（一般社団法人）ディペンダビリティ技術推進協会
第一回オープンシンポジウム

DEOSの成果とその活用

2014年6月25日

（一般社団法人）ディペンダビリティ技術推進協会理事長
（株式会社）ソニーコンピュータサイエンス研究所
所　眞理雄

DEOSの成果

- 変化しつづけるシステムを対象としたこと
  - 長期運用・連続運用
  - 目的、環境、技術、法規制が変化
  - システム境界が変化　(外部システムとの接続)
  - 設計・開発と運用を分けられない

- 説明責任を果たせること
  - ステークホルダ合意に基づくシステムの設計・開発・運用
    - Cf. 妥当性検証に基づく設計開発・運用
  - ライフサイクルを通じた一元管理

DEOSの成果（2）

変化しないシステム

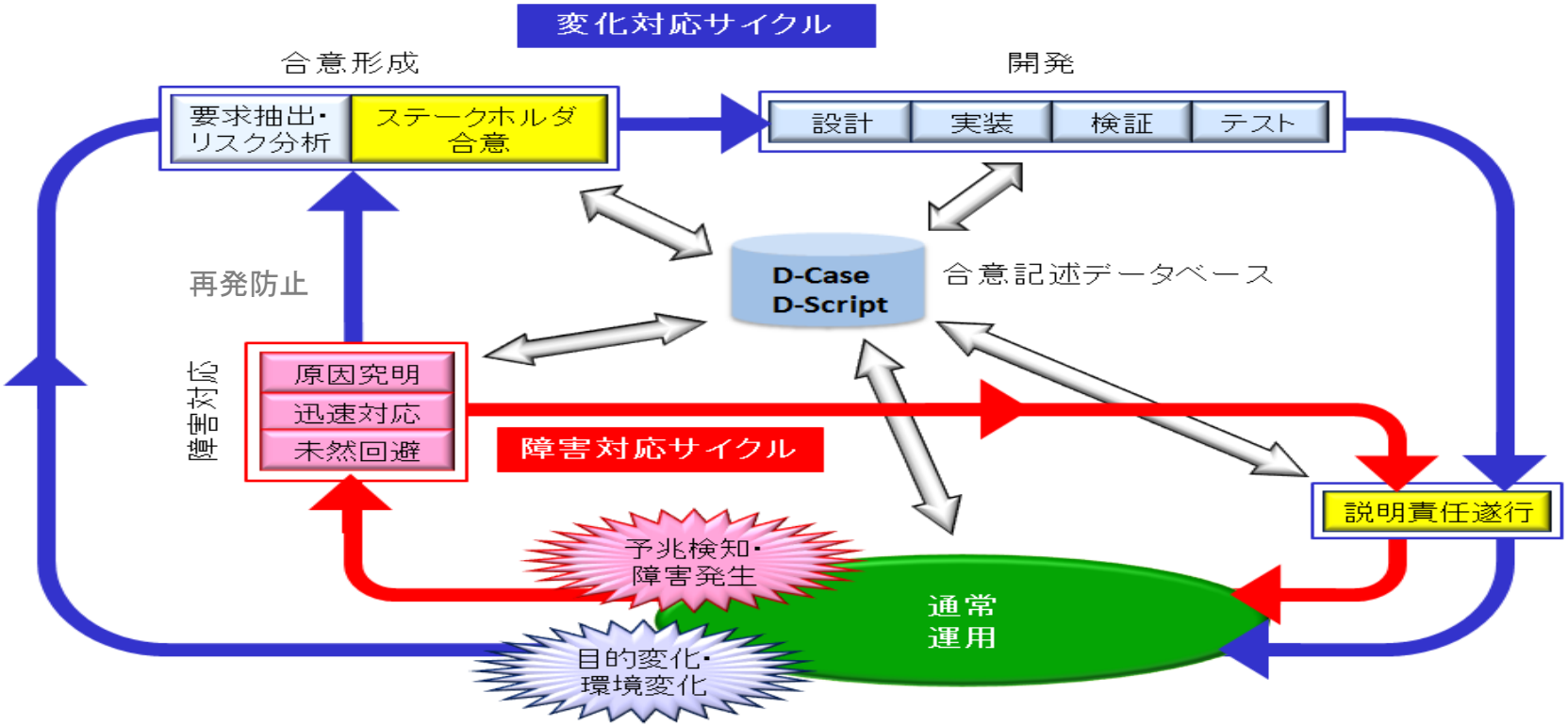
- ある一定期間システムの目的やシステムを取り巻く環境は変化しないと仮定
- 設計・開発フェーズと運用フェーズが分けられる
- 設計が正しいと仮定
- 検証・妥当性確認によるプログラム開発
- 検証・妥当性確認による説明責任　(設計の正しさについてはステークホルダー合意）

変化しつづけるシステム

- システムの目的やシステムを取り巻く環境は常に変化する
- 設計・開発フェーズと運用フェーズが分けられない
- 「正しい」とは何か
- ステークホルダー合意に基づく設計・開発と運用
- 設計・開発並びに運用に関する合意に基づく説明責任

DEOSプロセス

- 開発と運用の一体化
- 変化に対応するサイクルと障害に対応するサイクルからなる反復的なプロセス
- 再発防止のため、障害対応サイクルから変化対応サイクルへの経路
- ステークホルダ間の合意形成とその記録をベースとした説明責任の達成
- D-Scriptによる障害対応



