平成 18 年度

サイバークリーンセンター活動報告

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

1 はじめに 1
1.1 ボットの現状 1
1.2 CCCの概要 2
2 ボット対策システム運用グループ活動報告 4
2.1 概要 4
2.2 検体収集・攻撃事象検知 4
2.2.1 検体収集の概要 4
2.2.2 成果 5
2.2.3 今後の展開 7
2.3 注意喚起 8
2.3.1 ISPにおけるAbuse対応業務と課題 8
2.3.2 注意喚起の概要 10
2.3.3 成果 14
2.3.4 今後の展開 18
3 ボットプログラム解析グループ活動報告 19
3.1 概要 19
3.2 解析 19
3.2.1 簡易解析、詳細解析の処理フロー 19
3.3 静的解析 21
3.3.1 静的解析に関する研究 21
3.3.2 ボットの傾向分析 21
3.4 今後の展開 24
4 ボット感染予防推進グループ活動報告 25
4.1 概要 25
4.2 感染予防対策ベンダ 25
4.3 活動成果 26
4.4 今後の活動 26
5 まとめ 27

1 はじめに

近年、インターネット上で感染拡大している不正プログラムの一種「ボット」には非常に多くの亜種が存在し、従来のコンピュータウイルスの駆除手法による対応が困難となってきている。また、ボットによる攻撃・感染活動は限定的かつ水面下で巧妙に実施される傾向があることから、ユーザ自身が攻撃や感染の事実を認識しづらいという深刻な状況である。いつのまにかボットに感染してしまったユーザが、スパムメールやフィッシング、DDoS（分散協調型サービス不能攻撃）などサイバー攻撃の温床になっていると言われている。

このような状況において、安心・安全なインターネット環境の実現を目指し、ボットの攻撃・感染活動を効率的かつ安全に把握し、感染ユーザを特定して対策手法を具体的に提示することでボットの駆除を促すといった、総合的なボット対策が不可欠であることから、2006 年 12 月、総務省および経済産業省では、両省が共同で実施する「ボット対策プロジェクト」を開始し、同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（以下、CCC）」を開設した。

CCC では、関係機関、ISP（インターネットサービスプロバイダー）、ボット駆除ツール作成事業者、およびセキュリティベンダ等が有機的に連携した統合基盤を構築・運用し、ボット駆除の注意喚起活動を効果的かつ継続的に実施することにより、国内ボット感染者の撲滅を目指している。

1.1 ボットの現状

ボットとは、PC を悪用することを目的に作られた不正プログラム（Malware）の一種であり、ボットに感染した PC は悪意を持った攻撃者（ハーダー）から遠隔操作され、スパムメールの大量送信や、特定サイトへの DoS 攻撃などを行う。つまり、感染 PC を使用しているユーザの多く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」にもなってしまうのである。

ボットに感染した PC は攻撃者が用意した指令サーバなどに自動的に接続され「ボットネットワーク」といわれる数十～数万台の巨大ネットワークを形成し、大きな脅威となる。

これまでのウイルスなどは愉快犯的なものがほとんどであったのに対し、ボットの場合はボットネットの時間貸しや搾取した個人情報の販売など商用目的に移り変わっている。そのため感染した PC 自体では特に症状が現れないことからユーザに気づかれにくい特徴を持つとともに、自分自身をアップデートすることによりアンチウイルスソフトで発見しづらくするなど巧妙かつ悪質なものとなっている。

2005 年に Telecom ISAC Japan および JPCERT/CC 等で実施された調査によると、日本のインターネットブロードバンドユーザの 2～2.5%ほどがボットに感染していると推計された。国内のブロードバンドユーザを約 2000 万と仮定すると、40～50 万台の PC が感染していることとなる。仮に、これらボット感染 PC が一斉にサイバー攻撃に悪用されれば、世界中のインターネットを破壊することすら容易に可能である。

1.2 CCC の概要

ボットに感染してしまうユーザは、アンチウイルスソフトを導入していない、Windows Update を適用していない等セキュリティ対策が不十分なままの PC を使い続けているユーザがほとんどであり、またボットの特性からその感染に気づいていないことが多いと考えられる。CCC では、ISP を通じて、感染ユーザに対して「感染している事実」を通知し、ボットの駆除を促すというプロセスを実施している。

具体的には、先ず、①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。次いで、②ボット検体を解析して“駆除ツール”を作成する一方、③ISP 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。最後に、④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。

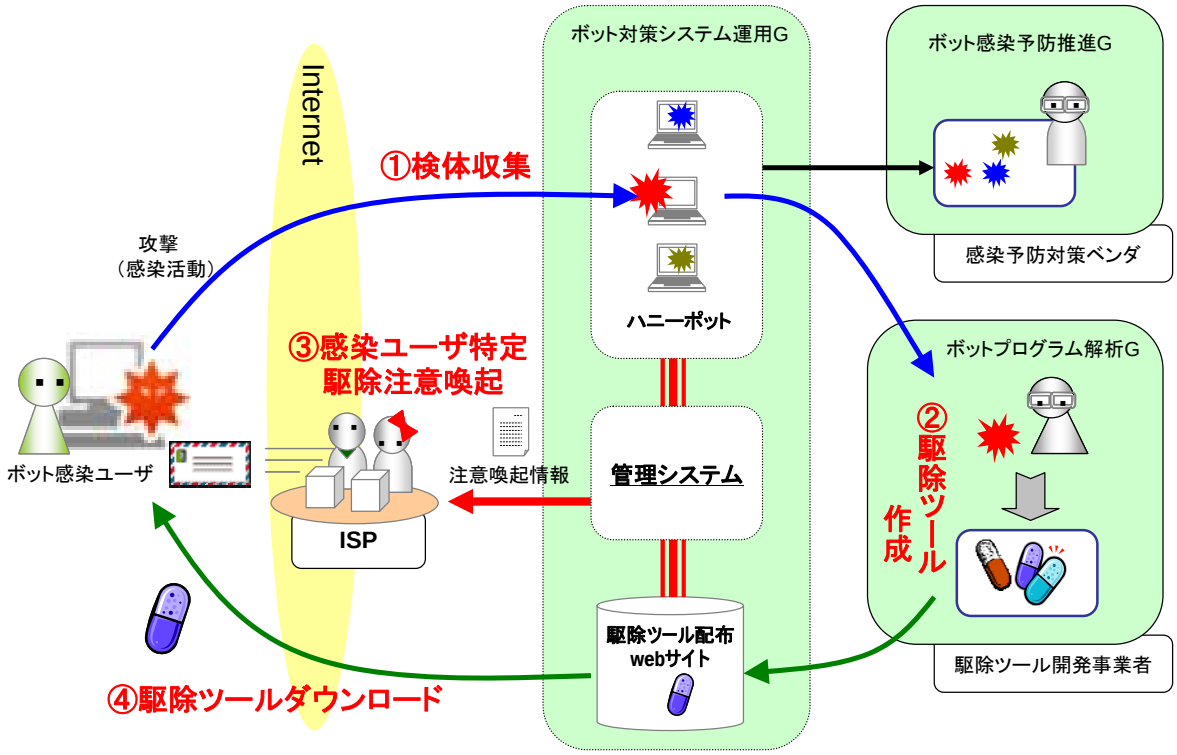

図 1.2.1 CCC の注意喚起プロセス

CCC は、サイバークリーンセンター運営委員会（CCC-SC）と業務内容に応じた 3 つのグループによる体制で、運用されている。

【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、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、ボットをはじめとする Malware の最新動向の

調査も行う。

<プロジェクト参加 ISP>

BIGLOBE、DION、hi-ho、IIJ、@nifty、OCN、ODN、Yahoo!BB

【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、検体をセキュリティベンダに適切に提供して各社のアンチウイルス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>

マイクロソフト株式会社、ソースネクスト株式会社、トレンドマイクロ株式会社

マカフィー株式会社、株式会社シマンテック

図 1.2.2 CCC 運営体制図

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、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し、ボットプログラム解析グループへ検体を引き渡す。
また、ISP と連携して感染ユーザの特定およびボット駆除の注意喚起を実施するとともに、ボットプログラム解析グループで作成されたボット駆除ツールを適切に管理し、感染ユーザへの配布を行っている。

