ボットの脅威との戦い

～サイバークリーンセンター（CCC）活動レポート～

2010 年 9 月 13 日

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/

（空白）

目次

1. はじめに

インターネットの利用が広く一般に普及するなか、不正アクセスや悪意のあるソフトウェアによる被害が増加している。悪意のある様々なソフトウェアはウイルス、トロイの木馬、スパイウエア、ボットなどに分類されるが、総称してマルウェア（Malware）と呼ばれる。

マルウェアの中でもボットは、PC の利用者に気づかれないよう密かに感染攻撃を行う特徴がある。ボットには、ウイルス対策ソフトに検知・駆除されない多くの亜種が短期間で発生することが多くなっており、PC の利用者が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 PC の利用者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、国内ボット感染者を限りなくゼロにする取り組みとして、2006 年度より総務省・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を中心としたボット対策活動を進めている。本レポートは、CCC を運営する 3 つのグループである、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り、これまでの成果報告書の中では提示できなかった運用やシステム構築のノウハウ、工夫なども盛り込み、限りなくオープンなものとした。

2. 背景と活動概要

2.1. ボットとは

今日、インターネットは我々の生活を支える重要なインフラのひとつとなっている。インターネットはプライベートからビジネスの場面において、あるいは子供から高齢者まで様々な場面で様々な人々によって利用され、国民にとって生活に不可欠なインフラとなりつつある。こうしたなか、インターネットを利用した様々な犯罪行為も増加している。

マルウェアは、悪意のあるソフトウェアを指す造語であるが、その定義範囲は広く、機能や感染形態から、ウイルスやワーム、トロイの木馬、ボットなどのタイプに分類がされる。なかでもボットは、ハーダー(Herder)と呼ばれるボットの指令者に遠隔で操作され、DDoS 攻撃やスパムメール、フィッシングなど、様々な不正行為に利用されるという特徴を持つ。

<感染攻撃とボットネット>

一般的にボットはインターネットを通じて自分自身が利用可能なネットワークに隣接したネットワーク(利用している IP アドレスに近い IP アドレス)の PC に対して感染攻撃を行う傾向がある。この時、感染攻撃の対象となった PC にセキュリティ上の脆弱性があるとその PC はボットに感染する。感染した PC は、ゾンビ PC と呼ばれることもあり、Command and Control サーバ(以下「C&C サーバ」と呼ぶ)といわれる中継サーバに自ら接続しボットネットと呼ばれるネットワークを形成する。ボットネットは、数千から数万のボットから形成される。

多くの場合、ボットは感染した PC(ボット感染 PC)上では目に見える不審な動きは見せないことから、ボット感染 PC の利用者は感染していることに気づかない。そして利用者が知らない間に、ハーダーが、C&C サーバを経由して様々な命令を出すことで、ボットネットに接続されているボット感染 PC は情報詐取をはじめ、スパムメール送信や DDoS 攻撃に利用されてしまう。

また、かつてのウイルスの感染で多かった PC の画面に花火を表示したりハードディスク上のファイルを消去したりと言った愉快犯的な活動をするのとは異なり、ボットは犯罪組織の情報詐取などに利用されている場合が多い。ボットネットが形成される仕組みを図 2-1 に、ボット感染 PC がハーダーの遠隔操作により引き起こす不正行為の例を図 2-2 に示す。

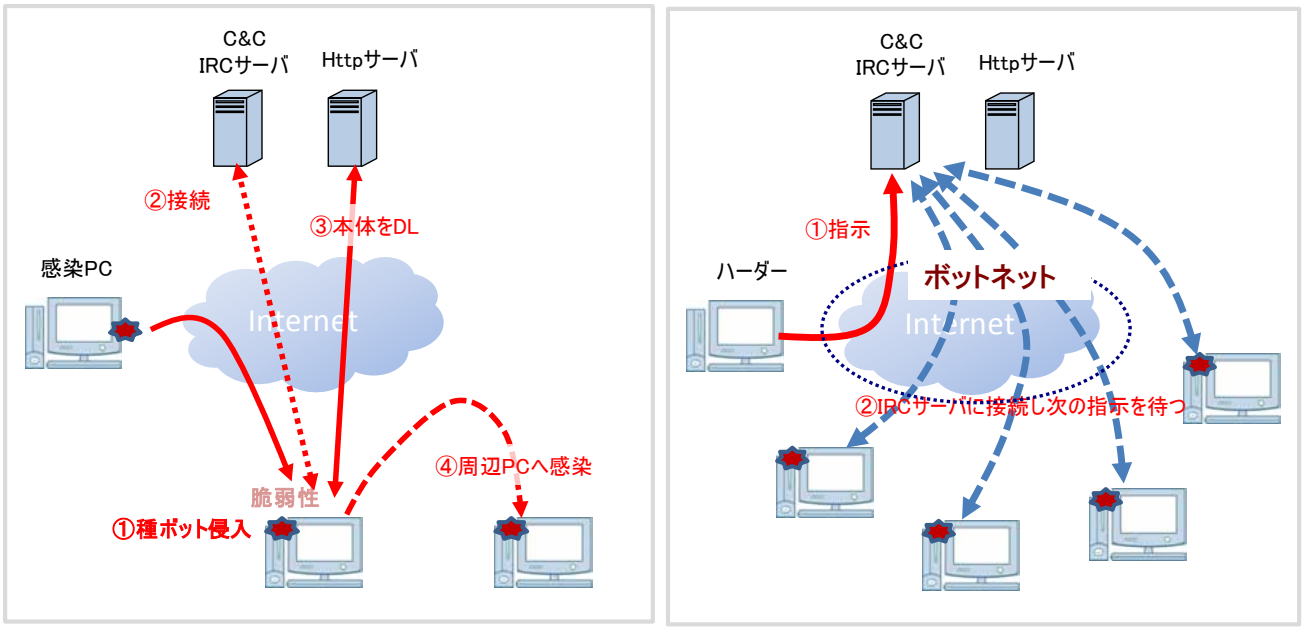


図 2-1 ボットネットが形成される仕組み

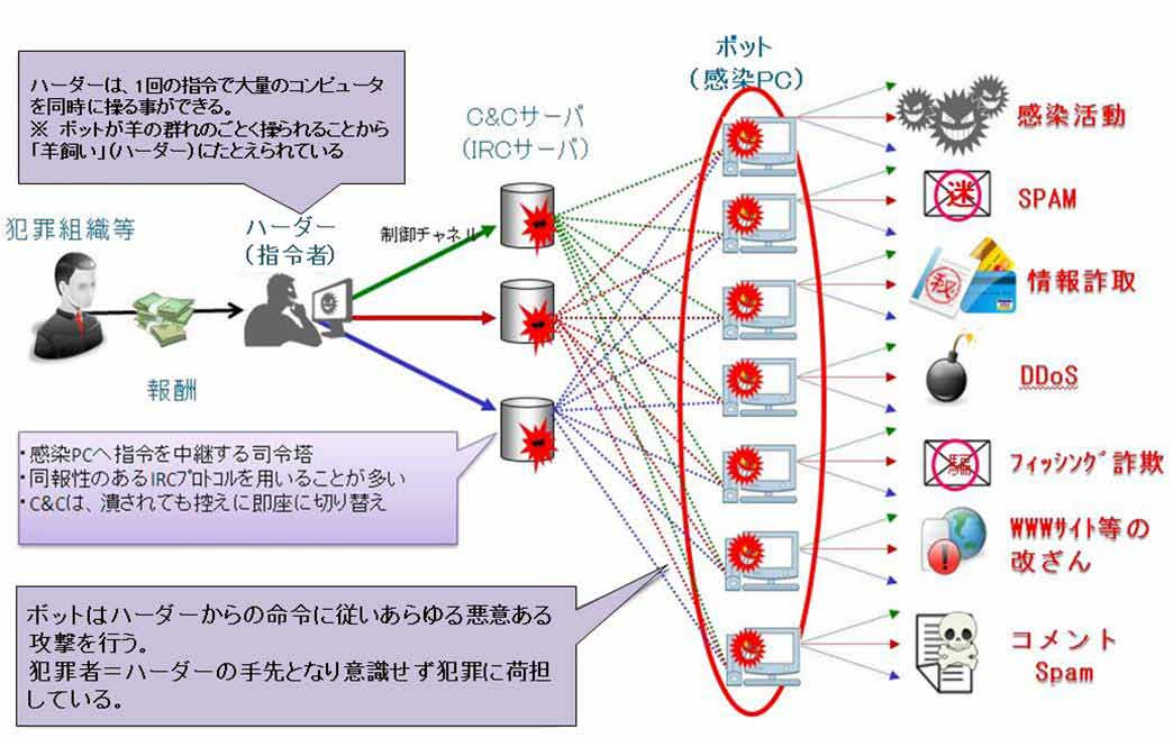


図 2-2 ボットネットによる不正行為の例

2.1.1. ボットの特徴

ボットの主な特徴としては、以下のようなものがある。

(1) 感染したPCを悪用する

コンピュータウイルスは PC を感染させる目的に動くのに対して、ボットは感染した PC を悪用することを目的としている。

(2) 感染したPCが加害者になる

ボットに感染した PC(ボット感染 PC) は、情報詐取などの被害に遭うだけでなく、ハーダーに操作され、DoS 攻撃を他の PC に仕掛ける発信源や、スパムメールの踏み台として送信元になるなど、加害者になることもある。

(3) ハーダーから遠隔操作される

ボット感染 PC はハーダーから遠隔操作により様々な命令を受け利用されることがある。

(4) ウイルス対策ソフトで検知されない

ボットはウイルス対策ソフトに検知・駆除されないように亜種が短期間で発生することが多く、感染に成功するとウイルス対策ソフトを更新させないなどの仕組みを持っている。

(5) 機能追加が簡単にできる

ボット感染 PC によりボットネットと呼ばれるネットワークを形成することで、ハーダーが遠隔操作により新たなボットのダウンロードや、新たな機能を追加することができる。こうした機能により、ウイルス対策ソフトで検知されないよう、ボット自体を変化させることも可能である。

2.1.2. ボットの感染状況

ボットの存在は、2002 年頃には既に確認されていたが、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 万人の内約 40-50 万人(感染率約 2-2.5%)が感染していると報告されている。

2.2. 対策の必要性

『2.1.1 ボットの特徴』で示したように、ボットは利用者が感染したことに気づかず被害を拡大させる特徴がある。

このため、感染拡大を防止するためには

- 感染攻撃事象検知によるボット感染PCの発見
- ボット感染PCの利用者への感染の告知と対策の依頼
- ボット感染PCの利用者によるボット駆除、再感染予防といった対策

を行う必要がある。

しかし、すべての PC の利用者がボット対策に関する正しい知識を持ち合わせているわけではないことや、ISP ではボット対策に関してスキームを持っていないこと、対策を検討し実施する場合のコスト負担の問題が

発生する PC の利用者や、ISP の努力のみでのボット対策は難しいのが実情である。

そのため、総務省と経済産業省は情報セキュリティ分野の関連団体、ISP、セキュリティベンダ等と協力し国の事業としてボット対策を行うサイバークリーンセンター（以下：CCC）が 2006 年 12 月から始動した。

2.3. CCCの概要

CCC は 2006 年度から 2010 年度までの 5 ヶ年で計画されている。2010 年 4 月の時点で、Telecom-ISAC Japan、JPCERT/CC、IPA を核に ISP76 社、ウイルス対策ソフトを開発、販売しているセキュリティベンダ 7 社をはじめ、多くのベンダや研究機関等が協力して推進している。

2.3.1. ボット対策へのアプローチ

ボット対策手法としては、いくつかのアプローチが考えられるが、CCC では、ボット感染 PC を発見し、ボット感染 PC の利用者に注意喚起するというアプローチを採用している。

CCC がボット対策をはじめるにあたり、以下の 3 つのアプローチが検討された。

(1) ハーダーへのアプローチ(ハーダーを捕まえる)

いくつかの国においては、警察組織等と連携し、ボットネットをコントロールしているハーダーを捕まえることによりボットの被害を抑えようという取り組みがされている。しかしながらボットネットを遠隔操作しているハーダーの通信を傍受し見つけることは、技術的に難しいだけでなく、日本における現行の法制度下では通信の秘密の侵害にあたることから実施できない。

また仮に見つけることができたとしても、そのハーダーの多くが海外にいることが想定されることから、日本単独での対策は難しい。ハーダーを捕まえることで一時的にボットによる不正行為を停止できたとしても、ボット感染 PC はそのまま残り続け、さらに感染攻撃を続けるという問題がある。

(2) C&Cサーバへのアプローチ(C&Cサーバを停止する)

C&C サーバを見つけて停止させることにより、ボットネットの機能を停止させることが可能である。そして C&C サーバを見つけることは、ハーダーを見つけるよりも容易である。しかしながら C&C サーバの多くは海外にあることから日本単独で C&C サーバを停止させることは難しい。

また仮にある C&C サーバを見つけて停止させることができたとしても、ハーダーは別の C&C サーバからの操作を行うことが可能で、ボットネットそのものを停止させることは難しい。

C&C サーバを停止させるのではなく、ボット感染 PC から C&C サーバへの通信を遮断する手法も考えられるが、日本における現行の法制度下では通信の秘密の侵害にあたることから実施することはできない。C&C サーバの停止、C&C サーバへの通信遮断のいずれの場合においても、ボット感染 PC はそのまま残り感染攻撃を続けるという問題が残る。

(3) ボット感染PCへのアプローチ

ボット感染 PC は感染拡大を行うために周りの IP アドレスに対し感染攻撃を行う。この IP アドレスレンジ帯をカバーするハニーポットといわれる「おとり PC」により攻撃元 IP アドレスと時刻を収集する。

ISP はこの IP アドレスと時刻から、その時間帯に割り当てられていたユーザ ID を特定し、その ID の利用者に対してボットを駆除するように注意喚起を行うことで、ボット感染 PC の駆除を行うことが可能である。

このように、ボット感染 PC の利用者に直接感染の事実を通知し駆除を促すことで、国内におけるボット感染 PC を減少させることが可能となる。更に、感染 PC の利用者一人一人に正しいセキュリティ知識を伝え、リテラシーを向上させることもできる。

以上のように、ハーダーへのアプローチや C&C サーバへのアプローチは技術的、法制度的問題から実効上困難であること、また仮に可能だとしてもハーダーや C&C サーバへのアプローチでは、国内のボット感染 PC は残り、継続して感染攻撃を続けることになり、さらなる感染拡大を生むことから根本解決にはならない。ボット対策のアプローチと対策方法や課題を図 2-3 に示す。

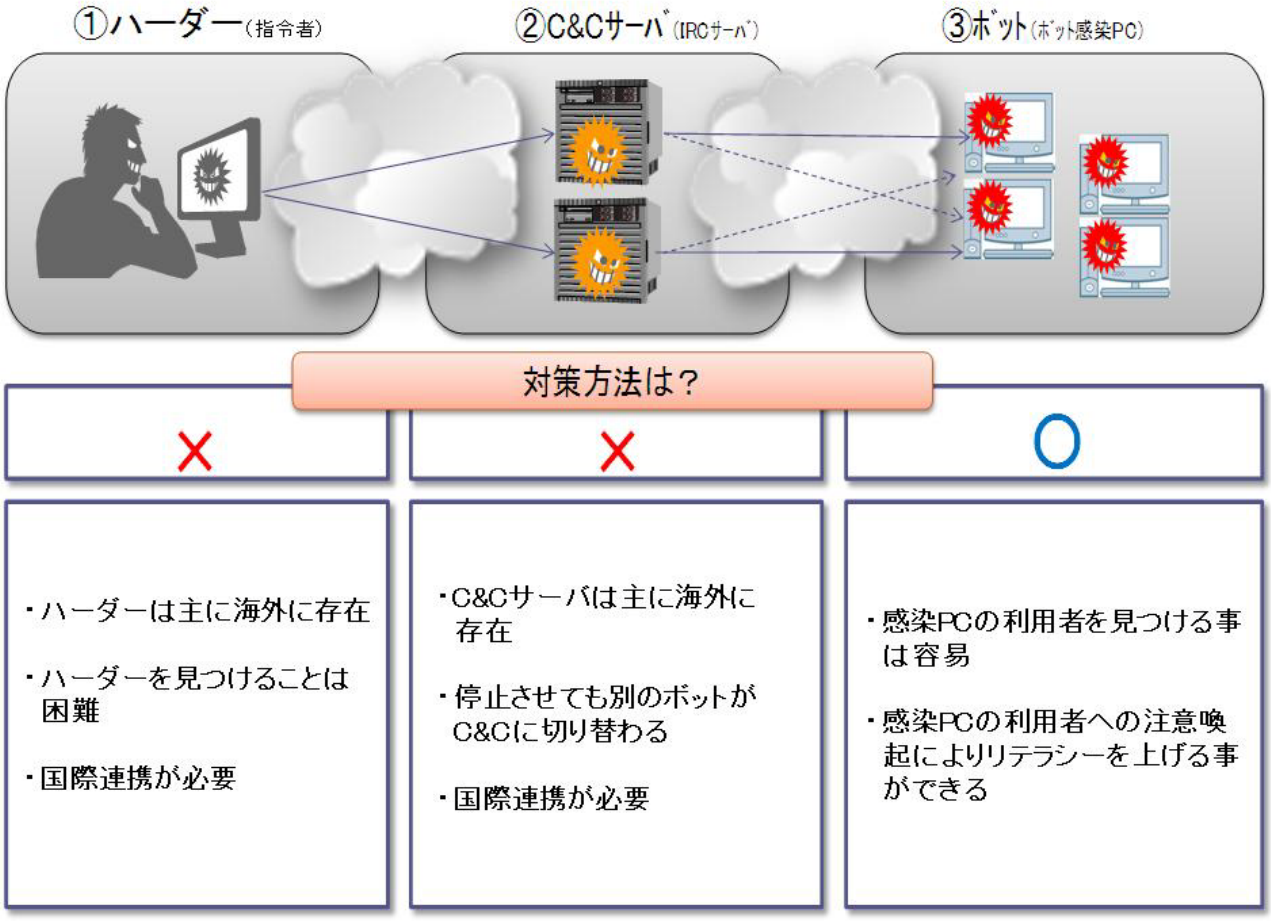


図 2-3 ボット対策のアプローチ

このことから、CCC ではボット感染 PC へのアプローチをベースに、ボット感染 PC を発見し、注意喚起活動を行うとともに正しいセキュリティ対策の普及啓発活動を行っている。

2.3.2. ボット対策を行うためのコンセプト

CCC では、ボット感染 PC をゼロにする活動を行う上で、3 つのコンセプトを掲げて活動を行っている。

(1) ボット感染PCを発見する

(2) ボット感染PCの利用者に具体的な対策手段を提供する

(3) ボットに再感染をさせない

2.3.3. CCC運営体制と役割

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。CCC の運営体制を図 2-4 に示す。

図 2-4 CCC 運営体制

(1) 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、ハニーポットシステムや注意喚起システムなど、本プロジェクトの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 PC の利用者への注意喚起などを行っている。さらに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、マルウェアの最新動向調査を行っている。

(2) 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、駆除ツールである CCC クリーナーを提供している。また、効率的な解析手法の検討なども行うほか、セキュリティベンダと連携してその対策技術の開発も行っている。

(3) 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、ボット対策システム運用グループで収集したボット検体を管理し、未知検体はセキュリティベンダに早期に提供しパターンファイルへ反映させる。これにより各社のウイルス対策ソフトを利用するユーザは、未知のボットが感染拡大する前に駆除することができる。この様に感染リスクを減らすことにより感染予防を推進している。

2.3.4. CCCのワークフロー

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各グループ間のワークフローを図 2-5 に示す。

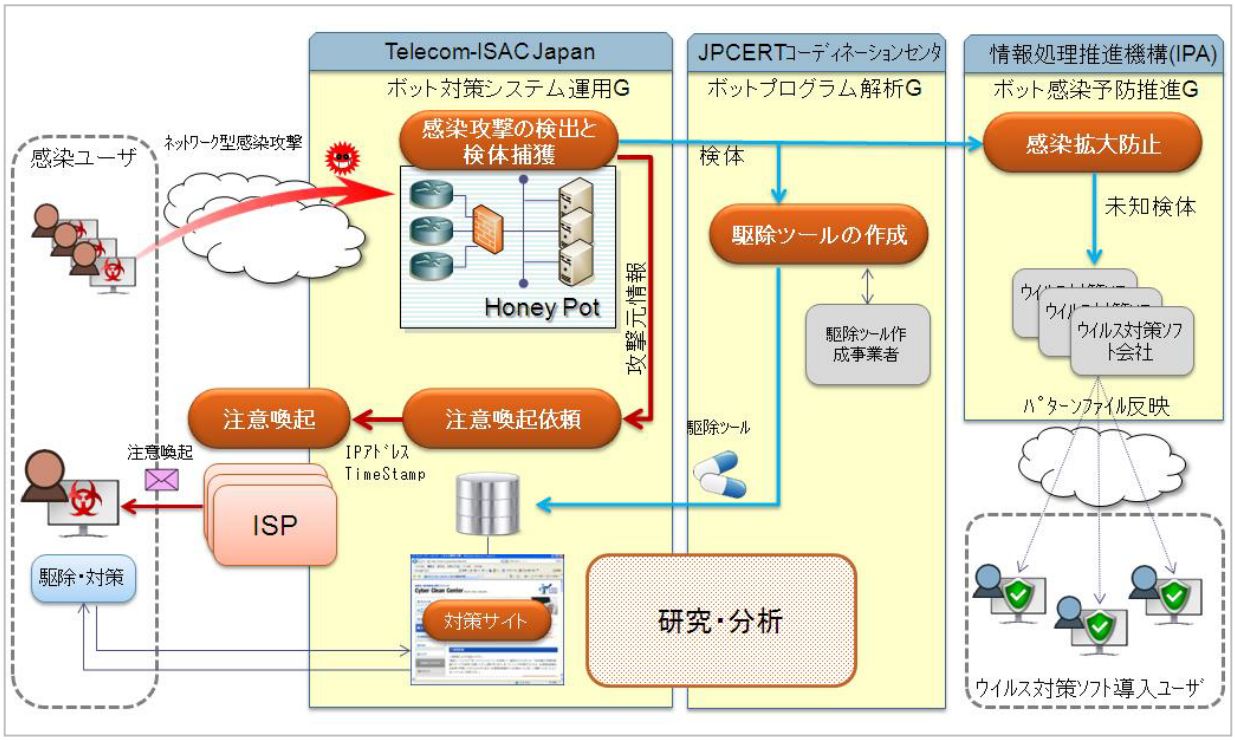


図 2-5 ワークフロー概要図

各グループではそれぞれ大まかに以下の役割の活動を行っている

運用 G	ボット感染ユーザを発見し注意喚起する	ボット感染ユーザを発見、注意喚起
解析 G	具体的な対策手段を提供	駆除ツールを作成する
予防 G	感染拡大防止活動	感染予防活動を行う

3. ボット対策システム運用グループの活動

ボット対策システム運用グループでは、ボット感染 PC の利用者へ注意喚起を行うために、まずはハニーポットシステムを利用してボット感染 PC の IP アドレスを収集する。次に、注意喚起システムを利用して、プロジェクト参加 ISP からボット感染 PC の利用者への注意喚起を行っている。

また、ハニーポットシステムで収集したボット等マルウェアはボットプログラム解析グループへ引き渡し、駆除ツールである CCC クリーナーのパターンファイルの更新に利用されるほか、ボット感染予防推進グループ経由で、セキュリティベンダに引き渡され、各社ウイルス対策ソフトのパターンファイル反映に寄与している。

ここでは、注意喚起活動を行なうにあたり行った手法検討、活動内容、活動実績の順に説明する。システムの詳細は活動内容で記載する。

3.1. 対策手法の検討

3.1.1. ボット感染PCの利用者を見つける

ボット感染 PC の利用者を見つけて注意喚起する上で重要なことは、見つけたボット感染 PC の利用者に対して確実にボットに感染していることを説明できることである。特に ISP からボット感染 PC の利用者に注意喚起する場合、ISP が何を根拠に注意喚起するのかを明確にしておく必要がある。

本プロジェクト開始前における ISP から感染 PC の利用者への注意喚起のトリガーはメール添付型ウイルスの受信者や Blaster、Sasser 等の明らかにウイルスから連続した大量の攻撃を受けた被害者等が容易にウイルスと判断できる場合の ISP への申告が主であった。

一方、感染攻撃により感染したボット感染 PC の利用者は、感染したこと自体に気がつくことが少なく、例え気がついたとしても、どの IP アドレスからの攻撃で感染したのかを特定および立証することは困難である。さらに ISP への申告があったとしても ISP は申告内容が正しいかどうかを判断することは困難である。

そこで、早期にボット感染 PC から行われる感染攻撃を見つけ出し、ボット感染 PC の利用者に対して注意喚起し、駆除および対策させることが急務とされ、本プロジェクトでは、多くのボット感染 PC から行われる感染攻撃を効率的に見つける方法を検討した。

