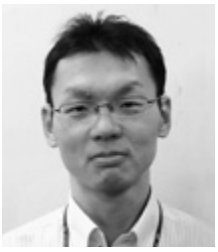
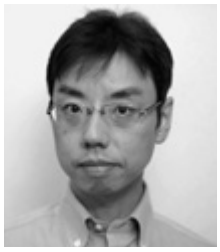
Goal Structuring Notationを用いた汎用的な安全要求の明確化と評価


柿本 和希[※1,a)] 川口 真司[※2,b)] 高井 利憲[※1] 石濱 直樹[※2,c)] 飯田 元[※1,d)] 片平 真史[※2,e)]

一般安全要求や安全に関する標準規格など，特定の分野のシステムに汎用的に適用される安全要求はあいまいな記述を含んでいる．あいまいな記述に対する解釈の誤りは要求の意図から外れた過不足のある設計につながるため，必要のないコストの増大や事故の原因となり得る．本研究では，汎用的な安全要求が暗黙的に仮定する知識などの暗黙知に着目し，それらを明確にすることにより，関係者の相互理解の促進やシステムの安全性の向上を目指した．具体的には，宇宙分野において用いられる，コンピュータによるハザード制御を行うシステムに対する安全要求（Computer Based Control System Safety Requirements，CBCS安全要求）を対象として明確化を行った．CBCS安全要求の明確化にはゴール構造化記法（Goal Structuring Notation，GSN）を用いた．更にその有効性を評価するため，宇宙航空研究開発機構の技術職員を対象とした比較評価実験を行った．実験の結果，一般安全要求の意図から外れた誤りの発見と訂正においてGSNによって正当の平均点が26%向上することを確認した．更に，GSN化によって思い込みによる危険性の見過ごしを防止する効果があることが確認できた．

Explication and evaluation of general safety requirements using GSN

Kazuki Kakimoto[※1], Shinji Kawaguchi[※2], Toshinori Takai[※1], Naoki Ishihama[※2], Hajimu Iida[※1], Masafumi Katahira[※2]

Safety requirements for a specific system domain, like general safety requirements and safety standards, tend to have obscure and ambiguous descriptions. Misinterpretations of them can cause excessively redundant or simply deficient safety design, which can be a trigger for cost escalation or an accident in the worst case scenario. In this research, we focus on implicit assumptions as a root of the ambiguousness mentioned above and propose a method to explicate an article in general safety requirements aiming for mutual understanding among stakeholders and improving system safety. The target of our research is Computer-Based Control System (CBCS) safety requirements, which are a safety standard for spacecraft systems, and the explication in our method is carried out by means of Goal Structuring Notation (GSN). In order to evaluate our proposal in a quantitative way, we performed a comparative experiment with the help of the Japan Aerospace eXploration Agency's engineers. The results of the experiment show that the average score for GSN-based CBCS safety requirements are 23% more effective in detecting and correcting errors in a given document on system safety than the average score for usual safety requirements written using natural language. Moreover, we conclude that GSN-based CBCS safety requirements can reduce misunderstandings among developers of a system and certifiers for safety.

※1　奈良先端科学技術大学院大学 情報科学研究科　Nara Institute of Science and Technology
※2　宇宙航空研究開発機構　Japan Aerospace eXploration Agency

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ほかに，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一般安全要求と呼ばれるものや，国際標準規格などの安全規格を考慮して開発を行い，定められた安全審査を受ける必要がある．一般安全要求や安全規格に準拠することにより保証を行うことや，審査を受けることはシステムが最低限の安全性を満たす客観的な証拠となるという点で重要である．

しかし，一般安全要求や安全規格の意図を理解した上で適切に安全性を審査することは困難である．その理由は大きく二つ存在する．一つめの理由は，審査活動にかかわる開発者及び審査者両方が持つ背景知識や経験に応じて解釈の深さが異なることである．例えば安全規格などでしばしば表れる「安全な状態」という表現をとっても，それを見るものが自動車組込みエンジニアか，航空機エンジニアかによって解釈が異なる．また経験の浅いエンジニアであればそもそも安全な状態が何かが分からない可能性もある．二つめの理由は，一般安全要求や安全規格は過去の設計や事故事例などの想定を踏まえて策定されていることである．評価対象システムを評価するには，これらの想定を理解した上で，評価対象システムでも同様の想定が成り立っているか，更には成り立っているとすればどの部分かを把握する必要がある．

一方，ゴール構造化記法（Goal Structuring Notation, GSN）[GSN2011]と呼ばれる記法を用いた安全性の保証が近年注目されている．従来の安全保証において，安全性に関する証拠が具体的にどのような安全性を保証しているのかはあいまいであった．しかしGSNを用いた安全保証においては，安全性にかかわる抽象度の高い主張が複数の具体的な主張に分解され，またそれらが客観的な証拠によって保証されることで，証拠が何を保証しているのかを明確にしている．

