平成 31年3月 28 日

平成 31年1月期観測資料

1　観測結果概要

平成 31 年1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 3,544.5 件で、平成 30 年 12 月期（以下「前期」という。）と比較して 450.1 件（11.3 %）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 49,572.8 個で、前期と比較して 1,026.9 個（2.0 %）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 970.6 件でした。また、着信元（送信元）IP アドレス数は、一日当たり 7,918.3 個でした。

DoS 攻撃被害検知件数は、一日当たり 11,902.5 件で、前期と比較して 960.2 件（8.8 %）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 316.5 個で、前期と比較して 0.97 個（0.3 %）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	372.45 件	－5.4%　（－21.47 件）
2 位	2 位	445/TCP	307.00 件	－9.5%　（－32.33 件）
3 位	3 位	1433/TCP	203.41 件	＋31.5%　（＋48.68 件）
4 位	5 位	52869/TCP	161.81 件	＋88.0%　（＋75.72 件）
5 位	7 位	22/TCP	83.69 件	＋9.8%　（＋7.45 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	52869/TCP	161.81 件	＋88.0%　（＋75.72 件）	4 位	5 位
2 位	1433/TCP	203.41 件	＋31.5%　（＋48.68 件）	3 位	3 位
3 位	5038/TCP	12.25 件	＋156.0%　（＋7.47 件）	23 位	38 位
4 位	22/TCP	83.69 件	＋9.8%　（＋7.45 件）	5 位	7 位
5 位	123/UDP	14.87 件	＋49.2%　（＋4.90 件）	20 位	24 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	445/TCP	307.00 件	－9.5%　（－32.33 件）	2 位	2 位
2 位	81/TCP	42.34 件	－39.3%　（－27.44 件）	8 位	8 位
3 位	8545/TCP	68.95 件	－28.4%　（－27.28 件）	6 位	4 位
4 位	23/TCP	372.45 件	－5.4%　（－21.47 件）	1 位	1 位
5 位	80/TCP	68.80 件	－18.0%　（－15.09 件）	7 位	6 位

[i] 一日・1IP アドレス当たり。

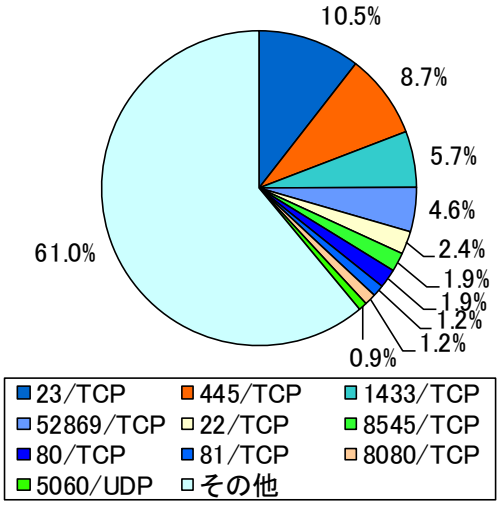

図 2-1　宛先ポート別比率（全て）[i]

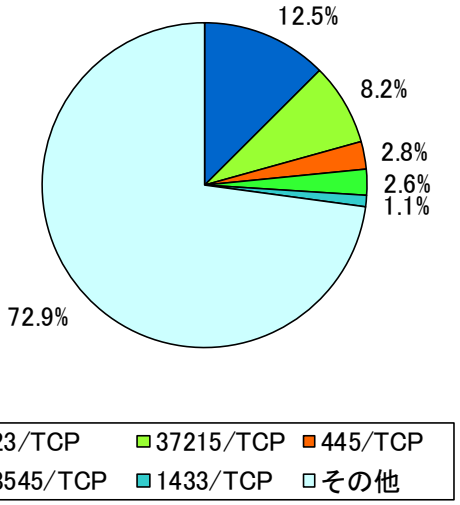

図 2-2　宛先ポート別比率（日本国内）[i]

