論証と合意のための
モデル: D-Case

2016年9月16日
MBD中部カンファレンス

DEOS協会D-Case部会
高井 利憲

背景: 論証と合意が必要となる場面

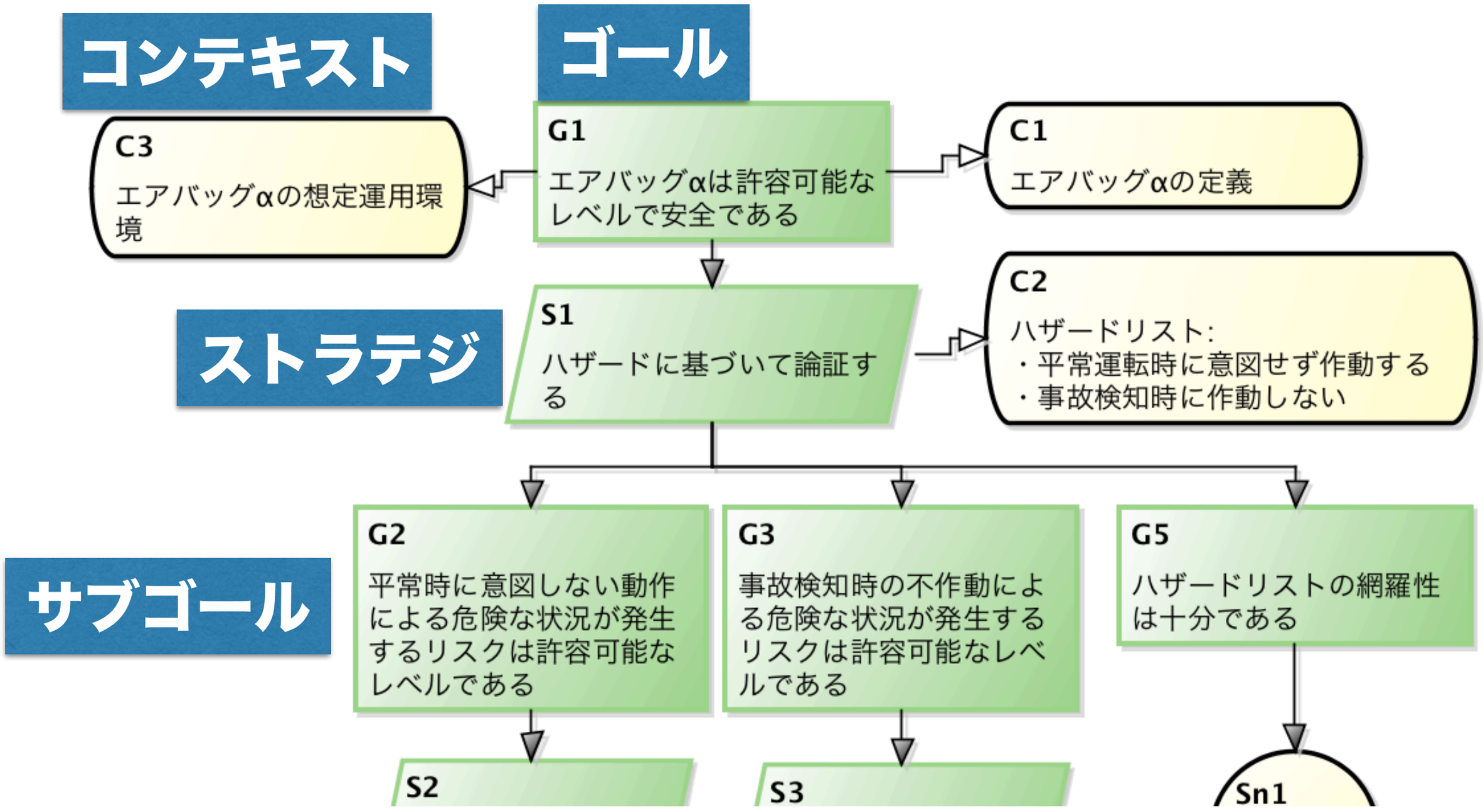
- サプライヤーからOEM
- Tier nからTier n+1
- 第三者認証機関へ
- 設計における意思決定
- 組織における意思決定
- デザインレビュー
- ソフトウェアレビュー
- ハザード分析＆リスクアセスメント
- テストケース設計
- 内部監査
- etc

