

平成 21 年 2 月 25 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 21 年 1 月期)

- ・ファイアウォールに対する総アクセス件数はやや増加
～ 12 月期に引き続き 445/TCP に対するアクセスが増加～
 - Microsoft Windows の脆弱性を悪用した攻撃の危険性
- ～ 特定のウェブアプリケーションを狙う攻撃も～
- ・不正侵入検知システムにおける不正なアクセスはやや減少

1 概説

平成 21 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、一日・1IP 当たり 271.8 件で、平成 20 年 12 月期と比較して +29.0 件と、やや増加 (+11.9%) した。

アクセス件数の上位 5 ポートは、135/TCP、445/TCP、ICMP Echo Request (以降、「8/ICMP」と表記する。) 1433/TCP 及び 1026/UDP の順であり、12 月期と比較して順位に変動はないものの、12 月期に引き続き、445/TCP が増加しており、Microsoft Windows 製品の Server サービスの脆弱性を悪用した攻撃の拡大が懸念される。また、8 日から 13 日に 80/TCP に対する米国等からのアクセスが増加した。これは、ウェブアプリケーションである「Roundcube Webmail」への侵入を試みる活動が行われた可能性がある。

アクセス件数の上位 5 か国は、中国、日本、米国、台湾及び韓国の順であり、12 月期と比較して順位に変動はないが、中国からのアクセスがやや増加した。

1 月期の不正侵入検知システム における不正なアクセスの検知件数は、一日・1IP 当たり 8.9 件で、12 月期と比較して、-1.3 件とやや減少 (-12.6%) した。

攻撃手法別では、第 1 位の Worm (SQL Slammer ワーム) がやや減少し、第 2 位の Scan は、横ばいとなった。また、発信元国/地域別において、上位 5 か国は中国、米国、日本、ベトナム及び韓国の順であった。

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」を参照のこと。

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

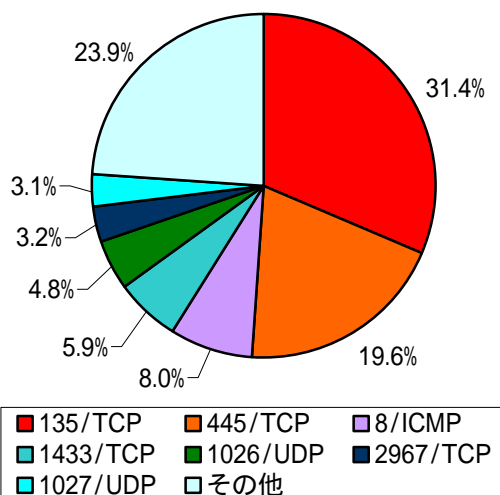
(1) 宛先ポート別推移(上位 5 ポート)

1 月期における上位 5 ポートは以下のとおりである。12 月期と比較して、順位に変動はない。445/TCP に対するアクセスの増加が目立つ。

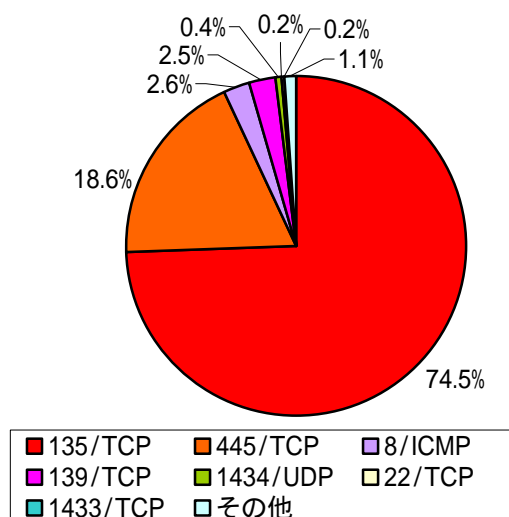
1 月期 順位	ポート	1 月期件数 (一日・1IP 当たり)	前期比 (一日・1IP 当たり)	12 月期 順位
1 位	135/TCP	85.43 件	+ 22.4% (+ 15.61 件)	1 位
2 位	445/TCP	53.25 件	+ 93.8% (+ 25.77 件)	2 位
3 位	8/ICMP	21.74 件	- 14.9% (- 3.80 件)	3 位
4 位	1433/TCP	16.06 件	- 16.2% (- 3.10 件)	4 位
5 位	1026/UDP	13.06 件	- 1.5% (- 0.20 件)	5 位

