一般社団法人 電子情報通信学会
THE INSTITUTE OF ELECTRONICS,
INFORMATION AND COMMUNICATION ENGINEERS

信学技報
IEICE Technical Report
KBSE2013-9 (2013-05)

D-Caseを利用したゴール分析プロセスの提案

宇都宮 浩之[i] 山本 修一郎[ii] 松野 裕[iii] 中澤 輝幸[i] 山本 佳和[i]

i 株式会社デンソークリエイト 〒460-0008 愛知県名古屋市中区栄 3-1-1
ii 名古屋大学情報連携統括本部情報戦略室 〒464-8601 愛知県名古屋市千種区不老町
iii 電気通信大学大学院情報システム学研究科 〒182-8585 東京都調布市調布ヶ丘 1-5-1
E-mail: i {hiroyuki, nakazawa, yama_y}@dcinc.co.jp
ii syamamoto@acm.org
iii matsuno@is.uec.ac.jp

あらまし システムを開発するには達成すべきゴールを明確化，詳細化してシステム要求を定義する必要がある．ゴールをシステム要求に変換するプロセスはゴール分析と呼ばれ，最終ゴール達成のために必要なサブゴールに分解することを指す．ゴール分析では上位ゴールをAND/OR関係で分解していくが，ゴール阻害要因から新たなサブゴールを定義することはない．本論文では上記補強のため，ゴール分析図にD-Caseを組合せたプロセスを提案する．

キーワード D-Case，ゴール分析

A Proposal on goal analysis process using the D-Case

Hiroyuki Utsunomiya[i] Shuichiro Yamamoto[ii] Yutaka Matsuno[iii] Teruyuki Nakazawa[i] and Yoshikazu Yamamoto[i]

i DENSO CREATE INC., 3-1-1 Sakae Naka-ku, Nagoya Aichi 460-0008 Japan
ii Nagoya University, Furo-cho. Chikusa-ku, Nagoya Aichi 464-8601 Japan
iii The University of Electro-Communications, 1-5-1 Chofugaoka, Chofu Tokyo 182-8585 Japan
E-mail: i {hiroyuki, nakazawa, yama_y}@dcinc.co.jp
ii syamamoto@acm.org
iii matsuno@is.uec.ac.jp

Abstract It is necessary to define system requirements by clarifying and refining goals to achieve. Although goal oriented requirements analysis methods can support to decompose goals with sub goals, these methods cannot be used to develop sub goals from factors preventing parent goals. In this paper, a process to combine goal tree with D-Case is proposed to complement the problem.

Keyword D-Case, Goal Analysis

1. はじめに

近年，ソフトウェアシステムは機能の多様化や接続先の増加に伴い複雑化の一途をたどっている．こういった状況の中では，開発段階でこれまで以上の品質保証活動を実施しても，製品出荷後の運用場面に入ってから重大な不具合が発覚するケースが増えている．

原因の多くは，要求分析段階で抽象的な要求を具体的な要求仕様に落とし込めていない，あるいは関連する他システムの挙動が押さえられていないなどが挙げられ，これを解決するために様々なゴール分析手法が開発されている．

本研究では，要求分析手法として一般的なゴール分析図[1]を取り上げ，システムのディペンダビリティを保証する D-Case[2]を組み合わせたゴール分析プロセスについて考察する．

2. D-Caseを利用したゴール分析プロセス

ゴール分析図と D-Case とを組み合わせたゴール分析プロセスとして，ゴール分析図に基づいて D-Case を作成する線形型プロセスと，D-Case によるリスク分析とゴール分析とを交互に進める反復型プロセスの2案を提案する(表 1).

表 1　D-Case を利用したゴール分析プロセス

No.	プロセス	確認契機
1	線形型プロセス	ゴール分析後
2	反復型プロセス	ゴール分解ごと

線型型プロセスではゴール分析図を作成した後に D-Case を作成することにより，必要なゴール分析図の修正点を検出して反映する．これに対して，反復型プロセスではゴール分析図を作成する過程でゴール分解ごとに D-Case を作成して必要な修正点を検出して反映する．

