

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（要約） （平成15年度第1 / 四半期）

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）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を分析

- 平成15年度第1 / 四半期分のデータによる。ただし、5月28日16:45~21:00の間、システム更新のためデータを取得していない。

2 分析結果に見る特徴

発信元は米国、オランダ、中国、韓国の順が多い

検知されたアラート情報を発信元国別に分類したところ、本四半期は143カ国からの攻撃を検知している。上位を占めるのは、アメリカ合衆国、オランダ及び中国であり、これら3カ国からの攻撃の検知件数だけで全体の約67%を占めている。また、前の四半期において全体の約2%を占めるにすぎなかったオランダからの攻撃が、今期では約20%を占めており、件数でも前の四半期比で約20倍となっている。

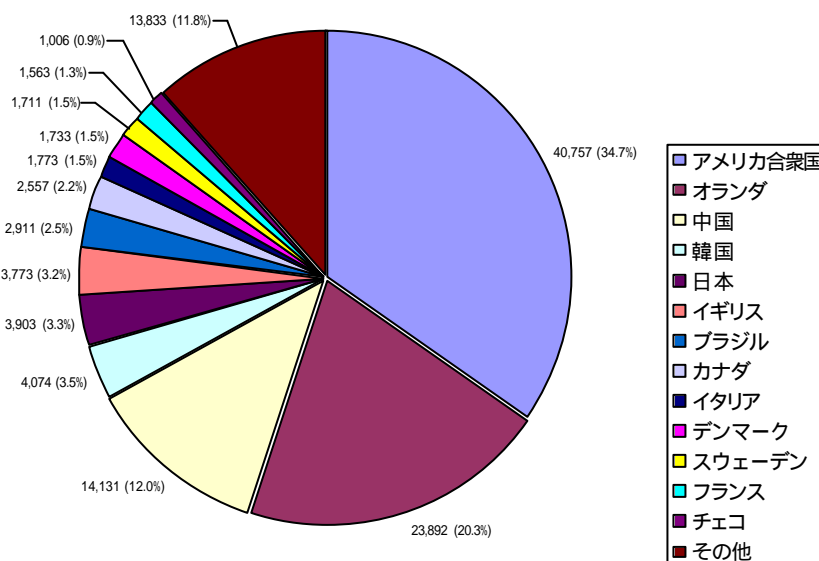
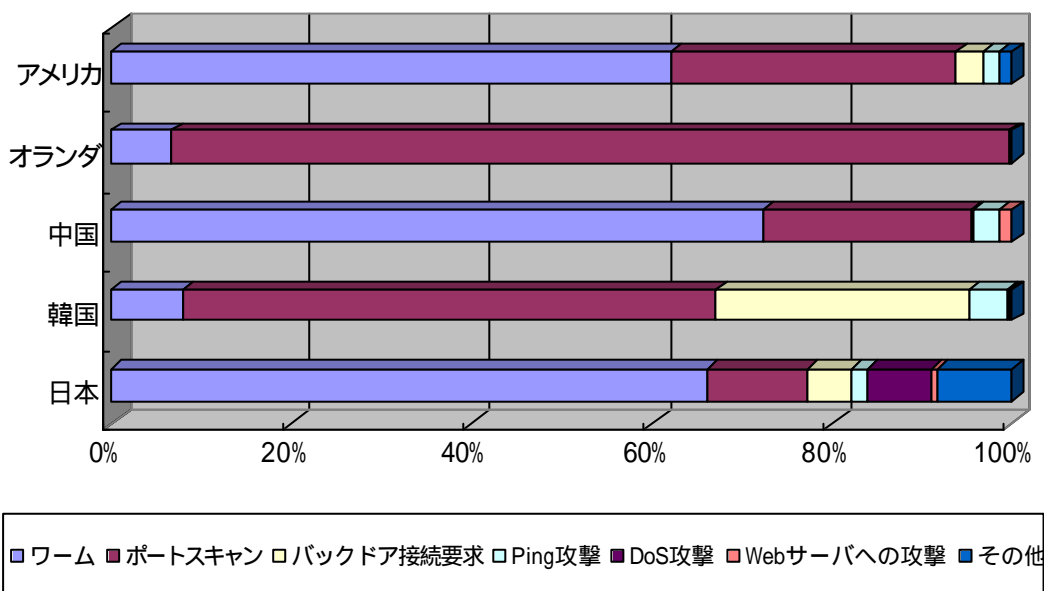


