令和元年12月25日

# 令和元年11月期観測資料

## 1　観測結果概要

令和元年11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5,030.8件で、令和元年10月期（以下「前期」という。）と比較して317.8件（6.7%）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52,859.9個で、前期と比較して2,837.8個（5.1%）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825.7件で、前期と比較して47.3件（6.1%）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6,660.9個で、前期と比較して806.2個（13.8%）増加しました。

DoS攻撃被害検知件数は、一日当たり6,869.0件で、前期と比較して1,653.2件（19.4%）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263.9個で、前期と比較して3,298.4個（92.6%）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 | 491.65 件 | ＋17.2%　（＋72.15 件） |
| 2 位 | 2 位 | 445/TCP | 259.03 件 | －15.4%　（－47.32 件） |
| 3 位 | 3 位 | 1433/TCP | 228.69 件 | ＋9.4%　（＋19.57 件） |
| 4 位 | 5 位 | 80/TCP | 105.93 件 | ＋56.1%　（＋38.08 件） |
| 5 位 | 6 位 | 8080/TCP | 62.51 件 | ＋11.0%　（＋6.19 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 | 491.65 件 | ＋17.2%　（＋72.15 件） | 1 位 | 1 位 |
| 2 位 | 80/TCP | 105.93 件 | ＋56.1%　（＋38.08 件） | 4 位 | 5 位 |
| 3 位 | 26/TCP | 32.85 件 | －[ii]　（＋30.97 件） | 15 位 | －[ii] |
| 4 位 | 9000/TCP | 33.88 件 | ＋385.0%　（＋26.90 件） | 14 位 | 52 位 |
| 5 位 | 4145/TCP | 27.11 件 | ＋421.1%　（＋21.91 件） | 19 位 | 62 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 | 259.03 件 | －15.4%　（－47.32 件） | 2 位 | 2 位 |
| 2 位 | 34567/TCP | 2.92 件 | －90.3%　（－27.08 件） | 112 位 | 13 位 |
| 3 位 | 3306/TCP | 10.22 件 | －65.6%　（－19.45 件） | 30 位 | 14 位 |
| 4 位 | 22/TCP | 57.89 件 | －20.1%　（－14.52 件） | 6 位 | 4 位 |
| 5 位 | 9001/TCP | 15.46 件 | －41.9%　（－11.14 件） | 25 位 | 19 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、前期比及び前期順位は記載していません。

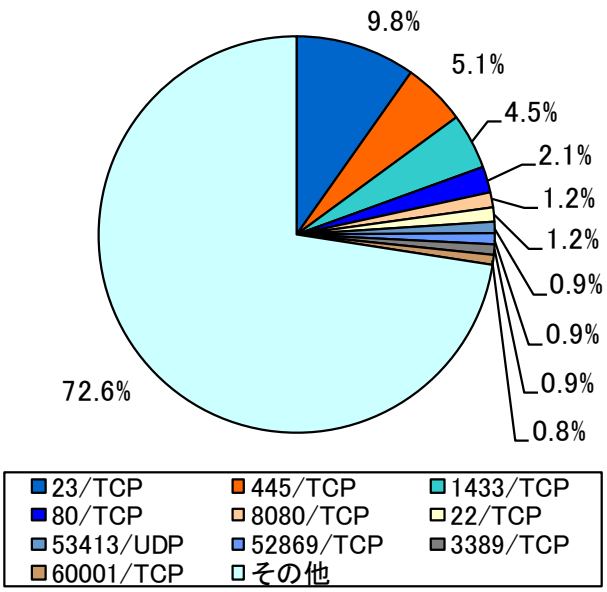


図 2-1　宛先ポート別比率（全て）[i]

