

平成 21 年 5 月 28 日

## 我が国におけるインターネット治安情勢

(平成 21 年 4 月期)

- ・ 445/TCP に対するアクセスが、依然として高い水準で推移  
～ 「Conficker」ワームの影響とみられる ～

### 1 概説

今期におけるセンサーに対するアクセス件数は、一日・1IP 当たり 368.2 件で、前期と比較して - 22.0 件 (- 5.6%) と、やや減少した。

アクセス件数の上位 5 ポートは、445/TCP、135/TCP、ICMP Echo Request (以降、「8/ICMP」と表記する。)、1433/TCP 及び 2967/TCP の順であった。

最もアクセス件数が多い 445/TCP は、一日・1IP 当たり 106.8 件と、全体の 29.0% を占めた。これは、昨年から流行している「Conficker」ワームの影響と考えられる。445/TCP に対するアクセスは、平成 20 年 10 月以降、増加傾向がみられ、引き続き警戒の必要がある。

アクセス件数の上位 5 か国は、中国、日本、米国、台湾及びロシアの順であった。

中国及び日本国内からのアクセスが減少したが、検知比率としては、中国及び日本で全体のほぼ 6 割を占めている。

今期のシグネチャを用いた不正侵入等の検知件数は、一日・1IP 当たり 25.6 件で、前期と比較して - 3.9 件 (- 13.1%) と、やや減少した。

## 2 注目すべきアクセス

### 2-1 135/TCP 及び 445/TCP に対するアクセス

日本国内からのアクセスは、平成 18 年 10 月以降、135/TCP に対するアクセスが 1 位、445/TCP に対するアクセスが 2 位という状況が続いていたが、今期において順位が逆転した(図 2-1)。

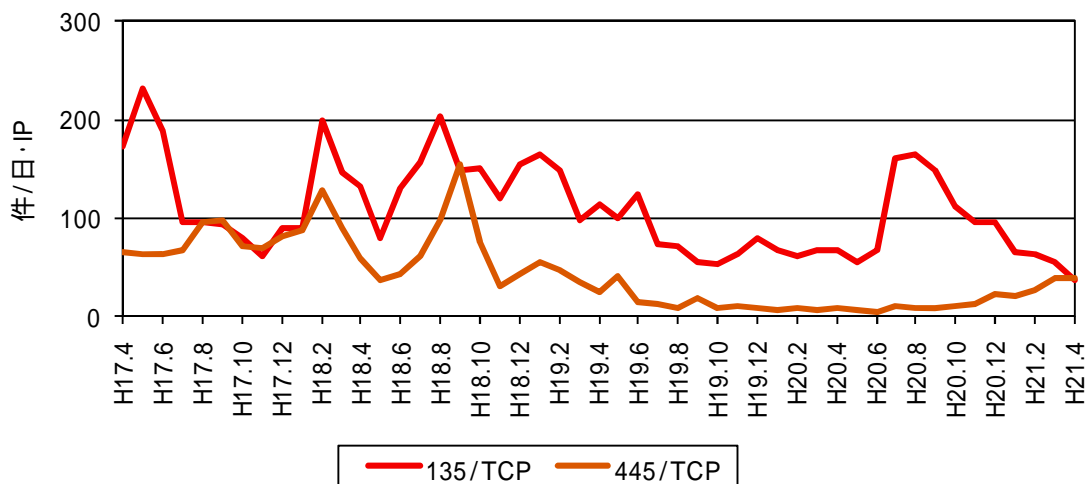


図 2-1 135/TCP 及び 445/TCP のアクセスの推移(平成 17 年 4 月以降、日本国内)

135/TCP は、Microsoft 社の Windows NT/2000/XP 等における共有ネットワーク(RPC)で使われるポートである。平成 15 年 7 月に Microsoft 社のセキュリティ情報(MS03-026)が公表され、この脆弱性を悪用する「Blaster」ワームが、平成 15 年 8 月に大流行したが、これより後では、当該ポートを利用するサービスの脆弱性を悪用したワームの大きな流行は確認されていない。

日本国内からの 135/TCP に対するアクセスは、平成 20 年 9 月以降、減少傾向となっており、鎮静化に向かっている可能性がある(図 2-2)。

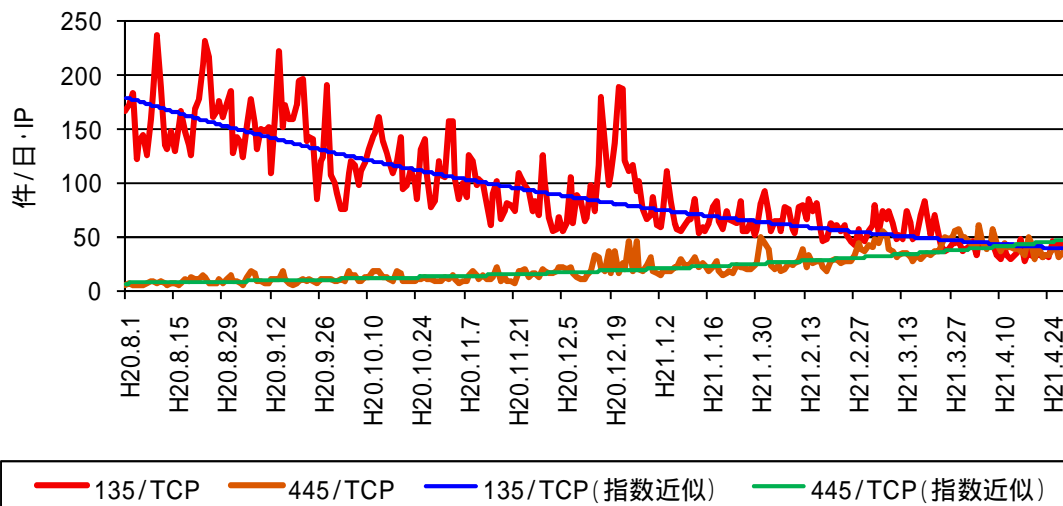


図 2-2 135/TCP 及び 445/TCP のアクセスの推移(平成 20 年 8 月以降、日本国内)

これに対して、445/TCP に対するアクセスは、平成 20 年 10 月以降、増加傾向がみられる(図 2-2)。

445/TCP は、Microsoft 社の Windows2000 以降の製品における共有ネットワーク(SMB)において使われるポートである。

この 445/TCP の増加傾向は、平成 20 年 10 月以降、多くの国において見られ、Microsoft 社のセキュリティ情報(MS08-067)で公表された脆弱性を悪用する、「Conficker」ワーム等の悪意のあるソフトウェアの感染の拡大によるものである<sup>†</sup>。

これまで述べてきたとおり、135/TCP に対するアクセスが減少傾向であるのに対し、445/TCP に対するアクセスは増加傾向がみられる。今後も 445/TCP に対するアクセスの動向について、引き続き警戒の必要がある。

<sup>†</sup> 「我が国におけるインターネット治安情勢(平成 20 年度第 4 / 四半期)」  
[http://www.cyberpolice.go.jp/detect/pdf/20090428\\_1.pdf](http://www.cyberpolice.go.jp/detect/pdf/20090428_1.pdf)

## 2 - 2 UDP spam の検知状況

4 月期のシグネチャを用いた不正侵入等の検知では、攻撃手法別で、UDP spam<sup>†</sup>を多数検知している。UDP spam の発信元国 / 地域別では、中国が多数を占める (図 2-3)。

