平成 19 年 2 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 19 年 1 月期)

・ファイアウォールに対するアクセスは増加傾向
　～日本国内を発信元とするアクセスが増加～
　～ボット又はウイルスと推測されるアクセスが増加傾向～
・不正侵入検知システムにおけるアラートは増加傾向

1 概説

平成 19 年 1 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 616,635 件で、一日当たり約 19,891 件（対前月比＋8.4%）と増加した。この増加の主な要因として、日本国内を発信元とするアクセスが増加（対前月比＋20.1%）したことが挙げられる。宛先ポート別では、上位 5 位までに対するアクセス全てが 12 月期より増加した。上位 5 位までの順位は、135/TCP、ICMP (Echo Request)、445/TCP、139/TCP、1434/UDP の順となった。

不正侵入検知システム※におけるアラート検知件数は 45,608 件で、一日当たりの検知件数は約 1,471 件（対前月比＋12.9%）であった。攻撃手法別において第 1 位の Worm（SQL Slammer）は 12 月期と同様、全体の 9 割以上を占めた。また、発信元国／地域別において、上位は、中国、米国、台湾、日本、ポルトガルの順であった。

※ 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

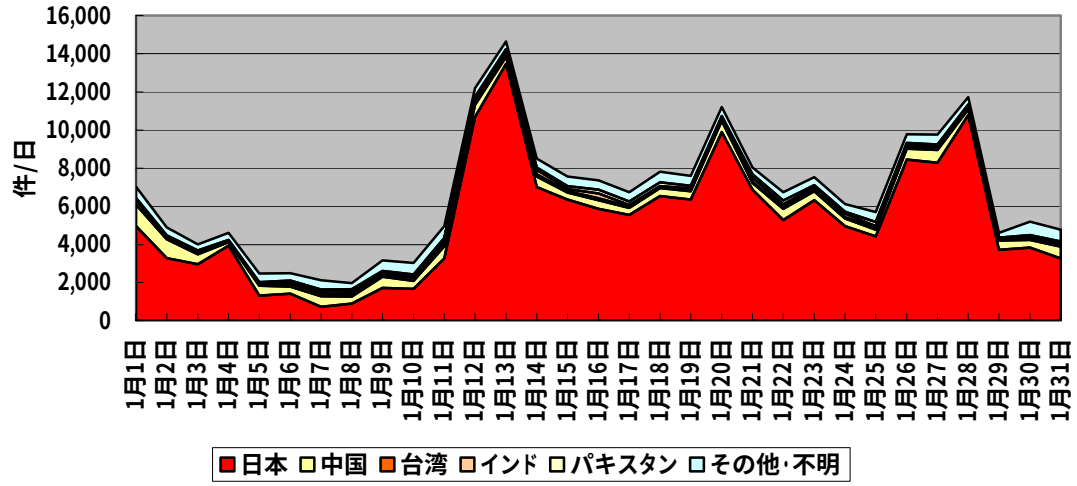
2.1 ファイアウォールに対するアクセス分析

(1) 宛先ポート別推移(上位 5 ポート、積み上げ)

1 月期における上位 5 ポートは以下のとおりである。上位 3 ポートに変動はなかったが、139/TCP 及び 1434/UDP に対するアクセスが増加し、12 月期に第 4 位であった 1026/UDP に対するアクセスが減少したことから、順位に変動があった。

