

平成 21 年 12 月 14 日

我が国におけるインターネット治安情勢

(平成 21 年 10 月期)

- ・445/TCP に対するアクセスが長期にわたって継続
～ Conficker ワームの感染拡大の可能性
- ・1024/TCP、3072/TCP を使用する SYN Flood 攻撃が継続
～ 米国内のサーバへの攻撃を検知
～ 攻撃用ツールは平成 12 年頃から出まわる

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 379.3 件で、前期と比較して - 41.3 件 (- 9.8%)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 22/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 177.6 件で、前期と比較して + 11.9 件 (+ 7.2%)と、前期に引き続きやや増加となった。445/TCP は、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 ワームによるアクセスが主な原因と考えられ、感染拡大が依然として継続していると推測される。

また、今期は 1024/TCP と 3072/TCP を宛先ポートとする跳ね返りパケットが増加した。複数の IP アドレスからパケットを検知しており、複数のサーバに対して、ツールを使用した SYN flood 攻撃が行われたものと考えられる。これについては、「2 分析 1024/TCP と 3072/TCP を使用する SYN flood 攻撃」で述べる。

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

今期の中国からのアクセスは、一日・1IP 当たり 89.9 件と、前期と比較して - 56.5 件 (- 38.6%)と減少した。何者かが行っていた 2967/TCP へのスキャン活動が停止したものと考えられる。また 8/ICMP への定期的なアクセスは一時的に停止していたが、10 月 27 日から再度アクセスが行われている。

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 10.9 件で、前期と比較して - 0.9 件 (- 7.7%)とやや減少している。

2 分析 1024/TCP と 3072/TCP を使用する SYN flood 攻撃

今期は、複数の発信元 IP アドレスからの、1024/TCP と 3072/TCP を宛先ポートとする跳ね返りパケットが増加した。複数のサーバに対して、攻撃パケットの発信元ポートを 1024/TCP と 3072/TCP とするツールを使用した SYN flood 攻撃が行われたと考えられる。

サイバーフォースセンターでは、以前から、今期と同様に 1024/TCP と 3072/TCP を宛先ポートとする跳ね返りパケットを検知しており、このツールによる攻撃が、継続的に行われているとみられる。

2-1 SYN flood 攻撃と跳ね返りパケットの検知

SYN flood 攻撃は、DoS 攻撃の一種である。SYN flood 攻撃では、標的となるサーバ(被害サーバ)の機能を停止させるために、大量の SYN パケットを送信する。この際、攻撃者の判別を困難にするために、発信元 IP アドレスを詐称することが多い。詐称された IP アドレスが、センサーの IP アドレスに一致した場合、被害サーバから来る SYN/ACK パケットや RST/ACK パケットを、センサーでは跳ね返りパケットとして検知する。

このため、跳ね返りパケットの宛先ポートは攻撃パケットの発信元ポート(ツールが使用するポート)となり、跳ね返りパケットの発信元 IP アドレスは、被害サーバの IP アドレスとなる。(図 2-1)

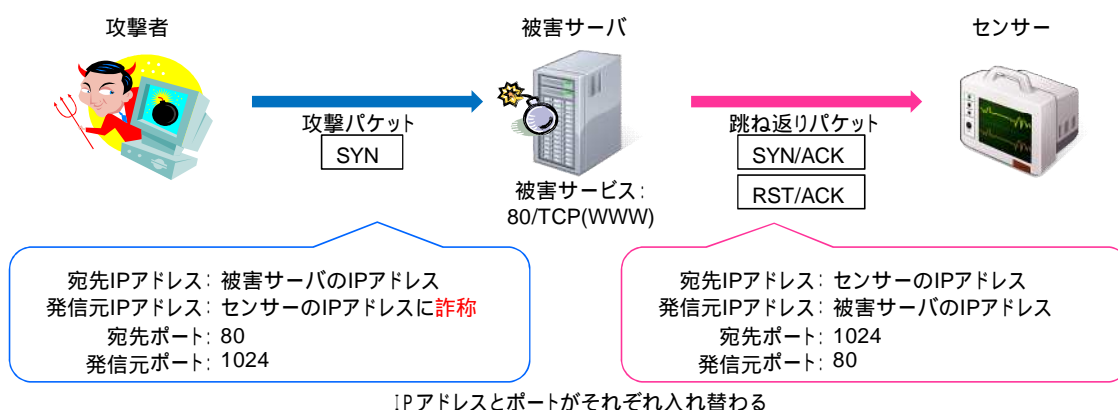


図 2-1 SYN flood 攻撃と跳ね返りパケット

2-2 1024/TCP と 3072/TCP の検知状況

今期は、複数の IP アドレスからの 1024/TCP と 3072/TCP を宛先ポートとする跳ね返りパケットが目立った。この跳ね返りパケットは、1024/TCP と 3072/TCP の検知件数が、ほぼ同数であることが特徴である。(図 2-2)

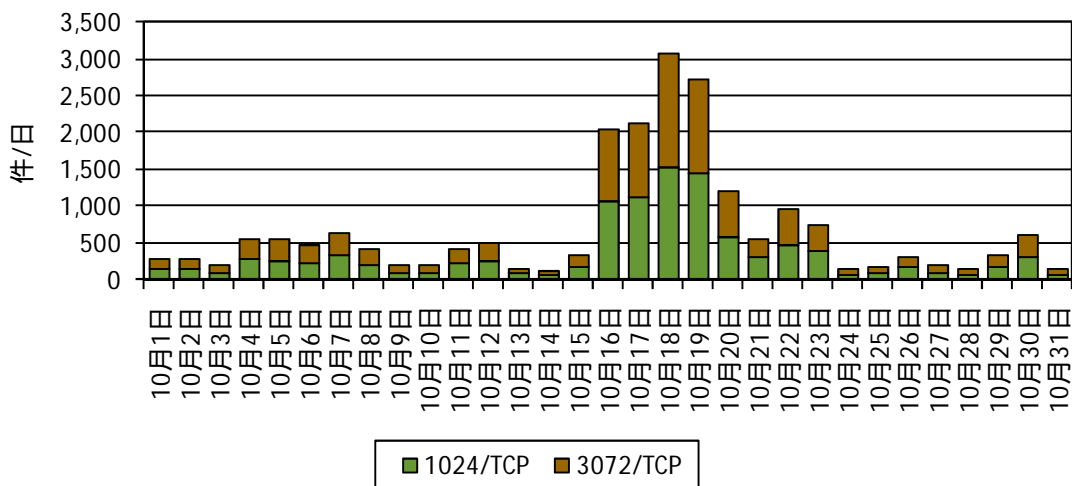


図 2-2 跳ね返りパケットの検知状況(宛先ポート:1024/TCP、3072/TCP)

今期において検知した、1024/TCP と 3072/TCP を宛先ポートとする跳ね返りパケットのほとんどは、これらのポートから攻撃パケットを発信する、何らかのツールによるものであったと考えられる。

2-3 米国の特定の IP アドレスへの DoS 攻撃の検知状況

10 月 11 日から 23 日にかけて、米国の特定の IP アドレスから、1024/TCP と 3072/TCP を宛先ポートとする大量の跳ね返りパケットを検知した。特に、10 月 16 日から 19 日の検知が多い。(図 2-3) この IP アドレスからは、9 月 18、19 日に同様の跳ね返りパケットを検知した後、断続的な検知が続いている。これらも、攻撃パケットの発信元ポートを 1024/TCP と 3072/TCP とするツールを使用した攻撃と考えられる。

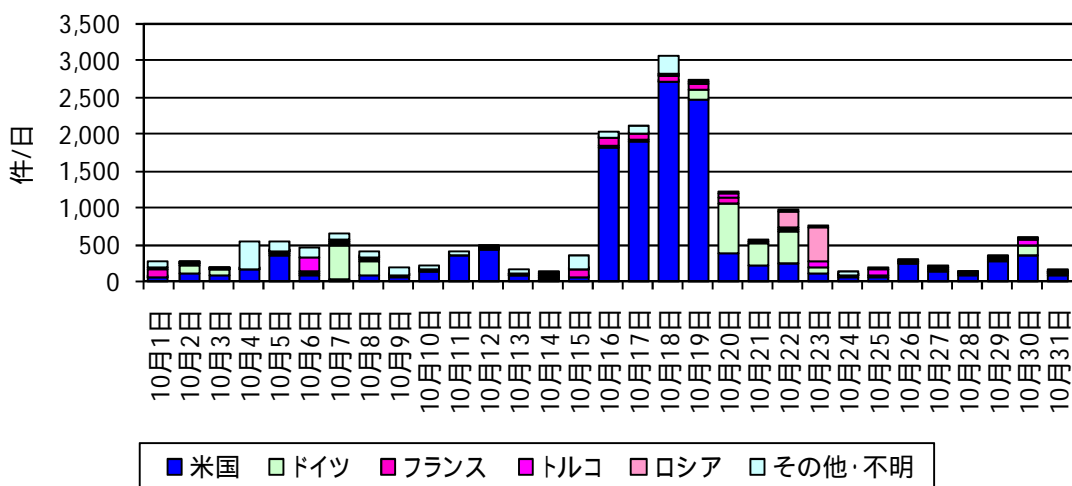


図 2-3 跳ね返りパケットの検知状況(国別、宛先ポート:1024/TCP、3072/TCP)

