平成 30 年 11 月 30 日

平成 30 年9月期観測資料

1　観測結果概要

平成 30 年9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 3,274.3 件で、平成 30 年8月期（以下「前期」という。）と比較して 302.8 件（10.2%）増加しました。また、発信元 IP アドレス数は、一日当たり 48,811.5 個で、前期と比較して 235.0 個（0.5%）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 1,113.5 件で、前期と比較して 253.5 件（29.5%）増加しました。また、発信元 IP アドレス数は、一日当たり 4,060.8 個で、前期と比較して 64.1 個（1.6%）増加しました。

DoS 攻撃被害検知件数は、一日当たり 7,481.0 件で、前期と比較して 9,130.4 件（55.0%）減少しました。また、発信元 IP アドレス数は、一日当たり 272.6 個で、前期と比較して 43.4 個（13.7%）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	356.97 件	－8.6%　（－33.78 件）
2 位	2 位	445/TCP	257.15 件	＋6.1%　（＋14.70 件）
3 位	6 位	52869/TCP	87.74 件	＋25.8%　（＋17.98 件）
4 位	5 位	1433/TCP	80.15 件	＋1.3%　（＋1.06 件）
5 位	3 位	22/TCP	78.95 件	－3.8%　（－3.16 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	87.74 件	＋25.8%　（＋17.98 件）	3 位	6 位
2 位	53413/UDP	44.23 件	＋51.9%　（＋15.12 件）	9 位	13 位
3 位	445/TCP	257.15 件	＋6.1%　（＋14.70 件）	2 位	2 位
4 位	6379/TCP	15.25 件	＋147.2%　（＋9.08 件）	20 位	36 位
5 位	5431/TCP	10.20 件	＋202.1%　（＋6.83 件）	25 位	55 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	23/TCP	356.97 件	－8.6%　（－33.78 件）	1 位	1 位
2 位	0/TCP	0.10 件	－[ii]　（－18.67 件）	－[ii]	16 位
3 位	2323/TCP	22.75 件	－26.7%　（－8.29 件）	13 位	12 位
4 位	8888/TCP	9.78 件	－37.4%　（－5.84 件）	26 位	19 位
5 位	37215/TCP	10.44 件	－32.6%　（－5.06 件）	24 位	20 位

[i] 一日・1IP アドレス当たり。

[ii] 今期のアクセス件数が僅かなため、前期比及び今期順位は記載していません。

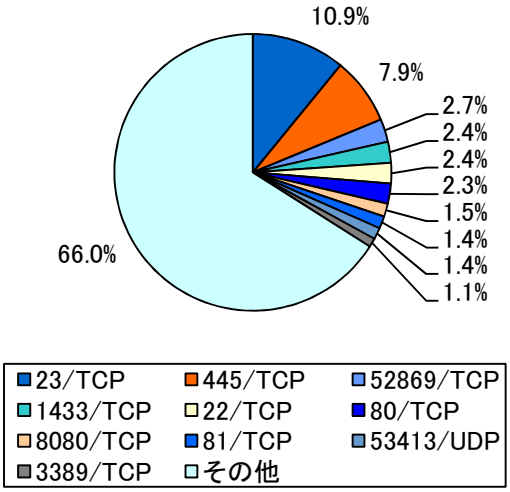

図 2-1　宛先ポート別比率（全て）[i]

