

## 15-A-16

### D-Case を用いたゴール共有による開発プロセスの適用<sup>1</sup>

#### ～ET ロボコンでの試行と成果～

#### 1. 概要

本編では、富士ゼロックス株式会社（以降、富士ゼロックス）において D-Case<sup>2</sup> を用いて開発のゴールを関連者で共有しながらソフトウェアを開発した事例を紹介する。ソフトウェアではでき上がったシステムが本来の要求と異なってしまいう事で、作り直しなどの手戻りが発生する事がある。こうした事態を防ぐために、どのようにして要求の意図を関係者間で理解し、共有して開発を進めて行くかが課題である。我々は ET ロボコン<sup>3</sup> での競技ロボット制御ソフトウェア開発で D-Case を活用し、ゴールを共有しながらソフトウェア開発を進める事で手戻りを削減し、円滑にプロジェクトを進められる事を確認した。また、D-Case を使う事でシステムの信頼性や設計根拠を示す事ができた。その結果、ET ロボコンでも競技部門、設計審査部門ともに上位の成績を残す事ができた。

#### 1.1. 課題と目標

本事例の開発対象は LEGO®MINDSTORMS®NXT で作成されたロボットを自律走行させて競う、ET ロボコンと呼ばれるコンテストで使用する組込みソフトウェアである。ET ロボコンは一般社団法人組込みシステム技術協会（JASA）が主催する ET ソフトウェアデザインロボットコンテストの愛称である。組込みシステム開発分野および同教育分野における若年層や初級エンジニアへの分析・設計モデリングの教育機会となることを目的に開催されている[1]。

富士ゼロックスでは 2010 年から継続して ET ロボコンに参加している。その狙いは、社内の若手技術者の設計スキル向上である。我々はオフィスで使用されている複合機やプリンターに搭載されている組込みソフトウェアを開発している。複合機のソフトウェアのソースコード規模は 2000 年時点では約 200 万行であったが、近年のネットワーク化対応や、それ

---

<sup>1</sup> 事例提供: 富士ゼロックス株式会社

コントローラ開発本部 土樋 祐希 氏、白坂 龍人 氏、吉崎 茜 氏、高橋 奈穂美 氏、増子 遼佑 氏  
基盤技術研究所 青野 博之 氏（事例提供当時）

<sup>2</sup> 一般社団法人 ディペンダビリティ技術推進協会（DEOS 協会）で提唱されている、システムのディペンダビリティについて説明責任を果たし、合意形成するためのツール

<sup>3</sup> 一般社団法人組込みシステム技術協会(JASA)が主催する ET ソフトウェアデザインロボットコンテストの愛称

に伴うセキュリティ機能の強化、そして外部機器との連携といったオフィス環境の変化に合わせて機能が增加し、現在では 1,000 万行を超えるほどに大規模化している(図 15-A-16-1) [4]。そして、その開発方式は既存のコードに修正を行う事で次の製品を作り出す派生開発が主となっている。そのため、新規に設計を行う機会は限られており、設計スキル獲得への必要性やモチベーションが開発者によってばらついている。特に若手層への設計機会が少なくなる事で設計力が低下し、新たな製品・サービス・ビジネスを作り出す力が弱まる懸念があった。ET ロボコンでは小規模ながらもチームでソフトウェアをスクラッチから作り、設計審査に向けて設計モデルを作成する。そして実際に他チームと性能を競う。こうした経験を通じてソフトウェア設計のスキルを高める事が ET ロボコンへの参加の狙いである。

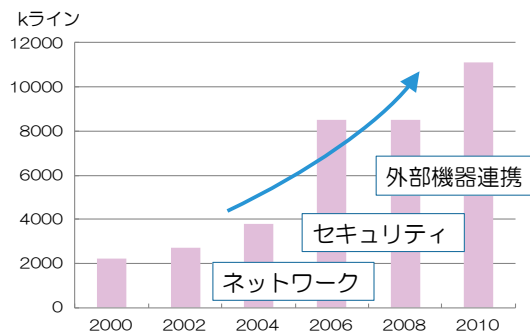


図 15-A-16-1 複合機ソフトウェアの規模の推移

ET ロボコンへの参加は 2010 年から行っている。2010 年、2011 年に参加した地方大会（南関東大会）の結果は表 15-A-16-1 の様であった。

表 15-A-16-1 2010/2011 年の ET ロボコンの結果（南関東大会）

参加年度	チーム名	モデル 審査評価	競技順位	総合
2010 年 (39 チーム中)	チーム A	B+	4 位	5 位
	チーム B	A	28 位	21 位
	チーム C	A-	10 位	7 位
2011 年 (37 チーム中)	チーム D	A (優勝)	11 位	2 位
	チーム E	A (準優勝)	23 位	14 位

(モデル審査評価はA+~Dまでの 12 段階であり、ここではAが最も良い評価で優勝)

幸い、設計審査に関しては B+ 以上の良い評価を受ける事ができた。しかし、競技順位に関しては設計審査に比較すると大きくばらついている事が分かる。参加して 2 年間の結果であるため、単に経験が足りないという事もあったと思われるが、大会終了後の参加者からのヒアリングや活動の振り返りによって、それまでの取組みで以下のような問題がある事が分かった。

- (1) 活動の全体像の共有ができていないまま作業を実施

チーム内の半数程度のメンバーが初めての取組みになるため、どのような事をしなくてはならないのかの全体像が見えず、当初の活動の立ち上がりが悪かった。また、目指している事の共有ができておらず、メンバー間での活動の方向性がずれるなど、必要な要件が抜けてしまう事があった。この事により、コンテストの結果が不満に終わるだけでなく、当初目指していた、“参加する事によるスキル向上”があまり感じられなかったという感想を持つメンバーもいた。

## (2) 非効率な開発作業

開発を進める上でチーム内での作業分担が行われる。例えばAさんはセンサの特性を調べ、Bさんは制御のアルゴリズムを検討するなどである。しかし、その作業が何のために行われるのかが理解されていないケースもあり、あまり重要でない作業に多くの時間を費やしてしまったり、逆に重要な作業を後回しにしてしまったりする事で、非効率な開発が行われていた。例えば難所と呼ばれる付加ポイント攻略に時間をかけ、コース攻略の基本となるライントレースがおろそかになり、難所に行く前にリタイアしてしまうなどである。そのため、かけた時間に対して大会では不本意な成績となってしまうケースがあった。

これらの問題は ET ロボコンの開発に留まらず、一般的なソフトウェア開発でも発生する。ソフトウェアは建築物や機械などとは異なり、直接触ったり、形として見たりする事ができない。ソフトウェアは概念的な集積であり、開発プロセスや意思決定の経緯も直接見る事ができない。単純な図面で全体が理解できるという事もない[7]。そのため、どのようなものを作ろうとしているのか要求側と開発者側ですり合わせる事は容易ではない。合意したつもりでもお互いに齟齬が発生する事もある。その結果、工数をかけて作ったものの、いざ使おうとした際に運用が困難となる、求められた性能が出ていないなどといった要因で手戻りが発生するなど、最悪、プロジェクトとして失敗する事もある。特に保守性や可用性、使用性などと言った非機能に関する要求を出す事は難しい。こうした不確定な要求の中で、関係者と合意しながらソフトウェアやシステムを作り上げる事は大きな課題である。

## 1.2. 本取組みの目標

以上のような課題をふまえ、2012年から ET ロボコンの開発に D-Case を活用し、合意形成をベースとした開発プロセスを導入した。本取組みの目標は以下の通りである。

- (1) D-Case を活動初期から活用し、チーム活動としてのゴールと全体像を示しながら開発を行う事
- (2) 手戻りを抑え、効率的な開発を通じて競技部門の成績を向上させる事
- (3) 第三者に対して設計意図と設計の妥当性、およびシステムの信頼性を示す事

