

# 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 3 / 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 3 / 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 148 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 60% を占めている。

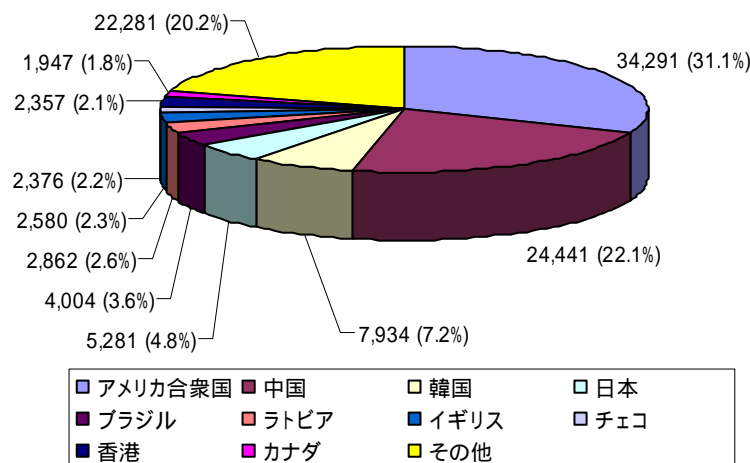
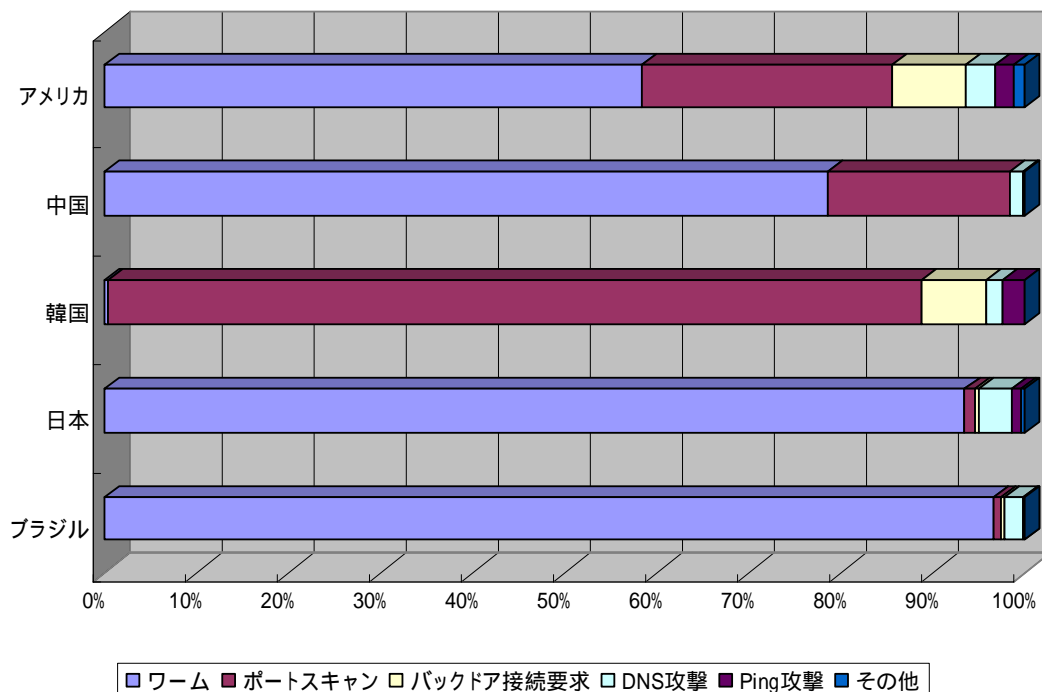


図 1 攻撃の発信元の国別分析

## 日本のワーム感染が増加

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。



国	ワーム	ポートスキャン	バックドア接続要求	DNS攻撃	Ping攻撃	その他	合計
アメリカ	20005	9366	2700	1143	691	386	34291
	58.3%	27.3%	7.9%	3.3%	2.0%	1.1%	100.0%
中国	19209	4823	0	365	43	1	24441
	78.6%	19.7%	0.0%	1.5%	0.2%	0.0%	100.0%
韓国	27	7012	566	132	195	2	7934
	0.3%	88.4%	7.1%	1.7%	2.5%	0.0%	100.0%
日本	4938	57	19	194	55	18	5281
	93.5%	1.1%	0.4%	3.7%	1.0%	0.3%	100.0%
ブラジル	3867	30	18	82	7	0	4004
	96.6%	0.7%	0.4%	2.0%	0.2%	0.0%	100.0%

