

情報技術解析平成 20 年報

# 別冊資料

平成 20 年のサイバーフォースセンターでの  
観測結果について

平成 21 年 2 月

警察庁情報通信局情報技術解析課

## 別冊目次

1	はじめに.....	2
2	インターネットにおける脅威の移り変わり .....	3
3	警察庁のインターネット定点観測の経緯.....	4
4	ファイアウォールに対するアクセス状況.....	5
4.1	観測結果の推移.....	5
4.2	宛先ポート別の推移.....	6
4.3	発信元（国/地域）別の推移.....	9
4.4	国内からのアクセス状況 .....	10
5	不正侵入検知システムによる検知状況 .....	12
5.1	攻撃手法別の推移 .....	13
5.2	発信元（国/地域）別の推移.....	14
5.3	国内からのアクセス状況 .....	15
6	サーバコンピュータに対する DoS 攻撃（SYNflood 攻撃） .....	16
6.1	DoS 攻撃検知件数.....	16
6.2	攻撃対象ポート別の検知件数 .....	17
7	ボットネットの観測結果.....	18
7.1	ボットネット観測数.....	18
7.2	ボットネットあたりの感染台数.....	19
7.3	国内のボット感染台数 .....	20
7.4	ボットネットの感染活動 .....	21
7.5	ボットネットからの DoS 攻撃.....	23
8	DNS サーバの動向.....	24
8.1	DNS サーバへの外部からの再帰的問い合わせ.....	25
8.2	DNS サーバのクエリポートの状況 .....	26
8.3	DNS サーバのセキュリティ .....	26
9	情報セキュリティ対策の向上のために .....	27
10	付録.....	29
10.1	特徴的なアクセス状況.....	29
10.2	ファイアウォールに対するアクセス件数 TOP50（ポート別） .....	33
10.3	ファイアウォールに対するアクセス件数 TOP50（国/地域別） .....	34

## 平成 20 年のサイバーフォースセンターでの観測結果について

### 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、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を提供しています。

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、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。

本年報が、安全・安心なインターネット社会への取り組みの一助となれば幸いです。

また、現在、警察庁ではインターネット定点観測システムの更新作業を行っており、現行システムでのインターネット定点観測は平成 20 年度限りとなります。平成 21 年度からは、新システムでの観測の運用が開始されます。これまでの観測がひとつの節目を迎えることから、平成 20 年の年報では警察庁が定点観測の分析結果の公開を開始した平成 14 年 7 月から平成 20 年 12 月までに観測した「インターネット定点観測」システムによる分析結果を取りまとめ、併せて公表しています。これまでに蓄積した全観測結果を見ることにより、インターネット情勢の変化や全体的な傾向の移り変わりを知る一助となれば幸いです。

## 2 インターネットにおける脅威の移り変わり

観測を開始した平成14年以降の脅威を見ると、平成15年に「SQL Slammer」ウイルスが世界的規模で感染数を増やし、韓国や米国では、同ウイルスの影響によりネットワークトラフィックが増大し、数時間にわたりインターネットサービスがダウンするという被害をもたらしました。同年には、「MSBlaster」等のネットワーク感染型ウイルスも猛威を振るいました。平成16年には、「Netsky」や「MyDoom」等のメール大量送信型ウイルスが出現し、ボットネットの被害が顕著に現れるようになりました。平成17年には、改ざんされたWebサイトを閲覧するだけでウイルスに感染する被害やSQLインジェクション攻撃による被害が表面化した年でもあります。平成18年は、P2Pネットワーク内で感染を広げる「Antinny」ウイルスの影響により、大規模な情報漏洩事案が多数発生していることについて、官房長官が「Winny」を介した情報漏洩について記者発表を行うなど、大きな社会問題になりました。P2Pネットワーク内への情報漏洩は現在も、後を絶たない状況が続いており、企業・組織に甚大な被害をもたらしています。

近年では警察庁において、USBメモリを経由して感染を広げるウイルスの活動、SQLインジェクションによるホームページの改ざんや情報漏洩、メールによる標的型攻撃等が確認されており、攻撃手法はより巧妙なものへと変化しています。また、システムの脆弱性に対する攻撃もより迅速なものになっている傾向が見られ、警察庁においてMicrosoftからOSの更新プログラムが公開された3日後には、この脆弱性を悪用した可能性があるアクセスの増加が観測されています。

### 3 警察庁のインターネット定点観測

定点観測は、全国の警察施設のインターネット接続点<sup>1</sup>に対するアクセス情報等を観測・分析することにより、インターネット上の「治安情勢」を直接把握し、観測・分析した情報を迅速に提供することを目的として運用を開始しました。インターネット定点観測は、不正侵入検知システム<sup>2</sup>の運用を皮切りに開始し、その後、ファイアウォール<sup>3</sup>に到達するパケットの集計、DoS 攻撃の被害を観測するシステム、ボットネットの動向を観測するシステムを新たに追加しました。

本資料の各システムの集計期間は以下のとおりです。

表 3-1 観測別の集計期間

観測名	集計期間
不正侵入検知	平成 14 年 7 月 から 平成 20 年 12 月
ファイアウォール	平成 15 年 7 月 から 平成 20 年 12 月
DoS 攻撃被害	平成 15 年 7 月 から 平成 20 年 12 月
ボットネット	平成 17 年 1 月 から 平成 20 年 12 月

<sup>1</sup>日本国内の複数の観測記録をもとに 1IP ごとに換算し分析しています。

<sup>2</sup>平成 21 年 1 月 31 日現在、387 種類のシグネチャが登録されています。

<sup>3</sup>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ません。

## 4 ファイアウォールに対するアクセス状況

### 4.1 観測結果の推移

ファイアウォールに対するアクセスは平成15年をピークに減少傾向が続いていますが、無差別なサイバー攻撃は高い水準で推移しています。平成15年のデータが突出している原因は、同年に大流行した「Welchia」ウイルスによるものと考えられます。

平成20年は前年と比較して一日・1IPあたり、約8.7件（約4%）減少したものの、ほぼ同水準で推移しています。

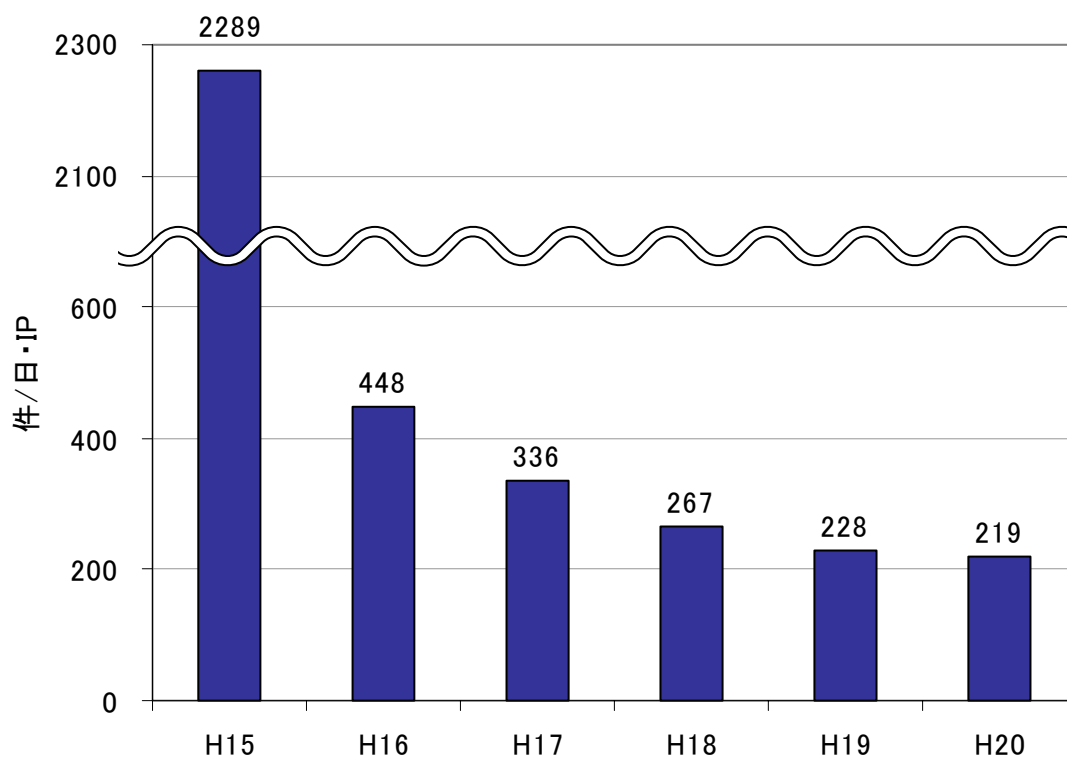


図 4-1 ファイアウォールに対するアクセス件数の推移

## 4.2 宛先ポート別の推移

ファイアウォールに対するアクセスの宛先ポート別では、Echo Request（以降、「8/ICMP」という。）が一日・1 IPあたり約 229 件と観測期間全体で最も多く、以下、135/TCP、445/TCP、139/TCP、1433/TCP と続いています。

観測期間全体で見ると、最も特徴的なものとして、平成 15 年 8 月から平成 16 年 1 月の間に、8/ICMP に対するアクセスが爆発的に増加しました。このアクセスは、「MSBlaster」ウイルスの亜種である「Welchia」ウイルスによるものと考えられます。平成 16 年 1 月以降から急激に減少していますが、この原因として、同ワームが平成 16 年 1 月 1 日以降に感染活動を停止し、自身をアンインストールするようプログラムされているためと考えられます。

平成 17 年以降は、Windows の共有サービス等で使用されている 135/TCP、139/TCP、445/TCP に対するアクセスが減少傾向にあります。これは、Windows のファイアウォール機能が初期設定で有効となっているためと考えられます。

Messenger スパムの通信に使用されている 1026/UDP、1027/UDP に対するアクセスは平成 17 年以降増加する傾向にあります。

1434/UDP、4899/TCP、80/TCP は、観測期間全体で見ると減少傾向にあります。

平成 20 年は、135/TCP が一日・1 IPあたり約 73.9 件と最も多く以下、8/ICMP、1026/UDP、1027/UDP、1433/TCP と続いており、前年と比較して一日・1 IPあたり、8/ICMP が約 21.3 件（約 41%）、445/TCP が約 8.2 件（約 46%）、139/TCP が約 3.3 件（約 53%）それぞれ減少したものの、1433/TCP が約 5.7 件（約 73%）増加しました。

平成 20 年 10 月 24 日に Microsoft から Microsoft Windows 製品の Server サービスの脆弱性に対する OS の更新プログラム (MS08-067) が公開されましたが、この脆弱性を悪用した攻撃の可能性のある 445/TCP へのアクセスの増加が 3 日後の 10 月 27 日に観測されており<sup>4</sup>、現在も増加傾向にあります。

---

<sup>4</sup> <http://www.cyberpolice.go.jp/detect/pdf/20081112.pdf> 「我が国におけるインターネット治安情勢について(平成 20 年 10 月期)」 4P、「445/TCP」グラフ参照。

