

平成 18 年 11 月 10 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 18 年 10 月期)

- ・ ファイアウォールに対するアクセスは減少傾向  
～ TCP445 番ポートに対するアクセスが激減 ～
- ・ 不正侵入検知システムにおけるアラートは微増

## 1 概説

平成 18 年 10 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 466,708 件で、一日当たり約 15,055 件 (対前月比-12.1%) と減少した。この減少の主な要因として、日本国内を発信元とする 445/TCP に対するアクセスが激減したことが挙げられる。これは、8 月に発表された Windows の脆弱性 (MS06-040) を突く攻撃又はウイルスが減少したものと考えられる。445/TCP に対するアクセスが減少したことから、上位 5 位までの順位は、135/TCP、445/TCP、139/TCP、ICMP(Echo Request)、1026/UDP の順となった。

不正侵入検知システム におけるアラート検知件数は 36,164 件で、一日当たりの検知件数は約 1,166 件 (対前月比+2.7%) であった。攻撃手法別において第 1 位の Worm (SQL Slammer) は、9 月期と同様、全体の 9 割以上を占めた。また、発信元国 / 地域別において、上位は、中華人民共和国、アメリカ合衆国、ベトナム、日本、ブラジル、台湾の順であった。

---

ファイアウォール及び不正侵入検知システムについては、「4 集計対象」参照

## 2 インターネット定点観測

### 2.1 ファイアウォールに対するアクセス分析

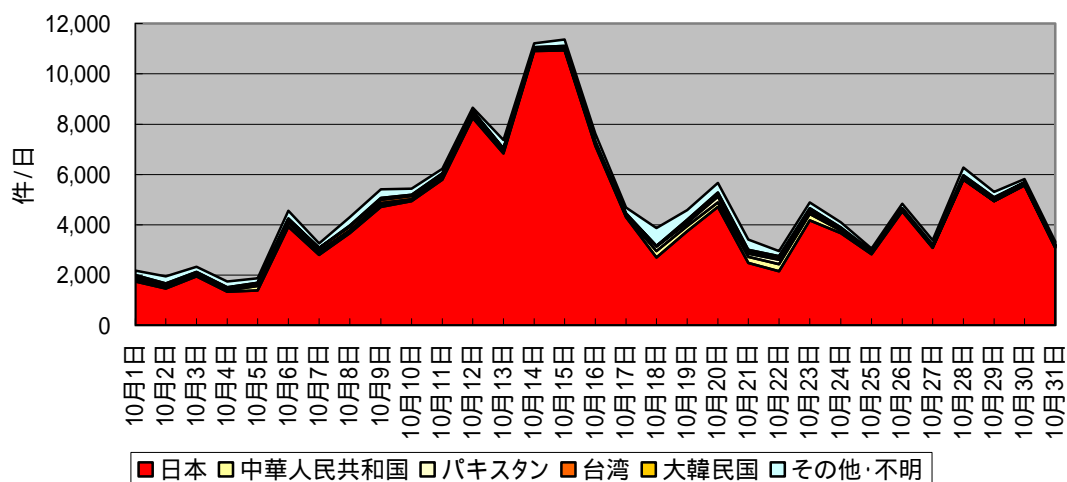
#### (1) 宛先ポート別推移(上位 5 ポート、積み上げ)

9 月期と 10 月期における上位 5 ポートは以下のとおりである。445/TCP に対するアクセスが激減し、順位に変動があった。一日当たりのアクセス件数について 9 月期との増減比較を、表の右側に示す。

