FOTによるモデルベーステストと品質コントロール
～自動車産業に向けた産総研の取り組み～

第1回セキュアシステムシンポジウム
2012年9月10日　みらいCANホール

北村崇師
システムライフサイクル研究グループ
セキュアシステム研究部門
（独）産業技術総合研究所

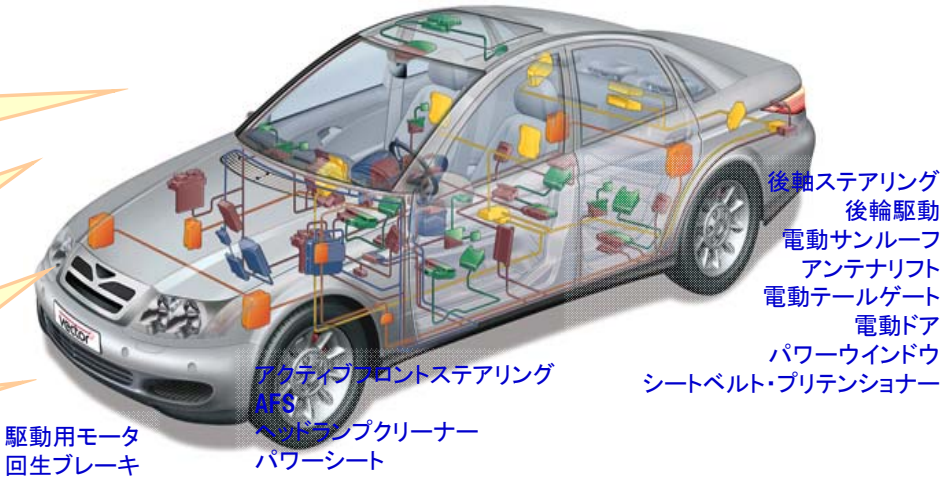
セキュアシステム研究部門

- セキュアサービス研究グループ
- 制御システムセキュリティ研究グループ
- **システムライフサイクル研究グループ**
  - メンバー
    - グループ長：大崎人士
    - 常勤・招聘研究員6名、ポスドク2名、他テクニカルスタッフ
  - 拠点：尼崎（兵庫県）、関西センター
  - 活動内容：
    - システム検証、ソフトウェア工学
    - 信頼性や安全性（Safety）を中心に
    - 適用領域：自動車、鉄道、施設インフラ、医療機器、他
- 高信頼ソフトウェア研究グループ
- 次世代セキュリティ研究グループ

自動車とソフトウェア

自動車の電子化・高機能化・スマート化に伴う、急速に進む車載ソフトウェアの複雑化・大規模化

- 電子関連部品の自動車総開発費に占める比率は約50%（2005時点）
- 50 以上の車載電子制御ユニット（ECU）
- ネットワーク接続による複数ECUの協調制御
- 数百万行のコード



