令和３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：03901

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　超多数・多種移動体による人流・物流のためのダイナミックセキュアネットワークの研究
◆受託者　ジャパンデータコム株式会社、学校法人早稲田大学
◆研究開発期間　令和3年度～令和5年度（3年間）
◆研究開発予算（契約額）　令和3年度から令和4年度までの総額100百万円（令和3年度17百万円）

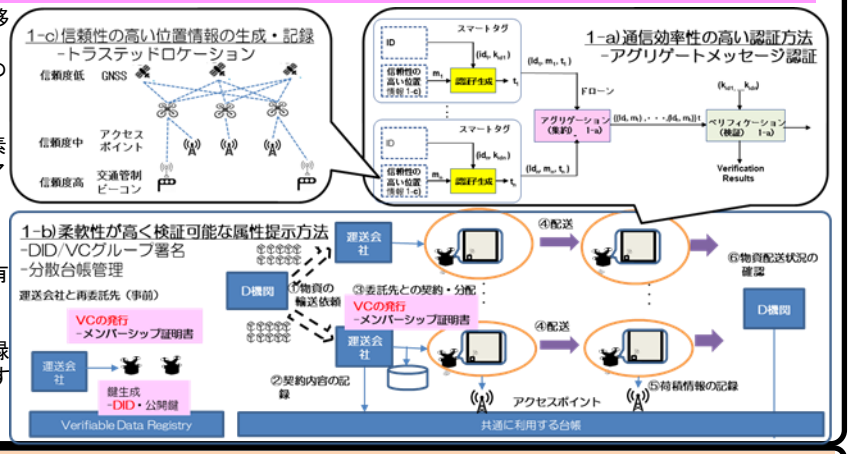
２．研究開発の目標

移動体を高密度、超多数で安全に協調稼働させるための、グリゲートメッセージ認証等によるセキュアかつ高効率な認証、分散台帳による高信頼で柔軟な情報秘匿・共有、高信頼な位置情報の取得等の技術から構成されるセキュリティ基盤技術を開発する。セキュアで広域の高信頼性、超低遅延通信（URLLC）を実現し、現在の5G通信を超える、超高速、大容量、超低遅延、超多数同時接続の機能を活かしたセキュリティ基盤技術を目標とする。

３．研究開発の成果

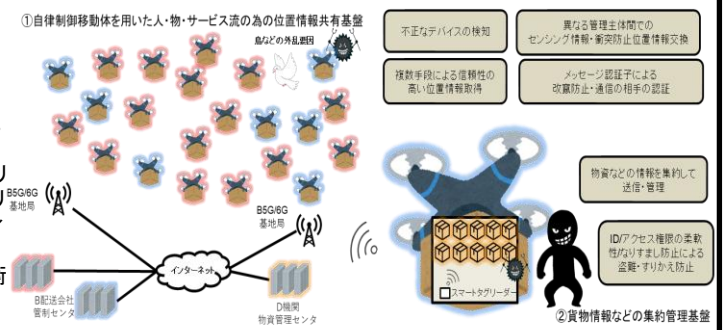
研究開発項目1：ワイヤレス通信の効率的かつセキュアな情報交換方法のための要素技術研究

超多数・多種移動体による人流・物流のためのセキュリティ基盤に求められる3つの要素技術、セキュアかつ高効率な認証技術、高信頼で柔軟な情報秘匿・共有技術、信頼性の高い位置情報の生成・記録技術、を開発する。



研究開発項目2：ソフトウェア・ハードウェア実装に向けた応用研究

複数事業者による多数機同時運航および物流管理に必要とされる研究開発項目1の要素技術から構成されるセキュリティ基盤の研究を行う。また、二つのシナリオ（「移動体の衝突防止のためのシナリオ」「物資管理のためのシナリオ」）を想定したセキュイリティ基盤のプロトタイプをそれぞれ構築し、提案する要素技術を実証する。



研究開発項目1：ワイヤレス通信の効率的かつセキュアな情報交換方法のための要素技術研究

1-a)通信効率性の高い認証方法

（B5Gにおける移動体および搭載物資の認証・制御に必要な情報の高効率な通信方式の実現）

●アグリゲート認証技術による相手認証技術では、適切な対話処理の導入により通信データ量が削減可能、との知見を得た
●デジタル署名に基づくアグリゲート署名技術では、格子構造に基づく構成の拡張としてグループテストアルゴリズムの応用により不正メッセージの特定が可能、との知見を得た

