# 形式仕様記述入門
# ～問題を早めに見つける～

国立情報学研究所　石川　冬樹
f-ishikawa@nii.ac.jp
2009/10/06 @ SPI Japan 2009

# 自己紹介

- 2007年より国立情報学研究所助教
- 活動分野
  - サービスコンピューティング
  - ソフトウェア工学，*特に形式仕様記述の応用・教育*

トップエスイー　http://topse.jp/
産業界の技術者向け先端ソフトウェア工学教育コース
- 「科学的アプローチ」のビジョンを伝える
- 毎年30人程度（現在5期生募集中）

形式手法実践ポータル　http://fmug.grace-center.jp/
入門サイトを構築中

# 目次

- **形式手法とは？**
- 形式仕様記述とは？
- 適用事例紹介
  - ICチップ（フェリカネットワークス）
  - 鉄道系システム（パリ地下鉄など）

# 形式手法？

数理論理学などに基づき品質の高い
ソフトウェアを効率よく開発するための
科学的・系統的アプローチ

システムの注目する側面を正確に，曖昧さのない言語で表現する

- 開発の早い過程の中間成果物において，
  - *曖昧さや思い込みを排除*
  - *科学的・系統的な分析・検証により品質向上*
- 後の過程の誤り発覚による手戻りを防止

# 形式手法？

- 仕様や設計を「きちんと」書こうとする過程により
  - 曖昧さを解消することになる
  - 不正確，不整合も表面化する
  - システムに対する理解が深まる
- 仕様や設計を「きちんと」書いた結果により
  - 誤解なく情報を共有できる
  - 科学的・系統的な分析・検証ができる
  - 分析・検証をツールに支援させることができる

# 形式手法？

*厳密な文法・意味論，*
*理論的裏付けを持つ記法を用いて*

- 仕様や設計を「きちんと」書こうとする過程により
  - 曖昧さを解消することになる
  - 不正確，不整合も表面化する
  - システムに対する理解が深まる
- 仕様や設計を「きちんと」書いた結果により
  - 誤解なく情報を共有できる
  - 科学的・系統的な分析・検証ができる
  - 分析・検証をツールに支援させることができる

*中間成果物の品質をそれを構築した時点で*
*確認するとともに，後の過程へ引き継いでいく*

# 形式手法への期待・その必要性

- ソフトウェアシステム開発への要求の高まり
  - 成果物の品質・信頼性
  - 開発手法・プロセスの系統化・効率化
- 評価・認証
  - （例） ISO/IEC 15408（Common Criteria）：セキュリティの高レベルな保証の要件として，設計の形式検証が含まれている
- ソフトウェア工学スキル・カリキュラム
  - （例） J-07SE：「形式手法」「ソフトウェアV&V」

# 目次

- 形式手法とは？
- **形式仕様記述とは？**
- 適用事例紹介
  - ICチップ（フェリカネットワークス）
  - 鉄道系システム（パリ地下鉄など）

# 仕様

- M. Jacksonによる「仕様」の概念


適用領域（与えられたもの）　機械領域（作られるべきもの）

ソフトウェア博物誌—世界と機械の記述
M. Jackson（玉井・酒匂訳），トッパン

- 開発におけるポイント
  - 「どう実現するか」より「（システムが）何をするか」に注力して議論，定義していきたい
  - 誤り，曖昧さ，不整合などが残されていると，後の過程において大きな手戻りのコストを引き起こす

# 形式仕様記述とは？

- 形式仕様記述：
  - （主に機能的な）仕様を記述する
    - データ構造とそれに対する操作
    - 厳密だが抽象的なモデルの構築
  - 分析・検証を行う
  - 実装につなげていく

