

平成 18 年 8 月 22 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 7 月期)

- ・ファイアウォールに対するアクセスは増加
～日本を発信元とするアクセスが増加～
- ・不正侵入検知システムにおけるアラートはやや減少
～中華人民共和国を発信元とするアクセスが増加～
～SOCKS Proxy へのスキャンなどが増加～

1 概説

平成 18 年 7 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 433,179 件で、一日当たり約 13,974 件（対前月比 + 13.6%）と増加した。この増加の主な要因として、日本を発信元とするアクセスが増加（対前月比 + 21.0%）したことが挙げられる。一方、宛先ポート別の上位 5 位までの順位は、6 月期と変わらず 135/TCP、445/TCP、ICMP(Echo Request)、139/TCP、1433/TCP の順であった。

不正侵入検知システム におけるアラート検知件数は約 42,418 件で、一日当たりの検知件数は約 1,368 件（対前月比 - 2.3%）であった。攻撃手法別において第 1 位の Worm（SQL Slammer）は、6 月期とほぼ同様に、全体の約 9 割を占めた。また、発信元国 / 地域別において、上位は、中華人民共和国、大韓民国、アメリカ合衆国、日本、台湾、インドの順であった。中華人民共和国を発信元とするアラートが増加し、インドが大幅に減少した。攻撃手法としては、SOCKS Proxy（企業などの内部ネットワークとインターネットを接続するために配置されるもの）へのスキャンなどが顕著であった。

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

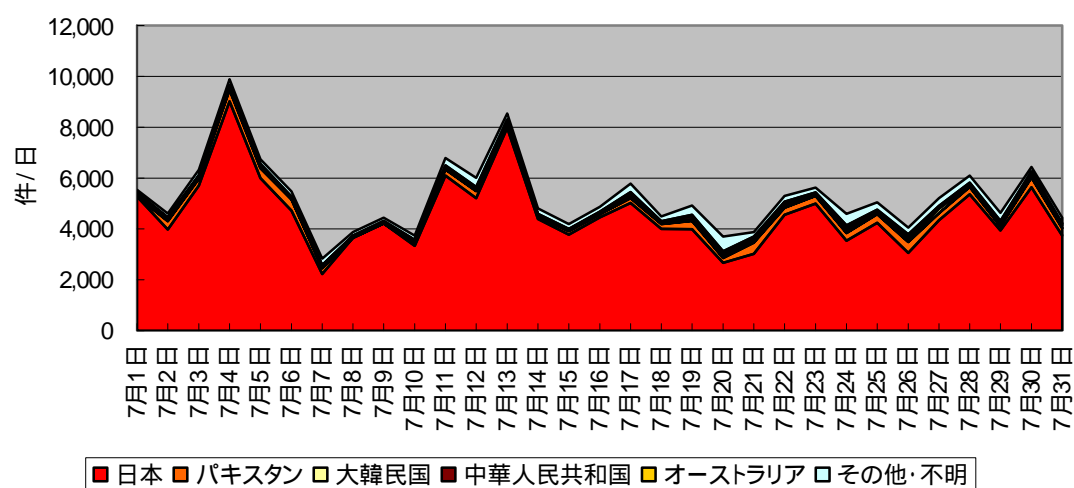
2.1 ファイアウォールに対するアクセス分析

(1) 宛先ポート別推移(上位5ポート、積み上げ)

6月期と7月期における上位5ポートは以下のとおりである。順位に変動は見られなかった。また、7月期一日当たりのアクセス件数及び6月期との増減比較を、表の右側に示す。

