インターネットサービス事業者における サイバーセキュリティ対策の取組み

株式会社KDDI総合研究所　スマートセキュリティグループ グループリーダー　三宅（みやけ）　優（ゆたか）

1. はじめに

インターネットにおけるサイバー攻撃が増加するとともに巧妙化が進んでおり、攻撃の影響も深刻化している。そのため、サイバーセキュリティ対策は各国において重要な課題となっており、ITU-TにおいてもStudy Group 17（SG17、Security）において、サイバーセキュリティが重要なトピックの一つとなっている。日本においても、様々なサイバーセキュリティに対する取組みが行われているが、本稿では、インターネットに接続されたマルウェア感染端末を減らすことを目的としたインターネットサービス事業者（ISP）におけるセキュリティ対策の取組みについて説明を行う。

2. マルウェア感染端末の影響と対策

インターネットでは常に多種多様なサイバー攻撃が行われているが、その攻撃にはボットネットに感染した端末が使われることが多い。メールに添付したアプリ・文書やWebページの閲覧等によりインターネット利用者にマルウェアをダウンロードさせ、それを端末上で動作させることで、指令サーバからの命令に従って各種攻撃（DoS/DDoS攻撃、迷惑メールの送付、端末内の情報の収集、他の端末への不正アクセスやマルウェアの感染活動等）を行う。マルウェア感染端末による攻撃は、ISPが運用するネットワーク設備、インターネット上のサービス提供事業者の設備及びインターネット利用者の端末に対して攻撃を行うため、インターネットの安定運用とインターネット利用者の保護のためにはマルウェア感染端末を減らしていくことが重要である。近年は、セキュリティ対策が一般のPC、スマートフォン等に比べて弱いIoT端末がネットワークに数多く接続されており、これらの端末へのマルウェア感染が問題となってきている。また、マルウェアにおいては対策ソフトでの検知を回避する亜種が作られており、セキュリティ対策を行っている端末でも感染する可能性があることが指摘されている。そのため、ISPは総務省等の関係機関と連携しながらマルウェア感染端末を減らすための対策を行ってきている。

3. 通信の秘密とサイバーセキュリティ対策

日本においては憲法において通信の秘密が保証されており、電気通信事業者の取扱中に係る通信の秘密については、電気通信事業法、有線電気通信法、電波法により罰則をもって保護されている。そのため、ISPは加入者の通信を監視して特定の条件に合致するものを検出したり、それを自動的に処理（フィルタリング）することはできない。しかし、通信当事者の同意がある場合は通信の秘密に該当しないとされている。また、違法性阻却事由がある場合にも通信の秘密を侵すことが許容されている。これには、人命保護や児童の権利保護、通信事業を行う上で必要な行為（課金、運用に必要な対応等）、が含まれている。そこで、日本インターネットプロバイダー協会、電気通信事業者協会、テレコムサービス協会、日本ケーブルテレビ連盟、日本データ通信協会テレコム・アイザック推進会議（当時）は「インターネットの安定的な運用に関する協議会」を設立し、2007年に「電気通信事業者における大量通信等への対処と通信の秘密に関するガイドライン」を策定した。本ガイドラインは適宜更新され、最新版は2018年11月に「電気通信事業者におけるサイバー攻撃等への対処と通信の秘密に関するガイドライン」として発行されている。このガイドラインには、電気通信事業者がDoS攻撃等のサイバー攻撃、マルウェアの感染拡大、迷惑メールの大量送信及び壊れたパケット等（以下、大量通信等）を識別しその通信の遮断などの対処を実施するにあたって、電気通信事業法等の関係法令に留意し適法に実施するための参考情報が記載されている。ISPは、本ガイドラインに従ってサイバーセキュリティ対策を実施している。

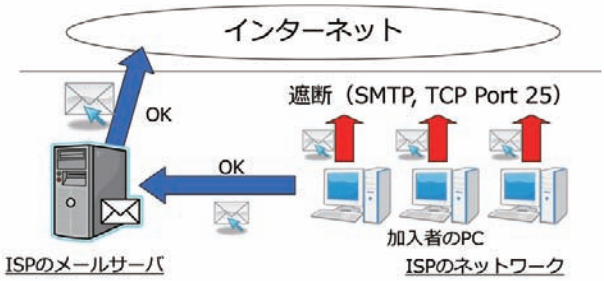
4. 迷惑メール対策

ITU-Tにおいても迷惑メール（スパムメール）への対策が重要課題とされており、特に、途上国から対応を求める意見が多くなっている。これは、迷惑メールが攻撃（マルウェア感染、標的型攻撃）に利用されていることと、迷惑メールがメール全体の50%以上を占めており、通信のリソース（設備、トラフィック容量）に影響を与えているためである。