図 2 国別攻撃手法

今期は、アメリカと韓国のポートスキャンが減少した一方で、アメリカと中国のワームと DNS 攻撃が増加している。前期に引き続き、日本はワームの増加が続いている。

### 攻撃件数は減少、発信元ホスト数は増加

当期におけるアラートの検知件数の合計は、約 110,000 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 1,200 件、約 420 ホスト程度で推移している。ポートスキャンやバックドア接続要求が減少したため、結果的にアラートの総件数は減少している。一方、ワームの増加に伴い、発信元ホスト数が増加している。

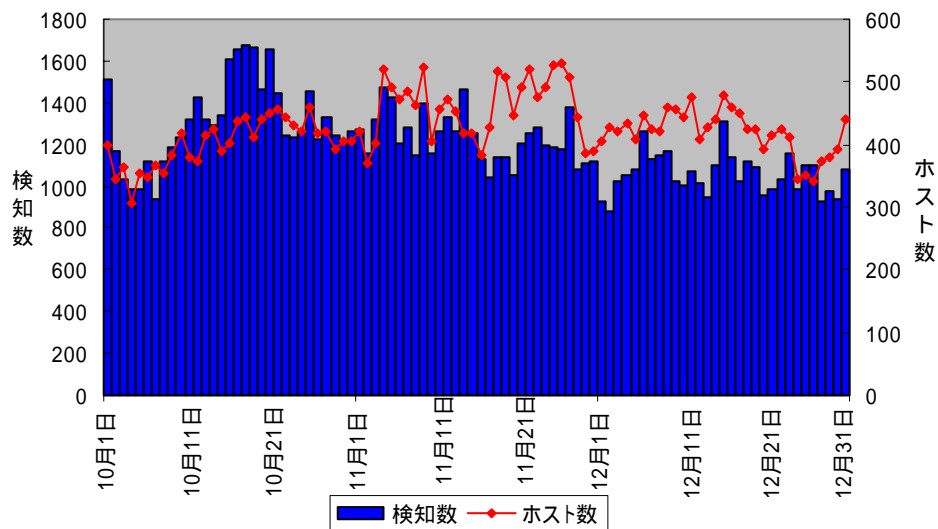


図3 第3/四半期における攻撃状況の推移

## ワームとDNS 攻撃が増加

攻撃手法別では、「ワーム」と「ポートスキャン」で全体の約 88%となった。前期と比べると、「ワーム」と「DNS 攻撃」が増加している。「DNS 攻撃」は、アメリカと中国を発信元とするものが多い。特定のホストを発信元とする攻撃が減少したことに伴い、「ポートスキャン」、「バックドア接続要求」、「Ping 攻撃」の件数は前期と比べると減少した。

