

平成 17 年下半期（7～12 月）における botnet 観測システム観測結果

- ・ **bot の感染活動**
～新しい脆弱性をねらう感染活動が発生～
- ・ **bot の情報収集活動～キーロガーが増加～**

下半期における観測結果の特徴

注意 以下の観測結果は、サイバーフォースセンターの観測システムで把握した botnet について、その実態を示したものである。

bot に感染したコンピュータ～bot 数調査はより困難に～

本システムでは、bot 数調査は指令サーバへ接続数を調査する命令を送信してその結果を集計している。本システムで把握した bot に感染したコンピュータ数は、上半期と比べて 95.9%減少した。下半期の減少は、bot 数調査命令の結果を返さないよう改造又は設定変更された指令サーバが増加していること及び個々の botnet そのものが小さくなってきていることが原因と推測される。

指令サーバ～高まる botnet の生き残り性能～

指令サーバのドメイン数は、上半期と比べ 17.5%減少し、指令サーバの IP アドレス数は 36.1%増加した。これは、指令サーバの冗長化を図るために、1つの指令サーバドメインに複数の IP アドレスを割り当てる傾向が強くなっているものと推測される。

bot の感染活動～新しい脆弱性をねらう感染活動が発生～

今期は、Zotob ワームで使用されたプラグアンドプレイの脆弱性（MS05-039）、Server Message Block（SMB）プロトコルの脆弱性（MS05-027）等をねらった感染活動が新たに観測されている。これからも、新たな脆弱性をねらった感染機能が bot に追加されていくものと推測される。

bot の情報収集活動～キーロガーが増加～

上半期と比べネットワーク情報表示機能の使用が大幅に減少した一方、キーロガーの使用が大幅に増加している。これは、犯罪者が、ID やパスワードのような利用価値の高い情報の収集に力を入れているものと推測される。

bot の攻撃活動～より防御の困難な攻撃手法への移行～

防御技術が確立してきた SYNflood 攻撃は上半期と比べ 81.5%減少したが、UDPflood 攻撃が 66.8%増加、SYNFlood・ACKflood を複合した攻撃も 414.2%増加しており、より防御が困難な攻撃方法への移行が進んでいるものと推測される。

まとめ～高まる botnet の危険性～

以上のとおり、botnet の活動の傾向は、より危険な方向に変化を続けている。コンピュータの利用者は、bot に感染しないために「オペレーティングシステムやアプリケーションの修正プログラムの適用」、「ウイルス対策ソフトの導入及び定義ファイルの更新」といった基本的な情報セキュリティ対策を、常に心がけることが大切である。

目次

1	概要.....	P.4
2	botnet 観測結果.....	P.4
(1)	接続 bot 数.....	P.4
(2)	botnet 指令サーバ(国別).....	P.6
(3)	botnet 指令サーバ(接続ポート別).....	P.6
3	botnet 活動状況.....	P.7
(1)	感染活動状況.....	P.8
(2)	情報収集活動状況.....	P.10
(3)	攻撃活動状況.....	P.11
(4)	チャット.....	P.12
4	おわりに.....	P.13

1 概要

サイバーフォースセンターでは、botnet の現状を把握するため、botnet 観測システムを構築し、平成 17 年 1 月から運用している。以下では、17 年下半期における観測結果を紹介するので、今後の botnet 対策の参考としていただきたい。

なお、botnet の概要については、17 年 1 月 27 日から *@police* に掲載している「ボットネット(botnet)に注意」¹ を、17 年上半期観測結果及び命令の解説については「平成 17 年上半期（1～6 月）における botnet 観測システム観測結果」²を参照願いたい。

2 botnet 観測結果

(1) 接続 bot 数

図 1～3 は観測している botnet に接続されたコンピュータについて集計したものである。

図 1 の bot の国・地域別比率では、上位の国々の割合には大きな差はない。「その他の国」とは、国が判別できた IP アドレスのうち、上位 7 位以外の合計である。「不明」とは、国が判別できない、又は意図的に隠されている IP アドレスの合計である。この割合が多い理由としては、botnet を観測する仕組み（システム）の存在が botnet 使用者の間で知られてきており、意図的に IP アドレスを隠すように bot が改良されている場合が多くなってきているためである。

図 2 の上半期との比較では、下半期の bot 台数が上半期と比べて 95.9%減で大幅に減少している。当システムでは、bot 数調査は指令サーバへ接続数を調査する命令を送信してその結果を集計している。下半期の減少は、bot 数調査命令の結果を返さないよう改造又は設定変更された指令サーバが増加していること及び個々の botnet のサイズが小規模化していることが主な原因と推測される。