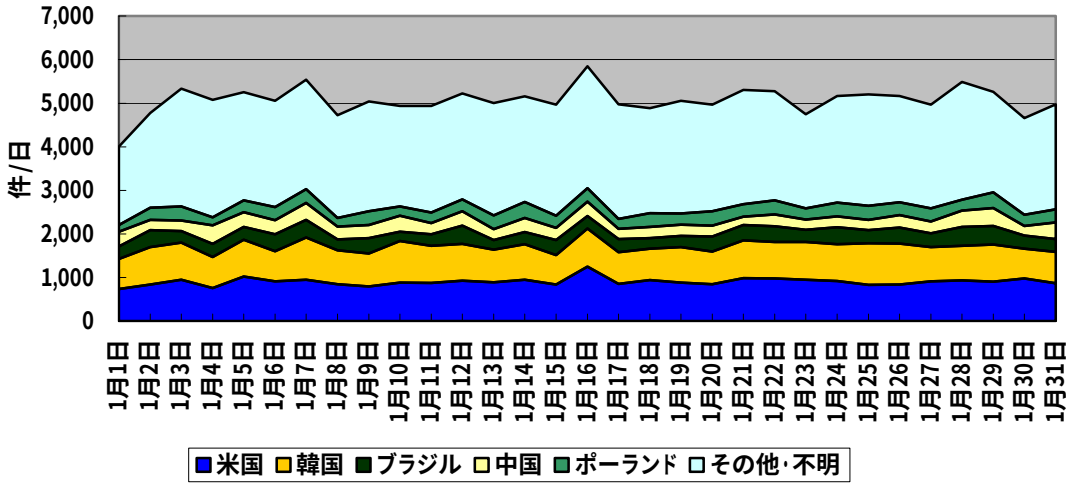
1 月期	ポート	前月比(一日当たり)	12 月期
1 位	135/TCP	約＋10.4% (約＋622 件)	1 位
2 位	ICMP(Echo Request)	約＋10.2% (約＋470 件)	2 位
3 位	445/TCP	約＋18.1% (約＋352 件)	3 位
4 位	139/TCP	約＋4.7% (約＋34 件)	6 位
5 位	1434/UDP	約＋13.4% (約＋84 件)	7 位

■ 135/TCP



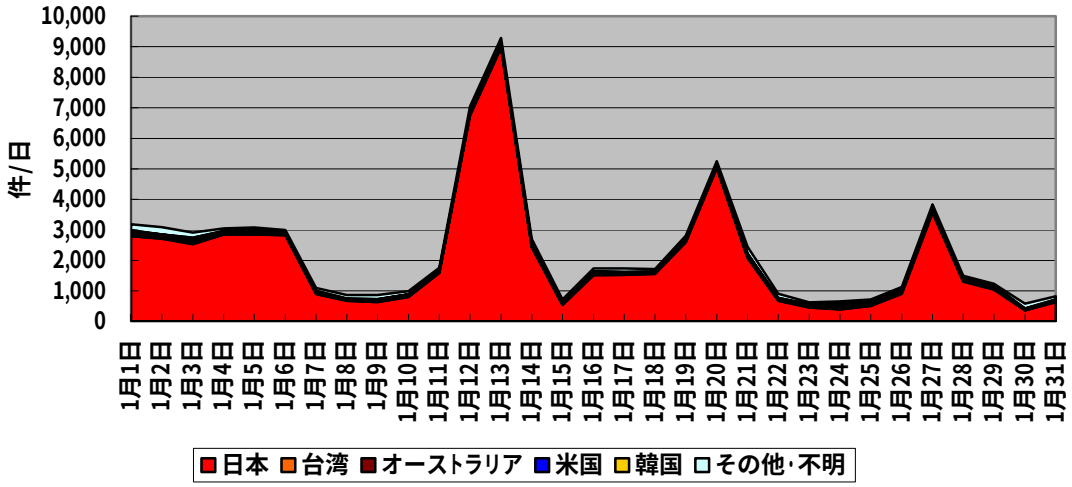
1 月 13 日、20 日、27 日に、アクセスの大半を占める日本国内からのアクセスが急増したことから、12 月期に比べ全体として大幅な増加となった。これは、特定の IP アドレスから短時間に 445/TCP と共に繰り返しアクセスがあったことが原因であるが、ボット又はウイルスの感染拡大活動と推測される。

■ ICMP(Echo Request)



1 月 2 日以降、その他・不明に分類される国からのアクセスが増加したことから、12 月期に比べ全体として大幅な増加となった。感染活動にあたり、大量の ICMP(Echo Request)を発生させるウイルスの存在を確認している。

