平成 31年3月 28 日

平成31年2月期観測資料

1　観測結果概要

平成 31 年2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 3,789.8 件で、平成 31 年1月期（以下「前期」という。）と比較して 245.3 件（6.9 %）増加しました。また、着信元（送信元）IP アドレス数は、一日当たり 49,221.5 個で、前期と比較して 351.3 個（0.7 %）減少しました。

不正侵入等の行為（以下「不正侵入等」という。）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 943.0 件で、前期と比較して 27.6 件（2.8 %）減少しました。また、着信元（送信元）IP アドレス数は、一日当たり 7,756.1 個で、前期と比較して 162.2 個（2.0 %）減少しました。

DoS 攻撃被害検知件数は、一日当たり 13,220.3 件で、前期と比較して 1,317.8 件（11.1 %）増加しました。また、着信元（送信元）IP アドレス数は、一日当たり 375.7 個で、前期と比較して 59.2 個（18.7 %）増加しました。

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	446.75 件	＋19.9%　（＋74.30 件）
2 位	2 位	445/TCP	348.84 件	＋13.6%　（＋41.84 件）
3 位	3 位	1433/TCP	95.36 件	－53.1%　（－108.05 件）
4 位	20 位	123/UDP	90.24 件	＋507.0%　（＋75.38 件）
5 位	5 位	22/TCP	87.89 件	＋5.0%　（＋4.20 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	123/UDP	90.24 件	＋507.0%　（＋75.38 件）	4 位	20 位
2 位	23/TCP	446.75 件	＋19.9%　（＋74.30 件）	1 位	1 位
3 位	445/TCP	348.84 件	＋13.6%　（＋41.84 件）	2 位	2 位
4 位	5038/TCP	26.74 件	＋118.2%　（＋14.49 件）	16 位	23 位
5 位	5060/UDP	38.21 件	＋25.1%　（＋7.67 件）	11 位	10 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	1433/TCP	95.36 件	－53.1%　（－108.05 件）	3 位	3 位
2 位	52869/TCP	86.75 件	－46.4%　（－75.05 件）	6 位	4 位
3 位	80/TCP	59.19 件	－14.0%　（－9.60 件）	8 位	7 位
4 位	8291/TCP	20.82 件	－8.3%　（－1.89 件）	19 位	16 位
5 位	27019/TCP	1.07 件	－57.3%　（－1.44 件）	－[ii]	－[ii]

[i] 一日・1IP アドレス当たり。

[ii] 今期及び前期のアクセス件数が僅かなため、今期順位及び前期順位は記載していません。

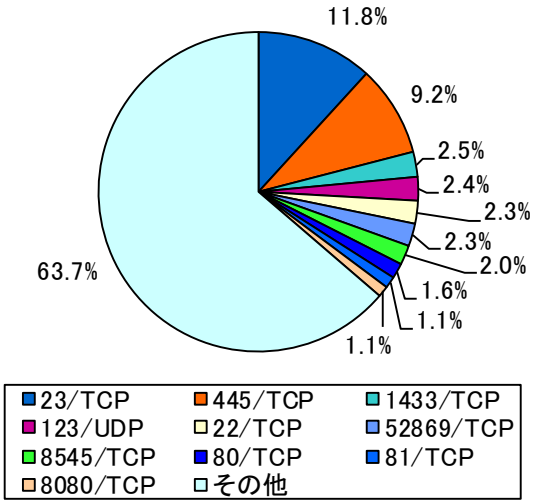

図 2-1 宛先ポート別比率(全て)[i]

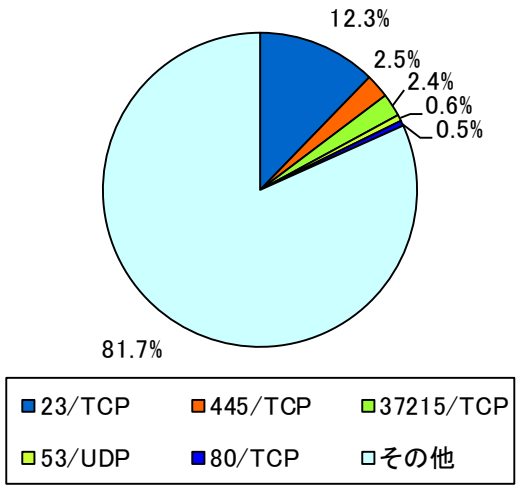

図 2-2 宛先ポート別比率(日本国内)

