令和５年度事後事業評価書

政策所管部局課室名：サイバーセキュリティ統括官室

評価年月：令和５年８月

１　政策（研究開発名称）

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

２　研究開発の概要等

（１）研究開発の概要

・実施期間

令和２年度～令和４年度（３か年）

・実施主体

国立大学法人横浜国立大学
国立研究開発法人情報通信研究機構
国立大学法人九州大学
国立大学法人神戸大学
学校法人早稲田大学
株式会社セキュアブレイン
ジャパンデータコム株式会社

・総事業費

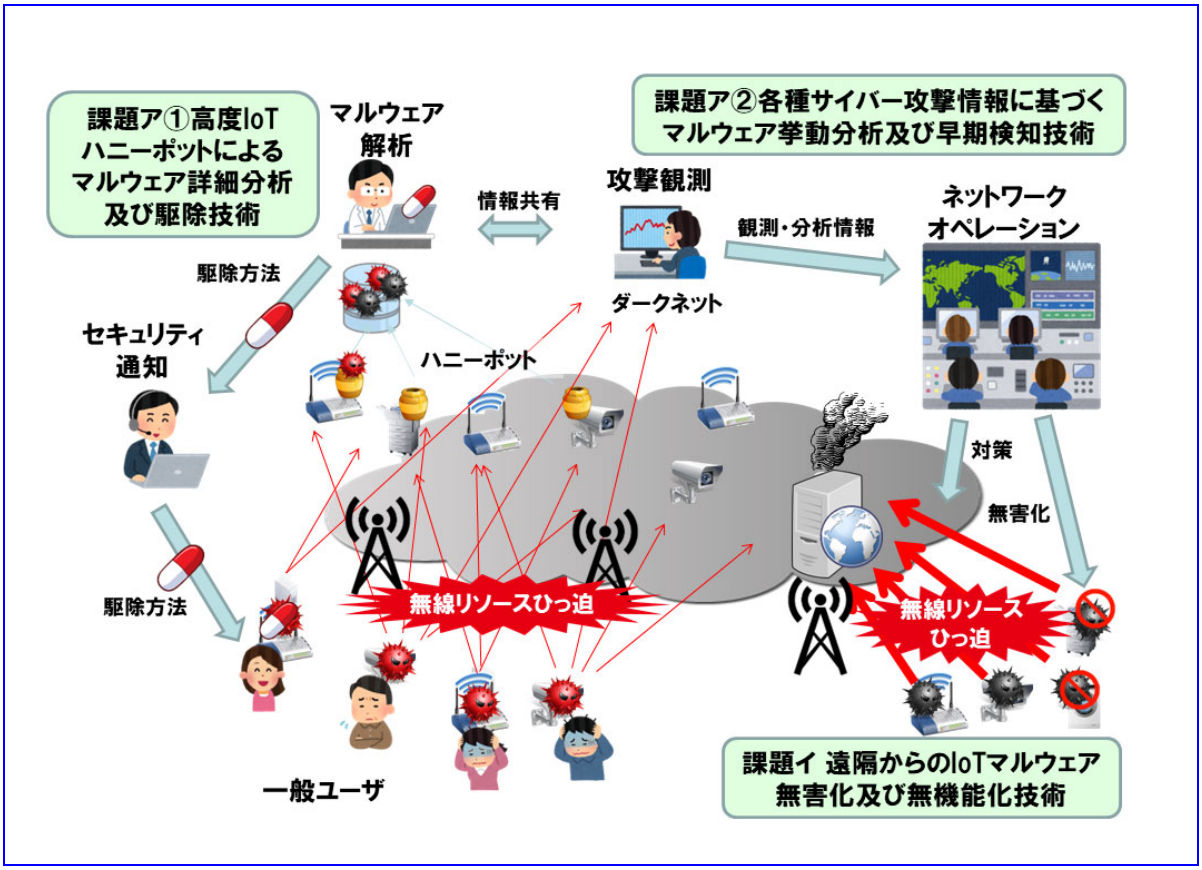
1,062 百万円

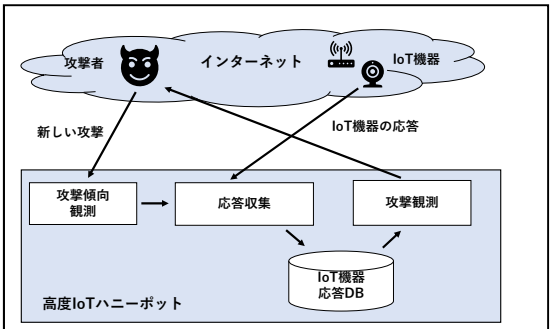
令和２年度	令和３年度	令和４年度	総　額
379 百万円	354 百万円	329 百万円	1,062 百万円

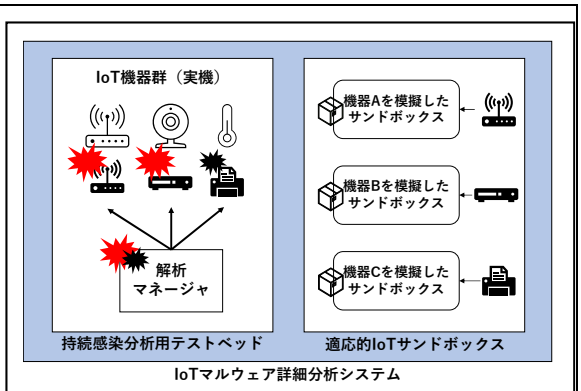
予算要求段階では総額 10 億円超となるか未定だったため、事前事業評価は未実施。

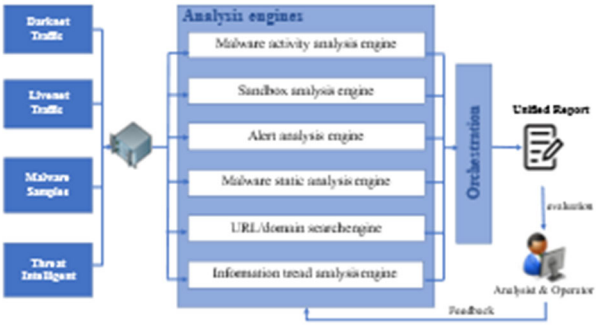
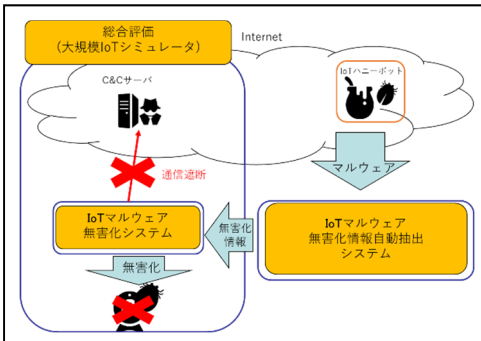
・概　要

