令和元年11月28日

令和元年10月期観測資料

1　観測結果概要

令和元年10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 4,713.0 件で、令和元年9月期（以下「前期」という。）と比較して 694.1 件（12.8%）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 55,697.8 個で、前期と比較して 1,428.0 個（2.6%）増加しました。

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 778.4 件で、前期と比較して 20.6 件（2.6%）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 5,854.8 個で、前期と比較して 1,914.2 個（24.6%）減少しました。

DoS 攻撃被害検知件数は、一日当たり 8,522.3 件で、前期と比較して 6309.0 件（285.0%）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 3,562.3 個で、前期と比較して 3,329.3 個（1,428.7%）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	419.50 件	－8.5%　（－38.92 件）
2 位	2 位	445/TCP	306.35 件	－23.8%　（－95.82 件）
3 位	11 位	1433/TCP	209.12 件	＋498.2%　（＋174.16 件）
4 位	3 位	22/TCP	72.41 件	－37.6%　（－43.54 件）
5 位	4 位	80/TCP	67.85 件	－1.2%　（－0.83 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	1433/TCP	209.12 件	＋498.2%　（＋174.16 件）	3 位	11 位
2 位	9001/TCP	26.60 件	－[ii]　（＋23.61 件）	19 位	－[ii]
3 位	3306/TCP	29.67 件	＋108.8%　（＋15.46 件）	14 位	25 位
4 位	59013/UDP	10.04 件	－[ii]　（＋10.04 件）	34 位	－[ii]
5 位	51145/UDP	9.87 件	－[ii]　（＋9.87 件）	35 位	－[ii]

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	445/TCP	306.35 件	－23.8%　（－95.82 件）	2 位	2 位
2 位	22/TCP	72.41 件	－37.6%　（－43.54 件）	4 位	3 位
3 位	23/TCP	419.50 件	－8.5%　（－38.92 件）	1 位	1 位
4 位	81/TCP	34.18 件	－39.0%　（－21.89 件）	11 位	6 位
5 位	34567/TCP	30.00 件	－27.3%　（－11.28 件）	13 位	9 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。

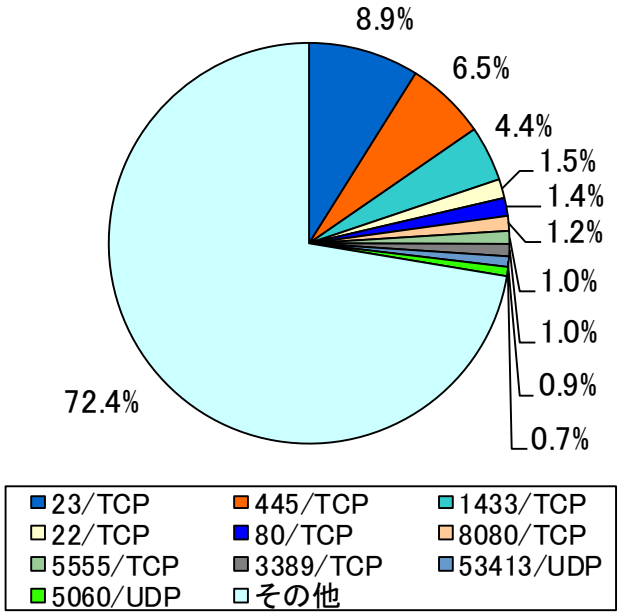

図 2-1　宛先ポート別比率（全て）[i]