そこで本論文では，コンピュータによるハザード制御を行うシステムに対する安全要求（Computer Based Control System safety requirements，CBCS 安全要求）[NASA 1995]を対象にGSNを用いて明確化を行った．本研究における明確化とは，安全規格などにおける抽象度の高い条文が具体的にはどのような要求によって保証されるのかを明確にすることである．更にその明確化の試みが安全性の向上に有効かどうかを評価した．

以降，本論文は２節で背景を，３節でGSNを用いたCBCS安全要求の明確化の指針と実例について説明する．４節では評価実験の概要と結果を述べ，５節でその結果と限界について考察する．６節ではまとめとして，本論文の結論と今後の課題を述べる．

2　背景

2.1　Computer Based Control System安全要求

CBCS安全要求とは国際宇宙ステーション（International Space Station，ISS）の建造にあたってアメリカ航空宇宙局（National Aeronautics and Space Administration，NASA）が定めた一般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が義務付けられている．またCBCS安全要求の適用対象とな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NASAに対して保証しなければならない．実際に日本が設計及び開発を行ったきぼう（The Japanese Experiment Module, JEM）と，こうのとり（The H-2 Transfer Vehicle, HTV）の開発においても安全審査が行われ，NASAに対して安全性の保証を行った．

2.2　CBCS安全要求適用時の課題

CBCS安全要求はISSに関連する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CBCS安全要求を適用するには，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．しかし開発者や審査者の背景知識や経験によって，条文の解釈には幅が生じてしまう．また，過去の開発における解釈自体が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．背景知識や経験の違いによる解釈のずれは，条文の意図から外れた過不足ある設計につながるため，後の手戻りや事故の要因となり得る．

本研究では，CBCS安全要求におけるあいまいな記述がもたらす課題を以下の二つと考える．

課題１　条文を満たすために考慮する必要がある情報が，条文において明示されていない記述（読み取ることが難しい情報を暗黙的に仮定している記述）

課題２　条文の解釈がシステムに依存する記述

課題１及び２について実際の条文を用いて説明する．

CBCSは既知の安全な状態で起動する（箇条 3.1.1.1）

この条文は「システム起動時の初期化が完了した時点で既知の安全な状態であれば良い」と解釈することもできるという点であいまいである．しかし，本来の意図は「システムに電源を投入してから初期化を行っている間においても安全な状態を保つべき」という所にあり，安全審査においても起動中に安全性が求められる．ところが条文の本文中では起動中の状態については直接触れられておらず，背景となる知識がなければ起動中の安全化が求められていることは読み取れない可能性が高い．

また条文中の「安全な状態」という記述は，解釈がシステムに依存すると考えられる．なぜなら安全な状態はシステムごとに異なり，また同一のシステムであってもシステムの状態や周囲の状況によって異なり得るからである．このように条文の意図を理解して開発を行うには，明示されていない情報やシステムに依存する情報を知識や経験をもとに正確に解釈することが求められる．

2.3 Goal Structuring Notation (GSN)

GSNとはKellyら [Kelly1997]によって提唱された，安全性に関する議論を構造化するための記法であり，現在はGSN Community Standardによって記法が定義されている [GSN2011]．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客観的に保証することができる．ゴール, ストラテジ, ソリューションはそれぞれ長方形，平行四辺形，円形のノードで示される．記述例を図 1 に示す．

図 1 ではG1のトップゴールがS1のストラテジによってハザードごとの議論に分解されている．C1はコンテキストと呼ばれるノードであり，議論の背景や前提条件を示す役割を持っている．ここではハザードごとの議論を記述する際の前提となる，ハザード分析結果へのリンクを示している．またG3の下についているひし形のノードはundevelopedと呼ばれ，現段階では未定義であり，開発の今後において達成すべき主張や観点であることを示す．

