

平成 21 年 9 月 30 日

## 我が国におけるインターネット治安情勢

(平成 21 年 8 月期)

- ・ マイクロソフト社によるセキュリティ情報の公開後に特定ポートへのアクセス増加  
～ セキュリティ情報に関係するポートに対する攻撃の可能性～
- ・ 445/TCP に対するアクセスが、高い水準で推移  
～ 「Conficker」ワームの流行が継続～

### 1 概説

今期のセンサーに対するアクセス件数は、一日・1IP 当たり 412.0 件で、前期と比較して + 51.9 件 (+ 14.4%)とやや増加した。

8 月 12 日、マイクロソフト社からセキュリティ情報が公開された。その後、セキュリティ情報に関連したポートに対するアクセスの増加を観測した。何者かが攻撃対象を探索していると考えられる。これについて「2 分析 セキュリティ情報の公開とアクセス状況」で述べる。

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。)、2967/TCP 及び 1433/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 142.9 件で、前期と比較して + 11.8 件 (+ 9.0%)と、やや増加している。前期はやや減少となったが、今期は再び増加に転じており、特に日本国内からのアクセスが前期と比較して + 7.5 件 (+ 26.5%)と増加した。445/TCP については、マイクロソフト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」ワームによるアクセスが多くを占めると考えられる。

発信元国・地域別で見ると、中国及びロシアからのアクセスが増加した。それぞれ特定の IP アドレスからの跳ね返りパケットを大量に検知したことが影響している。

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 11.4 件で、前期と比較して + 0.4 件 (+ 3.9%)とほぼ横ばいであった。今期は、シグネチャ分類における、DNS の検知が大幅に増加したが、そのほとんどの検知は、ドイツを発信元とするもので、その原因は DNS 誤設定によるものと考えられる。

## 2 分析 セキュリティ情報の公開とアクセス状況

### 2-1 今期のセキュリティ情報公開後に見られたアクセス増加

平成 21 年 8 月 12 日、マイクロソフト社はセキュリティ情報として、9 件の脆弱性情報と、その修正プログラムを公開した。これらのセキュリティ情報の中で、5 件は使用するポートを公表している。そのうち 3 件のポートに対して、セキュリティ情報の公開後にアクセスの増加が見られた。

このアクセス増加の特徴は、セキュリティ情報公開後に増加するが、数日ですぐに収束するというものである。これは、何者かがセキュリティ情報の公開をきっかけにして、攻撃対象となるホストを探索している可能性が高いと考えられる。

今回のセキュリティ情報公開後、アクセスの増加が見られたポートに対するアクセスの推移は、次のとおりである。

#### ■ 554/TCP (MS09-038<sup>1</sup>)

554/TCP は、RTSP (Real Time Streaming Protocol) と呼ばれる、ネットワーク上で音声や動画をリアルタイムに配信するためのプロトコルで使用されるポートである。

セキュリティ情報の公開前には、554/TCP に対するアクセスを全く検知していないが、公開日以降、散発的にアクセスを検知した(図 2-1)。12 日と 14 日のアクセスは、特定の 1IP アドレスからのものである。

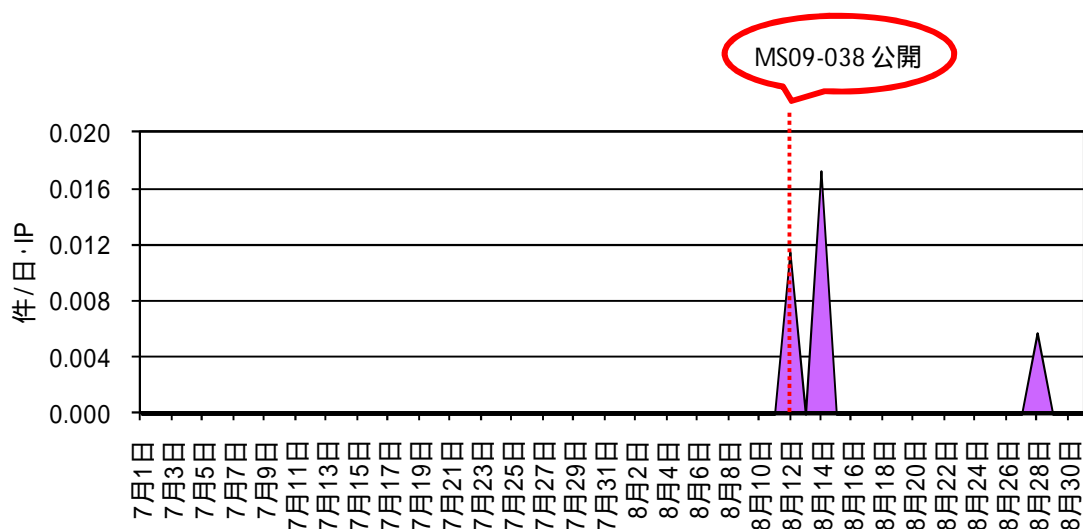


図 2-1 554/TCP に対するアクセス

<sup>1</sup> <http://www.microsoft.com/japan/technet/security/bulletin/MS09-038.msp>

## ■ 42/TCP (MS09-039<sup>1</sup>)

42/TCP は、Windows でコンピュータ名と IP アドレスの対応付けを行う、WINS (Windows Internet Name Service) で使用されるポートである。Windows ユーザは、WINS を利用することで、IP アドレスの代わりにコンピュータ名を使用して、同じネットワーク上にある他の Windows マシンに接続することが可能となる。

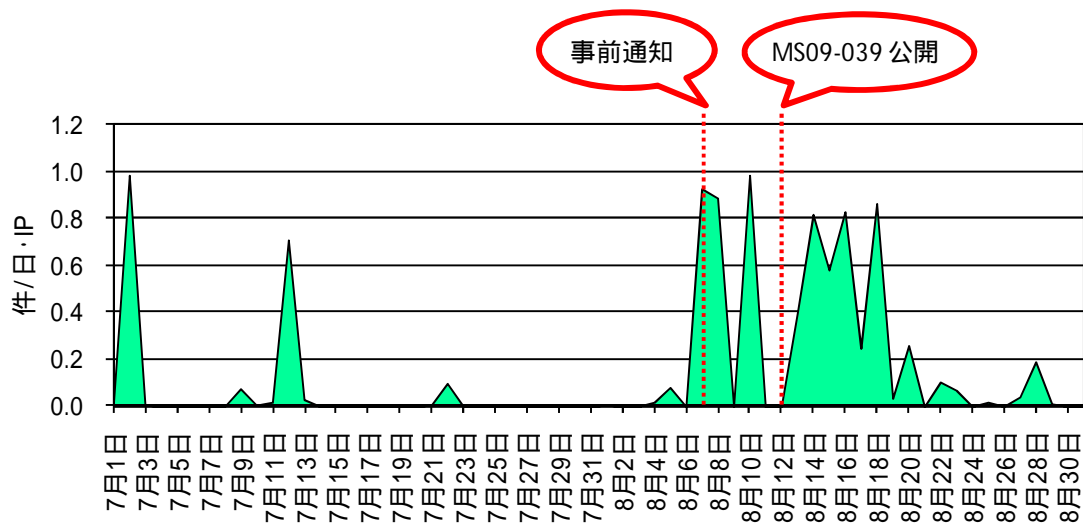


図 2-2 42/TCP に対するアクセス

42/TCP に対するアクセスでは、8月12日のセキュリティ情報公開日以降だけではなく、それ以前に、セキュリティ情報の事前通知後にもアクセスの増加が見られた(図 2-2)。8月7日、8日及び10日のアクセスは、それぞれ発信元 IP アドレスが異なる、特定の IP アドレスからのものである。

7月2日及び12日のように、42/TCP に対しては普段から散発的に 1IP アドレスからのアクセスが観測されている。8月7日以降にも、セキュリティ情報の公開に起因したとみられるアクセスのほか、普段から散発的に観測されるアクセスも含まれていると考えられる。

