

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 3 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 3 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が増加

当月期におけるアラートの検知件数は 47,293 件、検知ホスト数 13,212 件であり、2 月期と比較すると検知件数は約 11.0%(4,640 件) 増、検知ホスト数は約 9.3%(1,127 件) 増となった。図 1 のグラフを見ると検知件数が若干減りつつある。これは中国を発信元とする「SQL Slammer Worm」が減少しつつあるからである。

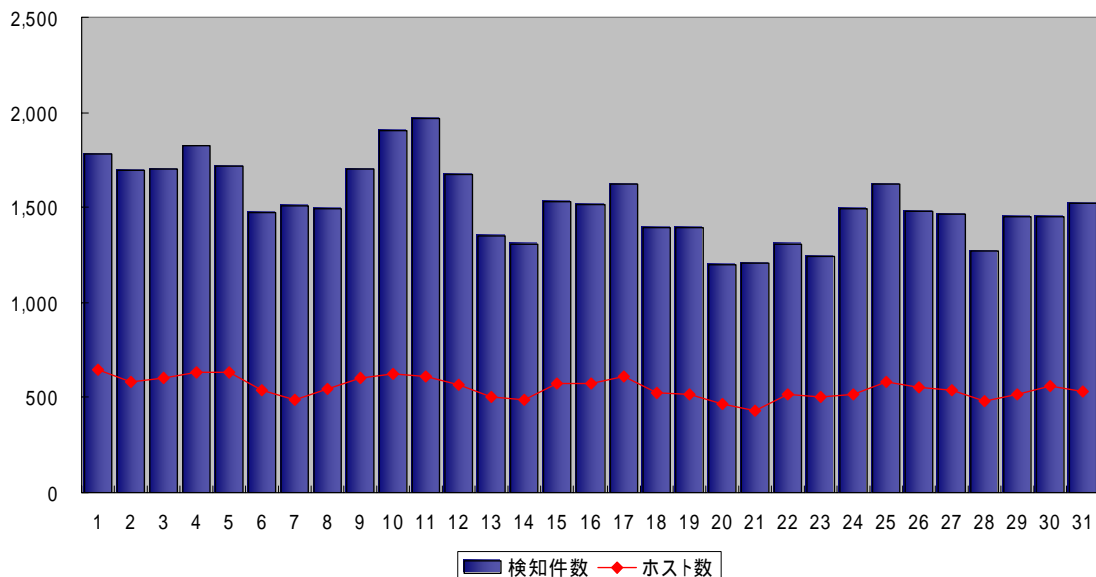


図 1 3 月期における攻撃状況の推移

主要国の Worm 系アラートが増加

検知されたアラート情報の発信元国別・地域別での分類を図2に示す。

当月は、Worm 系アラート (SQL Slammer Worm) 以外のアラートが減少しており、特にアメリカを発信元とする BackDoor 系アラート (Sub7 v2.2 probe) Scan 系アラート (Proxy attempt) の減少が目立つ。また、主要国における Worm 系アラート (SQL Slammer Worm) の検知件数が増加傾向にある。特に中国を送信元とする「SQL Slammer worm」が先月に引き続き急増しており、検知ホスト数及び検知件数を前月と比較すると、それぞれ約 12% (89 ホスト)、約 28% (3,516 件) 増加している。