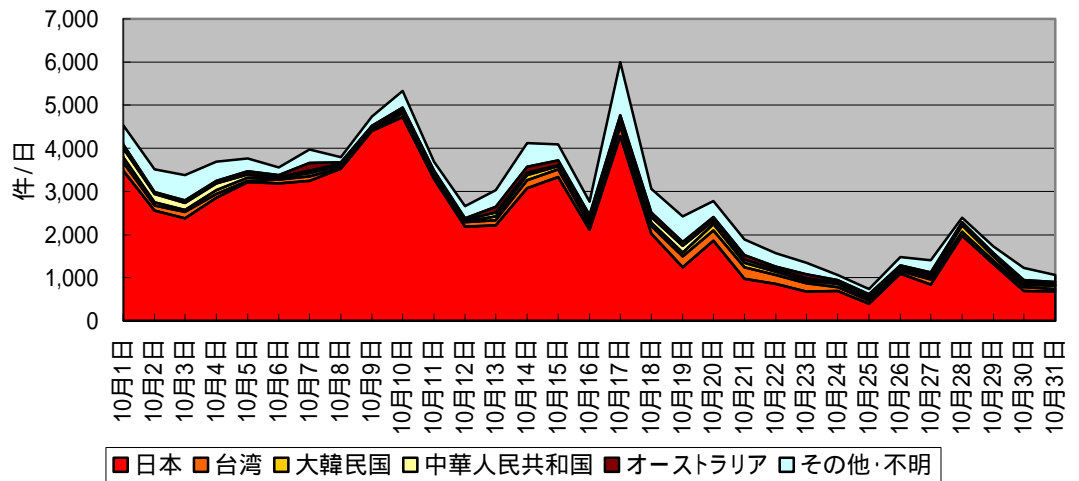
ポート	9 月期	10 月期	前月比(一日当たり)
135/TCP	2 位	1 位	約-1.1% (約-53 件)
445/TCP	1 位	2 位	約-46.7% (約-2,568 件)
139/TCP	4 位	3 位	約+12.9% (約+133 件)
ICMP(Echo Request)	3 位	4 位	約-7.9% (約-88 件)
1026/UDP	5 位	5 位	約+12.2% (約+96 件)

#### 135/TCP

全体として大きな変動は見当たらなかった。国内からのアクセスが大半を占めている。10 月 15 日前後に急激な増加があるが、これは特定のネットワークアドレスからのアクセスが増加したためである。

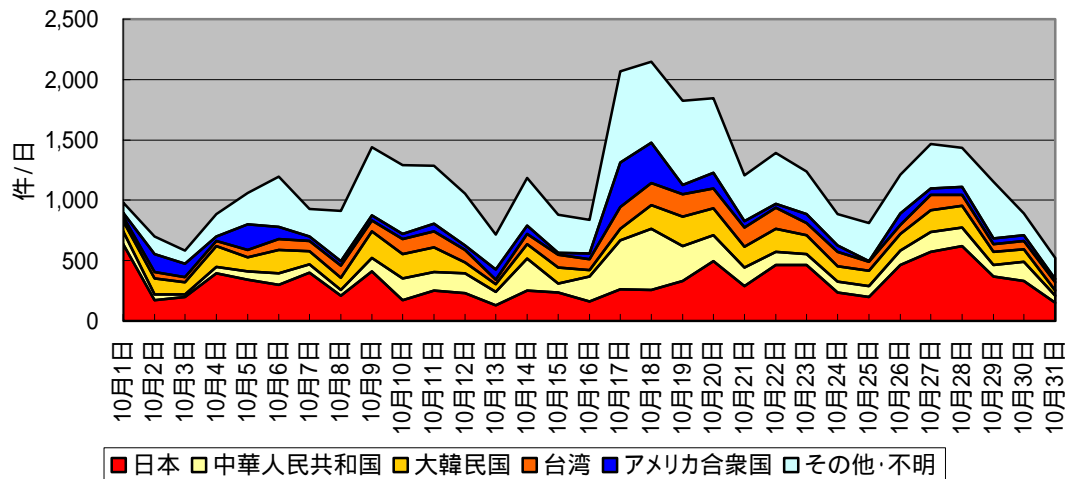


### 445/TCP



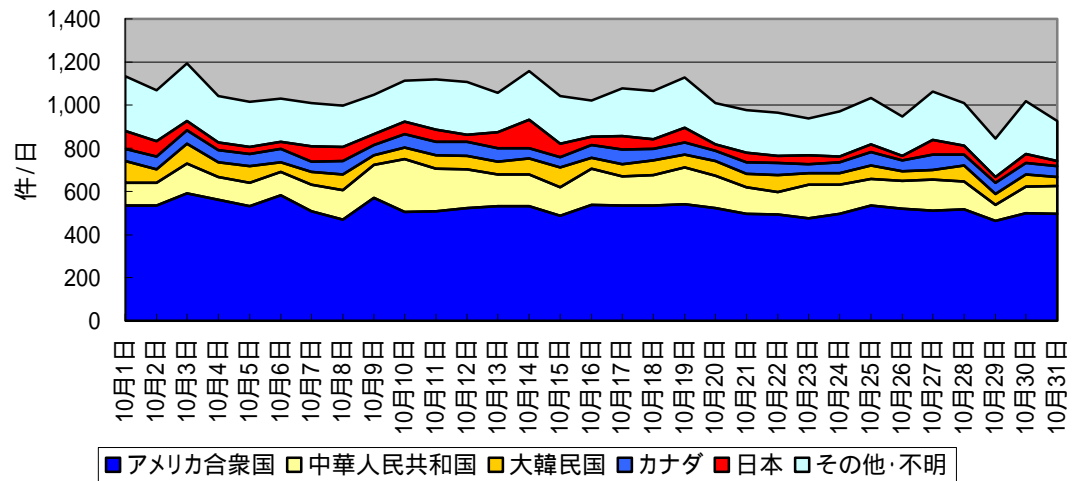
アクセスの大半を占める日本国内からのアクセスが大幅に減少したことから、全体としても大幅な減少となった。アクセスが減少した理由として、8月に発表された Windows の脆弱性（MS06-040）を突く攻撃又はウイルスによる被害が減少したことが考えられる。

