平成 21 年 8 月 31 日

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)

- 韓国、米国に対するサイバー攻撃が発生
  ～韓国の一部サイトから、サイバー攻撃の影響と見られるパケットを観測～
- 1521/TCP に対するアクセスが急増
  ～Oracle 社製データベースソフトへの攻撃ツールをインターネット上で確認～
- 445/TCP に対するアクセスが、依然として高い水準
  ～「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 360.1 件で、前期と比較して－58.8 件（－14.0%）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 4899/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 131.1 件で、前期と比較して－5.7 件（－4.2%）と、やや減少している。445/TCP については、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と考えられ、感染拡大は沈静化したものと推測される。しかしながら、ワーム発生前と比較すると 4.9 倍のアクセス件数があり、依然として高い水準で推移していることから、引き続き警戒が必要である。

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り、中国及び日本で全体のほぼ 5 割を占めた。

今期は中国からのアクセスが減少したが、これは 135/TCP、2967/TCP へのアクセスが減少したほか、中国が発信元の大半を占めていた UDP spam を、6 月 20 日以降に検知しなくなった事が影響している。

今期は、韓国や米国の主要官庁などのウェブサイトが大規模なサイバー攻撃を受けたと報道された。警察庁では、このサイバー攻撃の影響と見られる韓国からのパケットを観測した。「2-1 韓国･米国に対するサイバー攻撃」で述べる。

また、今期は 1521/TCP に対するアクセスが増加している。1521/TCP は Oracle 社製データベースソフトで使用されるポートであり、攻撃者がツールを用いてスキャン行為を行っている可能性がある。「2-2 Oracle 社製データベースソフト」で述べる。

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 11.0 件で、前期と比較して－5.9 件（－34.8%）と減少した。これについても、中国からの UDP spam を検知しなくなったことが大きく影響している。

2　分析 ― 注目すべきアクセス

2-1　　韓国･米国に対するサイバー攻撃

平成 21 年 7 月に入り、韓国や米国の主要官庁などのウェブサイトが、大規模なサイバー攻撃の被害を受けたと報道された。

今回のサイバー攻撃は、不正プログラムに感染し、攻撃者に乗っ取られた多数のパソコンが、攻撃の発信元になったといわれている。この不正プログラムには、多数の亜種が存在しているが、事前に攻撃時刻と攻撃先が書き込まれたものが利用されたとのことである。被害サーバは、不正プログラムに感染した多数のパソコンから、指定された時刻に大量のアクセスが行われるため、全てのアクセスを処理しきれず、サービス不能状態になる。これは、DDoS 攻撃と呼ばれるサイバー攻撃である。(図 2-1)

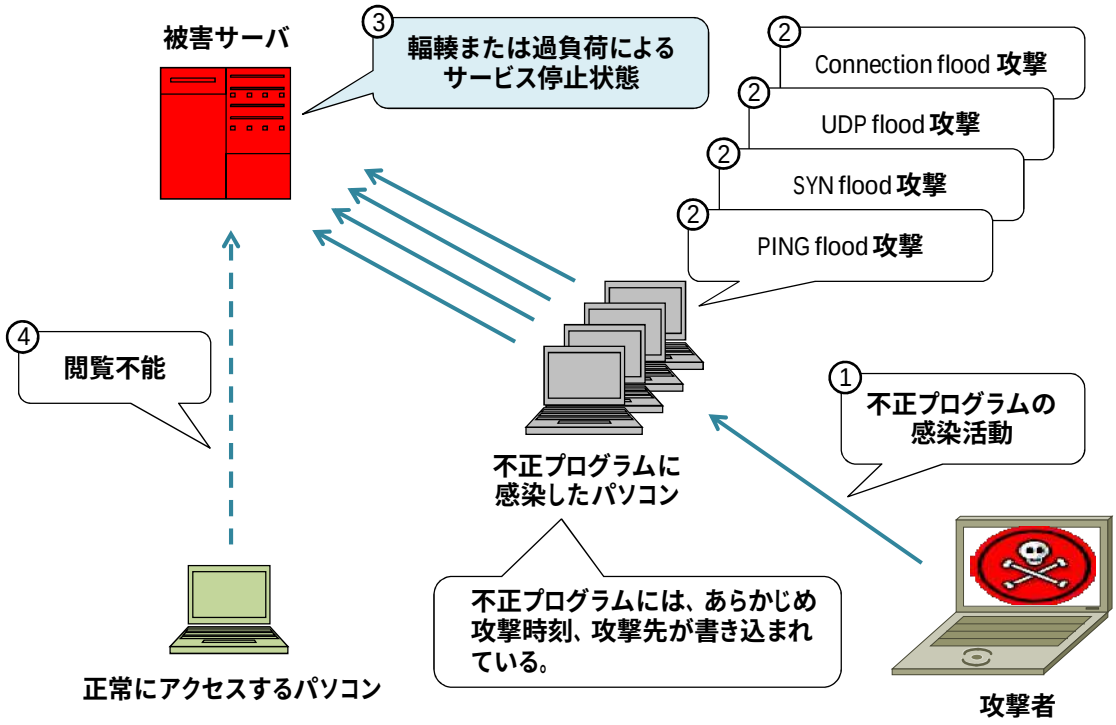

図 2-1　不正プログラムによる DDoS 攻撃

韓国や米国の主要官庁などのウェブサイトが、大規模なサイバー攻撃の被害を受けたとされる同じ時期、警察庁では、韓国の特定サイトから、サイバー攻撃の影響とみられるパケットを観測した（図 2-2）。

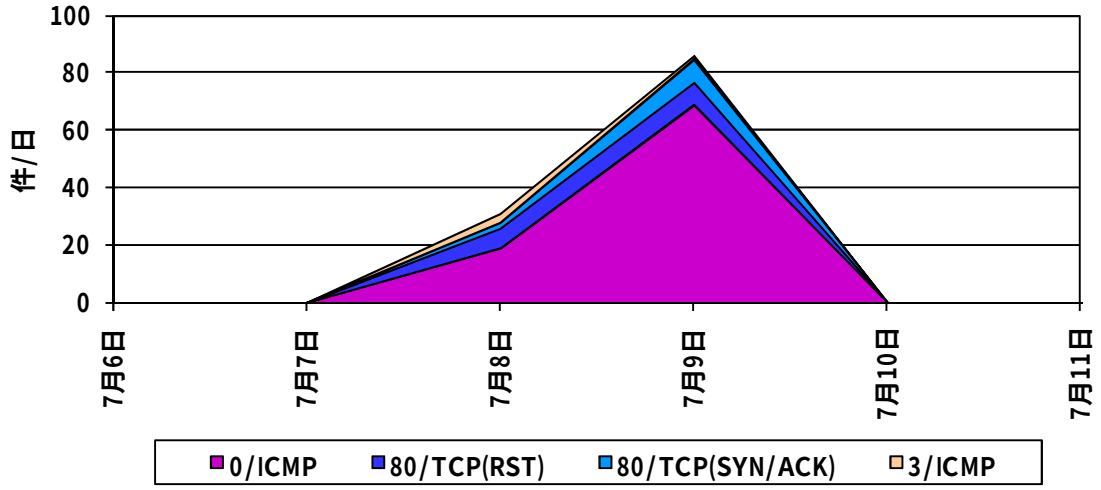

図 2-2 韓国の特定サイトを発信元とするアクセスの推移

7 月 8 日から 9 日にかけて、0/ICMP が観測された。0/ICMP は、8/ICMP に対する応答パケットであり、この時期、韓国の特定サイトは、大量の 8/ICMP パケットを送りつけられる、PING flood 攻撃を受けた可能性が高い。

また、同様に 80/TCP の RST パケットや SYN/ACK パケットが観測された。SYN パケットを大量に送りつけられる、SYN flood 攻撃が併用されていたものと考えられる。

7 月 8 日には、3/ICMP も観測されている。この 3/ICMP は、80/UDP に対するアクセスが受け付けられずに戻ってきたものであった。韓国の特定サイトは、大量の 80/UDP を送りつけられる、UDP flood 攻撃も受けていた可能性がある。

なお、当該特定サイト以外のサイトからのパケットは観測されなかった。これら他のサイトへは、発信元の偽装を行わない Connection flood 攻撃など、別の攻撃が行われた可能性がある。

2-2　Oracle 社製データベースソフトへの攻撃ツール

(1)　定点観測センサーでの 1521/TCP の検知状況

1521/TCP は、Oracle 社製データベースソフトを使用したサーバに、ネットワーク経由で接続する際に利用されるポートであり、主にリモートからの SQL の実行に利用される。

1521/TCP に対するアクセスは 7 月 8 日から増加しはじめ、下旬にはさらに急増した。

発信元国・地域別では、中国を発信元とするものが多く、7 月 8 日以降の今回のアクセスでは、全体の 92%を占めている(図 2-3)。また、発信元ポートが 6000 となっているものが、全体の 99%となっていることも大きな特徴である(図 2-4)。発信元ホスト数についても、7 月下旬から急増している(図 2-5)。

