平成19年度

サイバークリーンセンター(CCC)活動報告

ボット対策プロジェクト

サイバークリーンセンター

https://www.ccc.go.jp/

目次

1 はじめに

昨今、インターネット利用において Malware と呼ばれる様々な悪意のあるソフトウエアによる被害が増加している。

Malware とは、「悪の」という意味の接頭辞「mal-」と「ソフトウエア」を組み合わせた造語で、利用者の PC 等に侵入・攻撃などの被害を起こすように設計されたソフトウエアの総称である。Malware には、狭義のウイルス・トロイの木馬・ワーム・ボット[1]などがあり、その中でも特にボットは、個人ユーザの PC に侵入して遠隔操作することにより、ターゲットに対してスパムメールやフィッシング・DDoS 攻撃・情報を盗み出すといった行動をさせることができる。ボットに感染し遠隔操作されているネットワークはボットネットと呼ばれ、サイバー犯罪の温床になっている。

このような状況で、セキュリティ対策の重要性が日々高まっている。しかし、現状では、対策が個々のユーザに委ねられているため、初心者など、十分なセキュリティ知識を持たない多くのユーザがボットに感染し、被害が広がっている。また、民間のセキュリティベンダは、独自に Malware の検体を収集し、個別にパターンファイルや駆除ソフトの提供を行っているが、最新のパターンファイルでは検知できない Malware の増加やその亜種の大量発生、および、局地的感染が広がっており、セキュリティベンダが単独で全ての Malware に対応することは、難しい状況となってきている。これらの状況を改善するため、2006 年 12 月、総務省および経済産業省は共同で実施する「ボット対策プロジェクト」をスタートした。本プロジェクトでは、ISP 事業者およびセキュリティベンダと緊密に連携し、ボット感染ユーザに注意喚起を行うことにより、ボットの脅威を減らしていくことを目的とした活動を行っている。また、プロジェクトのポータルサイトとして「サイバークリーンセンター（CCC）」（https://www.ccc.go.jp/）を運営している。

本書は、平成 19 年度活動報告として、CCC を運営する 3 つのグループ、ボット対策システム運用グループ・ボットプログラム解析グループ・ボット感染予防推進グループの活動をまとめたものである。

1.1 ボットとは

ボットは、PC を悪用することを目的に作られた悪性プログラムで、ネットワークなどを通じて感染活動を行い、ハーダーと呼ばれる悪意のある指令者によりコントロールされる様子がロボット（Robot）に似ていることから、ボット（Bot）と呼ばれて

[1] ボットプログラム、ボットウイルスと呼称することもある

いる。

ボットに感染すると、インターネットを通じてハーダーが PC を遠隔操作し、「迷惑メールの大量配信」「特定サイトの攻撃」などの迷惑行為をはじめ、情報を盗み出す「スパイ活動」といった行動をさせることができる。

ボットには、キーボード操作履歴やコンピュータに保存されている情報を外部へ送信する機能を有するものもある。このため、クレジットカード番号や ID・パスワードなどを盗み出されたり、メールソフトのアドレス帳に登録してあるアドレスを収集されるなど、PC 内の情報が外部に漏洩した被害が報告されている。また、システムファイルなどの書き換えや、スパムメールの送信などに利用されることによる CPU の過負荷のために、PC のパフォーマンスが低下することがある。そして、最悪の場合 OS の再インストールが必要になることもある。

1.2 ボットネットの現状

ボットネットは、数十～数百万台のボット感染 PC から構成され、C&C（Command & Control）サーバを介してハーダーと呼ばれる指令者によりコントロールされる巨大ネットワークを形成している。感染した PC は、ハーダーからの命令によって操られ、例えば、フィッシング目的などのスパムメールの大量送信や、特定サイトへ DDoS 攻撃などに利用されることから、大きな脅威となっている。感染 PC を使用しているユーザは、知らぬ間に犯罪の踏み台にされ、「被害者」であると同時に「加害者」にもなっている。

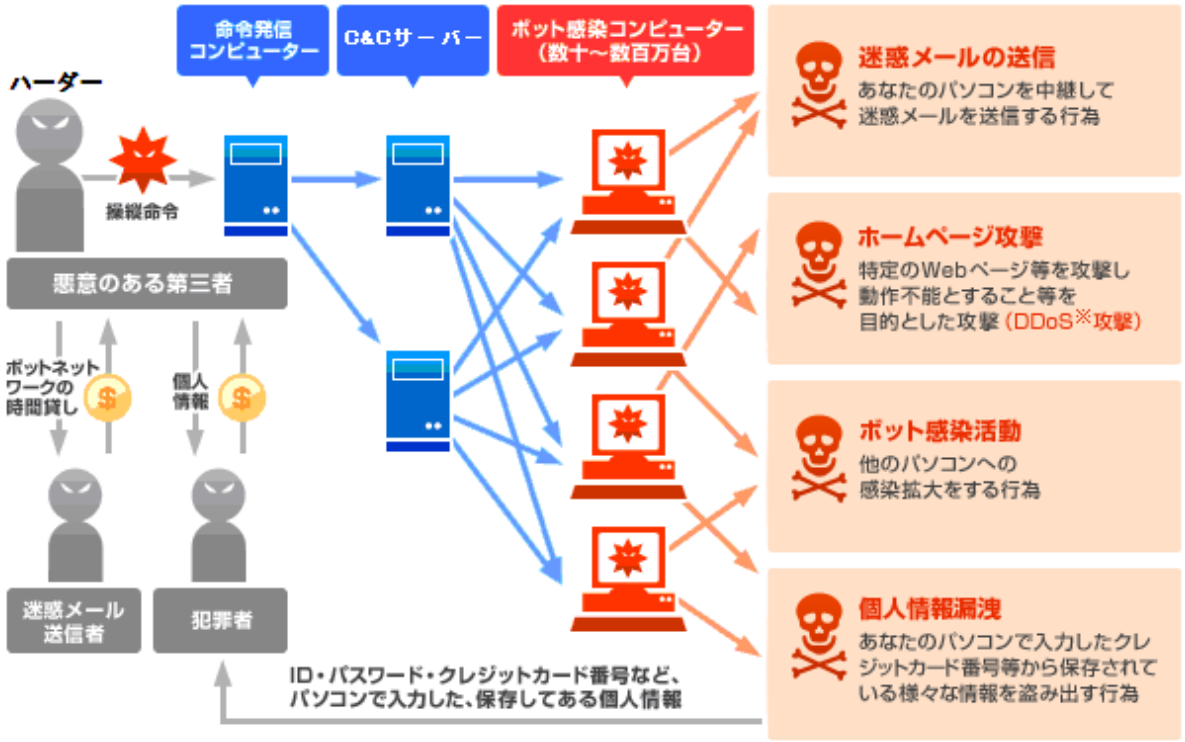


図 1-1 ボットネットの脅威

2005 年の Telecom-ISAC Japan および JPCERT コーディネーションセンターなどの調査では、国内において 40 万から 50 万台の PC がボットに感染し、ボットネットを構成していると推定しており、現在インターネットで飛び交う悪質なプログラムの約 8 割がボットと見られている。また、セキュリティ対策をしていない PC をインターネットに接続すると約 4 分でボットに感染することが分かっている。

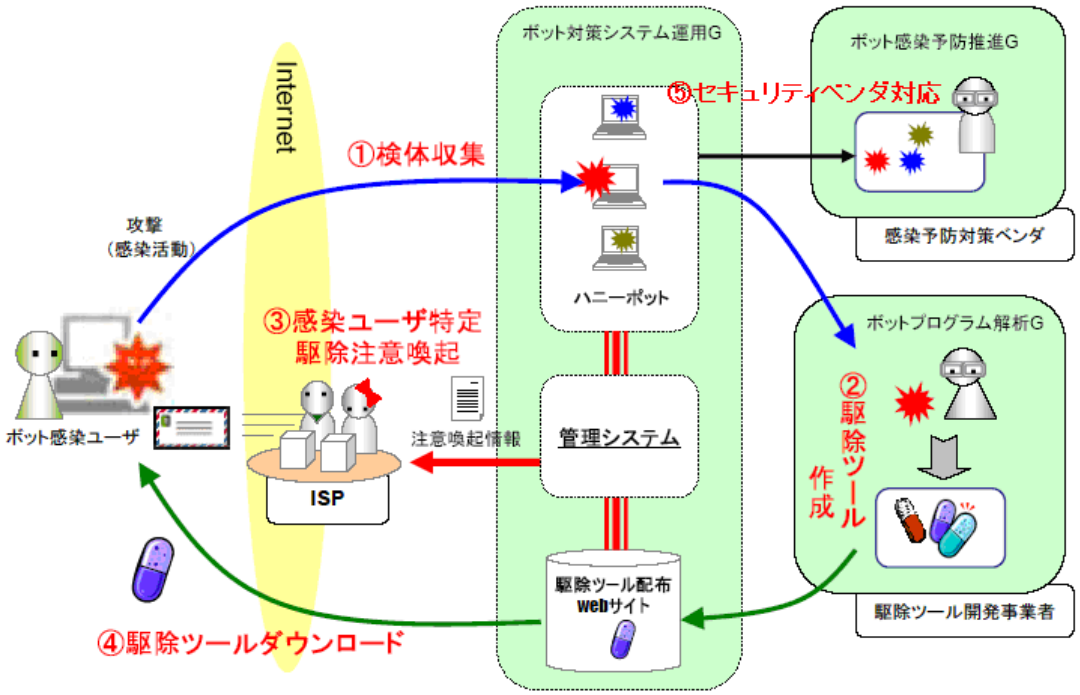
こうしたボットネットによる被害は世界中で発生している。2007 年 5 月には、エストニア共和国の政府や銀行などのサイトが大規模な DDoS 攻撃を受け、その際、ボットネットが使われたといわれている。こうしたボットネットが原因とされる DDoS 攻撃は、2003 年にマイクロソフトのサイトが攻撃を受けて以来、数多く報告されている。

