2011 年 7 月 21 日

東京証券取引所と DSF 成果を活用した
形式手法適用実証実験を IPA SEC 主催で開始
～DSF が「形式手法活用ガイド」を正式リリース～

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
株式会社 CSK
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、株式会社 CSK の 6 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、独立行政法人 情報処理推進機構 ソフトウェア・エンジニアリング・センター（以下、IPA SEC）のワーキンググループに参加し、株式会社東京証券取引所のエンタプライズ系ソフトウェア（※2）を対象とした形式手法（※3）の有効性実証実験（以下“本実験”）を実施します。

形式手法とは、品質の高いソフトウェアを効率よく開発するために、数学を基盤とした矛盾のない仕様書を書いて、それが正しいかどうかを検証する手法のことです。そのため、高信頼・高品質が求められる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。しかし、エンタプライズ系ソフトウェアについては適用事例が少なく、その効果も一般に公開されていません。そこで DSF はエンタプライズ系ソフトウェアに形式手法を適用するための事例およびノウハウの収集を行っています。

ソフトウェアを開発するプロジェクトにとって、形式手法の利活用は作業期間や作業コストに影響します。よって事前に発注者（ユーザ）と受注者（ベンダ）が合意するために、利活用の可否を判断する情報（形式手法によって除去できる欠陥の数や作業人月など）が必要です。そこで本実験では上記情報を収集し、実験実施後に実験報告書として IPA SEC から公開します。

なお本実験では、DSF が作成した形式手法活用ガイド（以下“本ガイド”）を活用します。本ガイドはエンタプライズ系ソフトウェアを対象とした形式手法の適用手順や典型的な形式記述の例をまとめたものです。本実験と並行して DSF メンバで本ガイドの社内評価の開始準備が整ったことにより、DSF 社内外の実利用で評価いただける品質に達したものとして、本日より DSF 公式ホームページで正式リリースいたします。

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

また DSF は本実験を通じて得られた知見を本ガイドにフィードバックし、2012 年 3 月に改訂版として公開します。

【国内における形式手法に対する関心の高まりについて】

経済産業省は「新世代情報セキュリティ研究開発事業」により、情報家電などの組込みソフトウェアに対する形式手法適用のケーススタディを収集し、普及促進のためガイダンスを作成しました。また同省北海道経済産業局は、北海道および中部地区に拠点を持つ中小ソフトウェア企業を中心に組込みソフトウェアを対象とした現場普及活動を行っています。

さらに IPA SEC は本実験以外にも、形式手法を利用できる人材の育成や過去事例の整理を中心とした形式手法の普及活動を行っています。

このように形式手法に対する関心が高まる中で、DSF は社会における重要性が飛躍的に高まるエンタプライズ系ソフトウェアを対象とした初の形式手法活用ガイドを作成しました。また公的機関である IPA SEC や発注者の立場である株式会社東京証券取引所と連携して本実験を実施し、結果を実験報告書としてまとめます。

【有効性実証実験について】

本実験は IPA SEC のワーキンググループで実施し、メンバとして DSF および株式会社東京証券取引所、さらに有識者が参加します。具体的には、エンタプライズ系かつ高信頼が求められるシステムを多く保有する株式会社東京証券取引所で現在稼働中のソフトウェアの設計書を対象に、形式手法活用ガイドの手順に従って設計書の不整合や曖昧さなど設計書としての欠陥の除去を実施します。また株式会社東京証券取引所の評価を得た上で、開発中に発見した欠陥との比較や除去した欠陥の数や種類、作業人月などを実験報告書にまとめます。これにより報告内容に発注者の見解を取り入れることができるため、報告内容の信頼性を向上することができます。さらに有識者から実験データの客観的な分析を加えることで、報告内容の信頼性および汎用性を高めます。

【形式手法活用ガイドについて】

本ガイドは、形式手法による設計書の欠陥除去手段の確立を目的とし、受注者（開発プロジェクト）向けにその手順と参考となる形式記述の例をまとめたものです。以下三つのラインアップについて個別に説明します。