<sup>1</sup> <http://www.microsoft.com/japan/technet/security/bulletin/MS09-039.msp>

## ■ 23/TCP (MS09-042<sup>1</sup>)

23/TCP は、Telnet で使用されるポートである。Telnet とは、ネットワークに接続されているコンピュータを遠隔で操作するためのサービスである。

セキュリティ情報 (MS09-042) で公開された脆弱性は、「既に悪用コードが存在している『NTLM の資格取得の反映の脆弱性』に類似している」として、マイクロソフト社が注意を促している<sup>2</sup>。

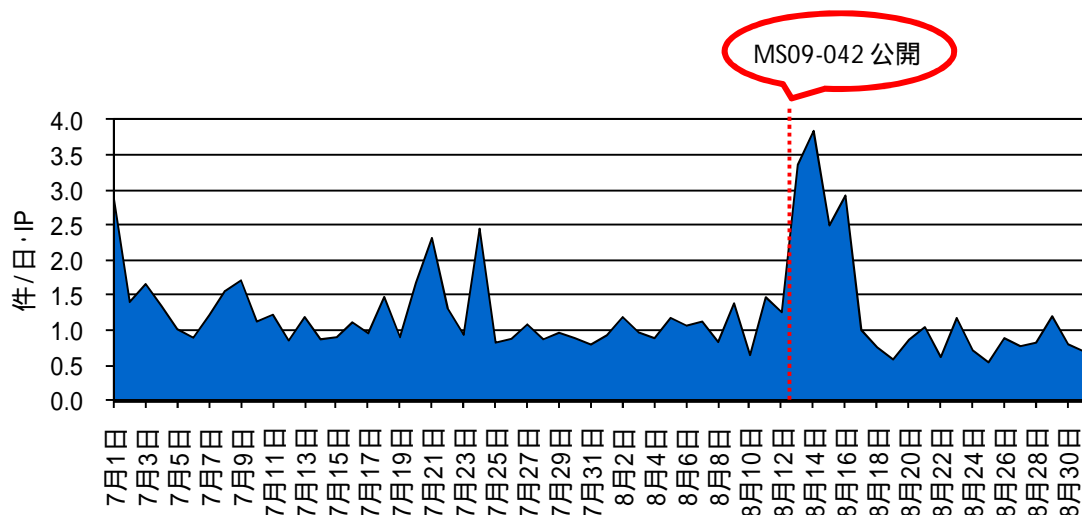


図 2-3 23/TCP に対するアクセス

23/TCP に対しては、常時アクセスがあるが、セキュリティ情報が公開された 8 月 12 日から 17 日にかけて、アクセスの増加が見られた(図 2-3)。これらアクセスの発信元は、特定の IP アドレスからのものではなく、多数の IP アドレスからのアクセスを観測した。ボットネットを利用して、数多くのコンピュータから 23/TCP に対してアクセスを行った可能性が考えられる。

<sup>1</sup> <http://www.microsoft.com/japan/technet/security/bulletin/MS09-042.msp>

<sup>2</sup> 「2009 年 8 月のセキュリティ情報」の「Exploitability Index(悪用可能性指標)」より引用  
<http://www.microsoft.com/japan/technet/security/bulletin/ms09-aug.msp>

## 2-2 過去のセキュリティ情報公開後に見られたアクセス増加

マイクロソフト社は、修正プログラムを伴うセキュリティ情報だけでなく、セキュリティ上の問題や攻撃の回避方法を示した「セキュリティ・アドバイザリ」を公開することがある。2008年12月には、セキュリティ・アドバイザリの公開後に、次のようなアクセスの増加が見られた。

### ■ 1433/TCP(セキュリティ・アドバイザリ 961040<sup>1</sup>)

マイクロソフト社は、2008年12月23日にSQL Serverに関するセキュリティ・アドバイザリを公開した。この公開日から6日間、SQL Serverが使用する1433/TCPに対するアクセスが一時的に増加した(図2-4)。

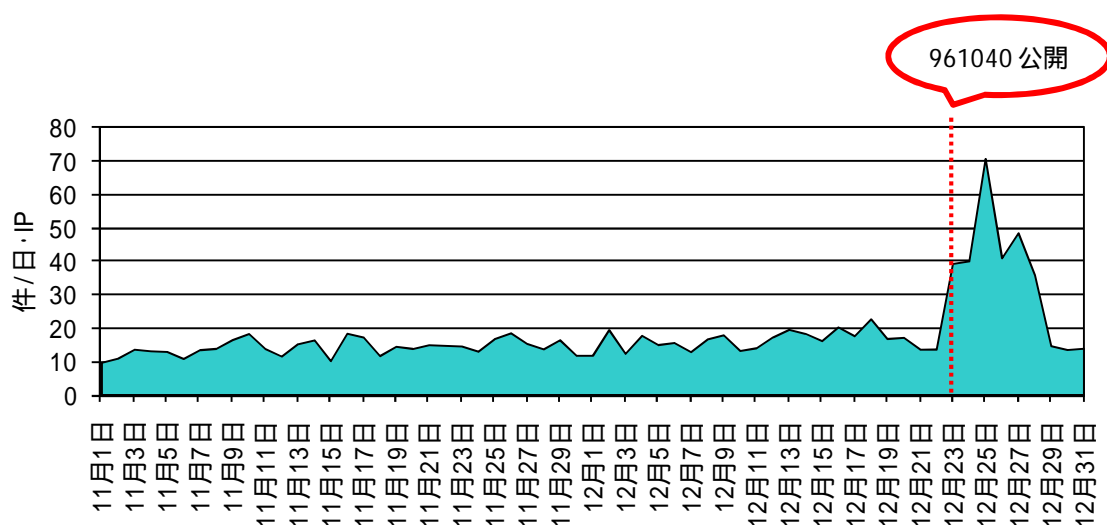


図 2-4 1433/TCP に対するアクセス

セキュリティ・アドバイザリ961040が公開された時点で、既にこの脆弱性の検証コードがインターネット上に公開されているとの情報があり、警察庁でも注意喚起を行った<sup>2</sup>。

12月23日から28日にかけてのアクセス増加は、特定の1IPアドレスから広範囲のIPアドレスに対してアクセスが行われていた。何者かが、セキュリティ・アドバイザリ961040で公開された脆弱性を持つ攻撃対象を探索していたものと考えられる。

<sup>1</sup> <http://www.microsoft.com/japan/technet/security/advisory/961040.mspx>

<sup>2</sup> 「SQL Server の脆弱性について」

[http://www.cyberpolice.go.jp/important/2008/20081223\\_125244.html](http://www.cyberpolice.go.jp/important/2008/20081223_125244.html)

### 2-3 攻撃者が探索した範囲の推測

これまでに述べた、セキュリティ情報の公開に起因したとみられるアクセスの増加について、アクセス増加を観測したセンサーの IP アドレスから、攻撃者が探索した範囲を推測する。

554/TCP に対するアクセスは、数か所のセンサーで観測した。観測したセンサー同士の IP アドレスは、互いに離れており、ランダムな探索が行われた可能性がある。

42/TCP、23/TCP 及び 1433/TCP に対するアクセスは、ほぼすべてのセンサーに対してアクセスがあった。広い IP アドレス範囲にわたって探索行為が行われたと考えられる。

表 2-1 探索範囲

セキュリティ情報	宛先ポート	アクセスを観測したセンサー	推測される探索範囲
MS09-038	554/TCP	数か所	ランダムな IP アドレス
MS09-039	42/TCP	すべて	広範囲の IP アドレスを網羅
MS09-042	23/TCP	すべて	広範囲の IP アドレスを網羅
961040	1433/TCP	ほぼすべて	広範囲の IP アドレスを網羅

554/TCP に対するアクセスを除いて、探索範囲は広範囲の IP アドレスを網羅していると推測される。554/TCP に対するアクセスについても、アクセス数が少ないため、結果的にランダムな IP アドレスを探索したように見えただけの可能性も否定できない。