ニュージーランドでは、2007 年 11 月に 100 万台以上のボットネットを構築した男性が逮捕されている。また、カナダのケベック州でも、約 100 万台のボットネットを運用・不正アクセスし、4,500 万ドルの損害を与えたとして逮捕されている。

また、ボットの感染手法も変化してきており、2008 年 3 月には、国内有名サイトがボットなどを配布するよう改ざんされるという事件が発生している。ボットの新種・亜種は日々発見されており、これは、ボットが自己メンテナンス機能により頻繁にバージョンアップを行っていること、かつソースコードが流通しているため、形態・機能を簡単に追加できることに起因していると考えられる。

1.3 サイバークリーンセンター（CCC）の概要

CCC では、上記のようなボットの感染被害を限りなくゼロにするため、プロジェクト参加 ISP やセキュリティベンダ等の協力のもと、図 1-2 に示すような活動を通じてボット感染ユーザに注意喚起を行っている。



①検体収集	ボットに感染している PC からの攻撃事象（感染活動）を“おとり PC（HoneyPot：ハニーポット）”で検知し、ボット検体を収集する。
②駆除ツール作成	ボット検体を解析して“駆除ツール”を作成する。
③感染ユーザ特定・駆除注意喚起	ISP と連携して攻撃の発信元を特定し、駆除注意喚起メールを送信する。
④駆除ツールダウンロード	メールを読んだ感染ユーザが、駆除注意喚起メールに従って、CCC の対策ページから駆除ツールをダウンロードして適用し、ボットを駆除する。
⑤セキュリティベンダ対応	セキュリティベンダに対して、収集したボット検体を提供する。各ベンダは、その検体を対策ソフトのパターンファイルに反映する。

図 1-2 CCC 活動概要

CCC は、サイバークリーンセンター運営委員会（CCC-SC）のもと、業務内容に応

じた 3 つのグループで構成され、活動している。

図 1-3 CCC 運営体制図

【ボット対策システム運用グループ】（Telecom-ISAC Japan）

ハニーポットをはじめとする本プロジェクト基幹システムの運用、プロジェクト参加 ISP を介したボット感染ユーザへの駆除注意喚起を行っている。また、ボットなどの最新動向の調査も行う。

<プロジェクト参加 ISP> 平成 20 年 3 月末現在

IIJ、BIGLOBE、OCN、au one net、@nifty、hi-ho、ODN、Yahoo!BB、インターネット MAGMA、IC-NET、ガオネット、tigers-net.com、BaycomNet、bai サービス、ASAHI ネット、@NetHome、サイラスネット、ブロードスター、isao.net、ZOOT、ipc 東海インターネットサービス、VECTANT、PIKARA、NETWAVE、WAKWAK、SANNET、mopera／mopera U、InfoSphere、TikiTiki インターネット、メガ・エッグ、アーバンインターネット、LCV-Net、LCNet、ZAQ、KATCH ケーブルインターネットサービス、KCN-Net、SYNAPSE、KCN インターネットサービス、群馬インターネット、ROSENET、MediaCat、ケイオプティコム eo、KIP-Internet、CATVY インターネット、ケーブルワンケーブルインターネット、TOKAI ネットワーククラブ、JWAY ケーブルインターネ

ット、エスシーエヌネットワークサービス、DAC システム、仙台 CAT-V NET、高岡ケーブルネットワーク、Commuf@、e-mansion、TAM インターネットサービス，Net3 インターネット、aikis、avis、TCN ケーブル NET、コーラルネット、TSTnet、DTI、NCM ケーブルインターネットサービス、N-plus、能越ネット、ParkNet、@はんのう、Aitainet、ファミリーネット・ジャパンサイバーホーム、VRTC ネット、Web しずおか、Infovalley、FUSION GOL、Plala、愛・ネット、ミライネット、Mediatti NET、C-able インターネット

【ボットプログラム解析グループ】（JPCERT コーディネーションセンター）

収集されたボット検体の特徴や技術の解析を行い、駆除ツールを作成する。また、効率的な解析手法の検討なども行うほか、駆除ツール開発事業者と連携してその対策技術の開発も行う。

＜駆除ツール開発事業者＞

トレンドマイクロ株式会社

【ボット感染予防推進グループ】（情報処理推進機構）

CCC で収集されたボット検体を最終的に管理し、検体を感染予防対策ベンダに適切に提供して各社のウイルス対策ソフトのパターンファイルへ反映させることにより、ボットへの感染予防を推進する。

<感染予防対策ベンダ>

株式会社アンラボ、株式会社 Kaspersky Labs Japan、株式会社シマンテック、ソースネクスト株式会社、トレンドマイクロ株式会社、マイクロソフト株式会社、マカフィー株式会社

2 ボット対策システム運用グループ活動報告

2.1 概要

ボット対策システム運用グループでは、ボットに感染している PC をなくすことを目的とし、検体収集解析と注意喚起を実施している。

検体収集解析フェーズでは、ボット感染ユーザからの攻撃事象（感染活動）を検知してボット検体を収集する。収集した検体をボットプログラム解析グループへ検体を引き渡し、駆除ツールの作成を依頼する。

注意喚起フェーズでは、作成された駆除ツールを受け取り、ISP と連携して感染ユーザの特定を行い、感染ユーザへの注意喚起メールを送信する。メールを受け取ったユーザは対策サイトを通じて駆除ツールをダウンロードする。また、一般ユーザに向けても CCC 公式サイトを通じて配布を行っている。

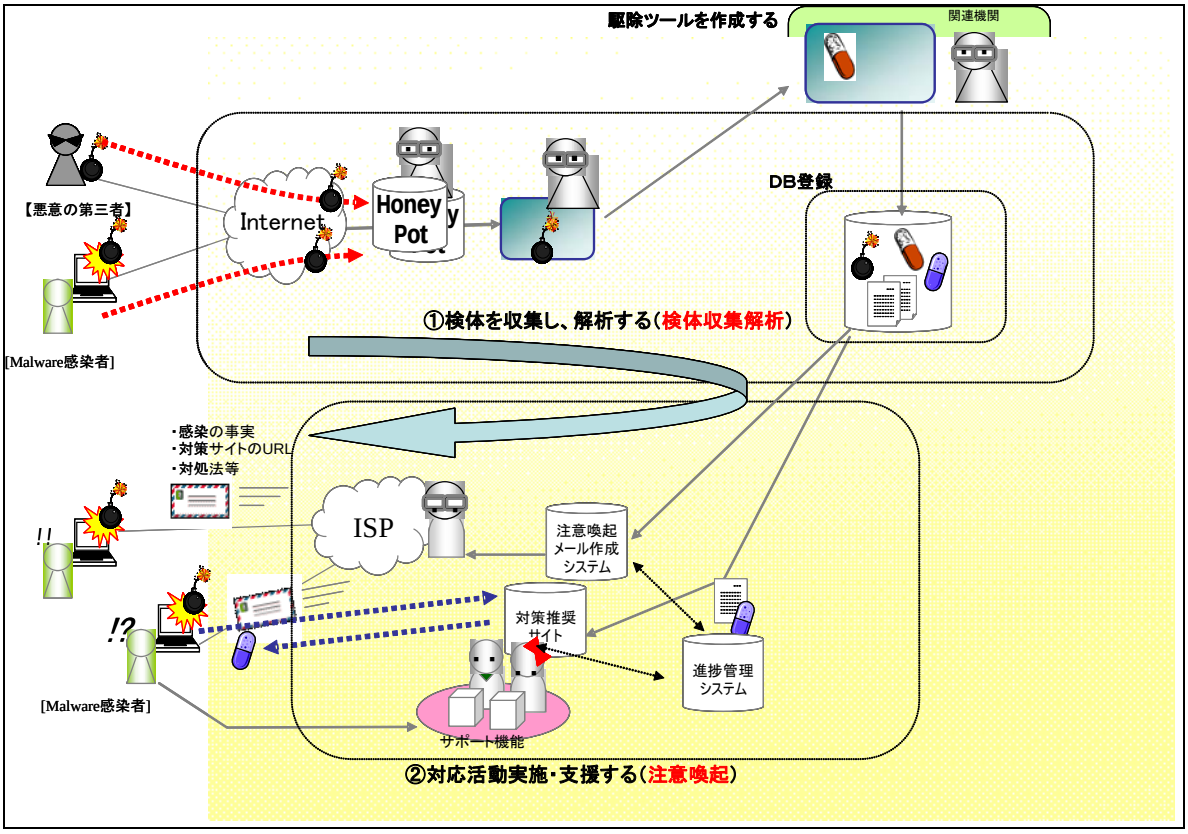


図 2-1 システム運用グループ全体像

2.1.1 検体収集 解析

ボット感染ユーザに注意喚起を行うためのトリガー（きっかけ）として、感染ユーザからの攻撃事象（感染活動）を検知しボット検体の収集を行っている。ボットの感

染手法には様々なタイプがあるが、PC の OS の脆弱性を狙って感染するものが多い。このことから、脆弱性を残したおとり端末（ハニーポット）を設置することによってボットの感染活動を観察し、ISP により感染 PC を特定することができる（ユーザ特定）。ハニーポットで多数のボット検体を収集することにより、駆除ツール作成が可能となる。収集した時点での検体には、同一の検体や既にウイルス対策ソフトに対応済みの検体が含まれている。重複した検体を整理する作業のことを「同定解析」と呼び、解析済みの検体を「同定検体」と呼ぶ。この同定検体をウイルス対策ソフト（トレンドマイクロのスキャン時における最新パターンを使用）にてスキャンし、ウイルス対策ソフトに対応済みの検体を除く作業（既知未知解析）を行う。このうち、未対応であった検体（未知検体）に対して駆除ツール作成を依頼する。