## 1.3. 課題解決のための仮説設定

D-Case はシステムのディペンダビリティを示すための手法である。ディペンダビリティ

とは情報システムの信頼性や安全性など、情報システムが提供するサービスを安心して継続的に利用できる性質を統合した概念である[5]。D-Case は York 大学の Tim Kelly らが提案した Safety Case[8]と呼ばれる高安全性システムの保証するドキュメントをベースに考案されたものである。Safety Case の表記法にはいくつかあるが、D-Case は Goal Structuring Notation (GSN) [9]の記法をベースに拡張したものである<sup>4</sup>。D-Case ではゴールを木構造的に分解する。詳細化されたゴールは、最終的にはエビデンス（テスト結果など実際の検証結果など）により、実現している事が保証される。システム全体のディペンダビリティに関する構造を示す事で、各関係者との合意が取りやすくなる事が期待される。

通常 D-Case はシステムのライフサイクルで生成されるドキュメントをもとに作られ、従来のシステム開発や運用で生成されるドキュメントを置きかえるものではない。しかし、D-Case を先に記述し、D-Case で要求されるドキュメントを生成するための活動をシステムライフサイクルで行う手法も考えられている[5]。本取り組みでは後者の手法を取った。先に D-Case を作成し、開発者間で合意を取りながら開発を進める事で、開発の全体像を共有する事ができる。また、各活動をゴールと結び付けられるので、何のためにその活動をするのか、何を行う必要があるのかを明確にでき、手戻りを防ぐ事ができる。また、開発が終了した時点でそれまでに作成した D-Case によりシステムの信頼性を示す事ができるはずである。こうした仮説に基づき、D-Case を先行して作成する開発プロセスの実証を行った。

## 2. 取組みの対象と適用技術

### 2.1. ET ロボコンの概要

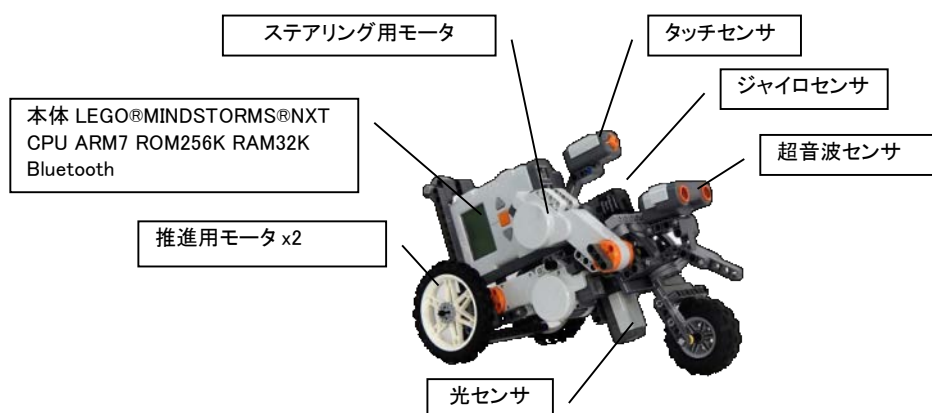
本取組みの対象は前述の通り ET ロボコン用のロボットに搭載するソフトウェアである。本取組みに関する情報として ET ロボコンについて説明する。ET ロボコンの課題は毎年変わるため、本編では 2014 年度の課題について説明する。

ET ロボコンは 2002 年に UML の普及を目的とした UML ロボットコンテストとして始まり、2005 年より ET ロボコンとして名称を変えて毎年開催され、2014 年で通算 13 回目の開催となった。全国の企業、大学、専門学校、高校などが参加しており、2014 年は 336 チームが参加している。参加者は全国 11 か所で開催される地方大会で競い、各地方大会で上位のチームには 11 月に行われる全国大会への出場権が与えられる。

本コンテストでは LEGO®MINDSTORMS®を使ったロボットに搭載するソフトウェアで競技を行う。ソフトウェアのコンテストであるため、ロボット（ハードウェア）は全てのチームで同一の構成であり、各チームの性能差は主としてソフトウェアの優劣によって決まる。図 15-A-16-2 に 2014 年度に使用したロボットを示す。

---

<sup>4</sup> ツールとして実装するための形式化やゴールノード間に必ずストラテジノードを挿入するなど、実用上の工夫がされている



写真出典 ET ロボコン 2014 デベロッパー部門競技規約 1.0.0[2]

図 15-A-16-2 2014 年度 ET ロボコンで使用した機体  
(デベロッパー部門アドバンストクラス)

各チームはこのロボットに搭載するソフトウェアを記述し、図 15-A-16-3 に示す競技フィールドを自律走行させる。基本的にはコースの黒線をロボットに装着された光センサによってとらえ、ラインレースを行う。コースは IN コースと OUT コースの 2 種類があり、それぞれのコースを 1 度ずつ走らせる。基本的にはスタートからゴールに要した時間で競うが、コースには難所と呼ばれる通過箇所があり、そこを通過する事でボーナスポイントを獲得する事ができる。ゴールまでに要した時間からボーナスポイントを減じた値をリザルトタイムと呼び、IN と OUT のリザルトタイムを足した値が一番小さいチームが優勝となる。

本コンテストの特徴は、コンテスト対象として走行を競う競技部門だけでなく、どのようにソフトウェアを作成したかを評価する設計部門が存在する点である。各チームは競技大会に先立って設計審査用の資料（設計モデル）を提出する。設計モデルは A3 用紙 5 ページから構成され、設計審査の基準に従った記述が必要となる。表 15-A-16-2 に 2014 年に示された審査基準を示す。提出した設計モデルは事前に審査員によって採点され、競技終了後に発表される。競技結果と設計審査の結果をもとに総合部門としての順位が決まり、全国大会に出場できるかどうかは総合部門の結果で決まる。このようなルールとする事で、若手エンジニアの設計レベル向上を目指している。



写真出典 ET ロボコン 2014 デベロッパー部門競技規約 1.0.0[2]

図 15-A-16-3 ET ロボコン 2014 年の競技フィールド

表 15-A-16-2 2014 年度の審査基準[3]

審査基準	項目	説明
制御技術	要素技術	機能を実現するための要素技術についての調査・検討・検証結果が記述されているか？
	制御戦略	定義された要素技術を使って、どのように機能を実現しているかが記述されているか？
	一貫性	要素技術と制御戦略で記述された内容が一貫しており矛盾はないか？
設計技術	機能	走行体が提供する機能が記述されているか？
	構造	① 機能を実現するために必要な要素が記述されているか？
		② 構造面での複雑さを低減させる工夫がなされているか？
	振る舞い	③ 定義された要素を使って、どのように機能を実現しているかが記述されているか？
④ 振る舞い面での複雑さを低減させる工夫がなされているか？		
一貫性	構造と振る舞いで記述された内容が一貫しており矛盾はないか？	
未確定仕様への対応	-	段階的に確定される仕様に対応して、ソフトウェアを効率的に修正可能とするための工夫がなされているか？

2014 年の ET ロボコンの競技および設計審査で大きな特徴となったのが、新設された仕様未確定エリアである。仕様未確定エリアとは、格子状に黒線が引かれた板上を走行するエリアである。ただし、単に走行するだけでなく格子の交点にはペットボトルが、格子の枠内にはコーンと呼ばれる半円状の立体物が障害物として部分的に配置される。これらの障害物がどの位置に置かれるか、全体で何個置かれるかは大会前日まで（全国大会では当日朝まで）参加者に知らされない。そのため、置かれる位置が知らされた時点でそれに対応したソフト

ウェアの変更が必要となる。短い期間でソフトウェアの変更が必要であるため、いかに変更しやすいソフトウェアにするかを設計の時点で考慮しなくてはならず、設計モデルの審査基準においても明確に表明する事が求められた。

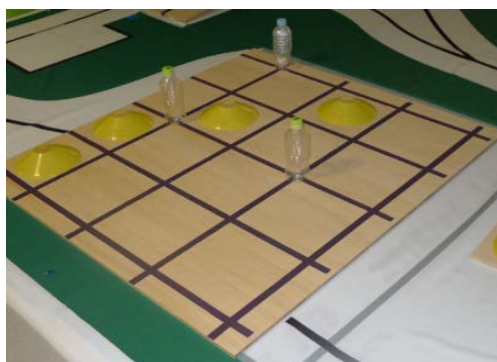



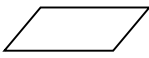

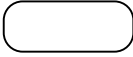
図 15-A-16-4 仕様未確定エリアの配置例  
(実際はペットボトルには水が入れられる)