なお、図 3 の bot 数の週別推移で 11 月と 12 月に bot 数が急増しているのは、bot 数調査が可能な幾つかの中規模 botnet を観測できたことが原因である。

観測期間	自 平成 17 年 7 月 1 日 至 平成 17 年 12 月 31 日
指令サーバのドメイン数	118 ドメイン（前期比 25 ドメイン減、17.5%減）
bot 数	52,723 台（前期比 1,232,524 台減、95.9%減）
bot 数（日本）	5,178 台（前期比 139,334 台減、96.4%減）

¹ ボットネット(botnet)に注意 [PDF: 約 85KB]

http://www.cyberpolice.go.jp/detect/pdf/H170127_botnet.pdf

² 平成 17 年上半期（1～6 月）における botnet 観測システム観測結果 [PDF: 約 73KB]

http://www.cyberpolice.go.jp/detect/pdf/20051025_botnet.pdf

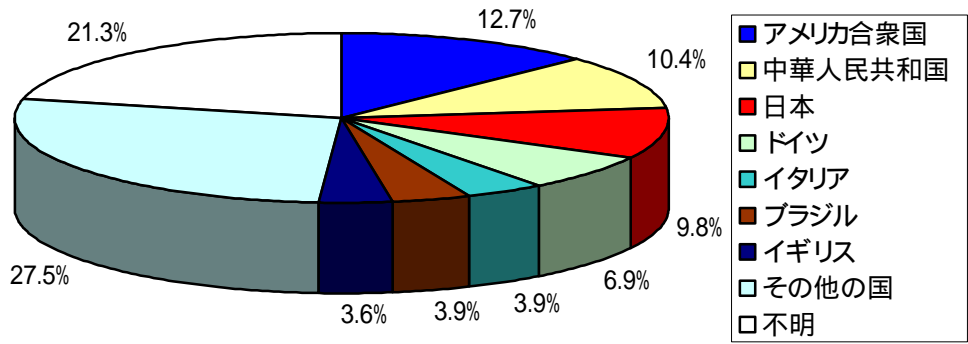


図1 botの国・地域別比率

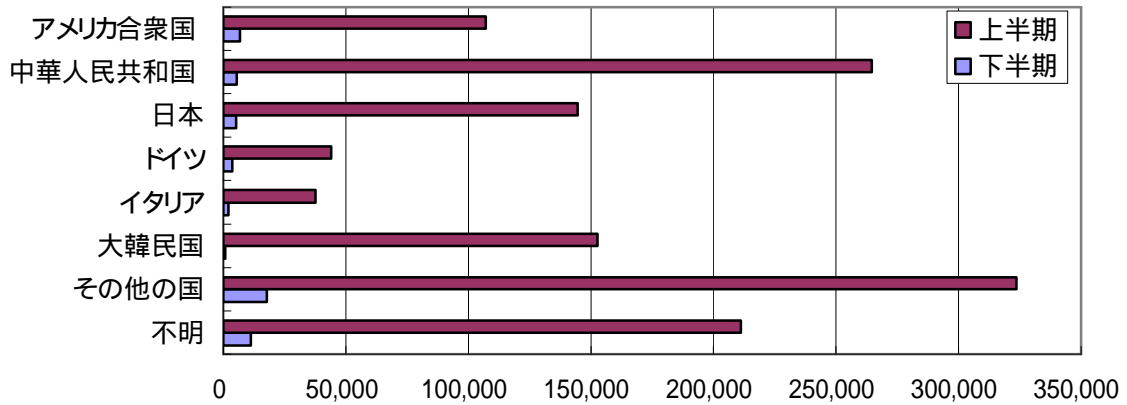


図2 botの国・地域別台数(前期比)

