

平成 17 年 12 月 9 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 11 月期)

## 1 概説

平成 17 年 11 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 404,000 件であり、前月比で約 11%の減少であった。前月に引き続き、アクセス件数上位のポートに対するアクセスが減少したことが主な要因である。





アクセス件数の第 1 位から第 3 位を占め、ワーム等の感染活動にも悪用される 445/TCP、135/TCP、139/TCP が、それぞれ前月比で約 17%、18%、15%の減少となっている。とりわけ、445/TCP の件数は、Microsoft Windows の脆弱性 (MS05-039) が発表された 8 月以前の水準まで低下している。

しかし、SQL Slammer ワームでも悪用される 1434/UDP に対するアクセス件数は、前月比で約 24%増加しており、特に中国からのアクセス件数が前月比で約 30%増加している。

不正侵入検知システムにおけるアラート検知件数は約 55,000 件であり、前月比で約 26%の増加であった。これは、攻撃手法における Worm (SQL Slammer) 検知件数が、7 月期後半以降高水準を維持しており、前月比で約 25%増加したことが主な要因である。

## 2 @police (Topics) 掲載事項

@police において 11 月期に掲載を行った主なものは次のとおり。

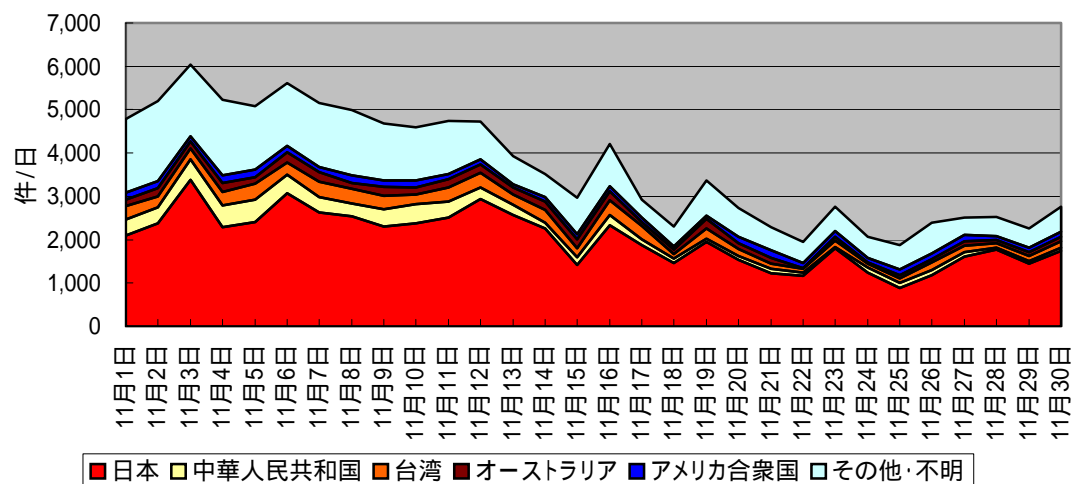
分類	掲 載 事 項
•	FIRST への加盟について(11/1)
	Cisco 社製ネットワーク機器の脆弱性について(11/4)
	マイクロソフト社のセキュリティ修正プログラムについて (MS05-053)(11/9)
	ISAKMP を実装した機器の脆弱性について(11/18)
	Java Runtime Environment(JRE)等の脆弱性について(11/30)