検知した跳ね返りパケットの発信元ポート(被害サーバにおける被害サービス)は、80/TCP (WWW)、53/TCP(DNS)及び3306/TCP(MySQL)であった。攻撃者が10月16日から23日にかけて、これらのサービスを順に攻撃したことがわかる。(図2-4)

跳ね返りパケットは、ほとんどがSYN/ACKパケットであったが、53/TCPに対する攻撃があった10月22日の19時から23時に、RST/ACKパケットを検知している。RST/ACKパケットは、そのサービスが起動していない場合や、被害サーバの負荷が増えて接続処理できない場合などに送信される。したがって、この時間は被害サーバはサービス不能に陥っていた可能性がある。

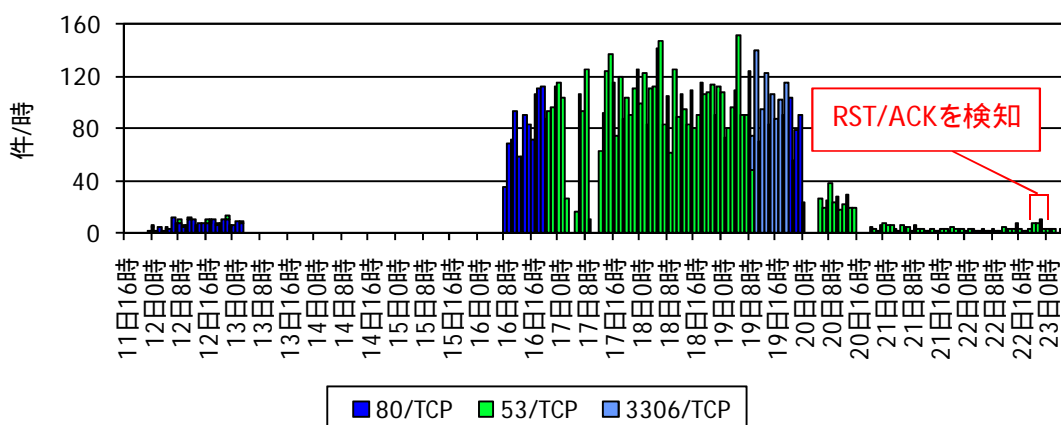


図2-4 米国の特定IPからの跳ね返りパケット(発信元ポート別)

2-4 1024/TCPと3072/TCPのこれまでの検知状況

サイバーフォースセンターでは、以前から継続的に1024/TCPと3072/TCPへの跳ね返りパケット¹を検知している。1024/TCPと3072/TCPへの跳ね返りパケットの検知件数は、ほぼ同数になっており、今期と同様に、ほとんどがツールを使用した攻撃によるものと考えられる。(図2-5)

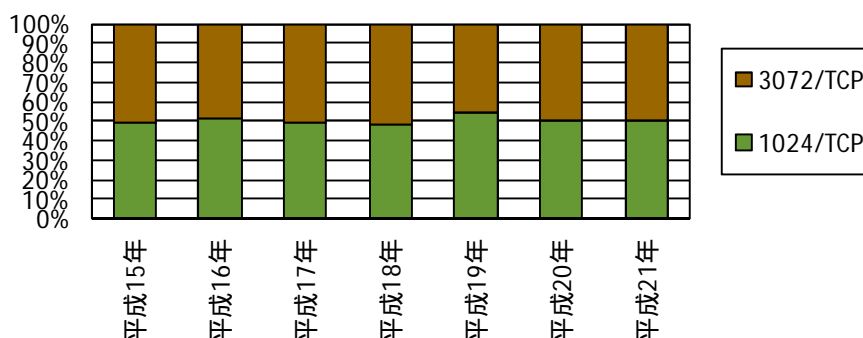


図2-5 跳ね返りパケットの宛先ポートの比率¹

¹ 平成15年7月から、平成21年は1月から今期(10月)までの期間を集計している。平成16年までは、跳ね返りパケット(SYN/ACK、RST/ACK)を区別していないため、全パケットを集計している。

なお、平成 19 年は、1024/TCP が 3072/TCP よりも多くなっている。これは、平成 19 年 4 月 16 日に、中国の特定の IP アドレスから 1024/TCP への跳ね返りパケットを大量に検知したためである。この攻撃は、跳ね返りパケットの宛先ポートが 1024/TCP のみであるなどの検知状況の特徴から、攻撃パケットの発信元ポートを 1024/TCP と 3072/TCP とするツールを使用した攻撃とは異なるものと考えられる。(図 2-5、図 2-7)

跳ね返りパケットの発信元ポート(被害サーバにおける被害サービス)別では 80/TCP(WWW)が最も多いが、53/TCP(DNS)、22/TCP(SSH)や 6667/TCP(IRC)なども見られる。特に、DNS に対する攻撃は、ウェブサーバなどのすべてのサービスに影響を与えるため、被害が大きくなる可能性がある。(図 2-6)

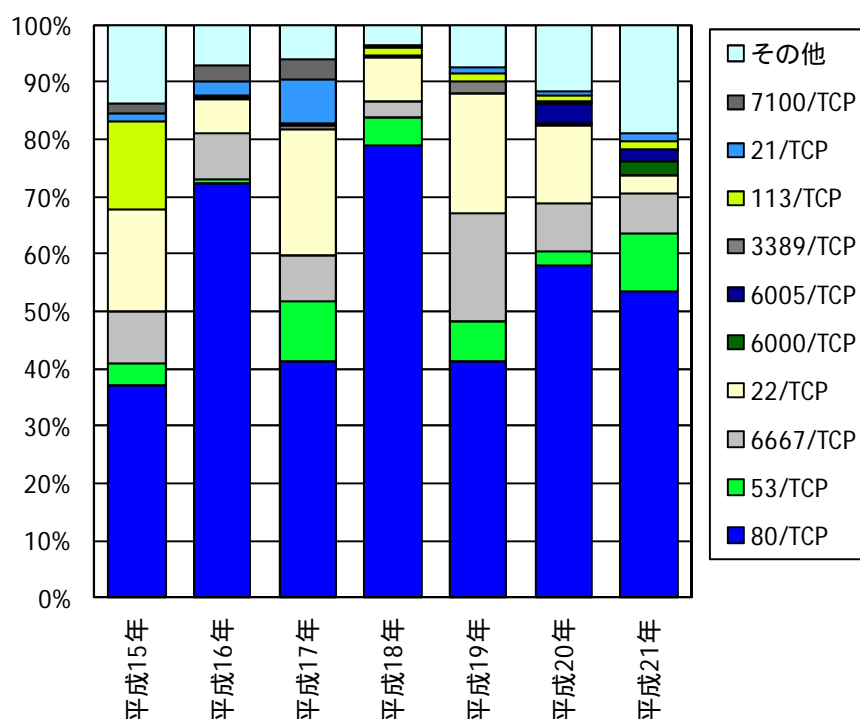


図 2-6 跳ね返りパケットの発信元ポートの比率¹ (宛先ポート:1024/TCP、3072/TCP)

平成 18 年 10 月 18 日から 11 月 9 日にかけて、英国の特定の IP アドレスから 80/TCP を宛先ポートとする跳ね返りパケットを大量に検知しており、英国の特定のウェブサーバが長期にわたって攻撃されていたと推測される。

また、日本国内では、平成 20 年 1 月 23 日に、特定の IP アドレスから 22/TCP を宛先ポートとする多くの跳ね返りパケットを検知している。この攻撃では、検知したパケットがすべて SYN/ACK パケットであることなどから、被害サーバはサービスを維持できていたものと推測される。

¹ 平成 15 年 7 月から、平成 21 年は 1 月から今期(10 月)までの期間を集計している。平成 16 年までは、跳ね返りパケット(SYN/ACK、RST/ACK)を区別していないため、全パケットを集計している。

