令和２年１月 30 日

令和元年 12 月期観測資料

1　観測結果概要

令和元年 12 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 5,463.5 件で、令和元年 11 月期（以下「前月期」という。）と比較して 432.7 件（8.6%）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 47,712.6 個で、前月期と比較して 5,147.4 個（9.7%）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 894.6 件で、前月期と比較して 68.9 件（8.3%）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 6937.6 個で、前月期と比較して 276.6 個（4.2%）増加しました。

DoS 攻撃被害検知件数は、一日当たり 8,946.7 件で、前月期と比較して 2,077.6 件（30.2%）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 341.1 個で、前月期と比較して 77.2 個（29.3%）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	371.08 件	－24.5%　（－120.56 件）
2 位	2 位	445/TCP	241.21 件	－6.9%　（－17.82 件）
3 位	3 位	1433/TCP	214.64 件	－6.1%　（－14.05 件）
4 位	24 位	123/UDP	178.59 件	＋942.0%　（＋161.45 件）
5 位	4 位	80/TCP	77.71 件	－26.6%　（－28.22 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	123/UDP	178.59 件	＋942.0%　（＋161.45 件）	4 位	24 位
2 位	8545/TCP	62.68 件	＋60.3%　（＋23.58 件）	6 位	12 位
3 位	34402/TCP	14.44 件	－[ii]　（＋14.39 件）	26 位	－[ii]
4 位	34403/TCP	14.40 件	－[ii]　（＋14.36 件）	29 位	－[ii]
5 位	34298/TCP	14.41 件	－[ii]　（＋14.33 件）	27 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	今月期件数[i]	前月期比[i]	今月期順位	前月期順位
1 位	23/TCP	371.08 件	－24.5%　（－120.56 件）	1 位	1 位
2 位	80/TCP	77.71 件	－26.6%　（－28.22 件）	5 位	4 位
3 位	60001/TCP	12.78 件	－68.1%　（－27.25 件）	34 位	10 位
4 位	445/TCP	241.21 件	－6.9%　（－17.82 件）	2 位	2 位
5 位	9000/TCP	16.83 件	－50.3%　（－17.05 件）	24 位	14 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。

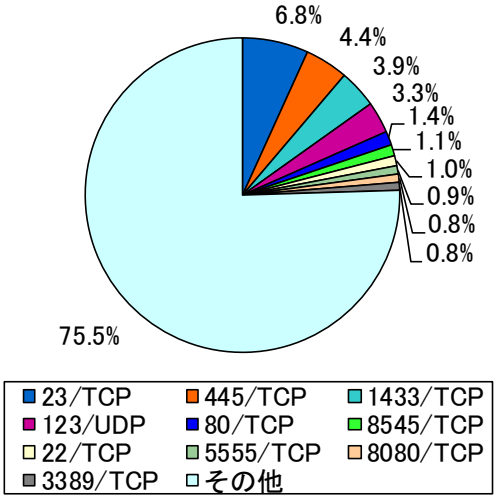

図 2-1　宛先ポート別比率（全て）[i]

