

実務家のための形式手法

厳密な仕様記述を志すための形式手法入門 第二版

事例:種々の事例

事例:種々の事例(このモジュールについて)



形式手法導入に**様々な取り組み**があることを知り、形式手法導入の**検討や計画立案**の際に参考となる手がかりを得るためのモジュール

■ 事前知識・経験

- 形式手法の導入を検討、計画している
- 形式手法の有用性についての基礎知識
- 形式手法導入のガイダンス

■ 学習目標

- 様々な取り組みがあることを知り、自らの導入に際して有用な知見の手がかりを得る

■ 主な学習項目

- 形式手法導入に関する活動例
- 種々の適用ドメイン例
- 複数のアプローチ例(段階的詳細化、モデル検査、…)

SEC-FM1-04-2

Copyright © 2012,2013 IPA

IPA Software Engineering Center

2

講師の方へ:

このモジュールでは、種々の事例を取り上げている。

1. 類似した事例を探し、より詳しい調査の糸口とする
2. それぞれの目的と効果を見極め、自分たちのプロジェクトへどのように応用するかといった点を意識するようにお話しください。

事例 1: 人材育成



- 教材
 - Web: いくらでも存在
 - 日本語の教科書/資料: いろいろある
- コース
- 活動
 - 情報処理推進機構 (IPA/SEC)
 - 人材育成WG、厳密な仕様記述WG
 - 調査報告書(「情報系の実稼働システムを対象とした形式手法適用実験報告書」など)
 - 経済産業省「新世代情報セキュリティ研究開発事業」
 - 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
 - 国立情報学研究所 (NII)、産業技術総合研究所 (AIST)
 - 宇宙航空研究開発機構 (JAXA)
 - 大学
 - その他いろいろ

SEC-FM1-04-2

Copyright © 2012,2013 IPA

IPA Software Engineering Center

3

形式手法を導入する目的をはっきりさせる。

現状の問題点がなににであるか、形式手法でなにをどの程度改善したいのかを自分たちで見極めないと、情報の海に溺れてしまう。

事例 2: 初期の適用事例



- CICS: IBM Hursley Lab. & Oxford Univ. (Z)
- 原子力発電: Rolls-Royce (VDM)、
カナダダーリントン(SCR/Darlington Method)
- 鉄道: パリ地下鉄信号システム (B method)、中国鉄道局 &
UNU/IIST (RAISE)
- 航空管制: NASA (theorem provers)
- 航空機: A330/340 (Z)
- 医療: 放射線システム (Z)、サイクロトロン、HP
- ハードウェア設計: Tektronix (Z)
- マイクロプロセッサ開発: Inmos (Z,CSP,ML)、FM8501、
FM9001 (Boyer-Moore)

形式手法は、ソフトウェアシステムだけではなく、マイクロプロセッサなどハードウェアの開発にも使われている。

Tektronixがオシロスコープの開発に仕様記述言語 Z を使った事例もある。

抽象度、記述の対象はどこにでも設定できる。

CICS: Customer Information Control System



- IBM Hursley Lab. & Oxford Univ.
- 800,000行の中の300,000行を改訂
 - 37000行 : Z仕様記述、設計
 - 11000行 : Z(部分的)
- 2000頁の形式的に記述された文書
- 開発コスト : 9%削減

■ 参考文献

I. Houston and S. King: CICS Project Report Experiences and Results from the Use of Z in IBM, Proc. VDM'91, Lecture Notes in Computer Science, Vol. 551, Springer-Verlag, 1991.

この事例は Z という形式仕様記述言語を使って、IBMのHursleyにある研究所とオックスフォード大学の研究所が協力して当時としても大きなシステムである、Customer Information Control System (顧客情報管理システム)の一部を作り直した。

2000ページのフォーマルなドキュメントが最終的な直接的な成果物で、開発コストが9%削減されたという論文もある。

事例 3: 産業界における形式手法[J.-R.Abrial]



■ Correct by Construction

- 抽象モデル
- 具象モデル
- 実行可能コード

■ 証明

- 不変条件の保存
- 正しい詳細化

■ 事例

- $B \Rightarrow Ada$
- パリ地下鉄14号線(1998年)
- ロワシー空港シャトル(2006年)

■ 参考文献

J. R. Abrial: Formal Methods in Industry: Achievements, Problems, Future,
Proc. 28th International Conference on Software Engineering, pp. 761–768,
2006.