本章では ET ロボコンのゴール分析を事例に各々のプロセスを説明する．

2.1. 線形型プロセス

線形型とはゴール分析図を先に作成し，その後出来上がったゴール分析図のディペンダビリティを D-Case を用いて検証するプロセス型式である．

2.1.1. ゴール分析図の作成

線形型においては，まず通常通り top ゴールを設定してゴール分析図を作成する．

今回は top ゴールに「勝つためにリザルトタイムを小さくする」を設定し，ゴール分析図を作成した(付図 1)．

2.1.2. D-Case によるゴール分析図の検証

作成したゴール分析図について，D-Case で論証する．今回は top ゴールに「ゴール分析図はディペンダブルである」を設定し，top ゴールを保証する 3 つのサブゴールを抽出した(図 1)．

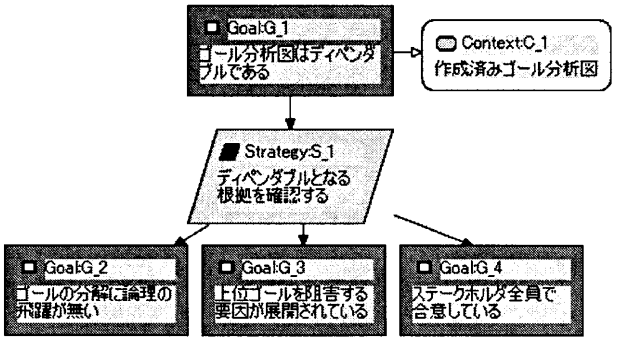


図 1 D-Case による検証(2 段目まで)

「ゴールの分解に論理の飛躍が無い」とは，文字通り上位ゴールと下位ゴールとが整合していることを確認し，サブゴールの設定漏れを検出するためのサブゴールである．ゴール分析図に記載される全ての親子関係にあるゴールに対して検証する．

「上位ゴールを阻害する要因が展開されている」とは，ゴール阻害要因＝リスクを抽出，達成すべきゴールとして設定するためのサブゴールである．ゴール分析図に記載される全てのゴールに対して検証する．

この検証項目は，ゴール分析においては上位ゴールを満たすように分解することが通例であり，リスクが抽出されることは少ないため，これを補うために追加している．

「ステークホルダ全員で合意している」とは，関係者間でシステムが達成すべきゴールを合意できていることを確認するためのものである．今回の実証ではこちらについては割愛する．

2.1.3. D-Case による検証結果の反映

D-Case による検証にて検出された新たなサブゴール，もしくは修正点をゴール分析図に反映し，ゴール分析図全体を再作成する(付図 2)．

今回の D-Case による検証では，以下に示す修正 M1 と追加 A1,A2 を検出した．

M1：変更前
『確実にゴールする
　＝確実にスタートする
　　＋コースを外れず走行する』
M1：変更後
『確実にゴールする
　＝スタート合図で確実にスタートする
　　＋コースを外れず走行する』
A1：変更前
『コースを外れず走行する』
A1：変更後
『コースを外れず走行する』の下位に
『コースから外れても復帰できる』を追加
A2：変更前
『制限時間内になるべく多くの障害物をクリアする』
A2：変更後
『制限時間内になるべく多くの障害物をクリアする』の下位に『障害物のないところは速く走行する』を追加

このように完成したゴール分析図に対して D-Case による検証をすることにより，ゴール分析図作成時には見えなかったリスクや論理飛躍を検出できる．

2.2. 反復型プロセス

反復型とはゴール分析図と D-Case によるリスク分析とを交互に進めるプロセスである．

線形型とは異なり，D-Case を「完成したゴール分析図の検証」ではなく「ゴールを分解する際のリスク分析」に使う．

2.2.1. ゴール分析を開始する

反復型においても，先にゴール分析図から着手する．ただし，top ゴールから 1 段階の分解まで(合計 2 段目まで)で止めておく(図 2)．

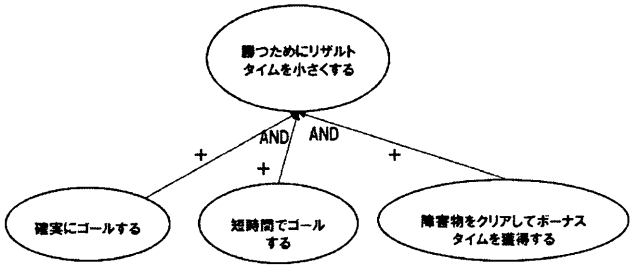


図 2 ゴール分析図(2 段目まで)

