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
KBSE2013-41 (2013-9)

# ゴール構文表を利用したディペンダビリティケースのゴール分析法について

松村　昌典†　山本修一郎††

† 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
†† 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, ††yamamotosui@icts.nagoya-u.ac.jp

**あらまし**　ディペンダビリティケースではゴール記述法が属人的であるため，理解や分析の効率が低下するという問題がある．この問題に対処するため，ゴール構文表により，ゴールを明確に記述する方法を提案している．本稿では，入退出管理システムのディペンダビリティケースのゴール文に対して，ゴール構文表を適用することにより，用語関係を抽出する実験を実施する．これにより，ゴール構文表を用いたゴール分析法の有効性について考察する．
**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，ゴール文の型，ゴール構文表

# Analysis method for the goals of dependability cases using goal syntax table

Masanori MATSUMURA† and Shuichiro YAMAMOTO††

† Graduate School of Information Science, 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, ††yamamotosui@icts.nagoya-u.ac.jp

**Abstract**　The efficiency of analysis and understanding of Dependability Case is reduced because we write goals in gross. To deal with this problem, we defined the method to clear the goals using Goal Syntax Table. In this paper, we describe the examination and the result to use Goal Syntax Table to the goal of Dependability Case of the access control system and the report the discussion of the efficiency of the goal analysis using Goal Syntax Table.
**Key words**　Dependability, Dependability Case, Type of Goals, Syntax table of Goals

## 1. はじめに

システムのディペンダビリティを保証し説明責任を果たすための手法の一つに，ディペンダビリティケース[1]（Dependability case，アシュアランケース[2]とも呼ぶ）がある．

ディペンダビリティケースのゴールは命題文として記述される．しかし，そのゴール文は記述者によって記述法が大きく異なり，また記述者が当然であると思っている内容を省略してゴール文を記述することにより，他者がゴール文の理解することが困難になるということがある．そこで，ディペンダビリティケースのゴール文を明確に記述するために，私たちはゴール構文表を用いる方法を提案している．しかし，ゴール構文表を用いることにより，「どの点においてゴール文が明確になるのか」，また「どのようなゴール文がゴール構文表で記述することが可能か」ということが明確でない問題がある．

本稿では，入退出管理システムのディペンダビリティケースのゴール文に対して，ゴール構文表を適用することにより，用語関係を抽出する実験を実施する．これにより，ゴール構文表を用いたゴール分析法の有効性について考察する．

本稿の構成は次のとおりである．2章では，ディペンダビリティケースを説明する．3章では，前回の発表で提案したゴール構文表を述べる．4章では，ゴール構文表を入退出管理システムのディペンダビリティケースのゴール文に適用して結果を述べる．5章では，考察を述べる．6章では，今後の課題を記述し，最後にまとめを述べる．

## 2. ディペンダビリティケース

アシュアランスケースは，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ディペンダビリティケースと呼ぶ．

Goal Structuring Notation（GSN）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．これらの表記法を用いて，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することで，トップゴールが満足されことを明確に確認できる．図 1 に，GSN で記述したディペンダビリティケースの例を示す．

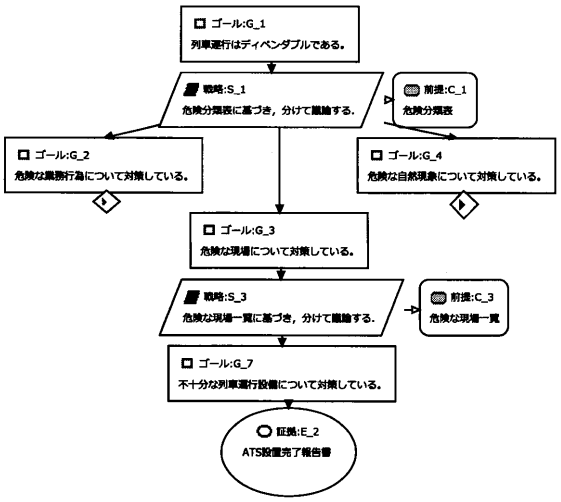


図 1　GSN で記述したディペンダビリティケースの例

ディペンダビリティのコンテクストやエビデンスは文書名などの複合名詞で記述される．またストラテジノードも「○○について分けて議論する」というように，記述パターンは定型化できる．一方ゴールの記述基本規則 [3] は，「主部，状態を示す述部が記述している肯定文の命題」のみであり，自由に記述することができる．そのため，ゴール記述法が属人的であり，理解や分析の効率が低下してしまう問題がある．

