アングル

経営者はアーキテクチャと形式手法を忘れてはいけない

高信頼性システム技術作業部会委員
グローバル情報社会研究所株式会社　代表取締役社長
藤枝 純教

本記事は、次の3項目を念頭に執筆した。

(1)自動車や宇宙、航空、原子力、医療、スマート・グリッド、ITS※1等の高性能・高信頼性が要求されるシステムの開発と検証管理の技術能力を確保し、国際競争力を持つ。このことに日本のIT企業が寄与する。

(2)クラウド・コンピューティング及び国際的なアウトソーシングにより低コストかつ短い時間で開発し、高信頼のサービス提供により高い顧客満足度を獲得するにあたり、アーキテクチャの持つ意味が極めて高く、かつ高信頼性検証能力確保への投資は経営的に成り立つ、ということを経営者に認識していただく。

(3)上記2項目の実践のために、IT管理者がアーキテクチャ・ベースのモデル化と形式手法の採用の必要な理由を理解し、それを推進する。

1. 21世紀の日本のIT戦略を考える

1.1 これまでのIT化とこれからの挑戦

1980年代後半からの日本は、積極的な投資と標準化を進めた結果、世界一流の通信インフラを持つに至った。しかし、ユーザ企業においては、西欧流のCIO※2やアーキテクトを育てずにベンダ任せとすることが多く、またグローバルでオープンなスタンダードを導入する戦略をとらなかった。その結果、BPR※3に基づく新規アプリケーションの開発というより、レガシー・システムの保守・維持により情報システムが守られてきた。

一方、組込み業界においては、主力製造部門の家電、携帯、自動車、産業ロボット機器等、成功したセクターがあるが、現在では国内需要の飽和と海外の消費低迷に米国、中国、インド、欧州、東欧成長諸国からの追上げが加わっており、大変厳しい状況である。

そこで、このような問題を受け、本稿では、2030年に向けて、アーキテクチャと形式手法を駆使する新しい2つの産業戦略を提案したい。

①製造業のソフトウェア技術をより一層、安全で高度なものにし、高機能・高信頼性を確保出来るミッション・クリティカル・システム分野へシフトする。

②サービス業の生産性を、EA※4をドライバに環境や顧客中心目線で徹底して最適化し、システム化する“サービスの最適化プロジェクト”を興す。

1.2 欧州と米国の高機能・高性能・高信頼性産業への取り組みの歴史から学ぶ

欧州における、形式手法への取り組みは、1960年代のTony HoareのTheorem Proving、Robin MilnerのLCF※5、1973年Cliff JonesのVDM※6、Jean-Raymond Abrialの1977年のZ言語※7、1996年のBメソッド※8とVDMの標準化に続き、2002年にはZ言語がISOで認証された。また、2005年以降、これら形式手法を、鉄道、自動車、航空管制、原子力、電子マネー等に利用するプロジェクトに対し、欧州では戦略的な支援が行われている。一方、アーキテクチャは、1960年代のSOP※9、1970年代のBSP※10、次いでザックマンのEA、1995年からのTOGAF※11、FEA※12、DODAF※13等米国主導となった。しかし、2005年頃から欧州でも対米航空宇宙機器ビジネス市場に参入すべく世界標準を取り入れ、米国の自動車及び航空機製造エンジニア協会（SAE※14）が標準として決めたAADL※15をAirbus、EADS、Thalesら各社が取り込み、その上で形式手法を使うアプローチを2006年から始めた。2009～2010年の欧州高信頼性プロジェクトでは、次の節で述べるが、AADLを取り入れている。

※1 ITS：Intelligent Transportation Systems，高度道路交通システム
※2 CIO：Chief Information Officer
※3 BPR：Business Process Re-engineering
※4 EA：Enterprise Architecture
※5 LCF：Logic for Computable Functions
※6 VDM：Vienna Development Method，IBMのウィーン研究所で開発された形式手法の1つ。
※7 Z言語：Z notation，Jean-Raymond Abrialを中心にオックスフォード大学のプログラミング研究グループによって開発された形式手法の1つ。Z記法、Zメソッドとも言う。
※8 Bメソッド：B method，Jean-Raymond Abrialを中心に開発された形式手法の1つ。Z言語とも関連がある。
※9 SOP：Study Organization Plan，IBMで開発された設計手法の1つ。
※10 BSP：Business System Planning，IBMで開発された、業務、データ、組織を構造化する手法。
※11 TOGAF：The Open Group Architecture Framework
※12 FEA：Federal Enterprise Architecture
※13 DODAF：Department of Defense Architecture Framework
※14 SAE：Society of Automotive Engineers
※15 AADL：Architecture Analysis & Design Language，米SAEが策定したアーキテクチャ記述言語。

