令和２年２月 26 日

令和2年1月期観測資料

1　観測結果概要

令和2年1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 4,840.1 件で、令和元年 12 月期（以下「前月期」という。）と比較して 623.4 件（11.4%）減少しました。また、送信元 IP アドレス[i] 数は、一日当たり 47,268.4 個で、前月期と比較して 444.2 個（0.9%）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 859.3 件で、前月期と比較して 35.3 件（3.9%）減少しました。また、送信元 IP アドレス数は、一日当たり 8888.5 個で、前月期と比較して 1,950.9 個（28.1%）増加しました。

DoS 攻撃被害検知件数は、一日当たり 10,016.5 件で、前月期と比較して 1,069.8 件（12.0%）増加しました。また、送信元 IP アドレス数は、一日当たり 483.9 個で、前月期と比較して 142.9 個（41.9%）増加しました。

[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。

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	23/TCP	356.27 件	－4.0%　（－14.82 件）
2 位	2 位	445/TCP	232.57 件	－3.6%　（－8.64 件）
3 位	3 位	1433/TCP	199.70 件	－7.0%　（－14.94 件）
4 位	5 位	80/TCP	74.01 件	－4.8%　（－3.70 件）
5 位	12 位	52869/TCP	73.72 件	＋96.5%　（＋36.19 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	今月期件数[i]	前月期比[i]	今月期順位	前月期順位
1 位	52869/TCP	73.72 件	＋96.5%　（＋36.19 件）	5 位	12 位
2 位	81/TCP	51.11 件	＋75.0%　（＋21.90 件）	8 位	17 位
3 位	4567/TCP	19.71 件	－[ii]　（＋16.05 件）	21 位	－[ii]
4 位	1900/UDP	32.43 件	＋84.8%　（＋14.88 件）	15 位	23 位
5 位	88/TCP	14.41 件	＋110.7%　（＋7.57 件）	24 位	48 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	今月期件数[i]	前月期比[i]	今月期順位	前月期順位
1 位	123/UDP	49.39 件	－72.3%　（－129.19 件）	9 位	4 位
2 位	26/TCP	4.42 件	－86.6%　（－28.55 件）	64 位	14 位
3 位	4145/TCP	9.10 件	－66.3%　（－17.92 件）	31 位	18 位
4 位	1433/TCP	199.70 件	－7.0%　（－14.94 件）	3 位	3 位
5 位	23/TCP	356.27 件	－4.0%　（－14.82 件）	1 位	1 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。

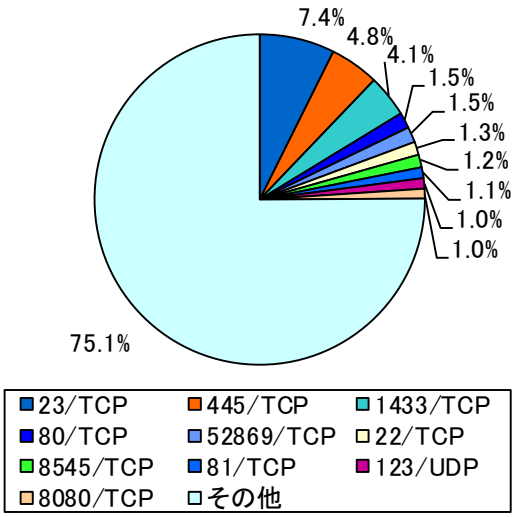

図 2-1　宛先ポート別比率（全て）[i]

