（革新）様式 1-4-2 (2022-1)

令和４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。

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４年度から令和７年度（4 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　351 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	2	2
	外国出願	0	0
外部発表等	研究論文	2	2
	その他研究発表	35	35
	標準化提案・採択	0	0
	プレスリリース・報道	2	2
	展示会	1	1
	受賞・表彰	1	1

（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) B5G を見据えた新たな要件整理を完了するという目標に対し、サイバー・フィジカルシステムの実例およびセキュリティ課題の基本的な調査を行い、近傍デジタルツインと広域デジタルツインの要件についての基本的な整理が完了した。また、ネットワーク内の通信データから IoT デバイスの識別を行う技術を確立するという目標に対して、フローデータを用いた IoT デバイス識別技術の研究を行い、空間的変化によるモデルの性能劣化(コンセプトドリフト)に対応したデバイス識別モデルの生成技術を開発した。

1-b) セキュリティ対策用デジタルツインに集約するべき情報の要件や、脅威情報の集約後に行うべき対策についてサイバー・フィジカル両方の観点からの検討を完了するという目標に対し、各種サービスのためのデジタルツインにおいて、サイバー空間およびフィジカル空間における複数のセキュリティ機構を統括するメタセキュリティのフレームワークを提案した。

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) IoT 機器の探索や攻撃に起こり得る変化について検討、世界的な研究動向を調査するという目標に対し、検討の結果、IPv6 では NAT 機能が利用されないため多くの機器がインターネットから直接アクセス可能であり、IoT 機器が探索や攻撃の対象となるリスクが明らかになった。また、ミュンヘン工科大学の IPv6 空間のスキャン活動を中心とした調査を完了した。さらに、IoT ハニーポットや IoT マルウェア解析の基盤技術となり得る技術の最新動向を調査し、当該課題への適用可能性を検討するという目標に対し、IoT 機器のネットワークサービスのみを部分的に再現するエミュレーション技術を適用したハニーポット、IoT 機器のファームウェアを解析環境上で動作させるリホスティング技術を適用した解析技術の要件検討を完了した。

2-b) 広域ネットワーク網における異常観測のための要件を調査するという目標に対し、異常検知の高速化において代表とされる手法を中心とした調査を完了した。また、異常検知の対象を広げていくための技術開発を行うという目標に対し、Federated Learning(FL)を用いた複数拠点における異常通信検知技術の研究を行い、いくつかの拠点の学習データに異常通信が含まれている場合でも FL によって検知精度の劣化を防ぐことができることを確認した。

2-c) 公開情報プロファイリング、ローカルプロファイリング、リモートプロファイリングについて調査と要件の検討を行うという目標に対し、調査と要件検討を達成した。具体的には、公開情報プロファイリングの試行として、公開されているマニュアルを用いて約 50 機種の標準設定やセキュリティ機能の有無を調査し、要件を検討した。加えて、ローカルプロファイリングとして、ペネトレーションテストによる実機の調査を行い、要件を検討した。その過程で、6 社の IoT デバイスから計 14 件の脆弱性を発見、IPA に届け出た。また、リモートプロファイリングの調査と要件検討を実施し、Telnet や FTP などのポート情報に加えて、WebUI の情報もプロファイリングに有用との結論を得た。

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）ツリーベースのアンサンブル学習モデルを対象に、IoT 回路の不正回路特徴量を最適化するという目標に対して、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。これらの各モデルに対して、それぞれ 39 個、48 個、32 個、39 個の具体的な不正回路特徴量を見出した。さらに、これらが IoT 回路の不正回路の検知に有効であることを示し、機械学習モデルによる不正回路検知の初期成果を得た。

3-b）フィジカルデバイスレポジトリの構築に向けた基礎設計を行うという目標に対し、フィジカルデバイスレポジトリに登録する情報として、IoT 回路や IoT デバイスに関するセキュリティ観点での管理に必須となる情報を整理し、データベースの基礎設計を完了した。将来的なレポジトリの基本機能の標準化に向けて、国内外の最新の研究動向を調査するという目標に対し、外部システムとの連携に向けて、API の実装に関連する最新の研究動向を調査し、API として必須となる機能の基礎設計を完了した。

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）B5G の具体的なアプリケーションとして、モビリティの九つの型のシステムモデルを設計した。MS（運転者がネットワークから情報も得ず手動で運転する）、MN（運転者がネットワークから補助情報を得ながら手動で運転する）、SS（車載センサにより他車や設置物との接近を検知しアラートや運転制御で運転者を補助する）、これら３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。査読付収録論文２件や収録論文２件など目標をはるかに上回る外部発表を行った。

4-b）今年度実施なし

（8）今後の研究開発計画

以下の表１に示すスケジュールで進める。

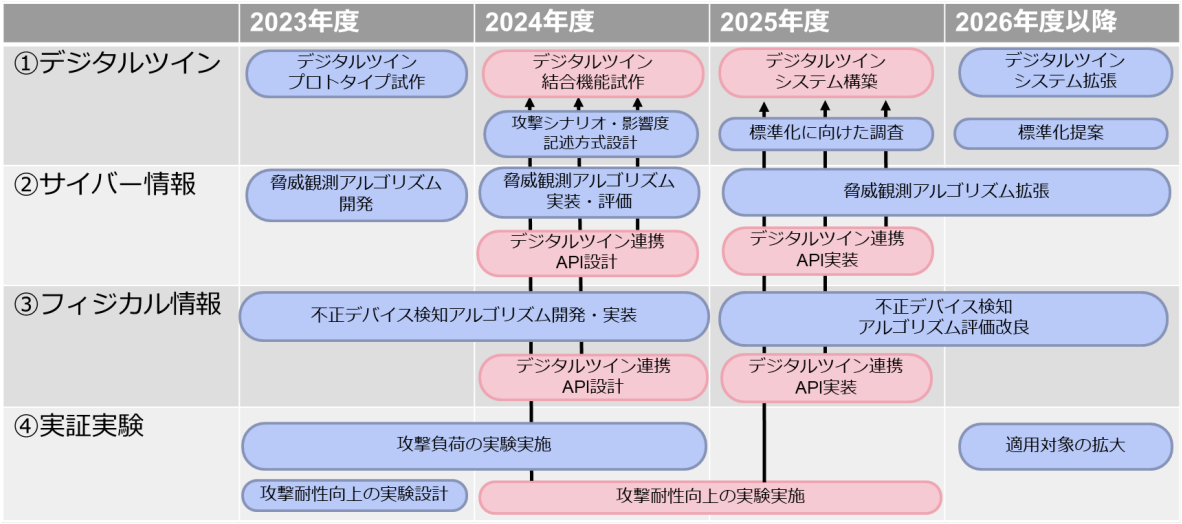

表 1: 研究開発計画

2023 年度はデジタルツインのプロトタイプ施策および、デジタルツインへ入力する脅威情報取得のためのアルゴリズム開発や、実アプリケーションにおける実験実施設計を行う。

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。

終了後の 2026 年度以降も標準化提案、システムやアルゴリズムの拡張を進めていく。