令和5年度研究開発成果概要図（目標・成果と今後の成果展開）

採択番号：05201

1．研究課題・受託者・研究開発期間・研究開発予算

◆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
◆受託者　株式会社KDDI総合研究所、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
◆研究開発期間　令和4年度～令和5年度（2年間）
◆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）

2．研究開発の目標

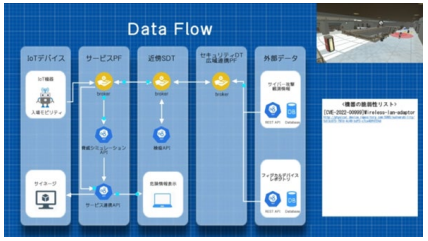
◆サイバー・フィジカル連携型のセキュリティ対策に必要な情報を収集するためのサイバー空間、フィジカル空間双方での観測技術やデバイスプロファイリング技術を確立し、セキュリティ対策の高度化を目的としたデジタルツインを生成する。
◆局所的に観測された攻撃やIoTデバイスの異常な振る舞いをデジタルツインに反映し、広域への影響の分析や的確な対策実施をサポートするサイバー・フィジカル攻撃防御技術を実現する。

3．研究開発の成果

①デジタルツイン生成技術

（研究開発目標）
・B5Gを見据えた新たな要件について調査・検討するとともに、デジタルツイン生成の基礎技術を確立する。
・研究開発項目2, 3, 4との連携の仕様を具体化し、セキュリティ対策用のデジタルツインとしての仕様策定を完了させる。

（2年間の成果）



デジタルツイン連携基盤のプロトタイプを開発。各研究開発項目の成果を活用したセキュリティ対策仕様を策定した。

1-a) デジタルツイン生成技術
1-b) 次世代IoTサイバー・フィジカル攻撃防御技術
2-b) 次世代IoT広域観測技術

②ネットワーク探索・観測技術

（研究開発目標）
2-a)次世代IoT近傍観測技術
2-c)次世代IoTデバイスプロファイリング技術

技術動向等の調査に基づく要件検討を実施し、設計方式を定め方式を検討する。

（2年間の成果）
2-a) IPv6空間探索と実機調査により、インターネットからアクセス可能な多数のIoT機器を検出した。また脅威情報の観測技術とマルウェア解析技術の方式検討を完了し、実装を前倒して行い、実際に攻撃を観測・分析することで攻撃活動の実態を明らかにした。
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・要件検討と、方式の基礎検討を完了。さらにデータ連携を見据えて保存すべき情報を精査した。

③フィジカルデバイス異常検知技術

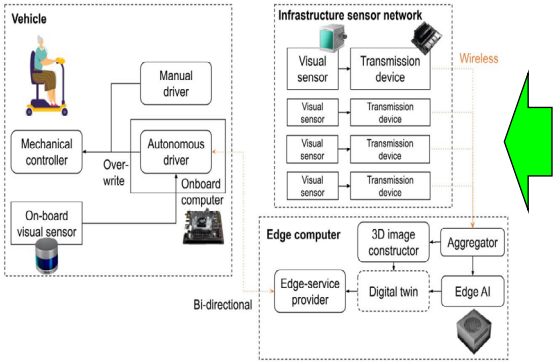
フィジカルデバイスの不正検知技術とレポジトリの構築

（研究開発目標）
③では、フィジカルデバイス不正検知技術を研究開発し、これをベースにフィジカルデバイスレポジトリを構築する。

（2年間の成果）
3-a）では、機械学習によるIoT回路の不正検知技術、IoTデバイスの不正動検知のフレームワークを構築した。
3-b）では、製品情報と脆弱性情報を管理する「フィジカルデバイスレポジトリ」の基礎機能とAPIの実装を完了した。

3-a)フィジカルデバイス不正検知技術、3-b)フィジカルデバイス不正検知技術

④セキュリティ基盤の実証



（2年間の成果）
4-a）セキュリティ攻撃負荷実験
・モビリティを対象に、九つの型を網羅するシステムモデルを設計
・MS、MN、MD、SS、SN、ASの型について実験システム構築・セキュリティ攻撃負荷実験を完了

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
・MS、MN、SS型に対しての実証実験の仕様策定を完了
・Aの実験で得た実データに基づいてセキュリティ攻撃を受けた際の走行データをシミュレーションし、経路予測が可能なことを実証

4. 特許出願、論文発表等、及びトピックス

国内出願	外国出願	研究論文	その他研究発表	標準化提案・採択	プレスリリース 報道	展示会	受賞・表彰
4 (2)	0 (0)	10 (8)	99 (64)	0 (0)	3 (1)	2 (1)	6 (4)

※成果数は累計件数、( )内は当該年度の件数です。

(1)標準化を見据えてNICT統合ビッグデータ研究センターとの連携を開始
本セキュリティ基盤におけるデジタルツイン連携のアプローチとして、NICT統合ビッグデータ研究センターの提唱するデジタルツインオーケストレータの適用に関する検討を開始するとともに、ITU-T等でユースケースの標準化を行う方向で同センターと議論を進めている。

(2)「am I infected?」の、NOTICE連携開始、およびMCPC award受賞
本研究のデータを活用しているWebサービス「am I infected?」の、総務省・NICT「NOTICE」プロジェクトとの外部連携を開始した。また同サービスが、MCPC award 2023 サービス＆ソリューション部門 優秀賞を受賞した。

(3)研究のための不正なIoT回路生成フレームワークを構築完了
IoT回路の不正検知技術において、検知対象となる不正なIoT回路そのものを、強化学習によって生成するフレームワークを構築した。同フレームワークを用いて、研究用の、より識別難度の高い不正回路の生成が可能となる。

(4)日本機械学会と、本研究の提案アーキテクチャに関する意見交換を実施
自動車やIoTのセキュリティの専門家との意見交換会を開催し、本研究の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に関する、産業視点での議論を行った。

5. 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、2024年度以降の下記計画事項を、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。

◆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。