日本においては、「スパムメール対策推進協議会」を設立して、ISP、各種団体、政府機関、等が連携した取組みを行っている。また、迷惑メールの送信に対して罰則規定

がある法律の制定も行われた。ISPにおいては、各社で迷惑メールフィルタリングの仕組みを導入するとともに、OP25B（Outbound Port 25 Blocking）や送信者認証技術を導入した。

図1にOP25Bの仕組みを示す。インターネットサービスの加入者がISPのメールアカウントを利用してメールを送信する場合には、ISPが指定したメールサーバにメールを送信し、そのメールサーバから受信側のメールサーバへと送られる。現在、迷惑メールのほとんどはマルウェアに感染した端末からボットネットの指令により送付されており、その端末がメールを送る際には直接、送信先のメールサーバへ接続することが多い。そのため、ISPにおけるインターネット加入者の端末からインターネット上のメールサーバへの直接送信をブロックするために、TCPの25番ポートによる通信を遮断している。2009年時点で日本のほとんどのISPがOP25Bを導入している。



■図1. OP25Bにおけるメール送信制御

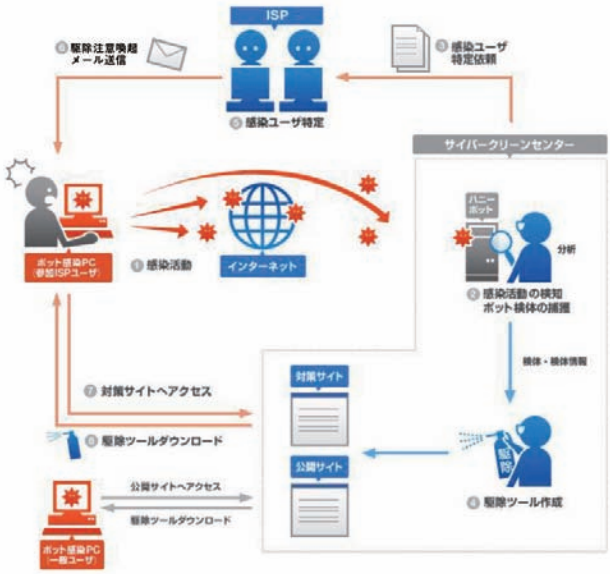
日本における迷惑メール対策の取組み事例は、ITU-T勧告X.1240シリーズの補足文書「Supplement on countering spam and associated threats」において米国での事例とともに紹介されている。

5. マルウェア感染対策

日本においては、ISPが提供するネットワークに接続されているマルウェア感染端末や、感染の可能性がある脆弱な端末に対して影響を抑える取組みを行ってきた。本章では、その取組みについて説明を行う。

5.1. サイバークリーンセンター（CCC：Cyber Clean Center）

2006～2011年の期間において、総務省、経産省及びネットワークセキュリティ団体が連携して取り組んだサイバークリーンセンター（CCC）のプロジェクトでは、ボットに感染した端末の特定、ボットの駆除、再感染の防止の取組みを



■図2. サイバークリーンセンターの活動（CCC紹介ホームページより引用）

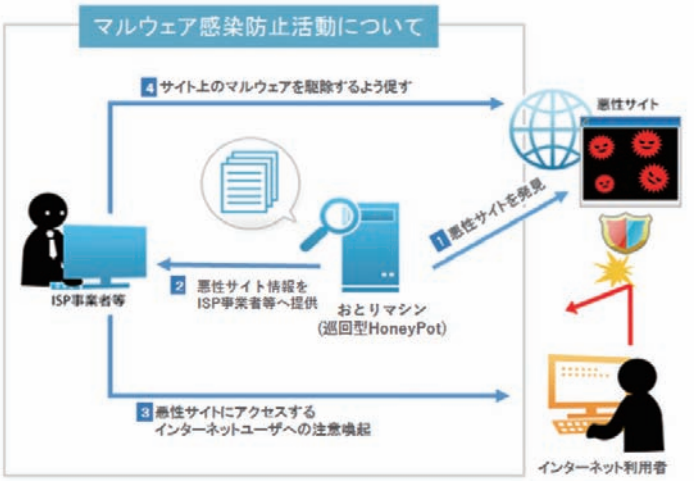
行った。図2に、CCCで行われた活動の概要を示す。

CCCでは、ボットに感染した端末からの攻撃活動をハニーポットと呼ばれる検知装置で補足し、その端末のIPアドレスを特定する。ISPは、IPアドレスから感染ユーザの特定を行い、そのユーザに対して注意喚起を行ってボット駆除方法等の情報を提供する。また、ハニーポットはボットの検体を収集し、新たな検体が見つかった場合は、その検体を駆除できるように駆除ツールを更新する。