SEC-FM1-04-2

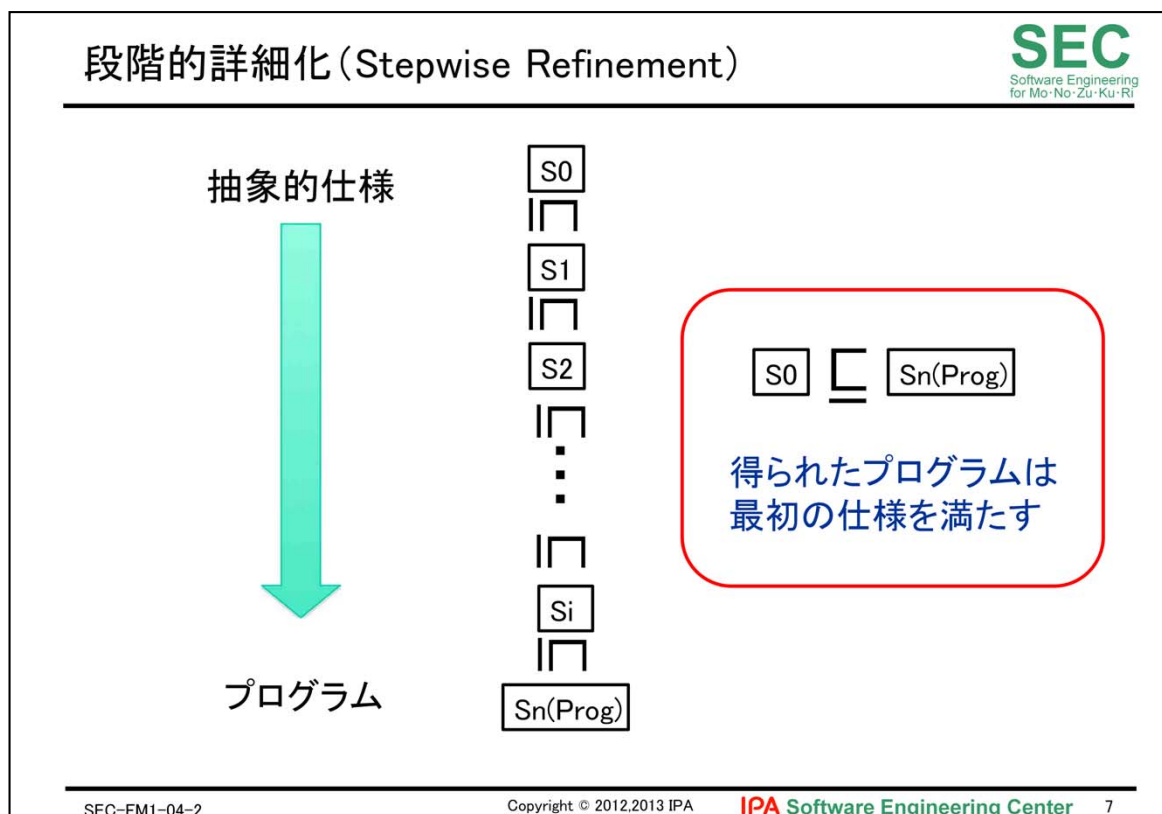
Copyright © 2012,2013 IPA

IPA Software Engineering Center

6

事例 3 は、B Method の提唱者である Raymond Abrial による。

Ada は、高水準手続き型プログラミング言語である。



この事例で用いられた段階的詳細化手法では、抽象的な仕様から少しずつ証明しながら具体化し、最後はAdaという高水準手続き型言語に落としこんだ。

図は、一段階具体化されたものは、その直前の仕様をきちんと満足するという関係を表す。

この詳細化の関係が成り立つことを証明しながら、少しずつ少しずつ具体化していくのが、理想的な形式手法適用である。

2つの適用事例



■ 対象システムの要素変数

路線長	8.5km	路線長	3.3km
駅数	8	駅数	5
最小列車間隔	115s	最小列車間隔	105s
最高速度	40km/h	最高速度	26km/h
列車編成数	17	列車編成数	14
一日あたり利用者数	350,000	一時間あたり利用者数	2,000

