第3回形式手法の産業応用ワークショップ

駅務機器ソフトウェア開発における形式手法の活用事例

2012年11月12日

オムロンソーシアルソリューションズ 幡山 五郎
産業技術総合研究所 大崎人士　相馬大輔　Nguyen Van Tang

OMRON

目次

1. 背景と研究概要
2. 形式記述
3. 上流工程大規模テスト
4. まとめ

1. 背景と研究概要①

ソフトウェア開発における仕様品質の課題

組み込みソフトウェア開発において、要求定義工程で発生する不具合は全体の25%。
その不具合のうち50%以上は結合テスト以降に発見され、手戻りが発生している。

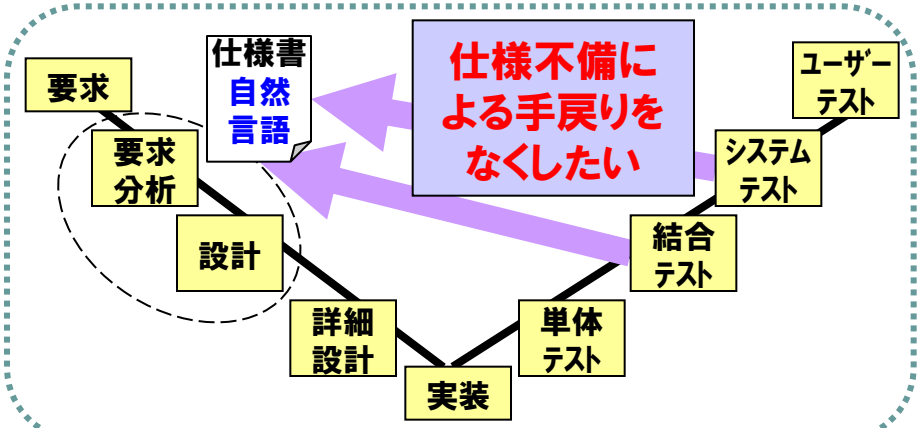
出所：経済産業省2010年版組込みソフトウェア産業実態調査報告書

駅務機器ソフトウェア

自動改札機や自動精算機、券売機などに組み込まれているソフトウェア

ICカード化、相互乗り入れの増加
⇨ルールや機能の複雑化
　データ量の増加

公共インフラを担う機器として高い信頼性が求められている。



1. 背景と研究概要②

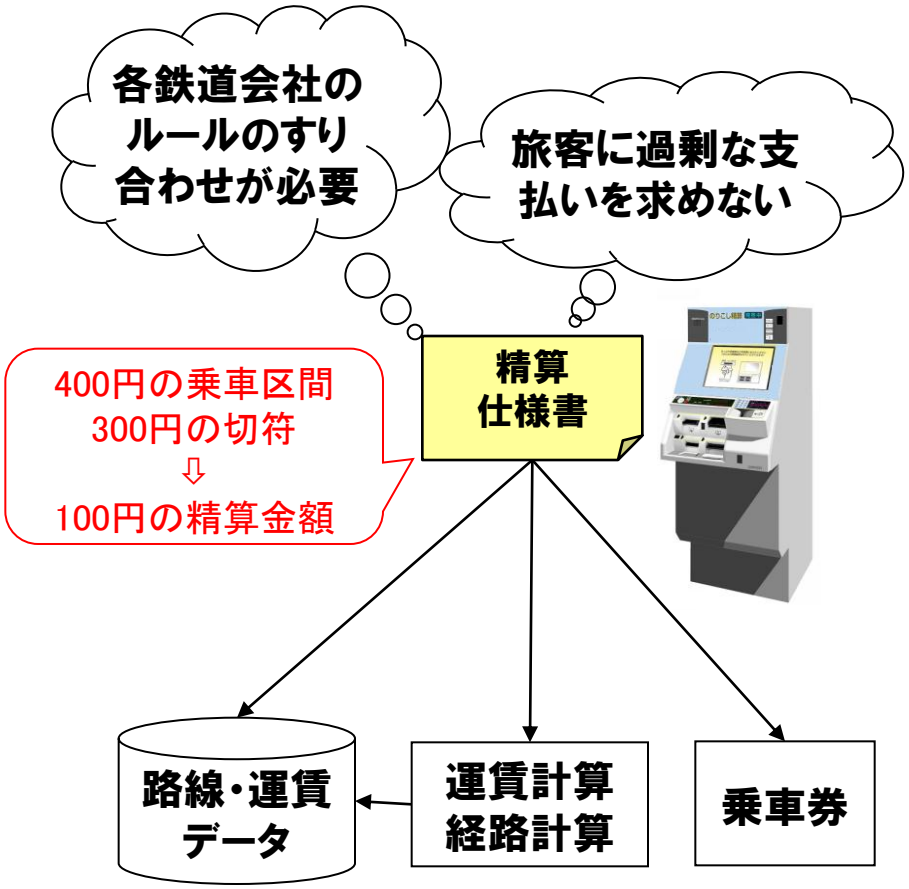
- 産業技術総合研究所との共同研究
  - 2008年10月～2011年3月
  - 本発表の範囲は2009年4月～2010年9月に実施した研究
  - 産総研2～3名＋オムロン2～3名
  - VDM開発経験者：なし
- 研究目標
  - 仕様書の誤解釈による不具合を除去
  - 仕様書の経年劣化防止
  - 仕様書の妥当性の確認
- 試行内容
  - 形式記述言語VDM++で仕様書を記述（2章 形式記述）
  - VDM仕様書のテスト実施（3章 上流工程大規模テスト）