図1 攻撃の発信元の国別分析

攻撃手法にも国別特徴

多くのアラートを検知した上位 5 カ国のアラートの種別を図 2 に示す。全般的に言えるのはワームの占める割合が増加していることである。これは「SQL Slammer worm」の増加が主な要因であり、アメリカからは前の四半期の 2.5 倍以上、中国からは 13 倍以上と大幅に増加している。本四半期、急激に増加したオランダからの攻撃の主なものはポートスキャンである。そのほとんどが特定の IP アドレスを発信元とした、ネットワーク上で WWW proxy を探す行為を検知したものである。韓国からは「SQL Slammer worm」も漸増しているが、それ以上にポートスキャンが増加しており、韓国からの攻撃の 6 割近くを占めている。日本からの攻撃では「SQL Slammer worm」は件数、割合ともほとんど変化がない一方、ポートスキャン系の攻撃は半分程度に減少している。



国	ワーム	ポートスキャン	バックドア接続要求	Ping攻撃	DoS攻撃	Webサーバへの攻撃	その他	合計
アメリカ	25318	12915	1237	724	0	9	554	40757
オランダ	1627	22181	35	45	0	0	4	23892
中国	10209	3285	25	410	4	194	4	14131
韓国	322	2412	1145	169	3	15	8	4074
日本	2583	433	187	70	279	23	328	3903

図 2 国別攻撃手法

攻撃件数が激増

当期におけるアラートの検知件数の合計は、約 120,000 件であった。また、1 日当たりの平均検知件数、検知ホスト数はそれぞれ約 1,300 件、約 400 ホスト程度で推移している。前の四半期の総件数は約 51,000 件であったので、2 倍以上に増加していることとなる。この増加の主な原因は「SQL Slammer worm」である。

