令和３年３月 30 日

令和3年2月期観測資料

1　観測結果概要

令和3年2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 5,438.3 件で、令和3年1月期（以下「前月期」という。）の 6,531.8 件と比較して 1,093.5 件（16.7%）減少しました。また、送信元 IP アドレス[i] 数は、一日当たり 45,808.0 個で、前月期の 49,522.1 個と比較して 3,714.1 個（7.5%）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 1,071.4 件で、前月期の 1,312.1 件と比較して 240.7 件（18.3%）減少しました。また、送信元 IP アドレス数は、一日当たり 12,048.1 個で、前月期の 12,514.3 個と比較して 466.2 個（3.7%）減少しました。

DoS 攻撃被害検知件数は、一日当たり 13,283.3 件で、前月期の 19,854.2 件と比較して 6,570.9 件（33.1%）減少しました。また、送信元 IP アドレス数は、一日当たり 684.9 個で、前月期の 685.9 個と比較して 1.0 個（0.1%）減少しました。

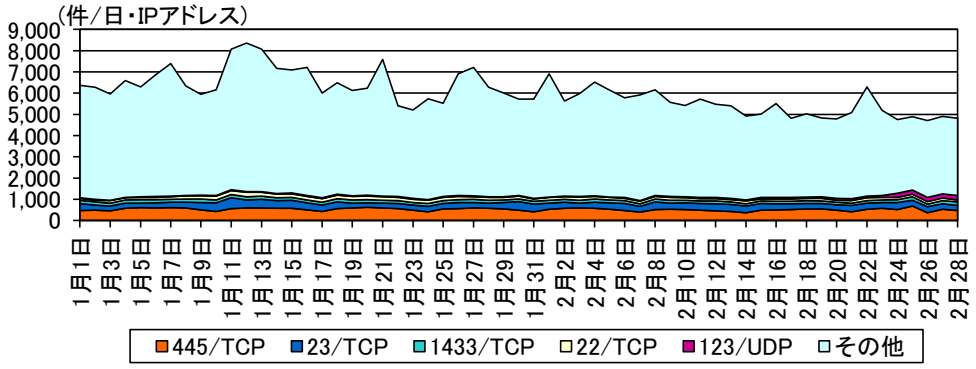

図 1-1　宛先ポート別検知件数の推移

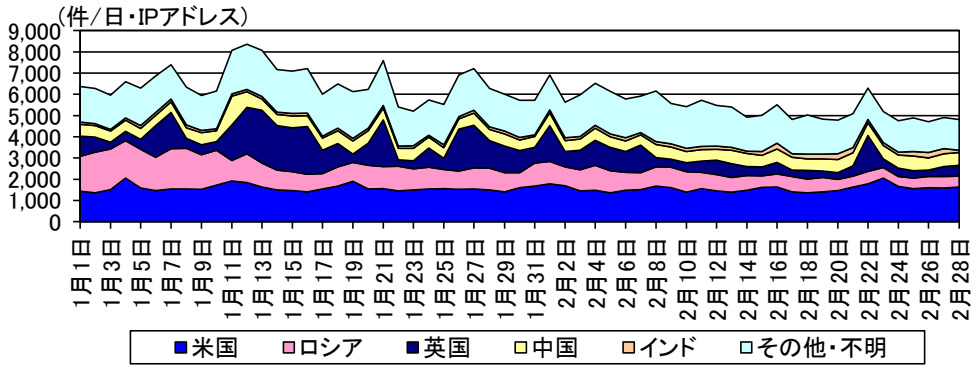

図 1-2　送信元国・地域別検知件数の推移 [ii]

[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　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	507.14 件	－5.8%　（－31.17 件）
2 位	2 位	23/TCP	293.09 件	－2.5%　（－7.40 件）
3 位	3 位	1433/TCP	127.95 件	－11.5%　（－16.58 件）
4 位	4 位	22/TCP	113.88 件	－20.6%　（－29.53 件）
5 位	13 位	123/UDP	81.95 件	＋155.0%　（＋49.81 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	123/UDP	81.95 件	＋155.0%　（＋49.81 件）	5 位	13 位
2 位	53/UDP	57.37 件	＋211.7%　（＋38.96 件）	7 位	21 位
3 位	0/TCP	44.18 件	＋148.3%　（＋26.39 件）	10 位	22 位
4 位	8291/TCP	35.41 件	＋43.2%　（＋10.67 件）	14 位	17 位
5 位	26/TCP	13.92 件	＋309.4%　（＋10.52 件）	30 位	118 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	52869/TCP	22.36 件	－60.6%　（－34.37 件）	21 位	6 位
2 位	445/TCP	507.14 件	－5.8%　（－31.17 件）	1 位	1 位
3 位	22/TCP	113.88 件	－20.6%　（－29.53 件）	4 位	4 位
4 位	1433/TCP	127.95 件	－11.5%　（－16.58 件）	3 位	3 位
5 位	8545/TCP	8.07 件	－58.2%　（－11.22 件）	48 位	20 位

[i] 一日・1IP アドレス当たり。

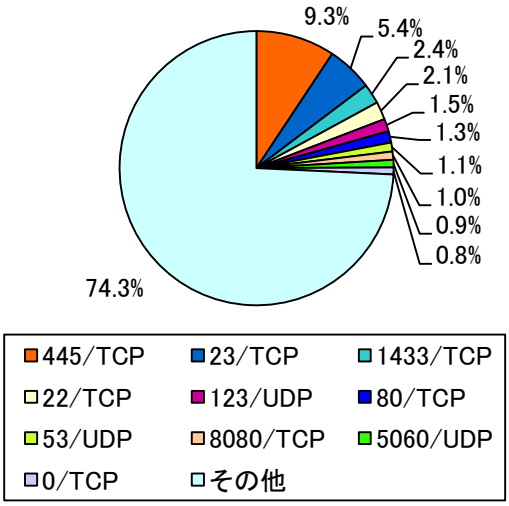

図 3-1　宛先ポート別比率（全て）[i]

