特集
マルウェア

6

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

有村浩一（（財）日本データ通信協会 Telecom-ISAC Japan 推進協議会／NTT コミュニケーションズ（株））

サイバークリーンセンター誕生のきっかけ

2004 年春

国内大手のインターネットサービスプロバイダ(以降，ISP）である事業者 A の商用メールサーバに対して大量のスパムメールが発信された．発信元のメールアドレスを国内大手の ISP である事業者 B, C に偽装していたことから，膨大な数の宛先不明に伴うエラーメールが事業者 B, C の商用メールサーバに殺到した．多量のエラーメールはサーバに大きな負荷をかけ，サービス継続さえ困難な状況となった．図 -1 に示すこの攻撃は，明らかに従来のスパムメールの手法とは異なっていた☆1．

ボットのしわざ！？

感染すると，外部からの指示を待ち与えられた指示に従って各種の処理をまるでロボットのようにこなすことから，ボットと呼ばれている新型マルウェア．多くの亜種が存在するため従来のシグネチャ型のアンチウイルスソフトでは検出困難である．感染と攻撃活動を制御しているため，感染の事実にすらユーザは気がつかない．この新たな脅威に対して，ISP ができることといえば IP アドレス単位で通信をブロックすることであるが，発信元が広範囲に渡るため，対策手法として使うことができない．こうして，深刻な脅威に直面した ISP を中心にボット対策が検討されはじめたのである．

総務省・経済産業省の連携プロジェクト「サイバークリーンセンター（Cyber Clean Center，以降，CCC と記す）」は，新型マルウェア，ボットから我が国のインターネットを守ることを目的とした，2006 年 12 月に開始した我が国初の大規模かつ本格的なボット対策プロジェクトである．本稿では，CCC の概要を紹介し，この対策の効果を考察する．また，CCC の設立に至った経緯，プロジェクト開始前に実施したボット実態調査，そこから導いた CCC 対策設計のプロセスなどを紹介する．

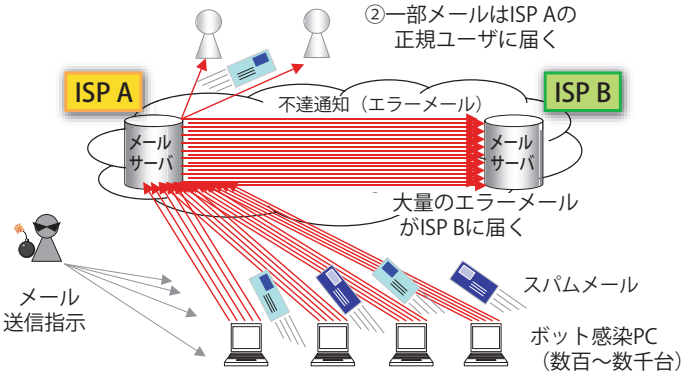

図 -1　ボットによる攻撃の表面化

ボット実態調査

Telecom-ISAC Japan☆2 の会員会社であった 3 社は，新たな攻撃事象を Telecom-ISAC Japan の会員に事例紹介し情報共有を図った．その結果，同様の脅威の増大に備え，Telecom-ISAC Japan 会員が中心となり業界横断的な調査と対策検討を行うことになった．調査の結果，本スパムメール発信は，その様態から，当時日本ではまだあまり知られていなかったボットネット☆3 による可能性が濃厚になったこと，ネットワークを通じて PC の脆弱性を攻撃して感染を拡大する「ネットワーク感染型☆4」であること，そして，感染力が強く ISP のサービス継続

☆1 事業者 A は緊急対処のために事業者 B, C と連携を図るとともに，メール発信元の IP アドレスを解析したところ，メール発信元が数百から数千あり，少数のメール発信元から大量発信するそれまでのスパムメールとは様態が明らかに異なることが判明した(図 -1)．

☆2 日本国内の大手の ISP や通信事業者などを会員とする非営利会員制組織．2002 年発足．会員数 18 社（2009 年 11 月現在）．情報通信サービスの安全かつ安心な運用の確立を目的に，テレコム通信事業者を含む会員が関連情報を共有分析し，サイバー空間で発生する 1 事業者では手に負えない大規模な問題に対して業界横断的にタイムリーな対策をとる場を提供するための活動を行う．
https://www.telecom-isac.jp/

