SCIS 2022 2022 Symposium on
Cryptography and Information Security
Osaka, Japan & Online, Jan. 18 – 21, 2022
The Institute of Electronics,
Information and Communication Engineers

人工知能搭載システムに対する安全性論証の現状と セキュリティ論証に向けた課題 ～自動運転システムの例～

Current Status of Safety and Security Assurance for System using AI

溝口 誠一郎 * 櫻井 幸一 †
Seiichiro Mizoguchi Kouichi Sakurai

キーワード 人工知能，安全論証，サイバーセキュリティ論証，自動車

あらまし

人工知能はその適用先を広げ，日常の様々なシーンで利用されている．その役割は，システム外部からの情報の分析であり，その分析結果がシステムの振る舞いを決める，所謂，意思決定のために利用されることも多い．そのため，倫理的な理由などにより，人工知能を用いるサービスやシステムについて，その説明責任を問われる場合もある[1][2].

自動車分野において，自動運転技術の領域でも同様の議論がなされる．例えば，自動運転中に起きた事故は誰の責任かという問題である．これには，そのシステムがどういう入力を元にどういう出力をしたかを説明できなければ，その落としどころを議論することはできない．

技術的な側面から，システムの安全性を論証する規格として，機能安全[3]や SOTIF[4]がある．機能安全は，E/E システムの故障に着目し，故障が発生しても安全機構により安全目標侵害を防止するという方針で，安全性に関わるリスクを許容できるレベルまで下げることを目的としている．さらに SOTIF では，機能安全が主な対象とする故障だけでなく，意図した機能の仕様の不十分性，性能限界，又は合理的に予見可能なミスユースから生じる危険事象のリスクを許容できるレベルまで下げることが目的である．

これらの論証は，システムのコンセプトから，システムのハードウェアやソフトウェアの実装のレベルまで分析の対象となっているが，最近では，システムの振る舞いがソフトウェアに大きく依存するようになった．そのため，システムの信頼性を語る上で，ソフトウェアの管理はより重要となり，併せてサイバーセキュリティ対策も重要となった. これは, システムの安全性を語る上で, ソフトウェアの信頼性やセキュリティはそのベースとなるからである.

法規の側面では，自動車の場合，自動車が持つ機能，およびそれを実現する装置単位で安全に関する技術基準が保安基準として定められている．例えば，Automated Lane Keeping System は, UN-R157[5]として WP.29[6]によって定められ，各国の保安基準として採用されている．そして，安全性のベースとなるセキュリティとソフトウェア管理については，同じく UN-R155[7]と UN-R156[8]として組織レベルでの対応が求められている．本稿では，これらの法規と照らし合わせて，AI を利用したシステムの安全性とサイバーセキュリティ論証に取り組むうえでの課題について述べる．

* DNV ビジネスアシュアランスジャパン株式会社, DNV Business Assurance Japan
† 九州大学大学院システム情報科学研究院, Kyusyu University

参考文献

[1] ENISA, https://www.enisa.europa.eu/
[2] Responsible AI Guidelines, https://www.diu.mil/responsible-ai-guidelines
[3] ISO-26262, Road Vehicles – Functional Safety
[4] ISO/PAS 21448, Road vehicles — Safety of the intended functionality
[5] UN-R157 – Automated Lane Keeping Systems
[6] The UNECE World Forum for Harmonization of Vehicle Regulations, https://unece.org/wp29-introduction
[7] UN-R155 – Cyber security and Cyber security management system
[8] UN-R156 – Software Update and software update management system