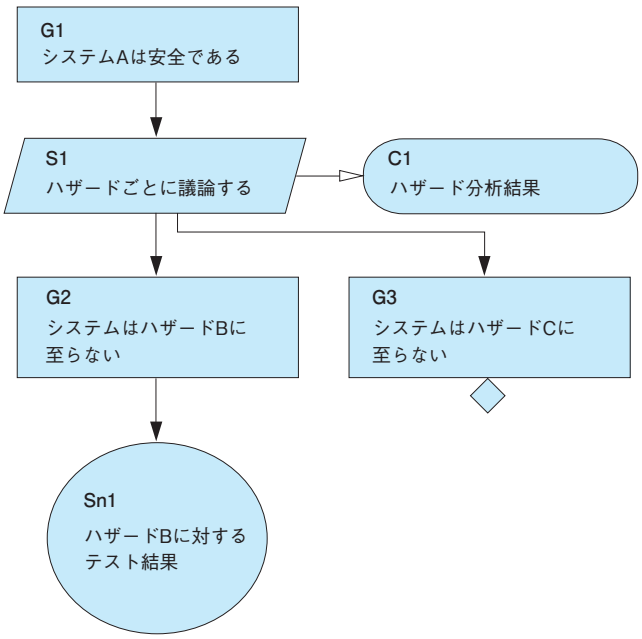


図1　GSNによる記述例

GSNを用いてシステムの安全性に関する主張を記述したものはアシュアランスケース [OMG2013] やD-Case [DEOS2015]などの形で標準化が進んでおり, 自動車 [Palin 2011]や医療 [Ray2013]，鉄道 [Souma2014]，航空宇宙 [Denny2012]，軍事 [Tanaka2012] などの分野で安全性の保証を目的に利用が検討されている．過去の研究においても無人軍事航空システムへの適用 [Denny2012]や超小型衛星への適用 [Tanaka2012]など高い安全性が求められるシステムへの適用において，更に，安全性だけでなくセキュリティの分野 [Kawakami2015]においてもその有効性が確認されている．

2.4 関連研究

一般安全要求や安全規格を用いた規範的な安全保証とGSNを用いた安全保証の比較を行った研究として，Hawkinsらは国際安全標準とGSNによる保証を実際に行った上で定性的な比較を行った [Hawkins2013]．Hawkinsらは，規範的な安全保証では規格に従うことで安全性にかかわる証拠をそろえやすいメリットがある一方で，それらの証拠がどのように安全性に寄与するのかは暗黙的であると主張した．またGSNを用いた安全保証においても，どのように安全性が保証されているのかが明確になる一方で，経験の浅い開発者はどのようにゴールを設定し記述すれば良いか分かりづらいとしている．結論として，Hawkinsらは安全要求，安全規格によって求められる保証を，GSNを用いて記述することで，二つの安全保証を相補的に用いるべきであると主張している．

GSNを用いて一般安全要求・安全規格の明確化を行った研究として, Hollowayら [Holloway2015]はDO178C [RTCA 2011] という航空機搭載システム・機器を対象とした安全規格の明確化を行っている．Hollowayらは既存の安全規格では求められるエビデンスがどのように安全性に寄与するかは暗黙的であると主張した上で，それらのエビデンスがどのような理由で求められているのかをGSNを用いて明確化した．しかしこの研究では設計に対する要求の明確化は行われておらず，また評価実験が行われていないためその有効性については明らかになっていない．

3 GSNを用いたCBCS安全要求解釈の明確化

本節ではCBCS安全要求の明確化を行った際の指針と実例について述べる．

3.1 CBCS安全要求をGSN化する上での指針

過去の開発で得られた，読み取ることが難しい情報を明確化する

課題 1 を解決するため，暗黙的に仮定された読み取る

ことが難しい情報を明示することで開発者と審査者との相互理解を支援できるように記述した．読み取ることが難しい情報の明確化にはJEMやHTVの開発における解釈から暗黙知を引き出し，それらをGSNに記述した．過去の開発において行われた過去の解釈をもとにした設計は安全審査を通過しているため，条文本来の意図に近い解釈が行われていると考えられるからである．

解釈がシステムに依存する記述に対してはステークホルダ間での合意を要件とした

解釈が対象となる個別のシステムに依存する記述は一般的な解釈を持たないため，過去の解釈を記述するだけでは条文の明確化を行うことができない．解釈がシステムに依存する記述に対しては，開発対象ごとに解釈を定め，それらについてステークホルダ間で合意を得る必要がある．

そこで課題２を解決するため，条文中のシステムに依存する部分を明確化し，それらへの解釈についてステークホルダ間で合意を得ることを目的とするゴールを導入することにより，GSN版CBCS安全要求における要求とした．

議論構造を設計と検証に分けて記述する

CBCS安全要求は設計に対する要求と検証に対する要求を明確に区別して構成されている．そのためGSNで記述する場合においても，要求が設計と検証のどちらに対するものなのかを明確にするため，GSNにおける議論構造上で分けて記述した．

明確化された条文に対して複数回のレビューを行う

CBCS安全要求の明確化において誤った解釈や不足した記述を防ぐため，一つの条文に対して安全審査の参加経験がある開発者二人以上により複数回のレビューを行った．

3.2 GSNによって明確化したCBCS安全要求（GSN版CBCS安全要求）の条文例

3.1節で述べた指針に従って明確化を行った．2.2節で例示したCBCS安全要求の箇条3.1.1.1の条文を明確化したものが図２である．一番上のゴールは実際の条文である．