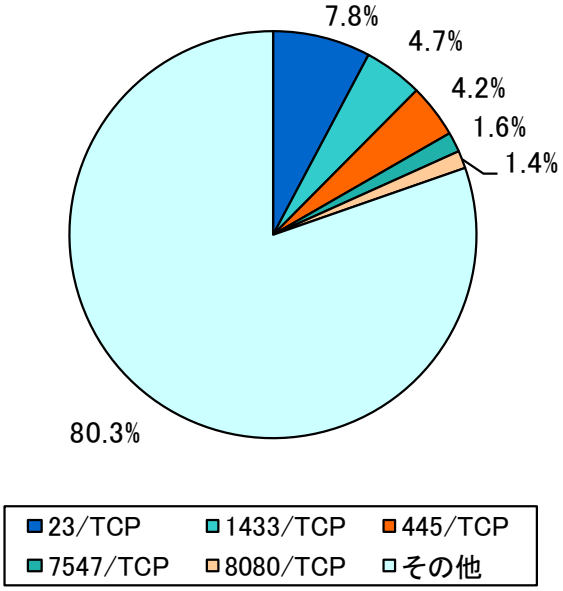


図 2-2　宛先ポート別比率（日本国内）

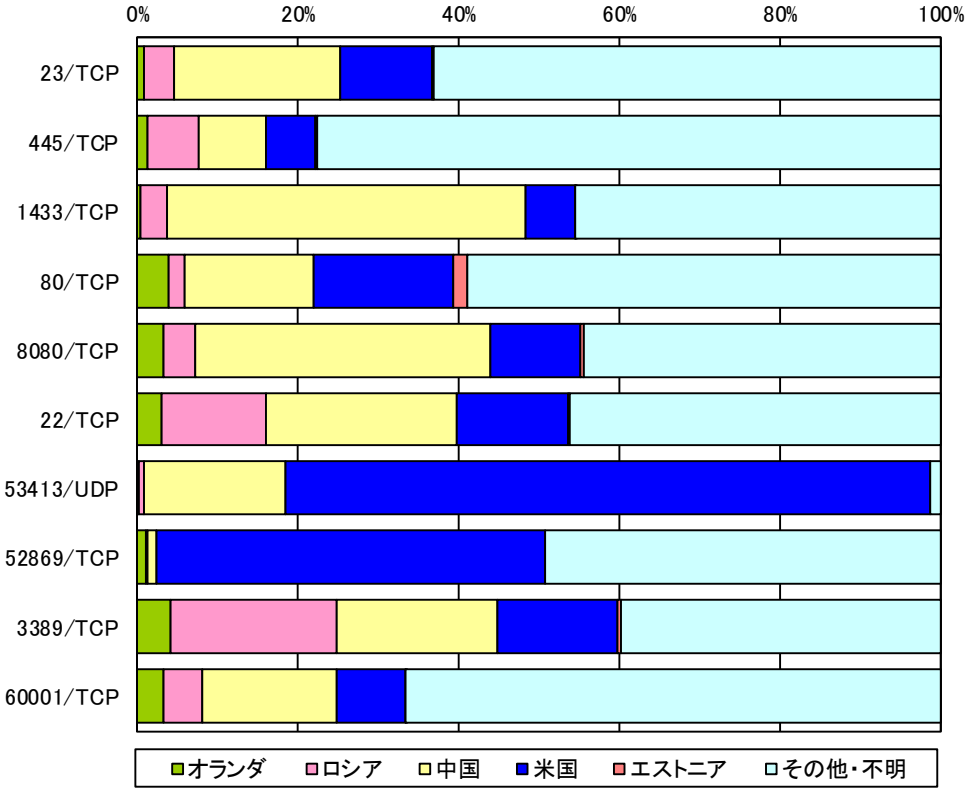


図 2-3　宛先ポート別上位の着信元国・地域別比率 [ii]