セキュリティ情報の公開に起因したとみられる探索行為は、インターネット上の IP アドレスを網羅する形で、広範囲に探索されたと考えられる。

## 2-4 まとめ

本章で取り上げたアクセスには、次のような特徴があった。

表 2-2 アクセスの特徴

- セキュリティ情報の公開後にアクセスが増加
- アクセスの増加は数日間
- 探索範囲は広範囲の IP アドレスを網羅

これらのことから、何者かがセキュリティ情報の公開後に攻撃対象を広範囲に探索している可能性が高い。セキュリティ情報の公開直後は、修正プログラムの適用が進んでおらず、脆弱性を突く攻撃への対策が取られていない機器が多いと考えられる。このような機器は、攻撃者にとっては格好の標的となり、大規模な攻撃に繋がることも考えられる。

セキュリティ情報により公開された脆弱性に対しては、何者かが意図的に探索を行っていると思われるアクセスがあることを確認した。これは、セキュリティ情報の公開直後であっても、公開された脆弱性を突く攻撃が行われる可能性があることを示している。

このため、常に最新のセキュリティ情報に目を向け、セキュリティ情報が公開された時には、素早く修正プログラムを適用するなどの対策を行う必要がある。

### 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、依然として上位を占めている。上位 3 位までの順位は、平成 21 年 3 月以降変動がない。445/TCP 及び 8/ICMP は、前期と比較してやや増加となった。8/ICMP は、7 月 30 日以降、特定の IP アドレスからの定期的なアクセスを大量に検知している。135/TCP は横ばいであった。

今期増加 5 位の 17566/TCP は、8 月 19 日及び 20 日に大量のアクセスを検知した。国別では、ポーランドからのアクセスが 60%を占め、ヨーロッパの国々からのアクセスが上位を占めた。また、前期において一時的に増加した 62400/TCP に対するアクセスは、今期はほとんど見られなかった。このような 10000 以上のポートに対する一時的なアクセスの増加はしばしば観測される。一部に P2P ソフトウェアに関連するものが見られるが、その目的が判明しないものも多い。

表 3-1 宛先ポート別検知件数

今期 順位	前期 順位	ポート	今期 件数	前期比	増加順位	減少順位
1 位	1 位	445/TCP	142.92 件	+ 9.0% (+ 11.83 件)	2 位	
2 位	2 位	135/TCP	56.09 件	- 2.1% (- 1.19 件)		3 位
3 位	3 位	8/ICMP	36.77 件	+ 19.8% (+ 6.08 件)	3 位	
4 位	6 位	2967/TCP	23.40 件	+ 131.9% (+ 13.31 件)	1 位	
5 位	4 位	1433/TCP	22.73 件	- 15.3% (- 4.11 件)		2 位
...			...			
7 位	5 位	4899/TCP	5.74 件	- 45.2% (- 4.74 件)		1 位
...			...			
11 位	13 位	1521/TCP	2.61 件	+ 28.5% (+ 0.58 件)	4 位	
...			...			
18 位	16 位	8088/TCP	1.05 件	- 23.6% (- 0.32 件)		5 位
...			...			
26 位	-	17566/TCP	0.46 件	- <sup>1</sup> (+ 0.46 件)	5 位	
...			...			
-	27 位	62400/TCP	ごく僅か	- 99.8% (- 0.58 件)		4 位

<sup>1</sup> 前期の検知件数が少なかった(0.002 件)ため、前期比率は記載していない。

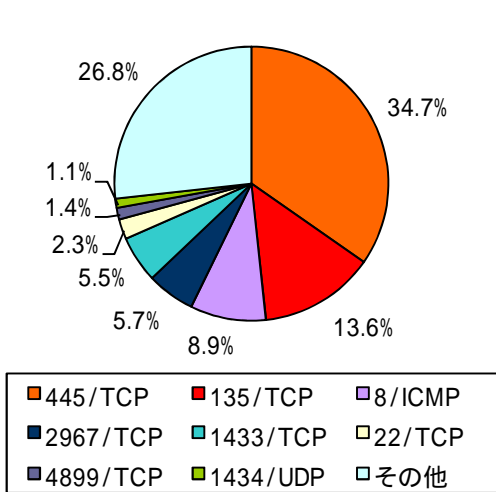


図 3-1 世界の宛先ポート比率<sup>1</sup>

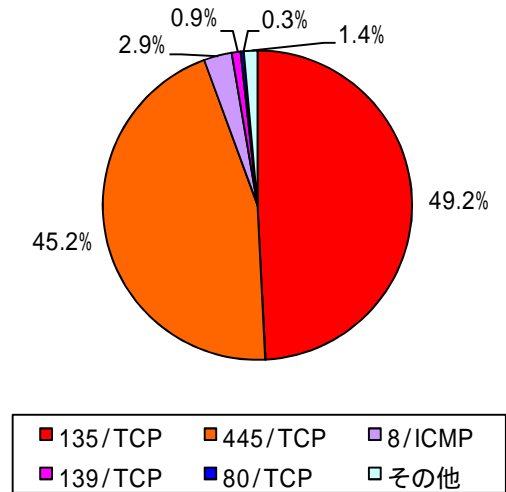


図 3-2 日本の宛先ポート比率<sup>1</sup>

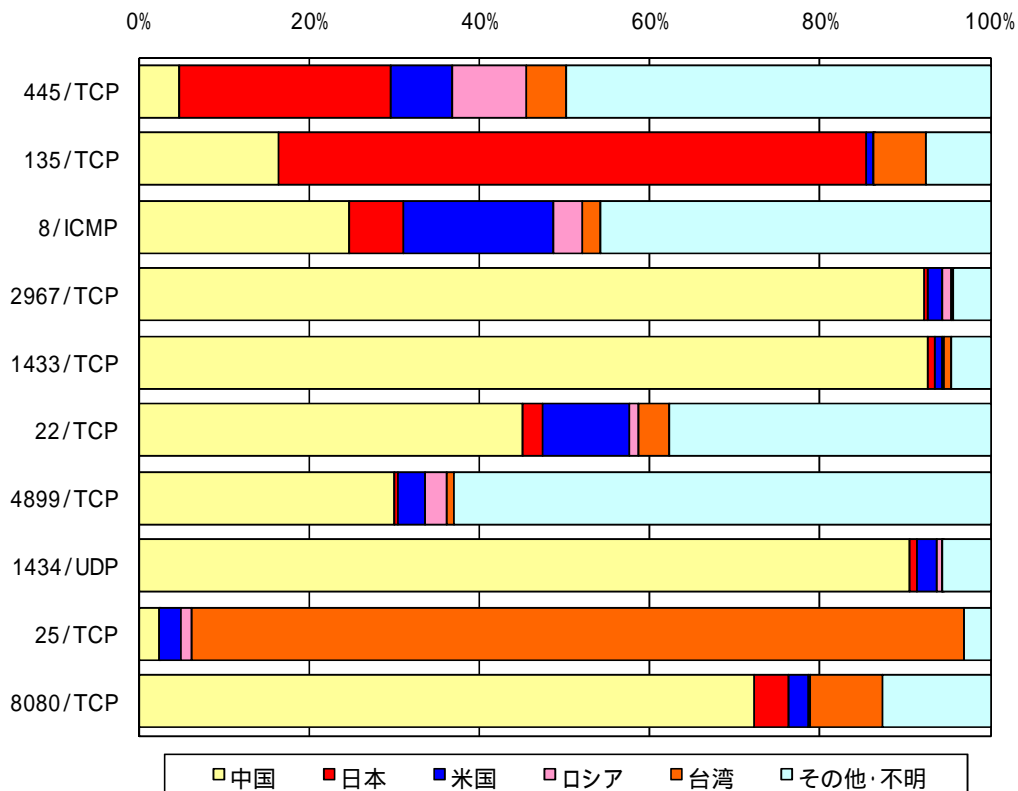


図 3-3 宛先ポートの国・地域別比率

<sup>1</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

今期 1 位の 445/TCP は、前期と比較してやや増加しており、「Conficker」ワームの流行が継続しているものと考えられる。

今期 3 位の 8/ICMP は、前期と比較してやや増加となった。7 月 30 日以降、中国を発信元とする特定の 1IP アドレスからの定期的なアクセスを大量に検知しており、何者かがスキャン活動を継続している可能性がある。