1.3 AADLを利用した欧州高信頼性プロジェクト

このプロジェクトには、①Eclipseベースのオープンソースである TOPCASED ツールを使った形式検証（2,000万ユーロ、28社）、②欧州宇宙開発局主導のAADLベースプロジェクトのSPICES（1,600万ユーロ、15社）、③同じくAADLとUMLプロファイルを使うAxlog、Thales社ら29社連合プロジェクトのASSERT、④米Carnegie Mellon University の SEI※16、University of Illinois at Urbana-Champaign、Vanderbilt大学と欧州の42社の組込み共同プロジェクトのARTIST2、⑤2006年からの次世代自動車設計に関する研究会Beyond AutoSAR、⑥2007年からのIntegrated Modular Avionicsに関する欧米共同の基礎研究等が含まれる。

1.4 AADLを利用した米国信頼性プロジェクト

米国での高信頼性プロジェクトの中心は、個別の形式手法から1995年になると米国国防総省におけるアーキテクチャ事件（2.2節）を契機に、アーキテクチャに焦点が移ってきた。一般企業はEAを、そして航空や自動車等の高機能高信頼性製品を作る企業はAADLをそれぞれ採用し、設計を分析検定するアプローチをとるようになった。

2007年からは、AADLベースでRFP※17を出し、AADLで書かれたソフトを仮想検査・検定し、下流までの発注判断を可能にするためのプロジェクトであるAVSIが実施された。このプロジェクトでは、米国航空・防衛システムの中心ベンダ8社、Boeing、Lockheed Martin、Honeywell、Raytheon Company、Rockwell Collins等に、SEIがまとめ役として参加し、2009年に第1次結果（全部で第4次まで）をまとめている。

1.5 日本が欧州、米国の高信頼性プロジェクトから学ぶこと

日本においても、宇宙航空・重工業・精密機械・自動車等の各社のトップ・アーキテクトにアーキテクチャと検証能力を集中研修するプロジェクトを興す必要があろう。

欧米ではアーキテクチャと形式手法を駆使出来るコンピュータ・サイエンスの博士数百名（推定）が1960年代以降の40年間で実社会に出てこれらの仕事をしているという。日本はどうだろうか？　残念ながら、最近20年のバブル崩壊後、不景気対応に追われ、多くの民間企業にはそこまでの余力が無い。そのため、国がリードすべきであろう。今、本腰で強化しなければ日本が尊敬される未来は実現出来ないのではないかと危惧している。

2 高信頼性検証能力への投資は経営的に成り立つのか？

情報システムのコストは、金融業務システムや航空会社等の業務システムでは膨大と広く知られているが、それ以上に半導体工場の自動化設備等の設備投資では数千億円単位である。また製品開発には開発費だけではなく、失敗や補償のためのコストも含まねばならず、衛星1個の打ち上げ失敗の損失は保険を入れると200億円、自動車はもちろん、1個1個は安い携帯電話、ペースメーカやAED※18等でもリコールコストや人命、飢餓等の補償金等を入れれば1件で何百億円になりかねない。航空機であれば約数百億円以上、宇宙船になれば数千億円、原子炉やITSやスマート・グリッドの構築等大規模なインフラシステムにおける致命的損失となれば兆円レベルにも及ぶ可能性がある。よって事故や不具合がソフトウェアやシステムに絡んで起きたりするリスクに対しては、企業存続どころか国家の威信をかけて取り組まなければならないものもある。

事故や不具合における非がベンダにあったとしても、発注側であるユーザにも、検収した責任があるであろう。社会がソフトウェアやシステムに対してますます高い信頼性を求める環境においては、開発規模が増大していく中で、経営者はコストと信頼性を鑑みながら投資しなければならない。そのためには、高信頼性保証の自己管理能力を確保することであり、そのための人材教育が必要であるが、育成には大学卒で数年から10年はかかる。

