

日本ーインド 国際共同研究拠点「ICT 領域」 平成 30 年度 年次報告書	
研究課題名（和文）	安全な IoT サイバー空間の実現
研究課題名（英文）	SECURITY IN THE INTERNET OF THINGS SPACE
日本側研究代表者氏名	岡村 耕二
所属・役職	九州大学サイバーセキュリティセンター・教授/センター長
研究期間	平成 28 年 10 月 1 日～令和 3 年 9 月 30 日

1. 日本側の研究実施体制

氏名	所属機関・部局・役職	役割
岡村 耕二	九州大学・サイバーセキュリティセンター・教授	代表 (PI)、WP5 リーダー
久住 憲嗣	九州大学・大学院システム情報科学研究所・准教授	WP1 リーダー
小出 洋	九州大学・情報基盤研究開発センター・教授	WP1 メンバー
鄒 天翔	九州大学・大学院システム情報科学府・修士 2 年生	WP1 メンバー
井上 弘士	九州大学・大学院システム情報科学研究所・教授	WP2 リーダー
谷口 倫一郎	九州大学・大学院システム情報科学研究所・教授	WP2 メンバー
小野 貴継	九州大学・システム LSI 研究セン	WP2 サブリーダー

	ター・准教授	
園山 泉紘	九州大学・大学院システム情報 科学府・修士2年生	WP2 メンバー
アラムサラー ガディ エール	九州大学・大学院システム情報 科学府・修士2年生	WP2 メンバー
櫻井 幸一	九州大学・大学院システム情報 科学府・教授	WP3 リーダー
フォン ヤオカイ	九州大学・大学院システム情報 科学府・助教	WP3 メンバー
ダニロ ヴァスコン セロス ヴァルガス	九州大学・大学院システム情報 科学府・助教	WP3 メンバー
ス ジャウエイ	九州大学・大学院システム情報 科学府・博士3年生	WP3 メンバー
金子 晃介	九州大学・サイバーセキュリティ センター・准教授	WP4 リーダー
岡田 義広	九州大学・附属図書館・教授	WP5 リーダー
石 偉	九州大学・附属図書館・助教 助教	WP5 メンバー
アラー モハメッド	九州大学・サイバーセキュリティ センター・テクニカルスタッ フ	WP6 メンバー
ポムケオナ サヌパ ーブ	九州大学・大学院システム情報 科学府・博士2年生	WP6 メンバー
アリエル ロドリゲス	九州大学・大学院システム情報 科学府・修士2年生	WP6 メンバー

2. 日本側研究チームの研究目標及び計画概要

平成 30 年度は、研究開発してきた要素技術をワークパッケージ (WP) 内、あるいは WP 間で統合し、IoT 空間の安全化に具体的に貢献できるビジョンを示し、その実用化を視野に入れて企業連携にも取り組む。WP1、WP2 はそれぞれ WP 内で研究開発してきた「IoT システム開発支援技術」「セキュアかつ省電力実行環境開発支援」「攻撃検知手法」「イベントモニタリング」「機械学習アルゴリズムの活用手法」を統合し、セキュア・省電力な IoT システム開発支援法、IoT システムの異常検知手法を実現する。WP3 はより進んだ脅威情報やその検知などの対処法をプロジェクト全体に提供する。WP4 は、具体的なアプリケーションのプロトタイプの開発に着手する。教育を担当する WP5、WP6 は、これらの WP1-4 により

開発される具体的な安全な IoT システムを対象にした、その利用者・管理者を教育するための教育システムの開発を行う。さらに連携して安全な IoT システム運用・利用の教育コースの開発を行う。このように WP1-6 で、IoT システムを安全にするための手法を具体的に提示する。

これまでは、スマートビルディングを想定した研究を進めてきたが、今後は具体的な IoT 機器・システムへの対応を行い、研究結果をわかりやすく提示できるよう努める。特に、IoT 機器を扱う WP1-2、セキュリティ技術を扱う WP3、インフラを含むアプリケーション・システムを扱う WP4、教育を扱う WP5-6 を統合した具体的な IoT システム、例えば、電力会社と家庭で電力とクレジット（仮想通貨）が交換される電力グリッドを統合的に安全に設計、運用、利用できる設計・開発から運用・利用教育・研修の提案など、本国際プロジェクトの貢献をわかりやすく提示する。さらに、研究成果を元に企業との連携に努め、これらの活動を研究代表者のリーダーシップにより取り進める。

