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8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

－　全国の警察施設におけ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8月期分のデータによる。

2　分析結果に見る特徴

○　攻撃の検知数が大幅に減少

当月期における攻撃の検知数は34,973件、検知ホスト数8,634件であり、7月期と比較すると検知数は約8,100、検知ホスト数は約990件減少した。これは、SQL Slammerワームの活動と1080番ポートへの攻撃が大幅に減少したことが主な原因である。

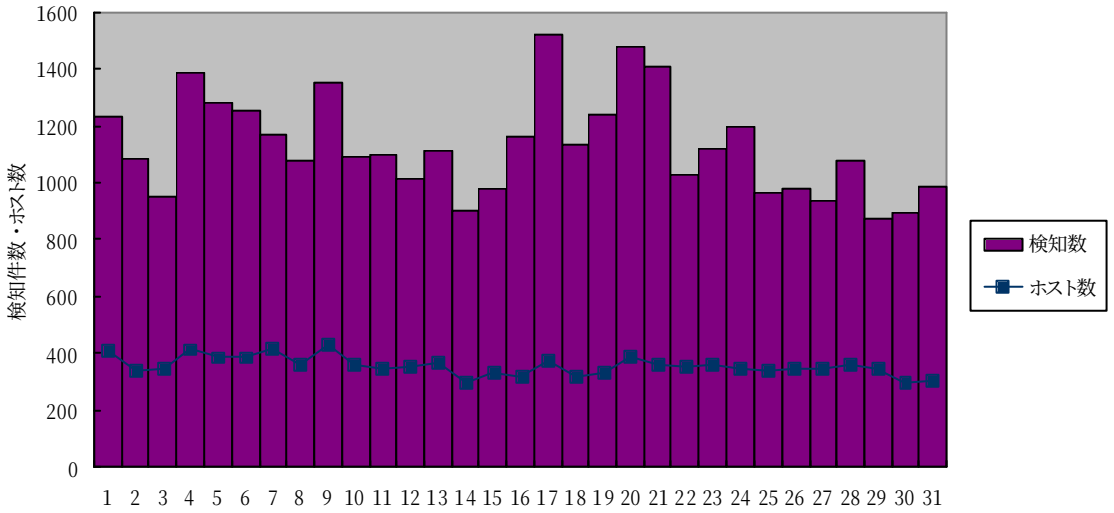


図1　8月期における攻撃状況の推移

○　**発信元の上位国は米国、韓国、中国**

検知された攻撃を発信元国別で分類したところ、当月期は 111 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、韓国及び中国であり、これら 3 カ国からの攻撃の検知件数だけで全体の 57%を占めている。

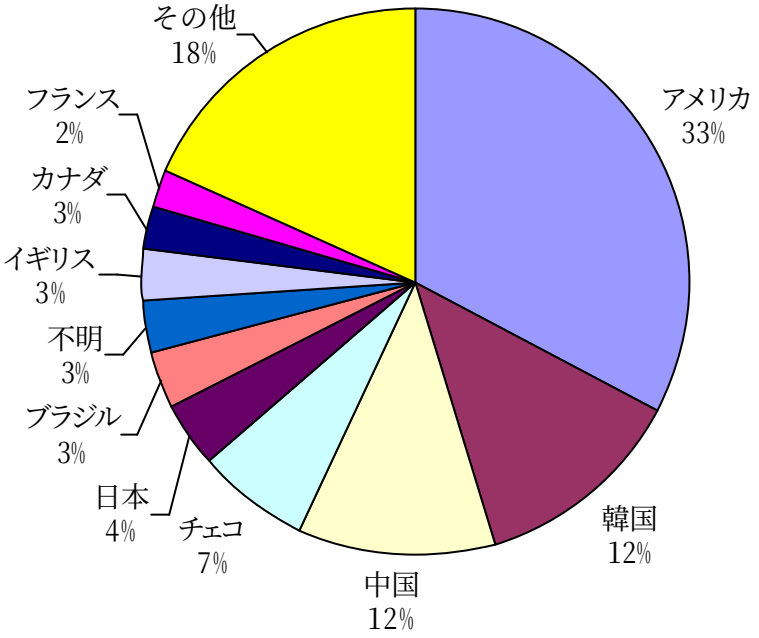
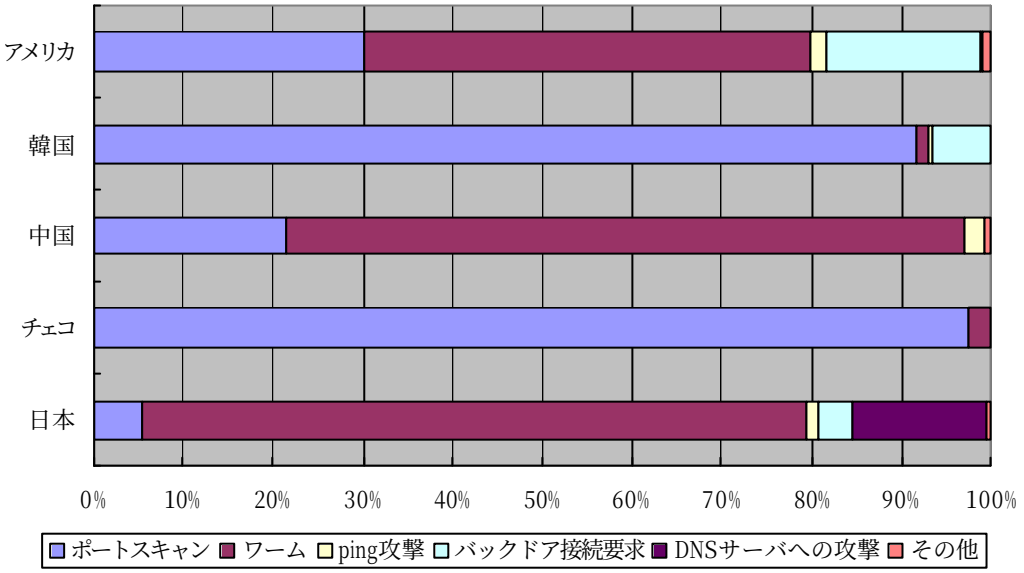


