2010 年 11 月 24 日

ディペンダブル・ソフトウェア・フォーラムが成果第一弾を公開

～エンタプライズ系で初めて形式手法活用ガイドを公開～

株式会社ＮＴＴデータ
富士通株式会社
日本電気株式会社
株式会社日立製作所
株式会社東芝
大学共同利用機関法人　情報・システム研究機構　国立情報学研究所

株式会社ＮＴＴデータ、富士通株式会社、日本電気株式会社、株式会社日立製作所、株式会社東芝の 5 社と、大学共同利用機関法人 情報・システム研究機構 国立情報学研究所（※1）が参加するディペンダブル・ソフトウェア・フォーラム（Dependable Software Forum、略称名は DSF）は、活動成果の第一弾として、エンタプライズ（※2）市場向けのソフトウェアを対象とした初めての形式手法活用ガイドを、本日より DSF 公式ホームページに公開します。本ガイドは、エンタプライズ系ソフトウェアを開発するプロジェクトメンバが実際の開発場面に形式手法（※3）を導入するときの参考になると期待します。

DSF 公式 Web サイト
http://www.nttdata.co.jp/dsf/

現在、社会システムはより高信頼・高品質が求められています。また、自動車や家電等のハードウェアに組み込まれる組込み系ソフトウェアを中心に、形式手法を適用した開発を推奨する動きがあり、形式手法に注目が集まっています。そこで、2009 年 12 月に DSF を設立し、具体的に活動するワーキンググループである形式手法適用評価 WG（Formal Methods Application WG、略称名は FMAWG）の中で、形式手法適用事例、及びノウハウを蓄積してきました。

形式手法活用ガイドは、ディペンダブル・ソフトウェア（※4）実現の有力な手段である形式手法を実際の開発現場で有効に活用するために各参加企業が連携して作成しています。

形式手法はエンタプライズ系ソフトウェアの開発に適用する場合のコストが膨らむという固定観念と活用できる技術者の不足のため、適用事例が少なく、その効果も一般に公開されていません。そこで、DSF は適用効果を確かめるべく記述実験を行い、形式手法がエンタプライズ系ソフトウェア開発上流工程での誤り発見に効果があることを確認しました。具体的には、レビューによって誤りが除去されたと考えられる設計書を形式手法で記述し直すことにより、複数の設計書で書かれている内容の矛盾や仕様の解釈が複数あるという誤りを新たにいくつか発見することができました。

また、同時に上記実験の結果、形式手法の実務への適用には以下 4 点の課題が重要であることが分かりました。

課題 1. 現場利用を踏まえた適用手順や体制

課題 2. 形式手法を用いる際の定石や作法の知識

課題 3. 形式手法に関するスキルや教育方法

課題 4. より現実的な開発場面での効果や利点・欠点

DSF は上記のうち、課題 1～3 について対策を検討しました。

- 課題 1 に対して、エンタプライズ系ソフトウェア開発の上流工程における、要件定義工程の次段階である設計工程に対して、形式手法の適用手順をまとめました。
- 課題 2 に対して、エンタプライズ系ソフトウェア開発で想定される一般的な設計書の形式記述作成方法に対して、典型的な解決例一覧と、一部、具体例を含む詳細な書き方の解決例を記述しました。
- 課題 3 に対して、スキル教育で必要なスキルマップやセミナプログラムを設定し、DSF メンバを対象としたセミナを実施して評価しました。

【形式手法活用ガイドについて】

形式手法活用ガイドの個々の説明は以下の通りです。

項番	名称	説明
1	形式手法活用ガイドの紹介	・2010 年 11 月時点での各々のガイド項番 2～5 の位置付けとその概要を説明
2	図書館システム記述実験報告書	・技術者育成の教材である図書館システム設計書を読解して、形式手法による記述を行い、設計書の誤りを抽出した実験報告書 ・設計書の誤りを見つけることができるという形式手法の効果の一事例報告として利用可能
3	形式手法適用手順例	・形式手法の 1 つである Event-B（※5）の適用手順例を解説したもの ・ソフトウェア開発プロジェクトに合わせて効果的な適用手順を見つける参考例として使用することを想定
4	形式手法イディオム集（※6）	・エンタプライズ系ソフトウェアにおける形式記述の典型的な表現（Event-B 版と SPIN（※7）版） ・設計書の内容を形式記述で作成する場面で参考にすることを想定 ・形式記述を作成する人による記述方法の違いを最小化し、形式記述の品質を高めることを狙う
5	形式手法スキルアップセミナ報告書	・形式手法を実践するスキルを教育するときに参考になる報告書 ・スキルマップや教育プログラムの作成、スキルレベルの評価等を形式手法の 1 つである Event-B に対して行ったもの ・形式手法スキル教育の一事例報告として利用可能