3. 日本側研究チームの実施概要

研究面

WP1 は、ドメイン特化モデリング言語を用いて、セキュリティ、プライバシー要件を満たさなくなると実行できなくなる機能を持つ IoT デバイス用のモジュールを開発可能とする開発環境のプロトタイプを開発した。WP2 は、マイクロプロセッサチップが提供するパフォーマンス・モニタリング・カウンタ (PMC) の情報を、人工知能を用いて、特徴量を抽出し、プログラムの実行時にプロセッサが脅威を動的に検出できる機能の開発を行った。WP3 は IoT での脅威検知技術を軽量化するために深層学習画像分類技術に基づく IoT 環境での軽量なマルウェア検知システムを開発した。また、ワークショップを通じて脅威情報やその検知などの対処法をプロジェクト全体に提供した。WP4 は、ブロックチェーン技術を利用した安全な IoT フレームワークを実現するために、IoT に適したブロックチェーンの改良を行った。そのために、ブロックチェーンのデータサイズが肥大化する問題を解決する技術、IoT 環境において安全に分散計算を行える技術、さらに、ブロックチェーンに利用されている合意形成アルゴリズムについて、IoT に合わせた軽量なアルゴリズムの開発を行った。WP5 では、他の WP の研究成果を逐次反映した教材開発を進めた。そのため、IoT 脅威情報の素材データを蓄積・管理するデータベースのデータを教材として統合表示するオーサリングシステムを開発した。さらに LA(Learning Analytics)を可能とするウェブ教材閲覧システムや IoT のシリアスゲーム教材の開発を行った。WP6 では、サイバーセキュリティ演習装置で、IoT セキュリティについて短時間で教育可能な演習コース、効率的な自学を行うために IoT デバイスの仕様書などから選択式の小テスト問題を自動的に作成する技術を開発した。さらに、スペシャリストの教育としてペネトレーションテストに新たに注目し、IoT システム全体のペネトレーションテストを行えるツールの開発を行った。研究代表者が中心となって、WP 1-2 では、異常検知可能なセキュア・省電力 IoT システム開発支援法で開発される IoT デバイスを用い、WP4 ではブロックチェーンによるインフラで、従来のスマートビルディングの開発のサブセットとして、電力とクレジットを交換できるシステムを、WP3 の知見に基づいて安全に行えるシステムとその管理・利用のための教育についての取り組みを始めた。また WP5-6 の研究成果を用いてこのシステムの仕様から安全安心な導入・運用教材にも取り組み始めている。

交流面

2018年6月にインド工科大学デリー校より Kolin Paul 教授、7月に Sanjiva Prasad 教授が、九州大学に中期滞在し、その間に関連する WP での共同研究打ち合わせに加えて、九州大学大学院システム情報学府で、集中講義を行った。これによって、本プロジェクトに参加していない九州大学の大学院生がインド工科大学の教授から九大の講義では得られない知見を得ることができた。なお、九大での Paul 教授、Prasad 教授による講義の様子は、ビデオで録画し、WP5 によってビデオ教材としてアーカイブされ、九州大学サイバーセキュリティセンターのホームページにて、SICORP メンバーに公開されている。また、本研究の主な対象である IoT と 5G に密接な関係があることを強く認識し、2018年9月にデリーで開催された合同ワークショップのサブテーマを「5G and IoT Security」と設定し、インド側で 5G に先進的に携わっているインドの屈指の ICT 企業である TCS (TATA Consultancy Service)、インドの通信機器メーカーである Tajas Network、5G の世界標準の規格で最先端である Huawei から講演者を呼び、さらには、日印の有識者によるパネルディスカッションも行われた。その結果、インドにおいて世界規模で先端的な 5G、またそのセキュリティに関するワークショップを開催することができ、日本側のメンバーも多くの 5G 研究者、技術者との交流ができた。