多様化・高度化する IoT 機器への攻撃の中で、特に多発している IoT マルウェアによる分散型サービス妨害攻撃(DDoS 攻撃)では、攻撃による不正・不要・不健全な無線通信の急激な発生に伴う無線リソースのひっ迫が懸念されている。そこで、本研究では、IoT マルウェアの収集・分析に必要なシステム及び IoT マルウェアの収集、分析、駆除技術を開発する。また、攻撃行動の全体像を把握するために多角的な研究を行い、各成果を連携した統合分析プラットフォームを構築し、さらに、IoT 機器における IoT マルウェアの活動を阻止する無害化技術や、IoT 機器を遠隔制御（システム停止を含む）する IoT システム無機能化（機能停止）技術を開発し、攻撃による無線リソースのひっ迫の解消に資する。

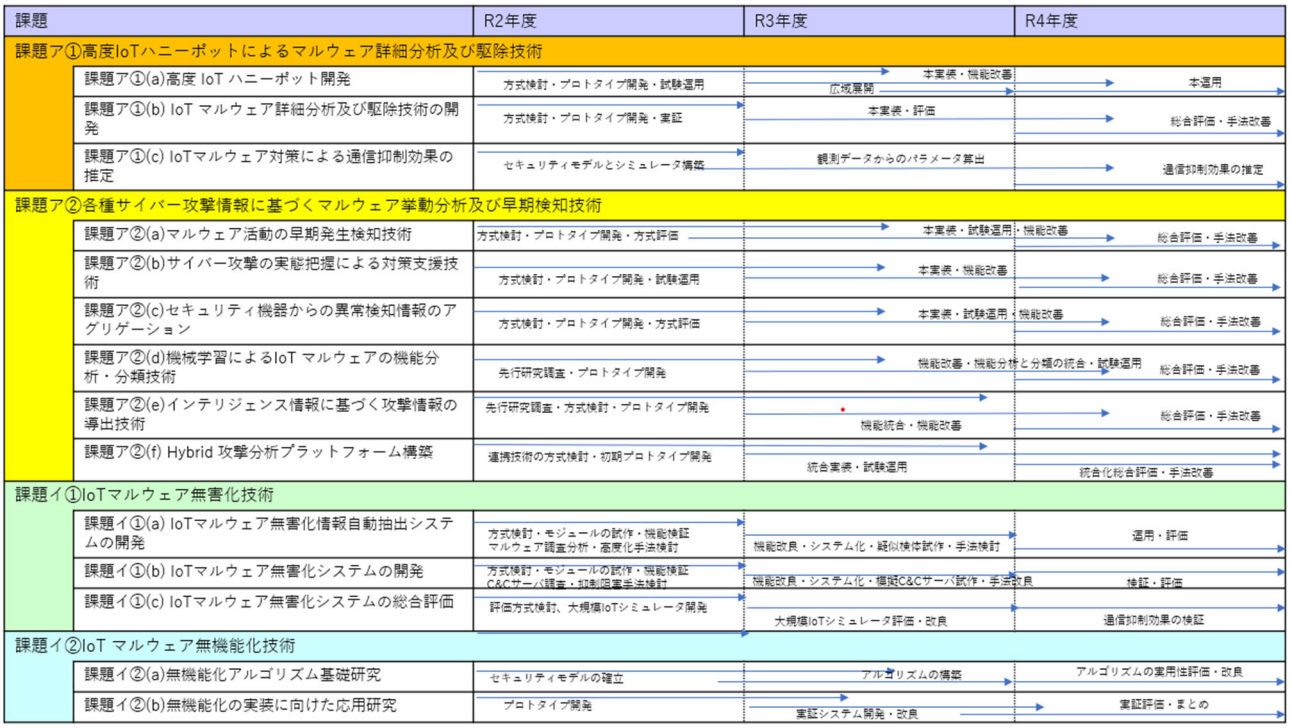


技術の種類	技術の概要
ア①高度 IoT ハニーポットによるマルウェア詳細分析及び駆除技術	ア①(a)：高度 IoT ハニーポット 高度 IoT ハニーポットのアーキテクチャは、攻撃傾向観測機能、応答収集機能、攻撃観測機能の３つの機能から構成される（図１）。攻撃傾向観測機能は、アクセスされた HTTP パスを監視することで、新たな攻撃対象を特定する。具体的には、新たに閾値以上の IP アドレス（攻撃者と想定）からアクセスされた HTTP パスを新たな攻撃対象とみなす。新たな攻撃対象が特定されると、応答収集機能は、その HTTP パスを持つ IoT 機器をインターネットから見つけ出す。そして、特定したデバイスからその HTTP パスに関連する応答（HTTP ヘッダーとボディ）を取得し、データベースに記録する。最後に、攻撃者がハニーポットにアクセスすると、攻撃観測機能は、HTTP パスに基づき、IoT 機器の応答を攻撃者に返す技術。  図１：高度 IoT ハニーポットのアーキテクチャ ア①(b)：IoT マルウェア詳細分析及び駆除技術