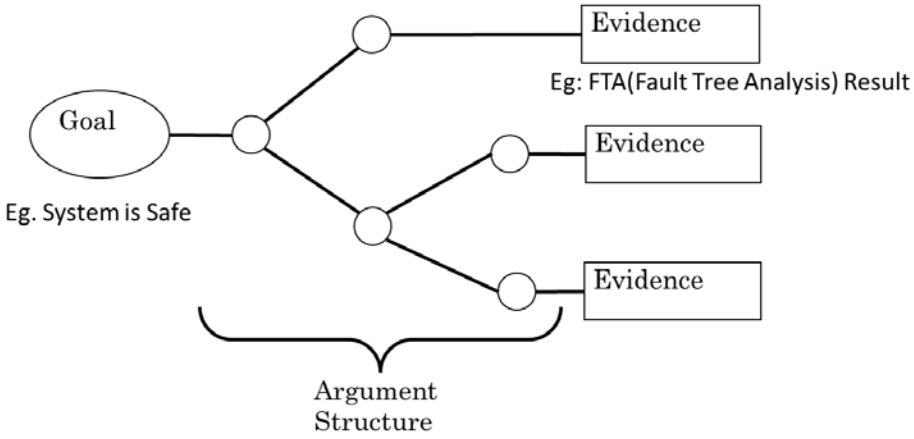
DEOSプロセス

Assuredness（確信）によるステークホルダ合意の形成

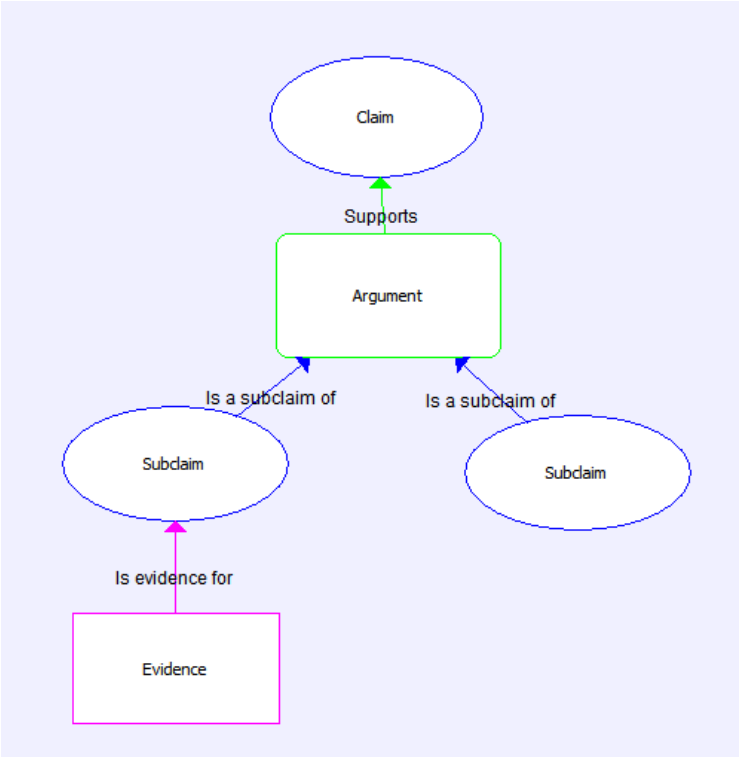
- **Assurance (確信)は構造化された議論と要求が具体的な方法で実現されていることを示す信頼に足るEvidence（根拠あるいは証憑）が示されることによってなされる。**
  - **要求が安全性に関するものであればSafety Assurance、ディペンダビリティーに関するものであればDependability Assuranceである。**

1. **Assuranceの対象はGoal（あるいはClaim）として示される。**
2. **GoalはSub-Goalに分割される。Sub-Goalはさらに下位のSub-Goalに分割されうる。すべてのSub-Goalが満たされたときにその上位のGoalが満たされる。各Sub-Goalは適切なEvidenceによって満たされる。**

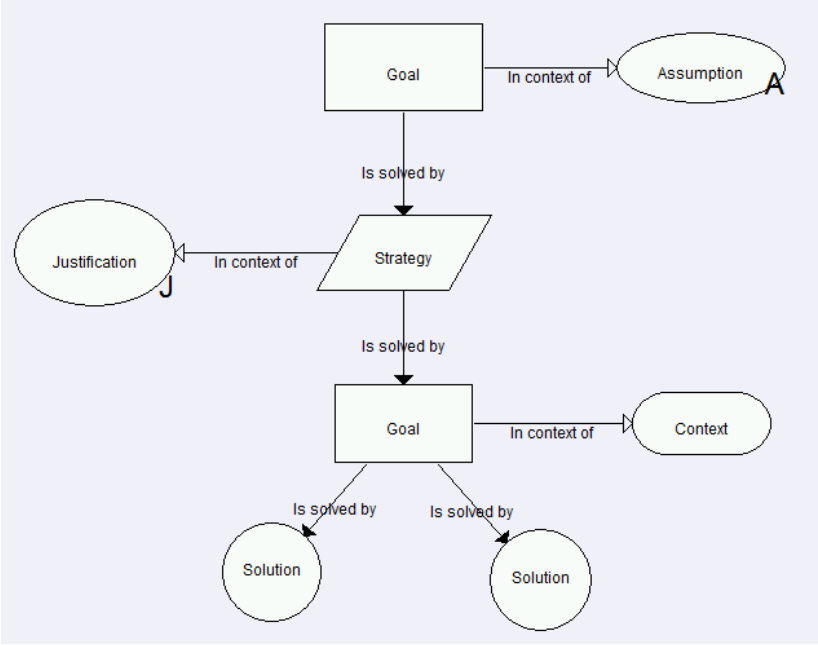
Assuredness の記法例



Abstract Assurance Case Structure
See ISO/IEC 15026



CAE Graphical Notation
(www.adelard.com/asce/choosing-asce/cac.htm)