2.1.2 注意喚起

ボット対策システム運用グループでは、ハニーポットで収集したボット検体の通信を解析して感染ユーザの ISP を特定し、感染ユーザ情報を ISP へ伝達している。その後、ISP が感染ユーザに対して、ボット感染の事実と駆除を促すメールを送信するという手法で注意喚起を行っている。下記にそのプロセスを示す。

① 検体収集・解析システムで収集する攻撃事象（感染活動）情報から、感染ユーザが利用している ISP を特定する。
② 特定された ISP がプロジェクト参加 ISP の場合は、その ISP に対し、ユーザの特定および注意喚起を依頼する。（平成 18 年度は 8ISP と協力して感染ユーザの特定を実施してきたが、平成 19 年度はさらに拡大して 68ISP とし、国内における ISP のカバー率を向上させた。）
③ 各 ISP では、感染ユーザの特定を行い、電子メールなどを利用して当該感染ユーザへ注意喚起を行う。

2.2 活動状況・成果

本プロジェクトでは、毎月の注意喚起活動実績を、図 2-2 のような形で CCC 公式サイト（https://www.ccc.go.jp/）にて公開している。

その内容は、検体収集・解析実績（図中①～⑦）と一般公開サイト駆除ダウンロード総数の情報である。

2008 年 3 月時点で、累計 7,673,279 体の検体を収集し、同定された検体は 215,338 種類であった。そのうち、収集時点で市販のウイルス対策ソフトで検知できないものが、10,082 体あった。注意喚起については、232,487 通のメールを 54,703 人に対して実施し、約 29%の感染ユーザが駆除ツールをダウンロードし、対策を実施していただいた。

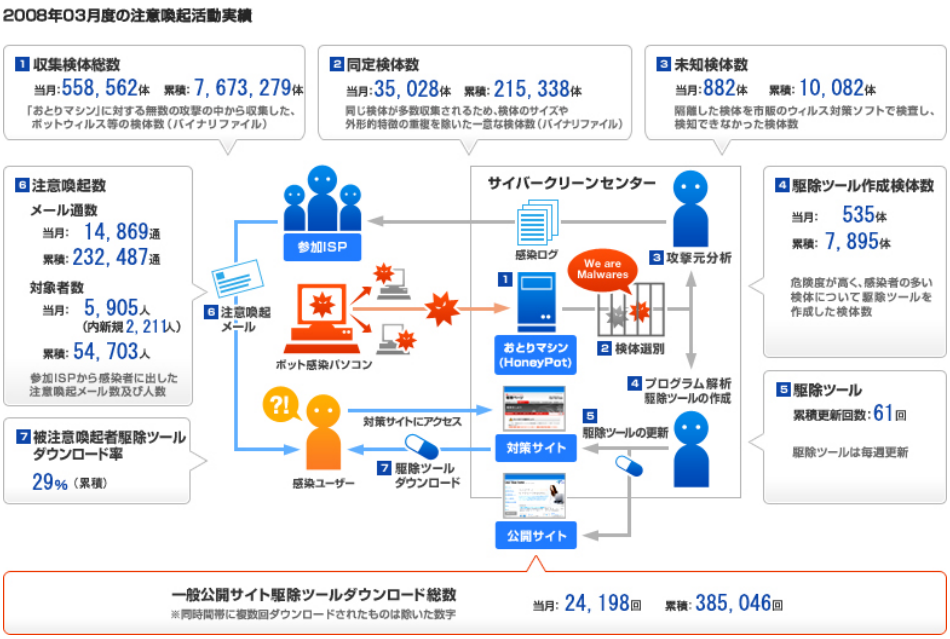


図 2-2 活動実績　2008 年 3 月度実績および 2007 年 2 月からの累積

2.2.1 検体収集・解析

ボット感染ユーザに対する注意喚起を行うためには、ボットの感染活動・攻撃活動を捕捉し、駆除ツール作成のために、ボット検体を収集・解析することが必要である。

ここでは、2007 年 4 月～2008 年 3 月までの検体収集解析の状況を示す。

(1) 検体収集数の推移

検体収集・解析システムは、ネットワーク回線を利用して、ボットをハニーポットと呼ばれるシステムに誘導し、ボット検体として収集を行っている。

一月あたりの検体収集数は、約 54 万体（一日あたりでは約 1.8 万体）である。この時点で収集した検体の中には、重複した検体や既知の検体も含まれている。

収集した検体の月毎の推移を、図 2-3 に示す。

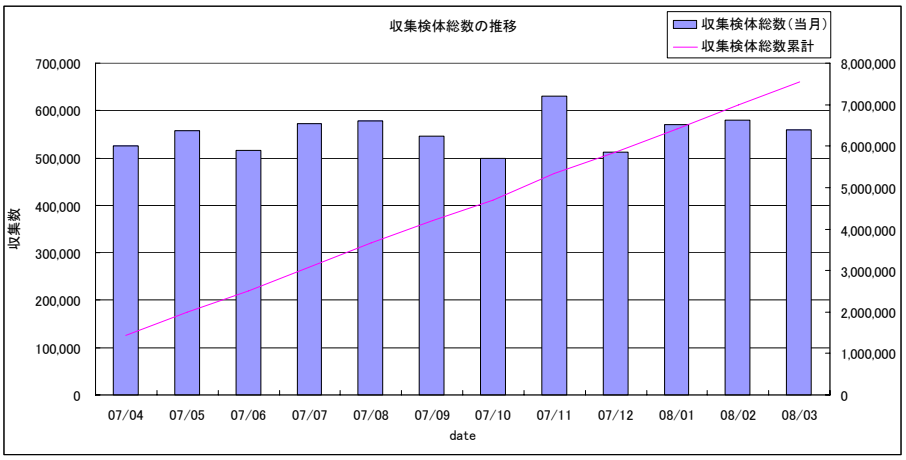


図 2-3 収集検体総数の推移

(2) 同定検体数の推移

収集した検体を同定解析した同定検体数の、一月あたりの平均値は約 1.5 万体で、一日あたりに換算すると約 500 体を収集している。

同定検体数の月毎の推移を、図 2-4 に示す。2007 年 10 月、11 月で減少が見られるが、これは海外のある特定サイトからの数種類のボット配布が一時期に減少したためである。2008 年 2 月には、ハニーポット内部の実行ファイルに寄生感染するファイル感染型ウイルスが増殖したため種類数が増加していた。特に多量に増殖を繰り返している検体は爆裂型のボットで、攻撃数が多いものであった。2 月以降、このタイプのウイルスが更に増加の傾向にある。

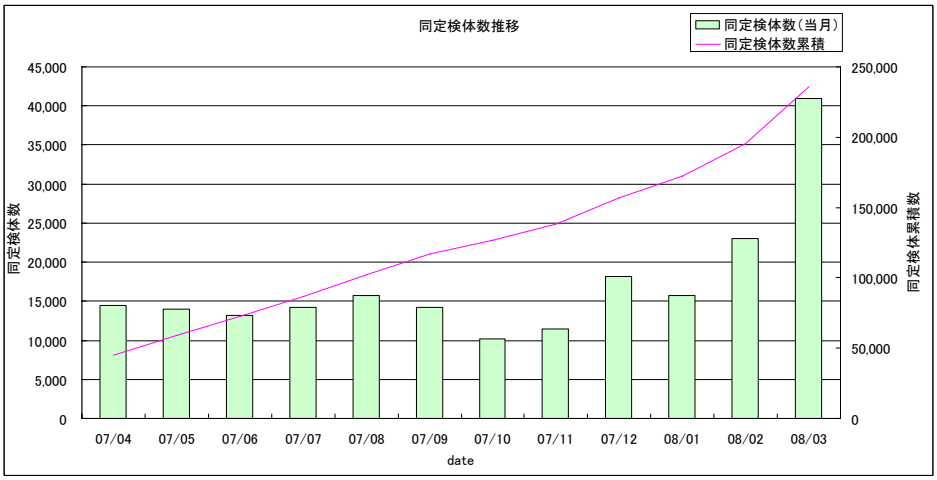


図 2-4 同定検体数の推移

(3) 同定検体数の既知未知の推移

同定検体を既知未知（市販ウイルス対策ソフトに対応済みか否か）解析した結果の統計から、既知未知判定結果は、一月あたり平均して約 1.5 万体の同定検体のうち、1.4 万体が既知、0.1 万体（約 7%）が未知であった。一日に換算すると