	適応的 IoT サンドボックスにて高度 IoT ハニーポットや VirusTotal 等で収集された IoT マルウェア検体の分析を行い、持続感染性の有無を判定する。その上で、持続感染分析用テストベッドに実機を配置し、IoT マルウェアの駆除手法を検討、試行し、駆除方法を確立させる技術（図２）。 ア①(c)：IoT マルウェア対策による通信抑制推定技術 ISP（インターネットサービスプロバイダー）毎の注意喚起シミュレータ、ワイブル分布に基づく数理モデルを用いたマルウェア生存率及び削減率の線形予測シミュレータの実装と、攻撃データの実測値を用いた検証による、通知周期や注意喚起の割合を ISP 規模毎に可変とした、通常時及びパンデミック時の高精度マルウェア削減率及び不正通信削減率の予測技術。  図２：IoT マルウェア詳細分析システム
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	ア②(a)：マルウェア活動の早期発生検知技術 マルウェアが活動の初期段階でスキャン活動を行うことに着目し、新たなマルウェア活動の兆候を可能な限り早期に検知する技術。 ア②(b)：サイバー攻撃の実態把握による対策支援技術 IoT マルウェア検体やその通信の挙動をより長期的に動作させる攻撃実態を観測する技術、マルウェアの通信の中から C&C 通信(マルウェア制御通信)を判別する技術。 ア②(c)-1：セキュリティアラートの重要度診断・スクリーニング技術 セキュリティ情報イベント管理機器(SIEM)が検出・発行する様々な種類の多数の異常アラートから、対応が必要な重要なアラートを機械学習を用いて自動的に抽出する技術。 ア②(c)-2：仮想統合セキュリティアプライアンスの構築 既存のネットワーク侵入検知システム（NIDS）はそれぞれ偏った特性があるため、通常は一つの組織で複数の NIDS を運用することが多い。こうした NIDS の使用形態の簡略化を目的とした、複数の既存 NIDS の特長を併せ持つ単一の NIDS を機械学習によって構築する技術。 ア②(d)：機械学習による IoT マルウェアの機能分析・分類技術 増加し続ける IoT マルウェアの状況に対応するため、多量のマルウェア検体群を生物学で用いられる進化系統樹を利用したクラスタリング（分類技術）と、亜種がもつ特徴的な機能を抽出するために、関数列呼び出しグラフ（FCSG）という知識表現法を用いて機能分析する技術。 ア②(e)-1：脅威情報・脆弱性情報からのインテリジェンス情報の抽出技術 脆弱性情報の識別子(CVE-ID)から MITRE ATT&CK のデータを引き出すなど、ある脆弱性情報からそれに関係する攻撃手法や攻撃者集団等の情報を自動的に導出する技術。 ア②(e)-2：時系列マッピングに基づく攻撃分析技術 ランキングに基づく検索に加えて、個々の情報を適切な空間に配置して可視化することにより、文書間の関係の経時的な変化を追跡する方法論を構築する技術。 ア②(f)：Hybrid 攻撃分析プラットフォームの構築

	近年のマルウェア挙動の多様化・高度化を踏まえ、IoT マルウェアの解析に特化し、ダークネット/ライブネット、ハニーポット、インテリジェンス情報など複数のデータソースからビッグデータとしてデータを収集・蓄積し、前出の各種の解析エンジン（ア②(a)-(e)）を用いて並列に解析し、解析結果を連携・統合する。統合された分析結果は、Web ページ上で段階的詳細化がなされる形で一覧表示される技術（図３）。  図３：ハイブリッド攻撃分析プラットフォーム
イ①:IoT マルウェア無害化技術（無害化：マルウェアの機能のみを停止させること）	イ①(a)：IoT マルウェア無害化情報自動抽出システムの開発 IoT マルウェアには無害化に用いる情報（無害化情報）が当該 IoT マルウェアに搭載されているものが多数存在している。この情報を利用し、実際の C&C サーバ(マルウェア制御用サーバ)に代わって無害化情報を配信することで、IoT マルウェアを無害化することを目指し、これら多数の IoT マルウェアから無害化情報を自動的に抽出する技術（図４の右側）。  図４：IoT マルウェア無害化技術の全体像 イ①(b)：IoT マルウェア無害化システムの開発 検知、ルーティング、無害化情報配信の３つのモジュールで構成される IoT マルウェア無害化システムにて、イ①(a)で取得した無害化情報を配信することで IoT マルウェアを無害化する技術（図４の左下）。 イ①(c)：IoT マルウェア無害化システムの総合評価技術 既存のネットワークシミュレータである ns-3 をベースに、IoT 機器や IoT マルウェアの通信挙動をシミュレートする大規模ネットワークを疑似的に構築し、IoT マルウェア固有の動作をプラグインとして追加することで多種多様なマルウェアをシミュレーションし、IoT マルウェア無害化の効果を評価する技術（図４の左上）。
イ②:IoT マルウェア無機能化技術（無機能化：IoT 機器を安全に停止させること）	イ②(a)：無機能化アルゴリズム基礎技術 遠隔からネットワーク内で緊急対応が必要になった IoT 機器（群）や、撤去・廃棄の対象となった IoT 機器（群）の機能を安全に停止させるという IoT システムの無機能化機能を実現する、放送型認証*方式(BA：Broadcast Authentication)を採用した高機能認証技術。 *放送型認証:ブロードキャスト通信路を介して受信者全員に同じ制御用データを送りながらも、任意の受信者集合の一部だけが制御コマンドを受理する機能を実現できる技術。 イ②(b)：無機能化の実装に向けた応用技術 イ②(a)で開発したアルゴリズムを実装した遠隔安全停止システムを構築し、プロトコル評価を含めたシステム構築に関する実証評価を通して 99%以上の実装・実現精度で安全に遠隔から機能停止する技術。

・スケジュール



（2）達成目標

本研究開発では、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、①サイバー攻撃データやマルウェア解析に基づく、IoT マルウェアの挙動検知及び駆除技術、②マルウェアに感染した IoT 機器を安全に無害化・無機能化技術をそれぞれ確立し、無線通信リソースの効率的かつ安定的な利用環境を提供することで、無線リソースのひっ迫を抑止し電波の有効利用を図る。

○関連する主要な政策

Ⅴ．情報通信（ICT 政策）　政策 13「電波利用料財源による電波監視等の実施」

○政府の基本方針（閣議決定等）、上位計画・全体計画等

名称（年月日）	記載内容（抜粋）
サイバーセキュリティ戦略（令和 3 年 9 月 28 日）	4.4.横断的施策 4.4.1 研究開発の推進 （2）実践的な研究開発の推進 ③ 攻撃把握・分析・共有基盤の強化」として ・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。
電波有効利用成長戦略懇談会　報告書（平成 30 年 8 月 31 日）	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）	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靭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）	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。