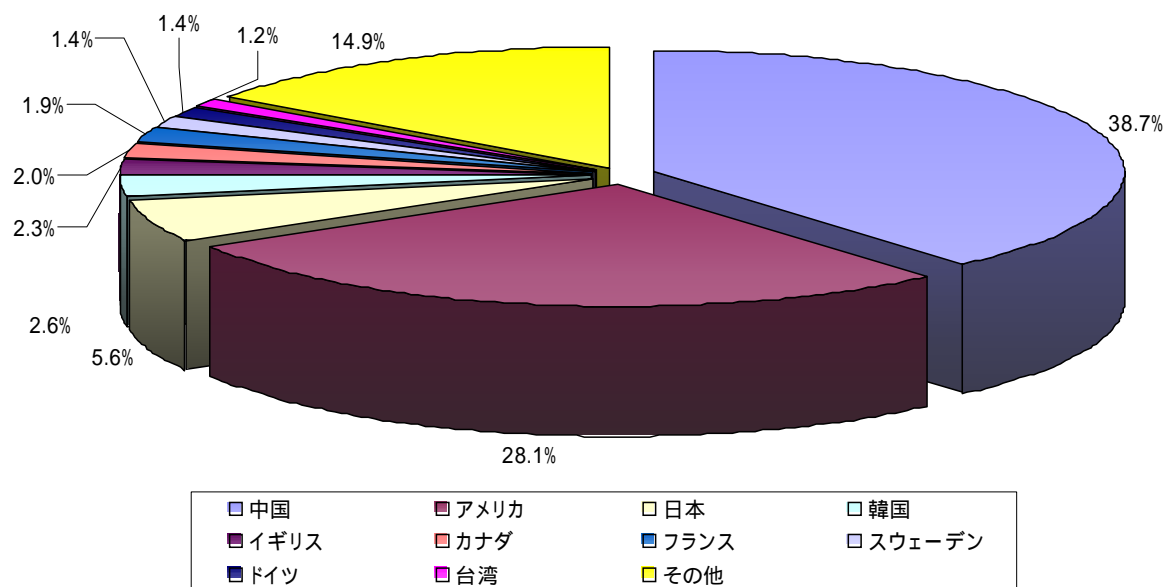


図2 攻撃発信元の発信元・国別・地域別分析

攻撃手法の国別・地域別特徴

中国、アメリカおよび日本の Worm 系アラート (SQL SLAMMER worm)、韓国の Scan 系アラート (Proxy attempt) の割合が前月と比べそれぞれ増加している。それ以外は、前月とほぼ同じ傾向である。また、韓国の Worm 系 (SQL Slammer worm) の検知比率が著しく低いのが見て取れる。原因は不明だが、韓国が何らかの対策をとっているのではないかと考えられる。