[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。

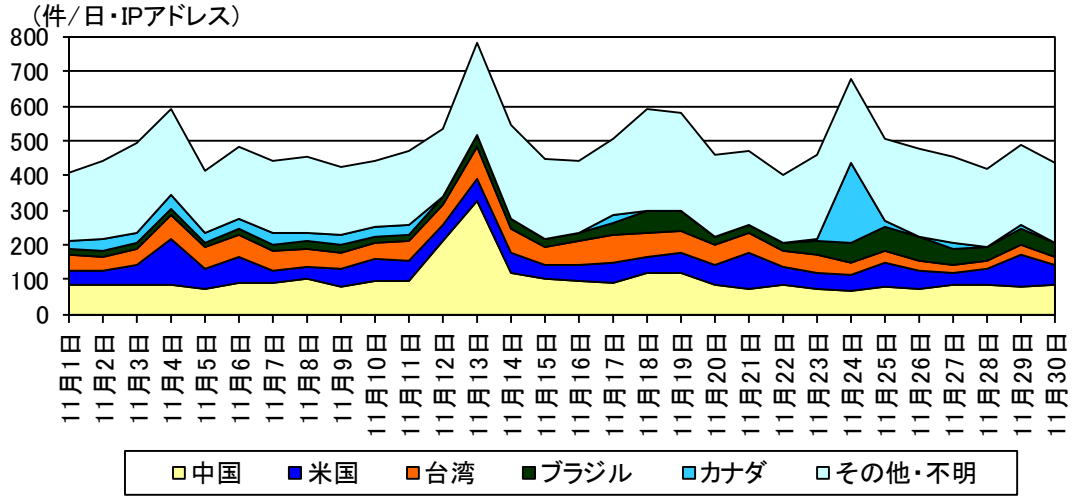


図 2-4　センサーのポート 23/TCP における検知件数の推移

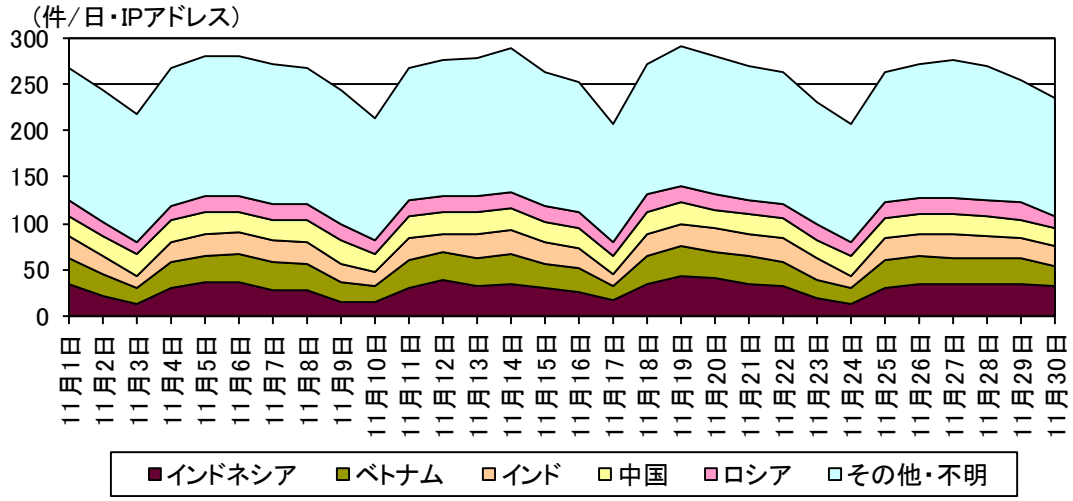


図 2-5　センサーのポート 445/TCP における検知件数の推移

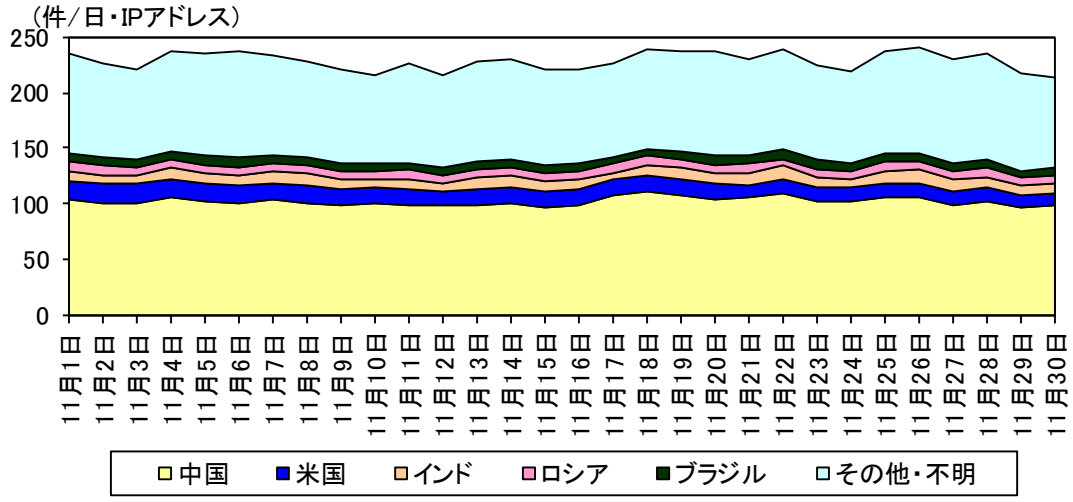


図 2-6　センサーのポート 1433/TCP における検知件数の推移

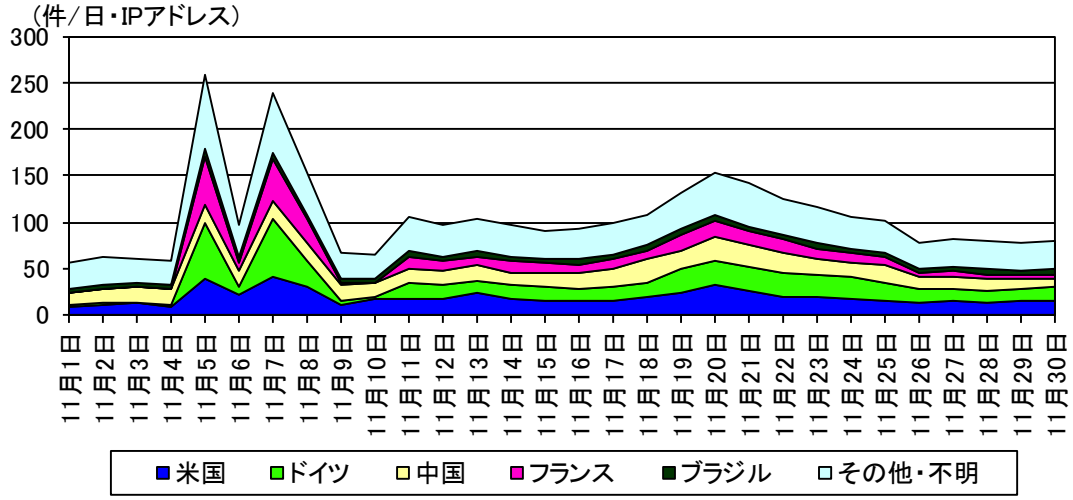


図 2-7　センサーのポート 80/TCP における検知件数の推移

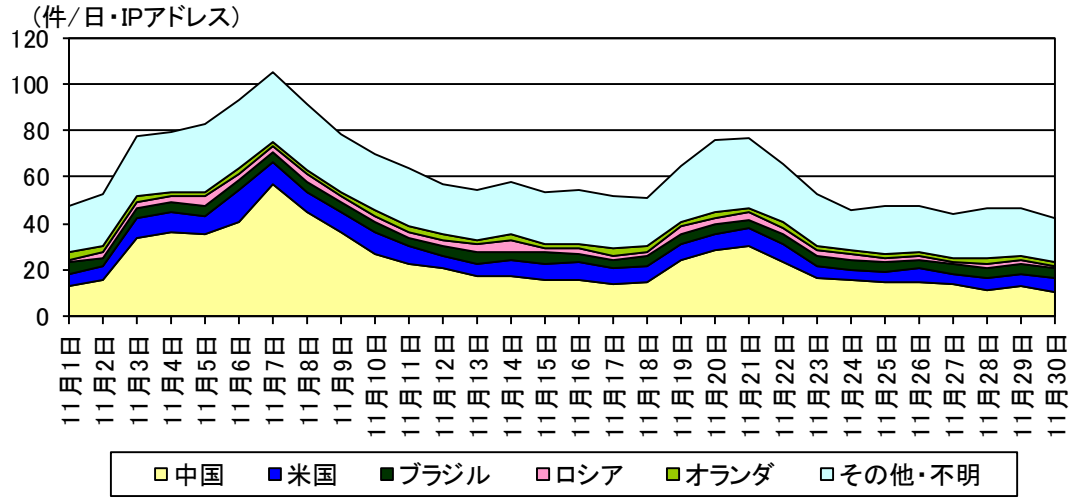


図 2-8　センサーのポート 8080/TCP における検知件数の推移

## 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 | オランダ | 1,229.95 件 | ＋23.0%　（＋229.63 件） |
| 2 位 | 2 位 | ロシア | 839.49 件 | －5.0%　（－43.83 件） |
| 3 位 | 3 位 | 中国 | 657.45 件 | ＋7.1%　（＋43.82 件） |
| 4 位 | 4 位 | 米国 | 574.69 件 | －1.1%　（－6.44 件） |
