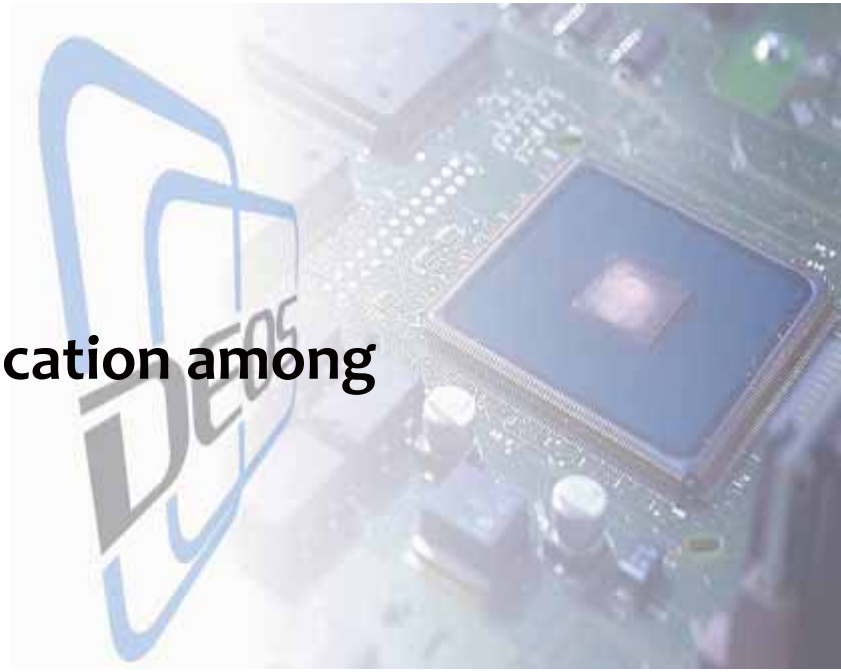
Embedded Technology 2010



説明責任を支援する技術(1)

–D-Case: A Language for Communication among Stakeholders

松野 裕
東京大学 情報基盤センター スーパーコンピューティング部門
matsu@cc.u-tokyo.ac.jp

December 2, 2010

JST 科学技術振興機構
Japan Science and Technology Agency

本日の内容

- D-Case: ステークホルダ間における、ディペンダビリティ合意形成のためのモデリング言語
- 受付ロボットを例にとったD-Case記述例
- D-Case Toolsの紹介
- ディペンダビリティ合意内容と、システムの同期の保証
  - D-fopsとの連携(詳細は次の発表で)
- Challenges to Open Systems Dependability
  - オープンシステムの「変化」に対応するためのプロセスとシステム
  - D-Case's Challenge : プロセスによるディペンダビリティ維持と、システムの構成によるディペンダビリティの維持の組み合わせの精緻化

D-Case Team Members

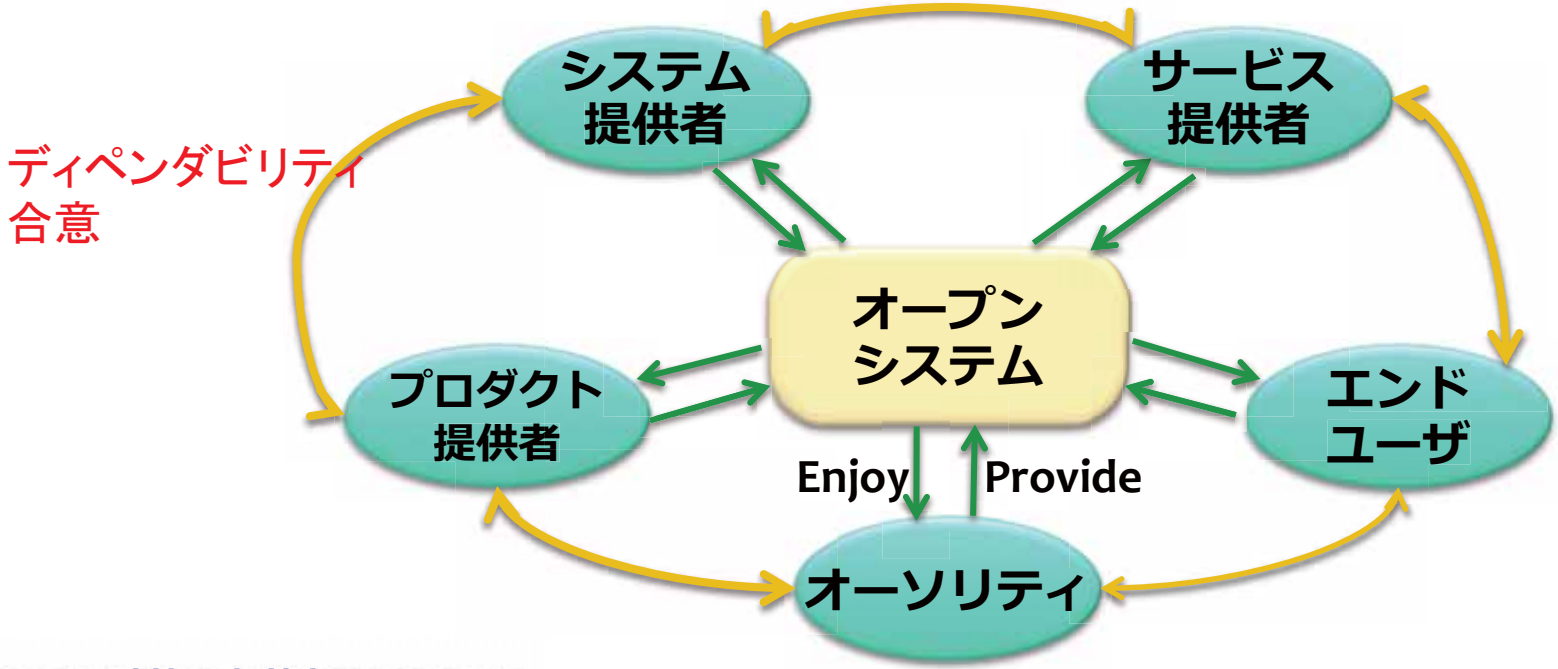
- 松野裕 / 東大
- 中澤仁 / 慶大
- 武山誠 / 産総研
- 高井利憲 / 産総研
- 松崎健男 / 産総研
- 田口研治 / 産総研
- 伊東敦 / 富士ゼロックス
- 上野肇 / 富士ゼロックス
- 髙村博紀 / DEOS Center
- Thanks to D-fops team and DEOS Center