(2) 宛先ポート別比率

発信元/全世界



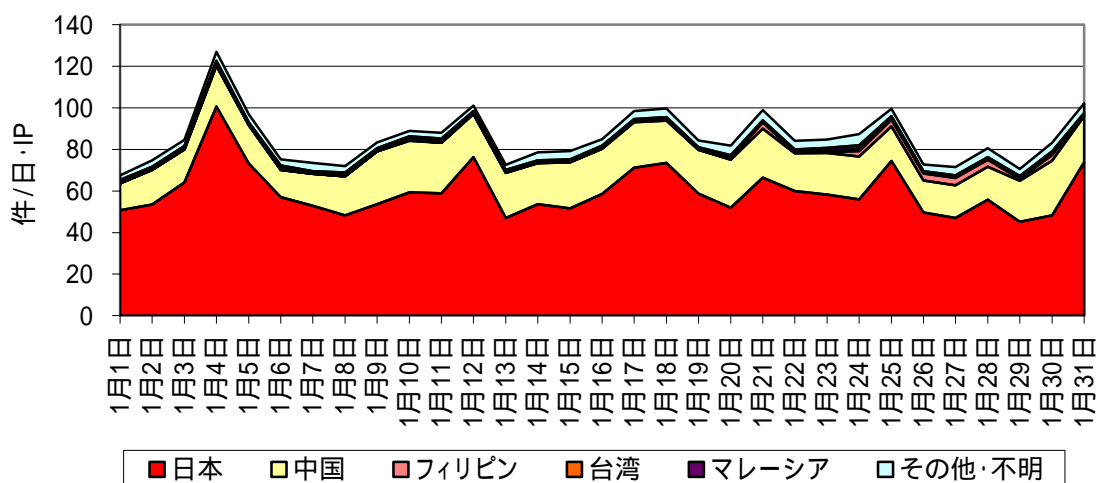
発信元/日本



当データは、小数点第二位で四捨五入しているため、合計が 100%にならないことがある。

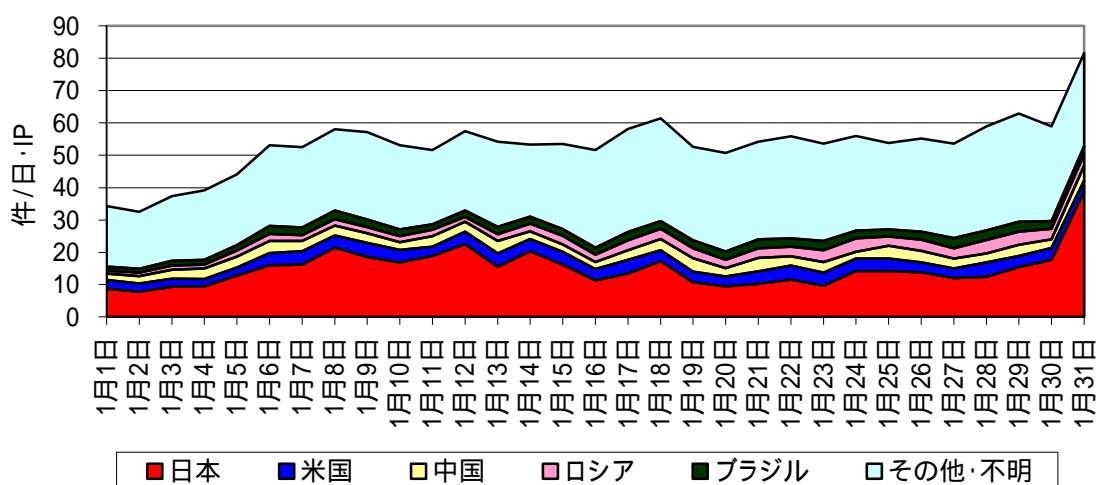
(3) 宛先ポート別推移

135/TCP



12月期と比較して、135/TCP に対するアクセスがやや増加した。12月期に引き続き、国内及び中国からのアクセスが大半を占めた。

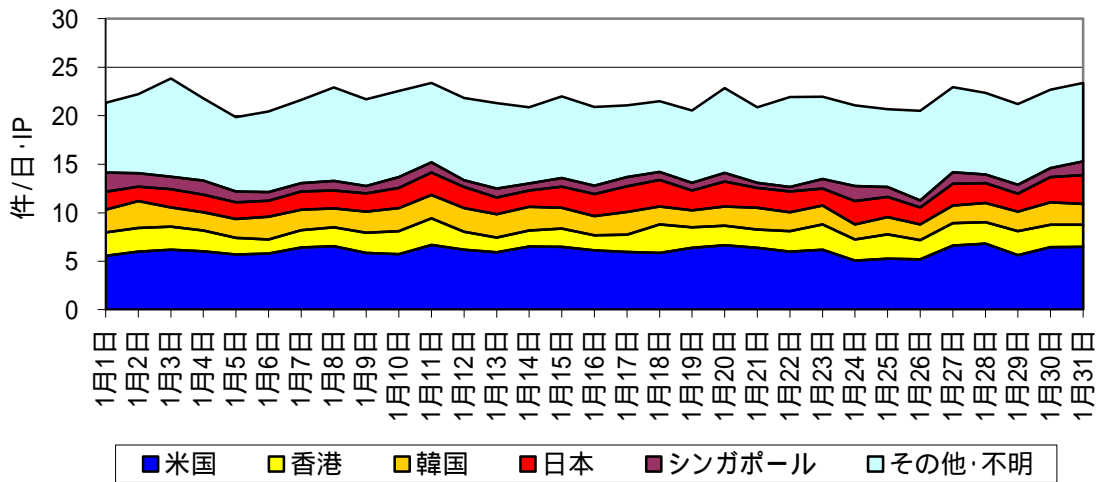
445/TCP



12月期に引き続き、445/TCP に対するアクセスが増加しており、Microsoft Windows 製品の Server サービスの脆弱性を悪用した攻撃が行われている可能性があることから、被害の拡大が懸念される。

