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
KBSE2012-57 (2012-11)

ディペンダビリティ用語辞書構築方法の提案

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の図式要素の名標ならびに名標間の関係を定義するための用語辞書については明確ではなかった．このため本稿ではディペンダビリティ用語辞書の構築方法を提案する．

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 method to construct a word dictionary 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, as dependability cases sometimes become huge and hard to maintain, it is useful to construct a word dictionary and relationship diagram used in dependability cases. In this paper, we propose a method to construct a word relationship diagram for 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分析する際，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，用語関係図を提案する．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．システムの要素間の関係を明確にすることで，ディペンダビリティケースの作成を容易化できる．本稿では，ディペンダビリティケースの図式要素の名標ならびに名標間の関係を定義するためのディペンダビリティ用語辞書の構築方法を提案する．

本稿の構成は以下のとおりである．2節において，用語関係図を説明する．3節において，ディペンダビリティケースから用語関係図への作成方法を説明する．4節において，用語関係図の適用例を紹介する．5・6節においては，作成した用語関係図の分析結果を記述している．7章では用語関係図とディペンダビリティケースについて考察する．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名標ならびに名標間の関係を定義する．その結果，用語関係を用いることにより，ディペンダビリティケースの作成を容易化できる．

用語関係図を構成する要素は以下の 3 つである.

- ノード
- 関係名
- 矢印

システム内の人，物，活動等の書かれたノードに対し，ノード間に関係があれば矢印を書き，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．関係名は接続されている 2 つのノードに関する動作であり，ノードは動作対象になる．ノードと関係名で文を構成すると，名詞と動詞の関係になる.

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.

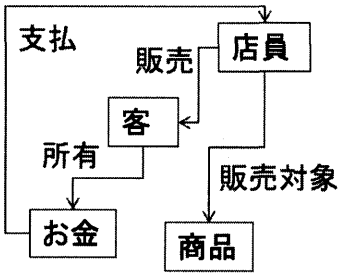

図 1　商品売買システムの用語関係図の例

3. ディペンダビリティケースから用語関係図への作成方法

ディペンダビリティケースから用語関係図の作成方法を以下に記述する.

(1) ディペンダビリティケースのコンテクスト，エビデンス，ゴール，ストラテジの順で，以下の示す分析 (ノード名分析) を行う.

(1.1) 記述されている用語を抽出する.

(1.2) ディペンダビリティケースに記述されていないが，システムにおいて重要な用語があれば追加する.

(1.3) 記述した用語に対し用語間の関係を吟味する.

(1.4) 図式化する.

(2) 図の中に同じノードがあればを結合する.

(3) 結合したノード間に複数の同じ関係名の付いている矢印があれば一つにする.

4. 適　用　例

以下では，列車運行システムのディペンダビリティケースに対して作成した用語関係図を説明する.

4.1 列車運行システムのディペンダビリティケース

列車運行システムのディペンダビリティケースは付録:図 A·1 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.

4.2 ディペンダビリティケースから用語関係図を作成する例

列車運行システムのディペンダビリティケースから用語関係図を作成した例を説明する．3 章で述べた手順でノード名分析を行った．その分析と結果を示す.

なお以下では，用語関係図の要素を「ノード"危険分類表"・関係名"具体化"」のように，ディペンダビリティケースの要素を「ノード C1」のように記述する.

- コンテクストノード名分析

コンテクストノードに記述されているものは，主に設計書・分析結果である．それには分析対象が存在する．コンテクストのノード名分析では，分析対象との関係を明確に記述する.

危険分類表 (ノード C1) があることで，具体的な危険事象を知覚できる．そこで，危険分類表より，各危険事象への関係として関係名"具体化"と記述する．これは図 2 に示した.

