

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：成功事例

形式手法導入の成功事例（フェリカネットワークス（株）の事例）から、形式手法導入の検討や計画立案の際に有用な知見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

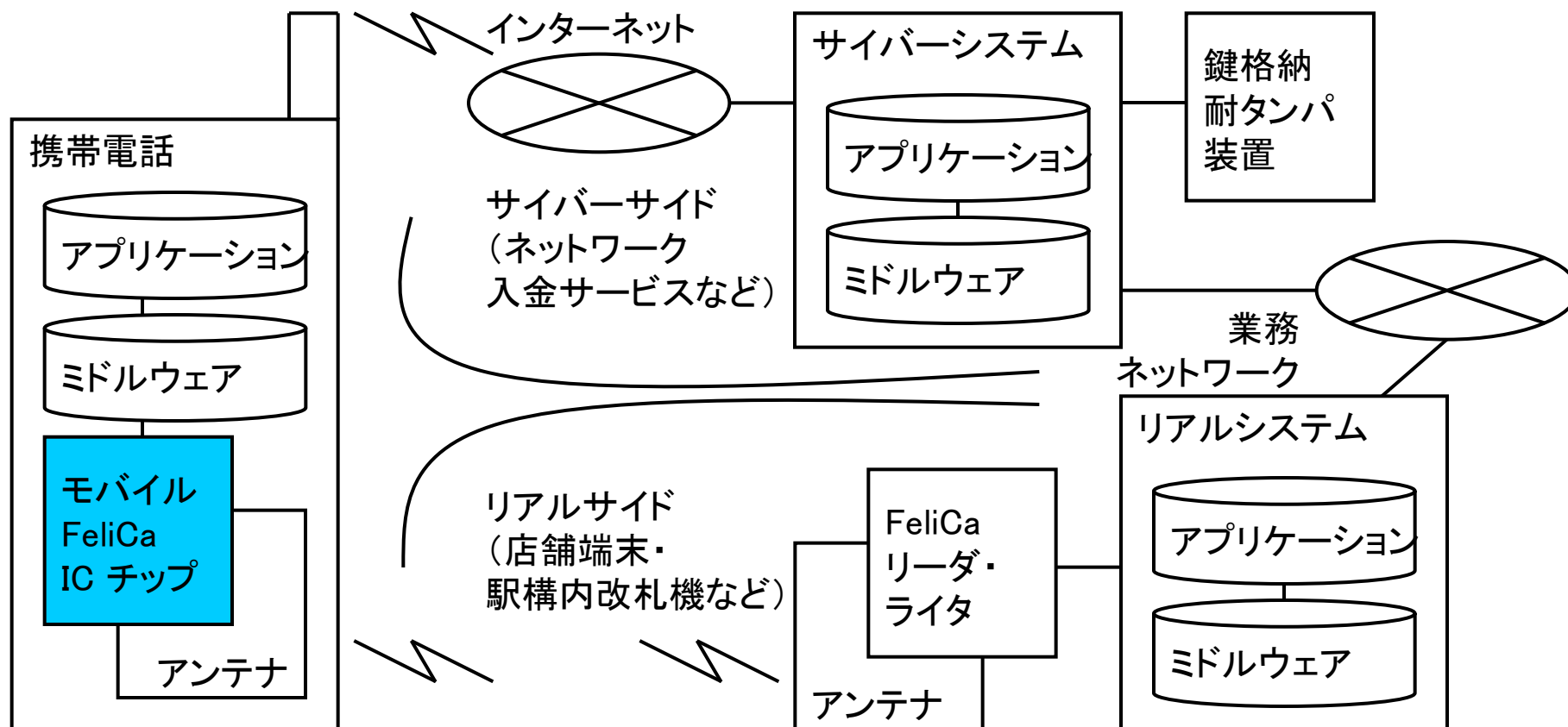
■ 学習目標

- 過去の成功事例から、自らの導入に際して有用な知見を得る

■ 主な学習項目

- 成功と言われている事例では
 - どのようにプロジェクトに形式手法を導入したか
 - どのような成果を得たか

- 電子マネーや公共交通機関の乗車券、定期券などに応用される、社会インフラを構成するセキュリティソフトウェアである
- 日本中の携帯電話に組み込まれる
- 社会的責任が重い
- システムやサービスの根幹に関わる**重大なトラブル**が発生することで、フェリカネットワークス自身のみならず、一般ユーザの生活や、サービス事業者、携帯電話メーカー、移動体通信事業者のビジネスに影響が及ばないよう、品質の確保に当たらなければならない