## 2.2. D-Case 概要

本取組みでは D-Case を活用した開発を行った。ここでは D-Case について説明する。

D-Case はシステムに対する要求とその実現についてのステークホルダ間の合意を構造的に記述する記法である。表 15-A-16-3 に D-Case で使用する表記の一部を示す[2]。

表 15-A-16-3 D-Case の表記

名称	表記	説明
ゴール (Goal)		対象システムに対して、議論すべき命題
ストラテジ (Strategy)		ゴールが満たされることをサブゴールに分割して議論する場合の分割のしかた
エビデンス (Evidence)		詳細化されたゴールを最終的に保証するもの
コンテキスト (Context)		ゴールや戦略を議論するとき、その前提となる情報

D-Case では対象システムが満たすべき「ゴール」を置き、それを「ストラテジ」の観点に従ってサブの「ゴール」に分解する。サブの「ゴール」はさらに下位の「ゴール」に分解されていく。最終的に詳細化された「ゴール」はそれがシステムとして満たされている事を

「エビデンス」によって保証する。「エビデンス」は例えばテスト結果、形式手法による検証結果、レビュー結果などが含まれる。「ゴール」の詳細化が適切であれば下位の「ゴール」が「エビデンス」によって保証される事で、上位の「ゴール」が満たされている事を示す事ができる。「コンテキスト」は「ゴール」や「ストラテジ」に対する前提となる情報、制約などを示す。「コンテキスト」を記述する事で記述された D-Case の理解性や納得性を高める事ができる。

D-Case を記述する事で、システムのディペンダビリティ（信頼性や強靭性、安全性などのシステムが備えるべき能力）を示す事ができる。

図 15-A-16-5 に D-Case を使用した記述例を示す。

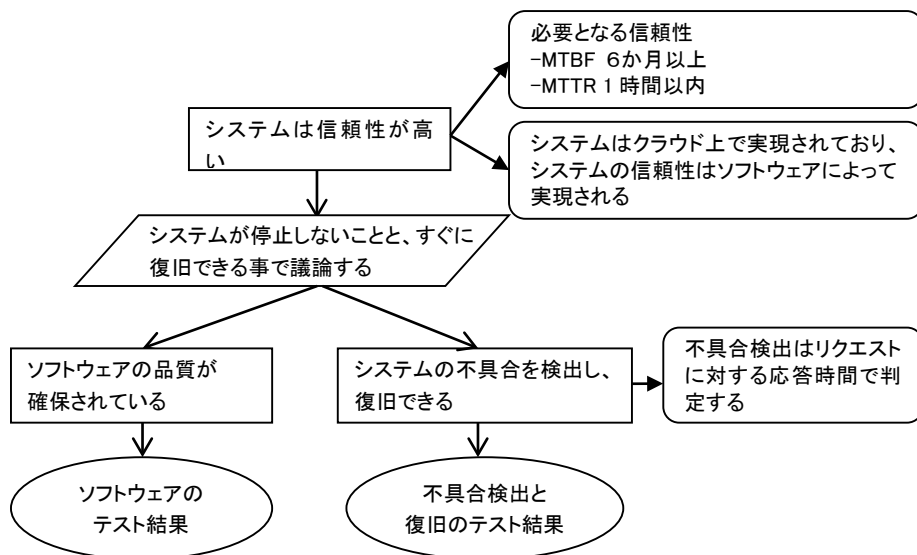


図 15-A-16-5 D-Case の記述例

この例ではあるシステムで信頼性が求められる際の議論構造を示している。トップゴールによって信頼性が必要であることを表明し、コンテキストを利用して具体的な制約を示している。ここでは MTBF<sup>5</sup>と MTTR<sup>6</sup>の要求があることから、システムの稼働時間と不具合時の復旧時間を観点として議論する事になっている。この観点がストラテジで示されており、さらに「ソフトウェアの品質が確保されている」と「システムの不具合を検出し復旧できる」というサブゴールに分解されている。システムの信頼性がサブゴールでソフトウェアの品質になっているのはトップゴールに「本システムがソフトウェアで実現されている」という前提があるため、その動作基盤に関する議論はここでは行わない事になっているからである。ソフトウェアの品質が確保されている事はそのソフトウェアのテスト結果をエビデンスとする事で保証される。また、システムの不具合を検出した際の動作についても、その機能が適切にテ

<sup>5</sup> Mean Time Between Failure: 平均故障間隔。故障発生から次の故障が発生するまでの平均期間

<sup>6</sup> Mean Time To Repair: 平均修復時間。故障が発生してから修復するまでの平均時間



ストされたという結果をエビデンスとする事で保証できる。エビデンスによってその上のゴールが保証されれば、さらに上位のゴールも満たされると考える。この場合では2つのエビデンスをもって「システムは信頼性が高い」という事が達成されている事を示している。このような構造を示して、ステークホルダ間でゴール分解や観点に不足がないか、ゴールに対するエビデンスが適切かを議論し、最終的に合意する。

本取組みでは D-Case を使い、チーム内で議論を進めながら開発を行った。そのプロセスは概ね以下の通りである。

- (1) チーム内のメンバーでロボコン活動のゴールを議論し、トップゴールとする
- (2) ゴールを D-Case で詳細化し、チーム内で妥当性について議論する
- (3) 詳細化したゴールを満たすために必要な項目を仮のエビデンスとして抽出
- (4) 仮のエビデンスを獲得するためのアクティビティの計画・実施
- (5) 開発を進める途中で気づいた項目や、外部から入ってきた情報についても D-Case に追加する
- (6) (2) から (5) を繰り返し、D-Case の洗練とエビデンス獲得を進める
- (7) 第三者説明用に D-Case を再度見直す

## 2.3. 解決のため採用したツール

近年 D-Case を記述するツールがいくつか出てきている。D-Case Editor<sup>7</sup> は Eclipse のプラグインとして D-Case を記述する事ができる。D-Case ステンシル<sup>8</sup>は Microsoft Power Point 上で小規模な D-Case を記述できる。D-Case Weaver<sup>9</sup> は Web Browser 上で動作する D-Case 記述ツールである。また、商用のツールもいくつか出てきている。これらを使用する事で D-Case の記述が容易になる。ただし、ET ロボコンの設計モデルは提出枚数が A3 用紙 5 枚と限られており、必要な情報を詰め込むためレイアウト上の制約が生じる。ツールでは細かいレイアウトの調整が難しい事もあり、本取組みでは上記のツールは使用せず Power Point の基本の図形セットで記述を行った。こうした制約がない場合はツールで記述した方が効率が良いと考えられる。

## 3. ET ロボコンでの D-Case の活用取組みと結果

### 3.1. 計画、準備

社内の ET ロボコンの参加概要について説明する。過去参加者から構成される推進メンバーが活動全体の計画及び推進、勉強会の開催を行っている。図 15-A-16-6 に 2014 年度 ET ロボコン活動の大まかなスケジュールを示す。11 月の全国大会は地区大会で出場権を得ない

<sup>7</sup> <http://www.dcase.jp/>

<sup>8</sup> <http://www.jst.go.jp/crest/crest-os/tech/D-CaseStencil/index.html>

<sup>9</sup> <http://www.jst.go.jp/crest/crest-os/tech/DCaseWeaver/index.html>

と参加できないため、当初の計画では確定していない。そのため、4月から地区大会がある9月までの期間を主として計画を立てている。D-Caseの取組みは2012年から行っているが、計画や内容としては大きくは変わっていない。

例年3月に社内でETロボコン活動の説明会を行い、参加メンバーの募集を行う。毎年新規にメンバー募集を行うため、半数程度は新規メンバーとなる。その後、集まったメンバーでチームを構成し、活動の進め方などを共有する。2014年度に集まったメンバーは12名であった。そのうち今回D-Caseの取組みを行ったチームはデベロッパー部門に参加した5名から構成されるチームである。この5人は全員がETロボコン初参加であり、4名は入社2年目の新人であった。

