JPCERT CC®

ボットネットの概要

～報告書～

有限責任中間法人 JPCERT コーディネーションセンター

第1章 はじめに

ウイルスやワームによる大規模インシデントは、これまでに多数の被害をもたらした情報セキュリティ上の重要な問題と言える。しかし、2004 年 4 月の Sasser ワームを最後に、大規模なウイルス・ワームの感染は報告されていない。唯一の例外は、限定的な被害をもたらした 2005 年 8 月の Zotob だけである。

一方で、フィッシング詐欺による金銭的な被害の発生や、スパイウェアによるアカウント情報の流失が報道される事が増えている。さらに、2006 年には、スピア攻撃（Targeted Trojan）による政府機関などへの侵入の試みが報道された。このような変化は、ボットネットを中心とした、アンダーグラウンドビジネスの確立が背景にあるものといわれている。先に紹介した Zotob も、ボットネットを構築するボットと呼ばれるものである事も、この変化を象徴的に物語っている。

日本おいてボットネットが注目されるようになったのは、2004 年の 7 月に、大量のスパムメールが送信された事件がきっかけとなった。この事件では、メールのあて先（ユーザ名）が総当りであったたこと、また、メールの送信元アドレスが偽装されていたことから、大量のエラーメールが ISP のメールサーバに送られ、大きな負荷をかけた。これらのメールは、数百～数千のソース IP アドレスから送信されていることなど、従来の第三者中継を利用するスパムとは明らかに異なる様態であったために TELECOM ISACJapan が調査を行ったところ、ボットネット(Zombie Cluster の存在が明らかになり、スパムの送信元として利用されるだけではなく、DDoS 攻撃も可能であること、感染機能も持つことなどが分かり、今までに無い大きな脅威に直面していることが分かってきた。

この脅威を把握し対策を立案することを目的として、平成 16 年度に JPCERT/CC、 TELECOM ISAC Japan でボットネットの調査を行ったところ、ボットネットは、ウイルスやワームといった単に感染を広げていくものとは本質的に異なる脅威であることが分かってきた。つまり、ワームやウイルスは、プログラムを解析することで動作や脅威を予測し、対策を行うことができるが、ボットネットは、人的な操作によって任意の活動を行うため、存在が潜在化するだけでなく、任意のタイミングで任意の活動を行うことが可能であり、さらに、ボットネットを利用してボットの自身の更新を行うことができる点が大きく異なっている。

しかしながら、ボットネットの脅威については、問題の本質をつかむことが難しい面があり、結果としてボットネットの対策が後手にまわってしまっている。本ドキュメントでは、ボットネットについての実態を、多くの方に知ってもらうことを目的として、「ボットネットの基本的な仕組み」、「ボットネット被害の例」、「ボットネットの脅威の背景」について紹介する。

第2章 ボットネットの基本的な仕組(用語解説)

2.1 ボットネットとは

ボットネットとは、ボットと呼ばれるウイルスの一種が構成するネットワークの総称で、数百～数万台の規模で構成される。ボットネットは、通常のウイルスやワームとは異なり、**HERDER**(牧夫)または **MASTER** と呼ばれる人間の指示により、DDoS 攻撃やスパムメールの送信といったさまざまな活動を行う。

ボットネットの多くは、IRC メカニズムを使ってネットワークを構成する。IRC メカニズムを利用するボットを **IRC ボット**、IRC ボットで構成するボットネットを **IRC ボットネット**と呼ぶ(図 1)。なお、IRC メカニズムの他に、P2P(Pear to Pear 図 2)や Web の仕組みを利用するボットも存在するため、制御の中心となるサーバを **C&C**(Command and Control)または **C&C サーバ**(Command and Control Server)と呼ぶことが増えてきている。

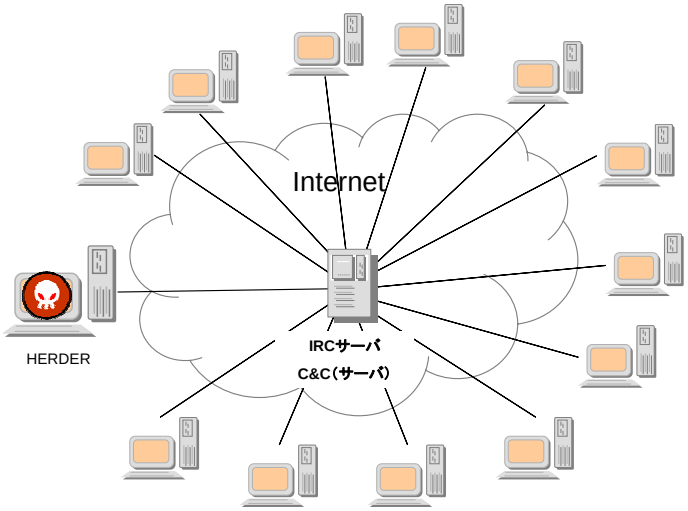

図 1 IRC ボットネットのイメージ

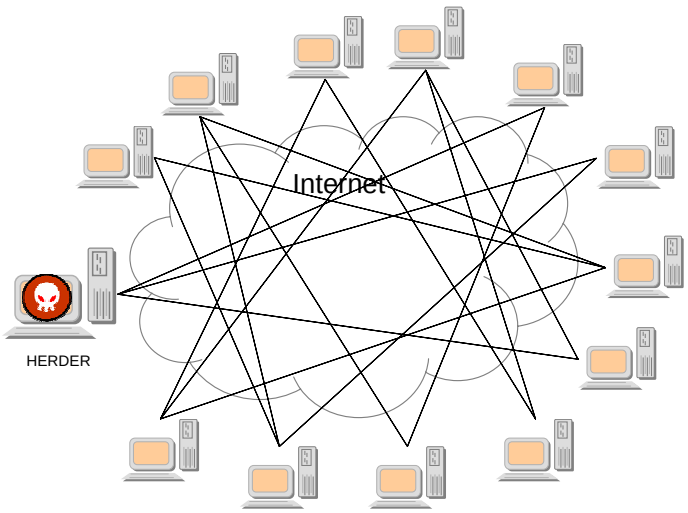

図 2 P2P ボットネットのイメージ(Pure P2P)

IRC ボットネットは、IRC メカニズムが実装されている複数のサーバを一つの IRC システムとして利用する場合がある。(図 3)。

このような構成をとった場合、大規模なボットネットの維持・管理が容易になるばかりでなく、一つのサーバが停止した場合でも、ボットが他のサーバに再接続を行うことでボットネットの機能を維持することができるようになる。

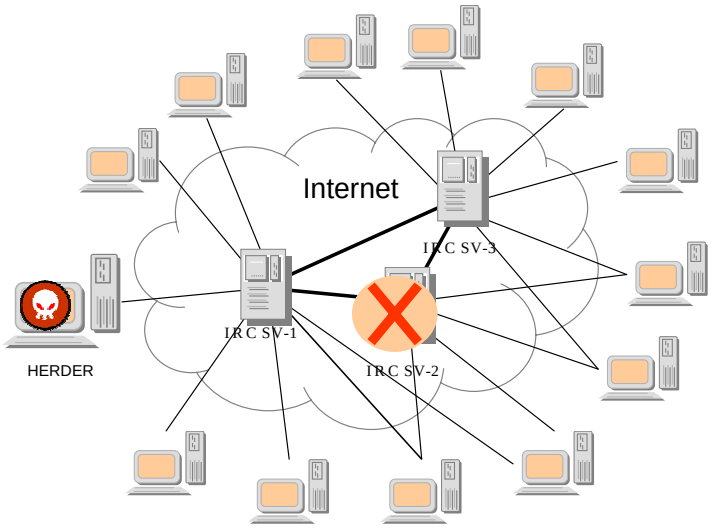

図 3 複数の C&C サーバを使用した堅牢性の確保

ボットネットの堅牢性を確保するため、C&C サーバのアドレスを短い TTL(Time To Live)で DNS サーバに登録する場合がある。この場合、C&C サーバに問題が発生した場合でも、DNS サーバのエントリーを書き換えることにより、C&C サーバを容易に他のサーバに切り替える事が出来る。

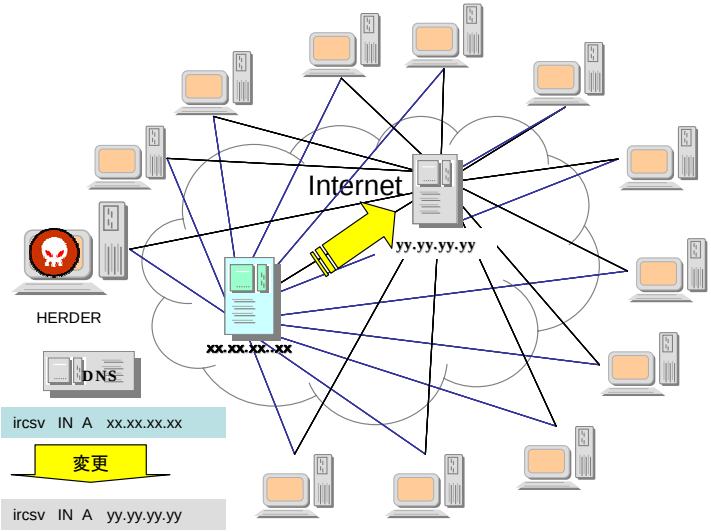

図 4 ダイナミック DNS を利用した C&C サーバの切替え

2.2 ボットネットと他のマルウェアの違い

ボットには、DDoS 攻撃機能、スパム送信機能、情報収集機能、感染機能など、数多くの機能が実装されている。このため、ボットはスパイウェアであり、ワームであり、バックドアであると言うことができる。ボットがこれらのスパイウェアやワームといったマルウェア（広義のウイルス）と異なる点は、個々の機能ではなく、ここまでに紹介したようなネットワークを構成する部分にある。違いを分かりやすくするために、マルウェアを表 1 のように分類した。各項目は排他的なものではなく、複数の項目に属するマルウェアが存在する。ボットの形態については、「有害プログラムの現在・過去・未来」に詳しく記載する。

