2022（令和 4）年 7 月 7 日

自動運転車の安全性に数学的証明を与える新手法を開発

～論理的安全ルールの効率的導出により自動運転の社会受容を加速～

情報・システム研究機構 国立情報学研究所（ＮＩＩ、所長：喜連川 優、東京都千代田区）のアーキテクチャ科学研究系教授 蓮尾 一郎 らの研究チームは、科学技術振興機構（ＪＳＴ、理事長：橋本 和仁、東京都千代田区）の戦略的創造研究推進事業 ERATO蓮尾メタ数理システムデザインプロジェクト(*1)（ERATO MMSD、研究総括：NII アーキテクチャ科学研究系教授 蓮尾 一郎）のもと、自動車の自動運転システムの安全性に強い数学的保証を与える技術とその基礎理論を開発しました。

本研究では、自動運転安全性の数学的証明のための既存の方法論「RSS（責任感知型安全論、responsibility-sensitive safety）」に注目し、その応用範囲を大きく拡大し実世界へ本格展開できるよう拡張した手法「GA-RSS（goal-aware RSS）」を確立しました。形式論理学(*2)の知見を用いた今回の拡張によって、非常停止などの目標達成を求める複雑な運転シナリオに対しても、安全性の数学的証明が可能になります。

本研究成果は, 2022 年 7 月 5 日（米国東部時間）に IEEE Transactions on Intelligent Vehicles のオンライン版で公開されました。

【ポイント】

- 自動車の自動運転を社会が受け入れるためには、安全性の保証とトレーサブルな（論理的議論を追跡できる）説明が必須である。
- 数学的証明は厳密な安全性保証であり、究極の安全性保証のかたち。しかし、実際の自動運転システムへの適用は簡単ではなかった。
- 既存の方法論「RSS（責任感知型安全論、responsibility-sensitive safety）を形式論理的に拡張し、安全ルール導出のためのソフトウェアサポートを設計したことにより、複雑な運転シナリオでも安全性の数学的証明が可能になった。
- 自動運転の社会受容・普及の加速が期待される。

国立研究開発法人 科学技術振興機構（JST）
広報課
〒102-8666 東京都千代田区四番町 5 番地 3
TEL：03-5214-8404 FAX：03-5214-8432
E-Mail：jstkoho@jst.go.jp

大学共同利用機関法人 情報・システム研究機構
国立情報学研究所
総務部企画課 広報チーム
〒101-8430 東京都千代田区一ツ橋 2-1-2
直通：03-4212-2164 FAX：03-4212-2150
E-Mail：media@nii.ac.jp