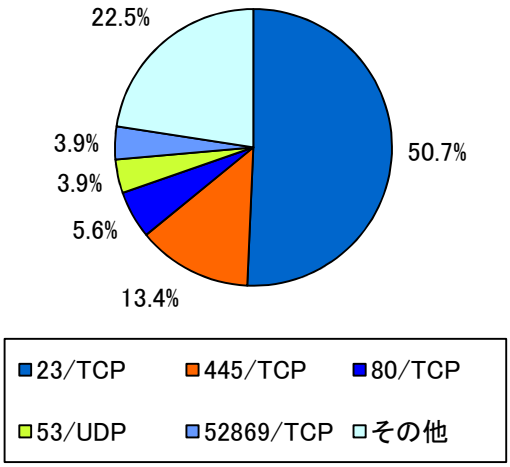

図 2-2　宛先ポート別比率（日本国内）

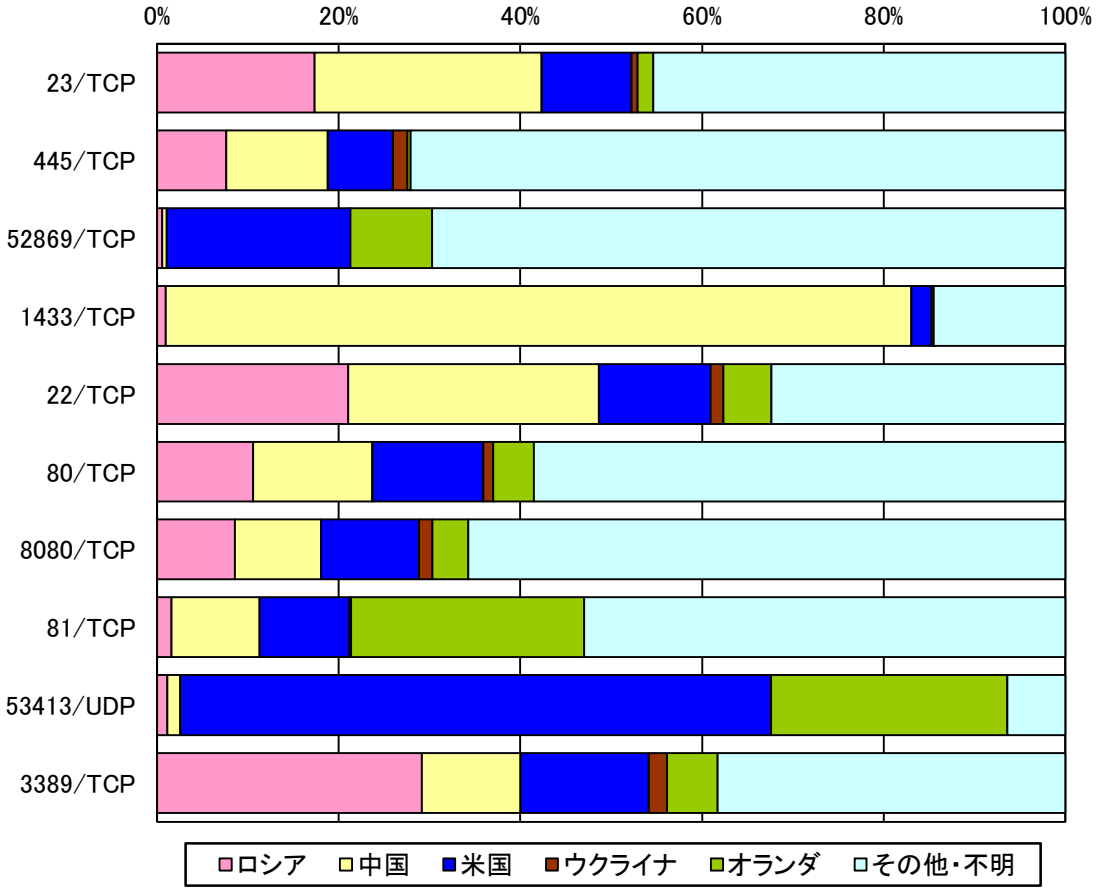

図 2-3　宛先ポート別上位の発信元国・地域別比率 [ii]

[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] 発信元の国・地域については、当該国・地域に割り当てられた IP アドレスを指しています。以降も同様の表記です。

