人工知能学会
第15回知識流通ネットワーク研究会
SIG-KSN-015-05

コンテクスト依存表（CDM）に基づくD-Case作成法の提案

A proposal the method to construct D-Case based on Context Dependency Matrix

松村 昌典[1] *　森崎 修司[1]　渥美 紀寿[2]　山本 修一郎[2]
Masanori Matsumura[1]　Shuji Morisaki[1]　Noritoshi Atsumi[2]　Shuichiro Yamamoto[2]

[1] 名古屋大学大学院情報科学研究科
[1] Graduate School of Information Science, Nagoya University
[2] 名古屋大学 情報連携統括本部 情報戦略室
[2] Strategy Office, Information and Communications Headquarters Nagoya University

概要: アシュアランスケースの記述方法としてGSNが提案されている．GSNでは，ノード名が自然言語で記述されるため，内容が曖昧であるという問題がある．本稿では，GSNの前提条件の依存関係を記述できる行列CDMに基づいて，GSNのノード名と構造を系統的に作成する手法を提案する．また，提案した手法を適用した結果に基づいて，適切なGSNを記述できることを示す．

Abstract: GSN(Goal Structuring Notation) is proposed for describing Assurance Cases. There is a problem that content of GSN tends to ambiguous because GSN nodes are described by natural languages. In this paper, the method to create GSN based on Context Dependency Matrix(CDM) is proposed. The CDM describes the dependency relationship among context descriptions in GSN. It is also shown that the appropriate GSN can be created based on the method by using a running example.

1 はじめに

システムが指定された品質を持つことを保証するためにアシュアランスケース（D-Caseとも呼ぶ）を記述する手法がある．その記述方法としてよく利用されているGoal Structuring Notation（GSN）は自然言語で記述されるため，ノードに曖昧な内容が記述されたり，無関係な内容が記述されたノード間を誤って繋げたりする可能性がある．このような曖昧さや誤りがD-Case内に存在すると，ゴールを客観的に論証できない．これらを解決するために，いくつかの記述法が提案されている[1]．しかし現在提案されている記述法は抽象的であり，具体的にシステムの何をどのように論証し，D-Caseに記述すればよいか明確でない場合がある．そこで，システムにおける満たすべき条件やその対象（システムコンテクスト）や対象や条件の関係を明確にし，それらを記述したコンテクスト依存行列（CDM）に基づきD-Case作成法を提案する．

*松村 昌典
名古屋大学大学院情報科学研究科
〒 464-8601 愛知県名古屋市千種区不老町
E-mail: matsumura.masanori@e.mbox.nagoya-u.ac.jp

2 アシュアランスケースとD-Case

アシュアランスケース[2]は，システムが指定された品質を持つことを保証するための手法である．特に安全性を重視して記述する場合，アシュアランケースはセーフティケースと呼び，欧米では防衛や航空，鉄道などの分野で利用されている．またシステムがディペンダビリティをもつことを保証するためのアシュアランケースをD-Case[3]と呼ぶ．

Goal Structuring Notation（GSN）[4]はアシュアランスケースを表記する手法の一つである．GSNとは，議論すべき要求を分割，構造化することで，その要求を満たしているかどうかを図で確認することができる表記法である．要求を木構造に分割し体系立てることで，議論を構造化して確認することができる．議論すべきゴール（主張，要求）をトップゴールに定め，ストラテジ（議論の考え方，戦略）に基づき，ゴールを複数のサブゴールに分割する．ゴールを繰り返し段階的に詳細化していき，分割したゴールに記述されている命題が，エビデンス（証拠，ソリューション）によって満足される場合，そのゴールと対応するエビデンスを接続して，分割を終了する．またコンテクスト（制約，条件）をゴールやストラテジに接続して，各要素の前提条件を記述することができる．これらの表記法により，最下層まで分割された

すべてのサブゴールをエビデンスで保証し，トップゴールが満足されことを明確に確認できる．

3　システムコンテクストの概念

本稿で説明している，システムコンテクストとは，単に仕様書や設計書等の文や文脈を示すだけではなく，システムに存在する制約やステークホルダ，要求などといったシステム関わる人，物，条件のことを示している．言い換えれば，システム自体の分析やリスク分析，ゴール分析等から抽出した『システムに関する情報（システム構成やリスク等)』である．これらを抽出し，これらをシステムの要素や満たすべき原則（条件）を体系的に整理することで，システムコンテクストの範囲内で D-Case で論証することが可能になる．

