

我が国におけるインターネット治安情勢の分析について (平成 15 年度 12 月期)

1 概要

サイバーフォースセンターの 24 時間監視体制

- 全国の警察施設に対するサイバー攻撃の監視

サイバーフォースセンターでは、全国の警察施設のインターネット接続点において、侵入検知装置 (Intrusion Detection System: IDS) 及びファイアウォールによる攻撃の監視を行っている。

インターネット治安情勢の分析

- 平成 15 年度 12 月期分のデータによる。(IDS 及びファイアウォールのログ)

2 侵入検知装置分析結果に見る特徴

アラートの検知件数及び検知ホスト数は減少

当月期におけるアラートの検知件数は 32,766 件、検知ホスト数 9,930 件であり、11 月期と比較すると検知件数は約 3,300 件、検知ホスト数は約 703 件減少した。

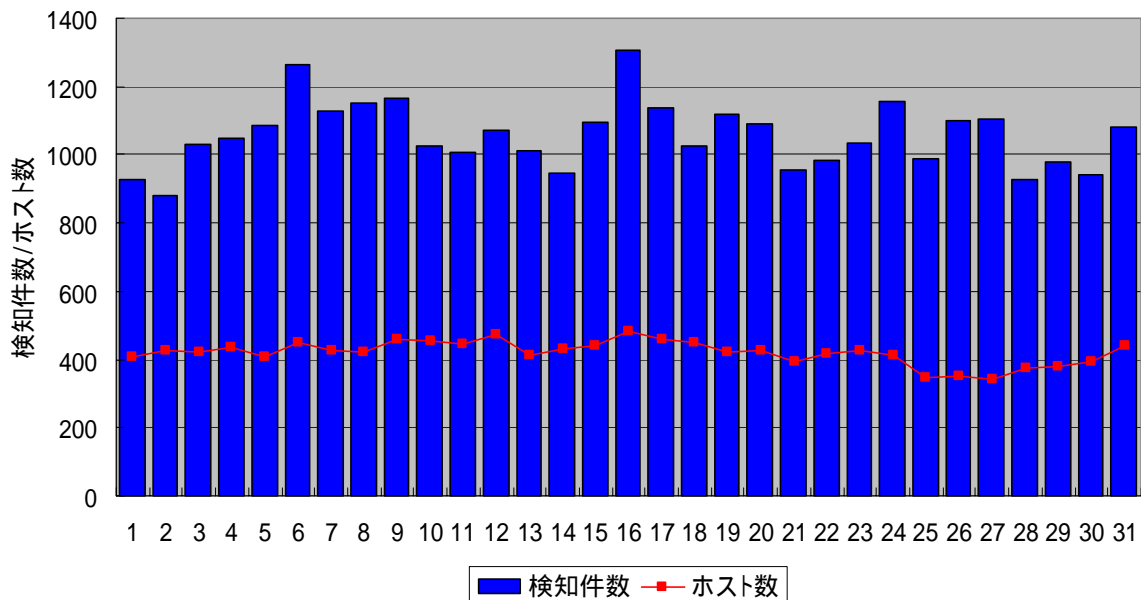


図 1 12 月期における攻撃状況の推移

中国及び日本からの攻撃が増加

検知されたアラート情報の発信元国別での分類を図 2 に示す。

11 月期に上位を占めていた国の大多数で検知件数が減少しているが、中国及び日本からの攻撃のみ検知件数が増加している。これは、中国及び日本からのワーム関連の攻撃の増加によるものである。