オープンシステムディペンダビリティ (1/3)

- ディペンダビリティとは、障害など、さまざまリスクにシステムが対処し、サービスを継続することができる、システムの性質である
  - 安全性、可用性、信頼性などを包括する概念として議論されてきた(Jean-Claude Laprie 他)
- オープンシステムとは、システムの機能、構造、境界が時間と共に変化するシステムである
  - オープン性はネットワーク化・複雑化の本質である
- JST CREST DEOSプロジェクトでは、オープンシステムにおけるディペンダビリティを根底から考え、それを実現するためのアーキテクチャおよびプロセスを研究開発している

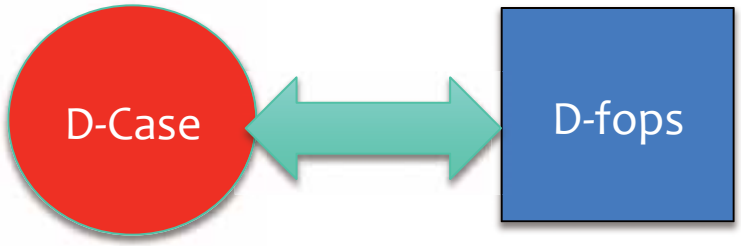
オープンシステムディペンダビリティ (2/3)

- オープンシステムでは、すべてが不確実であり、すべてを理解できるステークホルダは存在しない
  - ステークホルダ達は、最善を尽くして、**合意**して、ディペンダビリティを達成しなければならない
  - システムは、**合意**の根拠(エビデンス)を提供し、**合意**を確実に実行しなければならない



オープンシステムディペンダビリティ (3/3)

- D-Case: ステークホルダ間の合意形成のためのディペンダビリティモデリング言語、記述プロセス、記述支援ツール
- D-fops: 合意のエビデンスの提供、合意の確実な実行のためのアーキテクチャ
  - 詳細は次の発表で



ステークホルダがディペンダビリティについて合意し、システムがそのためのエビデンスを提供し、合意の確実な実行を行なうことが、オープンシステムにおける、ステークホルダとシステムの説明責任につながると考える

D-Case: ステークホルダ間の合意形成のための ディペンダビリティモデリング言語

現在のD-Case
は右のような
ノードを持つ木
構造をしている

イギリスなどで、
原発など、
高い安全性が
求められるシステム
を開発・運用する
際、認証機関に
提出が義務付けら
れるまでに普及している
Safety Case
をもとにしている

