FeliCa

SEA Forum : 形式仕様記述手法の実践に関わる連続セミナー(2)

システム開発への
形式手法の適用による品質の確保

仕様の可読性向上と
形式仕様のテストへの活用を考える

2010年9月13日(月) ソニー株式会社 中津川泰正　栗田太郎

Copyright 2010 Sony Corporation.

アジェンダ

FeliCa

- 形式仕様記述手法適用の効果
  - 仕様の品質と伝達力の向上に向けて
- 形式仕様記述手法の技術導入
  - 仕様記述を学んだ過程
- 仕様記述と検証の理想と現実
  - 初めての仕様記述とその課題
- 開発現場における課題への取り組み
  - 仕様の読みやすさと仕様の動作の両立
  - 形式仕様を用いたプログラムの仕様準拠テスト
- まとめ

Copyright 2010 Sony Corporation.

仕様記述を学んだ過程

形式仕様記述手法の技術導入

Copyright 2010 Sony Corporation.

学びのリスト (形式仕様記述手法をとおして)

FeliCa

- ドメインエンジニアリング
  - フレームワーク設計
  - ライブラリ設計
  - データ構造設計

- オブジェクト指向分析
- 関数型プログラミング

- データ構造と アルゴリズム
- 論理学
  - 命題論理
  - 述語論理
  - 時相論理

集合・写像

- VDMTools の使い方
- LTSA ツールの使い方
- テスト技法

- 信頼性を高める
  - 契約による設計

- VDM 言語仕様
- FSP 言語仕様
- UML

- 仕様の構造
  - 事前条件
  - 事後条件
  - 不変条件

Copyright 2010 Sony Corporation.

論理学

FeliCa

- **命題論理**

  not 否定 (ではない)

  and 連言 (かつ)

  or 選現 (または)

  => 含意 (ならば)

  <=> 同等

  = 相当 (等しい)

  <> 不等 (等しくない)

- **述語論理**

  forall 全称限量子

  全ての ～について

  ～ が成り立つ

  exist, exist1 存在限量子

  ～の条件を満たす

  ～ が存在する

- **時相論理**

  until

  release

  next, finally, globally,

  all, exists

Copyright 2010 Sony Corporation.

仕様の構造 {P} A {Q} (Floyd-Hoare Triple)

FeliCa

- P : 事前条件
  - 処理 A の実行前に満足すべき条件
- Q : 事後条件
  - 処理 A の実行後に満足すべき条件
- 正しさの基準として事前条件・事後条件
  - 処理 A のみから正しさを判断することはできない

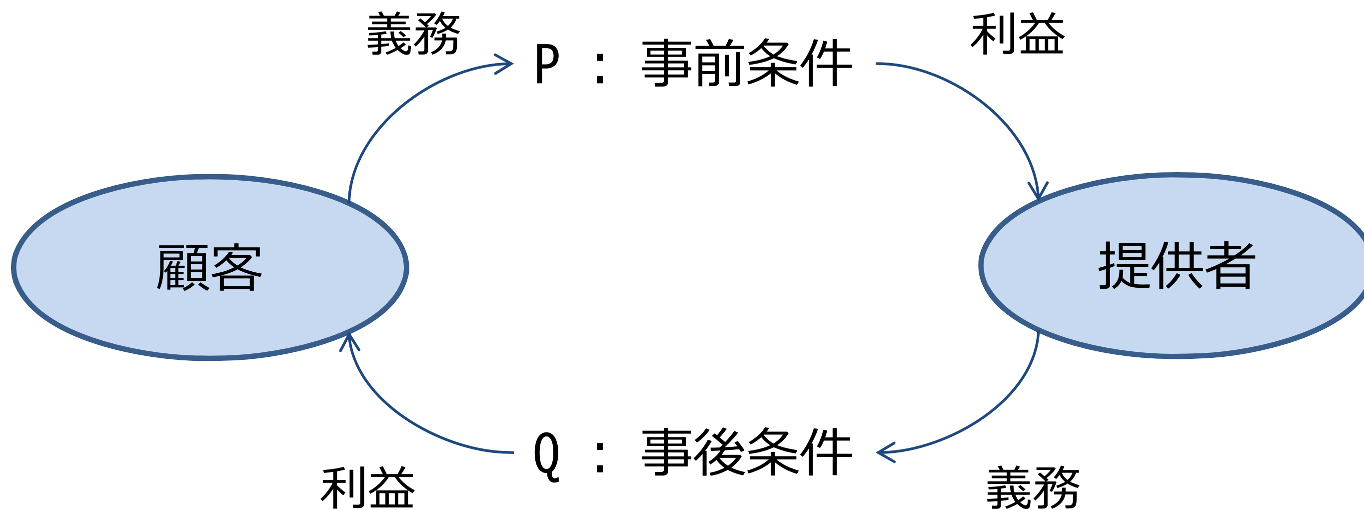
```
public 最大値を取り出す: set of nat -> nat
最大値を取り出す(正数集合) ==
  Impl_最大値取得(正数集合)
pre
  正数集合 <> {}  -- 事前条件
post
  RESUTL in set 正数集合 and
  forall n in set 正数集合 & n <= RESULT;  -- 事後条件
```


Copyright 2010 Sony Corporation.

契約による設計 (design by contract)

FeliCa

- {P} A {Q} をサービスの提供者と顧客の間で取り交わされる契約というメタファで表現した



サービス提供者が顧客に対して：
「もしそちらが P を満たした状態で A を呼ぶと約束して下さるならば、お返しに、Q を満たす状態を実現することをお約束します。」

Copyright 2010 Sony Corporation.