31日における国内からのアクセスの増加は、一時的にスキャン行為が行われた可能性がある。

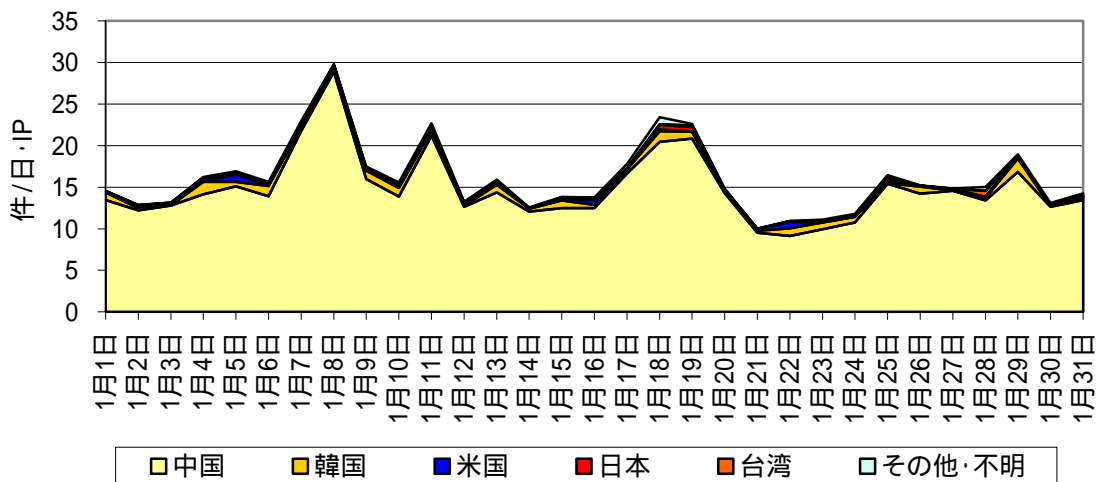
8/ICMP



12月期と比較して、米国、香港及び韓国からのアクセスがやや減少し、日本からのアクセスは横ばいとなった。

全体としては、12月期に引き続き、アクセスに穏やかな減少傾向が見られる。

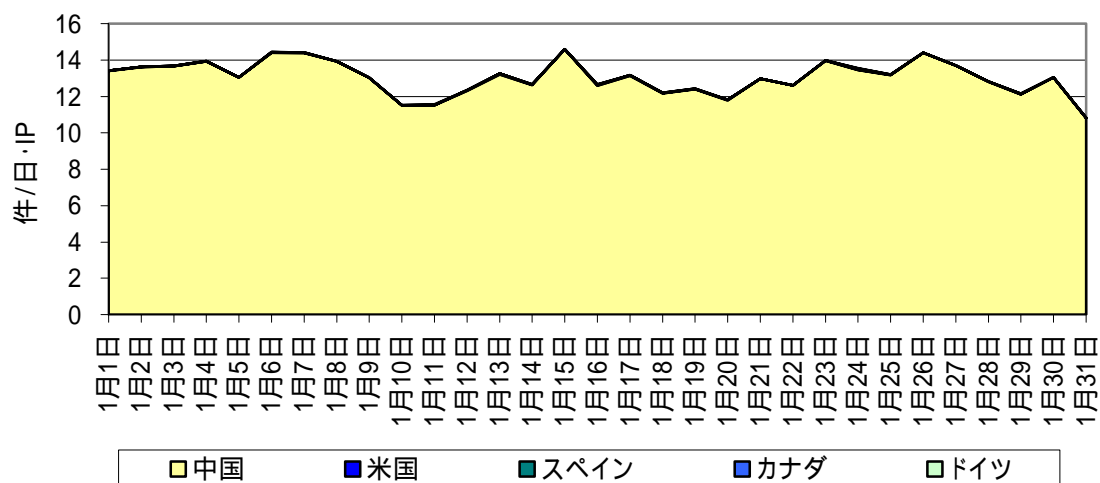
1433/TCP



12月期と比較して、大半を占める中国からのアクセスが横ばいとなったことから、全体としても横ばいとなった。

7日から8日、11日及び18日から19日におけるアクセスの増加は、いずれも同一のポットネットからのアクセスであった可能性がある。

1026/UDP



12月期と比較して、大半を占める中国からのアクセスが横ばいとなったことから、全体としても横ばいとなった。

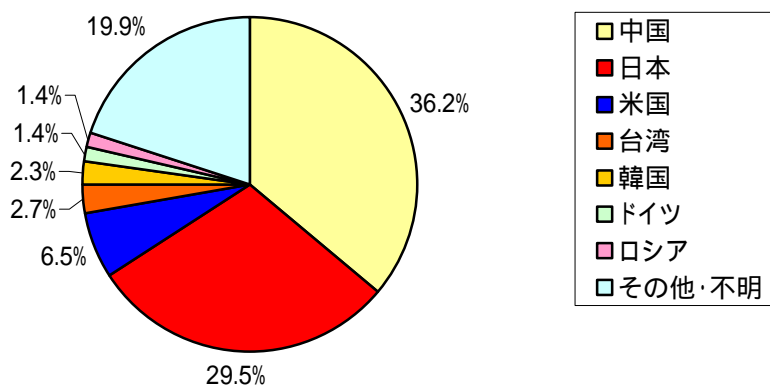
1026/UDP に対するアクセスの多くは、Windows の Messenger サービスに対するスパムであり、受信したコンピュータにおいて、商品の購入を促す広告等の表示を目的としたものであった。