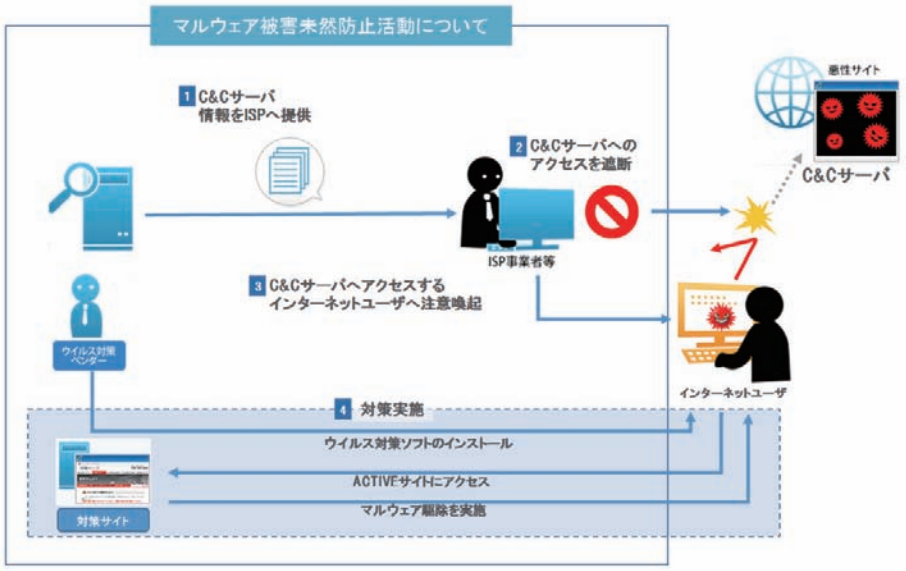
このプロジェクトでは、延べ108,726人の感染ユーザに注意喚起を行い、ボット感染端末の駆除と感染活動の抑制に貢献した。

5.2. ACTIVE（Advanced Cyber Threats response InitiatiVE）

ACTIVEは2013年から開始したプロジェクトで、総務省、日本国内のISP事業者及びセキュリティベンダ等の事業者が国内のインターネット利用者を対象に、マルウェア駆除の注意喚起をする等の実証実験を行う官民連携の取組みである。これまでCCCで行ってきたハニーポットを利用したマルウェア感染ユーザの特定と注意喚起に加え、ハニーポットを利用してマルウェアの感染活動を行う悪性サイトの発見とその悪性サイトにアクセスしようとするインターネット利用者への注意喚起（図3）及びボットネット感染端末の操作を行う指令サーバ（C&Cサーバ）への通信の遮断とその端末ユーザへの注意喚起・マルウェア駆除情報の提供（図4）



■図3. ACTIVEにおける悪性サイトにアクセスするインターネット利用者への注意喚起（ACTIVE紹介ホームページより引用）



■図4. ACTIVEにおけるC&Cサーバへのアクセス遮断とインターネット利用者への注意喚起（ACTIVE紹介ホームページより引用）

を行っている。

ACTIVEにおける悪性サイトへのアクセス発見及びC&Cサーバへの通信の遮断にはDNSを利用している。DNSサーバに悪性サイト、C&Cサーバのリストを組み込み、インターネット利用者がこれらのサイトへのアクセスを行うためにDNSサーバを利用してIPアドレスを検索する際に、リストに掲載されているホスト名と一致しているかを確認し、一致した場合には、アクセスの遮断（注意喚起サイトへの誘導等）を行っている。

5.3. NOTICE（National Operation Towards IoT Clean Environment）

総務省と国立研究開発法人情報通信研究機構（NICT）は、ISP各社と連携し、サイバー攻撃に悪用されるおそれのあるIoT機器の調査及び当該機器の利用者への注意喚起を行う取組み「NOTICE（National Operation Towards IoT Clean Environment）」を2019年2月から開始した。本プロジェクトは、2017年10月に総務省から発行された「IoTセキュリティ総合対策」に基づいて実施された施策の一つである。