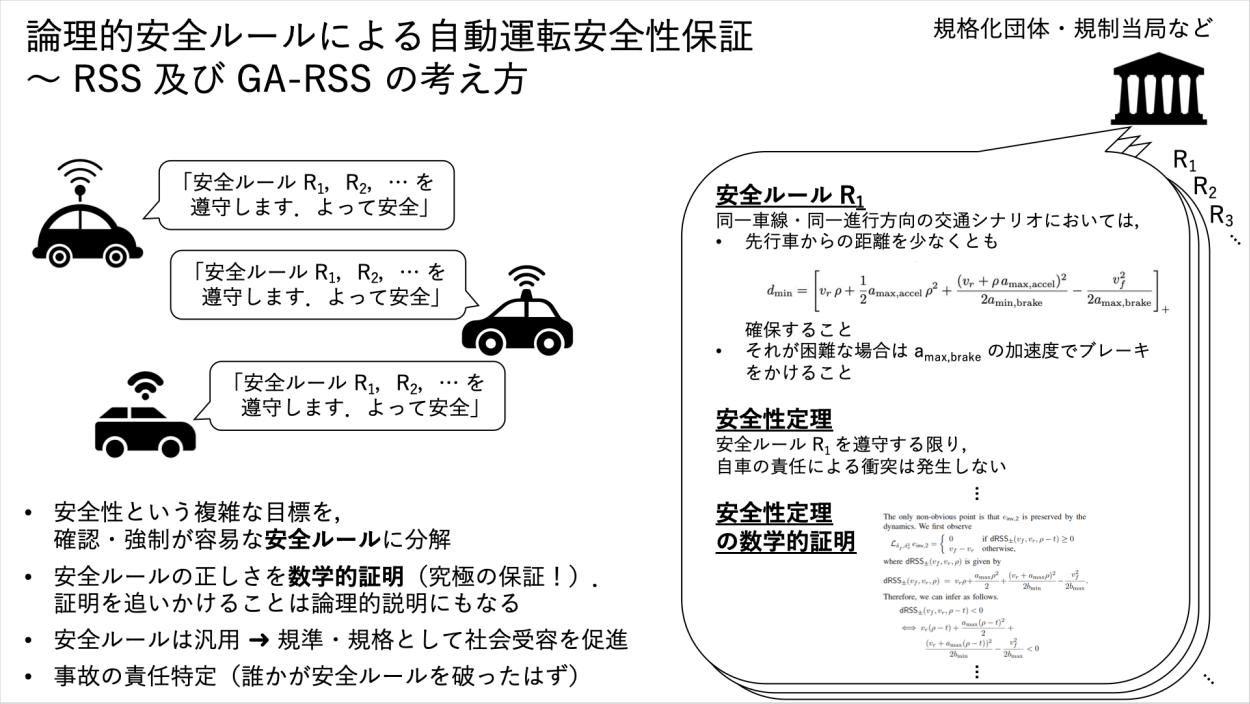
【背景】

今後の社会に期待されている自動車の自動運転技術の普及のためには、自動運転車の安全性を高めるだけでは十分ではありません。高い安全性を社会に対して保証しそれを説明して、自動運転車を公道に受け入れてもらう必要があります。そのための現在主流のアプローチが、事故統計データによる保証や、計算機シミュレーションによるテストです。しかし、これらの経験論的・統計的アプローチには「なぜ十分に安全だと言えるのか」、「社会を納得させる説明ができるか」といった問いがつきまとうため、人間にとってよりわかりやすい安全性説明のための論理的アプローチの創出が強く望まれています。

この状況で近年注目を集めているのが、インテル社が提唱する RSS という方法論です（図 1）。RSS は、交通安全のためのルールを明示的な数式として書き表し、さらにその数式の妥当性を証明することによって、自動運転車の安全性に数学的証明を与えることを目指します。数学的証明は、その保証の度合においても、証明の過程を明らかにすることで結論の正しさを説明できることにおいても、まさに究極の安全性保証のかたちです。

自動運転のような複雑なシステムの安全性を数学的に証明することは一般に困難ですが、RSS は証明の対象を自動運転車が従うべき「論理的安全ルール」に絞ることで、これを可能にしています。RSS で策定した論理的安全ルールは、メーカー・車種などに依存しない一般的なものであり、国際規格や業界標準・交通法規として活用できるため、自動運転の社会受容を大きく加速させると期待されています。

現在、この RSS は産業界と学界で大きな興味を集めていますが、論理的安全ルールの策定及び証明のための技術的基盤が発達しておらず、その応用範囲は分岐のない道路における先行車の追従などの単純な運転シナリオに限られていました。