### 139/TCP



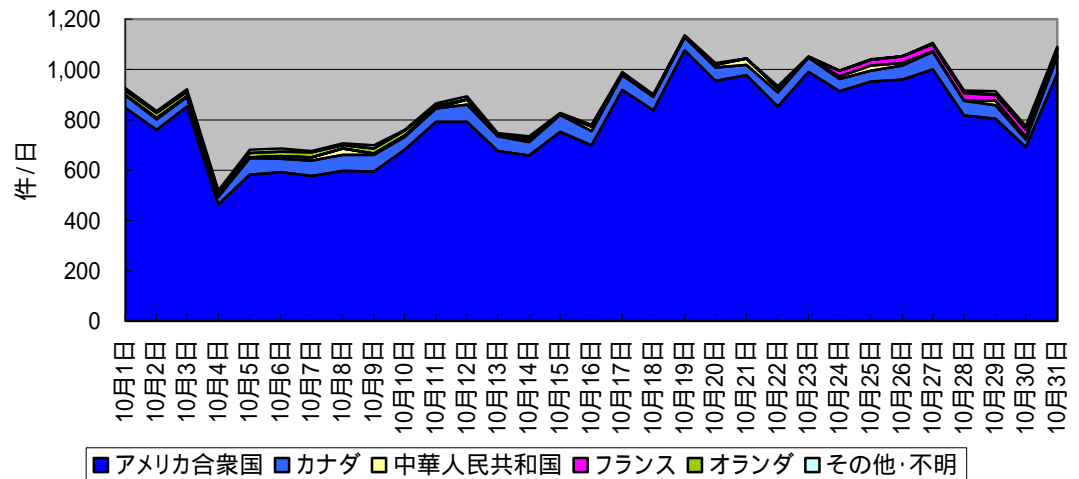
日本国内からのアクセスは減少したが、国外からのアクセスが増加したため、全体としても増加となった。

### ICMP(Echo Request)



アメリカ合衆国からのアクセス数は変わらないものの、中華人民共和国からのアクセス数が減少したことから、全体としても減少となった。

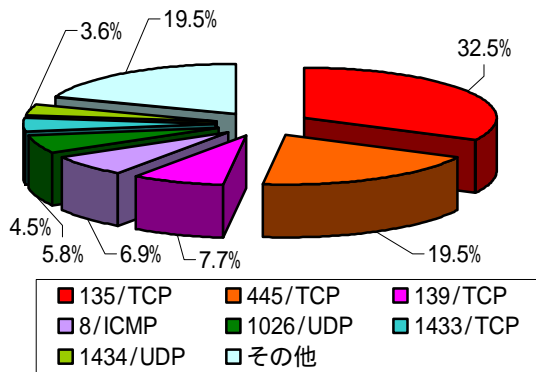
### 1026/UDP



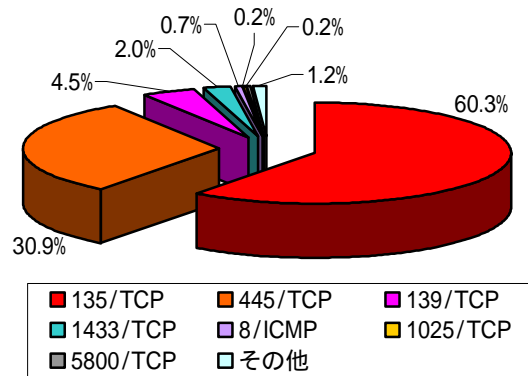
アクセスの大半を占めるアメリカ合衆国からのアクセスが引き続き増加しているため、全体としても増加となった。このポートは、マイクロソフト社の Messenger Service が使用しているものであり、アクセスの多くは同サービスを悪用したスパムと考えられる。