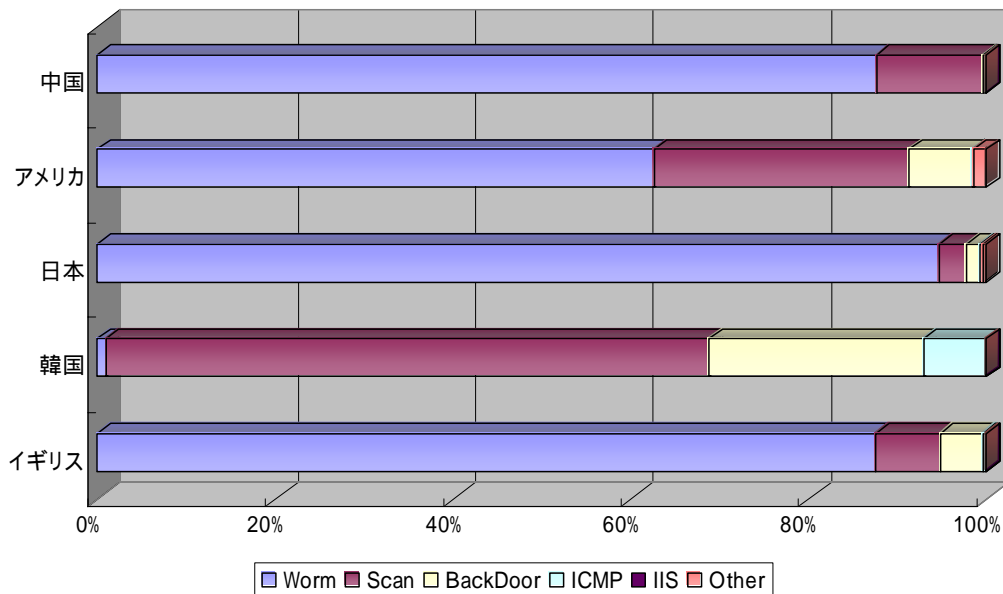


図3 国別・地域別攻撃手法

3 月期に検知した主な攻撃の分類

大分類	アラート	大分類	アラート
BackDoor	BACKDOOR hack-a-tack attempt	ICMP	redirect host
	BackOrifice2000		redirect net
	Sinit Discovery Packet		superscan echo
	Sub7 v2 2 probe		ICMP Traceroute
Scan	nmap TCP	Worm	SQL SLAMMER worm
	Portscan Detection Attack	IIS	WEB-IIS ISAPI_ida(idq.htx) access
	synscan portscan	Other	Bind 4 nslookupComplain Format bug
	Window size of 55808 TCP Packet		Linux Traceroute
	Window size of 55808(SYN) TCP Packet		Traceroute サービスの検出
Proxy attempt	IP Fragmentation		
			MIME Header Attachment

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。

当月期は主要国からの「SQL Slammer worm」の検知件数が増加し、「SQL Slammer worm」以外のアラートの検知件数が減少したので、Worm 系アラートの占める割合が増加し、前月が約 62%であったのに対し、今月は約 75%となっている。

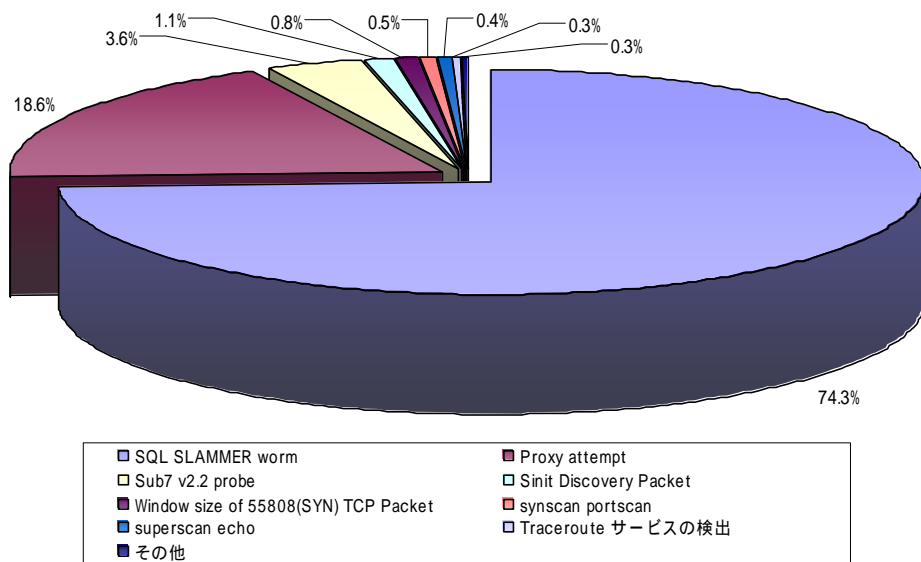


図 4 攻撃手法別検知件数比

3 ファイアウォールログ分析結果に見る特徴

総アクセス件数が減少

当月期の国別・地域別件数の比率を図 5 に示す。当月期は前月期と比較して総アクセス件数が約 6 万件増加した。上位 10 カ国の顔ぶれは前月とまったく変わらない。変化があったのは、日本とアメリカの順位が入れ替わったことである。原因としては、前月中旬に発生した Welchia.B ワームにより国内からの TCP135 番ポートと TCP445 番ポートが増加し、アメリカからの Welchia ワームと思われる ICMP のアクセス数が減少したためである。

