

平成 17 年 10 月 12 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 9 月期)

1 概説

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 526,000 件であり、前月期比約 10%の減少であった。これは、445/TCP において増加が見られるものの、139/TCP、1433/TCP がそれぞれ、前月期比約 49%、32%減少していることが主な要因である。それにとともに、総アクセス数に占める 445/TCP のアクセス数の割合も増加している。また、Zotob ワーム等の活動に起因すると推測される 445/TCP のアクセス数は、当月期において減少傾向にあるものの、前月比約 15%増加していることから、Zotob ワーム等の活動に注意が必要である。

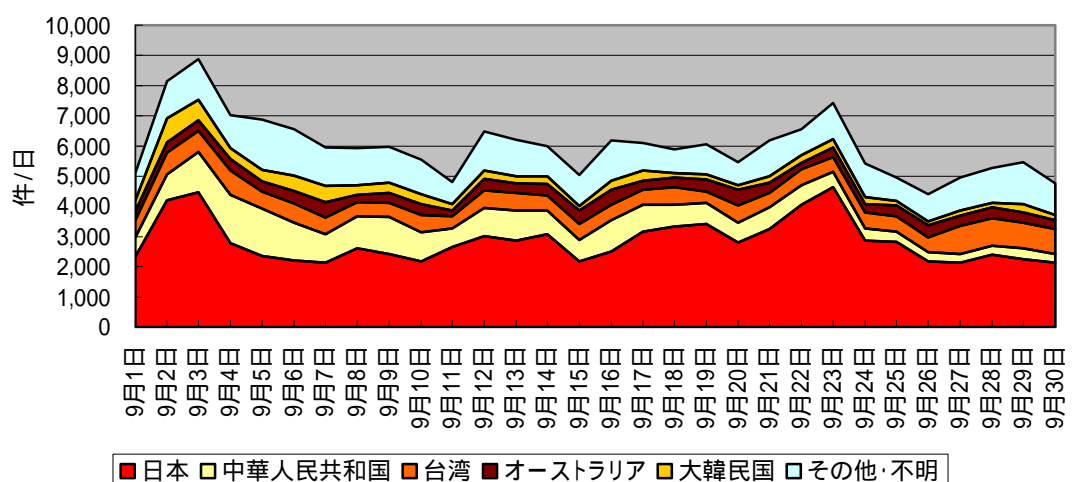
侵入検知システムにおけるアラート検知件数は約 46,000 件であり、前月比約 18%の減少であった。これは、攻撃手法における Worm (SQL Slammer) \ scan の検知件数がそれぞれ、前月比約 14%、58%減少したことが主な要因である。しかし、SQL Slammer の検知件数は、7 月期の後半において急増した水準を維持し、7 月期比約 45%増加しているので、引き続き注意が必要である。

2 インターネット定点観測

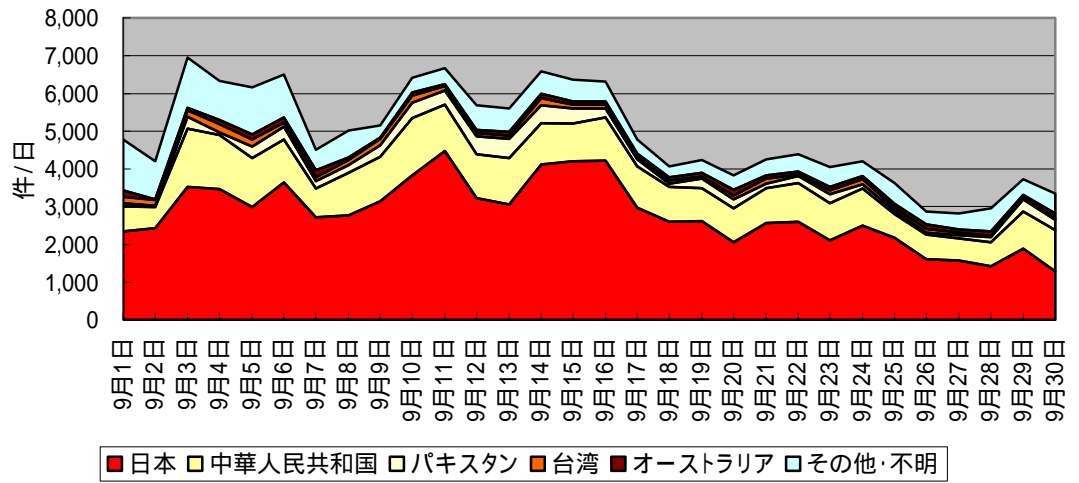
2.1 ファイアウォール / Firewall

(1) 宛先ポート別推移(上位 5 ポート、積み上げ)