表 1: パリ地下鉄 14 号線の
要素変数

表 2: ロワシー空港シャトルの
要素変数

表 1 の事例は、パリ地下鉄14号線、表 2 の事例は、ロワシー空港シャトルであり、類似した事例だが、適用した年代や環境が異なる。

2つの適用事例



■ 対象システムの成果

成果項目	パリ地下鉄	空港シャトル
ADA によるプログラム行数	86,000	158,000
証明数	27,800	43,610
対話的証明の割合	8.1%	3.3%
対話的証明にかかった人月	7.1	4.6

事例の比較

SEC-FM1-04-2

Copyright © 2012,2013 IPA

IPA Software Engineering Center

9

少しずつ具体化するので、証明の数が 27,800 や 43,610 と多い。

しかし、ほとんどは小さな証明である。

パリ地下鉄の事例では、91.9% が自動で証明ができ、残りの 8.1% を人間が証明した。

空港シャトルの事例は、96.7% もツールにより自動的に証明され、残りの 3.3% のみを人間が証明した。

出来上がったソースコードは、パリ地下鉄の事例で 86,000 行、空港シャトルの事例は 158,000 行の記述量である。

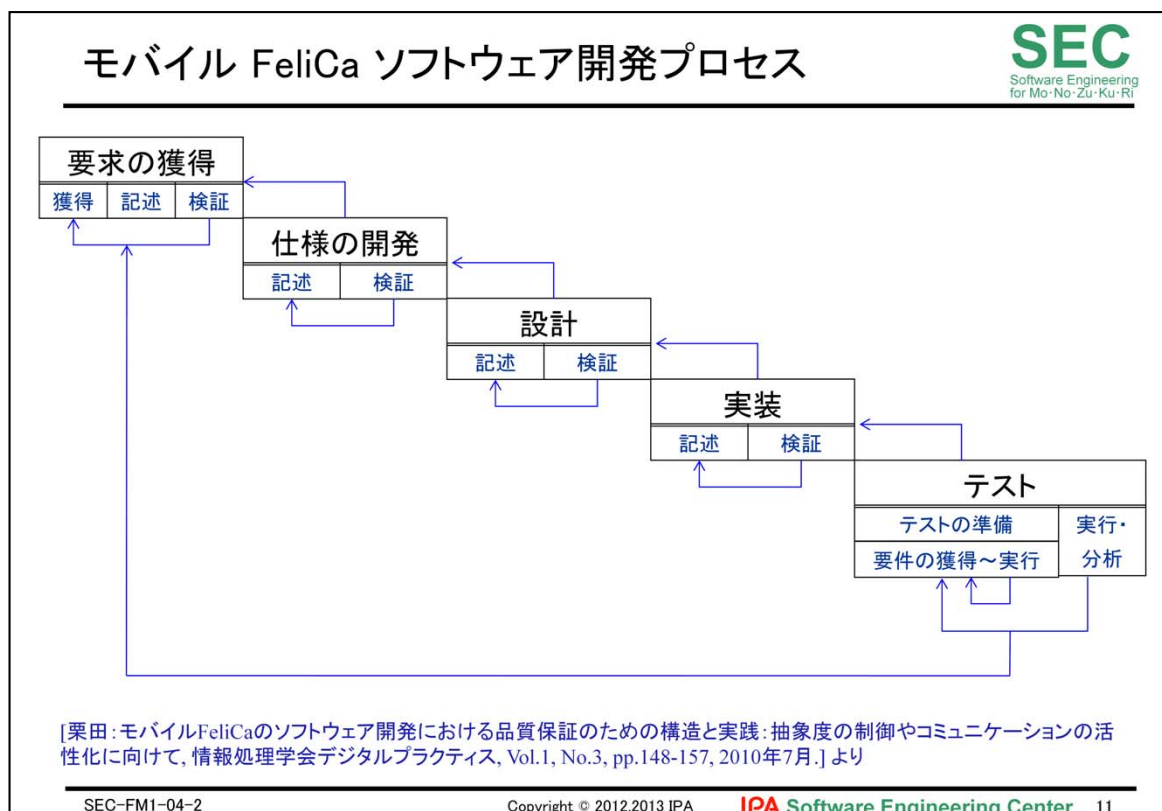
これだけの量に抑えられているのは、絶対に間違いが起きてはいけないところに限定して、狭く深くフォーマルメソッドを適用しているからである。

