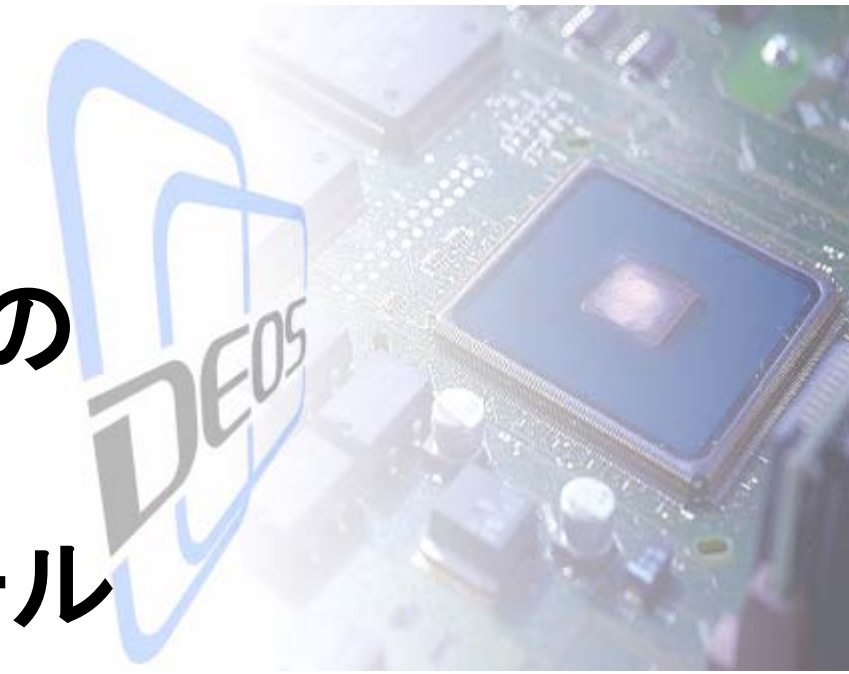
D-Case:
変化し続けるシステムの
ディペンダビリティ
合意形成の方法とツール

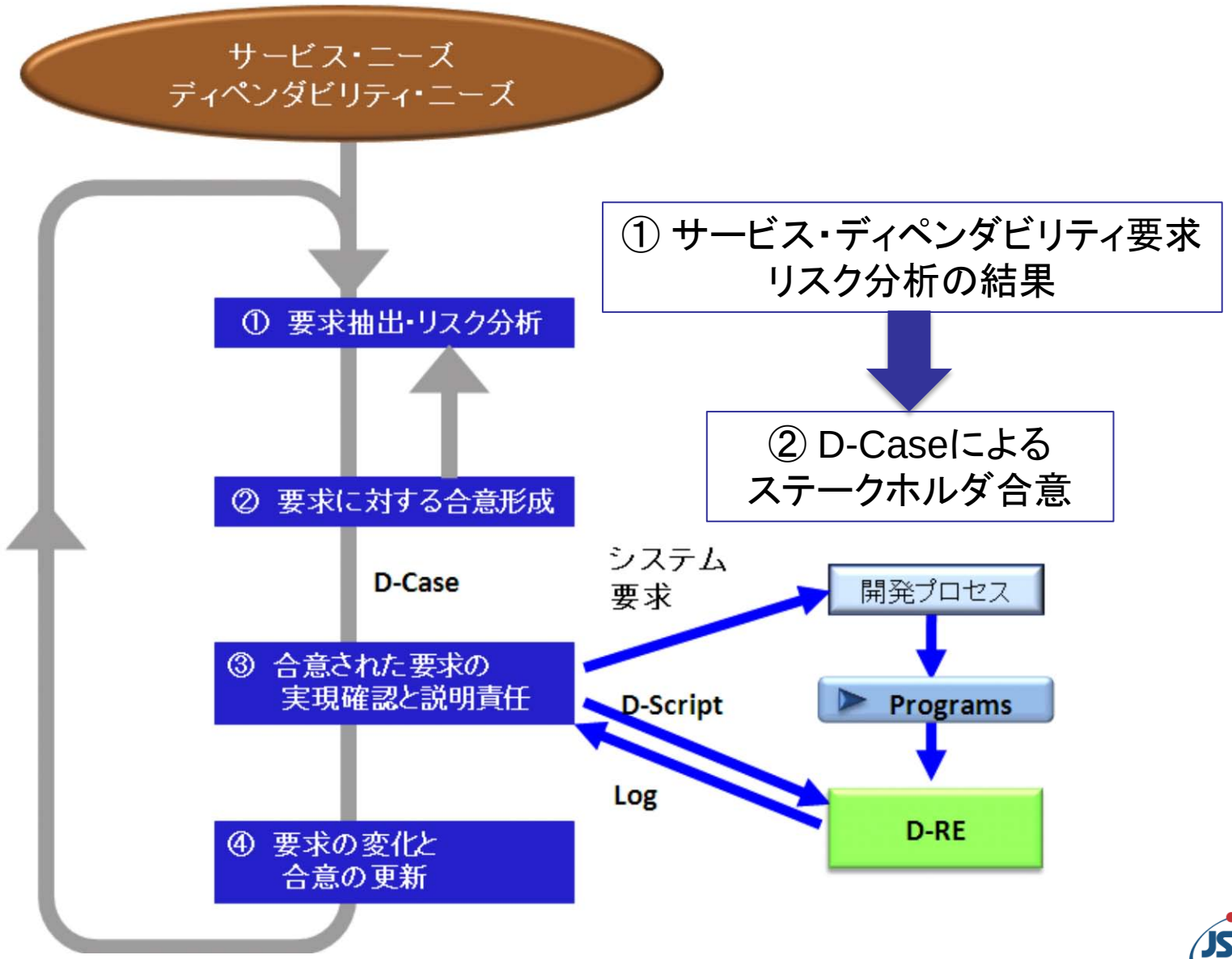


東京大学情報基盤センター
スーパーコンピューティング研究部門
松野裕
matsu@cc.u-tokyo.ac.jp

内容

- DEOSにおけるD-Caseの役割と特徴
- Safety Caseと、D-Caseの新規性
  - D-Case記述例
- 企業における事例
- D-Caseツール
- 今後：ISO26262などの認証支援とDEOSの国際展開
- まとめ

