

変化に対応するD-Caseの 補助的な文法の提案

2014年12月19日（金）

奈良先端科学技術大学院大学 高井利憲

東京大学 木藤浩之

（協力 チェンジビジョン）

背景1：確証バイアス

- 米国のシステム安全の専門家であるNancy Levesonがセーフティケースに対する批評を述べた際に用いた概念
 - ▶ 人々は、自分が支持する主張に沿う証拠を集めがち
 - ▶ 人々は、集まった証拠を、自分が支持する主張に沿う意味で解釈しがち
 - ▶ システムが安全であることの証拠は、どんなシステムに対しても任意の数だけ集められる

Nancy Leveson



<http://sunnyday.mit.edu>

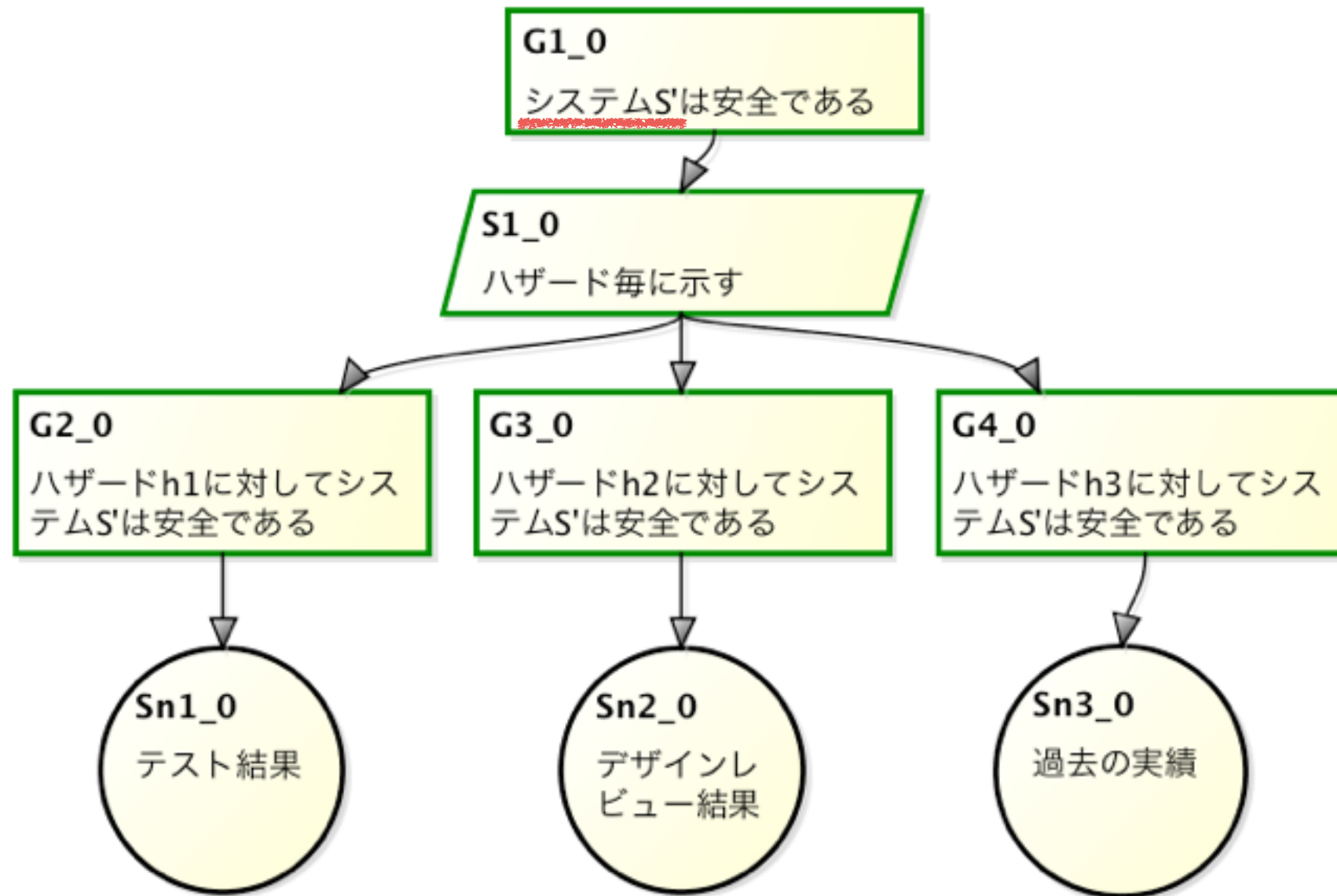
Nimrod accident report



http://news.bbc.co.uk/2/shared/bsp/hi/pdfs/28_10_09_nimrod.pdf

セーフティーケース → リスクケース？

背景2: 変化への対応



- 対象システムやその環境に変更があった場合、原理的にはD-Caseの全てのノードを再レビューする必要がある

現状GSNの表記法の課題

- 刻一刻と変わる状況に対応できない
 - ▶ **トップゴールの変更**は、その影響はD-Case全体に及ぶため**高コスト**
 - ▶ **トレーサビリティ**の維持も**高コスト**
- D-Case変更の記録が残りにくい
 - ▶ **却下された変更案**などは、その情報が残りにくい
- 確証バイアスに陥りやすい
 - ▶ 支持意見は記述しやすいが、**反対意見の系統的な表現方法はない**

