自律型モビリティシステム（自動走行技術、自動制御技術等）の開発・実証
Ⅰ　自律型モビリティシステムの高信頼化に係る技術の確立
Development and demonstration project on autonomous mobility system (self-driving technology, automatic control technology)
Ⅰ　Research and Development on Secure Management Technologies for Autonomous Mobility System

代表研究責任者　岡本学　　株式会社日立製作所

研究開発期間　　平成 28 年度

【Abstract】

・We have developed a basic platform to securely and reliably accommodate an autonomous mobility system. The platform is built on top of three technologies which are "lifecycle management of network slices", "cybersecurity management", and "slice-discard management". The lifecycle management of network slices provides resources' isolation among services in order to guarantee resource allocations and to localize security threats. The cybersecurity management provides a detection of various cyber attacks including denial of services (DoS) and spoofing by an escalation of flow analysis. The slice-discard management blocks malcious data flows by sharing information of discard configurations among switches to transmit data packets. A prototype system was developed, and its performances were evaluated. Specifically, three different types of slice were created and each resource was isolated from that of other slices. Above mentioned cyber attacks for the mobility system were detected. In addition, detected malcious data flows were discarded even if a cyber attacker moved between base stations. As a result, the effecviveness of developed technologies for the autonomous mobility system was verified.

1　研究開発体制

○ **代表研究責任者**　　岡本学　（株式会社日立製作所）
○ **研究分担者**　　川村　龍太郎†（日本電信電話株式会社†）
○ **総合ビジネスプロデューサ**　中村　秀治（三菱総合研究所）
○ **ビジネスプロデューサ**　　渡辺　一弘（株式会社日立製作所）
　　吉野　修一†（日本電信電話株式会社†）

○ **研究開発期間**　平成 28 年度
○ **研究開発予算**　総額　166 百万円

２　研究開発課題の目的および意義

我が国が超高齢化と労働人口減少を迎える中、過疎地も含めた高齢者の安全・安心な生活、多様な経済活動の生産性確保等を図るため、様々なセンサー情報等も活用し、ICT 基盤技術と連携して、高信頼・高精度な自動走行を実現する自律型モビリティシステム（自動走行技術、自動制御技術等）の開発を推進する。自律型モビリティシステムは、多様な分野における持続的な成長の基盤として期待されており、主要国でも官民を挙げた大規模プロジェクトが始動しているため、我が国でも本施策を早急に推進する必要がある。

このため、自動走行に必要な高度地図データベースの更新・配信のための通信技術の開発や、自動走行技術、自動制御技術等を活用した安全・安心な自律型モビリティシステムの開発及び利活用実証を推進することで、自律型モビリティシステムを支えるICT 基盤技術の確立及び研究成果に関する国際標準の獲得等による我が国の国際競争力の向上に寄与することを政策目標とする。

本研究開発課題では、自律型モビリティシステムの高信頼化に係る技術の確立を目的として、サイバー攻撃の検知・判断技術と連携した仮想ネットワークスライス技術による異常トラヒックの遮断・隔離技術の有用性及び実用性を検証する。

３　研究開発成果（アウトプット）

今回、課題Ⅰ「自律型モビリティシステムの高信頼化に係る技術の確立」を目的に研究開発を実施した。

自律型モビリティシステムを安全･安心に運用するための高信頼化に係わる研究開発として、仮想ネットワークスライス技術により自律モビリティシステム用ネットワークをセキュアに他サービスと分離し、サイバー攻撃の検知・判断技術と連携することにより、サイバー攻撃から該当トラヒックを遮断・隔離する技術の確立を目的に研究開発に取り組んだ。

以下に研究成果を示す。

３．１　課題Ⅰ－ア）　自律型モビリティシステム用ネットワークスライス生成・管理技術

自律型モビリティシステムは、「ネットワークを介して受信する情報」と「自律型モビリティ自身が検知した情報」に基づき、自律的に移動を制御することが求められる。このため、自律型モビリティシステムに属する自動走行車両等がネットワークを介した複数のサービスの提供を受ける場合、自律型モビリティシステム内のアプリケーションを、サービスの重要度に応じて独立した仮想ネットワーク上の複数のスライスにそれぞれ接続し、各仮想ネットワークの品質が保証される必要がある。