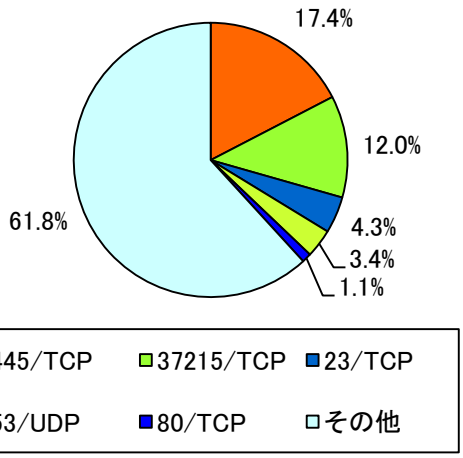

図 3-2　宛先ポート別比率（日本国内）

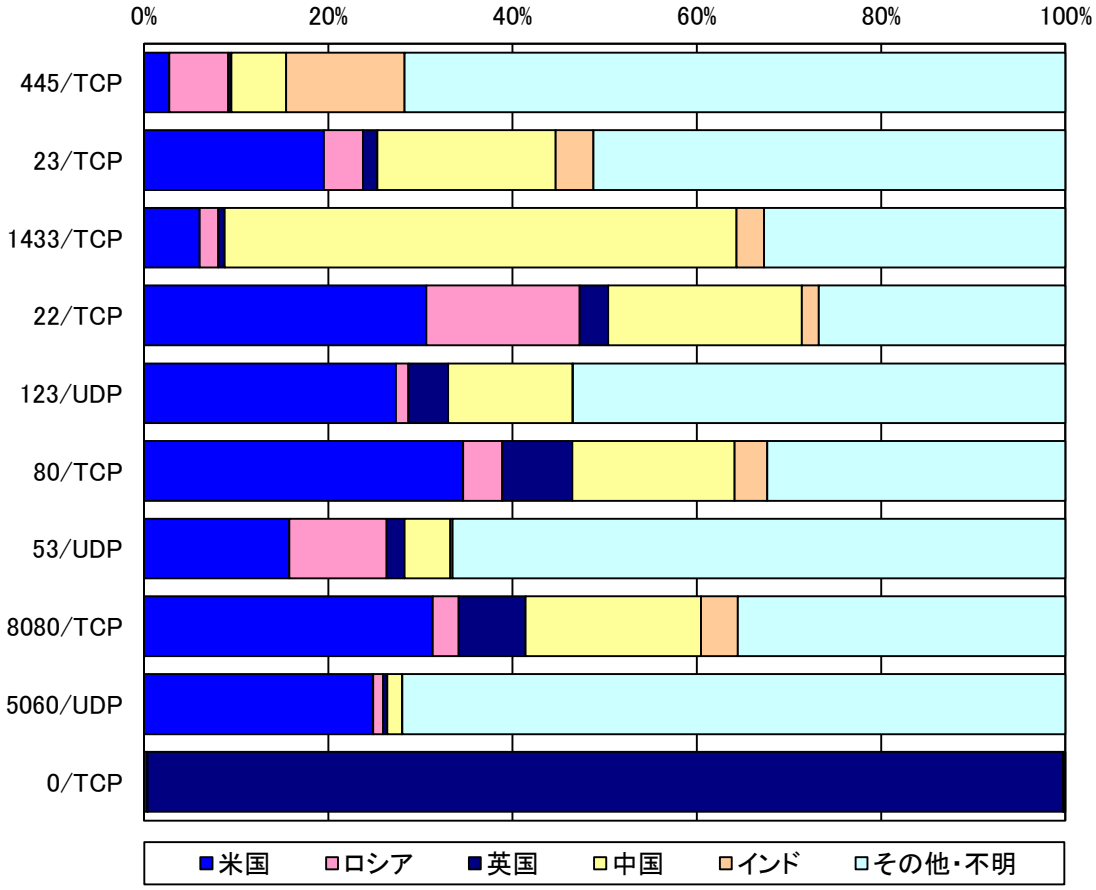

図 3-3　宛先ポート別上位の送信元国・地域別比率

[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。

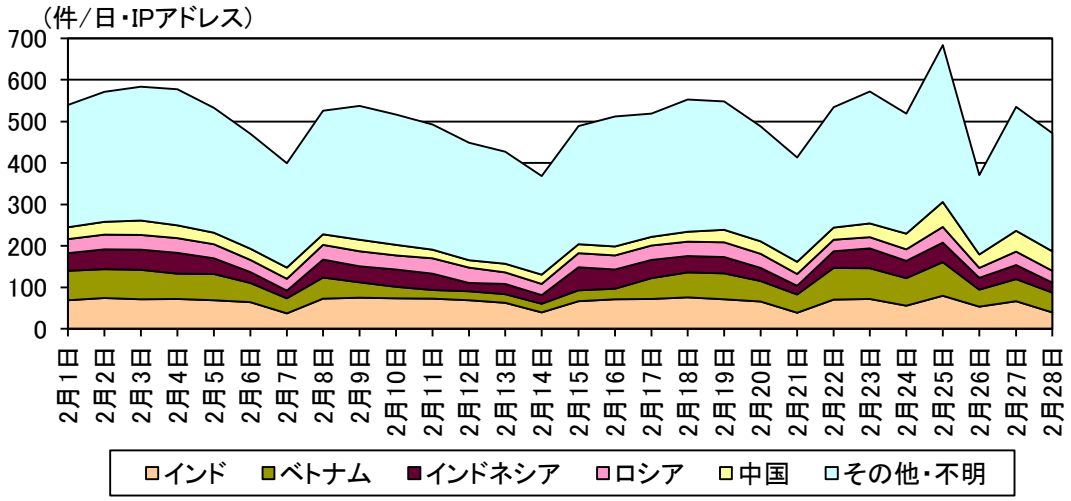

図 3-4　センサーのポート 445/TCP における検知件数の推移

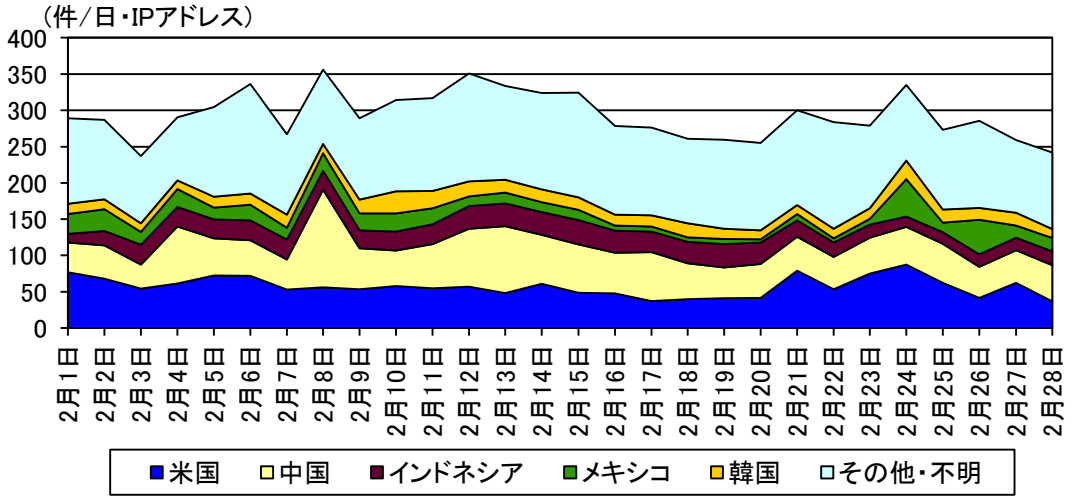

図 3-5　センサーのポート 23/TCP における検知件数の推移

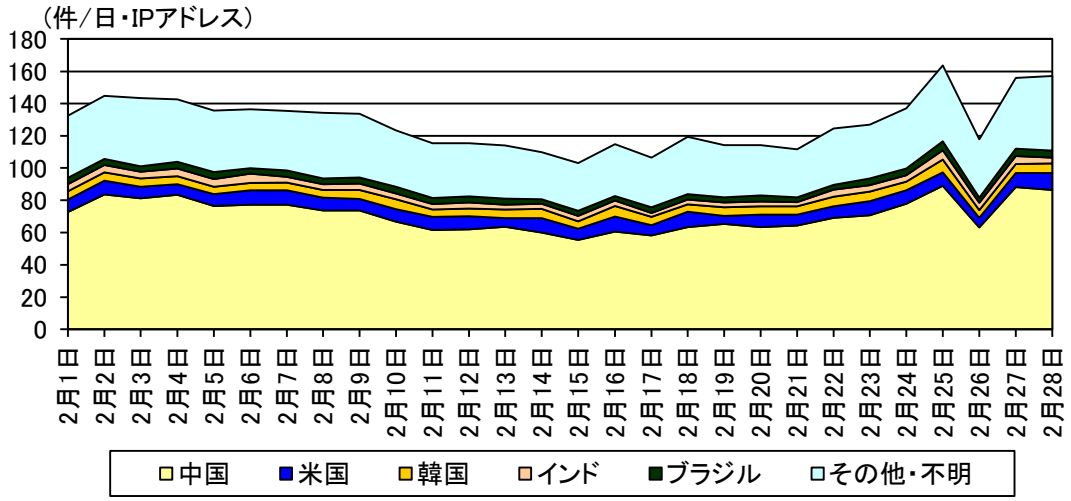

図 3-6　センサーのポート 1433/TCP における検知件数の推移

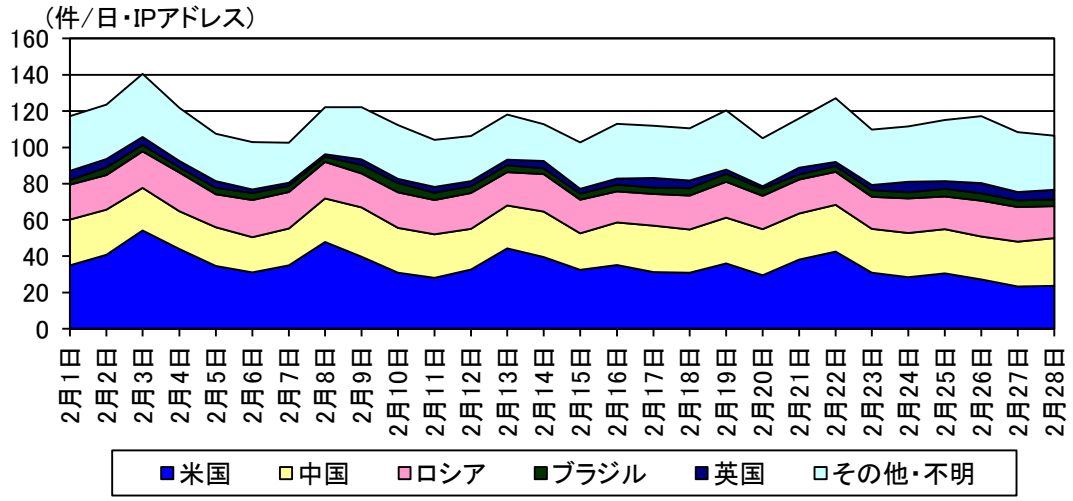