1. 背景と研究概要③

試行対象：ある鉄道会社の精算仕様書

精算仕様書とは

- 自動精算機の精算金額の計算方法を文章や表で記述した要求仕様書
- 各鉄道会社で、
  １種類～数種類の精算仕様書
- 相互乗り入れの増加
  ⇨精算ルールの複雑化
- 課題
  - 誤解釈の可能性低減
  - 妥当性の確認



精算仕様書が関係するコンポーネント

2. 形式記述① 精算仕様書の形式仕様記述のまとめ

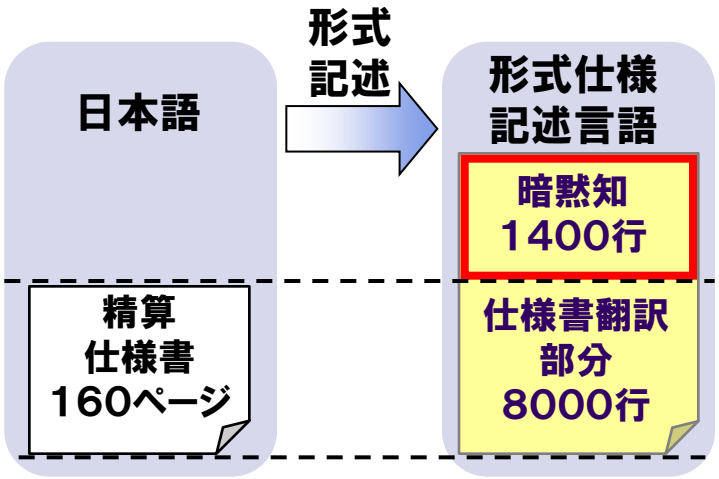
形式記述結果

形式記述工数：6人月
（仕様理解の時間は除く）

記述量：36クラス
9400行

仕様書の不備指摘件数：
29件
＝曖昧19件＋矛盾3件＋漏れ7件

課題：可読性の向上
形式記述の精度



効果①　仕様書の誤解釈を生みやすい記述の列挙

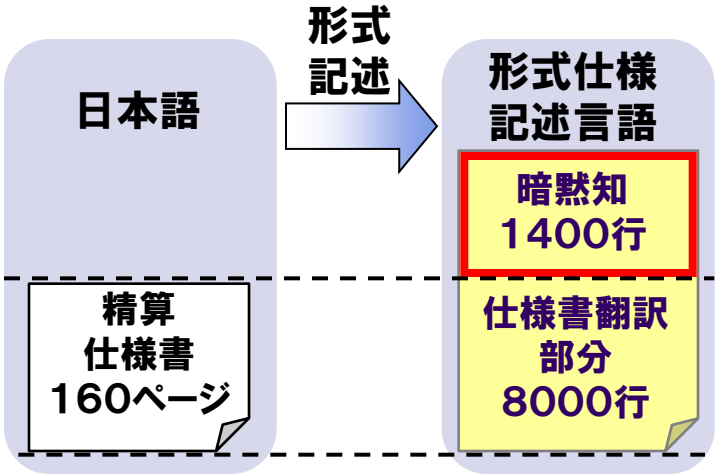
効果②　再利用性の高い仕様書の構造の提案
仕様書の構造に起因するア課題の洗い出し

