Distributed via
@police
https://www.npa.go.jp/cyberpolice/

令和元年6月 21 日

平成31年4月期観測資料

1　観測結果概要

平成 31 年4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 3,428.0 件で、平成 31 年3月期（以下「前期」という。）と比較して 300.3 件（9.6%）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 43,537.6 個で、前期と比較して 3,962.0 個（8.3%）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 1,147.0 件で、前期と比較して 312.9 件（37.5%）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 8,466.4 個で、前期と比較して 338.8 個（3.8%）減少しました。

DoS 攻撃被害検知件数は、一日当たり 15,130.4 件で、前期と比較して 6,280.5 件（71.0%）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 340.4 個で、前期と比較して 7.8 個（2.2%）減少しました。

Copyright 2019 Cyber Force Center, NPA JAPAN

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	514.30 件	＋3.8%　（＋18.70 件）
2 位	2 位	445/TCP	407.99 件	－5.7%　（－24.49 件）
3 位	3 位	52869/TCP	87.92 件	－25.4%　（－29.93 件）
4 位	4 位	22/TCP	70.20 件	－10.3%　（－8.09 件）
5 位	5 位	80/TCP	52.27 件	＋1.9%　（＋0.98 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	37215/TCP	31.09 件	＋311.1%　（＋23.52 件）	11 位	35 位
2 位	9001/TCP	22.22 件	－[ii]　（＋20.67 件）	14 位	－[ii]
3 位	23/TCP	514.30 件	＋3.8%　（＋18.70 件）	1 位	1 位
4 位	53/UDP	15.27 件	＋87.1%　（＋7.11 件）	23 位	30 位
5 位	53413/UDP	41.70 件	＋18.5%　（＋6.52 件）	7 位	9 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	52869/TCP	87.92 件	－25.4%　（－29.93 件）	3 位	3 位
2 位	445/TCP	407.99 件	－5.7%　（－24.49 件）	2 位	2 位
3 位	9527/TCP	1.35 件	－91.5%　（－14.61 件）	－[iii]	20 位
4 位	2323/TCP	21.74 件	－31.9%　（－10.20 件）	16 位	12 位
5 位	5555/TCP	24.03 件	－27.0%　（－8.91 件）	13 位	10 位

[i] 一日・1IP アドレス当たり。

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

[iii] 今期のアクセス件数が僅かなため、今期順位は記載していません。

Copyright 2019 Cyber Force Center, NPA JAPAN

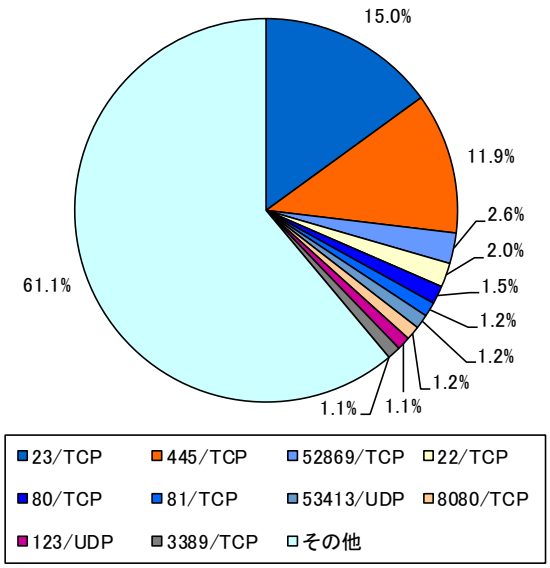

図 2-1　宛先ポート別比率（全て）[i]