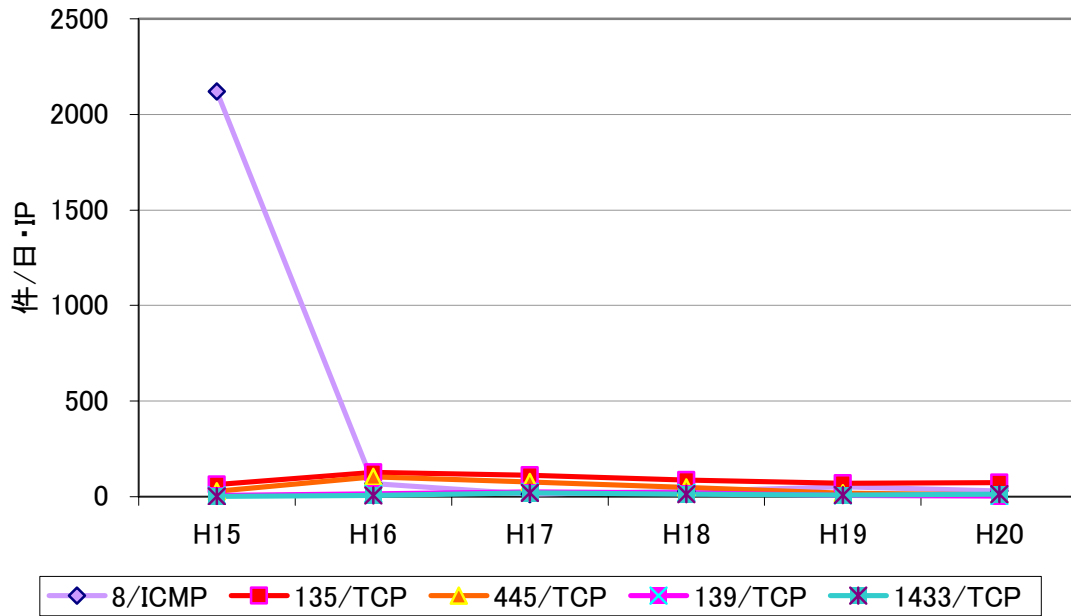


図 4-2 宛先ポート別のアクセス件数の推移 (1~5 位)

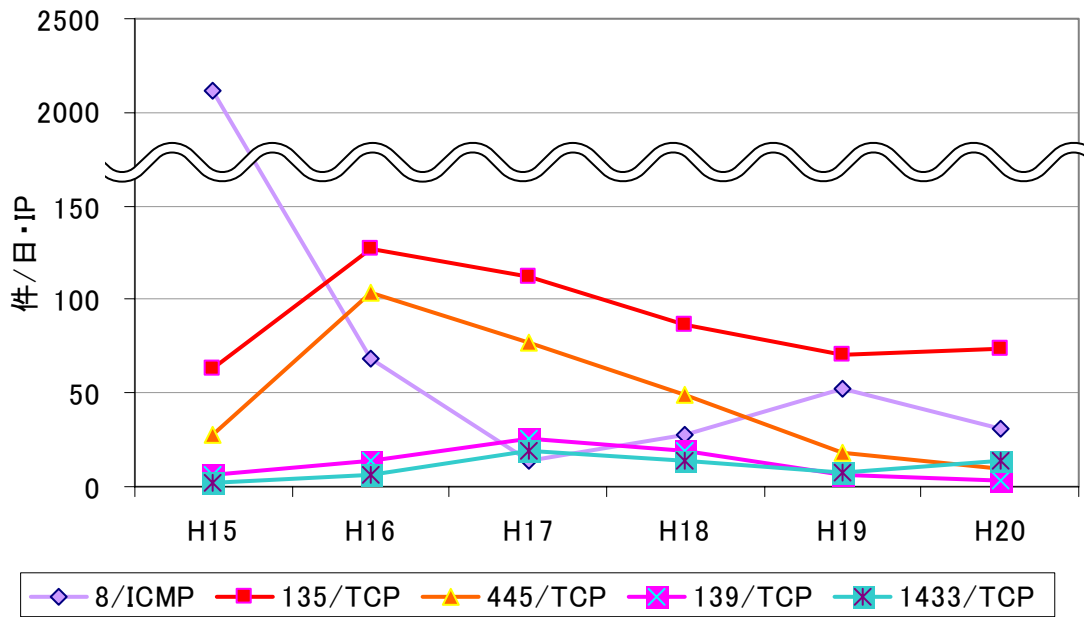


図 4-3 宛先ポート別のアクセス件数の推移 (1~5 位)

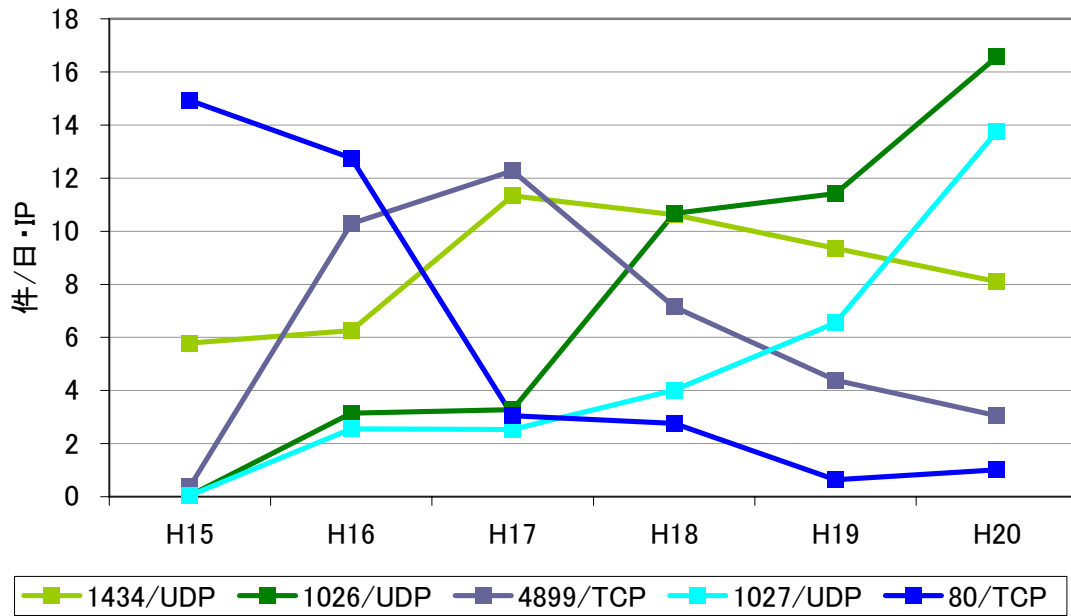


図 4-4 宛先ポート別のアクセス件数の推移 (6~10位)

### 4.3 発信元（国/地域）別の推移

ファイアウォールに対するアクセスのうち、アクセスしてきた発信元（国/地域）別では、日本が最も多く、以下、米国、中国、韓国、カナダと続いています。平成15年のアクセス件数が突出しているのは、「Welchia」ウイルスの活動が原因と思われる、8/ICMPのアクセスが影響しています。

観測期間全体で見ると各国/地域からのアクセス件数は、いずれも減少傾向となっています。

平成20年は、アクセスしてきた発信元（国/地域）別では、中国が最も多く、以下、日本、米国、台湾、韓国と続いており、前年と比較して一日・1IPあたり、中国からのアクセスが約41.7件（約98%）の大幅な増加が見られました。これは、1026/UDPが約13.9件（約560%）、1027/UDPが約11.6件（約543%）、1433/TCPが約6.8件（約159%）とそれぞれ大幅に増加しているためです。

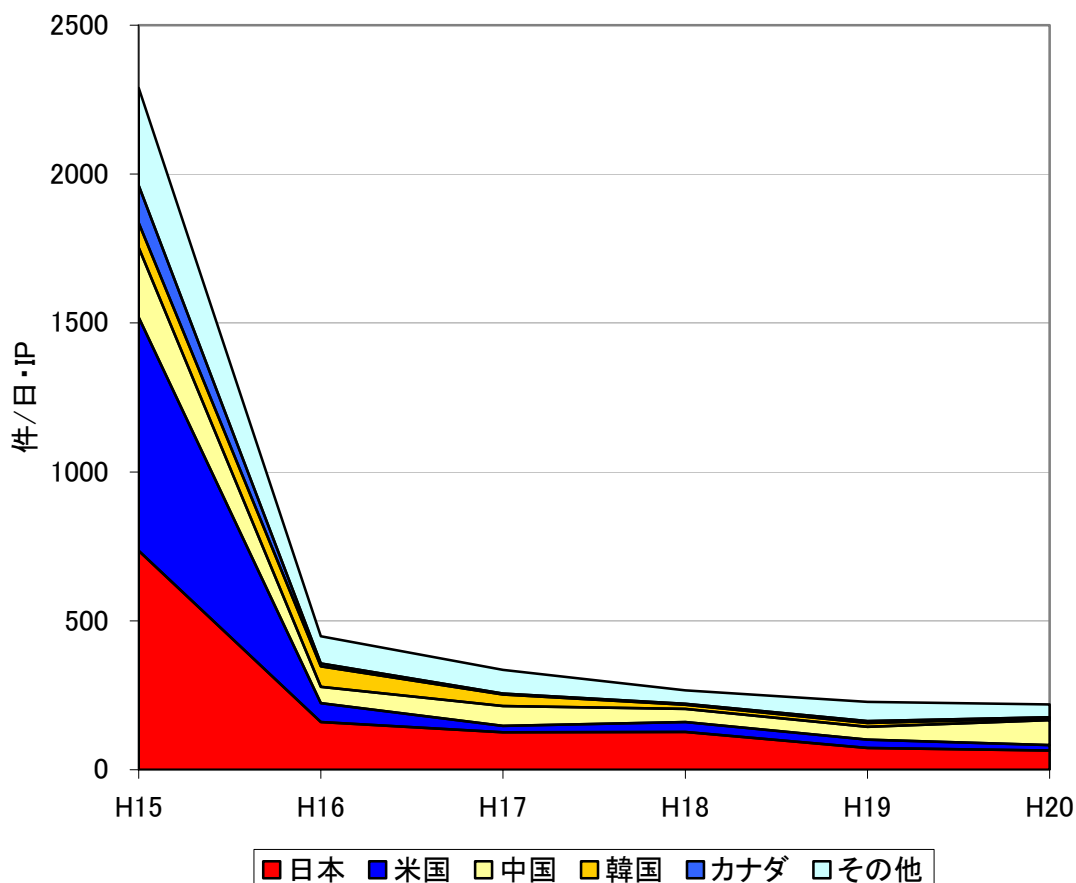


図 4-5 発信元（国/地域）別の推移

#### 4.4 国内からのアクセス状況

日本国内からの、ファイアウォールに対するポート別アクセス件数の上位 5 位は、8/ICMP、135/TCP、445/TCP、139/TCP、1433/TCP の順でした。

日本国内からのアクセスにおいても、平成 15 年に「Welchia」ウイルスの活動が原因と思われる、8/ICMP への大量のアクセスが確認できます。

平成 16 年以降で、アクセス件数の推移を見ると、全体的にアクセス件数は減少傾向にあります。特に、平成 19 年には 445/TCP に対するアクセス件数が、前年と比較して、約 25.3 件（約 65%）減少しています。