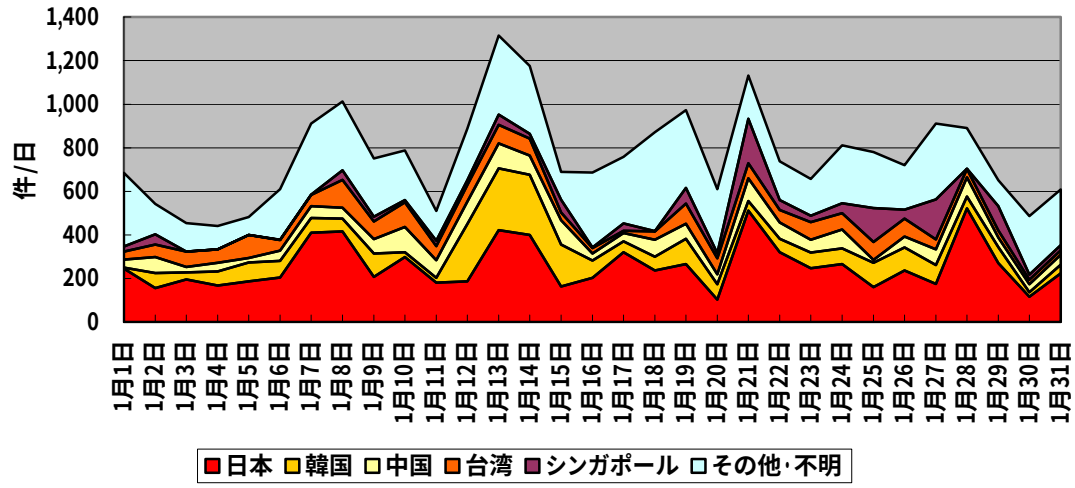
■ 445/TCP



1 月 13 日、20 日、27 日に、アクセスの大半を占める日本国内からのアクセスが急増したことから、12 月期に比べ全体として大幅な増加となった。

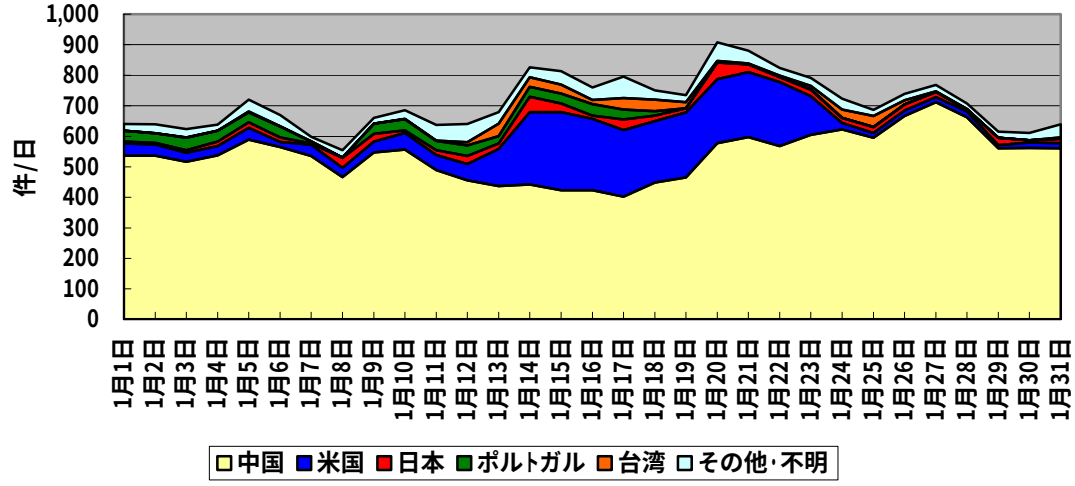
急増した時刻には、445/TCP 及び 135/TCP に対して同一 IP アドレスからのアクセスがあったもので、これらのポートへ同時にアクセスするボット又はウイルスによるものと推測される。

■ 139/TCP



中国からのアクセスが減少したが、それ以外の国からのアクセスが増加したことから、12 月期に比べ全体としても微増となった。

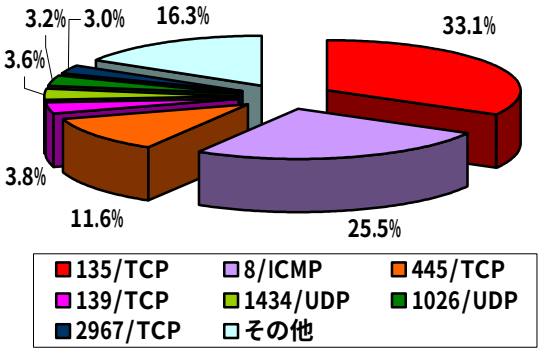
■ 1434/UDP



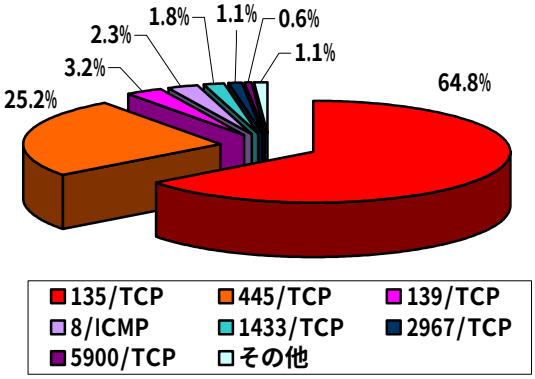
1 月中旬に米国からのアクセスが急増したことから、12 月期に比べ全体として増加となった。このポートは SQL Server で使用しているもので、このソフトウェアの脆弱性を突くウイルス（SQL Slammer ワーム）によるアクセスと推測される。

