

一般社団法人

ディペンダビリティ技術推進協会

D-Case部会

はじめての D-Case



20
18



はじめての D-Case

2018 年 6 月 5 日

一般社団法人 ディペンダビリティ技術推進協会

D-Case 部会

もくじ

- 1 はじめに
- 2 D-Case 手法の背景
- 3 D-Case 記法の基本
- 4 D-Case ステップ
 - 4.1 ステークホルダの分析
 - 4.2 D-Case の記述
 - 4.3 合意形成の実施
 - 4.4 D-Case ステップの例
- 5 ステップ実施に向けたヒント
 - 5.1 前提ノードの重要性
 - 5.2 前提ノードの設定上の注意
 - 5.3 ゴール分割の例
- 6 D-Case ステップの実例
 - 6.1 テスト戦略の合意
 - 6.1.1 テスト戦略とは
 - 6.1.2 テスト戦略の立て方とD-Case
 - 6.2 ET ロボコンの実例
 - 6.2.1 ET ロボコンの概要
 - 6.2.2 D-Case の適用
- 7 まとめ
- 8 参考文献
- 9 用語

1 はじめに

人に何かを伝えることは簡単そうで難しいものです。開発現場の中での作業依頼や、打合せでの伝達事項など、うまく伝わったと思っていても、手戻りや発注ミスなど開発効率の低下や品質の低下などにつながるが発生しています。なぜでしょうか？ これは共通に理解していることは何かに配慮せずに「伝えたいこと(主張したいこと)」だけを伝えることに原因があります。伝えたいことの根拠や、前提条件など必要な情報を添える必要があるのです。これらの「伝えるため」に必要な項目を図示できるようにしたのが D-Case であり、よりよい伝達手段の提供を狙っています。

本書は、DEOS 協会(*1-1) D-Case 部会および連携している企業各社メンバからなる技術交流会活動において、初学者に向けた D-Case 記述のガイドブックが必要であろうとの認識により共同でまとめたものです。実際に効果を上げた事例もでてきています(6 章を参照してください)。

D-Case は、JST CREST の DEOS プロジェクト(*1-2)から誕生した重要な技術の1つであり、現在は DEOS 協会において研究・普及活動を継続しています。本技術交流会には D-Case の社内での利用・活用に関心のあるメンバが参加しており、D-Case 研究者とともに活用の検討・普及に向けた活動を進めています。

大規模、複雑化し変化し続けるシステムが提供する商品やサービスを利用者が安心して継続的に利用できるようにするためには、関係者同士の共通の理解や合意および説明責任が必要になると考えています。D-Case は、これらの共通の理解や合意および説明責任を遂行するための技術・ツールとして研究・開発・実証実験(*1-3)が進められています。

D-Case は、システム全体を対象とした比較的大規模な論証のために活用することもできますが、開発や企画の中での指示伝達、意思疎通、共通理解などのコミュニケーションの向上に向けた、比較的小規模な論証のために活用することもできます。

初心者がいきなり大規模な D-Case を記述することは現実的ではなく、まずは小規模な D-Case から始めることをお勧めします。このことから、本ガイドでは初心者に向けた比較的小規模な D-Case の記述方法を実例も交えながらわかりやすく解説したものとしました。

本書の構成は目次に示した通りです。

2 章では D-Case の背景に関して述べ、3 章で D-Case 記法の基本、4 章で D-Case の基本的な作成のステップについて説明しています。この第 3 章と第 4 章は初心者にとっては必須の内容であり、複雑で高度な内容は排除し簡潔に述べられているので短時間でスタートラインに立つことが可能となっています。また、理解を促進するために 4.4 章として D-Case 作成の例も示しています。5 章では実際に記述する際のヒントについて述べています。実際にいくつかの D-Case を記述しながら、適宜 5 章を参照することにより躓きやすいポイントからの脱出の助けになればと考えています。6 章では、開発におけるテストフェーズに関して D-Case を適用することにより、手戻りの削減を実現した例や、ET ロボコンの開発に D-Case を適用して、開発者間のコミュニケーション向上および審査員へのアピール向上により高成績につなげた実例を示しています。この実例全体や一部を参考に、まずはいくつかの D-Case の記述にトライすることをお勧めします。

本ガイドが、開発や企画の現場における指示伝達、意思疎通、共通理解の向上に関して、多少でも有効なヒントを提供するものとなれば幸いです。

(*1-1) <http://deos.or.jp/index-j.html>

(*1-2) <http://www.jst.go.jp/crest/crest-os/osddeos/index-j.html>

(*1-3) <http://www.dcase.jp/p/jcase.html>

2 D-Case 手法の背景

D-Case 手法は JST CREST DEOS プロジェクトのサブプロジェクトの1つとして 2009 年より研究が開始されました。当時、IT システムの複雑化とネットワーク化が増し、システムのデューパビリティをどのように維持するかが課題になっていました。現在では、システムの IoT 化などにより、複雑化とネットワーク化はより進展しました。最近、大手企業でのシステム品質の監査で問題になる事例がニュースになっていますが、システムの進化に追いつけず、上層部と現場のコミュニケーションがうまくいっていないことが原因の一つと考えられます。D-Case は、このシステム開発におけるコミュニケーションの課題を解決するためには、アシュアランスケース(assurance cases)、およびその記法の 1 つである GSN(Goal Structuring Notation)が良いのではないかと考え、研究開発、ワークショップの開催などを行っています。

アシュアランスケース(assurance cases)の対象は主にシステムの安全性で、その場合セーフティケース(safety cases)と呼ばれます。セーフティケースには色々な定義がありますが、その定義の1つは以下になります。

「A safety case is a structured argument, supported by evidence, intended to justify that a system is acceptably safe for a specific application in a specific operating environment (*2-1).」

「セーフティケースは、システムが特定の運用環境で特定のアプリケーションに対して許容可能な安全であることを正当化することを意図した、証拠によって裏付けられた構造化された論証(以降議論を論証とする)である。」

(*2-1) Defence Standard 00-56 Issue 4 (Part 1): Safety Management Requirements for Defence Systems. UK Ministry of Defence. p. 17

セーフティケースはイギリスを中心に、主に安全性に関する国際規格において要求項目になっています。自動車の機能安全規格であり、日本でも利用が進んでいる ISO26262 でも提出が義務付けられています。

アシュアランスケースの基本的な考え方は、システムの安全性などをトップゴールにして、議論を尽くして、証拠を元に保証するという考え方です。D-Case プロジェクトでは、システムのディペンダビリティにこの考えを適用し、簡単なディペンダビリティケース(dependability case)を作ってみようというのが最初の試みでした。これらのディペンダビリティケースを見た複数の企業の方から「企業間にまたがるシステム開発における合意形成に有効なのではないか」という評価を得ました。以後、組込みシステムを中心に、ディペンダビリティケースの記述を試みました。dependability case (*2-2)では英文で長く、日本では馴染みにくいことから、D-Case という名称になりました。以後、多くの企業の方と共同で、様々なシステムの D-Case を試作し、その記述法を「D-Case ステップ」としてまとめています。

(*2-2) Defence Standard 00-56 Issue 4 Dependability case は国際規格 IEC62741:2015 で規定されていますが、本冊子では、「ディペンダビリティ」に関するアシュアランスケースという一般的な意味で用いています。(Part 1): Safety Management Requirements for Defence Systems. UK Ministry of Defence. p. 17

3 D-Case 記法の基本

簡単に D-Case(*3-1)の説明をします。

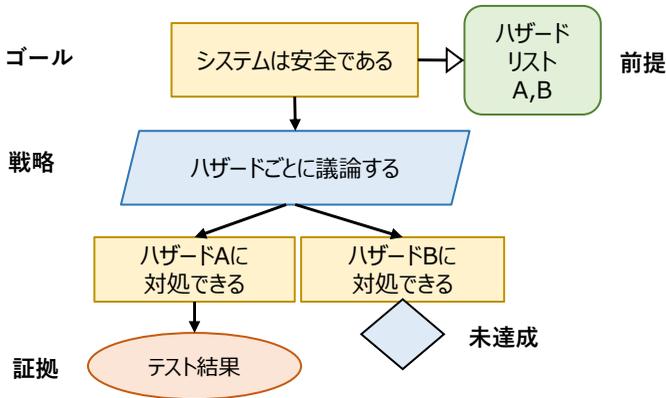


図 3-1 D-Case の簡単な例

この D-Case では、あるシステムの安全性議論を表しています。一般にシステムの安全性を議論するには様々な議論の方法があります。ここでは、ハザード分析の結果として、ハザード A,B があったという前提で議論しています。この前提を元に、議論をハザードごとに分けます。D-Case では議論を主に木構造で展開していきます。展開は好きなだけできますが、無限にすることはできないので、最後に詳細化された主張を担保する証拠をおきます。この例では、「ハザード A に対処できる」というゴールノードの主張が正しいことの証拠として『テスト結果』があることを示しています。一方「ハザード B に対処できる」というゴールに対してはひし形のノードがつけられています。これは「未達成ノード」といい、その時点で

(*3-1) D-Case には2つの意味があります。一つは GSN に DEOS プロジェクトで議論されてきたモニタリングや、モジュールやパラメータなどを構文に加えた表記法としての意味です。もう一つは、本書で説明されている D-Case ステップを用いた手法としての意味です。本書では、この2つを D-Case と呼ぶことにします。

まだゴールに対して十分な議論や証拠が無い場合に用いられます。

GSN は主に5種類のノードを用いて記述します。ゴール、前提、戦略、証拠、未達成ノードです。それぞれの意味を下の表に示します。記号の中は文例です。

ノード	記号	説明
ゴール (Goal)	システムは安全である	ステークホルダ間で合意したい主張
戦略 (Strategy)	部品ごとに説明	上位のゴールの分解の仕方を説明
前提 (Context)	テスト仕様書	議論の前提となる情報
証拠 (Evidence)	テスト結果	ゴールが達成できていることを示す証拠 テスト結果などのモノ、ドキュメント
未達成 (Undeveloped)		まだ具体化できていないゴールや説明であることを示す