逆に検知件数が減少した国では、スキャン系又はワーム系の攻撃の検知件数が減少している。

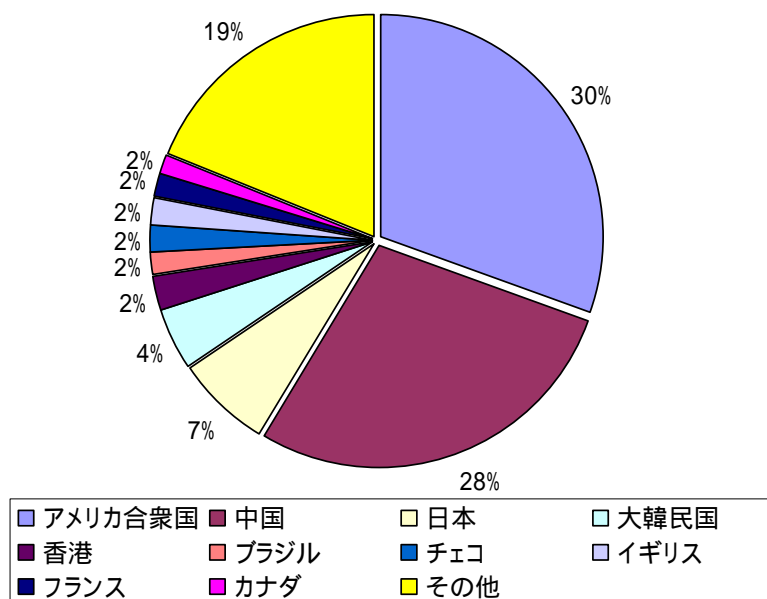


図 2 攻撃発信元の国別分析

チェコに関しては「Window size of 55808(SYN) TCP Packet」の占める割合が約 90%であり、「Stumbler」や「Randex.C」などによる影響も考えられ、送信元 IP アドレスを詐称している可能性が高い。

ワームの割合がやや増加

11月期と比較するとWormの割合がやや増加し、Scanの割合が減少している他はほとんど変化が見られない。

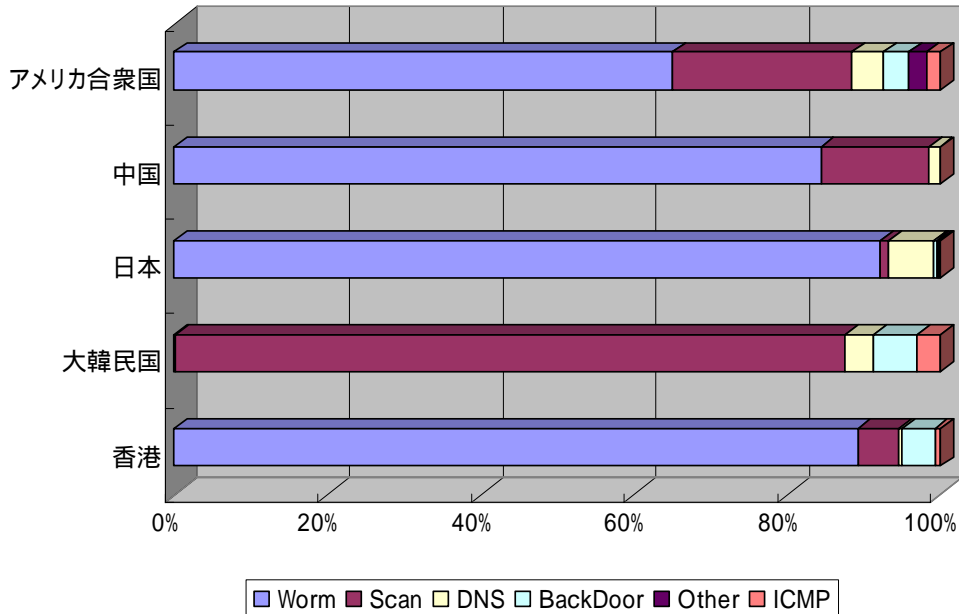


図3 国別攻撃手法

12月期に検知した主な攻撃の分類

大分類	アラート内容	大分類	アラート内容
BackDoor	IP Unknown Protocol	ICMP	PING NMAP
	Back Orifice2000		redirect host
	Sub7 v2.2 probe		redirect net
Portscan Detection Attack	superscan echo		
Scan	Proxy attempt	Worm	SQL SLAMMER worm
	SYN FIN scan	Other	Traceroute サービスの検出
	synscan portscan		IPFragmentation
	Window size of 55808(SYN) TCP Packet		Linux Traceroute
	Window size of 55808 TCP Packet		
DnS	named version attempt		
	DNS Hostname Overflow Attack		
	DNS HINFOデコード		