平成 20 年は、ポート別アクセス件数の上位 5 位は、135/TCP、445/TCP、8/ICMP、139/TCP、1433/TCP の順となっており、前年と比較して一日・1 IP あたり、445/TCP が約 8.4 件（約 63%）減少しましたが、詳細を見ると平成 20 年 12 月頃からアクセスが増加に転じています。

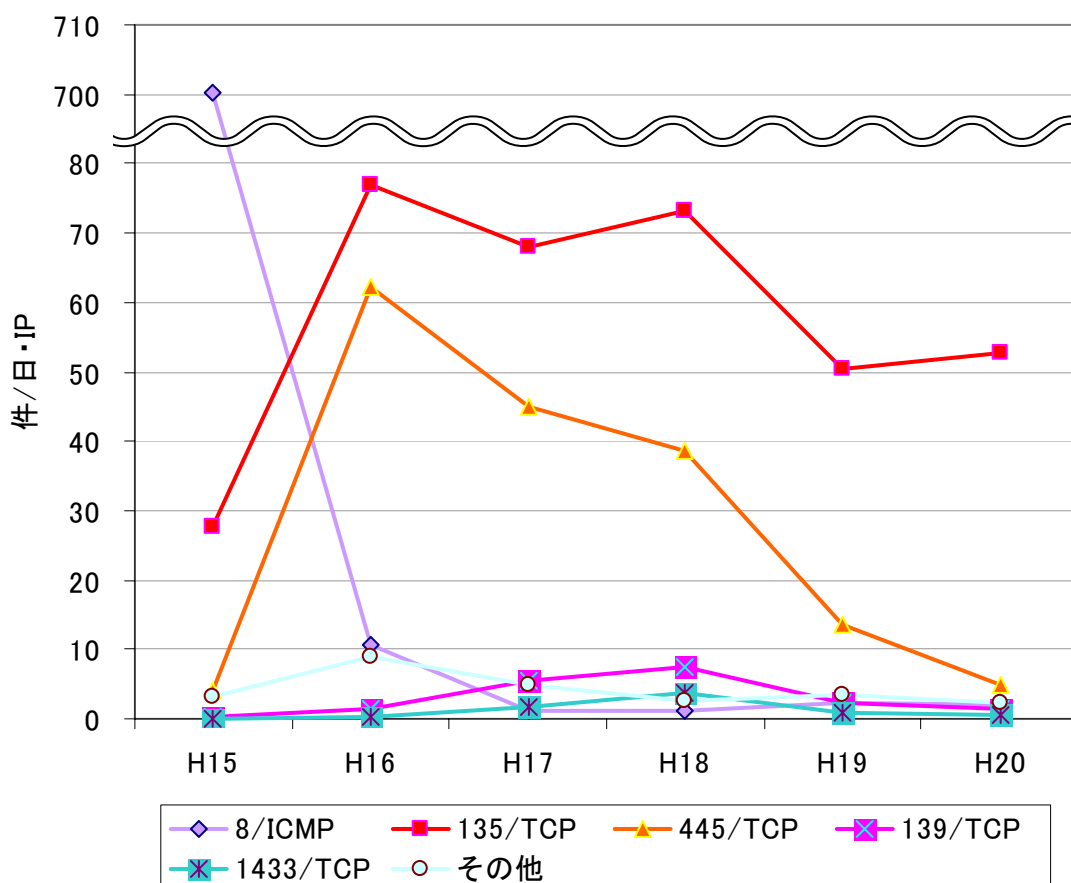


図 4-6 日本国内からのアクセス件数

表 4-1 主な使用ポートの一覧

ポート	主に利用するアプリケーション及び用途
8/ICMP	コンピュータ機器間のネットワーク診断
22/TCP	コンピュータのリモートアクセス
80/TCP	HTTP サーバ
135/TCP	Windows 系 OS の RPC
139/TCP	Windows ネットワークのファイル共有
445/TCP	Windows2000/XP/vista 等のファイル共有
1026/UDP	Windows Messenger サービス
1027/UDP	Windows Messenger サービス
1080/TCP	プロキシサーバの一種である socks サーバ
1433/TCP	Microsoft SQL Server(データを検索)
1434/UDP	Microsoft SQL Server(サーバの監視)
2967/TCP	Symantec Client Security 、 Symantec AntiVirus
3128/TCP	プロキシサーバの一種である squid サーバ
4899/TCP	リモートコントロールソフト (Radmin)
5168/TCP	Trend Micro ServerProtect
5900/TCP	リモートコントロールソフト (VNC)
8080/TCP	HTTP proxy

## 5 不正侵入検知システムによる検知状況

不正侵入検知で検知したアラート<sup>5</sup>の件数は、観測を開始した平成14年と平成15年を比較すると一日・1IPあたり約4.4件の急激な増加がみられます。これは、「Worm」が増加したためです。平成15年に「SQL Slammer」ウイルスが現れ、感染を広げました。その後は、平成17年をピークに検知件数の大半を占める「Worm」は減少しています。

平成20年は、前年と比較して一日・1IPあたり、約1.4件（約13%）減少しましたが、観測を開始した当初から依然として高水準で推移しています。

なお、シグネチャは、状況に合わせて適宜変更しており、これが検知件数に影響している場合があります。

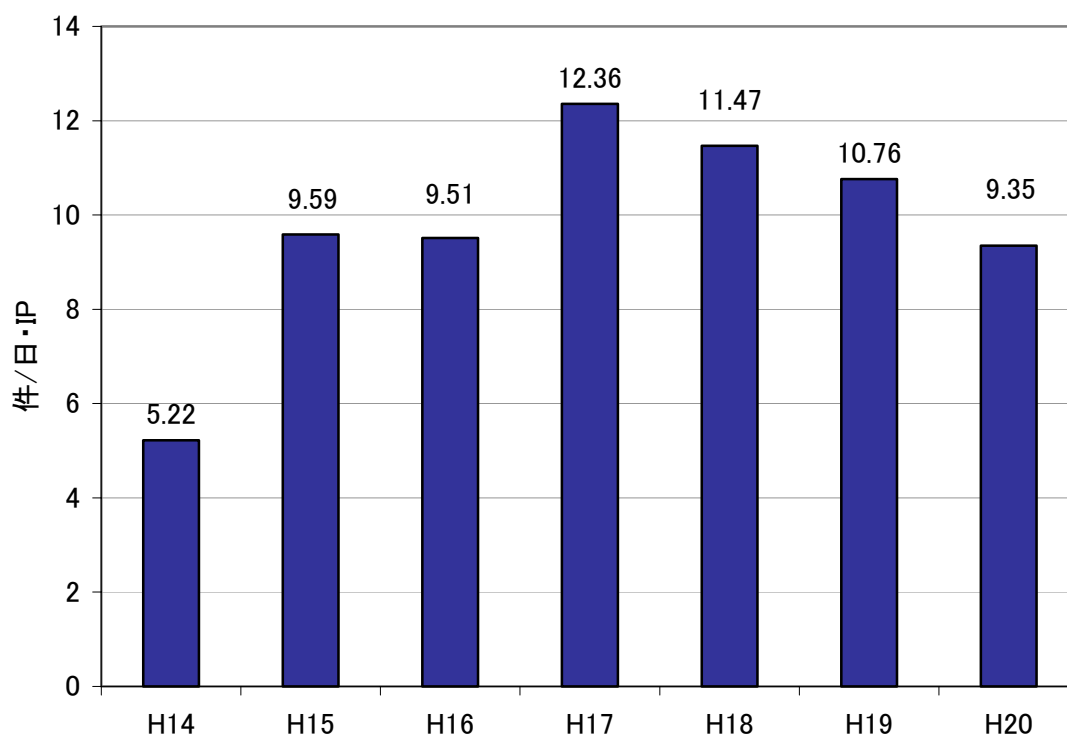


図 5-1 検知数の推移

<sup>5</sup>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

## 5.1 攻撃手法別の推移

「Worm」は、初めて確認された平成15年に急激に増加し、平成17年をピークに減少していますが、平成20年においても攻撃手法別では大部分を占めています。この理由として、「Worm」として検知されたウイルスの感染速度が速いことに加え、セキュリティパッチを適用していないコンピュータが未だに多く存在することが考えられます。

観測期間全体では、「Worm」の感染活動によるものが全体の約75%、インターネットに接続されたコンピュータを探索する「Scan」によるものが約15%を占めており、合わせて全体の約9割を占めています。

平成20年は、「Worm」が最も多く以下、「Scan」、「ICMP」と続いており、前年と比較して一日・1IPあたり、「Worm」が約1.19件（約13%）、「Scan」が約0.46件（約35%）それぞれ減少しましたが、「ICMP」は約0.0033件（約52%）の減少が見られました。

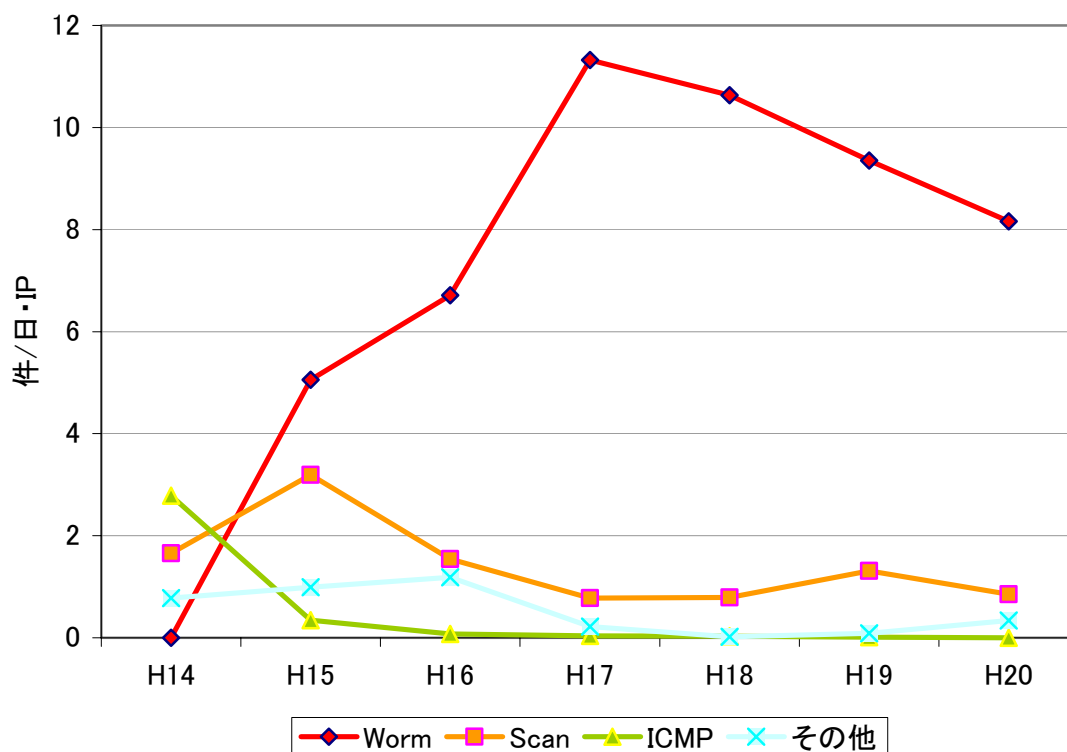


図 5-2 攻撃手法別の推移

## 5.2 発信元（国/地域）別の推移

不正なアクセスの発信元（国/地域）は、観測期間全体において、中国が全体の約53%と最も多く、以下、米国、日本、韓国、台湾と続いています。中国からのアクセスは、平成17年に急激に増加し、以後、高水準を維持しています。これらのアクセスの大部分は「Worm」によるものです。