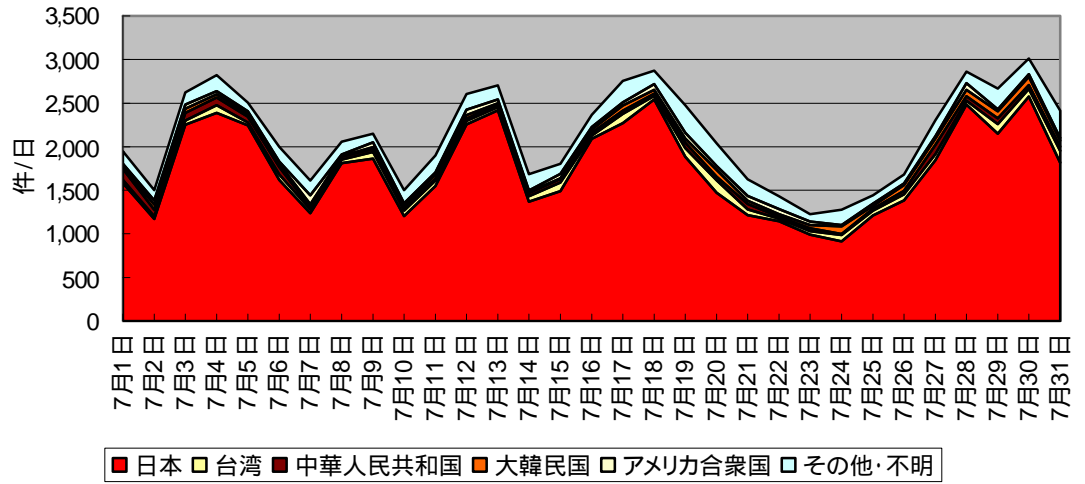
	6月期	7月期	7月期一日当たり	一日当たりの増減
1位	135/TCP	135/TCP	約 5,253 件	約 + 883 件 (約 + 20.2%)
2位	445/TCP	445/TCP	約 2,125 件	約 + 505 件 (約 + 31.1%)
3位	ICMP(Echo Request)	ICMP(Echo Request)	約 1,238 件	約 - 12 件 (約 - 1.0%)
4位	139/TCP	139/TCP	約 837 件	約 + 107 件 (約 + 14.7%)
5位	1433/TCP	1433/TCP	約 714 件	約 + 34 件 (約 + 5.0%)

135/TCP



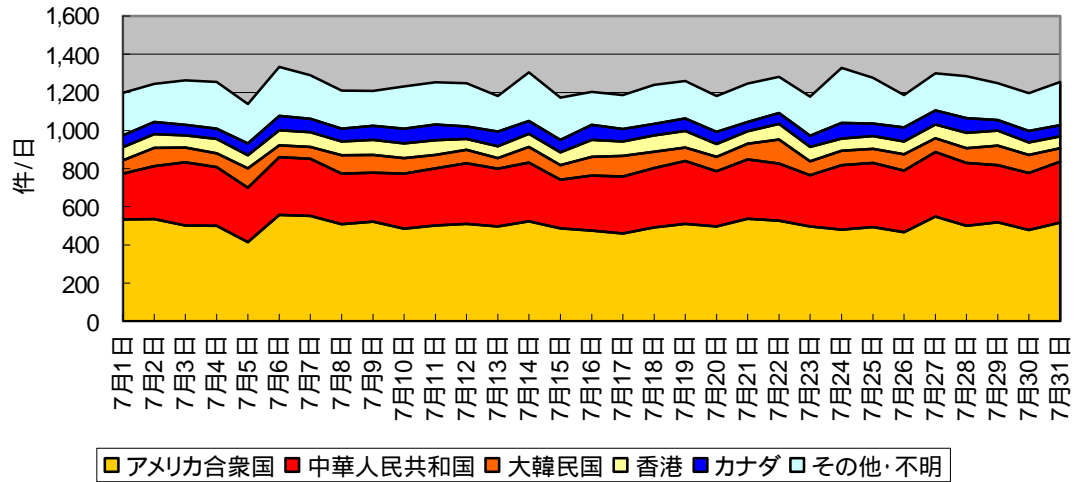
中華人民共和国からのアクセスが半減する一方、アクセスの大半を占める日本国内からのアクセスが増加したことから、全体としては増加となった。3日から5日にかけてアクセス増加が顕著であるが、これは特定ホストからのものである。

445/TCP



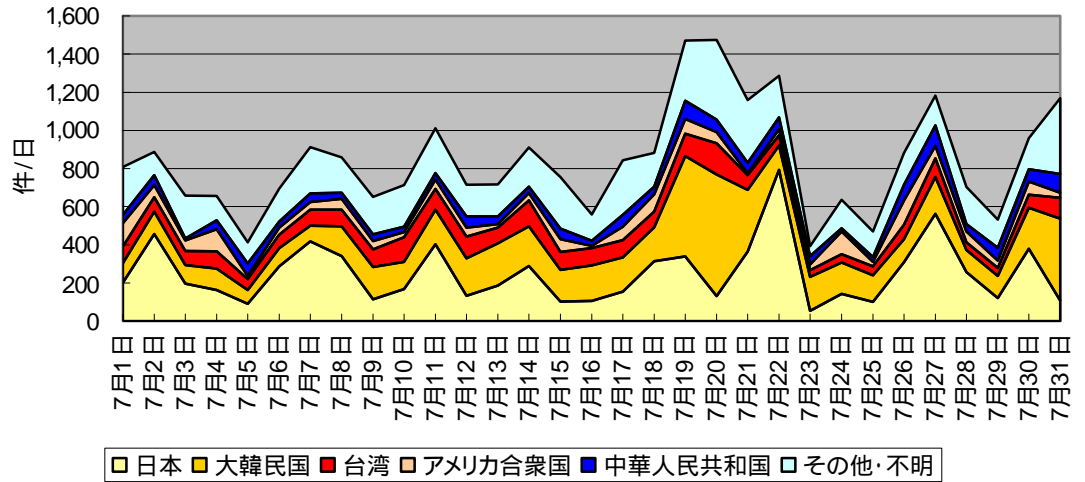
中華人民共和国、アメリカ合衆国からのアクセスがやや減少した一方、日本、大韓民国からのアクセスが増加したことから、全体としては増加となった。

