

平成 16 年 9 月 13 日

我が国におけるインターネット治安情勢について

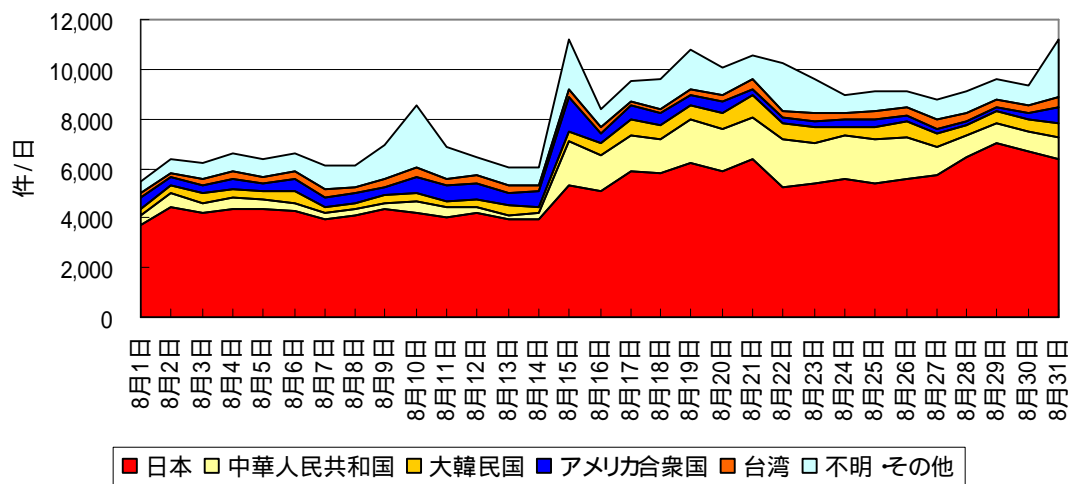
(平成 16 年 8 月期)

1 インターネット定点観測

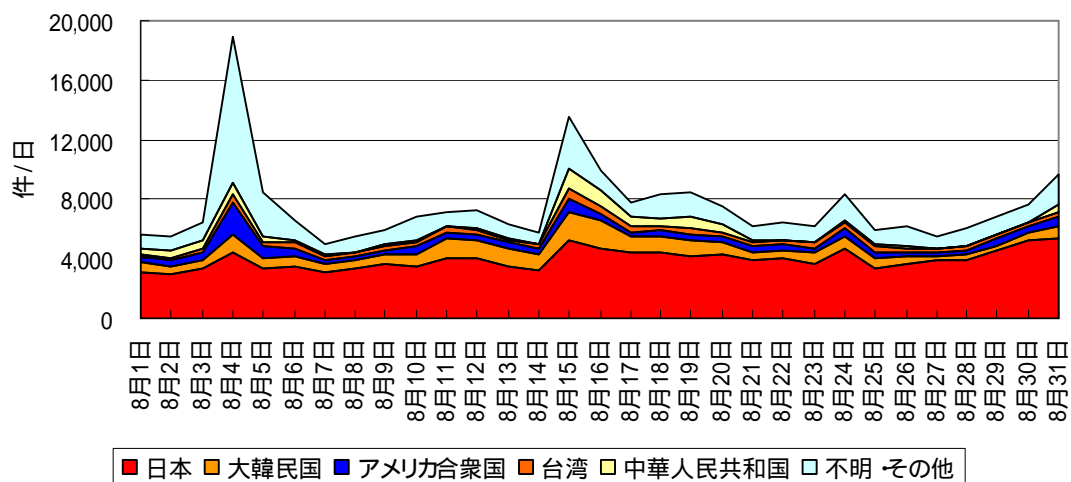
1.1 ファイアウォール / Firewall

(1) 宛先ポート別推移(上位 5 ポート、積み上げ)

