

形式仕様記述シリーズ

シリーズリーダー

国立情報学研究所
石川 冬樹

講師

宇宙航空研究開発機構
小林 努

株式会社 proof ninja
今井 宜洋

ソニー株式会社
栗田 太郎



扱う技術アプローチ

- 厳密な記述を用い強力な検証技術も活用
 - 仕様や設計のあいまいさに起因する問題を排除
 - 上流工程での問題検出による効率化・高品質化（プログラムに対する強力な検査も）
 - テストなどあらゆる活動の基盤を底上げ

```
class イベント参加登録システム
  登録済みユーザ集合 : set of 「ユーザ識別子」;
  定員 : nat1;
  inv card 登録済みユーザ集合 <= 定員

  抽選登録する : set of 「ユーザ識別子」 ==> 「ユーザ識別子」
  抽選登録する(引数ユーザ集合) == is not yet specified
  pre
    card 登録済みユーザ集合 < 定員
    and exists ユーザ in set 引数ユーザ集合 & ユーザ not in set 登録済みユーザ集合
  post
    登録済みユーザ集合 = 登録済みユーザ集合~ union {RESULT}
    and RESULT in set 引数ユーザ集合 and RESULT not in set 登録済みユーザ集合~;
```

記述イメージ

技術の利用イメージ(一例)

実装詳細を捨象

重要な制約を明記
(これからできるコードは
何を守るべきなのか)

厳密化

```
class イベント参加登録管理システム
  登録済みユーザ集合 : set of 「ユーザ識別子」;
  定員 : nat!;
  inv card 登録済みユーザ集合 <= 定員

  抽選登録する : set of 「ユーザ識別子」 ==> 「ユーザ識別子」
  抽選登録する (引数ユーザ集合) == is not yet specified
  pre
    card 登録済みユーザ集合 < 定員
    and exists ユーザ in set 引数ユーザ集合 & ユーザ not in set 登録済みユーザ集合
  post
    登録済みユーザ集合 = 登録済みユーザ集合 ~ union {RESULT}
    and RESULT in set 引数ユーザ集合 and RESULT not in set 登録済みユーザ集合~;
```

自然言語による
仕様書や設計書

フィードバック
置き換えてしまった事例も

上流との
整合性確認も

様々な検査

- テスト
- 証明など
強力な検査
- 具体例生成による
妥当性確認なども

```
class イベント参加登録管理システム
  登録済みユーザ集合 : set of 「ユーザ識別子」;
  定員 : nat!;
  inv card 登録済みユーザ集合 <= 定員

  抽選登録する : set of 「ユーザ識別子」 ==> 「ユーザ識別子」
  抽選登録する (引数ユーザ集合) == is not yet specified
  pre
    card 登録済みユーザ集合 < 定員
    and exists ユーザ in set 引数ユーザ集合 & ユーザ not in set 登録済みユーザ集合
  post
    登録済みユーザ集合 = 登録済みユーザ集合 ~ union {RESULT}
    and RESULT in set 引数ユーザ集合 and RESULT not in set 登録済みユーザ集合~;
```