### 3 インターネット定点観測

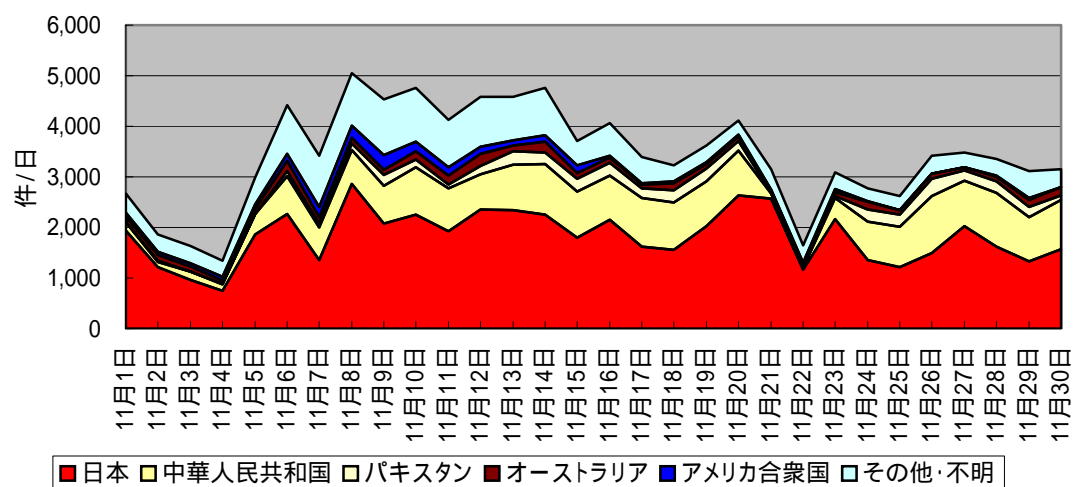
#### 3.1 ファイアウォール / Firewall

##### (1) 宛先ポート別推移(上位 5 ポート、積み上げ)

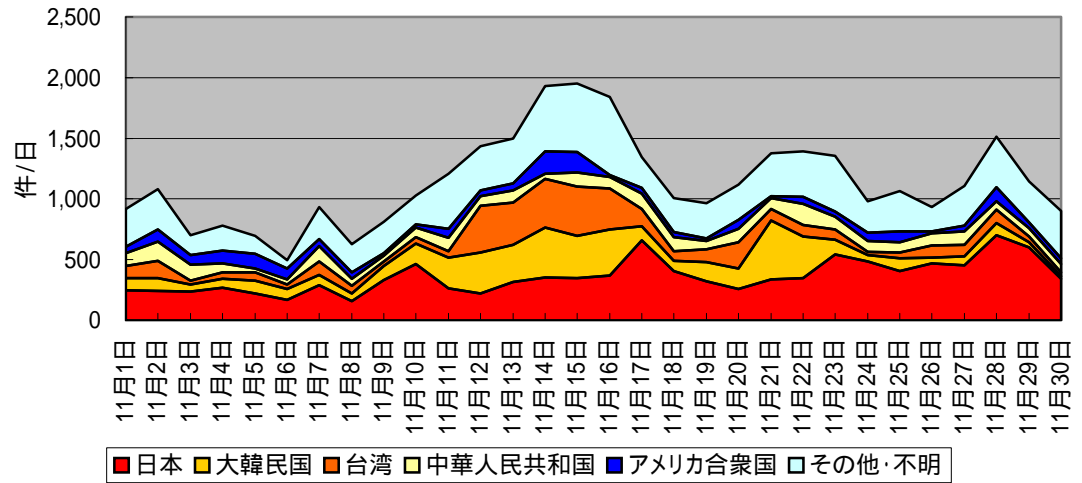
445/TCP