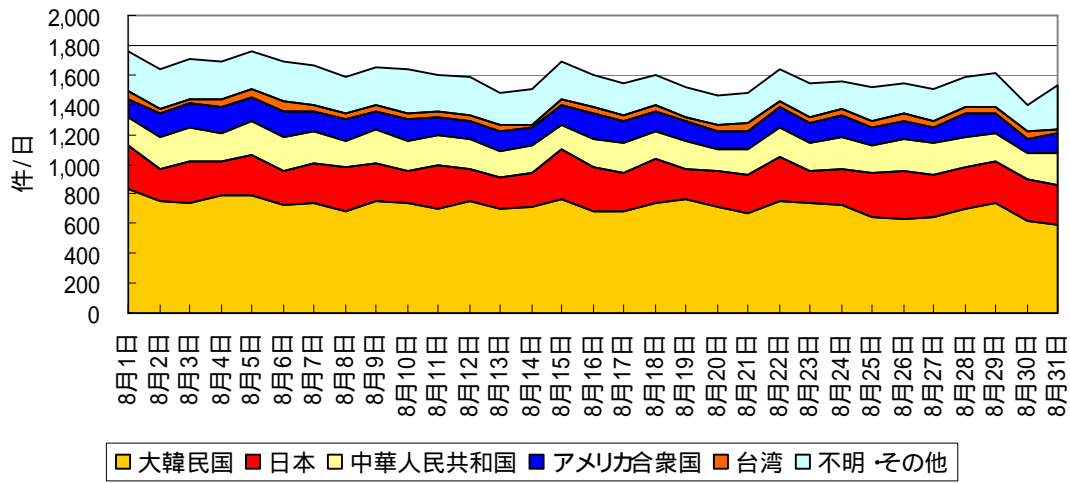
445/TCP



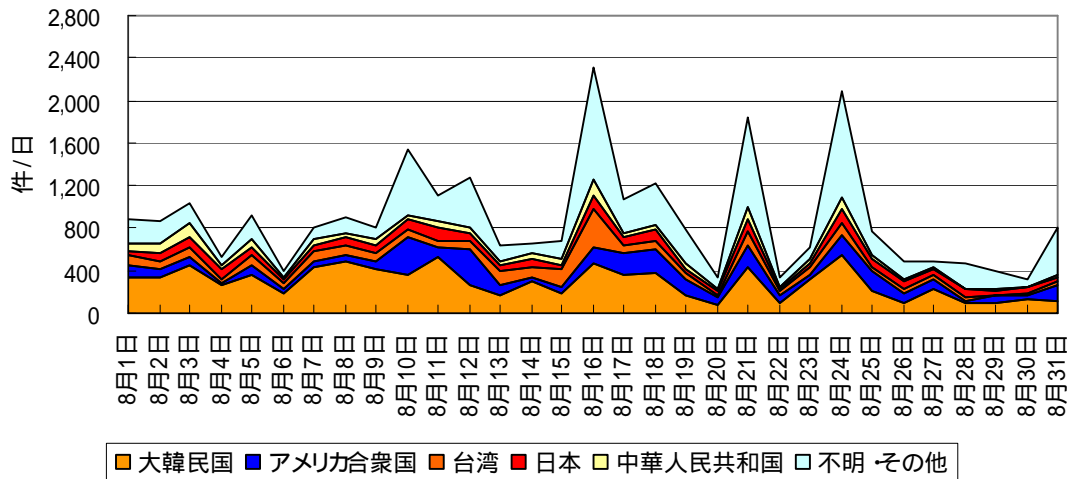
135/TCP



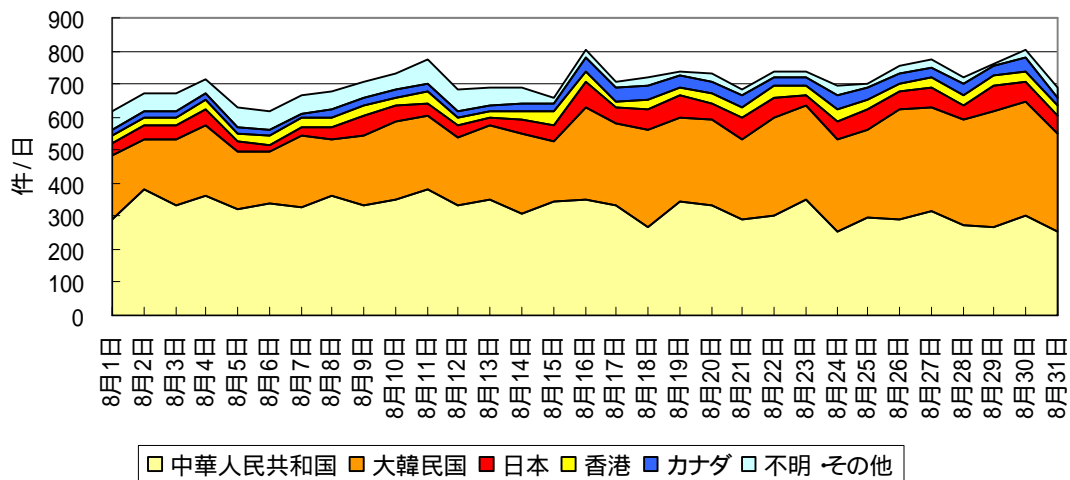
ICMP



139/TCP

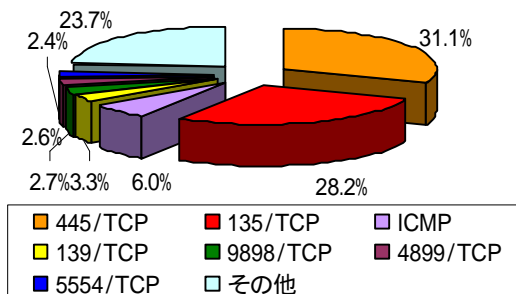