VDM++ 言語としての機能

FeliCa

- 仕様記述機能
  - 述語論理
  - 不変条件、事後条件、事前条件、陰仕様記述
  - 並行動作、同期制御
  - 集合、列、写像、レコード、型変数
- 関数型プログラミング言語機能
  - パターン、内包
  - 関数、ラムダ式、高階関数
- オブジェクト指向プログラミング言語機能
  - クラス、インスタンス、継承、操作

Copyright 2010 Sony Corporation.

VDM++ 言語仕様 クラスの構成

FeliCa

```
class クラス名 is subclass of スーパークラス
   instance variables

   values
   types
   operations
   functions

   thread
   sync

end クラス名
```


Copyright 2010 Sony Corporation.

VDM++の関数定義

FeliCa

- 陰関数定義
- 陽関数定義
- 拡張陽関数定義

Copyright 2010 Sony Corporation.

VDMTools の機能

FeliCa

- 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

Copyright 2010 Sony Corporation.

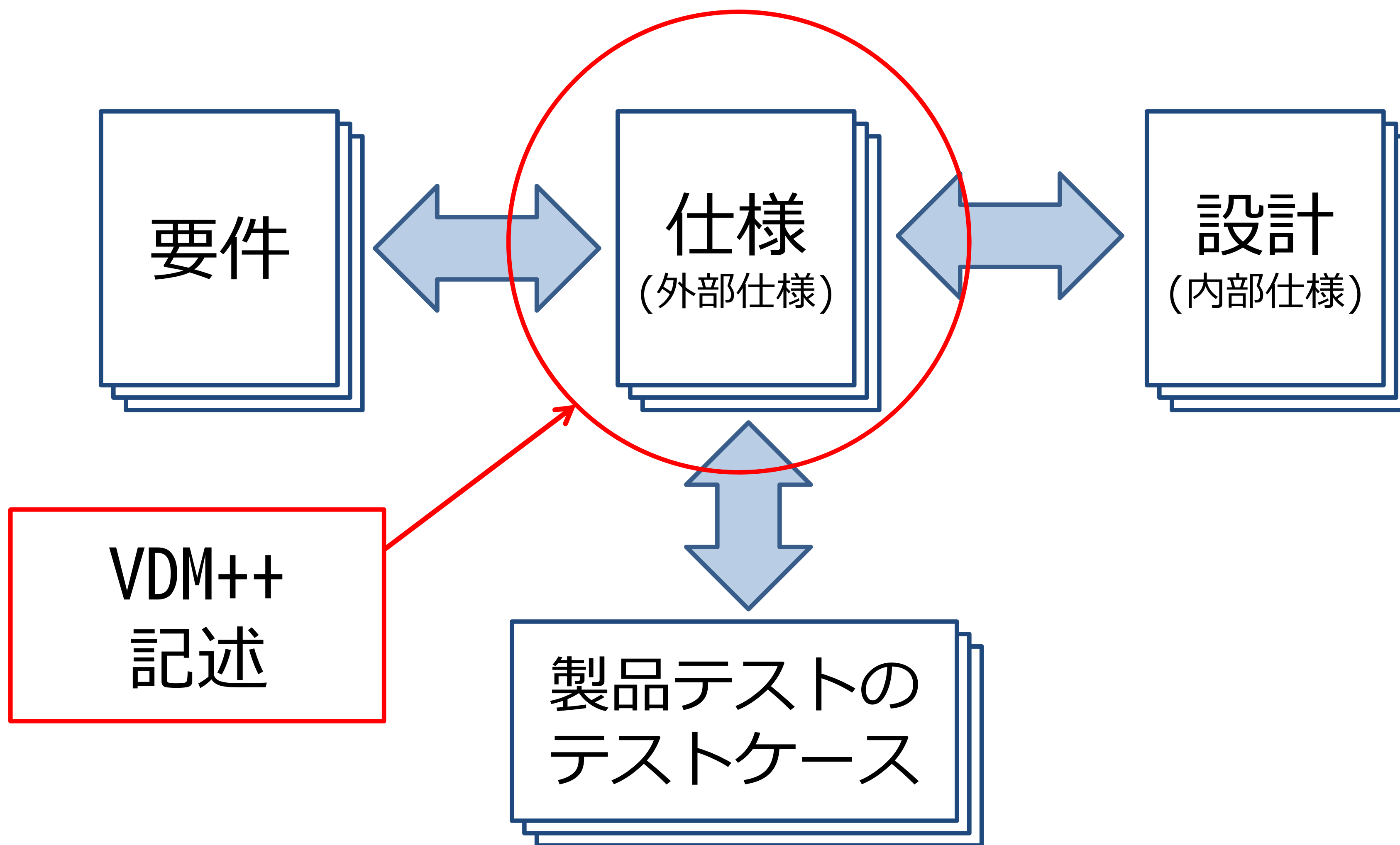
はじめての仕様記述とその課題

仕様記述と検証の理想と現実

Copyright 2010 Sony Corporation.