ソフトウェア危機
ハードウェア技術の進歩と IT 化に伴い、品質・費用・時間等の面で、市場の需要を満たすソフトウェアを供給できない状況

課題1:ISO26262 への対応

ISO26262：自動車機能安全規格

- 2011年11月に正式発行
- 欧州では2013年にも関連の法規制が導入

安全性の規格
- 電気、電子、プログラマブル電子:IEC61508
- 飛行機:DO-178
- 医療機器:IEC 62304

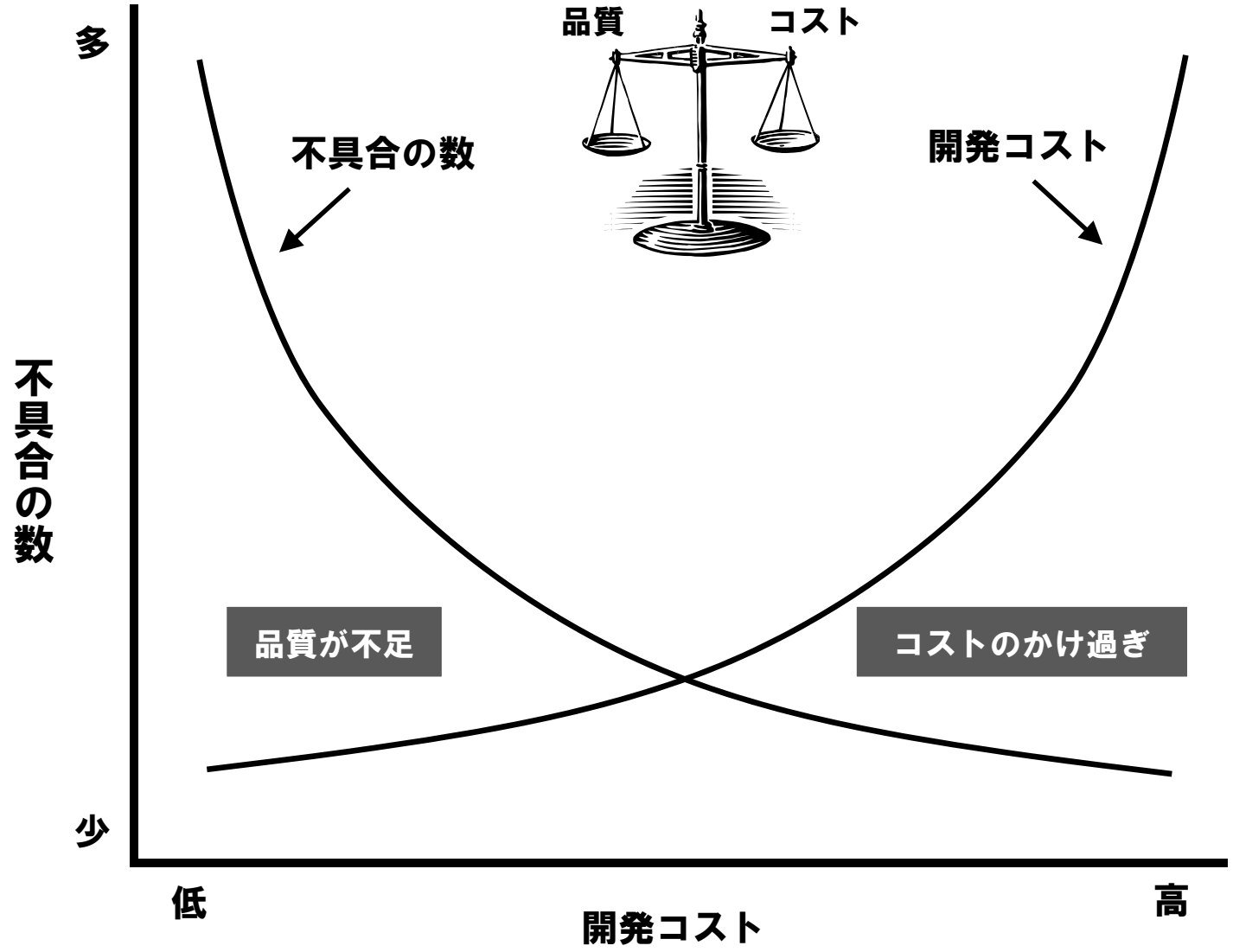
安全・信頼性に関する考え方の変化

自社の基準、努力
- 信頼関係に依拠する開発

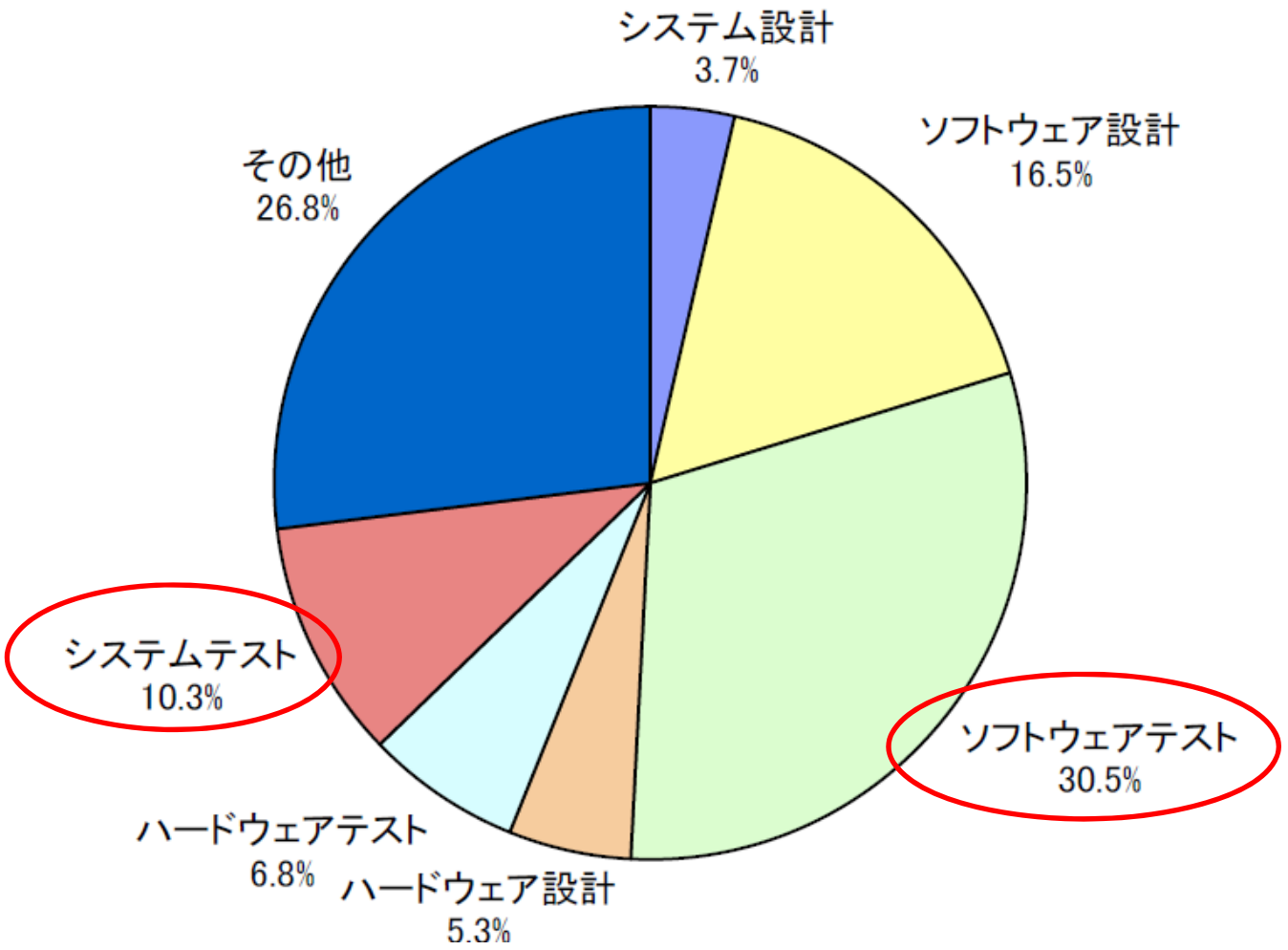
→

第三者による評価
- 開発エビデンスが必要
- 「エビデンス指向開発」

課題2：品質とコストの両立



システム検証が大きな工数を占める

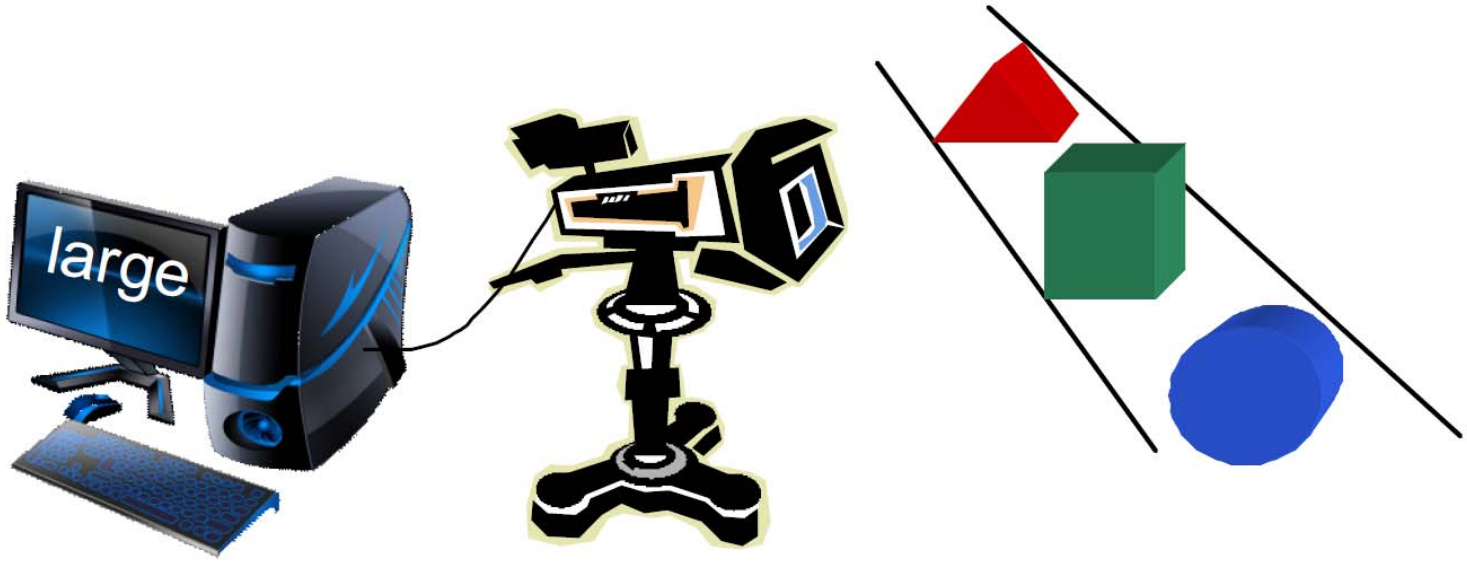


組込みシステム開発における工程ごとの工数比率

2008年版組込みソフトウェア産業実態調査報告書(プロジェクト責任者向け調査)(METI)

フィーチャ指向テスト
Feature Oriented Testing（FOT）

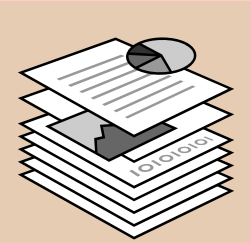
例：様々なブロックのサイズを認識するコンピュータビジョンシステムのテストケース設計



