

# 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7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）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7月期分のデータによる。

## 2 分析結果に見る特徴

### 発信元の上位国は米国、中国、韓国

検知されたアラート情報を発信元国別で分類したところ、当月期は112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、中国及び韓国であり、これら3カ国からの攻撃の検知件数だけで全体の56%を占めている。前月まで大量の攻撃を検知していたオランダはcyberangels.nlからのTCP1080ポートへの大量の攻撃がなくなり第17位に下降している。

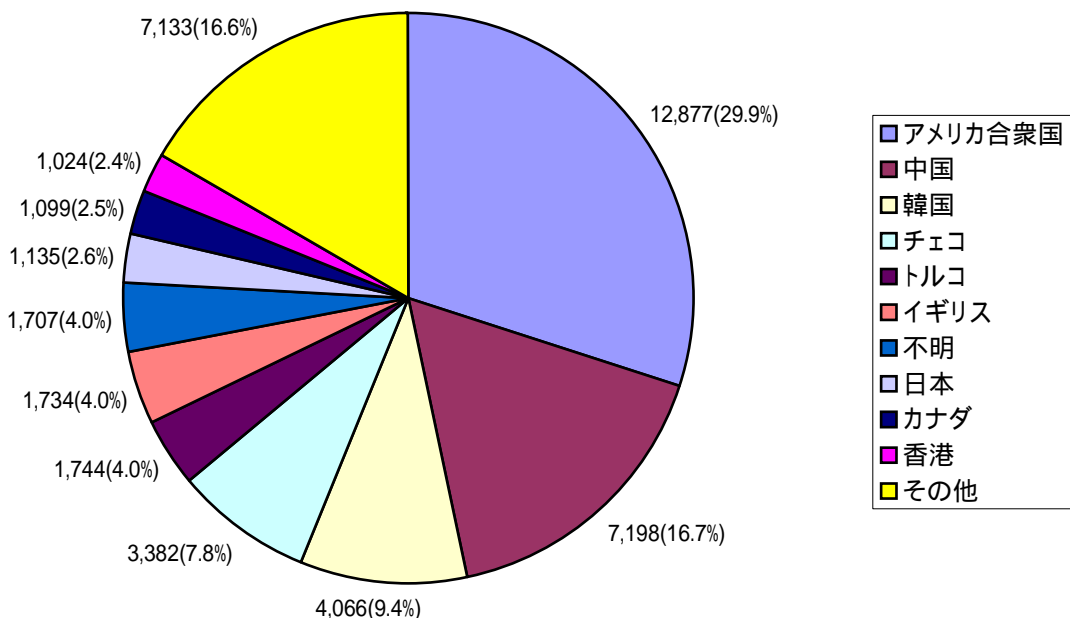
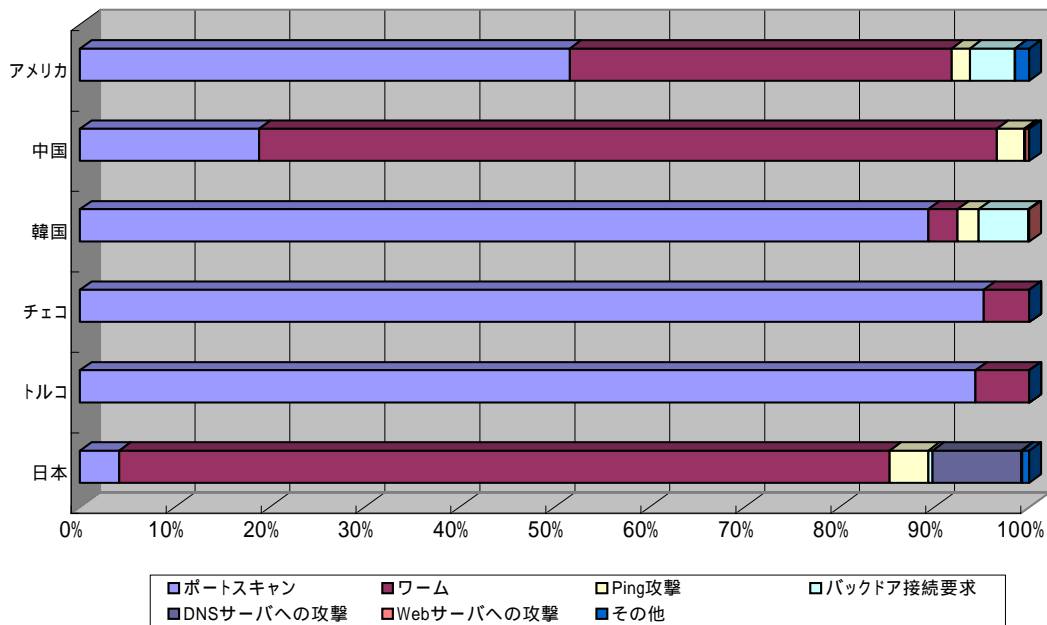


