

## 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 : 2018年度～2021年度 (36か月)
- ◆研究開発予算 : 総額45百万円

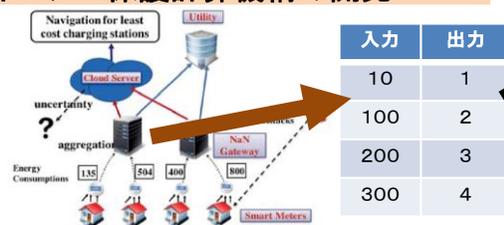
## 2. 研究開発の目標

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



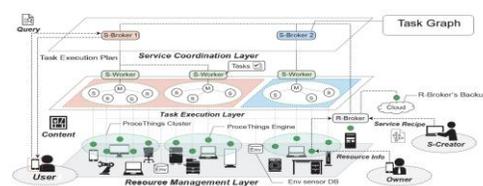
## 研究開発成果: 表探索によるプライバシー保護計算技術

完全準同型暗号で様々な計算(関数)を実現する上では、①当該関数を使わない計算に置き換えるか、②表を用い近似計算結果の表探索に置き換えることが不可欠。両手法を開発し、テキサス州200家庭の2014-2016年の電力消費データを用い、200W/800Wの異常電力消費を検知。パワーグリッドでの異常検知は1時間毎に検知できることが要求条件。

- ①の手法: 異常検知を10秒間隔で実現。平文と同じ検知精度を達成。
- ②の手法: 異常検知を5分間隔で実現。平文とほぼ同じ検知精度を達成。表探索自体は、任意の引数値に対する表探索を実現。

## 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。

- エッジコンピューティングミドルウェア基盤を開発し、分散経路探索を実装・評価。
- 経路探索におけるプライバシー保護機構、さらに、プライバシー保護レベル、計算時間、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。
- モビリティを対象とした異常検知手法を開発。

## 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。

- 現実データに基づく大阪市広域の車両モビリティ再現技術を確認し、同地区の車両データを収集。マルチモーダル経路決定アルゴリズムの評価に活用。
- 実環境の人と車のセンシングデータを用い、兵庫県北部の観光地区における行動シミュレーションを実施し、行動データセットを構築。

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)	3 (1)	23 (3)	0 (0)	0 (0)	0 (0)	3 (1)

※成果数は累計件数、( )内は当該年度の件数です。

- (1) 日米共著論文6編を含む26編の論文(国際論文誌3編、国際会議論文16編)を研究成果として発表
  - ・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(米国側共同研究者との共著)
  - ・エッジ分散処理アーキテクチャに関する研究成果を、IEEE Accessや国際ワークショップMUSICAL2021で発表
  - ・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、SmartComp2021と、IEEEの論文誌Accessで発表(米国側共同研究者との共著)
- (2) 国際ワークショップIEEE BITSを開催(国際会議IEEE SMARTCOMPIに併設)
  - 第1回2019年6月12日、Residence Inn By Marriott Arlington Pentagon City
  - 第2回2020年9月14日、オンライン開催
  - 第3回2021年8月23日、オンライン開催

ワークショップ概要:クラウド/IoT環境におけるセキュリティ、プライバシー、信頼性、回復力、堅牢性を備えた安全なコンピューティングと効率的なデータ管理に関する理論と実装に焦点を当てた論文を募集。2019~2021年に、それぞれ、7編、3編、7編が査読を経て採択。招待講演やパネルディスカッションも含め、スマートコミュニティアプリケーションの安全安心な実現方法について活発な議論が行われた。

5. 研究開発成果の展開・普及等に向けた計画・展望

本研究開発では、FHEを用いたプライバシー保護機構、異常検知や信頼性決定をプライバシー・セキュリティと資源のトレードオフを考慮しながら実現する仕組み、それらを組み込んだミドルウェア基盤を実現した。これらの開発により、エネルギーとモビリティを対象としたスマートコミュニティアプリケーションを安全安心に運用するための基礎技術を確立できたと考えている。内閣府の「スーパーシティ構想」の推進など、今後、都市のスマートシティ化が加速していくと予想される。本研究開発の成果であるミドルウェア基盤を都市OSに組み込む取り組みや標準化についての活動等を通して、本研究開発成果の普及に向けた取り組みを行っていく。5G/B5Gが普及することにより、エッジノード間の通信やFHEの暗号文の通信にかかる時間や安定性が飛躍的に高まり、提案基盤の実用化が進むと考えられる。

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)