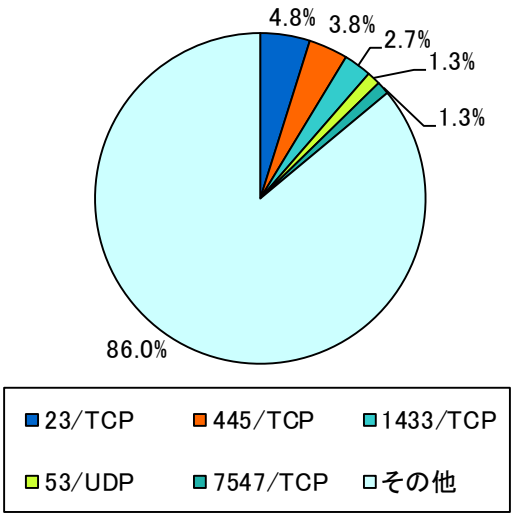

図 2-2　宛先ポート別比率（日本国内）

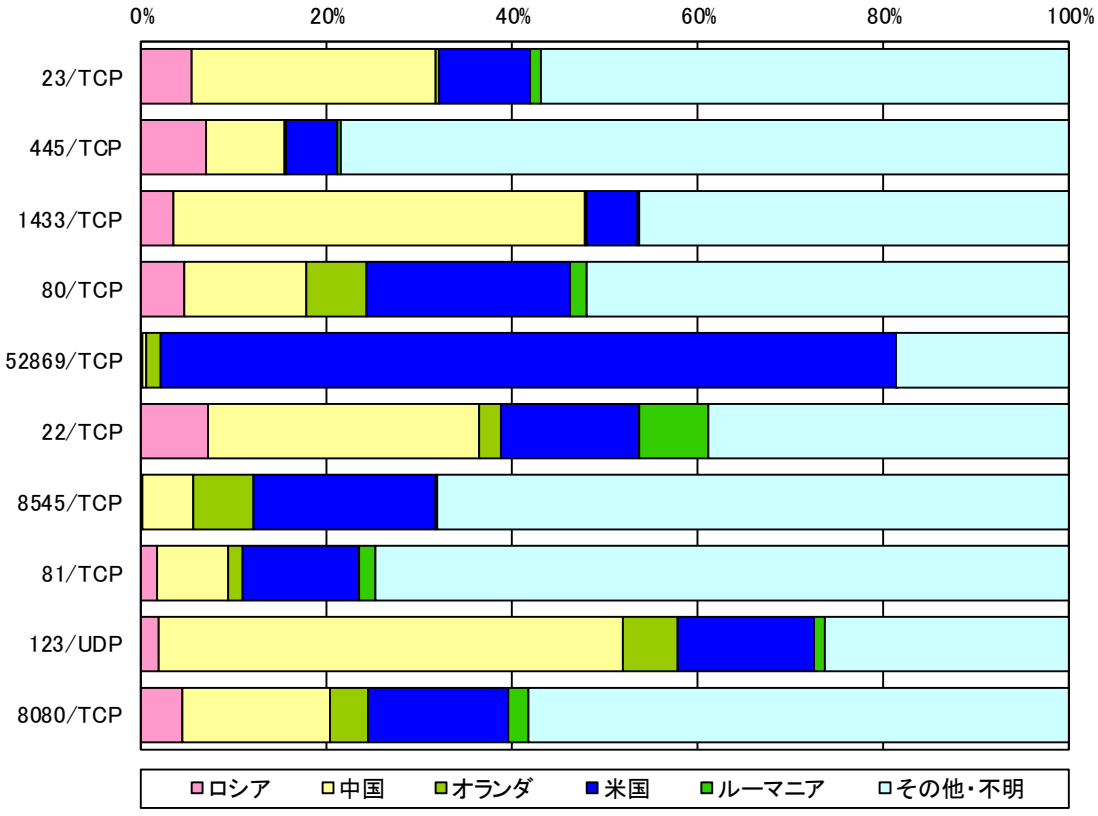

図 2-3　宛先ポート別上位の送信元国・地域別比率 [ii]

[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] 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。

