導入へのガイダンス(A)

SEC形式手法人材育成作業部会(編)

このモジュールについて

主に管理者としての立場から、形式手法を円滑に導入するために考慮すべき事項について理解し、形式手法導入の計画立案を開始できるようになるためのモジュール

- 事前知識・経験
  - 形式手法の有用性を理解した上で導入に前向きに検討している
  - 形式手法を具体的に適用する知識・スキルはない
- 学習目標
  - 形式手法の導入に必要な知識とスキル
  - 管理者として円滑な導入を支援するために必要な姿勢
- 主な学習項目
  - 直接的効果に加え間接的効果の重要性
  - 導入実践時のポイントと典型的な誤認識
  - 選び方(分類と代表的な手法)
  - コスト(教育時、形式モデル構築時)

形式手法適用の効果

- 直接的効果
  - 成果物
  - 記述物
  - 分析／証明結果
- 間接的効果
  - 開発対象の理解とその共有
  - 開発プロセス改善
  - コミュニケーション改善
  - 開発者の自信

ありがちな例:-)

- 社内で形式手法担当者を1名決める
- その担当者に丸投げ
  - 調査、勉強
  - 試行
  - 評価
- 問題点=孤立
  - 開発プロセスとの関連なし
  - 開発現場との連携なし
  - 試行対象のドメインに(必ずしも)精通していない
  - 現場への導入の道筋も提示されていない
- ありがちな結論
  - 形式手法は(うちでは、まだ)使えない!

実践のポイント

- 管理職の意識
  - 形式手法への関心、期待、推進力
  - 担当ドメインエキスパートの意欲への影響
- 厳密な記述と議論
  - 最初の戸惑い
  - 新鮮な感動
  - 慣れ
  - 維持継続の努力と支援
- コミュニティ
  - 普段の相談相手
  - 高度なことも相談できる専門家（師匠）

形式手法に関する七つの社会通念 [Hall:90]

- 形式手法はソフトウエアが完全であることを保証できる
- 形式手法とは須らくプログラムの証明である
- 形式手法はセーフティクリティカルシステムにのみ有効である
- 形式手法は高度に訓練された数学者を必要とする
- 形式手法は開発コストを増加させる
- 形式手法はユーザには受け入れられない
- 形式手法は現実の大規模ソフトウェアには使われない

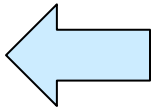
形式手法に関する七つの真実 [Hall,1990]

- 開発の初期の段階での誤りの発見に有効
- 開発対象のシステム自体を深く考えさせることに寄与
- いかなる応用分野にも有効
- 数学を基礎としてはいるものの、プログラムよりは理解し易い
- 開発コストを減少させる
- 顧客が購入しようとしているものの理解を助ける
- 産業界における実用プロジェクトに用いられて成功

日本企業における七つの反応

- 実際の適用事例は興味深く魅力的
  - フエリカネットワークスの K さん=ひっぱりだこ!
- 実世界から孤立した完全な世界
- 高度に数学的
- 実際に自分たちで適用するのは困難
- 自分の問題にぴったり合致する実例が必要
- 経営者を説得するのが難しい
- コストおよび効果が不明

よく訊かれること

どれを選んだら良いのか?　  　形式手法/ツール=100以上

- すぐには回答できかねます
  - 十分な情報提供が必要
    - 開発対象、開発プロセス、目的、要員、期間、予算、etc.
- 自らの決断と責任
- 取り敢えずVDMとSPINを使ってみたら
  - ある程度のことはできます
  - 日本語の書籍もあります
  - 形式手法に対する感触を得られます

形式手法の歴史

- プログラムの正しさ(検証)=1960年代～
- 検証理論に関する研究の発展=1970年代～
- 形式仕様記述言語/方法論/ツールの開発
  - VDL(Vienna Description Language), VDM(Vienna Development Method)
  - Z Notation
  - Bファミリー(B Method, Event- B)
  - Larch
  - OBJ
  - HOL
  - モデル検査

  etc.
- 適用事例蓄積と実用化

マクロな観点とミクロな観点

Formalism-in-the-Large

(cf. Programming-in-the-Large)

- モデル化 (Modeling)
- 抽象化 (Abstraction)
- 機能 (Function)
- 構成 (Construction)
- アーキテクチャ (Architecture)

Formalism-in-the-Details

(cf. Programming-in-the-Small)