本研究開発では、自動走行車両等の移動に追随して仮想ネットワーク上でスライスに継続的に接続し、複数のスライスにおいて一定レベルのサービス品質を継続的に利用可能とする技術を確立する。

以下に述べる研究成果により、「自律型モビリティシステム用ネットワークスライス生成技術」と「自律型モビリティシステム用ネットワークスライス接続管理技術」の基礎技術を確立した。自動走行車両等のエリア移動において継続的なネットワークスライス接続の実現に向けた隣接エリア間の連携制御を想定した基礎技術となる。

課題Ⅰ－ア）－①　自律型モビリティシステム用ネットワークスライス生成技術

本研究開発では、ローカルサーバを収容し広域に分散する多数のローカルネットワークとそれらを繋ぐコアネットワークにおいて、複数ネットワークを跨る通信であっても、同一サービスの通信は一つのネットワークスライスに閉じた通信となるよう仮想ネットワークを構成する技術を確立した。また、適用サービスの数に応じて、異なるネットワークスライスを３層以上構築し、ネットワークスライス間での通信は不可能にし、各スライスを分離・独立させる技術を確立した。図 １にネットワークスライス構成概要を示す。

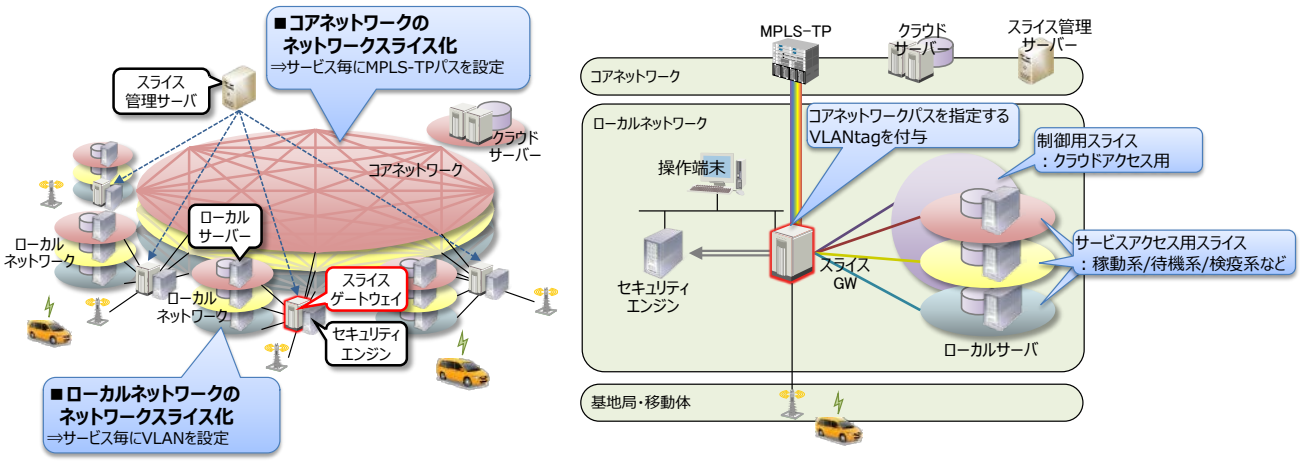

図 １　ネットワークスライス構成概要

スライス生成では、下記の技術要素により、同一サービスに関して複数エリアに分割されるローカルネットワークを中継網を介して接続することで、サービス毎に複数エリアにまたがるネットワークスライスを生成する技術を確立した。

a）ローカルスライス生成技術

各ローカルネットワークにおいて、収容するサービスに応じて仮想的にネットワークを分割し、対応する VLAN の決定や、サービスの優先順位の判断、必要な帯域の割り当てを行う技術を確立した。

b）隣接エリア間パス生成技術

物理的なネットワーク配置に応じて、中継網（コアネットワーク）において隣接するローカルエリア間の通信パスをサービス単位で設定し、同一サービスの通信パスとローカルの仮想ネットワークを対応付けする技術を確立した。