また図 3(a) について，危険業務一覧 (ノード C2) を作成する際，業務行為について分析を行い，危険な業務行為を発見する必要がある．よってノード"業務行為"に対し，関係名"分析対象"，関係名"危険分析"があり，関係名"危険分析"とノード"危険な業務行為分析結果"を接続する．さらに，そこからノード"危険な業務行為一覧"を関係名"一覧化"で接続する．ノード C3，C4，C5 も関係名"分析対象"，"危険分析 (予見分析)"，"一覧化"を用いることで，コンテクスト内の重要な用語の関係性が明確にできる.

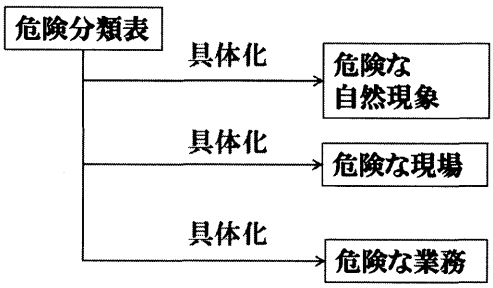

図 2　ディペンダビリティケースノード C1 のノード名分析結果

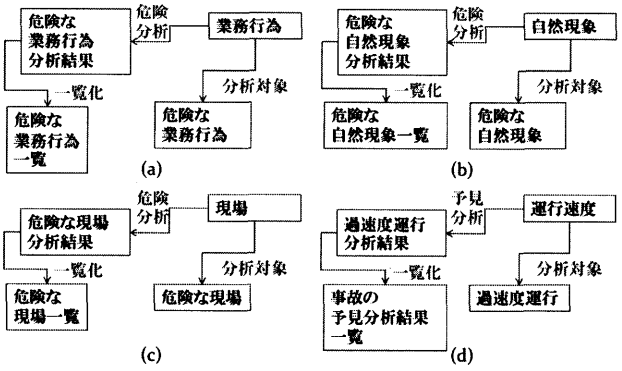

図 3　ディペンダビリティケースノード C2-C5 のノード名分析結果

- エビデンスノード名分析

エビデンスノードに記述されているものは，設計書・報告書である．危険分析を行うことで得られた対策を行っている証跡である．言い換えると，危険分析を行った結果からエビデンスが導かれる．そこで用語関係図では，エビデンス要素を危険分析結果一覧から関係名"対策"で接続する．

図 4(a) について，列車運転業務設計 (ノード Sn1) は，ノード"事故の予見分析結果一覧"から関係名"対策"で接続する．ノード Sn2 も同様の方法で記述できる．

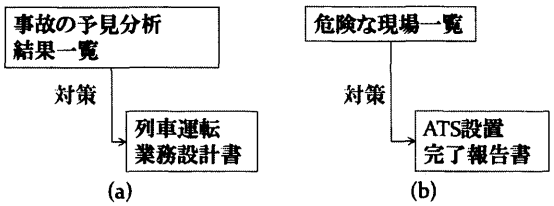

図 4　ディペンダビリティケースノード Sn1，Sn2 のノード名分析結果

- ゴールノード名分析

ゴールノードに記述されているものは，満たすべき主張である．これは，主張に対して満たすかどうかを分析する対象となっている．つまりゴールに該当する用語関係図ノードは関係名"分析対象"を接続するべきである．

また，ディペンダビリティケースでは，ゴールノードを段階的詳細化することによって，サブゴールに分割される．同様に用語関係図も，ゴール要素ノードとサブゴール要素ノードを接続する．

ディペンダビリティケースでの列車運行業務は，3 つの要素 (自然現象，現場状況，業務行為) が影響するため，用語関係図も関係名"自然環境"，"活動"でそれぞれの要素を接続する．「業務危険行為について対策をしている．(ノード G2)」に該当するノード"危険な業務"から，サブゴールである「過速度運行に対処している。(ノード G5)」に該当するノード"過速度運行"を関係名"分析対象"で接続する．これは図 5 に示している．