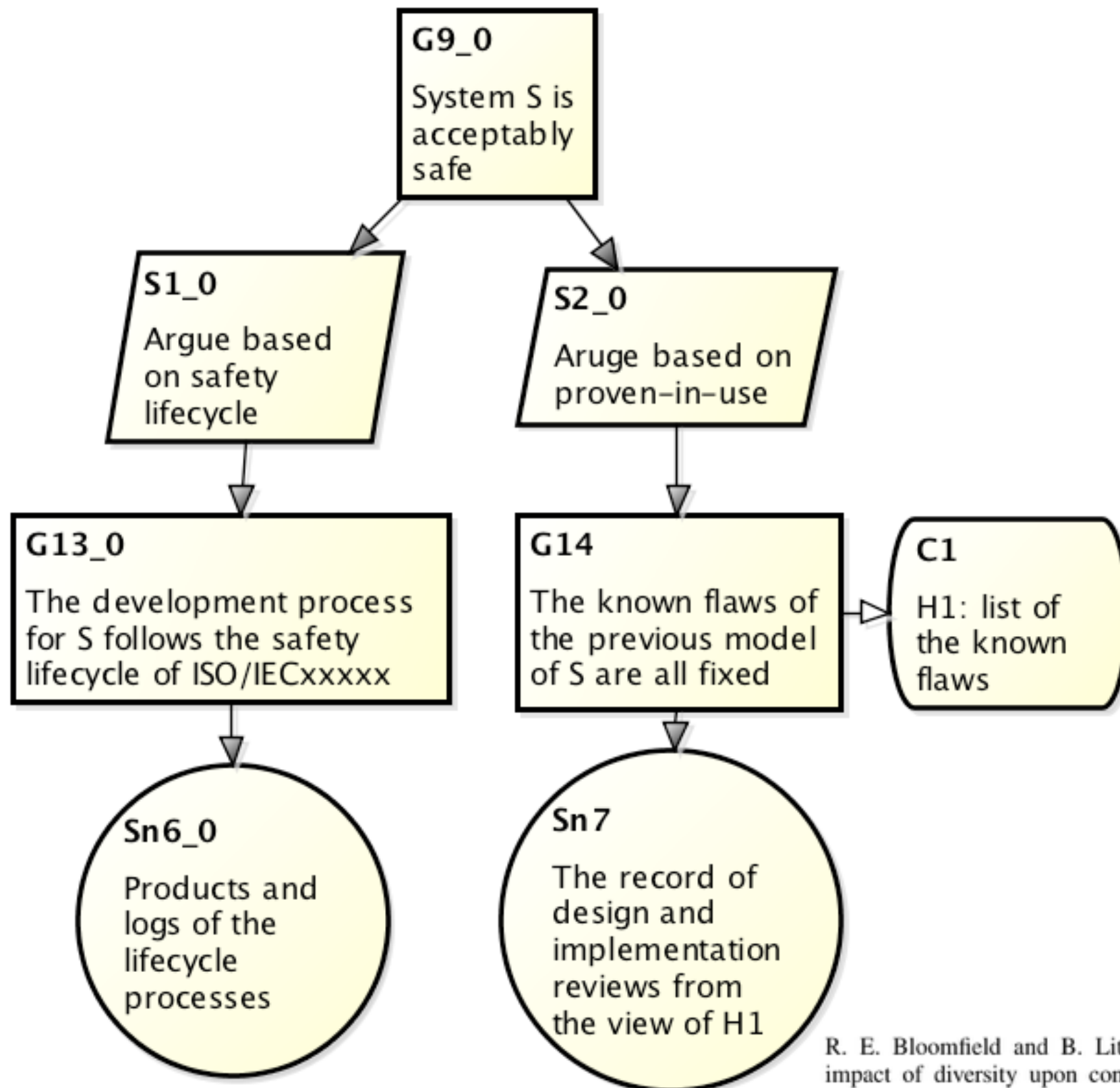


GSNの補助的な表記法を提案

提案表記法の目的

- 反論の系統的な記述方法を与えることにより却下された選択肢などの議論も表現可能なGSNの補助的な文法を提案する
 - ▶ ステップ1: 各ノードにいくつか**属性**を導入
 - ▶ ステップ2: 各ノードにいくつか**状態**を導入
 - ▶ ステップ3: 属性に基づき**状態を決定**する方法を導入