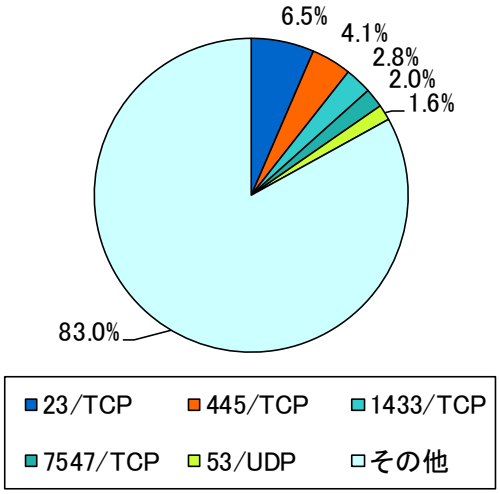

図 2-2　宛先ポート別比率（日本国内）

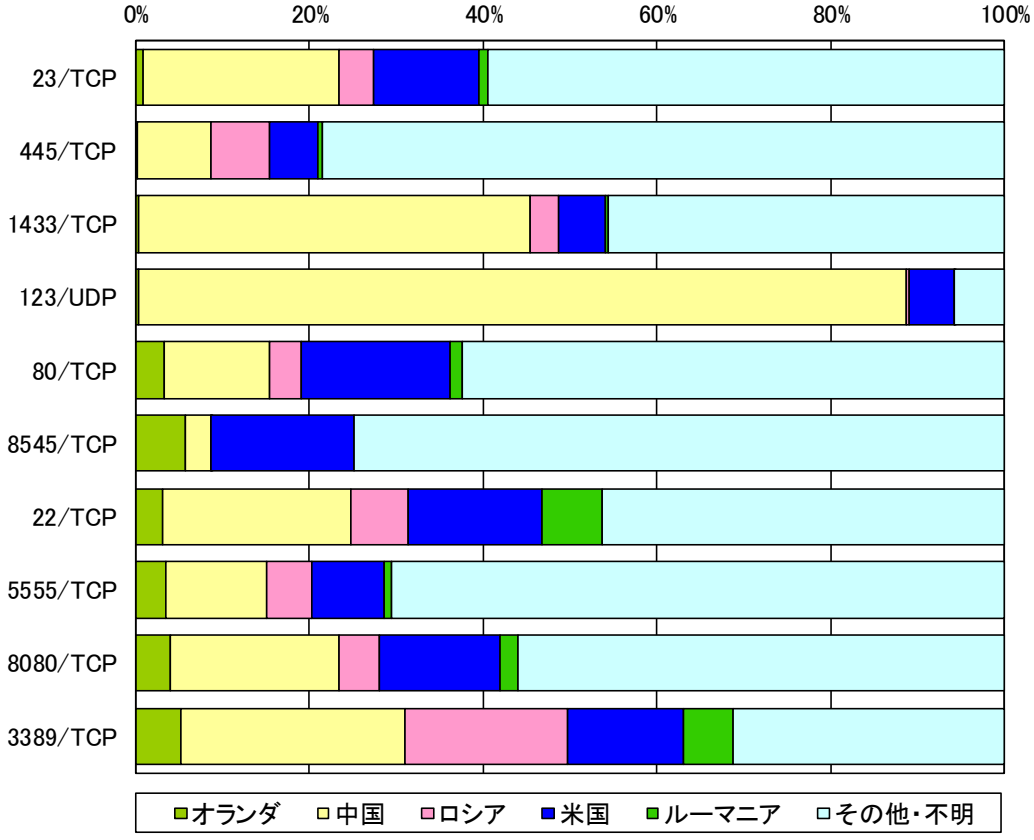

図 2-3　宛先ポート別上位の着信元国・地域別比率 [ii]