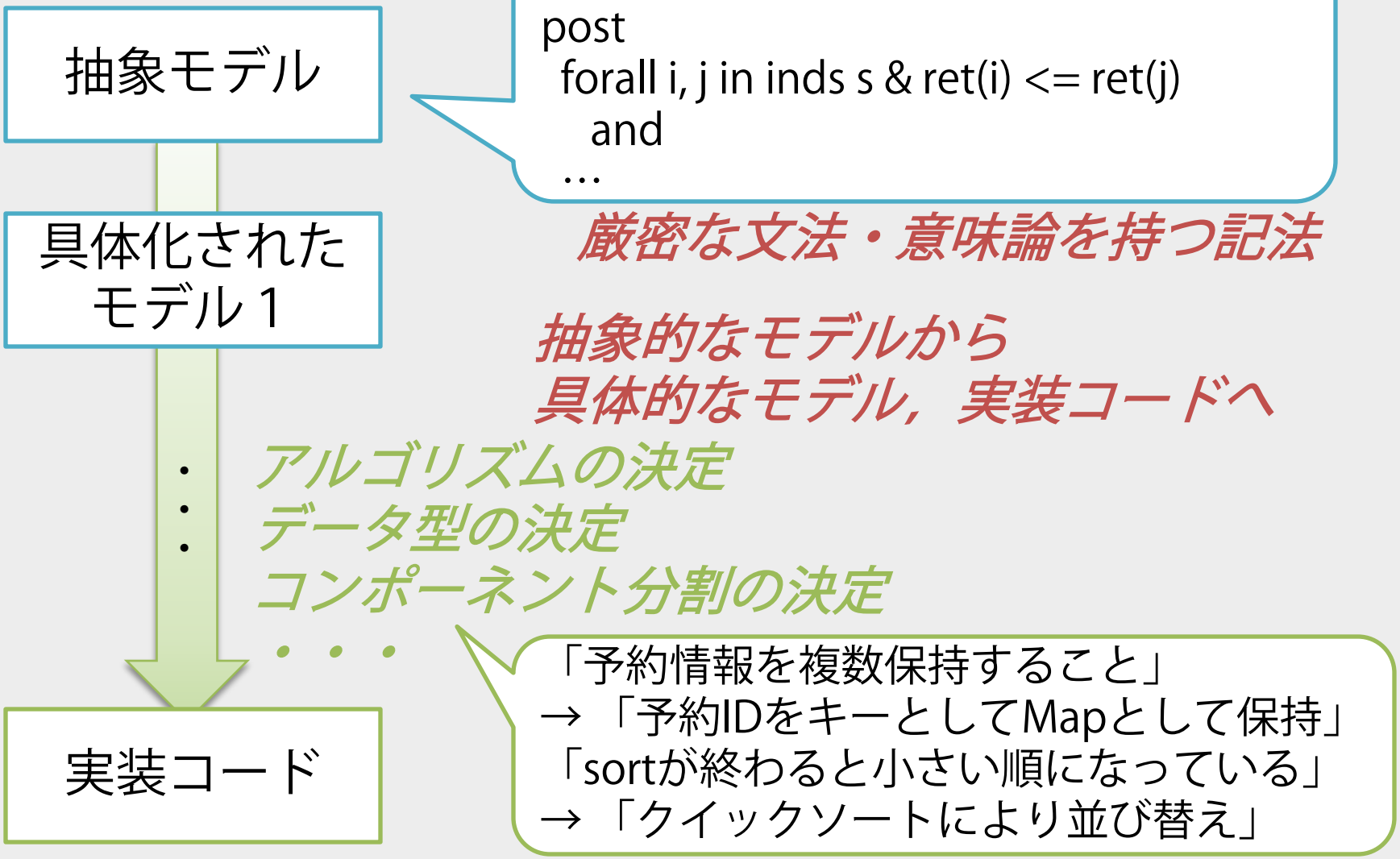
*意図・目的に応じた様々な言語*

*意図・目的に応じた様々な手法・ツール*

「モデル検査」と補完 → 青木先生のお話：

状態遷移の可能性が複雑な部分（非決定性によりテストが困難な部分）をピンポイントで抜き出して記述し，網羅的な状態探索による検証を行う

# 形式仕様記述によるモデル化・プロセス



# 形式仕様記述における検証・妥当性確認

- 定理証明：「法則」により確認
  - 三段論法，帰納法，・・・
    - 「定員未満のときのみ予約追加を受け付ける」
    - ⇨「予約追加により定員を超えることはない」

      （これは整数に関する不等式に関する証明となる）
- モデル検査・テスト：「観測」により確認
  - テスト：特定の状況（のみ）を再現して確認
    - ユニットテスト，受け入れテスト，・・・
  - モデル検査：可能な状態遷移を網羅的に探索
    - 通常仕様全体ではなく，並行制御プロトコルなど状態遷移が難しい部分に絞って適用する