図1 攻撃発信元の国別分析

## アメリカ合衆国、韓国及びトルコからの TCP1080 ポートへのスキャンが増加

多くのアラートを検知した上位 5 カ国及び国内のアラート種別を図 2 に示す。全体的にはポートスキャンの占める割合が多くなっており、大部分は TCP1080 ポートへの攻撃となっている。先月に比べアメリカ合衆国からの TCP1080 ポートへの攻撃が 1,259 件増加、SQL Slammer ワームが 4,007 件減少したため、ポートスキャン系の割合が約 18%上昇している。韓国も TCP1080 ポートへの攻撃が約 1.8 倍になり、ポートスキャン系の割合が 14% 上昇している。また、当月よりトルコからの TCP1080 ポートへの攻撃が始まり 1,644 件検知している。チェコからウィンドウサイズ 55808 の TCP パケットを多く検知したが、ウイルスの感染により送信元が詐称されている可能性がある。国内における動向としては、先月に比べ総検知数は約 250 件減少し、SQL Slammer も減少しているが、相変わらず 80%以上を SQL Slammer が占めている。

注)TCP1080 ポートへの攻撃は、もっぱら WWW の閲覧を代行するプロキシと呼ばれるコンピュータを探る行為であると推測される。



国	ポートスキャン	ワーム	Ping攻撃	バックドア接続要求	DNSサーバへの攻撃	Webサーバへの攻撃	その他	合計
アメリカ	6642	5181	246	610	3	0	195	12877
	51.6%	40.2%	1.9%	4.7%	0.0%	0.0%	1.5%	100.0%
中国	1358	5593	207	9	0	27	4	7198
	18.9%	77.7%	2.9%	0.1%	0.0%	0.4%	0.1%	100.0%
韓国	3632	126	90	213	0	5	0	4066
	89.3%	3.1%	2.2%	5.2%	0.0%	0.1%	0.0%	100.0%
チェコ	3220	162	0	0	0	0	0	3382
	95.2%	4.8%	0.0%	0.0%	0.0%	0.0%	0.0%	100.0%
トルコ	1645	99	0	0	0	0	0	1744
	94.3%	5.7%	0.0%	0.0%	0.0%	0.0%	0.0%	100.0%
日本	47	921	46	5	106	1	9	1135
	4.1%	81.1%	4.1%	0.4%	9.3%	0.1%	0.8%	100.0%

図 2 国別攻撃手法

### オランダからの TCP1080 ポートへの攻撃止む

当月期におけるアラートの総検知数は 43,099 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 1390 件、約 396 件で推移している。先月の総検知数は 46,997 件であったので、約 3900 件減ったことになる。これは、オランダのドメイン cyberangels.nl からの TCP1080 ポートへの攻撃が止まったことが主な原因である。

先月、cyberangels.nl からの攻撃は総計で約 9 千件に上っていたが、7 月 1 日を最後に検知されなくなった。これは、cyberangels.nl とスパム業者との関わりがイギリスの記者によって明らかにされたことを受け、7 月 1 日付で上位プロバイダからサービスを打ち切られたことが原因である。現在、cyberangels.nl ドメインはオランダの反スパム団体に管理されており、詳細な経緯が [www.cyberangels.nl](http://www.cyberangels.nl) より参照可能である。

