# 事務システムにおける形式仕様適用例

佐原伸
日本フィッツ(株)
トレードワン事業部
ss@shinsahara.com



# 事務処理ソフトウェアの問題点

- 曖昧な仕様に起因するトラブルが非常に多い
  - 自然言語により曖昧かつ手続的に仕様を記述
  - それを手続的にプログラミングしていく
  - 重大な欠陥を含み，保守性が無く，再利用性のないソフトウェアが大量に生産されている

# 自然言語仕様の問題点

- 自然言語の曖昧さに起因する設計の欠陥
- 手続的な記述から「意味」を把握する困難
- 仕様記述段階で不完全な手続的設計が混入することによる後続工程の困難
- 自然言語による記述といっても，一種の疑似コード的記述が必要となり，疑似コードの構文をその場で「発明あるいは決定」する時間も馬鹿にならない



# 形式仕様記述言語の採用

- VDM採用
  - デンマークIFAD社のVDM++[2]とツールVDMTools
    - 型チェック・仕様インタープリタ・Roseリンク・C++/Java生成
  - 採用理由
    - 実用的で「買える」製品はVDMToolsとB
    - 教科書や例題がVDMの方が多い
      - VDMの方が多少の経験があった
      - VDMの日本での使用実績も多少あった
    - VDM-SLはISO標準だが、Bは２社が喧嘩していた
    - IFAD社と縁があった

# 対象システム

- トレードワン・システムのサブシステム開発に使用
  - 証券バックオフィス・システムのパッケージ
  - マル優管理システム（昨年秋）
  - オプション・システム（現在）
- システムのアーキテクチャ
  - 3層モデル
  - クライアント側はWebLogic Server上にJavaで開発
  - サーバー側はWebLogic Enterprise上に C++で開発
  - データベースはオラクルを使用している



# マル優管理システム

- 開発期間
  - 2000年９月～2001年１月初旬
- 開発要員
  - ソフトウェア開発歴20年以上で，フルタイムが3人，0.4人月/月が2人，0.2人月/月が1人の計6人で，投入工数としては4人月/月である
    - 一人を除いて全員証券業務作成の経験はなく，VDM++の使用も初めて
    - C++，Javaを初めて本格的に使用した
    - 形式手法・形式仕様に関しては，4人が知識を持っていて，ある程度の経験もあった

# マル優管理システム

- 工程
  - サブシステムの設計工程から
    - 「要求仕様定義・分析工程は終わった」ことになっていた
      - ドメイン専門家は３代目
        - 「私にもどうしてこうなっているか分からないんです」
- スケジュール
  - 開発着手から約2ヶ月で一部機能を単体テスト終了
  - 2ヶ月半で全機能を単体テスト終了
- 予想ステップ数
  - 3万行



# マル優管理システム

- 入力
  - 業務詳細仕様書
    - システム要求」を記述した文書であるが，機能中心に分割され，手続的に記述されていて，実際にはいわゆる「詳細設計書」に近い
  - データベース仕様書
  - 画面仕様書
  - チェック仕様書

# マル優管理システム

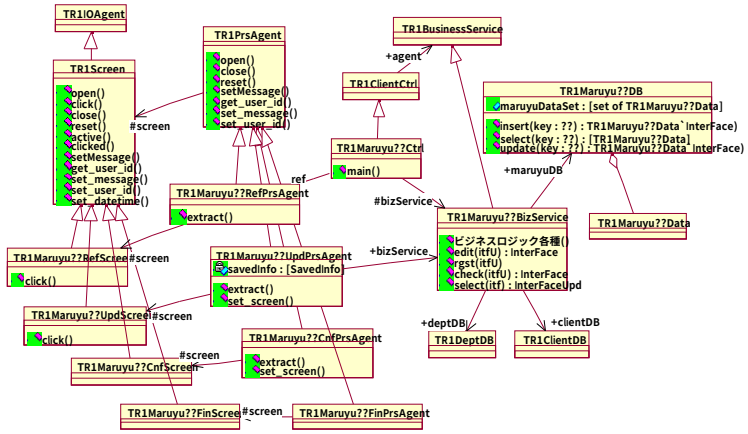
- VDM++適用機能
  - VDMToolsの構文チェック・型チェック機能を主として使用し，詳細設計
  - クラス図のドキュメント化は，Rational社Roseツールとの相互接続機能使用
    - だんだん使わなくなった
  - 「トレードワン」システムと独立のVDM++共通ライブラリーのテストには，VDMToolsの仕様実行インタープリタとコードカバレージ機能を使用



# マル優管理システム

- クラス構成
  - GUI層・ビジネスロジック層・データ層を次図のように構成
- 共通クラス
  - Object > TR1Object > TR1Date
  - 日付、集合、系列、文字列、整数、文字

