

平成 18 年 3 月 14 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 2 月期)

- ・ファイアウォールに対するアクセスに増加傾向
- ・日本を発信元とする 135/TCP ポートへのアクセスが増加
- ・不正侵入検知システムにおけるアラートは増減なし

1 概説

平成 18 年 2 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 510,000 件で、一日当たりでは約 18,200 件/日(対前月比 + 32%)と増加した。今回のアクセス増加の主な要因は、IP アドレスの近い PC をねらって感染活動を行うワーム等によると考えられる 135/TCP に対するアクセスの増加であり、日本を発信元とするアクセス件数が大幅に増加している。宛先ポート別では、上位 5 位までの順位に変化はないが、前述した 135/TCP と同様にワーム等の攻撃によると思われる 445/TCP に対するアクセス件数も増加した。135/TCP、445/TCP と並んでワーム等の感染活動に悪用される 139/TCP は、1 月期に引き続き減少傾向を示している。発信元/国地域別では、上位 5 位までの順位に変化はないが、第 1 位の日本を発信元とするアクセス件数が、135/TCP に対するアクセス増加のため大幅に増加している。前月期には減少傾向であった 135/TCP に対するアクセスが大幅に増加していることから、135/TCP の脆弱性を狙ったワーム等に注意が必要である。

不正侵入検知システムにおけるアラート検知件数は約 38,000 件で、一日当たりの検知件数は約 1,350 件/日(対前月比 + 2.4%)であった。攻撃手法別において第 1 位の Worm (SQL Slammer) は、1 月期と同様、全体の 9 割を占めている。発信元国/地域別では、上位 5 位までの順位に変化はなく中華人民共和国、アメリカ合衆国、日本、大韓民国、台湾となっている。

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)

1 月期と 2 月期における上位 5 ポートは以下のとおりである。上位 5 ポートについて、順位に変化はなかった。

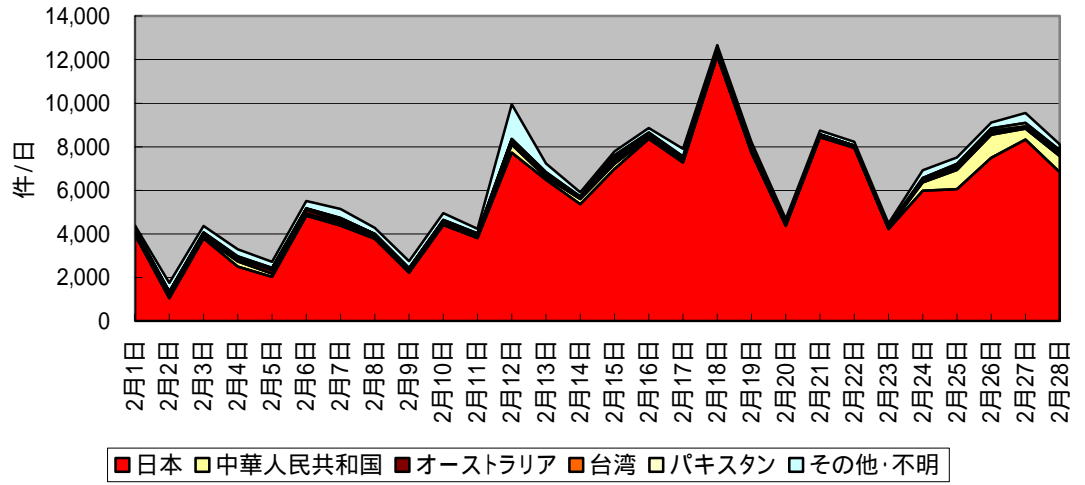
	1 月期	2 月期
1 位	135/TCP	135/TCP
2 位	445/TCP	445/TCP
3 位	139/TCP	139/TCP
4 位	ICMP(Echo Request)	ICMP(Echo Request)
5 位	1433/TCP	1433/TCP