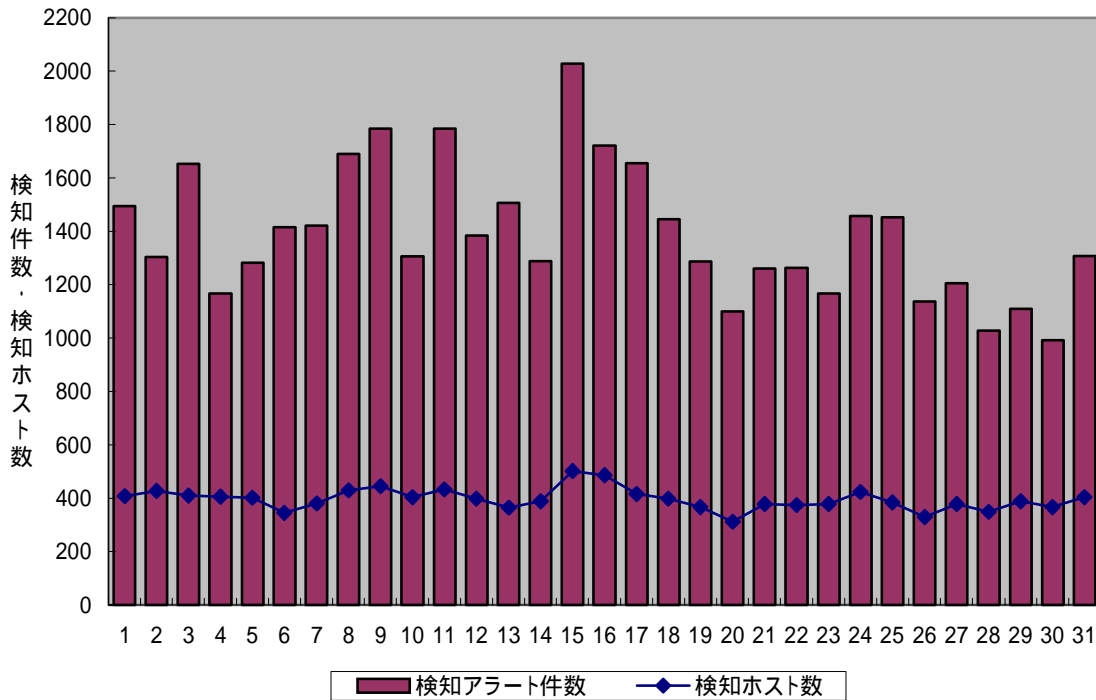


図 3 7 月期における攻撃状況の推移

## 攻撃手法による分析

当月期はポートスキャン系がワーム系の割合よりわずかに多くなった。これは、アメリカ合衆国からの SQL Slammer ワームが先月に比べ 4 割以上の大幅な減少となったためである。中国からの SQL Slammer ワームが 5 月下旬より増加し高い検知数で推移していたが、7 月下旬に沈静化している。

また、7 月中旬に発表された Windows RPC インターフェスの脆弱性 (MS03-026) を悪用した攻撃は検知されなかった。

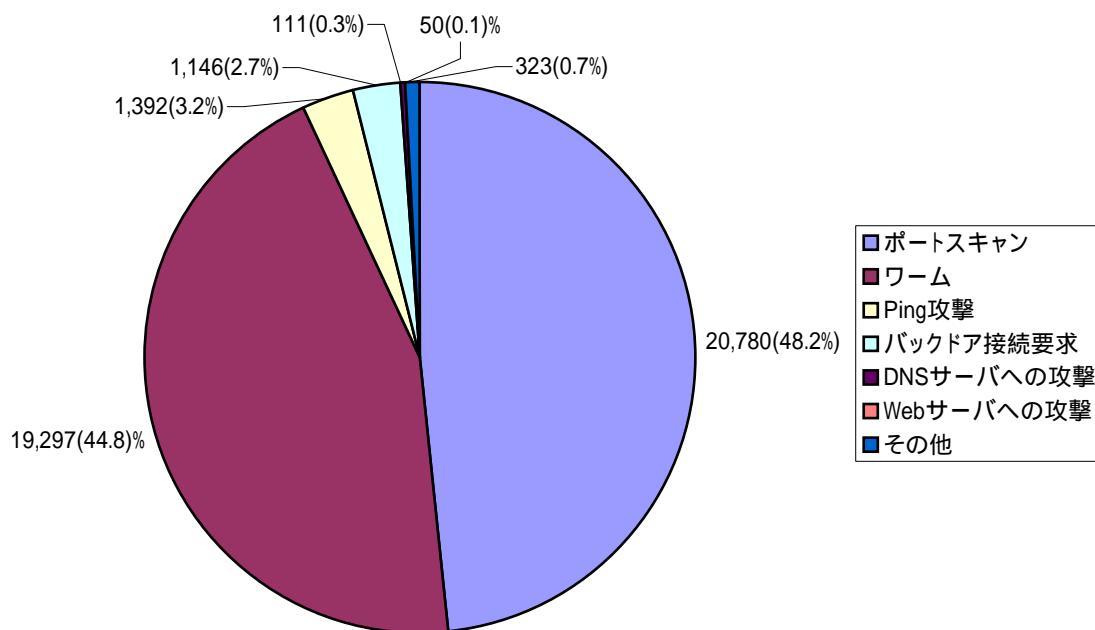


図 4 攻撃手法による分析

## 7 月期に検知した攻撃の分類

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	Large ICMP Packet	ワーム	SQL SLAMMER worm
	PING NMAP	Webサーバへの攻撃	IIS/PWS Escaped Characters Decoding Command Execution
	redirect host		WEB-IIS ISAPI .ida access
	redirect net	バックドア接続要求	Back Orifice2000
	superscan echo		Sub7 v2.2 probe
ポートスキャン	ident version	DNSサーバへの攻撃	DNS HINFOデコード
	nmap TCP		DNS Hostname Overflow Attack
	NMAP XMAS		DNS named iquery attempt
	NULL scan		非特権ポートDNS ZONEトランスファ
	Portscan Detection Attack	その他	SYN Flood
	Proxy attempt		FTP No Password
	SYN FIN scan		MIME Header Attachment
	Window size of 55808 TCP Packet		IP Duplicate
	Packet		Linux traceroute
			Traceroute サービスの検出

