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
KBSE2012-63 (2013-01)

ディペンダビリティケース用語構成規則の提案

松村 昌典† 松野 裕†† 山本修一郎††

† 名古屋大学 工学部 〒464-8601 愛知県名古屋市千種区不老町
†† 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
E-mail: †matsumura.masanori@e.mbox.nagoya-u.ac.jp, ††{matsu,yamamotosui}@icts.nagoya-u.ac.jp

あらまし ディペンダビリティケースを作成するための図式表記法が提案されている．しかし，ディペンダビリティケースで使用されている用語が統一されていないという問題がある．このため本稿では，ディペンダビリティケース用語を統一的に構成する規則を提案する．

キーワード ディペンダビリティ，ディペンダビリティケース，用語関係図

A proposal on a rule to construct a word of Dependability Case

Masanori MATSUMURA†, Yutaka MATSUNO††, and Shuichiro YAMAMOTO††

† School of Engineering Nagoya University
Furo-cho, Chikusa-ku, Nagoya, Aichi, 464-8601 Japan
†† Strategy Office, Information and Communications Headquarters Nagoya University
Furo-cho, Chikusa-ku, Nagoya, Aichi, 464-8601 Japan
E-mail: †matsumura.masanori@e.mbox.nagoya-u.ac.jp, ††{matsu,yamamotosui}@icts.nagoya-u.ac.jp

Abstract A few graphical notations for dependability cases have been proposed including GSN(Goal Structuring Notation). However, there is a problem that words in Dependability Cases are not unified. In this paper, we propose rules to consistently identify words used in dependability cases.

Key words Dependability, Dependability Case, Word Relationship Diagram

1. はじめに

ディペンダビリティケースでは，人・物・活動等に対する関係性が明確ではないという問題がある．例えば，列車運行システムのディペンダビリティケースでは"業務"と"列車運転業務設計書"の関係は記述しない．しかしディペンダビリティケースを記述する際，これらの用語間の関係を知らないと，図を作成するのは難しい．

そこで，その関係性を明確にする一つの方法として，用語関係図を用いる．用語関係図とは，人・物・活動等を要素としてその要素間の関係をまとめた図である．ディペンダビリティケースで使用されている用語や用語関係を明確にすることは，ディペンダビリティケース記述や理解の助けとなる．前回の発表[1]では，用語関係図からディペンダビリティケースの変換方法は記述していたが，完全に構成規則として変換できるかは明確にしていなかった．本稿では，理解や記述を容易にすることで，ディペンダビリティを比較・評価をする方法の一つとして，ディペンダビリティケース用語を統一的に構成する規則を提案する．

本稿の構成は次のとおりである．2節において，前回提案した用語関係図を説明する．3節において，現在の課題について記述する．4節において，構成規則の提案とその適用例を順に記述し，5節に3節であげた問題との結果を述べる．6章において，本稿についての考察を記述して．最後に今後の課題について述べる．

2. 用語関係図について

用語関係図 (Word Relationship Diagram) とは，人・物・活動等を要素としてその要素間の関係をまとめた図である．用語関係図を作成することによって，ディペンダビリティケースの図式要素の用語や用語関係を定義する．その結果，用語関係図を用いることにより，ディペンダビリティケース記述や理解を容易化できる．

関係図の構成要素は以下の3つである．

- ノード
- 関係名
- 矢印

人，物，活動等の書かれたノードに対し，ノード間に主要な関係があれば実線矢印を書き，その矢印に関係名を書く．各

ノードには矢印がいくつか接続することができる.

例として，商品売買システムの用語関係図を図 1 の図示する. 以下の用語間の関係を元に作成した.

- 店員は商品を販売対象としている.
- 店員は客に販売する.
- 客はお金を所有している.
- 店員にお金を支払う.