☆3 ボットと呼ばれるマルウェアに感染したホストの集合体である．当時はゾンビ・クラスタと称した．

☆4 ネットワーク感染型としては，ワームに属する CodeRed や MSBlaster が有名である．

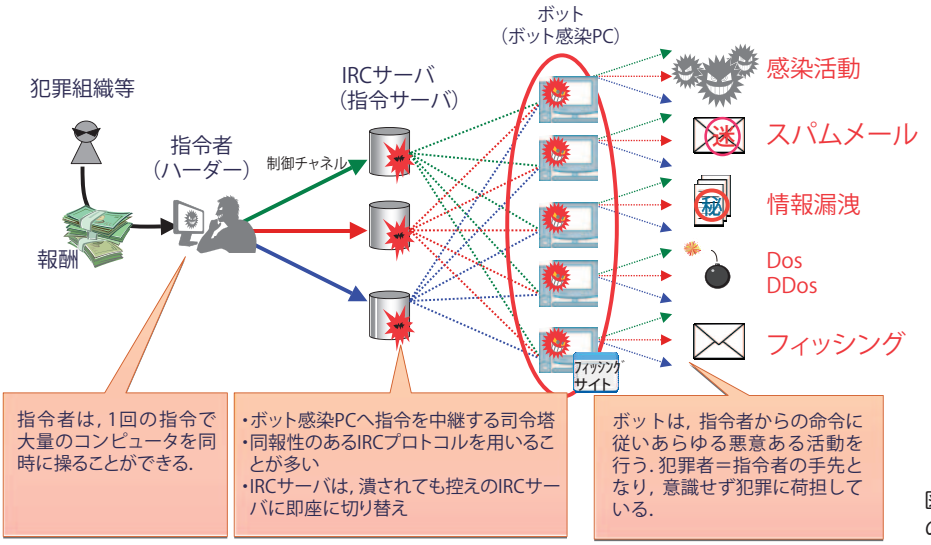

図 -2　ボットネットの構造

に最もリスクを与えることなどが分かってきた．

●調査概要

ボット対策の立案にあたり，ボットの機能と仕組みと我が国の感染実態を知ることが必要である．当初の調査結果を踏まえつつ，ボットの機能と仕組みを解明するために，ネットワーク感染型ボットとして当時よく知られていた Agobot（別名：Phatbot/Gaobot）のプログラムをインターネットから入手し，プログラムを分析する静的解析と，実験環境下で実際にプログラムを動作させる動的解析を行った．後者のハニーポットによる観測には，Telecom-ISAC Japan の ISP 会員の協力を得た．調査内容の詳細は文献 1)に譲り，ここでは CCC 業務設計や運用上，役立てた知見を紹介する．

●静的解析・文献調査

対アンチウイルスソフト対策

ボットにはポリモーフィックエンジン☆5 が搭載され，実行コードを暗号化することでアンチウイルスソフトによる検出を避けていた．これにより最新版シグネチャでも検出が困難で，未検出検体の数と種類も多数になる事態が予想された．

それだけではない．

600 を超えるアンチウイルスソフトの実行プロセスリストを持ち，このリストにあるプロセスを停止させる．30 以上のアンチウイルスソフト関連のアップデートサイトへのアクセスを妨げ，シグネチャ更新を防ぐ．このようなさまざまな妨害工作により，アンチウイルスソフトが意図通り動かずにボットに感染した PC（以降，ボット感染 PC）の復旧には相当の手間がかかりそうである．エンドユーザ対策が煩雑化することが懸念された．

ボットネットの構成

調査が進むにつれて，ボット感染 PC をネットワークで制御するボットネットの全体像も明らかになってきた．多くのボットネットは同報性のある IRC☆6 プロトコルを通信チャネルとして使用し，ボット感染 PC と接続する．ハーダー☆7 と呼ばれる指令者が(複数台の）IRC サーバ（当時，ボットを制御する指令サーバとして IRC サーバが使われていた）を介してボット感染 PC をリモート操作して悪意ある各種活動を行うことが分かってきた（図 -2）．全体像把握は対処方針立案の参考となった．

●動的解析

脆弱性を残した Windows2000（SP なし）を利用して小規模なハニーポットを構築し，複数の ISP が提供した IP アドレスへの攻撃トラフィックを誘導し，ボットとの通信状況を観測した．また，このハニーポットで収集した検体を実験的に構築したネットワーク環境下で動作させることで動的解析を行った．

収集検体の既知・未知分類結果

42 日間 192 個の IP アドレスを使用し，1 日あたり 758 件，88 種類のボット検体を収集した．これらを最新版シグネチャを実装した市販アンチウイルスソフトにより既知・未知に分類した．検出数では 90% が既知検体であったが，検体種別では 80% が未知であった．多数の既知のボットが活動を行うとともに，1 日平均約

☆5 ボットが感染する際に自らをランダムな暗号化コードで書き換え，暗号化するために使用する機能のこと．毎回自らを書き換えることでアンチウイルスソフトのシグネチャを用いたパターンマッチング方式による検出を困難にする．

☆6 Internet Relay Chat の略で，インターネット上のチャットシステムで使用されるプロトコルである．

☆7 ボットに感染した複数の PC を羊の群れのごとく操ることから「羊飼い」（Herder）に例えられている．

70種類の新規検体が作られていることになる．これらは，最新版シグネチャを持つアンチウイルスソフトでも防ぎきれない．

IRCサーバの構成

収集した検体の中から，数の多い検体100種類を選び，静的解析から検体に埋め込まれたドメイン名を取り出した．これらのドメイン名の登録状況とIPアドレス調査の結果，①公開されたIRCサーバ等にアクセスするためのドメイン名ではないこと，②約20%のボットが複数のIRCサーバを持つこと，③Dynamic DNSサービス等を利用するものが半数を占めたこと，④IRCサーバに複数のドメイン名が割り当てられていることが明らかになった．②〜④の実装は大規模なボットネットの維持・管理を容易にするだけではなく，IRCサーバの発見を困難にし，1つのIRCサーバが停止しても他のIRCサーバが機能を補償してボットネット全体の可用性を高める効果がある．

感染方法(攻撃に利用される脆弱性)