1 月期に減少傾向を示していた 135/TCP に対するアクセス件数は、大幅に増加した。2 月期の一日当たりのアクセス件数は、約 6,400 件/日であり、1 月期と比較すると約 +2,900 件/日(約 +85%)と大きく増加している。これは 2 月 12 日以降日本を発信元とするアクセス件数が増加していることが主な要因である。135/TCP は、多くのワーム等が感染活動に悪用するポートである。これらの中には、感染した PC と IP アドレスが近い PC をねらって感染活動を行うものがある。今月期の 135/TCP に対するアクセスの約 82%が、送信元 IP アドレスと送信先 IP アドレスの第 1、第 2 オクテットが等しいものであり、今月期に日本を発信元とするアクセスが増加した要因は、このようなワーム等の感染活動が活発化したためであると推測される。

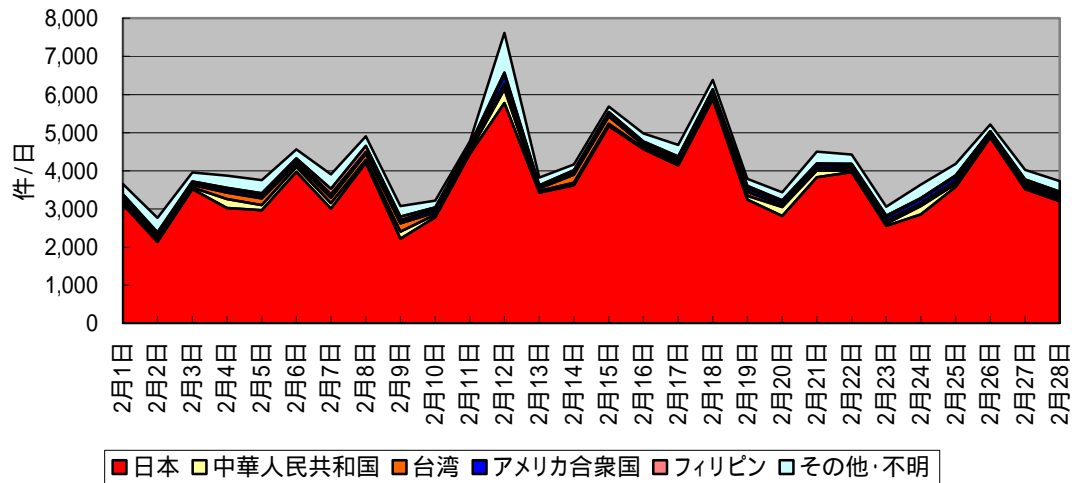
445/TCP に対する 1 日当たりのアクセス件数は、約 4,300 件/日であった。445/TCP に対するアクセス件数は、2005 年 10 月期以降減少傾向を示していたが、前月比約 +820 件/日(約 +24%)と増加した。

