CBCS 安全要求の適用性向上に向けた可視化の取り組み

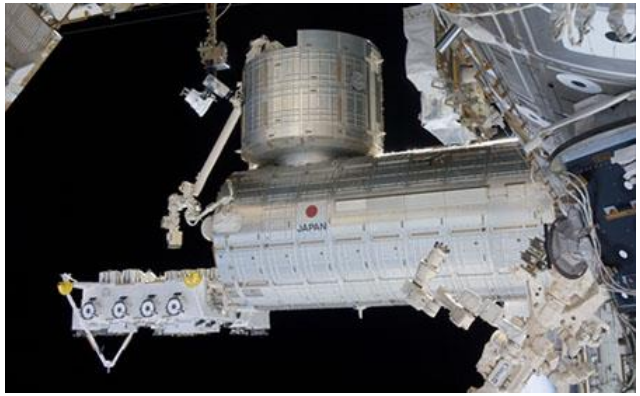
奈良先端科学技術大学院大学
超高信頼ソフトウェアシステム検証学研究室
（JAXA 教育連携研究室）

柿本 和希

本研究は JAXA 第三研究ユニットと共に実施された

Computer-Based Control System (CBCS) 安全要求

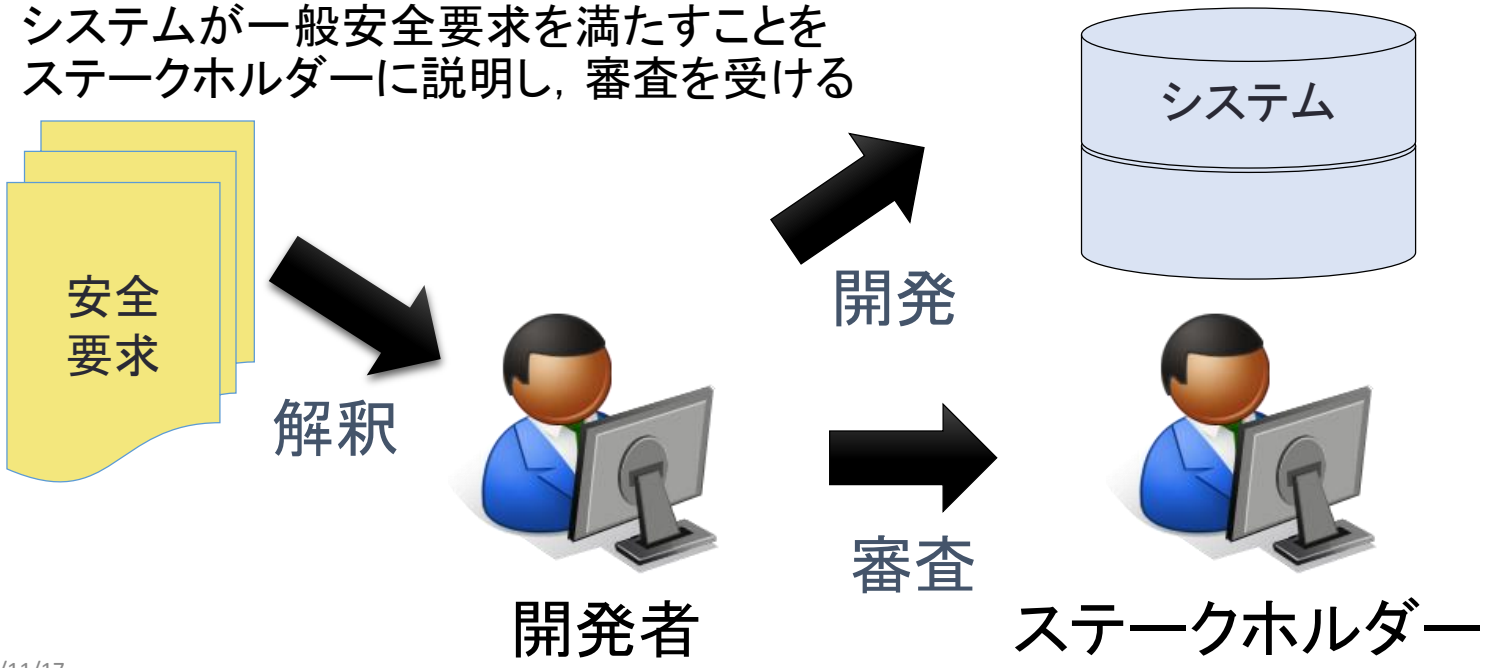
- 国際宇宙ステーション（ISS）の建造にあたって，NASAが定めた安全要求
  - ISS に関連する全てのコンピュータシステムに対して適用される一般安全要求
  - CBCS 安全要求の適用されるシステムは，NASA に対する安全審査を通過する必要がある
  - きぼう（JEM）や こうのとり（HTV） の開発においても，CBCS安全要求を満たしていることの保証と説明をNASAに対して行った
- 一般安全要求: 特定分野のシステムに汎用的に適用される安全要求



