令和元年10月2日

# 令和元年7月期観測資料

## 1　観測結果概要

令和元年7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 3,888.0 件で、令和元年6月期（以下「前期」という。）と比較して 160.8 件（4.3%）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 46,169.7 個で、前期と比較して 5,280.8 個（12.9%）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 671.9 件で、前期と比較して 8.4 件（1.3%）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 8,015.6 個で、前期と比較して 356.3 個（4.7%）増加しました。

DoS 攻撃被害検知件数は、一日当たり 7,775.3 件で、前期と比較して 3,348.5 件（75.6%）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 234.8 個で、前期と比較して 18.6 個（7.3%）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 | 441.76 件 | −23.1% | （−132.75 件） |
| 2 位 | 2 位 | 445/TCP | 394.17 件 | −0.1% | （−0.22 件） |
| 3 位 | 3 位 | 22/TCP | 90.09 件 | ＋8.2% | （＋6.81 件） |
| 4 位 | 4 位 | 37215/TCP | 83.25 件 | ＋13.7% | （＋10.06 件） |
| 5 位 | 5 位 | 80/TCP | 59.74 件 | ＋11.2% | （＋6.03 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 | 8545/TCP | 45.48 件 | ＋51.7% | （＋15.49 件） | 7 位 | 14 位 |
| 2 位 | 8291/TCP | 33.16 件 | ＋67.1% | （＋13.32 件） | 12 位 | 17 位 |
| 3 位 | 9527/TCP | 19.31 件 | ＋190.2% | （＋12.66 件） | 24 位 | 38 位 |
| 4 位 | 37215/TCP | 83.25 件 | ＋13.7% | （＋10.06 件） | 4 位 | 4 位 |
| 5 位 | 2323/TCP | 27.15 件 | ＋55.2% | （＋9.65 件） | 15 位 | 20 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 | 441.76 件 | −23.1% | （−132.75 件） | 1 位 | 1 位 |
| 2 位 | 5500/TCP | 16.39 件 | −46.2% | （−14.08 件） | 25 位 | 13 位 |
| 3 位 | 5555/TCP | 29.14 件 | −23.6% | （−8.99 件） | 13 位 | 9 位 |
| 4 位 | 5038/TCP | 26.57 件 | −16.1% | （−5.09 件） | 16 位 | 12 位 |
| 5 位 | 0/TCP | − [ii] | − [ii] | （−3.40 件） | − [ii] | 58 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、今期件数、前期比及び今期順位は記載していません。

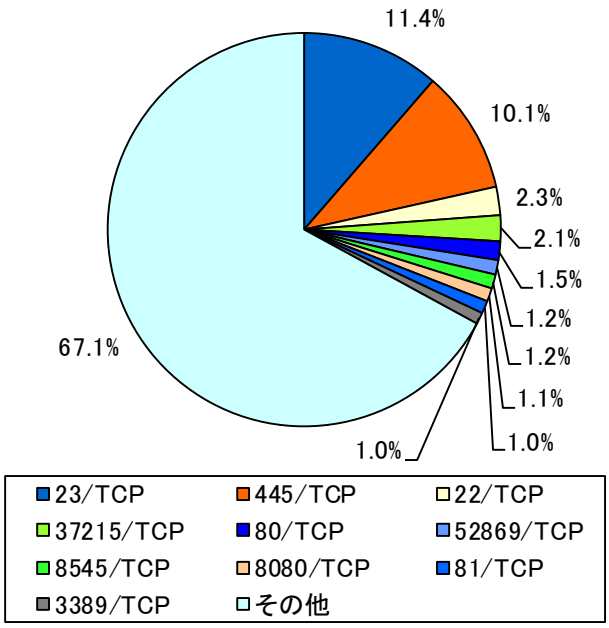


図 2-1　宛先ポート別比率（全て）[i]

