平成20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 本プロジェクトの目的 1
1.1 ボットネットの現状 1
1.2 サイバークリーンセンター（CCC）の概要 3
2 ボット対策システム運用グループ活動報告 7
2.1 概要 7
2.1.1 検体収集解析 8
2.1.2 注意喚起 8
2.2 活動状況・成果 8
2.2.1 検体収集・解析 9
2.2.2 注意喚起 13
2.3 今後の展開 16
3 ボットプログラム解析グループ活動報告 17
3.1 概要 17
3.1.1 検体解析数と駆除ツール反映数に関する指標 17
3.2 駆除ツールの作成 18
3.2.1 駆除ツールの機能追加 18
3.2.2 検出状況の分析 19
3.3 ボット分析 26
3.3.1 バージョンアップによる検体の変化の分析 26
3.3.2 同一サイトから配布される検体の変化の分析 30
3.3.3 特徴を持つ検体の詳細解析結果の分析 32
3.4 今後の展開 34
4 ボット感染予防推進グループ活動報告 35
4.1 概要 35
4.2 感染予防対策ベンダ 35
4.3 活動成果 36
4.4 今後の活動 36
5 まとめ 37
6 さいごに 38

1 本プロジェクトの目的

インターネットの利用が広く一般に普及する中、Malware による被害が増加している。これらの Malware はインターネット上で感染活動を繰り返していることから、何らかの対策がされなければインターネット利用者は危険な状態に置かれている。Malware は悪意のある様々なソフトウエアの総称であるが、一般的には、ウイルス、トロイの木馬、スパイウエア、ボットなどに分類される。Malware の中でもボットは、一度感染してしまうとボットネットといわれる巨大なネットワークを形成し、Herder（羊飼い）により知らぬ間に遠隔で操作され、DDoS 攻撃やスパムメール、フィッシングなど、様々な犯罪行為に利用されている。ボットの感染手口は巧妙になってきており、かつてのウイルスが感染後にパソコンの画面に花火を表示したりハードディスクのファイルを消去したりと愉快犯的な活動をするのに対し、ボットはユーザに気づかれないようひそかに感染活動を行う特徴がある。ボットには、ウイルス対策ソフトに検知・駆除されないように多くの亜種を持つ、あるいは、一度感染するとウイルス対策ソフトを更新させないなど、様々な工夫がされており、ユーザが自ら対策を行うことが難しくなってきている。そのため、ボット対策をユーザ自らの対策だけに委ねるのではなく、国が主導し ISP やセキュリティベンダ、セキュリティ関連機関等と連携したボット対策を推進することが重要となってきている。

「サイバークリーンセンター（以下 CCC）」は、こうした背景のもと、国内ボット感染ユーザを限りなくゼロにする取り組みとして、平成 18 年度から総務省・経済産業省連携プロジェクトとして開始され、ISP と連携した注意喚起活動によるボット対策を進めている。

本書は、平成 20 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 Herder 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、Herder 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、特定サイトへの DDoS 攻撃などの犯罪行為に利用されることから、インターネット利用者の安全を脅かす、大きな脅威となっている。このように、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、単に「被害者」であるのみならず「加害者」にもなっている。

ボットは、2002 年頃には既に確認（トレンドマイクロでは、AGOBOT を 2002 年の後半に情報公開）されていたが、2004 年頃からその感染が顕著になってきた。2005 年 6 月に Telecom-ISAC Japan と JPCERT/CC が行った調査では、国内ブロードバンドユーザ約 2,000 万人*のうち約 40-50 万人（感染率約 2-2.5%）が感染していると推計してい

る。CCC が 2008 年 6 月に国内ボット感染者数を調査したところ、ブロードバンドユーザ約 3,000 万人*のうち約 30 万人（感染率約 1%）と推計した。(*総務省統計データ「ブロードバンドサービス等の契約数の推移」から推計)

ボット感染率が低下している理由としては、CCC によるボット対策が大きく寄与していることが考えられるが、その他の要因としてウイルス対策ソフトの普及、よりセキュアな OS への移行、ブロードバンドルータの導入など環境的な要因も考えられる。

国内のボット感染率が諸外国と比べて非常に低いことは、マイクロソフトの「PC 1000 台あたりの Malware 感染 PC 数分布図」で報告されている。これは、CCC によるボット対策の活動が一助になっているのではないかと推測される。

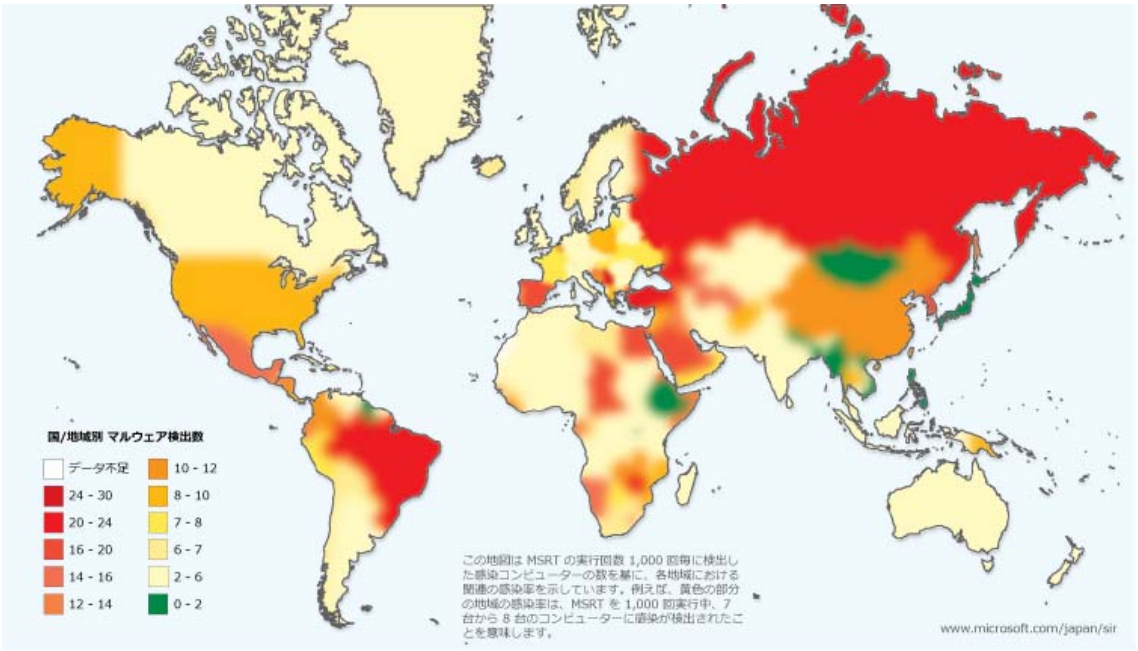

図 1.1-1　PC 1000 台あたりの Malware 感染 PC 数分布図

（出典：http://www.microsoft.com/japan/security/contents/sir.mspx）

1.2 サイバークリーンセンター（CCC）の概要

CCC では、国内のボットの感染ユーザ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 1.2-1 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。

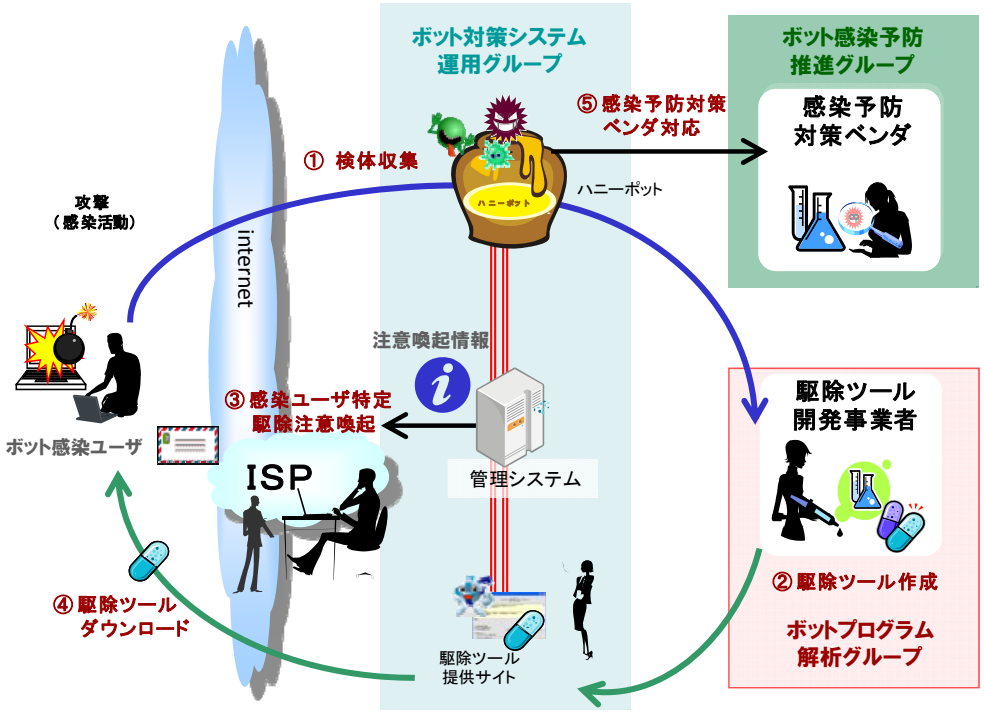

図 1.2-1　CCC 活動概要

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。（ボット対策システム運用グループ）
② 駆除ツール作成	収集されたボット検体を解析して“駆除ツール”を作成する。（ボットプログラム解析グループ）
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。（ボット対策システム運用グループ）
④ 駆除ツールダウンロード	注意喚起メールを受け取った感染ユーザが、メールで指定された駆除ツール提供サイトにアクセスし、駆除ツールをダウンロードする。（ボット対策システム運用グループ）
⑤ 感染予防対策ベンダ対応	各感染予防対策ベンダにボット検体を提供し、各ベンダは対策ソフトのパターンファイルに反映する。（ボット感染予防推進グループ）

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 1.2-2　CCC 運営体制

【ボット対策システム運用グループ】（Telecom-ISAC Japan）

ボット対策システム運用グループでは、ハニーポットなどの検体収集解析システムや注意喚起システムなど、本プロジェクト基幹システムを運用し、ボットの収集解析やプロジェクト参加 ISP によるボット感染ユーザへの注意喚起などを行っている。収集されたボット検体はボットプログラム解析グループに渡され、駆除ツールのパターンファイルに反映されるほか、ボット感染予防推進グループ経由で、国内主要感染予防対策ベンダに引き渡され、各種ウイルス対策ソフトのパターンファイルへの反映に寄与している。

さらにボット対策システム運用グループでは、ボットの新たな脅威に対応し、効果的な対策を進めるため、セキュリティベンダ等と連携し、Malware の最新動向調査を行っている。

