

D-Case実証評価研究会の 設立にあたって

名古屋大学 情報連携統括本部 情報戦略室
教授 山本修一郎
特任講師 松野 裕

Copyright Prof. Dr. Shuichiro Yamamoto 2012

1

第1回 D-Case実証評価研究会

- 開催日時 2012年9月14日 13:30～17:30
- 開催場所

〒460-0008 名古屋市中区栄3-1-1 広小路第一生命ビル
株式会社 デンソークリエイト10階会議室
(<http://www.denso-create.jp/access/index.html>)

Copyright Prof. Dr. Shuichiro Yamamoto 2012

2

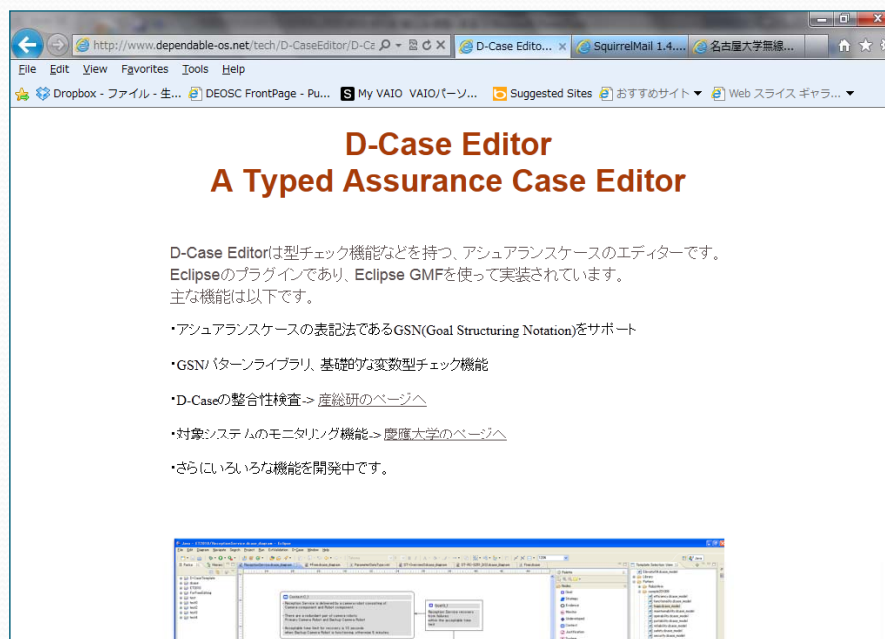
主要内容

- D-Caseとは
 - DEOSプロジェクト
 - ディペンダビリティケース
- D-Case実証評価研究会の目的
 - D-Caseの教育
 - D-Case適用支援技術の研究
 - D-Case統合環境の試行評価
- 研究会の構成と参加条件
- 今後の予定

DEOS-- Dependability Engineering for Open Systems

- 科学技術振興機構JSTの戦略的創造研究事業CRESTのひとつ
 - <http://www.crest-os.jst.go.jp/>
- 「オープンシステムディペンダビリティ」概念を提唱
 - プロジェクト白書 DEOS-FY2011-WP-03J
 - 変化しつづけるシステムのサービス継続と説明責任の全う
- システムのディペンダビリティを保証するために、ディペンダビリティケースを作成できるD-Caseエディタを開発(2011)
- ディペンダブル組み込みOS研究開発センター
 - <http://www.dependable-os.net/>

D-Case エディタ:GSNの編集管理ツール



<http://www.dependable-os.net/tech/D-CaseEditor/>

Copyright Prof. Dr. Shuichiro Yamamoto 2012

5

ディペンダビリティとは

人間行動
コンポーネント
法制度
自然物理現象

ディペンダビリティ

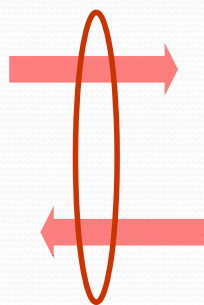
- アベイラビリティ性能及びこれに影響を与える要因、すなわち信頼性性能、保全性性能及び保全支援能力を記述するために用いられる包括的な用語