技術の利用イメージ：有名な産業界事例

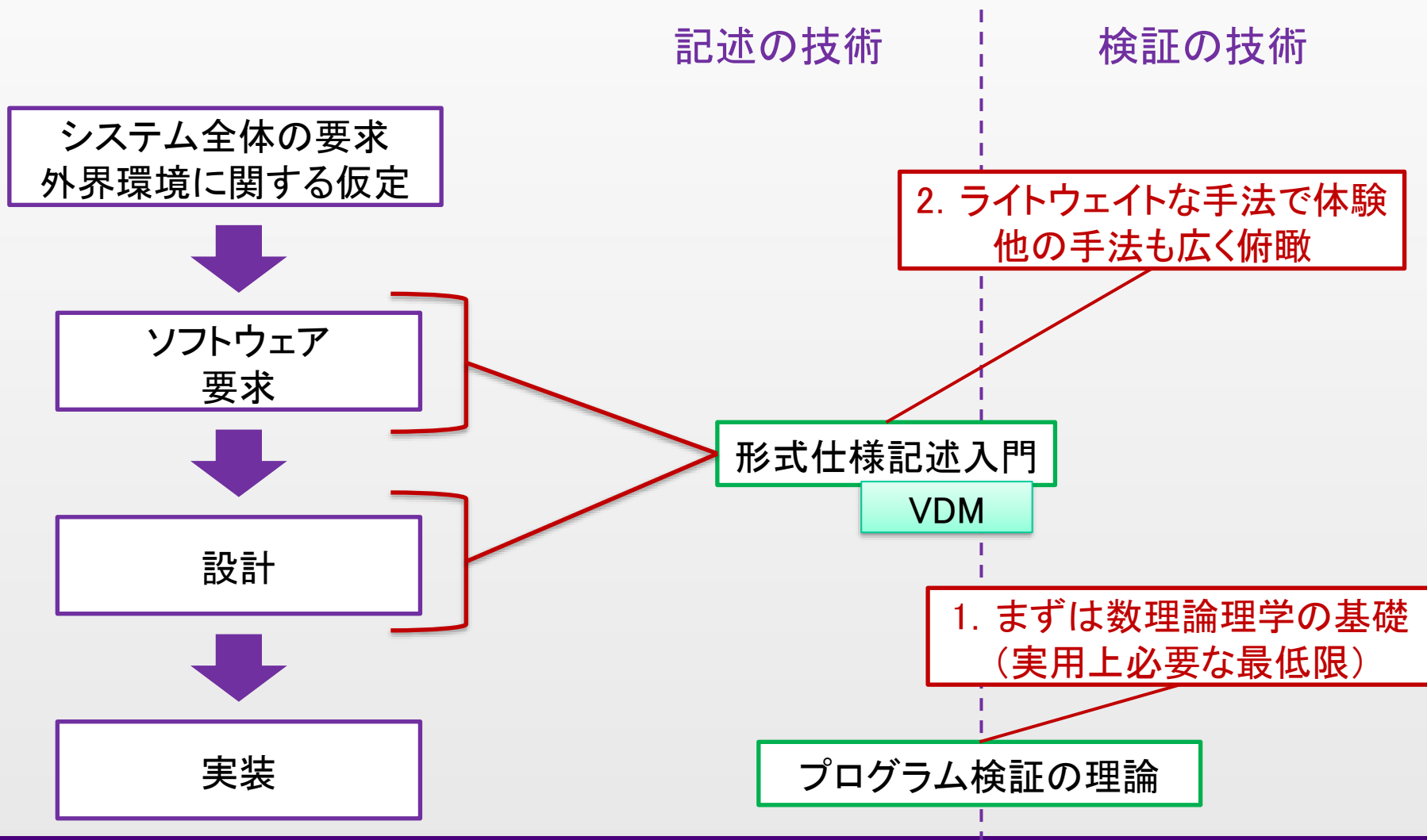
- FeliCaチップ：外部仕様を厳密に記述，テスト
 - 多数の実装者や外部パートナーが活用する対象
 - 後工程で検出された不具合のうち，
記述の問題に起因するものはゼロに
- パリ地下鉄や空港シャトル，世界各国に展開：
正しさが保証されたコードを仕様から導出
 - 重要な部品について，数学的証明を通して
仕様遵守が保証された形で段階的に詳細化
 - 高信頼プロセス：仕様の議論・定義に大半の工数，
「正しさを維持し実装へ」，単体テストは不要



