令和4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年度から令和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4年度83百万円）

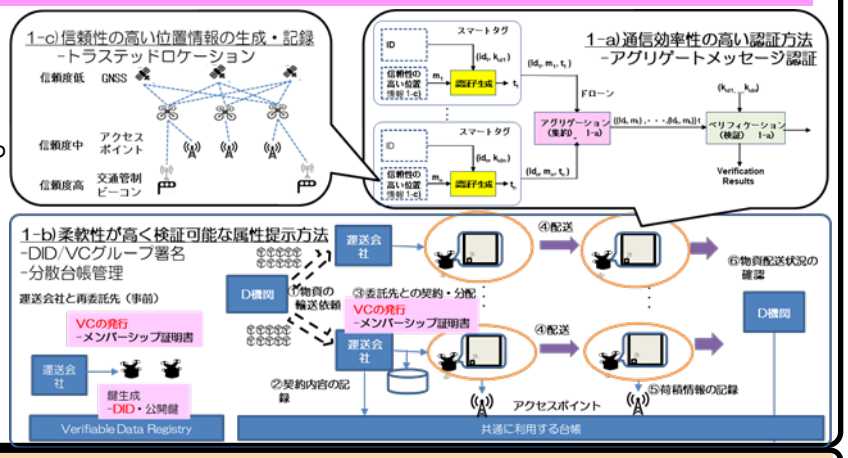
２．研究開発の目標

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

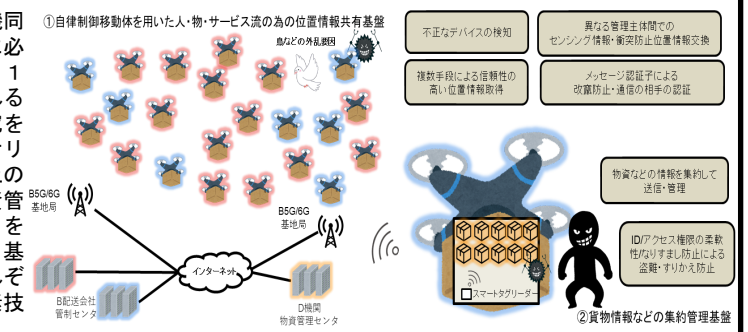
研究開発項目1：ワイヤレス通信の効率的かつセキュアな情報交換方法のための要素技術研究

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）

●アグリゲート認証技術による相手認証技術の研究では、新たにアグリゲート相手認証（片側認証方式）における形式的モデル、セキュリティ要件の定式化を行い、グループテストとメッセージ認証方式（MAC）による一般的構成法を開発
●アグリゲート署名技術の研究では、集約者と検証者の間でグループテストアルゴリズムの実行により格子ベース構成で「不正データ」を特定することも可能、との知見を獲得

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方式によるフレームワーク上にVPを活用することでグループ署名を可能にする基盤を構築、更にログから署名した移動体が特定できることを確認
●物資を配送する移動体が柔軟性高く検証可能な属性を提示するプロトコルを策定、２人の所有者がそれぞれ２台の移動体を所有するというシナリオで検証、機能を確認

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）

●位置情報の生成については、複数のセンシングデバイスと機械学習による識別器を用いたGNSS偽装データの検出方法を開発、高い再現率93%と適合率97%の両立を確認
●位置情報の記録については、研究開発項目1-a）で生成されるメッセージ認証子に基づいて時系列データを記録する方法を試作、機能を確認

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）

●課題1-aの成果を組み込んだ衝突防止プロトタイプを開発し、ドローン間での位置情報共有、想定するリスクへの対応を確認、遅延時間の目標値（0.1秒）についても、既存の設備による実測結果から、想定される通信・ハードウェアの性能向上により達成する見込みであることを確認
●課題1-bの成果を組み込んだ物資管理プロトタイプを開発し、確実な物資の配送、想定するリスクへの対応を確認、周波数帯域削減効果の目標値（66%）についても、複数の仕分けパターンにおける実装評価結果から、達成する見込みであることを確認

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	標準化提案	プレスリリース報道	展示会	受賞・表彰
2 （1）	0 （0）	0 （0）	9 （8）	0 （0）	0 （0）	0 （0）	0 （0）

●研究開発成果の展開・普及等に向けた計画（標準化）

※成果数は累計件数、（ ）内は当該年度の件数です。

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方式の動向を調査し、標準化に貢献できる領域を検討していく。

また、ITU-Rへの寄書の国内窓口のひとつとなっているBeyond 5G推進コンソーシアム白書分科会および国際委員会への参加を継続し、ホワイトペーパーへの寄書から貢献を検討していく。

さらに、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については標準化に向けて標準化先団体等の調査を実施する。

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

●アグリゲート相手認証ではシミュレーションによる性能評価結果を分析し、66%以上の周波数帯域削減効果を得ることを確認し、また、共通鍵等の管理用方式を考案・整理する

●アグリゲート署名による相手認証技術では、前年度に構築した基本方式の分析・評価により更なる改良・拡張等を目指す

1-b)柔軟性が高く検証可能な属性提示方法

●それぞれの組織が所有する移動体を一つ一つ識別する属性について、同じ属性を持っている相手に対して、鍵共有による暗号通信が可能になる機能を提供する

●新規移動体の追加を容易にし、想定したシナリオに対して、偽造された属性や、古い属性を提供した場合に、提示先が正しくそのことを見破ることができることを確認する

1-c)信頼性の高い位置情報の生成・記録

●信頼性の高い位置情報を生成するための検証処理について、片道処理時間が0.04秒、往復応答0.1秒以内に完了することを確認する

●PoCや実証実験において、設定したユースケース・シナリオに対してリスク事象が発生しないことを確認する

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

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、大規模環境下での目標性能の実現可能性を確認する

●移動体の衝突防止のためのシナリオについてはドローンの位置情報送信から飛行制御情報入手までの遅延時間が0.1秒の実現可能性とその場合の要件等を整理する

●物資管理のための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を得ることを確認し、そのための要件等を整理する

●小規模環境での機能・性能評価のために前年度に構築した衝突防止シナリオに関するプロトタイプを使用し、デモシステムを構築、イベント等でのデモによる社会認知・普及活動を展開する