（革新）様式 1-4-2 (2025-1)

令和７年度研究開発成果概要書

採 択 番 号　　08101
研究開発プロジェクト名　　デジタルツインによるサイバー・フィジカル連携型セキュリティ基盤

（１）研究開発の目的

Beyond 5G においてサイバー空間とフィジカル空間の融合が進展すると、攻撃やその影響もサイバー空間だけでなくフィジカル空間にも拡大し、これまでにない全く新しいセキュリティ脅威が顕在化する。例えば、（１）広域ネットワークから観測されることなく、フィジカル空間で IoT デバイスそのものに攻撃が行われる。（２）攻撃を受けた IoT デバイスが、フィジカル空間で異常や不正動作を起こす、もしくは近傍のサイバー空間でしか観測できない振る舞いとして現れる。

上記の例は広域ネットワークからは観測されず、その一方、こうしたケースはサイバー空間とフィジカル空間が融合する Beyond 5G において急激に増大することが予想される。現状ではこうした攻撃や影響を観測し対策するインフラが整っていないため、たまたま局所的に攻撃や不正動作が観測されたとしても、広域ネットワークの影響の有無や、対策の要否について的確に判断することができず、社会全体として効果的な対策を講じることも困難である。

この課題解決を目指しサイバー空間とフィジカル空間双方、近傍と広域で得られる情報を用いてデジタルツインによるセキュリティ対策を行う基盤を構築し、実際のサイバー・フィジカルシステムにおける実証実験を行う。

（２）研究開発期間

令和６年度から令和７年度（２年間）

（３）受託者

株式会社ＫＤＤＩ総合研究所＜代表研究者＞
国立大学法人横浜国立大学
学校法人早稲田大学
学校法人芝浦工業大学

（４）研究開発予算（契約額）

令和６年度から令和７年度までの総額 200 百万円（令和７年度 100 百万円）
※百万円未満切り上げ

（５）研究開発項目と担当

研究開発項目１　脅威情報を含めたデジタルツイン生成技術の研究開発
1-a）デジタルツイン生成技術　（株式会社ＫＤＤＩ総合研究所）
1-b）次世代 IoT サイバー・フィジカル攻撃防御技術　（株式会社ＫＤＤＩ総合研究所）
研究開発項目２　デジタルツイン生成のためのネットワーク探索・観測技術
2-a）B5G のための次世代 IoT 近傍観測技術　（国立大学法人横浜国立大学）
2-b）B5G のための次世代 IoT 広域観測技術　（株式会社ＫＤＤＩ総合研究所）
2-c）次世代 IoT デバイスプロファイリング技術　（国立大学法人横浜国立大学）
研究開発項目３　フィジカルデバイスから得られる情報を用いた異常検知技術の研究開発
3-a）フィジカルデバイス不正検知技術　（学校法人早稲田大学）
3-b）フィジカルデバイスレポジトリ構築・連携技術　（株式会社ＫＤＤＩ総合研究所）
研究開発項目４　Beyond 5G のアプリケーションを対象としたセキュリティ基盤の実証
4-a）モビリティシステムに対するセキュリティ攻撃負荷実験　（学校法人芝浦工業大学）
4-b）提案セキュリティ基盤によるセキュリティ攻撃耐性向上の実証（学校法人芝浦工業大学）

（6）特許出願、外部発表等

		累計（件）	当該年度（件）
特許出願	国内出願	6	4
	外国出願	0	0
外部発表等	研究論文	6	4
	その他研究発表	118	71
	標準化提案・採択	4	1
	プレスリリース・報道	1	1
	展示会	2	2
	受賞・表彰	6	3

（7）具体的な実施内容と最終成果

研究開発項目1　脅威情報を含めたデジタルツイン生成技術の研究開発

1-a）デジタルツイン生成技術

本項目の最終目標は、近傍の各種サービスやネットワークから得られる情報と、研究開発項目 2、3 で取得できる情報を組み合わせることでセキュリティ対策のためのデジタルツインを生成し、研究開発項目 4 の実アプリケーション上での動作までを完了することである。

