（革新）様式 1-4-2 (2022-1)

令和５年度研究開発成果概要書

採 択 番 号　　05201
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。

（2）研究開発期間

令和４年度から令和５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４年度から令和５年度までの総額 698 百万円（令和５年度 348 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　フィジカル空間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	4	2
	外国出願	0	0
外部発表等	研究論文	10	8
	その他研究発表	99	64
	標準化提案・採択	0	0
	プレスリリース・報道	3	1
	展示会	2	1
	受賞・表彰	6	4

（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) デジタルツインを活用したセキュリティ対策基盤のアーキテクチャ設計を完了した。本アーキテクチャは、脅威情報を収集する広域連携プラットフォーム、所要のサービスを提供するサービスデジタルツイン、およびそれらから得られる情報を用いてセキュリティ対策機能を付与するモジュールである近傍セキュリティデジタルツインから構成される。さらに、広域連携プラットフォーム、サービスデジタルツイン、近傍セキュリティデジタルツインのプロトタイプを構築し、コンポーネント間のデータ連携が円滑に行えることを確認した。

1-b) 1-a)で設計したアーキテクチャにおいて、研究開発項目 2,3,4 で得られた成果を活用してセキュリティ対策を行う際の動作仕様を策定した。研究開発項目 2,3 で発見したサイバー・フィジカル両方の観点での脅威情報を広域プラットフォームに蓄積し、近傍セキュリティデジタルツインを用いて研究開発項目 4 をはじめとした B5G アプリケーションでのセキュリティ対策に活用する。さらに、研究開発項目 4 におけるシミュレーション、研究開発項目 2,3 で開発した脅威検知手法を用いて近傍セキュリティデジタルツインで脅威を発見し、広域プラットフォームに蓄積された情報と突き合せて詳細分析を行う、というシナリオを設計した。

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 時代における IoT 機器探索、サイバー攻撃・マルウェア等の脅威情報の観測、マルウェア解析の設計方針および方式検討という目標に対し、方針策定、方式検討を完了し、実装を前倒して実施した。IoT 機器探索では IPv6 空間探索と実機調査により、機器の実装に起因して、多くの機器がインターネットからアクセス可能であることを明らかにした。脅威情報の観測では高度な通信制御や状態監視に基づく観測方式と実機の IoT 機器を用いて、実際にサイバー攻撃やマルウェア等の観測を行った。マルウェア解析では動的解析結果とハニーポットの観測結果を突合することで攻撃活動の実態を明らかにした。

2-b) Federated Learning を用いた異常通信検知を実際に複数拠点で収集した IoT デバイスの通信データに適用し、評価を行った。また、異常が疑われるデバイスをほかの地点で検出する技術として、デバイス識別技術を適用し、様々な手法を様々なデータセットで評価し、汎用的に使える手法の調査を行った。また、スケーラビリティ評価のため、異常通信検知用データセットを IoT データの特性を加味して拡張するツールを開発した。

2-c) ローカルプロファイリング、公開情報プロファイリング、リモートプロファイリングに関する調査・要件検討の実施と方式の基礎検討を行うという目標を達成し、データ連携を見据えて保存すべき情報を精査した。ローカルプロファイリングとして商用ツールを用いた IoT 機器のファームウェアの分析を行い、さらにファームウェアのリリース日(公開情報)とファームウェアに含まれる脆弱性の公開日の関係性から、メーカーの脆弱性への対応の差を分析した。リモートプロファイリングとして WebUI のクラスタリングにより IoT 機器を発見する方式を検討し、海外の ISP を対象に方式の検証を行い 200 種類以上の IoT 機器を発見した。

研究開発項目３：フィジカル空間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) IoT 回路の不正検知技術の研究開発に対し、IoT 回路情報から不正回路を表す特徴量を体系化し、ツリーベースのアンサンブル学習モデルとして、ランダムフォレスト、XGBoost、LightGBM、CatBoost の 4 種類を対象に IoT 回路の不正回路特徴量を最適化した。さらに、不正回路の識別を行い、平均 F 値として 0.87 を得た。さらに、IoT デバイスの不正検知技術では、IoT デバイス上でアプリケーションプログラムの動作から、さまざまなアプリケーションプログラムの電力波形を収集し不正検知技術基盤を確立した。