【ゴール】

フェリカネットワークス発の次世代モバイル FeliCa サービスの実現

【具体的な目標】

モバイル FeliCa IC チップファームウェアおよび周辺ツールの開発

【期間】

約 3 年 3 ヶ月

【メンバー数】

約 55 名

【平均年齢】

約 30 歳

【要件獲得・仕様開発】**曖昧な仕様**に起因するトラブル

上流工程の不具合を下流工程で修正するコスト

→ 仕様記述言語を用いた**厳密な仕様の記述**に挑戦

【設計・実装】**設計が不明確であること**に起因するトラブル

設計不良によるトラブル

→ 状態遷移モデルの**網羅的なモデル検査**に挑戦

【テスト】**テスト項目の増大。項目の抜け漏れ**によるトラブル

人に依存したテスト

→ 効率良く品質を確保するための**組み合わせテスト**技法の活用

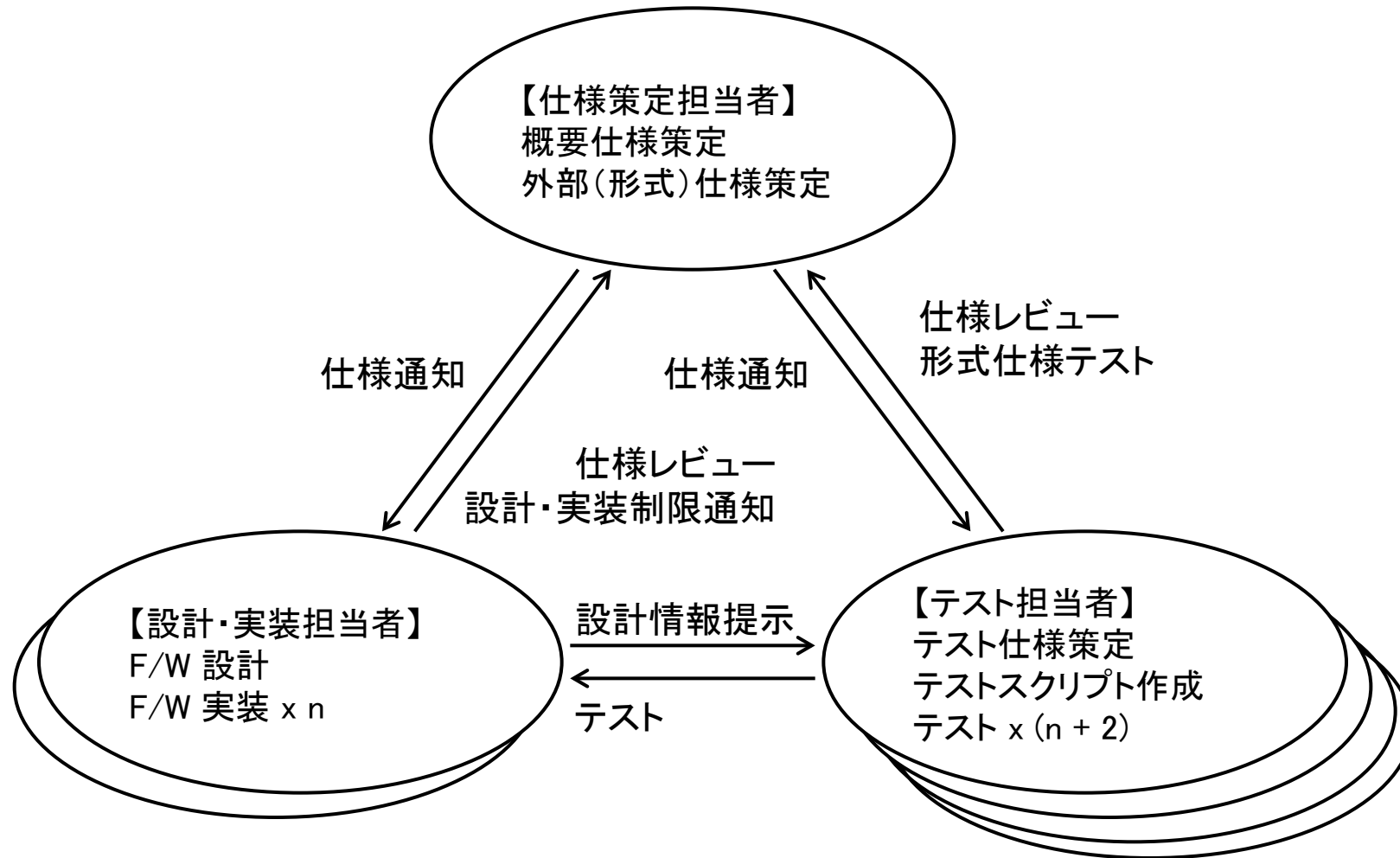
【プロジェクトマネジメント】**ステークホルダとの調整不足**に起因するトラブル