第1世代の VDM++ の適用範囲

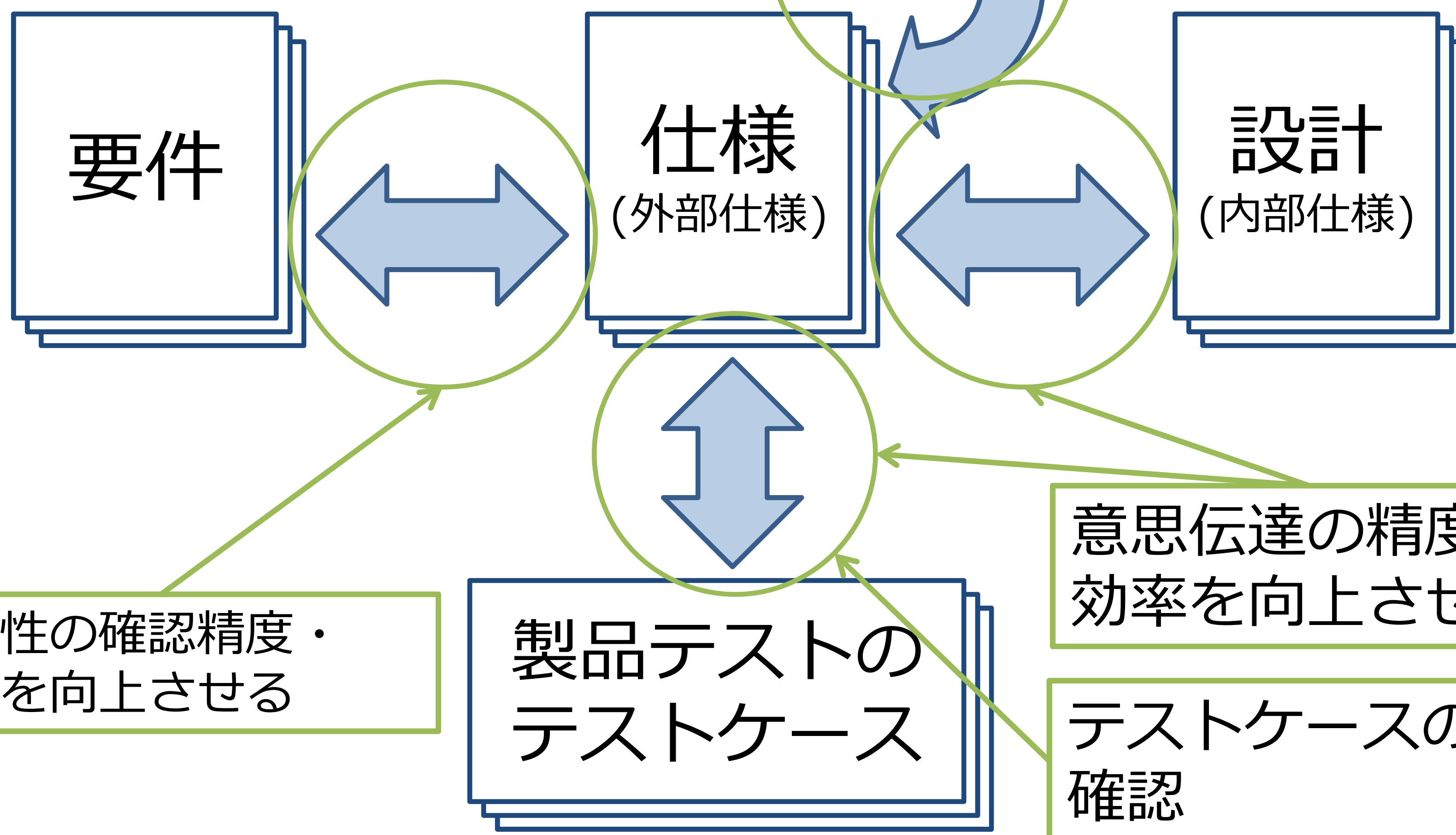
FeliCa



Copyright 2010 Sony Corporation.

品質確保の枠組み (仕様を中心に考えた場合)

FeliCa



Copyright 2010 Sony Corporation.

形式仕様記述の構成

FeliCa

テスティング
フレームワーク

構成

テンプレート

仕様記述
フレームワーク

アクティビティ

仕様記述のための
設計
モジュール分割など

ドメイン固有
ライブラリ

ドメイン固有
データ構造定義

汎用ライブラリ

Copyright 2010 Sony Corporation.