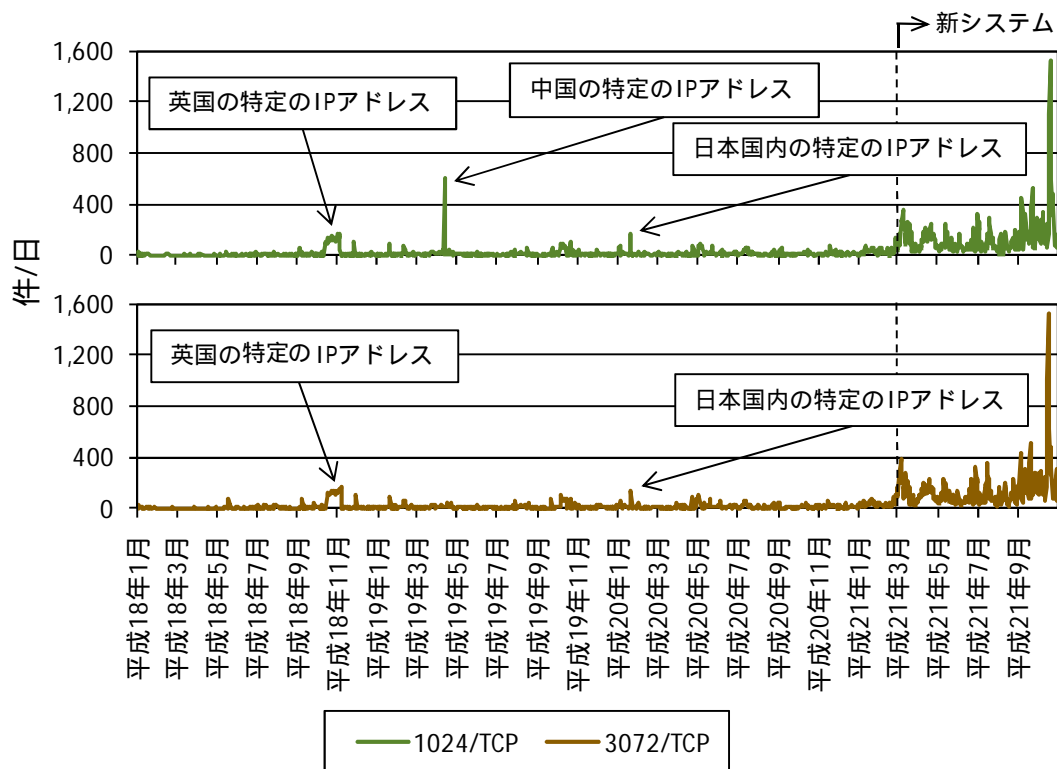


図 2-7 跳ね返りパケットの検知状況¹ (宛先ポート: 1024/TCP、3072/TCP)

2-5 1024/TCP と 3072/TCP を使用する攻撃ツール

1024/TCP と 3072/TCP を宛先ポートとする跳ね返りパケットは、ほとんどが特定のツールを使用した DoS 攻撃によるものと考えられる。

このツールと考えられるプログラムがインターネット上に公開されていることを確認している。このプログラムは、攻撃パケットの発信元 IP アドレスを、 2^{31} 個の IP アドレスからランダムに詐称し、攻撃パケットの発信元ポート(跳ね返りパケットの宛先ポート)は、1024/TCP 又は 3072/TCP をランダムに指定する仕様になっており、プログラムの仕様と検知状況が一致している。

このツールは、平成 12 年 8 月頃からインターネット上で入手可能となっていた模様である。

¹ 平成 21 年 3 月以降は、システム更新による検知性能向上により、検知件数も増加している。

2-6 まとめ

今期は、1024/TCP と 3072/TCP を宛先ポートとする跳ね返りパケットが増加した。

この跳ね返りパケットは、攻撃パケットの発信元ポートを 1024/TCP と 3072/TCP とするツールを使用した攻撃によるものがほとんどであると考えられる。このツールは、平成 12 年 8 月頃からインターネット上で入手可能であった模様であり、長年にわたって悪用されていたと考えられる。

SYN flood 攻撃などの DoS 攻撃を行うツールは、このツールの他にも、インターネット上に数多く存在しており、攻撃先の IP アドレスやポート番号などを入力するだけの、技術的な知識のない者でも容易に攻撃が可能なものも存在する。

今年 7 月には、米国や韓国の政府機関などのウェブサイトが、大規模なサイバー攻撃 (DoS 攻撃) の被害を受けたと報道された。日本国内においても、平成 16 年 8 月に、複数の政府機関に対する DoS 攻撃が発生し、これらのウェブページの閲覧に支障が生じている。

DoS 攻撃は、容易に実行が可能であり、これまでも日常的に攻撃が行われてきた。ボットネットを使用した大規模な DDoS 攻撃も発生しており、今後も、DoS 攻撃による被害が予想される。

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

前期に引き続き、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。(図 3-1、表 3-1)

今期 1 位の 445/TCP に対するアクセスは、引き続き増加傾向が見られ、Conficker ワームの感染拡大が依然として継続していると考えられる。

今期 3 位の 8/ICMP に対するアクセスは、前期と比較してやや減少した。以前から継続していた中国の特定の IP アドレスからの定期的なアクセスが、10 月 7 日に停止したためである。しかし、10 月 27 日から、同じ IP アドレスからの定期的なアクセスを再度検知しており、何者がスキャン行為を再開したのと考えられる。(図 3-6)

前期 4 位だった 2967/TCP に対するアクセスは、中国の特定の IP アドレスからのアクセスがなくなったため、大幅に減少した。前期における 2967/TCP へのアクセスは、発信元ポートの大半が 6000 であり、短時間に大量のアクセスが見られるなど、ツールによるアクセスの特徴を持っていた。何者かが、継続して行っていたツールによるスキャン活動を停止した可能性が考えられる。

10 月 24 日にベトナムの特定の IP アドレスから 1433/TCP に対するアクセスが急増した。(図 3-7) このアクセスは現在も継続しており、発信元ポートがすべて 6000 であることから、2967/TCP と同様にツールによるスキャン活動が行われている可能性がある。

ツールを用いた発信元ポート 6000 からのアクセスについては、1521/TCP に対するスキャンツールがインターネット上で配布されている事を確認しており¹、今期検知した 6000 を発信元とする 2967/TCP 及び 1433/TCP についても、同様にツールが存在し、使用されている可能性がある。

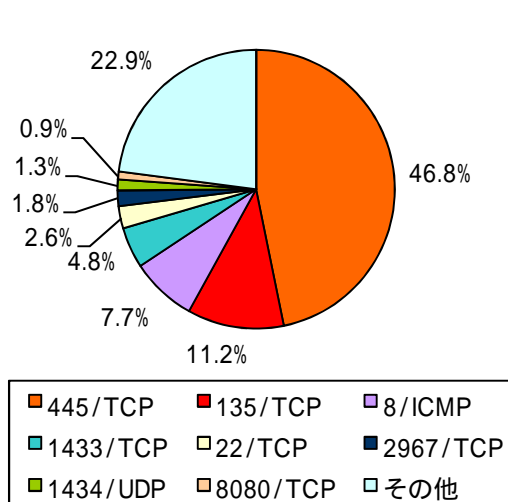


図 3-1 世界の宛先ポート比率²

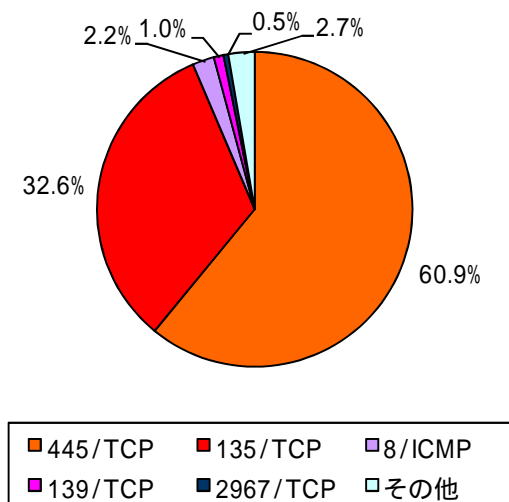


図 3-2 日本の宛先ポート比率²

表 3-1 宛先ポート別検知件数

¹ 「我が国におけるインターネット治安情勢(平成 21 年 7 月期)」 p.4 「2-2 Oracle 社製データベースソフトへの攻撃ツール」, <http://www.cyberpolice.go.jp/detect/pdf/20090831.pdf>