今回のアクセスは、発信元ポートが 6000 であるなど共通点が多く、何らかの同一の手法によりアクセスが行われた可能性が高いと考えられる。

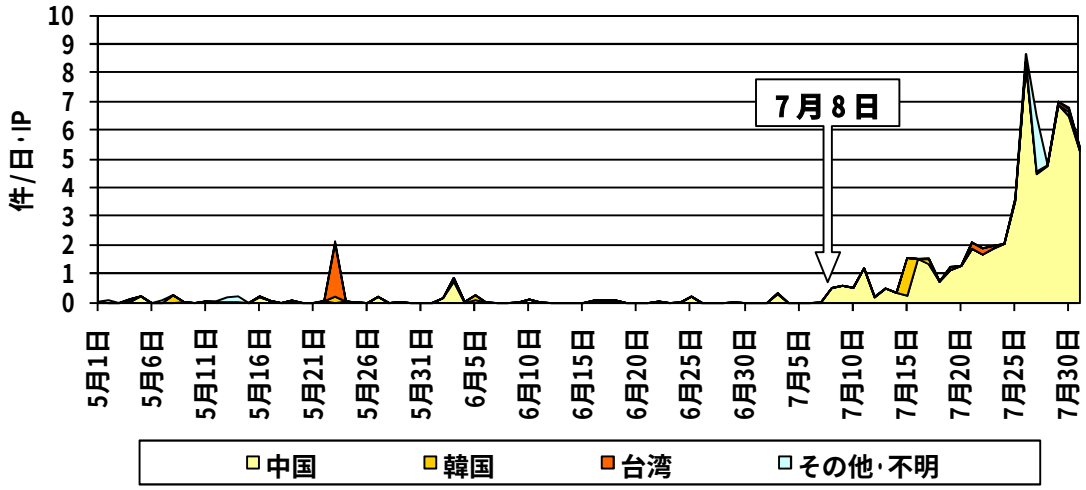

図 2-3　1521/TCP に対するアクセス（発信元国・地域別）

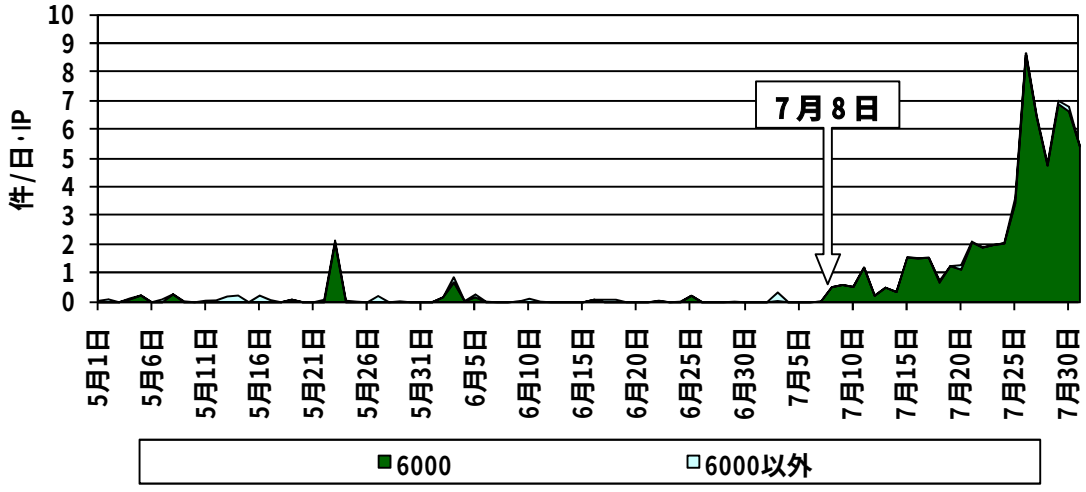

図 2-4　1521/TCP に対するアクセス(発信元ポート別)

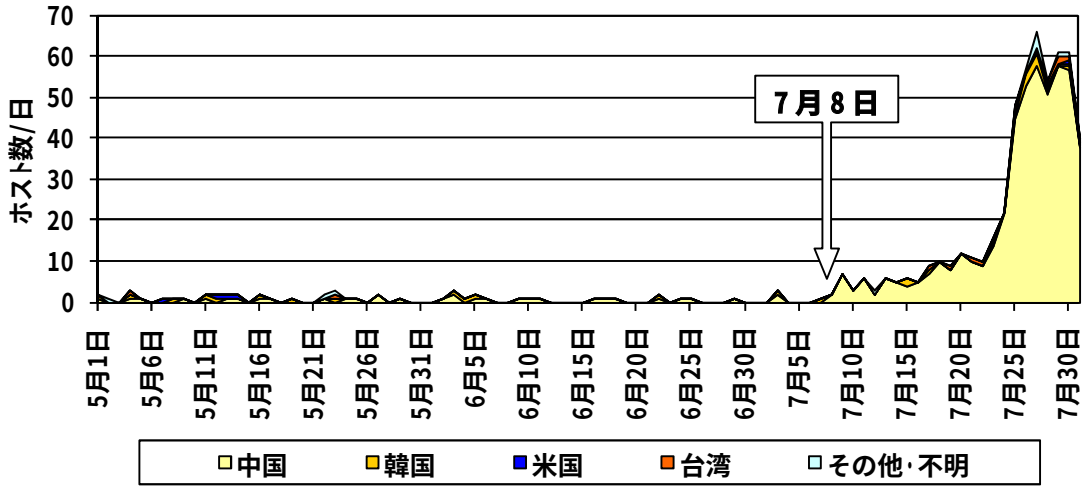

図 2-5 1521/TCP に対するアクセス(発信元ホスト数)

(2) SYNACKER センサー

今回、定点観測センサーで検知した 1521/TCP に対するアクセスはすべて、TCP セッションを確立するための接続要求に関係するパケットであった。そこで、アクセスの目的を調査するため、TCP に対するアクセスに応答する「SYNACKER」センサーを用意し、観測を行った (図 2-6)。

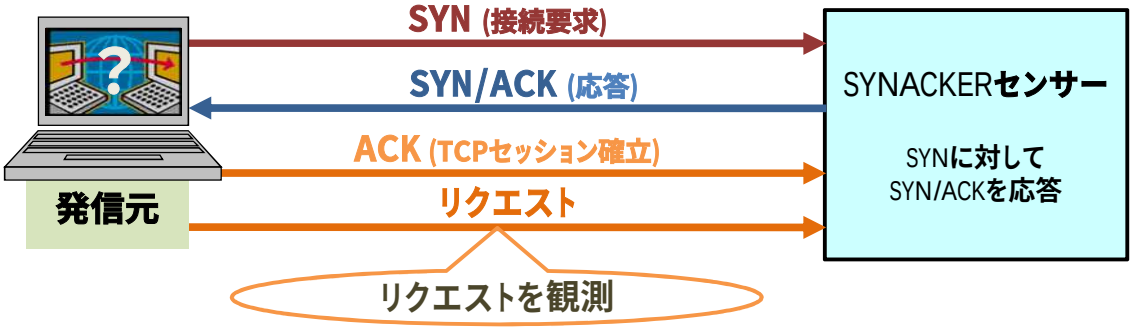

図 2-6 TCP の SYN パケットに応答する観測センサー(「SYNACKER」センサー)

(3) 1521/TCP に対する通信の流れ

「SYNACKER」センサーでは、次のようなアクセスを観測した。

まず、発信元ポート 6000 から SYN パケットが送信され、「SYNACKER」センサーに到達する。「SYNACKER」センサーが応答すると、時間をおいて、6000 とは別のポート番号から、「SYNACKER」センサーに対して、Oracle 社製データベースソフトへの接続を要求する。(図 2-7)

