4. 組織へのフォーマルメソッドの導入方法

本章では、フォーマルメソッドを組織に導入する際の障害を解決するための手順やポイントを示す。本章の概要は以下の通りである。

対象読者	(1)ベンダー上級管理者 (2)開発プロジェクト管理者 (3)開発技術者、等
目的	フォーマルメソッドを組織に導入する際の作業プロセス(導入プロセス)と導入のポイントについて整理する。さらに導入検討の際に有用と思われる情報源(研修サービス、コミュニティ等の情報)についても現状をまとめる。
想定知識	ソフトウェア開発プロセスの概略。
得られる知見等	● フォーマルメソッドの導入プロセス ● 導入のポイント ● 導入検討に有用な情報源(研修サービス、コミュニティ等の情報)

4.1. フォーマルメソッドの導入プロセスパターン

フォーマルメソッドを組織に導入する際の手本となるプロセスを導入パターンとして示す。これらのプロセスパターンは、国内の企業・団体(約10組織)におけるフォーマルメソッド適用に関する代表的な事例(表 4-1)およびフォーマルメソッド導入関する留意点等をまとめた文献[21],[22]等に基づき、典型例をパターンとしてまとめたものである。

表 4-1:導入プロセスの参考としたフォーマルメソッド適用事例

適用対象	適用の目的	手法・ツール	導入組織
IC カードファームウェア	仕様記述、検証	形式仕様記述言語 VDM++、VDM Tools、モデル検査 SPIN	開発組織
鉄道信号システム	仕様記述	形式仕様記述言語 VDM	開発組織
運賃計算システム	仕様記述	形式仕様記述言語 VDM＋＋、VDM Tools	開発組織
複写機制御ソフトウェア	検証	モデル検査 SPIN	開発組織
電力関連システム	検証	モデル検査 SMV	開発支援組織

[21] Jonathan Bowen, Ten Commandments of Formal Methods, Ten Years Later, 2006, Computer, Vol. 28,. No.4, pp.56–63.

[22] Jonathan P. Bowen and Michael G Hinchey, Seven More Myths of Formal Methods, IEEE Software, 1995, Vol.12, pp.34-41

宇宙制御システム	検証	モデル検査 SPIN,UPPAAL,他	開発支援組織

パターンは、適用の目的と導入組織の役割によって表 4-2 の通り、仕様記述導入パターン(開発)、検証導入パターン(開発)、検証導入パターン(開発支援)の 3 つのパターンにまとめている。

表 4-2:導入プロセスのパターン分類

		適用の目的	
		仕様記述	検証
導入組織	開発組織	仕様記述導入パターン(開発)	検証導入パターン(開発)
	開発支援組織	―	検証導入パターン(開発支援)

各パターンとも導入の工程として、おおよその手順は共通している(各パターンにおいては導入工程における各フェーズの実施内容が異なっている)。その手順と本ガイダンスの参考箇所との対応は以下の通りである。

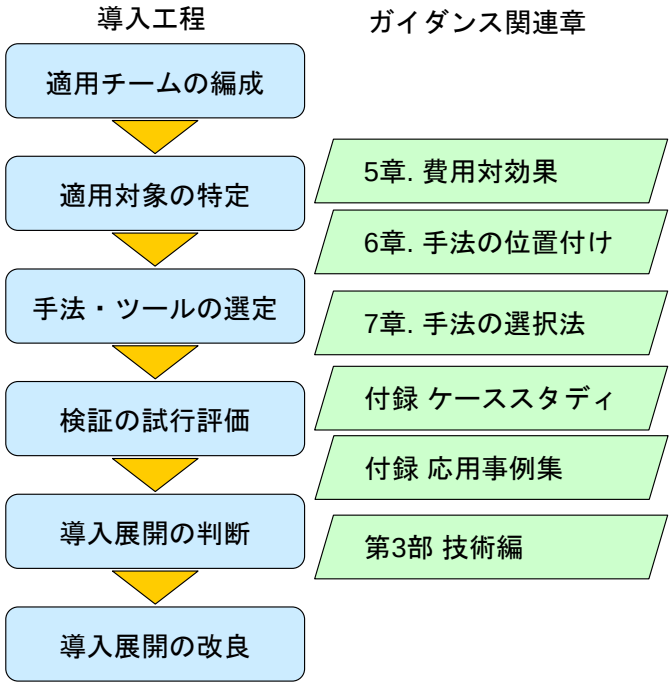

図 4-1:導入プロセスの概略(共通部分)

