平成 31 年2月 1日

平成 30 年 12 月期観測資料

1　観測結果概要

平成 30 年 12 月期(以下「今期」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 3,994.6 件で、平成 30 年 11 月期(以下「前期」という。)と比較して 696.2 件(21.1 %)増加しました。また、発信元 IP アドレス数は、一日当たり 50,599.7 個で、前期と比較して 3,333.5 個(7.1 %)増加しました。

DoS 攻撃被害検知件数は、一日当たり 10,942.3 件で、前期と比較して 5,926.3 件(118.1 %)増加しました。また、発信元 IP アドレス数は、一日当たり 317.5 個で、前期と比較して 20.6 個(6.1 %)減少しました。

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（今期順位）

今期順位	前期順位	ポート	今期件数[i]	前期比[i]
1 位	1 位	23/TCP	393.91 件	＋5.5%　（＋20.64 件）
2 位	2 位	445/TCP	339.33 件	＋37.3%　（＋92.27 件）
3 位	3 位	1433/TCP	154.73 件	＋76.8%　（＋67.19 件）
4 位	17 位	8545/TCP	96.23 件	＋437.9%　（＋78.34 件）
5 位	8 位	52869/TCP	86.08 件	＋97.6%　（＋42.52 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	今期件数[i]	前期比[i]	今期順位	前期順位
1 位	445/TCP	339.33 件	＋37.3%　（＋92.27 件）	2 位	2 位
2 位	8545/TCP	96.23 件	＋437.9%　（＋78.34 件）	4 位	17 位
3 位	1433/TCP	154.73 件	＋76.8%　（＋67.19 件）	3 位	3 位
4 位	52869/TCP	86.08 件	＋97.6%　（＋42.52 件）	5 位	8 位
5 位	23/TCP	393.91 件	＋5.5%　（＋20.64 件）	1 位	1 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	今期件数[i]	前期比[i]	今期順位	前期順位
1 位	53413/UDP	26.80 件	－21.6%　（－7.37 件）	14 位	10 位
2 位	3389/TCP	30.56 件	－13.1%　（－4.59 件）	10 位	9 位
3 位	8088/TCP	17.22 件	－15.4%　（－3.14 件）	19 位	15 位
4 位	5431/TCP	5.14 件	－36.2%　（－2.92 件）	37 位	28 位
5 位	8080/TCP	47.96 件	－5.5%　（－2.79 件）	9 位	7 位

[i] 一日・1IP アドレス当たり。

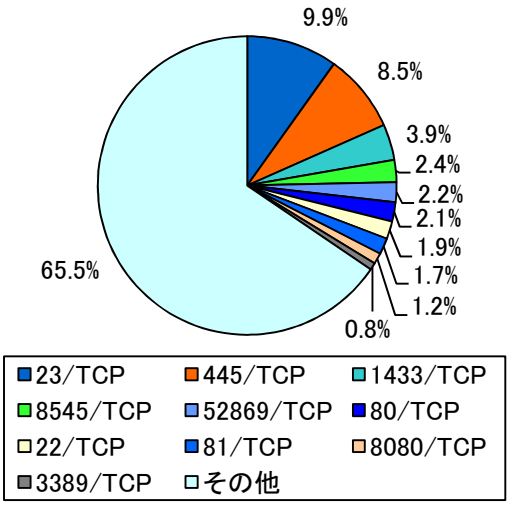

図 2-1　宛先ポート別比率（全て）[i]

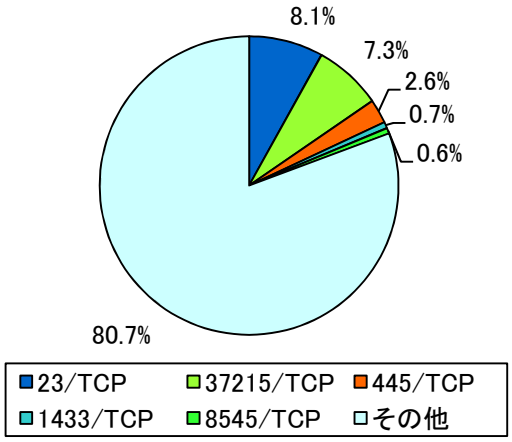

図 2-2　宛先ポート別比率（日本国内）[i]