ICMP(Echo Request)



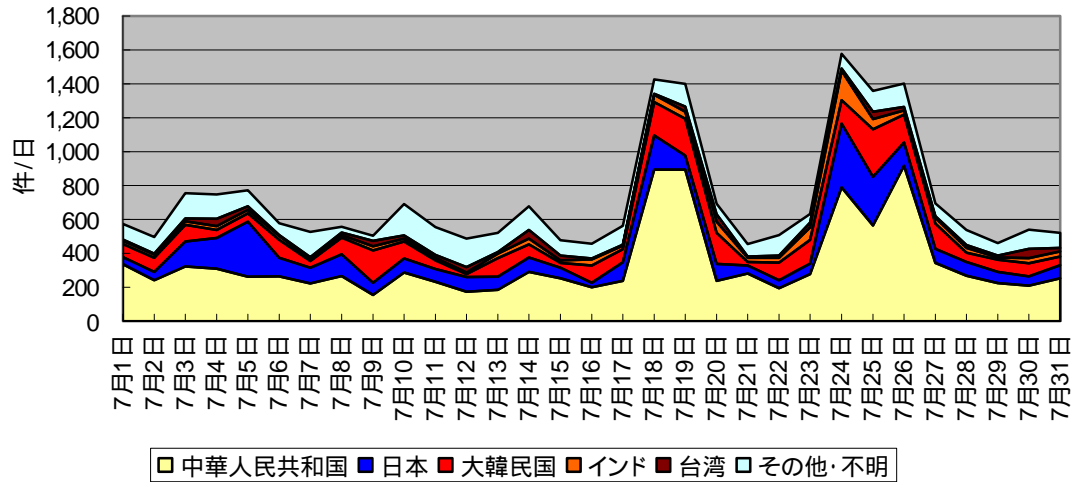
大韓民国からのアクセスがやや増加した一方、香港、カナダからのアクセスがいずれもやや減少したことから、全体としては微減となった。

139/TCP



日本国内からのアクセスが減少する一方、大韓民国、台湾を発信元と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。

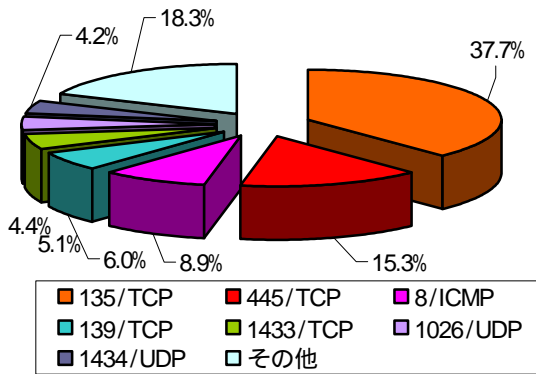
1433/TCP



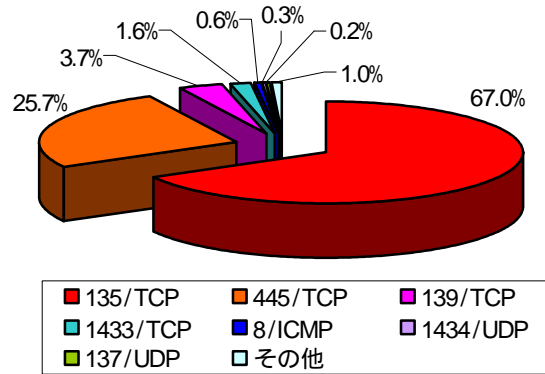
中華人民共和国、大韓民国からのアクセスが増加する一方、日本、インド、台湾からのアクセスがやや減少したことから、全体としては微増となった。