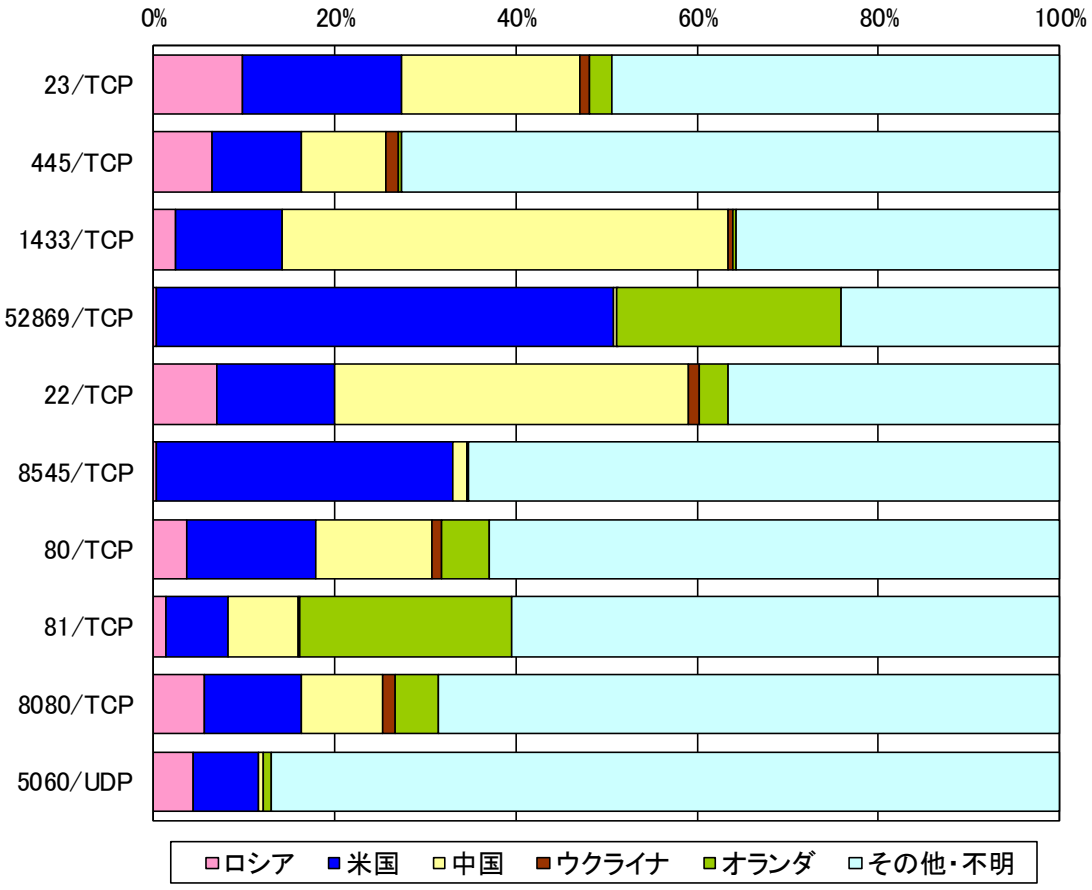

図 2-3　宛先ポート別上位の着信元国・地域別比率 [ii]