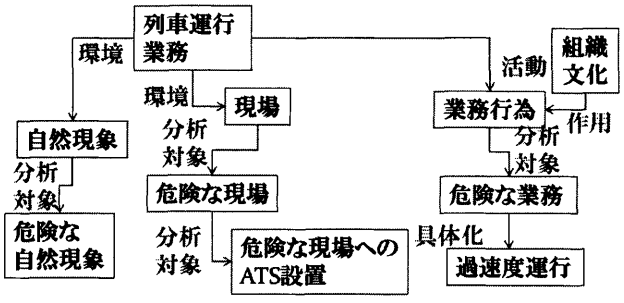

図 5　ディペンダビリティケースのゴールノード名分析結果

- ストラテジノード名分析

省略記述をしていないディペンダビリティケースのストラテジは，エビデンスのみ接続される．つまり各ストラテジには必ず被分解ゴールとの対応関係がある．一方，列車運行システムのディペンダビリティケースでは，対応関係にあるゴールとストラテジに同じ用語が含まれる．よってストラテジノード名分析はゴールノード名分析と同じ図が記述できる．

- 4 つの図の結合

4 つの図を結合をして用語関係図を作成する．同じノードを結合し，複数存在する関係名を消去したことで，付録:図 A·2 を作成した．

5. 用語関係図の関係名一覧

列車運行システムの用語関係図で 9 種類の関係名で記述した．関係名は表 1 に説明している．

表 1　関係名一覧

関係名	意味	例
一覧化	分析結果 A とそれをまとめた資料 B との関係	危険性分析→ (一覧化) 危険な自然現象一覧
危険分析	ある用語 A における危険に対し，分析を行うという関係	自然現象→ (危険分析) 危険な自然現象 分析結果
予見分析	ある用語 A における予見に対し，分析を行うという関係	運行速度→ (予見分析) 過速度運行分析結果
分析対象	ある用語 A と，その中で分析する要素 B との関係	自然現象→ (分析対象) 危険な自然現象
自然環境	ある用語 A と，確認すべき環境状況 B との関係	列車運行業務→ (自然環境) 自然現象
活動	ある用語 A と，確認すべき活動状況 B との関係	列車運行業務→ (活動) 業務行為
作用	ある用語 A と，それに影響を及ぼす用語 B との関係	組織文化→ (作用) 業務行為
具体化	ある用語 A と，その具体的な内容である用語 B との関係	危険な業務行為→ (具体化) 過速度運行
対策	ある用語 A に対するための必要な書類 B との関係	事故の予見分析結果一覧→ (対策) 列車運転業務設計書

6. 用語関係図の関係パターン分析

用語関係図を作成した結果，付録:図 A·2 のようになった．用語関係図を分析した結果を記述する．

付録:図 A·2 で規則正しい部分 (点線で囲っている部分) が存在する．この部分はすべて図 6 のような形をしている．この部分では，ある事象や人・物・活動等について危険分析を行うことにより，分析結果を作成している．これは，ディペンダビリティケースにおける，コンテクストに基づいて，ストラテジやサブゴールのコンテクストを記述する箇所と似通った性質をもっていることがわかる．用語関係図のこの部分を用いてディペンダビリティケースを作成することができる．

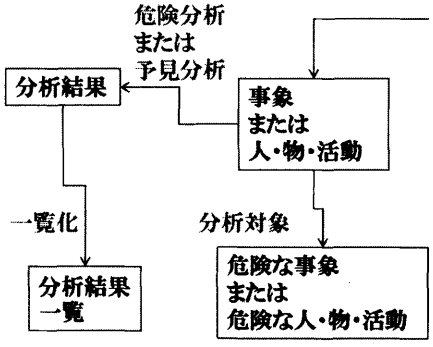

図 6　用語関係図の規則性

7. 用語関係図からディペンダビリティケースへの作成規則

用語関係図を分析することで，ディペンダビリティケースと類似する点が分かった．類似する箇所を吟味すること，用語関係図からディペンダビリティケースを作成する3つの作成規則についてそれぞれ記述する．