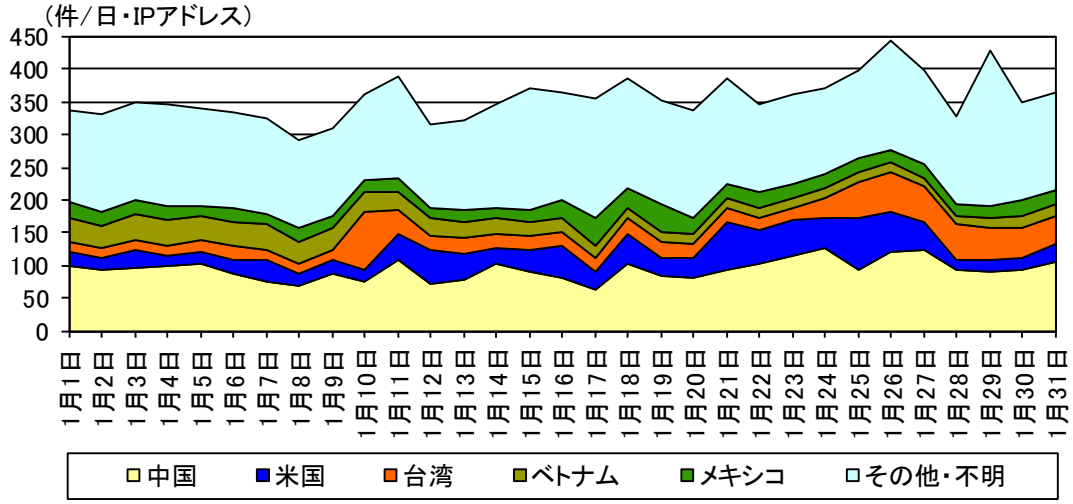

図 2-4　センサーのポート 23/TCP における検知件数の推移

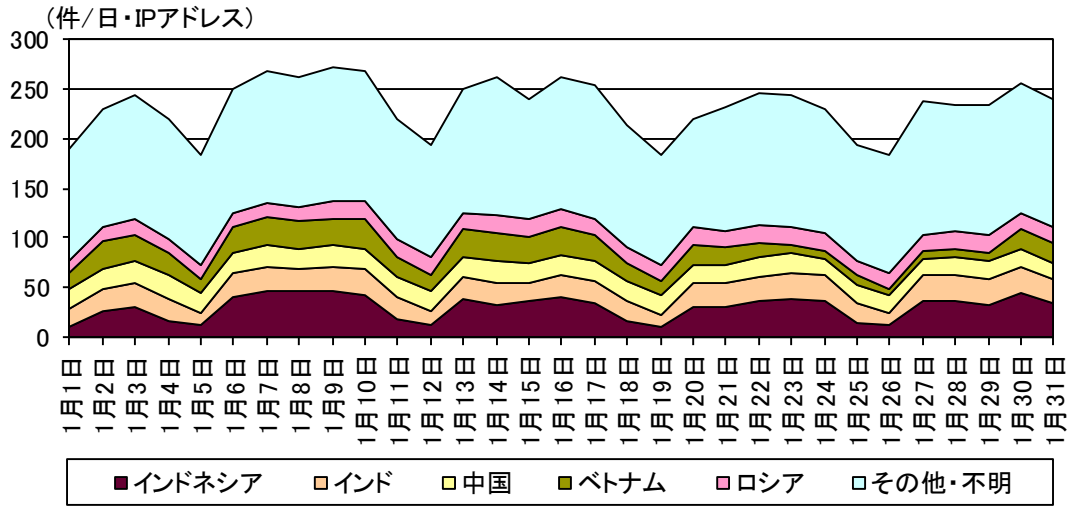

図 2-5　センサーのポート 445/TCP における検知件数の推移

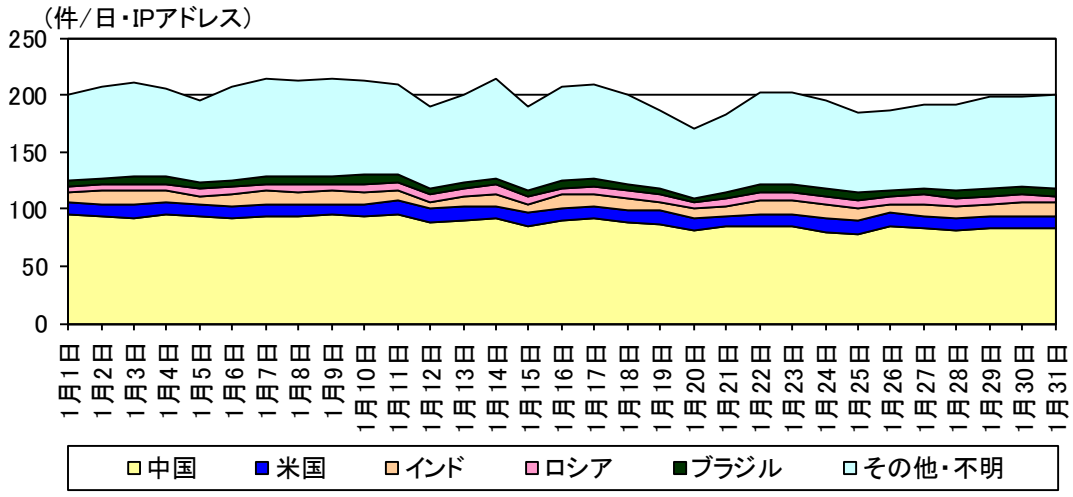

図 2-6　センサーのポート 1433/TCP における検知件数の推移

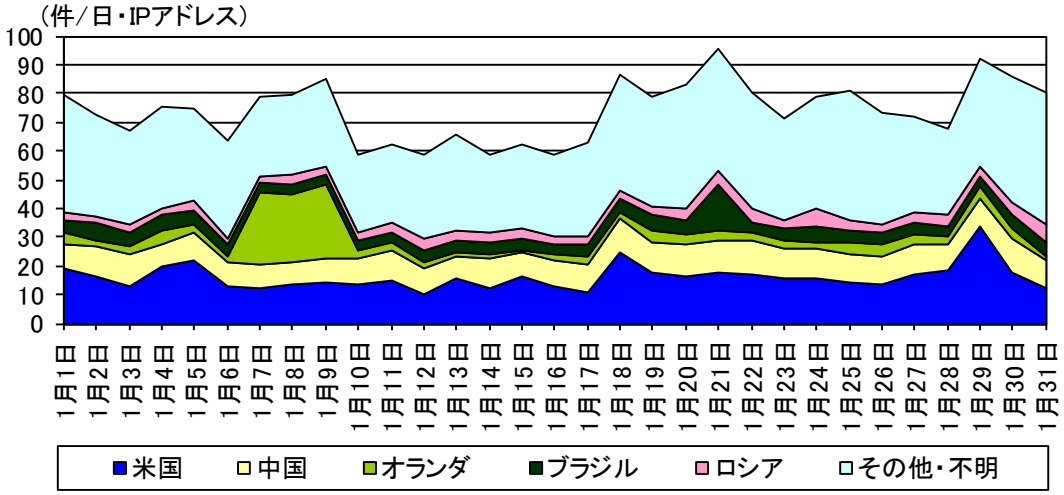

図 2-7　センサーのポート 80/TCP における検知件数の推移

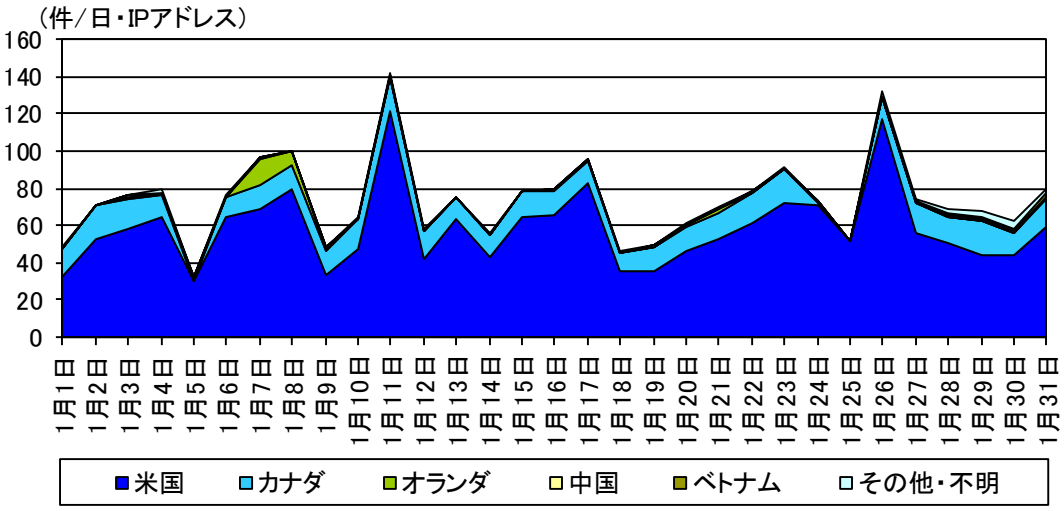

図 2-8　センサーのポート 52869/TCP における検知件数の推移

2-2　送信元国・地域別アクセス検知件数

表 2-4　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	3 位	ロシア	1,322.33 件	＋66.1%　（＋526.40 件）
2 位	2 位	中国	849.45 件	－12.2%　（－117.58 件）
3 位	1 位	オランダ	626.32 件	－55.7%　（－787.56 件）
4 位	4 位	米国	545.70 件	＋3.9%　（＋20.40 件）
5 位	5 位	ルーマニア	134.74 件	－42.3%　（－98.67 件）

表 2-5　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	ロシア	1,322.33 件	＋66.1%　（＋526.40 件）	1 位	3 位
2 位	米国	545.70 件	＋3.9%　（＋20.40 件）	4 位	4 位
3 位	フランス	76.38 件	＋28.7%　（＋17.04 件）	9 位	13 位
4 位	英国	55.32 件	＋32.8%　（＋13.65 件）	13 位	19 位
5 位	イタリア	34.39 件	＋57.0%　（＋12.48 件）	20 位	26 位