4月はチーム構成と並行して環境教育を行う。環境教育はロボットを動かした事がないメンバー向けに行う教育で、過去参加者1名、新規参加者2名程度の小さなグループを作り、ロボットを使った簡単な課題を実践する。課題は例えば「スタート地点から1m先にある目的ポイントで停止する」といったものである。このような課題を解く事で開発環境の設定、ロボットへのソフトウェアダウンロードの手順、ロボット用の各種APIの学習を行う。また、実際にロボットを動かしてみると、右と左で同じモータの出力をしているにも関わらず、目的の位置から右に大きくずれてしまうといったような物理的な問題を発見する事ができる。ロボットのドメインを知らない開発者にとって、初期のこのような立ち上げは有効である。

5月から活動が本格化し、8月に提出するモデルを記述する上で必要となる基礎知識の勉強会を行った。勉強会でを行う内容は開発プロセス、UMLモデル（ユースケース図、クラス図、状態図、シーケンス図など）、基本的なロボット制御などである。また、本取組みで使用するD-Caseに関しても記法と簡単な実習を2時間ほど行った。また、並行してETロボコン主催者側から提供されているサンプルコードをベースにロボットを動作させ、社内に用意したコース上を実際に走らせ、ロボットの特性を調査した。D-Caseの作成は勉強会が終わってから順次作成し、推進メンバーのレビューなどを通じてブラッシュアップしていった。7月に入ると8月の設計モデル提出に向けて提出用モデル作成作業に入る。ここではそれまで作っていたモデルやD-Caseを見直して洗練するとともに、審査員や第三者からみても分かりやすいように構成や見栄えなどの調整を行った。その後モデルに合わせた形でコードを実装した。ここではそれまでメンバーが作ってきた要素的なアルゴリズムや制御を寄せ集め、モデルに記述したフレームワーク上で動作するようにした。その後、大会に向けて主に走行の調整を行い、地区大会に臨んだ。

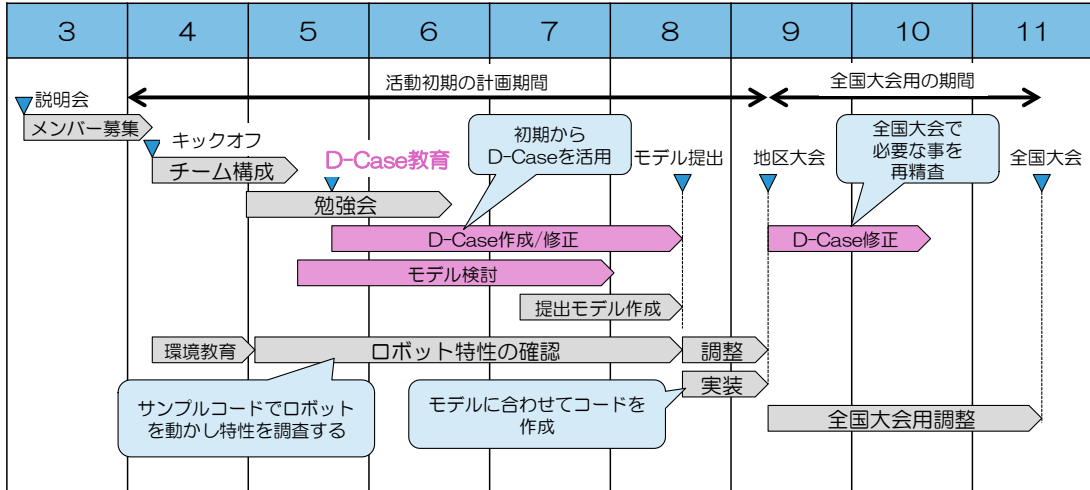


図 15-A-16-6 2014 年度のスケジュール

### 3.2. 実施

前述した活動の中で、どのように D-Case を作成・修正していったかを 2.2 で示したプロセスに沿って説明する。

- (1) チーム内のメンバーでロボコン活動のゴールを議論し、トップゴールとする

チーム構成のフェーズでメンバーは何を目指すかを議論した。この議論には個人ベースのものと、チームベースのものがあった。ET ロボコンの活動では自分たち自身が要求者と言えるため、初期の時点で何をを目指すかを合意する事が重要である。この議論は特に決まった形式があるわけではなく、通常のディスカッションである。この議論を通じ、「MDD<sup>10</sup>で性能の良いソフトウェアを作り、地区大会で総合優勝する」という目標を立てた。MDD はモデル駆動開発の事であり、単に大会結果だけでなくこうしたスキル向上に関する目標も明確にした。この目標を D-Case のトップゴールとした。

- (2) ゴールを D-Case で詳細化し、チーム内で妥当性について議論する

このトップゴールに対し、トップゴール達成に必要なサブゴールを抽出し、初期の D-Case を作成した (図 15-A-16-7)。トップゴールを分解する上で、トップゴールに含まれている目標別に分解を行う事にした。その分解の観点がストラテジノードの「目標要素ごとに検討」として記述されている。そして、その観点に基づいてトップゴールを「MDD によるソフトウェア開発」「ソフトウェアの高品質化」「地区大会総合優勝」の3つのサブゴールとして示している。「地区大会総合優勝」はさらにその評価要素をベースに「モデリング部門優勝」「競技部門上位入賞」としている。この D-Case は初期のものなので語彙や背景情報などは洗練されていないが、構造的に示す事によ

<sup>10</sup> Model Driven Development(モデル駆動開発)

り、チームメンバーで方向性の確認をする事ができた。

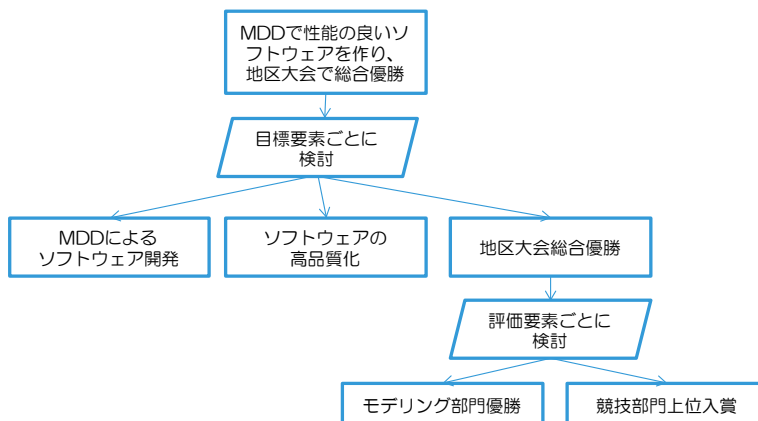


図 15-A-16-7 活動初期に作成した D-Case

初期の D-Case をベースに、さらに詳細化を進めた。その際、関連する情報はコンテキストとして関連付けた。図 15-A-16-8 が詳細化を進め、コンテキストによって情報を付け加えた D-Case である。一部、図 15-A-16-7 などからゴールの表現が変わっているが、これは議論を進める中で表現を変えたものである。