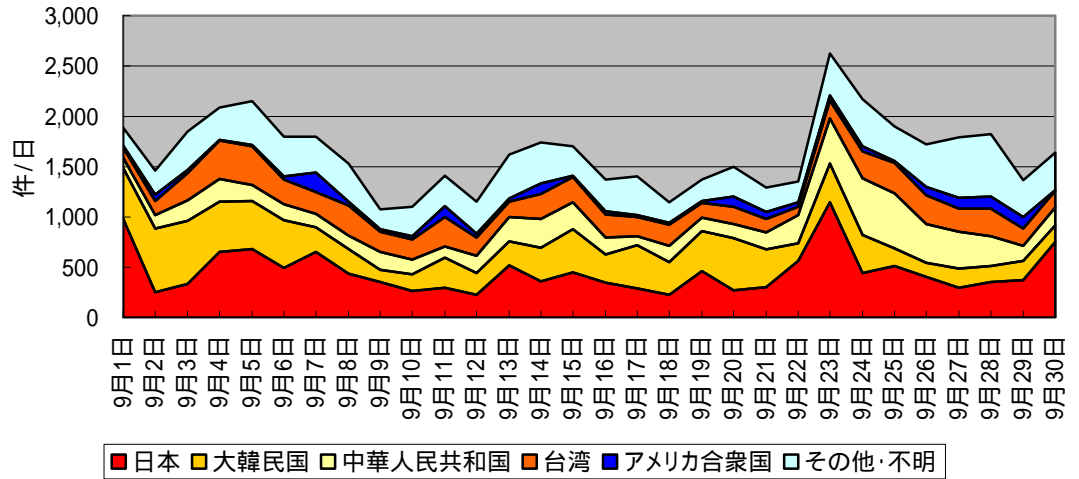
445/TCP



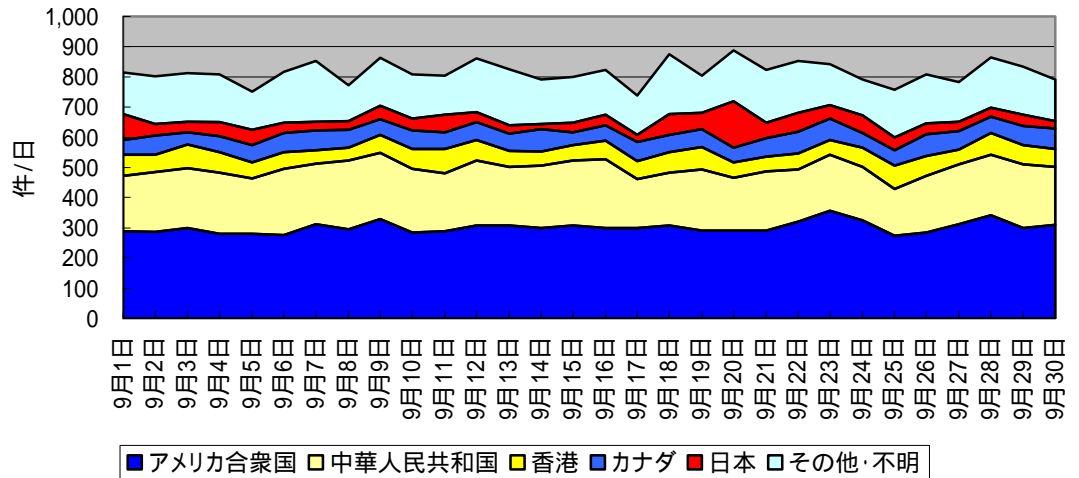
135/TCP



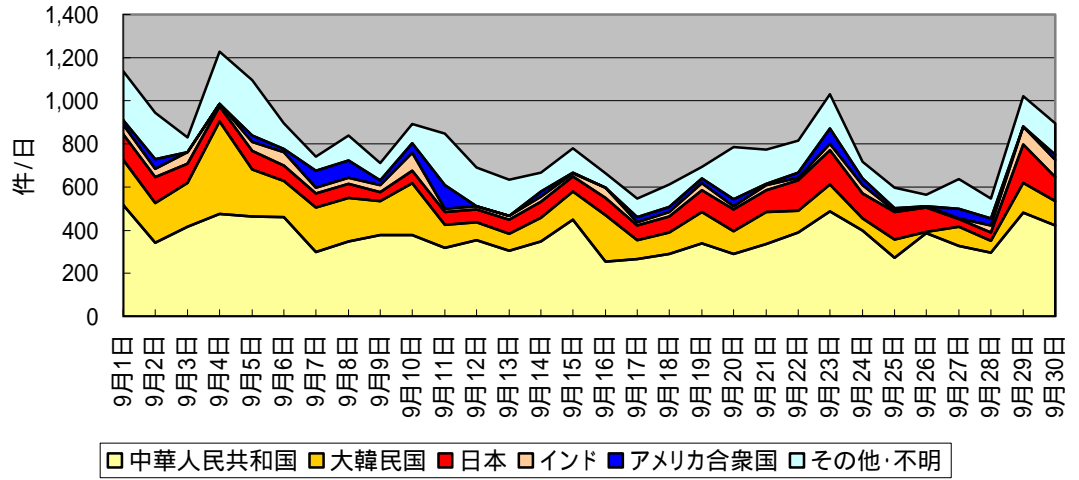