² 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。

今期 順位	前期 順位	ポート	今期件数 (一日・1IP 当たり)	前期比 (一日・1IP 当たり)	増加 順位	減少 順位
1位	1位	445/TCP	177.63 件	+ 7.2% (+ 11.93 件)	1位	
2位	2位	135/TCP	42.40 件	- 7.9% (- 3.65 件)		3位
3位	3位	8/ICMP	29.08 件	- 16.8% (- 5.86 件)		2位
4位	5位	1433/TCP	18.06 件	- 4.5% (- 0.85 件)		
5位	6位	22/TCP	9.87 件	- 7.7% (- 0.83 件)		
6位	4位	2967/TCP	6.89 件	- 77.8% (- 24.12 件)		1位
...			...			
12位	15位	5900/TCP	2.29 件	+ 41.6% (+ 0.67 件)	5位	
13位	18位	23/TCP	2.21 件	+ 57.9% (+ 0.81 件)	2位	
14位	8位	1080/TCP	2.08 件	- 39.3% (- 1.35 件)		5位
...			...			
16位	21位	1024/TCP	1.97 件	+ 68.6% (+ 0.80 件)	3位	
17位	20位	3072/TCP	1.88 件	+ 59.9% (+ 0.70 件)	4位	
...			...			
29位	14位	1025/TCP	0.38 件	- 83.6% (- 1.93 件)		4位

