令和2年度研究開発成果概要図 （目標・成果と今後の研究計画）

採択番号：19301

１．研究課題・受託者・研究開発期間・研究開発予算

◆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
◆実施機関　　：国立大学法人奈良先端科学技術大学院大学、学校法人早稲田大学、国立大学法人大阪大学
◆研究開発期間：平成30年度から令和3年度（36か月）
◆研究開発予算：総額45百万円（令和2年度15百万円）

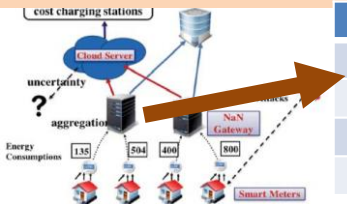
２．研究開発の目標

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。

３．研究開発の成果

研究開発項目２：プライバシー保護計算機構の開発

スマートコミュニティから生成される各種データのプライバシー保護のため、異常検知等の各種計算を暗号化されたデータのままで行う技術



入力	出力
10	1
100	2
200	3
300	4

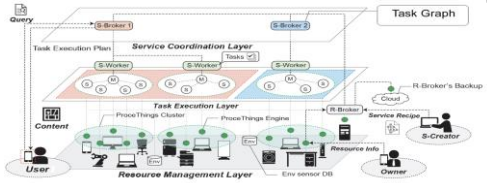
研究開発成果：表探索によるプライバシー保護計算技術

完全準同型暗号で様々な計算（関数）を実現する上では、表探索（Lookup Table）による近似計算結果の探索を効率よく実現することが不可欠。

- ●表探索における範囲探索を実現。これにより、任意の引数に対応。約100万個のエントリを持つ関数に対して4.04秒（8スレッド実行時）での高速処理を実現。
- ●表探索以外の手法として、表を用いずに異常検知を行う手法について、テキサス州200家庭の2014-2016年の電力消費データを用い評価し、暗号化前と同精度で異常検知を10秒間隔で実現できることを確認。

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

スマートコミュニティから生成される各種データの様々な処理をエッジコンピューティング環境でQoSを考慮しながら行うための分散処理技術



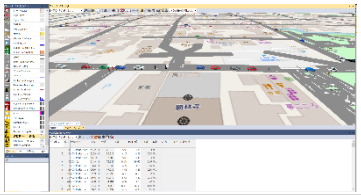
研究開発成果：エッジ環境でのタスク割当とデータ集約・匿名化

スマートコミュニティから生成される各種データを、様々なQoSを保証しながら処理するためには、エッジノードの資源管理、タスクの適切な分割と適切なノードへの割当が不可欠。

- ●秘匿性、整合性および可用性を満たしながらデータを集約する手法として、Private Information Retrieval（PIR）とFHEを組み合わせた経路探索手法を開発。
- ●経路探索において、PIRを適用する地理的範囲、交差点の数を変化させることで、プライバシ保護レベル、計算時間の短さ、計算結果の正確さの3つの指標間のトレードオフを考慮可能な方法を開発。

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

スマートコミュニティ向けのスマートモビリティサービスやアプリケーションの評価のためのモビリティモデル設計と広域モビリティ再現技術



研究開発成果：スマートモビリティ評価のためのモデル開発

スマートコミュニティ向けの広域スマートモビリティサービスやアプリケーションを評価するためには、現実的な車両や人のモビリティモデルと実際の交通状況データセットに基づき再現した広域モビリティの再現技術の開発が不可欠。

- ●現在マルチモーダル交通最適化を図っている自治体と連携し、マルチモーダル経路推定アルゴリズムに基づいた経路決定シミュレーションを実施
- ●現実的な移動モデルを組込んだ交通シミュレータを用い、同自治体の観光地区における実地域の地図を用いた行動シミュレーションを実施し、初期的データを収集。

4. 特許出願、論文発表等、及びトピックス

国内出願	外国出願	研究論文	その他研究発表	標準化提案・採択	プレスリリース 報道	展示会	受賞・表彰
0 （0）	0 （0）	2 （1）	20 （8）	0 （0）	0 （0）	0 （0）	2 (1)

※成果数は累計件数、（ ）内は当該年度の件数です。

本研究開発における基幹技術である表探索によるプライバシー保護計算技術に関する研究成果をIEEEの国際会議ICBDA2020、パワーグリッドを対象とした異常検知手法の提案・実データによる評価結果をIEEEの国際会議SmartGridCommで発表した。また、エッジ分散処理アーキテクチャに関する研究成果を国際ワークショップMUSICAL2021で発表した。さらに、スマートコミュニティアプリケーションである分散経路探索への応用に関する研究成果をIEEEの国際会議ICFC2020、ISORC2020と、IEEEの論文誌Accessで発表した（米国側共同研究者との共著）。また、これらの成果発表を通じ、要素技術の実現に加え、具体的なスマートコミュニティアプリケーションを想定した評価モデルを構築できたと考えている。

5. 今後の研究開発計画

令和2年度は、表探索によるプライバシー保護計算技術（研究開発項目2）、エッジ分散処理ミドルウェアアーキテクチャ（項目4）、スマートモビリティ評価のためのモデル開発（項目5）を昨年度に引き続き実施した。すべての項目において研究開発は順調に進んでおり、それぞれの項目で研究成果を挙げることができた。令和3年度は、それぞれの項目における技術を進展させるとともに、全ての機能を統合したミドルウェアを完成させる予定である。また、外国の実施機関との連携も順調に進んでいる。具体的には、スマートモビリティアプリケーションを実行するミドルウェアの実装と評価（項目4、NAIST）をヴァンダービルト大と実施し、令和2年度に共著論文を3編発表した。また、表探索によるFHE計算（項目2、早稲田大）を用いた異常検知技術（項目1、ミズーリ工科大）の実装と評価、トレードオフ機構（項目3、ヴァンダービルト大）のミドルウェア（項目4、NAIST、阪大）上への実装と評価、評価環境（項目5、阪大、ヴァンダービルト大）の構築と評価について、関連機関で議論を継続しており、令和3年度に共同研究成果発表を見込んでいる。

6. 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）
ウエスタンミシガン大学（アメリカ）