139/TCP



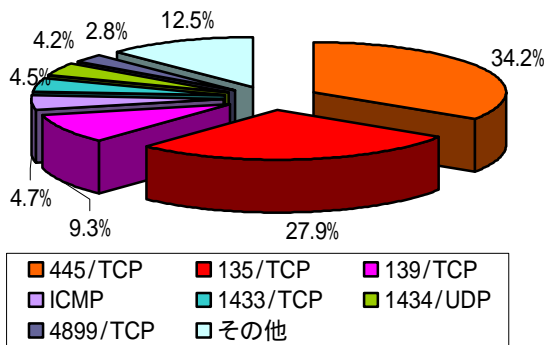
ICMP



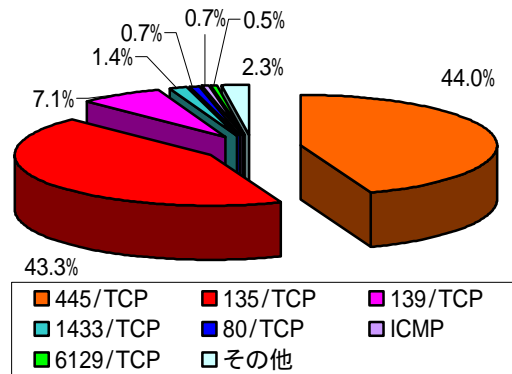
1433/UDP



(2) 宛先ポート別比率
