

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

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、…）

## ■ 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

## 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)

- 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.

## ■ Correct by Construction

- 抽象モデル
- 具象モデル
- 実行可能コード

## ■ 証明

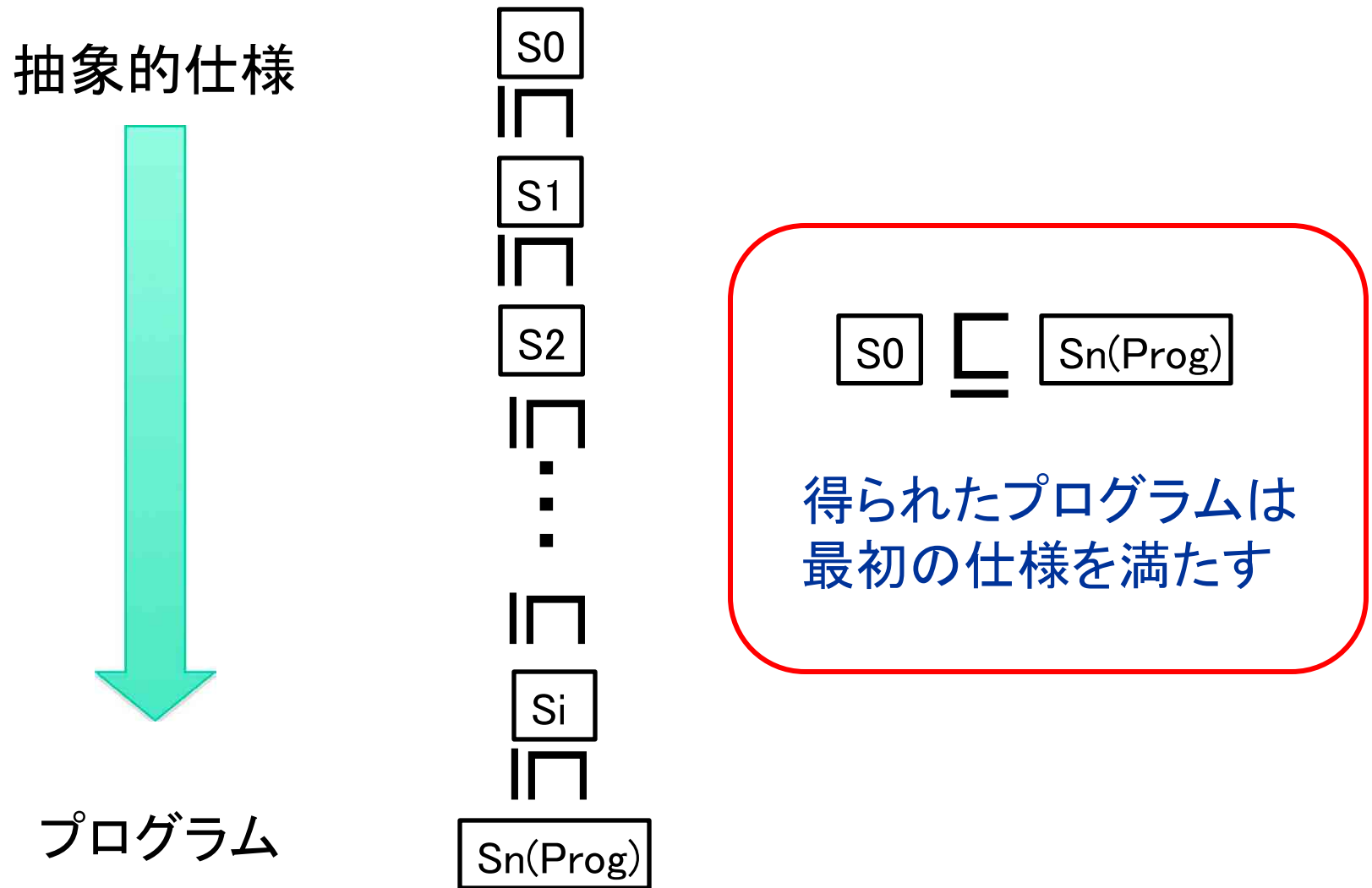
- 不変条件の保存
- 正しい詳細化