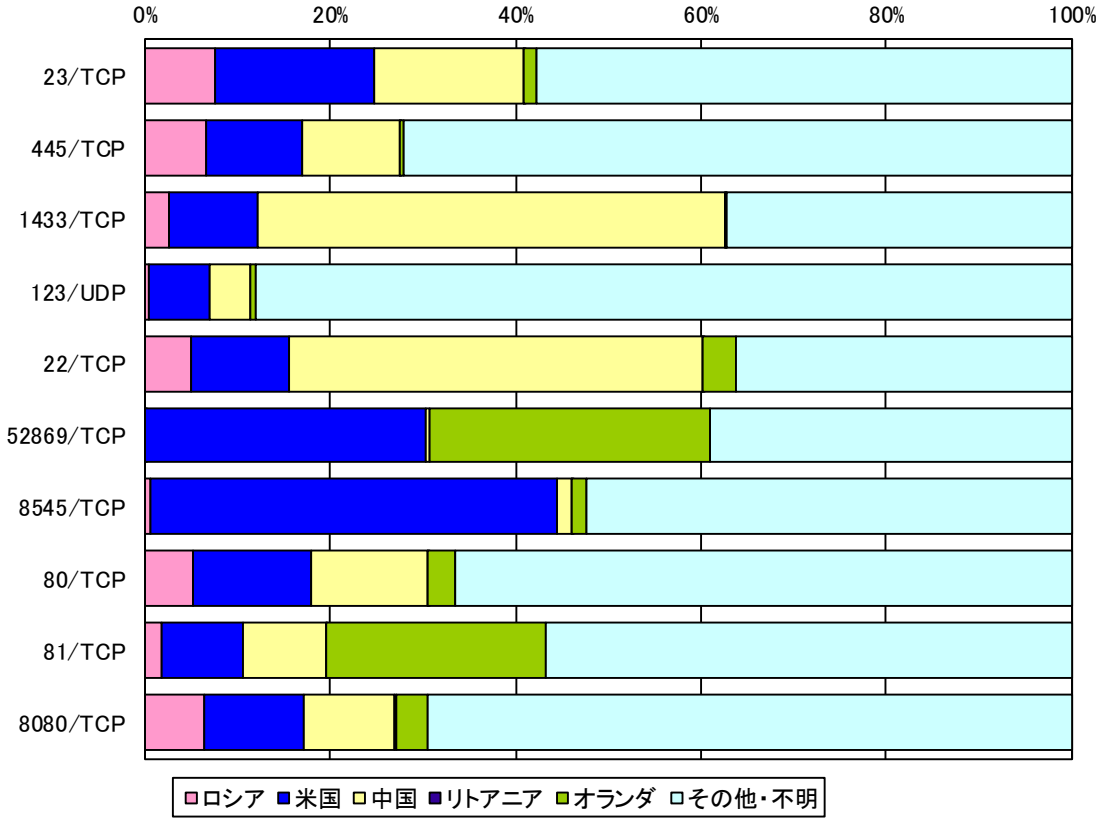

図 2-3 宛先ポート別上位の着信元国・地域別比率 [ii]

[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] 着信元国・地域については、判明した着信元(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。