ボットは、ボット感染 PC が利用している IP アドレスの近接アドレスに対し、PC の脆弱性を利用した感染攻撃を行うため、ボット感染 PC が利用する IP アドレスに近接した IP アドレスにハニーポットを設置することで、効率的に攻撃事象を収集することができるようにした。これらの感染 PC の多い IP アドレスレンジ帯をカバーするために、多数の ISP の協力によりこの IP アドレスレンジ帯を用意することが出来た。

ボット対策システム運用グループでは、このようなハニーポットを多数運用し、ハニーポットへ感染攻撃をしてきた攻撃元 IP アドレス（感染 PC が利用する IP アドレス）、タイムスタンプを記録することでボット感染 PC の利用者を見つけている。

ハニーポットは一般的に特定のオペレーティングシステム（以下「OS」という。）やソフトウェアをエミュレートするロー・インタラクション型ハニーポット [1]と「本物」のOSを用いたハイ・インタラクション型ハニーポット [2]に大

[1] ロー・インタラクション型ハニーポット：マイクロソフト社 OS の主要な脆弱性をエミュレートし、すばやく攻撃を検知し処理することが可能である。攻撃情報に関して、時刻、通信プロトコル、送信元 IP、送信元ポート、宛先 IP、宛先ポート、Exploit タイプを記録することができる。

別され、本プロジェクトではハイ・インタラクション型ハニーポットを採用している。ハイ・インタラクション型ハニーポットは「本物」のOSを使用することから、実際のボット感染PCの利用者が利用する環境と近い環境でボットに感染させることができる。

またハイ・インタラクション型ハニーポットではボット感染 PC からの感染攻撃を観察できるだけでなく、実際に感染させることでボット本体を収集することが可能である。実際にボットを収集できることは以下の 2 つの観点で有効である。

一つ目は、ボット感染 PC からの感染攻撃により感染させられたボットを記録・保存することで、感染攻撃を行ったボット感染 PC がどのボットに感染しているかを証拠としてボット感染 PC の利用者へ説明できることである。こうした証拠を示すことで、ISP は自信を持ってボット感染 PC の利用者に注意喚起をすることが可能となる。

二つ目は、収集したボットに対応した CCC クリーナーを作成できることである。ボットを収集した時点で CCC クリーナーが未対応であった場合、注意喚起を受けたボット感染 PC の利用者はボットを駆除できない。そこで未対応であった場合には、迅速にパターンファイルを作成し、CCC クリーナーに反映した時点で ISP より注意喚起を行う対策システムを提供している。

3.1.2. ボット感染PCの利用者への注意喚起

ボット感染 PC の利用者を見つけた次のステップは、ボット感染 PC の利用者への注意喚起である。

注意喚起の手法としては、ISP の加入者全員に対しメールや Web サイトにより注意喚起を行う広報手法と、ボット感染 PC の利用者個々に対しメール、電話、封書で郵送等により注意喚起を行う個別手法が考えられる。

広報手法は、注意喚起の稼働の観点から、比較的簡単な方法ではあるが、ボットに感染しているかどうかに関わらず送信することから、ボット感染 PC の利用者に対策をしてもらうという本来の目的につながりにくい。同様に Web サイトのトップページなどへ注意喚起の掲示を行った場合でも、そもそも、対策を案内する Web サイト(以下、「対策サイト」という)自体を見てもらえない可能性が高い。

個別手法は、ボット感染 PC の利用者に対して個別に通知するため、利用者に読んでもらえる可能性が高くなり、利用者自身に所有する PC がボットに感染していることを認識してもらえるため効果的である。

よって個別手法を採用し、注意喚起の伝達手段としてメール送信を採用した。

また、従来 ISP が行っていたウイルス感染 PC の利用者への注意喚起は、メールに対策手順を長文で記したものであったが、メールでの説明には限界があり確実な対策を行うことが望めない。このため、メールと Web サイトを組み合わせ、メールのみでは伝えづらい具体的な対策手法を Web サイト上で図等を用いて様々なレベルの方にも分かりやすく、伝える手法を採用した。

なお、ISP からの注意喚起メールには、注意喚起文とともにに利用者を識別するトラッキング ID 付きの対策サイト URL を記載し、これにより感染 PC のユーザ毎に対策の進捗状況を把握することが可能となっている。この手法の採用で注意喚起メールでは、対策サイト URL を記載するため、フィッシング等の詐欺的手法に間

---

[2] ハイ・インタラクション型ハニーポット：マイクロソフト社 OS を仮想 OS として採用し、実際に感染させ一定時間毎にリセットを行うことで感染後にダウンロードするボットの本体など様々なタイプのマルウェアを捕獲することが可能である。ボットの情報に関して、時刻、通信プロトコル、送信元 IP アドレス、送信元ポート、宛先 IP アドレス、宛先ポート、ファイルサイズ、SHA1 ハッシュ値、ファイル名、ディレクトリ名を記録することができ、攻撃元のボット感染 PC の利用者も特定できる。

違われる可能性がある。また、フィッシング等の防衛手段として関係団体が安易にクリックしないという対策をアナウンスしている状況もある。このため、注意喚起メールの信頼性を如何に高めるかが重要となる。そこで送信元をボット感染 PC の利用者が加入しているISPとし、メール本文内に本プロジェクトが国の施策であること、URL は日本国政府を示す go.jp ドメインとしサーバ証明書を取得し、SSL とすることで、第三者機関からのサイト証明を行うことで信頼性を高めている。

3.1.3. 注意喚起を効果的かつ効率的にする手法

ISP が多数のボット感染 PC の利用者に対して注意喚起メールを送信するにあたり、ISP のカスタマーサポートの負担を出来る限り少なくし、数多くの注意喚起メールを効率的に送信できること、また注意喚起を行ったボット感染 PC の利用者の対策進捗状況に応じて再注意喚起メールを送信するなど柔軟な対応ができる事等を検討した。この検討は、注意喚起活動において ISP の協力が必須であり、ISP がプロジェクトに参加するか否かの判断材料ともなるため重要な意味を持っていた。

具体的には個々のボット感染 PC 利用者の対策進捗状況と今までの感染履歴を管理する進捗管理システムと、それと連携し注意喚起メールを容易に送信する機能を持つ注意喚起システムを ISP に提供している。

注意喚起システムは ISP が手間をかけずに個々の注意喚起メールの本文作成や、送信間隔等を自動的に調整しながら運用できる環境※1 を提供している。これは「シナリオ」、すなわち、状態とその時のイベント（事象）により次のアクションと次の状態をあらかじめ定義し、定義した流れに従って動作するもので、これにより効率的な運用を実現し、ISP オペレータの負担は低減することが出来る。

注意喚起を受けたボット感染PCの利用者が効果的にボットを駆除する手段として、ボット専用の駆除ツールであるCCCクリーナーを提供することとした。CCCクリーナーを提供する理由としては誰でも、ソフトウェアのインストールなしで簡単に使用できること、既にインストールされたウイルス対策ソフトと競合[3]を起こさないことなどから、ツール型のCCCクリーナーを提供することとした。

また、ウイルス対策ソフトをインストールしていない PC の利用者は、ウイルス対策ソフトを導入し常時保護ができるようにすることが重要であるが、ボットに感染した状態では、ボットが行うhosts改ざん、レジストリ改ざん、プロセスの停止等、セキュリティを高めることに対する阻害を行うことから、ウイルス対策ソフトをボットの影響なしにインストールさせるためには、あらかじめボットの駆除を行っておく必要があった。

また、ボット感染駆除のための対策サイトは、対策の方法について曖昧さや、不明な点が多いと、注意喚起を行ったISPへの問い合わせの増加を招き、ISPのカスタマーサポート[4]に過度の負担となる。このため、様々なレベルの利用者にも分かりやすいボットの対策方法を記述した対策サイトを用意し、ISPにボット駆除のための取り組みに参加してもらいやすい環境を整えている。

※1　具体的には注意喚起メールの送信間隔、送信回数に応じた本文の内容選択出来るほか、ボット感染 PC の利用者の種別（企業／個人）、新規感染 or 再感染、複数感染の有無等をパラメータとした自動調整が可能である

[3] プロジェクト発足当時はウイルス対策ソフトでは検出できないボットが多数あり、ウイルス対策ソフトをインストールしていても感染してしまった場合があったため、ウイルス対策ソフトとの競合を考慮した。

[4] ボット駆除の対策方法等の案内は、本来 ISP のサポート範囲外。

3.2. 活動内容

ボット対策システム運用グループが行っている注意喚活動は、大まかには次の 3 つに分類される。

(1) ボットを収集する

ハニーポットシステムを設置し、ボットを収集する。収集したボットは、ボットプログラム解析グループに引き渡す。

(2) ボット感染PCの利用者を見つける

ハニーポットシステムで収集したボットの感染ログ(IP アドレス、日時)を当該参加 ISP に提示し、その時にその IP アドレスを利用していたボット感染 PC の利用者を見つける。

(3) ボット感染PCの利用者に注意喚起する

利用 ISP よりボット感染 PC の利用者へ、ボット感染に対しての注意喚起メールを送信する。注意喚起メールには、ボットを駆除するための対策サイト(図 3-1)の URL を記載しており、その URL には、ボット感染 PC の利用者毎に異なる文字列(トラッキング ID)を埋め込んでおり、進捗状態を ISP 側で確認することが可能となっている。

ボット感染 PC の利用者は、受信した注意喚起メールの内容に記載された対策サイト URL にアクセスすることで、「ボットの危険性」に関する説明を理解し、最初に Microsoft Windows Update を行い、CCC クリーナーのダウンロードを実施し、ダウンロードした CCC クリーナーによりボットの駆除を実施する。 その後の作業として、ウイルス対策ソフトのインストールの実施を推奨している。対策サイト上の「完了連絡」によりISP に対して完了の連絡を実施する。ボット対策システム運用グループでは、この一連の利用者が行う対策内容によりボット感染 PC の利用者の対策状況を確認している。

図 3-1 対策サイト

運用グループでは注意喚起活動を効率よく行うために、ワークフローを設計し、それを効率化するためのシステムを構築した。次章では、ワークフローおよびシステムの説明を行い、さらに課題とその対策について説明する。

3.2.1. ワークフローおよびシステム

注意喚起活動を効率よく行うためのワークフローを図 3-2 に示す。

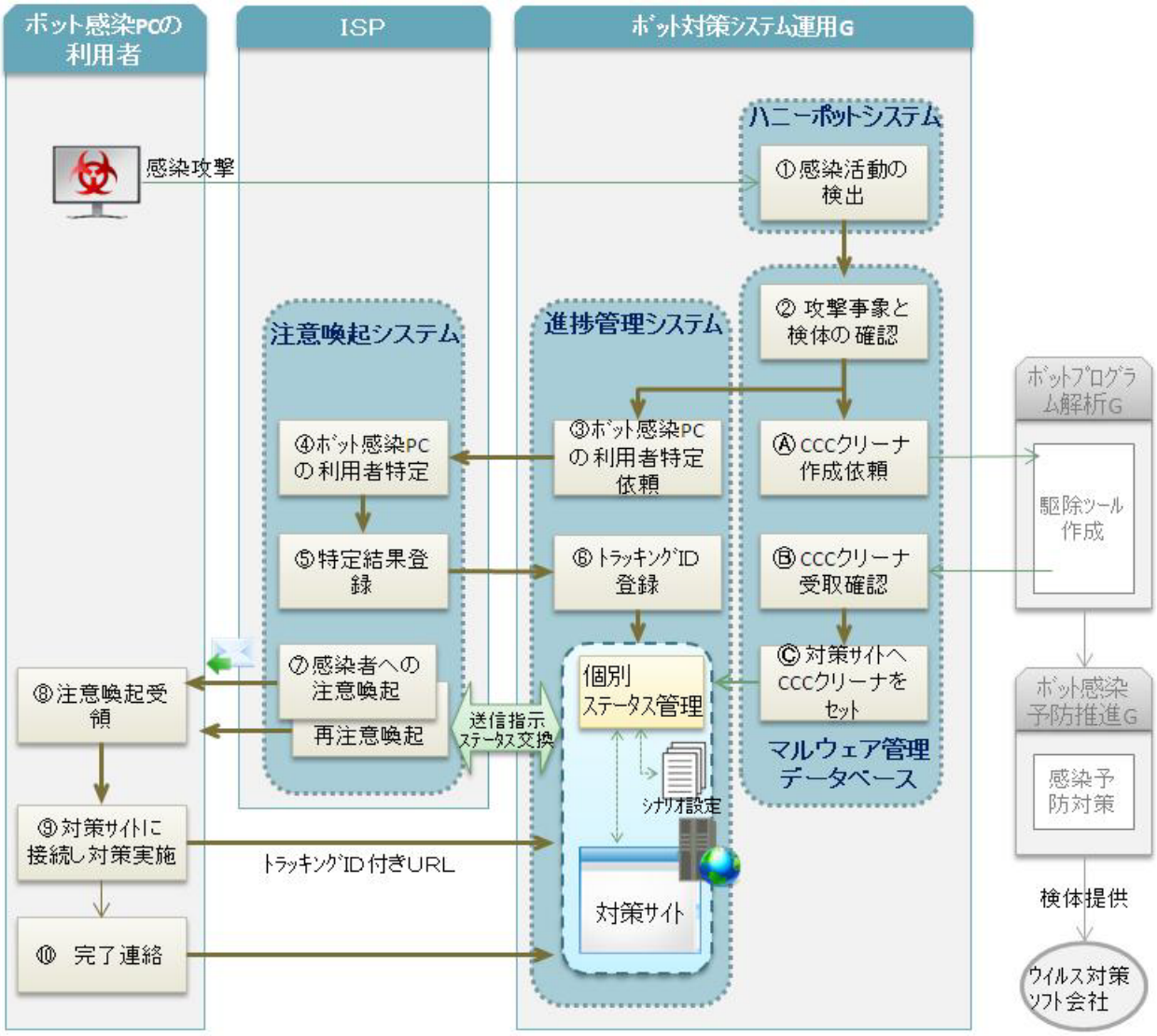


図 3-2 ワークフロー図

ワークフローの概要は以下のとおりである。

① 感染攻撃の検出（ボット対策システム運用グループ）

ハニーポットシステムを利用して、ボット感染 PC からの通信を観察し、ボット感染 PC の攻撃元の IP アドレス、感染攻撃時刻情報などを収集する（攻撃事象）とともにボットを収集する。

② 攻撃事象と検体の確認（ボット対策システム運用グループ）

ハニーポットシステムで収集したボット検体と付随する攻撃事象情報を取得する。ボット検体についてはすでに取得したことのあるボット検体であるかどうかを照合し、新規に収集した検体については、ウイルス対策ソフトを使用し対応済みかどうかを確認する。攻撃事象についてはデータベースに登録する。

(A)　CCC クリーナー作成依頼（ボット対策システム運用グループ）

新規に収集した検体は、攻撃件数、②で調査したウイルス対策ソフトの対応状況の情報とともにボットプログラム解析グループに引き渡し、CCC クリーナーの更新を依頼する。

(B)　CCC クリーナー受取確認（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が更新した CCC クリーナーを受け取り、対象となるボットが駆除できるか、異常動作はしないかの動作確認をする。

(C)　対策サイトへ CCC クリーナーをセット（ボット対策システム運用グループ）

最新の動作が完了した CCC クリーナーを対策サイトへアップロードし、ボット感染 PC の利用者がダウンロードできる状態にするとともに、対応した検体の反映情報を入力し対象となる注意喚起をスタートさせる。

③　ボット感染PCの利用者特定依頼（ボット対策システム運用グループ）

攻撃事象の攻撃元 IP アドレスから該当する ISP を特定した後、ボット感染 PC の利用者を特定するためのボット感染 PC の利用者特定依頼リストを生成し、ISP へ生成したリストを引き渡し、ボット感染 PC の利用者の特定を依頼する。

④　ボット感染PCの利用者特定（ISP）

注意喚起システムにより取得した攻撃事象データ（攻撃元 IP アドレス、感染攻撃時刻情報）よりボット感染 PC の利用者を特定するとともに、注意喚起に必要な氏名、Email アドレス等のデータ、及び利用者が個人、企業、サービス提供事業者かのデータを入力した特定結果リストを作成する。

⑤　特定結果登録（ISP）

注意喚起システムを使用して、前項で作成したデータを入力し、進捗管理システムとの間でユーザを一意に利用者を判別させるようにするための U_ID を割り当てを行い個人情報などの削除(フィルタリング)した上で特定結果リストを進捗管理システムへ登録する。

⑥　トラッキングID登録（ボット対策システム運用グループ）

進捗管理システムは、特定結果リストの登録により、トラッキング ID を付与し、データベースに登録する。

⑦　感染者への注意喚起（ISP）

進捗管理システムは、各 ISP の設定したシナリオ条件、CCC クリーナーの対応状況に従って進捗管理を行い、注意喚起依頼リストを生成する。ISP は注意喚起システムにて進捗管理システムから注意喚起依頼リストを取得し、シナリオのステータスに応じた注意喚起テンプレートを用い、ボット感染 PC の利用者に対して注意喚起メールを送信する。（封書の場合もあり）

⑧　注意喚起受領（ボット感染PCの利用者）

ボット感染 PC の利用者は、利用している ISP よりボット感染の事実と対策の必要性とともに対策サイトの URL（トラッキング ID 付き）の記載された注意喚起メールを受け取る。

⑨　対策サイトにアクセスし対策実施（ボット感染PCの利用者）

注意喚起を受けたボット感染 PC の利用者は、注意喚起メールに記載された対策サイトの URL（トラッキング ID 付き）にアクセスし、提示された内容に従ってボット駆除を実施する。

⑩　完了連絡（ボット感染PCの利用者）

ボット感染 PC の利用者は、対策サイトの駆除・対策手順に従ってボット駆除を行った後、対策サイトに表示される完了連絡ボタンをクリックすることにより、ボット駆除の完了を進捗管理システムへ送信する。進捗管理システムは、これによりシナリオを完了とし、その注意喚起をクローズする。

3.2.2. システムによる業務効率化

(1) ハニーポットシステム

ハニーポットとは、ボットをはじめとするマルウェアや、攻撃元の情報の収集を行うシステムである。ボットは、PC に感染すると隣接した IP アドレスに対して感染攻撃を行い、感染攻撃が成功した場合は PC を制御して感染を拡大する特性を持つ。

本プロジェクトの開始にあたっては、PC の利用者の環境に近い方がボットとともにボット感染 PC の利用者を確実に検知できるであろうという理由で、ハイ・インタラクション型ハニーポットであるマルウェア収集型ハニーポットを採用した。ハニーポットは一般的にマルウェア以外のファイルも収集してしまう傾向があるが、本プロジェクトのハニーポットでは、ホワイトリスト機能を実装しており、特定のファイルやディレクトリに関してはマルウェアとして扱わないことで、マルウェア以外のファイルの混入を防ぎ、解析にかかる負荷を軽減することができる。

ハニーポットはネットワークの設計方法によって、マルウェアを収集する能力や、攻撃元の情報を収集する能力は大きく違ってくる。以下は、ハニーポットの能力を最大化するための工夫である。

①　ハニーポット間で感染をしないための設計

ボットは、ハニーポットに感染するとネットワークを経由して周辺のハニーポットの脆弱性に対する攻撃を行うためマルウェア収集型ハニーポットでは、互いに感染攻撃を受けパフォーマンスが低下する可能性がある。そこで、ハニーポット毎にネットワークセグメントを分離し、ファイアウォール等でハニーポット間の通信を遮断する設計とした。

②　日本国内のボット感染PCを効率的に検知するための設計

ボットは、感染した PC の持つ IP アドレスの近接 IP アドレスに対して感染拡大活動を行う特性がある。この特性を利用し、日本国内のボット感染 PC を効率的に検知するために、ボット感染 PC と IP アドレスの近い、コンシューマ向け ADSL、及び光回線を収集用の回線とし多数 ISP から複数回線接続した。

さらに、広範な IP アドレスをハニーポットに割り当てるため、動的 IP アドレス回線の特性を生かし定期的に回線の切断、接続を繰り返すようなルータを開発した。

(2) マルウェア管理データベース

マルウェア管理データベースは、ハニーポットシステムで収集した感染攻撃事象を整理し、必要なときに情報が引き出せるよう情報をデータベース化したシステムである。このシステムでは、ハッシュ値を比較することによってハニーポットシステムで収集したボット等マルウェアがすでにデータベースに登録されているか否かを確認し、未登録であるマルウェアのみデータベースに登録する。

新しく登録されたマルウェアは駆除ツールを作成するためにボットプログラム解析グループへ送付される。

ボット対策システム運用グループでは作成された駆除ツールをボットプログラム解析グループより受け取ると動作確認を行い、対策サイトへアップロードし、ボット感染 PC の利用者が使えるようにする。

(3) 注意喚起システムと進捗管理システム

ボット感染 PC の利用者に注意喚起を行うためには、ISP の協力がなければ、この活動を進めることは困難である。ISP が注意喚起にかかわる業務の負担を低減するために下記のコンセプトの基にシステムを構築した。

- ●注意喚起を行った利用者が、対策サイトにアクセスしたのか、どこまで実施したのか完了したのか等の進捗管理を行えること。
- ●注意喚起メールの送信にあたっては、個別メールの送信を短時間で行えること。(差し込みメール送信)
- ●注意喚起間隔、複数回注意喚起をしていく段階での注意喚起文の変更など、きめ細かに設定できること。
- ●駆除・対策手順を案内する対策サイトの内容がわかりやすく、ユーザ自身で実施可能であり、ISP への個別問い合わせの増大につながらないこと。
- ●個人情報は ISP のみが把握し CCC が管理するサーバ上では、一切保有しないこと。

注意喚起システムと進捗管理システムにおける特徴を以下に示す。

① トラッキングIDを使用した進捗管理

ボット感染 PC への対処状況の進捗管理は注意喚起ワークフローの要である。この管理はトラッキング ID で実現した。実現方法をトラッキング ID の付与手順(図 3-3)とともに示す。