図 1 に，既存の D-Case 記述手順モデルを示す．D-Case を記述する手順として（1）システムコンテクストを明確化するために，システム自体の分析やリスク分析，ゴール分析等を行い，(2）得られた情報から，システムの満たすべき条件を元に D-Case を記述する．分析結果から D-Case に記述する手法があり，例としてシーケンス図から D-Case を生成する規則が提案されている．

システムコンテクストには，2 つの属性“ 対象 ”と“ 条件 ”が存在し，各システムコンテクストはどちらか一つの属性を持つ．“ 対象 ”の属性であるシステムコンテクスト（以下，対象コンテクストと記述）は，システムの構成要素や，ステークホルダ等のようなシステムに関わる要素である．“ 条件 ”の属性であるシステムコンテクスト（以下，条件コンテクストと記述）は，ある対象コンテクストに対して満たすべき原則（条件）であるものを指す．例えば,「自動車は乗客をどんな事故が発生しても守る仕組みを持つ.」というシステムコンテクストがある場合，対象コンテクストは,「自動車」,「乗客」であり，条件コンテクストは,「どんな事故が発生しても守る仕組みを持つ」となる．

システムコンテクスト間の関係として，3 つが挙げられる．対象コンテクスト間の関係（対象-対象間），条件コンテクスト間の関係（条件-条件間），対象コンテクストと条件コンテクスト間の関係（対象-条件間）である．各関係は以下の時成り立つ．

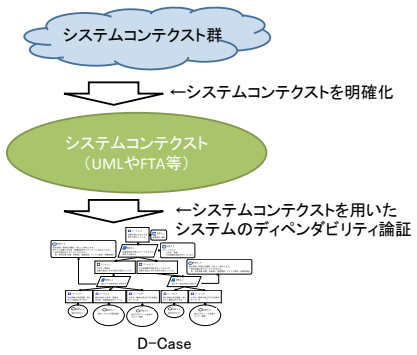


図 1: 既存の D-Case 記述手順モデル

- 対象-対象間 (以下，O-O 関係と記述)

  ある対象コンテクスト A がもう一方の対象コンテクスト B の構成要素となっている場合（例：「乗り物」と「自動車」）

- 条件-条件間 (以下，C-C 関係と記述)

  ある条件コンテクスト A がもう一方の条件コンテクスト B を具体的に記述した内容である場合（例：「大きな故障が発生しない」と「エンジン故障が起きない」）

- 対象-条件間 (以下，O-C 関係と記述)

  ある対象コンテクストがある条件コンテクストに対して，満たされるべき条件として記述できる場合（例：「自動車に対してエンジン故障が起きない」）

4　提案規則

4.1　コンテクスト依存表（CDM) の記述

本節では，コンテクスト依存表（Context Dependency Matrix：以下，CDM と記述）と，CDM 記述規則を説明する．

4.1.1　CDM

本稿では，D-Case を記述するための CDM を提案する．CDM はシステムに存在する様々なコンテクストとそれらの関係を示す表である．表 1 に，CDM の例を示す．CDM の記述によって，D-Case に記述すべき要素や条件を整理できる．

CDM は表 2 のように，要素（システムコンテクストの用語や条件文）E，属性 A，関係 R を表形式で記述される．(ある成分に対し，その行に記述されている要素 $e \in E$ を行要素，その列に記述されている要素 e' を列要素と記述する.）各要素を第 1 行，第 1 列に同順序で記述し，表の対角成分に「対象」または「条件」という属性を記述する．O-O 関係または C-C 関係が成り立つなら

表 1: CDM の例:ETC システムに対する簡易的な CDM

	ETC料金支払システム	システム構成	車	無線アンテナ	支払いシステム	車にETCカードが挿入されている	アンテナが無線リスナー状態である	車にETCカードが挿入されていない状態であると，ドライバへ通知する．
ETC料金支払システム	対象	+	+	+	+	@	@	
システム構成		対象	+	+	+	@	@	
車			対象			@		@
無線アンテナ				対象			@	
支払いシステム					対象	@	@	@
車にETCカードが挿入されている．						条件		
アンテナが無線リスナー状態である．							条件	
車にETCカードが挿入されていない状態であると，ドライバへ通知する．								条件

