令和5年度研究開発成果概要図（目標・成果と今後の成果展開）

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5年度までの総額130百万円（令和5年度30百万円）

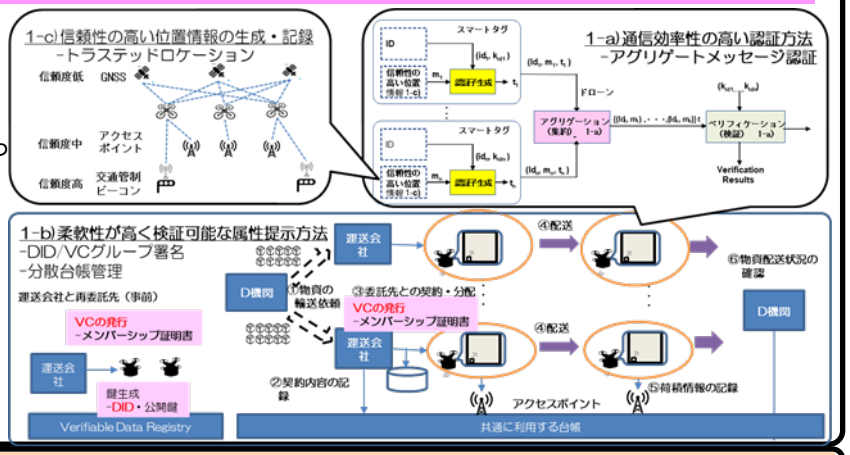
２．研究開発の目標

移動体を高密度、超多数で安全に協調稼働させるための、ア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

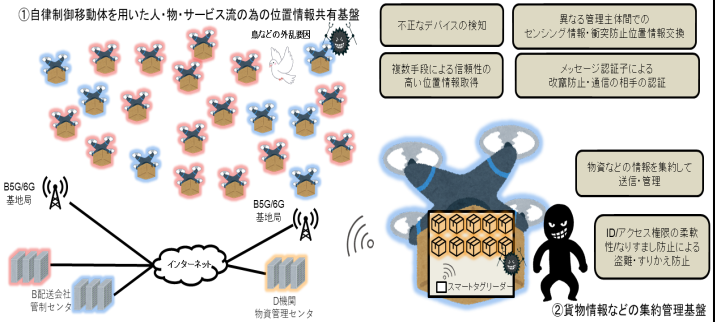
研究開発項目1：ワイヤレス通信の効率的かつセキュアな情報交換方法のための要素技術研究

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）

通信データ量の大幅削減と不正エンティティ特定を同時に実現する以下の技術開発を行った。

●アグリゲートメッセージ認証技術による相手認証技術の構築を目標に、世界で初めての「共通鍵暗号基盤に基づくアグリゲート相手認証技術」を構築した。
●アグリゲート署名技術による相手認証技術の構築を目標に、世界で初めての「公開鍵暗号基盤に基づくアグリゲート相手認証技術」を構築した。

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）

●W3CにおけるDIDとVC方式のフレームワークにVPを活用する基盤を試作。2人の所有者が2台の移動体を所有する物資管理シナリオとして柔軟性高く検証可能な属性提示方法を実現
●概念実証（PoC）では、シナリオに対して、偽造された属性や古い属性を提示先が正しく見破ることができることを確認。また、制御・記録ミス、監査不能の発生がないことを確認

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）

●位置情報の生成では、機械学習によるGNSS位置情報の偽装検知を開発し、高い性能（適合率0.97、再現率0.93）と処理時間1m秒以内の完了を確認
●位置情報の記録では、時系列データのメッセージ認証手法を試作、想定するユースケースに対する問題発生ゼロを確認

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

（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）

●大規模環境を想定したシミュレーションにより性能評価を行い、衝突防止シナリオについては、 66%以上の帯域削減および片道・往復遅延時間がそれぞれ40ms、100msの実現可能性とその場合の要件等を整理した。物資管理シナリオについては、100万台以上のスマートタグ情報の送信における付加するセキュリティ情報の66%以上の周波数帯域削減効果の確認及びそのための要件等を整理した。また、衝突防止シナリオに関するプロトタイプをベースに構築したデモシステム展示により、社会認知・普及活動を展開した。

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
5 (3)	0 (0)	2 (2)	19 (10)	0 (0)	0 (0)	1 (1)	3 (3)

※成果数は累計件数、( )内は当該年度の件数です。

トピックス

・ACNS2023 Best Poster Award受賞

・MobiSec2023 KISTI Best Paper Award受賞

・NICT社会実装支援プロジェクトにて、グラレコを実施、同グラレコはEdgeTech2023に出展。

・早稲田大学オープンイノベーションフォーラム2023にて、研究成果をPR

・Decentralized Identity Foundation DIF HackathonにてDIF Second Place/ TBD (Block) First Place/ Trinsic First Placeを受賞

・DID(Decentralized Identifiers)に基づくVC(Verifiable Credentials)方式における属性の表現方法を規定するW3C(World Wide Web Consortium)のRDF Dataset Canonicalization and Hash Working Groupミーティングに参加し、DIDとVC方式の動向を調査

5. 研究開発成果の展開・普及等に向けた計画・展望

(1)計画

本研究開発終了後には研究開発で得た成果を基に国際標準化への貢献の可能性を探ってゆく。具体的には本研究開発で実装した新しいVPデータフォーマットの提案やアグリゲートメッセージ認証及びそれに基づく相手認証技術のユースケースに関するTechnical Reportを提出できるような国際標準機関や業界団体などを探ってゆく。

また、産業応用については、構築したデモシステムで得られた知見やEdgeTechに出展したグラレコなどを活用しながら展示会への出展を視野に成果の認知度向上に努めてゆく。さらに現在調整中のEdgeTech訪問者との打ち合わせなどを通じて、社会実装に向けた課題の有無や引き合い企業の要望などを洗い出し、ドローン産業に限らず他の産業等での活用も視野に営業活動の推進に努める。

(2)展望

近未来のドローン物流・人流時代の実現に向けた研究開発の一翼を担う本研究開発課題の成果は、関連産業界のみならず広く社会にインパクトを与えるものと期待している。

また、Beyond5G時代への新たな無線通信時代に向けても、その活用の可能性を具体的事例として示しつつ、その事例に組み込んだBeyond5G通信網の効率的利用を可能とする技術は、電波リソースの有効活用を可能とし国民的利益に資するもの、と期待している。

今後の展望として、本研究で得られた成果展開にむけて、今後の運送業やドローン産業の動向、取り巻く市場状況やその時々の情勢を注視しながら、用途を限定せず、IoT分野や自動車等、他分野での応用を視野に成果展開の可能性を探っていきたい。