ブラックボックステストとホワイトボックステスト

ブラックボックステスト（BBT）

- 仕様に基づきテストケースを作成
- 例：同値類分割、境界値分析、組合せテスト
- 実装が要件を満たすかを検査

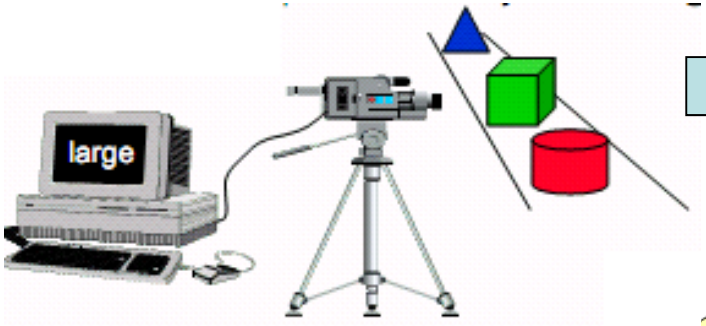


システム仕様

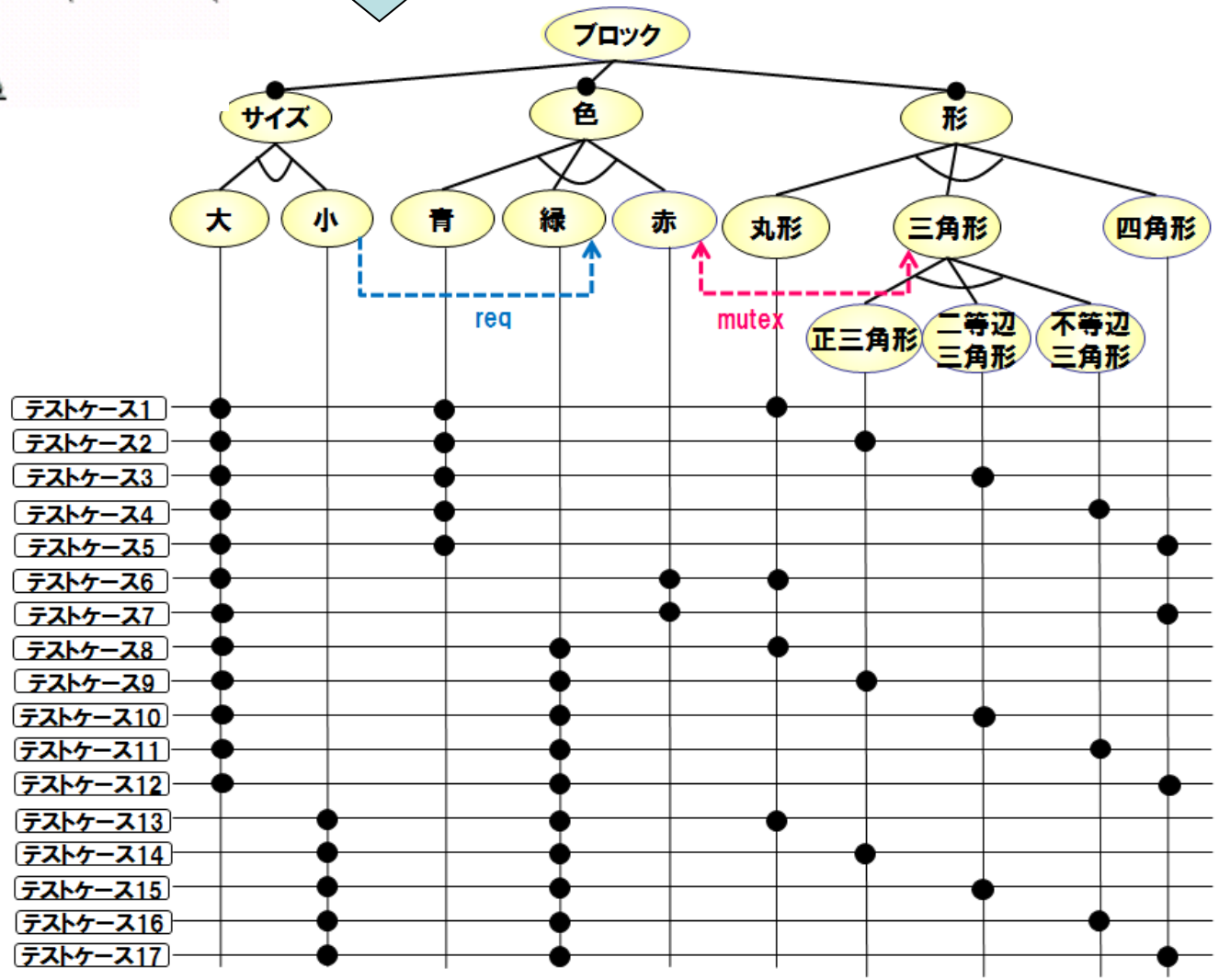
プログラム

ホワイトボックステスト（WBT）

- プログラム構造に基づきテストケースを作成
- 例：命令網羅（C0），分岐網羅率（C1），条件網羅（C2）



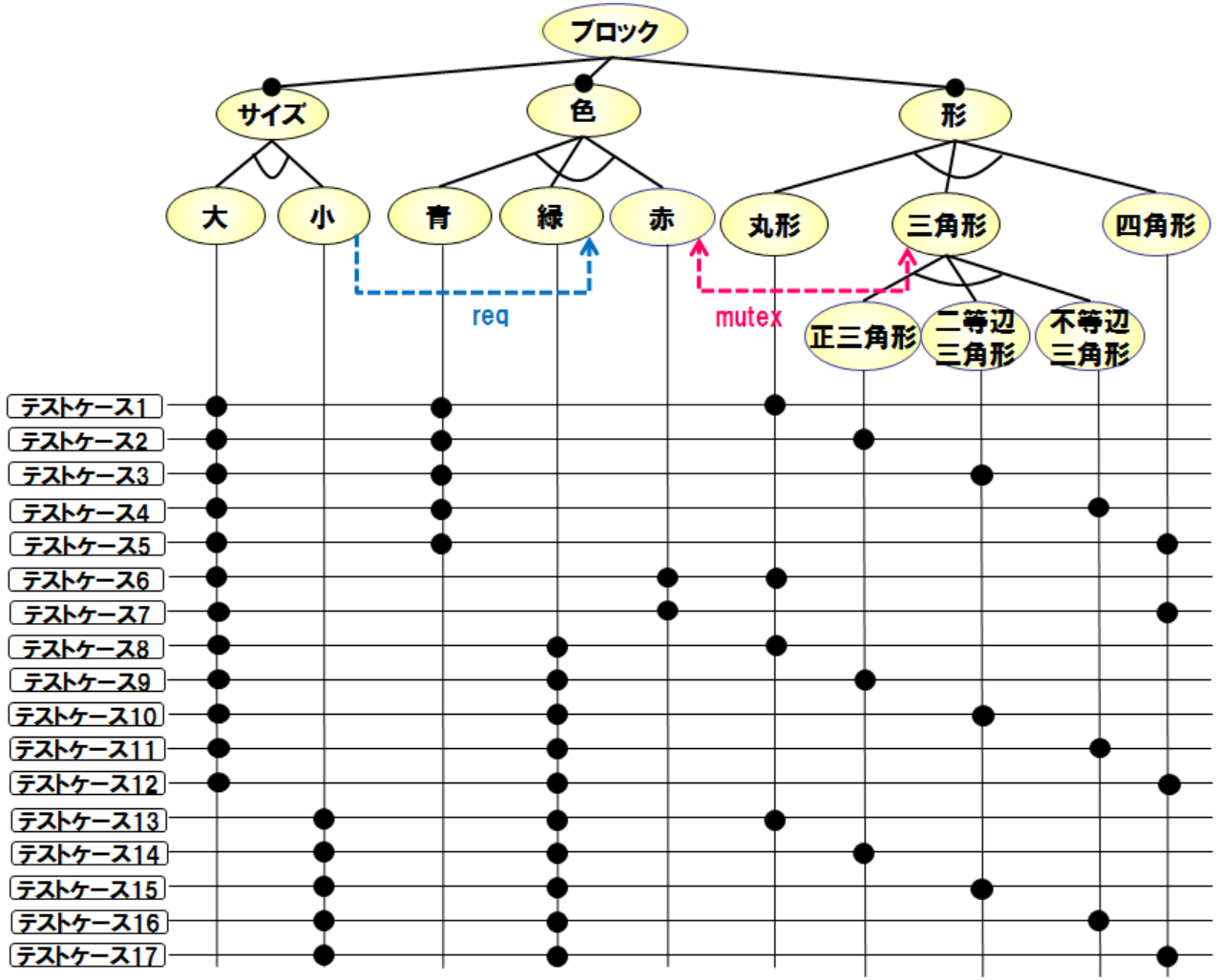
システムの入力領域をAnd-or 木を用いてトップダウンに分析、テストケース設計



