製品ライフサイクルでの高信頼化技術

Advanced Technologies for System Dependability through the Product Life Cycle

巻頭言

形式手法に基づく高信頼システムのライフサイクル管理

Life Cycle Management of Dependable Systems Based on Formal Methods

片山　卓也
KATAYAMA Takuya

高信頼情報システムの開発における形式手法への期待が大きくなっています。形式手法は，システムの仕様を数学的な記法により明確に記述し，その検査や検証を機械的に行うことで，システムの信頼性を高めようとする技術です。高信頼システムの開発には，利用環境の把握とそれに基づくシステム設計，及び設計内容の明確な記述と解析が必要であることを考えれば，形式手法に対する期待の高さが理解できます。形式手法が，特に欧米などで，一部の先進的なシステムの開発に使われ，その成功が広く知れわたったこともその原因であろうと思われます。

しかしながら，現実の商用システムの開発に形式手法が使われているかというと，これは必ずしも正しくありません。形式手法導入のバリアとしてよく言われることは，形式仕様記述言語が一般技術者にはなじみがなく，形式検証ツール，特に定理証明ツールの利用が困難なことです。モデル検査ツールのような自動化ツールについては多少事情が異なりますが，検証ツールに関してはより使いやすくするための技術開発が必要であると考えます。

一方，形式仕様記述言語については，もしそれが実行可能言語であれば，形式検証ツールの利用を待たずとも信頼性の高い仕様を獲得することは可能です。事実，そのような方法により，高信頼システムの開発に成功している事例は少なくありません。このような利点があるにもかかわらず，いまだ産業界がその利点を享受できない理由は，ソフトウェア ライフサイクル全体を通じた開発管理体系のなかに，それを組み入れることが容易でないことによるものと思われます。多くの基幹的ソフトウェアは，要求や運用条件の変更などに対応して進化し続ける必要があります。それらのライフサイクルのなかで常に変更され続けるのが通常の姿であり，そのための運用管理体系のなかで利用されています。

既存の運用管理体系のなかに新しい技術を導入することが簡単でないことは理解できますが，形式手法の導入は，この運用管理体系全体を系統的に構築し，運用管理コストを大幅に低減させる可能性を高めます。明確な記述に基づくシステムの解析可能性と形式的解析ツールの利用により，従来よりも系統的で質の高いソフトウェア ライフサイクル管理が可能になると考えられます。これこそが，形式手法がもっとも貢献できることであると思っています。

北陸先端科学技術大学院大学　学長，工学博士　　President, Japan Advanced Institute of Science and Technology