(4) 発信元国 / 地域別推移(上位 5 か国)

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。12 月期と比較して、順位に変動はない。中国からのアクセスがやや増加した。日本からのアクセスについては、日々の変動が中国より大きく、増加傾向は明らかでないが、やや増加した。

1 月期 順位	国/地域	1 月期件数 (一日・1IP 当たり)	前期比 (一日・1IP 当たり)	12 月期 順位
1 位	中 国	98.45 件	+ 7.5% (+ 6.88 件)	1 位
2 位	日 本	80.19 件	+ 11.3% (+ 8.12 件)	2 位
3 位	米 国	17.80 件	- 32.0% (- 8.39 件)	3 位
4 位	台 湾	7.25 件	+ 0.5% (+ 0.04 件)	4 位
5 位	韓 国	6.31 件	+ 1.9% (+ 0.12 件)	5 位

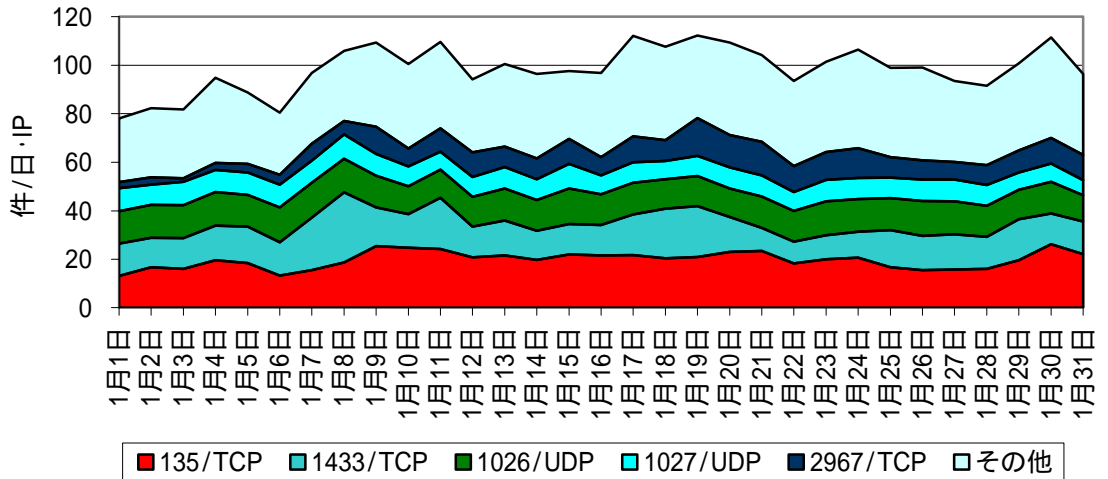
(5) 発信元国 / 地域別比率



当データは、小数点第二位で四捨五入しているため、合計が 100%にならないことがある。

(6) 発信元国 / 地域別推移

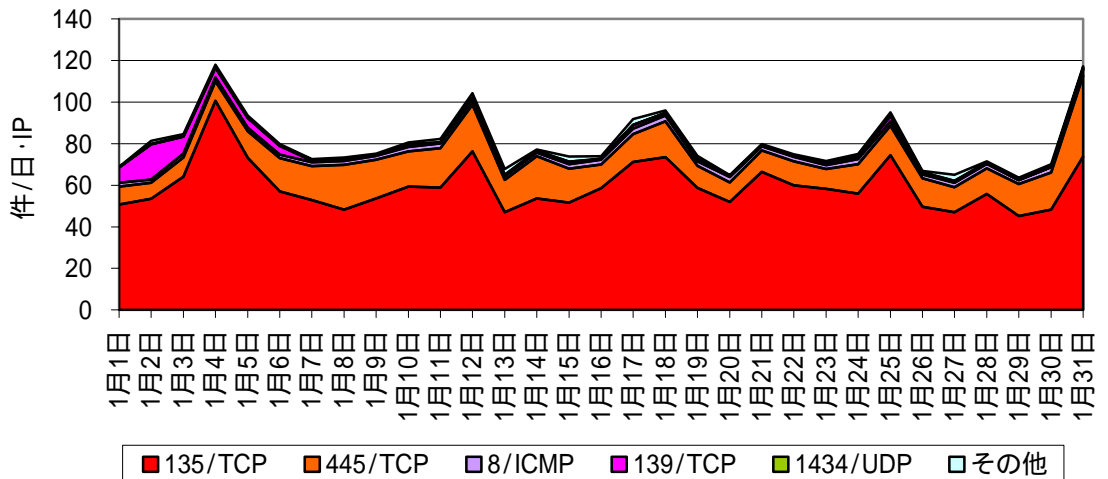
中国



12月期と比較して、135/TCP に対するアクセスが増加し、2967/TCP に対するアクセスが大幅に増加したことから、全体としてはやや増加となった。

2967/TCP は、Symantec 社の製品である「Symantec Client Security」及び「Symantec AntiVirus」で使用されるポートであり、2006年5月にその二つの製品に特権昇格の脆弱性があることが公表されている。