9898/TCP

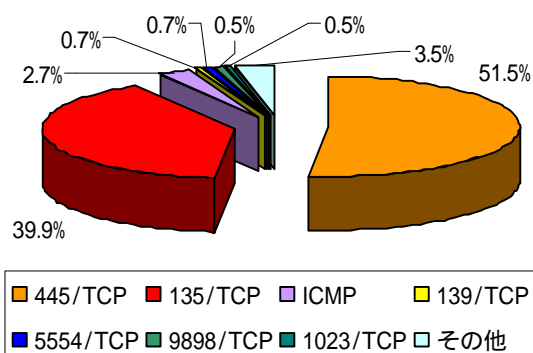


(2) 宛先ポート別比率

全世界

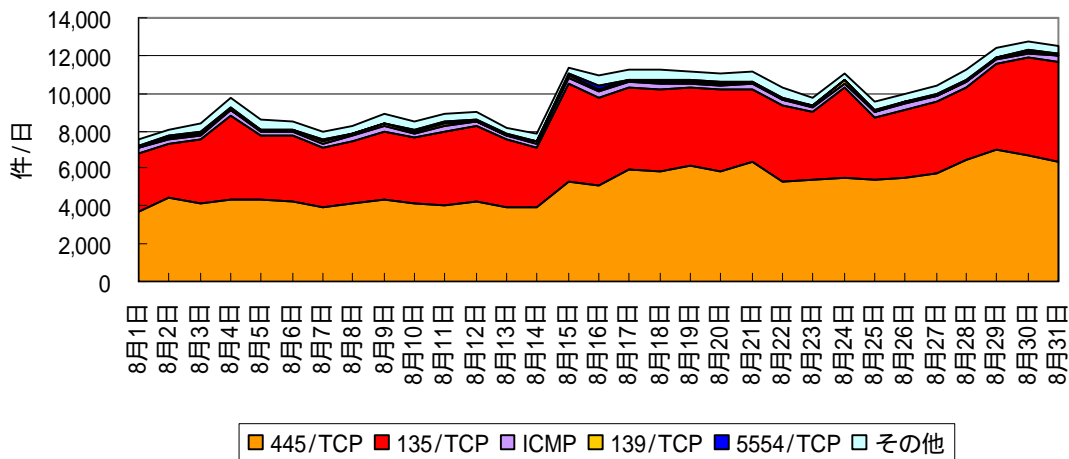


日本

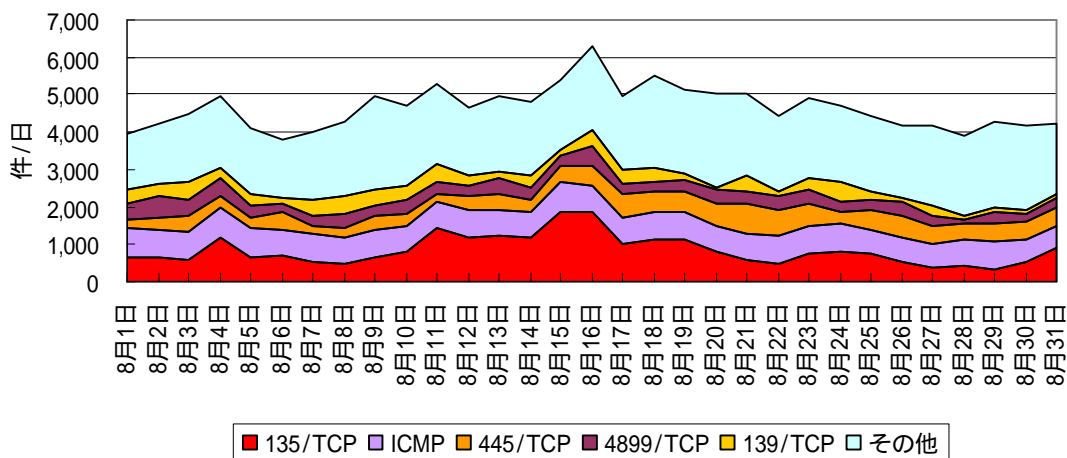


(3) 発信元国/地域別推移(上位5カ国、積み上げ)