小型モビリティサービスを対象としてセキュリティデジタルツインによるセキュリティ対策の実証を完了させ、次世代モビリティに関する研究発表会（2025ADAM 発表会）で動態展示を行った。

1-b）次世代 IoT サイバー・フィジカル攻撃防御技術

本項目の最終目標は、1-a）で生成したデジタルツインを用いて、観測された攻撃や脅威情報をもとに、自律的にセキュリティ対策を行う技術を開発することである。

NICT が提唱するデジタルツイン連携オーケストレータの概念を導入し、パブリッククラウド上でデジタルツイン間連携に関する適合性および実用性の検証を完了させた。

ITU-T FG-MV（Focus Group on metaverse）に提案したメタバース相互接続におけるセキュリティ対策シナリオが FG-MV の成果文書となり、さらに、今会期に設立された SG21 の勧告 H.770.1 に反映させることができた。

研究開発項目2　デジタルツイン生成のためのネットワーク探索・観測技術

2-a）B5G のための次世代 IoT 近傍観測技術

本項目の最終目標は、IoT におけるサイバー攻撃等の脅威を定常的に収集・蓄積する次世代 IoT ハニーポット技術と、収集した IoT マルウェア検体を解析する次世代 IoT マルウェア解析技術を開発することである。また、収集された脅威情報を分析する技術を開発することである。

高度な通信制御や状態監視に基づく実機の IoT 機器を用いた次世代 IoT ハニーポットを実装し、4 種類の機器を用いた長期間の攻撃観測により脅威情報の収集・蓄積に有効であることを確かめた。

IoT マルウェアに搭載された妨害機能を検出する次世代 IoT マルウェア解析技術を実装し、実マルウェア 500 検体を動的解析することで他の侵入者の活動の妨害機能の検知に有効であることを確かめた。観測結果から新規の攻撃を検知する技術や時系列分析する技術を実装し、ゼロデイ疑いがある攻撃を含む計 50 件の攻撃の検知と脆弱性の開示から攻撃の拡大・収束に至るまでの実態を明らかにした。また、エクスプロイトの時系列分析の論文がセキュリティ系の難関カンファレンス（ASIACCS 2026）に採録された。

2-b）B5G のための次世代 IoT 広域観測技術

本項目の最終目標は、IoT 向け B5G スライスを流れる通信を対象に異常検知を行う技術を開発することである。

通信キャリアのネットワークにおけるフローデータを用いた異常検知技術を確立させ、査読付き論文 1 件が採択された（2026 年 2 月に発表）。

2-c）次世代 IoT デバイスプロファイリング技術

本項目の最終目標は、IoT 機器のリスクに関する情報を包括的に収集する次世代 IoT デバイスプロファイリング技術を開発することである。

ファームウェア解析によるプロファイリング、ネットワーク応答を利用したプロファイリング、公開情報を用いたプロファイリングの 3 種類のプロファイリング手法を実装し、のべ 700 機種の IoT デバイスを用いて性能評価を実施し、プロファイリング手法が有用であることを確かめた。また、 IPv6 環境でも約 100 機器のプロファイリングを行い、有効性を確かめた。

また、研究開発項目 1-a に、機器の応答をもとに、機器メーカー名・機種を特定するためのシグネチャを提供した。

プロファイリング技術を活用したセキュリティ診断サービスを運用し、約 21 万ユーザーを診断した。また、その診断サービスの効果を分析した論文がセキュリティ系のトップカンファレンス(USENIX Security 2025)に採録された。

研究開発項目３　フィジカルデバイスから得られる情報を用いた異常検知技術の研究開発

3-a）フィジカルデバイス不正検知技術

本項目①「IoT 回路の不正検知技術」の最終目標は、（第 1 段階）ならびに（第2段階）の 2 つの段階を経て、多様な IoT 回路に対して、機械学習ベースの不正回路検知技術を確立、②「IoT デバイスの不正検知技術」の最終目標は、電力波形の形状距離をもとに「正常動作」と「異常動作」を識別し、異常動作がない IoT デバイスと、異常動作を含む IoT デバイスとを識別・分類する基盤アルゴリズムを確立することである。さらに 3-b）で構築されるフィジカルデバイスレポジトリとの実動作することを確認することである。