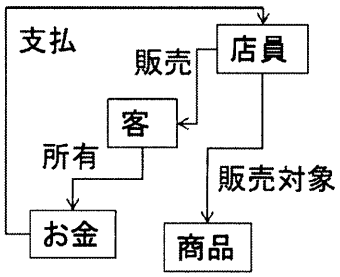


図 1　商品売買システムの用語関係図の例

3.　現在の課題

用語関係図について，現在の課題は以下の通りである.

- 関係名の種類分け

関係名には種類があり，規則があると予想している. これをいくつかの例からどのような関係名があるか整理する必要がある. この結果，ディペンダビリティケースの必要であるべき欠落ノードを発見・評価することができる.

- ディペンダビリティケースから用語関係図への作成規則の考案

前回の発表では，不十分ではあるが用語関係図からディペンダビリティケースへの生成規則を提案した. しかし，ディペンダビリティケースから用語関係図への変換も可能であると予想している. そこで，ディペンダビリティケースから用語関係図への生成規則を考案する. この結果，用語関係図とディペンダビリティケース間の相互変換を実現することができる.

- 用語関係図から作成したディペンダビィケースのノード欠落の対処

前回の発表で提案した，用語関係図からディペンダビリティケースへの生成規則を適用すると，予想したディペンダビリティケースとは異なるものが生成された. 用語関係図とディペンダビリティケース間の同値変換を実現するために生成規則や図を修正する必要がある.

4.　構成規則の提案

以下では，前回の発表で提案した「用語関係図からディペンダビリティケースへの生成規則 (W2D)」の変更点と，今回提案する「ディペンダビリティケースから用語関係図への生成規則 (D2W)」を記述する. また用語関係図に加えて，用語関係図に使用されている用語を定義する「用語構成規則」を提案する.

なお，用語関係図とディペンダビリティケースの変換と用語関係規則の関係の概要は図 2 に記述している.

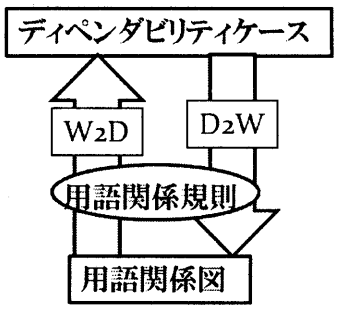


図 2　関係概要

4.1　用語関係図からディペンダビリティケースへの生成規則 (W2D)

4.1.1　分析対象と分析

列車運行システムの用語関係図は図 3 に示す. これは列車運行システムのディペンダビリティケースに使用されている用語を抽出し，それぞれの関係を明示することで作成した.

この図で共通している部分として，図 4 に示すような箇所があり，これはディペンダビリティケースの「コンテクストに基づいて，ストラテジ分解をし，サブゴールで議論する」といった，似通った性質をもっている. この性質に注目してディペンダビリティケースを作成する生成規則を提案する.

なお，本稿では前回の発表で提案した時に作成した元の図が異なるため，改めて修正した規則を提案することとする.

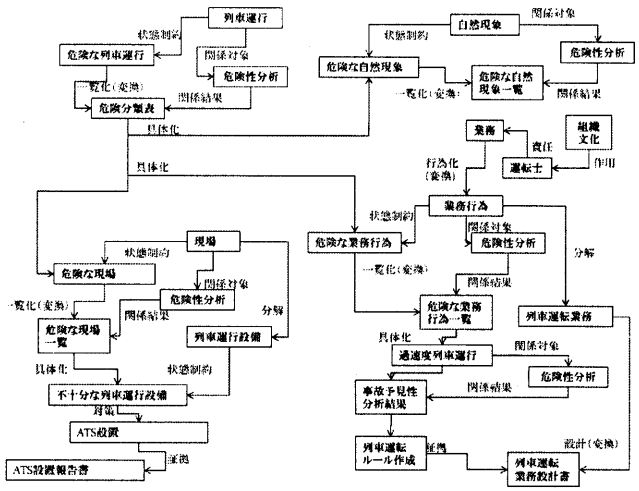


図 3　列車運行システムの用語関係図

4.1.2　生成規則

1　用語関係図からトップゴールを定める. トップノードを用いて,「X はディペンダブルである.」という命題文に書き換え，ディペンダビリティケースのトップゴールとする.