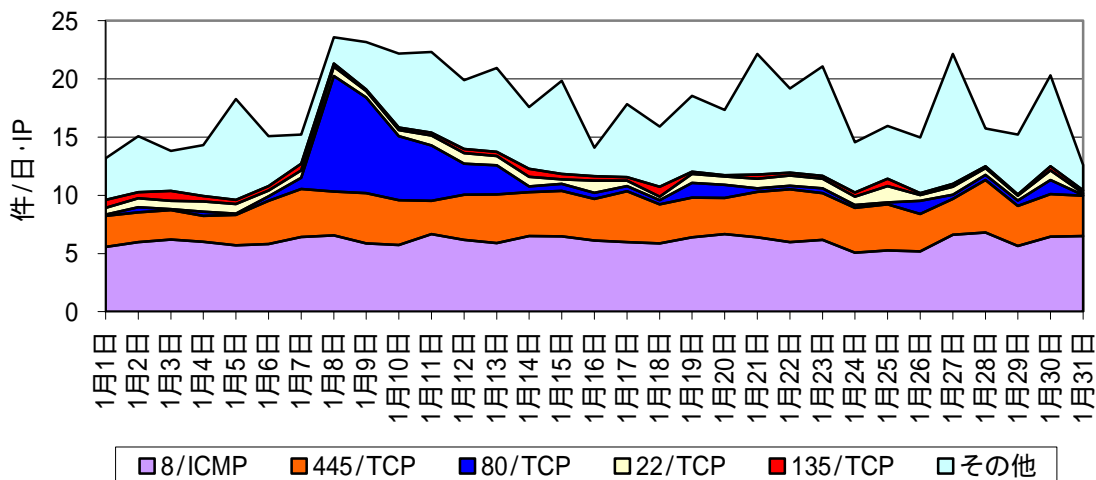
日本



12月期と比較して、445/TCP に対するアクセスが増加し、139/TCP に対するアクセスが大幅に減少した。

445/TCP に対するアクセスについては、12月に引き続き、Microsoft Windows 製品の Server サービスの脆弱性を悪用した攻撃が行われている可能性があることから、被害の拡大が懸念される。

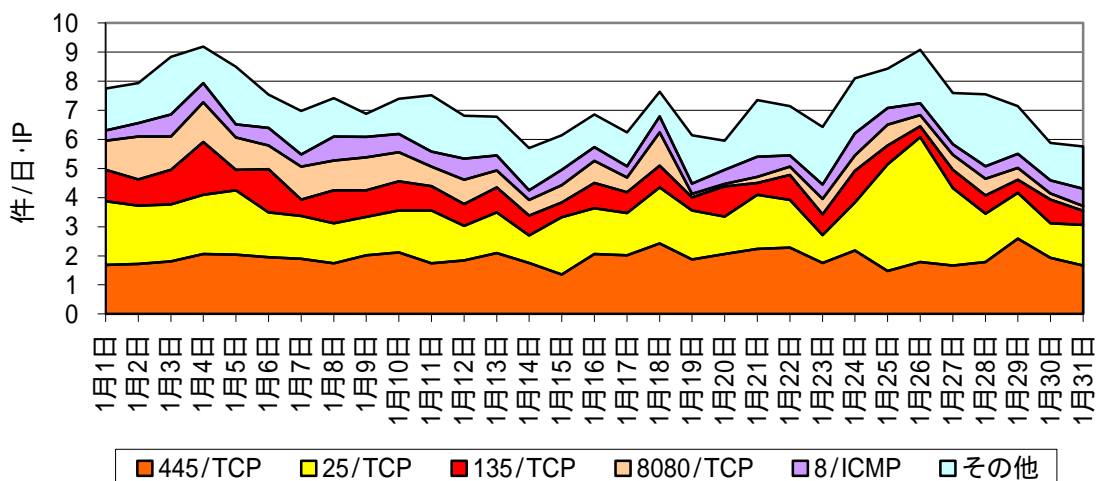
米国



12月期と比較して、8/ICMP に対するアクセスがやや減少し、445/TCP に対するアクセスが増加した。22/TCP 及び 135/TCP に対するアクセスは横ばいとなった。

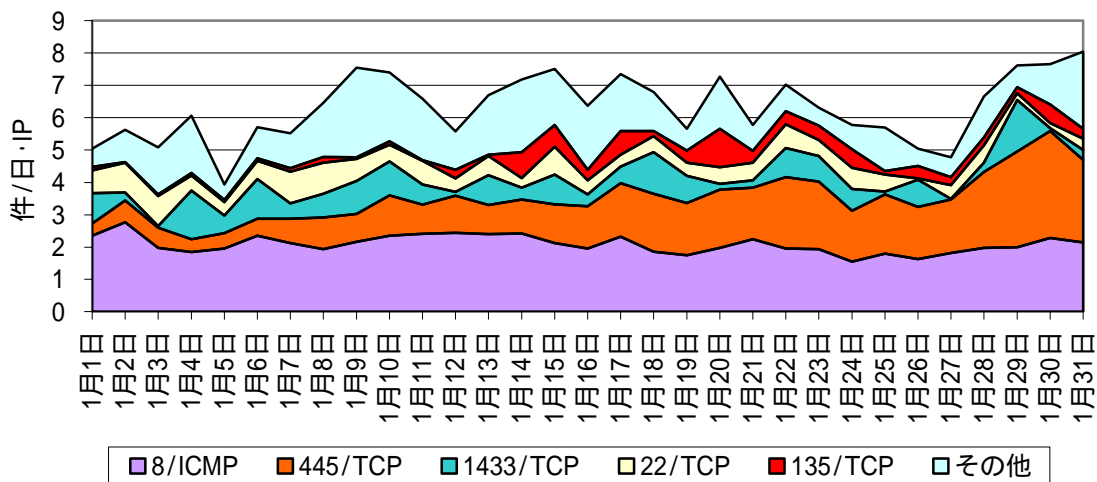
8日から13日に80/TCP に対するアクセスが増加した。これは、12月16日にセキュリティアップデートがリリースされた、RoundCube プロジェクトが提供するウェブメールソフトである「Roundcube Webmail」への侵入を試みる活動がボットネットにより行われた可能性があり、同様のアクセスを、ドイツ、オランダ等からも検知した。