事例 4: モバイル FeliCa 開発への適用



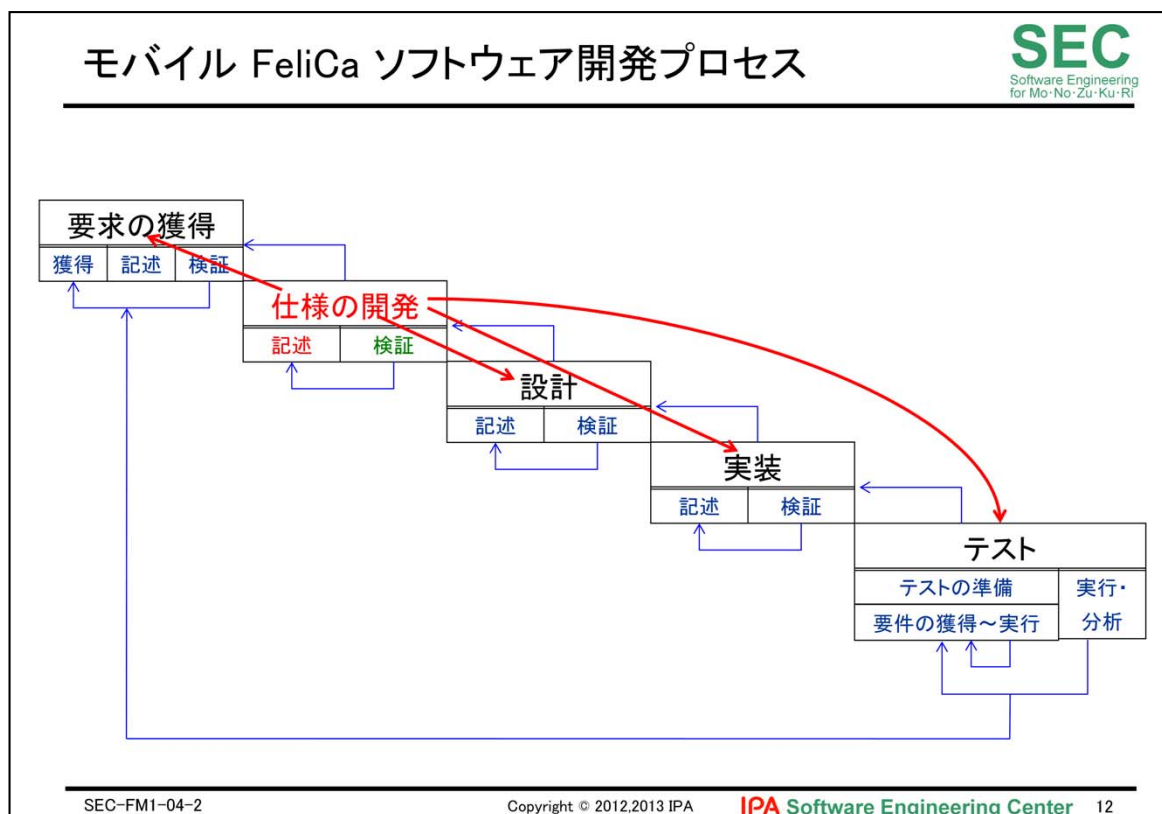
- 仕様記述言語 VDM++ と仕様開発環境 VDMTools を用いて、外部機能仕様を動作する形式仕様として表した
- 作成した仕様書は以下の通り:
 - 自然言語による 383 ページのプロトコル仕様書
 - 形式仕様記述言語 VDM++ による 677 ページの外部仕様書
- 仕様書のコード量はテストコードを含め、約 10 万行
- C++ 言語によるファームウェアのソースコードは一種類のチップにつき約 11 万行
- 開発時における仕様関連のトラブルは少なかった
- IC チップの出荷後、ファームウェアの品質に関連するトラブルはない