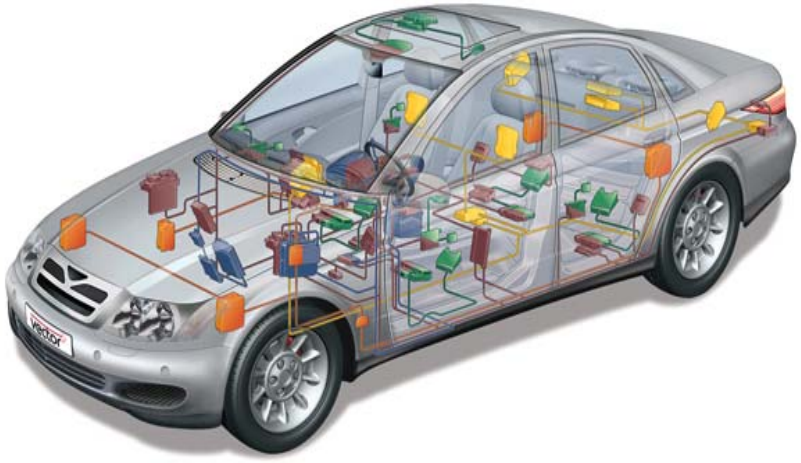
以下の仕様を反映

1. 赤色で三角形のブロックはない
2. 小さいサイズのブロックは緑色である

フィーチャダイアグラム＝
And-or 木 + 木横断的制約

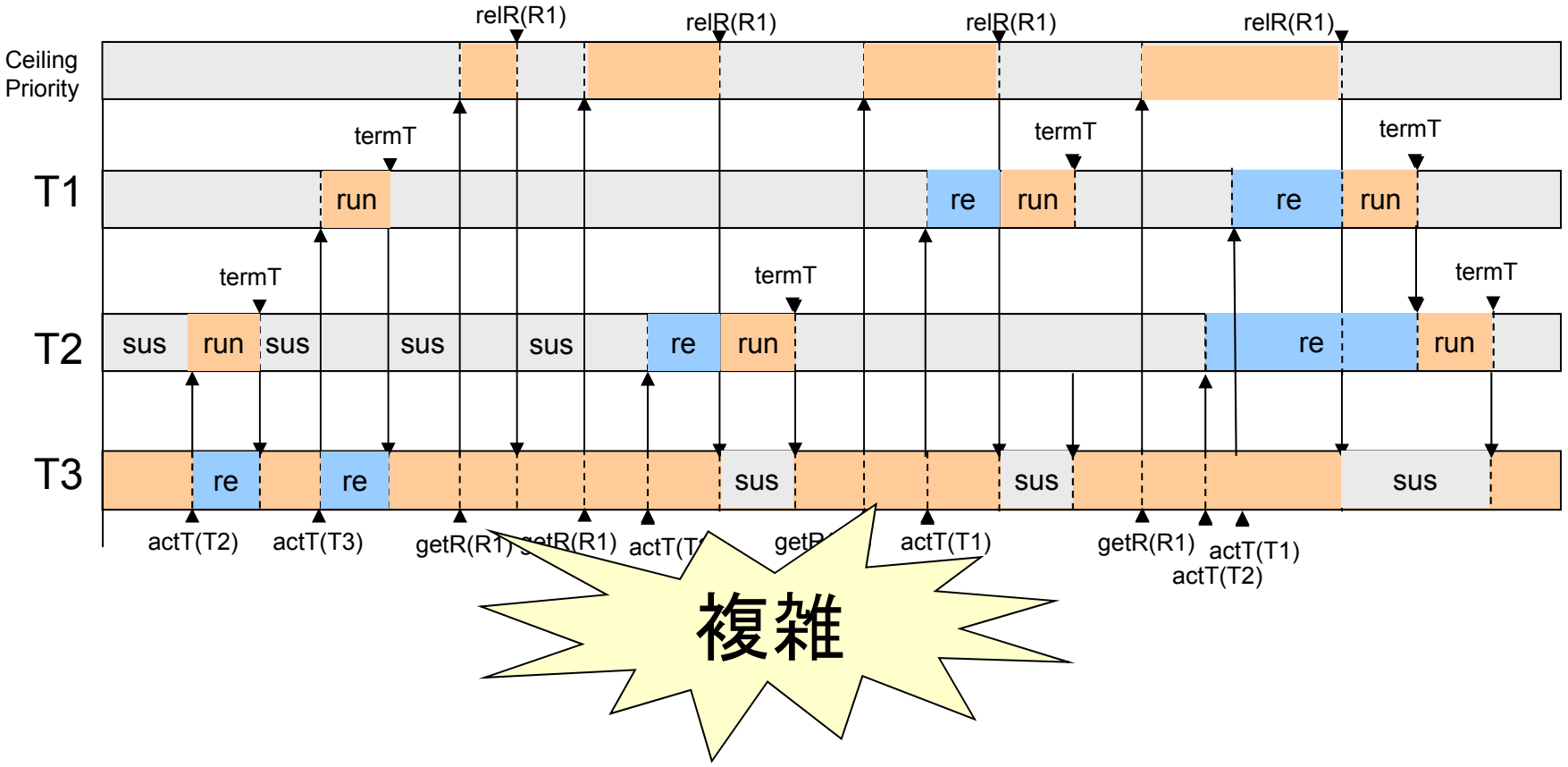


OSEK/VDX-OS への適用



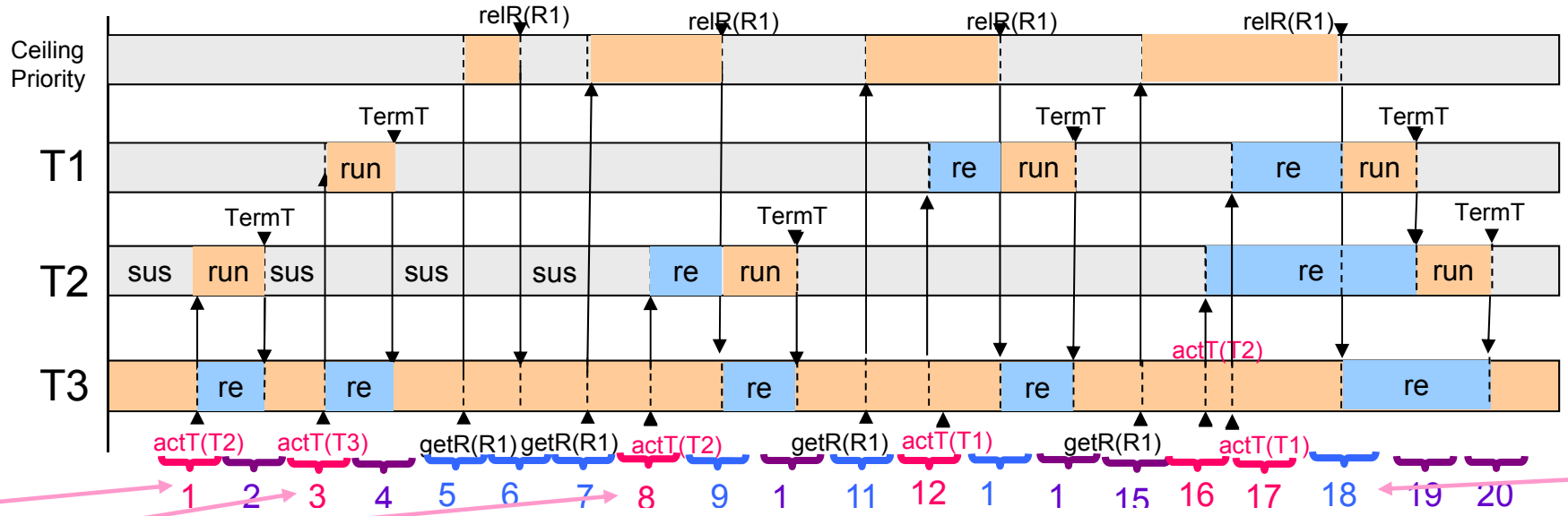
OSEK-OS のテストケース例

OSEK-OS:優先度上限プロトコル



テスト技術者から聞き取り調査

実際のテストケースの観点