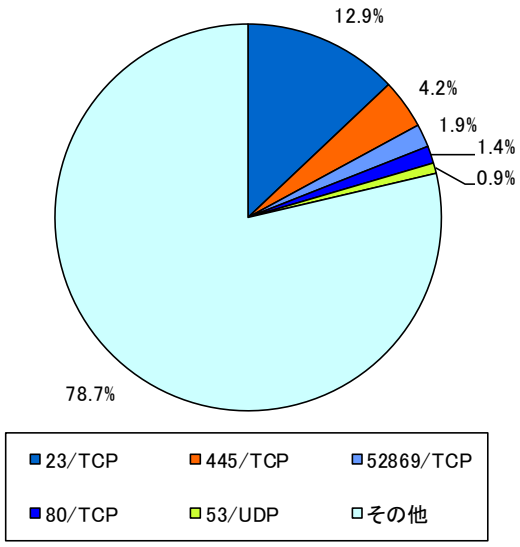

図 2-2　宛先ポート別比率（日本国内）

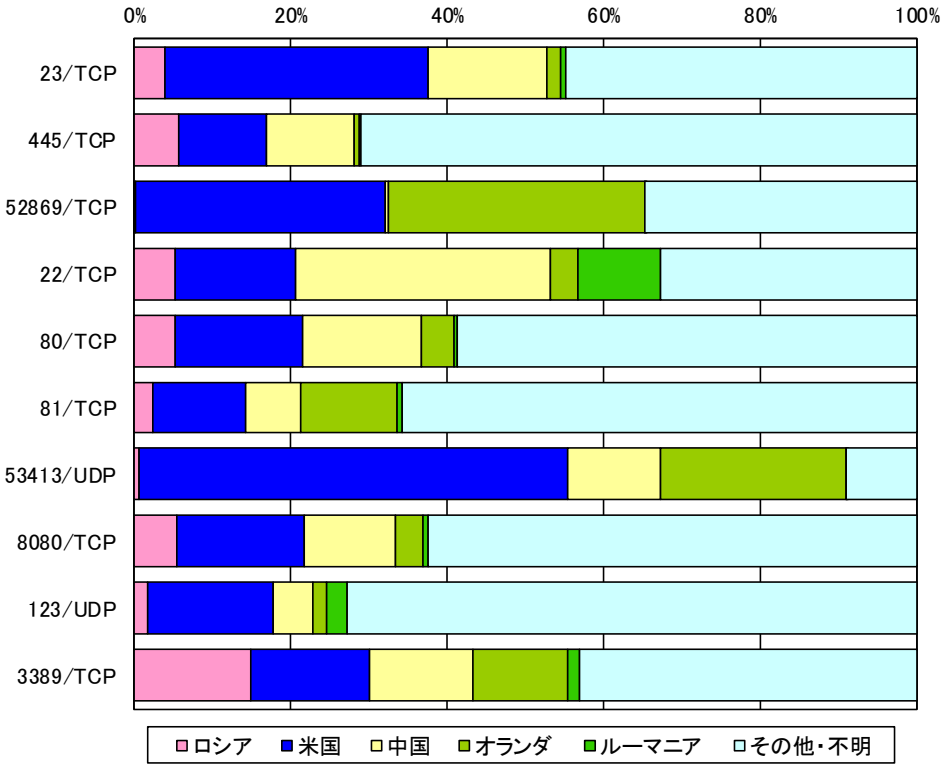

図 2-3　宛先ポート別上位の着信元国・地域別比率 [ii]