なお、ボット感染ユーザに対してボットの駆除注意喚起を促す手法としては、画一的な周知メールを配信する方法が効率的と思われる。しかしながら、ボットに感染するユーザは、OS のアップデートをしていないなど、セキュリティ対策への意識が高くないユーザが多いと思われるため、画一的な周知を受けて自ら率先して対策を実施することが難しいと考えられた。そこで本プロジェクトでは、ISP と連携して感染ユーザを特定した上で、感染の事実とボット駆除の注意喚起を個別に行う手法（オーダーメード治療）を採用している。

ここで、オーダーメード治療を実施するには感染ユーザの正確な特定が不可欠であり、そのためにはボットに感染した PC からの感染活動を検知することが重要である。本プロジェクトでは、多数のハニーポットを配置することによって感染活動を安全かつ確実に検知し、感染活動の発信元や、感染したボットのタイプなどを解析して、感染ユーザを特定する手法を採用している。

2.2 検体収集・攻撃事象検知

2.2.1 検体収集の概要

ボット感染ユーザに注意喚起を行うためのトリガーとして、感染ユーザからの攻撃（感染活動）を検知しボット検体を収集する。ボットの感染活動は、ワーム型、メール添付型、P2P 型、Web 型など様々なタイプが考えられるが、本プロジェクトでは PC の脆弱性を狙って感染活動を行うワーム型に焦点をあて、意図的に脆弱性を残したハニーポットによって感染活動を検知する方法を採用している。
本プロジェクトのハニーポットは、プロジェクト参加 ISP を利用しているユーザに近い IP アドレスレンジを幅広く効率的にカバーできるよう考慮されており、ごく近隣に限定的に感染活動を行うボットをも効率よく収集することが可能である。
また、検体を収集するためのハニーポットについては世界中で様々な研究が行われているが、本プロジェクトにおいてはボット検体自体の収集・分析が主目的ではなく、感染ユーザに対しボット駆除の注意喚起を確実に行うためのトリガーとしてボット検体の収集を行うものであることか

ら、多様な検体を数多く収集するだけでなく、その検体が、いつ・どこから送られてきたかなどの情報を確実に取得するための創意工夫をしている。

2.2.2 成果

ボットの攻撃事象の検知を開始した2006年11月24日から2007年3月末時点までの実績として、攻撃事象の検知数（ボット検体が完全体で収集できた場合のみ)、検体数（ハッシュ値で区別した種類数)、および収集した検体のうち市販のアンチウイルスソフトで検知できなかった検体数について以下に示す。なお、プロジェクト当初は小規模な検証用システムにおける暫定運用であったが、2007年2月6日より本格的な運用を開始している。

表 2.2.1　攻撃検知数および検体数

攻撃事象検知数	974,999
ボット検体数（種類）	31,082
市販アンチウィルスソフトで検知できなかった検体数	1,711

毎日500種類程度のボット検体が収集され、そのうち20～30種類は市販のアンチウイルスソフトでも検知できないボットであった。

また、本格運用（2007年2月6日以降）においては、検知した攻撃事象の送信元に関する詳細な分析も実施した。送信元IPアドレスを日次で分析し、本プロジェクトに参加しているISP、その他の国内ISP、海外の3項目に分類して集計した結果を下記に示す。

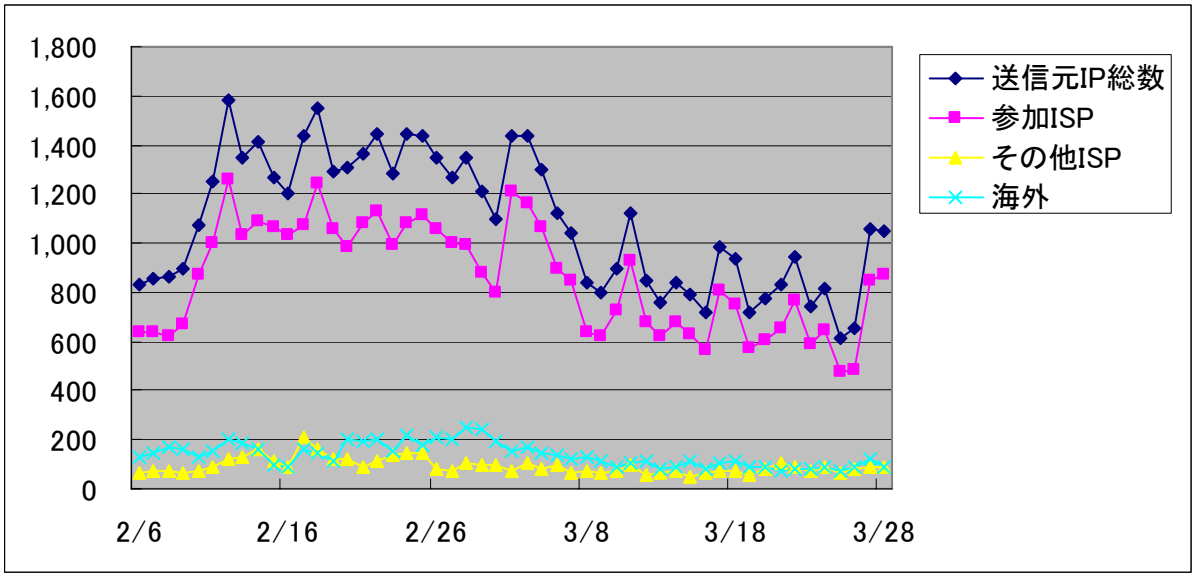

図 2.2.1 攻撃事象送信元 IP 数（日毎）

攻撃事象送信元 IP 数の 1 日あたりの平均値を下記に示す。参加 ISP に属する IP からの攻撃が約 8 割を占める結果となった。

表 2.2.2 攻撃事象送信元 IP 数（1 日あたり）

	参加ISP	その他ISP（国内）	海外
送信元IP数[IP/日]	858	93	137
率[%]	78.9%	8.5%	12.6%

また、海外からの攻撃を国別に集計すると、TOP10 は CN：中国、TW:台湾、KR：韓国、US：アメリカ、HK：香港、PH：フィリピン、IN：インド、MY：マレーシア、TH：タイ、VN：ベトナムとなる。日本の IP アドレスレンジに近いアジアから攻撃が集中していることがわかる。

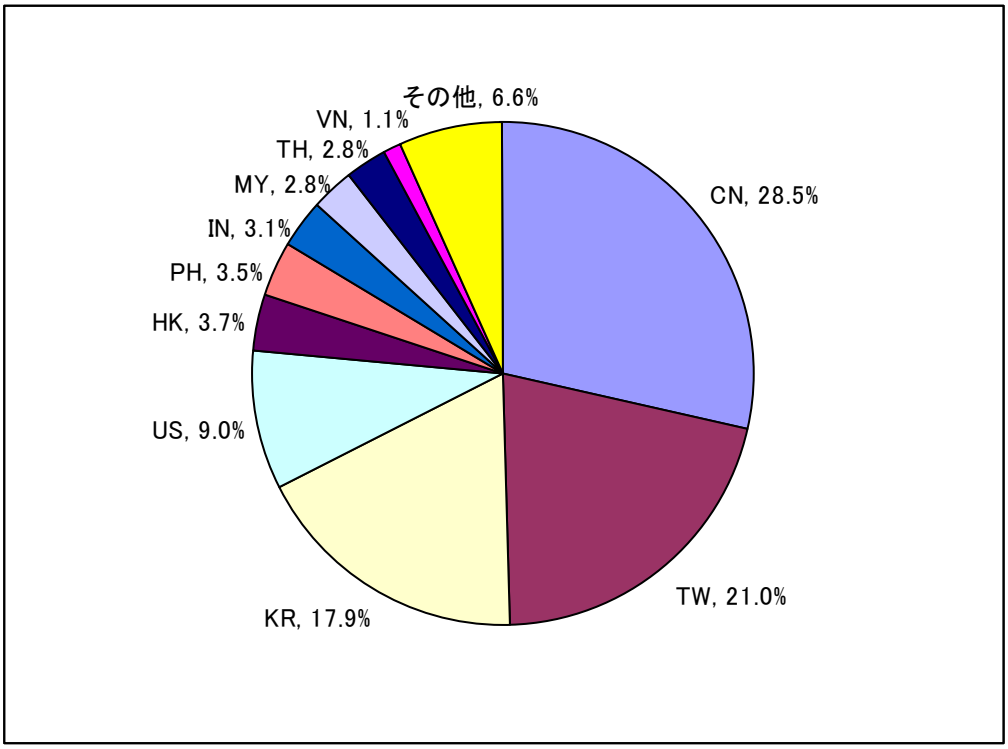

図 2.2.2　海外からの攻撃事象数

本プロジェクトにおいては、参加 ISP を介した注意喚起の対象となる感染ユーザを検知したいという観点から、参加 ISP が管理する IP アドレスがハニーポットにアサインされるよう設計している。前述の結果から、ボットの感染活動は感染ユーザ近傍の IP アドレスに対して限定的に行われる傾向があることが改めて確認できた。