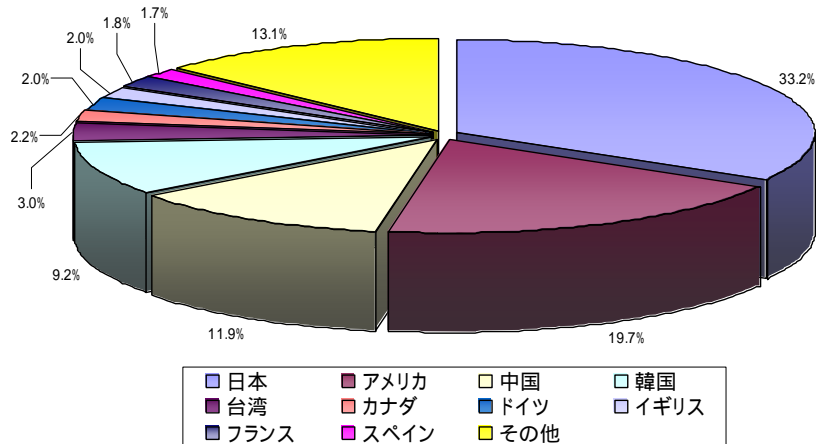


図 5 国別・地域別検知件数比

国毎のポート別比率

上位 5 ケ国の宛先ポート番号別比率を図 6 に示す。当月期は、前月発生した Welchia.B の影響により TCP135 番ポート、TCP445 番ポートの占める割合が高くなっている。また、韓国からの TCP1025 番ポート、TCP6129 番ポートの割合が高いのは、Gaobot ワームの亜種による感染活動が原因と推測される。

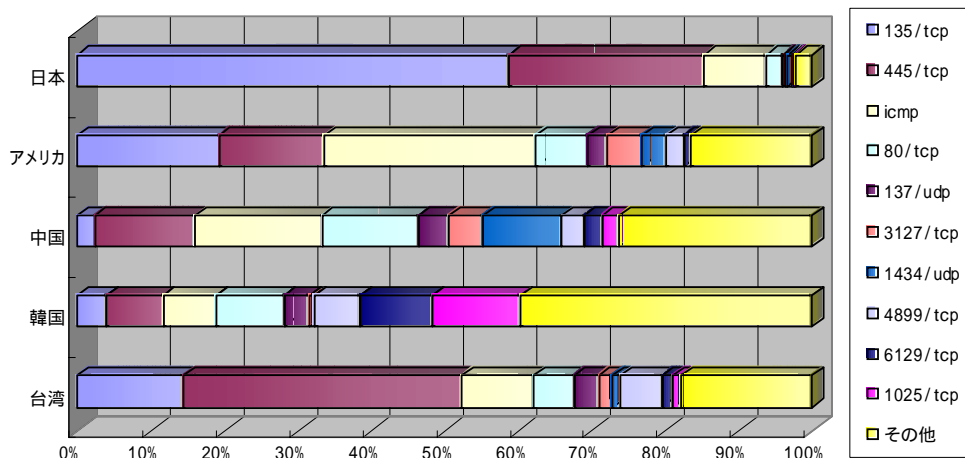


図 6 上位 5 ケ国宛先ポート番号別比率

宛先ポート別比率及びポート毎の国別・地域別比率

当月期の宛先ポート番号別比率を図 7、宛先ポート番号別の発信元国別・地域別比率を図 8 に示す。ICMP が先月の約 30%から約 15%と半分の値となっている。その他のポートでは、Blaster ワームと Welchia.B ワームが使用する TCP135 番ポート、Welchia.B ワームが使用する TCP445 番ポート、TCP80 番ポートへのアクセスの総数が全体の約半分を占めている。また、前月期は Mydoom.A の発生により当該ワームがバックドアとして使用する TCP3127 番ポートの割合が増加していたが今月に入り減少傾向にある。今月期、新たに増加してきた TCP4899 番ポートは Famatech 社の「Radmin」で使用されるポートであり、同ソフトウェアにおける脆弱性や脆弱な設定を標的としたアクセスであると推測される。それ以外のポートについては、前月期とほぼ同じ傾向にある。

