令和2年 12 月 24 日

令和2年 11 月期観測資料

1　観測結果概要

令和2年 11 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 7,402.7 件で、令和2年 10 月期(以下「前月期」という。)の 6,454.4 件と比較して 948.2 件(14.7%)増加しました。また、送信元 IP アドレス[i]数は、一日当たり 50,815.0 個で、前月期の 56,637.5 個と比較して 5,822.5 個(10.3%)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 1,144.8 件で、前月期の 1,067.7 件と比較して 77.1 件(7.2%)増加しました。また、送信元 IP アドレス数は、一日当たり 10,673.7 個で、前月期の 10,831.9 個と比較して 158.2 個(1.5%)減少しました。

DoS 攻撃被害検知件数は、一日当たり 12,724.0 件で、前月期の 14,695.6 件と比較して 1,971.6 件(13.4%)減少しました。また、送信元 IP アドレス数は、一日当たり 696.4 個で、前月期の 625.4 個と比較して 71.0 個(11.4%)増加しました。

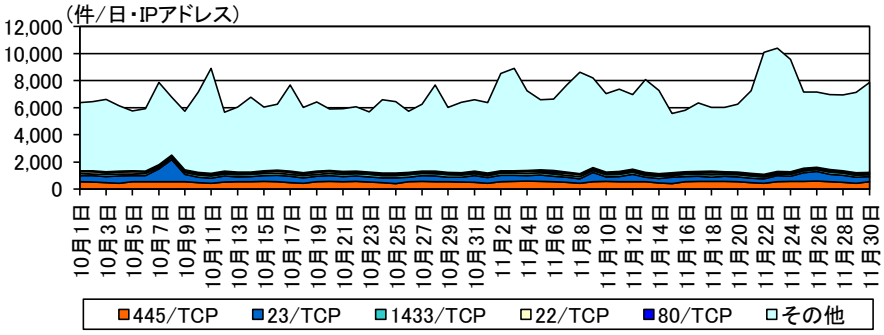

図 1-1　宛先ポート別検知件数の推移

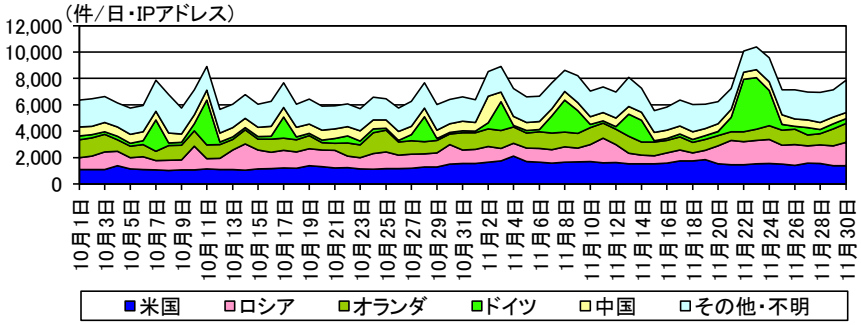

図 1-2　送信元国・地域別検知件数の推移 [ii]

[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	523.77 件	＋0.8%　（＋4.13 件）
2 位	2 位	23/TCP	433.99 件	-9.2%　（-43.80 件）
3 位	3 位	1433/TCP	153.90 件	－1.0%　（－1.57 件）
4 位	4 位	22/TCP	110.96 件	－6.3%　（－7.41 件）
5 位	5 位	80/TCP	85.17 件	＋12.9%　（＋9.76 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	500/UDP	46.38 件	－[ii]　（＋43.86 件）	12 位	－[ii]
2 位	52869/TCP	42.30 件	＋167.5%　（＋26.49 件）	14 位	23 位
3 位	81/TCP	48.99 件	＋52.7%　（＋16.91 件）	9 位	13 位
4 位	38725/UDP	16.75 件	－[ii]　（＋16.75 件）	27 位	－[ii]
5 位	8/ICMP	65.38 件	＋22.7%　（＋12.10 件）	6 位	7 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	23/TCP	433.99 件	－9.2%　（－43.80 件）	2 位	2 位
2 位	22/TCP	110.96 件	－6.3%　（－7.41 件）	4 位	4 位
3 位	53/UDP	17.60 件	－25.0%　（－5.87 件）	25 位	17 位
4 位	8291/TCP	34.79 件	－12.9%　（－5.14 件）	15 位	12 位
5 位	2376/TCP	2.43 件	－66.1%　（－4.75 件）	178 位	45 位

[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。

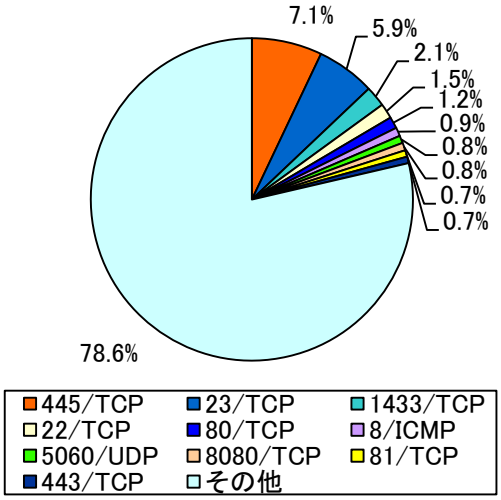

図 3-1　宛先ポート別比率（全て）[i]