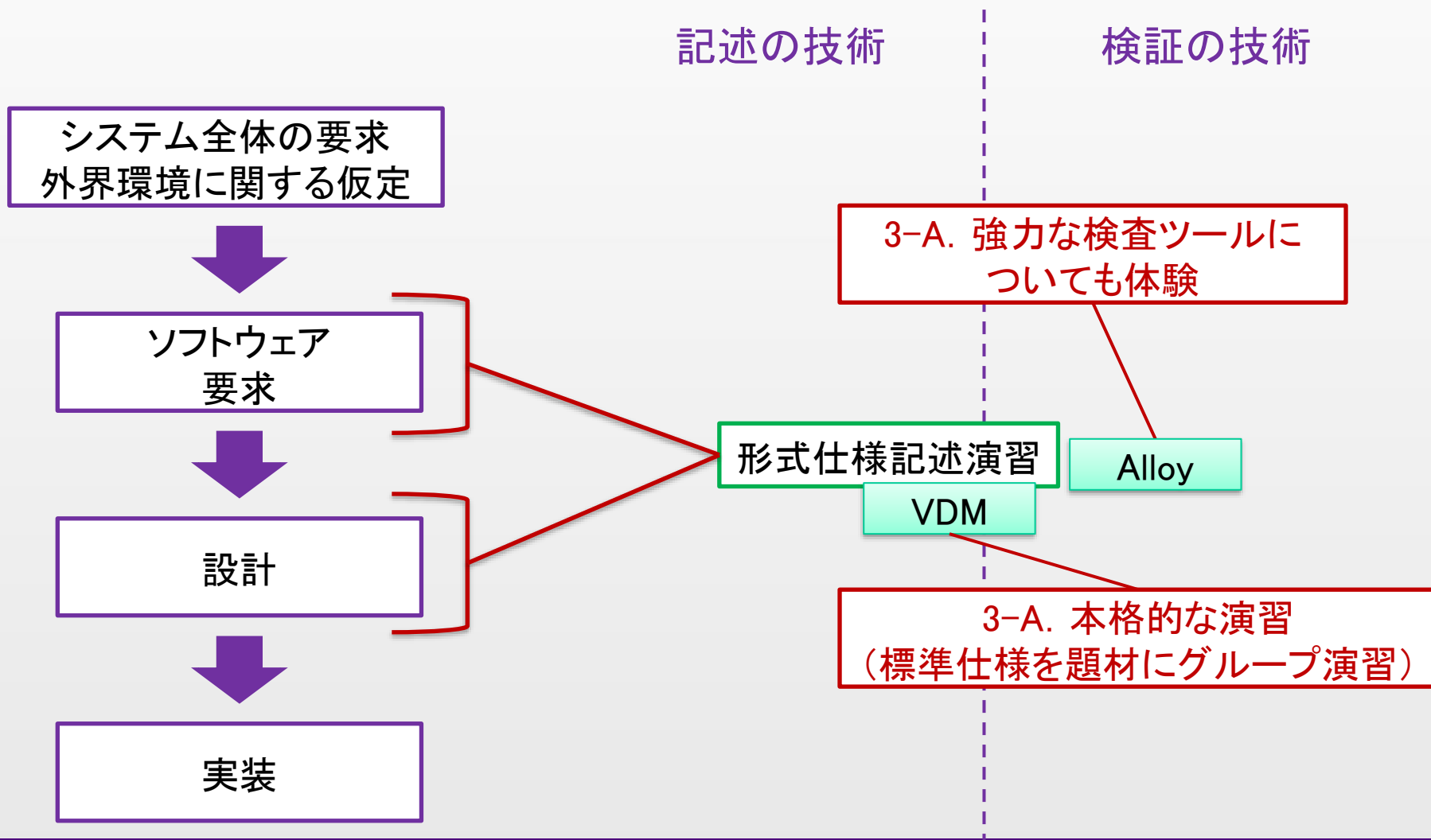
受講生のこれまでの試み

- トップエスイーでのこれまでの演習・制作
 - ビジネスプロセス, チップ処理ワークフロー, クラウドストレージ管理, アクセス制御, など多様な領域での試行
 - 海外外注先への仕様書記述(日本語問題回避)
 - 仕様書・設計書に関する定形化・機械処理(テスト仕様導出の自動化など)
- 最近の実践演習
 - 自社システムを想定したケーススタディ
 - 鉄道運賃やTDLファストパスの仕様記述

