論文の内容の要旨

氏名：越　山　　勉
博士の専攻分野の名称：博士（工学）
論文題名：記述者視点に基づく GSN のパターン分類によるセーフティケース記述の容易化に関する研究

本研究はセーフティケース記述の容易化に関する研究である。セーフティケースの表記法として GSN（Goal Structuring Notation）と呼ばれるグラフィカルな表記法を用い、GSN で記述されたセーフティケースを記述者の観点からパターン化することによりセーフティケース記述を容易化することを目的としている。セーフティケースとは高度な安全性が求められるシステムや製造物について、それらを使用するユーザや認証機関に対し、達成されている安全性について示すための文書のことである。セーフティケースは、近年自動車業界においても重要視されてきており、機能安全における国際規格や、最近の自動運転技術の開発においても、その必要性が増している。セーフティケースは、可視的かつ階層、構造的に表現がなされることが求められており、GSN が表記法として普及しつつある。

一方で、実際のシステムや製造物に対して用意されたセーフティケースを目にすることは稀であり、特に日本企業においては普及が進んでいない。そのためセーフティケースをどのように記述するべきなのか、基本的な段階から広く受け入れられる手法は現在も存在していないと考える。

そこで、本研究では、セーフティケースの記述の容易化をするために、GSN を用いた 6 種類へのパターンを提案した。さらに、それらについて論文等に挙がっている GSN サンプルとの比較を行い、これらパターンの妥当性及び可用性について評価した。また、ワークショップを開催し、これらパターンを用いて、GSN を読み取る、又は作成することを、技術者を対象に演習として実施し、パターンの有効性について評価した。

第１章　序論

本研究の背景と目的、本論文の構成などを示した。高い安全性が求められるシステムの開発運用においてセーフティケースが求められていることを背景として示し、セーフティケースを、GSN を用いて容易に記述することを目的とし、そのために記述者の視点に基づいた GSN のパターンを提案することを示した。

第２章　GSN の基本構造について

GSN の文法および木構造における論理展開についての検討を行った。GSN において論理的な説明の展開を記述者視点で構造的に構成しようとする場合、主張同士の関係を捉えることが重要である。また、GSN で用いられる部品のうちストラテジによって、枝分かれするゴールの構成についての指針を示すことに加え、主張の変換を含む場合があることに着目した。本研究では従来研究とは異なり、ゴールに加えてストラテジにも着目し、それらに含まれる主張同士の関係性を捉えることをパターン分類に先立っての構造解釈の方針として示した。

第３章　GSN のパターン分類

本研究では、主張同士の関係に着目した 6 個の GSN パターンの定義、提案を行った。本章で 6 個のパターンの分類に至った過程についてと、それぞれの違いを識別する着眼点について整理した。

また、それぞれのパターンが持つ特徴についての分析を行った。それらは主張としての親ゴールから子ゴールへの関係、子ゴール同士の関係によって分類されており、記述者の視点に基づいている。子ゴールの主張の達成から親ゴールの主張の達成を導く関係においては“必要条件もしくは十分条件”、“演繹的もしくは帰納的”、“強めている、もしくは弱めている”といった特徴についてパターン間における違いを見出した。

本章では、6 パターンについては以下のように定義、分類を行った。

(a)部分選択

親ゴールの主張に対して、部分的な要素として子ゴールの主張が置かれるパターンである。子ゴールの主張は、親ゴールの主張に対して網羅性はないが、親ゴールの主張を示すのに妥当、かつ受容できると見なす記述者の意図があるものとして作成されている。

(b)二重否定

親ゴールの主張に対して、二重否定の関係としての子ゴールの主張への置き換えであり、置き換え前後は等価な関係である。“安全である”を説明することは難しいが、“危険がない”ことを説明することが容易な場合などにおいて、このような変換が使われると考えられる。

(c)基準化

子ゴールの主張が、親ゴールの主張を包括する、より厳しい基準とされる場合のパターンである。記述者にとって、より明示し易い基準への置き換えや、判断が曖昧な場合において、それらの判断を行う際に明確になるようにするための置き換えを示している。

(d)視点変換

“設計の確実さがある”といった親ゴールの主張に対して子ゴールの主張として“ソースコードレビュで確認する”といった場合のように説明のアプローチとしての視点の置き換えを行っているパターンである。