攻撃手法による分析

図 4 に攻撃手法別の検知件数比を示す。

当月期は「Scan」の割合が減少し「ワーム」の割合が増加しており、依然として「ワーム」による攻撃が全体の 2/3 以上を占める結果となった。

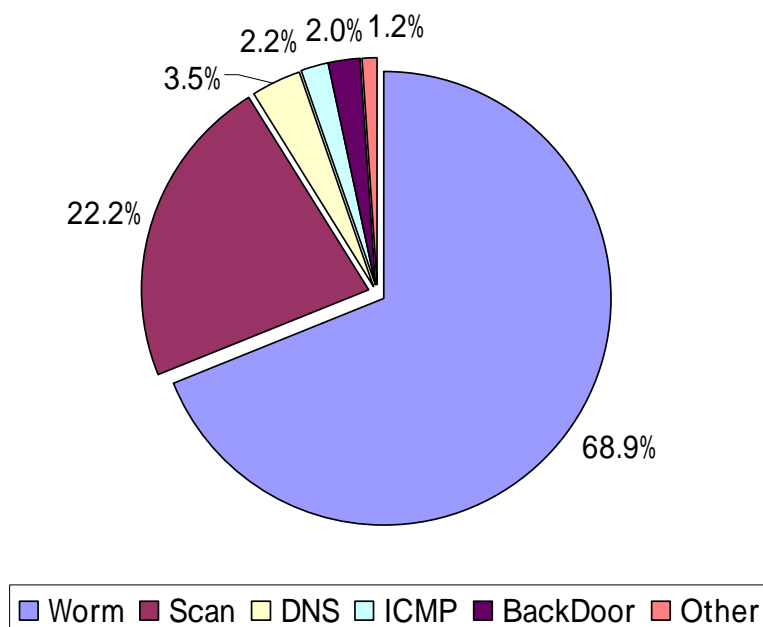


図 4 攻撃手法別検知件数比

地域別の攻撃の時間的推移

図 5 に検知件数の多い西ヨーロッパ、東アジア及び北アメリカの 3 地域における時間帯別検知状況を示す。なお、時間は次のとおり現地時間に近い時間帯に補正したものである。西ヨーロッパ：GMT、東アジア：JST (GMT + 9:00)、北アメリカ：CST (GMT - 6:00)

西ヨーロッパ地域及び東アジア地域では、深夜時間帯の攻撃は少なくなっている。

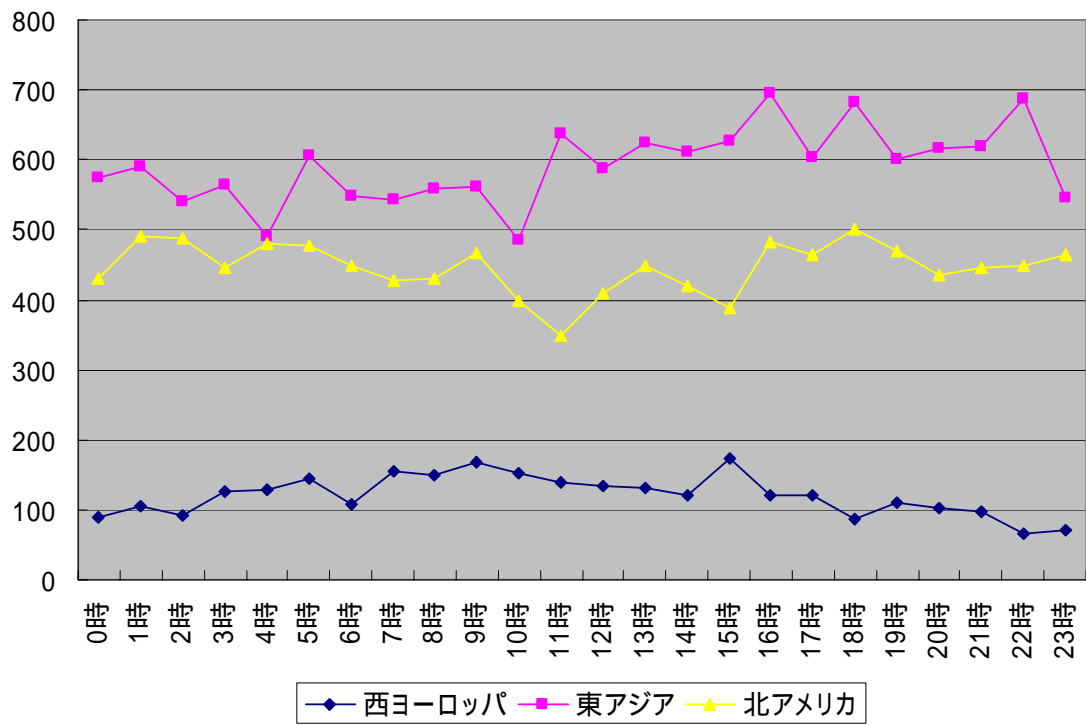


図5 西ヨーロッパ、東アジア、北アメリカの時間帯別検地件数

3 ファイアウォールログ分析結果に見る特徴

総アクセス件数は、僅かに減少

当月期における総アクセス件数は5,283,584件(平均約170,438件/日)で、前月比約1.3%(約7万件)減となった。これは、ICMPの件数が約2%減少(約10万件)したものであり、ICMPを除いた他のポートへのアクセス件数は約3万件の増加となっている。

