フォーマルメソッド導入ガイダンス

～ソフトウェアの安全性・信頼性向上のための技術導入に向けて～

Version 1.0

2011 年 6 月

株式会社 三菱総合研究所

はじめに

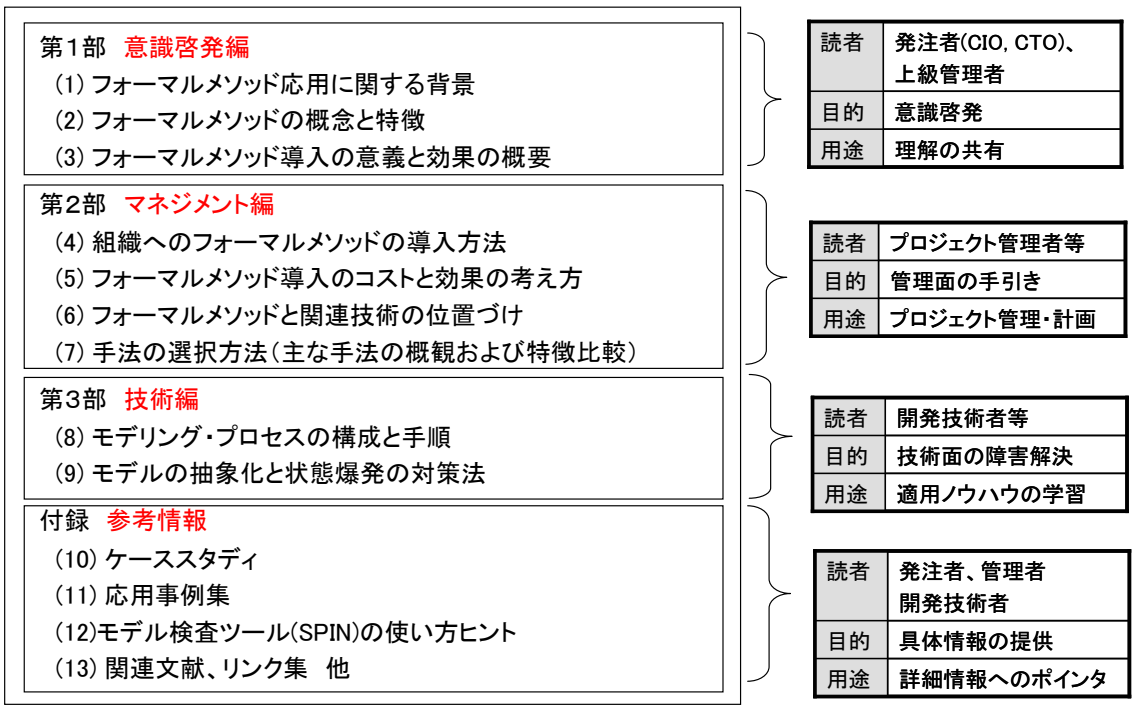
本導入ガイダンスは、ソフトウェアの信頼性・安全性等を向上させるための技術であるフォーマルメソッド（＝形式手法）を開発現場に普及促進させることを目的として、経済産業省「新世代情報セキュリティ研究開発事業」における委託プロジェクト「モデル検査による組込みソフトウェア検証とモデリングパターン化の研究開発」において作成したものである。導入ガイダンスは、フォーマルメソッドやソフトウェア開発に関わる国内の有識者から構成されるフォーマルメソッド導入ガイダンス検討委員会（18 章に記載）においてレビューしたものである。

本書の目的

ソフトウェア等の安全性、信頼性、セキュリティ等の向上に関わるフォーマルメソッドをソフトウェア関連産業の開発現場に普及させるために、普及の障害となっている問題点に対して、マネジメント面および技術面の具体的な解決策、手順、考え方、ノウハウ等を示す。本ガイダンスにより、フォーマルメソッドの有効性や限界を把握し、その導入効果が期待できる対象や方法を判断しつつ、具体的な導入を行う際の手引きとして利用されることが期待される。