発信元/全世界

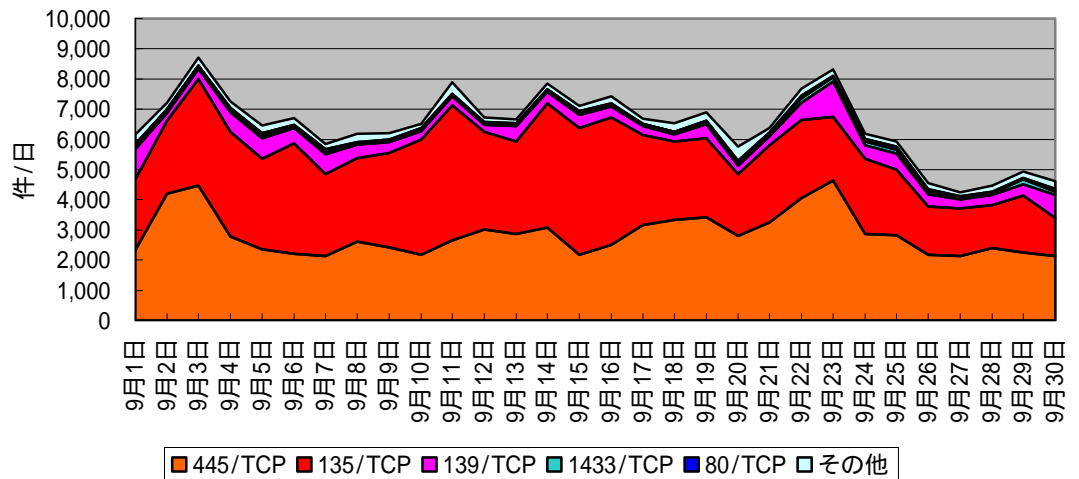


発信元/日本

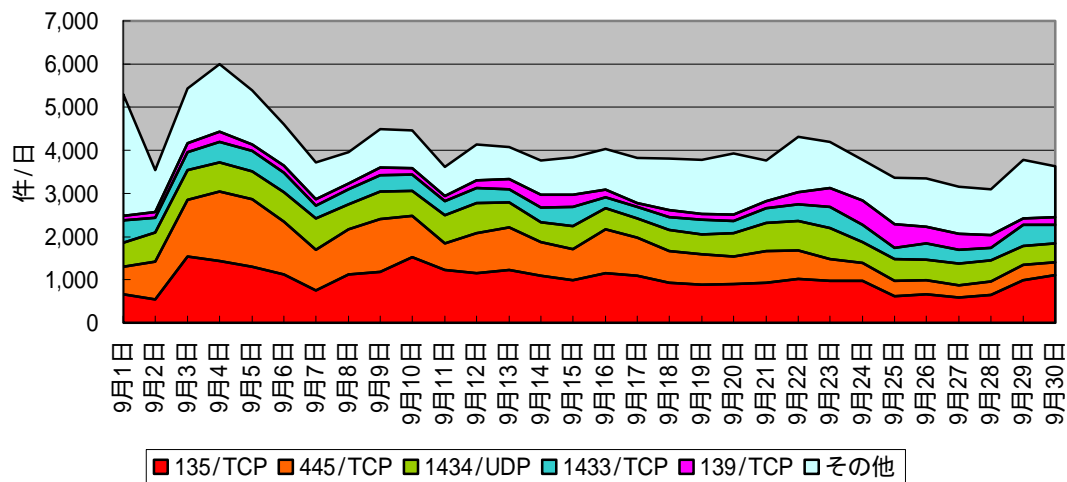


(3) 発信元国/地域別推移(上位5か国、積み上げ)

