令和6年度研究開発成果概要図（目標・成果と今後の研究計画）

採択番号：08101

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）KDDI総合研究所、（大）横浜国立大学、（学）早稲田大学、（学）芝浦工業大学
◆研究開発期間　令和6年度～令和7年度（2年間）
◆研究開発予算（契約額）　令和6年度100百万円

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。

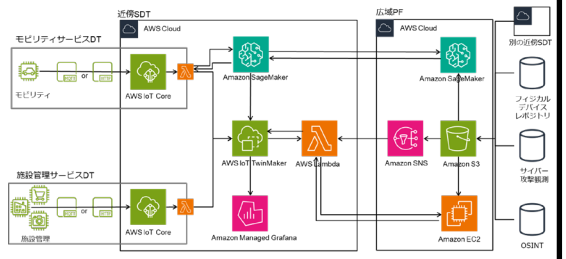
3．研究開発の成果

①デジタルツイン生成技術

（研究開発目標）

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
→広域連携を含めてデジタルツインAPIの基礎実装を完了させ、セキュリティ対策に活用できるようにする

（成果）



セキュリティ用デジタルツインシステムの基礎実装を完了し、対策シナリオでの動作を確認した

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

脅威情報観測技術、マルウェア解析技術、プロファイリング手法を実装し、観測網の拡張と性能評価を実施する。

（成果）

2-a) ISP回線を用いて実機のIoT機器を用いた観測技術を拡張した。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した。IoTマルウェアに搭載された他者を妨害する機能を調査する仕組みを動的解析システムに実装した。さらに、実検体を用いて妨害機能の実態調査を行った。
2-c) 3種類のプロファイリング手法を実装し、数種類のIoTデバイスを用いて試験運用を行い、性能評価を実施した。また、IPv6環境でもプロファイルの有効性を確認。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、約13万ユーザを診断した。

③フィジカルデバイス異常検知技術

（研究開発目標）

3-a）フィジカルデバイス不正検知技術

- ネットの特徴量に基づく機械学習ベースの不正回路検知技術を確立
- 正常波形と異常波形とが識別可能な形状距離を設計

3-b）フィジカルデバイスレポジトリ構築・連携技術

- フィジカルデバイスレポジトリの外部連携を念頭に、国内外の研究動向調査

（成果）

3-a）フィジカルデバイス不正検知技術

- 複数のアンサンブル学習モデルを組み合わせることで、高い不正回路検知技術を確立。さらにグラフ学習の可能性を確立。
- 形状距離で波形の識別技術を確立。

3-b）フィジカルデバイスレポジトリ構築・連携技術

- 文献を調査し、表記ゆれ処理を課題として抽出。表記ゆれを考慮した検索機能を実装し、クラウド上での動作検証を完了。

④セキュリティ基盤の実証

（研究開発目標）

■ 4-a)にて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の取得
  - 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)にてMS、MN、SS型に対して実証実験を行い定量的結果の取得
  - 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

4-a)セキュリティ攻撃負荷実験
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

（成果）

■ 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、定量的な結果を取得
■ 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、定量的なデータを取得
■ 専門家だけでなく一般的な技術者に広く読まれている査読付技術雑誌IEEE Security & Privacy Magazineに論文が採録・出版

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)	4 (4)	49 (49)	3 (3)	0 (0)	0 (0)	3 (3)

※成果数は累計件数、（ ）内は当該年度の件数です。関連課題(05201)における令和６年度成果を含みます。

① デジタルツインのユースケースに関する、ITU-T技術報告書の標準化提案・採択
- 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。

② プロファイリングを活用したセキュリティ診断サービスが高い評価を得た
- 当該サービスに関する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(発表は2025年8月）。

③ IoT不正技術の検出で国際会議最優秀論文賞、他
- 国際会議IoTSMS 2024（International Conference on Internet of Things: Systems, Management and Security 2024）にて、Best Paper Awardを受賞。
- フィジカルデバイスレポジトリにおける外部連携に関する知財「検索装置、検索方法及び検索プログラム, 特願2024-203642」を出願。

④ 広範囲な読者層を持つ技術雑誌への論文採録
- 研究開発項目4について、専門家だけでなく一般的な技術者に広く読まれている査読付技術雑誌 IEEE Security & Privacy Magazine に論文が採録・出版された。

5. 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。