(e)合わせ技

(d)と同様に視点の置き換えであるが、複数の子ゴールの主張によって構成されるパターンである。子ゴールの主張同士の内容は“通常時の動作”と“非常時の動作補償”のように、副となる側が主となる側の脆弱な要素を補う関係や、“設計上における技術的な確認”と“品質管理”のような、それぞれが別の側面の視点同士を相互に組み合わせている場合を指す。

(f)MECE

構造的な関係や、一連の工程や、プロセスといった、全体としての構成が明確である場合に、その各部分を子の主張に分解された形態である場合を指す。漏れなく重複がない関係より、MECE（Mutually Exclusive、Collectively Exhaustive）と呼称する。

第４章　GSN のパターンマッチング

インターネット上で公開、入手が可能な論文に挙がっている GSN についてパターンマッチングを行った。89 個の論文、271 の GSN 図を対象として、パターン数 717 個所についてのマッチングを行い、それらの全てにおいて、6 パターンのいずれかに当てはまることが確認され、6 パターンの可用性が示された。

一方で、パターン(b)(f)以外は、等価でない、なんらかの変換や置き換えがなされていると見なされるが、調査したパターンの 2/3 以上が、パターン(b)(f)以外であった。このことは、記述者による GSN の構成を用いた説明においては、暗黙のうちに何かしらの変換や基準化が行われていることを意味する。また、そのことは GSN 上での階層間の関係は、決して等価である必要性はなく、抽象的な性質（安全性など）の対象について、説明、論証する上では、変換や基準化が行われることが必然的なものであるといったことを傾向として読み取ることができた。

第５章　ワークショップによる検証

ワークショップは、2 回実施した。1 回目は特定企業の SE、2 回目は一般公募として参加を募った。参加者は共に 11 名であり、実施時間は 3 時間程度である。内容は、6 パターンの考え方の説明を行った上で、演習として参加者により 6 パターンを用いての GSN 作成をする構成にした。演習の課題では、全参加者に対して同じトップゴール（最上位の親ゴールの主張）が与えられ、各参加者それぞれが、それ以下の階層を記述したが、記述された GSN モデルは参加者ごとに異なった。結果的に 6 パターンすべてが参加者により作成された GSN モデルに含まれていた。このことは 6 つのパターンが、記述者（参加者）の視点の違いに対応していることが示唆される。参加者の中には GSN についての知見がない人も含まれていたが、短時間の実施の間に実際に GSN の作成を行うことができるようになるまでに GSN についての習得ができたことは、本ワークショップ、及び 6 パターンのアプローチが GSN 初心者にとっても有効であることを示唆している。ワークショップは新型コロナウィルスの影響により、リモートによる実施として行う必要があった。そのためリモート環境においても効率的に実施するため

の工夫とツールの選定を行った。

第６章　既存研究における分類と考察

既存研究における分類との比較を行った。6 パターンの分類の幾つかは既存研究における特徴の考え方を包含していることが確認された。さらに本研究における 6 パターンの分類は、実際の GSN モデルの調査の結果を踏まえていることにより、実際に存在する GSN モデルの特徴に即したパターンとしていることが明確になった。また木構造を持つ議論構造の考え方についての既存研究において、機構上の冗長性の設計思想の 1-out-of-2 と対比されているものがあり、GSN モデルを用いた表現と 1-out-of-2 との比較および考察を行った。

第７章　冗長機構への適用の検証

冗長機構における機構構成と、その機構における安全性の主張のそれぞれについて、機構上の設計表現と GSN による表現のそれぞれの可用性についての考察を行った。また、相互を組み合わせて表現する試行として自動運転機能を題材とした適用事例を示した。

第８章　結論

GSN モデルの記述を容易にするための 6 個の GSN モデルの提案を行った。既存の GSN モデルに対してパターンマッチングを行った。既存の分類をカバーできていることに加え、6 パターンが実際の GSN サンプルの特徴に一致した、より実際的なものであることを確認した。またワークショップにおいて参加者が GSN を作成する演習を行い、これらパターンの考え方が、GSN を容易に作成することに貢献できることを示した。冗長性を持つ安全機構との関連性について、それらの安全性について GSN を用いて説明する場合の考察を事例の作成と共に行った。今後、産業界でのセーフティケースの実例の調査をさらに実施し、ワークショップを開催することにより、本研究の成果が産業界で用いられることが期待される。