



## 先進的な設計・検証技術の適用事例

SEC 調査役

室 修治

SEC 研究員

春山 浩行

SEC 研究員

藤原 由起子

SEC 研究員

佐々木 方規

### 1 はじめに

ソフトウェアの高信頼性を確保するためには、その開発プロセスに踏み込んで、見える化や高度化に取り組む必要がある。そのために、色々な開発方法論や手法が提案され、その有用性も報告されているが、現場レベルでは具体的な導入方法が不明であるとか、効果が見通せないとか、実システム開発における失敗が怖いなどの理由により、広範囲な実用にはつながっていないのが実情である。そのような中であっても、先進的な手法を導入し、その改善に取り組み、実システムの開発にも適用するという実践的な事例が多く存在する。

利用者が安心して製品・システムを使えるようにするために、これらの事例を数多く収集し、それを共有する

ことにより、我が国のソフトウェア開発の水準を高めていくことが重要であると考えます。そこで、開発プロセスのうち、最近「見える化」の手法が充実してきた「上流設計」、及び「検証」に着目し、その先進技術の普及を図ることとした。これまでに、先進的な取り組みを行っている団体・企業などから適用事例を収集してきた。

これらは、平成 26 年度 5 月に「先進的な設計・検証技術の適用事例報告書 2013 年度版」として公開した<sup>※1</sup>。

今後は、更に事例数を増やし、最終的には収集した事例を俯瞰して、有用性や適用領域を整理したガイドラインを作成する予定である。

【脚注】

※1 <http://www.ipa.go.jp/sec/reports/20140530.html>

## 2 今回収集した事例の特徴

- ① 各方面のご協力をいただき、20件以上の事例を収集でき、多岐にわたる内容になっている。
- ② 設計・検証に関する先進的な適用事例を紹介したものであり、導入上の工夫や効果なども記載しており、今後の導入の参考になるものである。
- ③ 各社、各団体の現場で活躍されているリードオフマン的な方々に紹介していただいた事例であり、高度な内容も含んでいる。

## 3 収集した事例の一覧

今回収集した事例を、設計と検証に大別して、表1に示す。

## 4 普及に向けた活動

有用な技術や手法の普及のために、以下の2つの観点でセミナーを開催している。

- ① 導入への関心を高めるための事例紹介セミナー
- ② 具体的な技術や手法に関する技術セミナー

昨年度は、ソフトウェアの高信頼化に関連した技術（MBSE、形式手法など）に関するセミナーを開催した。

今後も事例紹介セミナーとその事例に適用されている技術に関するセミナーを企画・開催していく予定である。

知識習得の場として、ぜひ活用していただきたい。

## 5 事例紹介

以下に、今回収集した事例をいくつかピックアップし、その概要を紹介する。

### (1) 「アシュアランス技術を用いた鉄道信号の革新」 (事例提供元 東日本旅客鉄道株式会社)

現行の列車運行を止めることなく、運行管理システムを刷新していく取り組みにおいて、システムの安定稼働を保証する技術（アシュアランス技術）をいかに適用したかを解説している。とくに、既に稼働中の装置と試験中の装置が混在する状況において、すべてのデータの中から自律分散的に自身が扱うべきデータを判断し、他に影響を与えることなく稼働可能としている点に特徴がある。

日本の列車制御の安全性は、世界に誇れるものであり、それを実現する技術の一端を興味深く知ることができる。

### (2) 「要件定義段階における信頼性向上の取り組み事例紹介」(事例提供元 ビッグロブ株式会社)

コンシューマ向けサービス開発や受託システム開発においては、短期開発、コスト削減の条件の元で品質確保を行わなければならない。この問題を軽減するのに効果的だった要件分析手法、優先度付けの方法、ツールの活用方