(2) 宛先ポート別比率

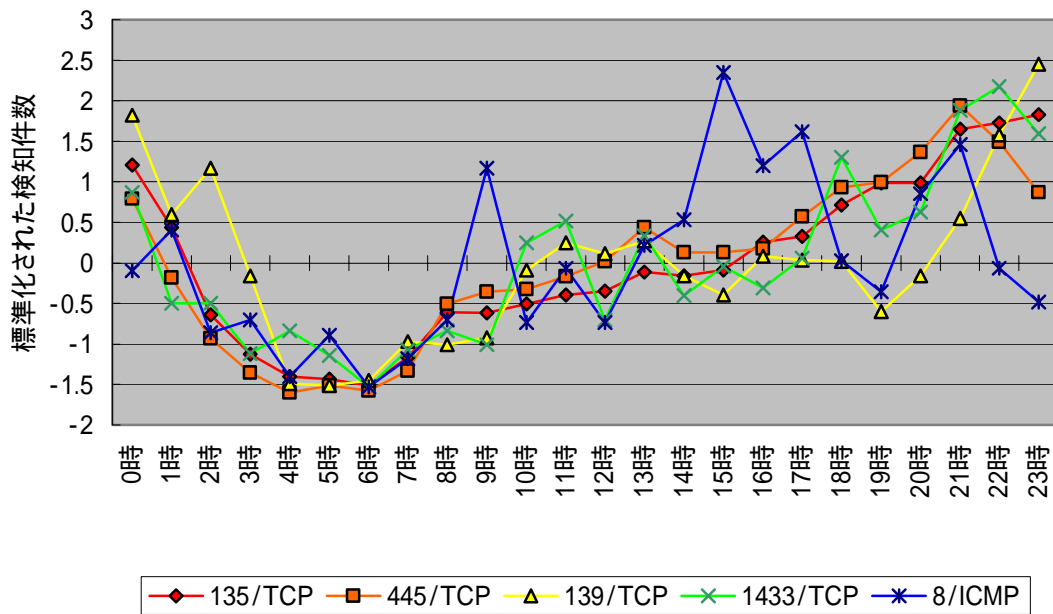
発信元/全世界



発信元/日本



(3) 国内の時間帯推移(上位 5 ポート)



注) 件数は、宛先ポートごとに次の式により標準化した。

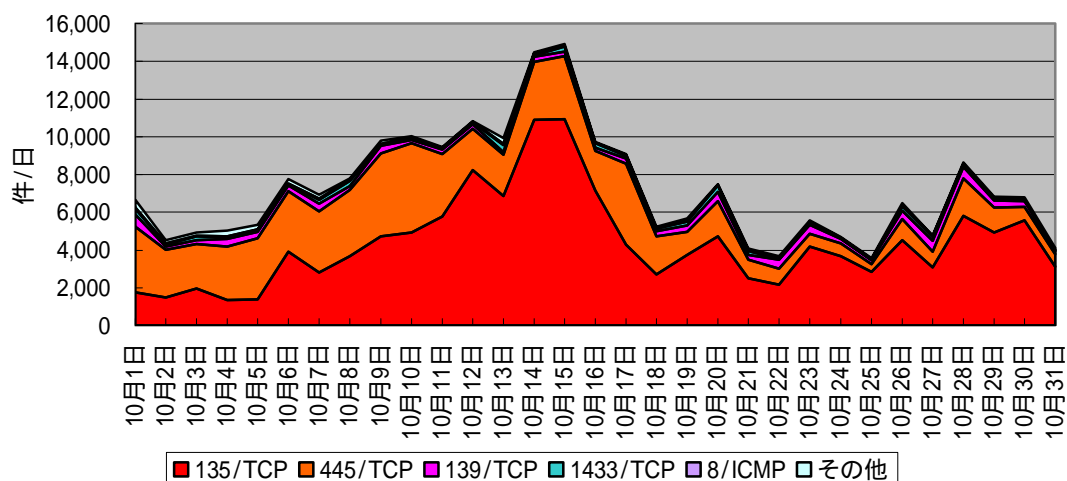
$$\text{標準化された検知件数} = (\text{その時間帯での検知件数} - \text{平均値}) / \text{標準偏差}$$