(2) 宛先ポート別比率

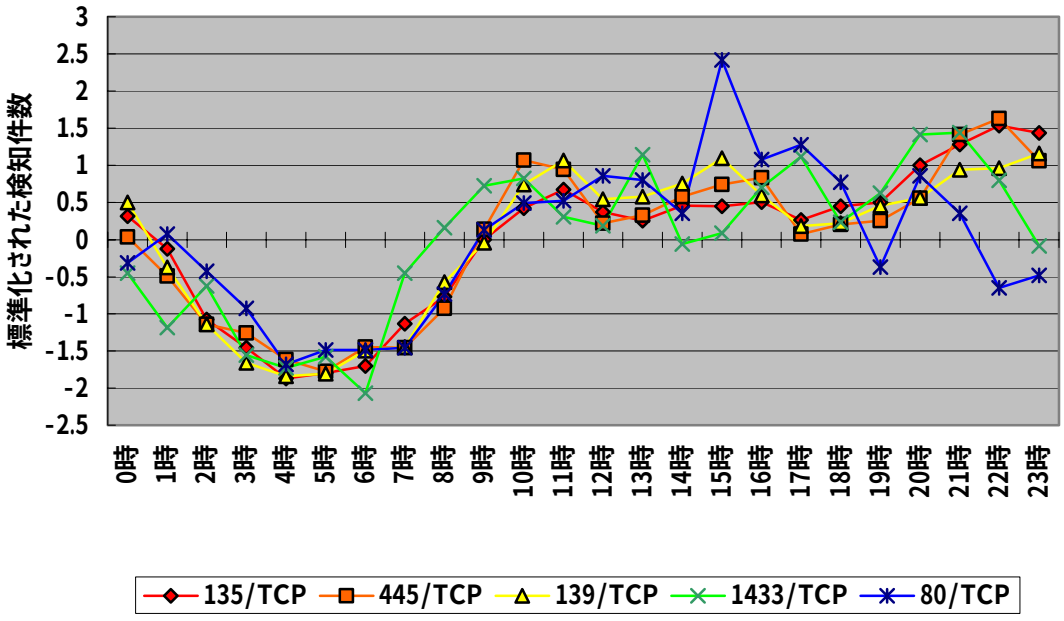
■ 発信元/全世界



■ 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。

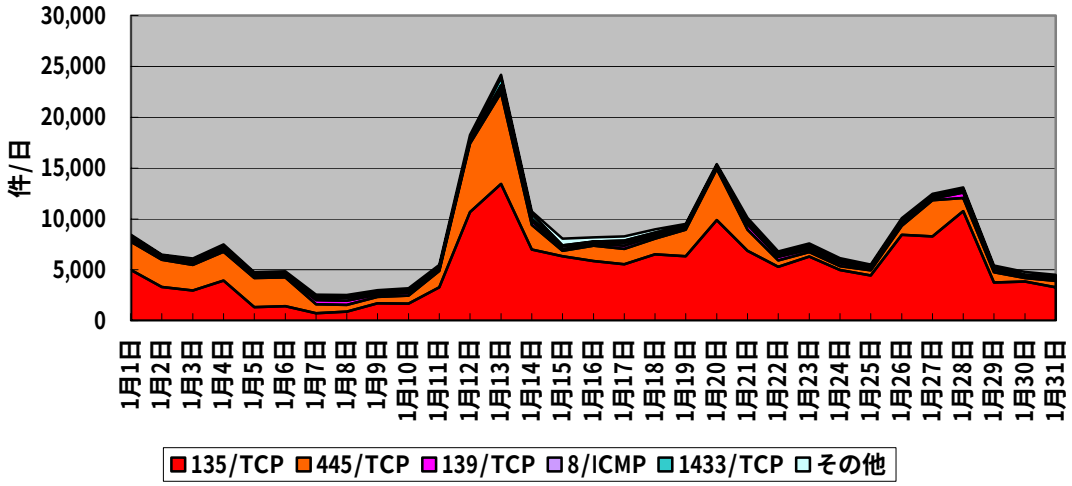
標準化された検知件数 = (その時間帯での検知件数 － 平均値) / 標準偏差

(4) 発信元国／地域別推移(上位 5 か国、積み上げ)