未知検体を約 30 体収集していることになる。

同定検体数の既知未知の月毎の推移を、図 2-5 に示す。未知同定検体数は、月毎にばらつきはあるが、割合は減少していることが分かる。また、未知同定検体数累積(折れ線グラフ)の傾きを見ると、徐々に緩やかになっていることから、未知検体の増加数も 2007 年当初よりは減少傾向にあることが分かる。

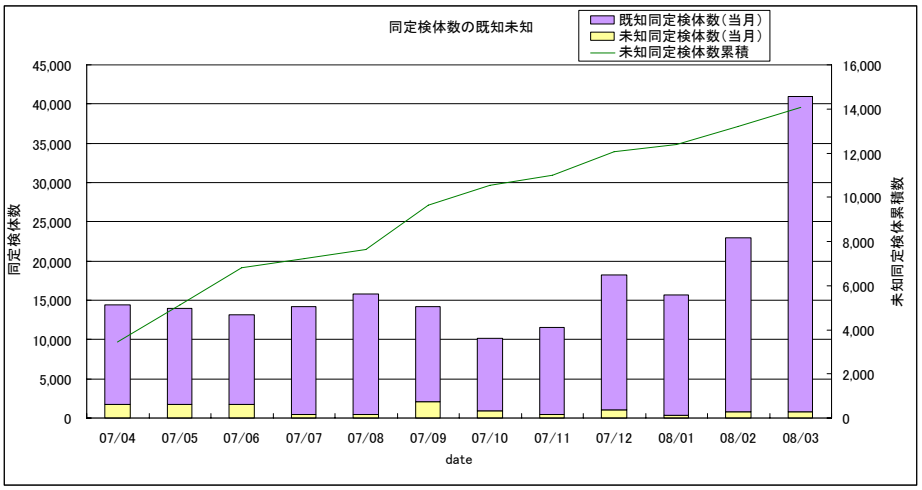


図 2-5 既知未知同定検体数の推移

全体の収集数で、11 月が多いにもかかわらず同定検体数が少ないのは、10 月 11 月に攻撃数の多いボットが流行したためである。流行した年間の経緯を、図 2-6 に示す。

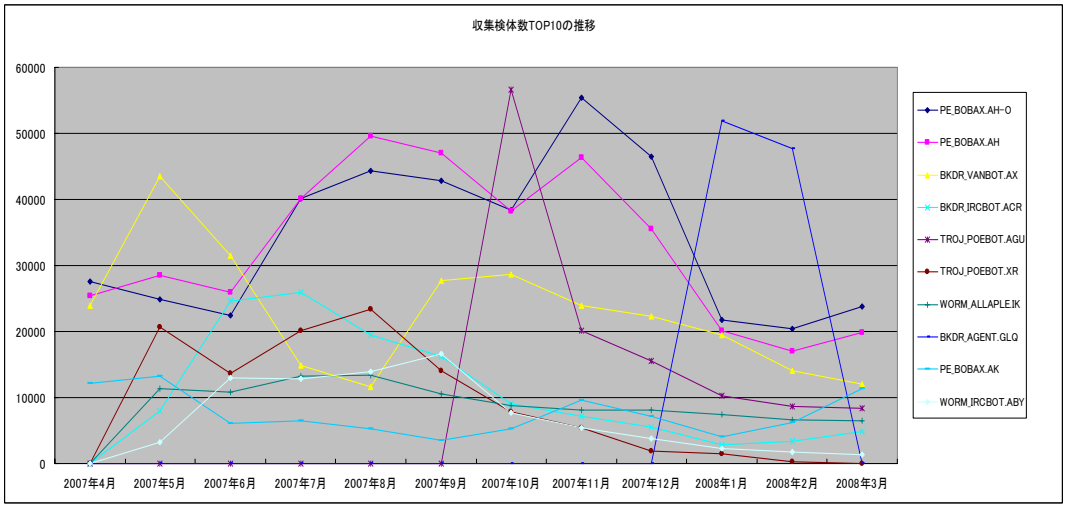


図 2-6 収集した検体中、攻撃数上位 10 体の推移

(4) ボットの配布元

ボットは、国内からのみならず海外からも配布されている。

収集した検体の配布元(攻撃元)を、国内・海外・感染したハニーポット間(内

部感染）で分類した月毎の推移を、図 2-7 に示す。国内からの攻撃数は若干減少傾向にあるが、海外からの攻撃が増加しているため、総攻撃数（検体収集数）が多少増加している。

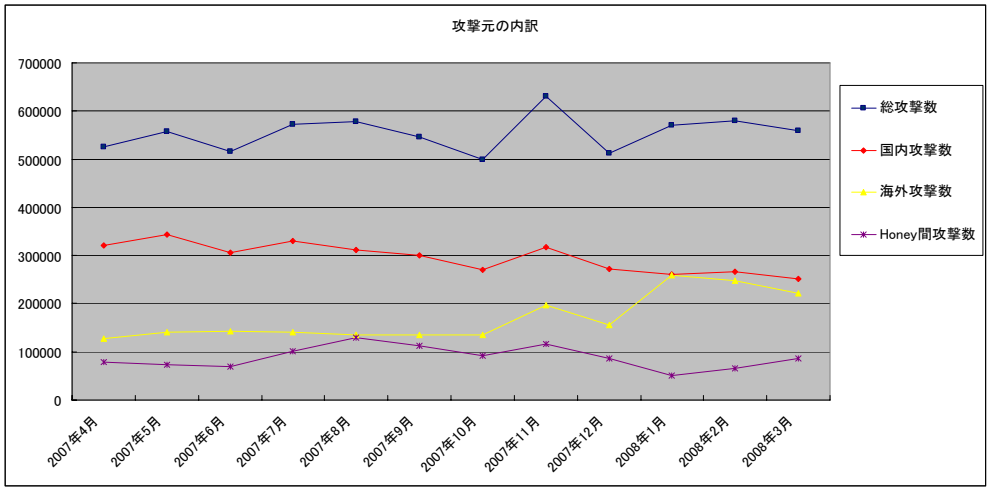


図 2-7 攻撃元の内訳

総攻撃数の内訳を、国内・海外・感染したハニーポット間（内部感染）の比率で表したものが、図 2-8 である。この図を見ても海外からの攻撃の割合が増加し、国内からの攻撃が減少していることが分かる。

海外からの攻撃が増加している原因は、特定の海外サイトからの攻撃活動が活発になってきたためと考えられる。

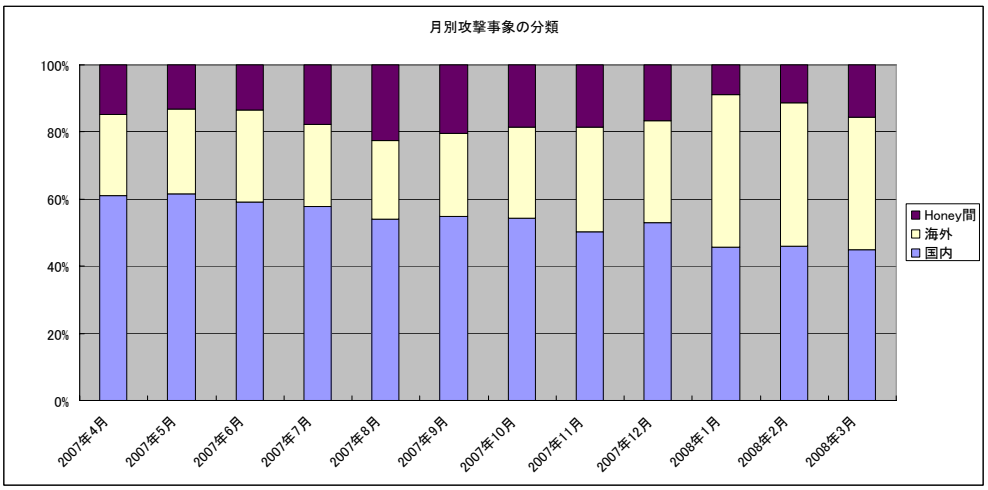


図 2-8 攻撃元の比率

2.2.2 注意喚起

(1) ユーザ対策実施状況

ボット感染 PC をなくすためには、ボット感染ユーザを特定し、注意喚起することが重要である。ボット対策システム運用グループでは、プロジェクト参加 ISP との連携により、感染ユーザに対してメールによる注意喚起を行ってきた。

平成 19 年度に送信した注意喚起メールは 232,487 通、注意喚起したユーザ数は 54,703 人であった（図 2-2 参照）。

平成 19 年度の注意喚起メールによる対策サイトへの訪問率は約 39%であり、駆除ツールダウンロード率が約 30%、WindowsUpdate 率が約 27%となっている。また、すべての対策を実施して完了報告をした率は約 15%であった（図 2-9 参照）。

