

平成 21 年 3 月 26 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 2 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
 - ～ 445/TCP に対するアクセス増加が続く～
 - Microsoft Windows の脆弱性を悪用した攻撃の危険性
 - ～ 1433/TCP に対するアクセスが増加～
 - Microsoft SQL Server の脆弱性を悪用した攻撃の危険性
 - ～ 2967/TCP に対するアクセスが増加
 - Symantec 製品の脆弱性を悪用した攻撃の危険性
- ・不正侵入検知システムにおける不正なアクセスはやや増加

1 概説

平成 21 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、一日・1IP 当たり 307.1 件で、平成 21 年 1 月期と比較して +35.3 件と、やや増加 (+13.0%) 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 2967/TCP の順であり、2967/TCP が順位を 1 つ上げた。

昨秋頃から増加傾向にある 445/TCP に対するアクセスが、今期もやや増加 (+22.2%) 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可能性がある。1433/TCP 及び 2967/TCP も増加 (それぞれ +29.4%、+76.1%) した。1433/TCP については Microsoft SQL Server の脆弱性を悪用した攻撃の可能性がある、2967/TCP については Symantec 製品の脆弱性を悪用した攻撃の可能性がある。

中国及び韓国からのアクセスが増加 (それぞれ +26.5%、+27.3%) した。アクセス件数の上位 5 か国は、中国、日本、米国、韓国及び台湾の順となり、1 月期と比較して韓国と台湾が入り替わった。中国については 1433/TCP 及び 2967/TCP に対するアクセスの増加が影響し、韓国については 445/TCP に対するアクセスの増加が影響している。

2 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 9.71 件で、1 月期と比較して、+0.79 件とやや増加 (+8.8%) した。米国からの Scan の増加が目立つ。

攻撃手法別では、第 1 位の Worm (SQL Slammer ワーム) は横ばいで推移した一方で、第 2 位の Scan が増加 (+72.3%) した。

発信元国 / 地域別において、上位 5 か国は中国、米国、ベトナム、日本及び台湾の順であった。また、米国からの検知件数が大幅に増加 (+127.5%) した。

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

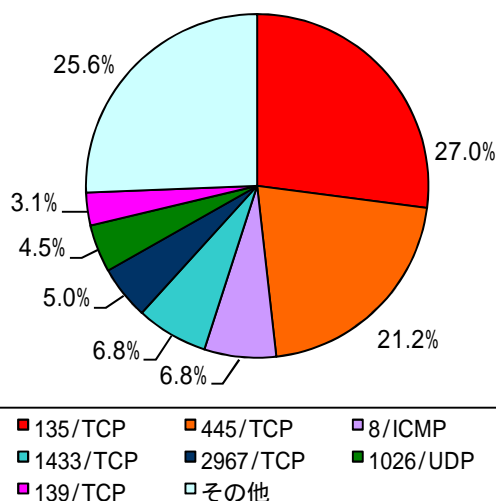
(1) 宛先ポート別概要

2 月期における上位 5 ポートは以下のとおりである。1 月期と比較して、445/TCP 及び 1433/TCP に対するアクセスが増加した。445/TCP に対するアクセスは 2008 年 9 月から増加傾向にある。2967/TCP も増加し、順位を 1 つ上げた。

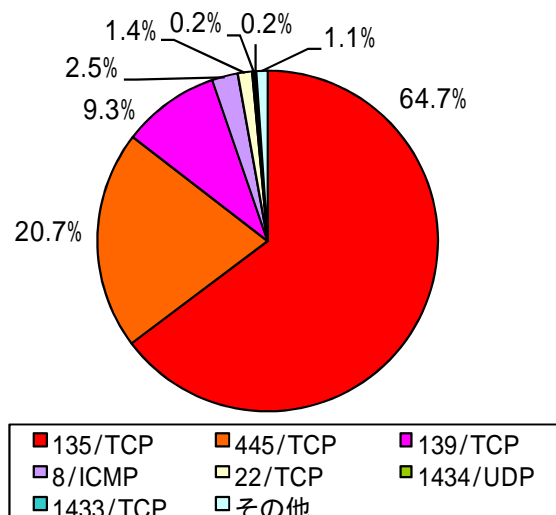
2 月期 順位	ポート	1 月期件数 (一日・1IP 当たり)	前期比 (一日・1IP 当たり)	1 月期 順位
1 位	135/TCP	83.05 件	- 2.8% (- 2.38 件)	1 位
2 位	445/TCP	65.04 件	+ 22.2% (+ 11.79 件)	2 位
3 位	8/ICMP	20.83 件	- 4.2% (- 0.91 件)	3 位
4 位	1433/TCP	20.79 件	+ 29.4% (+ 4.73 件)	4 位
5 位	2967/TCP	15.50 件	+ 76.1% (+ 6.70 件)	6 位