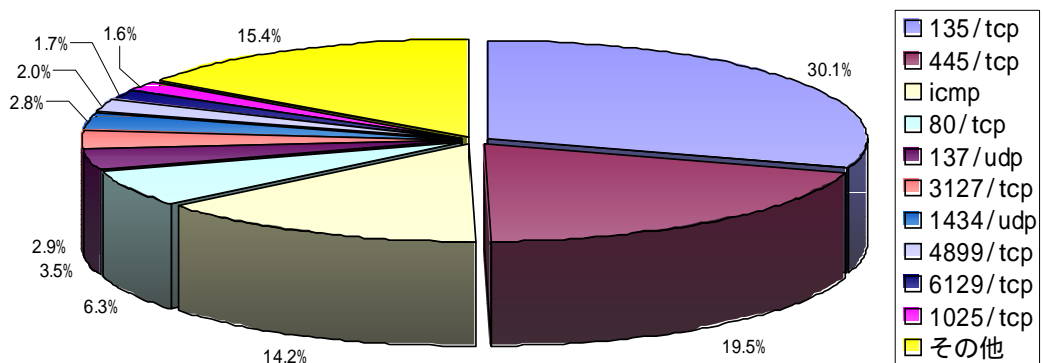


図 7 宛先ポート番号別比率

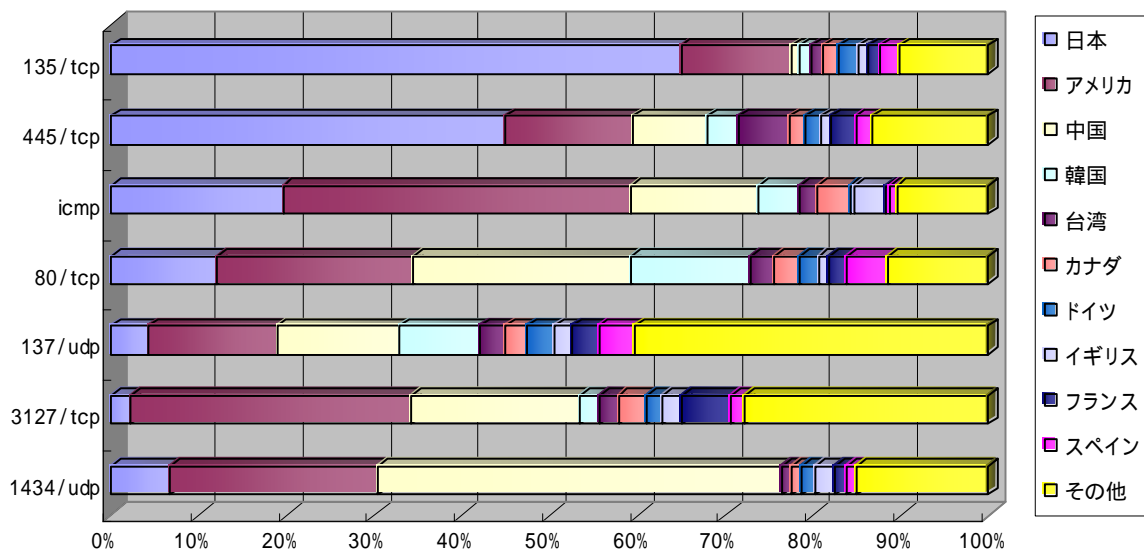


図 8 宛先ポート番号毎の国別・地域別比率

ポート別及び国別・地域別検知件数の推移

主要な宛先ポート番号別のアクセス件数の推移を図9に、発信元国別・地域別のアクセス件数の推移を図10に示す。

3月31日にその他のアクセス件数が急増している原因は、特定のIPアドレスを発信元とするポートスキャンのためである。

また、3月23日、24日におけるその他のアクセス数の増加は、Windowsのメッセンジャサービスを利用したスパム広告が使用するUDP1026番ポート、UDP1027番ポートに対するアクセス数によるものである。国別・地域別で見ると韓国を発信元とするアクセスが多い。(図10参照)

