

## 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 4 / 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 4 / 四半期分のデータによる

### 2 分析結果に見る特徴

#### 発信元は中国、米国、日本の順で多い

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 149 カ国からの攻撃を検知している。上位を占めるのは、中国、アメリカ合衆国及び日本であり、これら 3 カ国からの攻撃の検知件数だけで全体の約 68% を占めている。

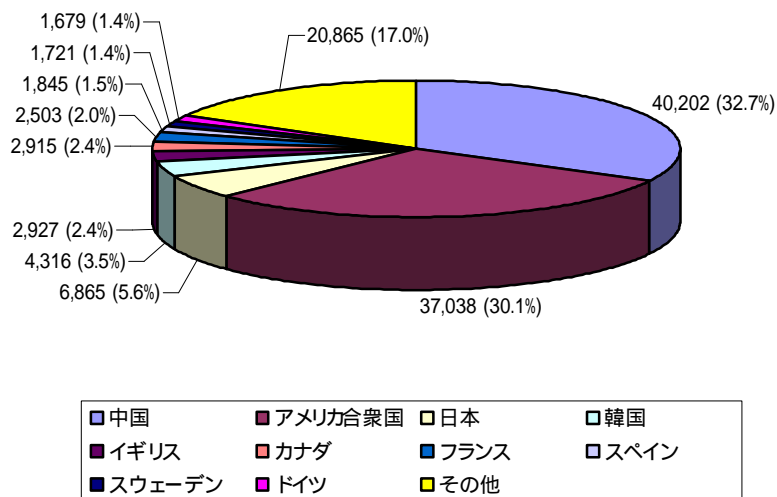
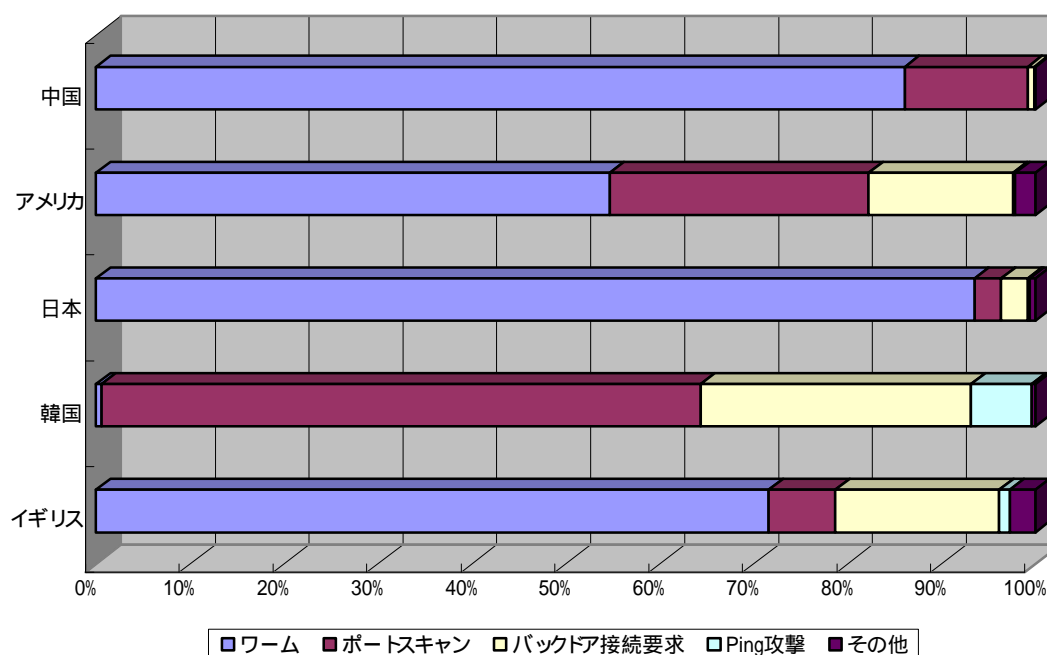


図 1 攻撃の発信元の国別分析

## 中国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	Ping攻撃	その他	合計
中国	34,627	5,260	261	46	8	40,202
	86.1%	13.1%	0.6%	0.1%	0.0%	100.0%
アメリカ	20,253	10,220	5,681	90	794	37,038
	54.7%	27.6%	15.3%	0.2%	2.1%	100.0%
日本	6,421	193	198	9	44	6,865
	93.5%	2.8%	2.9%	0.1%	0.6%	100.0%
韓国	24	2,754	1,243	277	18	4,316
	0.6%	63.8%	28.8%	6.4%	0.4%	100.0%
イギリス	2,097	207	510	33	80	2,927
	71.6%	7.1%	17.4%	1.1%	2.7%	100.0%

