

# D-Case 入門セミナー

## ～高信頼なシステム開発に必要な考え 方の基本を身につけよう！～

### 2013年7月31日(水)、キャッツ新横浜 セミナールーム

## 開催報告

電気通信大学 松野裕

キャッツ 穴田啓樹

### はじめに

近年組み込みシステムの機能安全性や、ディペンダビリティの必要性が認識されています。近年の組み込みシステムは、ネットワークを通じて様々なシステムとつながるようになり、その影響は社会一般に広がっています。そのため、特にお客様や他社の相手先様、さらには社会全体のステークホルダーに自社で開発したシステムやソフトウェアがディペンダブルであることを論証する思考技術と説明技術がますます必要になってきています。しかし、これまでこれらの技術に入門する機会が少なく、せっかく高い機能安全性を持った組み込みシステムなどを開発しても、なかなかお客様などに伝わらないという問題がありました。

そこで今回、DEOS プロジェクトの成果である「D-Case」を紹介し、ツールによるアシュアランスケース(assurance case)作成を体験できるセミナーを企画しました。アシュアランスケースは、システムの安全性やディペンダ

ビリティを、利用者などの利害関係者に納得してもらい、保証するための手法として、近年イギリスを中心に普及しつつあります。D-Case は、専門的な知識と経験が必要なアシュアランスケースを、より広く、企業の方に使っていただけるよう工夫した手法とツールです。

DEOS プロジェクト（「実用化を目指した組込みシステム用ディペンダブル・オペレーティングシステム」）は科学技術振興機構（JST）の戦略的創造研究推進事業 CREST の研究領域のひとつです。DEOS プロジェクトの詳細は <http://www.dependable-os.net/osddeos/index.html> , D-Case の詳細は <http://www.dcase.jp> を御覧ください。

## セミナーのねらい

セミナーの対象者は、安全性、セキュリティなど高信頼性が要求されるソフトウェア開発のリーダー、マネージャーの皆様など、筋道立てて議論し、チームをまとめていく必要のある方を対象としました。

セミナーの目的として、初心者が D-Case の面白さ、有効性を感じてもらい、そのためのゴールとして、

- ・ D-Case の基本構文を理解すること
- ・ 基本的な D-Case を書くこと
- ・ 手順を追いながら、例題 D-Case を書くこと

を設定しました。

## セミナーの内容

セミナーは以下の構成でした。

- ・ D-Case の必要性(30分)
  - 名古屋大学 山本修一郎
- ・ DEOS/D-Case の最新動向(40分)
  - DEOS センター 屋代眞、日本 IBM 豊田学
- ・ D-Case 超入門(140分)
  - 電気通信大学 松野裕、キャッツ 穴田啓樹

D-Case はアシュアランスケースをベースとした、システムの安全性やディペンダビリティを保証するための手法とツールです。セミナーの導入として、名古屋大学の山本教授より、現在そしてこれから、なぜ安全性やディペンダビリティの保証が重要になってきているのか、説明を行いました。次に D-Case を実際に企業のみなさまに使っていただくために、DEOS でどのような開発研究が行っているか、最新の情報を DEOS センターの屋代氏、日本 IBM の豊田氏より紹介してもらいました。システムの安全性やディペンダビリティの情報は開発運用時に生成される多くのドキュメントやモデルに記述されます。D-Case はそれらドキュメントを用いて、システムの安全性やディペンダビリティを保証します。屋代氏と豊田氏の講演では、最新のシステムモデリング言語である SysML と D-Case の組み合わせを開発中のツール連携を中心に講演してもらいました。

D-Case の背景と必要性と、最新の開発研究を紹介した後どのように D-Case を使っていけばいいのかをできるだけわかりやすく、初心者の方にわかっていただけるよう、ツールを使った演習も含めたチュートリアルを電気通信大学の松野とキャッツの穴田により行いました。2時間20分の長丁場でしたが、参加者の皆様に熱心に参加していただきました。

## 開催結果

### 参加者

セミナー参加の募集をしたところ、わずか2日で定員の15名を超える応募があり、数人の方にはご参加いただくことができず、申し訳ありませんでした。参加者のみなさまは、主に組み込み、通信、家電、第3者検証などを分野の企業の方が主でした。システムの安全性やディペンダビリティ、保証に関して全くの初心者の方々ではなく、経験が豊富にある方も参加され、身の引き締まる思いでした。D-Case を最近耳にされて参加された方もおり、様々なレベルや要望にできるだけお応えできるよう、工夫しました。