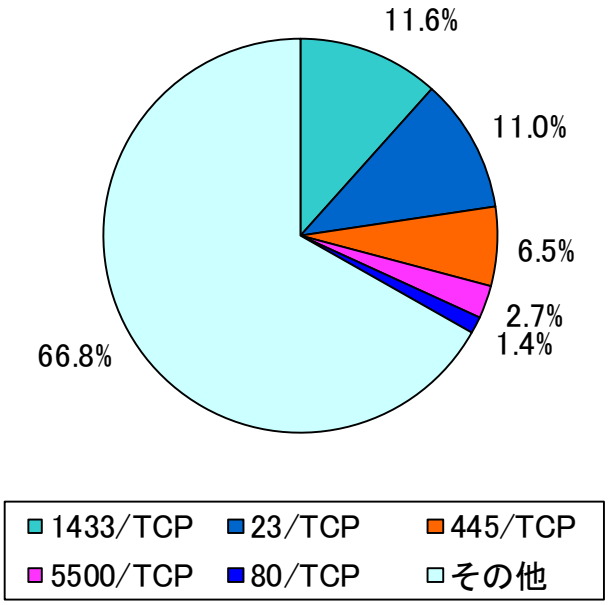

図 2-2　宛先ポート別比率（日本国内）

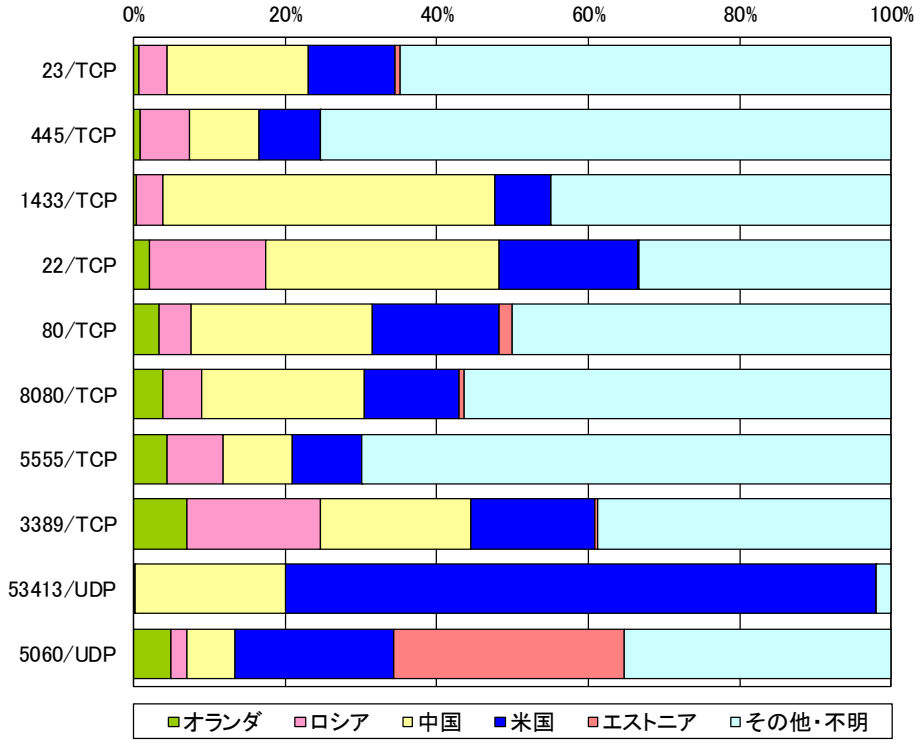

図 2-3　宛先ポート別上位の着信元国・地域別比率 [ii]