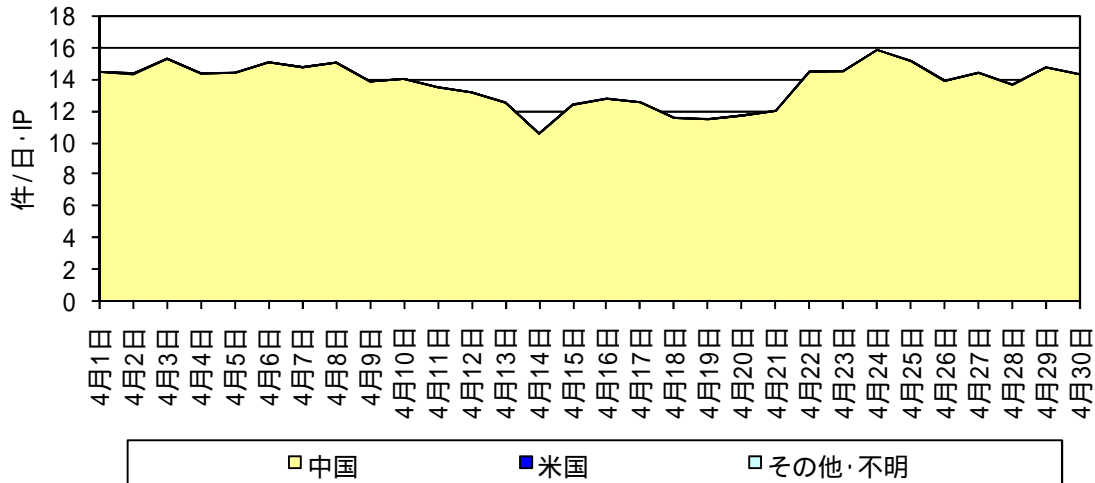


図 2-3 UDP spam 発信元国 / 地域別アクセスの推移

UDP spam の発信元は、IP アドレスが連続する複数のグループに分類される。今期は3つのグループからの検知があった (図 2-4)。各グループからのアクセスを、安定して検知している。

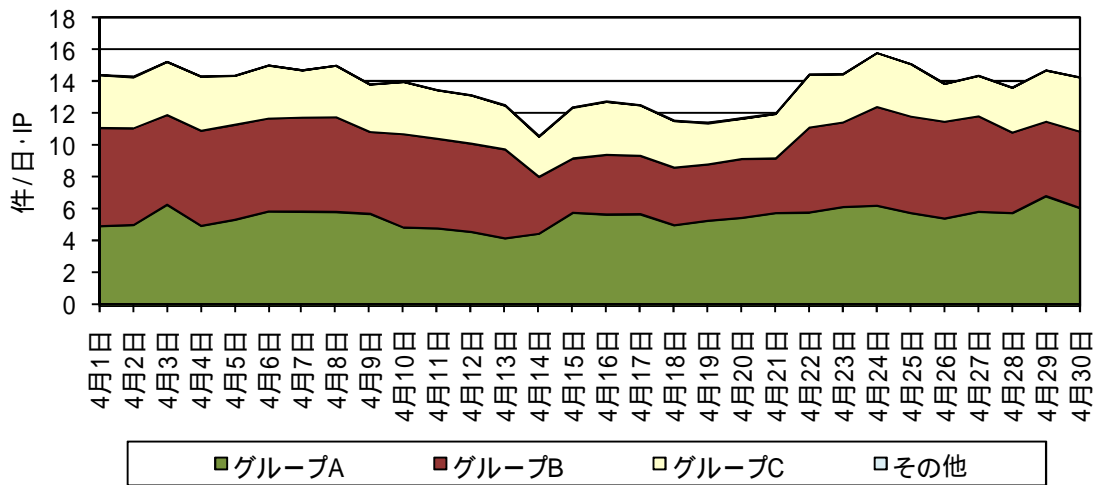


図 2-4 UDP spam 発信元グループ別アクセスの推移

各発信元グループからのアクセスは、一斉に変化することが観測された。図 2-5 の 33 ~ 34 時では、グループ内の全ての IP アドレスからの検知がない。これは、回線異常、または、何者かが一斉指令を行い、送信活動の停止、再開を行っている等の可能性が考えられる。

<sup>†</sup> UDP spam については、新たにシグネチャを追加し、平成 21 年 3 月期から観測を行っている。

<sup>‡</sup> 「Messenger スパムの情勢について」

[http://www.cyberpolice.go.jp/server/rd\\_env/20080821\\_MessengerSpam.pdf](http://www.cyberpolice.go.jp/server/rd_env/20080821_MessengerSpam.pdf)

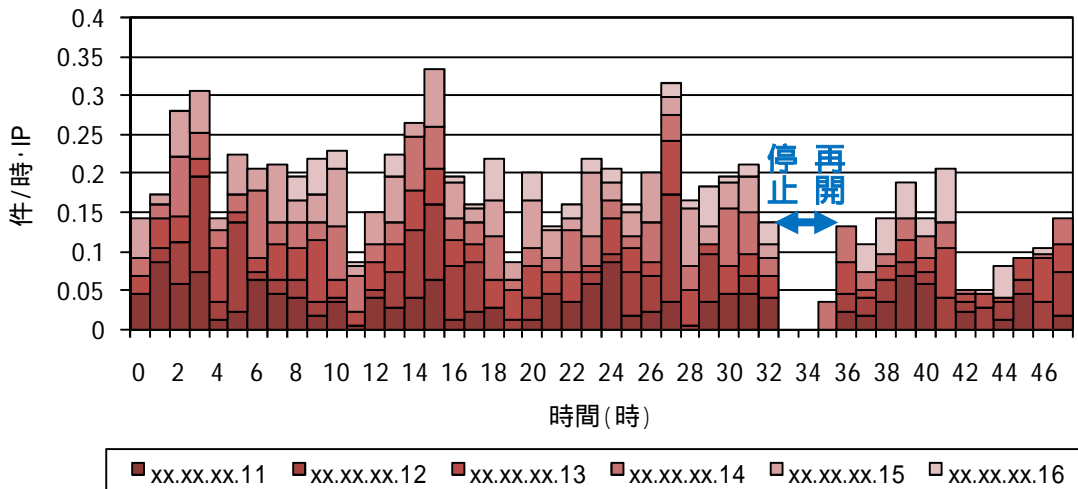


図 2-5 グループ B の検知状況が一斉に変化する例

また、図 2-6 のように、ある時刻を境に、一斉にメッセージが変更されることも確認した。何者かが手動または自動でメッセージを変更するシステムの存在がうかがえる。メッセージの内容は、何らかのプログラムをダウンロードするように促すものが多い。