データベースソフトへの接続要求には、発信元において接続に利用したツールとみられる、実行ファイル名とフォルダ名が含まれていた (図 2-8)。

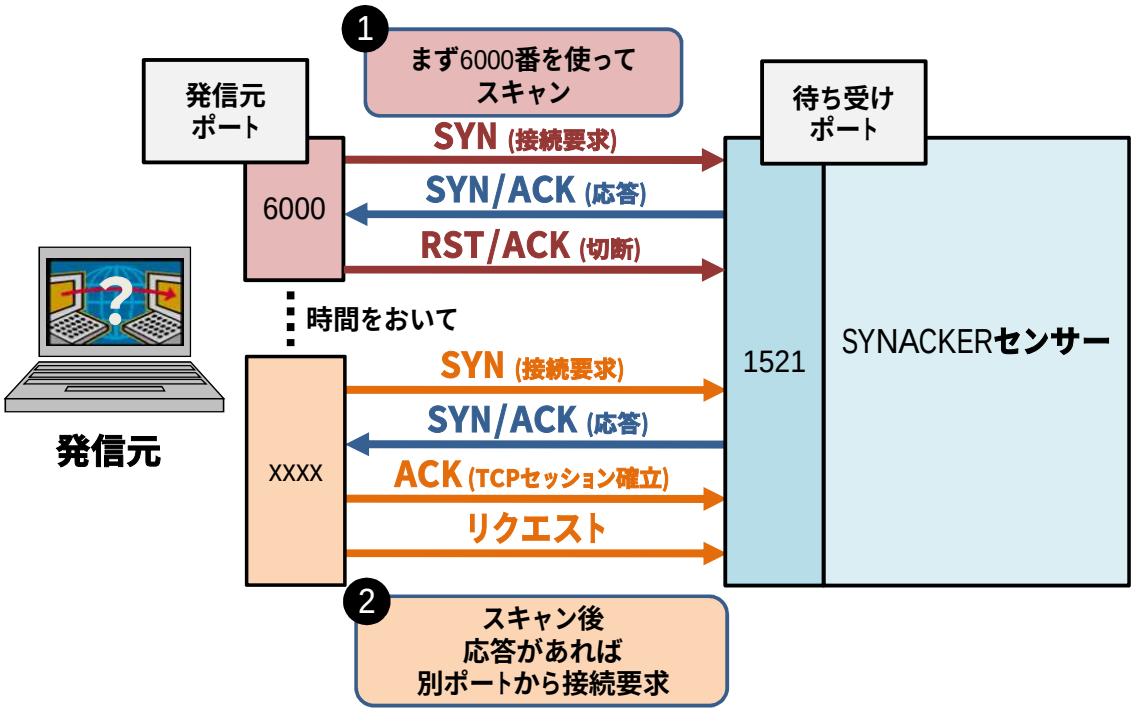

図 2-7 「SYNACKER」センサーで検知した 1521/TCP へのスキャン活動

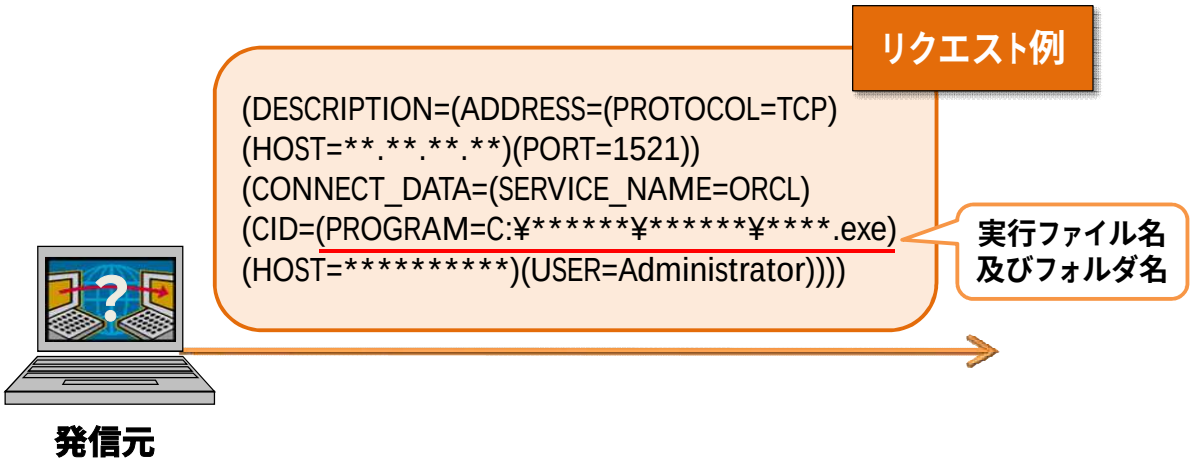

図 2-8 「SYNACKER」センサーで検知したリクエスト(*の部分は状況により変化する)

(4) 1521/TCP に対するスキャンツール

インターネット上で調査したところ、1521/TCP に対してスキャンを行うツールを配布している中国語のサイトを発見した(図 2-9)。この配布されているツールをダウンロードしたところ、ツールのファイル名が「SYNACKER」センサーで観測したリクエストの内容に含まれる実行ファイル名と一致していた。また、このツールを実行すると、発信元ポート 6000 を使用して、1521/TCP に対して SYN スキャンを行うことも確認できた。これは、定点観測センサーで検知した、1521/TCP に対する

観測状況と一致する。

また、中国語のブログのサイトで、同名のツールを紹介した 7 月 8 日付けの記事も確認できた。これは、定点観測センサーで 1521/TCP に対するアクセス増加を観測した時期と合致する。

図 2-9 ツール配布サイト

1521/TCP へのアクセス増加は、上述のような当該ポートへのスキャンを行うツールが、中国サイトを始めとするインターネット上で配布され、このツールが広く利用された事が原因と考えられる。

7月15日にはOracle社からデータベースソフト等の脆弱性情報及び修正プログラムが発表されている。また、8月1には、通信販売サイトのデータベースから、個人情報が窃取される事案も発生している。

これらの事から、Oracle 社の脆弱性情報発表をきっかけとして、データベースからの個人情報の窃取を目的とする、ツールを用いたスキャン行為が行われたため、1521/TCP に対するアクセスが急増したと考えられる。

このような攻撃の対処方法として、外部からデータベースサーバに接続する必要がない場合には、ファイアウォール等で制限を行うなどのアクセス管理を徹底されたい。また、外部からの利用が必要な場合にも、接続する IP アドレスを制限することや、デフォルトのポート番号 1521 から別のポート番号に変更し、運用することが有効である。

インターネット上では、攻撃を自動的に行うようなツールが配布されており、攻撃者はコンピュータの脆弱性を狙って常に活動している。これらの攻撃に利用されている脆弱性については、OS やアプリケーションベンダーから提供されるセキュリティ情報等を定期的に確認し、セキュリティパッチの適用や、機器の設定情報の確認を行うなどの対策を行う事が重要である。

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

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。前期と比較して、445/TCP のアクセス件数はやや減少しているものの、依然として高い水準で推移している。これは、「Conficker」ワームの流行が継続しているものと考えられる。

今期の増加 3 位である 1521/TCP は、Oracle 社製データベースソフトへの接続で利用されるポートである。1521/TCP に対するアクセスは、過去 1 年のデータを見ても、最高で 0.24 件/IP･日と低い水準で推移していたが、今期に入り、急激な件数の増加が見られた。1521/TCP の増加については、「2-2 Oracle 社製データベースソフト」で述べている。

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	131.08 件	−4.2% (−5.68 件)		1 位
2 位	2 位	135/TCP	57.28 件	+1.9% (+1.07 件)	5 位	
3 位	3 位	8/ICMP	30.69 件	+11.9% (+3.27 件)	1 位	
4 位	4 位	1433/TCP	26.84 件	+11.9% (+2.85 件)	2 位	
5 位	7 位	4899/TCP	10.48 件	+21.6% (+1.86 件)	4 位	
6 位	5 位	2967/TCP	10.09 件	−33.6% (−5.11 件)		2 位
…			…			
13 位	74 位	1521/TCP	2.03 件	−[1] (+1.96 件)	3 位	
…			…			
17 位	8 位	23/TCP	1.29 件	−76.8% (−4.26 件)		3 位
…			…			
−	13 位	1026/UDP	ごく僅か	−99.9% (−2.80 件)		4 位
…			…			
−	17 位	1027/UDP	検知なし	−[1] (−2.08 件)		5 位

[1] 前期の検知件数が少数、もしくは検知なし（1521/TCP の前期検知件数は 0.07 件、1027/UDP の今期検知なし）のため、前期比率は記載していない。

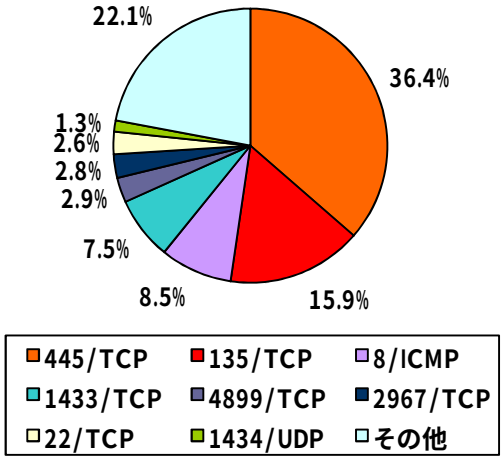

図 3-1 世界の宛先ポート比率[1]

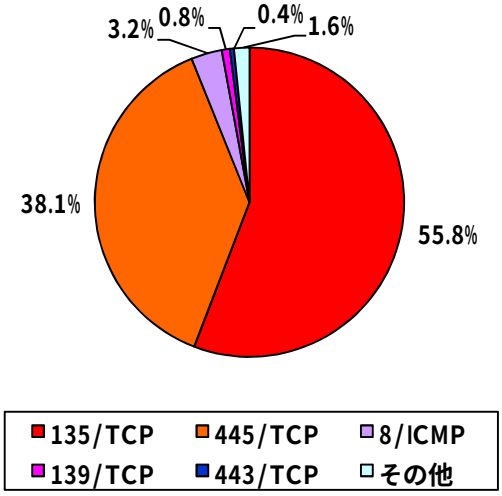

図 3-2 日本の宛先ポート比率[1]