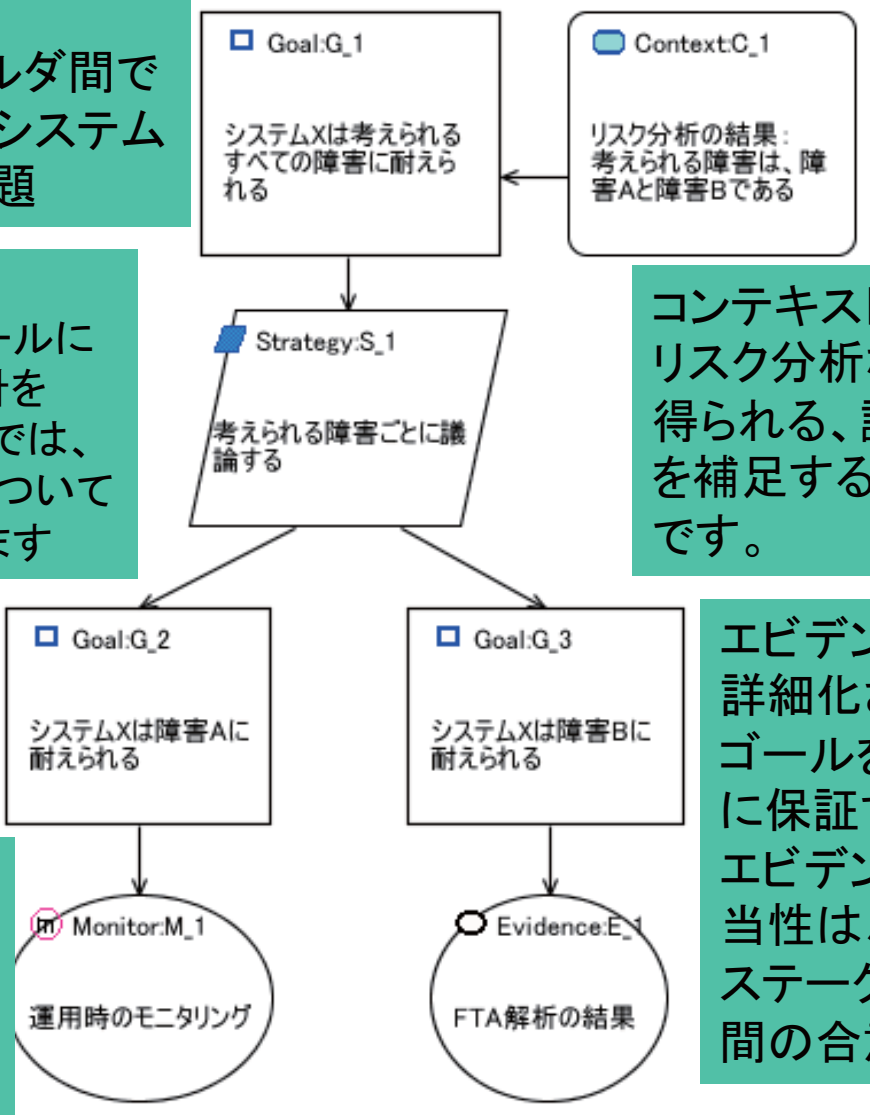
ゴール:
ステークホルダ間で
合意すべきシステム
に関する命題

ストラテジ:
ゴールをサブゴールに
わけるときの方針を
記述します。ここでは、
障害Aと障害Bについて
場合分けしています

コンテキスト:
リスク分析などから
得られる、議論
を補足する情報
です。

エビデンス:
詳細化された
ゴールを最終的
に保証するもの。
エビデンスの妥
当性は、
ステークホルダ
間の合意による

モニタリング:
システムの運用時
のモニタリング
によって得られる
エビデンス

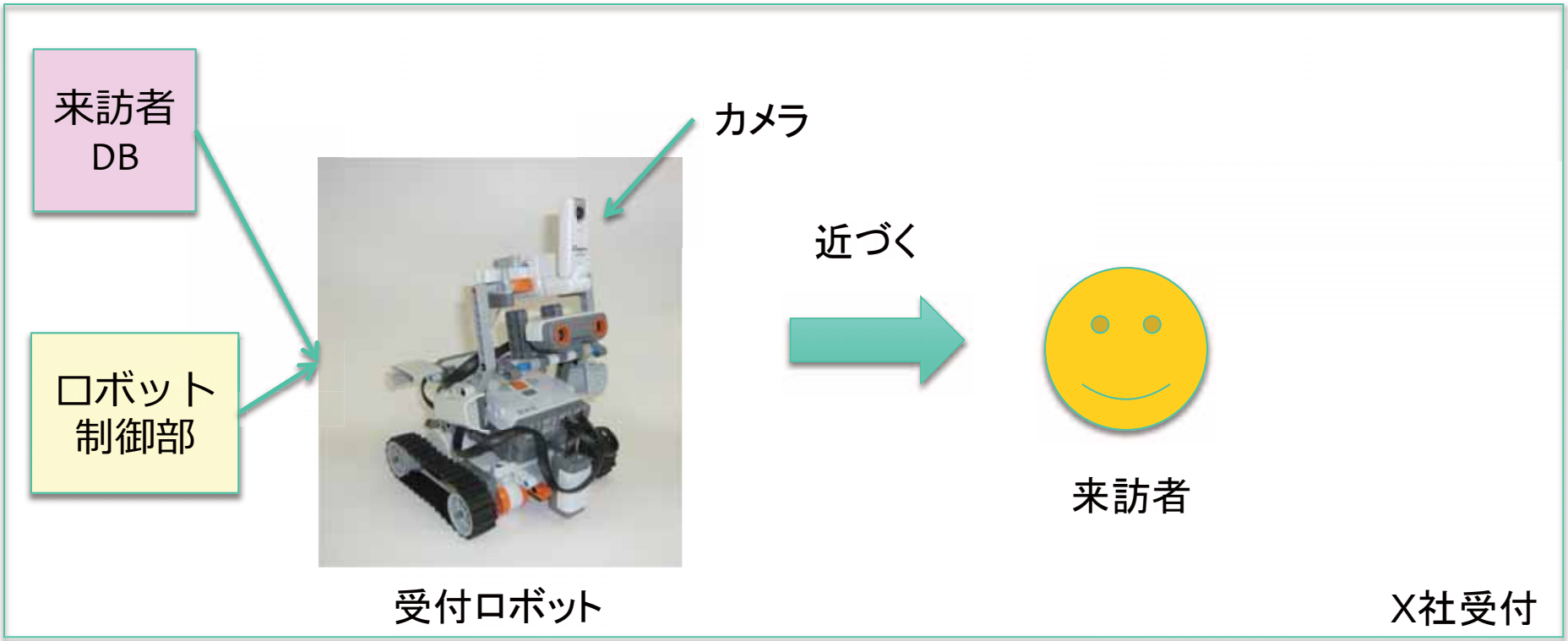


Safety Case

- Caseとは、法廷用語で「論拠」という意味
- イギリスで頻発した深刻な障害の教訓から生まれた
  - Piper Alpha北海油田事故（1988年, 167名死亡）など
- 単にある手順などに従うのではなく、なぜその手順でシステムの安全性が保てるかエビデンスをもとに議論することの重要性が認識され、認証機関への提出が義務付けられるまでになった
- 国際標準規格でも義務付けられるようになりつつある
  - ISO 26262: 自動車の機能安全規格
- DEOSでは、Safety Caseに関わるISOやOMGにおける標準化活動、海外の研究者との研究交流を活発に行っている

受付ロボットを例にしたD-Case記述例

- 会社への来訪者の受付を行なうロボットを考える
  - ロボットにはカメラがついている
  - 来客を認識すると、近づき、顔認識を行なうことにより、来訪者を判別するとする



D-Case記述プロセス
(現在議論中。D-25デモ会場にて冊子を配布中)