従って、現時点で本プロジェクトにまだ参加していない ISP や CATV との連携拡大を行うにあたっては、それぞれの ISP や CATV で管理する IP アドレスをハニーポットに割り当てることが有効であると考えられる。

参加 ISP 以外のその他国内からの攻撃元は、ISP、CATV などの他にも、企業、学校等が該当する。本施策の目標を達成するため、これらへの対応も実施していくことが重要である。

2.2.3 今後の展開

2.2.3.1 ハニーポットの高度化

より効果的な注意喚起活動への足がかりとなるべく、現行のハニーポット方式の高度化を図る。具体的には、現在ハニーポットで採用している OS の対象範囲を広げユーザ環境により近い環境にすることや、検体収集ポイントの拡大（現在は東京のアクセスポイントのみ）などについて、その具体的なプランニングと効果を検討する。

2.2.3.2 新たな検体収集手法の検討

OS の脆弱性を狙うワーム型感染タイプの検体収集だけでなく、P2P 型、WEB 型といった多様な感染形態にも対応した検体収集手法の検討を行い、より広範囲の感染ユーザに対する注意喚起を行うことを予定している。

2.3 注意喚起

2.3.1 ISP における Abuse 対応業務と課題

本プロジェクトでは、ハニーポットで捕獲したボット検体の通信を解析し、その送信元である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。ここで、CCC のハニーポット運用部門における通信解析により取得できるのは、ボット送信元の IP アドレスや時刻情報などである。よって、どの ISP が管理する IP アドレスかは調査できるものの、感染ユーザ自身の連絡先（メールアドレスなど）まで究明できるわけではない。

一般的に、個人や組織が「インターネットにおける不適当な行為」の被害を受け、その行為者に注意を促したいとしても、直接の行為者に連絡することはできず、またこのような事案について総括的に対応できる窓口がほとんど存在していない。従って、行為者の IP アドレスを確認し、ISP に対応を依頼することになる。

各 ISP において、自社のユーザによるサービスの違法利用や迷惑行為といった案件へ対応するために、「Abuse 対応」なる業務が ISP の本来業務として位置づけられている。“Abuse”という名称は、RFC 2142（*注） において「公共における不適当なふるまいがあった場合の連絡先窓口」として、Abuse というメールボックス名が規定されていたことに起因する。

*注　RFC：IETF (Internet Engineering Task Force) におけるインターネットコミュニティの標準等の検討が公表される一連の文書

本プロジェクトにおいても、感染ユーザに対する具体的なアプローチは、プロジェクトに参加する ISP の Abuse 対応部門との連携が不可欠である。Abuse 対応窓口に注意喚起を依頼する手法は、スパムメールの対応等において既に一般化しているものの、その業務の特性から課題も多い。多数の感染ユーザに対して短時間のうちに、かつできるだけ少ないコストで注意喚起することを実現するためには、ISP における Abuse 対応業務の実情を深く理解して課題を克服し、各 ISP とシームレスに連携した注意喚起プロセスを確立する必要がある。

2.3.1.1 ISP における Abuse 対応業務の概要

多くの ISP において、Abuse 対応窓口は顧客管理部署の一部門として存在している。これ

は、Abuse 案件に該当する行為があった場合、行為者となっているユーザを特定し連絡を行うほか、必要に応じてユーザに対するサービスの提供停止や強制退会等の措置を講ずるといった一連の業務が、顧客管理の範囲として考えられているためである。

しかしながら、通常の顧客管理事務と Abuse 対応とでは業務上必要とされる知識と経験が大きく異なる。具体的には、Abuse 案件の処理を進める為には、以下のような知識や経験が必要となる。

●ネットワークに関する知識

Abuse 案件の申告があった場合、果たしてそれが本当に自社のユーザによる行為なのかを見極める必要がある。例えば スパムメールの申告があった場合、メールの From アドレスやメールヘッダが偽装されていないかを判断できる知識が必要とされる。

●法的分野に関する知識

電気通信事業者である ISP は電気通信事業法により規律されているものであることから、サービス提供者として知りえる情報や技術的に可能な方策があっても、調査や対応に利用できない場合がある。また、不正利用をするユーザであっても消費者であり、安易に強制退会の措置を講ずることは消費者としてのユーザの権益を害することとなる。従って、このような法的知識を持った上で個別の案件について対応方針を決定していくスキルが要求される。

●ユーザのふるまいやクレームに関する経験値

Abuse 対応をする場合、担当者はクレームにさらされることがある。不正利用の被害を被っている申告者からのクレームと、何らかの措置があった場合のユーザからのクレームである。

上記のような知識や経験を持ち合わせた顧客管理担当者は希少であり、多くの ISP ではそれぞれの分野の専門部署が連携して対応方針を決定し、顧客管理部門に落とし込む、といった運用形態がとられている。

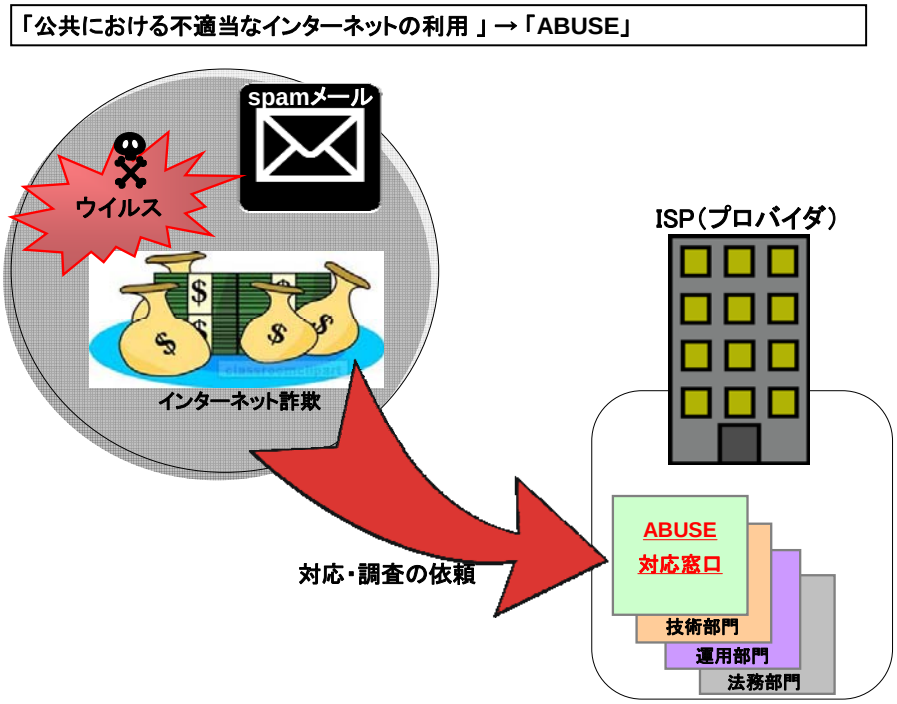

図 2.3.1　Abuse 案件とは

2.3.1.2 Abuse 対応業務における課題

前述のとおり、個人および組織からのユーザ対応依頼やクレームに対し、ごく限られたリソースで対応しているのが現状である。さらに、一部のセキュリティベンダ等においては、スパムメールやウイルスによるアクセスに関する情報を収集し、ISP に対し機械的に大量の対応依頼メールを送信している例もある。