(2) 宛先ポート別比率

発信元/全世界



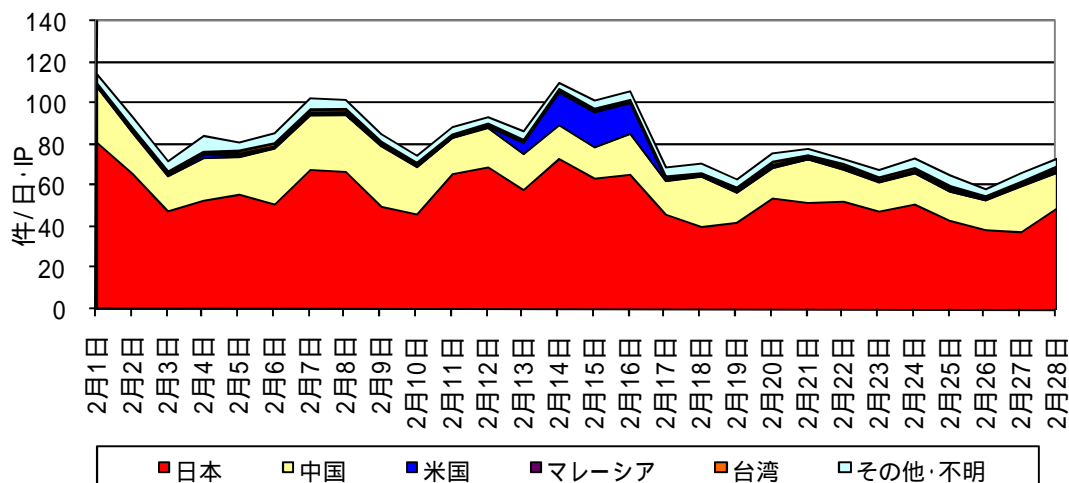
発信元/日本



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(上位 5 ポート)

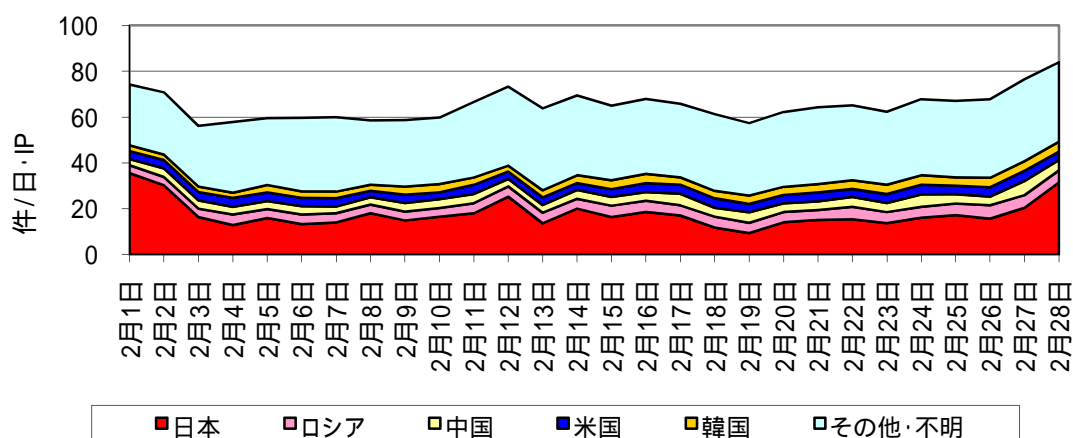
135/TCP



1月期と比較して、135/TCP に対するアクセスは横ばいであったが、月後半にかけて緩やかな減少傾向がみられる。1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。

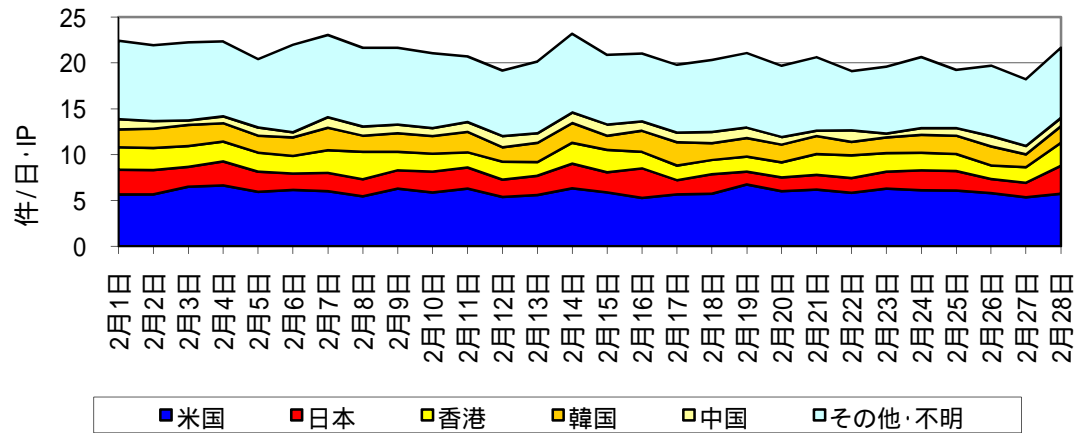
14日から16日における米国からのアクセス増加は、特定の1 IP アドレスからのものである。