図 3-7　センサーのポート 22/TCP における検知件数の推移

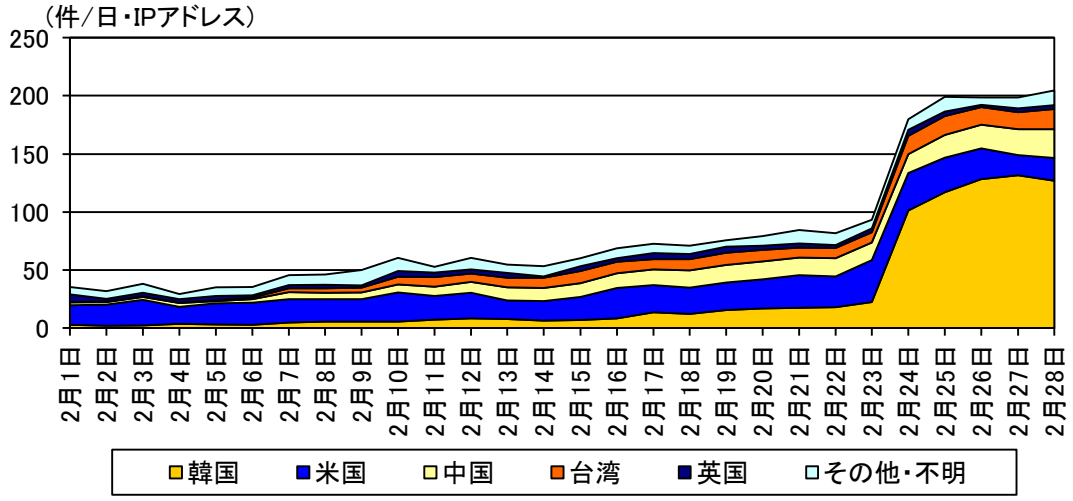

図 3-8　センサーのポート 123/UDP における検知件数の推移

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	1,560.38 件	－1.4%　（－21.60 件）
2 位	2 位	ロシア	733.82 件	－40.5%　（－499.37 件）
3 位	3 位	英国	654.23 件	－44.4%　（－521.61 件）
4 位	4 位	中国	578.96 件	＋1.0%　（＋5.72 件）
5 位	8 位	インド	167.31 件	＋50.8%　（＋56.35 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	インド	167.31 件	＋50.8%　（＋56.35 件）	5 位	8 位
2 位	ポーランド	83.37 件	＋80.6%　（＋37.20 件）	12 位	17 位
3 位	ベリーズ	71.33 件	＋95.4%　（＋34.83 件）	14 位	22 位
4 位	ドイツ	92.45 件	＋59.5%　（＋34.50 件）	10 位	12 位
5 位	韓国	78.43 件	＋74.7%　（＋33.53 件）	13 位	19 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	英国	654.23 件	－44.4%　（－521.61 件）	3 位	3 位
2 位	ロシア	733.82 件	－40.5%　（－499.37 件）	2 位	2 位
3 位	ブルガリア	136.35 件	－47.0%　（－120.85 件）	7 位	5 位
4 位	ウクライナ	89.43 件	－49.7%　（－88.47 件）	11 位	6 位
5 位	南アフリカ	9.85 件	－72.0%　（－25.33 件）	37 位	23 位

