

# 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2 / 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）及びファイアウォール(Firewall)によって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2 / 四半期分のデータによる

## 2 分析結果に見る特徴

### 発信元は米国、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145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約58%を占めている。

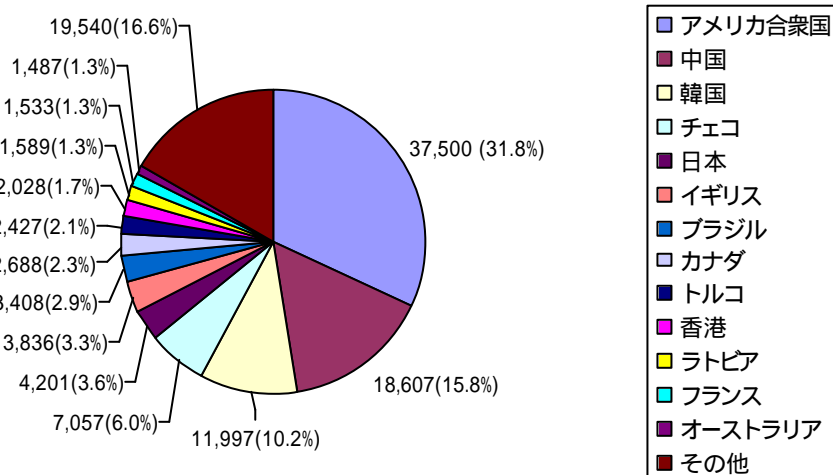


図1 攻撃の発信元の国別分析

## アジア地域を発信元とする攻撃が増加

図2にアラート検知数の上位5カ国におけるアラート種別を示す。

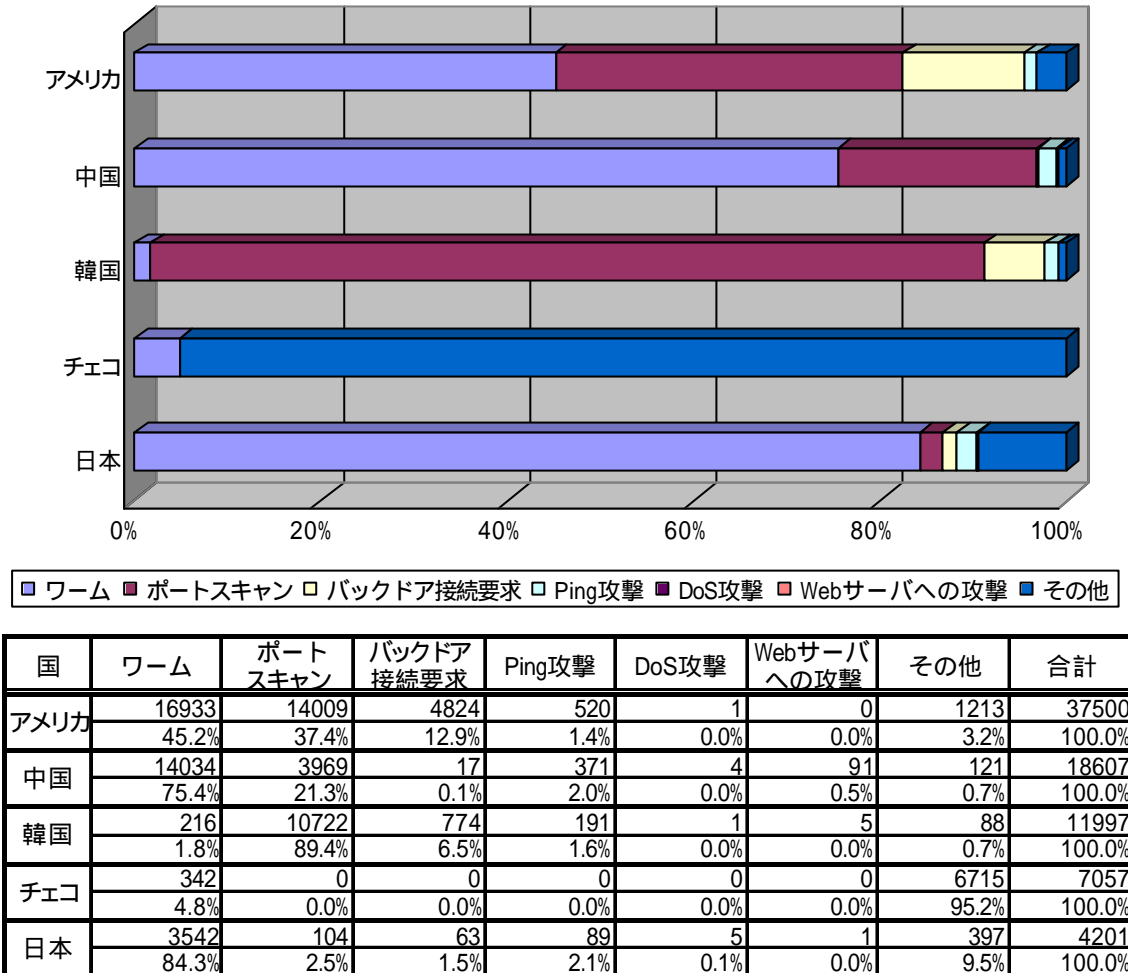


図2 国別攻撃手法

前期と比較して国別の傾向を見ると、アメリカのバックドア接続要求、韓国のポートスキャン、中国と日本のワームが増加している。アラート数では、アメリカを発信元とする総件数は減少したものの、中国、韓国、日本といったアジア地域を発信元とする攻撃が増加している。