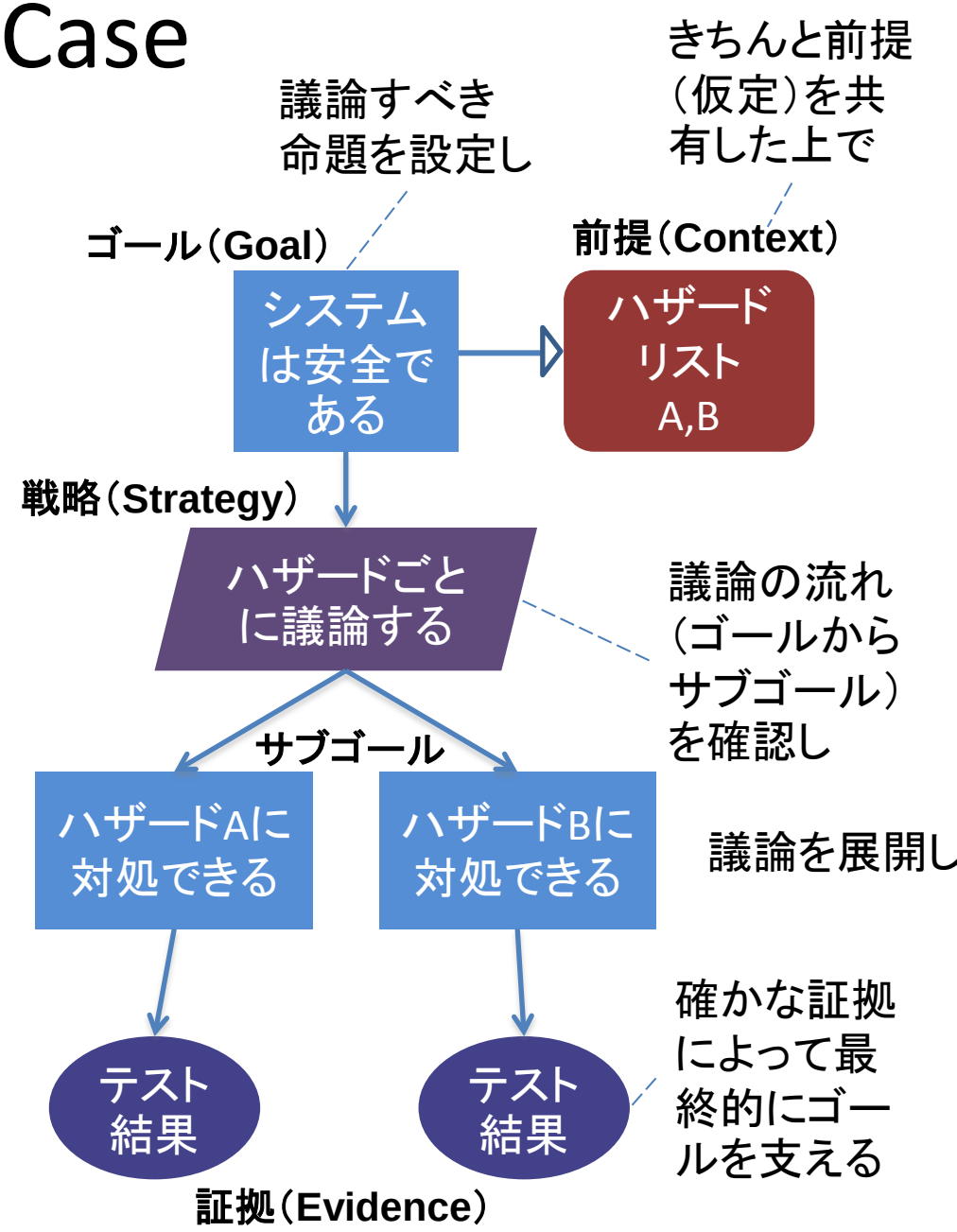


Graphical Notation of GSN
(www.adelard.com/asce/choosing-asce/gsn.htm)

D-Case

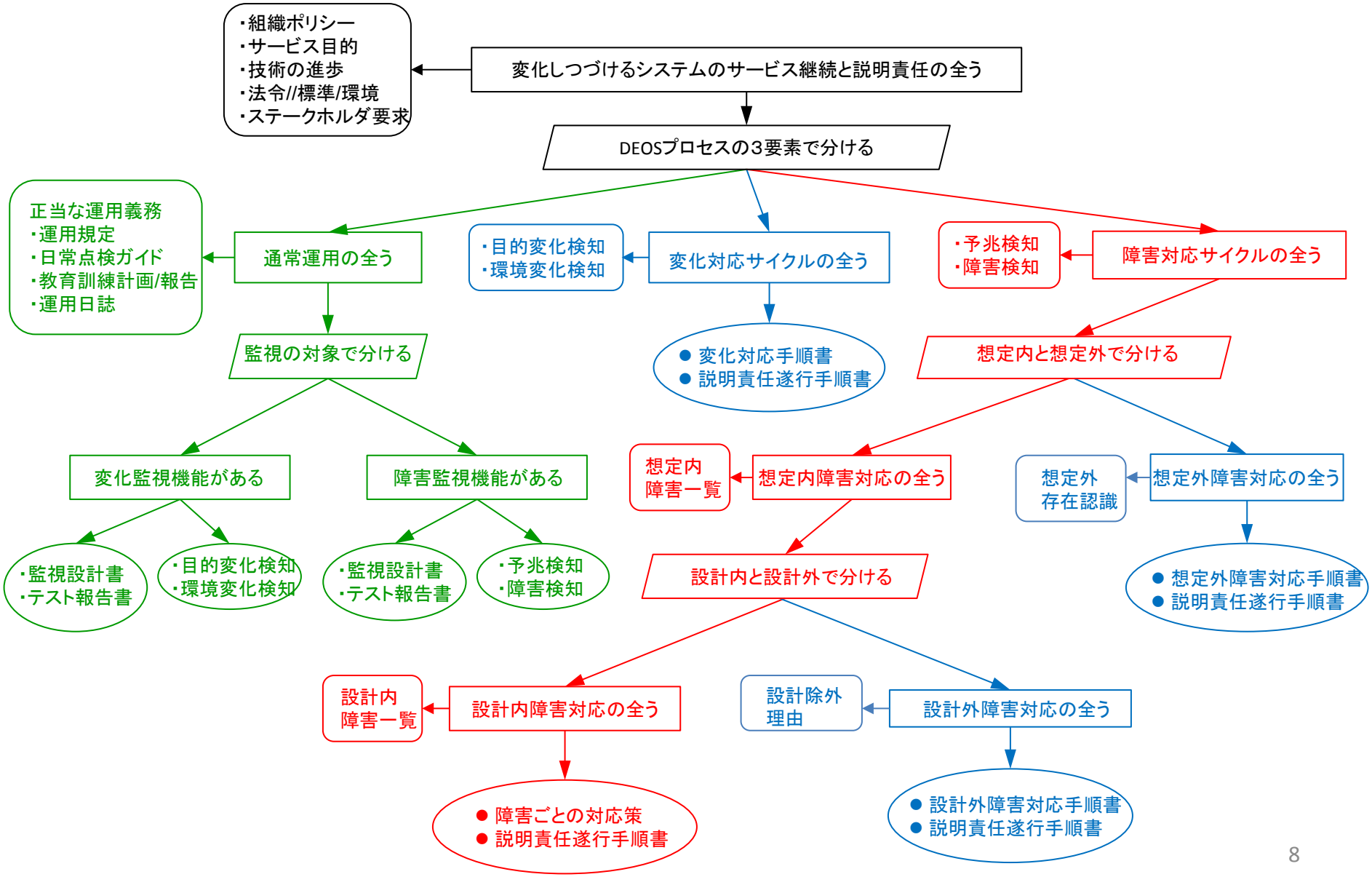
ライフサイクルを通じて、システムのディペンダビリティをステークホルダが合意し、社会に説明責任を果たすための手法とツール

- Assurance Caseをベースとした議論のための方法・ツール
- 開発・運用を通じて一貫して活用
- Goal、Strategy、Context、Evidence (incl. Monitoring、External)、および Undeveloped NodesからなるGSN (Goal Structuring Notation) による表現
- 自然言語あるいはSBVRやAgdaなどの疑似自然言語による記述
- D-Case記述の歴史的な記録（合意に基づく変更履歴の記述）が説明責任遂行を支援