上記の3つのパターンは導入を成功に導く典型例を示すもので、広く網羅しているわけではない。たとえば、仕様記述を適用の目的とし、開発支援組織が導入する際のパターンは成功事例の情報が得られなかったため、提示していない。ただし、上記の導入パターンの仕様記述導入パタ

ーン（開発）と検証導入パターン（開発支援）を参考に導入手順を検討することは可能である。実際に導入する際には、ここで提示しているパターンを参考に、各自の組織環境、適用対象などの事情に合わせて、導入計画を検討することが重要である。

各パターンの記述項目は以下の通りである。

項目	内容
導入組織	フォーマルメソッドを適用する組織。たとえば、システムの設計やソフトウェア開発を行う開発部門、システムの検証を担当する組織や品質管理部門、ツールや方法論等の整備普及を行う組織等。
適用対象	フォーマルメソッドを開発工程のどのフェーズでどこに適用するか。たとえば、新規開発システムの仕様記述や設計書に対する検証、既存システムの仕様書に対する記述、既存システムのプログラムコードに対する検証等。
導入によって解決したい課題 （適用の目的）	フォーマルメソッドによって解決したい課題。たとえば、仕様書の品質向上（曖昧な記述、記述漏れやあやまりの除去）、設計段階でのシステム検証、既存システムの不具合除去やテストではカバーできない検証の実施など。
利用する手法・ツール	形式仕様記述言語、モデル検査等のフォーマルメソッドの手法と具体的なツール例。
導入手順	フォーマルメソッドの導入計画、準備から実施にいたる作業項目。たとえば、適用対象の特定、情報収集とツールの選定、有効性評価、ツール・ドキュメント整備、教育、本格導入と評価等。
参考事例	当該パターンのベースとなった具体的事例に関する情報。

以下に各パターンの具体的な手順を示す。それぞれベースとなる事例は存在するが、パターンとして抽象化・整理を行っているため、実際の事例における導入の経緯とは異なる点もあることに留意されたい。

4.1.1. 仕様記述導入パターン（開発）

- 導入組織
  組込みシステム・制御システム、企業情報システム等の開発部門におけるソフトウェア開発チーム。
- 適用対象
  フォーマルメソッドを開発工程の中に組織的に組み込む。具体的には、システム開発の上流工程（外部仕様書あるいは機能仕様書の作成）にフォーマルメソッドを適用する。

- 導入によって解決したい課題

  外部仕様書の品質確保（記載した内容の曖昧性、記述漏れ、間違いの排除）。開発従事者間における仕様・設計に関するコミュニケーションの改善。
- 利用する手法・ツール

  形式仕様記述言語およびツール（VDM++および VDM Tools、B method および Atelier B 等）。ただしモデル検査ツールの活用でも課題解決に繋がるケースもある。
- 導入手順

  (1) チーム編成

  形式仕様言語の導入検討、準備、推進を行うチームを編成する。推進チームは、ソフトウェアエンジニアリングに関する知見を持つ者や、形式仕様言語の有効性・限界を把握している者で構成する。推進者の負担軽減とフォーマルメソッドの適用における困難な問題を解決するために、外部有識者からの協力を得られる体制を構築する。

  推進チームは以降の活動を行う。

  (2) 適用対象範囲の特定

  開発対象となるソフトウェアにおいて、ソフトウェア全体の開発に形式仕様言語を適用するのか、一部のモジュールに適用するのか、その範囲と適用する詳細度を特定する。詳細度は、要求仕様、基本設計、詳細設計等の適用するレベルの選択を意味する。

  (3) 手法・ツールの選定

  適用対象とするソフトウェアの外部仕様書の作成に対し、手法の特徴、適用実績、ドキュメント・書籍やツールのサポート状況等の観点で候補となる手法・ツールを選定する。ドキュメント・書籍等で得られる情報には限界があることから、手法を熟知している外部有識者から技術指導を受けることが効果的である。《手法・ツールの選定にあたっては、本ガイドの「7. 手法の選択方法」も参照のこと》