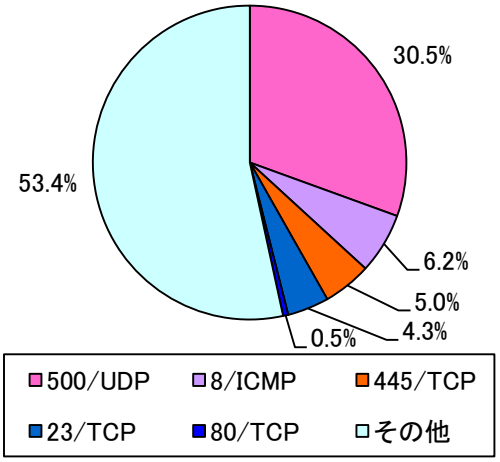

図 3-2　宛先ポート別比率（日本国内）

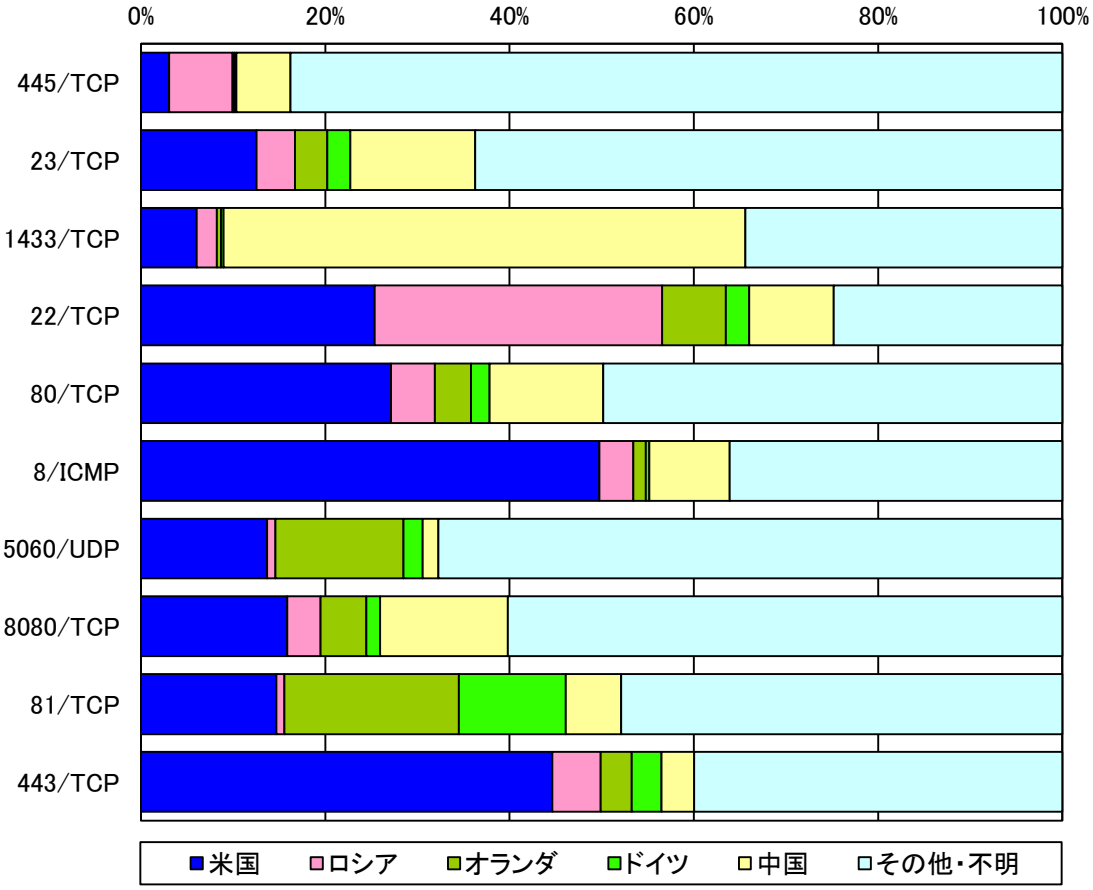

図 3-3　宛先ポート別上位の送信元国・地域別比率

[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。

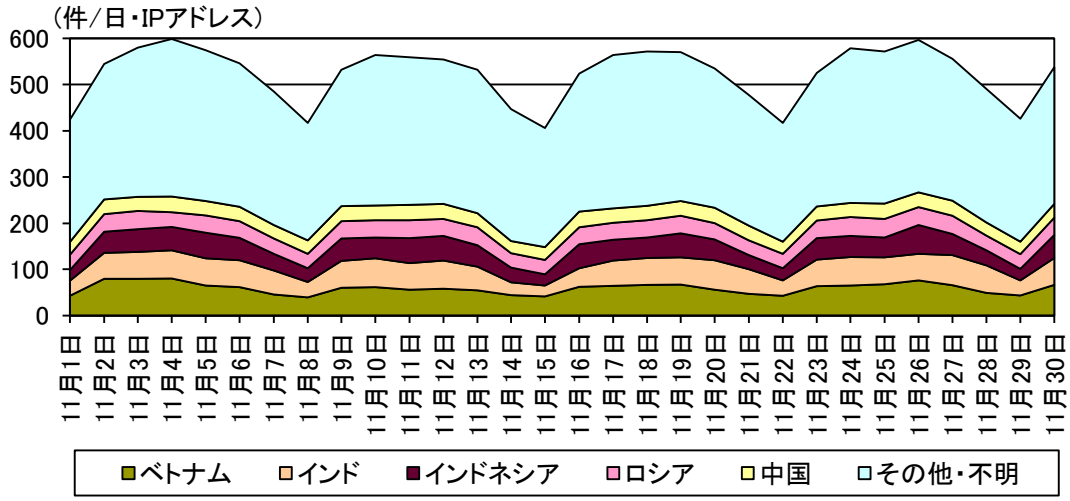

図 3-4　センサーのポート 445/TCP における検知件数の推移

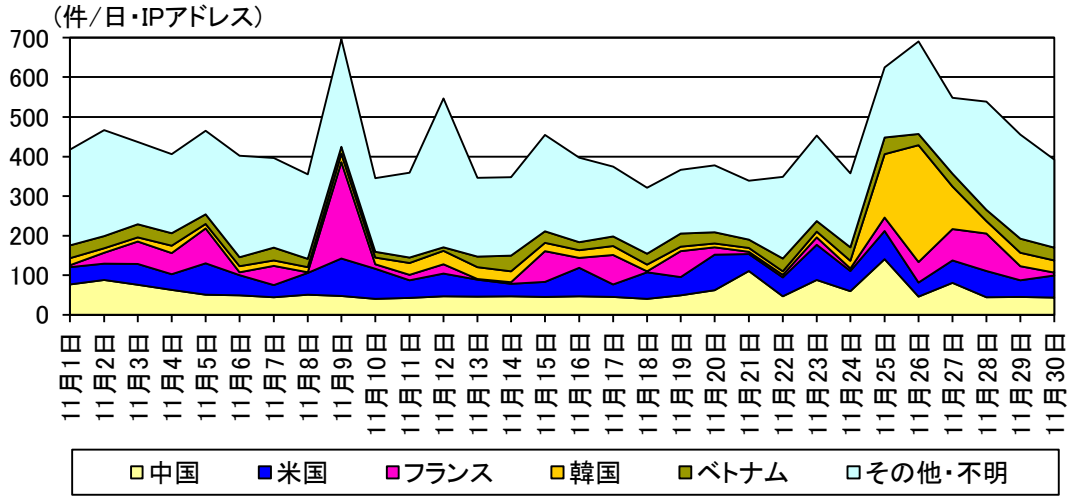

図 3-5　センサーのポート 23/TCP における検知件数の推移

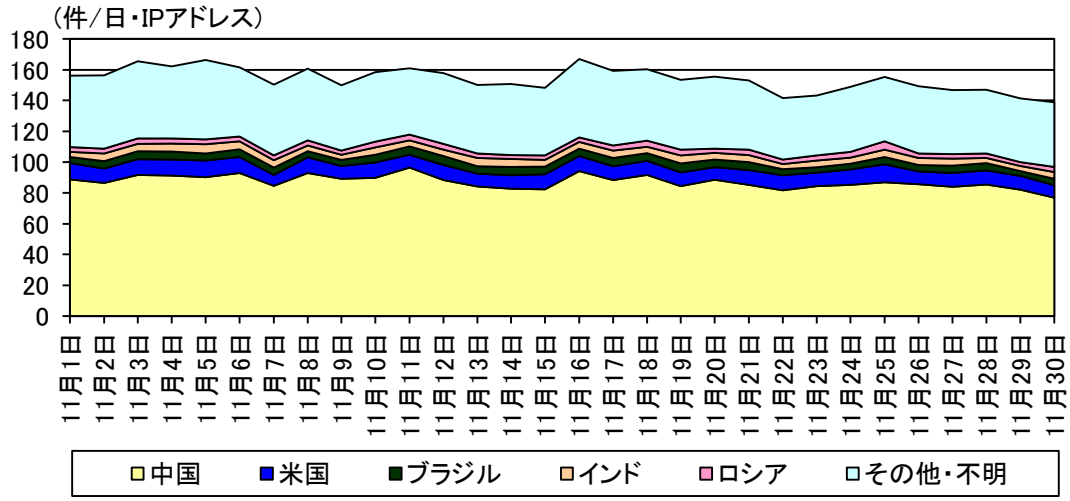

図 3-6　センサーのポート 1433/TCP における検知件数の推移

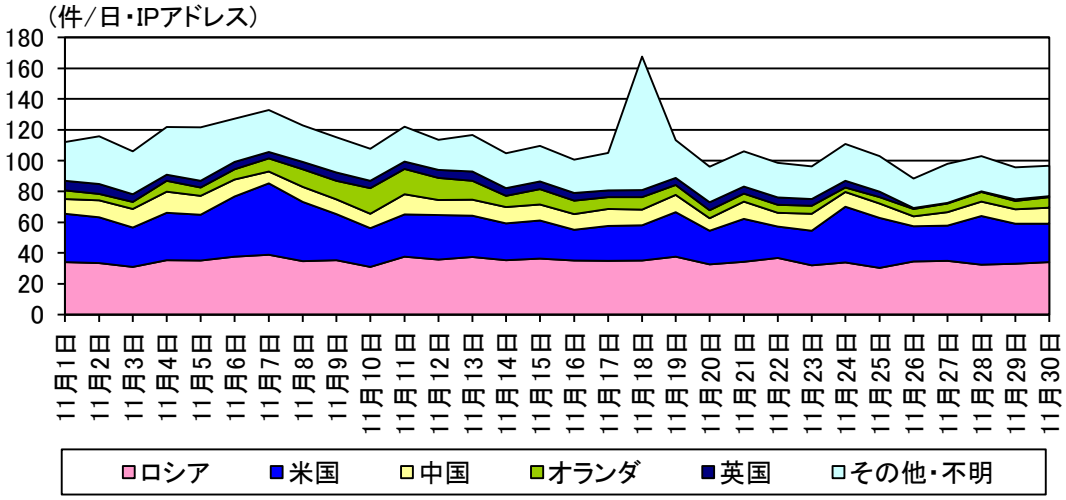