当月期の発信元の国別件数比率を図6に示す。若干順位の変動はあるものの中国がICMPの減少により、前月比29%減となった以外は、上位国の大勢は変わらない。

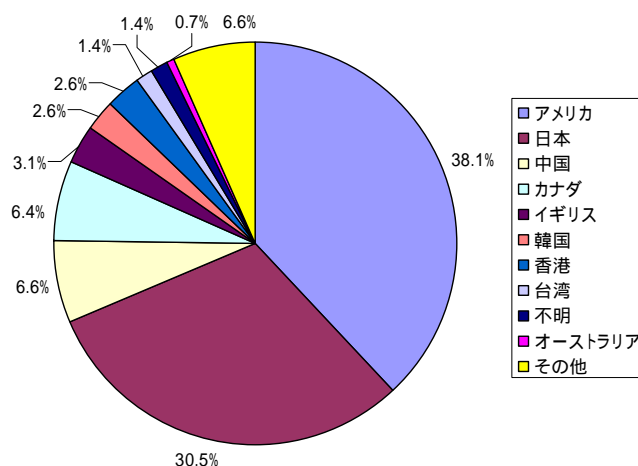


図6 国別件数の比率

国毎のポート別比率

上位5か国の宛先ポート番号別比率を図7に示す。当月も、前月に引き続き、WelchiaワームによるとみられるICMP、BlasterによるとみられるTCP135番ポートへのアクセスを大量に検出している。また、国内からは、依然としてTCP135番ポートへのアクセスが多い。中国は、その他が約40%を占めているが、これは広範囲なポート番号へのアクセスが多いためである。なお、8月に発生したWelchiaワームは、2004年1月1日以降に起動された場合に活動を停止する機能が組み込まれていることから、ICMPの件数は、今後減少していくと考えられる。

注) 当月報作成時点は、すでにICMPは、1月1日以降大きく減少している。詳細は、「年末年始におけるワームの活動状況について」(平成16年1月6日付け)を参照。

(@police http://www.cyberpolice.go.jp/detect/pdf/H160106_worm.pdf)

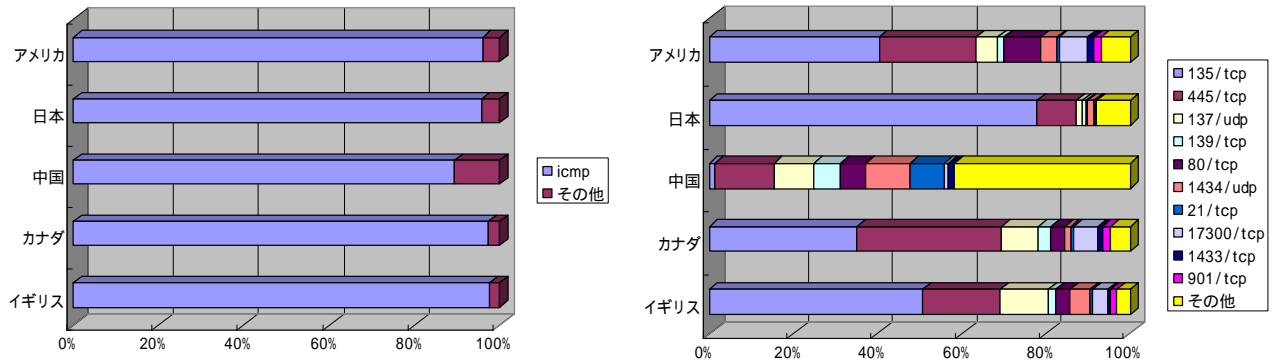


図7 上位5カ国宛先ポート番号別比率（右図はICMPを除外）

ポート別比率及びポート毎の国別比率

当月期の宛先ポート番号別比率を図8、宛先ポート番号毎の発信元国別比率を図9に示す。ICMPを除いたポート番号別比率では、Blasterワームが使用するTCP135番ポート、Windows系OSのファイル共有で 사용되는UDP137番、TCP139番、TCP445番ポートへのアクセス件数が多く、全体の72%を占めている。また、前月から増加したTCP139番ポートの件数は、当月は前月比約11%減となっているが、韓国からのアクセスは逆に増加しており前月比約22%増、占める割合も56%となっている。

