

平成19年上半期におけるインターネット治安情勢について

インターネットに接続したコンピュータに対する無差別なサイバー攻撃は高水準にとどまっています。更に、昨年末に確認されたワームの活動と思われる攻撃が継続的に続くなど、攻撃に利用される手口は、一部に変化が見られます。また、インターネットを介した攻撃者の命令に基づき動作するプログラムであるボットも継続的に高水準で活動をしており、感染台数等に大きな減少傾向は見られません。

1 はじめに

警察庁では、国民生活又は社会経済活動に重大な影響を及ぼすおそれのある情報システムに対する犯罪を未然に防止し、あるいは被害の拡大防止を図るために必要となる情報を収集する手段のひとつとして、全国の警察施設のインターネット接続点におけるアクセス情報等を観測・分析し、情報セキュリティの向上に資する情報の提供等を実施しています。

本資料は、サーバの管理者を中心としたインターネット利用者のセキュリティ対策の参考としていただくため、インターネットに接続するだけで発生するリスクについて、平成19年1月から6月までの上半期に警察庁がインターネットを直接観測することにより把握した情報を取りまとめ公表するものです。

2 定点観測の結果

全国の警察施設のインターネット接続点¹に設置してあるファイアウォール²と侵入検知装置³の記録を全般的に分析したものを以下で紹介いたします。

2.1 全般的なアクセス状況：無差別な攻撃は高水準で横ばい

今期は、大規模に感染したワーム型ウイルスの発生がなかったこともあり、インターネットに接続されたコンピュータに対する無差別なサイバー攻撃は横ばいでした。

今期、警察庁のファイアウォールに対する総アクセス件数は約 2,830,000 件で、前期と比較して約 5%減少しましたが、前年同期比較では約 8%増加しました。また、警察庁で侵入検知装置を利用して検知したワーム等の活動は約 237,000 件で、前期と比較して約 4%増加しましたが、前年同期比較では約 5%減少しました。