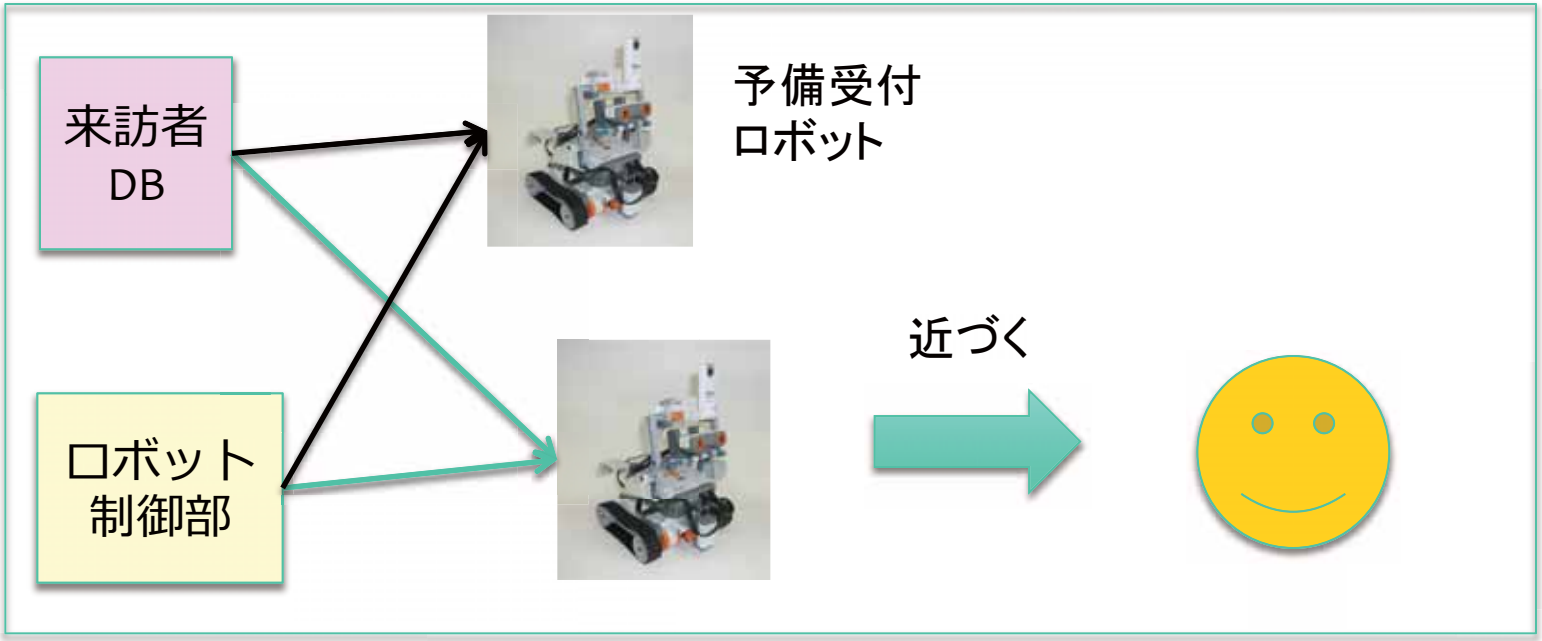
リスク分析結果例:
客に不用意に近づく
→ 安全性
客を待たせる。
30秒以上待たせる
と支障が生じる可能
性がある。
5分が我慢の
限界。
→ 可用性
(ここでは、可用性
を考える)

カメラ、受付ロボット、
制御部などに
分けて、受付ロボット
が最悪でも5分以上客
を待たせない
ことを議論する

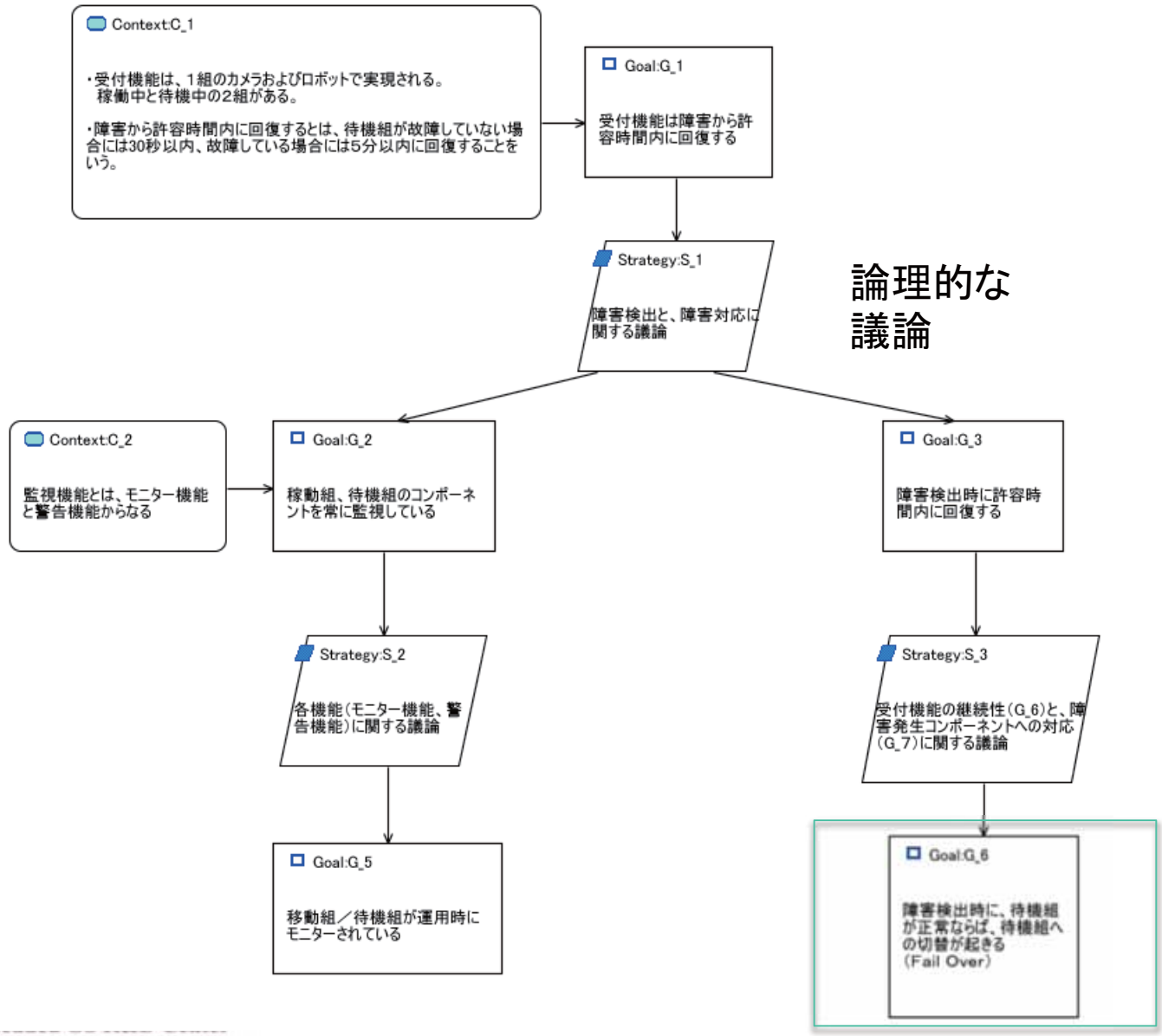
受付ロボットの
開発・運用プロセス
などによって、障害
対応などが
行えることを
議論する