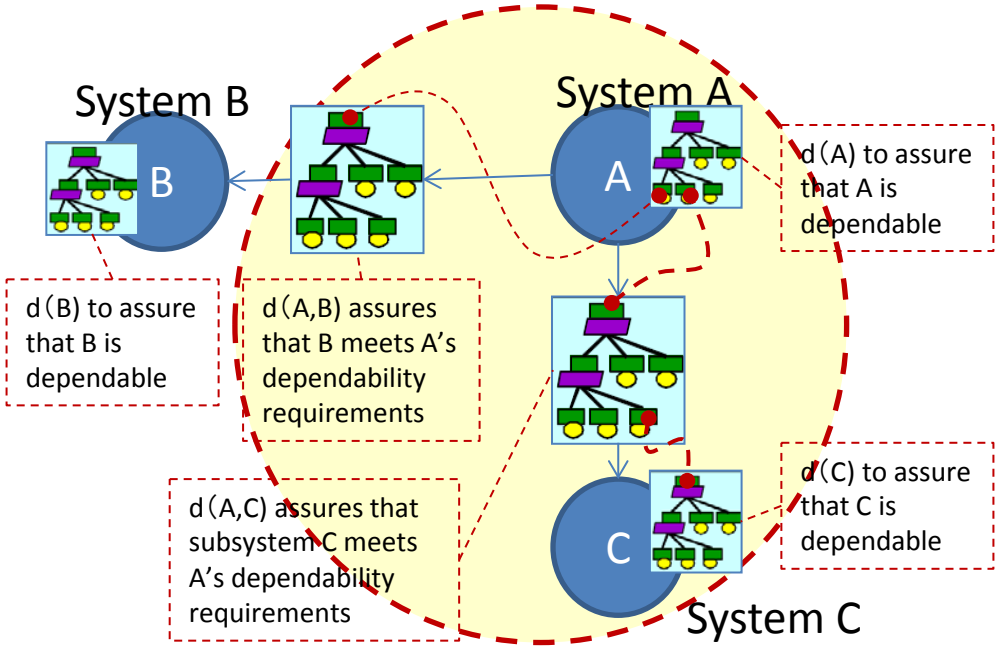
出展　D-Case超入門、2013 D-Case委員会（http://www.dcase.jp）

D-Case によるDEOS プロセスの記述



外部システムとの接続

- 出来あいのソフトウェア
- 以前に開発されたレガシーコード
- ネットワークを経由した外部サービス
- Cloudなど未知の環境上でシステムが稼働
- モジュール化による巨大D-Caseの記述
- D-Case を書いてシステムを開発する “Forward Engineering” と既開発システムからD-Caseを書く “Reverse Engineering”

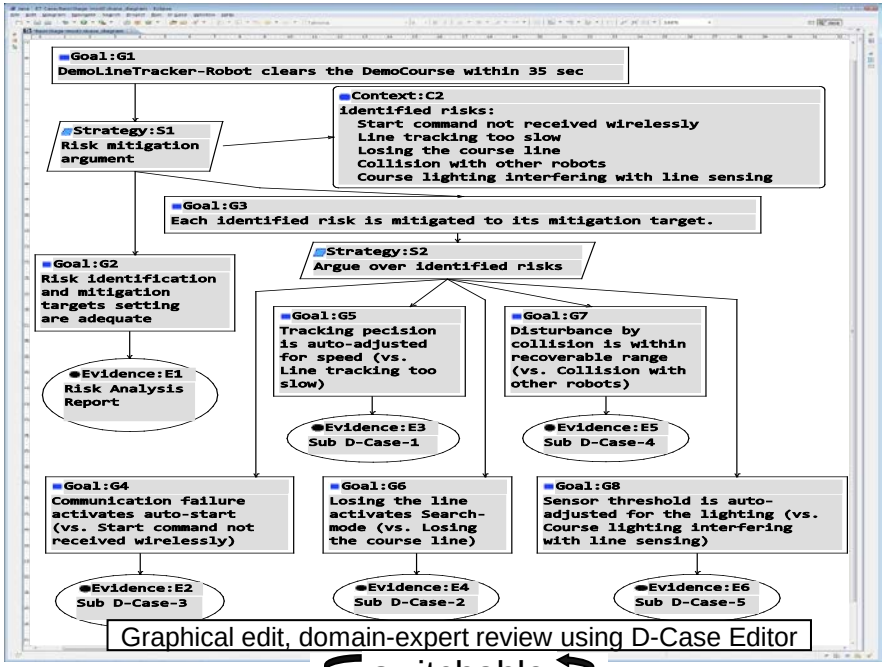


巨大化したD-Caseの無矛盾性の担保

- 実用システムになるとノード数は数千を超える。ノード数1万やそれ以上に対しても実利用できなければならない。(モジュール化とコンポジショナリティ)
- 変化に対応するごとに、新しいD-Caseに変更される。この時、そのD-Caseが“矛盾”が無いものであるかどうか、チェックできなければならない。
- オープンシステムに対しては“完全性”は期待できず、“矛盾”の定義も難しい。
- 形式的手法は役に立つのか？