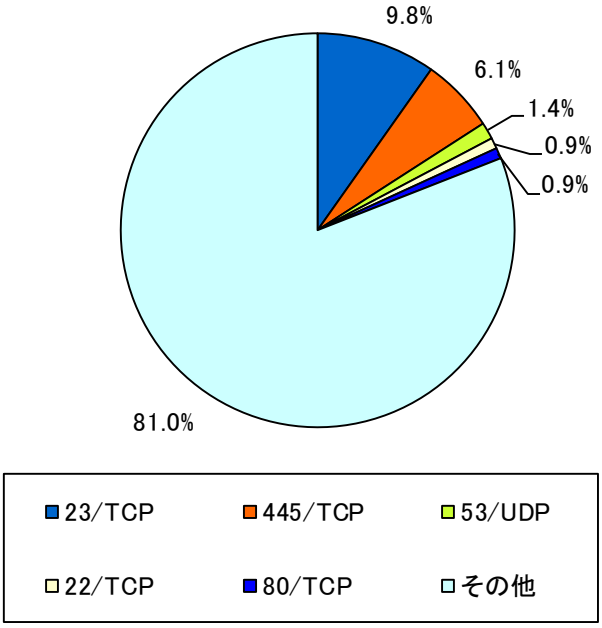


図 2-2　宛先ポート別比率（日本国内）

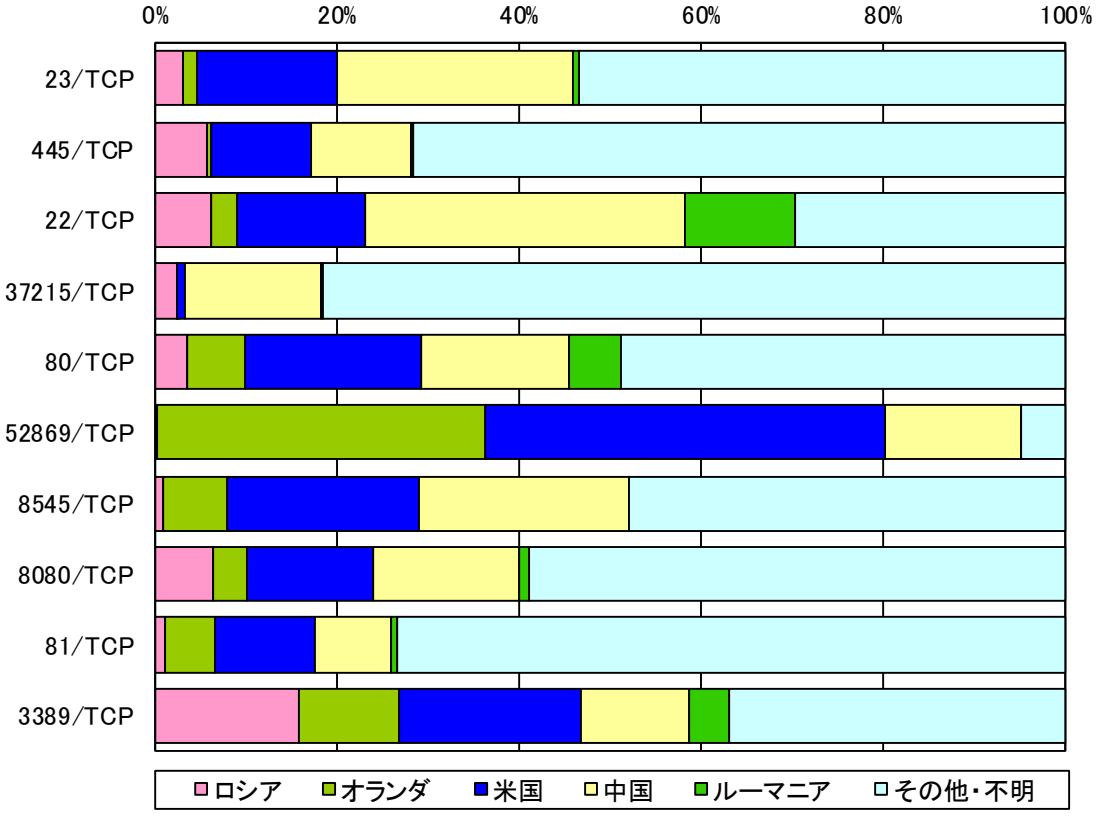


図 2-3　宛先ポート別上位の着信元国・地域別比率 [ii]