2　用語関係図から関係名"一覧化 (変換)"，を分割探索する.

3　関係名"一覧化 (変換)"の矢印が示しているノード Y を用いて,「Y に基づき，分けて議論する」というストラテジを最近作成したディペンダビリティケースの上位ゴールに接続する. そのストラテジにコンテクスト「Y」を接続する. もし，ノード Y がない，もしくはノード Y が示しているノードがなければ，

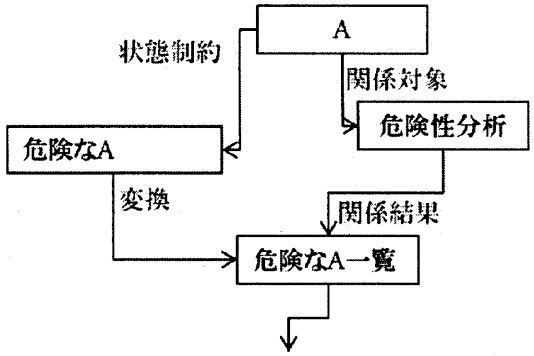


図 4　用語関係図に現れる共通の部分

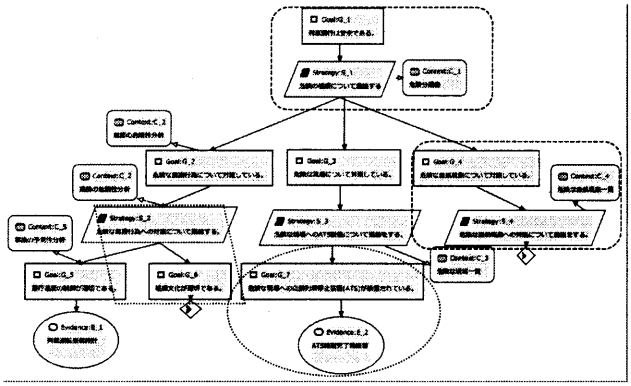


図 5　列車運行システムのディペンダビリティケース

代わりに最近作成した上位ゴールにアンデベロップを接続する.
4　ノード Y が示している 1 つ以上のノード Z を用いて,「Z について対策している.」という命題文に書き換え，ディペンダビリティケースのサブゴールとする．もし，ノード Y が示しているノードがなければ，代わりにアンデベロップを接続する.
5　ノード Y を示している矢印があれば，それらすべてのノード A において,「A において適切である (存在する)」というゴールをさらに付加する.
6　関係名”対策”を発見するまで [2]-[5] を繰り返す.
7　関係名”対策”を発見した場合はさらに探索していき，関係名”証拠”の矢印が示しているノード E を用いて,「E」というエビデンスを最近作成したディペンダビリティケースの上位ゴールに接続する.

4.1.3　適　用　例

付図 1 は，上記の手法で作成したディペンダビリティケースである．用語関係図を作成する際に参考にした元のディペンダビリティケース (図 5) と比較すると，達成すべきゴールノードが増加した.

4.2　ディペンダビリティケースから用語関係図への生成規則 (D2W)

4.2.1　分析対象と分析

列車運行システムのディペンダビリティケースを図 5 に示す. はじめに”列車運行は安全である.”をトップゴールに定める. 危険分類表から列車運行に対する危険は 3 つあると分 かるため, それぞれの危険 (業務危険行為, 危険な現場, 危険 な自然現象) について議論する. 危険分析の結果, それぞれのサブゴールを記述している. 最後に, エビデンスとなるような 設計書や報告書等を記述している.

列車運行システムの用語関係図を分析を行った．列車運行システムの中に共通の部分を探し，その部分がディペンダビリティケースと比較し，どの箇所に対応するかどうかを吟味した. 以下のように同じ構造パターンをした箇所が存在することが分かった.