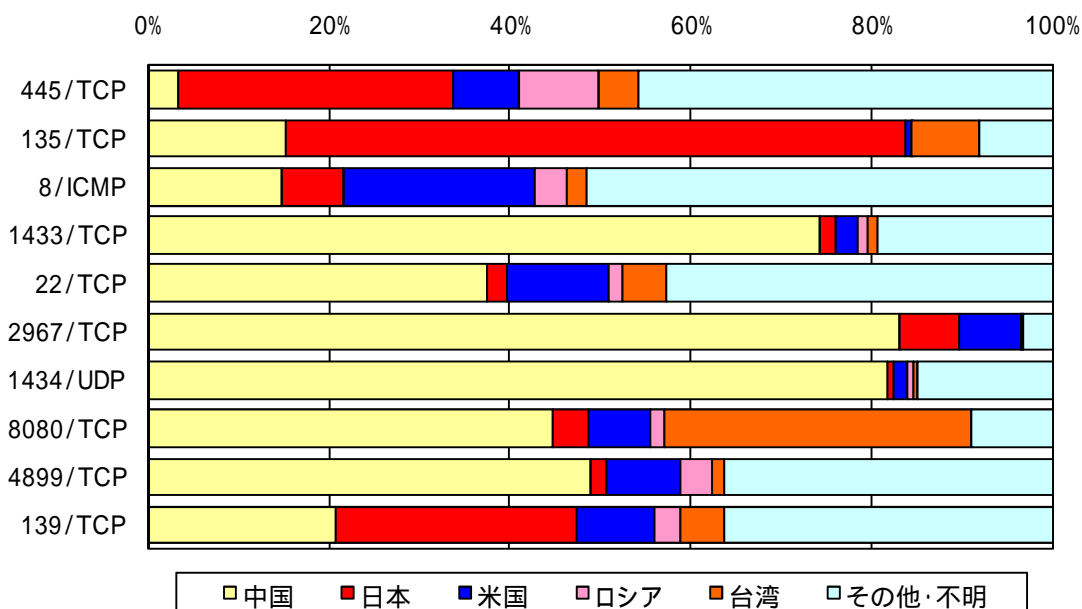


図 3-3 宛先ポートの国・地域別比率

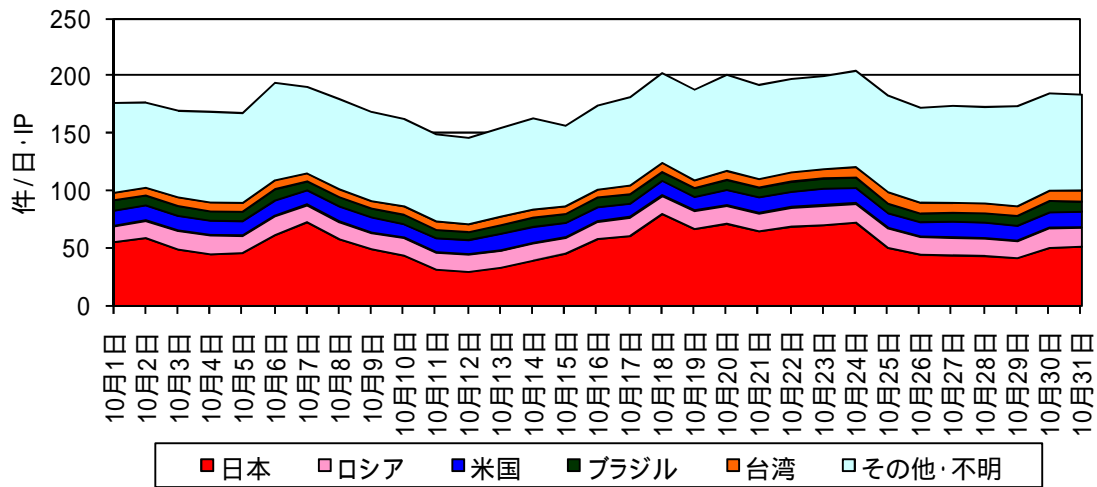


図 3-4 宛先ポート 445/TCP に対するアクセスの推移

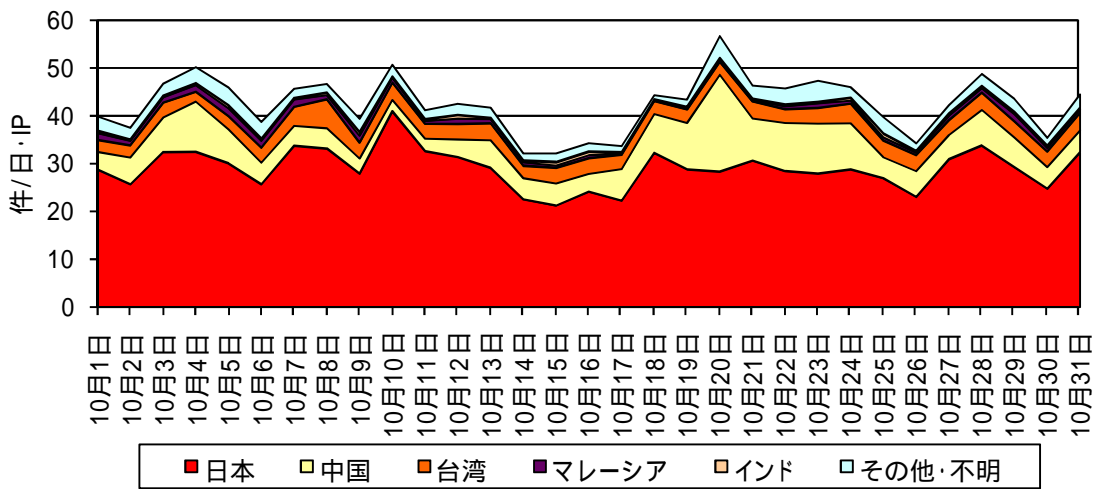


図 3-5 宛先ポート 135/TCP に対するアクセスの推移

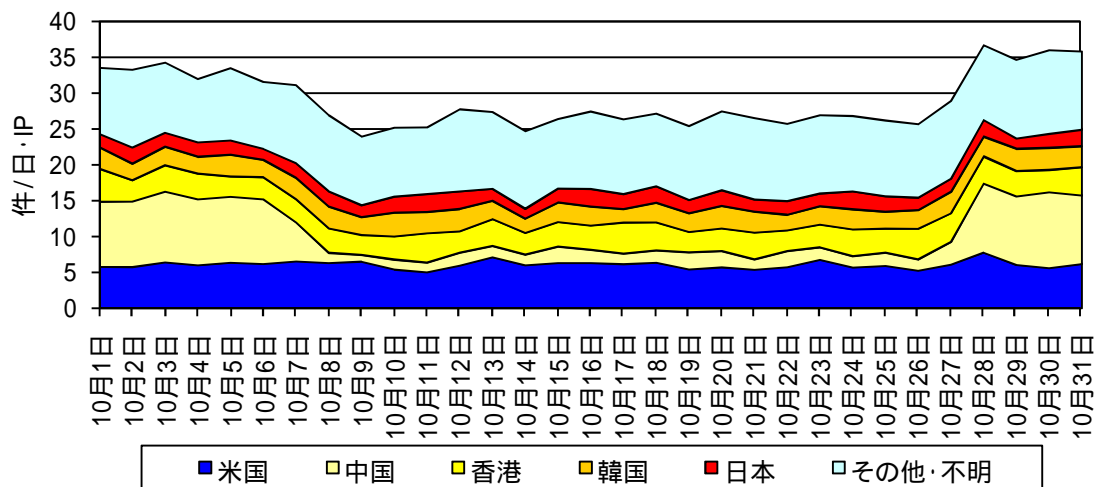


図 3-6 8/ICMP のアクセスの推移

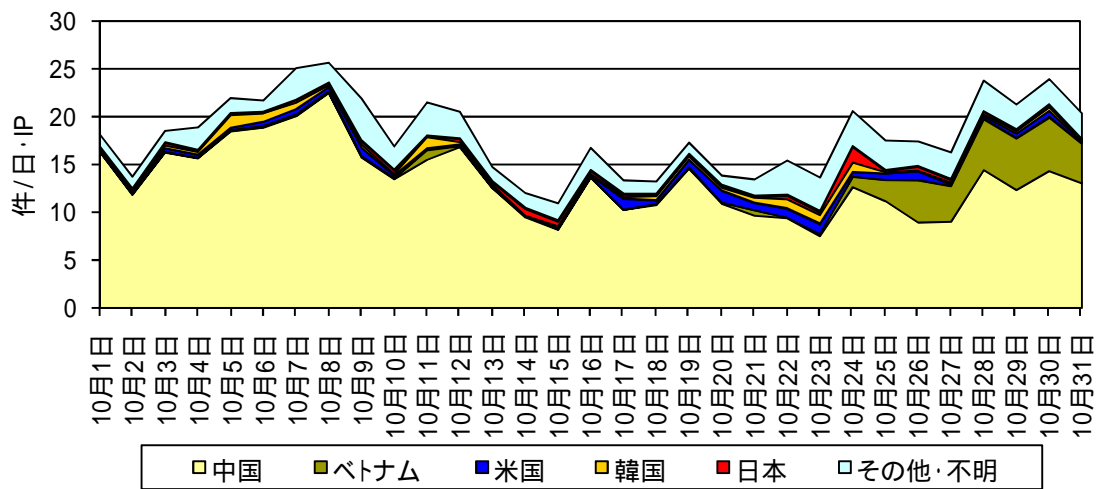


図 3-7 宛先ポート 1433/TCP に対するアクセスの推移

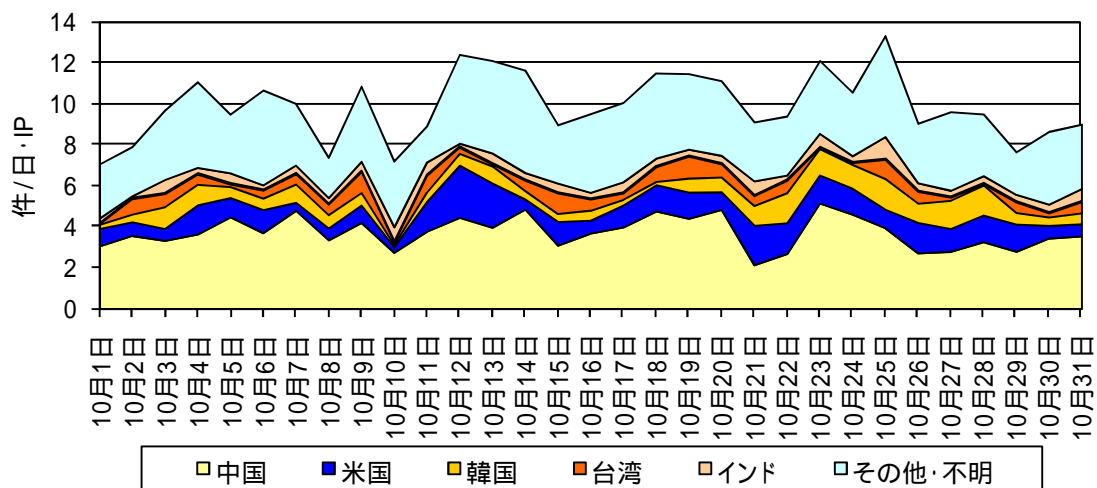


図 3-8 宛先ポート 22/TCP に対するアクセスの推移

3-2 発信元国・地域別

前期に引き続き上位 5 か国の順位に変動はなかった。しかし、今期は中国からのアクセス減少が顕著であった。(図 3-9、図 3-10、表 3-2)

中国からは、2967/TCP 及び 8/ICMP に対するアクセスが大幅に減少した。特定の IP アドレスから 2967/TCP に対して行われていたスキャンが 9 月 29 日に停止している。また、別の IP アドレスから行われていた 8/ICMP へのアクセスは、10 月 7 日に一旦停止したが、10 月 27 日から再び検知している。(図 3-6、図 3-12)

今期増加順位 1 位のフィリピンについては、10 月 25 日に特定の IP アドレスから、5644/TCP を発信元ポートとする大量の跳ね返りパケットを検知した。5644/TCP は、オンラインゲームでも使用されており、何者かがオンラインゲームサービスの妨害を目的とし、フィリピンのサーバに対して DoS 攻撃を行っていたと考えられる。