  (4) 適用の試行・評価

  開発対象となるソフトウェアの一部あるいは類似の小規模なソフトウェア等を対象に選定した手法の適用を試行し、手法の有効性を評価する。手法やツールの適切な利用方法、限界を踏まえて評価を行う必要があるため、手法・ツールを熟知している外部有識者と共同で試行評価を行う。また、実際の記述では、対象システムのドメイン知識が不可欠となるため、当該ドメインに詳しい者の協力が必要である。

  (5) 導入可否の判断

  上記の試行評価の結果から、導入可否の判断を行う。導入を決めた場合は、導入計画を策定する。導入準備、プロジェクトへの適用および評価等で以降に記すような活動を計画し、そのための体制を確保する。《導入可否の判断に関しては、費用対効果の面での検討も必要である。本ガイドの「5.フォーマルメソッド導入に関するコストと効果の考え方」も参照のこと》

  (6) 周辺環境の整備

導入の準備として、開発チームのメンバーに手法・ツールを使ってもらうための周辺ツールの整備（対象ソフトウェアを前提とした仕様テンプレートや開発フレームワークの整備など）やドキュメント整備を実施する。

(7) 研修の設計と実施

さらに、手法・ツールと周辺ツール（仕様テンプレートや開発フレームワーク等）の使い方に関する研修を設計し、実施する。研修の設計にあたっては、手法を理解するために必要な基礎知識（特に論理、集合、写像などプログラミング以外の知識）についても整理し、研修内容に組み込む。

(8) 実践適用

実際の開発プロジェクトに適用する。適用の際には、手法およびツールに関する質問や適用に際しての問題点を開発チーム内で常に共有し、対応できる体制を整えておくことが必要である。

(9) 有効性評価と適用方法の改良

開発工程の各フェーズでかかった工数や不具合検出数などの定量データに基づき、コストおよび品質の両面から適用の有効性を評価する。また、開発チームのメンバーから、手法・ツールの利用に関する質問（良く出た質問）や手法・ツールの良い点・課題などの声を集める。これらの結果に基づき、2 回目以降の開発に向けて、ツールやドキュメント、開発プロセスの改善を行う。チームメンバーの習熟により、2回目以降の開発では初回の開発より工数の削減が期待できる。

- 参考事例

栗田：「仕様書の記述力を鍛える －モバイル FeliCa 開発における形式仕様記述手法の導入事例」、日経エレクトロニクス, pp133-152, 2007

高橋他：「鉄道信号システムへのフォーマルメソッドの適用」、鉄道と電気技術、Vol.20、No.2、2009

幡山他：「フォーマルメソッドによる仕様品質向上への取り組み～運賃計算仕様書の記述の改善～」、鉄道サイバネ・シンポジウム、2010

4.1.2. 検証導入パターン（開発）

- 導入組織

組み込みシステム・制御システム等の製造部門におけるソフトウェア開発チーム。

- 適用対象

開発中あるいは開発済みのシステムの設計書（UML 等で記述した設計モデル）やプログラムコードに対する検証を行う。

- 導入によって解決したい課題

設計フェーズや製造フェーズで作りこんでしまった不具合がテストフェーズでも検出できない場合がある。複数プロセスが並行動作する非同期制御システムで再現性の低い不具合

では不具合除去が難しい。こうした不具合を可能なかぎり検出・除去したい。

- 利用する手法・ツール

  モデル検査 SPIN、SMV、UPPAAL 等

- 導入手順

  (1) 適用チームの編成

  モデル検査の概要を理解できる技術者をメンバーとした適用チームを構成する。適用にかかる負担を減らすため、チームでの実施が望ましい。また、モデル検査手法・ツールのより深い知見の習得のため、手法・ツールを熟知している外部有識者の協力が望ましい。適用チームは以下の活動を行う。

  (2)適用対象範囲の特定

  適用対象となる設計モデルやプログラムコードを特定する。また、デッドロックなど検証したい内容を明らかにする。適用対象がプログラムコードで不具合が明確には、その不具合の現象に基づいて検証内容を明確化する。