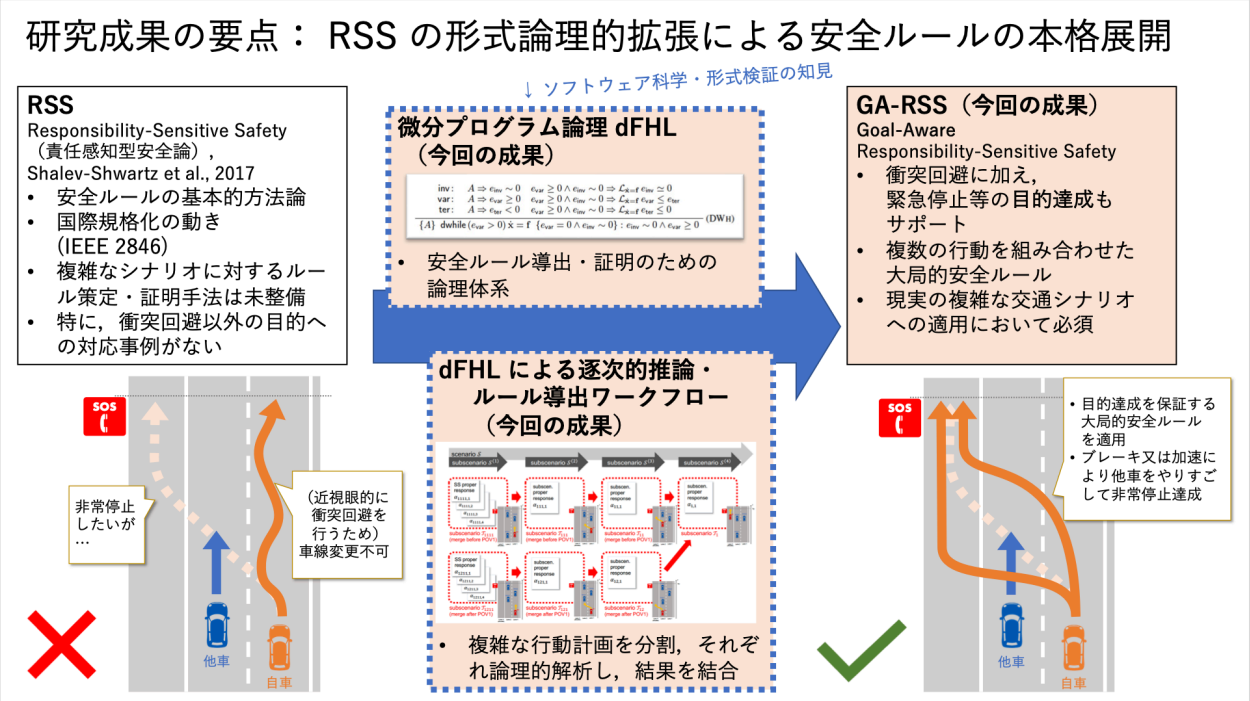


<図 1> 提案手法「GA-RSS」と RSS に共通する自動運転安全性への数学的証明によるアプローチ。数学的に厳密な論理的安全ルールを提案し、さらに「この論理的安全ルールを遵守する限り事故を起こさない」ことを「安全性定理」として数学的に証明する。

【研究手法・成果】

このような現状の下、我々は、RSS の弱点の克服するため、我々が持つ形式論理学の専門性を活かしてRSSの技術的基盤を新たに確立し、これに基づいてRSSの新たな拡張であるGA-RSS（goal-aware RSS）を提案しました。従来の RSS が単純な運転シナリオに対する衝突回避のみをターゲットとしていたのに対して、GA-RSS は「他車との衝突を回避しながら安全な地点に非常停止する」といった目標達成を求める複雑な運転シナリオに対しても、論理的安全ルールを策定し、その正しさを証明することができます。RSS の方法論を本格的に展開し、現実の多様で複雑な運転シナリオ群に適用するために、今回の GA-RSS への拡張は必須の技術です。

GA-RSS 拡張を可能にする技術的基盤として、我々は今回 dFHL（differential Floyd-Hoare logic、微分フロイド・ホーア論理）と名付けた形式論理の体系を提案し、これに基づく論理的安全ルール導出ワークフローとソフトウェアサポートを設計・実装しました（図 2）。dFHL は、自動車の制御のようなデジタル・アナログの両方にまたがるハイブリッドシステム (*3) の安全性証明を効率的に行うための形式論理の体系であり、ソフトウェア研究で良く知られている「フロイド・ホーア論理」を拡張して考案しました。この新しい論理体系 dFHL によって、自動運転車の複雑な行動計画を分割し逐次的に解析することが可能になり、RSS の適用範囲が大きく広がりました。



<図 2 > RSS（左）に微分プログラム論理 dFHL（中）を組み合わせることで GA-RSS（右）への拡張を実現し、多様な自動運転の状況へ適用できるようになった。この非常停止の例では、従来の RSS 安全ルールは近視眼的な衝突回避行動を強制するため、他車が邪魔になって車線変更が実行できず、非常停止という目標も達成できなかった。一方、今回提案の GA-RSS 安全ルールのもとでは、加速やブレーキによって他車をやりすごす大局的な行動計画を安全ルールに組み込むことができ、非常停止という目標を達成できる。