JIS Z 8115

イベント



期待する性能



応答



信頼性, 保全性

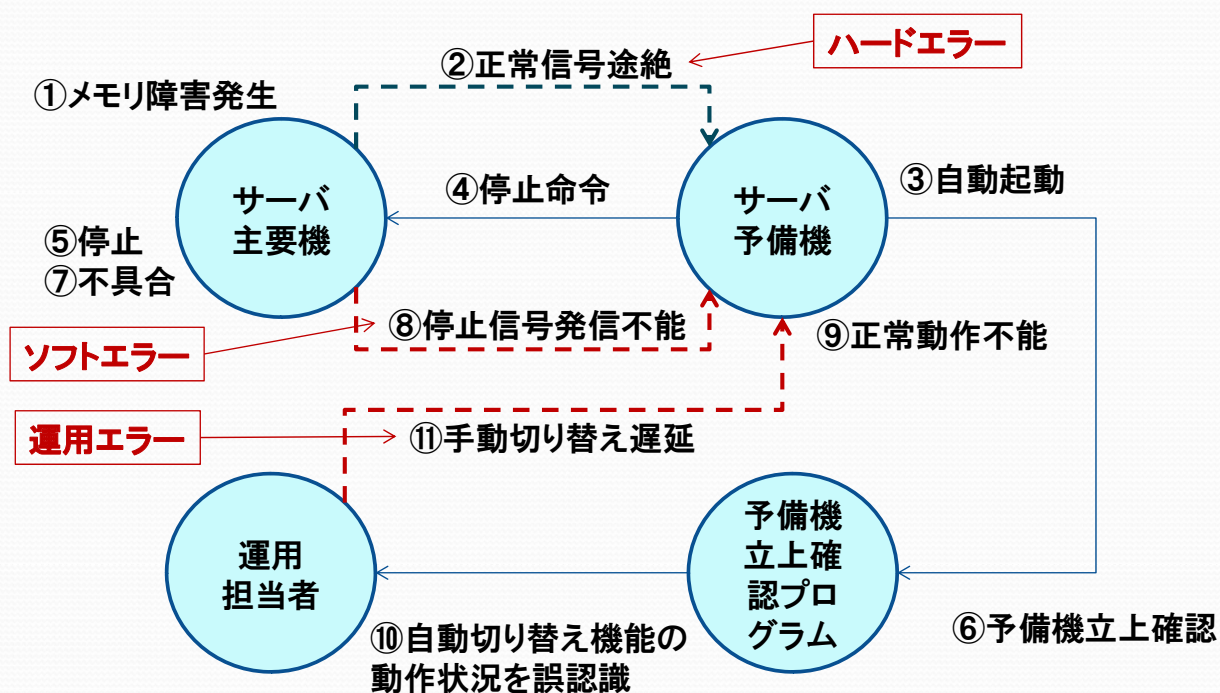
Copyright Prof. Dr. Shuichiro Yamamoto 2012

大規模複雑なITシステムの問題点

キーポイント	問題点
連携システム Coalitions of systems	大規模複雑なITシステムでは、要素システムが異なる組織によって独立に所有され管理されるために、相互連携作用による影響を事前に予測できない
還元主義の限界 Break down of reductionism	要素システムに分解して逐次的に改善するという還元主義では、大規模複雑なITシステムを開発、統合、展開できない
社会技術的システム Socio-Technical systems	大規模複雑なITシステムでは、人間、組織、社会、政治的要因を技術的要因に加えて考慮する必要がある

Ian Sommerville, Dave Cliff, Radu Calinescu, Justin Keen, Tim Kelly, Marta Kwiatkowska, John Mcdermid, and Richard Paige, Large-Scale Complex IT Systems, Communications of The ACM, pp.71-77, Vol.55, No.7, 2012

