

平成 17 年 6 月 8 日

# 我が国におけるインターネット治安情勢について

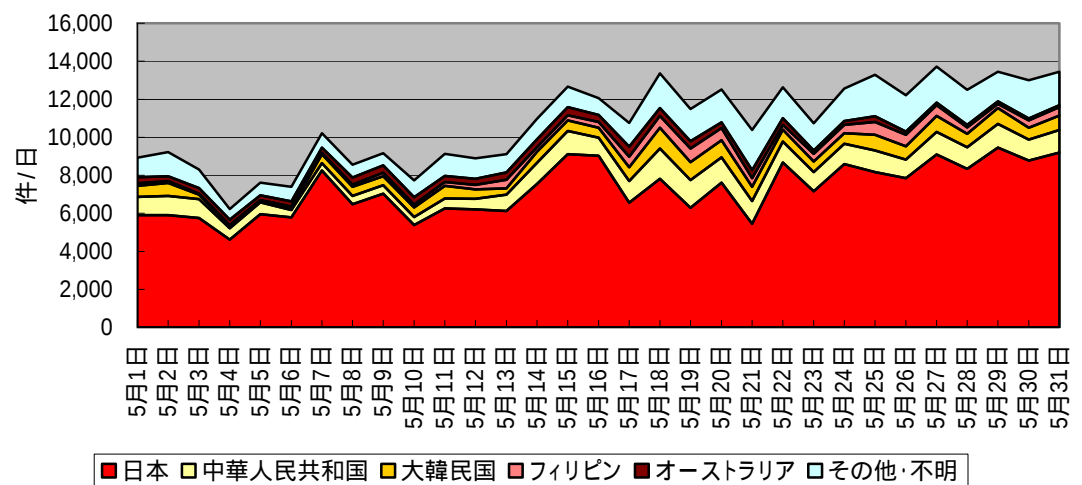
(平成 17 年 5 月期)