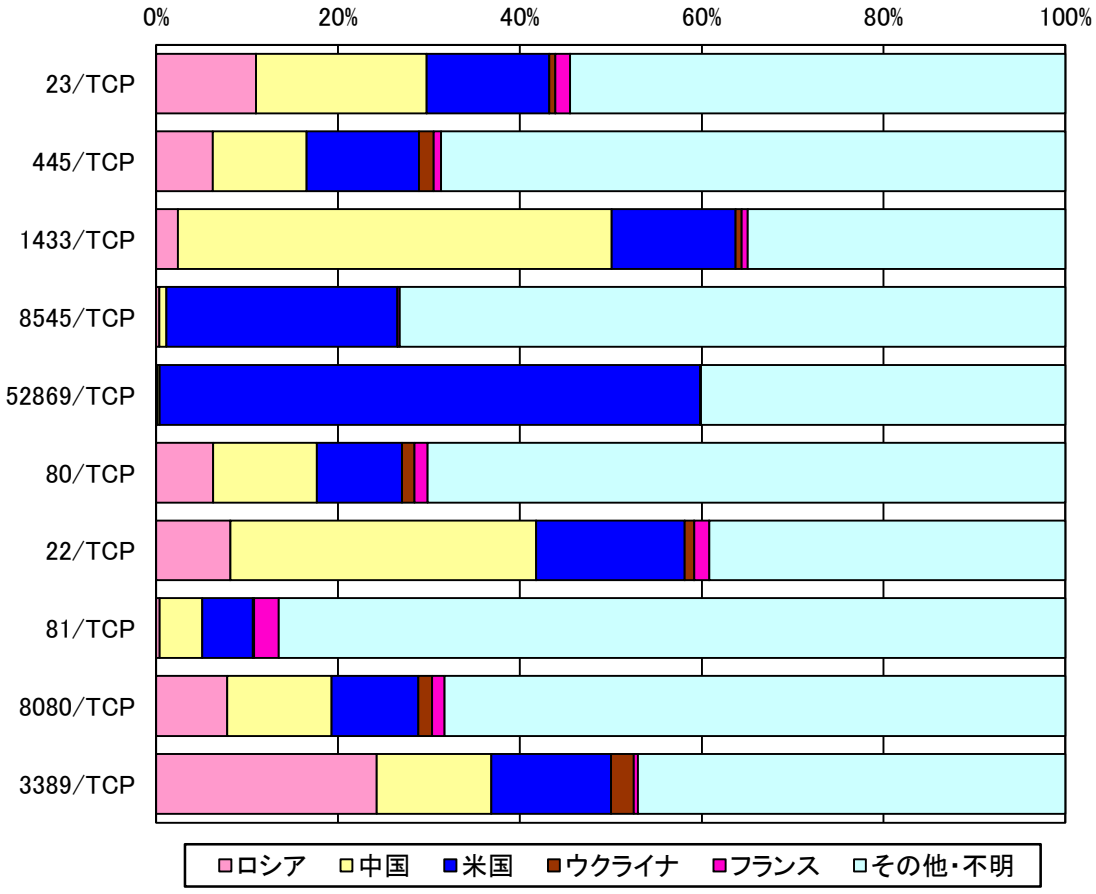

図 2-3　宛先ポート別上位の発信元国・地域別比率 [ii]