図 3-7　センサーのポート 22/TCP における検知件数の推移

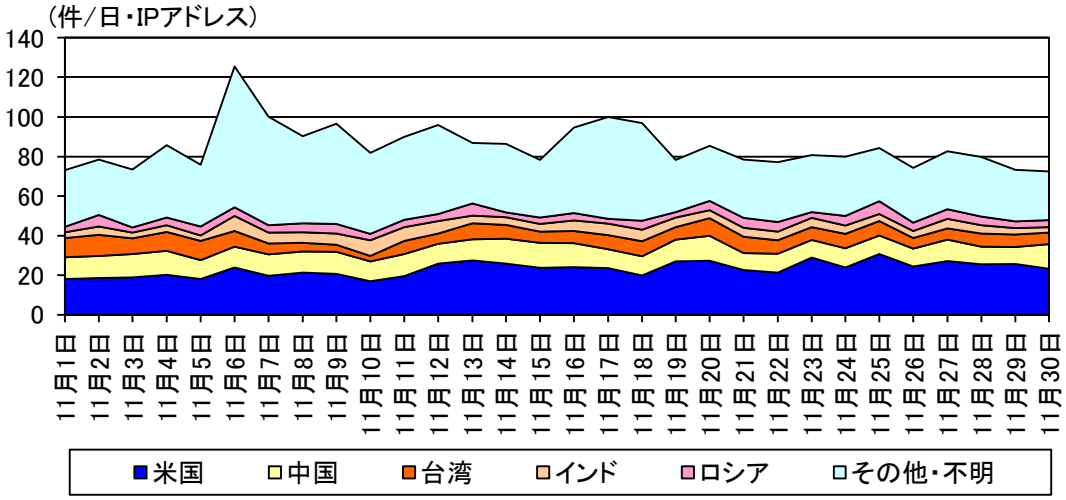

図 3-8　センサーのポート 80/TCP における検知件数の推移

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	1,597.42 件	＋35.1% （＋414.79 件）
2 位	2 位	ロシア	1,221.48 件	＋7.2% （＋81.89 件）
3 位	3 位	オランダ	1,077.30 件	＋5.4% （＋55.28 件）
4 位	5 位	ドイツ	931.28 件	＋81.5% （＋418.21 件）
5 位	4 位	中国	649.23 件	－6.3% （－43.39 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	931.28 件	＋81.5% （＋418.21 件）	4 位	5 位
2 位	米国	1,597.42 件	＋35.1% （＋414.79 件）	1 位	1 位
3 位	日本	143.62 件	＋219.7% （＋98.70 件）	8 位	22 位
4 位	ロシア	1,221.48 件	＋7.2% （＋81.89 件）	2 位	2 位
5 位	オランダ	1,077.30 件	＋5.4% （＋55.28 件）	3 位	3 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	ブルガリア	49.30 件	－65.1% （－92.13 件）	20 位	8 位
2 位	ベトナム	120.70 件	－28.6% （－48.24 件）	9 位	6 位
3 位	中国	649.23 件	－6.3% （－43.39 件）	5 位	4 位
4 位	ルーマニア	54.43 件	－39.9% （－36.15 件）	17 位	10 位
5 位	ウクライナ	59.94 件	－20.2% （－15.20 件）	15 位	12 位