2. 形式記述② 誤解釈を生みやすい記述－1

記述1
仕様書外の暗黙知が多い

仕様書に書かれていないさまざまな用語が使われており、ドメイン知識の少ない設計者の仕様理解を困難にしている。

記述改善策
関連知識の体系化



使われる用語は必ず定義が必要となる。
すべての用語の型が明確化。
すべての述語の入力と出力の型が明確化。

分類	定義される項目
乗車券	原券価値 連絡駅 6の字定期
路線図	線区 駅 連絡駅関係 ラッチタイプ
運賃	社局単独運賃 経路に対する運賃 乗継割引

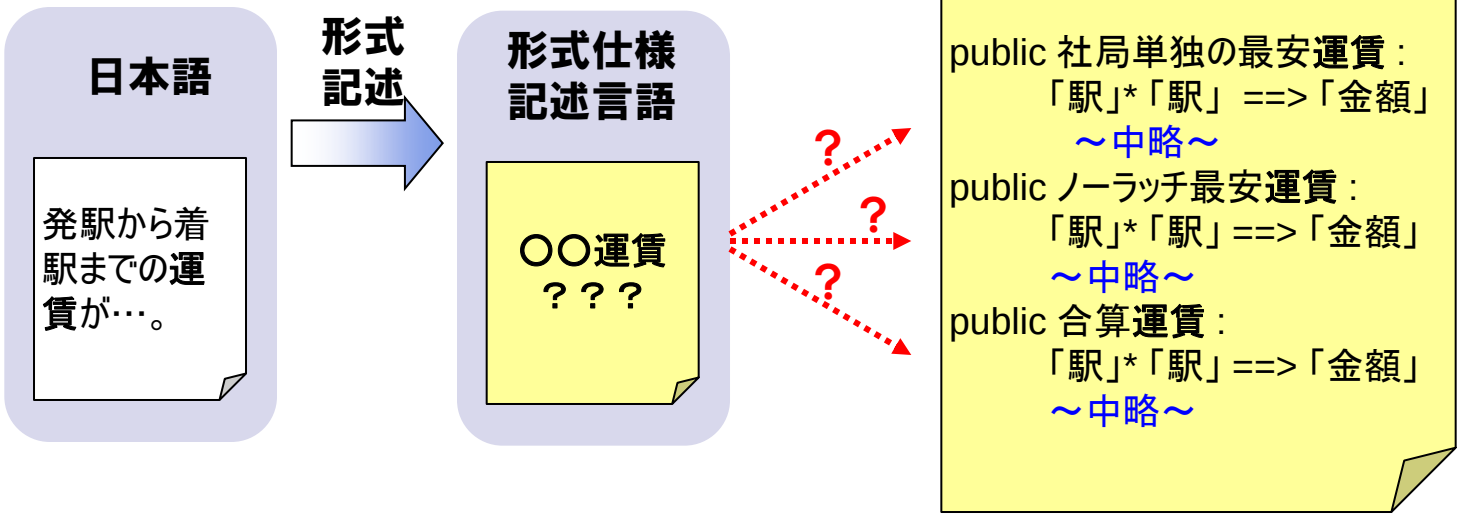
表. 精算仕様書の暗黙知の例

2. 形式記述③ 誤解釈を生みやすい記述-2

記述2
複数の意味で使われる用語

多義語の意味の区別を文脈から判断する必要がある場合、設計者の誤解釈が起こりうる。