2.1 不適当なソフトウェアテストによって生じた経済コストの証言-1

ソフトウェアの信頼性に対する議論を高める火付け役となったのは、2002年5月に米商務省技術標準局（NIST※19）が発表した“The Economic Impact of Inadequate Infrastructure for Software Testing”という報告書である。この中で、不適当なソフトウェアの品質と、そのテスト方法が不適切なためのコストが米国経済全体で年間595億ドル、そのうち約1/3（223億ドル）は、最適なテストが実行されていれば不必要なコストであったと報告されている。更に、ベンダでなく、“ユーザ”がソフトウェアの欠陥を修復する費用が約60%（383億ドル）に達していると報告されている。

2.2 アーキテクチャ管理が高信頼性管理の基礎であることの証言-2 —エンタプライズ・アーキテクチャの必然—

1980年代後半米国国防総省において、システムトラブルを原因とする幾つかの事故が起きたという。この時の原因調査委員会が、その真の原因は、プログラマのエラーではなく、陸海空軍がベンダごとに固有の、部分的に相互接続性に問題のあったアーキテクチャで設計されたことにあったと指摘した。このことから、オープンな共通アーキテクチャを確立するために、TAFIM※20という共通のアーキテクチャ設計ガイダンスが1986年に最初に書き始められ、1995年に完成した。TAFIMは、既に大統領府予算管理局と米国国防総省のDISA※21に渡されており、1994年にはDISAから正式にThe Open Groupに渡され、1995年

※16 SEI：Software Engineering Institute
※17 RFP：Request For Proposal
※18 AED：Automated External Defibrillator，自動体外式除細動器
※19 NIST：National Institute of Standards and Technology
※20 TAFIM：Technical Architecture For Information Management
※21 DISA：Defense Information Systems Agency，米国国防情報システム局

に官民両用に使えるオープンアーキテクチャとして、TOGAF1という名称で発行された。その後改訂が進められ、2002年にTOGAF7で技術アーキテクチャ、DODAF設計にもマッピングされ、2002年にTOGAF8でビジネス、2009年にはTOGAF9でソリューションアーキテクチャへの橋渡しがされた。現在では、TOGAFホームページから12万件ダウンロードされ、80カ国、1万4,000人がTOGAF9を含めThe Open Groupのアーキテクト認証者となっている。米国国防総省・英国国防省がDODAF/MODAFを推進したことは、“ディペンダビリティはアーキテクチャに始まる”という最初の教訓となった。一方、日本でのEAは遅れており、民間ではEAの実践がほとんど進まず、外資系以外は例外を除いて、人事的にアーキテクトという職種がユーザにも、ベンダにも定着していない。

なお、The Open Group の Dependability Through Assuredness WGではTOGAFと形式手法をつなぐことを目標に、AADLグループとも交流し、コンピュータで実行出来るアーキテクチャの研究を続けている。

2.3 アーキテクチャ段階でのエラー摘出が高信頼性確保の基礎であることの証言-3 —アーキテクチャの段階で正しい要件を正しく表記し、誤謬を排除出来るかが鍵—

高信頼性システム開発には、EAとして正規にアーキテクチャを構築するプロセスを実施し、その要件定義に関係する部品間、アクター間の関係条件をモデル化し、形式手法を駆使して、その“正しさ”を検証する必要がある。

2.1節で紹介したNIST発表の2002年の論文に基づきSEIは、経営者に認識して欲しいとしたポイントを以下のように報告している。

これは、要求から設計完了までのアーキテクチャを決める段階の管理こそ高信頼性確保と検証の要であるという証明である。

①要求からコンポーネント設計の終了までに、ソフトウェアシステム全体の70%のエラーが発生し、組み込まれる。そのうちこの段階でエラーとして発見されたのがたった3.5%であり、この段階で直すコストを1とする。
②コーデイング・ユニットテスト段階で組み込まれたエラーは20%だが、16%はこの段階で見つかり、ここで直せればコストは5。
③インテグレーションテスト・システムテスト段階で生まれるエラーは10%だが、ここで見つかるエラーは50.5%で、エラーを修正するコストは10。
④アクセプタンス(検収)テストで組み込まれるエラーはゼロだが、見つかるエラーは9%、修正するコストは15。
⑤その後出てくるエラーはなんと20.5%もあり、修正コストは30。