図2 国別攻撃手法

韓国を除き、各国共にワーム及びポートスキャンの件数が増加しており、中国のワームの増加率が特に大きくなっている。

韓国はポートスキャンが減少したが、「Sub7 v2.2 probe」の一時的な急増のために、バックドア接続要求の比率が増加している。

### 攻撃件数及び発信元ホスト数が増加

当期におけるアラートの検知件数の合計は、約 123,000 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 1,250 件、約 500 ホスト程度で推移している。

1 月 31 日から 2 月 2 日の 3 日間における検知数及びホスト数の増加は、バックドア接続要求の一時的な急増が原因である。また、2 月中旬より中国からのワームが増加し、総検知数及びホスト数が増加している。

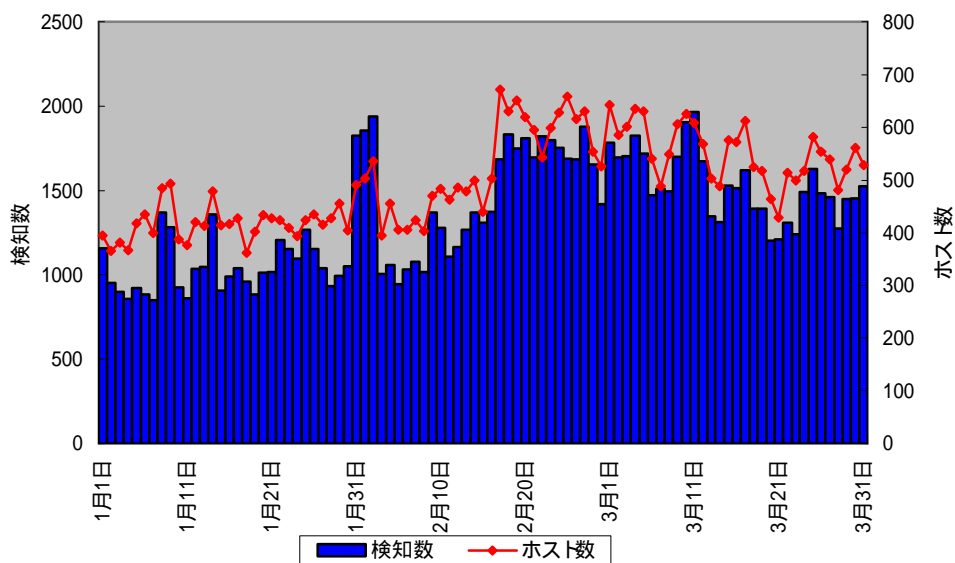


図3 第4/四半期における攻撃状況の推移

### ワームは増加、ポートスキャンは減少

攻撃手法別では、前期から引き続き「ワーム」が増加している。特定ホストを発信元とする攻撃が減少したため、前期に比べ「ポートスキャン」の件数が減少している。

Sinit あるいは Calypso と呼ばれるトロイの木馬が発信するパケットを、「バックドア接続要求」の「Sinit Discovery Packet」として検知するよう変更したために、前期に多かった「DNS 攻撃」はほとんど検知されていない。(前期は DNS 攻撃の「DNS Hostname Overflow Attack」として計上。)

