令和元年10月2日

令和元年８月期観測資料

1　観測結果概要

令和元年８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 4,576.2 件で、令和元年7月期（以下「前期」という。）と比較して 688.2 件（17.7%）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 49,004.3 個で、前期と比較して 2,834.5 個（6.1%）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 625.9 件で、前期と比較して 46.0 件（6.8%）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 7,607.7 個で、前期と比較して 407.9 個（5.1%）減少しました。

DoS 攻撃被害検知件数は、一日当たり 2,866.5 件で、前期と比較して 4,908.8 件（63.1%）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 228.9 個で、前期と比較して 5.9 個（2.5%）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	452.95 件	＋2.5%　（＋11.19 件）
2 位	2 位	445/TCP	392.96 件	－0.3%　（－1.21 件）
3 位	3 位	22/TCP	106.59 件	＋18.3%　（＋16.51 件）
4 位	6 位	52869/TCP	68.43 件	＋49.4%　（＋22.63 件）
5 位	5 位	80/TCP	57.95 件	－3.0%　（－1.79 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	51.18 件	＋277.8%　（＋37.63 件）	9 位	26 位
2 位	52869/TCP	68.43 件	＋49.4%　（＋22.63 件）	4 位	6 位
3 位	5555/TCP	49.37 件	＋69.4%　（＋20.23 件）	10 位	13 位
4 位	22/TCP	106.59 件	＋18.3%　（＋16.51 件）	3 位	3 位
5 位	81/TCP	56.02 件	＋39.5%　（＋15.86 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	37215/TCP	32.94 件	－60.4%　（－50.31 件）	15 位	4 位
2 位	9527/TCP	3.84 件	－80.1%　（－15.47 件）	62 位	24 位
3 位	8545/TCP	33.19 件	－27.0%　（－12.29 件）	13 位	7 位
4 位	8088/TCP	7.98 件	－58.8%　（－11.37 件）	33 位	23 位
5 位	5038/TCP	16.18 件	－39.1%　（－10.39 件）	24 位	16 位

[i] 一日・1IP アドレス当たり。

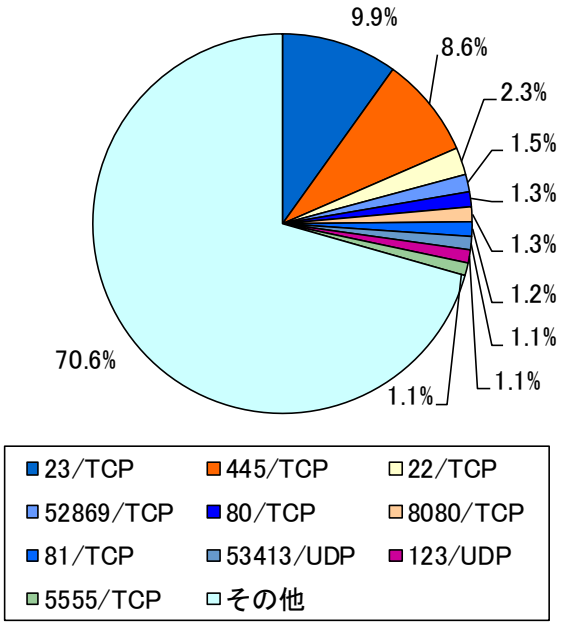

図 2-1　宛先ポート別比率（全て）[i]