### アンケート結果

半日を費やしたセミナーは無事に終了し、その場で多くのご質問を受け、良い雰囲気でした。参加者の皆様に、以下のアンケートをお願いしました。

Q1. ディペンダビリティについて理解できましたか？

Q2. GSN ノードの使い分けを理解できましたか？

Q3. ノードの文章の書き方を理解できましたか？

Q4. 文書から D-Case を作成する方法を理解できましたか？

Q5. ツールの基本的な使い方を理解できましたか？

※ 5 択（1：全くできなかった ～ 3：普通 ～ 5：十分できた）で記入

Q1 から Q5 に進むにしたがって、応用レベルの確認になっています。

アンケート結果を下に示します。

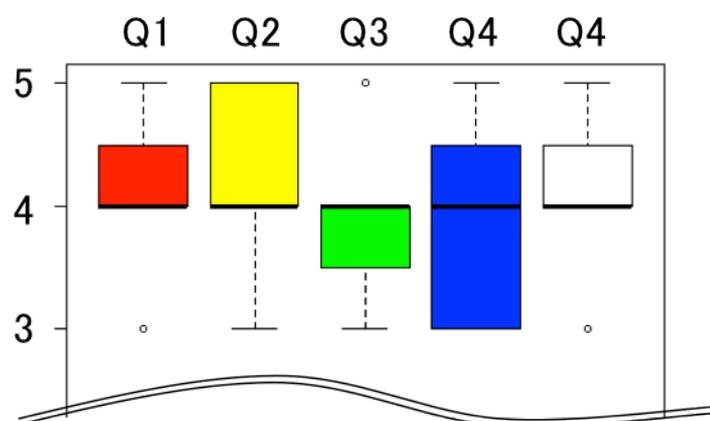


図 アンケート結果

図を見ると、参加者はディペンダビリティの基本からチュートリアルの内容について、おおむね理解されたことがわかります。入門者から、すでにご経験が深い方までいたため、応用レベルの確認の質問になるほど多少ばらつきがでる結果となりましたが、ほとんどすべての参加者からポジティブな評価を受けました。

### 参加者のみなさまのご意見

アンケートに自由記述欄には、以下の様な多くのご意見をいただきました。

- ・ お客様と合意形成だけでなく、自身の考えの整理に活用できる。
- ・ 自動車業界へ展開できそう。
- ・ FMEA や HAZOP と組み合わせると効果がありそうだがコストが気になる
- ・ D-Case 実証実験が行われることを期待する

- ・ 議論のループを解消できそう
- ・ D-Case の具体例がないと現場に普及させるのは難しそう
- ・ テストの考え方に活用できそう
- ・ D-Case 記述方法について、わかりやすく理解できた
- ・ 実際に利用する際に議論構造パターンの具体例が必要だと感じた
- ・ 受託開発における説明、自己確認に活用できそう
- ・ 経験を積まないと身につかないものと思った
- ・ より多くの例を穴埋めなどで解いていくとわかりやすいかもしれない
- ・ SysML と連携は単にトレーサビリティであって D-Case 単体で十分そう
- ・ 独学でやるより教えてもらったことで理解できたような気がする
- ・ 実際に手を動かして効率よい書き方を習得していく必要があると感じた
- ・ 既存開発にどう組み込むか検討が必要
- ・ 私の所属する部署で品質説明力強化やお客様に対するシステムサービス保証が関心事になってきている。折をみて社内に D-Case を伝える場を持ちたいと考えている
- ・ システム障害原因究明を行う際に D-Case を活用できないか考えている

我々が考えている利用シーン以外にも、参加者のみなさまに独自の利用シーンを考えてくださるなど、大変参考になるご意見を頂きました。同時に既存開発への組み込みなど、実際の現場への適用への課題もいただき、今後への示唆を頂きました。

## まとめ

7月31日に、キャッツセミナーとして行われた、安全性やディペンダビリティ保証のための手法とツールである D-Case の入門セミナーの報告を行いました。参加者の皆様との活発なやりとりを通じて、D-Case が日本企業のみなさまにお役にたてるかもしれないという、強い可能性を感じさせていただきました。今後よりわかりやすく、実践的なセミナーおよびツールを、実証実験や最新の研究成果をもとに提供していきたいと思っております。どうぞ今後も何卒よろしくお願いたします。