表 2-6　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	オランダ	626.32 件	－55.7%　（－787.56 件）	3 位	1 位
2 位	中国	849.45 件	－12.2%　（－117.58 件）	2 位	2 位
3 位	スイス	4.84 件	－95.8%　（－110.34 件）	43 位	7 位
4 位	ルーマニア	134.74 件	－42.3%　（－98.67 件）	5 位	5 位
5 位	ブラジル	52.19 件	－34.0%　（－26.83 件）	15 位	10 位

[i] 一日・1IP アドレス当たり。

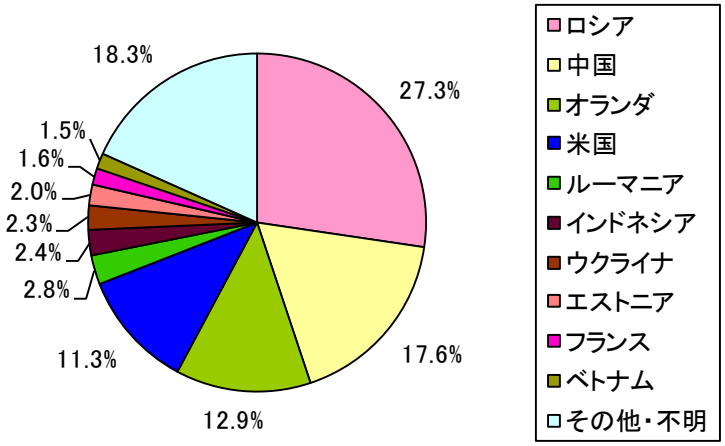

図 2-9　送信元国・地域別比率

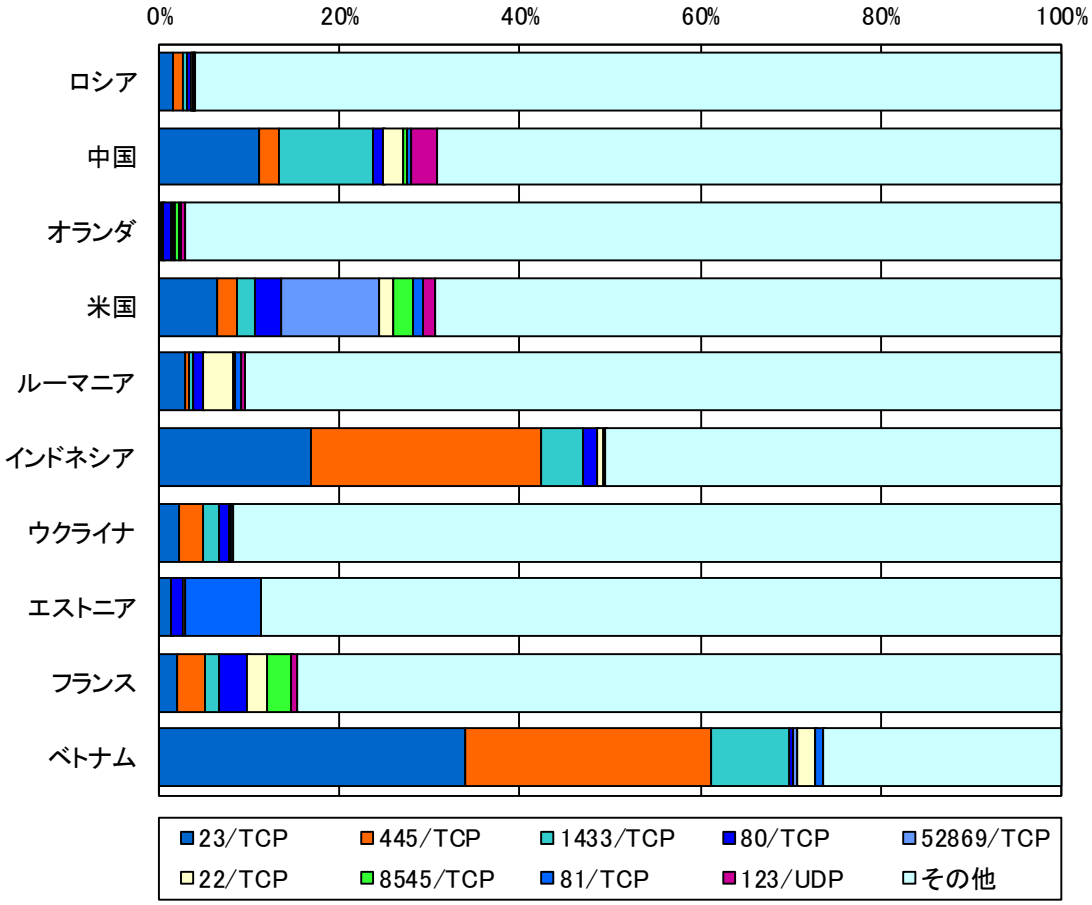

図 2-10　送信元国・地域別上位の宛先ポート別比率

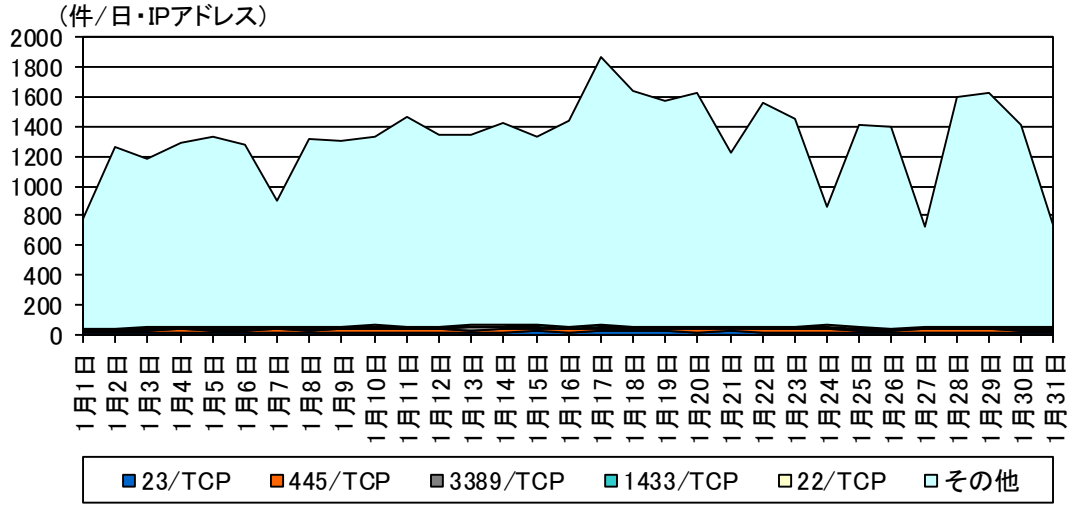

図 2-11　ロシアからの検知件数の推移

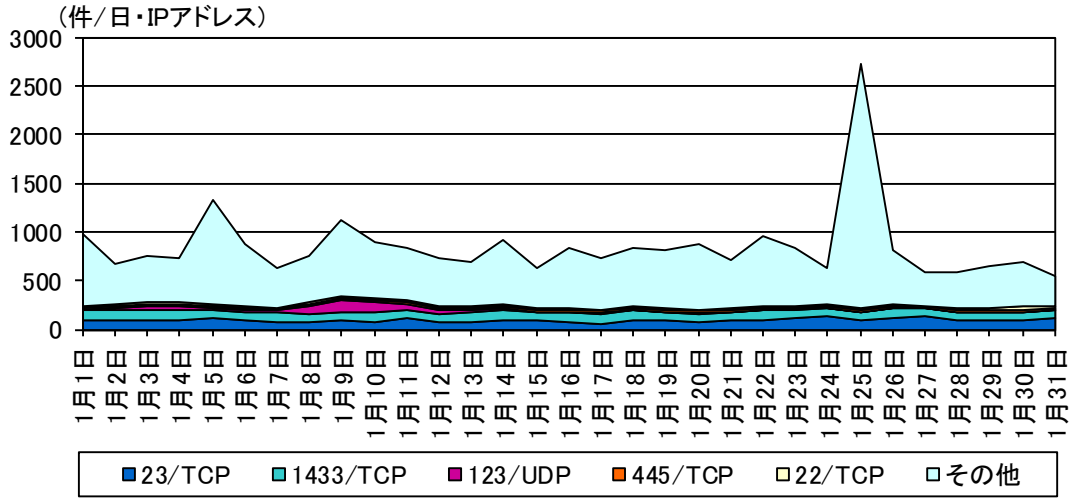