＜プロジェクト参加 ISP＞ 平成 21 年 3 月末時点

株式会社インターネットイニシアティブ（IIJ）、NEC ビッグローブ株式会社（BIGLOBE）、NTT コミュニケーションズ株式会社（OCN）、KDDI 株式会社　（au one

net)、ニフティ株式会社（@nifty)、株式会社ハイホー（hi-ho)、ソフトバンクテレコム株式会社（ODN)、ソフトバンク BB 株式会社（Yahoo! BB)、株式会社アイエムエス・ドット・ジェーピー（インターネット MAGMA)、株式会社 IC-NET（IC-NET)、アイテック阪急阪神株式会社（ガオネット，tigers-net.com，BaycomNet，bai サービス)、株式会社朝日ネット(ASAHI ネット)、株式会社テクノロジーネットワークス （@NetHome)、株式会社インターリンク（ZOOT)、インターネット・プロ東海株式会社（ipc 東海インターネットサービス)、株式会社ヴェクタント （VECTANT)、株式会社 STNet(PIKARA, NETWAVE)、株式会社エヌ・ティ・ティ エムイー （WAKWAK)、株式会社 NTT データ三洋システム (SANNET)、株式会社エヌ･ティ･ティ ドコモ (mopera／mopera U)、株式会社エヌ・ティ・ティピー・シーコミュニケーションズ（InfoSphere)、NTT メディアサプライ株式会社 （DoCANVAS，ぽっけ，BB-WEST，スルガ，Wellith，SUISUI，MAST-BB)、株式会社エヌディエス （TikiTiki インターネット)、株式会社エネルギア・コミュニケーションズ（メガ・エッグ，アーバンインターネット)、エルシーブイ株式会社 （LCV-Net)、河口湖有線テレビ放送有限会社 （LCNet)、関西マルチメディアサービス株式会社（ZAQ)、株式会社キャッチネットワーク（KATCH ケーブルインターネットサービス)、近鉄ケーブルネットワーク株式会社（KCN-Net)、株式会社グッドコミュニケーションズ（SYNAPSE（シナプス))、熊本ケーブルネットワーク株式会社（JCN 熊本）(KCN インターネットサービス)、群馬インターネット株式会社（群馬インターネット)、KMN 株式会社 （ROSENET，MediaCat)、株式会社ケイ・オプティコム(eo)、KCN 京都(KCN 京都インターネット)、株式会社ケー･アイ･ピー(KIP-Internet)、株式会社ケーブルテレビ山形(CATVY インターネット)、株式会社ケーブルワン （ケーブルインターネット)、株式会社ザ・トーカイ（TOKAI ネットワーククラブ)、株式会社サンライズシステムズ（両毛インターネット)、株式会社 JWAY（ケーブルインターネット)、湘南ケーブルネットワーク株式会社(エスシーエヌネットワークサービス)、白露カンパニー株式会社（DAC システム)、仙台 CATV 株式会社（CAT-V NET)、高岡ケーブルネットワーク株式会社（高岡ケーブルネットワーク インターネット接続サービス)、中部テレコミュニケーション株式会社（Commuf@（コミュファ))、株式会社つなぐネットコミュニケーションズ（e-mansion)、株式会社ティエイエムインターネットサービス (TAM インターネットサービス, Net3 インターネット)、株式会社デオデオ (デオデオエンジョイネット)、株式会社テレコムわかやま（aikis)、株式会社電算（avis)、東京ケーブルネットワーク株式会社（TCN ケーブル NET)、トナミ運輸株式会社 （コーラルネット)、となみ衛星通信テレビ株式会社（TSTnet)、株式会社ドリーム・トレイン・インターネット（DTI、サイラスネット，ブロードスター，isao.net)、株式会社長崎ケーブルメディア （NCM ケーブルインターネットサービス)、株式会社長野県共同電算（JANIS)、株式会社グローバルネットコア（N-plus)、能越ケーブルネット株式会社（能越ネット)、パークネット株式会社（ParkNet)、飯能ケーブルテレビ株式会社（@はんのう)、ひまわりネットワーク株式会社（Aitainet（アイタイネット))、株式会社ファミリーネット・ジャパン（サイバーホーム)、株式会社ブイ・アール・テクノセンタ

ー（VRTC ネット）、株式会社富士通ソフトウエアテクノロジーズ　（Web しずおか）、株式会社富士通長野システムエンジニアリング（Infovalley（インフォバレー））、フュージョン・ネットワークサービス株式会社　（FUSION GOL）、株式会社 NTT ぷらら（Plala）、株式会社ふれあいチャンネル（愛・ネット）、三重データ通信株式会社（三重インターネットサービス）、ミクスネットワーク株式会社（ミクスインターネット）、株式会社ミライコミュニケーションネットワーク（ミライネット）、株式会社メディアッティ・コミュニケーションズ（Mediatti NET）、山口ケーブルビジョン株式会社（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）

ボットプログラム解析グループでは、ボット対策システム運用グループで収集されたボット検体の特徴や技術の解析を行い、駆除ツール開発事業者と連携して、駆除ツールを作成している。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）

ボット感染予防推進グループでは、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している。

＜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、国内ボット感染ユーザを限りなくゼロにすることを目的に、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（ボットの感染活動）を検知し、ボット検体を収集している。収集したボット検体は、ウイルス対策ソフトによる既知未知解析や実際の動きを観察する動的解析を行っている。こうして収集したボット検体はボットプログラム解析グループへ引き渡し、ボットプログラム解析グループにより駆除ツールが作成される。

注意喚起フェーズでは、ボット感染ユーザからの攻撃事象をもとにボット感染ユーザが利用している ISP を特定し、該当 ISP へその攻撃事象に関する情報を渡し、ISP ではその情報をもとにユーザを特定し、ISP からボット感染ユーザに対してボット感染事実を伝える注意喚起メールを送信している。注意喚起メールを受け取った感染ユーザは、メールの指示に従い、ボット対策システム運用グループが運用している駆除ツール提供サイトにアクセスし、ボット対策を行っている。駆除ツール提供サイトには、ボットプログラム解析グループにより作成された駆除ツールをダウンロードできるほか、WindowsUpdate やウイルス対策ソフトの導入、ブロードバンドルータの利用など、ボット対策に必要な様々な情報を提供している。これらのボット対策情報は、注意喚起を受けたボット感染ユーザ向けのみならず、一般ユーザ向けにも CCC 公式サイトを通じて提供している。

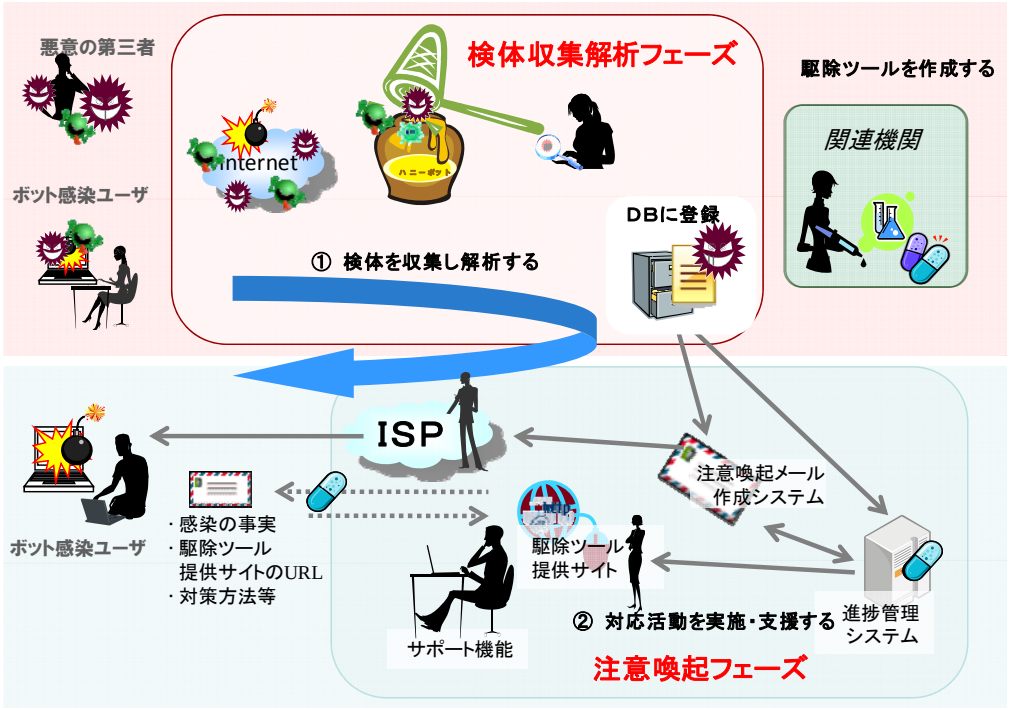

図 2.1-1 ボット対策システム運用グループ全体像

2.1.1 検体収集解析

CCC におけるボット対策の最初のステップとして、感染ユーザからの攻撃事象（ボットの感染活動）を検知し、ボット検体を収集解析することが重要である。そのため、ボット対策システム運用グループでは、ハニーポット（脆弱性を残したおとり端末）を用いたボット検体の収集活動を行っている。

収集されたボット検体には同一の検体や既にウイルス対策ソフトで対応できる検体も含まれる。そこでボット対策システム運用グループでは、まず重複した検体を整理（同定解析）する。次に同定された検体について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）で既にウイルス対策ソフトで対応済みかどうかを確認（既知未知解析）する。そして未知のものについては実際に動かしてみてボットであることを確認（動的解析）し、ボットプログラム解析グループに駆除ツールの作成を依頼している。

2.1.2 注意喚起

ボット対策システム運用グループでは、2.1.1 検体収集解析に示したボット検体の収集解析と同時に、ハニーポットで検知した攻撃事象（攻撃元 IP アドレスや時刻情報）をもとに、ボット感染ユーザへの注意喚起を行っている。注意喚起にあたり、攻撃元 IP アドレスから感染ユーザが利用している ISP を特定し、ISP 毎に攻撃事象情報を渡し、注意喚起依頼をしている。ISP では、ボット対策システム運用グループから渡された情報をもとに、感染ユーザを特定し、感染ユーザに対して、メールによる注意喚起を行っている。ボット対策システム運用グループでは、感染ユーザ毎に対策サイトのページを用意し、注意喚起メールを受け取った感染ユーザに対して、駆除ツールの配布や WindowsUpdate、ウイルス対策ソフトの導入、ブロードバンドルータの利用など、ボット対策を行う上で不可欠な情報を提供している。また感染ユーザ毎に対策サイトのページを用意することにより、感染ユーザがどこまで対策を実施しているか進捗状況を把握することを可能とし、ISP によるきめ細かなユーザサポートを行っている。

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、CCC 公式サイト（https://www.ccc.go.jp/）にて公開している。（図 2.2-1）

2009 年 3 月時点で、累計 13,534,588 体の検体を収集し、同定された検体は 870,277 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、22,871 体あった。注意喚起については、373,207 通のメールを 79,050 人に対して実施し、約 30%の感染ユーザが駆除ツールをダウンロードしている。

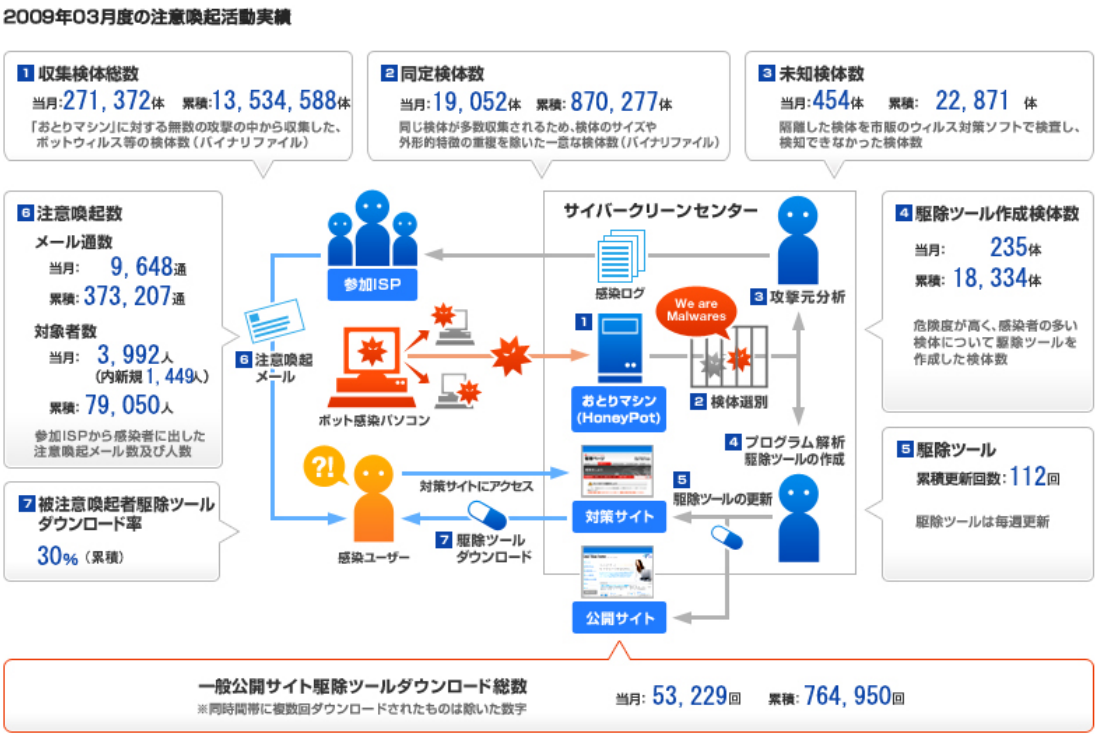

図 2.2-1　活動実績　2009 年 3 月度実績および 2007 年 2 月からの累積

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、2008 年 4 月～2009 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。