7.1 規則1:ゴール・ストラテジの作成規則

ディペンダビリティケースのゴールは，危険分析をした結果に基づいて，対策の証跡を記述する．用語関係図におけるディペンダビリティケースのゴール・ストラテジノードの該当箇所を探索するために，まず関係名"危険分析"，"予見分析"を見つける．そこから分析した対象を探索し，その部分が適当に対処されていれば，分析対象をもとに対策を施していることを保障したことになる．もし，ある分析対象がさらに分割・具体化されていれば，保障するべき要素も分割して議論するということであり，これはディペンダビリティケースのストラテジと類似している．以下は，ゴール・ストラテジの作成手順である．

1 トップゴールを定める．トップゴールと関係する用語のある用語関係図ノードA(以下，トップゴールノードと記述する)から用語A'を抽出し，「A'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 トップゴールノードAから関係名"危険分析"，"予見分析"を分割探索する．

3 関係名"危険分析"の矢印が出ているノードXから関係名"分析対象"を探し，矢印が示すノードBの用語B'を抽出する．

4 「B'について対策(実行)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ゴールとする．

5.1 ノードAの下位にノードBが接続されている場合は，4で作成したゴールの下に「B'の対策(実行)について議論する.」というストラテジを接続する．そのノードBから2から繰り返す．

5.2 ノードAの下位にノードが接続されていなければ，探索を終了する．

7.2 規則2:エビデンス・コンテクストの作成規則

用語関係図では，脅威に対する分析によって一覧化した分析結果に基づいて，対策の証跡を次のノードに記述している．よって，ここからディペンダビリティケースにおけるエビデンスとその上位にあるコンテクストを導出できる．また，脅威に対する分析を一覧化した資料は，その対策を講じるために必要となるため，この書類がコンテクストとなる．しかし，問題はコンテクストが接続される箇所である．コンテクストはトップゴールからエビデンス間にあるゴール・ストラテジノードの数ほどあり，適切なコンテクストの接続先を吟味することが必要である．コンテクスト要素が必要となるエビデンスにいちばん近いゴールまたはストラテジが理想的であるが，現在あまり明瞭でない．そこで用語関係図からディペンダビリティケースを作成する際，以下の考えのもとコンテクストの接続先を決定する．

ある事象に対し脅威が存在すると仮定する．脅威に対する分析を行い，その対策を講じる必要がある．そして一覧化した書類を作成しなければならない．コンテクストの作成に起因するゴールまたはストラテジに接続するべきである．つまり，以下は，コンテクスト・エビデンスの作成手順である．

1 トップゴールノードAから関係名"対象分析"，を分割探索する．

2 関係名"対象分析"の矢印が出ているノードXから，関係名"危険分析"，"予見分析"の矢印から走査し，関係名"対策"を発見する．

3 関係名"対策"の矢印が示しているノードCをコンテクストとする．

4 関係名"対策"の矢印を出しているノードEをエビデンスとする

5 関係名"対象分析"の矢印が指しているノードGから作成したストラテジ(またはゴール)に接続する．

7.3 規則3:アンデベロップの作成規則

アンデベロップとは接続されているゴールやストラテジを満たすためのストラテジやサブゴール，エビデンスが存在しない場合に使用する．用語関係図では，分析した結果一覧化した資料はあるもの，用語名"対策"が接続されていない場合は，アンデベロップを記述する．アンデベロップはディペンダビリティケースの葉に接続されるため，用語関係図の最下位の用語"対象分析"を検索することでわかる．以下は，アンデベロップの作成手順である．

1 トップゴールノードAから関係名"対象分析"を分割探索する．

2 関係名"対象分析"の矢印が出ているノードXから，関係名"危険分析"，"予見分析"の矢印から走査し，関係名"対策"を発見する．

3.1 関係名"対策"が発見できれば，矢印が示しているノードEをエビデンスとする．規則2の3へ．

3.2 関係名"対策"が発見できなければ，アンデベロップを作成する．

4 ノードXの関係名"対象分析"の矢印から走査し，その末端の用語に相当するゴールまたはストラテジに接続する．

7.4 作成規則の適用例

図A·3は，上記の手法で作成したディペンダビリティケースの図である．実際のディペンダビリティケースの各ノードの言葉は違うものの，意味はほとんど同じと考えてもよい．しかし比較の結果，大きく異なる箇所がある．それは以下の通りである．

