日本―スペイン、ドイツ、トルコ　国際共同研究 「レジリエント、安全、セキュアな社会のための ICT」 2022 年度　年次報告書	
研究課題名（和文）	将来社会を支える次世代 IoT のための有機的レジリエント・セキュア無線ネットワーク
研究課題名（英文）	Organically Resilient and Secure Wireless Networks for Next-Generation IoT Technologies to Serve Future Connected Societies (ORACLE)
日本側研究代表者 氏名	石橋　功至
所属・役職	国立大学法人　電気通信大学・教授
研究期間	2021 年 4 月 1 日～2024 年 3 月 31 日

1．日本側の研究実施体制

氏名	所属機関・部局・役職	役割
石橋 功至	電気通信大学・先端ワイヤレス・コミュニケーション研究センター・教授	セキュアな物理層通信および分散アーキテクチャの提案と解析
石川 直樹	横浜国立大学・大学院工学研究院・准教授	信号形式に基づくセキュア通信技術の研究
佐藤 光哉	電気通信大学・人工知能先端研究センター・助教	分散セキュア無線アーキテクチャの設計

2．日本側研究チームの研究目標及び計画概要

本提案では、計算量に依存せず、安定して高い安全性を実現する次世代 IoT 向けセキュリティ技術を創出することを研究目標とする。本プロジェクトでは、目標達成のために、研究課題を 4 つの技術的ワークパッケージ（以下 WP）に分割し、それぞれについて検討を進めていく。具体的には、WP2:ポスト量子・軽量暗号技術、WP3:セキュアな物理層無線信号処理、WP4:分散セキュア無線アーキテクチャ、WP5:暗号解読法・トレードオフ解析の 4 つを考え、2021 年度上期では WP2、WP3 の動向調査をまず実施し、下期からは両 WP の基礎検討に加え、WP4、WP5 の動向調査を開始する。本課題は無線通信（主に日本側が専門）とセキュリティ（主に欧州側が専門）という両分野の学際的研究の側面を持つことから、初年度ではまず両分野における最先端の研究状況を正確に整理、共有し、チームとして方向性を共有し、長い目で連携効果が最大となることに重点を置く。その上で全ての検討の基盤と

なる基礎検討を行う。

3. 日本側研究チームの実施概要

次世代 IoT システムでは、無線通信を介して様々な情報を伝送し、これらを機械学習によって分析することで、人々にとって有益な価値を創出することが期待されている。このような観点から、2022 年度では、無線通信・機械学習における様々な攻撃に対処可能である次世代 IoT システムを実現するための要素技術について検討を行った。具体的には、4 つの技術的ワークパッケージ（以下 WP）、WP2:ポスト量子・軽量暗号技術、WP3:セキュアな物理層無線信号処理、WP4:分散セキュア無線アーキテクチャ、WP5:暗号解読法・トレードオフ解析について、それぞれ研究開発を実施した。

WP2 では、電気通信大学が中心となり、完全分散型ネットワークを対象とした連合機械学習（DFL: Decentralized Federated Learning)のセキュア化の設計と評価を行い、端末間の信頼度が不明瞭な環境における学習アルゴリズムとして有用であることが示唆される結果を得た。今後は、国際論文誌へ投稿する予定である。また WP2 について横浜国立大学が中心となって、無線物理層から抽出した真性乱数を効果的に活用可能な物理層暗号化技術を提案した。攻撃者が無制限の計算資源を持つ場合であっても、通信の存在自体が第三者に検知されなければ、攻撃リスクを最小限に抑えることができる。提案手法では、検知確率の観点で従来のカオス MIMO と同等の安全性を保証しながら、符号語の生成に必要とされる乱数を大きく削減できること、検出計算量の観点では、従来のセミブラインド検出器に対して計算量を 1/3 程度に抑えられることを明らかにした。これらの成果は米国電気電子学会 Institute of Electrical and Electronics Engineers(IEEE)の Q1 国際誌（IEEE Wireless Communications Letters）に採録された。

WP3 では、主に 2021 年度に引き続き電通電気通信大学が中心となり、セルフリー大規模 MIMO において、従来の正規受信者に対して受信電力を高めるのではなく、盗聴者における信号受信電力を最小化するテンソル分解に基づくプリコーディング手法について検討を進め、ドイツチームと共著で、国際学術論文誌に投稿、出版した。当該論文については、掲載雑誌内にて Popular Article として複数回取り上げられる等、その高い新規性が認められている。また各送信アンテナごとに異なる周波数オフセットをランダムに加えるプリコーディング手法も併せて提案し、国内の研究会にて発表した。本成果は無線通信研究会にて優秀発表賞を受賞している。また、これらの手法に加えて新たに、MIMO 通信路における通信路の時空間相関を利用した認証技術を開発し、計算機シミュレーションにより、上記の提案手法は従来手法と比較して、より高い確率で非正規送信者の検出に成功することを確認した。

WP4 では、電気通信大学が中心となり、差分プライバシを適用した連合機械学習(DP-FL: Differentially-Private Federated Learning)を対象とした設計と評価を行った。今年度成果により、画像分類データセット MNIST と畳込みニューラルネットを用いた分類タスクにより提案方式のベンチマークを行った結果、従来の算術平均に基づく DP-FL と比較して、学習精度を同学習ラウンド数において 20-25 ポイント程度向上できることを明らかにした。サーバ側で有する評価用のデータセットの数や質によって学習特性が左右されるため、これらの構成法の議論が直近の課題となる。また分散アーキテクチャにおける鍵配送に関して、電気通信大学-ジェイコブス大学ブレーメン間で連携の上、ニューラルネットを用いた物理層セキュリティにおけるペア鍵共有のための電力制御方式の検討を行った。計算機シミュレーションにより、提案手法による鍵共有が可能であることを確認した。ここまでの検討は、単一アンテナに基づくものであった。自由度等の問題から鍵共有におけるレート改善に限界があることから、MIMO への拡張が課題となる。

WP5 では、各 WP で開発された物理層セキュリティ技術についてクラメール・ラオの下限(CRLB)を用いた安全性解析を行い、提案手法の有効性の範囲を明らかにした。これらの結

果は各 WP にフィードバックし、次年度さらに検討を進める予定である

これらの成果に加えて、WP4 から WP5 に関する 2022 年度分成果を、広く社会に還元するため、Deliveable2.2 として日欧共同でレポートにまとめ、ウェブサイトに掲載した。

・ Oracle ウェブサイト（報告書・英語）
https://sites.google.com/view/concertjapan-oracle/wps-and-deliverables

今後は、これらの要素技術を統合し、次世代 IoT がシステムとして、どれだけの安全性を達成し、どのような価値を生み出せるかについて議論していく予定である。