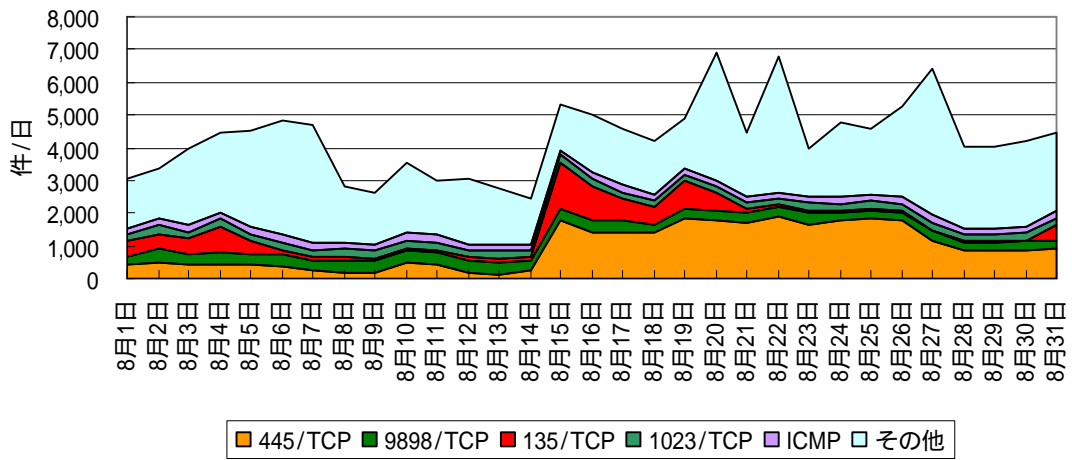
日本



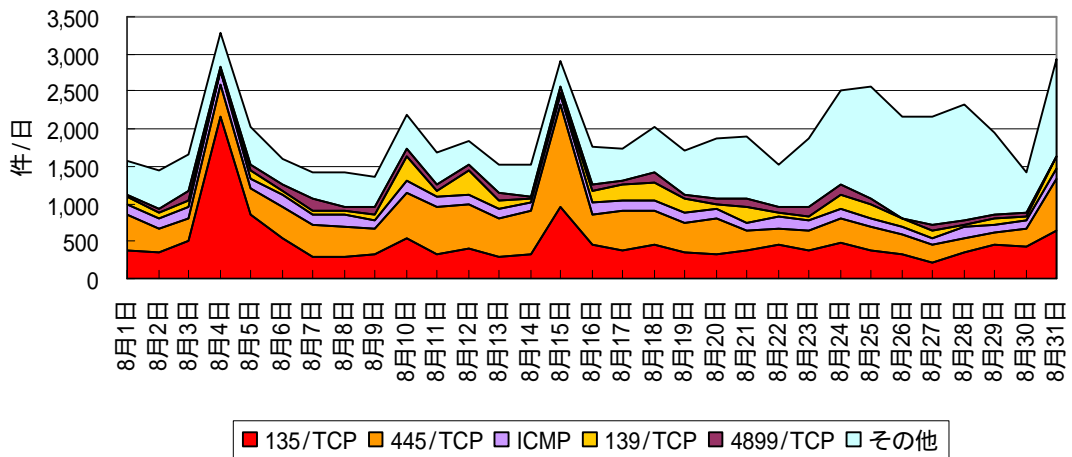
大韓民国



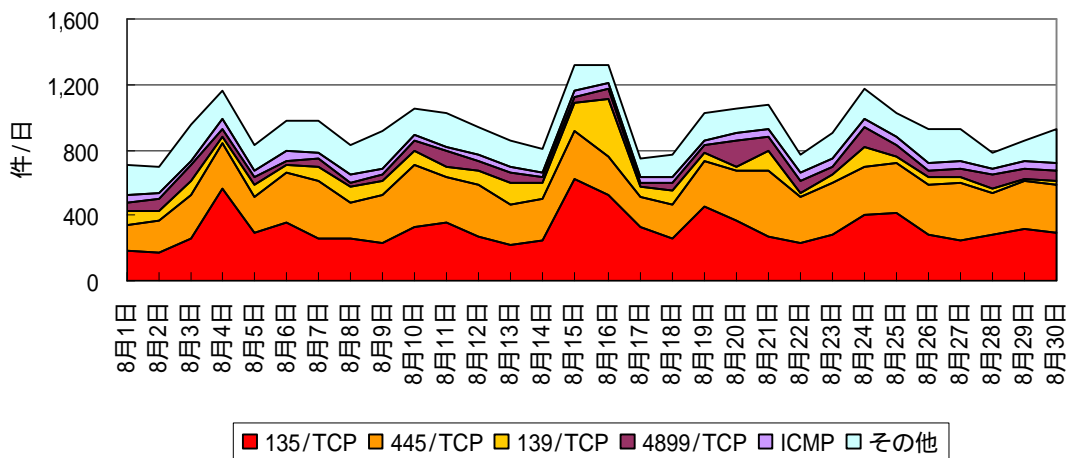
中華人民共和国