ｃ）サーバ（エッジ／クラウド）間の転送技術

該当エリアを管轄する最寄りのエッジサーバとサービス毎に異なるクラウドサーバの配置に応じたパス管理テーブルを生成し、通信パスを確立する技術を確立した。

図 2 にネットワークスライスを管理・生成するスライスゲートウェイおよびスライス管理サーバのモジュール構成を示す。スライスゲートウェイのモジュール構成として、スライス管理サーバ/セキュリティエンジンとの通信を受け持つ North-bound では、REST-API を定義し指示/通知を行う仕組みとし、ルータ(AX8616R)とのインタフェースを受け持つ South-bound では AX8616R が持つ Python インタフェースを使用し、コマンドの実行、状態監視を行う仕組みとした。Event-Manager は North-bound/South-bound からのイベントを処理し、移動体/ネットワークスライスをデータベースとして管理する。また、移動体の状態監視を行うため、周期処理を持ち移動体からのローカルサーバへのアクセスを監視する構成とした。

スライス管理サーバは、自律型モビリティシステムの構成要素であるスライスゲートウェイを管理するとともに、スライスゲートウェイの隣接情報を管理し、移動体がスライスゲートウェイに接続した際に接続情報を隣接するスライスゲートウェイにも配信することで、移動体の移動に追随する仕組みとしている。また、移動体およびネットワークスライスのセキュリティ状態を管理し、移動体やネットワークスライスがサイバー攻撃を受けるなどの異常が発生した場合には、それらがローカルネットワークから遮断されたことを、管理サーバに通知するとともに、隣接するスライスゲートウェイにも通知する構成とした。

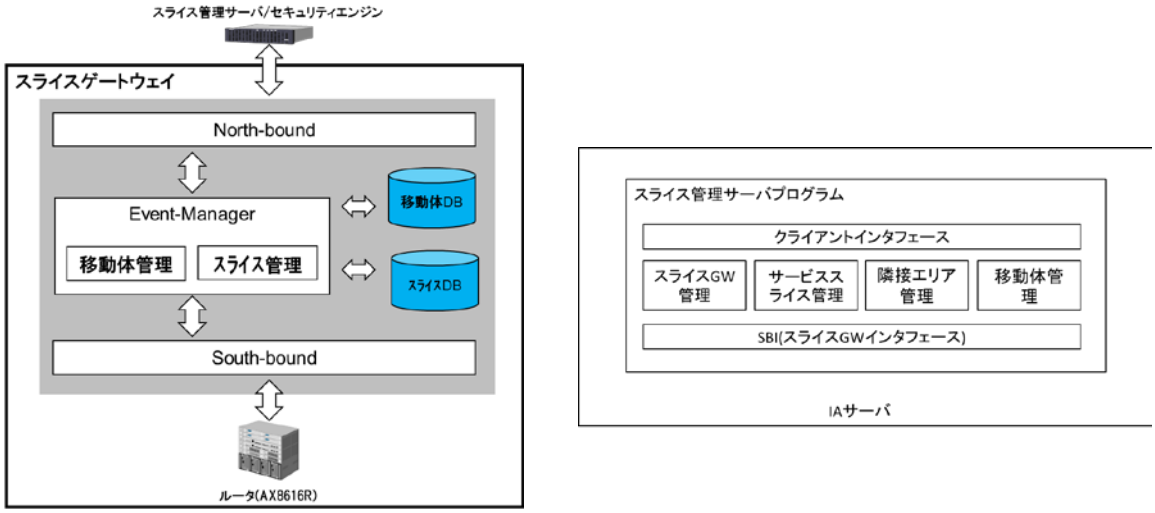

図 2　スライスゲートウェイ(左)、スライス管理サーバ(右)モジュール構成

課題Ⅰ－ア）－②　自律型モビリティシステム用ネットワークスライス接続管理技術

本研究開発では、ローカルネットワークにおけるネットワークスライス管理を行うスライスゲートウェイにおいて、自律走行車両等から受信したパケットの宛先情報等から接続先サービスを特定し、そのサービスを収容するネットワークスライスへ接続し、一定レベルのサービス品質を提供する技術を確立した。