http://www.jaxa.jp/projects/iss_human/kibo/index_j.html

一般安全要求の保証の流れ

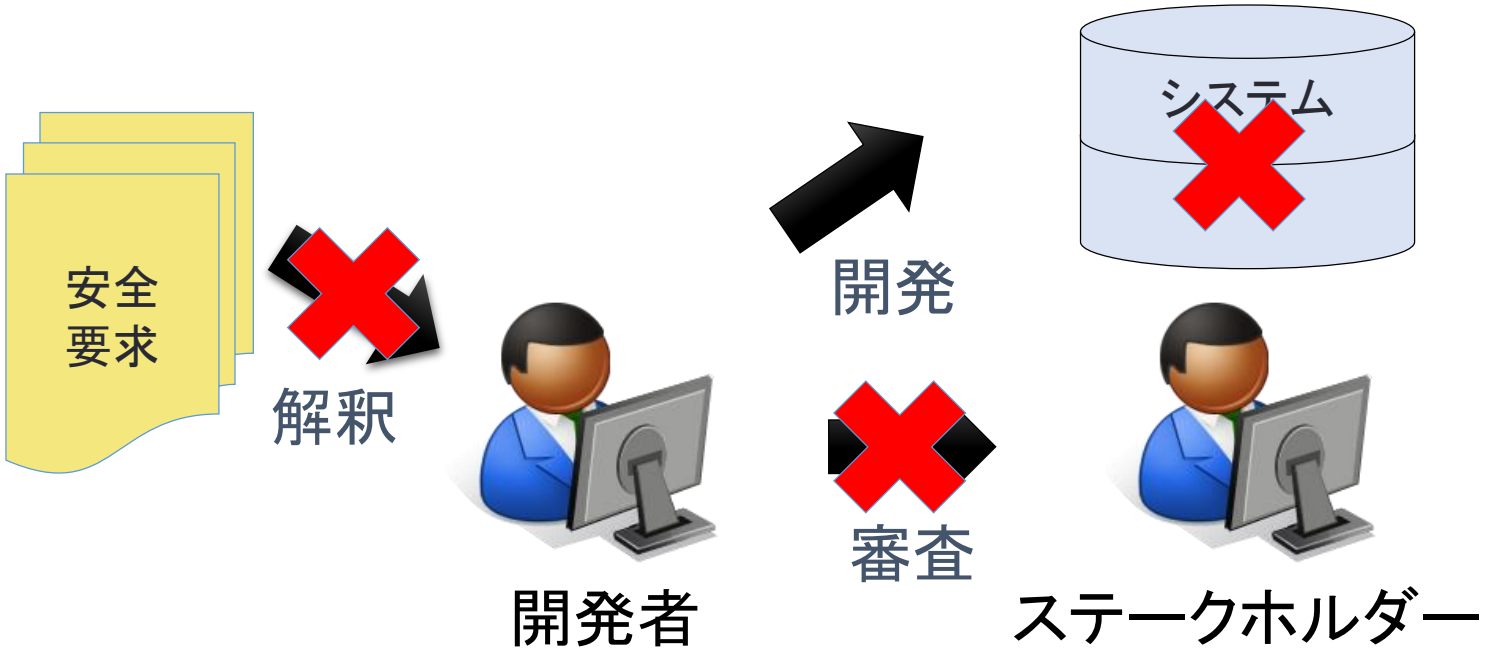
1. 解釈
   - 一般安全要求において，実際にはどのようなことが求められるかを理解する
2. 開発
   - 解釈をもとに，安全要求に従ってシステムの開発を行う
3. 審査
   - システムが一般安全要求を満たすことを
     ステークホルダーに説明し，審査を受ける



一般安全要求の問題点

- 暗黙的な記述が存在しており，その解釈に幅がある

- 条文の意図から外れた解釈
  - 危険性が残留したシステム
  - 安全審査における危険性の見落とし



CBCS安全要求における暗黙的な記述例

条文: 3.1.1.1
『CBCSは既知の安全な状態で起動する』
実際の条文

読み取ることが難しい情報

暗黙知
起動時だけではなく，起動中も安全化が必要

例外事項
異常起動を起こす可能性がある場合でも安全化されていればよい

システムに依存する記述

『既知の安全な状態』がどのような状態を指すか明確ではなく，定義がシステムやシステムの状態に依存してしまう

実際に考慮する必要のある暗黙的な情報

研究目的とアプローチ

- 目的:暗黙的に記述された一般安全要求の条文を明確化する

- アプローチ:Goal Structuring Notation (GSN) を用いて条文を可視化する
  - 期待すること:
  1. 一般安全要求に対する正しい理解・解釈の支援
  2. 一般安全要求を用いた設計・審査の効率化の支援