[i] 一日・1IP アドレス当たり。

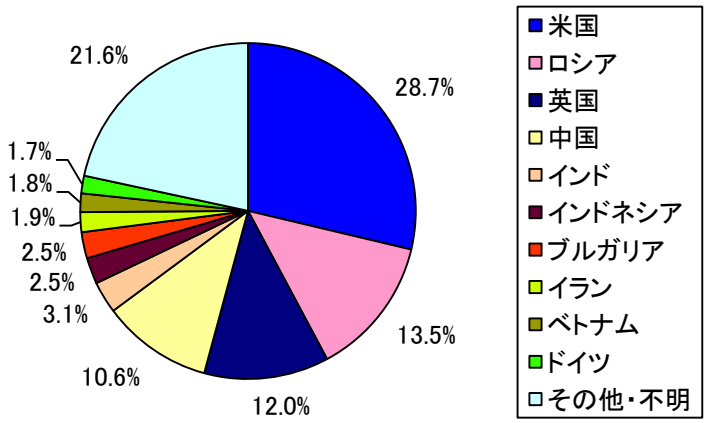

図 3-9　送信元国・地域別比率

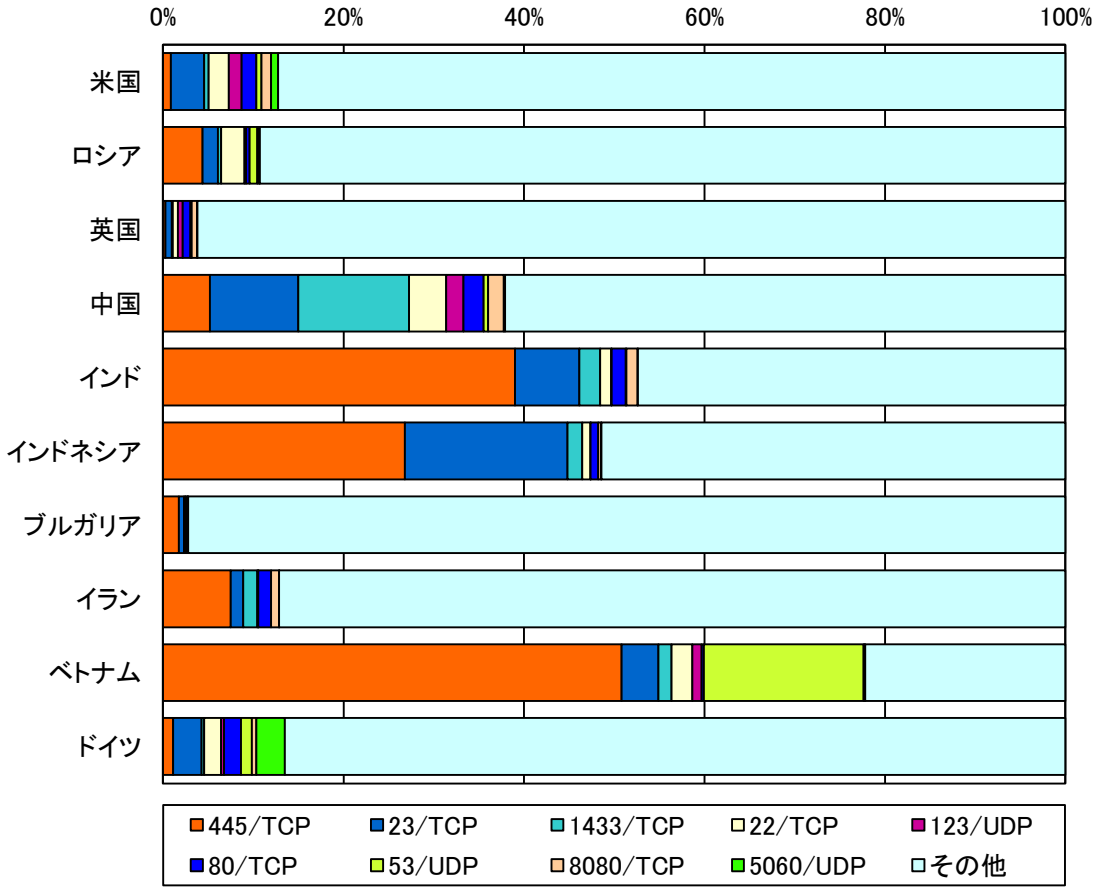

図 3-10　送信元国・地域別上位の宛先ポート別比率

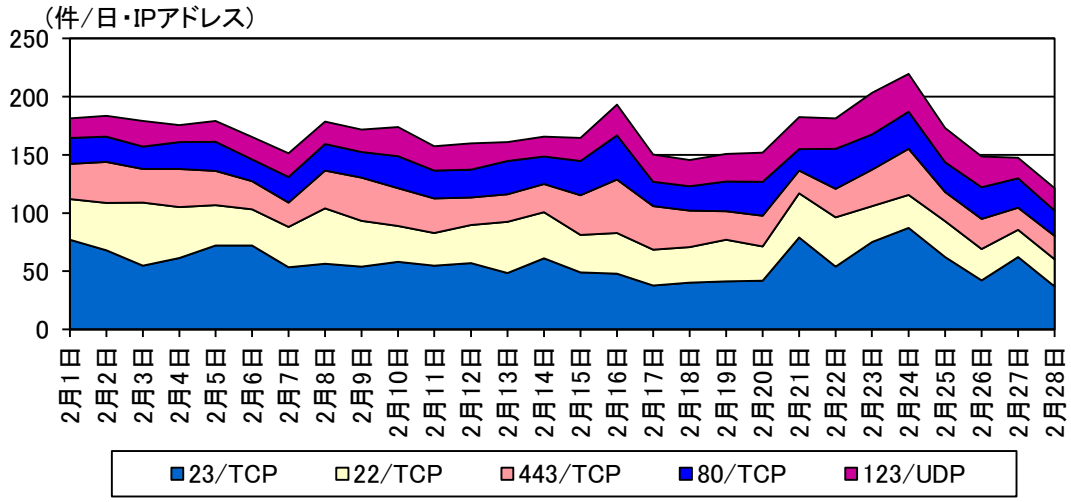

図 3-11　米国からの上位5ポートの検知件数の推移

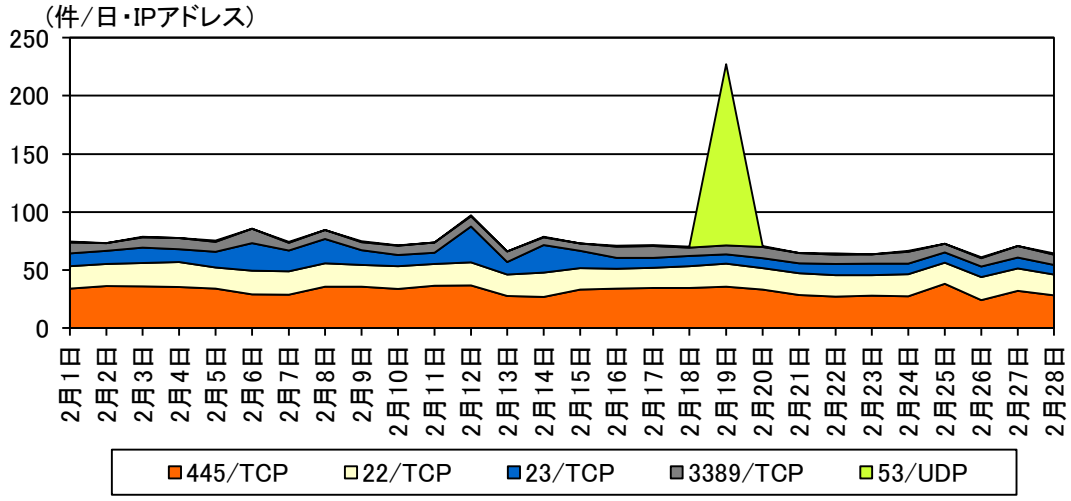

図 3-12　ロシアからの上位5ポートの検知件数の推移

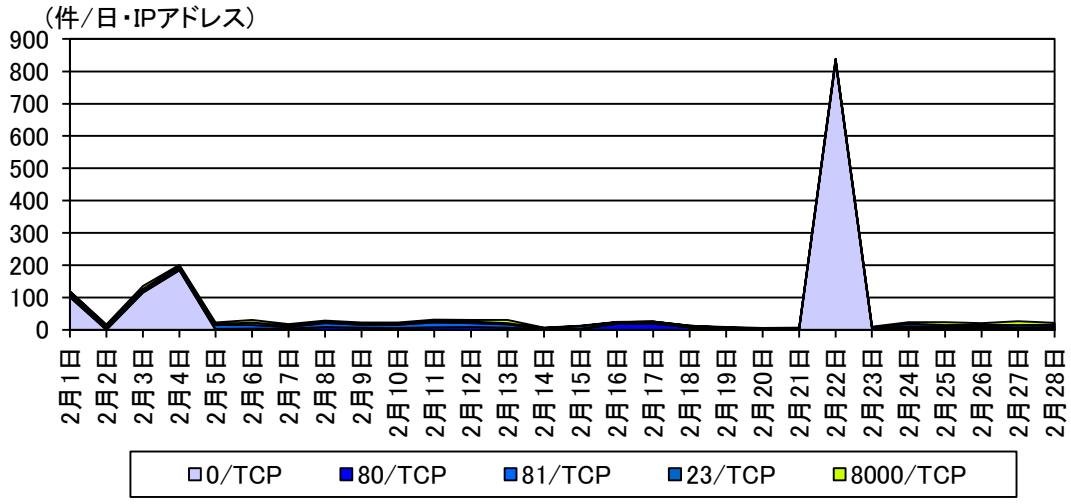

図 3-13　英国からの上位5ポートの検知件数の推移

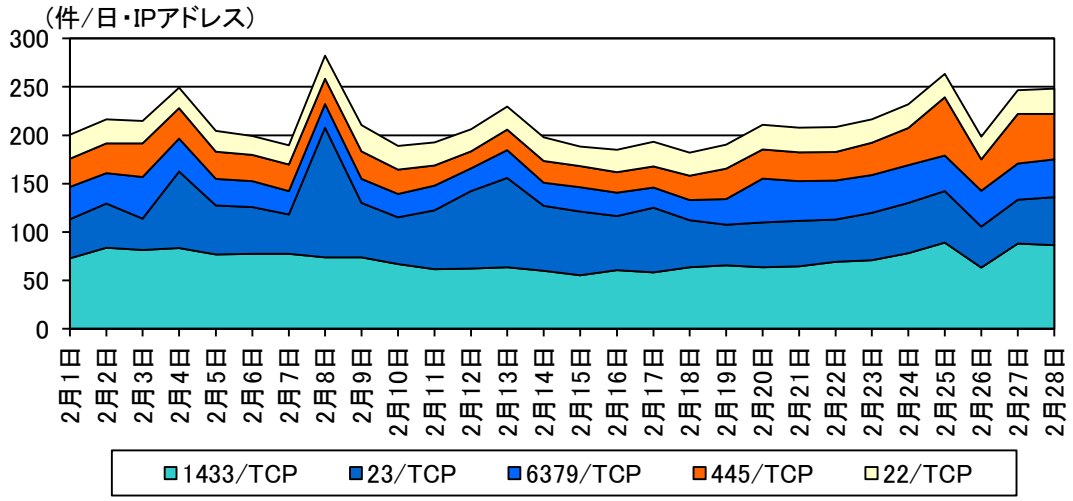