金融システム障害、故障信号に不具合



参考)日経新聞電子版, 2012/2/10 2:00

ディペンダビリティとセキュリティ

- 可用性: 正しいサービスを提供できること
- 信頼性: 正しいサービスを持続できること
- 安全性: ユーザと環境に破滅的な事態を生じさせないこと
- 一貫性: 不適切な変更がないこと
- 保守性: 修理・修正できる能力

AVIZZHENIS ET AL.: BASIC CONCEPTS AND TAXONOMY OF DEPENDABLE AND SECURE COMPUTING, IEEE TRANSACTIONS ON DEPENDABLE AND SECURE COMPUTING, VOL. 1, NO. 1, JANUARY-MARCH 2004

Copyright Prof. Dr. Shuichiro Yamamoto 2012

9

ISO/IEC 15026 保証(アシュアランス)ケース

- 保証ケースの構造と内容に対する最低限の要求を規定
- 保証ケースの内容
 - システムや製品の性質に対する**主張** (claim)
 - 主張に対する系統的な**議論** (argumentation)
 - この議論を裏付ける**証跡** (evidence)
 - 明示的な**前提** (explicit assumption)
- 議論の過程で、補助的な主張を用いることにより、最上位の主張に対して証跡や前提を階層的に構成
- ディペンダビリティに対する保証ケースがディペンダビリティケース

参考) ISO/IEC 15026-2:2011, Systems and Software engineering—Systems and Software assurance—Part2: Assurance case

Copyright Prof. Dr. Shuichiro Yamamoto 2012

10

ISO 26262における安全性ケース

- ISO_26262 自動車 機能安全 パート10
 - 機能安全についてのガイドライン
 - 5.3節「安全性ケースについて理解する」
- 安全性ケースを記述する手法
 - GSN
 - CAE(Claims- Argument- Evidence)
- 安全性の議論
 - 開発対象システムとしてのプロダクトについての議論
 - システム開発やアセスメントのプロセスについての議論
- 安全性ケースの開発ライフサイクル
 - 安全性ライフサイクルと統合された反復的な活動

(参考) ISO_26262-10_2012(E)- Road vehicles — Functional safety —
Part 10: Guideline on ISO 26262

Copyright Prof. Dr. Shuichiro Yamamoto 2012

11

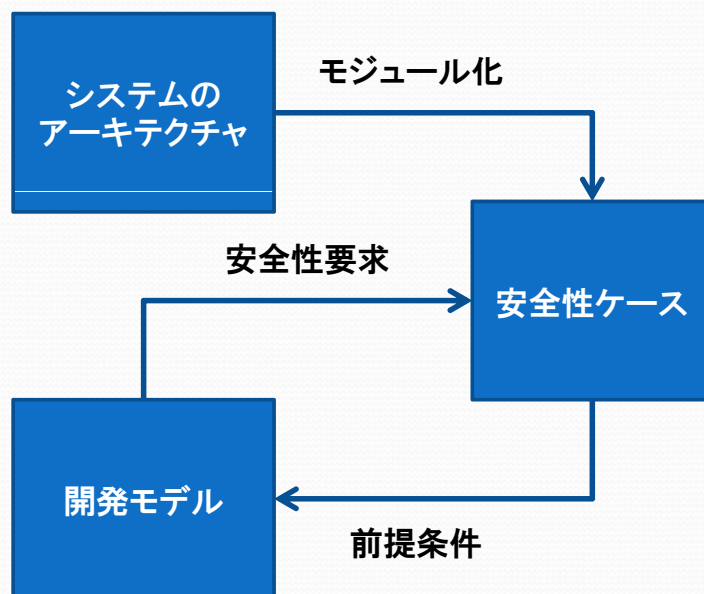
適用事例

適用機関	安全性確認事例
航空機	戦闘機の航空電子システム
英国国防省	サイト
英国地方鉄道	信号システム
潜水艦	推進システム
英国軍	航空管制システム
英国地下鉄	ジュービリー線の拡張システム
スウェーデン	航空制御システム
ロールスロイス	エンジン制御システム
MAN Nutzfahrzeuge AG	走行制御
航空宇宙	GPS
NASA	無人飛行機