[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。

Copyright 2019 Cyber Force Center, NPA JAPAN

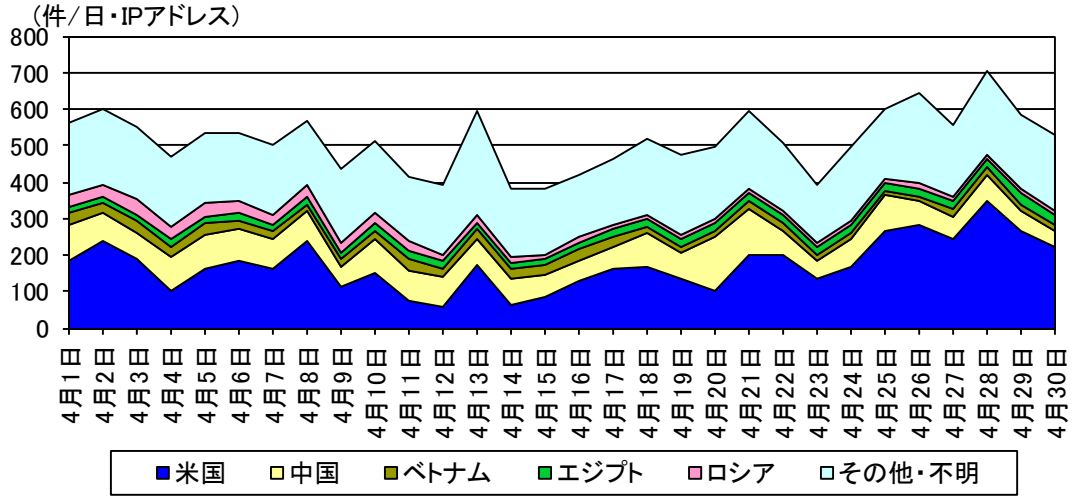

図 2-4　センサーのポート 23/TCP における検知件数の推移

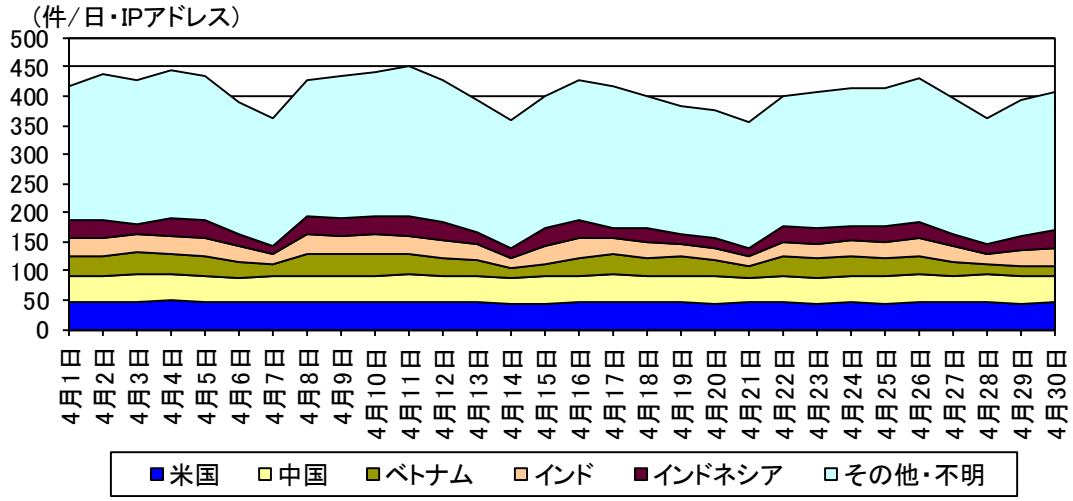

図 2-5　センサーのポート 445/TCP における検知件数の推移

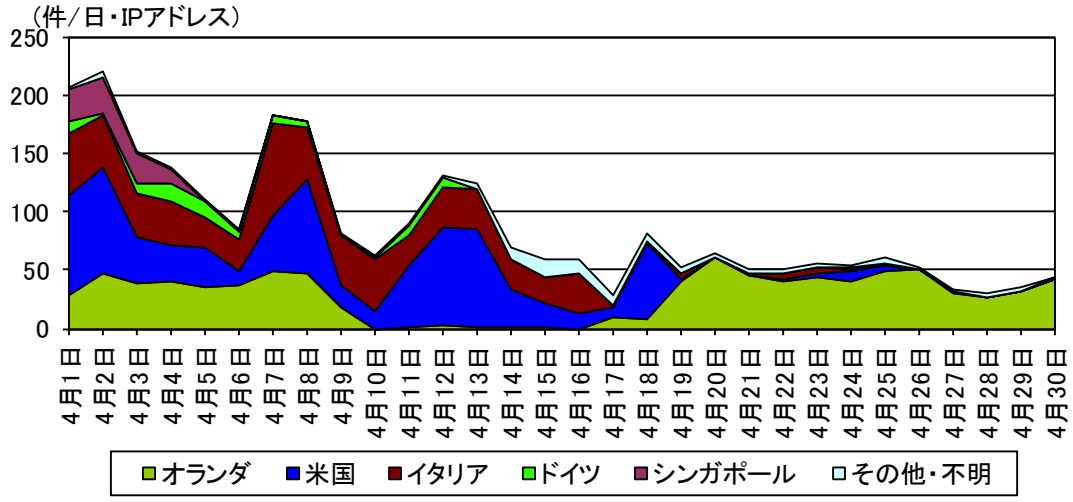

図 2-6　センサーのポート 52869/TCP における検知件数の推移

Copyright 2019 Cyber Force Center, NPA JAPAN

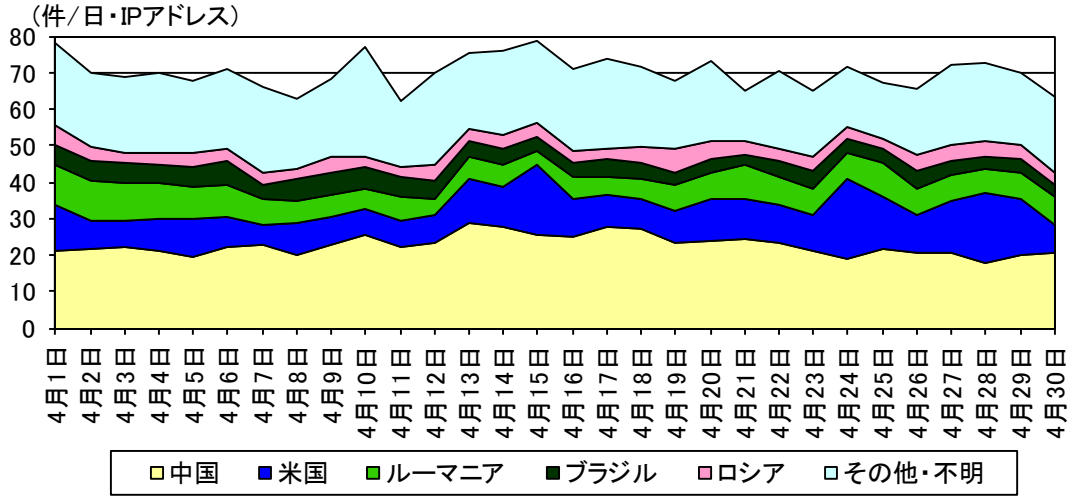

図 2-7　センサーのポート 22/TCP における検知件数の推移

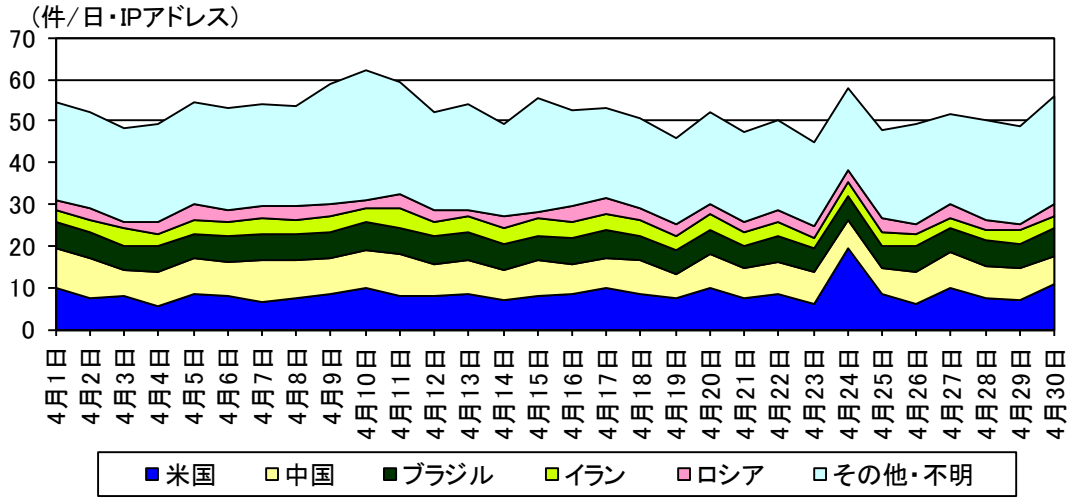

図 2-8　センサーのポート 80/TCP における検知件数の推移

Copyright 2019 Cyber Force Center, NPA JAPAN

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	877.15 件	＋40.9%　（＋254.57 件）
