平成 30 年 1 月 12 日

平成 29 年 11 月期観測資料

1　観測結果概要

平成 29 年 11 月期（以下「今期」という。）のセンサーに対するアクセス件数は、一日・1IP アドレス当たり 2,040.5 件で、平成 29 年 10 月期（以下「前期」という。）と比較して 314.1 件（18.2%）増加しました。また、発信元 IP アドレス数は、一日当たり 59,041.2 個で、前期と比較して 16,197.4 個（37.8%）増加しました。

シグネチャを用いて検知した不正侵入等の行為（以下「不正侵入等」という。）の件数は、一日・1IP アドレス当たり 698.7 件で、前期と比較して 24.1 件（3.3%）減少しました。また、発信元 IP アドレス数は、一日当たり 1,055.5 個で、前期と比較して 118.5 個（10.1%）減少しました。

DoS 攻撃被害観測において検知した件数は、一日当たり 19,449.1 件で、前期と比較して 7,203.3 件（58.8%）増加しました。また、発信元 IP アドレス数は、一日当たり 341.2 個で、前期と比較して 54.0 個（13.7%）減少しました。

2　インターネット定点観測 ― センサーに対するアクセス

2-1　宛先ポート別

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	818.59 件	＋43.1%　（＋246.49 件）
2 位	2 位	445/TCP	146.73 件	＋12.7%　（＋16.54 件）
3 位	3 位	22/TCP	115.48 件	＋11.0%　（＋11.46 件）
4 位	4 位	1433/TCP	112.65 件	＋11.3%　（＋11.40 件）
5 位	6 位	2323/TCP	74.62 件	＋56.8%　（＋27.04 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	23/TCP	818.59 件	＋43.1%　（＋246.49 件）	1 位	1 位
2 位	2323/TCP	74.62 件	＋56.8%　（＋27.04 件）	5 位	6 位
3 位	445/TCP	146.73 件	＋12.7%　（＋16.54 件）	2 位	2 位
4 位	22/TCP	115.48 件	＋11.0%　（＋11.46 件）	3 位	3 位
5 位	1433/TCP	112.65 件	＋11.3%　（＋11.40 件）	4 位	4 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	53413/UDP	43.05 件	－24.9%　（－14.31 件）	6 位	5 位
2 位	123/UDP	11.74 件	－29.3%　（－4.85 件）	17 位	12 位
3 位	2375/TCP	1.03 件	－81.4%　（－4.52 件）	99 位	23 位
4 位	1900/UDP	12.50 件	－26.5%　（－4.52 件）	15 位	11 位
5 位	5060/UDP	24.41 件	－6.9%　（－1.82 件）	10 位	8 位

[i] 一日・1IP アドレス当たり。

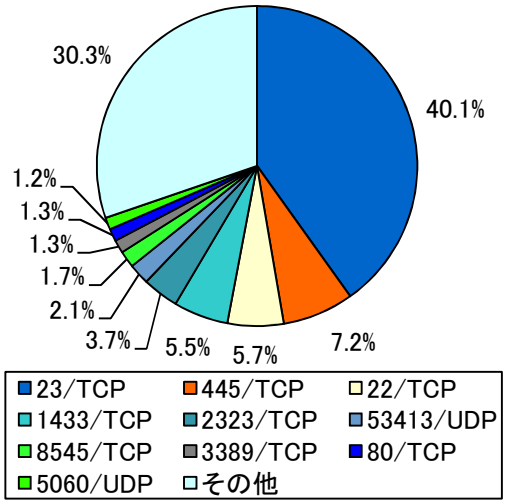

図 2-1　宛先ポート別比率（全て）[i]

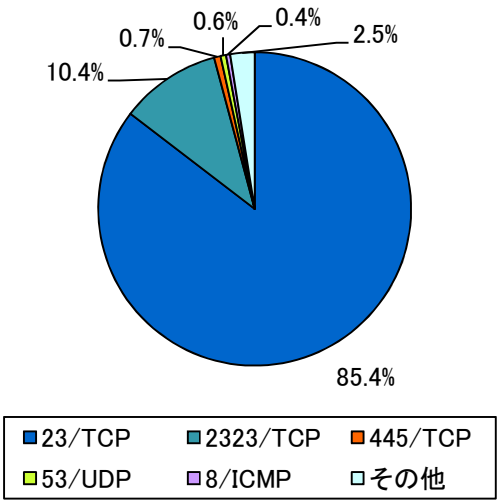

図 2-2　宛先ポート別比率（日本）[ii]