[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。

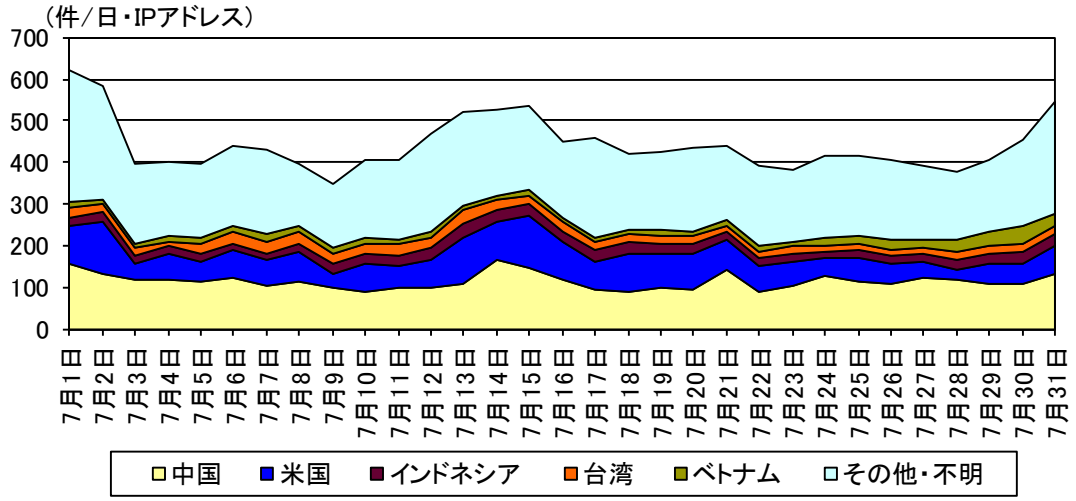


図 2-4　センサーのポート 23/TCP における検知件数の推移

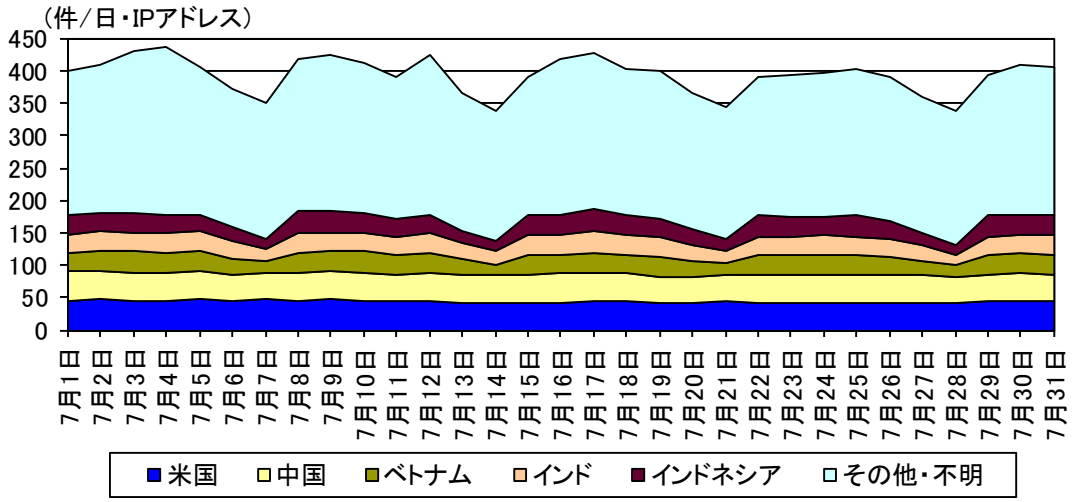


図 2-5　センサーのポート 445/TCP における検知件数の推移

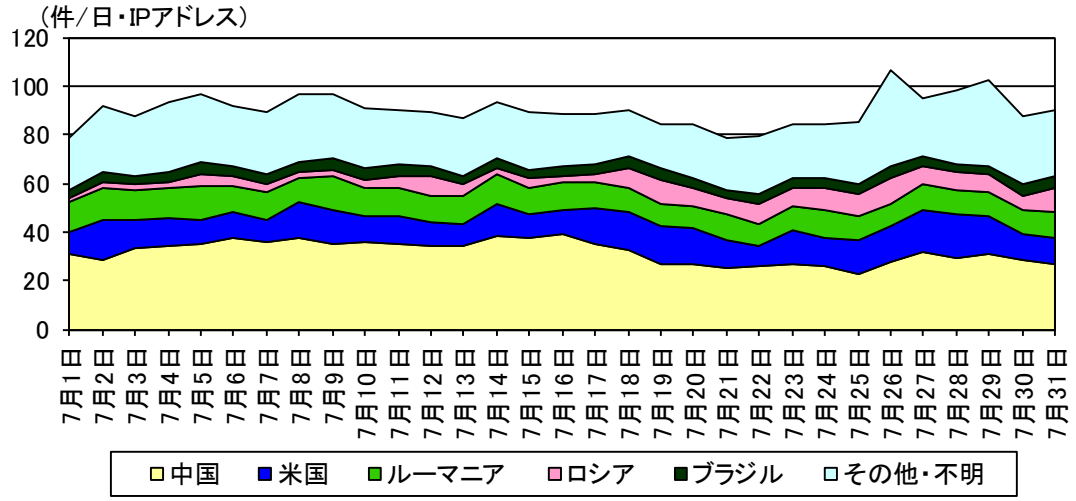


図 2-6　センサーのポート 22/TCP における検知件数の推移

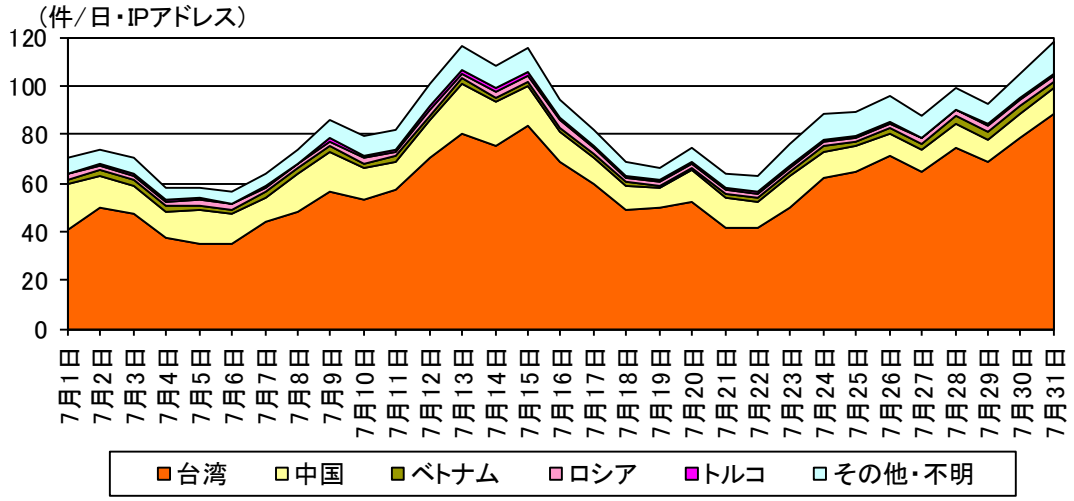


図 2-7　センサーのポート 37215/TCP における検知件数の推移

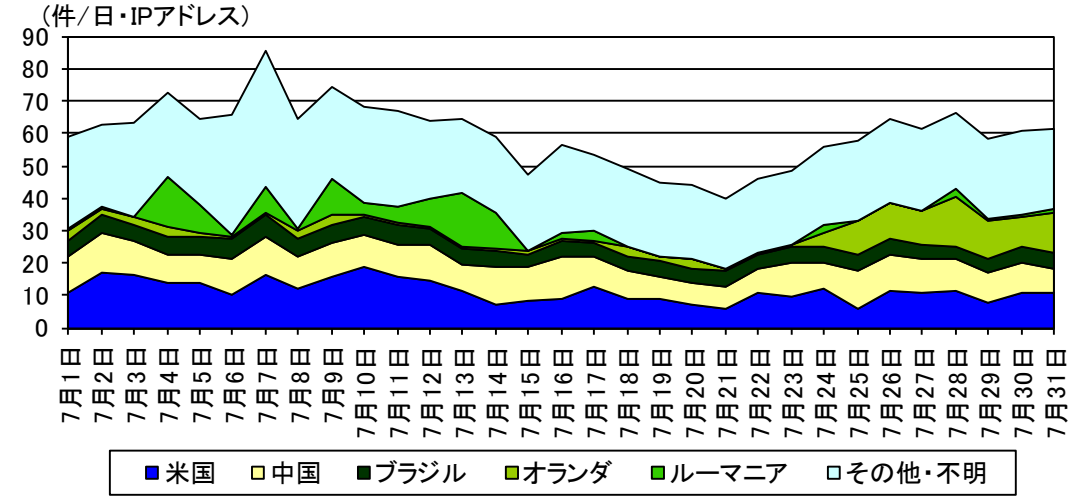


図 2-8　センサーのポート 80/TCP における検知件数の推移

## 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 | 1 位 | ロシア | 694.19 件 | －10.3% | （－79.84 件） |
| 2 位 | 4 位 | オランダ | 687.49 件 | ＋88.3% | （＋322.44 件） |
| 3 位 | 2 位 | 米国 | 582.03 件 | －12.2% | （－80.59 件） |
| 4 位 | 3 位 | 中国 | 499.34 件 | ＋20.0% | （＋83.25 件） |