[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。

[ii] 発信元の国・地域については、当該国・地域に割り当てられた IP アドレスを指しています。以降も同様の表記です。

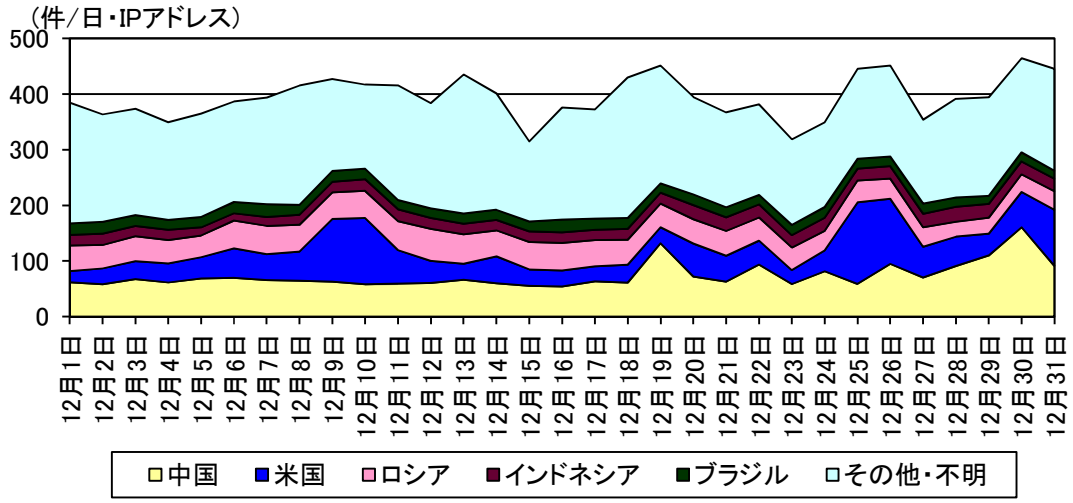

図 2-4　センサーのポート 23/TCP における検知件数の推移

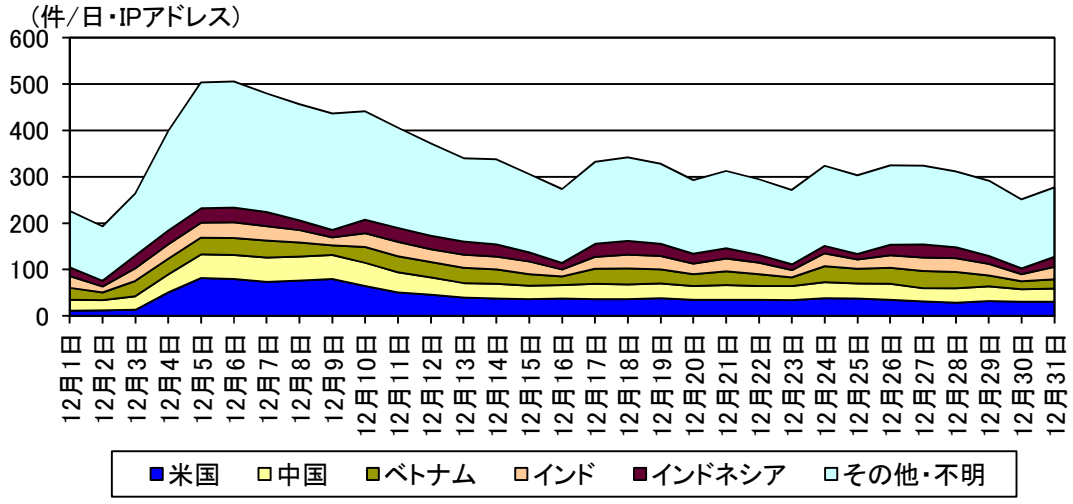

図 2-5　センサーのポート 445/TCP における検知件数の推移

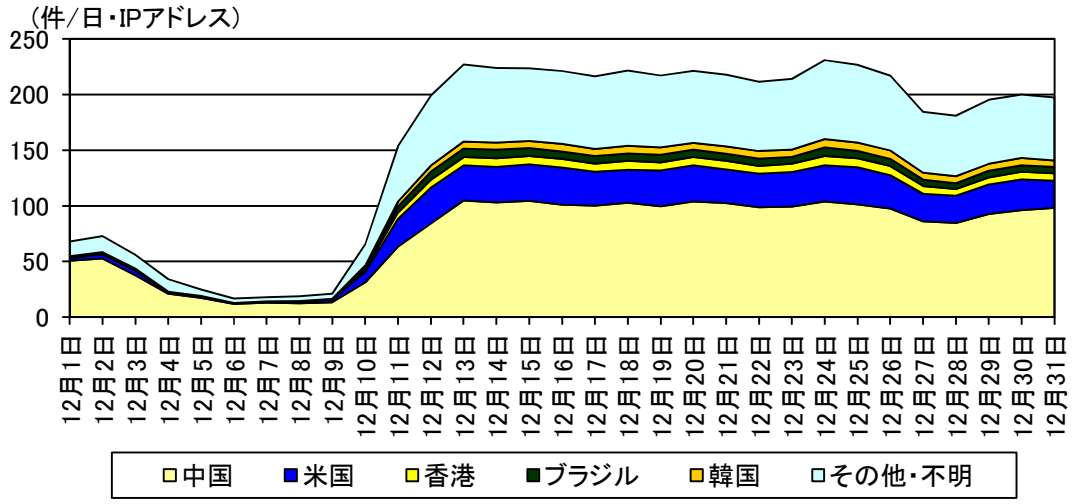

図 2-6　センサーのポート 1433/TCP における検知件数の推移

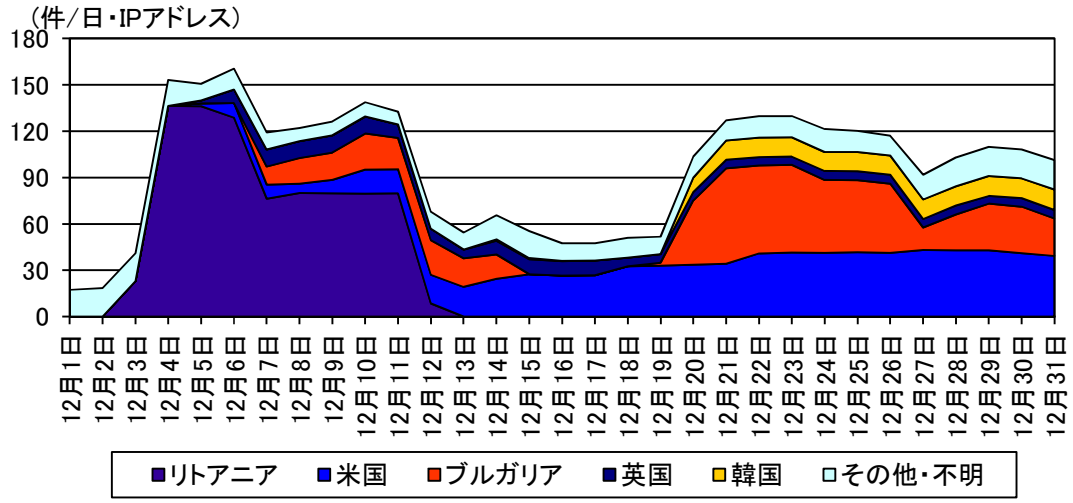