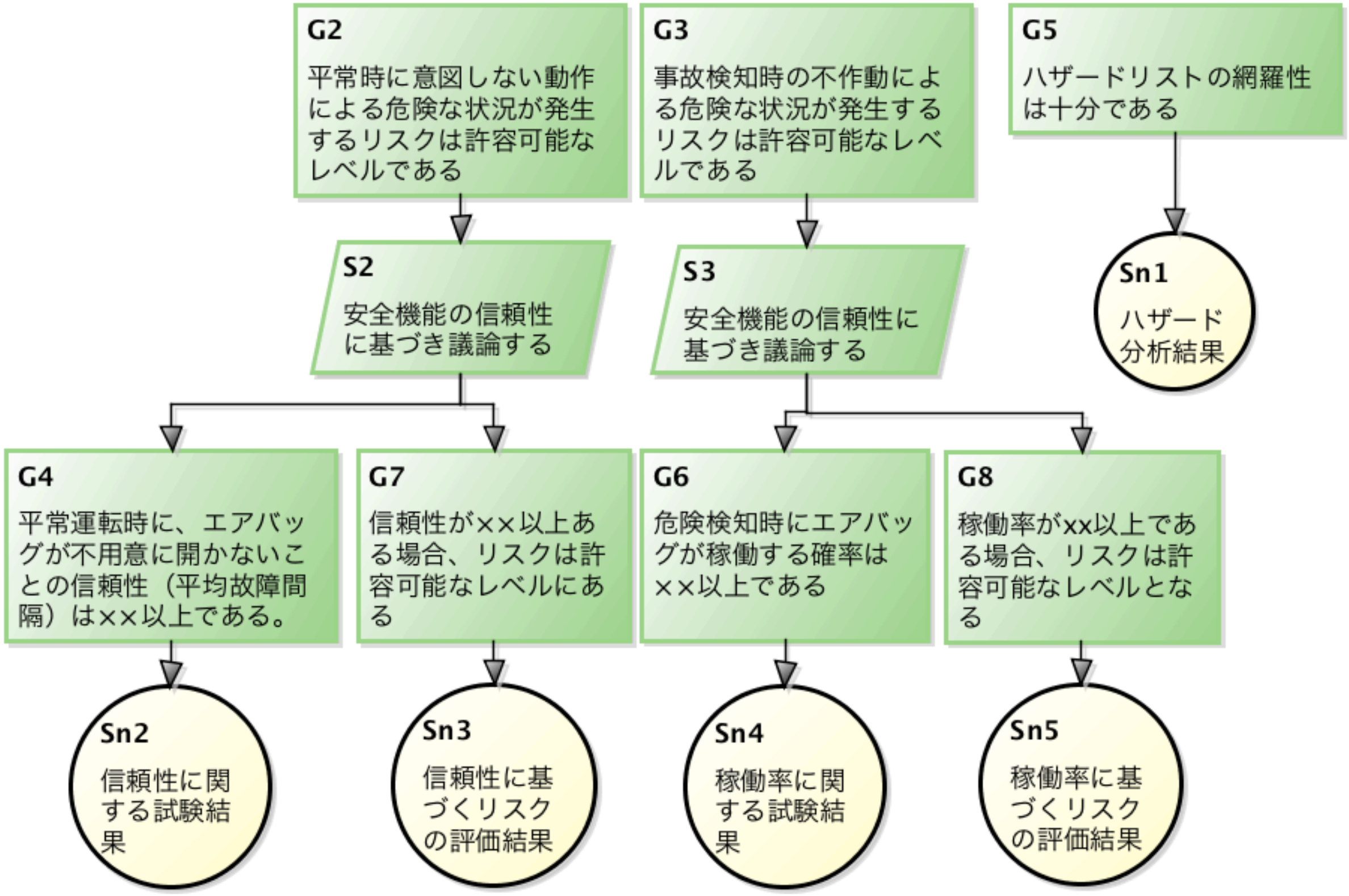
D-Case: 論証と合意のためのモデル

背景

- **オープンシステムディペンダビリティ**
  - **変化し続けるシステム**において、利用者が期待する便益を安全かつ**継続的に提供**しつつ、ステークホルダーや社会への**説明責任**を全うできること
- **ゴール構造化表現（GSN, Goal Structuring Notation）**
  - 1990年代初頭から英国ヨーク大学を中心に研究
  - 任意団体であるGoal Structuring Notation Working Groupにより標準化が進められている
    - GSN community standard version 1
- **D-Case**
  - GSNをベースとした表記法に基づく、オープンシステムディペンダビリティにおける説明責任を達成するための方法論