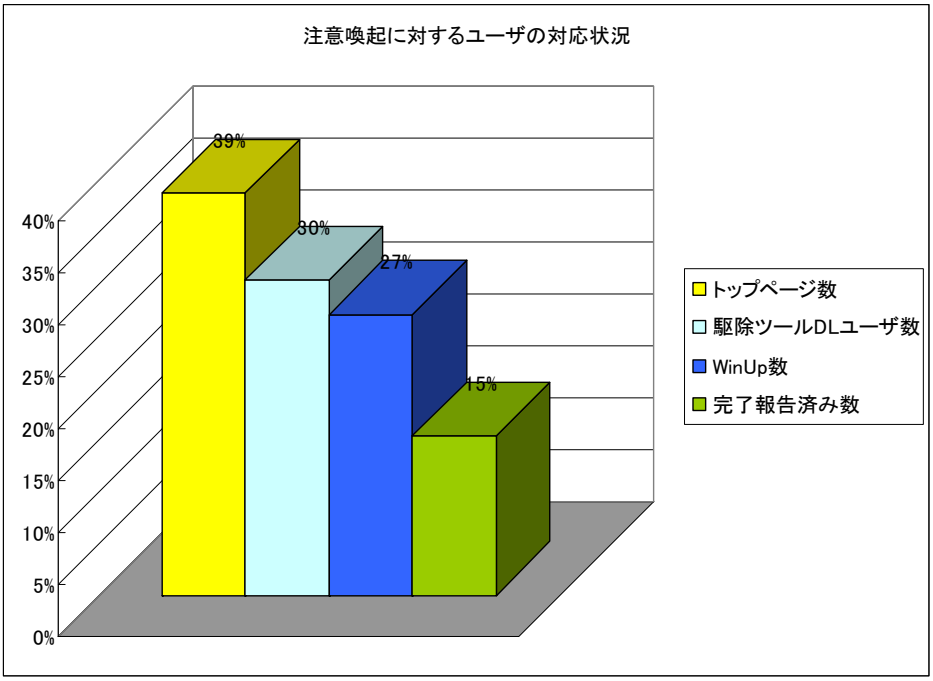


図 2-9 注意喚起に対するユーザの対応状況（2007 年 4 月～2008 年 3 月）

(2) ユーザサポート状況

注意喚起ユーザに対するユーザサポートは各プロジェクト参加 ISP が担当しているが、プロジェクト参加 ISP からエスカレーションされた一部のユーザについては、ボット対策システム運用グループでサポートを実施した。これらのユーザサポートを通じていくつかの問題点が浮き彫りになった。

① WindowsUpdate ができないケース

・hosts 改ざんによる WindowsUpdate サイトへの接続が妨害される
・ファイル感染型（特に VIRUT）の拡大に伴い、WindowsUpdate の途中でシステムファイルへの感染がおこる
・WindowsXP SP2 で LANdriver の最適化が行われると PC および回線のリソースを消費してしまい、Web 接続がタイムアウトとなる

② ブロードバンドルータが導入されていないケース

・ボット対策システム運用グループで直接サポートしたユーザの約 9 割が、ブロードバンドルータを導入していなかったために、OS の脆弱性を狙った攻撃により感染していた

③ ウイルス対策ソフトに対する誤解があるケース

・PC にプリインストールされているウイルス対策ソフトを、購入時のままパターンファイルを更新せずに使い続けているユーザが多い
・パーソナルファイアウォール機能をウイルス対策ソフトと勘違いしている（パーソナルファイアウォールとウイルス対策ソフトを併用して使用している場合で、不正なアクセスなどがあった時、ウイルス対策ソフトのパターンが更新されていなくても、パーソナルファイアウォールが警告を出すため、ウイルス対策ソフトが機能していると誤解しているユーザがいる（実際にはウイルス対策ソフトのパターンが古く、ボットを駆除できないにもかかわらず、警告メッセージがでるためセキュリティ対策が動作しているように見えてしまう））
・ISP が提供するメールウイルス検知サービスで十分だと思っているユーザがいる（メールウイルス検知サービスでは、脆弱性を狙って感染するボットや Web にアクセスしただけで感染するボットには対応できない）

CCC では WindowsUpdate をボットに対する基本的な対策として案内しているが、実際には WindowsUpdate を実施していないためにボットに感染しているユーザが多い。これらのユーザに WindowsUpdate を依頼したところ、ボット感染が原因で WindowsUpdate が実施できないケースがいくつも見られた。

ブロードバンドルータの導入は、脆弱性を狙って感染するボットに対しては非常に有効な対策である。しかし、セキュリティ意識が比較的高いユーザにおいても、ブロードバンドルータの有効性について十分に認識されていないことがわかった。

ウイルス対策ソフトについては様々な誤解があり、せっかくウイルス対策ソフ

トを導入しても、動作が重くなったなどの理由でアンインストールしてしまうケースも見受けられた。

(3) ボット対策効果向上に向けた取り組み

ボット対策システム運用グループでは、ボット対策効果の向上に向け、いくつかの改善を行ってきた。そのひとつは、感染ユーザがアクセスする対策サイトの改善である。対策サイトでは、駆除ツールの配布をはじめボット対策の様々な情報を提供しているが、当初対策実施までのページ数が多かったことから、最終的な対策を実施する前に対策を中止してしまうユーザが多かった。そこでページ構成を見直し、対策を 1 ページで表現するように改善した。

また、当初、駆除ツールの実施後、WindowsUpdate を実施するよう案内していたが、せっかく駆除ツールでボットを駆除しても、WindowsOS に脆弱性があり、WindowsUpdate の途中でボットに再感染してしまうケースが多く見られたことから、WindowsUpdate 後に、駆除ツールを実施するよう手順を見直した。

その他、ブロードバンドルータの導入を手順化するなど、逐次対策サイトの改善を行った。

もうひとつの大きな取り組みとしては、一部のプロジェクト参加 ISP で、注意喚起手法として、メールに加えて郵送による注意喚起を実施したことである。これまでのメールによる注意喚起では、メールを読まず対策を実施しないユーザがいたことから、一部郵送による注意喚起を実施したところ、対策サイトへのアクセス率が、メールによる注意喚起の場合の約 30%から約 50%に向上した。

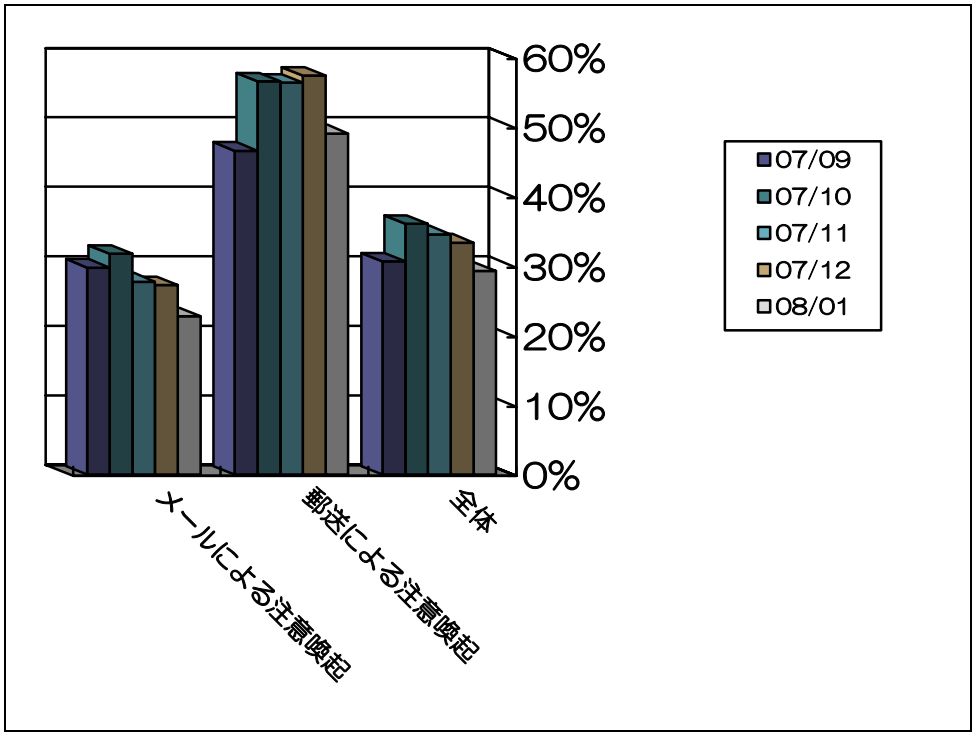


図 2-10 ある ISP における郵送による注意喚起の効果

(4) 新たな取り組み

平成 19 年度は、ボット対策プロジェクトを日本国内に広く浸透させるため、新たな取り組みを行った。

まず 1 点目は、プロジェクト参加 ISP 数の拡大である。平成 19 年度当初は 8ISP の協力の下、注意喚起活動を実施してきたが、注意喚起対象者の拡大や ISP との連携の強化、およびユーザに向けた啓発活動を推進するため、国内 ISP に広く呼びかけ、平成 19 年度末現在でプロジェクト参加 ISP は 68ISP に拡がった。なお、ISP のボット対策プロジェクトへの参加形態は、①各 ISP におけるボット感染ユーザ数などにより、CCC 側のシステムに直接接続して感染ユーザを特定・注意喚起する方式、②特別なシステムを用意することなく CCC からの依頼に基づき注意喚起を行う方式の 2 方式とした。