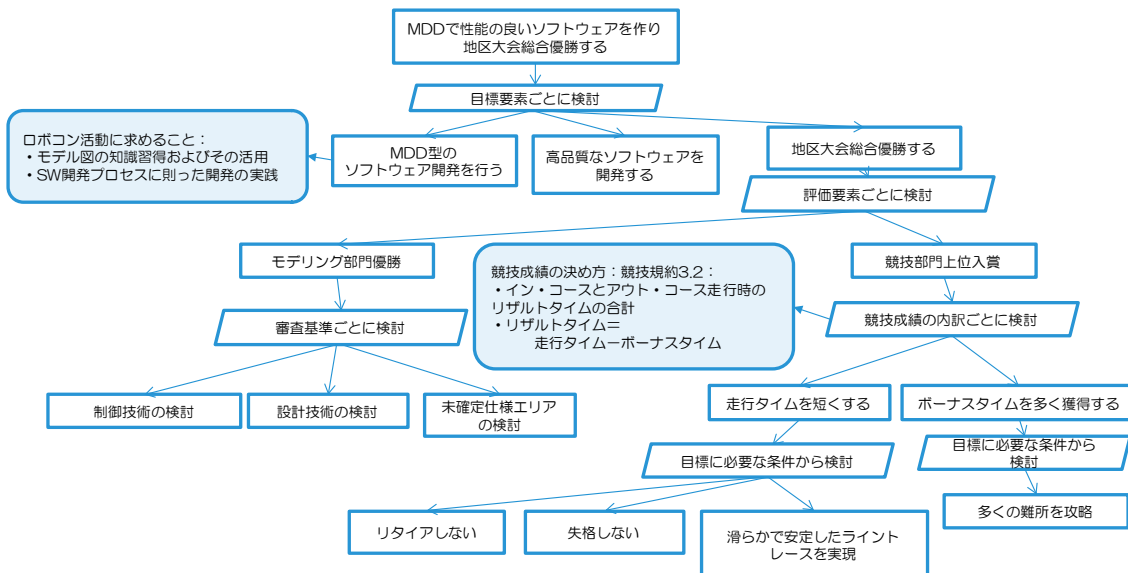


図 15-A-16-8 詳細化を進めた D-Case

図 15-A-16-8 では2つのコンテキストが記述されている。「MDD 型のソフトウェア開発を行う」に対しては、チームの議論の中で出た活動目標を補足情報として加えている。また、「競技成績の内訳ごとに検討」というストラテジに対してはその前提となる競技規約の情報を記述している。コンテキストを使用する事で各ゴールやストラテジの意図が見えやすくなる。メンバー間の共有も進みやすくなり、第三者に対しても

分かりやすくなる。ここまでのゴールの分解はゴールを満たす要素の観点で分解している。上位のゴールを満たすために必要な項目がある程度明確である場合、このような分解方法を使う事ができる。このような分解方法は完全分解または要求記述分解のパターンである[5]。

(3) 詳細化したゴールを満たすために必要な項目を仮のエビデンスとして抽出

D-Case の分解・詳細化分解を進め、そのゴールが満たされている事を示す項目が何かを検討する。検討された項目は仮のエビデンスとして D-Case 上に記述する。図 15-A-16-9 に図 15-A-16-7 の「リタイアしない」というサブゴールに対して詳細化し、仮のエビデンスを記述した D-Case を示す。

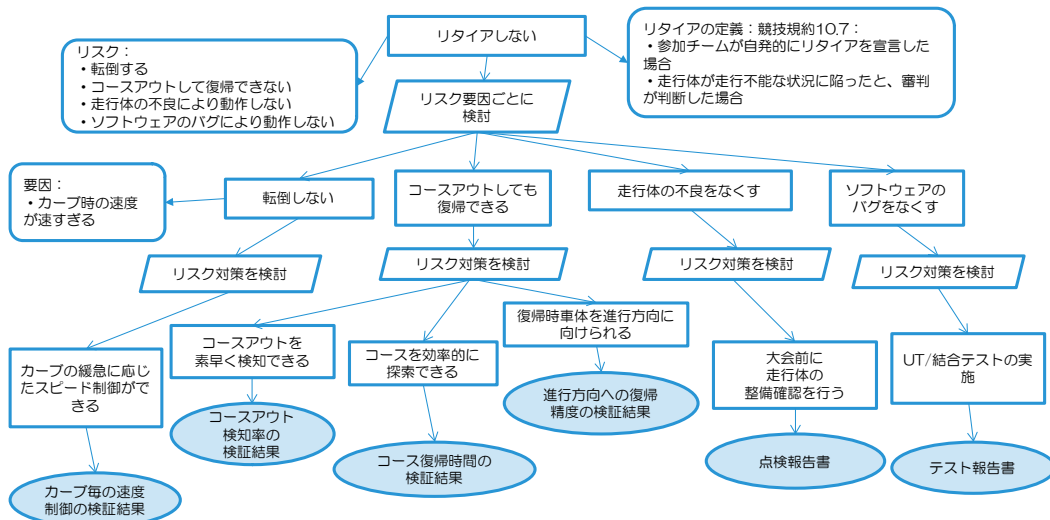


図 15-A-16-9 エビデンスを記述した D-Case

ここで、「リタイアしない」に関する分割について説明する。「リタイアしない」というゴールに対してはこれまでのように単純に要素で分解する事は難しい。そこで、リタイアをする要因をリスクとして抽出し、それが起きない事をサブゴールとしている。このような反例的なゴールの抽出は D-Case による分析でしばしば用いられる。ここではリタイアするリスクとしてコンテキストで「転倒する」「コースアウトする」「走行体の不良で動作しない」「ソフトウェアのバグにより動作しない」を抽出した。この D-Case を作成した時点ではまだロボットの特性をつかみ切れていないため、ある程度の想像も含んだ形で抽出している。ドメインの知見やデータがある場合には、リスク分析などに基づき抽出したリスクを使用した方が良い。「転倒する」に対する反例のサブゴールとして「転倒しない」を上げた。「転倒しない」サブゴールに対しては「転倒する」要因を上げ、それに対して満たすべきサブゴールを抽出した。同様にゴール分解を他のリスクに対しても行う。「リスクに対する対応」などのように、それが起きない事を直接分解できないような場合は、このように発生するリスクに対す

る反例をゴールとして進める方法を取る事で対応した。

サブゴールが満たされる事を、何らかのデータやテストを行う事で示す事ができそうと判断した時点で、その必要な項目をエビデンスノードとして記述する。これを仮のエビデンスと呼ぶ事にする。例えば「コースアウトを素早く検知できる」というサブゴールを満たすためには作成したソフトウェアに対し、コースアウト検知率に関する確認を行い、それがあるレベル以上にあれば検出が可能であることを示せる。

注意したいのはこの時点で抽出された仮のエビデンスは必ずしも達成できるものとは限らない点である。特に活動初期でロボットの特性が分からない状態では実現可能性が見えない事が多い。しかし、事前にゴール分解や必要なエビデンスをメンバーで議論して共有する事で、進め方の全体像が見えるようになった。

#### (4) 仮のエビデンスを獲得するためのアクティビティの計画・実施

次に抽出された仮のエビデンスに対し、確認用のソフトウェアを作成し実際のデータやテストを行い本来の証拠としてのエビデンスを獲得する。このエビデンス獲得作業は WBS(Work Breakdown Structure)のアクティビティとして管理を行った。アクティビティとして納期を決め、担当をアサインした上でステータスを管理した。この活動を通じてゴールを満たすと言えるデータを獲得できた場合には D-Case は変更せず、エビデンスを確定したものとした。達成したものとそうでないものの違いを表す表記は色を変える事で状態が分かるようにした。一方、作業を開始したものの、想定したデータの取得が困難であるなど、技術的課題や期間の関係でゴールの実現が難しいケースもある。このような場合には他のやり方を検討し、仮のエビデンスを別途作成するか、ゴールの見直しが必要となる。実際に図 15-A-16-9 の「コースを効率よく探索できる」というサブゴールに対するアクティビティを行う上で、コースアウト時にコースを探索して再度戻るといった事が技術的に難しい事が判明した。そのため、コースアウトしないというサブゴールは D-Case から外し、コースアウトしないようにする方式をベースに方針を切り替えた。

このように仮のエビデンスに対するアクティビティを行う上では実現できない可能性も含め作業を行い、必要に応じて D-Case の見直しを行う事が必要である。この場合でも D-Case がある事で影響範囲が見えやすく議論もしやすい。

#### (5) 開発を進める途中で気づいた項目や、外部から入ってきた情報についても D-Case に追加する

作成した D-Case は固定的なものせず、随時見直しを行った。新たに得られた情報や、活動を進めていく上で気づいた点も追加した。図 15-A-16-10 はそうした情報に基づいて D-Case のサブゴールを追加した例である。サブゴール「外乱光の影響を受けない」はロボットが黒線検知に使用している光センサに対して外乱光が入ることにより、制御のパラメータが狂ってしまうリスクに対して用意されたゴールである。これらは公開されている過去のモデルや過去参加者のアドバイスを参考に設定した。