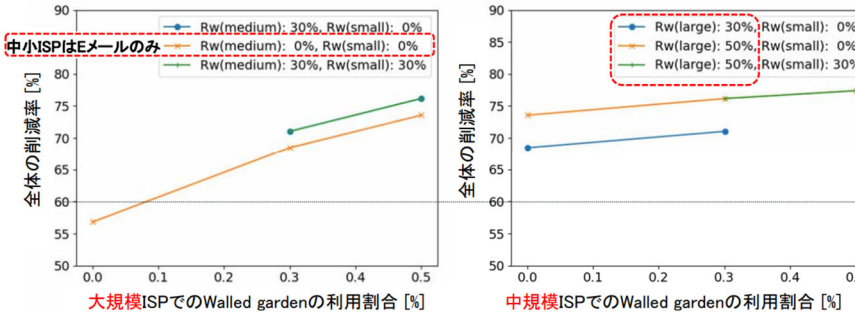
（３）目標の達成状況

本研究開発では、高度 IoT ハニーポットによる攻撃観測に基づき、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し、評価対象に対し 70%以上の成功率で駆除する技術を確立した。この技術を用いて、約６割の感染 IoT 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割削減させる目標に対し、６割以上の通信を削減するために必要な感染ユーザへの通知手段を明らかにし、全体として目標を上回って達成した。

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・相関解析を行う技術を確立させることで、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 以下に短縮する目標に対し、全体として目標を上回って達成した。

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し、無害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を行う目標に対し、全体として目標を上回って達成した。さらに、緊急対応や廃棄対象の IoT 機器に対し、対象機器を遠隔から停止させる無機能化アルゴリズムとして、放送型認証方式を提案・開発し、具体的なユースケースを想定して、当該アルゴリズムの実装・システム化を実施した。具体的な実証実験を通して、100%の精度で安全に遠隔から対象の IoT 機器の無機能化を行うことを達成でき、99%以上の精度の目標に対し、全体として目標を上回って達成した。

技術の種類	目標の達成状況
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	ア①(a)：高度 IoT ハニーポット 高度 IoT ハニーポットの広域展開を行い、少なくとも 10 か国・地域に配置し、プロジェクト終了までに 10 種類以上の機器・脆弱性を狙った攻撃を観測する目標に対し、17 カ国・地域で観測を実施し、101 種類の脆弱性を狙った攻撃を観測し、目標を大幅に超えて達成した。 また、未分類の攻撃や脆弱性の分析、機器の拡張を行い、攻撃挙動の観測・分析手法の高精度化を検討する目標に対し、高度 IoT ハニーポットに 17,672 種類の機器応答を組

	み込み、模倣可能な機器を大幅に拡張した。観測した攻撃を分析するプラットフォームを構築することで、攻撃挙動の観測・分析手法の高精度化を達成した。さらに攻撃コードのライフサイクルの一部を明らかにしたという目標以上の成果を得た。加えて、高度 IoT ハニーポットで収集したマルウェア検体を研究機関へ提供するウェブサイトを開設し、2023 年 3 月 31 日時点で 26 か国 138 の研究組織、企業などにデータを提供した。また、高度 IoT ハニーポットのアクセス情報を、横浜国立大学が運営するマルウェア感染・脆弱性検査サービスに提供し、8 万ユーザ以上の IoT 機器のマルウェア感染診断に活用した。 ア①(b)：IoT マルウェア詳細分析及び駆除技術 (1)持続感染分析用テストベッドに 10 種類以上の実機を配置する目標に対し、12 種類配置することに成功し、目標を達成した。また、高度 IoT ハニーポットや VirusTotal 等で収集された IoT マルウェア検体の分析を行い、(2)90%以上の精度で持続感染性の有無を判定する目標に対し、41 検体に対して 92%の精度で持続感染の有無を判定し、目標を達成した。(3)70%以上の成功率で駆除する技術を確立する目標に対し、100%の駆除に成功し、目標を上回る成果を得た。 ア①(c)：IoT マルウェア対策による通信抑制推定技術 各 ISP からの IoT マルウェア感染ユーザへの通知モデルを用いた注意喚起シミュレータと、IoT マルウェア生存率及び削減率の線形予測シミュレータを実装し、攻撃データの実測値による検証を行い、本手法の有用性を示した。図５は通知手段の違いによる IoT マルウェア削減率のシミュレーション結果を示したもので、中小規模 ISP がメールのみの通知であっても、大規模 ISP の１割が Walled garden 等の通知手段による注意喚起を実施できれば、６割の不正通信の削減が達成可能であることを示した。  図５：通知手段の違いによる削減率
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	ア②(a)：マルウェア活動の早期発生検知技術 マルウェア活動・サイバー脅威をリアルタイムに検知可能なエンジンを構築し、イベント検知率について、90%以上の検知精度を実現する目標に対し、再現率 100%を達成し、また、アラート結果のリアルタイム提供を実現した。 また、主要イベントとは関係のない調査目的のスキャンパケット等を除外するための技術を確立し、誤検知数を令和２年度比で 50%削減する目標に対し、約 90%削減することができ目標を達成するとともに、その要素技術について特許を出願した。さらに、本研究開発の成果論文で使用した NICTER 観測データ（ダークネット・トラフィックデータ）の公開を開始し、2023 年 3 月 31 日時点で、国内外の 5 つの組織に提供した。 ア②(b)：サイバー攻撃の実態把握による対策支援技術 C&C 通信(マルウェア制御通信)の判定手法の検知精度を向上させ、偽陽性率 0.1%、偽陰性率 10%を実現する目標に対し､C&C 通信の判定手法の検知精度として偽陽性率 0.000007%以下、偽陰性率 0.009%以下を実現し、目標を上回る成果を得た。また、C&C 通信の判定手法を長期動的解析システムに適用し運用を開始する目標に対し、120 並列のシステムを構築し目標を達成した。さらなる研究成果として、C&C 通信をエミュレートする Milker を開発し、780 個の C&C サーバの長期観測を実現した。 ア②(c)-1：セキュリティアラートの重要度診断・スクリーニング技術 AI を活用した実用的なアラート選別・可視化システムを構築し、実際の SOC(セキュリティオペレーションセンター)運用環境でインシデント対応時間を 50%削減する目標に対

し、重要度の高いアラートを再現率 99%にて検出する技術を構築し、重要度の低いアラートの 90%除外を実現し、実際のオペレーション環境に流れるデータを利用して有用性を評価した結果、検証すべきアラート数の 50%以上削減を実現し、目標を達成した。