2967/TCP は、前期と比較して大幅に増加し、今期 4 位となった。8 月下旬におけるアクセスの増加は、中国を発信元とする特定の IP アドレスからのアクセスによるものである。2967/TCP に対するアクセスのほとんどが発信元ポート 6000 であり、スキャン活動を行うツールの存在がうかがえる。

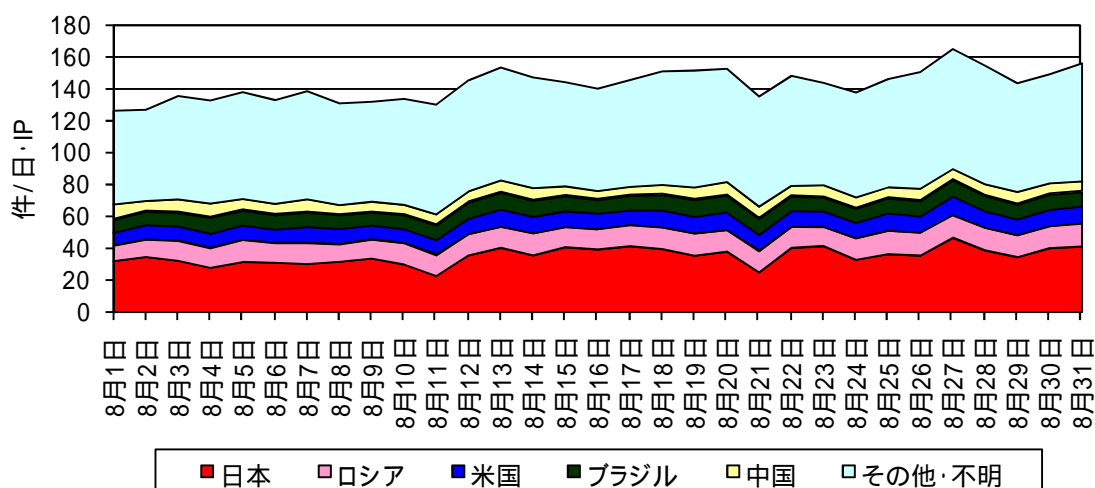


図 3-4 宛先ポート 445/TCP に対するアクセスの推移

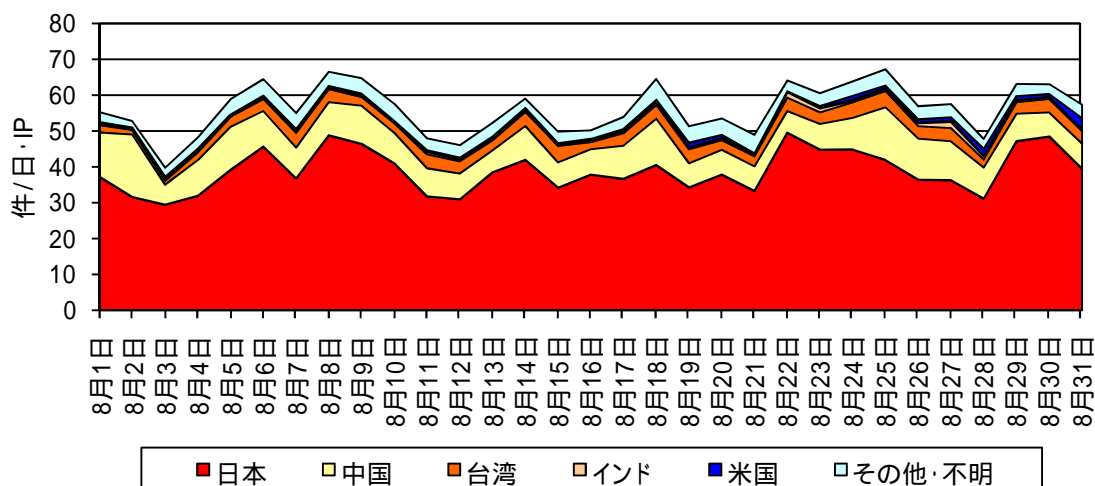


図 3-5 宛先ポート 135/TCP に対するアクセスの推移

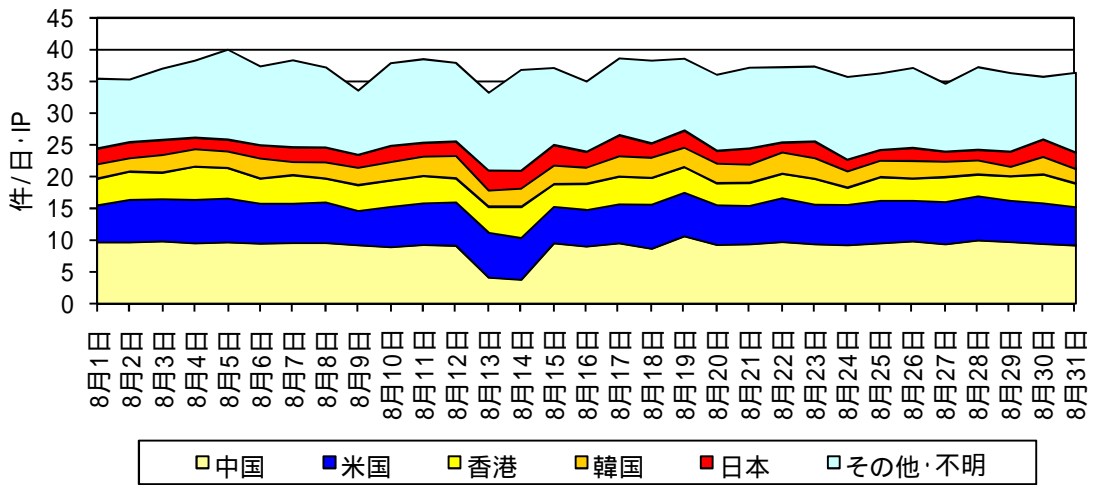


図 3-6 8/ICMP のアクセスの推移

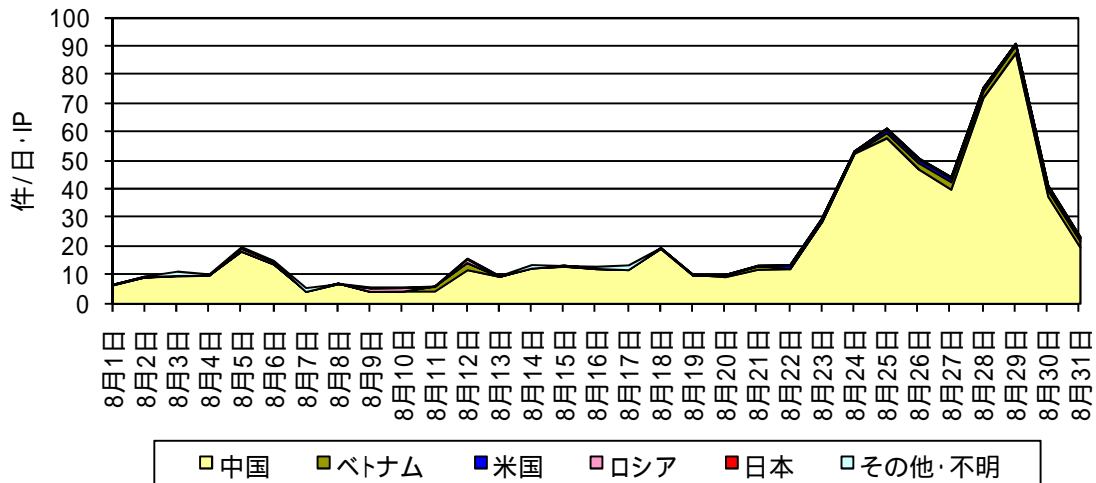


図 3-7 宛先ポート 2967/TCP に対するアクセスの推移

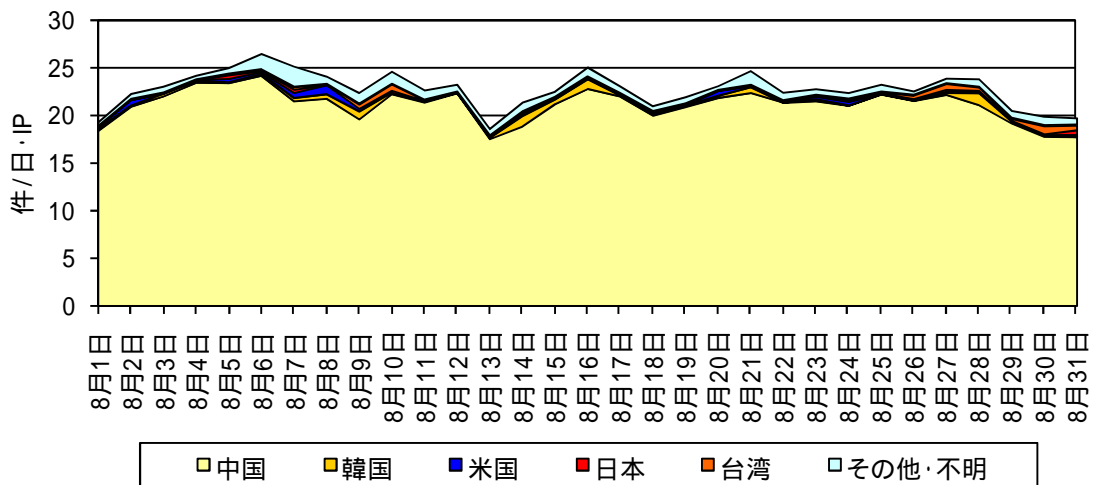


図 3-8 宛先ポート 1433/TCP に対するアクセスの推移

### 3-2 発信元国・地域別

#### (1) 概要

上位 5 位までの国・地域別の順位に変動はない。中国、ロシアからのアクセスの増加が目立ち、それぞれ今期増加順位 1 位、2 位となった。これらは、8 月上旬に中国、8 月中旬にロシアを発信元とする、それぞれ特定の IP アドレスからの跳ね返りパケットを大量に検知したことが主な原因となっている。また、8 月 23 日に、米国を発信元とする特定の IP アドレスからの跳ね返りパケットを大量に検知しており、今期は跳ね返りパケットの増加が目立った。

445/TCP に対するアクセスは、日本からのアクセスは増加、米国、ロシア及び台湾からのアクセスはやや増加となった。各国において「Conficker」ワームの流行が継続しているものと考えられる。「Conficker」ワームは、ネットワーク経由のほか、リムーバブルディスク経由で感染を拡大させることも可能であり、感染力の強さをうかがうことができる。