記述改善策
多義語は明確に区別できるように記述する



複数の意味で使われる用語は各々で別の名前で定義されており、どの意味で使われているかが明確となる

2. 形式記述④ 誤解釈を生みやすい記述－3

記述3
適用範囲が不明確なルール

特殊ルール間の優先順位や適用範囲が不明確なケースがあり、設計者の誤解釈が起こりうる。

記述改善策
ルールの適用範囲の明確化
ルールの優先順位の明確化

日本語

○○の場合は△△の方法で精算する。

××の場合は▽▽の方法で精算する。

ただし、精算駅がA駅の場合は…。

形式記述

形式仕様記述言語

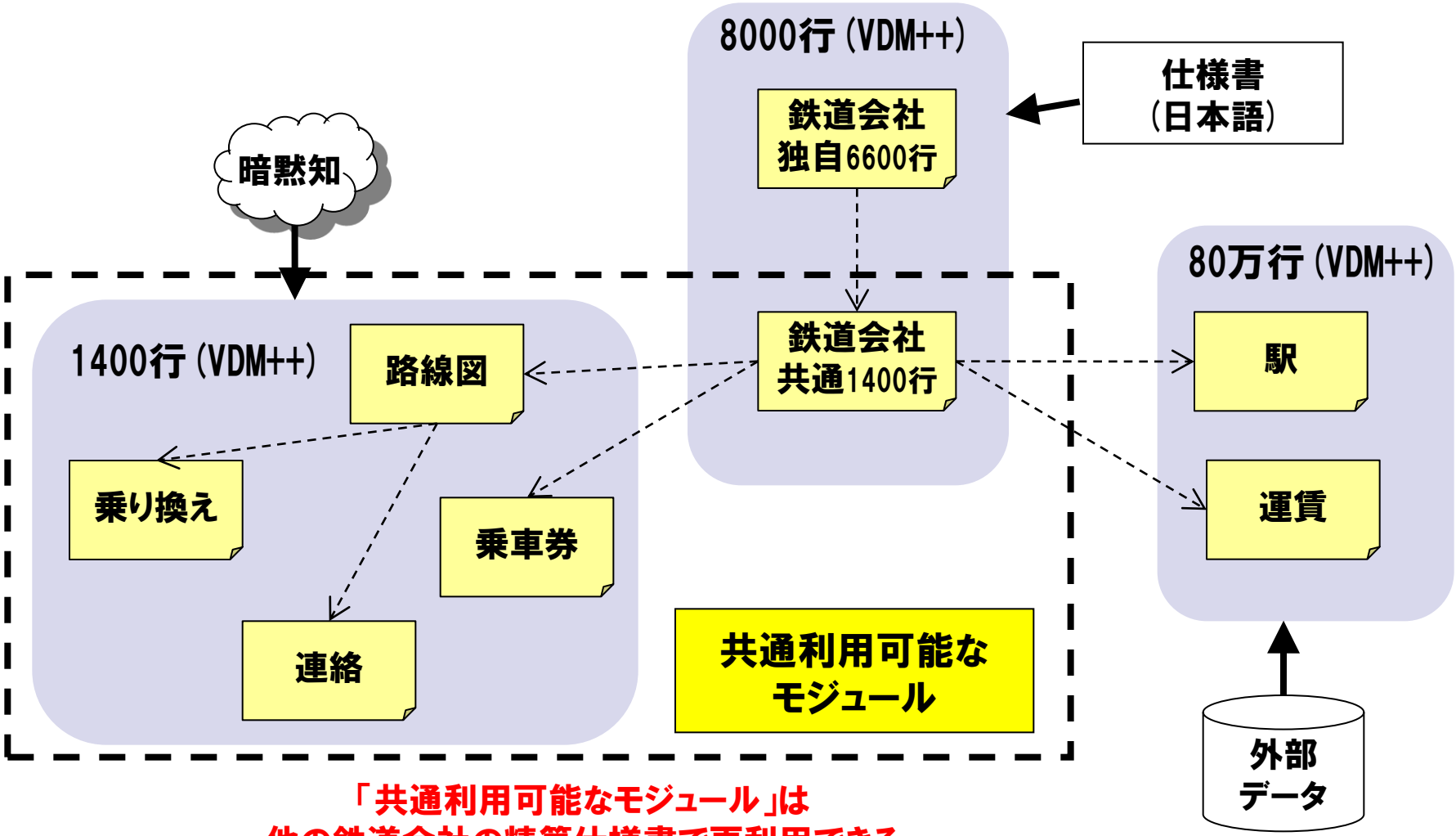
```
if  精算駅＝A駅 then
      精算結果＝（略）
else
      （略）
```