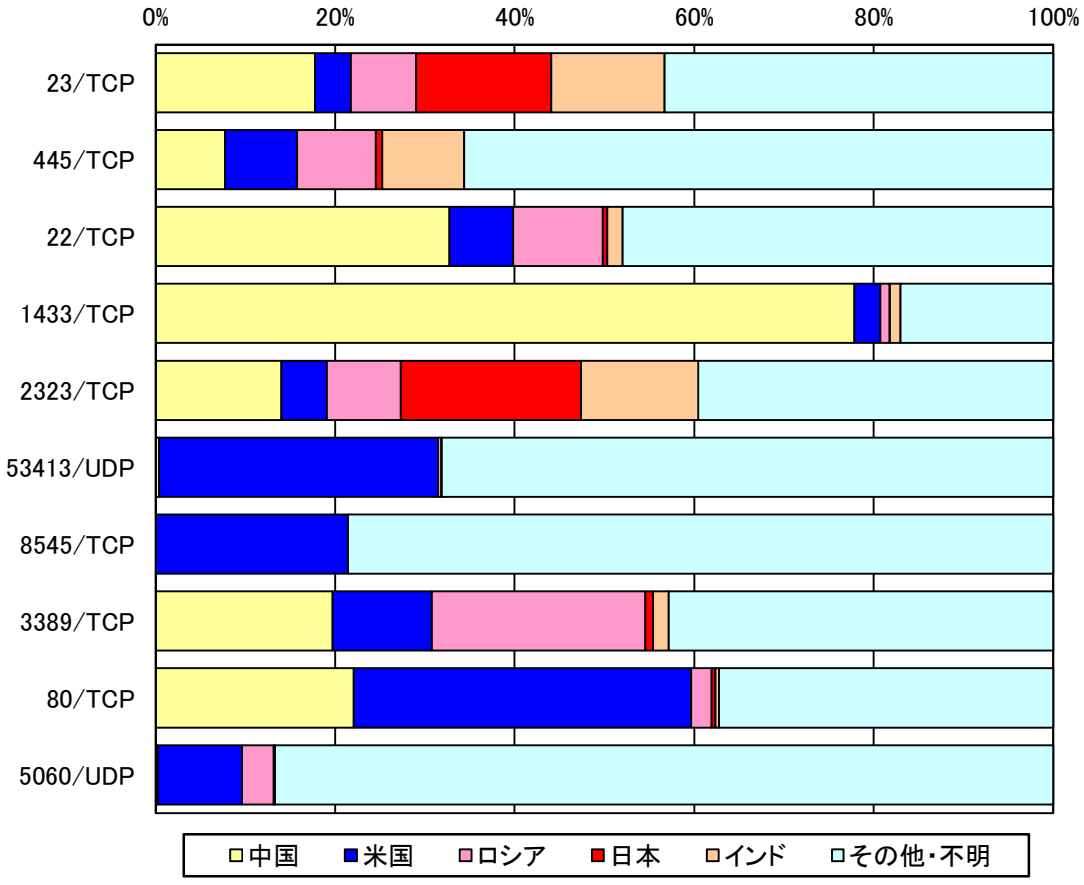

図 2-3　宛先ポート別上位の発信元国・地域別比率 [iii]

[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%になりません。
[ii] 発信元国・地域が日本国内からのアクセスのみ集計しました。
[iii] 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。