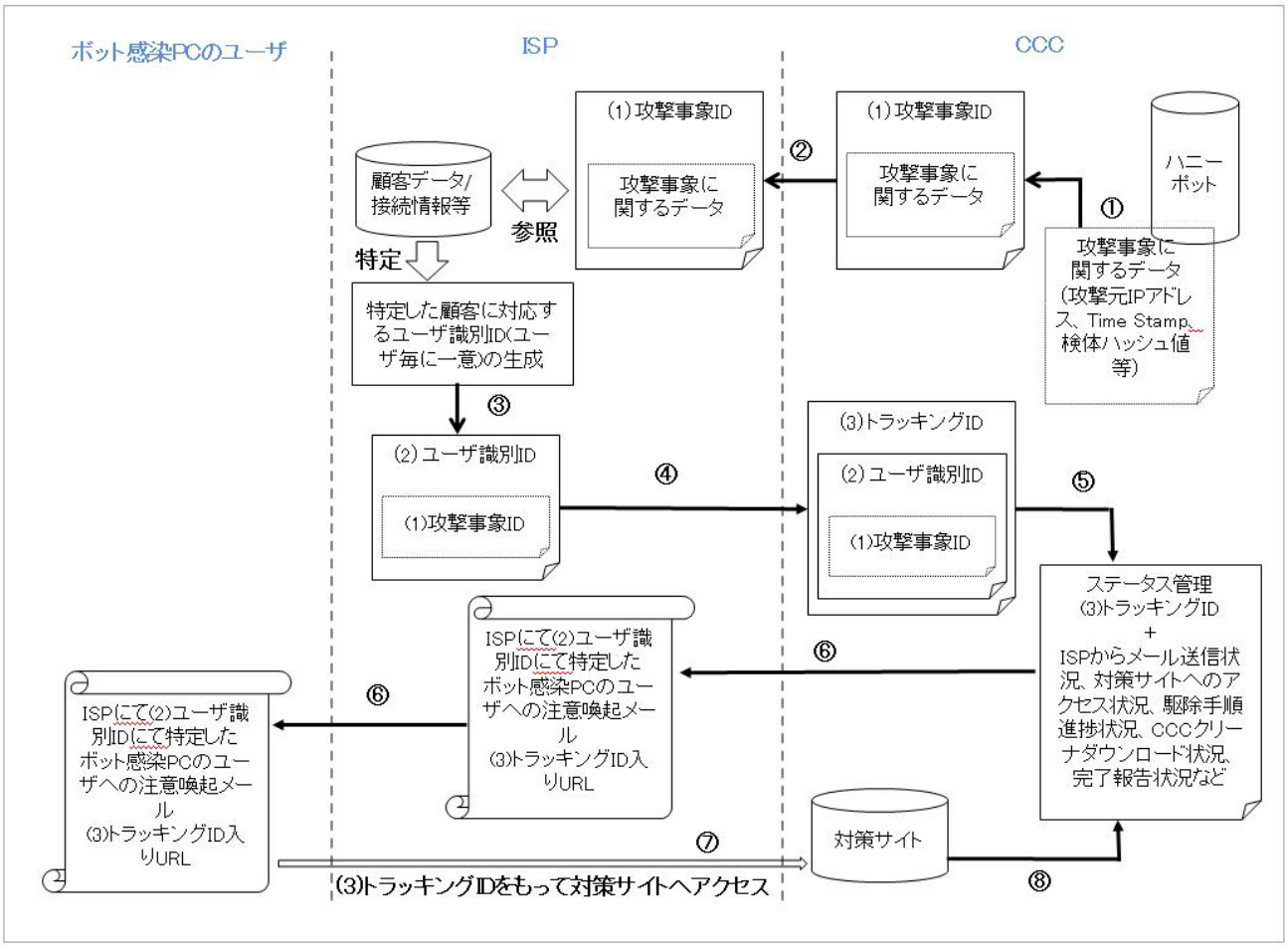


図 3-3 トラッキング ID の付与手順

i. トラッキング ID 付与手順

CCC では攻撃事象に関するデータ(発信元 IP アドレス、発信日時、検体ハッシュ値等)をハニーポットで収集し、これらのデータに CCC で攻撃事象 ID を付与する(図 3-3①)。攻撃事象 ID を付与したデータは攻撃元 IP アドレスを手がかりに当該 ISP へ送付する(図 3-3②)。ISP は受領したこれらのデータと自社内の顧客情報、接続情報などと突合してボット感染している顧客を特定する。ISP は個人・顧客情報保護・通信の秘密の観点からむやみに特定者情報を開示できない。代わりに、ISP はユーザごと一意にユーザ識別 ID を付与し、CCC へ送付する(図 3-3③)。CCC はこの情報に対して、トラッキング ID を一意に付与する(図 3-3④)。CCC ではトラッキング ID を使い、この攻撃情報に対する駆除手順の進捗に係る情報(ISP からのメール発出状況、対策サイトへのアクセス状況、対策サイト内での駆除手順の進捗状況、CCC クリーナーダウンロード状況、完了報告状況など)をステータス情報として管理する(図 3-3⑤)。また、CCC は ISP に対してトラッキング ID を指定し、注意喚起メール送信を依頼する。ISP はトラッキング ID と対応づいたユーザ識別 ID を手がかりにボット感染ユーザへ注意喚起メールを送信する(図 3-3⑥)。ISP から注意喚起メールを受け取った感染ユーザはメール本文中のトラッキング ID 入り URL を使い対策サイトへアクセスする(図 3-3⑦)。対策サイトでの行動やボット駆除手順進捗状況はトラッキング ID をキーにステータス管理する(図 3-3⑧)。

ii. トラッキング ID によるステータス管理

感染ユーザの中には、複数種類のボットへの同時感染、再感染、メールを何回出しても対策サイトにアクセスしない、対策サイトで案内した対策手順の最後までたどり着かず途中でやめるなど、様々な状況がある。トラッキング ID による記録情報の分析からこれらの状況が分かる。新規の攻撃事象に対して、CCC で攻撃事象 ID に A を付与すると、ISP 側では攻撃事象 ID A に対してユーザ識別 ID B を付与する。次に、CCC ではユーザ識別 ID B に対してトラッキング ID C を付与したとする。別の攻撃事象 A2 に対して同じユーザであればユーザ識別 ID B が付与されるので、攻撃事象 ID A と A2 の攻撃事象に関するデータのうち検体に関する情報（例、ハッシュ値）などを比較し、別の検体であれば複数種類のボットへの同時感染と判断できる。また、ユーザ識別 ID B のボット感染ユーザがステータス管理上、完了報告をしていた場合、その後に新規の攻撃事象 A3 を捕獲し、ISP 側でこれに対してユーザ識別 ID B を付与した場合には、再感染と判断できる。CCC では駆除手順進捗を完了報告まで状況管理をしているのでユーザ識別 ID で進捗の状況の判断ができる。

また、CCC はトラッキング ID を元に ISP に注意喚起メール送信依頼を行うので、攻撃事象 ID に対して発出したメール回数が判明する。ISP 側では発出回数に応じて、（文面を次第に強い表現にするなど）メール本文の入れ替える段階的対応が可能になる。ISP からメール送信の際にこの段階的対応を省力的に実現する目的で、CCC は ISP に対してメール送信ツール（注意喚起クライアント）を提供した。これには段階的な文面をあらかじめセットでき、CCC から送られてきた（メール発出回数などの）ステータス情報入りの送信リストをもとに、クライアントツールの中で発出回数にあわせた文面を自動的に読み込み、メール送信を行う。

② 対策サイトの開設

従来 ISP が行っていたウイルス感染 PC の利用者に対する注意喚起においては、メールに駆除手順を記載して案内を行っていた。しかし、この方法では、利用者の理解度は低くなり、結局対処を行わない、行えないユーザが多くなり、完了率の低下を招き、さらに注意喚起稼働を引き上げる悪循環となっていた。このため、駆除から再感染防止対策までの手順をわかりやすく記載した対策サイトを設け注意喚起を受けた利用者が、出来るだけ自身で対処できるようにしている。また、この対策サイトは、利用者個々に一意のトラッキング ID を付与した URL を入れ注意喚起を行い、利用者が対策サイトにアクセスしたのか、どの手順まで実施したのかを確認でき、駆除・対策の完了も対策サイト上から行うようにしている。ここで、取得したデータは進捗管理システムで管理し注意喚起ステータスの管理を行っている。また、ユーザ個別の感染状況、及び対策状況を ISP のサポートと共有することで、ユーザサポート及び注意喚起対策の変更などの検討に生かされている。

(4) 一般公開サイト

ISP 経由での注意喚起で設けた対策サイトとは別にボット対策用の一般公開サイト（https://www.ccc.go.jp/）を用意している（図 3-4）。このページは、広く一般のユーザに情報を共有することにより、「ボットの脅威」に対する認知度の向上を目指すために用意した。誰でもボットウイルスに感染しているかをチェック・駆除することができ、ボットに感染しない安全なPC環境を作るための手順等も紹介している。また、全てのボット感染ユーザをハニーポットシステムで見つけることはできないため、このサイトは、メディア等を通じて幅広く広報的に注意喚起する場合の参照先として利用している。

図 3-4 一般公開サイト

3.2.3. プロジェクト開始後の課題と対策

注意喚起システムと進捗管理システムを運用することにより、ボットの収集、ボット感染 PC の検出、そしてボット感染 PC の利用者への注意喚起というプロセスで、注意喚起活動を行うことが可能となった。注意喚起活動の開始当初は想定していたとおり、多くのボットを収集し、ボット感染 PC を検出することができた。ところが、2009 年に入り収集できるボット数と検出できるボット感染 PC の利用者が減少に転じた。この減少は、CCC の活動成果によるボット感染 PC の減少だけでなく、ハニーポットシステムに対する攻撃側の対抗措置が取られていることも考えられた。そこで、新たな方式のハニーポットシステムの導入を行った。また、注意喚起活動を効率化する活動や改善を行っている。

これらの注意喚起対象者の減少に対する対策と、注意喚起活動を効率化する活動の一環である対策サイトへの訪問率の取り組みを以下に紹介する。

(1) 注意喚起対象者数の減少に対する対策

① 攻撃事象検知型ハニーポットの採用

マルウェア収集型ハニーポットでは、設計時のポリシー「見つけたボット感染 PC の利用者に対して確実にボットに感染していることを説明できること」に沿って、感染攻撃元からボットが収集できた IP アドレスのみ注意喚起の対象とし、感染攻撃のみでボットが収集できない事象や収集したボットが動作しない事象については注意喚起の対象としていなかった。

2008 年 10 月からマルウェア収集型ハニーポットによる注意喚起対象者数が減少に転じ、実際の

感染率と収集数に大きな差異が見られるようになった。また、2007 年 11 月から導入した CCC クリーナーのログ報告機能（後述（4）-①項　CCC クリーナーのログ収集）により、注意喚起を行った感染 PC の感染の実態も把握できるようになり、必ずしもユーザは、CCC で捕捉したボットのみではなく、非常に多くのマルウェアに感染し、未知のウイルスにも多く感染している状況であった。このため、当初の「ボットを捕獲できた IP アドレスのみに注意喚起を行う」という考えではなく、ウイルス感染の事実を早期に伝えることが重要ではないのかという見地に至り感染攻撃のみのユーザを注意喚起対象とするため検討に入った。ただし、単なるポートスキャンのような明確にボットからの感染攻撃と言えない物を排除し、明確に注意喚起の根拠となりうる攻撃のみを識別することが要求され、2009 年 6 月脆弱性攻撃のパターンを識別できるロー・インタラクション型ハニーポットである攻撃事象検知型ハニーポットを導入した。この 2 つのタイプのハニーポットを組み合わせることによって、ボット感染 PC の利用者への効率的な注意喚起と多様なボットの収集を両立している。

(2) 対策サイトへの訪問率向上の取り組み

①　メール送信間隔の最適化

注意喚起システムでは、シナリオの設定により任意にメールの送信間隔、再注意喚起回数を設定できるようにしているが、送信間隔によってボット感染 PC の利用者の対策サイトへの訪問率が異なることが、実施結果より分かってきた。7 日に 1 度、3 回のメール送信を設定していた ISP では、対策サイトへの訪問率が 20%を割った。

調査によるとメールマガジンの場合は、送信日から 3 日までが最も読まれ以降は殆ど読まれないと言われている。また、対策サイトにアクセスがなかった注意喚起対象者に、1 週間後の同じ曜日に送信したとしても、その注意喚起対象者にとっては、その曜日はメールを読まないまたは読んでも実施する時間がない等の理由により実施しないことが想定される。このため、送信間隔を 3 日に一度送信し、メールの読まれる確率を維持すると共に、曜日がずれることにより、実施する可能性を高めるようにし 10%の訪問率向上を実現した。

②　注意喚起メール本文の改良

3 日以内であっても、気がつかれずに読まれない場合も存在する。調査によると、メールの題名に【重要】と書かれているメールは、ダイレクトメールで多用され「本当は重要ではない」という意識がある。このため、メールの題名の書き出しを【重要】ではなく、一般的に使われない【緊急】に変更するとともに、1 文字インデントし、メールのタイトルリスト上で少しずれた表示が行われるようにし、メールを目立たせるような工夫を行った。

また、メールの本文も、ユーザは全てを読まず冒頭の数行のみで判断する傾向があるため、数行以内で自身が危険な状態にあることをわからせる文とすることや、メールマガジンの手法を取り入れ罫線で重要部分を囲むなど重要部分を目立たせる、伝えたい内容を先頭にできるだけ簡潔に配置するといった工夫を行い、アクセス率の向上を図った。

③　封書の郵送による注意喚起

メールによる注意喚起を各 ISP 共に主としているが、ISP のメールを使わずに Yahoo!メール、Gmail 等の Web メールを使う利用者が増えていることにより ISP のメールアカウントに送信しても見られて

いないケースが多く存在する。またメールを受信していて、ISP の注意喚起メールに気づいたとしてもその重要性に気づかないユーザも存在する。

封書による注意喚起を実施した ISP では、メールと比べコストが増え、実施に際しては大きな問題となった。しかし、メールのみの注意喚起では、対策サイトへのアクセス率が 30%と低く対策が進まなかった。読まれていないかもしれないメールを数十通送信しても、対処がされないのでは、封書を送り確実に対処をしていただいた方が効果が期待できるという想定の下、2 回注意喚起メールを送信し、対策サイトにアクセスをしない注意喚起対象者に対し、封書による注意喚起を実施した。

これにより、対策サイトへのアクセス率は、実施前の 30%から 60%に上がったものの、未だ想定より低い状況であった。そこでアウトバウンドコールにて対象者に聞き取りを実施したところ、ISP がユーザに対し送るダイレクトメールと同じ封筒を使っていたため、注意喚起の封書をダイレクトメールと誤認し開封されないケースがあることが判明した。

注意喚起の封筒はダイレクトメールで利用する封筒と異なるデザインのものに変更すると共に、ダイレクトメールで使われる「親展」、「重要」などという記載も避け、封筒の表面に赤文字で大きく回線利用に関しての注意喚起であることが分かるメッセージを印刷することにより、その封書が重要であることを認識していただくことに期待した。これにより、対策サイトへのアクセス率は更にあがり 80%以上を維持できるようになり、注意喚起対象者数も減少に転じるようになった。

④ ISPによる電話サポート

日本の ISP のコールセンターの多くは、ユーザへのサービスの観点から通話料無料のフリーダイヤルを利用し問い合わせも無料で行っている。一方 PC メーカ、OS メーカ、ウイルス対策ソフト会社などは、通話料は発信者負担で、問い合わせ料金も場合によっては有料となるため、ユーザは、ISP へ気軽に相談する傾向がある。しかし、通常 ISP では、マルウェア感染に関しては、サポート外であり問合せがあった場合には、PC メーカ、OS メーカ、ウイルス対策ソフト会社などでサポートを受けるように案内をしている。ただ、対応先では感染した PC の初期化を勧められるのみで、十分なサポートが行われないのが実情である。

また、PC の初期化を行ったとしても、ネットワーク型感染に対しての対策の案内を行うメーカは少ないため、再感染するケースが多いのが現状である。

この様なケースでも適切な案内を行える様に CCC では ISP に日ごろのサポートのための勉強会を実施し、その中で、ウイルス感染が引き起こす事象の説明や、PC の初期化時のルータ機器の重要性等について指導している。

一方、中には、PC メーカ等にサポートを依頼しようとしても、”状況を上手く伝えられない”、”コールセンターにつながらない”、”回復までに何をしたらよいかわからない”など諦めて放置するケースも見られる。実際に進捗状況を見ても一度駆除を行おうとしたが、何らかの理由により断念しそれ以降何もしないユーザが存在する。

このようなユーザは今までの方法で何度注意喚起を行っても、対策を行わない（行えない）ことから、一部の ISP は、サポート範囲外であるが、セキュリティ対策に対し、インバウンドで質問を受け付ける取り組みを実施している。実施 ISP においては、PC の初期化方法などは、パソコンメーカへのサポートを依頼するものの、回復および再感染防止対策までの一連のアドバイスを遠隔サポートを行いながらワンストップで行っており、高い回復率を実現している。

(3) 対策サイトの対策手順の最適化

対策サイトでの現在の対策手順は、以下のとおりである。

1. WindowsUpdate の実行
2. CCC クリーナーの実行
3. ウイルス対策ソフトの導入
4. ルータの導入

初期の頃は、1と2を逆にした手順をユーザに示していた。Windows Update には時間がかかるため、まずは CCC クリーナーでボットの駆除を行った方が良いと考えていた。しかし、この手順では、Windows Update を後にしたことで、CCC クリーナー実行でボットの駆除に成功しても、外部からの感染攻撃で感染する根本原因が修正されていないため、Windows Update を完了するまでの間に再感染をするユーザが多く出てしまった。そのため、先に Windows Update を実行する手順に変更した。また、本来であれば、ルータの導入も同様に、感染源である外部からの感染攻撃を遮断してから行うべきであるが、購入しなければならず、手順の流れが途切れる。購入をしていないから実施しないという行動になることが予想されたため、4番目のままとした。

(4) その他の工夫や改善

① CCCクリーナーのログ収集

当初、CCCクリーナーは、駆除した駆除結果のログ [5]を作成する機能は持っていたが、そのログをCCCへ報告する機能は持っていなかった。CCCクリーナーの機能の向上に役立てるためCCCへ送付し解析に役立てることが可能になった。

但し、ログ送信は無条件に行わず、CCC クリーナーの利用者の同意のもと、送信の可否が選択できる様になっている。

② CCCクリーナーでのWORM_DOWNADウイルス [6]の対策について

CCC クリーナーは Administrator 権限で動作するため、SYSTEM 権限で動作する WORM_DOWNAD を駆除することはできない。一部のウイルス対策ソフト会社は WORM_DOWNAD の専用駆除ツールを提供しているが、既に WORM_DOWNAD に感染してしまっている PC から各社のドメインへのアクセスは阻害されることから、実際にはこうした専用駆除ツールを入手して WORM_DOWNAD を駆除することは難しい。このような状況では、WORM_DOWNAD に感染した PC の回復手段としては、初期化しかなくなる。このことが利用者にとって駆除の大きな障壁となっているだけではなく、そのまま放置されるケースもある。そこで CCC では、トレンドマイクロ社が提供する「WORM_DOWNAD 駆除ツール」を CCC ドメインのサーバで提供することにより、ドメイン阻害を受けることなく駆除ツールの提供を可能とした。

---

[5]駆除結果ログ：利用環境として、PC の OS、OS のサービスパック適応状況、PC の IP アドレス種別（グローバル／ローカル）、PC のメモリ容量駆除結果として、駆除したマルウェア名、駆除した件数、失敗件数を記録している。

[6] WORM_DOWNAD は、マイクロソフトが 2008 年 10 月に修正パッチを緊急リリースした「MS08-067」の脆弱性を悪用するワーム型ウイルスで、脆弱性以外にも USB メモリなどのリムーバブルメディア経由や WEB サイトへのアクセスなどで感染する亜種などもあり、国内での感染被害が増加しているウイルスである。

③ CCCによる電話サポート

CCC では、当初はメールのみで質問を受けメールにより回答を行っていた。しかし CCC クリーナーの利用者がどこで困っているのか、どういう考え方をしているのかなどが、メールでは把握できない。よりよい対策手順や、分かりやすいヘルプを作成するためには、利用者の状況を確実に把握する必要があることから、質問時のメールに電話番号を記入してもらい、コールバックにてユーザのサポートを実施し、手順に反映を行った。

ISP からの間接的な情報だけではなく、利用者と直接対応し、状況を細かく把握することは効果的な対策手順とするために非常に有効な手段である。

④ ISP向けセミナー・勉強会の開催

多くのボット感染 PC の利用者へアプローチしていくためには、より多くの ISP がプロジェクトに参加し注意喚起を行う必要があるため、2008 年から毎年、年 2 回 ISP 向けのセミナーを開催している。開催当初はプロジェクト参加 ISP 数を増加させることが主たる目的であったが、現在では、プロジェクト参加 ISP 数をさらに増加させることに加え、既にプロジェクトに参加している ISP がより効果的に注意喚起活動、対策普及啓発活動ができるよう、最新のボット状況や、ボット対策成功事例等の紹介や情報共有もあわせて行っている。また、2009 年は、ISP のカスタマーサポート担当者向けの勉強会の開催も行った。

3.3. 活動実績

CCC の活動実績として、活動実績を一般公開サイト（https://www.ccc.go.jp/）において、注意喚起活動実績を 2007 年 5 月より、当月分実績と累計の実績を毎月掲載している。

3.3.1. 2010 年 3 月度の注意喚起活動実績

ハニーポットシステムで収集したボット等マルウェアの総数は累計で 1,600 万以上（収集したマルウェアの同定数は 100 万）にもおよび、そのうち約 3 万もの未知のマルウェアを収集した。注意喚起活動はプロジェクト参加 ISP が実施し、累計で約 48 万通のメールによる注意喚起を、約 10 万人の対象者に対して行った。

その結果、注意喚起を実施した対象者のうち、31.6%が CCC クリーナーをダウンロードし、ボット対策を実施した。一般公開サイトにおいては、累計で 120 万回以上の CCC クリーナーのダウンロードが行われている。

2010 年 3 月度に公開サイトに掲載した意喚起活動の実績を図 3-5 に示す。

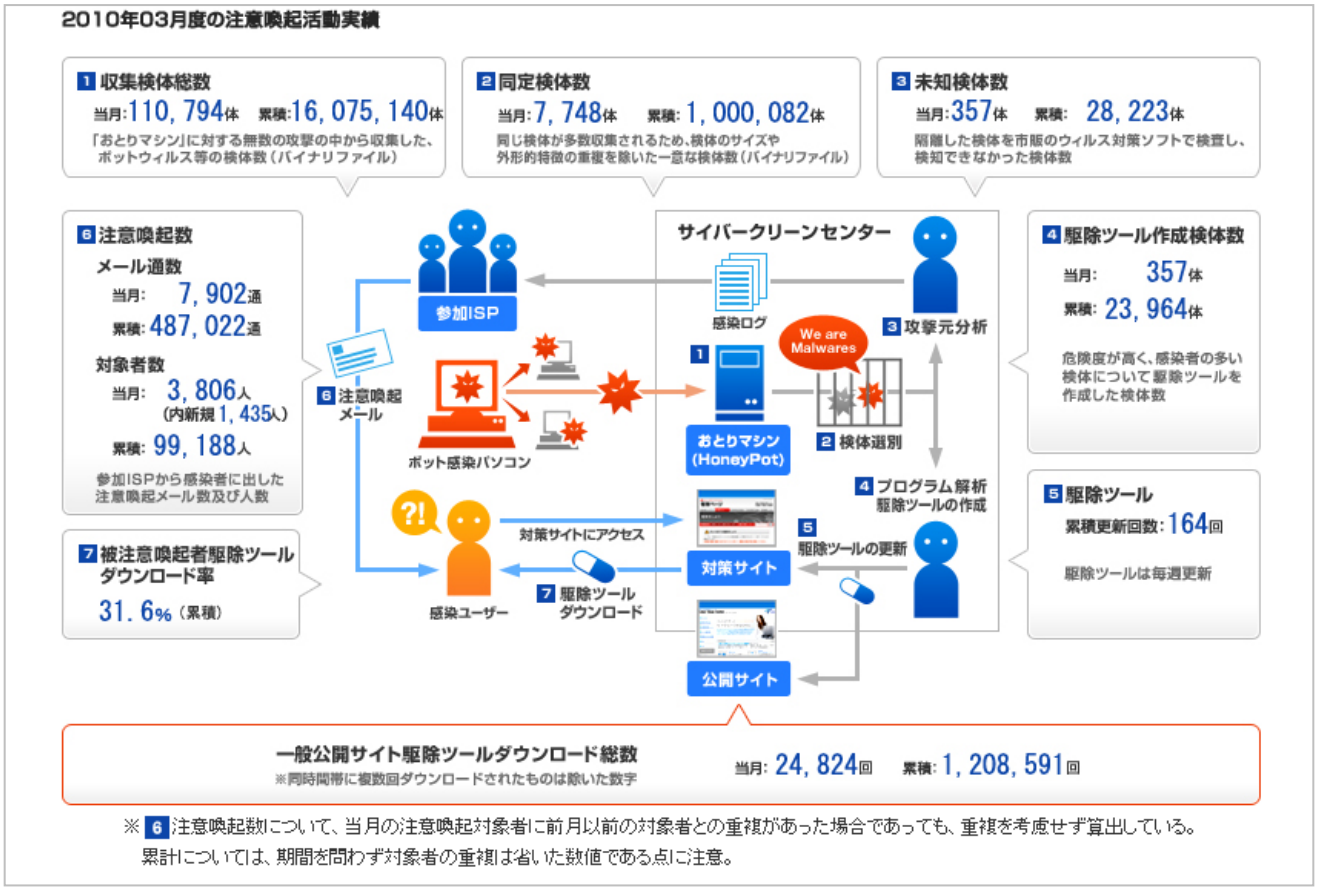


図 3-5 2010 年 3 月度の注意喚起実績

3.3.2. マルウェア収集数の推移

図 3-6 は収集したマルウェア総数の推移を示したものであるが、横軸は時間軸（日単位）、縦軸はマルウェア収集数を表し、青はウイルス対策ソフトで検知した既知マルウェア数、赤が未検知であった未知マルウェア数を表している。

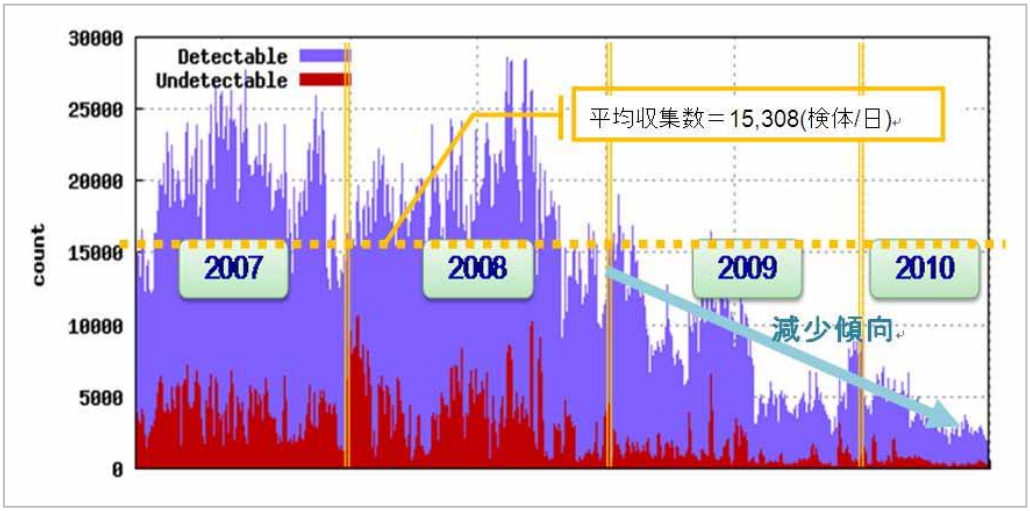


図 3-6 収集したマルウェア総数の推移

収集したマルウェア総数に占める未知マルウェア比率(Undetectable/(Detectable+Undetectable)で計算)は、平均で約 16%となっている。収集数は 2009 年より減少傾向が現れ、2010 年度を見ると減少傾向が顕著に現れている。