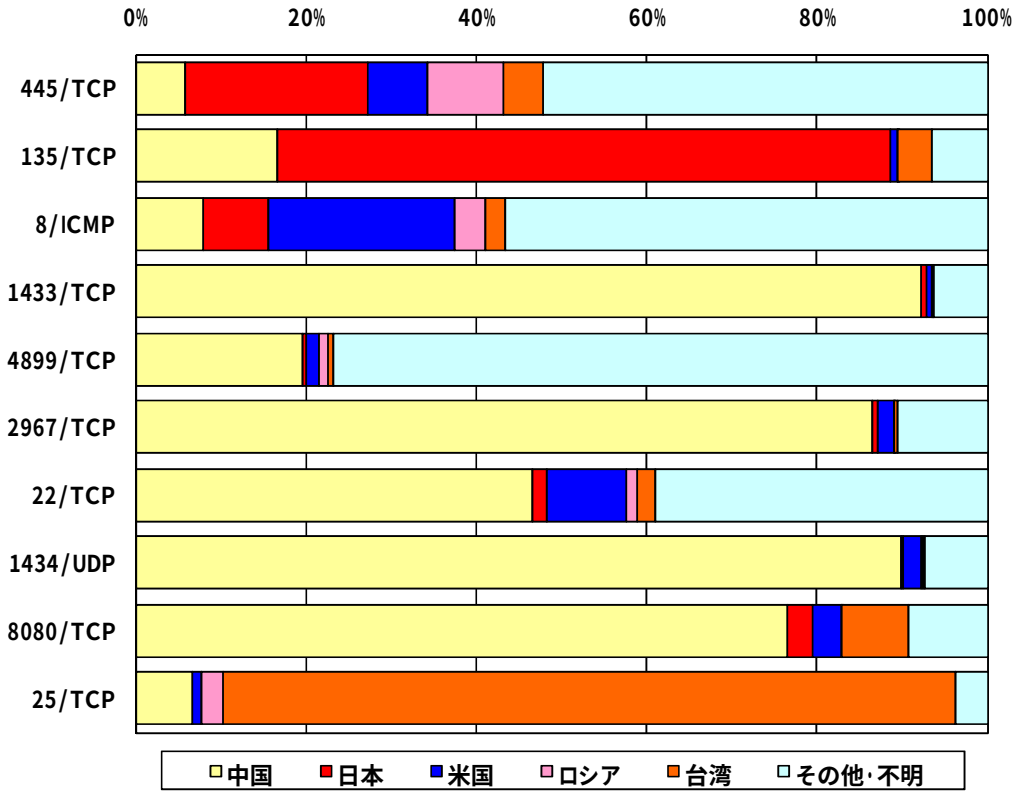

図 3-3 宛先ポートの国別比率

[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。

(2) 推移

今期 1 位の 445/TCP は、前期と比較して、アクセス件数がやや減少したものの、「Conficker」ワーム発生前の 2008 年 10 月と比較すると、4.9 倍のアクセス件数があり、依然として高い水準で推移している(図 3-5)。アクセス件数は、前期の後半に減少傾向がみられたが、今期に入って下げ止まり、ほぼ横ばいで推移している。

今期 3 位の 8/ICMP では、30 日と 31 日に中国からのアクセス増加がみられる。これは、特定の 1IP アドレスからのアクセスが増加したもので、8 月 1 日以降も当該 IP アドレスからのアクセスは継続している。何者かがスキャン活動を行っている可能性がある。

今期 5 位の 4899/TCP は、famatech 社製のリモートコントロールソフトウェアである Radmin で利用されるポートである。4899/TCP に対して、10 日から 16 日にかけてみられる、韓国を発信元とするアクセスは、特定の 1IP アドレスからのものである。何者かが Radmin の稼働するコンピュータを探索する、スキャン活動を行っていた可能性がある。一方、南米地域を発信元とするアクセスは、各国とも複数の IP アドレスが発信元である[1]。また、南米地域を発信元とするアクセスの時間帯推移をみると、24 時間周期で変化する日周型の特徴がみられた[2]。これは、家庭で使用されているセキュリティ対策を行っていないコンピュータに感染した、ボット又はウイルス等によるスキャン活動と考えられる。

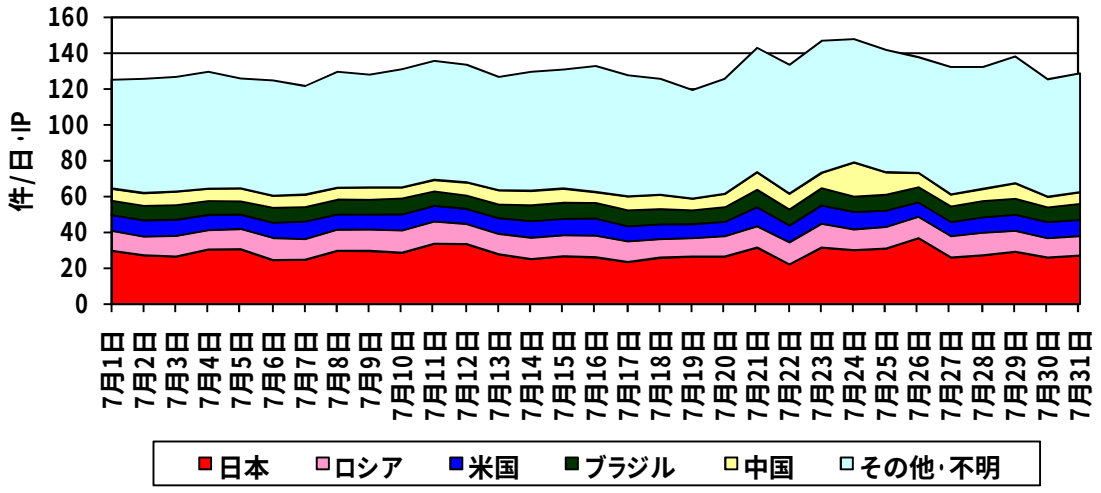

図 3-4 宛先ポート 445/TCP に対するアクセスの推移

[1] 各国の発信元 IP アドレス数は、アルゼンチンが 468 個、コロンビアが 461 個、ベネズエラが 275 個である。

[2] 「日周型」については「我が国におけるインターネット治安情勢(平成 21 年 5 月期)」P.8 「2-1 時間帯別検知状況」参照 http://www.cyberpolice.go.jp/detect/pdf/20090707.pdf

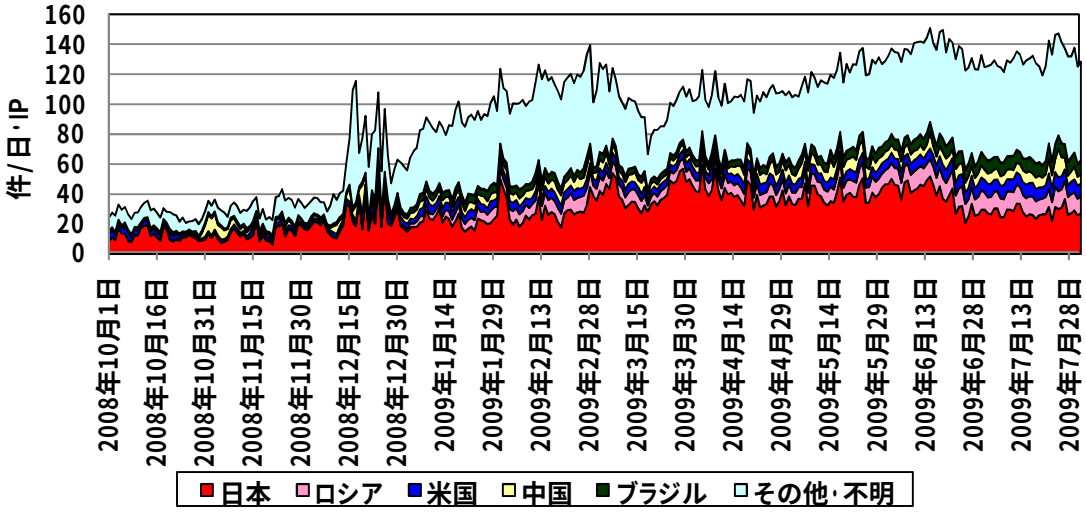

図 3-5 宛先ポート 445/TCP に対するアクセスの推移 (2008 年 10 月以降)