ISP に寄せられる個々の案件について、担当者は IP アドレスとタイムスタンプを頼りにユーザを特定しユーザ対応を行うが、これは大変手間のかかる作業であり、さらに ISP のセキュリティポリシ上、顧客管理システムや認証サーバの情報を参照できるスタッフは限られているため定常的に稼動が逼迫し、対応に苦心している状況にある。

ISP において、Abuse 対応業務は ISP の社会的責務として認識されてはいるものの、コストセンターとしての位置づけであることは事実であり、リソース増強も容易には望めない。

従って、本プロジェクトにおける ISP と連携したユーザ注意喚起のプロセス確立においては、プロジェクト参加 ISP に対する業務負荷の軽減を念頭に置く必要がある。

2.3.2 注意喚起の概要

感染ユーザにボット駆除注意喚起を実施するプロセスの確立にあたっては、ISP の負荷軽減を考慮するとともに、感染ユーザが確実に注意喚起を受領し、確実にボット駆除を実施する有効なものでなければならない。本プロジェクトにおいては、カスタマサポートに造詣の深い有識者など

各参加 ISP からも意見を収集しながら、効果的なプロセスの確立を目指している。

2.3.2.1 注意喚起プロセスに求められること

●ISP との連携

ISP における Abuse 対応にはリソースの不足という問題がある一方で、ボットの特性を考えた場合、注意喚起の効果を最大限に発揮させる為には短時間の内に広範囲なユーザに対して注意喚起を実施し、ボット感染 PC からボットを駆除させなければならない、という命題が存在する。本プロジェクトにおいて、ISP の業務負荷となる具体的な項目は、

①顧客特定業務
②注意喚起メール送信業務
③ユーザサポート業務（問い合わせ対応）

であるため、これらの業務について ISP の負荷を軽減できるような仕組みが必要である。上記のうち顧客特定業務に関しては、ISP 毎に顧客管理システムや認証サーバの仕様が異なるため、業務フローの検討は各社に委ねているが、それ以外の業務に関しては本プロジェクト側から ISP に対しアプリケーション等を提供することによって負荷軽減を可能としている。

また、ISP が本来業務として Abuse 対応を行うための理由付けとして、「自社の提供するサービスを利用した公共における不適当なふるまい」が存在することが必要とされる点に関しては、感染ユーザが本プロジェクトの設備に対しボットを感染させた事実をもって、同様の通信をインターネット上に広く行っている蓋然性が高いものとして ISP に対応依頼を行うことで整理されている。

●即応性

ボットの特性の 1 つとして、外部からの遠隔操作によって自身をバージョンアップさせアンチウイルスソフトのパターンファイルによる検出を回避する挙動がある。この特性によって、ハニーポットで捕獲した時点では駆除ツールでの駆除が可能なボットであっても、ユーザによる駆除実施までに時間が経過しバージョンアップされてしまった結果駆除ができない、という結果が容易に想定される。

従って、ユーザ特定、駆除ツール開発、ユーザ注意喚起の一連のプロセスの確立にあたっては、関係各所がシームレスに連携し、可能な限り効率性を追求しなければならない。

●広範囲な対象ユーザ

感染ユーザは特定の ISP やネットワークに依存せず、均等に存在しているという調査結果も出ており、感染ユーザへの対応には、複数の ISP が協力してユーザへの注意喚起を進めていく体制が必要であると言える。

2.3.2.2 注意喚起の仕組み

本プロジェクトでは、前項を踏まえ、ISP が定常的な業務として継続的に注意喚起を実施できることを主眼とした仕組みとして、以下のような業務モデルの設計を行っている。

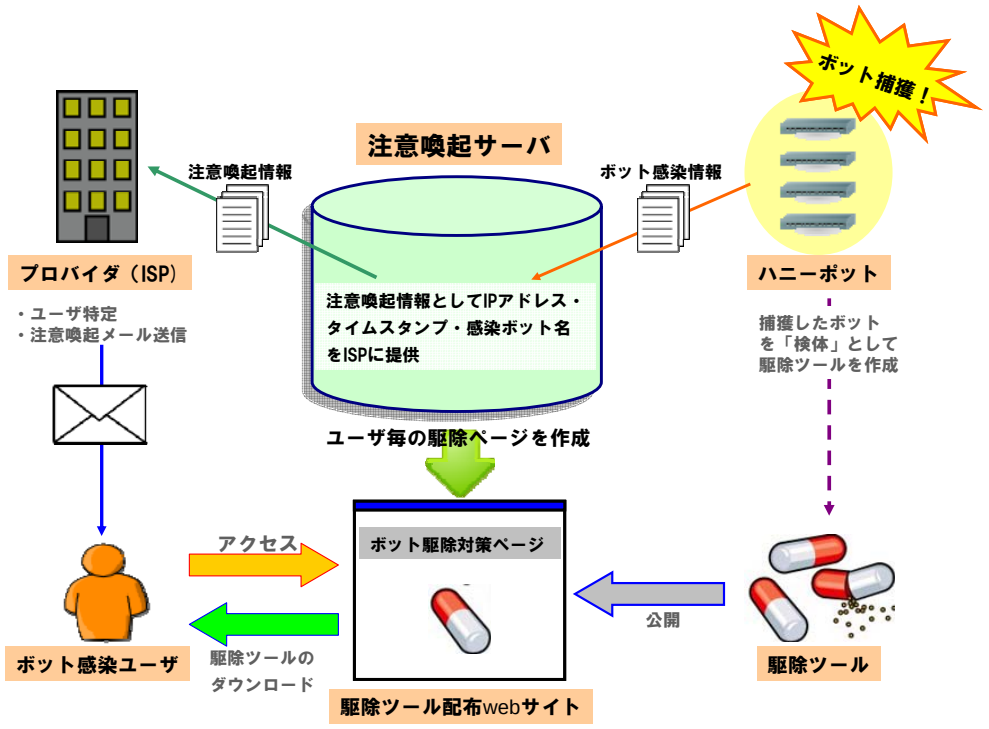

図 2.3.2　注意喚起の業務モデル

●注意喚起サーバ

ハニーポットに感染活動を仕掛けたボットの通信元 IP アドレスと時刻情報は、感染ユーザを特定するための注意喚起情報として ISP に提供される。注意喚起情報は ISP の定常業務に馴染むことを考慮し、専用サーバ（注意喚起サーバ）からのダウンロード方式で提供される（メール等による逐次通知方式では定常業務化が困難）。

ISP は任意のタイミングで注意喚起情報をダウンロードし、この情報を元にユーザの特定を実施し、ユーザに対し注意喚起メールを送信する。注意喚起メールには対策サイト（駆除ツール配布 web サイト）の URL が記載されており、ユーザに対策サイトを訪問させ駆除ツールをダウンロードさせることが目的となる。

●トラッキング ID

本プロジェクトでは感染ユーザ個別の ID となるトラッキング ID（氏名など個人を特定できる情報ではない）を生成し、このトラッキング ID を URL の一部としてユーザ毎に駆除ツール配布のための web サイトを公開している。

駆除ツール配布 web サイトはトラッキング ID によってユーザの訪問記録を取得している。訪問記録の取得ポイント（トラッキングポイント）はサイト内の各所に設定されており、トラッキングの記録を確認することでユーザがサイトを訪れたかどうか、駆除ツールをダウンロードしたかどうかを容易に把握することができるようになっている。

●注意喚起通知メールと対策サイト

ISP は注意喚起情報の IP アドレスと時刻情報を元に感染ユーザの特定を行い、ボット感染に関する通知と対策サイトの URL が記載されたメールを該当ユーザに送信する。

駆除ツール配布 web サイトには駆除ツールと共にボットに関する基本情報や駆除ツール実行の手順といったコンテンツが存在するほか、再感染予防に関するコンテンツも充実させている。これらのコンテンツは視覚的にユーザフレンドリーであることを意識して作成しており、メールの送信者である ISP に対し基本的な問い合わせが発生することを防いでいる（ISP のユーザサポート業務の軽減）。また、駆除ツール配布 web サイトが go ドメインで運用されていることもユーザに対する信頼性を高めている。