139/TCP に対する 1 日当たりのアクセス件数は、約 1,200 件/日であった。1 月期と比較すると約 -210 件/日(約 -14%)減少した。

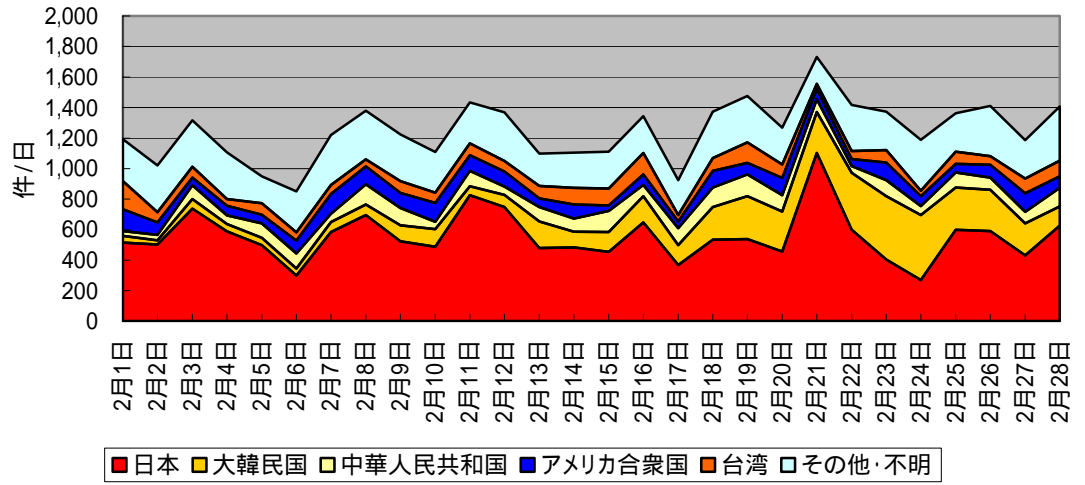
135/TCP



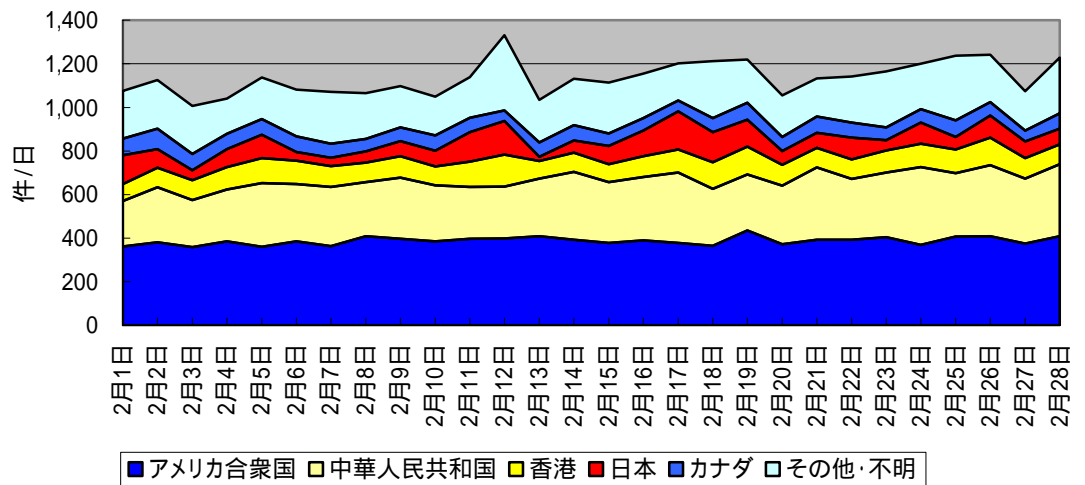
445/TCP



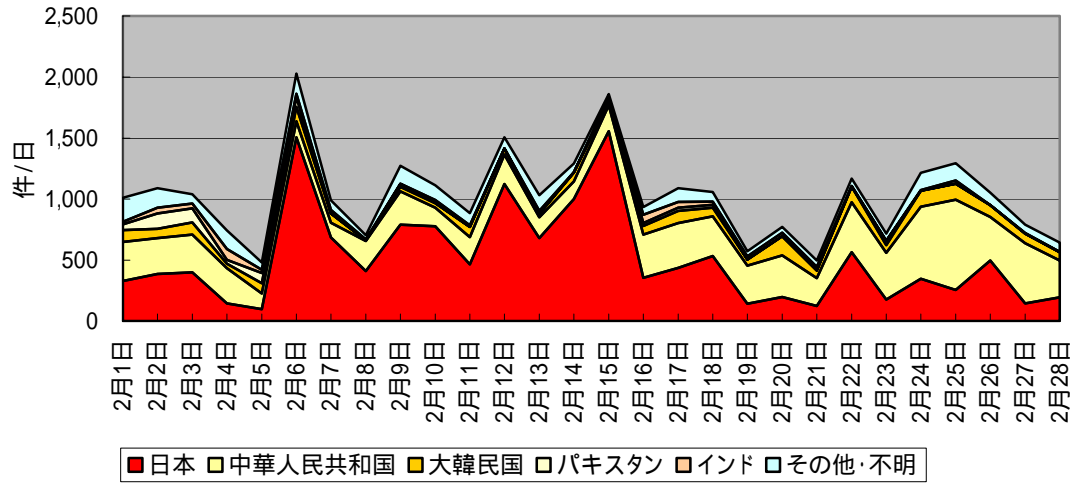
139/TCP



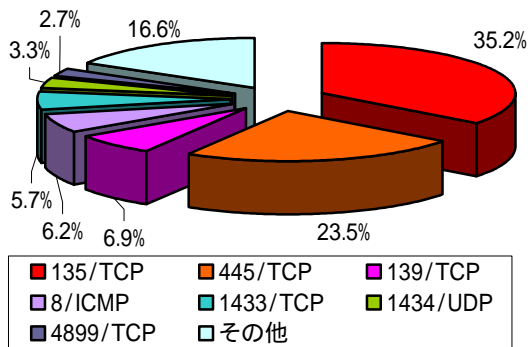
ICMP(Echo Request)