445/TCP



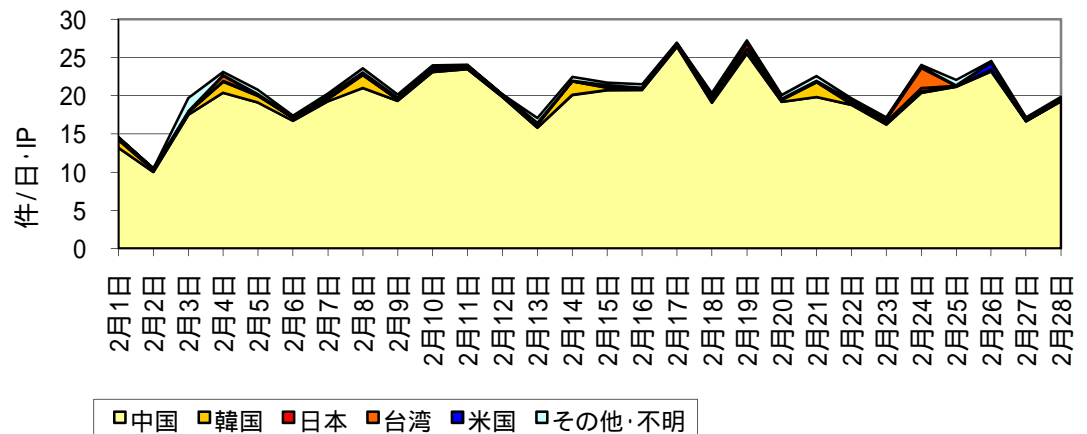
1月期に引き続き、445/TCP に対するアクセスが増加しており、Microsoft Windows 製品の Server サービスの脆弱性を悪用した攻撃が拡大している可能性がある。

8/ICMP



2008年12月からみられる緩やかな減少傾向が2月期においても確認された。

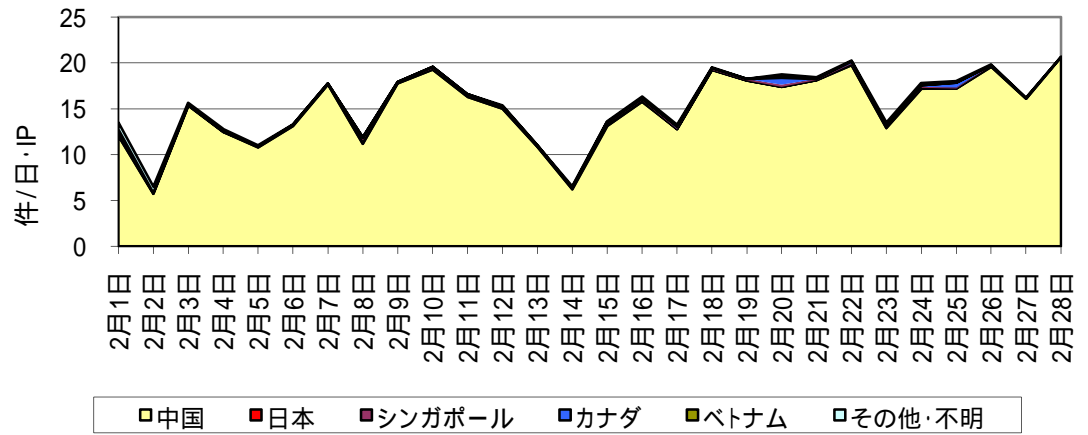
1433/TCP



1月期に引続き、中国からのアクセスが大半を占め、全体として増加した。

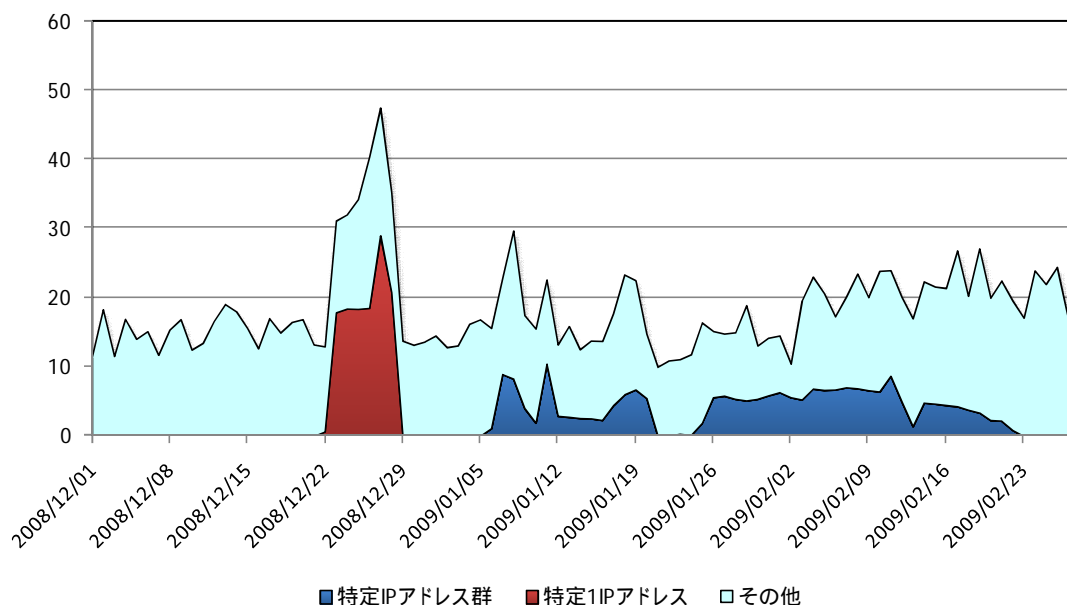
1433/TCPはMicrosoft SQL Serverが使用するポートであり、この製品の脆弱性を悪用した攻撃の可能性がある。

