別添４

＜基本計画書＞

電波の有効利用のための IoT マルウェア無害化/無機能化技術等に関する研究開発

１．目的

2020 年には、全世界の IoT 機器は 400 億台を超えると予測されているなか、IoT 機器は医療や農業、自動車をはじめとする多くの業界での利用に加え、新たなワイヤレス通信インフラとなる 5G においても、その活用は大きく注目されている。一方でこれらの IoT 機器に感染し、大量の不正な無線通信を行うマルウェアも増加傾向にあり、それに伴う無線リソースのひっ迫が懸念されている。

国立研究開発法人情報通信研究機構（NICT）がサイバー攻撃活動の観測・分析結果として公表している「NICTER 観測レポート 2018」によると、2018 年に観測された攻撃回数は３年前の約４倍に増加しており、そのうちのおよそ半数が IoT 機器を狙った攻撃であった。実際に、2016 年 10 月にはマルウェア Mirai に感染した 10 万台以上の IoT 機器を踏み台にした DDoS 攻撃により、米国 DYN 社の DNS サービスが停止するという事案が発生した。また、2018 年５月には世界 54 カ国で 50 万台を超える IoT 機器が マルウェア VPNFilter に感染していることが確認されている。近年、このような IoT 機器を踏み台とした大規模な攻撃（数百 Gbps から 1Tbps を超えるトラフィック）が度々確認されており、電波の有効利用の観点から対策が急務となっている。

本研究開発では、その原因の根本となる IoT マルウェア及び関連情報の詳細分析技術の開発を行うとともに、遠隔からの IoT マルウェアの無害化及び無機能化が実現できるようにし、上記に示す不正/不要/不健全な無線通信トラフィックの発生を抑止することで、安心・安全な IoT 機器の利活用を促進するとともに、IoT 環境における無線リソースひっ迫の解消を図る。

２．政策的位置付け

・電波有効利用成長戦略懇談会 報告書（平成 30 年８月 31 日　総務省）

第２章 電波利用の将来像と実現方策

５．ワイヤレスがインフラとなる社会の実現に向けた取組

（２） ワイヤレス成長戦略政策パッケージ

（ア） 技術を創る（研究開発プロジェクト、実証・イノベーション等）

⑥　 高い信頼性を備えたワイヤレス環境

・IoT 無線機器の爆発的な普及に伴い、IoT 無線機器の認証データの増大による無線ネットワークへの負担増大や、IoT 無線機器が DDoS 攻撃等の踏み台として悪用されるセキュリティ脅威等が増大している。このため、安全・安心なワイヤレス環境の実現に向けた、サイバーセキュリティに関する研究開発等を推進することが必要である。

・「サイバーセキュリティ戦略」（平成 30 年７月 27 日閣議決定）
４．目的達成のための施策
4.4. 横断的施策
4.4.2. 研究開発の推進
(1) 実践的な研究開発の推進
・我が国が、サイバー攻撃に対する検知・解析能力を含むサイバー空間の状況把握能力を高め、防御等の対処能力や強靱性の確保等サイバー空間における安全保障の確保にも資する研究開発を推進する。具体的には、政府機関や企業等の組織を模擬したネットワークに攻撃者を誘い込み、攻撃活動を把握することや、ネットワーク上の脆弱な IoT 機器の調査のための広域ネットワークスキャンの軽量化を目指した研究開発等を進める。

・「サイバーセキュリティ研究・技術開発取組方針」（令和元年５月 17 日
サイバーセキュリティ戦略本部　研究開発戦略専門調査会）
４．今後の取組強化の方向性
③　攻撃把握・分析・共有基盤の強化
・サイバー攻撃の巧妙化・複雑化・多様化や、IoT 機器の普及に伴う脆弱性拡大等のサイバー攻撃の脅威動向に適切に対処するため、AI 等の先端技術も活用しつつ、サイバー攻撃の観測・把握・分析技術や情報共有基盤を強化する。

３．目標

IoT 機器の急速な普及に伴う近年の多様な通信環境において、セキュリティ上の問題により発生する不正/不要/不健全な無線通信トラフィックに対応するため、（ア）各種サイバー攻撃データやマルウェアの解析に基づく、IoT マルウェアの挙動検知及び駆除技術、（イ）マルウェアに感染した IoT 機器を安全に無害化及び無機能化する技術をそれぞれ確立する。DDoS 攻撃の規模、被害は年々拡大しており、本研究開発が終了する令和４年には、平成 30 年の約 1.6 倍のトラフィックになるとの試算がある。本研究開発により、IoT 機器に感染し大規模な攻撃活動を行うマルウェアのうち６割に対して、駆除や無害化などを実現する。その結果、感染した IoT 機器による不正通信に対して６割程度の通信量削減効果を得ることで、無線リソースのひっ迫を解消し、電波の有効利用を図る。