#### (4) 発信元国 / 地域別推移(上位 5 か国、積み上げ)

9 月期と 10 月期における上位 5 位までの国 / 地域は以下のとおりである。アメリカ合衆国からのアクセスが増加、中華人民共和国からのアクセスが減少したため順位に変動があった。一日当たりのアクセス件数について 9 月期との増減比較を、表の右側に示す。

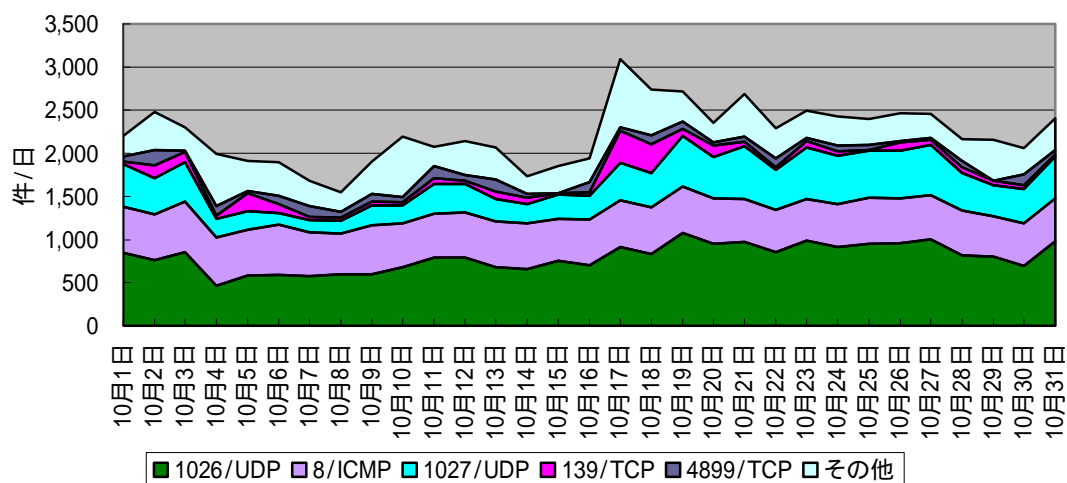
	9 月期	10 月期	前月比 (一日当たり)
1 位	日本	日本	約-24.8% (約-2,389 件)
2 位	中華人民共和国	アメリカ合衆国	約+6.9% (約+143 件)
3 位	アメリカ合衆国	中華人民共和国	約-6.5% (約-139 件)
4 位	大韓民国	大韓民国	約-14.4% (約-104 件)
5 位	台湾	台湾	約+11.0% (約+48 件)

#### 日本



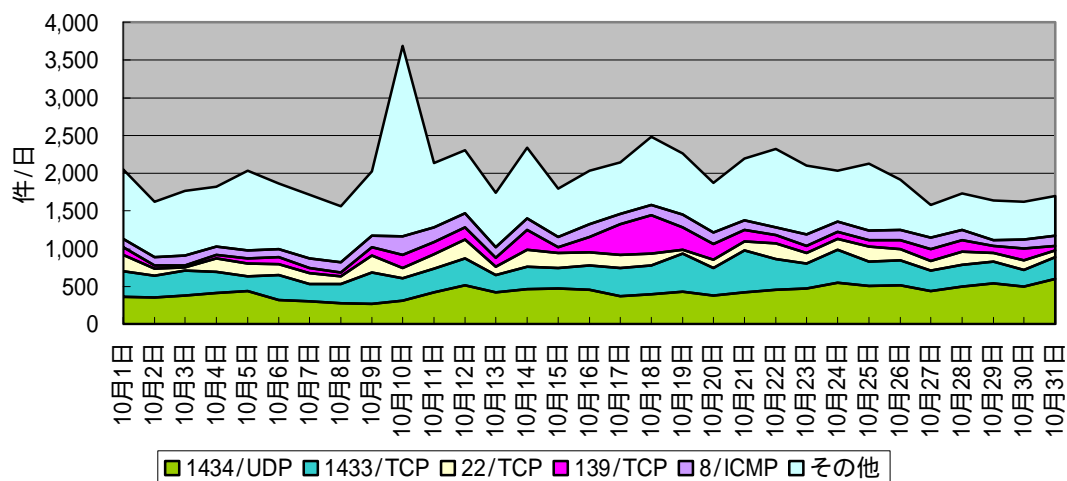
445/TCP に対するアクセスが大幅に減少したため、全体として大幅な減少となった。445/TCP のアクセスが減少した理由として、8月に発表された Windows の脆弱性 (MS06-040) を突く攻撃又はウイルスが減少したものと考えられる。