12 月期と 1 月期における上位 5 位までの発信元国／地域は以下のとおりである。順位に変動はなかった。また、一日当たりのアクセス件数について、12 月期との増減比較を表の右側に示す。

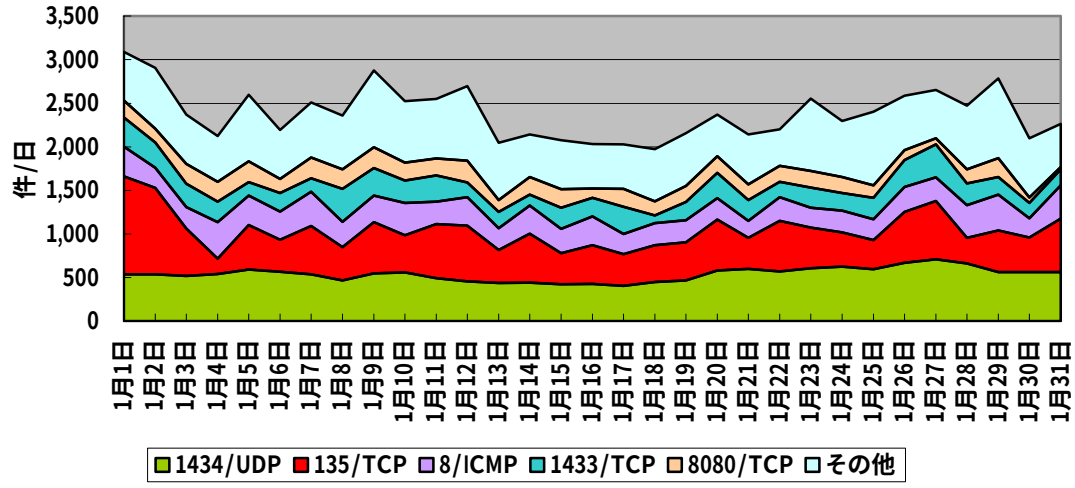
	12 月期	1 月期	前月比（一日当たり）
1 位	日　本	日　本	約＋20.1% （約＋1,369 件）
2 位	中　国	中　国	約－18.3% （約－535 件）
3 位	米　国	米　国	約－18.4% （約－531 件）
4 位	韓　国	韓　国	約＋27.0% （約＋285 件）
5 位	台　湾	台　湾	約－0.9% （約－6 件）

■ 日本



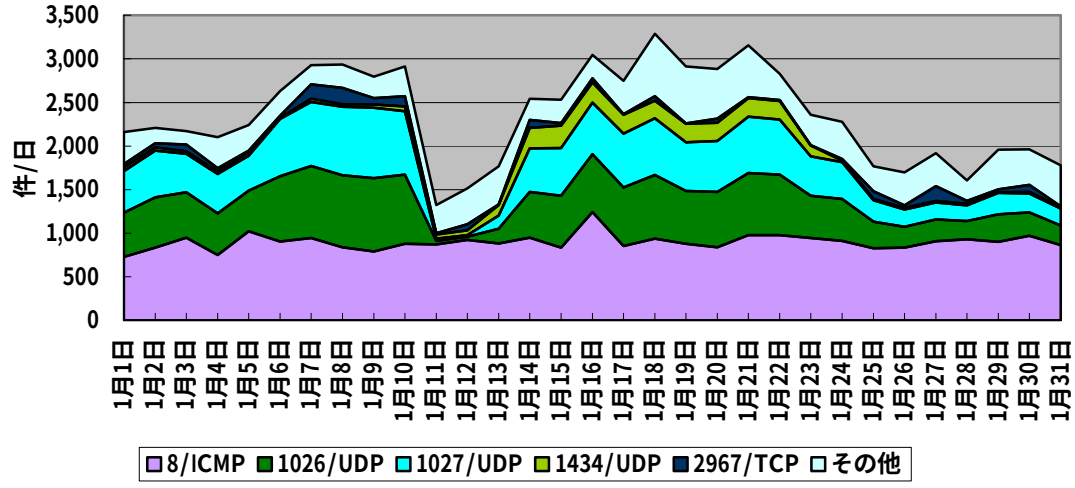
12 月期に比べ 135/TCP 及び 445/TCP に対するアクセスが急増したことから、全体として大幅な増加となった。