観測した攻撃の半分以上はMS03-026とMS04-011を利用した攻撃が占めていた[☆8]．これらの知見は感染PC対策の回復手順設計に活用した．

感染直後の他PCへの感染拡大活動

ボットには，次のような特徴がある．感染直後に感染したIPアドレスの近傍IPアドレスをスキャンして感染拡大行為を行う，IRCサーバへの接続直後に，実行ファイルを更新する．これらの特徴はハニーポットに対するIPアドレス割り当て，リセット間隔時間設定，内部感染防止対策などの性能設計の参考にした．

●感染実態調査

感染率

静的解析の結果から判明した複数のドメイン名の名前解決を行うIPアドレスはボットに感染している，と見なして感染率を定義した．すなわち，ボット感染率は，一定期間内にDNSの名前解決を行った総IPアドレス数に対する複数の名前解決をしたIPアドレス数の比である．Telecom-ISAC Japanを通じてISPに対して行った感染率の調査の結果，複数のISPの回答から，2〜2.5%の感染率と推計した．当時の日本のブロードバンドユーザ数が2,000万人なので，国内のボット感染数は40〜50万人となる．これらの数値からボット感染の規模が得られた．

ISPにおけるDNSアクセスを観測すれば，ボットに感染しているIPアドレスが特定できる．そのIPアドレスからユーザが特定できれば，ユーザにボット対策を働きかけることができる．このことはその後のボット対策策定のヒントとなった．

☆8 MS03-026は2003年に流布したMSBlasterが感染の際に利用した脆弱性で，MS04-011は2004年に流布したSasserが感染の際に利用した脆弱性である．

ボットネット構成要素，対策検討内容	対策評価
1. 指令者(ハーダー) • 日本を狙う指令者は日本にいないことが多い • 指令者の発見，逮捕はそもそも法執行機関の役割 • 指令者を割り出すことは技術的困難	実施が難しい
2. IRCサーバ(指令サーバ) • 日本を攻撃するIRCサーバは主に海外に存在する • 潰しても潰してもボット感染PCが次々とIRCサーバに昇格する仕組みが動的解析で判明．きりがない • 各国とも犯罪者を捕まえるために意図的にIRCサーバを観察対象として活動させているケースがあり，容易に手が出せない	実施が難しい
3. ボット感染PC，ボット感染ユーザ • ISPであれば，自社の感染ユーザ(お客様)に個別にアプローチでき，ボット駆除の注意喚起を行うことが可能 • その際に再感染防止についての対応も周知・依頼すればユーザリテラシーの底上げも期待できる • ボット駆除の注意喚起を顧客満足度向上の機会につなげる	ISPとの協力により実施可能

表-1　ボットネット構成要素に対する対策評価

CCCプロジェクト誕生

●ボット対策の方針立案

ボット対策を感染ユーザ対策に絞り込んだ理由

ボット対策の対象候補には，ボットネットを構成する3要素，すなわち，指令者（ハーダー），感染PCを制御するIRCサーバ，ボット感染PC（ボット感染ユーザ）がある．これらの各候補に対する対策評価をISPの立場から検討した(表-1)．

以上の検討から，対策の対象をボット感染PC，ボット感染ユーザに絞り込んだ．

注意喚起ワークフロー設計方針

ボット感染ユーザへの対処は，感染ユーザの特定と注意喚起，感染PCからのボット駆除，再感染防止の抜本的対策実行への誘導からなる．当時の感染率から，我が国の感染PC数を想定し，その規模をこなすプロセスの設計が目標となる．感染事象は多数で昼夜問わず発生することから，自動化・省力化・24h7d運転のワークフローとシステム設計を目指す．

これまで，ISPやセキュリティ関連団体はユーザに対して電子メール，Webサイト，他のメディア媒体を通じてセキュリティ啓発や感染対策について繰り返し情報提供を行ってきたが，メッセージを受け取ったユーザが