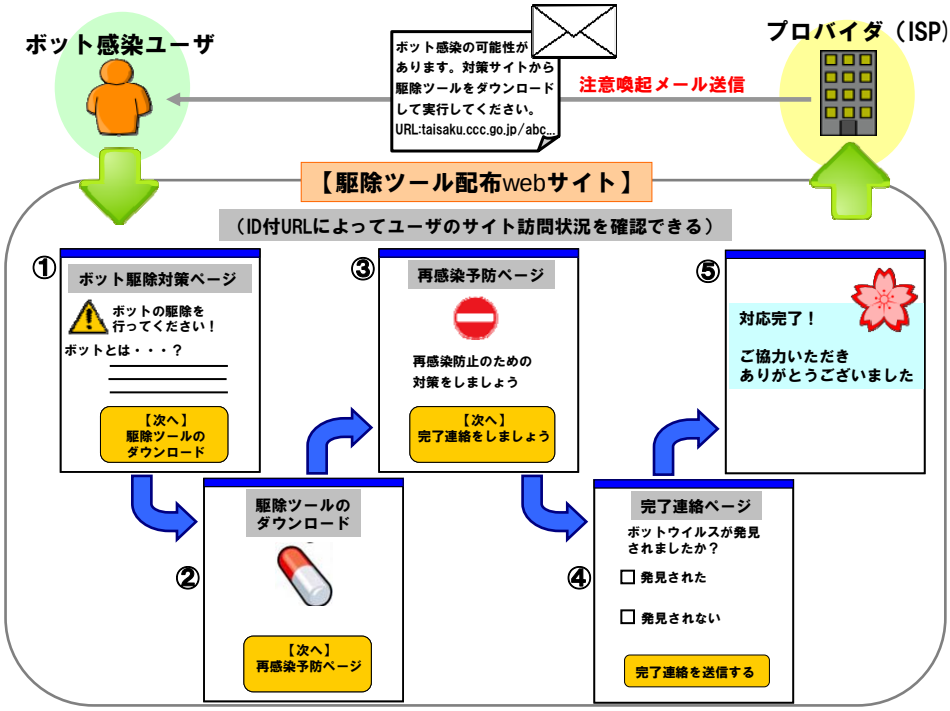

図 2.3.3　駆除ツール配布 web サイト構成図

●メール送信支援

また、本プロジェクトでは、メール送信業務の支援ツールとして、本業務専用のメール送信アプリケーションを ISP に配布している。このアプリケーションはセンター側サーバと連携し、テンプレート化されたメール文面をユーザの属性（個人 or 法人、はじめての感染 or

複数回の感染など）によって選択でき、設定された間隔でメールを送信することが可能である。

対策サイトにユーザが訪問したか、駆除ツールをダウンロードしたか等の履歴はトラッキング ID 単位で確認可能で、ISP に対しては任意のタイミングで参照できる形式にて提供される。

●注意喚起実施のサイクル

ハニーポットでのボット捕獲からユーザへの駆除ツールの提供までの処理時間が最短になるよう業務サイクルの設計、関係各所との調整を行った結果、駆除ツールの更新は 1 週間周期で実施し、これに同期して、駆除ツールの更新により駆除可能となったボットに感染するユーザに対し注意喚起を行うサイクルとしている。

ただし、すでに駆除ツール対応済のボットに感染したユーザから攻撃事象を検知した場合は、駆除ツール更新を待つ必要性がないため、すぐにユーザ特定、注意喚起メールの送信を実施するというサイクルも実施している。

2.3.3 成果

プロジェクト参加 ISP と連携した感染ユーザへの注意喚起結果について、2006 年 11 月から 2007 年 3 月末において、注意喚起を行ったユーザ数は 7,916、駆除ツールのダウンロードを行ったユーザ数は 1,861 であった。

なお、注意喚起の実効度を検証するための注意喚起を 2 回実施しており、この結果を踏まえて本格的な運用を開始している。以下に、その詳細な結果を示す。

2.3.3.1 注意喚起事前検証の結果

第 1 回注意喚起検証は、2006 年 11 月 25 日～30 日の間にハニーポットで検知した攻撃事象に関して通信元を解析し、本プロジェクトの取り組みに参加する ISP のうち 7 社によって 12 月 15 日からユーザへの注意喚起を実施した。また、第 2 回注意喚起検証は 2007 年 1 月 6 日～11 日の間に検知した攻撃事象に対し、参加 ISP8 社によって 1 月 25 日からユーザへの注意喚起を実施した。注意喚起を行ったユーザ数、および駆除ツールのダウンロード数を下記に示す。また、注意喚起を受けた感染ユーザの駆除ツール配布 web サイトへの訪問率、駆除ツールダウンロード率、Windows Update へのリンク率、結果報告率を示す。

表 2.3.1 注意喚起事前検証での注意喚起ユーザ数と駆除ツールダウンロード数

	注意喚起ユーザ数	駆除ツールDL数
第1回注意喚起検証	105	31
第2回注意喚起検証	575	114

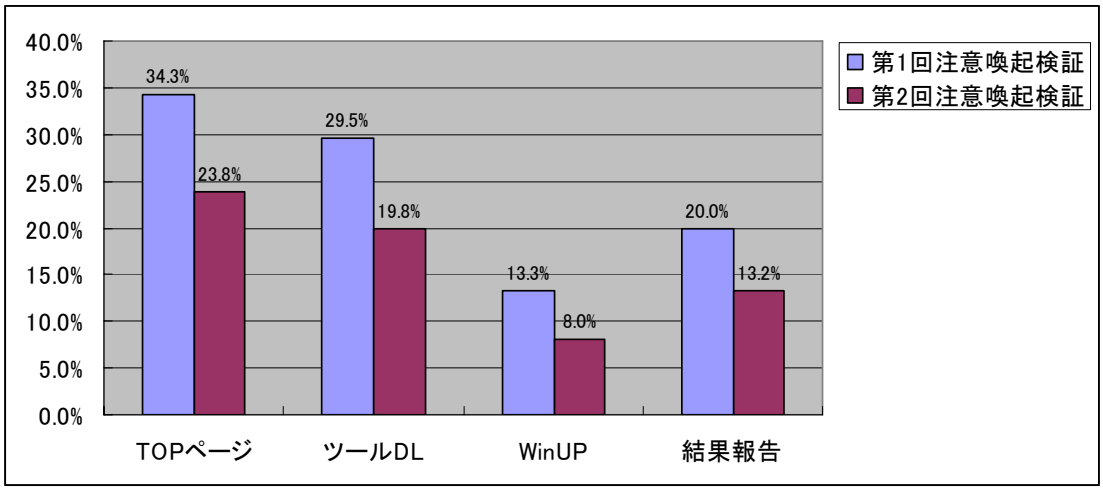

図 2.3.4　注意喚起事前検証における注意喚起実績

駆除ツール配布 web サイトの TOP ページへの訪問率は 3 割前後であった。この数字を向上させるためには、例えば注意喚起の業務サイクルにおいて、サイトにアクセスして来ないユーザに対し繰り返し通知を行うなど、ボット感染の事実を確実に認知させる対応が必要である。あわせて、ボット感染の事実をユーザが真摯に受け止め、インターネット初心者であっても容易に対策行動がとれるような工夫も重要と思われる。

web サイト訪問者の傾向としては第 1 回・第 2 回とも共通しており、駆除ツールのダウンロードまでは多くのサイト訪問者が実施しているにも関わらず、ダウンロード以降のページで紹介される再感染予防のための Windows Update や、サイトの末尾にて駆除結果を CCC に報告する「完了連絡」の実施については、実施していないユーザが相当数存在することが判明した。この点に関しては、web サイトの構成や文言の工夫などシステム本格稼動時の対策サイトの設計に反映している。