[i] 一日・1IP アドレス当たり。

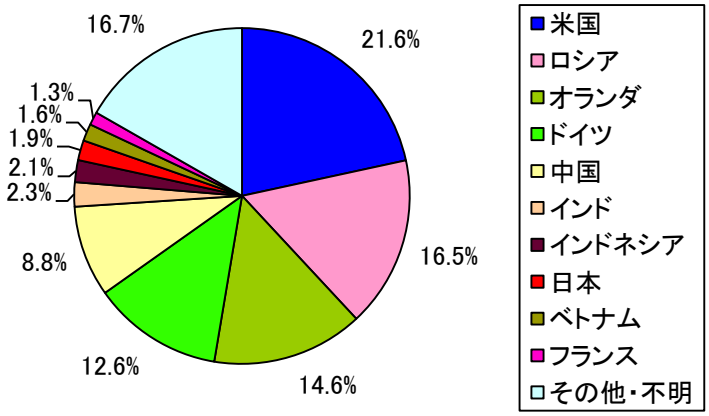

図 3-9　送信元国・地域別比率

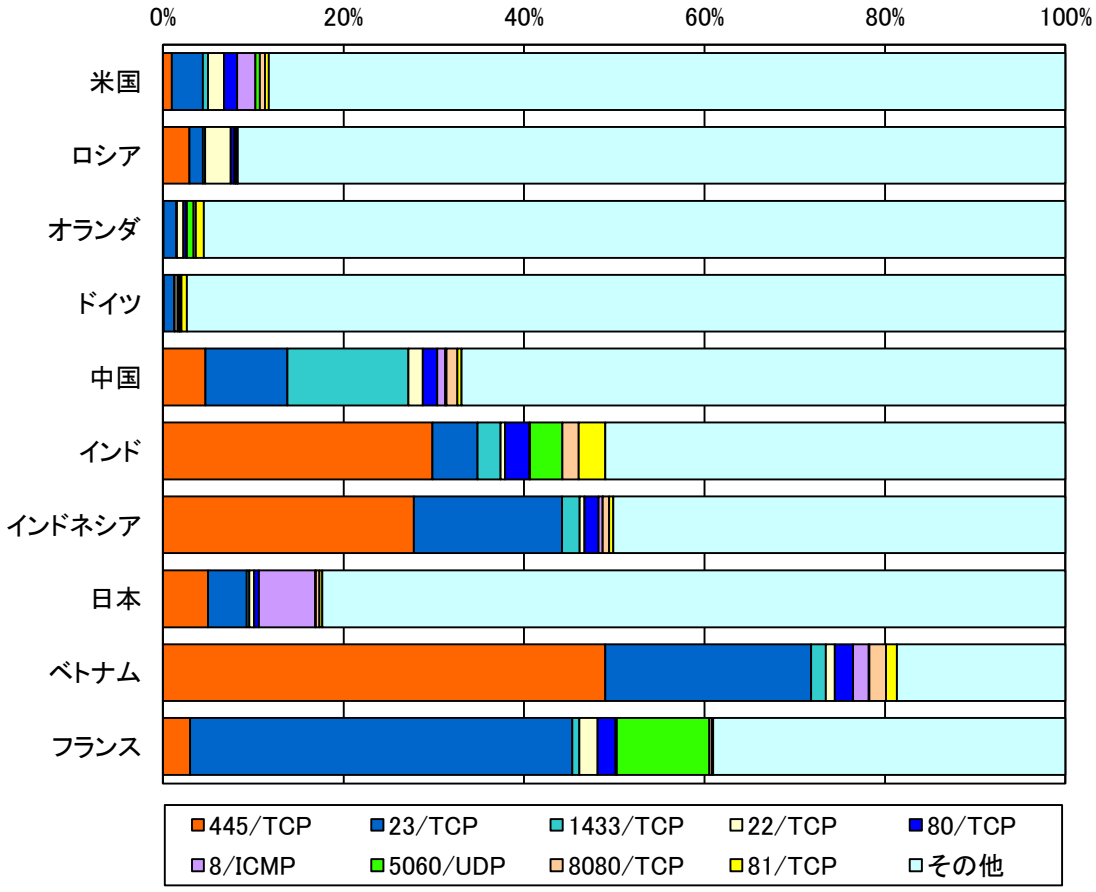

図 3-10　送信元国・地域別上位の宛先ポート別比率

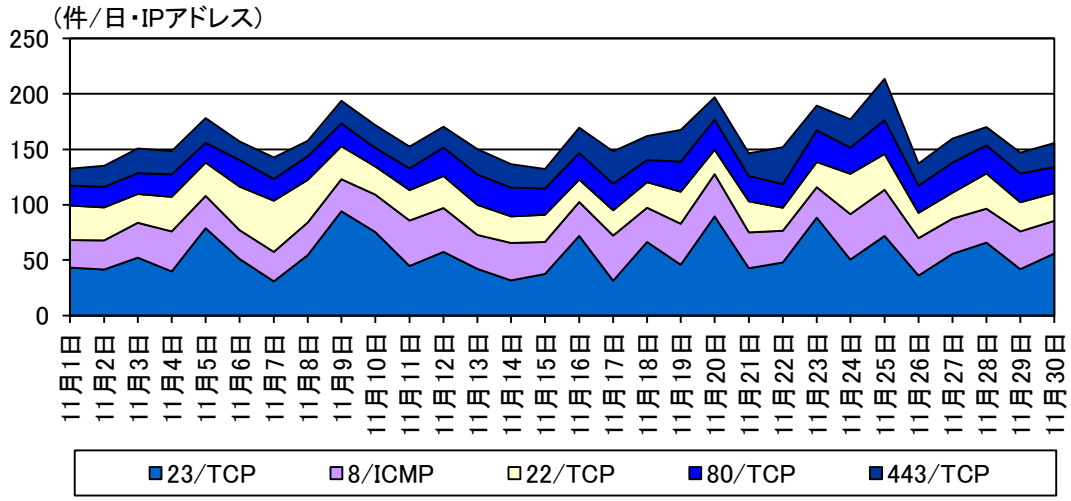

図 3-11　米国からの上位5ポートの検知件数の推移

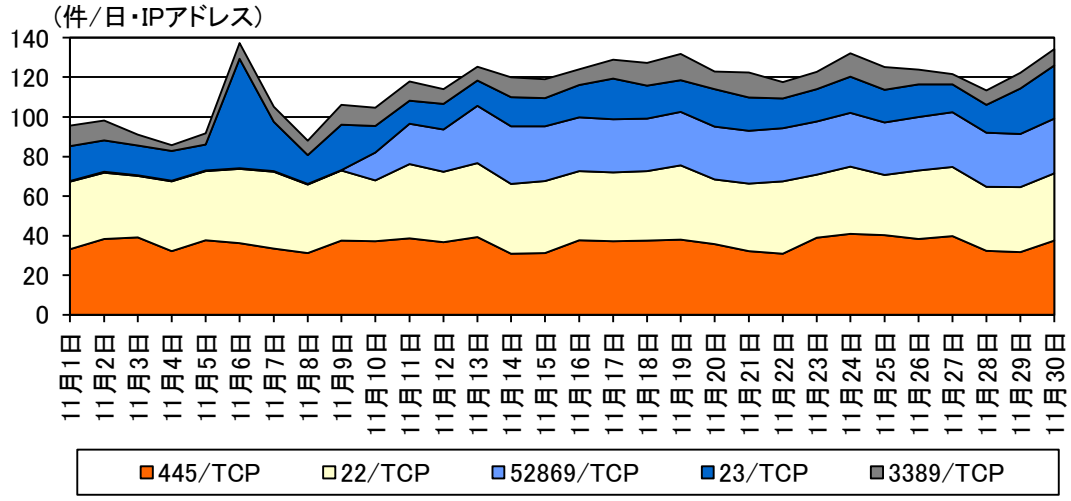

図 3-12　ロシアからの上位5ポートの検知件数の推移

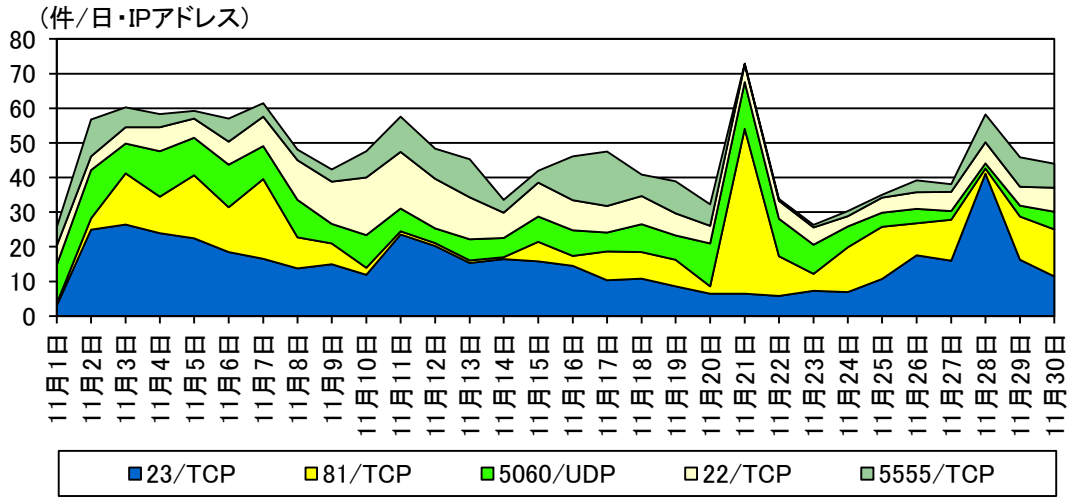

図 3-13　オランダからの上位5ポートの検知件数の推移

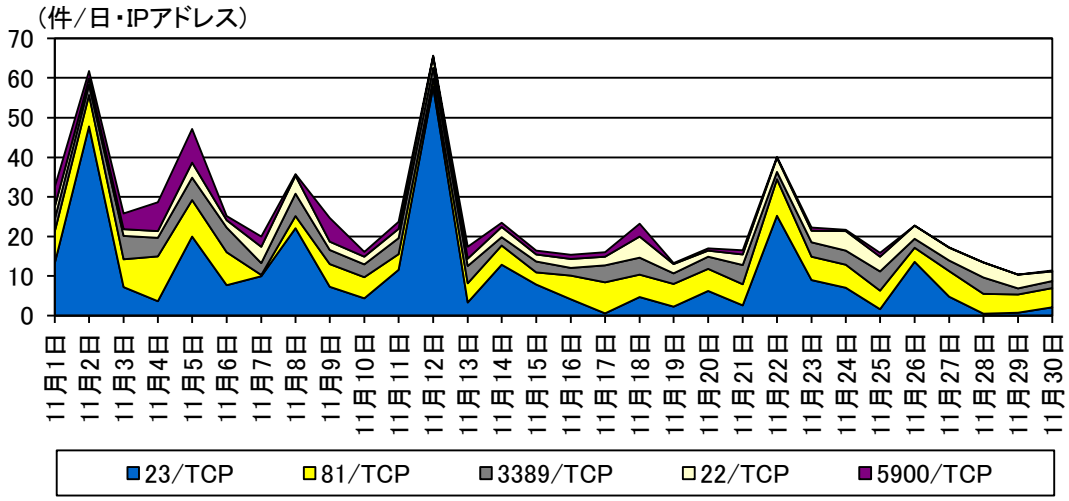