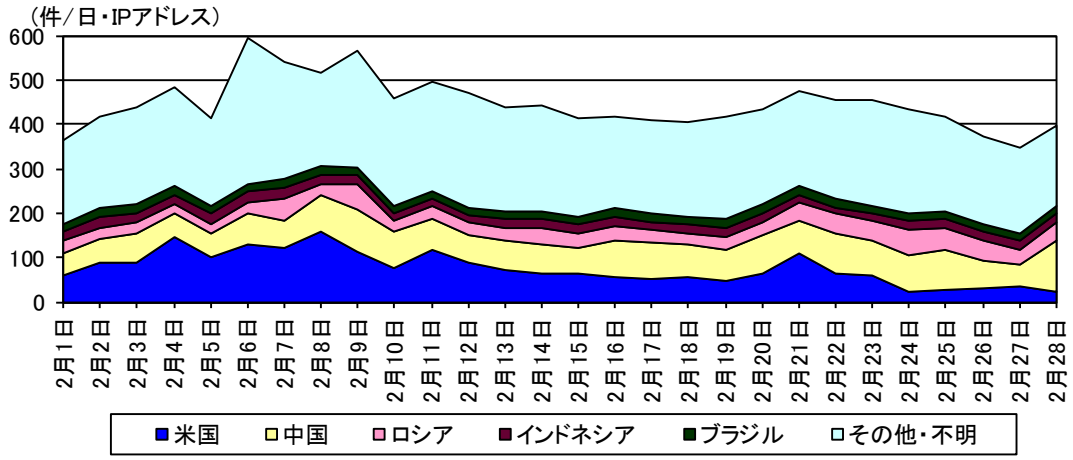

図 2-4　センサーのポート 23/TCP における検知件数の推移

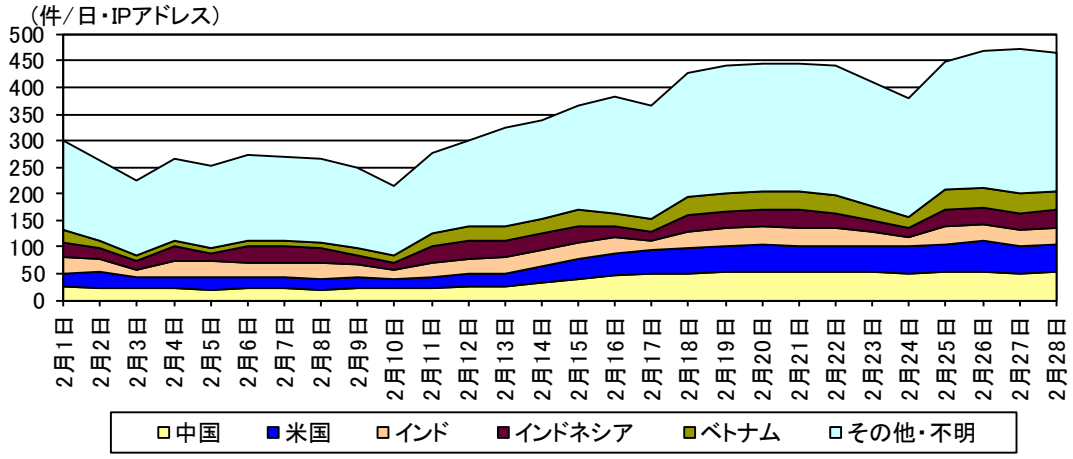

図 2-5　センサーのポート 445/TCP における検知件数の推移

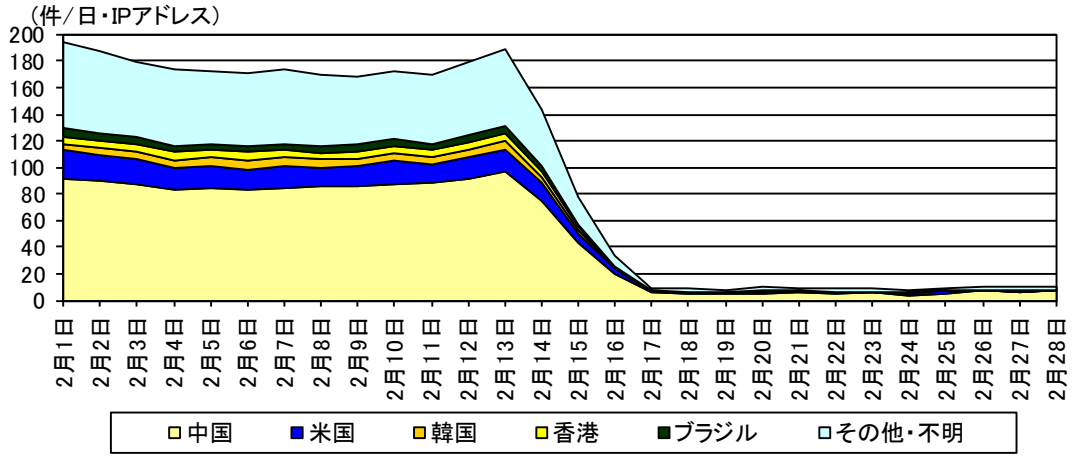

図 2-6　センサーのポート 1433/TCP における検知件数の推移

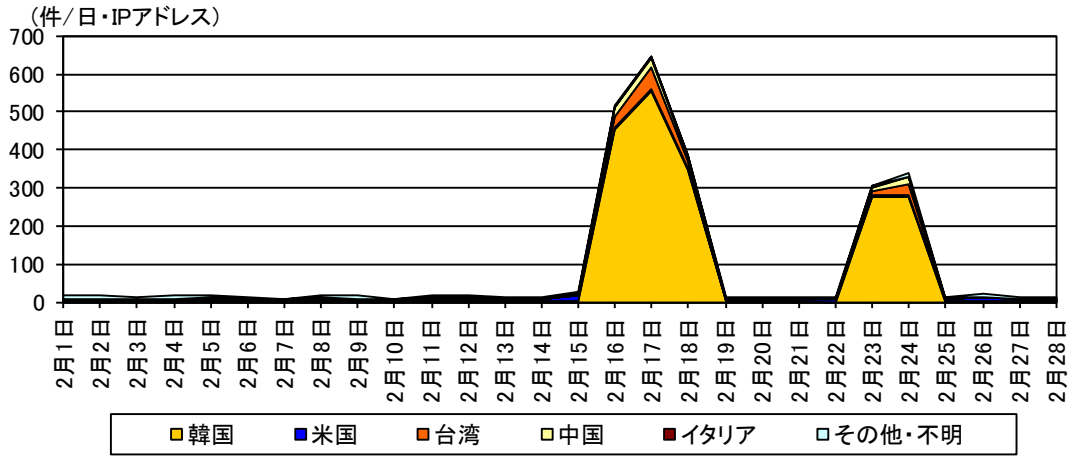

図 2-7　センサーのポート 123/UDP における検知件数の推移

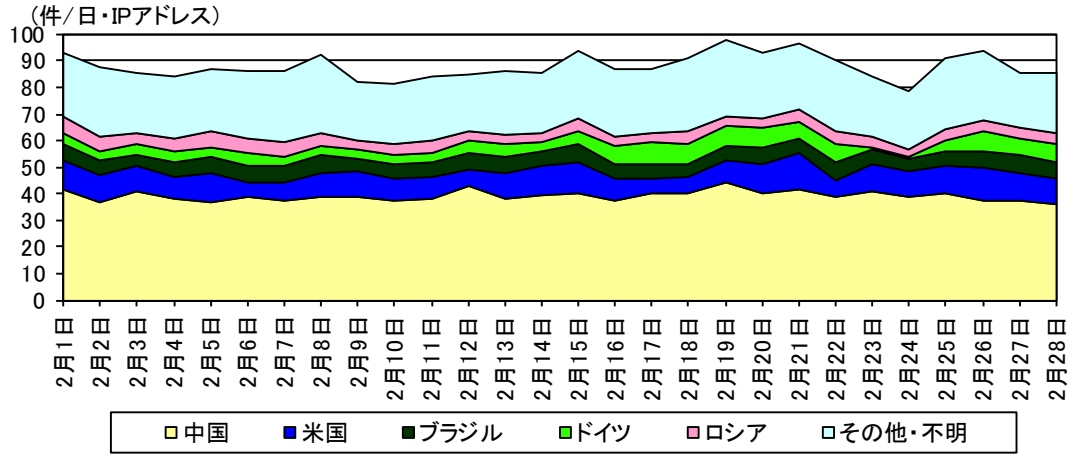

図 2-8　センサーのポート 22/TCP における検知件数の推移

2-2　着信元国・地域別アクセス検知件数

表 2-4　着信元国・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	853.80 件	＋18.9%　（＋135.80 件）
2 位	2 位	米国	529.31 件	－9.6%　（－55.99 件）
3 位	3 位	中国	418.56 件	－6.2%　（－27.67 件）
4 位	6 位	リトアニア	252.15 件	＋111.0%　（＋132.64 件）
5 位	5 位	オランダ	155.86 件	－1.7%　（－2.62 件）

表 2-5　着信元国・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	ロシア	853.80 件	＋18.9%　（＋135.80 件）	1 位	1 位
2 位	リトアニア	252.15 件	＋111.0%　（＋132.64 件）	4 位	6 位
3 位	韓国	109.82 件	＋140.0%　（＋64.07 件）	6 位	17 位
4 位	パナマ	87.82 件	＋141.8%　（＋51.49 件）	9 位	22 位
5 位	ルーマニア	70.02 件	＋82.6%　（＋31.68 件）	13 位	21 位