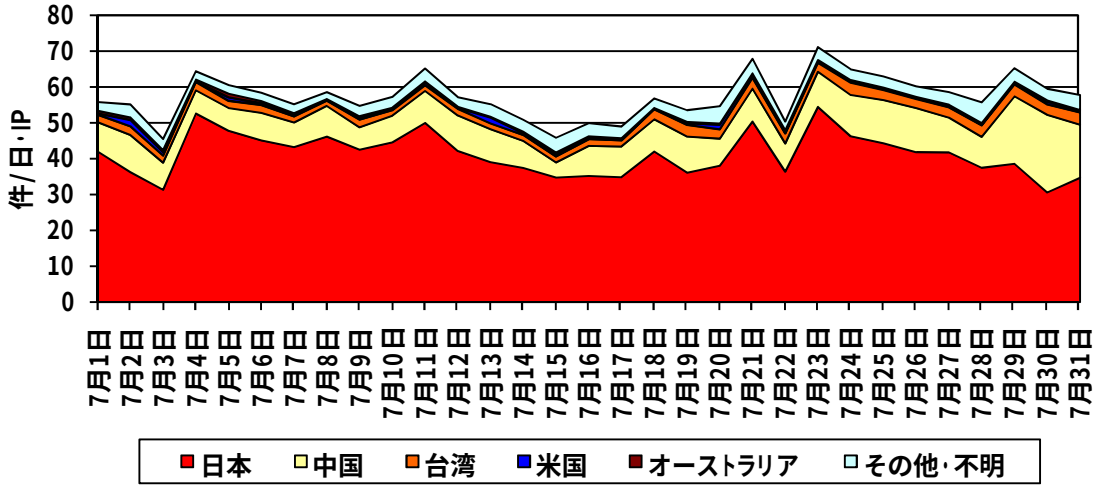

図 3-6 宛先ポート 135/TCP に対するアクセスの推移

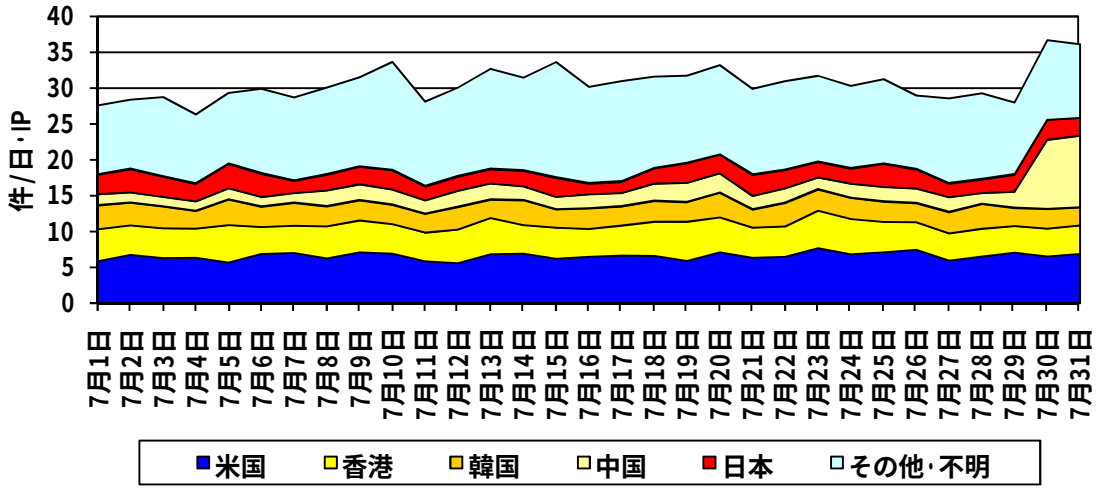

図 3-7 8/ICMP のアクセスの推移

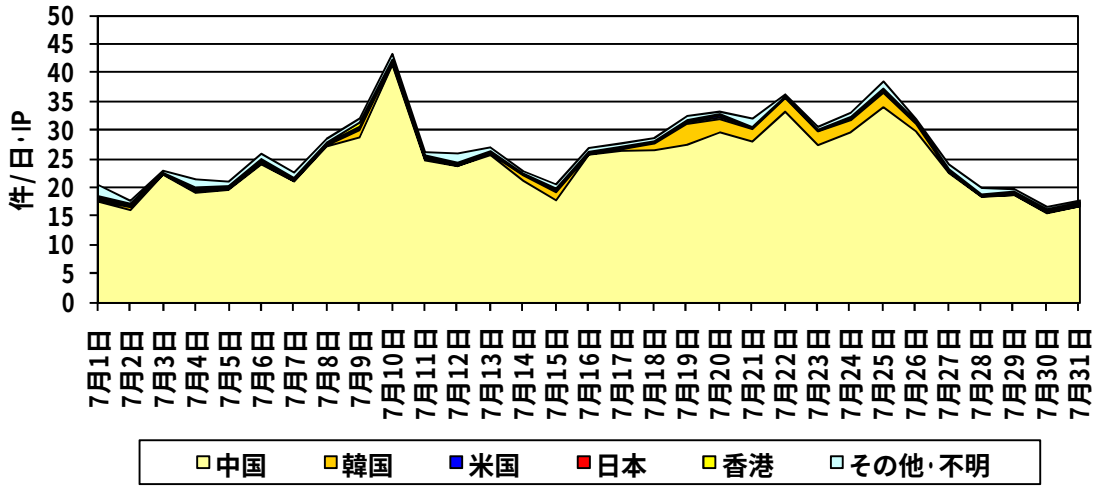

図 3-8 宛先ポート 1433/TCP に対するアクセスの推移

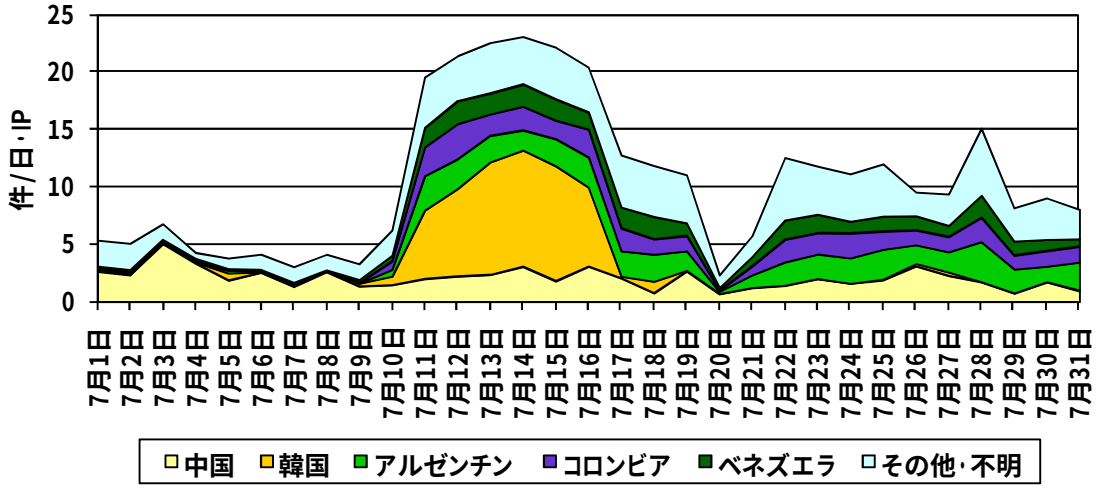

図 3-9 宛先ポート 4899/TCP に対するアクセスの推移

3-2　発信元国･地域別

(1)　概要

今期における国／地域別検知状況では、中国及び日本国内からのアクセスの減少が目立つ。

中国からのアクセスでは、2967/TCP と 135/TCP へのアクセスが減少していた。どちらのアクセスも、発信元ポート 6000 が大半を占めていたが、逆に中国の発信元ポート 6000 から、今期、1521/TCP へのアクセスが急増しており、スキャン行為の対象を移行する過程で、2967/TCP 及び 135/TCP へのアクセスが一時的に減少した可能性も考えられる。

また、6 月 20 日以降、中国からの 1026/UDP、1027/UDP へのアクセスが途絶えており、今期の検知も 0 件であった。これも中国からのアクセスが減少した一因となっている。

日本については「Conficker」ワームの感染拡大が沈静化した事が原因と考えられる。

前期と比較して、検知件数の順位には変動はない。

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	114.66 件	−30.8%　(−51.09 件)		1 位
2 位	2 位	日本	73.94 件	−10.9%　(−9.07 件)		2 位
3 位	3 位	米国	23.99 件	−1.6%　(−0.38 件)		
4 位	4 位	ロシア	14.64 件	−3.1%　(−0.47 件)		
5 位	5 位	台湾	13.36 件	+8.8%　(+1.08 件)	2 位	
6 位	7 位	韓国	11.51 件	+22.1%　(+2.08 件)	1 位	
7 位	6 位	ブラジル	11.16 件	+8.0%　(+0.82 件)	3 位	
…			…			
9 位	12 位	アルゼンチン	5.62 件	+13.4%　(+0.66 件)	4 位	
…			…			
11 位	9 位	インド	5.45 件	−9.6%　(−0.58 件)		4 位
…			…			
23 位	18 位	トルコ	2.00 件	−26.7%　(−0.73 件)		3 位
…			…			
31 位	41 位	イスラエル	1.17 件	+58.7%　(+0.43 件)	5 位	
…			…			
74 位	42 位	ペルー	0.11 件	−83.9%　(−0.58 件)		5 位

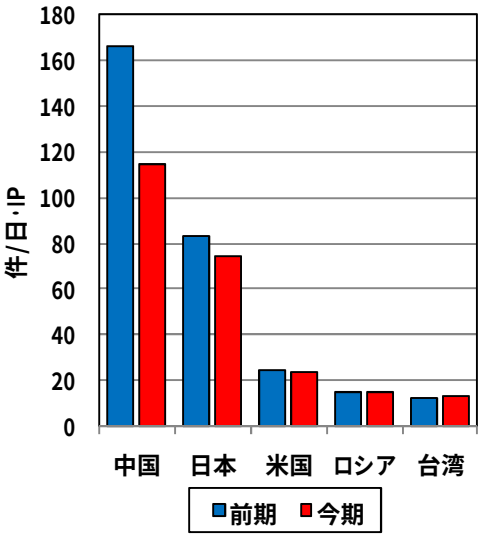

図 3-10 国／地域別検知件数の前期との比較(上位 5 カ国)

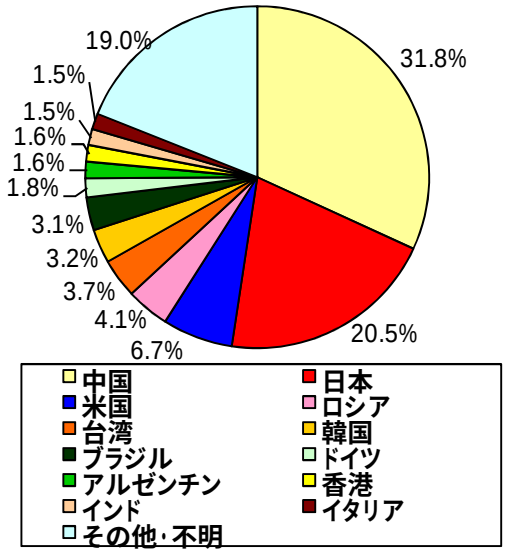

図 3-11 発信元国・地域別比率[†]