- 「組織文化が適切である．(ノードG6)」以下が存在しない．
- 「危険な自然現象への対処について議論をする．(ノードS4)」が存在しない．

8. 考　　察

用語関係図からディペンダビリティケースを作成することで，ディペンダビリティケース内の用語間の関係を明確にすることができ，ディペンダビリティケース作成の容易化できる．しか

し以下のような課題がある．

8.1 他システムでの用語関係図の適応

本稿では，列車運行システムのディペンダビリティケースより用語関係図を作成し，さらにディペンダビリティケースに再変換して分析してみることを行ったことを記述している．しかし，列車運行システム以外のシステムについても同様な用語関係図を作成することができ，ディペンダビリティケース作成規則のもとに適切なディペンダビリティケースを作成することができることについては確認をしていない．そこで，他システムについて用語関係図を作成し，実際に本稿で記述している内容に相違がないか調査する必要がある．

8.2 関係名の種類分け

関係名には，用語が違うが用語関係図内での意味は等しく使用されるものがある．まだ関係名間の関係は明確になっていない．さまざまな用語関係図から関係名を抽出して調査する必要がある．

関係名の関係を明確にすることで，用語関係図の文法を構築することができ，用語関係図にさまざまな関係名を使用することができる．その結果，用語関係図を記述するだけでディペンダビリティケースを作成することができるようになると期待している．

8.3 用語関係図から作成したディペンダビリティケースのノード欠落の対処

用語関係図から作成したディペンダビリティケースには，ノードの欠落 (ノード G6，S4) を生じている箇所がある．以下に，推測される欠落を生じさせる原因推測を記述した．

- アンデベロップを接続する位置が作成規則で明確になっていない．
- "組織文化"への矢印がまだ存在するが，作成した用語関係図には記述されていない．

今後，組織文化への矢印の存在性を確認することによって，ディペンダビリティケースの作成方法は適切であるかどうか確認する必要がある．

8.4 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

本稿では，用語関係図からディペンダビリティケースへの作成規則を記述しているが，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は記述していない．そこで，今後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を明確にし，ディペンダビリティケースと用語関係図が相互変換できるようにする．

そうすることによって，システムの評価を多面的に見ることができ，システムにおける信頼性向上のための一つの手法を考える糸口となることを考える．

8.5 用語関係図の省略可能性の吟味

用語関係図はいくつか矢印が 1 つのノードに接続される可能性があるため，図は大きく複雑なものとなる．これでは用語関係図の有用性は低い．そこで用語関係図を作成する際，図の大きさや複雑さを軽減するために省略できる箇所が存在するかどうかを考え，どのように省略可能かを吟味する必要がある．

9. おわりに

本稿では用語関係図という図法を用いて，そこからディペンダビリティケースを作成するための補助となる関係名を抽出することを提案した．これによりディペンダビリティケースの作成を安易化できる．また，用語関係図からディペンダビリティケースを自動生成ツールの作成もできると推測している．しかし他システムに対しての用語関係図を現在分析していないため，他システムでも本稿の内容に適応できているかを確認して用語関係図の洗練化を進めていく必要がある．それに応じて以下の課題が存在することが分かった．

- 他システムでの用語関係図の適応
- 関係名の種類分け
- 用語関係図から作成したディペンダビリティケースのノード欠落の対処
- 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
- 用語関係図の省略可能性の吟味

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] DEOS プロジェクト http://www.crest-os.jst.go.jp
[2] D-Case Editor
http://www.dependable-os.net/tech/D-CaseEditor/
[3] 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.
[4] 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　録