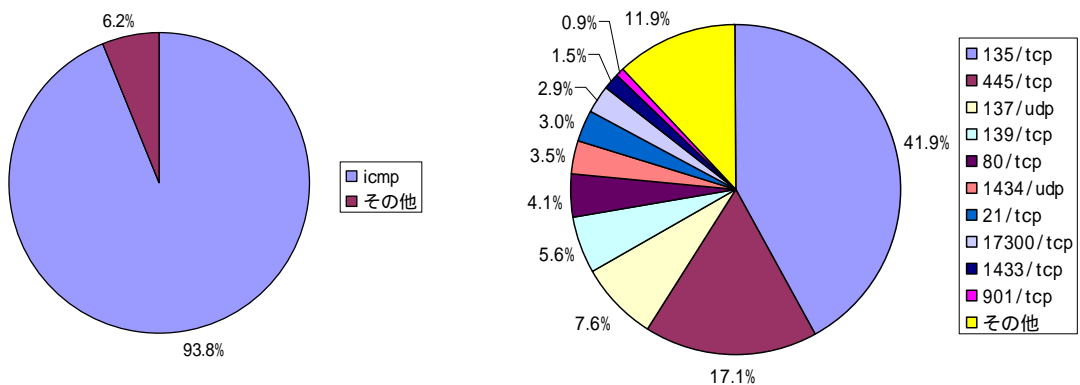


図8 宛先ポート番号別比率（右図はICMPを除外）

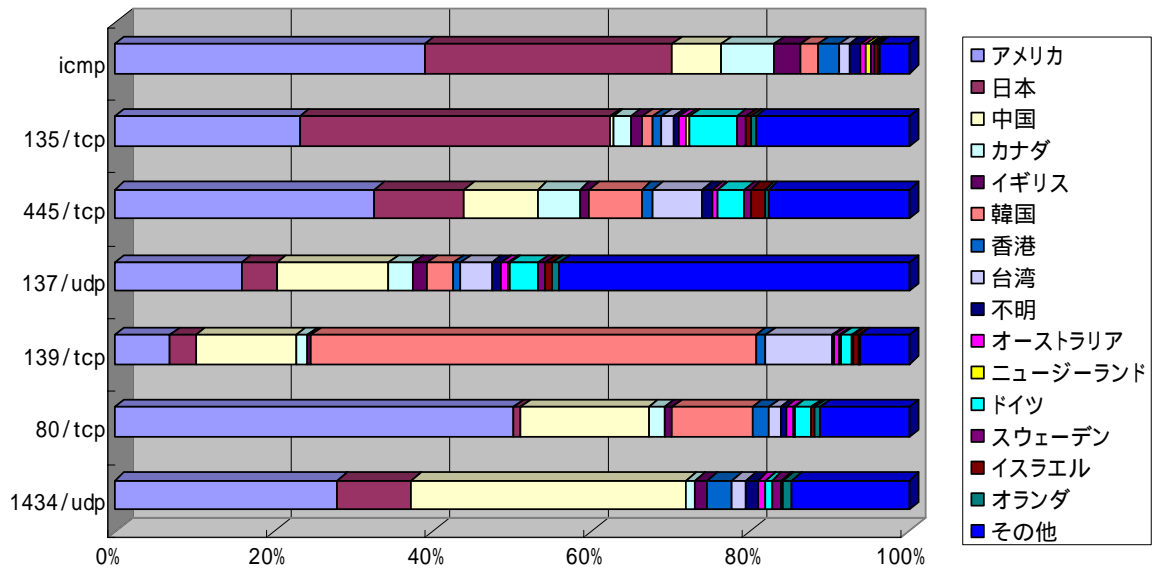


図 9 宛先ポート番号毎の発信元国別比率

ポート別及び国別件数の推移

主要な宛先ポート番号へのアクセス件数の推移を図 10、発信元国別推移を図 11、図 12 に示す。

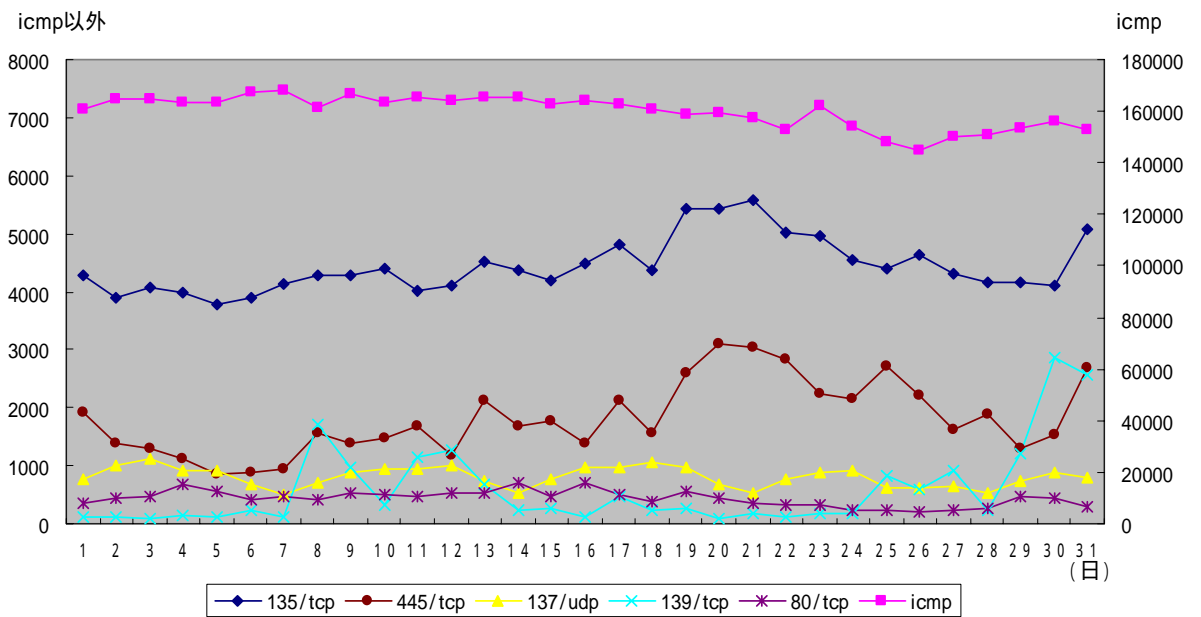


図 10 主要な宛先ポート番号へのアクセス件数の推移

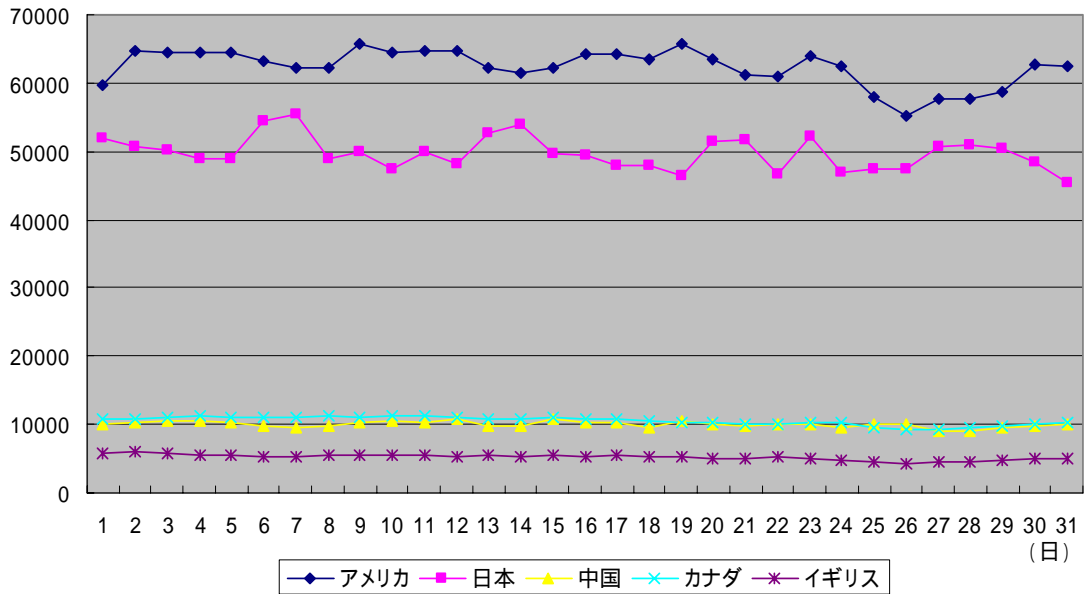


図 11 ICMP の国別件数の推移