また、移動元、移動先のスライスゲートウェイ間にて自律走行車両等の端末情報を継承するため、移動先となり得る隣接エリアのスライスゲートウェイに対し先回りして端末情報を転送する技術を確立した。また、端末情報を受け取った隣接エリアのスライスゲートウェイでは、エリア移動してきた自律走行車両等のローカルサーバへの接続を滞りなく行う（サービス接続遅延を極小化する）ため、対象の自律走行車両等用に予め接続準備を実施する技術を確立した。

３．２　課題Ⅰ－イ）自律型モビリティシステムに対するサイバー攻撃の検知・判断技術

自律型モビリティシステムでは、実際の自動走行車両等の制御に関わる通信を行うことも想定され、ネットワークを経由したサイバー攻撃を迅速に検知する必要がある。自律型モビリティに対する脅威としては、「自動走行に必要な情報の不達を意図した攻撃（大量のパケットを送信するDoS 攻撃等）」と「自動走行に必要な情報に対する攻撃（なりすまし端末やマルウェアに感染した端末による虚偽情報の送信等）」の大きく２種類に整理されると考えられる。

本研究開発では上記の２種類の脅威に対応するため、自動走行車両等とエッジサーバの間でパケットの通信状況をモニタリングする技術､モニタリングされたパケットからDoS 攻撃や改ざんなどの異常を検知する技術、異常を検知した場合の手動運転等の安全動作への移行のための判断機構技術等を確立する。

本研究開発では、自律型モビリティシステムに対するサイバー攻撃を迅速に検知・判断する技術を確立するために、脅威レベルに応じて分析の詳細度を変化させる多層型検知技術を適用し、自律型モビリティシステムにおけるセキュリティ上の脅威を効率的に検知する基礎技術を確立した。また、検知した脅威に対して、ネットワークからの遮断等の推奨する通信制御上の対処方法を判断する基礎技術を確立し、対処内容を課題Ⅰ－ア）のネットワークスライスに伝達するためのインタフェースを規定した。

課題Ⅰ－イ）－①　自律型モビリティシステム向け多層型検知技術

自律型モビリティシステムにおいて想定される脅威（プローブ情報を大量に送信する DoS 攻撃、ダイナミックマップを大量に送信する DoS 攻撃、虚偽のプローブ情報の送信）を検知する方法として、分析対象のトラヒックあるいは自律型モビリティの脅威レベルに応じて分析手法の詳細度を変化させる多層型分析手法により、効率的な検知を実現する基礎技術を確立した。

例えば、虚偽プローブ情報を送信する攻撃（虚偽プローブ攻撃）を検知するための多層型分析手法の分析プロセスを図 3 に示す。

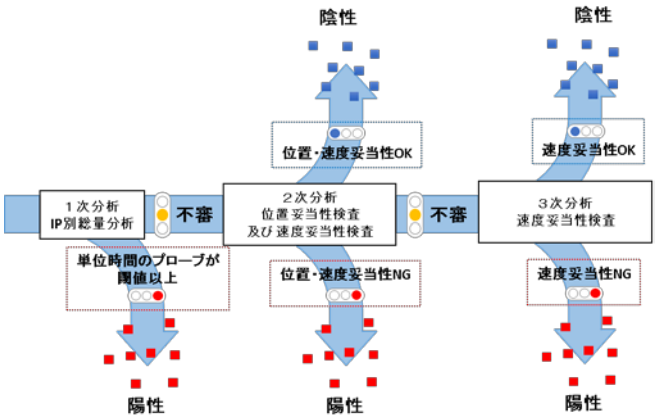

図 3　多層型分析手法の分析プロセスの例（虚偽プローブ攻撃時）

虚偽プローブ攻撃に対する検知は 1 次で IP 総量分析、2 次で位置情報妥当性検査及びサンプリングデータにおける速度妥当性分析、3 次で広範サンプルにおける速度妥当性分析を行う構成とした。