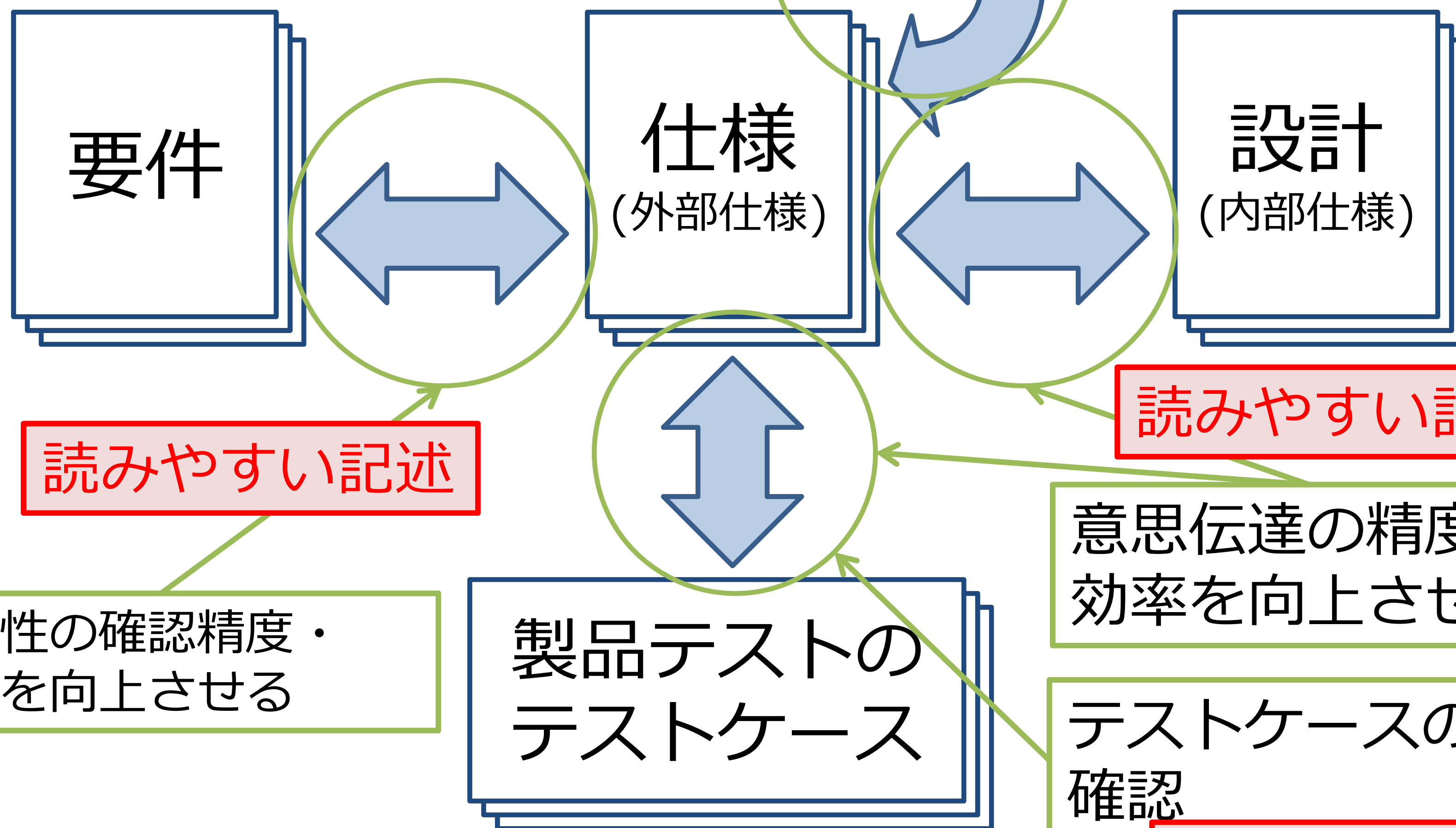
第1世代の課題と発展

FeliCa

- これまでのまとめ
  - 陽関数で仕様記述のフレームワークを構築
- 課題
  - 書いてあるが、読み取ってもらえなかった（17%）
    - 動かすための仕組みが読むための記述の可読性を阻害した
- 発展
  - テストに活用する

Copyright 2010 Sony Corporation.

品質確保の枠組み (仕様を中心に考えた場合)



Copyright 2010 Sony Corporation.

形式仕様記述の構成

FeliCa

発展：テストに活用する

構成

テスティング
フレームワーク

テンプレート

仕様記述
フレームワーク

ドメイン固有
ライブラリ

ドメイン固有
データ構造定義

汎用ライブラリ

アクティビティ

仕様記述のための
設計
モジュール分割など

テスト戦略
テスト設計

Copyright 2010 Sony Corporation.

読みやすさと仕様の動作の両立

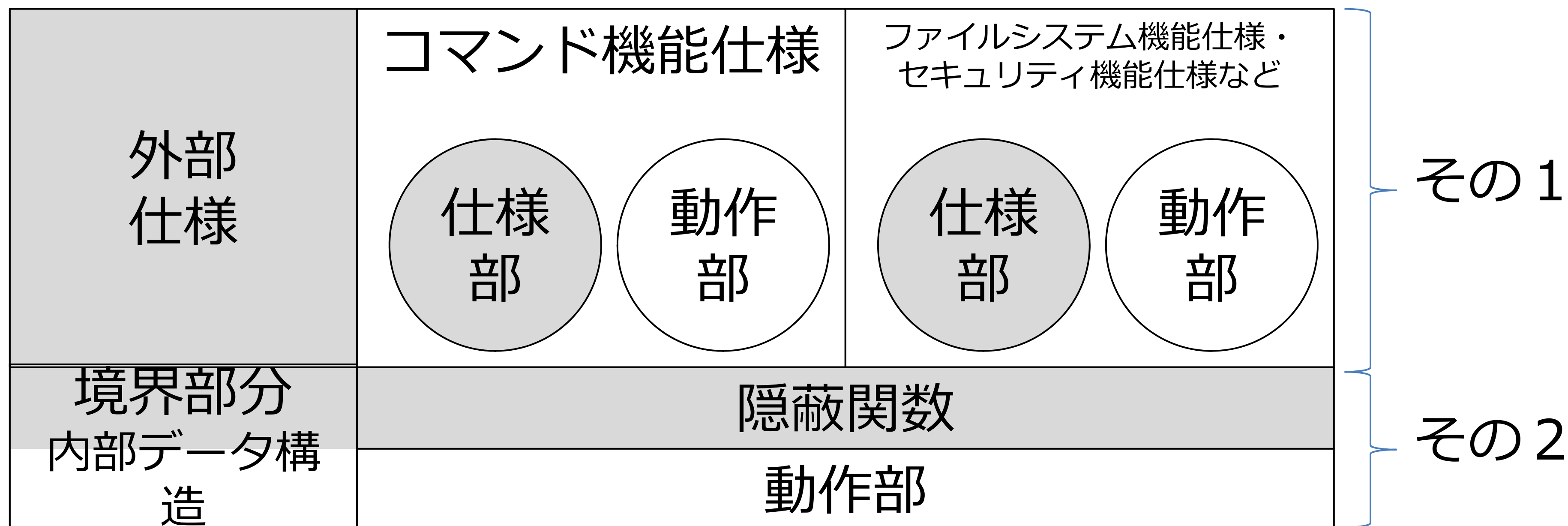
開発現場における課題への取り組み

Copyright 2010 Sony Corporation.