2 位	2 位	米国	623.92 件	＋15.9%　（＋85.46 件）
3 位	3 位	中国	368.51 件	－2.7%　（－10.33 件）
4 位	4 位	オランダ	273.68 件	＋36.4%　（＋72.97 件）
5 位	5 位	ルーマニア	99.69 件	－21.2%　（－26.80 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	877.15 件	＋40.9%　（＋254.57 件）	1 位	1 位
2 位	米国	623.92 件	＋15.9%　（＋85.46 件）	2 位	2 位
3 位	オランダ	273.68 件	＋36.4%　（＋72.97 件）	4 位	4 位
4 位	台湾	57.70 件	＋48.1%　（＋18.73 件）	12 位	16 位
5 位	エストニア	76.97 件	＋26.6%　（＋16.17 件）	7 位	11 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	イタリア	56.83 件	－40.8%　（－39.13 件）	13 位	6 位
2 位	ルーマニア	99.69 件	－21.2%　（－26.80 件）	5 位	5 位
3 位	英国	37.93 件	－36.4%　（－21.73 件）	18 位	12 位
4 位	ウクライナ	12.60 件	－57.0%　（－16.67 件）	31 位	20 位
5 位	インドネシア	81.24 件	－13.6%　（－12.80 件）	6 位	7 位