多層型分析手法と従来手法（単層型分析手法）との性能比較として、経過時間毎に増加する虚偽プローブ攻撃に対する処理時間の測定結果を図 4 に示す。5 分経過後では、単層型分析手法では 20 秒程度かかっているところ、多層型分析手法では 50 ミリ秒程度の処理時間で済んでおり、多層型分析手法の場合は単層型分析手法に比べて処理コストが少なく効率的な分析が実現できていることが分かる。

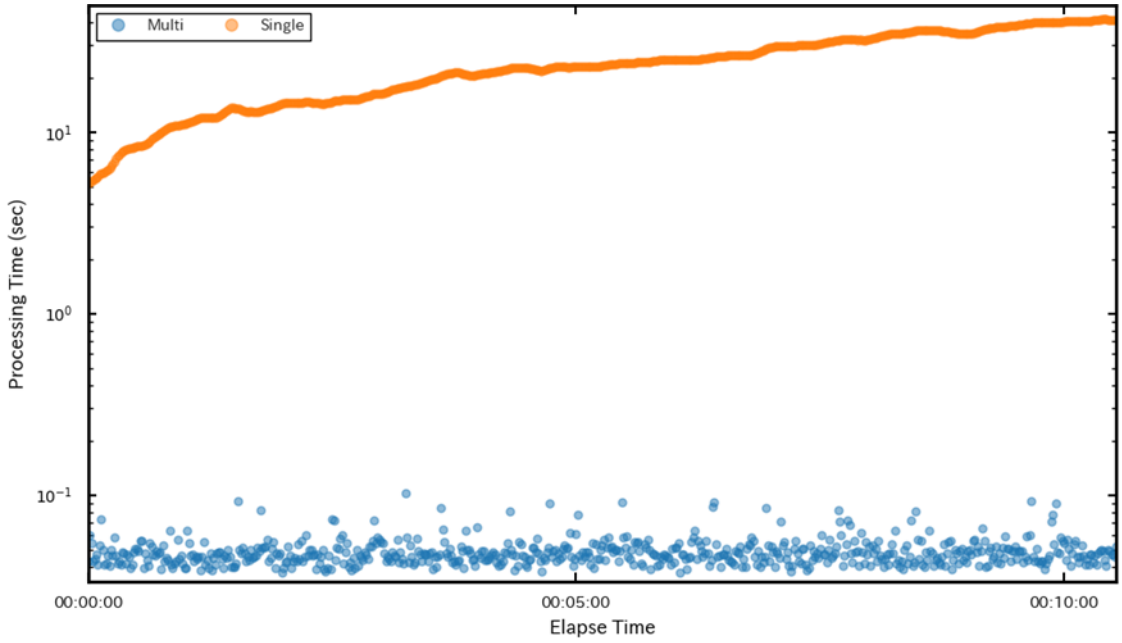

図 4　単層型分析手法（橙色）及び多層型分析手法（青色）の処理時間の平均値

課題Ⅰ－イ）－②　自律型モビリティシステム向け分散協調型検知技術

攻撃の疑いのある自動走行車両等が他のエリアに移動した後においても移動に追随してローカルネットワーク間で分析を継続し、途切れることなく効率的に攻撃を検知する技術の確立に向けて、自律型モビリティと移動網、エッジサーバ等のネットワーク構成と接続の方式について、取りうる形態の比較評価を行い、セキュリティ確保の観点から推奨される構成を明らかにした。

課題Ⅰ－イ）－③　検知結果に応じた通信制御上の対処方法の判断技術およびネットワークスライスへの対処方法の伝達インタフェースの規定

多層型分析手法による分析結果に基づき現在のシステムの脅威の状況を判定し、その状況から必要な通信制御上の対処方法を判断する技術を確立した。また、判断した通信制御上の対処方法を課題Ⅰ－ア）のネットワークスライスにおける通信制御装置（スライスゲートウェイ）に通知するインタフェースを規定した。