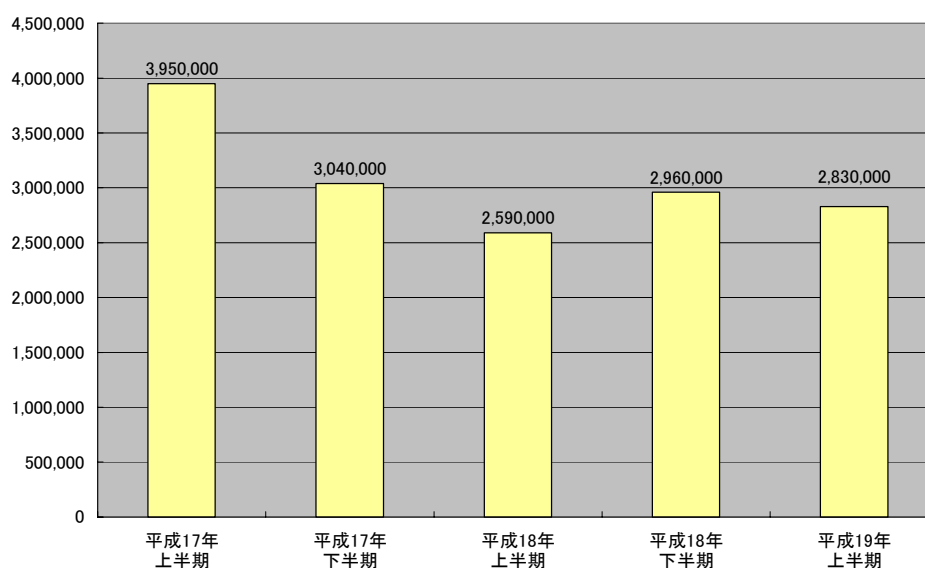


図 2-1 ファイアウォールへのアクセス件数の推移

1 日本国内の 57 の拠点の観測記録をもとに分析しています。

2 集計は、incoming のトラフィックのみ対象とし、outgoing のトラフィックは対象としていません。

3 平成 19 年 6 月 30 日現在、364 種類のシグネチャが登録されています。

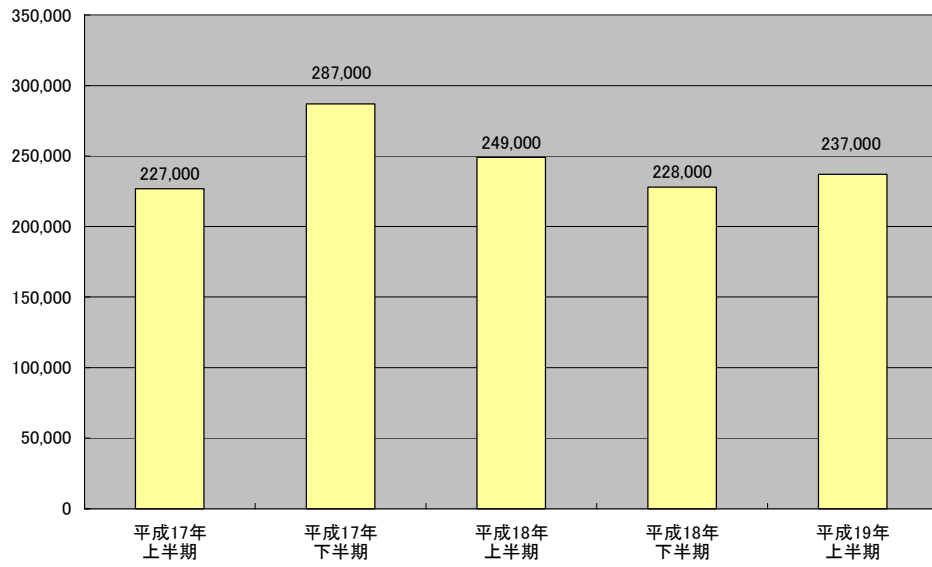


図 2-2 侵入検知装置でのアラートの検知数の推移

2.2 宛先ポート別の推移

警察庁のファイアウォールに対するアクセスのうち、ICMP(Echo Request)、1027/udp、2967/tcp へのアクセスが大幅に増大し、特に 2967/tcp へのアクセスは、前期と比較して約 678%増加しました。2967/tcp へのアクセスは、昨年 12 月中旬に確認されたシマンテック社のセキュリティ製品の脆弱性（昨年 5 月に公表されている）を突くワームが利用するもので、アジア地域を発信元とするものが多く、日本国内からのアクセスも多いものでした⁴。なお、ICMP(Echo Request)はネットワークの疎通調査等に、1027/udp は Windows の Messenger サービスを利用したスパムの通信に利用されることが多いものです。

また、これまで上位を占めてきた 445/tcp と 139/tcp へのアクセスは前期比で 50%前後減少しました。

	平成17年 上半期	平成17年 下半期	平成18年 上半期	平成18年 下半期	平成19年 上半期
135/tcp	8,022	4,823	4,493	5,365	4,691
ICMP(Echo Request)	724	884	1,232	1,975	3,707
445/tcp	4,588	4,236	2,679	2,909	1,471
1026/udp	257	119	431	784	840
1434/udp	557	734	633	578	573
1027/udp	200	89	143	313	539
2967/tcp	-	-	-	64	498
139/tcp	1,117	1,776	1,130	1,067	457
22/tcp	212	273	335	349	407
1433/tcp	1,247	959	889	671	404

表 2-1 宛先ポート別の1日あたりのアクセス件数の推移

⁴ 詳細は、「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 18 年度第 3 / 四半期）、（平成 18 年度第 4 / 四半期）及び（平成 19 年度第 1 / 四半期）をご覧ください。

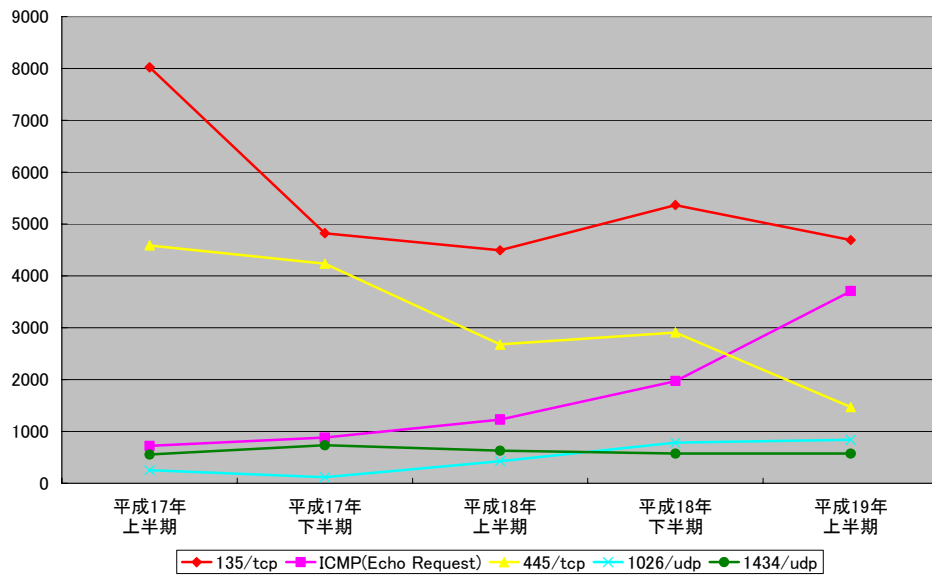


図 2-3 宛先ポート別の1日あたりのアクセス件数の推移(1位から5位)