[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。

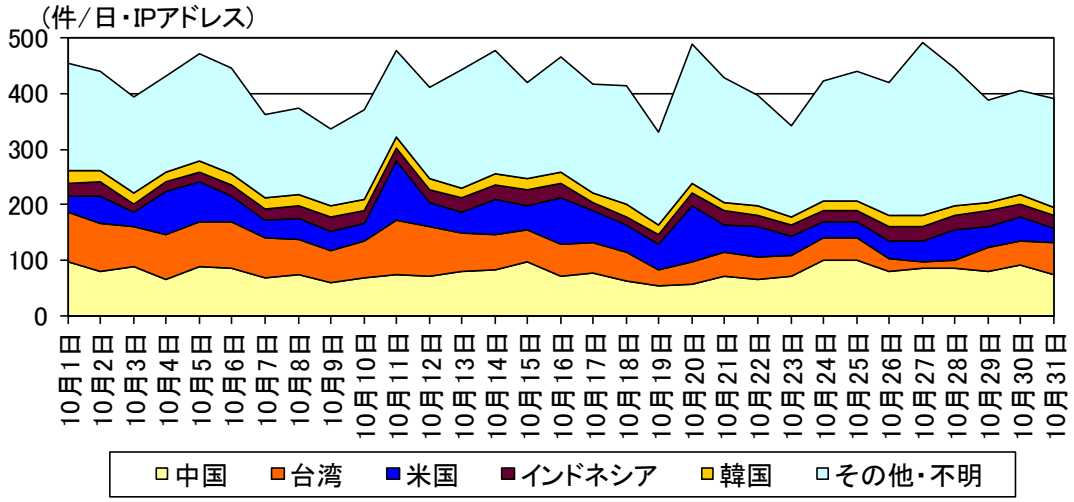

図 2-4　センサーのポート 23/TCP における検知件数の推移

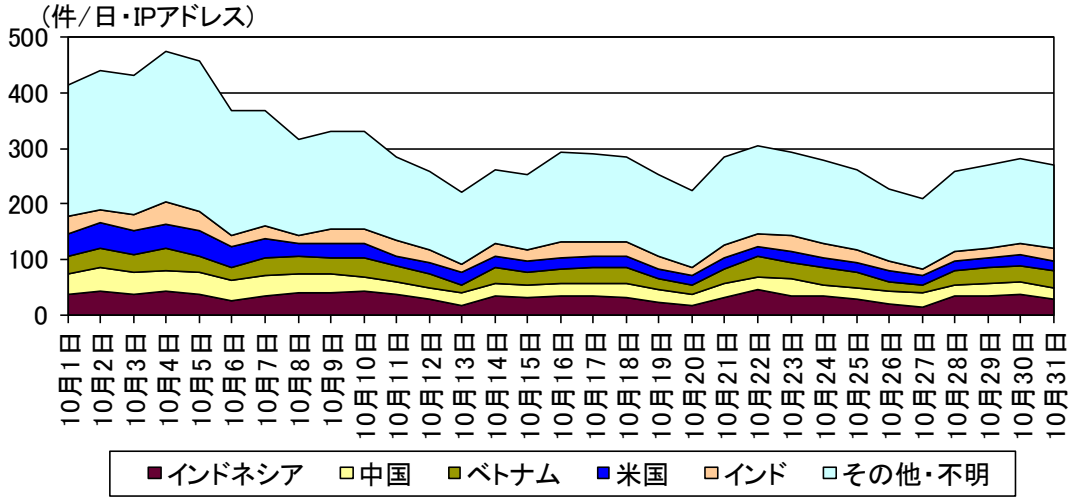

図 2-5　センサーのポート 445/TCP における検知件数の推移

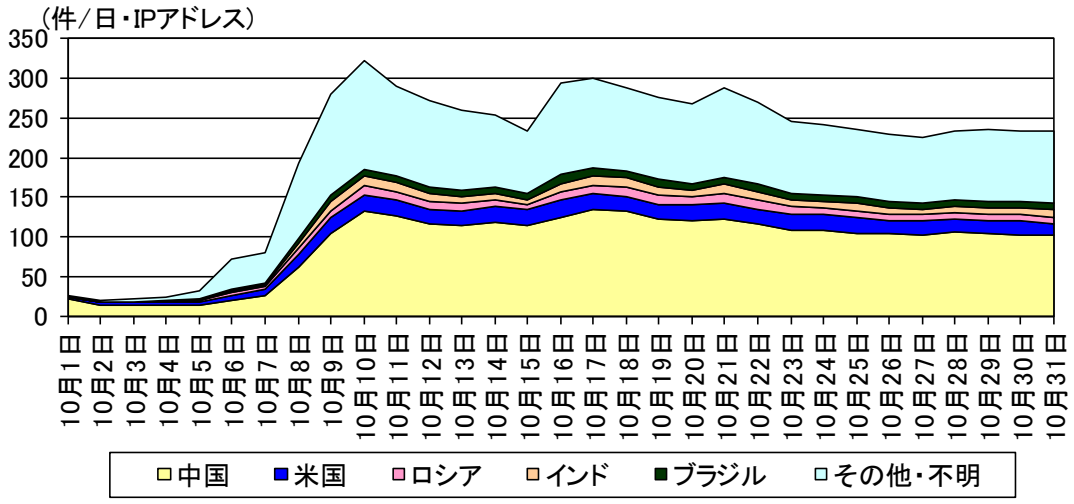

図 2-6　センサーのポート 1433/TCP における検知件数の推移

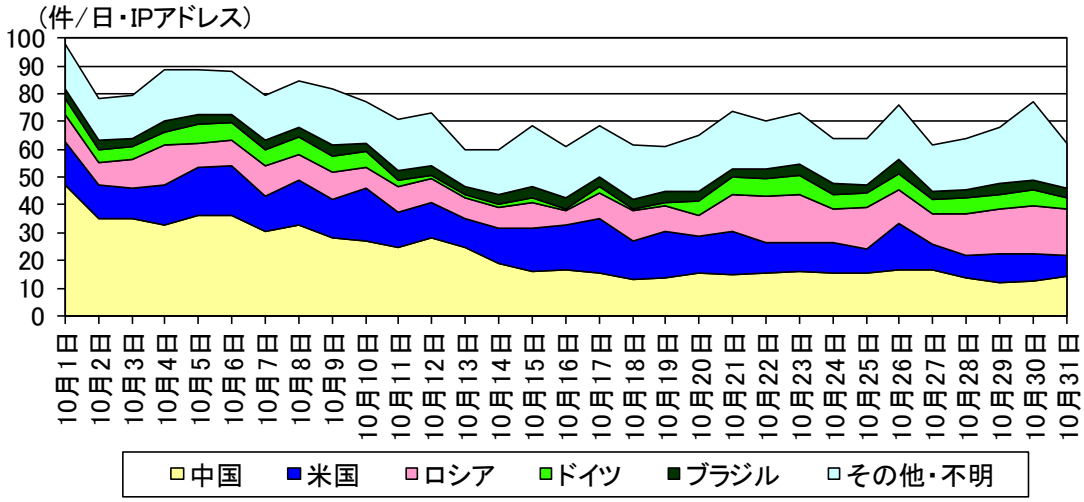

図 2-7　センサーのポート 22/TCP における検知件数の推移

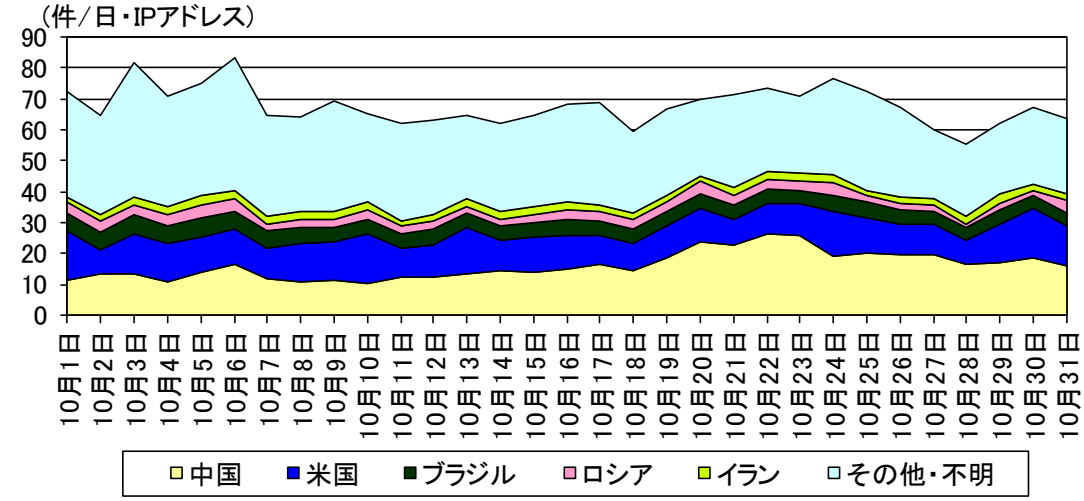

図 2-8　センサーのポート 80/TCP における検知件数の推移

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	オランダ	1,000.32 件	－37.6%　（－602.42 件）
2 位	2 位	ロシア	883.32 件	＋7.7%　（＋63.28 件）
3 位	3 位	中国	613.64 件	＋3.7%　（＋21.69 件）
4 位	4 位	米国	581.13 件	＋5.0%　（＋27.70 件）
5 位	7 位	エストニア	129.15 件	＋5.8%　（＋7.06 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	883.32 件	＋7.7%　（＋63.28 件）	2 位	2 位
2 位	米国	581.13 件	＋5.0%　（＋27.70 件）	4 位	4 位
3 位	カナダ	45.77 件	＋94.1%　（＋22.18 件）	16 位	26 位
4 位	中国	613.64 件	＋3.7%　（＋21.69 件）	3 位	3 位
5 位	インドネシア	127.58 件	＋14.6%　（＋16.28 件）	6 位	9 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	オランダ	1,000.32 件	－37.6%　（－602.42 件）	1 位	1 位
2 位	英国	36.49 件	－78.5%　（－133.55 件）	17 位	5 位
3 位	スイス	1.20 件	－97.5%　（－47.36 件）	77 位	16 位
4 位	スペイン	98.47 件	－22.4%　（－28.41 件）	9 位	6 位
5 位	フランス	75.70 件	－23.6%　（－23.43 件）	10 位	11 位