パターン 1　分解部パターン

分解部パターンは，図 5 の四角点線部分である．あるノード A を中心に，関係名”状態制約”，”関係対象”，”関係結果”，”一覧化 (変換)”で複数のノードがつながれている．ディペンダビリティケースのあるゴールに対し，コンテクストの内容の元，ストラテジ分解を行う一連の分解構造と対応する．構成要素は，ゴール，そこに接続しているストラテジ (存在すれば，コンテクスト) 各々1 つである.

パターン 2　証拠部パターン

証拠部パターンは，図 5 の平行四辺形点線部分である．あるノード A から，関係名”対策”，”証拠”，でノードがつながれている．ディペンダビリティケースのあるゴールに対し，エビデンスを導出する箇所に対応する．構成要素は，ゴール，そこに接続しているエビデンス (存在すれば，コンテクスト) 各々1 つである.

パターン 3　前提部パターン

前提部パターンは，図 5 の楕円点線部分である．あるノード A に対して，必要な前提条件が記述されている部分．ディペンダビリティケースのあるストラテジに対し，ゴールを導出する箇所に対応する．構成要素は，ストラテジ 1 つ，そこに接続している複数のゴールである.

4.2.2　生 成 規 則

分析の結果を元に，ディペンダビリティケースから用語関係図の生成規則を記述する.

用語関係図の生成にあたり，まず元となるディペンダビリティケースから 3 つのパターンに分ける．その後，それぞれのパターンに分けて部分的な用語関係図を生成し，最終的にすべての図における同名のノードを結合させ，同名の関係名による冗長性を無くすことによって用語関係図を生成する.

◎分解部パターン

1　あるゴールの用語「G」を抽出し，ノード G とする．ゴール文が「G は安全である」といったものであれば，[2-1] へ進む. ゴール分が「G について対策をする」であれば，[2-2] へ進む
2-1　ノード G からノード”分析”を関係名”関係対象”で接続する．また，ノード X”危険な G”を関係名”状態制約”で接続する．[3] へ進む.
2-2　用語「G」から形容部分を取り除いたノード G’ を生成し,

ノードG'からノードGを関係名"状態制約"で接続する．ノードG'からノード"分析"を関係名"関係対象"で接続する．[3]へ進む．

3　ゴールのコンテクストが存在すれば，コンテクストの用語「G-C」を抽出し，ノードG-Cとする．ノードG-Cからノードを関係名"前提条件"で接続する．ストラテジにコンテクストが存在すれば，[4-1]へ進む．そうでなければ，[4-2]へ進む

4-1　ストラテジに接続しているコンテクストの用語「S-C」を抽出し，ノードS-Cとする．ノード"分析"から，ノードCを関係名"関係結果"で接続する．また，ノードXから，ノードS-Cを関係名"一覧化(変換)"で接続する．[5]へ進む．

4-2　関係名"状態制約"で示されているノードから，関係名"具体化"で接続する．[5]へ進む．

5　ノードS-Cからの矢印が存在するならば，以下のサブゴールについて同様に繰り返す．

◎証拠部パターン

1　あるゴールの用語「G」を抽出し，ノードGとする．ゴールにコンテクストが存在すれば，[2-1]へ進む．そうでなければ，[3]へ進む

2-1　コンテクストの用語「C」を抽出して，ノードCとする．ノードGからノード"分析"を関係名"関係対象"で接続し，ノード"分析"からノードCを関係名"関係対象"で接続した後，ノードGからノードCを関係名"一覧化(変換)"で接続する．[3]へ進む．

3　ノードC(ノードCが存在しなければ，ノードG)から，ノードGの対策をノードAとし，関係名"対策"で接続する．

4　ゴールに接続しているエビデンスの用語「E」を抽出する．ノードAからノードEを関係名"証拠"で接続する．

◎前提部パターン

1　前提パターン中のすべてのゴールから用語Xを抽出し，ノードXとする．

2　[1]における上位のゴールGについて，ノードXから矢印を示していき，ノードXまでたどりつくまで[3]を行う．

3　あるノードAに対し，その関係のある用語「B」をノードBをし関係名で接続する．

4.2.3　適　用　例

付図2は，上記の手法で作成した用語関係図である．元の用語関係図(図3)と比較すると，一部のノードやそれに付随する関係名が減少した．

4.3　用語関係規則

4.3.1　用語関係規則の定義

用語関係図は，ノードやそれに付随する関係名には関係があり，規則が存在すると推測できる．ここで，列車運行システムの用語関係図内にある用語名について分類化し吟味した結果．表1のように分けることができた．この用語関係規則を用いて関係名を分類することができ，関係名と用語関係図の構造と比較することによって，関係名の妥当性を評価することができると考えている．