各年での特徴的な点を述べると、2007 年、2008 年の年間収集数は既知・未知合わせて 500 万件以上のマルウェアを収集した。理由としては、既知マルウェアにおいては、感染すると PC 内部で他のファイルに次々と感染するファイル感染型のウイルス PE_BOBAX 系、PE_VIRUT 系がハニーポット内部で大量に増殖したためである。

未知マルウェアにおいては、カナダのマルウェア配布サイトより 1 週間サイクルにて新しい未知マルウェアが大量に収集されていたことが挙げられる。2009 年からはファイル感染型ウイルスの減少、カナダのマルウェア配布サイトからの未知マルウェア収集数の減少などにより、収集数は大幅に減少した。

3.3.3. 注意喚起数の推移

注意喚起対象ユーザ数遷移を図 3-7 に示す。この図からは、新規注意喚起対象者数は減少傾向となっており、着実にボット感染 PC の利用者は減少していることがわかる。

再注意喚起対象者も減少傾向ではあるが、2007 年 4 月と 2010 年 6 月を比較すると新規ユーザに比べ減少幅が小さい。これは、初回に注意喚起を行った際に反応のなかった対象者は、再度喚起をしても反応する可能性が低いためと見られる。

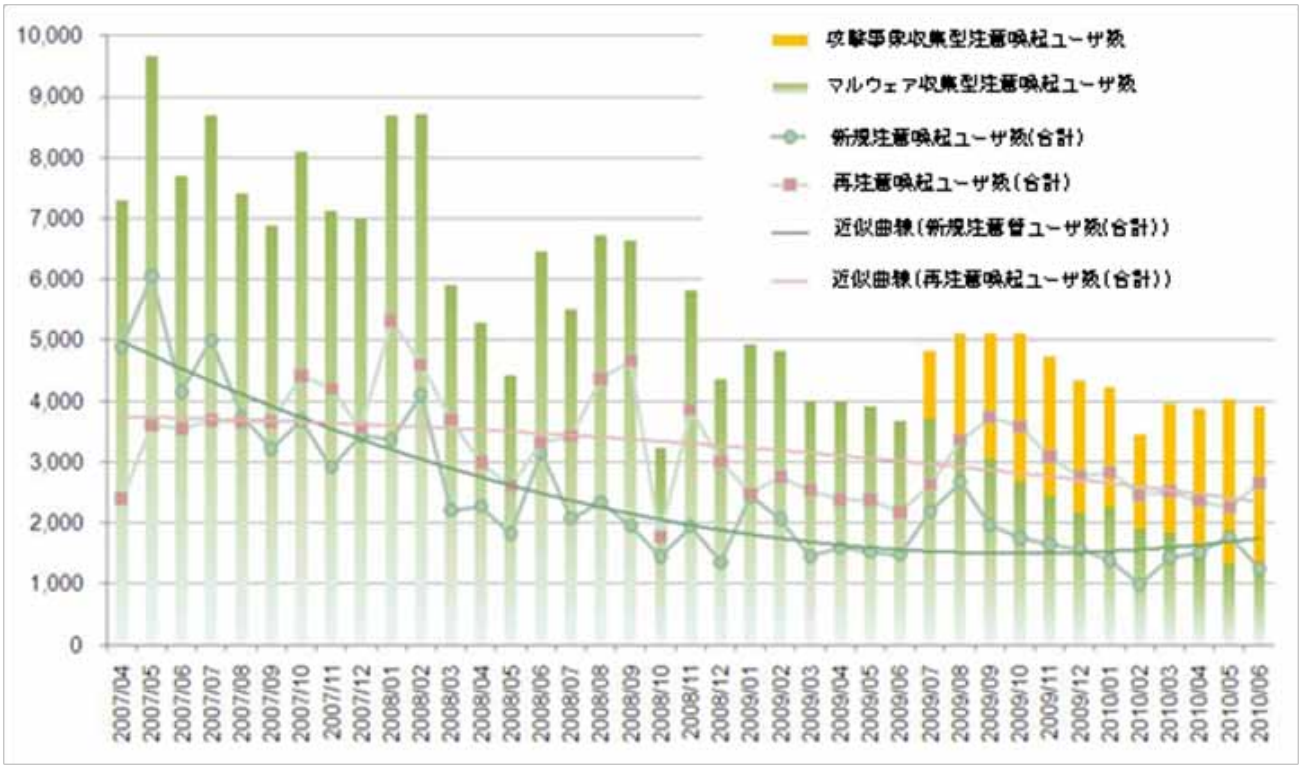


図 3-7 注意喚起対象ユーザ数遷移(2007 年 04 月～2010 年 06 月)

注意喚起対象者の対策サイトにおける対応率（注意喚起したユーザの数を 100 として、対策サイトのトップページへアクセスした割合、それ以降のサイト内での遷移で Microsoft Windows Update へアクセスした割合、CCC クリーナーをダウンロードした割合、最後に完了報告ボタンを押した割合）を年度単位で表したのが図 3-8 である。どの対策項目においても集計開始時の 2007 年に対して 2009 年度は対応率が上がっている。

2007 年度で Microsoft Windows Update と CCC クリーナーダウンロードの対応率がそれぞれ 22%、30%であり、2008 年度では逆転して 43%、29%となっているが、2008 年に手順の順番を入れ替え Microsoft Windows Update を CCC クリーナーダウンロードよりも先にしたためと考えられる。

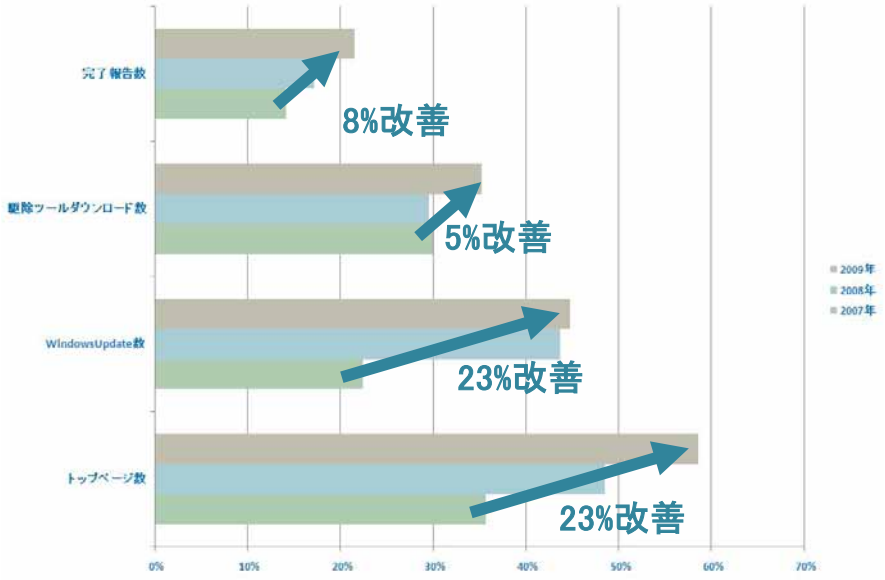


図 3-8 注意喚起対象者の対応率

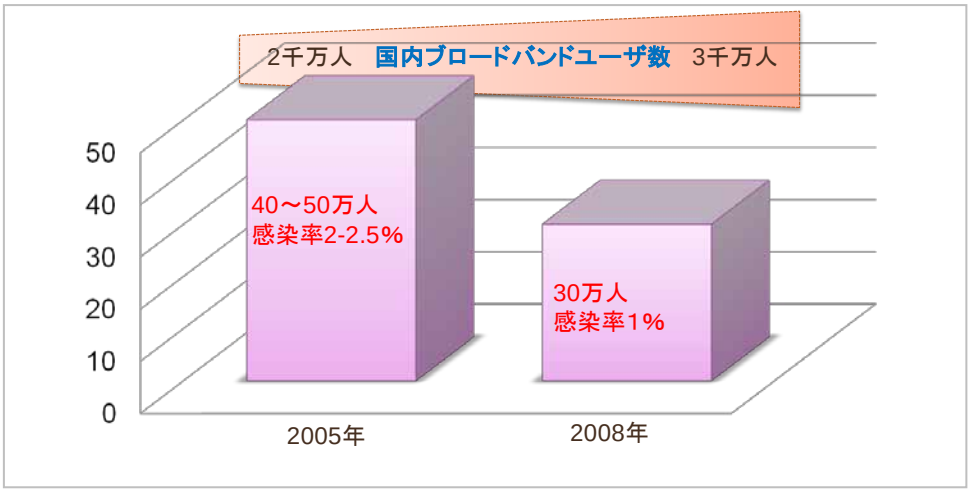
3.3.4. 感染率推移

プロジェクト開始以前の 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 [7]の内約 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。

その後、2006 年にCCCが活動を開始し、ボット対策を行ってきたが、2008 年 6 月にCCCで同様の調査をしたところ、国内ブロードバンドユーザ約 3,000 万人 [8]の内約 30 万人（感染率約 1%）と推計した。

国内ブロードバンドユーザにおけるボット感染者数および感染率の推移を図 3-9 に示す。

[7] 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



【Telecom-ISAC、JPCERT/CC 調べ】

図 3-9 国内ブロードバンドユーザにおけるボット感染者数および感染率の推移

3 年間でブロードバンドユーザ数が 1,000 万人も増加しているのに対して感染率は下がっており、CCC の取り組みによる成果の表れとみられる。ただし、CCC の取り組みだけではなく、PC に搭載される OS がよりセキュアな OS へ移行が進み、インターネットに接続するだけで感染することが少なくなってきたことも、感染率が低下した要因の 1 つと考えられる。

4. ボットプログラム解析グループの活動

4.1. 活動内容

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が運用するハニーポットで収集した検体の解析・分析を実施し、3.1 で説明されているように感染ユーザの感染 PC からボットを駆除するための駆除ツールの作成を中心に活動を行っている。図 4-1 にボットプログラム解析グループの行っている 3 つの活動について示す。

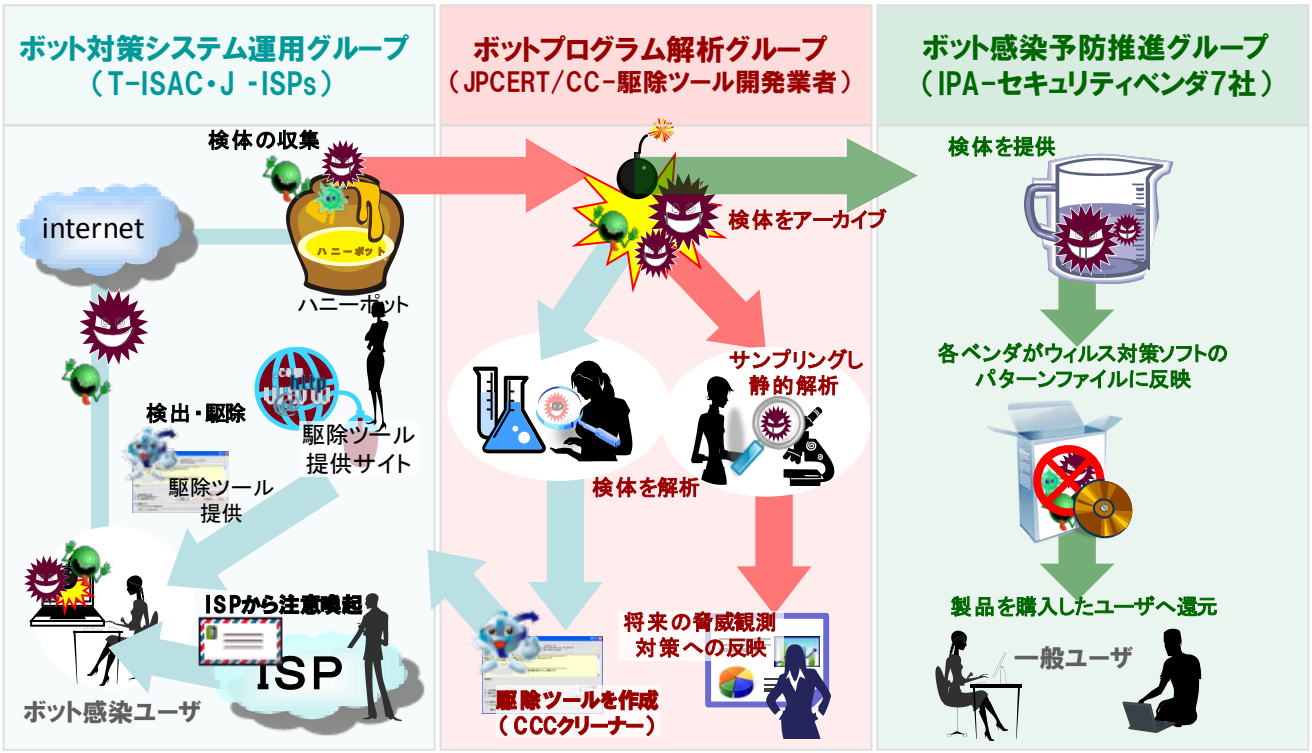


図 4-1 CCC グループの各役割

① 駆除ツール（CCC クリーナー）の作成

ボット対策システム運用グループの運用するハニーポットで収集した検体の解析を行い、解析結果を反映させた駆除ツール（CCC クリーナー）を作成し提供している。

② 収集した検体の詳細な分析

将来の脅威予測や対策への反映を目的として、ハニーポットで収集した検体の中で特徴的な検体を、詳細に分析している。また、2008 年度に CCC クリーナーに実装した検出情報送信機能によって収集したログの分析も併せて行っている。

③ ボット感染予防推進グループへの検体提供

各ウイルス対策ソフトのパターンファイルへの反映を目的とし、収集した検体をボット感染予防推進グループに提供している。

本報告書では、平成21年度に行った活動について、CCCクリーナーの作成と、ログおよび検体の分析を中心として報告する。

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のハニーポットで収集したマルウェア(以下、「検体」という)の解析・分析を中心とした活動を行っている。本項では、ボットプログラム解析グループの活動のうち CCC クリーナーの作成と、ログおよび検体の分析を中心として報告する。

4.2. CCCクリーナーの作成

ボットプログラム解析グループでは、市販のウイルス対策ソフトで未対応の検体について解析を行い、簡易駆除ツールである CCC クリーナーに反映している。

平成 21 年度は、CCC クリーナーの安定的な供給を目的に、運用の見直しによる作業の効率化を推進した。手作業部分の自動化や駆除ツールの動作確認テスト方法の分業化等を推進し、CCC クリーナーの作成(更新)を 164 回行った。また、ハニーポットで収集した検体の CCC クリーナーへの反映状況は、2007 年 2 月からの累積は以下のとおりとなり、反映率は 99.47%となっている。

1) CCC クリーナーに反映した検体数 = 23,964
2) 既知確認検体数 = 970,814
3) 収集した検体の同定検体数 = 1,000,082
4) CCC クリーナー反映率 =(① + ②)÷ ③ ＝ 99.47 %

これは、収集された検体の 99.47%を、CCC クリーナーおよび各ウイルス対策ソフトで検出できるということであり、収集された検体を十分に活用できているといえる。

1) CCC クリーナーに反映した検体数:
   各ウイルス対策ソフトで検出できなかった検体を CCC クリーナーに反映した数
2) 既知確認検体数:
   収集した時点で既に CCC クリーナーが対応していると確認できた検体数
3) 収集した検体の同定検体数:
   同一の検体が多数収集されるため、それら重複を除いた検体数

4.2.1. CCCクリーナーの機能

CCC クリーナーは、ボットプログラムの駆除機能以外にも、使用するユーザの視点で検討し、その結果をツールに反映している。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への警告

ファイル感染型ボットは、実行されるとアプリケーションやシステムファイルといった実行形式のファイ

ルに次々と感染する。このような性質上、完全な駆除が難しく、CCC クリーナーで駆除を行っても感染した状態が続く可能性が考えられる。そのため、CCC クリーナーではファイル感染型を検出した場合にポップアップ警告を表示する。(図 4-2)

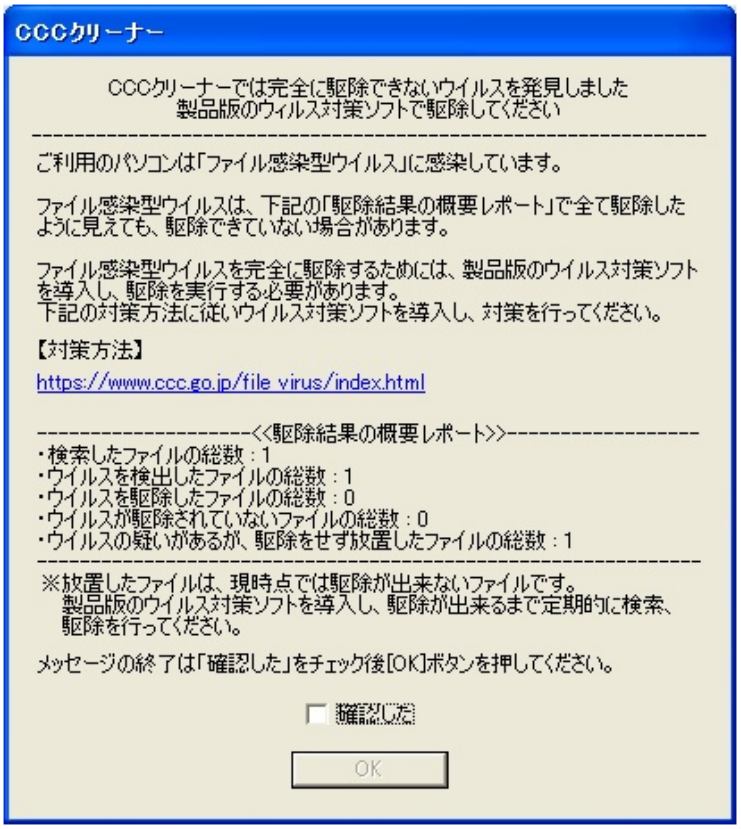


図 4-2 ファイル感染型を検出した場合の警告のポップアップ

また、システムフォルダ以下の重要なファイルが感染しており、かつ駆除ができない状態であった場合、該当ファイルの隔離を行うと OS が起動しなくなる等の問題が発生する可能性があるため駆除作業を中止する。(図 4-3)

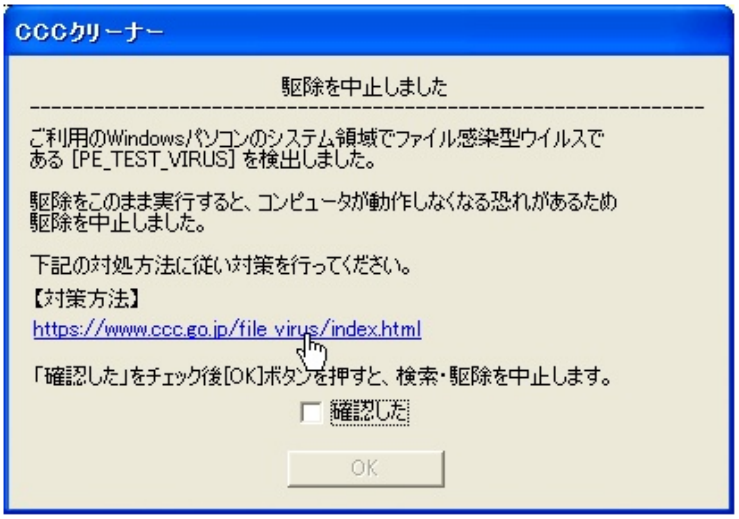


図 4-3 駆除中止時のポップアップ

(2) 検出情報送信機能

CCC クリーナーが検出した PC の状態や利用環境の情報を分析し、有効な対策の検討に役立てるため、CCC クリーナーでは検出情報の送信機能を実装している。CCC クリーナーを使用した際に利用者が任意で送信の可否を選べるログ（以下、送信ログ）には、含まれる情報を表 4-1 に示す。

表 4-1 検出情報の送信機能によって送信される情報

項目	内容
実行時間	実行した日時、スキャンに要した時間
OS 情報	Windows OS のバージョンと、適応されているサービスパック番号
メモリ情報	搭載物理メモリ量
ネットワーク環境	実行環境の IP アドレスタイプ（グローバルまたはプライベート）
hosts ファイル 改ざん有無	デフォルトの hosts ファイルに変更が加えられているかどうか
駆除結果	各種ファイル数、エラー情報
検出マルウェア名	検出されたマルウェア名および該当ファイルの SHA-1 ハッシュ値

本年度実施した、送信ログの分析内容については 4.3.2 に記載している。

(3) hostsファイルの改ざん復旧機能

改ざんされた hosts ファイルによって Microsoft Windows Update やウイルス対策ソフトの更新が阻害されないよう、hosts ファイルの改ざん復旧機能を実装している。hosts ファイルの改ざんが確認できた場合には警告(図 4-4)を表示し、「復旧」が選択された際にはバックアップを作成した上で hosts ファイルをデフォルトの状態に復旧する。

図 4-4 hosts ファイルの改ざん検出ポップアップ

(4) サービスパック適用状況の確認機能

Windows には OS の自動アップデート機能があるが、マルウェアによって無効にされていたり、PC 利用者によってはアップデート実施が不十分であることなどの理由で、PC の OS のアップデートは必ず行われているとはいえない状態である。そのため、CCC クリーナーは、実行した PC の OS に最新のサービスパック(以下 「SP」という)やセキュリティパッチが適用されているかを確認し、不十分であった場合はポップアップ(図 4-5)を表示し、CCC クリーナーの利用者に Windows Update の実施を促している。

図 4-5 サービスパック適用チェック

(5) 接続形態の確認機能

PC がブロードバンドルータなどを介さず直接インターネットに接続されている場合、ブロードバンドルータを導入している環境に比べマルウェアに感染しやすくなる。

そのため、CCC クリーナーは PC に割り当てられている IP アドレスが、グローバル IP アドレスかプライベート IP アドレスかを確認する機能を実装している。PC に割り当てられている IP アドレスがグローバル IP アドレスであった場合には、警告ポップアップ(図 4-6)を表示しブロードバンドルータの導入を促している。

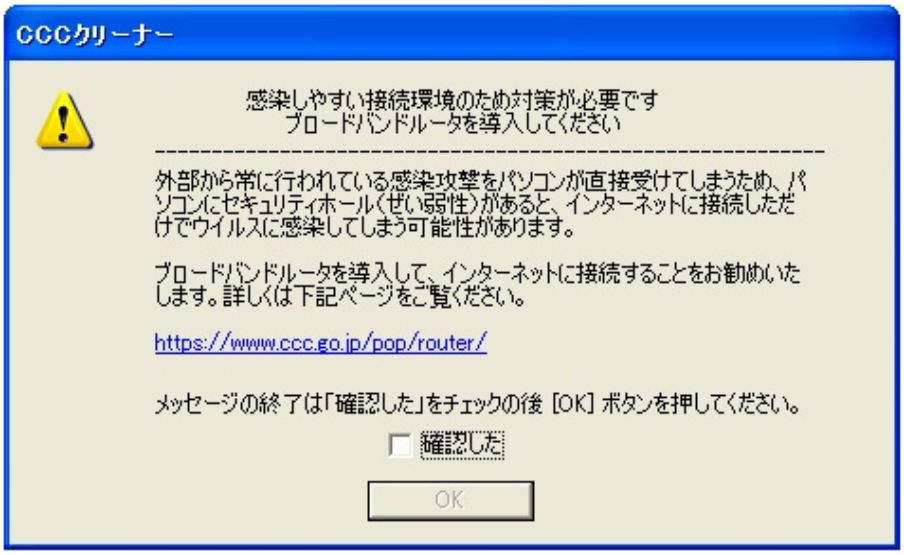


図 4-6 グローバル IP アドレスの警告ポップアップ

(6) 有効期限の設定

CCC クリーナーは、自動的にパターンの更新が実施されない。そのため、古いパターンが搭載された CCC クリーナーを使用できないようにするため、有効期限を設けて CCC クリーナー実行を制限している。この機能により、常に最新版の CCC クリーナーのダウンロード促し、実行してもらうことが可能となっている。図 4-7 に、有効期限が切れた CCC クリーナーを実行した際のポップアップを示す。

図 4-7 有効期限が切れた CCC クリーナーの実行結果

4.3. ボットの解析・分析

4.3.1. ボット解析・分析の概要

(1) 目的

ボットプログラム解析グループでは、将来の脅威の予測や予防策を探るために、現在流行しているボットを解析・分析し、流行しているボットの脅威の特定や、得られた知見を蓄積、および得られたデータの分析を目的としている。