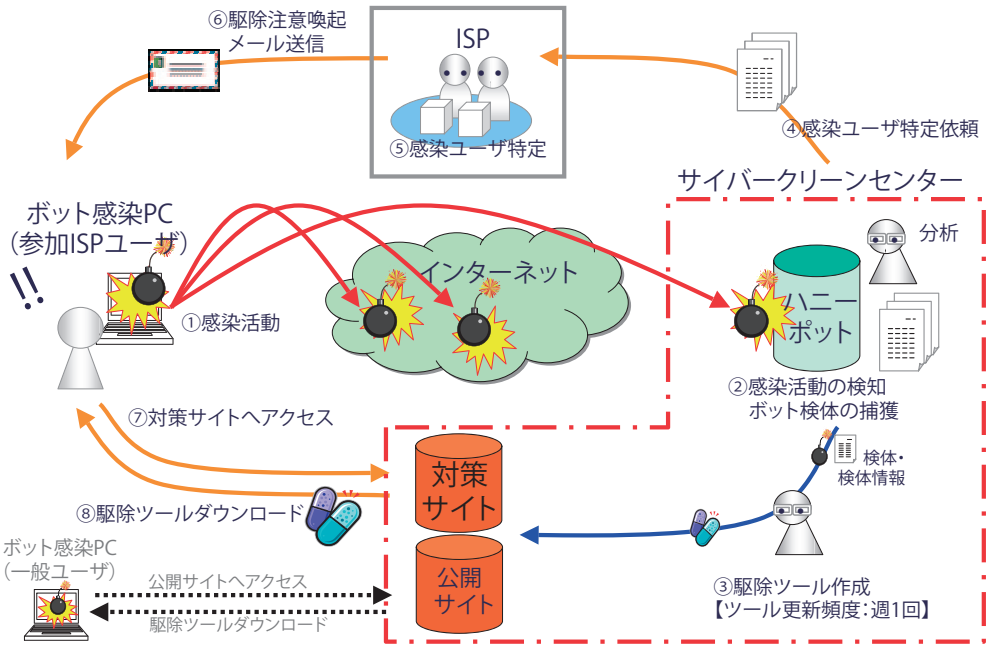

図 -3　CCC 注意喚起ワークフロー

手を動かさない限りその効果は上がらない．感染事実を通知しただけでは，ユーザはボット駆除対策のために手を動かせない．特に，市販のアンチウイルスソフトで駆除できない未知のボットについては，駆除手段がないまま通知することになる．そこで，ハニーポットで収集したボット検体を元に駆除ツールを作成し，具体的な対策手順とともに通知する．さらに，注意喚起対象者に対してボット感染ユーザであること，ボットが外部に感染拡大しようとする攻撃トラフィックが捕捉可能であること，感染拡大の際にハニーポットに感染させるボットは既知・未知を問わず収集可能であることを周知させて積極的に防止活動をさせることを試みた．

●注意喚起ワークフローの概要

CCC にはハニーポット群と対策情報発信のために 2 つの Web サイト（以降，対策サイト，公開サイトと記す）がある．これらの設備を使用して，図 -3 に示す CCC 注意喚起ワークフローを実現している．

感染活動(図 -3，①)

ボット感染 PC はインターネットを介して感染活動を行う．

感染活動の検知，ボット検体の収集(図 -3，②)

ハニーポットでは，発信日時，発信元 IP アドレス，脆弱性を攻撃してハニーポットに送り込まれたボット検体を記録ならびに収集する．

駆除ツール作成(図 -3，③)

ハニーポットで収集したボット検体を元に駆除ツール「CCC クリーナー」を作成する．日本で活動するボットの駆除効果を高めるために，日本での感染拡大の兆しがある検体や急増する未知検体を駆除の重点対象としている．CCC のハニーポットにおける検体収集数の状況，収集検体の既知・未知分析結果などを元に重点駆除対象を総合判定し，CCC クリーナーを定期的に（現状は週 1 回）更新する☆9．

感染ユーザ特定依頼(図 -3，④)

提供予定の CCC クリーナーが駆除対象とするボットの発信元 IP アドレスは，感染活動の検知，ボット検体の収集作業で記録済みである．しかし，発信元 IP アドレス等を手がかりに感染 PC を所有する感染ユーザを個別特定できるのは ISP だけである．そこで，発信日時と発信元 IP アドレスのリストを作成し，ISP に感染ユーザの特定依頼を行う．

感染ユーザ特定(図 -3，⑤)

CCC からユーザ特定依頼を受領した ISP は発信日時に発信元 IP アドレスを使用した感染ユーザ（連絡先）を特定する．こうして，ボット感染 PC，そのボットを駆除する CCC クリーナー，ボット感染 PC を所有する感染ユーザの情報（連絡先）が 1 本の糸のようにつながっていく．ボット感染症状に応じてユーザ(患者)に適した CCC クリーナー（薬）を届ける，いわば「テーラーメードな薬の提供」が実現できる．