４．研究開発内容

(1) 概要

近年、IoT 機器を狙ったサイバー攻撃が増加している。マルウェアに感染するなどして攻撃者に IoT 機器を乗っ取られると、当該機器を踏み台としたサイバー攻撃に悪用され、不正な無線通信を大量に発生させるおそれがある。具体的な事例では、平成 29 年に国内通信キャリアが提供するモバイルルータが大量にマルウェアに感染し、1 日に最大で約 14,000IP アドレスからの攻撃が観測された。Mirai 等に代表

される IoT マルウェアは、感染時に 100Mbps を超える攻撃通信を発生させる能力があるとされており、大規模な感染が発生すると大量の不正通信によって無線リソースが消費される可能性がある。

このような IoT 機器を悪用した攻撃に起因する不正な無線通信を抑止するためには、IoT 機器の利用特性を考慮した上で、感染したマルウェアの駆除または無害化や、当該機器の使用停止などを行えるようにすることが重要である。従来、このような場合には端末にマルウェア対策ソフトをインストールすることが一般的であったが、IoT 機器においてはリソースの制約等により困難な場合が多く、マルウェア対策ソフトによらず、IoT マルウェアを駆除及び無害化/無機能化する新たな技術の確立を目指す。

本研究開発では、Web カメラ、ネットワークプリンタ、ルータ等の IoT 機器の通信に利用される LPWA、WPAN、無線 LAN、セルラー（LTE、4G、5G）、広帯域移動無線アクセスシステム（BWA）等の無線ネットワークにおいて、マルウェア感染による不正/不要/不健全な無線通信を抑止するため、様々な手法により収集したサイバー攻撃関連データ分析やマルウェア挙動解析に基づく IoT マルウェアの挙動検知及び駆除技術、マルウェアに感染した IoT 機器を安全に無害化及び無機能化する技術を開発する。これにより、従来時間を要していたサイバー攻撃やマルウェア挙動解析に要する時間、IoT 機器に感染しているマルウェアが存続する期間が大きく短縮され、その結果、不正/不要/不健全に利用される無線リソースを大幅に軽減することができる。

(2) 技術課題および到達目標

技術課題

ア　IoT マルウェアの挙動検知及び駆除技術

ア①　高度 IoT ハニーポットによるマルウェア詳細分析及び駆除技術

IoT 機器を狙ったサイバー攻撃は多様化しており、従来から悪用されている Telnet を介した侵入だけでなく、IoT 機器が有する様々な脆弱性を突いた攻撃が増加している。また、これまで IoT 機器に感染したマルウェアの多くは、機器の再起動により自動的に削除されたり、活動を停止したりすることが知られていたが、2018 年に持続感染性を有する（再起動後も活動を継続する）マルウェア VPNFilter が報告され、その後も多くの持続感染性を有する IoT マルウェアの事例が見つかっている。

マルウェア挙動解析のためにはハニーポットによるマルウェアの捕獲が重要な技術となる。従来の IoT 向けハニーポットは、Telnet などの特定のサービスの脆弱性を狙う IoT マルウェアを対象としており、事前に想定されたサービス群への攻撃を観測するものであった。そのため、IoT 機器が有する様々な脆弱性を突いた新しい攻撃の観測を行い、最新の IoT マルウェア検体をタイムリーに収集できることが重要である。さらに、収集した IoT マルウェアに対して、持続感染性の有無や持続感染のメカニズムを分析する技術、IoT 機器の所有者

による駆除方法を導出する技術が求められている。このため、以下の研究開発を行う。

・Telnet など特定のポートやサービスに限定せず、攻撃対象となっている機器やサービスの変遷に応じて、様々な攻撃を柔軟に観測可能な高度 IoT 向けハニーポットを開発し、日々新たに発生する IoT マルウェアの収集技術を確立する。
・ハニーポットで収集したマルウェア検体の挙動解析により、持続感染性を有する IoT マルウェアの特徴的な挙動（例：不揮発性メモリ領域への書き込み等）を解析し、持続感染性の有無の判定及び持続感染メカニズムの解析を行う。さらに、これらの分析に基づき、IoT 機器上で IoT マルウェアを駆除する技術を開発し、感染機器の所有者自身で実施できる駆除方法を確立する。