表 3-2 発信元国・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	増加順位	減少順位
1 位	1 位	中国	155.71 件	+ 35.8% (+ 41.05 件)	1 位	
2 位	2 位	日本	78.76 件	+ 6.5% (+ 4.82 件)	3 位	
3 位	3 位	米国	25.36 件	+ 5.7% (+ 1.37 件)	5 位	
4 位	4 位	ロシア	19.55 件	+ 33.5% (+ 4.91 件)	2 位	
5 位	5 位	台湾	15.55 件	+ 16.4% (+ 2.19 件)	4 位	
...			...			
7 位	6 位	韓国	8.72 件	- 24.3% (- 2.80 件)		1 位
...			...			
12 位	10 位	香港	5.09 件	- 9.2% (- 0.52 件)		5 位
...			...			
18 位	14 位	英国	2.63 件	- 31.8% (- 1.23 件)		2 位
...			...			
29 位	24 位	チリ	1.37 件	- 28.0% (- 0.53 件)		4 位
...			...			
36 位	26 位	ベネズエラ	0.99 件	- 36.4% (- 0.57 件)		3 位

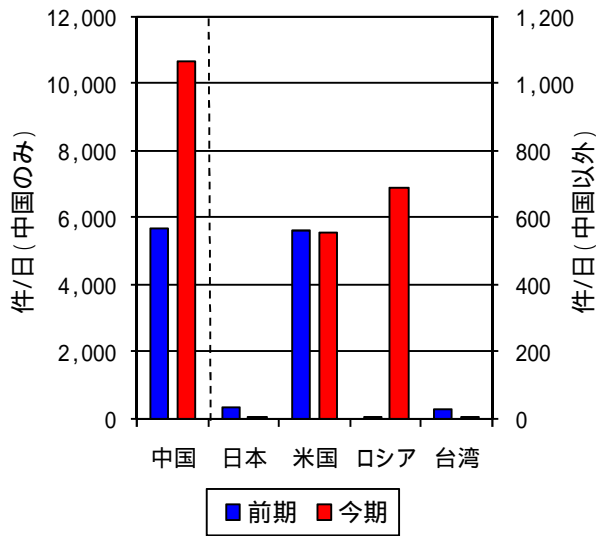


図 3-9 発信元国・地域別 跳ね返りパケット件数

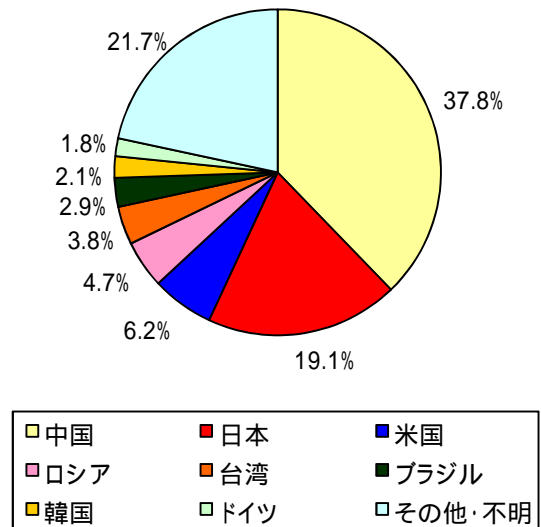


図 3-10 発信元国・地域別比率<sup>1</sup>

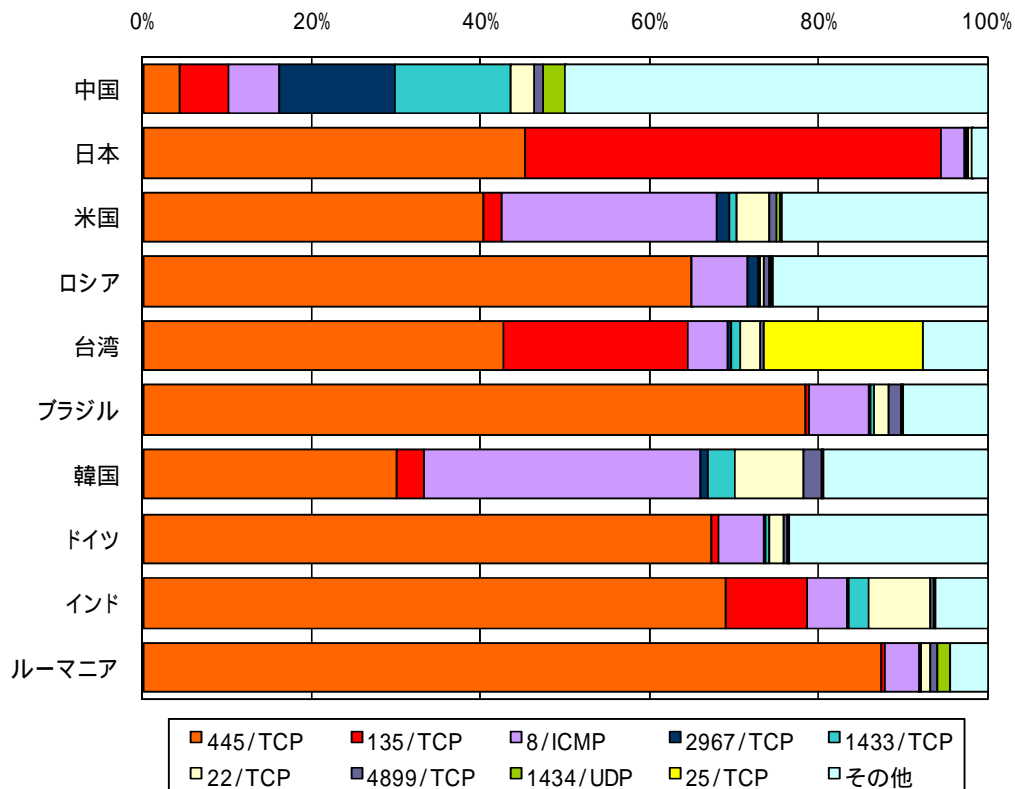


図 3-11 発信元国・地域別上位のポート別比率

<sup>1</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、前期と比較して増加となった。8月上旬にその他のポートが増加しているが、これは特定の IP アドレスからの跳ね返りパケットを検知したものである。中国は、今期に限らず、他の国・地域と比較して跳ね返りパケットの比率が高い。また、8月下旬の 2967/TCP の増加は、特定の IP アドレスからのアクセスによるものである。