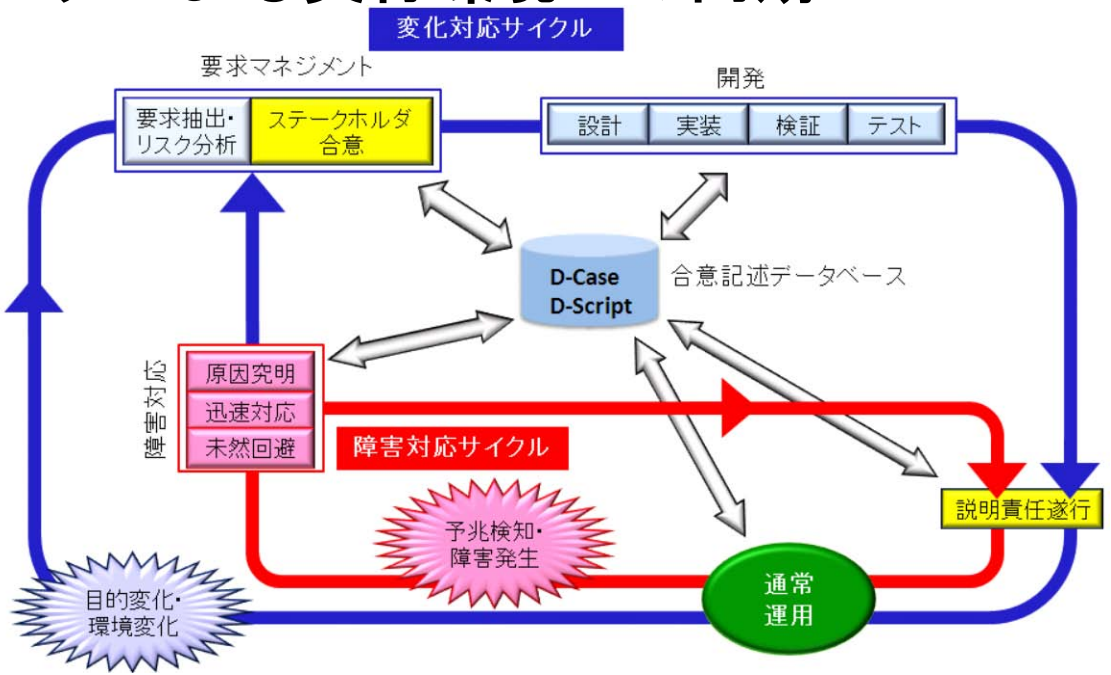
D-Caseの役割：合意形成のための手法とツール



D-Caseの特徴

DEOSプロセスの核である

- 変化対応サイクル
  - サービス・ディペンダビリティ要求、リスク分析、テスト・ベンチマーク結果、…の参照・更新
- 通常運用、障害対応サイクル
  - モニタリングによる実行環境との同期

