# ソフトウエア IV&V（独立検証及び有効性確認）
# Software Independent Verification and Validation (IV&V)

## プロジェクトに応じた適用技術の研究
## Research on applied methodologies according to project characteristics and needs

情報技術開発共同センター
Information Technology Center
奥田一実、片平真史、石濱直樹
Kazumi Okuda, Masafumi Katahira, Naoki Ishihama

Abstract

Software IV&V (Independent Verification and Validation) technology has been studied after the space shuttle Challenger accident was occurred. Jaxa is also applying new methodologies of IV&V to software in real space projects. Several techniques have been applied and known as effective approach to high reliability software development in JAXA. In this research, the new methodologies were studied and applied to support project team's software development. As a result of this study, the applicability and effectiveness are confirmed.

## 1. はじめに

本研究では平成 12 年度より高信頼性ソフトウエア開発技術の１つとして、ソフトウエア IV&V 技術の構築及び実プロジェクトへの適用を実施してきている。また、本研究は、奈良先端科学技術大学院大学との共同研究のもと実施している。

## 2. 研究の概要

平成15年度は以下の項目について研究を行った。

### (1) ソフトウエア IV&V に関する新規技術の研究

以下のソフトウエアIV&Vの新規技術について、実プロジェクト評価作業において必要性が発生し、研究を実施した。

上流工程に関する技術

- 要求仕様記述評価法
- 自然言語/形式的仕様モデル(モデル検査)
- 衛星姿勢制御系モデル化技術
- 仕様記述に基づくモデルシミュレーション
- 衛星姿勢制御系チェックリスト

下流工程に関する技術

- コード検査
- 下流工程におけるリバースエンジニアリング
- 試験網羅性評価法

共通技術

- COTS/再利用ソフトウエアの評価法
- コードクローン、オーバホール応用技術

### (2) 実プロジェクトへの適用

以下の実プロジェクトにソフトウエアIV&V技術を適用し、プロジェクトにおける課題抽出するとともに、手法の実証を実施した。

- 宇宙ステーション関連（３プロジェクト）
- 人工衛星（３衛星）
- 地上装置（２システム）

### (3) 動向調査、情報交換

NASA や ESA の IV&V 担当者との情報交換を実施し関連会議へ参加した。JAXA の IV&V 研究内容およびIV&V活動状況について報告・意見交換を実施した。

## 3. 成果の概要

(a) 上流工程に関する技術

要求仕様書の記載時の留意事項を一般文献やNASA JPL などの研究者から得た情報を元に宇宙用の要求仕様記述評価ガイド（IV&V 用）を策定した。

また、昨年度開発した、要求仕様書の形式的仕様モデルの評価のための自然言語による入力方式を用いた形式的仕様モデルのモデル検査を実証し、SPIN ツールなどとの併用によるモデル検査（一貫性解析、完全性解析、トレーサビリティ

解析、リーチャビリティ解析）の手法を整備した。

上記で考案した状態遷移モデルに基づくモデル評価技術に加え、フローチャートなどのアルゴリズムなどを評価するために、Uppaal という欧州のツールを使用し、姿勢制御系ソフトウエアの評価手法を考案した。Uppaal によるモデル構築後、C 言語のプログラムに自動変換し、仕様記述に基づくシミュレーションを実現できる環境を構築することができた。

一方、宇宙ステーション関連と比べ、評価方法および評価作業時間に制限のある人工衛星の IV&V 評価を実現するために、これまでの不具合やレビュー経験を元に、衛星姿勢制御系ソフトウエアチェックリストを作成し、実際の作業で有効性を評価した。上流工程における形式的仕様モデルを用いた網羅的な解析は大変効果があるが、時間・方法に制限がある場合、チェックリストによる評価で十分な成果をあげることができた。

(b) 下流工程に関する技術

開発がある程度進んだプロジェクトに対する評価技術として、コードチェックツールを用いた評価作業を実施した。splint や gcc などを応用した自作ツール、また、市販の Codewizard を活用した実プロジェクトに対するコード検査および結果の抽出方法を確立し、コードレベルの課題抽出に十分に活用できることがわかった。

また、詳細設計書からソースコード作成段階に発生する誤り・抜けを発見するために、ソースコードから詳細設計（フローチャート）を作成するツールを自作し、詳細設計書との比較により課題抽出ができることが確認された。

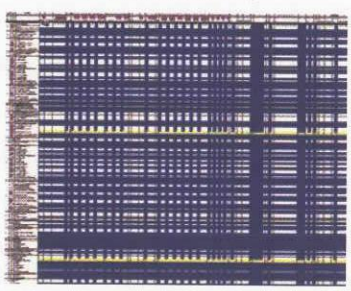

図３－１　試験ケース削減事例
（青の部分が根拠を持った削減ができた部分）

また、試験段階における試験網羅性を評価する技術として試験ケースの正当性のある削減方法（例を図３－１に示す）を考案し、実プロジェクトへの適用により効果的なフィードバックを実現できた。

(c) 共通技術

その他、共通技術として、COTS や既開発ソフトウエアの再利用時の IV&V 評価プロセスの検討を開始し、また、コードクローンやオーバホール手法の応用技術の研究として、信頼性評価、及び上流工程への活用方法の検討を開始した。また、各解析に共通的に利用できる XML に類似したモデル記述方法を設定するとともに、モデル間の等価性の検証技術として、判定アルゴリズムの開発を開始した。

## 4.　まとめ

これまでの研究において、上流工程から下流工程までの一通りの評価方法を準備した。特に、ソフトウエア IV&V の研究を通じて、

- 宇宙開発で利用できるソフトウエア開発技術を研究・実証し、適用性を判断した上で実用化させる。
- 実プロジェクトのソフトウエアを評価し、適切なフィードバックをかける。

が十分に可能であることが実証できた。

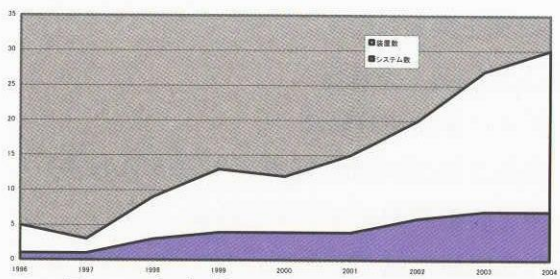


図4－1　実プロジェクトへのIV＆V適用数の推移

図 4-1 に示すように実プロジェクトへの適用数が急速に増加する傾向にあるため、要員の増強を図り、評価方法の追加充実を図るとともに、プロジェクトの特性およびソフトウエア IV&V 作業の制約などから作業方法をサイジングできるアプローチについて検討する必要がある。