表1　用語関係規則一覧

規則	記法	説明
制約化	左辺 = 右辺1 / 右辺2	左辺は右辺1の状態に制約された右辺2である
変換化	左辺 = 右辺1 + 右辺2	左辺は右辺2の型に変換された右辺1である
関係化	左辺 = 右辺1 ` 右辺2	右辺1に対して右辺2が左辺で示される関係を持つ
具体化	左辺 |= 右辺	左辺は右辺の具体化である
分解化	左辺 != 右辺	左辺は右辺から分解されている
対策化	左辺 <- 右辺	左辺は右辺の問題への対策である
生成化	左辺 = 右辺1(右辺2)	右辺1により，右辺2を対象として左辺を生成する
証拠化	左辺 @ 右辺	左辺は右辺から導かれた証拠である

5.　生成規則考案結果と課題解決

D2Wを作成することによって既存のディペンダビリティケース用語における評価を可能にした．また，前回の発表で提案したW2Dを用いると，生成したディペンダビリティケースに欠落ノードがあったが，それを関係名を用語関係規則で分類し，そこから新たにW2Dを修正した結果，欠落ノードのないディペンダビリティケースが生成できた．

6.　考　　察

本稿では，ディペンダビリティケースと用語関係図との相互変換するような生成規則を提案した．しかしその結果，以下の課題がでてきた．これらの課題について説明する．

6.1　他システムでの用語関係図の適用

本稿では列車運行システムの用語関係図やディペンダビリティケースから双方の分析を行い，相互変換を行う生成規則の提案をした．また，その変換に必要な用語関係規則を提案した．しかし，これら規則の正しさや有用性はまだ評価できていない．

この問題を解決するするために，いくつかの他システムに対しても適用していきその生成されたディペンンダビリティケースや用語関係図について評価する必要がある．

6.2　W2Dで生成したディペンダビリティケースのゴールノード増加における対処

W2Dで生成したディペンダビリティケースでは元のディペンダビリティケースと比較すると，ゴールノードが増加している．増加したゴールノードを分析すると，ゴールノードの命題文の前提条件にもなりうる内容，つまりコンテクストの内容にも変換することができる．その箇所は，ディペンダビリティケースにおいて書かれることのない暗黙の前提条件であり，用語関係図ではそれを抽出する手がかりになると予想できる．

この問題を解決するために，増加したゴールノード議論を深めていく必要がある．

6.3 D2W で生成した用語関係図のノード欠落についての議論

D2W で生成した用語関係図では元の用語関係図と比較すると，一部のノードと関係名が欠落している．欠落したノードと関係名は以下の通りである．

ノード"列車運行設備
　関係名"分解"
　関係名"状態制約"
ノード"列車運転業務"
　関係名"分解"
　関係名"設計 (変換)"

欠落したノードは，現在生成する際には使用していないので，ノード欠落について対処すべきかどうかを議論する必要がある．

6.4 ゴールノード要素における positeve・negative 性の議論

今回，D2W を考えるにあたり，ディペンダビリティケースの構造だけでなく，ノード内の文章も吟味して変換する必要が出てきた．それはディペンダビリィケースに記述されるゴールノードの文章は以下のように分類され，その分類によって D2W 規則が異なることが分かったためである．

◎　安全性等を具体化できる内容

図 5 の列車運行システムにおいては，ゴールノード (G-1)「列車運行は安全である.」というように，positeve 性の文章 (以下，type P) できている．