- モデル化 (Modeling)
- 分析 (Analysis)
- 性質 (Property)
- 検証 (Verification)
- 検査 (Testing)

基礎理論

多様性と多面性

- Z Notation: 抽象化、表記法、実行不能、ツール群
- VDM-SL :親しみやすい表記法、ツール群、利用者のコミュニティ
- VDM++ : オブジェクト指向、アーキテクチャ/部品
- B Method: 抽象状態機械モデル
- Event-B : B による状態機械をイベント駆動ネットワークにより結合したモデル
- RAISE : EU の ESPRIT プロジェクトとして産業界での形式手法導入を意図して VDM 等の考え方を参考にして開発
- OBJ : 代数的仕様記述
- CSP, CCS : プロセス代数
- モデル検査 : 有限状態機械モデル、振舞い分析/検証

その他いろいろ

形式手法の一部の分類

モデル規範:　　VDM・Z Notation・B Method等と，ツールを利用

- 集合論や命題論理、述語論理が基礎となる
- 不変条件、事前条件、事後条件を記述する
- 情報の構造や、ある状態から他の状態への変化をモデル化する
- 専用言語の利用によるコンパクトな仕様記述，曖昧さの除去，仕様の「実行」、「テスト」、「回帰テスト」、定理証明等の可能性が広がる

モデル検査:　　PROMELA，LTS 等の言語と SPIN (PROMELA)，LTSA (LTS) 等のツールを利用

- 振舞い仕様を，状態遷移モデルと，モデルが満たす条件として記述することで，全状態空間を生成し，自動検査する
- 従来の「テスト」では見つからない潜在的な障害を発見できる

現状、どのような形式手法の適用が多いか？

- 形式手法の種類
  - モデル規範型
    - VDM, RAISE(VDM+OBJ+CSP的仕様), B Method, Z Notation, ...
    - 現場の技術者が理解しやすい
  - 性質規範型
    - CafeOBJ(OBJ3), Maude, ...
    - まだ現場に適用するには時期尚早
  - モデル検査
    - SPIN,SMV, ...
    - 採用する意味はあるが、現場の技術者には難しい

軽量手法としてのVDM

- 形式手法の検証方法とツール
  - 証明
  - 段階的洗練
    - RAISETool, Rodin, Coq, ...
    - 採用する意味はあるが、現場の技術者には難しい
  - モデル検査
    - SPIN, LTSA, NuSMV, ...
  - 仕様実行
    - VDMTools, ...
    - 現場の技術者に理解しやすく、形式検証の第一歩として採用

形式手法とVDMの有用性

- 理論的にも経験的にも形式手法が有効
- VDMToolsで使用するVDMは、現場寄りの形式手法
  - 証明やモデル検査は、長期的にはやるべきだが、すぐにはできない
- VDM導入は、さほど難しくない
  - 3ヶ月程度の教育とコンサルティング
  - 既存の役立つソフトウエアエ学ツールと協調して、より効果が出る
- モデル化は、以下が重要
  - モデル化の範囲を決め、仕様を分割統治
  - 名詞から型、述語から関数または操作
  - 陰仕様を作成してから、静的検証
  - 陽仕様を作成してから、動的検証
- VDMは構造化日本語仕様として使うことができる