３．３　課題Ⅰ－ウ）　自律型モビリティシステム用ネットワークスライス遮断・縮退技術

自律型モビリティシステムに対するサイバー攻撃を回避するためには、ネットワークが自動走行車両等を追随しながらも、サイバー攻撃の規模や対象範囲に応じてネットワーク遮断等の対応を行うことが必要である。

本研究開発では、自律型モビリティシステムに対するサイバー攻撃の規模や範囲に動的に対応し、課題Ⅰ－イ）のサイバー攻撃の検知・判断に従い、自律型モビリティシステム用ネットワークスライスを遮断・縮退することでサイバー攻撃を回避する技術を確立するとともに、自動走行車両等を追随して、仮想ネットワークへの再接続を可能とする技術の開発を行う。

本課題における研究開発では、自律型モビリティシステムに対するサイバー攻撃の規模や範囲に動的に対応し、課題Ⅰ－イ）のサイバー攻撃の検知・判断に従い、自律型モビリティシステム用ネットワークスライスを遮断・縮退することでサイバー攻撃を回避する「ネットワークスライス遮断・縮退技術」の基礎技術を確立した。また、自律走行車両等の移動に追随して、仮想ネットワークへの再接続を可能とする技術「ネットワークスライス再接続技術」の基礎技術を確立した。これらはサイバー攻撃の規模や自動走行車両等の移動速度に応じたスライス遮断・縮退操作に関する優先制御を想定した基礎技術となる。

図 4 に移動体の遮断とローカルサーバの切替(遮断･再接続)概要を示す。

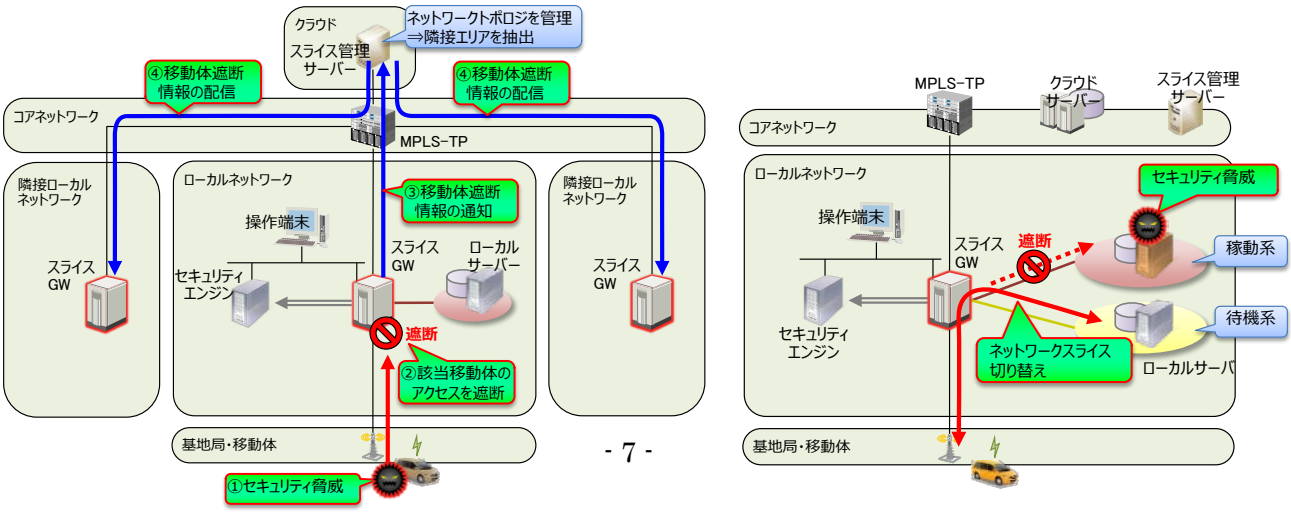

図 3　移動体の遮断とローカルサーバの切替(遮断･再接続)概要

課題Ⅰ－ウ）－①　ネットワークスライス遮断・縮退技術

サイバー攻撃に対して、課題Ⅰ－イ）のサイバー攻撃の検知・判断に従い、且つ攻撃側及び被害側のモビリティに対応して、攻撃側と被害側の双方の移動体に追随してスライスの遮断・縮退情報をローカルネットワーク間で継承する技術を確立した。