[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。

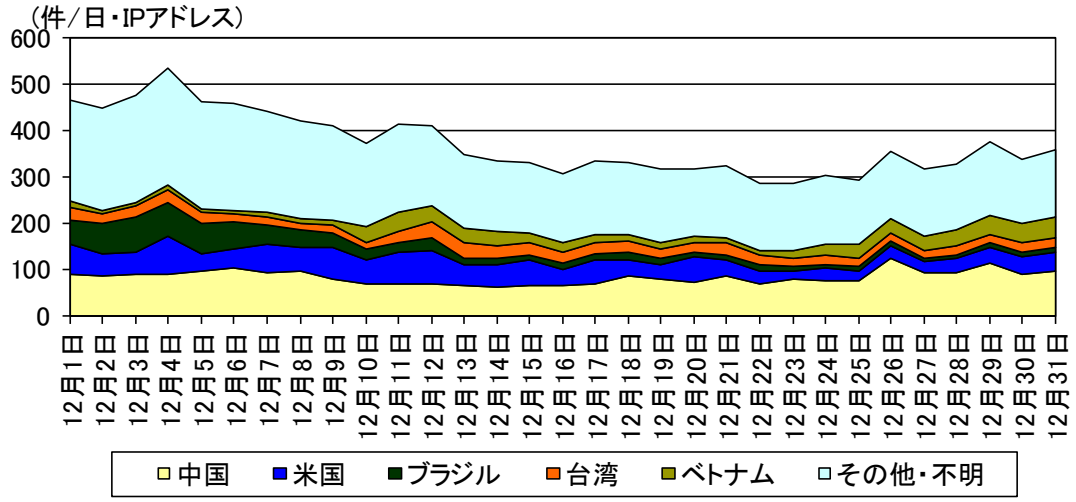

図 2-4　センサーのポート 23/TCP における検知件数の推移

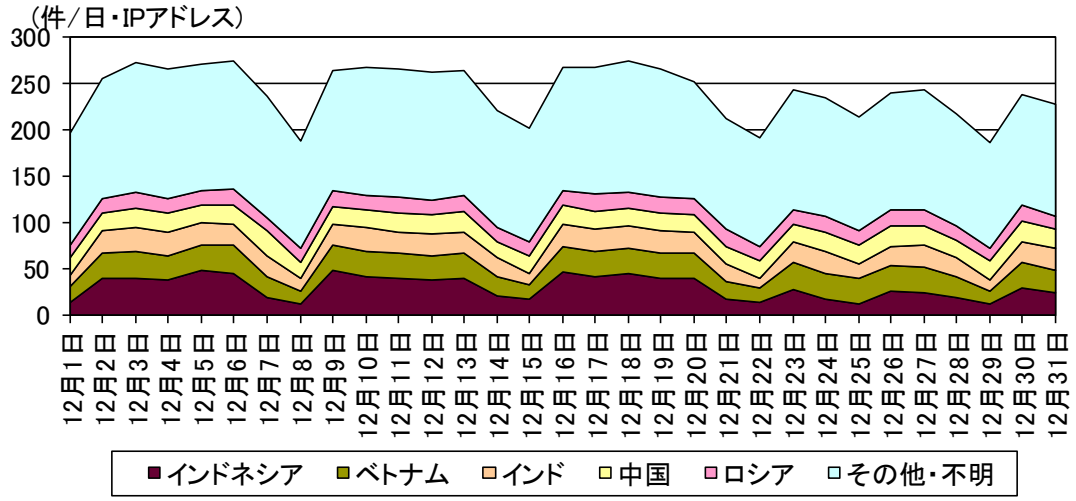

図 2-5　センサーのポート 445/TCP における検知件数の推移

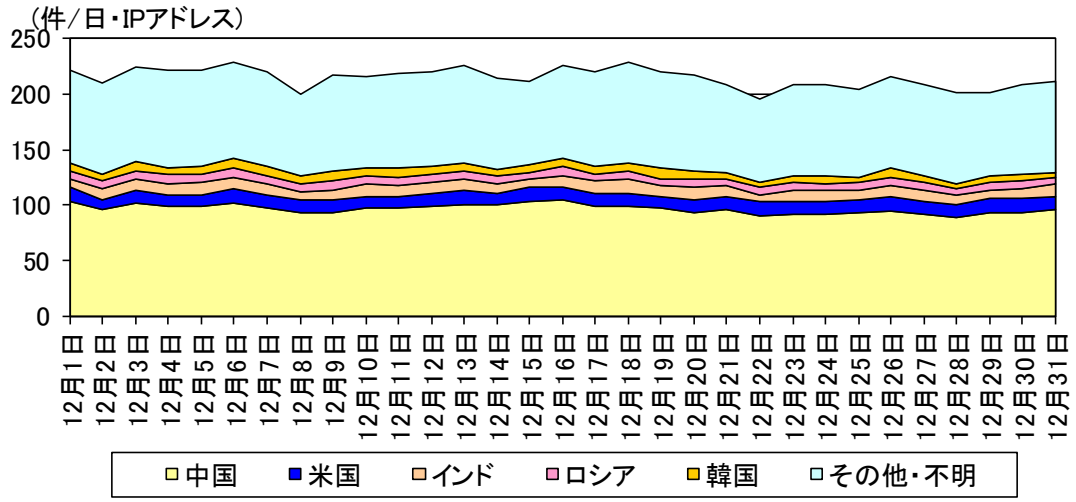

図 2-6　センサーのポート 1433/TCP における検知件数の推移

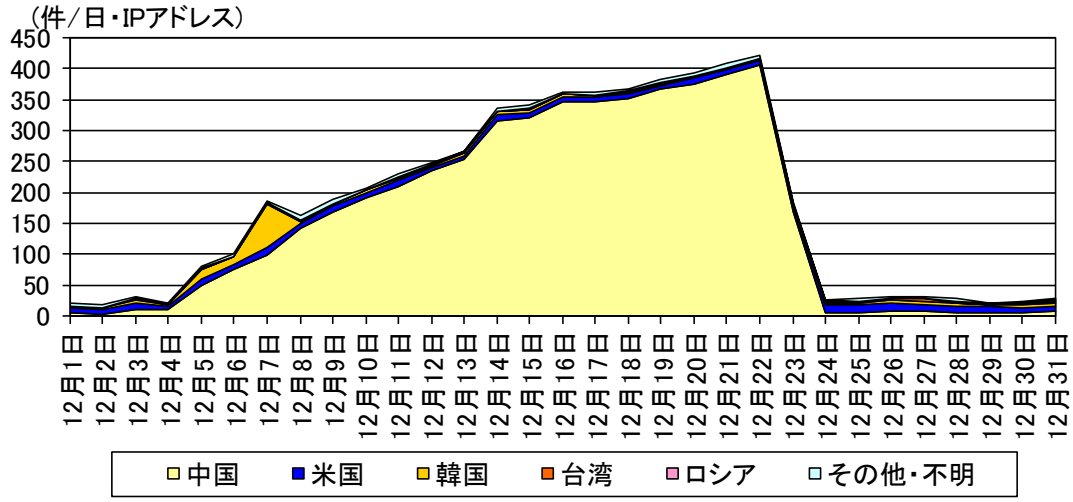

図 2-7　センサーのポート 123/UDP における検知件数の推移

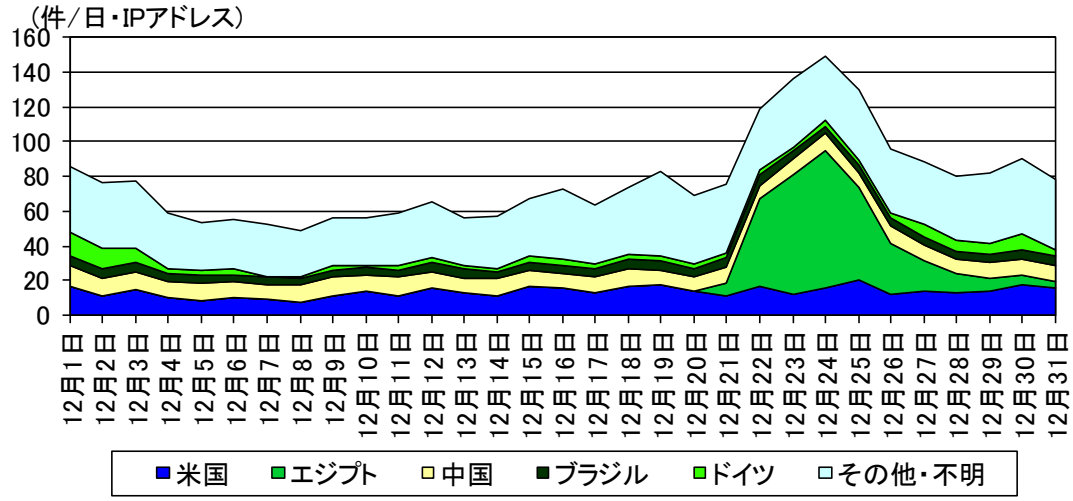

図 2-8　センサーのポート 80/TCP における検知件数の推移

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	オランダ	1,413.88 件	＋15.0%　（＋183.93 件）
2 位	3 位	中国	967.03 件	＋47.1%　（＋309.58 件）
3 位	2 位	ロシア	795.93 件	－5.2%　（－43.56 件）
4 位	4 位	米国	525.30 件	－8.6%　（－49.38 件）
5 位	6 位	ルーマニア	233.41 件	＋91.5%　（＋111.55 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	今月期件数 [i]	前月期比 [i]	今月期順位	前月期順位
1 位	中国	967.03 件	＋47.1%　（＋309.58 件）	2 位	3 位
2 位	オランダ	1,413.88 件	＋15.0%　（＋183.93 件）	1 位	1 位
3 位	ルーマニア	233.41 件	＋91.5%　（＋111.55 件）	5 位	6 位
4 位	スイス	115.18 件	＋181.6%　（＋74.28 件）	7 位	21 位
5 位	ウクライナ	102.05 件	＋145.4%　（＋60.47 件）	9 位	20 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	今月期件数 [i]	前月期比 [i]	今月期順位	前月期順位
1 位	スペイン	4.99 件	－95.9%　（－115.40 件）	45 位	7 位
2 位	米国	525.30 件	－8.6%　（－49.38 件）	4 位	4 位
3 位	ロシア	795.93 件	－5.2%　（－43.56 件）	3 位	2 位
4 位	フランス	59.34 件	－41.9%　（－42.86 件）	13 位	9 位
5 位	台湾	52.47 件	－40.0%　（－34.95 件）	16 位	11 位