(2) 宛先ポート別比率

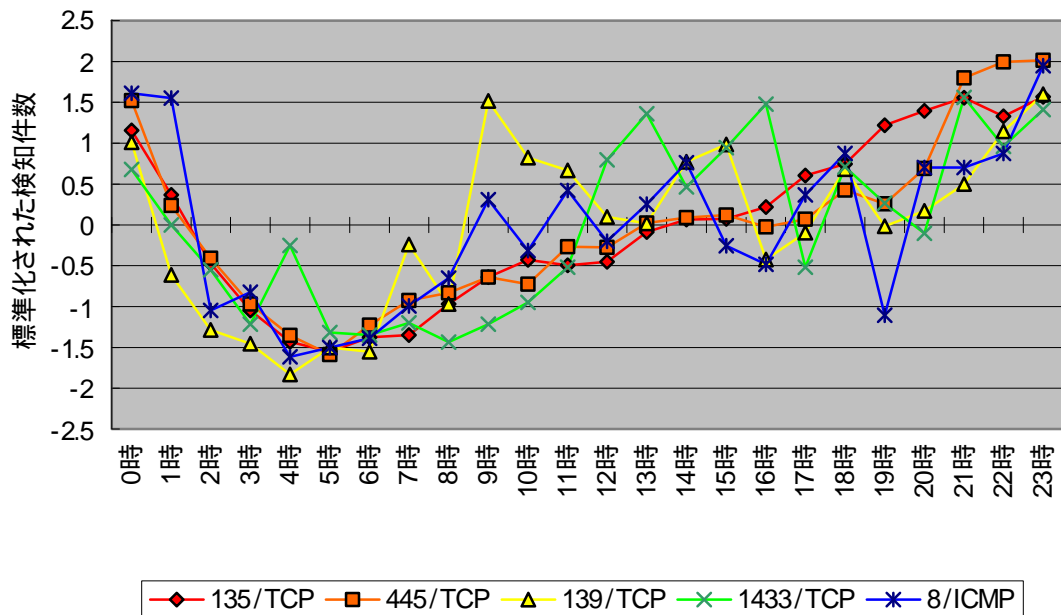
発信元/全世界



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。

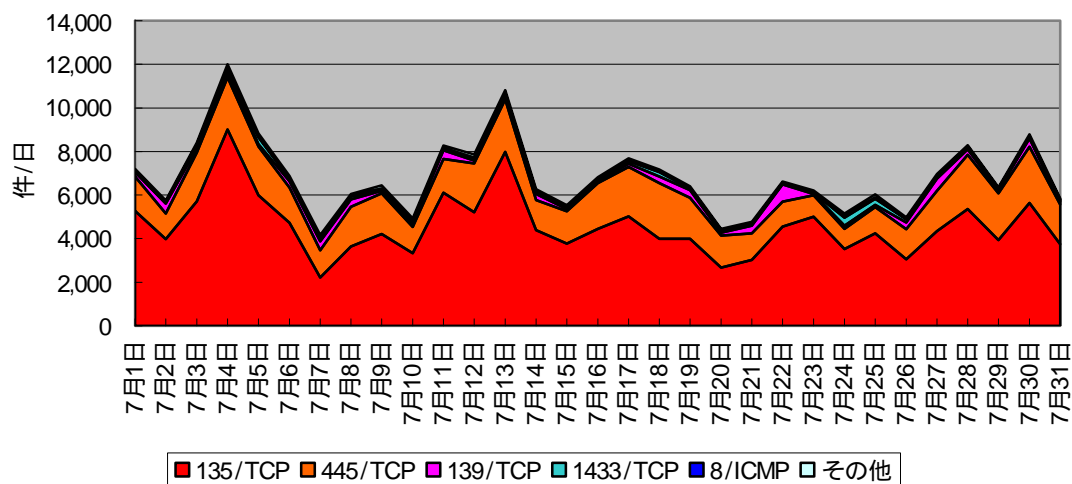
$$\text{標準化された検知件数} = (\text{その時間帯での検知件数} - \text{平均値}) / \text{標準偏差}$$

(4) 発信元国/地域別推移(上位5か国、積み上げ)

6月期と7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か国の順位に変動は見られなかった。また、7月期一日当たりのアクセス件数及び6月期との増減比較を、表の右側に示す。