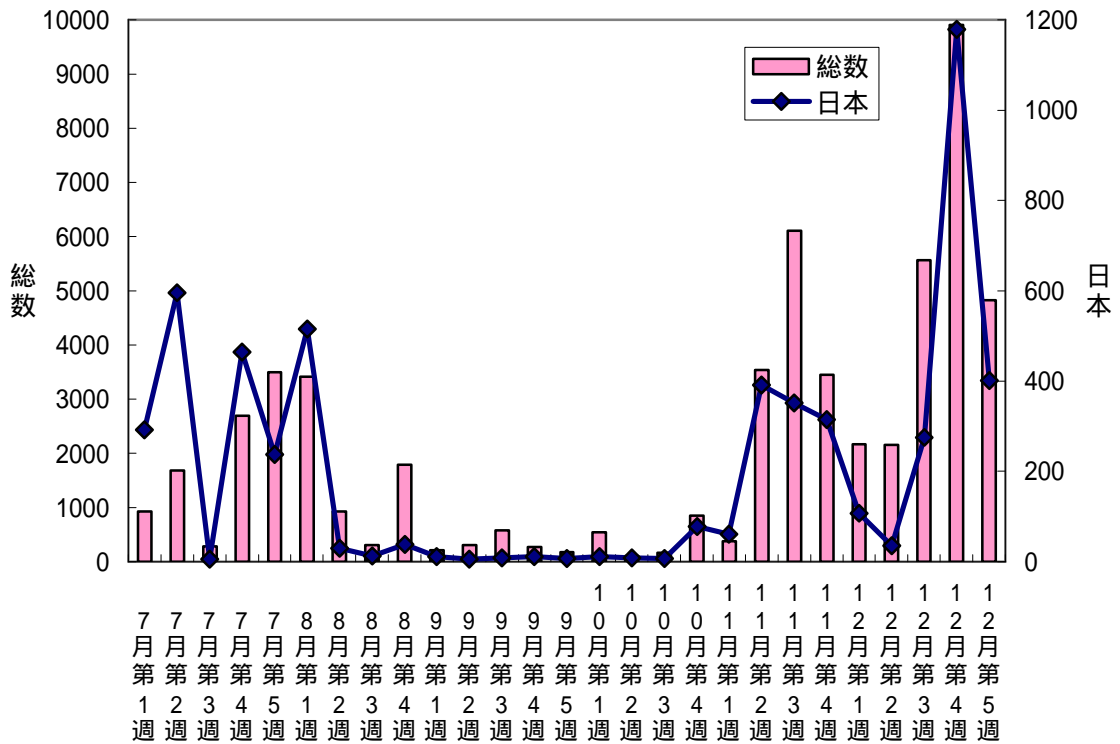


図3 bot数の週別推移

(2) botnet 指令サーバ(国別)

図4は当システムで観測しているbotnet 指令サーバのIPアドレスの国・地域別比率である。指令サーバに使用されているドメインは、複数のIPアドレスを割り当てているものも多い。指令サーバドメイン数は、前期と比べ17.5%減少し、指令サーバIPアドレス数は36.1%増加した。

指令サーバの1ドメイン当たりの指令サーバIPアドレス数は、前期が約4.6個に対して今期は約7.7個であり、このことから、1つの指令サーバドメインに複数のIPアドレスを割り当てる傾向がより強くなってきていると推測される。このように複数のIPアドレスを割り当てることにより指令サーバの冗長化を図っているものと思われる。

また、日本のIPアドレスを使用している指令サーバは48アドレスあり、DNSを逆引きした結果、そのうち42アドレスが国内プロバイダの一般利用者に割り当てられていると推測されるホスト名であったことから、概ね個人ユーザのPCと推測される。

観測期間	自平成17年7月1日 至平成17年12月31日
指令サーバのドメイン数	118ドメイン(前期比25ドメイン減、17.5%減)
指令サーバのIPアドレス数	904アドレス(前期比240アドレス増、36.1%増) 1ドメインに対してIPアドレスが複数設定されている場合が多いため、指令サーバドメイン数とは異なる
指令サーバのIPアドレス数(日本)	48アドレス(前期比45アドレス減、48.4%減)

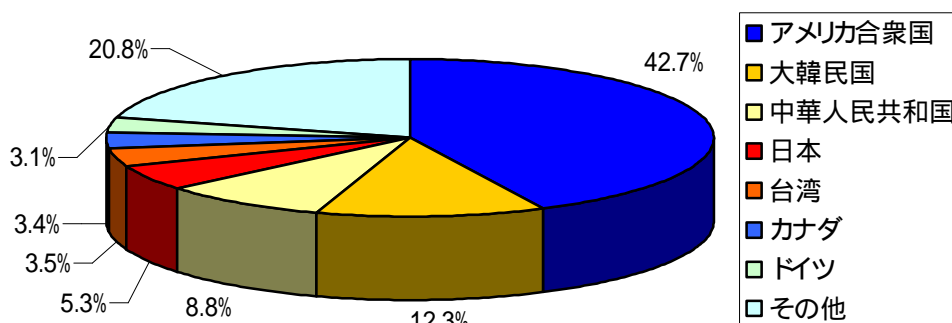


図4 指令サーバの国・地域別比率

(3) botnet 指令サーバ(接続ポート別)