[i] 一日・1IP アドレス当たり。

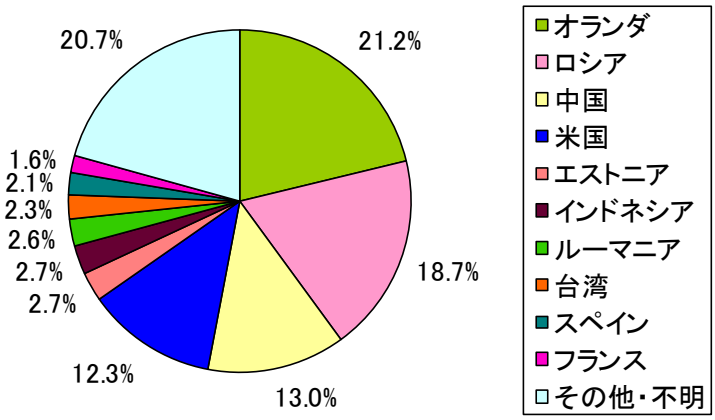

図 2-9　着信元国・地域別比率

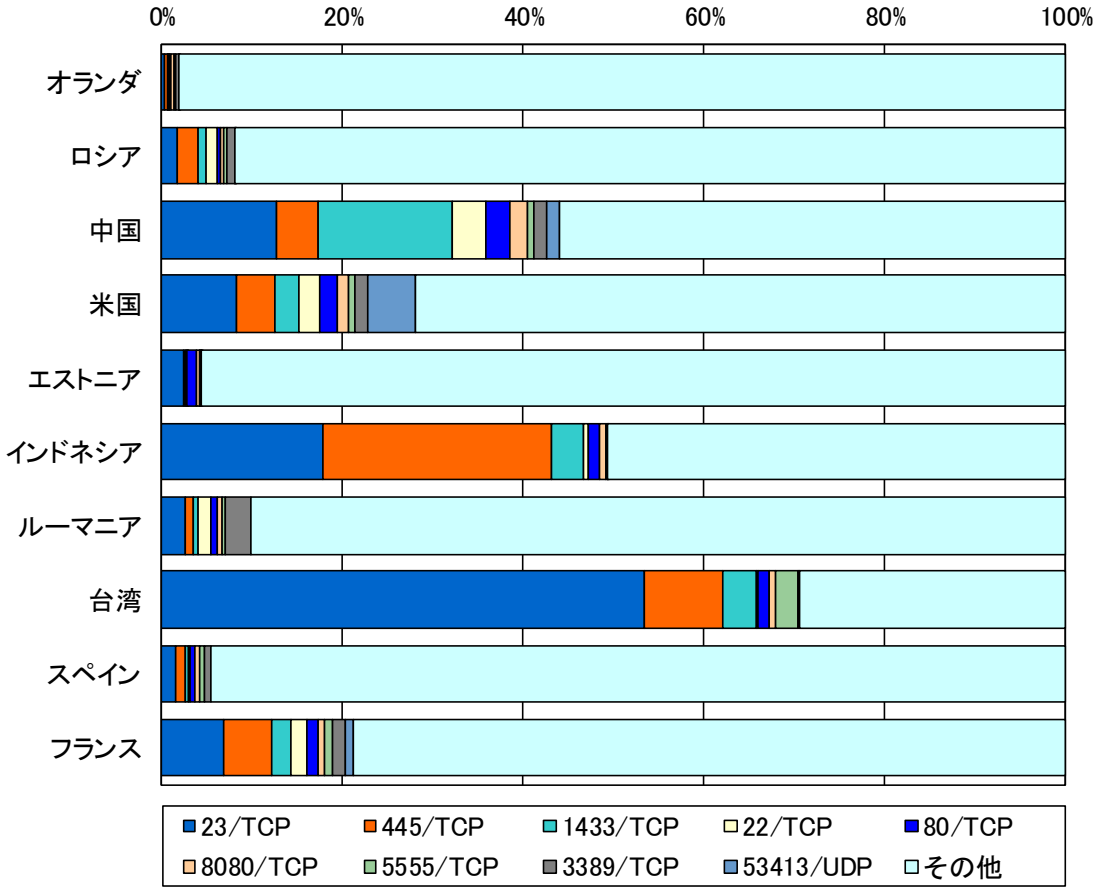

図 2-10　着信元国・地域別上位の宛先ポート別比率

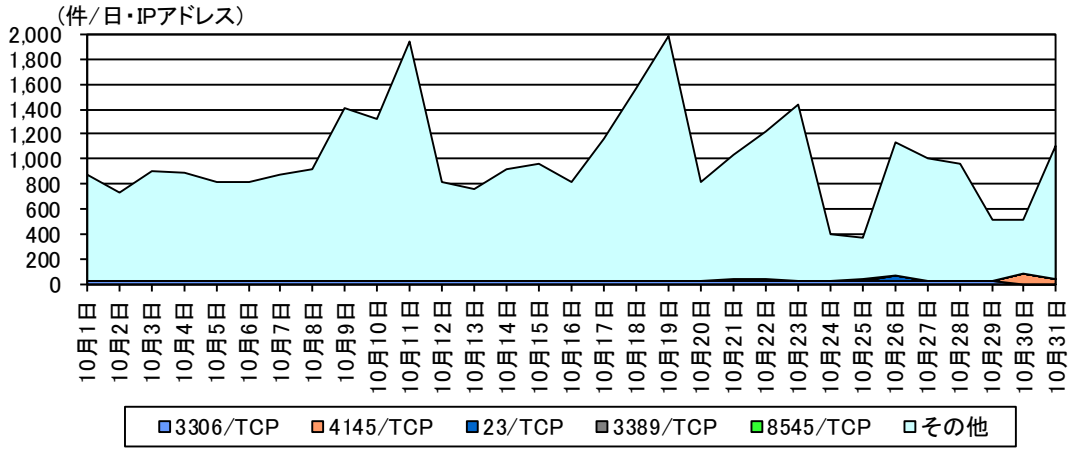

図 2-11　オランダからの検知件数の推移

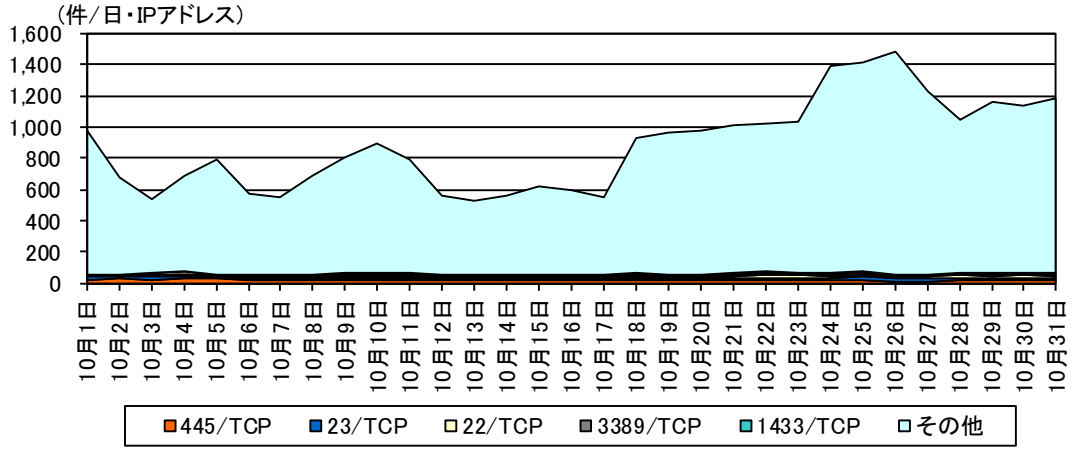

図 2-12　ロシアからの検知件数の推移

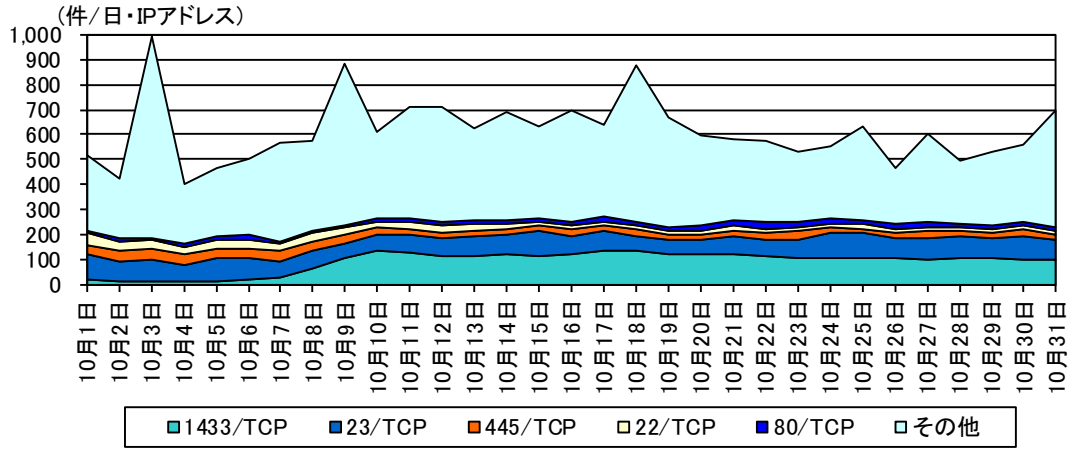

図 2-13　中国からの検知件数の推移

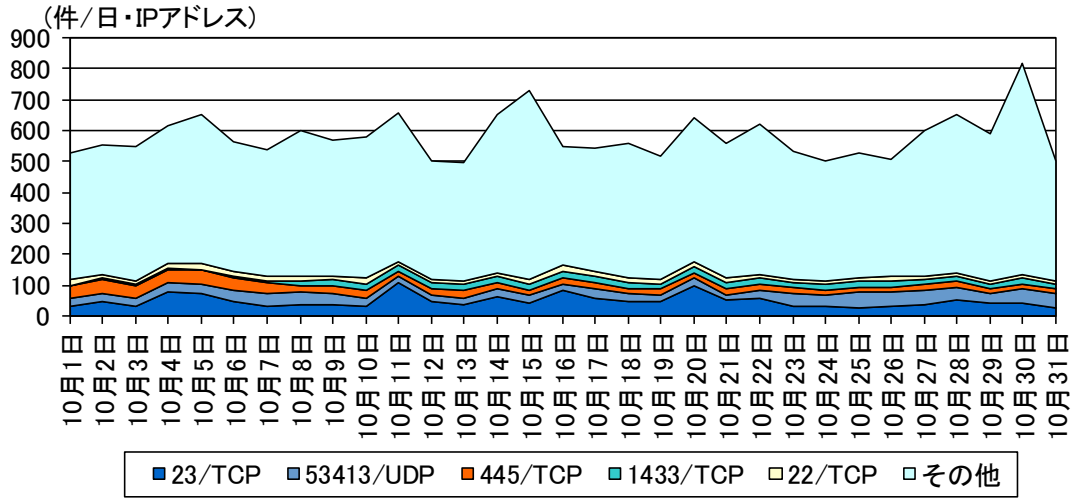