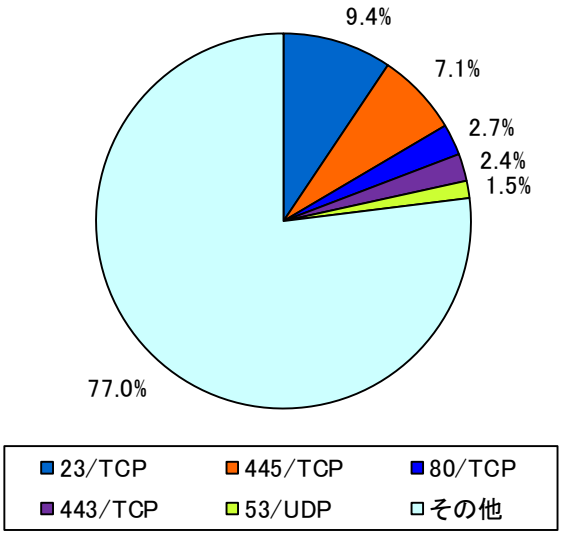

図 2-2　宛先ポート別比率（日本国内）

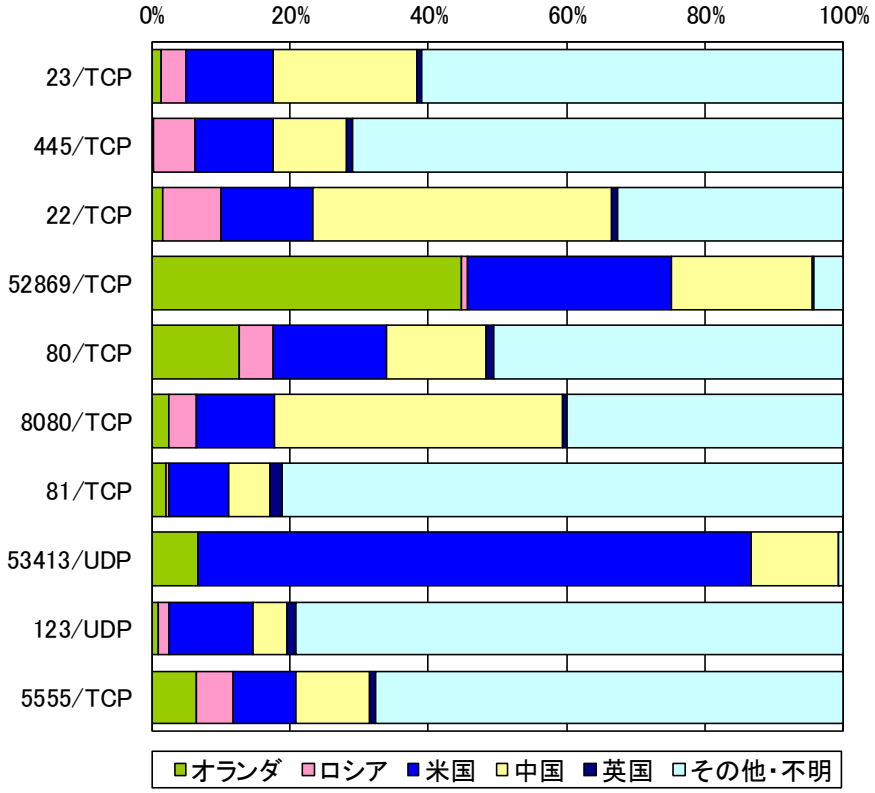

図 2-3　宛先ポート別上位の着信元国・地域別比率 [ii]