平成 20 年度の一月あたりの平均検体収集数は、約 49 万検体であった。この中には、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 2.2-2 に示す。

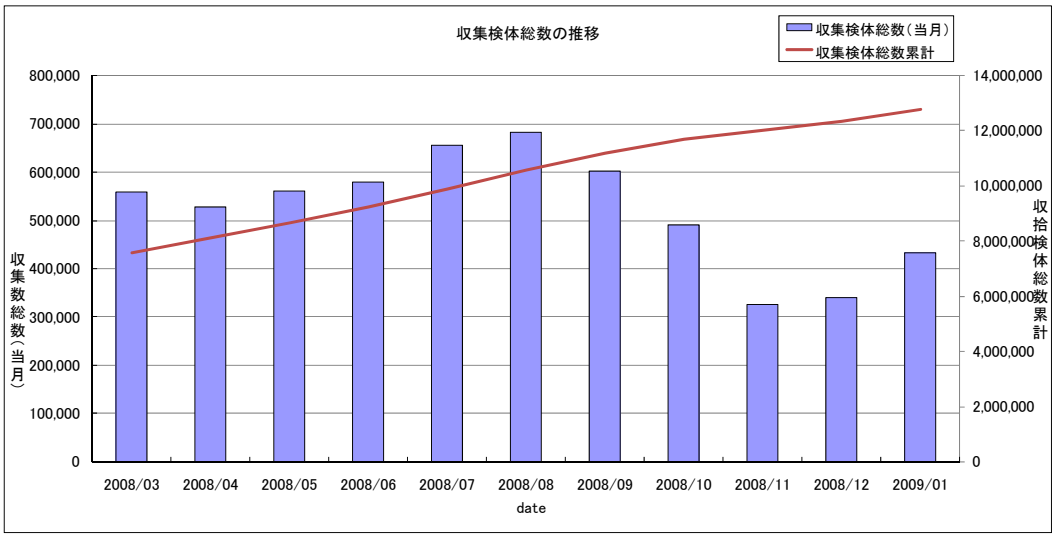

図 2.2-2 収集検体総数の推移

(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 5.5 万検体で、一日あたりに換算すると約 1,800 検体を収集している。

同定検体数の月毎の推移を、図 2.2-3 に示す。2008 年 7 月、8 月で同定検体数が増加しているが、これはシステムのプロセスで実行中の EXE ファイルおよび SCR ファイル（スクリーンセーバ）等に寄生感染するファイル感染型ウイルスの増殖により種類数が増加したためである。2008 年度下半期は、このファイル感染型ウイルスの減少により同定検体数が減少している。

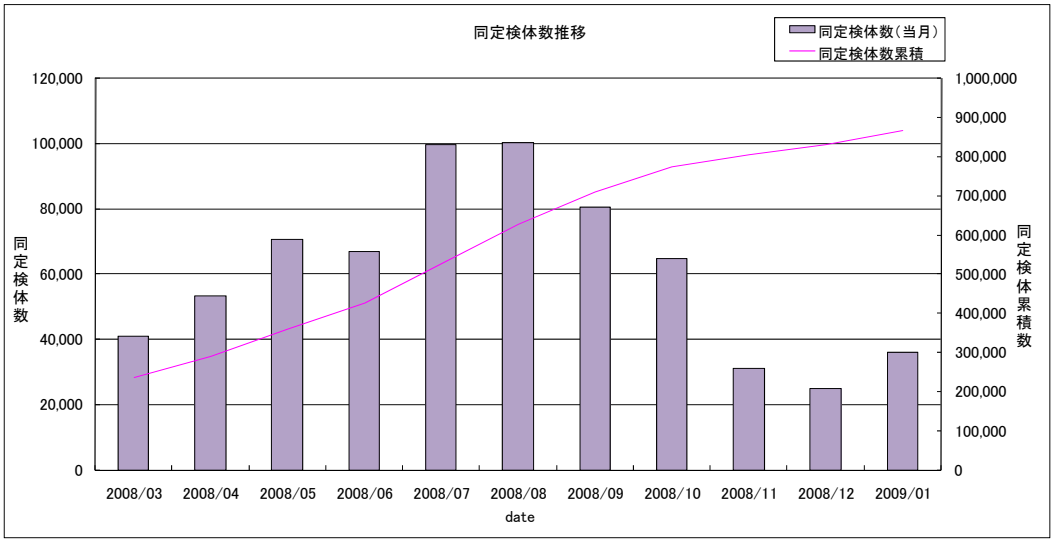

図 2.2-3 同定検体数の推移

(3) 同定検体数の既知未知の推移

同定検体を既知未知解析した結果の統計によると、一月あたり平均して約 5.5 万検体の同定検体のうち、約 5.4 万検体が既知、約 1,000 検体が未知であった。一日に換算すると未知検体を約 30 検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 2.2-4 に示す。未知同定検体数は、月毎にばらつきはあるが減少していることが分かる。

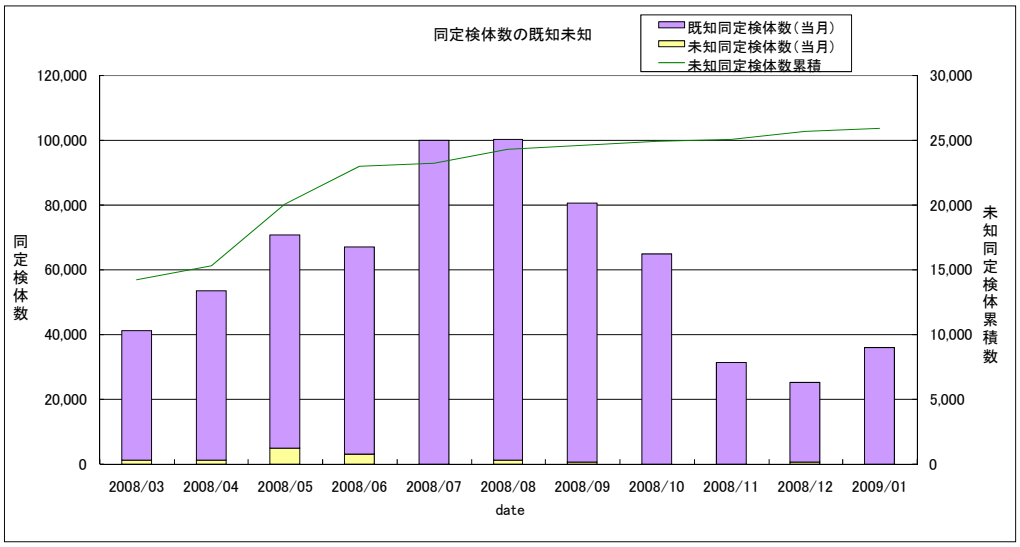

図 2.2-4 既知未知同定検体数の推移

収集した検体のトレンドに関して、年間の推移を、図 2.2-5 に示す。収集した検体で特徴的な動きを示したのが TSPY_KOLABC.CH で、2009 年 2 月に急増し 2009 年 3 月に激減している。これは 2008 年 12 月から 2009 年 2 月にかけて海外の特定サイトで大量配布されたことによる。2009 年 3 月に入り、その特定サイトからの配布が止まったことと連動して収集数も減少した。

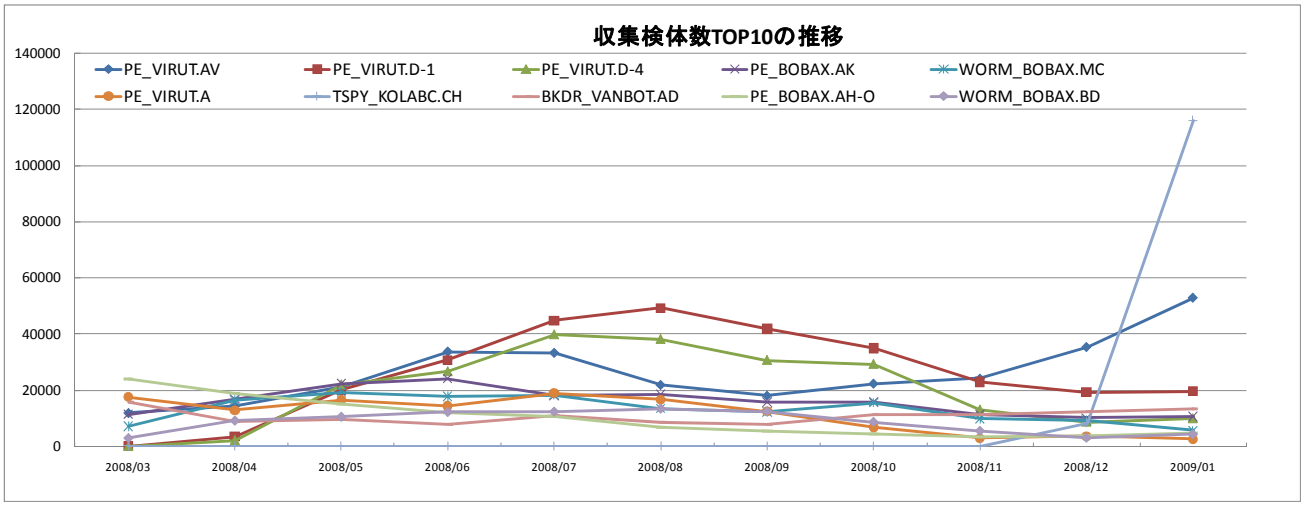

図 2.2-5 収集検体 Top10 の推移

(4) 特殊な環境下での検体収集

ボットの感染活動は、ネットワークを介し OS 等の脆弱性を狙った攻撃により感染、拡散が行われており、実際の攻撃に利用される通信ポートについては、特定ポートに集中する傾向がある。そのため、CCC ハニーポットの一部環境において、主要な通信ポートについて意図的に外部方向からの通信を遮断することで、感染抑止の対策となり得るか調査を行った。