プロジェクトが**コントロール**されていないことによるトラブル

【チーム運営】**コミュニケーション不足、スキル不足**に起因するトラブル

【第三者評価】**客観的な評価の欠如**

セキュリティ実装の妥当性証明の困難性



- 正しい仕様を自然言語で書くのは困難である
 - 曖昧さの排除が困難である
 - ツールによるチェックができない
 - 仕様を書きながら「擬似コード」を考えなければならないことが多くあるが、文法の検討に時間がかかる
- 図表のレイアウト検討や記述にも時間がかかる
 - 変更管理が困難である
 - 仕様っぽいものが誰にでも書けてしまう…
- UML など適用が困難である？
 - 自然言語で詳細を記述するため、結局自然言語仕様と同様の問題が発生する
 - ツールによるチェックがほとんどできない
 - 記法に曖昧さが多いため、形式手法より学習が困難である
 - 再利用のための仕掛けがない

■ VDM の選定理由

- 仕様策定段階から動作可能
- モデル化から動作確認まで広い範囲での適用が可能である

■ VDM の特徴

- VDM++ = VDM-SL (ISO で標準化) + OO
- VDMTools
 - 仕様の構文チェック
 - 仕様の型チェック
 - 証明課題の生成
 - 実行可能仕様の逐次実行とデバッグ支援
 - 実行可能仕様のコードカバレッジ計測
 - 実行可能仕様から C++ 言語や Java 言語への変換
 - Java 言語から VDM++ 言語への変換
 - 各種 CASE ツールとの連動
 - 仕様の清書支援