表 1 ウイルス（マルウェア）の分類

感染形態に対する呼び方	**狭義のウイルス** メールやメディアを使って感染する 何らかのアクションで感染するもの	**トロイの木馬型感染** 実行を行わないと感染しないもの 実行ファイルの添付など	**ワーム** プログラムの脆弱性を使ってネットワークから感染する 利用者のアクションが無くても感染する	**受動型感染** WEBなどにアクセスすることで感染する
動作に対する呼び方	**感染活動** 感染活動、拡散活動を行う 必ずしも自動的とは限らない	**バックドア** 外部からの操作を有効にする機能を持つプログラムの総称	**スパイウェア** 利用者が意図しない動作を行うもので、情報を外部に送出する。	**DDoS Zombie** DDoS攻撃を行うための、ノード
形態に対する呼び方	**（単独：名称なし）** 特に連携をとらないもの DDoS機能をもつウイルスも、特に連携はとらない場合、このカテゴリ	**疎なネットワーク** バックドア機能を持つウイルスなどで構成される疎なネットワーク Sobig.Fなど	**密なネットワーク** DDoS Zombieに見られるような、ネットワーク構成感染・更新と操作が分かれているモデル	**ボットネット（ゾンビクラスタ）** 多数のノードを分散システム的に管理できる仕組みを持つもの
手法に対する呼び方	**フィッシング**	**SPEARフィッシング**	暴露型ウイルス	迷惑メール送信

2.3 ボット・ボットネットの機能

代表的なボットである Agobot(別名　Phatbot/Gaobot)を解析したところ、図 5 のような機能が実装されていることが分かった。なお、Agobot は Windows だけではなく、Linux 上でも動作することが確認されている(表 2)。

以下に代表的な機能を解説する。

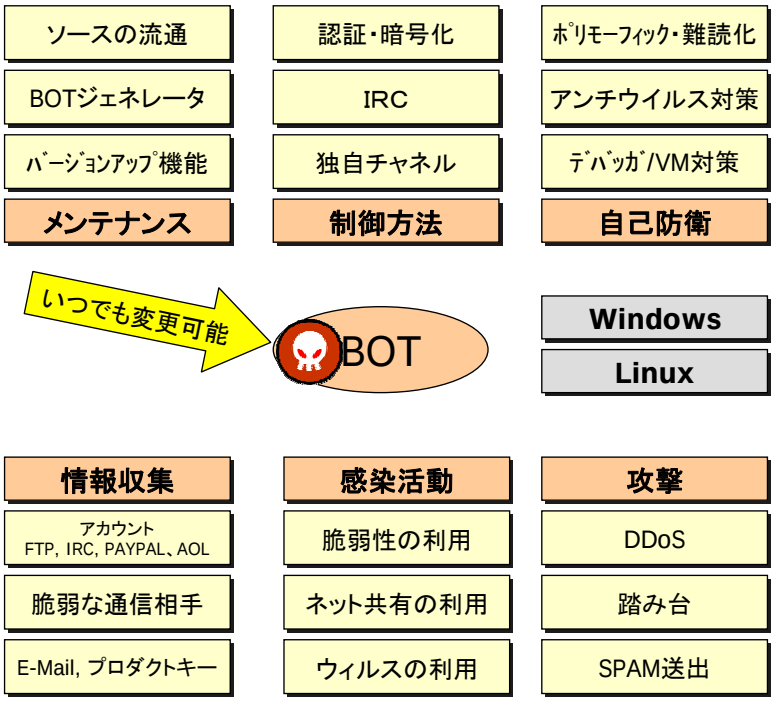

図 5　Agobot の代表的な機能

表 2　Agobot で動作検証済みとされるプラットフォーム

Debian 3.0	2.4.20-3-k6	libc6 / gcc version 3.3.1 20030728 (Debian prerelease)
Slackware 9.0	2.4.20	libc6 / gcc version 3.2.2
FreeBSD 4.8		libc6 / gcc version 3.3.1 20030728 (Debian prerelease) / compiled in debian
SuSe 8.1	2.4.21	libc6 / gcc version 3.2
Windows 2000 Server English	SP4	Visual Studio 6.0 SP5
Windows 2000 Server English	SP3	Visual Studio 6.0 SP5
Windows 2000 Pro English	SP4	Visual Studio 6.0 SP5
Windows 2000 Pro English	SP3	Visual Studio 6.0 SP5
Windows 2000 Pro German	SP1	Visual Studio 6.0 SP5

Windows 2003 Server English	SP0	Visual Studio 6.0 SP5
Windows 2003 Server English	SP1	Visual Studio 6.0 SP5
Windows XP Pro English	SP0	Visual Studio 6.0 SP5
Windows XP Home Polish	SP1	Visual Studio 6.0 SP5

2.3.1 メンテナンス機能

ボットネットのソースコードは、インターネット上で大量に流通している。

Agobot は、ソースコードだけではなく、開発環境として流通しており、ボットの動作を制御できる GUI プログラムも用意されていた。なお、Gaobot のソースコードは GPL となっている。

また、ボット自身を更新するための仕組みも用意されており、任意のタイミングでボットの入れ替えが可能であることがわかった。

2.3.2 制御方法

制御方法としては IRC を利用することが一般的だが、パスワードによるチャネルの保護や、暗号化(SSL)による通信の保護機能も実装されている。

また、実験的に P2P を使った通信手段が実装されていることから、今後は P2P を主要な通信経路として利用する可能性がある。P2P に移行した場合、ボットネット対策がより難しくなる点が懸念されている。

2.3.3 自己防衛

ボットには、様々な自己防衛機能が用意されている。主な防衛機能を以下に紹介する。

(1) アンチウイルス対策

ボットはアンチウイルスソフトの活動を阻害する。ボットは、アンチウイルスソフトのプロセスリストを持っており、このリストに含まれるプロセスを見つけると、そのプロセスを削除する。

さらに、システムの hosts ファイルに対して、アンチウイルスベンダのアドレスをループバックアドレス(127.0.0.1)等で書き込むことにより、アンチウイルスベンダが運営するサイトへのアクセスを阻害し、パターンファイルの更新を防いでいる。

プロセスリストおよびアドレスリストは、メンテナンス機能を使って常に更新されているものと考えられる。

(2) パターンマッチング対策・コード解析対策

コード解析を避ける目的で、ポリモーフィックエンジンの実装や、UPX(the Ultimate Packer for eXecutables ：実行可能ファイルを圧縮するツール)などを使った難読化も用意されている。

ポリモーフィックは、ランダムに生成される鍵を使って実行ファイルを暗号化する方法で、ひとつの実行ファイルが複数のパターンを持つため、パターンマッチングによる検出が難しくなる。

難読化は、実行ファイルを実行可能なままで変換する技術で、やはりパターンマッチングによる検出が難しくなる。

実際のボットは、これらの技術が組み合わされている場合も多く、単にボットに含まれる文字列を取り出すだけでも大変な手間がかかってしまう。

(3) デバッガ・仮想環境対策

Agobot は、デバッガ上または VMware 等の仮想システム上で実行されていることを検出する機能があり、これを検出した場合、活動を停止したり、自分自身を消去するものがある。

2.3.4 情報収集

ボットは単に攻撃を行うだけではなく、様々な情報の収集を行う。代表的なものを以下に紹介する。

(1) アカウント等の収集

ボットは、システムや通信内容からアカウントやアドレス、プロダクトキーの収集を行う。以下に Gaobot が収集するアカウント等の情報を記載する。

- AOL のアカウント
- FTP のアカウント
- PAYPAL へのアクセス
- E-Mail アドレス
- IRC 通信のオペレータ権限
- Windows のプロダクトキー
- 各種ゲームのプロダクトキー