表 2-6　着信元国・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	ウクライナ	52.78 件	－78.6%　（－193.66 件）	19 位	4 位
2 位	米国	529.31 件	－9.6%　（－55.99 件）	2 位	2 位
3 位	中国	418.56 件	－6.2%　（－27.67 件）	3 位	3 位
4 位	南アフリカ	28.87 件	－35.8%　（－16.11 件）	23 位	18 位
5 位	ベトナム	53.76 件	－17.0%　（－10.99 件）	18 位	12 位

[i] 一日・1IP アドレス当たり。

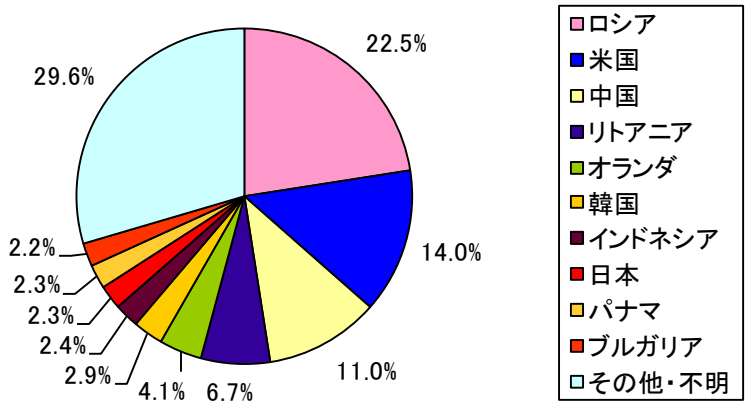

図 2-9　着信元国・地域別比率

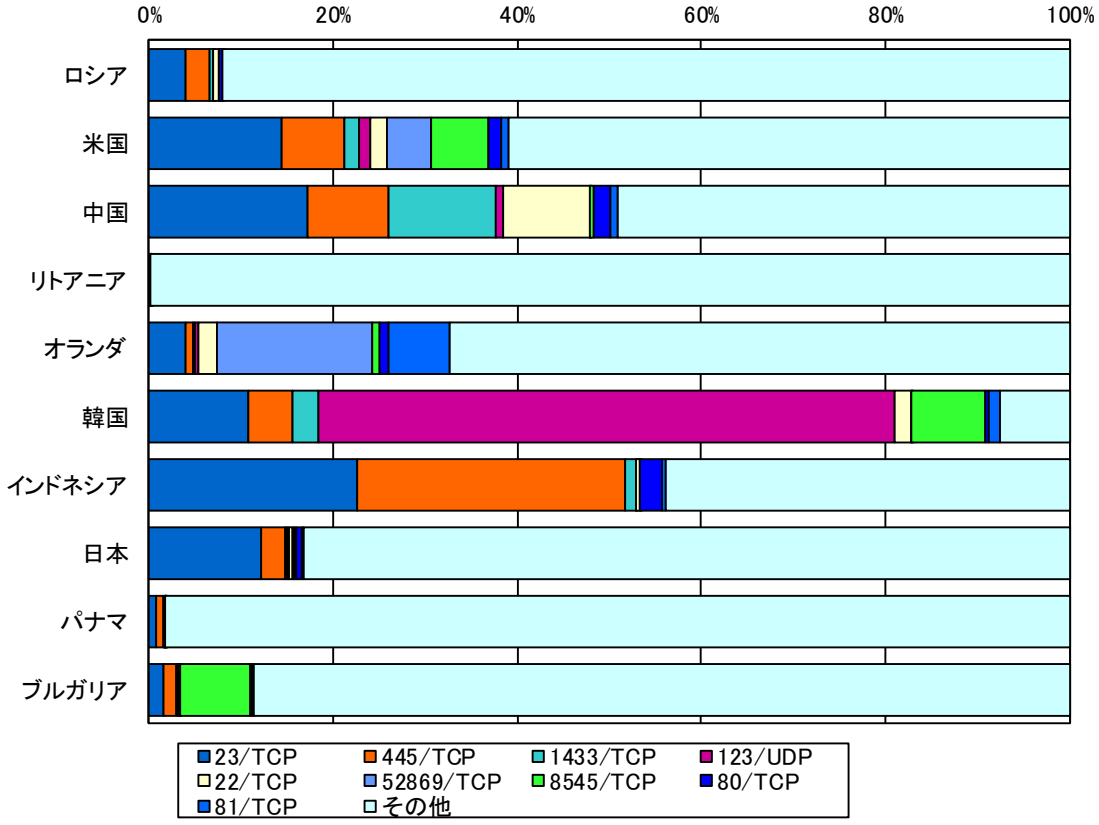

図 2-10　着信元国・地域別上位の宛先ポート別比率

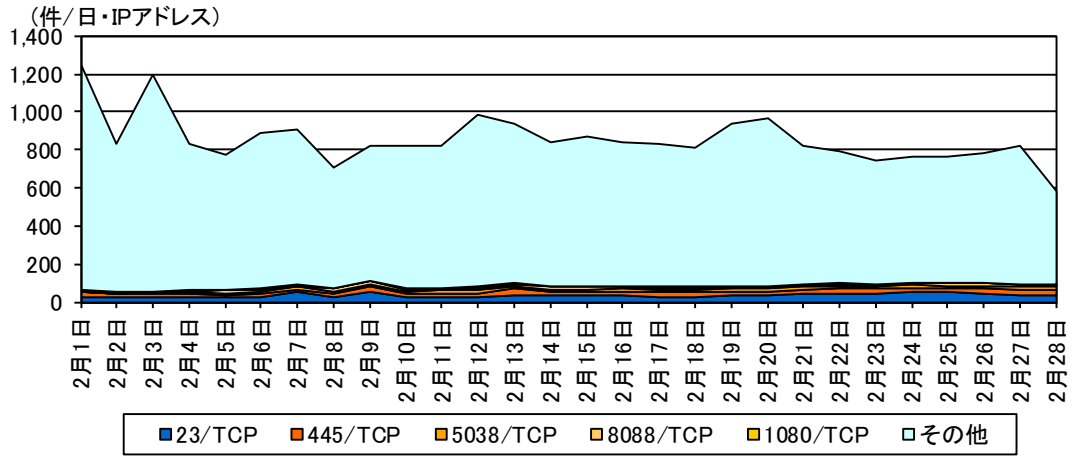

図 2-11　ロシアからの検知件数の推移

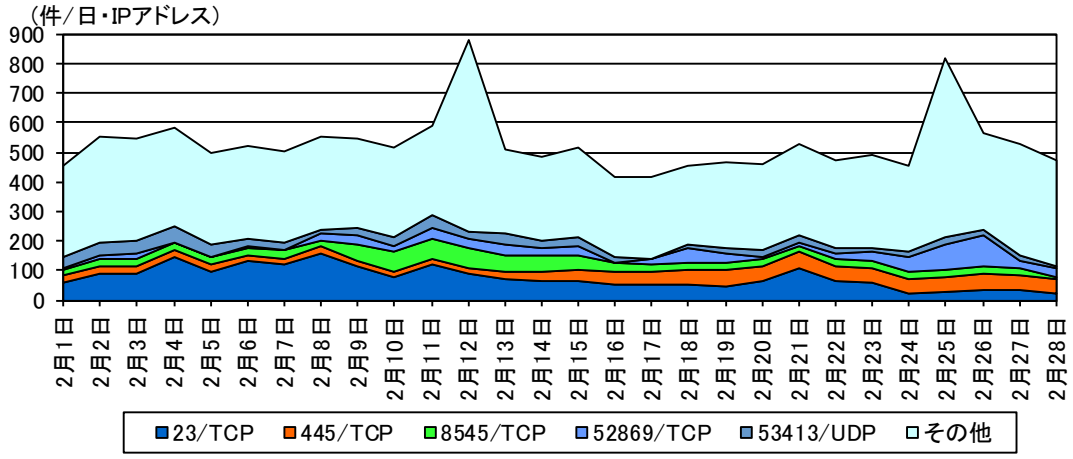

図 2-12　米国からの検知件数の推移