  - Goal Structuring Notation
    - 議論を可視化するための記法
    - 安全性に関する議論を記述する目的でも用いられる

研究の概要

NAIST

- CBCS安全要求をGSNを用いて表現する
- 予備実験の実施
- 本実験の実施

JAXA

- CBCS安全要求に関する情報提供
- GSN化されたCBCS安全要求のレビュー
- 本実験環境の提供

JAXA 業務における GSN 版一般安全要求の活用を目指す

関連研究（ Explicate ‘78: 78 Discovering the Implicit Assurance Case in Do-178C ）

- DO-178C（航空機システムにかかわる国際規格）に含まれる暗黙的な記述のGSNを用いた視覚化の研究[1]
  - 既存の安全規格には多くの暗黙的な記述が含まれている
    - 何故のその検証や文書が必要かは述べられていない
  - DO-178Cの各安全度レベルにおいて必要な検証や文書の視覚化
    - 設計にまで踏み込んだ視覚化は行っていない
    - 評価が行われていない

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

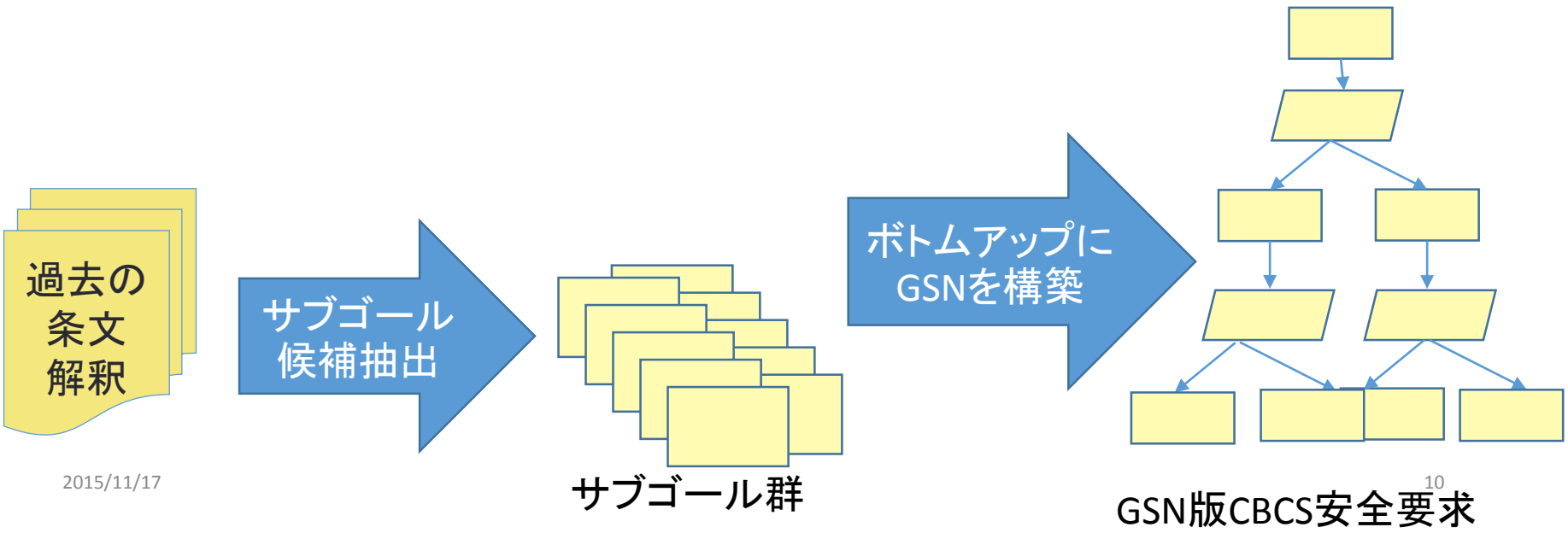
関連研究(Assurance cases and prescriptive software safety certification: A comparative study)

- アシュアランスケース（GSN）による保証と安全規格による
  保証(prescriptive)を比較した研究[2]
  - 実際に簡単なシステムの保証を行い，5つの観点に分けて定性的に比較
  - それぞれ完全ではなく，相補的に用いるべきであると主張
    - 安全規格を元にエビデンスを揃え，エビデンスの役割をアシュアランスケースを用いて説明するなど