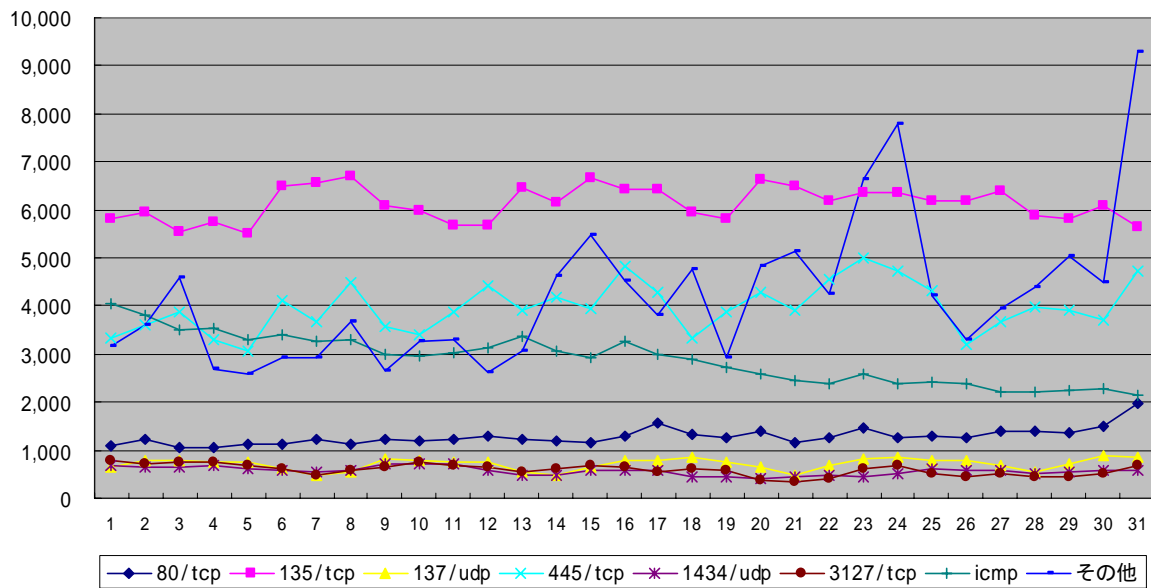


図9 主要な宛先ポート番号別検知件数の推移(1日単位)