ア②(c)-2：仮想統合セキュリティアプライアンスの構築
アプライアンスが生成するアラートの元となるトラフィックを分析し、アラート元を特定し、特定したアラートの特徴を学習することで、検知精度が高く、誤検知率及び見逃し率が増大しない仮想統合セキュリティアプライアンスを構築する目標に対し、アラートとイベントの関連付け方法を確立し、kitsune 特徴量とペイロード特徴量に基づく仮想統合セキュリティアプライアンスを実装し、T-Pot 観測データを用いて重要アラート(Nirvana-level 7 以上)を正解ラベルとした実環境評価で、F1 スコア※0.39 を獲得し、目標を達成した。(商用アプライアンスの最高値は 0.07 程度)
※F1 スコア:トレードオフ関係にある再現率と適合率のバランスを示す指標で、1 に近いほど性能が良いことを示す。

ア②(d)：機械学習による IoT マルウェアの機能分析・分類技術
マルウェア検体ファイル間の類似度に基づきマルウェアを分類する技術と、逆アセンブルによる機能推定技術を統合したシステムを開発し、精度を維持しつつ、20 万検体のクラスタリングを実現すると同時に、精度を保ったまま計算時間を 50%削減し、未知のマルウェアの機能を効果的に推定する手法を確立する目標に対し、進化系統樹を用いた分類手法と、クラスタ特徴を FCSG (関数呼び出し列グラフ)で表す手法を構築した。進化系統樹作成法を数十万件まで対応可能に拡張して 20 万検体の評価を実施し、オンライン方式により、精度を保ったまま計算時間を 50%以上削減できることを確認した。そして上記分類手法と機能解析を統合し、未知マルウェアの機能推定のための包括的システムにて推定が可能となり目標を達成した。

ア②(e)-1：脅威情報・脆弱性情報からのインテリジェンス情報の抽出技術
脅威情報や脆弱性情報を基に攻撃キャンペーンに関する情報などを導出する。数万件規模の文書データに対して精度を高く有意義な情報を抽出すると同時に、その処理に必要なコストを低減する技術を確立する目標に対し、脅威情報の分類手法と脆弱性情報の分類手法を開発、さらに NVD[1)]や CWE[2)] などの脆弱性情報のオントロジーを MITRE ATT&CK[3)]につながるように拡張し、攻撃の痕跡から脆弱性を持つ製品や攻撃キャンペーンの情報を現実的な時間で導出でき技術確立の目標を達成した。
1)米国国立標準技術研究所 (NIST) が運営する脆弱性データベース
2)米国の非営利団体 MITRE が運営する「共通脆弱性タイプ」
3)米国の非営利団体 MITRE が分類したサイバー攻撃の戦術、技術のフレームワーク

ア②(e)-2：時系列マッピングに基づく攻撃分析技術
インテリジェンス情報が時系列としてどのように変化しているかを追跡する技術を確立し、実際のオペレータがより効率的に業務を実施するための技術基盤を構築することにより、オペレータがインテリジェンス情報の収集・整理に要する時間を 15%以上削減する目標に対し、確率的埋め込み技術、関連度による biplot 表示技術を開発し、実データに対して統計分析を実施し、攻撃分析のための視覚化と分析手法を評価した。その結果、Hybrid 攻撃分析プラットフォームとの連携により、マルウェアの変遷を追跡するいくつかの新しい事例を発見でき、時系列情報の経時変化を視覚化する技術としての成果を確認した。

ア②(f)：Hybrid 攻撃分析プラットフォームの構築
(a)-(e)で構築する各分析エンジンの連携を可能とした Hybrid 攻撃分析プラットフォームを設計、構築して (図６参照)、NICT が管理する Web サイト上に本システムを公開する目標に対し、各分析エンジンと連携するための API を整備し、実オペレーションに基づき連動分析シナリオを構築し、そのシナリオについて各分析エンジンを連動させて自動化を実現・実装して目標を達成した。さらには、「アプライアンス発行のアラート対応シナリオ」でオペレーション時間を 1/3 以下に短縮できることを確認した。内部向けと外部向けに別個のデモ・評価用 Web システムを用意して、有識者による評価・フィードバックを獲得し、目標以上の成果を上げた。

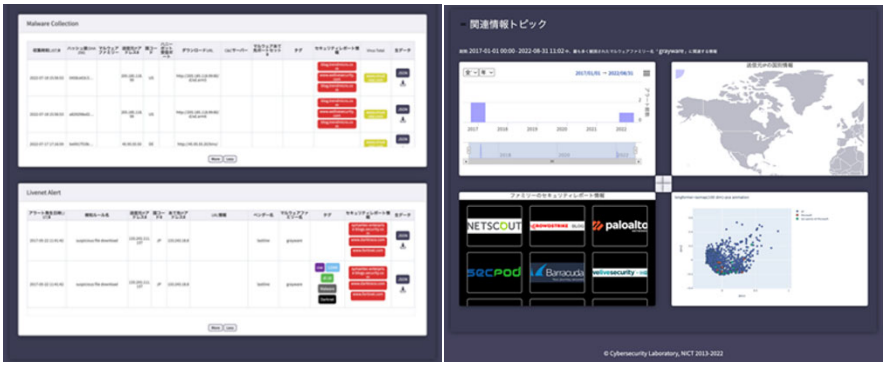
<table>
<tr><td></td><td> 

図６：プロトタイプシステムのスナップショット</td></tr>
<tr><td>イ①IoT マルウェア無害化技術</td><td>イ①(a)：IoT マルウェア無害化情報自動抽出システムの開発
実在する IoT マルウェア 1,000 種（亜種含む）を対象として、70%以上の精度で無害化情報の有無及びその抽出可否を判定し、抽出可能な情報を自動抽出する目標に対し、ア②(d)の技術と連携して無害化情報自動抽出技術を確立した。開発したシステムで実在する IoT マルウェア 4,953 検体（亜種含む）で評価を行った結果、77.04%の精度で無害化情報の有無及びその抽出可否を判定し、抽出可能な情報の自動抽出を実現し目標を達成した。また、今後取り入れられると考えられる高度な手法を実装した IoT マルウェアの疑似検体を 5 種程度試作し、それらへの対策を検討した上で、無害化情報の抽出、無害化の有効性を検証する目標に対し、5 種の疑似検体を試作し、各高度化手法に対応した対策を用いることで無害化の有効性を検証することができ、目標を達成した。