なお，対応づけたこれらの情報はトラッキング ID と呼ぶ固有番号で情報管理し，処理状況の進捗管理などに活用する．

☆9　この作業は，プロジェクト協同パートナーである JPCERT/CC が担当している．

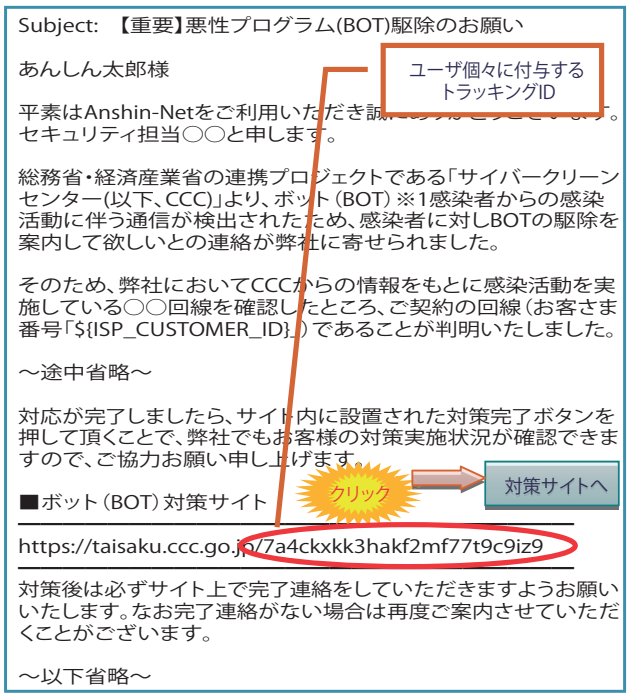

図 -4　注意喚起メール文例とトラッキング ID

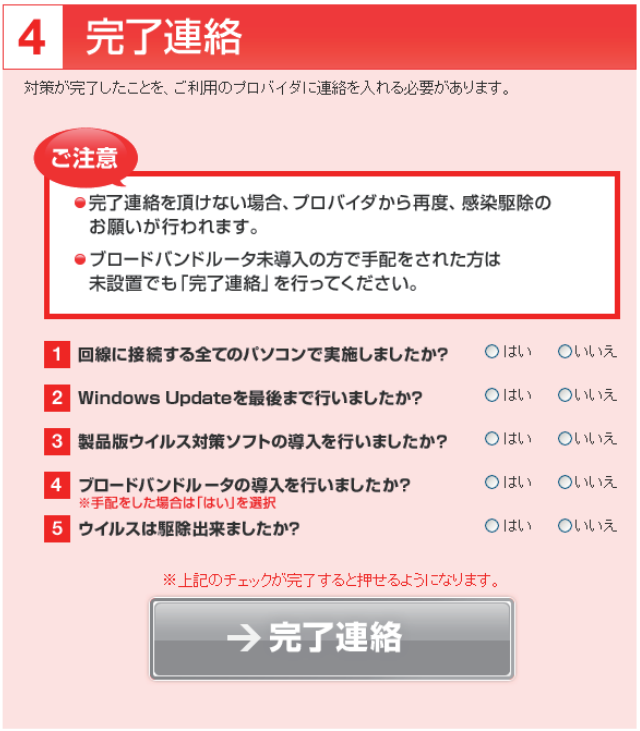

図 -5　完了連絡画面の例

駆除注意喚起メール発信(図 -3，⑥)

完成した CCC クリーナーは図 -3 の公開サイト(https://www.ccc.go.jp/)と対策サイトの両方にアップする．公開サイトは一般向けの CCC 情報発信用の Web サイトである．インターネットを利用する一般ユーザは最新版の CCC クリーナーをこの公開サイトから入手できる．また，ボットの駆除対策手順，感染防止のための知識などの情報発信にも使用する．

一方，対策サイトは感染ユーザのためのサイトである．CCC クリーナーを対策サイトへアップするタイミングに合わせて，ISP は特定できた感染ユーザに注意喚起の電子メールを発信する(図 -4)．

メール内容は，(1) ボット感染 PC が行った外部への感染活動を観測したこと（感染事実の通知)，(2) 観測活動の履歴（攻撃日時，管理のために CCC 側で付与したボットの ID）へのアクセス方法，(3) ボット駆除の依頼，(4) 駆除に適した CCC クリーナーの無料提供案内とその入手方法（対策サイトへのアクセス）などである．CCC クリーナー提供という具体的な解決方法をセットにした駆除依頼を行うことで，メールの読み捨てを防ぎ，ボット駆除の実施率引き上げを狙った．

メールで案内する対策サイトの URL にはトラッキング ID を含む工夫をした (図 -4)．これにより，アクセス先にて感染状況に応じたきめ細かな提供情報が可能となる．また，対策サイトへのアクセス状況，サイトでの作業推移状況，CCC クリーナーのダウンロード状況など感染ユーザの行動特性が感染事象ごとに管理できる．行動特性の分析結果は注意喚起ワークフローの効果測定と改善に有益であった．

駆除ツールダウンロード・ツール実行(図 -3，⑧)

駆除対策手順に従い，CCC クリーナーを感染 PC にダウンロードして実行し駆除対策を終了すると，CCC クリーナーは駆除状況（検索したファイル総数，駆除したファイル総数，ボットを検出したファイル総数，ボット駆除ができたファイルの総数，駆除されていないファイルの総数など）を記載したログを作成し，それらをクリーナー実行結果のレポートとしてポップアップ表示する．最後に，図 -5 のようなアンケートに回答いただき，完了連絡を行う．完了連絡時に，ユーザ了解のもと，回答結果，CCC クリーナー駆除状況，感染していたボット名リストを CCC へ送信する．

これらの情報はハニーポットでは観測しきれない感染ユーザの実態を示す情報であり，ボット対策の改善に活用する．以上の処理を循環させることにより，ボット感染 PC を減らしていく．

●注意喚起ワークフローにおける各種工夫

注意喚起の効果向上のためにワークフローの随所に行った代表的な工夫を紹介する．

go.jp ドメイン利用

ボット感染対象者に注意喚起メールを発信し，メール本文の URL にて Web サイトに誘導し，CCC クリーナ

ーの利用を促す方式は，フィッシング詐欺の手口と紙一重である．電子署名付きメールにより発信元なりすましやデータ改ざんを防止する技術はあるが，ボット感染ユーザの多くがセキュリティの初心者であろうから，受信した電子署名付きメールの扱いが分からず破棄する可能性が高い．電子署名付きメール本文の冒頭に取扱方法を記載しても解決策とはならない．そこで次善策として，CCC のシステムは go.jp ドメインで運用し，総務省・経済産業省によるプロジェクトであることを強調することとした．対象者の疑念を少しでも払拭する効果を狙っている．

ハニーポット

ハニーポットの運用規模とボット収集能力が本システムの注意喚起力を左右する．日本のボット感染を減らす目的から，国内インターネットアドレス空間をできるだけ広くカバーすることを追求した．現システムでは，ハニーポットで検知した攻撃元 IP アドレスが，(/16 単位の換算で) 国内インターネットアドレス空間のうち 7 割をカバーする規模で運用している．

限られた時間でボット感染 PC を検出するには，ハニーポットに割り当てる IP アドレスを頻繁に変更すると効果的である．そこで，動的 IP アドレスのブロードバンド回線を用いて IP アドレスの自動再割り当てを実行している．