表 2: CDM の概形

	e1	e2	e3	e4	e5	⋯	en
e1	対象	+	+	@	@		
e2		対象		@	@		
e3			対象		@		
e4				条件	+		
e5					条件		
⋮						⋱	
en							****

ば，要素 A が記述されている行と要素 B が記述されている列（要素 A と要素 B は，3 章で記述した O-O 関係，C-C 関係の説明に対応している）が交差しているセルに“ + ”を記述する．表 2 の例では,「e_2 と e_3 は e_1 に含まれている」という関係である．また，O-C 間で「“ 対象 ”が“ 条件 ”を満たす」という文に当てはまるような関係であるならば，対象コンテクストが記述されている行と条件コンテクストが記述されている列が交差しているセルに“ @ ”を記述する．表 2 の例では,「e_2 は e_4 を満たしている」という関係である．なお，CDM に記述されている要素が N 個であれば，$(N+1)*(N+1)$ のセルで構成された表になる．

4.1.2 CDM の記述規則

以下に，CDM の記述規則を示す．

1. リスク分析やゴール分析等を用いて，システムやプロセス等のシステムコンテクストの用語や条件文を抽出する．
2. システムコンテクストの中で，対象コンテクストと条件コンテクストとなる要素を書き出す．
3. 表 2 のように，要素を CDM の一行目，一列目にそれぞれ順に記述する．
4. 各行のシステムコンテクストに対し，表の対角成分にシステムコンテクストの属性（条件または対象）を記述する．
5. コンテクスト間で O-O 関係や C-C 関係が存在する場合，抽象側の要素が記述されている行と具体側の要素が記述されている列と交差部分のセルに“ + ”を記述する（表 2 の例では，e_2 と e_3 または e_1 である．）
6. コンテクスト間で O-C 関係が存在する場合，対象コンテクストが記述されているの行と条件コンテクストが記述されている列の交差部分のセルに“ @ ”を記述する．（表 2 の例では，e_2 と e_4 である．）
7. ある行（ある列）に対し“ @ ”が記述されているセルがない場合，満たすべき条件（システムに関係する要素）を考え，列（行）を追加する．

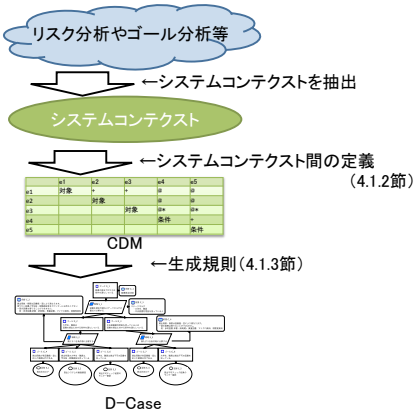


図 2: CDM と D-Case とシステムコンテクストの関係

4.1.3 CDM と D-Case の関係

CDM はシステムのコンテクストやコンテクスト間が明確に記述されている表である．D-Case はシステムがコンテクストに記述されている条件や制約を満たしているかを確認するための図である．そのため，D-Case を記述するための前提として，CDM が必要である．

従来の D-Case のコンテクスト抽出手法においては，CDM のようなシステムのコンテクストを明確にする手法として FTA（Falut Tree Analysis），FMEA（Failure Mode and Effects Analysis）等を用いたリスク分析 [5] や NTR フレームワーク（Non Functional Requirements Framework），i*（アイ・スター）等を用いたゴール分析が挙げられる [6]．それらの手法から抽出したリスクや要求をコンテクストとし，CDM でコンテクスト間を明確にする．

これらをまとめると以下の図 2 のように表すことができる．

4.2 CDM に基づく D-Case 生成規則

以下に，CDM から D-Case を生成する規則を記述する．CDM によって体系的にシステムコンテクストを整理し生成規則を適用することで，CDM に記述されている要素が条件を満たしているかどうかを確認できる D-Case を生成できる．