形式仕様

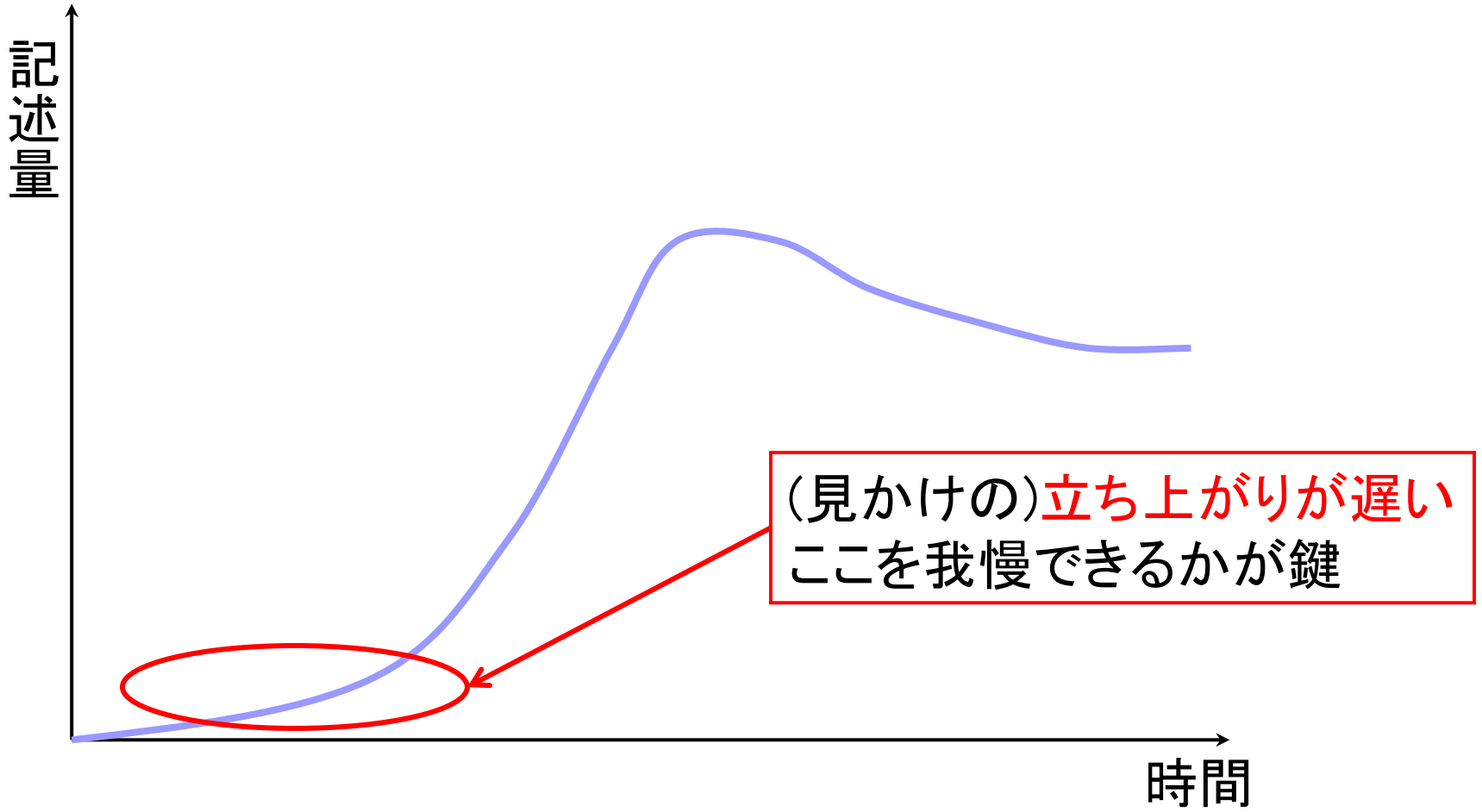
- 読むのは、難しくない
  - 簡単な解説
  - 形式仕様のレビュー(OJT)
- 書くには、経験が必要:
  - ドメイン知識、抽象化能力
  - 言語仕様 (syntax)
  - 対象のモデル化 (semantics)
  - イディオム (pragmatics)
- アニメーション/視覚化
  - 仕様実行のこと
  - multi-lingual
  - multi-aspect

VDMの教育

	セミナー	教材	コンサルティング	受講者	備考
SCSK	4日間	英語	無し	平均年齢50歳弱 形式手法知識 4人有 ソフトエ学知識 有	VDN記述予定者半数(2人)が英語で脱落 c++Java,形式手法について、実践経験無し
フエリカネットワークス	4日間	日本語	3ケ月/週1回	平均年齢20歳代 形式手法知識無 ソフトエ学知識無	
産業技術総合研究所,オムロン	無し 自習	日本語 [Fitzgerald:10] [佐原:08]	無し	平均年齢30歳代 形式手法知識 1人だけ有 ソフトエ学知識無	周囲に形式手法経験者多数

数理モデル作成プロセス

- [Anthony Hall: Seven Myths of Formal Methods, IEEE Software, Vol.7, No.5, 1990]



サマリー

主に管理者としての立場から、形式手法を円滑に導入するために考慮すべき事項について理解し、形式手法導入の計画立案を開始できるようになるために、主に以下を学習

- 直接的効果に加え間接的効果の重要性
- 導入実践時のポイントと典型的な誤認識
- 選び方(分類と代表的な手法)
- コスト(教育時、形式モデル構築時)