- 新たな考え方・ツールの必要性:　D-Case in Agda
- 議論部分だけでなく、オントロジー部分(語彙と定義)を定式化することで機械検査を可能にした

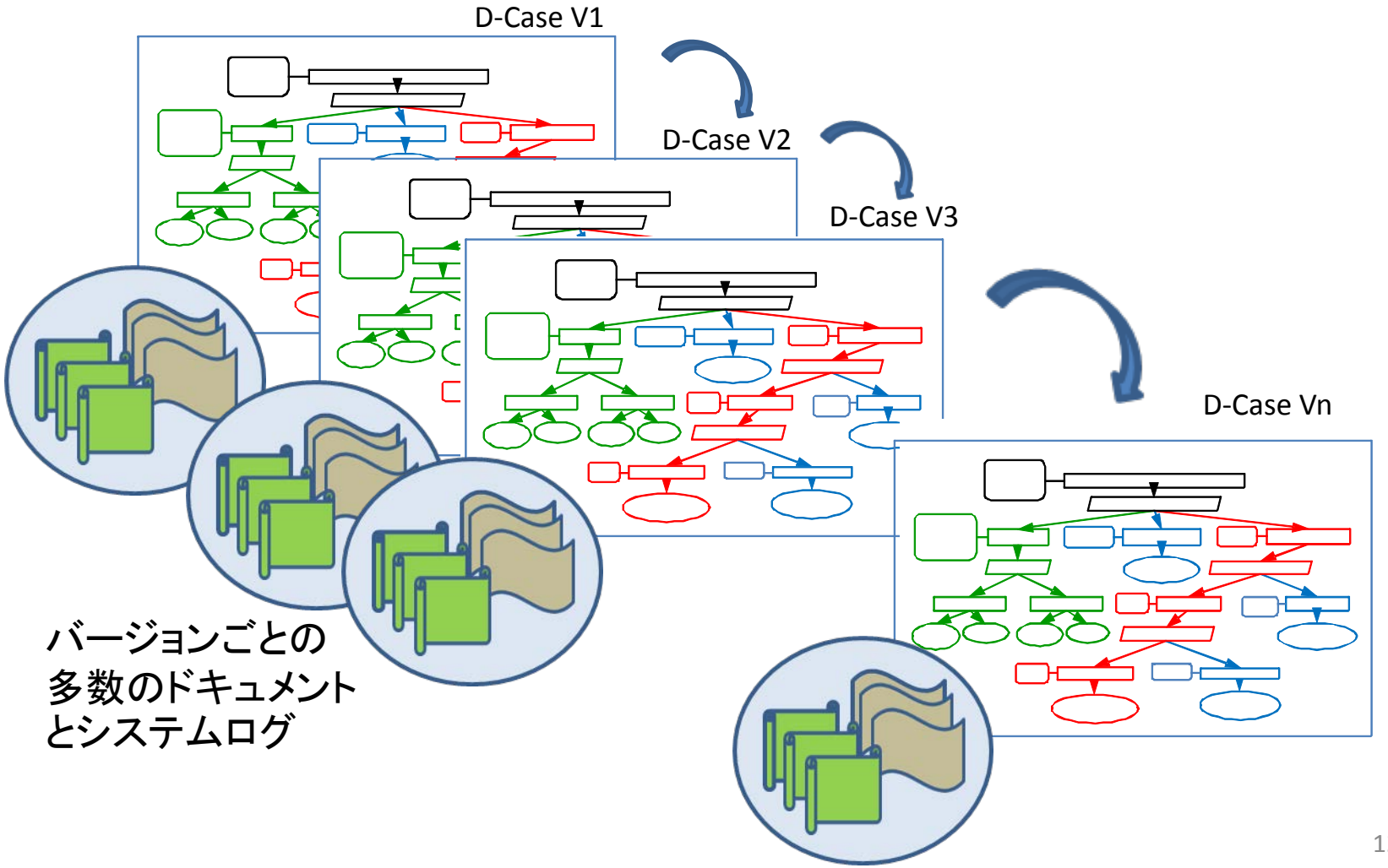
D-Case in AgdaによるD-Case Verification




```
⟪ DemoGoal "35 sec"
/ "DemoLineTracker-Robot clears the DemoCourse within 35 ·
Context[ "identified risks:\n\ \  Start command not recei·
/ ⟨ _$_ / "Risk mitigation argument" ⟩
  · (⟪ (R.AllMitigated → R.Objective) / "Risk identificat·
     ∋ ⟨ Risk-Analysis-Report / "Risk Analysis Report" ⟩)·
  · (⟪ ((x : Identified-Risk) → Mitigated x) / "Each iden·
     ∋ ⟨ R.riskCase Mitigated / "Argue over identified ri·
       · (⟪ Mitigated Cmd-not-received / "Communication f·
          ∋ ⟨ sub-d-case Cmd-not-received / "Sub D-Case-3·
       · (⟪ Mitigated Tracking-too-slow / "Tracking pecis·
          ∋ ⟨ sub-d-case Tracking-too-slow / "Sub D-Case-·
       · (⟪ Mitigated Losing-line / "Losing the line acti·
          ∋ ⟨ sub-d-case Losing-line / "Sub D-Case-2" ⟩⟩)
       · (⟪ Mitigated Collision-with-other-robots / "Dist·
          ∋ ⟨ sub-d-case Collision-with-other-robots / "S·
       · (⟪ Mitigated Course-lighting-interfering-with-li·
          ∋ ⟨ sub-d-case Course-lighting-interfering-with·
]
-U\**-  BasicStage-mod2.agda    56% L99     (Agda:Checked)--<
```

合意記述データベース

- D-caseによる合意の記述やシステム状態の履歴を如何に保存し、説明責任遂行を支援するか?

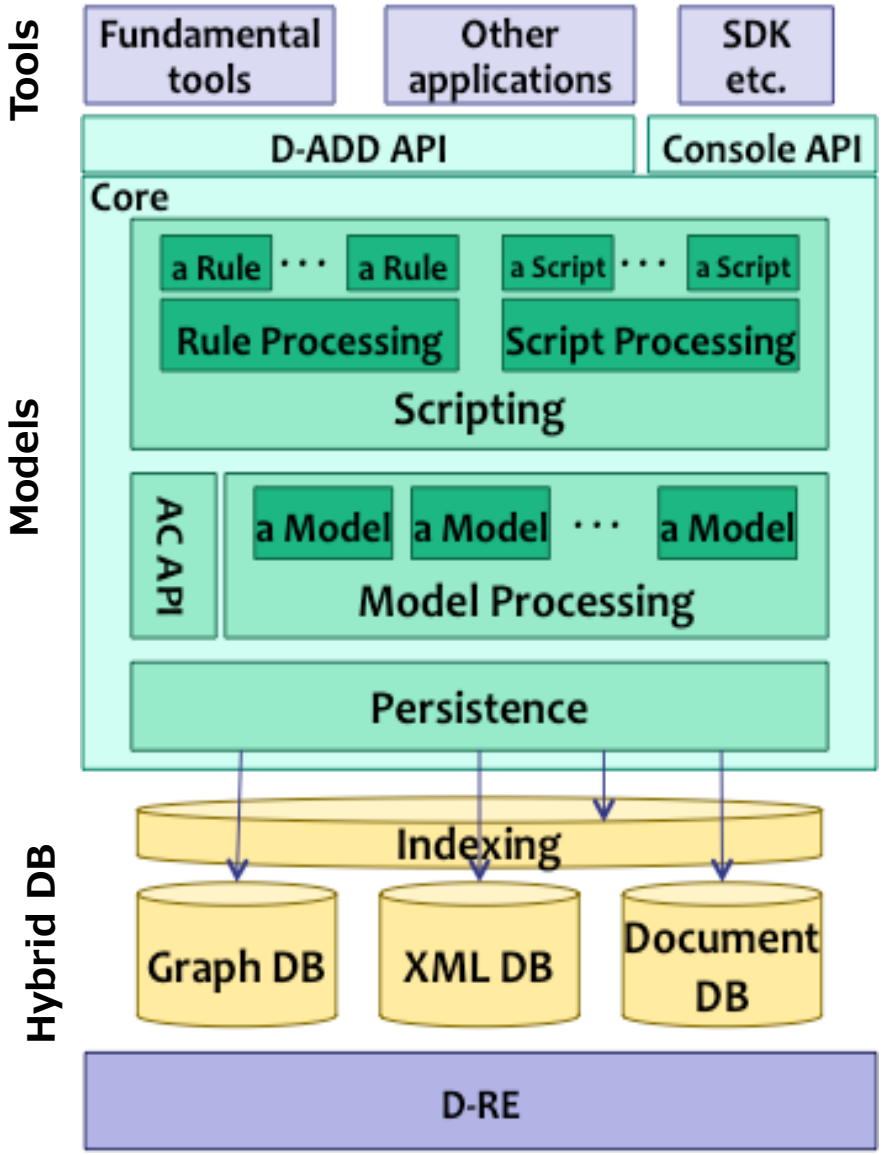


合意記述データベースの構造

- **Supporting Consensus Building**
  - D-Case修正時の影響範囲の明確化
  - 多人数でのD-Case開発手法
  - ステークホルダの責任範囲の明確化
- **Supporting Accountability Achievement**
  - 合意形成と説明責任の連携を担保
  - 障害時の原因ノード探索、齟齬推測
  - 対応策の合意形成支援
  - 対応策の開発・導入支援