項番	名称	説明	前回リリース（ドラフト版）からの変更点
1	形式手法活用ガイドの紹介	・形式手法活用ガイドの各ラインアップの位置づけを解説します。	・発注者（情報システム部門）を対象に、形式手法の活用メリットに対する解説を追加しました。 ・発注者（情報システム部門）および受注者（管理者、技術者）を対象に、形式手法で発見できる欠陥の解説を追加しました。 ・受注者（管理者）を対象に、形式手法適用手順を選択する手段として、形式手法を適用する目的ごとに対応する適用手順の一覧を追加しました。
2	形式手法適用手順	・形式手法（VDM++（※4），SPIN（※5），Event-B（※6））の適用手順を解説します。 ・受注者（管理者、技術者）が形式手法を適用する際に手順を検討する参考として使用することを想定します。	・形式手法イディオム集への参照関係を追加し、作業の流れの中で利用可能なイディオムを整理しました。 ・VDM++編、SPIN 編を新規作成しました。 ・Event-B 編に 2 適用手順を追加しました。
3	形式手法イディオム集	・形式手法適用手順から参照する、形式記述の典型的な表現を解説します。 ・受注者（技術者）が形式記述を作成する際に参考として使用することを想定します。	・VDM++編を新規作成しました。 ・SPIN 編の 7 イディオムを改訂しました。 ・Event-B 編に 18 イディオムを追加しました。

【現在までの歩み】

ＤＳＦは、エンタプライズ系ソフトウェアの信頼性・安全性向上のため、現場への形式手法導入課題を解決する活動として 2009 年 12 月 22 日に形式手法適用評価ワーキンググループ（以下、“ＦＭＡＷＧ”）を設立しました。

ＦＭＡＷＧは形式手法の記述実験で得られた知見をベースに検討し、成果物第一弾として 2010 年 11 月に形式手法活用ガイドのドラフト版を公開しました。その後もさらに活動を継続し、代表的な三つの形式手法（VDM++、SPIN、Event-B）について形式手法活用ガイドの充実を図りました。本実験と並行して DSF メンバで本ガイドの社内評価の開始準備が整ったことにより、DSF 社内外の実利用で評価いただける品質に達したものとして、今回正式版としてリリースしました。

【今後の活動について】

DSF は本実験に参加、形式手法利活用の可否を判断するために必要な情報（形式手法によって除去できる欠陥の数や作業人月など）を収集し、実験報告書として IPA SEC から公開します。また同時に、本実験で本ガイドの手順に従った欠陥除去を実施した経験から本ガイドの課題抽出および対策を実施し、2012 年 3 月に改訂版として公開します。

【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、株式会社 CSK の 6 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)、株式会社 CSK（代表取締役社長 社長執行役員 中西 毅）の 6 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）エンタプライズ系ソフトウェア

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機能を実現するソフトウェアのこと。

（※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、対象とするシステム・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）VDM++

VDM（Vienna Development Method）と呼ばれる形式手法で使用するオブジェクト指向形式言語。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、作成した形式記述の型チェックやテストによってシステムが満たすべき特性の検証を行う。株式会社 CSK が VDM 開発支援ツールの VDMTools を無償提供している。

（※5）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。分散ソフトウェアなどの並行ソフトウェア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。

（※6）Event-B

ソフトウェアの分析、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。検証すべきことの多くを自動検証できる。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。

【本件に関するお問い合わせ先】

報道関係のお問い合わせ先

株式会社 NTT データ 広報部 杉山 TEL：03-5546-8051

富士通株式会社 パブリックリレーションズ本部 広報ＩＲ室 兒玉
TEL：03-6252-2174

日本電気株式会社 コーポレートコミュニケーション部 中島 TEL：03-3798-6511

株式会社日立製作所 情報・通信システム社 広報部 菊池 TEL：03-5471-8900

株式会社東芝 広報室広報担当 水野・吉村 TEL：03-3457-2100

株式会社 CSK 広報・IR 部 秦 TEL：03-6438-3050

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
企画推進本部 広報普及チーム 岡本
TEL：03-4212-2131 MAIL：kouhou@nii.ac.jp

その他のお問い合わせ先

株式会社 NTT データ 技術開発本部 塚本 TEL：050-5546-8779

富士通株式会社 共通技術本部 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 福地 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

株式会社 CSK 開発本部 植木 TEL：03−5290−3872

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