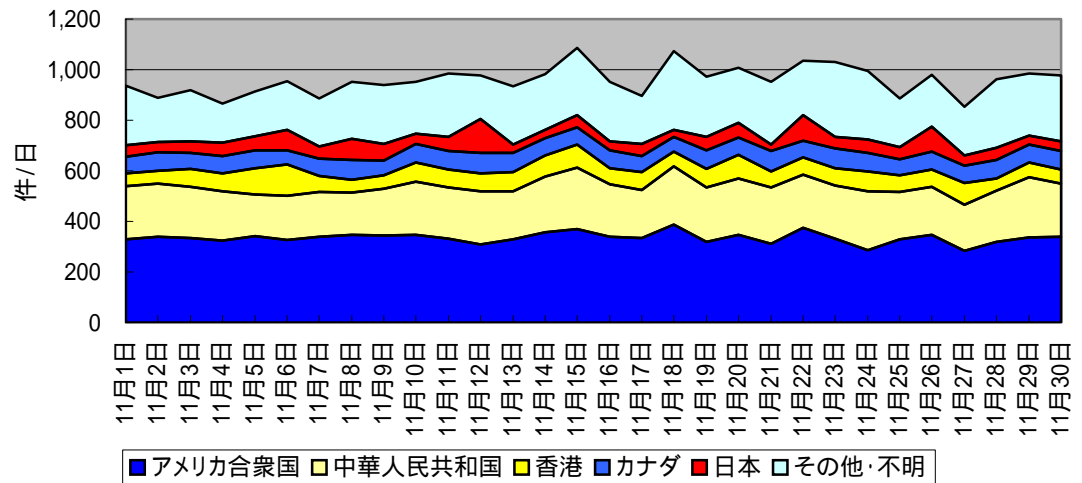
135/TCP



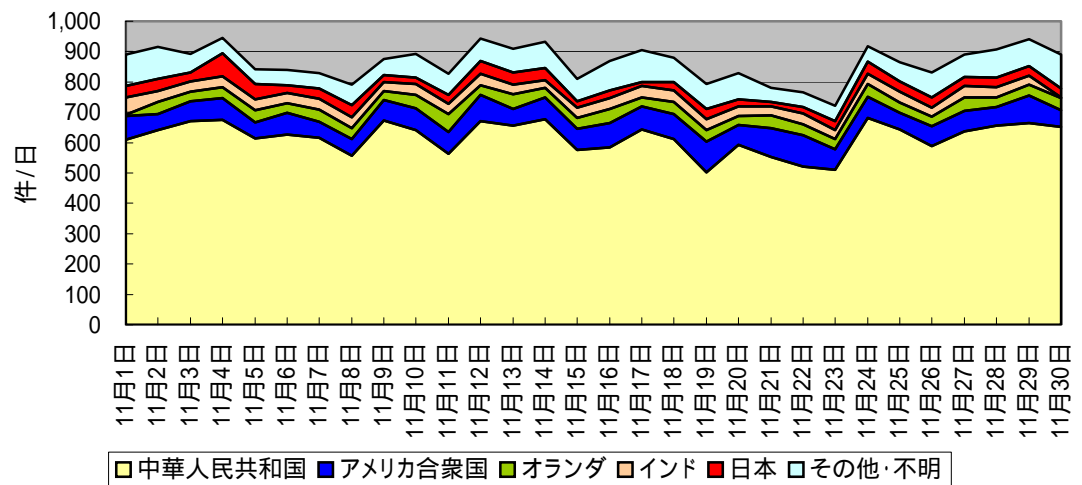
139/TCP



ICMP

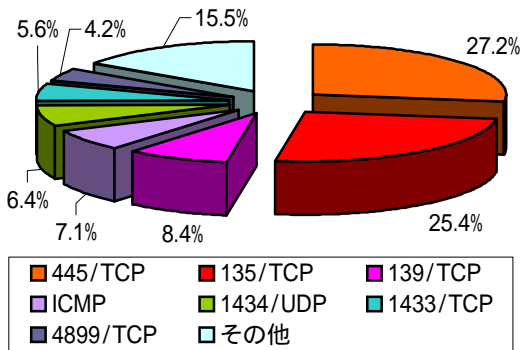


1434/UDP