平成20年は、中国からのアクセスが最も多く以下、米国、日本、台湾、インドと続いており、前年と比較して一日・1IPあたり、中国が約0.4件（約5%）、日本が約0.02件（約11%）それぞれ減少しましたが、米国は、約0.25件（約39%）増加しています。

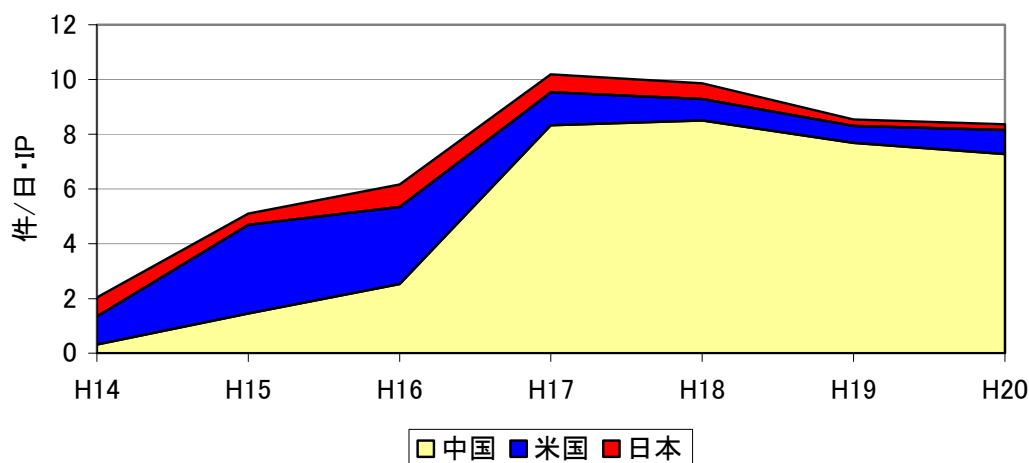


図 5-3 発信元（国/地域）別の推移（1～3位）

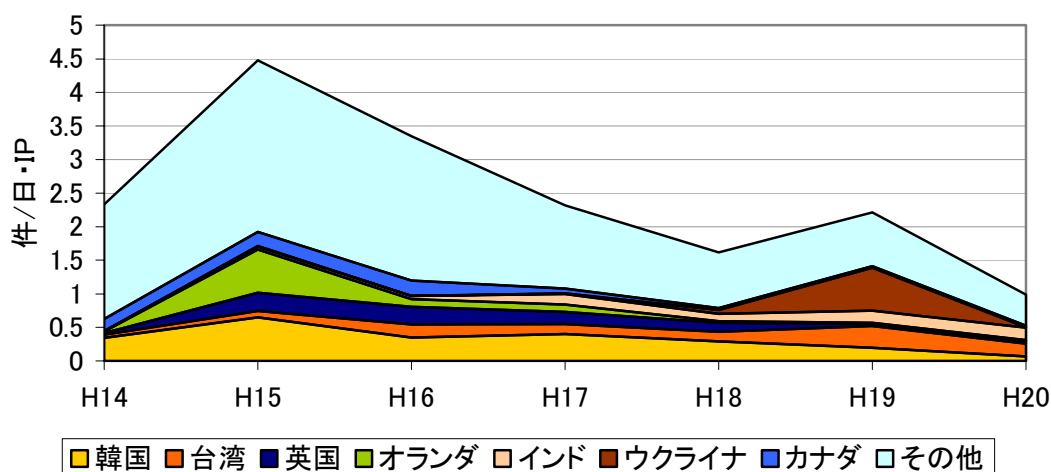


図 5-4 発信元（国/地域）別の推移（4位以下）

### 5.3 国内からのアクセス状況

不正侵入検知システムによる不正なアクセスの検知件数のうち、日本国内のコンピュータからのものは、平成16以降、減少傾向が続いています。

平成20年は、「Worm」が最も多く以下、「Scan」、「ICMP」と続いており、前年と比較して、「Scan」が増加したものの、大部分を占める「Worm」が減少したことから、一日・1IP当たり約0.02件（約11%）減少しました。

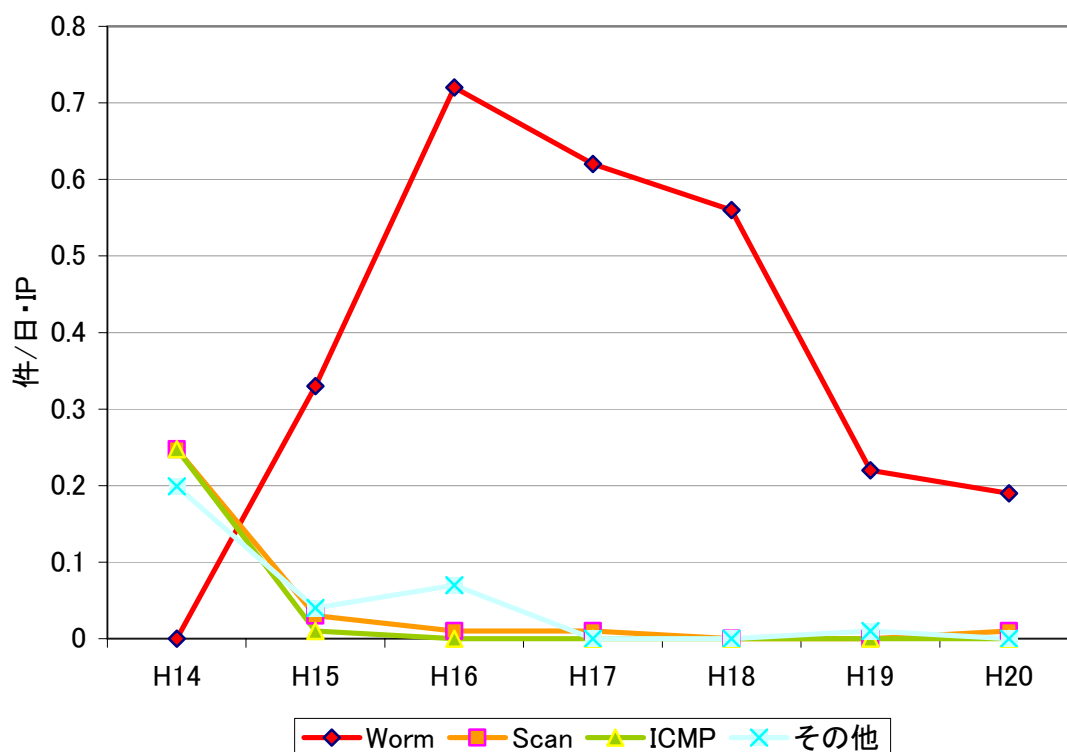


図 5-5 日本国内からのアクセス件数の推移

## 6 サーバコンピュータに対する DoS 攻撃 (SYNflood 攻撃)

警察庁のファイアウォールに送信された SYN/ACK パケット及び RST/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 SYNflood 攻撃の兆候について観測しています。

### 6.1 DoS 攻撃 (SYNflood 攻撃) 検知件数

SYNflood 攻撃の検知件数は、観測期間全体において、平成 19 年まで減少傾向にありましたが、平成 20 年は、377,825 件観測され、前年と比較すると 286,408 件 (約 313%) の大幅な増加が見られました。

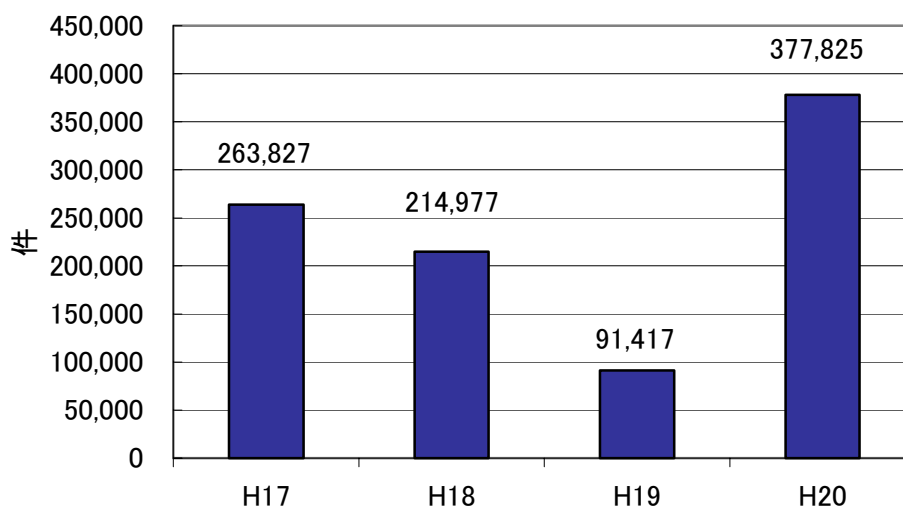


図 6-1 DoS 攻撃 (SYNflood 攻撃) の検知件数

## 6.2 攻撃対象ポート別の検知件数

DoS 攻撃の攻撃対象ポートは、観測期間全体において、80/TCP に対する攻撃が最も多く、以下、7000/TCP、1723/TCP、7100/TCP、3389/TCP と続いています。平成 20 年の検知件数における 80/TCP の割合は約 80%であり、主にウェブサーバに対して SYNflood 攻撃が行われていると考えられます。

平成 17 年及び 18 年は、主にファイルサーバ及びオンラインゲーム等で使用されている 7000/TCP に対する攻撃を観測しましたが、19 年には大幅に減少しました。

平成 20 年は、80/TCP に対する攻撃が最も多く、以下、1723/TCP、7000/TCP、3389/TCP、7100/TCP と続いており、前年と比較すると、1723/TCP が 11,444 件（約 7,529%）7100/TCP が 359 件（約 5,129%）、80/TCP が 236,629 件（約 355%）、7000/TCP が 4776 件（約 201%）のそれぞれ大幅な増加が見られました。