図 3-14 ドイツからの上位5ポートの検知件数の推移

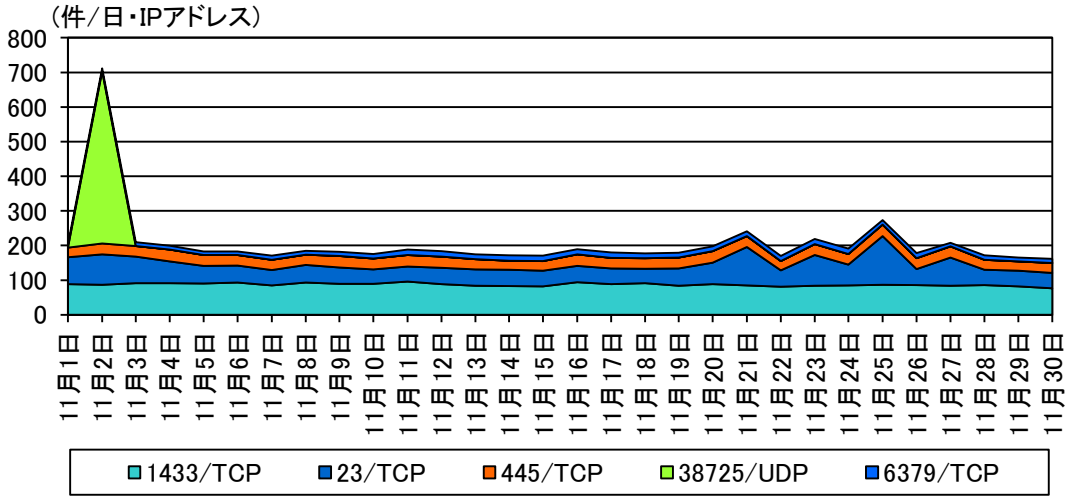

図 3-15 中国からの上位5ポートの検知件数の推移

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	INDICATOR-SCAN	543.73 件	＋62.7%　（＋209.44 件）	1 位	
2 位	1 位	Microsoft Windows Terminal server	258.81 件	－25.2%　（－87.17 件）		1 位
3 位	3 位	SMBv1	150.79 件	－3.8%　（－5.96 件）		3 位
4 位	5 位	SERVER-APACHE	46.42 件	－8.6%　（－4.39 件）		4 位
5 位	6 位	ICMP	29.06 件	＋7.0%　（＋1.89 件）	3 位	