課題Ⅰ－ウ）－②　ネットワークスライス再接続技術

自律型モビリティシステムにおける自律走行車両等の再接続に関し、不正なデータパケットにより自律走行に必要な情報を受信できないような状況において、スライスを切り替えることで不正動作するローカルサーバを切り離し、被害側の自律走行車両等に対して攻撃発生前と異なるスライスのローカルサーバへの接続を可能とする基礎技術を確立した。被害側の自律走行車両等のハンドオーバに対応して異なるローカルサーバへ再接続可能とするため、ネットワークスライスの遮断・縮退に連動し、正常なサービス提供が可能なスライスへ再接続する技術を確立した。

4　政策目標（アウトカム目標）の達成に向けた取組みの実施状況

○標準化

総務省「自律型モビリティネットワークの高信頼化に係る技術の確立」課題ア：自律型モビリティシステム用ネットワークスライス生成･管理技術に係る成果の標準化を推進するため、平成 28 年 12 月 5 日から平成 28 年 12 月 9 日まで、ITU-T FG IMT-2020 (Geneva, Swiss)に参加し、開発技術に関連した標準化動向を調査するとともに、ネットワークリソース利用調停に関する提案を行った。

自律型モビリティプロジェクトでは、ローカルネットワークスライス間を高信頼な伝送パスで接続する方針であり、特に伝送パス設定調停方式の開発を進めている。そこで、本方式の標準化を推進するため、ソフトウェアにより管理可能なネットワークにおけるアプリケーション基本仕様書に対して、伝送パス設定調停について記述追加を提案し承認された。

○事業化

本研究開発において、自律型モビリティシステムを安全･安心に運用するための高信頼化に係わる基礎技術の有用性を確認した。自律型モビリティシステムにおいて、高度地図データベースは、安全・安心に自動走行するために重要な情報であり、高信頼にモビリティに情報伝達するためにも、セキュアな仮想ネッ

トワークを実現・提供する技術の有用性を確認できたことは重要な成果であると考える。

今後、自動運転のみならず、エッジコンピューティングに配備する IoT データの多様化・大容量化が予想され、限りあるネットワークインフラ上への複数の仮想ネットワーク収容の実現がサービス発展の重要要素になるものと考える。今後、各種社会インフラ分野として必要となるネットワーク要件の調査・検討を引き続き実施し、社会実装時に必要となる機能やアーキテクチャの明確化を行い、製品化を目指していく。

５　政策目標（アウトカム目標）の達成に向けた計画

今回の研究開発の成果を踏まえ、引き続き研究開発に取り組むと共に、対外アピール活動を継続し、自律型モビリティシステムの社会実装に向け活動を推進する。

本研究開発成果の社会展開に向けた政策目標（アウトカム目標）の達成に向けた活動として、事業化・製品化、標準化に関する今後の計画について以下に示す。

○事業化・製品化

担当	課題	ターゲット	時期	目標
日立	課題 ア 課題 ウ	通信事業者 社会インフラ事業者	2018年度	ICT基盤技術（自律型モビリティシステム全体）の総合実験
			2019年度～	自律型モビリティシステム対応ネットワークスライス制御システムに関する製品化
NTT	課題 イ	サービスプロバイダ、SIer	2018年度	ICT基盤技術（自律型モビリティシステム全体）の総合実験
			2019年度～	ICT基盤技術の実証環境提供、商用化支援

○標準化

今後、標準化活動については、自律型モビリティ等、様々なネットワーク要件を具備した IoT サービスを収容するネットワークスライス技術の標準化について引き続き活動を推進する。

６　査読付き誌上発表論文リスト

特になし

７　査読付き口頭発表論文（印刷物を含む）リスト

特になし

８　その他の誌上発表リスト

特になし

９　口頭発表リスト

[1]日本電信電話株式会社　田中裕之、株式会社日立製作所　岡本学
“自律型モビリティシステムを支えるＩｏＴデータ高速処理技術および高信頼な通信制御について”
スマートＩｏＴ推進フォーラム（東京）（2016 年 9 月 27 日）