近年のボットは感染後にユーザに気づかれないよう，目立たず静かに動作する．ボット感染の自覚がないユーザが ISP から注意喚起メールを受領した際に，言われなき疑いと考え ISP に対して抗議してくるかもしれない．たとえば，感染させるために脆弱性を探そうとする行動だけでは確実な証拠とは言えない．そこで，ハニーポットでは感染行動だけではなく，確実に不正行為を行うボットのバイナリがハニーポットにダウンロードされ，それが起動して外部に通信を始める事象までを記録保存して，証拠を固めた．

感染したハニーポットは外部に向けた感染活動を行う．感染活動の通信はすべて遮断しなければならないが，ポート番号が頻繁に変化するためファイアウォールで制御するのは非常に煩雑である．そこで，CCC では，検体解析により外部攻撃に使用するポート番号のリストを作成し制御する方法を採用した．

また，ボットは近隣の IP アドレスに対して感染活動を行う．大量に並べたハニーポット同士が，互いに感染活動を繰り返さないよう，すべてのハニーポットは異なる VLAN へ収容し，ルーティングしない仕様にした．

トラッキング ID

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．

感染ユーザの中には，複数種類のボットに同時感染したり，メールを何回出しても対策サイトにアクセスしなかったり，案内した対策手順の最後までたどりつかなかったりすることも多い．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．

CCC はトラッキング ID を元に ISP に注意喚起メール発信依頼を行うので，トラッキング 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といった段階的対応が可能になる．この段階的対応を自動化するメール発信ツール(注意喚起クライアント)を開発した．

CCC クリーナー更新日・注意喚起メール送出日

CCC クリーナー更新間隔や注意喚起メール送出日間隔は，注意喚起ワークフローの能力を左右する重要な基本値である．間隔を狭くすれば，ボット攻撃の変化を追従する素早い対応が可能となるがコスト上昇要因となる．多すぎる警告メールは駆除協力意志を損なうかもしれない．そこで，現状では，クリーナー更新頻度は週 1 回とし，注意喚起メールを週 1 回発信している．注意喚起メールはボット感染ユーザに週の中日あたりに届く工夫をした．日常が忙しいユーザは週末に作業することを期待し，週末までの記憶に残る 2, 3 日前を狙っている．我々の繊細な配慮をどうか汲んでいただきたい．

CCC クリーナーの有効期限

CCC クリーナーもプログラムである以上，不具合が発生する可能性がある．不幸にして，配布した CCC クリーナーに深刻な不具合（ユーザのデータを破壊するなど）が見つかった場合に，その影響をいかに最小とするべきか？

もちろん，不具合の修正だけではなく，すでに使用中のユーザに対して使用停止と削除依頼の通知を行うが，必ずしも，すべてのユーザに確実に通知できる保証はない．ユーザによっては，必ずしも削除してくれるとは限らない．このような運用を経てたどり着いた 1 つの答えが，CCC クリーナーに動作有効期限を設定する方法である．

注意喚起ワークフローの適法性

ボット感染ユーザへ注意喚起のメッセージを届けるための身元特定や，感染 PC の通信情報を収集する行為などは，電気通信事業法や個人情報保護法などを遵守して行わなくてはならない．プロジェクト開始前にワークフローに係る法的な懸念点を検討した．

(1) 個人・顧客情報保護

CCC 注意喚起の要は，感染 PC のユーザ（正確には，感染 PC が接続しているインターネットの利用申込者）に注意喚起を届けるところにある．発信元 IP アドレス