GSN/D-Caseの例


コンテキスト
ゴール
C3
エアバッグαの想定運用環境
G1
エアバッグαは許容可能なレベルで安全である
C1
エアバッグαの定義
ストラテジ
S1
ハザードに基づいて論証する
C2
ハザードリスト:
・平常運転時に意図せず作動する
・事故検知時に作動しない
サブゴール
G2
平常時に意図しない動作による危険な状況が発生するリスクは許容可能なレベルである
G3
事故検知時の不作動による危険な状況が発生するリスクは許容可能なレベルである
G5
ハザードリストの網羅性は十分である
S2
S3
Sn1


G2
平常時に意図しない動作による危険な状況が発生するリスクは許容可能なレベルである
G3
事故検知時の不作動による危険な状況が発生するリスクは許容可能なレベルである
G5
ハザードリストの網羅性は十分である
S2
安全機能の信頼性に基づき議論する
S3
安全機能の信頼性に基づき議論する
Sn1
ハザード分析結果
G4
平常運転時に、エアバッグが不用意に開かないことの信頼性（平均故障間隔）は××以上である。
G7
信頼性が××以上ある場合、リスクは許容可能なレベルにある
G6
危険検知時にエアバッグが稼働する確率は××以上である
G8
稼働率がxx以上である場合、リスクは許容可能なレベルとなる
Sn2
信頼性に関する試験結果
Sn3
信頼性に基づくリスクの評価結果
Sn4
稼働率に関する試験結果
Sn5
稼働率に基づくリスクの評価結果

ソリューション

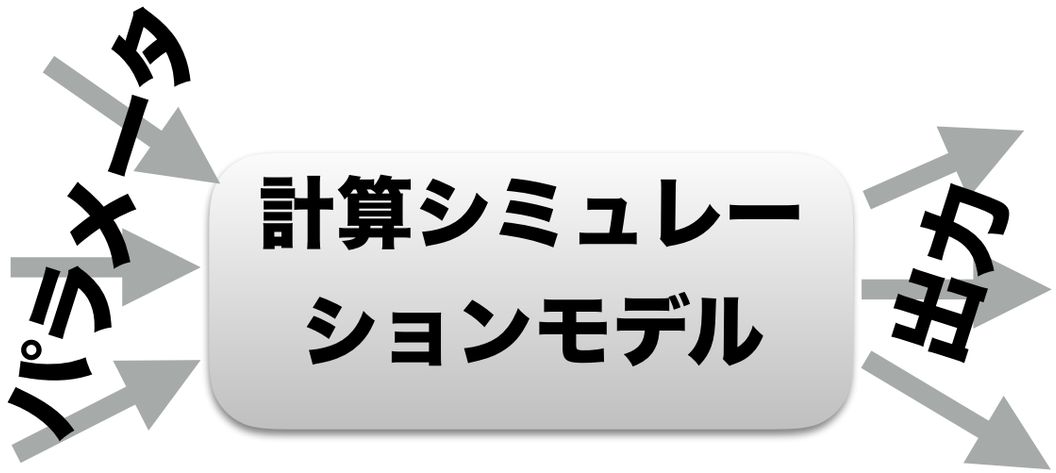
GSN/D-Caseによる論証の表現で期待できること

- ゴールを明示化することにより、**論証ケース毎の論証の目標**を共有することができる
- コンテキストにより、**論証の前提条件や制約、仮定**などを共有することができる
- ストラテジにより、ゴールをサブゴールに分割する**論証の方針**を共有することができる
- ソリューションにより、**証拠に基づく論証**を強制することができる
- トップゴール、ストラテジ、サブゴール、コンテキスト、ソリューションによって**論証の構造**を明示化することにより、**合意可能な箇所と不可能な箇所、時間経過により論証の主張が成り立たなくなった際の影響範囲**などを共有できる