- 厳密な仕様の策定と記述
 - 第三者テストが可能になる
 - 運用・保守が可能になる
 - 再利用性が向上する
 - グローバル展開が可能になる

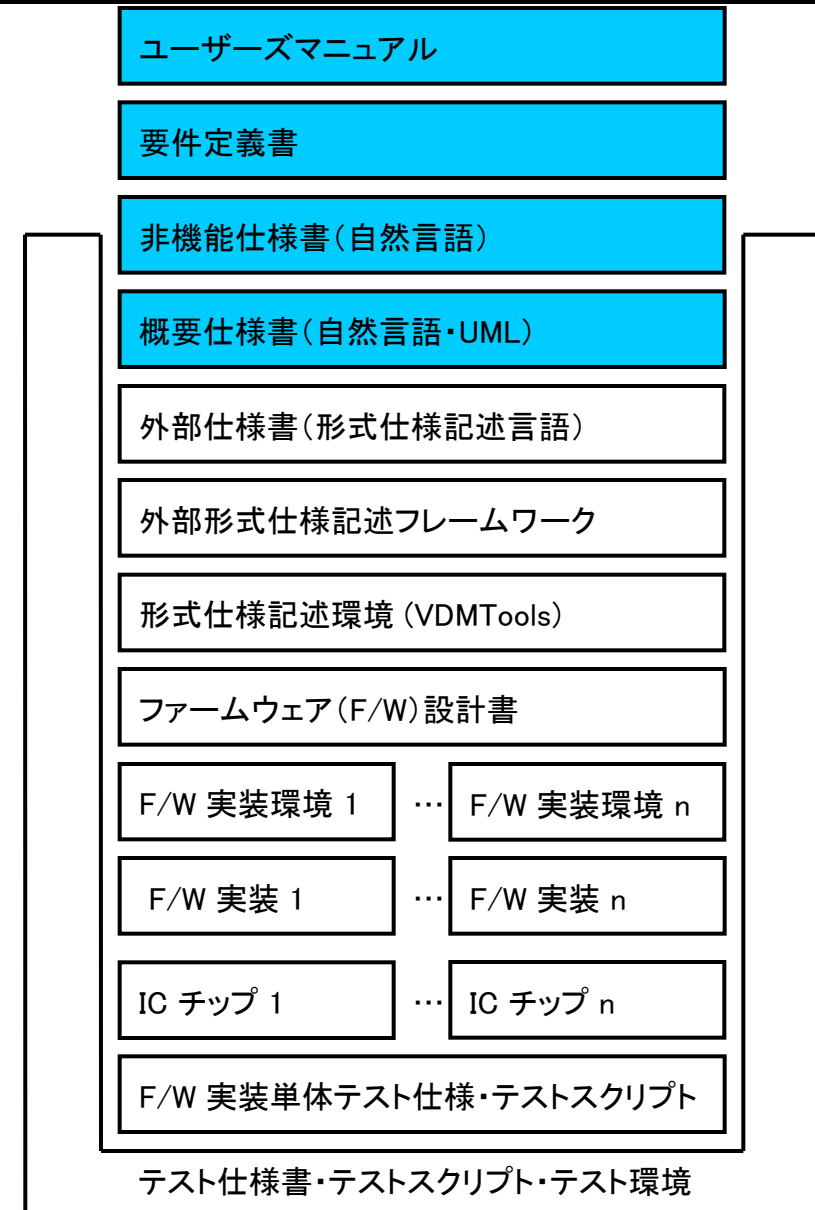
- 仕様を活用した開発プロセスの確立
- 仕様の多方面からの精査
- 仕様のテスト
 - 仕様のテスト
 - 「テスト仕様」のテスト

- コミュニケーションの促進

■ 以下は自然言語で記述した

- ユーザーズマニュアル
- 要件定義書
- 非機能仕様書
- 概要仕様書

■ 形式言語と自然言語それぞれによる記述の**整合性確保**、自然言語で書いた文書の**品質確保**に課題が残る



- 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

表1 仕様開発フェーズで修正した誤りの件数

誤りの発見工程	件数
仕様の記述	162
仕様の実行と単体テスト	116
仕様のレビュー	93
設計実装担当者・テスト担当者とのコミュニケーション	69
合計	440

