2012 年 4 月 20 日

東京証券取引所の設計書を対象とした実験で形式手法の有効性を実証

～実験結果をもとに DSF が「形式手法活用ガイド」を完成～

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
SCSK 株式会社
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
独立行政法人情報処理推進機構

独立行政法人情報処理推進機構（以下、IPA）(注 1)は、株式会社東京証券取引所で実際に運用しているシステムの設計書を対象にして、ディペンダブル・ソフトウェア・フォーラム（以下、DSF）の活動成果である形式手法活用ガイド（以下“本ガイド”）に従って、形式手法(注 2)適用実証実験（以下“本実験”）を 2011 年 8 月より行い、形式手法の有効性を実証しました。IPA は本実験の結果を報告書（以下“本書”）にまとめ、IPA 公式 Web サイト(http://sec.ipa.go.jp/reports/20120420.html)で公開します。

DSF は、障害を起こさないソフトウェア（ディペンダブル・ソフトウェア）を実現するために、形式手法のソフトウェア開発への導入を目指し 2009 年より活動してきましたが、本実験の結果を受けて本ガイドを改訂し、最終版を DSF 公式 Web サイト(http://www.nttdata.co.jp/dsf/)で公開します。

なお DSF には、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、SCSK 株式会社の 6 社および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 (注 3) が参加しています。

【概要】

DSF は、ディペンダブル・ソフトウェアを実現するために、実践的、かつ系統的・論理的な設計技術を確立させる研究開発を行い、ソフトウェアに起因するシステム障害の低減を目指し活動してきました。具体的には、エンタプライズ系ソフトウェア(注 4)の分野では開発現場への形式手法導入を支援するガイドが今までなかったことから、DSF は国内で初めて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本ガイドを作成し、2011 年 7 月 21 日に公開しました。

また、IPA は、昨今の形式手法の利用が進んでいない原因は参考となる形式手法を適用した事例情報がないことであると考え、実運用中のシステムに形式手法を適用したときの効果と具体的な作業工数の測定を目的に、本ガイドに従って 2011 年 8 月より本実験を行いました。

具体的には、東京証券取引所で実際に運用しているシステムの、すでにレビュー実施済みの設計書に形式手法を適用したところ、設計書レビューでは発見されなかった指摘事項(注5)を発見できました。また、東京証券取引所が設計書を修正すべきであると評価した指摘事項のうち半数以上は、従来では実装やテストといった設計工程以降で発見されていたものでしたが、今回形式手法を用いた検査によって設計工程で発見できたことから、設計工程以降に発生する作業の手戻りが削減できる可能性を示すことができました。

DSF は本実験にメンバーとして参加し、実験の実作業を担いました。さらに DSF は、本実験で新たに考案あるいは改善した手順や記述方法をより実践的な知見として本ガイドに取り入れ、活動の集大成として本ガイドの最終版を本日公開します。

なお、DSF は所有する成果物の著作権を 2012 年 6 月に IPA に譲渡する予定であり、2012 年 6 月末日に活動を終了しますが、参加各社において本取り組みの成果を生かし形式手法の普及に努めます。また、IPA は今回の実験成果を形式手法の現場普及を目指した教材に取り入れ、開発現場が形式手法を適切に活用できるよう普及を図ります。さらに本実験とは異なる観点を含めた形式手法の実証実験を継続して行い、形式手法を有効活用するための知識体系を整理していく予定です。

本実験と本ガイドについては、別紙をご参照ください。

（注 1）　独立行政法人情報処理推進機構　理事長　藤江　一正

（注 2）　形式手法（フォーマルメソッド、Formal Methods）

数理論理を基礎として、対象とするシステムやソフトウェアの機能・振る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、要求や設計仕様の矛盾、抜け漏れ等の誤りを発見することができる。

（注 3）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（代表執行役　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）、SCSK 株式会社（代表取締役社長：中井戸　信英）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）

（注 4）　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。

（注 5）指摘事項

形式手法適用者が、設計書の機能仕様を形式手法で記述、検証したときに指摘した事項。

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	■ その他のお問い合わせ先
株式会社ＮＴＴデータ 広報部　平形・高橋 TEL：03-5546-8051	株式会社ＮＴＴデータ 技術開発本部 塚本・田端 TEL：050-5546-8779
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 小川・遠藤 TEL：03-6252-2174	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 コーポレートコミュニケーション部 上田 TEL：03-3798-6511	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 広報部 菊池 TEL：03-5471-8900	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 広報室広報担当 吉村 TEL：03-3457-2100	株式会社東芝 ソフトウェア技術センター 長谷川 TEL：044-549-2458
SCSK 株式会社 広報部 秦・神谷 TEL：03-5166-1150	SCSK 株式会社 ソリューション・機能事業部門 開発ソリューション事業本部 開発部 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 総務部企画課 広報チーム 坂内 TEL：03-4212-2164 E-mail：kouhou@nii.ac.jp	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
独立行政法人情報処理推進機構 戦略企画部　広報グループ 横山・白石 TEL：03-5978-7503	独立行政法人情報処理推進機構 技術本部 ソフトウェア・エンジニアリング・センター 向山 TEL：03-5978-7543