D-Caseの事例

シミュレーション計算の妥当性に関する合意のためのD-Case(*1)

- **背景**: システム要求に基づき作成したシミュレーションモデルが、現実とかけ離れていた
  - **直接の原因**: モデルを簡単化しすぎ、制約条件が不適切であった
  - **有識者によるレビューをしていたにもかかわらず**
  - 上流設計者、製造担当者、レビューア、テスト担当者等の**認識が一致していなかった**



→ D-Caseを適用へ

(*1) 森: 三菱電機におけるD-Case活用事例ー期待結果の明確化と合意を目指してー, ET, 2014.

ゴールを共有

分解の妥当性を共有

有識者の位置付けを明確化

G1
シミュレーション結果が妥当である

C1
システム要求

S1
システム要求毎に分解

M1
相対的な順序づけができる

G3
ユーザがパラメータの選択に参考にできる

Sn1
原理の説明体制等

論点にフォーカスをあてる

G4
相対的な順序付けができる

S2
経験則の有無で分解

C2
経験則をまとめた文書

G5
経験則 ある条件の場合、 計算結果が経験値通りである

G6
経験則が無い条件の場合、計算結果が妥当である

Sn2
経験値との比較結果

S3
別の検証手段の有無で分解

G7
別の検証手段がある場合、計算結果が妥当である

G8
別の検証手段が無い場合、計算結果が妥当である

Sn3
検証結果

不確実性が残る箇所を共有

結論「開発の早い段階からエビデンス収集、合意活動 → 手戻りを防げた」

例題: 耐熱タイル自動防水処理ロボット

- スペースシャトルのまわりを覆う耐熱タイルの
  検査と防水処理を自動で行うロボット

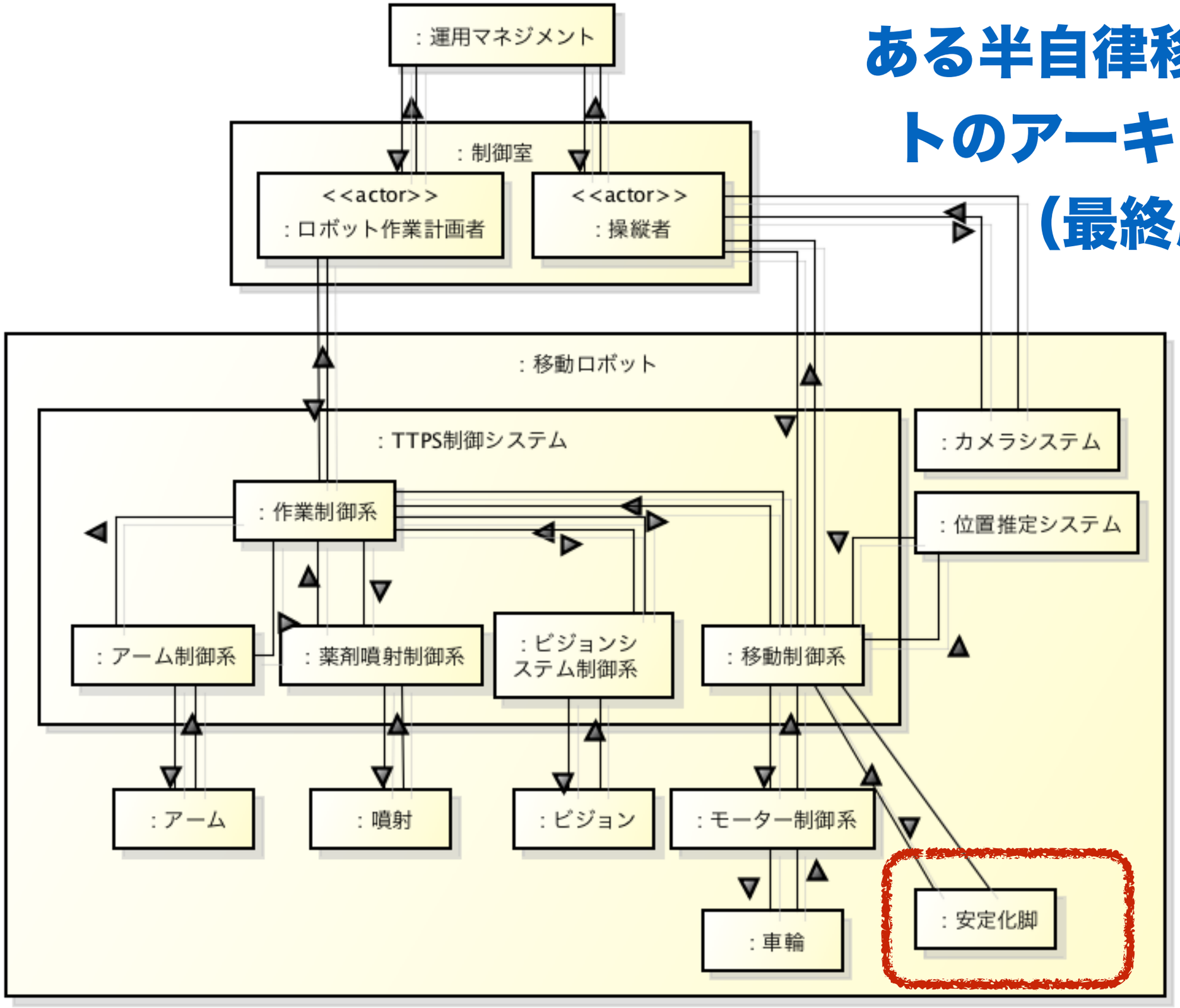
(*2) 写真はイメージです

Nancy G. Leveson: Engineering a Safer World, MIT Press, 2011

(*2)http://www.maesei.co.jp/item/kani/12/view

例: モデルの妥当性に関する根拠に基づく論証の共有

ある半自律移動作業ロボットのアーキテクチャ設計（最終版）(*1)



(*2) 写真はイメージです

(*1) Nancy G. Leveson: Engineering a Safer World, MIT Press, 2011

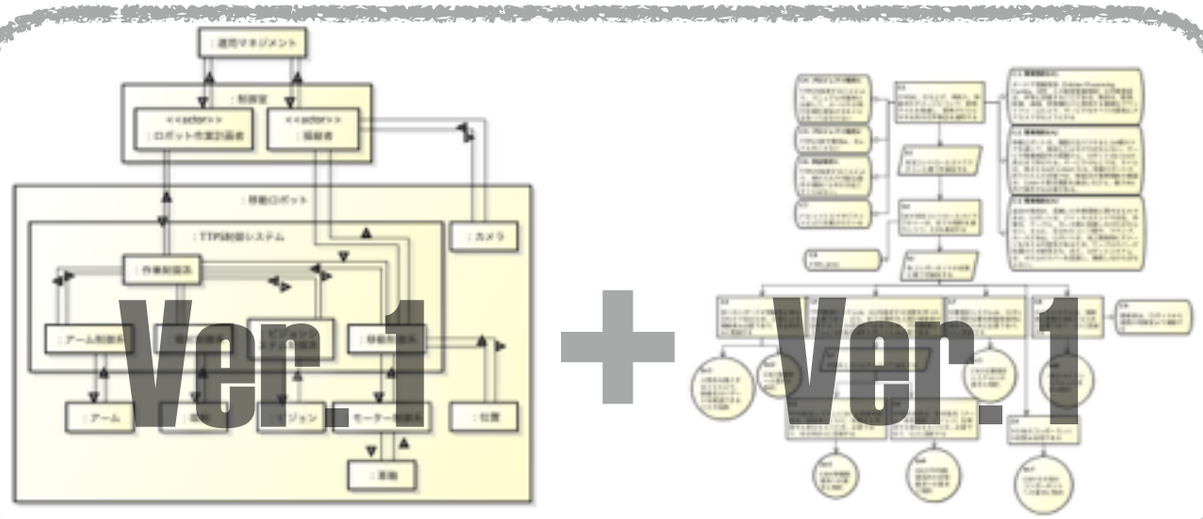
(*2)http://www.maesei.co.jp/item/kani/12/view

