1. フォーマルメソッド応用に関する背景

電力、通信、金融分野等の重要インフラシステム、自動車、鉄道、航空機、医療機器等のセーフティクリティカル・システム[4]、情報家電等の様々な分野においてソフトウェアの大規模化、複雑化が日々進んでいる。このような中、ソフトウェアの不具合に起因する大規模な事故がしばしば発生していることから、ソフトウェアの安全性・信頼性[5]等を確保するための技法や工夫に対する要求が高まっている。

米国商務省技術標準局(NIST)は、ソフトウェアの品質等に関わる問題提起をするレポートにおいて、ソフトウェアの不十分な品質と、テスト方法の不適切さのために発生する損失が米国経済全体で年間 595 億ドル(約 5 兆 4000 億円)[6]に達すると報告している。

このような問題に対する対策アプローチの一つとしてフォーマルメソッド(=形式手法)に注目が集まっている。欧米では、鉄道、航空機、金融、セキュリティ分野などにおいて、ソフトウェアの安全性・信頼性を高めるためにフォーマルメソッドを適用した実践的な事例が増えている。フォーマルメソッドは、システムやソフトウェアの要求や設計仕様を、数学的に意味付けられた言語を用いて記述し、ツールを用いた論理的な検証[7]を行うことにより、従来のソフトウェア・テストでは困難であった性質の保証や不具合の検出などに利用される技術である。

フォーマルメソッドの導入効果として代表的なもには以下のようなものがある:

- 品質向上による事故損害リスクの低減

  従来のテストでは検出できない不具合の検出や、厳密な仕様記述を通じて設計者とプログラマーの間で生じる誤解の防止などにより、ソフトウェアの品質を向上し、事故損害のリスクを低減する。従来のテストでは、並行動作するシステムのタイミングに関する検証は困難である。

- 品質に関する客観的な保証や説明責任の向上

  論理に基づく検証により、検証結果に対して一定の保証を与えることが可能になる。これにより、人命や重大なセキュリティに関わるシステムの動作や性質の正しさについて一定の保証を与えることができる。重要インフラ事業者やセーフティクリティカル・システムの提供者は、利用者に対してシステムの安全性について十分な対策をとっていることを示すことが求められており、そのような要求を客観的に示すことに適している。

- 開発効率やプロセスの改善

  開発プロセスの要求や設計等の上流に重点を置くことにより、不具合を早期に取り除き

---

[4] システムの障害が、人命や身体を危険に陥れるような可能性のあるもの。

[5] ソフトウェアの信頼性、システムの信頼性、安全性の違いや関係については、第 6.1 章で詳しく記述する。

[6] NIST Study, Planning Report 02-3: "The Economic Impacts of Inadequate Infrastructure for Software Testing", 2002

[7] ソフトウェアに対してテストデータを与えて実行することにより検査するのではなく、ソフトウェアの仕様や前提などから、論理的な推論に基づき満たされる性質を検証する。

見通しの良い開発プロセスとすることで、開発の生産性を向上する。

従来のソフトウェア開発のように作ってしまってから下流工程でテストを行う場合、見つかった不具合の修正に大幅な手戻り工数が発生していた。フォーマルメソッドの利用により、要求、設計等の開発の上流工程においてある程度の検証や解析が可能となり、プログラムを実装する前に早期に問題を発見し、下流工程からの手戻り等のコスト発生を防止する。

フォーマルメソッドによる品質向上の効果を考える上で、事故リスクの損害規模の把握が重要である。通常、ソフトウェアの利用者や開発者は、ソフトウェアに関わる事故リスクとして、サービスや業務の停止による収益の逸失、復旧コスト、リコール・回収コストなど直接被害を想定することが多いが、企業に対する信用失墜により、将来に渡るビジネスへのマイナス影響を含む企業価値への影響を十分に認識されていることは少ない。情報セキュリティ経済学の分野では、情報システムに関するセキュリティ事故によるこのような企業価値への影響を評価する手法について検証が進んでおり、直接被害以上に信用失墜のマイナス影響が大きいことが示されている[8,9]。例えば、情報システムの不具合等による情報セキュリティ事故(不正アクセス、機密情報漏洩等)に係わる日本の上場企業が抱える潜在リスクは 29 兆円と見積られ、一社平均 79 億円の潜在リスクを抱えている。このようなリスクが十分に認識されていないことは深刻な問題である。