図 2-14　米国からの検知件数の推移

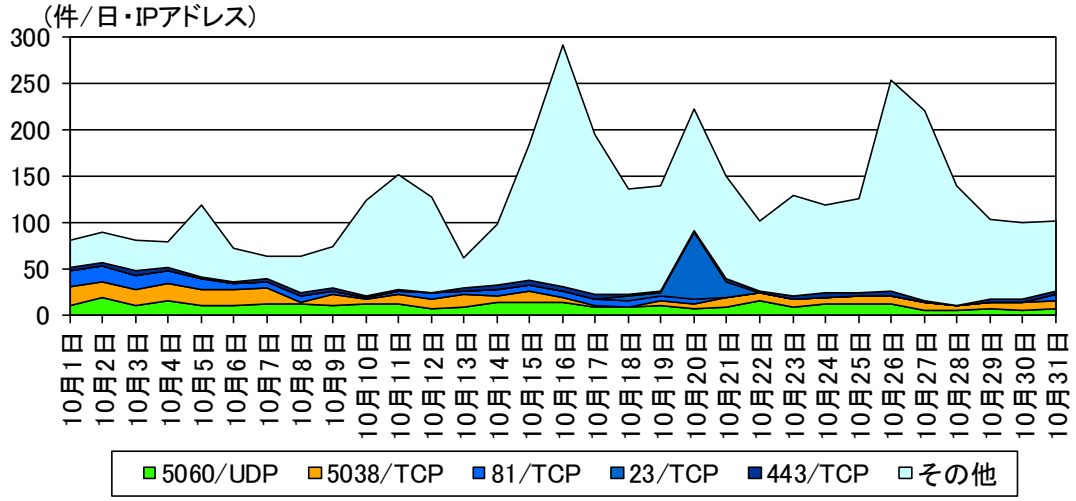

図 2-15　エストニアからの検知件数の推移

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	355.70 件	＋46.2%　（＋112.48 件）	1 位	
2 位	2 位	Microsoft Windows Terminal server	189.59 件	－16.7%　（－38.00 件）		2 位
3 位	3 位	SMBv1	92.43 件	－45.8%　（－78.11 件）		1 位
4 位	5 位	ICMP	25.94 件	＋7.9%　（＋1.90 件）	3 位	
5 位	4 位	VOIP	22.70 件	－44.3%　（－18.06 件）		3 位