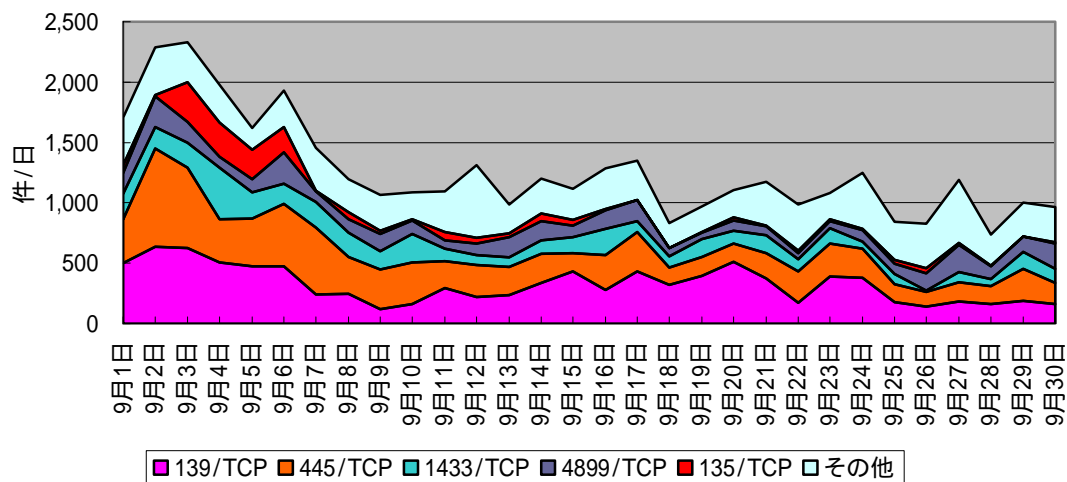
日本



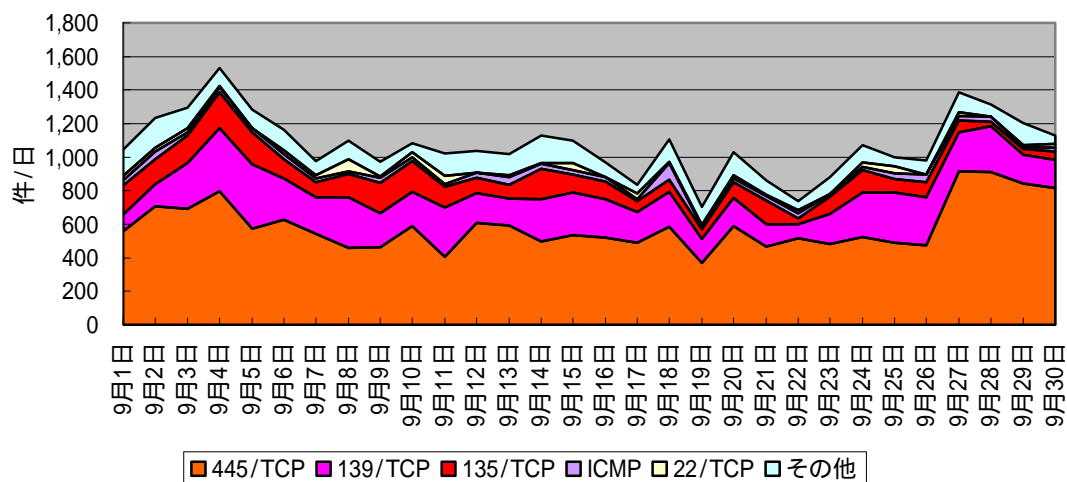
中華人民共和國



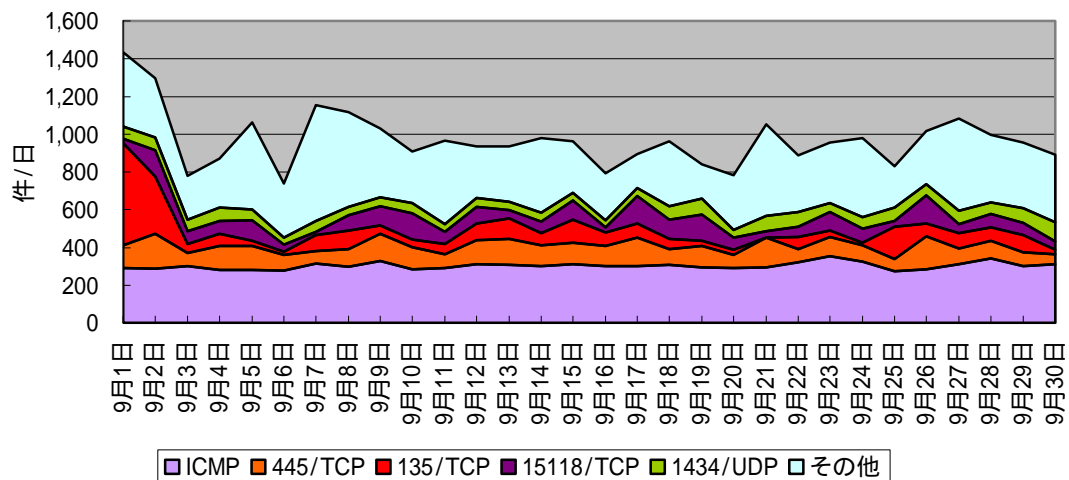
大韓民国



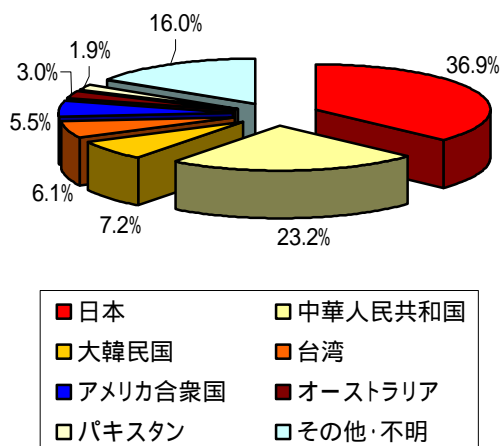