なお、チェコは「その他」に計上される「Window size of 55808(SYN) TCP Packet」の件数が多かったが、発信元のIPアドレスは詐称されている可能性が高い。

### 攻撃件数は横ばい

当期におけるアラートの検知件数の合計は、約 118,000 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 1,280 件、約 380 ホスト程度で推移している。8 月には検知数が減少傾向であったが、9 月に入ってから再び増加し、結果的に検知数は前期と大きな差は見られない。

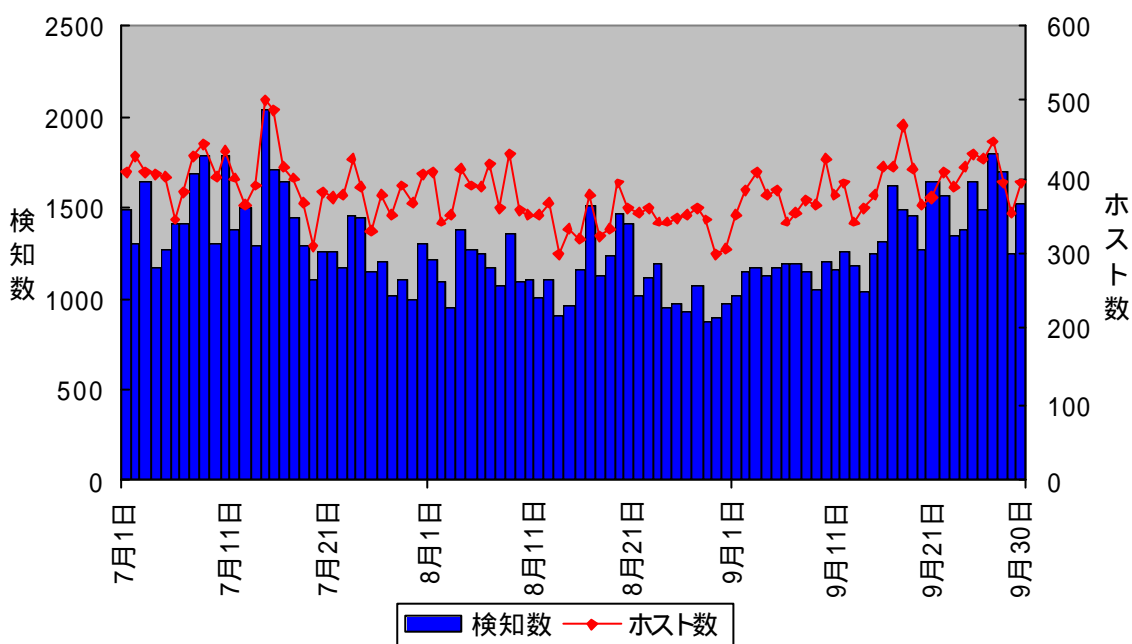


図3 第2/四半期における攻撃状況の推移

## バックドア接続要求が増加

攻撃手法別では、「ワーム」と「ポートスキャン」で全体の約8割となった。前期と比べると、バックドア接続要求が増加しており、8月以降、アメリカを発信元とする攻撃を多数検知している。「Ping 攻撃」、「DoS 攻撃」、「Webサーバへの攻撃」の件数は前期と比べると減少した。「その他」はWindow size of 55808(SYN) TCP Packet の検知数によって増加することとなった。