## 1 インターネット定点観測

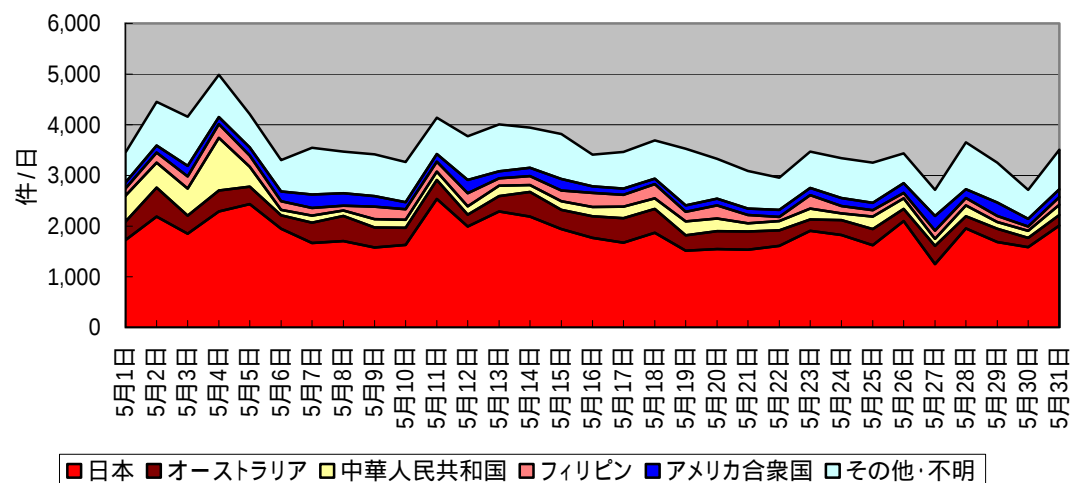
### 1.1 ファイアウォール / Firewall

#### (1) 宛先ポート別推移(上位 5 ポート、積み上げ)

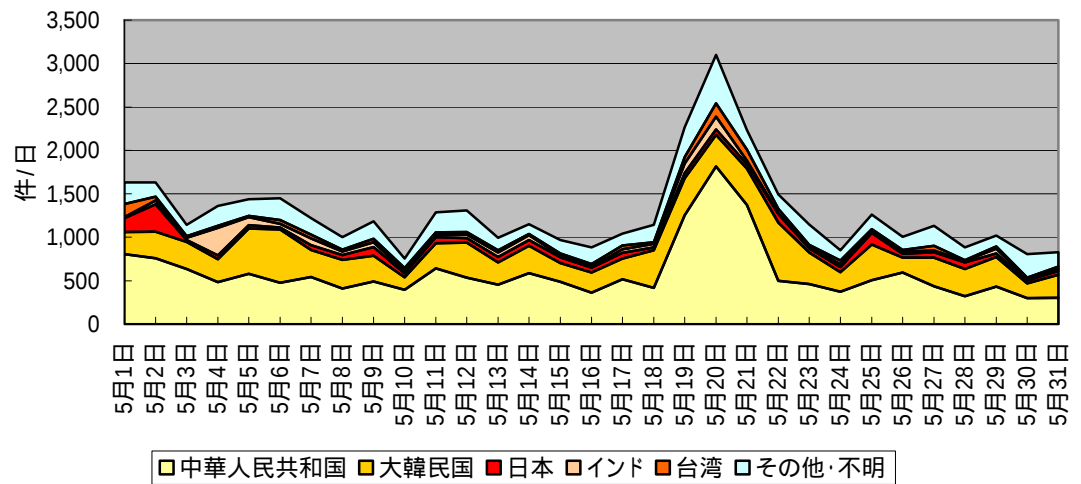