図 2-7　センサーのポート 8545/TCP における検知件数の推移

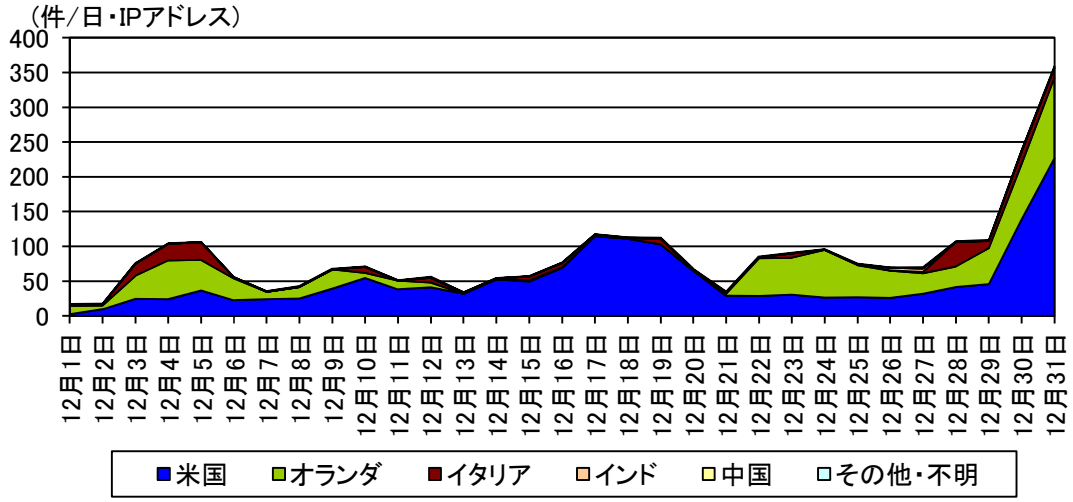

図 2-8　センサーのポート 52869/TCP における検知件数の推移

2-2　発信元国・地域別アクセス検知件数

表 2-4　発信元国・地域別検知件数（今期順位）

今期順位	前期順位	国・地域	今期件数 [i]	前期比 [i]
1 位	1 位	ロシア	740.92 件	＋1.6%　（＋11.90 件）
2 位	4 位	中国	517.04 件	＋37.0%　（＋139.72 件）
3 位	3 位	米国	498.28 件	＋30.7%　（＋116.93 件）
4 位	2 位	ウクライナ	490.25 件	＋9.9%　（＋44.00 件）
5 位	5 位	フランス	196.00 件	＋15.3%　（＋25.97 件）