我が国の情報セキュリティ政策を検討する情報セキュリティ政策会議(議長:内閣官房長官)において決定された国の中期戦略「国民を守る情報セキュリティ戦略」(2010 年 5 月)においては、情報家電、モバイル端末、電子タグ、センサ等あらゆるものがネットワークに繋がる環境において情報セキュリティを確保する方策として、開発者に対する検証ツールや安全性評価体制の整備等の環境整備・技術課題の解決を図ることを掲げている。また、「国民を守る情報セキュリティ戦略」に基づき策定された年次計画「情報セキュリティ 2010」においては、情報技術の社会基盤化に伴い、情報システムに起因する事故が、経済活動全体の停滞や国民生活の生命・財産そのものにかかわるリスクをもたらしかねない状況が生まれつつあるため、対症療法的ではなく根本的な問題解決を目指した技術への取り組みを掲げている。このように、政府としても、情報システムやソフトウェアの品質を高めるための根本的な技術の確立に力を注いでいる。

一方、新興国を中心とした鉄道や電力など社会インフラ投資の増加、組込みシステム等の市場のグローバル化、ソフトウェア開発のオフショア・アウトソーシングの増加など、グローバル化が進む経済活動において、我が国のソフトウェア産業が国際競争力を向上させるために、品質の高さ追求することのみならず、品質の高さを客観的に説明する努力が求められている。また、経済・社会生活に浸透したソフトウェアを含むシステムの品質に対して、利用者である一般国民に対する説明責任も求められている。フォーマルメソッドは、鉄道、航空、プラント、セキュリティなどさまざまな分野における安全性・信頼性を確保するための手法として国際標準の中で採用され、国際的

[8] 経済産業省、「グローバル情報セキュリティ戦略」、2006

[9] Masaki Ishiguro, Hideyuki Tanaka, Kanta Matsuura, The Effect of Information Security Incidents on Corporate Values in the Japanese Stock Market, WESII 2006

に受け入れられる技術として活用することができる。さらに、オフショア・アウトソーシング[10]が国際的に進展する中で、これまで日本が得意としてきたものづくりの方式が変化してきている。今後、国内のソフトウェア関連企業は下流工程で付加価値を確保することが難しくなっており、付加価値の高い要求や設計などの上流工程で収益を確保するものづくりの方式を実現する上でフォーマルメソッドの導入は有効と考えられる。

以上のように、ソフトウェア開発に関わる環境は大きな転換期を迎えている。ソフトウェアに関わる事業者、発注者、開発者は、ソフトウェアの安全性・信頼性・セキュリティを確保するための有望な技術としてフォーマルメソッドに注目し、組織としての導入とその方法について具体的に検討する時期に来ている。

フォーマルメソッドには、様々な有効性があるにも関わらず、欧米と比較して国内の開発現場にはあまり導入が進んでいない。その理由として以下のようなことが挙げられる:

- 従来のソフトウェア開発手法を利用する開発者にとって、馴染みの無い概念やスキルが必要となり、新たな取組みのきっかけが得にくい。
- 実績に関する情報が得にくく、また、コストと効果に対する評価が難しいため、導入の意思決定が難しい。
- 導入初期の障壁を乗り越えるための組織としての導入ノウハウや留意点を示したガイダンスが少ない。

本導入ガイダンスは、このような障害を緩和し、フォーマルメソッドを開発現場へ普及促進させることを目指すものである。特に、フォーマルメソッドの費用対効果については、定量評価が難しい部分もあるが、第 5 章において費用と効果の全体像を示し、具体的なデータを示すことで、どの程度の評価が可能か示すようにした。

[10] 開発等を含む自社内の業務の一部までゃ全てを物価の安い海外(オフショア)の外部企業に委託する形態。