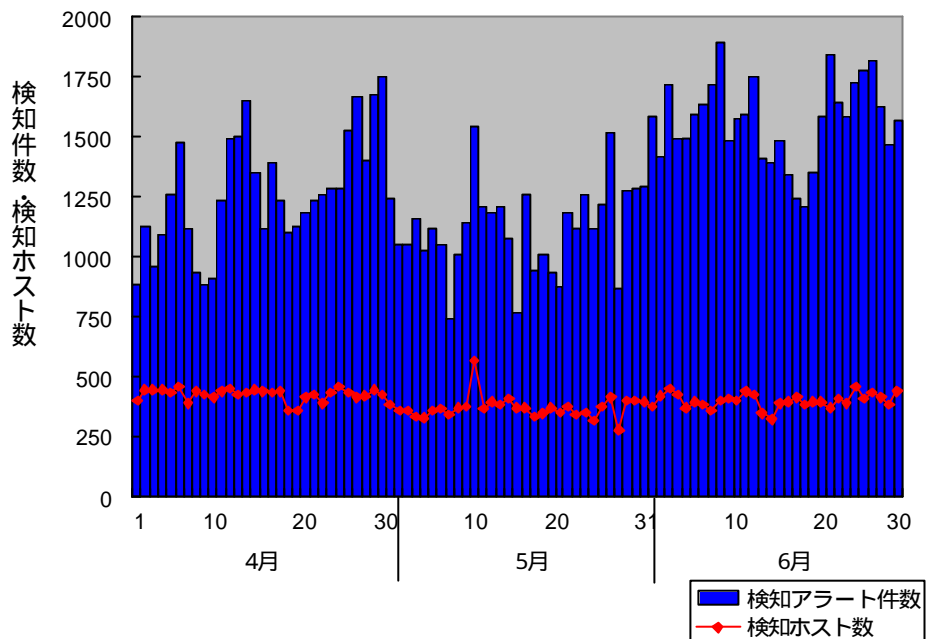


図3 第1/四半期における攻撃状況の推移

再び蔓延しつつある Slammer ワーム

図4が示すとおり前期と同様にワームが、かなりの割合を占めており、割合、件数ともに前期を上回っている。ワームの約40%はアメリカ合衆国からの攻撃である。「Ping攻撃」、「バックドア接続要求」、「Webサーバへの攻撃」、「DoS攻撃」、「その他」の割合は前期と比べると減っているが、件数では、ほぼ横ばいとなっている。

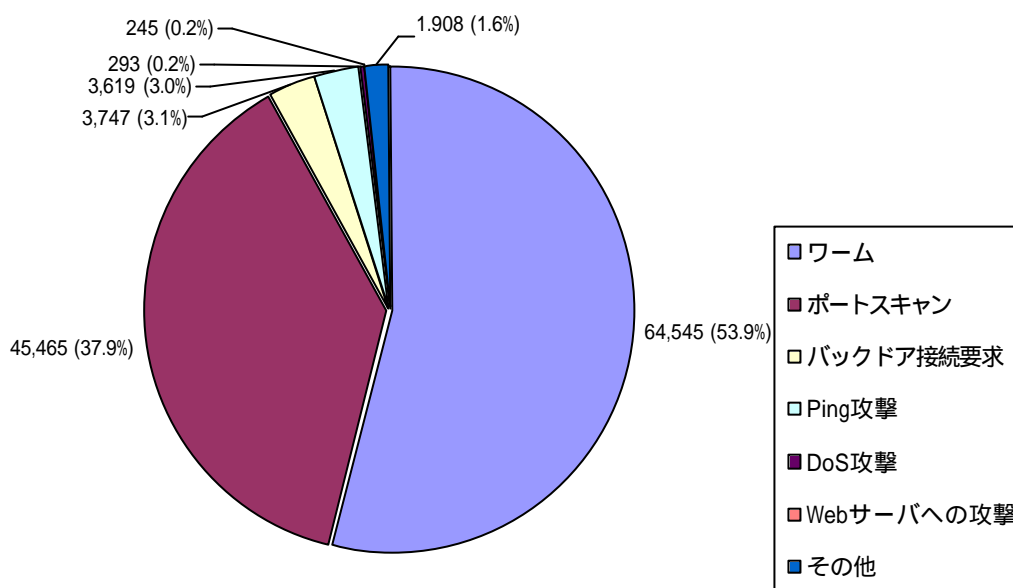


図4 攻撃手法による分析

攻撃種別の分類

大分類	代表的なシグネチャ名	大分類	代表的なシグネチャ名	
Ping攻撃	PING NMAP	バックドア接続要求	Sub7_v2.2 probe	
	superscan echo		Back Orifice2000	
	redirect host	Webサーバへの攻撃	WEB-IIS ISAPI_ida access	
	redirect net		IIS/PWS Escaped Characters Decoding Command Execution	
	Large ICMP Packet		Web Cmd completed	
ポートスキャン	Proxy attempt	その他	FTP Bad login	
	SYN FIN scan		Traceroute サービスの検出	
	NULL scan		IPFragmentation	
	nmap_TCP		Connection_Closed MSG from Port 80	
	FIN scan		Linux Traceroute	
	Portscan Detection Attack		IP Duplicate	
	Port sweep		Window size of 55808(SYN) TCP Packet	
	NMAP_XMAS		DNS HINFOデコード	
	DoS攻撃		tcp_denial_of_service	DNS named inquiry attempt
			Teardrop attack	named version attempt
SYN Flood		SQL SLAMMER worm		
IP Denial-of-Service Attacks		ワーム		