  (3)手法・ツールの選定

  適用対象となるシステムの特性(並行性やリアルタイム性など)と検証項目の内容にもとづき、モデル検査手法の特徴、ドキュメント・書籍やツールのサポート状況等から利用する手法・ツールを選定する。ドキュメント・書籍等で得られる情報には限界があるため、手法・ツールを熟知している有識者から技術指導を受けることが効果的である。《手法・ツールの選定にあたっては、本ガイドの「7. 手法の選択方法」も参照のこと》

  (4)適用の試行・評価

  適用対象となるシステムの設計モデルあるいはプログラムコードから、検証対象となる部分をモデル検査の記述言語で記述し、検証を試行評価し、有効性を検証する。適切な記述や検証の方法、検証の限界、検証結果の分析方法を理解して、評価を行う必要があるため、手法・ツールを熟知している有識者と共同で試行評価を行うことが望ましい。また、選択した形式手法によっては検証には高い技術レベルが要求されるものがあるため、検証部分は外部にアウトソーシングすることが効果的な場合もある[23]。また、実際の記述では、対象システムの設計および実装に係る詳細情報とドメイン知識が不可欠となるため、開発当事者等の協力が必要となる。

  (5)適用可否の判断

  上記の試行評価の結果から、他のシステム・モジュールの検証にも導入するかどうかの判断を行う。導入する場合は、他のシステム・モジュールにも展開するためのツール整備を行う。たとえば、設計モデル(xUML や状態遷移表等で記載されたもの)やプログラムコードからモデル検査の記述言語(SPIN の場合は Promela)への変換ツール、検証結果(不具合に関する情報)の分析ツール等を整備する。《導入可否の判断に関しては、

[23] 検証サービスを提供する企業は、フランス ClearSy などある。国内では、形式手法を専門とするベンチャー企業が設立される例も見られるが、企業数はまだ少ない。

費用対効果の面での検討も必要である。本ガイドの「5.フォーマルメソッド導入に関するコストと効果の考え方」も参照のこと》

(6) 有効性の評価と適用法の改良

他のシステムやモジュールにも適用し、適用可能なシステムの規模や検出できる不具合の条件（検証可能な項目）等について評価を行う。また、適用チーム外のメンバーが利用できるようにするためのドキュメント整備や評価結果に基づくツールの改良整備を行う。

・ 参考事例

村石他：「Model Checking を適用した実践的非同期制御検証」、ソフトウェアテストシンポジウム JaSST'07、2007

篠崎他：「モデル検査のデバックへの適用」 ソフトウェアテストシンポジウム JaSST'06、2006

篠崎他：「支援ソフトウェアを活用した実践的モデル検査」 ソフトウェアテストシンポジウム JaSST'08、2008

只野他：「モバイル FeliCa IC チップ開発における SPIN を用いたモデル検査による品質確保」、信学技法 SS2010-21、2010

4.1.3. 検証導入パターン（開発支援）

・ 導入組織

開発現場に対する支援部門・品質保証部門（開発現場へのツール展開や成果物に対するレビューやテスト支援などを担当するチーム）

・ 適用対象

開発中あるいは開発済みのシステムの設計書（UML 等で記述した設計モデル）やプログラムコードに対する検証を行う。

・ 導入によって解決したい課題

開発部門が抱える以下の不具合を検出・除去する支援をしたい。または開発部門に以下の不具合を検出・除去する手法やツールを展開したい。

設計フェーズや製造フェーズで作りこんでしまった不具合がテストフェーズでも検出できない場合がある。複数プロセスが並行動作する非同期制御システムで再現性の低い不具合では不具合除去が難しい。

・ 利用する手法・ツール

モデル検査 SPIN、SMV、UPPAAL 等

・ 導入手順

(1) 適用チーム編成

モデル検査の概要を理解できる技術者をメンバーとした適用チームを構成する。適用

にかかる負担を減らすため、チームでの実施が望ましい。また、モデル検査手法・ツールのより深い知見の習得のため、手法・ツールを熟知している外部有識者の協力が望ましい。適用チームは以下の活動を行う。《手法・ツールの選定にあたっては、本ガイドの「7. 手法の選択方法」も参照のこと》