台湾



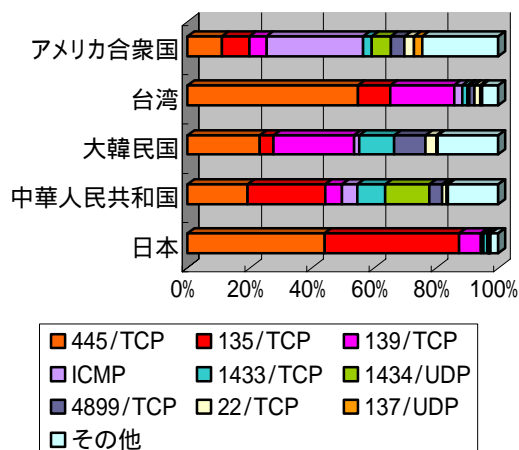
アメリカ合衆国



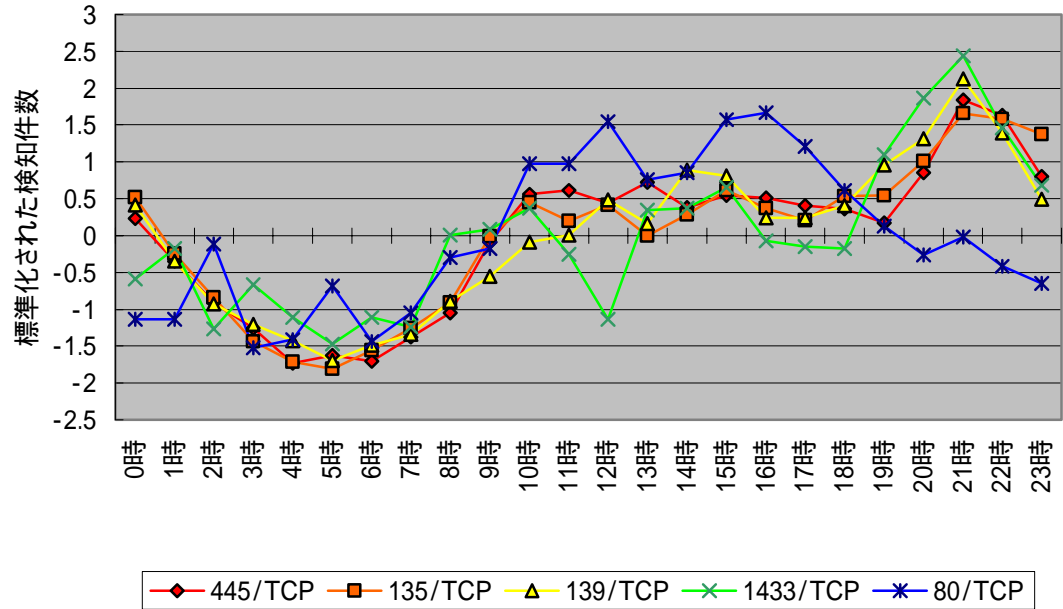
(4) 国/地域別比率



(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)