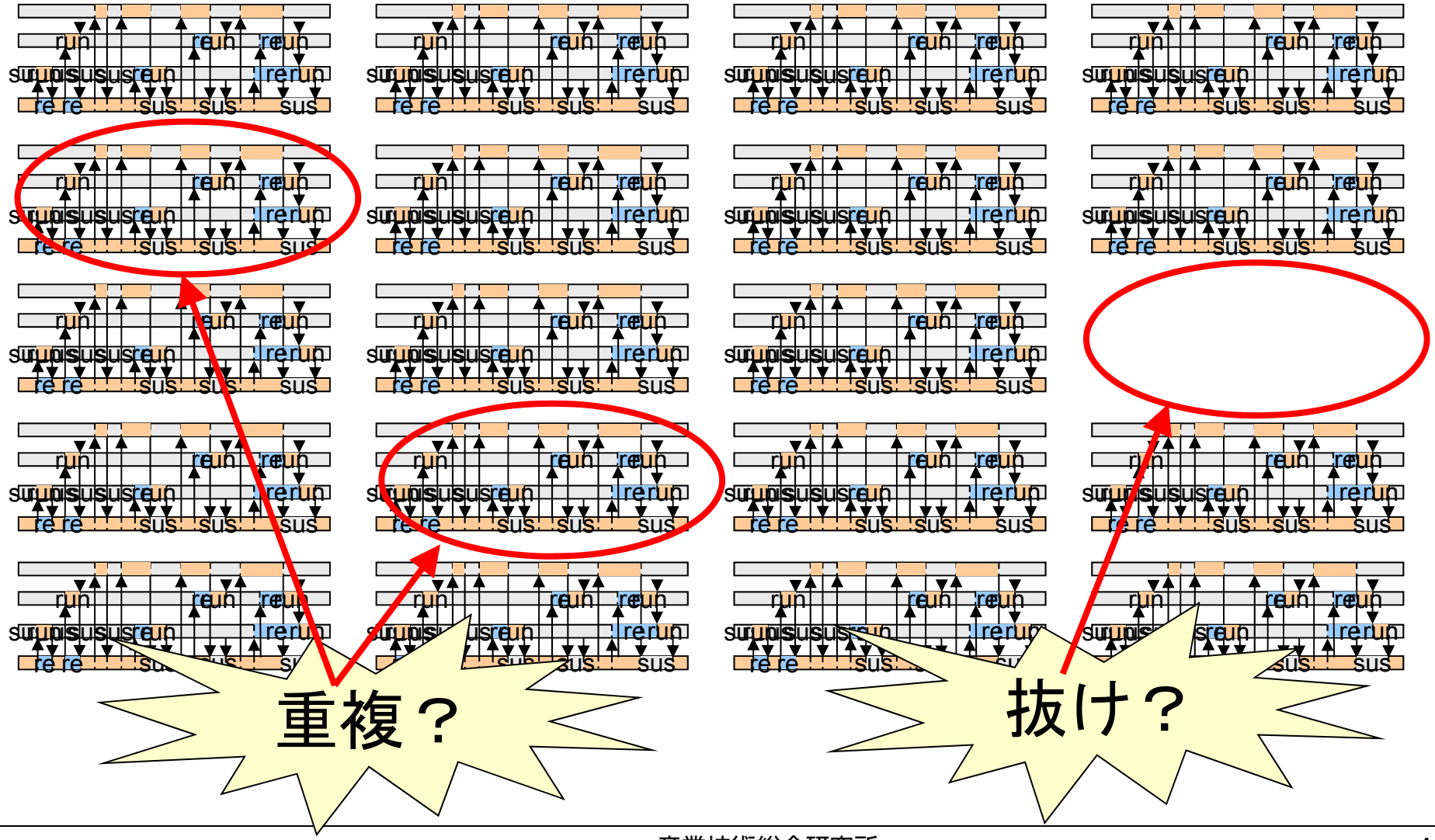
17. ある資源を取得中に，実行タスクと資源競合関係にあり，かつ，実行タスクより優先度の低いタスク（T1）をActivateする場合

8. ある資源を取得中に，実行タスクと資源競合関係になく，かつ実行タスクより優先度の高いタスク（T2）をActivateする場合

3. 実行タスクと資源競合関係にあり，かつそのタスクより優先度の高いタスク（T2）をActivateする場合

1. 実行タスクと資源競合関係になく，かつそのタスクより優先度の高いタスク（T2）をActivateする場合

テストケースセットの不安



テスト関心事(Features)