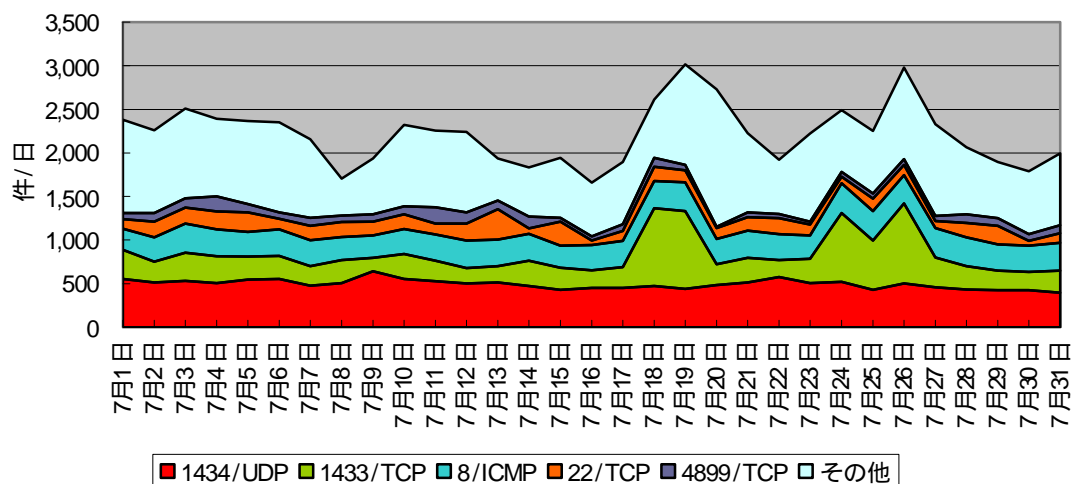
	6月期	7月期	7月期一日当たり	一日当たりの増減
1位	日本	日本	約6,838件	約+1,188件 (約+21.0%)
2位	中華人民共和国	中華人民共和国	約2,215件	約+65件 (約+3.0%)
3位	アメリカ合衆国	アメリカ合衆国	約1,692件	約+12件 (約+0.7%)
4位	大韓民国	大韓民国	約840件	約+110件 (約+15.0%)
5位	台湾	台湾	約369件	約+39件 (約+12.0%)

日本



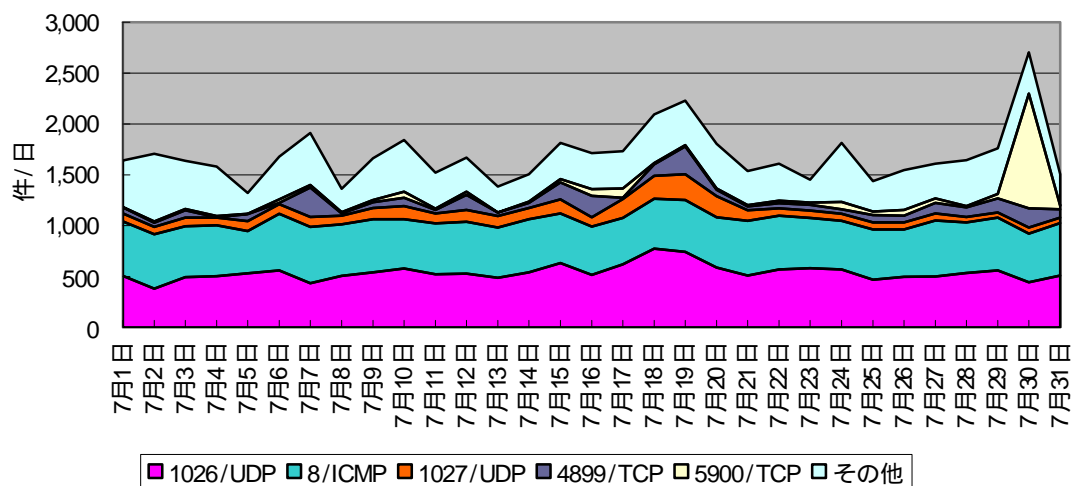
135/TCP、445/TCP に対するアクセスが増加する一方、それ以外のポートに対するアクセスはやや減少したが、全体としては増加となった。これは日本国内の特定ホストからのアクセス増加が主な要因である。

中華人民共和国



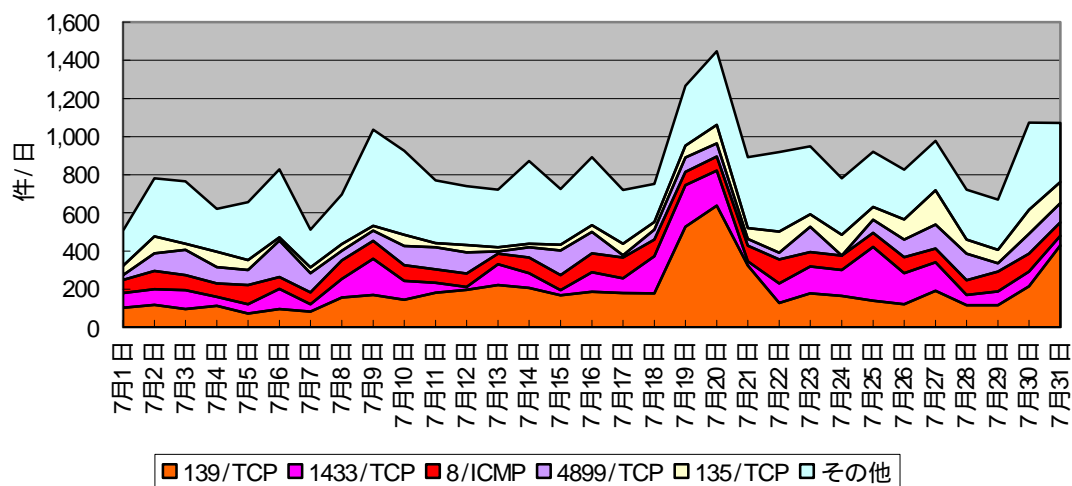
1433/TCP、その他に対するアクセスが増加する一方、135/TCP に対するアクセスは減少した。全体としては微増となった。