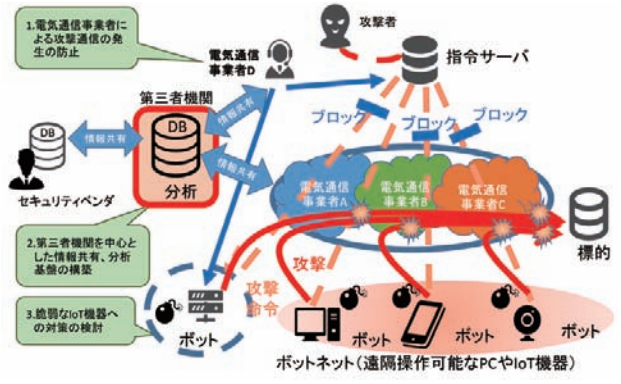
「IoTセキュリティ総合対策」は、セキュリティ対策が不十分なIoT機器の増大したことによりIoT機器への攻撃、侵入行為が増加し、マルウェア感染してボット化したIoT機器による被害が顕著となってきたために、これに対応するための取組みについてとりまとめられたものである。具体的施策として、(1) 脆弱性対策に係る体制の整備、(2) 研究開発の推進、(3) 民間企業等におけるセキュリティ対策の促進、(4) 人材育成の強化、(5) 国際連携の推進、を対象としている。表に、主な取組み項目を示す。

■表. 総務省IoTセキュリティ総合対策における主な取組み項目

具体的施策	主な取組み項目
脆弱性対策に係る体制の整備	• IoT機器に対するセキュリティ認証マークの付与 • セキュリティ検査の仕組み作り • 重要IoT機器の脆弱性調査 • 被害拡大防止のための取組み
研究開発の推進	• 広域ネットワークスキャンの軽量化 • ハードウェア脆弱性への対応 • AIを利用したサイバー攻撃検知・解析
民間企業等におけるセキュリティ対策の促進	• 民間企業のセキュリティ投資の促進 • 事業者間での情報共有を促進するための仕組みの構築 • 情報共有時の匿名化処理に関する検討
人材育成の強化	• 実践的サイバー防御演習（CYDER）の充実 • 2020年東京大会に向けたサイバー演習の実施 • IoTセキュリティ人材の育成
国際連携の推進	• ASEAN各国との連携 • 国際的なISAC間連携 • 国際標準化の推進

これらの取組みの一環として、「IoT化に伴うサイバー攻撃の深刻化」に対応することを目的として、サイバー攻撃の送信元となるマルウェア感染機器などの情報を共有するための制度を整備し、通信事業者による利用者への注意喚起・攻撃通信のブロック等を促進するために、電気通信事業法を2018年に改正した。これに伴い、インターネットサービスを提供する通信事業者間でサイバーセキュリティに関する情報を共有し、その情報を基に攻撃通信発信源のブロックや、脆弱なIoT機器への対策を行うための取組みを開始した。(図5)

情報共有の結節点として適切に情報を取り扱う第三者機関「認定送信型対電気通信設備サイバー攻撃対処協会」を法律上に位置付け、情報の収集、分析、共有等の枠組みを明確化し、NOTICEを開始した。NOTICEにおいては、NICTにおいて機器調査としてインターネット上のIoT機器に対してスキャンを行うことによりパスワード設定に不備のある機器のIPアドレスを特定し、その情報を第三者機関を通じてISPに情報提供する。情報を受け取ったISPは、パスワード設定に不備があるIoT機器の利用者を特定し、設定変更の注意喚起を行う。



■図5. 第三者機関を結節点とした情報共有のイメージ
（出典：総務省資料）

IoT機器を経由したサイバー攻撃が増加している理由として、全て同じID／パスワードを初期値として設定していたIoT機器が売られていたことと、よく使われる簡単なID／パスワードを設定している利用者が多く存在していたことによる。そのため、このような機器に対応を呼びかける活動を開始した。この取組みのために、国立研究開発法人情報通信研究機構法（NICT法）の一部を改正し、NICTの業務にパスワード設定に不備のあるIoT機器の調査等を5年間の時限措置として追加している。

6. おわりに

本稿では、インターネット上におけるサイバー攻撃の活動を軽減する日本のISPの取組みについて説明した。日本においては憲法に定められている通信の秘密に配慮し、各ISPがTelecom-ISAC/ICT-ISAC等の社団法人、政府機関、セキュリティベンダ、OSベンダ等と連携して取り組んできた。IoT時代に移行し、今後は更にセキュリティ的に脆弱な機器がインターネットに接続されていくと考えられている。また、攻撃手法も巧妙化し、検知が難しいサイバー攻撃が増加しつつある中、インターネットの安定運用にはマルウェアに感染した端末の対処を行い、感染活動を抑制するための取組みが必須である。今後も、最新の動向を注視し、時代に即した対応が求められていくと考えられる。

（2019年3月19日　ITU-T研究会より）