文章で一般的なルール、表でより詳細なルールを記述することもあるが、それらの間の優先順位が明確でない場合もある。

ルールの適用範囲は明確であり、また同じルールを複数箇所に分けて書くことも無い。

2. 形式記述⑤ 仕様書の構造-1

形式記述仕様書の構造

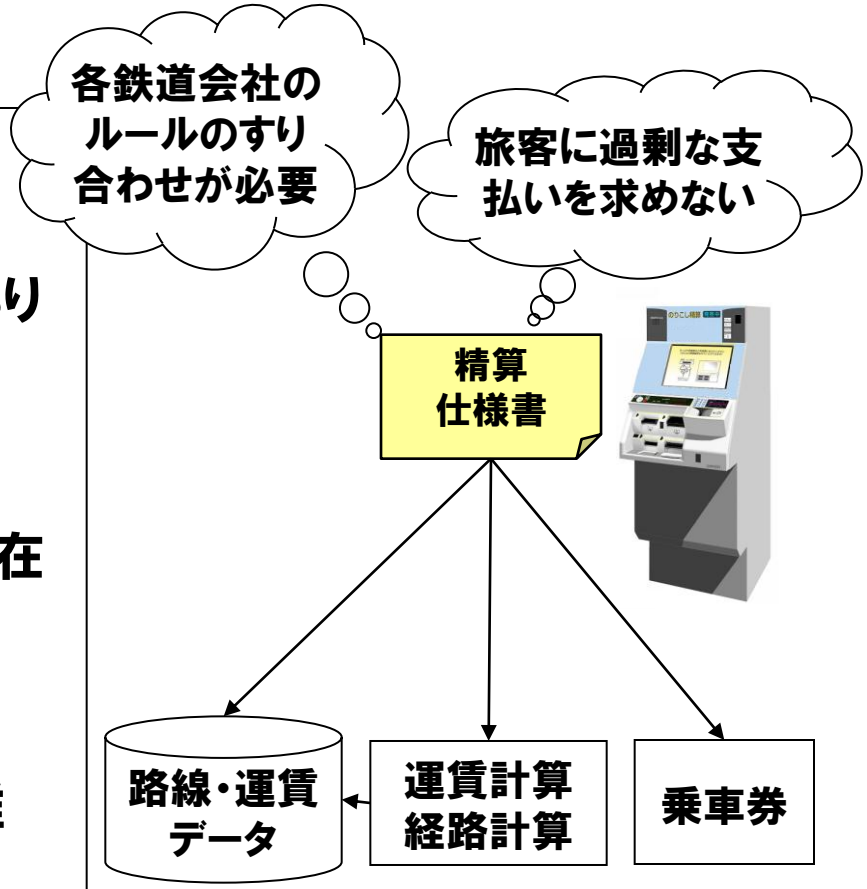


「共通利用可能なモジュール」は
他の鉄道会社の精算仕様書で再利用できる
⇨仕様書およびプログラムのメンテナンスの向上。

2. 形式記述⑥ 仕様書の構造-2

日本語仕様書のアーキテクチャの課題

- 精算仕様書に運賃計算の記述あり
  精算仕様書に乗車券のエンコードの記述あり
- 扱える乗車券の全容が不明確
  扱えない乗車券の全容が不明確
- 各鉄道会社で共通な仕様と独自仕様が混在
  ⇨仕様変更時のメンテナンスが煩雑
  ⇨共通な仕様部分に用語の不統一
- 路線や運賃変更時の影響範囲調査が困難
  - 路線形態や運賃の前提が不明確
  - 適用条件が一般化されていないルール