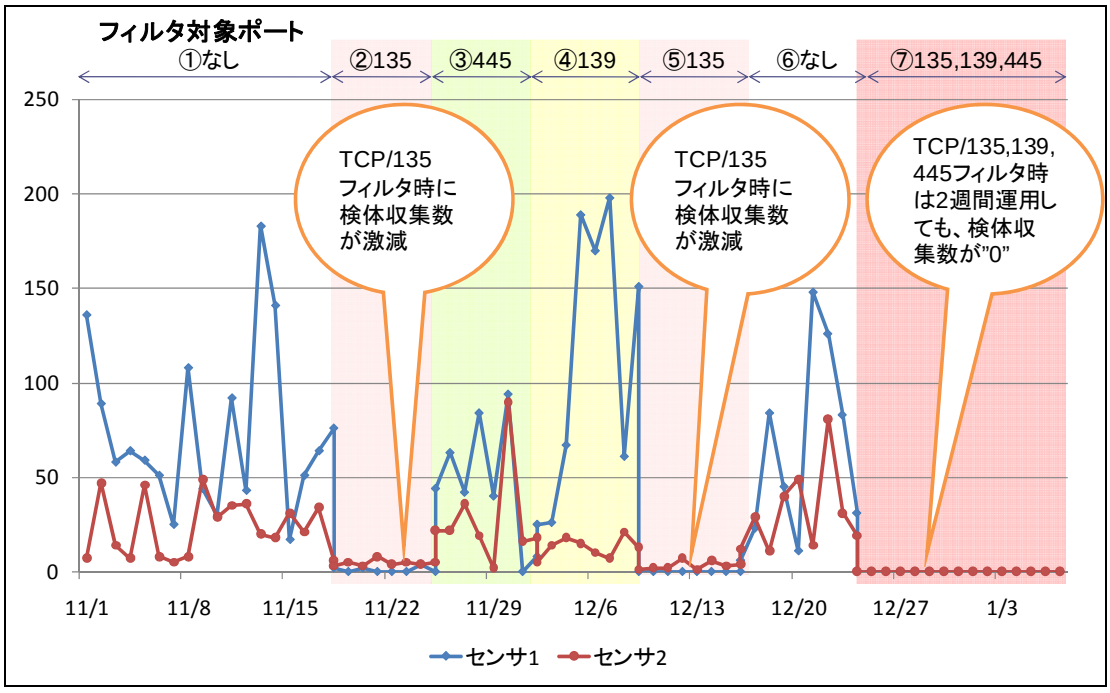

図 2.2-6 特定ポートをフィルタリングした場合の検体収集数推移

調査にあたっては 2 台のハニーポット（センサ 1、センサ 2）を用い、フィルタ条

件を変更しながら検体収集数の変化を観測したが、TCP/135 ポートのフィルタリング効果が最も大きく、さらに TCP/139、TCP/445 を加えた複数ポートフィルタリング時は、約 2 週間のハニーポット運用期間において検体収集数が 0 という結果が得られた。これは能動的に感染を広めるタイプのボットや Malware については、同様の対策を実施することで感染防止につながることを意味している。しかしながら、現在このような Malware に感染するユーザが後を絶たないのは、基本的な対策である WindowsUpdate の適用、ウイルス対策ソフトの導入、ブロードバンドルータの設置などが適切に実施されていない可能性が高いと考えられる。このような基本的な対策が実施できないユーザに対して、現状様々な課題はあるが将来的に ISP 等のネットワーク側でのフィルタリングやポートのブロック等が実現すれば、非常に大きな効果が望めるものと思われる。

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 20 年度に送信した注意喚起メールは 373,207 通、注意喚起したユーザ数は 79,050 人であった（図 2.2-1 参照）。平成 20 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 41%であり、WindowsUpdate 率が約 31%、駆除ツールダウンロード率が約 30%となっている。また、全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 2.2-7）

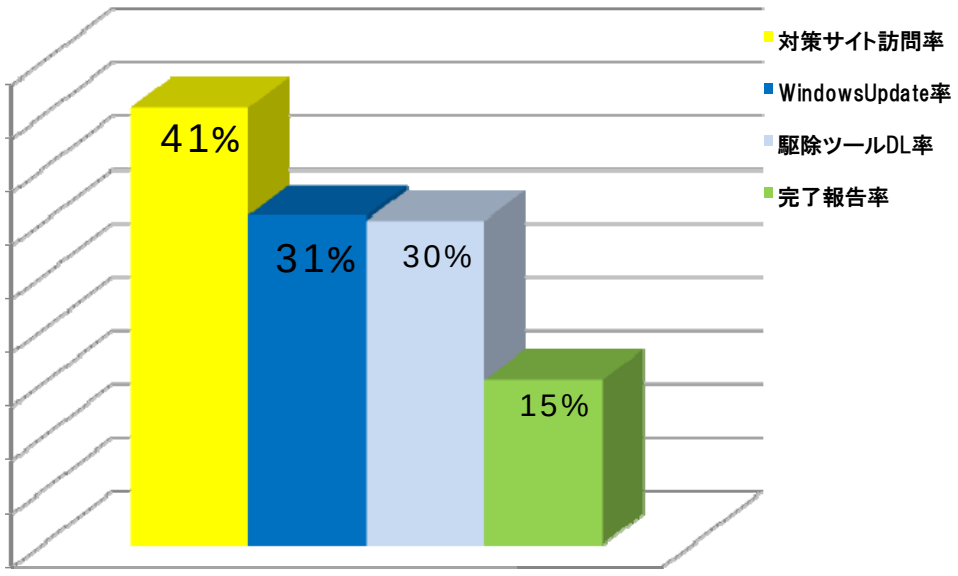

図 2.2-7 注意喚起に対するユーザの対応状況

(2) 効果

本プロジェクトにおける注意喚起効果の流れを図 2.2-8 に示す。2008 年 4 月から 2009 年 3 月までの注意喚起の状況で、総攻撃数（検体収集数）は 1,775,068 の攻撃を受け、注意喚起対象 IP アドレスは 206,896 であった。1,775,068 の攻撃元が 206,896 の IP アドレスであるのは、同一の IP アドレスから複数の攻撃を受けているためである。この 206,896 の IP アドレスをプロジェクト参加 ISP にてユーザを特定した結果、24,836 人が感染ユーザとして識別された。これらの感染ユーザに対し、プロジェクト参加 ISP では 97,935 回にわたり注意喚起を実施し、その結果 12,665 人が感染者対策サイトにアクセスし、7,664 人が駆除ツールをダウンロードしたことが分かった。

総攻撃数	1,775,068
↓	
注意喚起対象 IP アドレス	206,896
↓	
ユーザ識別数	24,836
↓	
注意喚起数（メール通数）	97,935
↓	
対策サイトアクセスユーザ数	12,665
↓	
駆除ツール DL 数	7,664

図 2.2-8 注意喚起成果

また、図 2.2-9 に新規注意喚起対象ユーザ数の月単位の遷移状況（2007 年 2 月～2009 年 3 月）を示しているが、ISP による注意喚起数が減少してきており、本プロジェクトにおける注意喚起活動の成果があらわれていると考えている。

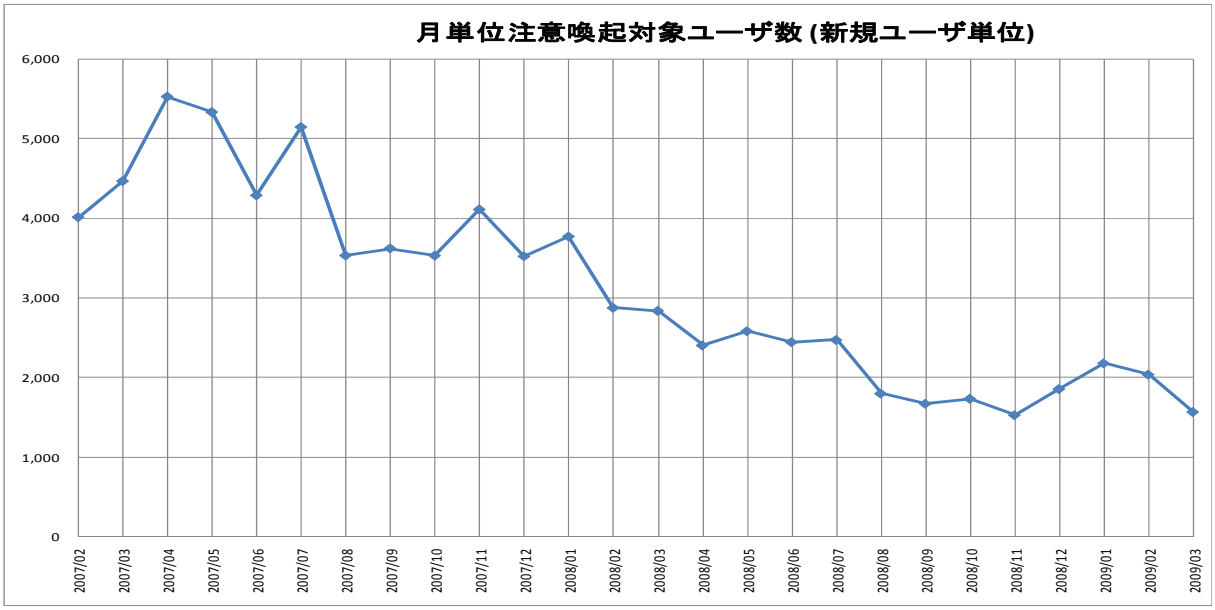

図 2.2-9 新規注意喚起対象ユーザ数遷移（2007/02～2009/03）

(3) その他の取り組み

平成 20 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、情報セキュリティの日*（平成 21 年 2 月）の関連行事として「ボット駆除活動キャンペーン」を実施した。「ボット駆除活動キャンペーン」は、プロジェクト参加 ISP のみならず、CEPTOAR-Council**準備会を通じて紹介いただいた業界各社（自治体、証券、電力、ガス、鉄道等）の Web サイトに CCC へのリンクを張ってもらう等、業界横断的な取り組みとなった。

（*http://www.nisc.go.jp/isd/index.html）

（**重要インフラ連絡協議会）

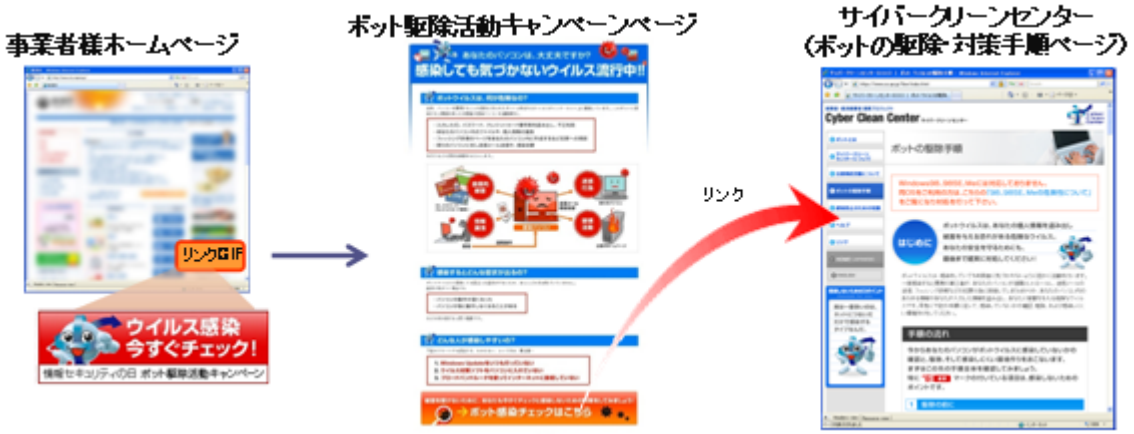

図 2.2-10　ボット駆除活動キャンペーン

2.3 今後の展開

本プロジェクトの活動期間を通じ新規注意喚起対象ユーザ数の減少が続くことから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、本プロジェクトの取り組みに対する認知度も高まっている。

平成 21 年度は、平成 20 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実施することにより、ボット感染ユーザのさらなる減少を目指していく。そのためには、感染ユーザを効率的に見つけていく仕組みづくりを進めるほか、注意喚起に対するユーザの行動を確実に促すための様々な取り組みを行っていく。