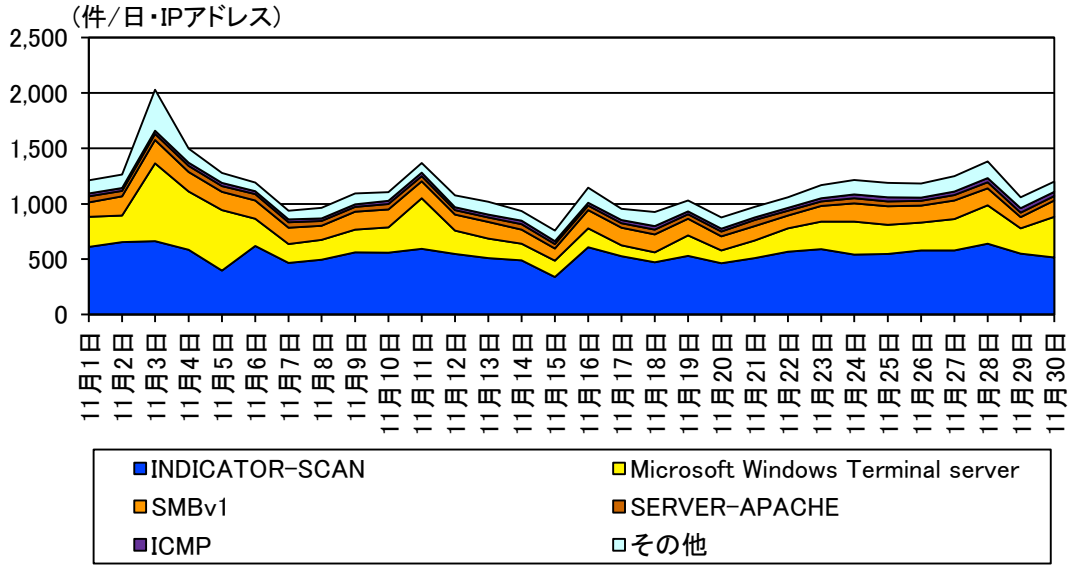

図 4-1　不正侵入等の攻撃手法別検知件数の推移

[i] 一日・1IP アドレス当たり。

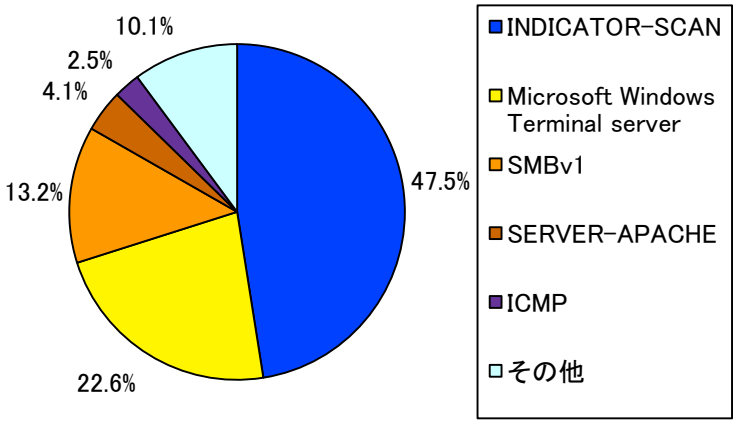

図 4-2 不正侵入等の攻撃手法別検知比率

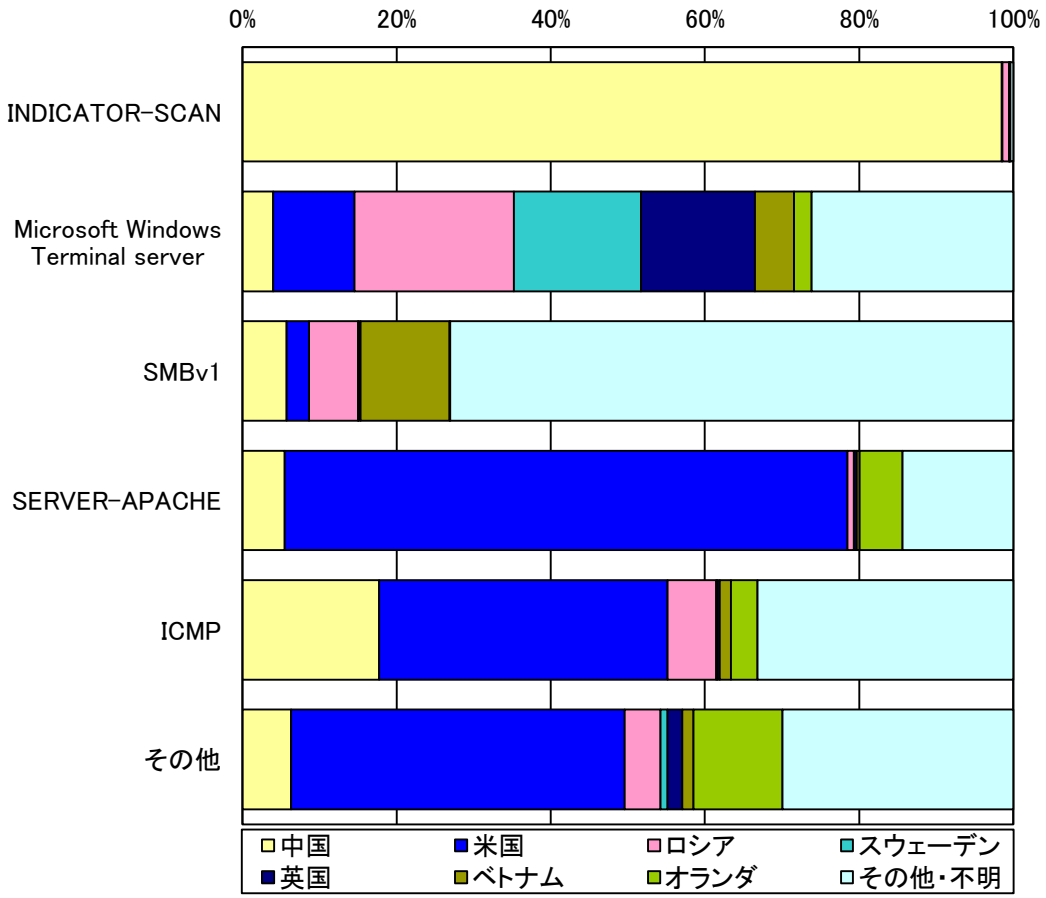

図 4-3 不正侵入等の攻撃手法の送信元国・地域別検知比率

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	569.53 件	＋57.9% （＋208.87 件）
2 位	2 位	米国	127.19 件	－14.8% （－22.13 件）
3 位	3 位	ロシア	75.40 件	－25.6% （－25.97 件）
4 位	70 位	スウェーデン	43.74 件	－[ii] （＋43.47 件）
5 位	18 位	英国	41.24 件	＋402.4% （＋33.03 件）