2967/TCP



大半を占める中国からのアクセスが増加したことから、全体としても増加した。
2967/TCP は、Symantec Client Security 及び Symantec Antivirus が使用するポートであり、これらの製品の脆弱性を悪用した攻撃の可能性がある。

(4) 1433/TCP の状況について



Microsoft SQL Server の脆弱性が 2008 年 12 月 23 日に公表され、2009 年 2 月 11 日に修正プログラムが提供されている。

脆弱性ととも実証コードが公表された日に特定の 1IP アドレスからのアクセスが急上昇した。当該 IP アドレスからのアクセスはこの時のみであることから、脆弱性の調査目的のアクセスであった可能性がある。その後、6 つの連続した IP アドレスから構成される特定 IP アドレス群からのアクセスが 2009 年 1 月 7 日及び 2009 年 1 月 26 日からの 2 度にわたって行われ、2009 年 2 月 23 日頃消滅した。また、上記特定アドレス以外の不特定多数の IP アドレスを発信元とするアクセスが 2009 年 2 月 3 日頃から増加し、2 月中は増加傾向を見せていた。

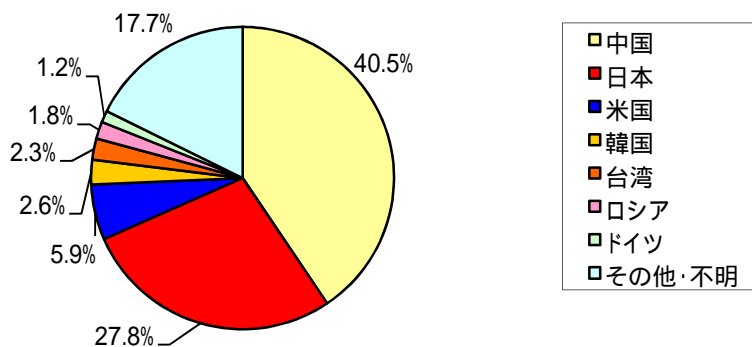
これらのことから、当該脆弱性を狙ったアクセスが不特定多数へと拡散している状況がうかがえる。

(5) 発信元国 / 地域別概要

2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。1月期と比較して、中国及び韓国からのアクセス増加が目立つ。中国については、1433/TCP及び2967/TCPに対するアクセスが増加し、韓国については445/TCPに対するアクセスが増加した。

2月期 順位	国/地域	2月期件数 (一日・1IP当たり)	前期比 (一日・1IP当たり)	1月期 順位
1位	中国	124.55件	+26.5% (+26.10件)	1位
2位	日本	85.51件	+6.6% (+5.32件)	2位
3位	米国	18.18件	+2.1% (+0.38件)	3位
4位	韓国	8.04件	+27.3% (+1.73件)	5位
5位	台湾	7.01件	-3.3% (-0.24件)	4位