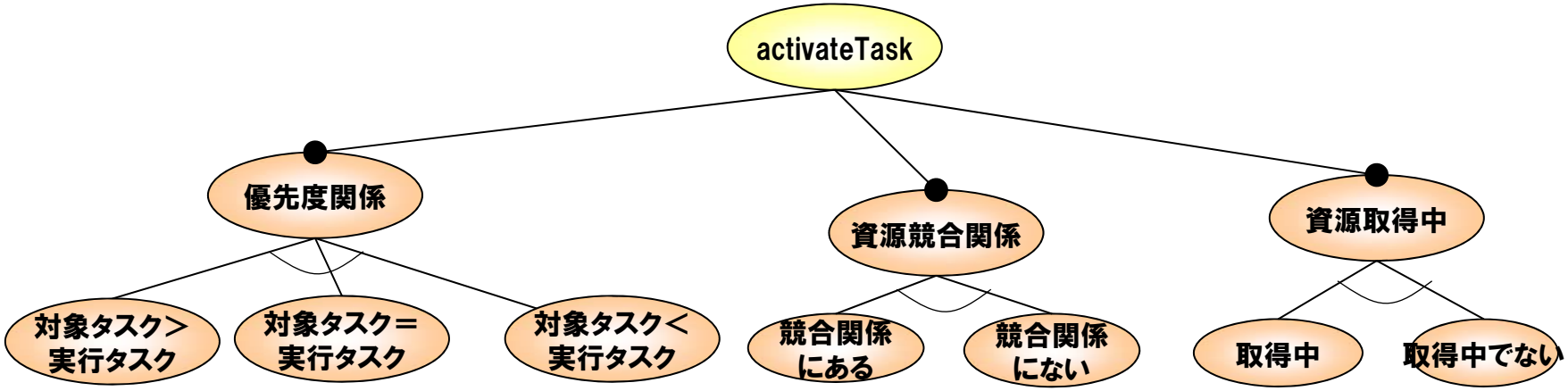
先の例を見ると

- 優先度関係はより高いか、低いか、等しいか
- 資源競合関係にあるかないか
- 資源取得中かそうでないか

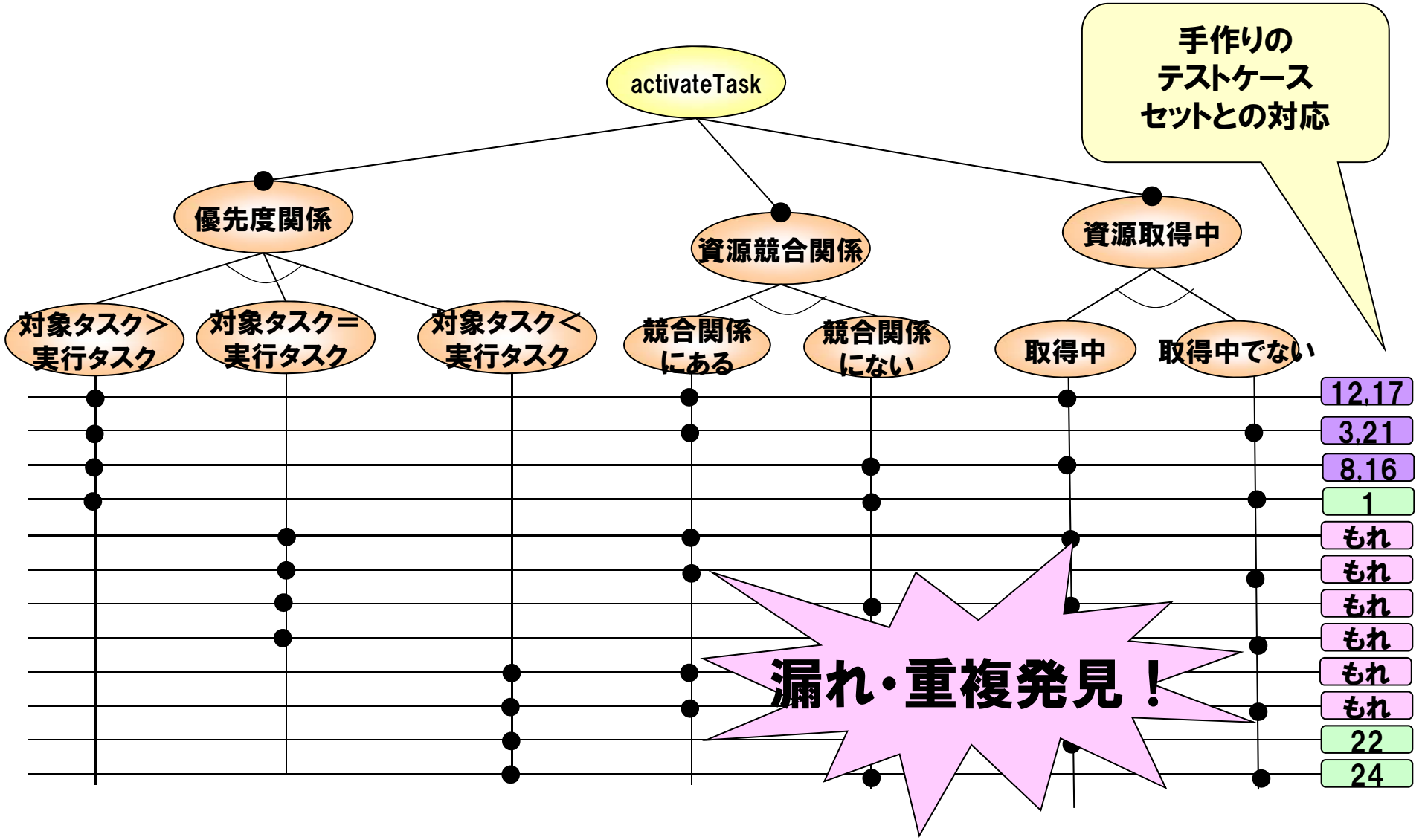
という観点(テスト関心事)の組み合わせで「activateTask」が動作する状況を考えていることがわかる

テストケース設計

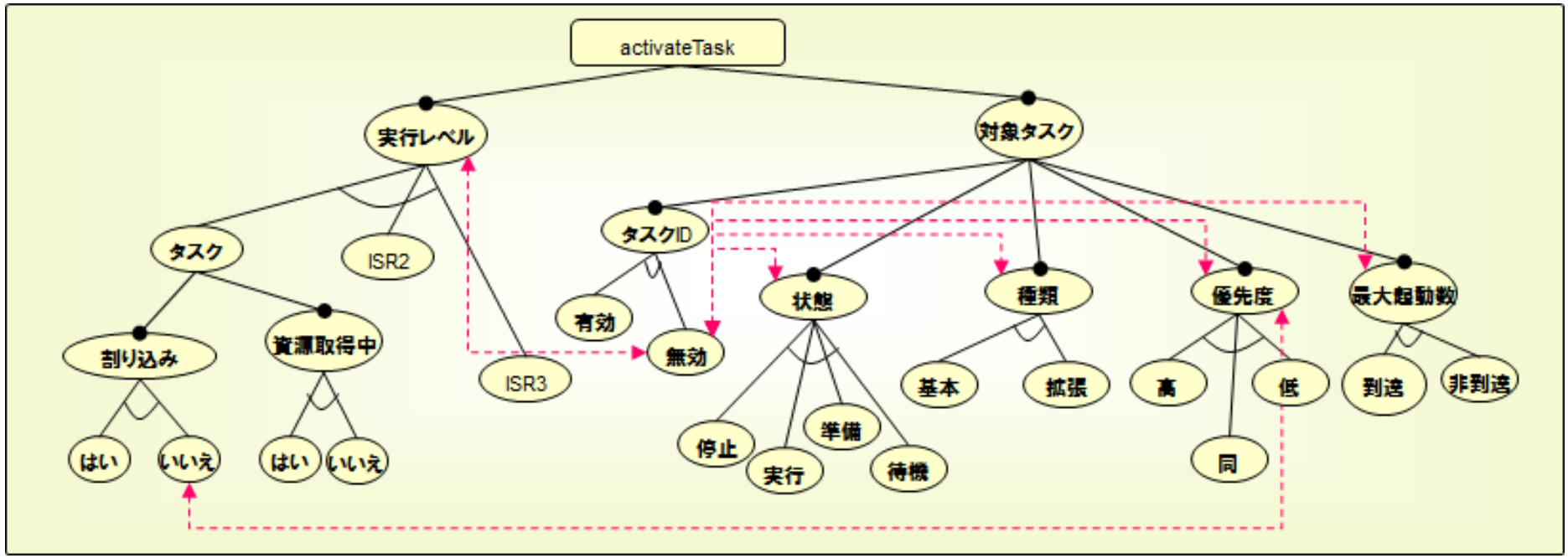
テスト関心事を Feature ダイアグラムを用いて整理することによって、テストケース設計