受付ロボットの障害対応に関するステークホルダ合意

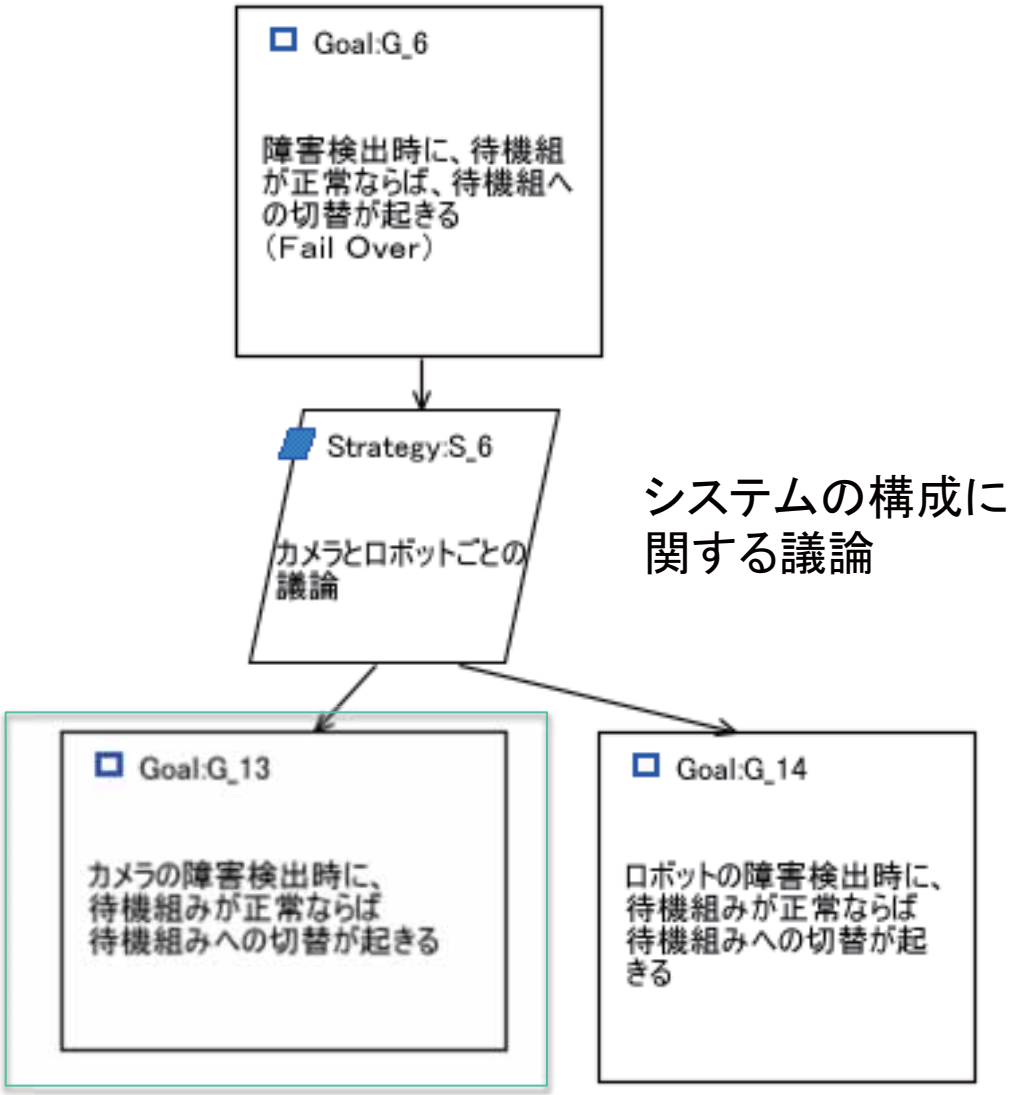
- 予備の受付ロボットを用意し、受付ロボットに障害が発生した場合、Fail Overすることにより、客を殆どの場合30秒以上、最悪5分待たせないようにすることで、開発者、利用会社などのステークホルダが合意したとする
- 合意は、「受付機能は障害から許容時間内に回復する」をトップゴールとしたD-Caseによりされたとする



