自動運転システムの形式検証手法の確立に向けて

Towards the Establishment of Formal Verification Methods for Autonomous Driving Systems

冨田 尭 (Takashi Tomita)[1]

[1] 北陸先端科学技術大学院大学 (Japan Advanced Institute of Science and Technology)
e-mail: tomita@jaist.ac.jp

1　概要

近年，自動運転システムの実用化に向けた研究開発や実証実験が活発に行われている．安全安心なモビリティ社会の実現のためには，自動運転を構成する認識，判断・経路計画，制御などすべての要素を包括した合理的かつ実行可能な仕様・シナリオ記述方法や検証・テスト方法が必須である．

本講演では，自動運転システムの安全性・信頼性を保証するための形式手法及び検証ツールの開発に向けた取り組みについて紹介する．

数理的技法による情報セキュリティの 2024 年度後半&2025 年度前半の研究動向

Research Trends in the Formal Approach to Information Security in the Second Half of FY2024 and the First Half of FY2025

荒井 研一 (Arai Kenichi)[1], 鈴木 幸太郎 (Suzuki Koutarou)[2], 中林 美郷 (Nakabayashi Misato)[3], 花谷 嘉一 (Hanatani Yoshikazu)[4], 三重野 武彦 (Mieno Takehiko)[5], 山本 光晴 (Yamamoto Mitsuharu)[6], 吉田 真紀 (Yoshida Maki)[7], 米山 一樹 (Yoneyama Kazuki)[8]

[1] 長崎大学 (Nagasaki University), [2] 豊橋技術科学大学 (Toyohashi University of Technology), [3]NTT 社会情報研究所 (NTT Social Informatics Laboratories), [4] 株式会社 東芝 (Toshiba Corporation), [5]EPSON AVASYS 株式会社 (EPSON AVASYS CORPORATION), [6] 千葉大学 (Chiba University), [7] 情報通信研究機構 (National Institute of Information and Communications Technology), [8] 茨城大学 (Ibaraki University)

e-mail : [3]misato.nakabayashi@ntt.com

1 はじめに

数理的技法は暗号プロトコルやシステムの安全性検証など，情報セキュリティの様々な分野で応用されている．本発表では，数理的技法による情報セキュリティに関する 2024 年度後半&2025 年度前半の研究動向として，2024 年 9 月から 2025 年 8 月までに開催されたトップ会議における関連論文の発表件数や特色，概要について紹介する．さらに，全体を通したトレンドや特に注目されている分野と論文を紹介する．

2 調査した会議と関連論文の件数

本発表のために調査した会議と関連論文の件数は以下の通りである．なお，関連論文は論文のタイトルおよびアブストラクトから抽出している．

2.1 The ACM Conference on Computer and Communications Security (CCS) [6]

セキュリティ 4 大会議の一つ．暗号寄りの理論的な発表と実利用システム対象の実用的な発表がバランスよく含まれる．形式手法を用いた事例研究が盛ん．2024 年度は 15 件の関連論文が発表された．

2.2 Symposium on Security and Privacy (S&P) [1]

セキュリティ 4 大会議の一つ．理論的・実用的両方の発表が含まれるが，より実用を意識した発表が多い．数理的技法を用いた事例研究が盛ん．2025 年度は 1 件の関連論文が発表された．

2.3 USENIX Security [2]

セキュリティ 4 大会議の一つ．評価実験による実証を伴う実利用システムの安全性解析に関する発表が多い．数理的技法分野ではツールに関する発表が多く見られる．2025 年度は 7 件の関連論文が

発表された．

2.4 The Network and Distributed System Security Symposium (NDSS) [3]

セキュリティ 4 大会議の一つ．特に分散環境下でのシステムなどの安全性解析や安全な開発に関する実用的な発表が多い．数理的技法分野の応用は少ない．2025 年度の関連論文は 4 件であった．

2.5 Computer Security Foundations Symposium (CSF) [4]

数理的技法によるセキュリティを主要なフォーカスの一つとした歴史ある会議．その後の研究に大きな影響を与えるような理論的な成果が集まる．フレームワークの提案や拡張，性質の証明，理論的限界の解明などに関する発表が多い．2025 年度は 13 件の関連論文が発表された．

2.6 International Conference on Computer Aided Verification (CAV) [5]

1980 年代から続く形式検証分野のトップ会議．検証の基礎となる理論から応用までを幅広くカバーする．例年セキュリティのセッションもある．2025 年度の関連論文は 5 件であった．

参考文献

[1] 46th IEEE Symposium on Security and Privacy Web Page, `https://sp2025.ieee-security.org/`.

[2] 34th USENIX Security Symposium Web Page, `https://www.usenix.org/conference/usenixsecurity25`.

[3] The Network and Distributed System Security (NDSS) Symposium 2025 Web Page, `https://www.ndss-symposium.org/ndss2025/`.

[4] 38th IEEE Computer Security Foundations Symposium Web Page, `https://csf2025.ieee-security.org/`.

[5] 37th International Conference on Computer Aided Verification Web Page, `https://conferences.i-cav.org/2025/`.

[6] The 31st ACM Conference on Computer and Communications Security (CCS) Web Page, `https://www.sigsac.org/ccs/CCS2024/`.