##### ■ 135/TCP



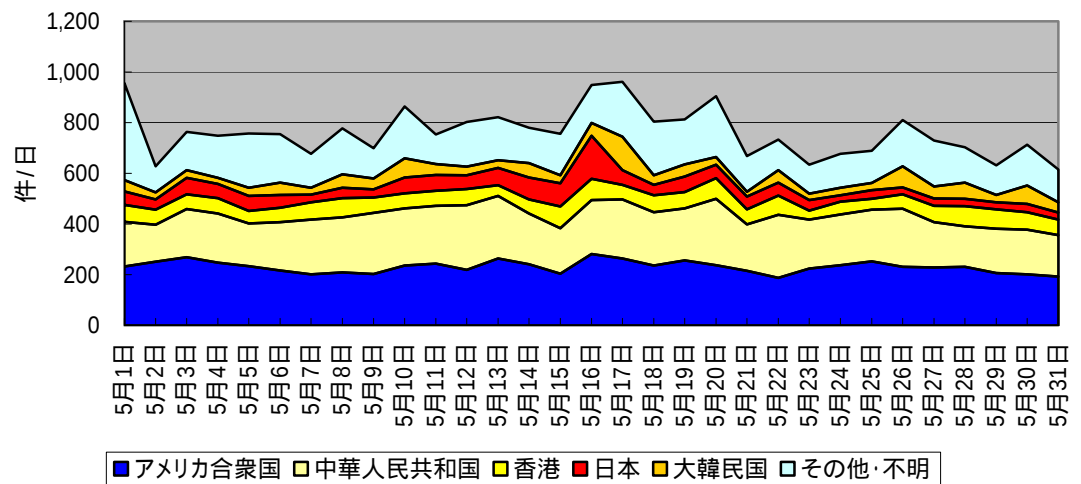
##### ■ 445/TCP



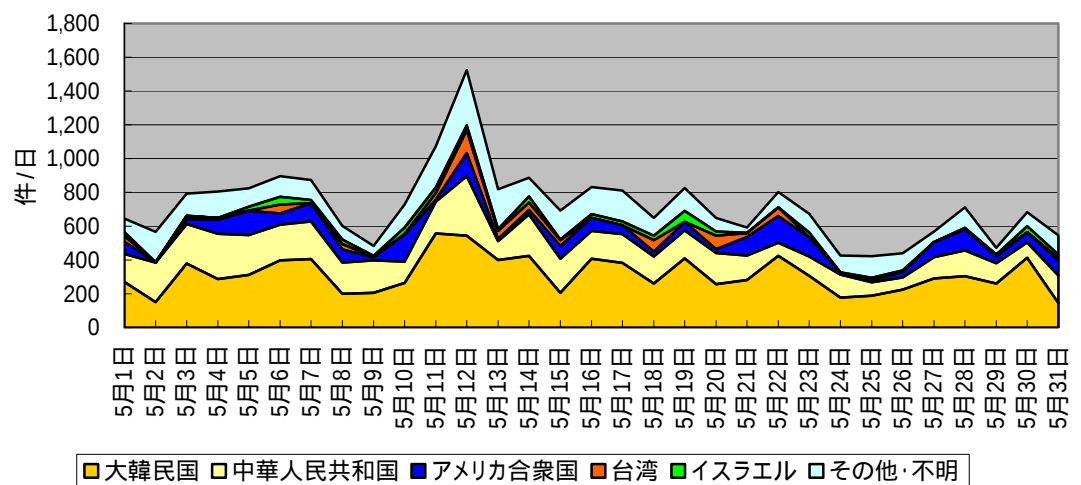
■ 1433/TCP



■ ICMP

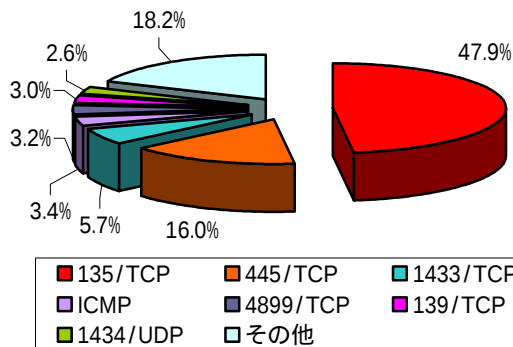


■ 4899/TCP