【今後の展望】

RSS を社会応用する試みはすでに活発であり、インテル社による実製品への応用や、IEEE P2846 における国際規格化の議論などが進んでいます。今回の成果の GA-RSS は、RSS の適用範囲を単純なシナリオから、非常停止などに代表される複数の行動の組み合わせでの目的達成を求めるような現実的で複雑なシナリオへと大きく広げるものであり、産業界での安全性保証の取り組みや、国際規格策定に向けた動きに大きく貢献できるものと確信しています。GA-RSS の活用で RSS の考え方がより広く適用できるようになり、自動運転の様々な状況の安全性に広く数学的証明という究極の保証を与えることができれば、自動運転に対する社会の不安を払拭でき、自動運転の社会普及と産業発展へ向けた大きな弾みになります。

論理的安全ルールは、数多くの運転シナリオそれぞれに対し、個別に策定し証明する必要があります。今回成果のルール導出ワークフローと今回設計したソフトウェアサポートを用いれば、複雑なシナリオに対しても、数週間程度の作業という現実的な工数で論理的安全ルール策定が可能です。こうして作成した論理的安全ルールはメーカー・車種などに依存しない一般的なものであり、社会全体の資産として永年にわたり使用することができます。

ERATO MMSD プロジェクトでは、今回提案したワークフロー及びソフトウェアサポートを活用して、より多くの運転シナリオへの論理的安全ルール策定を進めていきます。また、論理的安全ルール策定のさらなる効率化・省力化のための、理論研究とソフトウェア開発も進めていきます。

蓮尾一郎 教授からのコメント：

「証明を書くための言語（論理体系）を設計し、証明を書く営みにソフトウェアによるサポートを与えるのが、形式論理学の研究を行ってきた我々の社会貢献のミッションです。今回は、マツダ株式会社のみなさまとの協働の機会を得て、自動運転という重要な応用分野に対し貢献を行うことができました。長年研ぎ澄ましてきた理論的研究が今回（応用上の）日の目を見たと思っていますし、また同時に、数学的・理論的な基礎研究の重要性を示す一例でもあると考えています。

ERATO MMSD プロジェクトは、他プロジェクト（MIRAI eAI プロジェクト[(*4)]、CREST CyPhAI プロジェクト[(*5)]、CREST ZT-IoT プロジェクト[(*6)] など）とともに、NII の包括的ソフトウェア研究拠点としての活動の一翼を担っています。ERATO MMSD プロジェクトは、特にソフトウェア科学の理論的・数学的基盤の追究を通じて、物理情報システム・人工知能システム・システムセキュリティなど、新たな応用分野への貢献を行っていきます。」

【研究プロジェクトについて】

本研究は科学技術振興機構 戦略的創造研究推進事業 ERATO 蓮尾メタ数理システムデザインプロジェクト（JPMJER1603）の一環で行われました。また本研究では、マツダ株式会社との協働も行いました。[(*7)]

【論文タイトルと著者】

タイトル：Goal-Aware RSS for Complex Scenarios via Program Logic

著　　者：Ichiro Hasuo, Clovis Eberhart, James Haydon, Jeremy Dubut, Brandon Bohrer, Tsutomu Kobayashi, Sasinee Pruekprasert, Xiao-Yi Zhang, Erik Andre Pallas, Akihisa Yamada, Kohei Suenaga, Fuyuki Ishikawa, Kenji Kamijo, Yoshiyuki Shinya, Takamasa Suetomi

掲 載 誌：IEEE Transactions on Intelligent Vehicles

D　O　I：https://doi.org/10.1109/TIV.2022.3169762

発 表 日：2022 年 7 月 5 日（火）（米国東部時間）

〈メディアの皆様からのお問い合わせ先〉

大学共同利用機関法人 情報・システム研究機構 国立情報学研究所
総務部企画課 広報チーム
TEL：03-4212-2164　E-mail：media@nii.ac.jp