(2) 脆弱なサーバ等の収集

Gaobot は、感染した PC のトラフィックを盗聴し、次の文字列を含む通信が行われた IP アドレスを収集する。

- OpenSSL/0.9.6
- Serv-U FTP Server
- OpenSSH_2

2.3.5 感染活動

Agobot には複数の感染機能が用意されているが、ボットの感染ルートは自身の感染機能に限定されるわけではない。

(1) 脆弱性を利用した感染

MS Blast などのネットワークワームと同様に、脆弱性を利用した感染を行う。

(2) Windows の共有機能を利用した感染

Windows の共有機能を使って感染活動を行う。

脆弱な設定や、安易なパスワードを利用する。

(3) 脆弱なアカウントを利用した感染

Windows や SQL サーバに対して、脆弱なアカウントに対する辞書攻撃を行う。

(4) ウイルス等のバックドアを利用した感染

Bagle や Mydoom が用意するバックドアを利用して感染する。

2.3.6 攻撃機能

ボットネットの攻撃機能として、DDoS 攻撃とスパム送信を取り上げる。

(1) DDoS 攻撃

ボットネットを使った DDoS 攻撃は強力であり、極めて厄介である。

Mark Handley の試算では、現在の高速ネットワーク環境においては、数百台規模のボットネットで任意のサイトに対する DDoS 攻撃を成功させることができるとしている。

Agobot は、複数の DDoS 攻撃方法が実装されており、また、任意の攻撃を追加することも容易である。

(2) スパム送信(Proxy 機能)

ボットネットを使ったスパムの送信は、IRC を経由したコマンドではなく、ボットの Proxy 機能を使って実行される。スパムの送信に多数のボットを利用した場合、多数の IP アドレスからメールが送信されることになり、IP あたりのスパム送信数を少なくすることが出来る。このため、IP アドレスあたりのメール送信数に基づくスパム対策を回避する事ができる。

2.4 ボットネットの利用のされ方

ボットネットの多様な機能を使って、アンダーグラウンドビジネスが行われているといわれている(図 6)。具体的な事例は、次章で紹介する。

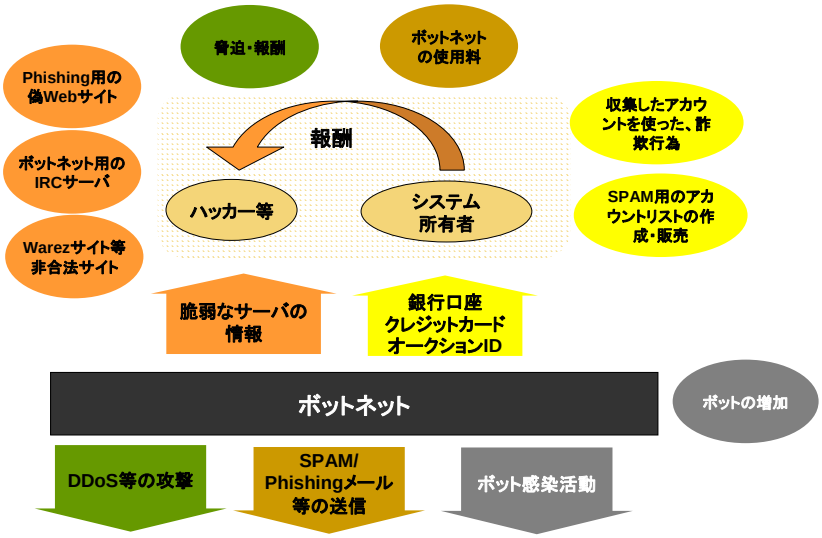

図 6 ボットネットとアンダーグラウンドビジネス

(1) スパム向けのボットネットのレンタル

ボットネットがスパムの送出に利用されているが、必ずしも HERDER が送信しているわけではなく、スパム送信者に対して、ボットネットに所属するボットの貸し出しを行うことで収益を得ている[1]。

なお、ボットネットによるスパムの送信は、IRC メカニズムなどの C&C 機能ではなく、ボットを OPEN Proxy として利用する。

(2) DDoS 攻撃による脅迫

ボットネットを使った DDoS 攻撃は、威力があるだけではなく、任意のタイミングでの開始・停止が可能である。

このため、DDoS 攻撃を仕掛けるぞとして脅迫を行い、脅迫に応じない場合は DDoS 攻撃によりターゲットのサービスを停止させるということが行われているといわれている。

(3) 脆弱なサーバ情報の収集

ボットネットでは、前述のスパム送出や DDoS 攻撃が話題になることが多いが、むしろスパイウェアとしての情報収集活動が中心的な活動と考えられる。

情報収集活動のひとつとして、脆弱なバージョンで稼動するサーバに関する情報を収集する。対象となるサーバは、主に UNIX 系のシステムが多い。

この情報を利用し、脆弱性を持つサーバが、C&C サーバ、Phishing サイト、Warez[2]サイトなどとして利用されるものと考えられる。

(4) クレジットカード番号等の収集

大規模なスパイウェアとしてボットネットを利用することで、大量のアカウント情報（クレジットカード番号、銀行口座情報、オークション ID、システムアカウント）やメールアドレスを取得することができる。

これらの情報が詐欺行為に利用されると、アカウント情報を盗まれた人にに金銭的な被害が発生する。

なお、これらの情報を収集した者が必ずしも直接詐欺行為を行うわけではなく、この情報を販売することで収益を得ている場合が多いといわれている。

(5) ボットの増殖・ワームのリリース

ワームの拡散速度は、初期のワーム数に大きく影響を受ける。Witty ワームなど悪質なワームの中には、ボットネットを利用して初期感染が行われたといわれるものが存在する[3]。

2.5 代表的なボット

すでに多数のボットが存在し、ソースコードや開発環境が容易に入手できることから、ほぼ無限に亜種が存在する。

---

[1] Mark Handley, University College London: “Dos-resistant Internet Subgroup Report” http://www.thecii.org/dos-resistant/ meeting-1/cii-dos-summary.pdf

[2] Warez：海賊版などの違法なソフトの意味

[3] The Honynet Project & Research Alliance, “Know your Enemy: Tracking botnets” http://www.honeynet.org/papers/bots/

ここでは、”Honynet Project “Know your Enemy: Tracking Botnets”[3]で取り上げられている代表的なボットについて、今回の調査で明らかになったその特徴を記載する。

(1) Agobot/Phatbot/Gaobot

最もよく知られたボットで、Windows と Linux で動作し、多数の亜種が確認されている。ソースコードは C++で記載され、GPL が宣言されている。一方で、以下の内容を含むドキュメントがある。

> 1. do not ever tell anyone about this site and group.
> 2. do not ever leak any shit to any person outside of group.
> 3. any exe's that you compiled from this source code is for your use only.
> 4. exe's should be kept to yourself.
> 5. if you have friend who wanting to give you bots. give them your other bot like sdbot.
> 6. I may add more rules here.
>
> results of not following those rules:
> being wonked for life from us.
> your sites will be reformatted.

トレンドマイクロ社によれば、Agobot に関する最初の登録があったのは 2002 年の 11 月である[4]。それから 3 年半を経過した現在の状況は、Agobot は”Phatbot”と呼ばれるようになり、数百の亜種を形成している。
ソフトウェア開発という観点において、インターネット上で入手可能なソースコードを比較した場合、Agobot は他の種と比較して最も洗練されたコーディングがなされているといえるだろう。
インターネット上に広く流通している Agobot のソースコードは、C および C++ を用いて 2 万行ほどの内容から形成されている。このソースコードによれば、Agobot は以下の機能を持つことが判読できる。

(1) IRC を使用した命令指揮機能
(2) 複数の脆弱性を悪用可能な感染機能
(3) 多様な DoS 攻撃機能
(4) ポリモーフィックエンジンによる難読化機能
(5) ネットワーク盗聴機能
(6) 感染 PC からの機密情報収集機能
(7) キーロガー機能
(8) (修正プログラム適用や設定変更による)自己防衛機能
(9) 広く利用されているデバッガによる解析の検知機能

---

[4] ウイルスデータベース(トレンドマイクロ株式会社)WORM_AGOBOT.A
http://www.trendmicro.com/vinfo/virusencyclo/default5.asp?VName=WORM%5FAGOBOT%2EA&VSect=T

これらの機能はモジュール方式によって実装されているため、後から容易に機能を追加することも可能である。また、Windows および Linux のどちらにもでも利用可能なコーディングがなされているという特色も持っている。

(2) SDBot

最も活発なボットで、トレンドマイクロ社の分類では、2005 年 3 月現在で、257 種類の亜種があるとされている。ソースコードは、C で書かれており、やはり、GPL を採用している。

トレンドマイクロ社の登録によれば、2003 年の 7 月に SDBot はウイルスとしての最初の登録が行われている[5]。SDBot は Agobot とは対照的に、非常に簡素な作りをしているが、今や非常に多くの亜種が発生している。インターネット上で見つけることのできる SDBot のソースコードは、C 言語によって記述されたわずか 2000 行のプログラムでしかない。ソースコードは GPL のもとで公開されており、基本構造として IRC による命令指揮機能を提供するのみにとどまっている。ただし、SDBot のソースコードに手を入れることは非常に容易であり、かつ、Agobot 同等の機能を提供するためのパッチもインターネットにおいて流通している。このようなパッチの流通が「カスタムメイド」なボットないしボットネットを作る犯罪者を支援する形になっていることは想像に難くない。