The Structure of D-ADD

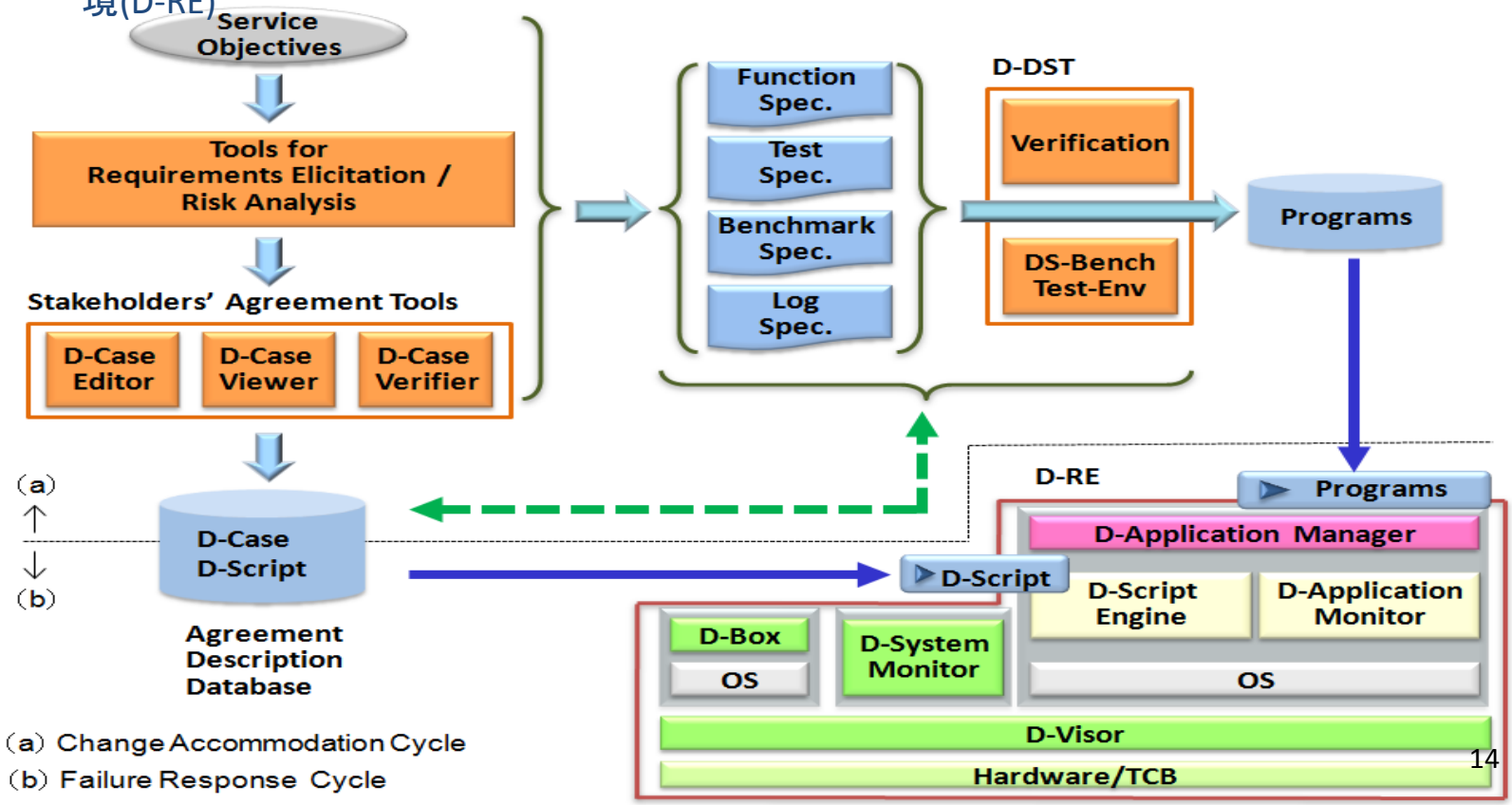
- **Tools**
  - Consensus Building
  - Accountability Achievement
- **Models**
  - Models and Rules
  - Persistence
- **Hybrid DB**
  - Connecting various DB by indexing



DEOSアーキテクチャと要素技術

DEOSプロセスの実行を支援するDEOSアーキテクチャ

- 要求マネジメントとステークホルダー合意を支援するためのツール (D-Case, D-Case Tools)
- 要求マネジメントプロセスを支援し、D-Caseを安全に維持するAgreement Description Database (D-ADD)
- 変化に対応できる開発・運用を実現するスクリプト言語 (D-Script)
- プログラム検証、ベンチマーキングなどを支援するDEOS開発支援ツール(D-DST)
- プログラムを実行、システムの状態をモニターして記録、障害に対処するためのDEOS実行環境(D-RE)



DEOS技術の利用状況

- ローコスト衛星システムのD-Case記述（慶大白坂准教授）
- ファイルサーバーシステムのD-Case記述（2000ノード超：D-Case in Agda⇔D-Case editor）＠神奈川大学
- D-Case講習会の開催：　多数の企業の参加と実問題へのD-Caseによる記述実験（名大、電通大）
  - 自動車エンジン制御開発への適用（トヨタ）
  - 超小型人工衛星への適用(NESTRA)
  - ロボットETロボコンへの適用　伊東　敦　氏 (富士ゼロックス)
  - ロボットETロボコン要件定義宇都宮 浩之氏（デンソークリエイト）
  - その他、非機能要件保証、受入れテスト十分性保証など
- 2足歩行ロボットへのD-RE/ART-Linuxの適用（産総研）
- 科学未来館の館内を自由に走行させて来館者と触れ合う「人と共生するロボット」の開発や「自動走行車」の開発にDEOSプロセスを利用し、現在運用中（産総研）

主なDEOS要素技術・ツール群

- ステークホルダ合意形成支援ツール
  -> D-Case Editor
- Webブラウザ版 D-Case Editor
  -> D-Case Weaver
- パワーポイント用 D-Case ステンシル
  -> D-Case Stencil
- D-Case整合性検査ツール
  -> D-Case/Agda
- D-Script （ D-Caseの記述を基にアプリケーションプログラムを動的に制御）
  -> 準備中
- D-ADD （ DEOS Process/D-Caseを支えるりポジトリー）
  -> 準備中
- ソフトウェア検証ツール
  -> モデル検査器
- D-Caseモデリング環境連携
  -> D-Case OSLC
- テスト支援ツール
  -> DS-Bench/Test-Env (DS-Bench/D-Cloud)
- シングルIPアドレスクラスタ
  -> Dependable Single IP Address Cluster (SIAC)
- 仮想マシンモニタとOS監視ツール
  -> D-Visor + D-System Monitor
- 改竄検知機能付き記録装置
  -> D-Box
- システムレコーダー
  -> System Recorder
- DEOSを実現するサービスを提供するための実行環境
  -> DEOS Runtime Environment (D-RE)