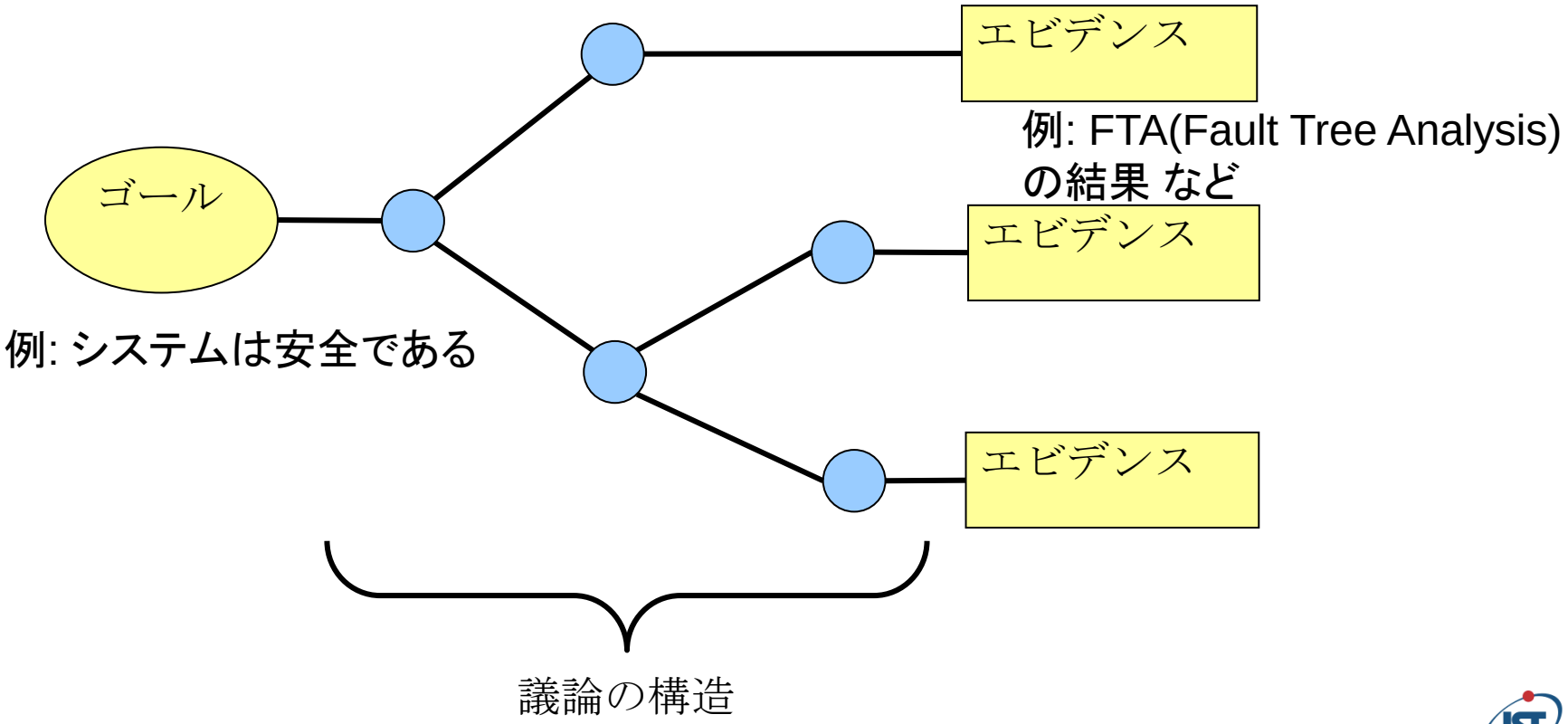


内容

- DEOSにおけるD-Caseの役割と特徴
- Safety Caseと、D-Caseの新規性
  - D-Case記述例
- 企業における事例
- D-Caseツール
- 今後：ISO26262などの認証支援とDEOSの国際展開
- まとめ

Safety Caseとは

- **システムの安全性を保証するために、エビデンスを元に、トップダウンに展開する文書形式**



Safety Caseの背景

- 1988年の北海油田事故(167名死亡)などを契機に、欧米で規格認証の際に提出が義務付けられるまでに普及
  - 手順のみでなく、なぜ安全性が保たれるのか、明示された議論で、エビデンスをもとに保証する。導入により北海油田における事故が減少
- ISO 26262 (TC22/SC3, 自動車の機能安全規格)の work product の一つ
- 現況
  - イギリスにおいては、高安全、軍事システムの調達に必須
    - MoD Defence Standard 00-56
  - アメリカ: US. Food and Drug Administration (FDA)
    - “A safety case is the best way to both document and review a submittal based on a risk management approach because the argument shows the proportionality of the mitigation”
  - 日本: ISO 26262の影響
    - “最大のインパクトは、安全性の根拠を、より説明しやすくするよう自動車メーカーに迫る点である。”
      日経エレクトロニクス2011.1.10

D-Caseの新規性

- 変化し続けるシステムに対応する
  - システムのモニタリングとの連携による、記述内容とシステムの挙動の一致
- いつでも、必要なとき、説明責任を果たす
  - 開発ツールなどとの連携による、システムのディペンダビリティのトレーサビリティの確保

D-Caseの主要なノード

ゴール

保証したい
こと、命題
例：
システムは
安全である

ストラテジ

ゴールを
サブゴールに
分けるときの
考え方
例：個別の障害ごとに
議論する

エビデンス

ゴールが
成り立つことを
最終的に
保証するもの
例：テスト結果、
運用事例など

コンテキスト

システムの状態、
環境など、ゴール
を議論するときの
前提など
例：リスク分析の
結果得られた
ハザードのリスト

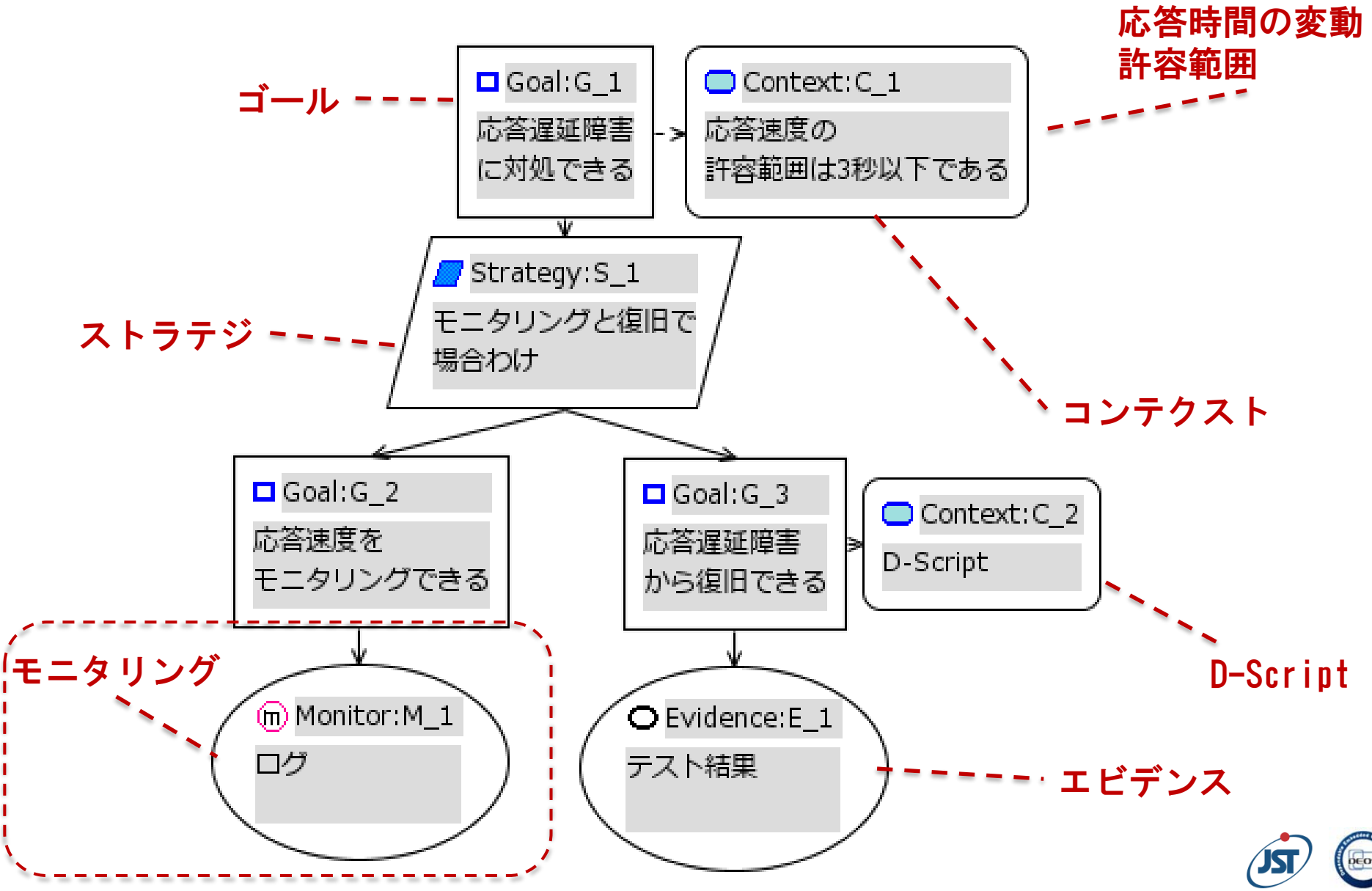
Safety Caseの表記法である、
Goal Structuring Notation
(GSN)を元にしている