図 2-12　中国からの検知件数の推移

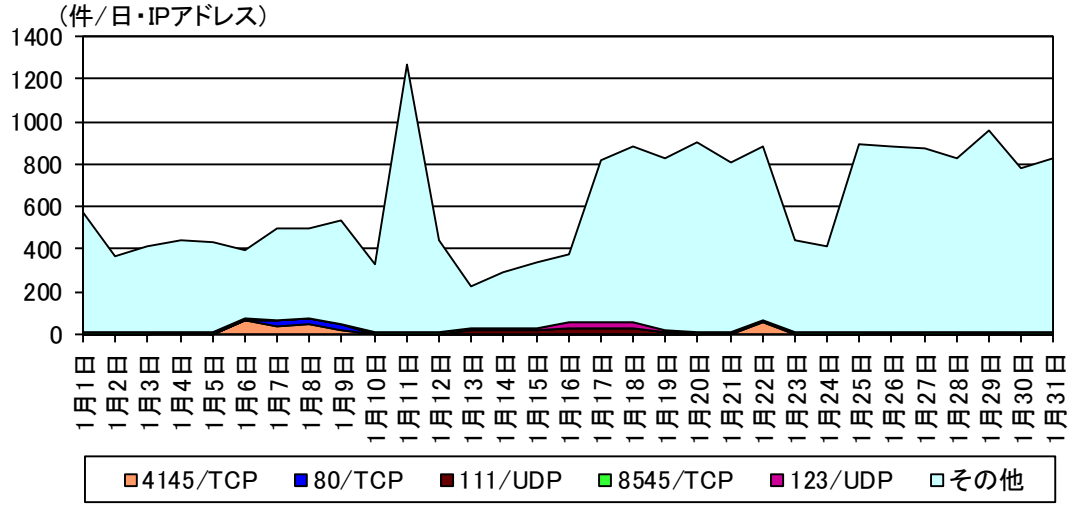

図 2-13　オランダからの検知件数の推移

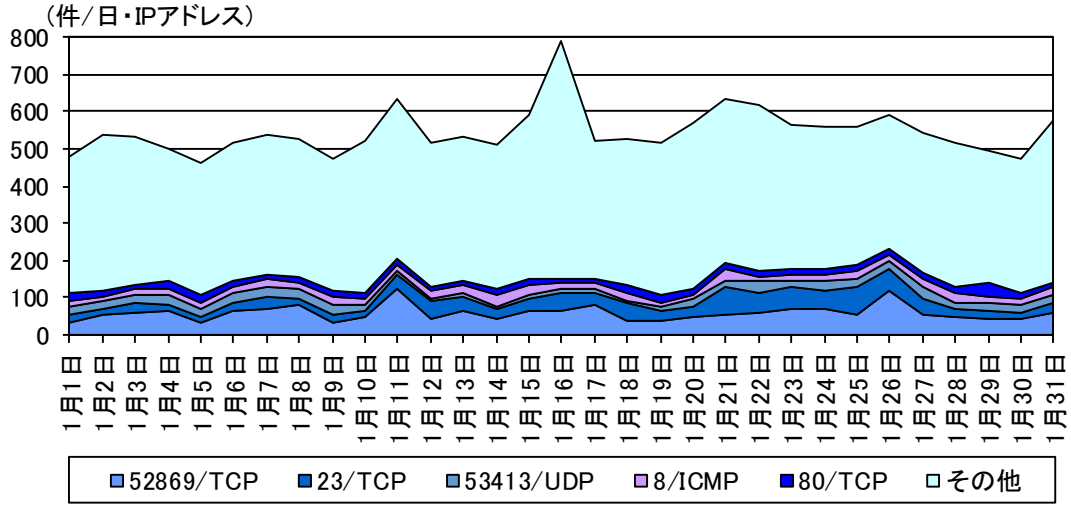

図 2-14　米国からの検知件数の推移

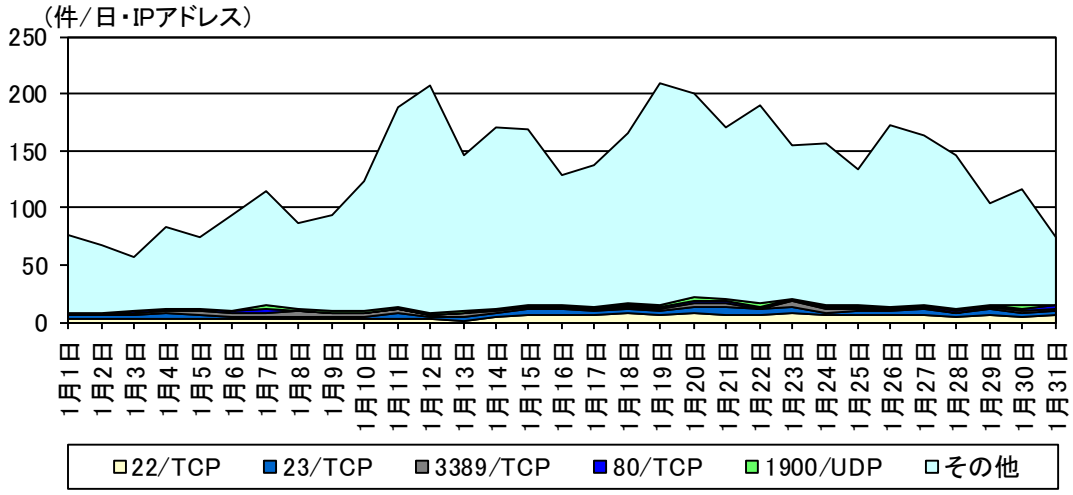

図 2-15　ルーマニアからの検知件数の推移

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	Microsoft Windows Terminal server	319.47 件	＋10.2%　（＋29.69 件）	1 位	
2 位	1 位	INDICATOR-SCAN	270.28 件	－20.1%　（－68.16 件）		1 位
3 位	3 位	SMBv1	110.18 件	－4.3%　（－4.99 件）		3 位
4 位	12 位	OS-WINDOWS	26.26 件	－ [ii]　（＋20.61 件）	2 位	
5 位	5 位	ICMP	23.75 件	－12.1%　（－3.27 件）		4 位