DEOS HP DEOSを支える技術:
http://www.jst.go.jp/crest/crest-os/osddeos/tech.html

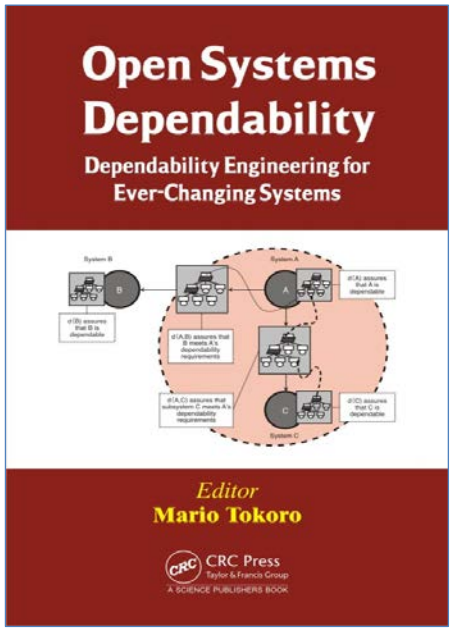
標準化活動

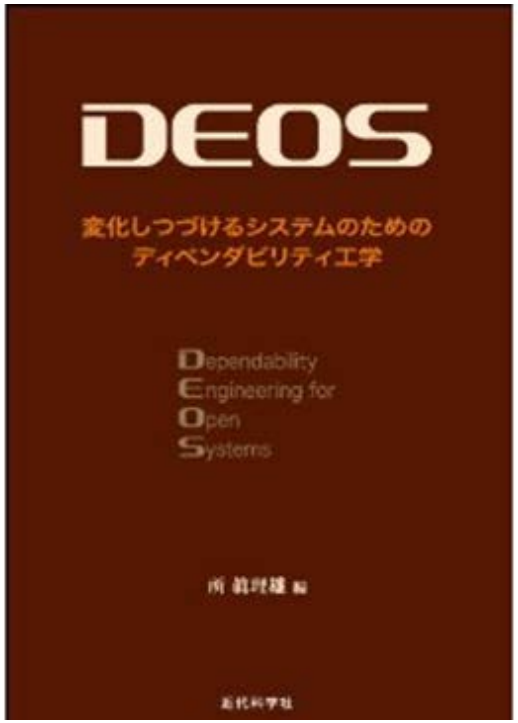
- IEC TC56 (Dependability)
  - IEC 62853 Open Systems Dependabilityの策定を2013年1月に開始
  - IEC60300-1 : Dependability management、IEC 62741: Dependability caseにExpertとして参加
  - WG4　Information System Aspect of DependabilityにConvenerとして参加
- ISO/IEC JTC1/SC7 (System and software engineering)
  - ISO/IEC15026: System and software assurance（co-editor)
- The Open Group
  - RTES部会における標準化活動
  - Open Dependability Through Assuredness™(*)　標準V1.0発表　（2013年7月15日）
- OMG (SysA: Systems Assurance Task Forceで活動)
  - “Machine Checkable Assurance Language”の提案
  - “Dependability Assurance Framework for Safety-Sensitive Consumer Devices”の提案

(*): Dependability Through Assuredness is a trademark of The Open Group

書籍出版

- **M. Tokoro(ed.), “Open Systems Dependability - Dependability Engineering for Ever-Changing Systems”, （2012年11月、CRC Press）**
  - 所 眞理雄編、「DEOS – 変化しつづけるシステムのためのディペンダビリティ工学」、（2014年6月、近代科学社）





一般社団法人ディペンダビリティ技術推進協会（略称DEOS協会）

- **2013年10月22日に設立**
- **事業継続・説明責任遂行の手法の確立**
  - OSDとDEOSプロセスの深化・発展
  - 目的・対象別のDEOSプロセス適用支援
  - ディペンダビリティー向上・標準化のための社会貢献
  - DEOS成果を活用したサービス継続、説明責任が果せるサービス、製品開発
    - ビジネス継続性の向上・運用保守コストの削減
- **オープンシステムディペンダビリティー技術の標準化**
  - OSD/DEOS標準化情報の共有
  - OSD/DEOSに関する標準化活動
- **DEOSに関連した産業の育成**
  - システム構築、ツール、コンサルティング、認証など新規事業創出
  - ディペンダビリティー要件の厳しいビジネス領域の立ち上げ
- **オープンシステムディペンダビリティー技術の研修**
  - ツール・サンプルシステムの先行試用、無償使用
- **会員間での非競争領域の共有（情報、事例、基盤プラットフォームの構築、等）**

DEOS協会会員（2014年6月）

正会員

株式会社アックス
アップウィンドテクノロジー・インコーポレイテッド
オムロン株式会社
サイオステクノロジー株式会社
株式会社サイバー創研
株式会社ジェーエフピー
株式会社 Symphony
株式会社ソニーコンピュータサイエンス研究所
株式会社チェンジビジョン
株式会社デンソークリエイト
パナソニック株式会社
PCIソリューションズ株式会社
富士ゼロックス株式会社
富士ゼロックスアドバンストテクノロジー株式会社
富士ゼロックス情報システム株式会社
株式会社富士通ディフェンスシステムエンジニアリング
株式会社豆蔵
株式会社Minoriソリューションズ
横河電機株式会社株式会社

学術会員

大野 毅（横河電機）
加賀美 聡（独立行政法人産業技術総合研究所）
片平 真史（独立行政法人 宇宙航空研究開発機構）
木藤 浩之（東京大学）
木下 佳樹（神奈川大学）
倉光 君郎（横浜国立大学）
河野 健二（慶應義塾大学）
白坂 成功（慶應義塾大学）
高井 利憲（奈良先端科学技術大学院大学）
高村 博紀（横河電機）
武山 誠（神奈川大学）
田丸 喜一郎（情報処理推進機構）
中川 雅通（パナソニック）
中原 早生（神奈川大学）
平井 誠（神奈川大学）
松野 裕（電気通信大学）
森口 草介（神奈川大学）
森田 直（Interactor Promotions）
屋代 眞
山本 修一郎（名古屋大学）
湯浅 能史（神奈川大学）
横手 靖彦（サイバーアイ）