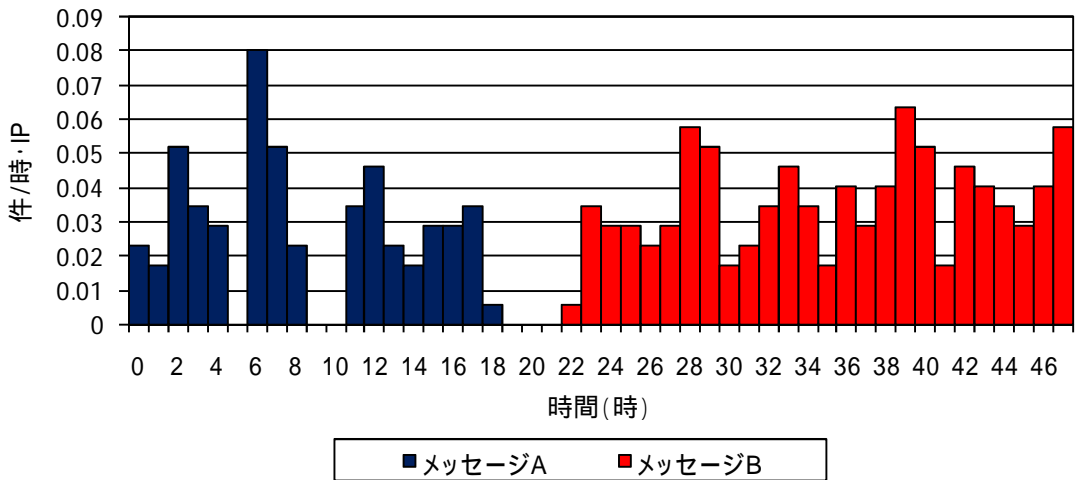


図 2-6 メッセージが変化する例

このような UDP spam は、ほぼすべてのセンサーで検知している。送信者は、送信先のアドレスブロック、メッセージ内容を役割分担しながら不特定多数の IP アドレスへメッセージを送信できる安定したシステムを保有しており、複数の発信元 IP アドレスを詐称、あるいは実際に複数のホストを使用しているものと考えられる。

Windows XP SP2 以降の OS であれば、Messenger サービスが標準で無効になっていることから、UDP spam 自体の脅威は小さいと考えられる。しかし、今後このシステムを使用して、新たな脆弱性への攻撃を行うことも考えられる。

### 3 インターネット定点観測 センサーに対するアクセス

#### 3-1 宛先ポート別

##### (1) 概要

ワームやボットの感染活動に利用される 445/TCP、135/TCP 及び 8/ICMP に対するアクセスが上位を占めている。

445/TCP に対するアクセスは「Conficker」ワームの影響もあり、今期も多かった。135/TCP に対するアクセスは減少しているものの、依然として多く、特に発信元が日本であるものが多い(図 3-3)。445/TCP 及び 135/TCP の詳細は、「2-1 135/TCP 及び 445/TCP に対するアクセス」で述べている。

今期増加順位 2 位の 1225/UDP は、突発的なものであった。今期では、1225/UDP 及び 1747/UDP に対する突発的なアクセスがあったが、これらの目的は確認できていない。今期増加順位 4 位の 17832/TCP は、跳ね返りパケット\* であった。

表 3-1 宛先ポート検知件数

今期 順位	前期 順位	ポート	今期 件数	前期比	今期 増加順位	今期 減少順位
1位	1位	445/TCP	106.83 件	+ 5.4% (+ 5.50 件)	1位	
2位	2位	135/TCP	60.42 件	- 23.4% (- 18.43 件)		1位
3位	3位	8/ICMP	28.44 件	- 5.0% (- 1.48 件)		4位
4位	4位	1433/TCP	22.51 件	- 0.1% (- 0.03 件)		
5位	5位	2967/TCP	10.91 件	- 11.6% (- 1.43 件)		
...			...			
8位	9位	139/TCP	8.50 件	+ 11.9% (+ 0.91 件)	5位	
9位	7位	1434/UDP	5.90 件	- 31.3% (- 2.69 件)		2位
...			...			
12位	11位	8080/TCP	3.49 件	- 30.8% (- 1.55 件)		3位
13位	23位	23/TCP	3.12 件	+ 229.4% (+ 2.17 件)	3位	
...			...			
16位	-	1225/UDP	2.34 件	- †(+ 2.34 件)	2位	
...			...			
20位	-	17832/TCP	1.54 件	- †(+ 1.54 件)	4位	
...			...			
-	18位	38951/TCP	検知なし	- ‡(- 1.47 件)		5位

\* 跳ね返りパケットとは、DoS 攻撃の一種である SYN flood 攻撃において、発信元 IP アドレスを無作為に詐称した攻撃パケットに対する応答パケットのこと。

† 前期の検知件数が少なかった(1225/UDP は 0 件、17832/TCP は 0.01 件)ため、前期比率は記載していない。

‡ 今期の検知件数が 0 件であるため、前期比率は記載していない。

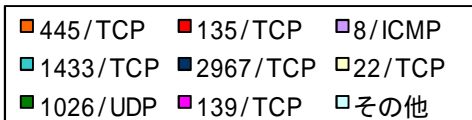
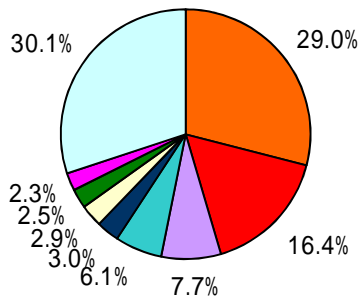


図 3-1 世界の宛先ポート別比率<sup>†</sup>

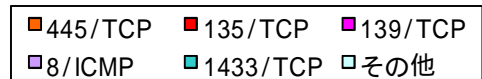
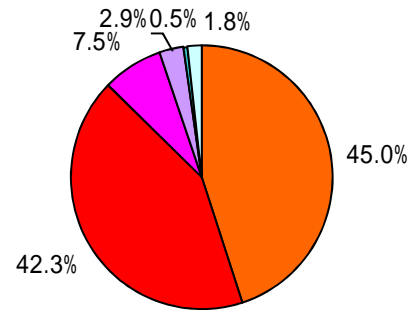