[i] 一日・1IP アドレス当たり。

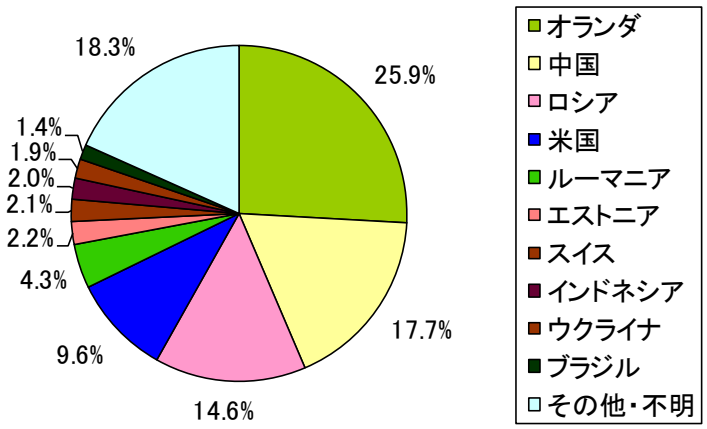

図 2-9　着信元国・地域別比率

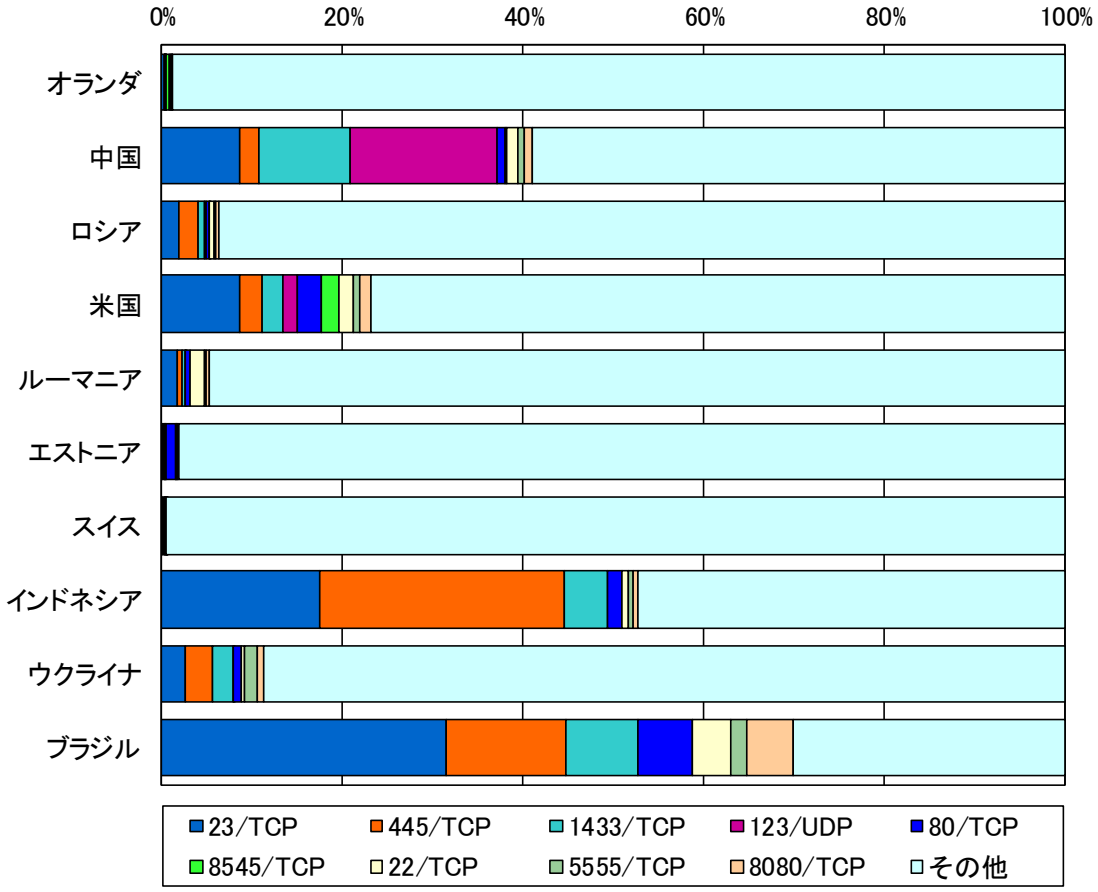

図 2-10　着信元国・地域別上位の宛先ポート別比率

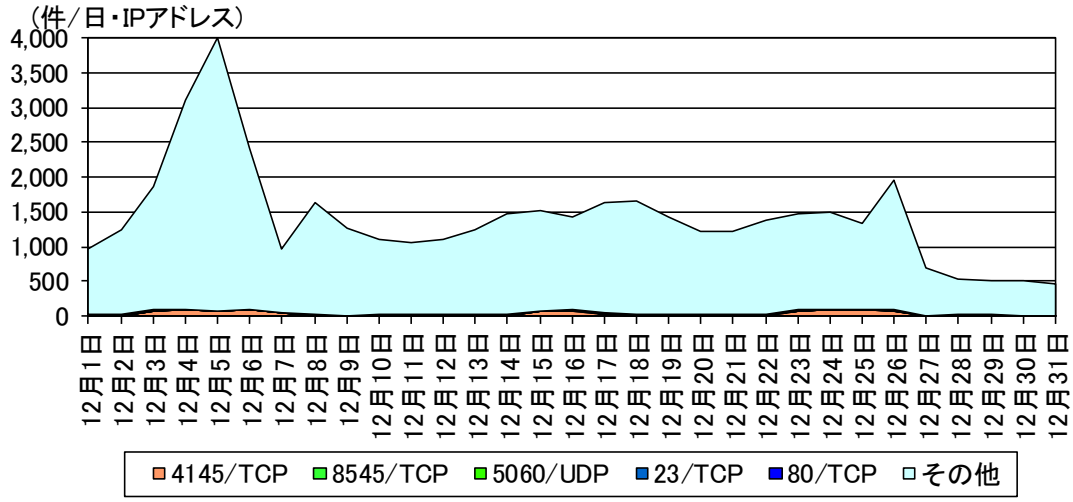

図 2-11　オランダからの検知件数の推移

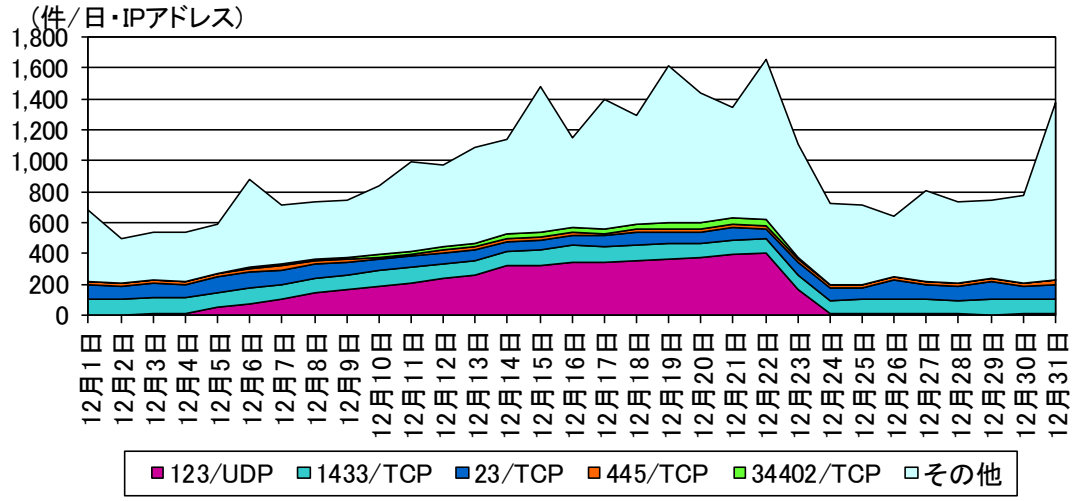

図 2-12　中国からの検知件数の推移

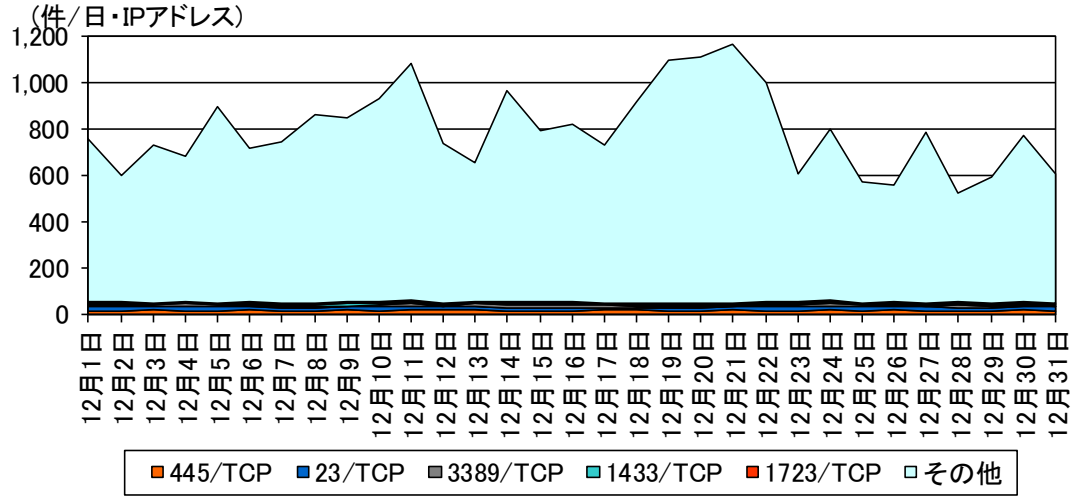

図 2-13　ロシアからの検知件数の推移

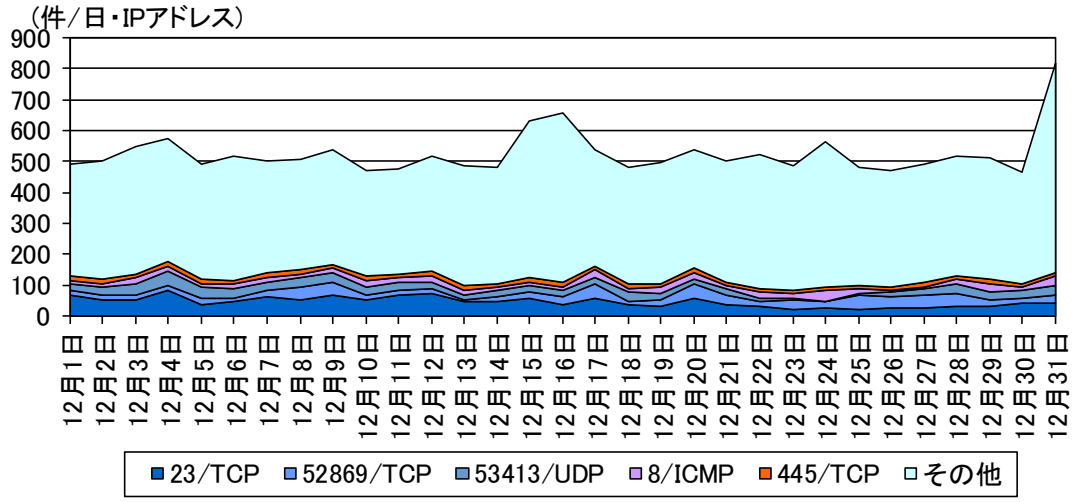

図 2-14　米国からの検知件数の推移

