

## 形式的仕様記述を用いた

# 高信頼ソフトウェア開発プロセスの研究を開始

～名古屋と北海道を形式手法に基づくソフトウェア開発の先進地域に～

(株)ヴィッツは、北海道を拠点としている(地独)北海道立総合研究機構 産業技術研究本部、北海道電子機器(株)、(株)マイクロソフトウェア、(株)リック、北海道大学大学院情報科学研究科、(独)産業技術総合研究所らとコンソーシアムを形成し、名古屋大学大学院情報科学研究科附属 組込みシステム研究センター、苫小牧工業高等専門学校、株式会社日本除雪機製作所、北海道日本電気ソフトウェア株式会社、トヨタ自動車株式会社、アイシン精機株式会社、ルネサスエレクトロニクス株式会社らのアドバイザ協力を得て、形式的仕様記述を用いた高信頼組込みソフトウェア開発に関するプロジェクトを開始します。本プロジェクトは、経済産業省北海道経済産業局 平成 22 年度戦略的基盤技術高度化支援事業に採択されております。

我が国の得意分野である電子機器開発において、組込みソフトウェアの開発規模は爆発的に増大しています(例えば、自動車ソフトウェアは 8 年で 19 倍もの規模拡大が進んでいる、との報告があります)。そのため、従来型のソフトウェア開発技法では品質維持に期間と工数を要し、困難となりつつあり、組込みソフトウェアに起因する課題が顕在化しつつあります。こうした問題を解決するため、本プロジェクトでは、高品質・高信頼性ソフトウェア開発のための有力な技術の一つである「形式手法」に着目し、組込みソフトウェア開発に対する適用ノウハウの確立と、国内ソフトウェア開発現場への技術普及を目指します。

形式手法とは、ソフトウェアの仕様や設計を、数学、論理学に基づく形式的な表現を用いて表現することで記述の曖昧さを排除したり(形式的仕様記述)、その記述内容の正しさを数学的理論に基づいて検証したり(形式検証)することによって、より高い品質のソフトウェア開発を実現する手法です。形式手法の考え方自体の歴史は古く、1970 年代から大学レベルでは様々な手法が研究されてきましたが、数学理論などの専門知識が必要であり、企業のソフトウェア開発現場への技術普及は進んでいませんでした。

しかし、欧州を中心とする産業界では地道な取り組みが続けられ、1990 年代頃から鉄道や航空宇宙などの高信頼システムを中心に実製品開発への適用が徐々に進んでいます。また、欧州主導で策定された国際規格(機能安全規格 IEC 61508 など)では、特に高い水準の安全性が必要な製品での形式手法の適用が義務づけられるといった動きもあり、我が国の産業界としても技術対応が求められる状況となっています。

本プロジェクトでは、自動車部品の制御ソフトウェアや TCP/IP 通信ミドルウェアなど既存の実ソフトウェア製品の要求仕様に基づき、「B メソッド」「VDM」などの形式的仕様記述手法を試験導入しながらソフトウェアの再開発を行います。その結果を基に、形式仕様記述使用を前提としたソフトウェア開発プロセスや要員スキル評価の枠組みを構築すると共に、従来型手法に基づく開発結果と比較し改善効果の評価を行います。また、試験導入や効果分析で得られた知見に基づき、形式的仕様記述の導入を補助する支援ツールや、技術者向け教育教材などの形での製品化を行います。これにより、国内ソフトウェア業界への形式的仕様記述の技術普及を加速させ、北海道を中心とし全国に広がる形式手法の高度活用企業グループの形成を目指します。

本研究で得られる成果にもとづき形式仕様記述技術の活用をすすめることによって、現在の組込みソフトウェア開発が抱える以下の問題を軽減または解決することが出来ます。

### (1) 上流工程の不具合の早期発見・除去

現在のソフトウェア開発プロセスでは、要求定義や設計などの上流工程で混入した不具合が、下流工程に至るまで発見されず、その修正のために大きな手戻りが発生し開発コスト増大の要因となっています。上流工程から形式仕様記述を導入する事で、不具合を上流工程の段階で早期発見・除去する事が可能となり、製品品質の向上と手戻りによる開発工数・コストの削減に寄与します。