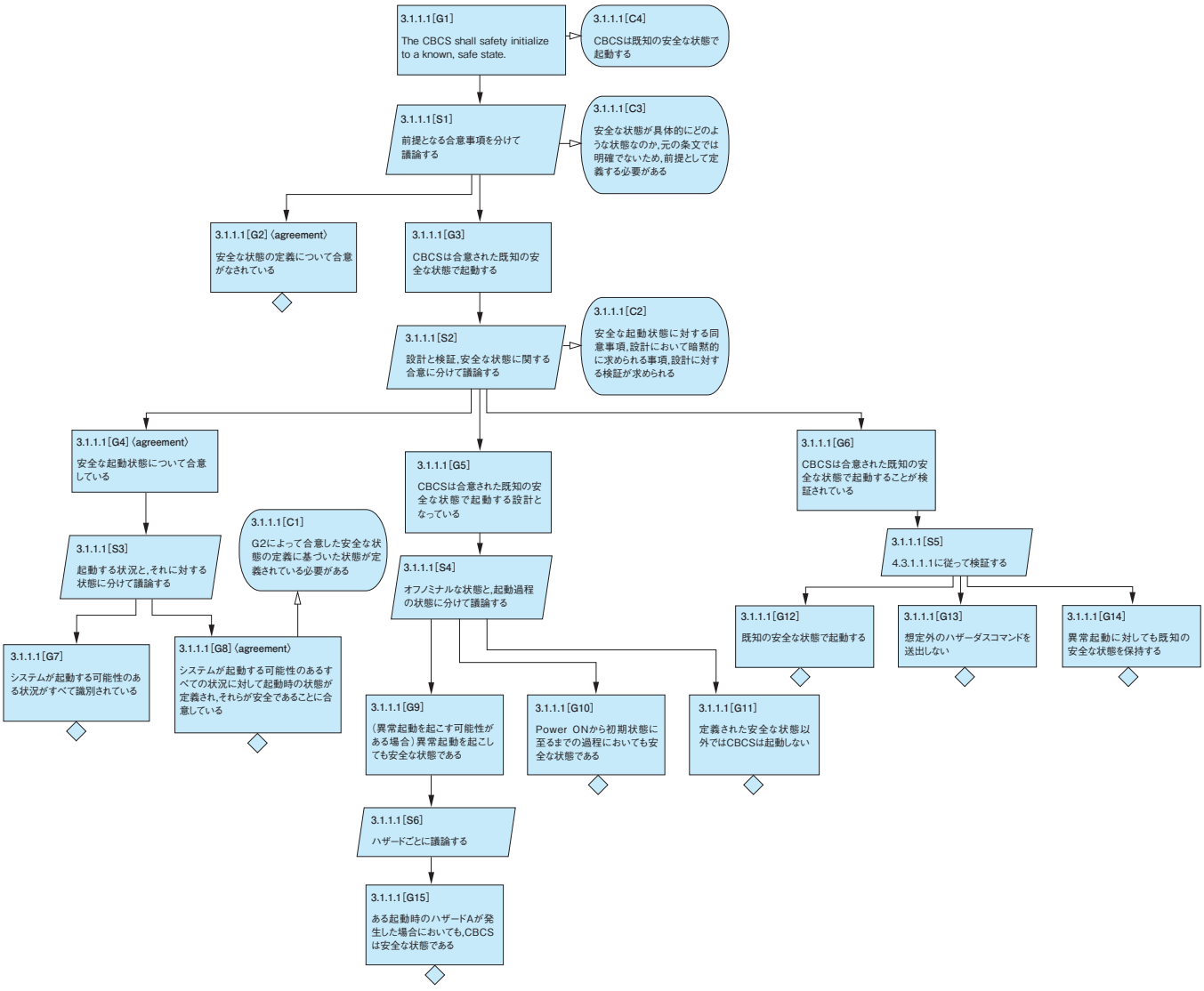


図２　GSNによって明確化されたCBCS安全要求の条文

課題１への対応として，読み取ることが難しい情報を暗黙的に仮定した記述に対して明確化を行った部分に対応するのがG5「CBCSは合意された既知の安全な状態で起動する設計となっている」以下からなる議論構造である．ここでは2.2節で示した例のほかに，異常起動を起こす場合でも安全化がなされていれば良いといったような例外事項などを記述している．

課題２への対応として，システムに依存する記述に対する明確化を行っているのがG2「安全な状態の定義について合意がなされている」はじめG4，G7，G8，S3からなる議論構造である．ここではシステム起動時の安全な状態を，システムが起動する可能性のある場合すべてに対して定義し，それぞれが安全であることについて合意することを求めている．