[i] 一日・1IP アドレス当たり。

Copyright 2019 Cyber Force Center, NPA JAPAN

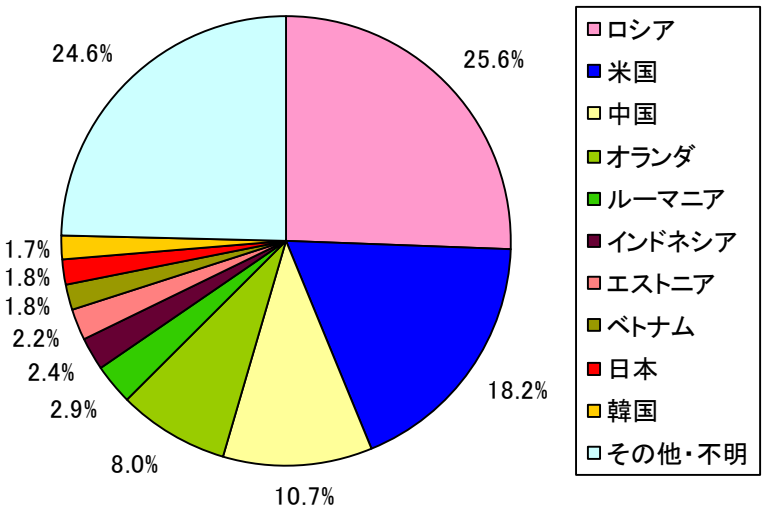

図 2-9　着信元国・地域別比率

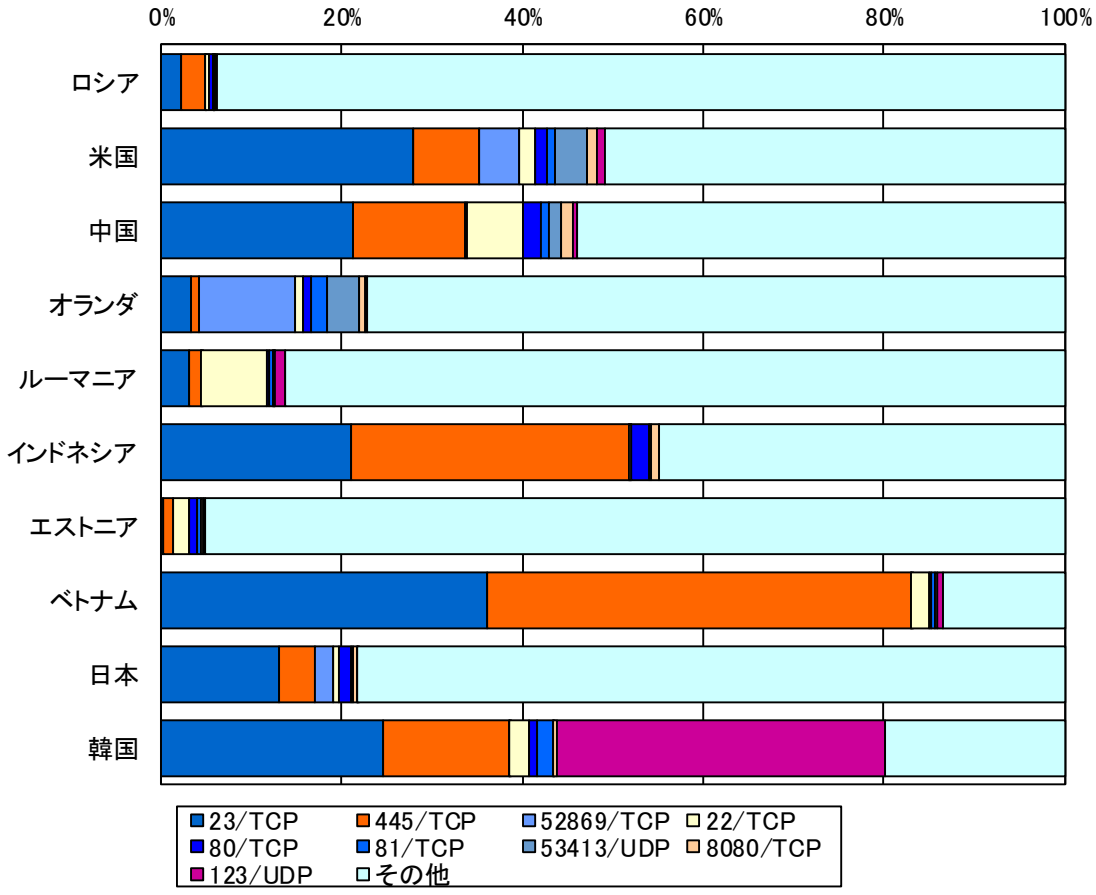

図 2-10　着信元国・地域別上位の宛先ポート別比率

Copyright 2019 Cyber Force Center, NPA JAPAN

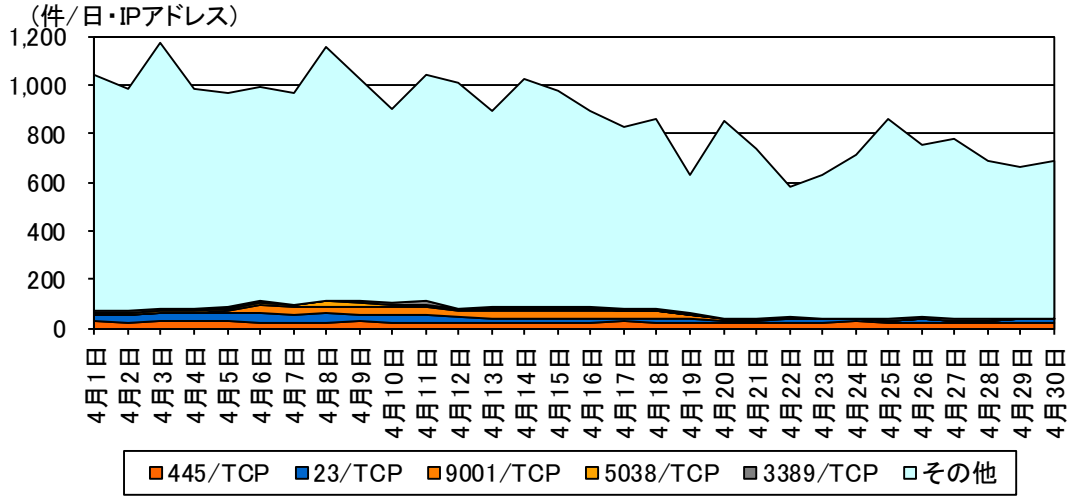

図 2-11　ロシアからの検知件数の推移

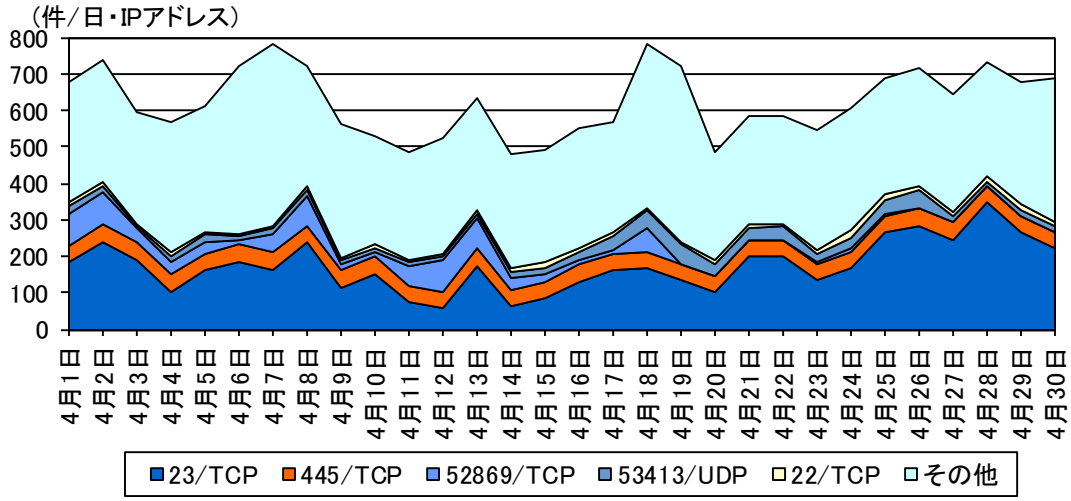

図 2-12　米国からの検知件数の推移

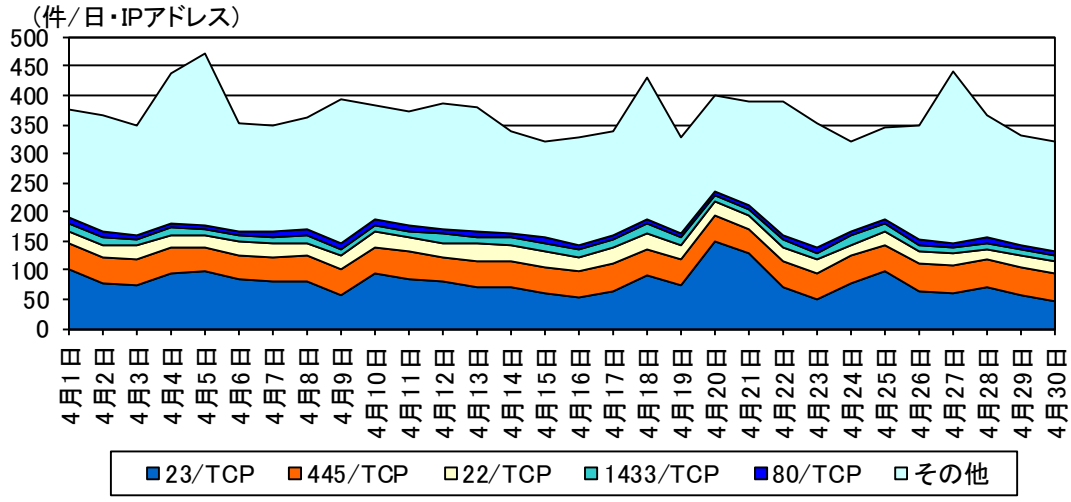

図 2-13　中国からの検知件数の推移

Copyright 2019 Cyber Force Center, NPA JAPAN