### (2) 高信頼機能安全規格への対応

機能安全国際規格 IEC 61508 では、要求される安全度に応じて 4 段階の SIL(安全度水準)を定めていますが、

最も高い SIL4 では設計段階からの形式手法の利用が規格で義務づけられています。そのため、鉄道、航空宇宙、原子力など高信頼が要求される製品の輸出企業においては、今後、形式手法への対応が必須になることが予想されます。

### **アイシン精機株式会社 第一電子系技術部 鈴木延保氏からのコメント**

今回のプロジェクトにより、車載組込みソフトウェア開発の要件定義、設計における形式仕様記述の活用が促進される事を期待します。

車載組込みシステムの高信頼化、効率化の課題は多岐に渡っていますが、そのため近年は設計の厳密性がより求められる傾向にあります。現在の「MISRA-C コーディングルール」や「モデルベース開発」の普及もその流れの一環ですが、今後は上流のアーキテクチャ設計や仕様書記述での厳密性強化が更に進み、その延長として形式仕様記述への対応が重要になってくると認識しています。

本プロジェクトの成果が国内の車載組込みソフト開発における形式仕様記述活用が早期に普及する起爆剤となる事を期待し、製品適用に向けたアドバイスや検証にご協力したいと思います。

### **北海道日本電気ソフトウェア株式会社第二ソリューション事業部 第一システム部長 鶴見直樹氏からのコメント**

コンピュータが重要な社会インフラを担う中、ソフトウェアの品質は、社会に対して大きな影響を与えるまでに至っています。形式手法は、これまでのソフトウェアの曖昧性を排除し、ソフトウェアの品質を飛躍的に向上させる手法として、非常に大きな意味を持つと考えます。しかし、形式手法を現場で適用するためには、まだハードルが高いのも事実です。この研究では、ツールや教育プログラムの開発を行うことで、形式手法を実際の現場で適用するための道筋を付ける物と期待しています。メーカーの立場として、実際の現場で適用する立場からコメントするなど、ご協力したいと考えています。

### **北海道大学大学院情報科学研究科 教授 栗原正仁氏のコメント**

このような時代が来るとは驚きです。60年ほど前から地道に研究されてきた「ソフトウェア科学」と「人工知能」の技術がいま合体して、「形式手法」という「ソフトウェア工学」の実用技術として、産業界の現場の技術者に受け入れられようとしています。これはソフトウェアの「職人芸」的な世界に「科学」と「人間の理性」を導入した革命的な出来事かもしれません。今後は、形式手法が、「確かなソフトウェアを作れるが、特殊で手間がかかる手法」ではなく、「確かなソフトウェアを作ることができる、普遍的で効率の良い手法」として北海道から発信できるよう、研究に取り組んでいきたいと思っています。

### **株式会社ヴィッツ 代表取締役 脇田周爾のコメント**

今回採択された研究事業は、当社が注力しております自動車産業、次世代ロボット産業、産業機械産業や機能安全事業にとって大変重要なテーマであり、全社一丸でこの研究事業を成功させたいと考えております。

当社は、平成18年度の戦略的基盤技術支援事業に採択をいただき、その研究途中から関連事業の事業化を実現し、また、研究終了後に国際認証機関（ドイツ TÜV-SÜD）から開発成果を利用した機能安全プロセス認証を取得しています。今回取り組む形式手法の実践的活用技術は、我が国の組込ソフトウェアの品質、信頼性を今後も維持しつづけるため不可欠となる技術です。本事業の活動により、形式手法実践に関する先導的企業グループを確立し先進地域とすべく、尽力していきたいと思っています。

### **問い合わせ先**

本発表に関するお問い合わせは、以下をお願いします。

株式会社ヴィッツ

総務部：安場、佐藤（技術的内容；組込制御開発部：服部）

TEL: (052) 220-1218