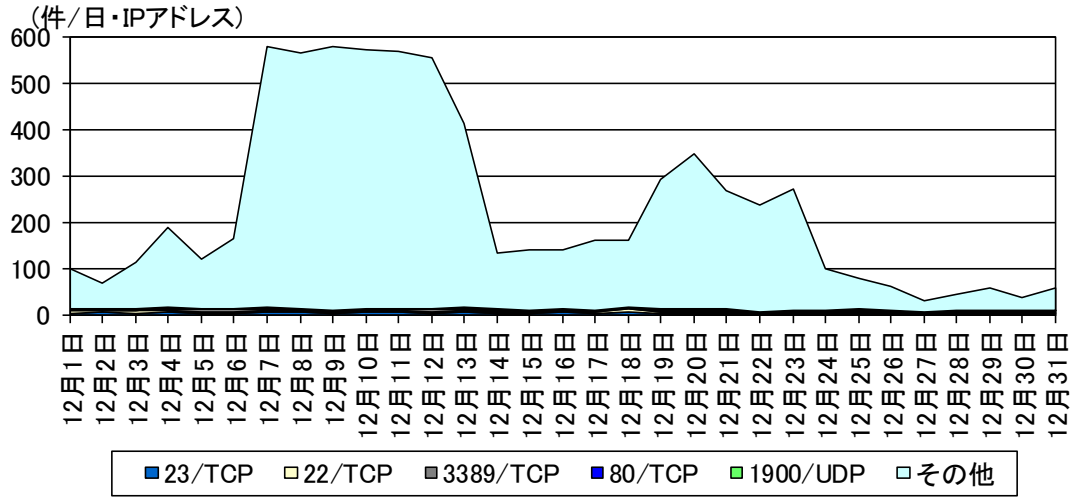

図 2-15　ルーマニアからの検知件数の推移

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	1 位	INDICATOR-SCAN	338.44 件	−5.0%　（−17.85 件）		1 位
2 位	2 位	Microsoft Windows Terminal server	289.78 件	＋22.5%　（＋53.15 件）	1 位	
3 位	3 位	SMBv1	115.18 件	＋9.2%　（＋9.71 件）	3 位	
4 位	8 位	Remote Desktop	31.21 件	＋200.2%　（＋20.82 件）	2 位	
5 位	4 位	ICMP	27.02 件	＋20.4%　（＋4.57 件）	4 位	