詳しくは、「事例:成功事例」を参照すること。



これは、フェリカネットワークスで実施しているソフトウェア開発プロセスである。

典型的なウォーターフォールモデルに準拠している。



この開発プロセスの中で、仕様の開発の、仕様記述の部分のみ、VDM++を使って厳密に仕様を記述した。

しかし、上流の要求にも影響がおよび、日本語で記述されているドキュメントも改善した。

つまり、仕様記述のみフォーマルな記述をしたことが、開発プロセス全体に効果を及ぼしている。

これは、浅く広くフォーマルメソッドを適用した事例です。

事例 5: ソフトウェアモデル検査



[Miller, et al., Communications of ACM, Vol.53, No.2, Feb. 2010]

■ Rockwell Collins & Univ. Minnesota

■ 航空システム

■ 変換フレームワーク:既存ツールの連携

- MATLAB、Simulink、SCADE、...
- NuSMV、SAL、PVS、...
- C, Ada

■ 適用事例

- 状態数 = 10^{120}
- 状態数 = 10^{37} 563 性質確認、98エラー検出
- 状態数 = 10^{13} 62 性質確認、12エラー検出

SEC-FM1-04-2

Copyright © 2012,2013 IPA

IPA Software Engineering Center 13

どのようなところを狙うかで、使い方も使う道具立ても変わってくる。

モデル検査の事例として、Rockwell CollinsとMinnesota大学の共同研究で、航空システムに対し、様々なツールを連携させて、モデル検査の有限状態遷移図でシステムを記述し、システムを網羅的に確認した。

一番大きな状態数は、10の120乗であったが、どのような成果が得られたかは不明。

別の例では、10の37乗の状態を網羅的に検査した結果、563個の性質を確認し、98個の不具合を見つけた。

また、10の13乗の状態を網羅的に検査し、62個の性質を確認し、12のエラーを検出した例もある。

事例 6: 福岡の地場企業との共同研究



- 福岡の中堅企業
- 品質第一
- 最初は、すべて自社開発
- 今は、設計までで実現は外部に発注

問題点

技術移転/新人育成
システムの全容が理解できていない
発注する際の仕様と検収
再利用による開発効率の向上

自分たちの問題に合った手法を、合ったように使うということがポイントになる。

福岡の中堅企業との共同研究の初期の頃に、その企業が持っている具体的なシステムに対して形式手法を適用した時は、技術移転や新人教育の話があった。

また、システムが複雑になり、全容を理解できる人がいなくなると、発注する際、仕様に何をどの様に記述すればよいかわからず、でき上がったものを検収するときに、何をどの様に確認すればよいかわからない といった問題を抱えていた。

さらに、色々な類似するシステムがあり、再利用性を高めて開発効率を高めたいという要求もあった。

形式手法適用の経緯



- 大学側からの売込みと対象の選定
- Zのチュートリアル
- ドメインエキスパートから聞き取り
- 仕様記述の種々の版の作成と検討
 - 機能
 - モデル化
- 共通語としてのZ
 - コミュニケーションの道具
- アニメーション、プロトタイピング
- 文書の体系化
 - 用語集+形式的定義へのリンク

