様式 1-4-2 (2020-1)

令和元年度研究開発成果概要書

採 択 番 号　　：19301
研究開発課題名　：スマートコミュニティを支える高信頼ネットワーク構成技術の研究開発
副　　題　　：STEAM：スマートコミュニティを支えるエネルギーとモビリティを対象としたセキュアな高信頼フレームワーク

（1）研究開発の目的

本研究開発では、将来のスマートコミュニティ実現に不可欠な高度交通システムとスマートエネルギーシステムを対象に、安全性と信頼性を担保しながら、エッジコンピューティングでそれらのアプリケーションを実現する高信頼ネットワーク基盤の研究開発を行う。様々な脅威モデルのもとでも、アプリケーション意思決定プロセスの安全性・信頼性保証、および個々のデータプライバシー保護を実現する新しい計算スキームを提唱し、実用性の観点からセキュリティレベルと計算資源のトレードオフ問題を追求する。それらの機能を有するエッジコンピューティングミドルウェア基盤を開発し、アプリケーション実データを利用した都市スケールの有効性評価を行う。

（2）研究開発期間

平成 30 年度から令和 3 年度（3 年間）

（3）実施機関

国立大学法人奈良先端科学技術大学院大学＜代表研究者＞
学校法人早稲田大学
国立大学法人大阪大学

（4）研究開発予算（契約額）

総額　45 百万円（令和元年度 15 百万円）
※百万円未満切り上げ

（5）研究開発項目と担当

研究開発項目１：不確実性に対し堅牢かつ安全な意思決定方式の開発（参考）
1．異常検知技術（ミズーリ工科大学）
2．信頼モデル構築技術（ミズーリ工科大学）
3．意思決定モデル構築技術（ミズーリ工科大学）

研究開発項目２：プライバシー保護計算機構の開発
1．表探索によるプライバシー保護計算技術（早稲田大学）
2．範囲検索の実現技術（早稲田大学）
3．FHE および差分プライバシーによる異常検知技術（早稲田大学）

研究開発項目３：セキュリティ・プライバシーレベルと計算資源のトレードオフ解析（参考）
1．プライバシー制約のもとでの閾値決定手法（ヴァンダービルト大学）
2．動的状況のもとでの閾値決定手法（ヴァンダービルト大学）
3．暗号化を要するセンサーデータの決定手法（ヴァンダービルト大学）

研究開発項目４：統合ミドルウェア基盤の設計開発研究開発
1．「地産地処」分散計算と集約機構（奈良先端科学技術大学院大学）
2．通信と集約処理における匿名化機構（奈良先端科学技術大学院大学）
3．トレードオフを考慮した意思決定機構（大阪大学）

研究開発項目５：スマートコミュニティ応用事例による評価

１　マルチモーダル経路計画への応用と評価（大阪大学）

２　トランザクティブ・エネルギーへの応用と評価（ヴァンダービルト大学）

（6）特許出願、外部発表等

		累計（件）	当該年度（件）
特許出願	国内出願	0	0
	外国出願	0	0
外部発表等	研究論文	1	0
	その他研究発表	12	8
	標準化提案	0	0
	プレスリリース・報道	0	0
	展示会	0	0
	受賞・表彰	1	1

（7）具体的な実施内容と成果

研究開発項目２：プライバシー保護計算機構の開発

2-1．表探索によるプライバシー保護計算を実現するため、任意の関数計算を表探索に置き換え、完全準同型暗号により暗号化された入力値をもとに関数の計算結果を表探索（表は関数毎に予め用意されているとする）により探索し、暗号化された計算結果を返すプログラムを開発した。昨年度開発した１入力関数を拡張し２入力関数への対応を行った。約 160 万個のエントリを持つ１入力関数に対して６秒、約 6700 万個のエントリを持つ２入力関数に対して３分での高速処理を実現し、電力を対象とした異常検知（数十分毎に検知を想定する場合）への適用可能性を示した。

2-2．範囲検索の実現を行うために、まず２つの暗号データ（A,B）に対して大小関係の結果を暗号化された１（A≧B の時）あるいは０（A＜B の時）を返す仕組みについて検討し、プログラム構築を行った。さらに、表探索をする上で、補間された値と真の値との間の誤差を小さく抑える手法について検討を行った。なお、表計算を用いずに異常検知を行う手法についても検討を行い、研究開発項目１－１のプログラム上でのインプリメントを進めた。

研究開発項目４：統合ミドルウェア基盤の設計開発研究開発

4-1．「地産地処」分散計算と集約機構においては、エッジコンピューティング環境において動作するセキュアで信頼できるミドルウェアアーキテクチャの機能要件を整理し、スマートモビリティならびにスマートエネルギーアプリケーションに資するミドルウェアの設計開発を行った。具体的には、遅延を抑制しながらデータ集約を実現する機構、計算リソースや推定実行時間をプロファイリングする機構、ならびにそれをベースに分散したエッジノードに柔軟に割り当てるタスク割当機構を開発した。

4-2．通信と集約処理における匿名化機構と 4-3．トレードオフを考慮した意思決定機構においては、エッジコンピューティング環境においてプライバシーを保護しながらデータ送信・集約する手法に関する検討を行った。具体的には、データの k-匿名性を基にデータ送信におけるユーザの意思決定を支援する手法、エッジでの匿名化処理を適用するデータを一定の予算内に収まるよう取捨選択することでリスクの最小化と利益の最大化をバランス良く行う手法を開発した。

研究開発項目５：スマートコミュニティ応用事例による評価

5-1．マルチモーダル経路計画への応用と評価においては、スマートトランスポートシステムにおける道路利用量に対する経路推定を行う手法を開発した。大阪市を模したシミュレーション環境において、経路計画に必要な経路集合の推定が高い精度で可能であることを示した。

（8）外国の実施機関

ミズーリ工科大学（アメリカ）＜代表研究者＞

ヴァンダービルト大学（アメリカ）