1-b)柔軟性が高く検証可能な属性提示方法

（多種多様な移動体の混在運用で必要となる柔軟性高く検証可能な属性提示方法の実現）

●二人の所有者がそれぞれ所有する2台の移動体にVCを発行し、どの4台の移動体も、第三者に自身の所有者の情報を検証可能な形で提供できる手法を設計した
●所有者情報を第三者に提供した際、第三者が記録する検証ログから、所有者を確認できても、移動体自身は特定できないが、その検証ログを所有者に還元した場合は、所有者は提供した移動体が特定できる方式を調査・検討した

1-c)信頼性の高い位置情報の生成・記録

（移動体群の連携移動に必要な移動体の信頼性の高い位置情報の生成・記録方法の実現）

●近接する実空間移動体へ伝達する情報を生成する技術の方式の調査・試作・評価を行い、簡単な実験において、位置情報の偽装を98%以上検出できる知見を得た
●事故等の検証用の位置情報の記録方法について、改ざん発生ゼロとなる方法について調査・比較により、検証対象構成案を複数抽出した

研究開発項目2：ソフトウェア・ハードウェア実装に向けた応用研究

（想定する二つのシナリオにおける研究開発項目1の要素技術の実証環境の実現）

●二つのシナリオの実現性を検証するユースケースの検討を実施、「移動体の衝突防止のためのシナリオ」については首都高上空に設置された空中交通レーンを飛行する大量のドローンの交通制御、「物資管理のためのシナリオ」については車両とドローンを併用した複数の発送先への大量の物資配送、とした
●上記ユースケースを想定した「衝突防止シナリオに関する実験」、「物資管理シナリオに関する実験」の為のプロトタイプ、および「超多数・超多種接続に関する実験」の為のソフトウェアプロトタイプ（シミュレーションシステム）の仕様（原案）を作成

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
1（1）	0（0）	0（0）	1（1）	0（0）	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。

トピックス：

①本研究で想定するシナリオに適切な通信方式検討のため、複数の通信機器ベンダーへのヒアリングを実施

②本研究で想定するシナリオに適切なシステムモデル検討のため、ドローン物流サービスプラットフォーム事業者へのヒアリングを実施

５．今後の研究開発計画

研究開発項目1：ワイヤレス通信の効率的かつセキュアな情報交換方法のための要素技術研究

1-a）通信効率性の高い認証方法

●アグリゲートメッセージ認証技術による相手認証技術では、検証サーバと移動体との通信の中継サーバの間で対話的処理を行うことにより、中継サーバがカバーするエリア内すべての端末の相手認証に必要なデータ量を従来技術に比べて削減する方式を完成

●デジタル署名に基づくアグリゲート署名技術では、令和3年度に検討した拡張性に関する研究を進め、本課題が想定するシナリオ下における効果的な情報の収集・集約を実現する方式を検討

1-b）柔軟性が高く検証可能な属性提示方法

●令和3年度に検討した移動体による検証可能な属性提示方法について試作を行い、機能検証を実施

●平常時には開示していない移動体を特定する情報を、グループ署名を活用したログから検証可能な方法で提供できる枠組みを検討

1-c）信頼性の高い位置情報の生成・記録

●令和3年度に検討した位置情報の偽装検出方法については、さらに位置情報の信頼性を高める他の手法も加え、試作および評価を実施

●複数の位置計測手段から得られるデータとアクセスポイントの特性、さらに位置計測データの時系列の履歴を用いて「信頼度」を求めるアルゴリズムを開発（位置情報の検証の処理時間は0.04秒以内に収まることを確認）

●令和3年度に抽出した移動体の位置情報の記録手法に対する試作および評価を行い、リスク事象が発生しないことを確認

研究開発項目2：ソフトウェア・ハードウェア実装に向けた応用研究

●「移動体の衝突防止のためのシナリオ」に関する実験

1-cで得られる位置情報の1-aのアグリゲートメッセージ認証を用いて位置情報を共有する方法について、移動体の機能を模擬するデバイス、中継サーバの機能を模擬するサーバで構成される小規模なプロトタイプを構築し実験・評価により、研究開発項目1の提案方式を実証

●「物資管理のためのシナリオ」に関する実験

1-bの検証可能な属性提示方法と1-aのアグリゲートメッセージ認証を用いて、物資に付与されたスマートタグの情報を完全性を担保しながら集約し、検証するための方式について、移動体の機能を模擬するデバイス、中継サーバの機能を模擬するサーバで構成される小規模なプロトタイプを構築して実験・評価を行い、研究開発項目1の提案方式を実証

●「シナリオ①②における超多数・超多種接続」に関する実験

簡易的なソフトウェアプロトタイプを構築して超多数・超多種接続を考慮した実験を行い、シナリオ①②における超多数・超多種接続時においてもシナリオ①の中間目標である片道処理時間が0.04秒、往復応答0.1秒未満、シナリオ①②の中間目標である66%以上の周波数帯域削減効果を達成できる見込みであることを確認