図 3-14　中国からの上位5ポートの検知件数の推移

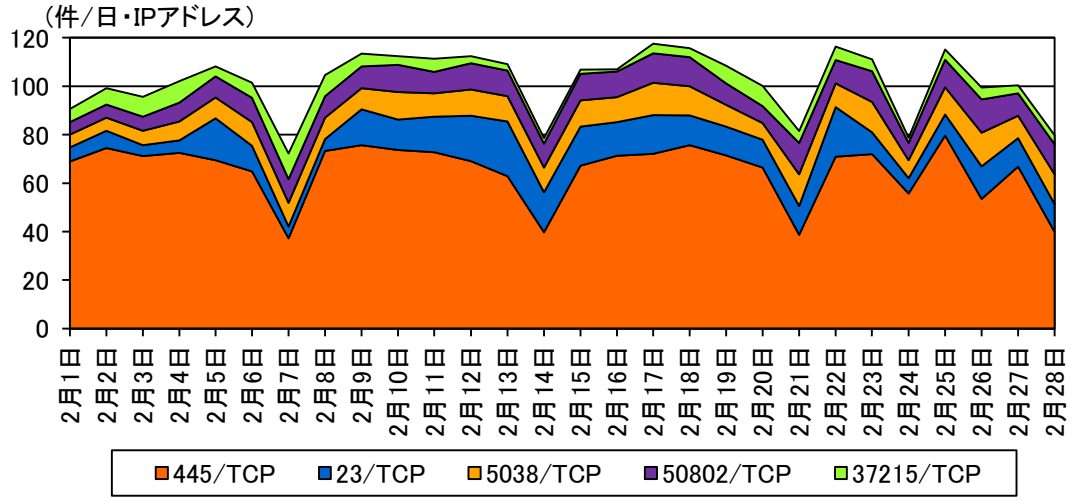

図 3-15　インドからの上位5ポートの検知件数の推移

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	509.25 件	＋10.1%　（＋46.57 件）	1 位	
2 位	3 位	SMBv1	206.41 件	－0.1%　（－0.25 件）		
3 位	2 位	Microsoft Windows Terminal server	149.72 件	－64.1%　（－266.86 件）		1 位
4 位	4 位	SERVER-APACHE	47.04 件	－0.4%　（－0.20 件）		
5 位	6 位	ICMP	31.86 件	＋10.8%　（＋3.09 件）	4 位	