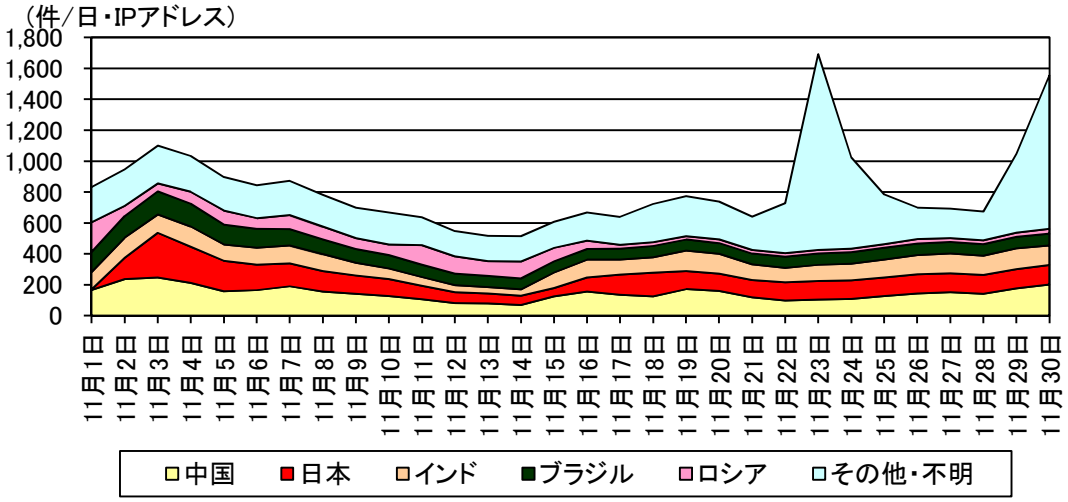

図 2-4 宛先ポート 23/TCP に対するアクセス件数の推移

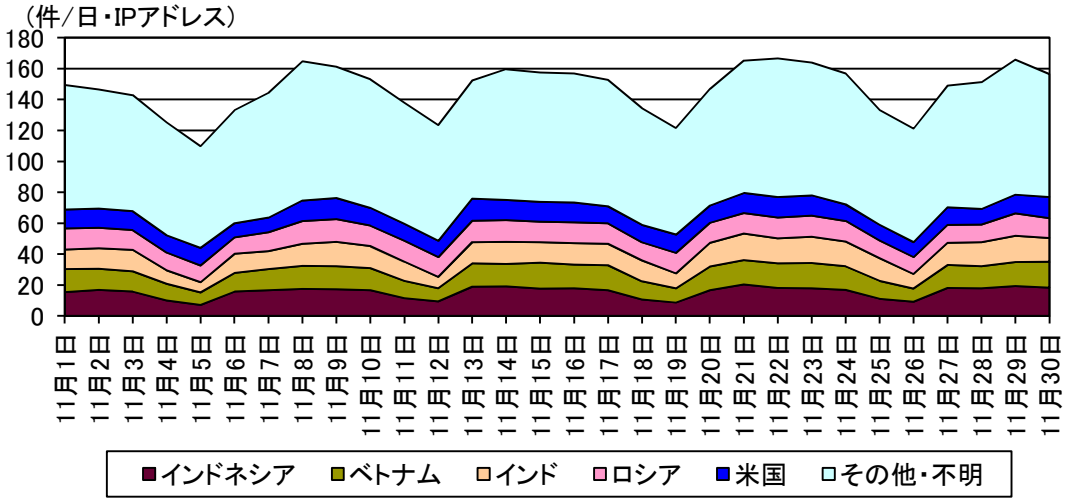

図 2-5 宛先ポート 445/TCP に対するアクセス件数の推移

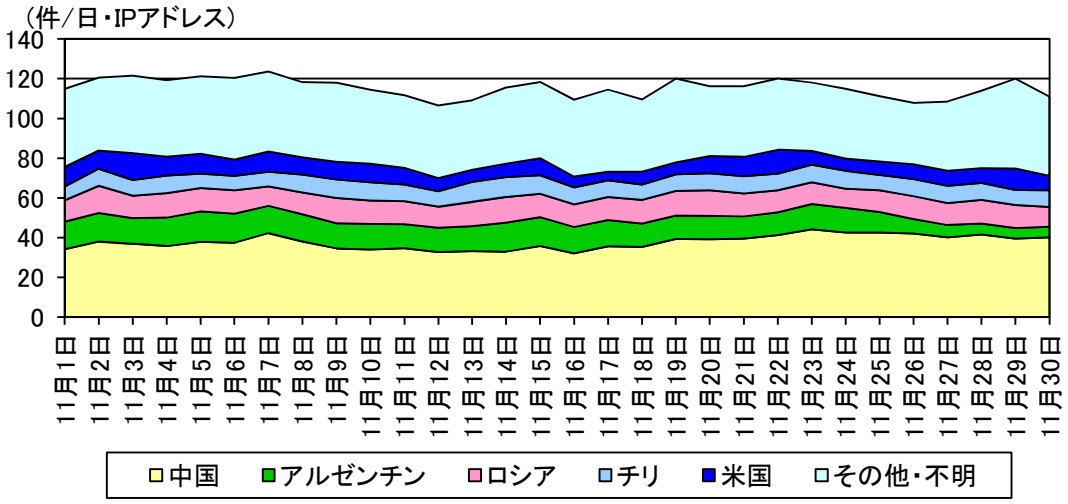

図 2-6 宛先ポート 22/TCP に対するアクセス件数の推移

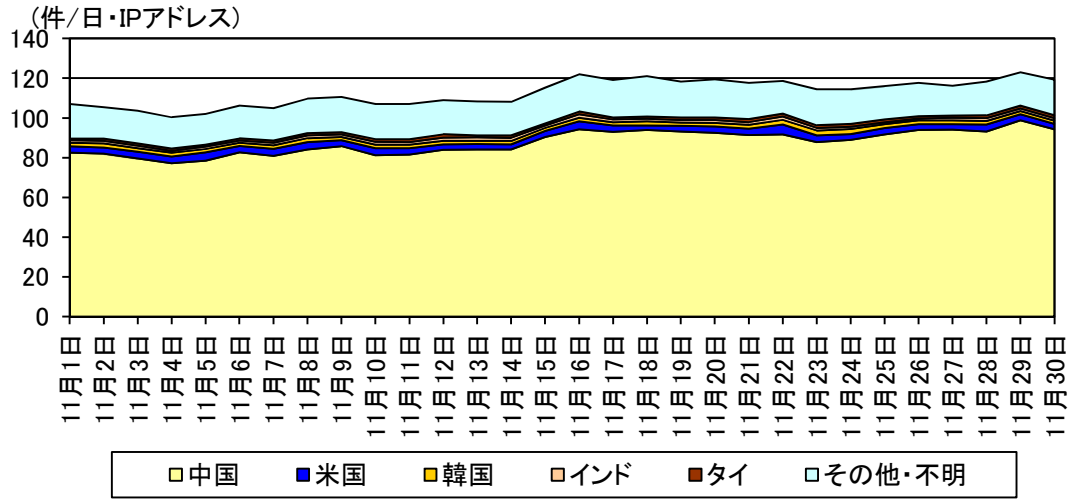

図 2-7　宛先ポート 1433/TCP に対するアクセス件数の推移

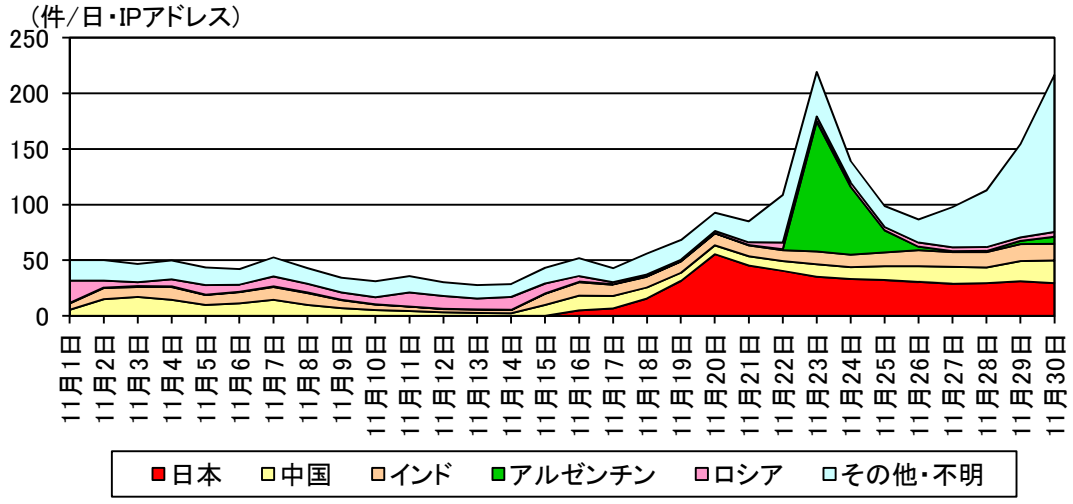

図 2-8　宛先ポート 2323/TCP に対するアクセス件数の推移

2-2　発信元国・地域別

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	中国	415.07 件	＋10.5%　（＋39.40 件）
2 位	2 位	米国	232.57 件	－15.0%　（－41.10 件）
3 位	3 位	ロシア	204.43 件	＋26.7%　（＋43.04 件）
4 位	30 位	日本	143.92 件	－[ii]　（＋136.72 件）
5 位	5 位	インド	134.52 件	＋17.6%　（＋20.14 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	日本	143.92 件	－[ii]　（＋136.72 件）	4 位	30 位
2 位	アルゼンチン	82.36 件	＋243.3%　（＋58.37 件）	8 位	13 位
3 位	ロシア	204.43 件	＋26.7%　（＋43.04 件）	3 位	3 位
4 位	中国	415.07 件	＋10.5%　（＋39.40 件）	1 位	1 位
5 位	インド	134.52 件	＋17.6%　（＋20.14 件）	5 位	5 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	米国	232.57 件	－15.0%　（－41.10 件）	2 位	2 位
2 位	ブラジル	106.25 件	－11.0%　（－13.07 件）	6 位	4 位
3 位	オランダ	53.41 件	－18.2%　（－11.89 件）	9 位	7 位
4 位	フランス	43.32 件	－13.4%　（－6.69 件）	11 位	8 位
5 位	イラン	7.19 件	－29.1%　（－2.95 件）	36 位	22 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、前期比は記載していません。