| 5 位 | 5 位 | エストニア | 127.30 件 | －1.4%　（－1.85 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 | 1,229.95 件 | ＋23.0%　（＋229.63 件） | 1 位 | 1 位 |
| 2 位 | 中国 | 657.45 件 | ＋7.1%　（＋43.82 件） | 3 位 | 3 位 |
| 3 位 | スイス | 40.90 件 | －[ii]　（＋39.71 件） | 21 位 | －[vi] |
| 4 位 | フランス | 102.21 件 | ＋35.0%　（＋26.51 件） | 9 位 | 10 位 |
| 5 位 | ブラジル | 91.75 件 | ＋37.7%　（＋25.14 件） | 10 位 | 12 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 | ロシア | 839.49 件 | －5.0%　（－43.83 件） | 2 位 | 2 位 |
| 2 位 | ラトビア | 7.37 件 | －72.5%　（－19.43 件） | 43 位 | 26 位 |
| 3 位 | 台湾 | 87.41 件 | －17.7%　（－18.85 件） | 11 位 | 8 位 |
| 4 位 | インドネシア | 115.79 件 | －9.2%　（－11.79 件） | 8 位 | 6 位 |
| 5 位 | ベトナム | 62.16 件 | －12.8%　（－9.13 件） | 13 位 | 11 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、前期比及び前期順位は記載していません。