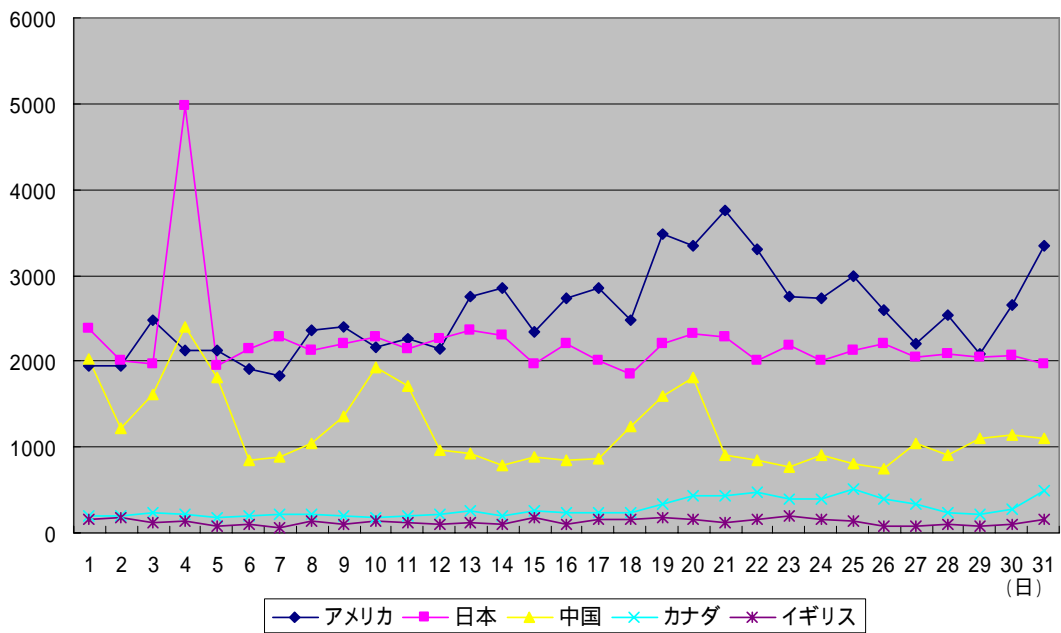


図 12 国別件数の推移 (ICMP は除外)

4日に、日本の件数が一時的に増加しているのは、日本国内のプロバイダのユーザに使用されていると考えられるIPアドレスからひとつの拠点に対してポートスキャンが行われたためである。

トラフィックの特異動向と@police 上の注意喚起

当月、特異な動きがあったトラフィックについてポート番号別にグラフ化したものを図 13,14,15 に示す。増加傾向を示したトラフィックについては、@police 上で注意喚起を行った。

TCP139 番ポートへのアクセス件数は、8 日頃から増加し、13 日には通常のトラフィックにもどったが、29 日頃から再度増加した。なお、この増加の主な発信元は韓国となっている。