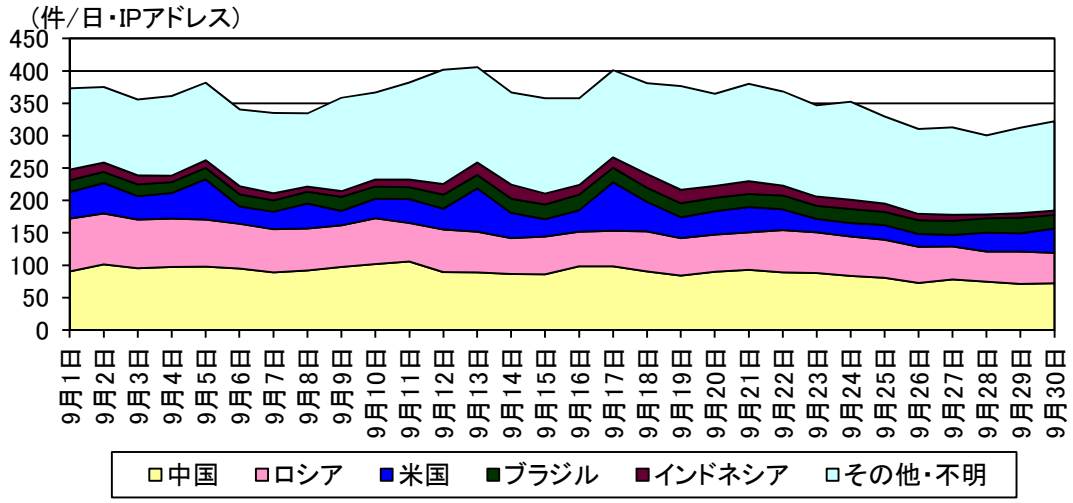

図 2-4　センサーのポート 23/TCP における検知件数の推移

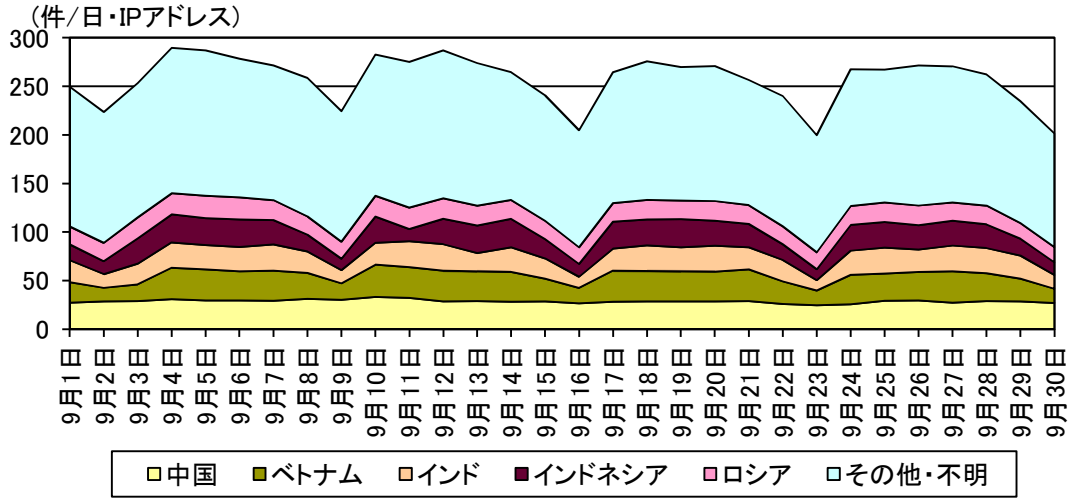

図 2-5　センサーのポート 445/TCP における検知件数の推移

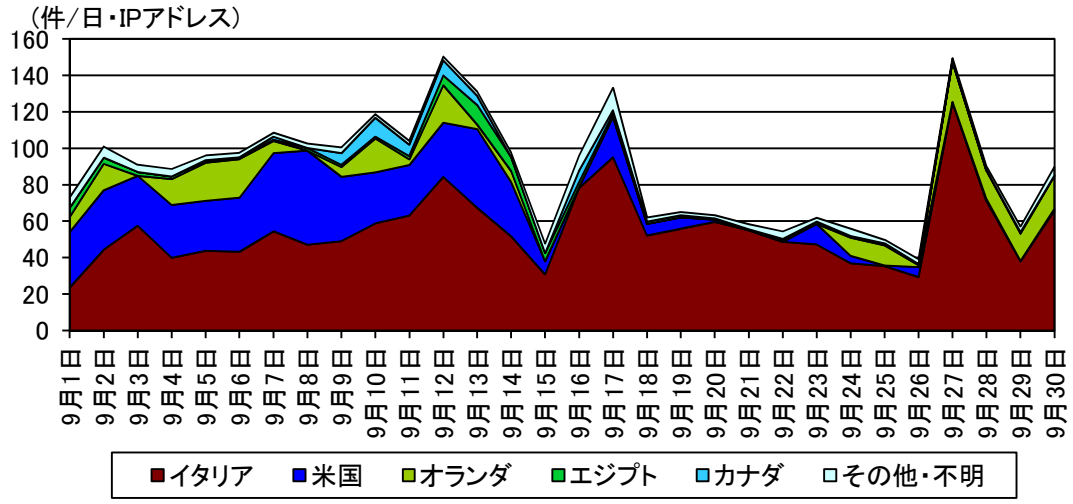

図 2-6　センサーのポート 52869/TCP における検知件数の推移

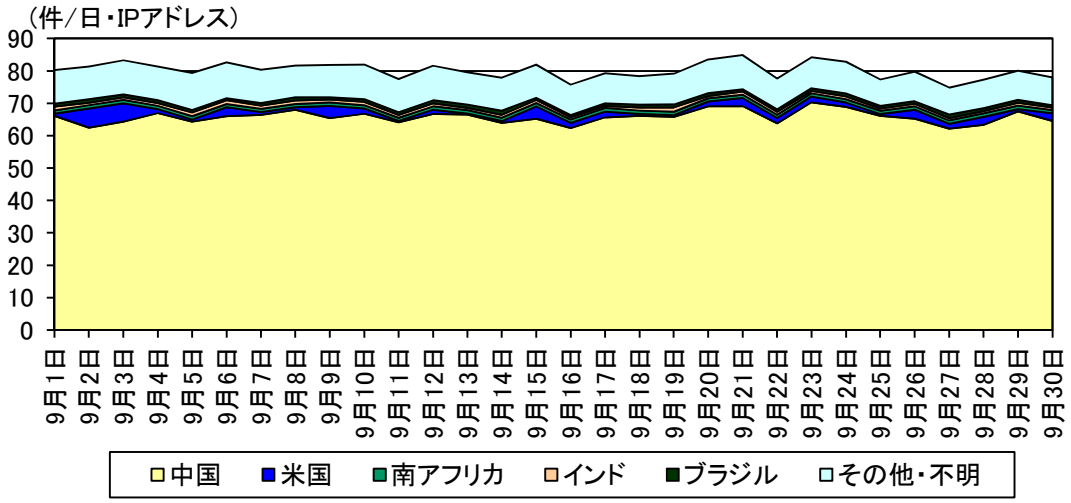

図 2-7　センサーのポート 1433/TCP における検知件数の推移

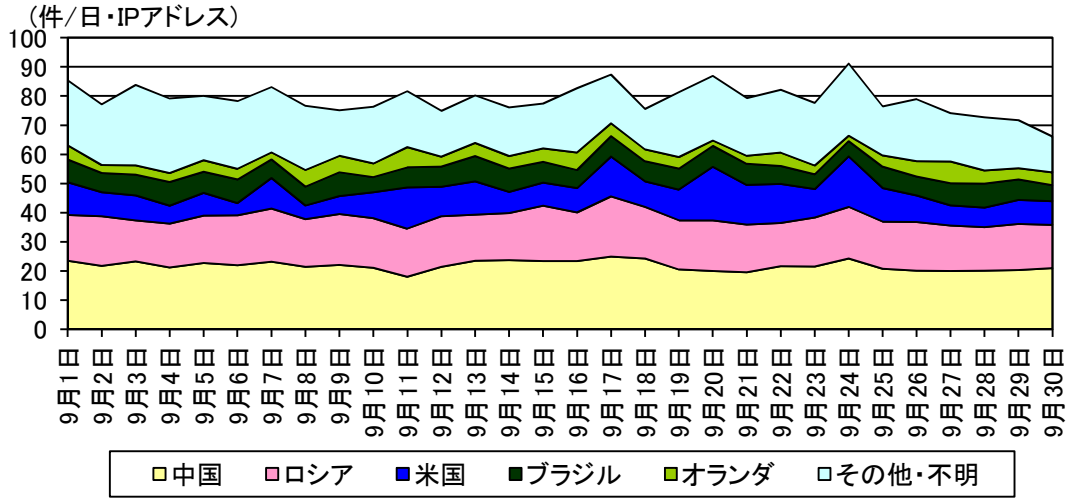

図 2-8　センサーのポート 22/TCP における検知件数の推移

2-2　発信元国・地域別アクセス検知件数

表 2-4　発信元国・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	951.01 件	＋11.9%　（＋100.88 件）
2 位	2 位	中国	380.65 件	－10.6%　（－45.32 件）
3 位	3 位	米国	376.76 件	－1.0%　（－3.91 件）
4 位	7 位	ウクライナ	283.68 件	＋306.6%　（＋213.91 件）
5 位	4 位	オランダ	180.66 件	－17.1%　（－37.24 件）

表 2-5　発信元国・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	ウクライナ	283.68 件	＋306.6%　（＋213.91 件）	4 位	7 位
2 位	ロシア	951.01 件	＋11.9%　（＋100.88 件）	1 位	1 位
3 位	フランス	101.97 件	＋240.5%　（＋72.03 件）	6 位	18 位
4 位	ドイツ	86.25 件	＋119.0%　（＋46.88 件）	8 位	13 位
5 位	ブルガリア	50.46 件	＋113.2%　（＋26.79 件）	12 位	20 位

表 2-6　発信元国・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	チリ	6.18 件	－88.1%　（－45.90 件）	37 位	10 位
2 位	中国	380.65 件	－10.6%　（－45.32 件）	2 位	2 位
3 位	オランダ	180.66 件	－17.1%　（－37.24 件）	5 位	4 位
4 位	スイス	3.77 件	－79.2%　（－14.31 件）	45 位	24 位
5 位	エジプト	27.93 件	－26.6%　（－10.13 件）	19 位	14 位