図 2　攻撃発信元の国別分析

○ **アメリカ合衆国及びトルコからの TCP1080 ポートへのスキャンが減少**

多くの攻撃を検知した上位 5 カ国のアラート種別を図 2 に示す。先月に比べアメリカ合衆国からのポートスキャンが 3,187 件減少したため、ポートスキャン系の割合が減少しており、1,381 件増加したバックドア接続要求の割合が大幅に増加している。韓国は TCP1080 ポートへの攻撃が、チェコは、ウィンドウサイズ 55808 の TCP パケットを多く検知したため、ポートスキャンの割合がほとんどを占めている。なお、ウィンドウサイズ 55808 の TCP パケットは、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高い。日本における動向としては、7 月期と比較してバックドア接続要求が多少増加したが、相変わらず SQL Slammer がアラートの 8 割近くを占めている。



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	その他	合計
アメリカ	3,455	5691	191	1981	6	123	11,447
	30.2%	49.7%	1.7%	17.3%	0.1%	1.1%	
韓国	3,997	59	19	287	0	0	4,362
	91.6%	1.4%	0.4%	6.6%	0.0%	0.0%	
中国	880	3,091	101	0	0	27	4,099
	21.5%	75.4%	2.5%	0.0%	0.0%	0.7%	
チェコ	2,319	62	0	0	0	0	2,381
	97.4%	2.6%	0.0%	0.0%	0.0%	0.0%	
日本	69	948	17	50	190	7	1,281
	5.4%	74.0%	1.3%	3.9%	14.8%	0.5%	

図 3　国別攻撃手法

○　攻撃手法による分析

当月期は世界的にポートスキャンが大幅に減少したため、ワームの割合が半分近くを占めている。また、アメリカ合衆国からのバックドア接続要求が 3 倍以上増加したため、バックドア接続要求の割合が増加している。