図 3-2 GSN のノード

ノードのつなげ方を説明します。

前提ノードは、ゴールもしくは戦略ノードにリンクされます。前提ノードをリンクする場合は、白抜きのリンクを用います。ゴールには戦略、証拠、未達成ノードがリンクされます(未達成ノードをリンクする場合は矢印を省略します)。この場合、黒抜きのリンクを用います。ゴールと未達成は、矢印を用いずに直接つなげます。

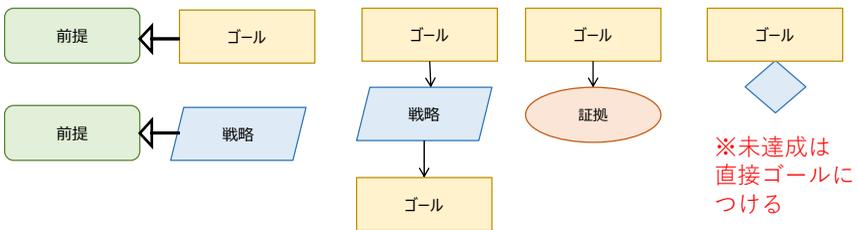
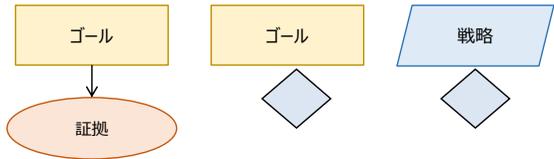


図 3-3 ノードのつなげ方

D-Case は、基本的にはゴールの分割による木構造の形をしています。ゴールを戦略にもとづき、説明しやすいサブゴールに分割します。D-Case の終端には証拠か未達成ノードを置きます。

終端は必ず
「証拠」か「未達成」



「ゴール」は「戦略」に基づき
サブゴールに分解する

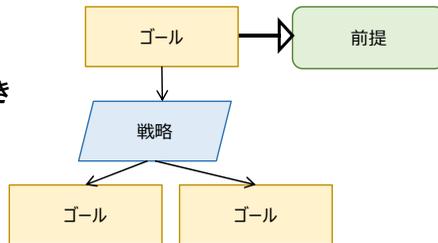


図 3-4 D-Case の木構造

4 D-Case ステップ

ステークホルダ(Stakeholders)は日本語では利害関係者と訳されますが、近年では、ステークホルダの範囲が広がっています。例えば企業の製品、サービスの不具合に対して、メディアが一斉に報道し、直接の利用者ではない一般の人々からも非難を受け、社会全体に対してお詫びをするニュースを度々聞くようになりました。このようにステークホルダは多様になってきており、それらのステークホルダを出来る限り認識する必要があります。しかしながらそれらすべてのステークホルダのための D-Case を記述することは不可能です。そのため D-Case ステップでは、対象とするステークホルダをステップ1でまず想定します。

D-Case を記述するにあたっては、ステークホルダの分析が必要です。ステークホルダが何に重点を置いているのか、何に興味関心があるのかを明確化することにより、D-Case に記述する情報量を小さくすることができます。ステークホルダの明確化を含めた D-Case のステップは次のようになります。

- D-Case ステップ 1. ステークホルダの分析
- D-Case ステップ 2. D-Case の記述
- D-Case ステップ 3. 合意形成の実施



図 4-1 D-Case の3つのステップ

以下にそれぞれのステップを説明します。

4.1 ステークホルダの分析

D-Case を利用して論証を行い正しく合意形成するためには、ステークホルダの明確化が必要ですが、それを行うためにはステークホルダの分析が必要になります。また、論証相手にその妥当性を判断できる基準を与えるために、合意形成したい内容について具体的な対象とあるべき状態(あるべき姿)をトップゴールノードに設定する必要があります。

ステークホルダの分析では、合意形成したい内容を踏まえてステークホルダの立場や関心ごとを分析するほか、論証に影響を与えるステークホルダの立場や関心ごとを分析する必要があります。

例えば、企業内で「自動運転を普及させ、販売する」という目標があり、メーカ広報担当者が「自動運転は楽しいことがユーザに伝わる」ことをトップゴールとした議論を例にすると、メーカ広報担当者は提案を行う人であり、関係者であるTV・CM担当やカタログ担当、アンケート担当の狙いや関心ごとなどを踏まえて議論に臨みます。一方、メーカ判断者は提案を受け議論により判断を行う人であり、関係者である商品企画担当の企画コンセプトや、開発担当や販売担当の狙いや関心ごとなどを踏まえて議論に臨み判断を行います。また、何れの立場においてもユーザの関心ごとについての理解や考慮なしには、価値ある議論はできないといえます。

図 4-2 企業での合意形成におけるステークホルダの関係を示します。

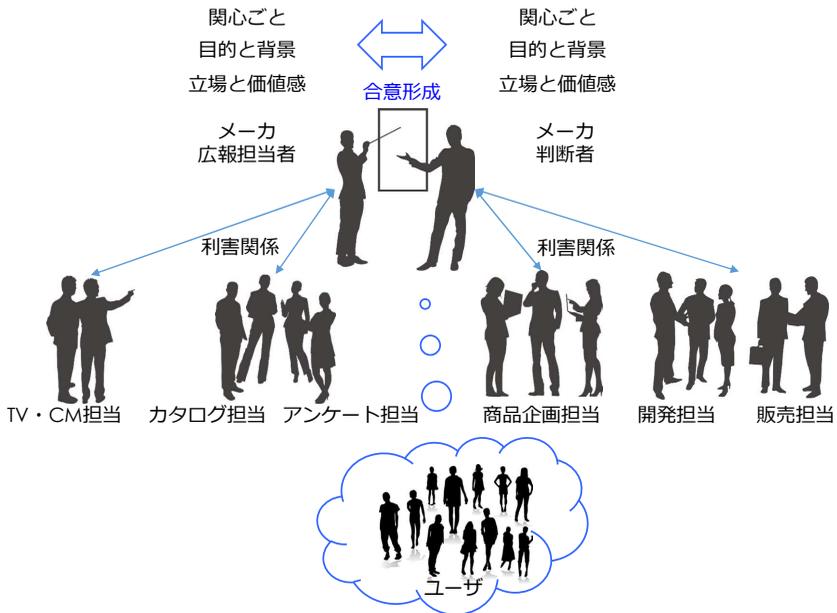


図 4-2 企業内での合意形成におけるステークホルダ

上記例では、メーカー判断者は説明を受ける側としてのステークホルダになります。また、ステークホルダには、直接関与する人と、間接的に関与する人と分類できるほか、合意形成に影響を与える人としても分類することができます。

D-Case の利用によりステークホルダ間の理解を深め認識を合わせ合意形成するためには、ステークホルダの関心ごとに加えて、合意する目的とその背景、各々の立場と感じる価値、合意に影響を与える利害関係を理解しておく必要があります。

表 4-1 に企業におけるステークホルダの立場と関心ごとの分析例を示します。

表 4-1 企業におけるステークホルダの立場と関心ごと

ステークホルダの立場	関心ごと
メーカー判断者	商品内容と広報内容がマッチし商品が売れる
商品企画担当	企画コンセプトと広報内容がマッチしている
開発担当	広報内容が開発内容とマッチしている
販売担当	試乗会に多くのユーザが来場して商談としたい
メーカー広報提案者	ユーザにメリットを伝え商品が売れる
TV・CM担当	TV・CMでユーザに分かり易く伝えたい
カタログ担当	カタログで分かり易く説明したい
アンケート担当	試乗会で有効なアンケート結果を得たい
ユーザ	ファミリーで楽しく車を使いたい

次に、一般的なディーラでの商談を例にすると、ディーラ営業担当がお客様の要望に合う商談を提案して合意を得たい場合、直接関与する人はお父さんですが、お母さんの理解なしには商談は進みません。また、両親の要望に応えれば資金面での心配は減ります。さらに営業責任者/上司の関心ごとを理解していれば、値引きも可能となります。ディーラ営業担当者はこれらの関心ごとや、立場や背景を理解し、ディーラ内の関心ごとにも加味した上で商談を進めなければ商談成立(合意)には至らないといえます。

図 4-3 にディーラでの商談(合意)におけるステークホルダの関係を示します。また、表 4-2 にディーラでの商談におけるステークホルダの立場と関心ごとの分析例を示します。

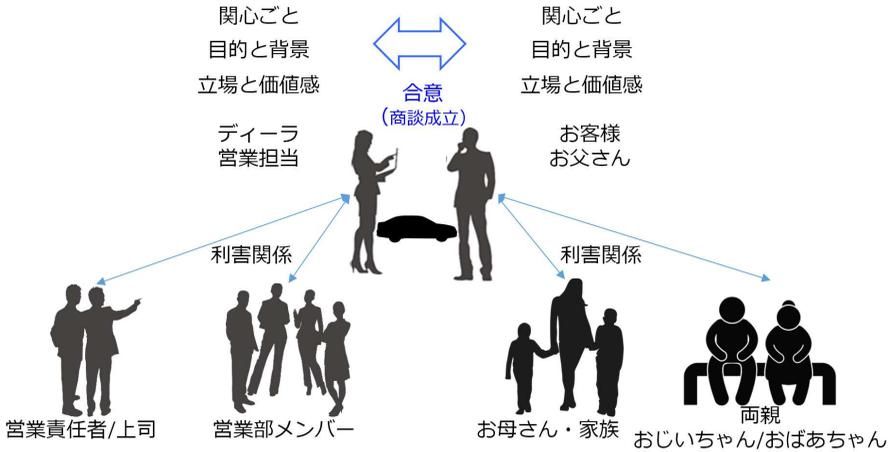


図 4-3 ディーラでの商談(合意)におけるステークホルダ

表 4-2 ディーラでの商談におけるステークホルダの立場と関心ごと

ステークホルダの立場	関心ごと
お客様/お父さん	高い新車を買いたいが、お母さんの理解がないと買えない
お母さん/子供	両親や子供が安心して乗れる車なら良いかも、でも資金が心配
おじいちゃん/おばあちゃん	乗降りが楽な車でないとイヤだ、資金の補助もできるが
ディーラ/営業担当	あと一台新車を売って今月の販売目標を達成したい
営業責任者/上司	ディーラの販売実績を更に上げるため値引きはOK
営業部メンバー	担当者の販売成績を上げて欲しい、でも・・・