障害回復D-Case: トップレベル

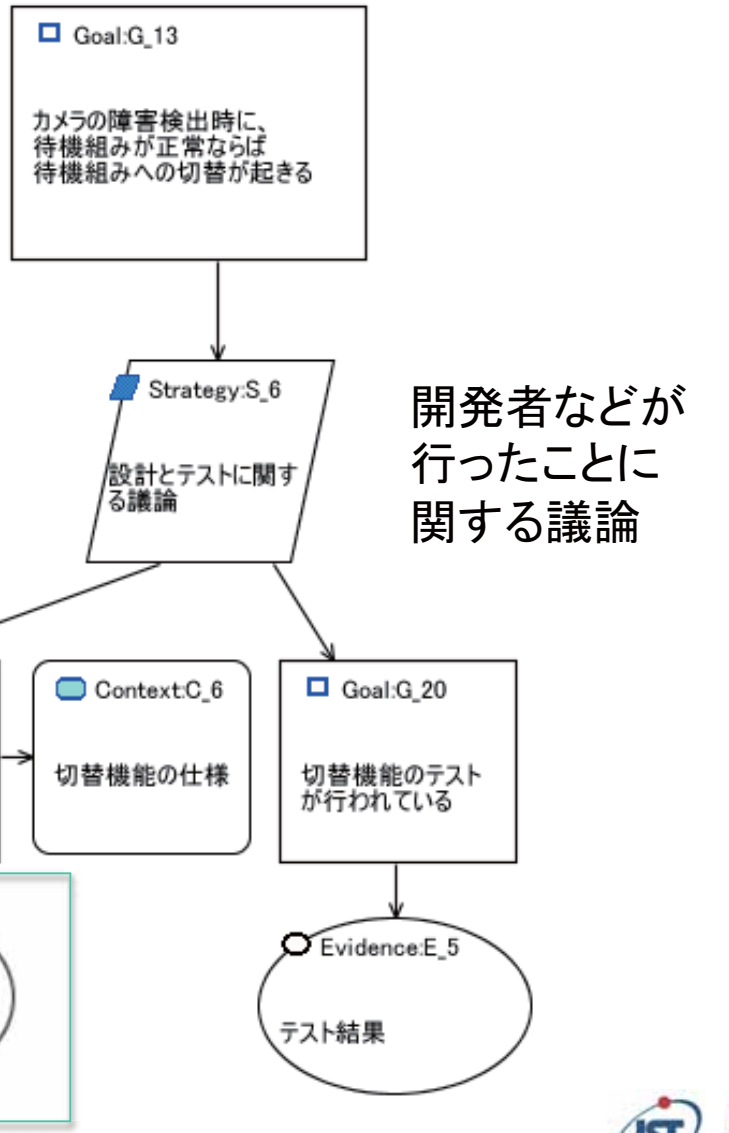


障害回復D-Case: Fail Overに関する議論



システムの構成に関する議論

障害回復D-Case: カメラ故障によるFail Overに関する議論



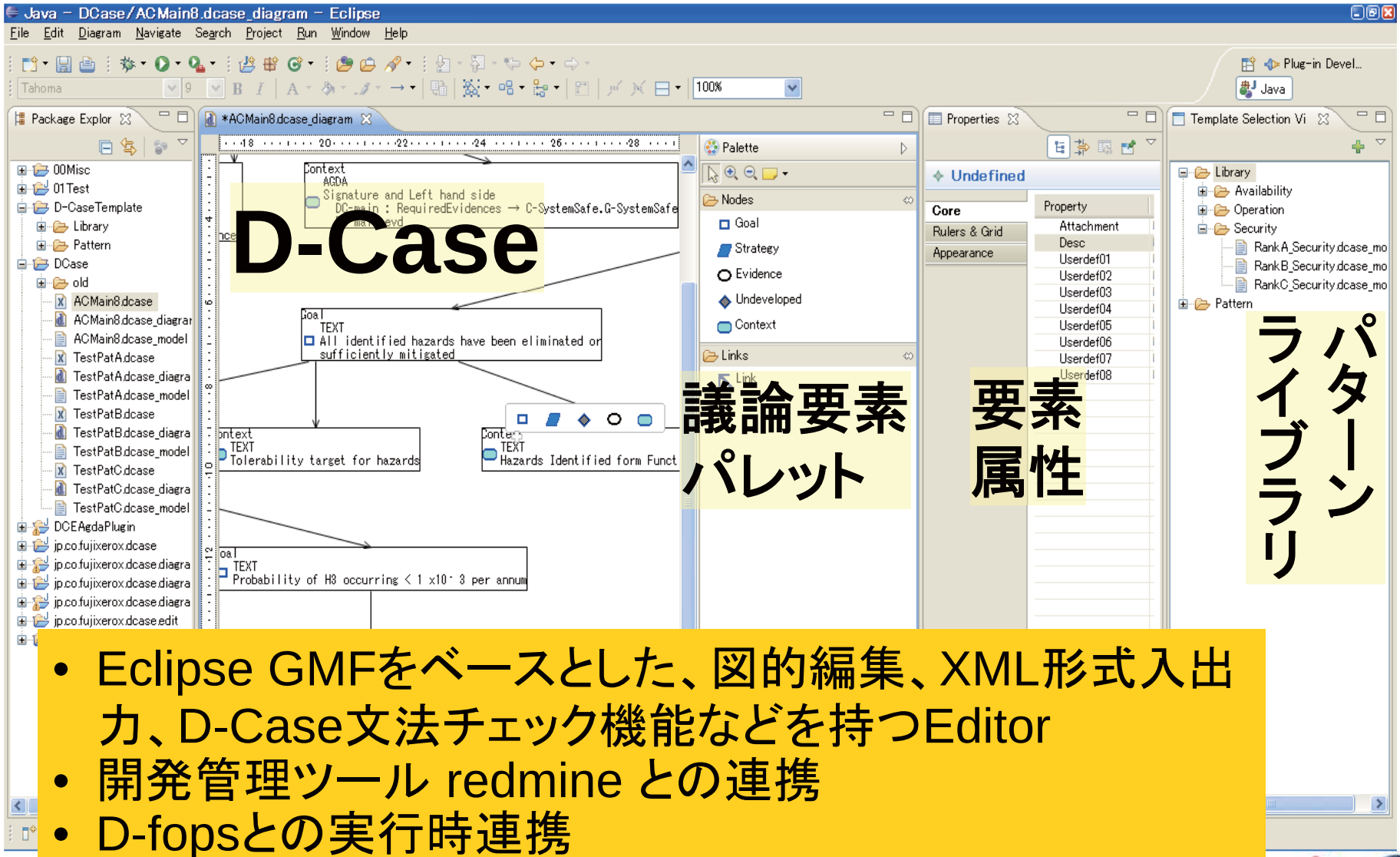

```
if exec /damd/videocheck.sh id="{id}" {n}
then /damd/demo1.sh {ACTION} camera-error
```