(2) 分析対象

CCC クリーナーの送信ログ、ハニーポット収集検体の二つのデータを分析対象としている。

① CCCクリーナーの送信ログ

検出情報送信機能によって受信し、収集した送信ログ収集した送信ログを分析することで、以下の情報を得ることができる。

- CCC クリーナーを実行した PC の環境に関する情報
- 流行しているマルウェアに関する情報
- CCC クリーナーを実行した PC で検出されたボットと、ハニーポットで収集している検体との差異に関する情報

これらの情報を、次に挙げるハニーポット収集検体の分析と結びつけることで、より効果的な対策検討につなげることが可能となる。

② ハニーポット収集検体

ハニーポット収集検体とは、ボット対策システム運用グループの運用しているハニーポットにて収集しているマルウェアのことである。実際に収集した検体を詳細分析することによって、マルウェアの持つ機能の詳細を明らかにすることにより、傾向や変化を把握し、そこから将来の脅威予測、対策検討を

行う。

2009 年度における収集傾向を図 4-8 に示す。

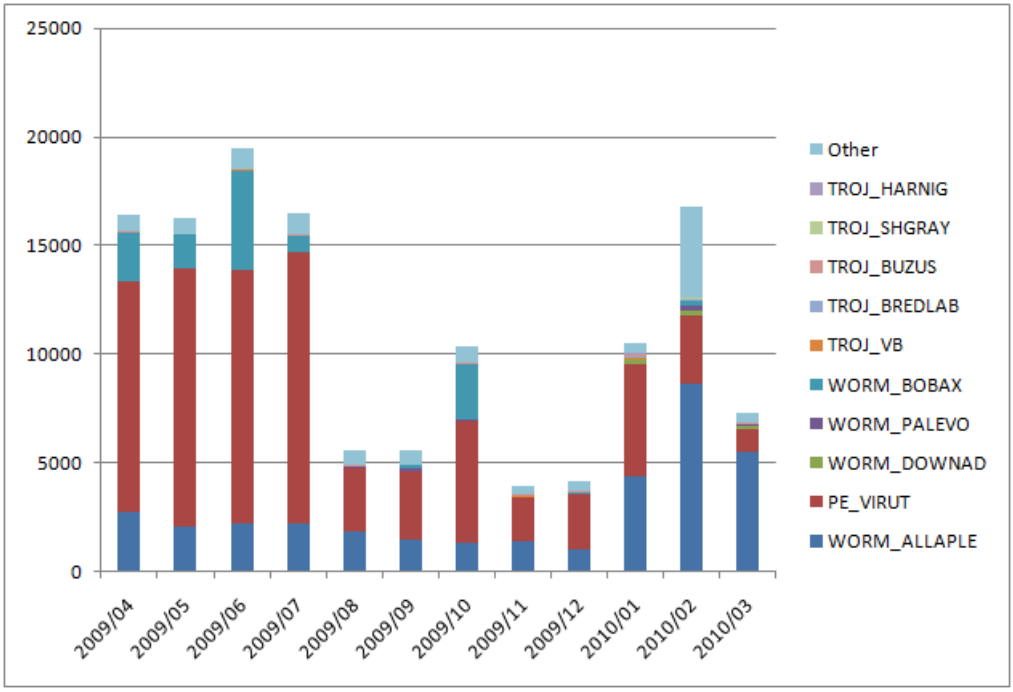


図 4-8 ハニーポットにおける検体の収集傾向

4.3.2. CCCクリーナー送信ログの分析

(1) 送信ログの傾向

① 送信ログの受信数

送信ログの受信数の推移を図 4-9 に示す。2009 年度 4 月、9 月、10 月の送信数増加は、CCC の活動がメディアで報じられたことで CCC クリーナーのダウンロード数が増加したためと考えられる。

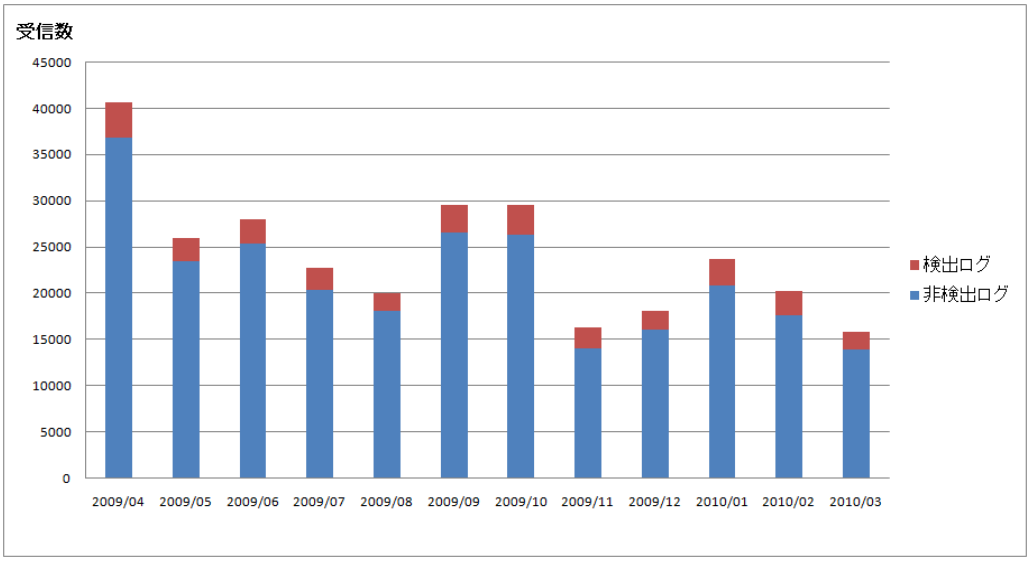


図 4-9 送信ログの受信数の推移

② OS別の収集傾向

CCC クリーナー実行環境における OS および SP 適用状態の傾向を図 4-10 に示す。2009 年 1 月以降 Windows XP SP3、Windows Vista SP2 の増加が見られており、サービスパック適用状況の確認機能により SP 適用を促した効果が見られたと考えられる。

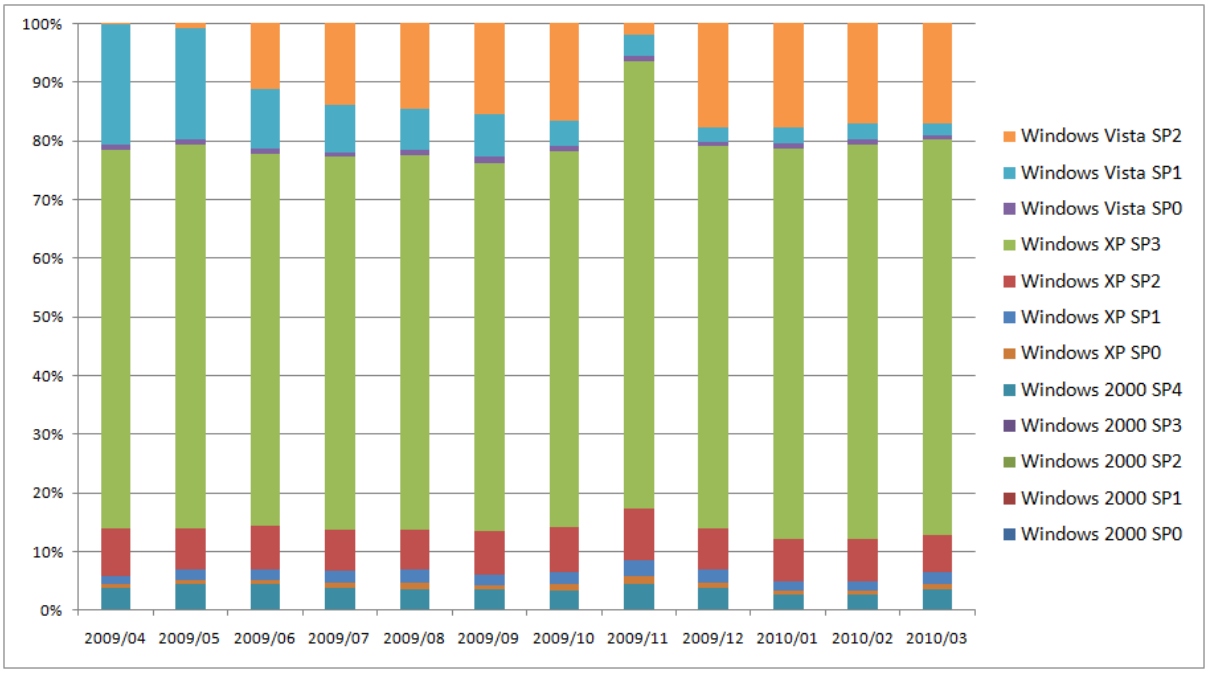


図 4-10 OS の比率の推移

③ 送信ログの検出傾向

一般サイトの利用者および注意喚起対象者のマルウェアの検出傾向をそれぞれ図 4-11 および図 4-12 に示す。一般サイトの利用者は WORM_ONLINEG などのオンラインゲームアカウントの窃取を狙った検体や、Mal_Otorun といったリムーバブルメディア等の自動実行機能を悪用した検体が目立つ。注意喚起対象者では、検出傾向が図 4-8 のハニーポットの収集傾向と似ており、ファイル感染型マルウェアである PE_VIRUT が確認できる。また PE_VIRUT 以外では一般サイトの PC の利用者の傾向と同様、リムーバブルメディア等の自動実行機能を悪用した検体も多く確認できており、ハニーポットで収集できていないマルウェアによる感染の拡大も見られた。

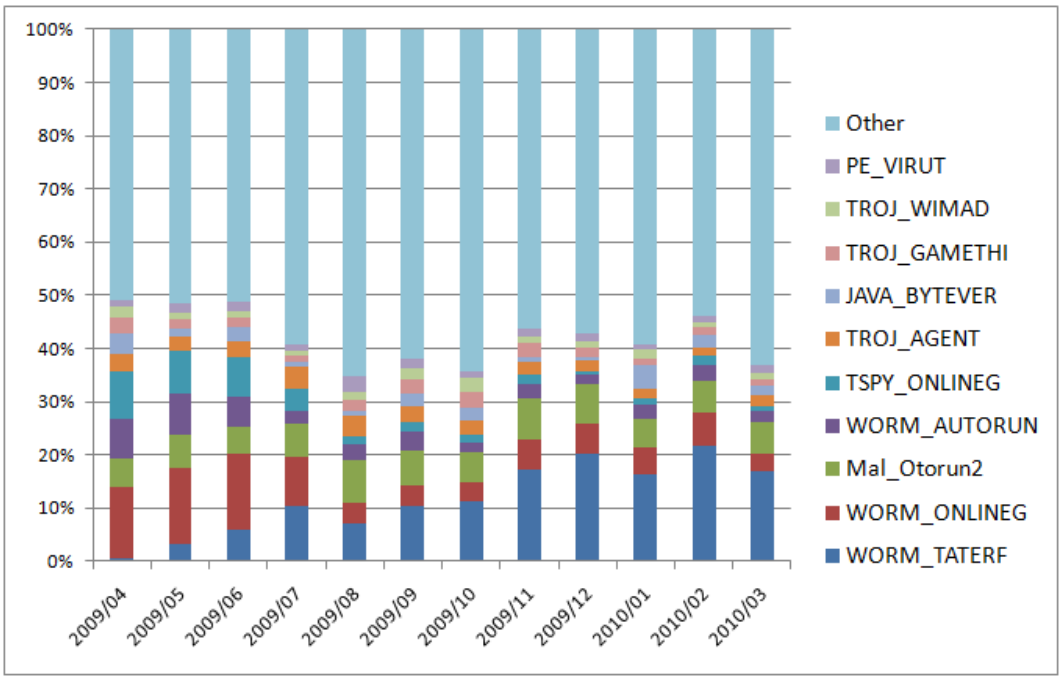


図 4-11 一般サイトの利用者の検出傾向

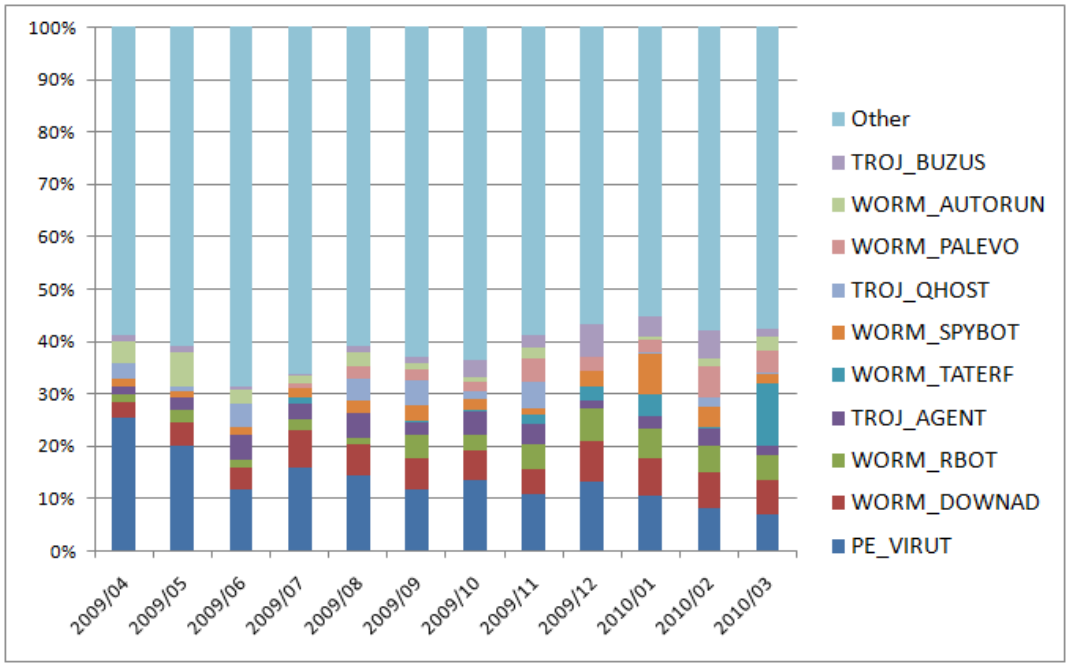


図 4-12 注意喚起対象者の検出傾向

④ OSのSP別検出比率

一般サイトの利用者(図 4-13)および注意喚起対象者(図 4-14)における OS の SP 別検出率を示す。両 PC の利用者で共通している点としては、SP のバージョンが上がるほど感染率が低くなる点、Windows Vista の環境では感染率が低い点が挙げられる。

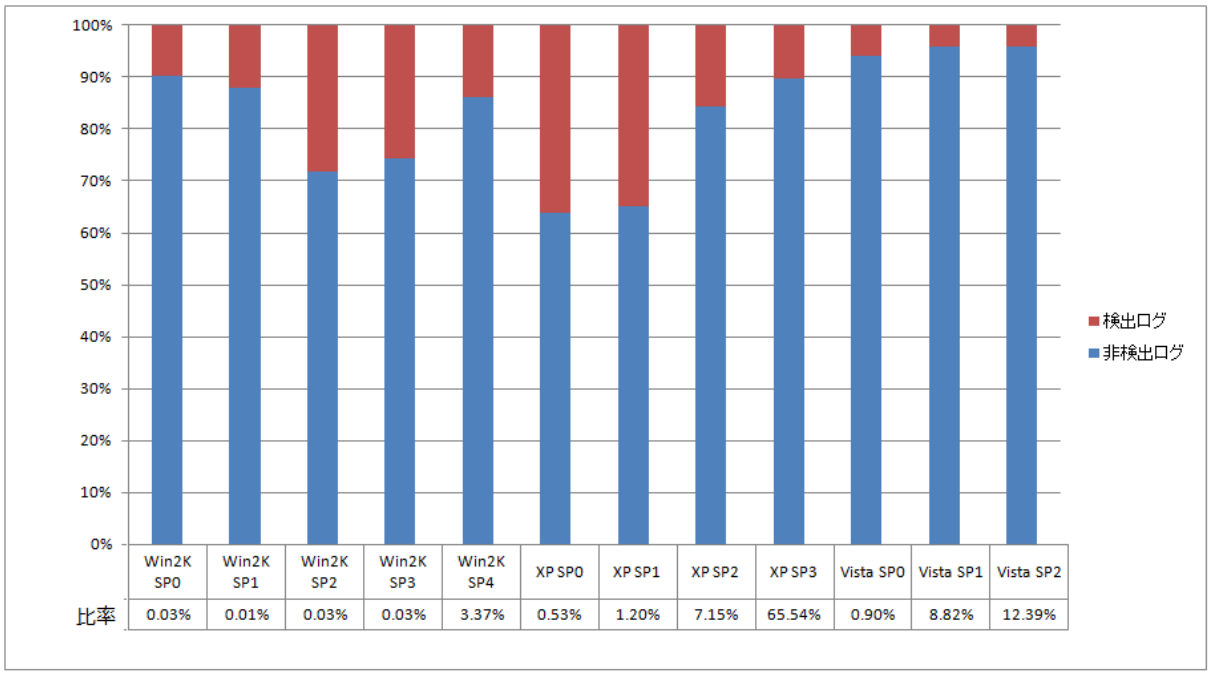


図 4-13 OS の SP 別の検出率（一般サイトの利用者）

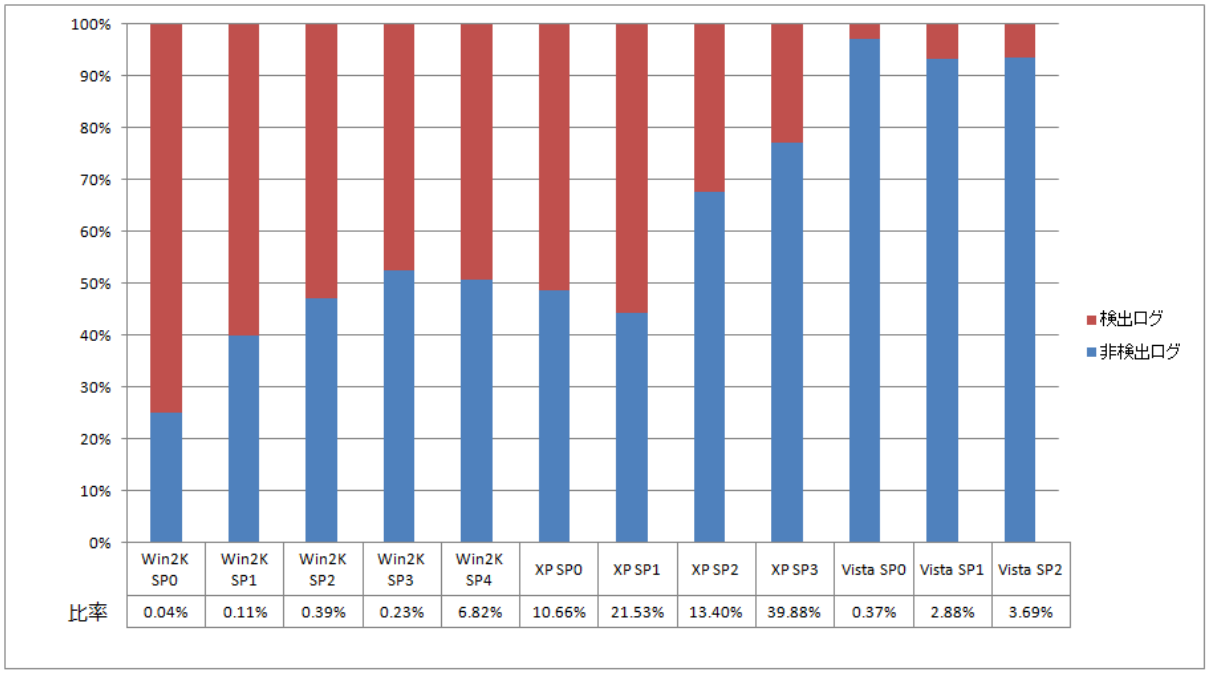


図 4-14 OS の SP 別の検出率（注意喚起対象者）

⑤ ネットワーク環境の傾向 （IPアドレスタイプ）

一般サイトの利用者および注意喚起対象者の IP アドレスタイプをそれぞれ図 4-15 および図 4-16 に示す。プライベート IP アドレスの環境が、一般サイトの利用者では 70%に近いのに対し、注意喚起者では 20%程度である。また、注意喚起者の半数がグローバル IP アドレス環境であることが分かる。

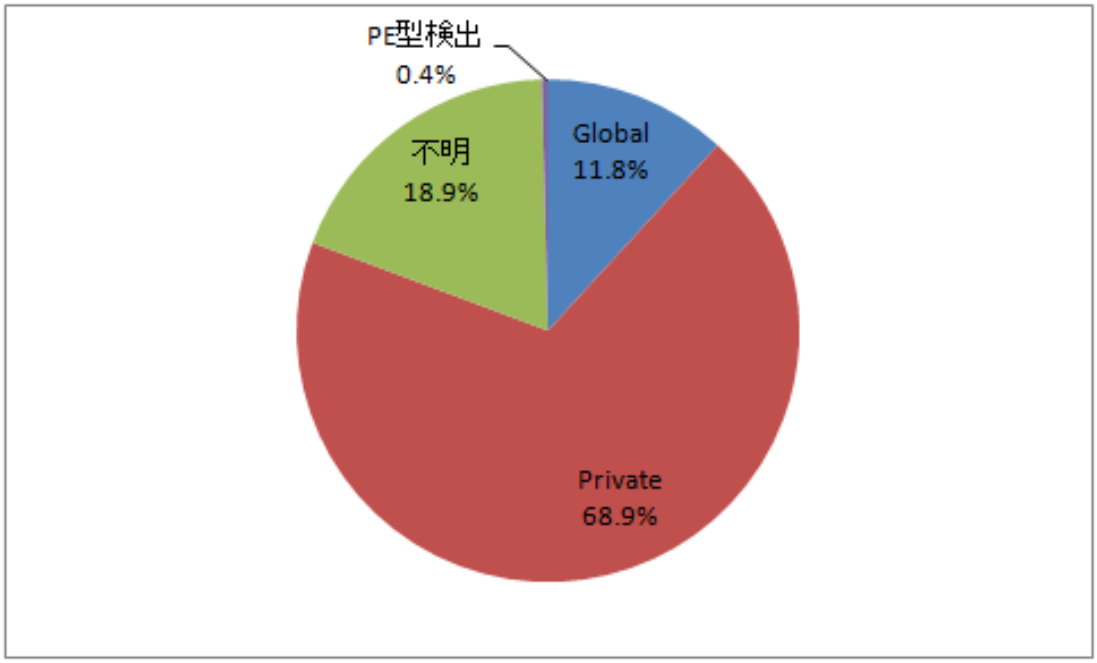


図 4-15 一般サイトの利用者の IP アドレスタイプ比率

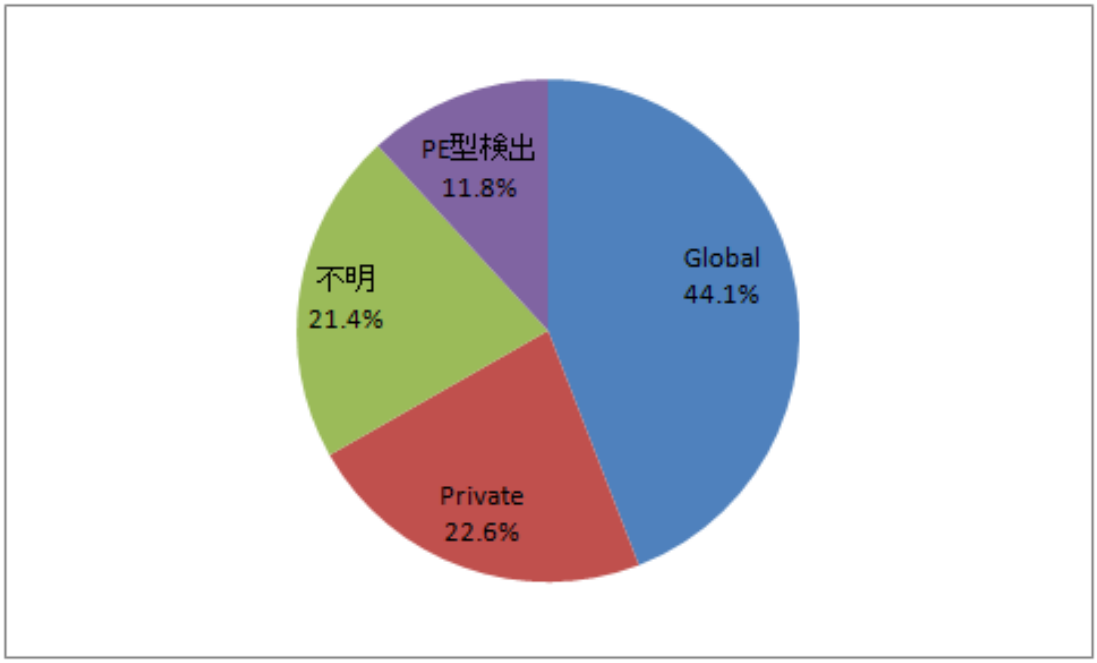


図 4-16 注意喚起対象者の IP アドレスタイプ比率

⑥ ネットワーク環境別の検出比率

ネットワーク環境別の検出比率を図 4-17 に示す。グローバル IP アドレス環境では検出ログが 16%、プライベート IP アドレス環境では検出ログが 10%を占めていた。ネットワーク環境によって検出比率が変化しているが、それだけではなく OS の状態や PC の使用環境などにも依存すると考えられる。