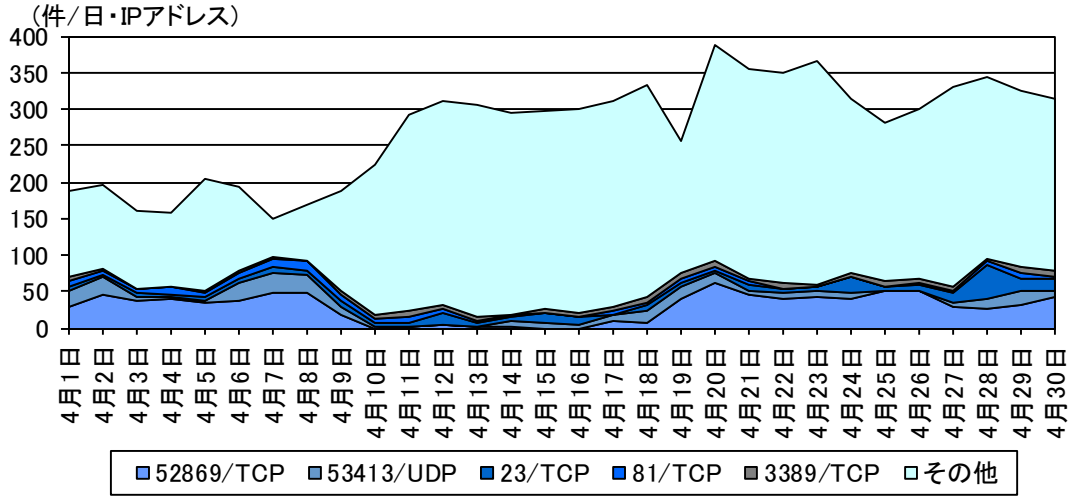

図 2-14　オランダからの検知件数の推移

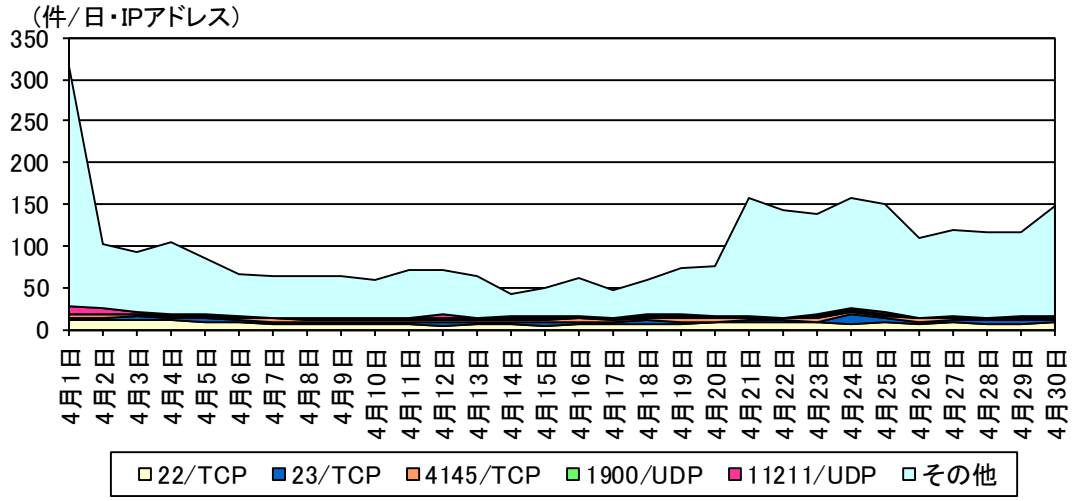

図 2-15　ルーマニアからの検知件数の推移

Copyright 2019 Cyber Force Center, NPA JAPAN

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	465.99 件	＋8.4%　（＋36.09 件）	3 位	
2 位	3 位	Microsoft Windows Terminal server	289.53 件	＋142.9%　（＋170.34 件）	1 位	
3 位	2 位	SMBv1	157.34 件	－7.7%　（－13.13 件）		1 位
4 位	7 位	Remote Desktop	107.06 件	－ [ii]　（＋97.92 件）	2 位	
5 位	4 位	VOIP	30.05 件	＋28.7%　（＋6.70 件）	5 位	