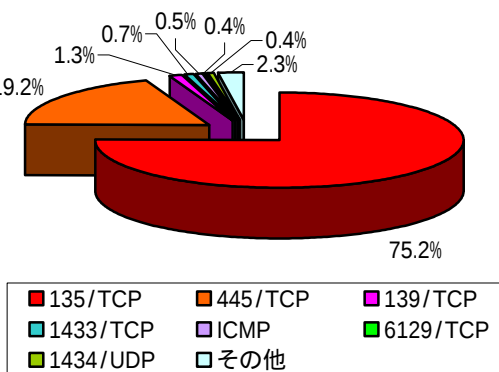


## (2) 宛先ポート別比率

### ■ 全世界

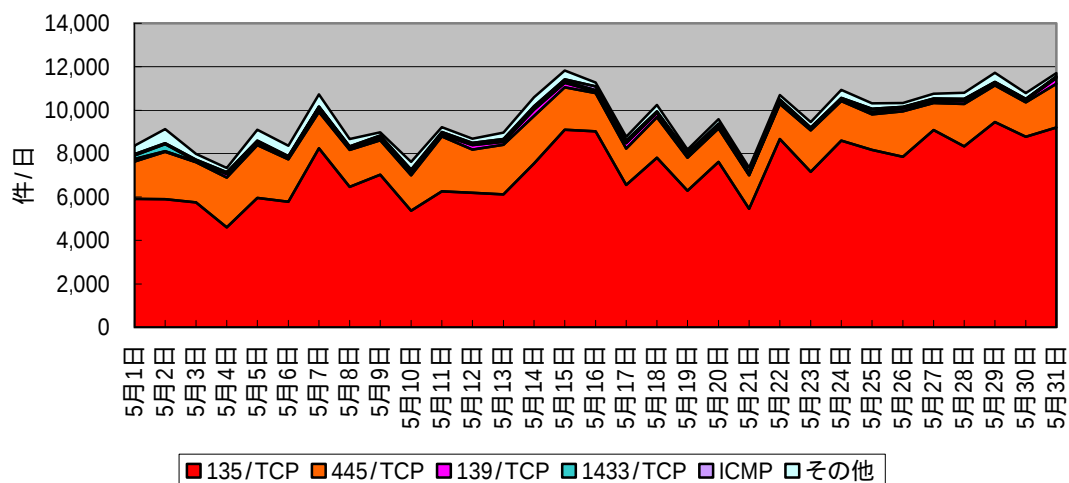


### ■ 日本

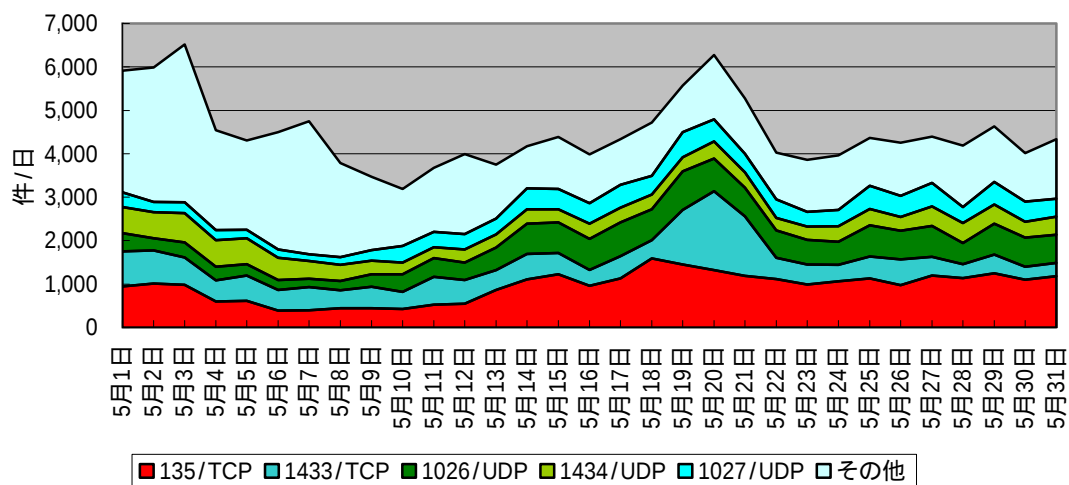


## (3) 発信元国/地域別推移(上位 5 か国、積み上げ)