[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。

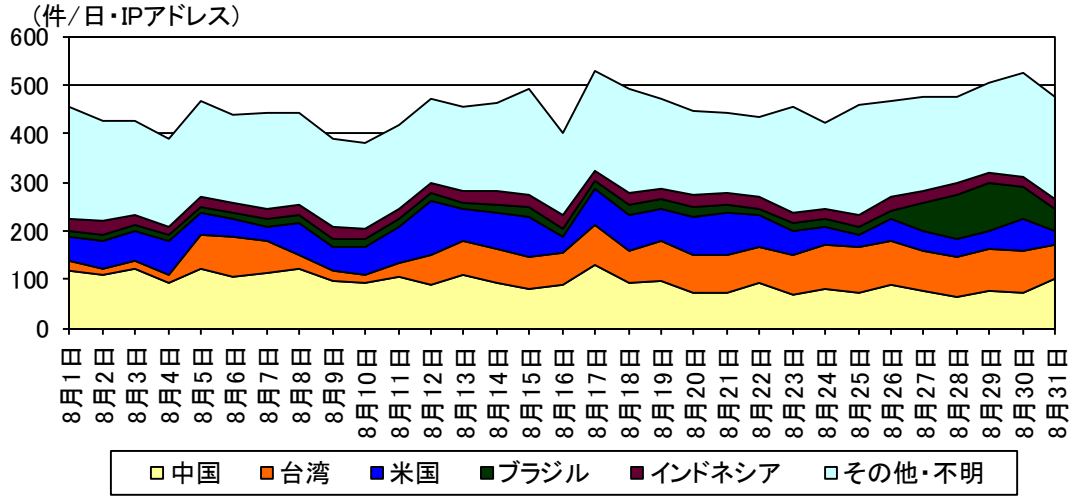

図 2-4　センサーのポート 23/TCP における検知件数の推移

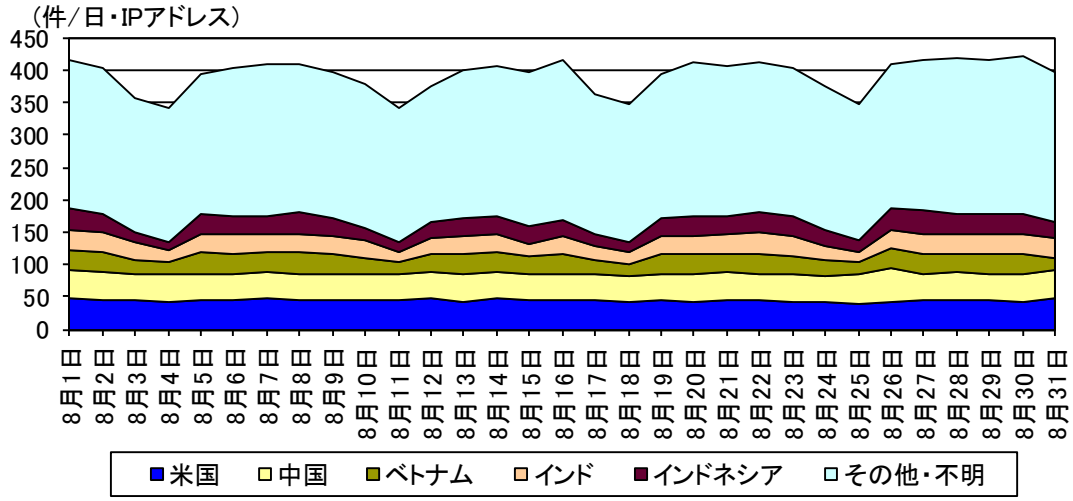

図 2-5　センサーのポート 445/TCP における検知件数の推移

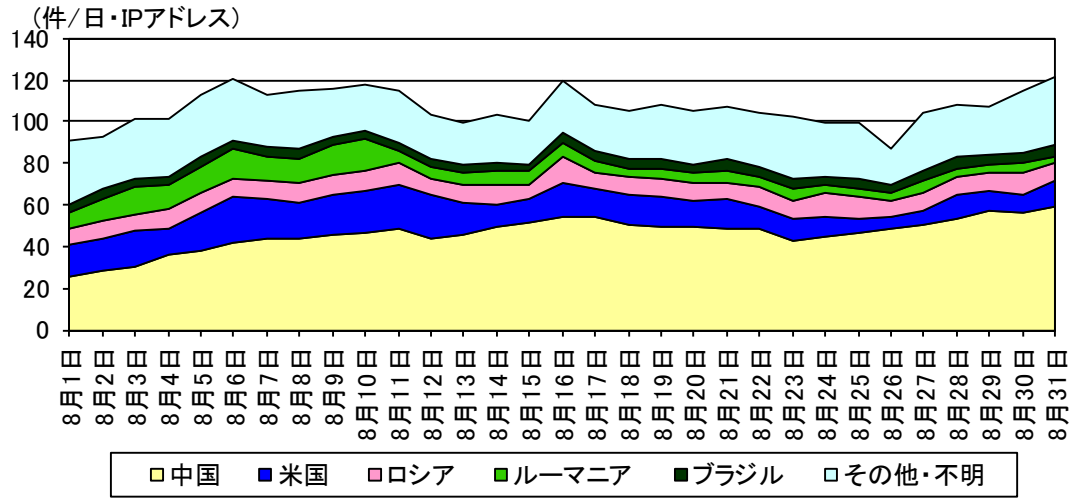

図 2-6　センサーのポート 22/TCP における検知件数の推移

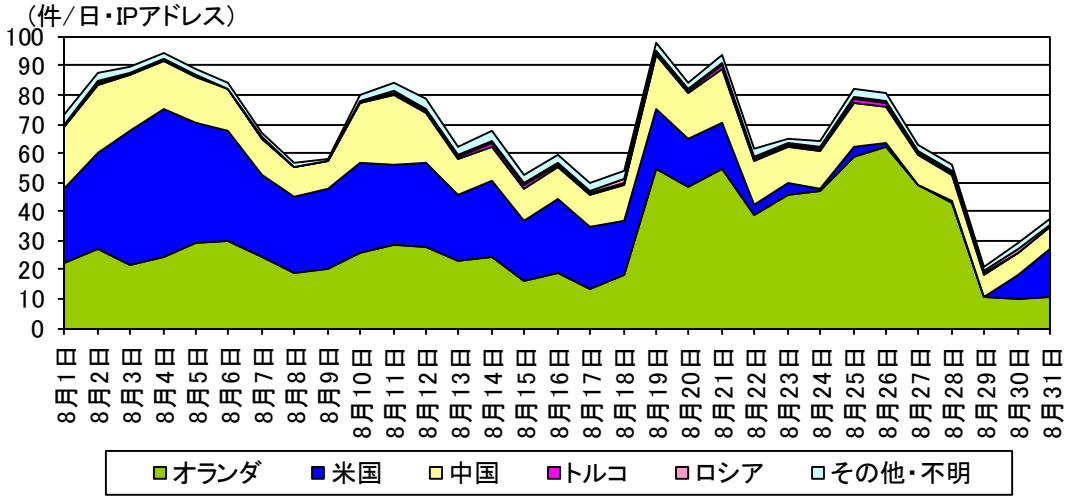

図 2-7　センサーのポート 52869/TCP における検知件数の推移

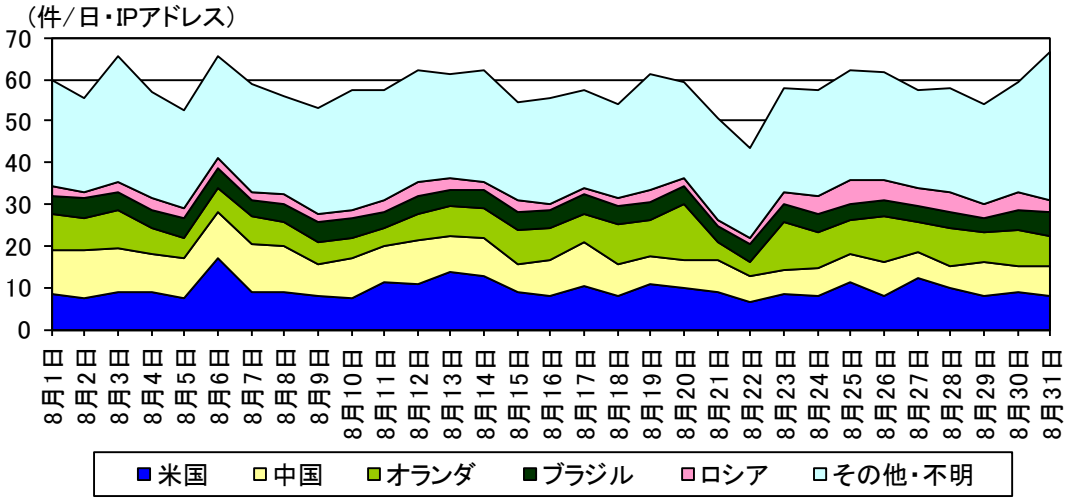

図 2-8　センサーのポート 80/TCP における検知件数の推移

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	2 位	オランダ	1,038.49 件	＋51.1%　（＋351.00 件）
2 位	1 位	ロシア	806.88 件	＋16.2%　（＋112.69 件）
3 位	3 位	米国	597.18 件	＋2.6%　（＋15.15 件）
4 位	4 位	中国	513.86 件	＋2.9%　（＋14.51 件）
5 位	13 位	英国	124.64 件	＋164.8%　（＋77.56 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	オランダ	1,038.49 件	＋51.1%　（＋351.00 件）	1 位	2 位
2 位	ロシア	806.88 件	＋16.2%　（＋112.69 件）	2 位	1 位
3 位	英国	124.64 件	＋164.8%　（＋77.56 件）	5 位	13 位
4 位	スペイン	95.65 件	＋173.4%　（＋60.66 件）	11 位	16 位
5 位	韓国	81.24 件	＋89.8%　（＋38.44 件）	12 位	14 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	ルーマニア	116.30 件	－8.2%　（－10.38 件）	7 位	5 位
2 位	セーシェル	4.22 件	－67.4%　（－8.72 件）	49 位	31 位
3 位	リトアニア	17.55 件	－31.9%　（－8.21 件）	25 位	19 位
4 位	モルドバ	4.87 件	－61.2%　（－7.67 件）	47 位	33 位
5 位	エストニア	116.65 件	－6.0%　（－7.41 件）	6 位	6 位