[i] 一日・1IP アドレス当たり。

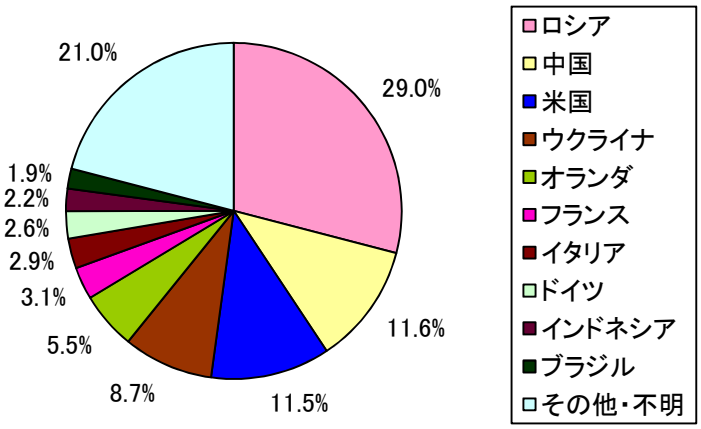

図 2-9　発信元国・地域別比率

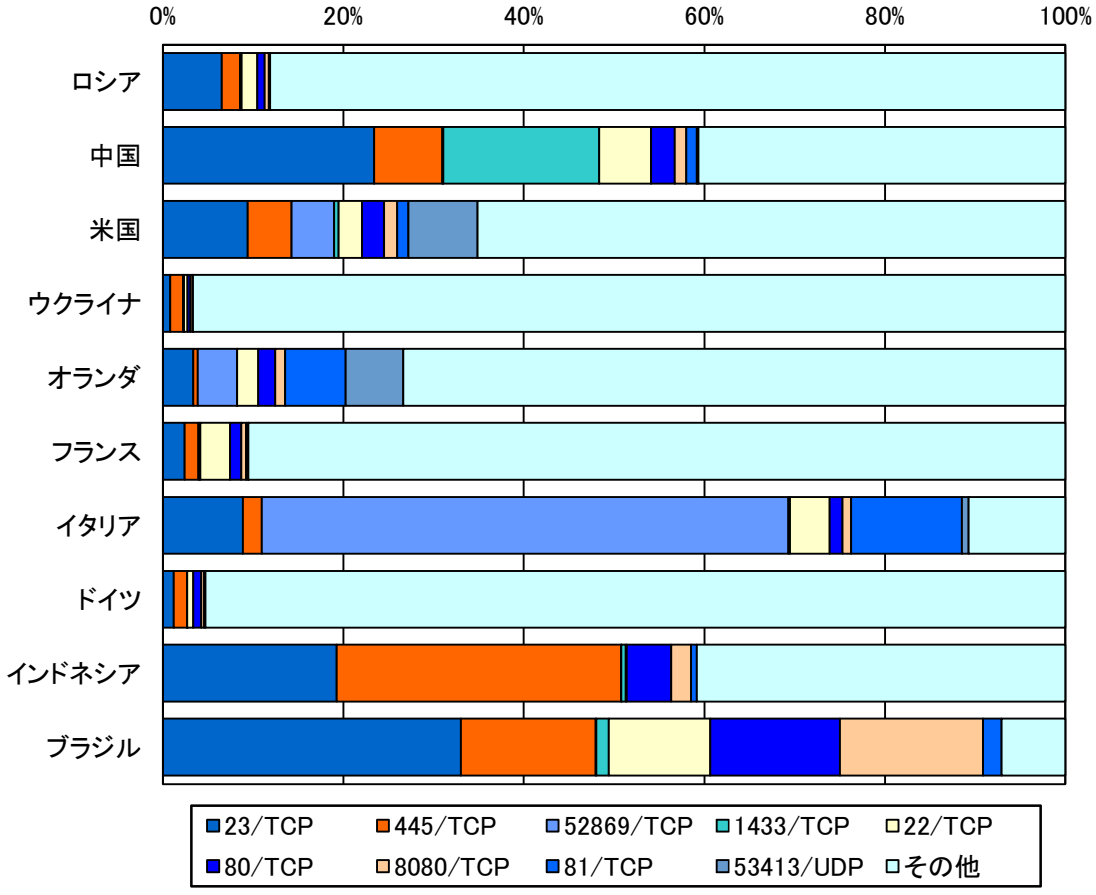

図 2-10　発信元国・地域別上位の宛先ポート別比率

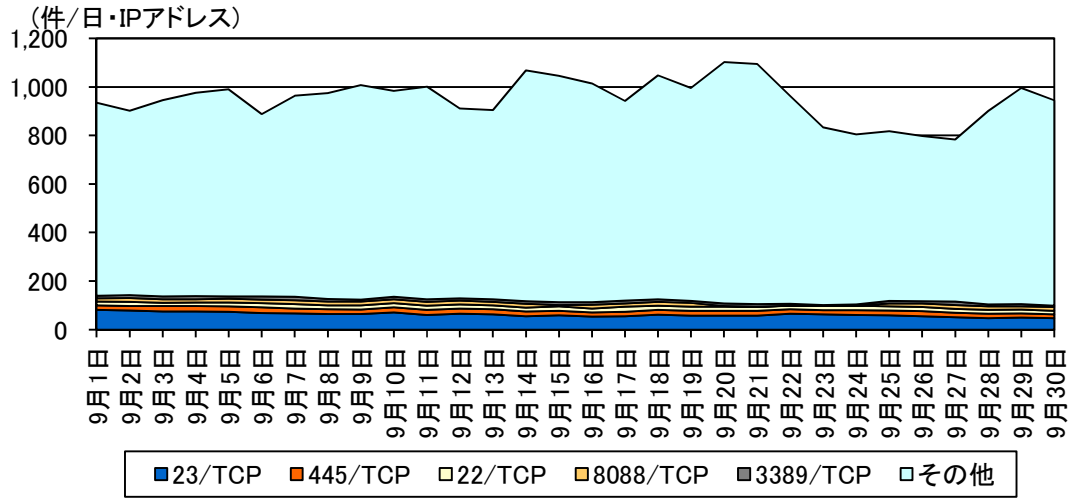

図 2-11　ロシアからの検知件数の推移

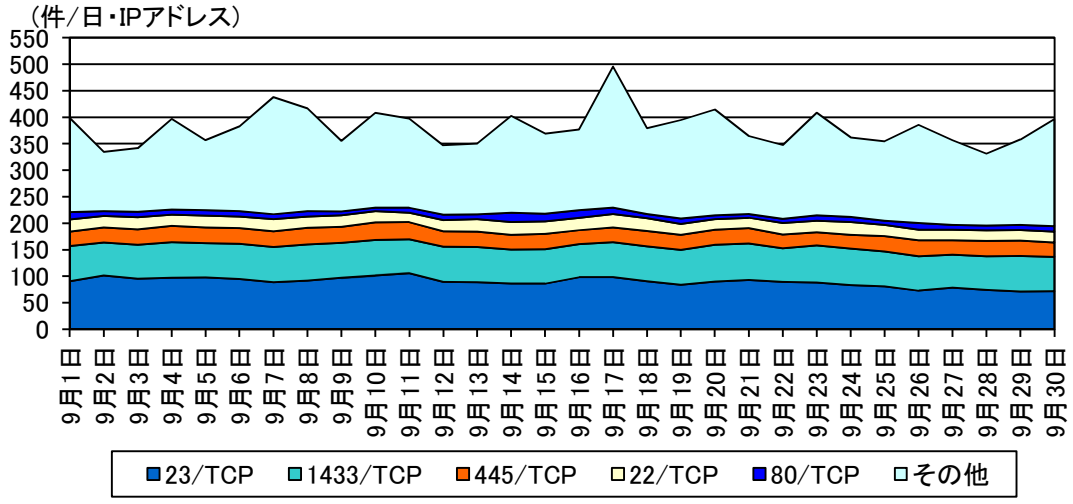

図 2-12　中国からの検知件数の推移

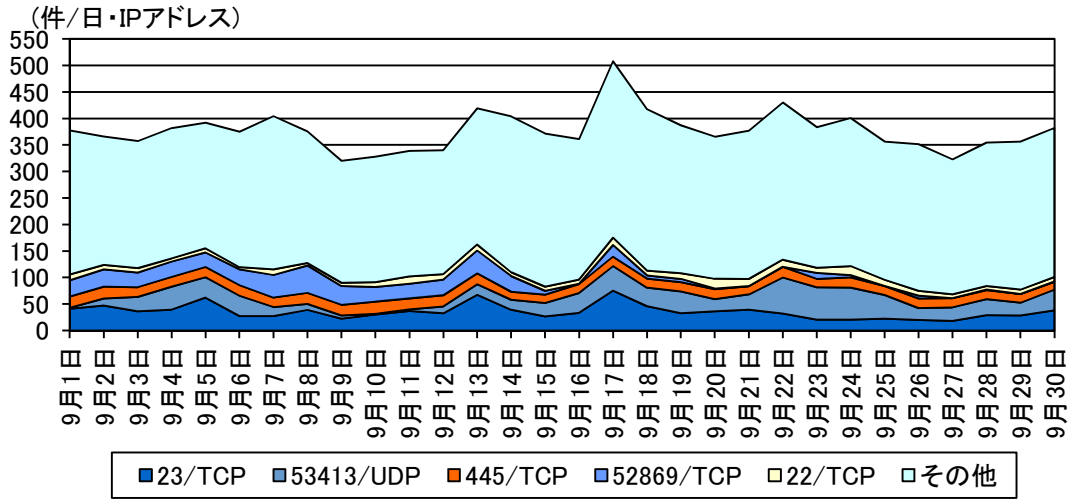

図 2-13　米国からの検知件数の推移

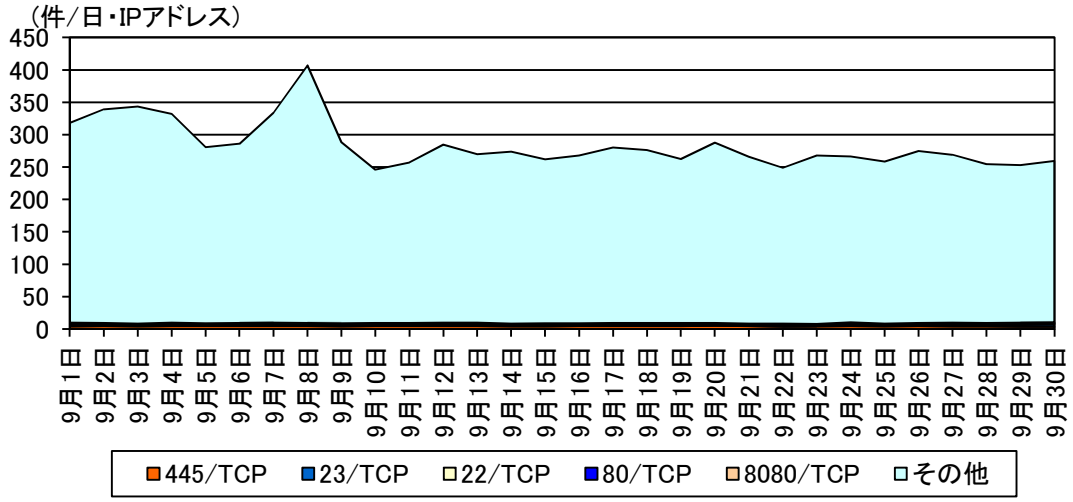