アメリカ合衆国



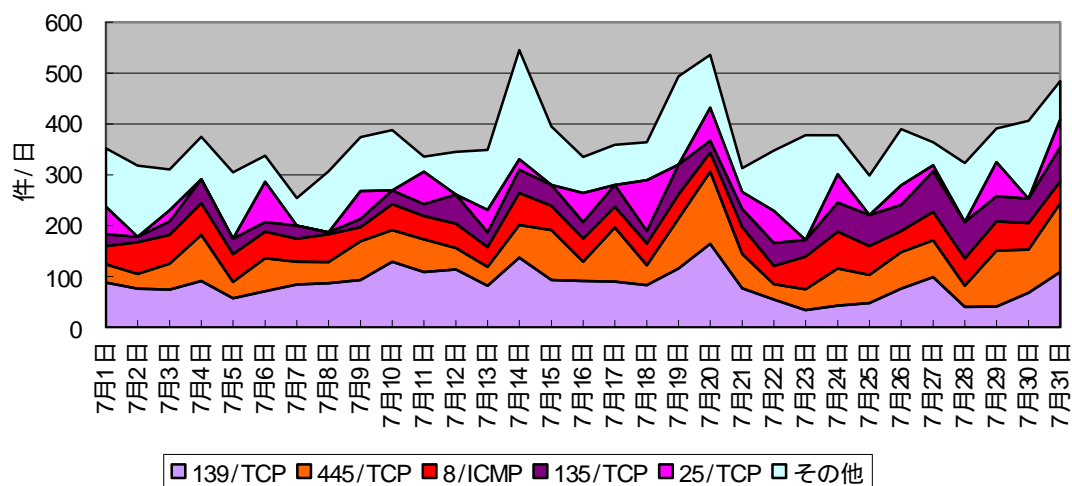
445/TCP に対するアクセスが減少する一方、5900/TCP に対するアクセスが大幅に増加した。特に 30 日のアクセス増加が顕著であり、アクセスの多くは、ボットネットによるスキャンと推測される。

大韓民国



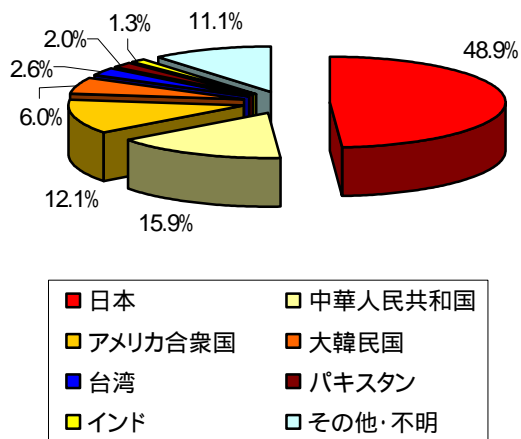
22/TCP に対するアクセスが減少する一方、25/TCP、135/TCP、139/TCP に対するアクセスが増加した。全体としては増加となった。