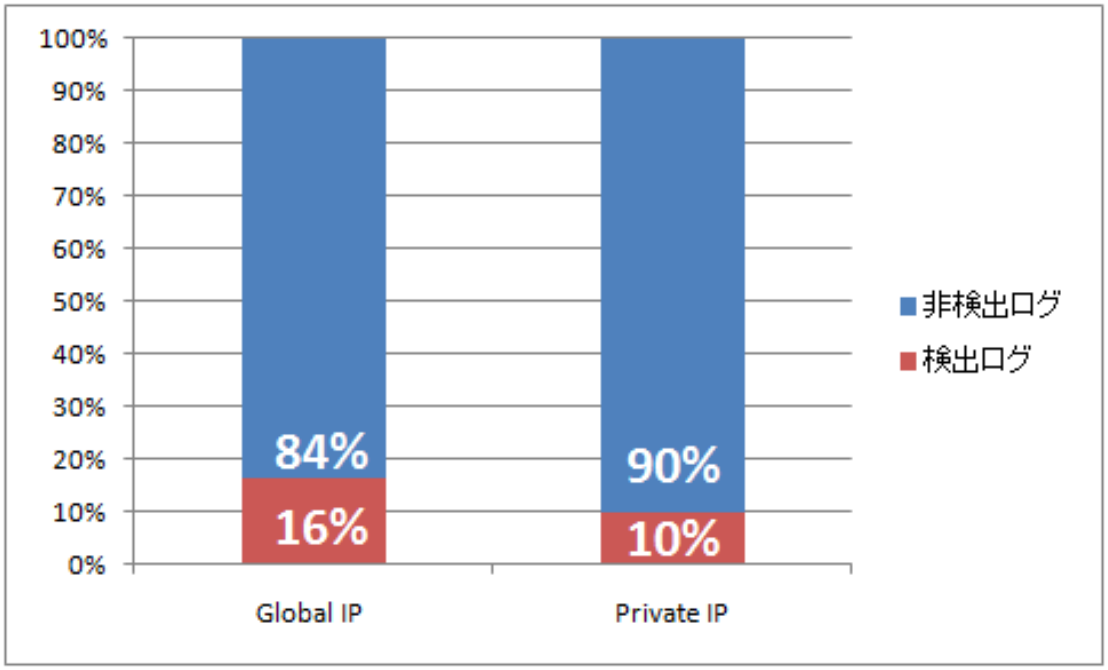


図 4-17 ネットワーク環境別の検出比率

⑦ 特定期間における送信ログの傾向

注意喚起ユーザにおける、注意喚起後の対応状況の調査を目的として、2009 年 9 月から 12 月まで注意喚起ユーザからの送信ログの受信傾向を調査した。調査から得られた結果を図 4-18 及び図 4-19 に示す。OS が最新の状態ではない(アップデートをしていない、アップデートが不十分)ユーザが 7 割近くいること、また多くのユーザがファイル感染型 Malware を検出していることから、多くのユーザ環境でセキュリティ対策が不十分である実態が見られる。

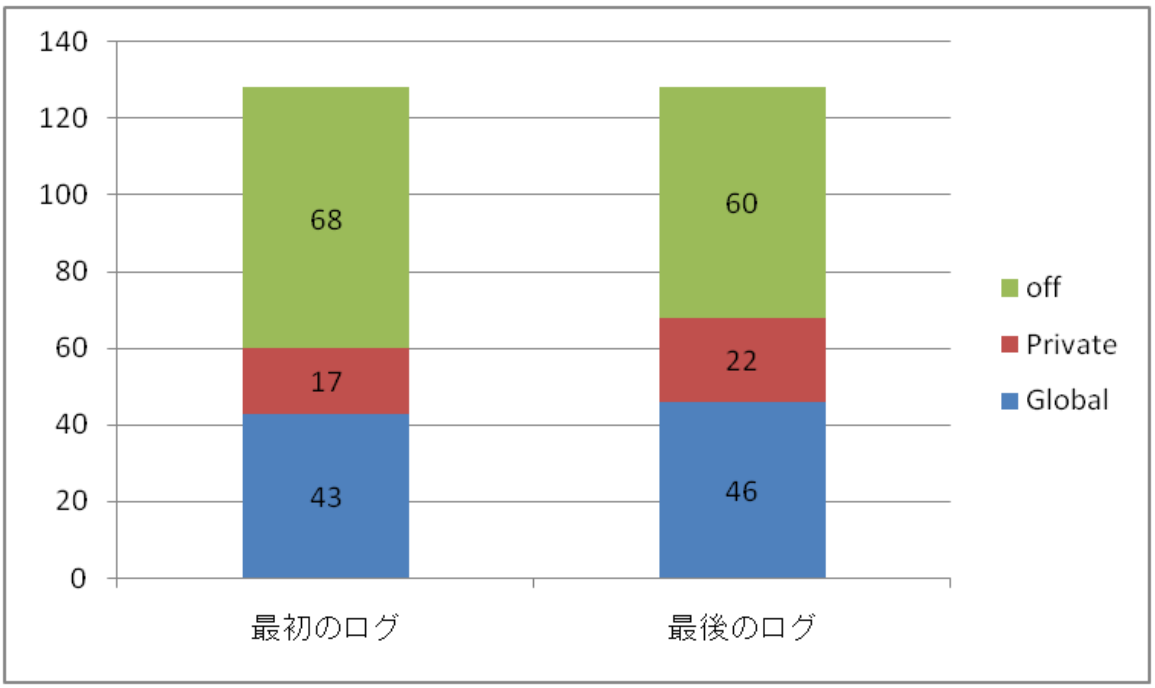


図 4-18 ネットワーク環境の変化

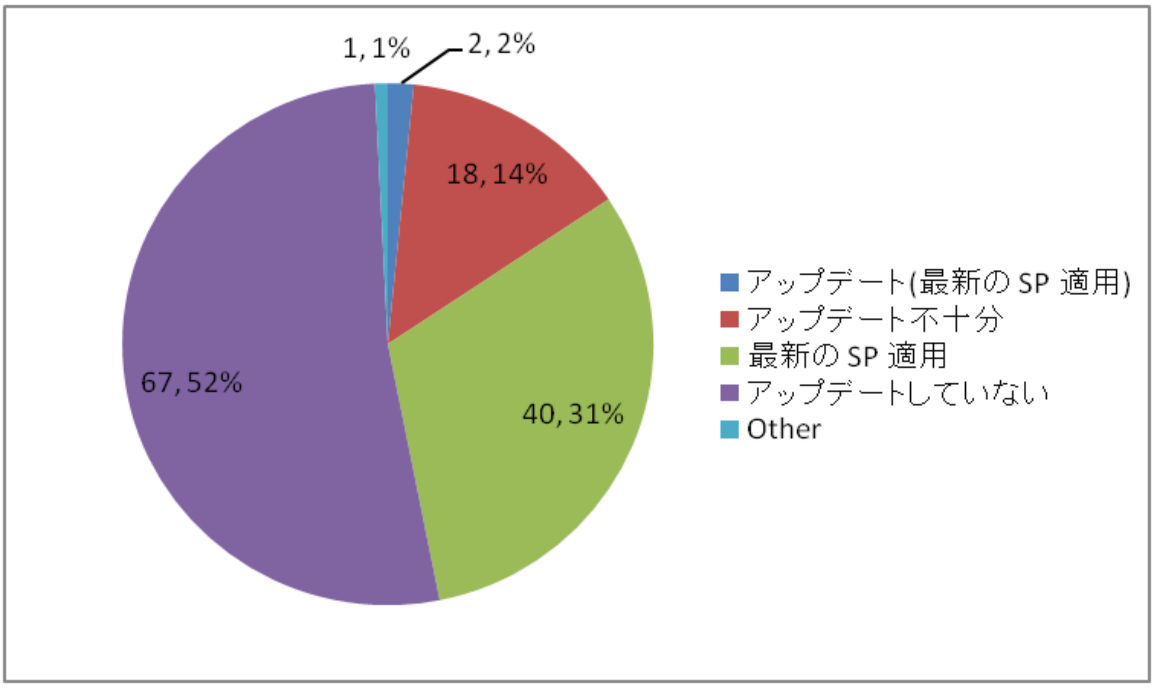


図 4-19 OS のアップデート状況

(2) 送信ログの関連性分析

近年マルウェアによる攻撃手法は複雑化、多様化しており、複数のマルウェアの連携により一連の攻撃を成立させている場合もある。このような状況下で特定の 1 検体や総数だけを見ていては、攻撃活動の全容を把握し効果的な対策に結びつけることは難しい。

そこで 2009 年度は、件数や特定検体のみならず、様々な要素の関連性を調べることによって対策の検討を行うべく、送信ログからマルウェア同士の関連性やマルウェアとユーザ環境の関連性を調査した。

① 分析手法

今回は関連性分析の手法としてアソシエーション分析を用いた。

アソシエーション分析は、大量のデータから意味のあるアソシエーションルールを抽出するデータマイニング手法である。アソシエーションルールは、トランザクションにおいて、ある条件 X が与えられた時に結果 Y が起きるというルールである。この条件 X をルールの条件部、結果 Y を結論部といい、

$$X \Rightarrow Y$$

で表す。また、トランザクションに含まれる全てのデータ数を N、条件 X を満たすデータを x、結論 Y を満たすデータを y とすると、トランザクション中のルールの出現率（支持度）と条件が現れた際に結論が現れる確率（確信度）は、

$$Supp(X \Rightarrow Y) = \frac{x \cap y}{N}, \quad Conf(X \Rightarrow Y) = \frac{x \cap y}{x}$$

で表される。

② 分析手順

送信ログからアソシエーションルールを抽出した後、次の関連性を表すルールに絞り込み、分析を行った。

- マルウェア間の関連性
- OS とマルウェアの関連性
- ネットワーク環境とマルウェアの関連性

③ 分析結果

ⅰ） マルウェア間の関連性

マルウェア同士の関連性に関するルールの内、確信度が上位のルールの抜粋を表 4-2 および表 4-3 に示す。確信度が高いということは、ルールの条件と結論の結び付きが強いことを意味し、マルウェア同士の連携が行われている可能性を示している。支持度は、ルールの起こりやすさを意味し、マルウェアの組み合わせの流行の状況を示している。

表 4-2 マルウェア（固有名）同士の関連性を示すルール

条件部	結論部	支持度（%）	確信度（%）
JAVA_BYTEVER.AC	JAVA_BYTEVER.AB	0.6	100.0
JAVA_BYTEVER.AC	JAVA_BYTEVER.A	0.6	100.0
JAVA_BYTEVER.AB, JAVA_BYTEVER.A	JAVA_BYTEVER.AC	0.6	99.0
JAVA_BYTEVER.AB	JAVA_BYTEVER.A	0.6	97.8
JAVA_BYTEVER.AB	JAVA_BYTEVER.AC	0.6	96.9
WORM_ONLINEG.ZYM	TSPY_ONLINEG.MCL	0.5	96.3
WORM_AUTORUN.DDV	TSPY_ONLINEG.MCL	0.5	94.2
TROJ_QHOST.JM	BKDR_AGENT.GLQ	0.6	91.1
WORM_AUTORUN.DDV, TSPY_ONLINEG.MCL	Mal_Otorun2	0.4	86.9
WORM_ONLINEG.ZYM, TSPY_ONLINEG.MCL	Mal_Otorun2	0.4	86.1

表 4-3 マルウェア（ファミリー名）同士の関連性を示すルール

条件部	結論部	支持度（%）	確信度（%）
TROJ_GAMETHI, WORM_ONLINEG	Mal_Otorun	1.0	89.1
TSPY_ONLINEG, WORM_AUTORUN, Mal_Otorun	WORM_ONLINEG	1.5	87.5
PE_BOBAX, PE_VIRUT	WORM_BOBAX	1.0	87.5
WORM_ONLINEG,TSPY_ONLINEG,WORM_AUTORUN	Mal_Otorun	1.5	85.7
PE_BOBAX	WORM_BOBAX	1.5	84.8
TSPY_ONLINEG, WORM_AUTORUN	WORM_ONLINEG	1.8	83.4

表 4-2 では、支持度と確信度共に高い数値であったのは JAVA_BYTEVER ファミリー同士のルールである。JAVA_BYTEBER は悪意のある Java アプレットまたはそれを利用する JavaScript の検出

名であり、Web 感染型の攻撃起点として使用される。支持度の高さから、このタイプの Web 感染型が流行していることが分かる。

しかし、Web 経由の攻撃起点のマルウェアと、ダウンロードされるマルウェア（偽ウイルス対策ソフトや動画コーデックなど）との関連性が見られなかった。これは、ダウンロードされるマルウェアが多岐にわたるためと考えられる。

表 4-3 では、WORM_AUTORUN（Mal_Otorun）ファミリーと TSPY（WORM）_ONLINEG ファミリーが含まれるルールが目立つ。WORM_AUTORUN（Mal_Otorun）は USB メモリ等のリムーバブルメディアを感染媒体とする検出名であり、TSPY（WORM）_ONLINEG はオンラインゲームのアカウント情報を窃取するマルウェアの検出名である。このことから、リムーバブルメディアを経由して感染するマルウェアはオンラインゲームアカウントの窃取を目的としていることが分かる。

ii） OSと検出マルウェアの関連性

Windows XP に関するルールの内、送信ログ全体における Windows XP の割合である 84.1%を越える確信度を持つルールを一部抜粋したものを表 4-4 に示す。

表 4-4 Windows XP とマルウェアの関連性を示すルール

条件部	結論部	支持度（%）	確信度（%）
TROJ_GAMETHI,WORM_ONLINEG,Mal_Otorun	Windows XP	1.1	99.4
WORM_TATERF, WORM_ONLINEG, Mal_Otorun	Windows XP	1.3	98.9
Cryp_Krap, Mal_Otorun	Windows XP	1.8	98.5
WORM_ONLINEG, TSPY_ONLINEG, Mal_Otorun	Windows XP	2.3	98.4
Cryp_Krap	Windows XP	2.3	98.0
WORM_ONLINEG,TSPY_ONLINEG,WORM_AUTORUN	Windows XP	1.7	97.9
WORM_DOWNAD	Windows XP	2.6	91.5

マルウェア同士の関連性において見られたリムーバブルメディア経由でのオンラインゲームアカウント窃取攻撃が、ほとんど Windows XP でしか検出されていないことが分かる。その他にも WORM_DOWNAD についても Windows XP に偏りが見られている。

Windows Vista に関するルールの内、送信ログ全体における Windows Vista の割合である 6.5%を越える確信度を持つルールを抜粋したものを表 4-5 に示す。

表 4-5 Windows Vista とマルウェアの関連性を示すルール

条件部	結論部	支持度（%）	確信度（%）
TROJ_GETCODEC	Windows Vista	0.3	22.1
TROJ_WIMAD	Windows Vista	0.5	17.9
WORM_ANTINNY	Windows Vista	0.3	13.4
TROJ_FAKEAV	Windows Vista	0.2	13.0
HTML_IFRAME	Windows Vista	0.2	10.4

Windows Vistaの場合には、偽動画コーデックの検出名や、P2Pや偽ウイルス対策ソフトといった、ソーシャルエンジニアリング[9]を利用するタイプの検出名に偏りが見られた。

Windows2000 に関するルールの内、Windows 2000 の割合である 9.1%を越える確信度を持つルールを

表 4-6 に示す。

表 4-6 Windows 2000 とマルウェアの関連性を示すルール

条件部	結論部	支持度(%)	確信度(%)
TROJ_QHOST	Windows 2000	0.8	28.3
BKDR_VANBOT	Windows 2000	0.5	25.7
TROJ_RANKY	Windows 2000	0.3	23.5
TROJ_PROXY	Windows 2000	0.4	23.2
WORM_KOLABC	Windows 2000	0.3	22.9
WORM_SDBOT	Windows 2000	0.6	21.5
TROJ_DROPPER	Windows 2000	0.4	20.1
WORM_IRCBOT	Windows 2000	0.3	19.9
PE_SALITY	Windows 2000	0.2	18.2

Windows 2000 では、近年流行しているリムーバブルメディア経由やWeb 経由で感染するようなタイプよりも、ネットワーク感染するタイプの名称が目立つ結果となった。

iii) ネットワーク環境と検出マルウェアの関連性

結論が p(プライベート IP アドレス)となっているルールの内、対象とした送信ログ中のプライベート IP アドレスの割合である 49.0%を越える確信度を持つルールを抜粋したものを表 4-7 に示す。

表 4-7 プライベート IP アドレスとマルウェア名のみのルール抜粋

条件部	結論部	支持度(%)	確信度(%)
Cryp_Krap	Private IP Address	2.1	90.7
Cryp_Krap, Mal_Otorun	Private IP Address	1.7	90.0
WORM_TATERF, Mal_Otorun	Private IP Address	1.9	87.0
WORM_TATERF,WORM_ONLINEG,Mal_Otorun	Private IP Address	1.1	86.3
TROJ_GAMETHI,WORM_ONLINEG,Mal_Otorun	Private IP Address	0.9	83.6
WORM_TATERF, TSPY_ONLINEG	Private IP Address	0.9	82.3
TROJ_GAMETHI, Mal_Otorun	Private IP Address	1.1	81.8
WORM_ONLINEG,TSPY_ONLINEG,Mal_Otorun	Private IP Address	1.9	81.7
WORM_ONLINEG, Mal_Otorun	Private IP Address	3.1	80.9

[9] パソコンの利用者などから、話術や盗み聞き、盗み見あるいは、誤操作を誘発させるなどの「社会的」な手段によって、パスワードなどのセキュリティ上重要な情報を入手すること。

条件部	結論部	支持度(%)	確信度(%)
Cryp_Nsanti	Private IP Address	0.9	70.1
TSPY_ONLINEG	Private IP Address	3.9	69.0
TROJ_FAKEAV	Private IP Address	0.9	68.9
Cryp_Xed	Private IP Address	1.5	68.8
TROJ_WIMAD	Private IP Address	2.1	67.9
Cryp_Naix	Private IP Address	2.2	66.1
WORM_AUTORUN	Private IP Address	3.5	65.4
WORM_EMBEDDED	Private IP Address	0.7	63.9

プライベート IP アドレスでは、リムーバブルメディア感染型の検出が目立っている。プライベート IP アドレスにおける Windows XP の割合は 85.3%であり、かつ Windows XP でのリムーバブルメディア感染ルールの確信度が 100%に近いことから、この結果は Windows XP の割合が大きく出ているからであると推測できる。

その他には、偽ウイルス対策ソフトや偽動画コーデックの検出名がグローバル IP アドレスに比べ多く見られている。これらは Windows Vista にて多く見られたが、確信度の高さからプライベート IP アドレスに起因する固有の傾向であると考えられる。

同様に、結論が g(グローバル IP アドレス)となっているルールの内、対象となった送信ログ中のグローバル IP アドレスの割合である 15.5%を越える確信度を持つルールの抜粋したものを表 4-8 に示す。

表 4-8 グローバル IP アドレスとマルウェア名のみのルール抜粋

条件部	結論部	支持度(%)	確信度(%)
WORM_DOWNAD	Global IP Address	1.7	58.1
BKDR_RBOT	Global IP Address	1.0	41.6
WORM_KOLABC	Global IP Address	0.5	39.7
BKDR_SDBOT	Global IP Address	0.5	39.4
WORM_EMBEDDED	Global IP Address	0.4	36.1
TROJ_INJECT	Global IP Address	0.4	30.3
WORM_ALLAPLE	Global IP Address	0.7	30.2
BAT_FTPER	Global IP Address	0.3	29.2
Cryp_Naix	Global IP Address	0.8	22.6
WORM_AUTORUN, TROJ_AGENT	Global IP Address	0.3	21.8
BKDR_IRCBOT	Global IP Address	0.3	21.1
BKDR_VANBOT	Global IP Address	0.4	21.1
TROJ_GETCODEC	Global IP Address	0.3	20.6

グローバル IP アドレス環境では、WORM_DOWNAD の検出が目立つ。他にも、BKDR_RBOT や WROM_KOLABC、WORM_EMBEDDED、WORM_ALLAPLE といった、ネットワーク攻撃によって感染を拡大するタイプの検出がプライベート IP アドレスに比べ多くなっていた。

4.3.3. 収集した検体の分析

本項では、ボット対策事業のハニーポットにて収集した検体の分析について、2009 年度に実施した内容を述べる。

(1) 分析プロセス

ハニーポットで収集した検体は 2009 年 3 月末時点で 1,000,082 件であり、そのすべての検体を詳細に分析することは困難を極める。そこで、ボットプログラム解析グループではまずはサーフィス分析、簡易分析などでといった比較的短時間で実施できる分析手法で、検体をサンプリングした後に、詳細な分析を実施することで、効率的な分析を実施している。

それぞれ検体の分析手法を以下に示す。

① サーフィス分析

検体の外見的特徴となる、様々なファイル情報やウイルス対策ソフト検出名を取得する。短時間かつ自動で取得でき、同じ検体を見抜くことなどが可能である。

② 簡易分析

検体を自動動的解析環境で実行し、検体の挙動のデータを収集し、その結果を分析する。自動で実行でき、所要時間は比較的短いが、取得できるデータに限界がある。

以上プロセスによってサンプリングを行った後に、詳細分析を行う。

③ 詳細分析

検体を逆アセンブルまたはデバッグし、アセンブリコードを解析する。詳細分析により、検体を動かしただけでは実行されないコードも含め、検体の挙動の詳細が把握できる。なお、詳細分析の実施には、高度な技術を持つ解析者および多大な時間が必要となる。

そして詳細分析の結果から得られた知見をもとに、今後のボット対策を検討する。

(2) 分析結果

2008 年度と同様に、収集した検体をサンプリングし、特徴的と思われる検体について詳細分析を実施した。2009 年度に解析を行った検体のサマリを抜粋したものを表 4-9 に示す。

表 4-9 解析を行った検体のサマリ

番号	特徴
1	Zeus trojan。
2	ファイルの後方に暗号化されたプログラムが存在する。本体は IRC ボット。
3	Delphi で作られている。
4	HTTP2P で通信を行う。
5	デバイスドライバが DNS の阻害を行っている。
6	パッカーによって巨大なバイナリとなっている。TCP 接続数の制限を解除する。
7	スタック上にコードを展開して実行している。
8	作成したデバイスドライバが svchost.exe にコードを注入する。
9	デバイスドライバで SDT の書き換えを行う。
10	HTTP の改ざんを行う。アフィリエイト。
11	フック関数がドライバと DLL に分かれていて解析が困難。
12	Internet Explorer, Firefox, Opera の send, recv をフックする。
13	ntfs.sys を置き換え、service.exe にコードを注入して実行する。
14	アンパック時に rdtsc を使用してジャンプ先を混乱させる。Borland-C 系のコンパイラで作成されている。
15	自分自身のコピーを作成し、PE ヘッダを書換え DLL にする。
16	IRC ボット。autorun.inf を作成する。
17	FTP アカウントの収集、Web 改ざん。
18	パッカー部は Delphi で作成されている。本体は HTTP Proxy。
19	デバイスドライバが DLL を注入。DLL は Delphi で作られている。
20	多くのファイルを作成するが、すべては Mozilla の一部である。本体は Visual Basic で作られている。
21	文字列の難読化以外は特に特徴なし。
22	cdrom.sys を書換え、コードを注入するデバイスドライバに変更する。
23	ファイル感染型。

以上の検体に見られた具体的な機能としては、以下の機能が挙げられる。

- FTP アカウント収集および収集アカウントを用いた Web サイト改ざん機能
- メールアドレス収集およびスパムメール送信機能
- DoS 攻撃機能
- アフィリエイトサイトの表示および自動アクセス機能
- OpenSSL を用いた暗号化通信機能
- カーネルモードマルウェアによる各種情報および操作の隠ぺい機能
- カーネルモードマルウェアによる通信の改ざん機能
- 耐解析機能

なかでも特徴的な点について以下に記載する。

① 脆弱性を狙う機能

2009 年度分析を行った検体に、脆弱性を突くことで特権の昇格を試みるものが存在した。具体的に狙われていた脆弱性を表 4-10 に示す。

表 4-10 狙われた脆弱性

セキュリティ情報番号	概要
MS08-025	Windows カーネルの脆弱性により、特権が昇格される。
MS08-066	Microsoft Ancillary Function ドライバの脆弱性により特権が昇格される。

この機能は、Windows Vista や Windows XP の制限ユーザといったアクセス制御を回避し、カーネル特権にて任意のコードを実行することが狙いであると考えられる。