なお,“ システムコンテクスト ”と“ D-Case のコンテクストノード ”を書き分けるため，前者を「対象（条件）コンテクスト」，後者を「D-Case のコンテクスト」と記述する．

1. CDM の各列で，O-C 関係を示す記号（@）が最も多く付いている対象コンテクストすべて取り出し，対象コンテクストの中で O-O 関係の最上位の（最も対象コンテクストを包含している）ものを対象コンテクスト X とする．

2. 対象コンテクスト X の用語を用いて，D-Case のゴール x「○○に対して，条件が満たされている」を生成する．
3. 対象コンテクスト X と O-O 関係を示す記号（+）を持つサブ対象コンテクストがあれば，D-Case のストラテジ s「○○に関して，以下の観点で分解する」をゴール x に接続する．O-O 関係を示す記号（+）がなければ，手順 6 へ
4. ストラテジ s に D-Case のコンテクスト c を接続する．コンテクスト c には，手順 3 のサブ対象コンテクストを列挙する．
5. ストラテジ s に 1 つ以上のサブゴール g を接続する．各サブゴール g には，D-Case のコンテクスト c に記述したサブ対象コンテクストの用語を用いて，D-Case のゴール x「○○に対して，条件が満たされている」を記述する．手順 3 へ．
6. 対象コンテクスト X に対し，O-C 関係を示す記号（@）を持つ条件コンテクストがあれば，D-Case のストラテジ s「○○が満たすべき条件毎に分解する」をゴール x に接続する．O-C 関係を示す記号（@）がなければ，手順 12 へ
7. ストラテジ s に D-Case のコンテクスト c を接続する．コンテクスト c には，手順 6 の条件コンテクストを列挙する．
8. ストラテジ s に 1 つ以上のサブゴール g を接続する．各サブゴール g には，コンテクスト c に記述した条件コンテクストの用語を用いて，D-Case のゴール x「○○は△△という条件を満たしている」を記述する．
9. 対象コンテクスト X に対し，C-C 関係を示す記号（@）を持つ条件コンテクストがあれば，D-Case のストラテジ s「○○が満たすべき条件を分解する」をゴール x に接続する．C-C 関係を示す記号（@）がなければ，手順 12 へ
10. ストラテジ s に D-Case のコンテクスト c を接続する．コンテクスト c には，手順 9 の条件コンテクストを列挙する．
11. ストラテジ s に 1 つ以上のサブゴール g を接続する．各サブゴール g には，D-Case のコンテクスト c に記述した条件コンテクストの用語を用いて，D-Case のゴール x「○○は△△という条件を満たしている」を記述する．手順 9 へ
12. D-Case の最下位ゴールに適切なエビデンスを接続する．

5 提案規則の実行例

4.2 節で示した，CDM から D-Case への生成規則を用いて D-Case の作成を行う．今回の目的として，図書貸出システムのシステムコンテクストから D-Case を生成を行うことにより，記述内容が満たすべき条件をすべて網羅しているかどうかを確認する．

5.1 適用対象

図書の貸出プロセスの CDM へ生成規則を適用した．貸出に関係するものは以下の通りである．図書の貸出プロセスは，本大学の図書館の貸出プロセス [7] をモデルとして，箇条書きで記述しており,「図書を貸出す機能」のみを対象にしている．これらのシステムコンテクストからプロセス要素とそれらの満たすべき条件を整理して記述した CDM を付表 1 に示す．図書貸出の CDM は 19 の対象や条件を持つ．なお，適用対象に CDM に基づく D-Case 生成規則の 1 から 11 を適用した（D-Case のエビデンスノードは生成しない）．

- 関係対象要素
  - 各図書館・ 室
  - 図書の種類（普通図書，貴重図書など）
  - 貸出可能である人（名大生，名大職員,「図書館利用証」を持参した外部の人）
- 満たすべき条件
  - 貸出対象者である
  - 各図書館・ 室の貸出期間に準じた貸出を行っている
  - 各図書館・ 室の貸出冊数制限に準じた貸出を行っている
  - 貸出不可である
  - 一部の図書館・室で貸出不可である
  - 学生証や職員証を持っている