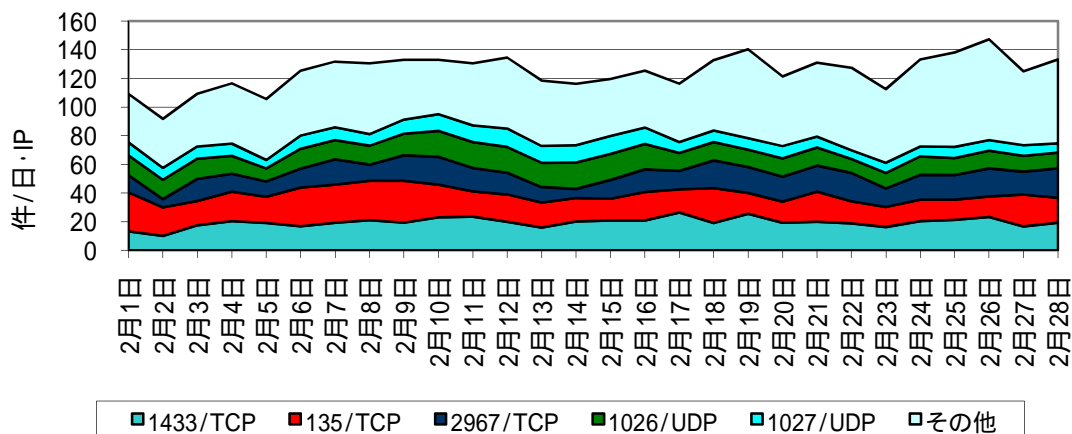
(6) 発信元国 / 地域別比率



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。

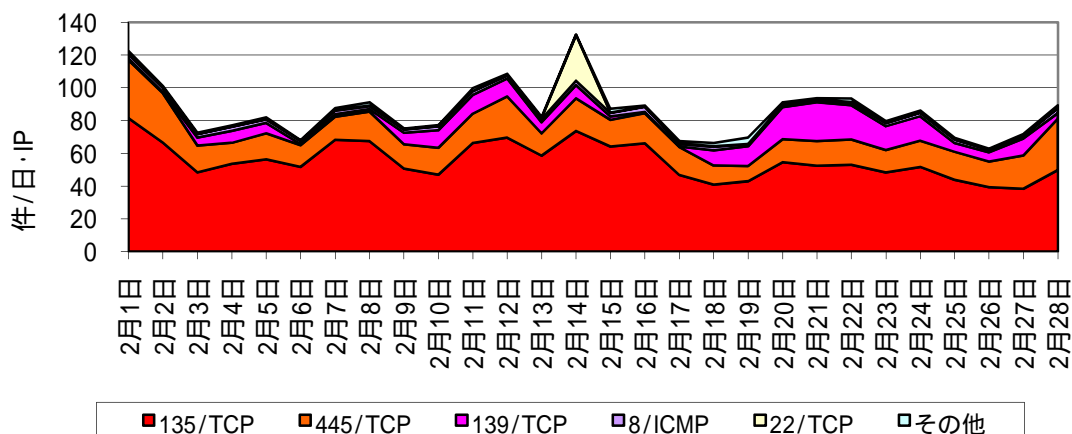
(7) 発信元国 / 地域別推移(上位 5 か国)

中国



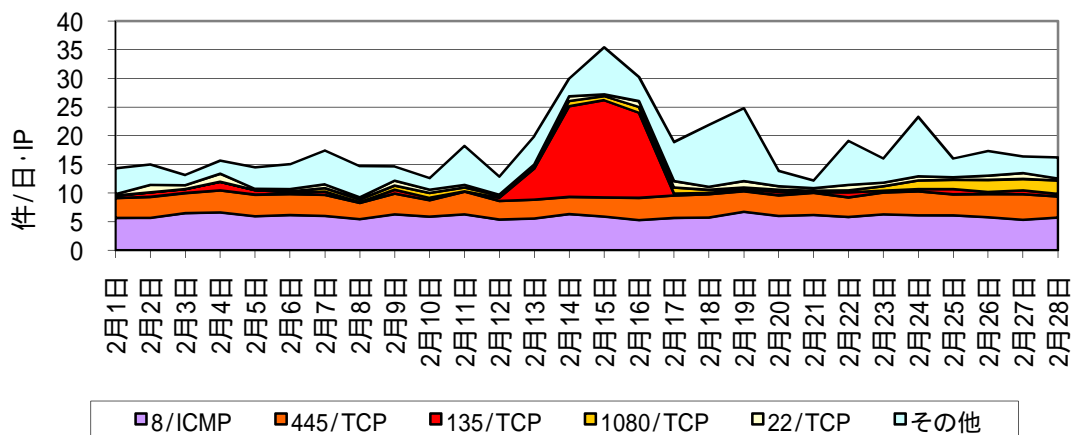
1 月期と比較して、1433/TCP 及び 2967/TCP に対するアクセスが増加したため、全体としても増加した。1433/TCP 及び 2967/TCP に対するアクセスは、その大半が中国からのものである。

日本



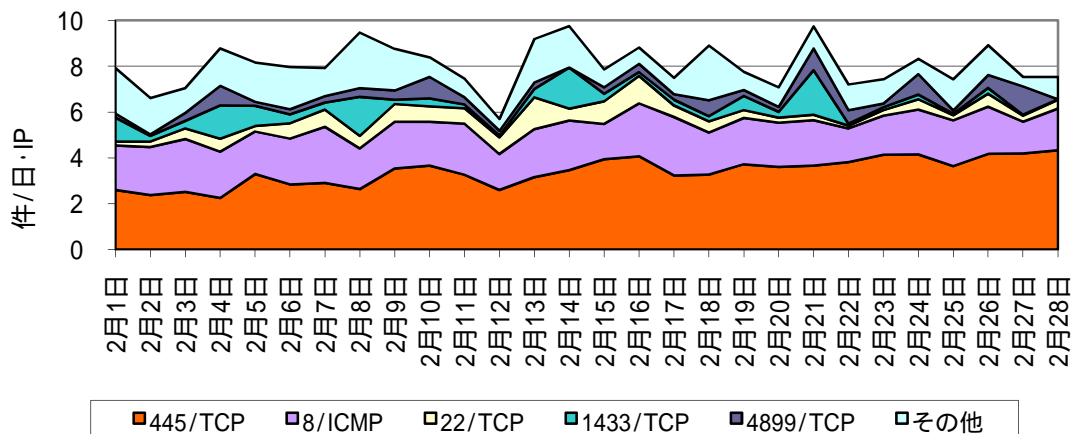
1 月期において減少していた 139/TCP に対するアクセスが大幅に増加した一方で、アクセスの大半を占める 135/TCP 及び 445/TCP が横ばいであったため、全体としても横ばいであった。