図5は当システムで観測対象となった指令サーバの接続ポート別の比率を示したものである。最も多かったポートは、一般的なIRCサーバで使用される6667/tcpであり、全体の5割を占めている。次に多かったのがプロキシサーバで使用されている8080/tcpであり、以下は、60000/tcp以上、特に65000~65535/tcpが比較的多くなっている。これらの比率の傾向は上半期と比較して大きな変化はない。

観測期間	自平成17年7月1日 至平成17年12月31日
指令サーバのドメイン数	118ドメイン（前期比25ドメイン減、17.5%減）
指令サーバのポート数	143個 指令サーバには複数のポートが存在することもあるため、ドメイン数よりも多い。

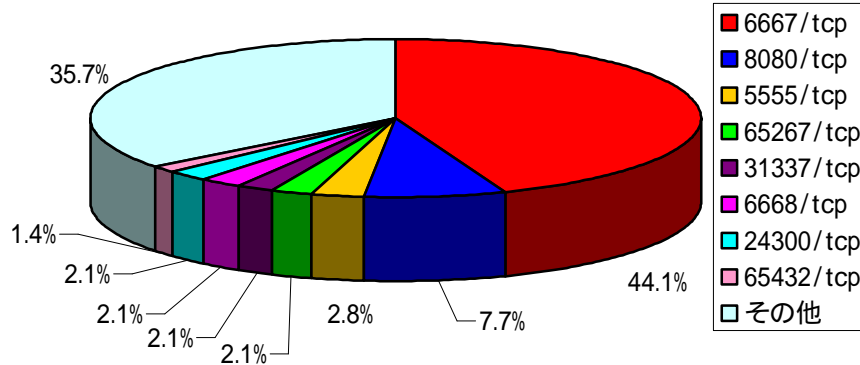


図5 指令サーバの接続ポート別比率

3 botnet 活動状況

図6は当システムで観測した命令等の流れを図に表したものであり、図7～8は当システムで観測した命令等を種類別に分類・集計したものである。最も多かったのはチャットで、下半期の58.2%を占めている。この増加の原因は、ある特定のbotnetにおいて12日間で3万数千件に上るチャットが観測されたためである。

なお、前期同様、命令実行結果を除外しているのは、指令サーバによって実行結果を表示しないもの（別チャンネルで表示など）が存在するためである。

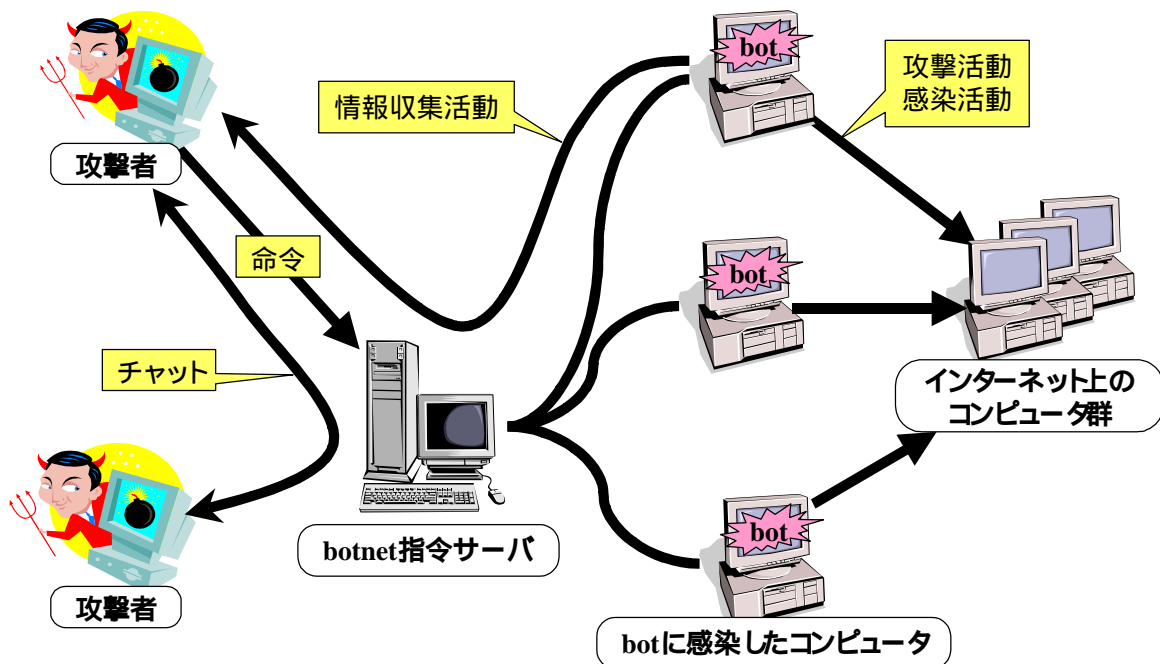


図6 命令種類別関係図

観測期間	自平成17年7月1日 至平成17年12月31日
指令サーバのドメイン数	118ドメイン（前期比25ドメイン減、17.5%減）
命令総数	84,315件（前期比41,778件減、33.1%減）