図 3-2 日本の宛先ポート別比率<sup>†</sup>

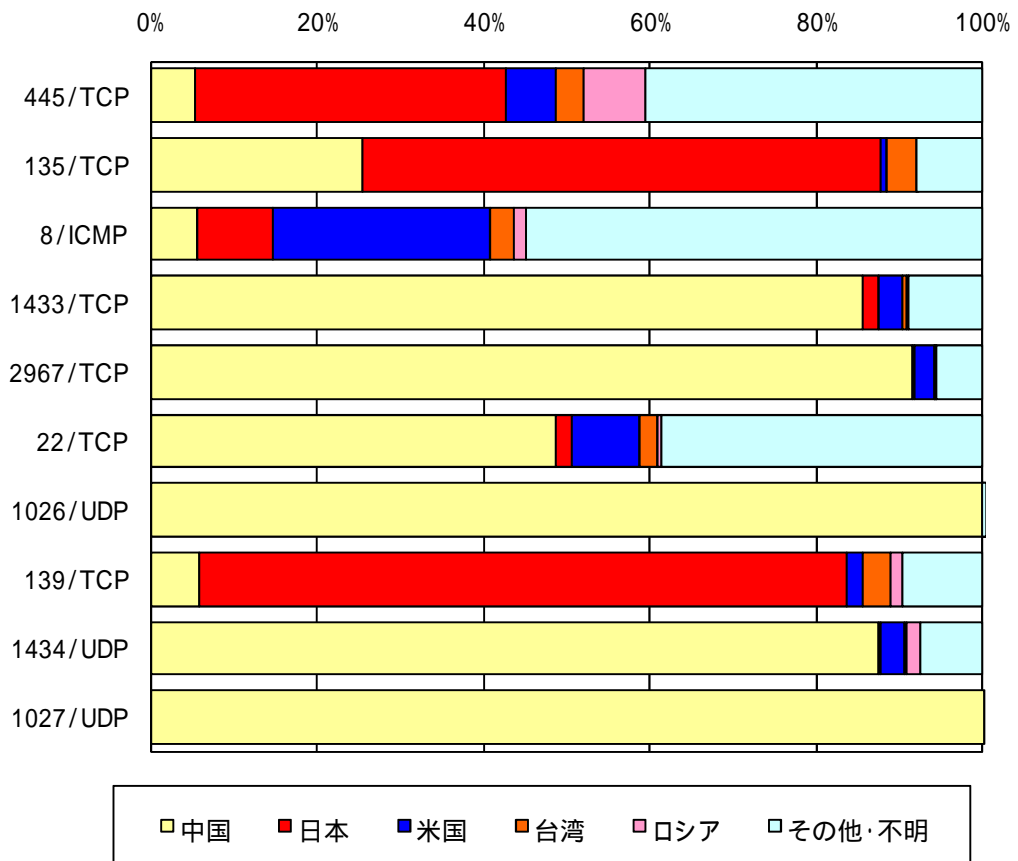


図 3-3 宛先ポートの国別比率

<sup>†</sup> 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) 推移

445/TCP は Microsoft 社の Windows2000 以降の製品における共有ネットワーク(SMB)において使われるポートであり、135/TCP は Microsoft 社の Windows NT/2000/XP 等における共有ネットワーク(RPC)で使われるポートである。8/ICMP は PING でのネットワーク診断で使用される。445/TCP、135/TCP 及び 8/ICMP は今期での大きな変動はなかった。445/TCP 及び 135/TCP の詳細は、「2 - 1 135/TCP 及び 445/TCP に対するアクセス」で述べている。

1433/TCP は、Microsoft SQL Server で使用されるポートであり、2967/TCP は Symantec 社製品で使用されるポートで、それぞれ 2009 年 2 月、2007 年 4 月に脆弱性が発表されている。