台湾

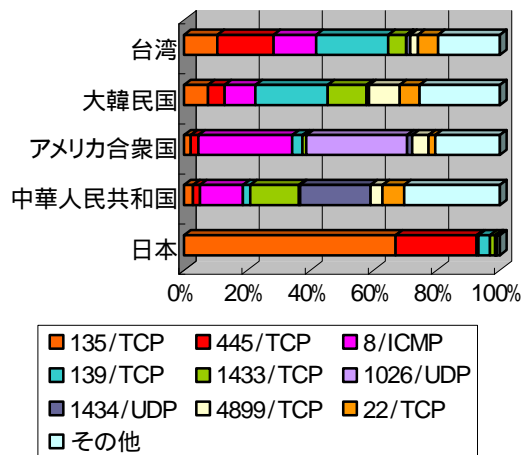


25/TCP、1433/TCP に対するアクセスが減少する一方、22/TCP、139/TCP に対するアクセスが増加した。全体としては増加となった。

(5) 国 / 地域別比率

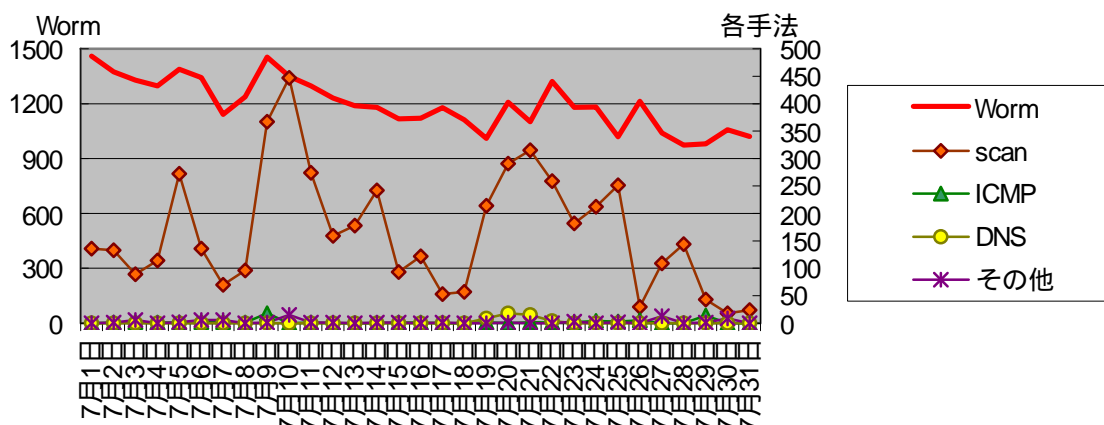


(6) 上位国 / 地域の宛先ポート別比率



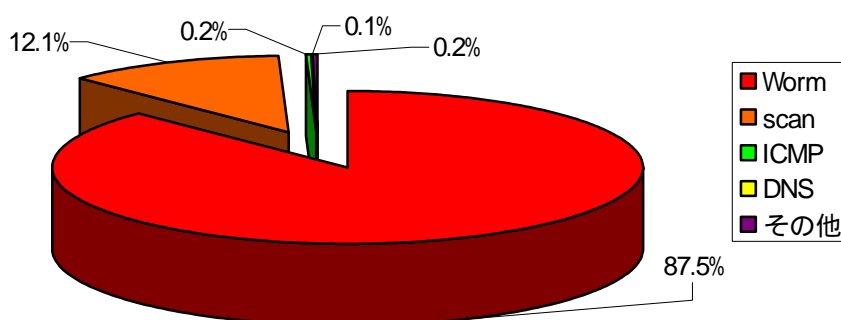
2.2 不正侵入検知システムにおけるアラート検知分析

(1) 攻撃手法別推移

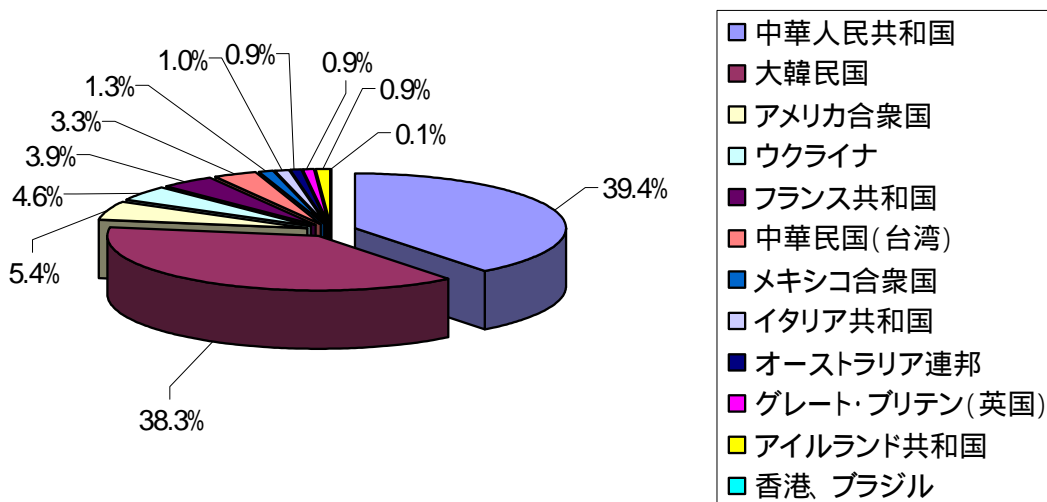


第1位のWorm(SQL Slammer)は、一日当たりの検知件数が約1,197件であり、6月期と比較して約-29件(約-2.3%)と減少した。第2位のscanは、一日当たりの検知件数が約165件であり、6月期と比較して約+45件(約+37.5%)と増加した。7月9日から10日にかけて増加しているscanは、大韓民国からのものが多数を占めている。