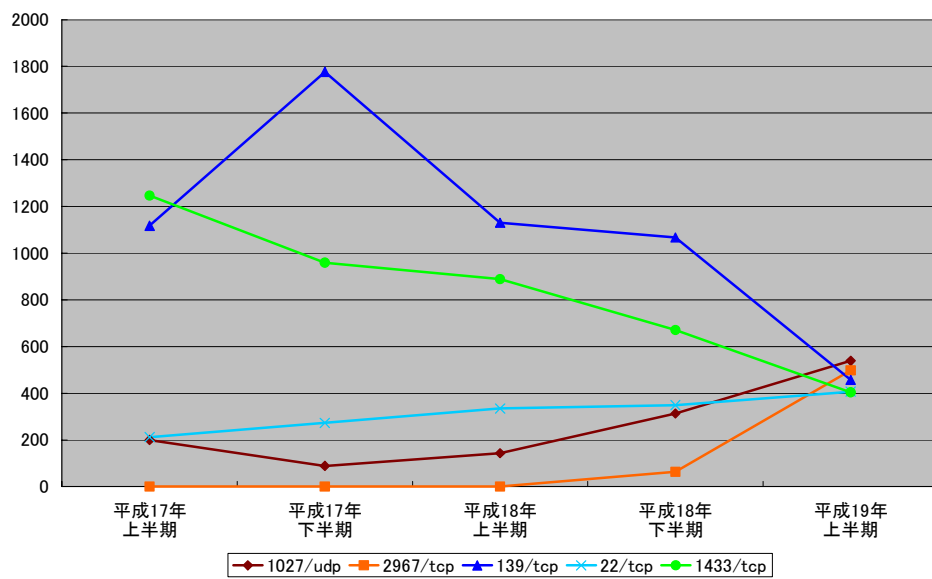


図 2-4 宛先ポート別の1日あたりのアクセス件数の推移(6位から10位)

2.3 発信元（国／地域）別の推移

警察庁のファイアウォールへのアクセス件数が多い発信元の国／地域に大きな変動はありませんでしたが、日本国内からのアクセスが前期と比較すると約26%減少しました。

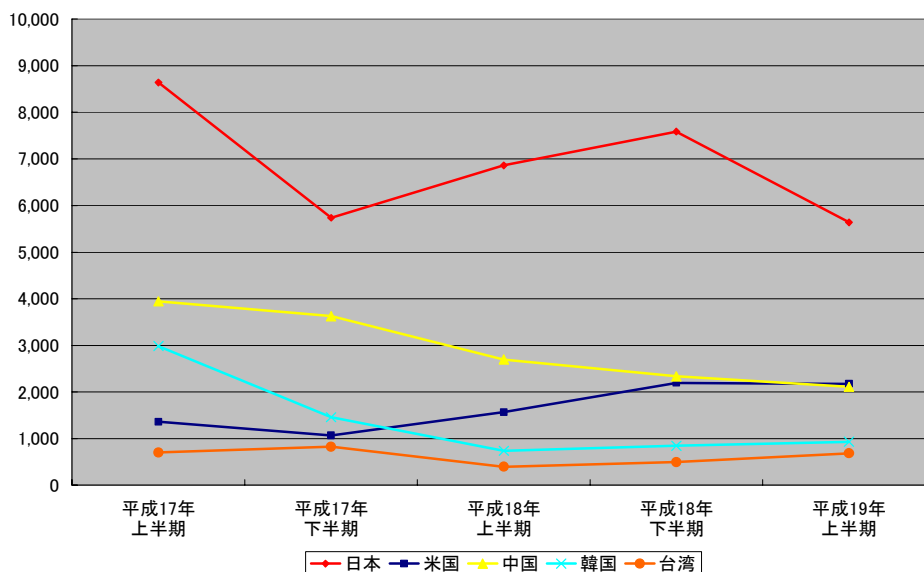


図 2-5 発信元(国／地域)別の1日あたりのアクセス件数の推移(1位から5位)

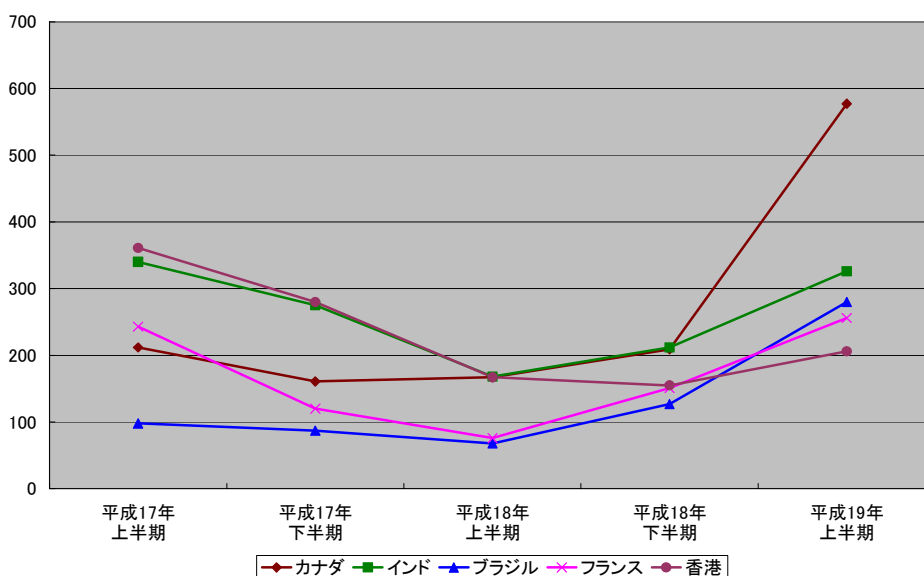


図 2-6 発信元(国／地域)別の1日あたりのアクセス件数の推移(6位から10位)

	平成17年 上半期	平成17年 下半期	平成18年 上半期	平成18年 下半期	平成19年 上半期
日本	8,642	5,737	6,862	7,586	5,640
米国	1,358	1,069	1,566	2,195	2,175
中国	3,945	3,627	2,699	2,334	2,112
韓国	2,987	1,457	737	845	931
台湾	702	824	395	496	684
カナダ	212	161	167	209	577
インド	340	275	168	212	326
ブラジル	98	87	68	127	280
フランス	243	120	76	151	256
香港	361	280	167	155	206