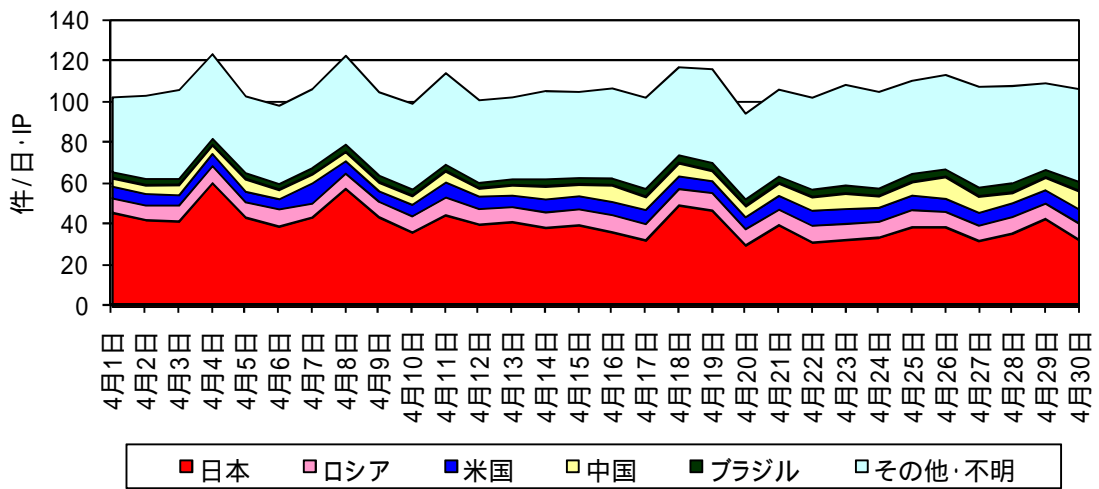


図 3-4 宛先ポート 445/TCP に対するアクセスの推移

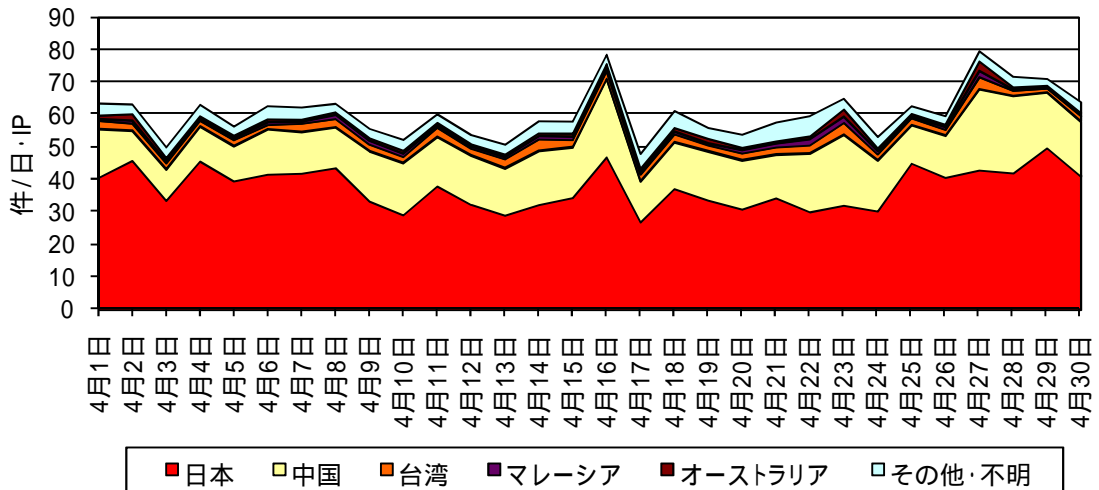


図 3-5 宛先ポート 135/TCP に対するアクセスの推移

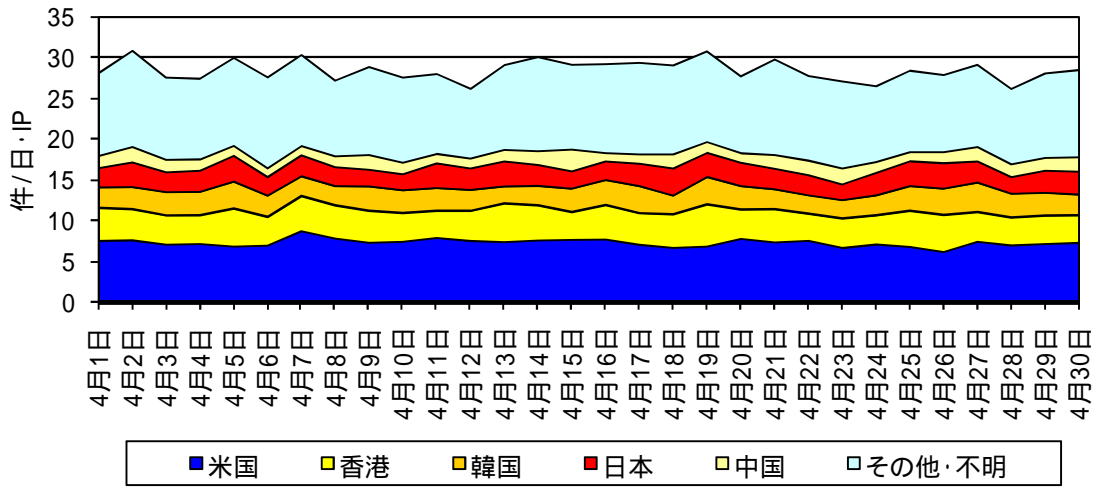


図 3-6 8/ICMP のアクセスの推移

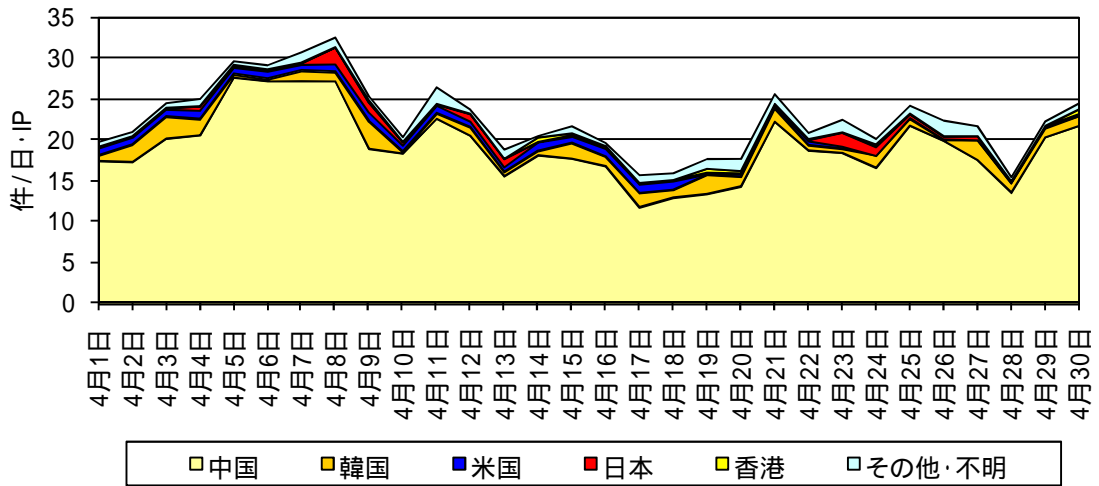


図 3-7 宛先ポート 1433/TCP に対するアクセスの推移

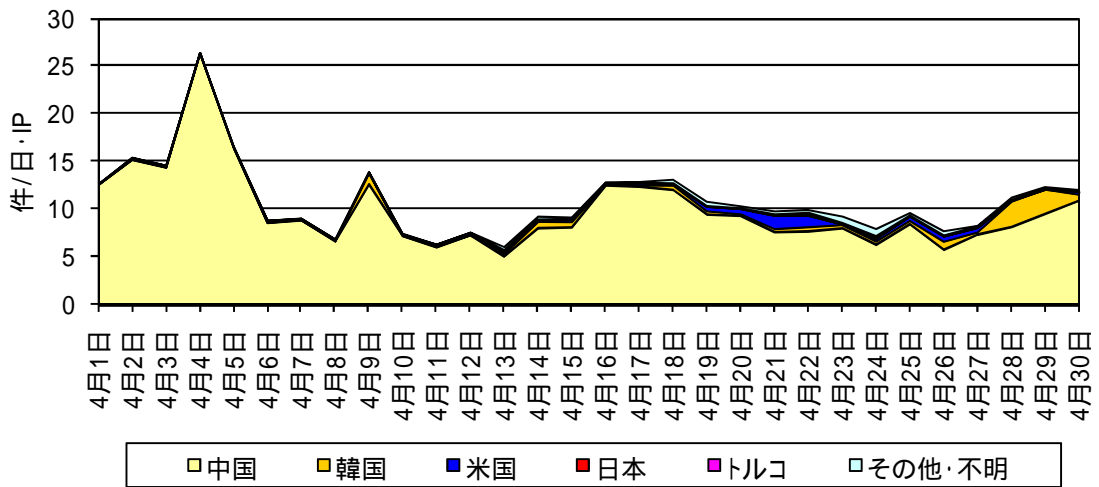


図 3-8 宛先ポート 2967/TCP に対するアクセスの推移

### 3-2 発信元国 / 地域別

#### (1) 概要

今期における国 / 地域別検知状況は、以下のとおりである。検知件数上位 8 位までに登場する発信元国 / 地域では、台湾から 135/TCP に対するアクセスが増加した影響で、台湾の順位が前期 5 位から今期 4 位となった。中国及び日本国内からのアクセスの減少が目立ち、検知件数の順位に変動はないものの、それぞれ今期減少順位 2 位、1 位となった。検知比率としては、中国及び日本で全体のほぼ 6 割を占めている。

米国、フランス等から、P2P ソフトウェアの通信と考えられるアクセスを、短期間に複数回、大量に検知した。ただし、発信元 IP アドレスは詐称されている可能性が高い。

表 3-2 国 / 地域別検知件数

今期 順位	前期 順位	国/地域	今期件数	前期比	今期 増加順位	今期 減少順位
1 位	1 位	中国	129.09 件	- 7.7% ( - 10.75 件)		2 位
2 位	2 位	日本	88.92 件	- 16.2% ( - 17.15 件)		1 位
3 位	3 位	米国	26.70 件	+ 5.8% ( + 1.46 件)	1 位	
4 位	5 位	台湾	12.26 件	+ 13.1% ( + 1.42 件)	2 位	
5 位	4 位	ロシア	11.51 件	+ 5.1% ( + 0.56 件)		
6 位	6 位	韓国	9.83 件	- 8.7% ( - 0.93 件)		3 位
7 位	7 位	ブラジル	7.60 件	+ 16.9% ( + 1.10 件)	3 位	
8 位	8 位	香港	5.97 件	+ 16.3% ( + 0.84 件)	5 位	
...			...			
12 位	14 位	フランス	3.95 件	+ 28.5% ( + 0.87 件)	4 位	
13 位	11 位	英国	3.34 件	- 16.3% ( - 0.65 件)		5 位
...			...			
44 位	28 位	イスラエル	0.58 件	- 55.9% ( - 0.73 件)		4 位