安定化脚を導入するまでの経緯

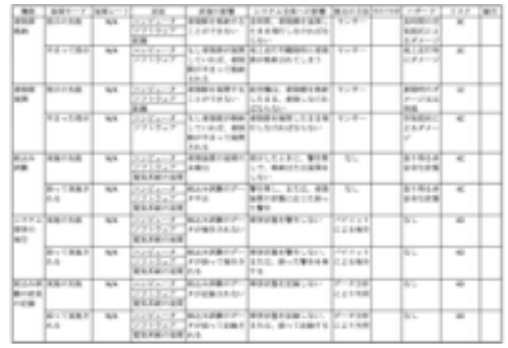
これらの経緯は残りにくい

1. 安定化脚無しバージョンで設計
2. ハザード分析
3. 複数の制御系に起因する振動問題によるハザード発見
4. 本体の重量増による安定化設計案検討
5. 人や設備との衝突時の危険性の増加により却下
6. 本体の全長増による安定化設計案検討
7. 動作環境の制約により却下
8. 作業時のみ展開する安定化脚案検討
9. ハザード分析
10. 問題がないことを確認

D-Caseを活用した設計根拠の可視化

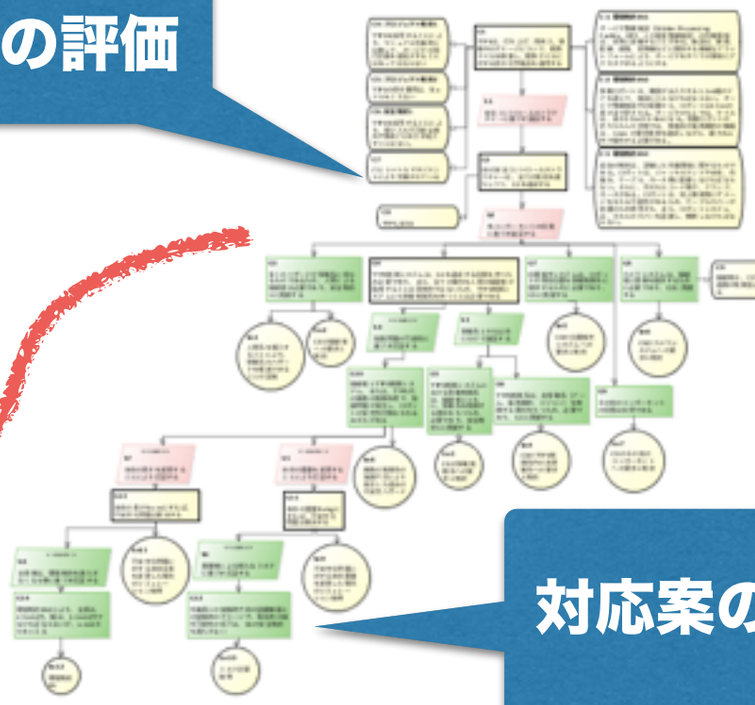


1. D-Caseで予め論証

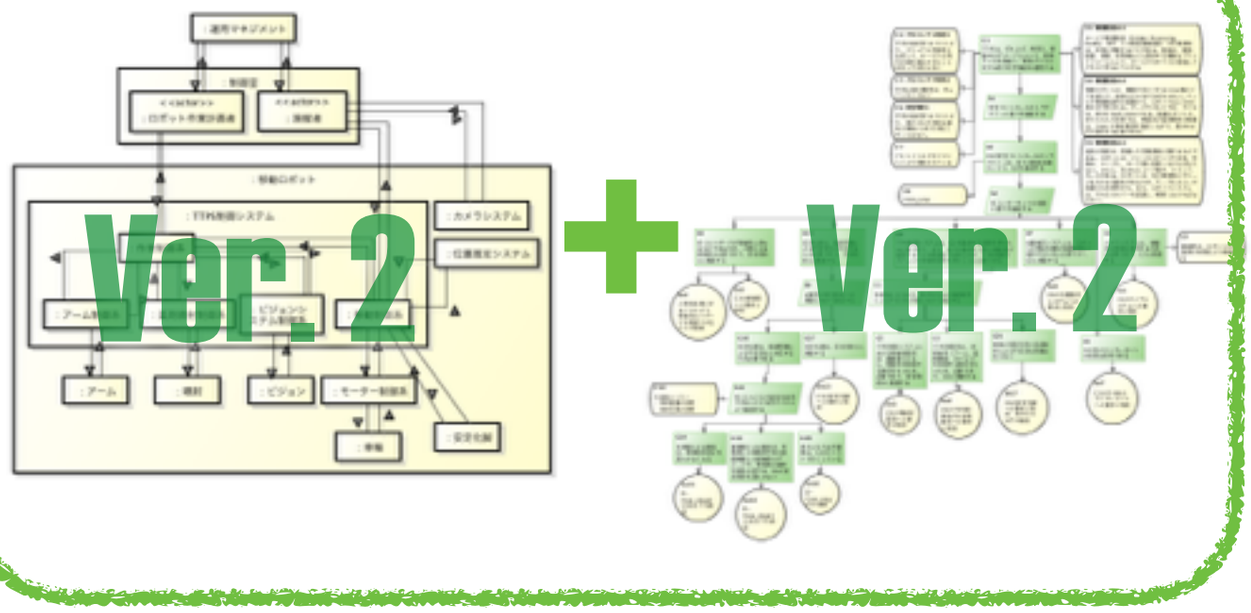