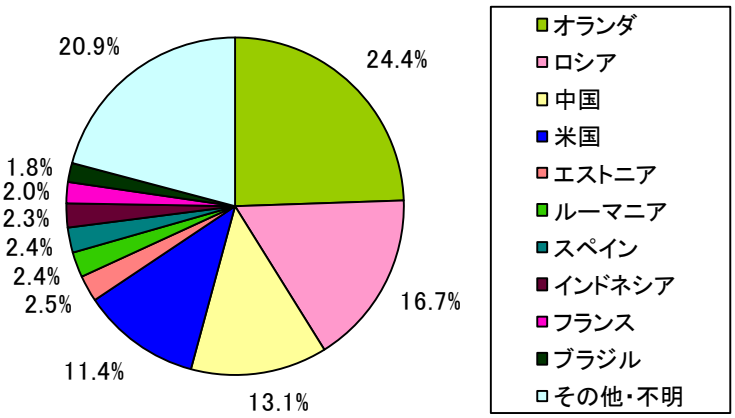


図 2-9　着信元国・地域別比率

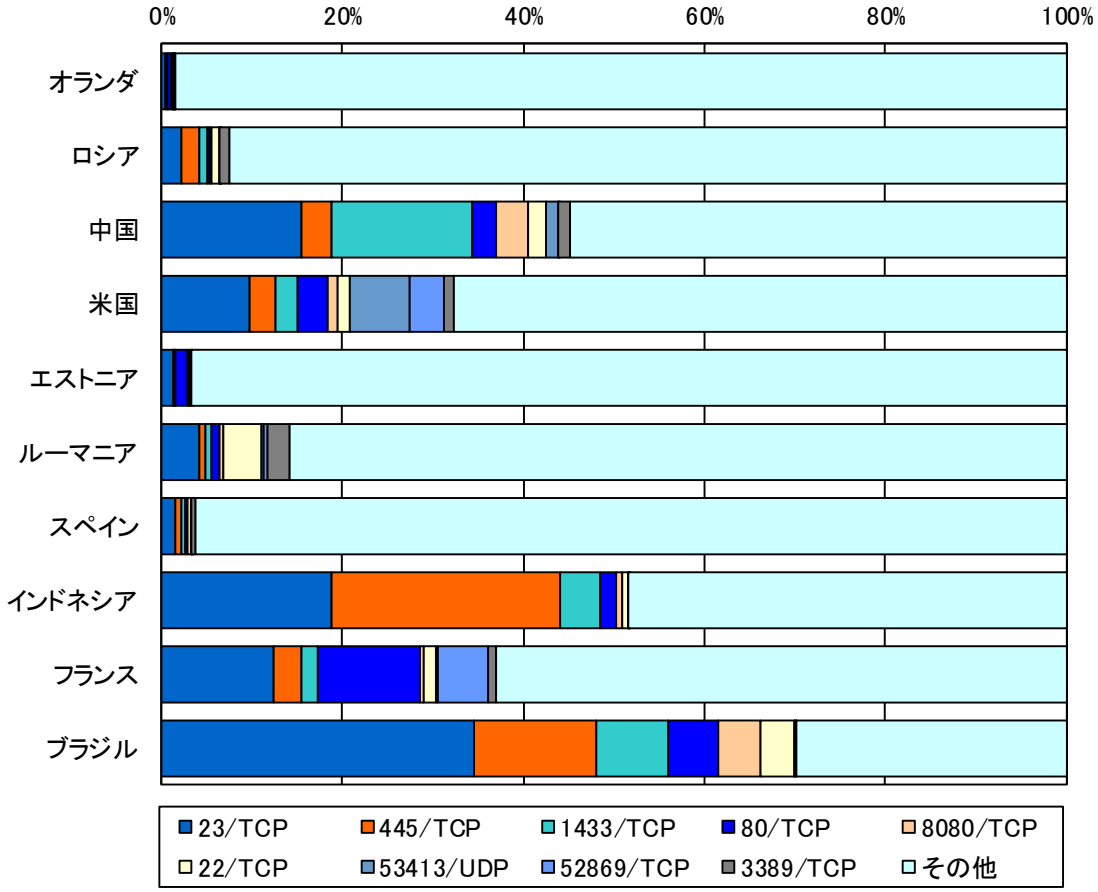


図 2-10　着信元国・地域別上位の宛先ポート別比率

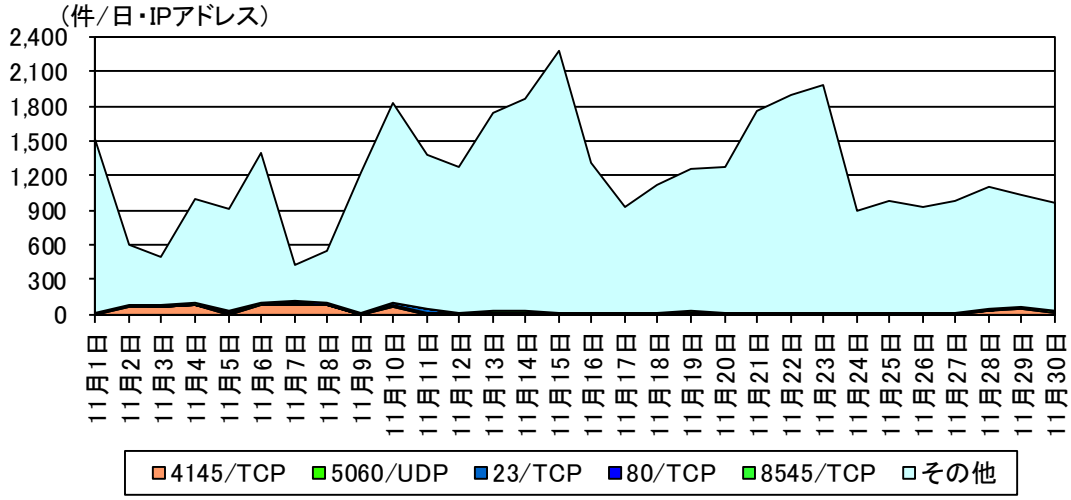


図 2-11　オランダからの検知件数の推移

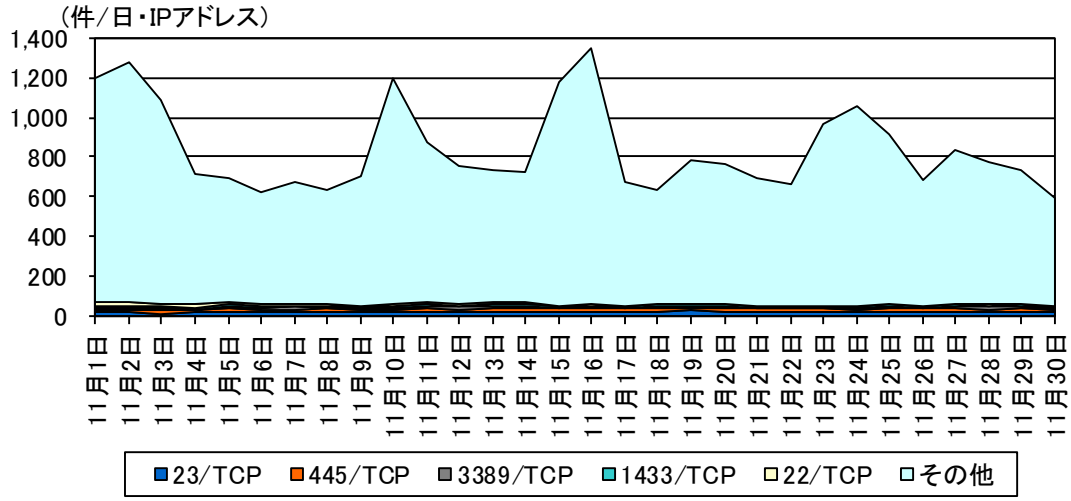


図 2-12　ロシアからの検知件数の推移

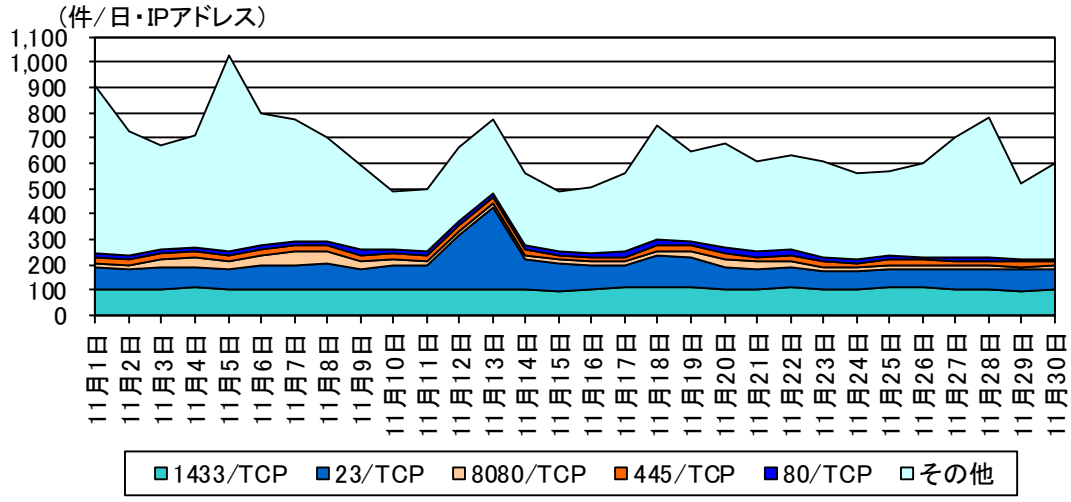


図 2-13　中国からの検知件数の推移

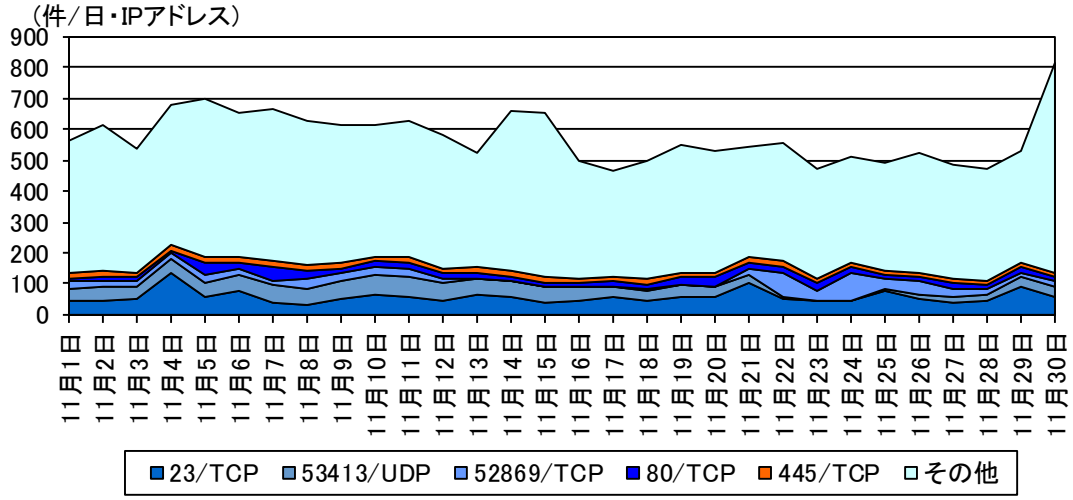


図 2-14　米国からの検知件数の推移