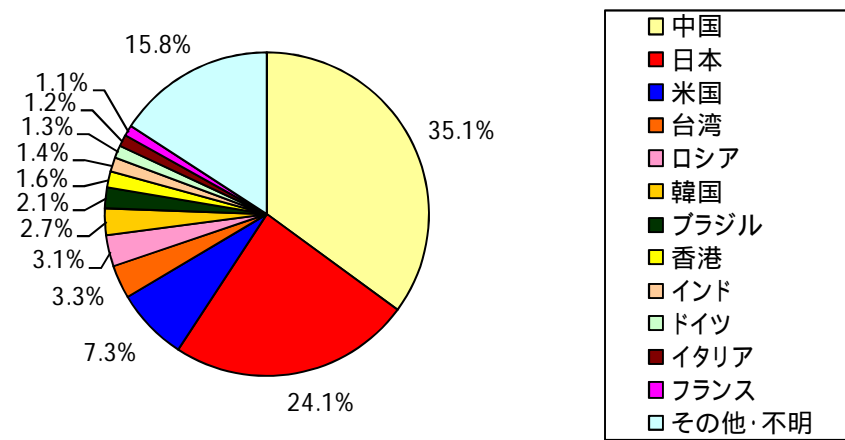


図 3-9 発信元国 / 地域別比率<sup>†</sup>

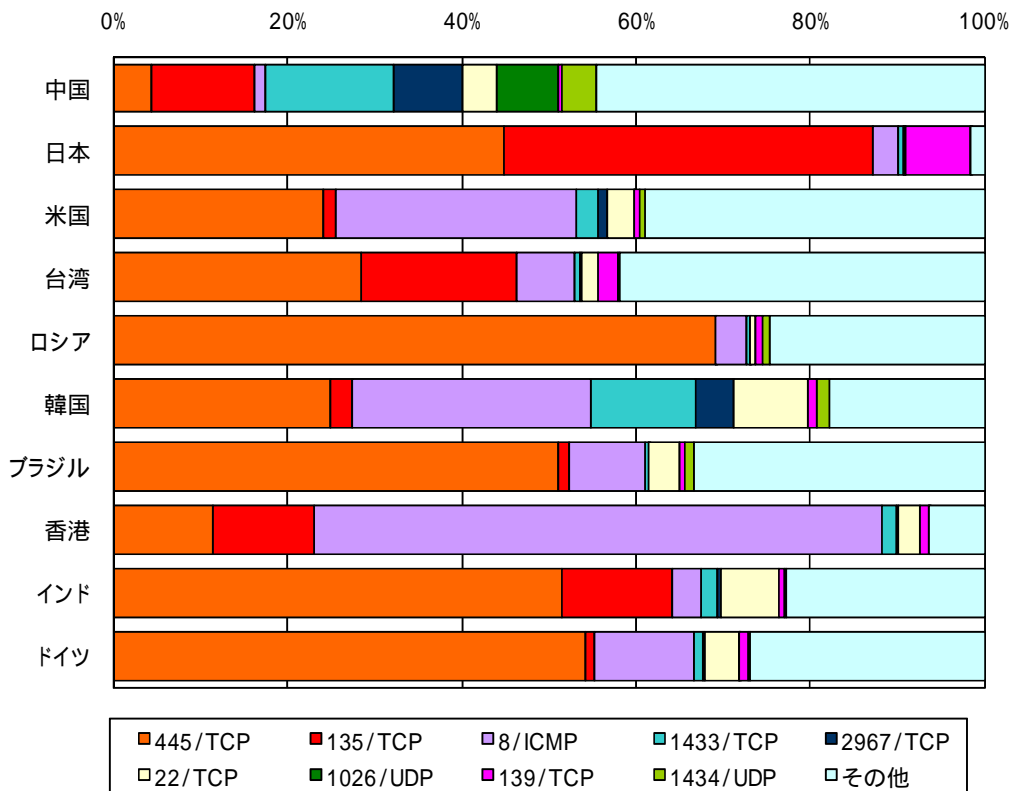


図 3-10 発信元国 / 地域別上位のポート別比率

<sup>†</sup> 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) 推移

中国からのアクセスは、他の多くの国・地域と異なり、2967/TCP や 1026/UDP 等が上位ポートとなっている。日本国内からのアクセスは、2006 年 10 月以降初めて、135/TCP と 445/TCP の順位が逆転した。また、台湾からのアクセスにおいて、8 日及び 25 日から 27 日にかけて、その他のポートが増加しているが、これはいずれも跳ね返りパケット\*を検知したものである。

日本国内からのアクセスについては、「2 - 1 135/TCP 及び 445/TCP に対するアクセス」で詳しく述べている。

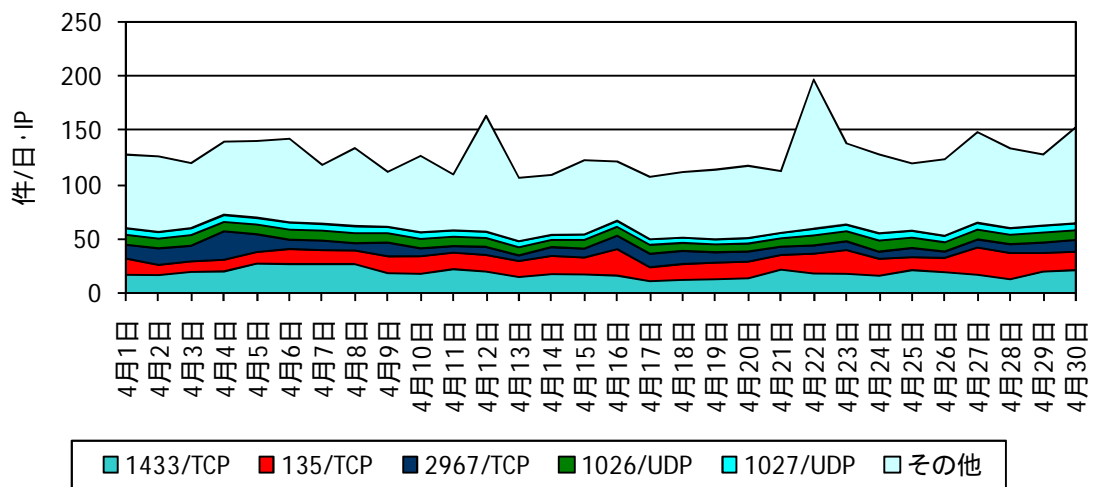


図 3-11 中国からのアクセスの推移

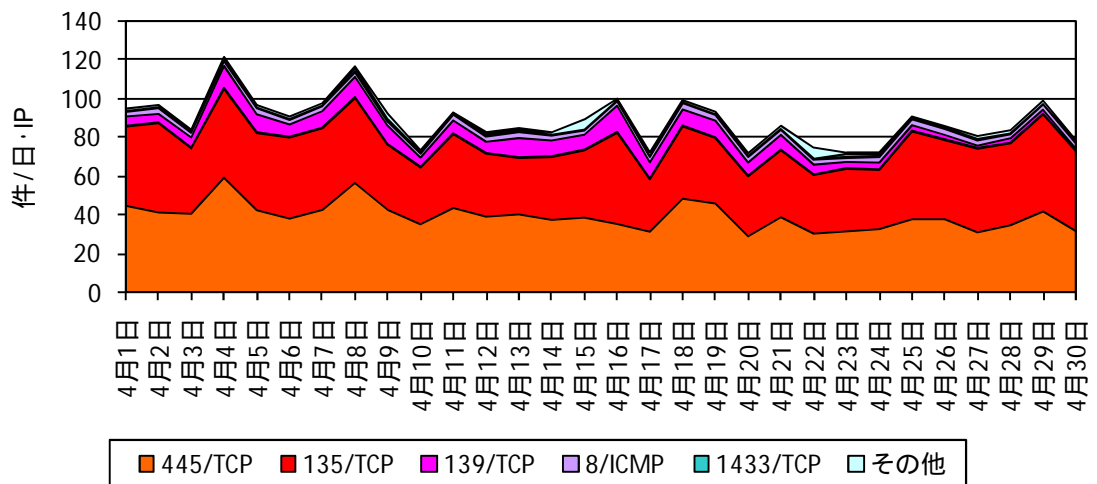


図 3-12 日本からのアクセスの推移

\* 跳ね返りパケットとは、DoS 攻撃の一種である SYN flood 攻撃において、発信元 IP アドレスを無作為に詐称した攻撃パケットに対する応答パケットのこと。