2. ハザード分析

発見されたハザードの評価



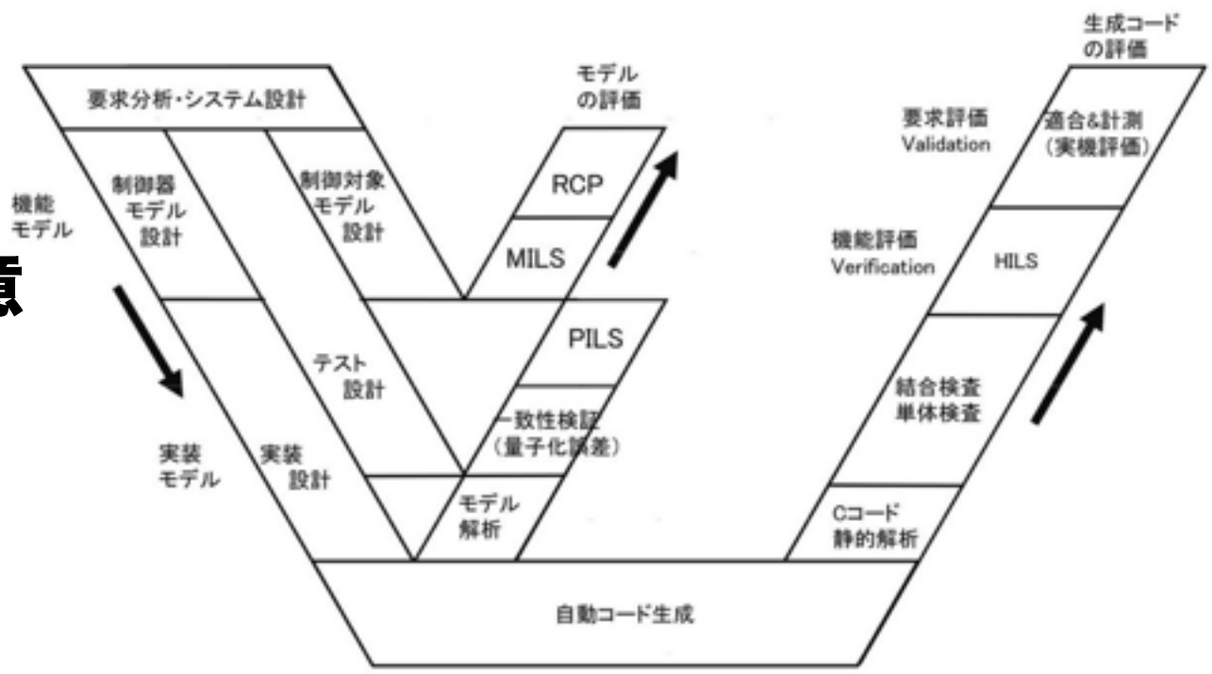
3. D-Case上で議論



4. 議論の結果を反映

モデルベース開発におけるD-Case の役割として期待できること

- **MBDを採用する開発プロセスの妥当性に関する論証と合意**
- **各モデルの妥当性に関する論証と合意**
  - **一つのモデル内の整合性**
  - **採用しなかった選択肢からみた対象モデルの優位性**
- **各モデルによるシミュレーション結果の位置付けに関する論証と合意**
- **各モデルに基づくテストケース設計の妥当性に関する論証と合意**
- **自動コード生成によって保証される性質に関する論証と合意**