なおこの例では、説明する側と説明を受ける側の間で、D-Case そのものを使い商談を進めることは現実的ではないため、D-Case で考えた内容を踏まえながら、説明資料や商談材料を使い商談を進めていくことになります。

4.2 D-Case の記述

ステークホルダを明確化した場合、D-Case の記述ステップは、従来提案されてきた D-Case の記述ステップに加えて、ステークホルダの観点を加えた記述ステップになります。

1. 参加者の興味関心からトップゴール、前提情報を設定する。
2. 参加者の興味関心から戦略を設定し、サブゴールに分割する。
3. それぞれの証拠を最終ゴールに設定する。

2. は必要に応じて繰り返します。後述しますが、あまり D-Case の木構造が深くなると、理解しづらい D-Case になるので、なるべく繰り返し回数は少なくなるようにします。

普通の文章と同じように、記述する間、あるいは記述がひとまず終わったら、その内容をいいか悪いか評価する必要があります。D-Case などのモデルを評価するには、明確な基準が必要です。D-Case の評価基準として ISO/IEC 25000 SQuaRE などのソフトウェア品質特性などを用いることも考えられます。D-Case 手法では、これまでの経験から、合意形成を行うためには以下の表 4-3 の評価基準を導入します。

表 4-3 D-Case の評価基準

評価基準	内容
前提の妥当性	説明者、判断者が共有すべき前提が過不足なく、適切な場所に配置されているか
論証の妥当性	論証の展開、証拠が論理的に問題なく、かつ判断者が判断できる内容になっているか
規模の妥当性	説明される側が数分規模で理解出来る規模になっているか

この基準に従った D-Case の評価例を示します。

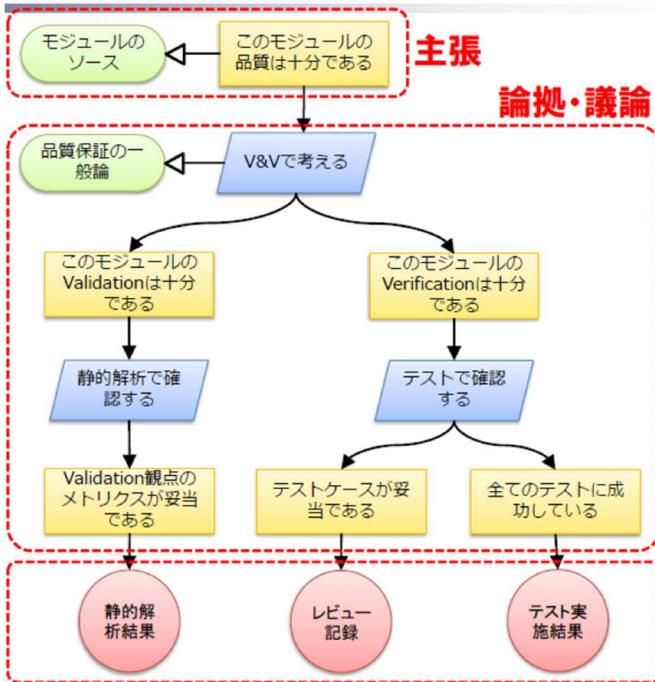


図 4-4 モジュールテストに関する D-Case の例

例えばシステムのモジュールテストに関して図 4-4 のような D-Case を記述したとします。評価基準に従って評価してみましょう。

- 前提の妥当性。トップゴールの前提ノードが「モジュールのソース」だけしかありません。トップゴールノードが「品質が十分である」であるので、どの程度の品質であれば十分であるといえるのか、明確ではありません。また、品質を高めることは、時間があればいくらでもできるので、開発期間が明示されていないとどこまで品質管理に時間をかければよいのかわかりません。したがって、前提の妥当性は低いといえます。

この D-Case を評価してみます。

- 前提の妥当性。トップゴールノードの前提ノードとして「プロジェクトのスケジュール体制」と「A 社 SW 品質基準」が新たに加わり、決められた期限内に、A 社 SW 品質基準を満たすことゴールノードであることがわかります。よって前提は妥当であるといえます。
- 論証の妥当性。「A 社 SW 品質基準」の内容がわかるようになっており、そのなかで推奨されている技法「メトリクスによる判定」、「テストケースの妥当性、テストの網羅性」による論証を展開しています。この改訂されている D-Case でも、手段による戦略ノードが用いられているのはマイナスで、ゴールを達成するための手段（「メトリクスによる判定」を採用）は前提ノードに記述すべきですが、改定前の D-Case より論証の妥当性は上がっています。
- 規模の妥当性。改定前の D-Case よりも前提ノードが増え、サブゴールノード、証拠ノードが増えています。スライド1枚程度に収まっているので、規模は妥当であるといえます。ただしこれ以上複雑になると、妥当性は低下します。D-Case の詳細化と理解のしやすさはトレードオフの関係にあるので、説明される側が数分規模で理解出来る規模、例えばスライド1枚程度という目安をもって D-Case を書きます。

4.3 合意形成の実施

合意形成の手順として、ステークホルダ全員が D-Case を描き合意形成を図る場合と、ステークホルダの一部が D-Case を用意し、合意形成を図る場合が考えられます。

ステークホルダ全員が合意形成を行う場合、プロジェクトで D-Case を見ながら、議論し、評価し、必要ならば改訂をしながら合意形成を行います。ステークホルダの人数はこれまでの経験から、最大でも5名程度にしたほうがよいです。

ステークホルダの一部が D-Case を用意する場合、D-Case と同等の情報量を持つ、絵や文章を用意して合意形成を行う方がよく、インフォグラフィックなどの応用が考えられます。

図 4-6 は Facebook で、一般市民が放射線測定について2週間程度議論した内容を、ま
ず D-Case でまとめて、次にインフォグラフィックを用いて参加者に提示した例です。

例としている D-Case は「天気による影響を気をつける」というトップゴール(より適切なゴ
ールとしての表現は「天気による影響を受けても適切に放射線を測定できる」などですが、
一般の方にわかりやすい表現にしています)を、天気に関連する要素の影響(雨、雪、落
雷、宇宙線、風)ごとに分けて議論しています。このような D-Case をいくつか提示したとこ
ろ、参加者が D-Case に馴染みがないこともあり、あまり参加者の議論は活性化しませんでした。
そこでインフォグラフィックを用いて、同じ内容を、よりわかりやすく図示しました。上か
ら2番目の「天候に気をつけよう」が、「天気による影響を気をつける」という D-Case に相当
します。このインフォグラフィックにより、議論は再び活性化しました。このように、前提とゴール
、戦略、証拠の構造があれば、D-Case の表記に拘る必要はありません。



図 4-6 放射線測定に関する Facebook の議論の D-Case、
インフォグラフィックによる合意形成の例

4.4 D-Case ステップの例

D-Case ステップ1: ステークホルダの分析

D-Case で説明することで「最終的に合意してもらいたいこと(=トップゴール)」を明確にします。トップゴール(「ゴールノード」)は、説明する側、される側にとって何等かの共通する関心、関係性があることが前提になります。同時に、それらの内容について、直接的及び間接的に、関心や利害関係を持つ人達(ステークホルダ)について確認します。

事例では「自動運転は便利だ」といったことが説明する側、される側にとっての共通の関心事であり、最終的な目的になっています。また、それらを説明する上で、自動運転のユーザーが主なステークホルダであることを確認します。



図 4-7 「D-Case ステップ1」

D-Case ステップ2: D-Case の記述

D-Case の記述ステップに従って D-Case を作成していきます。D-Case の各ノードに用いられる単語や表現は、説明される側の知見においても容易に理解されるものであることが必要です。

また、説明における「前提」については、より上流層において、「前提ノード」を用いて、明確にしておくことで、それ以降の説明や、全体の構成、規模において、発散されることなく進めることが可能となります。

事例では、対象とするユーザの範囲を「ファミリーユーザ」として、上流ノードにて限定的にすることにより、以降の「ユーザにとってのメリット」を考える際の的を絞りやすくなっています。

次に、ユーザ(ここでは「乗る人」)にとっての「メリット」を、「運転者」と「同乗者」に分割した上でサブゴールとして設定しています。ユーザの「メリット」については、ここでは、このように 2 つに分けて考えることが、効率的かつ効果的であり、また、上位のゴールとの間における説明においても合理的であると考えられたこととなります。

次に事例では、この 2 つに分けられた「ユーザに対するメリット」について、それぞれ 3 つずつ挙げています。(なぜ、これら 3 つに選定されたかは、説明(前提)が必要かもしれませんが、ここでは、説明される側にとっても、妥当とみなされる見込みや根拠があるものと仮定します。)