② 耐解析機能の普及

以前から見られていた耐解析機能については、2009 年度の検体で多数見られた対解析機能を表 4-11 に示す。

表 4-11 耐解析機能一覧

項目	機能概要
PCI バスの調査	PCI バスに接続しているデバイスの ID を調査し仮想マシンを検出
IDTR の調査	割り込みディスクリプタテーブルレジスタ(IDTR)の値を調査し仮想マシンを検出
ユーザ名の調査	sandbox や vmware などのユーザ名かどうかを調べ、動的解析環境を検出
API の戻り値の調査	API を不正な引数で呼び出し、その戻り値から動的解析環境を検出
DNS 応答の確認	特定ドメインの名前解決を行い、その IP アドレスが自身の保持する正しいアドレスと一致するかを確認し、動的解析環境を検出
コードインジェクション	別プロセスにコードを注入することで動的解析やマルウェアの発見を阻害
文字列とデータの加工	文字列とデータを加工しておき、使用するタイミングでデコードすることにより、静的解析を阻害
コードの難読化	コード中に無駄な命令を挿入することで静的解析を阻害

それぞれの機能は以前から見られている機能ではあるものの、2009 年度に解析した検体の 3 分の 2 が表 4-11 のいずれかの機能を持っていたため、今後これらの機能の搭載が標準になっていくものと推測される。

③ 難読化された通信機能

2008 年度後期に観測された、HTTP と P2P を組み合わせた環境で OpenSSL 暗号化通信を行うタイプの検体について詳細な分析を行った。HTTP はファイアウォールの回避、暗号化通信は以上で示した通信内容の解析の阻害、P2P は作成者やハーダーの隠ぺいや可用性の向上を目的としていると考えられる。また、2009 年後半に見られた Web 感染型攻撃(いわゆる Gumblar)によってダウンロードさ

れるボットがこの機能を持つ検体と同種であることが分かっている。このような検体は、HTTP2P と表現されることのあるこの通信機能では、以下のようにしてマルウェア同士の通信が行われる。

i） 保持している大量のIPアドレスリスト（デフォルトのピアリスト）とランダムな文字列からURLを生成（例: http:// 192.0.2.1/xrhlb.png）
ii） 実際の通信で使用するXML形式のデータをOpenSSLのデフォルト証明書を用いて暗号化
iii） 暗号化したデータをPOSTメソッドで生成したURLに送信
iv） 同様に暗号化されたデータを受信

また、暗号化したデータを用いて行われる通信は以下のとおりである。

- 接続先との認証
- コマンドの送受信
- スパムメール送信
- スパムメール送信に必要なデータの送受信
- ファイルのダウンロードと実行
- 自身のファイルの更新
- DoS 攻撃の実行
- ピアリストの更新、各種アクセス制御

④ カーネルモードマルウェアの普及と高度化

2009 年度はルートキット等のカーネルモードマルウェアを生成する検体が多く見られた。カーネルモードマルウェアは 2008 年後期から数が増えてきており、その機能としてはファイルやプロセス等の隠ぺいといったルートキット機能が主である。詳細分析した検体には、ファイルやプロセス等の隠ぺい以外に、以下の高度な機能を有する検体も見られた。

- API を使用しないファイルの操作
- WinSock を使用しない TCP 送受信

これらは通常アプリケーションが行う手順を省略し、直接デバイスドライバとやり取りを行うため、分析の回避・阻害、自己隠ぺい、フィルタ等の影響を受けない等の理由から使用されていると考えられる。このような機能の実装には高度な技術力が必要とされるため、マルウェア作成者の技術力の向上が伺える。また、フィルタドライバ技術を利用することでユーザの通信を改ざんする検体も見られた。フィルタドライバ技術を利用することで、カーネルモードマルウェア作成のコスト削減が図れるため、今後普及することが考えられる。

4.3.4. 対策の検討

2009 年度は、2008 年度の分析結果を踏まえて提案した対策についての調査、および 2009 年度の分析結果に基づく対策の検討を行った。

(1) サイト閉鎖コーディネーションに関する調査

① 背景

2008 年度の詳細分析結果で、マルウェアを配布するサイトでは、ハッシュ値が異なる同一機能の検体を日々配布している結果が得られた。これは、ウイルス対策ソフトの検出回避が目的であると考えられ、何らかのツールを用い、常にウイルス対策ソフトに検出されないよう活動を行っていると考えられる。

このような、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マルウェア配布サイトについて、ISP に対してサイトの停止の働き掛け(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ため、2009 年度のサイト閉鎖コーディネーションに関する調査を行った。

② 調査地域

カナダおよび米国、ロシアおよび東欧

③ 調査の概要

調査地域のセキュリティの有識者に対して、以下の 6 つのカテゴリについてヒアリングを実施した。

i) サイバーセキュリティ全般について
ii) ハニーポット等によるボットの捕獲
iii) ボット駆除ツールとワクチンの公開等の取り組み
iv) ISPのAbuse窓口(サービスデスク)の協業
v) マルウェア配布サイトへのコーディネーションについて
vi) マルウェア配布サイトのブラックリスト等での対応について

④ 調査結果のまとめ

i) カナダ・米国

カナダと米国における ISP においても、ボット対策は当然行われている。CCC と同じように、ボットの振る舞いを理解し、その早期発見のためにハニーポットあるいはハニーネットを利用し、また、ボット感染 PC の利用者を見つけ出すためにネットワークトラフィック分析を行い、ボットが使用することが知られているポートへの通信や、感染初期に示す特異な振る舞いをとらえることで、感染していることを見いだしている。

しかしながら、こういった活動は基本的に各 ISP 個別での対策であり、CCC で行われているようなISP が協力・協業の下でのボット対策活動は、カナダおよび米国では行われていない。以下のような状況がそういった活動が行われていない理由と考えられる。

1) セキュリティ対策と各種ツール

一般にセキュリティ対策は、サービスとして顧客に提供するものであり、また、ハニーポット等のツールはサービス優位性を増すものであり、他社に無償で公開したり共有したりするものではないという認識があること。

2) 情報の共有

顧客に関わる情報やPII[10]（Personal Identifiable Information）はプライバシー保護の観点から、情報の共有が規制されている。また、ISPは関係機関へボットの挙動についての情報を提供する場合もあるが、その場合においても、法律の範囲内であり、かつビジネス的な関係に基づいていること。

3) abuse[11]窓口（サービスデスク）協業

基本的にコストセンターであり、多くが外部委託を利用しており、通常、顧客への対応を少なくしようとする傾向にあること。

4) マルウェア配布サイトへの対応

マルウェア配布サイトへの対応には、個人あるいは組織からの訴訟等の何らかの法的措置が行われていることを前提として、国内の規則と法律に従って裁判所に何らかの記録を提出する必要がある場合には対応するが、一般的にコスト等の面からそういった対応を避ける傾向にあること。

全体的にビジネス面での利益あるいは法的な面での強制がない限り、公共性だけでISP 間のセキュリティ対策面での協業は行われない状況であり、CCC のような取り組みは成り立ちにくいとのことである。

また、海外とのセキュリティ対策に関しての調整機関としては、National CSIRT(National Computer Security Incident Response Team)12やFIRST (Forum of Incident Response and Security Teams)13が中心となっており、日本においてもJPCERT/CCが対応組織として、現在の状況に即している。

ii） ロシア・東欧

ロシア・東欧おける ISP においても、基本的にボット対策の活動は各 ISP 個別で行われており、CCC で行われているような ISP が協力・協業の下でのボット対策活動は現状ない。

しかしながら、今回対応頂いたロシアの有識者とのインタビューで得られた情報として、ロシアの ISP が集まったある会合において、日本のボット対策推進事業が話題になり、同様の取り組みを民間ベースで行ってはどうかという話し合いが行われたそうである。

どれだけ実際的な取り組みであるのかは現時点で定かでないが、今後、何らかの活動が行われるようであれば CCC の取り組みが参考にされると考えられる。

⑤ 考察

今回の調査において、CCC の取り組みの一貫としてのサイト閉鎖コーディネーションとするよりは、既存のインシデント対応調整連携（FIRST および、各機関の CSIRT 連携）をより一層深め、それぞれの各機関がさらに連携を深めながらサイト閉鎖コーディネーション等を実施することがより効果的であると考えられる。

---

[10]個人情報を示す

[11] ISP などにあるネットワーク上の迷惑行為またはその迷惑行為を通報する窓口

[12]コンピュータに関するセキュリティの問題に関する報告を受け取り、調査し、対応活動を行う組織体の名称

[13] コンピュータに関するセキュリティの問題に関する報告を受け取り、調査し、対応活動を行う CSIRT の国際組織

(2) 2009 年度の分析結果に基づいた対策の検討

2009 年度を通じて行った分析の結果から、次のような傾向が今後見られると考えられる。

- ソーシャルエンジニアリングによる誘導と脆弱性による特権昇格の普及
- 高度なカーネルモードマルウェアの普及
- 暗号化および P2P 形式の通信の普及

Windows Vista 以降において UAC といった厳しいアクセス制御がなされているため、今後は PC の利用者自身にマルウェアを実行させようとするソーシャルエンジニアリング手法が増加することが考えられる。そして実行後にローカルで脆弱性を突き特権昇格を行うことで、感染端末で自由に活動する動きが懸念される。

また、通信の暗号化、システム上での隠ぺいを組み合せることでマルウェアの発見が困難になり、P2P のような通信形態でマルウェア作成者や管理者に辿り着けないようになることが懸念される。

① 一般のPC利用者目線での対策

一般の PC 利用者が実施すべき対策として、以下の対策が挙げられる。

- プライベート IP アドレス化
- OS と各種ソフトウェアのアップデート
- OS のアップグレード
- ソーシャルエンジニアリングの認知

送信ログの分析にてネットワーク環境による感染傾向において、グローバル IP アドレス環境の危険性を確認しており、ブロードバンドルータの導入など PC がインターネットに直接接続されない環境作りが必要であると考えられる。

特にモバイル端末などについてはグローバル IP アドレスが割り当てられている状況が多いため脅威について周知・徹底が必要であると考えられる。

また、OS 等ソフトウェアのアップデートが行われていない環境の危険性は、送信ログ分析の結果だけでなく、検体の分析結果からも見られ、また一般においても広くいわれ続けていることである。

対策としてのソフトウェアのアップデートは、CCC クリーナーの SP 適用状況確認機能、CCC の Web サイトでの普及啓発等により、一般の PC 利用者への認知度が高まってきていると考えられる。継続して、普及啓発を行う必要がある。

OS のアップグレードについては、関連性分析の結果で見えた流行している攻撃手法への対策として効果的であると考えられるだけでなく、UAC 等の高度なアクセス制御やドライバ署名機能が搭載されることでカーネルモードマルウェア対策等にも有効なため、今後一般の PC 利用者に対してアップグレードを促す活動を行うことが望ましい。

同時に、今後ローカライズ等によってより判別しづらくなることが予想される偽ウイルス対策ソフト等の出現に鑑み、予めソーシャルエンジニアリングに関する認知を高めておかなければならないと考えられる。

② 分析技術の高度化

マルウェアの分析はマルウェア対策を検討する上で必要不可欠である。その中で、今後も継続して技術が高度化するマルウェアに対抗するためには、分析技術のさらなる高度化や効率化が必要となる。

具体的には、次の分析手法の確立が必要と考えられる。

・ カーネルモードマルウェアの簡易分析手法の確立
・ カーネルモードマルウェアも含めたアンパッキング技術の開発
・ 加工された文字列やデータの簡易デコードおよび収集方法の開発
・ 難読化されたコードの整理技術の開発
・ より実機に近い仮想化環境の開発
・ 分析技術者の能力向上と育成
・ 分析情報の共有
・ 多人数リアルタイム分析による詳細分析時間の短縮方法の確立

③ より大きな枠組みでの対策

ボット感染者を減らすだけではなく、ボット作成者を減らすための施策も対策として有効であると考えられる。日本でもマルウェアの作成・頒布行為を処罰する立法措置が望まれる。

また、現在のボットの最終目的は、スパムメールの送信、アフィリエイトサイトのクリック、特定サイトへの DDoS 攻撃といった金銭につながる機能の提供である場合が多い。そのため、感染対象となる一般の PC 利用者や解析者での目線だけでなく、その目的を達成するためのコストを増加させるための対策を実施することで、ボット作成者減少につなげられるのではないかと考えられる。

具体的には、次の対策が考えられる。

・ スパムメール対策関連技術である SPF や OP25B 等の普及啓発
・ アフィリエイトサイト保護のための技術開発
・ DDoS 対策に関する研究

マルウェアの活動は国境を越えて行われており、予防策としての国際連携とインシデント発生時の国際連携が必須となるため、今後さらなる国際連携活動を行い、関係機関間の連携を強化しておく必要があると考えられる。

4.4. 今後の展開

2010 年度は、以下のとおり、2009 年度の活動を継続しつつ、活動の高度化・安定化・効率化を目指す。

(1) CCCクリーナーの作成

収集検体の解析作業を継続し、CCC クリーナーを安定して供給する。

(2) ボットの解析・分析

2009 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

2009 年度と同様に、ボット対策の普及啓発活動支援を行う。

また、緩やかな民間事業への移行の検討や、CCC クリーナーに変わる代替処置の検討を行う。

5. ボット感染予防推進グループの活動

5.1. 概要

ボット感染予防推進グループは、広く一般の PC 利用者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、セキュリティ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、の PC の利用者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、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。

5.2. 感染予防対策ベンダ

本プロジェクトに参加するセキュリティベンダは検体の厳格な管理基準を設定し、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。

こうしたセキュリティベンダを感染予防対策ベンダと呼び、一般の PC の利用者の 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。

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

5.3. 活動成果

感染予防対策ベンダが 2009 年 3 月から 2010 年 3 月末（報告月：2009 年 5 月から 2010 年 4 月）までに、本プロジェクトにおいて取得した検体を各ベンダのウイルス対策ソフト（パターンファイル）へ反 映した 状況について、既に反映済み（提供前から検知可能のもの）、今回反映（パターンファイルに新規登録した もの）、未反映（反映しなかったもの）にわけて、2009 年度の各ベンダの平均値を表 5-1 に示す。

表 5-1 パターンファイルへの反映状況

状況	2009 年度平均
既に反映済み	96.5%
今回反映	2.7%
未反映	0.8%

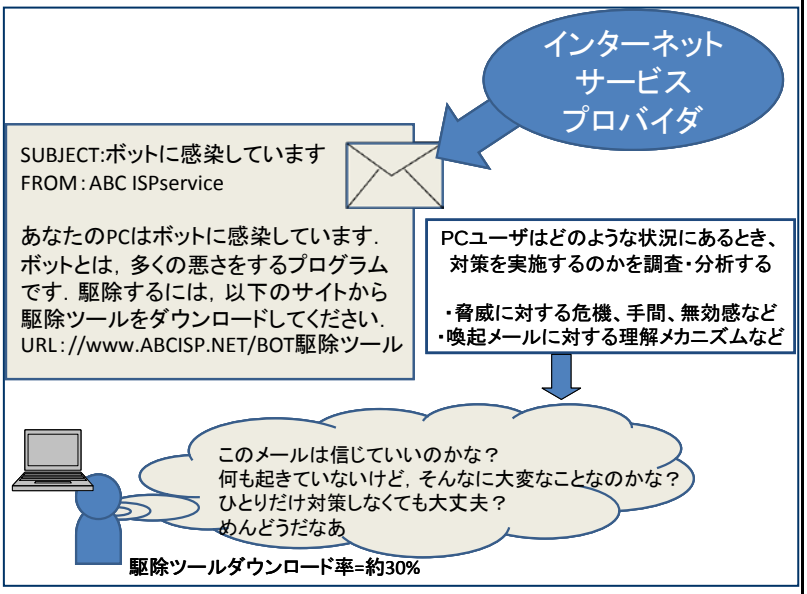
「既に反映済み」および「今回反映」の数値を足した 99.2%とは、本プロジェクトで取得された検体の 99.2%をウイルス対策ソフトで検知できるということである。この数値は本プロジェクトの成果のひとつとして、収集された検体が十分活用されている状況と考えられ、一般の PC の利用者のボット感染予防に十分寄与していると考えられる。

5.4. 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継続して反映されるよう、各ベンダと連携して本プロジェクトに取り組んでいく。

コラム：ボット対策と行動科学（Bot measurement and Human Behaviour）

ボットは、感染PCに直接の障害を引き起こすことは少ないため、感染PCのユーザにとって感染したことによる受ける被害を実感しにくい。このため、個人にとって、その対策をするメリットが少ないと感じているかもしれない。CCCのボット感染者への注意喚起で、ボット対策を実行するユーザが低い率にとどまっている理由を、個人の意思決定のメカニズムから調査する研究が、情報処理推進機構（IPA）で実施されている。意思決定に関する研究は、社会科学領域で行われており、これらの領域の知見をボット対策事業に援用し、ボット対策の向上を図るためには、どのような施策が適切であるかを明らかにすることが目的である。調査はWebアンケート調査によって実施されていた。ボットによる「個人が受ける被害をいかに想定しているか」、「対策をしたことで得られる効果をどのように認知しているか」、「対策をすることの手間をどのように考えるか」、「その効果はISPなどのネットワーク全体にとって有効であると考えているか」などの認知の要素を調査している。この調査では、対策を促すメッセージを受けたユーザの8割は対策をすべきと考えた。このとき、対策をすることの手間をそれほど負荷に感じていないこと、また、自分のPCに障害が起きることを恐れる危機感が強い場合に、対策を実行する意思をもつ傾向が見られた。つまり、対策を実行する意思を持たせるためには、手間感を減らすことと危機感を持たせることが必要ではないかと思われた。



次に、「説得の心理学」の研究を援用し、脅威を知らされた場合のユーザの行動を調査することも行っている。これは、どのようなメッセージであれば脅威を知らせたユーザが対策行動を行うか、を調査するもので、セキュリティ対策を推進させるメッセージのあり方として参考となることを期待している。この調査もWebアンケートで実施していたが、ユーザは、その対策の「効果」を感じられるメッセージに対して、より対策行動意思をもつことが明らかになっている。また、多くのユーザはメッセージの内容を詳細に理解して対策を実施するのではなく、ISPなどの送信元の信頼や媒体の信頼などに大きく影響を受けることがわかった。これらの調査により、個人がボットのような直接の被害を感じる機会が乏しい脅威については、対策の手間を減らすこと、危機感だけでなく対策をすることの効果をより直感的に理解できるようなメッセージにすることが、対策行動を推進する要因になると考えられた。IPAでは、さらにアンケートだけでなく、心理学実験も実施しており、これらの分析を通して、対策を推進するための効率的なメッセージのあり方についての指針が示されることが期待される。IPAの活動は以下のURLで見ることができる。また、「RSAカンファレンスTOKYO 2010」や2009年から開催されているIPA主催の「情報セキュリティと行動科学ワークショップ」などでも、活動が報告されている。

URL: http://www.ipa.go.jp/security/economics/

6. グループ横断的な取り組み

6.1. マルウェア対策人材の育成

CCC では、ボット感染者を見つけて注意喚起を行うという直接的なボット対策に加え、より広い視点で、3 つのグループが協力しマルウェア対策人材育成支援も行っている。

CCC が人材育成支援を行うのは、マルウェア対策は短期的なの対処療法ではなく、中長期的な視点に立って対策を検討していくことが重要であり、そのためには将来のマルウェア対策を担う人材育成が不可欠と考えているからである。

ここでは CCC が取り組んできた IT Keys(先導的 IT スペシャリスト育成推進プログラム)と MWS(Malware 対策研究人材育成ワークショップ)について説明する。

(1) IT Keys(先導的ITスペシャリスト育成推進プログラム)

IT Keys(IT specialist program to promote Key Engineers as security Specialists)は文部科学省が進める先導的 IT スペシャリスト育成推進プログラムのひとつで、関西圏を中心とした情報系 4 大学院(奈良先端科学技術大学院大学、大阪大学、京都大学、北陸先端科学技術大学院大学)および 4 企業・団体(独立行政法人 情報通信研究機構、特定非営利活動法人 情報セキュリティ研究所、一般社団法人 JPCERT コーディネーションセンター、エヌ・ティ・ティ・コミュニケーションズ株式会社)が力を結集し、各々が得意とする専門分野の教育プログラム、実環境による演習プログラム等を有機的に連携させることにより、組織における情報セキュリティ問題に対して主導的役割を果たすことのできる多面的・総合的能力とともに、経験に基づく知識と勘を兼ね備えた実践型人材の育成を目指している。

CCC では、2008 年度より IT Keys のリスクマネジメント演習を担当し、4 大学修士 1 年生を対象に、CCC の活動に関するセミナーや、解析演習、セキュリティ企業見学等を企画した。リスクマネジメン演習の環境やプログラムは CCC の独自のノウハウを活用し、設計、構築を行った。

【実施期間】
2008 年 9 月 16 日～9 月 19 日(4 日間)
2009 年 9 月 15 日～9 月 18 日(4 日間)
【主な実施内容】
ボット感染＆分析演習(ボット対策システム運用グループが担当)
静的解析演習(ボットプログラム解析グループが担当)
ウイルス等ネットワークにおける脅威の変遷と対策(ボット感染予防推進グループが担当)

(2) MWS(マルウェア対策研究人材育成ワークショップ)

MWS(マルウェア対策研究人材育成ワークショップ)は、マルウェアに関する専門知識を備えた研究者や実務者を育成していくことを目的に 2008 年度より情報処理学会と連携して開催しているワークショップである。

MWS では、CCC で収集しているボット観測データを「研究用データセット CCC DATAset」(マルウェアハッシュ値、攻撃通信データ、攻撃元データの 3 つから構成されるボット観測データ群)として活用し、「研究

成果の共有」「切磋琢磨する環境」の場、「学術系発表活動」の場を提供した。 マルウェア対策研究人材育成ワークショップ（MWS）を以下の要領で開催した。

【実施期間】
MWS2008：2008 年 10 月 8 日～10 日（沖縄）
MWS2009：2009 年 10 月 19 日～21 日（富山）
【主催】
サイバークリーンセンター運営委員会、（社）情報処理学会

MWS（MWS2008/MWS2009）の特徴のひとつとして、複数の研究者が CCC から提供された同じ研究用データセットを活用するため、研究者間で研究成果を共有できることが挙げられる。同じ研究用データセットを用いても研究者によって解析プロセスが異なるため結果データも異なる。

これらの研究成果を本ワークショップで発表し、研究者間で共有することにより具体的な成果の水平展開を図り、セキュリティ研究人材育成につなげるほか、具体的なスキルアップ目標や、先進的な研究テーマの発見など、研究者の評価育成の場を形成している。

さらに MWS2009 では、CCC DATAset を制限時間内で解析し、出題された課題に対して、攻撃通信データ、マルウェア名等を回答する MWS Cup というユニークな企画も実施された。採点については、出題に対する解答の正誤で判定する技術点と、解析手法の発表により審査委員が判定する芸術点と、技術点＋芸術点で判定する総合点により、それぞれ技術賞、芸術賞、総合優勝が決められた。

研究内容は「研究用データセット CCC DATAset」の構成される観測データ群と対になっている。ボットの感染攻撃と研究内容に関連を図 6-1 に示す。

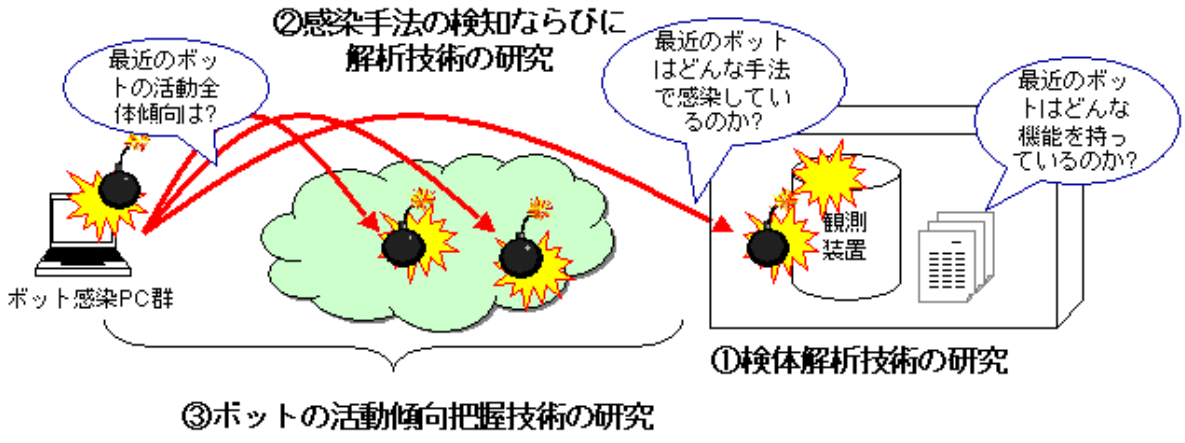


図 6-1 各研究分野と CCC DATAset の関係

① 検体解析技術の研究（マルウェアのハッシュ値）

研究用データセットを提供するためのハニーポットで取得したマルウェアのハッシュ値を利用した研究。マルウェアのハッシュ値は、解析結果を照合できるマルウェア、関連性をもって解析ができる複数のマルウェア、特徴的な機能を有するなど技術的に目を通しておきたいマルウェアに絞り込んで選定し