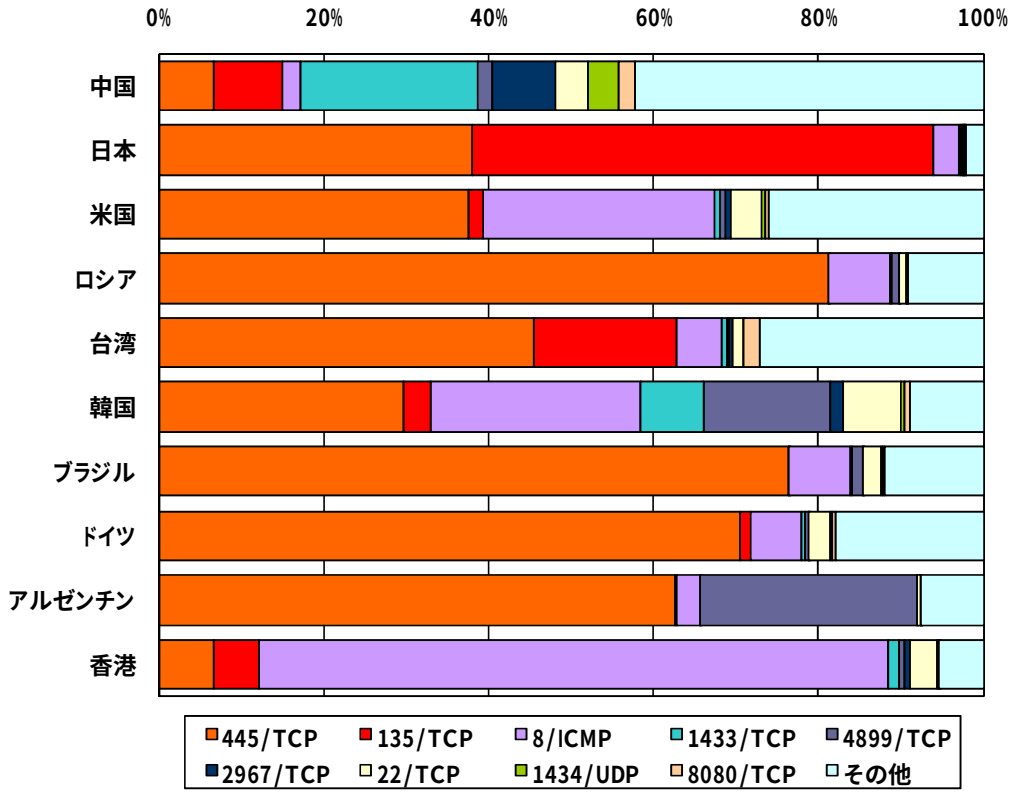

図 3-12 発信元国・地域別上位のポート別比率

[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。

(2) 推移

日本国内からのアクセスは、445/TCP に対するものが、前期と比較して 11.2 件減少しているが、今期中の推移としてはほぼ横ばいとなっており、「Conficker」ワームの感染拡大は沈静化したものの、依然として駆除されずに残っている状況がうかがえる。

米国からのアクセスでは、2 日から 5 日にかけて、「その他」の分類に属するポートでの増加がみられる。これは跳ね返りパケット を検知したものである。同じ時期、韓国や米国の主要官庁などのウェブサイトに対する大規模なサイバー攻撃が発生しており、その影響とみられる韓国からの跳ね返りパケットを観測している(「2-1 韓国・米国に対するサイバー攻撃」)。しかし、米国からの 2 日から 5 日の跳ね返りパケットについては、米国の攻撃対象とされるウェブサイトの IP アドレスからのものは含まれておらず、今回の大規模なサイバー攻撃との関連性は低いと思われる。