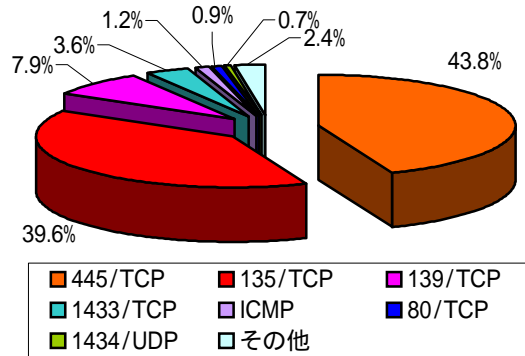


(2) 宛先ポート別比率

発信元/全世界

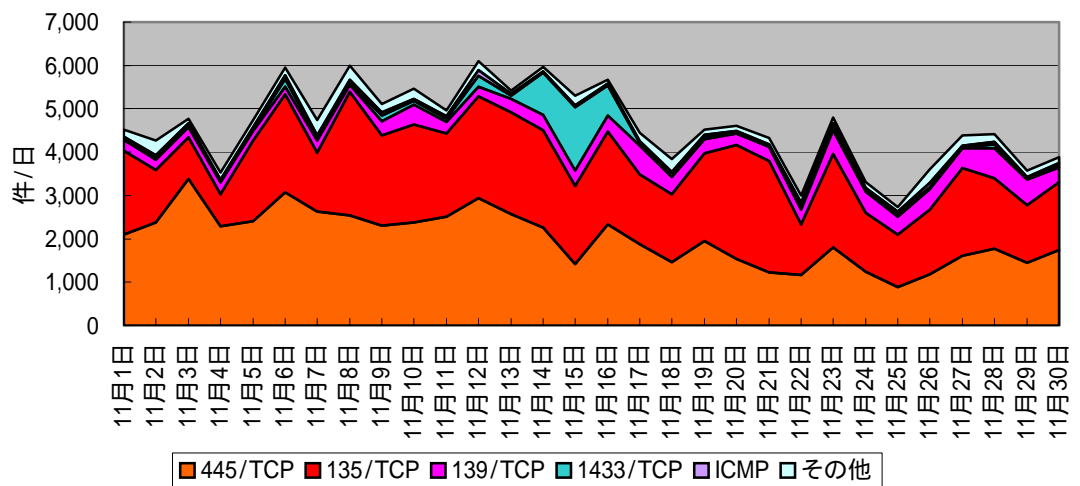


発信元/日本

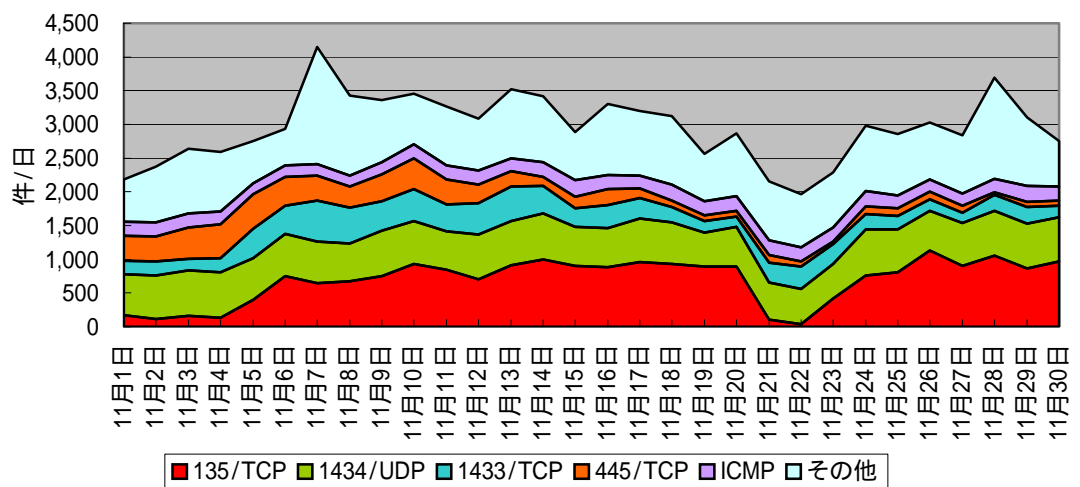


(3) 発信元国/地域別推移(上位5か国、積み上げ)