仕様記述フレームワークの概要

FeliCa

- 仕様部と動作部の分離



Copyright 2010 Sony Corporation.

（その1）拡張陽関数定義を選択

FeliCa

- 陰関数を使って宣言的に仕様を記述できる
- 陰関数の場合，テストケースごとに
入力と出力の内部データ構造を作成しなければならない。

  ⇒ テスト工数を考慮して拡張陽関数を選択
- 仕様部と動作部を記述場所により明確に
分離することができる
- 欠点
  – 仕様部と動作部の二箇所で同じような
記述をしなければならない？

Copyright 2010 Sony Corporation.

拡張陽関数定義を選択

コマンド機能モジュールの構成	実行行数	比率
共通部	7,680	67%
仕様伝達部	1,691	15%
仕様動作部	2,089	18%
合計	11,460	

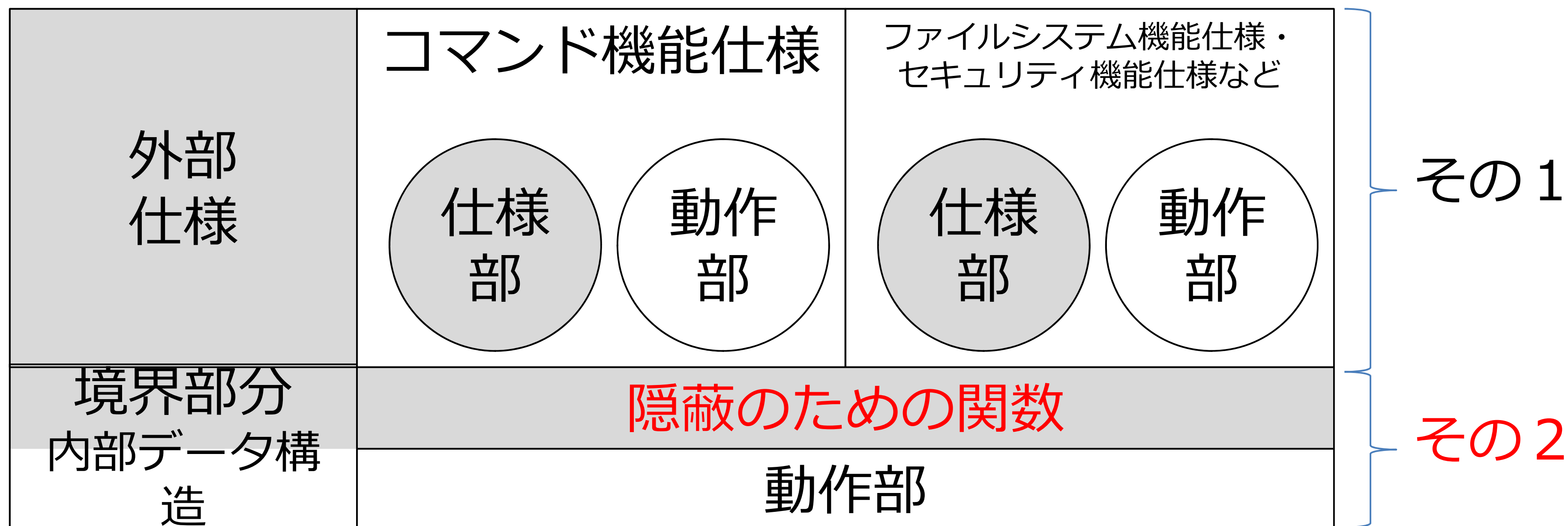
- 欠点
  - 仕様部と動作部の二箇所で同じような記述をしなければならない？

Copyright 2010 Sony Corporation.

仕様記述フレームワークの概要

FeliCa

- 仕様部と動作部の分離



Copyright 2010 Sony Corporation.

型を隠蔽しない場合の例

FeliCa

```
-- 仕様の型
public NAME = seq of char;
public ADDRESS = seq of char;
public CARD ::
    Name : NAME
    Address : ADDRESS;

-- BOOK 型を隠蔽しない場合
public BOOK = map NAME to CARD;
```

内部仕様もこのデータ構造に従う必要があるか？

Copyright 2010 Sony Corporation.

型を隠蔽しない場合の例

FeliCa

```
public 新規カード登録 : BOOK * CARD -> BOOK
  新規カード登録(bk, cd) ==
    bk munion {cd.Name |-> cd}
  pre cd.Name not in set dom bk
  post rng RESULT = rng bk union {cd};
```

仕様理解する上で、必要のない
型について理解しないといけないので
読みづらい

Copyright 2010 Sony Corporation.