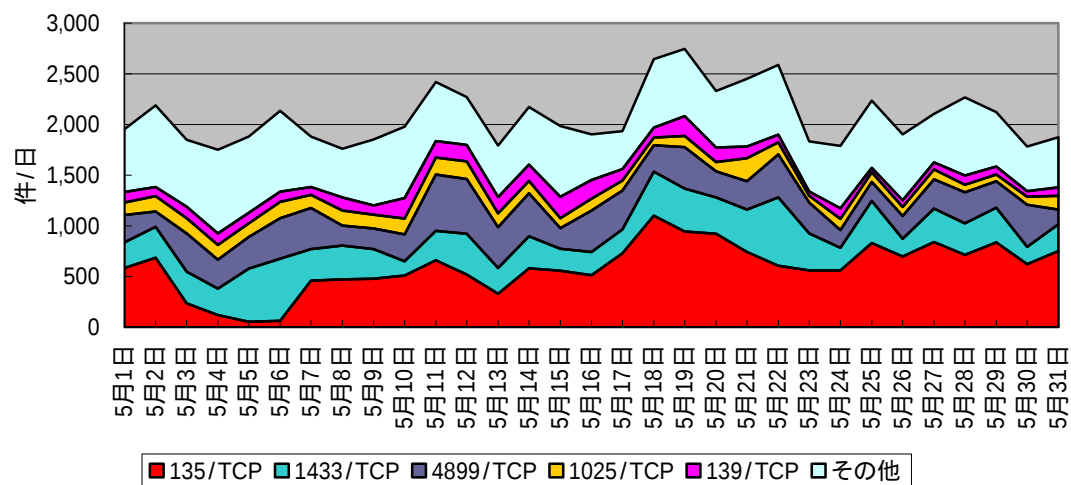
### ■ 日本



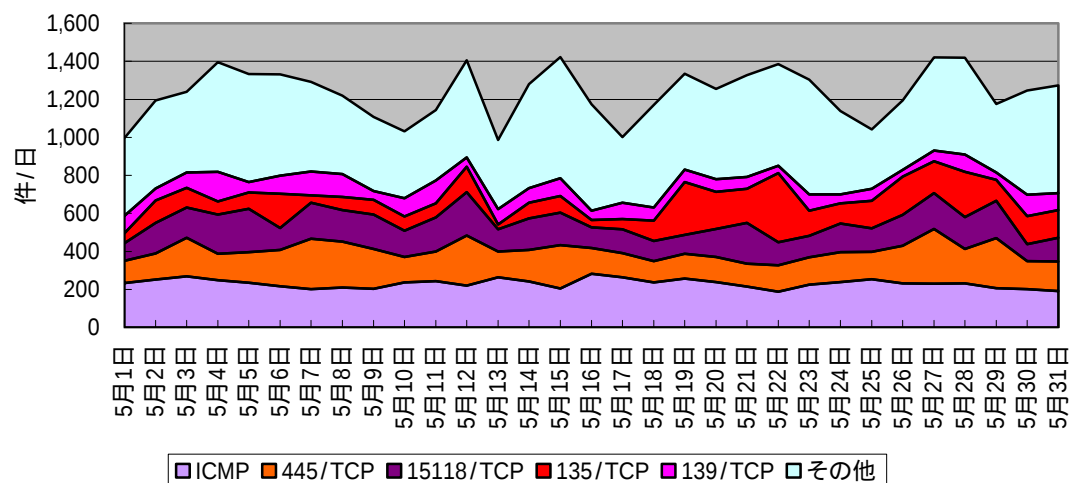
### ■ 中華人民共和国



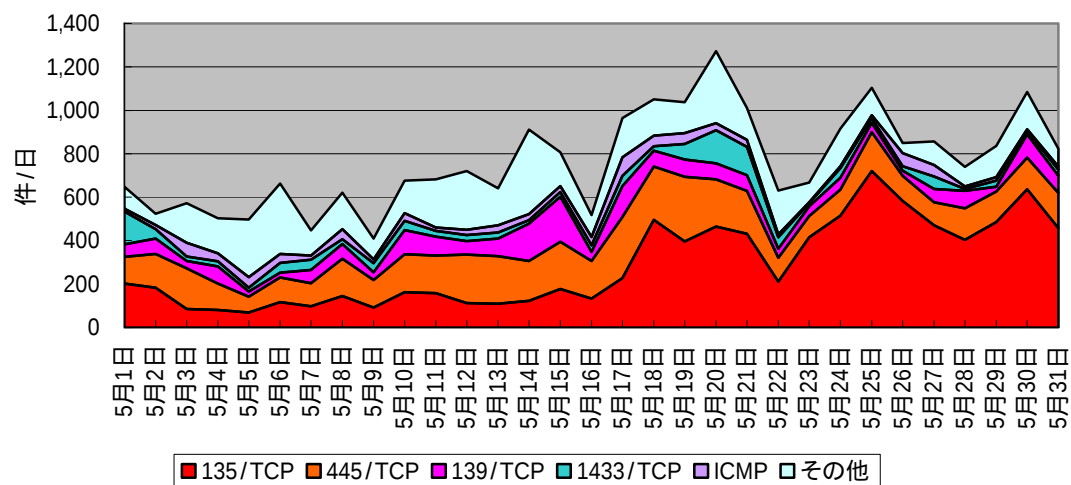
## ■ 大韓民国



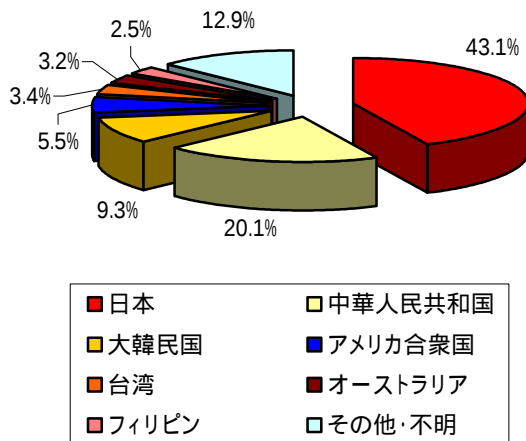