[2] HawkiRichard ns el al. (2013): “Assurance cases and prescriptive software safety certification: A comparative study” Safety Science

CBCS安全要求のGSN化:
読み取ることが難しい情報の明確化

- 過去の条文解釈の中に含まれる，条文からだけでは読み取ることが難しい情報（暗黙知，例外事項）を用いてGSN化を行った
  1. 過去の条文解釈から，読み取ることが難しい情報を実際に考慮するべき事項(サブゴール)として抽出する
  2. 安全要求の条文をトップゴールとして，ボトムアップにGSNを構築する



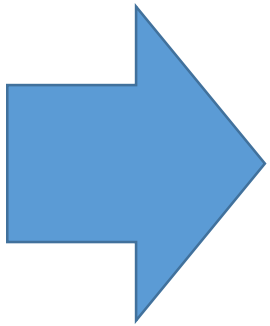
CBCS安全要求のGSN化:
システムに依存する記述の明確化

- 個別のシステムに依存する事項は，過去の設計解をゴールとすることができない

  - 開発するシステム内での解釈を定義し，開発者内で合意する事を本研究におけるゴールとした
  - 解釈の定義について合意する事を目的としたゴールに<agreement>という属性を付加し，合意ゴールとして識別した

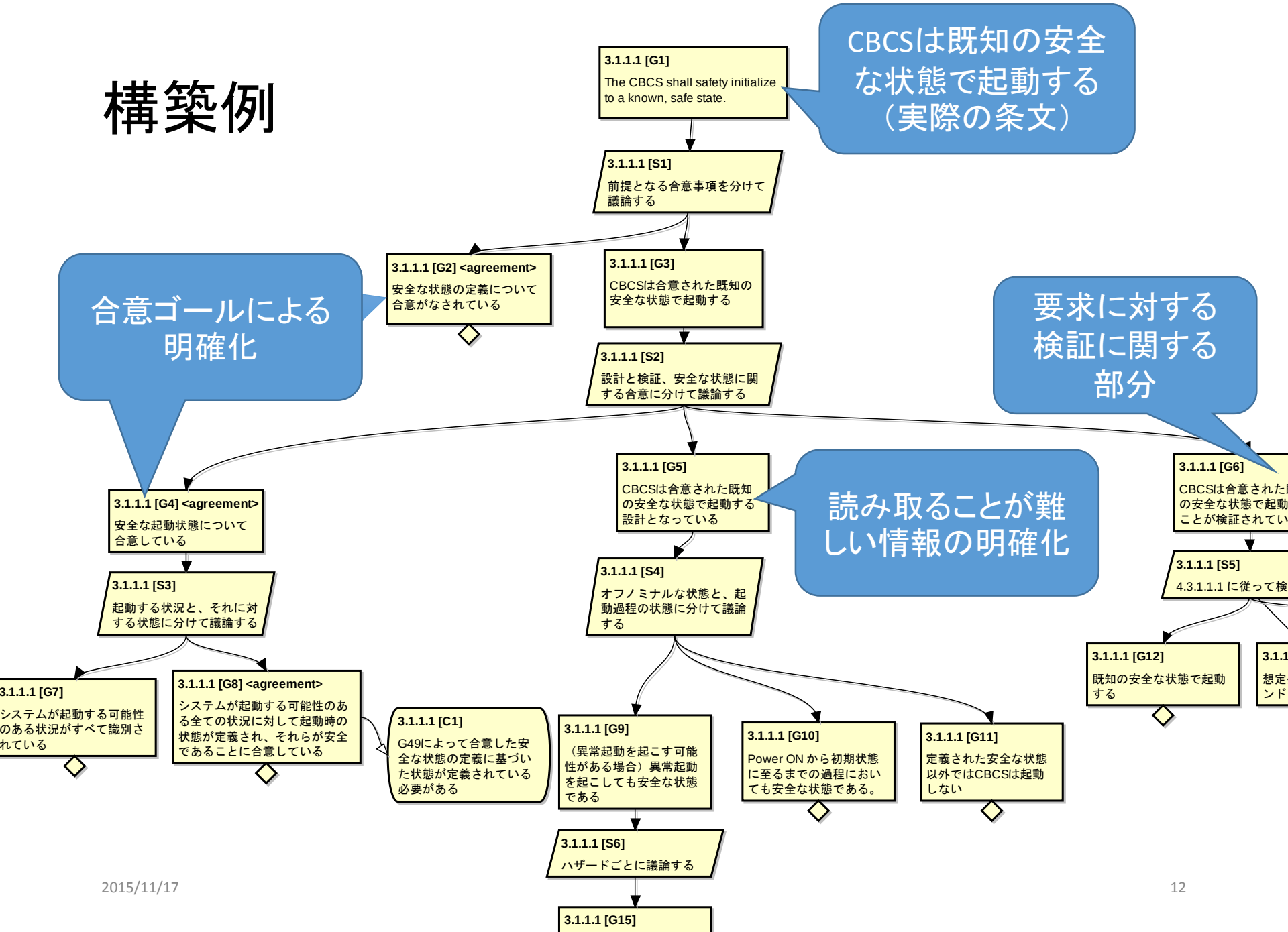
システムに依存する記述

『既知の安全な状態』

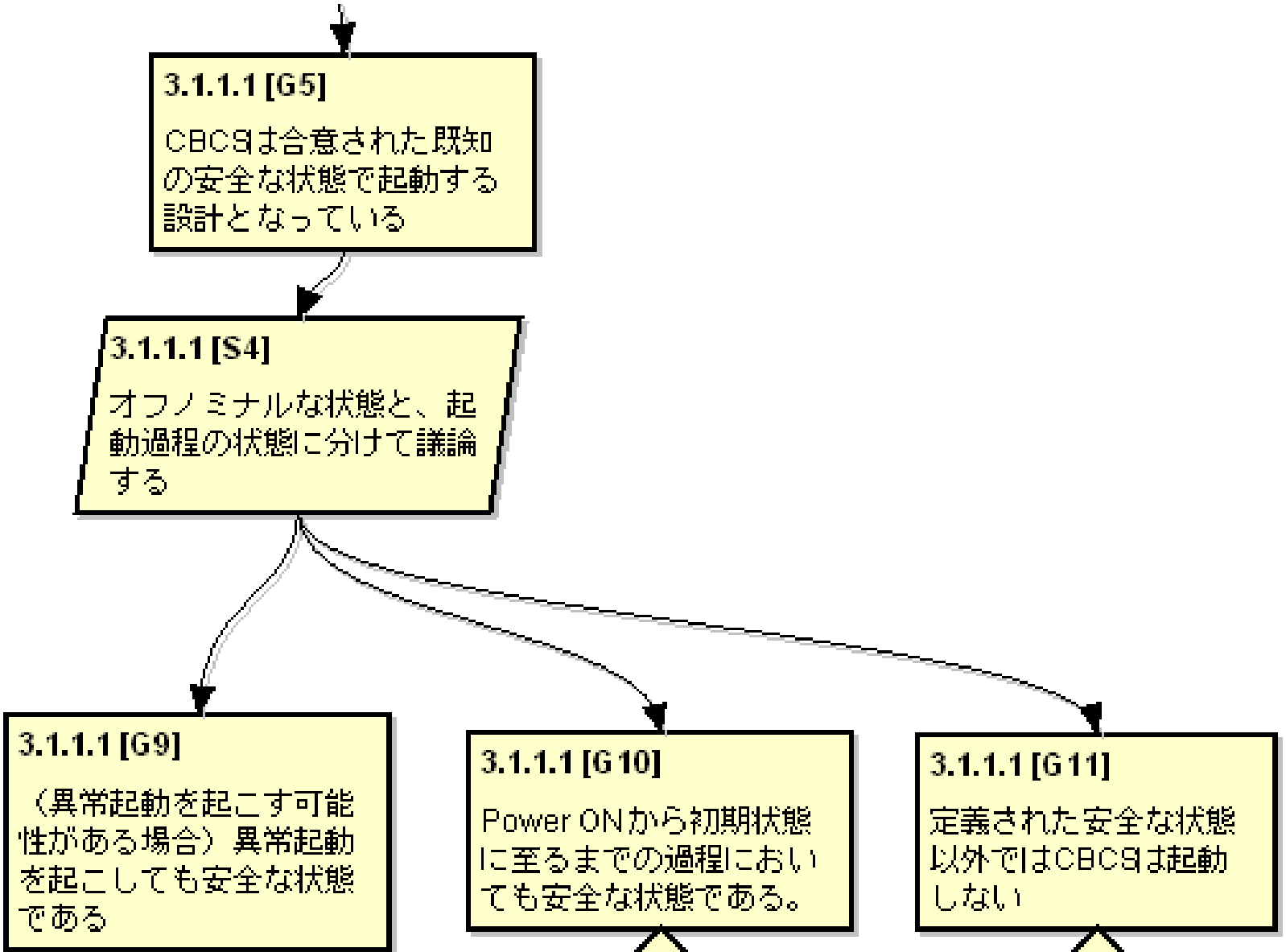


SG1<agreement>
開発対象のシステムにおける安全な状態が定義されている

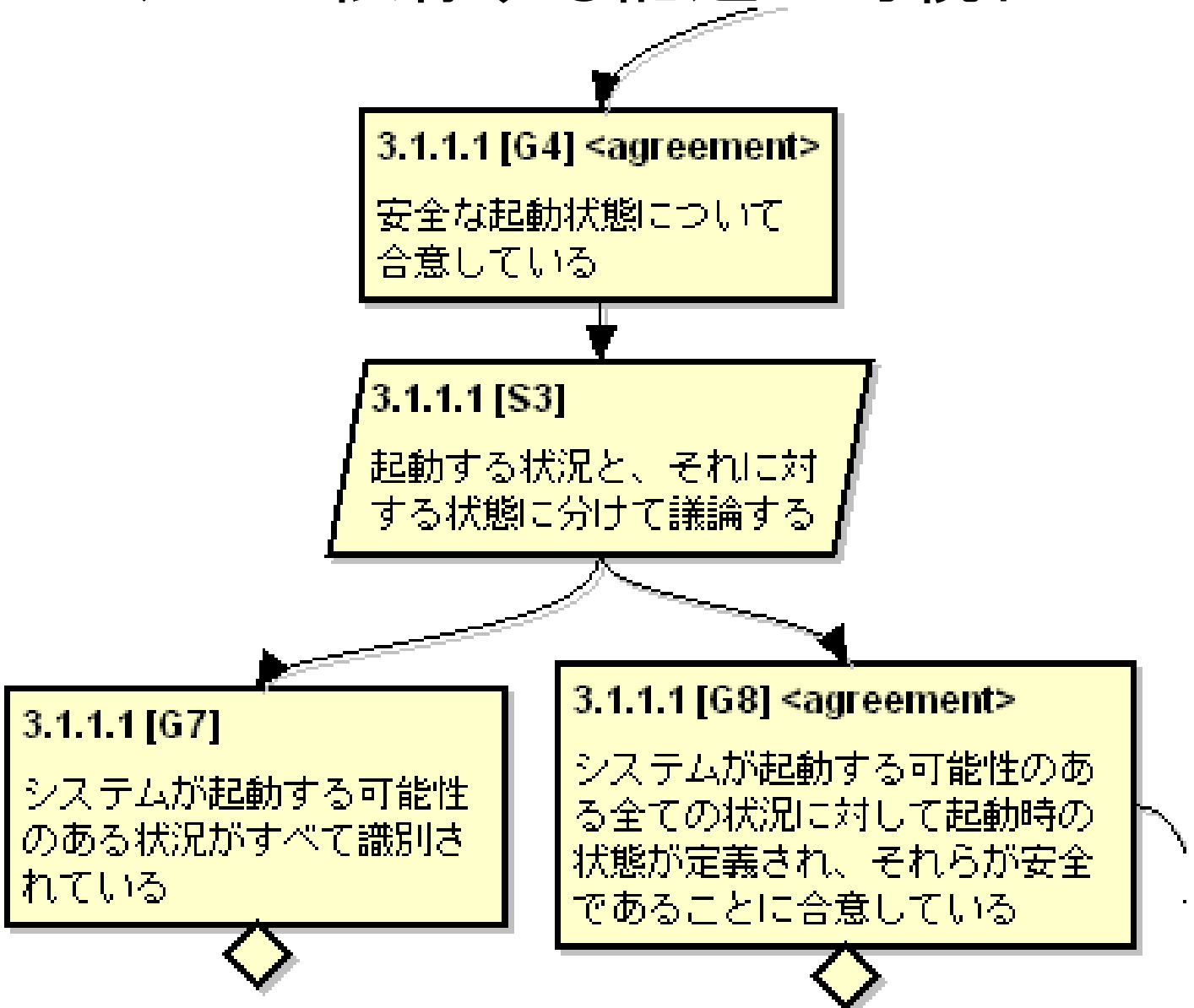
構築例


3.1.1.1 [G1]
The CBCS shall safety initialize to a known, safe state.
CBCSは既知の安全な状態で起動する（実際の条文）
3.1.1.1 [S1]
前提となる合意事項を分けて議論する
3.1.1.1 [G2] <agreement>
安全な状態の定義について合意がなされている
3.1.1.1 [G3]
CBCSは合意された既知の安全な状態で起動する
合意ゴールによる明確化
3.1.1.1 [S2]
設計と検証、安全な状態に関する合意に分けて議論する
要求に対する検証に関する部分