10 月 11 日から 23 日にかけて、米国の特定の IP アドレスから、1024/TCP と 3072/TCP を宛先ポートとする大量の跳ね返りパケットを検知した。(図 3-14) これについては「2-3 米国の特定の IP アドレスへの DoS 攻撃の検知状況」で述べている。

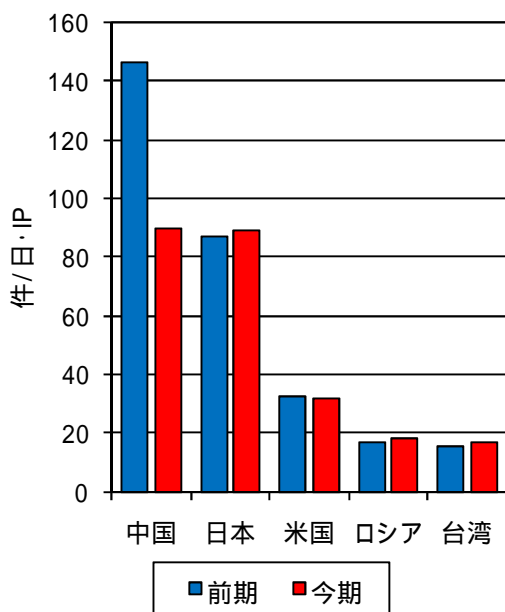


図 3-9 国・地域別検知件数の前期との比較

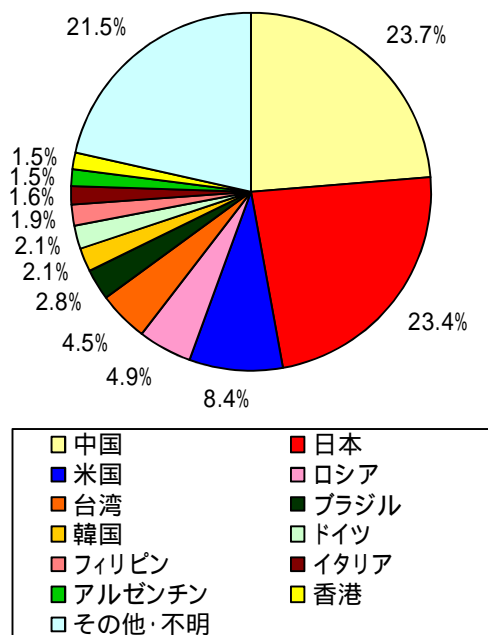


図 3-10 発信元国・地域別比率¹

¹ 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 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 (一日・1IP 当たり)	前期比 (一日・1IP 当たり)	増加 順位	減少 順位
1位	1位	中国	89.94 件	- 38.6% (- 56.48 件)		1位
2位	2位	日本	88.91 件	+ 1.7% (+ 1.48 件)	4位	
3位	3位	米国	31.94 件	- 1.0% (- 0.31 件)		
4位	4位	ロシア	18.44 件	+ 9.0% (+ 1.52 件)	3位	
5位	5位	台湾	17.17 件	+ 10.9% (+ 1.69 件)	2位	
6位	6位	ブラジル	10.55 件	- 4.4% (- 0.48 件)		4位
...			...			
9位	25位	フィリピン	7.16 件	+ 326.1% (+ 5.48 件)	1位	
...			...			
15位	14位	カナダ	4.44 件	- 10.1% (- 0.50 件)		3位
...			...			
19位	15位	ウクライナ	3.02 件	- 27.5% (- 1.15 件)		2位
...			...			
33位	26位	オーストラリア	1.15 件	- 28.6% (- 0.46 件)		5位
...			...			
43位	70位	ペルー	0.86 件	+ 361.8% (+ 0.67 件)	5位	