また，ディペンダビリティケースの別の問題として，対象システムの規模によりディペンダビリティケース記述に必要な工数が増加することに対し，再利用性を高める研究 [4] が行われている．ディペンダビリティケースの一部をモジュール化したものを利用する際は，利用者がその内容を理解するために，ノードに記述された文や語を明確にする必要がある．このため，ゴールを明確に記述する手法が必要である．

## 3. ゴール構文表

ディペンダビリティケースのゴール文を明確に記述するために，ゴール構文表を用いる．ゴール構文表は，ゴール構文 [5] を表で表したものである．ゴール構文表は，ゴール文を【原因】,【リスク】,【リスク対策・望ましい状態】と三部分に分け，さらにそれぞれを主部，条件部，述部に文を分解して記述する．【原因】には，リスク，リスク対策，望ましい状態に至る原因を記述する．【リスク】には，避けるべきエラーやエラー状態を記述する．【リスク対策・望ましい状態】には，リスクで記述した状態を避けたり，被害を軽減するための対策や仕様等で定義された望ましい状態等を記述する．また，主部述部には文の要素を分解し，また条件部には環境条件や制約条件等を記述する．

ゴール構文表を用いることによって，ゴールから抽出した用語に加え，省略された文の主部等を明確に記述することで，文の曖昧性を下げることができる．例えば，「作業中に電源ユニットは作業者の高温部への接触のリスクに対処できる．」というゴール文に対して，表 1 のように，記述できる．

表 1　ゴール構文表の例

| | 主部 | 条件部 | 述部 |
|---|---|---|---|
| 原因 | 作業者が | 作業中に | 高温部へ接触する |
| リスク | 作業者が | | 怪我をする |
| リスク対策<br>望ましい状態 | 電源ユニットが | | リスクに対処できている |

## 4. 実　　験

本稿では，ゴール構文表を用いたゴール分析法の有効性について考察するために，入退出管理システムのディペンダビリティケースのゴール文に対して，ゴール構文表を適用することにより，用語関係を抽出する実験を実施する．

### 4.1 方　　法

実験対象の各ゴール文から，以下の方法でゴール構文表を記述する．その際どのようなゴール構文表が記述できたか分析する．

（1） 複文であれば単文にする．

（2） ゴール文を【原因】,【リスク】,【リスク対策・望ましい状態】を示す部分へ分割する．

（3） 各部分に対し，主部，述部，条件部を明確にする．その方法は後述する．

（4） 各部分に対し，主部，述部，条件部をゴール構文表に記述する．

各部分に対し，主部，述部，条件部を明確にする方法として，以下のことを行う．

- 主部が明確でない，もしくは不足している場合は，対象としているゴールに対する上位ゴールの主部を補う．その方法でも明確に理解できない場合は，文脈から主部を推定する．

• 述部は (1) 状態のみ，(2) 活動のみ，(3) 活動状態に分けられるが，(2) はゴール文として不適切であるので，(2) に対してのみ，述部に「正しく」のような状態をを修飾する，述部とする．

• 条件部は環境条件，制約条件を句（主語と述語動詞を含まない複数の語と定義する）へ変換する．

例えば，「2 次記憶媒体が書き込まれている間に，停電が発生しても 2 次記憶媒体のファイルが破損することはないように設計している．」のようなゴール文に対して，【原因】：2 次記憶媒体が書き込まれている間に停電が発生する，【リスク】：2 次記憶媒体のファイルが破損する，【リスク対策・望ましい状態】：リスクを考慮した設計になっている，へ分割できる．次に，各部分の主部，述部，条件部を明確することで，ゴール構文表として図 2 のように，記述できる．【原因】を示している部分においては，条件部に相当する「2 次記憶媒体が書き込まれている間に」という部分が句ではないので，「2 次記憶媒体への書き込み中に」のように句に変換して記述した．また，主部が明確に記述されていない【リスク対策・望ましい状態】を示している部分においては，対象のゴール文に対する最近の上位ゴールの主部から補った．

表 2　実験方法で記述したゴール構文表の例

| | 主部 | 条件部 | 述部 |
|---|---|---|---|
| 原因 | 停電が | 2 次記憶媒体への書き込み中に | 発生する |
| リスク | 2 次記憶媒体のファイルが | | 破損する |
| リスク対策 望ましい状態 | ソフトとハードのインターフェースが | | リスクを考慮した設計になっている |