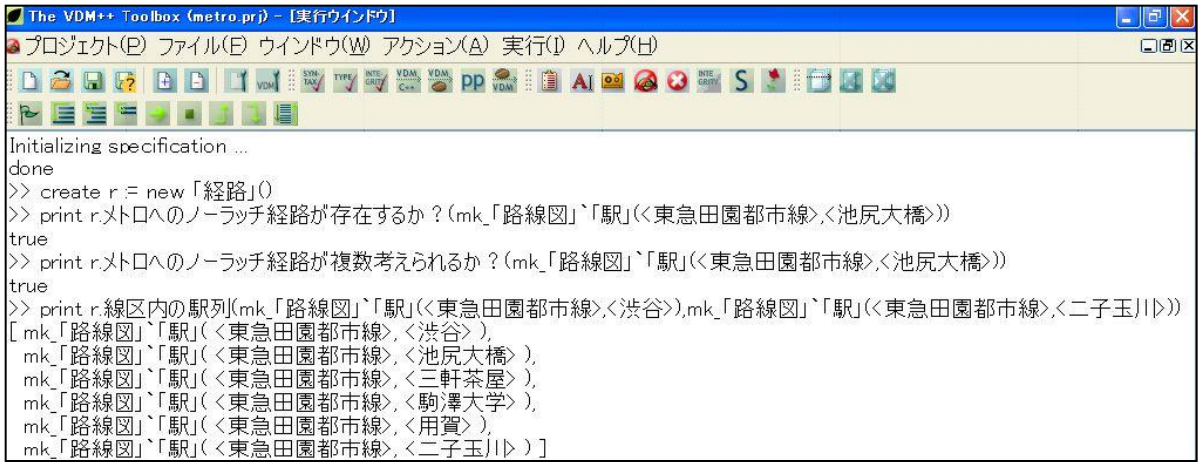


仕様の前提条件の不統一により、他社の仕様を形式記述する際に「鉄道会社共通部分」にかなりの修正が必要となった。

3. 上流工程大規模テスト①

仕様書テストの実行方法

- 形式記述仕様書をVDMToolsで実行
- 精算機の精算金額計算プログラムのテストケースおよびテスト結果を利用



仕様書テストの必要性・効果

- 形式記述仕様書に記述のあいまい性はないが、
  - 日本語仕様書の誤解釈(知識不足、ミスリーディングな記述)
  - VDM++言語のコーディングミス
  - 日本語仕様書が鉄道会社の意図と異なる内容

  に起因する不具合混入の可能性あり
    - ⇨ 仕様書テストで結果の期待値との比較により検出。
- 各関数への事前条件・事後条件・不変条件のチェックにより、ルール間の齟齬の発見。

3. 上流工程大規模テスト②

仕様書テストの方針

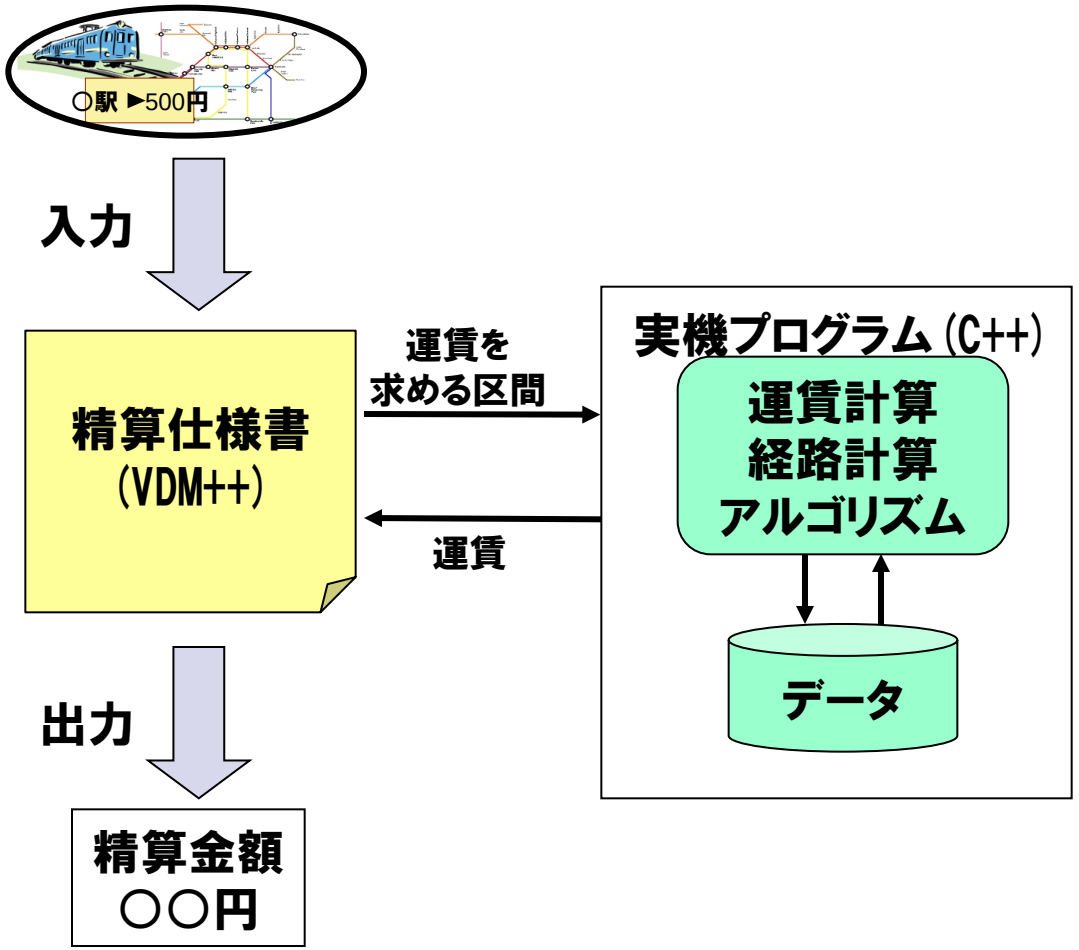
- 精算仕様書の妥当性の確認が目的
- 運賃計算アルゴリズムやデータの妥当性は別の手段で確認