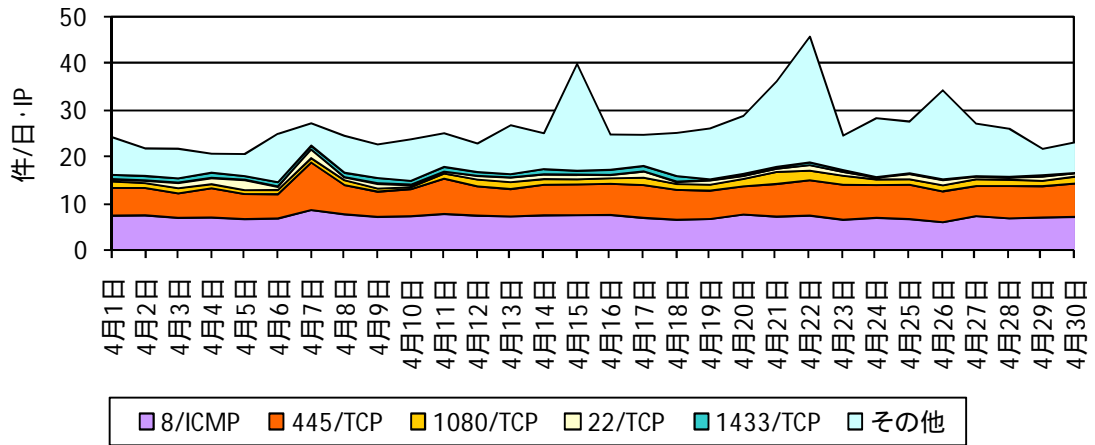


図 3-13 米国からのアクセスの推移

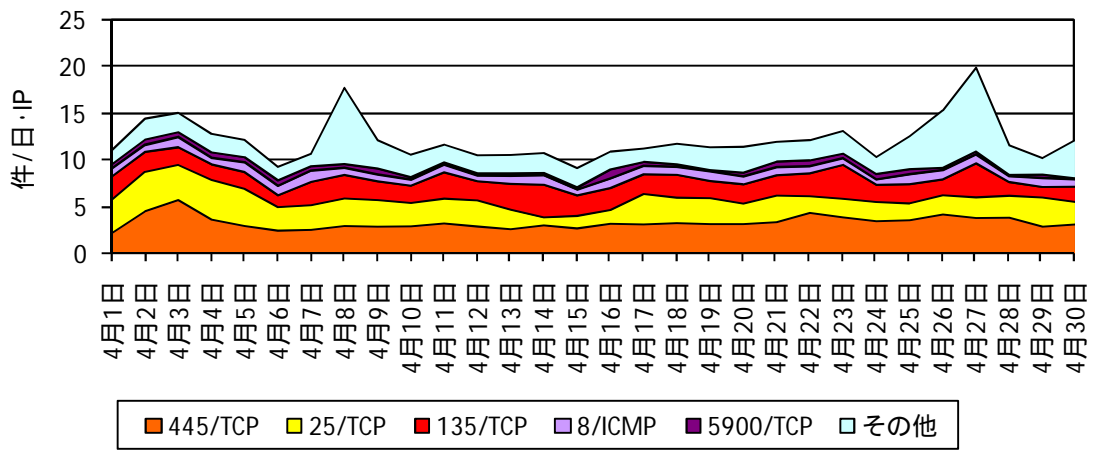


図 3-14 台湾からのアクセスの推移

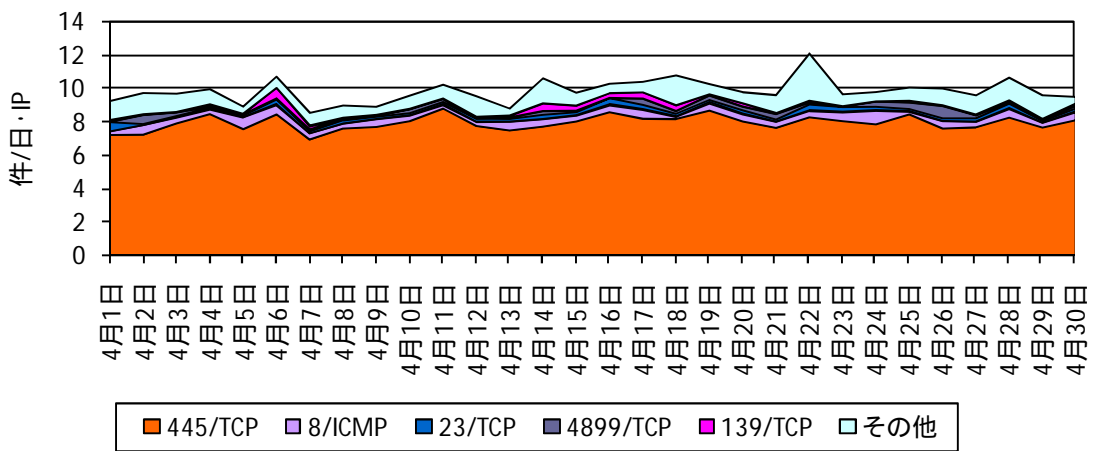


図 3-15 ロシアからのアクセスの推移

## 4 インターネット定点観測 シグネチャを用いた不正侵入等の検知

### 4-1 攻撃手法別

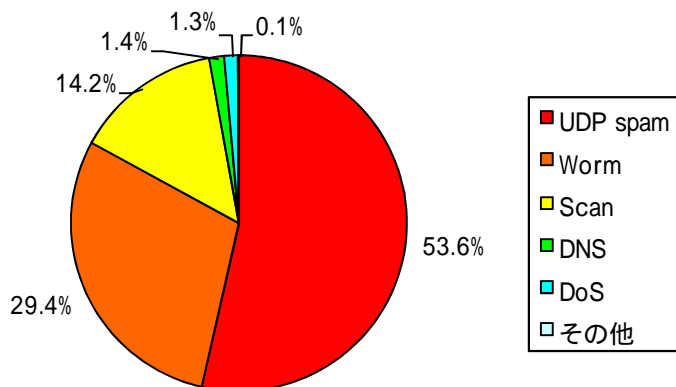


図 4-1 シグネチャを用いた不正侵入等の攻撃手法別検知比率†

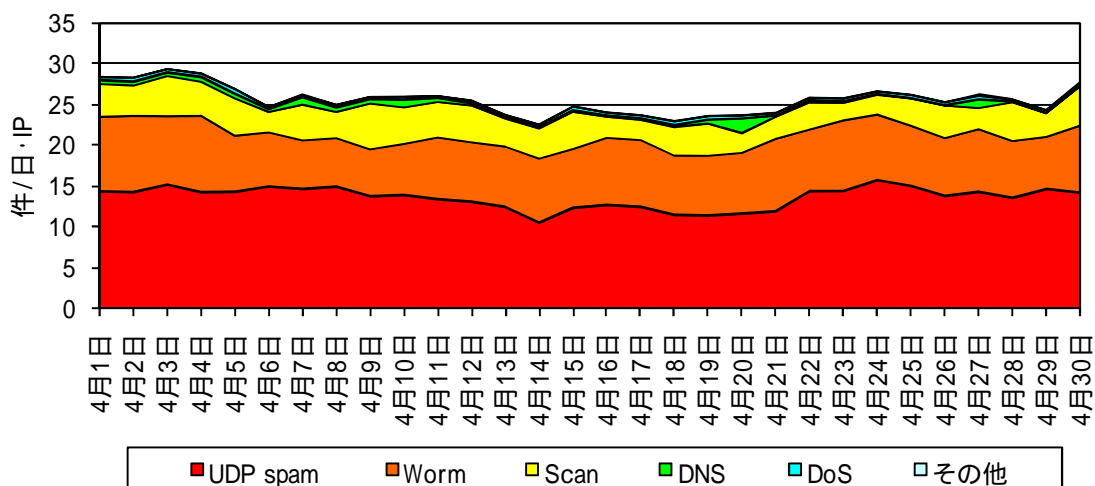


図 4-2 シグネチャを用いた不正侵入等の攻撃手法別検知推移

4月期のシグネチャを用いた不正侵入等の検知件数は、一日・1IP 当たり 25.6 件で、前期と比較して - 3.9 件(- 13.1%)と、やや減少した。

攻撃手法別では、UDP spam、Worm、Scan、DNS 及び DoS の順であった。攻撃手法別の上位 3 位までで、全体の大半を占めている。

UDP spam については、「2-2 UDP spam の検知状況」で詳しく述べている。

† 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。

表 4-1 シグネチャを用いた不正侵入等の攻撃手法別検知件数

今期 順位	前期 順位	攻撃手法	今期 件数	前期比		今期 増加順位	今期 減少順位
1 位	1 位	UDP spam	13.72	+ 7.5%	+ 0.95 件	1 位	
2 位	2 位	Worm	7.52	- 26.7%	- 2.74 件		1 位
3 位	3 位	Scan	3.63	- 32.4%	- 1.74 件		2 位
4 位	4 位	DNS	0.37	- 9.5%	- 0.04 件		5 位
5 位	5 位	DoS	0.34	- 5.1%	- 0.02 件		6 位

#### 4 - 2 発信元国 / 地域別

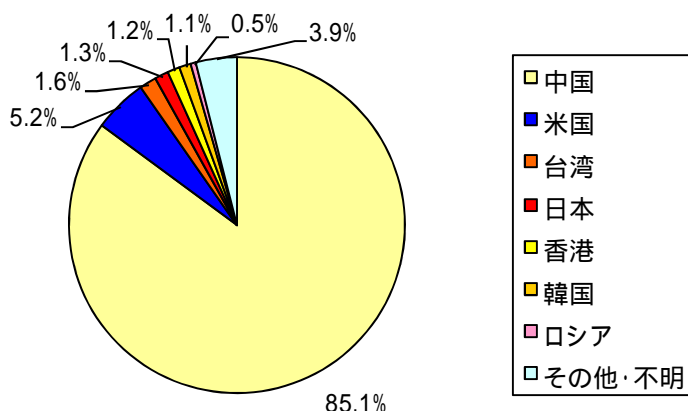


図 4-3 シグネチャを用いた不正侵入等の発信元国 / 地域別検知比率<sup>†</sup>

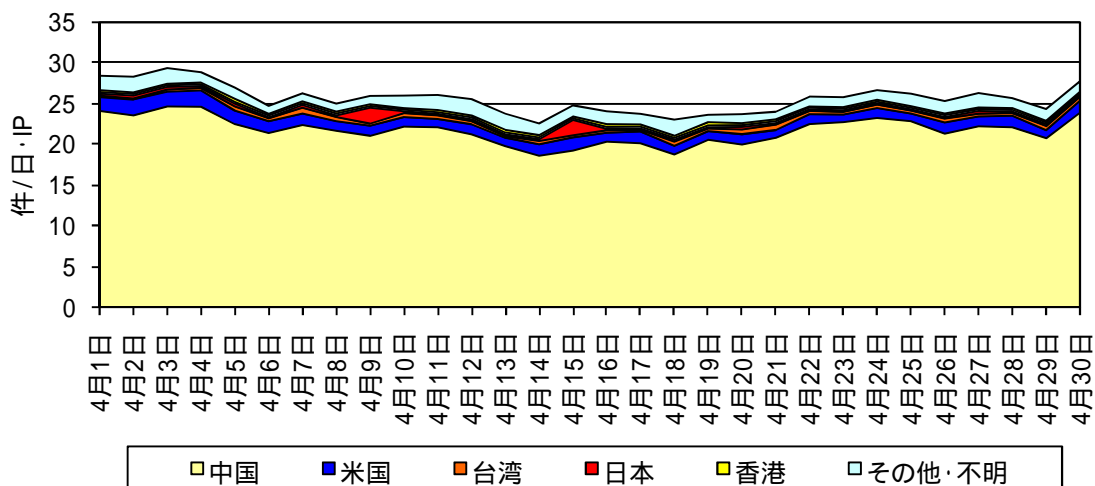


図 4-4 シグネチャを用いた不正侵入等の発信元国 / 地域別検知推移

発信元(国/地域)別の上位5か国までの傾向は、中国、米国、台湾、日本及び香港の順であった。中国を発信元とする攻撃手法別の検知状況は、UDP spam、Worm、Scan がそれぞれ62.9%、24.0%、12.1%を占め、米国を発信元とする攻撃手法別の検知状況は、Worm、Scan がそれぞれ72.0%、13.4%を占めている。

UDP spamについては、「2 - 2 UDP spam の検知状況」で詳しく述べている。



<sup>†</sup> 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。