# 形式仕様記述の代表例

- VDM（VDM-SL，VDM++）
  - インタプリタ実行・テストによる検証・妥当性確認を中心としたライトウェイトな手法
  - *フェリカネットワークスによる最近の適用事例*
- B-Method
  - 「正しさを保証した実現」のため，定理証明を主軸としたプロセスを定義
  - *鉄道系システムにおける多くの適用事例*
  - EUプロジェクトにおいて，位置づけの異なるEvent-B手法・ツールも構築されている
- Z，Alloy，・・・

# 目次

- 形式手法とは？
- 形式仕様記述とは？
- **適用事例紹介**
  - ICチップ（フェリカネットワークス）
  - 鉄道系システム（パリ地下鉄など）

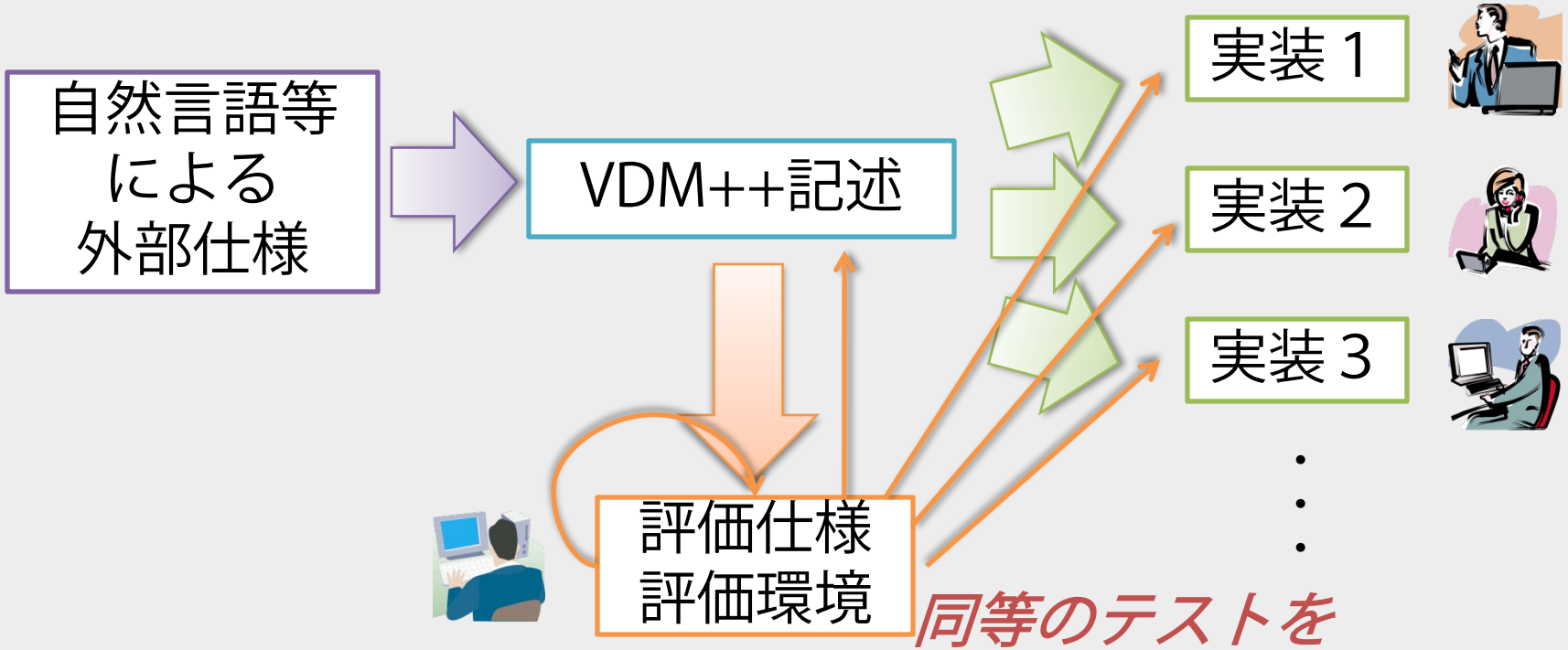
# VDM適用事例： 概要

- ICチップ
  - 適用対象： 外部仕様
    - 複数の実装者への入力となる共通仕様
    - 外部仕様をVDM++により記述し，インタプリタによる実行を通してテストを行う
  - 目的
    - 厳密な仕様の策定
    - 自然言語・UML・VDM++による多方面からの分析・精査プロセス導入
    - VDM++や様々な実装で共用できる評価環境構築
    - 意識，考察，コミュニケーション促進