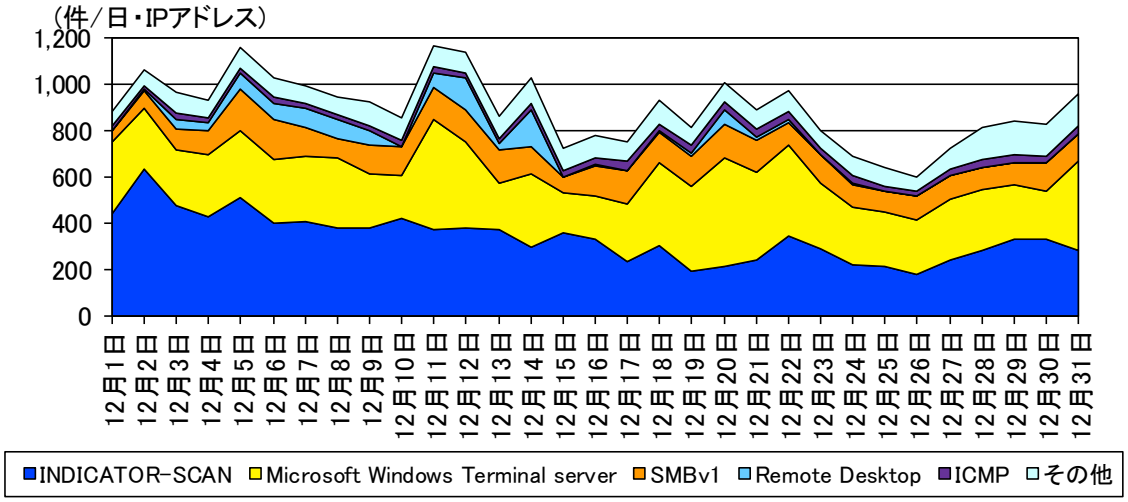

図 3-1　不正侵入等の攻撃手法別検知件数の推移

[i] 一日・1IP アドレス当たり。

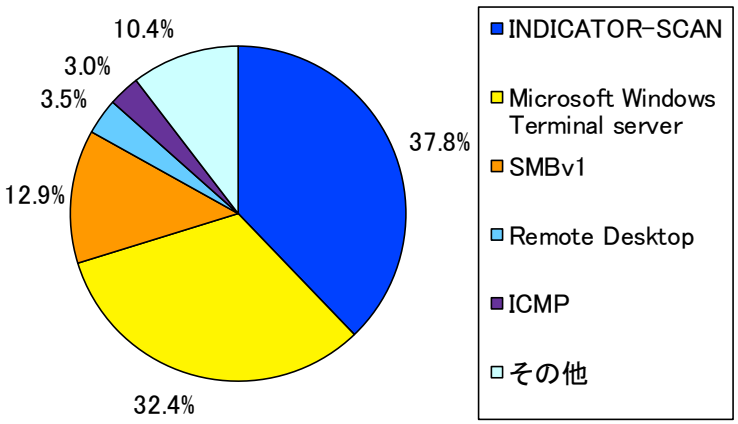

図 3-2 不正侵入等の攻撃手法別検知比率

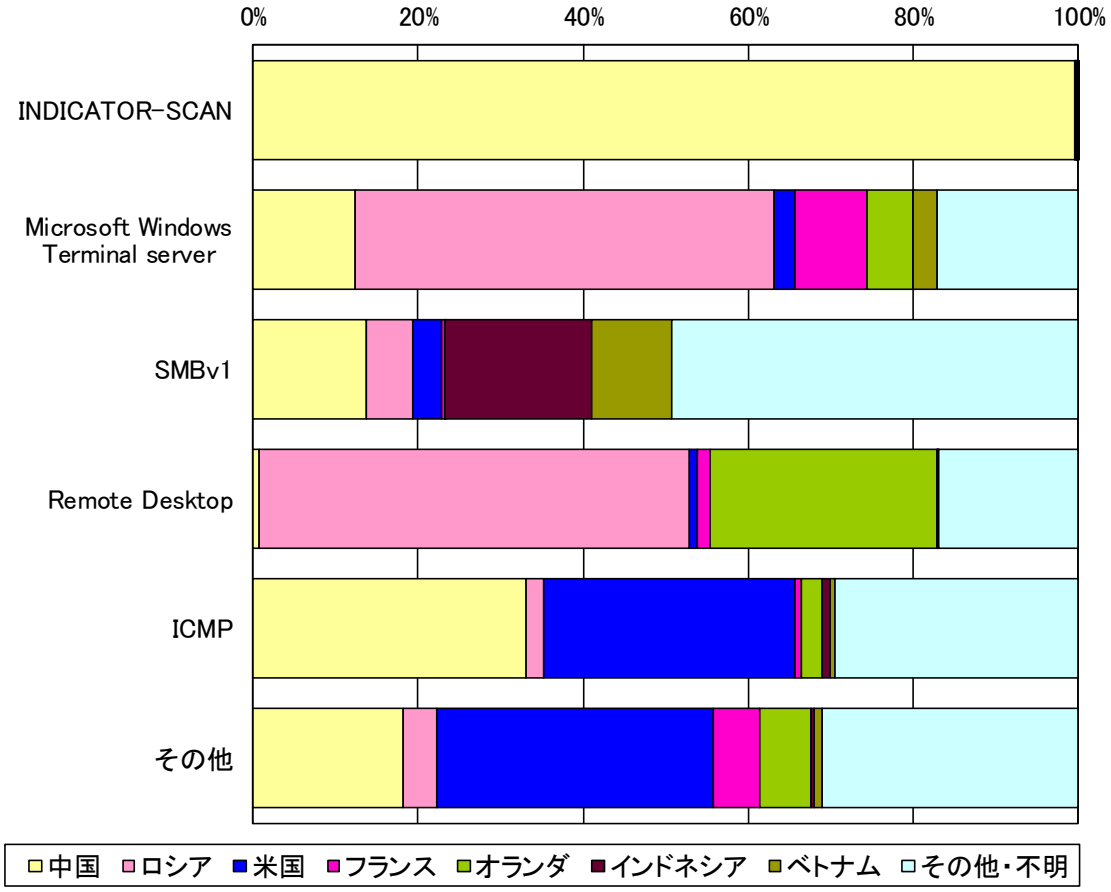

図 3-3 不正侵入等の攻撃手法の国・地域別検知比率

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	414.61 件	＋6.5% （＋25.14 件）
2 位	2 位	ロシア	173.92 件	＋55.7% （＋62.23 件）
3 位	3 位	米国	51.78 件	－13.8% （－8.31 件）
4 位	8 位	フランス	31.87 件	＋81.4% （＋14.30 件）
5 位	6 位	オランダ	31.14 件	＋54.8% （＋11.02 件）