## ■ 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.



## ■ 対象システムの要素変数

路線長	8.5km
駅数	8
最小列車間隔	115s
最高速度	40km/h
列車編成数	17
一日あたり利用者数	350,000

表 1: パリ地下鉄 14 号線の  
要素変数

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

表 2: ロワシー空港シャトルの  
要素変数

## ■ 対象システムの成果

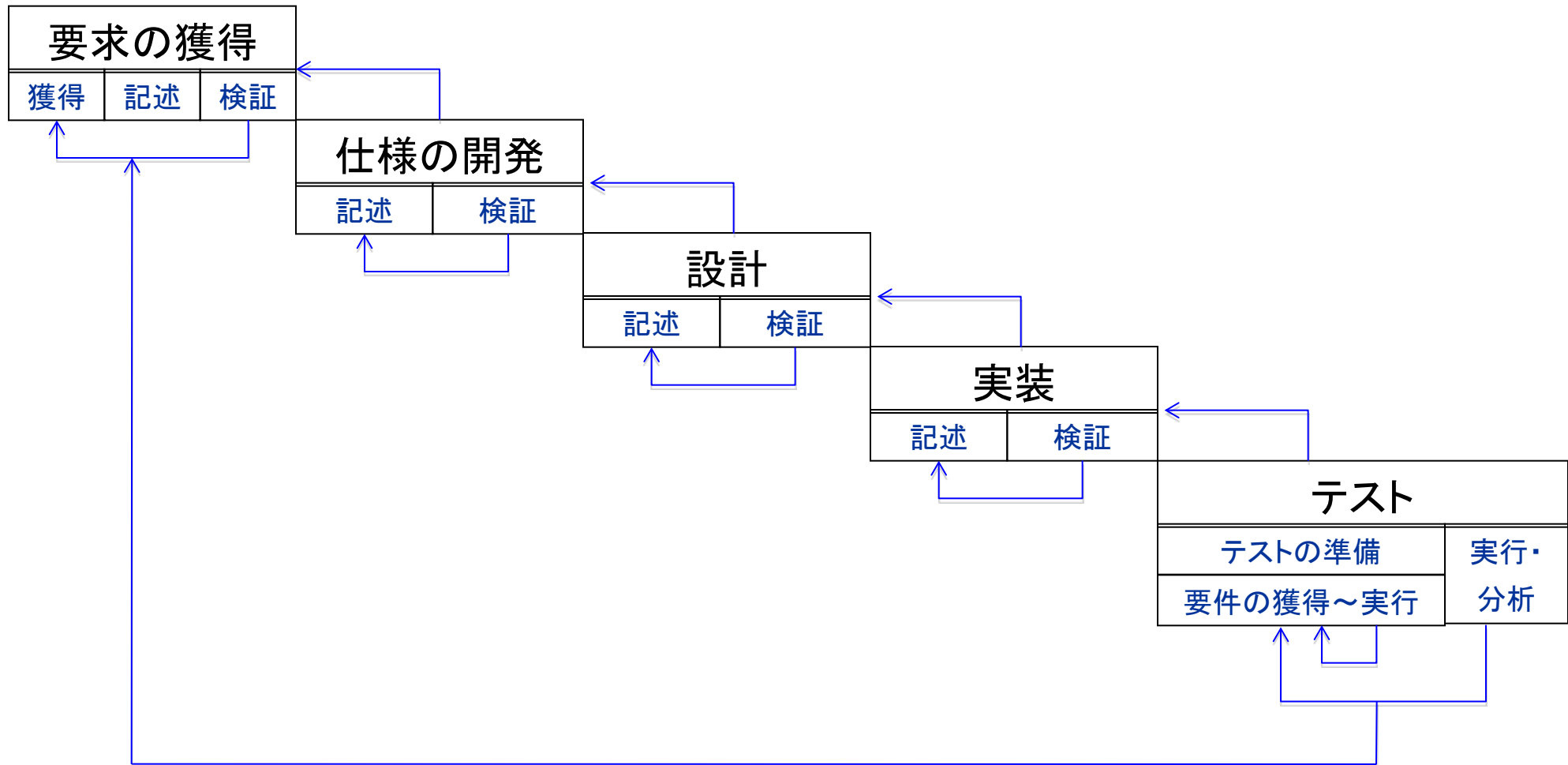
成果項目	パリ地下鉄	空港シャトル
ADA によるプログラム行数	86,000	158,000
証明数	27,800	43,610
対話的証明の割合	8.1%	3.3%
対話的証明にかかった人月	7.1	4.6