# VDM適用事例： 参考文献

- 仕様書の記述力を鍛える～モバイルFelica開発における形式仕様記述手法の導入事例～
  - 栗田太郎，日経エレクトロニクス2007年2月12日号
- 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
  - 栗田太郎，情報処理学会学会誌2008年5月
- その他，国際会議ICFEM 2008でのチュートリアル（日本人向け）など

# VDM適用事例： プロセス




*同等のテストを*
*VDM++や各実装に行う*

*ツールによる支援*

- *制約チェックを行いながらの*
  *インタプリタを用いた実行*
- *ユニットテストフレームワーク*
- *カバレッジ測定*

# VDM適用事例： 規模

- 3年3か月
- 50〜60人でのプロジェクト
- VDM++約10万行
- 対応するC/C++実装約11万行
- 対応する自然言語マニュアル677ページ

# VDM適用事例：主な効果

- 「仕様不明確」ということが不具合の原因となったのは不具合のうち1.8%のみだった
  - 「記述が曖昧で意図が不明瞭である」という質問よりも「仕様に書いてあるがわからない」という質問が増えた

    *深く読まざるを得ないのでわかった気になれないのでは*
- 仕様の評価工程において，ある実行パスでの事後条件エラーなど，レビューで見つけられなかった不具合を発見できた

# 目次

- 形式手法とは？
- 形式仕様記述とは？
- **適用事例紹介**
  - ICチップ（フェリカネットワークス）
  - **鉄道系システム（パリ地下鉄など）**

# B-Method適用事例： 概要

- 鉄道系システム

  （パリの地下鉄やパリ空港シャトルなどにおける
  自動運転システム，その他NY等でも事例あり）

  - 適用対象
    - 安全性の核となるソフトウェア部分
    - B-Methodに基づき，定理証明を用い正当性を保証しながら段階的に詳細化，実装を導く
  - 目的
    - 設計エラー・コーディングエラーを排除する