Copyright Prof. Dr. Shuichiro Yamamoto 2012

12

モデルベース開発における安全性ケース



参考) Wagner, S.; Schätz, B.; Puchner, S.; Kock, P., A Case Study on Safety Cases in the Automotive Domain: Modules, Patterns, and Models, Software Reliability Engineering (ISSRE), 2010 IEEE 21st International Symposium on Digital Object Identifier: 2010 , pp. 269 – 278

安全性ケースアーキテクチャ

水準	説明	プロダクト	プロセス	環境・ユーザ
概念	論理機能を定義	概念プロダクトに対する安全性の議論	概念開発プロセス安全性の議論	システム安全性に対して環境・ユーザとの相互作用を確認 ユーザの振る舞いについての仮定(運転手の反応時間など) 環境条件(道路の傾斜, 路面状況, 風速など)
統合	機械・電子要素の統合	統合プロダクトに対する安全性の議論	統合開発プロセス安全性の議論	
機能	機械・ソフトウェア・電子回路への分解	機能プロダクトに対する安全性の議論	機能開発プロセス安全性の議論	

参考) Wagner, S.; Schätz, B.; Puchner, S.; Kock, P., A Case Study on Safety Cases in the Automotive Domain: Modules, Patterns, and Models, Software Reliability Engineering (ISSRE), 2010 IEEE 21st International Symposium on Digital Object Identifier: 2010 , pp. 269 – 278

ディペンダビリティケースの用途

- 環境と相互作用するシステムや製品が持つ不確実性やリスクに対してシステムや製品が望ましい性質を持ち、危険な状況に陥らないことを保証
- ディペンダビリティケースを作成した結果にも、主張が持つ性質の影響度とその不確実性を反映
- 主張に含まれる不確実性を関係者が許容できるかどうかをディペンダビリティケースの作成を通じて議論
- システムや製品の開発プロセスにおける計画や、人間活動、意思決定などに対する保証

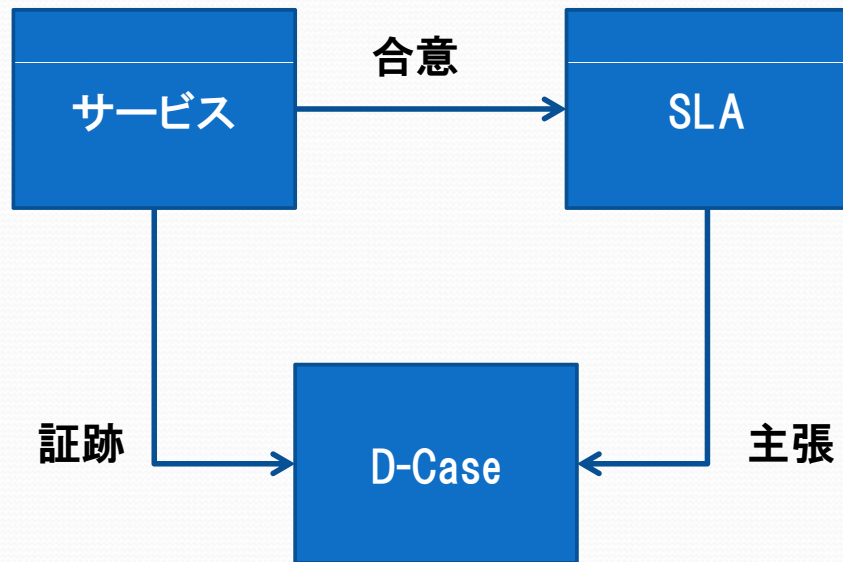
Copyright Prof. Dr. Shuichiro Yamamoto 2012