表 2-2 発信元(国／地域)別の1日あたりのアクセス件数の推移

2.4 攻撃手法別の推移

侵入検知装置を利用して検知したアラート⁵のうち、「Scan」が大幅に増加し、前期と比較すると約2倍に増加しました。なお「Scan」の多くは「Proxy attempt」が占めていました。

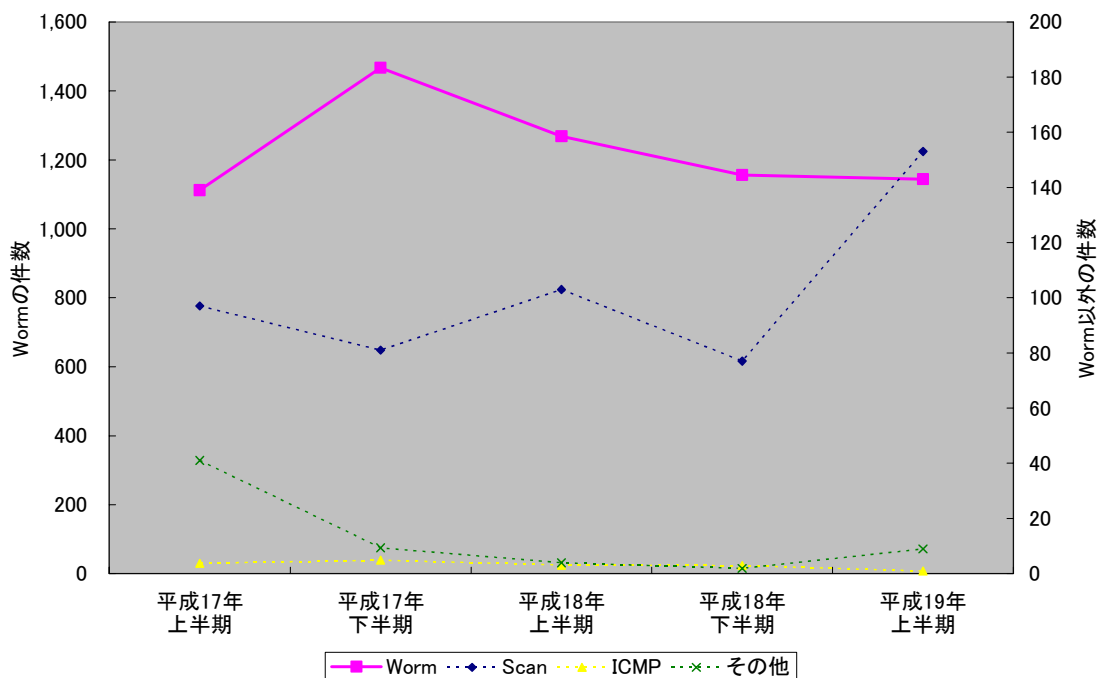


図 2-7 攻撃手法別の1日あたりのアラート件数

	平成17年上半期	平成17年下半期	平成18年上半期	平成18年下半期	平成19年上半期
Worm	1,112.0	1,467.0	1,268.0	1,156.0	1,144.0
Scan	97.0	81.0	103.0	77.0	153.0
ICMP	3.7	4.9	3.1	2.9	0.9
その他	41.0	9.3	3.9	1.9	8.9

表 2-3 攻撃手法別の1日あたりのアラート件数

⁵ 侵入検知装置で検知された各シグネチャは、以下のとおりに分類しています。

Worm : SQL Slammer

Scan : Proxy attempt, Port sweep, SYN FIN scan, FIN scan, NMAP TCP, NMAP XMAS, NMAP Fingerprint, Portscan Detection Attack, Window size of 55808 (SYN) TCP Packet

ICMP : Superscan Echo, redirect host, redirect net, Ping Flooding

2.5 サーバコンピュータに対する DoS 攻撃（SYN flood 攻撃）

ファイアウォールに送信された SYN/ACK パケットを分析することにより、DoS 攻撃の一手法である SYN flood 攻撃の兆候について観測を行ったところ、SYN flood 攻撃の検知件数は約 25,900 件となり、前期と比較して約 67%減少しました。