事例の比較

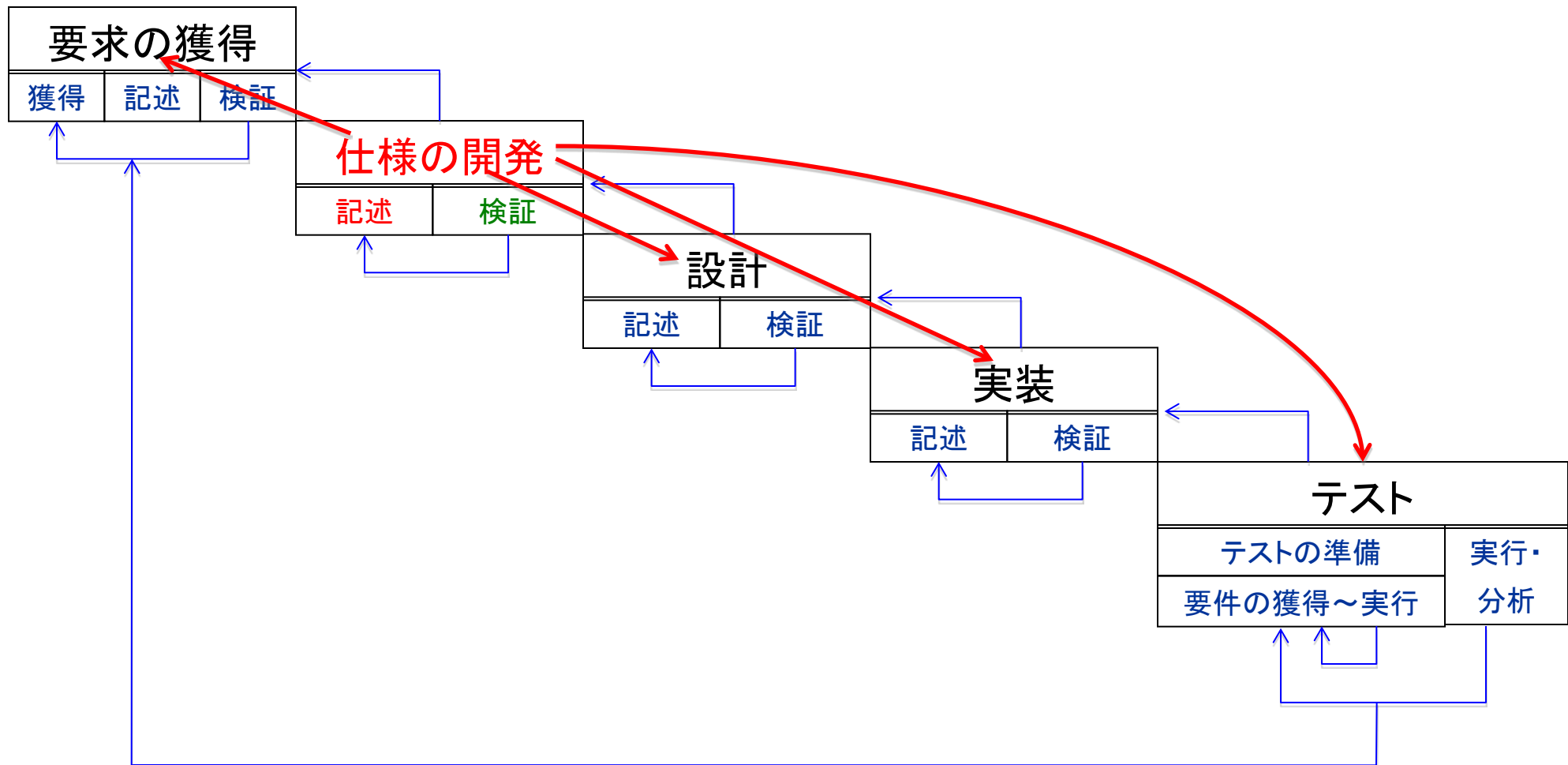
# 事例 4: モバイル FeliCa 開発への適用

- 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

# モバイル FeliCa ソフトウェア開発プロセス



[栗田: モバイルFeliCaのソフトウェア開発における品質保証のための構造と実践: 抽象度の制御やコミュニケーションの活性化に向けて, 情報処理学会デジタルプラクティス, Vol.1, No.3, pp.148-157, 2010年7月.] より



[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

- 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