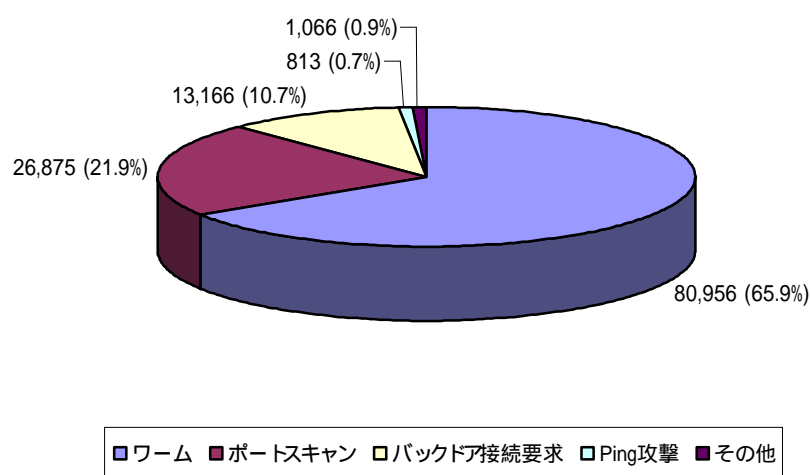


図 4 攻撃手法による分析

### 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
ワーム	SQL SLAMMER worm	Ping攻撃	superscan echo
ポートスキャン	Proxy attempt		redirect host
	Window size of 55808(SYN) TCP Packet		redirect net
	synscan portscan	その他	Traceroute サービスの検出
	Window size of 55808 TCP Packet		Linux Traceroute
nmap TCP	Source Port 20 to <1024		
バックドア 接続要求	Sub7 v2.2 probe		Bind 4 nslookupComplain Format bug
	Sinit Discovery Packet		ICMP Traceroute
	BACKDOOR hack-a-tack attempt	IP Fragmentation	
	IP Unknown Protocol	UDP Bomb	
	BackOrifice2000		DNS HINFOデコード

## ファイアウォールに対するアクセス

IDS が監視するネットワーク内に配置された、ファイアウォールにおける宛先ポート別の着信パケット数(件数)の推移(累積件数の上位 5)を図 5 に示す。

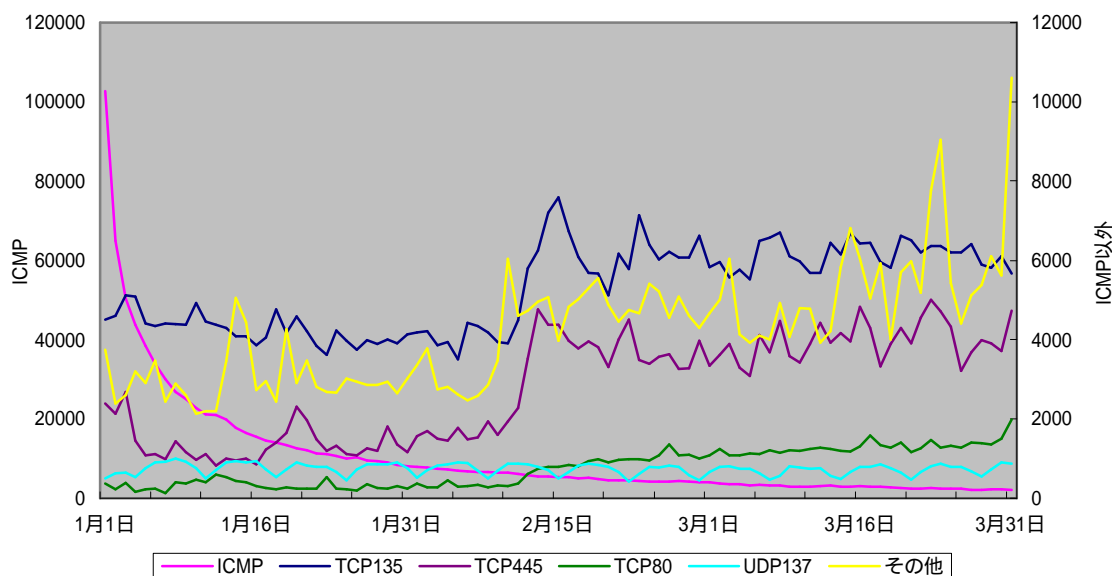


図 5 ファイアウォールへのアクセス状況(日毎)

昨年 8 月に発生した Welchia ワームの活動停止期限である 2004 年 1 月 1 日以降、ICMP の件数が急速に減少している。しかし、2 月 12 日の Welchia.B ワームの発生に伴い、TCP135、TCP445、TCP80 に対するアクセスが増加している。

### 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

第4/四半期は、ポートスキャンの件数が減少したものの、SQL Slammer ワームが増加したために、総検知件数及びホスト数が増加する結果となった。特に中国からの SQL Slammer ワームが著しく増加したが、国内やアメリカ等からの検知も増加している。SQL Slammer ワームは、その発生からほぼ1年が経過したが、一向に減少する気配を見せない。2004年1月1日以降、Welchia ワームの活動は停止し始めているが、同ワームの亜種が2月中旬に発生している。当期の SQL Slammer 及び Welchia ワームの動向を見ると、過去の脆弱性を未だに修正せずに運用しているコンピュータが相当数に上るものと推定される。当期は Welchia ワーム及びその亜種を含め、過去に公表された複数の脆弱性を悪用するウイルスが増加傾向にある他、Mydoom や Beagle、Netsky 等のウイルスが蔓延することとなった。オペレーティングシステム(OS)や各種アプリケーションに対する修正プログラムの適用や、ウイルス対策ソフトウェアの導入及び定期的な定義ファイルの更新といった基本的なセキュリティ対策の徹底が必要である。