イ①(b)：IoT マルウェア無害化システムの開発
無害化情報の自動抽出が可能であった検体に対して、開発した IoT マルウェア無害化システムを用いて 90%以上の精度で無害化を行う目標に対し、Mirai、Bashlite 検体をあわせた無害化成功率で 96%を実現し、目標を達成した。加えて、イ①(a)で無害化機能がない、或いは無害化情報の一部しか抽出できない検体に対しても、準無害化（シンクホール方式）を検討・検証し、成功率 98.93%を実現した。また、C&C サーバ(マルウェア制御サーバ)の抑制・阻害手法を提案し、安全性や実現性等の観点から評価を行う目標に対し、C&C サーバの抑制・阻害手法を提案し、安全性・実現性の評価を実施したところ、93 種類のマルウェア（C&C サーバ）を全て無害化することに成功し、目標を達成した。

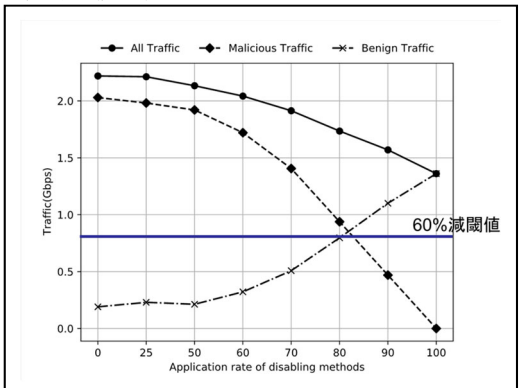
イ①(c)：IoT マルウェア無害化システムの総合評価技術
開発したシステムの総合評価を行い IoT 感染マルウェアに対し約 6 割を無害化することで、大規模感染インシデント時に発生する DoS トラフィックの約 6 割削減に貢献し、無線リソースのひっ迫の解消効果を示す目標に対し、実機・エミュレータ環境で Mirai のパラメータを実測し、大規模 IoT シミュレータを用いた評価を実施した。IoT 機器 1,000 台、ネットワーク数 25 の条件下で、ネットワークへの無害化適用率を 84%程度とすることで、悪性トラヒックの約 6 割削減が可能であることを確認し、目標を達成した（図 7）。
 

図 7：無害化による悪性トラフィックの低減</td></tr>
<tr><td>イ②:IoT マルウェア無機能化技術</td><td>イ②(a)：無機能化アルゴリズム基礎技術
IoT 機器制御用アルゴリズムを確立し、想定するセキュリティモデルにおいて基盤アルゴリズムが理論的にほぼ 100%のセキュリティを達成する目標に対し、現代暗号学観点から放送型認証方式と呼ぶ高機能認証技術を世界で初めて提案し(図８)、システム構成の開</td></tr>
</table>

	発、及び評価を実施した。認証方式を構成する IoT 制御用アルゴリズムに対して、理論的にほぼ 100%のセキュリティを確保するための推奨パラメータを示し、その条件下で効率的に動作することを確認し、目標を達成した。さらに実用性観点から、軽量かつ高度な制御を可能とする基盤アルゴリズムを完成させた。 イ②(b):無機能化の実装に向けた応用技術 課題イ②(a)で開発した安全に機能停止させるための暗号学的な認証符号や認証アルゴリズムを実装した遠隔安全停止システム及びアルゴリズムの高精度の実装方法の追求のために実証実験システムを構築し、フィールド実証実験環境において、99%以上の実装・実現精度で安全に遠隔機能停止できることを示すことを目標に、遠隔安全停止システムを構築し、軽量認証に基づく放送型認証を実装しスマートファクトリーを想定とした実証環境で評価を行い、100%の精度で安全に遠隔から機能停止できることを確認し、目標を達成した。

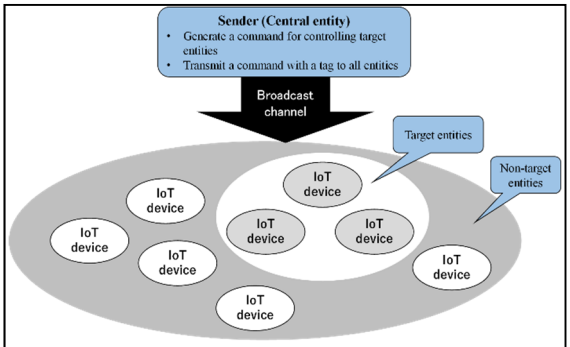


図８：放送型認証（BA）の概念イメージ

3　政策効果の把握の手法

研究開発の評価については、各要素技術における目標の達成状況、論文数や特許出願件数などの指標が用いられ、これらを基に専門家の意見を交えながら、必要性・効率性・有効性等を総合的に評価するという手法が多く用いられている。この観点に基づき、「電波利用料による研究開発等の評価に関する会合」(令和５年６月 22 日)において、目標の達成状況等に関して外部評価を実施し、政策効果の把握に活用した。

また、外部発表や特許出願件数、国際標準提案件数等も調査し、必要性・有効性等を分析した。

4　政策評価の観点・分析等

○研究開発による特許・論文・研究発表・国際標準の実績からの分析

研究開発による特許・論文・研究発表・国際標準の実績については下表の通り。

特に、無機能化のための放送型認証方式の提案(課題イ②(a))を柱として、そのユースケース分析(課題イ②(b))を含めた標準化提案を ITU-T SG17 に提出し、草案の内容として合意を得られた。また、IEEE S&P2022、ASIACCS2021 といった高難易度の採択などを含めた口頭発表数、特許出願件数も当初目標を大幅に上回っており、本研究開発の必要性、有効性が認められた。

主な指標	令和２年度	令和３年度	令和４年度	合計
査読付き誌上発表論文数	１件（　１件）	４件（　２件）	16 件（　14 件）	21 件（　17 件）
査読付き口頭発表論文数（印刷物を含む）	２件（　２件）	22 件（　22 件）	27 件（　26 件）	51 件（　50 件）
その他の誌上発表数	０件（　０件）	０件（　０件）	４件（　３件）	４件（　３件）
口頭発表数	33 件（　２件）	41 件（　６件）	69 件（　９件）	143 件（　17 件）
特許出願数	０件（　０件）	１件（　０件）	３件（　０件）	４件（　０件）
特許取得数	０件（　０件）	０件（　０件）	０件（　０件）	０件（　０件）
国際標準提案数	０件（　０件）	０件（　０件）	１件（　１件）	１件（　１件）
国際標準獲得数	０件（　０件）	０件（　０件）	０件（　０件）	０件（　０件）
受賞数	１件（　０件）	８件（　２件）	３件（　１件）	12 件（　３件）
報道発表数	０件（　０件）	１件（　０件）	１件（　０件）	２件（　０件）