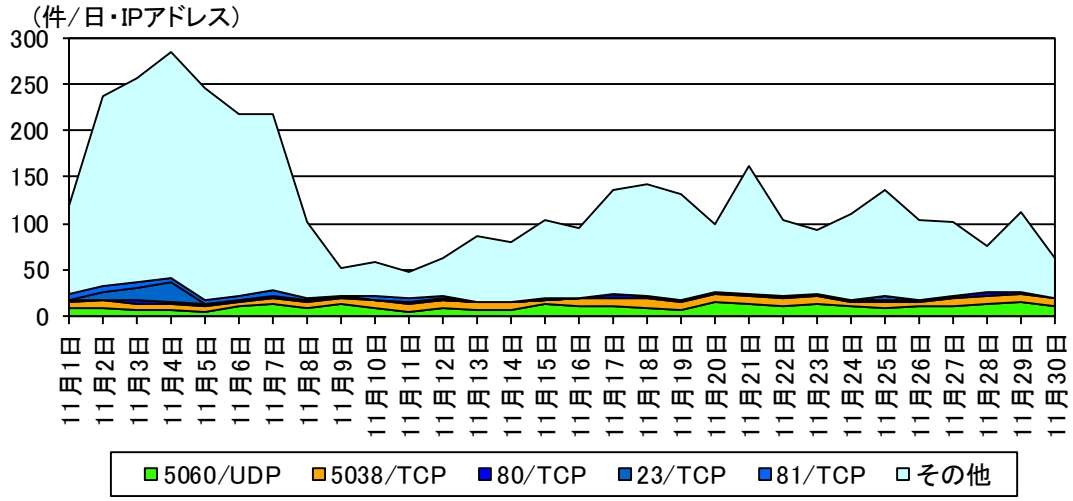


図 2-15　エストニアからの検知件数の推移

## 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 | 356.29 件 | ＋0.2%　（＋0.59 件） | | |
| 2 位 | 2 位 | Microsoft Windows Terminal server | 236.64 件 | ＋24.8%　（＋47.05 件） | 1 位 | |
| 3 位 | 3 位 | SMBv1 | 105.47 件 | ＋14.1%　（＋13.04 件） | 2 位 | |
| 4 位 | 4 位 | ICMP | 22.45 件 | －13.4%　（－3.49 件） | | 3 位 |
| 5 位 | 5 位 | VOIP | 14.19 件 | －37.5%　（－8.51 件） | | 2 位 |