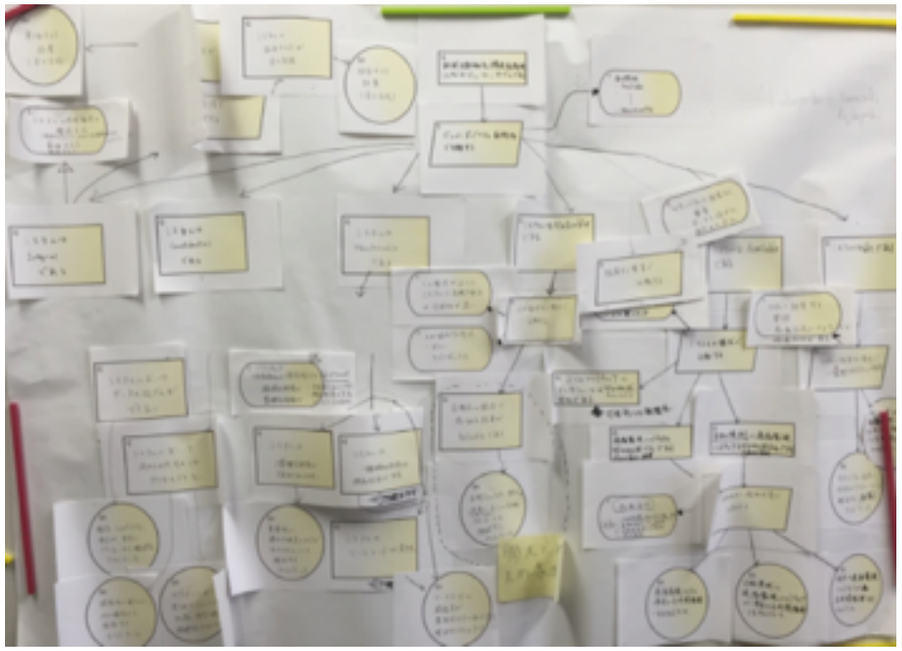
モデルベース開発とエンジニア育成の最前線, TechShare, 2014

モデルとD-Caseまとめ

- D-Caseは、モデルの根拠や背景、採用されなかった選択肢とその理由などを構造的に記録しておくことにより、変化に強いモデルベース開発を可能にする

D-Caseの活動例

- 奈良先端大での演習
  - 学生のチームにより、モデルの定義、ハザード分析、D-Caseによる論証と合意のプロセスを実習
    - テーマ例：介護ロボット、内蔵インシュリンポンプ、スマートアラーム
  - 企業との合同ワークショップなども含む
    - テストケースの設計と妥当性に関する論証



- その他、DEOS協会およびD-Case研究会のWeb ページに情報があります

イベント案内

- 第2回 D-Caseワークショップ@名古屋
  - テーマ：D-Caseを用いて設計品質を可視化してみよう
  - 日時：9月30日(金)
- 第11回 D-Case研究会のお知らせ
  - 日時：10月28日（金）
  - 場所：名古屋大学東山キャンパス
- 日経Automotive主催技術者塾
  「ソフトウエア設計開発者向け安全性論証記述徹底トレーニング」
  - 日時：10月31日（月）
  - 場所：東京

補足と関連情報

- GSNやD-Caseに基づく論証パターンがいくつか提案されています
- 自動車の業界団体であるJasParは現在、ISO26262対応時に必要となる安全性論証のパターンをGSNで与えるガイドを作成しています
- MISRAも、ISO26262で要求されているセーフティケースの記述ガイドラインをGSNで与えようとしています