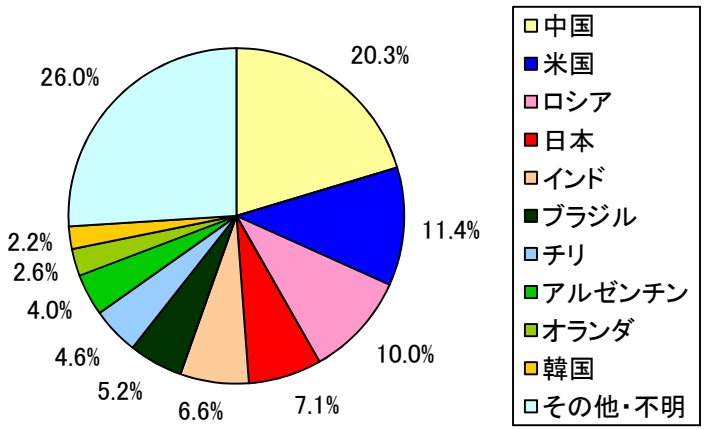

図 2-9　発信元国・地域別比率

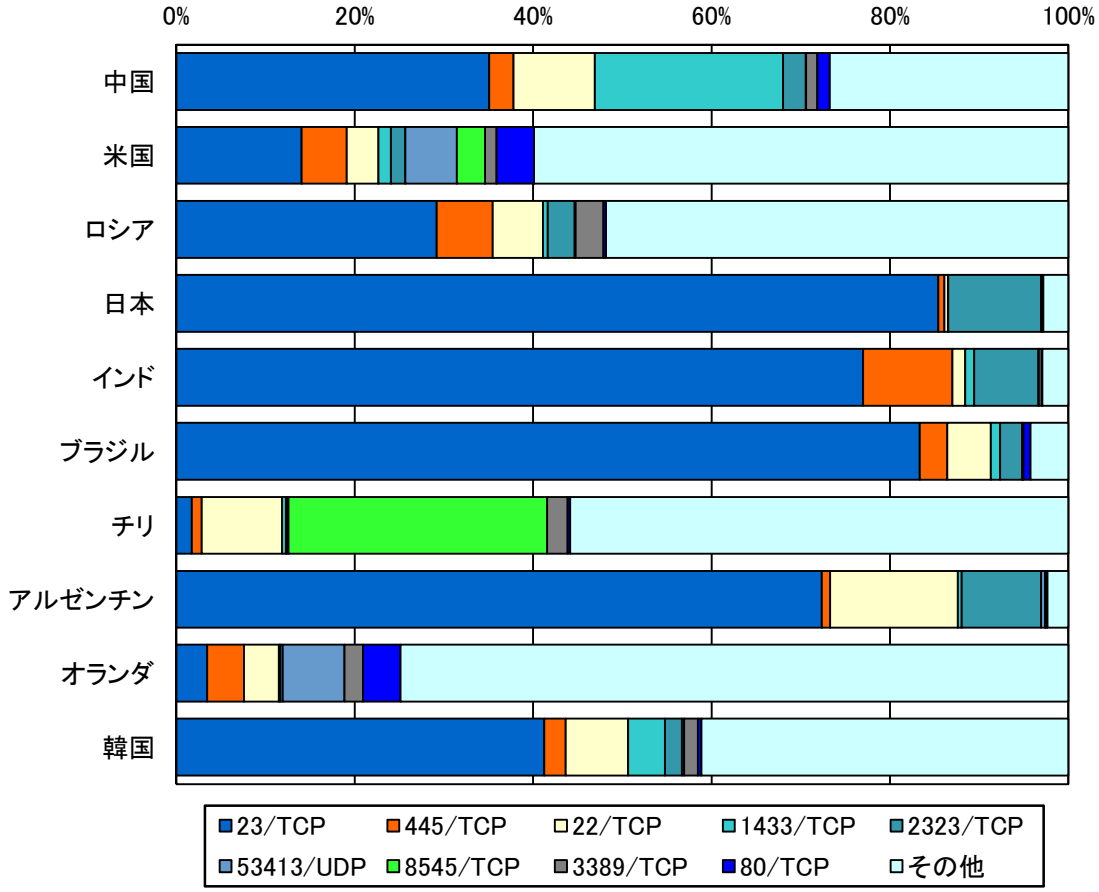

図 2-10　発信元国・地域別上位の宛先ポート別比率

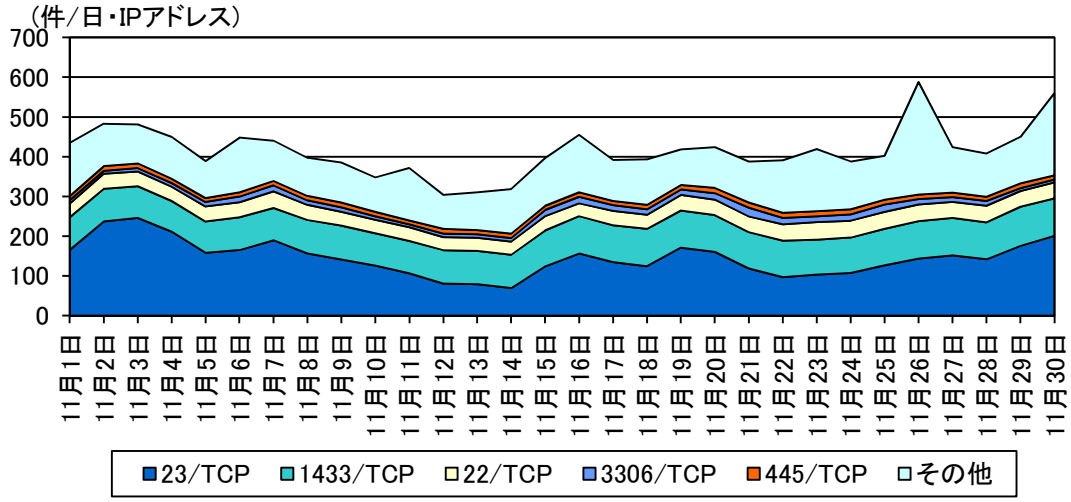

図 2-11　中国からのアクセス件数の推移

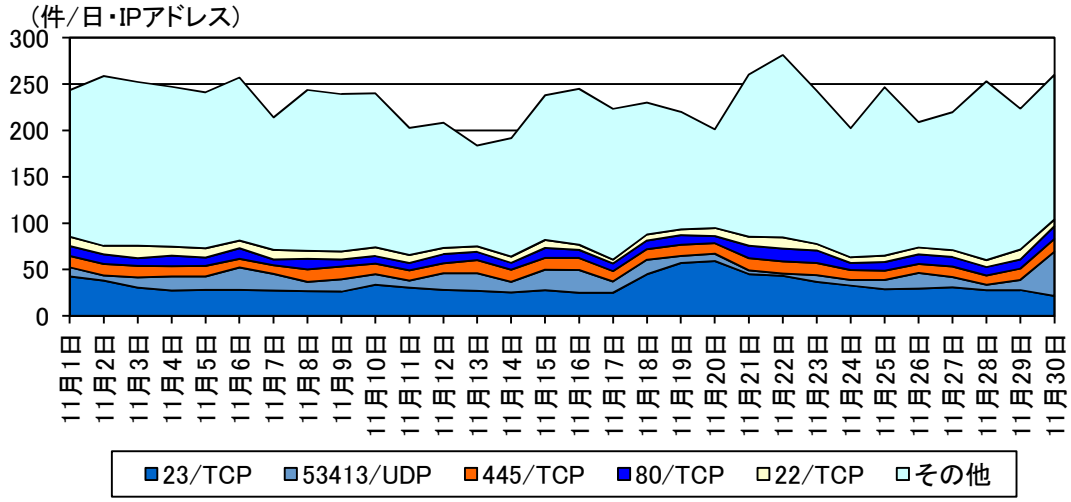

図 2-12　米国からのアクセス件数の推移

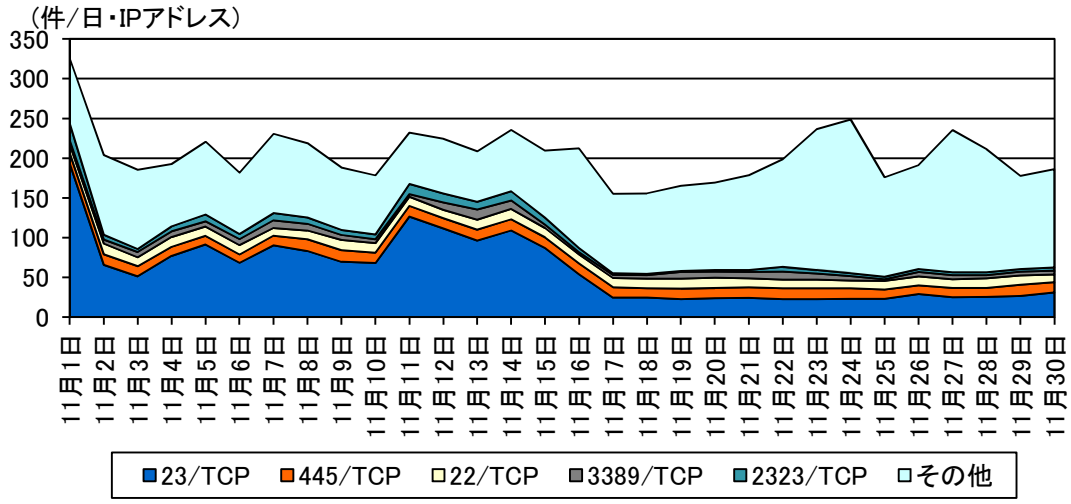

図 2-13　ロシアからのアクセス件数の推移

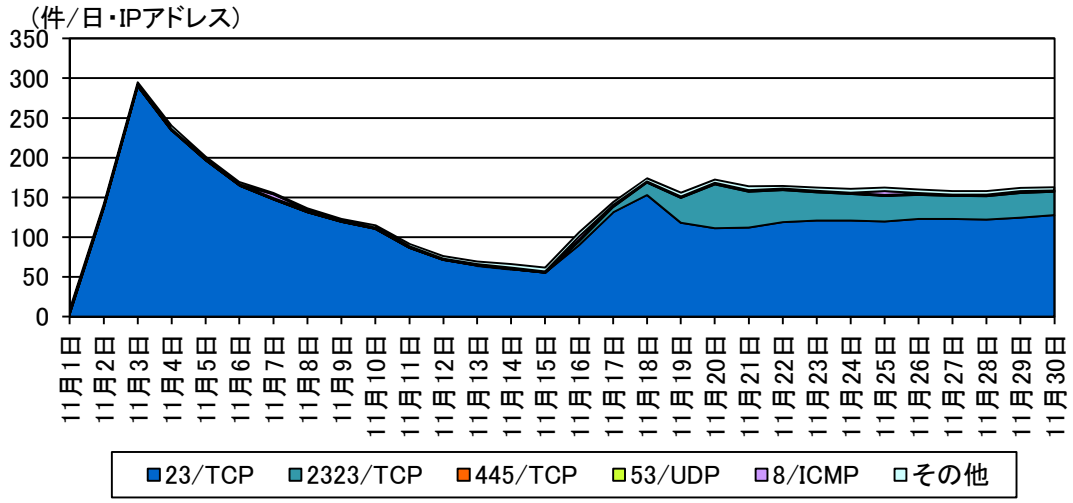

図 2-14　日本からのアクセス件数の推移