報　道　掲　載　数	０件（　０件）	０件（　０件）	０件（　０件）	０件（　０件）

注１：各々の件数は国内分と海外分の合計値を記入。（括弧）内は、その内海外分のみを再掲。

注２：「査読付き誌上発表論文数」には、定期的に刊行される論文誌や学会誌等、査読（peer-review（論文投稿先の学会等で選出された当該分野の専門家である査読員により、当該論文の採録又は入選等の可否が新規性、信頼性、論理性等の観点より判定されたもの））のある出版物に掲載された論文等（Nature、Science、IEEE Transactions、電子情報通信学会論文誌等及び査読のある小論文、研究速報、レター等を含む）を計上する。

注３：「査読付き口頭発表論文数（印刷物を含む）」には、学会の大会や研究会、国際会議等における口頭発表あるいはポスター発表のための査読のある資料集（電子媒体含む）に掲載された論文等（ICC、ECOC、OFC など、Conference、Workshop、Symposium 等での proceedings に掲載された論文形式のものなどとする。ただし、発表用のスライドなどは含まない。）を計上する。なお、口頭発表あるいはポスター発表のための査読のない資料集に掲載された論文等（電子情報通信学会技術研究報告など）は、「口頭発表数」に分類する。

注４：「その他の誌上発表数」には、専門誌、業界誌、機関誌等、査読のない出版物に掲載された記事等（査読の有無に関わらず企業、公的研究機関及び大学等における紀要論文や技報を含む）を計上する。

注５：PCT（特許協力条約）国際出願については出願を行った時点で、海外分１件として記入。（何カ国への出願でも１件として計上）。また、国内段階に移行した時点で、移行した国数分を計上。

注６：同一の論文等は複数項目に計上しない。例えば、同一の論文等を「査読付き口頭発表論文数（印刷物を含む）」及び「口頭発表数」のそれぞれに計上しない。ただし、学会の大会や研究会、国際会議等で口頭発表を行ったのち、当該学会より推奨を受ける等により、改めて査読が行われて論文等に掲載された場合は除く。

○各観点からの分析

観点	分析
必要性	IoT マルウェアによる被害は近年顕著に増加しており、サイバーセキュリティ戦略（2018 年７月 閣議決定）などにおいても、IoT セキュリティ対策技術のための研究開発の重要性が指摘されている。 本研究開発は、IoT マルウェアの無害化等による周波数の有効利用を実現する技術を開発するだけでなく、IoT 環境におけるセキュリティの確保を通じて安全・安心な社会インフラの実現に資することから、研究開発すべき課題として着目した。 また、民間が行うセキュリティ対策のうち、IoT 機器のユーザがその対価を払うインセンティブがあるような脅威（例えば、プライバシ侵害や個人情報、オンラインサービスのアカウント情報の窃取など）に対しては、民間において対策導入が進む可能性があるものの、DDoS 攻撃の踏み台や他機器への感染攻撃などのようにユーザ自身への被害が明確でないものについては、ユーザがコストをかけてまで製品を購入する状況にはなっておらず、民間としてのセキュリティベンダ側も本格的な対策技術の開発に踏み切れていない状況である。 これらの点から本研究開発で取り組む先進的な技術は、国民の財産である電波資源の有効利用及び国民の生活インフラである ICT 空間の安全・安心の確保に資するものであり、国が実施すべき研究開発として推進する必要がある。よって、本研究開発には必要性があったと認められる。
効率性	本研究開発を実施するに当たっては、IoT マルウェアの調査・解析及びその特性・性質に関する専門的知識や研究開発実績を有する受託者が、蓄積されたノウハウ・知見を有効に活用することで効率的で質の高い研究開発が進められた。 また、実施期間中も受託各機関の研究代表者・実務者においては定期的に各機関の進捗状況や課題が調整・共有され、さらに外部の有識者と受託者から構成される運営委員会や、外部有識者による継続評価において、研究進捗や進め方等について助言を受けるなど、効率的な実施のため情報交換が積極的に行われた。 最後に、予算要求段階、公募実施の前段階、提案された研究開発提案を採択する段階、研究開発の実施段階及び研究開発の終了後における、実施内容、実施体制及び予算額等について、外部専門家・外部有識者から構成される評価会において評価を行い、効率的に実施した。 よって、本研究開発には効率性があったと認められる。
有効性	IoT マルウェアの挙動検知及び駆除技術及びマルウェアに感染した IoT 機器を安全に無害化・停止する技術を確立することにより、不正な無線通信トラヒックの発生を抑止できるようになるため、IoT 環境における無線リソース逼迫の解消に寄与することができた。 また、学識経験者・有識者で構成される研究開発運営委員会を通じて、技術的内容だけでなく、研究

	成果の展開方策等についても議論をすることで、研究成果の実用化等へ向けた高い確実性が得られた。 さらに、高度 IoT ハニーポットの攻撃観測結果やマルウェア解析結果を 26 か国 138 研究組織に提供し、一部のセキュリティ商品に実装されていること、本研究開発の技術を活用したマルウェア感染・脆弱性検査サービスを令和 4 年 2 月から開始し 9 万人以上の利用者があること、ITU-T において放送型認証方式の標準化提案を行っていること、計画を超える数の特許申請を行っていること等、実用化に向けて積極的な取組を行っている。 よって、本研究開発には有効性があったと認められる。
公平性	IoT 機器は多くの分野で利用される一方、IoT 機器に感染して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、無線リソースの逼迫が懸念されている。本研究開発は、IoT 機器に感染するマルウェアの詳細分析技術の開発を行うとともに、IoT マルウェアの無機能化及び機能停止を実現するものであり、不正な無線通信トラヒックの発生を抑止し、電波の有効利用に大きく寄与するものであることから、広く無線局免許人や無線通信の利用者の利益となる。 また、本研究開発の実施に当たっては、開示する基本計画に基づき広く提案公募を行い、提案者と利害関係を有しない複数の有識者により審査・選定した。 よって、本研究開発には公平性があったと認められる。
優先性	IoT 機器はネットワークとの常時接続性、軽量性、管理主体の曖昧さ等の特徴を有していることから、マルウェアに感染し易く DDoS 攻撃等の踏み台となって無線通信トラヒックを増大させ、他の無線サービスによる無線利用を阻害するおそれがある。近年では、このような IoT 機器を踏み台とした大規模な攻撃が度々確認されており、周波数の有効利用の観点から対策が急務となっている。本研究開発は、IoT 機器に感染するマルウェアの無機能化及び機能停止を実現し、IoT 機器へのマルウェア感染に起因するサイバー攻撃による無線リソース逼迫を低減し、健全な IoT 機器を有効に活用できる安心・安全な社会の実現に寄与するものである。 よって、本研究開発には、優先性があったと認められる。