台湾



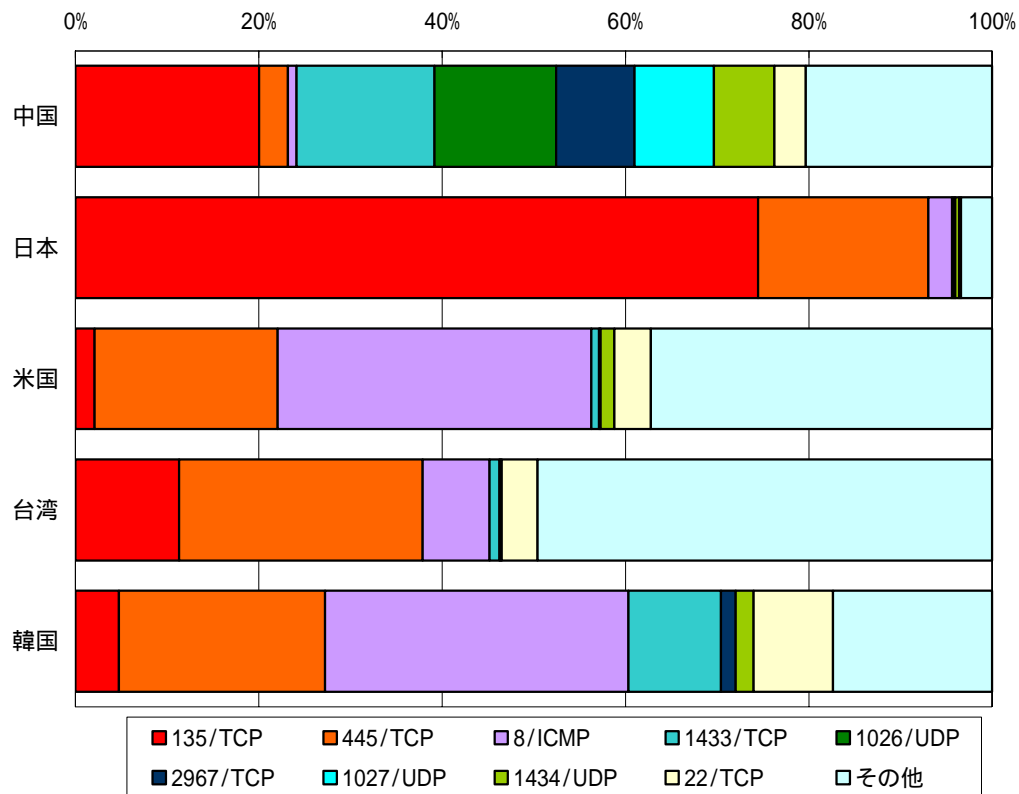
12月期と比較して、445/TCP 及び 135/TCP に対するアクセスが増加し、8080/TCP 及び 8/ICMP に対するアクセスが減少した。25/TCP に対するアクセスは横ばいとなった。全体としては横ばいとなった。

韓国



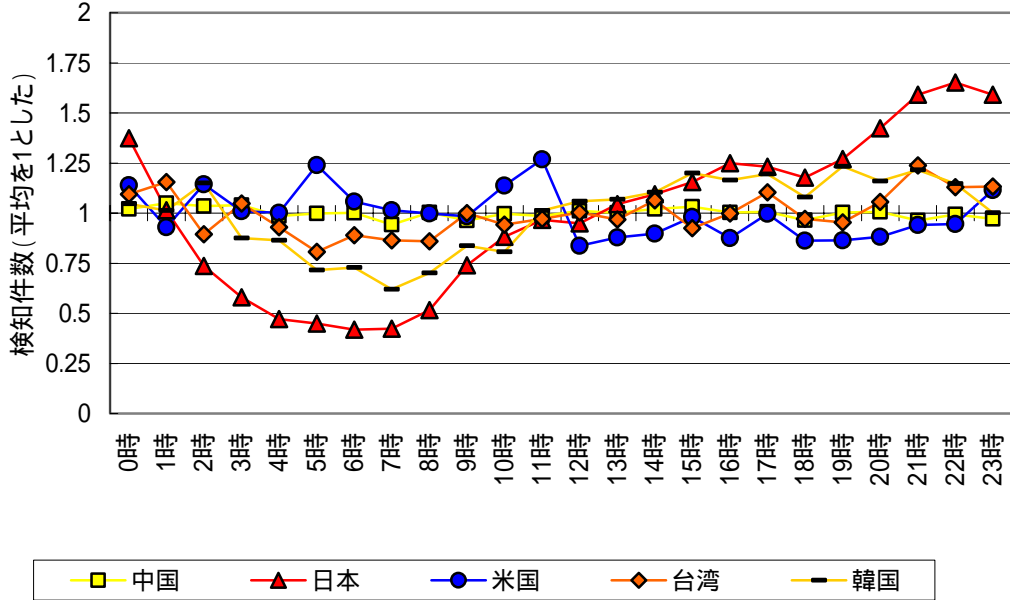
12月期と比較して、445/TCP に対するアクセスが、12月期に引き続き大幅に増加し、8/ICMP に対するアクセスがやや減少した。全体としては横ばいとなった。