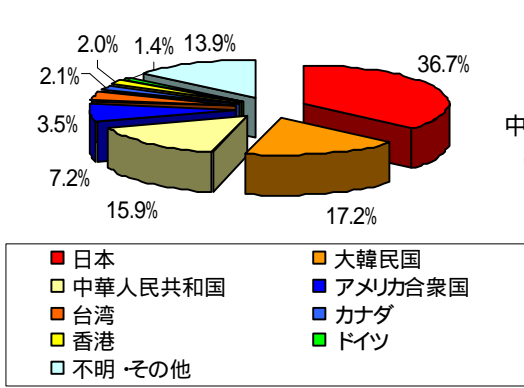
アメリカ合衆国



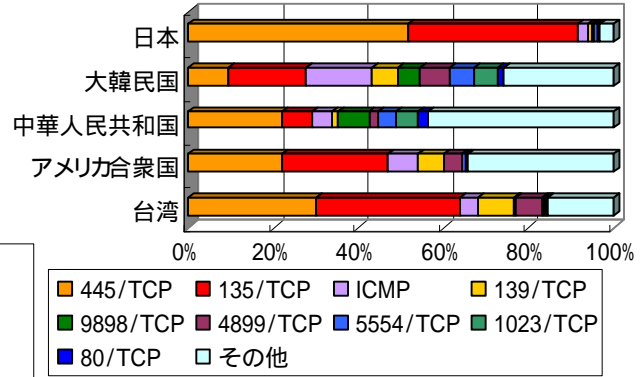
台湾



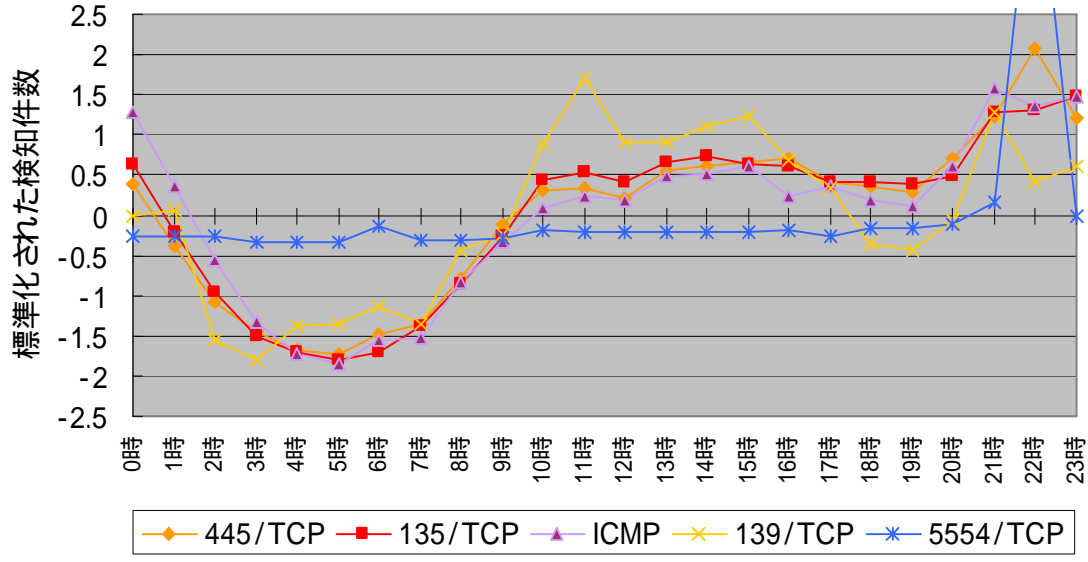
(4) 国/地域別比率



(5) 上位国/地域の宛先ポート別比率