(2) 適用対象範囲の特定

適用対象となる設計モデルやプログラムコードを特定する。また、デッドロックなど検証したい内容を明らかにする。適用対象がプログラムコードで不具合の存在が分かっている場合には、その不具合の現象に基づいて検証範囲を絞り込む。

(3) 手法・ツールの選定

適用対象となるシステムの特性（並行性やリアルタイム性など）と検証項目の内容にもとづき、モデル検査手法の特徴、ドキュメント・書籍やツールのサポート状況等から利用する手法・ツールを選定する。ドキュメント・書籍等で得られる情報には限界があるため、手法・ツールを熟知している有識者から技術指導を受けることが効果的である。

(4) 適用の試行・評価

適用対象となるシステムの設計モデルあるいはプログラムコードから、検証対象となる部分をモデル検査の記述言語で記述し、検証を試行評価し、有効性を検証する。適切な記述や検証の方法、検証の限界、検証結果の分析方法を理解して、評価を行う必要があるため、手法・ツールを熟知している有識者と共同で試行評価を行うことが望ましい。また、実際の記述では、対象システムの設計および実装に係る詳細情報とドメイン知識が不可欠となるため、開発当事者等の協力が必要となる。

(5) 適用可否の判断

上記の試行評価の結果から、他のシステム・モジュールの検証にも導入するかどうかの判断を行う。導入には、当該部門が、フォーマルメソッドを活用し、開発部門を支援する形態と、開発部門に対し、フォーマルメソッドの導入を支援・促進する形態がある。前者の場合、フォーマルメソッドの想定ユーザは開発支援部門であり、後者の場合は、開発部門の現場の技術者である。導入する際はどちらの導入形態とするかを定めた上で、導入計画を策定する。いずれの場合も、導入準備、プロジェクトへの適用および評価等で以降に記すような活動を計画し、そのための体制を確保する。《導入可否の判断に関しては、費用対効果の面での検討も必要である。本ガイドの「5.フォーマルメソッド導入に関するコストと効果の考え方」も参照のこと》

(6) 周辺環境の整備

導入準備として、他のシステム・モジュールに展開するためのツール整備を行う。たとえば、設計モデル（xUML や状態遷移表等で記載されたもの）やプログラムコードからモデル検査の記述言語（SPIN の場合は Promela）への変換ツール、検証結果（不具合に関する情報）の分析ツール等を整備する。

(7) 実践適用

実際に他のシステムやモジュールにも適用し、適用可能なシステムの規模や検出できる不具合の条件（検証可能な項目）等について評価を行う。また、今後の利用に必要なドキュメント整備や評価結果に基づくツールの改良整備を行う。

(8) 適用方法の改良

開発部門に導入を支援する場合は、そのためのツールの改良整備、ドキュメント整備を行う。たとえば、ツールの使い方に関する研修を設計し、実施する。研修の設計にあたっては、手法を理解するために必要な基礎知識（特に時相論理などプログラミング以外の知識）についても整理し、研修内容に組み込む。開発現場から、ツールの利用に関する質問を受け付ける体制を作る。また、手法・ツールの良い点・課題などの声を集め、さらなる整備・改善につなげる。

- 参考事例

  篠崎、早水：「企業におけるフォーマルメソッドの実践」、組込みシステム技術に関するサマーワークショップ　SWEST10　2008

  篠崎他：「支援ソフトウェアを活用した実践的モデル検査」 ソフトウェアテストシンポジウム JaSST'08、2008

  氏原：「JAXA における高信頼性ソフトウェア開発のためのモデル検査の実用化」、システム設計検証技術研究会、2010

  氏原他：「宇宙機搭載ソフトウェアの高信頼化を目的とした第三者評価活動(Independent Verification and Validation: IV&V）の成果と今後の課題」、第5回システム検証の科学技術シンポジウム、2008

4.2. フォーマルメソッド導入のポイント

前節で触れた導入事例の多くに共通する成功要因や導入を検討・試行したものの本格導入に至らなかったケースの障害要因からフォーマルメソッド導入のポイントを以下にまとめる。