(7) 上位国 / 地域の宛先ポート別比率

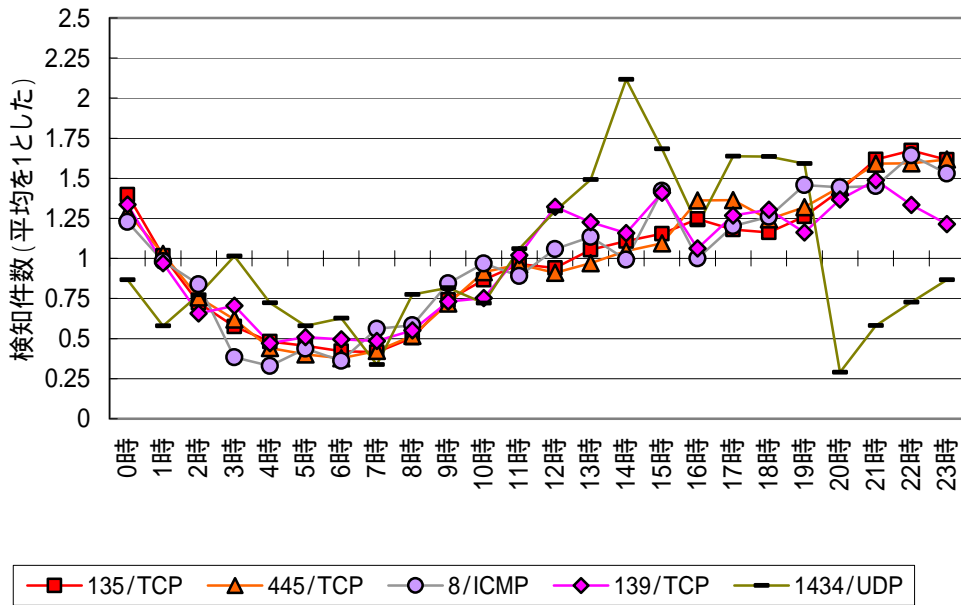


(8) 時間帯推移

上位5 各国

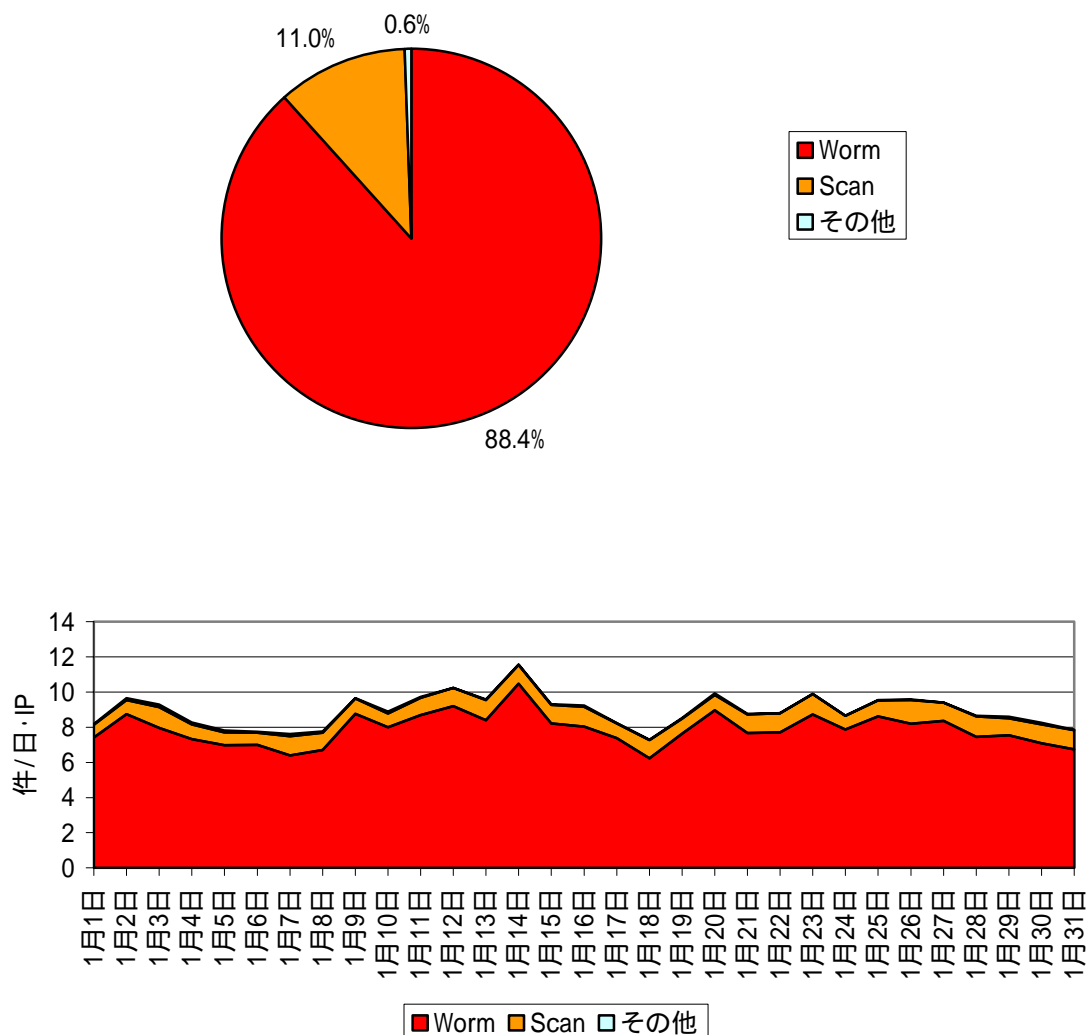


上位5 ポート(国内)



2.2 不正侵入検知システムにおける不正なアクセスの検知分析

(1) 攻撃手法別

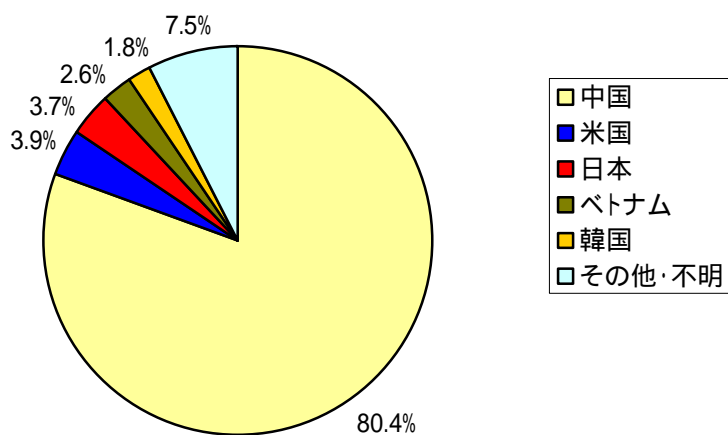


1月期の不正侵入検知システムにおける不正なアクセスの検知件数は、一日・1IP当たり8.92件で、12月期と比較して、-1.29件とやや減少(-12.6%)した。

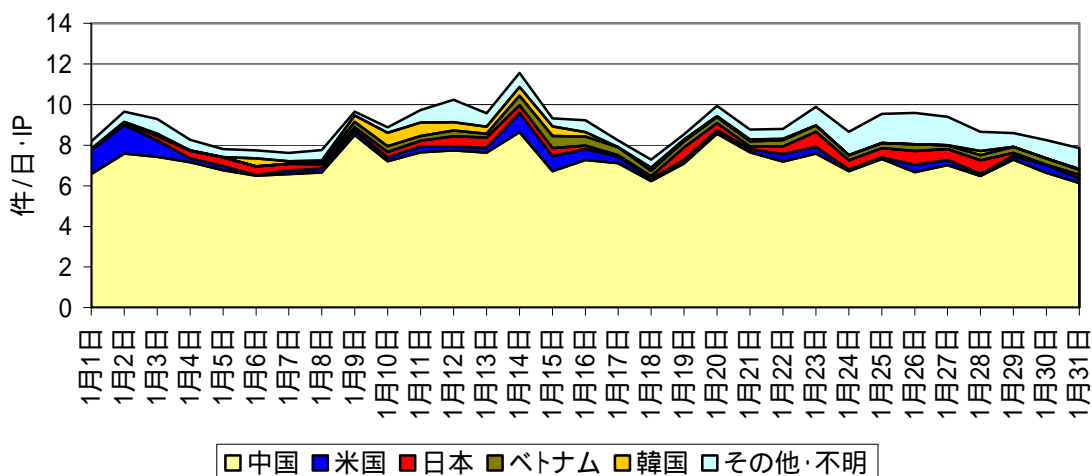
また、1月期における第1位のWorm(SQL Slammer ワーム)は、一日・1IP当たりの検知件数が7.89件で、12月期と比較して、-0.98件とやや減少(-11.1%)した。第2位のScanは0.98件で、-0.06件と横ばい(-5.6%)となった。

当データは、小数点第二位で四捨五入しているため、合計が100%にならないことがある。

(2) 発信元国 / 地域別



12月期に引き続き、中国を発信元とする不正なアクセスを最も多く検知している。中国を発信元とするアクセスの大半は、Worm (SQL Slammer ワーム) である。



12月期と比較して、全体の大部分を占める中国を発信元とする検知件数が、一日・1IPあたり - 0.92件とやや減少 (- 11.3%) し、第2位の米国を発信元とする検知件数が一日・1IPあたり - 0.51件と大幅に減少 (- 59.6%) したことから、全体としても、やや減少となった。

当データは、小数点第二位で四捨五入しているため、合計が100%にならないことがある。

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
●	インターネット治安情勢更新(平成20年度第3四半期報を追加)(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 (MS08-070,071,072,073,074,075,076,077)(1/16)更新
●	インターネット治安情勢更新(平成20年12月報を追加)(1/16)
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 (MS09-001)(1/14)

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 に集計している。

不正侵入検知システム

各定点の不正侵入検知装置には、平成 21 年 1 月 31 日現在、387 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、分類における上位 2 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。

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。