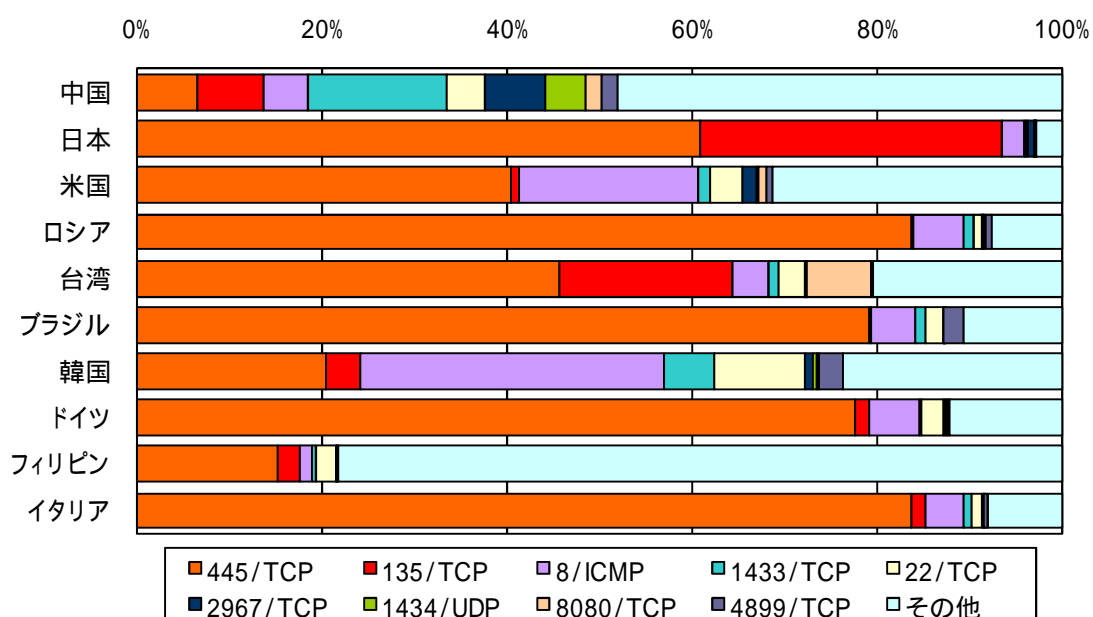


図 3-11 発信元国・地域別上位のポート別比率

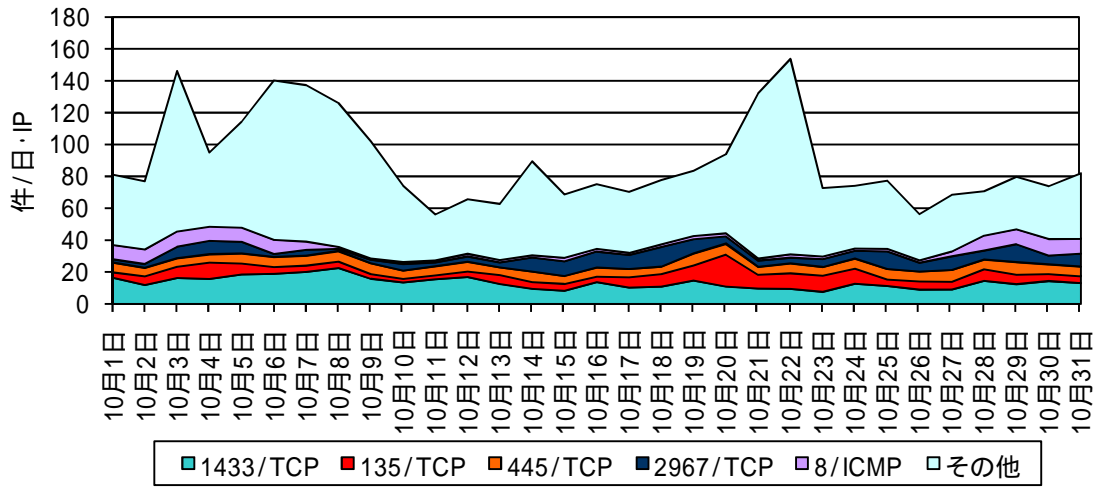


図 3-12 中国からのアクセスの推移

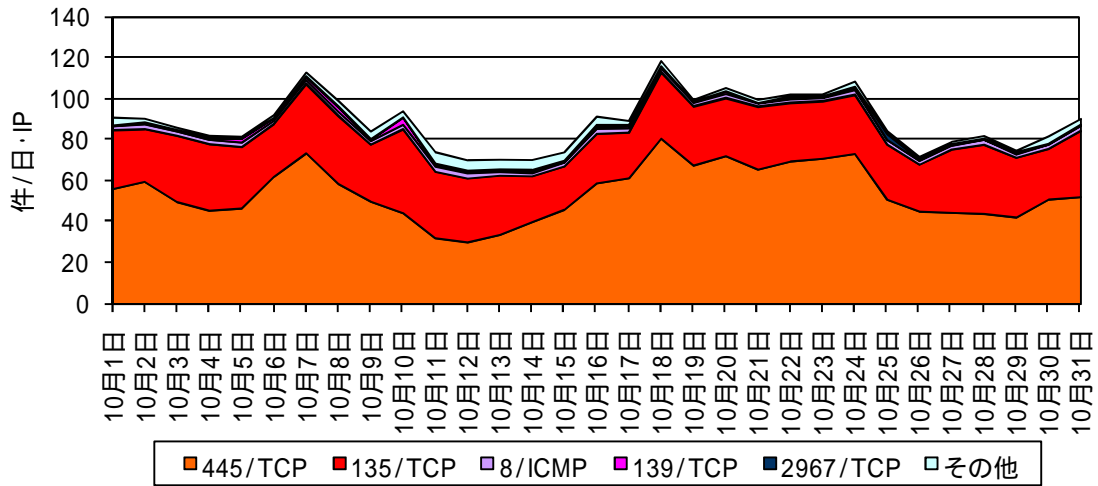


図 3-13 日本からのアクセスの推移

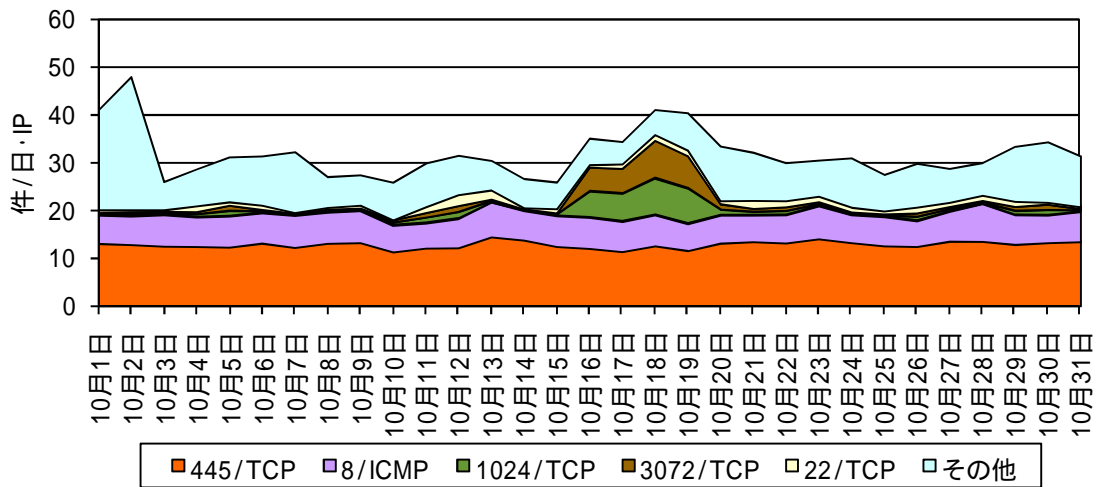


図 3-14 米国からのアクセスの推移

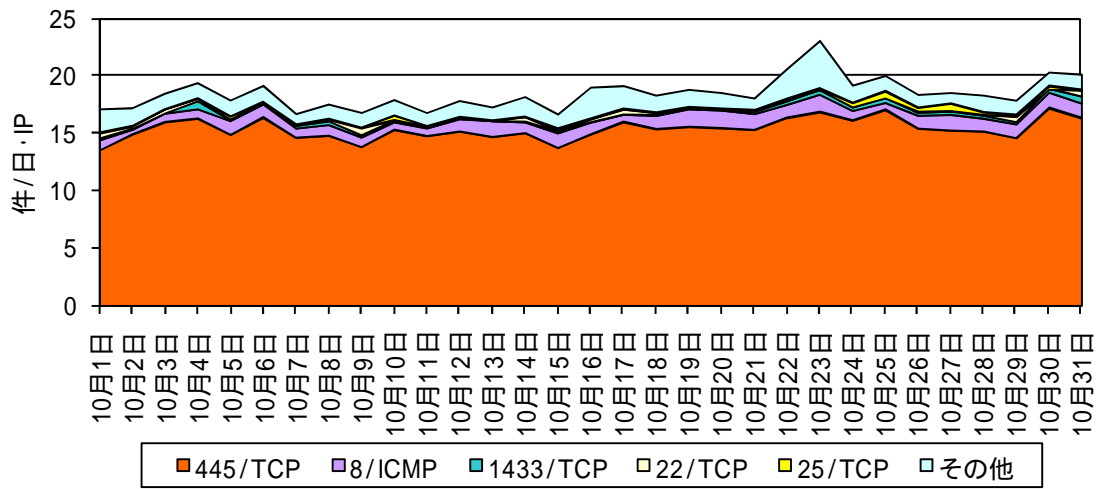


図 3-15 ロシアからのアクセスの推移

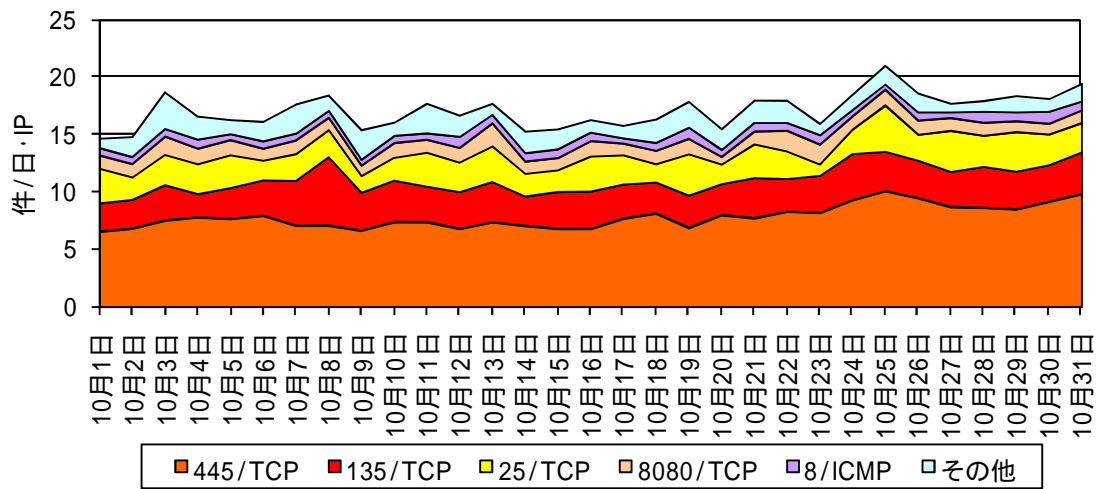


図 3-16 台湾からのアクセスの推移

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

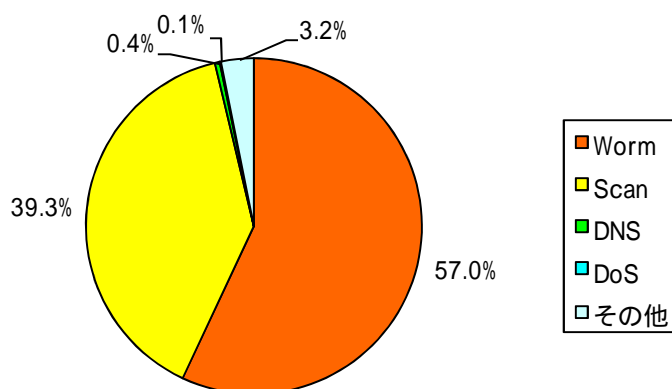


図 4-1 シグネチャを用いた不正侵入等の攻撃手法別検知比率¹

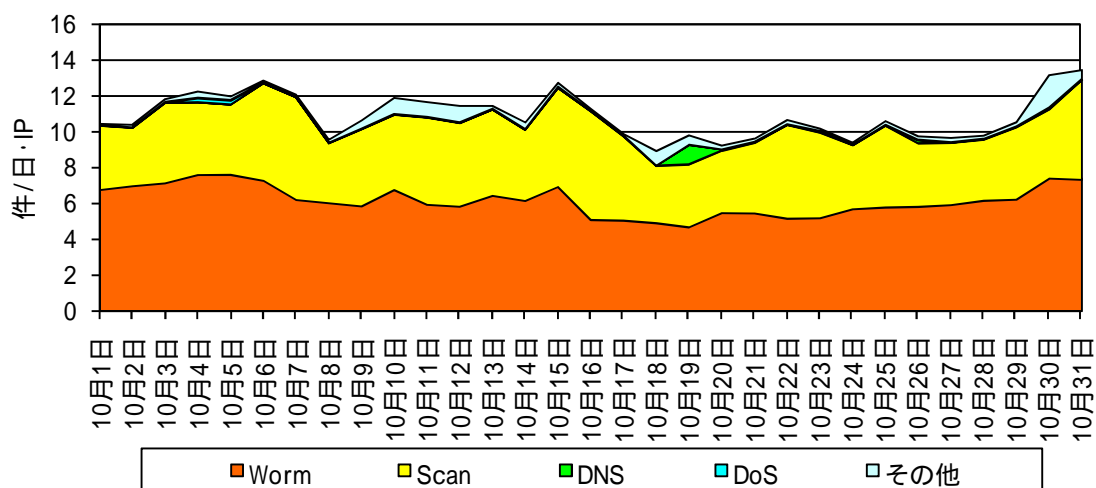


図 4-2 シグネチャを用いた不正侵入等の攻撃手法別検知推移

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 10.9 件で、前期と比較して - 0.9 件 (- 7.7%) とやや減少した。

攻撃手法別では、「DNS」の検知件数が大幅に減少した。これは、7月31日から続いていたDNSの誤設定が原因と考えられるドイツからの検知が、9月16日以降なくなったためである。誤設定が修正されたものと考えられる。

「Worm」の検知件数は一日・1IP 当たり 6.2 件であり、約 3/4 が SQL Slammer ワーム、約 1/4 が Nachi ワームである。この 2 つのワームの検知件数は共に緩やかな減少が続いている。

¹ 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 (一日・1IP 当たり)	前期比 (一日・1IP 当たり)	増加 順位	減少 順位
1 位	1 位	Worm	6.20 件	+ 3.6% (+ 0.21 件)	1 位	
2 位	2 位	Scan	4.28 件	+ 4.3% (+ 0.18 件)	2 位	
3 位	3 位	DNS	0.05 件	- 94.9% (- 0.91 件)		1 位
4 位	4 位	DoS	0.01 件	- 96.9% (- 0.42 件)		2 位