本記事を読まれる経営者の皆様は自社において上記①～⑤をチェックされ、問題があれば解決策を提案するようにCIOに指示をして欲しい。

先の2.1節の証言-1では、適正な検証法があればテストのコストの37.5%がセーブ出来、本節の証言-3では、要求からコンポーネント設計の終了までに70%のエラーが発見され、訂正されると見て44%、楽観的には、70%超のテストコストの節約が出来ると指摘されているが、実際にそれを行う方法については答えが出ていない。私はこの4年間にThe Open GroupのDependability Through Assuredness WGを通して、アーキテクチャ・フォーラムのメンバ等に個人的に会い、意見を聞いた。Tony Hoare、Daniel Jackson、Manfred Broy、Patrick Cousot氏ら世界の形式手法の巨匠たち、NASAやBoeing、Lockheed Martin、Rockwell Collins、Raytheonらのアーキテクトたちとの議論で得た私の上記コスト節約に関する結論は、①オープンで標準化された正規のEAプロセスを通して要件とビルディングブロック間の関係を精査し、②問題の性質に合わせて、多角的な複数の形式手法の最適適応による信頼性確保を基本とすることである。

3 標準化された正規のEAプロセスと多角的な形式手法の最適適応と信頼性確保が基本

—日本ではアーキテクチャも形式手法も世界から10年以上は遅れていると思われる—

3.1 アーキテクチャの定義

アーキテクチャの定義に関し、IEEE Std 1471 : ISO/IEC 42010を少し拡張したThe Open Groupの定義は次の通りである。

「アーキテクチャとは、複数のコンポーネントが一体となった共通の目的を持った組織体が、現在の、各コンポーネントと全体、またコンポーネントの相互関係や環境との関係を論理的に表現し、未来のターゲット・ゴールに向けて、いかにこれを設計し、発展させるかのプリンシプルである。」

3.2 形式手法の定義

形式手法の定義は、「設計の正しさの証明を集合論・論理学・数学を土台に証明するフォーマルな検証理論」である。方式的には述語論理証明によるLCF、VDM、Bメソッド、Z言語等に対し、最近はライトウエートな新しい形式手法として、次の2つ等が登場してきた。

① MITのDaniel Jackson教授のALLOY※22
②コンピュータ処理能力が向上したことから静的アナライザとして形式化する *École normale supérieure Paris* のPatrick Cousot教授の抽象解釈によるモデルチェック方式

3.3 EAも形式手法も抽象化・論理化が基礎

形式手法を経験した誰もが感じる困難は、高い抽象化能力を持った“形式手法アーキテクト”を育てることだと言う。この抽象化はシステムが高度化しソフトのステップが数億ステップになるシステム複数を相互に接続するには、高信頼性システムが必要となる。このような構造の精密性・強靭性を確保するためには、高度な抽象化能力が必要になり、また複雑性を抽象化・単純構造化するトップダウン設計を行った上で、形式手法を駆使して無矛盾性を確保する必要が出てくる。

1990年頃から生まれてきたEAは、まさに、企業やその製品群、プロジェクトの目標から構造、成果物を設計するための抽象化プロセスの標準化であり、テンプレートであり、マネージメント・プラクティスである。

アーキテクチャは、howのエンジニアリングではなくwhat、who、where、when、why、why notを追求するサイエンスと考えるのが適切である。アーキテクチャが、正確に、パラレルプロセスを可能に出来る形で、トップダウンで、抽象解釈された分割設計出来れば、指数関数的に広がる状態推移のモデルチェックにも形式的検証の一般での利用のフィージビリティが現実味を帯びてくる。