# マル優管理システム






# マル優管理システム

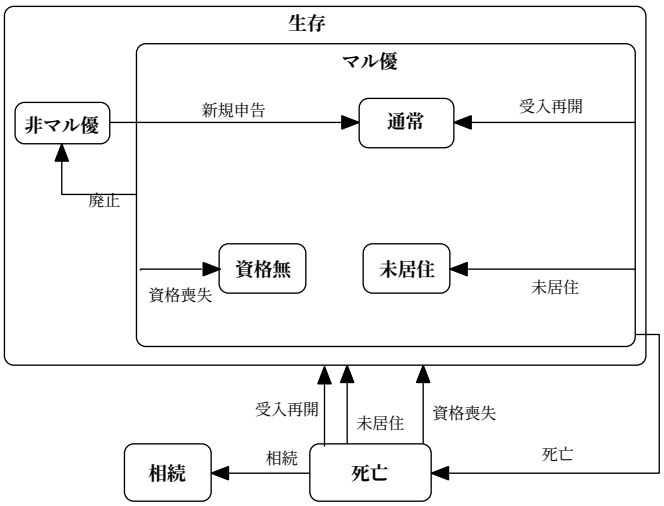
- 制約の記述
  - システム開発の最終段階で，サブシステム間インタフェースや，業務詳細仕様書に起因する欠陥が数多く発見されたため，業務詳細仕様書を見て修正することが困難になり，マル優管理システムの制約を記述し整理しなければならなくなった．これは，本来，設計に先立って行うべきことであり，前述の時間的制約のため省略した作業であるが，やはり必要となった．

# マル優管理システム

- 主要な制約
  - マル優顧客の状態（次図）
    - 業務詳細仕様では一つの区分の値として，状態と遷移が混在する形で記述されていたため，仕様に様々な漏れが生じていた
  - 管理項目の制約式
    - 全部で２２個抽出
  - 帳票を作成するためのデータの時系列制約
    - 業務上は重要ではないが...
    - バッチ処理時における、オンライン時との乖離の修正に使っていたため，設計仕様および効率上重要な制約となった



# マル優管理システム



# マル優管理システム

- 制約式の例
  - 「マル優口座が存在し，かつ，その口座のマル優取扱区分が，通常か未居住か資格無であり，かつ，以下の式が成り立つこと．ここで，Σは「顧客毎の合計」を意味する．」
    - マル優申告額 = マル優余裕額 ＋ Σ一般投信マル優残高 ＋ Σマル限限度額
    - マル優残高 = Σ累投証券残 ＋Σ一般投信マル優残高
    - 累投証券残 ≦ マル限限度額
  - この制約式は，「ある特定の条件下で，マル優限度額を越えた買付がいくらでもできてしまう」という業務詳細仕様書に隠れていた重大な意味的欠陥を発見することに役立った



# マル優管理システム(適用結果)

| 分類 | VDM++仕様 | Java | C++ | プログラム合計 |
|---|---|---|---|---|
| 事務処理共通クラス | 774行 | | | |
| トレードワン共通クラス | 1342行 | | | |
| 制約仕様 | 1539行 | | | |
| 詳細設計 | 8102行 | 9403行 | 9028行 | 1万8431行 |
| 合計 | 1万1856行 | 9403行 | 9028行 | 1万8431行 |

# マル優管理システム(連結前の欠陥)

| 欠陥・修正原因 | 件数 |
|---|---|
| サブシステム間インタフェースの了解違いによるもの | 9 |
| ユーザーレビューによる機能追加 | 1 |
| 業務詳細仕様書の考慮漏れ | 1 |
| 用語集の未整備による項目定義の誤解 | 1 |
| 合計 | １２ |



# マル優管理システム

- リリース後の欠陥
  - 0
- 単体テスト以前の欠陥の原因＝５７
  - 業務詳細仕様書の考慮漏＝３５
  - チェック仕様書の考慮洩れ＝１３
  - 管理上のミス＝３
    - エラーメッセージの申請忘れなど
  - ユーザー要求＝２
  - 画面仕様書・テーブル仕様書＝それぞれ２

# マル優管理システム

- 最終履歴
  - 開発期間＝３ヶ月
  - 工数　＝13.3人月
    - 開発　＝12人月
      - 仕様作成　＝５人月
      - プログラム作成　＝６人月
      - 管理　＝１人月
    - 修正　＝1.5人月
      - 仕様修正　＝0.8人月
      - プログラム修正　＝0.5人月
      - 管理　=0.5人月



# マル優管理システム

- 考察
  - 品質
    - 連結テスト以後の欠陥
      - すべてVDM++適用以前の工程で発生
      - VDM++適用以前の工程で発生した欠陥のうち，発見可能だった業務詳細仕様書の欠陥は，単体テスト以前にすべて発見し修正
  - 生産性
    - COCOMOによる見積の３分の１

# マル優管理システム

- VDM++
  - 仕様を２～３回書き直し
  - 仕様の修正余波を型チェックシステムが指摘
  - 共通クラスは仕様実行とカバレージで１００％テストできた
  - 従来手法より，仕様記述言語の曖昧さが無く，言語レベルが高いので，仕様を書きやすい
    - 特に役立ったもの
      - » 集合・系列の内包表記、パターンや束縛、構成子、限量子



# オプション・システム

- 日経２２５のオプション・システム
- VDM++適用範囲
  - 要求分析工程から適用
  - VDM++インタープリタによる要求仕様検証
  - テスト・フレームワーク作成
    - UseCaseに対応したテストシナリオでビジネス要求をテスト
  - 設計フレームワーク詳細化
    - 通称「トレイ・モデル」
  - VDM++の日本語化
    - 識別子、文字列、注釈

# オプション・システム

- 例
  - 系列クラスのコードカバレージ例
    - バッチファイルの順序の定義などに重要
    - UNIX版TeXで処理したので、赤色の部分が未実行仕様
      - Windows版MSWordでも同様の出力
  - 自動権利処理仕様のたたき台
    - 日本語UseCaseの曖昧さを発見
      - 「SQ値と権利行使価格が等しい」⇨ 円未満と円の比較になる
      - 「受け渡し金額＝...」⇨ 結果は円未満があるが...
    - 限月処理のための日付クラスも添付
      - Windows版TeXで処理したため、未実行部分が赤くならないが...