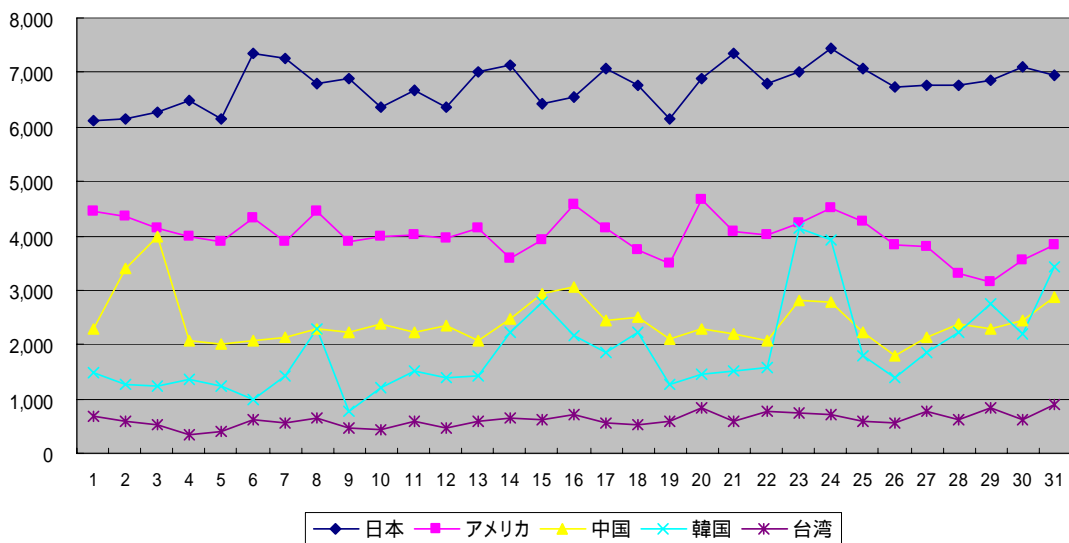


図10 発信元・国別・地域別検知件数の推移

トラフィックの特異動向

当月期に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 11～12 に示す。

3 月期中に観測された特異なアクセス状況について図 11～図 12 に示す。

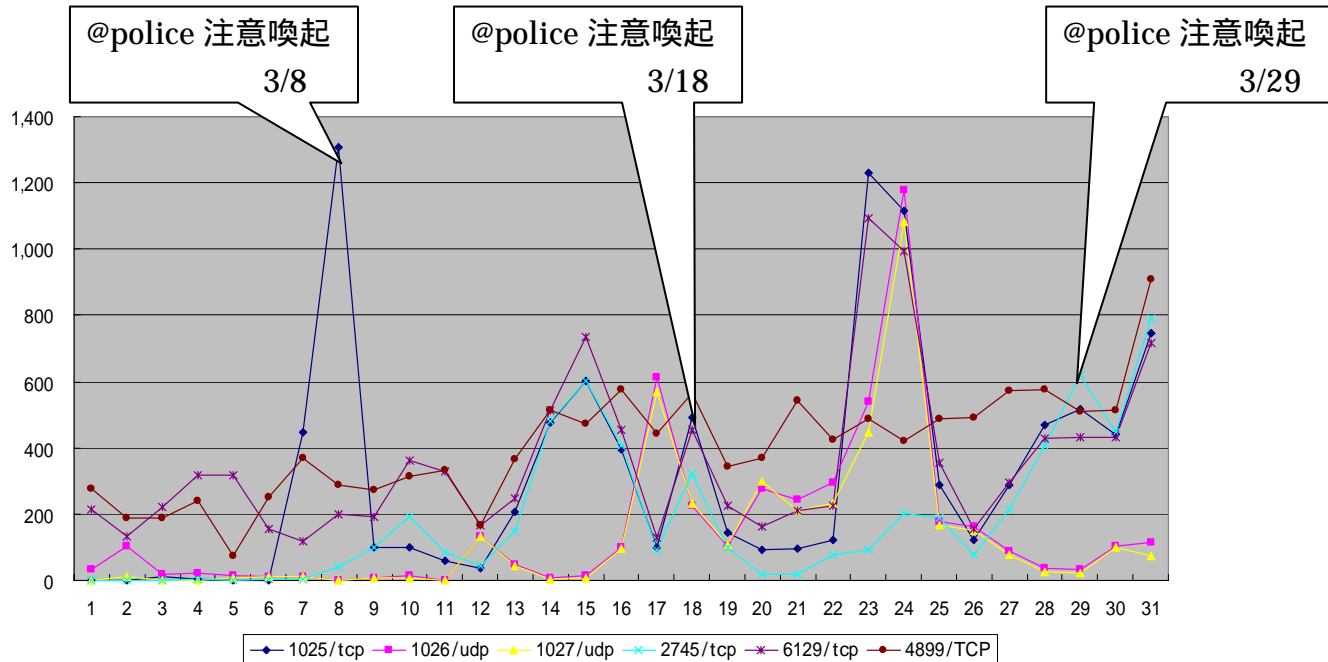


図 11 特異な動きのあったポートへのアクセス件数の推移

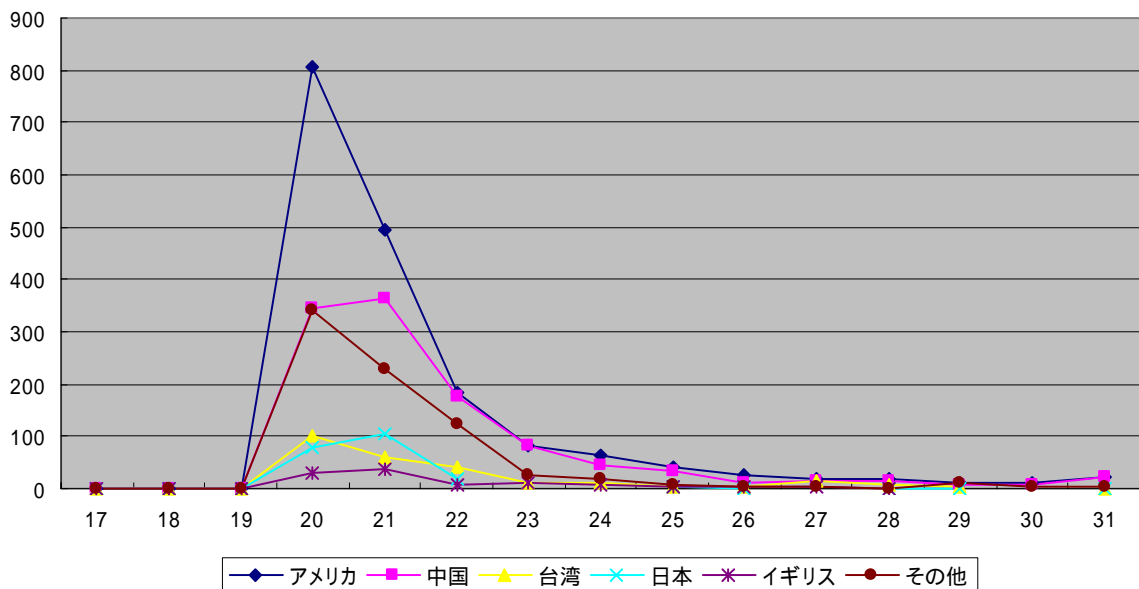


図 12 送信元ポート UDP4000 からのアクセス件数の推移 (1 日単位)

図 11 の 3 月 8 日に急増した TCP1025 番ポートは、Windows の Remote Procedure Call (RPC) を使用する Distributed Component Object Model (DCOM) の脆弱性を標的としたものと推定される。また、3 月 18 日、23 日、24 日の UDP1026、1027 番ポートの増加は、前述したとおり Windows のメッセンジャサービスを利用したスパム広告が原因である。3 月 29 日の TCP1025、2745、6129 番ポートに対するアクセス件数の増加は、Gaobot 等のワームによるものと推測される。

図 12 は、UDP4000 番を送信元とするアクセス数を示したものである。これは Internet Security Systems (ISS) 社製の複数の製品に脆弱性があり、その脆弱性を利用するワーム (Witty ワーム) の感染活動によるものである。

@police 掲載記事

- ・ TCP1025 番ポートに対するトラフィックの増加について (3/8)
http://www.cyberpolice.go.jp/important/20040308_231816.html
- ・ UDP1026, 1027 番ポートに対するトラフィックの増加について (3/18)
http://www.cyberpolice.go.jp/important/20040318_182007.html
- ・ UDP4000 番ポートを発信元ポートとするトラフィックの増加について (3/20)