①「IoT 回路の不正検知技術」では、まず（第 1 段階）複数のアンサンブル学習モデルを用いた機械学習ベースの不正回路検知技術を確立、（第 2 段階）グラフならびに属性情報をグラフ学習することで不正／正常ノードを識別する基盤アルゴリズムを確立した。②「IoT デバイスの不正検知技術」では、波形間の形状距離を測定し、正常波形と異常波形とが識別可能な形状距離を設計し、形状距離により正常／波形の識別に成功した。加えて、これらがフィジカルデバイスレポジトリで実動作することを確認した。

さらに①「IoT 回路の不正検知技術」、②「IoT デバイスの不正検知技術」に関して、基盤アルゴリズムの改良に取り組み、異常回路や異常動作に頑健な基盤アルゴリズムの構築を完了した。

3-b）フィジカルデバイスレポジトリ構築・連携技術

本項目の最終目標は、フィジカルデバイスレポジトリを構築し、API を通じて外部システムとの連携を実証することである。

フィジカルデバイスレポジトリの構築を完了し、外部連携 API についても確立した。また、デジタルツイン基盤との連携を通じて、B5G ユースケースにおける活用を実証した。

さらに、フィジカルデバイスレポジトリを用いて既知の脆弱性情報を収集した。この情報も活用し、社会実装に向けた課題抽出ならびに標準化に向けた調査を完了した。

研究開発項目４　Beyond 5G のアプリケーションを対象としたセキュリティ基盤の実証

4-a）モビリティシステムに対するセキュリティ攻撃負荷実験

本項目の最終目標は、定義した 9 つすべてのモビリティ型に対するセキュリティ攻撃負荷実験において定量的結果を得ることである。

対象のすべての型に対する実験を完了した。

さらに、セキュリティ攻撃としてセンサデータの改ざんなどの高度な攻撃の採用を行うほか、4-a）の内容を包含したセキュリティフレームワークの論文が IEEE Security & Privacy Magazine に採録され、世界的に評価を得た。

4-b）提案セキュリティ基盤によるセキュリティ攻撃耐性向上の実証

本項目の最終目標は、4-a）で実証を行った 9 つの型について網羅的な実証実験を行うことである。一定以下の負荷であれば、攻撃を無効化し正常動作を継続可能であることを、一定以上の負荷に対しても、誤動作の回避と正常動作への復旧が可能であること、前者と後者の境界となる負荷のしきい値を明らかにし、従来の機能ごとの個別セキュリティ対策に比べ、提案セキュリティ基盤がそのしきい値を 10 倍に引き上げることを示すことである。

点群データから抽出した特徴量の変化を確認することで異常検知する技術、複数の環境 LIDAR センサから点群と点群の関係特徴を抽出し正常時と比較することで異常検知する技術、点群データ間の類似度を算出することで異常検知する技術を確立し、スタンドアローン型・ネットワーク型・デジタルツイン型の網羅的検知を完了させた。

異常発生時に異常系を切り離し正常系に切り替える技術を確立した。本技術の確立により、一定以下の負荷無効化、および一定以上の負荷に対する誤動作回避と正常復旧、負荷のしきい値を特定した上でその値を 10 倍以上に引き上げることを完了させた。

さらに、研究開発項目 4 として、外部発表目標である研究論文 2 件、査読付収録論文 3 件に対し、研究論文 2 件、査読付収録論文 3 件、その他学会発表など 8 件発表した。また、特許出願を 1 件行い、その内容についてプレスリリースを発出した。

（8）研究開発成果の展開・普及等に向けた計画・展望

①計画

本課題の提案アーキテクチャを、自動運転モビリティを最初のターゲットとして実装の上で、NICT オーケストレータを活用して横展開する。

個別技術についても、それぞれに適したプラットフォームやサービスに組み込む形で展開する。

国際標準化や産業財産権についても継続的な提案・出願を進める。

②展望

上記の自動運転モビリティをパイロットケースとして、技術の有効性を実世界で証明し、他産業への展開を加速させる。

関連性の高い研究開発テーマとして、デジタルツイン運用自動化やフィジカル AI のセキュリティ等を想定し、標準化提案や知財化に反映させる。