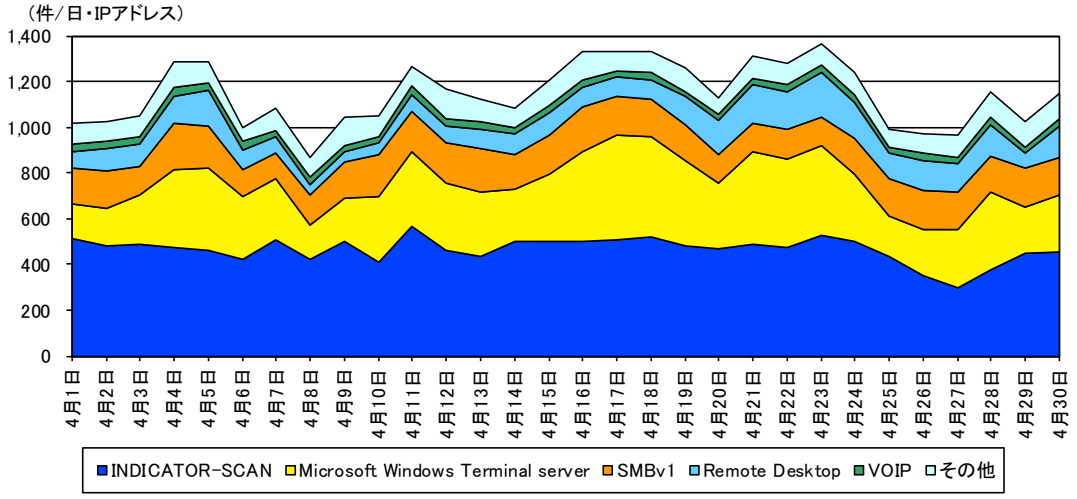

図 3-1　不正侵入等の攻撃手法別検知件数の推移

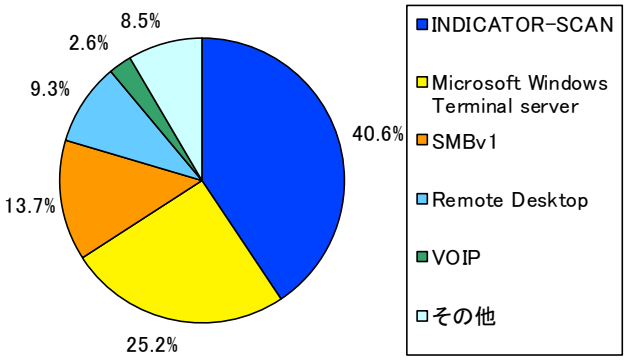

図 3-2　不正侵入等の攻撃手法別検知比率

[i] 一日・1IP アドレス当たり。

[ii] 前期のアクセス件数が僅かなため、前期比は記載していません。

Copyright 2019 Cyber Force Center, NPA JAPAN

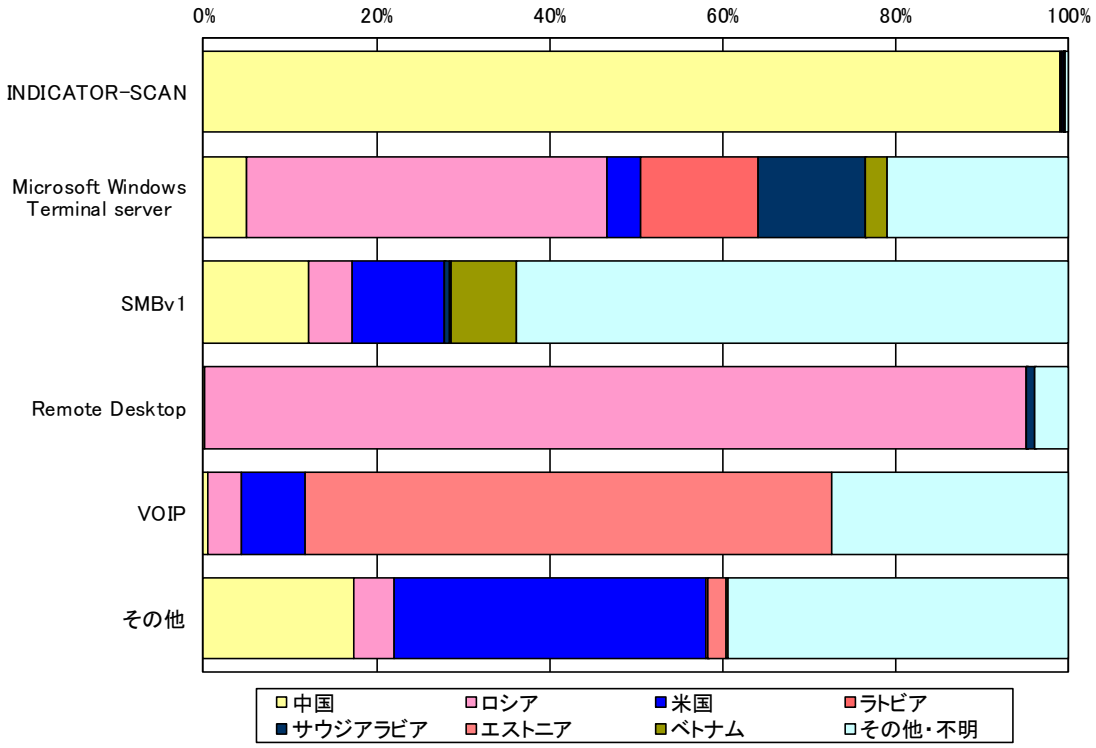

図 3-3 不正侵入等の攻撃手法の国・地域別検知比率

Copyright 2019 Cyber Force Center, NPA JAPAN

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	512.56 件	＋5.5% （＋26.64 件）
2 位	3 位	ロシア	236.09 件	＋669.8% （＋205.42 件）
3 位	2 位	米国	66.45 件	＋1.5% （＋0.98 件）
4 位	4 位	ラトビア	40.01 件	＋32.8% （＋9.88 件）
5 位	― [ii]	サウジアラビア	37.93 件	― [ii] （＋36.92 件）