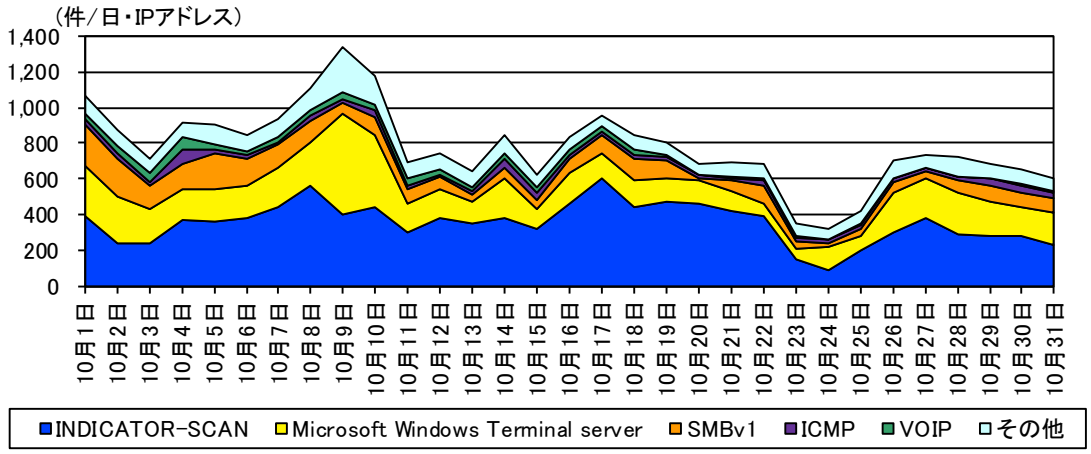

図 3-1　不正侵入等の攻撃手法別検知件数の推移

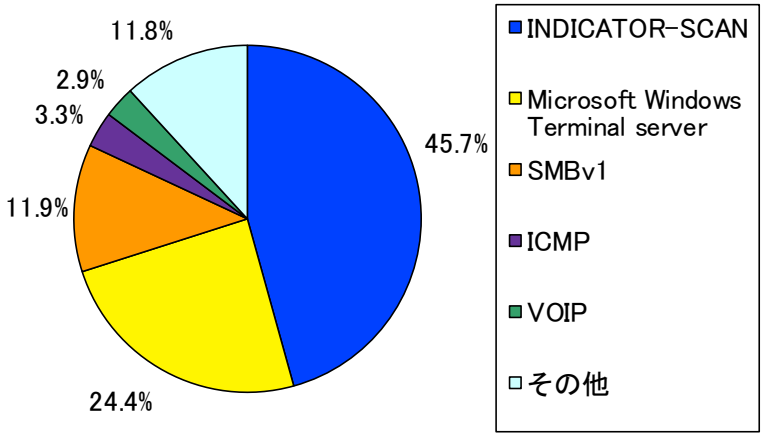

図 3-2　不正侵入等の攻撃手法別検知比率

[i] 一日・1IP アドレス当たり。

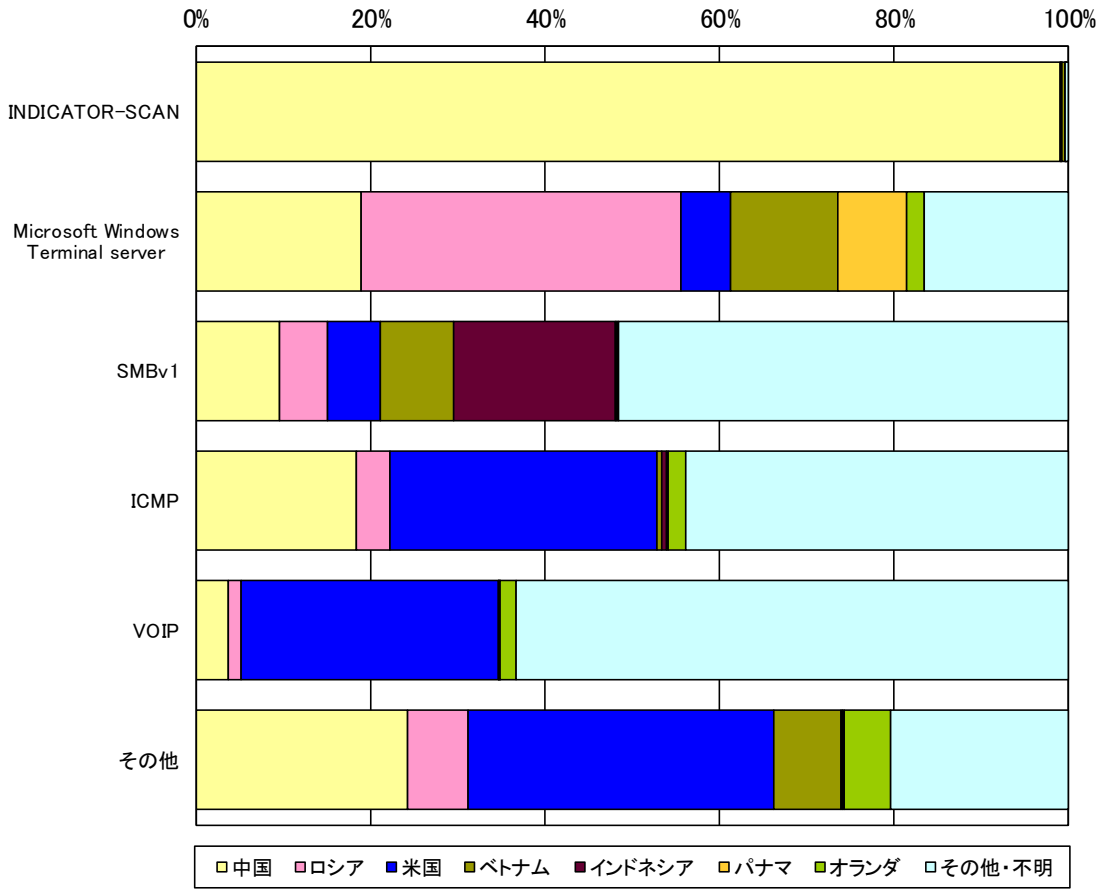

図 3-3 不正侵入等の攻撃手法の国・地域別検知比率

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	425.13 件	＋35.8% （＋111.98 件）
2 位	2 位	ロシア	82.49 件	－8.4% （－7.59 件）
3 位	3 位	米国	63.81 件	－18.1% （－14.11 件）
4 位	4 位	ベトナム	39.10 件	－31.0% （－17.55 件）
5 位	5 位	インドネシア	17.87 件	－31.4% （－8.17 件）