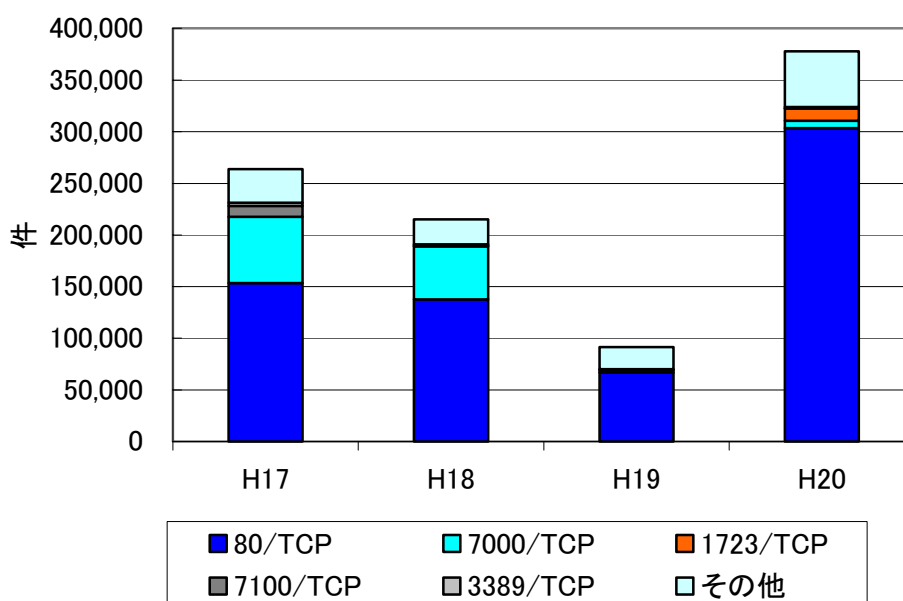


図 6-2 攻撃対象ポート別の検知件数 (SYN flood 攻撃)

## 7 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。海外では、4万～10万台のコンピュータからなるボットネットを操っていた疑いでオランダ人の兄弟2人を逮捕した事例<sup>6</sup>が報道されています。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示します。

### 7.1 ボットネット観測数

平成17年から平成19年までの間は、ボットネットの観測数が増加しており、平成19年は、平成17年と比較して約128%増加しました。平成20年は、前年と比較して、404件（約55%）減少しました。

平成20年に観測したボットネットは331個で、そのうち平成20年に新たに把握したものが136個でした。

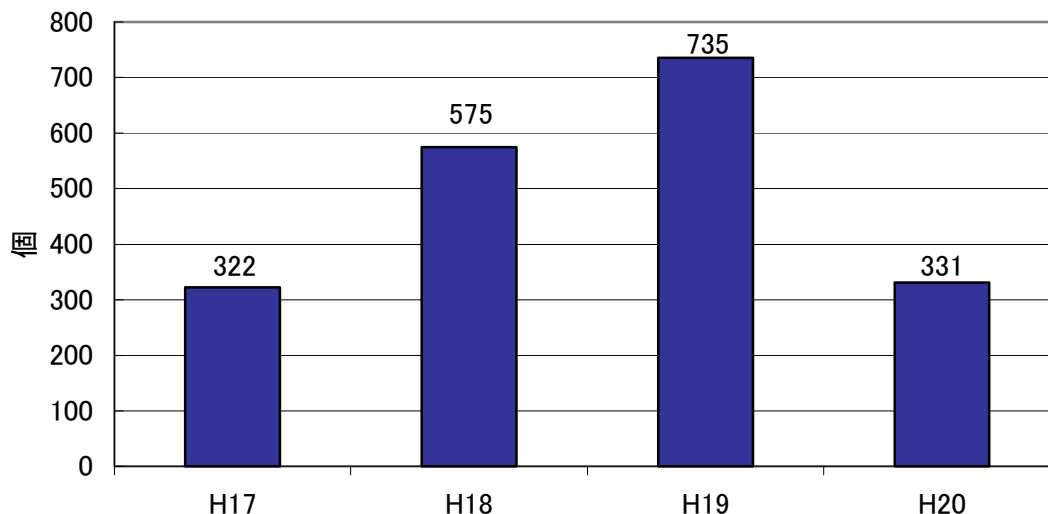


図 7-1 ボットネット観測数

<sup>6</sup> [http://www.theregister.co.uk/2008/08/04/dutch\\_botnet\\_herders\\_arrested/](http://www.theregister.co.uk/2008/08/04/dutch_botnet_herders_arrested/)

## 7.2 ボットネットあたりの感染台数

一つのボットネットに接続しているコンピュータの平均台数（ボットネットあたりのボット感染台数）は、平成17年には、6,964台でしたが、平成18年以降は、3,000台前後で推移しています。

平成20年は、一つのボットネットに接続しているコンピュータの平均台数は、3,281台でした。

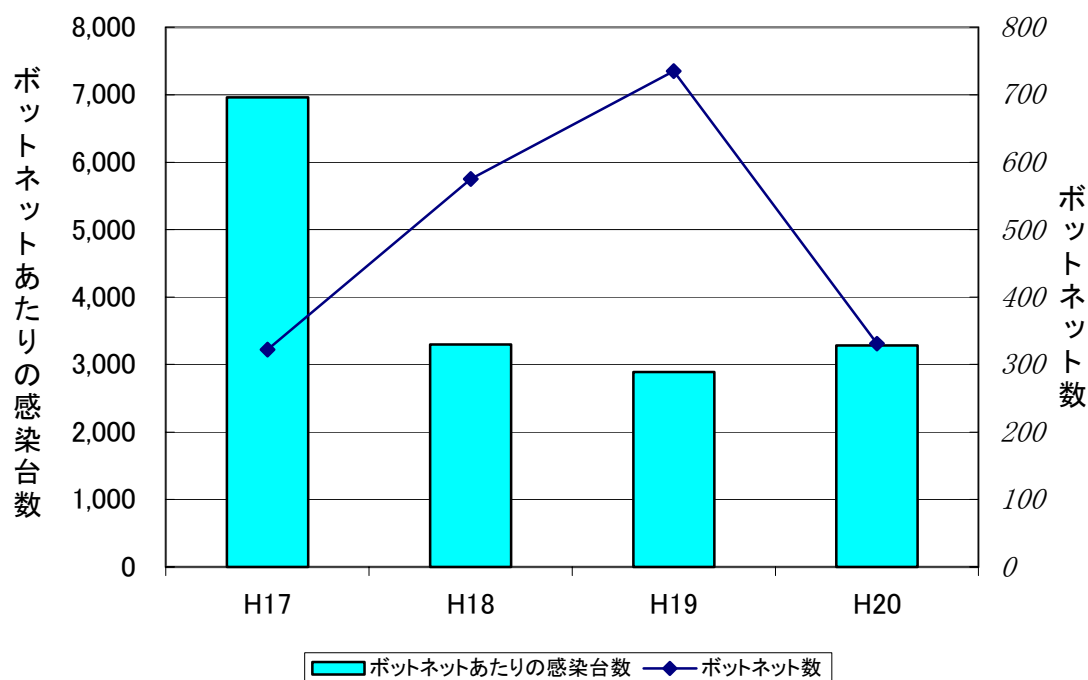


図 7-2 ボットネットあたりの感染台数

表 7-1 ボットネットあたりの感染台数の推移

	平成17年	平成18年	平成19年	平成20年
ボットネット数	322	575	735	331
感染台数を調査できたボットネット数	192	311	303	168
ボット感染台数	1,337,167	1,025,253	874,980	551,226
ボットネットあたりのボット感染台数	6,964	3,297	2,888	3,281

### 7.3 国内のボット感染台数

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、観測期間全体で見ると減少傾向にあります。

平成20年は、ボットに感染したコンピュータの台数は、551,226台でした。分析の結果、このうち日本に存在すると考えられるものは、16,529台で、最も多く観測した平成17年の149,609台と比較して133,080件（約89%）、前年と比較すると30,424件（約65%）減少しています。

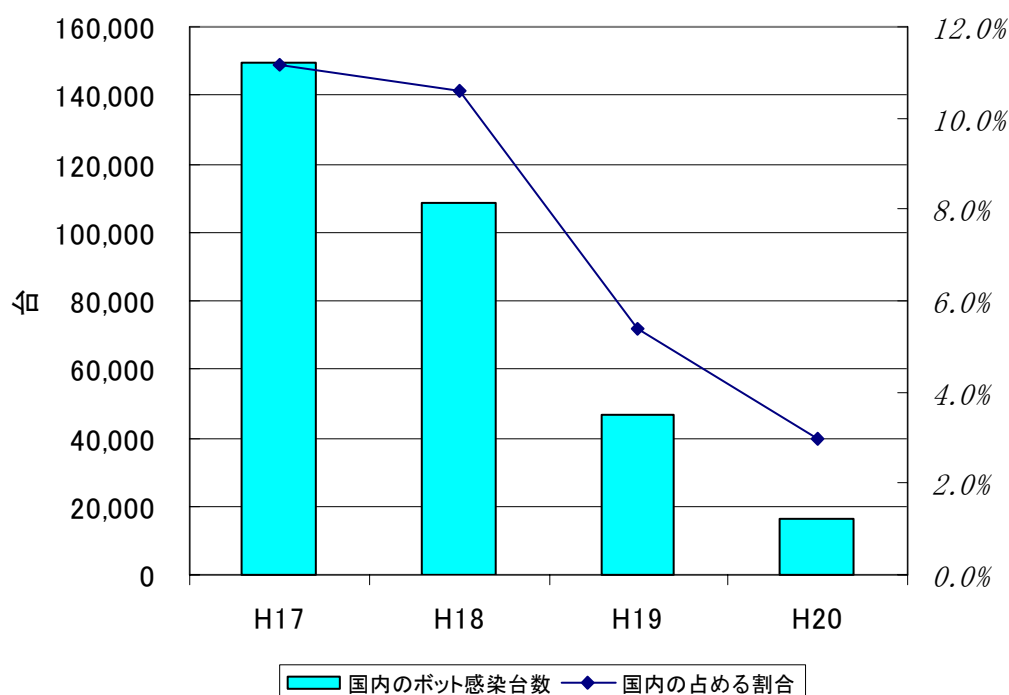


図 7-3 国内のボット感染台数

表 7-2 国内のボット感染台数の推移

	平成17年	平成18年	平成19年	平成20年
国内のボット感染台数	149,609	108,626	46,953	16,529
世界のボット感染台数	1,337,167	1,025,253	874,980	551,226
国内の占める割合	11.2%	10.6%	5.4%	3.0%

## 7.4 ボットネットの感染活動

警察庁では、観測したボットネットの指令サーバがボットネットに対して、指令した命令を観測しています。平成 17 年以降のボットの感染活動を分析した結果、135/TCP を狙ったものが最も多く、次いで 445/TCP、139/TCP、1433/TCP、5900/TCP と続きます。感染活動の大半は、マイクロソフト社の Windows のサービスの脆弱性を狙ったものでした。

平成 18 年以降では、命令数は多くないものの、5900/TCP を狙ったものが増加傾向にあります。平成 19 年には、2967/TCP を狙ったものが観測されました。

平成 20 年の命令数は、135/TCP を狙ったものが最も多く、次いで 445/TCP、5900/TCP、139/TCP、1433/TCP と続いており、前年と比較すると、138,996 件（約 182%）の大幅な増加が見られました。