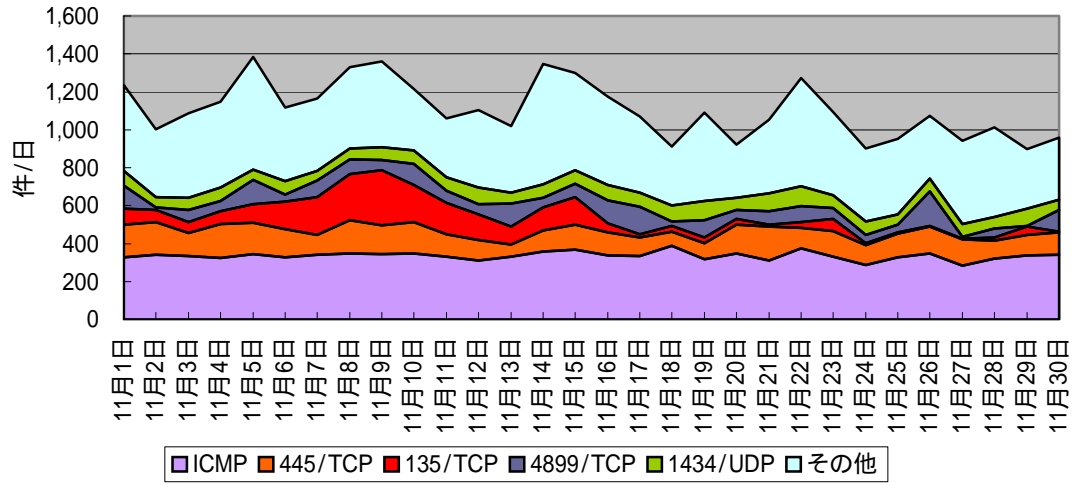
日本



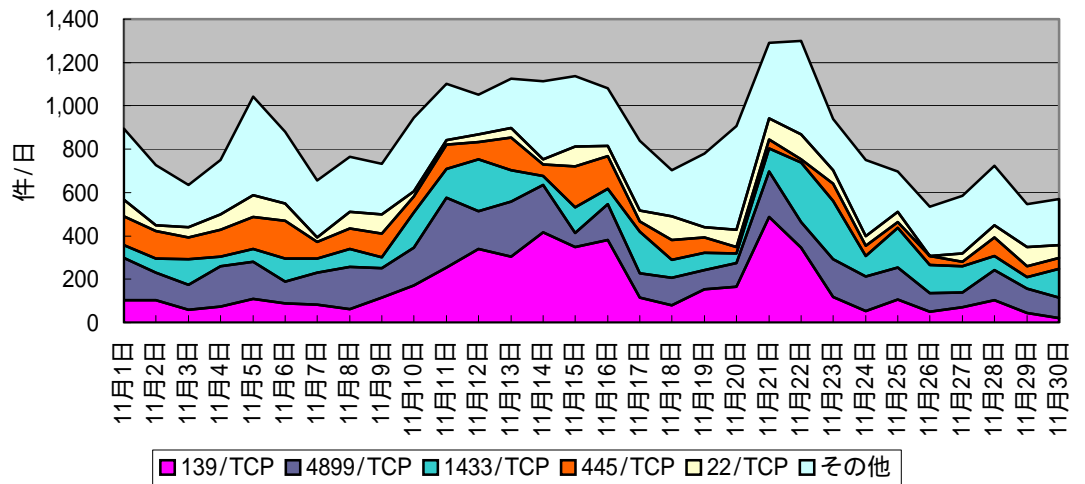
中華人民共和国



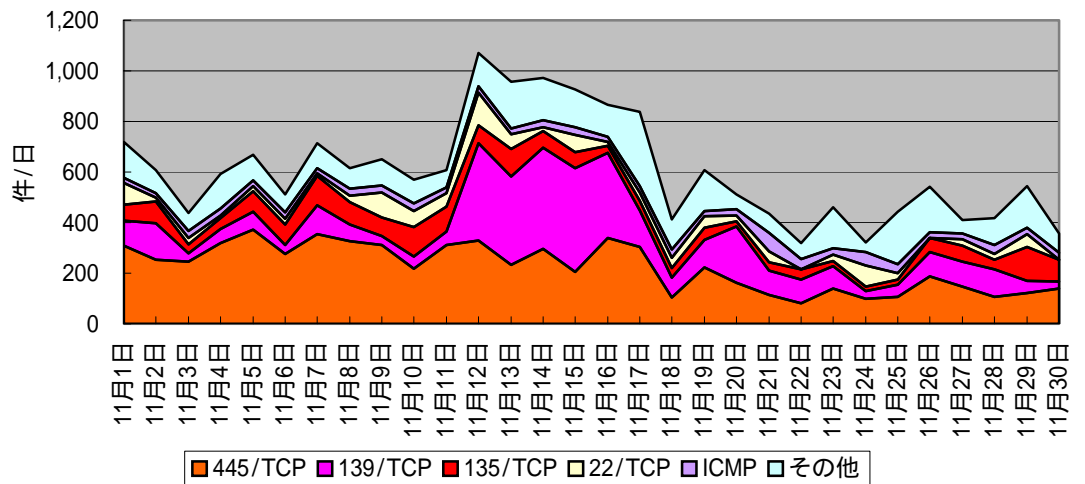
**アメリカ合衆国**



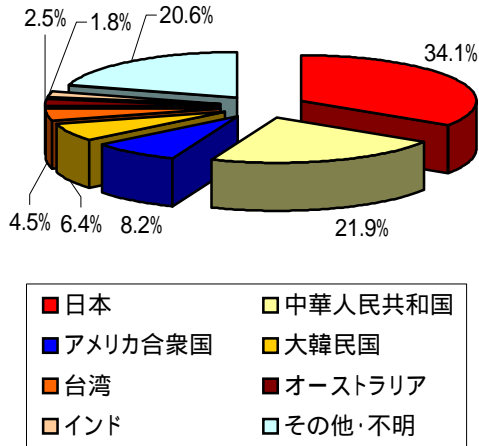