### 4.2 対　　象

実験対象である入退出管理システムは，IC カードリーダ，サーバ，データベース（DB）から構成されている．システム構成を図 2 に示す．このシステムは社員管理を想定しており，社員の持つ IC カードのある端末を IC カードリーダにかざすことで入退出管理システムがユーザ PC，管理者 PC へメッセージを送信する仕組みである．ディペンダビリティケースの各ノード数を表 3 に示す．

実験対象のディペンダビリティケースは，ある機能に対し入力，処理，出力がディペンダブルであることを示すような形式である「完全分解パターン」をとって議論展開を記述している [6]．またリスクに対する内容をゴールに記述していないため，比較的ディペンダビリティケースが単純であり，ゴール 1 つに対する文の量も少ない．

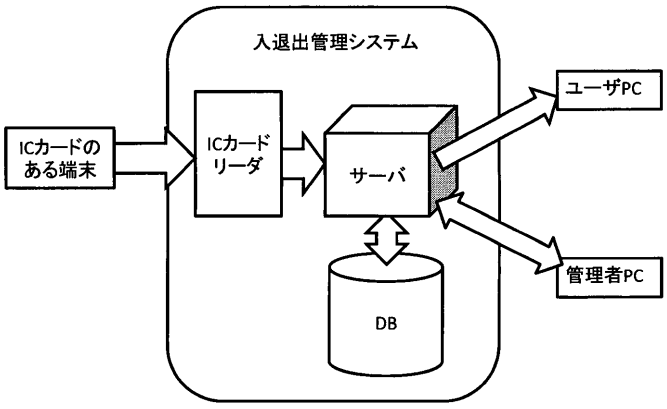


図 2　入退出管理システムのシステム構成図

表 3　入退出管理システムのディペンダビリティケースの各ノード数

| ノードの種類 | ノード数 |
|---|---|
| ゴール | 278 |
| ストラテジー | 115 |
| コンテクスト | 30 |
| エビデンス | 143 |
| 合計 | 566 |

### 4.3 結　　果

実験した結果は以下の通りである．

• ゴール全 278 個から 279 個のゴール構文表を生成した．

• 主部を補完したゴール構文表が 139 個 (全 279 個中，約 50%) 存在した．

• 主部を補完した 139 個のゴールで上位ゴールの主部を補完した．

• 上位ゴールの主部を補完する方法では不適切なゴールは存在しなかった．

• 複文で記述された以下のゴールが 1 個存在した．

「DB に入退出情報の書き込みを行い，処理結果を受け取ることができる．」

• どのゴール構文表においても，【原因】，【リスク対策・望ましい状態】示している部分が記述されていない．

• すべてのゴールからゴール構文表を生成できた．

## 5. 考　　察

### 5.1 システム知識不足による主部補完の困難性

今回の実験では，各部分に対して主部は，対象ゴールに対する最近の上位ゴールの主部としたが，提案した方法で誰もが同じゴール構文表を記述できるとはいえない．

例えば，ディペンダビリティケースの一部を図 3 に示す．ゴール G1.1.2.1 について，表 4 に示すようなゴール構文表が記述できるが，上位ゴール G1.1.2 から補完した主部「社員情報の入力」を「社員情報の入力処理」のことであると気づけば，適切に上位ゴールから主部を補完できる．しかし，システム知識が省略されることによって，そのシステム知識が不足している人がディペンダビリティケースを読むと，理解ができないという場合がある．ディペンダビリティケースの記述者は，どのよ

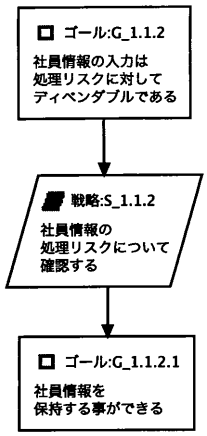


図 3　主語補完対象のディペンダビリティケースの一部

うなモジュールがどのような機能を持つことが理解できている前提で記述しているため，主部を省略している場合がしばしばある．そのために，他人が記述したディペンダビリティケースは主語等を補いながら読む必要があり，時には，上記のように理解できない場合や，誤った理解をする可能性がある．

表 4　ゴール G1.1.2.1 から記述したゴール構文表

| | 主部 | 条件部 | 述部 |
|---|---|---|---|
| 原因 | | | |
| リスク | | | |
| リスク対策<br>望ましい状態 | 社員情報の入力処理が | | 社員情報を保持可能である |