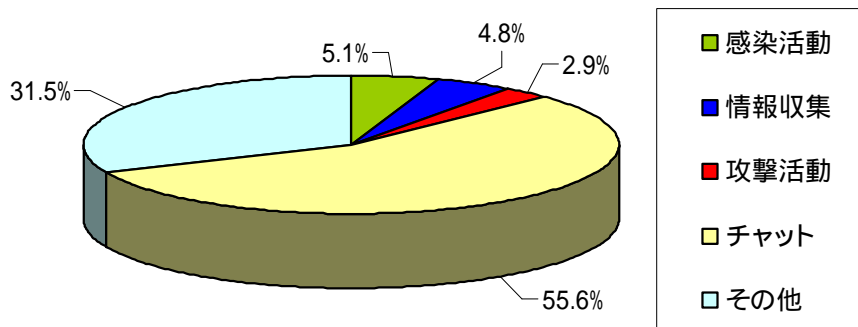


図7 命令活動別比率

各命令の詳細は後述

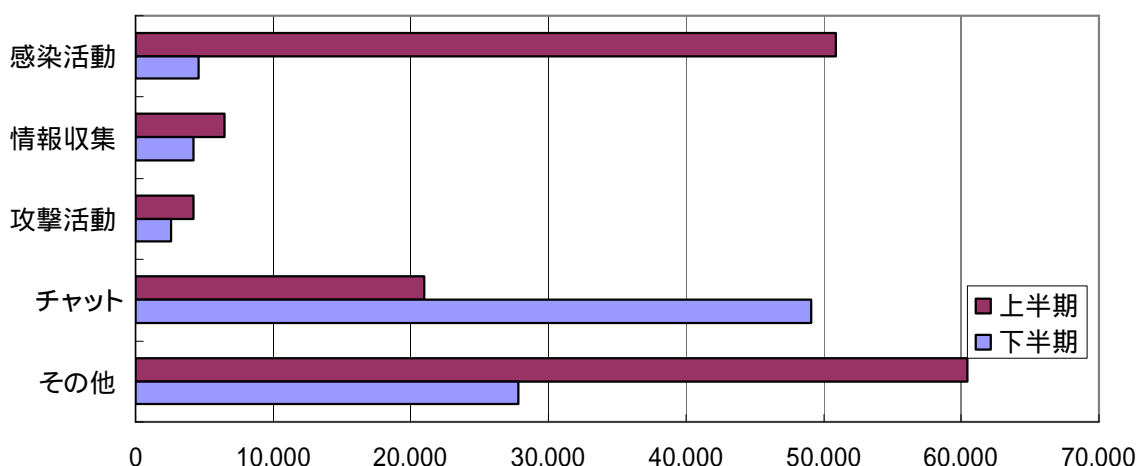


図8 命令活動別件数（前期比）

(1) 感染活動

図9～11は当システムで観測した感染活動命令を集計したものである。

図9の手段別比率では、前期と同じく135/tcpポートを通じてWindowsのdcomの脆弱性を悪用して感染を拡大する命令が最も多く、全体の半分近くを占めている。

図10のポート別比率では、135/tcpについてはdcom135が大部分を占めるため、図9とそれほど変化はない。しかし、445/tcpは、Isassの脆弱性を始め、今期新たに観測されたZotobワームで使用されたプラグアンドプレイの脆弱性（MS05-039）、同じくServer Message Block（SMB）プロトコルの脆弱性（MS05-027）といった様々な種類の感染活動が観測されている。

図11の上半期との比較では、感染活動命令の件数は91.1%減少しており、135/tcp

へ dcom の脆弱性を悪用して感染を拡大する命令も 93.6%減少、445/tcp へ lsass の脆弱性を悪用して感染を拡大する命令も 88.9%減少している。この原因としては、前期では目立っていた、同一指令サーバから、繰り返し同一感染活動命令が発せられるという状況が減少した点が挙げられる。また、今期に観測された感染活動の種類は 18 種類で、前期の 34 種類と比べると半減しており、感染の拡大の手段がより有効な感染方法に絞られてきたものと推測される。