(3) RBot

トレンドマイクロ社の登録によれば、2004 年の 4 月に RBot はウイルスとしての最初の登録が行われている[6]。ソースコードが流通しているボットとしては後発になるが、現状で最も多い被害件数がトレンドマイクロ社に寄せられている※[6]。

インターネット上に流通している RBot のソースコードを分析してみると、以下の特徴が見て取れた。

(1) Windows 用に特化している

(2) 非常に多くの脆弱性を感染に利用することができ、かつ、それが最初から実装されている

(3) Web サーバや FTP サーバなどの機能も充実している

興味深い点としては、RBott に感染した PC にインストールされたファイル交換ソフトを伝播に利用する機能が実装されている点である。これは、eDonkey、KaZaA、LimeWire といった主要なファイル交換ソフトのアップロード用フォルダに RBot が自分自身を設置することで実現される。わが国においても、ファイル交換ソフトによる機密情報の流出事件が相次いでいる中で、このような機能が、広く流布しているボットに実装されている点は重要視してよいであろう。

(4) GT-Bots

米コンピュータアソシエイツ社によると、GT-Bot の最初のウイルス登録は 1998 の 4 月である[7]。これは、これまで紹介した中で最も早くその登録が行われている種のボットであることになる。ちなみに GT は(Global Threat:全世界

---

[5] ウイルスデータベース(トレンドマイクロ株式会社)WORM_SDBOT.GEN
http://www.trendmicro.com/vinfo/virusencyclo/default5.asp?VName=WORM%5FSDBOT%2EGEN&VSect=T

[6] ウイルスデータベース(トレンドマイクロ株式会社)WORM_RBOT.A
http://www.trendmicro.com/vinfo/virusencyclo/default5.asp?VName=WORM%5FRBOT%2EA&VSect=T

[7]米コンピュータアソシエイツ eTrust Spyware Encyclopedia GTBot

的脅威)の略称である。GT-Bot は HideWindow プログラムを使用し、Windows 用の mIRC クライアントを操作することで IRC による命令指揮機能を実現させている。GT-Bot は、さまざまな攻撃プログラムを同梱するパッケージソフトウェアとして展開することで、より多くの機能を実装させることができる。

(5) SpyBot

トレンドマイクロ社の登録によれば、2003 年の 6 月に SpyBot はウイルスとしての最初の登録が行われている。Agobot および SDBot のように、SpyBot は今や非常に多くの亜種が発生しているため、ここで説明の対象とした。

インターネット上で見つけることのできる SpyBot のソースコードは、C 言語によって記述された 3000 行のプログラムである。SpyBot の IRC による命令指揮機能は SDBot の発展形である。このことは、命令指揮機能のエンジン部分が SDBot と同一であることに顕著である。しかしながら、SpyBot は Agobot ほどの基本機能も持ち合わせておらず、また SDBot ほど積極的に機能拡張が行われた形跡は見当たらない。

(6) Kaiten/Q8Bot

UNIX/Linux 向けのボット。ボット本体はひとつのファイルになっており、wget などを使ってソースコードをダウンロードし、コンパイルすることが容易にできる。

(7) Perl Bots

Perl を使ったボットも確認されている。

UNIX/Linux で、perl を使ったアプリケーション(AWSTATS 等)の脆弱性を利用して感染する場合に利用されていることが確認されている。

---

http://www3.ca.com/securityadvisor/pest/pest.aspx?id=453073312

第3章 ボットネット被害の例

ボットによる代表的な事件をいくつか紹介する。

インターネットの検索サイト（google.co.jp）を使い、bot/zombie/ボット/ゾンビをキーワードとして検索を行ったところ、66 件の記事が見つかった。

記事の件数を表 3 に、記事の概要を表 4 に記載する。なお、表 3 において英文の記事については、翻訳したものを括弧書きで追記している。

表 3 見つかったボットネットの記事の数

	2002 年	2003 年	2004 年	2005 年
1 月		1		1
2 月			1	1
3 月			1	3
4 月			2	
5 月			5	3
6 月			5	1
7 月			1	6
8 月		1	3	7
9 月			4	3
10 月	1			6
11 月	1	3	2	2
12 月		1	1	
合計	2	6	25	33

表 4 ボットネット記事の概要

2002/9/24	「ウイルスの進化」を示した Slapper ワーム http://www.itmedia.co.jp/news/0209/24/ne00_slapper.html P2P ネットワークを形成する Slapper ワームの感染規模が約 7000 台で頭打ちとなった。だが、このようなワームはサイバー兵器として使えると懸念する専門家も
2002/10/7	2002/10/7 Slapper の修正を続けるウイルス作者たち http://www.itmedia.co.jp/news/0210/07/ne00_mighty.html Slapper ワームの亜種が少なくとも 4 つ発見されており、今後も増えていくと予想されている。もっとも、SSL の脆弱性を突くワームは「ピークを過ぎた」と指摘されている DevNull では「Kaiten」と呼ばれる広く知られたハッキングツールを利用する。これを使って、インターネットチャット上のあるチャネルを経由して感染サーバとワーム作者が交信する――と Symantec のセキュリティアーキテクト、Elias Levy 氏は説明している。
2003/1/9	2003/1/9　Sobig.a and the Spam You Received Today (Sobig.a とあなたが今日受け取っている Spam) http://www.lurhq.com/sobig.html This is the sordid tale of how a lone computer virus opened the door for millions of spam emails every day worldwide. In order for the reader to understand how this happened, this paper will explain some concepts in spam, viruses and backdoors. Viruses sometimes leave backdoors, also known as ″trojans″ on systems they infect; this is nothing new. The idea is to give the virus writer control over a large quantity of infected computers, establishing a virtual army of computers to do his or her bidding. The author of the virus discussed in this paper had a different idea: using a virus as the delivery mechanism, install anonymous proxy servers on thousands of computers worldwide. Instead of seeking to control the hosts, the virus author merely intended to establish a network of relay points through which they could direct their own connections, concealing their true origin wherever they went on the Internet. Whether or not the author intended it for the purpose of spam, this proxy network has been co-opted by spammers who use it to constantly flood the Internet with a variety of unsolicited commercial email while hiding from potential retribution.
2003/8/15	Microsoft.com falls to DOS attack (Microsoft.com が DOS で停止) http://www.computerworld.com/securitytopics/security/holes/story/0,10801,84074,00.html?from=story_picks The company is working with law enforcement officials looking into the attack
2003/8/21	2 Sobig.F ウイルスの成長率は過去最悪の可能性 http://internet.watch.impress.co.jp/cda/news/2003/08/21/203.html

	18 日ごろに発見された新しいウイルス「Sobig.F」が急速に感染を広めている。ウイルス対策会社の英 MessageLabs とロシアの Kaspersky は、共に Sobig.F が成長率において過去最悪のウイルスであると認めた。
2003/11/4	WorldPay floored by malicious attack （WorldPay がアタックで倒れる） http://www.theregister.co.uk/2003/11/04/worldpay_floored_by_malicious_attack/ WorldPay – the Royal Bank of Scotland's Internet payment outfit – appears to have been floored by a malicious attack.
2003/11/5	WorldPay fights 'massive, orchestrated' attack （WorldPay 大規模かつ組織的な攻撃と戦う） http://www.theregister.co.uk/2003/11/05/worldpay_fights_massive_orchestrated_attack/ WorldPay, the Royal Bank of Scotland's Internet payment transaction outfit, is continuing to fight a sustained Internet attack which has left its services mostly unavailable for a second day.
2003/11/11	WorldPay recovers from massive attack (WorldPay が大規模な攻撃から復帰) http://www.theregister.co.uk/2003/11/11/worldpay_recovers_from_massive_attack/ Analysis WorldPay's systems are back running normally this week following the most serious and sustained Internet attack on a UK business to date.
2003/12/9	Mafia recruiting spammers, crackers, AV chief warns （マフィアがスパマー、クラッカーをリクルートしていると、アンチウイルスベンダが警告） http://www.theregister.co.uk/2003/12/09/mafia_recruiting_spammers_crackers_av/ Spammers, beware – organised criminals are positioning themselves to take a slice of your business. Virus writing – once the sole province of hooligans – has edged itself into the arena of organised crime with viruses like Sobig-F that are capable of setting up a spam-sending proxy network.
2004/2/22	Trojans as spam robots: the evidence （スパムロボットとして活動しているトロイの木馬の証拠） http://www.theregister.co.uk/2004/02/22/trojans_as_spam_robots/ German magazine c't says it has evidence that virus writers are selling the IP addresses of PCs infected with Trojans to spammers. Spammers use these infected systems to unlawfully distribute commercial email messages, without the knowledge of their owners.
2004/3/21	Phatbot primed to steal your credit card details （Phatbot は、あなたのクレジットカードの詳細を盗み出す準備は出来ている） http://www.theregister.co.uk/2004/03/21/phatbot_primed_to_steal_your/ A Trojan horse-type computer virus called Phatbot can steal credit card numbers and launch denial of service attacks on Web sites. The new virus made its debut on the Internet on Friday (18 March), clogging bandwidth, stealing personal data and