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、解析結果を反映させた駆除ツールを作成している。今年度は駆除ツール実行環境の確認機能（サービスパック適用確認機能など）、検出状況送信機能の収集情報の拡張など駆除ツール実行環境の実態把握やユーザへの対策の促進のための機能の拡張を行った。

また、駆除ツールへの反映のための解析を実施するとともに、将来への脅威予測や対策への反映を目的として、収集した検体の中で特徴的な検体を中心に、静的解析技術による詳細解析を実施している。

上記に加え、2007 年度と同様にボット感染予防推進グループへボット検体の提供も継続して行っている。

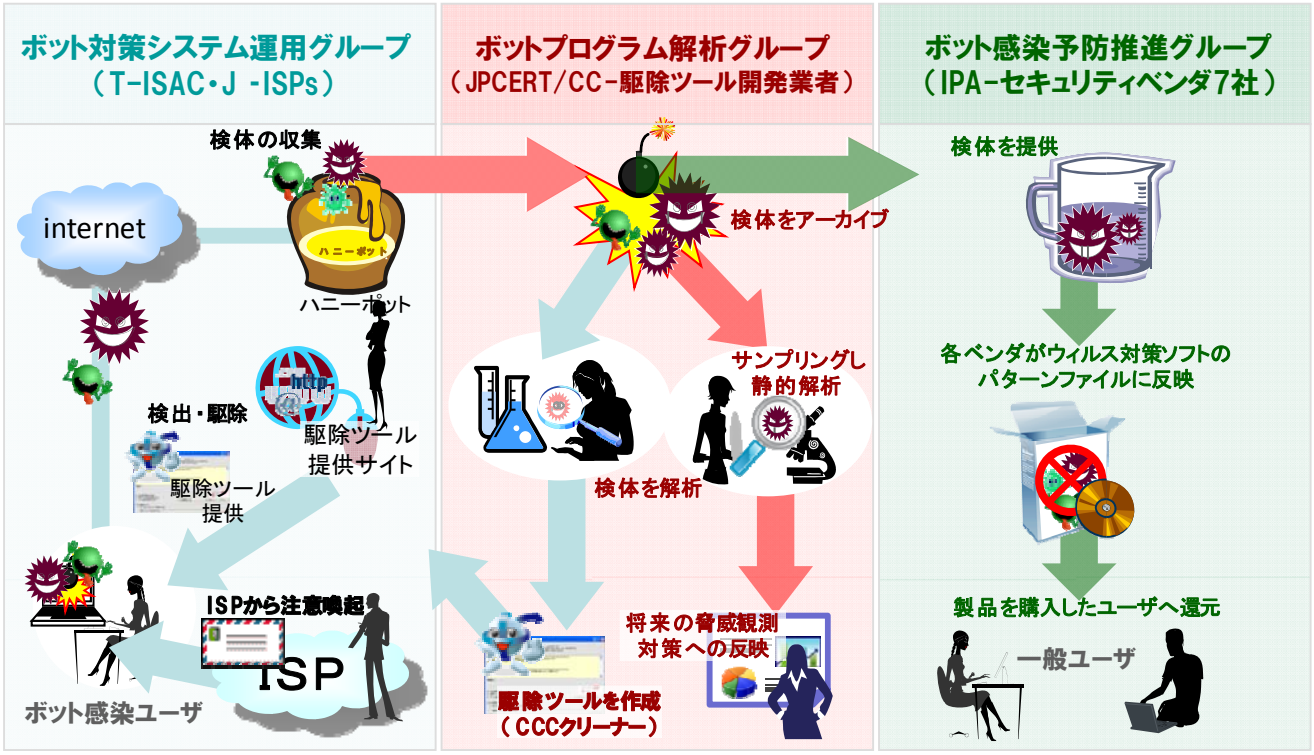

図 3.1-1 CCC の各グループの役割

3.1.1 検体解析数と駆除ツール反映数に関する成果

2007 年 2 月からの累積の同定検体数を母数として、駆除ツール作成検体数と簡易解析数（既知）による駆除ツールの反映状況としては 99.38%となっている。

① 駆除ツール作成検体数　=　18,334
② 簡易解析数（既知）=　846,510
③ 同定検体数　=　870,227
④ 駆除ツール反映率　=（① + ②）÷ ③　＝　99.38 %

これは、収集された検体のうち 99.38%のボット検体をウイルス対策ソフトと駆除ツールで検知できるということであり、収集された検体が十分活用されている状況が伺える。

① 駆除ツール作成検体数：
危険度が高く、感染者の多い検体について、駆除ツールを作成した検体数
② 簡易解析数（既知）:
収集した検体のうち、すでに既知の検体であり、既存のツールにおいても対応可能であると確認された検体
③ 同定検体数:
同じ検体が多数収集されるため、検体のサイズや外形的特徴の重複を除いた一意な検体数

3.2 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解析し、駆除ツールを作成している。

3.2.1 駆除ツールの機能追加

平成 20 年度では、ユーザの視点に立った改善をすることを目的として、駆除ツールの機能追加を行った。各機能について以下に記載する。

① ファイル感染型ボット処理時の対応の追加
システムフォルダ以下に ファイル感染型ボットが感染しており、かつ駆除できなかった場合、ポップアップを表示し、当該ファイルの駆除を行わずに検索・駆除処理の中止をするように動作内容を変更した。また、上記の場合を除いてファイル感染型ボットを検知した場合には、ポップアップ表示にて警告を行うよう変更を行った。本機能の追加によりファイル感染型に感染していること、およびファイル感染型に感染した場合の対処方法をユーザに伝えることができるようになった。

② 検出状況送信機能の改善
既存の駆除ツールで既に実装されていた検出状況送信機能で送信する情報の追加を

行った。本機能を改善することで駆除ツール実行環境のより多くの情報の収集が可能となり、次項 3.2.2 などの統計情報としての活用やより効果的な対策の検討などに使用することが可能となった。検出結果により送信される情報は以下のとおりである。

- 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 Malware 名
- エラー情報
- 搭載メモリ量
- ファイル感染型ボットの検出結果
- hosts ファイル改ざん確認結果
- 接続状態判断結果

なお、検索・駆除完了後にポップアップが表示され、ユーザが情報を送信するかどうかを選択できるようになっている。

③ サービスパック適用確認機能

各 Windows 環境に最新のサービスパックが適用されているかを確認する機能を実装した。2009 年 3 月 31 日現在では、Windows XP は SP3 未適用、Windows Vista は SP1 未適用、Windows 2000 は SP4 未適用の場合に、警告ポップアップを表示する。本機能を追加することでユーザにサービスパックの適用状況について容易に周知が可能となった。

④ hosts ファイルの改ざん修復機能

Windows Update やウイルス対策ソフト更新の阻害や、ファーミング攻撃を防ぐため、駆除ツール実行時に hosts ファイルを確認し、改ざんされている可能性がある場合にポップアップを表示しユーザへの注意喚起を行うとともに、既存の hosts ファイルをリネームしデフォルト設定の hosts ファイルを作成する機能を実装した。

⑤ 接続形態判断機能

駆除ツールを実行している PC の IP アドレスがプライベート IP アドレスかグローバル IP アドレスかを確認し、グローバル IP アドレスであった場合に警告ポップアップを表示する機能を追加した。本機能を追加することでユーザ環境におけるブロードバンドルータが駆除ツール実行環境に導入されているか確認することが可能となった。

3.2.2 検出状況の分析

駆除ツールの検出状況送信機能にてユーザに任意で送付いただいた検出状況送信ログ

（以下、送信ログ）の収集結果を以下に記載する。

① 送信数推移 （対象期間: 2008 年 4 月-2009 年 03 月）

送信ログの収集数の推移を以下に記載する。2009 年 2 月に送信ログ数が急増しているが、これはセキュリティの日のイベント開催期間でそのイベント効果およびマスコミなどの影響で CCC サイトへのアクセスも増加したことによる。

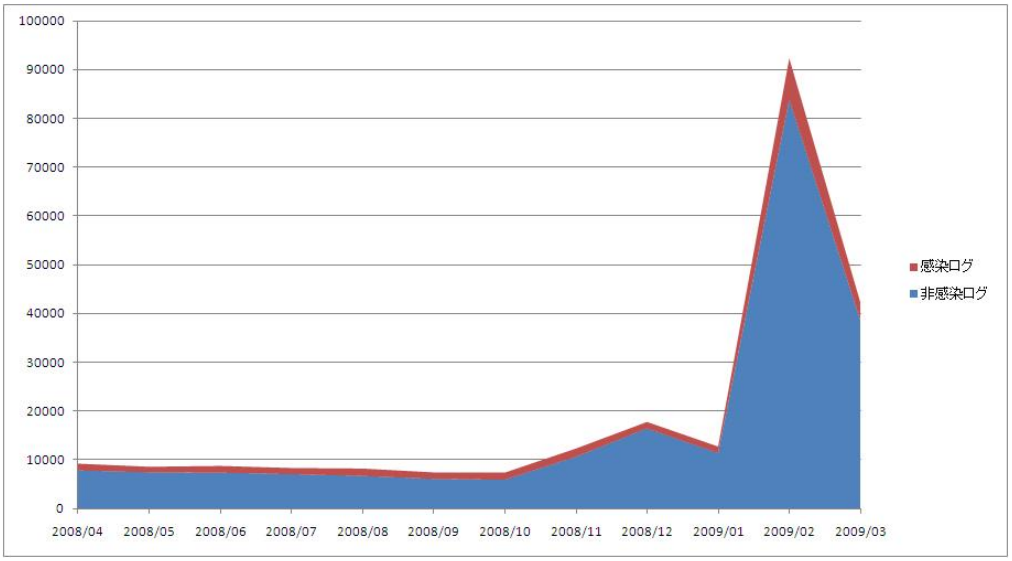

図 3.2-1 送信ログ収集数推移

② OS 別の収集比率 （対象期間: 2008 年 04 月-2009 年 03 月）

OS 別の収集比率を以下に記載する。ログ送信ユーザの OS は依然として Windows XP が多くを占めていることが確認できた。

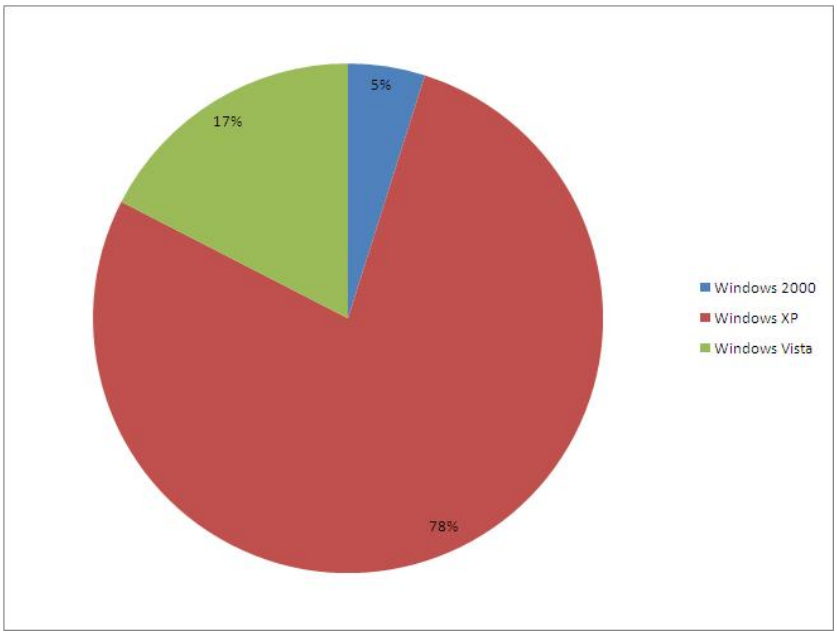

図 3.2-2 OS 別の収集比率

③ OS 別収集傾向 （対象期間: 2008 年 04 月-2009 年 03 月）

OS 別の収集数の推移を以下に記載する。2008 年 11 月以降において Windows XP SP3、Windows Vista SP1 の増加が顕著に見られた。なお、2009 年 1 月から 2 月にかけてのグラフの突出は、セキュリティの日のイベント効果などによるログ報告の絶対数の影響を受けている。