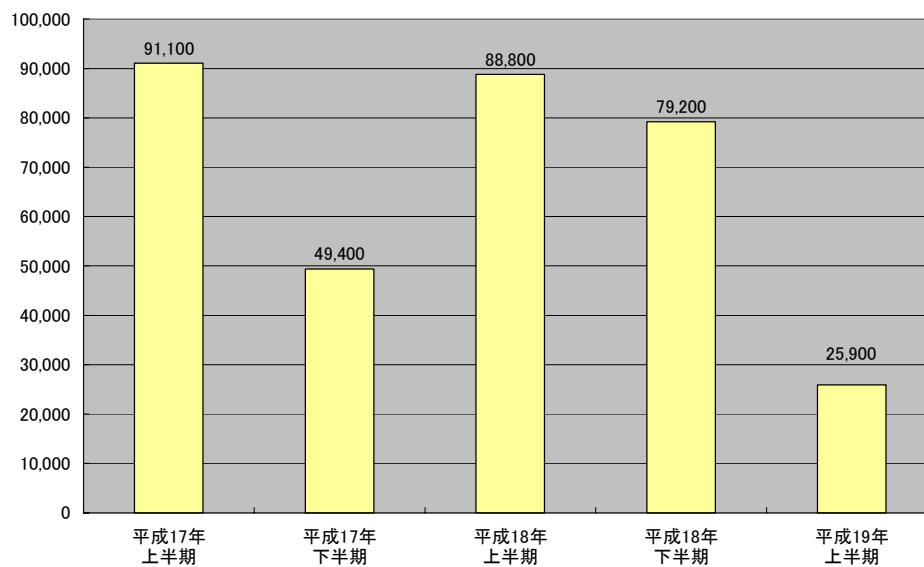


図 2-8 DoS 攻撃(SYN flood 攻撃)の推移

2.6 国内からの攻撃

今期、警察庁で侵入検知装置を利用して検知したワーム等の活動のうち、日本国内のコンピュータからのものは約 5,200 件あり、前期と比較して約 22%減少しました。また、ファイアウォールへの日本国内のコンピュータからのアクセス件数は約 1,020,000 件あり、前期と比較して約 27%減少しました。

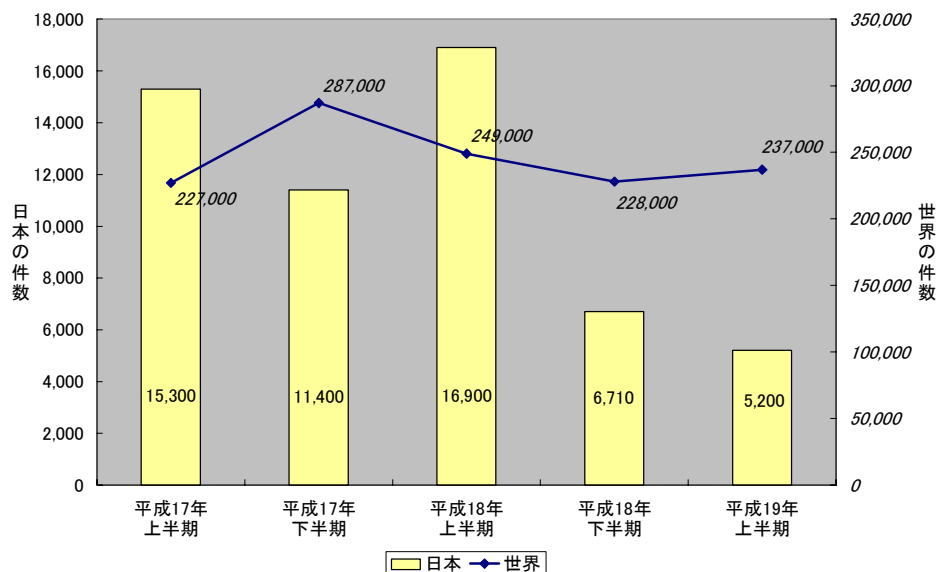


図 2-9 日本国内からのアクセスへのアラート件数の推移

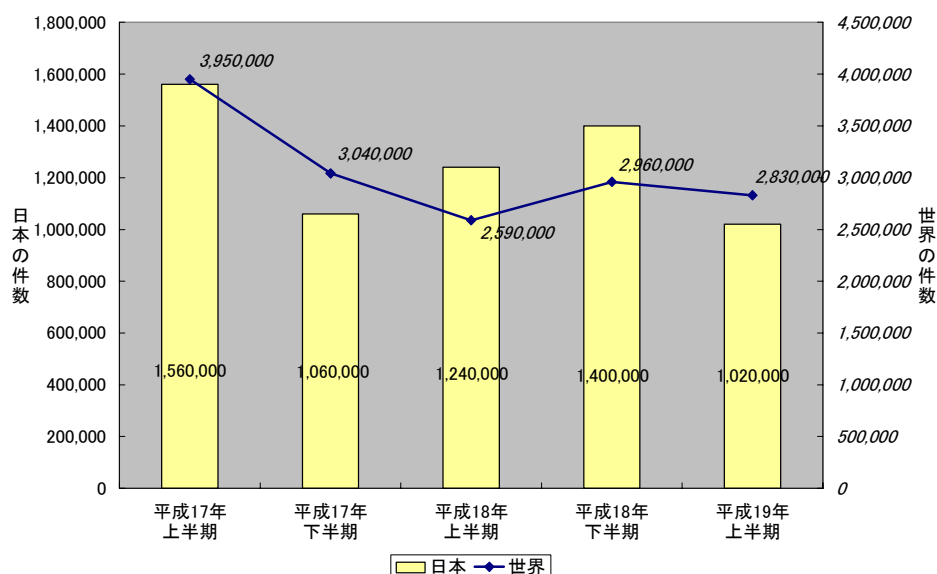


図 2-10 日本国内からのファイアウォールへのアクセス件数

3 ボットネットの観測結果

ボットは不正プログラム的一种で、プログラムの脆弱性を悪用するなどして他人のコンピュータに感染し、コンピュータを遠隔操作できる状態になったことを攻撃者に伝えて命令を待ちます。攻撃者はボットに感染した多数のコンピュータを一斉に操作できるようにネットワーク化した「ボットネット」を構築し、DoS 攻撃等を行うための道具として利用しています。日本では、ボットネットを利用した検挙事例はありませんが、海外では、ボットネットを使用して、他のシステムのサービスを利用できなくさせた人物、又は自分自身の Web サイトを宣伝するために迷惑メールを数千万通も送った人物等が複数検挙された事例⁶があります（米、6月）。ボットは DoS 攻撃、迷惑メールの大量送信のほか、個人情報等の窃取、フィッシング詐欺等に利用されるおそれがあります。以下では、警察庁で実施したボットネットの観測結果を紹介します。