■ 中国



12 月期に比べほぼ全てのポートにおいてアクセスが減少したことから、全体として大幅な減少となった。

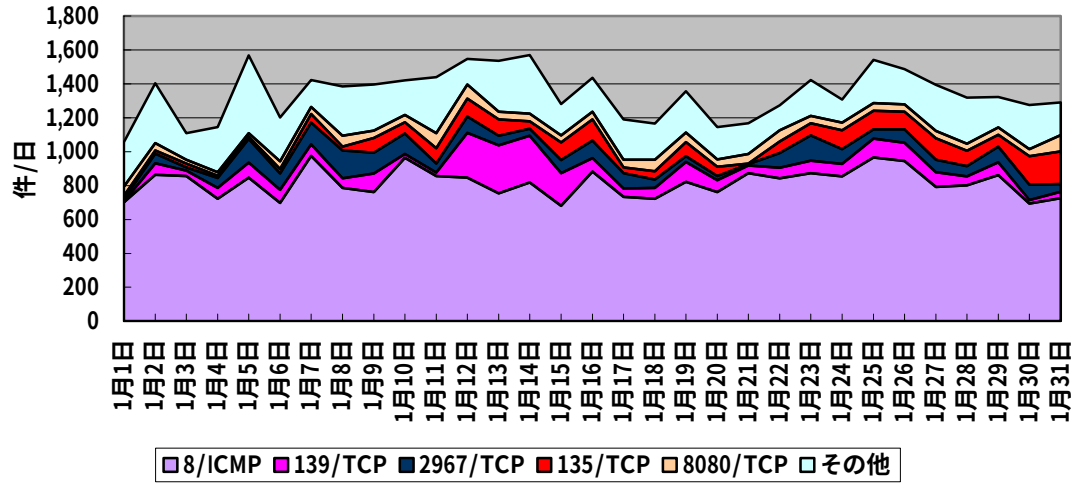
■ 米国



12 月期に比べ ICMP(Echo Request)に対するアクセスが減少したことから、全体として大幅な減少となった。

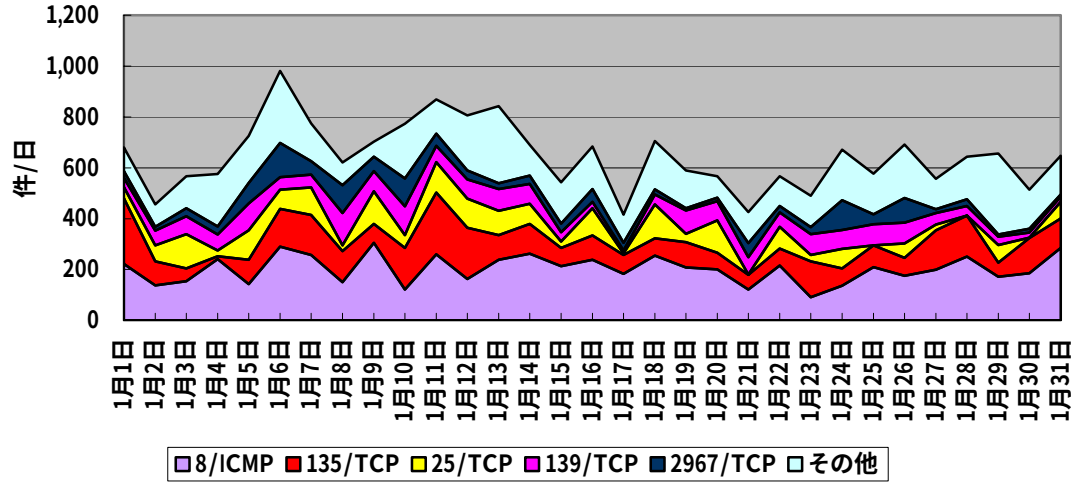
また、1026/UDP 及び 1027/UDP に対するアクセスは、12 月期に比べその件数の差が小さくなっている。1026/UDP 及び 1027/UDP は、 Windows の Messenger サービスを悪用したスパムに利用されるポートであり、利用されるポートが 1026/UDP から 1027/UDP へ変遷している。