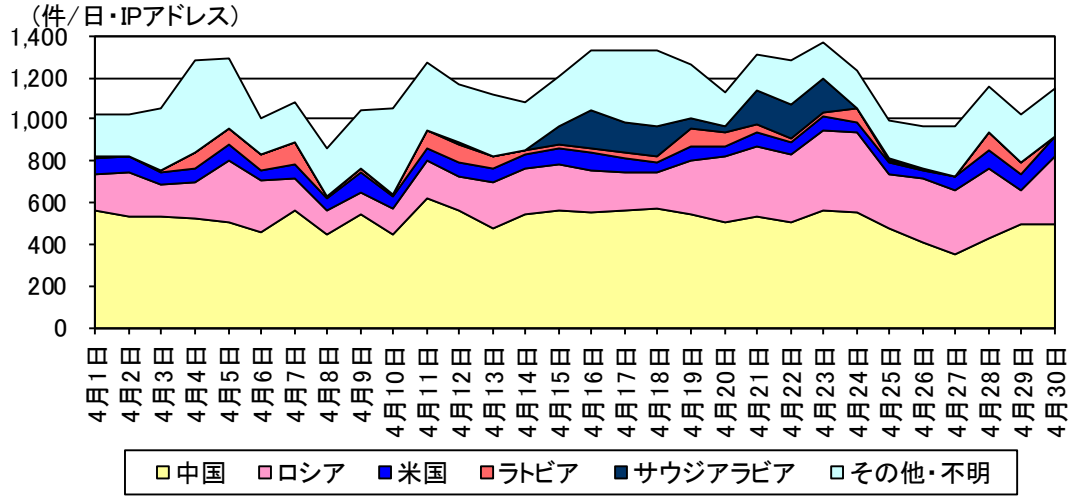

図 3-4 不正侵入等の着信元国・地域別検知件数の推移

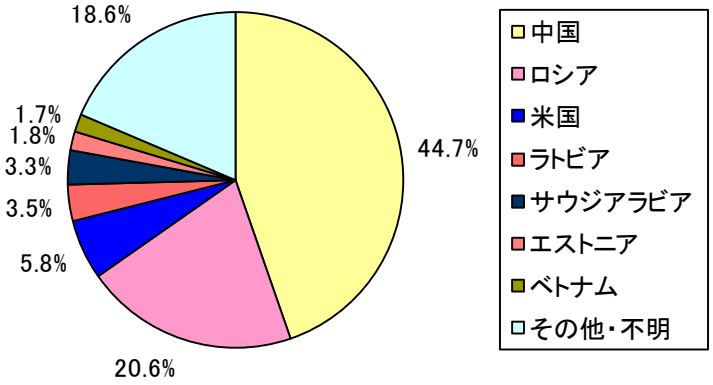

図 3-5 不正侵入等の着信元国・地域別検知比率

[i] 一日・1IP アドレス当たり。

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

Copyright 2019 Cyber Force Center, NPA JAPAN

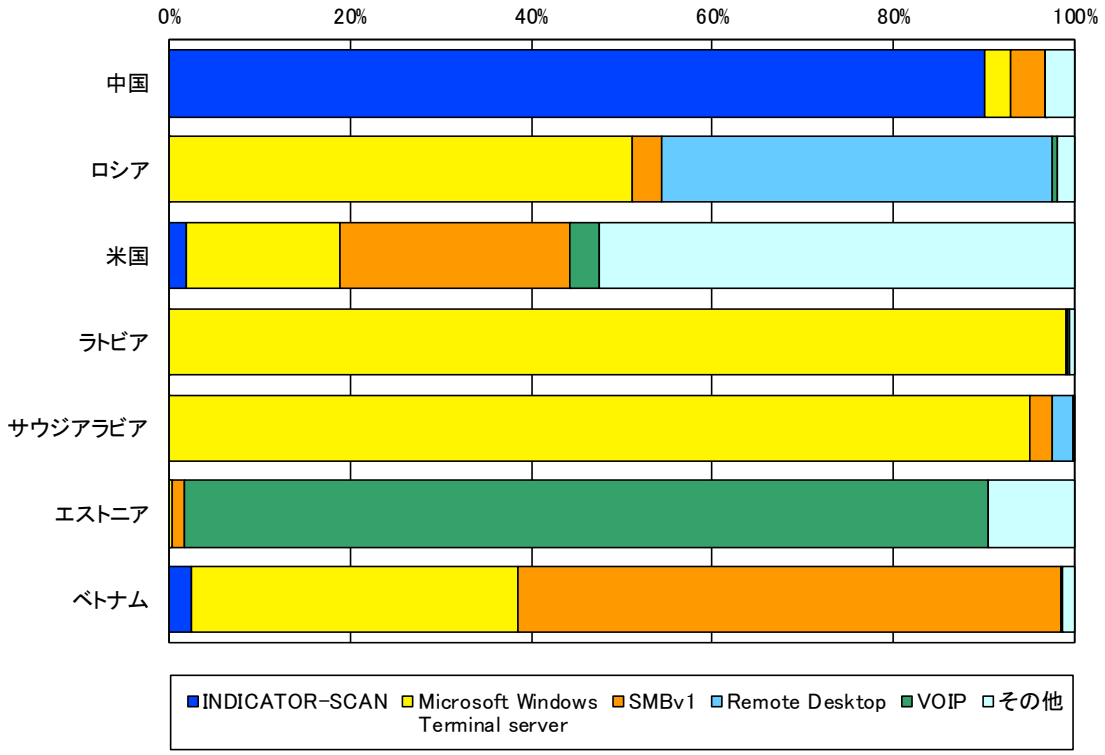

図 3-6　不正侵入等の着信元国・地域別上位の攻撃手法別検知比率

Copyright 2019 Cyber Force Center, NPA JAPAN

4　DoS 攻撃被害の観測結果

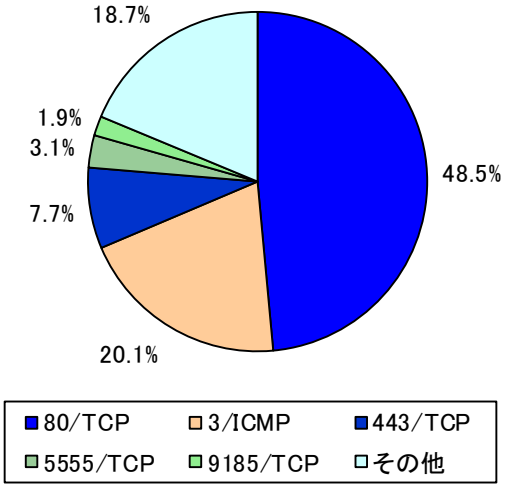

図 4-1　跳ね返りパケット着信元ポート別比率

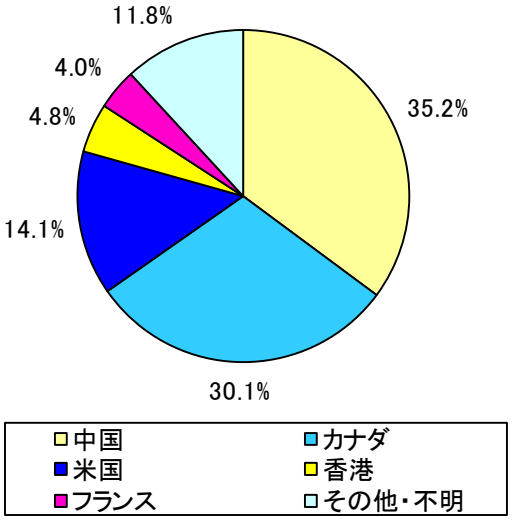

図 4-2　跳ね返りパケット着信元国・地域別比率

Copyright 2019 Cyber Force Center, NPA JAPAN

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

Copyright 2019 Cyber Force Center, NPA JAPAN

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

Copyright 2019 Cyber Force Center, NPA JAPAN