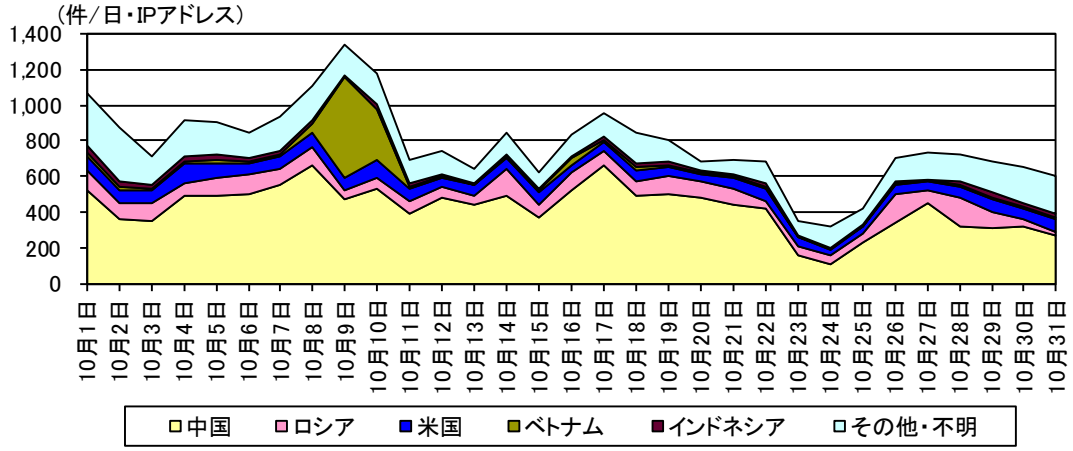

図 3-4 不正侵入等の着信元国・地域別検知件数の推移

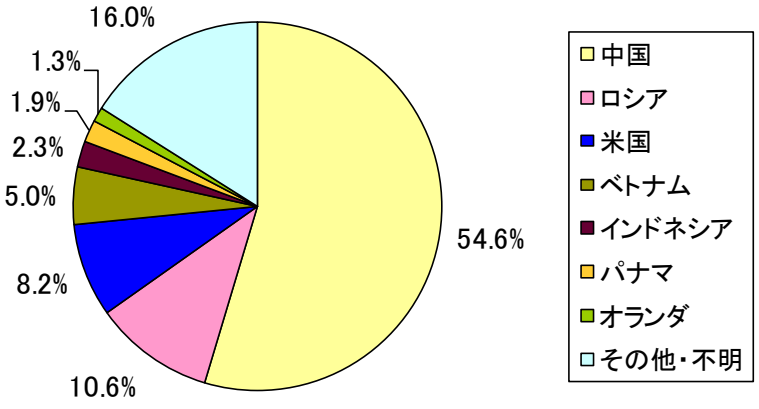

図 3-5 不正侵入等の着信元国・地域別検知比率

[i] 一日・1IP アドレス当たり。

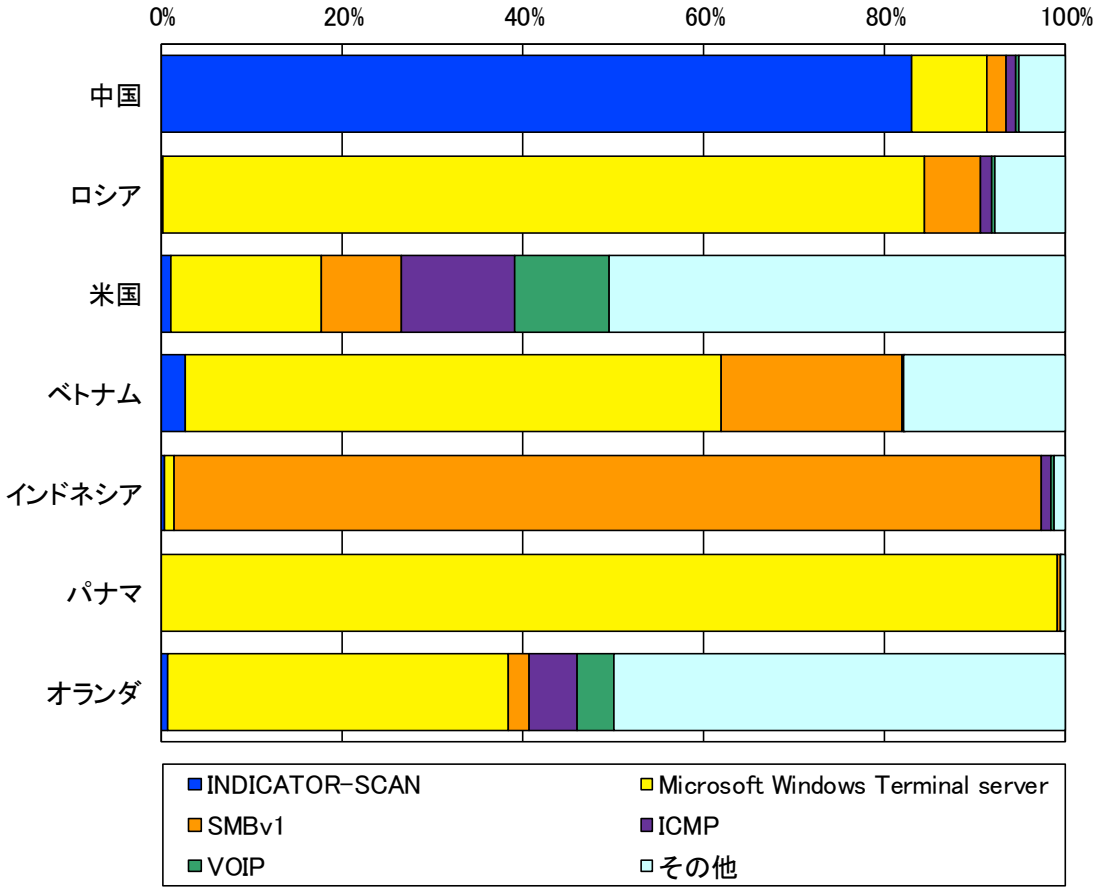

図 3-6 不正侵入等の着信元国・地域別上位の攻撃手法別検知比率

4　DoS 攻撃被害の観測結果

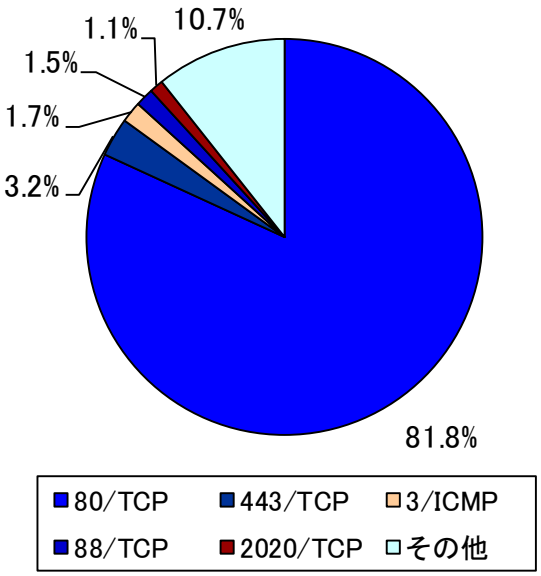

図 4-1　跳ね返りパケット着信元ポート別比率

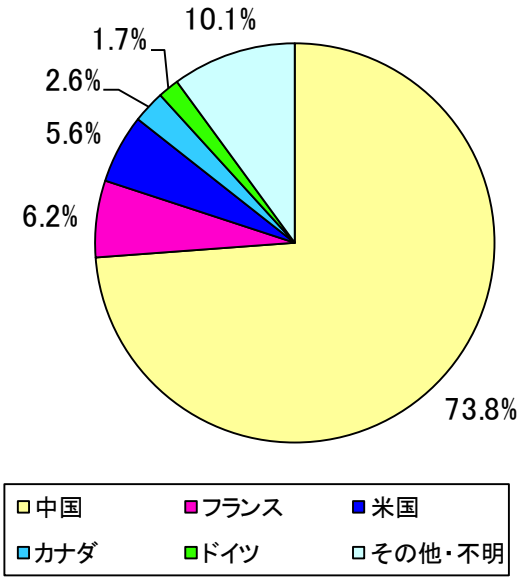

図 4-2　跳ね返りパケット着信元国・地域別比率

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