**大韓民国**



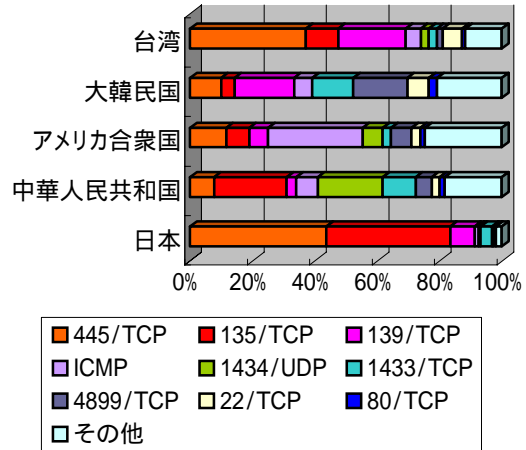
**台湾**



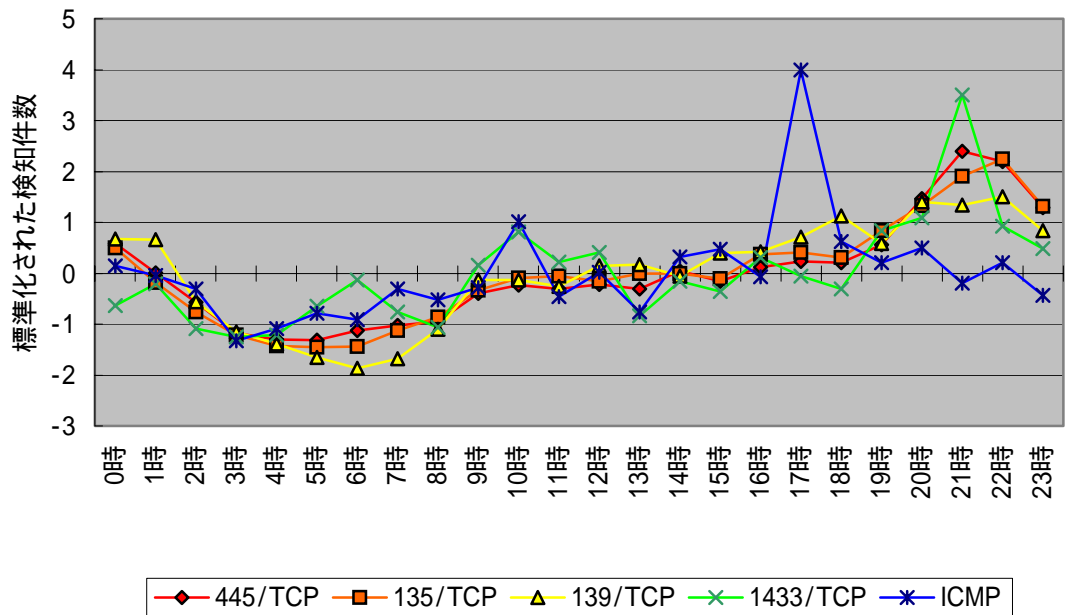
(4) 国/地域別比率



(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)

