

特集

フォーマル メソッドの 新潮流

編集にあたって

塚田恭章 ● 日本電信電話(株)
NTTコミュニケーション科学基礎研究所

本号では、数理論理学を応用してシステムの高い信頼性を確保する技術であるフォーマルメソッドを特集する。フォーマルメソッドについては、何十年も前からいろいろとあちらこちらで特集が組まれてきたかもしれない（それほどまでにフォーマルメソッドは重要なテーマであるといえる）。その一方で、50年後、いやひょっとしたら100年後も引き続き特集が組まれるような気がしてならない（それほどまでにフォーマルメソッドは難しいテーマであるともいえる）。しかし、いま、フォー

ルメソッドは確実に新しい展開を見せているように思う。10年前には感じられなかった、それでいて10年後を大いに期待させる新潮流—そのフォーマルメソッドの「いま」を読者に伝えることが本特集の目的である。

本特集で扱うフォーマルメソッドの新潮流には大きく分けて2つある。1つは、フォーマルメソッドが産業界からも注目を集め、実際に使われるようになってきたという点である¹⁾。以前は大学の研究室で実験的に使用されてきたフォーマルメソッドが、社会基盤となるような

重要な情報システムの構築に使われるようになってきている。欧米に遅れをとっていたフォーマルメソッドの産業界への応用が、国内でも本格的に活性化し始めた。新しい潮流のもう1つは、今までになかったような新しい領域にフォーマルメソッドが適用されるようになってきたという点である。ハードウェア・ソフトウェアといった伝統的な対象はもとより、社会や法、プライバシーやセキュリティなど、いまフォーマルメソッドの適用領域は急速に拡大しつつある。

上記の2つの潮流を伝えるべく、本特集を以下の3つのパートから構成した。

Part I：歴史と概要

1. フォーマルメソッドの過去・現在・未来—適用の実践に向けて—

Part II：産業界への応用

2. フォーマルメソッドのフィールドワーク
3. 携帯電話組込み用モバイル FeliCa IC チップ開発における形式仕様記述手法の適用
4. C 言語へのフォーマルメソッドの適用

Part III：新領域の開拓

5. フォーマルメソッドの新展開—検証進化可能電子社会の中核技術—
6. 匿名性とプライバシーのためのフォーマルメソッド
7. フォーマルメソッドによる暗号安全性

本特集は荒木啓二郎氏(九州大学)の「フォーマルメソッドの過去・現在・未来—適用の実践に向けて—」で幕を開ける。歴史的な視点からフォーマルメソッドを概観し、過去の盛衰や現在につながる新しい流れ、さらには未来への可能性について紹介する。

Part II「産業界への応用」では、形式仕様記述・モデル検査・定理証明などフォーマルメソッドの各種技法について、それぞれの産業界への応用例を紹介する。木下佳樹氏・高井利憲氏・大崎人士氏(産業技術総合研究所)による「フォーマルメソッドのフィールドワーク」は、組込みシステムをはじめとするシステム開発の現場へのフォーマルメソッドの導入実験について、豊富な実例をもとに紹介したものである。栗田太郎氏(フェリカネットワークス(株))による「携帯電話組込み用モバイル FeliCa IC チップ開発における形式仕様記述手法の適用」は、実際のシステム開発の現場でフォーマルメソッドを実践された立場から、その効果について解説する。宮崎義昭氏・橋本祐介氏(日本電気(株))による「C 言語へのフォーマルメソッドの適用」は、C 言語で記述されたソースコードをモデル検査する技術と、その社内プロジェクトへの適用事例の解説である。

Part III「新領域の開拓」では、フォーマルメソッドの新しい適用分野である社会、匿名性・プライバシー、暗号などについて紹介する。二木厚吉氏(北陸先端科学技術大学院大学)による「フォーマルメソッドの新展開—検証進化可能電子社会の中核技術—」は、フォーマルメソッドをベースに電子社会の健全性、安全性・安心性、進化可能性を確保する試みについての解説である。真野健氏(日本電信電話(株))による「匿名性とプライバシーのためのフォーマルメソッド」は、匿名性やプライバシーといった新しいセキュリティにまで適用領域を拡大しつつあるフォーマルメソッドの解説である。萩谷昌己氏(東京大学)による「フォーマルメソッドによる暗号安全性」は、近年世界的に研究が活性化している、フォーマルメソッドと暗号理論との境界領域についての解説である。

本特集は、新しい展開を見せるフォーマルメソッドの最近の話題を紹介するものであるが、技術領域としてのフォーマルメソッドをすべてカバーするものではない。より包括的な優れた解説として、中島震氏による文献2)をおすすめする。信頼度の高いシステムを構築するアプローチに興味のある学生や、企業において高信頼システムの研究開発に従事する読者が、本特集を通じてフォーマルメソッドへの関心を少しでも高めていただければ大きな喜びである。

【補足：本特集で用いられる用語について】

非常に残念なことではあるが、英語の「formal methods」に対応する決定的な日本語が今なお存在しないのが実状である。「フォーマルメソッド」、「形式手法」、「数理的技法」などの訳語が各人の流儀で用いられている。本特集では、特集タイトル・各記事タイトルまでは「フォーマルメソッド」で統一し、各記事の本文中では執筆者に日本語の選択をお任せした。ただし、「形式的な手法」は、読者に誤解を与える可能性があるため、使用を控えていただいた。「形式的」という日本語が「形式だけで内容がなく役に立たない」という意味合いを時として強く持つためである。

謝辞 本特集の編集にあたっては、本誌編集委員の佐伯元司氏(東京工業大学)に、企画から閲読まで多岐にわたって多大なる支援を頂戴した。ここに深く感謝したい。

参考文献

- 1) 北郷達郎：特集 バグ・ゼロ目指し脚光浴びる「形式手法」、日経コンピュータ 2006年7月24日号, pp.60-64 (2006).
- 2) 中島 震：ソフトウェア工学の道具としての形式手法, NII テクニカルレポート NII-2007-007J (2007). <http://research.nii.ac.jp/TechReports/07-007J-j.html>

(平成 20 年 4 月 2 日)