CBCS 安全要求の適用性向上に向けた可視化の取り組み

柿本 和希[1] 川口 真司[2] 高井 利憲[1] 石濱 直樹[2] 飯田 元[1] 片平 真史[2]

Visualization of CBCS safety requirement to optimize the use of CBCS safety requirement

KAKIMOTO Kazuki KAWAGUCHI Shinji TAKAI Toshinori
ISHIHAMA Naoki IIDA Hajimu KATAHIRA Masafumi

ねらい 本研究では，JAXA における安全審査業務の効率化のため，CBCS 安全要求に含まれる暗黙知を明確化することを目的としている．

キーワード 一般安全要求，CBCS 安全要求，ISS, Goal Structuring Notation

Target: This paper makes a implementation of CBCS safety requirements explicit to optimize safety review.

Keywords: General Safety Requirements, CBCS safety requirements, ISS, Goal Structuring Notation

1. はじめに

安全性にかかわるシステムの開発において，開発者はシステム固有の安全要求の他に，特定分野のシステムに対して汎用的に適用されるような規格や安全要求を考慮して開発を行う必要がある．それらの多くは汎用性を高めるために抽象的に記述されており，開発者の知識や経験によってその解釈は様々である．

Holloway ら [1] は GSN という安全性に関する議論を可視化する記法を用いて，航空機向け組み込みソフトウェア規格である DO-178C [2] に含まれる暗黙的な記述の可視化を行った．しかし彼らは評価実験を行っておらず，GSN を用いて規格を可視化する効果については明らかにされていない．

そこで本研究では，GSN を用いて，宇宙分野で利用される汎用的な安全要求の一つである CBCS 安全要求 [3] に含まれる暗黙的な情報の可視化を行い，評価実験を通じてその有効性を示す．

2. 背景

2.1. CBCS 安全要求

CBCS 安全要求とは ISS 建造にあたって NASA が定めた安全要求の一つであり，ISS に関連するコンピュータを用いた制御機能を含むシステムに対して適用される．また CBCS 安全要求の適用されるシステムの開発において，開発者はシステムが CBCS 安全要求を満たすことを保証しなければならない．

2.2. Goal Structuring Notation (GSN)

GSN とは Kelly ら [4] によって提唱された，安全性に関する議論を可視化するための記法である．

GSN では，システムが満たすべき抽象的な要求をトップゴール（主張）とし，それらがストラテジ（観点）によってより具体的なサブゴールに分割される．ゴールの分割を繰り返すことで依存関係が可視化され，末端のサブゴールがそれぞれソリューション（証拠）によって保証されることでトップゴールが満たされることを保証する．

3. CBCS 安全要求適用の問題点

CBCS 安全要求は ISS 関連のシステムに広く適用されることを想定し，自然言語によって抽象的に記述されている．そのため安全要求の適用には抽象的に記述された条文において，実際にはどのようなことが求められているのかを解釈しなければならない．しかし開発者の知識や経験によって条文の解釈には幅が生じてしまい，また過去の開発において行われた解釈自体が CBCS 安全要求を理解する上での暗黙知として存在している．条文の意図から外れた解釈は危険性の見過ごしに繋がる恐れがあり，危険であると言える．

4. GSN による CBCS 安全要求の記述

3 節で述べた問題点を解決するために，GSN を用いて CBCS 安全要求の抽象的に記述された条文を可視化した．可視化においては，CBCS 安全要求の各条文を GSN のトップゴールとして記述し，過去の開発における知見を元にそれらを分割した事項を実際に満たすべきサブゴールとして記述した．