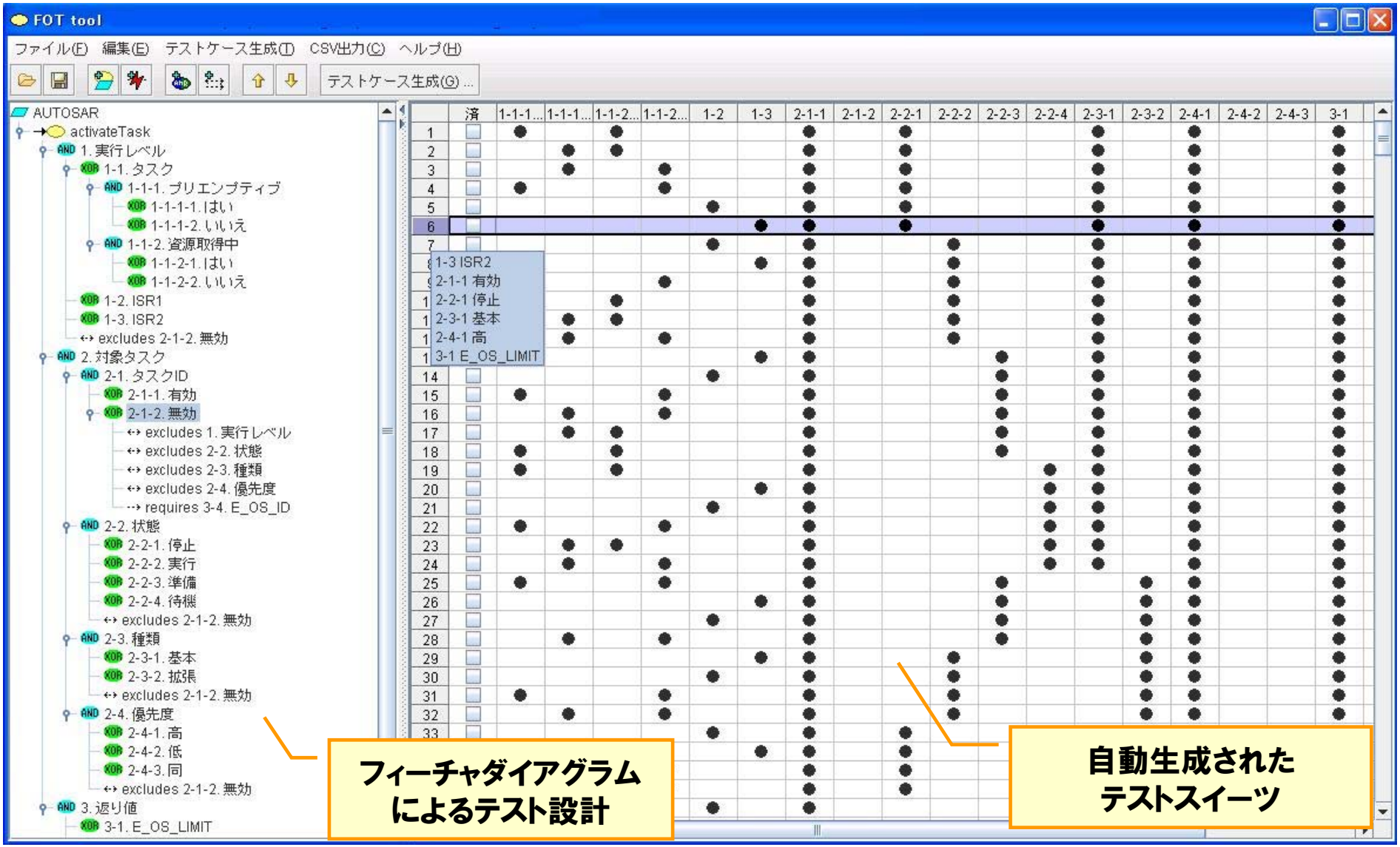
このテストケース設計のテストケースセット



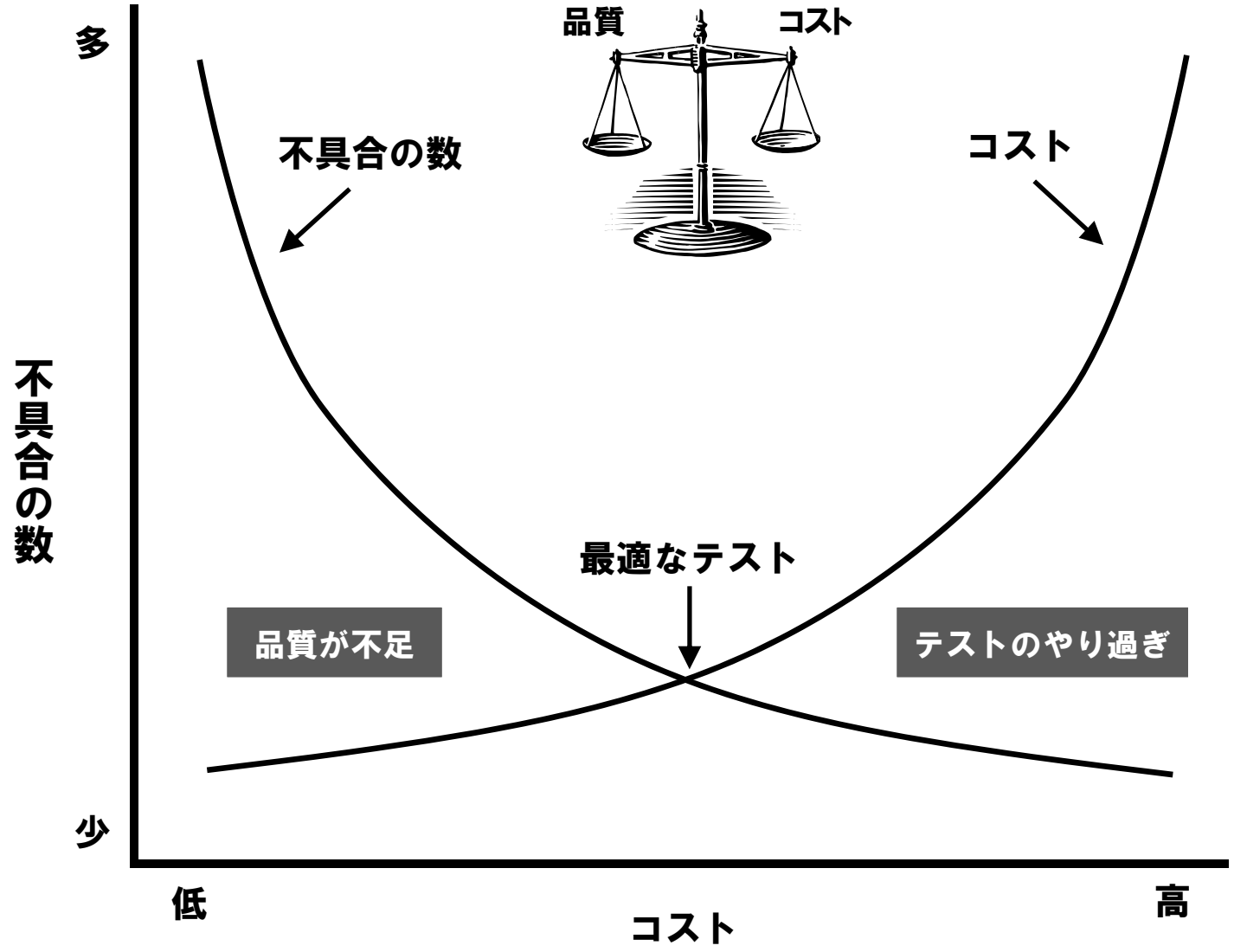
FOT による OSEK-OS テストケース設計



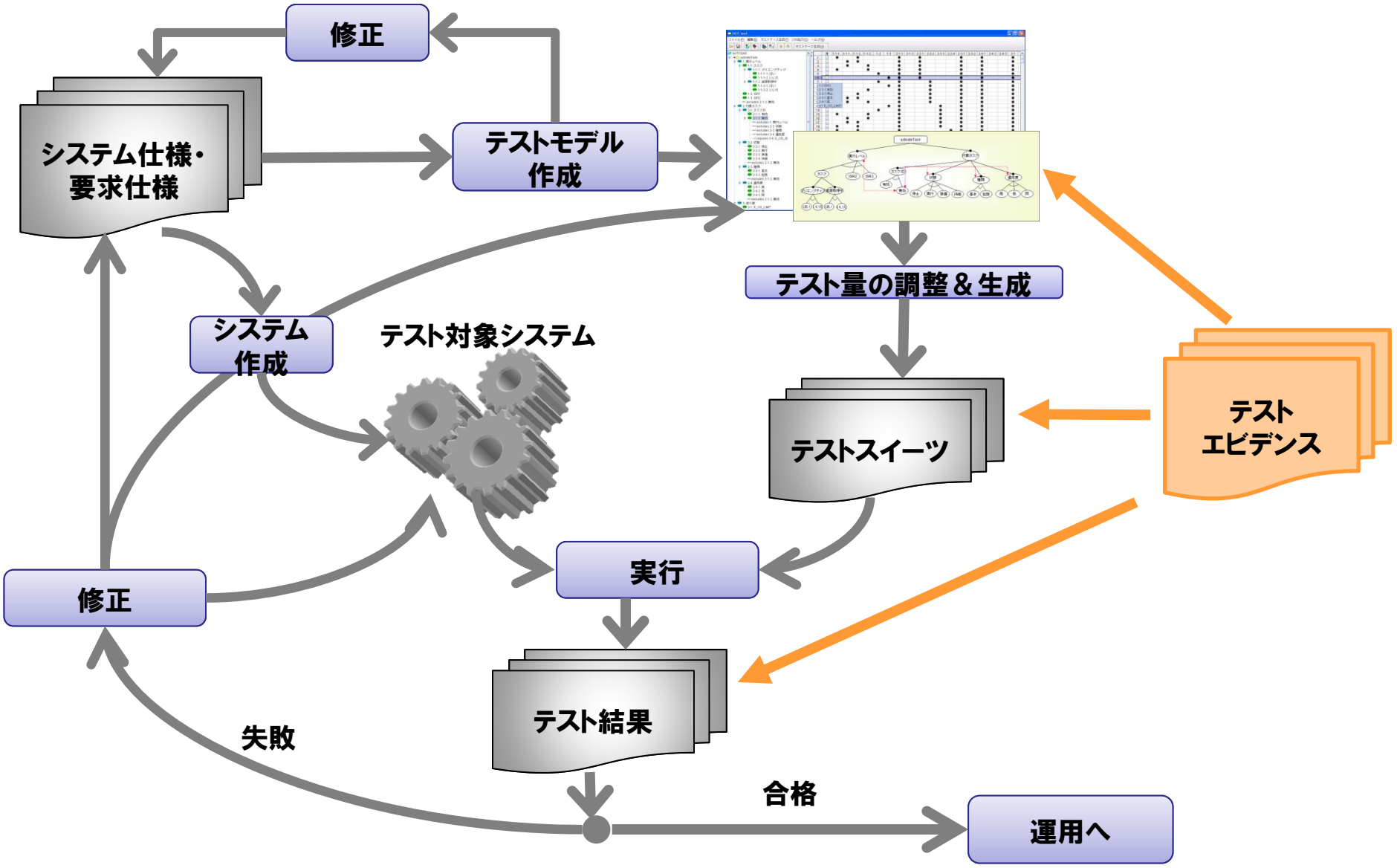
FOT ツール


FOT tool
ファイル(F) 編集(E) テストケース生成(T) CSV出力(C) ヘルプ(H)
テストケース生成(G) ...
AUTOSAR
activateTask
1. 実行レベル
1-1. タスク
1-1-1. プリエンプティブ
1-1-1-1. はい
1-1-1-2. いいえ
1-1-2. 資源取得中
1-1-2-1. はい
1-1-2-2. いいえ
1-2. ISR1
1-3. ISR2
excludes 2-1-2. 無効
2. 対象タスク
2-1. タスクID
2-1-1. 有効
2-1-2. 無効
excludes 1. 実行レベル
excludes 2-2. 状態
excludes 2-3. 種類
excludes 2-4. 優先度
requires 3-4. E_OS_ID
2-2. 状態
2-2-1. 停止
2-2-2. 実行
2-2-3. 準備
2-2-4. 待機
excludes 2-1-2. 無効
2-3. 種類
2-3-1. 基本
2-3-2. 拡張
excludes 2-1-2. 無効
2-4. 優先度
2-4-1. 高
2-4-2. 低
2-4-3. 同
excludes 2-1-2. 無効
3. 返り値
3-1. E_OS_LIMIT
済
1-3 ISR2
2-1-1 有効
2-2-1 停止
2-3-1 基本
2-4-1 高
3-1 E_OS_LIMIT
フィーチャダイアグラム
によるテスト設計
自動生成された
テストスイーツ

テスト量を調整



開発時の使用法


修正
システム仕様・
要求仕様
テストモデル
作成
テスト量の調整＆生成
システム
作成
テスト対象システム
テストスイーツ
テスト
エビデンス
実行
修正
テスト結果
失敗
合格
運用へ

まとめ

- 自動車産業での取り組み
- FOT（Feature Oriented Testing）
  - 既存のブラックボックステスト要素技術を統合
    - 同値類分割、モデルベース、組み合わせテスト
  - テストケース量の調整
    - 品質コントロール
  - テストエビデンス作成支援
    - 認証にかかるコストを低減
- 今後：鉄道分野での適用

システムライフサイクル研究グループの主な取り組み

テスト設計支援技術

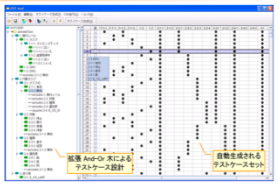
■ 概要

システムテストのためのテスト設計支援、テストケース自動生成
（セミコンダクター企業様との共同研究）

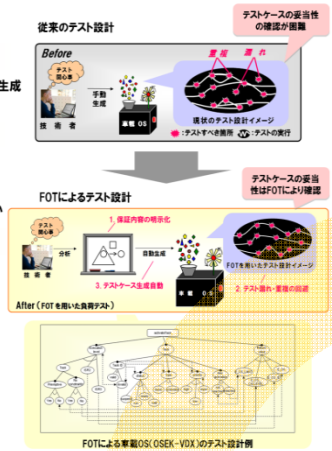
■ 背景

- 不具合の約70%が仕様・設計工程に起因
- 開発の入口で織り込まれた不具合は、開発の出口で検出
- テストの根拠を明示化するための効率の良い手段が少ない

■ テスト設計支援



FOTツール



FOTによる車載OS（OSEK-VDX）のテスト設計例

技法・ツール開発

検証サービスと「さつき」

■ 概要

- 「組込みシステム検証施設整備事業」（経産省）としてクラスタシステムの建設を2007年に計画。
- 2009年6月から試験運用を開始。
- 2010年7月から組込みシステム産業振興機構との合同事業「開発支援事業」（右図）の中で、検証サービスを支える基幹システムとして活用開始。
- 2011年1月から 「さつき」をもちいた検証サービスを提供開始。