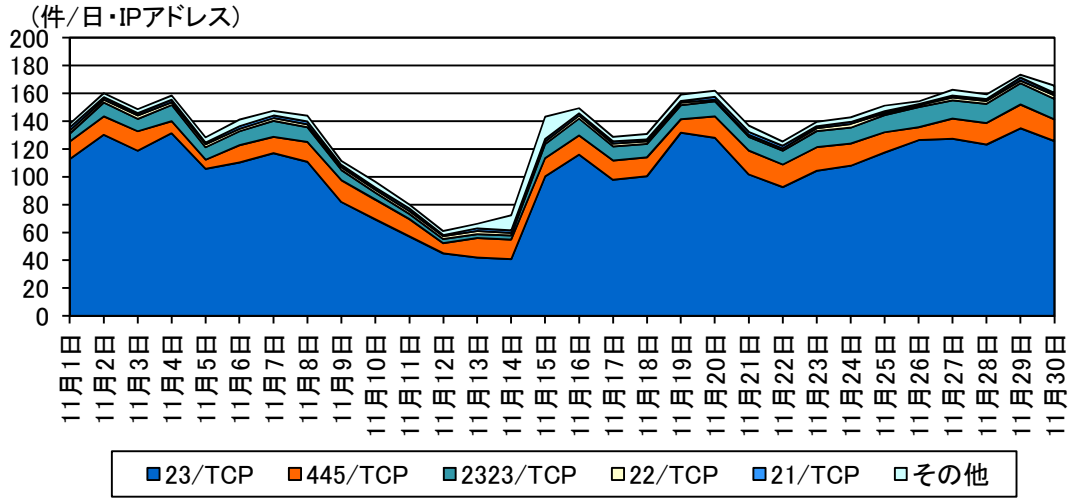

図 2-15　インドからのアクセス件数の推移

3　インターネット定点観測 ― 不正侵入等の検知

3-1　攻撃手法別

表 3-1　不正侵入等の攻撃手法別検知件数（今期順位）

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	582.17 件	－8.7%　（－55.53 件）		1 位
2 位	2 位	VoIP	57.18 件	＋80.6%　（＋25.53 件）	1 位	
3 位	3 位	Scan(Password)	30.36 件	＋44.8%　（＋9.39 件）	2 位	
4 位	4 位	DNS	13.10 件	＋2.6%　（＋0.33 件）	4 位	
5 位	5 位	ICMP	11.19 件	＋7.8%　（＋0.81 件）	3 位	