表 2-5　発信元国・地域別検知件数（増加順位）

増加順位	国・地域	今期件数 [i]	前期比 [i]	今期順位	前期順位
1 位	リトアニア	151.24 件	＋7496.1%　（＋149.25 件）	7 位	56 位
2 位	中国	517.04 件	＋37.0%　（＋139.72 件）	2 位	4 位
3 位	米国	498.28 件	＋30.7%　（＋116.93 件）	3 位	3 位
4 位	日本	100.00 件	＋298.6%　（＋74.91 件）	9 位	19 位
5 位	ウクライナ	490.25 件	＋9.9%　（＋44.00 件）	4 位	2 位

表 2-6　発信元国・地域別検知件数（減少順位）

減少順位	国・地域	今期件数 [i]	前期比 [i]	今期順位	前期順位
1 位	ブルガリア	63.89 件	－21.5%　（－17.54 件）	13 位	8 位
2 位	メキシコ	17.12 件	－43.1%　（－12.98 件）	26 位	18 位
3 位	パナマ	3.69 件	－63.6%　（－6.46 件）	51 位	31 位
4 位	セーシェル	4.54 件	－36.5%　（－2.61 件）	49 位	38 位
5 位	パキスタン	8.30 件	－17.1%　（－1.72 件）	36 位	32 位