## 地域別の攻撃の時間的推移

図 5 に攻撃数の多い北アメリカ、東アジア、西ヨーロッパの各地域におけるポートスキャン系とワーム系の攻撃時間帯の推移を示す。ワーム系は人手を介さず自動的に実行されているため、ポートスキャン系に比べワーム系は時間による変化が小さい。一方で、北アメリカと東アジアのポートスキャン系では起伏が激しく、時間的な変化が大きくなっている。また、北アメリカと東アジアのポートスキャン系は夜間から朝方にかけて検知数が増加しているが、西ヨーロッパにおいては若干昼間の時間帯が多くなっている。

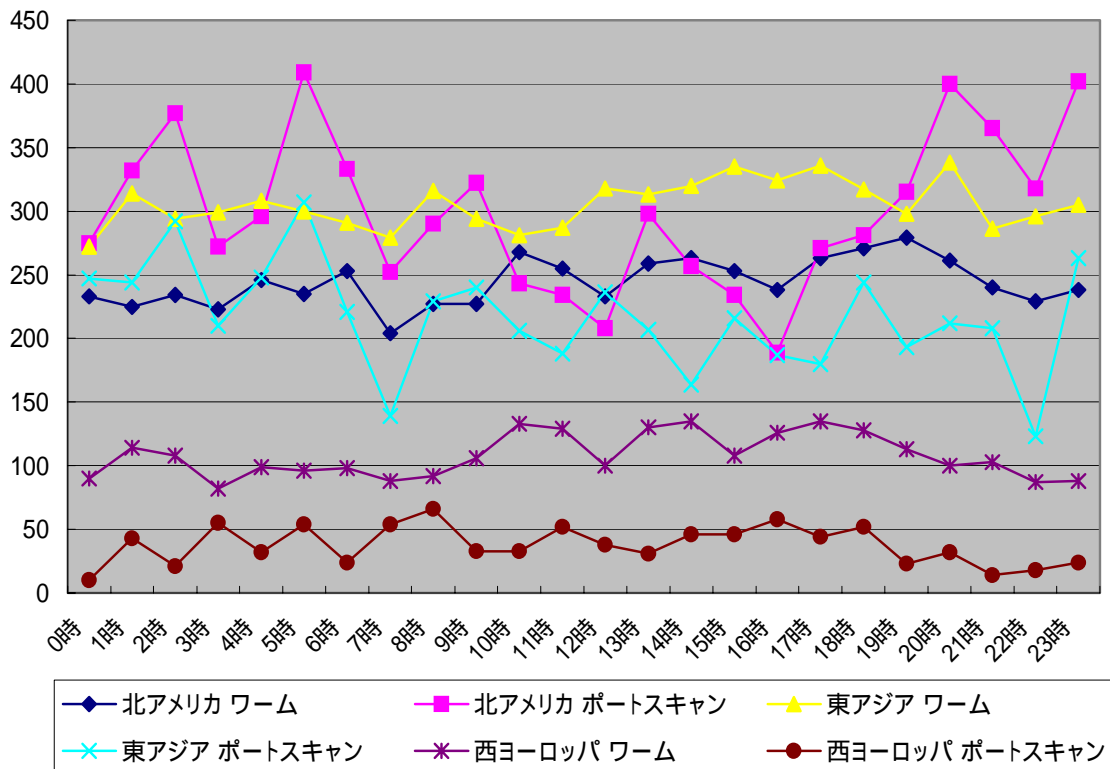


図 5 地域別の攻撃の時間的推移

## おわりに

7月期の検知ネットワークにおける総検知数は、先月に比べ約 3900 件減少した。これは、オランダからの TCP1080 ポートへの攻撃が減少したことが主な原因である。一方で、アメリカ、韓国及びトルコ等からの TCP1080 ポートへの攻撃は増加傾向にあるため今後の動向が懸念される。SQL Slammer ワームについては、アメリカが大幅に減少し、また、増加傾向にあった中国も当月末には沈静化傾向にある。当月期は Microsoft Windows の脆弱性が数多く発見されている。特に RPC を脆弱性とした攻撃は現在のところ検知していないが、深刻な問題であるため今後も十分注意する必要がある。