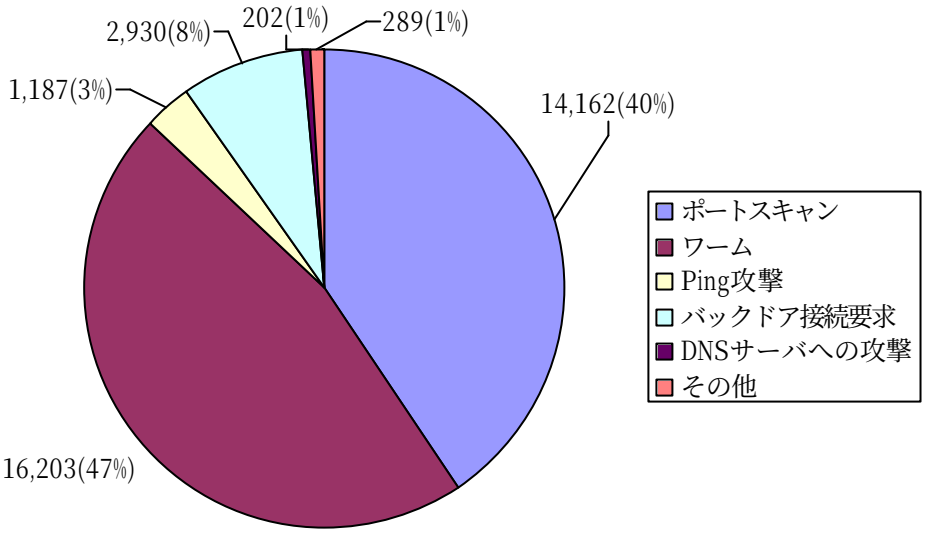


図 4　攻撃手法による分析

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	バックドア接続要求	IP Unknown Protocol
	PING NMAP		Sub7 v2.2 probe
	redirect host	DNSサーバへの攻撃	DNS Length Overflow Attack
	redirect net		DNS HINFOデコード
	superscan echo	その他	MIME Header Attachment
ポートスキャン	Portscan Detection Attack		Traceroute サービスの検出
	Proxy attempt		Linux Traceroute
	FIN scan		IP　Duplicate
	SYN FIN scan		Stick Attack
	nmap TCP		UDP FLOOD
	Window size of 55808(SYN) TCP Packet		EXPERIMENTAL SMTP HELO overflow attempt
	Window size of 55808 TCP Packet		WEB-IIS ISAPI .ida access
ワーム	SQL SLAMMER worm		

○　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攻撃時間帯別のアラート検知件数の推移を示す。東アジアで早朝の検知数が若干少なくなっている他は、時間帯別での検知数に大きな変動は見られない。

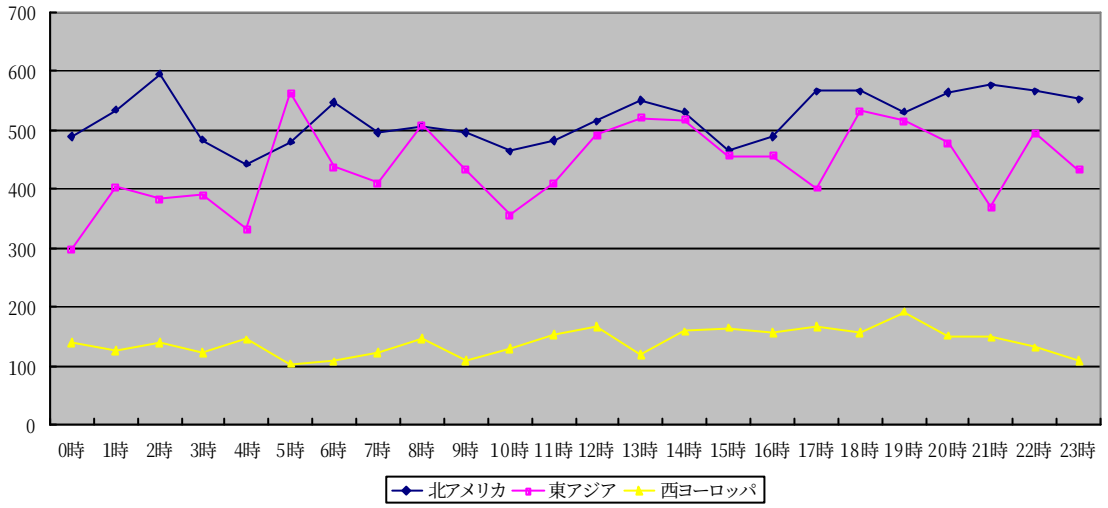


図 5　地域別の攻撃の時間的推移

○　おわりに

8 月期の検知ネットワークにおける総検知数は、7 月期に比べ約 8,100 件減少した。これは、SQL Slammer ワームが約 3,100 件減少、TCP1080 ポートへの攻撃が約 5,500 件減少と大幅に減少したことが主な原因である。しかしながら、バックドアの存在を確認する行為が 1,784 件増加しており、今後の動向が懸念される。