【今後の活動について】

今後、DSF は、「課題 4. より現実的な開発場面での効果や利点・欠点」の対策として、より開発現場に近い場面を想定して形式手法適用の有効性を評価する実証実験を企画します。また、今回公開した成果を実証実験で利用するために、イディオム集の充実、及び形式手法適用手順のさらなる具体化等の改善を図ります。そして、実証実験を通して成果の妥当性や形式手法効果の実証を図り、2011 年度末に実証実験結果を反映させた最終成果を提供する予定です。

【「形式手法適用評価 WG（FMAWG)」について】

FMAWG は、ディペンダブル・ソフトウェア実現の有力な手段である形式手法に着目し、具体的な検討活動を行うワーキンググループです。FMAWG は、実際の開発現場で有効に活用できる形式手法の適用事例や適用ノウハウを蓄積・公開し、形式手法を適用したシステム開発の可能性を追求する WG です。

【注釈】

（※1）株式会社ＮＴＴデータ、富士通株式会社、日本電気株式会社、株式会社日立製作所、株式会社東芝の 5 社と大学共同利用機関法人 情報・システム研究機構 国立情報学研究所

株式会社ＮＴＴデータ（代表取締役社長：山下　徹)、富士通株式会社（代表取締役社長：山本　正已)、日本電気株式会社（代表取締役 執行役員社長：遠藤 信博)、株式会社日立製作所（執行役社長：中西　宏明)、株式会社東芝（取締役 代表執行役社長：佐々木　則夫）の 5 社と、大学共同利用機関法人 情報・システム研究機構 国立情報学研究所（所長：坂内　正夫）

（※2）エンタプライズ

企業活動を営むための業務システムや社会基盤を支える情報システムのこと。

（※3）形式手法（フォーマルメソッド，Formal Methods）

数理論理学を基盤として、対象システム・ソフトウェアの機能・振舞いについて正確な記述と系統的な検証を行う手法・技術の総称。対象を厳密に記述することにより、要求や設計の矛盾、抜け漏れ等の誤りに気付く。さらにツールを用いて検証することにより、要求や設計の矛盾、抜け漏れ等の誤りを発見することができる。

（※4）ディペンダブル・ソフトウェア（Dependable Software）

利用者が信頼・安心して利用できる、頼りになるソフトウェアであり、可用性、信頼性、安全性、機密性、完全性、保守性といった複合的要件を満足する。

- 可用性（Availability）：利用者がシステムを使用し続けることができる性質

- 信頼性（Reliability）：システムのハードウェアやソフトウェアが故障する頻度
- 安全性（Safety）：システムが人間や環境に危害を及ぼす度合い
- 機密性（Confidentiality）：アクセスを許可された者だけがシステムで管理する情報にアクセスできること
- 完全性（Integrity）：システムで管理する情報を保護して、正確かつ完全である（改ざんされない）こと
- 保守性（Maintainability）：システムが故障したときの修理のしやすさのこと

（※5）Event-B

システムの分析、設計を行う形式手法。集合論と一階述語論理と呼ばれる数学の概念を用いて仕様を表現し検証する。特に、仕様を段階的に詳細化、具体化する過程で正しさを検証する作業を繰り返し行う。欧州連合（European Union）のフレームワークプログラム（FP) 7 支援研究プロジェクト DEPLOY が統合仕様開発ツール RODIN を開発し無償公開している。

（※6）イディオム

ソフトウェアにおける形式記述の典型的な表現。

（※7）SPIN

モデル検査法と呼ぶ自動検証の方法を提供するツール。G.J. Holzmann 博士が開発、無償公開しており、国内の産業界ならびに大学等の教育機関でも関心が高い。分散システムなどの並行システムの表現を記述すること、ならびに自動検証に向いている。調べることができる性質としては「デッドロックが発生しない」といった基本的なものに加えて、線形時相論理と呼ばれる形式で表現した処理進行に関わる性質がある。

【本件に関するお問い合わせ先】
株式会社ＮＴＴデータ　技術開発本部　吉田・塚本　TEL：050-5546-9729
富士通株式会社　システム生産技術本部　銀林　TEL：03-6424-6276
日本電気株式会社　ソフトウェア生産革新部　岩崎　TEL：03-3798-8405
株式会社日立製作所　情報・通信システム社
プロジェクトマネジメント統括推進本部　石川　TEL：03-5471-2942
株式会社東芝　ソフトウェア技術センター　長谷川　TEL：044-549-2409
大学共同利用機関法人　情報・システム研究機構　国立情報学研究所
アーキテクチャ科学研究系　中島　TEL：03-4212-2507