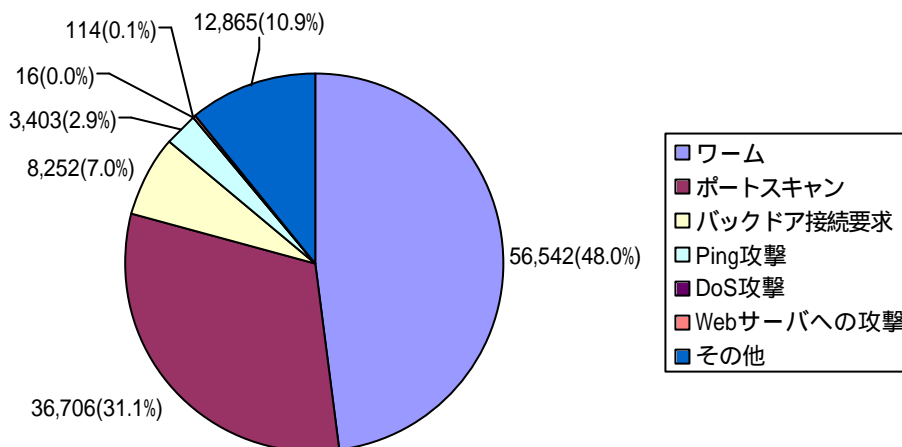


図4 攻撃手法による分析

## 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	DoS攻撃	tcp denial of service
	superscan echo		Tear-drop attack
	redirect host		SYN Flood
	redirect net		IP Denial-of-Service Attacks
	Port sweep		Stick Attack
	Portscan Detection Attack		UDP Bomb
ポートスキャン	Large ICMP Packet	その他	MIME Header Attachment
	Proxy attempt		Traceroute サービスの検出
	SYN FIN scan		IP Fragmentation
	NULL scan		Linux Traceroute
	nmap TCP		IP Duplicate
	FIN scan		Source Port 20 to <1024
ワーム	NMAP XMAS		webtrends scanner
バックドア接続要求	SQL SLAMMER worm		Window size of 55808 TCP Packet
	Sub7 v2.2 probe		Window size of 55808(SYN) TCP Packet
Webサーバへの攻撃	Back Orifice2000		DNS HINFOデコード
	WEB-IIS ISAPI_ida access		DNS named iquery attempt
	IIS/PWS Escaped Characters Decoding Command Execution		named version attempt

## Blaster 及び Welchia ワームの発生

8 月には Windows の Remote Procedure Call (RPC) に関する脆弱性を利用したワームが発生し、世界中で数多くの感染被害が報告された。図 5 は検知ネットワークシステムのファイアウォールにおいて観測した TCP135 番ポートに対するアクセスと ICMP エコー要求の検知数の推移であるが、Blaster ワーム（8 月 12 日発生）と Welchia ワーム（8 月 18 日発生）が利用するプロトコルの検知数が急増した。特に ICMP は、9 月に入ってからも同様の検知数が続いており、被害の大きさを示している。