5.2 適用結果

実験を行った結果は以下の通りである．CDM に記述しているシステムのコンテクスト 19 個から，D-Case は 46 ノード（ノード数はそれぞれ，ゴール:22，ストラテジ:11，コンテクスト:13）生成された．

生成された D-Case のノード内容を確認した結果，ノードの記述内容やそれらのノード間の関係は妥当であると確認できた．また，CDM を見ることにより，新たなシステムコンテクストを発見することができた．今回の適用例では，以下のようなゴールを考えることができ，これらのゴールを適切な場所に配置することができた．こ

れらのノードの発見は通常では気づきにくいと思われるが，明確に確かめたわけではない．

また，生成された D-Case の構造が階層的であり，理解しやすいと考えられる．

- ストラテジ（戦略）ノード S_12 の下に『外部の人は「図書館利用証」を持参している』というゴールノードを記述することができる．図書貸出に対し「外部の人は「図書館利用証」を持参している」という条件を考慮していなかったことが分かった．
- ストラテジノード S_2 の下に『各図書館・室は，各図書館・室の開館時間内での貸出を行っているという条件を満たしている』というゴールノードを記述することができる．図書貸出に対し，「各図書館・室の開館時間内での貸出を行っている」という条件を考慮していなかったことが分かった．

6 考察

6.1 適用結果について

適用結果からシステムコンテクストを抽出し，CDM を記述することによって，CDM の記述内容を保証する D-Case が記述できることが分かった．CDM を記述し，生成規則を用いて D-Case を記述すると，以下の 2 つの利点があると考えられる．

- CDM から，新たな満たすべき条件を発見することができる．
- D-Case の各部分が階層的に記述でき，理解しやすい．

また，生成した D-Case を分析することにより，新たなシステムコンテクストを発見することができた．これは，システムコンテクストに対し CDM を用いて満たすべき条件を整理することにより，D-Case が体系的に記述できたためであり，比較的理解しやすい図になっていると考えられる．

一方，今回の適用例としては，システムコンテクストがある程度存在し，それから記述した CDM が正しいという前提の元で行っている．そのため，以下に記述した状況の際に提案規則を使えるか不確実である．

- システムコンテクストが極端に少ない場合
- コンテクストの抽出に誤りがあった場合
- D-Case 作成に不必要なコンテクストが CDM にある場合

6.2 CDM 記述方法の課題

CDM を用いて D-Case を記述する方法の課題として以下なものが存在する．

- すべてのシステムコンテクストに対して関係を議論すべきかどうかという問題
- 現実的な時間内で CDM が記述可能であるかに対する問題
- CDM を用いて記述した D-Case は，そうでない D-Case と比べて有意であるか

7 おわりに

本論文では，システムのコンテクストと，コンテクスト間の関係を明確に定義できる CDM に基づく D-Case 作成法を提案した．また，提案手法を図書館システムに適用した．この結果，19 個のコンテクストからなる CDM に基づいて，46 ノードからなる D-Case を作成できることを具体的に明らかにした．

参考文献

[1] 山本修一郎，松野　裕，ディペンダビリティケース分解パターンについての考察，信学技報，vol. 112, no. 496，KBSE2013-80. pp. 67-72，2013 年 3 月．

[2] Peter Bishop, Robin Bloomfield, Sofia Guerra, The future of goal-based assurance cases, DSN, 2004.

[3] 松野裕, 高井利憲, 山本修一郎. D-Case 入門 〜ディペンダビリティ・ケースを書いてみよう！〜. 株式会社ダイテックホールディング, 2012. ISBN: 978-4-86293-079-8.

[4] Tim Kelly and Rob Weaver. The goal structuring notation - a safety argument notation. In Proc. of the Dependable Sys- tems and Networks 2004, Workshop on Assurance Cases, 2004.