日本からの 445/TCP に対するアクセスは、前期は減少となったが、今期は前期比 + 7.5 件 (+ 26.5%) と増加に転じた。日本においては、6 月下旬から 7 月にかけて減少が見られ、一時的に「Conficker」ワームの感染拡大が沈静化した。8 月に入り、再び拡大傾向にあると考えられる。

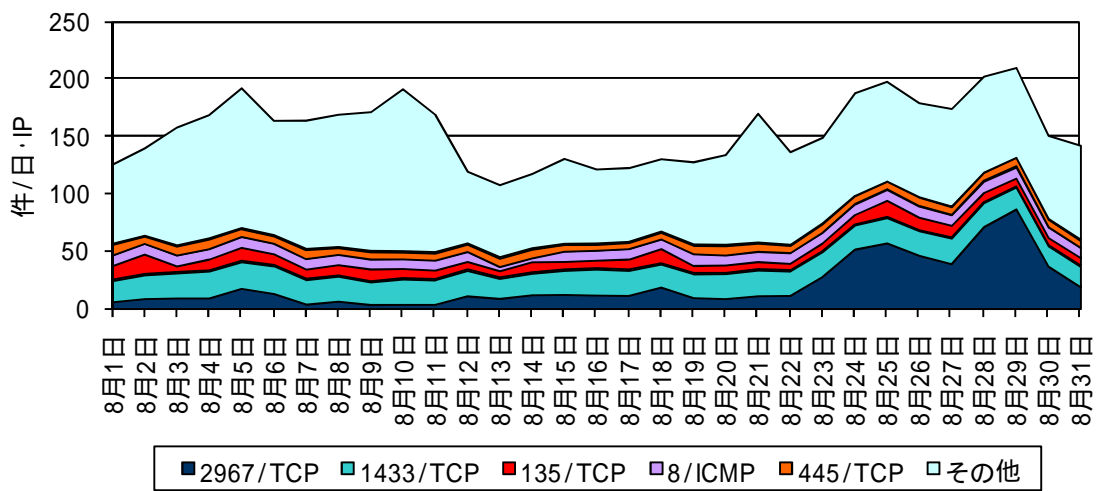


図 3-12 中国からのアクセスの推移

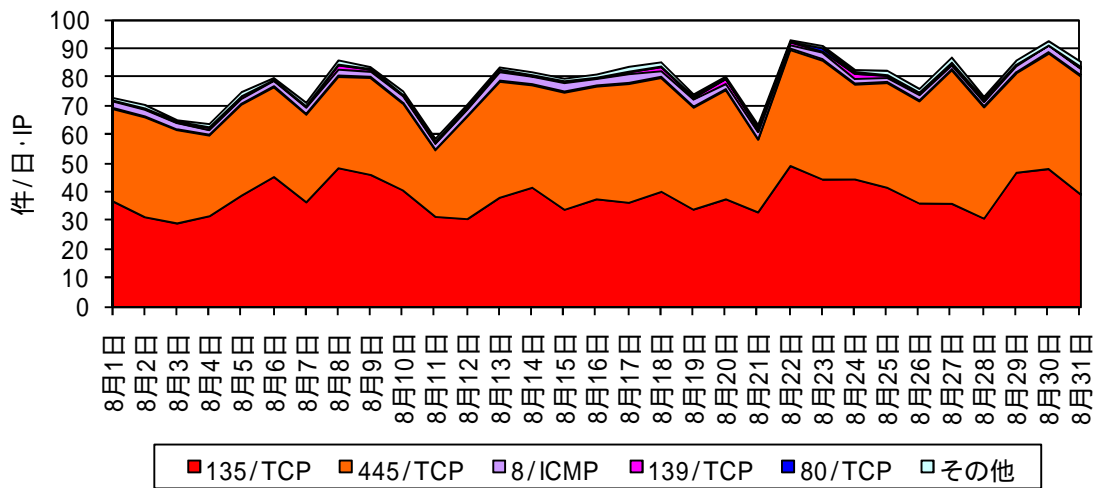


図 3-13 日本からのアクセスの推移

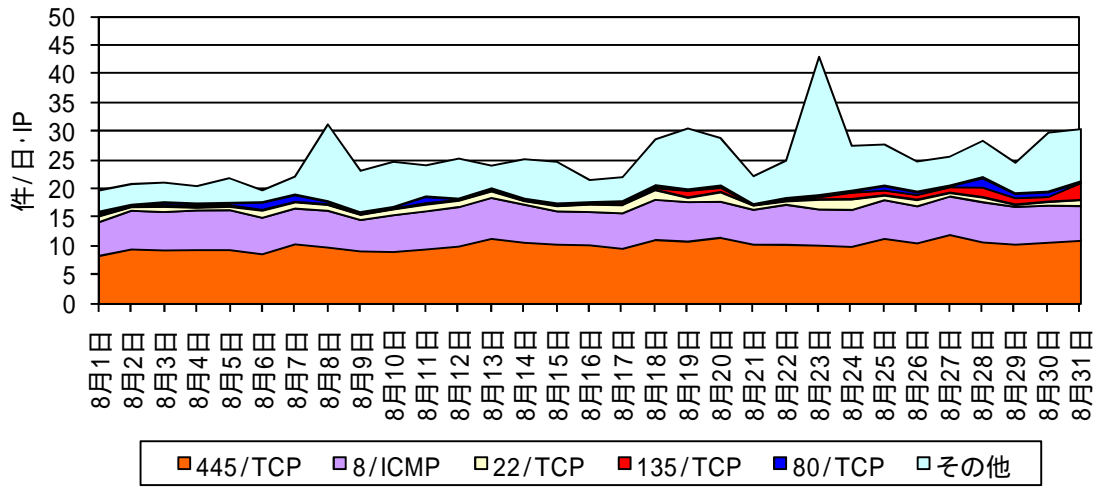


図 3-14 米国からのアクセスの推移

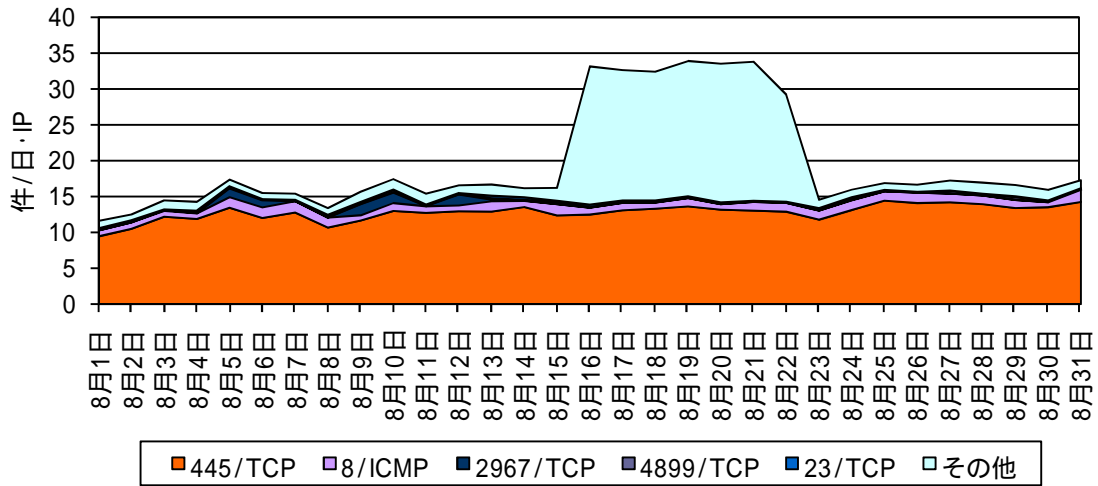


図 3-15 ロシアからのアクセスの推移

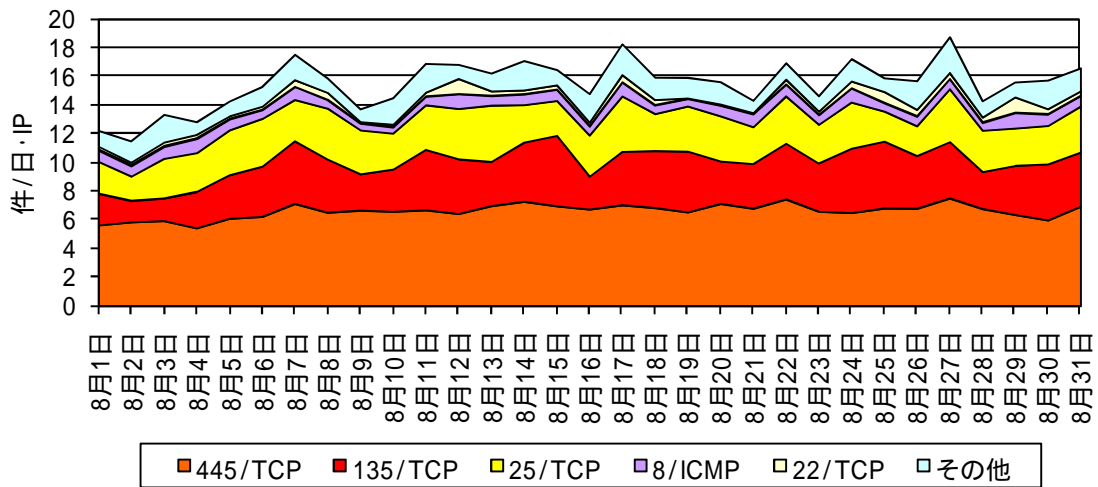


図 3-16 台湾からのアクセスの推移

## 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

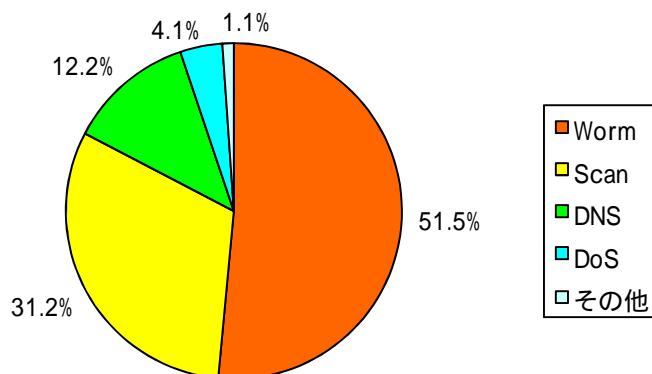


図 4-1 シグネチャを用いた不正侵入等の攻撃手法別検知比率<sup>1</sup>

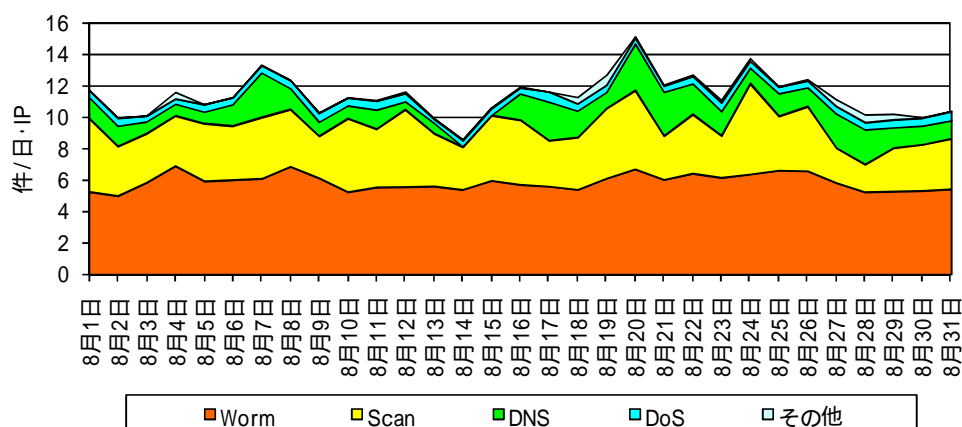


図 4-2 シグネチャを用いた不正侵入等の攻撃手法別検知推移

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 11.4 件で、前期と比較して +0.4 件 (+3.9%)とやや増加した。攻撃手法別では、Worm 及び Scan で、全体の 8 割を超えている。

また、今期は DNS の検知件数が一日・1IP 当たり 1.39 件であり、前期と比較して +1.13 件 (+436.1%)と大幅に増加した。これは特定の IP アドレスを発信元としており、DNS の誤設定が原因と考えられる。この特定の IP アドレスを発信元とするものを除いた DNS の検知件数は一日・1IP 当たり 0.15 件で、前期と比較して -0.07 件 (-31.8%)と減少した。なお、この特定の IP アドレスを発信元とした通信は 7 月 31 日から継続して検知している。

<sup>1</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 4-1 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	Worm	5.86件	- 5.3% (- 0.33件)		2位
2位	2位	Scan	3.55件	- 11.0% (- 0.44件)		1位
3位	4位	DNS	1.39件	+ 436.1% (+ 1.13件)	1位	
4位	3位	DoS	0.46件	+ 29.6% (+ 0.11件)	2位	