最も下位(末端)には、各サブゴールの達成を示すために「証拠ノード」が用いられます。それぞれに用いられる証拠の素材や要素については、それぞれの「(サブ)ゴールノード」達成に対して、妥当性を持ったものである必要があります。

事例では、「静粛性」や「会話のし易さ」といったサブゴールの達成を下支えするための「証拠ノード」として、「TVCM」や「カタログ」といった素材が用意され、それぞれのユーザにとって納得できる妥当性を持った判断材料になると考えられています。

このように、意識されたステークホルダを考慮した上での、各ノードに個々に記述される用語そのものの妥当性に加え、ゴールとその下に位置するサブゴール、サブゴール同志、及び「証拠ノード」との組み合わせにおいて、説明される側にとっても合理的、かつ適切な構成(及び構成全体の大きさ)を以て作成されていることが求められます。

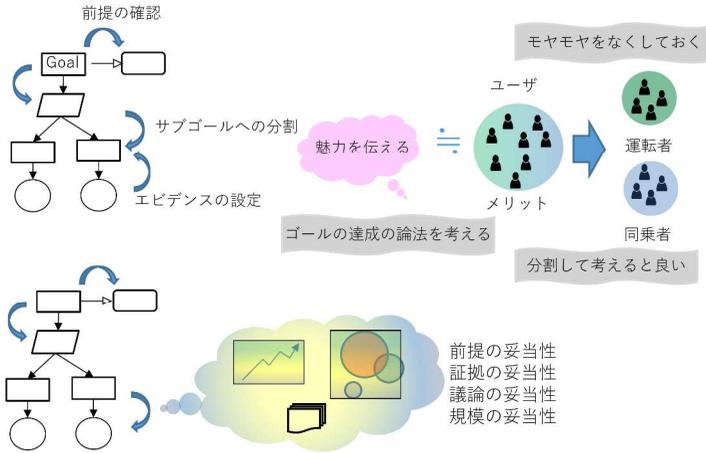


図 4-8 「D-Case ステップ2」

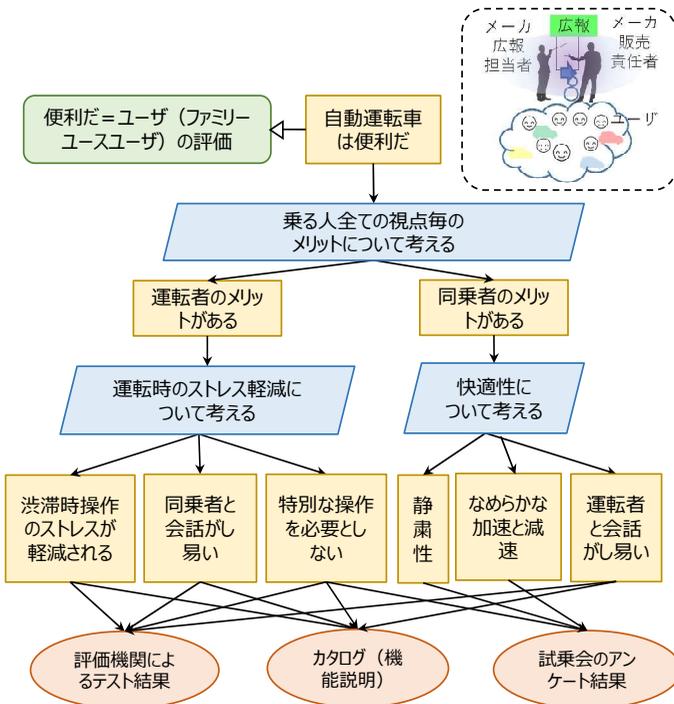


図 4-9 「D-Case ステップ2」における D-Case 記述

D-Case ステップ3: 合意形成の実施

合意形成は、提案側とそれを聞き入れる側によって成立します。それは、1対1であったり、1対複数、又は複数対複数であったりしますが、たいいていの場合、双方はそれぞれの側における目的や利害を共有している代表の立場として登場します。事例では、「自動運転の利便性」をメーカーの広報担当の代表といった提案側から立場として説明がなされ、それを聞き入れる側としてそれら提案の妥当性を「営業側」として判断する役割を担う代表者として登場する事例になっています。

作成された D-Case 上において、下方末端の「証拠ノード」により下支えをされた「サブゴール」の達成と、それらの組み合わせによる、より上位に位置する「(サブ)ゴール」が達成されるものとしての合意形成が行われます。

事例では「自動運転車は楽しいことを伝える」といった最上位目標に対し、まずは末端として「TV CM、その他広告」、「カタログ」といった「証拠ノード」に下支えされた各サブゴール(=各ユーザメリット)がそれぞれが達成されるものとして説明がされ合意形成がなされます。(ここでは、それらの達成は「運転者」と「同乗者」のそれぞれの視点におけるメリットを満たすには十分であるものと仮定します。)さらには「運転者」と「同乗者」の組み合わせの構成により、トップゴールが達成されるといった合理性故にトップゴールの達成がなされるものとして説明がなされ、最終的な目標(トップゴール)としての「自動運転車は便利だ」についての合意形成がなされます。

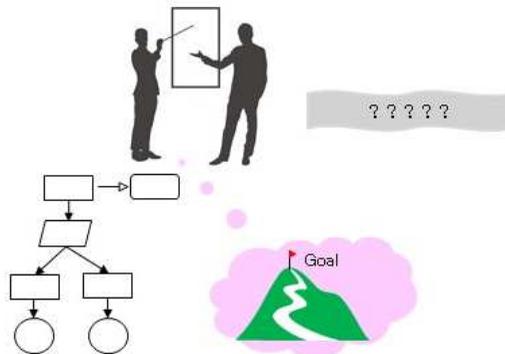


図 4-10 「D-Case ステップ3」

5 ステップ実施に向けたヒント

5.1 前提ノードの重要性

D-Case により目的へ向う主張を行い論証する上で、前提ノードは論証する前提や背景を示すためのノードです。これがあることにより論証する対象や範囲、前提条件や制約などを示し明確にすることができます。適切に前提ノードを記述することによって、論証が発散してしまうことや、噛み合わないという事態を回避することができるため、前提ノードの設定の良し悪しが、D-Case の有効性を大きく左右するともいえます。

前提ノードで使用する用語や文書はステークホルダの間で共通に理解できるように、適切な選択をする必要があります。用語や文書の理解や解釈が異なっていると、論証が空疎しやすくなり、戦略ノードの妥当性や証拠ノードの適切性について合意を取りにくくなります。

5.2 前提ノードの設定上の注意

前提ノードはゴールノード、戦略ノードに対して補完的に用いることができます。それらの表現における用語や語句について、説明や概念、および参照先とするべき情報源や実体の指定、その他補足的説明を記述することができます。

例えば、ゴールノードや戦略ノードに対して補完させることで、下方に続くサブゴールノードの説明範囲を明確、かつ発散しないようにすることが可能となります。

同時に、補完的な説明が、前提ノードに分離されることで、説明の流れにそった説明がより簡潔に表現できるようにもなります。

一方で、前提ノードには、主張や戦略展開に関係する規格や規制、標準などを含める際には、主張の合意にとって必要な範囲だけが選択又は指定されるようにします。広く一般的な規格などを含めてしまうと、議論が不必要に続いてしまうことや、戦略がより複雑になってしまう傾向があるので注意が必要です。

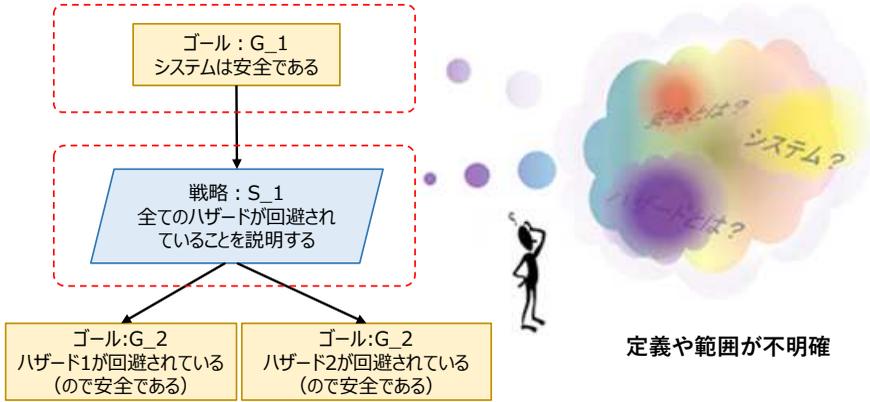


図 5-1 定義や範囲が不明確な例

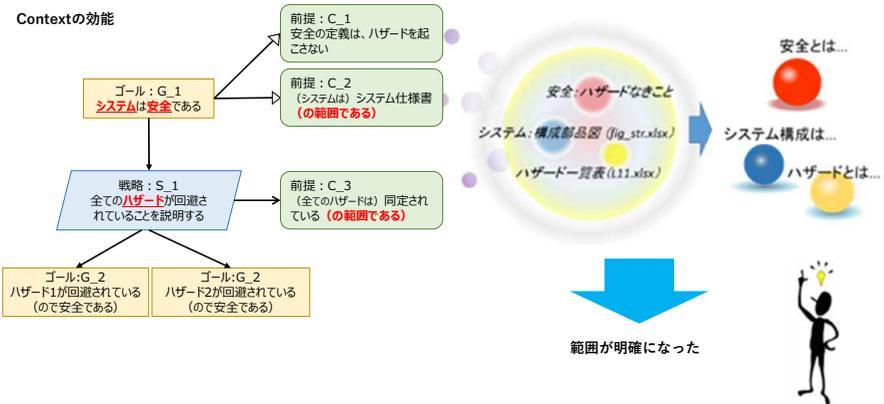


図 5-2 範囲が明確になった例

例) 以下のように、前提ノードにおける表現や定義が明確化される。

- 「ゴール: 全てのハザードについて考える」 ⇔ 「前提: ハザードリスト(HZ_list.xlsx)」
- 「ゴール: ソフトウェアにフォールトがない」 ⇔ 「前提: フォールトは仕様で規定された操作に基づき導出される」