[i] 一日・1IP アドレス当たり。

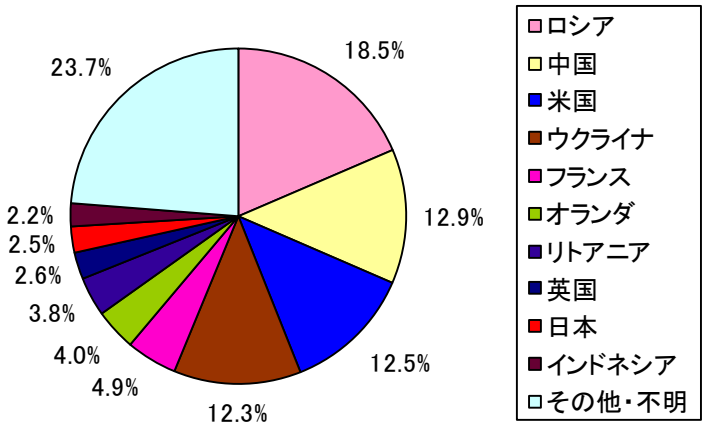

図 2-9　発信元国・地域別比率

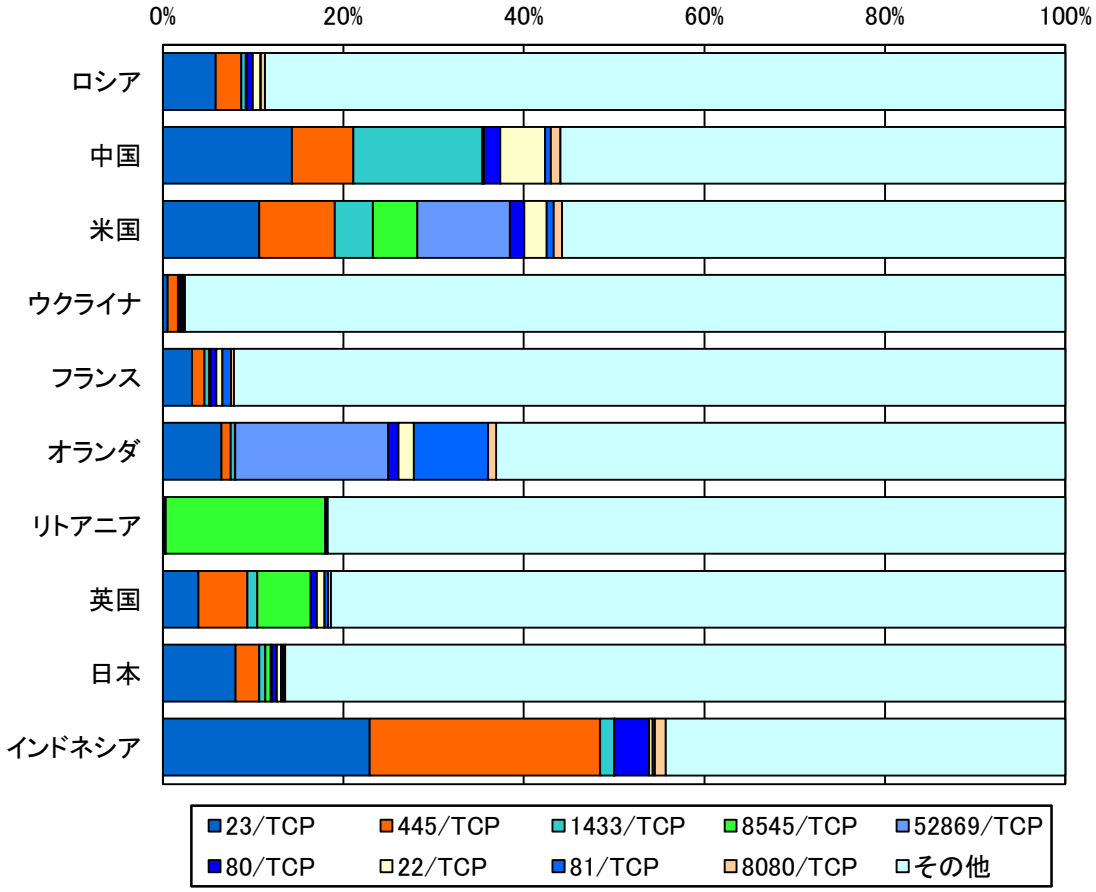

図 2-10　発信元国・地域別上位の宛先ポート別比率

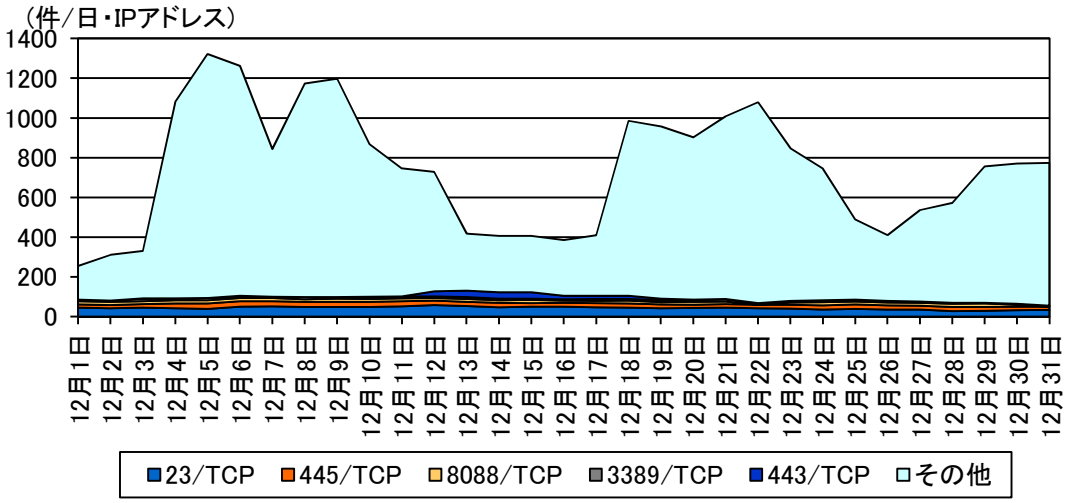

図 2-11　ロシアからの検知件数の推移

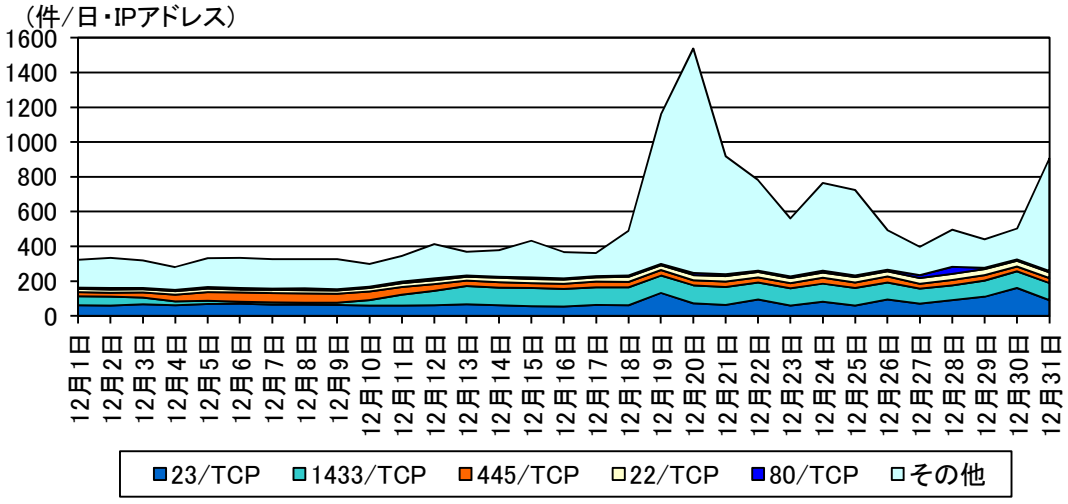

図 2-12　中国からの検知件数の推移

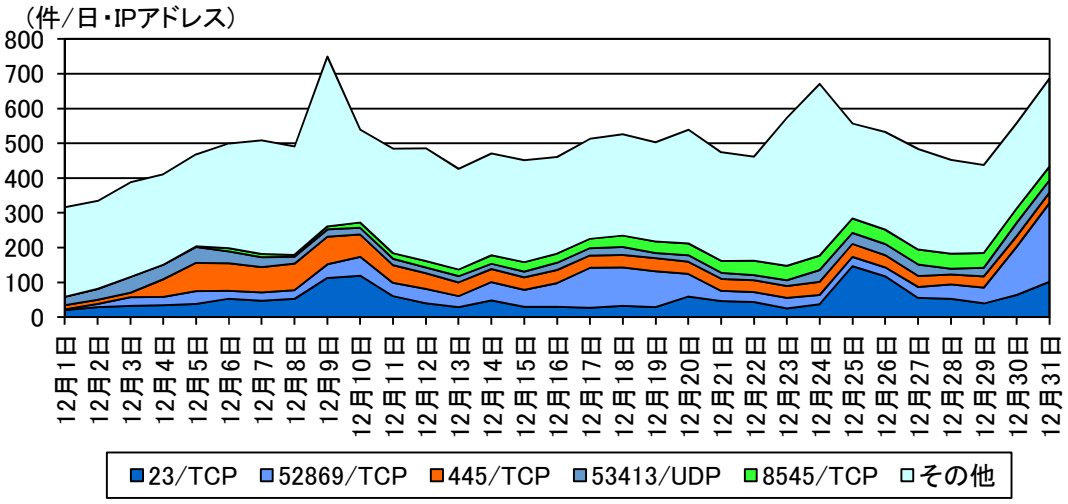