図 2-14 ウクライナからの検知件数の推移

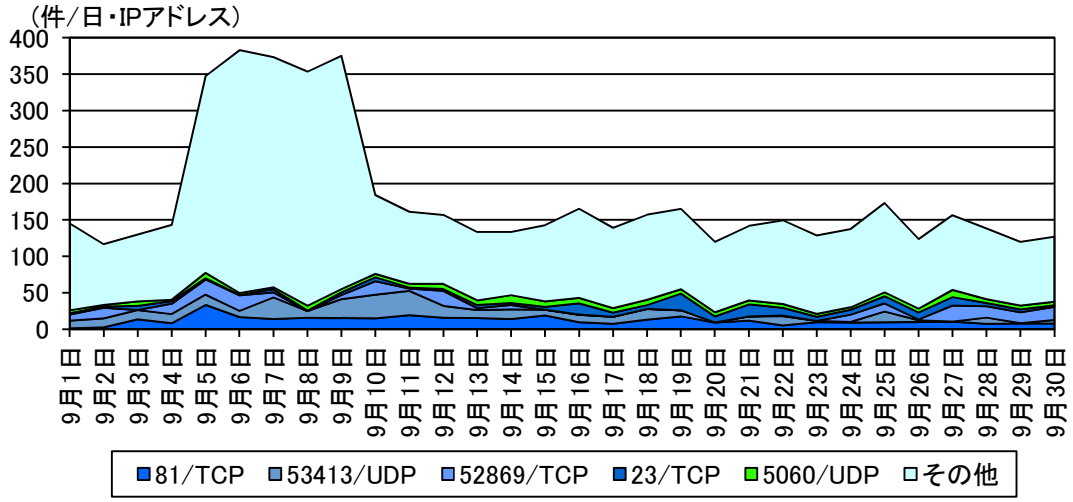

図 2-15 オランダからの検知件数の推移

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	1 位	Scan	538.84 件	＋33.0%　（＋133.66 件）	1 位	
2 位	2 位	DNS	501.55 件	＋30.6%　（＋117.65 件）	2 位	
3 位	3 位	VoIP	35.33 件	＋3.5%　（＋1.18 件）	4 位	
4 位	5 位	ICMP	16.96 件	＋16.2%　（＋2.36 件）	3 位	
5 位	4 位	Scan(Password)	14.46 件	－17.3%　（－3.03 件）		1 位