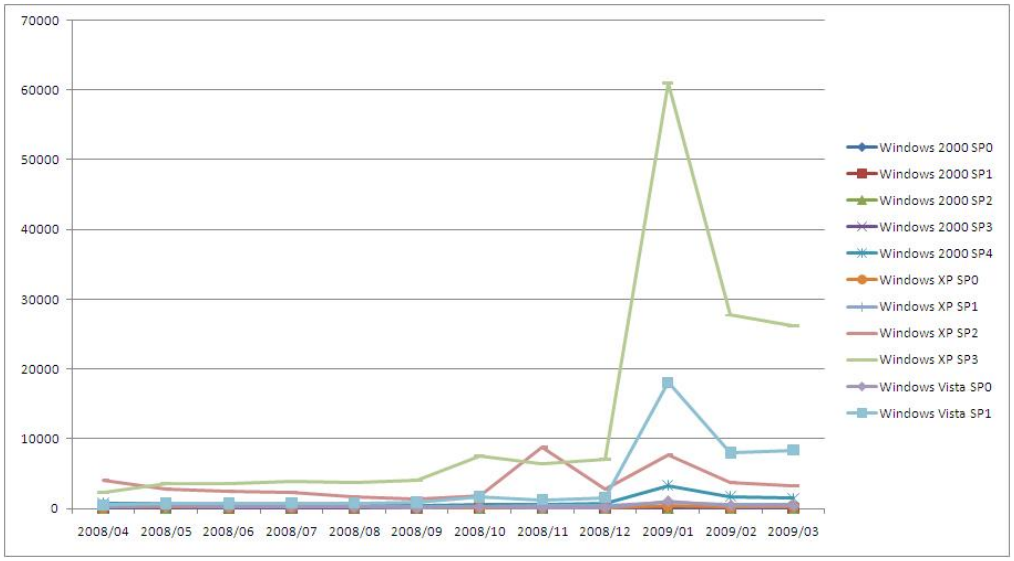

図 3.2-3 OS 別送信ログ収集数推移

④ OS のサービスパック別の感染比率 （対象期間: 2008 年 04 月-2009 年 03 月）

OS のサービスパック別の感染比率を以下に記載する。送信ログの総数は各 OS のサービスパック毎に異なるが、ユーザが多い Windows XP ではサービスパックが高いほど感染率が低い傾向が見られた。

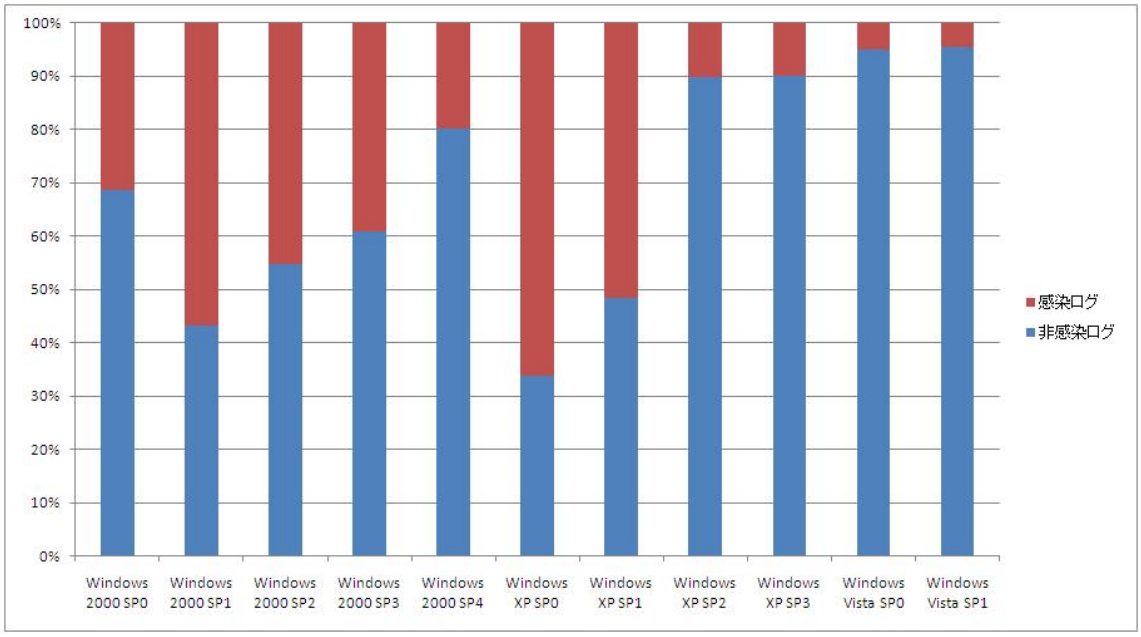

図 3.2-4 OS のサービスパック別感染比率

⑤ ブロードバンドルータ導入状況 （対象期間: 2008 年 12 月-2009 年 03 月）

感染が確認された、全体の 9%を占めるユーザの接続形態判断の結果の状況を以下に記載する。グローバル IP アドレスの割合は、一般サイトのユーザでは 19%であり、注意喚起を受けたユーザについては 44%であった。ブロードバンドルータの導入されていない環境がまだ多く存在するものと考えられる。

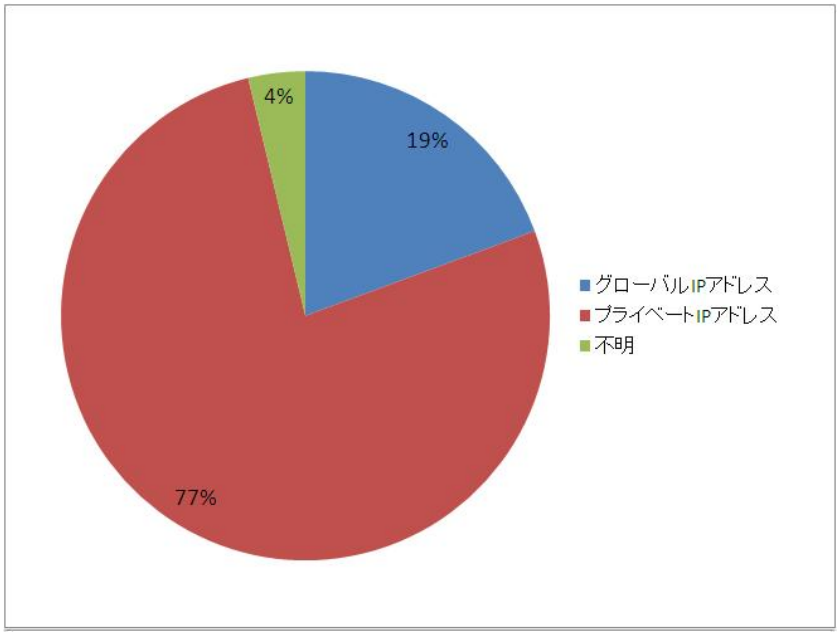

図 3.2-5 一般サイトユーザの IP アドレス比率

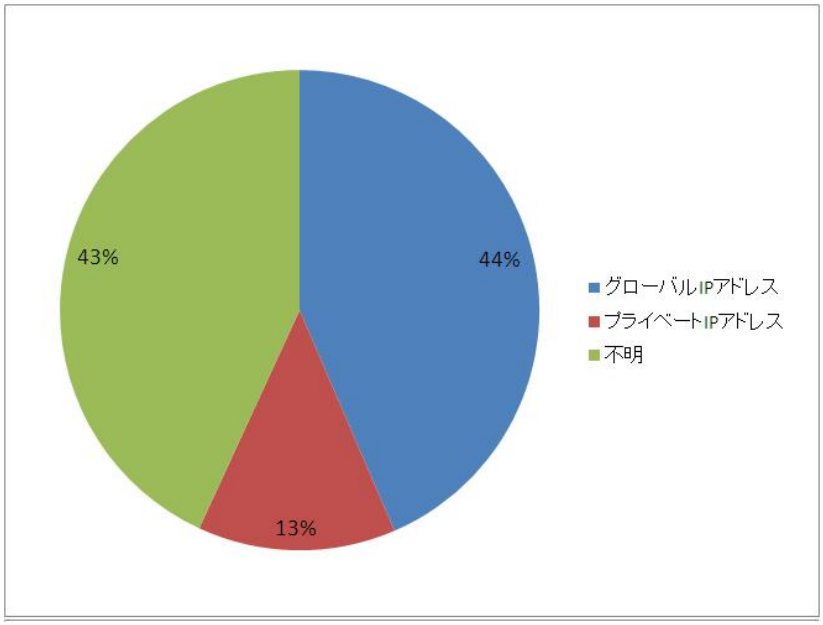

図 3.2-6 注意喚起を受けたユーザの IP アドレス比率

⑥ hosts ファイル改ざん状況 （対象期間: 2008 年 12 月-2009 年 03 月）

感染が確認された、全体の 9%を占めるユーザの hosts ファイルの改ざんの検出結果を以下に記載する。一般サイトのユーザでは 5%、注意喚起を受けたユーザでは 11%の割合で hosts ファイルの改ざんが検出されており、hosts ファイルの改ざんによるサイト接続への影響を受けているユーザが多く存在すると考えられる。