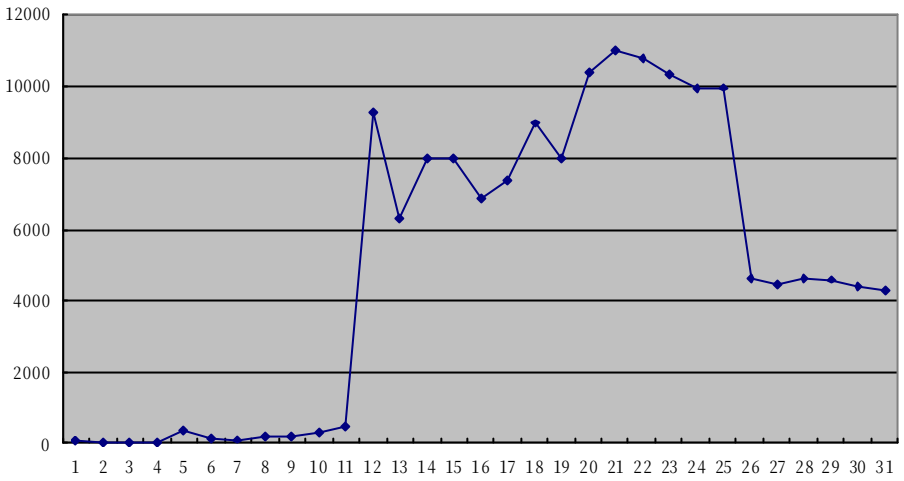
8 月期は、マイクロソフト社から公表された Windows の脆弱性(MS03-26)を利用したワームが複数登場し猛威を振るっているが、全国の警察施設のインターネット接続点は、これらワームに対して極めてセキュリティの高い設定であることから、ワームの感染行為が発生しないため、侵入検知装置においてはワームの動向は検知されていない。Windows の脆弱性(MS03-26)を利用したワームの動向については、参考「Windows RPC の脆弱性を使用するワームの発生について」で解説する。

参考

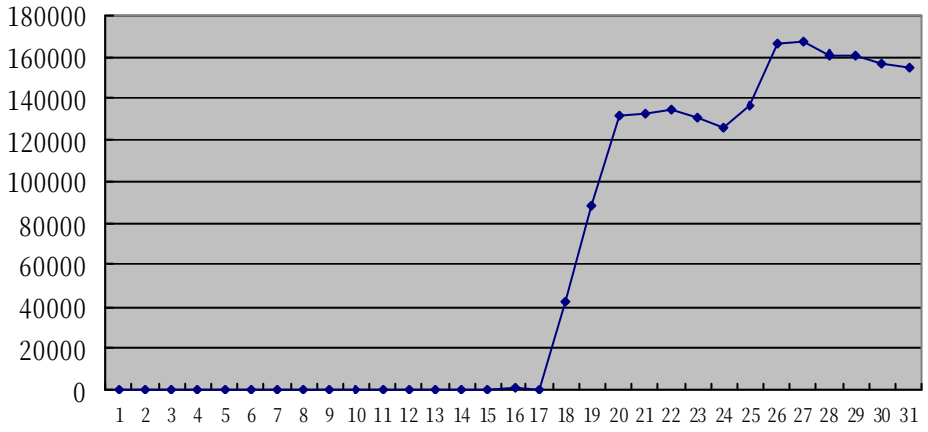
Windows RPC の脆弱性を使用するワームの発生について

7 月 17 日､マイクロソフト社から公表された Windows の脆弱性(MS03-26)は、多くの Windows OS が対象であり、脆弱性がある RPC の機能がデフォルトで有効になっていることから、ワーム等が発生した場合の影響の大きさが懸念されていた。7 月下旬には、この脆弱性を悪用する攻撃コードが公開され、インターネット上の脅威が高まるなか、当サイバーフォースセンターにおいても、IDS への検知シグネチャの追加並びにファイアウォールのログについて、脆弱性に関連するポートへのアクセス状況（ port135/TCP、ICMP 等）の分析を行い、動向を注視していたところ、日本時間 8 月 12 日午前 2 時頃からへのアクセスが急激に増加し始めたことから、Blaster ワーム（別名 MSBLAST 又は Lovsan）の発生を認知した。さらに、18 日午前 11 時頃からは、ICMP を送信した後、応答のあったホストに対し RPC DCOM（MS03-26）及び WebDAV の脆弱性（MS03-007）を悪用するワーム Welchia（別名 Nachi）によると考えられる ICMP トラフィックの急増を認知した。これらの認知状況をもとに、インターネットユーザに対し、@police（http://www.cyberpolice.go.jp/）を通じて注意喚起を行うとともに、ワームの解析結果等の情報を提供した。

なお、IDS を設置しているインターネット接続点は、今回発生したワームに対しても安全に設定していることから、感染活動における最初の接続要求の段階でブロックされるため、これらワームの活動は、IDS では検知されていない。しかしながら、ワーム発生時には平常時と比較して、極めて多数の接続要求が発生することから、今回は、ファイアウォールにおける接続要求を拒否した件数を分析し、当該ワームの大まかな動向を把握したものである。



port135/tcp のアクセス件数の推移



ICMP の件数の推移

注）26 日以降件数が変化したのは、一部のファイアウォールの ICMP echo request に対するポリシーを変更したためである。これは、従前、同ポリシーが 57 拠点で斉一でなかったため、Welchia ワームの感染活動に対する反応に差異が生じたことから、将来の同種事案に備え、ICMP echo request に対して返答しない設定に統一したものである。