	initiating denial of service attacks.
2004/4/30	The illicit trade in compromised PCs （感染した PC の違法な取引） http://www.theregister.co.uk/2004/04/30/spam_biz/ Investigators are piecing together the complex relationships between the virus writers, middlemen and criminal gangs held largely responsible for the growth of spam in recent months.
2004/5/11	Agobot 作成容疑者もドイツで逮捕される http://japan.cnet.com/news/sec/story/0,2000050480,20065907,00.htm Microsoft は 10 日（米国時間）、コンピュータに侵入して密かにシステムを乗っ取るプログラム「Agobot」を作成しインターネット上にばらまいたとされる男を、ドイツ当局が逮捕したことを認めた。
2004/5/11	トロイの木馬「Agobot」作成の容疑者逮捕 http://www.itmedia.co.jp/news/articles/0405/11/news010.html 危険度の高いトロイの木馬プログラム「Agobot」と「Phatbot」を作成したとして、ドイツの警察が 21 歳の男を逮捕した。男は容疑を認めているが、警察当局によれば、Sasser ワーム作成容疑で先に 18 歳の少年が逮捕された事件とは無関係だという。
2004/5/12	Phatbot ワーム作者の逮捕が、ゾンビ PC の取引を暴く http://www.cyberpolice.go.jp/international/europe_russian/20040515_000619.html Phatbot arrest throws open trade in zombie PCs http://www.theregister.co.uk/2004/05/12/phatbot_zombie_trade Phatbot ワームと Agobot ワームを作成した容疑で、ドイツ南部のバーデン・ヴュルテンベルク州に住む匿名の男が逮捕されたことにより、ゾンビコンピュータ(トロイの木馬型のワームに感染し、攻撃者からの命令で攻撃を行うコンピュータ)の違法な取引の解明が明るみになった。Netsky ワームよりは一般的ではない、Phatbot、MyDoom 及び Bagle のようなウイルスは、感染したコンピュータを操るために使用されている。これらのウイルスに感染したコンピュータは、スパムの中継装置として、又は分散サービス不能攻撃のために利用される。また、感染したコンピュータを利用することで、攻撃者は IP(Internet Protocol)アドレスのブラックリストによる防御を回避することが可能となる。ウイルス、ワームの作者は一般的に、感染したコンピュータのネットワークを取引している。Blaster ワームがインターネットで猛威を振るった 2003 年の夏には、10,000 台の感染コンピュータが 500 ドルで売られており、Abusive Hosts Blocking プロジェクトのアンドリュー・カーク氏によると、現在の価格は、恐らく当時の 2 倍になっているという。また、感染コンピュータの利用接続には、そのたびごとに 10 セントかかる。
2004/5/12	Phatbot arrest throws open trade in zombie PCs （Phatbot 作成者逮捕される） http://www.theregister.co.uk/2004/05/12/phatbot_zombie_trade/ The arrest of the suspected author of the Phatbot Trojan could lead to valuable clues about the illicit trade in zombie PCs. The arrest of the alleged Phatbot perp was overshadowed by the unmasking of the admitted Sasser author, Sven Jaschan. But the Phatbot case may shed the mostlight into the dark recesses of the computer

	underground.
2004/05/15	ドイツ警察、Agobot 作成容疑者を釈放 http://www.itmedia.co.jp/enterprise/0405/15/epi01.html トロイの木馬「Agobot」を作成したとしてドイツの警察に逮捕された 21 歳の男が 5 月 14 日釈放された。広報官によれば、Agobot に関する捜査は現在も継続中。
2004/6/15	Update: Akamai blames 'global DNS attack' for disruptions (Akamai のトラブルは、広範囲の DNS 攻撃が原因と非難) http://www.computerworld.com/developmenttopics/websitemgmt/story/0,10801,93837,00.html?from=homeheads Update: Akamai blames 'global DNS attack' for disruptions But a Web performance monitoring firm said it has no evidence of a wider attack
2004/6/15	ガートナー社:米国においてフィッシング詐欺が増加と報告 http://www.cyberpolice.go.jp/international/north_america/20040617_190553.html Gartner: Phishing on the rise in U.S. http://news.com.com/Gartner:+Phishing+on+the+rise+in+U.S./2100-7349_3-5234155.html ガートナー社の新しい調査結果によると、米国における窃盗被害中、フィッシング攻撃による被害が最も急速に増加しているとのことである。当座預金口座が窃盗被害にあったとの届出は、昨年中 198 万人に達しており、フィッシング詐欺は、被害総額 24 億ドル、被害者一人当たりの平均は 1200 ドルに上る。同社の 5 月の報告によれば、5700 万の消費者がフィッシング詐欺の電子メールを受け取っているとのことである。同社のアナリストであるアビバ・リタニ氏は、パーソナルコンピュータの 3 台に 1 台はキーロガーのようなスパイウェアが仕掛けられていると推測している。銀行は大半の詐欺に対しては適切な管理態勢をとっているが、フィッシング詐欺やキーロガーを利用した攻撃に対しては直接対抗する手段を持ち合わせていない。またフィッシング詐欺は、オンライン口座を新しく利用する人々を最大の標的としている。このような攻撃に対処し、銀行と顧客の関係を強化するために、より強力な消費者認証システムが必要とされている。
2004/6/16	Akamai Attack Highlights Threat From Bot Networks (Akamai への攻撃は、ボットネットの脅威を明らかにした) http://news.netcraft.com/archives/2004/06/16/akamai_attack_highlights_threat_from_bot_networks.html Akamai Attack Highlights Threat From Bot Networks Security Have hacker-controlled "botnets" grown mighty enough to disrupt even Akamai's content distribution network and its 15,000 servers? Until yesterday, the notion seemed far-fetched. But Akamai today offered more details on a distributed denial of service attack by a large network of "zombie" machines that bogged down its DNS system for several hours.
2004/6/16	Akamai now says it was targeted by DDoS attack (Akamai が DDoS アタックのターゲットであったことを認める) http://www.computerworld.com/printthis/2004/0,4814,93862,00.html Akamai now says it was targeted by DDoS attack It had earlier blamed a larger, global attack for yesterday's outage

	News Story by Jaikumar Vijayan
2004/06/17	「ゾンビ PC にやられた」--アカマイ、DNS サーバへの DDoS 攻撃を認める http://japan.cnet.com/news/sec/story/0,2000050480,20069290,00.htm 今週、Google や Yahoo などの主要ウェブサイトがアクセス不能状態に陥ったが、その原因となった DNS サーバへの攻撃は、「ボットネット」--つまり、ゾンビ状態にした家庭用パソコンを多数使ったものだったと、インターネット・インフラプロバイダの Akamai Technologies が 16 日（米国時間）に明らかにした。
2004/7/28	DDoSers attack DoubleClick （DoubleClick が DDoS 攻撃を受ける） http://www.theregister.co.uk/2004/07/28/ddosers_attack_doubleclick/ Internet ads firm DoubleClick was the victim of a distributed denial of service attack yesterday. A flood of malicious traffic from a network of zombie machines reduced DoubleClick's ability to serve ads over the Web, affecting many of its high-profile customers. Services have now been restored to normal. But at the height of the assault yesterday afternoon (UK time) the availability of Web pages featuring ads served by DoubleClick was severely reduced.
2004/8/26	FBI busts alleged DDoS Mafia (FBI DDoS マフィアを逮捕) http://www.securityfocus.com/news/9411 A Massachusetts businessman allegedly paid members of the computer underground to launch organized, crippling distributed denial of service (DDoS) attacks against three of his competitors, in what federal officials are calling the first criminal case to arise from a DDoS-for-hire scheme.
2004/8/31	U.S. Defense, Senate Computers are Zombie Spammers （国防総省、上院のコンピューターはゾンビスパマー） http://news.netcraft.com/archives/2004/08/31/us_defense_senate_computers_are_zombie_spammers.html U.S. Defense, Senate Computers are Zombie SpammersSecurity When the U.S. Justice Department stepped up its investigation of cybercrime, it found spam originating from an unexpected source: hundreds of powerful computers at the Department of Defense and the U.S. Senate. The machines were ″zombies″ that had been compromised by hackers and integrated into bot networks that can be remotely controlled to send spam or launch distributed denial of service attacks.
2004/8/30	Hackers hijack federal computers （ハッカーが米連邦政府のコンピュータを乗っ取る） http://www.usatoday.com/tech/news/computersecurity/2004-08-30-cyber-crime_x.htm Hundreds of powerful computers at the Defense Department and U.S. Senate were hijacked by hackers who used them to send spam e-mail, federal authorities say.