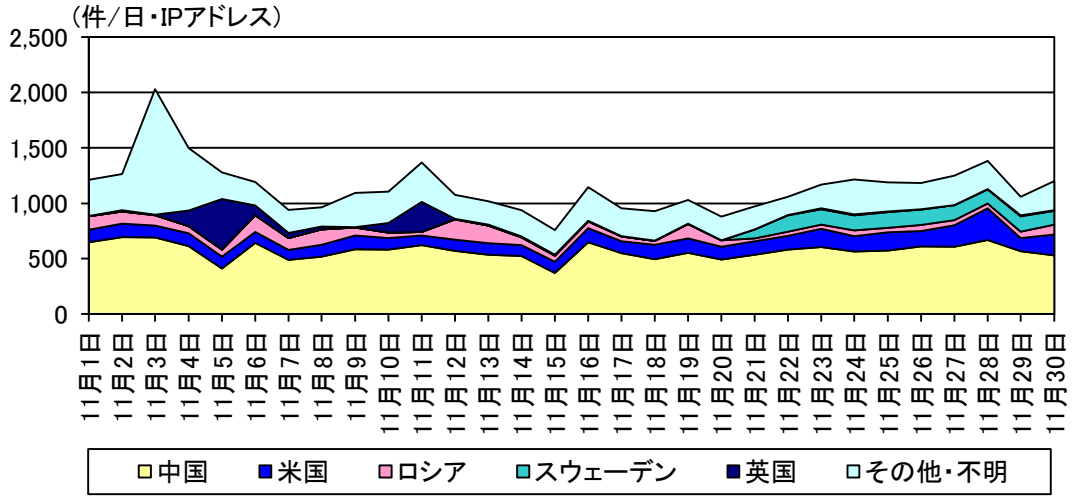

図 4-4 不正侵入等の送信元国・地域別検知件数の推移

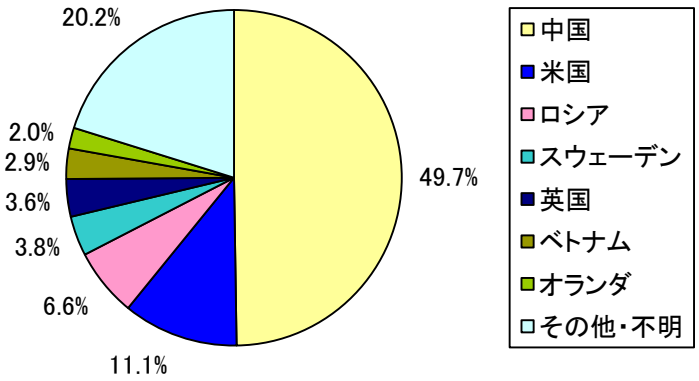

図 4-5 不正侵入等の送信元国・地域別検知比率

[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。

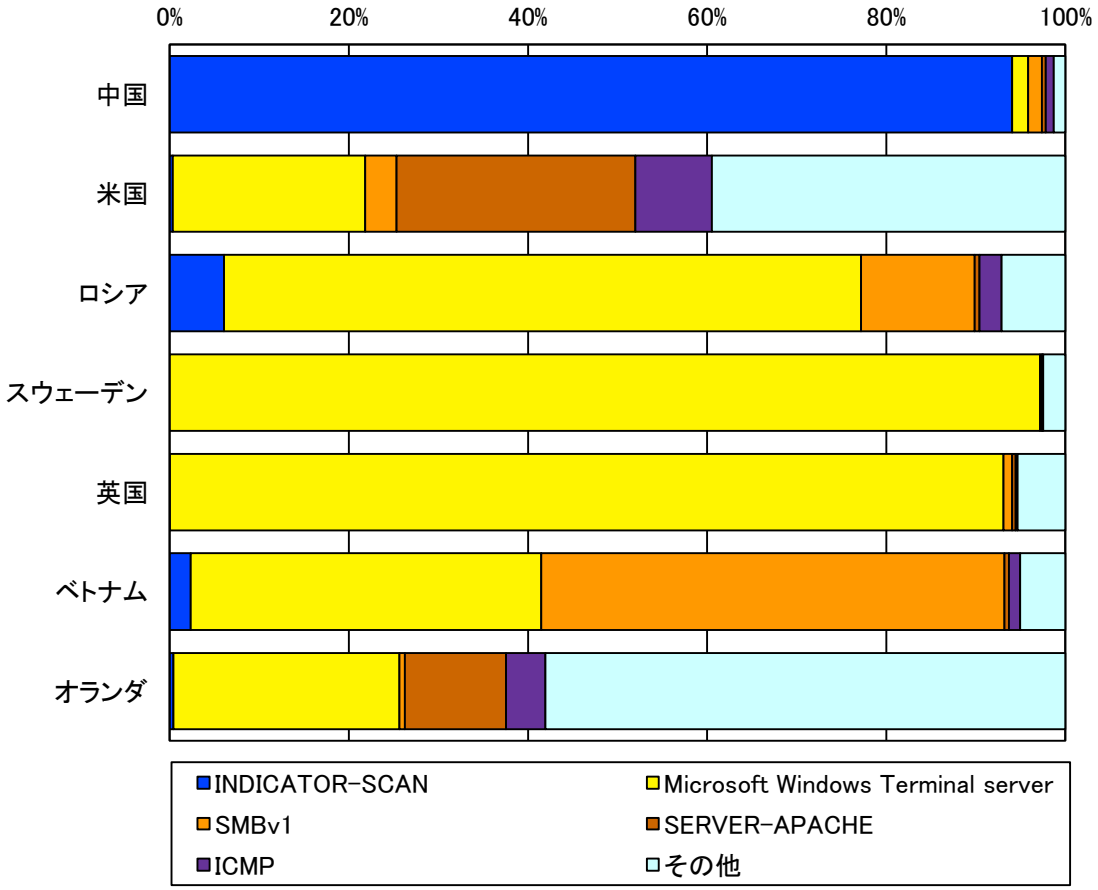

図 4-6 不正侵入等の送信元国・地域別上位の攻撃手法別検知比率

5　DoS 攻撃被害の観測結果

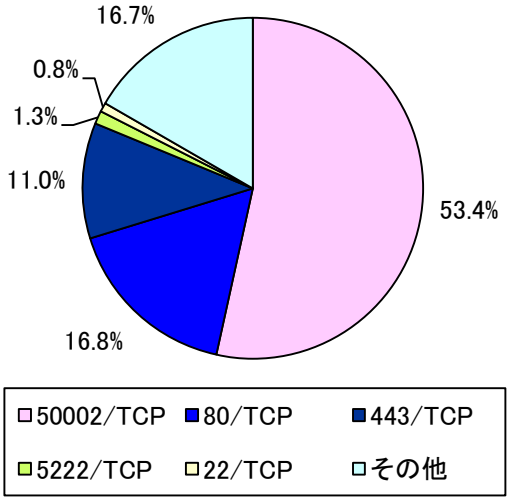

図 5-1　跳ね返りパケット送信元ポート別比率

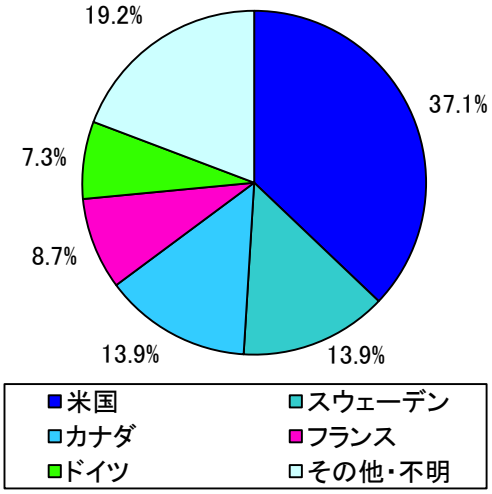

図 5-2　跳ね返りパケット送信元国・地域別比率