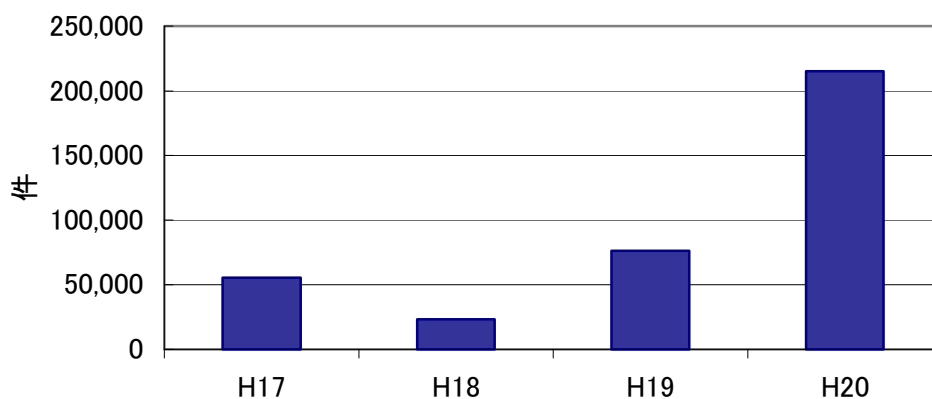


図 7-4 ボットネットでの感染活動数

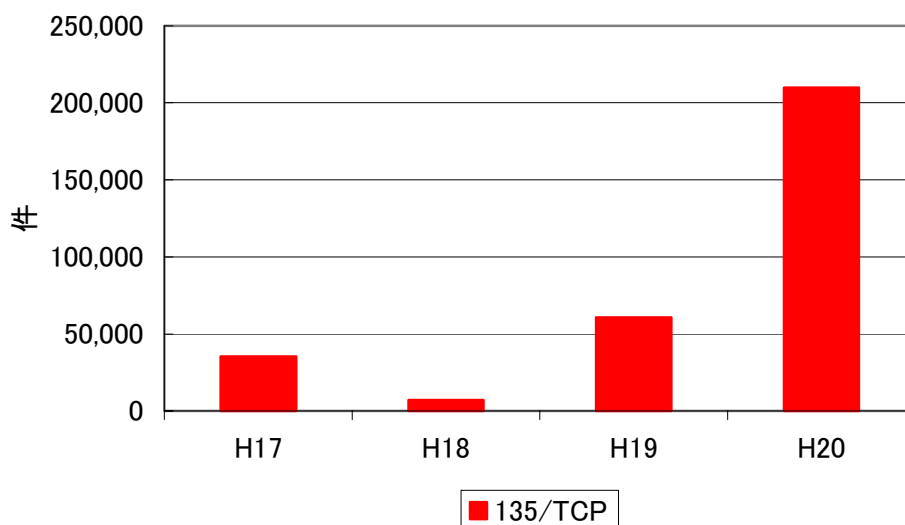


図 7-5 ボットネットでの感染活動数(ポート別 135/TCP のみ)

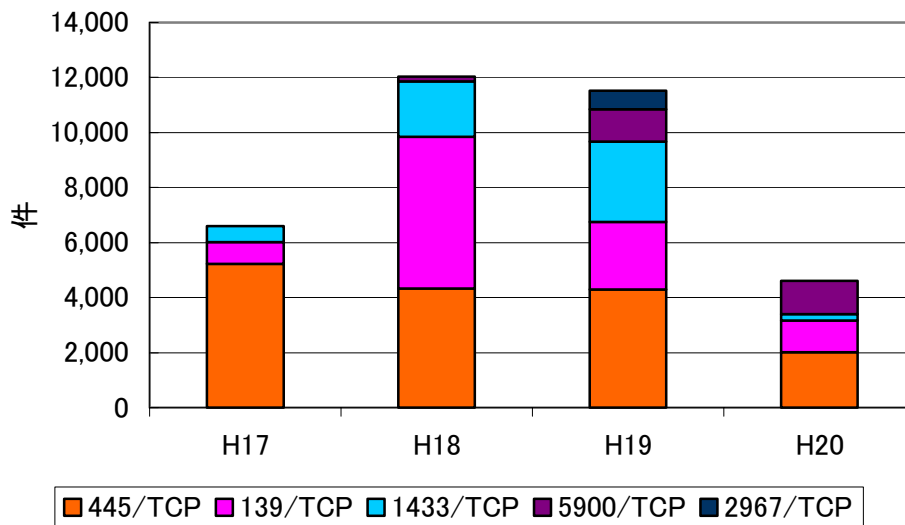


図 7-6 ポットネットでの感染活動数(ポート別 135/TCP 以外)

表 7-3 感染活動に利用される主な脆弱性 (ポート別)

ポート	感染活動命令において利用される主な脆弱性
135/TCP	マイクロソフト社 Windows DCOM の脆弱性 (MS03-026,039)
445/TCP	マイクロソフト社 Windows LSASS の脆弱性 (MS04-011)
	マイクロソフト社 Windows ASN.1 の脆弱性 (MS04-007)
	マイクロソフト社 Windows Server サービスの脆弱性 (MS06-040)
139/TCP	マイクロソフト社 Windows NetBIOS を対象にブルートフォース攻撃
	マイクロソフト社 Windows ASN.1 の脆弱性 (MS04-007)
1433/TCP	マイクロソフト社 MS-SQL Server を対象にブルートフォース攻撃
5900/TCP	遠隔操作ソフト RealVNC の脆弱性
2967/TCP	シマンテック社セキュリティ対策ソフトの脆弱性 (SYM06-010)

## 7.5 ボットネットからの DoS 攻撃

警察庁では、観測したボットネットの指令サーバがボットネットに対して、指令した DoS 攻撃命令を観測しています。

平成 17 年以降の DoS 攻撃命令を分析したところ、SYNflood 攻撃が最も多く、年々増加しています。一方、UDPflood 攻撃や PINGflood 攻撃（ICMPflood 攻撃を含む）は、平成 19 年以降、減少に転じています。

平成 20 年は、SYNflood 攻撃が最も多く、以下、UDPflood 攻撃、PINGflood 攻撃と続いており、前年と比較すると、総計で 62,136 件（約 486%）の大幅な増加が見られました。

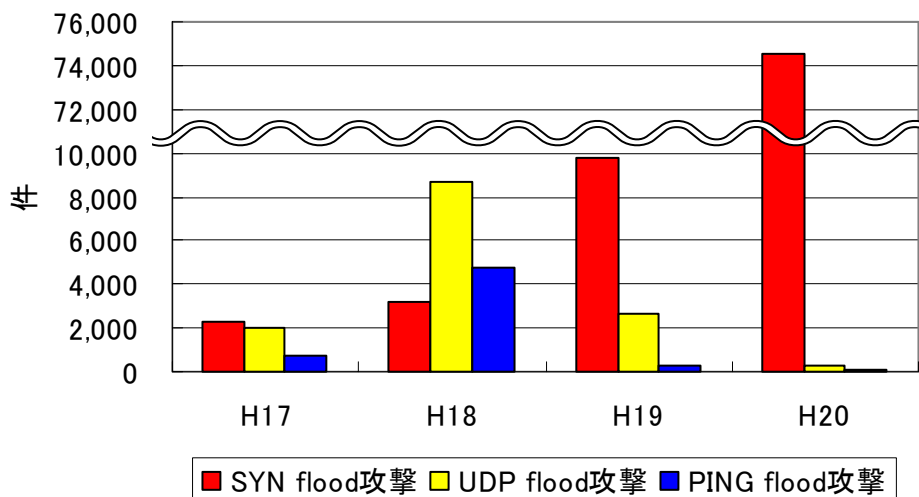


図 7-7 ボットネットでの DoS 攻撃命令数

表 7-4 ボットネットでの DoS 攻撃命令数

	平成 17 年	平成 18 年	平成 19 年	平成 20 年
SYN flood 攻撃	2,273	3,239	9,810	74,508
UDP flood 攻撃	1,982	8,701	2,694	305
PING flood 攻撃	724	4,748	278	105
総計	4,979	16,688	12,782	74,918

## 8 DNS サーバの動向

DNS (Domain Name System) は、インターネットにおいてコンピュータのホスト名と IP アドレスを対応付けるサービスです。DNS は、平成 20 年 7 月に、DNS サーバの実装にキャッシュポイズニングの脆弱性があることが報じられ話題となりました。

この脆弱性を悪用された場合、利用者が普段から利用しているアドレスにアクセスしただけで、DNS サーバに登録された偽のウェブサイトへと誘導することができます。さらに、DNS サーバが外部に対して再帰的な問い合わせを許可している場合、攻撃者はキャッシュポイズニング攻撃の成功・失敗を容易に確認できるため、キャッシュポイズニング攻撃を受ける可能性が高まることが懸念されます。

警察庁サイバーフォースセンターでは、平成 18 年 7 月に、分析レポート「DNS の再帰的な問い合わせを悪用した DDoS 攻撃手法の検証について」<sup>7</sup> を公開、また、平成 20 年 8 月に「DNS サーバの現状調査」<sup>8</sup> を公開し、DNS の脆弱性について、注意喚起を行いました。

本章では、DNS サーバの状況について最新の調査結果を示します。

---

<sup>7</sup> [http://www.cyberpolice.go.jp/server/rd\\_env/pdf/20060711\\_DNS-DDoS.pdf](http://www.cyberpolice.go.jp/server/rd_env/pdf/20060711_DNS-DDoS.pdf)

<sup>8</sup> [http://www.cyberpolice.go.jp/server/rd\\_env/pdf/20080821\\_DNS.pdf](http://www.cyberpolice.go.jp/server/rd_env/pdf/20080821_DNS.pdf)

## 8.1 DNS サーバへの外部からの再帰的問い合わせ

平成 20 年 4 月に調査した 2,022 台の DNS サーバのうち平成 20 年 12 月の時点で利用可能な DNS サーバ 2,014 台について外部からの再帰的問い合わせ状況を調査しました。平成 20 年 4 月の調査では、外部からの再帰的問い合わせを許可する DNS サーバは調査対象サーバ全体の約 49%でしたが、平成 20 年 12 月の調査では、調査対象サーバ全体の約 39%に減少しました。外部からの再帰的問い合わせを許可する DNS サーバは、減少傾向にあります。

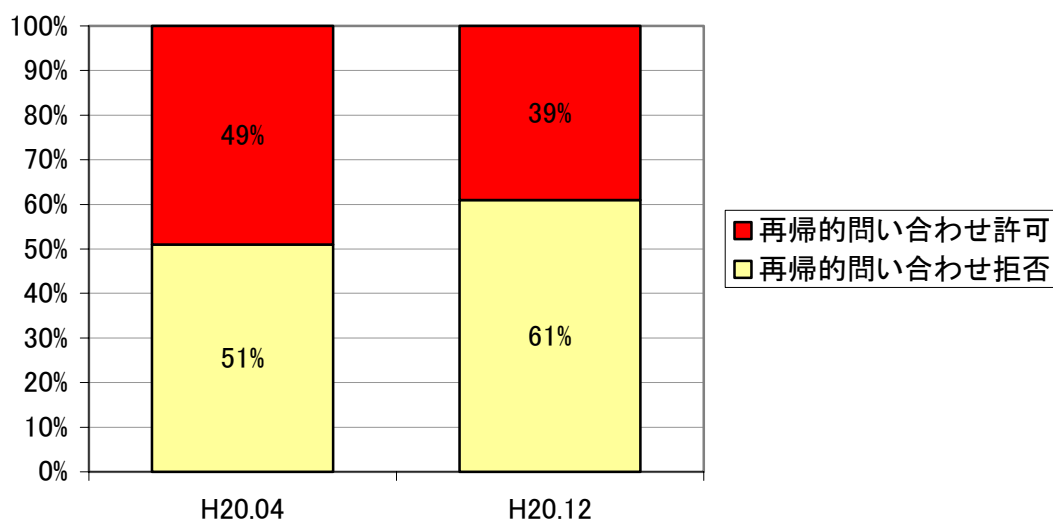


図 8-1 外部からの再帰的問い合わせが可能な DNS サーバの割合

## 8.2 DNS サーバのクエリポートの状況

DNS サーバのクエリポートが推測されやすい場合、DNS キャッシュポイズニング攻撃を受ける可能性が高くなります。

日本国内の主要な DNS サーバ 649 台について、クエリポートの状況を、平成 20 年 12 月に調査しました。調査の結果、クエリポートが推測可能な DNS サーバは全体の約 33%でした。