## アメリカ合衆国



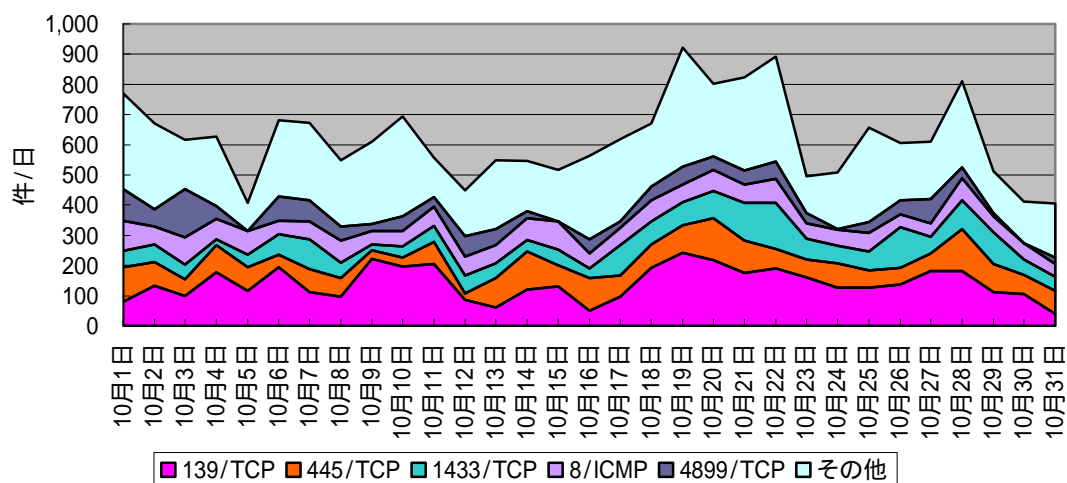
先月から引き続き、1026/UDP、1027/UDP に対するアクセスが増加したことから、全体としては増加となった。1026/UDP 及び 1027/UDP はマイクロソフト社の Messenger Service が使用しているものであり、アクセスの多くは同サービスを悪用したスパムと思われる。

## 中華人民共和国



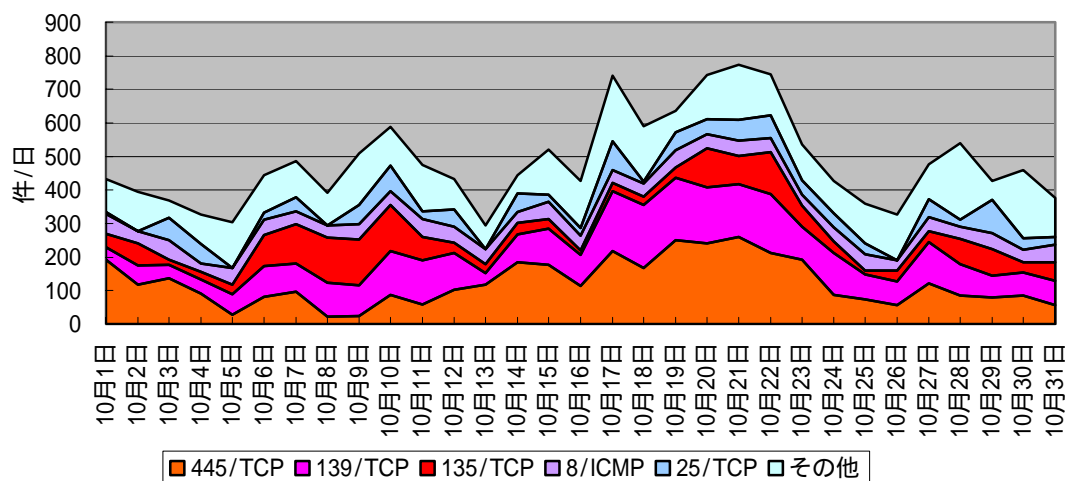
先月と比較して大きな動きは無かった。10月10日前後の急激な増加は、特定のネットワークからの複数ポートへのアクセスが要因となっている。