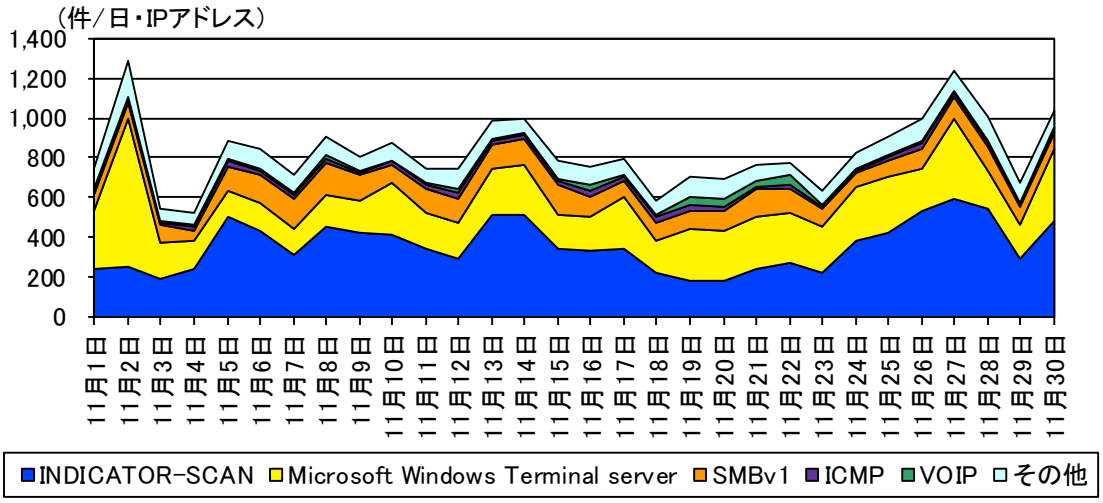


図 3-1　不正侵入等の攻撃手法別検知件数の推移

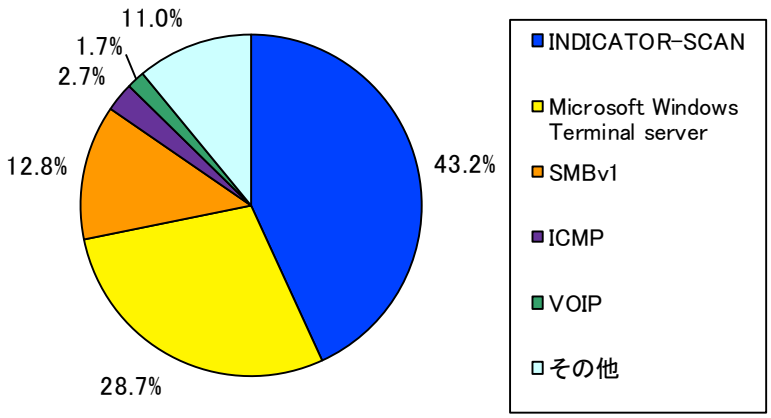


図 3-2　不正侵入等の攻撃手法別検知比率

[i] 一日・1IP アドレス当たり。

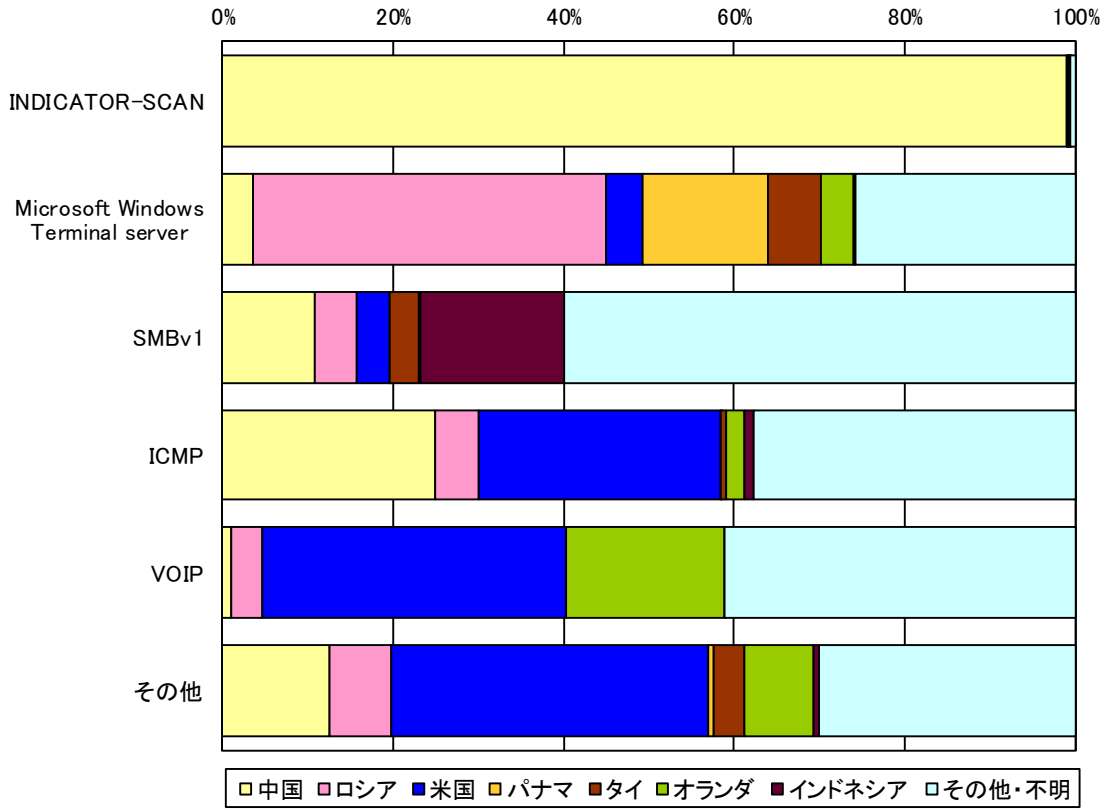


図 3-3 不正侵入等の攻撃手法の国・地域別検知比率

### 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 | 389.48 件 | －8.4% （－35.65 件） |
| 2 位 | 2 位 | ロシア | 111.69 件 | ＋35.4% （＋29.20 件） |
| 3 位 | 3 位 | 米国 | 60.10 件 | －5.8% （－3.71 件） |
| 4 位 | 6 位 | パナマ | 35.56 件 | ＋137.2% （＋20.56 件） |
| 5 位 | 14 位 | タイ | 21.51 件 | ＋296.7% （＋16.09 件） |