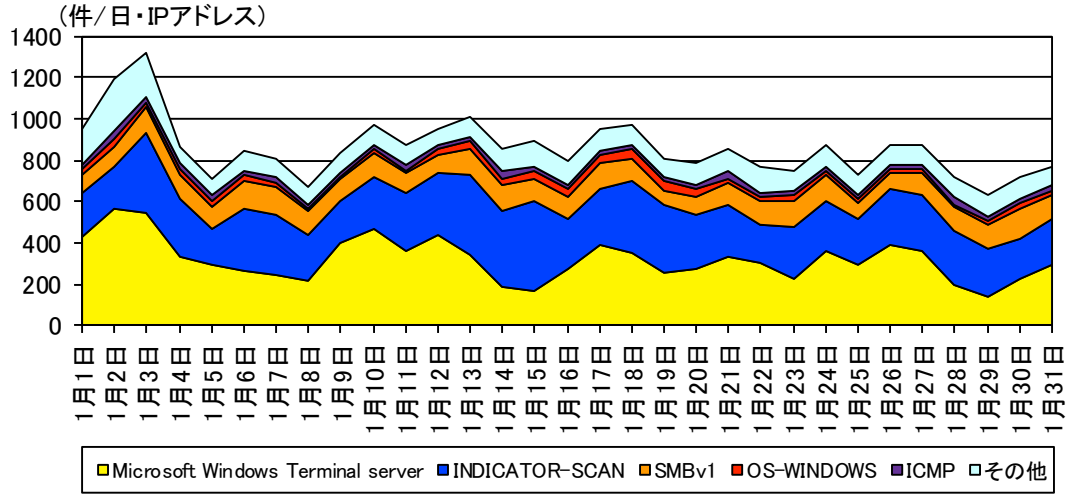

図 3-1　不正侵入等の攻撃手法別検知件数の推移

[i] 一日・1IP アドレス当たり。

[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。

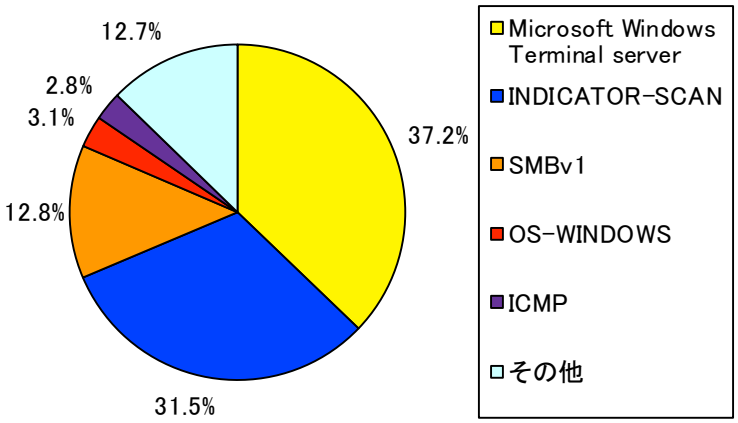

図 3-2 不正侵入等の攻撃手法別検知比率

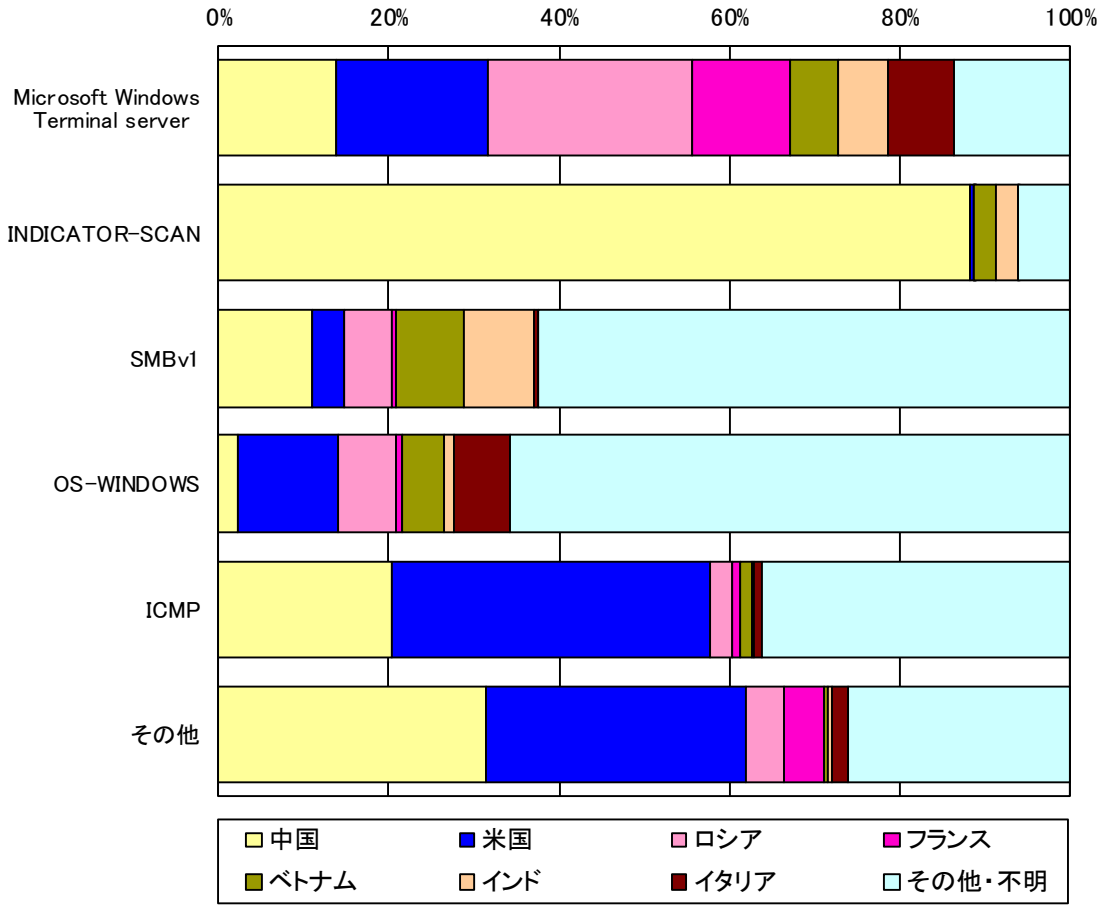

図 3-3 不正侵入等の攻撃手法の国・地域別検知比率

3-2 送信元国・地域別アクセス検知件数

表 3-2 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	334.43 件	－19.3% （－80.19 件）
2 位	3 位	米国	108.09 件	＋108.7% （＋56.31 件）
3 位	2 位	ロシア	89.80 件	－48.4% （－84.12 件）
4 位	4 位	フランス	42.49 件	＋33.3% （＋10.62 件）
5 位	7 位	ベトナム	36.55 件	＋73.9% （＋15.53 件）

