＜年次報告書＞
第 1 年度（2025 年度）
日 ASEAN 科学技術・イノベーション協働連携事業（NEXUS）
日本－ベトナム「半導体」研究領域

研究課題名（和文）	AI-IoMT デバイス向けマルチコア RISC-V CPU 及び AI アクセラレータをベースにしたセキュア AI システムオンチップの実装とその応用
研究課題名（英文）	Implementation of Secure AI System-on-Chip based on Multi-core RISC-V CPU and AI Accelerator for AI-IoMT Devices and Applications
研究期間	2025 年 10 月 20 日～2029 年 3 月 31 日

氏名	所属 部署　役職
範 公可	電気通信大学 大学院情報理工学研究科　教授
Nguyen Van Toan	東北大学 工学研究科　准教授

1. 研究進捗状況と成果

IoT/IoMT 向けの RISC-V ベース・ハードウェアセキュリティを調査し、AI アルゴリズム解析環境（C/Python)と LSI 設計フローを確立した。PPA 最適化： 組込み用から Out-of-Order 構成までを対象に、RVA23 プロファイルと電力・性能・面積（PPA）のトレードオフを解明。

24GHz ドップラーレーダを用いた非接触バイタル計測システムの開発と精度検証を実施。ハードウェア：アナログ 2 段階フィルタにより、微小な呼吸・心拍成分を分離抽出する小型計測系を構築。アルゴリズム： 心拍の高次高調波（第 2～4）の整数比から基本周波数を再構成する「高調波相関手法」を提案。心拍と呼吸が重なる条件下でも高精度な推定が可能。

受動的放射冷却（RC）を統合したフレキシブル熱電デバイスの開発に成功。FTEG（発電）： 厚さ 110μm の RC 層を統合した超薄型構造（2.26mm）を開発。「大気の窓」を利用した放熱により温度勾配を 1.33° C 向上させ、最大 3.51μW/cm² の出力を実現。FTEC（冷却）： RC 層とペルチェ効果を組み合わせたハイブリッド冷却により、同一消費電力で冷面温度を 2.1° C 低下。AI-IoMT SoC の局所冷却への適用を実証。

UEC、東北大、ベトナム諸機関（VNU-HCM 等）間の強固な連携体制を構築。会議・セミナー： キックオフミーティング（2025 年 11 月）のほか、ISET や ICEBA 等の国際会議で成果発表。ベトナムの主要工科大学にて技術ワークショップを連続開催。技術指導： オープンソース EDA ツールを用いたアナログ集積回路設計の集中講義を実施（2026 年 3 月)。共同研究： ホーチミン市工科大学から講師・准教授級の研究者を招聘し、UEC にて共同研究を推進。次世代を担う若手研究者（ECR）の確保と高度教育を加速。東北大学： 博士課程進学予定者 3 名に対し、マイクロ・ナノ加工技術や高性能熱電材料に関する専門トレーニングを開始。電気通信大学： 5 名の ECR 候補者が博士後期課程に入学合格（2026 年 4 月入学)。

2. 代表的な成果事例

1. N. V. Toan, et al., Flexible Thermoelectric Generator with Radiative Cooling for Body-Heat-Driven Self-Powered BLE Sensing System, Sustainable Materials and Technologies, 45, e01640, 2025.
2. N. V. Toan, et al., Flexible Thermoelectric Cooler with Optimized Fill Factor and Radiative Cooling Integration for Energy-Efficient Wearable Thermal Management, *Sustainable Materials and Technologies*, 46, e01742, 2025.
3. P. P. Duong.,et al., Constructing 8x8 S-Boxes with Optimal Boolean Function Nonlinearity. *Cryptography*, *9*(4), 67.
4. Dam, D.-T., et al., Accelerating Post-Quantum Cryptography: A High-Efficiency NTT for ML-KEM on RISC-V. *Electronics*, *15*(1), 100.
5. Nguyen, T. V. H., et al., Design Phase-Locked Loop Using a Continuous-Time Bandpass Delta-Sigma Time-to-Digital Converter. *Electronics*, *15*(3), 675.
6. P. -P. Duong., et al., Dynamic S-Boxes Block Cipher for Side-Channel Attack Resistance, IEEE Access, vol. 13, pp. 198523-198539, 2025.
7. Nguyen, H.-S., et al., Non-Contact Heart Rate Estimation via Higher Harmonic Analysis Using 24-GHz Doppler Radar: Validation in Humans and Anesthetized Cat. *Signals*, *7*(2), 24.