http://www.cyberpolice.go.jp/important/20040320_221628.html
- ・ ISS 製品の脆弱性及び Witty ワームの発生について (3/21)
http://www.cyberpolice.go.jp/important/20040321_232408.html
- ・ TCP1025, 2745, 6129 番等のポートに対するトラフィックの増加について (3/29)
http://www.cyberpolice.go.jp/important/2004/20040329_215022.html

4 おわりに

当月期は、侵入検知装置におけるアラートの総検知件数は前月比約 11.0%の増加となった。中国からの「SQL SLAMMER worm」の件数は前月に引き続き増加したが、月末になるにつれ減少傾向となった。その一方で、アメリカ及び日本を発信元とする検知数が増加している。また、「SQL SLAMMER worm」以外のアラートは全体的に減少している。ファイアウォールに対するアクセスでは、前月中旬に発生した Welchia.B ワームにより国内からの TCP135 番ポートと TCP445 番ポートが増加したため、総アクセス件数が前月比 10.4%増となった。また、Internet Security Systems (ISS) 社の BlackICE 及び RealSecure 製品の ICQ インスタントメッセージ解析処理の問題を悪用した Witty ワームが発生し、UDP4000 を送信元とするアクセス数が一時的に増加した。また、Netsky、Beagle(4月26日現在、それぞれ Netsky.Z、Beagle.V まで発生している)ワームの亜種が多数発生した月であり、@police で注意喚起をおこなった。さらに複数の脆弱性を利用し感染を広める Gaobot ワームの亜種も多数発生し、感染活動に関連するポート(TCP1025、TCP3127、TCP2745、TCP6129 等)の増加が観測されている。

最近のワームの傾向として複数の脆弱性を攻撃するもの、また他のワームが開いたバックドアなどを利用するワームが増加している。これを防ぐためには、ウイルス対策ソフトの使用やソフトウェアの脆弱性を解消する修正プログラムの適用を行うなど、使用しているコンピュータのセキュリティ対策の徹底に努めることが必要である。