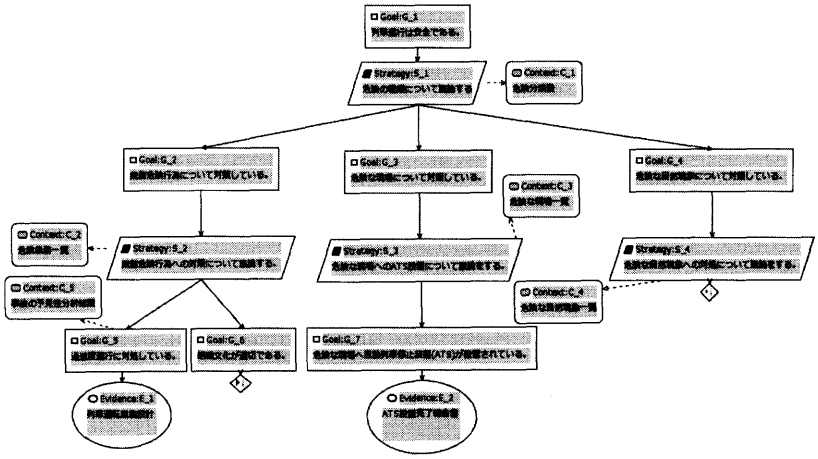

図 A·1　列車運行システムのディペンダビリティケース

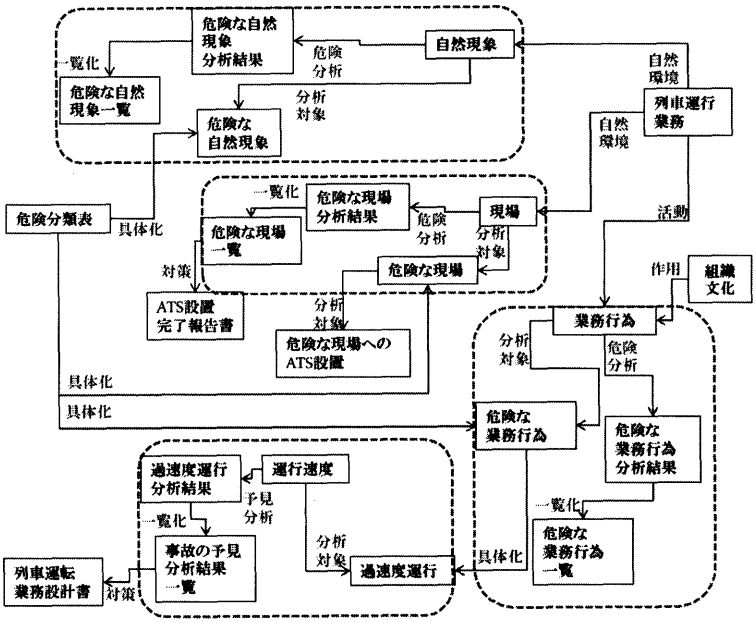

図 A·2　列車運行システムの用語関係図

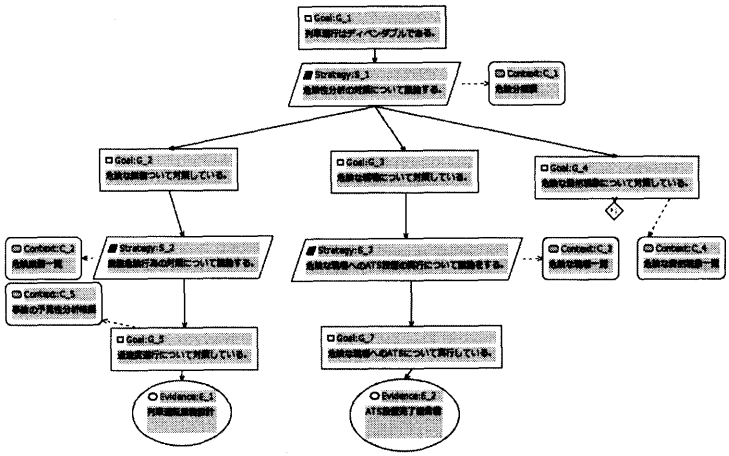

図 A·3　用語関係図からディペンダビリティケースに再変換した結果