その他，CBCS安全要求をGSN化した結果は［Kakimoto 2016］を参照のこと．

4　評価

4.1　評価実験

GSN版CBCS安全要求に対する評価実験として，安全審査に対する有効性の調査を目的とした実験を行った．本稿における評価実験に関する諸元をまとめたものが表１である．評価実験においては，以下の点に着目して評価を行った．

１．安全性に対する効果
２．コストに対する効果

本評価実験ではJAXA技術職員を対象として安全審査を想定した評価を行った．被験者数は20名で，GSN版安全要求を用いたグループ（以下，GSNグループ）と従来のCBCS安全要求のみを用いたグループ（以下，従来グループ）の各10名ずつに分けた．グループ分けはGSNや対象システムに対する知識や開発経験の有無を事前に調査し，大きな偏りがないように努めた．

表１　実験諸元

評価対象	被験者数	設問設定	作業内容	実験時間
JAXA 技術職員	全20名 GSNグループ：10名 従来グループ：10名	HTVを想定した，誤りを含む 架空のハザードレポートに対する 安全審査	誤りの発見 対策の修正 自己評価	事前説明：10分 安全審査：～40分 自己評価アンケート：10分

各グループは公開されたHTVの情報［Torano2009, Shirasaka2011］をもとに作成した架空の「ハザードレポート」に対して安全審査を行った．ハザードレポートには想定される「システムの逸脱（想定外のシステムのふるまい）」と「逸脱の原因」が既知の情報として記載されている．また「逸脱に対応するCBCS安全要求の条文」及び「逸脱に対する対策」が記載されている（これらには誤りが含まれる）．被験者は対応する条文と対策がCBCS安全要求に沿った内容であるかを審査し，「誤りの発見」及び「対策の修正」を行った．「誤りの発見」では審査時の誤りの検出への支援効果を，「対策の修正」では開発時への支援効果の測定をそれぞれ想定している．評価実験で用いた問題文は［Kakimoto2016］を参照．

本実験では，下記３つの観点についてGSN版CBCS安全要求を用いた場合とそうでない場合でデータの収集を行った．

観点１　課題に対する正答数（全４問）
観点２　平均回答時間（最大40分）
観点３　達成度に対する自己評価（５段階）

観点１及び観点３では，それぞれ安全性に対する定量的，定性的な観点からの評価を行った．また観点２では安全審査にかかった時間から，安全審査におけるコストに対する効果をそれぞれ評価している．

観点１では被験者が誤りを発見し，対策を正しく修正できていたものを正解として採点した．観点２については，両方のグループに対して事前に10分の説明を行った上で，上限40分で課題の回答時間を計測した．また観点３について課題終了後にアンケート形式で達成度に関する以下の質問を行った．

質問a　誤り，不足を見つけることができたか
質問b　CBCS安全要求を満たすためにどのような対策が必要なのかが分かったか

各質問に対して被験者は「５：よくできた」から「１：できなかった」の５段階で回答した．質問aと質問bではそれぞれ，誤りの発見に対する達成度と対策の修正の達成度に対する自己評価の収集を目的とした．

4.2　実験結果

観点１に対する結果を図３に示す．図３では1Q－（IQR×1.5）～ 3Q＋（IQR×1.5）の範囲から外れたものを外れ値として扱っている．（1Qは第１四分位数，3Qは第３四分位，IQRは四分位範囲．）観点１において，GSNグループの正答数は従来グループに対して高くなっていることから分かる．また二つのグループの平均点の差が偶然誤差の範囲内で

あるという帰無仮説を立て，有意水準５％でWelchのt検定を行った．その結果，危険率2.77%で帰無仮説が棄却されたため，二つのグループには有意な差があると言える．

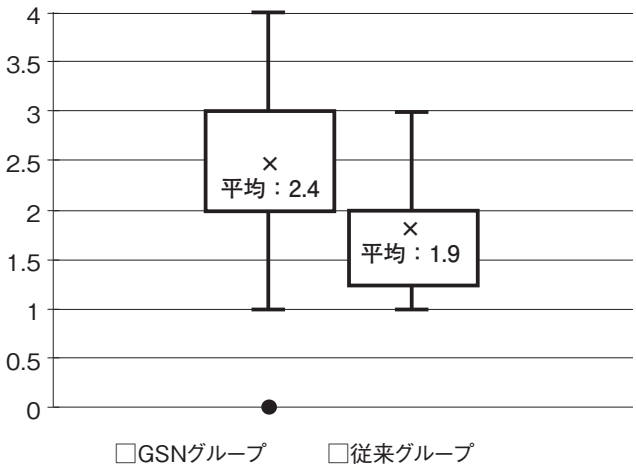


図３　正答数の分布

観点２に対する結果を表２に示す．観点２についてはGSNグループの回答時間が38.4分と従来グループ（33.7分）と比較して14%長くなった．これはGSNによってCBCS安全要求の解釈を記述することで情報量が増加し，GSNを読む作業とハザードレポートの情報をGSN版CBCS安全要求と比較する作業が加わったことが原因であると考えられる．