別紙

【形式手法適用実証実験について】

IPA では、ソフトウェアおよびシステムの安全性・信頼性の確保を重要な課題と捉え、形式手法の普及を含めたさまざまな取り組みを行っています。

本実験はそのような活動の一環として、IPA　技術本部ソフトウェア・エンジニアリング・センターの統合系システム・ソフトウェア信頼性基盤整備推進委員会が設置した「形式手法技術部会ワーキンググループ（形式手法適用実証 WG)」において 2011 年 8 月から 2012 年 3 月にかけて実施したものです。実験の題材には、東京証券取引所で実際に開発されたソフトウェアの設計書を使用し、本ガイドの 2011 年 7 月 21 日公開版に沿って設計書の検査に形式手法を適用しました。

本実験は、東京証券取引所で実運用中のシステム設計書延べ 716 ページを対象に、設計作業終了直後の設計書の内容を形式手法で記述、検証を行い、55 件の指摘事項を抽出しました。そのうち、22 件の指摘事項は、東京証券取引所が設計書を修正すべきであると評価したものです。また、22 件の指摘事項を分析したところ、半数以上の 13 件の指摘事項が実際の開発では設計書作業より後の工程で発見したことが判明しました。本結果から、通常の開発では実装やテストといった設計作業後の工程で見つかる指摘事項が、形式手法を用いた検査によって設計工程で見つかり、設計工程以降に発生する作業の手戻りが削減できる可能性を示すことができました。また、ページあたりの基本設計レビュー実績工数の基本統計量 (注 6) との比較により、設計書の改善点発見手段として一般的に使用されているレビュー手法と形式手法とでは、作業効率に大きな差がないことを確認しました。さらに本書は、形式手法で発見した改善点や作業コスト、作業効率、作業者のスキル、作成した形式記述について、作業者 14 名（約 560 人時分）のデータを公開することで、形式手法導入を検討する発注者や受注者に実開発に近くより精度の高い情報を提供します。

本実験の結果をさまざまな視点で評価するために、発注者および受注者、学識経験者が委員として本実験に参加しました。本実験の結果に対して、発注者の委員は「設計書等の品質を向上させるための方策の一つとして、従来のレビューに加えて形式手法を採用することは十分可能であると思われる」との見解を示しました。また学識経験者の委員は、形式手法の効果を確認できたことと作業工数等の具体的なデータを得られたことを評価しました。これらの評価は実際に形式手法導入を検討した例として活用できるため、発注者や受注者にとって形式手法利活用の可否を判断する助けとなります。

【形式手法活用ガイドについて】

2011 年 7 月 21 日に公開した本ガイドの改訂にあたり、DSF は本実験のため新たに考案

あるいは改善した手順や記述方法を本実験中に記録しました。また DSF 関連のグループ会社や本実験メンバーである発注者に依頼し、本ガイドに対する全 101 件の改善要望コメントを収集しました。

改善要望コメントへの対応として、本ガイド中の用語や概念について解説を追加したため全ラインアップで可読性が向上しました。その他については以下表で個別に掲載します。

項番	名称	説明	前回リリース（2011 年 7 月 21 日公開版）からの変更点
1	形式手法活用ガイド 導入の手引き	・形式手法の概略および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。	・名称を「形式手法活用ガイドの紹介」から「形式手法活用ガイド 導入の手引き」に変更しました。 ・形式手法の効果に関する本書の記述を本ガイドに引用したため、本ガイド単独で形式手法の効果から使い方までの概要を理解できるようになりました。
2	形式手法適用手順	・形式手法（VDM++(注 7)、SPIN(注 8)、Event-B(注 9)）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。	・形式手法適用手順に記載された 6 手順のうち、5 手順を活用して本実験を効率よく実施することができました。 ・本実験での記述に合わせた手順の見直しを行い、実際の開発で利用できる手順として洗練しました。 ・状況に合わせた適用手順のカスタマイズについて解説を追加したため、カスタマイズによる適用範囲が広がり、より多くの読者が使えるようになりました。 ・形式手法支援ツールの機能や使い方について解説を追加し、またすぐにツールに入力できる形で形式記述のサンプルを提供したため、形式手法の特徴であるツールを用いた検証を素早く実体験できるようになりました。
3	形式手法イディオム集	・形式手法（VDM++、SPIN、Event-B）適用手順から参照する、形式記述の典型的な表現を	・VDM++編、SPIN 編、Event-B 編合わせて 34 イディオムを本実験に活用することができ、実験作業の効率化

		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。	に寄与しました。 ・本実験で使用した形式記述をイディオムとして形式手法イディオム集に追加したため、活用できるイディオムが増えました（VDM++編に 3 イディオム追加しました)。

（注 6）　ページあたりの基本設計レビュー実績工数の基本統計量

“SECBOOKS ソフトウェア開発データ白書 2010-2011” p.209 掲載の「ページあたりの基本設計レビュー実績工数の基本統計量」のこと。

（注 7）　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仕様言語。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を検査する。SCSK 株式会社が VDM 開発支援ツールの VDMTools を無償提供している。

（注 8）　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ものがある。

（注 9）　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 が統合ツール RODIN を開発し無償公開している。