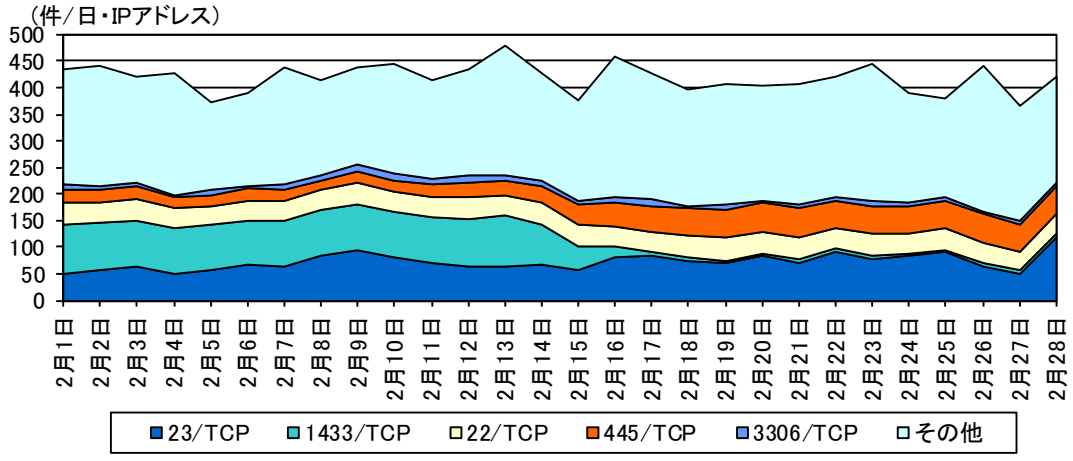

図 2-13　中国からの検知件数の推移

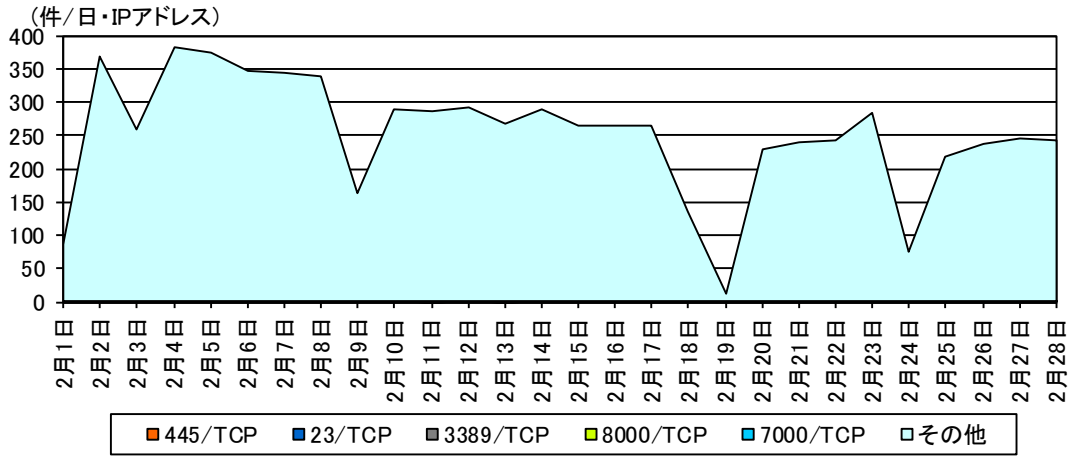

図 2-14 リトアニアからの検知件数の推移

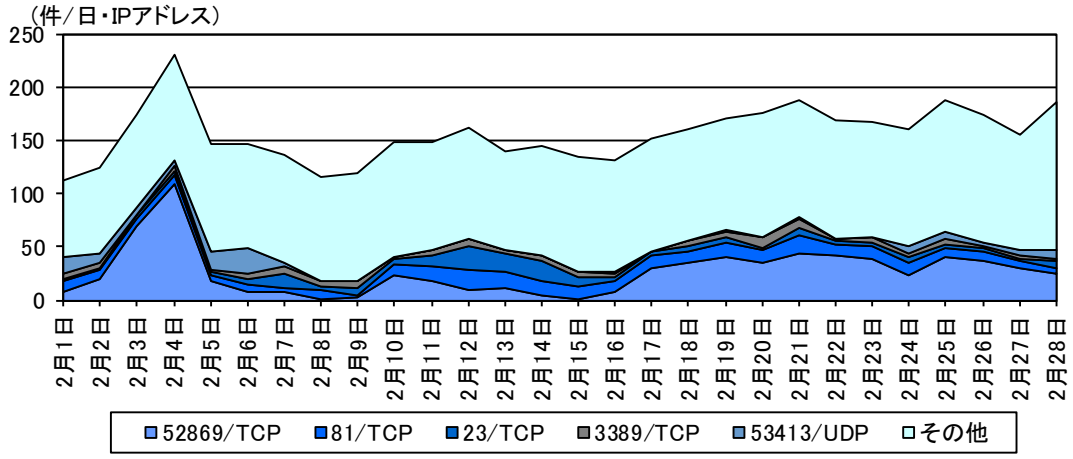

図 2-15 オランダからの検知件数の推移

3　不正侵入等の観測結果

3-1　攻撃手法別アクセス検知件数

表 3-1　不正侵入等の攻撃手法別検知件数

今期順位	前期順位	攻撃手法	今期件数 [i]	前期比 [i]	増加順位	減少順位
1 位	1 位	INDICATOR-SCAN	332.83 件	－10.2%　（－37.61 件）		1 位
2 位	2 位	Microsoft Windows Terminal server	274.43 件	－8.0%　（－23.91 件）		2 位
3 位	3 位	SMBv1	156.07 件	＋37.3%　（＋42.40 件）	1 位	
4 位	4 位	Remote Desktop	48.93 件	－12.9%　（－7.23 件）		4 位
5 位	6 位	VOIP	38.87 件	＋40.8%　（＋11.27 件）	2 位	