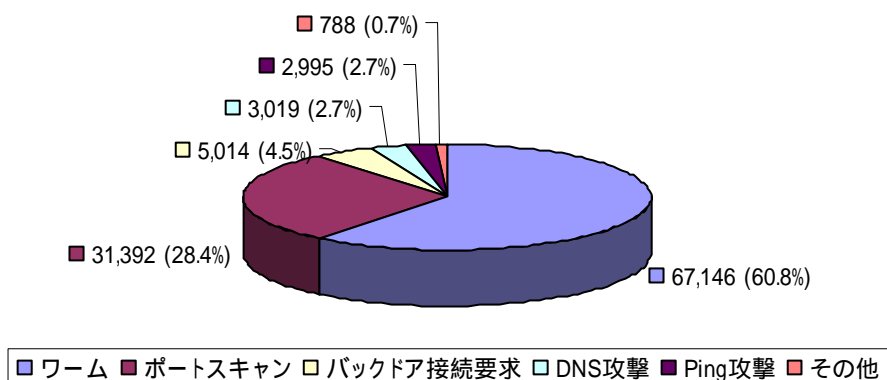


図 4 攻撃手法による分析

## 攻撃種別の分類

大分類	代表的なシグネチャ名
ワーム(Worm)	SQL SLAMMER worm
ポートスキャン (Scan)	Proxy attempt
	SYN FIN scan
	NULL scan
	nmap TCP
	FIN scan
	NMAP XMAS
	Window size of 55808 TCP Packet
バックドア接続要求 (BackDoor)	Window size of 55808(SYN) TCP Packet
	Sub7 v2.2 probe
DNS攻撃 (DNS)	Back Orifice2000
	DNS Hostname Overflow Attack
Ping攻撃 (ICMP)	DNS HINFOデコード
	named version attempt
	PING NMAP
	superscan echo
	redirect host
	redirect net
	Port sweep
	Portscan Detection Attack
Large ICMP Packet	
その他 (Others)	SYN Flood
	UDP Bomb
	Traceroute サービスの検出
	IPFragmentation
	Linux Traceroute
	IP Duplicate

## Blaster 及び Welchia ワームの活動状況

前期の8月に発生した Blaster ワーム及び Welchia ワームは、今期も引き続き、活動を継続していた。これらのワームは、ファイアウォールに対するアクセスを観測することで、その活動状況を推測することができる。図5にワームが使用する通信プロトコル（Blaster = TCP135 番ポート、Welchia = ICMP）について、発信元ホスト数と着信パケット数（件数）の推移を示す。

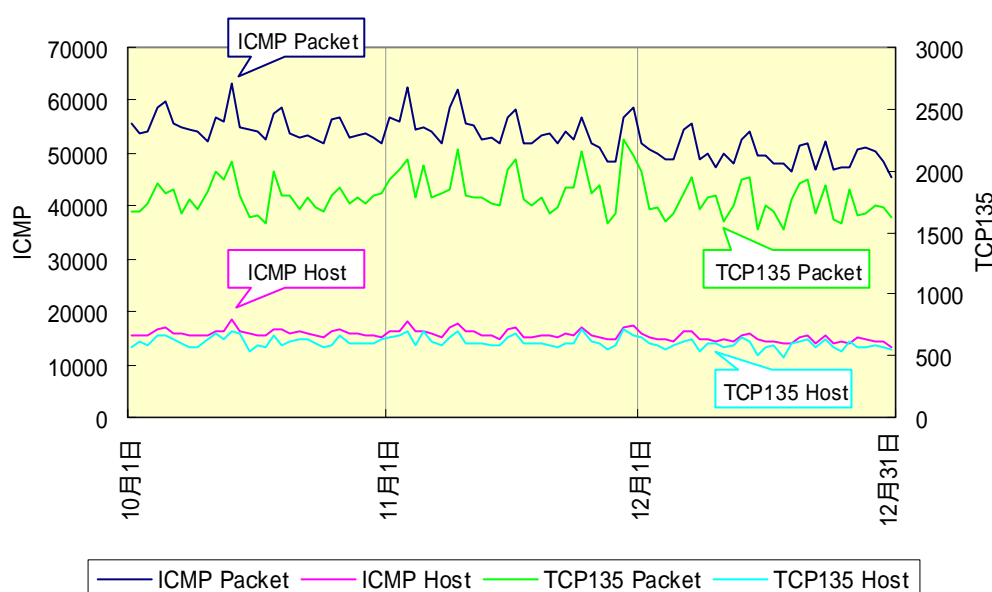


図5 ファイアウォールへのアクセス状況（日毎）

Welchia ワームは、2004 年 1 月 1 日に活動を停止する機能が組み込まれており、新年を迎えるのと同時に件数の減少が確認されている。

一方、Blaster ワームの活動は継続している。

### 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 @police」(<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。

さらに、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の促進や、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

警察庁では昨年 12 月に「国内の Slammer 及び Blaster ワームの感染活動に関する IP アドレス管理者への注意喚起について」([@police http://www.cyberpolice.go.jp/detect/pdf/H151222\\_worm.pdf](http://www.cyberpolice.go.jp/detect/pdf/H151222_worm.pdf))を行っており、今後、ワームの沈静化が期待される。

第 3/四半期における検知件数は、件数こそ減少することとなったが、発信元ホスト数が増加する結果となり、ワーム感染の拡大を物語っている。SQL Slammer ワームは、その発生からほぼ 1 年が経過しようとしているが、Blaster ワームと共に感染活動は継続している。2004 年 1 月 1 日以降、Welchia ワームの活動は停止するものの、亜種や新たなワームの発生に備えるためにも、セキュリティ対策の徹底が必要である。