| 5 位 | 8 位 | ルーマニア | 126.67 件 | ＋39.2% | （＋35.64 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 | 687.49 件 | ＋88.3% | （＋322.44 件） | 2 位 | 4 位 |
| 2 位 | 中国 | 499.34 件 | ＋20.0% | （＋83.25 件） | 4 位 | 3 位 |
| 3 位 | ルーマニア | 126.67 件 | ＋39.2% | （＋35.64 件） | 5 位 | 8 位 |
| 4 位 | インドネシア | 108.68 件 | ＋40.9% | （＋31.56 件） | 7 位 | 10 位 |
| 5 位 | スペイン | 34.99 件 | ＋528.8% | （＋29.42 件） | 16 位 | 45 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 | 日本 | 39.71 件 | －78.3% | （－143.47 件） | 15 位 | 5 位 |
| 2 位 | 米国 | 582.03 件 | －12.2% | （－80.59 件） | 3 位 | 2 位 |
| 3 位 | ロシア | 694.19 件 | －10.3% | （－79.84 件） | 1 位 | 1 位 |
| 4 位 | 香港 | 29.28 件 | －62.5% | （－48.83 件） | 18 位 | 9 位 |
| 5 位 | ドイツ | 25.27 件 | －58.0% | （－34.88 件） | 20 位 | 11 位 |