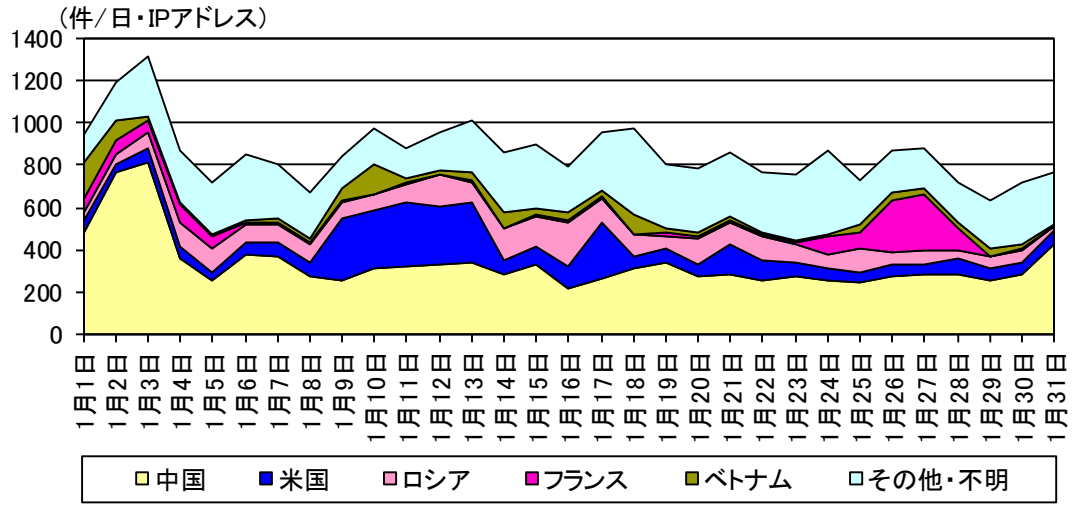

図 3-4 不正侵入等の送信元国・地域別検知件数の推移

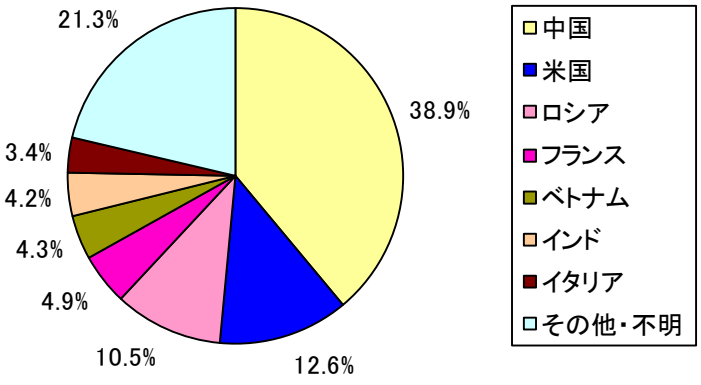

図 3-5 不正侵入等の送信元国・地域別検知比率

[i] 一日・1IP アドレス当たり。

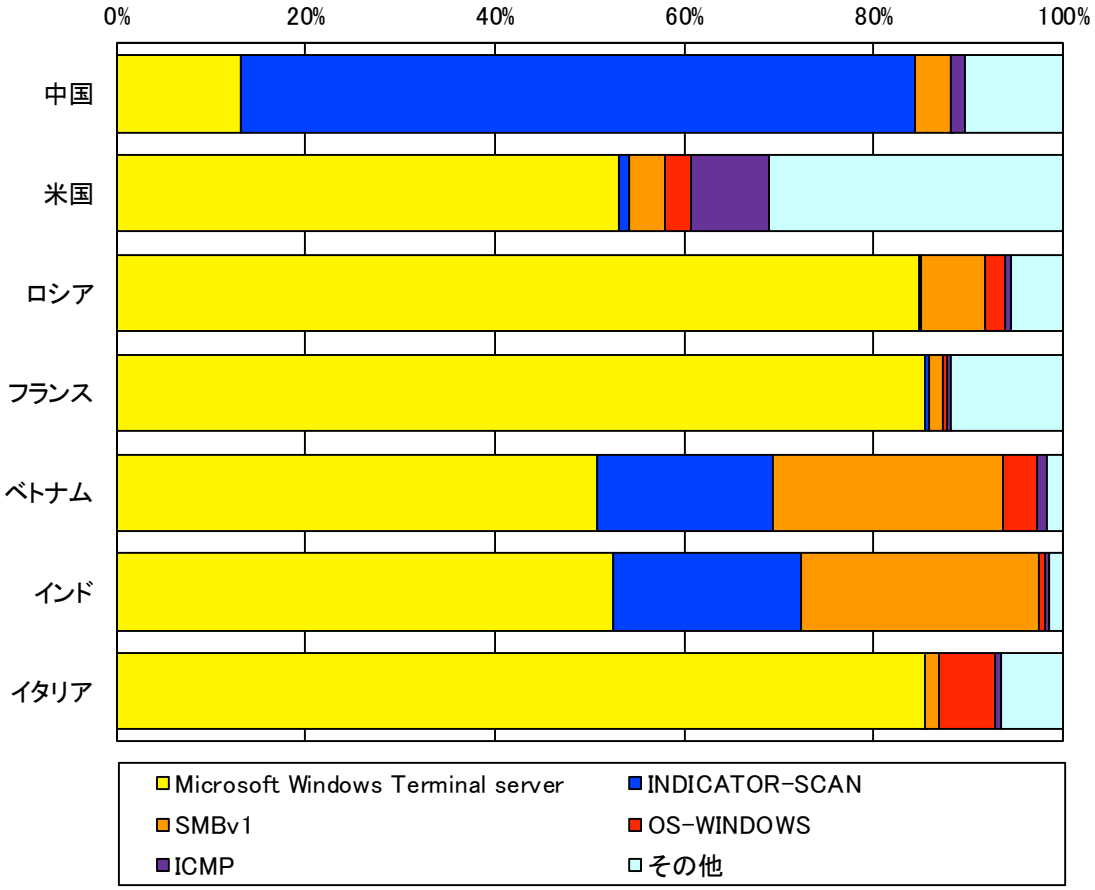

図 3-6 不正侵入等の送信元国・地域別上位の攻撃手法別検知比率

4　DoS 攻撃被害の観測結果

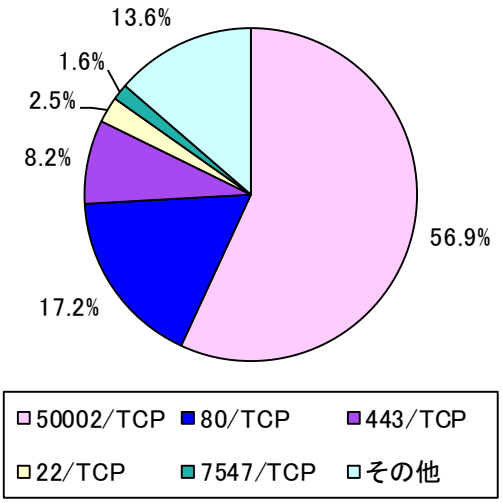

図 4-1　跳ね返りパケット送信元ポート別比率

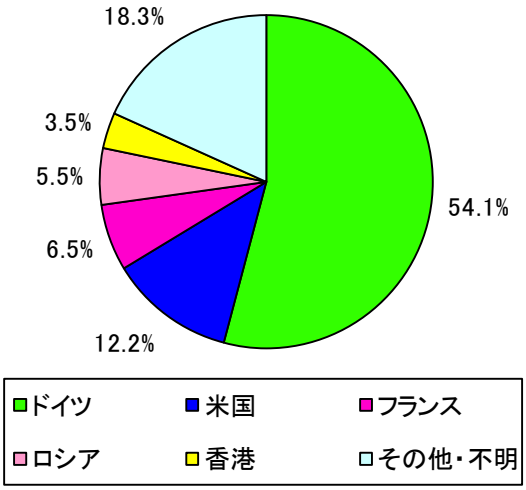

図 4-2　跳ね返りパケット送信元国・地域別比率

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