2.2.2. D-Case によるリスク分析を実施する

先に作成したゴール分析モデルの top ゴール「勝つためにリザルトタイムを小さくする」を D-Case の top ゴールに置き，ゴールを阻害する要因について論証する(図 3)．

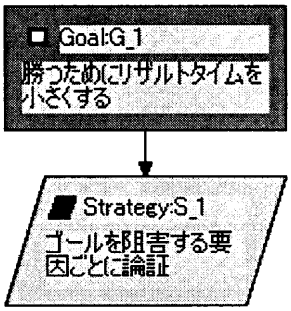


図 3 D-Case によるゴール阻害要因の論証

ここで抽出されたゴール阻害要因＝リスクを，先に作成したゴール分析図にフィードバックする．

2.2.3. ゴール分析と D-Case を反復する

D-Case で抽出したゴール阻害要因をサブゴールに追加したゴール分析図にて，再度ゴール分析を実施する．ただし，ゴール分析図のサブゴール分解は常に 1 段のみとし，抽出された各々のサブゴールを D-Case の top ゴールに設定して再びゴール阻害要因を抽出，ゴール分析図にフィードバックすることを繰り返す．

事例としてゴール分析図に現れたサブゴール「確実にゴールする」について D-Case によるリスク分析を実施した結果を示す(図 4)．

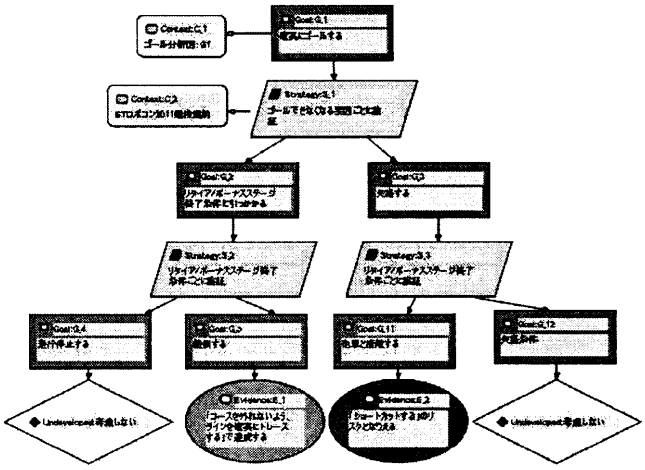


図 4 「確実にゴールする」のリスク分析

図 4 においては，ゴール分析図に現れたサブゴール「ショートカットする」に対するリスクとして『他車と接触する』を検出することができている．

このようにひとつの成果を開発する過程において D-Case を用いたリスク分析を用いることで，後の不具合となりうる要件(サブゴール)の漏れを少なくゴール分析図を完成させることができる．

3. 提案プロセスの有効性

以下の比較項目について，ゴール分析図単独で要求分析を実施した場合と提案手法で実施した場合とで比較する．

表 2 比較項目

No.	比較項目
1	D-Case による追加ゴールの発見度合い
2	誤りの伝播
3	要求分析完了までのトータルコスト
4	下位工程への誤りの流出可能性

No.1 は D-Case による論証を実施した場合に，ゴール分析図に対して追加のサブゴールを発見できることを指している．

No.2 はゴール分析において埋め込んだ誤りが検出されないまま最後まで伝播してしまうのか，もしくは作成中に検出されるのかを指している．

No.3 は D-Case による論証を実施している時間，および誤りを修正している時間を考慮したゴール分析図完成までのトータルコストを指している．

No.4 は完成したゴール分析図に誤りを含んだまま下位工程に流出する可能性を指している．

3.1. ゴール分析図単独型プロセスの評価

ゴール分析図単独で進める場合には，D-Case による新たなサブゴールの検出はされないことになる．また，誤りを埋め込んでもそれを検出する手段はゴール分析図完成後のレビューだけとなるため，作成初期に埋め込んだ誤りが末端まで伝播することになり，大きな手戻りを発生してしまう可能性がある．

一方，D-Case による論証時間は発生しないことになるが，誤りを埋め込んだままゴール分析図が下位工程に流出し，誤りを含んだままシステムが構築されることで後に大きな不具合を発生させる可能性がある．