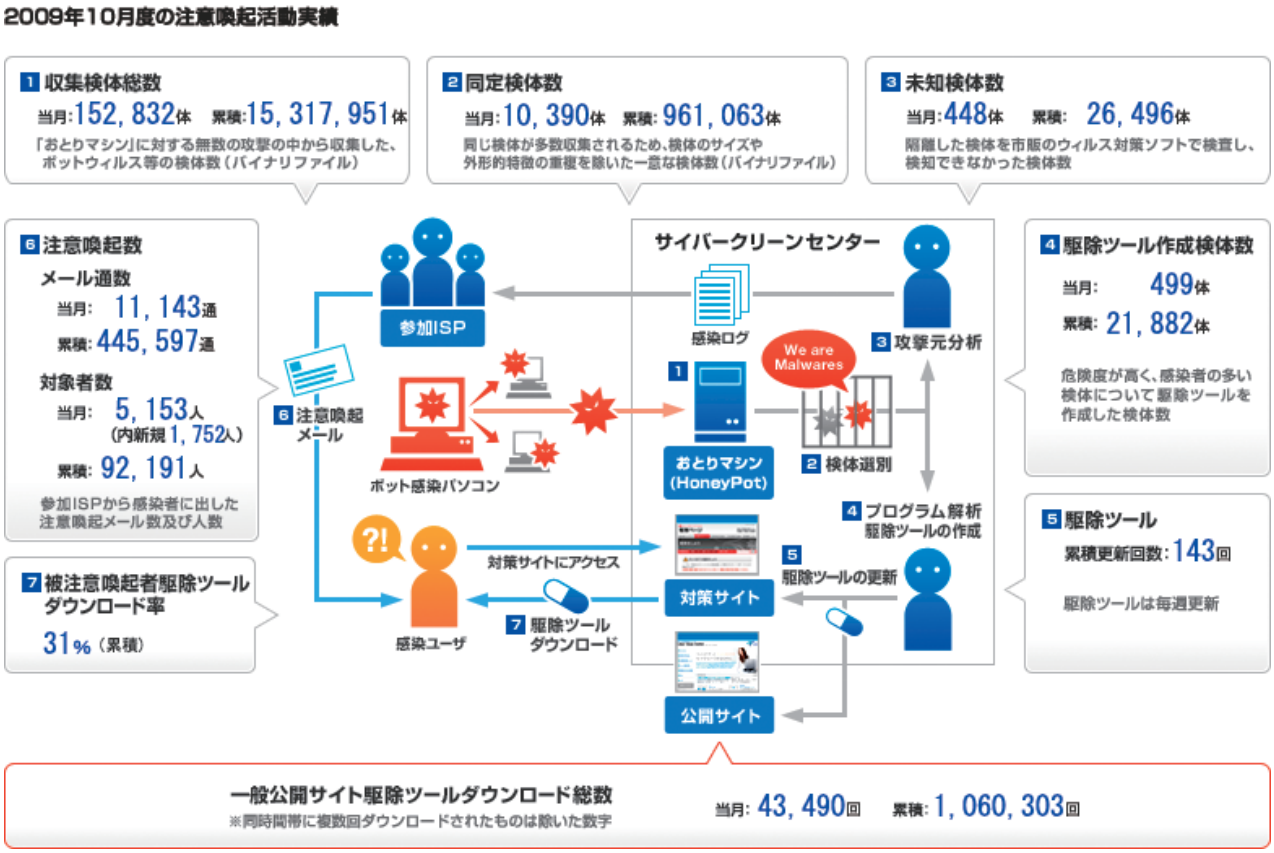

図 -6　2009 年 10 月度の注意気喚起活動実績

だけでは，ハニーポットが記録した発信日時に当該 IP アドレスを使用していた個人や連絡先を特定できない．特定には協力 ISP の社内情報（顧客契約情報，接続情報など）が必要である．これらの情報は法的保護を求められる重要秘密情報である．ワークフローでは ISP の社内情報を ISP が CCC や他の協力 ISP に提供したり，共有する設計にはなっていない．CCC と ISP との間では発信元 IP アドレスとユーザ識別 ID を共有するものの，ユーザ識別 ID だけではユーザの特定は不可能である．こうして，顧客・個人特定にかかる情報を CCC は有していないと結論づけている．

(2) 通信の秘密の侵害

ボット感染 PC から見ると，ハニーポットは通信相手である．ハニーポットを所有する CCC は，通信の片端に位置する当事者であり，意図しない攻撃通信を受けている被害者である．被害者が加害者を収容する ISP に対して，加害者の迷惑な通信行為を止める依頼を行い，ISP はその依頼を仲介していると位置付けている．これにより，ISP は，加害者の通信内容を無断で見たり，加害者の情報を被害者に無断で教えるなどの通信の秘密を侵害する行為は行っていないと解している☆10．

CCC プロジェクトの効果

●活動実績

2009 年 10 月までの活動実績を図 -6 に示す．数字は月間の実績とプロジェクト開始から 2009 年 10 月までの累積である．10 月の検体収集総数は約 15 万，累積数は約 1,500 万である．同じ検体が複数あるので重複を除くと（図中，同定検体数）月間で約 1 万，そのうち市販の（最新版）アンチウイルスソフトで検査して検知できなかった未知検体の種類数は月間 448 種類，1 日平均約 15 種の勘定となる．

当月の注意喚起のメール数は約 11,000 強で，累積は約 45 万である．1 人で複数台のボット感染 PC を所有したり，1 カ月間に複数回感染した場合，複数のメールを出す．したがって，対象者数はメール通数より少ない．当月約 5,100 人の注意喚起対象者数のうちメールを初めて出した対象者数（図中のうち新規）は約 1,700 である．この差，約 3,400 名が繰り返し注意喚起メールを受領している．根付いてしまったこれらのボット感染ユーザを減らしたいとの願いを込めて仲間うちでは「根ボッ

☆10 ISP からの注意喚起メール文面は，この法的解釈に則り，注意喚起依頼を仲介する内容となっている．以上をもって，協力 ISP や CCC によるボット感染ユーザの通信の秘密の侵害に対する見解としている．