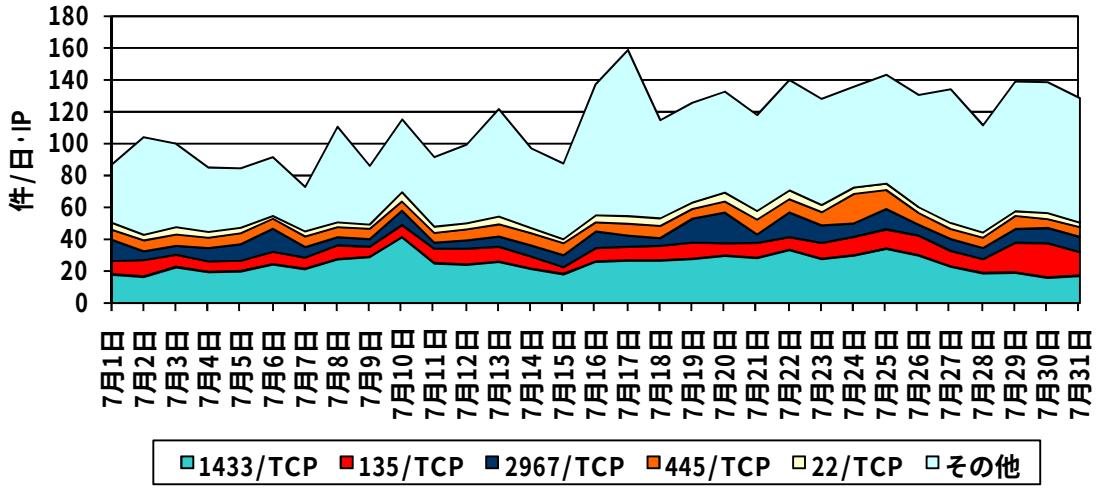

図 3-13 中国からのアクセスの推移

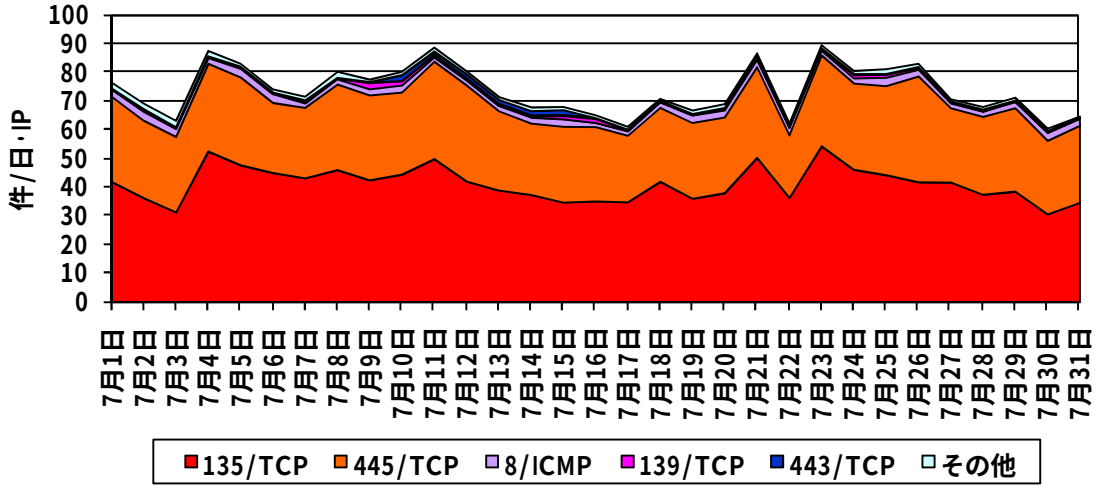

図 3-14 日本からのアクセスの推移

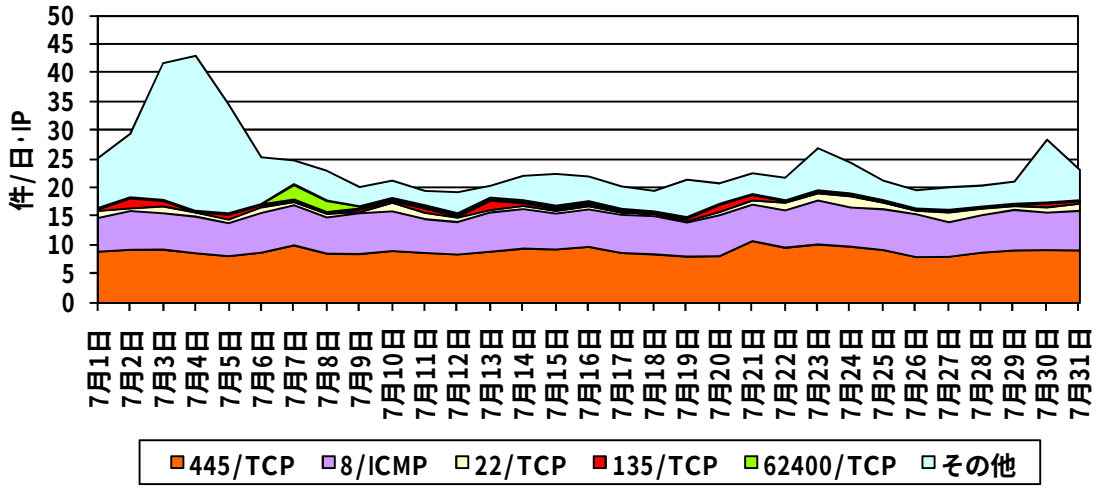

図 3-15 米国からのアクセスの推移

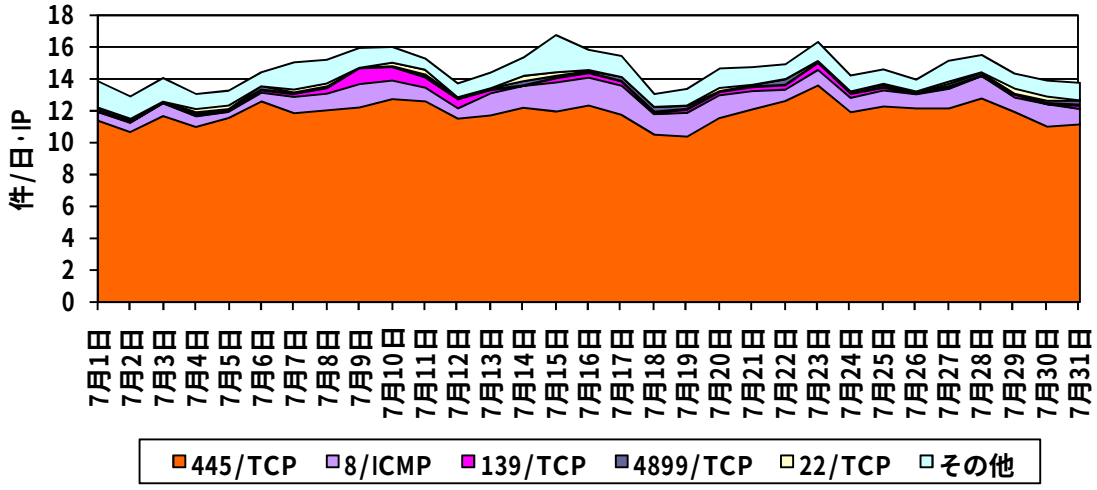

図 3-16 ロシアからのアクセスの推移

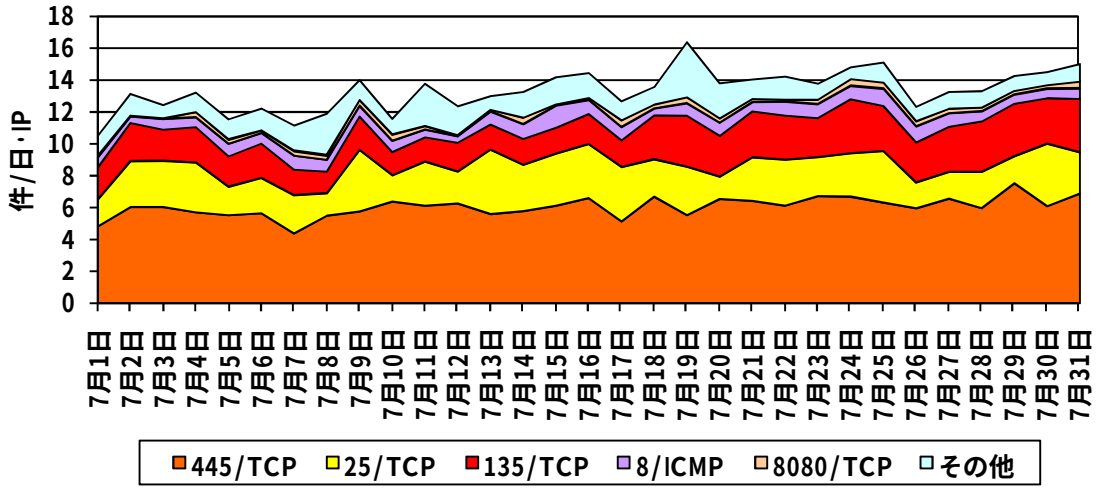

図 3-17 台湾からのアクセスの推移

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

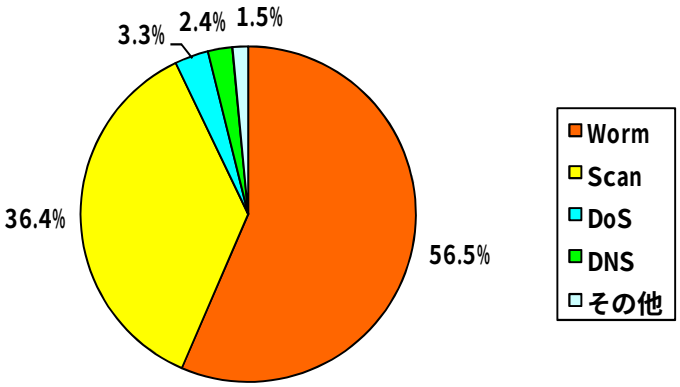

図 4-1　シグネチャを用いた不正侵入等の攻撃手法別検知比率[1]

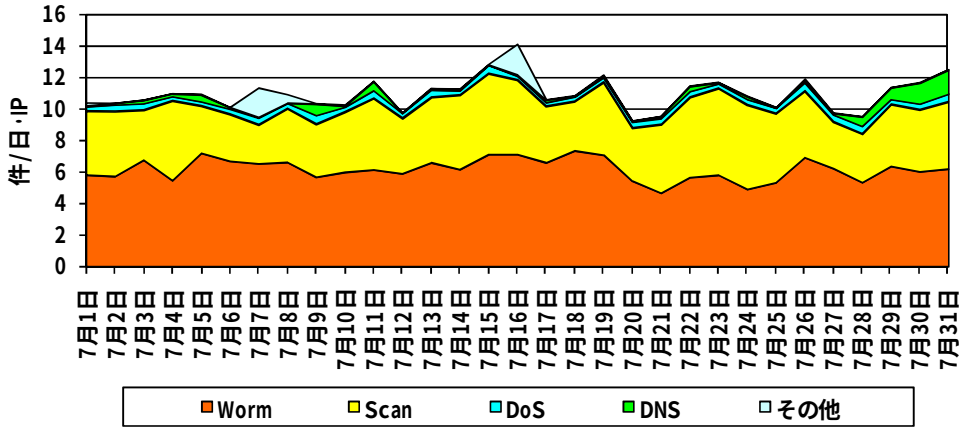

図 4-2　シグネチャを用いた不正侵入等の攻撃手法別検知推移

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 11.0 件で、前期と比較して－5.9 件（－34.8%）と減少した。これは UDP spam の検知が 6 月 20 日以降、ほぼなくなったことが主な原因である。UDP spam を除いた検知状況に大きな変化はない。

UDP spam は、送信を続けていた何者かが、一斉に送信を停止したか、何らかの理由で送信できなくなったものと考えられる[2]。

Worm の検知件数は緩やかな減少傾向が続いている。Worm の検知件数の約 3/4 が「SQL Slammer」ワーム、約 1/4 が「Nachi」ワームである。「SQL Slammer」ワームは緩やかな減少、「Nachi」ワームは極めて緩やかな減少が続いており、これらのワームの活動が徐々に沈静化している可能性がある。

[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。
[2] 平成21年上半期におけるインターネット治安情勢　http://www.cyberpolice.go.jp/detect/pdf/H21_kamihanki.pdf

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	6.19 件	−10.4% (−0.72 件)		2 位
2 位	2 位	Scan	3.99 件	−12.5% (−0.57 件)		3 位
3 位	5 位	DoS	0.36 件	+16.8% (+0.05 件)	1 位	
4 位	4 位	DNS	0.26 件	−47.3% (−0.23 件)		4 位
…			…			
−	3 位	UDP spam	検知なし	− (−4.36 件)		1 位

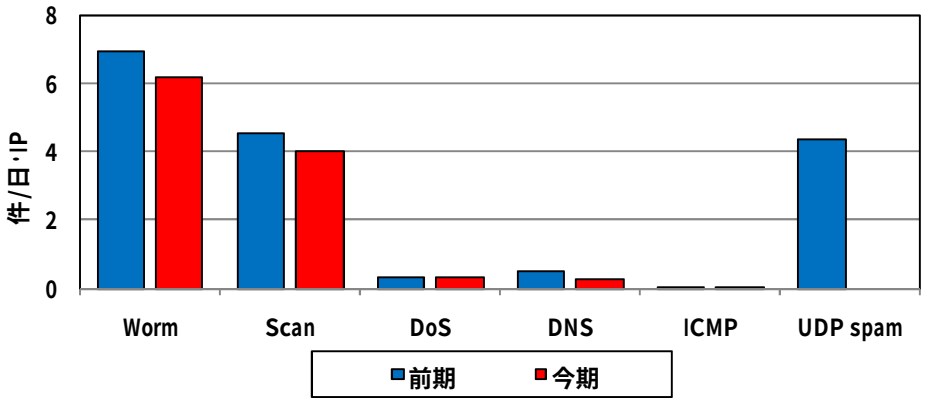

図 4-3 攻撃手法別検知件数の前期との比較(表 4-1 に関するもの)