[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。

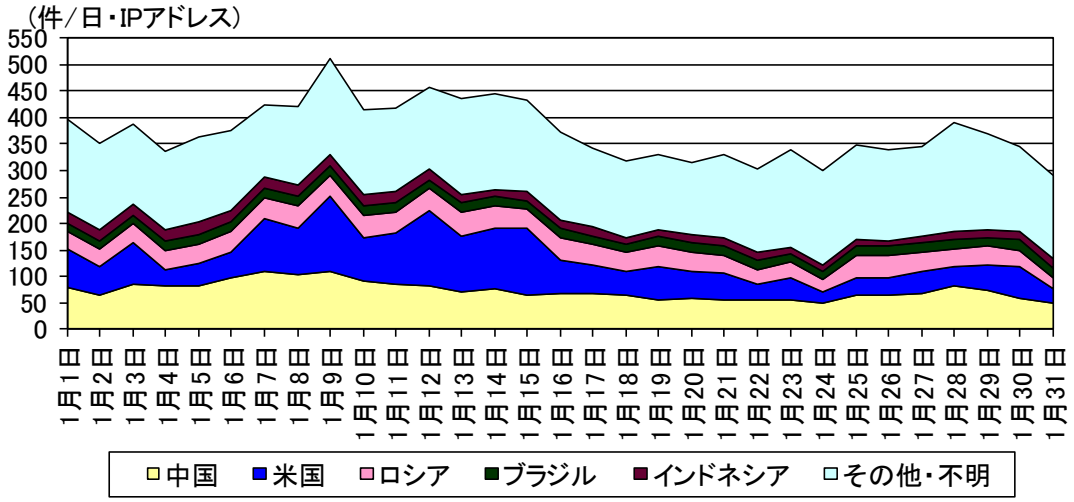

図 2-4　センサーのポート 23/TCP における検知件数の推移

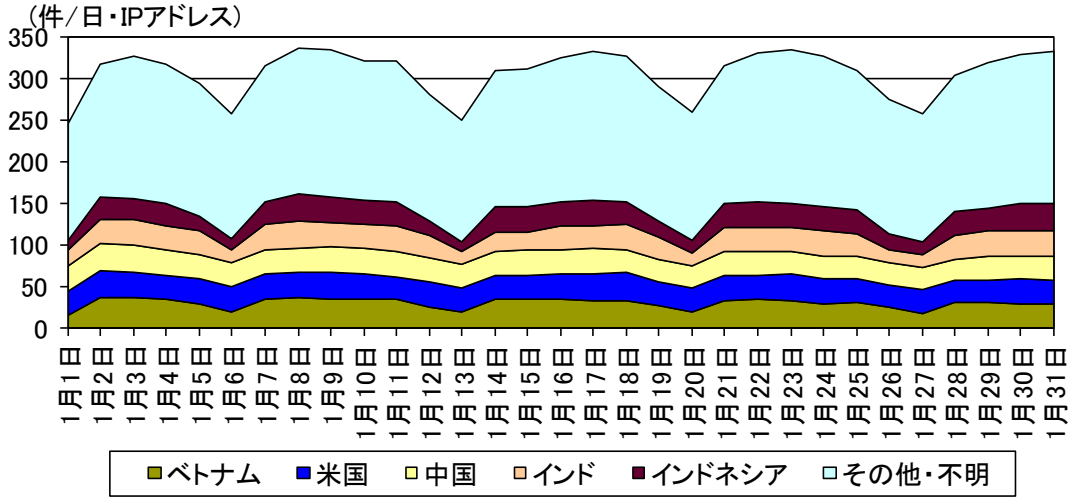

図 2-5　センサーのポート 445/TCP における検知件数の推移

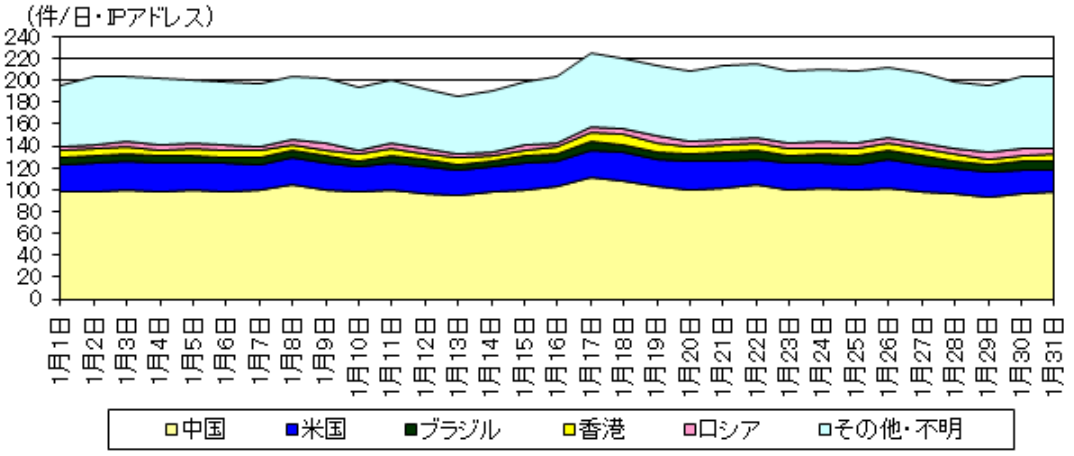

図 2-6　センサーのポート 1433/TCP における検知件数の推移

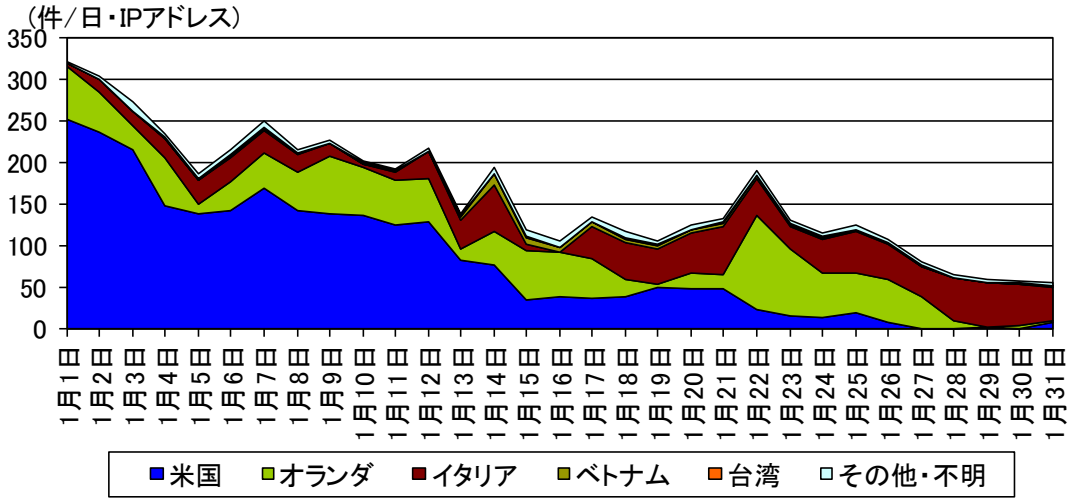

図 2-7　センサーのポート 52869/TCP における検知件数の推移

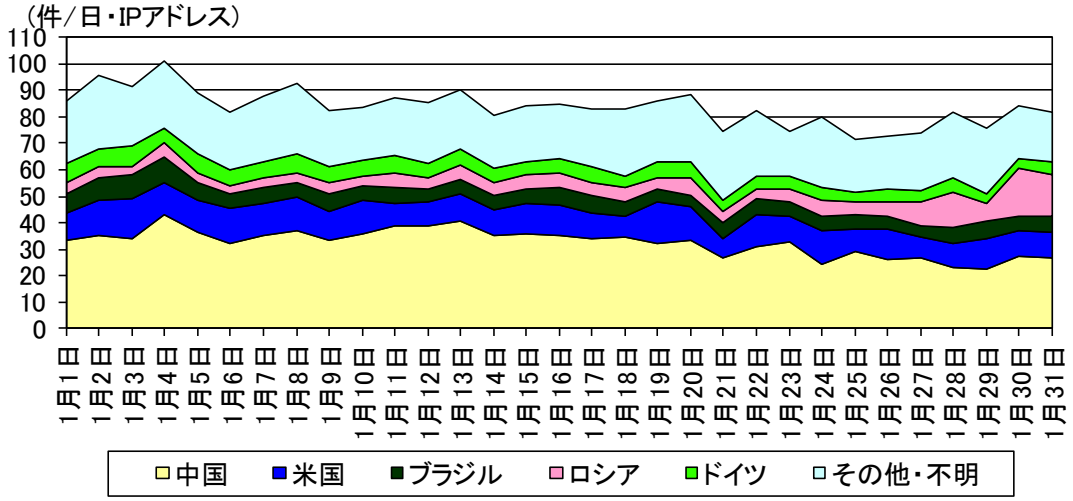

図 2-8　センサーのポート 22/TCP における検知件数の推移

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	ロシア	718.00 件	－3.1%　（－22.91 件）
2 位	3 位	米国	585.30 件	＋17.5%　（＋87.02 件）
3 位	2 位	中国	446.23 件	－13.7%　（－70.81 件）
4 位	4 位	ウクライナ	246.44 件	－49.7%　（－243.81 件）
5 位	6 位	オランダ	158.48 件	－0.5%　（－0.86 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	米国	585.30 件	＋17.5%　（＋87.02 件）	2 位	3 位
2 位	パナマ	36.33 件	＋883.4%　（＋32.63 件）	22 位	51 位
3 位	ブルガリア	86.87 件	＋36.0%　（＋22.98 件）	7 位	13 位
4 位	ルーマニア	38.34 件	＋81.7%　（＋17.24 件）	21 位	22 位
5 位	イタリア	72.45 件	＋19.7%　（＋11.94 件）	10 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	ウクライナ	246.44 件	－49.7%　（－243.81 件）	4 位	4 位
2 位	フランス	40.64 件	－79.3%　（－155.36 件）	19 位	5 位
3 位	中国	446.23 件	－13.7%　（－70.81 件）	3 位	2 位
4 位	英国	58.85 件	－43.3%　（－44.98 件）	13 位	8 位
5 位	リトアニア	119.51 件	－21.0%　（－31.73 件）	6 位	7 位