## ■ アメリカ合衆国



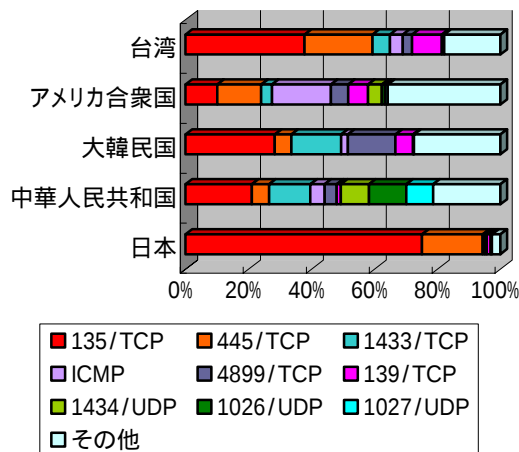
## ■ 台湾



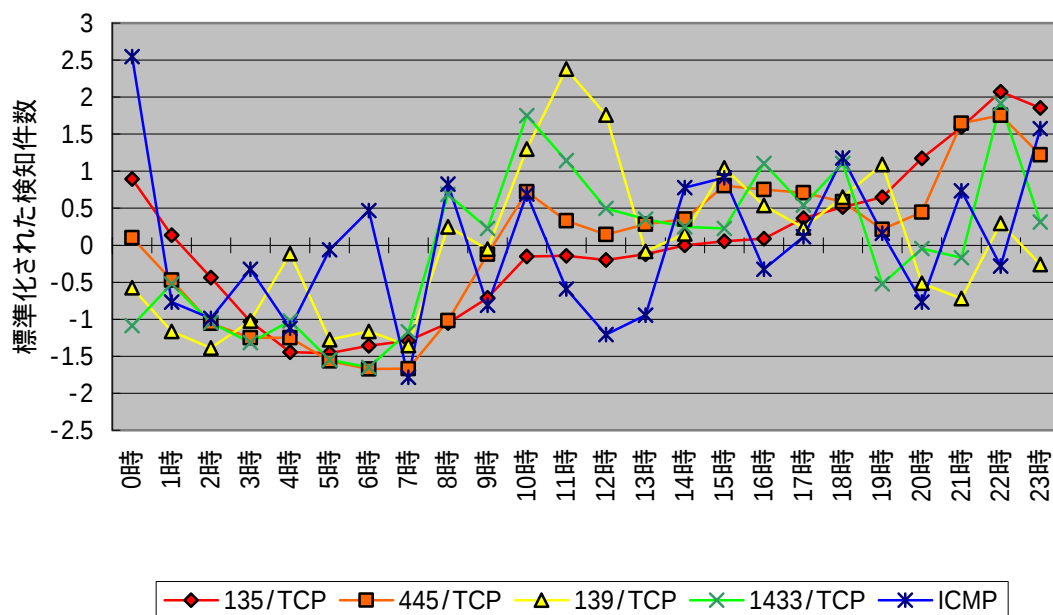
(4) 国/地域別比率



(5) 上位国/地域の宛先ポート別比率



(6) 国内の時間帯推移(上位 5 宛先ポート)