5.3 ゴール分割の例

4章で示した D-Case ステップについて、ここでは D-Case ステップ 2 で実施するゴール分割の方法として、リスク分析の結果をベースにした一例を示します。

D-Case ステップに沿って D-Case を作成していく際、大まかな論証構造を決め、戦略ノードとサブゴールノードを記述してトップゴールノードを分割していきます。しかし、どのような観点でトップゴールを分割していくかは、主張したい内容の特性によって、いくつかのパターンが考えられます。リスク分析をベースに D-Case を記述する場合、リスク分析によって得られた結果を用いて、そのリスクに対する対策がなされていることを示すことで、トップゴールとなる主張が成立することを説明します。

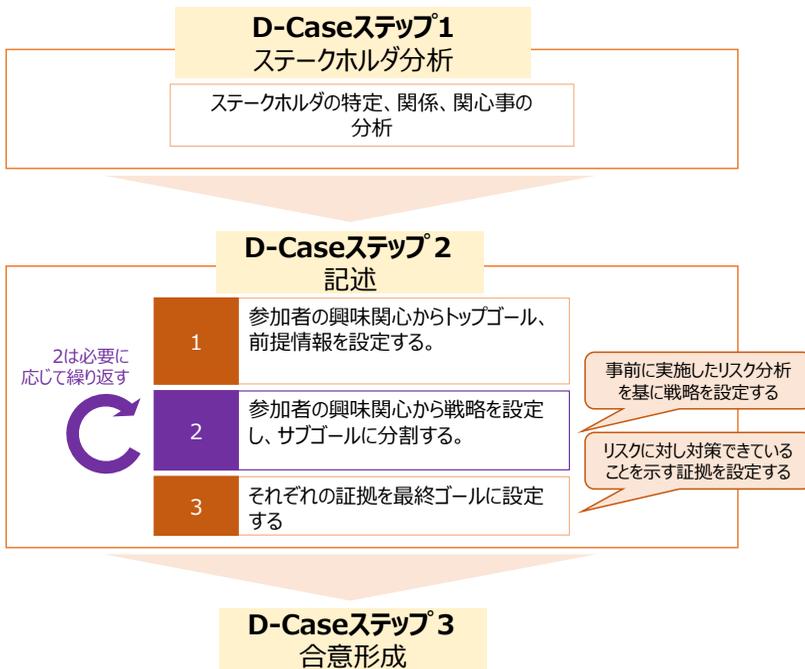


図 5-3 リスク分析をベースとした議論の分解

例として、「システムはディペンダブルである」というトップゴールに対して、ゴール分割した D-Case を図 5-4 に示します。本例におけるリスク分析結果のように、何らかの分析や検討の結果を基に D-Case を作成する場合、前提ノードを活用して、D-Case とそれらの結果とのトレーサビリティを確保することが重要です。ここでは前提ノードにリスクを列挙していますが、実際にはリスク分析した結果を示す資料が別途存在し、前提ノードにその資料の所在等を記載するケースが多いでしょう。これら関連資料や情報源を相互に確認できる状態にしておくことで、議論の発散を防ぎ、各ノードや論理構造の妥当性を評価しやすくなります。

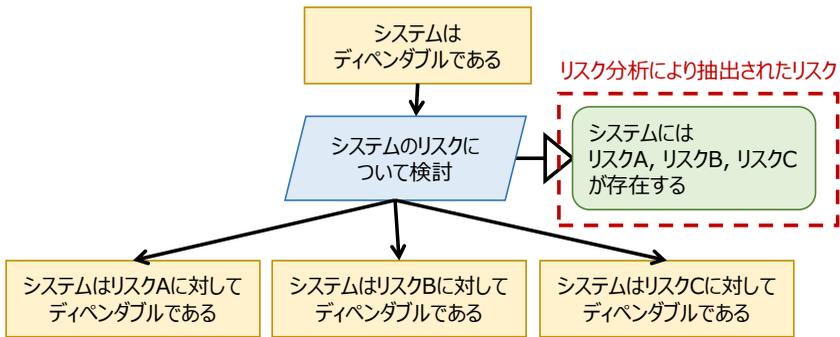


図 5-4 リスク分析をベースとしたトップゴールの分割例

議論を分解する方法としては、ゴールノードをシステム構成に従って分解したり、機能構成に従って分解したりするなど、他にも様々なパターンが考えられます。論証の対象によって、違和感のない分解パターンを検討し、議論を繰り返しながら論証構造をブラッシュアップしていくことが重要です。

6.2 章の D-Case 記述の一部では、本章で紹介したリスク分析に基づいた議論の分解を行っていますので、参考にしてください。

6 D-Case 記述の実例

6.1 テスト戦略の合意

ソフトウェアテストを実施後に、「本当にこれで十分なテストと言えるのか」、あるいは、「こういうテストを追加しなくても良いのか」と、もめることがあります。しかし、テストは最終工程ですのでリリースまでにできることは限られています。そのため、テスト実施後に出た意見については十分に議論することや、議論したとしてもその結果を反映することが困難です。

そこで、『テストすべきこと』に対して、テスト実施後に議論するのではなく、事前にテストに対する合意をステークホルダで取っておくことが大切です。本項ではテスト合意を取る手段として D-Case をテスト戦略へ適用した事例について説明します。

6.1.1 テスト戦略とは

ソフトウェアテスト戦略は、JSTQB 用語集 Version 2.3.J02 において、

組織や(一つ若しくは複数プロジェクトの)プログラムで実施するテストレベルと各テストレベルでのテスト内容を高位レベルで説明したもの。

と定義されています。ここで、テストレベルとは、コンポーネントテスト(ユニットテストとも呼ぶ)、統合テスト、システムテスト、受け入れテストなど、『段階的に実施するテストの区切り』のことです。(なお、厳密には違う概念ですが、テストレベルのことをテストフェーズと呼ぶ組織もあります。)

また、テスト内容とは、機能テストや性能テストなどのテストタイプすなわちテストの種類を指します。つまり、テスト戦略はテスト全体を時間軸(段階)や内容(種類)でどのように分割するかをざっくりと決めることです。

テスト対象のソフトウェアが非常に小さいもの(数時間でプログラミングが完了するようなソフトウェア)でしたらテストも数時間で終わる小規模なものになります。その場合には、テストを分割する意味はあまりありません。ところが、複数人のプログラマが数ヶ月もかけて開発するようなソフトウェアの場合には、テストも複数人で数週間は必要となります。そのような大規模のソフトウェアテストを実施するときにはテスト戦略を立ててテストを適切に分割するとともに、テスト全体の構造を考える必要があります。

ところが、上述のテスト戦略の定義に書かれたテストレベルや各テストレベルでのテスト内容の構造の作り方についての標準はありません。組織やソフトウェアごとに最適なテスト戦略は異なるからです。テスト戦略の具体的な内容やテストの全体構造は組織やプログラムのそれぞれで決める必要があります。

これまで、ほとんどの企業において、テスト戦略はテストを実施する組織あるいは品質保証部門が決定してきました。しかし、決定するといっても、テスト戦略のほとんどは、これまで実施してきたテストレベルやテスト内容の全体構造を踏襲するものでした。

このように戦略をプロジェクトごとに立てないやり方でもテスト対象が同じカテゴリのもの(カテゴリとは、例えば勘定系ソフトウェアや人事系ソフトウェアなど)であれば、ソフトウェアの性質が同じなので問題ありませんでした。

ところが昨今のプロジェクトでは、ビッグデータや IoT への対応など、これまでと全く異なる性質のソフトウェアをテストする必要に迫られています。そのようなときに、これまでと同じ構造のテストをしていると大きなテスト漏れが発生したり、テストの効率が非常に悪くなったりします。そこで、今日は、テスト設計を行うことの重要性に注目が集まっています。

6.1.2 テスト戦略の立て方と D-Case

テスト戦略の案を作るのはテストを実施する組織あるいは品質保証部門ですが、テスト戦略(案)は、関係部署で合意を取る必要があります。そこで、合意形成を目的として D-Case を活用してテスト戦略を作ることが大変有効です。以下にテスト戦略に D-Case を使用する主なメリットを列挙します。

- テストに対する合意形成レベルが向上する
 - 前提条件に以下のものを含め、妥当性の論証が可能(従来は明示されない場合がある)
 - ◇ 根拠は無いが前提としておいたもの(アサンプション)
 - ◇ 根拠のある前提条件(ジャスティフィケーション)
 - 論証のポイント(論拠)が明確で合意形成しやすい
 - 何を行いどのようなエビデンスを残せばよいかが明確になる
 - その場でステークホルダと一緒に作成して、合意を取ることができる

- テストに対する説明責任レベルが向上する
 - 戦略時に作った D-Case の証拠ノードをもとに説明
 - 条件や仕様が変わった場合、影響範囲がすぐに分かる
 - 運用中(リリース後)に証拠ノードに相当するものをモニタリングすることで、ゴールの合意レベルが保たれていることを確認できる

上記のメリットがあるため、D-Case を用いてテスト戦略を作成することは大変有効です。ところが実際にテスト戦略を立てようとするとうゴールノードの分割方法に時間がかかります。そこでテスト戦略を容易に作成できる『5 つのソフトウェアテスト戦略パターンテンプレート』(表 6-1)を作りました。このテンプレートは数十社以上で実際に行われているテスト構造を分析して作成し、すでに十数社へ適用した実績のあるものです。