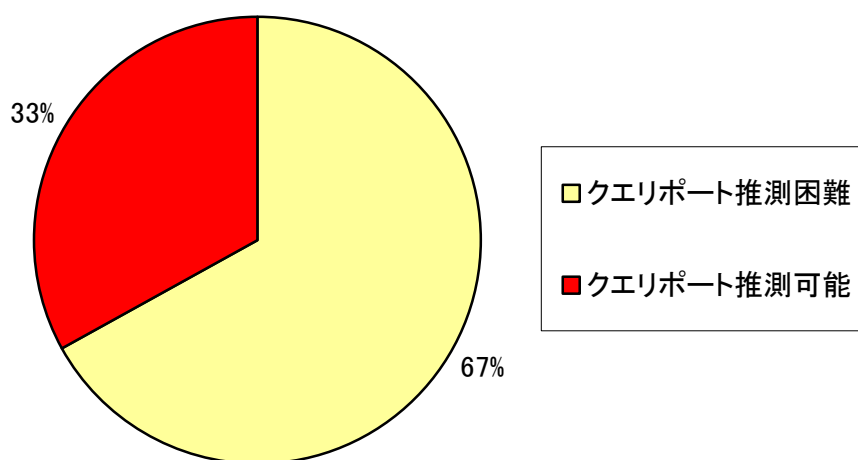


図 8-2 クエリポートの状況(平成 20 年 12 月調査)

## 8.3 DNS サーバのセキュリティ

平成 20 年 12 月の調査結果によると、再帰的な問い合わせを許可する DNS サーバは、減少傾向にあるものの、クエリポートを推測可能な DNS サーバとともに依然として多く存在していることが分かりました。これらの DNS サーバは、DNS キャッシュポイズニング攻撃又は再帰的問い合わせを悪用した DDoS 攻撃に利用される可能性があります。被害を未然に防止するためにも、DNS サーバの適切な運用に向け、セキュリティパッチの適用や設定の見直しなど、セキュリティ対策の確認をお願いします。

## 9 情報セキュリティ対策の向上のために

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、減少傾向が見られるものの高水準で推移しており、宛先ポートの一部に変化が見られるなど、攻撃の手口は常に変化しています。また、ボットは、観測できた感染台数こそ減少したものの、感染したコンピュータから他のコンピュータを攻撃する DoS 攻撃の一種である SYN flood 攻撃の増加が観測されています。更に他のコンピュータへの感染活動については依然として活発であることがうかがえます。

これらのサイバー攻撃がもたらす被害の態様は様々なものがあります。近年では、警察庁において SQL インジェクションによるものと思われるホームページの改ざんや情報の漏洩、メールを利用した標的型攻撃による悪意のあるソフトウェアの感染、USB メモリを経由して感染を広げるウイルスの活動による外部と隔離された内部ネットワークでの感染の拡大の危険性等が確認されています<sup>9</sup>。

しかしながら、幸いなことに、警察庁で観測された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最低限、以下のような措置を講じることが重要となります。

- ・ OS やアプリケーションの更新プログラムを適切に適用する
- ・ ウイルス対策ソフトを適切に運用する
- ・ ファイアウォールソフトを適切に運用する
- ・ メール添付ファイルやメール中のリンク先を不用意に閲覧しない

その他にもコンピュータの利用状況に応じて

- ・ 利用者や利用用途に応じてパソコンやユーザ・アカウント等を使い分ける
- ・ 適宜コンピュータ等の電源を切断する
- ・ 不要な機能を導入しない／使用不可能にする
- ・ データを暗号化する

---

<sup>9</sup> [http://www.cyberpolice.go.jp/detect/pdf/H20\\_kamihanki.pdf](http://www.cyberpolice.go.jp/detect/pdf/H20_kamihanki.pdf) 「平成20年上半期におけるインターネット治安情勢について」18P "警察庁で確認したその他の攻撃手法"

等を実施することも有効です。

また、企業等の情報セキュリティ管理者等の皆さんにとって、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講じることが推奨されるものとして、以下の対策が大変重要です。

- ・各ソフトウェアや機器のベンダからリリースされる脆弱性を修正するセキュリティ更新プログラムの適切な適用を行う
- ・ウイルス対策ソフトの適切な運用を行う
- ・使用しているソフトウェアのバージョンの適切な更新を行う
- ・パーソナルコンピュータ、Web サーバ以外にも DNS サーバやルータ等の機器においても適正な設定の確認とセキュリティ更新プログラムの適切な適用を行う
- ・データベースを利用する Web アプリケーションを構築、運用している場合は、SQL インジェクション対策について検証を行う
- ・証跡を定期的に確認し、異常を早期に発見・把握し適切な対策をとる

なお、各対策の実施に当たっては、事前に実施に伴う不具合の発生等を検証するために、ベンダから提供されているセキュリティ情報の確認を行うことも重要です。また上記の対策に加えて、情報セキュリティ対策及び事業継続計画等について十分検討し、先に掲げた一般的な個々の対策を講じるのみならず、適切な障害原因の究明や障害の兆候の迅速な発見・対応ができるよう、守るべき情報資産などに応じて組織としての態勢を適切に構築することが重要となります。

最後に、サイバー攻撃の手口は日々変化しており、その手口によって採るべき方策や注意すべき点が異なってくる場合があります。そこで、インターネットを利用している皆さんや企業等の情報セキュリティ管理者等の皆さんにあつては、可能な限りインターネット上の脅威やそれらへの対策等について関心を持ち、状況に応じて適切な措置を講じることをお勧めします。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。