講義構成・扱う技術（１）

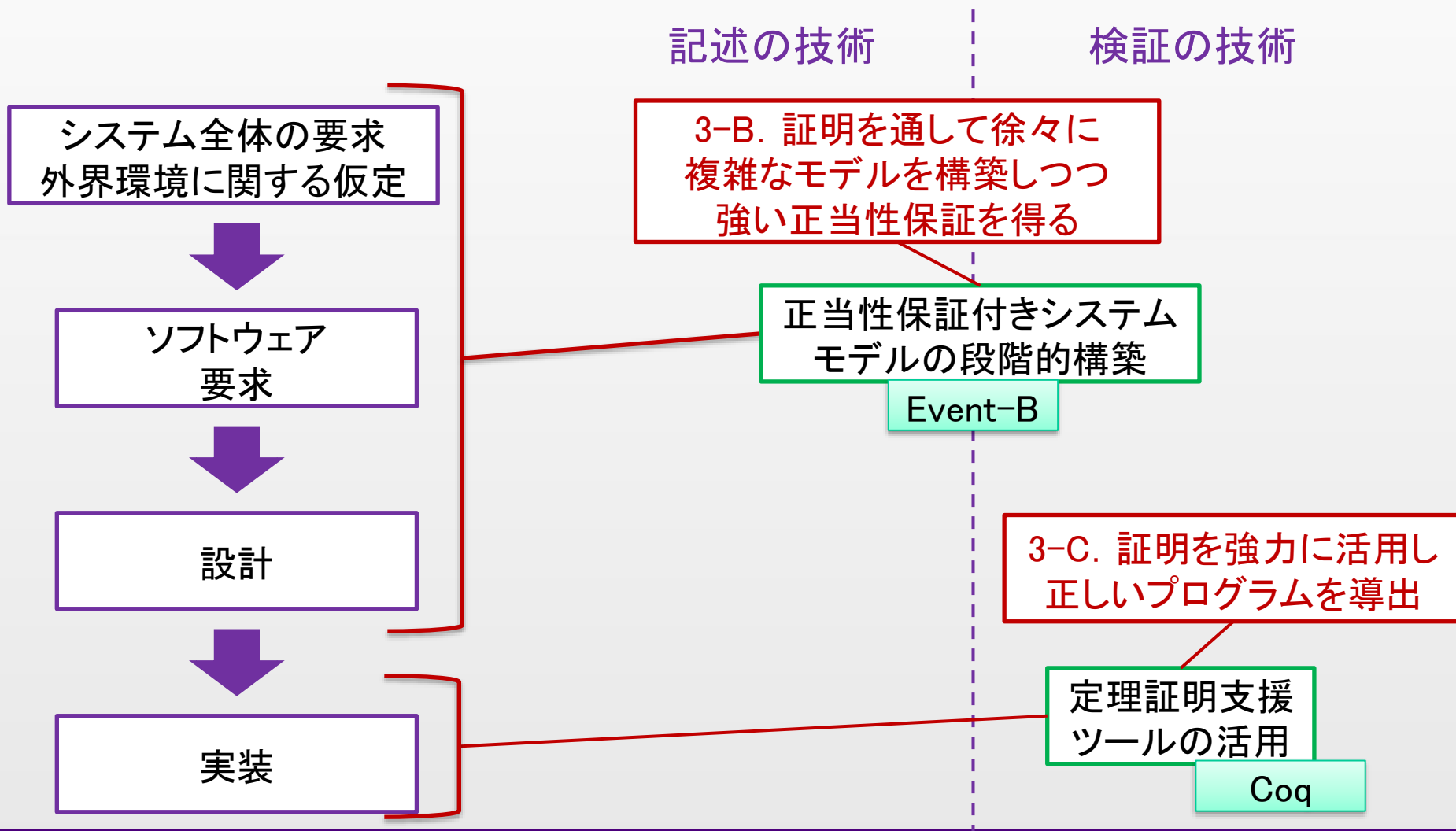


講義構成・扱う技術（２）



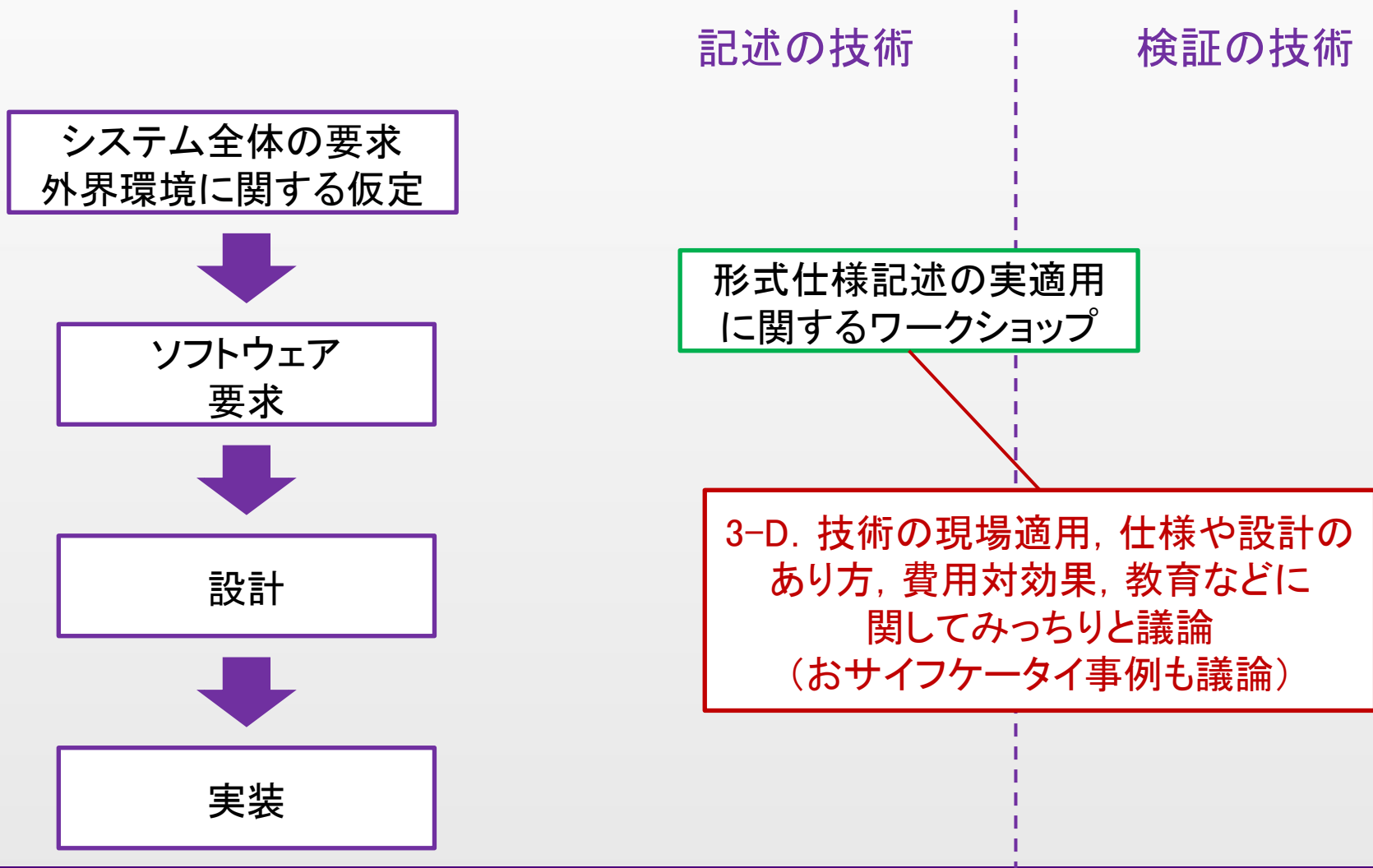


講義構成・扱う技術（3）





講義構成・扱う技術（４）





講義の履修方針に関するまとめ

■ まずは入門

1. プログラム検証の理論
2. 形式仕様記述入門

「飛ばして後ろだけ」も
できなくはないが推奨

■ 2では演習が足りないかも

2の続きなので2が必須

- 3-A. 形式仕様記述演習

■ より強力な検証アプローチに踏み込む 1, 2を理解した上での発展

- 3-B. 正当性保証付きシステムモデルの段階的構築
- 3-C. 定理証明支援ツールの活用

■ 議論

- 3-D. 形式仕様記述の実適用に関するワークショップ

自由議論なのでここだけ単独も可だが、2以降の経験があると議論が深まる



形式仕様記述シリーズ

- (機能)仕様における下記アプローチを習得
 - 抽象モデル化と“What”の厳密な記述
 - 正しさの検証・保証
- 「形式仕様記述」という技術活用への第一歩
- 様々な課題に対して幅広く生きる原則・基盤
 - モデルの抽象度制御(WhatとHowの分離)
 - あいまいさへの対処
 - 正しさの定義や種類, 様々な検証アプローチ