### 5.2　主部や述部の記述における曖昧性

図 3 のディペンダビリティケースにおいて，ゴール G1.1.2 と，ゴール G1.1.2.1 では，「社員情報」という用語が出てくる部位が異なる．ゴール G1.1.2 では主部の一部として存在するが，一方ゴール G1.1.2.1 では，述部の一部に存在する．このように，同じ用語が文構成の異なりによって，異なる部位に存在することは，ゴール文の読解を困難にする原因の一つだと考えられる．そのために，主部や述部にルールを設けることが必要である．

### 5.3　【原因】,【リスク対策・望ましい状態】について

今回の実験では，一つも【原因】,【リスク対策・望ましい状態】が存在しなかった．この理由として，このディペンダビリティケースの記述方法が，リスクはコンテクストに，リスク対策はゴールに記述するように完全にリスク部分とリスク対策部分を分離して記述していたためである．このようなディペンダビリティケースの一部を図 4 に示す．

この記述方法は，リスク記述が上位ゴールのコンテクストに記述されているため，下位ゴールとそのコンテクストを参照しながら読む必要があるが，比較的に他者がディペンダビリティケースを理解し易くなると推測できる．

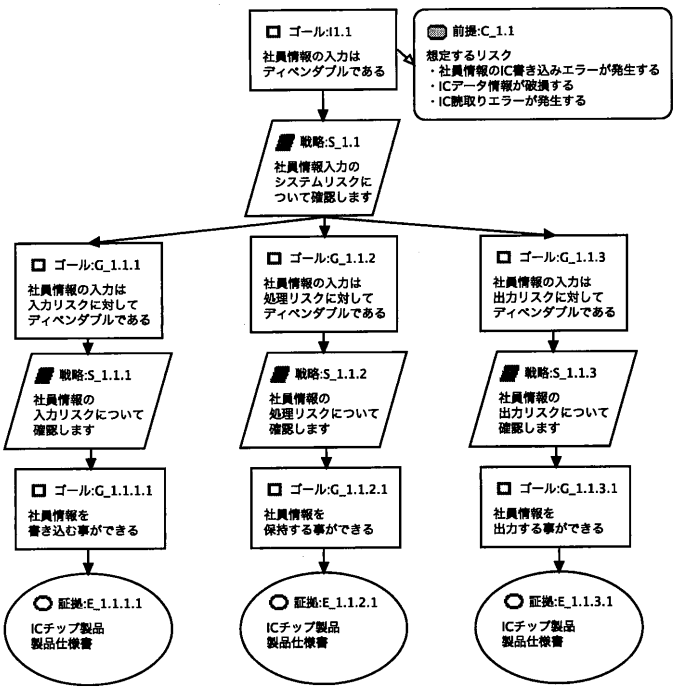


図 4　リスク部分とリスク対策部分を分離して記述している例

### 5.4　ゴール構文表の有用性

ゴール構文表ではゴールの用語について明確になり，ゴールの理解度を上げることができる．しかし，今回のように既存のディペンダビリティケースからゴール構文表をシステム知識のない第 3 者が記述すると，省略された用語を補う必要があり，そこで誤る可能性がある．そのために，ディペンダビリティケースを記述する際に，ゴールをゴール構文表で記述することによって，どのような人でも理解できるディペンダビリティケースになることが期待できる．

また，ゴール構文表を記述することにより，ゴール文の各用語との用語関係が明確になる．どのようなエラー状態に陥るかどうかを【リスク】を示す部分に記述し，それに基づいたリスク対策を【リスク対策・望ましい状態】を示す部分に記述することによって，リスクとそのリスク対策との関係が適切か正しい判断し易くなる．

また，ゴールの記述基本規則に従っていない以下のようなゴールに対しては，ゴール構文表を用いて明確に記述することを行う必要がある．

- 主部と述部が不明確であるゴール
- ゴールが文で記述されていないゴール（複合名詞で記述しているゴール等)

## 6.　今後の課題

### 6.1　ゴール構文表を用いたディペンダビリティケースの記述

5.3 節で述べた通り，ディペンダビリティケースのゴール文を読むためには，省略された用語があれば補う必要がある．そのため，始めからゴール構文表を用いてディペンダビリティケースを記述すれば，用語の曖昧性が軽減される．