## 大韓民国



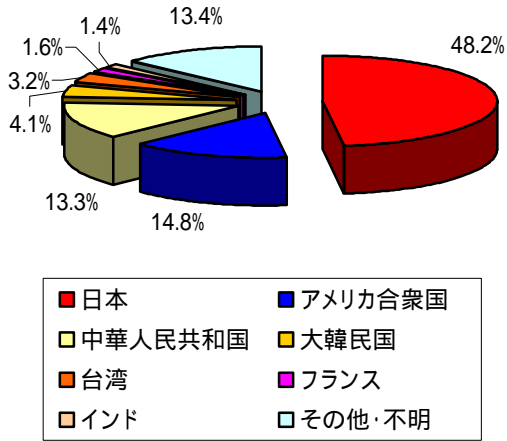
445/TCP に対するアクセスが大きく減少した。139/TCP、135/TCP に対するアクセスも減少しており、全体として減少となった。日本と同様、445/TCP のアクセスが減少した理由として、8月に発表された Windows の脆弱性 (MS06-040) を突く攻撃又はウイルスが減少したと考えられる。

## 台湾

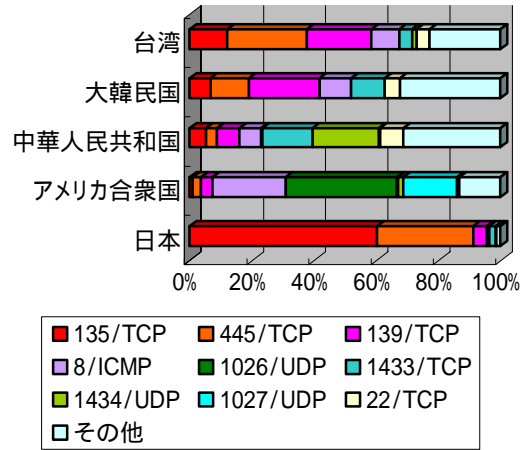


139/TCP に対するアクセスが増加したため、全体としても増加となった。

(5) 国 / 地域別比率

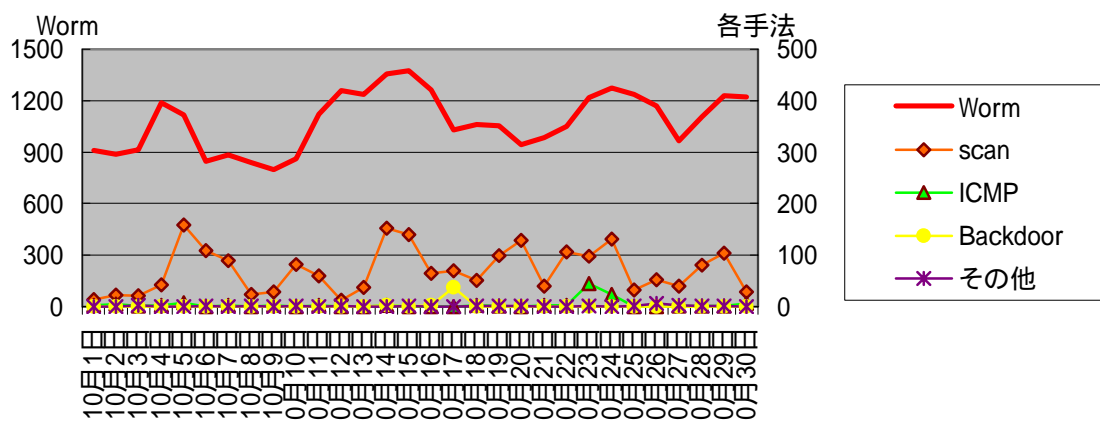


(6) 上位国 / 地域の宛先ポート別比率



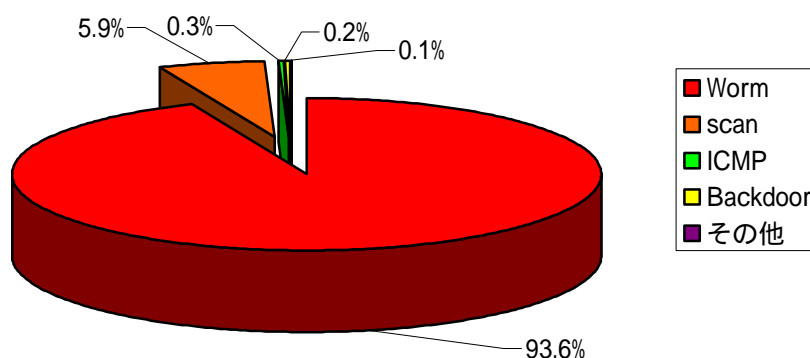
## 2.2 不正侵入検知システムにおけるアラート検知分析

### (1) 攻撃手法別推移

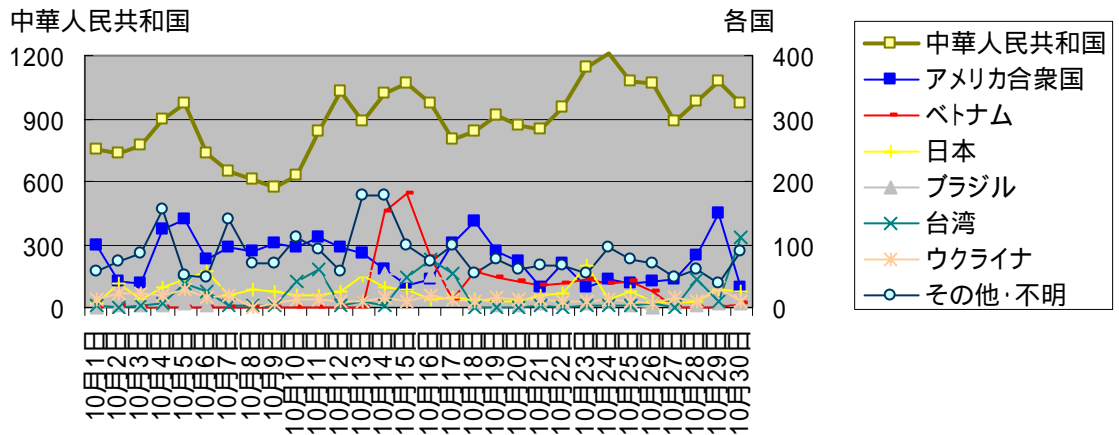


第1位のWorm (SQL Slammer) は、一日当たりの検知件数が約1,091件であり、9月期と比較して約+25件 (約+2.4%) と増加した。第2位のscan (SCAN SOCK Proxy attempt) は、一日当たりの検知件数が約68件であり、9月期と比較して約+3件 (約+5.0%) と増加した。

### (2) 攻撃手法別比率

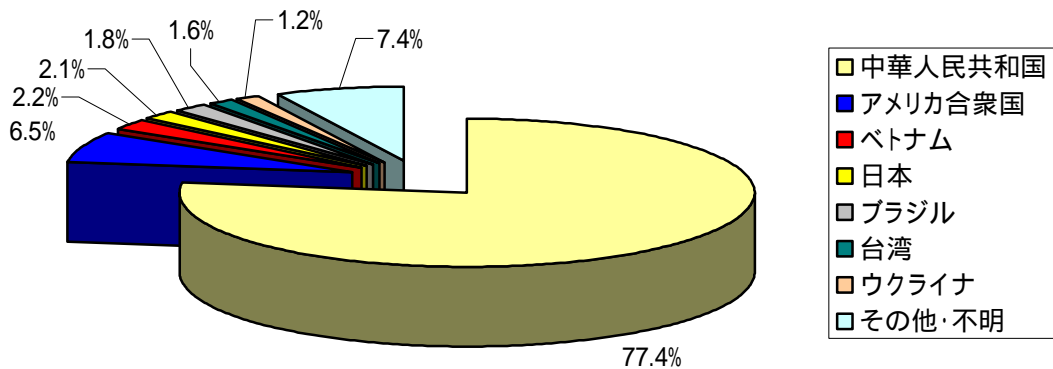


### (3) 発信元国 / 地域別推移



ベトナムを発信元とする検知件数が、10月14日から10月16日に急増している。  
これは、特定発信元からの Worm(SQL Slammer)によるものである。

### (4) 発信元国 / 地域別比率



中華人民共和国を発信元とするアラートの割合が依然高い。ベトナムが増加したが、これは Worm(SQL Slammer)による一時的なものである。

### 3 @police (Topics) 掲載事項

@police において 10 月期に掲載した主なものは次のとおりである。

分類	掲 載 事 項
注意	ジャストシステム社ワープロソフトー太郎の脆弱性について(10/18)更新
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 (MS06-056,057,058,059,060,061,062,063,064,065)(10/11)
注意	ジャストシステム社ワープロソフトー太郎の脆弱性について(10/4)更新

## 4 集計対象

### 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 のトラフィックは対象としていない。

なお、ICMP パケットに関しては、タイプごと<sup>1</sup>に集計している。

### 不正侵入検知システム

各拠点の不正侵入検知装置には、平成 18 年 10 月現在、約 360 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。