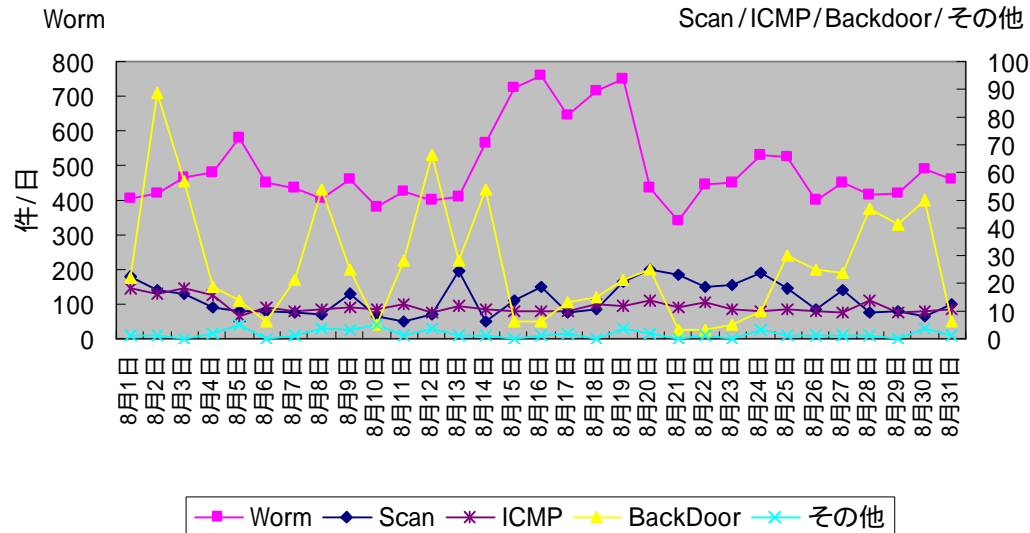
(6) 国内の時間帯推移(上位 5 宛先ポート)



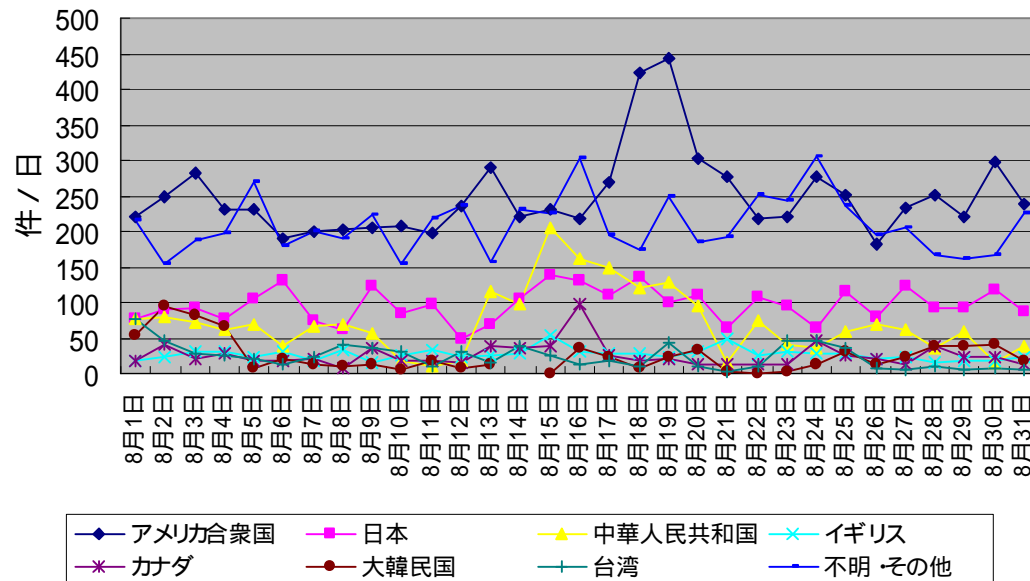
注) 標準化された検知件数 = (各時間帯の検知件数 - 平均値) / 標準偏差