[i] 一日・1IP アドレス当たり。

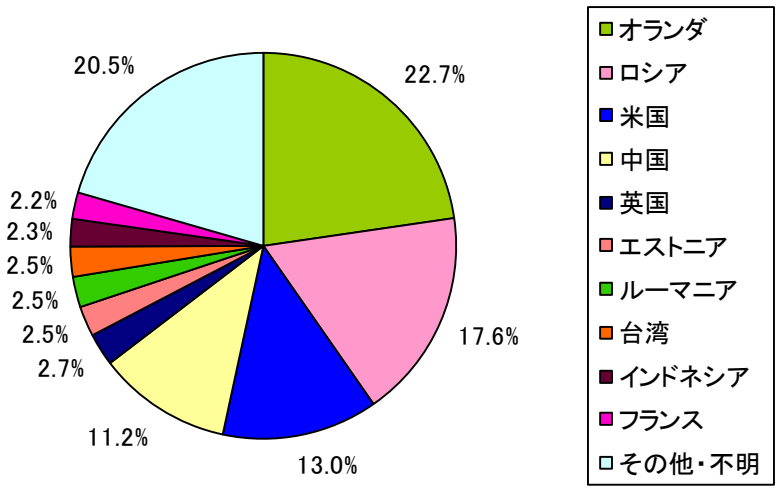

図 2-9　着信元国・地域別比率

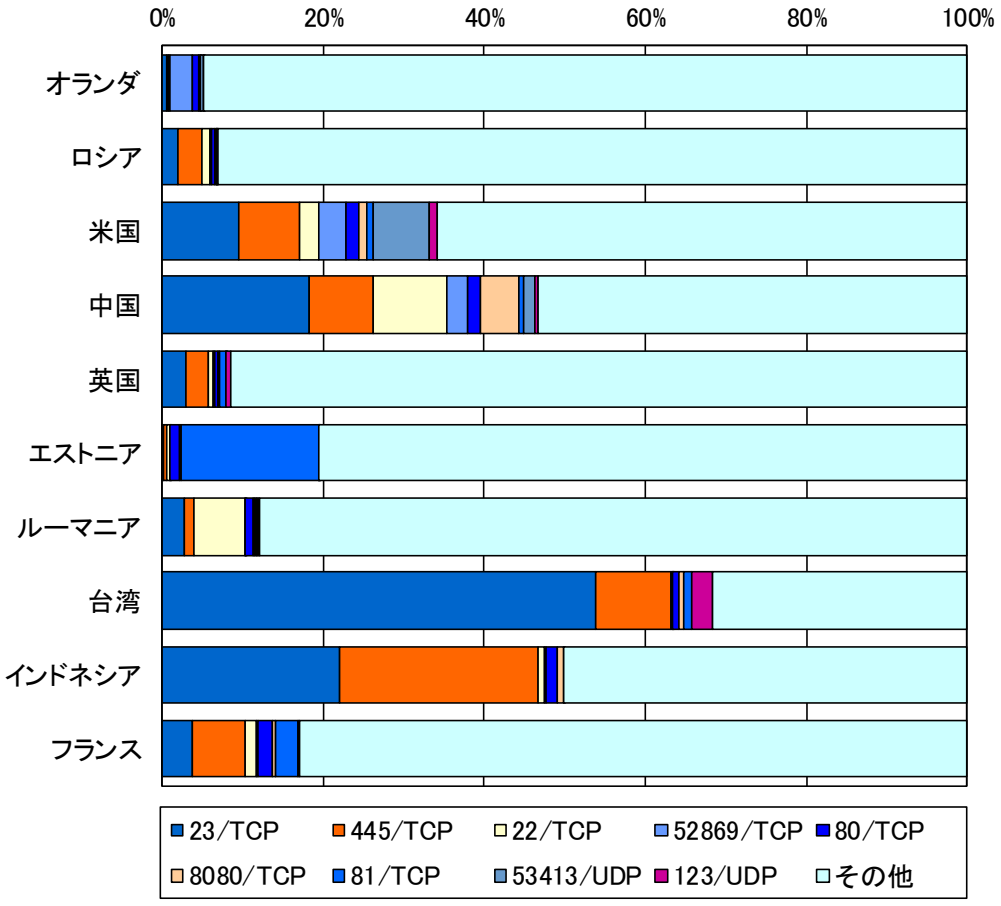

図 2-10　着信元国・地域別上位の宛先ポート別比率

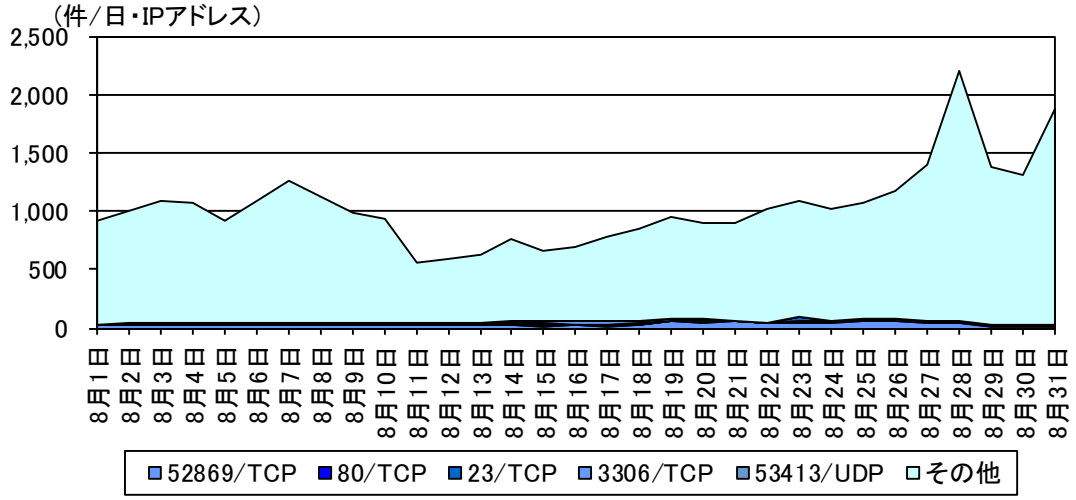

図 2-11　オランダからの検知件数の推移

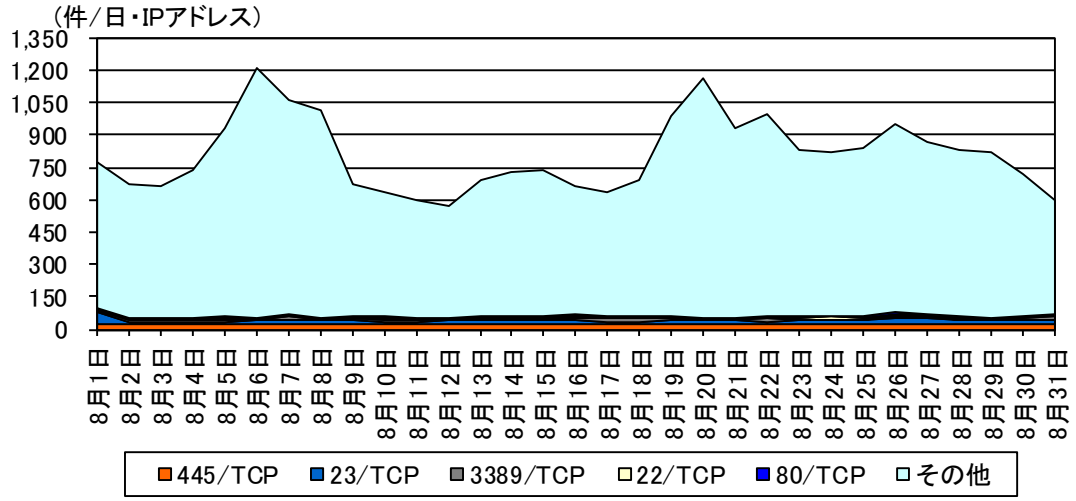

図 2-12　ロシアからの検知件数の推移

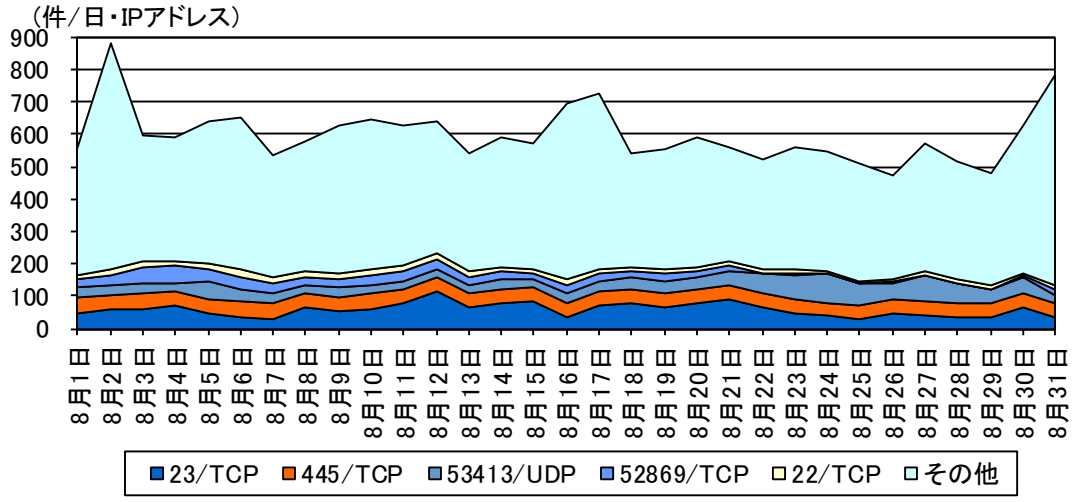

図 2-13　米国からの検知件数の推移

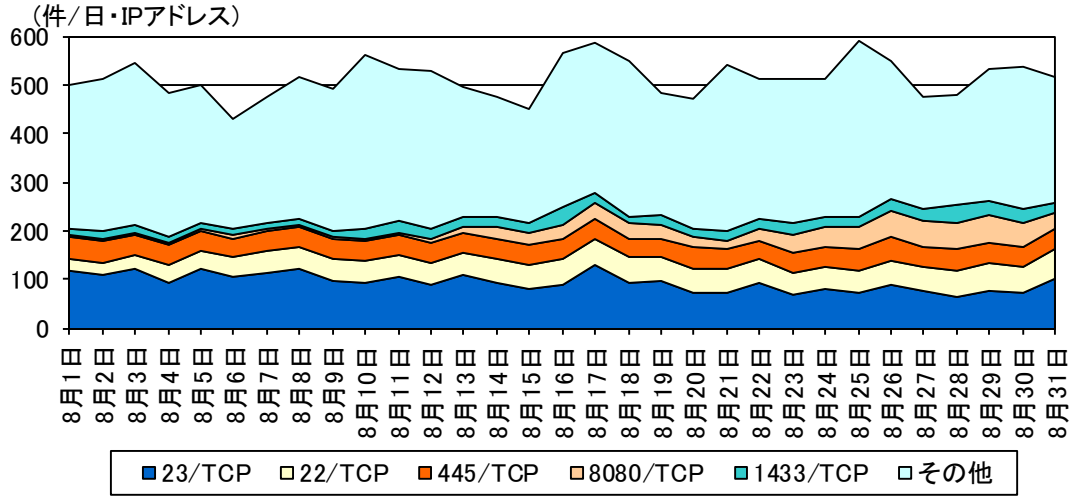