表 4-2 シグネチャを用いた不正侵入等の発信元国 / 地域別検知件数

今期 順位	前期 順位	国	今期 件数	前期比		今期 増加順位	今期 減少順位
1位	1位	中国	21.80	- 12.9%	- 3.24 件		1位
2位	2位	米国	1.32	- 17.8%	- 0.29 件		2位
3位	4位	台湾	0.42	+ 2.0%	+ 0.01 件		
4位	5位	日本	0.34	+ 16.9%	+ 0.05 件	1位	
5位	6位	香港	0.30	+ 9.7%	+ 0.03 件	3位	

## 5 @police (Topics) 掲載事項

@police において4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4四半期報を追加)(4/28)
●	インターネット治安情勢更新(平成21年3月報を追加)(4/28)
	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 (MS09-009,010,011,012,013,014,015,016)(4/15)
	ジャストシステム社ワープロソフトー太郎の脆弱性について(4/8)

## 6 集計方法

### ・センサーに対するアクセス

TCP 及び UDP はポートごとに集計し、以下ではスラッシュの前にポート番号を付けて表す。(例 135/TCP は TCP の 135 番ポートを表す。) ICMP パケットについては、タイプごとに集計し、以下ではスラッシュの前にタイプ番号を付けて表す。(例 8/ICMP は Icmp Echo Request を表す。)

### ・シグネチャを用いた不正侵入等の検知

各センサーの不正侵入検知装置には、平成 21 年 4 月 30 日現在、シグネチャは 2,885 種類が登録されている。検知された各シグネチャは、表 6-1 に示す分類に従って集計している。

また、シグネチャを用いた不正侵入等の検知を行うセンサーには、サーバ等の攻撃対象となる可能性のある機器を一切接続していない。そのため、UDP を利用している UDP spam や Worm 系の検知が、大きな割合を占めている。

表 6-1 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
Worm	SQL Slammer, Nachi, Dabber
Scan	Sweep of a subnet for active hosts, Proxy port probe, Port scan, TCP ACK ping
UDP spam	MSRPC Popup Message
DoS	Smurf denial of service, ICMP Echo Reply without Echo
DNS	DNS request made for all records, DNS port probe, RR denial of service
Others	Traceroute, ISAKMP Vendor ID, SIP message detected