@police 「TCP139 番ポートに対するトラフィックの増加について」

http://www.cyberpolice.go.jp/detect/pdf/H151211_139.pdf

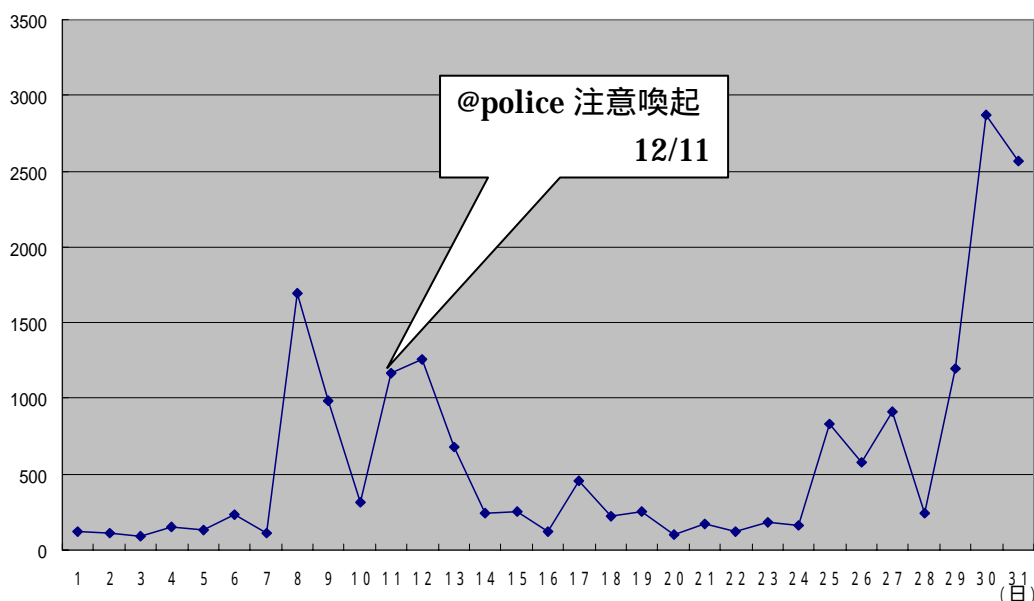


図 13 139/tcp アクセス件数の推移

10 月頃から増加した UDP53 番ポートへのアクセスは、依然として、当月も検知されており、Sinit と呼ばれるトロイの木馬の活動と考えられている。

@police 「UDP53 番ポートに対するトラフィックの増加について」

<http://www.cyberpolice.go.jp/detect/pdf/H151216udp53.pdf>

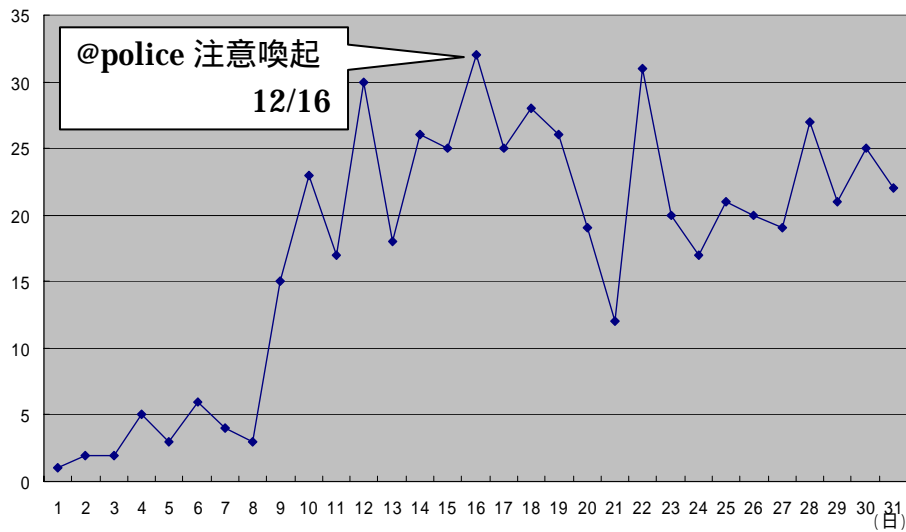


図 14 53/udp アクセス件数の推移

リモート管理ツールである「DameWare Mini Remote Control」の脆弱性が当月公開され、このツールで使用される TCP6129 番ポートへのアクセスの増加がセキュリティサイト「incidents.org」(<http://isc.incidents.org/diary.html?date=2003-12-21>)で報告されているが、当ネットワークにおいても、20日から、このポートへのアクセスが検知され始め、以後除々に増加してきている。発信元は、アメリカ、中国、韓国が多い。