3.1 ボットネットは増加

今期、警察庁で観測したボットネットは 598 個で、前期に比べ約 26%増加しました。そのうち今期に新たに把握したものが 348 個ありました。今期、最も大きなボットネットは約 10 万台のボットから構成されていました。

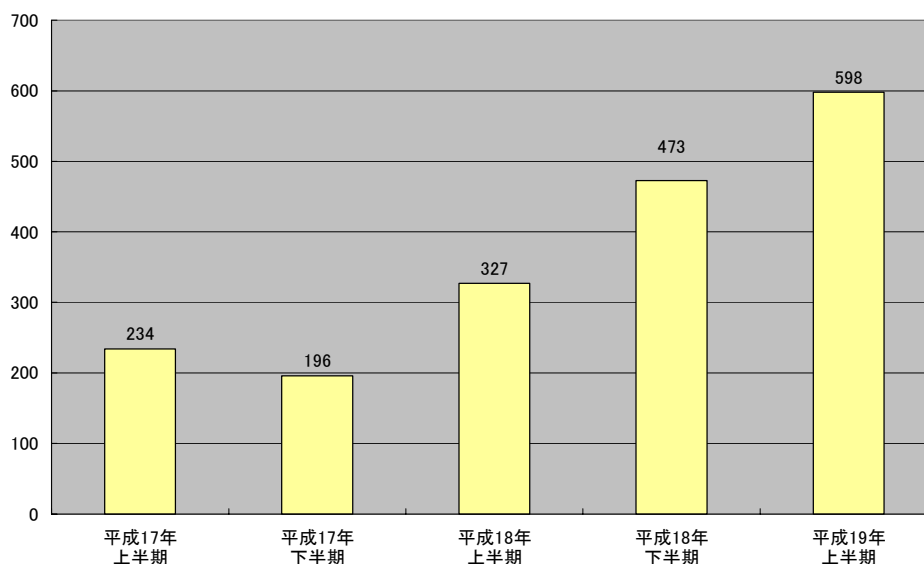


図 3-1 ボットネットの個数の推移

⁶ <http://www.fbi.gov/page2/june07/botnet061307.htm>

3.2 個々のボットネットは小規模化

一つのボットネットに接続されているボットに感染したコンピュータの平均台数は、今期約 1,414 台で、前期の 3,422 台と比べ、約 59%減少しています。

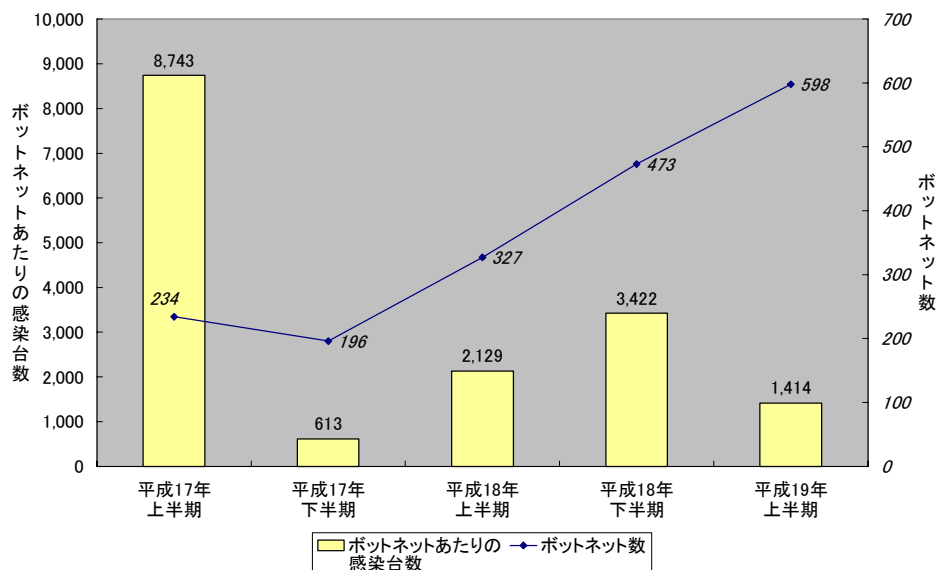


図 3-2 ボットネットあたりの感染台数の推移

	平成17年 上半期	平成17年 下半期	平成18年 上半期	平成18年 下半期	平成19年 上半期
ボットネット数	234	196	327	473	598
感染台数を調査できた	147	86	177	191	346
ボット感染台数	1,285,247	52,723	376,823	653,664	489,274
ボットネットあたりのボット感染台数	8,743	613	2,129	3,422	1,414