地域別の攻撃の時間的推移

図5に地域別の攻撃時間帯の推移を示す。本システムで統計を取り始めた当初は、地域ごとに各地域の深夜に相当する時間帯には攻撃が減少するという特徴がはっきりと出ていたが、前期ではあまり特徴が現れなくなり、当期ではさらに時間による特徴がみられなくなっている。これは、「SQL Slammer worm」等のように、人手を介さず24時間動作するプログラムに起因するアラートが検知件数の大きな部分を占めてきたためと思われる。

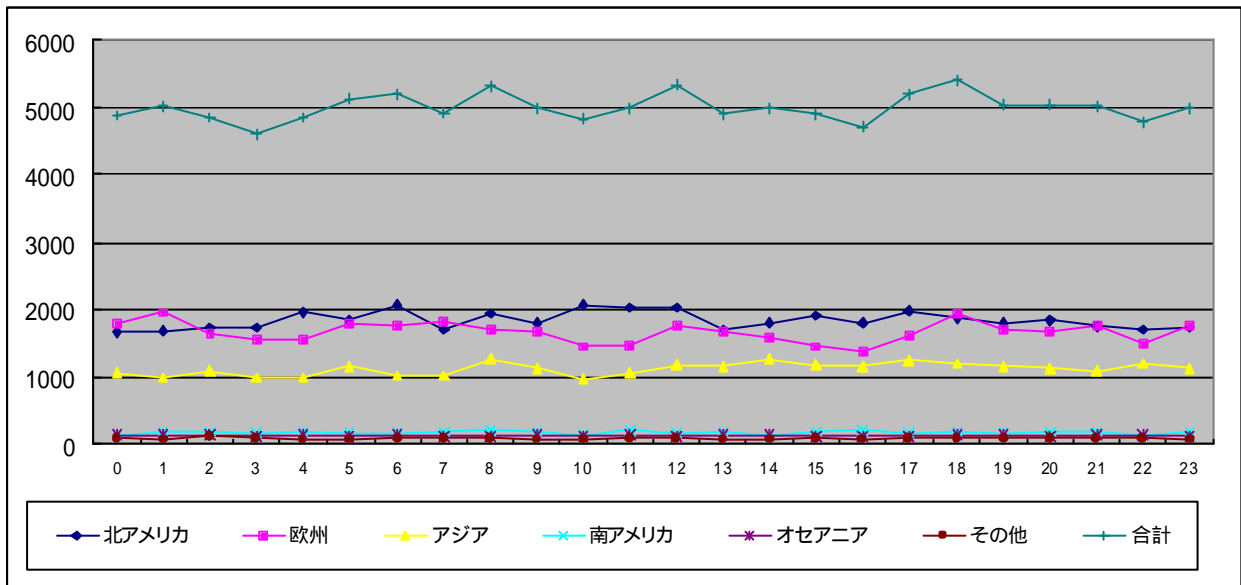


図5 地域別の攻撃の時間的推移

3 分析結果の活用

これらの分析結果については、本年3月に開設した「警察庁セキュリティポータルサイト」(<http://www.cyberpolice.go.jp>)などにより、国民一般に広報を行い、セキュリティに関する啓発活動に利用するほか、重要インフラ事業者等に情報提供し、各事業者等のセキュリティ向上のためのデータとして活用してもらうこととしている。また、わが国の状況を諸外国の機関に対して情報提供するとともに、関係国との情報共有を促進している。さらに、セキュリティ技術全般への寄与を目的として、学会等への公表を目指した官学連携を推進している。

4 おわりに

第1/四半期における検知件数は約120,000件で、前期の2倍以上と大幅に増加した。そのうち「Slammer」ワームが約65,000件となっている。本年1月25日に発生したこのワームは、発生から5ヶ月以上を経てもなお、活発に活動を続けている。他にも大量のスキャン行為などもあり、今後とも注意深く動向を見守る必要がある。