2004/9/7	IRC Botnet Found and Shutdown （IRC ボットネットを発見し、シャットダウン） http://isc.sans.org/diary.php?date=2004-09-07 We received a report this morning from the Telenor Security Operations Center(SOC) of an IRC botnet. The network contained over 10000 clients. The server has now been shutdown. If you have network traffic logs, you may want to check for connections from your hosts/network to the IRC server -- it was listening on IP 203.81.40.172 tcp port 10009
2004/9/9	Telenor takes down 'massive' botnet （Telenor が大規模なボットネットをシャットダウン） http://www.theregister.co.uk/2004/09/09/telenor_botnet_dismantled/ A network of more than 10,000 zombie PCs has been dismantled after security staff at Norwegian telco Telenor located and shutdown its controlling server.
2004/9/8	Going price for network of zombie PCs: $2,000-$3,000 （ゾンビ PC のネットワークの価格は、$2,000-$3,000） http://www.usatoday.com/tech/news/computersecurity/2004-09-08-zombieprice_x.htm Going price for network of zombie PCs: $2,000-$3,000 By Byron Acohido and Jon Swartz, USA TODAY In the calculus of Internet crime, two of the most sought-after commodities are zombie PCs and valid e-mail addresses.
2004/9/20	Rise of the Botnets （ボットネットの増加） http://www.theregister.co.uk/2004/09/20/rise_of_the_botnets/ The first half of 2004 saw a huge increase in zombie PCs. Also called bots, their average numbers monitored by security firm Symantec rose between January and June from under 2,000 to more than 30,000 per day – peaking at 75,000 on one day.
2004/11/17	「ネット攻撃の影に犯罪組織あり」--ベリサイン調査 http://japan.cnet.com/news/sec/story/0,2000050480,20075857,00.htm VeriSign が発表した最新の調査報告によると、オンライン攻撃の背後に犯罪組織がいるケースがこれまで以上に増えているという。 VeriSign は米国時間 16 日に発表した「Internet Security Intelligence Briefing」というタイトルのレポートのなかで、高度に組織化されたグループが複雑な攻撃を仕掛けるケースが増加していると述べた。 VeriSign のバイスプレジデント Mark Griffiths によると、犯罪組織が、家庭用 PC の設定を改ざんして攻撃を仕掛ける場合が増えているという。 「攻撃の内容が、子供のいたずらから、金銭を騙し取ることが目的の犯罪行為へと変わった」（Griffiths）
2004/11/25	専門家グループ、フィッシングの自動化に警鐘

	http://japan.cnet.com/news/media/story/0,2000047715,20076383,00.htm フィッシング対策ワーキンググループ（Anti-Phishing Working Group：APWG）によると、オンライン詐欺犯らが、影響範囲の拡大を狙ったソフトウェアツールやボットネットを使い、フィッシング行為の自動化を進めているという。
2004/12/21	Botnet used to boost online gaming scores （オンラインゲームの得点を稼ぐためにボットネットを利用） http://www.theregister.co.uk/2004/12/21/randex_botnet_fun_and_games/ Exclusive Teenagers convicted last week of setting up a huge network of compromised Windows PCs used it to gain an unfair advantage in online gaming – not to send spam.
2005/1/24	ギャンブルサイトを DDoS 攻撃から救うサービス http://hotwired.goo.ne.jp/news/business/story/20050126102.html オンライン・ギャンブルは、いつも格好の脅迫のターゲットで、脅迫行為はスーパーボウルの時期に限ったことではなく、かなり一般的に見受けられる。ギャンブルゲーム業界の分析を行なう米リバー・シティー・グループ社によると、オンライン・ギャンブル業界の 2004 年の売上は推定で 70 億ドルを超えたという。およそ 350 社にのぼる企業が少なくとも 1700 のギャンブル・サイトを運営している。また、オンライン・ギャンブルは、ほとんど法の規制の及ばない業界でもある――大半の企業が海外に本社を置いており、現地の警察には数千キロ離れたハッカーを追及するだけの捜査能力がないため、サイトの運営者たちは要求された金を支払わなければならないと感じる場合が多い。
2005/2/14	14-year-old 'downed Microsoft homepage for four hours' （14 歳がマイクロソフトのホームページを4時間停止させる） http://software.silicon.com/malware/0,3800003100,39127841,00.htm A teenage virus writer has been sentenced to three years' probation for committing a denial-of-service attack on Microsoft's homepage.
2005/3/14	Zombie PCs being sent to steal Ids （ゾンビ PC が、盗んだ ID の送信をはじめる） http://news.com.com/Zombie+PCs+being+sent+to+steal+IDs/2100-7349_3-5616202.html Bot nets, collections of compromised computers controlled by a single person or group, have become more pervasive and increasingly focused on identity theft and installing spyware, according to a Honeynet Project report.
2005/03/15	「ゾンビ PC が個人情報を盗む」--凶悪化するボットネットに警鐘 http://japan.cnet.com/news/sec/story/0,2000050480,20081328,00.htm Honeynet Project の報告によると、特定の個人やグループに支配権を奪われ、無力化されたコンピュータの集合体であるボットネットが、さらに勢力を拡大しており、しかも個人情報の窃盗やスパイウェアのインストールに使われることが増えているという。

2005/3/16	Bot nets use Windows for wicked work （ボットネットが、Windows を悪行のために使用） http://news.com.com/Bot+nets+use+Windows+for+wicked+work/2100-7349_3-5620592.html Despite Microsoft's renewed focus on security, recent research shows that computers running Windows XP and 2000 form the bulk of bot nets.
2005/5/23	Feds to fight the zombies （FBI がゾンビと戦う） http://news.com.com/Feds+to+fight+the+zombies/2010-1071_3-5715633.html Remote-controlled "zombie" networks operated by bottom-feeding spammers have become a serious problem that requires more industry action, the Federal Trade Commission is expected to announce on Tuesday.
2005/05/26	ウイルスよりもゾンビ PC--「サイバー攻撃の戦術に変化」と専門家 http://japan.cnet.com/news/sec/story/0,2000050480,20083909,00.htm ウイルス対策の専門家によると、ウイルス作者らは「Melissa」や「Blaster」のような世界的なウイルス流行を起こさないようにしているという。世界的流行となれば、ゾンビネットワークの構築／販売という彼らの中心的ビジネスに専念できなくなるためだ。
2005/5/26	Homeland Security flunks cybersecurity prep test （Homeland Security がサイバーセキュリティテストの準備に落第） http://news.com.com/Homeland+Security+flunks+cybersecurity+prep+test/2100-7348_3-5722227.html The U.S. Department of Homeland Security has failed to live up to its cybersecurity responsibilities and may be "unprepared" for emergencies, federal auditors said in a scathing report released Thursday.
2005/06/03	「Bagle」ワーム亜種 8 種類の来襲にウイルス対策企業が警戒 http://japan.cnet.com/news/sec/story/0,2000050480,20084127,00.htm 「被害を受けている PC に対するマーケットまで出現している。つい先日には、詐欺に関与している犯罪者やスパム業者が、乗っ取られた PC1 台につき約 5 セントを支払っていたことが判明している」（Thomas）
2005/7/6	「2005 年 5 月のフィッシング攻撃、226%増加で過去最悪」、米 IBM 調査 http://nikkeibp.jp/wcs/leaf/CID/onair/jp/comp/384379 米 IBM は米国時間 6 月 30 日,2005 年 5 月におけるネットワーク・セキュリティの脅威について調査した結果を発表した。それによると,当月はフィッシング攻撃が 226%増加し,今年 1 月のピークを上回った。 フィッシング攻撃が増加している理由は,大量の詐欺メールの送信に用いられる「ボットネット」が増えているため。ボットとは,第三者のパソコンを悪用することを主目的とした悪質なプログラムで,ボットが稼働している(ボットに感染している)マシンで構成されたネットワークをボットネットと呼ぶ。
2005/7/11	Report: Computer hijacking on the rise, （コンピューター乗っ取りの急増） http://news.com.com/Report+Computer+hijacking+on+the+rise/2100-7349_3-5783646.html

	Personal computers that play unwitting host to "zombie" code are proliferating at a startling pace, according to a new report.
2005/7/12	PC を乗っ取る「ボット」プログラムが急増――McAfee 調査 http://www.itmedia.co.jp/survey/articles/0507/12/news084.html McAfee の調査によれば、2004 年第 2 四半期は「ゾンビ PC」を生み出す「ボット」が大幅に増加したという。 セキュリティ企業の米 McAfee は 7 月 11 日、2005 年第 2 四半期の、不正または望まれないプログラムによる脅威に関する統計を発表した。これは McAfee の AVERT（Anti-virus and Vulnerability Emergency Response Team）が実施した調査報告で、望まれないプログラムの数は 2005 年第 1 四半期から第 2 四半期にかけて 12%伸びたという。
2005/07/12	ゾンビプログラムによるコンピュータの乗っ取りが急増 http://japan.cnet.com/news/sec/story/0,2000050480,20085262,00.htm ユーザーの知らない間に「ゾンビ」コードと呼ばれる悪質なプログラムのホストになってしまう PC が驚くべき勢いで増えていることが、新たに発表された調査レポートで明らかになった。
2005/7/16	「Sender ID や SPF を逆手にとったスパムが増加」、米 MX Logic の調査 http://nikkeibp.jp/wcs/leaf/CID/onair/jp/comp/386503 米 MX Logic は米国時間 7 月 11 日,スパム・メールに関する調査結果を発表した。それによると,攻撃者は,米 Microsoft のスパム対策仕様である「Sender ID」やスパム対策を目的とするメール認証技術「Sender Policy Framework(SPF)」を逆手にとってスパム・メールを送信しているという。
2005/7/.19	ISPs versus the zombies （ISP とゾンビの戦い） http://news.com.com/ISPs+versus+the+zombies/2100-7349_3-5793719.html Internet service providers face mounting pressure to keep their networks free of pests--not only for the benefit of their customers, but also for the good of the Internet in general.
2005/08/08	セキュリティ問題の国際化が投げかける難題 http://japan.cnet.com/special/story/0,2000050158,20086231,00.htm 「コンピュータにアドウェアを仕掛けさせても、1 台あたり数セントしか払わない会社がある。一部の人々にとって、4000 台のコンピュータにハッキングして、その報酬が 200 ドルというのは割の良い話ではない。だが、発展途上国では、200 ドルはかなりの金額だ」（FIRST の Reid）
2005/08/09	米でスパイウェアを使った大規模な個人情報盗難が発覚--FBI が調査へ http://japan.cnet.com/news/sec/story/0,2000050480,20086265,00.htm セキュリティ企業 Sunbelt Software は米国時間 8 日、50 もの銀行に関係した大規模な個人情報盗難が起きていることを発見したと述べた。
2005/8/8	「金儲けをたくらむプロ」のサイバー犯罪が増加、米 McAfee のガロット副社長 http://www.itmedia.co.jp/enterprise/articles/0508/08/news081.html 米 McAfee のセキュリティ研究機関 AVERT を統括するビンセント・ガロット氏によると、最近の脅威には「犯人のプロ化」「ターゲットの特化」という傾向が見られる。