ア②　各種サイバー攻撃情報に基づくマルウェア挙動分析及び早期検知技術

感染したマルウェアの活動が活性化すると、インターネット上の通信やシステムでの挙動などに、様々な形でその活動の痕跡が現れる。そのような情報の収集・調査によるサイバー攻撃の統計的な分析・評価は行われているが、マルウェア挙動分析を含めたサイバー攻撃の状況を正確に把握するには至っておらず、サイバー攻撃の初期挙動の自動的な検知・把握を行うことは重要な課題となっている。

近年、サイバーセキュリティに関連する大量のログデータなどの情報から特徴量を高速かつ効率的に処理・分析するために、機械学習の有用性が報告されている。そこで本研究開発では、機械学習等の技術を用いて、サイバー攻撃の全体像を把握し、サイバー攻撃の初期挙動を自動的に検知するための技術を確立する。具体的には、大量の通信データから収集できるサイバー攻撃関連情報、各種ブラックリスト等の脅威インテリジェンス情報、及び Web 上の様々なセキュリティに関する情報等を収集し、機械学習等の技術を用いてマルウェア挙動分析、攻撃の全体像の把握、及び攻撃の初期挙動を検知するため、以下の研究開発を行う。

・インターネット上で観測される、大量のスキャン等の攻撃通信データから IP アドレス、利用ポート番号、通信タイミング等の情報を抽出・整理し、機械学習等により分析することで、新たなマルウェアの発生や攻撃パターンを早期に検知する技術を開発する。
・マルウェアが C&C サーバ等の攻撃インフラに接続する通信の観測・分析を実施することにより、攻撃者の悪意ある挙動やその時間的な変化、マルウェア活性化のタイミング、攻撃インフラの変化（C&C サーバの変更等）など、サイバー攻撃活動の実態を把握し、IoT マルウェアによる大規模な攻撃の予測やテイクダウン等の対策に資する技術を開発する。

・セキュリティ監視機器等から出力される警告情報や各種ログ情報等について、機械学習等により異常性を分析・検知することで、悪性の通信やマルウェアの活動を効率的かつ早期に検知する技術を開発する。
・各種ブラックリスト等の脅威インテリジェンス情報や脆弱性情報、また Web 上のセキュリティに関する情報等を収集し、相互の関係性を分析することにより、マルウェアの活動や攻撃キャンペーン、そして攻撃者関連情報等を導出し、サイバー攻撃の早期検知に資する技術を開発する。
・上記の各種情報や課題ア①における IoT マルウェア解析情報（マルウェア感染情報、挙動情報等）等の異なる情報源について、様々な方法で多面的に機械学習等を用いて相関解析することにより、サイバー攻撃の全体像を把握するとともに、新たなサイバー攻撃の初期挙動を検知するための総合的な分析環境を構築する。

イ　遠隔からの IoT マルウェア無害化及び無機能化技術

マルウェアに感染した IoT 機器に対しては、ファイアウォール等で C&C サーバへの通信を遮断することにより無害化する対策が知られている。しかし、C&C サーバへの通信を完全に遮断することは難しいだけではなく、感染した IoT 機器内のマルウェアは活動し続ける可能性が高いため、IoT 機器本来の機能・性能に悪影響を与えてしまう。IoT 機器にマルウェア対策ソフトをインストールすることもリソースの制約等により困難な場合が多く、実用的な無害化の対策技術とはなっていないのが現状である。

さらに、本来は撤去・廃棄されるべき IoT 機器が、管理主体が曖昧なまま放置され続けることより、不要な無線通信やマルウェア感染による不正な無線通信を行い続けることについても問題となっていることから、IoT 機器への対策ソフト等のインストールを行わずに、マルウェアに感染した IoT 機器や不要となった IoT 機器による不正な無線通信を停止することを目的として、以下の研究開発を行う。

・課題アにおいて得られる結果を活用し、C&C サーバとマルウェアとの通信等の分析を行い、IoT マルウェアに対して自己停止を誘発させる等により無害化/無機能化するための情報（以下「無害化/無機能化情報」という）を抽出する。攻撃者の C&C サーバを模擬した疑似 C&C サーバを構築し、抽出した情報をマルウェアに対して送信することで、IoT 機器内でのマルウェアの活動を停止させる技術を開発する。
・マルウェアの亜種が大量に生成される中、最新の IoT マルウェアに対応するため、継続的にかつ迅速にマルウェア解析を行う必要がある。このため、無害化/無機能化情報の抽出を自動化し、常時更新することによって未知の脅威に迅速に対応する技術を開発する。
・不要となった IoT 機器を、外部モジュール等を用いて遠隔から安全に機能停