表 6-1 ソフトウェアテスト戦略パターンテンプレート

戦略パターン名	サブゴールノードの分割方法の例	採用の目安
品質特性戦略 (ISO25010)	例) JSTQB テストレベル コンポーネントテスト、統合テスト、システム テスト、受け入れテスト	開発プロセスとして、V 字モデルを使用している
レベルテスト戦略 (開発中間成果物依存)	例) ISO25010 の品質特性 機能適合性、性能効率性、互換性、使用 性、信頼性、セキュリティ、保守性、移植性	新商品開発時に品質特性のトレードオフが必要な場合
W モデル戦略 (レビューを踏まえたテスト)	例) W モデル 要求レビュー、仕様レビュー、設計レビュー、コードレビュー、テスト	上流工程の改善を行いたいとき
構成要素戦略 (テストアイテムの構造ベース)	例) 複合機 IIT、IOT、UI、ネット、認証、Scan、FAX、コピー	開発拠点が(多拠点に)分割しているとき
派生開発戦略 (派生・共通要素)	例) XDDP, SPL 母体(既存)、追加、母体と追加の組合せ	派生開発や SPL のとき

※この5つがテスト戦略の分割方法の全てではないことに注意してください。

上記のテンプレートを使用して、テスト戦略の D-Case を作成します。戦略パターン名が D-Case の戦略ノードとなります。サブゴールノードの分割は 2 段以下にすることを推奨します。1 段目の戦略と 2 段目の戦略は別のものを選んで構いません。次ページに『派生開発戦略パターン』のサンプルを示します。

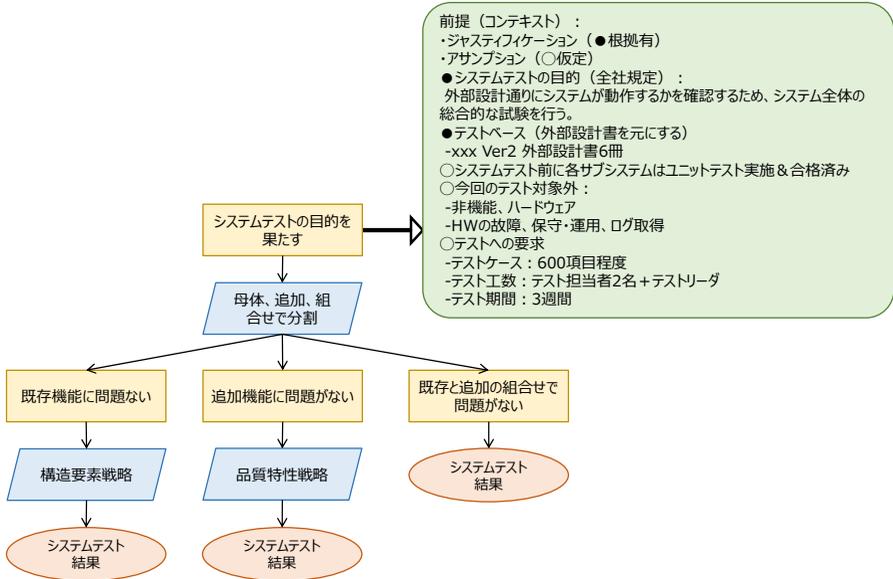


図 6-1 リスク分析をベースとしたトップゴールの分割例

6.2 ET ロボコンの実例

6.2.1 ET ロボコンの概要

ET ロボコンとは、一般社団法人組込みシステム技術協会が主催する、技術教育の場を提供することを目的としたソフトウェアコンテストです(*6-1)。LEGO® MINDSTORMS® を使った、共通のパーツ、構成からなるロボット(ハードウェア)に搭載するソフトウェアを対象とした競技です。参加チームは、指定されたコースを自律走行し、与えられたゲーム課題をクリアするシステムを開発します。開発にあたっては、分析・設計モデルを作成し、その内容を記述したモデルシート(A3 サイズ 5 枚以内)を提出します。そして、審査員によるモデルの審査結果と、走行競技の結果に基づいた総合評価によって順位が決定されます。

(*6-1) ET ロボコン公式サイト <http://www.etrobo.jp/>

6.2.2 D-Case の適用

本項では、富士ゼロックス株式会社が、ET ロボコンで適用してきた D-Case の事例を示します。ET ロボコンのコースや課題は開催年によって変更となるため、ここでは 2016 年に作成した D-Case を紹介します。なお、本項で掲載する D-Case は、レビュー前の検討段階のものも含まれます。

また、以後の説明において「ブロック」や「新幹線」といった言葉が出てきますが、これらは競技内のゲーム課題で用いられるものです。ここでは D-Case ステップの大まかな流れを感じ取っていただきたいため、ゲーム課題のルールや、課題をクリアすることで獲得できるポイントの算出方法などの詳細は省略します。

まず、ステークホルダを設定します。ここではステークホルダは開発者と審査員としました。ET ロボコンの場合、ステークホルダは主に競技規約や審査規約の内容から導かれます。4.1 で述べたように、ステークホルダの立場と主な関心ごとを分析すると、表 6-2 のようになります。

表 6-2 ステークホルダの設定と分析

ステークホルダの立場	関心ごと
開発者	新しい技術や手法にチャレンジし、スキルを向上させたい 高い評価を得られるソフトウェアを開発したい
審査員	課題の有効な解き方を示すモデルになっているか 検討された内容がわかりやすく記述されていることを期待する

しかし、D-Case の作成に関与しない審査員を意識して、最初から質の高い D-Case やモデルを作ろうとすることは、初心者にとっては困難です。そのため、まずは開発者間でのコミュニケーションに主眼を置き、D-Case を活用することにしました。

続いて、チーム内で議論してトップゴールノードを決定しました。過去の活動において、モデルシートを作成する工数が不足するという問題が発生していたため、この年のトップゴールノードは、「夏休み前にモデルシート提出可能状態にして総合優勝する」としました(例年、モデルシートの提出は夏休みから 2~3 週間後です)。図 6-2 に、トップゴールノードとその直後の階層のサブゴールノードを示します。このトップゴールノードは、チームメ

ンパー個人としての目標や、チームとしての目標に基づいて、活動全体の目標として設定したものです。そのため、本例のようにプロジェクトマネジメントの視点も含んだ形になることが多いです。設計スキルの向上という観点で、ET ロボコンへの参加を通して試してみたい技術手法や、開発プロセスなどを含めたトップゴールノードが設定されることもあります。

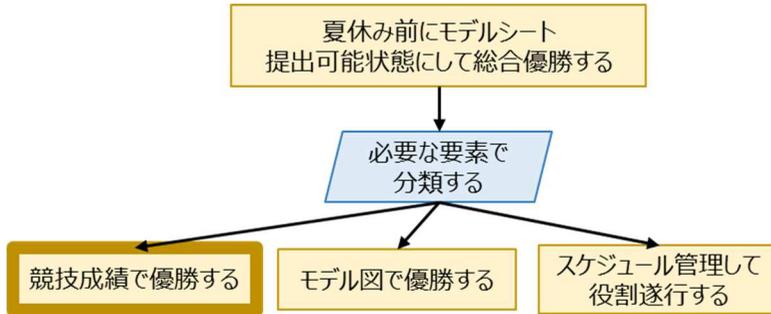


図 6-2 トップゴールノードと直後の階層

設定したトップゴールノードを元に、サブゴールノードへの分割と証拠ノードの抽出を行います。トップゴールノードの分解は、以下の 2 つのアプローチで進めていきました。

- ① トップゴールノードに近い(階層の浅い)サブゴールノードは、競技規約を分析することで分割する
 - ② トップゴールノードから遠い(階層の深い)サブゴールノードは、必要な要素やリスクを洗い出して D-Case としてまとめる
- これら二つの方法について説明します。

まず、①の方法について説明します。トップゴールノードに近いゴールノードの分割は、システムとして達成すべき既知の内容の詳細化である場合が多く、ET ロボコンの場合、競技のルールそのものの詳細化となります。

具体例として、図 6-2 の「競技成績で優勝する」というゴールノードを分解したものを図 6-3 に示します。

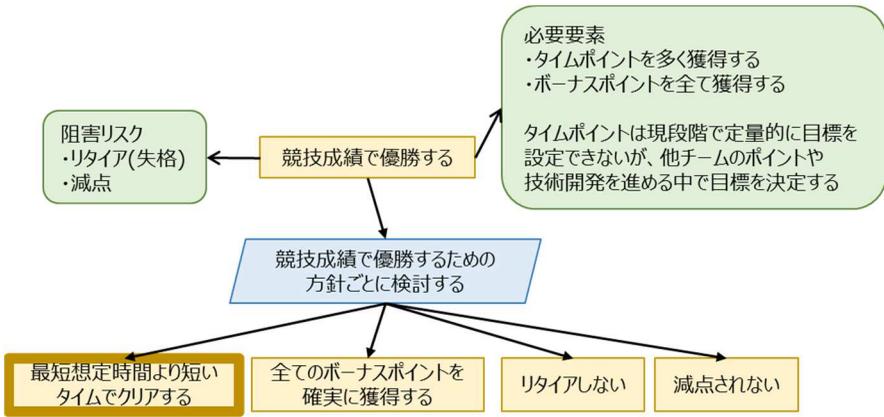


図 6-3 「競技成績で優勝する」の詳細化

競技成績で優勝するためには、短いタイムでクリアすることと、多くのボーナスポイントを獲得することが必須であり、さらにリタイアしないこと、減点されないこと、も求められます。これらは競技規約を理解することで抽出することができ、その内容を前提ノードとして付与しています。そして、これらの要素をサブゴールノードとして分割しました。