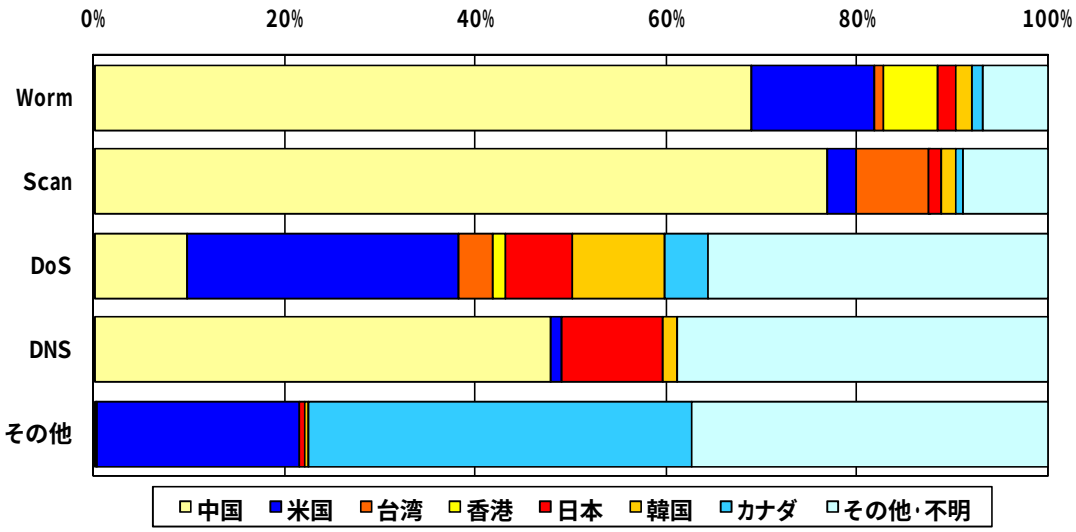

図 4-4 シグネチャを用いた不正侵入等の攻撃手法の国別比率

4-2　発信元国･地域別

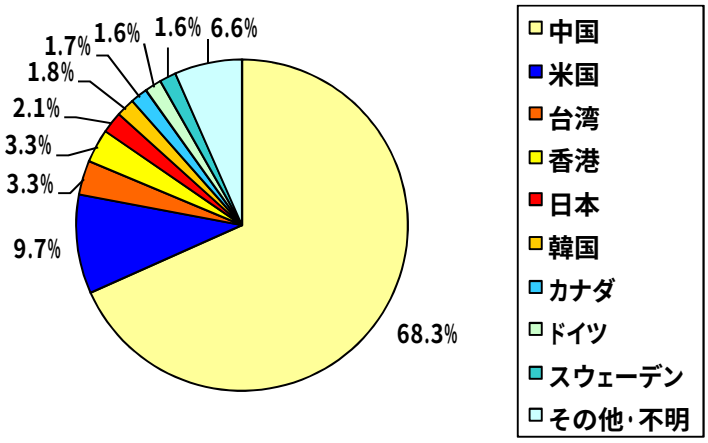

図 4-5　シグネチャを用いた不正侵入等の発信元国･地域別検知比率[1]

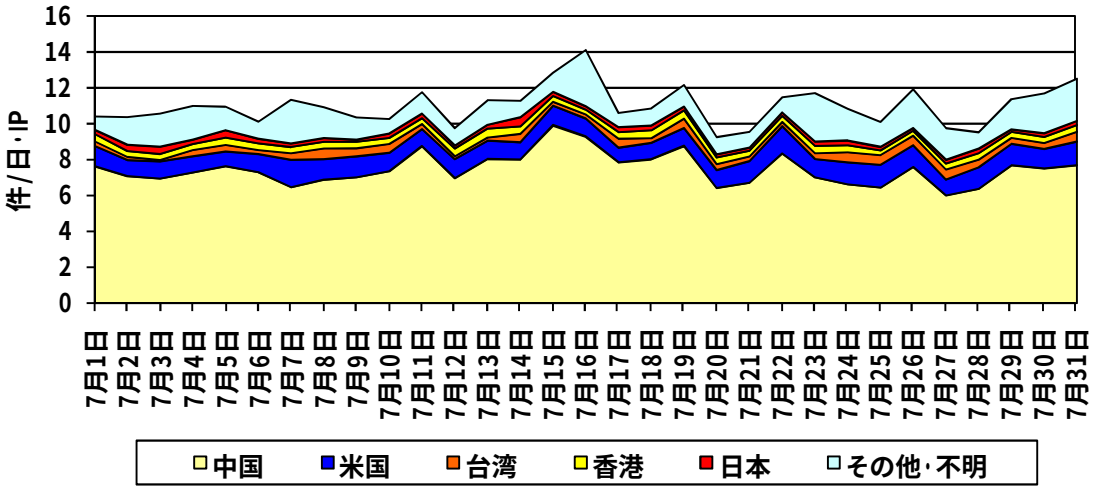

図 4-6　シグネチャを用いた不正侵入等の発信元国･地域別検知推移

今期は UDP spam の検知がなかったため、検知件数は前期に比べ減少した。特に、UDP spam の発信元の大半を占めていた中国の検知件数の減少が目立つ。

中国を発信元とする Worm の検知件数は「SQL Slammer」ワームが大半を占める。「SQL Slammer」ワームは複数の発信元から継続的に検知しており、管理が不十分なコンピュータが中国に存在することが考えられる。

米国及び日本を発信元とする Worm の検知件数は「Nachi」ワームが多く、米国では Worm の検知のうち 87.8%、日本では 89.5%を占めている。「Nachi」ワームの検知件数は、米国では緩やかな減少傾向にあるが、日本では、新システムで観測を始めた 3 月以降、横ばいとなっており、全国的な減少傾向は、国内よりも海外における減少が要因と考えられる。

[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	前期比	今期増加順位	今期減少順位
1 位	1 位	中国	7.48 件	−42.1% (−5.45 件)		1 位
2 位	2 位	米国	1.06 件	−12.6% (−0.15 件)		3 位
3 位	4 位	台湾	0.37 件	−2.7% (−0.01 件)		
4 位	5 位	香港	0.36 件	+7.3% (+0.02 件)	3 位	
5 位	6 位	日本	0.23 件	−14.8% (−0.04 件)		4 位
…			…			
7 位	7 位	カナダ	0.18 件	−16.8% (−0.04 件)		5 位
8 位	3 位	ドイツ	0.18 件	−54.3% (−0.21 件)		2 位
9 位	9 位	スウェーデン	0.18 件	+13.8% (+0.02 件)	4 位	
10 位	16 位	ブラジル	0.08 件	+160.8% (+0.05 件)	2 位	
11 位	33 位	メキシコ	0.07 件	+678.3% (+0.06 件)	1 位	
…			…			
17 位	27 位	イタリア	0.03 件	+131.7% (+0.02 件)	5 位	

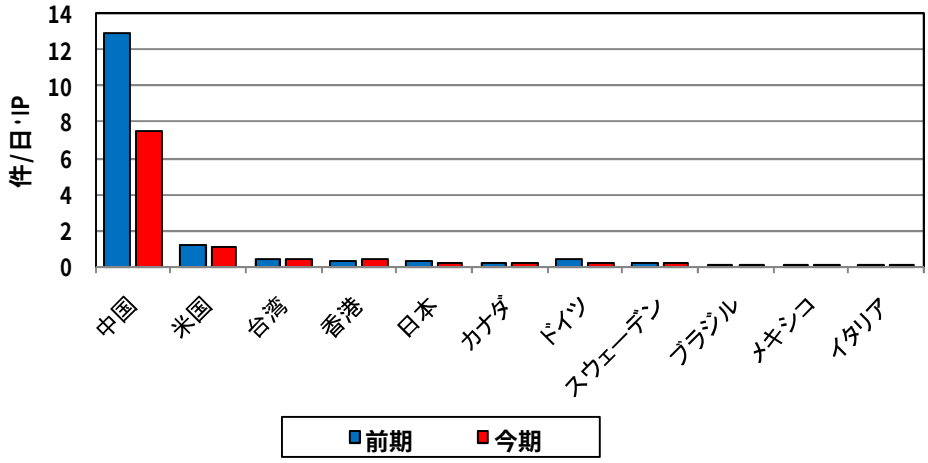

図 4-7 発信元国･地域別検知件数の前期との比較(表 4-2 に関するもの)

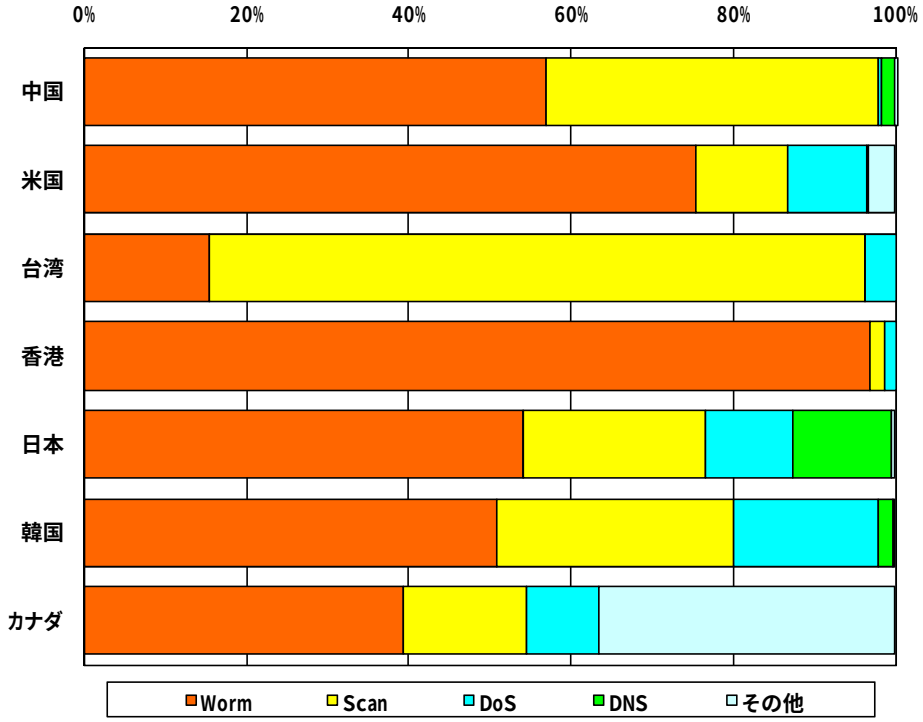

図 4-8 シグネチャを用いた不正侵入等の発信元国･地域別上位のシグネチャ別比率

5 @police (Topics)掲載事項

@police において 7 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 5 月報を追加)(7/7)
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 (MS09-028,029,030,031,032,033)(7/15)
●	DoS 攻撃機能を備えたウイルス（Mydoom 亜種）の概要について(7/21)
●	DoS 攻撃機能を備えたウイルス（Mydoom 亜種）の概要について（更新）(7/28)
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 (MS09-034,035)(7/29)

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 7 月 31 日現在、シグネチャは 2,886 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