止させるための技術を開発する。停止対象の IoT 機器のみを安全に停止させるための、認証信号の生成手法、管理手法を確立する。

到達目標

ア　IoT マルウェアの挙動検知及び駆除技術

ア①　高度 IoT ハニーポットによるマルウェア詳細分析及び駆除技術

高度 IoT ハニーポットによる攻撃観測に基づき、大規模攻撃の対象となっている IoT 機器群と当該機器を狙う IoT マルウェア検体群を特定する。さらにこれらの IoT マルウェア検体群と IoT 機器群の組み合わせに対して 90%以上の精度で持続感染性の有無を判定する技術を確立する。また、評価対象の IoT マルウェア検体群と IoT 機器群に対し、70%以上の成功率で駆除する技術を確立する。これにより、約６割の IoT 感染マルウェアを駆除し、大規模感染インシデント時に発生する DoS トラフィックを約６割削減できるため、無線リソースのひっ迫を解消することが可能となる。

ア②　各種サイバー攻撃情報に基づくマルウェア挙動分析及び早期検知技術

各種サイバー攻撃情報に基づく複数の分析結果及び課題ア①の分析結果を、機械学習等の技術を用いて多面的に統合・相関解析を行うことにより、攻撃の全体像を把握するとともに、攻撃の初期挙動を早期に自動検知する技術を開発し、重要なセキュリティイベントの発生検知に要する分析時間を、従来の人手で行っていた時間の 3/10 以下に短縮する。分析時間の短縮によりインシデント対応を早期に開始することで、大規模感染インシデントが発生した場合の無線リソースへの影響を軽減・抑止することができる。

イ　遠隔からの IoT マルウェア無害化及び無機能化技術

評価検証対象の IoT マルウェア検体群に対して 70%以上の精度で無害化/無機能化情報の有無及びその抽出可否を判定した上で、抽出可能な情報を自動抽出する技術を確立する。また、無害化/無機能化情報を抽出できた IoT マルウェアに対しては、90%以上の精度で実際に無害化/無機能化を行う。これにより、約６割の IoT 感染マルウェアを無害化し、大規模感染インシデント時に発生する DoS トラフィックを約６割削減できるため、無線リソースのひっ迫を解消することが可能となる。さらに、不要となった遠隔信号受信可能な IoT 機器に対して、99%以上の精度で安全に遠隔から機能停止を行うことを目標とする。

なお、上記の目標を達成するに当たっての年度毎の目標については、以下の例を想定している。

＜令和２年度＞

ア　IoT マルウェアの挙動検知及び駆除技術

ア①　高度 IoT ハニーポットによるマルウェア詳細分析及び駆除技術

高度 IoT ハニーポットのプロトタイプを開発し、試験的に IoT マルウェア検体収集を開始する。また、マルウェア詳細分析手法及び駆除手法の検証のためのプロトタイプを開発し、試験用の IoT マルウェア検体群について持続感染性分析や駆除方法の導出が可能であることを実証する。

ア②　各種サイバー攻撃情報に基づくマルウェア挙動分析及び早期検知技術

インターネット上の攻撃通信データの分析や脅威インテリジェンス情報等から得られる複数の情報群を様々な方法で多面的に統合・相関解析を行う分析プラットフォームを設計し、そのプロトタイプを構築する。

イ　遠隔からの IoT マルウェア無害化及び無機能化技術

IoT マルウェアの無害化/無機能化情報を抽出するための解析環境のプロトタイプを構築し、基本方式を設計する。さらに、疑似 C&C サーバを試作し IoT マルウェアに無害化/無機能化情報を送る機能を検証する。また、IoT 機器を遠隔で確実に機能停止させるための遠隔安全停止システムの基本設計及びプロトタイプを構築する。

＜令和３年度＞

ア　IoT マルウェアの挙動検知及び駆除技術

ア①　高度 IoT ハニーポットによるマルウェア詳細分析及び駆除技術

高度 IoT ハニーポットの実装により、最新の IoT マルウェア検体収集を行う。また、マルウェア詳細分析手法及び駆除手法の実装により、IoT マルウェアの持続感染性分析や駆除方法の導出を行う。

ア②　各種サイバー攻撃情報に基づくマルウェア挙動分析及び早期検知技術

分析プラットフォームのプロトタイプを用いて、各種挙動分析・検知技術の機能評価、性能評価、運用性評価等を実施し、必要な改善を行う。また、課題ア①の成果をベースに、統合・相関解析機能を拡充し、より精度の高いサイバー攻撃の全体像把握や初期攻撃挙動の検知を行う。