次に、②の方法について説明します。

トップゴールノードから遠いゴールノードになってくると、「システムが具体的にどう振る舞うべきか」ということを考える必要があり、上位ゴールノードを分解することが難しくなってきます。

具体例として、図 6-4 の「最短想定時間より短いタイムでクリアする」というサブゴールノードを考えてみます。短いタイムでクリアするためには、単純に考えるとモーターの回転速度を速くするといったことが思いつきますが、それに伴ってロボットが転倒したり、コースアウトしたりするリスクも発生します。このような要素やリスクの抽出は、抜け漏れが発生する可能性があり、参加メンバ全員が ET ロボコン初参加であったため、経験やノウハウもない状態でした。そのため、階層の深いゴールノードに対しては、上位ゴールノードを単純に詳細

化させるのではなく、対象となるゴールノードに対し必要な要素やリスクを洗い出してから、D-Case を構築するというアプローチを取りました。

今回のサブゴールノードの例では、走行コースを印刷したものにメンバで付箋を貼り付けていき、必要な要素やリスクなどを全て洗い出しました。この時点では、D-Case を書くということにとらわれず、なるべく多くの要素やリスクを抽出することを意識しました。

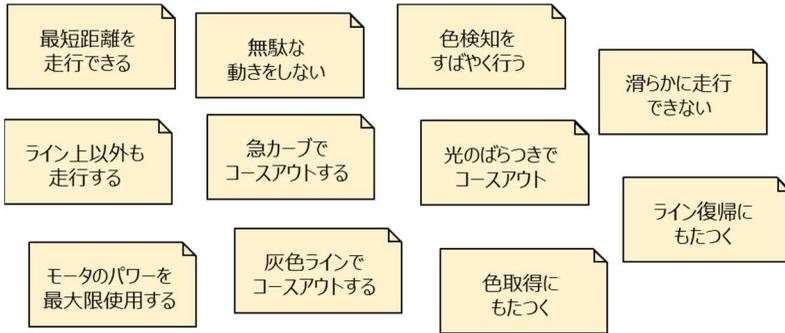


図 6-4 抽出した要素やリスク(一部)

次に、洗い出した要素のグルーピングを行い、D-Case としてまとめたものが、図 6-5 です。

抽出された要素は抽象度が揃っていないものも多いため、この段階で、論証の階層関係を意識した D-Case を作成します。付箋の内容は、D-Case ではサブゴールノードとして表現されています。

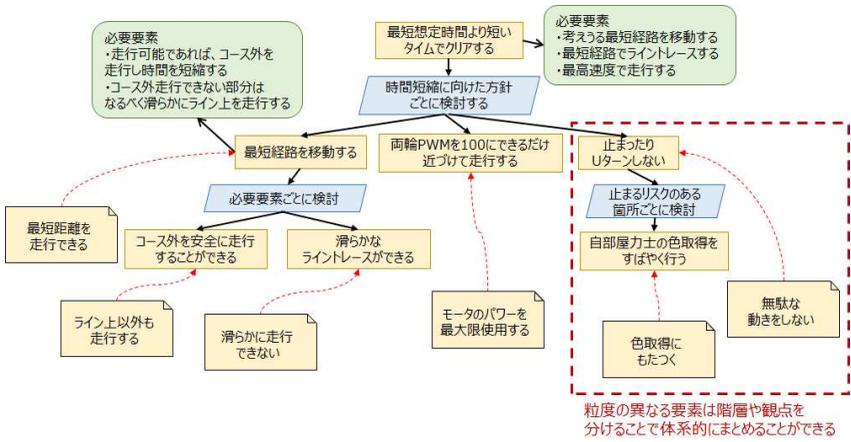


図 6-5 洗い出した要素からの D-Case の構築

そして、作成した D-Case に対してレビューを行い、必要に応じて要素を追加します。ここでは、「止まるリスクのある場所ごとに検討」という戦略ノードに対し、レビューの結果、「新幹線検知時に無駄な待ち時間を作らない」という新しい要素が追加されました。

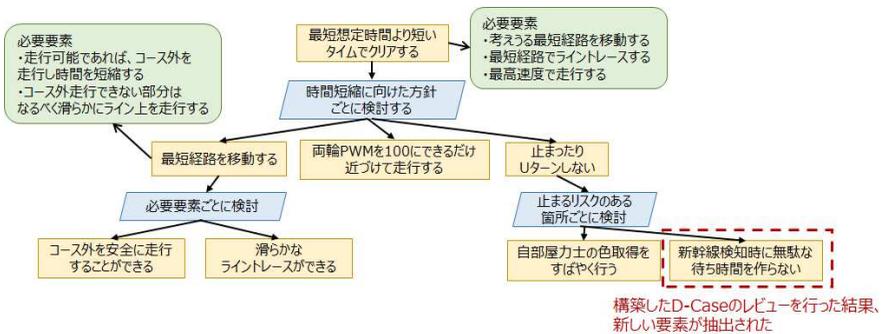


図 6-6 D-Case の評価による改訂

このように、抽出した要素を一旦 D-Case として体系立てた形でまとめることで、新たな要素を発見するきっかけを生むことができます。

サブゴールノードを分割したら、証拠ノードを抽出していきます。この時点では、必ずしも達成できる証拠ノードとは限らないため、仮の証拠ノードとしておきます。

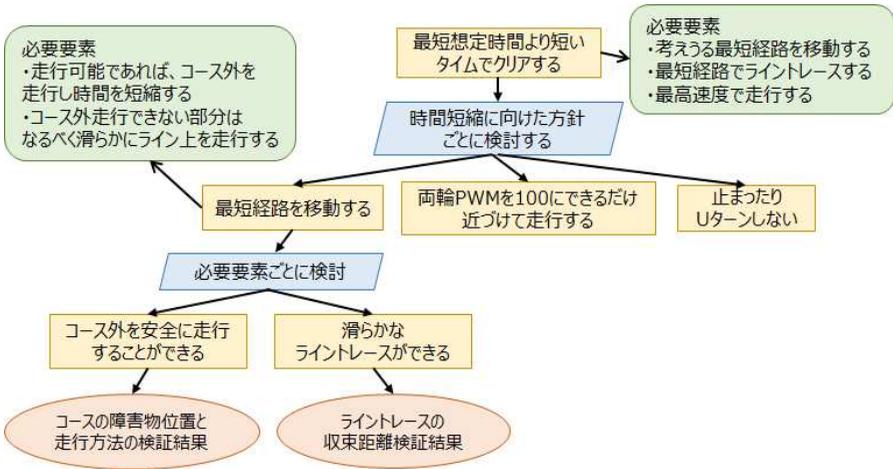


図 6-7 証拠ノードの設定

設定した仮の証拠ノードは、確定した証拠ノードになるよう、ノードごとに担当者をアサインし、実証データを取得していきました。図 6-8 に「ライントレースの収束距離検証結果」という証拠ノード対して検証を行った例を示します。

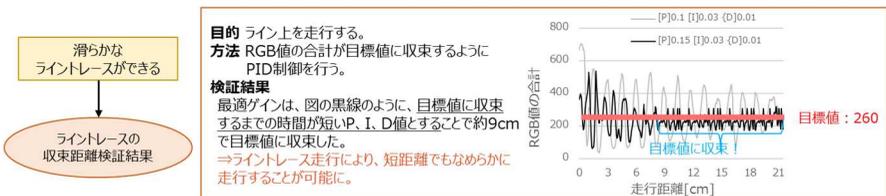


図 6-8 「ライントレースの収束距離検証結果」の証拠ノード記述

証拠ノードごとに担当者がアサインされることで、メンバのやるべきことが明確になり、証拠ノードの獲得状況を進捗管理に活用することもできます。また、検証の過程で必要に応じて D-Case を参照することで、その証拠ノードがなぜ必要かがすぐわかり、作業の目的や背景が共有しやすい、といったメリットもあります。

一方、証拠ノード獲得の中で、技術的課題や開発期間の制約などの要因で、実現が困難なケースもあります。その場合には、その証拠ノードが獲得できなかった場合に、D-Case のどこに影響があるかを確認し、別の方法でトップゴールノードを満たせないかを検討しました。このように、D-Case があることで、影響範囲の特定と代替案の検討が進めやすくなるという効果もあります。証拠ノードの検証を始める前に既に複数の方針が考えられる場合は、すぐに一つの方針に確定させることはせずに、証拠ノードの獲得を進めながら、最終的な方針を決定していく方法でも良いでしょう。

さらに、活動の途中で得た知見などは随時追記し、ノウハウを共有することも重要です。ここでは、証拠ノードを獲得する段階で獲得した知見を、新しくノードとして追加した例を図 6-9 に示します。

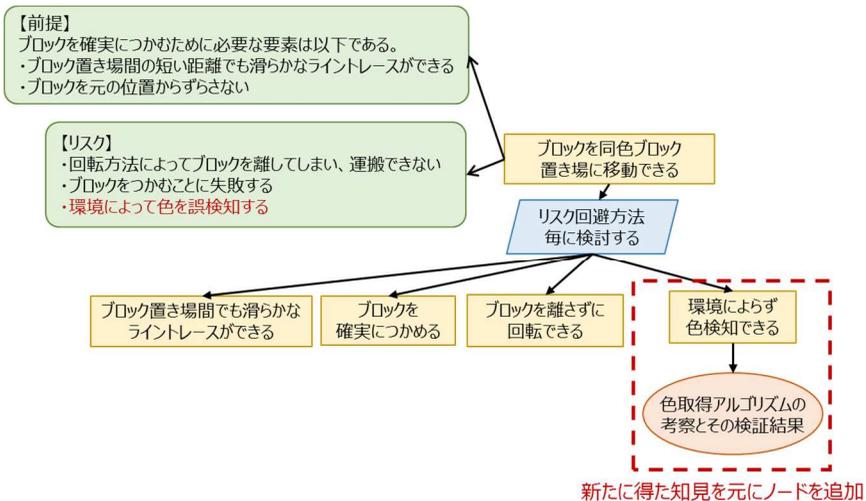


図 6-9 ノードの追加

図 6-9 では、ブロック並べの検証中に、色検知の結果が安定しないということが判明したため、新しくコンテキストにその情報を追記し、「環境によらず色検知できる」というゴールノードを追加しています。