- 2011年6月以降、「検証サービス」「さつき利用」を分離。利用者の目的に応じて組合せ自由なサービスに。

関西産学官協同プラットフォーム

検証クラスター「さつき」と システム構成

■ 利用例

- C言語ソースコードの不具合解析

  組込みシステム（Cソースコード6万行程度）が原因不明のフリーズ
  モデル検査による2ヶ月の調査により、コードレベルの原因究明

- 鉄道運賃精算システムの仕様検証

  首都圏鉄道の駅精算システムの基本仕様書を検証
  仕様書を形式モデル化し、64ノード（DualCore）上で動作テスト
  切符と定期券の組合せ80万件の入力を対象に、出力データを照合

サービス

②-1 鉄道システムの国際安全規格適合

■ 概要

第三者視点での高信頼システムの妥当性検証
トレーサビリティの実現
（JR西日本との共同研究）

■ 背景

・要求（安全性）と実現（信頼性）のミスマッチ
・開発コスト、特にテストの費用対効果に対する発注側の不信感
・国際安全規格への対応要求

■ 産業的価値

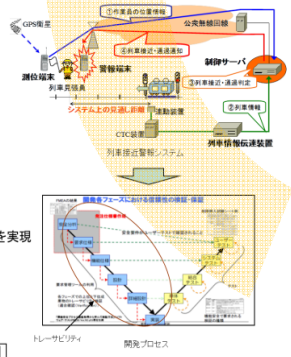
【トレーサビリティ】鉄道システム開発へのトレーサビリティツール適用
→要求仕様書、基本仕様書、テスト成果物間のトレーサビリティ検証を実現
【テスト妥当性検証】テスト工程の妥当性検証基準の策定
→発注者要求にもとづくテスト関連文書のレビュー方法を採用

■ 成果と事例

・列車接近警報システムの開発プロセスへ適用
・テスト工程の妥当性検証基準（素案）

次年度以降の成果目標

発注者の立場からの開発ガイドライン



検証事例

2 消費者機械の機能安全規格化

■ 概要

消費者機械（介護ロボット、スマートハウス、自動車など）の機能安全規格の策定
→ ISO26262（自動車）の開発プロセスへの反省にもとづく標準化
→ OMGにて原案策定（2年後）、最終的には ISO化

■ 背景

IPA/SEC（モデルベース開発技術部会）がプロジェクトチームを今年度発足
→ 産総研からは 中坊（知能システム）と田口（組込み）が参加※現在承認待ち
OMG/System Assuarance Task Forceで田口（組込み）がco-chairとして規格化の作業中

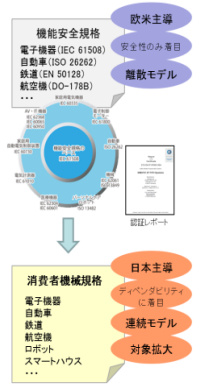
■ 産業的価値

【国際競争力向上】日本発の機能安全規格、日本の強みを生かす
【既存規格の改善】ISO26262の大幅な改善案
- 物理モデル記述の導入
- メタモデルによる規格の仕様化

■ これまでの成果

外部発表
- 松野浩、田口研治: 自動制御学会「システムのディペンダビリティ、安全保証の現在」、2011年11月
- K. Taguchi: OMG Seminar on Systems Assurance & Safety for Consumer Devices "Meta-modeling Approach to Safety Standards for Consumer Devices", June 2011, USA
- Y. Matsuno, K. Taguchi, Y. Nakabo, A. Ohata: Workshop on Dependable Systems of Systems "Iterative and Simultaneous Development of Embedded Control Software and Dependability Cases for Consumer Devices", Sep, 2011, UK

国内外委員
- 田口研治: OMG/System Assuarance Task Force Co-Chair



標準化