3-b) IoT 回路および IoT デバイスに対する不正検知結果を登録・活用するため、「フィジカルデバイスレポジトリ」の基礎実装および API 実装を完了した。基礎実装ではデータベースのテーブルを設計し、ユーザー管理等の各種機能を Web アプリとして実装した。特にテーブルの設計では、製品情報や脆弱性情報に加え、脆弱性の脅威度を示す値や脆弱性に関する事例等のフィールドを設定した。API の実装では、製品情報と脆弱性情報を集約する API を構築することで、API を用いない場合と比較して最大 76%情報集約の操作を効率化した。

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) 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九つの型のシステムモデルを設計した。その中から、MS、MN、MD、SS、SN、AS、{ ［手動運転(M)・運転補助(S)・自動運転(A)］ × ［スタンドアローン(S)・ネットワーク補助(N)・デジタルツイン(D)］ }これら６つの型について実験システムを構築し、フィジカル型、サイバー型、複合型セキュリティ攻撃実験を実施し、定量的結果を得た。研究論文２件、査読付収録論文５件、収録論文２件など目標をはるかに上回る外部発表を行った。

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のため、実証実験の仕様策定を行った。実験では研究開発項目 4-a)で構築したモビリティシステムに対して提案セキュリティ基盤により、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示す。研究開発項目 1 との連携として、4-a)の実験で得た結果を基にセキュリティ攻撃を受けた際の走行データのシミュレーションを行い、経路予測が可能なことを明らかにした。

（8）研究開発成果の展開・普及等に向けた計画・展望

本研究開発の、図 1 に示す 2024 年度以降の実施計画事項を、研究開発プロジェクト「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」（採択番号 08101）に引き継ぎ、最終目標の達成を目指す。

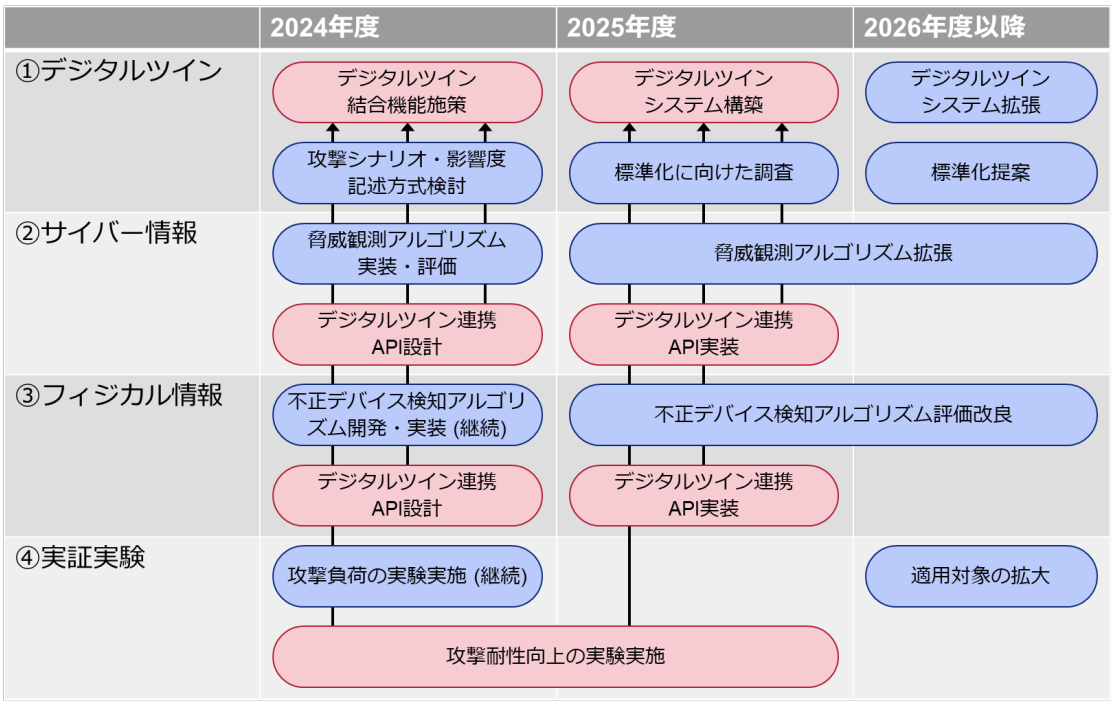

図１　研究開発計画

2024 年度は、アルゴリズムの性能評価や改良と並行して、各研究開発によって得られる脅威情報をデジタルツインへ連携するための機能設計や、実アプリケーションにおける実験を行う。
2025 年度は、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。さらには標準化に向けた調査を開始する。
さらに、当該プロジェクト終了後には、標準化提案や、成果展開へ向けたシステムやアルゴリズムの拡張を、進めていく。