[i] 一日・1IP アドレス当たり。

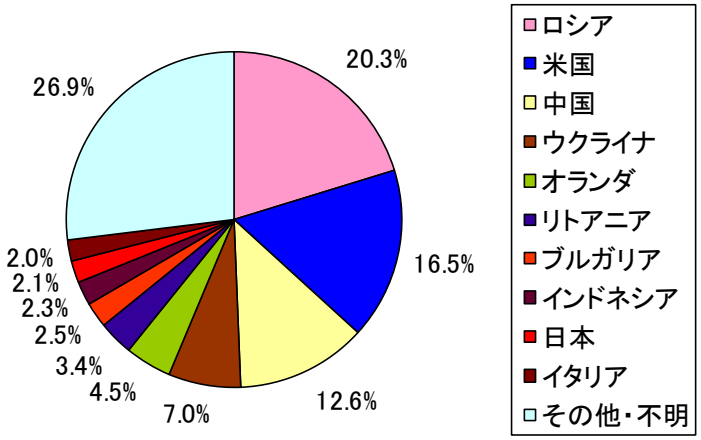

図 2-9　着信元国・地域別比率

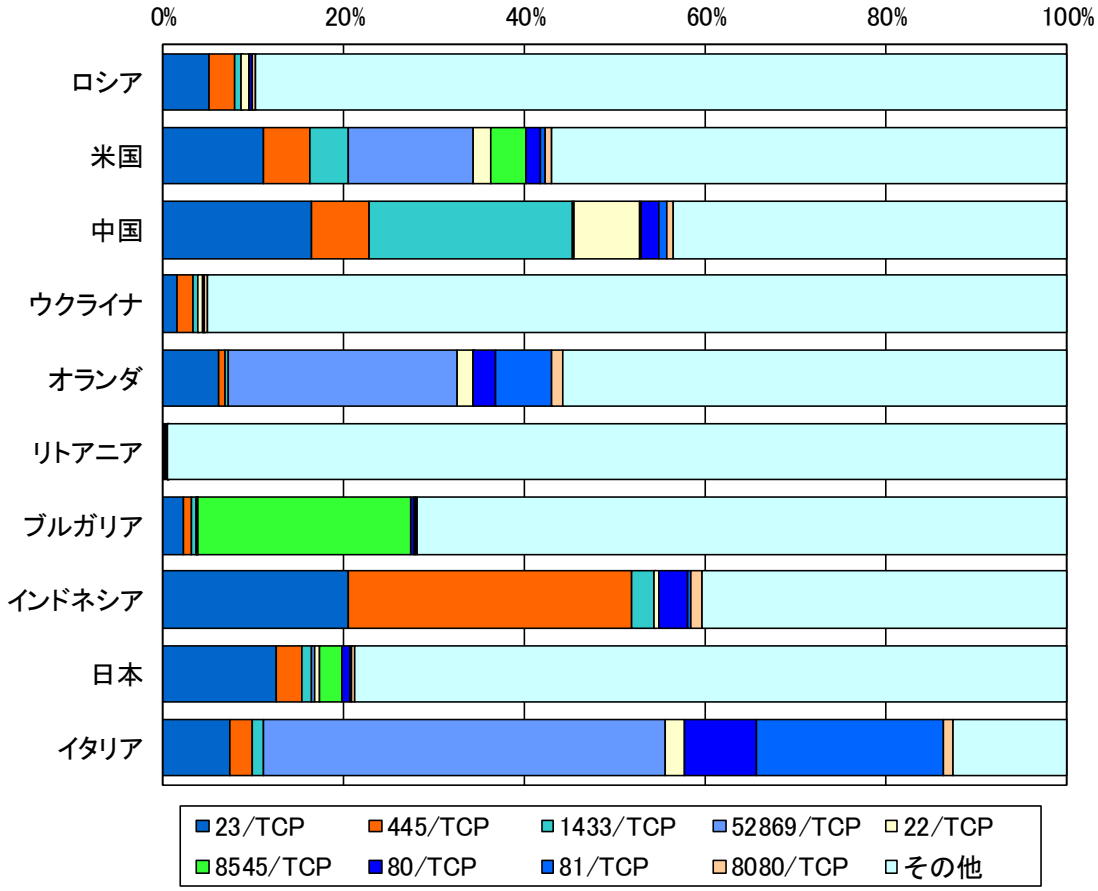

図 2-10　着信元国・地域別上位の宛先ポート別比率

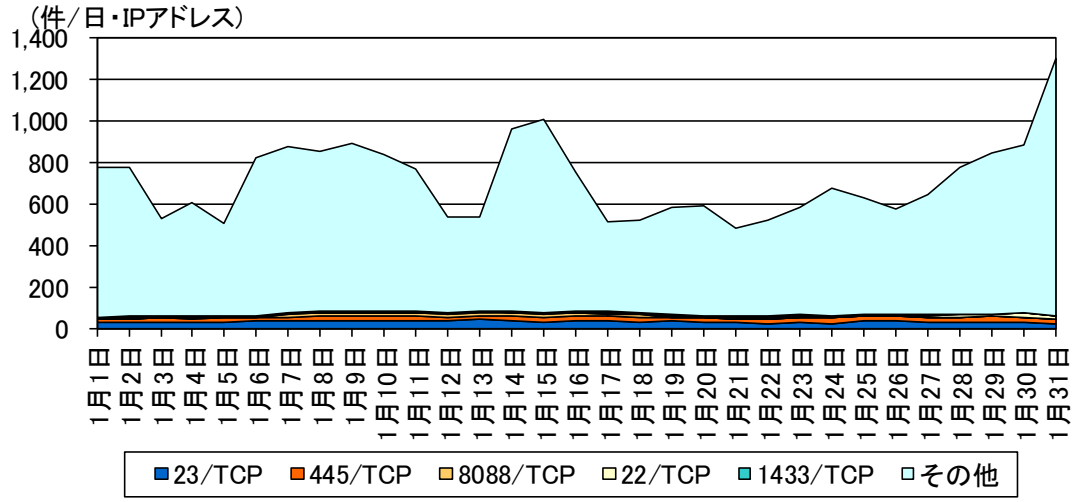

図 2-11　ロシアからの検知件数の推移

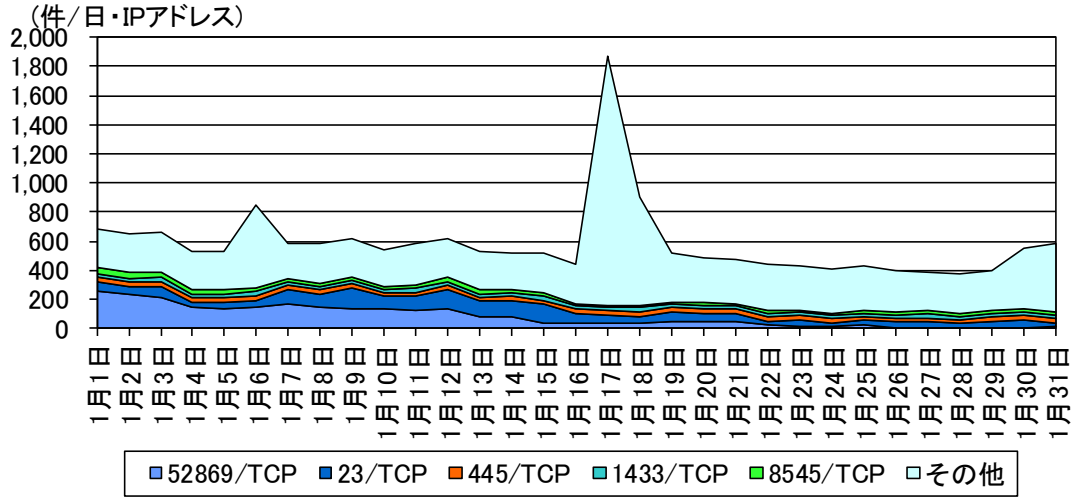

図 2-12　米国からの検知件数の推移

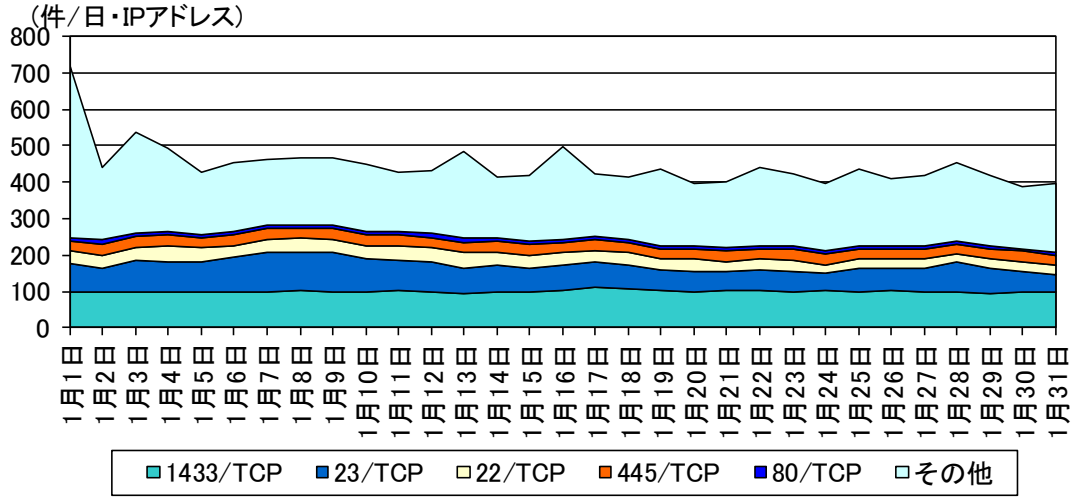

図 2-13　中国からの検知件数の推移

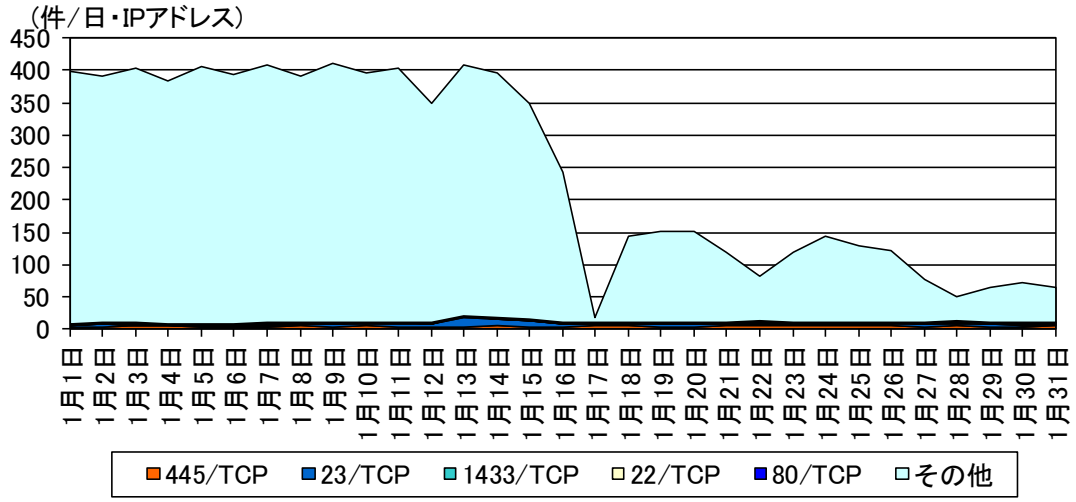