観測期間	自 平成 17 年 7 月 1 日 至 平成 17 年 12 月 31 日
指令サーバのドメイン数	118 ドメイン (前期比 25 ドメイン減、17.5%減)
感染命令総数	4,545 件 (前期比 46,323 件減、91.1%減)

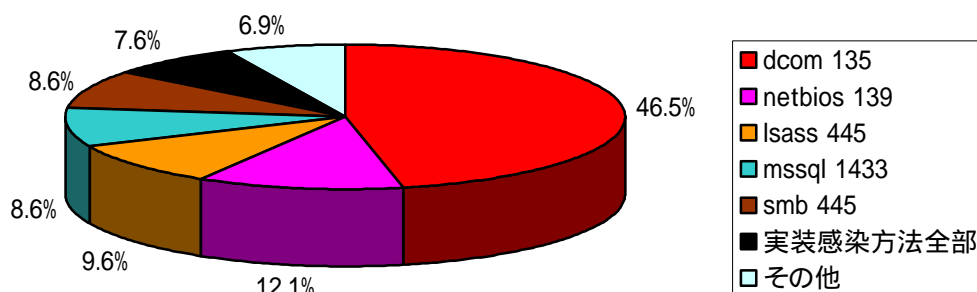


図 9 感染活動命令手段別比率

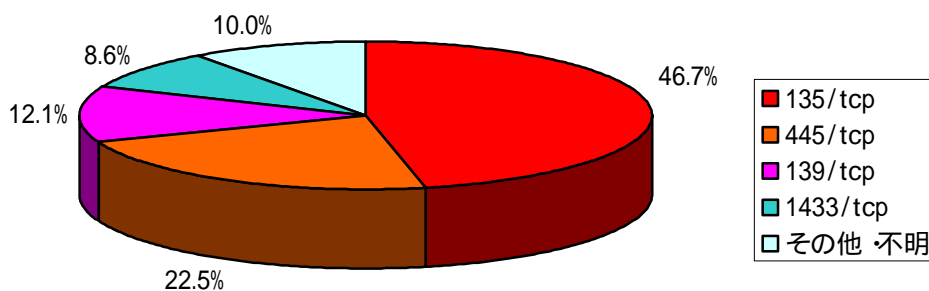


図 10 感染活動命令ポート別比率

「実装感染方法全部」は「その他・不明」に分類

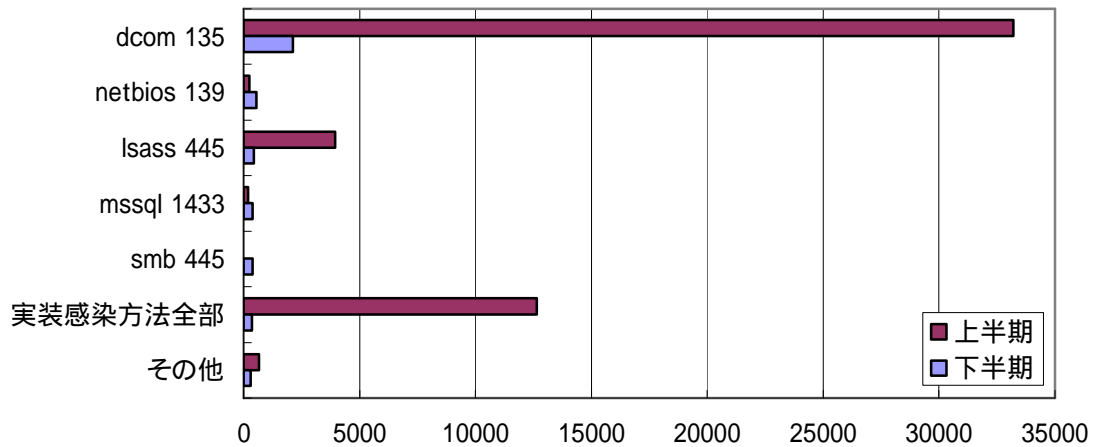


図 11 感染活動命令手段別（前期比）

（２）情報収集活動

図 12 は観測された情報収集活動に関する命令を集計したものである。前期と比較してネットワーク情報表示の命令が大幅に減少した一方、キーロガーに関する命令が大幅に増加した。これは、IP アドレスなどのネットワーク情報よりも、ID やパスワードのような犯罪者にとって価値の高い情報を収集する傾向が強くなってきているためと推測される。

観測期間	自 平成 17 年 7 月 1 日 至 平成 17 年 12 月 31 日
指令サーバのドメイン数	118 ドメイン（前期比 25 ドメイン減、17.5%減）
情報収集命令総数	4,208 件（前期比 2,227 件減、34.6%減）