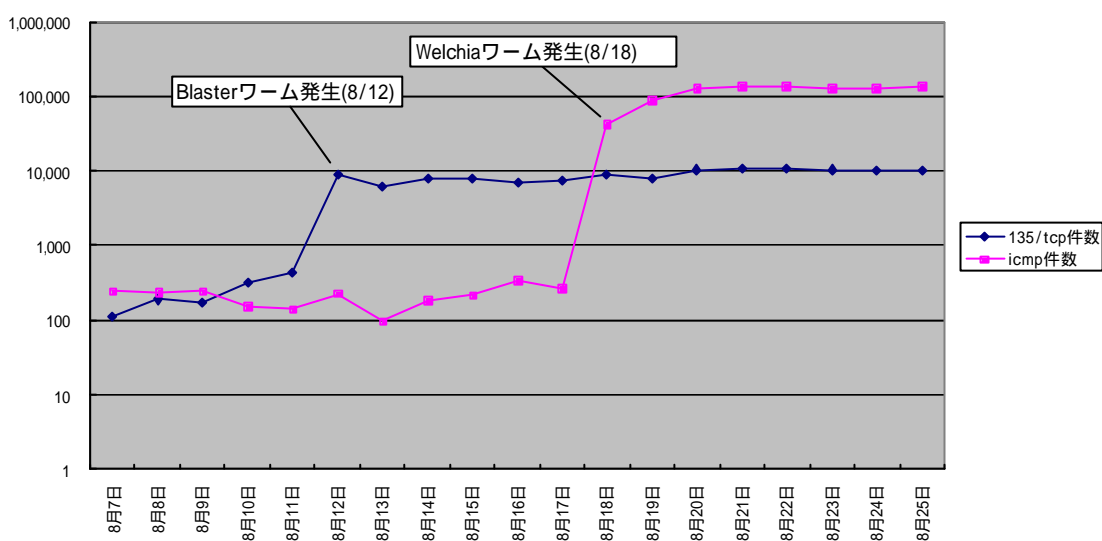


図 5 TCP135 ポート及び ICMP エコー要求の検知数推移（8/7～25）日毎

## 地域別における攻撃の時間的推移

図 6 に地域別の攻撃時間帯の推移を示す。

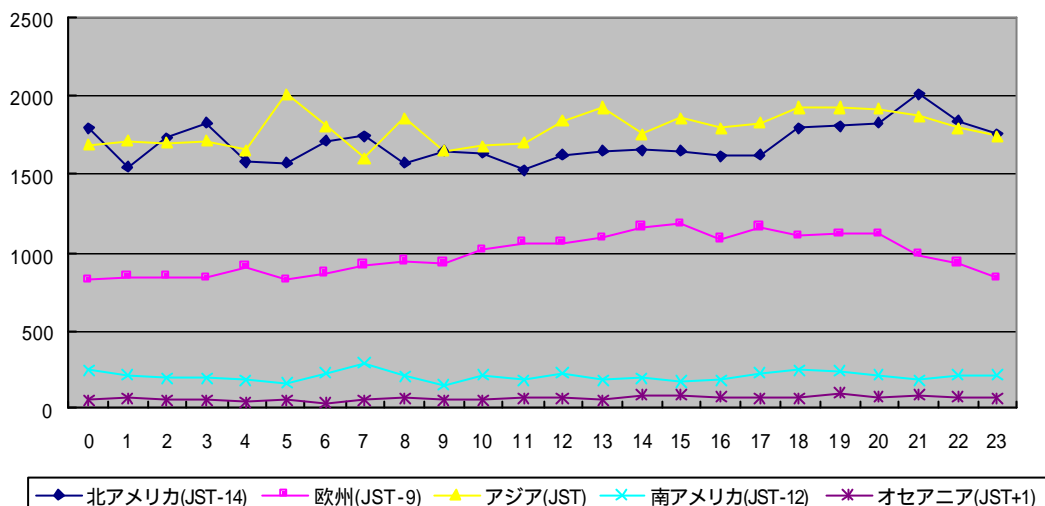


図 6 地域別の攻撃の時間的推移

アジア地域を発信元とする検知件数は、特に 5 時台と 8 時台が増加しているが、これは特定の日中国又は韓国から集中したためである。このような特異な日はあるものの、比較的、午後以降に検知数の増加が見られる地域が多い。

### 3 分析結果の活用

これらの分析結果については、「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、我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 2/四半期における検知件数は、前期と同様の件数となったが、この件数には 8 月に発生した Blaster ワームや Welchia ワームは含まれていない。これらのワームについては、ファイアウォールの分析結果より、その被害は世界規模に及ぶことが確認され、改めてワーム感染の脅威を示すものとなった。今後も新たなワームの出現が懸念されることや、発生から半年以上も経過した「SQL Slammer」ワームが未だに蔓延していること、加えて、数多くのスキャン行為を検知していること等から、さらなるセキュリティ対策の強化が必要と言える。自らが被害者のみならず加害者とならぬよう、今一度、セキュリティ対策の見直しが望まれる。