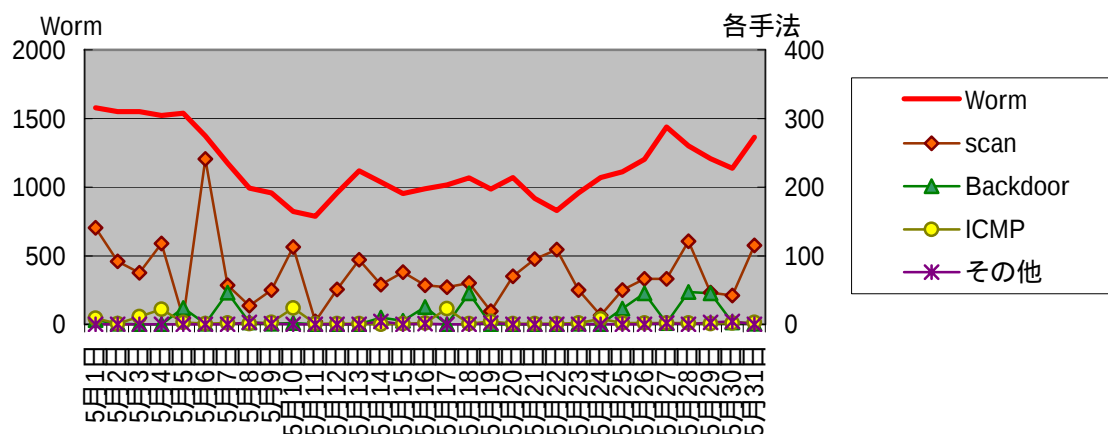


注) 件数は、宛先ポート毎に次の式により標準化した。

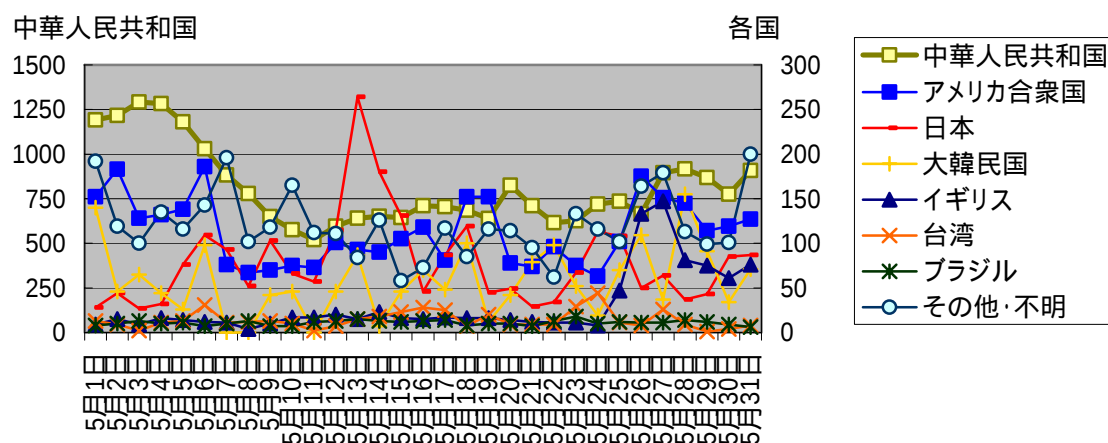
$$\text{標準化された検知件数} = (\text{その時間帯での検知件数} - \text{平均値}) / \text{標準偏差}$$