◎　危険性等を具体化できる内容

図 5 の列車運行システムにおいては，ゴールノード (G-3)「危険な現場について対策している.」というように，negateve 性の文章 (以下，type N) できている．

これを明確にすることによって，type P の内容と type N の内容を相互変換するような規則を考案でき，その結果ディペンダビリティケースの記述内容における分析を安易でき，また D2W によって生成される用語関係図をの構造を統一することができると推測できる．

この問題を解決するために，ゴールノードだけでなくディペンダビリティすべてのノードにおいて，type P と type N に分類することが可能であるか，分類することで用語関係図は変化してくるのかという 2 点において分析していく必要がある．

7. おわりに

本稿では，前回の発表で提案した用語関係図について，ディペンダビリティケースから用語関係図への変換規則 (D2W) と，用語関係図からディペンダビリティケースへの変換規則 (W2D) を提案した．また用語関係図に加えて，用語関係図に使用されている用語を定義する用語構成規則を提案した．これによりディペンダビリティケースと用語関係図の相互変換をすることができる．その結果，用語関係図によって必要な用語の整理や抽出ができ，ディペンダビリティケースの記述を容易化できる．また，既存のディペンダビリティケースを用語関係図に変換し，ディペンダビリティケース用語の欠落や曖昧性等を評価することができる．

現在，用語関係図・ディペンダビリティケース間の自動生成ツールの作成を目指している．しかし，他の事例に対する用語関係図を分析していないため，用語関係図の妥当性や有用性を評価できていない．このため，他の事例に適用して，これらについて確認する必要がある．

以上をまとめると，生成規則や用語関係図について，以下の課題があることが分かった．

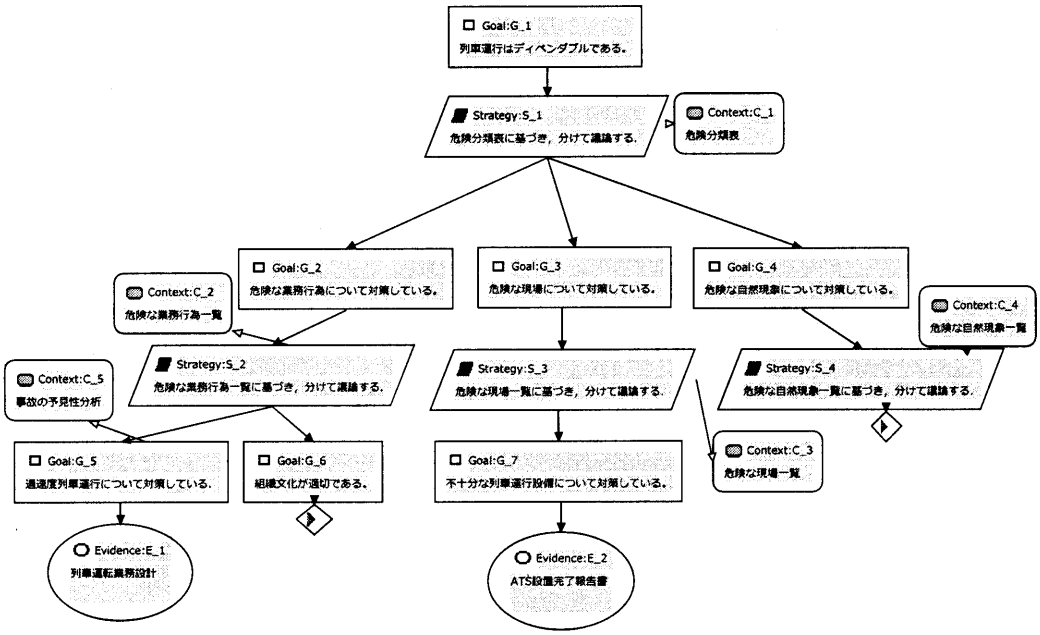
- 他システムでの用語関係図の適用
- W2D で生成したディペンダビリティケースのゴールノード増加における対処
- D2W で生成した用語関係図のノード欠落についての議論
- ゴールノード要素における positeve・negative 性の議論