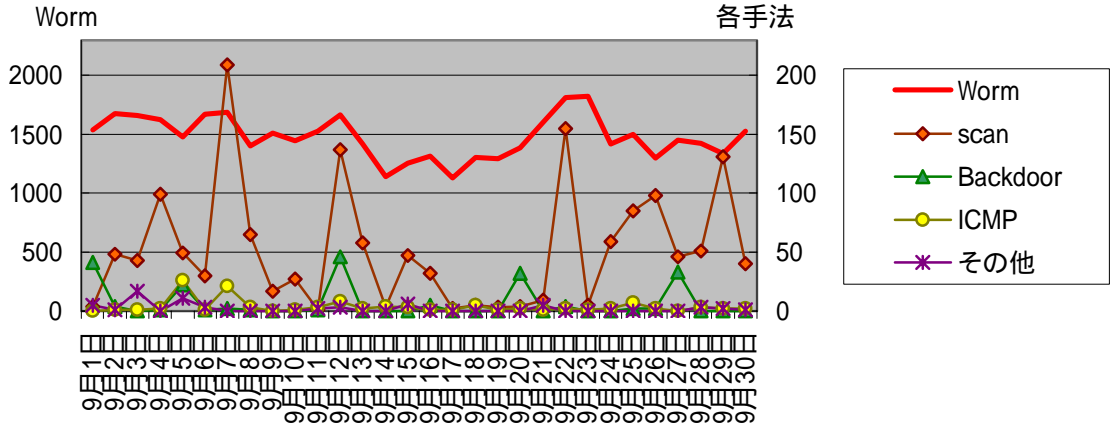


注) 件数は、宛先ポート毎に次の式により標準化した。

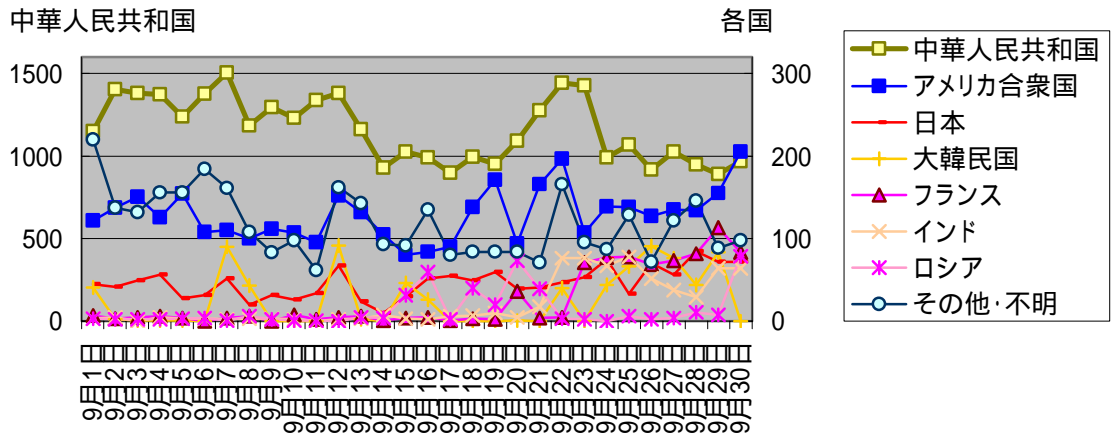
$$\text{標準化された検知件数} = (\text{その時間帯での検知件数} - \text{平均値}) / \text{標準偏差}$$

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

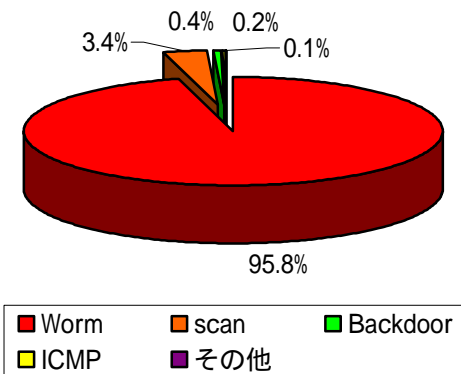
(1) 攻撃手法別遷移



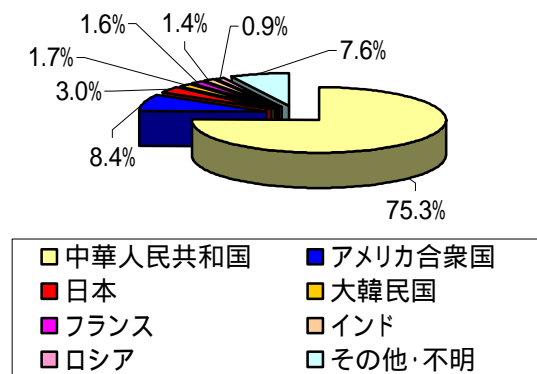
(2) 発信元国/地域別推移



(3) 攻撃手法別比率



(4) 発信元国/地域別比率



3 @police (Topics) 掲載事項

@police において9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
●	インターネット治安情勢更新(ネットワーク技術を悪用した個人情報の漏えいに注意を追加)(9/2)

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 9 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。