## 1.2 不正侵入検知システム/ Intrusion Detection System

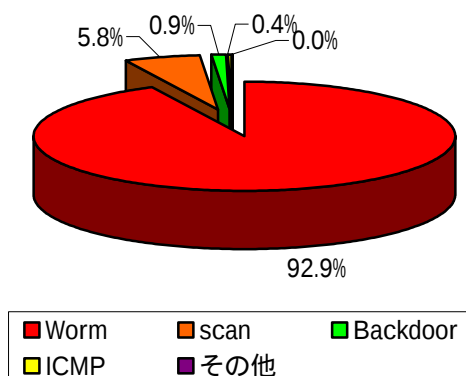
### (1) 攻撃手法別遷移



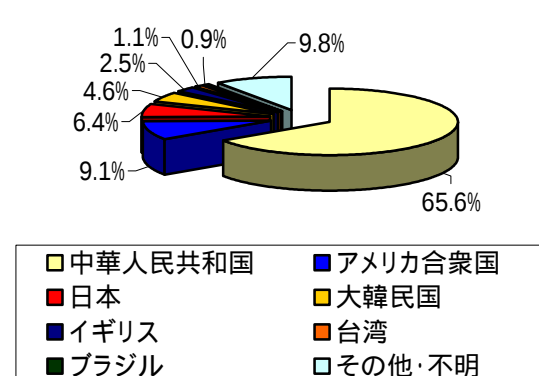
### (2) 発信元国/地域別推移



### (3) 攻撃手法別比率



### (4) 発信元国/地域別比率



## 2 @police (Topics) 掲載事項

@police において 5 月期に掲載を行った主なものは次のとおり。

| 分類                                                                                   | 掲 載 事 項                                                           |
|--------------------------------------------------------------------------------------|-------------------------------------------------------------------|
|  重要 | W32.Sober.O@mm ( W32/Sober.p@MM, WORM_SOBER.S ) ウイルスの発生について (5/3) |
|  重要 | マイクロソフト社のセキュリティ修正プログラムについて (MS05-024) (5/11)                      |
|  重要 | IPsec に関する脆弱性について (5/10)                                          |

## 3 おわりに

当月期におけるファイアウォールに対するアクセス件数は約 693,000 件であり、先月期に比べて約 18%増加している。これは、日本、中華人民共和国及び大韓民国を発信元とする 135/TCP に対するアクセスが、それぞれ約 48%、88%及び 52%増加したためである。特に日本はアクセスが増加傾向にあり、今後の動向に注意する必要がある。また先月期は、特定の拠点に対する大量のアクセス<sup>1</sup>により、発信元国/地域の 5 位にフランス共和国が入っていたが、今月期には同様な大量アクセスは観測されず、3 月期と同様、台湾が 5 位に入っている。

侵入検知システムにおけるアラート検知件数は約 38,000 件であり、先月期に比べて約 34%増加している。これは、中華人民共和国及び日本を発信元とする検知件数が、それぞれ先月に比べて約 55%及び 88%増加しているためである。攻撃手法別では、SQL Slammer ワームの検知件数が約 42%増加している。これは、中華人民共和国を発信元とする検知件数が、先月に比べて増加しているためである。また、攻撃手法別比率における SQL Slammer ワームの占める割合が、先月期の 87.1%から 92.9%に増加しているが、これも同国を発信元とする検知件数の増加によるものである。

---

<sup>1</sup> TCP5662 番ポートに対するアクセスの増加について  
[http://www.cyberpolice.go.jp/important/2005/20050409\\_113338.html](http://www.cyberpolice.go.jp/important/2005/20050409_113338.html)

## 4 グラフの説明

### ■ ファイアウォール

定点観測で集計対象としているファイアウォールは、すべての Incoming のパケットを破棄する設定となっている。集計は、Incoming のトラフィックのみ対象とし、Outgoing のトラフィックはカウントしていない。グラフでは、ファイアウォールに到着したパケット数の集計結果をプロットしている。

### ■ 不正侵入検知装置

各拠点の不正侵入検知装置には、平成 17 年 5 月現在、約 300 種類のシグネチャが登録されている。検知された各シグネチャは、次に示す分類に従って集計している。グラフには、各分類の上位 4 つとそれ以外(Others)の件数がプロットされる。

グラフに表示される分類と代表的なシグネチャ

| 分類       | 代表的なシグネチャ                                                                                                                                                 |
|----------|-----------------------------------------------------------------------------------------------------------------------------------------------------------|
| Backdoor | SubSeven, IP Unknown Protocol, BackOrifice, NetBus                                                                                                        |
| DDoS     | TFN Probe                                                                                                                                                 |
| DNS      | DNS HINFO decode, DNS Length Overflow Attack, DNS named iquery attempt, named version attempt                                                             |
| DoS      | SYN Flood, UDP Flood, Stick Attack, Land                                                                                                                  |
| ICMP     | Superscan Echo, redirect host, redirect net, Ping Flooding                                                                                                |
| Scan     | Proxy attempt, Port sweep, SYN FIN scan, FIN scan, NMAP TCP, NMAP XMAS, NMAP Fingerprint, Portscan Detection Attack, Window size of 55808(SYN) TCP Packet |
| Worm     | SQL Slammer                                                                                                                                               |
| Others   | Traceroute 検出, Connection Closed MSG from Port 80, IP Duplicate, IP Fragmentation 等を含み上位 4 つを除くもの                                                         |

・シグネチャは随時更新している。