Fサーバのパンフレット

- 「Fサーバは、これまで以上に安心してレンタルサーバーサービスをご利用いただくために品質保証制度(SLA)を設け、稼働率100%を保証した高いビジネス品質のサービスでお客様のビジネスを支えます」
- 「さらに人為的なデータ損失があった場合にそなえ、日に1回、外部サーバーにデータを保存していますので、お客様によるデータの誤消去があった場合にも、前日の状態に戻すことが可能です」
- 「数年前までは記述の通りだったが、現在は説明の通りと異なる。記述ミスで、修正をせずにいた可能性がある」

Copyright Prof. Dr. Shuichiro Yamamoto 2012

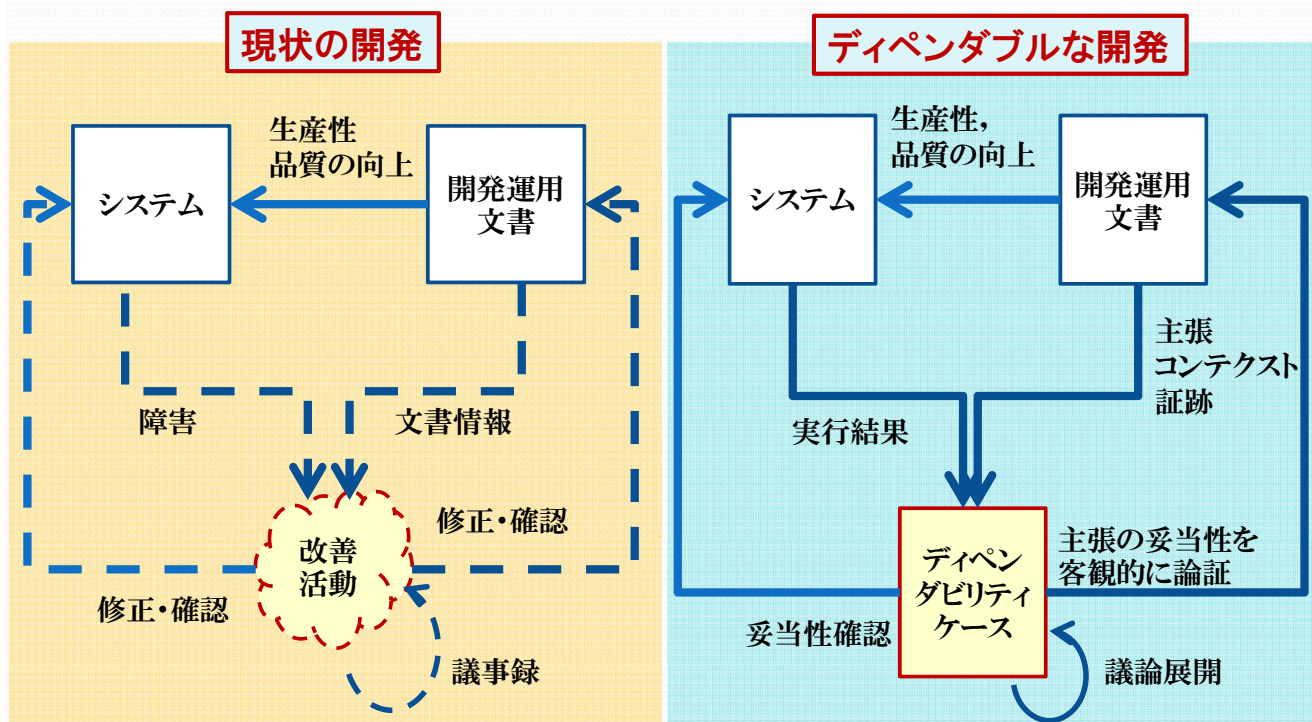