⇩

- 精算機に搭載されている精算金額計算ソフトウェアのプログラムの一部と連携

⇩

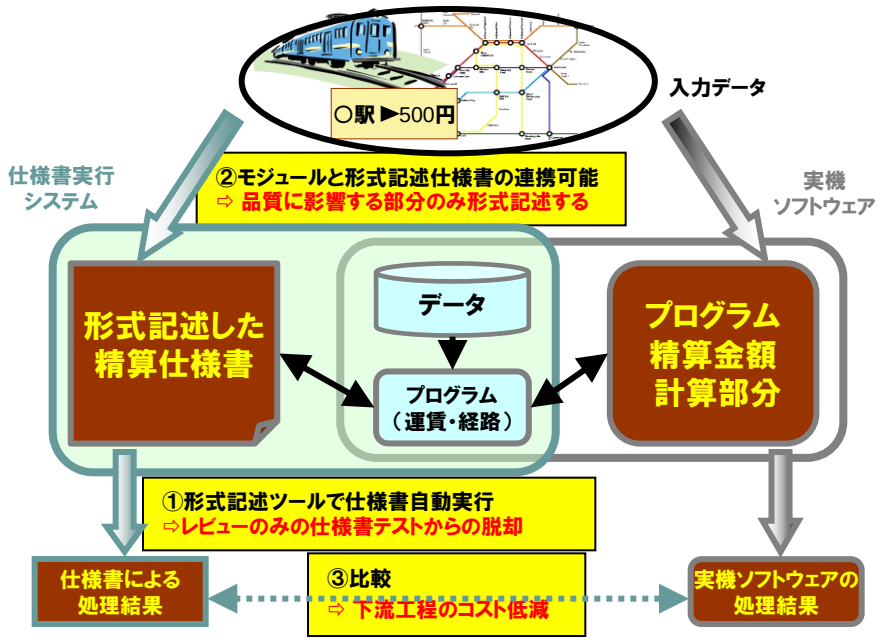
- 品質を担保すべき仕様のみの形式記述でテスト可能
- テストの実行速度向上



3. 上流工程大規模テスト③

実行環境

- 産総研検証サーバー「さつき」を利用
- 64コアCPUを利用し、80万ケースを5日間で実行
- 実行速度は実機の1/10～1/20



実行結果

- 検出不具合
  VDM仕様書のコーディングミス　26件
  ミスリーディングな日本語仕様書　2件

- 課題
  ①読みやすい形式仕様記述では処理速度が著しく下がる例がある
  （例 For all …）
  約10%のテストケースが実行不可能

  ②実機プログラムのデバッグに使うには形式記述の精度を向上させる必要あり
  実機との相違 およそ20%

4.まとめ

1. 問題を感じていた既存の運賃計算仕様書をVDM++で記述してその効果を確かめるための試行について発表した
2. もともと感じていた問題点(記述のあいまいさ、暗黙値、…)が具体的に列挙された
   →既存の日本語仕様書を修正
3. あまり意識をしていなかった仕様書の構造上の問題が明らかとなった
4. 日本語の仕様書を間違えずにVDM++に翻訳することが課題の一つ
5. 多数の運賃計算仕様書が存在し、それらをすべて翻訳することは社内で決心できていない
6. 「背水の陣」で取り組まないと進まないのであろう