表 3-1 ボットネットあたりの感染台数の推移

3.3 ボットネットからの DoS 攻撃は減少

警察庁で観測しているボットネットにおいて、指令サーバから出される命令の内容を観測したところ、DoS 攻撃に関する命令の総数は 6,441 件で、前期に比べて約 55%減少しているものの、SYN flood 攻撃に関する命令が前期より約 102%増加して、4,836 件となっています。

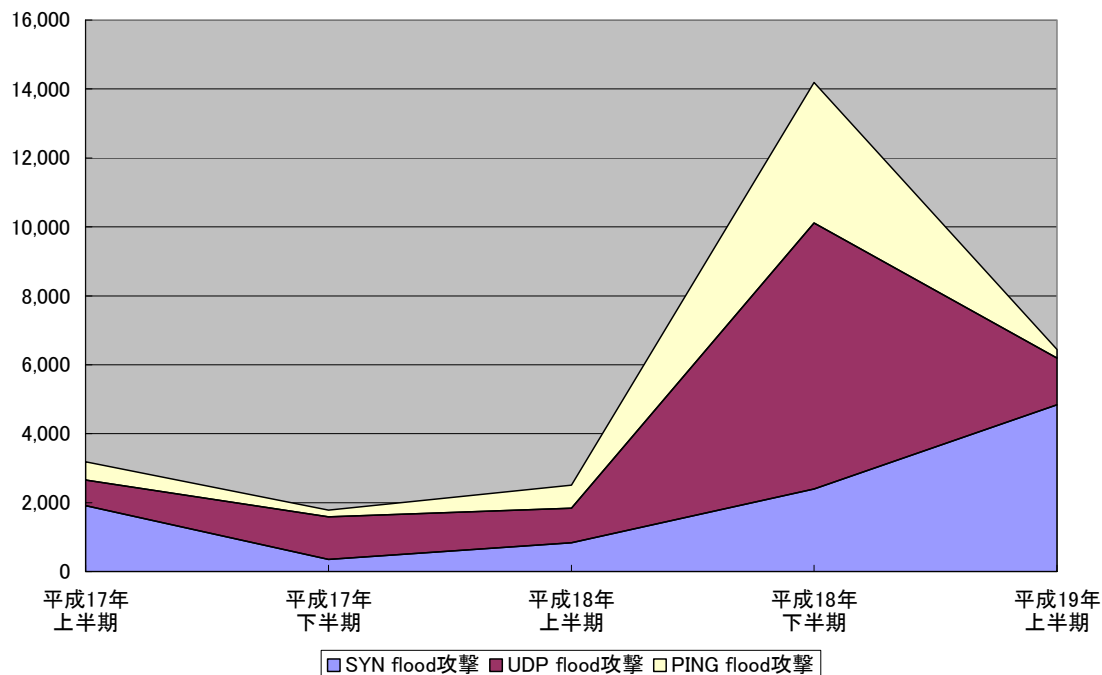


図 3-3 ボットネットでの DoS 攻撃命令数の推移

	平成17年 上半期	平成17年 下半期	平成18年 上半期	平成18年 下半期	平成19年 上半期
SYN flood攻撃	1,918	355	843	2,396	4,836
UDP flood攻撃	743	1,239	993	7,708	1,363
PING flood攻撃	528	196	667	4,081	242
総計	3,189	1,790	2,503	14,185	6,441

表 3-2 ボットネットでの DoS 攻撃命令数の推移

3.4 活発な感染・ダウンロード活動

ボットネットでは、指令サーバから感染しているコンピュータに対して、様々な命令が出されます。そのうち、ボットの感染端末の拡大や機能の更新に関係があると思われる感染命令及びダウンロード命令について分析したところ、今期の1日あたりの平均命令数は、感染命令が約28回、ダウンロード命令が約42回あり、感染活動や感染したコンピュータにボットの更新プログラムを始めとした何らかのデータを送りつける活動が頻繁に行われていることが窺えました。

また、感染命令の内容を分析したところ、マイクロソフト社のWindowsのサービスの脆弱性を狙ったと考えられるもの(445/TCP、135/TCP、139/TCPを対象としたもの)が約65%と依然過半数を占めていますが、前期と比べて減少傾向でした。一方、Microsoft SQL Serverのソフトの脆弱性を狙ったもの(1433/TCPを対象としたもの)、遠隔操作ソフトの脆弱性を狙ったもの(5900/TCPを対象としたもの)、シマンテック社のセキュリティ対策ソフトの脆弱性を狙ったもの(2967/TCPを対象としたもの)への攻撃は、合わせて約24%であり、前期より約12ポイント増加しています。また、その他のポートとしては80/TCP、1025/TCPへの攻撃も観測されており、ボットの感染活動が今まで以上に多様化していることを示しています。