5. 評価実験

本研究の有効性を確認するため，安全審査を想定した評価実験を行った．評価実験では，被験者となる

1 奈良先端科学技術大学院大学
Nara Institute of Science and Technology, Ikoma. Nara, Japan

2 宇宙航空研究開発機構
Japan Aerospace eXploration Agency, Tsukuba, Ibaraki, Japan

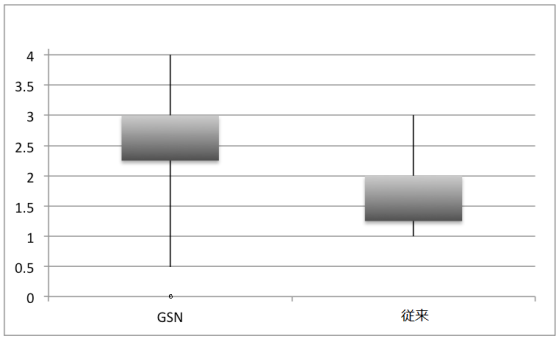

図 1 実験採点結果

Figure1 Experimental result

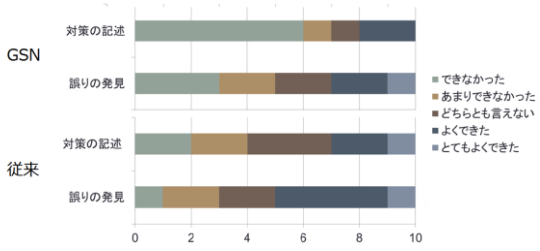

図 2 アンケート結果

Figure2 Result of questionnaire

JAXA 職員 20 名を，GSN によって記述した CBCS 安全要求を用いたグループと，従来の CBCS 安全要求のみを用いたグループとの各 10 名ずつのグループに分け，安全審査を想定した課題を解いていただき，客観的（適切に安全審査ができるか），主観的（適切に安全審査ができたと感じたか）の 2 つの側面の評価を収集した．

課題には HTV に関する公開された情報に基づき我々が作成したハザードレポートを用いた．ハザードレポートには意図的に誤りを含ませており，被験者にはハザードレポートが CBCS 安全要求に沿った内容であるかを審査し，条文と食い違っている場合には修正するよう指示した．またその後，課題への達成度に関するアンケート調査を行い定性的な評価の対象とした．

課題への回答は我々が 4 点満点で採点を行った．採点結果をグループごとに箱ひげ図で示したのが図 1 である．また採点結果に対して優位水準 5%で Welch の t 検定を行った結果，危険率 2.770…%で帰無仮説が棄却された．従って GSN によって記述された CBCS 安全要求を用いることで，安全審査の精度が上がると考えられる．また図 2 は，達成度に対するアンケート調査の結果である．アンケート結果から，従来の CBCS 安全要求を用いた場合の方が，課題を達成できたと感じた被験者が多かったことがわかる．

6. 考察

5 節の実験結果から，実際の正答数と被験者の自己評価がかい離していることがわかる．このことから我々は，GSN によって記述された安全要求を用いた場合と従来の安全要求を用いた場合のいずれか，またはその両方において開発者の自己評価と実際の結果がかい離していると考えた．そこで自己評価と実際の結果の関係について分析するため，達成度に関する質問への回答結果と正答数を用いてピアソンの積率相関係数（n = 10）を求めた（表 1）．

表 1 自己評価と正答数の相関

グループ	自己評価項目	正答数との相関係数
GSN	対策の記述	0.5459
	誤りの発見	0.6593
従来	対策の記述	-0.2516
	誤りの発見	0.1469

分析の結果から，GSN によって記述された CBCS 安全要求を用いたグループでは自己評価と実際の正答数に強い正の相関関係がみられる．一方，従来の CBCS 安全要求を用いたグループでは相関関係がみられない．

これら結果を実際の安全審査に置き換えると，GSN によって記述された CBCS 安全要求を用いた審査では開発者の実感と残存する対策の誤りや抜けに正の相関があると考えられるため，審査者が CBCS 安全要求を満たせていると考えた時点で十分に誤りや抜けが発見，修正されていると考えられる．しかし従来の CBCS 安全要求を用いた場合では，審査者が十分に満たせていると考えた時点でも，実際には多くの対策の誤りや抜けが存在していると考えられるため，非常に危険であると言える．

7. まとめ

本稿では GSN を用いて一般安全要求に含まれる暗黙的な記述を可視化することで，開発者への支援を行った．また作成した GSN に対する評価実験を行い，その有効性を示した．

8. 用語・文献

参考文献

[1] C. Michael Holloway (Feb. 2015): "Explicate '78: Discovering the Implicit Assurance Case in DO-178C", *23rd Safety-critical Systems Symposium*, 2-5 Bristol, UK.

[2] RTCA (2011a): Software Considerations in Airborne Systems and Equipment Certification. DO– 178C

[3] SSP 50038B (17 NOV 1995): Computer-Based Control System Safety Requirements –International Space Station

[4] Tim Kelly, John A McDermid(1997): Safety Case Construction and Reuse using Patterns,16th SAFECOMP

略号一覧

GSN: Goal-Structuring Notation, CBCS: Computer-Based Control System, ISS: International Space Station, HTV: H-II Transfer Vehicle