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」 2021 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 (ORACLE)
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	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、令和 3 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

令和３年度上期では、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・トレードオフ解析のうち、上期に WP2、WP3 の動向調査をまず実施し、調査結果に基づいて、いくつかの提案を行った。

WP2 では、カオス理論に基づく無線通信技術の動向調査を行った上で、シミュレーションにより検証可能なソースコードを実装し、再現コードを MIT ライセンスのオープンソースソフトウェアとして公開した。

- カオス偏移変調
  https://github.com/ishikawalab/wiphy/blob/master/wiphy/examples/kaddoum2011csk.py
- 差動カオス偏移変調
  https://github.com/ishikawalab/wiphy/blob/master/wiphy/examples/kaddoum2011dcsk.py
- カオス MIMO
  https://github.com/ishikawalab/wiphy/blob/master/wiphy/examples/okamoto2012chaos.py

カオス理論に基づく無線通信技術のうち、送信シンボル系列が正規分布に従う方式については、物理層セキュリティ分野で盛んに研究されている隠蔽通信（Covert Communication）技術の一種であると解釈でき、本プロジェクトで今後提案する方式の競合となる可能性が高い。

WP3 では、信号処理に基づいたセキュアな物理層通信技術について、最新の関連研究動向を調査し、整理した。この調査結果に基づいて、令和３年度下期にかけて、いくつかの新方式を提案・検討した。まず信号形式に基づくセキュアな通信技術として、任意の多変数最適化法を一方向性関数として用いる通信方式を提案した。本方式は、非同期かつ軽量な検出が可能であるため、特に IoT ネットワークや高速移動体通信に適している。また次世代の移動体通信技術として注目されているセルフリー大規模 MIMO におけるセキュリティについても検討を行い、盗聴者が正規通信者に物理的に接近した場合には、物理層のみではセキュアな通信が不可能であることを明らかにした。この課題に対して、正規通信者以外への漏洩を極限まで防ぐビーム設計と、正規通信者が持つ無線通信路の情報から、盗聴者の通信路をおおまかに推定し、機密保持容量を最大化するビーム設計をそれぞれ提案し、より高い安全性が実現可能であることを数値シミュレーションによって確認した。

WP2、WP3 に関する令和３年度分成果を、広く社会に還元するため、Deliveable2.1 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

WP4、WP5 については、令和３年度下期より動向調査を実施し、それぞれ最新の研究動向について整理した。特に WP4 では、主として既存アーキテクチャにおける脆弱性、特にここでは近年注目されている連合機械学習を実現するメッシュ型の無線ネットワークに着

目し、調査を実施した。これらの通信においては、端末内でのローカル学習とその結果の共有を繰り返すため、深層学習の分野で指摘されている Model Inversion 攻撃により、盗聴された学習器より学習に使用したプライベートなデータを推測でき、これが大きな脆弱性となることがわかった。そこで令和 3 年度では、差分プライバシと呼ばれる技術によって、プライバシを保護する連合機械学習について評価を行った。画像データセットである MNIST を畳み込みニューラルネットを用いて学習する環境を想定し、所望プライバシレベルに対する学習結果の特性について評価した。その結果、プライバシレベルが一定以上の場合は、連合機械学習を用いず、各端末内のローカル機械学習を実施した方が学習結果が高精度になり、さらにプライバシ面もクリアできるとの興味深い結果を得た。また、分散型アーキテクチャにおける安全な鍵配送に向けた検討も開始し、学習を用いることで、効率的で安全な乱数生成が可能であるとの初期結果を得た。これらの結果については、今後国際学会などで発表する予定である。