2.3.3.2 本格運用における注意喚起の結果

本格運用環境では、ハニーポット台数の増加等により攻撃事象の検知数が格段に向上し、駆除注意喚起対象ユーザが大幅に増加した。また、2 回の注意喚起検証によって得られた知見を元に、注意喚起メールの送信サイクルや駆除ツール配布 web サイトの更改を行った。

●注意喚起メール：メールを送信したにも関わらず、対策サイト上の「完了連絡」まで実施しないユーザに対して、複数回の注意喚起を実施。

●対策サイト：ボット駆除手順の説明ページ等を、ユーザにわかりやすい平易な表現に更改。また感染ユーザが訪問した際、ハニーポットにどのような通信を行ったかが確認できる機能を実装。

本格運用では、2007 年 2 月 5 日よりハニーポットで検知された攻撃事象を対象とし、2 月 19 日より ISP による注意喚起メールの送信を開始した。本格運用開始から 2007 年 3 月末までに注意喚起を行ったユーザ数、および駆除ツールのダウンロード数を下記に示す。

表 2.3.2　本格運用における注意喚起ユーザ数と駆除ツールダウンロード数

	注意喚起ユーザ数	駆除ツールDL数
本格運用 （2007年2月19日～3月末）	7236	1716

本格運用では、事前検証時に比べ約 10 倍の対応数を実現している。

また、駆除ツール配布 web サイトへの訪問率の遷移を下記に示す。
なお、2007 年 2 月 19 日からの注意喚起開始後、3 月 1 日の時点で注意喚起ユーザ数とサイトへの訪問数を集計して訪問率を算出し、約 1 週間毎に、注意喚起ユーザ数の増分とサイト訪問数の増分から訪問率を算出している。

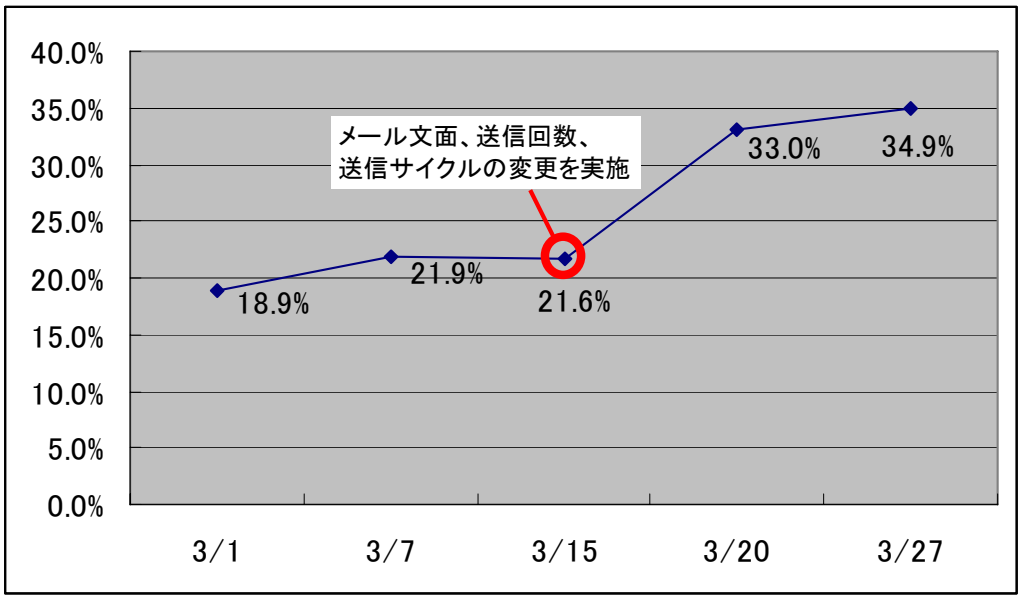

図 2.3.5 駆除ツール配布 web サイト訪問率の遷移

最初に集計を行った時点では、ページ訪問率が 2 割弱にとどまり事前検証での成果を下回っていた。各 ISP での注意喚起の実施状況について確認を行ったところ、注意喚起メールの文面について各社各様であり、また送信サイクル（メールを送信しても対応しないユーザに対し再送信する間隔）に関しては多くの ISP が一週間で運用している一方で、訪問率の高かった ISP は 3 日間で運用していた。よってサイト訪問率向上のため、訪問率の高い ISP に倣った運用を他の ISP においても実施することとし、文面に関してもユーザに対してより訴求

力のある内容を検討し、更改した。その結果訪問率は向上し、事前検証を上回る成果を得ることができている。

次に、駆除ツール配布 web サイトへの訪問率、駆除ツールダウンロード率、Windows Update へのリンク率、結果報告率を示す。

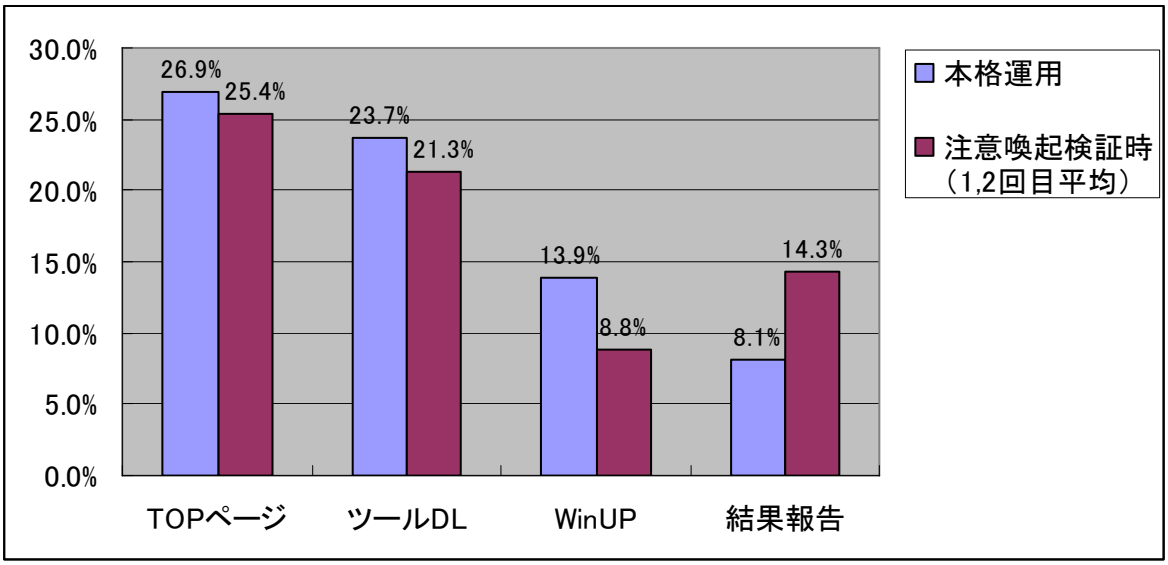

図 2.3.6 本格運用における注意喚起実績

注意喚起事前検証時のサイト構成は、駆除ツールのダウンロード、Windows Update、結果報告の手順が 1 つのページで説明されており、Windows Update へのアクセス率が伸び悩んでいる（駆除ツールのダウンロードの後、Windows Update は行わないまま結果報告している）要因になっていることが想定された。そこで本格運用では、それぞれの手順説明が分離され、駆除ツールダウンロード→Windows Update →結果報告、と段階的に手順を踏むような構成へ更改した結果、Windows Update への誘導には大きな効果があがっている。一方、結果報告率が悪くなっているが、これは、Windows Update に長時間を要したり、リブートが必要となるため、その時点でユーザ自身が対応を終結したケースが多かったものと思われる。

また、本プロジェクトにおいては、具体的な駆除ツール提供、詳細な手順の説明は web サイトにてわかりやすく提供し、感染ユーザに対するメールではボット感染の通知とサイトへの誘導に限定している。これは、ツール配布や手順説明までをメールで通知するような従来型のアプローチ手法では、ユーザの理解度があがらず ISP のカスタマセンターに多くの問い合わせが発生してしまう懸念があったためである。具体的数値による成果は目に見えないが、参加 ISP にヒアリングを行ったところ、従来手法にくらべて格段にユーザ問い合わせが少なかった感覚があると評価された。