2 点目は、ボット駆除活動宣言サイト（http://botkujo.jp/）の開設である。

ボット駆除活動宣言サイトは、一般ユーザ向けにボットの脅威をわかりやすく伝え、またプロジェクト参加 ISP の運用担当者のコメントなどを紹介することにより、ボット対策活動の普及啓発を進めることを目的としている。各プロジェクト参加 ISP には、ボット駆除活動宣言サイトへのリンクを張ってもらい、実際のボット対策については、ボット駆除活動宣言サイトから CCC 公式サイトへ誘導するようにしている。

図 2-11 ボット駆除活動宣言サイト（http://botkujo.jp/）

その他、ボットの脅威と対策をユーザにわかりやすく伝えるリーフレットの作成や、CCC の月次活動実績の公開（https://www.ccc.go.jp/）などを通して、ボット対策の普及啓発に努めてきた。

図 2-12 リーフレット

2.3 今後の展開

本プロジェクトの活動により、一部のプロジェクト参加 ISP では、感染ユーザ数が減少し始めるなど、本プロジェクトの地道な取り組みが効果を上げつつある。またこうした取り組みがメディアなどに取り上げられ、CCC 公式サイトのアクセス数が増加するなど、認知度も高まってきた。

平成 20 年度は、平成 19 年度に引き続き、ボット感染ユーザに対する注意喚起活動を継続することにより、感染 PC 数の更なる減少を目指す。そこで、プロジェクト参加 ISP との協力関係を密にし、出来るだけ多くのユーザに対策実施を促すとともに、注意喚起方法の工夫や対策サイトの改善などを積極的に進めていく。また、注意喚起活動と平行して、様々なチャネルを利用したボット感染を防ぐための啓発活動もあわせて行っていく予定である。

3 ボットプログラム解析グループ活動報告

3.1 概要

ボットプログラム解析グループは、ハニーポットで収集したボット検体の解析を行い、駆除ツールを作成する。なお、解析を行ったボットのうち、必要に応じて静的解析技術による詳細な解析を実施している。

3.2 解析

解析にあたっては、以下を実施している。

3.2.1 駆除ツールの作成

市販のウイルス対策ソフトで未対応の検体について、種類・感染に関するファイル情報などを調査し、駆除ツールを作成している。

(1) 対応リストの作成

影響度の大きい検体については早急な対応が必要なため、優先度をつけたリストを作成する。

・ボット対策システム運用グループから、検体および関連する情報を取得する。
・クライテリア（優先順位）により、解析を行う検体を抽出する。
クライテリアは表 3-1 の通りに設定している。

表 3-1 検体を抽出するクライテリア

クライテリア	検体の攻撃活動	ウイルス対策ソフトによる検体状況
1	有	駆除ツール開発事業者、および、他 2 社のウイルス対策ソフトで未知
2	有	駆除ツール開発事業者のウイルス対策ソフトで未知（他 2 社のウイルス対策ソフトで既知・未知は問わない）
3	無	駆除ツール開発事業者、および、他 2 社のウイルス対策ソフトで未知
4	無	駆除ツール開発事業者のウイルス対策ソフトで未知（他 2 社のウイルス対策ソフトで既知・未知は問わない）

・駆除ツールに反映することとなった検体について対応リストを作成する。

・ボット対策システム運用グループへ対応リストを送付する。

(2) 駆除ツールの作成

上記(1)対応リストの作成は毎日行う作業であるが、(2)駆除ツールの作成は週に一度行う作業である。

・毎週月曜日までに収集した検体について、解析および駆除ツールの作成を水曜日までに実施する。
・作成した駆除ツールを、ボット対策システム運用グループへ提供する。
・ボット対策システム運用グループは、注意喚起を受けたボット感染ユーザがアクセスする対策サイトを通して駆除ツールを配布する。また、一般ユーザ向けにも CCC サイトで駆除ツールを提供する。
・ISP は、ボット感染ユーザにボットの駆除依頼メールを送付する。

3.2.2 詳細解析の実施

上記解析の結果、実態を把握する必要があるボット検体やユーザへの影響度が大きい検体を対象に、以下の項目等に関する詳細な解析をしている。本処理は、不定期に実施する。

・ボット自体の行動パターン
・利用されている技術
・ボットの感染ルーチン

3.2.3 ボット感染予防推進グループへの検体の提供

ボット対策システム運用グループから提供された検体、および、関連する情報を、ボット感染予防推進グループへ提供している。

ボット対策システム運用グループから受け取った検体は、翌営業日の午前中にボット感染予防推進グループへの提供を実施していたが、より迅速に検体を提供し、セキュリティベンダが本プロジェクトで収集している検体へ対応することができるよう、オペレーションの変更を実施した。

これにより、ボット対策システム運用グループから受け取った検体を当日中にボット感染予防推進グループへ提供することとなり、変更前と比較し、1 日早く検体を提供することが可能となった。その結果、ボット感染予防推進グループから提供された以下のデータによると、対応パターンファイルがより早くユーザに流通することに寄与したことが分かった。（表 3-2）

表 3-2 検体提供時のパターンファイル反映状況

	変更前 20 日間	変更後 20 日
取得時に反映済みだった検体	97.0%	90.5%
取得時に未反映だった検体	3.0%	9.5%

3.3 駆除ツールの機能拡張

駆除ツールについて、ユーザの視点に立った改善することを目的として、機能を拡張した。拡張した内容は以下の通りである。

3.3.1 使用期限設定機能の追加 （平成 19 年度 4 月リリース）

最新の駆除ツールを使用せず、古い駆除ツールを使い続けても、新たなボットやその亜種に対応することができない。感染しているにもかかわらず、古い駆除ツールを使ってボットが発見されないことにより、「自分は感染していない」、「対策はとっているから安心」と勘違いしてしまうケースがある。このため、過去のパターンファイルを搭載した駆除ツールが使い続けられることのないように、使用期限を設定できるよう機能を追加した。

3.3.2 検体の種類に応じた標準設定モードの追加 （平成 19 年度 4 月リリース）

ボットは、PC のメモリに常駐してプロセスとして動き続けるタイプと、PC のリソースに感染しファイルとして存在するタイプがある。駆除ツールは、PC のリソースに感染したファイルを検索すると時間がかかるため、検索オプション設定を、当初、メモリ検索を標準設定（デフォルト設定）としていた。

しかし、駆除注意喚起を受けるユーザが感染したボットの特性に応じて、それぞれのタイプに分けた駆除ツールを提供することが必要であったため、検索対象(メモリまたはハードディスク)を選択できる標準設定モードを追加した。

その後、ファイル感染型（以降、PE 型と記述する）ボットが急増したことからメモリ検索およびファイル検索の両方が標準設定された駆除ツールを提供している。表 3-3 に駆除ツール標準設定の推移を示す。

表 3-4 駆除ツールの標準設定の推移

サイト	平成19年度4月以前のモード設定	平成19年度4月リリース時のモード設定	平成19年度11月以降のモード設定
感染ユーザ用対策サイト	メモリ検索のみが標準設定	駆除注意喚起を受けたユーザが感染した検体により、メモリ検索、または、ファイル検索が標準設定	メモリ検索とファイル検索の両方が標準設定
一般サイト	メモリ検索のみが標準設定	メモリ検索、ファイル検索の両方が標準設定	メモリ検索とファイル検索の両方が標準設定

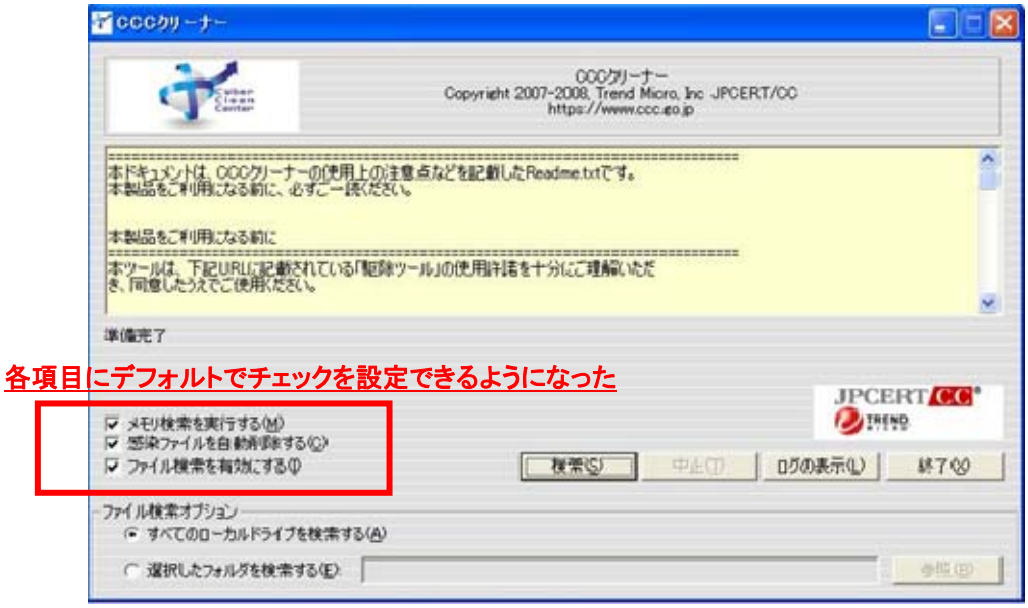


図 3-1 標準設定モードが反映された画面

3.3.3 Windows 98/Me への対応

平成 19 年度、「ユーザから Windows 98/Me に対応しているウイルス対策ソフトが少なくなっていることから、駆除ツールを Windows98/Me に対応させてほしい」という要望があった。しかし、Windows98/Me は、すでに OS ベンダであるマイクロソフト社のサポートが終了していたため、駆除ツールにおいても対応しないこととした。更に、各セキュリティベンダの動向を調査した結果、2008 年末頃に Windows98/Me に対応するウイルス対策ソフトのサポートも終了することが判明した。