■ 韓国



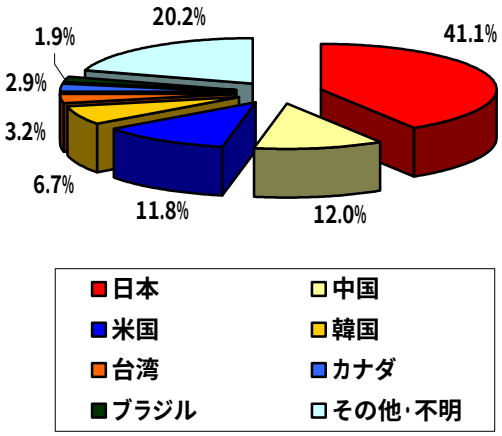
12 月期に比べほぼ全てのポートにおいてアクセスが増加したことから、全体として大幅な増加となった。

■ 台湾

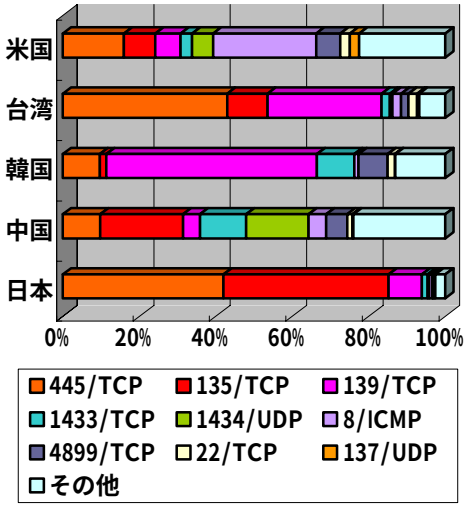


12 月期に比べ ICMP(Echo Request)、135/TCP 及び 139/TCP に対するアクセスは増加したが、それ以外のポートに対するアクセスが減少したことから、全体としては微減となった。