2.3.4　今後の展開

（１）注意喚起範囲の拡大

2007 年 3 月末の時点でボット駆除が実施されたユーザの数は、ボット感染者全体のうちまだほんの一部であり、注意喚起の範囲を拡大していくことは重要な課題である。ボットは近接する IP アドレスに対して感染活動を行うことから、これまで取得していない IP アドレスレンジを保持する ISP との協力や、小規模な ISP に対するソリューションを検討していく必要がある。また、現在通信元を解析できていない感染活動や、感染活動の初期的な挙動として exploit コードを送信してくる通信元に対して注意喚起を行うための検討なども行い、注意喚起の面的な拡大を図る必要がある。

（２）駆除ツール配布 web サイト訪問率の向上とサイト構成の更改

サイトの TOP ページ訪問率は最終的には 35%程度となっているが、まだ向上の余地が残されている。まず、ユーザ心理としてメールに記載された URL をクリックすることには抵抗がある（フィッシングに類似している）という懸念もあり、こういったユーザが安心してサイトを訪問できるよう、本プロジェクトが行っている手法自体の認知度を高めるなどの努力が必要である。

また、サイトを訪問したユーザを、駆除ツールのダウンロード以降の手順（再感染防止のためのインターネット環境の確認や対処完了の連絡）に誘導できていない点については、サイトの構成を再検討し、駆除ツールのダウンロードだけで手順が終わりではないことをユーザに理解してもらえるよう対処していく必要がある。

（３）感染・再感染予防に関する意識向上への貢献

感染したボットを駆除ツールによって駆除したユーザが、再度別のボットに感染してハニーポットに検知され、再び注意喚起メールが送信されるユーザが約半数（本格運用）にのぼっている。これは、グローバル IP アドレスを PC にて直接終端しているなどインターネット接続環境が貧弱であったり、脆弱性のある OS を利用し続けていることが原因であろうと想像される。駆除ツール配布 web サイトのコンテンツでは、これらへの対策として、ブロードバンドルータの使用や、Windows Update の実施を強く呼びかけているが、再感染のみならずボット感染自体の拡大抑止のためにも、他の組織やメディア等とも連携したユーザ啓蒙活動を推進していく必要がある。

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、ボット対策システム運用グループが捕獲したボット（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を使用して詳細な解析を実施する。

また、感染予防対策ベンダとして参加しているセキュリティベンダなどへ、捕獲されたボットを提供するシステムを運用している。

3.2 解析

解析にあたっては、以下の 2 種類の解析を実施している。

・簡易解析：既存の駆除ツールにおいて未対応の検体について、種類、感染に関するファイル情報等を調査し、駆除ツールを作成する

・詳細解析：簡易解析の結果、影響度の大きいもの、ボットの傾向分析や今後の解析手法に関与しそうな検体について、ボットが使用する脆弱性や振る舞い、利用されている技術などについて静的解析を実施する

3.2.1 簡易解析、詳細解析の処理フロー

3.2.1.1 簡易解析のフロー

本作業は、毎日行われる簡易解析、駆除ツール対応リスト作成の作業、および、週に一回実施される駆除ツール作成の二つの工程に分けられる。

1) 毎日行われる作業（簡易解析）

1-1) 対応リストの作成

(i) 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。

(ii) クライテリアにより簡易解析を行う検体を抽出する。

クライテリアは以下の基準で設定される。

① アンチウイルスソフト(駆除ツール開発事業者のアンチウイルソフト、および、他 2 社のアンチウイルスソフト)で未知の検体

② 駆除ツール開発事業者のアンチウイルスソフトで未知の検体(他 2 社のアンチウイルスソフトでは既知でも可)

③ 攻撃回数が多い検体

(iii) 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。

(iv) ボットプログラム解析グループより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。

1-2) ボット感染予防推進グループへの抽出された検体の提供

2) 週に一回行われる作業（駆除ツールの作成）

(i) 毎週月曜日までに捕獲した検体について、簡易解析、駆除ツールの作成を水曜日までに実施する。

(ii) 駆除ツールを水曜日の午後、ボット対策システム運用グループへ提供する。

(iii) ボット対策システム運用グループは、取得した駆除ツールを毎週水曜日に感染者が属する ISP に対して配付可能な状況にするとともに、サイバークリーンセンターのサイト上にて公開し、駆除ツールを提供する。

(iv) ISP は毎週木曜日以降に感染者にボットの駆除依頼のメールを送付する。

図 3.2.1に簡易解析、駆除ツールの作成、およびボット感染予防推進グループへのボットの提供に関する処理フローを示す。

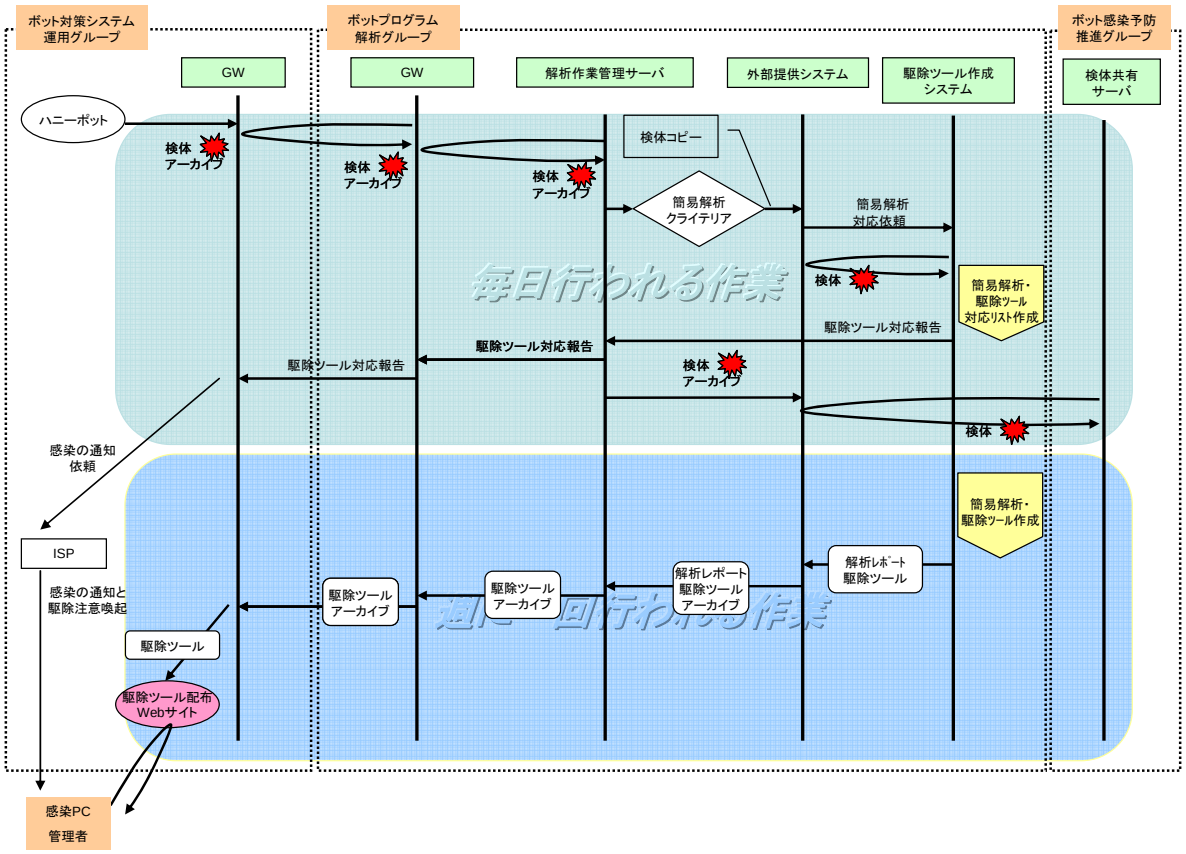

図 3.2.1　簡易解析の処理フロー

3.2.1.2 詳細解析のフロー

(i) 捕獲したボットのうち、詳細解析を行う検体を抽出する。

(ii) 抽出されたボット検体についてボットプログラム解析グループ、および駆除ツール開発事業者において詳細解析を実施する。

本処理は、不定期に実施する。

3.3 静的解析

3.3.1 静的解析に関する研究

静的解析（static analysis）とは、リバース・エンジニアリング（あるいはリバース・コード・エンジニアリング）によって調査対象プログラムの構造や仕様を分析することである。逆アセンブルしたプログラムコードをすべてチェックすることができるので、完全な挙動を把握することや、マルウェアが使うさまざまなテクニックを知ることができる。しかし、膨大な量のアセンブリ言語を解読しなければならないため、作業時間が掛かるというデメリットがある。また、逆アセンブルしたプログラムコードを分析するためには相当な経験が必要であり、OS やネットワーク、プログラミング言語など幅広い知識が不可欠となるが、現在のところ、静的解析に確立された手法はなく、エンジニアが試行錯誤しながらそれぞれ効率的な方法を発見しているのが現状である。静的解析を自動化するといった試みもあるが、完全に自動化し、成功している例はまだない。技術的に解決しなければならない点も多く、すぐに自動化された静的解析を実現するというのは難しそうである。複雑に進化するマルウェアに対抗するためには、今後も静的解析に関する研究は継続し、新しい効率的な手法を検討していかなければならない。