そこで、ユーザに対して、Windows98/Me を使用し続けることは、OS ベンダのサポ

ートが終了し、セキュリティ更新プログラムの提供も停止していることから、新たな脆弱性が発見された場合対応できないため、リスクがあることを訴えた。

また、暫定の回避策として、OS のアップグレード （PC の買換えを含む） までの一時的な対策と位置付けて、問い合わせをしてきたユーザに対して、メディアが掲載した記事（http://www.itmedia.co.jp/enterprise/articles/0707/10/news005.html）や、独立行政法人情報処理推進機構（IPA）情報セキュリティ「2007 年 5 月の呼びかけ」の記事（http://www.ipa.go.jp/security/txt/2007/05outline.html#5）を案内することとした。

3.3.4 Windows Vista への対応 （平成 19 年度 11 月リリース）

より多くのユーザに駆除ツールを使用してもらい、ボットの検出･駆除を推進するため、Windows Vista に対応した。

3.3.5 検出状況等送信機能 （平成 19 年度 11 月リリース）

駆除ツールの実行後、検出状況などを CCC へ送信する機能を追加した。ユーザより送信された情報を活用することにより、さらに効果的なボット対策の実現を目指した。

本機能にて送信する情報は、以下の通りである。なお、ユーザが情報を送信するか否かは、駆除ツール実行時に選択することができる。

- OS のバージョン情報
- 実行日時
- 検出数/駆除数/未駆除数
- 検出マルウェア名
- エラー情報

3.4 ボットの傾向

3.4.1 収集したボットの傾向

表 3-5 は、平成 19 年度に本プロジェクトで同定解析後のボットファミリーのトップ 15 である。このように、収集されたボットはワームだけではなく多岐にわたる。

表 3-5 収集したボットファミリー数トップ 15（平成 19 年度）

	ボットファミリー名 （トレンドマイクロ社 ウイルス対策ソフト検出名）	Type	同定検体数
1	WORM_ALLAPLE	ワーム型	86458
2	PE_VIRUT	PE 型	65234
3	WORM_BOBAX	ワーム型	10489
4	PE_BOBAX	PE 型	6420
5	WORM_CHELI	ワーム型	3061
6	PE_SALITY	PE 型	2136
7	WORM_RBOT	ワーム型	1360
8	PE_VBAC	PE 型	1107
9	BKDR_VANBOT	BKDR 型	1042
10	WORM_SDBOT	ワーム型	471
11	TROJ_AGENT	TROJ 型	394
12	BKDR_IRCBOT	BKDR 型	350
13	TROJ_QHOST	TROJ 型	337
14	BKDR_POEBOT	BKDR 型	299
15	WORM_IRCBOT	ワーム型	279

トレンドマイクロ社によると、各タイプの定義は、表 3-6 の通りである。

表 3-6 ボットのタイプと定義

Type	定義	URL
PE 型	「Portable Executable」という標準的な Windows の実行可能なファイル形式である。PE 形式（拡張子が COM、EXE、SYS など）に感染するファイル感染型ウイルスを「PE_xxxxxx」のように接頭語”PE”として検出する。	http://jp.trendmicro.com/jp/threat/glossary/p/pe/
ワーム型	ネットワークを通じて他の PC に拡散	http://jp.trendmicro.com/j

	することを目的とした不正プログラムを一般にワームと呼んでいる。	p/threat/glossary/jp-wa/worm/index.html
TROJ 型 （トロイの木馬型）	プログラムへの感染を行わない不正プログラムの総称。	http://jp.trendmicro.com/jp/threat/glossary/jp-to/troi-no-mokuba/index.html
BKDR 型 （バックドア型）	TROJ 型の一種。ネットワークを介して感染ユーザの PC を自由に操ったり、パスワードなど重要な情報を盗んだりすることを目的としている。	http://jp.trendmicro.com/jp/threat/glossary/jp-ha/backdoor-gaata/

最近の PE 型はファイル感染機能だけではなく、ワーム機能、バックドア機能、ダウンロード機能などを兼ね備えたタイプのものが多い。

PE 型ボットは、OS やアプリケーションの実行形式のオリジナルファイルへ悪性コードを埋め込む性質を持っている。一方、PE 型以外のタイプは、ボットそのものが一つのプログラムファイルである。このことから、攻撃者は自ら作成したボットを発見されまいとする隠蔽化だけではなく、発見されてしまうことを前提に、検出・駆除されにくいようにボットを設計していると推測できる。

3.4.2 PE 型ボットの急増

PE 型ボットは、OS やアプリケーションに存在するファイルに感染するため、同じ種類のボットであっても感染先のファイルが異なる場合がある。その場合は別検体としてカウントされてしまうため、1 台の PC 上で多数の感染が発見されることもある。

本プロジェクトのハニーポットで収集した検体を同定した後、ファミリー別に整理した統計（図 3-2）を見ると、2007 年 11 月以降から、PE_VIRUT ファミリーが急増していることが分かる。

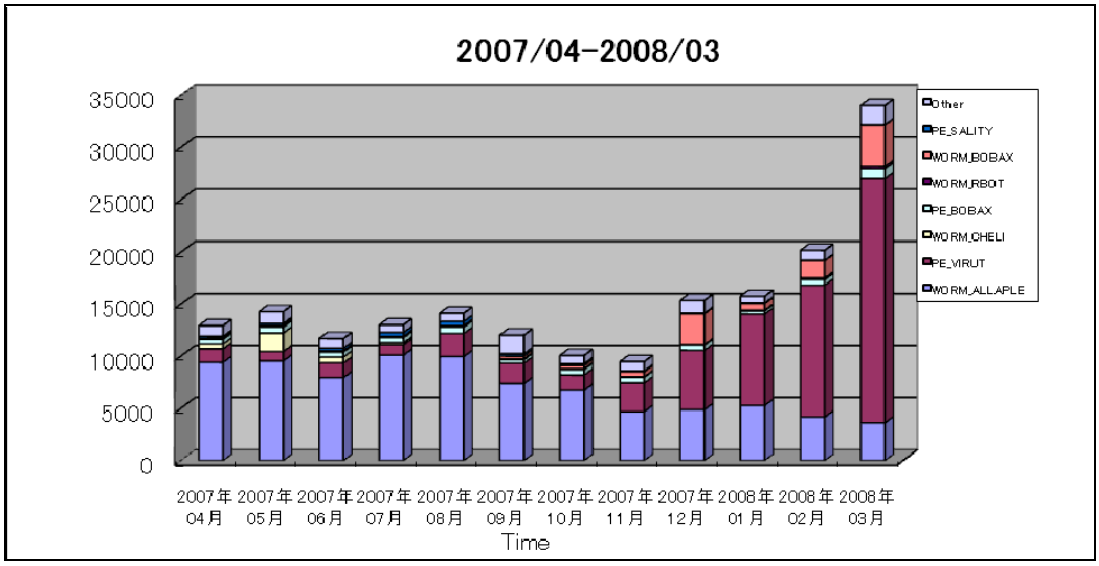


図 3-2 収集したボットファミリーの割合比較

PE_VIRUT ファミリーは、バックドア機能を備え、感染すると C&C サーバに接続し、IRC チャンネルを介してリモートコマンドを受信する機能を持っている。

3.4.3 PE 型ボットと駆除ツールにおける対応への課題

PE 型ボットは、感染手法において、オリジナルファイルのコードの先頭または末尾に悪性コードを追加するタイプ、オリジナルファイルの未使用部分に悪性コードを挿入するタイプ、オリジナルファイルのコードの一部またはすべてを悪性コードで上書きするタイプなどがある。

一方、駆除ツールは、PC のメモリ領域やディスク領域を順番に検索する機能であるため、検索・駆除処理中の過程で、まだ駆除していない感染ファイルから検索・駆除済みのファイルに感染活動が行われる場合がある。このような場合、駆除ツールでの検索・駆除結果が、「すべて駆除」となっていたとしても、駆除ができていない可能性がある。