図 2-14　中国からの検知件数の推移

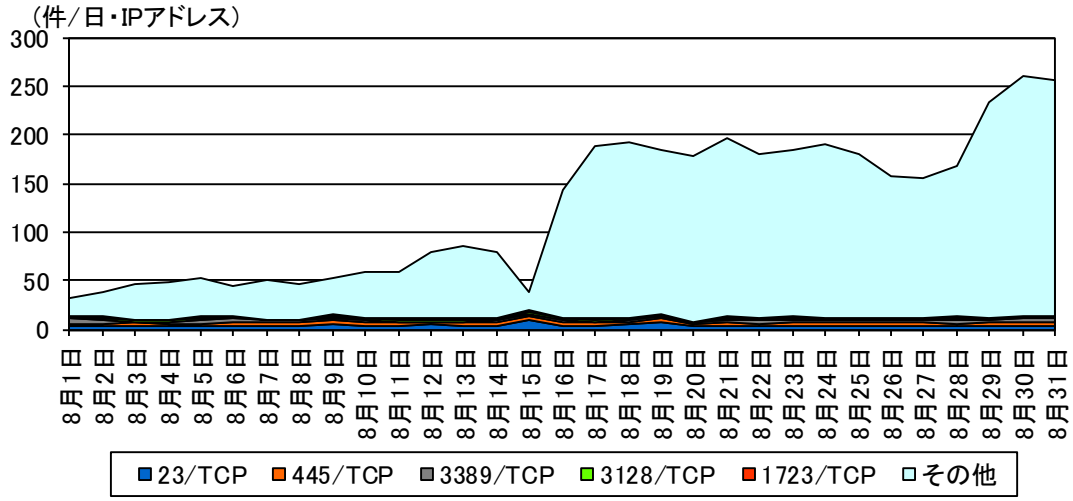

図 2-15　英国からの検知件数の推移

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	192.23 件	－18.7%　（－44.08 件）		1 位
2 位	2 位	Microsoft Windows Terminal server	159.13 件	＋0.9%　（＋1.45 件）	5 位	
3 位	3 位	SMBv1	131.62 件	－1.4%　（－1.85 件）		4 位
4 位	4 位	VOIP	33.00 件	－24.4%　（－10.67 件）		2 位
5 位	5 位	ICMP	26.94 件	＋27.6%　（＋5.82 件）	1 位	