図 2-13　米国からの検知件数の推移

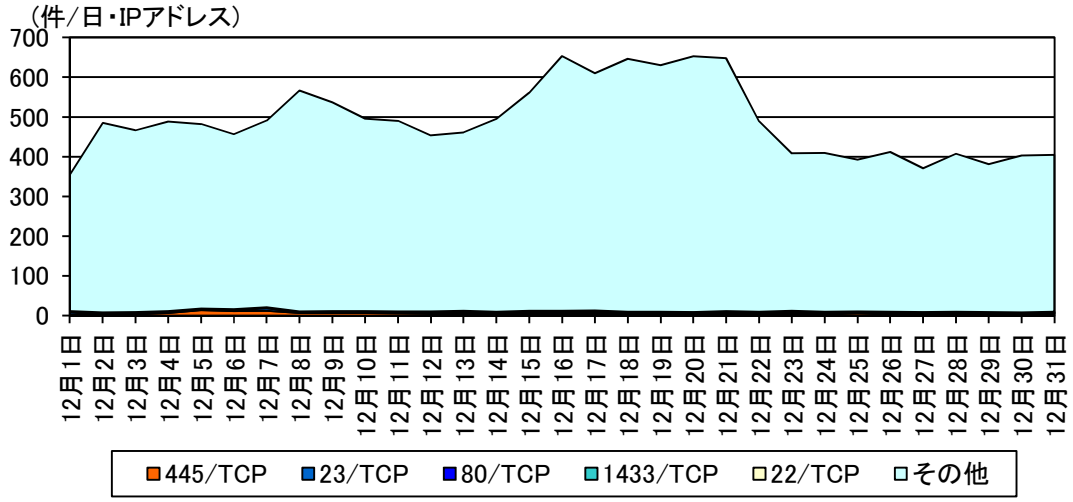

図 2-14　ウクライナからの検知件数の推移

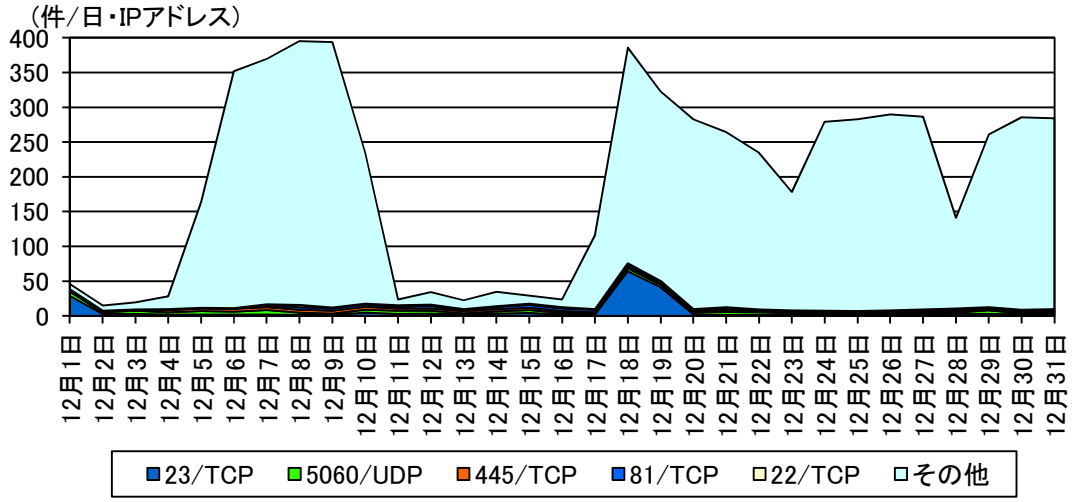

図 2-15　フランスからの検知件数の推移

3　DoS 攻撃被害の観測結果

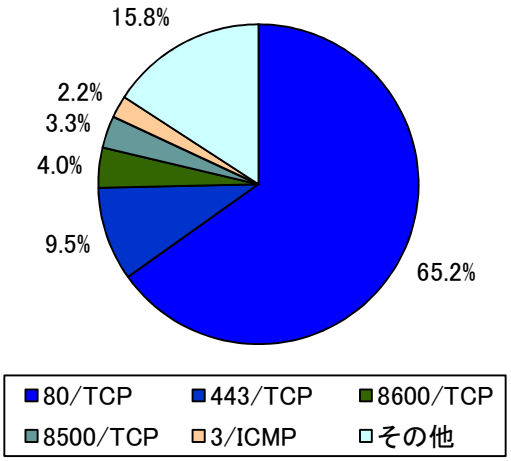

図 3-1　跳ね返りパケット発信元ポート別比率

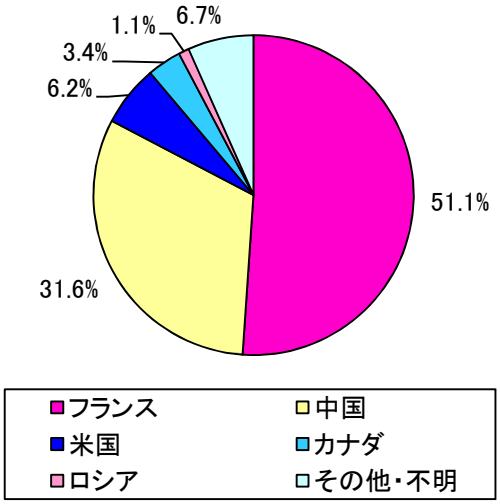

図 3-2　跳ね返りパケット発信元国・地域別比率

4　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。

4-1　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。）。

4-2　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 4-1 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 4-1　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
3 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