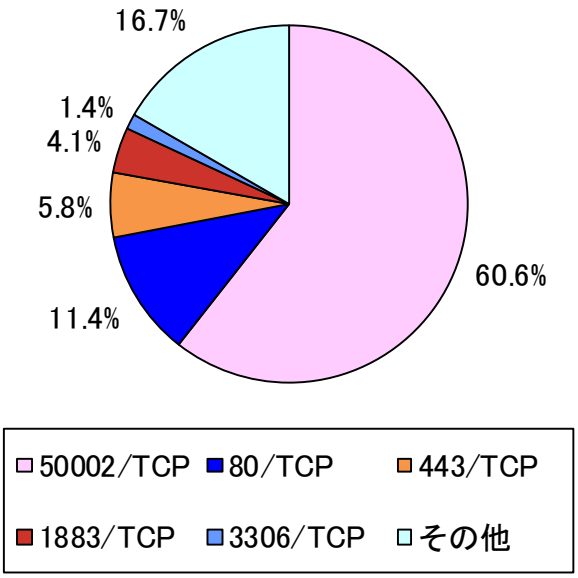

図 5-1　跳ね返りパケット送信元ポート別比率

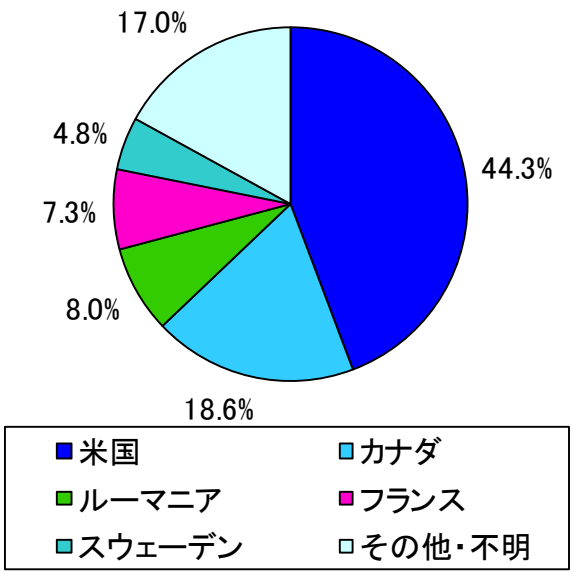

図 5-2　跳ね返りパケット送信元国・地域別比率