[5] *Marco Bozzano*，*Adolfo Villafiorita*（2010）. Design and Safety Assessment of Critical Systems, Auerbach Publications

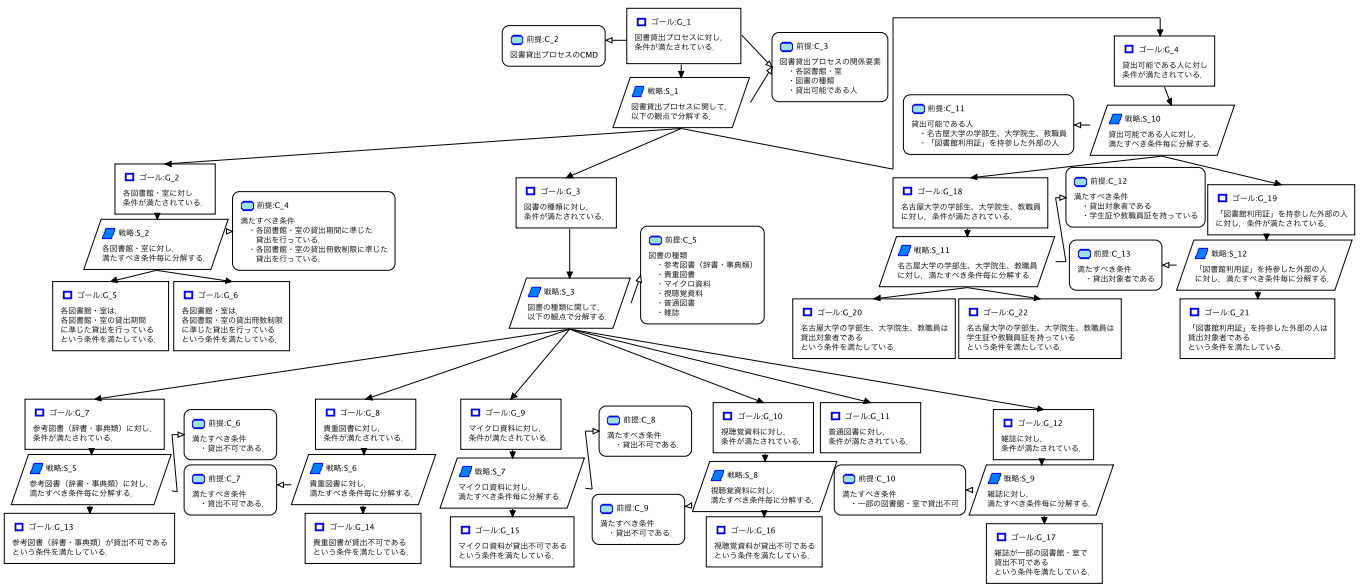
[6] 山本修一郎，要求工学基礎知識，名古屋大学情報連携統括本部情報戦略室，2012

[7] 名古屋付属図書館　名古屋大学附属図書館サービス案内　貸出，http://www.nul.nagoya-u.ac.jp/guide/index.html

付録

付表 1: 図書の貸出プロセスの CDM

CMDの大きさ：19	図書貸出プロセス	各図書館・室	図書の種類	参考図書（辞書・事典類）	貴重図書	マイクロ資料	視聴覚資料	普通図書	雑誌	貸出可能である人	名古屋大学の学部生、大学院生、教職員	「図書館利用証」を持参した外部の人	満たすべき条件	貸出対象者である.	各図書館・室の貸出期間に準じた貸出を行っている.	各図書館・室の貸出冊数制限に準じた貸出を行っている.	貸出不可である.	一部の図書館・室で貸出不可である.	学生証や職員証を持っている.
図書貸出プロセス	対象	+	+	+	+	+	+	+	+	+	+	+	@	@	@	@	@	@	@
各図書館・室		対象											@		@	@			
図書の種類			対象	+	+	+	+	+	+				@						
参考図書（辞書・事典類）				対象									@				@		
貴重図書					対象								@				@		
マイクロ資料						対象							@				@		
視聴覚資料							対象						@				@		
普通図書								対象					@						
雑誌									対象				@					@	
貸出可能である人										対象	+	+	@	@					
名古屋大学の学部生、大学院生、教職員											対象		@	@					@
「図書館利用証」を持参した外部の人												対象	@	@					
満たすべき条件													条件	+	+	+	+	+	+
貸出対象者である.														条件					
各図書館・室の貸出期間に準じた貸出を行っている.															条件				
各図書館・室の貸出冊数制限に準じた貸出を行っている.																条件			
貸出不可である.																	条件		
一部の図書館・室で貸出不可である.																		条件	
学生証や職員証を持っている.																			条件



付図 1: 実験で生成した図書の貸出プロセスの D-Case