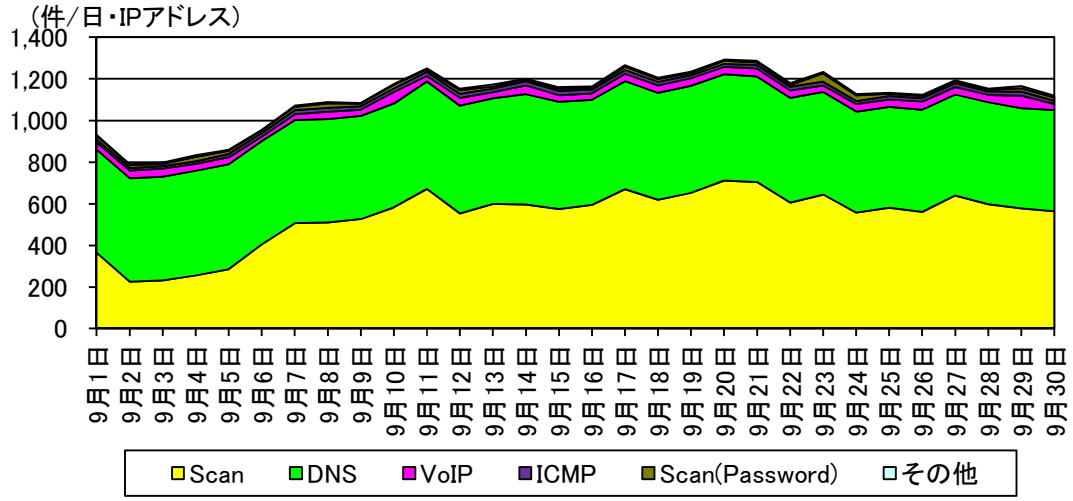

図 3-1　不正侵入等の攻撃手法別検知件数の推移

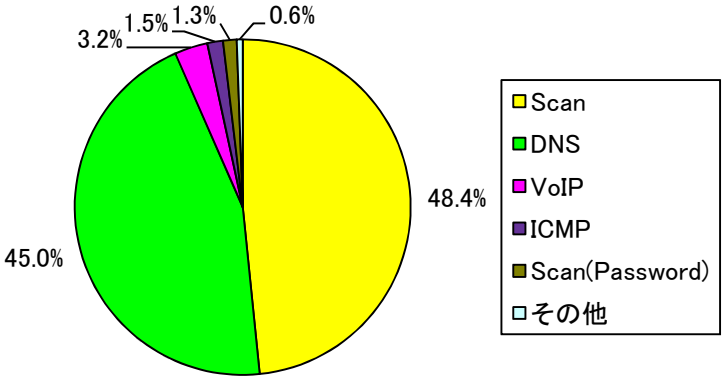

図 3-2　不正侵入等の攻撃手法別検知比率

[i] 一日・1IP アドレス当たり。

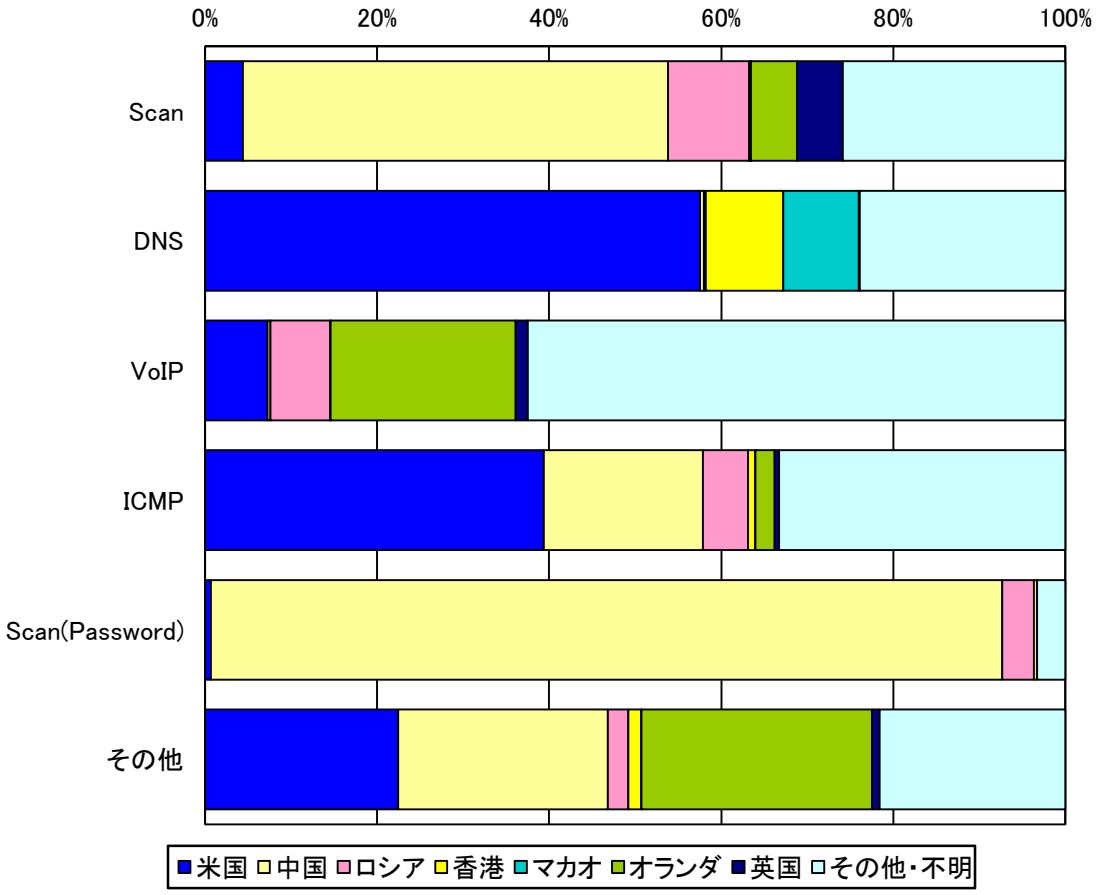

図 3-3　不正侵入等の攻撃手法の国・地域別検知比率

3-2 発信元国・地域別アクセス検知件数

表 3-2 不正侵入等の発信元国・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	米国	323.09 件	＋25.1% （＋64.78 件）
2 位	2 位	中国	286.56 件	＋41.0% （＋83.39 件）
3 位	5 位	ロシア	55.91 件	＋81.7% （＋25.14 件）
4 位	3 位	香港	46.77 件	＋27.1% （＋9.97 件）
5 位	4 位	マカオ	44.04 件	＋21.8% （＋7.87 件）

表 3-3 不正侵入等の発信元国・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	中国	286.56 件	＋41.0% （＋83.39 件）	2 位	2 位
2 位	米国	323.09 件	＋25.1% （＋64.78 件）	1 位	1 位
3 位	ロシア	55.91 件	＋81.7% （＋25.14 件）	3 位	5 位
4 位	英国	29.30 件	＋291.7% （＋21.82 件）	7 位	21 位
5 位	フランス	24.52 件	＋72.8% （＋10.33 件）	12 位	12 位

表 3-4 不正侵入等の発信元国・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	3.99 件	－51.2% （－4.18 件）	25 位	19 位
2 位	イタリア	5.06 件	－34.5% （－2.66 件）	21 位	20 位
3 位	ブラジル	24.72 件	－6.3% （－1.66 件）	9 位	7 位
4 位	ウクライナ	2.60 件	－38.8% （－1.65 件）	27 位	25 位
5 位	チェコ	11.31 件	－12.6% （－1.63 件）	16 位	13 位