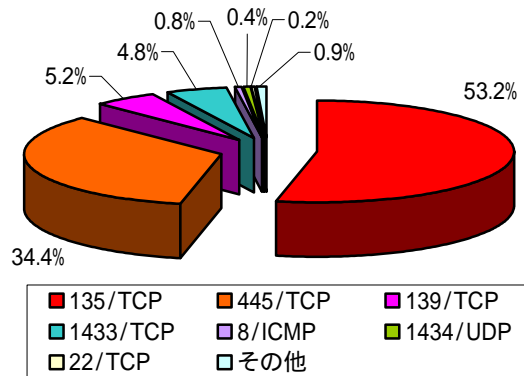
1433/TCP



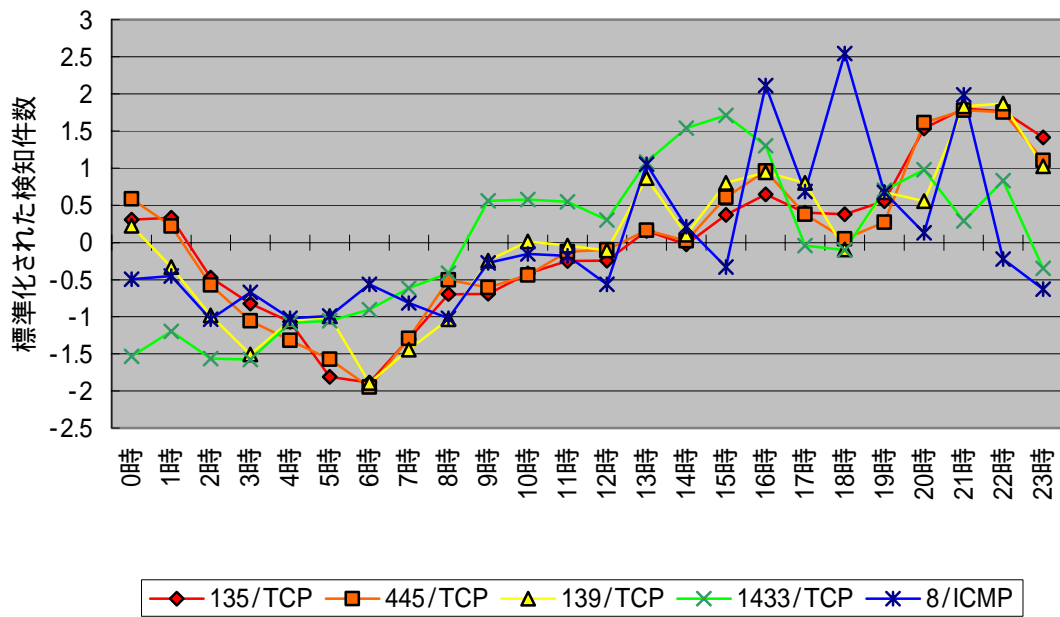
(2) 宛先ポート別比率 発信元/全世界



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)

1 月期と 2 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。上位 5 か国の順位に変化は見られなかった。