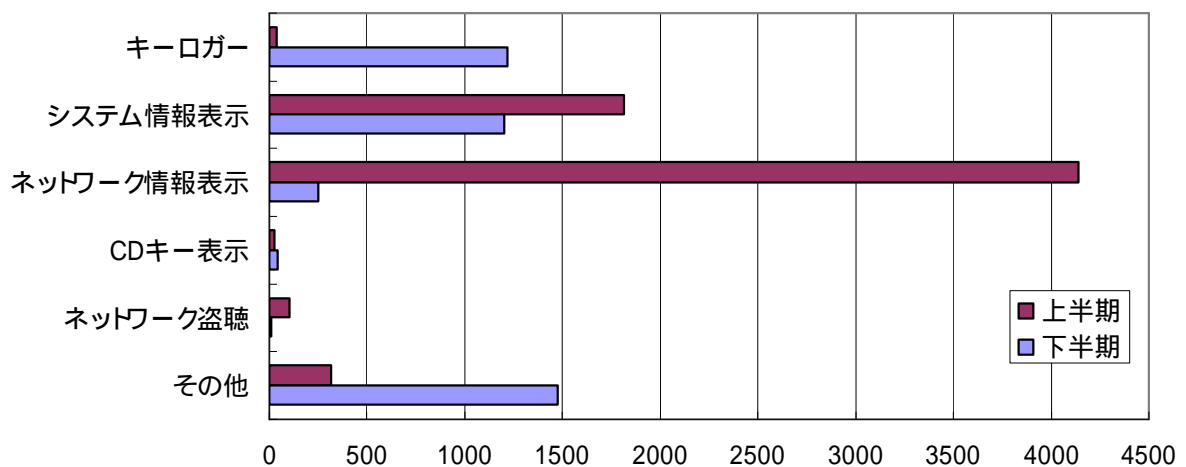


図 12 情報収集活動件数（前期比）

(3) 攻撃活動

図 13～15 は当システムで観測した攻撃活動命令について集計したものである。

図 13 の攻撃先国・地域別比率では、最も多いアルゼンチンと、次に多いセルビア・モンテネグロを合計すると全体の 5 割を占めている。これは、同じ IP アドレスに対して、多数の攻撃命令がなされたことから、件数が極端に多くなったことが原因である。なお、今期の国内の IP アドレスへの攻撃は観測されていない。

図 14 は、攻撃活動命令の手法別比率である。SYNFlood 攻撃は前期と比べ 81.5% 減少したが、UDPFlood 攻撃は 66.8% 増加した。また、SYNFlood・ACKFlood を複合した攻撃も 414.2% 増加したことから、攻撃手法がより防御が困難なものに移行してきているものと推測される。

図 15 は、当システムで観測した攻撃活動命令 (SYNFlood 攻撃のみ) の宛先ポート別比率である。最も多いポートは 80/tcp で、web サービスをねらった攻撃により、ホームページの閲覧を困難又は不能にさせることが目的と思われる。次に多い 6667/tcp は、IRC サービス (チャット) に使用するポートで、botnet 管理者同士が互いに争う中で、相手の botnet の指令サーバを攻撃しているものと推測される。

観測期間	自 平成 17 年 7 月 1 日 至 平成 17 年 12 月 31 日
指令サーバのドメイン数	118 ドメイン (前期比 25 ドメイン減、17.5%減)
攻撃命令総数	2,569 件 (前期比 1,611 件減、38.5%減) うち、日本対象の IP は無し