米国



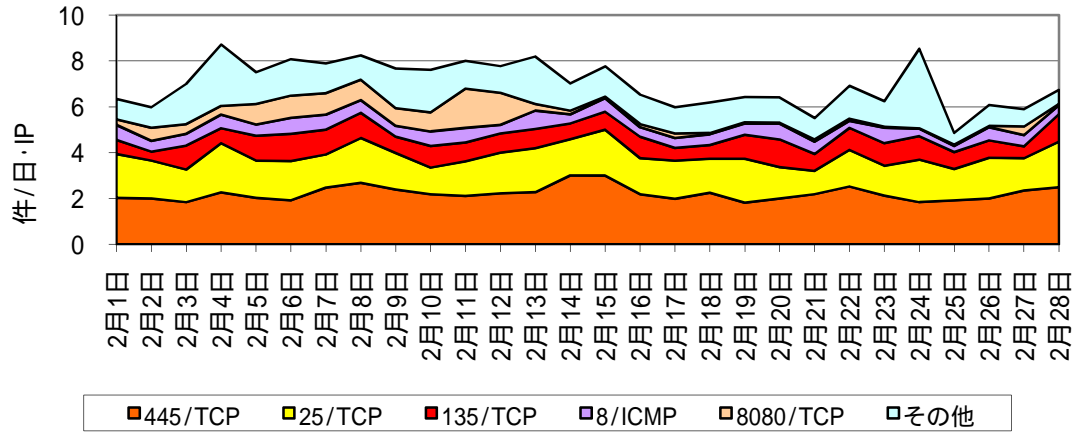
1月期と比較して、米国からのアクセスは、全体として横ばいであった。
 14日から16日における135/TCPに対するアクセス増加は、特定の1 IPアドレスによるものである。

韓国



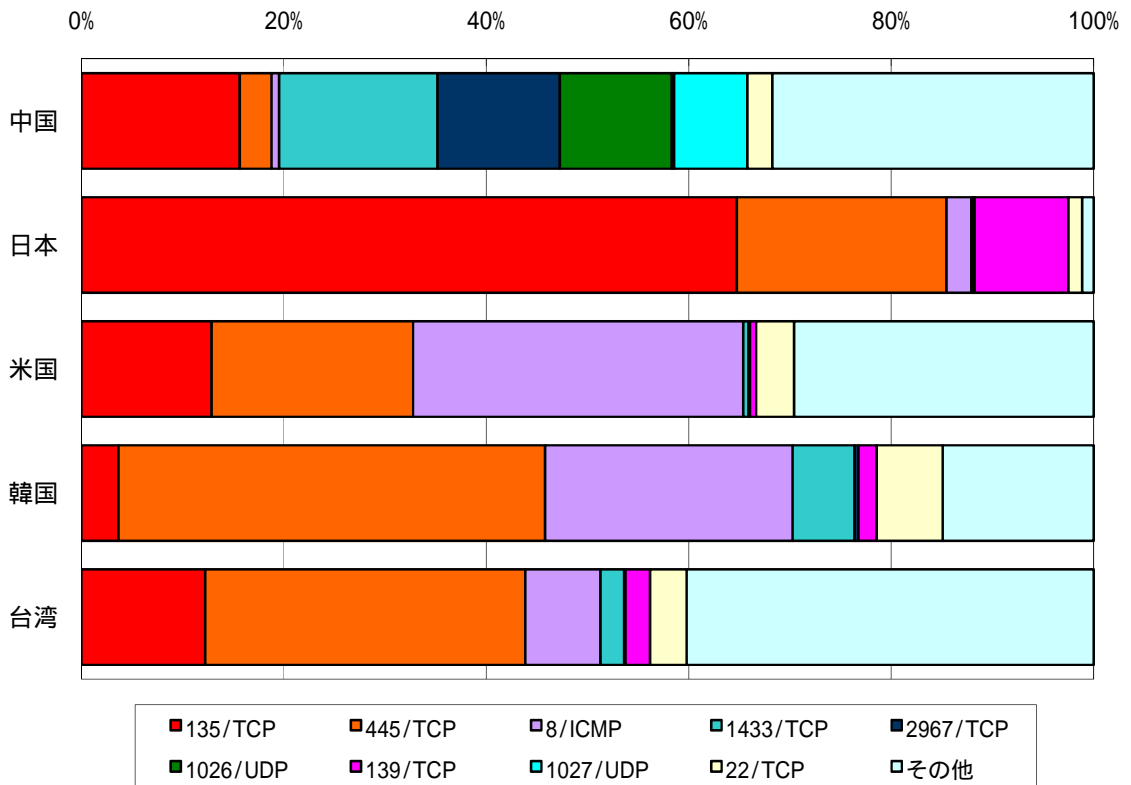
1月期と比較して、445/TCPに対するアクセスが大幅に増加したため、全体としても大幅な増加となった。445/TCPに対するアクセスは2008年12月頃から増加傾向がみられる。