SLAとD-Case



Copyright Prof. Dr. Shuichiro Yamamoto 2012

17

ディペンダビリティケースの効果例

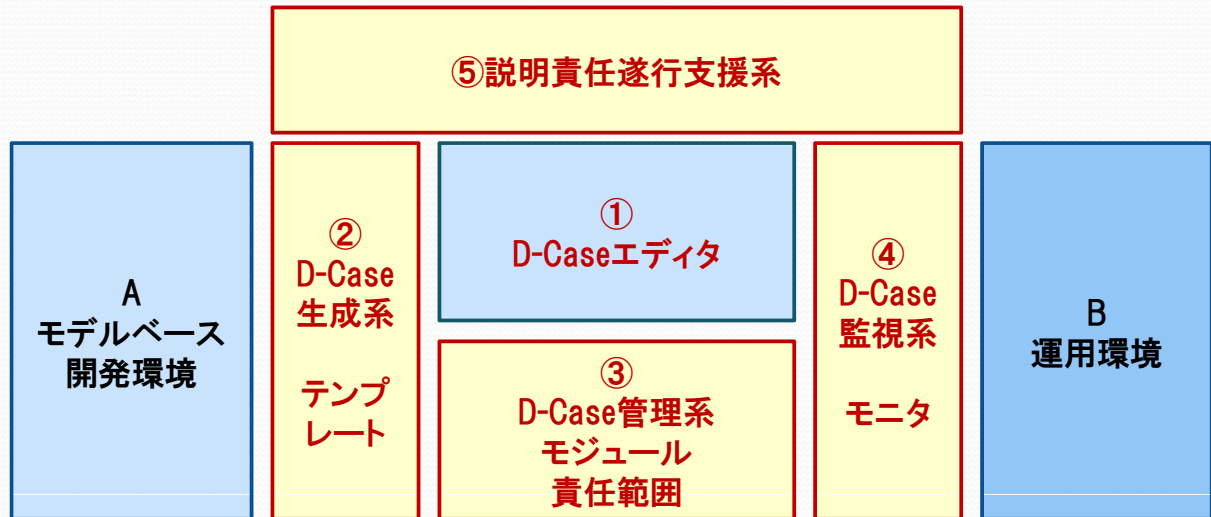


Copyright Prof. Dr. Shuichiro Yamamoto 2012

18

D-Case統合環境の構成例

- 本開発
- ① D-Caseを対話的に編集
 - ② モデル構成に基づきD-Caseの部分木(テンプレート)を生成
 - ③ D-Caseモジュールと対象責任者の範囲を管理
 - ④ システムの運用状況を提示するモニタインタフェースを提供
 - ⑤ 問題状況に対するD-Caseの責任範囲を提示