このように D-Case の作成とレビューを繰り返していくと、D-Case 全体が徐々に大規模になっていき、開発者全員が常に D-Case 全体を把握することは難しくなります。そのような場合は、関係者ごとに注目する部分にフォーカスして D-Case の作成やレビューを進めていき、必要に応じて D-Case 全体を参照して、一貫性が保たれているかを確認すると良いでしょう。

最後に、審査員に提出したモデルシートに掲載した D-Case を、図 6-10 に示します。

本項の最初に述べたように、審査員は D-Case の作成には関与せず、提出されたモデルシートの内容のみで審査を行います。そのため、開発者が D-Case の内容を説明しながらモデルの良さをアピールするということではできませんが、D-Case による論証構造は第三者にとってもわかりやすいものであると考え、D-Case そのものも、審査に対するアピールポイントの一つとしてモデルシートに掲載しています。

この D-Case は、これまで開発者間で作成してきた D-Case をベースとして、表 6-2 に示した読み手である審査員が期待することを踏まえて作成したものになっています。また、前提ノードや証拠ノードに、関連する制御モデルや設計モデルの該当箇所を文章やアイコンで示すことで、各モデル間におけるトレーサビリティの向上を図っています。

7 まとめ

本冊子では、合意形成のための手法である D-Case を、初めての方のために解説しました。D-Case はこれまで企業、大学の方との議論を通して、手法として整理してきました。D-Case の特徴である、前提とゴールを共有し、適切な論理展開を戦略ノードにより明示し、最後に論証を支える証拠ノードを置く構造は、論証として非常に基本に忠実で当たり前のものです。しかしシステムが複雑化、ネットワーク化するにつれ、この当たり前の構造でシステムの安全性やセキュリティ情報の共有し、合意していくことが難しくなっています。D-Case は、この課題に対してステークホルダに着目し、ステークホルダが理解できる範囲で合意形成を行うことを手法化しました。本冊子をご覧になって、例にあるような小さな D-Case では複雑・ネットワーク化、さらにはオープン化したシステムのディペンダビリティを保証することはできないのではないかと疑問に思われる方もいるかもしれません。この疑問はもつともです。では、オープンなシステムのディペンダビリティをできるだけ詳細、網羅的な D-Case で書けばよいのでしょうか。その答えは、我々の経験では残念ながらいいえです。どれだけ詳細、網羅的な D-Case を書いても、境界がないというオープンシステムの定義から、完全な D-Case を書くことはできません。この本質的な課題に対して、我々は、ステークホルダのネットワークを考え、個々のステークホルダが、D-Case を書くステップを提案しました。詳細であること、網羅的であることは、もちろん重要ですが、D-Case では「できる範囲」を常に意識します。

本書を読まれて、興味を持たれたら、まず、身近にある出来事やシステムを題材にして、D-Case を描かかれることをお勧めします。D-Case の活動は <http://www.dcase.jp> でご覧になれます。ワークショップなどの情報もありますので、ぜひ皆さまが D-Case を描いた経験を我々と共有させていただけたら大変幸いです。

8 参考文献

【文献】

1. D-Case 構文定義書
http://deos.or.jp/technology/obj/pdf/dcasesyntax_v1.0.pdf
2. 松野裕、山本修一郎、実践 D-Case デイペンダビリティケースを活用しよう！
3. DEOS 変化しつづけるシステムのためのデイペンダビリティ工学、近代科学社
4. Open Systems Dependability (Second Edition), CRC Press
5. D-Case を用いたゴール共有による開発プロセスの適用
～ET ロボコンでの試行と成果～
<https://sec.ipa.go.jp/seminar/20150717.html>

【論文】

1. Yutaka Matsuno, A Design and Implementation of an Assurance Case Language, In Proc. IEEE DSN2014, pp. 630-641
2. Hajime Fujita, Yutaka Matsuno, Toshihiro Hanawa, Mitsuhsa Sato, Shinpei Kato, and Yutaka Ishikawa. DS-Bench toolset: Tools for dependability benchmarking with simulation and assurance. In Proc. IEEE DSN2012, 8pages.
3. Yutaka Matsuno, Jin Nakazawa, Makoto Takeyama, Midori Sugaya, and Yutaka Ishikawa. Toward a language for communication among stakeholders. In Proc. of the 16th IEEE Pacific Rim International Symposium on Dependable Computing (PRDC'10), pages 93-100, 2010.
4. Yutaka Matsuno and Kenji Taguchi. Parameterised argument structure for GSN patterns. In Proc. IEEE 11th International Conference on Quality Software (QSIC 2011), pages 96-101, 2011.
5. Yutaka Matsuno, Hiroki Takamura, and Yutaka Ishikawa. A dependability case editor with pattern library. In Procs. IEEE 12th International Symposium on High-Assurance Systems Engineering (HASE), pages 170-171, 2010.

6. Yutaka Matsuno and Shuichiro Yamamoto. Consensus building and in-operation assurance for service dependability. In Proc. of CD-ARES, LNCS 7465, pages 639-653. Springer, 2012.
7. Yutaka Matsuno and Shuichiro Yamamoto. Toward dynamic assurance cases. In Proc. JCKBSE 2012, pages 154-160. IOS Press, 2012.
8. Yutaka Matsuno and Shuichiro Yamamoto. A new method for writing assurance cases. International Journal of Secure Software Engineering (IJSSE), Special Issue on Cybersecurity Scientific Validation, January 2013. Accepted for Publication.
9. Kohei Tanaka, Yutaka Matsuno, Yoshihiro Nakabo, Seiko Shirasaka, and Shinichi Nakasuka. Toward strategic development of hodoyoshi microsatellite using assurance cases. In Proc. of International Astronautical Federation (IAC2012), 2012.
10. Shuichiro Yamamoto and Yutaka Matsuno. A review method based on a matrix interpretation of GSN. In Proc. JCKBSE 2012, pages 36-42. IOS Press, 2012.
11. 伊東敦、松野裕. ET ロボコンを対象としたドメインからの D-Case による保証議論の構築. ソフトウェアシンポジウム 2012 予稿集, 2012.
12. 中澤仁、松野裕、徳田英幸. D-Case を用いたユビキタス・センサ・ネットワーク管理ツール. 電子情報通信学会論文誌(和文 B)ユビキタス・センサネットワークを支えるシステム開発 発論文特集, J95-B(11), 11 2012.
13. D-Case を用いたゴール共有による開発プロセスの適用
～ET ロボコンでの試行と成果～
<https://www.ipa.go.jp/sec/reports/20151118.html>

9 用語

【あ行】

- アシユアランスケース(assurance cases)
セーフティケース、ディペンダビリティケース、セキュリティケースなどの主張の正しさをステークホルダに確信させる文書。
(D-Case もアシユアランスケースの 1 種)

【か行】

- 議論
お互いの考えを提示、批評しあうことにより論じ合うこと。(およびその内容)
- ゴール(ゴールノード)
ステークホルダ間で合意したい主張(が記述されたノード)
- GSN (Goal Structuring Notation)
York University の T.Kelly により開発された構造化された議論の技術方法。
GSN Community Standard に詳細な記述方法が示されている。

【さ行】

- 証拠(証拠ノード)
ゴールが達成できていることを示す証拠(テスト結果などの、モノ、ドキュメントなど)(が記述されたノード)
- ステークホルダ(stakeholders)
利害関係者。システムやサービスに対して権利・義務・関心を持つ個人あるいは組織。
- セーフティケース(safety cases)
システムが特定の運用環境で特定のアプリケーションに対して許容可能な安全であることを正当化することを意図した、証拠によって裏付けられた構造化された文書。

- 前提(前提ノード)
議論の前提となる情報、ゴールや戦略が必要となる理由の情報(が記述されたノード)
- 戦略(戦略ノード)
上位のゴールの分解の仕方の説明(が記述されたノード)

【た行】

- ディペンダビリティ
利用者が期待するサービス・機能をシステムが継続的に提供する能力
- ディペンダビリティケース(dependability cases)
ディペンダビリティに関する主張をする文書。アシュアランスケースの 1 種。
- D-Case
合意形成のための記述の方法あるいは記述自体。DEOS 協会にてディペンダビリティケースを D-Case と呼称。
- D-Case ステップ
D-Case を作成し活用するためのステップ。準備、記述、合意の 3 ステップからなる。
- DEOS 協会
独) 科学技術振興機構の戦略的創造研究推進事業 CREST の研究領域として 2006 年に開始された DEOS プロジェクトで研究開発された成果を広く展開し、さらに発展させ、世の中のシステムのディペンダビリティ向上に貢献するために立ち上げられた一般社団法人。

【ま行】

- 未達成(未達成ノード)
まだ具体化できていないゴールや説明であることを示す(ノード)

【ら行】

- 論証

主張する命題が正しいことを証拠や理由を添えて論じること。

編著者（敬称略）

松野 裕	日本大学
高井 利憲	奈良先端科学技術大学院大学
大村 一世	日産自動車株式会社
岡田 学	日産自動車株式会社
越山 勉	日産自動車株式会社
斎藤 功	株式会社 ベリサーブ
秋山 浩一	富士ゼロックス株式会社
能條 英紀	富士ゼロックス株式会社
山浦 一郎	富士ゼロックス株式会社