図 2-14　ウクライナからの検知件数の推移

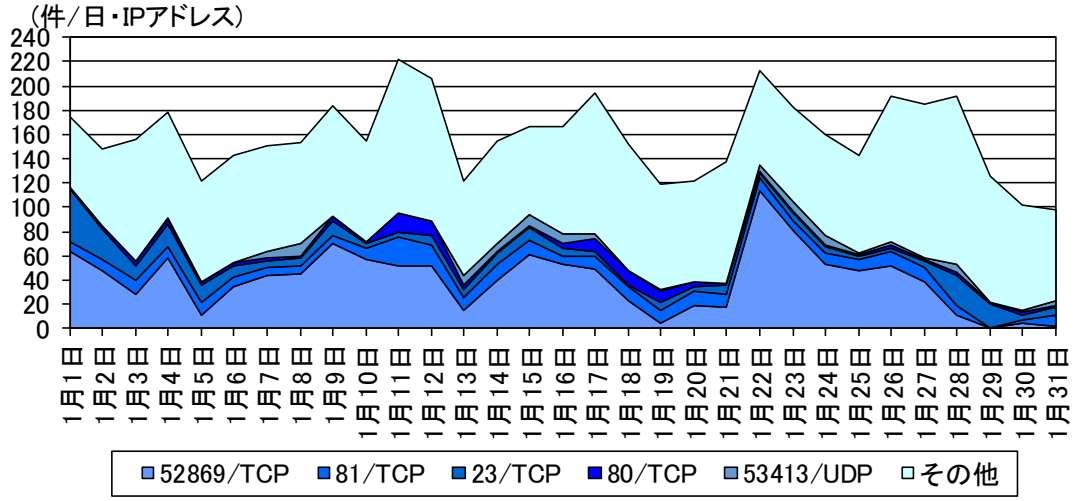

図 2-15　オランダからの検知件数の推移

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	－[ii]	INDICATOR-SCAN	370.44 件	－[ii]	－[ii]	－[ii]
2 位	－[ii]	Microsoft Windows Terminal server	298.34 件	－[ii]	－[ii]	－[ii]
3 位	－[ii]	SMBv1	113.68 件	－[ii]	－[ii]	－[ii]
4 位	－[ii]	Remote Desktop	56.15 件	－[ii]	－[ii]	－[ii]
5 位	－[ii]	ICMP	29.75 件	－[ii]	－[ii]	－[ii]