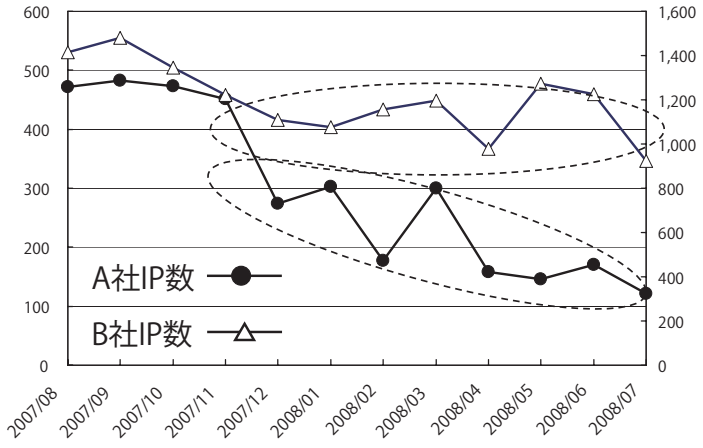

図 -7　協力 ISP2 社の注意喚起社数の月別推移

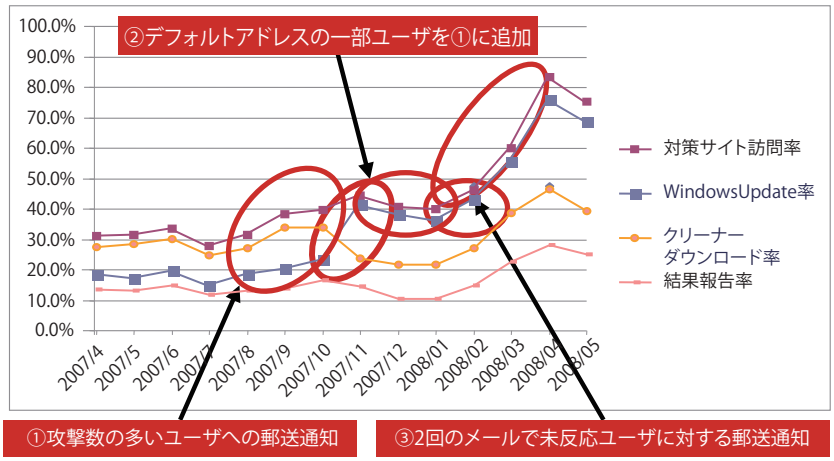

図 -8　郵送によるユーザ応答の向上

ト」と称している．

ボット駆除の効果

本ワークフローを運用することで，「果たしてボット感染 PC が減るのか？」

ワークフローによるボット駆除の効果を考察する．図 -7 は，協力 ISP2 社の注意喚起対象者数の推移を IP アドレス数で月別集計したグラフである．A 社は注意喚起を開始してから（2007 年 11 月）から減少傾向にある．B 社については，諸般事情でこの時期には注意喚起ワークフローに参加できていなかった．この B 社については，対象者は減少していない．この傾向の違いは，注意喚起ワークフローへの参加がボット感染の減少を会社単位でもたらすことを示唆している．

CCC プロジェクトの開始前に感染実態調査を行い，我が国のボットの感染率推計を実施した．ワークフロー運用後に改めて感染率を推計した．2005 年 6 月のブロードバンドユーザ 2,000 万人に対して 40 ～ 50 万人（2 ～ 2.5%），2008 年 6 月では 3,000 万人に対して 30 万人（1%）であった．CCC プロジェクト以外にも日本全体を対象としたセキュリティ対策があるので，すべてを CCC による効果とは評価できないが，ボット感染拡大の抑制に成功していると評価している．

注意喚起対象者応答率向上の工夫

ボット感染ユーザの協力なしにはボット駆除能力の向上は望めない．トラッキング ID を使い測定したサイト訪問率は約 40%，CCC クリーナーダウンロード率（図 -6）は約 30% であった．40% は低い数字ではないが，電子メールに対して無反応な 60% を動かす工夫が求められた．図 -8 に電子メールと郵送とを併用した ISP の工夫事例を紹介する．

郵送は電子メールより高コストなので，送付先の絞り込み要求が厳しい．本事例では，①攻撃数が多いユーザ，②攻撃数が多く，かつ，ISP が最初に付与したデフォルトのメールアドレスを使用していると思われるユーザ（メールアドレスがデフォルトのままのユーザは実際には電子メールを利用していないと思われる），③ 2 回の電子メールに未反応のユーザの順で郵送した．

3 段階の郵送実施により対策サイトへの訪問率は約 80% にまで向上した．

さらに，封筒開封率向上を狙い CCC のロゴシールを封筒に貼ったところ対策サイト訪問率が 15 ポイント低下してしまった．シールにより広告郵便と間違えられ，

開封されなかったのであろうか？　ボットとの闘いがあたかも未反応ユーザとの闘いになってしまった事例であった．

今後の課題

2009年12月現在「サイバークリーンセンター(CCC)」の活動は，注意喚起への協力ISPが73社に広がり，プロジェクト協同パートナーである(独)情報処理推進機構が行うCCCハニーポット検体の提供先アンチウイルスベンダが7社となり成果の利活用も進んでいる．世界でも先進的なこの取り組みにより，CCCのハニーポットが収集する我が国のネットワーク感染型ボットについては駆除が確実に進んでいる．しかし，当該ボットを日本から100%駆除することまではできていない．また，ボットの技術的発展はめざましく，感染手法の多様化が進んでおり，CCCのハニーポットでは収集できない，Webからの感染手法に基づくマルウェアが新たに拡大している．これらの総合対策の実現も喫緊の課題といえよう．

ボットとの戦いはまだまだ終わらない．

謝辞　日頃よりハニーポットと注意喚起ワークフローを運用するボット対策システム運用グループの皆様には，執筆にあたり興味ある多様な情報を多数提供いただいた．CCC運営委員会，プロジェクト協力ISP，アンチウイルスベンダの各位には取り組みに対して日頃よりご理解いただいた．ここに感謝いたします．

参考文献

1) 高橋，村上，須藤，平原，佐々木：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，Vol.47, No.8, pp.2512-2523 (Aug. 2006).

(平成22年1月20日受付)

有村浩一
pcd-director@telecom-isac.jp
平成14年NTTコミュニケーションズ，セキュリティマネジメント室にて全社情報セキュリティマネジメントシステム構築に従事．同時に，Telecom-ISAC Japanの設立と運営にかかわる．平成17年よりTelecom-ISAC Japan企画調整部部長となり現在に至る．