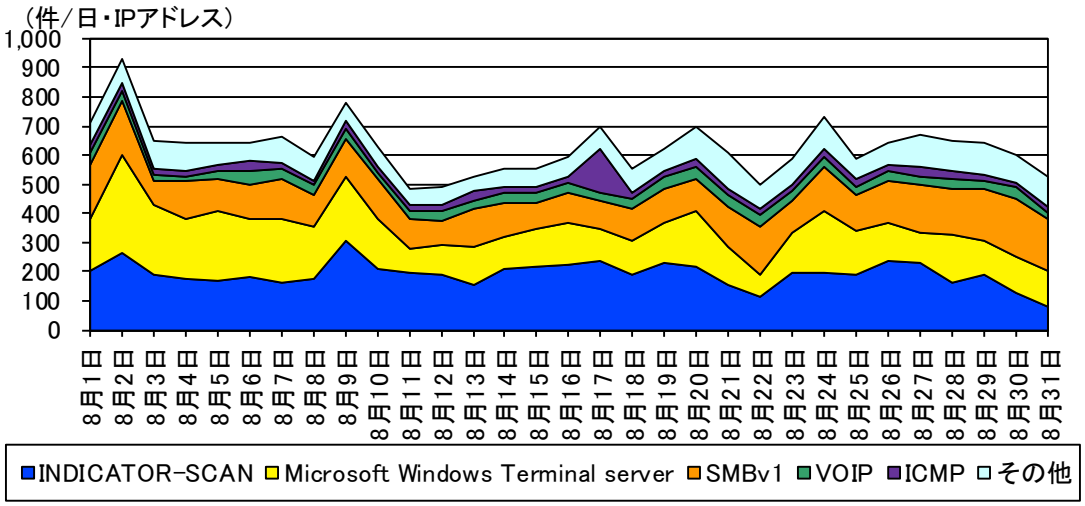

図 3-1　不正侵入等の攻撃手法別検知件数の推移

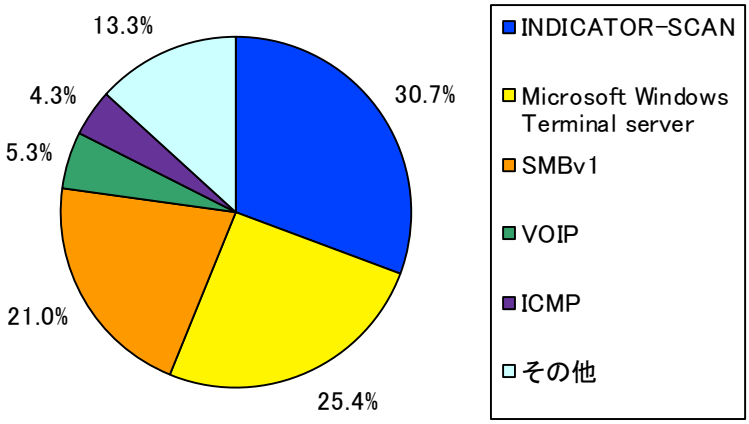

図 3-2　不正侵入等の攻撃手法別検知比率

[i] 一日・1IP アドレス当たり。

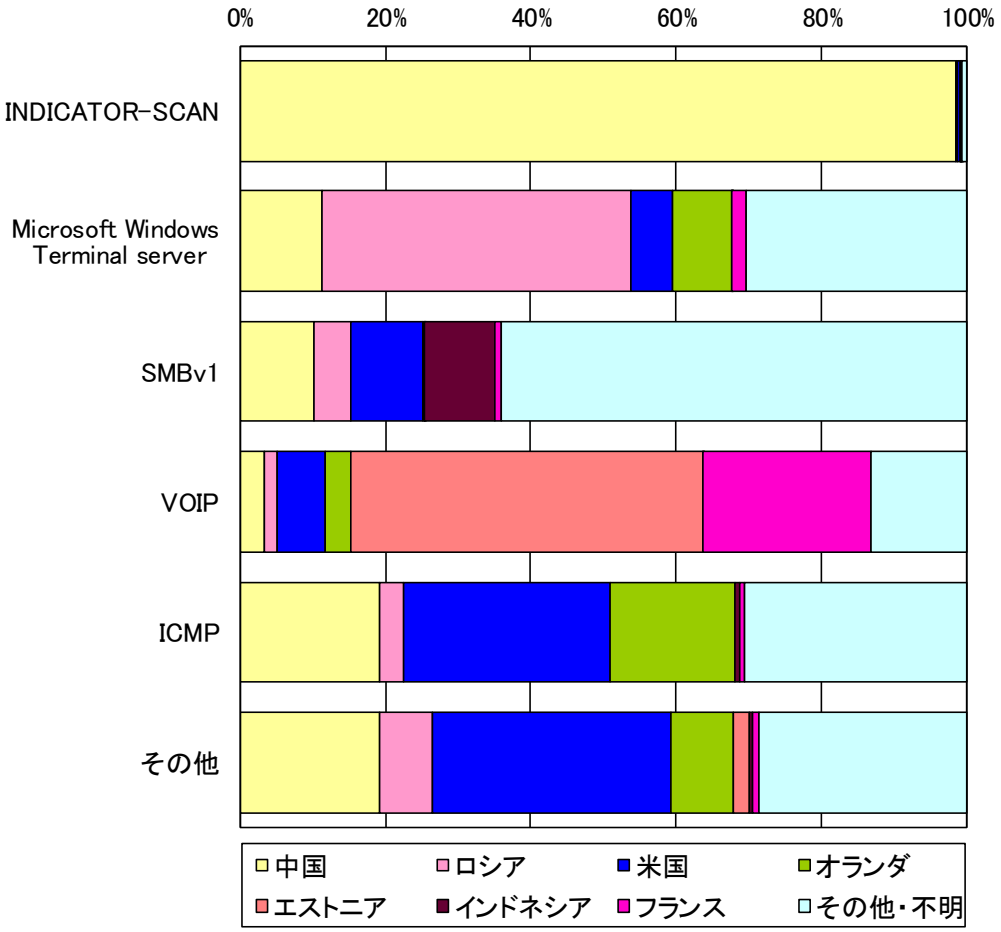

図 3-3 不正侵入等の攻撃手法の国・地域別検知比率

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	242.79 件	－16.7% （－48.59 件）
2 位	2 位	ロシア	81.99 件	＋9.4% （＋7.05 件）
3 位	3 位	米国	60.38 件	－2.6% （－1.60 件）
4 位	7 位	オランダ	26.17 件	＋91.3% （＋12.49 件）
5 位	10 位	エストニア	17.88 件	＋54.0% （＋6.27 件）