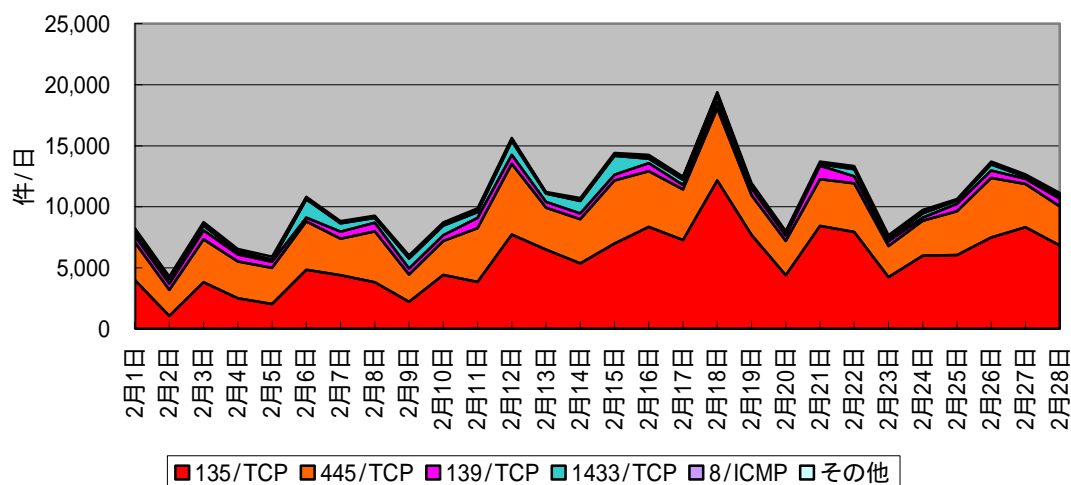
	1 月期	2 月期
1 位	日本	日本
2 位	中華人民共和国	中華人民共和国
3 位	アメリカ合衆国	アメリカ合衆国
4 位	大韓民国	大韓民国
5 位	台湾	台湾

日本を発信元とするアクセスの一日当たりのアクセス件数は約 10,600 件/日で、1 月期と比較すると約 +4,440 件/日(約 +72%)と大幅に増加した。今回の増加の要因は、前述した 2 月 12 日から 135/TCP に対するアクセス件数が増加したためである。日本を発信元とする 135/TCP に対する一日当たりのアクセス件数を 1 月期と比較すると約 2.2 倍に増加している。

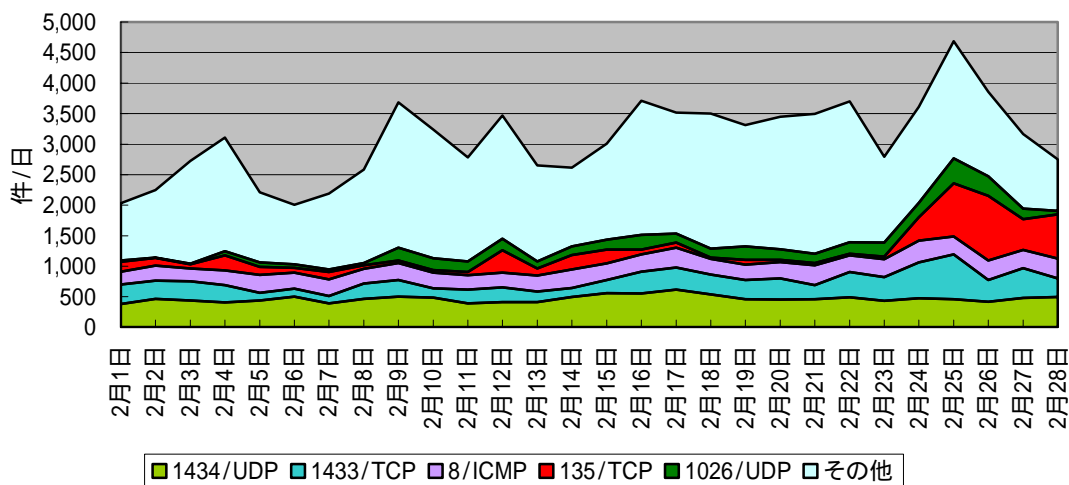
中華人民共和国を発信元とするアクセスの一日当たりの件数は、1 月期と比較して約 +17%と若干の増加が見られた。2 月 24 日以降、135/TCP に対するアクセス件数が、増加している。

アメリカ合衆国を発信元とするアクセスの一日当たりの件数は、1 月期と比較して、約 +8%と若干の増加が見られた。大韓民国、台湾については、いずれも 1 月期と比較して減少している。