オリジナルファイルのコードの一部またはすべてを悪性コードで上書きするタイプに感染した場合は、オリジナルファイルのプログラム情報が失われるため、復元することはできない。もし、オリジナルファイルが OS やアプリケーションの実行形式ファイルであった場合、リカバリ（初期化）が必要となることがある。また、それ以外のタイプの PE 型ボットに感染した場合は、市販のウイルス対策ソフトを導入し、パターンファイルをアップデートして、PC 内を常時監視させることにより、駆除および感染を防止することができる。

3.5 今後の展開

平成 19 年度は、平成 18 年度の現行スキーム（リスト作成、検体解析、駆除ツール作成）に加え、運用スケジュールの調整や駆除ツールの機能追加を行った。

平成 20 年度は、引き続き現行スキームの運用を行うことにより、駆除ツールの安定した提供を目指す。また、急増している PE 型ボットへの対応を行う予定である。

① 駆除ツールの機能拡張
PE 型ボットに感染した場合の警告表示や、その対策方法をユーザへ案内する機能を追加する。

② 駆除ツールの作成
駆除ツールを安定して供給する。

③ ボットの解析
蓄積した動的解析および静的解析の結果により、ボットなどに関する傾向分析を行う。

④ 普及啓発活動支援
ボット感染防止対策の普及活動支援を行う。

4 ボット感染予防推進グループ活動報告

4.1 概要

ボット感染予防推進グループは、広く一般ユーザにおけるボット感染予防策の強化および再発防止を図るべく、セキュリティベンダ（以下「感染予防対策ベンダ」という）と連携して、本プロジェクトに取り組んでいる。具体的には、感染予防対策ベンダに対して、本プロジェクトにて収集したボットを検体として提供し、各感染予防対策ベンダが販売しているウイルス対策ソフトのパターンファイルに反映させる。これにより、ユーザがウイルス対策ソフトのパターンファイルを最新のものに更新すれば、ユーザのウイルス対策ソフトは本プロジェクトで収集したボットを検出・駆除することができるようになり、セキュリティ対策の向上が期待できる。

4.2 感染予防対策ベンダ

本プロジェクトに参加する感染予防対策ベンダは、検体の厳格な管理基準を実施し、我が国内に解析部署があり、我が国でウイルス対策ソフトの供給・サービス提供に相当の実績を有している法人である。こうした感染予防対策ベンダの参加を得て、ユーザの PC などにおける感染予防を推進していく活動を行っている。

2007 年 11 月に株式会社アンラボ、株式会社 Kaspersky Labs Japan が新規加入した。

参加感染予防対策ベンダ一覧（50 音順 敬称略）

- 株式会社アンラボ
- 株式会社 Kaspersky Labs Japan
- 株式会社シマンテック
- ソースネクスト株式会社
- トレンドマイクロ株式会社
- マイクロソフト株式会社
- マカフィー株式会社

4.3 活動成果

感染予防対策ベンダが 2007 年 3 月から 2008 年 3 月末（報告月：2007 年 5 月から 2008 年 4 月）までに、本プロジェクトにおいて取得した検体のパターンファイルを各ベンダのウイルス対策ソフトへ反映した状況について、各ベンダ平均の数値を図 4-1 に示す。

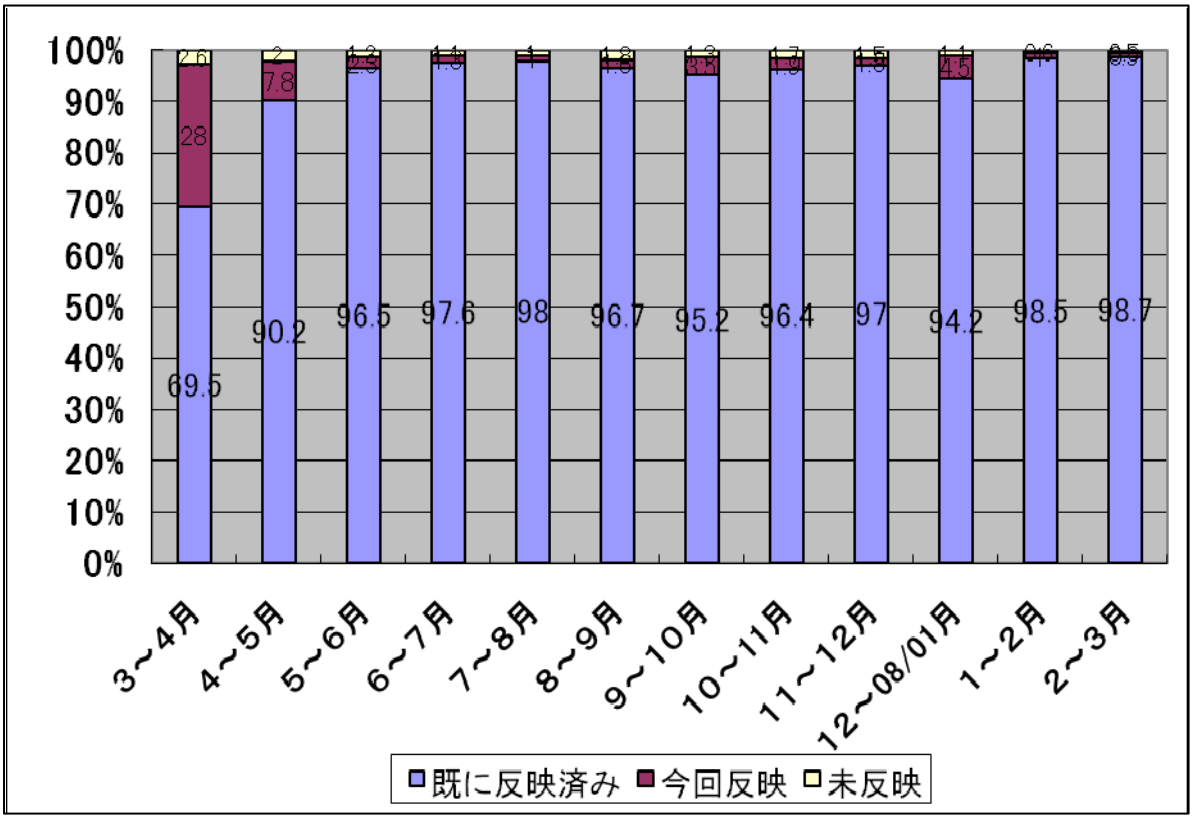


図 4-1 各社対応状況の推移

① 2007 年 10 月に検体受渡しスケジュールの短縮を行ったことで、若干「今回反映」の数値が増加している。
② 2007 年 11 月にハニーポットの XP 化が行われたが、反映率への影響は特に見られなかった。
③ 2007 年 12 月～2008 年 1 月は、あるベンダにおいて集計のトラブルが発生していた為「今回反映」の数値が増加している。

この数値は本プロジェクトの成果の一つとして、収集された検体が充分活用されていると考えられる。なお、現在参加している感染予防対策ベンダの国内におけるシェア合計は 90%以上となっており、平成 19 年度に登録された検体が、一般ユーザの感染予防に十分寄与していると判断される。

4.4 今後の活動

引き続き収集された検体の厳格な管理を行うとともに、各ベンダが販売しているウイルス対策ソフトのパターンファイルへの更なる反映を推進すべく、各ベンダと連携して本プロジェクトに取り組んでいく。

5 まとめ

平成 19 年度は、前年度の活動実績を踏まえ、各グループが連携して本格的にボット対策に取り組んだ年であった。

プロジェクト参加 ISP は当初の 8 ISP から平成 19 年度末には 68 ISP に増加した。駆除ツールについては、WindowsVista への対応や機能追加などを進め、より多くのユーザに効果的に利用していただけるものとした。また感染予防対策ベンダについても、平成 19 年度中に 2 社が新たに加わることにより、感染予防対策ベンダの国内シェアは約 90%となった。また、CCC の取り組みがメディアに取り上げられる機会も増え、CCC の認知度も徐々に向上してきている。

こうした取り組みにより、一部のプロジェクト参加 ISP で注意喚起対象者数が減少を見せるなど、対策効果を示唆する指標がいくつか見られ始めている。その一方で、ボットの機能や感染手法は日々変化してきており、こうした変化に対応していくため、よりいっそうの努力も必要である。

本プロジェクトでは、今後も継続的に活動を行い、より安心・安全なインターネット社会の実現に向け、大きく寄与していくことを目指したい。

6 さいごに

～ボットの被害を最小限にするために～

サイバークリーンセンター（CCC）では、ボットによる被害を最小限にするために、対策を推奨しています。

ボットの感染被害を確実に防ぐ方法はありませんが、下記に挙げた対策を実施することにより、ボットの被害を最小限にすることができます。

≪感染予防対策≫

1. コンピュータを最新の状態にする
2. ウイルス対策ソフトを必ず導入する
3. パーソナルファイアウォールを利用する
4. インターネット接続にブロードバンドルータを利用する
5. HTML 形式のメールはプレビューしない
6. 添付ファイル付きの電子メールには十分気をつける
7. ID とパスワードによる認証と強固なパスワードを使用する

詳細な手順は下記サイトにて公開しております。

https://www.ccc.go.jp/knowledge/index.html

ぜひ、皆様の PC の安全を守るため、ウイルス対策を宜しくお願いいたします。