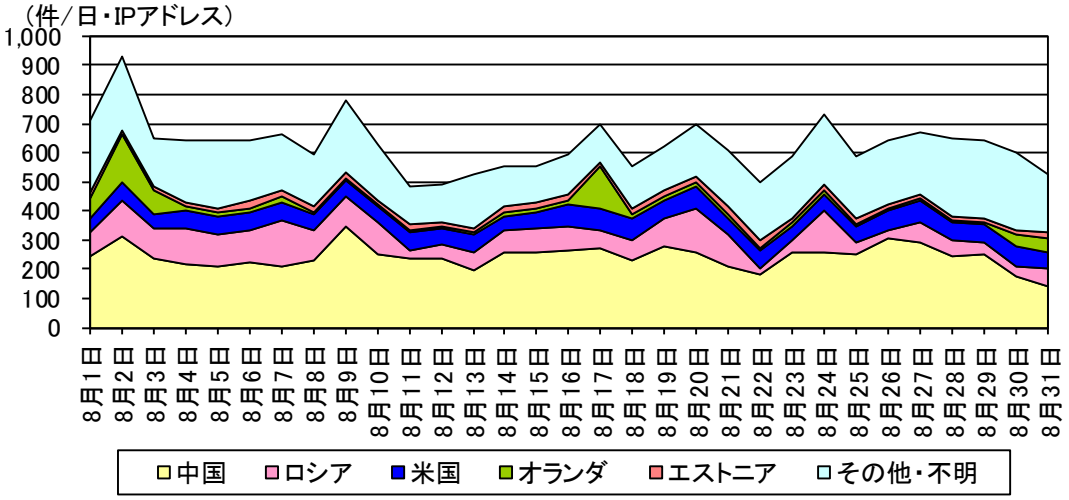

図 3-4 不正侵入等の着信元国・地域別検知件数の推移

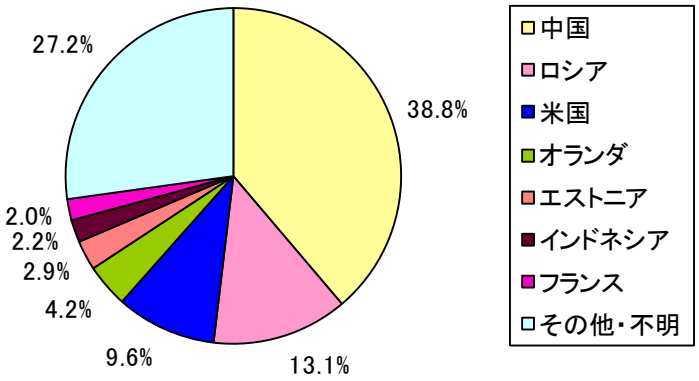

図 3-5 不正侵入等の着信元国・地域別検知比率

[i] 一日・1IP アドレス当たり。

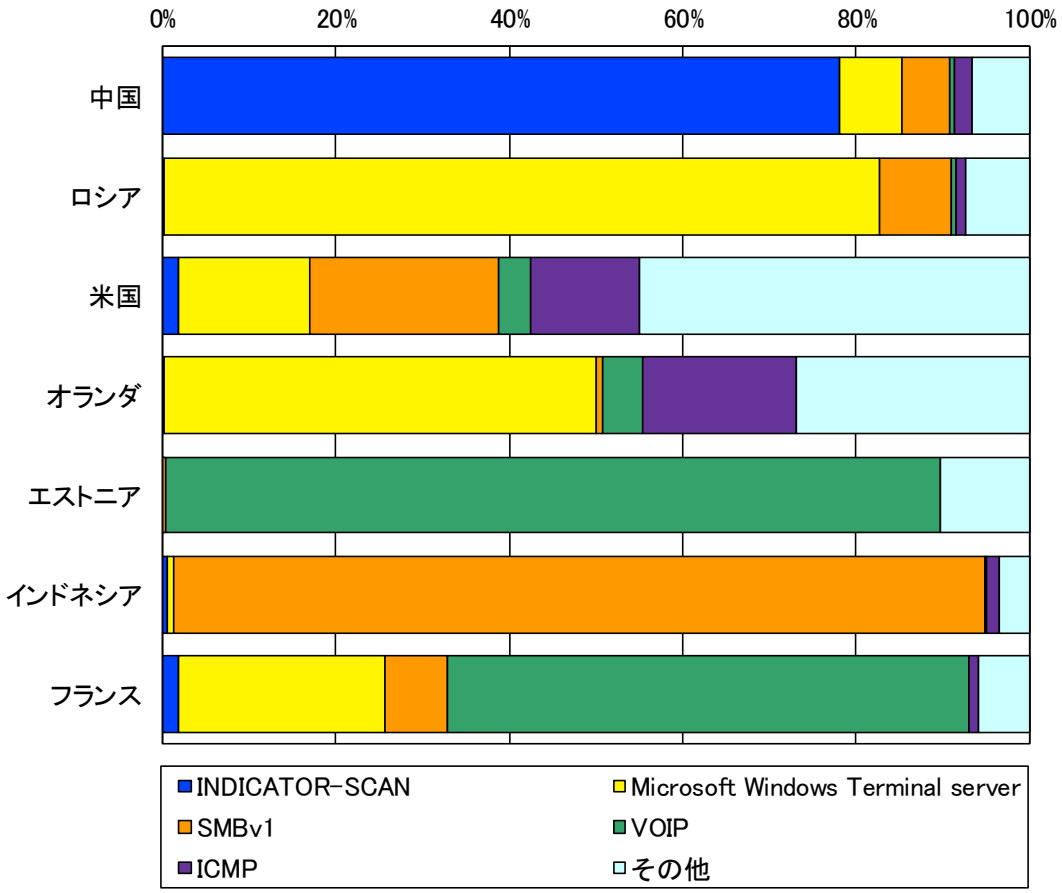

図 3-6 不正侵入等の着信元国・地域別上位の攻撃手法別検知比率

4　DoS 攻撃被害の観測結果

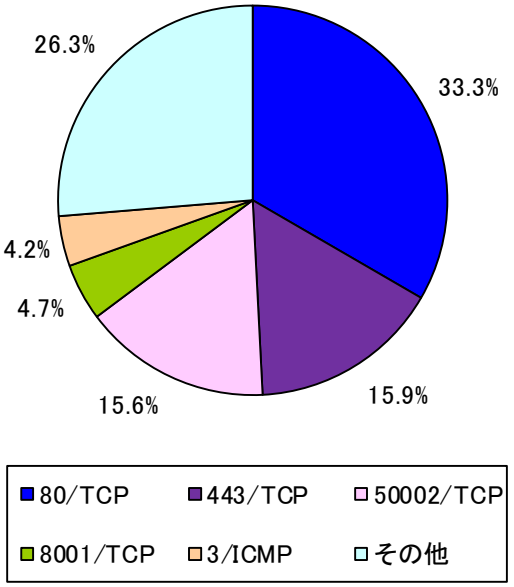

図 4-1　跳ね返りパケット着信元ポート別比率

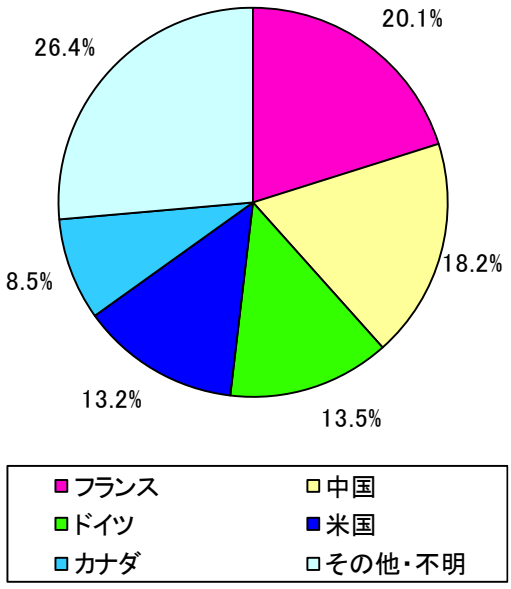

図 4-2　跳ね返りパケット着信元国・地域別比率

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