型を隠蔽する場合の例

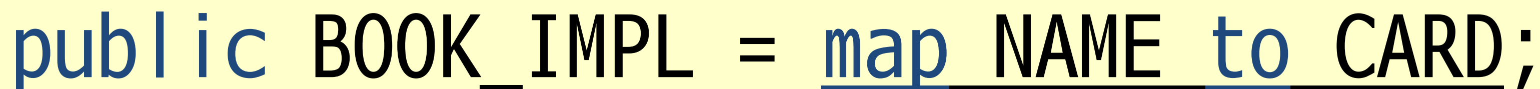
FeliCa

```
-- 仕様の型
public NAME = seq of char;
public ADDRESS = seq of char;
public CARD ::
    Name : NAME
    Address : ADDRESS;

-- 隠蔽対象の型
public BOOK = BOOK_IMPL;

-- 動作部の型
public BOOK_IMPL = map NAME to CARD;
```

この型定義を隠蔽する



Copyright 2010 Sony Corporation.

隠蔽のための関数による表現

FeliCa

```
public 新規カード登録 : BOOK * CARD -> BOOK
  新規カード登録(bk, cd) ==
    impl_新規カード登録(bk, cd)       -- 動作部
  pre cd.Name not in set 名前集合(bk)
  post カード集合(RESULT) = カード集合(bk)
  union {cd};
```

読みやすい

Copyright 2010 Sony Corporation.

隠蔽のための関数の例

FeliCa

```
-- 「隠蔽対象の型」BOOK型 の「隠蔽関数」
public カード集合 : BOOK -> set of CARD
  カード集合(bk) ==
    rng bk;
public 名前集合 : BOOK -> set of NAME
  名前集合(bk) ==
    dom bk;
```


Copyright 2010 Sony Corporation.

形式仕様を用いた
　　プログラムの仕様準拠テスト

開発現場における課題への取り組み

Copyright 2010 Sony Corporation.

概要

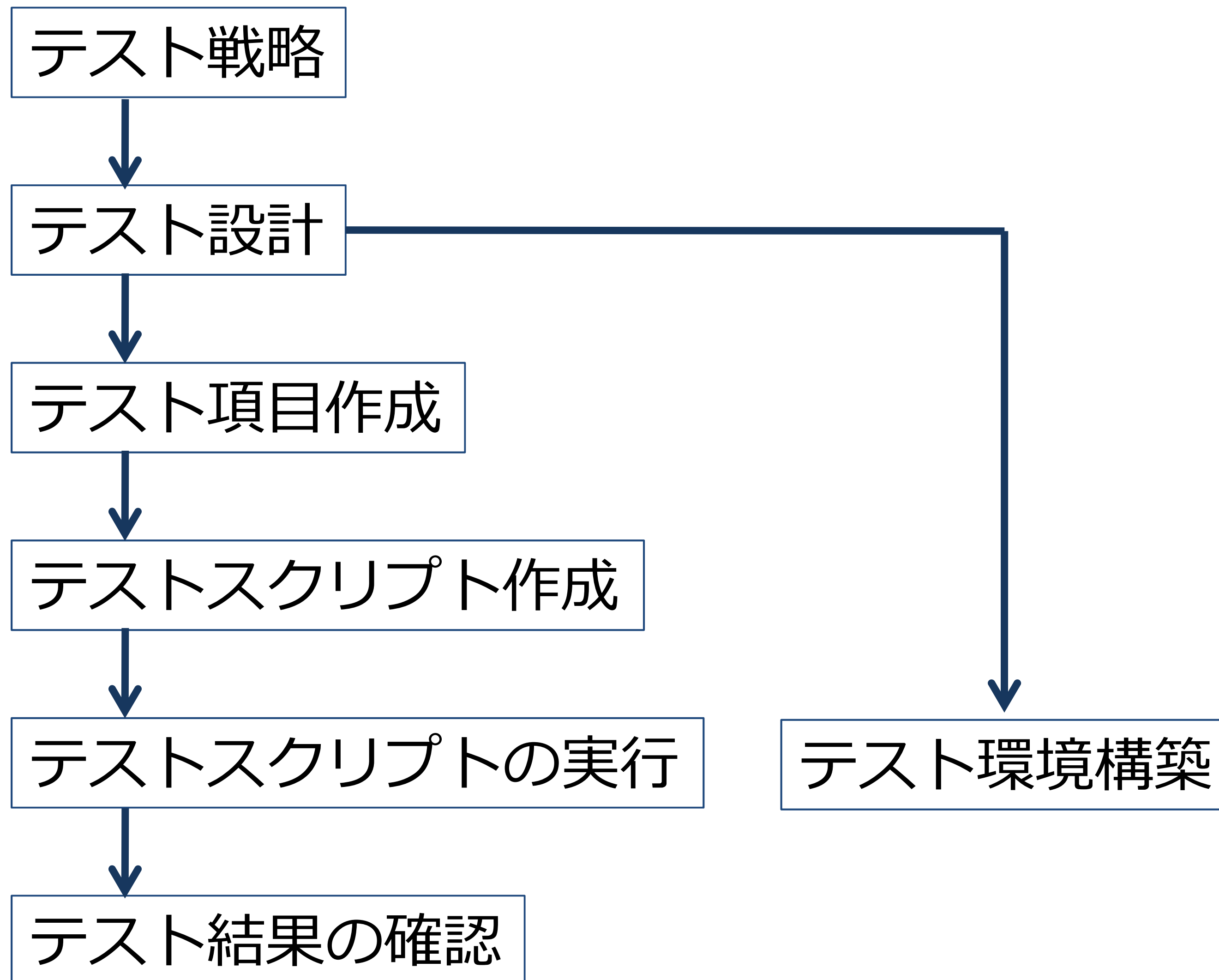
FeliCa

- ディシジョンテーブルの活用
- テストオラクルとして活用する

Copyright 2010 Sony Corporation.