[i] 一日・1IP アドレス当たり。

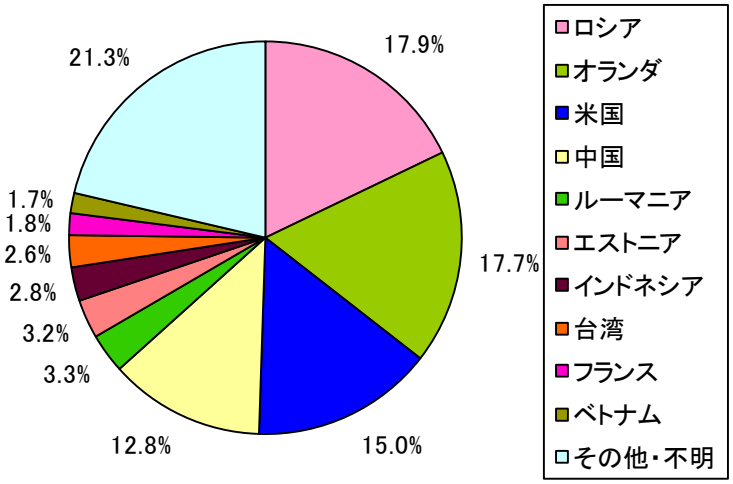


図 2-9　着信元国・地域別比率

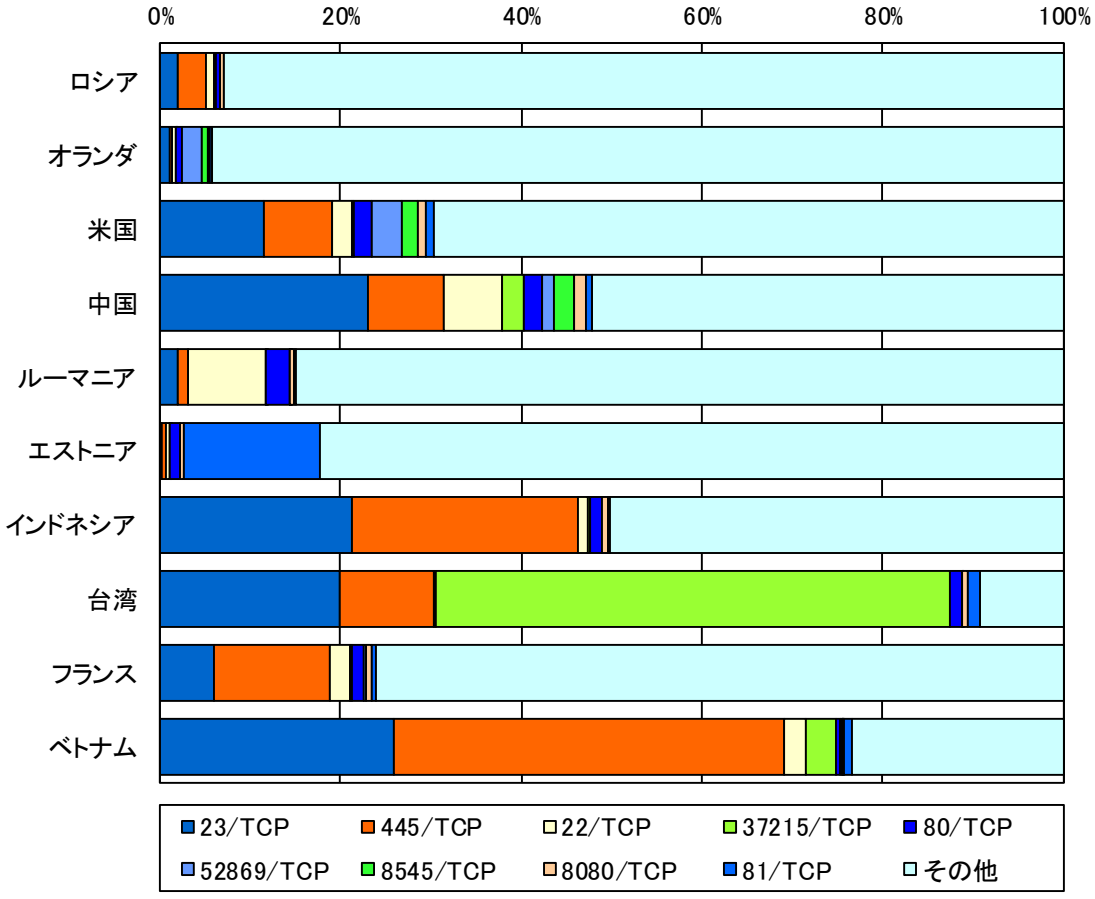


図 2-10　着信元国・地域別上位の宛先ポート別比率

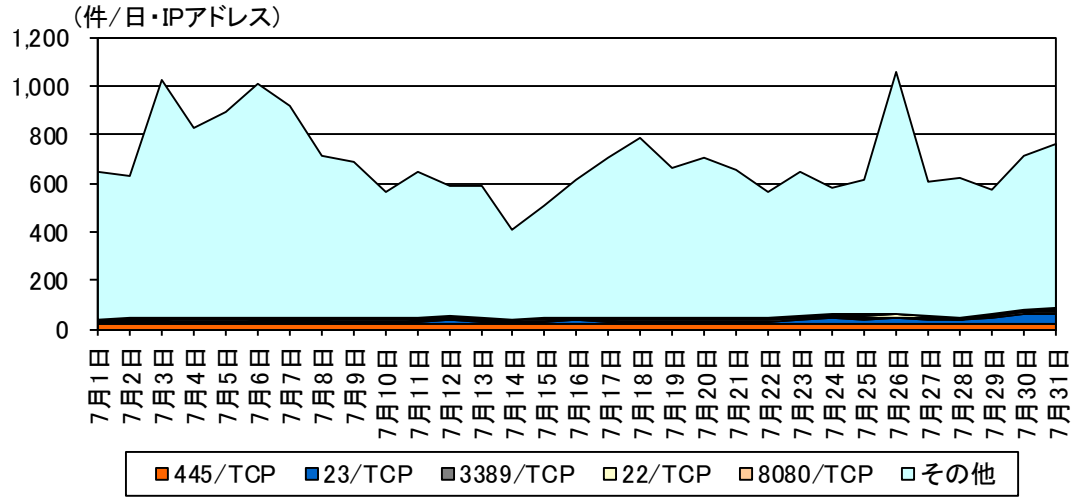


図 2-11　ロシアからの検知件数の推移

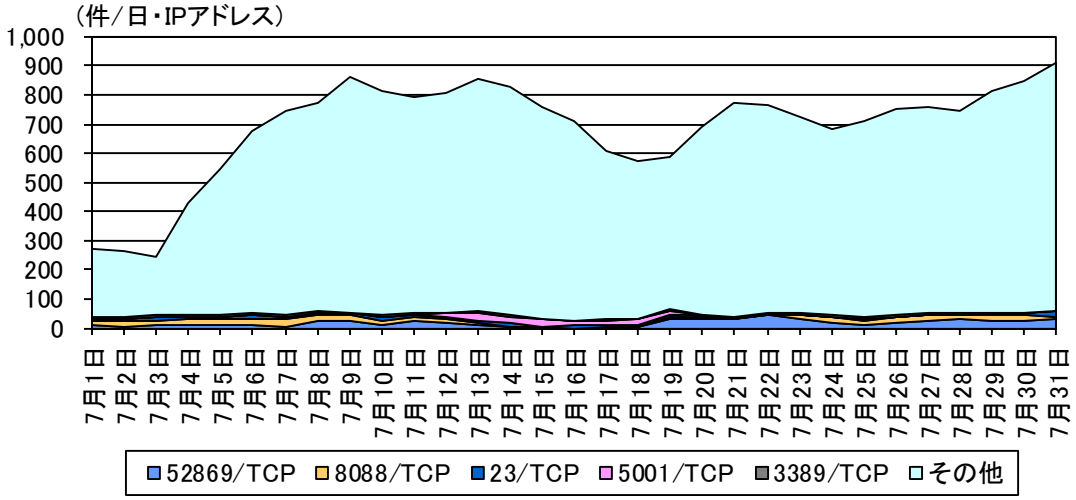


図 2-12　オランダからの検知件数の推移

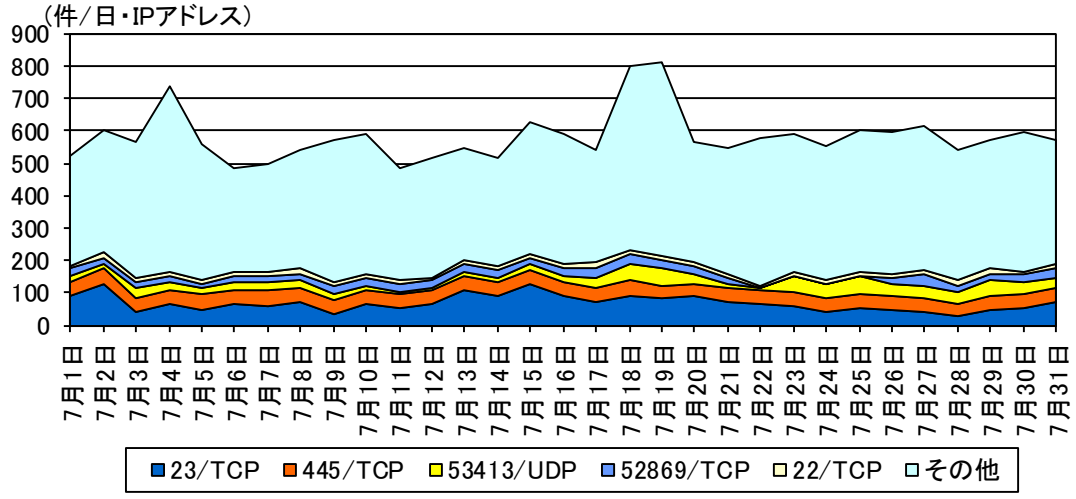


図 2-13　米国からの検知件数の推移

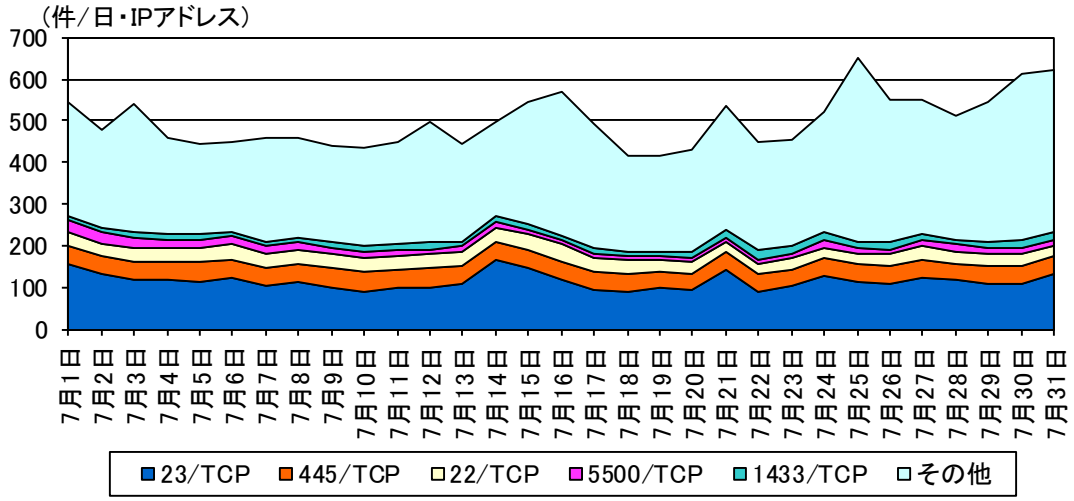


図 2-14　中国からの検知件数の推移