台湾



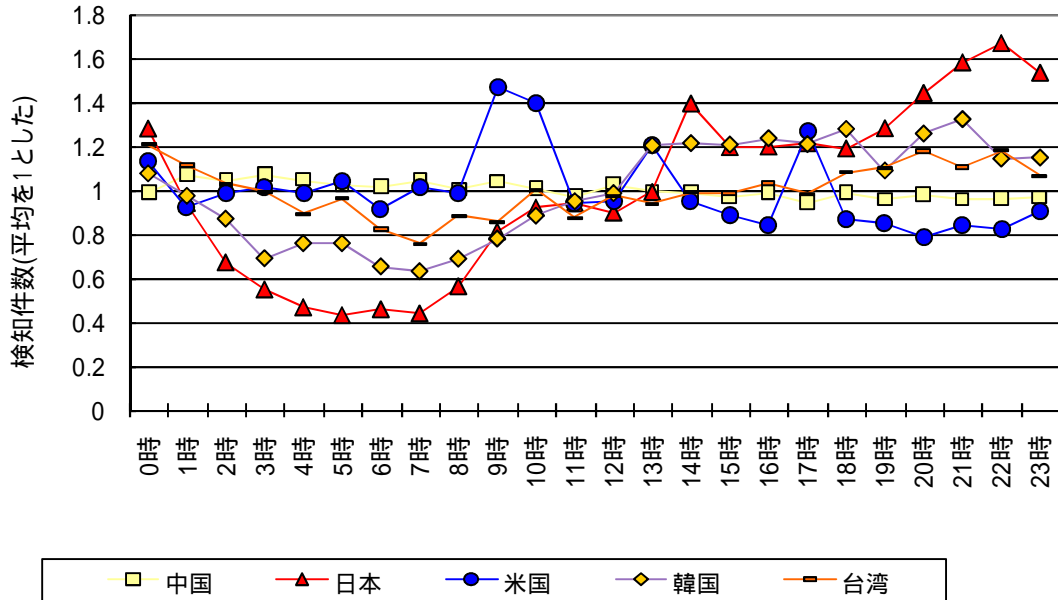
1月期と比較して、全体としては横ばいで推移した。24日の「その他」に分類されるアクセス増加は、1433/TCPに対する特定の1 IPアドレスからのものである。

(8) 上位国/地域の宛先ポート別比率

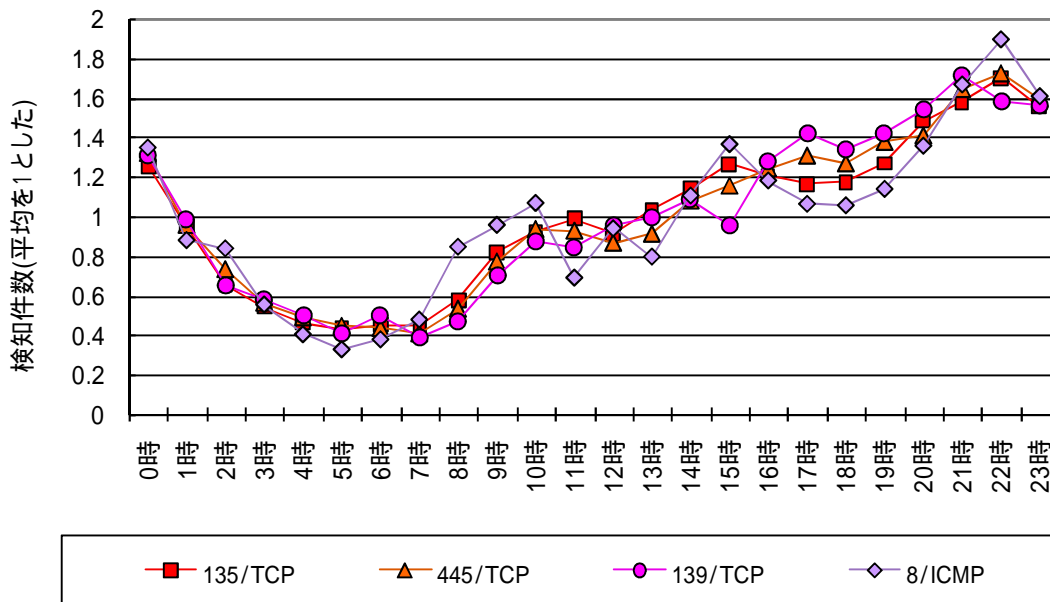


(9) 時間帯推移

上位 5 各国



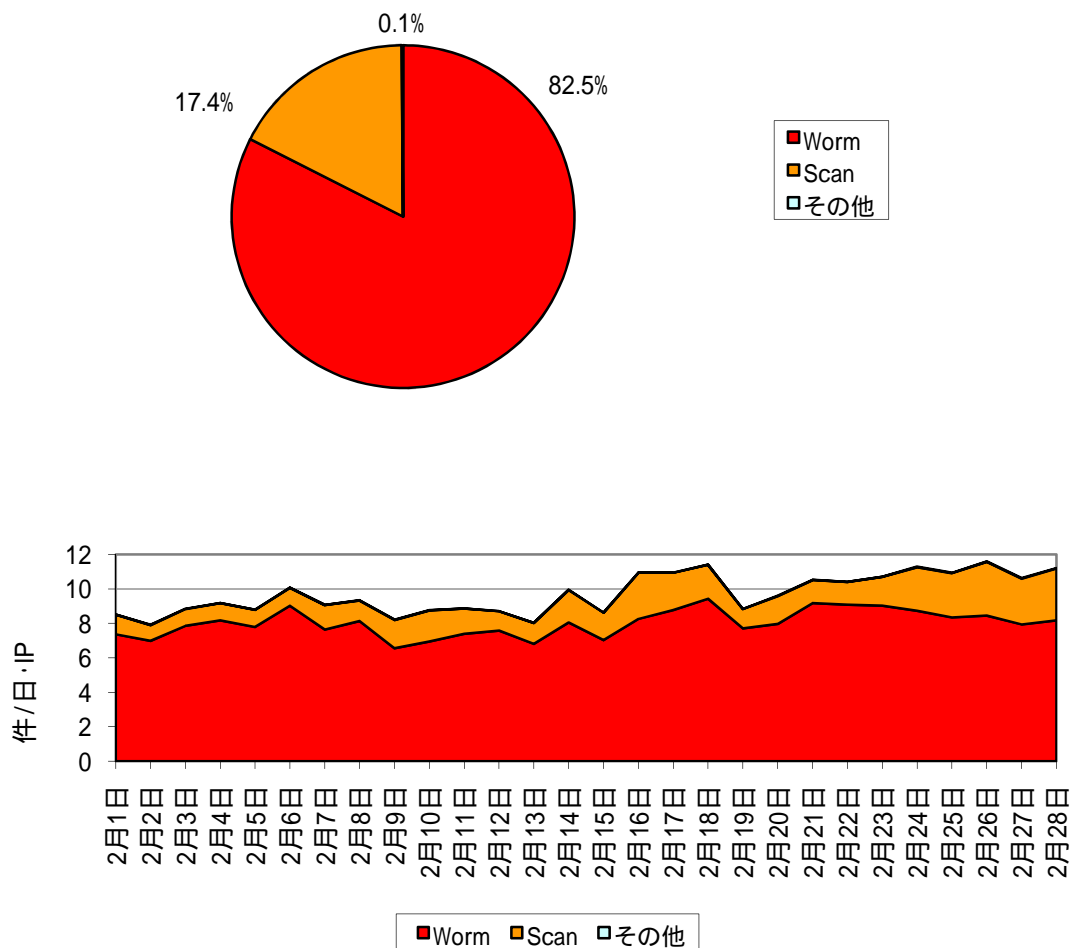
上位 5 ポート(国内)