3.1.1.1 [G4] <agreement>
安全な起動状態について合意している
3.1.1.1 [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
読み取ることが難しい情報の明確化
3.1.1.1 [G6]
CBCSは合意された既知の安全な状態で起動することが検証されている
3.1.1.1 [S3]
起動する状況と、それに対する状態に分けて議論する
3.1.1.1 [S4]
オフノミナルな状態と、起動過程の状態に分けて議論する
3.1.1.1 [S5]
4.3.1.1.1 に従って検
3.1.1.1 [G7]
システムが起動する可能性のある状況がすべて識別されている
3.1.1.1 [G8] <agreement>
システムが起動する可能性のある全ての状況に対して起動時の状態が定義され、それらが安全であることに合意している
3.1.1.1 [C1]
G49によって合意した安全な状態の定義に基づいた状態が定義されている必要がある
3.1.1.1 [G9]
（異常起動を起こす可能性がある場合）異常起動を起こしても安全な状態である
3.1.1.1 [G10]
Power ON から初期状態に至るまでの過程においても安全な状態である。
3.1.1.1 [G11]
定義された安全な状態以外ではCBCSは起動しない
3.1.1.1 [G12]
既知の安全な状態で起動する
3.1.1.1 [S6]
ハザードごとに議論する
3.1.1.1 [G15]

読み取ることが難しい情報の可視化



システムに依存する記述の可視化



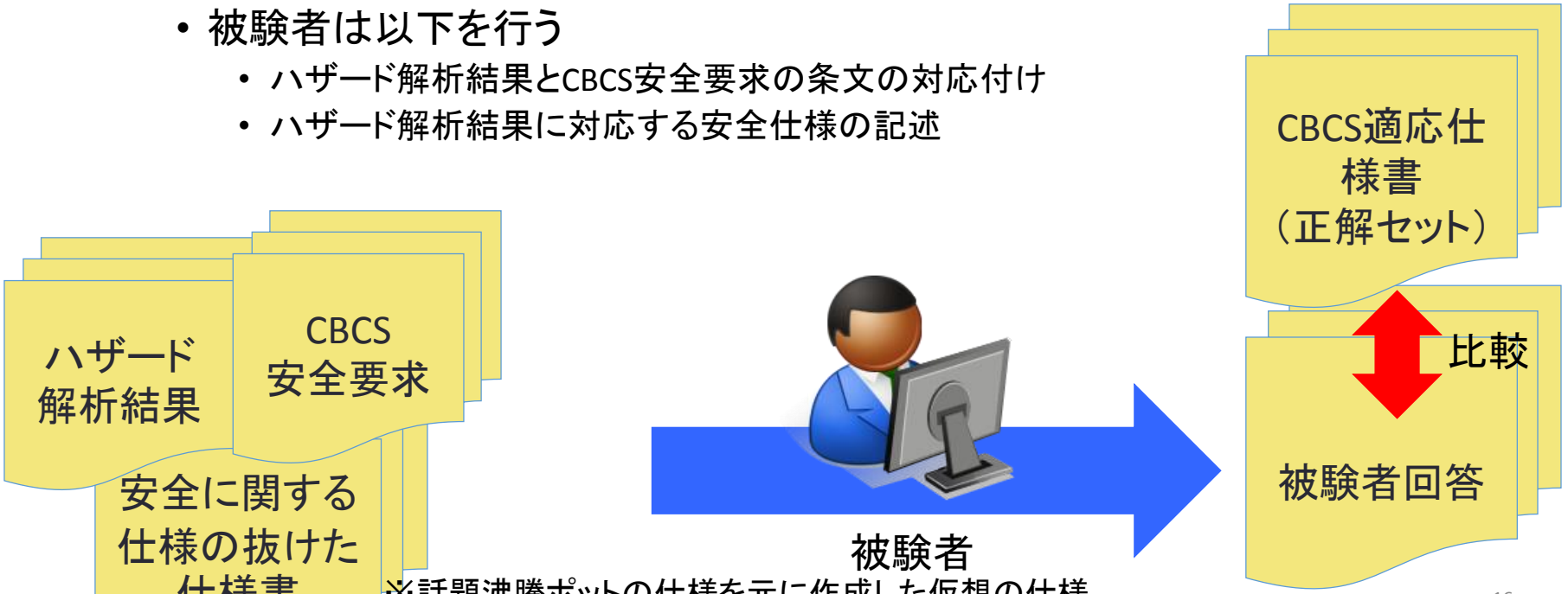
構築結果

- GSN化済みの条文: 12/38

	ゴール数	合意ゴール数	ストラテジ数
総計	168	14	66
平均	14	1.16	5．5
最大数 （1条文あたり）	25	3	12
最小数 （1条文あたり）	3	0	1

予備実験概要

- CBCS安全要求解釈とそれに基づく開発の支援効果の評価
- 実験対象者: 修士・博士課程の学生6名
- 電気ポットへのCBCS安全要求適用
  - 安全に関する仕様の抜けた仕様書(※)とハザード解析結果を用意する
  - 被験者は以下を行う
    - ハザード解析結果とCBCS安全要求の条文の対応付け
    - ハザード解析結果に対応する安全仕様の記述



