

研究タイトル：

高信頼で安全なソフトウェアに関する研究



氏名： 岡本 圭史 / OKAMOTO Keishi E-mail: okamoto@sedai-nct.ac.jp

職名： 准教授 学位： 博士(理学)

所属学会・協会： 日本ソフトウェア科学会, 日本数学会

研究分野： 数理論理学, モデル理論, 離散構造・数学的基礎, ソフトウェア工学

キーワード： 数理論理学, 数理議論学, 形式手法, 安全分析

 技術相談
 提供可能技術：

- ・数理論理学・数理議論学に基づくモデル化支援
- ・形式手法(形式仕様記述, モデル検査, SAT/SMT ソルバ等)の技術指導, 導入支援
- ・安全分析手法: STAMP/STPA の講習会実施, 導入支援

研究内容：

数理論理学・数理議論学に関する研究

形式手法の背景理論である数理論理学に関する研究を実施している。具体的には、形式手法のための数理論理構築やその数学的研究の証明に関する研究を実施。最近は、数理論理学の拡張である、数理議論学に関する研究も実施し、最近では以下の成果をまとめた。

1. A Bayesian Approach to Argument-Based Reasoning for Attack Estimation, Hiroyuki Kido and Keishi Okamoto, 2017年8月, Proceedings of the Twenty-Sixth International Joint Conference on Artificial Intelligence, IJCAI-17, pp.249-255
2. Balancing Between Cognitive and Semantic Acceptability of Arguments, Hiroyuki Kido and Keishi Okamoto, 2017年7月19日, Knowledge Science, Engineering and Management: 10th International Conference, KSEM 2017, Melbourne, VIC, Australia, August 19-20, 2017, Proceedings (Lecture Notes in Computer Science), pp.160-173

形式手法

高信頼なソフトウェア開発で用いられている形式手法に関する研究を実施している。具体的には、モデル検査法の応用や、SMT ソルバを用いたテストケース自動生成に関する研究を実施。最近は、形式仕様記述言語 VDM++ からプログラミング言語 C# への制約条件を含めた変換ツール開発に取り組んでいる。形式手法に関する企業への導入支援も行っている。

安全分析手法: STAMP/STPA

ソフトウェアや人間系を含めた複雑なシステムの安全分析に適していると言われる安全分析手法 STAMP/STPA に関する事例研究や自動化に関する研究に取り組んでいる。情報処理推進機構・ソフトウェア高信頼化推進委員会・システム安全性・信頼性分析手法 WG 委員として、STAMP/STPA の国内への普及活動にも携わり、以下の成果をまとめた。

1. STAMP ベース・ハザード分析支援ツールの概説と i-STAMP 紹介, 岡本圭史, 2017年11月17日, Embedded Technology 2017 SEC 先端技術入門ゼミ, パシフィコ横浜
2. STAMP/STPA チュートリアル(入門編), 岡本圭史, 2017年7月12日, ET-WEST2017 SEC 先端技術入門ゼミ, グラフフロント大阪
3. はじめての STAMP/STPA(実践編)～システム思考に基づく新しい安全性解析手法～(5章: STPA 支援手法執筆), 兼本茂, 岡本圭史他, 2017年5月25日, 独立行政法人情報処理推進機構, ISBN 978-4-905318-51-4
4. はじめての STAMP/STPA ～システム思考に基づく新しい安全性解析手法～, 荒木啓二郎, 岡本圭史他, 2016年4月28日, 独立行政法人情報処理推進機構 他

提供可能な設備・機器：

名称・型番(メーカー)

名称・型番(メーカー)	