22/TCP については特定の日に集中したアクセスがあり上位 5 位に入ったため、22/TCP に対するアクセスはグラフから除外した。

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

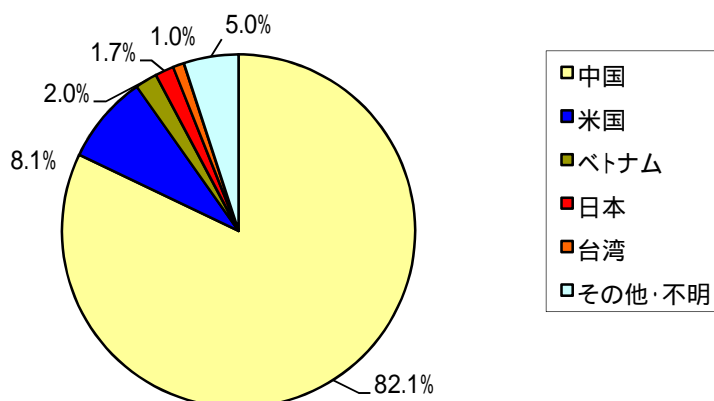


2月期の不正侵入検知システムにおける不正なアクセスの検知件数は、一日・1IP当たり9.71件で、1月期と比較して、+0.79件とやや増加(+8.8%)した。

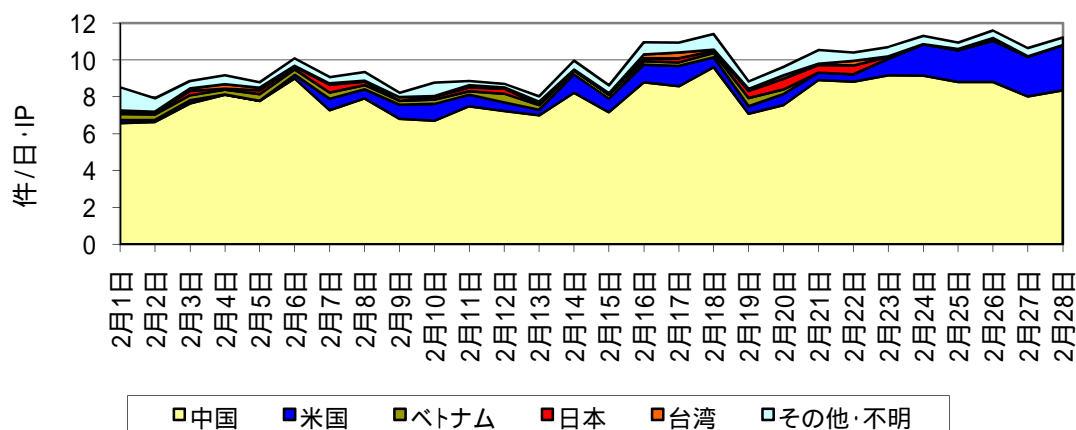
2月期における第1位のWorm(SQL Slammer ワーム)は、一日・1IP当たりの検知件数が8.01件で、1月期と比較して、+0.12件と横ばいだった。第2位のScanは1.69件で、+0.71件と増加(+72.3%)した。特に、米国からの検知件数が大幅に増加(+127.5%)した。

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



1 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。





1 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 7.97 件で、1 月期と比較して +0.80 件とやや増加 (+11.1%) した。第 2 位の米国を発信元とする検知件数が、一日・1IP あたり 0.79 件で、+0.44 件と大幅に増加 (+127.5%) した。

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
●	インターネット治安情勢更新(平成20年報を追加)(2/26)
	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 (MS09-002,003,004,005)(2/17)更新
	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 (MS08-037,038,039,040)(2/12)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 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 2 月 28 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。