(5) 国／地域別比率

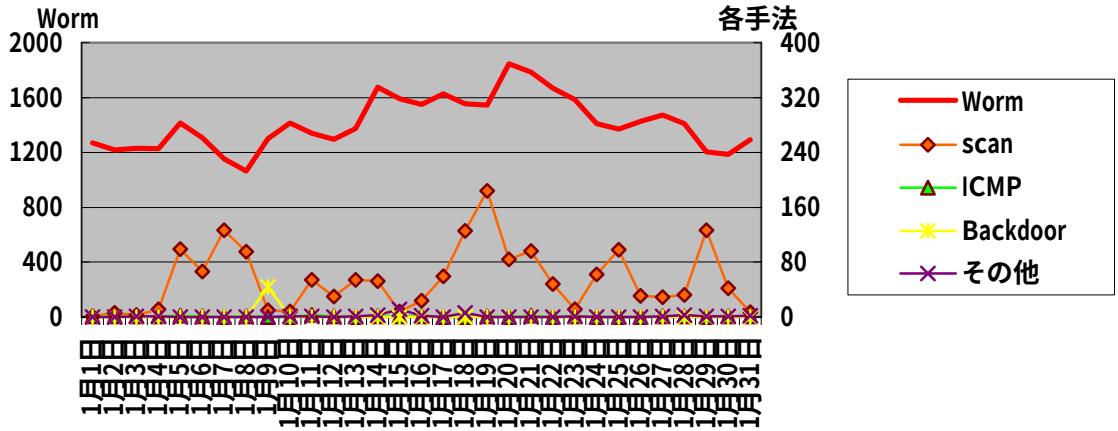


(6) 上位国／地域の宛先ポート別比率



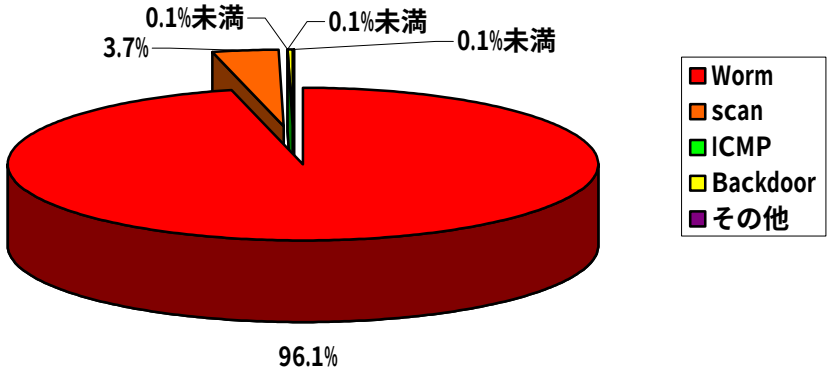
2.2 不正侵入検知システムにおけるアラート検知分析

(1) 攻撃手法別推移

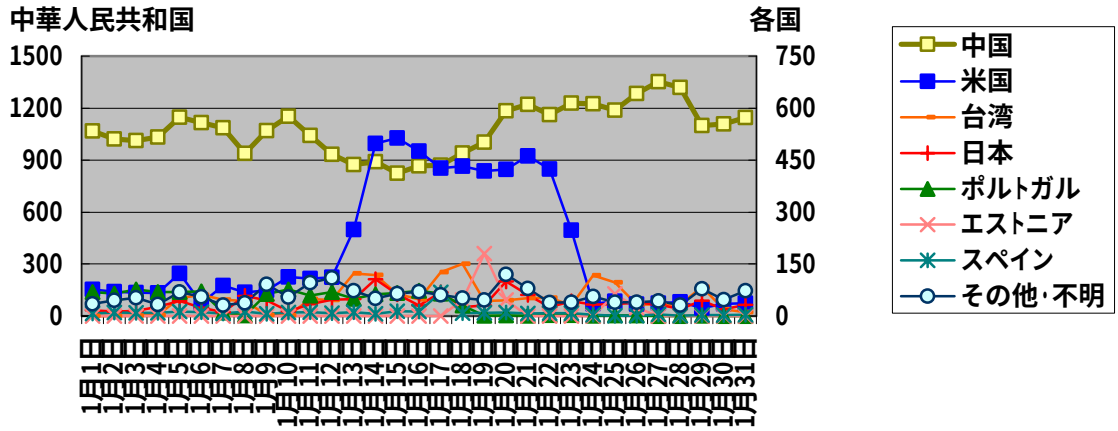


第 1 位の Worm（SQL Slammer）は、一日当たりの検知件数が約 1,414 件であり、12 月期と比較して約＋188 件（約＋15.3%）と増加した。第 2 位の scan は、一日当たりの検知件数が約 54 件であり、12 月期と比較して約－22 件（約－29%）減少した。

(2) 攻撃手法別比率

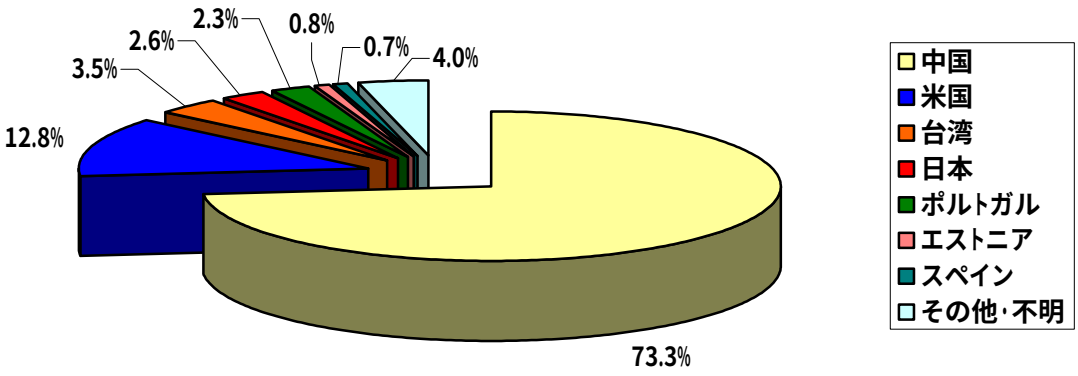


(3) 発信元国／地域別推移



1 月 13 日から 23 日において、米国を発信元とする検知件数が急増している。これは、特定発信元からの Worm（SQL Slammer）によるものである。

(4) 発信元国／地域別比率



中国を発信元とするアラートの割合が依然高い。第 2 位の米国及び第 3 位の台湾からのアラートが急増したことから、この 2 か国の割合が 12 月期に比べ大幅に増加した。

3 @police (Topics) 掲載事項

@police において１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 Word の脆弱性について(1/27)
注意	Cisco 社製ネットワーク機器の脆弱性について(1/25)
注意	QuickTime の脆弱性について(1/24)
	セキュリティ講座（ID・パスワード編）追加(1/22)
	第 19 回セキュリティ解説更新(1/22)
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 (MS07-001,002,003,004)(1/19)更新

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 19 年 1 月現在、約 360 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。