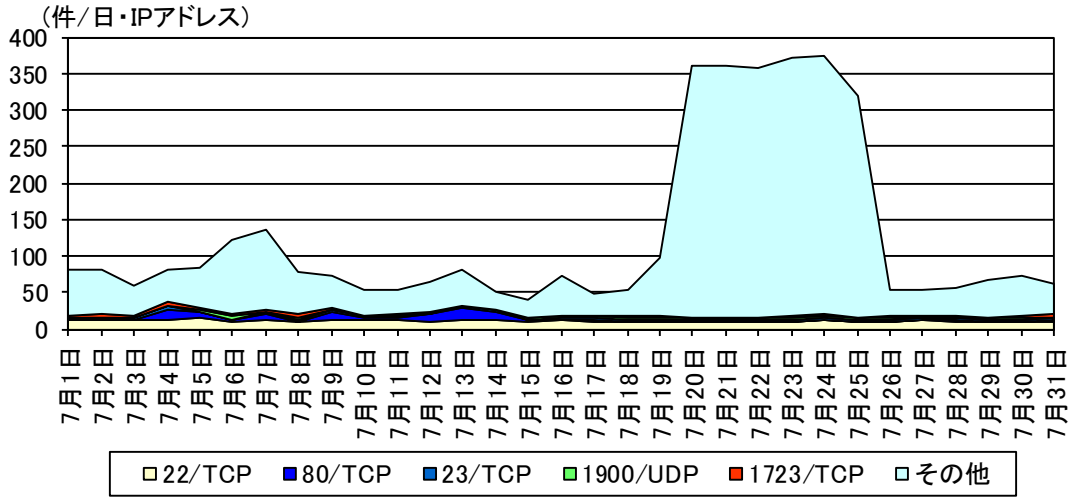


図 2-15　ルーマニアからの検知件数の推移

## 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 | 236.31 件 | ＋0.0%　（＋0.05 件） | | |
| 2 位 | 2 位 | Microsoft Windows Terminal server | 157.69 件 | －12.7%　（－23.03 件） | | 1 位 |
| 3 位 | 3 位 | SMBv1 | 133.47 件 | ＋6.6%　（＋8.28 件） | 2 位 | |
| 4 位 | 4 位 | VOIP | 43.67 件 | ＋32.2%　（＋10.64 件） | 1 位 | |
| 5 位 | 5 位 | ICMP | 21.12 件 | ＋16.9%　（＋3.05 件） | 3 位 | |

