令和4年度研究開発成果概要図（目標・成果と今後の研究計画）

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7年度（4年間）
◆研究開発予算（契約額）　令和4年度351百万円

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

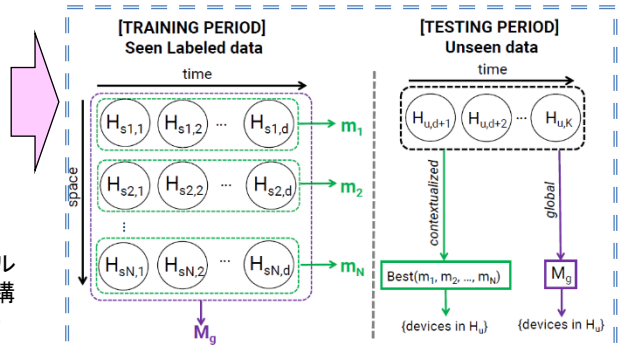
①デジタルツイン生成技術

A　デジタルツイン生成

フローデータを用いた軽量なIoTデバイス識別技術としてコンセプトドリフトへの耐性を有した機械学習方式を提案

B　次世代IoTサイバー・フィジカル攻撃防御技術

サイバー空間およびフィジカル空間における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



②ネットワーク探索・観測技術

A　次世代IoT近傍観測技術

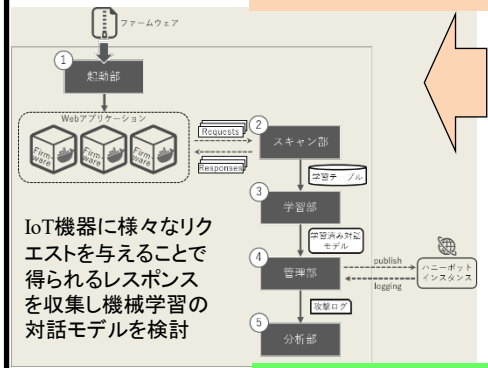
IoT機器のNWサービスを模擬したハニーポット構築技術を開発

B　次世代IoT広域観測技術

教師なし学習による異常検知に連合学習を用いることで、学習データに異常が混入したときの学習モデルの性能劣化を軽減

C　次世代IoTデバイスプロファイリング

約50機種のマニュアルから機器のデフォルト設定やセキュリティ機能の有無をプロファイリング可能であることを確認



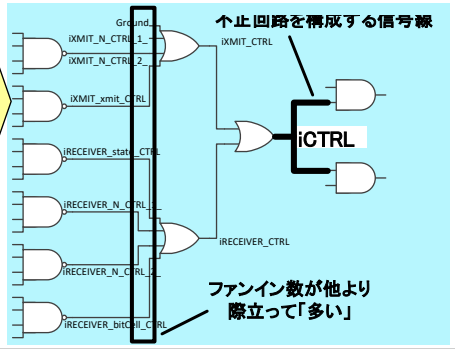
③フィジカルデバイス異常検知技術

A　フィジカルデバイス不正検知技術

4種類のツリーベースのアンサンブル学習モデルに対して、各々約40個の具体的な不正回路特徴量を発見し有効性を確認

B　フィジカルデバイスレポジトリ構築・連携技術

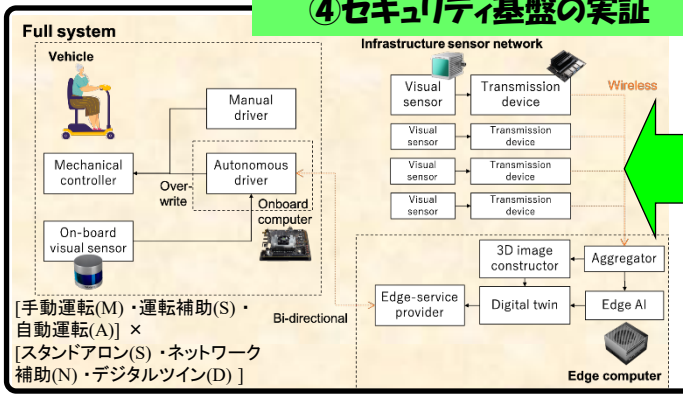
登録情報としてセキュリティ観点で管理に必須の情報を、基本的機能として利用者管理機能、製品情報管理機能、脆弱性評価情報管理機能に整理し基礎設計を完了



④セキュリティ基盤の実証

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
・今年度対象の型(MS, MN,SS)について実験システム構築・セキュリティ攻撃実験設計を完了



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
2 (2)	0 (0)	2 (2)	35 (35)	0 (0)	2 (2)	1 (1)	1 (1)

※成果数は累計件数、( )内は当該年度の件数です。

(1)メタセキュリティフレームワークの提案
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し、包括的なセキュリティソリューションを提供するメタセキュリティのフレームワークを提案し、論文投稿した。

(2)IoTデバイスプロファイリング技術の活用を開始
IoTデバイスに対するペネトレーションテストによるローカルプロファイリングを実施し、6社のIoTデバイスから計14件の脆弱性を発見し、IPAに届け出た。その内4件が修正され、CVE番号が発行された(CVE-2022-37406/CVE-2023-22370/CVE-2023-22375/CVE-2023-22376)。

(3)フィジカルデバイスレポジトリの設計、基礎技術の開発を完了
不正回路を表す特徴量を体系化し、さまざまなツリーベースのアンサンブル学習モデル(ランダムフォレスト、XGBoost、LightGBM、CatBoost)についてIoT回路の不正回路特徴量を最適化した。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デバイスの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。

(4)日本機械学会の企画として「機械のセキュリティ」に関する討論会を実施
自動車やIoTのセキュリティの専門家からなる講師陣による講演およびパネルディスカッションを行った。今後も今回の講師陣を中心に定期的に議論を行っていく予定であり、常に世界の最新の情報を収集し、柔軟に計画をアップデートできるよう備えている。

5. 今後の研究開発計画

研究開発項目1については、今年度提案したフレームワークや調査結果に基づいて、セキュリティ対策用デジタルツインに必要な機能の実装を進めていく。2023年度には研究開発項目2, 3, 4との連携仕様の具体化を進め、2024年度にプロトタイプを試作、2025年度は機能のブラッシュアップを行う。
研究開発項目2について、今年度先行的に実施したプロトタイピングと試行実験の結果に基づき、来年度目標である各技術の設計と具体的な方式検討を行う。2024年度にプロトタイプ実装・評価、2025年度は性能向上を行う。
研究開発項目3について、2023年度までにフィジカルデバイスレポジトリの基礎実装を完了させる。2024年度にはフィジカルデバイスレポジトリに登録された情報の活用や外部連携に向けた実装に着手し、2025年度までに、研究開発項目1や研究開発項目4との連携に向けた、外部連携APIの実装を完了させる。
研究開発項目4について、2022年度はモビリティ区分の9つの型のうち3つの型のみを対象にした。2023年度以降ですべての型をカバーし、負荷の影響と負荷耐性の向上を示す。