2005/8/17	Watch out for worm wars （ワームウォーを注視する） http://news.com.com/Watch+out+for+worm+wars/2100-7349_3-5837147.html The recent surge in worms could be part of an underground battle to hijack PCs for use in Net crimes, some security experts say--but others aren't convinced.
2005/08/18	「ワーム戦争勃発」は本当か--専門家の間で分かれる見解 http://japan.cnet.com/news/sec/story/0,2000050480,20086457,00.htm Windows 2000 の脆弱性を突くワームが急激に広がっているが、一部のセキュリティ専門家は、これがネット犯罪に悪用する目的で PC を乗っ取ろうとするウイルス作者グループ間の抗争の一部である可能性を示唆している・・・だが、この考えに納得していない専門家もいる。
2005/8/30	Zotob worm linked to credit card fraud ring （Ztob ワームは、クレジットカード詐欺集団とつながりが） http://news.com.com/Zotob+worm+linked+to+credit+card+fraud+ring/2100-7348_3-5844672.html Turkish authorities have linked one of the suspects in the Zotob worm case to individuals thought to be part of a credit card fraud ring, according to the FBI.
2005/08/31	Zotob ワームの容疑者、クレジットカード詐欺団に関与 http://japan.cnet.com/news/sec/story/0,2000050480,20086815,00.htm FBI によると、Zotob ワーム関連の捜査を進めるトルコの警察当局は、同事件の容疑者の 1 人がクレジットカード詐欺団の一員とされる複数の人物と関係していることを突き止めたという。
2005/9/8	DoS 攻撃の罪を認めたハッカー、首謀者は逃亡中(上) http://hotwired.goo.ne.jp/news/culture/story/20050912204.html いかがわしいインターネット・ホスティング会社のためにデジタル攻撃を行なったオハイオ州のコンピューター・ハッカーが禁固刑に直面している。ある裕福なビジネスマンに指図され、ライバル企業に対して仕掛けられた一連の壊滅的なサービス拒否(DoS)攻撃のうちの 1 つを実行したと認めたためだ。
2005/9/22	Botnets on the rise in Asia, Symantec says （シマンテックがボットネットがアジアで急増と警告） http://news.com.com/Botnets+on+the+rise+in+Asia%2C+Symantec+says/2100-7349_3-5876671.html More computers in the Asia-Pacific region are being hijacked and used remotely by hackers to send viruses, according to a recent study by security vendor Symantec.
2005/9/27	1 日平均 1 万 352 台の「ゾンビ PC」を観測～シマンテックが最新レポートを発表 http://www.rbbtoday.com/news/20050927/25824.html シマンテックでは、ネット上に存在する脅威を分析した最新の「インターネットセキュリティ脅威レポート」（第 8 号）を発表した。それによるとボットに感染した PC の数は同社が観測したものだけで、1 日平均 1 万 352 台（前期比約 140%増）にのぼった。
2005/10/7	Dutch police nab suspected 'bot herders' （オランダ警察がボットハーダーを逮捕）

	http://news.com.com/Dutch+police+nab+suspected+bot+herders/2100-7348_3-5891266.html Dutch police have arrested three individuals suspected of hacking into more than 100,000 computers worldwide and using the hijacked systems in online crimes.
2005/10/13	迷惑メール：米国からの発信は減少、韓、中が増加 http://news.goo.ne.jp/news/infostand/it/20051013/1405584.html 英ソフォスは 12 日（現地時間）、迷惑メールの発信地の最新ブラックリスト（05 年度上半期分）を発表した。ワースト 1 位は米国で、同社が調べた迷惑メールのうち 26.35%（前年同期は 41.5%）が同国から送信されていた。ただ、2 位は韓国で 19.73%（同 11.63%）、3 位は中国（本土と香港）で 15.7%（同 8.9%）となり、米国の割合が減って韓、中に流れている。
2005/10/21	'Bot herders' may have controlled 1.5 million PCs （ボットハーダーは、150 万台の PC を制御している） http://news.com.com/Bot+herders+may+have+controlled+1.5+million+PCs/2100-7350_3-5906896.html Three suspected Dutch cybercriminals could face a stiffer penalty with new evidence that they hacked about 1.5 million PCs worldwide, more than 15 times the original estimate.
2005/10/25	家庭用 PC の 8 割がスパイウェアに感染--米調査 http://japan.cnet.com/news/sec/story/0,2000050480,20075362,00.htm 家庭用 PC のおよそ 8 割がスパイウェアに感染しており、それらのユーザーの大半が感染に気付いていないことが、米国時間 18 日に発表された調査結果から明らかになった。
2005/10/28	マイクロソフト、スパムメール送信者を提訴--「おとりゾンビ」PC で業者を特定 http://japan.cnet.com/news/sec/story/0,2000050480,20089840,00.htm ゾンビ PC を使ったスパムメールの増加に歯止めをかけたい Microsoft が、複数のスパムメール業者を訴えた。これらの業者には、不正に乗っ取った PC を使って膨大な数の迷惑メールを送信していた疑いが持たれている。
2005/10/28	「ゾンビ・パソコン」迷惑メールを 1 台で 1800 万通発信 http://hotwired.goo.ne.jp/news/technology/story/20051028303.html 米マイクロソフト社は 27 日(米国時間)、いわゆる「ゾンビ・パソコン」の撲滅キャンペーンを開始した。「ゾンビ」を約 3 週間監視したところ、たった 1 台に 500 万回以上の遠隔操作が実行され、1800 万通を超える迷惑メールが発信されたことを紹介。愛機をゾンビにしないよう注意を呼びかけている。
2005/11/3	Calif. man charged in 'bot net' attacks （ボットネットアタックを行った男を逮捕） http://news.com.com/Calif.+man+charged+in+bot+net+attacks/2100-7348_3-5931935.html A 20-year-old man accused of using thousands of hijacked computers, or "bot nets," to damage systems and send massive amounts of spam across the Internet was arrested Thursday in what authorities called the first such prosecution of its kind.
2005/11/3	パソコン 40 万台にアドウェアを無断インストールした男、米国で逮捕 http://hotwired.goo.ne.jp/news/20051107105.html 米連邦捜査局(FBI)は 3 日(米国時間)、ロサンゼルス在住のジーンソン・アンチェタ被告(20 歳)を逮捕した。約 40 万台のウィンドウズ機に侵入し、ユーザーの知らぬ間にポップアップ広告を表示するアドウェアをインストールさせ

	た容疑だ。この手口で不正に得た利益はおよそ 6 万ドルにのぼるとされる。当局によれば、この種の犯罪で起訴にいたったケースは、米国ではこれが初めてだという。
2006/3/3	日本でもスピア型ウイルス、「対日アンチダンピング情報」装うメール確認 http://internet.watch.impress.co.jp/cda/news/2006/03/03/11103.html 特定の企業などを攻撃する「スピア型」のウイルスが日本でも見つかった。通商問題を専門とする民間の調査研究機関である公正貿易センターは 3 日、同センターのメールを装ったウイルスが発生していることを明らかにした。

第4章 ボットネットの脅威の背景

ボットネットは、インターネットにおける大きな脅威となっている。なぜボットネットが脅威となるのか、またどのような脅威となるのかを解説する。

4.1 ボット作者はハッカーとは限らない

ボットネットのソースコードや開発環境は、インターネット上で広く流通しており、なかには、GUI 機能を持った設定プログラムが用意されているものも存在する(図 7)。このプログラムで設定が行える主な項目を表 5 に記載する。また、ボットと同様に多種多様な攻撃ツールのコードがインターネット上で公開されており、これらをボットに組み込んで新しい機能を追加することも、さほど難しいことではない。