SEC-FM1-04-2

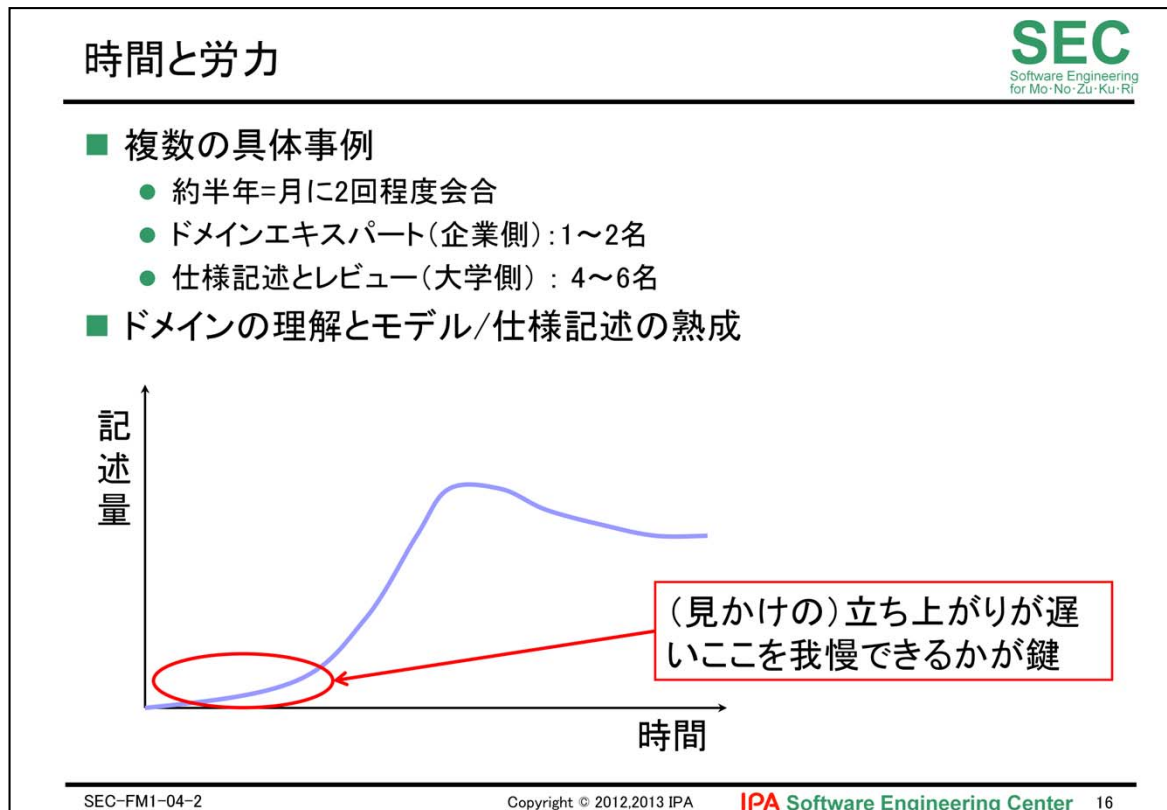
Copyright © 2012,2013 IPA

IPA Software Engineering Center 15

それなりの成果は出せたが、最大の反省すべきところは、企業側と大学側で完全に別々になっていたことである。

ドメインの知識を伺いながら形式仕様記述を大学側が行い、その記述を企業側にレビューしてもらっていた結果、形式手法が企業に定着しなかった。

企業が自ら工夫して適用しなければ、フォーマルメソッドは定着しないという教訓を得た。



二つの事例研究を行ったが、どちらも似たような経過をたどった。

モデルの熟成には時間がかかるので、そこを我慢できるかどうかも重要である。

これらは大学側にとっても初期の事例であった。

経験を積みめば、もっと早く対象システムの数理的モデルを構成できるであろう。

サマリー



形式手法導入に様々な取り組みがあることを知り、形式手法導入の検討や計画立案の際に参考となる手がかりを得るために、以下を学習

- 形式手法導入に関する活動例
- 種々の適用ドメイン例
- 複数のアプローチ例(段階的詳細化、モデル検査、…)



実務家のための形式手法

厳密な仕様記述を志すための形式手法入門

事例:種々の事例

独立行政法人情報処理推進機構
技術本部 ソフトウェア・エンジニアリング・センター
統合系システム・ソフトウェア信頼性基盤整備推進委員会
上流品質技術部会 人材育成WG(編)
2013年3月 第二版発行

記載されている個々の情報に関しての著作権及び商標はそれぞれの権利者に帰属するものです
なお、本書の内容は将来予告なしに変更することがあります