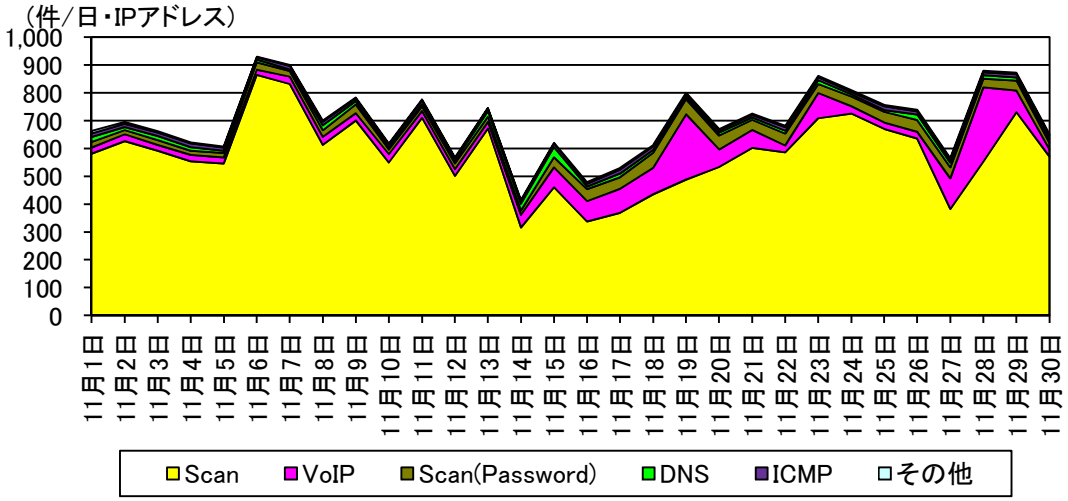

図 3-1　不正侵入等の攻撃手法別検知件数の推移

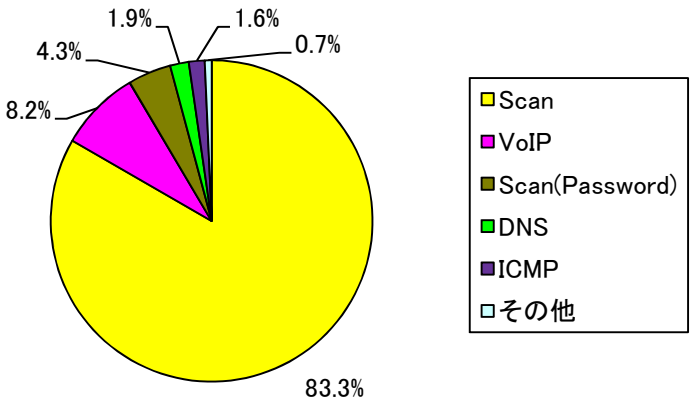

図 3-2　不正侵入等の攻撃手法別検知比率

[i] 一日・1IP アドレス当たり。

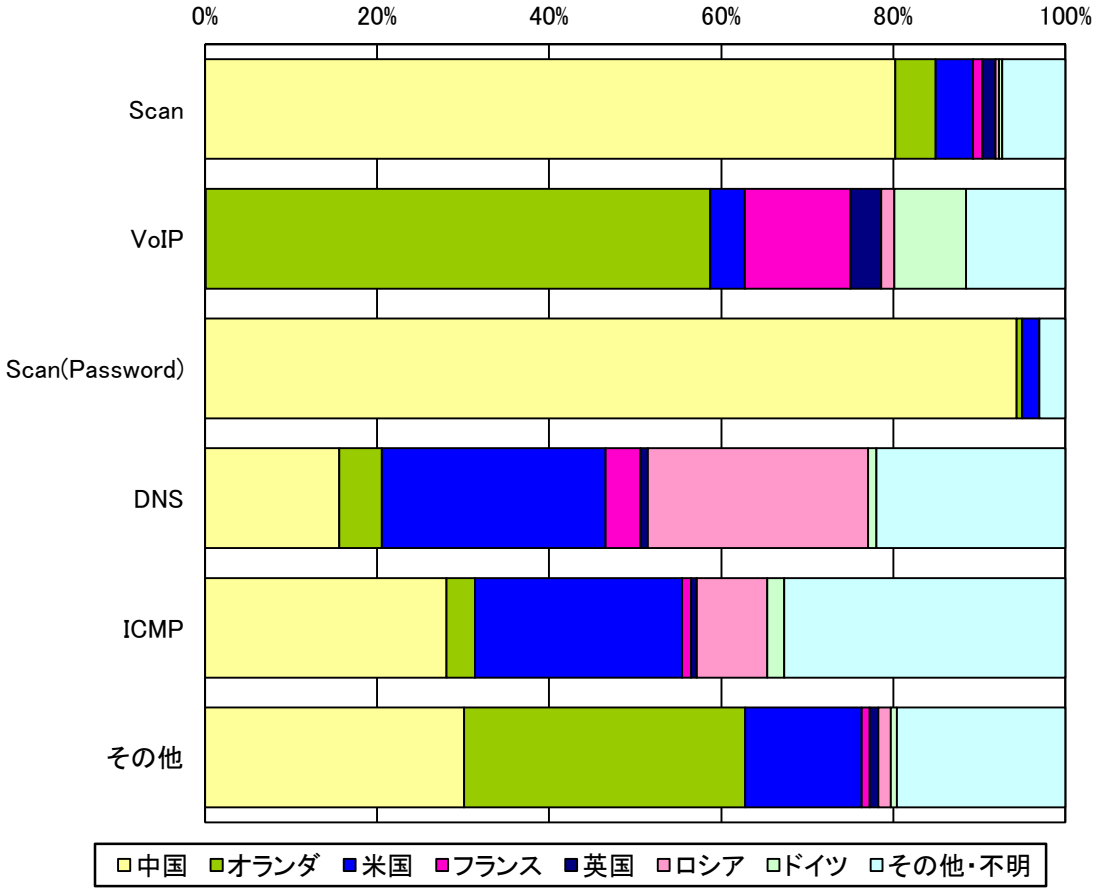

図 3-3 不正侵入等の攻撃手法の国・地域別検知比率

3-2 発信元国・地域別

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	中国	502.32 件	－2.7% （－14.09 件）
2 位	2 位	オランダ	63.55 件	＋45.6% （＋19.90 件）
3 位	3 位	米国	35.18 件	－13.9% （－5.68 件）
4 位	4 位	フランス	13.89 件	－5.7% （－0.84 件）
5 位	5 位	英国	11.16 件	－1.4% （－0.16 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	オランダ	63.55 件	＋45.6% （＋19.90 件）	2 位	2 位
2 位	ベネズエラ	2.43 件	＋590.6% （＋2.08 件）	15 位	37 位
3 位	ドイツ	7.47 件	＋23.4% （＋1.42 件）	7 位	10 位
4 位	日本	2.10 件	＋81.7% （＋0.94 件）	16 位	29 位
5 位	リトアニア	0.77 件	＋123.0% （＋0.43 件）	29 位	39 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	中国	502.32 件	－2.7% （－14.09 件）	1 位	1 位
2 位	米国	35.18 件	－13.9% （－5.68 件）	3 位	3 位
3 位	ベトナム	3.14 件	－57.7% （－4.29 件）	13 位	7 位
4 位	ロシア	7.58 件	－30.9% （－3.38 件）	6 位	6 位
5 位	ウクライナ	1.18 件	－70.5% （－2.83 件）	23 位	13 位