１０　出願特許リスト

[1] 鈴木敏明・星原隼人・久保広行・小河太郎
ネットワークシステム、ネットワーク管理方法およびネットワーク管理装置、
日本、特願 2017-007385、2017 年 1 月 19 日

[2] 鈴木敏明・小河太郎・中嶋淳
ネットワークシステム、ネットワーク管理方法および装置、
日本、特願 2017-011881、2017 年 1 月 26 日

[3] 原田貴史・伊藤宏樹・川田丈浩
対処指示装置、対処指示方法、対処指示プログラム、
日本、特願 2017-051831、2017 年 3 月 16 日

[4] 原田貴史・伊藤宏樹・川田丈浩
対処指示装置、対処指示方法、対処指示プログラム、
日本、特願 2017-051832、2017 年 3 月 16 日

１１　取得特許リスト

特になし

１２　国際標準提案・獲得リスト

[1] ITU-T FG IMT-2020、Hitachi, Ltd.,”Proposal on O3 Project descriptions
for the Baseline Document: Application of network softwarization to IMT-2020”,
2016/12/5

１３　参加国際標準会議リスト

[1]ITU-T・FG IMT-2020、ジュネーブ、2016 年 12 月 5 日～9 日

１４　受賞リスト

特になし

１５　報道発表リスト

（１）報道発表実績

特になし

（２）報道掲載実績

特になし

研究開発による成果数

	平成 28 年度
査読付き誌上発表論文数	0件（ 0件）
査読付き口頭発表論文数（印刷物を含む）	0件（ 0件）
その他の誌上発表数	0件（ 0件）
口頭発表数	1件（ 0件）
特許出願数	4件（ 0件）
特許取得数	0件（ 0件）
国際標準提案数	0件（ 0件）
国際標準獲得数	0件（ 0件）
受賞数	0件（ 0件）
報道発表数	0件（ 0件）
報道掲載数	0件（ 0件）

注１：各々の件数は国内分と海外分の合計値を記入。（括弧）内は、その内海外分のみを再掲。

注２：「査読付き誌上発表論文数」には、定期的に刊行される論文誌や学会誌等、査読（peer-review（論文投稿先の学会等で選出された当該分野の専門家である査読員により、当該論文の採録又は入選等の可否が新規性、信頼性、論理性等の観点より判定されたもの））のある出版物に掲載された論文等（Nature、Science、IEEE Transactions、電子情報通信学会論文誌等および査読のある小論文、研究速報、レター等を含む）を計上する。

注３：「査読付き口頭発表論文数（印刷物を含む）」には、学会の大会や研究会、国際会議等における口頭発表あるいはポスター発表のための査読のある資料集（電子媒体含む）に掲載された論文等（ICC、ECOC、OFC など、Conference、Workshop、Symposium 等での proceedings に掲載された論文形式のものなどとする。ただし、発表用のスライドなどは含まない。）を計上する。なお、口頭発表あるいはポスター発表のための査読のない資料集に掲載された論文等（電子情報通信学会技術研究報告など）は、「口頭発表数」に分類する。

注４：「その他の誌上発表数」には、専門誌、業界誌、機関誌等、査読のない出版物に掲載された記事等（査読の有無に関わらず企業、公的研究機関及び大学等における紀要論文や技報を含む）を計上する。

注５：PCT 国際出願については出願を行った時点で、海外分１件として記入。（何カ国への出願でも１件として計上）。また、国内段階に移行した時点で、移行した国数分を計上。

注６：同一の論文等は複数項目に計上しないこと。例えば、同一の論文等を「査読付き口頭発表論文数（印刷物を含む)」および「口頭発表数」のそれぞれに計上しないこと。ただし、学会の大会や研究会、国際会議等で口頭発表を行ったのち、当該学会より推奨を受ける等により、改めて査読が行われて論文等に掲載された場合は除く。