テストの流れ

FeliCa



Copyright 2010 Sony Corporation.

ディシジョンテーブルの活用

FeliCa

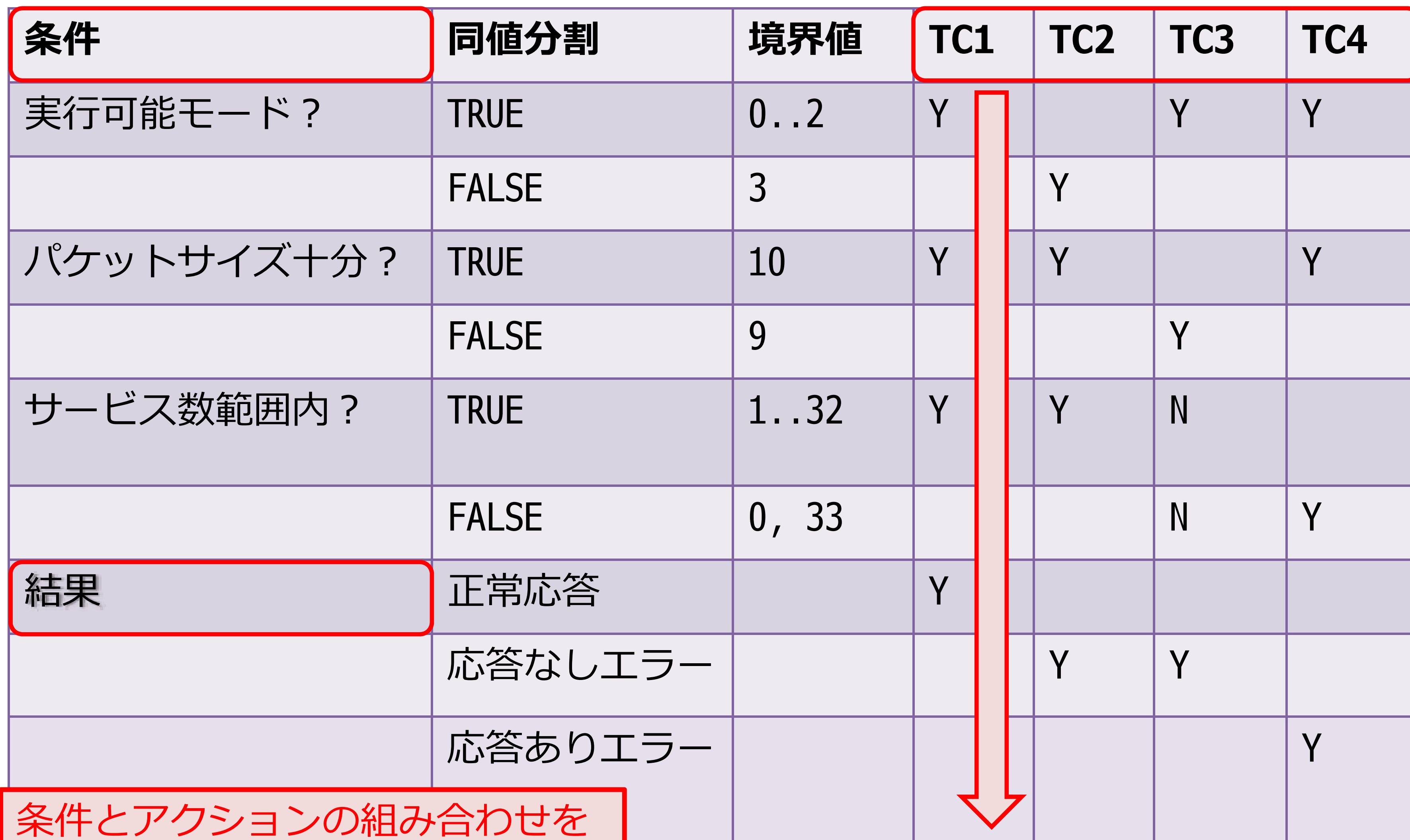
- テスト戦略を立てる（私たちの場合）
  - 条件分岐カバレッジを 100% にする
  - 同値分割と境界値分析を用いて、各同値の境界値が少なくとも一度はテストされるようにする

  ※ 他の観点のテストもあります
- 仕様記述とディシジョンテーブルの関係
  - 仕様記述の構造をそのまま、ディシジョンテーブルに対応させる
- 期待する効果
  - テスト項目の作成とレビューを容易にする

Copyright 2010 Sony Corporation.

