平成30年度研究開発成果概要図 （目標・成果と今後の研究計画）

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年度から平成33年度（36ヶ月）
◆研究開発予算：総額45百万円（平成30年度9百万円）

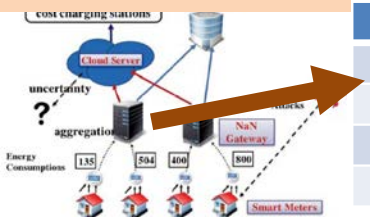
2．研究開発の目標

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

①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

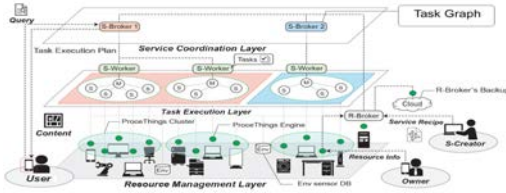
研究開発成果：表探索によるプライバシー保護計算技術

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。

- ●計算コストの大きいビット演算を用いず整数のままで表探索を実現する手法を提案し、従来手法に比較して約150倍の高層化を達成。
- ●表中にない値について近似値を得るための大小比較を実現。これにより（1）扱う整数範囲を限定せず、かつ、（2）比較結果を暗号化したままで後の計算で利用できることを確認。

②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



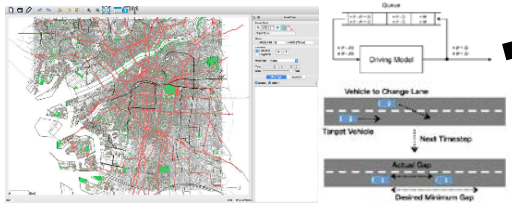
研究開発成果：エッジ分散処理ミドルウェアの初期プロトタイプ

スマートコミュニティから生成される各種データに適用される、研究開発項目1～3の機能を、遅延や帯域に関するQoSを保証しながら実現するためには、エッジノードの資源の管理、タスクの適切な分割と適切なノードへの割当てが不可欠。

- ●資源管理、サービス連携、タスク実行からなるミドルウェアアーキテクチャを設計。
- ●Dockerを用いて初期プロトタイプを実装し、オフィス空間におけるコンテキスト推定・クエリーサービスに応用し、複数エッジノードへのタスクの分散により、クエリー数が増えても応答時間を一定時間内に抑えることが可能なことを確認。

③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。

- ●マルチモーダル経路計画などのサービスをシミュレータ内で実現可能とするための評価プラットフォームを設計。
- ●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て初期プロトタイプを開発。大阪府の実地図と実渋滞データを基にした交通流再現が可能であることを確認。

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	プレスリリース報道	展示会	標準化提案
0（ 0 ）	0（ 0 ）	1（ 1 ）	4（ 4 ）	0（ 0 ）	0（ 0 ）	0（0 ）

※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エッジ分散処理ミドルウェアの研究成果を国際論文誌IEEE AccessおよびIEEEの国際ワークショップIQ2S'19で発表するとともに、スマートコミュニティから生成されるデータのプライバシ保護計算およびその高速化に関する研究成果を国際会議INDOCRYPT2019および電子情報通信学第11回データ光学と情報マネジメントに関するフォーラム（DEIM 2019）で発表した。
これらの成果発表を通じ、他の研究開発項目である、スマートコミュニティアプリケーションにおける異常検知技術（項目１）、セキュリティレベルと必要計算資源のトレードオフ意思決定（項目３）、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の構築（項目５）を実施していくための基礎を確立できたと考えている。

5. 今後の研究開発計画

平成30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。平成31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、項目間の連携を進めていく予定である。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、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、評価環境（項目５、阪大、ヴァンダービルト大）の構築について、関連機関で議論を進めており、平成31年度中に複数の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）