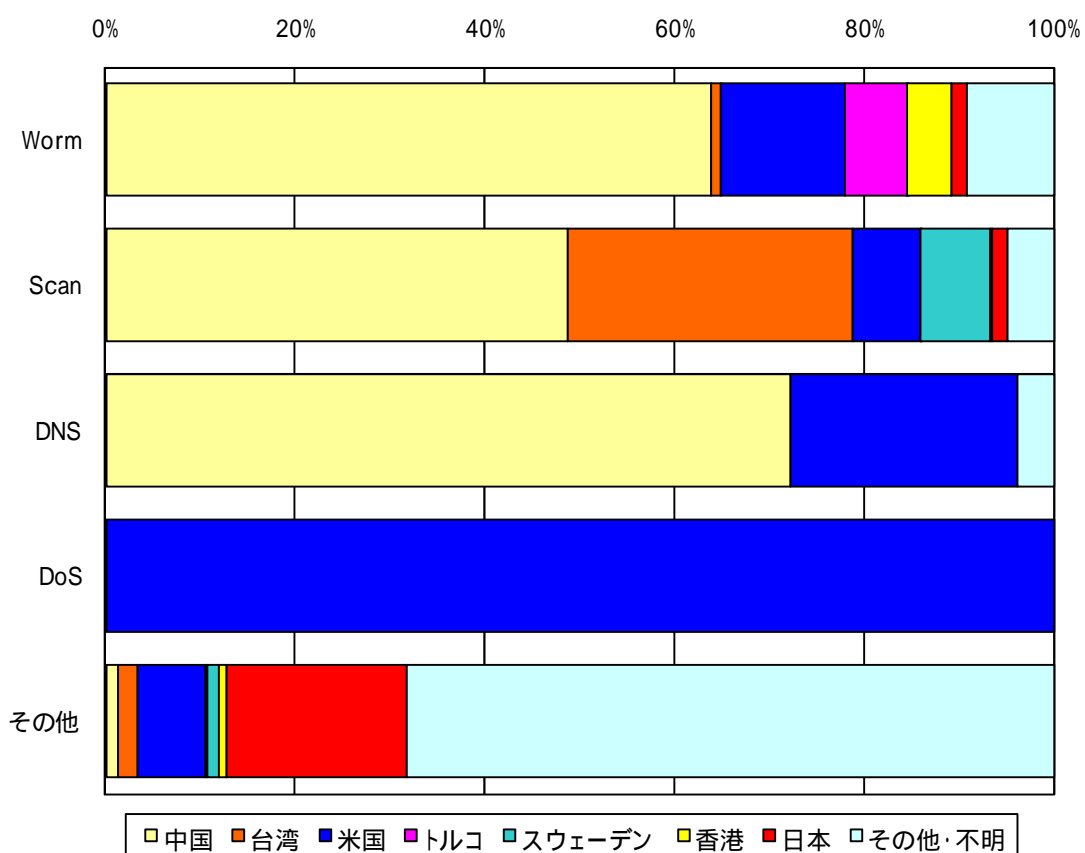


図 4-3 シグネチャを用いた不正侵入等の攻撃手法の国・地域別比率

4-2 発信元国・地域別

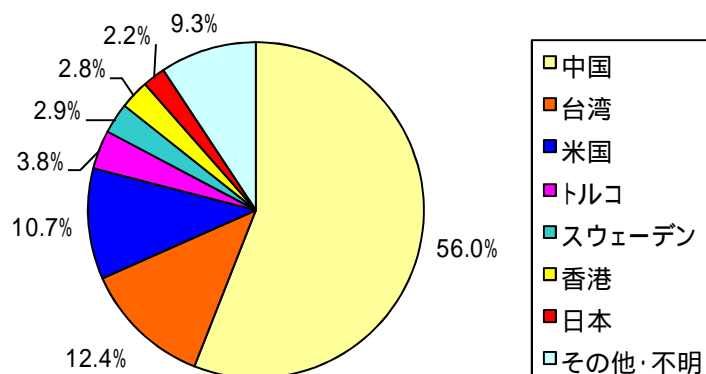


図 4-4 シグネチャを用いた不正侵入等の発信元国・地域別検知比率¹

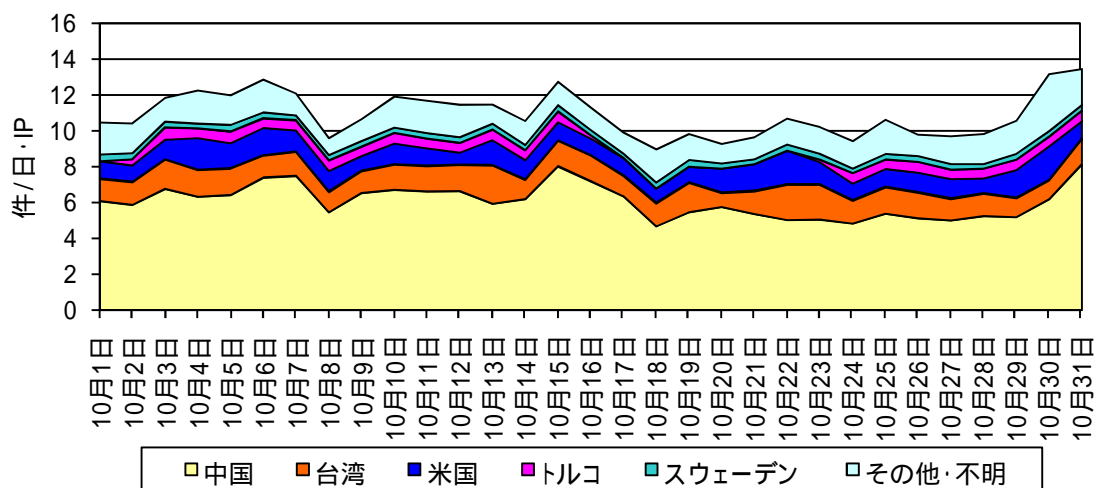


図 4-5 シグネチャを用いた不正侵入等の発信元国・地域別検知推移

今期は、台湾とトルコを発信元とする検知件数が増加している。

台湾を発信元とする検知件数は、一日・1IP 当たり 1.3 件で、ほとんどがプロキシサーバを探索する活動である。これは以前からの台湾の特徴である。

トルコの特定の IP アドレスから SQL Slammer ワームを断続的に検知している。これは、トルコ国内のサーバが SQL Slammer ワームに感染しているものと考えられる。

¹ 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 (一日・1IP 当たり)	前期比 (一日・1IP 当たり)	増加 順位	減少 順位
1位	1位	中国	6.09 件	- 4.0% (- 0.25 件)		3位
2位	5位	台湾	1.34 件	+ 116.0% (+ 0.72 件)	1位	
3位	2位	米国	1.16 件	- 9.4% (- 0.12 件)		4位
4位	11位	トルコ	0.41 件	+ 278.0% (+ 0.30 件)	2位	
5位	7位	スウェーデン	0.32 件	+ 11.9% (+ 0.03 件)	4位	
...			...			
9位	3位	アルゼンチン	0.11 件	- 85.9% (- 0.65 件)		1位
10位	9位	韓国	0.09 件	- 46.9% (- 0.08 件)		5位
11位	19位	ロシア	0.08 件	+ 91.2% (+ 0.04 件)	3位	
...			...			
15位	4位	ドイツ	0.03 件	- 95.5% (- 0.63 件)		2位
...			...			
22位	51位	パキスタン	0.02 件	- ¹ (+ 0.02 件)	5位	

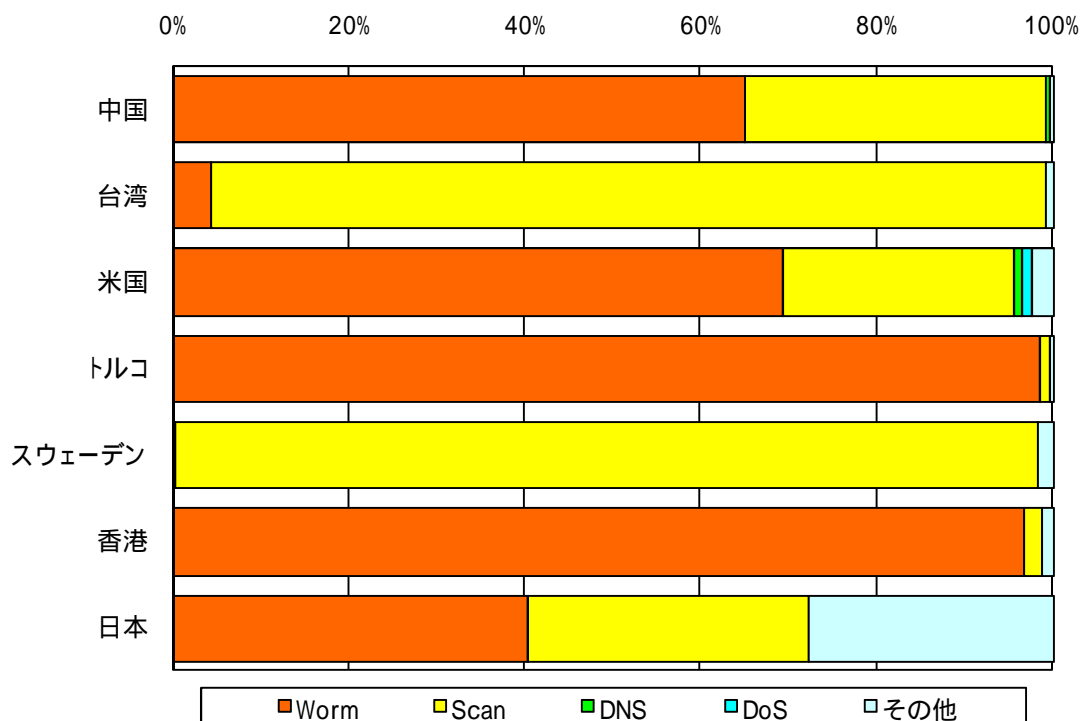




図 4-6 シグネチャを用いた不正侵入等の発信元国・地域別上位のシグネチャ別比率

¹ 前期の検知件数が少なかったため、前期比率は記載していない。

5 @police (Topics)掲載事項

@police において 10 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	アドビシステムズ社の Adobe Reader および Adobe Acrobat のセキュリティ修正プログラムについて(10/14)
 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 (MS09-050,051,052,053,054,055,056,057,058,059,060,061,062) (10/29)更新

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 10 月 31 日現在、シグネチャは 2,992 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