## 10 付録

### 10.1 特徴的なアクセス状況

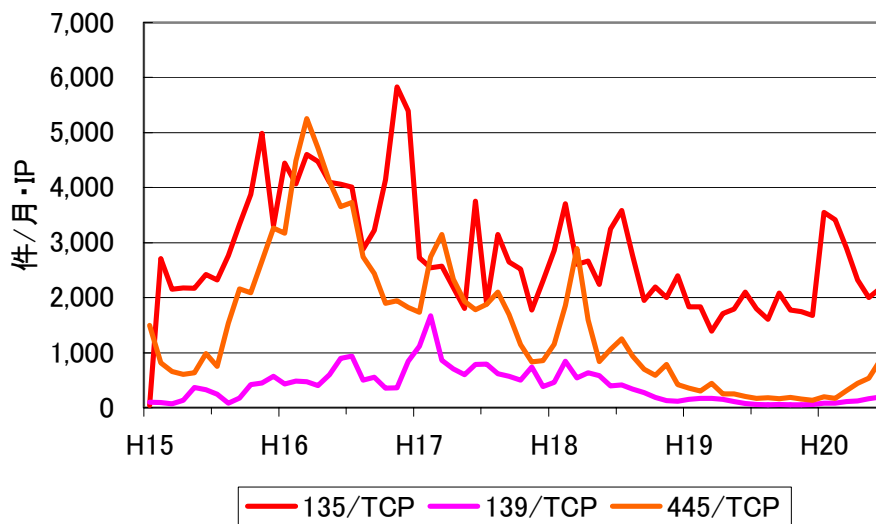


図 10-1 主に Windows で使用されるポートに対するアクセス件数の推移

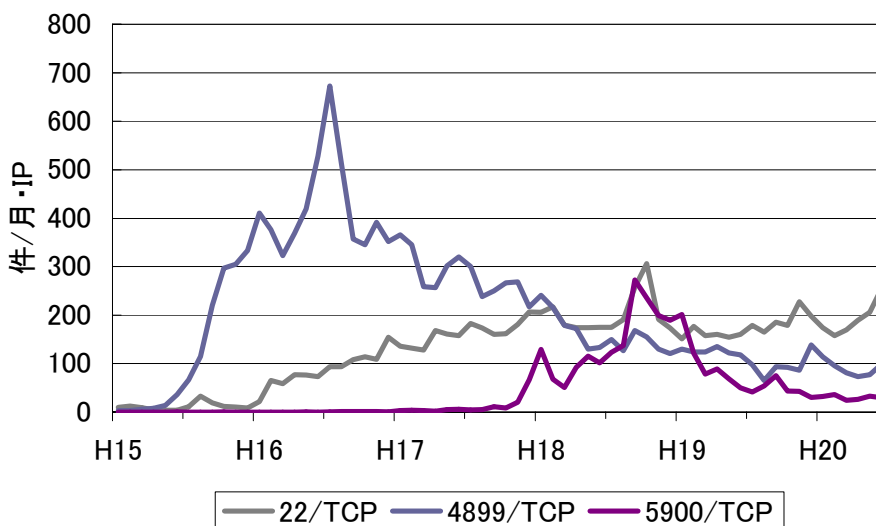


図 10-2 主に遠隔制御ソフトで使用されるポートに対するアクセス件数の推移

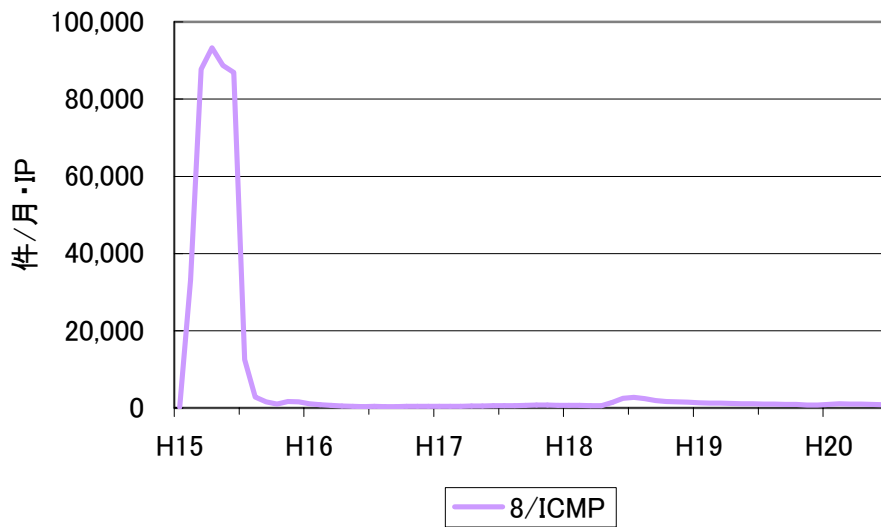


図 10-3 主にネットワークの疎通確認で使用されるアクセス件数の推移

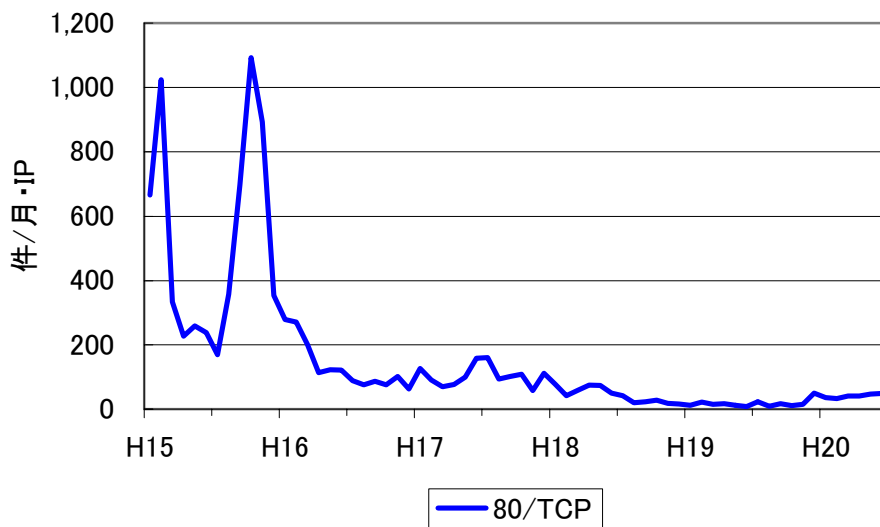


図 10-4 主に HTTP サーバで使用されるポートに対するアクセス件数の推移

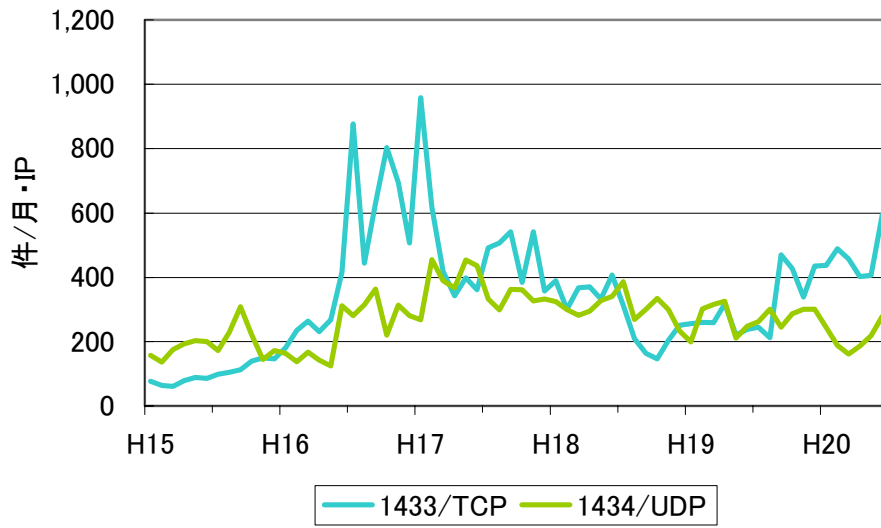


図 10-5 主に SQL Server で使用されるポートに対するアクセス件数の推移

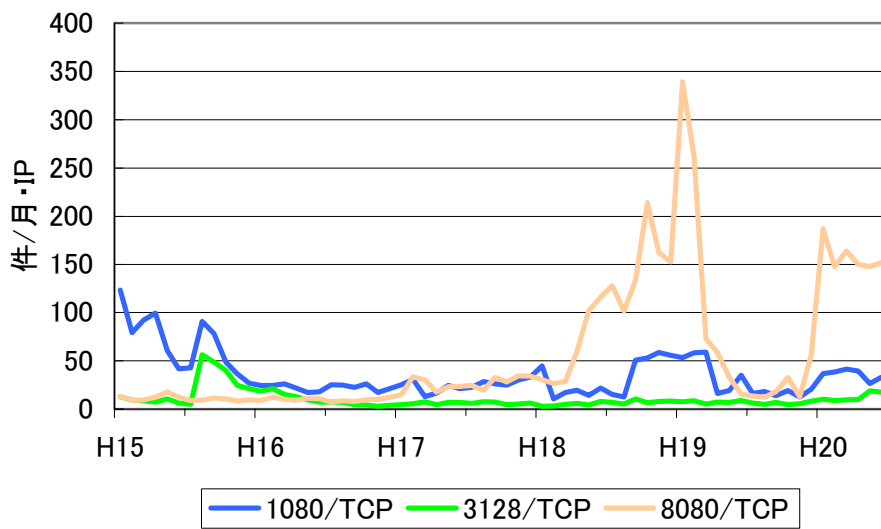


図 10-6 主にプロキシサービスで使用されるポートに対する  
アクセス件数の推移

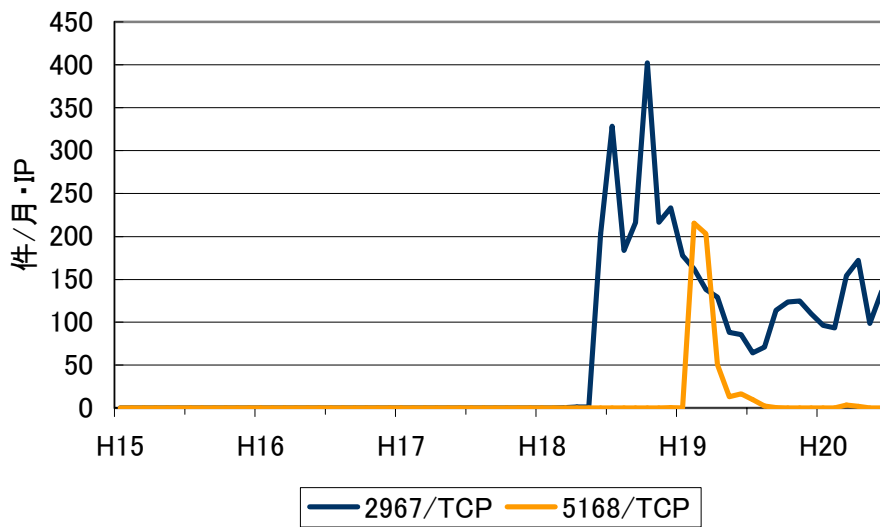


図 10-7 主にウイルス対策ソフトで使用されるポートに対するアクセス件数の推移

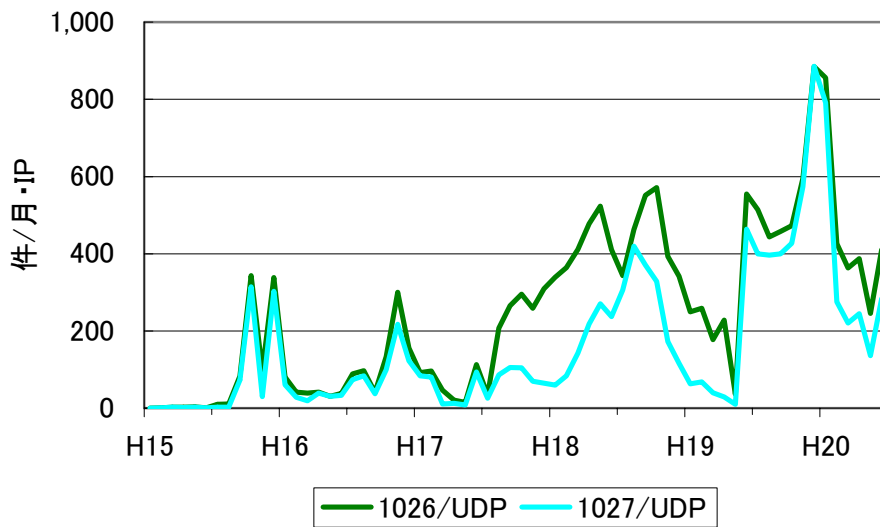


図 10-8 主に Messenger サービスで使用されるポートに対するアクセス件数の推移

## 10.2 ファイアウォールに対するアクセス件数 TOP50 (ポート別) <sup>10</sup>

順位	ポート	プロトコル	アクセス件数 (件/IP)	順位	ポート	プロトコル	アクセス件数 (件/IP)
1	8	ICMP	460,690	26	1080	TCP	2,320
2	135	TCP	183,224	27	1023	TCP	2,280
3	445	TCP	99,135	28	901	TCP	2,113
4	139	TCP	25,961	29	15118	TCP	1,673
5	1433	TCP	22,584	30	57758	TCP	1,506
6	1434	UDP	17,757	31	443	TCP	1,362
7	1026	UDP	16,490	32	3	ICMP	1,359
8	4899	TCP	13,646	33	5000	TCP	899
9	1027	UDP	10,754	34	42	TCP	781
10	80	TCP	10,137	35	23	TCP	750
11	137	UDP	10,097	36	10000	TCP	737
12	22	TCP	8,795	37	11	ICMP	677
13	1025	TCP	5,386	38	3128	TCP	672
14	6129	TCP	4,024	39	3306	TCP	648
15	2967	TCP	3,924	40	3410	TCP	624
16	8080	TCP	3,699	41	1028	UDP	525
17	2745	TCP	3,539	42	5168	TCP	517
18	21	TCP	3,318	43	35991	TCP	472
19	5900	TCP	2,942	44	12345	TCP	397
20	9898	TCP	2,812	45	111	TCP	396
21	5554	TCP	2,660	46	2100	TCP	391
22	3389	TCP	2,645	47	6588	TCP	311
23	25	TCP	2,396	48	1024	TCP	301
24	17300	TCP	2,390	49	27374	TCP	299
25	3127	TCP	2,373	50	3072	TCP	287

<sup>10</sup> 集計期間は、平成 15 年 7 月から平成 20 年 12 月まで。

### 10.3 ファイアウォールに対するアクセス件数 TOP50（国/地域別）<sup>11</sup>

順位	国	アクセス件数 (件/IP)	順位	国	アクセス件数 (件/IP)
1	日本	336,242	26	オランダ	2,323
2	米国	204,106	27	タイ	2,286
3	中国	150,026	28	トルコ	1,632
4	韓国	67,063	29	アルゼンチン	1,526
5	カナダ	32,076	30	マレーシア	1,501
6	台湾	26,679	31	ポルトガル	1,395
7	英国	16,662	32	デンマーク	1,203
8	香港	15,644	33	フィンランド	1,167
9	オーストラリア	9,510	34	ノルウェー	1,156
10	インド	8,400	35	ルーマニア	1,101
11	その他・不明	7,659	36	オーストリア	1,070
12	ドイツ	7,354	37	インドネシア	1,047
13	フランス	6,526	38	ベルギー	1,004
14	フィリピン	5,431	39	欧州連合	944
15	ブラジル	5,372	40	スイス	929
16	スペイン	4,662	41	ベトナム	897
17	ポーランド	3,996	42	チリ	799
18	ニュージーランド	3,534	43	南アフリカ	760
19	イスラエル	3,340	44	ギリシャ	688
20	イタリア	3,326	45	チェコ	687
21	パキスタン	3,015	46	ハンガリー	664
22	スウェーデン	2,935	47	ベネズエラ	583
23	シンガポール	2,849	48	エジプト	537
24	メキシコ	2,848	49	ウクライナ	528
25	ロシア	2,388	50	エストニア	488

<sup>11</sup> 集計期間は、平成 15 年 7 月から平成 20 年 12 月まで。