観点３に対する結果を図４に示すこの結果から誤りの発見と対策の記述の両方において，従来グループの方が高い自己評価を行う傾向にあることが分かる．

表２　平均回答時間

	平均回答時間
GSNグループ	38.4分
従来グループ	33.7分

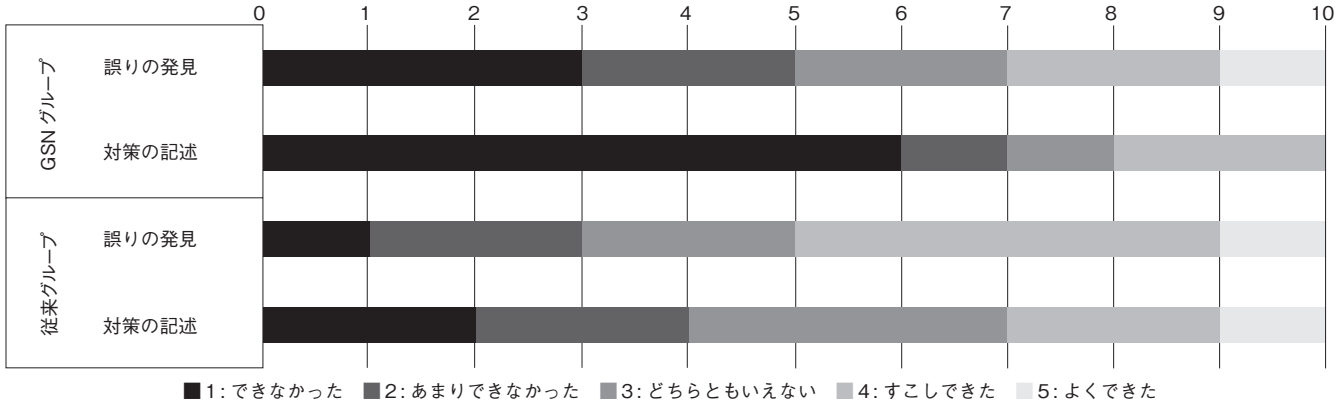


図４　達成度に対する自己評価結果

5　考察

5.1　実験結果に対する分析と考察

観点１の結果から，GSN版CBCS安全要求を用いることで安全審査の精度が上がることが分かる．しかし観点３の課題の達成度に関する質問への回答結果では，従来のCBCS安全要求を用いた場合のほうが課題を達成できたと答えた割合が大きく，実際の正答数と被験者の実感に差が生じていることが分かる．しかし課題の実際の達成度と自己評価には正の相関があるべきである．なぜなら，審査対象システムが安全審査を通過するのは，審査者が十分に安全であると判断した，すなわちその実感が得られたときだからである．このことから我々は以下の仮説を立て，追加の分析を行った．

仮説１　GSN版CBCS安全要求を安全審査に用いた場合，審査結果と審査者の実感に正の相関がない

仮説２　従来のCBCS安全要求を安全審査に用いた場合，審査結果と審査者の実感に正の相関がない

そこでこれら仮説について分析するため，課題の達成度に関する質問に対して１または２と回答したグループをネガティブ群，４または５をポジティブ群に分けて表３の比較を行った．また統計的な分析として，正答数と課題の達成度に関する自己評価への回答結果を用いてピアソンの積率相関係数（n=10）を求めた．

表３の結果からGSNグループでは正解数と質問への回答に正の相関関係が見られた．よって仮説１は成り立たず，GSNグループでは実際の正当数と被験者の実感に差が生じづらいと考えられる．一方，従来グループでは相関関係が確認できなかった．よって仮説２は成り立ち，従来グループでは実際の正答数と自己評価が必ずしもが関係しないと言える．

この結果からGSNによる暗黙知の明確化は経験の少な

い開発者だけではなく経験を積んだ，とくに自分の経験による設計で十分に安全要求が満たされると考える開発者に対しても有効であると考えられる．なぜなら従来の安全要求を用いた場合，経験を積んだ開発者が十分であると判断した場合においても不十分な設計がなされていた可能性があるからである．

また観点２ではGSN版CBCS安全要求を用いた場合の方が審査に時間がかかったことから，安全審査において従来よりも工数が掛かってしまうと予想される．しかし審査時間の増加は一割程度に留まっており，危険性の見過ごしによる手戻りや宇宙機システム自体の喪失，過剰な安全設計によるコストの増加に比べれば小さいと考えられる．

表３　正答数と自己評価の関係に対する分析結果

		全体の平均正答数	ポジティブ群平均	ネガティブ群平均	積率相関係数 (n=10)
GSNグループ	誤りの発見	2.78問	3.33問	2.25問	0.549..
	対策の修正		3.50問	2.5問	0.658..
従来グループ	誤りの発見	1.90問	1.80問	1.67問	−0.251..
	対策の修正		1.67問	2.25問	0.146..