ゴールの理解度を高めるために，主部や述部にルールを設け

て記述することを考える必要がある．例えば，以下のようなルールを設けることによって，ディペンダビリティケースの理解度が向上する．

（1） 主部はシステム構成に関わるモジュールやサブシステムといったオブジェクトに制限する

（2） 述部には「送信ができる」「送信可能である」「送信状態である」のような様々な記述方法を統一することなどのルールを設ける

また，ゴール構文表の各要素を詳細化していく過程で徐々に埋めていくといったディペンダビリティケースの記述法を考えることができる．

### 6.2 ゴール構文表を記述できるゴールとできないゴールとの境界の明確化

今回の実験では，すべてのゴールからそれぞれゴール構文表を記述できた．しかし，「どのゴールがゴール構文表で記述できるか」が明確でない．そのため，同様な実験を今後も続けていく必要がある．筆者らは同様に別のシステムのディペンダビリティケースで適用実験を進めているが，現在のところゴール構文表が記述できないゴールは 5.3 節で述べたような数個のゴールしか存在しない．

『ゴール構文表に記述できない』ということは，『対象ゴールは記述内容が明確でなく，システム知識を持っていない第 3 者は理解困難なものになっている』ということと捉えることができる．『ゴール構文表に変換できなければ，ゴール文を書き換えるべき』というゴール文における一つの評価として考えることができ，そのためゴール構文表が記述できるゴールと記述できないゴールの境界を明確することが必要になり，記述できないゴールが 5.3 節で述べたようなゴールのみであるかを確認すべきである．

### 6.3 ゴール構文表とディペンダビリティケースの用語関係図との関係の明確化

筆者らはディペンダビリティケースから抽出した用語や用語関係を定義するための手法として，ディペンダビリティケースに用語関係図 [7] [8] [9] を用いることを提案している．この手法を用いることによってディペンダビリティケースのノードに記述されている用語や用語関係を明確にすることができる．ディペンダビリティケースの記述内容を誰でも明確に理解するために，この手法とゴールを明確に記述することができるゴール構文表との関係を明確にし，ゴール構文表で抽出したゴール文の用語を用語関係図を用いて，用語や用語関係を定義する必要がある．そのためには，ゴール構文表や他ノードの記述内容や関係から用語関係図へ変換する規則を提案する必要がある．

## 7. おわりに

本稿では，入退出管理システムのディペンダビリティケースのゴール文に対して，ゴール構文表を適用することにより，用語関係を抽出する実験を実施し，ゴール構文表を用いたゴール分析法の有効性について考察した．この実験結果や考察から以下を明らかにした．

1） ゴール文からゴール構文表に記述すると，各部の主語を上位ゴールから補完できた．

2） リスクはコンテクストに，リスク対策はゴールに記述するような，完全にリスク部分とリスク対策部分を分離して記述したディペンダビリティケースの記述方法においては，他者がディペンダビリティケースを理解し易くなると考えられる．

3） すべてのゴールからゴール構文表を生成できた．

また，上記で述べたように以下のような課題を解決する必要がある．

- ゴール構文表を用いたディペンダビリティケースの記述
- ゴール構文表を記述できるゴールとできないゴールとの境界の明確化
- ゴール構文表とディペンダビリティケースの用語関係図との関係の明確化

## 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] 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.

[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] 松野 裕, 山本修一郎, アシュアランスケースのプログラミング言語技術の適用, 信学技報, vol. 112, no. 496, KBSE2012-81, pp. 73-78, 2013 年 3 月.

[5] 松村昌典, 山本修一郎, ディペンダビリティケースからの用語抽出実験についての考察, 信学技報, vol. 113, no. 71, KBSE2013-05, pp. 37-42, 2013 年 5 月.

[6] 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, KBSE2012-80, pp. 67-72, 2013 年 3 月.

[7] 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.

[8] 松村昌典, 松野 裕, 山本修一郎, ディペンダビリティケース用語構成規則の提案, 信学技報, vol. 112, no. 419, KBSE2012-63, pp. 29-34, 2013 年 1 月.

[9] 松村昌典, 松野 裕, 山本修一郎, ディペンダビリティケース用語構成規則の適用評価, 信学技報, vol. 112, no. 496, KBSE2012-79, pp. 61-66, 2013 年 3 月.

[10] DEOS プロジェクト http://www.crest-os.jst.go.jp

[11] D-Case Editor http://www.dependable-os.net/tech/D-CaseEditor/

[12] 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