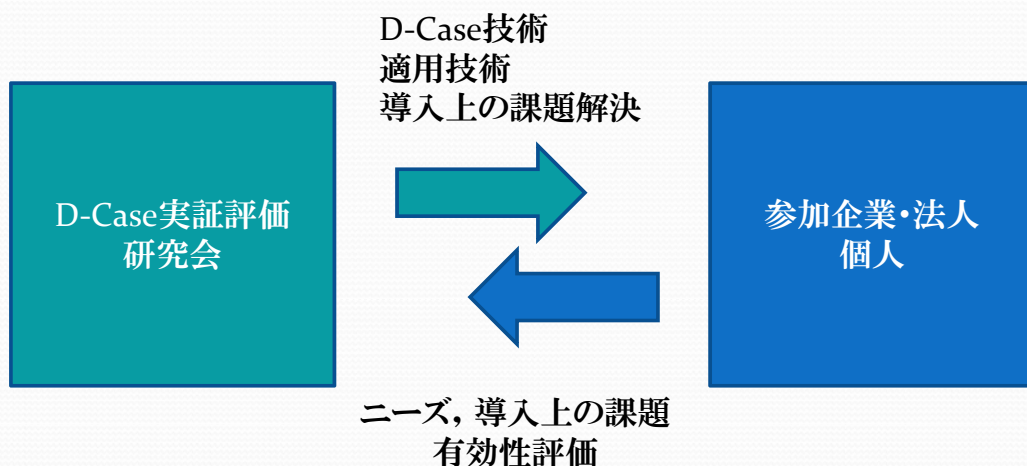
注) A,Bについては, 既存の標準的環境を想定

Copyright Prof. Dr. Shuichiro Yamamoto 2012

19

D-Case実証評価研究会の目的

- D-Caseの教育
- D-Case適用支援技術の研究
- D-Case統合環境の試行評価

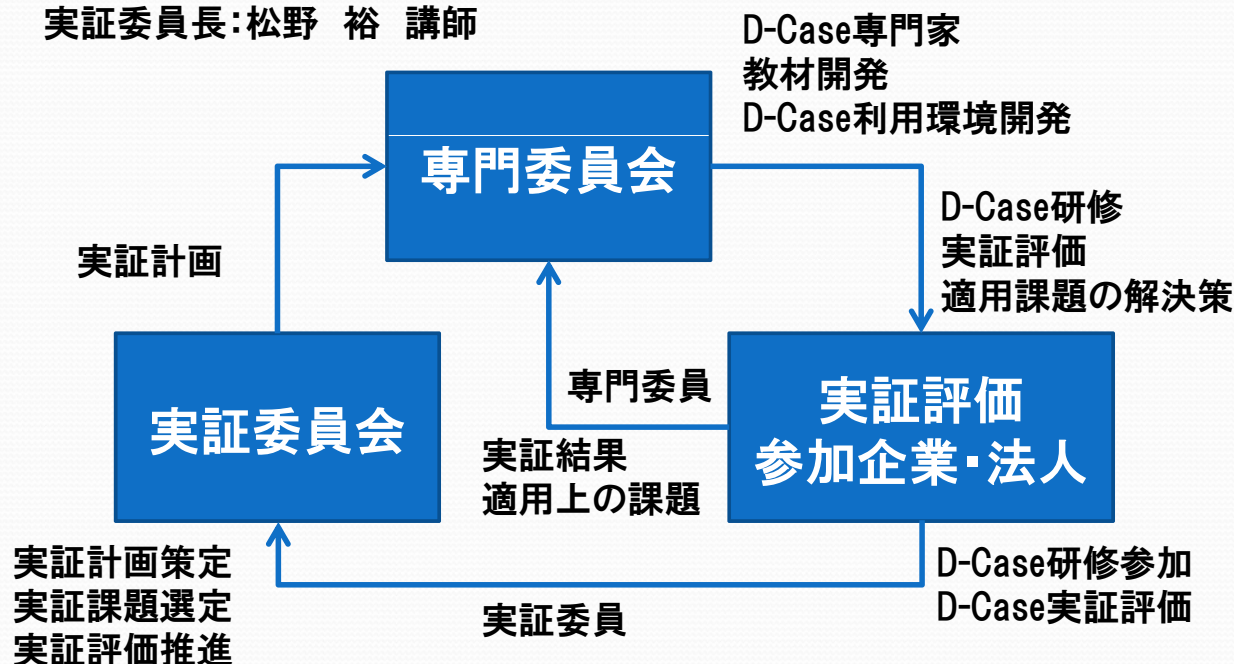


Copyright Prof. Dr. Shuichiro Yamamoto 2012

20

研究会の構成

専門委員長:山本修一郎 教授
実証委員長:松野 裕 講師



Copyright Prof. Dr. Shuichiro Yamamoto 2012

21

研究会への参加条件

- 参加費:無料
- 参加条件(例)
 - 無理のない範囲で協力していただきます
 - D-Case研修の受講, 演習レポート作成
 - D-Case研修アンケートへの回答
 - 研修については, 複数企業の方に参加していただく合同研修会と, 企業ごとに実施する個別研修会を用意します. 各研修会の参加者は20名から30名程度を考えています.
 - D-Caseエディタを用いて, 参加者が想定する典型的なシステムのディペンダビリティケースを作成して, 適用上の課題を研究会で報告していただきます
 - 公開研究会では, 機密保持上の問題が発生しないように, 業界標準的なシステムを対象とします
 - 個別研究会では, 組織ごとに参加者を限定するなどして, より具体的な課題についての研究にも対応します
 - 実証内容を評価分析する期間が必要になることから, 実証期間は3カ月以内を想定しています