5.2　限界と妥当性への脅威

本研究における一般安全要求の明確化の限界として，GSN版CBCS安全要求はあくまで条文に対する理解の助けや安全審査における議論の土台として利用することを想定していることが挙げられる．なぜならGSN版CBCS安全要求はCBCS安全要求を完全に満たすことを保証しておらず，従来のCBCS安全要求で明示的でない記述を過去の開発における解釈やエンジニアの知見の範囲で明確にしたものだからである．従って規格の認証プロセスなどの網羅性の求められる暗黙知の明確化においては，本稿において述べた手法に加えて網羅性の保証される情報の記述を行う必要があるといえる．

また明確化には情報の引き出し方に留意する必要がある．CBCS安全要求の明確化においては安全審査の結果や有識者間での議論の結果が記録されていた．よって条文の問題点や解釈が有識者間では共有されており，明確化を行う情報源となる文書の選定や有識者によるレビューを通して情報を引き出すことに対して特別な工夫を必要としなかった．しかしそれらの情報が有識者間においても共有されていない場合には，明確化の対象となる事項を明確にし，暗黙知の前提条件や特殊な状況下での制約といった引き出す際に漏れやすい知識に注意して情報を引き出すなどの工夫が必要であると考えられる．

内的妥当性への脅威

本研究の評価実験ではHTVを想定した架空のハザードレポートを用いたが，理想的な評価実験環境では実際のハザードレポートを用いるべきである．しかし現在運用されているシステムの，公表されていない安全性にかかわる問題を用いた結果を使って公に議論することは困難である．また架空のハザードレポートは公表されているHTVの情報に則って作成された上でJAXA技術職員のレビューをうけており，一定の妥当性は担保されると考えられる．

次に，４節の評価実験での採点の妥当性について述べる．被験者回答において，正しく対策の修正が行われているかどうかは我々の主観によって判断されている．しかし，採点には一定の基準を設けており，複数の評価者によって一貫して基準を適用していることをレビューしているため，主観による影響は最小限に抑えている．

外的妥当性への脅威

最初に，HTV以外のシステムに対するGSN版CBCS安全要求の適用性について述べる．CBCS安全要求は複数のシステムに対して適用される安全要求である．本研究ではHTVに対する安全審査を想定して評価実験を行ったが，本来は他のISSに関連するシステムに対しても評価実験を行うことが望ましい．しかし本研究における評価実験ではCBCS安全要求適用の一般的な手続きを採用しているため，他のシステムの保証においても同様に適用することができると考える．

次に，CBCS安全要求以外の，他の一般安全要求や安全規格に対するGSNを用いた明確化の有効性について述べる．Hawkinsら [Hawkins2013] は従来の安全規格は暗黙的であり，開発者が趣旨を理解するのは困難であると主張しており，CBCS安全要求と同様の問題がほかの安全要求においても存在することが分かる．GSNは議論構造を可視化するための汎用的な手法であるため，CBCS安全要求以外の一般安全要求や安全規格に対しても適用可能であると考える．しかし安全要求や規格ごとに保証プロセスの違いが存在するため，それらを考慮して明確化を行う必要がある．

6 おわりに

6.1 まとめ

本論文では宇宙分野で用いられる一般安全要求が実際にはどのような要件によって満たされるかを，GSNを用いて明確化した．一般安全要求の明確化は，開発者及び審査者の相互理解や安全審査の支援を目的として行った．また明確化したCBCS安全要求の有効性の評価を目的として，JAXA技術職員を対象とした評価を行った．評価の結果，GSNによって明確化されたCBCS安全要求を用いた場合，以下のメリット・デメリットがあることを確認した．