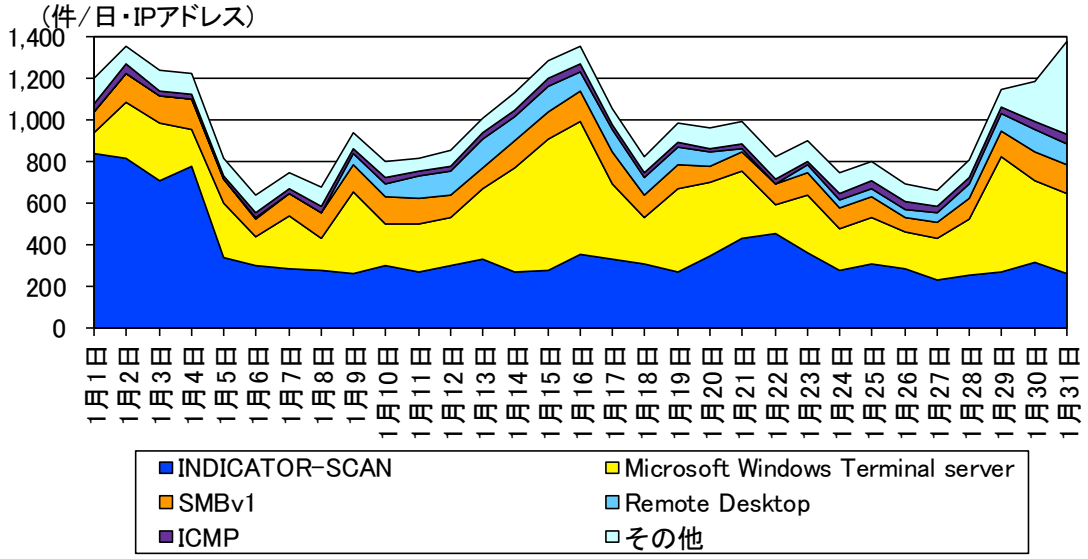

図 3-1　不正侵入等の攻撃手法別検知件数の推移

[i] 一日・1IP アドレス当たり。

[ii] 平成 31 年 1 月 1 日以降の不正侵入等の攻撃手法の検知については、攻撃手法の分類見直しを実施したため、前期との比較はありません。

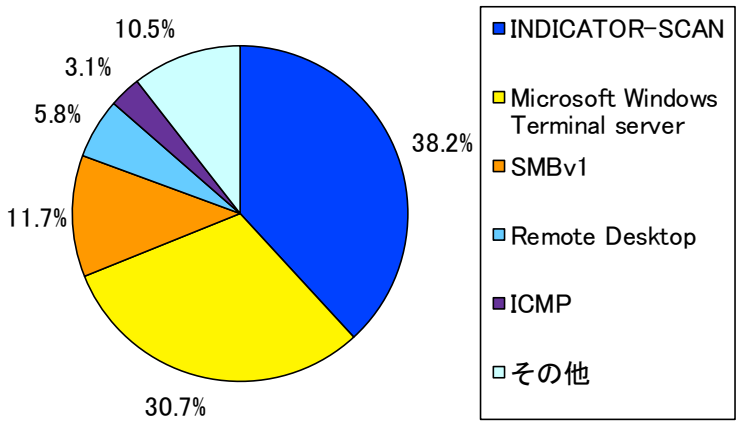

図 3-2 不正侵入等の攻撃手法別検知比率

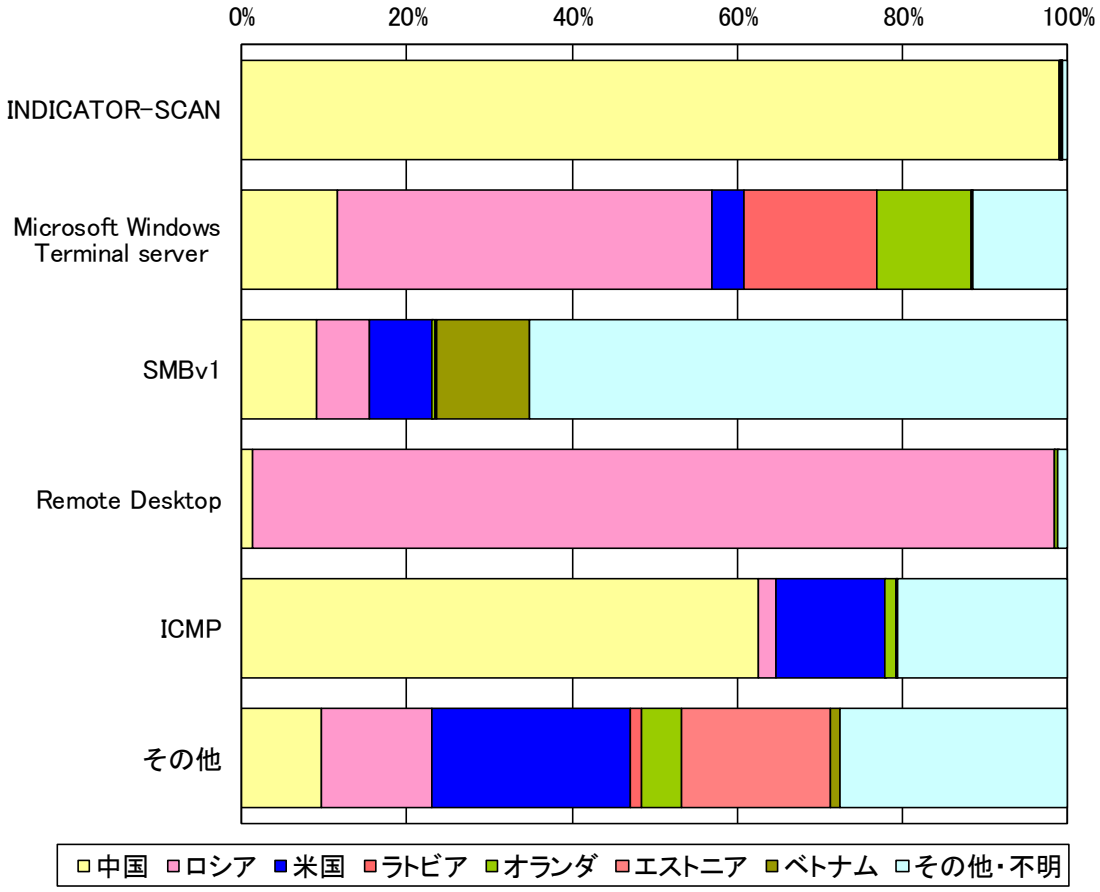

図 3-3 不正侵入等の攻撃手法の国・地域別検知比率

3-2 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	－[ii]	中国	441.02 件	－[ii]	－[ii]
2 位	－[ii]	ロシア	211.43 件	－[ii]	－[ii]
3 位	－[ii]	米国	49.63 件	－[ii]	－[ii]
4 位	－[ii]	ラトビア	49.41 件	－[ii]	－[ii]
5 位	－[ii]	オランダ	39.76 件	－[ii]	－[ii]