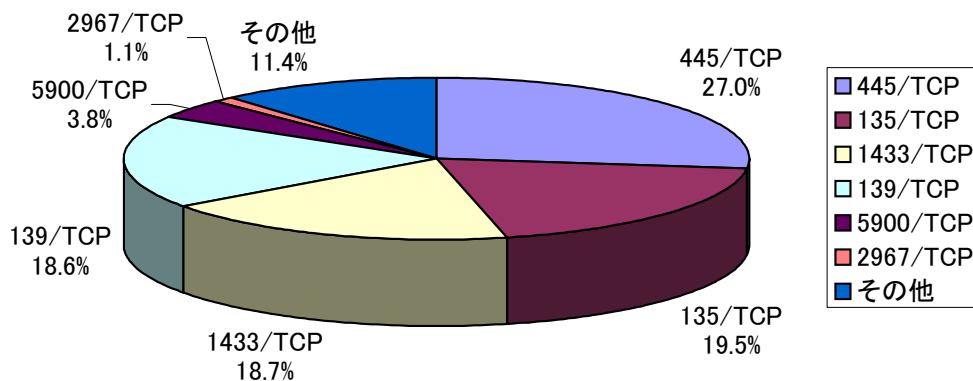


図 3-4 感染活動時の利用ポート内訳

3.5 国内のボットの感染コンピュータ数は横ばい

今期、警察庁で観測したボットに感染したコンピュータの台数は 489,274 台で、前期の 653,664 台と比べ約 25%減となっています。このうち日本に存在すると考えられるものは 32,064 台に上り、前期の 36,292 台と比べ約 12%減となっています。

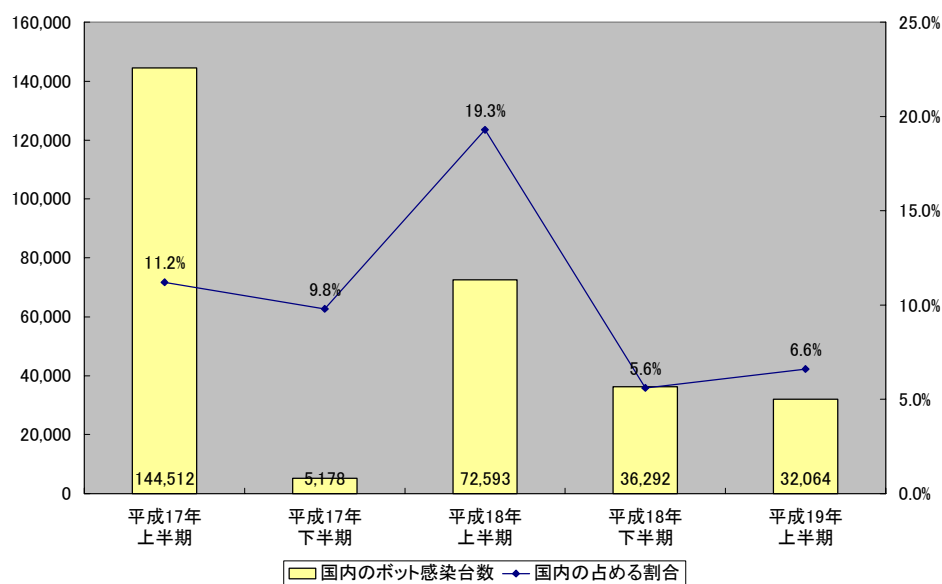


図 3-5 国内のボット感染台数の推移

	平成17年 上半期	平成17年 下半期	平成18年 上半期	平成18年 下半期	平成19年 上半期
国内のボット感染台数	144,512	5,178	72,593	36,292	32,064
世界のボット感染台数	1,285,247	52,723	376,823	653,664	489,274
国内の占める割合	11.2%	9.8%	19.3%	5.6%	6.6%

表 3-3 国内のボット感染台数の推移

4 情報セキュリティの向上のために

インターネットに接続したコンピュータに対する無差別なサイバー攻撃は高水準のまま横ばいの状況ですが、宛先ポートの一部に変化が見られたように、攻撃の手口には、新しいものが見受けられます。また、ボットは、感染台数に増加は見られませんでした。感染端末から他のコンピュータを攻撃する手法の DoS 攻撃の一種の SYN flood 攻撃の増加が観測されています。また、個々のボットネットに接続されている感染端末の数が減少し、ボットネットの数が増加していることから、ボットネットの撲滅がより困難となるよう変化している可能性があります。しかしながら、幸いなことに、これらの攻撃や感染の起点として利用されていると思われるソフトウェア等の脆弱性は必ずしも未知のものではありません。

そこで、インターネットの利用者の皆さんには、自らの情報資産を守るためのみならず、ボットに代表されるような、意図せず攻撃者に荷担してしまう類の脅威にも対応できるよう、ソフトウェア等のセキュリティ更新プログラムの適切な適用やウイルス対策ソフトの適切な運用に代表される一般的なセキュリティ対策を少なくとも講じていただくことが非常に重要となります。

また、企業等のサーバ管理者等の皆さんが、情報資産に対する様々な被害を未然に防いだり、軽減したりするにあたって、従来と異なる攻撃手口を利用した攻撃を迅速に発見するために、通信記録等を定期的に確認し、従来と異なる状況や公知の攻撃兆候をできるだけ迅速に把握することが特に重要となります。

警察庁では、今後とも、様々な機会を捉えて、情報セキュリティ対策に資する情報を積極的に提供し、安心して利用できる安全なインターネット社会の確立に努めて参ります。