D-fopsスクリプト

開発者などが
行ったことに
関する議論

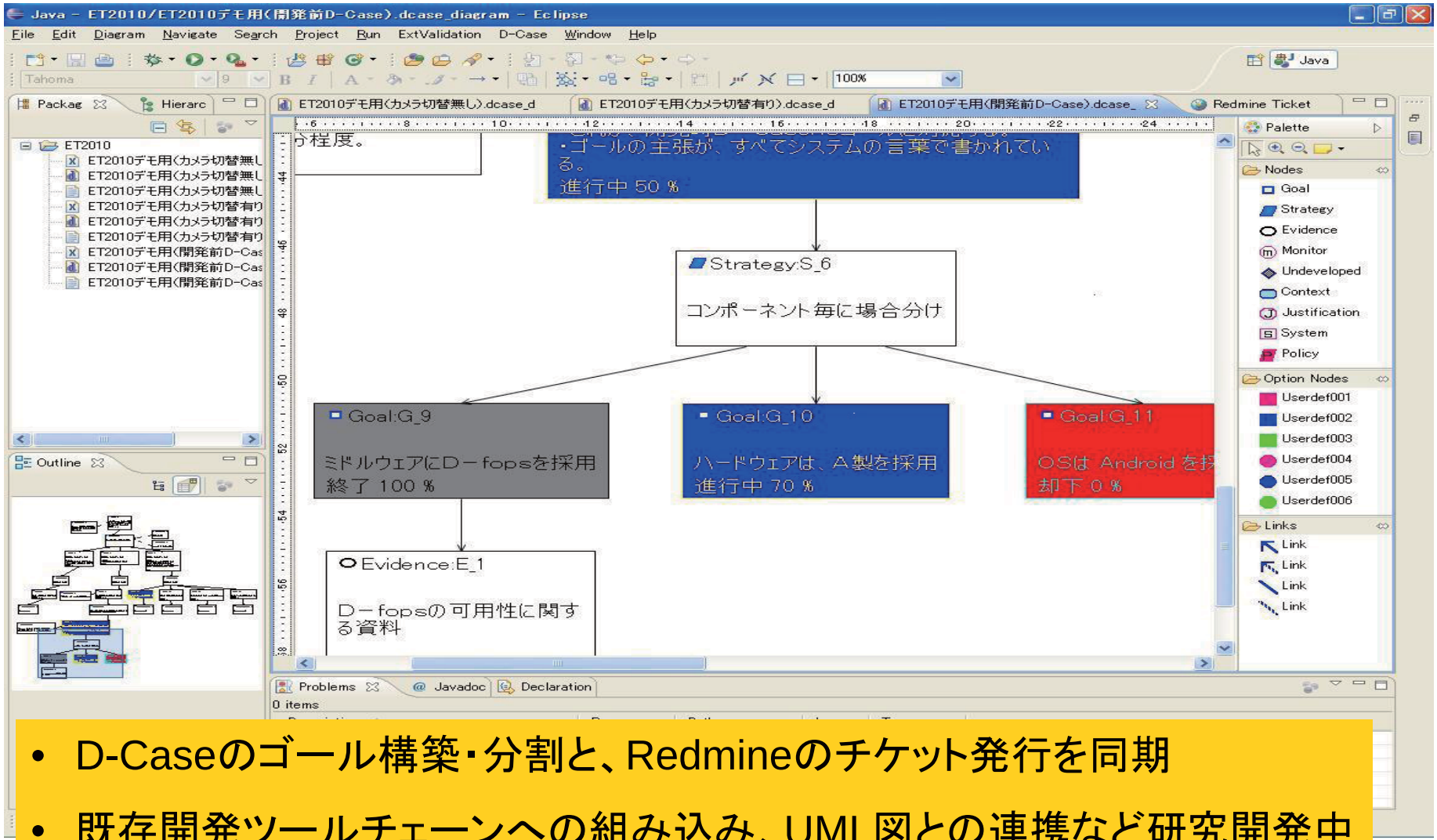
モニタノードに、制御
スクリプトを埋め込むことにより、
合意内容の確実な実行を
保証する

D-Case Tools: D-Case Editor



- Eclipse GMFをベースとした、図的編集、XML形式入出力、D-Case文法チェック機能などを持つEditor
- 開発管理ツール redmine との連携
- D-fopsとの実行時連携

D-Case Tools: D-Case EditorとRedmineの連携

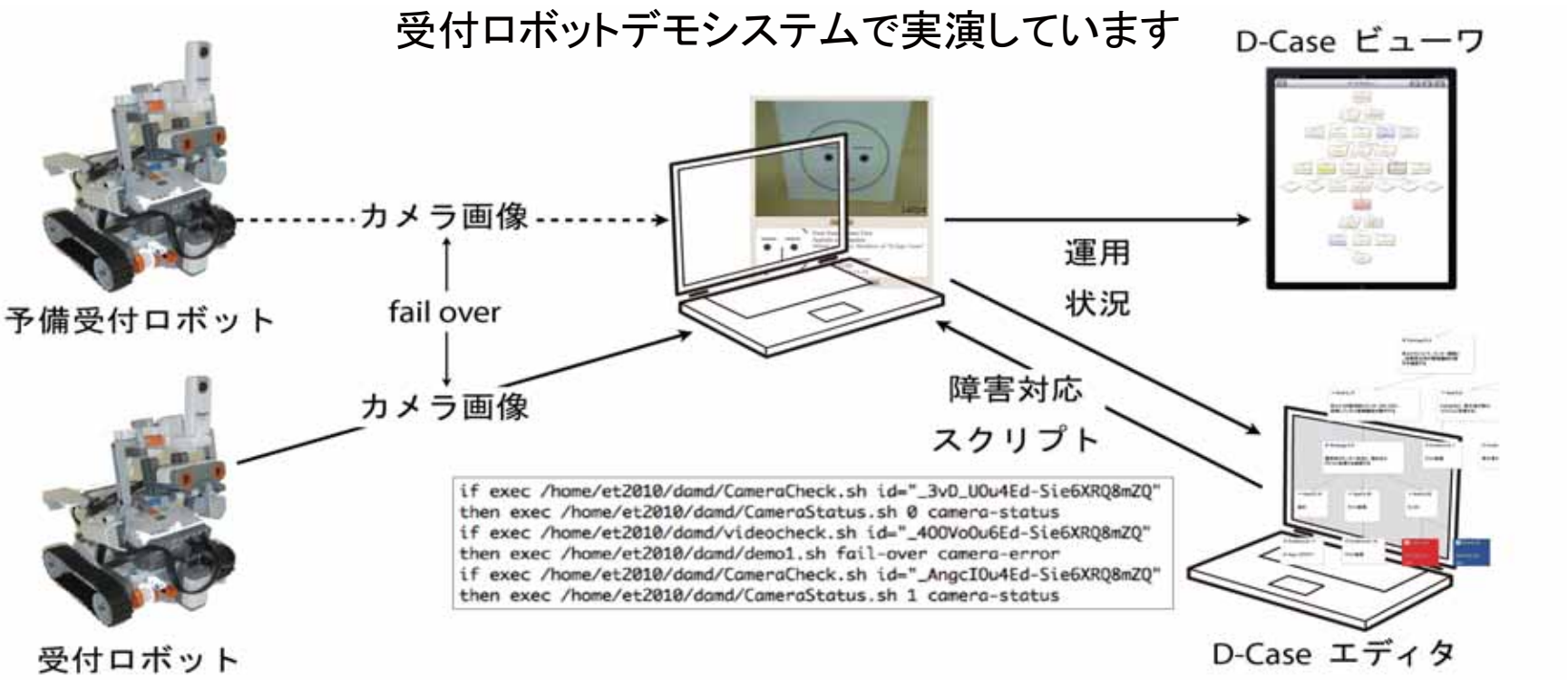


- D-Caseのゴール構築・分割と、Redmineのチケット発行を同期
- 既存開発ツールチェーンへの組み込み、UML図との連携など研究開発中

D-Case Tools: D-Case Viewer

- iPadで実装したD-Case Editorを閲覧機能に限定して軽量化したViewer
- システム運用時に、D-Caseを参考に障害対応をおこなうために用いる