3.2. 線形型プロセスの評価

線形型の場合には，先行してゴール分析図を作成する時間はゴール分析図単独型プロセスと代わらない．しかし，D-Case を用いてゴール分析図のディペンダビリティを検証することによって，後の不具合を先に検出，修正できる可能性がある．

一方，通常のレビューに加えて D-Case によるディペンダビリティの検証を実施している時間が加わるため，要求分析工程のトータルコストは増加し，ゴール分析図が完成してからの論証となるためゴール分析図に誤りが合った場合には手戻り時間が増加する．

3.3. 反復型プロセスの評価

反復型の場合には，ゴール分析図にてサブゴール分割を実施するたびに D-Case によるリスク分析を挟むことになるので，ゴール分析図完成までにかかる時間は増大する．しかし，D-Case を用いてリスク分析を実施し，適宜サブゴールの追加を行うことで，後の不具合を先に検出，修正できる可能性がある．また，逐次 D-Case に切り換えて論証するため，ゴール分析図に誤りがあれば即座に検出,修正できる可能性がある．

一方，通常のゴール分析に加えてサブゴールひとつひとつに対してリスク分析を行うので要求分析工程のトータルコストは増加することになる．

3.4. 評価結果まとめ

これまでの評価結果を以下にまとめる．

表 3　評価結果

No.	比較項目	①	②	③
1	D-Case による追加ゴールの発見度合い	—	高	高
2	誤りの伝播	する	検出可	逐次検出
3	要求分析完了までのトータルコスト	中	大	中
4	下位工程への誤りの流出可能性	中	小	小

①：ゴール分析図単独型プロセス
②：線形型プロセス
③：反復型プロセス

評価の結果，下位工程に誤りが流出しにくいという点において，D-Case を組み合わせたドール分析プロセスは有効ということがわかる．しかしながら，D-Case そのものの知識が必要なこと，および要求分析工程のトータルコストが増加することから，システムの特徴に合わせて適宜使い分けるのが得策と考える．どういった特徴のときにどの手段を選択するのかは未検証であるため今後の課題に譲る．現時点では協調すべき外部システムが少ない，小さいシステムにおいては線形型プロセスを選択しておき，協調すべき外部システムが多い，大きなシステムにおいては反復型プロセスを選択するほうが良いと考える．

4. 提案手法の限界について

提案したふたつの手法には，以下の限界がある．

① システムの運用まで含めた，提案手法の最終的な効果について検証していない
② D-Case 習得にかかるコスト，もしくは D-Case のプロフェッショナルに依頼して検証結果を得るまでのコストと時間とを加味していない
③ 比較的小さなシステムでは線形型，比較的大きなシステムでは反復型を推奨しているが，具体的なシステムの特徴や規模の閾値について検証していない

5. 今後の課題

今回，線形型を提唱するにあたり，D-Case による論証を先に実施する D-Case 先行線形型プロセスも考えられたが実証期間の都合で見送ることとした．

また，今回は成果物としてゴール分析図を対象として実証したが，提案した手法はゴール分析図に限らず全ての設計工程の全ての設計成果物に対しても適用できる可能性が示唆されたと考えている．

これらについては今後の課題である．

上述した提案手法の限界を解決するための課題と合わせ，以下の課題についても今後，研究に取り組んでいく予定である．

① D-Case 先行線形型プロセスの実証と評価
② システムの運用フェーズまで含めた提案手法の効果実測
③ D-Case 習得まで含めたトータルコストの評価

④ システムの特徴，規模など線形型と反復型の何れを適用すべきか判断するための判断基準の設定と妥当性検証
⑤ 提案手法の他設計成果物に対する適用と実証

6. 関連研究

従来のゴール指向分析[1]では，脅威に基づいてゴールを分解する手法は検討されていなかった．最近になって，ゴール指向に基づいてセキュリティ上の脅威分析に対するモデル化手法が Oladimeji らによって提案されている[2]．Oladimeji らは，否定ソフトゴール（N-softgoal, negative-softgoal）と逆貢献（inverse contribution）関係という概念を提案することにより，NFR フレームワークを拡張している．セキュリティ上の脅威を否定ソフトゴールで表現することができる．セキュリティゴールに対する脅威としての否定ソフトゴールならびに，否定ソフトゴールに対する対策ゴールを逆貢献関係で表現する．このような逆貢献関係を用いることにより，セキュリティソフトゴールを上位ゴールとすると，下位ゴールとして否定ソフトゴールに分解できる．同様にして否定ソフトゴールに対する対策としての下位ゴールを逆貢献関係によって分解できる．また NFR フレームワークと同様に，否定ソフトゴールを AND/OR 分解できる．否定ソフトゴールと逆貢献によって拡張されたソフトゴール依存グラフ（SIG, Soft Goal Interdependency Graph）が脅威 SIG である．