[i] 一日・1IP アドレス当たり。

[ii] 平成 31 年 1 月 1 日以降の不正侵入等の攻撃手法の検知については、攻撃手法の分類見直しを実施したため、前期との比較はありません。

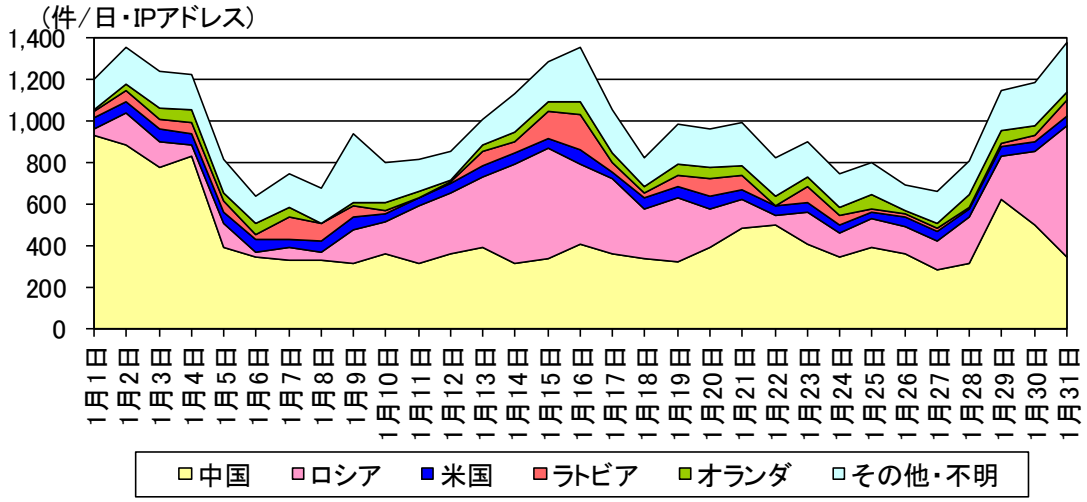

図 3-4　不正侵入等の着信元国・地域別検知件数の推移

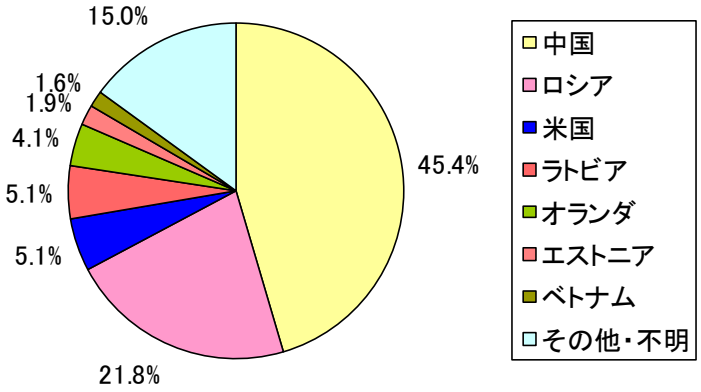

図 3-5　不正侵入等の着信元国・地域別検知比率

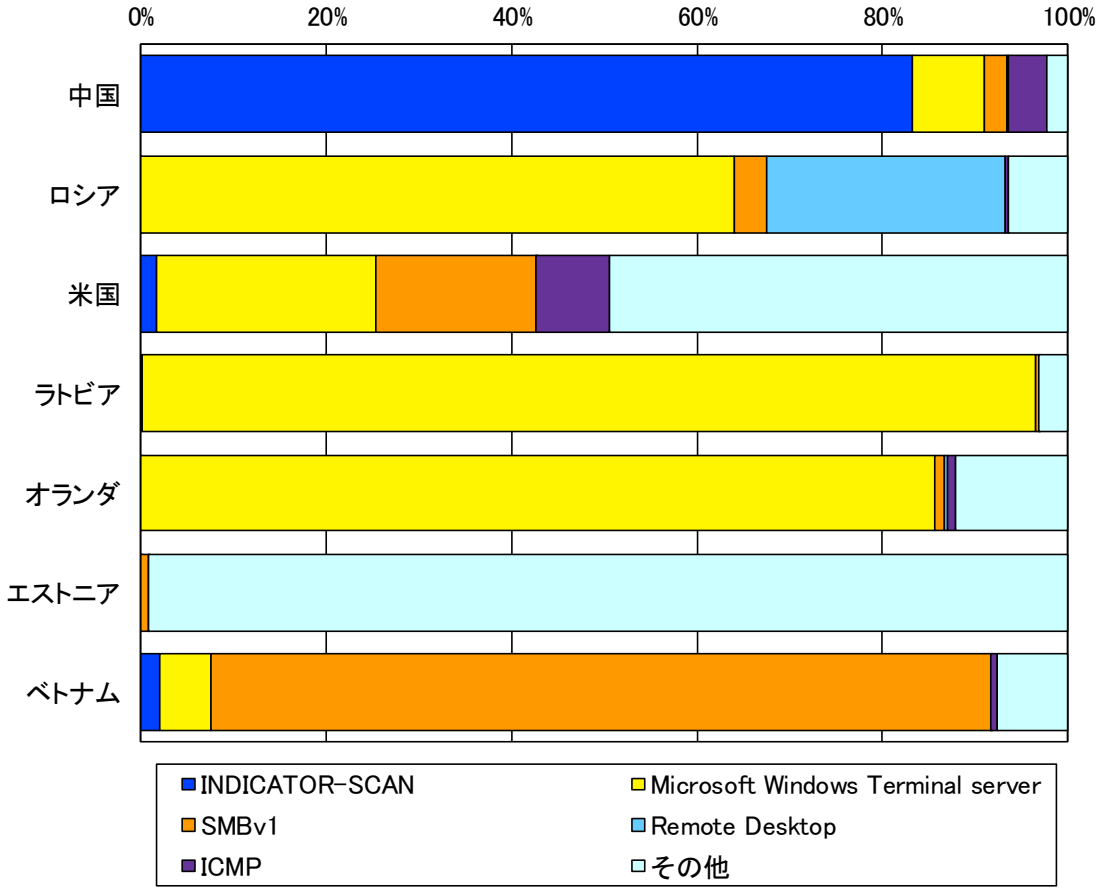

図 3-6　不正侵入等の着信元国・地域別上位の攻撃手法別検知比率

4　DoS 攻撃被害の観測結果

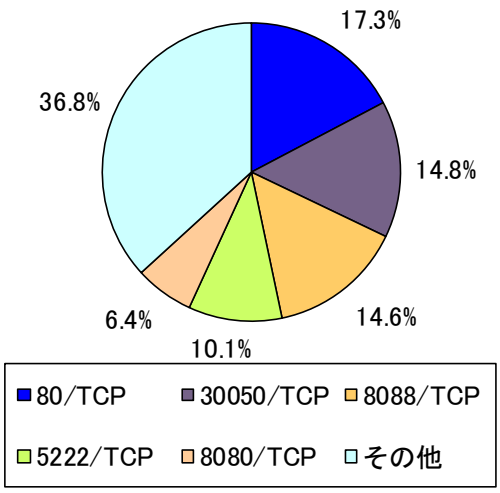

図 4-1　跳ね返りパケット着信元ポート別比率

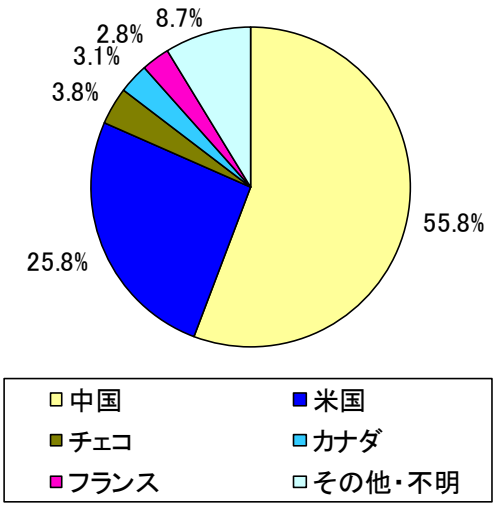

図 4-2　跳ね返りパケット着信元国・地域別比率

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