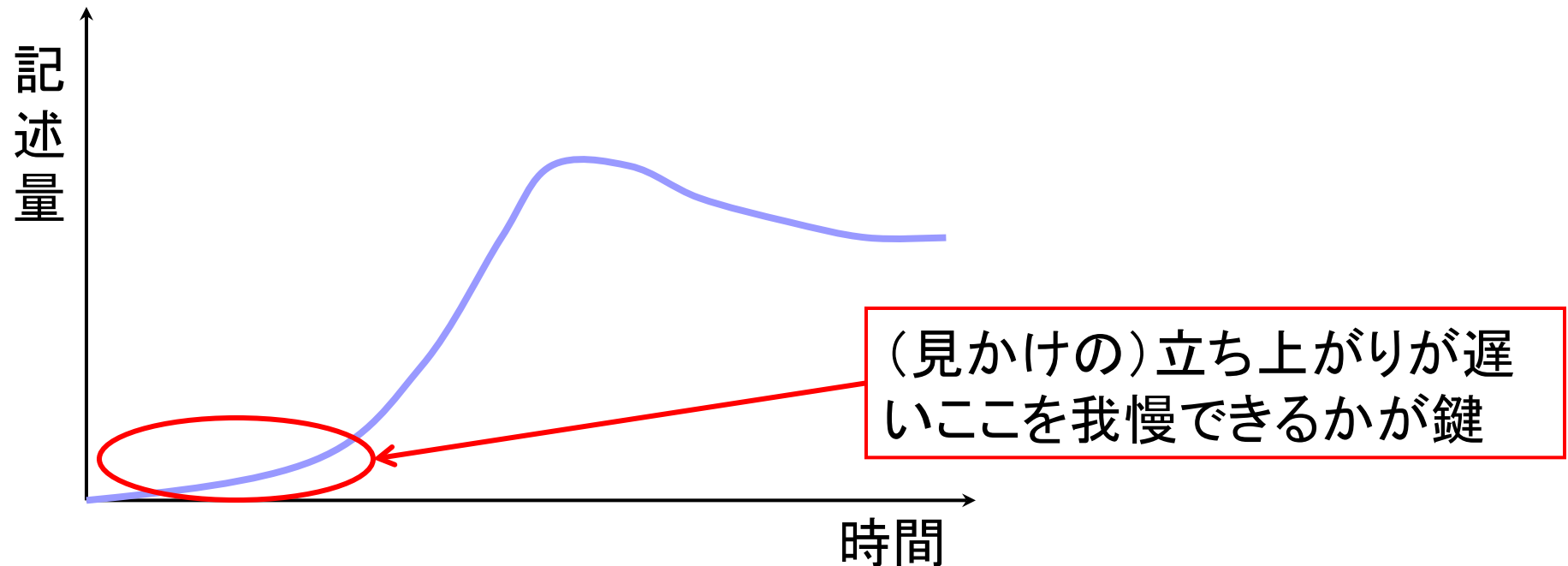
技術移転/新人育成  
システムの全容が理解できていない  
発注する際の仕様と検収  
再利用による開発効率の向上

- 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

## ■ 複数の具体事例

- 約半年=月に2回程度会合
- ドメインエキスパート(企業側): 1~2名
- 仕様記述とレビュー(大学側): 4~6名

## ■ ドメインの理解とモデル/仕様記述の熟成



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つい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