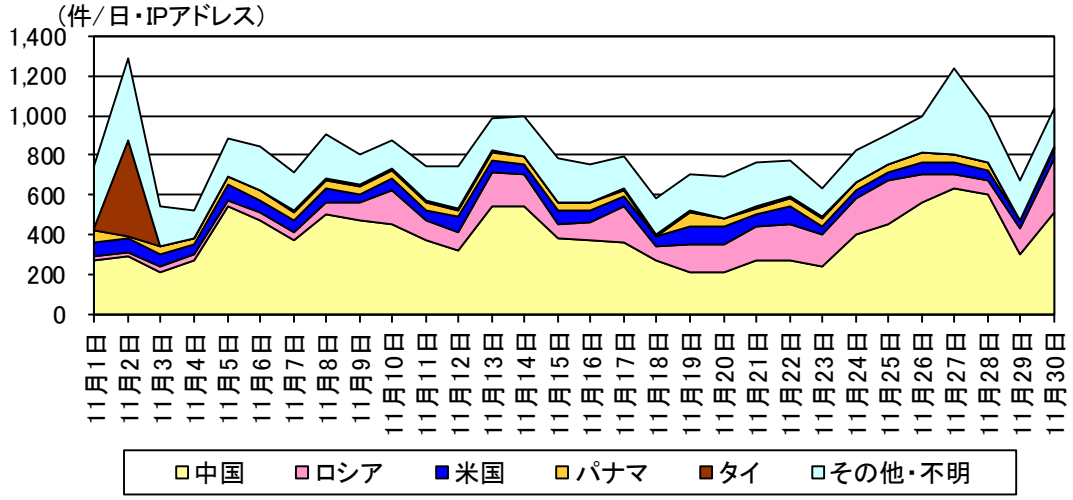


図 3-4 不正侵入等の着信元国・地域別検知件数の推移

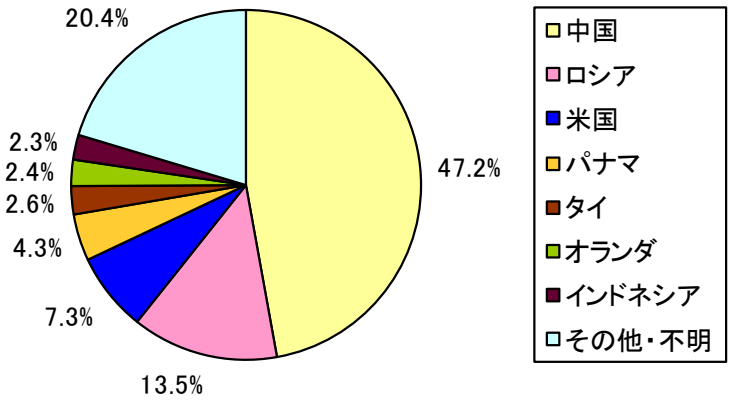


図 3-5 不正侵入等の着信元国・地域別検知比率

[i] 一日・1IP アドレス当たり。

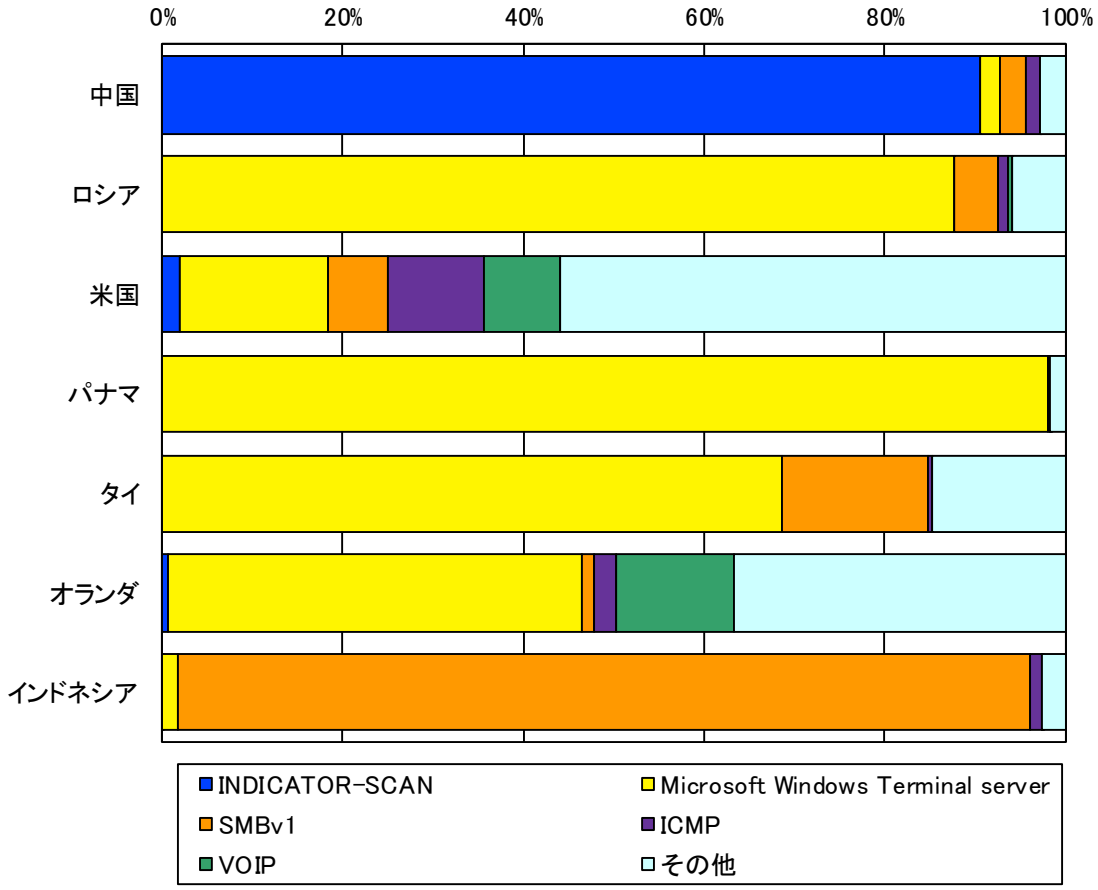


図 3-6 不正侵入等の着信元国・地域別上位の攻撃手法別検知比率

## 4　DoS 攻撃被害の観測結果

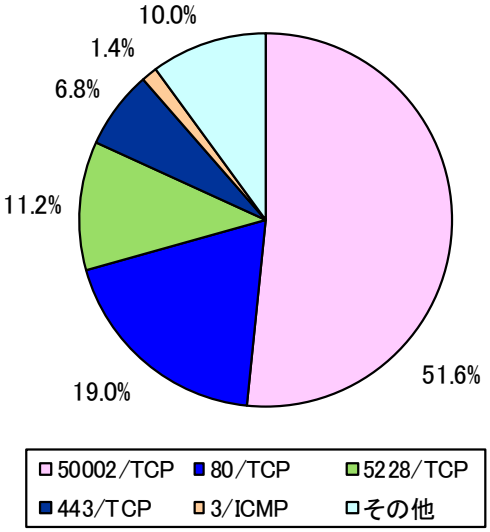


図 4-1　跳ね返りパケット着信元ポート別比率

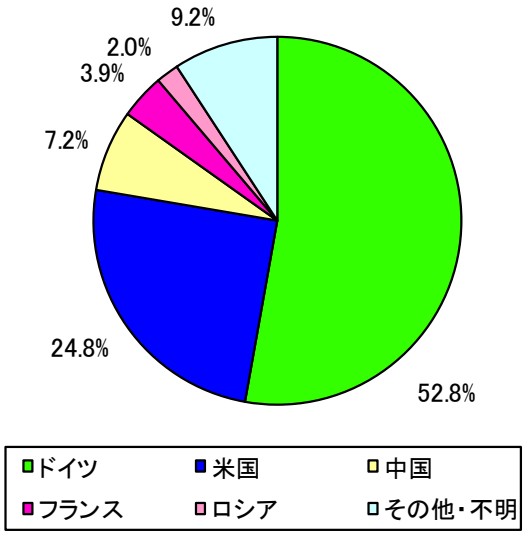


図 4-2　跳ね返りパケット着信元国・地域別比率

## 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 |