賛助会員

一般社団法人TERAS

ディペンダビリティ技術推進協会（DEOS協会）組織

ディペンダビリティ技術推進協会（DEOS Association）

理事長　所　眞理雄
理事　松田　晃一
理事　山浦　一郎
理事　屋代　眞
理事　竹岡　尚三
理事　平鍋　健児
監事　佐々木栄美子

理事会
理事長・理事・監事

戦略策定
活動計画策定
普及活動方針
事業化検討
資金計画策定
知財関連方針

事務局
竹岡・小阪・山浦・屋代

理事会運営
運営委員会
部会運営支援
普及・広報

運営委員会
理事会・部会主査/副主査・事務局

OSD部会
所（兼任）

OSD社会・事業適用
事業継続
説明責任
DEOSプロセス
DEOSアーキテクチャ

D-Case部会
山本・松野

D-Case実証評価研究会
D-Caseガイドライン
D-Case事例
D-Case普及促進
D-Case Tools

技術部会
加賀美・横手

D-ADD/D-Script
ArtLinux
D-RE/Monitoring
Security
CSSC連携

標準化部会
木下・森田

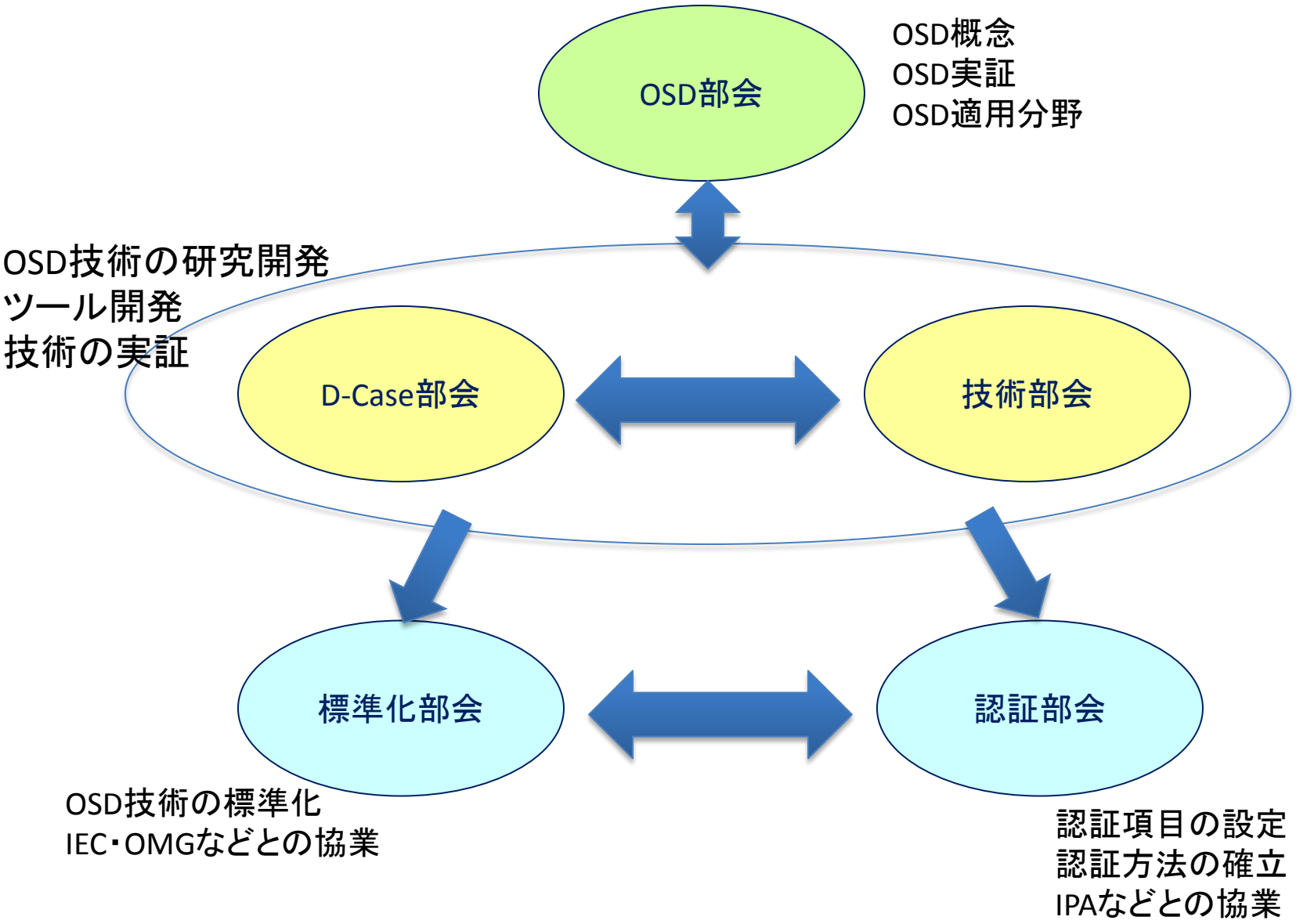
標準化戦略
国際規格化推進
TOG連携
IEC
OMG

NEW 認証部会
高村・TBD

認証方法
認証事業
教育・研修

2014年6月

DEOS協会部会


OSD部会
OSD概念
OSD実証
OSD適用分野
OSD技術の研究開発
ツール開発
技術の実証
D-Case部会
技術部会
標準化部会
認証部会
OSD技術の標準化
IEC・OMGなどとの協業
認証項目の設定
認証方法の確立
IPAなどとの協業

DEOS協会運営方針

- オープンシステムディペンダビリティー技術をもとに、世界を視野に社会貢献を目指す

- 運営
  - 小額から入会可能・受益者負担の会費による運営
  - 部会・WGに権限を与えた柔軟な運営を目指す
  - プロジェクト（WG）に対して事業会費（受益者負担の原則）
  - 日本国内にフォーカス
    - メンバーは日本国内に限定はしないが当面は国内での活動の充実を優先する

- ディペンダビリティー関連技術研究・開発機関、システム開発・運用ベンダー、ソフトウェア開発・運用ツールベンダー、システムユーザー・D-Case User企業（含む　損保、監査法人、など）、ディペンダビリティー関連ソフトウェア技術認証機関・コンサルタント、標準化団体などとの協力して目標を達成する事を目指しています。是非DEOS協会にご参加ください。

まとめ

- 変化しつづけるシステムのためのディペンダビリティ工学を提案し、体系化した。
- オープンシステムディペンダビリティの概念並びにDEOSプロセスは、ソフトウェアシステムに限らず多くの変化し続けるシステムに対応できる。
- これによって、合意に基づいた安全・安心社会の構築が可能となる。
- DEOS協会を通して普及・発展を推進し、将来の社会設計の基本概念・基盤技術として世界に貢献する。

JST/DEOS Project

http://www.jst.go.jp/crest/crest-os/

http://www.jst.go.jp/crest/crest-os/osddeos/index-j.html

DEOS協会

http://deos.or.jp