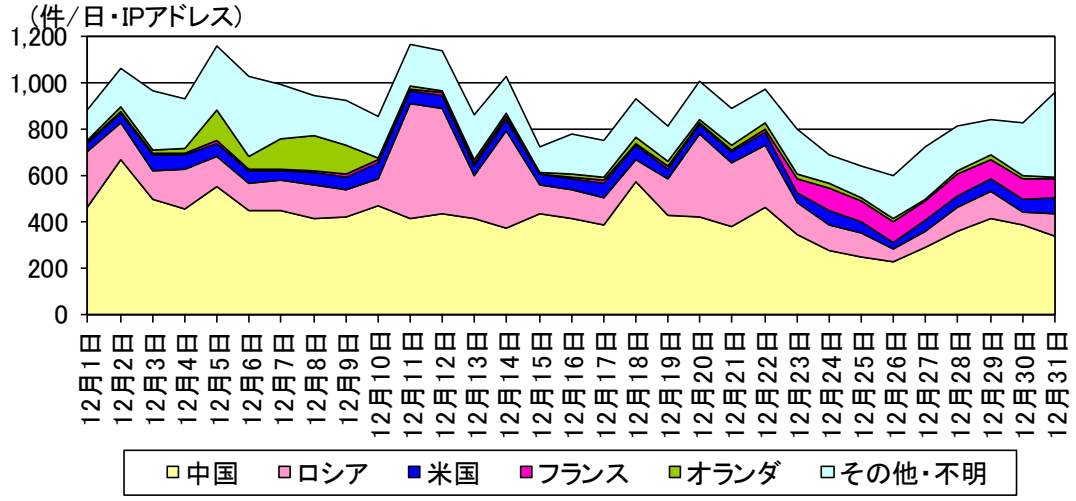

図 3-4 不正侵入等の着信元国・地域別検知件数の推移

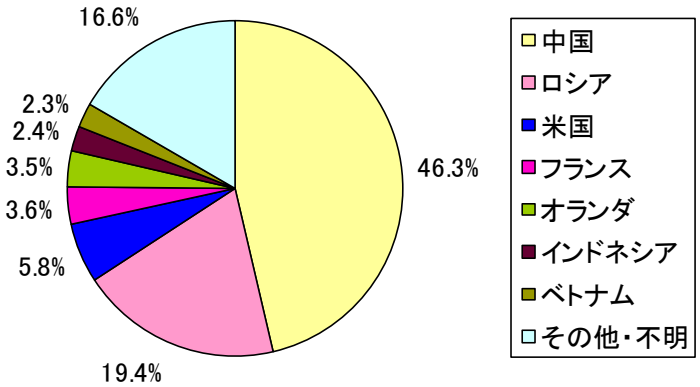

図 3-5 不正侵入等の着信元国・地域別検知比率

[i] 一日・1IP アドレス当たり。

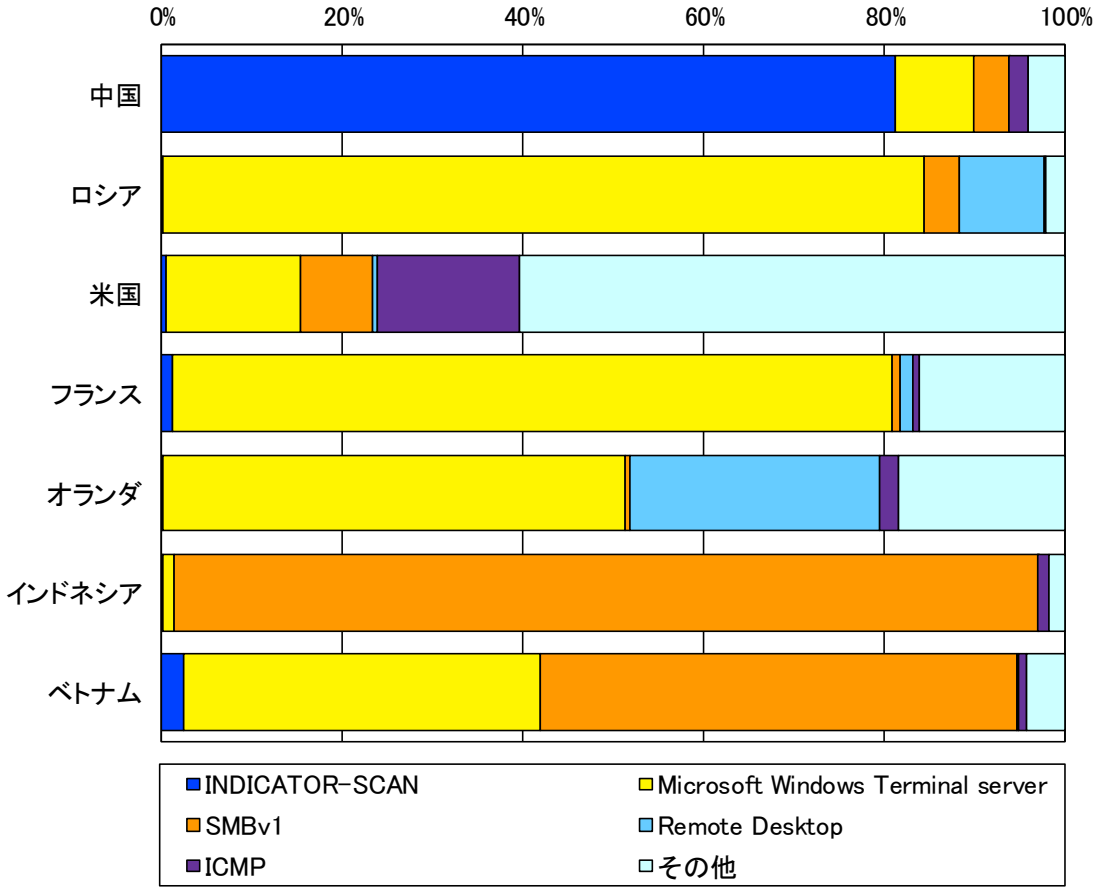

図 3-6 不正侵入等の着信元国・地域別上位の攻撃手法別検知比率

4　DoS 攻撃被害の観測結果

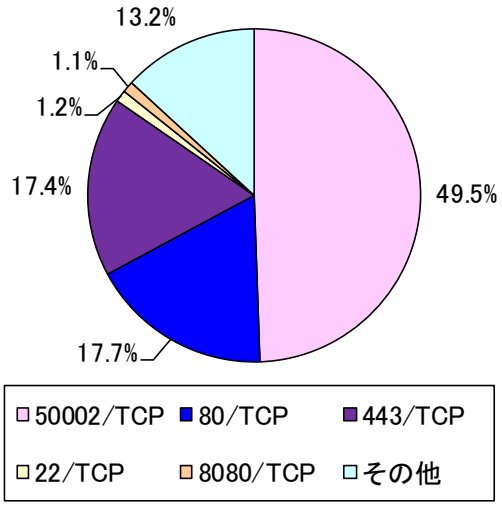

図 4-1　跳ね返りパケット着信元ポート別比率

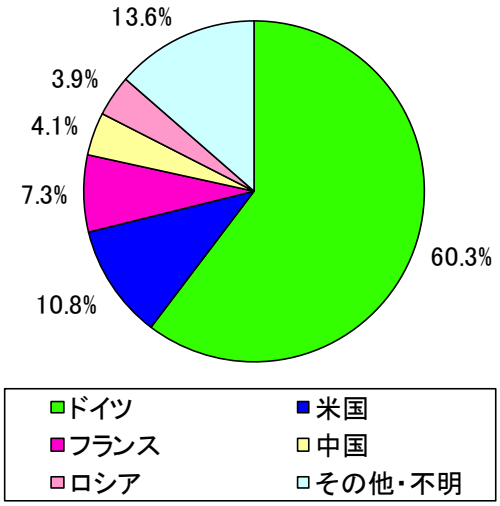

図 4-2　跳ね返りパケット着信元国・地域別比率

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