た。

② 感染手法の検知ならびに解析技術の研究（攻撃通信データ）

研究用データセットを提供するための観測装置で取得した通信のフルキャプチャデータを利用した研究。

③ ボットの活動傾向把握技術の研究（攻撃元データ）

研究用データセットを提供するための観測装置で取得したマルウェア取得時のログデータ（マルウェアの取得時刻、送信元 IP アドレス、送信元ポート番号、宛先 IP アドレス、宛先ポート番号、TCP または UDP、マルウェア検体のハッシュ値（SHA1）、ウイルス名称、ファイル名）を利用した研究。

6.2. マスメディアとの連携

CCC は、ISP と連携して数多くのボット感染 PC の利用者に注意喚起を行い、ボットの駆除や再感染防止に努めてきた。こうした CCC の取組みは、多くのメディアで紹介され、ボット対策の必要性が広く理解される事に役だっている。

CCC の活動を通じて、ボット感染者の多くが十分なセキュリティ対策を行っていないことが浮き彫りになった。また何度注意喚起してもなかなか対策を行わないボット感染 PC の利用者も多くいることが分かってきた。CCC ではボット感染 PC の利用者を見つけ、注意喚起し、具体的な対策手段を提供してきたが、最終的にボット対策を行うのはボット感染 PC の利用者自身に他ならない。そのためには PC の利用者一人ひとりの意識を変えていくための地道な普及啓発活動は欠かせない。

ひとつのアプローチとして、マスメディアとうまく連携することでボット対策効果を上げられることも分かってきた。一般公開サイトにおける CCC クリーナーのダウンロード数の推移を図 6-2 に示す。

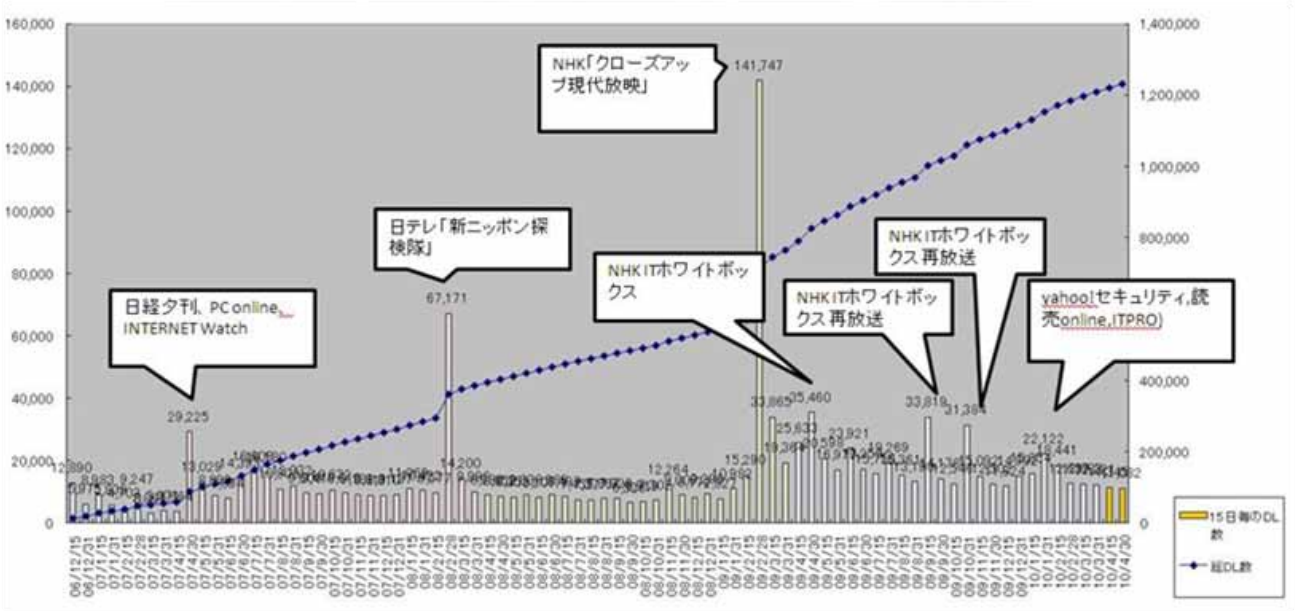


図 6-2 一般公開サイトにおける CCC クリーナーのダウンロード数の推移

CCC 開設当初よりマスメディアに CCC が取り上げられるたびに、一般公開サイトのアクセスが伸び、CCC ク

リーナーのダウンロード数が通常のダウンロード数より多くなっていることが分かっている。これはマスメディアに取り上げられることにより CCC の認知度が高まり、実際に CCC クリーナーのダウンロードという行動につながっていることを示している。このことは、ISP で行うメールによる注意喚起に「気付」かないボット感染 PC の利用者やハニーポットで検出できない PC ユーザにもマスメディアを利用することでリーチできる可能性を示しており、今後も積極的にマスメディアと連携し、広くボット対策の普及啓発を一般の PC ユーザへ図りたいと考えている。

6.3. 国際連携の必要性

ボットは国境を越えて感染するため、日本国内のボット感染 PC の利用者が減少し国内からの感染攻撃がなくなっても、海外のボット感染者が減少しなければ、ボット感染 PC からの感染攻撃がなくなることはない。攻撃事象収集型ハニーポットで収集した国別攻撃元 IP アドレス数の推移を図 6-3 に示す。この図 6-3 のグラフからは、国外からの攻撃が全体の 75%を占めていることが読み取れる。

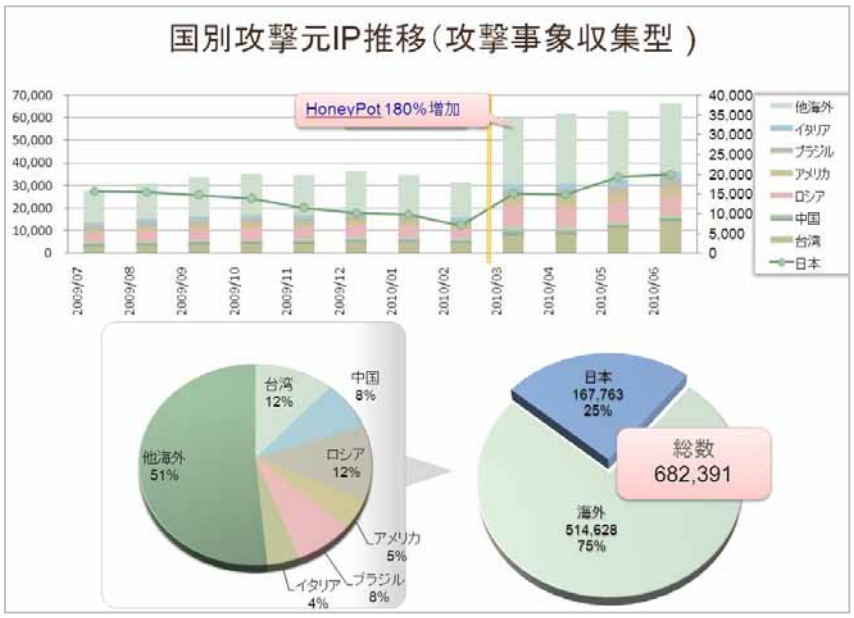
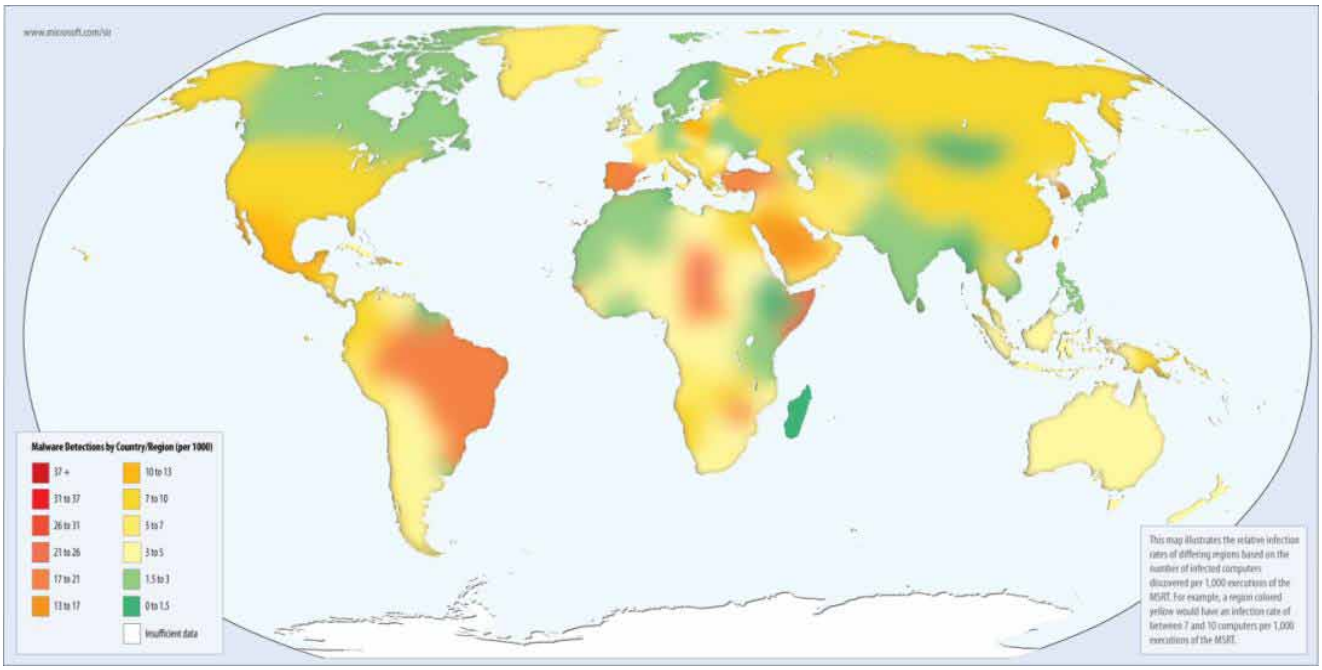


図 6-3 攻撃事象収集ハニーポットによる国別攻撃元 IP アドレス推移

2010 年 3 月にハニーポット台数を 20 台から 40 台の 2 倍に増設したことにより、国内や国外ともに攻撃事象の収集数が増加しているが、国内と国外の比率に関しては大きな変化はない。

マイクロソフト社が発表している Microsoft Intelligence Report July –December 2009(国別感染率)に示されているように、日本の感染率は世界的にみて非常に低いレベルに達している。



（Microsoft Security Intelligence Report 2009 July – December 2009 より）

図 6-4　国別感染率

国内のボット感染率を低く抑え続けるためには、国外からのボット感染を抑えることが重要である。そのためには、グローバルな視点に立ったボット対策を可能とする国際連携スキームを確立することが重要であると考えられる。

7. ボット対策として実施すべき事項

ボット対策として、PC 利用者一人ひとりが実施すべき個人でできる最低限のボット対策と、今後ボット感染を広めない対策についての提案を示したい。

(1) ブロードバンドルータを導入

ブロードバンドルータがなく PC が直接インターネットに接続する構成では、PC の OS や利用するソフトウェアにセキュリティホールと呼ばれるシステム上の欠陥や仕様上の問題点がある場合、外部からの感染攻撃により数分で感染してしまう恐れがある。

ブロードバンドルータを介して接続することにより、ブロードバンドルータの NAT 機能が外部からの感染攻撃を防いでくれるため、感染しにくい安全な環境を構築することができる。

参考:ブロードバンドルータの有効性(回線別地域別感染状況調査)

回線別地域別の感染ブロック(/16)率を 3 社の ISP で調査したところ、フレッツ ADSL においては、3 社とも同じように感染者が地域に依存することもなく捕獲できている。フレッツ光においては、西日本地域の感染検出ブロック率が、3 社とも低くなっている。これは、アクセス回線を提供する NTT 東日本、NTT 西日本において回線の提供時におけるルータを必須としているか否かによる。NTT 西日本では、光のアクセス回線は、「ファミリー100」と「光プレミアム」という 2 つの商品を提供しており、後者はルータが必須のサービスとなっており、会員数も光プレミアムが多い。このようにフィールドデータからもルータによりインターネット側からの感染攻撃による感染から防御されているため感染率が低いということがいえる。このことからもボット感染対策として、ルータが有効であることが分かる。

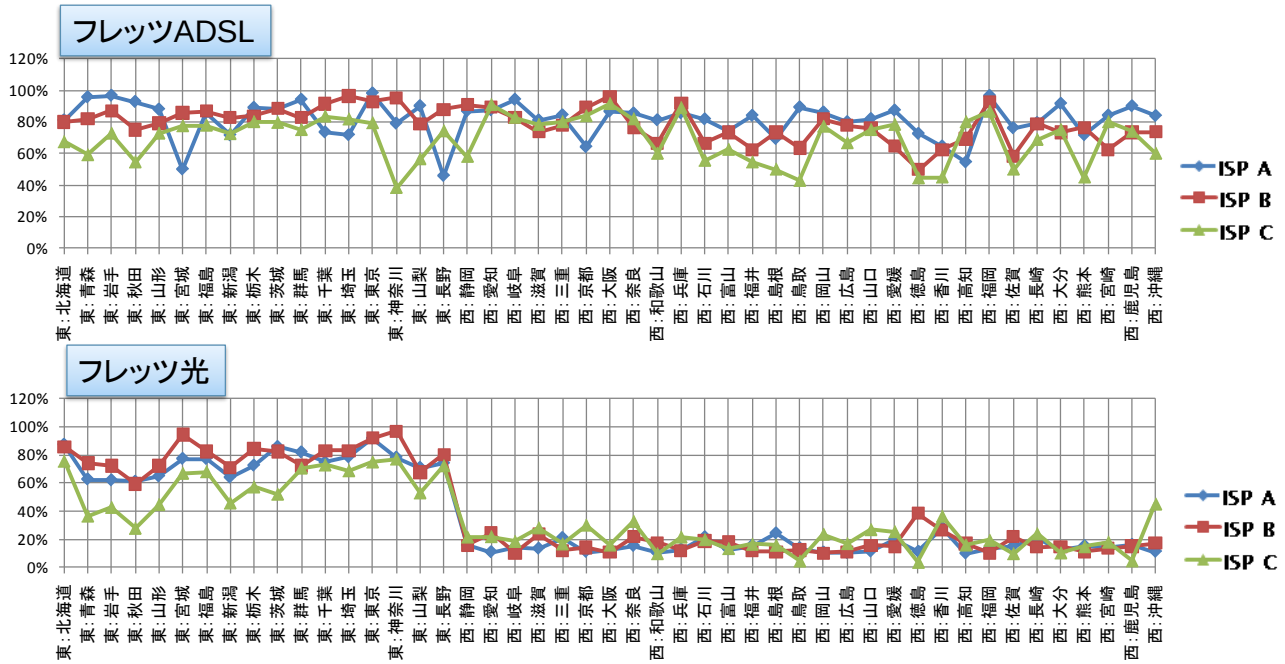


図 7-1 回線別地域別感染ブロック(/16)検出率

(2) OS、ソフトウェアのアップデートの実施

Windows をはじめとする各種 OS やソフトウェアで発見されたセキュリティホールは、製品の開発元から修正プログラムが公開される。

ソフトウェア等のセキュリティホールによってウイルスに感染したり、コンピュータが悪用されたりする場合が多くあることから、セキュリティホールを修正せずにそのまま利用することは非常に危険な状態で放置していることになる。

特に、Windows はボットのセキュリティホール攻撃で狙われやすいため、マイクロソフト社は「Microsoft Windows Update」を最低でも毎月必ず実施することを推奨している。

また、最近では PDF ビューワー「Acrobat Reader」「Adobe Flash Player」、「Java Runtime Enviroment」、「Microsoft Office」、などの周辺アプリケーションのセキュリティホールを狙ったマルウェアも確認されており、OS のアップデートだけでなく利用しているソフトウェアを常に最新の状態に保つことが重要である。

(3) ウイルス対策ソフトを導入

インターネット上には様々な危険が潜んでおり、インターネット上のサービスを利用することでコンピュータウイルスに感染する危険性がある。このため、ウイルス対策ソフトを利用してコンピュータウイルスに感染する危険性を軽減することができる。

また、ウイルス対策ソフトを利用していても、ウイルス定義ファイルの更新期限が切れている場合や、定期的な更新を行っていない場合には新種ウイルスに対応することができない。ウイルス対策ソフトは常に最新の状態に保ち、定期的にコンピュータをスキャンすることによって、ウイルスに感染していないことを常に確認することが重要である。

(4) ポートブロック実施の提案

ボットは特定の TCP/UDP ポートを利用して感染することが知られている。具体的にはボット感染の多くが、Windows のファイル共有サービス等で利用する（TCP/UDP ポート 135-139、445）を通じて行われており、これらのポートをブロックすることはボット感染拡大を防ぐ上で有効である。

CCC では特定ポートをブロックすることによるボット感染拡大防止に関する調査を行ってきた。その結果、これらの特定ポートをブロックすることで、ボットの感染拡大を抑止できることを確認している。2010 年 4 月 8 日から約 2 カ月間において行ったブロックするポート別のボット検体収集数の推移と Drop した攻撃事象を示すログ数を図 7-2 に示す。

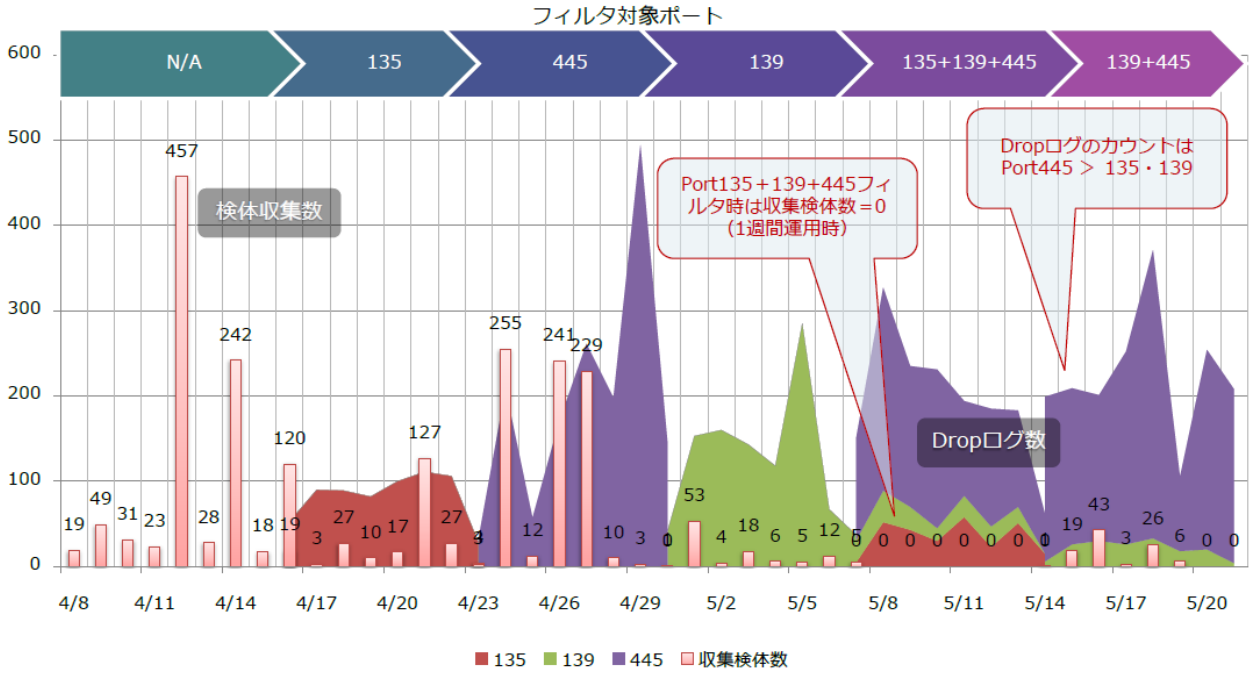


図 7-2 ポート別 ポートブロック効果

この調査では、4 月 8 日より、まず 1 週間何もポートブロックを行わず、ハニーポットへ感染攻撃が行われたかを確認後、ポート 135、ポート 445、ポート 139、そしてポート 135、139 および 445 の 3 つのポートを同時にブロック、最後にポート 139 と 445 の 2 つのポートを同時にブロックした場合について調査を行った。図中の棒グラフがボット収集検体数を示しており、個別ポートのブロックにおいても収集数の減少を確認できるが、3 つのポート（ポート 135、139、445）を同時にブロックした場合、期間中検体を収集することはなかった。

このように、特定ポートをブロックすることはボットの感染拡大抑止に非常に効果的であることから、今後のボット対策手法のひとつとして特定ポートのブロックを提案したい。

ポートブロックは、インターネットに接続する PC の利用者がブロードバンドルータやファイアウォールの設定をすることで実施できるが、その対応は利用者一人一人に委ねられることから、すべての PC の利用者がポートブロックを適用することは難しい。一方、ISP 側で一律的にポートブロックをすることで、すべての利用者を対象にボットの感染拡大を抑止することが可能となる。

しかしながら、現行の法制度下では ISP ネットワークでのポートブロックは通信の秘密の侵害に抵触する可能性があることから、法制度上の整備を進めていくことが必須となる。また、特定ポートをブロックすることが、利用者の利便性を損ねることがないか、ISP の運用上支障がないかなどについても十分に議論を重ねた上で慎重に検討を進めていく必要がある。

8. さいごに

2006 年 12 月、国内ボット感染者を限りなくゼロにするという目標を掲げて活動を開始したボット対策プロジェクト「サイバークリーンセンター(CCC)」は、総務省、経済産業省およびセキュリティ関連組織、企業が連携してボット対策を進めていくという我が国初の試みであるだけでなく、世界的に見ても数少ない事例といえる。

本プロジェクトでは、ISP やウイルス対策ベンダと連携して数多くのボット感染 PC の利用者に注意喚起を行い、ボットの駆除や再感染防止に努めてきた。こうした活動により、個々の ISP における注意喚起対象者数は減少傾向にあり、国内ブロードバンドユーザにおけるボット感染率は 2005 年に 2～2.5%であったのが、2008 年には 1% にまで減少した。本取組みは、多くのメディアで紹介され、ボット対策の必要性と活動に対する認知度も向上し、国外におけるボット対策関連組織等からも注目されるようになった。このことは、本活動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考えている。

しかしながら、いくつかの課題もある。そのひとつは、ボット感染 PC の利用者の多くが十分なセキュリティ対策を行っておらず、しかも何度注意喚起してもなかなか対策を行わないユーザが多くいることが分かっており、これらのユーザに対処していく必要があることである。本活動を通じて、ボット感染 PC の利用者を見つけ、注意喚起し、具体的な対策手段を提供してきたが、最終的にボット対策を行うのはユーザ自身に他ならない。そのためにはユーザー人一人に対するセキュリティ意識を向上させていくための地道な普及啓発活動を継続していく必要がある。

もうひとつは、ボット感染攻撃は国内からだけではなく海外からも行われていることから、国内ボット感染 PC をなくしていくためには、こうした海外からの感染攻撃に対しても国際的な連携フレームを活用し、コーディネーションをしつつ対処していく必要がある。そのためには、CCC の成功事例等を海外へ積極的に発信していく必要があるということである。

今後は、CCC のノウハウを活かして国際的にも連携できる体制を構築していき、ボット対策活動を継続した取り組みとして拡大するべきであると考えている。

参考文献

[1] 高橋正和、他. フィールド調査によるボットネットの挙動解析. 情報処理学会論文誌. 2006, Vol.47, No.8, p. 2512-2523.

[2] 有村浩一. ボット対策プロジェクト「サイバークリーンセンター」からみた国内のマルウェア対策. 情報処理. 2010, Vol.51, No.3, p.275-283.

[3]中津留勇、他. マルウェア検出情報ログの分析による対策の検討. 情報処理学会 コンピュータセキュリティ 研究報告. 2010, Vol.2010-CSEC-49, No.2.

[4] "IT Keys - 先導的 IT スペシャリスト育成推進プログラム. http://it-keys.naist.jp/, (参照 2010-08-20).

[5] "マルウェア対策研究人材育成ワークショップ. http://www.iwsec.org/mws/2010/, (参照 2010-08-20).

[6] "Microsoft Security Intelligence Report volume 8 (July - December 2009)." http://www.microsoft.com/downloads/details.aspx?FamilyID=2c4938a0-4d64-4c65-b951-754f4d1af0b5, (accessed 2010-08-20).

[7] "ボットネット概要." JPCERT/CC. 2007-04. http://www.jpcert.or.jp/research/2006/Botnet_summary_0720.pdf, (参照 2010-08-20).

[8] 小松文子、他:情報セキュリティ対策は社会的ジレンマか？－ボットネット対策への適用－. 情報処理学会 コンピュータセキュリティ 研究報告. 2009,Vol.2009-CSEC-46 No.41