謝　辞

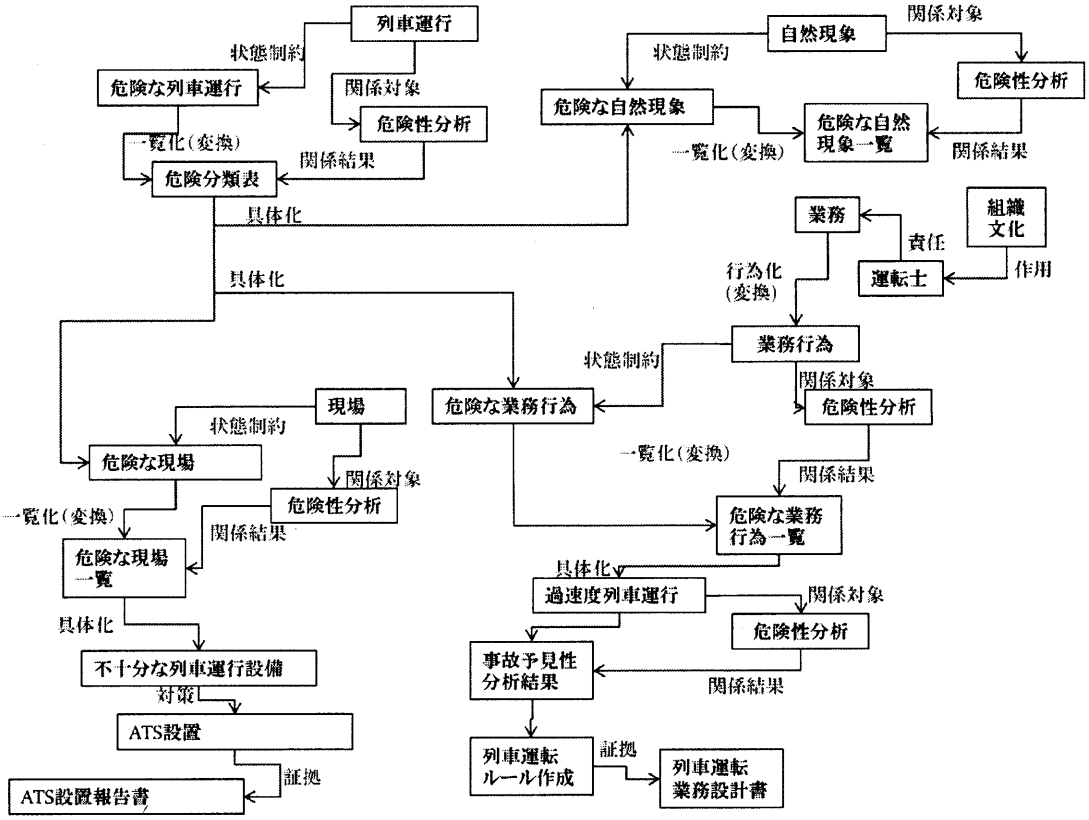
本研究は JST-CREST「実用化を目指した組み込みシステム用ディペンダブル・オペレーティングシステム」研究領域（DEOS プロジェクト）の支援を受けたものである．

文　献

[1] 松村昌典，松野　裕，山本修一郎，ディペンダビリティ用語辞書構築方法の提案，信学技報，vol. 112, no. 314, KBSE2012-57, pp. 115-120, 2012 年 11 月.
[2] DEOS プロジェクト http://www.crest-os.jst.go.jp
[3] D-Case Editor
http://www.dependable-os.net/tech/D-CaseEditor/
[4] Tim Kelly and Rob Weaver. The goal structuring notation - a safety argument notation. In Proc. of the Dependable Systems and Networks 2004, Workshop on Assurance Cases, 2004.
[5] 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



付図 1 W2D を行った結果のディペンダビリティケース



付図 2 D2W を行った結果の用語関係図