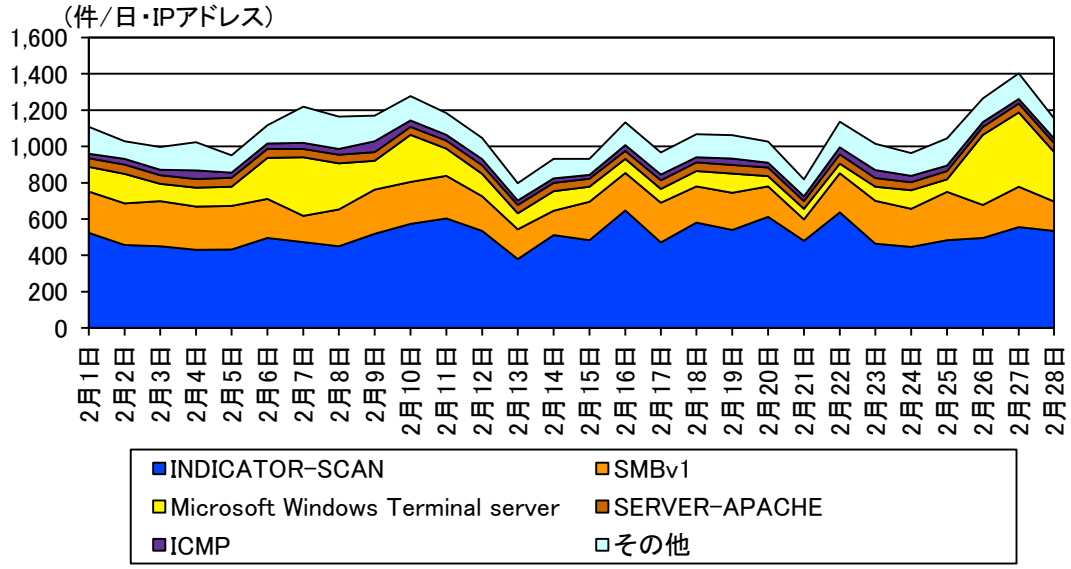

図 4-1　不正侵入等の攻撃手法別検知件数の推移

[i] 一日・1IP アドレス当たり。

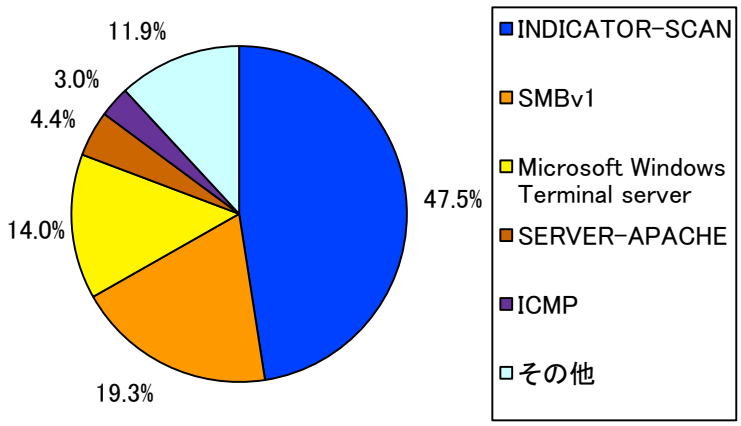

図 4-2 不正侵入等の攻撃手法別検知比率

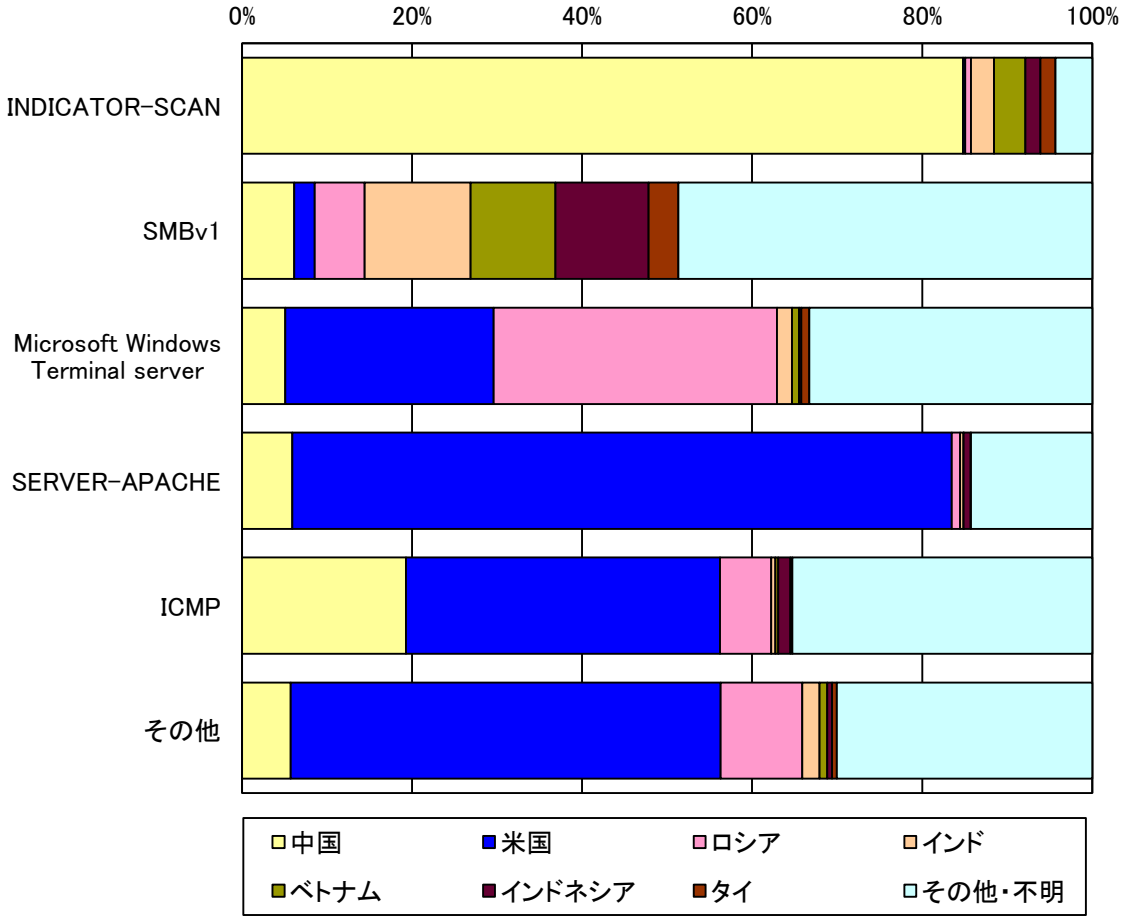

図 4-3 不正侵入等の攻撃手法の送信元国・地域別検知比率

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	468.30 件	＋8.0% （＋34.66 件）
2 位	2 位	米国	155.56 件	＋4.8% （＋7.15 件）
3 位	3 位	ロシア	80.23 件	－15.3% （－14.53 件）
4 位	5 位	インド	44.89 件	－28.9% （－18.23 件）
5 位	6 位	ベトナム	42.03 件	－32.9% （－20.57 件）