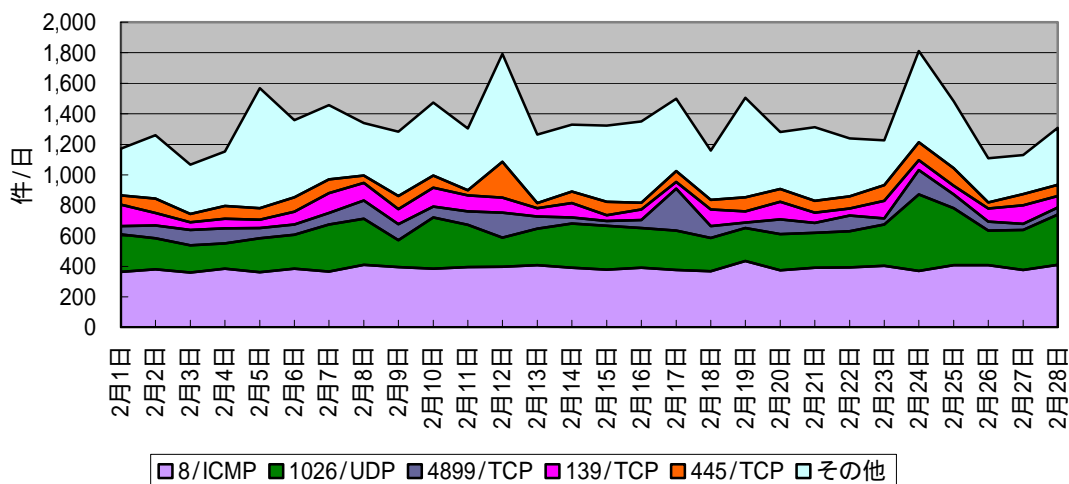
日本



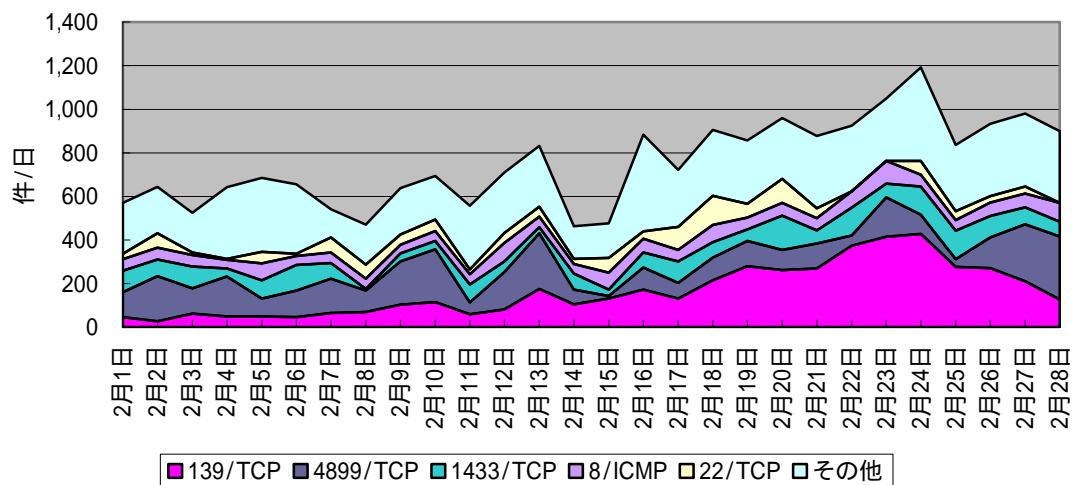
中華人民共和國



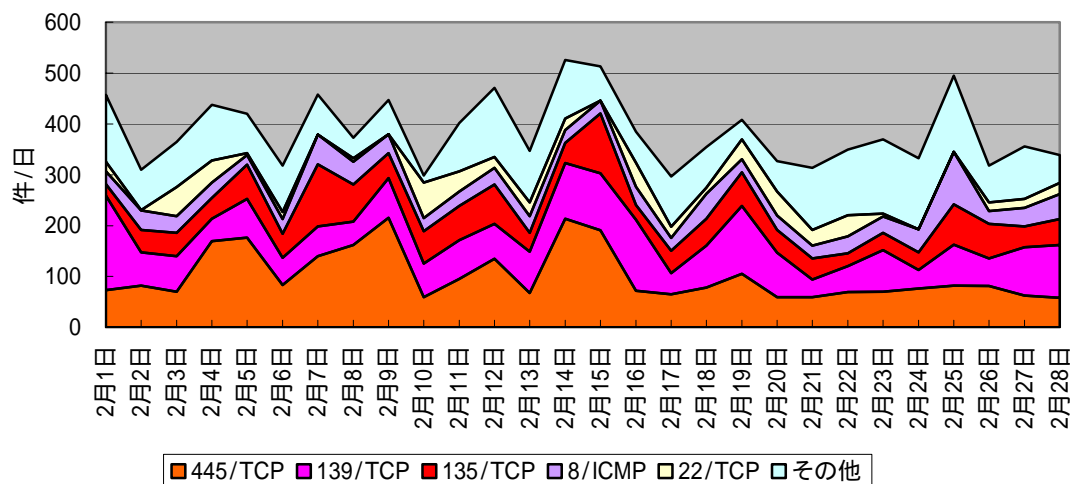
アメリカ合衆国



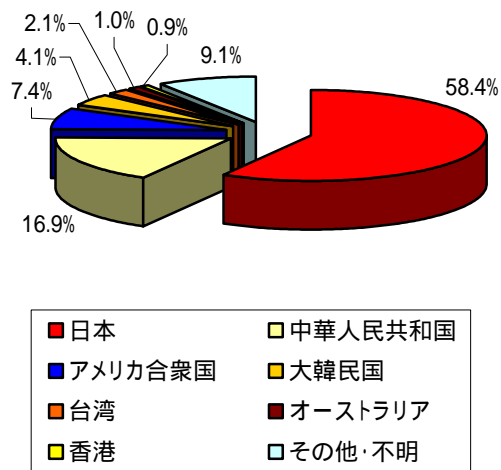
大韓民国



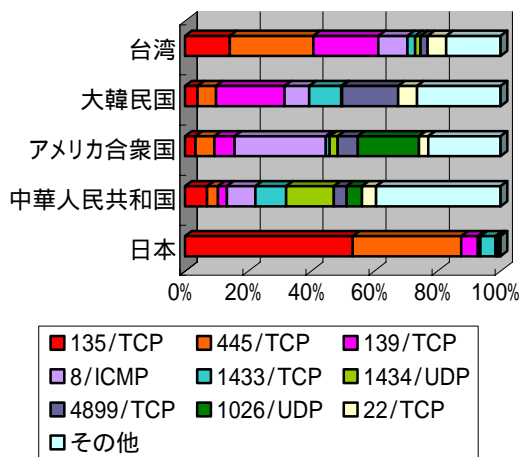
台湾



(5) 国 / 地域別比率

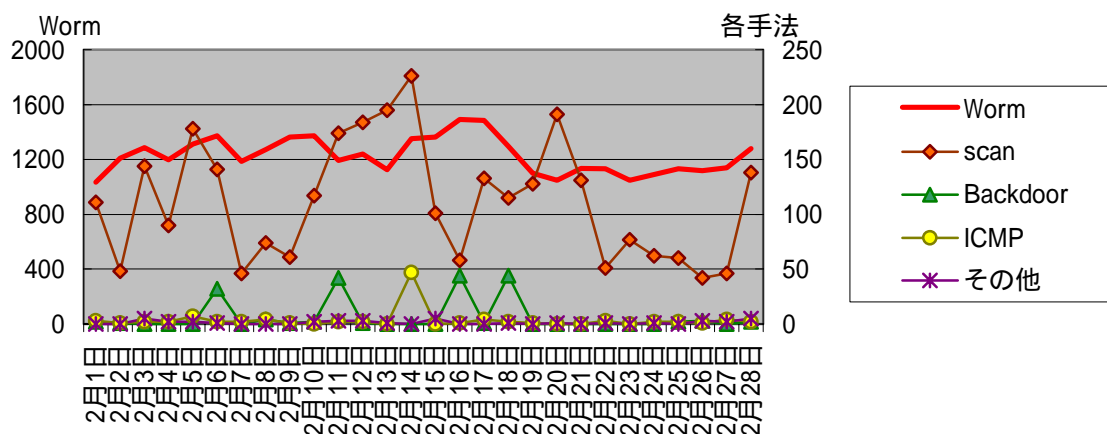


(6) 上位国 / 地域の宛先ポート別比率



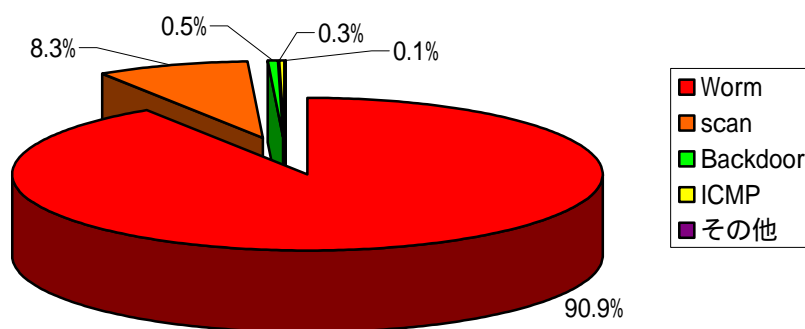