4.2.1. 適用チームの編成

前節であげた事例のいずれの組織においても導入推進役の存在が重要である。導入推進は単独の担当者によるものではなく、複数人で構成されるチームによって実施されている。導入プロセスパターンにあるように、導入の検討から本格導入まで多くの作業が考えられる。さらに技術的な検討においては単独の担当者では負担が大きく、組織で理解を得る途中で挫折するリスクも大きい。フォーマルメソッド導入の必要性に関して同じ問題意識を持つメンバーを集め、適用チームを編成することが重要である。社内コミュニティや勉強会等のテーマとしてフォーマルメソッドを提案することや、社内研究制度などを活用し、組織的に認められたチームを編成することも１つの方策である。適用チームに組織管理者を巻き込めれば、より効果的である。また、試行評価において、対象システムの設計および実装に係る詳細情報やドメイン知識が不可欠となるため、開発当

事者や当該ドメインに精通した者の協力が必要となる。

4.2.2. 適用対象・課題の明確化

フォーマルメソッドの導入目的として、仕様書の品質向上、設計段階での検証、既存システムの不具合除去等があげられている。フォーマルメソッドの有効性を検証するためには、実際のシステム開発案件において、こうした観点で現場が直面している具体的な課題を切り出し、適用を試みることが重要である。適用システムや課題が架空のものでは、その効果に関する訴求力は限定的である。しかしながら、現在進行中のプロジェクトに適用することはリスクが高い。開発済みのシステム案件で、今後、類似の開発プロジェクトが見込める案件の成果物への適用や、従来のテストとは異なるアプローチからの再検査が望ましいシステム(一部モジュール)への適用など、現開発プロジェクトに対する影響が少なく、フォーマルメソッド導入が今後の品質向上に寄与することがイメージしやすい案件を対象にすることが現実的である。

4.2.3. 外部有識者との連携

フォーマルメソッドに関する書籍やドキュメントも徐々に増えており、その概要を理解することは容易になりつつある。一方、実際の導入にあたっては、各手法・ツールの特性と限界を正確に理解し、正しい使い方による試行と評価を行う必要がある。しかしながら、このような実際の適用に必要な情報が充分に開示されているとはいえないのが現状である。外部有識者の支援なしに導入を進めることは、困難な問題に直面した際に適切な評価なしに導入を断念するケースに陥るリスクもある。フォーマルメソッドの導入に成功している多くの企業では外部有識者の支援が重要な役割を果たしている。

4.2.4. 試行評価を通じた成功体験

フォーマルメソッドは数学的知識を必要とし、一般のソフトウェア開発者・技術者にとって理解が難しいとの指摘がある。また、フォーマルメソッドに限らず、新規の開発手法の導入は手法の理解や習得などのために現場に追加の負担を強いることとなる。したがって、フォーマルメソッドの導入・展開にあたっては、導入現場のメンバーから導入の意義や有用性の理解を得ることが非常に重要である。こうした理解を得るために成功事例(公開情報)は必要であるがそれだけでは十分ではない。公表される成功事例はあくまでも他組織の事例であり、当事者の環境や開発自体は多様であり、自らの課題に適用できるかどうかが不明確であること、目に見えない技術的課題やデメリットが存在する可能性がその理由である。有用性の理解には、その有用性を自らが体験すること、すなわち成功体験が重要である。たとえば、「適用対象・課題の明確化」でも述べたように、現場が抱えている課題に対して適用を試み、従来のレビューやテストで検出できなかった仕様書のミスやシステム不具合が検出できたなど、分かりやすい形で成果を得られることが重要である。また、同時にフォーマルメソッド適用の限界や他のアプローチ併用の必要性を、体験を通じて理解することも必要である。

4.2.5. 管理者・導入現場の理解

フォーマルメソッドを組織的に導入するには、導入現場の理解以前に組織管理者あるいはプロジェクト管理者の理解が必要であることはいうまでもない。組織管理者あるいはプロジェクト管理者に対しては、「5. フォーマルメソッド導入に関するコストと効果の考え方」にあるようなフォーマルメソッドの意義とコストに関する理解を得ることが必要である。さらに、「適用対象・課題の明確化」、「評価試行を通じた成功体験」で指摘したように、従来のレビューやテストで検出できなかった仕様書のミスやシステム不具合が検出できたなど分かりやすい形で具体的な効果が得られ、品質、コスト、リスクの観点で見える化できれば、理解の促進が期待できる。