国立研究開発法人 科学技術振興機構（JST）
広報課
TEL：03-5214-8404　E-mail：jstkoho@jst.go.jp

〈JST の事業に関すること〉

国立研究開発法人 科学技術振興機構（JST）
研究プロジェクト推進部　今林文枝
TEL：03-3512-3528　E-mail：eratowww@jst.go.jp

（*1） ERATO 蓮尾メタ数理システムデザインプロジェクト：国立研究開発法人 科学技術振興機構（JST）の「戦略的創造研究推進事業 ERATO」に採択されている研究プロジェクトで、Society 5.0 の大きな柱となる物理情報システム(CPS)の品質保証手法の学術的研究を推進している。特に、CPS の典型例の一つとして注目される自動運転システムを重点応用対象として、その信頼性保証を支えるモデリング手法・形式検証手法・テスト手法、さらにこれらを包括する実用的な V&V 技術の研究開発に取り組んでいる。このような大きなチャレンジでは、ソフトウェア・制御・AI といった多様な学術分野の協働が必要となるため、学術分野融合の基礎となる数理的（メタ）理論も重視して研究を推進する。略称は ERATO MMSD。プロジェクト詳細は https://www.jst.go.jp/erato/hasuo/ja/参照。2022 年 3 月に本研究期間を終了し、現在は追加支援期間として研究を推進中（2025 年 3 月まで）。

（*2） 形式論理学：数学における証明を研究の対象とする数学の一分野。主要な応用としては、証明を書きやすくする論理体系の設計や、証明を書いてチェックするためのソフトウェアの実装などが挙げられる。チューリングマシンをはじめ現代の計算機ももともとは形式論理学から生まれた。

（*3） ハイブリッドシステム： 計算機によるデジタル・離散的ダイナミクスと、物理系によるアナログ・連続的ダイナミクス、これら両方の性質をあわせ持つ動的システムのこと。現代の工業製品のほとんどはマイコン制御されているので、ハイブリッドシステムの例になっている。

(*4) MIRAI eAI プロジェクト： JST における「未来社会創造事業　サイバー世界とフィジカル世界を結ぶモデリングと AI　超スマート社会の実現」（本格研究）に採択されている研究プロジェクトで、自動運転をはじめとして深層学習技術を用いた AI システムの安全性・信頼性確保・向上のため、細やかなニーズに応える AI の構築や修正が可能な技術に取り組む。正式名称は「機械学習を用いたシステムの高品質化・実用化を加速する"Engineerable AI"技術の開発」、研究代表者は NII アーキテクチャ科学研究系准教授 石川 冬樹。プロジェクト詳細は https://engineerable.ai/参照。

(*5) CREST CyPhAI プロジェクト： JST における「CREST 数学・数理科学と情報科学の連携・融合による情報活用基盤の創出と社会課題解決に向けた展開」に採択されている研究プロジェクトで、AI を構成要素として含む CPS（AI-CPS）の安全性・信頼性の担保のため、数学に基づく強固な形式的設計手法の研究に取り組む。正式名称は「AI 集約的サイバーフィジカルシステムの形式的解析設計手法」、研究代表者は京都大学大学院情報学研究科准教授・NII 客員准教授 末永 幸平。NII 情報学プリンシプル研究系准教授 岸田 昌子も主たる共同研究者として参画。プロジェクト詳細は https://www.cyphai.io/参照。

(*6) CREST ZT-IoT プロジェクト： JST における「CREST 基礎理論とシステム基盤技術の融合による Society 5.0 のための基盤ソフトウェアの創出」に採択されている研究プロジェクトで、形式検証とシステムソフトウェアの融合により、ゼロトラスト(ZT)の概念を踏襲した安全な IoT システムの実現を目指す。正式名称は「形式検証とシステムソフトウェアの協働によるゼロトラスト IoT」、研究代表者は NII アーキテクチャ科学研究系教授 竹房 あつ子。NII アーキテクチャ科学研究系助教 関山 太朗も主たる共同研究者として参画。プロジェクト詳細は https://zt-iot.nii.ac.jp/参照。

(*7) 本研究の内容は、マツダ株式会社の現在の製品には何ら関係ありません。