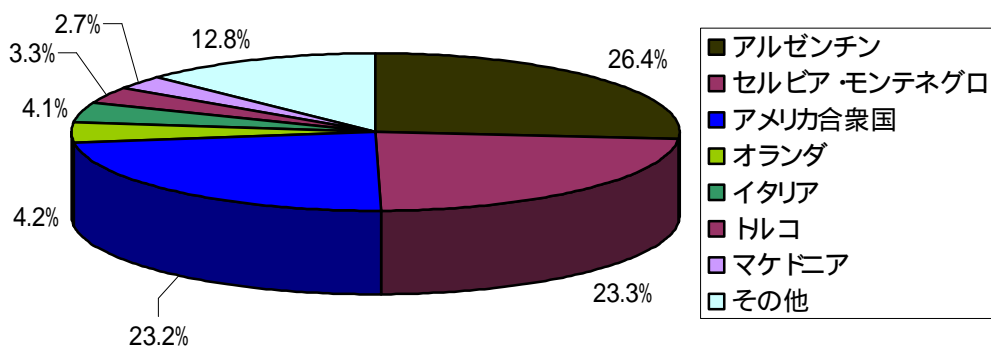


図 13 攻撃活動命令の攻撃先の国・地域別比率

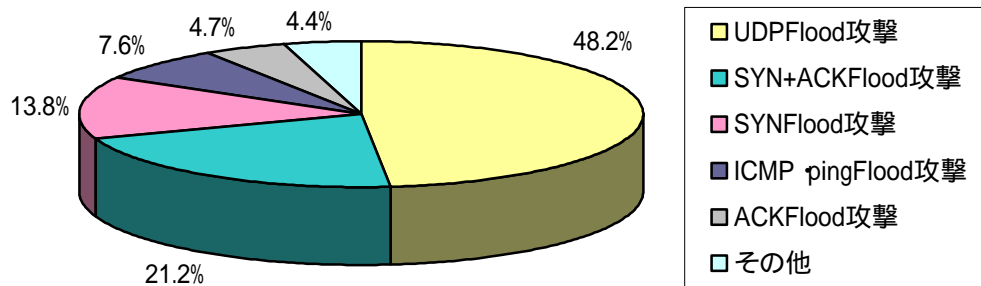


図 14 攻撃活動命令の手法別比率

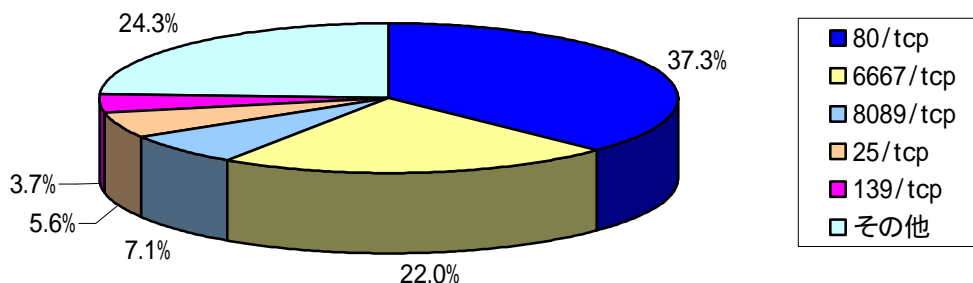


図 15 攻撃活動命令のポート別比率 (SYNFlood 攻撃のみ)

(4) チャット

一般的に botnet では、bot に指令を送るために IRC サーバを使用しているが、IRC は、本来チャット（キーボードを介した会話）のためのシステムであることから、いわゆるチャットにも使用可能である。ここで交わされる内容は、主に botnet 使用者同士が情報交換のために会話しているものと推測される。

ア チャット例 1（元は英語）

- > この bot は今スキャンしているが、rxbot には flood コマンドがない。
- > スキャンのみである。
- > ハッカーチームは gtbot を持っている。
- > しかし、私はそれをコンパイルする方法を知らない。
- > 私はこのチームのマスターである。
- > gtbot をコンパイルする方法を教えてください。
- > 私は持っている。
- > 私は rxbot の flood コマンドを持っている。
- > しかし、rxbot は最低で、gtbot の方がいい。
- > この bot にはログがある？。

- > あなたは、gtbot のためにダウンロードをする必要がある。
- > あなたは flood コマンドで攻撃できる。
- > そして、それを繰り返す。

イ チャット例 2 (元は英語)

- > このネットワークは小さい。
- > あなたは 1 つでも作ったことがあるのか？。
- > botnet を持っている大多数の人々は、少なくとも 1000 台の bot がある。
- > 少なくとも、ddos 攻撃をするために。
- > へー。
- > しかし、このネットは 100,000 台の bot がある。
- > あなたは bot を作ったことがある？。
- > もちろん。
- > これらのように、
- > まず始めに、できるだけ多くのコンピュータに、手動でウイルスをアップロードせよ。
- > r00ting として知られている。
- > その命令は、bot から netbios の有害プログラムに対して脆弱であるかどうかをインターネット上でランダムなコンピュータをスキャンさせるものである。
- > 脆弱であれば、bot をアップロードする。
- > 非常に簡略化された説明である、ところで。

4 おわりに

これまで述べた観測結果のとおり、botnet の活動の傾向は常時変化し続けている。コンピュータの利用者は、bot に感染しないために「オペレーティングシステムやアプリケーションの修正プログラムの適用」、「ウイルス対策ソフトの導入及び定義ファイルの更新」といった基本的な情報セキュリティ対策を、確実に実施することが重要である。

botnet 使用者による観測者対策により botnet 観測は困難になりつつあるが、サイバーフォースセンターでは、国内外の関係各機関との連携強化を含め、botnet の活動の把握に努めていく。