「デバッグ密度」= $440 / 40,000 =$ 約 11 エラー / 千行

→ 形式手法は、開発の初期段階における誤りの発見に有効である

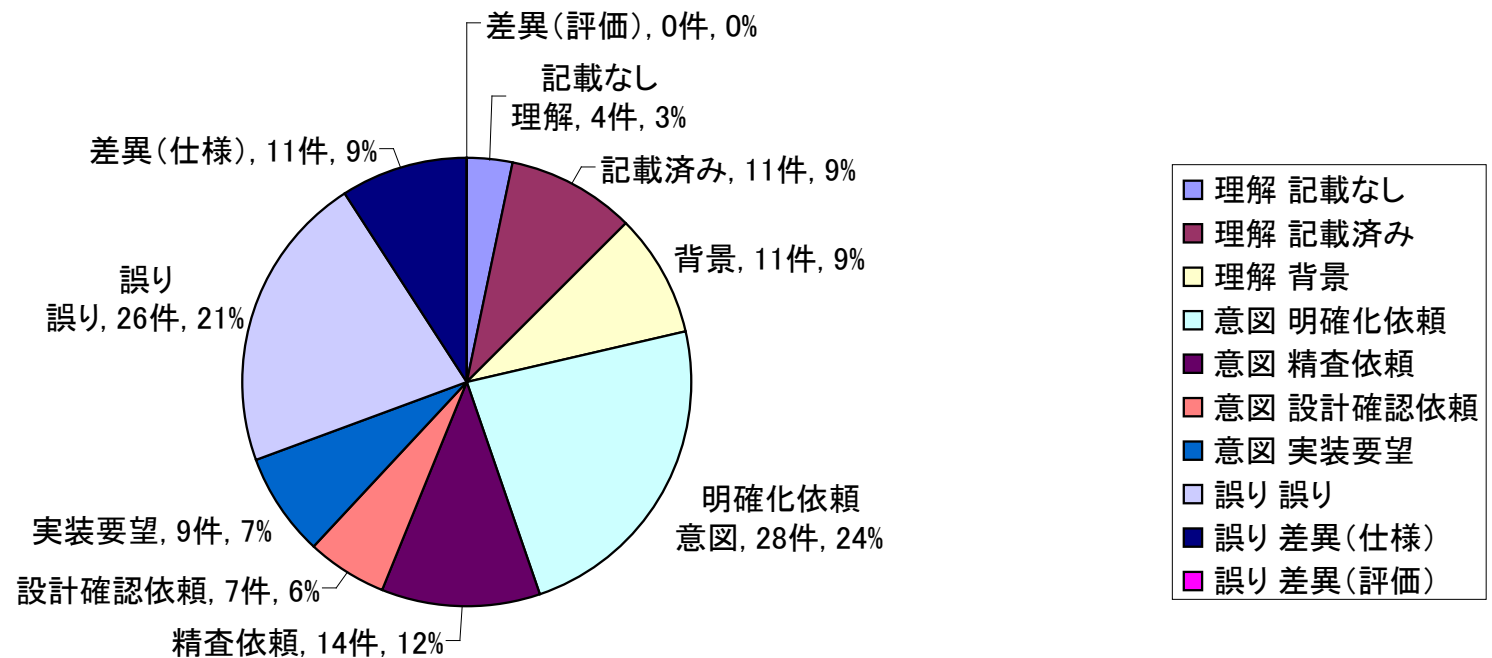
表 2 不具合原因の割合

不具合原因	割合
仕様記述もれ	0.2%
仕様記述誤り	0%
仕様不明確	1.8%
仕様見落とし	5.6%
仕様理解不足	10.7%
仕様確認不足	0%
仕様変更通知不徹底	0.2%
その他仕様関連外	81.5%