Copyright Prof. Dr. Shuichiro Yamamoto 2012

22

研究会での活動例

- 研修の受講
 - D-Caseの理解・疑問点の解消
- D-Case適用支援技術の研究
 - 適用ドメイン向けD-Case作成法の開発
 - D-Caseを活用した高信頼システム開発プロセスの構築
 - 研究会参加者間の課題と解決策の共有
 - 専門家からのフィードバック
- D-Case統合環境の試行評価
 - D-Caseエディタ
 - パターンテンプレート機能
 - モジュール化支援機能

研修形態

- 個人
 - 他の参加者との合同研修会に参加していただきます
- 企業
 - 20名程度以上の研修参加を希望される企業の場合、個別研修会を実施します
 - 個人および企業から少人数でご参加いただく場合、合同研修会に参加していただきます

参加企業・法人のメリット

- 機能安全における欧米で導入が進んでいるディペンダビリティケースの知識を日本語で習得できます
- 4年以上のGSN教育経験と、適用評価実績に基づいて開発された教材を用いて、初学者にも分かりやすく学習できます
- 機能安全の仕組みを開発プロセスに導入する上での課題を実証実験の中で解決できます
- ディペンダビリティケースを記述する世界標準になっているGSNを作成できるD-Caseエディタの最新環境をご利用できます
- D-Caseエディタ拡充機能へのご要望を反映できます
- City University of Londonと議論して研修教材を開発しており、ディペンダビリティケースに関する世界最高水準の内容です
- 研究会では海外の第一人者によるセミナーを企画します
- 企業別研修会・研究会の開催など、ご要望に応じて対応します

今後の予定

- 研究会の活動期間 2013年9月末までの1年間を予定
継続については、活動を通じて判断
- 第1回研究会にむけて、参加企業を募集中
- 研究会
 - 月例、隔月など開催間隔について調整
 - 参加企業の要望に応じて、個別研究会の実施も検討

研究会の開催計画

研究会の期間:2012年9月～2013年9月

	9月 10月 11月 12月	1月 2月 3月	4月 5月 6月	7月 8月 9月
研究会 月例(予定)	▲ ▲ ▲ ▲ 第1回(9/14)	▲ ▲ ▲	▲ ▲ ▲	▲ ▲ ▲ 終了
実証委員会	1期実証		2期実証	
専門委員会	研修 D-Case環境-0	分析評価 教材改訂 D-Case環境-1	研修	分析評価 教材改訂 D-Case環境-2

Copyright Prof. Dr. Shuichiro Yamamoto 2012

27

入会申請, お問い合わせ先

国立大学法人名古屋大学
情報連携統括本部情報戦略室

名古屋大学 情報連携統括本部(担当:石原)
電話:052-789-4357
メール: ishiharam at icts.nagoya-u.ac.jp

Copyright Prof. Dr. Shuichiro Yamamoto 2012

28

研究テーマ例

研究テーマ候補	内容例	課題
システム保証方法の評価	D-Caseを作成することにより, システムのディペンダビリティを確認する	対象システムの選定
サービス運用プロセスの高信頼化	サービス運用時に障害が発生したと想定して運用プロセスを点検することにより, 説明責任遂行上の不備がないことを確認する	運用マニュアルの整備
サービス運用実験	D-Caseを用いてサービスリスクを分析し, リスク対策を実施することにより, ディペンダビリティを保証する	運用環境I/Fの標準化
TOGAF Dependability Framework(DF)	DFを共同開発することにより, TOGへ共同提案する	TOGAF認定アーキテクト
d* framework	調達コンポーネントのディペンダビリティを保証するための技術を研究する	調達品の第三者保証
ソフトウェア開発プロセスの高信頼化	ソフトウェア開発工程の完了基準をD-Caseを用いて明確化することにより, 工程作業の妥当性を保証するとともに, 工程生産物体系を確立する	開発プロセスの標準化
ディペンダビリティ教育	上記実証を踏まえて, D-Caseを用いたディペンダビリティ研修コースを試行評価	受講生の確保