日本―インド　国際共同研究拠点「ICT 領域」 2019 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	2016 年 10 月 1 日　～　2021 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)、WP6 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院・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 サブリーダー
馮　皓	九州大学・大学院システム情報科学府・修士 1 年生	WP1 メンバー
小野 貴継	九州大学・システム LSI 研究センター・准教授	WP2 リーダー
井上 弘士	九州大学・大学院システム情報科学研究院・教授	WP2 メンバー
谷口 倫一郎	九州大学・大学院システム情報科学研究院・教授	WP2 メンバー
谷本 輝夫	九州大学・情報基盤研究開発センター・助教	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・博士 1 年生	WP2 メンバー

山方 大輔	九州大学・大学院システム情報科学府・修士 1 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研究院　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研究院　助教	WP3 サブリーダー
ヴァルガス ダニロ	九州大学大学院システム情報科学研究院　助教	WP3 メンバー
蘇 佳偉	九州大学大学院システム情報科学研究院　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
堤　優亮	九州大学・大学院システム情報科学府・修士課程 2 年	WP4 メンバー
秋山　仁志	九州大学・大学院システム情報科学府・修士課程 2 年	WP4 メンバー
馬　立茂	九州大学・大学院システム情報科学府・修士課程 2 年	WP4 メンバー
上拾石　弥生	九州大学・大学院経済学府・修士課程 1 年	WP4 メンバー
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	WP5 メンバー
芳賀 瑛	九州大学・附属図書館・助教	WP5 メンバー
高 天浩	九州大学・大学院システム情報科学府・修士 2 年	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 3 年生	WP6 メンバー
ピユシュ ガーシヤ	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・博士 1 年生	WP6 メンバー
謝 文	九州大学・大学院システム情報科学府・修士 2 年	WP6 メンバー
王 依依	九州大学・大学院システム情報科学府・修士 1 年	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

IoT デバイスやデータなどの研究の面では、これまでプロトタイプとして試作してきた IoT を網羅的にセキュアにする数々の基本的な技術を対象に、また、教育面では、IoT に携わる人間のための教材を対象に、それぞれの評価を行い、精度を上げる。そのために、よりセキュアで省電力なソフトウェアシステムの構築および、異常検知フレームワークをさらに改良・発展させることを目指す。さらに、IoT 環境での軽量かつ有効な攻撃検知法の改良お

よび性能評価を行い、IoT セキュリティのフレームワーク及びアプリケーションのさらなる研究開発を進める。SPOC 教材を用いた教育実践を行い、開発した SPOC 教材コンテンツを素に MOOC 教材の開発を実施する。また、サイバー演習を国際的に実施し、演習を行う上で必要な予習用の問題のより適切な自動生成技術の研究を進める。研究活動の結果は日印共同で論文として成果を発表する。さらにこれらの成果を基にして具体的な企業連携を目指す。

3. 日本側研究チームの実施概要

研究面

WP1 は、従来開発を進めてきたドメイン特化モデリング言語、コード生成器、実行環境を拡充した。エンドユーザがセキュリティやプライバシー保護要求を簡便に設定できる言語を定義し、提案言語を記述するための開発環境を構築した。また、生成されるコードに実行するデバイスに関する電力モデルを組み込むことにより、電力を考慮した事前検証が可能になり、省電力なソフトウェアシステムを構築した。さらに、IoT 実行環境において攻撃を検知して対処するべく、攻撃検知と脅威トレース手法を提案した。WP2 は、アーキテクチャレベルでのセキュリティバイデザインによるセキュリティ対策の研究を行っているが、2019 年度はプログラムの実行中にマルウェアであることを検出するオンライン検出手法の開発を実施した。本研究で開発したオンライン検出は、継続的にプログラムを監視するためにプログラム実行中に複数回のプロセッサに搭載されたパフォーマンスモニタリングカウンタチェックポイントを設け、カウンタの値に基づき機械学習により判定を行うものである。2019 年度は、オンライン検出を行うにあたり適したチェックポイント間隔の調査など、多角的に有効性を調査した。WP3 は、IoT システムに向けて軽量かつ有効な検知法の研究開発、SDN 環境での有効な攻撃検知法の研究開発、IoT マルウェアの分類法の研究開発を行った。WP4 は、IoT セキュリティのフレームワークの研究開発、IoT セキュリティのアプリケーションの研究開発を行うとともに、インド企業との連携を模索するための調査に取り組んだ。また、研究開発しているフレームワークを利用して、スマートビルディングなどの Society 5.0 社会を対象としたアプリケーションの研究開発を行った。2019 年度は、スマートビルディングを想定したエネルギーの管理を行うアプリケーションの研究開発を進め、研究途中の成果としてブロックチェーンを利用した電力取引情報のプライバシーを保護する手法の研究を行った。WP5 は、本プロジェクトの研究成果を教材コンテンツに含めた内容の充実を図るべく、本プロジェクトのこれまでの研究成果をまとめたショートビデオの作成を行った。本プロジェクトの研究成果の教材コンテンツ化については継続実施中である。WP6 は、サイバーセキュリティ教育のための e ラーニングコンテンツ(試験問題)作成手法の高度化、ペネトレーションツールに関するインドとの共同研究を進めた。e ラーニングコンテンツ(試験問題)作成手法の高度化では、従来の選択肢形式の問題を、オントロジーを用いて自動生成の効率を高めることに成功している。さらに、新しい教育コンテンツとして、穴埋め形式の問題に注目し、自動生成する研究を行った。ペネトレーションツールに関する共同研究は、昨年度に続き、IoT デバイスシステムを全体的に解析し、システムを通して(End to End, E2E)ペネトレーションテストできるフレームワーク IoT-PEN の研究開発を行った。今後は、IoT-PEN を使った、IoT デバイスシステムの教材について検討を行う予定である。

交流面

2019 年 4 月 18 日から 20 日まで、日本（熊本市）で、日本・インドメンバーによる中間とりまとめのワークショップを開催した。同ワークショップでは、全 WP の主要なメンバーによる各研究成果の共有や、本共同研究の社会への貢献方法などについて議論した。また、若手研究者によるワークショップも並行して行った。さらに、日本国内外から IoT に関連する研究活動を行っている研究者を招聘し、基調講演並びに様々な観点から議論を行った。日印双方の研究者が宿泊形式で行うことで夕食後もセッションを行い、非常に充実したワークショップを開催することができた。

また、日本のメンバーによって執筆あるいは、日印共同執筆による論文を国際会議や論文誌で公開した。