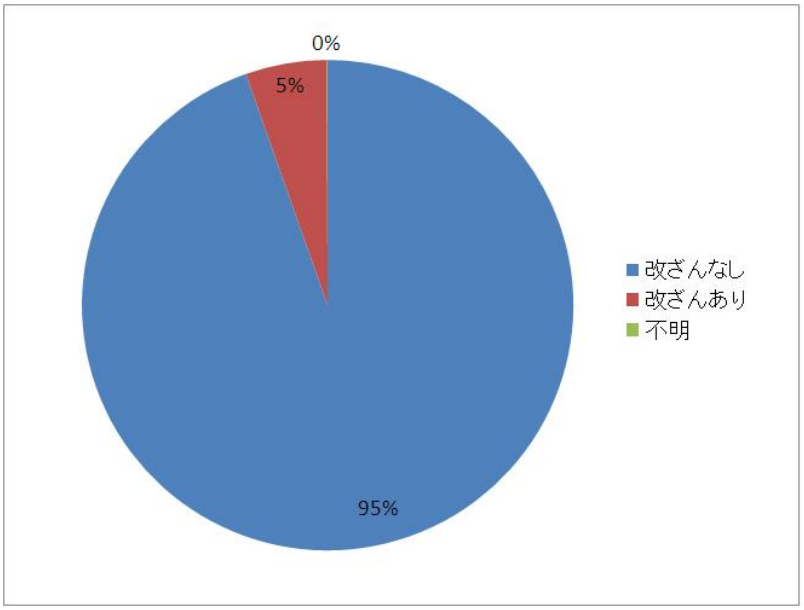

図 3.2-7 一般サイトのユーザの hosts ファイル改ざん検出比率

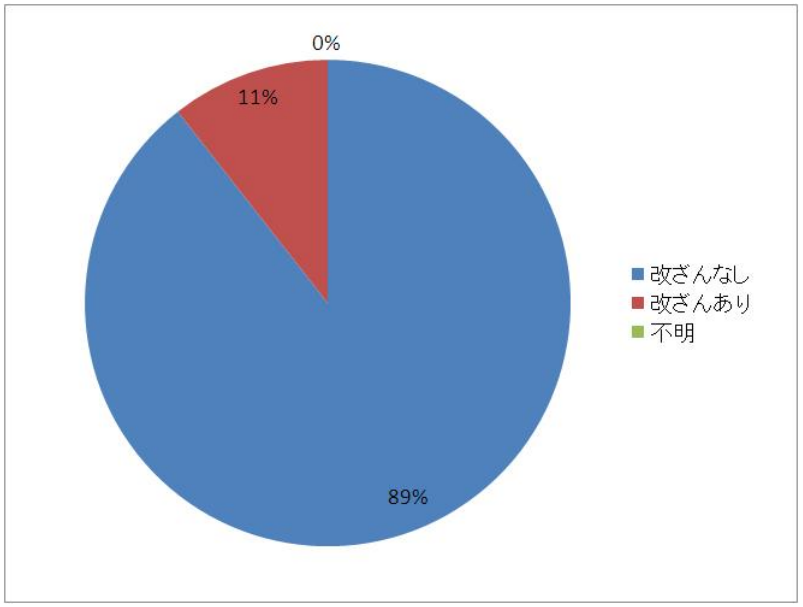

図 3.2-8 注意喚起を受けたユーザの hosts ファイル改ざん検出比率

⑦ 感染検体傾向 （対象期間: 2008 年 04 月-2009 年 03 月）

ユーザの環境における検出名の状況について以下に記載する。環境毎の感染傾向としては、ハニーポット（図 3.2-9 送信ログにおける感染検体比率）においては PE_VIRUT 系 （ファイル感染型） の感染やネットワーク経由の検体が収集されているが、送信ログ （ユーザ環境） （図 3.2-10 CCC ハニーポットにおける検体比率） においては PE_VIRUT 系 （ファイル感染型） だけではなく、WORM_AUTORUN などネットワー

ク攻撃以外の方法で感染したと思われる検体への感染傾向が見られた。

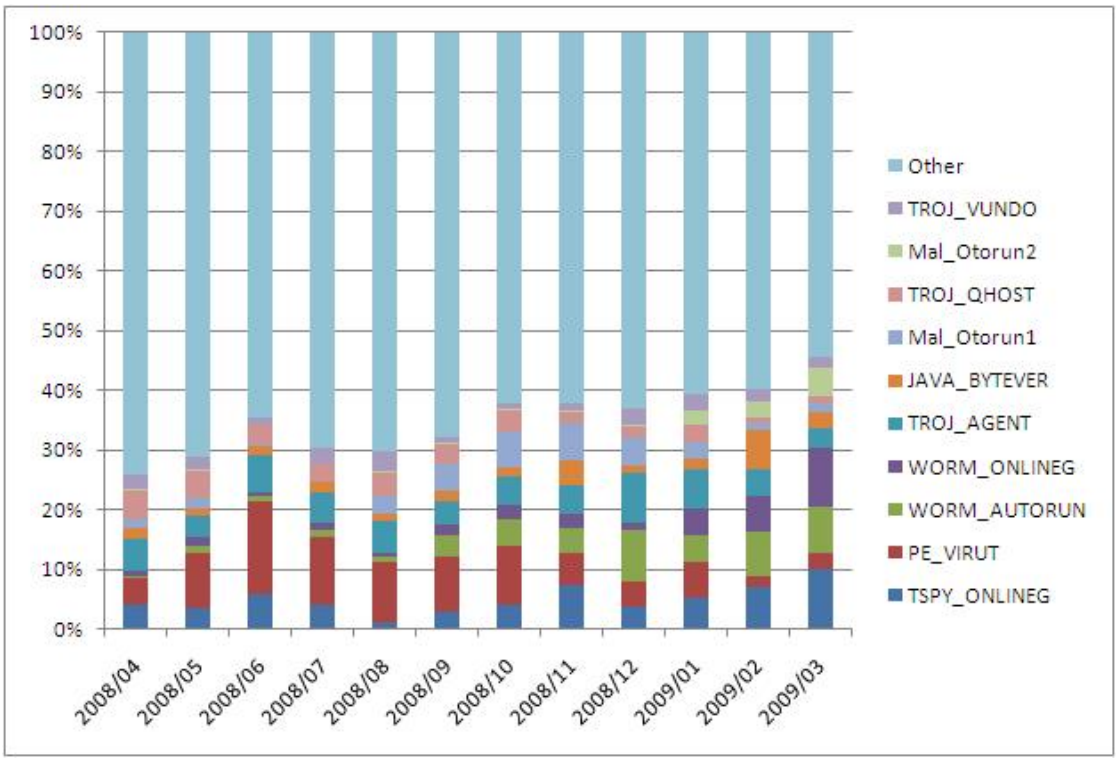

図 3.2-9 送信ログにおける感染検体比率

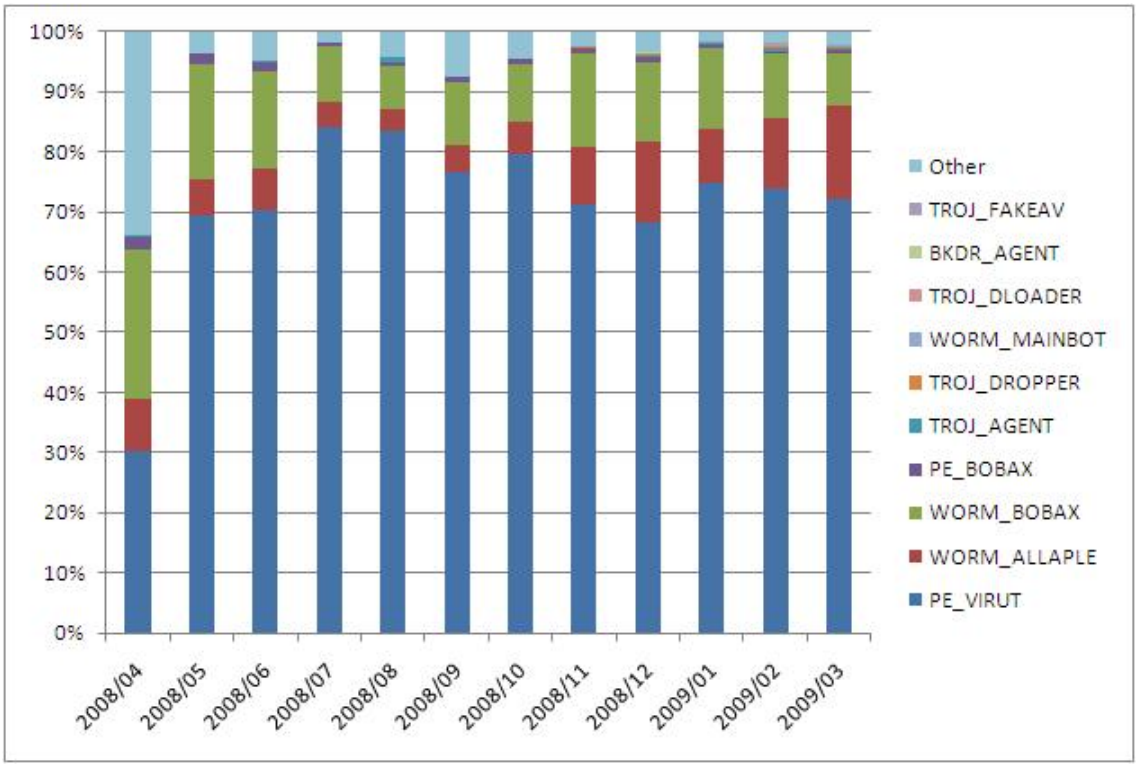

図 3.2-10 CCC ハニーポットにおける検体比率 （同定検体）

⑧ まとめ

送信ログの収集により駆除ツールを使用したユーザの環境では、ブロードバンドルータの導入や OS のパッチの適用が不十分な環境が多く、感染しやすい環境のままで使用されている状況が確認できた。また、USB 経由や Web 経由と思われる検出状況も見られており、この結果は最近の Malware の傾向として複数の感染経路を持っているということを表している。このような状況からも引き続きユーザへ以下の案内を継続して行っていくことが必要であると思われる。

- Windows Update の促進
- ブロードバンドルータの導入
- ウイルス対策ソフトウエアの導入

3.3 ボット分析

ボットプログラム解析グループでは、現在流行しているボットを定期的にサンプリングして解析することにより、トレンドとなっているボットの脅威を特定し、得られた知見を蓄積することで、将来の脅威の予測や予防策を探ることを目的としている。

解析内容の詳細について、以下に示す。

3.3.1 バージョンアップによる検体の変化の分析

将来の脅威予測を行うためのアプローチとして、検体のバージョンアップに着目した。本調査では、バージョンが上がるにつれて検体にどのような変化が見られるのか、またバージョンアップと時間との関係についても調査し、将来の脅威について考察を行った。

なお、バージョン情報の取得方法として、Windows のプロセス間排他制御に用いられるミューテックスの名前を使用した。

① ファミリーA

ファミリーA において確認できたバージョンは、以下の 4 つであった。

- v2.3
- v2.4tested
- v2.5
- v2.9

また、全てのバージョンに共通して以下の特徴が見られた。

- コードの特徴
  - C 言語で記述されたコード
- 機能の特徴
  - IRC に接続し、コマンドの受信を行う
    - 感染マシン上で任意のコマンド実行
    - ポートスキャン
    - ファイルのダウンロードと実行
    - 感染マシンの情報送信

各バージョンの解析結果を比較し、全体を通じて見られた変化をまとめたのが表 3.3-1 である。

表 3.3-1 ファミリーA の変化

新規機能	なし
耐解析機能	バージョンにより異なる機能が実装 ● パッカー変更 ● コード難読化 ● パラメータエンコード
既存機能	IRC コマンドの追加 サブファイルのダウンロード機能を削除 パラメータの変更
外見	コードの一部再構築

このファミリーでは、パッカーや難読化といった解析を阻害する機能の変化が目立っている。しかし、コードが変化しているにも関わらず、高度化されているわけではなかった。これは、耐解析性の高い有料のパッカーの使用や複雑なコード難読化の実装にはコストがかかり、また Malware 作成者の主な目的がウイルス対策ソフトの検出回避であるからではないかと考えられる。また、有料のパッカーが使用されない要因のひとつとして、パッカー本来の目的であるファイルサイズ削減を達成するためのみにパッカーが使用されており、有料のパッカーによる高度な難読化処理が必要ないためではないかと考えられる。

② ファミリーB

ファミリーB では、以下のバージョン番号が確認できた

- v011ALPHAA
- v0111ALPHAA
- v0122ALPHAA
- v0122ALPHAA27
- v0.2_Beta_711d43
- v0.66_Beta_erf

ファミリーB の全てのバージョンに共通して、以下の特徴が見られた。

- コードの特徴
  - UPX によってパッキング
  - 本体部は C 言語で記述されたコード
- 機能の特徴
  - 外部からの通信を受ける多機能バックドアを作成
    - TCP/UDP プロキシ等
  - クライアントの情報を外部に送信

各バージョンの解析結果を比較し、全体を通じて見られた変化をまとめたのが表 3.3-2 である。

表 3.3-2 ファミリーB の変化

新規機能	なし
耐解析機能	変化なし
既存機能	インターネット接続確認の追加 データ、重複起動チェックの追加 特定プロキシ機能の追加、削除 他バックドア確認機能の削除 ブラックリスト確認機能の追加 パラメータの追加
外見	コードの一部再構築

このファミリーでは、当該ファミリーのメインの機能であるプロキシとして動作するバックドアの高度化が目立った。バージョンが上がることでバックドアの機能や数が増加していた。同時に、ホスト情報やバックドアで取得した情報の送信先が複数個に増えたり、バックドアのスレッド数制限やスリープ時間の設定機能が追加されていたりした。