従来、ウイルスやワームは高度な技術を持った一部の人間だけが開発できると考えられてきたが、このような環境の変化に伴い、ある程度プログラムが組める人間であれば、容易にボットを作成することが可能な状況にある。

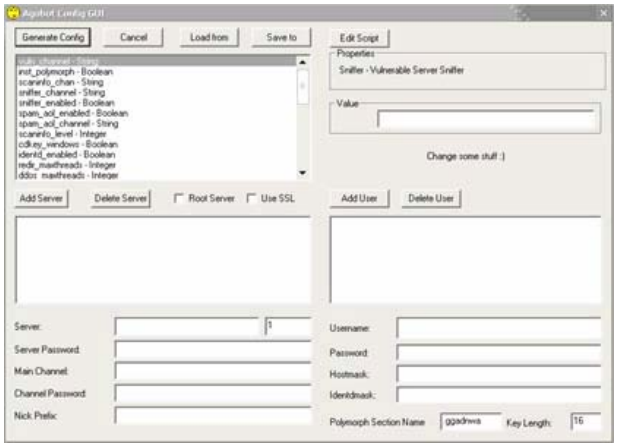

図 7 Agobot の設定ツール

表 5 Agobot の主な設定項目

項目名	説明
動作の指定	・盗聴プログラムを利用するかどうかを指定する ・感染活動の状況報告を行う通知レベル ・プロダクトキーの収集を行うかどうかを指定する ・ボットのサービス化を行うかどうかを指定する ・アンチウイルスプロセスの監視を行うかどうかを指定する ・オリジナルの実行ファイルを削除するかどうかを指定する ・ボットに対して送信されたログインコマンドの許可

IRC 関係	・脆弱なサーバとの通信を報告するためのチャンネル名, ・感染活動の状況を報告するためのチャンネル名 ・盗聴した情報を報告するためのチャンネル名 ・ニックネームにランダムな文字列を利用するかどうかを指定する ・ニックネームにコンピュータ名を利用するかどうかを指定する ・ルートサーバ、IRC サーバ ・IRC チャネルを SSL で暗号化 ・サーバに接続するためのパスワード ・チャネルを利用するためのパスワード ・ユーザ名およびパスワード
システムパラメータ	・Proxy 機能を提供するスレッドの最大数 ・DDoS 攻撃を行うスレッドの最大数 ・感染活動を行うスレッドの最大数 ・感染活動に利用するソケットの最大数 ・登録するサービス名を指定する
ポリモーフィックエンジン	・ポリモーフィックエンジンを利用するかどうかを指定する ・ポリモーフィックエンジンのセクション名 ・ポリモーフィックエンジンで利用するキー長

4.2 アンチウイルスでも検知できないものが少なくない

平成 16 年度の JPCERT/CC, Telecom ISAC-JAPAN が実施した調査では、収集した検体数の 90%をアンチウイルスソフトで検知することができたが、種類に着目すると、わずか 23%しか検出できなかった。

表 6 ハニーポットで取得した検体

	既知		未知		合計
	数	割合	数	割合	
検体数	35,741	90.3%	3,850	9.7%	39,591
種類	1,014	23.4%	3,324	76.6%	4,338

この調査結果は、容易に亜種を開発できる現状においては、パターンマッチングによるウイルス検知手法による防御は限界があることを物語っている。
パターンマッチング方式で、ボットの検出をすることが難しい理由は、次のようなものだと考えられる。

・IRC サーバやチャネルを変更することでハッシュ値やファイルサイズが変わってしまう

・ポリモーフィックエンジンや UPX などの難読化機能が組み込まれており、これを利用することで容易に実行ファイルを変えることができる
・ボット開発者は、最新のアンチウイルスソフトがボットを検知しないことを確認した上でリリースすることができる

現状では、開発側が圧倒的に有利な状況にあることから、パターンに依存しないウイルスの検知・防御手法の普及を急ぐ必要がある。

4.3 ボット自身の更新（UPDATE 機能）

ボットネットの大きな特徴として、ボット自身を更新する仕組みが実装されていることを挙げることができる。ボットネットに所属するボットは、HERDER からの指示により、一斉に自分自身を更新することが確認されている。
ボットが頻繁に更新される理由として、次のようなものがあると考えられる。

1) スパム送信などで利用される Proxy のポートを変更する（レンタル目的）
2) 感染用の C&C と、活動用の C&C を分離している
3) 利用する C&C を変更する
4) ボットネットを分割・統治する
5) 特定の目的に沿ったボットネットを構築する
6) 機能追加や不具合の修正を行う

ボットネットを使ったアンダーグラウンドビジネスの一つとして、ボットのレンタルを紹介した。ボットによるスパムの送信は、Proxy を利用することが分かっている。Proxy を使ったスパム送信を行うためには、Proxy のアドレスとポート番号のリストを入手する必要がある。
レンタル期間の切れた顧客がボットネットを利用することを防ぐためには、アドレスかポートを変更すればよいわけだが、現在のインターネット環境ではあまり IP アドレスが変わらない場合が多い。このため、唯一制御可能である Proxy ポートを頻繁に変更することで、レンタル期間が切れた顧客がボットネットを利用することを防いでいるものと考えられる。
平成 17 年度の調査では、ボットが感染に成功した場合、直後に自分自身の更新を行うことが確認されている。これは、上記の 2)に相当する動きと考えられる。

4.4 スパイウェア・ネットワークとしての機能

数万大規模のボットネットが多数確認されているが、現在の高速なインターネット接続環境においてボットネットを DDoS ツールとして利用する場合、小規模なボットネットで十分に商用サイトをダウンさせることができる。
たとえば、100Mbps のサイトに対して Flood 攻撃を行う場合、仮にボット側の平均通信速度が 1Mbps であったとしても、100 台で十分な計算になる。

一方で、ボットネットをスパイウェア・ネットワークとして考えた場合、大規模なボットネットを構築するメリットはきわめて大きいといえる。また、ボットネットは、単に情報を吸い上げるだけではなく、ここまでに紹介したような多様な操作が可能である上、ボット自体の更新を行うことが可能である。

この様な点を考えると、ボットネットを利用する上での主な目的は、DDoS などの攻撃ではなく、情報収集にあるものと考えられる（図 8）。

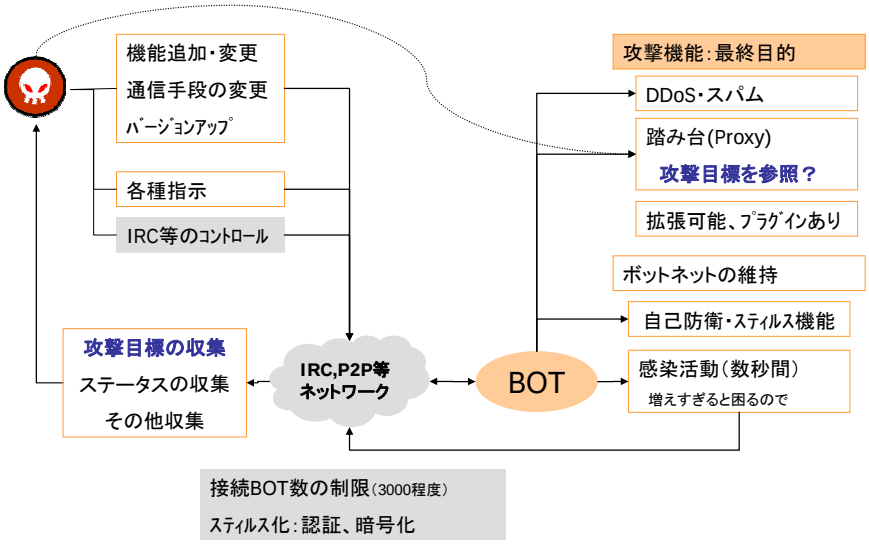

図 8 ボットネットの活動イメージ

第5章 おわりに

ボットネットは、攻撃者がはじめて手にした、現実的なコントロールが可能な分散型攻撃システムと言える。従来のワームやウイルスといった脅威は、無差別な目標に対する脅威であり、また、深刻な脅威にいたるまでが広がるまでに、一定の時間を必要とした。これに対し、ボットネットを使った攻撃は、特定の相手を選択的に攻撃することが可能であり、また、瞬時に攻撃を開始することが可能である。さらに、ソースコードがインターネット上で流通しており、日々改良が加えられており、今後どのような方向に進んでいくのかは予断を許さない。

このようなボットネットの脅威に対応していくためには、アンチウイルスベンダ、セキュリティベンダ、OSベンダ、ISP、CSIRT などが、単独で活動しても効果は期待できない。これらの関係するセクタが協調して、対応していく必要がある。また、攻撃の対象となった際には、国際的な協調が必要となることから、JPCERT/CC は現在連携をしている世界各国、経済地域の CSIRT とのさらなる連携強化および国内 CSIRT 構築やコンタクトポイントを確立し、国際間のインシデントハンドリングを強化していかなければならない。

また、インターネット利用者にとって、現在抱えている脅威がどのようなものであり、どのような対策が必要であるのかを、効果的に伝えていくことが必要である。