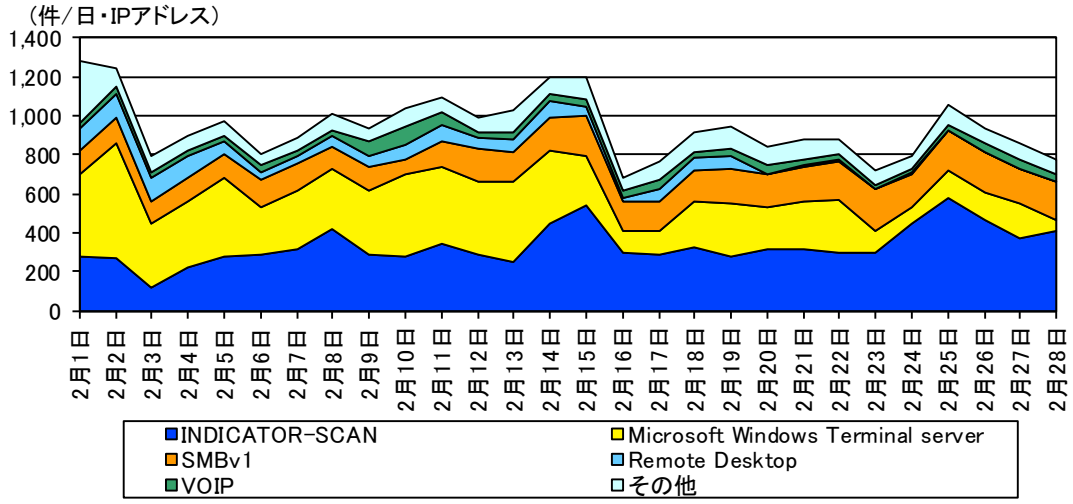

図 3-1　不正侵入等の攻撃手法別検知件数の推移

[i] 一日・1IP アドレス当たり。

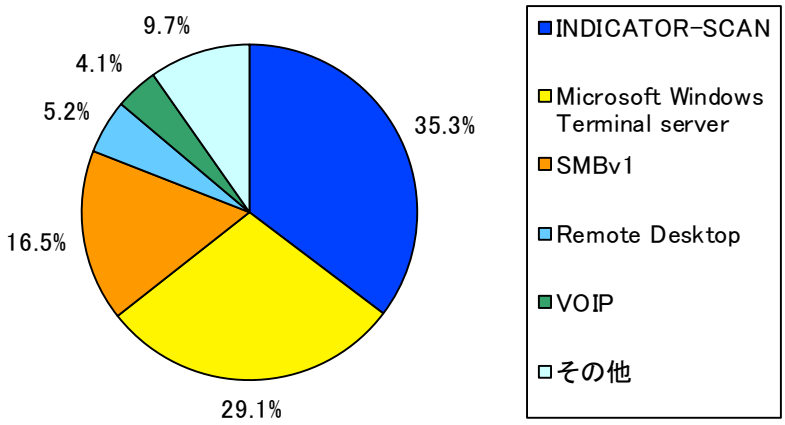

図 3-2 不正侵入等の攻撃手法別検知比率

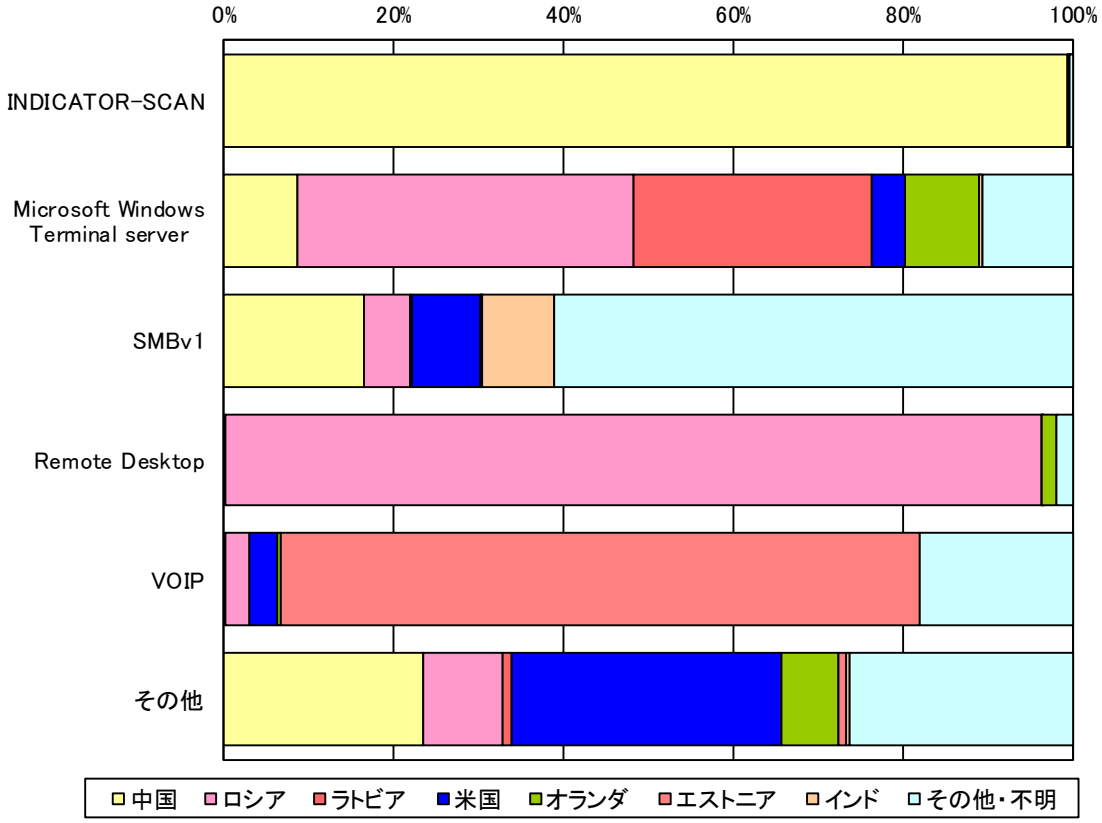

図 3-3 不正侵入等の攻撃手法の国・地域別検知比率

3-2 着信元国・地域別アクセス検知件数

表 3-2 不正侵入等の着信元国・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	中国	401.81 件	−8.9%	（−39.21 件）
2 位	2 位	ロシア	173.69 件	−17.8%	（−37.74 件）
3 位	4 位	ラトビア	78.26 件	＋58.4%	（＋28.85 件）
4 位	3 位	米国	54.66 件	＋10.1%	（＋5.03 件）
5 位	5 位	オランダ	31.87 件	−19.8%	（−7.89 件）