イ　遠隔からの IoT マルウェア無害化及び無機能化技術

課題ア①と連携し、その成果を活用することにより、IoT マルウェアの無害化/無機能化情報を抽出するシステムを実装する。さらに、多種多様な IoT マルウェアから抽出した無害化/無機能化情報等を IoT マルウェアに送る疑似 C&C サーバを構築する。また、安全機能停止のコア機能と IoT 機器を連動させ、遠隔安全停止システムを実装し、遠隔からの安全な機能停止を行うためのシステム全体を通した機能検証を行う。

＜令和４年度＞

ア　IoT マルウェアの挙動検知及び駆除技術

ア①　高度 IoT ハニーポットによるマルウェア詳細分析及び駆除技術

高度 IoT ハニーポットを実環境上で広域に展開し、最新の IoT マルウェア検体収集を充実化する。また、令和３年度に実装したマルウェア詳細分析手法及び駆除手法に対して総合評価を行い、各技術を改善する。

ア②　各種サイバー攻撃情報に基づくマルウェア挙動分析及び早期検知技術

分析プラットフォームの試験運用を開始し、サイバー攻撃早期検知情報をリアルタイムな警戒情報として掲示できるようにする。また、本試験運用を通じて分析プラットフォームの総合評価を行い、性能及び機能の改善を実施する。

イ　遠隔からの IoT マルウェア無害化及び無機能化技術

令和３年度に実装したシステムを改良し、IoT マルウェアの無害化/無機能化情報の抽出を自動化するとともに、疑似 C&C サーバと連動したシステムを構築する。本システムの総合的な評価を実施し、システムの改善を行う。また、令和３年度に実装した遠隔安全停止システムの総合評価を行い、機能および性能の最適化を実施する。

本研究開発により、IoT 機器に感染し大規模な攻撃活動を行うマルウェアのうち６割に対して、駆除や無害化などを実現する。本研究開発が終了する令和４年には、平成 30 年の約 1.6 倍のトラフィックになるとの試算があることから、感染した IoT 機器による不正通信に対して６割程度の通信量削減効果を得ることで、無線リソースのひっ迫を解消し、電波の有効利用を図る。

５．実施期間

令和２年度から４年度までの３年間

６．その他

（１）成果の普及展開に向けた取組等

①国際標準化等への取組

国際競争力の強化を実現するためには、本研究開発の成果を研究期間中及び終了後、速やかに関連する国際標準化規格・機関・団体へ提案を実施することが重要である。このため、研究開発の進捗に合わせて、国際標準への提案活動を行うものとする。なお、提案を想定する国際標準規格・機関・団体及び具体的な標準化活動の計画を策定した上で、提案書に記載すること。

②実用化への取組

研究開発期間終了後も引き続き取り組む予定の「本研究開発で確立した技術

の普及啓発活動」及び令和９年度までの実用化・製品展開等を実現するために必要な取組を図ることとし、その活動計画・実施方策については、提案書に必ず具体的に記載すること。特に、関連機関へのサイバー攻撃早期検知情報の提供等を継続して行う方策を記載すること。

（２）提案および研究開発に当たっての留意点

提案に当たっては、基本計画書に記されている目標に対する達成度を評価することが可能な具体的な評価項目を設定し、各評価項目に対して可能な限り数値目標を定めること。また、従来の技術との差異を明確にした上で、技術課題及び目標達成に向けた研究方法、実施計画及び年度目標について具体的かつ実効性のある提案を行うこと。

研究開発の実施に当たっては、関連する要素技術間の調整、成果の取りまとめ方等、研究開発全体の方針について幅広い観点から助言を頂くと共に、実際の研究開発の進め方について適宜指導を頂くため、学識経験者、有識者等を含んだ研究開発運営委員会等を開催する等、外部の学識経験者、有識者等を参画させること。

なお、本研究開発において実用的な成果を導出するための共同研究体制又は研究協力体制について、研究計画書の中にできるだけ具体的に記載すること。特に、先進的なサイバーセキュリティ研究に取り組んでいる大学、国立研究開発法人、セキュリティベンダー等による密な連携を前提とし、無線通信分野の研究者も交えて議論を行える体制を構築すること。加えて、技術開発だけにとどまらず、サイバーセキュリティに関する人材育成、普及にも留意すること。また、本研究開発成果がマルウェアによる無線通信トラフィックの抑制に効果があることを具体的に示すこと。