脅威 SIG の作成では，まずセキュリティに対するソフトゴールを分解する．次いで，それらのソフトゴールに対する脅威を否定ソフトゴールによって分解する．さらに，識別された否定ソフトゴールを緩和する対策ゴールを抽出する．

本提案では，ひとつのゴール分析図の中でリスク分析する代わりに，D-Case を用いてリスク分析を実施した結果をゴール分析図に反映している．したがって，ゴール分析図と D-Case という目的に応じた 2 種類の図式を組み合わせている点に特徴がある．また，脅威 SIG は，セキュリティ要求に対する手法である．これに対して本稿の手法はセキュリティ要求だけでなく，一般のリスク分析にも適用できる．今後，両手法の詳細な能力を明らかにするために，脅威 SIG と本提案の比較分析を実施する必要がある．

また，文献[5]では，要求モデリング手法における要素の結合方法の比較基準について網羅的な評価を提案している．本稿で述べた手法では，ゴールの分解関係と追加関係，並びに修正関係を用いている．

7. おわりに

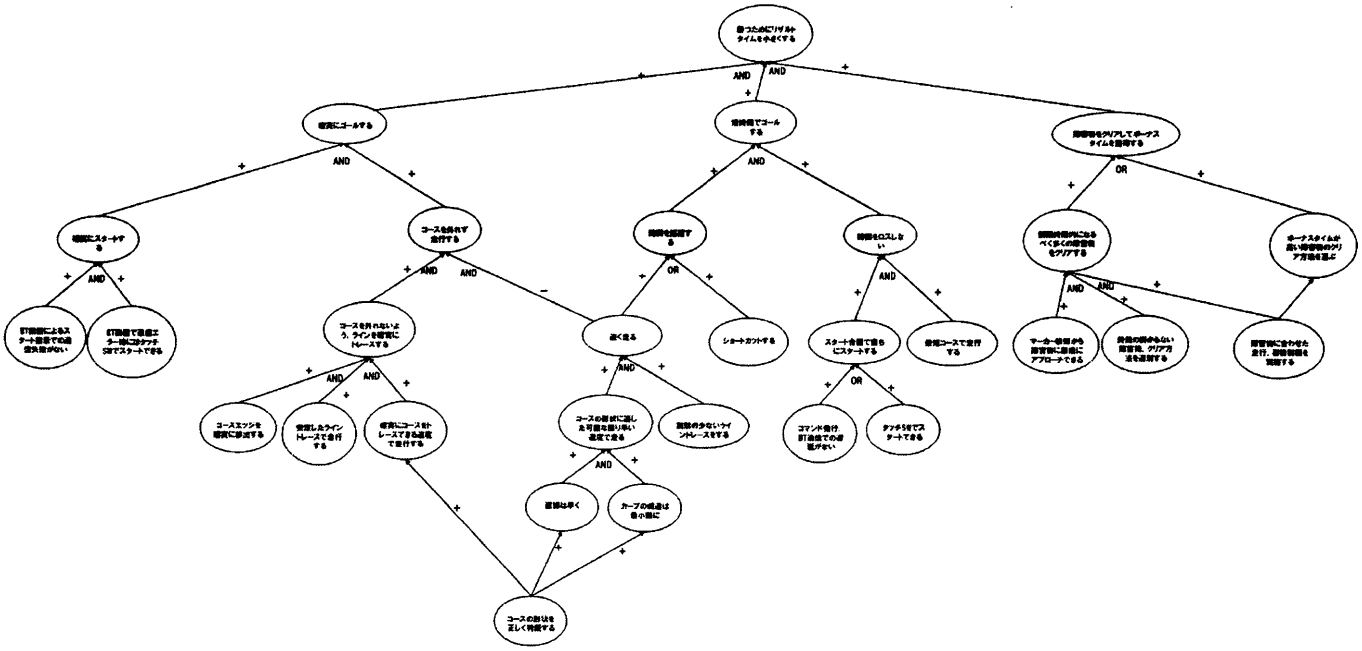
今回提案した成果先行線形型プロセス，反復型プロセスの何れも，ソフトウェアシステムの機能多様化，接続先増加などに起因する要求分析の抜け漏れを削減するための手段として有効であることが示された．