(2) 攻撃手法別比率

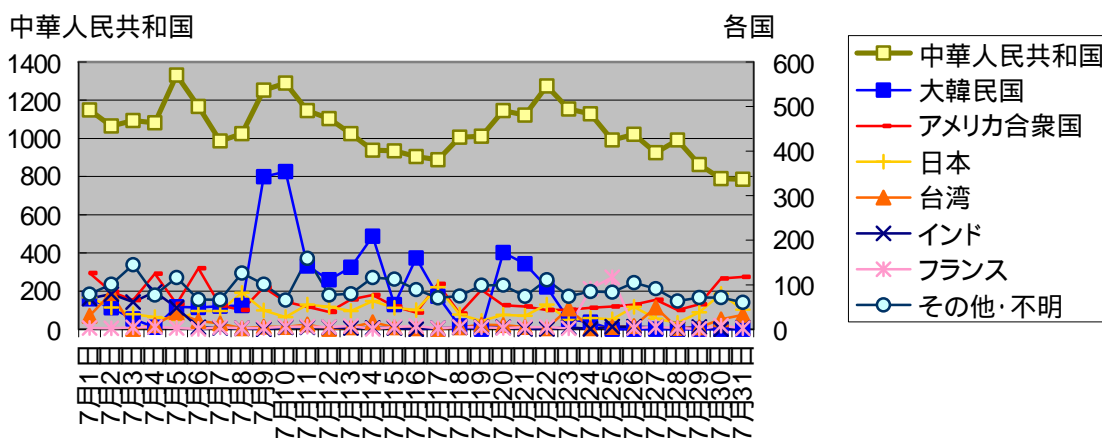


上記攻撃手法の分類うち、scan を発信元国 / 地域で分類した状況は以下とおりである。



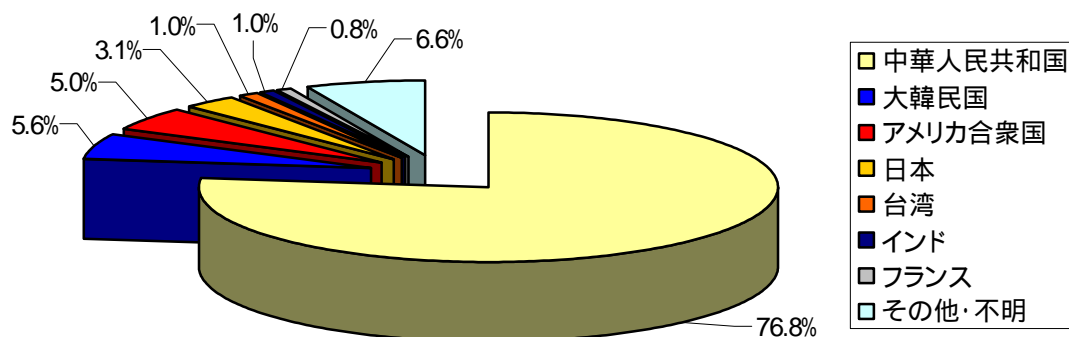
中華人民共和国を発信元とする scan (SCAN SOCK Proxy attempt) の一日当たりの検知件数は約 +64 件 (6 月期比約 +7137%) と大幅に増加する一方、大韓民国の一日当たりの検知件数は約 -42 件 (6 月期比約 -40%) と減少した。これらの scan は、特定ホストからのアクセス増加が主な要因であり、SOCKS Proxy (企業などの内部ネットワークとインターネットを接続するために配置されるもの) へのスキャンなどが顕著であった。

(3) 発信元国 / 地域別推移



大韓民国を発信元とする検知件数が、7月9日から10日にかけて増加している。この増加は、特定のホストから scan を検知したことが主な要因である。

(4) 発信元国 / 地域別比率



アメリカ合衆国を発信元とする検知件数が増加し、6月期から順位を1つ上げ第3位となった。6月期に第3位の日本は減少し、第4位となっている。また、今月期あらたに、フランスが第7位に加わった。これらの国を発信元とするアラートのほとんどがWorm (SQL Slammer)、scan (SCAN SOCK Proxy attempt) によるものである。

3 @police (Topics) 掲載事項

@police において7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 Microsoft PowerPoint の脆弱性について(7/18)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 (MS06-033,034,035,036,037,038,039)(7/12)

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 7 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(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。