（革新）様式 1-4-2 (2022-1)

令和６年度研究開発成果概要書

採 択 番 号　　08101
研究開発課題名　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 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	2	2
	外国出願	0	0
外部発表等	研究論文	4	4
	その他研究発表	49	49
	標準化提案・採択	3	3
	プレスリリース・報道	0	0
	展示会	0	0
	受賞・表彰	3	3

※関連課題(05201)における令和６年度成果を含む。

（7）具体的な実施内容と成果

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）研究開発項目２や３で構築するフィジカルデバイスレポジトリやプロファイル情報データベースのプロトタイプと接続できるようデジタルツイン API の基礎実装を完了する、という目標に対し、セキュリティ対策用デジタルツイン基盤のプロトタイプの実装を完了した。既存のサービスを提供するデジタルツインと接続する「近傍セキュリティデジタルツイン」（近傍 SDT）およびセキュリティ情報を集約・提供する「セキュリティデジタルツイン広域連携プラットフォーム」（SDTPF）を構築し、さらに SDTPF からフィジカルデバイスレポジトリを参照できるようにした。

1-b）研究開発項目 1-a)と研究開発項目 2,3 の連携によって生成したセキュリティ対策用デジタルツインのプロトタイプを利用し、サイバー・フィジカル両方が関わる攻撃の対策を行えるようにするという目標に対し、デジタルツイン連携による対策シナリオの設計を完了した。さらに ITU-T FG-MV WG5 の標準化文書におけるデジタルツインおよびメタバースの相互運用性のユースケースとしてセキュリティ対策シナリオを盛り込み（NICT と共同)、ITU FGMV-43 の成果文書に反映された。

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）サイバー攻撃・マルウェア等の脅威情報の観測、マルウェア解析のそれぞれに関して前年度に設計した方式に基づき実装を行い、観測網の拡張を行うという目標に対して、実機の IoT 機器を用いた観測技術を拡張し、ISP 回線を用いてインターネット上に設置された機器の状況をよりリアルに再現した。さらに、観測結果から新規の攻撃を抽出・分類する技術を確立することで目標を上回る成果を達成した。同様に、動的解析システムを拡張し、IoT マルウェアに搭載された他者を妨害する機能を明らかにすることで目標を上回る成果を達成した。

2-b）セキュリティ対策向けデジタルツインへの連携を想定して、API のプロトタイプを構築するという目標に対し、Federated Learning（FL）による多拠点のデータを用いた異常通信検知技術をデジタルツイン間連携で行う際の仕様策定を完了した。複数の近傍 SDT の異常検知モデルを SDTPF で連合させる構成となっており、近傍セキュリティデジタルツインと広域連携プラットフォームそれぞれで設ける機能の設計までが完了した。

2-c）プロファイリング手法の実装と、数種類の IoT デバイスを用いた試験運用と性能評価を実施するという目標に対し、プロファイリング手法(SCA ツールを用いたファームウェア解析によるプロファイリング、WebUI と Basic 認証の応答に基づくプロファイリング、公開マニュアルに基づくプロファイリング)を実装し、数種類の IoT デバイスを用いた試験運用と性能評価を実施し目標を達成した。具体的には、各プロファイリングを合計して、4 つの IoT のカテゴ

リ(ネットワーク機器、メディア機器、コンシューマ機器、産業用機器)について、プロファイリングを実施した。また、IPv6 環境についても、マニュアル調査等により、機器が持つリスクのプロファイリングを実施した。

さらに、プロファイリングを利用したセキュリティ診断サービスを運用し、目標を上回る成果をあげることができた。当該サービスの論文がセキュリティ分野のトップカンファレンスであるUSENIX Security’25 に採択された。

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)①まずネット特徴量に基づく機械学習ベースの不正回路検知技術の確立という目標に対し、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した。さらに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の確立という目標に対し、グラフ学習を用いることで回路情報全体を学習し不正を検知する基盤アルゴリズムを確立した。②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するという目標に対し、形状距離により正常／波形の識別に成功した。

3-b）フィジカルデバイスレポジトリの外部連携を念頭に国内外の最新の研究動向を調査するという目標に対し、国内外の最新の研究動向としてソフトウェア部品表の外部連携に関する文献を調査した。調査の結果、事業者やデータの違いに起因する表記ゆれの統一が課題であることを抽出し、大規模言語モデルを用いて解決する手法を設計して知財 1 件の出願を完了した。さらに、フィジカルデバイスレポジトリを外部システムと連携するため、表記ゆれを考慮して検索する機能を実装し、パブリッククラウド上での動作検証を完了した。

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）今年度の目標は、AN、AD、SD 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。目標を達成するために、各型のモビリティシステムの確立を課題とする。実験を実施し AN、AD、SD 型のいずれにおいてもセキュリティ攻撃の影響度を定量化する技術を確立した。定量的結果を取得し、今年度の目標を達成した。

（AN: 自動運転-ネットワーク補助、AD: 自動運転-デジタルツイン、SD: 運転補助-デジタルツイン）

4-b）今年度の目標は、MS、MN、SS 型に対して実証実験を行い定量的結果を得ることである。上記の目標を達成するために、データ改ざんに対する検知、LIDAR センサに対する物理的な攻撃に対する検知を課題とする。実験を実施し、MS、SS、MN 型のいずれにおいても異常検知する技術を確立した。定量的結果を取得し、今年度の目標を達成した。

（MS: 手動運転-スタンドアローン、MN: 手動運転-ネットワーク補助、SS: 運転補助-スタンドアローン）

外部発表３件（研究論文１件、査読付収録論文２件）の目標に対して、研究論文２件、査読付き収録論文１件の発表を行い、それに加えて、収録論文２件、査読付き国際会議ポスター発表４件の発表を行った。

（8）今後の研究開発計画

2025 年度は、最終年度として、各研究開発の成果とデジタルツインの繋ぎ込みを完了し、セキュリティ対策基盤として完成させる。具体的には以下の研究開発を進める。

- 研究開発項目１では、研究開発項目４を通じた実証により、2024 年度までに構築した機能のブラッシュアップを行う。
- 研究開発項目２では、2024 年度に実施したプロトタイプ実装・評価の結果を踏まえ、性能向上と、適宜他の研究開発項目へのデータ提供などを実施する。
- 研究開発項目３では、IoT 回路の不正検知および IoT デバイスの不正検知について、2024

年度までに構築した識別アルゴリズムをベースに、不正検知を行う技術を確立する。また、フィジカルデバイスレポジトリの外部連携 API の確立と、社会実装に向けた課題抽出を行う。

- 研究開発項目 4 では、Beyond 5G の具体的なアプリケーションとしてモビリティを対象としたセキュリティ基盤の実証を行う。フィジカル・サイバー攻撃に対する耐性の評価を行う。また、本研究開発成果により、その耐性が大幅向上することを実証する。

また、2024 年度に開始した、標準化に向けた取り組みを、継続して進める。