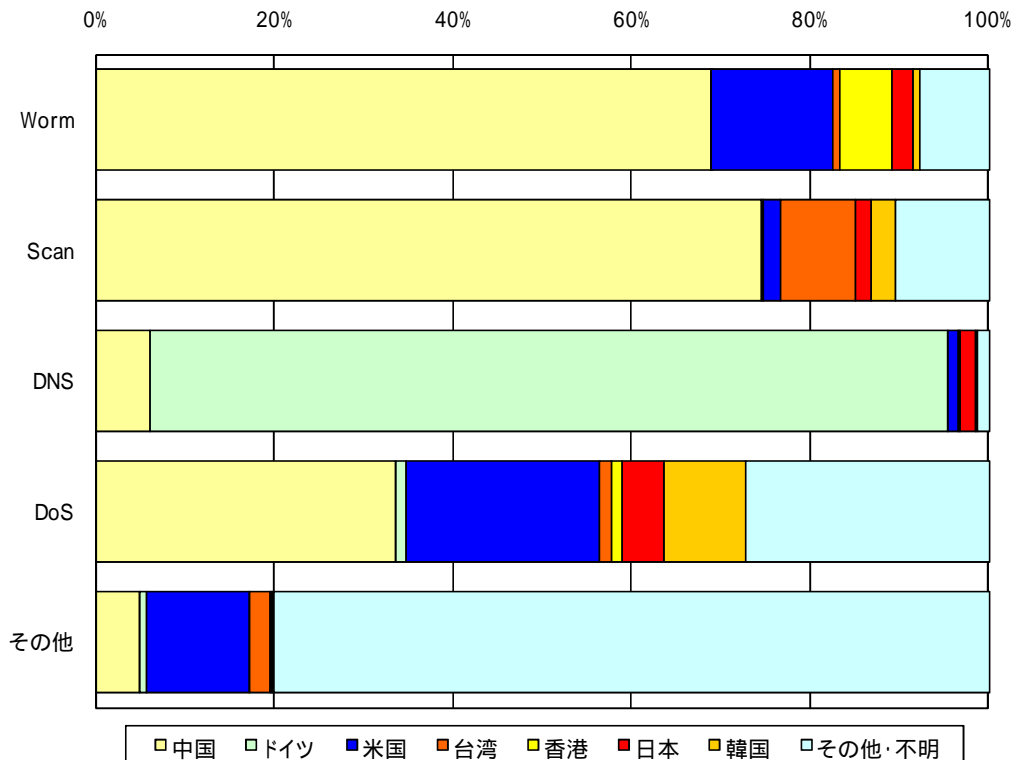


図 4-3 シグネチャを用いた不正侵入等の攻撃手法の国・地域別比率

#### 4-2 発信元国・地域別

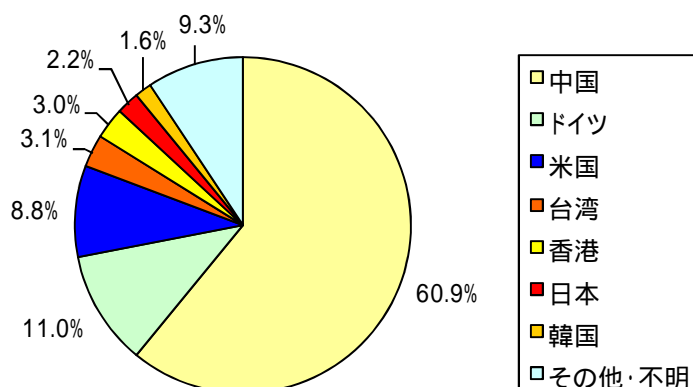


図 4-4 シグネチャを用いた不正侵入等の発信元国・地域別検知比率<sup>1</sup>

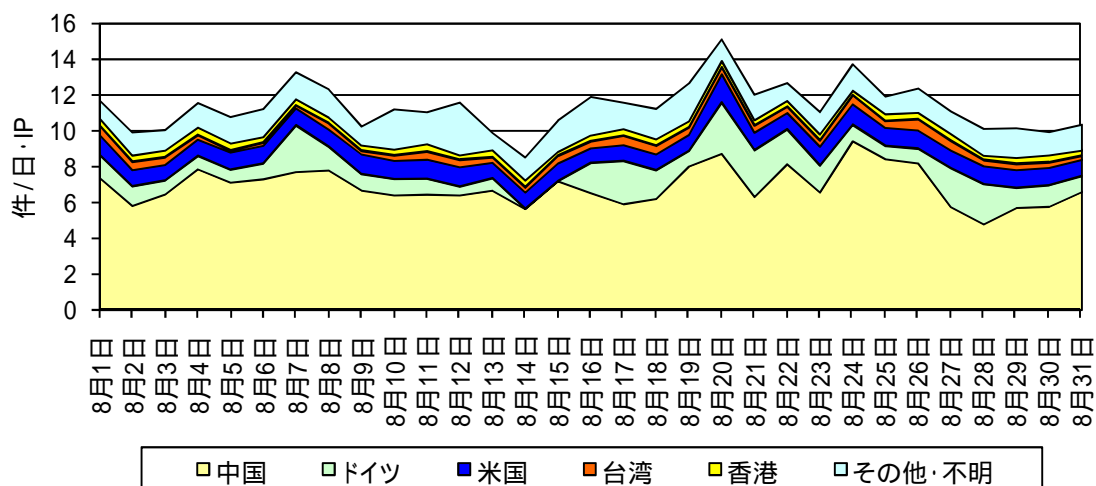


図 4-5 シグネチャを用いた不正侵入等の発信元国・地域別検知推移

今期は、ドイツを発信元とする検知件数が大幅に増加している。ドイツを発信元とするほとんどの検知は、DNS の誤設定が原因と考えられる。DNS 誤設定が原因と考えられる検知を除くと、ドイツを発信元とする検知件数は、一日・1IP 当たり 0.02 件とごく僅かであった。

<sup>1</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・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	6.93件	- 7.3% (- 0.55件)		1位
2位	8位	ドイツ	1.25件	+ 596.2% (+ 1.07件)	1位	
3位	2位	米国	1.00件	- 5.6% (- 0.06件)		3位
4位	3位	台湾	0.36件	- 2.5% (- 0.01件)		
5位	4位	香港	0.34件	- 4.4% (- 0.02件)		
...			...			
8位	9位	スウェーデン	0.12件	- 29.0% (- 0.05件)		5位
9位	7位	カナダ	0.10件	- 42.8% (- 0.08件)		2位
10位	12位	ルーマニア	0.09件	+ 88.6% (+ 0.04件)	3位	
11位	13位	英国	0.08件	+ 106.0% (+ 0.04件)	4位	
12位	27位	オランダ	0.07件	+ 591.2% (+ 0.06件)	2位	
...			...			
16位	43位	チリ	0.04件	+ 603.7% (+ 0.03件)	5位	
...			...			
31位	11位	メキシコ	0.01件	- 87.0% (- 0.06件)		4位

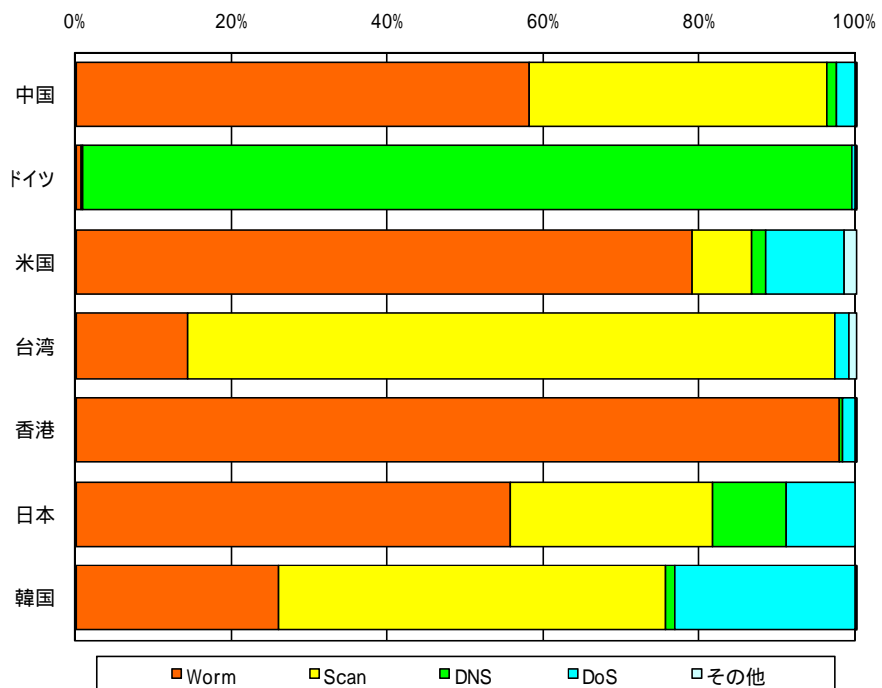


図 4-6 シグネチャを用いた不正侵入等の発信元国・地域別上位のシグネチャ別比率

## 5 @police (Topics)掲載事項

@police において 8 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 21 年 7 月報を追加)(8/31)
●	IOCE Annual Conference 2009 の開催について(8/26)
<b>重要</b>	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 (MS09-028,029,030,031,032,033)(8/20) 更新
<b>重要</b>	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 (MS09-036,037,038,039,040,041,042,043,044)(8/12)
●	インターネット治安情勢更新(平成 21 年上半期報を追加)(8/6)
<b>重要</b>	アドビシステムズ社の Adobe Flash Player、Adobe Reader および Acrobat のセキュリティ修正プログラムについて(8/1)

## 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 8 月 31 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、セッションの確立を必要としない、UDP を利用する Worm や Scan 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