ディペンダビリティ合意内容と、確実な実行の保証

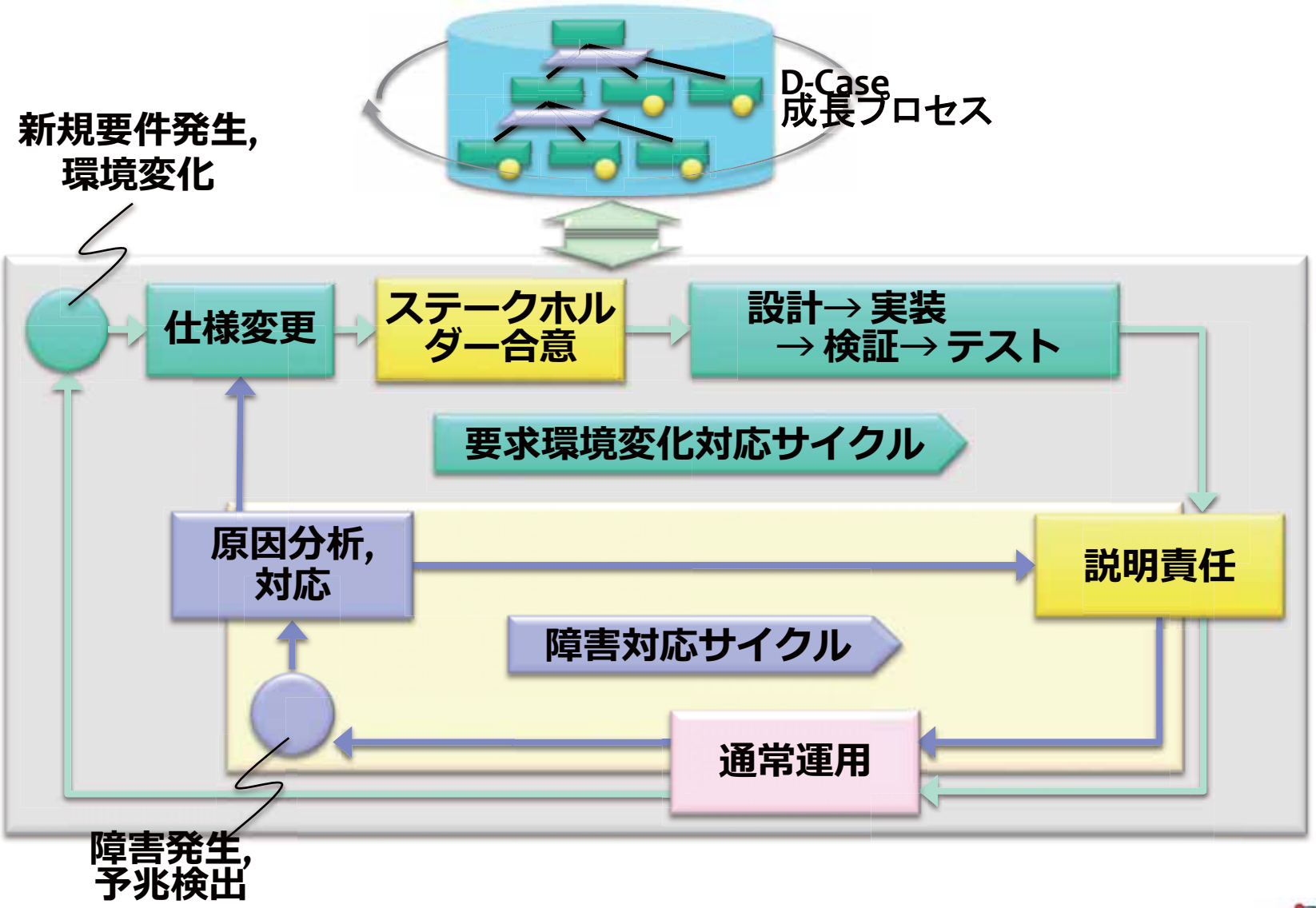


スクリプトが埋め込まれたD-Caseを受付システムに送ることにより、
合意内容の確実な実行を保証する。
詳細は次の発表で。
デモはD-25 DEOSブースの、D-Caseブースでしています

Challenges to Open Systems Dependability

- オープンシステムでは、すべてが変化する
- 変化に対応し、ディペンダビリティを維持し、合意することが、オープンシステムディペンダビリティである
- DEOSでは、変化を２種類に分類した
  - システム障害による変化
  - ステークホルダ要求・環境による変化
- これらの変化に対応するためのプロセス、その各フェーズで必要なアーキテクチャ・要素技術を開発中である
  - DEOSプロセスとD-fopsを中心としたDEOS要素技術
- cf. Resilience (Laprie他)

DEOSプロセス



詳細は次の発表で

D-Case's Challenges to Open Systems Dependability

- ステークホルダとシステムが変化に対応できることを、精緻に記述すること
  - DEOSプロセスによるディペンダビリティ維持と、システムの構成によるディペンダビリティ維持の組み合わせの精緻化

まとめ

- D-Case: ステークホルダ間のディペンダビリティ合意を記述するためのモデリング言語
- D-Case記述例
- D-Case Tools
- D-fopsとの連携(詳細は次の発表で)
- Challenge to Open Systems Dependability
  - DEOSプロセスとDEOS要素技術による達成
  - D-Case's Challenge = その精緻な記述