新たに追加した
ノード

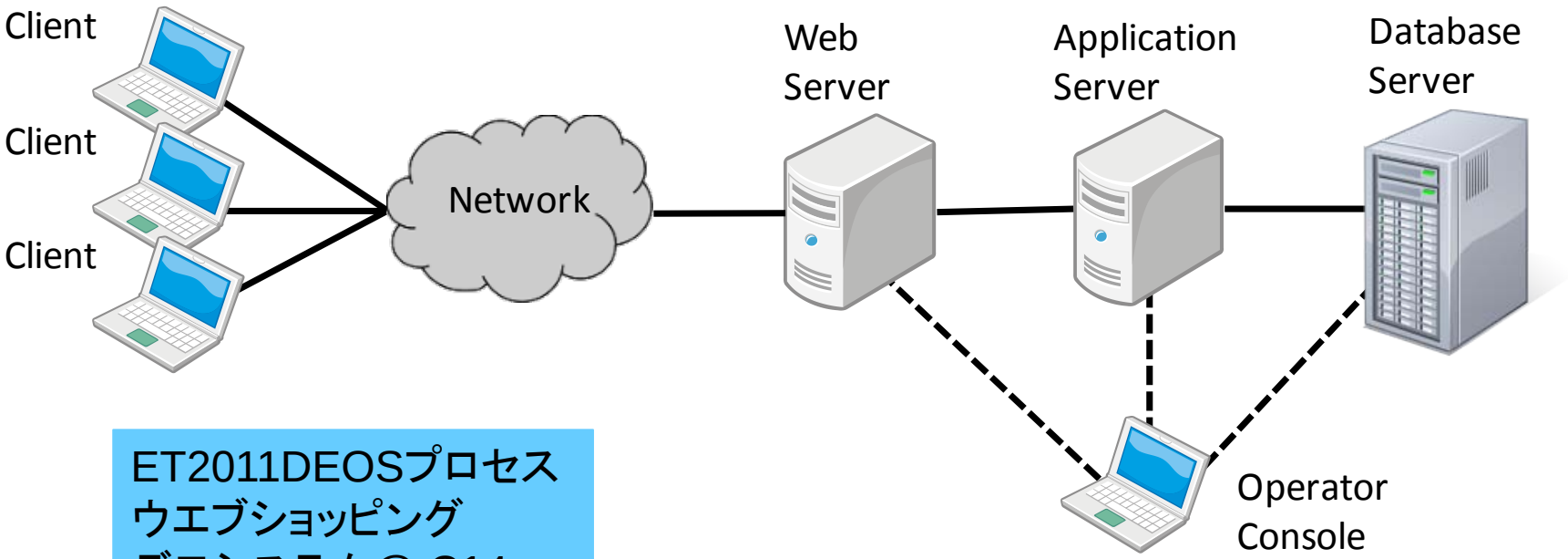
モニタリング

システムの
モニタリング結果
によるエビデンス

D-Caseの例


ゴール
Goal:G_1
応答遅延障害
に対処できる
Context:C_1
応答速度の
許容範囲は3秒以下である
応答時間の変動
許容範囲
Strategy:S_1
モニタリングと復旧で
場合わけ
ストラテジ
コンテクスト
Goal:G_2
応答速度を
モニタリングできる
Goal:G_3
応答遅延障害
から復旧できる
Context:C_2
D-Script
D-Script
モニタリング
Monitor:M_1
ログ
Evidence:E_1
テスト結果
エビデンス