５　政策評価の結果（総合評価）

本研究開発は、IoT 機器の急速な普及に伴う無線リソース逼迫の対策として、IoT マルウェアの検知及び駆除と IoT 機器の無害化・無機能化する技術の確立は必要性を十分に認めるところである。

IoT 機器の急速な普及に伴う無線リソース逼迫の対策として、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、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、IoT マルウェア無害化技術、IoT マルウェア無機能化技術を確立することにより、無線リソースの有効活用に寄与しており、目標を達成することができた。

よって、本研究開発には有効性、効率性等があると認められた。

＜今後の課題及び取組の方向性＞

・課題ア①：マルウェア収集、分析機構の運用を継続し、IoT におけるサイバー攻撃情報の収集・蓄積を図る。これらの情報をネットワークオペレータ、対策機関、研究機関等に提供すると共にマルウェア感染状態や脆弱性を診断するサービスを試験的に展開する。続いて、応用段階で展開するサービスの高度化や他のセキュリティサービスとの連携により、純国産サイバーセキュリティインテリジェンス提供サービスの実現を目指す。

・課題ア②：インテリジェンス収集、各分析エンジンを活用した分析結果の収集・蓄積を継続し、IoT におけるサイバー攻撃情報の収集・蓄積を図る。各分析エンジンの効果を継続してモニタリングし、改善に向けた応用開発を実施する。そして、マルウェア活動の発生検知精度の向上、攻撃検知アラートの品質向上、マルウェア進化系統樹の精度向上、インテリジェンス情報高度化等を実現する。続いて、応用開発を通じて収集、蓄積した情報等を外部で活用するサービスを実施する。ハイブリッド分析プラットフォームの分析起点となるダークネットトラフィック等についても、適切な形に加工してデータ公開を適宜実施する。プラットフォームを構成する技術についても、NICT 内部のオペレーションで利用可能な技術をツール化し、そのノウハウを外部機関等に

共有する。
・課題イ①：セキュリティ監視支援サービス提供に向けて、実用化に向けた技術提供形態を IoT 機器ベンダー等と検討し、明確化する。続いて、IoT 機器ベンダーの監視サービスの一部として、本無害化技術の技術供与を図る。複数の IoT 機器製品を監視して組織における IoT マルウェアの無害化を行うサービスへの展開を目指す。
・課題イ②：遠隔安全制御システムの技術サービスを利用する顧客、市場を発掘する。顧客への提供価値を見極め、付加価値の提供を期待できるサービス事業を特定して、無機能化デバイスの小型化や遠隔安全停止システムの高機能化を目指す。続いて、応用段階で進める小型化や高機能化について、これを特定のサービス供給用に実装することが必要で、これが実用化の鍵となる。応用段階で得たフィードバックを踏まえて想定されるユースケースにおける実証実験を少なくとも 1 件実施することを目指す。また、具体的なサービス提案ができるように準備を進める。

6　学識経験を有する者の知見の活用

「情報通信技術の研究開発の評価に関する会合」（令和５年６月 22 日）において、目標の達成状況や得られた成果等について、研究開発の目的・政策的位置付け及び目標、研究開発マネジメント、研究開発成果の目標達成状況、研究開発成果の社会展開のための活動実績並びに研究開発成果の社会展開のための計画などの観点から、外部評価を実施し、以下の御意見等を頂いたため、本研究開発の評価に活用した。

・　目標をすべて達成している。無線リソースのひっ迫の解消効果を定量的に示していただけると、電波資源有効利用の観点ではより良い。サイバー攻撃は日々変化しているが、それらに対応する分析プラットフォームを作成して、情報提供を広く目指している点は高く評価できる。
・　当初計画を超える性能が得られることを確認し、有効性を明らかにした。また著名な海外査読付き論文をはじめとして計画を上回る対外発表数を達成し、多くの受賞を得ている。
・　効果の評価実験のためのテストベッドとマルウェア分析システムなど多数のシステムを短期間に構築して広範囲の検証を行っており、予算は効率的に使用されたと考えられる。
・　ITU-T での勧告を目指した取り組みなどが行われている。ハニーポットによる攻撃の観測結果や収集された検体の解析結果を対策機関や企業に提供し、一部のセキュリティ商品に実装されている点や、IoT 機器の脆弱性を IPA 経由でメーカに届け出て脆弱性が修正された点なども評価できる。
・　本研究開発は、IoT 機器の急速な普及に伴う無線リソース逼迫の対策として、IoT マルウェアの共同検知及び駆除と IoT 機器の無害化・無機能化する技術の確立を目標としたものであり、最終年度にあたる本年度は、各要素技術において、実装・評価を完了し、目標性能を達成している。また、積極的な学術面での取り組みに加えて、ITU-T への草案の提出や計画を超える４件の特許申請を行っており、社会実装に向けた取り組みも着実に実施している。本研究開発全体としては、目標性能を達成する成果と学術面での積極性が評価できる。一方で、具体的にどのようにサービスへ実装し、研究開発成果の付加価値を生み出していくかといった点が課題と思われ、我が国のセキュリティ産業の競争力強化の一環として、本技術成果に基づく具体的な取り組みを期待したい。

7　評価に使用した資料等

○電波利用料による研究開発等の評価に関する会合　＜電波利用料＞
http://www.tele.soumu.go.jp/j/sys/fees/purpose/kenkyu/index.htm

○サイバーセキュリティ戦略（令和３年９月 28 日）
https://www.nisc.go.jp/pdf/policy/kihon-s/cs-senryaku2021.pdf

○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）
https://www.nisc.go.jp/pdf/council/cs/kenkyu/dai12/kenkyu_torikumi.pdf

○電波有効利用成長戦略懇談会　報告書（平成 30 年８月 31 日）
https://www.soumu.go.jp/menu_news/s-news/01kiban09_02000273.html

○サイバーセキュリティ戦略（平成 30 年７月 27 日）
https://www.nisc.go.jp/pdf/policy/kihon-s/cs-senryaku2018.pdf

○＜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（令和２年３月 23 日）
https://www.soumu.go.jp/main_content/000677037.pdf