また、後半のバージョンにおいては、それまでに追加されたバックドア機能や情報送信機能が大幅に削られており、機能の見直しやコードの最適化が行われているのではないかと考えることができ、全体を通じて丁寧なメンテナンスを伺わせる結果が得られた。

③ ファミリーC

ファミリーC は、以下のバージョンが存在することを確認できた。

- v2.0
- v3.0
- v3.5
- v6.0

全てのバージョンに共通して見られた特徴は以下のとおりである。

- コードの特徴
  - C 言語で記述されたコード
- 機能の特徴
  - TCP 135 Exploit による感染活動
  - ファイルのダウンロードと実行

各バージョンの解析結果を比較し、全体を通じて見られた変化をまとめたのが表 3.3-3 である。

表 3.3-3 ファミリーC の変化

新規機能	なし
耐解析機能	パッカーがバージョンアップ
既存機能	感染ホスト情報送信機能の追加 メッセンジャーを用いたメッセージ送信機能の追加 XP SP2 の TCP 接続制限対応の追加 パラメータの追加
外見	変化なし

このファミリーではメッセンジャーを使った攻撃機能や感染ホスト情報送信機能といったサブ機能の追加が見られた。メインであるネットワーク攻撃に関しては、攻撃コードの変更等は見られなかった。メイン機能の変化としては、パラメータの追加や、Windows XP SP2 以降で実装された TCP ハーフコネクション数の制限への対応 （攻撃

スレッド数の制限） を行っており、ファミリーA でも見られたメンテナンスの形跡が見られる。

全ファミリーの結果をまとめると、バージョンアップによる変化は、メンテナンスやウイルス対策ソフト回避を目的とした変化が目立っており、将来の脅威につながる新しい機能は見られなかった。一般のソフトウエアと同じく、バージョンアップでは新しく大きな変化が見られることはなく、将来の脅威予測のためにバージョンアップを追うというアプローチには限界が見受けられる。

上記を踏まえた上で、また別のアプローチによる検体の分析が必要であると言える。

3.3.2 同一サイトから配布される検体の変化の分析

同一のサイトから配布されている検体の変化を観測し、検体の変化傾向等を知ることで、将来の脅威に関する分析を行った。

調査内容は以下のとおり。

[1] システム運用グループの収集データから、検体を変えながら配布を続ける特定サイトの情報を抽出
[2] 配布されている検体の簡易解析、静的解析を実施
[3] サイト単位で検体の変化を分析

対象サイトは、未知検体の配布を継続して行っていた以下の 3 つのサイトである。

表 3.3-4 対象サイト概要

サイト / 項目	サイト 1（イギリス）	サイト 2（アメリカ）	サイト 3（日本）
対象期間	2008/10/03～2008/12/7	2008/12/31～2009/1/14	2008/12/06～2008/12/10
サイト生存期間	生存中（2 月 20 日時点）	15 日間	5 日間
ハッシュユニーク配布検体数	35 検体	19 検体	110 検体

対象となった各サイトの解析結果のサマリを以下に示す。

表 3.3-5 対象サイト解析結果サマリ

サイト / 項目	サイト 1（イギリス）	サイト 2（アメリカ）	サイト 3（日本）
配布検体	IRC ボット ポートスキャナ	IRC ボット ポートスキャナ	リモートシェル
平均配布期間	3 日/検体	3 日/検体	1 日/検体
平均配布数	1～2 検体/日	1～2 検体/日	20～60 検体/日
検体の変化	● 機能変更なし ● 本体が実行されるまでの部分が変化	● 機能変更なし ● 本体が実行されるまでの部分が変化	● 機能変更なし ● 本体が実行されるまでの部分が変化

どのサイトにおいても 1 日に複数種のハッシュユニーク検体を配布しており、配布されている検体は、ハッシュ値が違っても中身はサイト毎にほぼ同じ検体であることが分かった。つまり、イギリスとアメリカのサイトは IRC ボットとポートスキャナを、日本のサイトはリモートシェルを、ハッシュ値を頻繁に変更しながら配布していたことになる。なお、イギリスとアメリカの IRC ボットとポートスキャナは同じものであり、両サイトに何らかの関係性があるのではないかと考えられる。

ハッシュ値が異なるにも関わらず中身が同一である検体が多く、配布される目的としては、ウイルス対策ソフトの検出回避が挙げられる。Malware 作成者は日々何らかのツールを用い、一つの Malware 本体から次々とハッシュ値の違う検体を作成し、常にウイルス対策ソフトに検出されないよう運用を行っていると考えられる。

ハッシュ値の異なる検体を配布し続ける運用を行われた場合、検体入手後にウイルス対策ソフトのパターンへ反映したとしても、パターン反映時には既に同一ハッシュの検体が配布されておらず、検出されない別のハッシュ値を持つ検体が配布され、結果としてウイルス対策ソフトで対応できないという状況が発生する可能性が考えられる。近年ではジェネリックパターンやレピュテーションといった新しいアプローチで対策を行ってはいるものの、ウイルス対策ソフトは常に誤検出問題等を考えなければならないため、完全な対策は難しい状況である。

このような状況の中、ウイルス対策ソフトのパターン対応までの空白期間を利用する Malware 配布サイトについて、サイト閉鎖コーディネーションを行うことで対応できる可能性が考えられる。ウイルス対策ソフトでは断ち切れない未知検体継続配布の対策として、サイト閉鎖コーディネーションが実現可能かどうか、どの程度有効なのか、といった点について、今後調査・検討する必要がある。

3.3.3 特徴を持つ検体の詳細解析結果の分析

検体の特徴的な挙動を詳細に解析し、ボット対策推進事業で収集された検体の傾向を知るだけでなく、新しい技術が使用されているのか、また、技術が今後脅威となり得るかどうかを分析した。

調査内容は以下のとおり。

[1] 収集した検体の動的解析を実施し、特徴的な挙動を行う検体をサンプリング
[2] サンプリングした検体の静的解析を実施し、機能の詳細を把握し分析

動的解析の結果から抽出した検体は全 21 検体であり、各検体の詳細解析結果からは以下の特徴的な機能が見られた。

表 3.3-6 詳細解析結果から得られた特徴的な機能一覧

機能		説明
ボット機能	IRC	IRC にて Herder からの指令を受ける機能
	HTTP	特定のサーバに HTTP リクエストを送信し、そのレスポンスによって行動を決定する機能
	独自プロトコル	TCP/UDP の Well-known ポート上で、独自で実装したプロトコルを用いてコマンドのやり取りを行う機能
自己隠ぺい機能	API フックによる情報操作	プロセス、ファイル、レジストリ操作に関わる API を書き換え、情報を隠ぺいする機能
	コールバックによる DLL インジェクション	デバイスドライバを用いてプロセス起動を監視し、起動したプロセスに DLL インジェクションを行う機能
	OS 内部情報の操作	PEB（Process Environment Block）等、OS の内部情報を直接変更し、自身を隠ぺいする機能
耐解析機能	コードインジェクション	自身や自身が抱えるファイル、コードを別のプロセスに書き込み実行させる手法
	コード難読化	コード中に無駄なコードを挿入した

機能		説明
		り、ひとつの関数を細分化したりすることで、アセンブリコードを読みづらくさせる手法
	パラメータエンコード	使用する URL 等のパラメータをあらかじめエンコードした状態で保持し、使用する直前でデコードする手法
その他	UPnP を用いた情報取得	UPnP を用いてルータと通信し、グローバル IP アドレスを取得する機能
	外部サイトを用いた情報取得	外部サイトを用いて、グローバル IP アドレスや通信速度、ブラックリスト登録情報等を取得する機能
	システム改ざんによる設定変更	tcpip.sys を改ざんすることで、TCP ハーフコネクションの接続制限を解除する機能
	P2P	P2P ネットワークを構築し、多数のホストと通信する機能

調査を行った検体は、感染を広げるために OS の持つ脆弱性への攻撃や、多くの機能を持ったボットではなく、SPAM メールを送信することや、ファイルをダウンロードして実行するといった、目的や機能に特化した Malware が多く存在した。そして、それらの Malware はルートキット機能やコードインジェクションを利用して、感染を隠匿する処理を行っていた。このように必要な機能を長期間提供できるように Malware が作成されているのは、おそらく Malware を商用利用するためだと考えられる。

得られた特徴的な機能のひとつひとつを見ると、2008 年度になって初めて観測されたという機能は存在していなかった。しかし、独自プロトコルについては複数種のプロトコルが存在しており、それらの解析は現在も完了していない。独自の実装は今後発展し、より高度化し使用されることが考えられるため、引き続き解析を行っている。

新しい機能は見られなかったが、UPnP と tcpip.sys の改ざん処理、外部サイトを用いた IP アドレスの取得処理については、同様の処理が MS08-067 への攻撃で猛威を振るう W32.Downadup 系の Malware でも使用されていることが確認できた。シマンテック社の Malware 情報では W32.Downadup 系の Malware は感染拡大を目的とするワームに分類されており、同機能を持つそれぞれの検体との関連性は見あたらなかった。以上のことから、Malware 開発者は Malware に必要とされる機能を実現するために、他の Malware の処理情報を参考にするなど、何らかの手段で情報共有を行っているのではないかと考えられる。

動的解析では Malware 起動時の挙動を簡単に調査することができるが、ボットコマンド等のペイロードや、ボットコマンドの処理を詳細に調べることはできない。また、動的解析は Malware を一定時間だけ動作させて、その処理内容を記録するが、Malware の中には、頻繁に Sleep することによって、動的解析で決められた時間内に処理が全て完了しない場合が存在する。

静的解析では、Malware の細かな挙動やボットコマンドのペイロードとその処理内容、接続する可能性のある全サーバなどを調査することができる。しかし、静的解析には非常に時間と手間がかかり、Malware のコードが複雑な場合には十分に解析できない場合もある。

以上を踏まえ、次のようなことを行っていく必要があると考えられる。

- 解析済み Malware の解析情報などを共有するツールの作成
- zlib 等、Malware でよく利用されるライブラリの検出ツールの作成
- ルートキット機能の解析に必要なテクニックや情報の共有
- Malware の解析技術者の育成

3.4 今後の展開

平成 20 年度の活動では、駆除ツールの機能拡張やそれに伴うログ分析、および検体の継続的な解析を行った。次年度では、平成 20 年度の活動を継続し、さらなる安定化・効率化を目指す。

① 駆除ツールの作成、ログ分析

駆除ツールの安定した供給と共に、ユーザの検出状況送信ログの分析を継続して行う。

② ボット分析

平成 20 年度の活動で得られた結果を踏まえ、新たなアプローチによりボットの分析を行い、将来の脅威予測およびその対策を模索する。

③ 普及啓発活動支援

平成 20 年度と同様に、ボット感染防止対策の普及啓発活動支援を行う。

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ウイルス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ウイルス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ウイルスを検出・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 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（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 2008 年 3 月から 2009 年 3 月末（報告月：2008 年 5 月から 2009 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、2008 年度の各ベンダの平均値を表 4.3-1 に示す。

表 4.3-1　パターンファイルへの反映状況

	2008 年度平均
既に反映済み	98.6%
今回反映	1.1%
未反映	0.3%

「既に反映済み」および「今回反映」の数値を足した 99.7%とは、本プロジェクトで取得された検体の 99.7%をウイルス対策ソフトで検知できるということである。この数値は本プロジェクトの成果のひとつとして、収集された検体が十分活用されている状況と考えられ、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さら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

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我が国初の試みであり、世界的に見ても稀有な事例と言える。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言える。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。

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、ウイルス対策をよろしくお願いいたします。