D-Case記述例



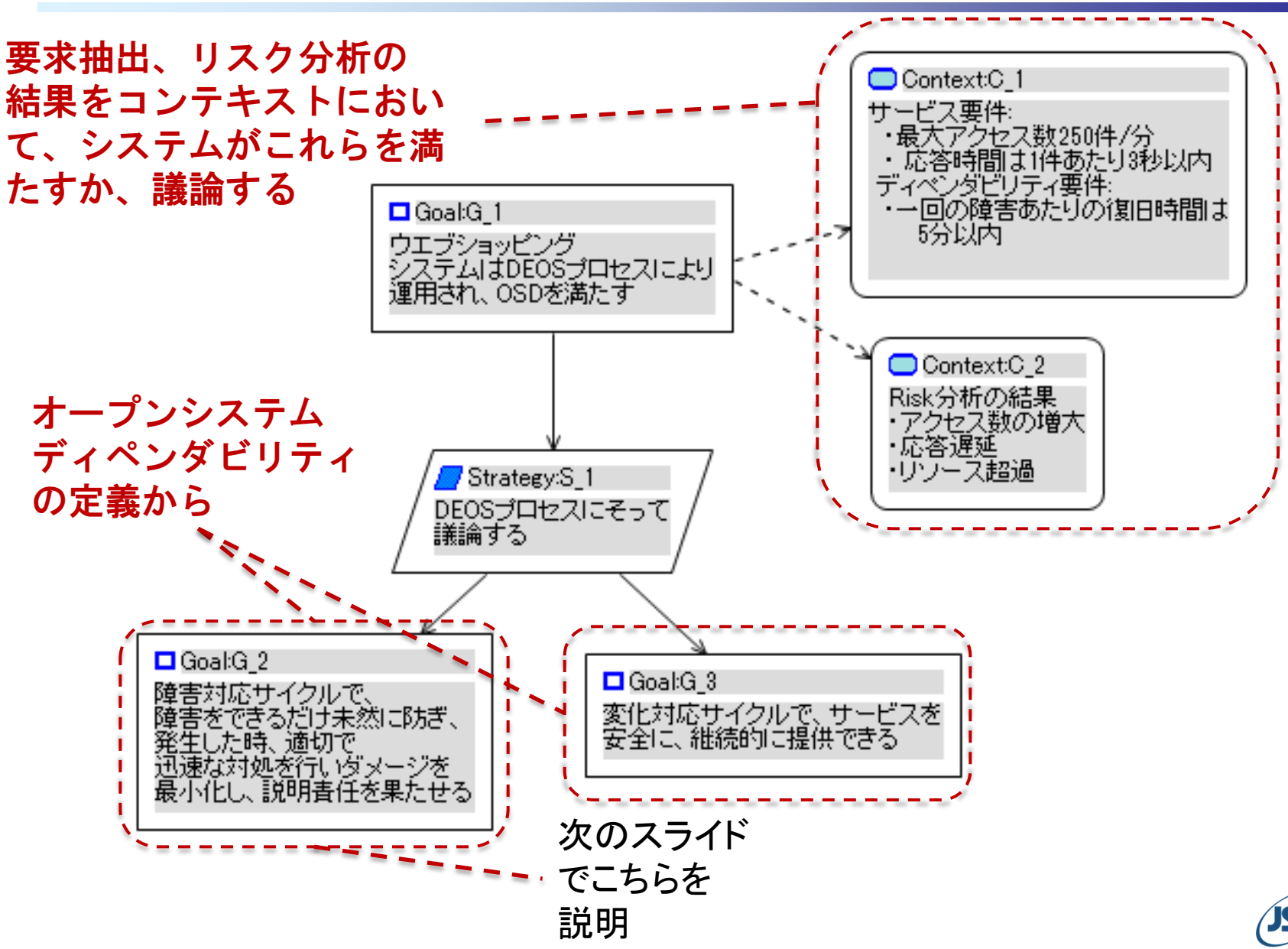
ET2011DEOSプロセス
ウエブショッピング
デモシステム@ C14

サービス要求
- アクセス数最大250件/分の規模の
  ウエブショッピングサービス
- 1件あたりの応答時間は3秒以内

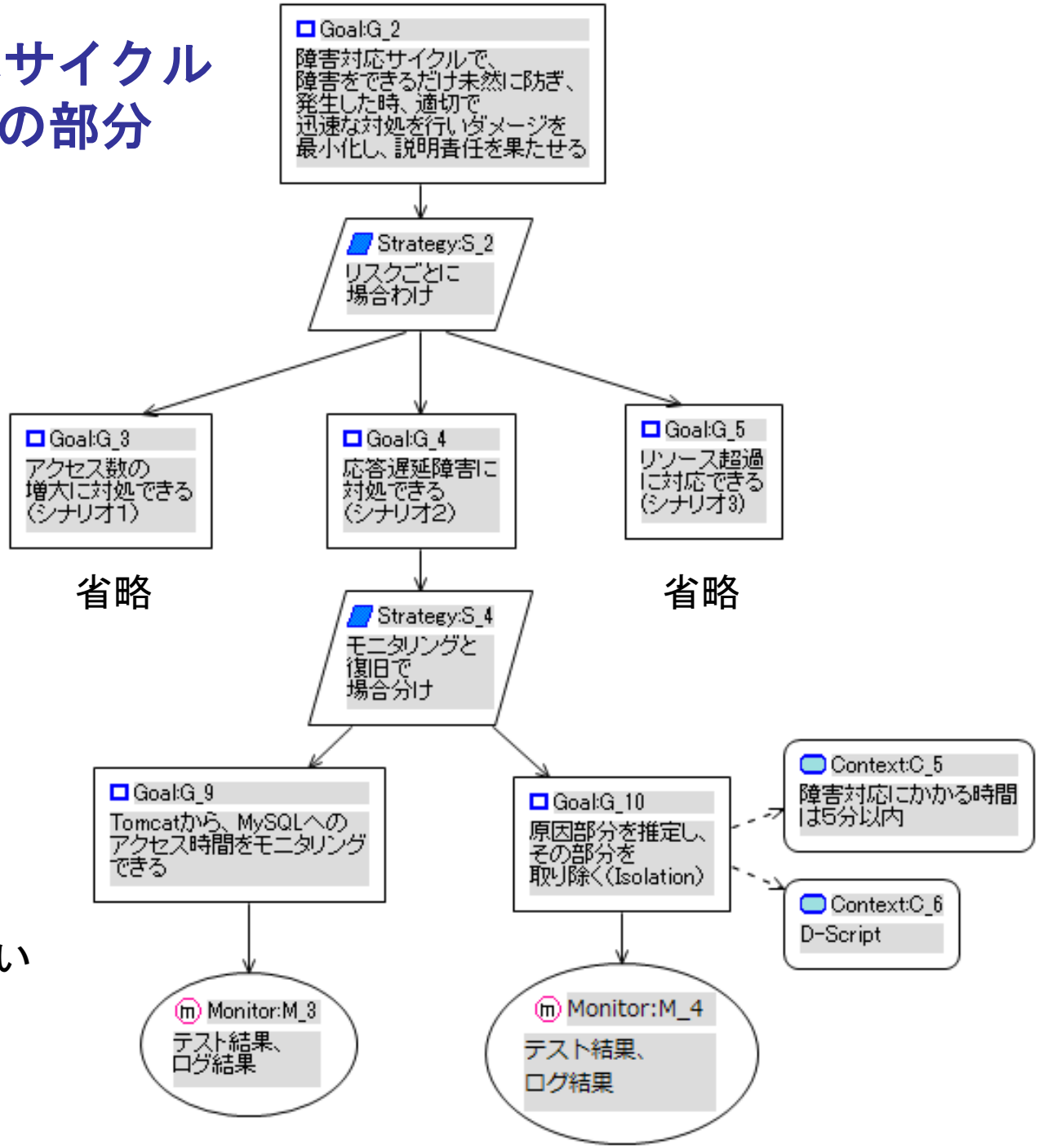
ディペンダビリティ要求
- 障害対処は5分以内

リスク分析の結果
- アクセス数の増大
- 応答遅延
- メモリなどの
  リソース超過

トップレベルのD-Caseの部分



障害対応サイクルのD-Caseの部分



くわしくは
ぜひC14ブース
にいらしてください

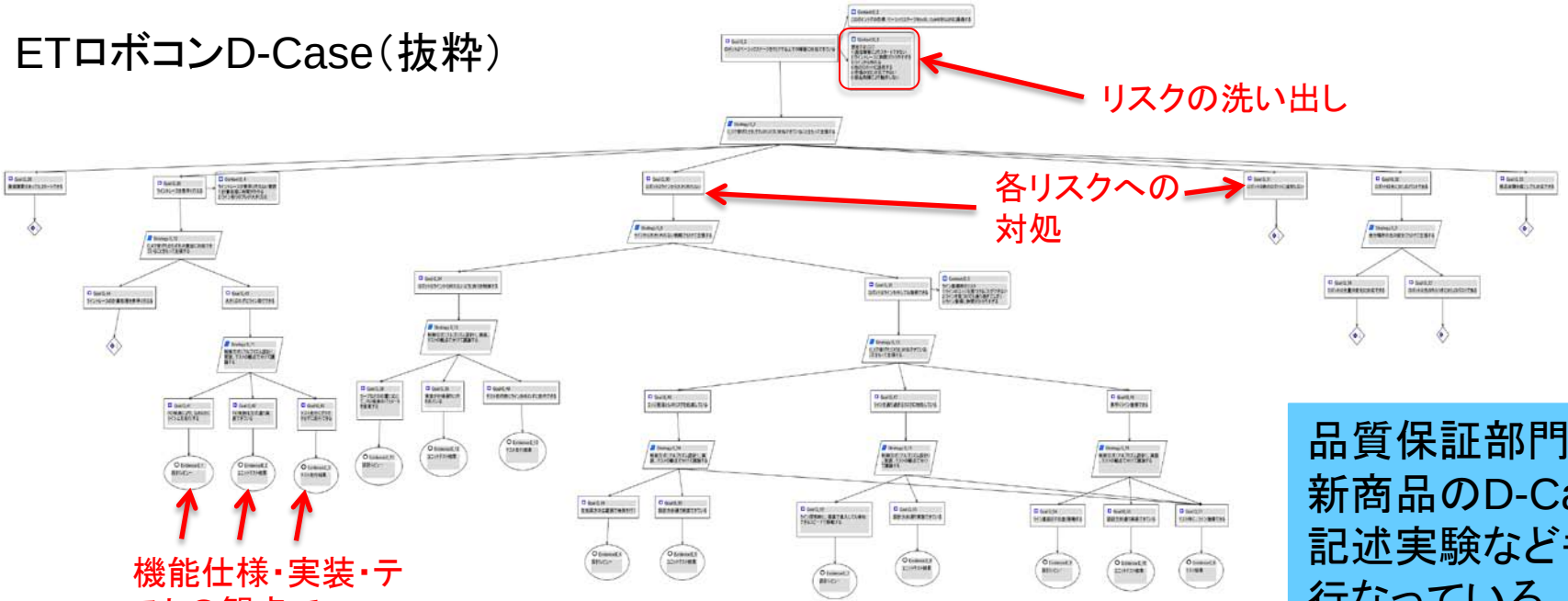
内容

- DEOSにおけるD-Caseの役割と特徴
- Safety Caseと、D-Caseの新規性
  - D-Case記述例
- 企業における事例
- D-Caseツール
- 今後：ISO26262などの認証支援とDEOSの国際展開
- まとめ

企業における事例 (1/2)

- ETロボコンにおけるD-Case記述実験
  - 企業参加チームをヒアリング
  - 各レースポイントごとにリスクを抽出し、対処方法を、機能仕様・実装・テストの観点で保証

ETロボコンD-Case（抜粋）



品質保証部門での新商品のD-Case記述実験なども行なっている

企業における事例 (2/2)

- ヒアリング結果

D-Caseへの評価	・議論やプロセスの振り返り・チェックをするにつかえそうだ。「この項目は検証の議論ばかりしているが、もっとリスクを低減する機能の議論をすべきだ」というようなことがわかるかもしれない ・作業やノウハウをプロセス化するのに使えそうだ ・ゴールとエビデンスの構造で、合意形成の状況や開発・運用の実施状況を把握できるのはよい
改善、要望点	・ツリー表示は大きくなると読みづらくなる。 ・エンドユーザなど全容を理解していない人が、ここから情報をよみとるのは負担が大きそうだ。全容の分かりやすさや見やすさ、項目の検索性、作りやすさを考慮してほしい