4 形式手法を駆使した高信頼性確保の標準化の今後の課題

4.1 ディペンダビィリティ（高信頼性）は経営の目標、アーキテクチャはその構造設計方式で、形式手法はその検証手法

経営者の方には、次の方法を提案したい。「自社の長期計画と短期計画のゴールと経営プリンシプルに合わせて、最適統合性確保のためにEAを駆使し、提供する主力製品やサービスの関係をモデル化し表現する。」このための最初のステップでは、経営面で①経済性、②生存持続性、③顧客満足度、④グローバル・オープン対応性の4つのビューポイントをEA的に確認する。その後、ディペンダビィリティに関し、下記の非機能6つのビューポイントでアーキテクチャのモデル検証を、出来れば形式手法を駆使して総合的検証を行う。

①安全性（Safety）の証明、②信頼性（Reliability）の証明、③可用性（Availability）の証明、④機密保持性（Security）の証明、⑤統一性（Integrity）の証明、⑥保守サービス性（Serviceability）の証明。

米国では、高信頼性システム検収において、ある条件下で形式手法が要求されており、そのための「非機能条件に対する検証の調達ガイド」として、DO-178BやDO-178Cが存在している。

4.2 アーキテクチャ・ベース・ディペンダビリティの専門課題と今後の課題

今後の課題を以下に列挙する。

①アーキテクチャのオープン統合はTOGAFで統一。
②コンピュータで実行可能なアーキテクチャに関する統合標準言語の策定—AADL、Archimate※23、SPEM2※24の位置付けと標準化—。
③トップダウン設計と並列処理を意識したアーキテクチャ分割の仕組みの確立。
④UML2、SysML2、AADL2とのインタオペラビリティを持つモデル化でTOGAFソリューション・トレーサビリティを確保。
⑤抽象解釈モデルに必要な上位モデルと下位モデルとのディペンダブルな関係のモデル化、そして抽象解釈の定式化と自動化への挑戦。
⑥設計から検証までアーティファクト（生成物）を一貫管理する設計支援・検証レポジトリーの確立。

5 提言：2030年に向けアーキテクチャ・ベース形式手法の産業戦略提案

5.1 製造産業の高品質ブランド戦略

最終目標としては、世界の高品質機器産業と先端成長各国の先端的インフラ事業を日本が取り込むことであろう。

ものづくり日本の次世代産業政策は、自動車やロボテックスの技術力の土台の上に、より高度な、高信頼性を保証するリアルタイム分野、国防、航空、宇宙に環境バイオ等次世代社会インフラ分野での超複雑で、安全性を担保するシステム開発と検証能力の分野へシフトしていくべきであろう。そのためには“アーキテクチャと形式検証によるディペンダビィリティ”能力確保とブランド化を達成するための20年プロジェクトとするべきであろう。

5.2 インフラサービス産業の高品質ブランド戦略

サービスビジネスのプロセスを顧客中心主義経営に基づくEAの手法で分析し、ボトルネックを発見し、長期的なシナリオで、このサービスサブセクターごとの生産性を創造的に向上させる“サービスのインテリジェント装置化”を興すべきであろう。次世代の例を自動車で言えば、現在の高級車は1,600万～2,000万ステップのソフトウェアと80個以上のECU※25を搭載しているが、次世代高級車では2～3億ステップ、将来のITS時代には宇宙・航空機と同じく10億ステップのソフトウェア開発が必要だという。業種別サービスのモデル化・形式化を通して生産性と信頼性を追及する狙いだが、IT関係では、システム・インテグレーションやサービスの形式手法を組み込んだ検証法の確立も重要な分野である。しかし、これは旧来の開発・検証方式では行えるものではない。

アーキテクチャと形式手法がシームレスに統合されたアーキテクチャ・ベース・モデル検証方式の確立と形式検証アーキテクトの育成が鍵となる。このクラスのアーキテクトを育成するには10年単位の研究・研修・現場経験サイクルが必要である。

“高信頼性は日本から”を合言葉に、20年計画で、EAアーキテクト及び形式手法検証アーキテクトを、自社SEと協力会社SE総数の3～5%とするための育成計画が必要だ。これを実現するためには、“高信頼性は日本から”という世界のマーケットに向けた産官学のプロジェクトが国家の重要政策として必要であろう。

※22 ALLOY：仕様記述言語，ALLOYはBメソッドとZ言語の合金を目指して名付けられた。
※23 Archimate：EA記述用の言語
※24 SPEM2：メタ・プロセス記述用の言語
※25 ECU：Electronic Control Unit