ディシジョンテーブルの例

FeliCa



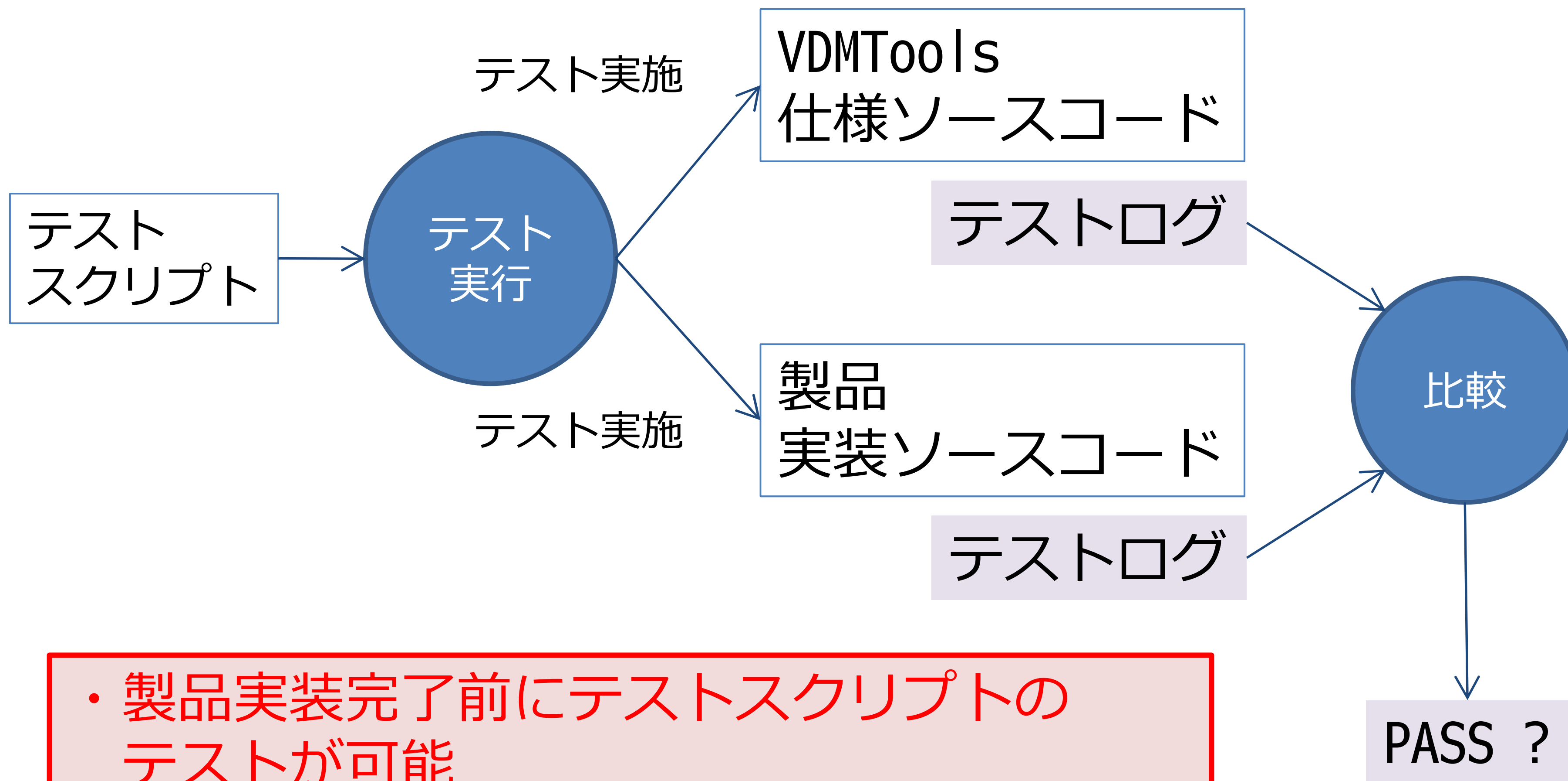
条件	同値分割	境界値	TC1	TC2	TC3	TC4
実行可能モード？	TRUE	0..2	Y		Y	Y
	FALSE	3		Y		
パケットサイズ十分？	TRUE	10	Y	Y		Y
	FALSE	9			Y	
サービス数範囲内？	TRUE	1..32	Y	Y	N	
	FALSE	0, 33			N	Y
結果	正常応答		Y			
	応答なしエラー			Y	Y	
	応答ありエラー					Y

条件とアクションの組み合わせを
テーブルで表現したもの

2010 Sony Corporation.

テストオラクルとして活用

FeliCa



- 製品実装完了前にテストスクリプトのテストが可能
- より広い範囲の期待値のチェックが可能(変わっていないことのチェックなど)

Copyright 2010 Sony Corporation.

まとめ

Copyright 2010 Sony Corporation.

まとめ (1/4)

FeliCa

- 形式仕様記述手法の技術導入
  - 仕様記述を学んだ過程

詳細な知識がなくてもはじめることができる

適用しながら学べる

Copyright 2010 Sony Corporation.

まとめ (2/4)

FeliCa

- 仕様記述と検証の理想と現実
  – 初めての仕様記述とその課題

読みやすさが第1世代の課題

動作部と仕様部を分離して仕様部を明確にした
- 拡張陽関数定義の利用
- データ構造を隠蔽する関数の利用

Copyright 2010 Sony Corporation.

まとめ (3/4)

FeliCa

- 開発現場における課題への取り組み
  - 形式仕様を用いたプログラムの仕様準拠テスト

ディシジョンテーブルの利用
- 仕様記述とディシジョンテーブルを対応づける
- テスト項目の作成とレビューを容易にする

テストオラクルとしての活用
- テストスクリプトのテストができる
- より広い範囲の期待値のチェックができる

Copyright 2010 Sony Corporation.

まとめ（4/4）

FeliCa

- 上流工程から下流工程において、品質について具体的な議論ができる
- 管理的側面・技術的側面・人間的側面において、様々な手法と連携して取り組むことが大切
  - 要件管理
  - プロジェクト管理
  - テスト技法
  - 設計技法
  - チームビルディング

Copyright 2010 Sony Corporation.