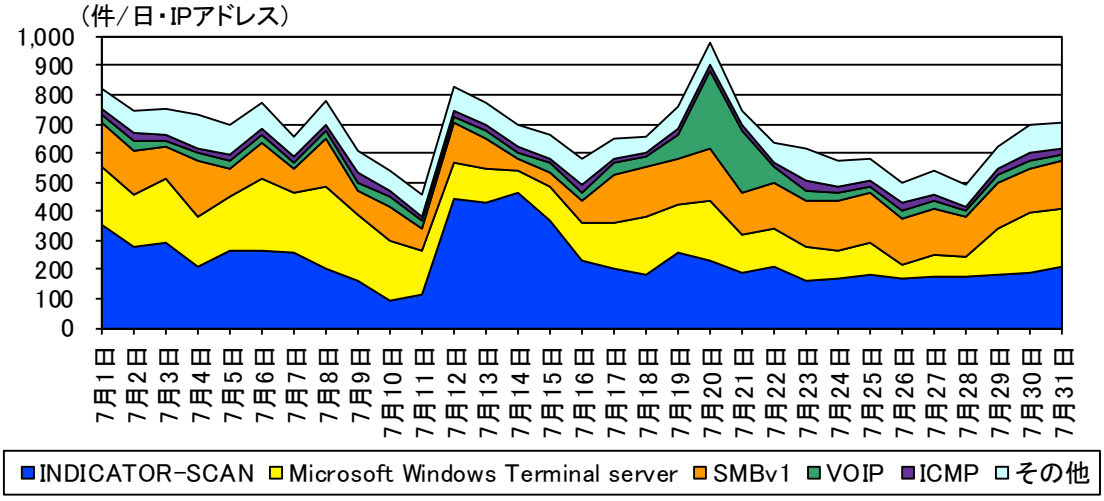


図 3-1　不正侵入等の攻撃手法別検知件数の推移

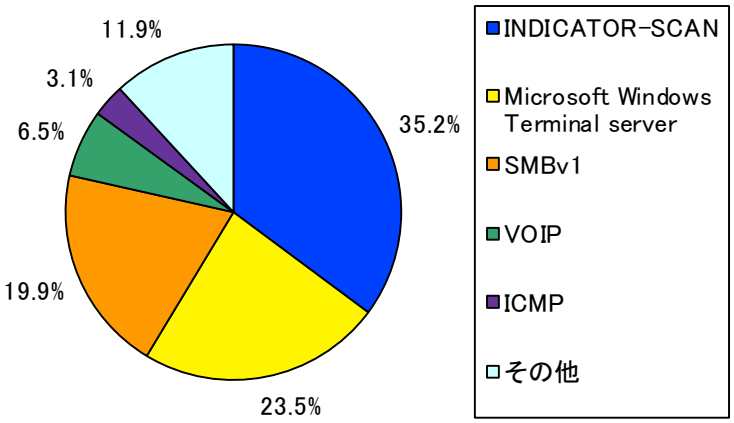


図 3-2　不正侵入等の攻撃手法別検知比率

[i] 一日・1IP アドレス当たり。

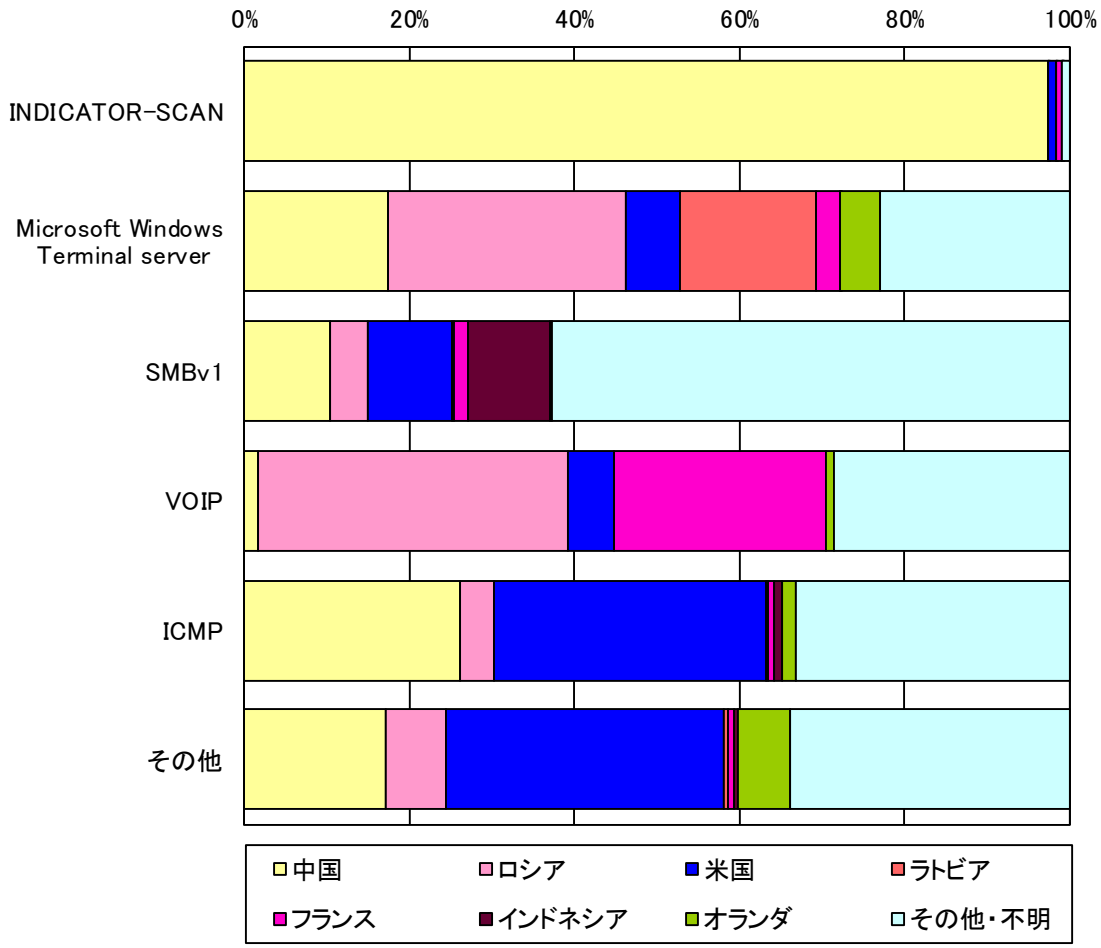


図 3-3　不正侵入等の攻撃手法の国・地域別検知比率

### 3-2 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 | 291.37 件 | ＋4.2% | （＋11.87 件） |
| 2 位 | 3 位 | ロシア | 74.94 件 | ＋37.5% | （＋20.45 件） |
| 3 位 | 2 位 | 米国 | 61.98 件 | －14.4% | （－10.45 件） |
| 4 位 | 4 位 | ラトビア | 26.79 件 | －17.6% | （－5.73 件） |
| 5 位 | 5 位 | フランス | 20.28 件 | ＋14.4% | （＋2.56 件） |