3.3.2 ボットの傾向分析

3.3.2.1 背景と目的

セキュリティ対策において、攻撃側の手口を知ることは重要である。すでに最初のボットが登場してから数年経過しているが、その間、ボットの感染、攻撃、隠蔽技術などのテクニックは変化し、より高度で複雑なボットに進化してきている。攻撃側の最新のテクニックを知らなければ、的外れな対策をしてしまう可能性が十分にある。

例えば、IRC 通信以外でコマンドを送受信するようなボットがあった場合、IRC 通信を遮断するといった対策は意味がないということである。

ボットの最新の手口を知るには、ネットワークのトラフィックを解析したり、ボットのプログラムを解析したりといった方法が考えられる。本調査では、ボットを静的解析手法で分析した。

3.3.2.2 傾向分析結果

同名や同ファミリとして重複せず、なるべく機能が異なる 20 検体のボットを静的解析したところ、以下のようなことが分かった。

1) 共通エンジン

完全に異なる機能を持つボットであっても、根幹部分は同じものを利用している場合があると考えられる。これは，ボットのソースコードがインターネット上で公開されているからだろう。更に多くのボットを静的解析して結論を出す必要があるが、多くのボットは共通エンジンを利用し、そこにさまざまな機能をアドオンさせていると思われる。現在，大量のボットが流通しているが，根幹部分が共通のものかどうかで分類すると，数種類に分類される可能性がある。

2) ボットコマンド

ボットには、ログインやログアウトするもの、IRC サーバへ接続するもの、ターゲットへ偵察するものや攻撃するもの等、非常に多くのコマンドが用意されている。

3) 脆弱性

以下の脆弱性等がボットで利用されていた。

- ユニバーサル プラグ アンド プレイ（UPnP）に含まれる未チェックのバッファによりシステムが侵害される（MS01-059）
- RPC インタフェースのバッファオーバーランによりコードが実行される（MS03-026）
- プラグ・アンド・プレイ・サービスの未チェック・バッファの脆弱性により、リモートで任意のコードが実行される危険性（MS05-039）
- pipe¥epmapper を使用した DCOMRPC の攻撃

4) パッカー

インターネット上には非常に多くのパッカーが存在しているが、ボットに利用されるのは約 15 種類程度である。

5) 難読化

API の改変による難読化を行うものが存在する。

6) アンパック・テクニック

アンパック・ルーチンで使われているアンチデバッギング手法がいくつか存在した。オフセット 0 での無効なメモリアクセスはその一つであり、最近のパッカーでは、比較的多く使われる手法である。

7) 変種として偽装

最近のボットを含むマルウェアでは、ハッシュ値の変化から定期的にコード改変が行なわれている可能性が疑われる。しかし、その一部のマルウェアには実際にコード改変機能が無いとの報告もある。アンチウイルスソフトでの検知を回避するため、変種を装うことで解析側の負荷を高めることを意図している可能性がある。

8) ボットのコンポーネント化

最近のボットを含むマルウェアでは、単機能または機能毎にコンポーネント化され、インターネットからダウンロードし、感染させる動作を行うものが増加しているという報告がある。

このようなマルウェアは、「DOWNLOADER (ダウンローダー)」と呼ばれている。１つの DOWNLOADER で複数のマルウェアを感染させることができる。また、機能拡張や変更・修正を加えることができる。そして、全容を把握することを困難にしてマルウェアが完全に駆除されることを回避させていると考えられる。一部のコンポーネントのみが駆除されても DOWNLOADER が残存している場合、再度感染する可能性がある。

3.4 今後の展開

2006 年度は、プロジェクト推進のための分析能力の強化と、解析作業の作成スキームの確立を目指して業務を遂行した。スキームの確立については当初想定していた範囲では達成することができたが、実施に伴って表面化する課題や時間経過とともに変化する事象への対応は継続的に発生している。本事業には、ボットの捕獲から駆除ツールの適用という大きな流れがあり、この部分の運用の安定化は必須である。

そのため、2007 年度は現行スキームの運用の安定性向上をまず優先し、事象の変化に追従してスキームや駆除ツールをチューニングできる体制を整えてゆくことを目指す。また、詳細解析に関しては、個々のボットの解析のみならず、より長い時間軸を持った傾向分析や解析技術の研究にも注力する。

なお、2006 年度末で駆除ツールのチューニングや機能拡張について下記のような必要性を認識している。これらは 2007 年度での実現を目指している。

(i) 駆除ツールの有効期限の設定機能の追加
(ii) 検体の種類に応じた標準検索モードの設定機能の追加
(iii) 駆除結果のトラッキング機能の追加
(iv) Rootkit への対応
(v) 駆除ツールの対応プラットフォームの拡充

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アンチウイルスソフトのパターンファイルに反映させることとする。これにより、ユーザがアンチウイルスソフトのパターンファイルを最新のものに更新すれば、ユーザのアンチウイルス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図ることになる。

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、我が国でアンチウイルスソフトの供給・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 等における感染予防を推進していく活動を行っている。

参加感染予防対策ベンダ一覧

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

4.3 活動成果

感染予防対策ベンダが 2007 年 3 月末までに、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アンチウイルスソフトへ反映した状況について、各ベンダ平均の数値を以下に示す。

表 4.1.1 各社対応状況

ボットプログラム解析グループより検体提供を受け、新しく感染予防対策ベンダが今回自社のパターンファイルに反映したもの	４８．２％
同種の検体について、ボットプログラム解析グループより検体提供を受ける前から既に感染予防対策ベンダが自社のパターンファイルで対応していたもの	４９．４％
パターンファイルに取り込まなかったもの	２．４％

1) 2006 年 12 月～2007 年 3 月までに本プロジェクトで提供した検体数の合計を「100%」として計算している。

2) 今回、新しく感染予防対策ベンダのパターンファイルに取り込んだものが各ベンダ平均 48.2%となっており、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、今回新たに登録された検体 48.2%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アンチウイルスソフトのパターンファイルへの一層の反映を推進すべく、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

2006 年 12 月より開始したボットネット対策プロジェクトは、総務省、経済産業省および関連組織、企業が連携して国内ボット感染者の撲滅を目指して取り組むというわが国初の試みであり、世界的に見ても稀有な事例といえる。本プロジェクトの取り組みにより、数多くのボット感染者に注意喚起を行い、ボットの駆除が行われ、その取り組みや成果が多くのメディアに取り上げられることにより認知度が上がってきたことは、本プロジェクトが一定の成果を上げ、その意義が広く理解されてきているといえる。とはいえ、ボットの感染者数は依然として多く、よりいっそう多くの感染者に注意喚起を行い、ボットの駆除につなげていく工夫が必要である。また、ボットによる脅威は日々進化しており、これらの脅威に対峙するための技術革新も必要となる。さらにはボットの脅威は国内のみならず海外にも存在するため、海外の関係機関との連携も視野に入れた活動の展開を検討する必要がある。本プロジェクトでは、今後も継続的に活動を行い、安心・安全なインターネット社会の実現に向け、寄与していくことを目指したい。