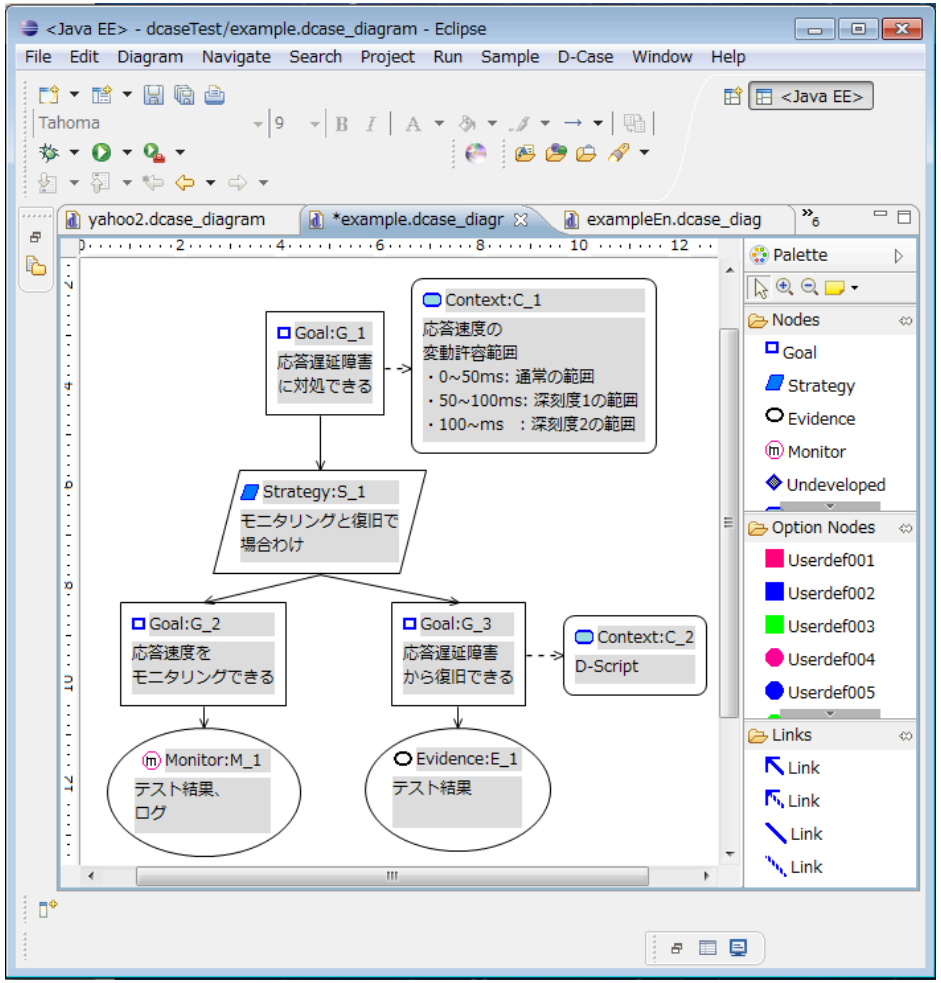
- DEOS側からのコメント
  - どのようなリスク分析手法が使われたのか？
  - リスクの列挙は十分か？
  - リスクの深刻度は考慮されているのか？
  - エビデンスの確認は、きちんとされているか？
  - 運用時だけでなく、要件定義、設計、開発、テストがきちんとされたか、議論されているか？

内容

- DEOSにおけるD-Caseの役割と特徴
- Safety Caseと、D-Caseの新規性
  - D-Case記述例
- 企業における事例
- D-Caseツール
- 今後：ISO26262などの認証支援とDEOSの国際展開
- まとめ

ツール紹介：D-Case Editor

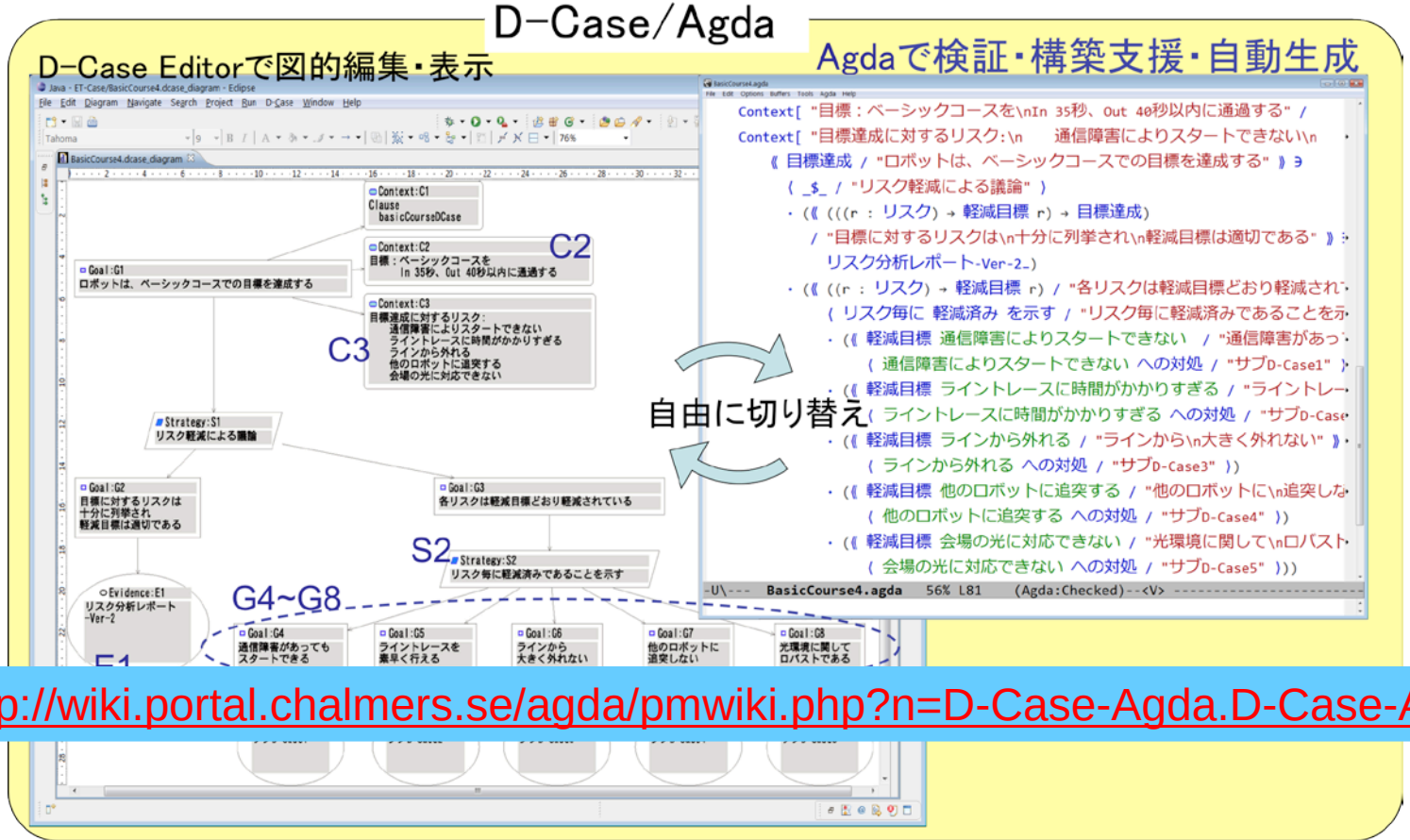
- EclipseプラグインとしてD-Case描画ツールを実装
- D-RE, DS-BenchなどのDEOSツール、Redmineなどの開発ツールとの連携機能をプロトタイプ実装
- 過去の事例やテンプレートを蓄積し、ネットワーク経由で参照可能なD-Case DBを実装を予定
- フリーウエアとして公開中。オープンソース化、商用化などを検討中