また、ロボットの特性を調べる中で、コース内の難所に設定されているマーカーと呼ばれる灰色線によって制御パラメータが大きく振れ、これによってコースアウトするケースがある事が分かった。そこで D-Case に「グレー線上でコースアウトしない」というサブゴールを追加し、対策及びエビデンス獲得を検討した。このように D-Case に加えていく事で、情報共有が進むとともに、それが全体にどのような影響を与えるかを検討する事ができた。

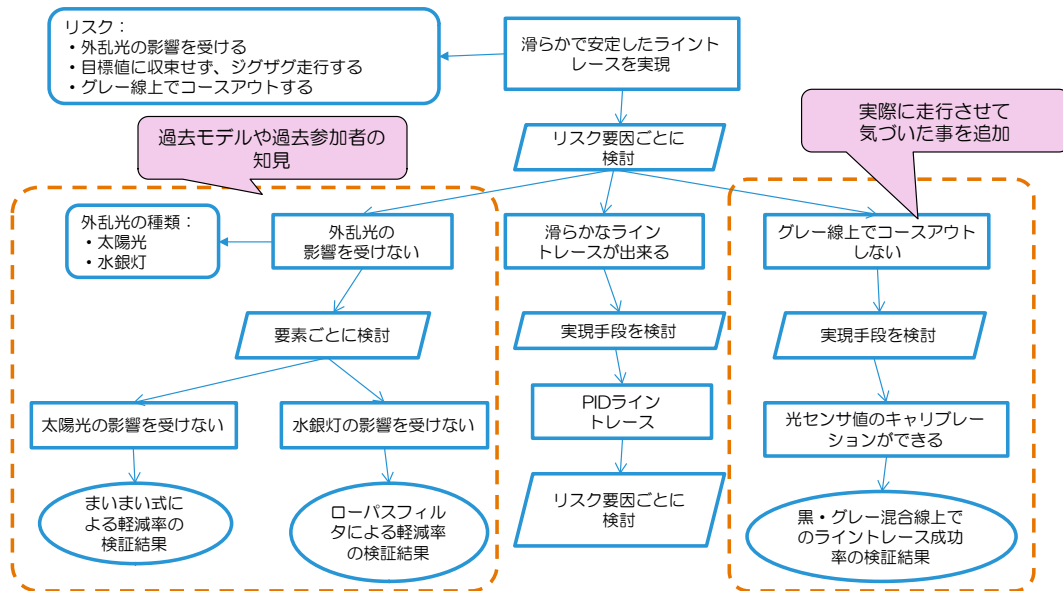


図 15-A-16-10 D-Case への情報追加

(6) (2) から (5) を繰り返す、D-Case の洗練とエビデンス獲得を進める

これまで述べたようなやり方でゴール分解とエビデンス獲得を行いながら開発を進めた。必要に応じて D-Case の構造も見直した。最終的には全てのエビデンスを獲得できる事が理想的であるが、実際には期間や人力的な問題で全てを保証する事は難しい。そのため、重要度・発生確率などからリスク分析を行い、影響度が低いと判断したものに関してはエビデンス獲得の作業を行わないことにした。

(7) 第三者説明用に D-Case を再度見直す

これまでの説明した D-Case は開発用に作成したものであるため、開発関係者以外では分かりづらい表記やゴール分解時にギャップが発生している事がある。図 15-A-16-11 にその例を示す。

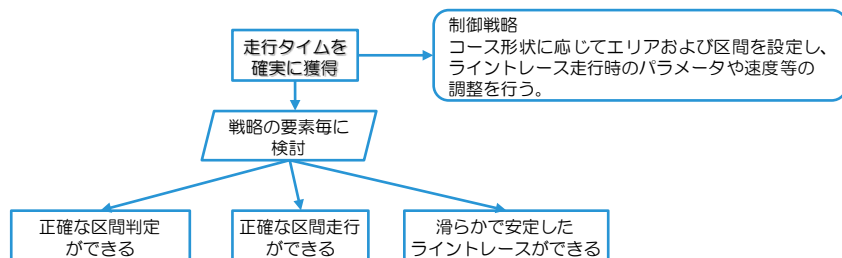


図 15-A-16-11 ゴール分解でのギャップが発生していた例

図 15-A-16-11 を見ると「走行タイムを確実に獲得」というゴールに対して、「正確な区間判定ができる」「正確な区間走行ができる」というように実現手段のサブゴールが出てきているため、これらが達成された場合に上位ゴールが達成できるかどうか分かりにくい。開発が進むと内部の実現方法などが見えてくるため、このようなギャップが発生してしまう事があった。そのため、外部の観点からレビューを行う事も必要である。本取組みでは推進メンバーがレビューを行い、その後図 15-A-16-12 のように修正した。

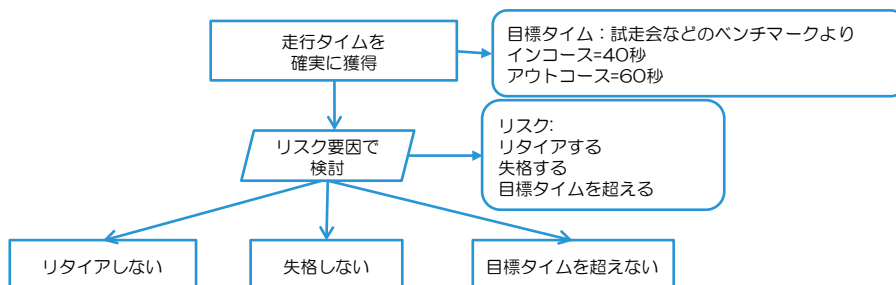
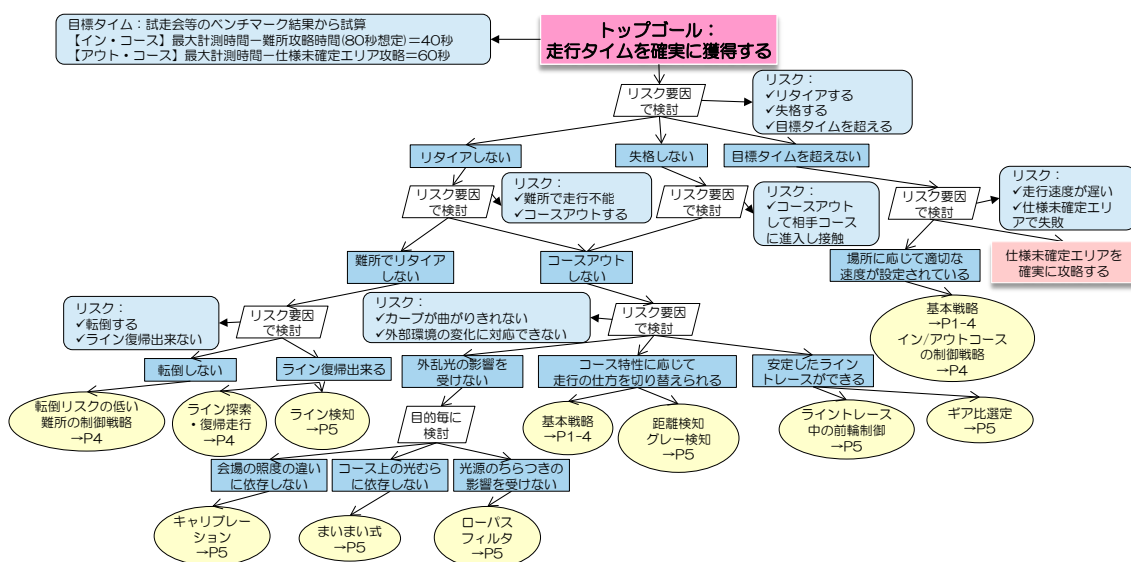


図 15-A-16-12 レビュー後の D-Case

「走行タイムを確実に獲得」というゴールは変更していないが、チームメンバーにヒアリングした結果、単純に走行タイムの獲得ができれば良いわけではなく、目標の時間がある事が分かった。そこで、コンテキストによって獲得したい時間の基準を明確にし、そのゴールが満たされない要因ごとの分解を行った。このようにして上下のゴールのバランスを取るようにした。ただし、この場合でもそれまで獲得していたエビデンスはほぼそのまま使う事ができた。