→ 仕様は書けている

→ 「読ませる仕様」の記述が課題である
→ DSL（仕様記述フレームワーク）の
検討と構築が重要

■ 自然言語によるマニュアル → 明確化依頼が多い

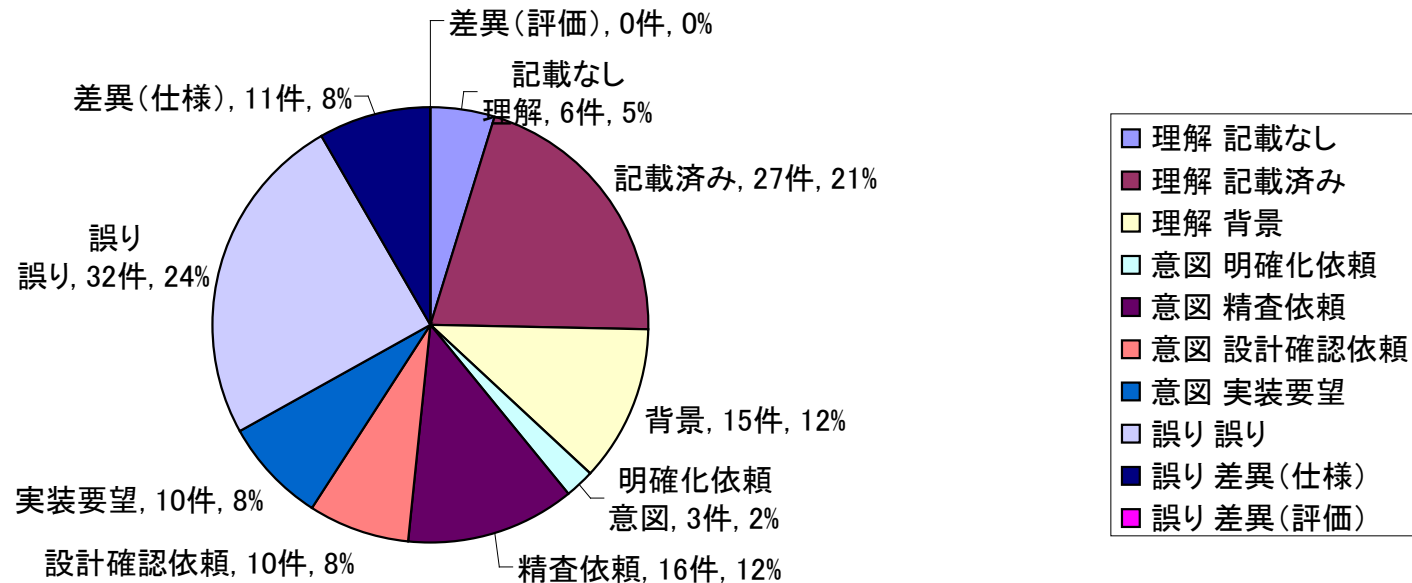


栗田太郎: 携帯電話組み込み用モバイル FeliCa IC チップ開発における形式仕様記述手法の適用,
情報処理情報処理Vol.49, No.5, pp.506-513, 2008年5月より引用

■ 形式仕様記述言語による外部仕様書

→ 「理解」に関する質問が多い

→ 仕様策定背景・経緯はコメントに記述する



栗田太郎: 携帯電話組み込み用モバイル FeliCa IC チップ開発における形式仕様記述手法の適用,
情報処理情報処理Vol.49, No.5, pp.506-513, 2008年5月より引用

- 自然言語・形式仕様記述言語の違い
 - 「理解」と「明確化依頼」以外は似通っている
- 自然言語
 - まずよくわからない…「明確化依頼」=「わかった」ととどまってしまう
- 形式仕様記述言語
 - 中途半端に「理解」できない。背景までつきつめて「理解」したい、納得したい
- 日本語での議論はつらい?
 - 記述から人格を消して「問題対私たち」とする

- 実装だけに有益なのではない
- 厳密な仕様はテストにも活用することができる
- 仕様 = テスト仕様・テスト環境 = 実装 が確認できる

- テスト担当者は緊張するとともに安心もできる
- 自然言語による仕様のみの場合、テスト担当者はよりどころになるものがない

- 上流工程、とくに仕様策定工程における**成果物の品質向上**に効果
- 仕様策定・実装・テストのイテレーションを多数回しても、ノイズが増幅されず、**仕様を洗練する**ことができる
- プロジェクト内の**コミュニケーションの活性化**に寄与する
- 他の工夫との組み合わせにおいて効果を発揮する
- 開発ドメインに応じて、**他の手法を組み合わせる**

■ 直接的な効果

- 記述と検証 → ゆくゆくは証明や段階的詳細化へ？
- 品質の確保

→ チームによる記述や検算の可能性を開く

■ 間接的な効果

- ドメインに対する認識・理解
- コミュニケーションの活性化
- 技能の向上（ドメインエンジニアリング、コミュニケーション）

→ ストレスの軽減や生活の改善につながる

- 問題に対して即時に対応できるように
 - 影響範囲の明確化
 - 回帰テスト

- マネジメントに安心感を与えられるように

- 何よりも、プロジェクトに参加しているメンバが、日々ストレスフリーに過ごすことができるように

形式手法導入の成功事例から、形式手法導入の検討や計画立案の際に有用な知見を得ることを意図し、以下を学習

- 成功と言われている事例では、どのようにプロジェクトに形式手法を導入したか、どのような成果を得たか

- 栗田太郎,「仕様の記述力を鍛える 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 2007年2月12日号, 133—152.
- 栗田太郎,「モバイル FeliCa のソフトウェア開発における品質確保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 (July 2010), 148—157.
- 栗田太郎,「形式手法の実践に対してよく尋ねられる質問とその回答」, SEC Journal Vol. 7 No. 1 (Mar. 2011), 34—39.

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：成功事例

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