※話題沸騰ポットの仕様を元に作成した仮想の仕様
話題沸騰ポット(http://www.sessame.jp/workinggroup/WorkingGroup2/POT_Specification.htm)

安全に関する仕様の抜けた仕様書の一部

振る舞い	CBCS 対応条文	逸脱	ハザード
コンセントの抜き差しでポットの起動・終了を行う.			
		起動時に異常な値がセットされている.	熱湯が噴き出す，意図しない沸騰行為.
		システム終了時などに蓋の開け閉め以外の動作が行える.	異常な水温の上昇，熱湯が噴き出す.
		電力供給が不安定になる.	異常な水温の上昇，低下.
温度制御行為をしていない状態でふたを閉じたら沸騰行為をする.			

安全に関する仕様の抜けた仕様書の一部

振る舞い	CBCS 対応条文	逸脱	ハザード
コンセントの抜き差しでポットの起動・終了を行う.			
		起動時に異常な値がセットされている.	熱湯が噴き出す，意図しない沸騰行為.
		システム終了時などに蓋の開け閉め以外の	異常な水温の上昇，熱湯が噴き出す.
			常な水温の上昇，下.
温度制御行為をしていない状態でふたを閉じたら沸騰行為をする.			

振る舞いの記述

対応条文の記述

予備実験結果: 正答数と回答時間

GSNによって記述されたCBCS安全要求を用いたグループ

	仕様の記述	対応付け	完答数	回答時間(分)
被験者A	11/27	12/27	**9/27**	**80分**
被験者B	15/27	14/14	**14/27**	**89分**
被験者C	1/27	2/27	**0/27**	**80分**

従来のCBCS安全要求を用いたグループ

	仕様の記述	対応付け	完答数	回答時間(分)
被験者D	11/27	9/27	**6/27**	**85分**
被験者E	8/27	5/27	**5/27**	**98分**
被験者F	10/27	4/27	**4/27**	**82分**

予備実験結果分析

- 正答数
  - GSNを用いたグループではより高い完答数が得られた
  - 0点の被験者が出てしまった
    - GSNの説明不足が原因であったため，GSNについての事前学習が重要である
  - 学生を対象としたため，全体的な正答率は低い

- 回答時間
  - GSN版CBCS安全要求の方が情報量が多いにもかかわらず，
    回答時間は同程度だった

予備実験結果: 被験者感想

- GSN
  - ハザードとの条文の対応付け，安全仕様の記述
    両方に対してGSNを参考にした
  - 自分の記述が正しいかどうかの確認作業に使った
  - GSNによって情報量が増えたことで，混乱してしまった

- 自然言語
  - 曖昧な表現があり，難しかった
  - 解いていくうちになんとなくわかってきた
  - 安全仕様について，どう書けばいいのかわからなかった

今後の予定

- JAXAエンジニアを対象とした本実験
  - 被験者数を増やし，統計的分析を行う
  - 実環境に近い環境での効果を検証する
- CBCS安全要求全体に対する理解の支援
  - 条文ごとのGSNではなく，条文間の関係の理解も含めた支援を行う
  - 条文間で矛盾する記述があるという指摘も存在する
- 合意ゴールの有効性確認
  - 合意を目的としたゴールを設定することによる開発への効果を検証する
  - 合意内容をアシュアランスケースに記述することによる安全審査への効果を検証する

JAXA内業務における適用への期待

- CBCS安全要求を適用した設計・開発の効率化
  - 経験の少ない開発者に対して，CBCS安全要求の理解を支援
  - CBCS安全要求の意図から外れた解釈の防止
- NASA に対する安全審査業務の効率化
  - GSN版CBCS安全要求をテンプレートとして作成した，アシュアランスケースを用いた保証・説明
  - 合意ゴールによる合意内容の共有
- 引き継ぎ業務の効率化
  - どのような解釈・合意がなされていたのかがわかるため，引き継ぎ業務を効率化できる

まとめ

- 背景: 開発者はシステムが一般安全要求を満たすことを保証する必要がある
  - CBCS安全要求は自然言語によって曖昧に記述されており，その解釈は開発者の知識や能力によって変わってしまう
- 提案: GSNを用いてCBCS安全要求を記述することで解釈・開発・審査を支援した
- 結果:
  - 一般安全要求の問題点を「読み取ることが難しい情報」と「システムに依存する情報」に分割した
  - 上記問題点に対応したGSNを構築した
  - CBCS安全要求の条文１２個を実際にGSN化した
  - 予備実験を実施し，本実験への準備を行った