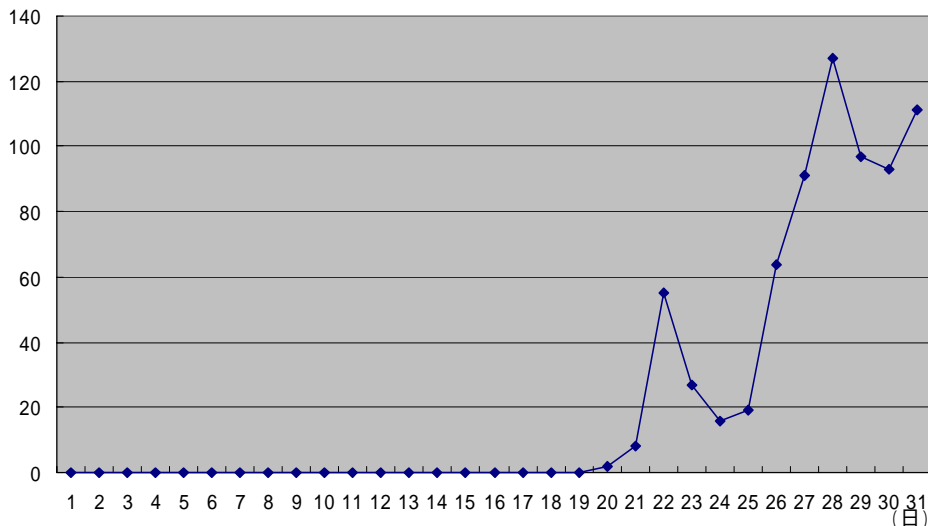


図 15 6129/tcp アクセス件数の推移

4 おわりに

当月期の特徴は、侵入検知装置におけるアラートの総検知件数が減少した反面、中国及び日本を発信元とする SQL Slammer ワームが増加したことである。また、ファイアウォールのログにおいては、依然、ICMP 及び TCP135 番ポートへのアクセスが多く検出されている。そのほか、TCP139 番及び TCP445 番ポートへのアクセスが散発的に増減を繰り返しており、UDP137 番も含めて、主に Windows 系 OS のファイル共有等で使用されているポートへのアクセスが多くなっていることから、引き続き動向に注視する必要がある。なお、沈静化の兆しが見えない Slammer 及び Blaster ワームについては、当月 22 日、「国内の Slammer 及び Blaster ワームの感染活動に関する IP アドレス管理者への注意喚起について」(@police http://www.cyberpolice.go.jp/detect/pdf/H151222_worm.pdf) に示したとおり、当ネットワークで検知したデータをもとに、各都道府県警察を通じて、国内の IP アドレス管理者に対し注意喚起を行った。