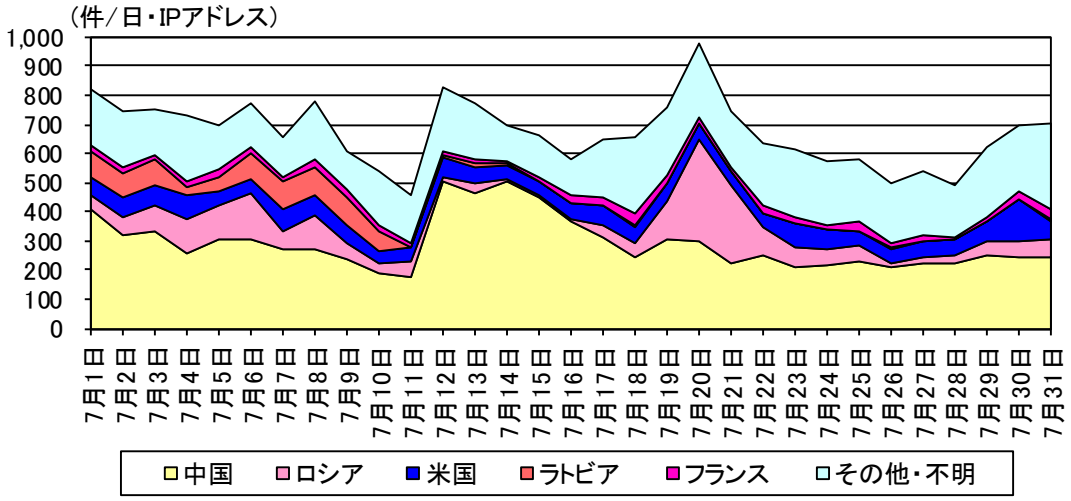


図 3-4 不正侵入等の着信元国・地域別検知件数の推移

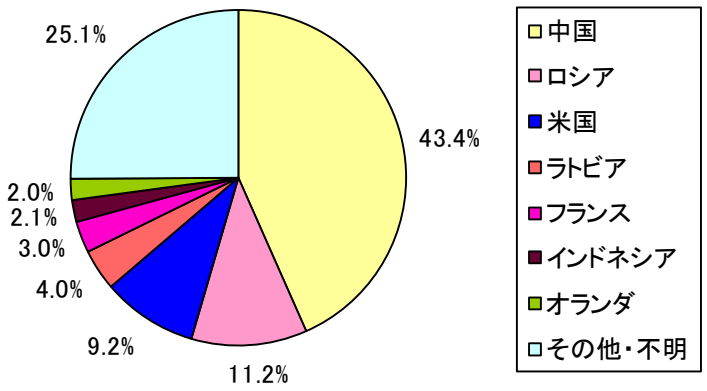


図 3-5 不正侵入等の着信元国・地域別検知比率

[i] 一日・1IP アドレス当たり。

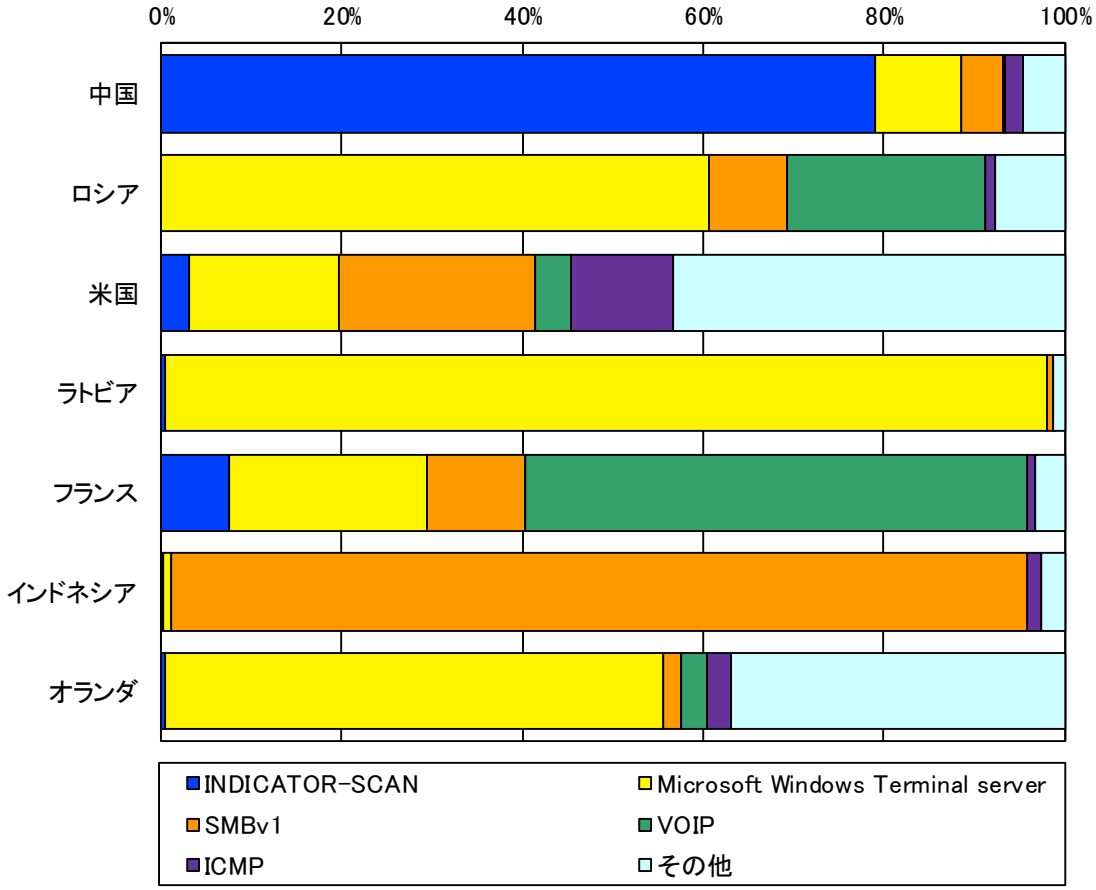


図 3-6 不正侵入等の着信元国・地域別上位の攻撃手法別検知比率

## 4　DoS 攻撃被害の観測結果

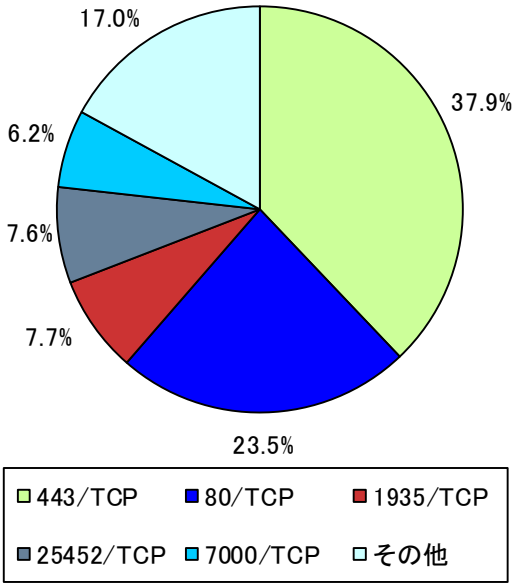


図 4-1　跳ね返りパケット着信元ポート別比率

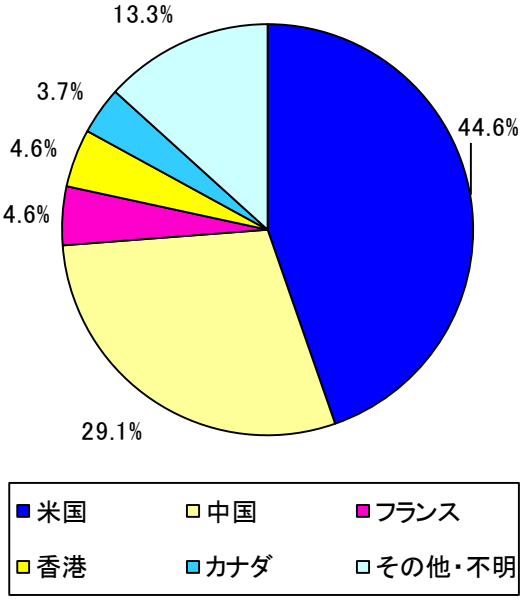


図 4-2　跳ね返りパケット着信元国・地域別比率

## 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<br>● UDP による問い合わせパケット等<br>● 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<br>● 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<br>● 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 |