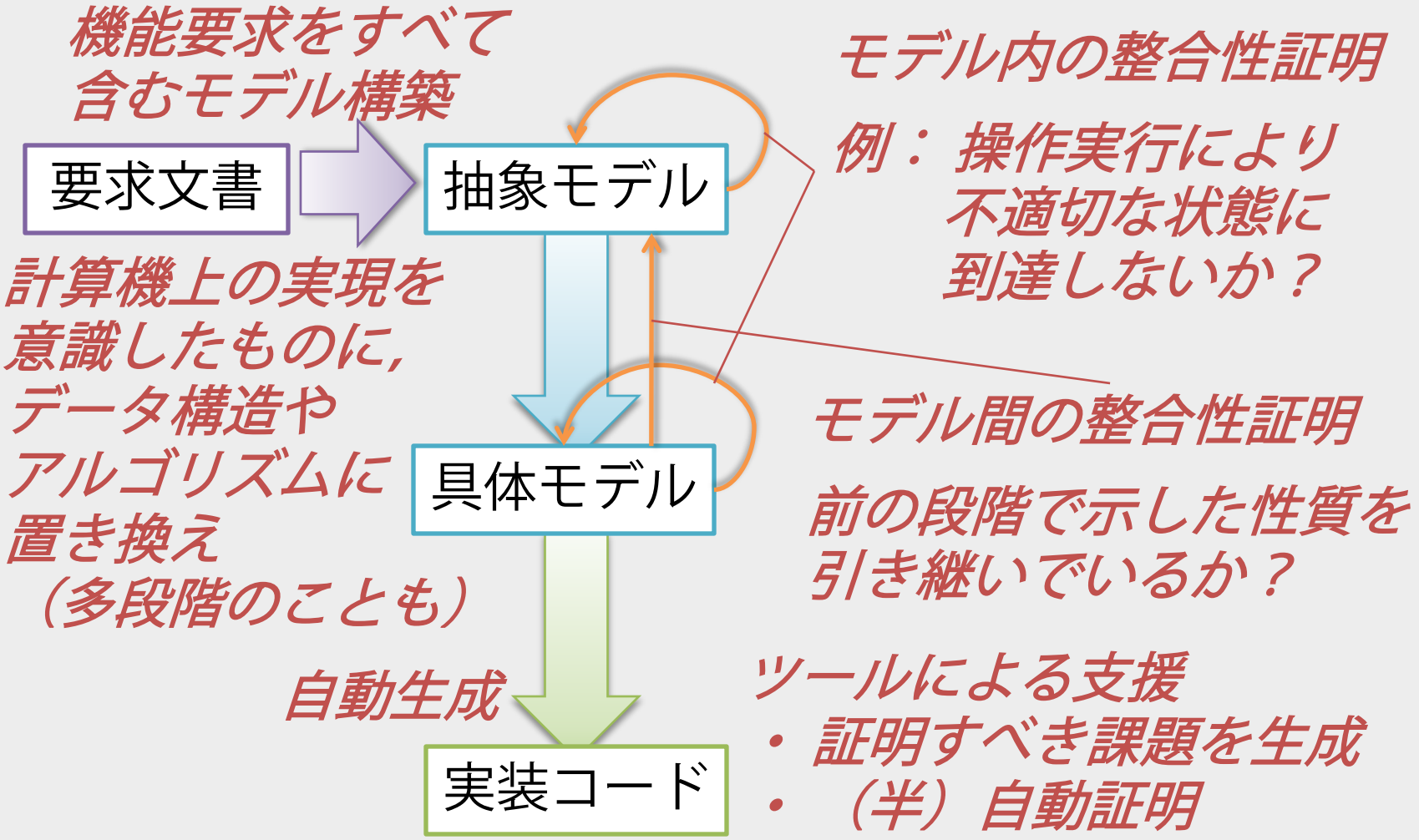
# B-Method適用事例： 参考文献

- パリ地下鉄の自動運転システム

  Météor　: A successful application of B in a large project
  - Matra Transport International, FM'99
- パリ空港の自動運転シャトル

  Using B as a High Level Programming Language in an Industrial Project: Roissy VAL
  - ClearSy & Siemens, ZB 2005
- 上記のまとめ
  - Formal Methods in Industry: Achievements, Problems, Future（J. R. Abrial, ICSE 2006）

# B-Method適用事例： プロセス



# B-Method適用事例： 規模・工数

| | パリ地下鉄<br>（FM’99） | 空港シャトル<br>（ZB’05） |
|---|---|---|
| 生成されたコード（ADA）のステップ数 | 86000 | 158000 |
| 行われた証明の数 | 27800 | 43610 |
| そのうち対話的証明の割合 | 8.1% | 3.3% |
| 対話的証明に要した人月 | 7.1 | 4.6 |

# B-Method適用事例： 規模・工数

- 空港シャトルにおける所要人月の割合
  - 準備： 5%
  - マネージメント： 8%
  - *抽象モデルの構築： 全体の55%*
    - うち18%が要求への質問，解析
    - うち5%がモデルのレビュー
    - うち16%が証明
  - 具体モデルの構築： 全体の24%
    - うち11%が証明
  - 設定管理，再現，ドキュメント化など： 8%

*「何を作るのか」の明確化・厳密化・正確化という，コストをかけるべきところにコストを*

# B-Method適用事例： 効果

- パリ地下鉄における最終的な効果
  - コード生成後，テストで見つかったバグはゼロ
    - B-Methodでは実装に至る各過程において正当性を検証し，その正当性を引き継いで実装コードを得るので，ユニットテストは理論上不要
  - その後の運用でもバグは見つからず

# まとめ

形式仕様記述

仕様を「きちんと」書こうとする

仕様を「きちんと」書いた結果を分析・検証する

- 開発の早い段階において，「その段階において決めたこと」（のみ）を抽象・形式モデルとして明確化するとともに，その品質を高める
- かけるべきコストを早い段階でかけ，後の過程での誤り等発覚による手戻りを防ぐ

ご清聴ありがとうございました！