本書の構成と対象読者

本書は、ソフトウェアの開発や利用に係わる関係者や組織で読まれることを想定している。4つのパートから構成され、それぞれの想定読者は大まかに章構成の右に示したとおりである。



第 1 部は、フォーマルメソッドに初めて接する人のための意識啓発を目的にフォーマルメソッドの概念や効果について示す。主に、ベンダー上級管理者や情報システムユーザ企業・事業者のCIO[1]、CTO[2]に向けた内容をまとめる。第 2 部は、フォーマルメソッド導入に関するプロジェクト管理における留意点や考え方をまとめる。主にベンダー上級管理者、開発プロジェクト管理者、開発技術者などに向けた内容をまとめる。第 3 部は、モデル検査を対象として、具体的な適用方法や技術的困難を解決する方法を示す。主に、開発技術者に向けた内容をまとめる。最後に、付録では、実システムに対するケーススタディ、フォーマルメソッドの実践応用に関する概要情報の事例集、手法選択に関する情報源等をまとめる。導入ガイダンス本編から参照される。

本書が対象とする情報システムは幅広く、重要インフラシステム、セーフティクリティカル・システム、家電など特定のハードウェアに組み込まれて利用される組込みソフトウェアから汎用システムによるエンタプライズ系への適用が想定される。

本書の対象範囲と読み方

フォーマルメソッドを開発現場に導入するための方法やノウハウは、マネジメントから技術に至るまで幅広い範囲に渡って必要となる。プロジェクトマネジメントを行う管理者とシステムやソフトウェアの設計開発等を主に行う技術者のそれぞれに求められる手法、ノウハウを、マネジメント領域と技術領域に分類すると大まかに下表のようにまとめることができる。

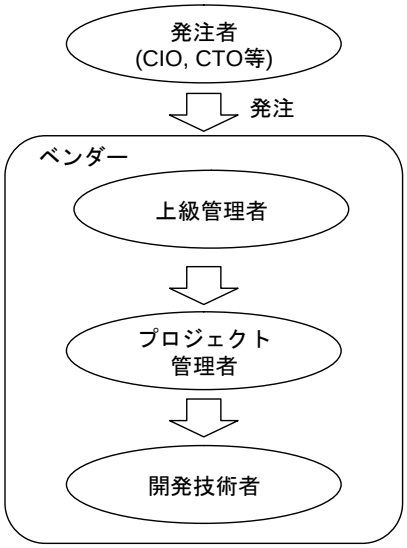
領域		対象者	
		管理者向け	技術者向け
	意識啓発	●形式手法を取り巻く環境と背景 ●形式手法の概要と特徴 ●導入効果と意義	●形式手法の概要と特徴 ●手法の比較情報 ●ケーススタディ
	組織管理・ プロジェクト管理	●費用対効果と具体的情報 ●組織への新技術の導入方法 ●形式手法導入の留意点 ●導入プロセスの手順	
	要求分析、 設計		●設計検証プロセス・アプローチ ●モデルの抽象化・状態爆発への対処 ●検証性質の記述パターン ●SPINオプションの使い方
	実装		(モデル検査ガイドブック(メルコパワー)等)
	テスト		(テストカバレッジの計測(VDMtools))

[1] CIO:最高情報責任者(Chief Information Officer)。企業において情報に関する資源を統括する最高責任者。

[2] CTO:最高技術責任者(Chief Information Officer)。企業において技術面を統括する最高責任者。

本ガイダンスは、管理者向けの意識啓発、組織管理、プロジェクト管理と、技術者向けの要求分析や設計などの上流工程に重点を置く。また、フォーマルメソッドの導入に関して、既存の文献ではあまり扱われていない領域のうち優先度の高い部分に重点を置くもので、フォーマルメソッドの導入方法を幅広く網羅するものではない。フォーマルメソッド導入の費用と効果の評価は困難な課題であるが、困難であることを理由に放置することなく、情報セキュリティ経済学などの関連する専門分野における知見に基づき、現在分かっていることや、何が困難であるかについて可能な限り示すことに努めた。技術編は、要求分析と基本設計工程を対象とし、実装やテスト工程は、既存の文献に委ねるなど、本ガイダンスの対象範囲を選別した。第 17.1 章などに示す既存の文献で具体的な方法が示されている領域については、本文でそれらの文献を参照することにより、本ガイダンスと合わせて活用して頂くことを想定する。