表1 「先進的な設計・検証技術の適用事例報告書 2013 年度版」掲載事例一覧

No.	標題	事例提供元
A-1	アシュアランス技術を用いた鉄道信号の革新	東日本旅客鉄道株式会社
A-2	XDDP 導入による派生開発の品質改善とその効果	株式会社日立産業制御ソリューションズ
A-3	組込み系の利用品質における「HMI 品質メトリクス」開発と適用事例	株式会社 U'eyes Design
A-4	要件定義段階における信頼性向上の取り組み事例紹介	ビッグロブ株式会社
A-5	要件定義の品質向上に向けた取り組み	富士通株式会社
A-6	ジェネレータツールを利用した高信頼開発、高速開発の実践	株式会社市進ホールディングス
A-7	設計工程における TERASOLUNA DS の適用	株式会社エヌ・ティ・ティ・データ
A-8	Grails/Groovy の適用推進	エヌ・ティ・ティ・ソフトウェア株式会社
A-9	個人依存開発から組織的開発への移行事例	三菱電機メカトロニクスソフトウェア株式会社
A-10	MBSE による双腕作業ロボット動作実行系のコンセプト設計	独立行政法人産業技術総合研究所 (AIST)
A-11	仕様記述言語 VDM++ を用いたシステムの仕様の記述	フェリカネットワークス株式会社
A-12	車載 ECU 開発における上流工程での品質確保	東芝情報システム株式会社
A-13	独自開発したモデル駆動開発プロダクトラインエンジニアリングの実践	株式会社デンソー
B-1	宇宙システムにおける上流工程仕様の妥当性確認技術	独立行政法人宇宙航空研究開発機構 (JAXA)
B-2	鉄道の機能安全 (RAMS) 認証支援のためのセーフティケース	独立行政法人産業技術総合研究所 (AIST)
B-3	非機能要求グレードの大学ポータルサービスへの適用	名古屋大学
B-4	冗長構成システム (クラウドなど) の耐故障性に対する検証技術	株式会社富士通コンピュータテクノロジーズ
B-5	単体ランダムテスト実行/可視化ツール "Jvis" の適用事例	宮崎大学
B-6	要求仕様明確化のための仕様記述技術 (USDM) 活用事例	株式会社ベリサーブ
B-7	形式手法を用いたセキュリティ検証	アーク・システム・ソリューションズ株式会社
B-8	形式仕様記述手法を用いた高信頼性を達成するテスト手法とその実践	フェリカネットワークス株式会社
B-9	Orthogonal Defect Classification 分析による欠陥除去と品質の成熟度可視化	オリンパスソフトウェアテクノロジー株式会社
B-10	モデル検査の適用による上流工程での設計誤りの発見	株式会社東芝
B-11	上流工程の要求を効率的に閉ループシミュレーションする次世代 SILS の開発	トヨタ自動車株式会社

法などを実践的な工夫を交えて具体的に紹介している。

これまでの常識とされた考え方に捉われることなく、現場感覚が垣間見える内容であり、セミナー講演を聞いた受講者からは、「目から鱗（うろこ）であった。」という感想も寄せられている。

**(3) 「仕様記述言語 VDM ++ を用いたシステムの仕様記述」(事例提供元 フェリカネットワークス株式会社)**

おサイフケータイ<sup>※2</sup>に搭載された IC チップファームウェアの開発にあたり、形式仕様記述手法を適用した効果を紹介している。この手法を導入しても、プログラム開発効率の低下は見られず、仕様に関するコミュニケーションの向上などの成果が得られたことを示している。

自然言語による仕様記述の方が、むしろ難しく感じる人がいるという実態報告にはうなづけるものがある。技術者にとっては数学的表現と国語的表現のいずれが理解しやすいのかと考えさせられるような問題提起を含んでいる。

**(4) 「宇宙システムにおける上流工程仕様の妥当性確認技術」(事例提供元 独立行政法人宇宙航空研究開発機構 (JAXA))**

宇宙システムのようなセーフティクリティカルシステムのソフトウェア開発では、上流工程の仕様定義での問題(不正確、不完全、想定不足など)がシステムの安全性を脅かすことが多い。本事例では、問題解決のため導入適用した「モデル検査」と「チェックリストベースレビュー」について、特徴や導入上の課題、解決策を紹介している。

宇宙システムは、我々の一般的なソフトウェアとは縁

遠いものと考えがちだが、ソフトウェアの開発現場ではレベルの高低はあれども、悩みは同じであり、特別なやり方が行われているわけではない。そういう意味で、ソフトウェアの信頼性を追求する活動は、大いに参考になるものである。

**(5) 「形式手法を用いたセキュリティ検証」(事例提供元 アーク・システム・ソリューションズ株式会社)**

組込み機器のソフトウェア開発において、セキュリティ要件を満たすために形式手法を適用した事例を紹介している。形式手法は、数学的な証明を与えてくれるため、客観的な観点でセキュリティの保証につながることに特徴がある。

適用効果を示すために、セキュリティの専門家に独立に分析してもらい、形式手法適用ツールを利用した場合の脆弱性指摘との違い(指摘箇所は同じ)までも考察しており、効果への見通しの参考になる内容である。

## 6 おわりに

今回の事例収集の取り組みは緒に就いたばかりであり、比較的大規模なソフトウェア開発が対象であったり、先端的な事例に着目している面がある。しかし、実際の開発現場では、もっと実状に即した対応がなされていたり、幅広い取り組みが存在すると想定される。それらを各方面のご協力を得ながら収集し、更に充実したものに仕上げていきたい。

**【脚注】**

※2 「おサイフケータイ」は株式会社 NTT ドコモの登録商標です。