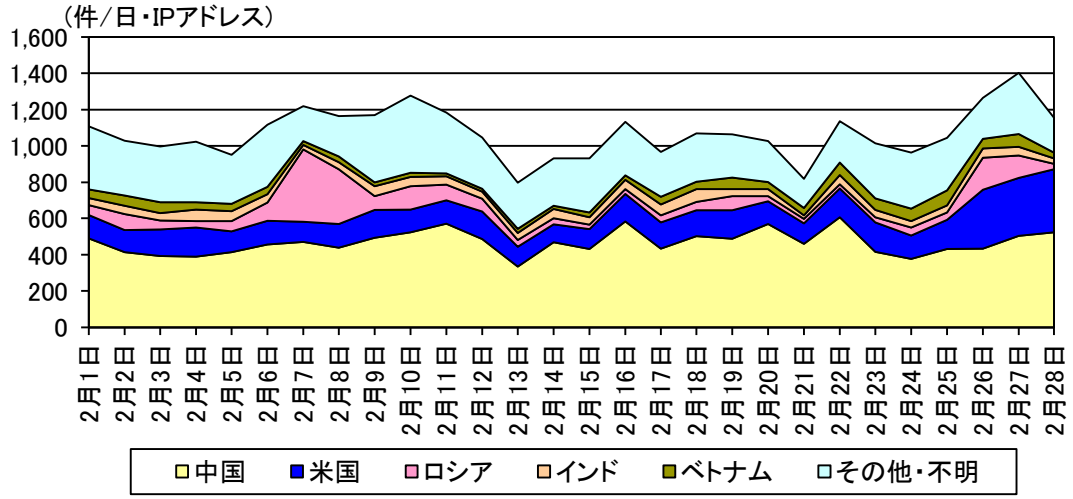

図 4-4 不正侵入等の送信元国・地域別検知件数の推移

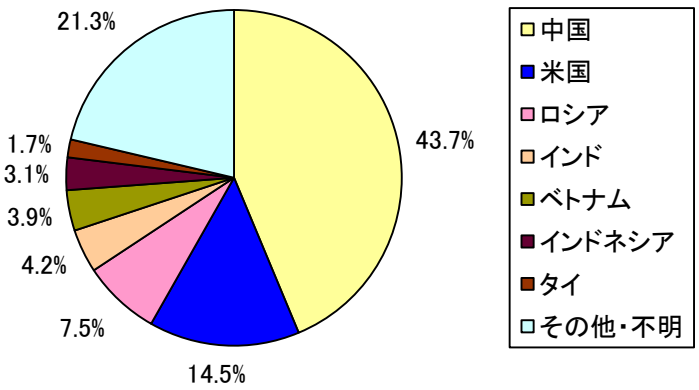

図 4-5 不正侵入等の送信元国・地域別検知比率

[i] 一日・1IP アドレス当たり。

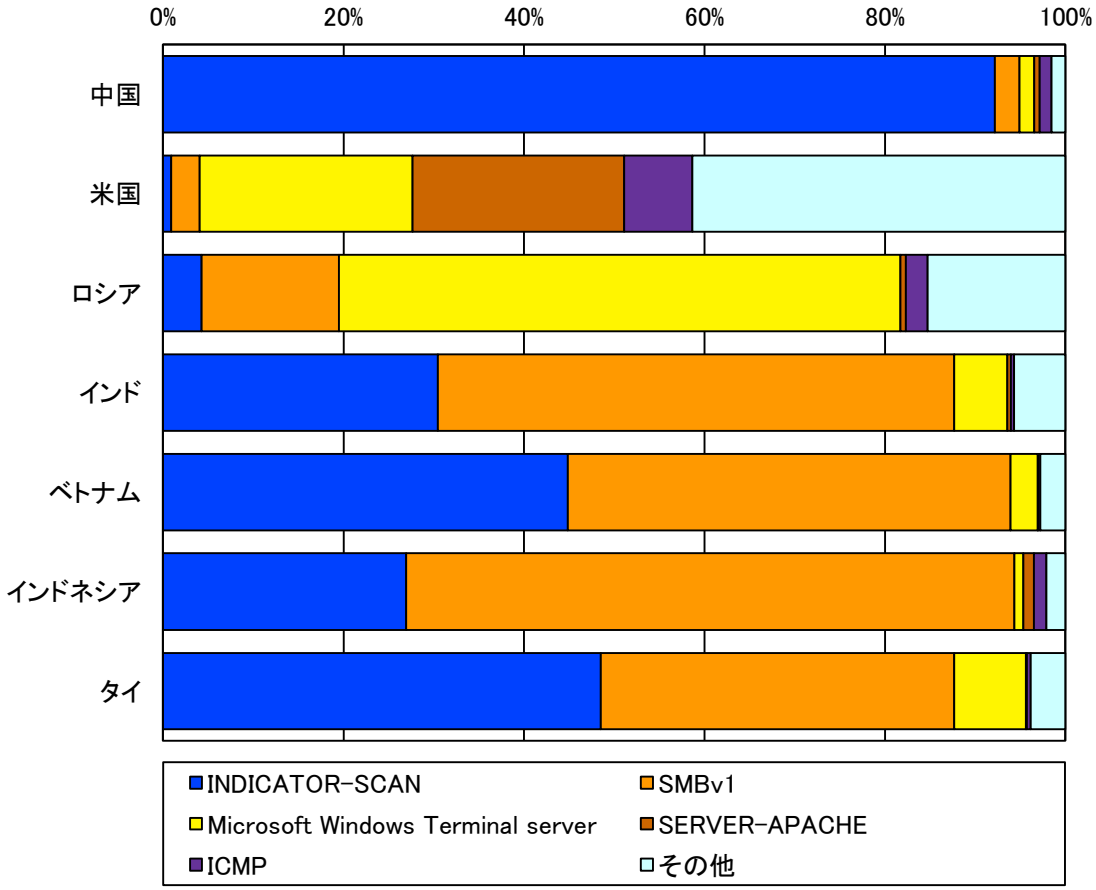

図 4-6 不正侵入等の送信元国・地域別上位の攻撃手法別検知比率

5　DoS 攻撃被害の観測結果

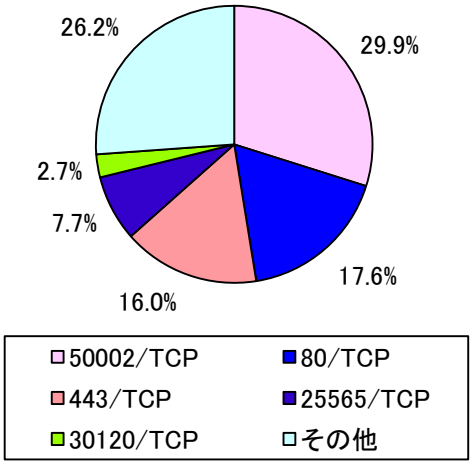

図 5-1　跳ね返りパケット送信元ポート別比率

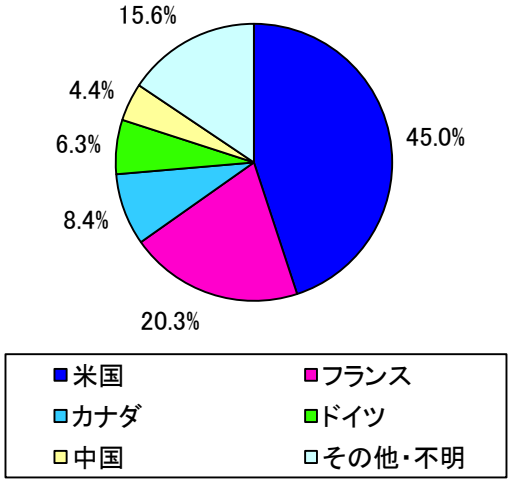

図 5-2　跳ね返りパケット送信元国・地域別比率