[i] 一日・1IP アドレス当たり。

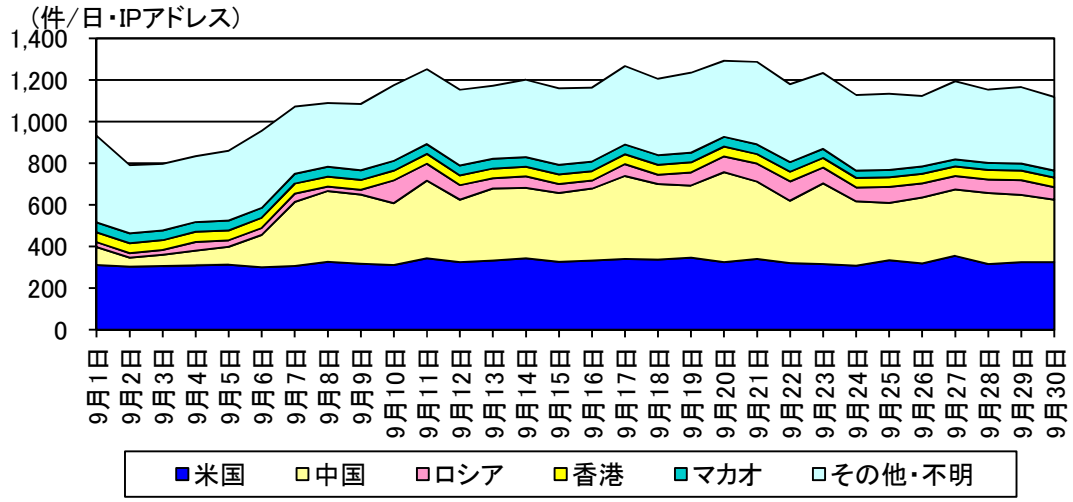

図 3-4　不正侵入等の発信元国・地域別検知件数の推移

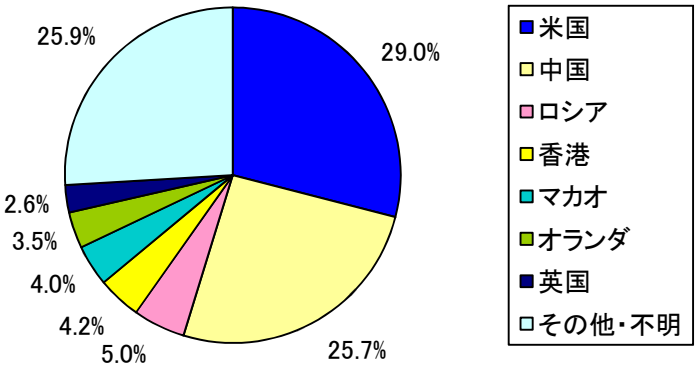

図 3-5　不正侵入等の発信元国・地域別検知比率

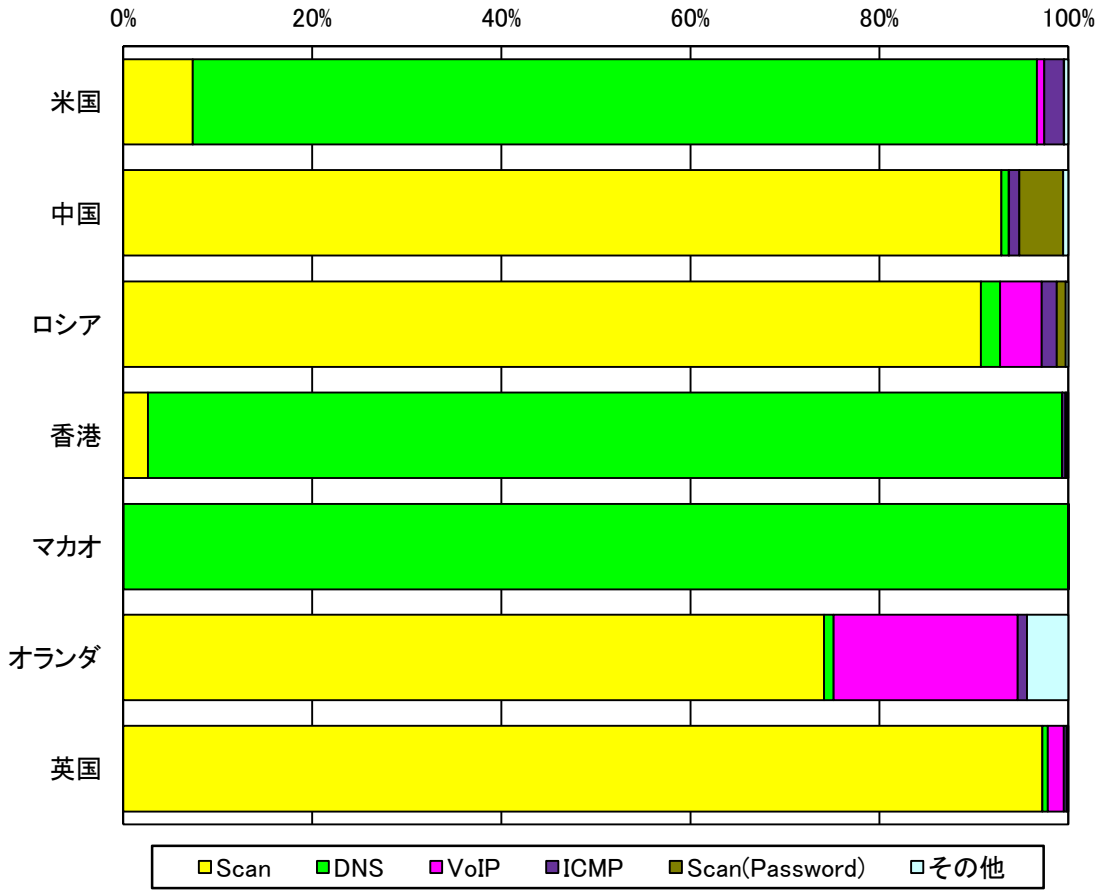

図 3-6 不正侵入等の発信元国・地域別上位の攻撃手法別検知比率

4　DoS 攻撃被害の観測結果

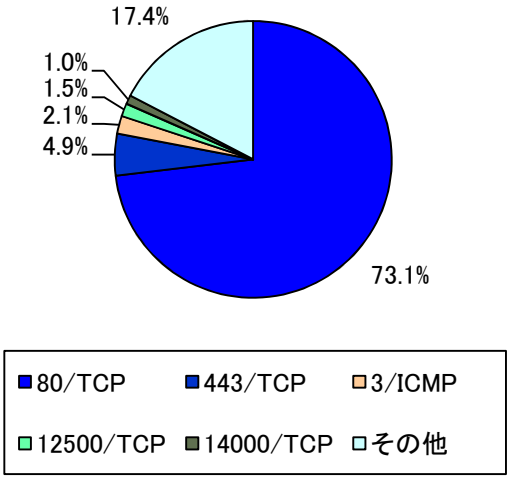

図 4-1　跳ね返りパケット発信元ポート別比率

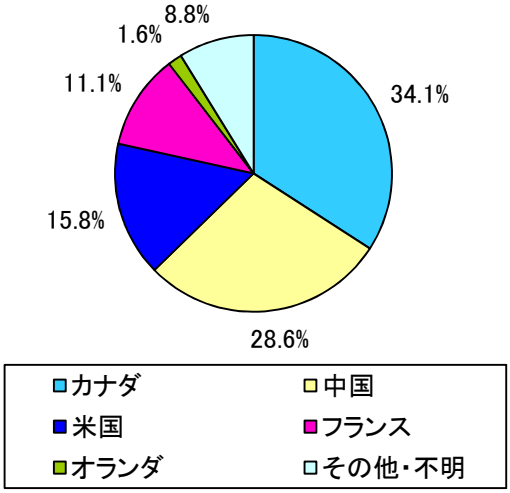

図 4-2　跳ね返りパケット発信元国・地域別比率

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
DNS	DNS に対するスキャン活動や不正なクエリ等の検知
DoS	DoS 攻撃の可能性があるパケットの検知
ICMP	ICMP パケットの検知
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の検知
Scan（P2P）	スキャン活動のうち、P2P に対する活動の検知
Scan（Password）	スキャン活動のうち、各種サービスの ID・パスワード等に対する活動の検知
UDP spam	UDP を使用したポップアップメッセージ等の検知
VoIP	VoIP に対するスキャン活動等の検知
Worm	インターネットを通じて拡散するワームの検知
Others	上記の分類に含まれないもの