http://www.il.is.s.u-tokyo.ac.jp/deos/dcase/

ツール紹介：D-Case/Agda 整合性検証ツール

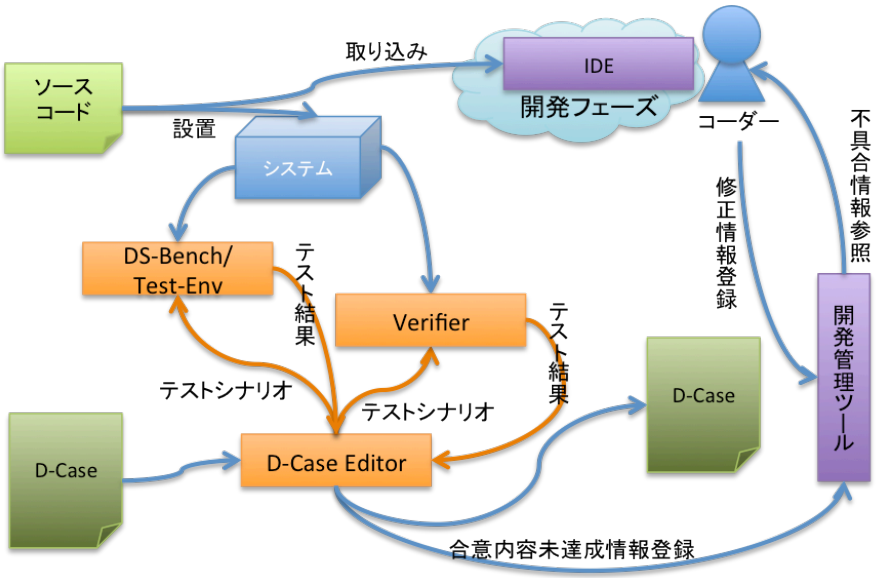
- 定理証明器AgdaによるD-Case構築支援
- 変化で生じる、見落としがちなD-Case不整合箇所を自動検出
  - 例: 考慮すべきリスクがすべて、議論されているかチェックする



http://wiki.portal.chalmers.se/agda/pmwiki.php?n=D-Case-Agda.D-Case-Agda

ツール連携

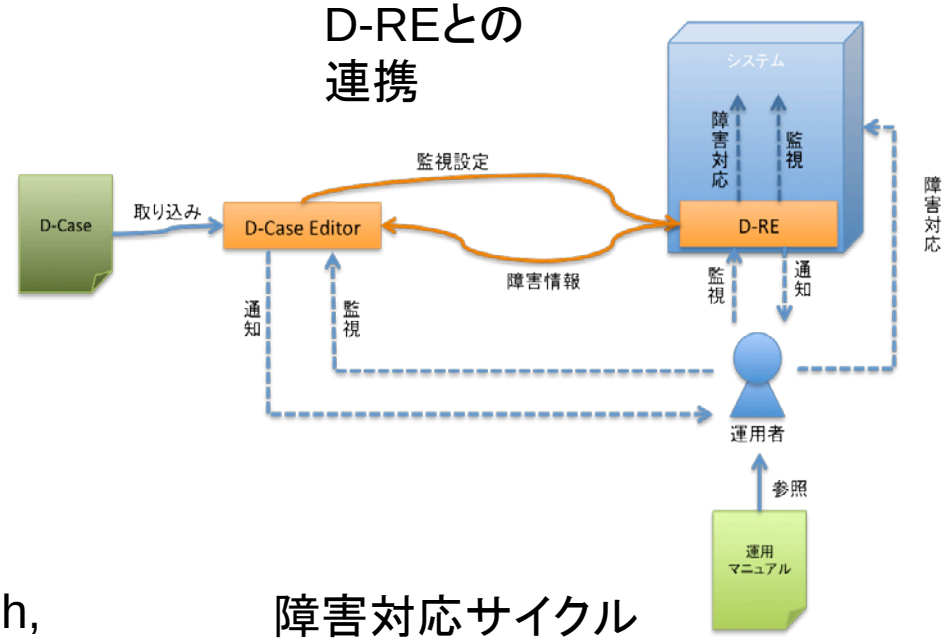
- D-Case利用シーンを提案する開発ツール連携
  - ベンチマークツールと連携して合意したディペンダビリティ要件の確認検証
  - 監視/運用ツールと連携して動作中システム自動障害回復



検証/テストフェーズ

DS-Bench,
Verifier
との連携

D-REとの
連携

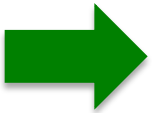


障害対応サイクル

今後：国際規格認証への応用とDEOSの国際展開

- ISO 26262などの認証支援
  - 要求事項をD-Caseで整理し、ISO26262のためのD-Caseパターンを作成予定
  - D-Case Editorから、パターンを利用できるようにする
- Object Management Group (OMG), Open Groupなどにおける国際標準化活動
  - Safety CaseメタモデルのOMG標準化に参加中
    - D-Case標準化へ
  - 消費者機械OMG標準化(共同提案中)
    - DEOS国際標準化へ

ISO26262など
・開発プロセスにおける検証・テストが中心
・欧米が中心



DEOS
・変化し続けるシステムの合意と説明責任が中心
・日本から提案

まとめ

- DEOSにおけるD-Caseの役割と特徴
- Safety CaseとD-Case
- 企業における事例
- D-Caseツール紹介
- 今後

企業のみなさまとの共同
研究をぜひお願いします！