メリット1　安全審査による誤りの発見とその修正数が26%向上した．

メリット2　従来の一般安全要求では審査者の思い込みによる危険性の見過ごしが発生する懸念があるが，GSNを用いた明確化ではそれが見られない．

デメリット1　従来の手法と比較してGSN化した安全要求による審査の所要時間は14%大きい．

6.2 今後の課題

本研究で提案した，GSNによる暗黙知の明確化を一般化することが今後の課題として挙げられる．他分野への応用として，ソースコードレビューにおける暗黙知の明確化が考えられる．ソースコードレビューにおいては，チェックリストを用いたレビューが代表的な支援手法として使用されている［Bando2011］．過去の研究においてDengerらはレビュー者の経験に応じてレビューの観点を設定するべきである［Denger2007］と主張しており，開発者の経験はコードレビューの品質に影響を与えるとされている．しかし背景知識や経験に応じてチェックリストの観点を設定した場合においても，チェックリストの各項目は過去の設計や事故事例などの想定をもとに策定されると考えられるため，一定の暗黙知を含むと予想される．暗黙知を含むチェックリストによるレビューにおける判断基準はレビュー者によって解釈が異なると考えられるため，従来の安全要求と同様にレビュー者の思い込みによる危険性の見過ごしが懸念される．そこで，チェックリストに含まれる暗黙知を，GSNを用いて明確化することによってソースコードレビューの品質の向上が期待できる．

謝辞　本稿4節の評価実験にご協力いただいた，宇宙航空研究開発機構 第三研究ユニットの方々に深く感謝いたします．

参考文献

［NASA1995］SSP 50038B Computer-Based Control System Safety Requirements –International Space Station, 1995.
［Kelly1997］Tim Kelly and John A McDermid, Safety Case Construction and Reuse using Patterns, 16th SAFECOMP, pp.55-69, 1997.
［GSN2011］The GSN Working group, GSN COMMUNITY STANDARD VERSION 1, 2011.
［OMG2013］Object Management Group, Structured Assurance Case Metamodel (SACM), 2013.
［DEOS2015］DEOS協会 D-CASE部会, D-CASE構文定義書, 2015.
［Palin2011］Rob Palin, David Ward, Ibrahim Habli and Roger Rivett, ISO 26262 safety cases: Compliance and assurance, 6th IET International Conference on System Safety, pp.1-6, 2011.
［Ray2013］Arnab Ray and Rance Cleaveland, Constructing Safety Assurance Cases for Medical Devices, 1st International Workshop on Assurance Cases for Software-Intensive Systems, pp.40-45, 2013.
［Souma2014］相馬 大輔, 田口 研治, 西原 秀明, 大岩 寛, 矢田部 俊介, 森 崇, RAMS の認証とセーフティケース, クリティカルソフトウェアワークショップ (WOCS2: Workshop of Critical Software System), 2014.
［Denny2012］Ewen Denny, Ganesh Pai and Ibrahim Habli, Perspectives on Software Safety Case Development for Unmanned Aircraft, Proceedings of the 42nd Annual IEEE/IFIP International Conference on Dependable Systems and Networks, pp.1-8, 2012.
［Tanaka2012］田中康平, 松野裕, 中坊嘉宏, 白坂成功, 中須賀真一, アシュアランスケースを用いた小型人工衛星の品質保証 – REAJ 第20回春季信頼性シンポジウム, pp.63-66, 2012.
［Kawakami2015］Henrique Kawakami, Roberto Gallo, Ricardo Dahab and Erick Nascimento, Hardware Security Evaluation Using Assurance Case Models, 10th International Conference on Availability, Reliability and Security (ARES), pp.193-198, 2015.
［Hawkins2013］Richard Hawkins, Ibrahim Habli, Tim Kelly and John McDermid, Assurance cases and prescriptive software safety certification: A comparative study, Safety Science 59, pp.55-71, 2013.
［Holloway2015］C. Michael Holloway, Explicate '78: Uncovering the Implicit Assurance Case in DO-178C, 23rd Safety-critical Systems Symposium, pp.2-5, Bristol, UK, 2015.
［RTCA2011］RTCA, Software Considerations in Airborne Systems and Equipment Certification DO–178C, 2011.
［Kakimoto2016］柿本 和希, ゴール構造化記法を用いた汎用的な安全要求の明確化, 奈良先端科学技術大学院大学　情報科学研究科　修士論文, 2016.
［Torano2009］虎野 吉彦, 小鑓 幸雄, 佐々木 宏, 鈴木 裕介, 植松 洋彦, 深津 敦, 山中 浩二, 麻生 大, 宇宙ステーション補給機 (HTV) 技術実証機の飛行結果, 平成21年度宇宙環境利用の展望, 第7章, pp.1-28, 2009.
［Shirasaka2011］白坂成功, 堀田成紀, 蒲原信治, 階層化 FDIR による高安全性航法誘導制御系の提案と宇宙ステーション補給機「こうのとり」での実現, 計測自動制御学会産業論文集 Vol.10, No.11, pp.91-99, 2011.
［Bando2011］坂東 祐司, ソフトウェアレビューにおける構造化チェックリストの表記方法の実験的評価, 奈良先端科学技術大学院大学　情報科学研究科　修士論文, 2011.
［Denger2007］C. Denger and F. Shull, A practical Approach for Quality-Driven Inspections, IEEE Software, Vol.24, Issue 2, pp.79-86, 2007.