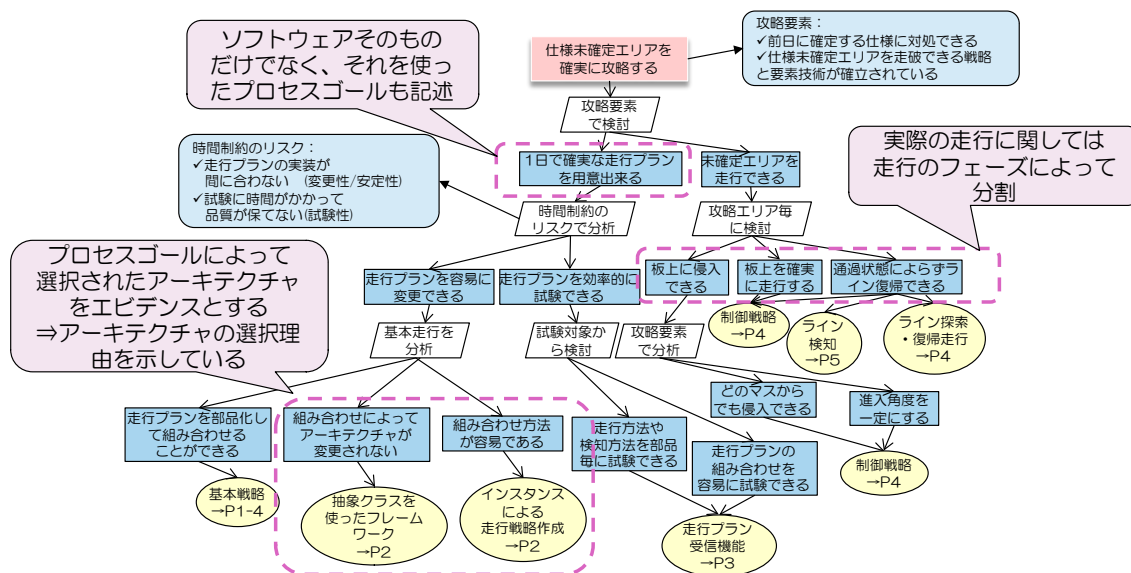
このようにして作成した D-Case のうち、提出モデルに記述した走行部分の D-Case を図 15-A-16-13、図 15-A-16-14 に示す。





注：図中に記述されているページ数は提出した設計モデル資料内の該当ページを示している。

図 15-A-16-13 提出した D-Case (走行部分)



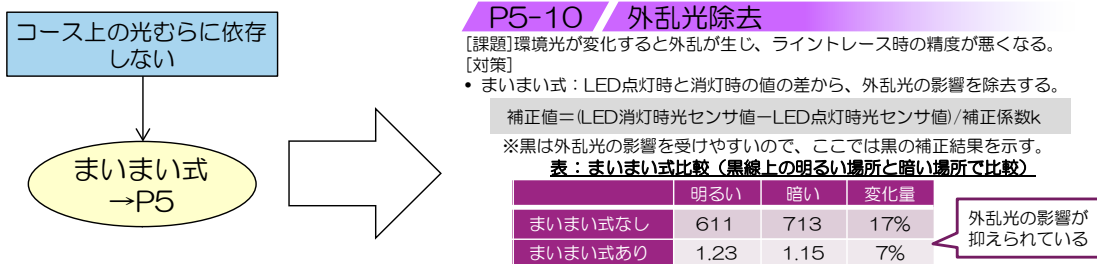
注：図中に記述されているページ数は提出した設計モデル資料内の該当ページを示している。

図 15-A-16-14 提出した D-Case (仕様未確定エリア部分)

図中のエビデンス内に記述されているページ数は提出した A3 用紙 5 ページからなる設計モデル資料内の該当するエビデンスが示されているページを示している。このようにエビデンスに対するリファレンスを示す事で D-Case を中心に設計資料を参照できるようにした。図 15-A-16-15 にエビデンスとして設計モデルに記述した例を示す。ここでは「コース上の光むらに依存しない」というサブゴールに対して、まいまい式というアルゴリズムを使用する事で達成できる事を D-Case 上で表明している。

そして、外乱光がある場合の影響をこのアルゴリズムによって軽減できる事を実際のデータによって示している。

また、図 15-A-16-14 の仕様未確定エリアに関する D-Case では本課題に対して重要な「1 日で確実な走行プランを用意できる」というプロセス上の要件を記述した。そのためには走行の組み合わせを容易にするためのアーキテクチャが必要である事を示し、クラス図などの設計要素と関連付けた。



注：図中に記述されているページ数は提出した設計モデル資料内の該当ページを示している。

図 15-A-16-15 エビデンスの記述

### 3.3. 結果の分析・まとめ

本取組みでは要求が不明確な状態から D-Case を活用し、チームメンバーで議論と合意をしながら開発を行った。このプロセスにより、チーム活動を進める上でのメリットと課題についてヒアリングを行った。以下にメンバーからの評価を紹介する。

#### 3.3.1. メリットに関して

- (1) D-Case を使ってゴールを分解する事で要求を発散させることなく進める事ができた

D-Case の上位ゴールをどうやって満足するかというルールに従う事で、議論の方向性を見失うことなく議論ができたとの意見が多く挙げられた。特にストラテジノードによって分解の観点を明記してある事で、後から見返した時や第三者に対しても議論の構造が分かりやすいとの意見もあった。SysML<sup>11</sup>の要求図などでは観点の記述が必須ではないため、ゴールの分解がどのように行われたか分からず、議論が戻ってしまう事がある。コメントなどのノードを使う事で補足する事はできるが、この点では観点を明示する D-Case の方が理解性が高いと考える。

- (2) 仮のエビデンスを先に出す事で必要な作業を先に抽出し、効率化がされ信頼性の向上に役立った

あらかじめゴールを満たすために必要な要素を抽出しているため、闇雲に作業を行うよりも何をすべきかが明確であり、またその目的も共有化されているため、作業が

<sup>11</sup> SysML: Systems Modeling Language

効率的と感じたようである。また、エビデンスの獲得はそのままシステムの信頼性の保証をする事につながるという意識を持てたという意見もあった。

- (3) 仮のエビデンス獲得をアクティビティとして計画する事で進捗管理がしやすくなった

(2) のメリットと関連するが、仮のエビデンスを使うことで、何をしなくてはならないかを計画しやすくなった。また、どのエビデンスが獲得できていて、どれができていないかを把握する事でどのあたりがゴールに影響がありそうなのかが分かり、進捗管理に役立ったとの意見もあった。また、ゴールが共有されている事もプロジェクトを進める上で有効であったと思われる。

### 3.3.2. 課題

- (1) ゴールの分解方法

ゴールを分解する際の観点をどのように使い分ければ良いか分からなかったとの意見があった。また、観点を決めた際も分解したゴールによって網羅されているのか、妥当なのかの評価が難しかったようである。参考文献[5]には多くの分解パターンが紹介されているが、こういった場合にどのパターンを使うのが良いのかを見極めることは今後の課題である。また、網羅性に関しては D-Case だけでなく従来の問題分析手法などを組み合わせる必要があると考える。

- (2) トレードオフの表現の仕方

ET ロボコンは他チームとの競技であるため、単にコースアウトしないという安全性だけを求めても「上位入賞」というようなゴールは満たせない。スピードを出すとその分制御が追いつかなくなり、コースアウトのリスクが高まる。このようなトレードオフの関連をどのように示すべきであるかが明確ではない。また、エビデンス獲得活動により実現が難しいと判断されたゴールを現状の D-Case では削除している。そのため、実現が困難で外したという情報が D-Case 上で参照する事ができず、後に再度議論に上がってしまう可能性がある。

いくつかの課題はあるが、D-Case を使う事でチームメンバー間のゴール共有が進み、エビデンスを先に抽出する事で作業の効率化ができたと言える。また、このプロセスを通じてシステムがゴールを満たす事を示す説明資料を作り上げる事ができた。