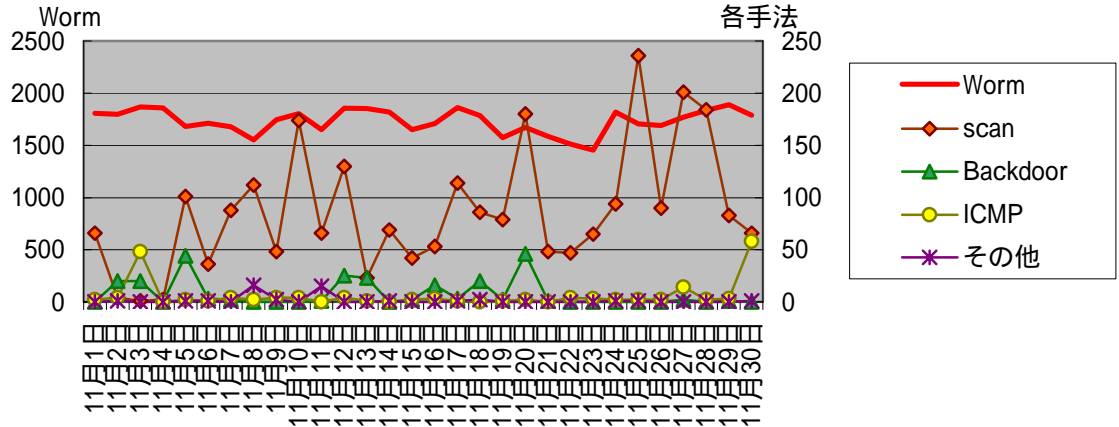


注) 件数は、宛先ポート毎に次の式により標準化した。

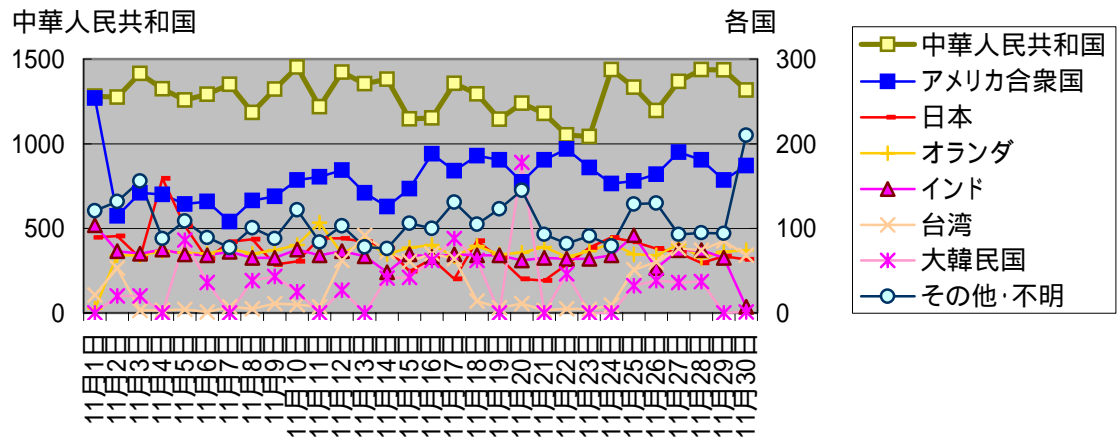
$$\text{標準化された検知件数} = (\text{その時間帯での検知件数} - \text{平均値}) / \text{標準偏差}$$

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

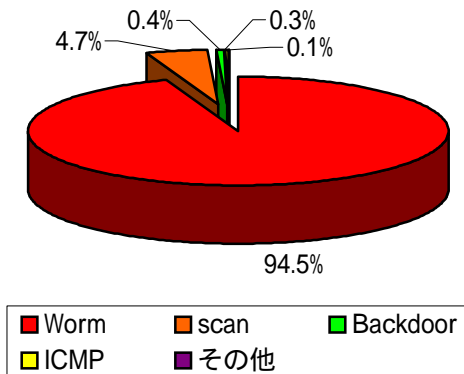
#### (1) 攻撃手法別遷移



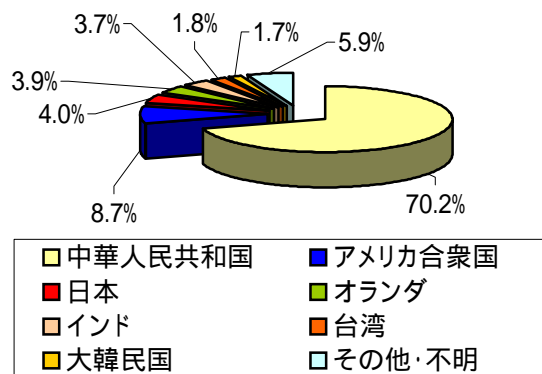
#### (2) 発信元国/地域別推移



#### (3) 攻撃手法別比率



#### (4) 発信元国/地域別比率



## 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。

### 不正侵入検知システム

各拠点の不正侵入検知装置には、平成 17 年 11 月現在、約 320 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。