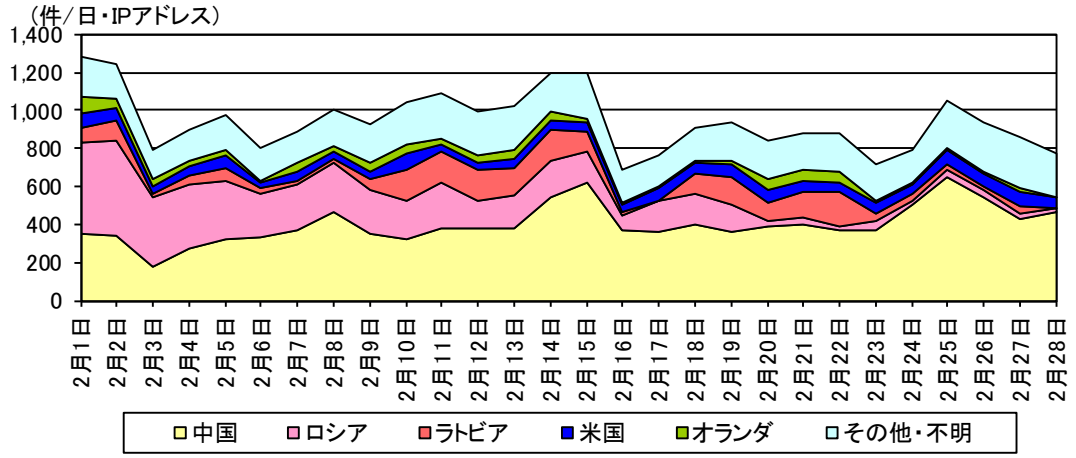

図 3-4 不正侵入等の着信元国・地域別検知件数の推移

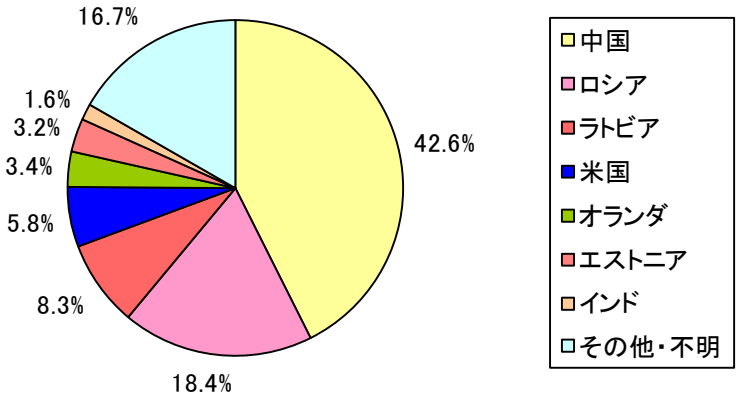

図 3-5 不正侵入等の着信元国・地域別検知比率

[i] 一日・1IP アドレス当たり。

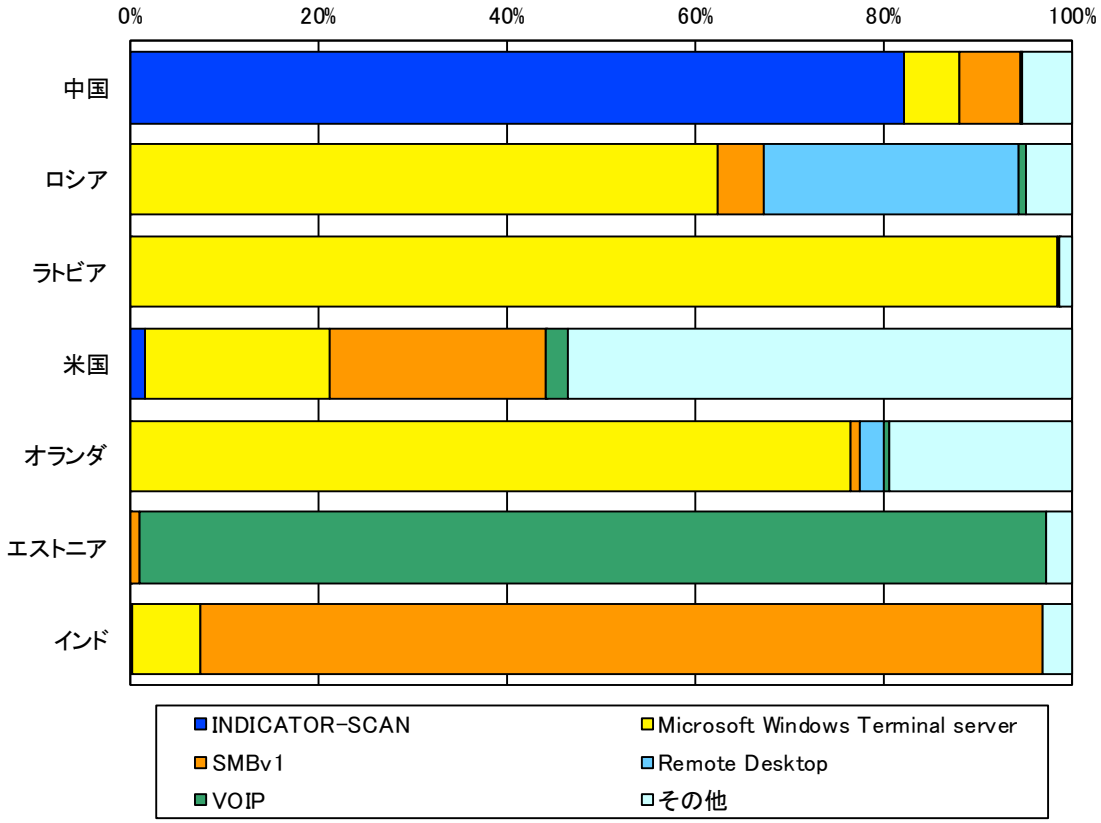

図 3-6　不正侵入等の着信元国・地域別上位の攻撃手法別検知比率

4　DoS 攻撃被害の観測結果

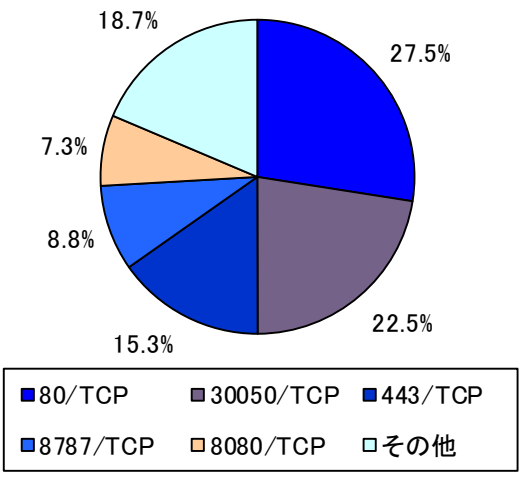

図 4-1　跳ね返りパケット着信元ポート別比率

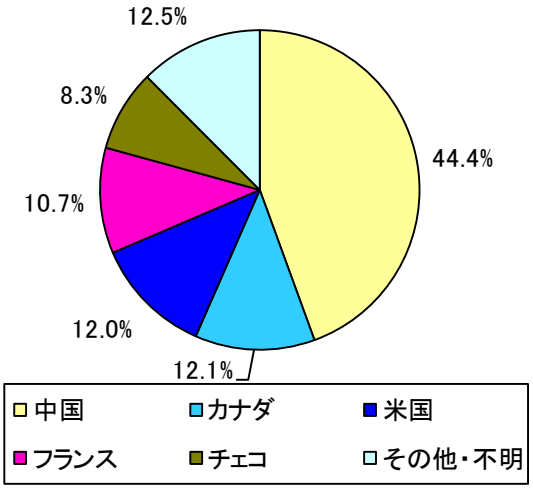

図 4-2　跳ね返りパケット着信元国・地域別比率

5　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。

5-1　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。）。

5-2　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 5-1 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 5-1　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
4 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

5-3　不正侵入等の検知

検知された各シグネチャ は、表 5-2 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 5-2 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-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