本取組みによって ET ロボコンでの成績がどのように変化したかを説明する。表 15-A-16-4 は D-Case の活用を始めた 2012 年からの ET ロボコンの成績の推移である。

表 15-A-16-4 2012 年以降の ET ロボコンの結果（南関東大会）

参加年度	チーム名	モデル 審査評価	競技順位	総合
2012 年 (34 チーム中)	チーム F	A (優勝)	6 位	2 位
	チーム G	B	7 位	6 位
2013 年 (27 チーム中)	チーム H	B+	4 位	4 位
2014 年 (10 チーム中)	チーム I	A- (準優勝)	1 位	1 位

(モデル審査評価はA+~D-までの 12 段階であり、ここではAが最も良い評価で優勝)

2013 年、2014 年で出場チームが減っているのは ET ロボコンの参加部門が分割され 2013 年は 2 クラス、2014 年度は 3 クラスに、分散されたためである。その影響も加味する必要はあるが、D-Case を用いて以降の競技部門の成績は比較的上位で安定してきている。特に 2014 年はチームメンバーに過去参加者がいなかった事、使用するロボットが過去に使用していたものから変更になった事で過去参加者の経験があまり使えなかった状況を考えると D-Case を使用したプロセスに一定の効果があったものと考えられる。

#### 4. 達成度の評価・取組みの結果

本取組みに対して 1.2 で挙げた各目標に対しての達成度は以下の通りである

- (1) D-Case を活動初期から活用し、チーム活動としてのゴールと全体像を示しながら開発を行う事

D-Case の勉強会を行い、チーム活動の初期から D-Case を使ったゴール設定を行った。活動に応じて D-Case を修正するなど、D-Case を中心とした開発の取組みを行う事ができた。

本手法により開発者からは要求の発散を抑える事ができたとの感想があり、D-Case による議論構造の明確化が寄与したのと考えられる。また、ソフトウェアに関する要求だけでなく、「MDD 型のソフトウェア開発をする」というメンバーのスキルアップに向けた目標も明確にできた。最終的に作成したコードは提出したモデル通りに実装されており、MDD 型の開発ができていた。参加者の一部には競技を優先し、モデルで書いた内容と実際のコードが異なってしまう事もあった。あらかじめ自分たちの目標を D-Case で明確にしてメンバーで共有する事で、安易なコード変更を防ぎ、モデルとコードを一致した状態で開発を進める事ができたと考えられる

- (2) 手戻りを抑え、効率的な開発を通じて競技部門の成績を向上させる事

本取組みの手法を導入した 2012 年からは競技部門の成績が安定して上位に入るようになり、一定の効果を上げている。ただし、本手法でどれだけ手戻りを抑えられているかはデータとして取得できていない。定性的な結果としては、各作業の目的を理

解する事で無駄な検証作業を抑える事ができたなどの感想が開発者から寄せられており、効果を感じてもらえた。また、エビデンス獲得作業をアクティビティとして計画・管理した事もプロジェクトを効率的に推進する上で有効であったと考えられる。さらにエビデンス獲得が困難であると分かった時点でその影響を D-Case で把握し、ゴールの見直しをするなどの対応を取った事も大きな手戻りを発生させなかった要因と考えられる。

### (3) 第三者に対して設計意図と設計の妥当性、およびシステムの信頼性を示す事

開発で作成された D-Case は第三者から見た際に分かりづらい事があった。そのため、外部視点でのレビューを行い調整した。また、エビデンスと検証結果を関連付くようにした。また、各種設計要素についてもその設計意図を D-Case 上で示した。その結果 2012 年度のモデルは ET ロボコンの審査員より「要求から技術検証まで十分にトレーサビリティが取れている」というコメントをいただいた。また、2014 年は地区大会において設計モデルで優勝するだけでなく、高信頼性や安全性に関して顕著な取組みが見られたチームに贈られる特別賞である IPA 賞も受賞する事ができた。D-Case を使った表記は第三者から見ても理解されやすいものと考えられる。

これまで述べたように、D-Case を使用してゴールを分解し、仮のエビデンスを先に抽出し、そのエビデンスを獲得するというプロセスを実行する事で、それまでの課題に対応する事ができた。しかしゴールの分解観点や網羅性の担保方法などにはまだ不確定な点も多い。本取組みにおいても地区大会では良い成績を残したものの、2012 年/2014 年に出場した全国大会は競技中にリタイアとなり、期待した成績が残せなかった。その理由は、2012 年は外乱光に対する考慮が不足し、2014 年は使用していた機体の組み合わせミスが全国大会直前に見つかри、それまでに調整していたパラメータではうまく動作しなかったためであった。このようなリスクの抽出漏れや、リスクの過小評価は D-Case を使ったとしても抽出できるとは限らない。ET ロボコン活動ではその目的がスクラッチからソフトウェアを作ることにあるため、D-Case も毎回作り直しているが、本来、ある特定の製品開発のような場合には何度か D-Case を運用する事が必要である。こうする事で D-Case 自体をノウハウとして蓄積し、リスクなどの抜け漏れを防ぐ事ができるものと考えられる。

## 5. 今後の取組と考察

本取組みでは ET ロボコンという比較的小さなプロジェクトで D-Case を使用したプロセスを導入し、成果を上げる事ができた。しかし、本プロセスが全体に対してどれくらいの効率化に寄与したかはメンバーの感想などの定性的なものが多く、定量的な評価ができていない。この点は今後の課題である。

今回の取組みをベースに業務のプロジェクトに対しても一部 D-Case の導入を始めている。ただし、複合機開発では規模が大きいため、既存のプロセスをすぐに入れ替える事は難しい。

そのため、まずプロジェクトとして目指す姿を共有するために **D-Case** を使用している。規模が大きい場合には詳細な目的までも含めてしまうとサイズが大きくなってしまいうため、上位の **D-Case** は本当に重要な要件に絞って **A3** 用紙 1 枚に収まるようにしている。まだ非公式な付加文書的な扱いであるが、今後プロジェクト内での意思疎通や意思決定の判断材料として広く使用されるように推進する予定である。また、エビデンスの関連付けについても現状プロセスとの整合を含め検討する予定である。

本取組みで行った方法はある側面ではアジャイル開発に近いプロセスと言える。アジャイル開発は文書作成よりも動作するコードを優先した反復型の開発スタイルであるが、**D-Case** を使用する事で顧客やメンバー間の意思疎通をより良く取れると考えられる。こうしたアジャイル開発への **D-Case** 取り込みも今後取り組んでいきたい。

参考文献

- [1] 2014 年 ET ロボコン概要、<http://www4038up.sakura.ne.jp/2014/gaiyou/intro.php>
- [2] ET ロボコン 2014 デベロッパー部門競技規約 1.0.0 、  
<http://www4038up.sakura.ne.jp/2014/gaiyou/kiyaku.php>
- [3] ET ロボコン 2014 デベロッパー部門審査規約、  
<http://www4038up.sakura.ne.jp/2014/gaiyou/shinsakiyaku.php>
- [4] 土樋 祐希、杉浦 英樹：10 MLOC in Your Office Copier, IEEE Software, November-December 2011 Vol.28
- [5] 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、近代科学社 ISBN9784764904613
- [6] 上野 肇、松野 裕：ET ロボコンを対象とした D-Case 記述事例、ソフトウェアシンポジウム 2013
- [7] 大槻 繁：ソフトウェア開発はなぜ難しいのか ～「人月の神話」を超えて、技術評論社、ISBN 4774152757
- [8] Peter Bishop, Robin Bloomfield：A Methodology for Safety Case Development. In Safety-Critical Systems Symposium (SSS 98), 1998.
- [9] Tim Kelly, Rob Weaver：The Goal Structuring Notation - A Safety Argument Notation, In Proc. of the Dependable Systems and Networks 2004 Workshop on Assurance Cases, July 2004
- [10] Yutaka Matsuno：A Design and Implementation of an Assurance Case Language, in Proc. of The 44th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN) 2014, pp. 630-641

掲載されている会社名・製品名などは、各社の登録商標または商標です。

独立行政法人情報処理推進機構 技術本部 ソフトウェア高信頼化センター (IPA/SEC)