本書は、章ごとに想定される読者層が異なる。ここでは、フォーマルメソッドに関わるステークホルダーを大まかに下図のように考える[3]。



それぞれのステークホルダーの位置づけと本ガイダンスの読み方は以下の通りである。

(1) 発注者（CIO、CTO 等）

発注者は、ベンダーに対して情報システムの開発を委託する組織である金融機関、重要インフラ事業者、情報システムのユーザ企業や政府などの組織において情報システムに関する技術的な責任を持つチームや CIO, CTO を指す。これらの人は、フォーマルメソッドを直接利用することはあまり想定されないが、厳格な受入れテストのためにフォーマルメソッドを理解することが求めら

[3] ステークホルダーには、ここで挙げる主体以外に、製品・サービスの利用者、事業会社の株主、部品サプライヤー、開発コンサルティング会社などが存在するが、ここでは開発現場へのフォーマルメソッド導入という観点で関連の深い主体を対象とする。

れる場合も考えられる。

これらの読者は、第 1 部の意識啓発および、第 2 部の費用対効果の章を読むことで、フォーマルメソッドの導入に関する考え方や参考情報が得られる。また、発注者であっても、納品物の検査などにおいて、フォーマルメソッドの適用結果をレビューする場合には、第 2 部および第 3 部、付録のケーススタディなどを読むことを勧める。

フォーマルメソッドのような新しい技術をベンダーが導入するためには、その費用対効果について発注者からの理解が得られることが重要である。ソフトウェアの不具合に起因する事故リスクなど、発注者の視点からシステム納入や出荷後の影響も含む費用対効果を考慮して、意思決定することが重要である。

(2) 上級管理者、プロジェクト管理者

ベンダーにおいて開発プロジェクトの責任者となるプロジェクト管理者と、その上位の立場にある上級管理者は、フォーマルメソッドの導入について意思決定を行う立場にある。フォーマルメソッドに初めて接する人で、直接フォーマルメソッドを使う立場には無い場合が多いと想定されるが、導入意思決定において、フォーマルメソッドの効果や制約を理解することが重要である。フォーマルメソッドは、単一のプロジェクトで最初から採算性を確保することは困難な場合が多く、複数のプロジェクトを想定して組織として導入意思決定が行える上級管理者の理解が重要である。委託開発ではなく、製品開発の場合、ベンダーが発注者と同様の視点をもつことも求められる。

これらの読者は、第 1 部の意識啓発の章をよみ、フォーマルメソッドの概要とその意義について知るとともに、第2部のフォーマルメソッド導入における留意点と費用対効果の章を読むことで、プロジェクト管理者等の現場の責任者と協力して、フォーマルメソッドの導入判断を行う。

(3) 開発技術者

開発技術者は、開発現場において実際にフォーマルメソッドを利用する人を想定する。読者として、はじめてフォーマルメソッドに触れる人とすでに利用経験のある人を想定する。初めてフォーマルメソッドに接する読者は、第 1 部を読むことでフォーマルメソッドの概要と意義を理解する。第 2 部はマネジメント編であるため、詳細に理解する必要はないが、マネジメント層とのコミュニケーションを円滑に行うために役立つため、目を通し、フォーマルメソッド導入プロセスの全体像を把握し、プロジェクト管理者をサポートする知見を得ることが望ましい。第 3 部の技術編は、既存のフォーマルメソッドに関する入門書を読んでいることを想定しており、既存のテキストを参照しつつ、それらを補完するノウハウを提供する。

フォーマルメソッドをすでに実践している人にとっても、第 1 部、第 2 部は有用である。また、第 3 部を読むにあたって、フォーマルメソッドに関する基礎的な知見があれば、そのまま第 3 部に読み進むことができる。さらに、付録のケーススタディなども参考に読むことを勧める。

第2章以降の本編では、各章の最初に想定読者と前提知識等を記載することで、読者に指針

を与えるようにした。