2.2 不正侵入検知システムにおけるアラート検知分析

(1) 攻撃手法別推移

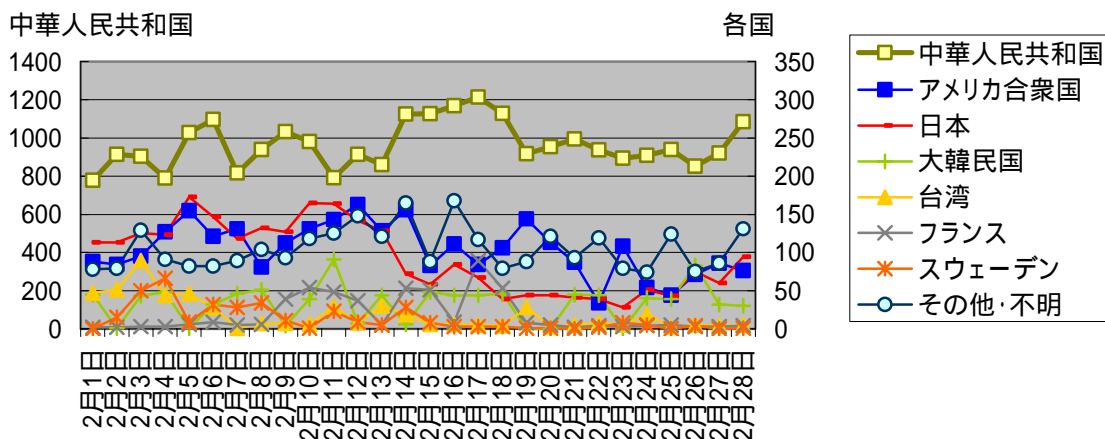


第1位のWorm(SQL Slammer)の一日当たりの検知件数は約1,200件/日であり、1月期と比較して大きな増減はなかった。中華人民共和国のWormの一日当たりの検知件数が減少(1月期比約-3%減)している一方で、日本を発信元とする検知件数が増加(1月期比約+30%増)している。

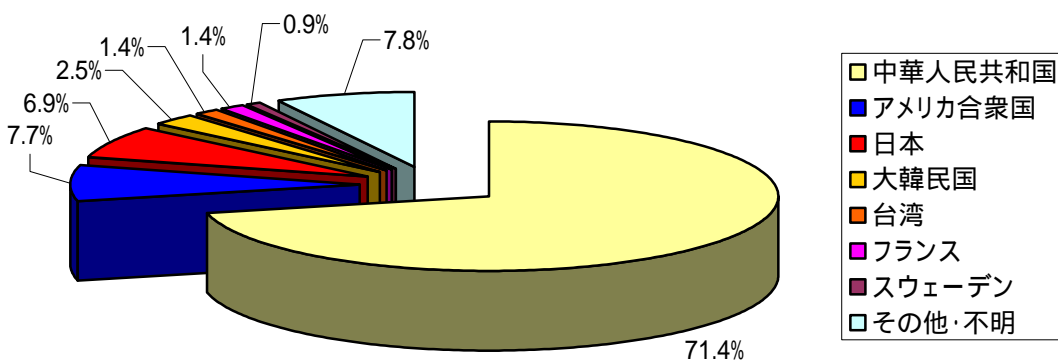
(2) 攻撃手法別比率



(3) 発信元国 / 地域別推移





(4) 発信元国 / 地域別比率



3 @police (Topics) 掲載事項

@police において2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
 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 (MS06-004,005,006,007,008,009,010)(2/15)
 重要	Java Runtime Environment(JRE)等の脆弱性について(2/9)

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¹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 2 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。

¹ グラフの凡例においては、スラッシュの前にタイプを付け加えている。