[i] 一日・1IP アドレス当たり。

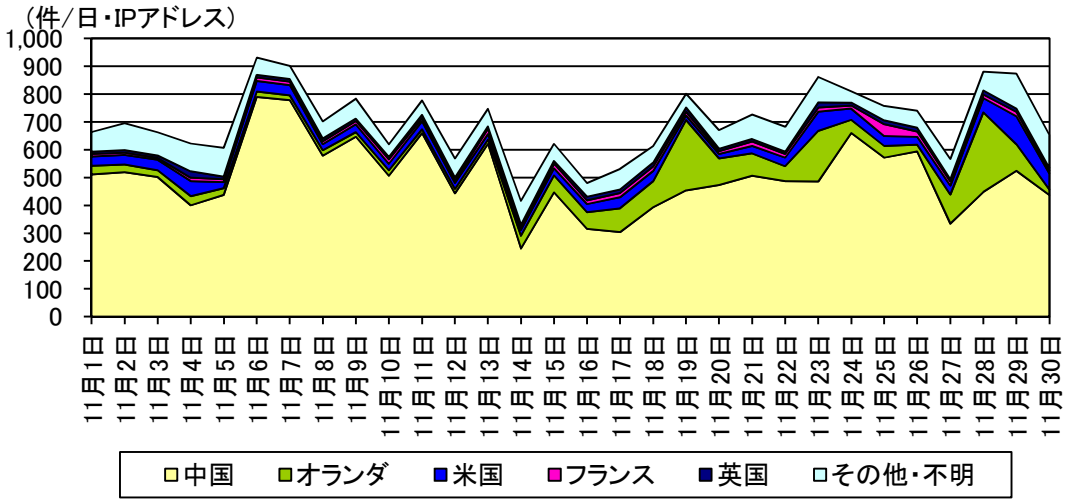

図 3-4　不正侵入等の発信元国・地域別検知件数の推移

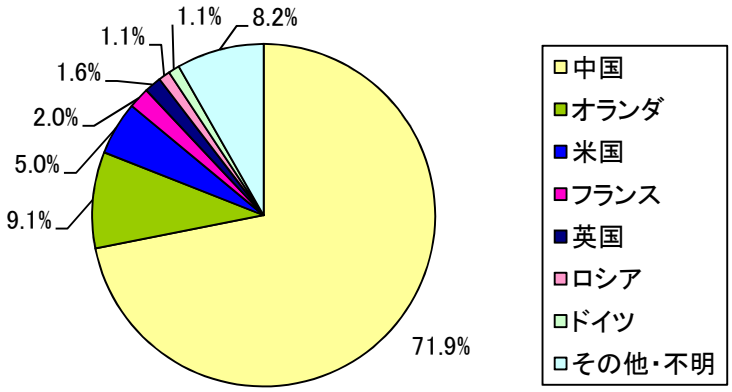

図 3-5　不正侵入等の発信元国・地域別検知比率

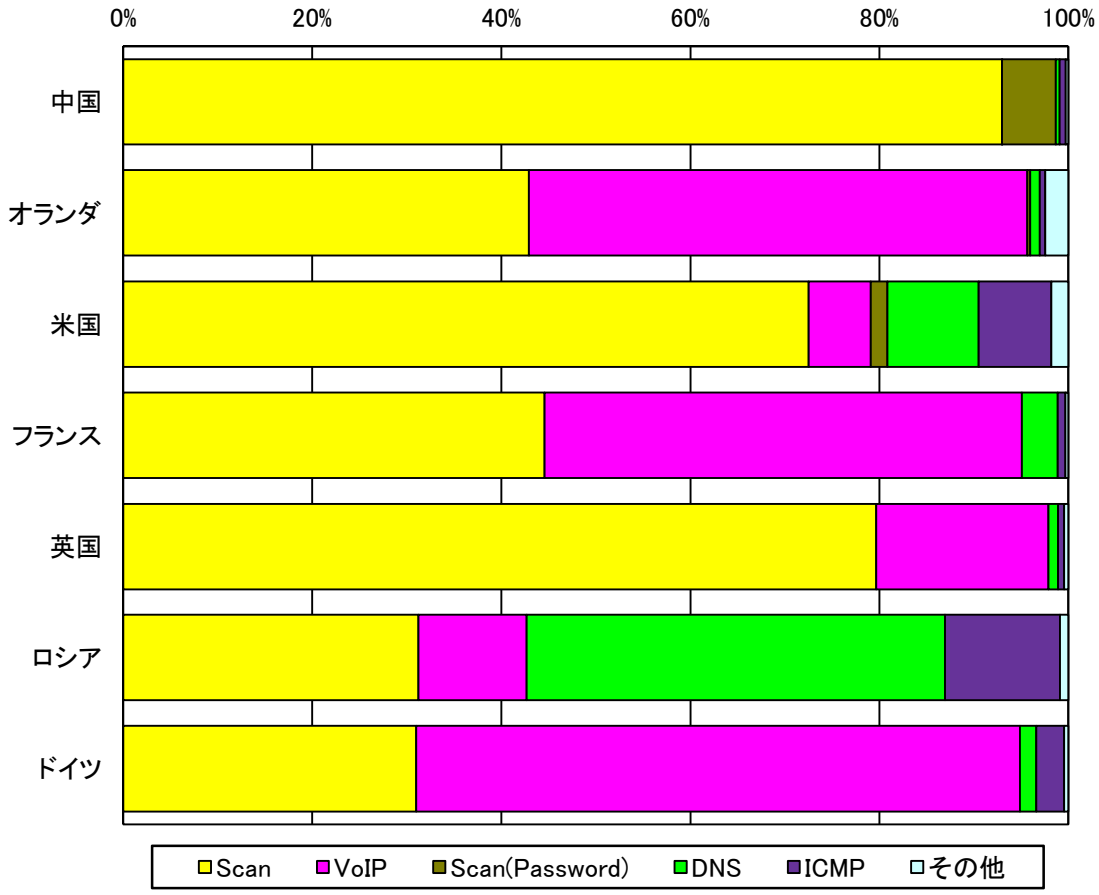

図 3-6 不正侵入等の発信元国・地域別上位の攻撃手法別検知比率

4　インターネット定点観測 ― DoS 攻撃被害観測状況

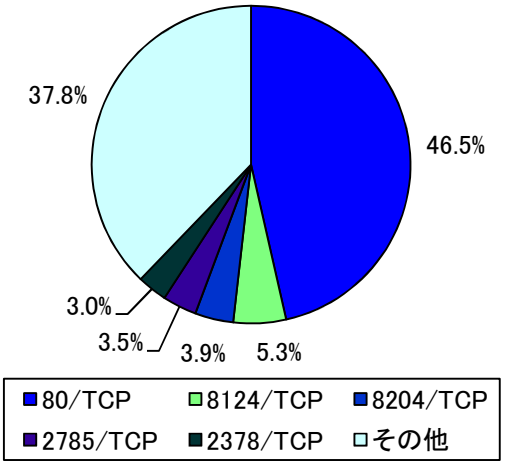

図 4-1　跳ね返りパケット発信元ポート別比率

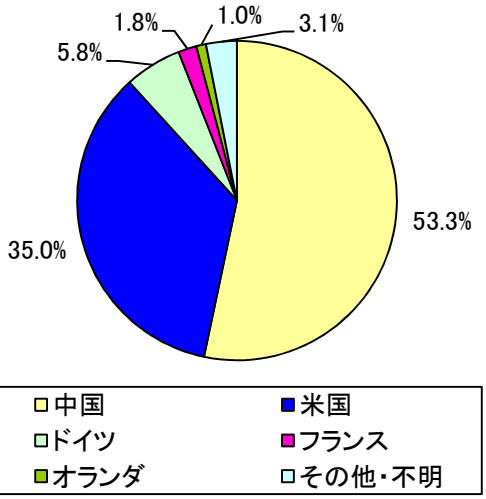

図 4-2　跳ね返りパケット発信元国・地域別比率

5　集計方法

警察庁では、インターネット定点観測システムにより、全国のインターネット接続点におけるアクセス情報等を観測・分析しています。各観測結果の集計については、次のとおり行っています。

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

インターネット定点観測システムが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 攻撃被害観測システムでは、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 インターネット定点観測 － センサーに対するアクセス	センサーに対するアクセス	● 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 インターネット定点観測 － DoS 攻撃被害観測状況	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計しています。

また、各センサーには、サーバ等の攻撃対象となる可能性のある機器を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

6　代表的なポート番号

アクセス件数が多い代表的なポート番号の概要は表 6-1 のとおりです。ただし各ポート番号は、定められた目的以外においても利用されることがあります。

表 6-1　代表的なポート番号の概要

ポート番号	概要
8/ICMP	本資料においては、ネットワークの疎通確認に用いる Ping 等に使用される ICMP Echo Request を表します。
22/TCP	SSH に使用されるポート。コンピュータのみに留まらず、多くのネットワーク接続機器においても使用されます。
23/TCP	Telnet に使用されるポート。コンピュータのみに留まらず、多くのネットワーク接続機器においても使用されます。
25/TCP	メール転送に用いる SMTP で使用されるポート。
53/UDP 53/TCP	DNS に使用されるポート。
80/TCP	HTTP に使用されるポート。
110/TCP	メール受信に用いる POP3 で使用されるポート。
135/TCP 135/UDP	ネットワークを経由したプログラム呼び出し（RPC）に使用されるポートであり、主に Microsoft Windows において使用されます。
137/TCP 137/UDP	Microsoft Windows の名前解決（NETBIOS）に使用されるポート。
139/TCP 139/UDP	Microsoft Windows のファイル共有（NETBIOS）に使用されるポート。
445/TCP 445/UDP	Microsoft Windows のファイル共有（Microsoft DS）や集中管理（Active Directory）に使用されるポート。Microsoft Windows の脆弱性（MS08-067）を悪用する Conficker ワームの感染活動にも使用されます。
1433/TCP	Microsoft SQL Server の管理や操作に使用されるポート。
3306/TCP	MySQL の管理や操作に使用されるポート。
3389/TCP	Microsoft Windows のリモートデスクトップ接続（RDP）に使用されるポート。
8080/TCP	HTTP に使用されるポート。HTTP プロキシで使用されることも多いです。