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

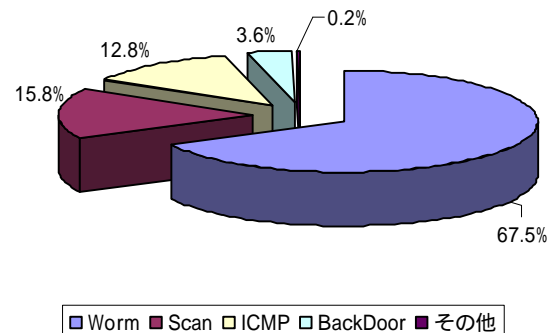
(1) 攻撃手法別推移



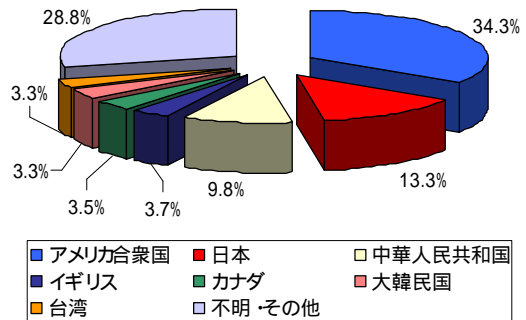
(2) 発信元国/地域別推移



(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 (抜粋)

@policeにおいて8月期の注意喚起等を行った主なものは次のとおり

分類	掲載事項
!重要	Beagle (Bagle) ウイルスについて(8/10)更新
!重要	Mydoom.Q ウイルスの蔓延について(8/16)
!重要	Cisco 社製ネットワーク機器の脆弱性について(8/28)

3 おわりに

当月期におけるファイアウォールのログ件数は約 822,000 件であり、先月に比べて約 1 割増加している。先月に引き続き、135/TCP 番ポート、445/TCP 番ポートに対するアクセスは高い水準で推移している。特に、8月中旬以降 445/TCP 番ポートへのアクセスが増加しているが、これは複数の IP からのパケットを富山・山形の 2 拠点で大量に検知したことによる。発信元 IP は広範囲にわたっているものの、そのほとんどは IP アドレスの第一オクテットが 2 拠点と同一であり、日本と中華人民共和国からが多数を占めた。

今回のファイアウォールの統計の上位 5 ポート内に 9898/TCP 番ポートが現れているが、これは日本時間 23 時前後に観測されている 1023/TCP、5554/TCP、9898/TCP 番ポートに対する Dabber.B ワームの感染活動によるアクセスが原因である。これらのポートに対するアクセスは、6月上旬から継続しているが、前月までが中華人民共和国からのアクセスが主であったのに対し、当月からは大韓民国からのアクセスも増加している。

侵入検知システムによるアラート件数は約 22,500 件であり、先月に比べて約 1 割減少している。これは SQL Slammer ワームによる検知件数が先月と比較して 3300 件程減少したことが主な要因である。国別の検知件数を先月と比較すると、日本からが約 1100 件、中華人民共和国からが約 750 件、台湾からが約 570 件減少している。一方、アメリカ合衆国からは約 220 件増加している。

ウイルス、ワームに関しては、電子メールを通じて感染活動を行う Beagle ウイルス、Mydoom ウイルスの亜種が新たに発生しており、@police において注意喚起を行った。

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 16 年 1 月現在、約 350 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 Hostname Overflow Attack, DNS HINFO decode, DNS Length Overflow Attack, DNS named iquery attempt, named version attempt
DoS	SYN Flood, UDP Bomb, UDP Flood, Stick Attack, Land, Teardrop
ICMP	PING NMAP, Superscan Echo, redirect host, redirect net, Large ICMP Packet, Ping Flooding, SMURF attack
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 5 つを除くもの

- シグネチャは随時追加している。