また，D-Case には成果物のディペンダビリティを検証する側面とゴールを阻害する要因を洗い出すリスク分析との側面があることから，両者の特徴を使い分けつつ全ての設計成果物の開発において D-Case を組み合わせることで後の不具合を削減することも可能と考えられる．

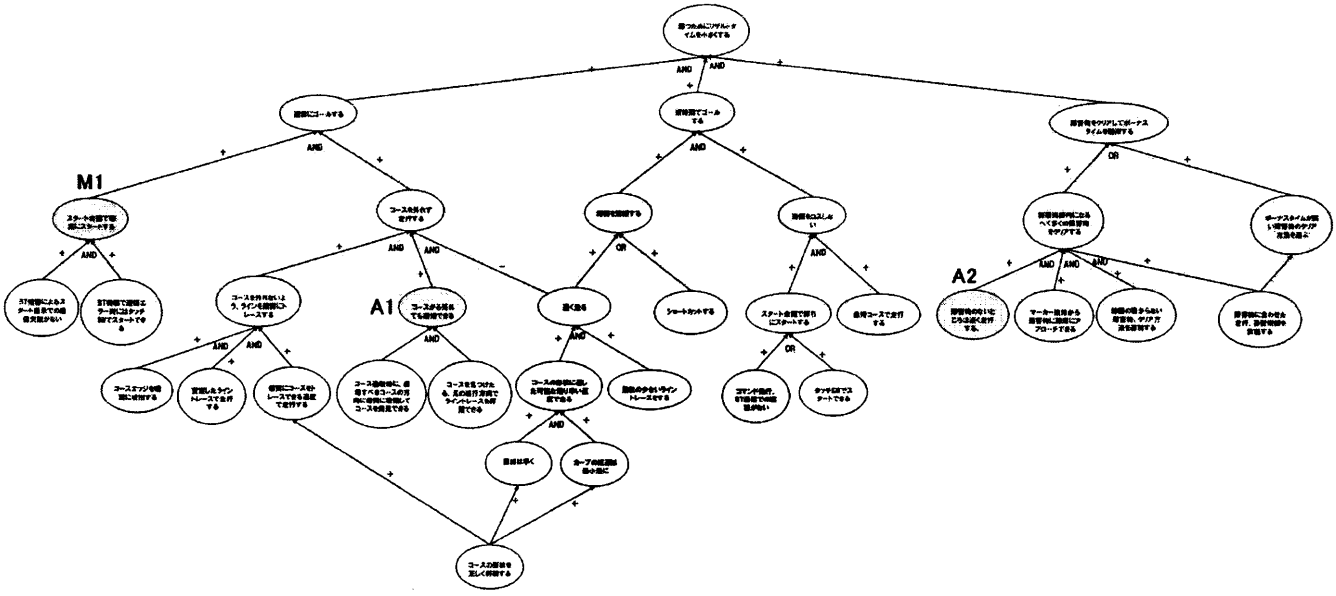
今後も D-Case 実証評価委員会の各種研究会をもとに多くの研究者と情報交換しながら課題の解決に努めていく予定である．

参考文献

[1] 山本修一郎，～ゴール指向による～システム要求管理，ソフト・リサーチ・センター，2007
[2] 山本修一郎，要求工学基礎知識，ダイテックオンデマンド出版，2013
[3] 松野　裕，山本修一郎，実践 D-CASE，ダイテックオンデマンド出版，2013
[4] Oladimeji EA, Supakkul S, Chung L (2006) Security threat modeling and analysis: a goal-oriented approach. In: Proceedings of the 10th international conference on software engineering and applications (SEA'06), pp 178–185
[5] Gunter Mussbacher et. al., Assessing composition in modeling approaches, **CMA '12:** Proceedings of the CMA 2012 Workshop



付図 1 ゴール分析図



付図 2 再作成したゴール分析図