Step 0: 多重議論(multi-legged argument)



R. E. Bloomfield and B. Littlewood, "Multi-legged arguments: The impact of diversity upon confidence in dependability arguments." in *DSN*. IEEE Computer Society, 2003, pp. 25–34. [Online]. Available: <http://dblp.uni-trier.de/db/conf/dsn/dsn2003.html#BloomfieldL03>

Step 1: Goal及びStrategy の属性

● Goal

▶ **Presumption** (通常Goal)

▶ **Except** (例外Goal)

* そのGoalの上のStrategyに対する**例外**の指摘

* **<<except>>**と表示

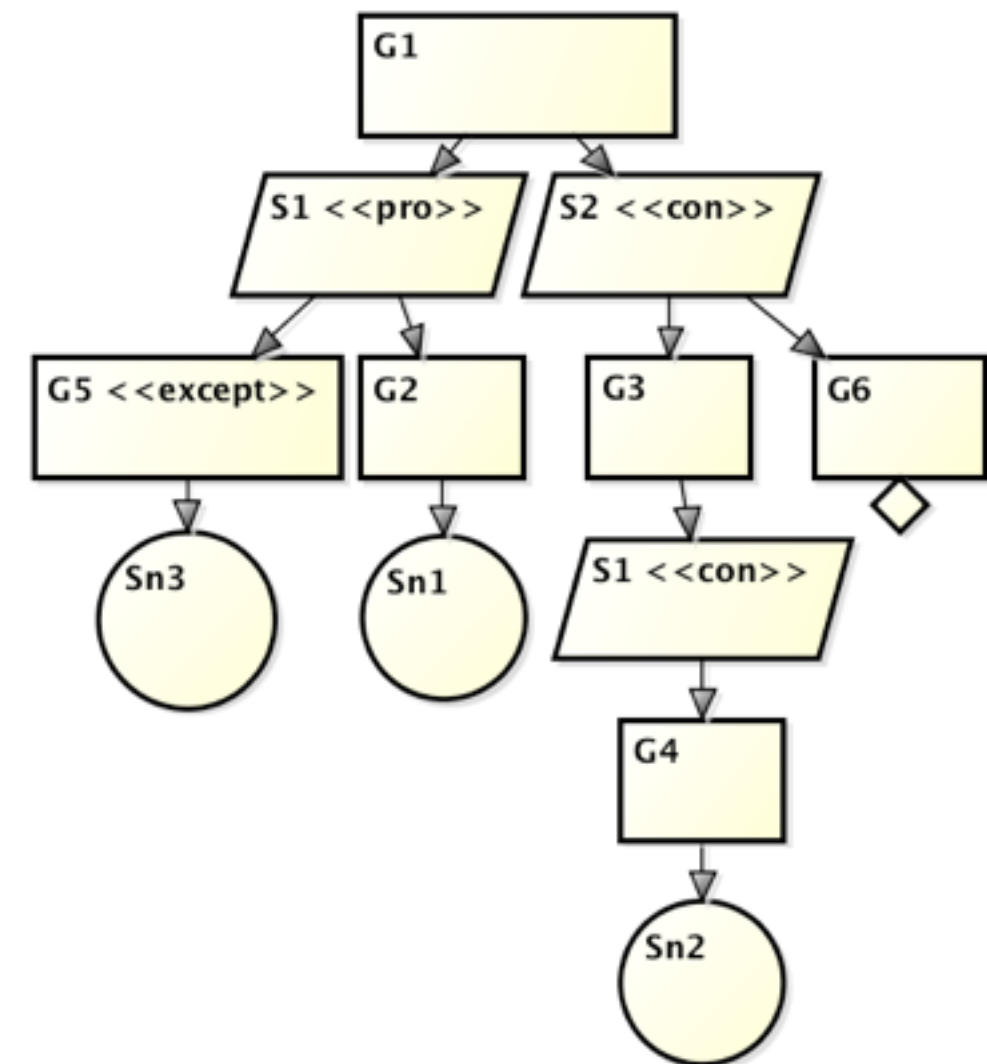
* **反論の表現の一つ**

● Strategy

▶ **Pro** (支持Strategy)

* Goalを支持する論証のStrategy

▶ **Con** (反論Strategy) (次のページへ)



● Strategy

▶ Con (反証Strategy)

- * Goal が**成り立たない**、または、**適切ではない**ことを示す論証のStrategy
- * Goalの**反例**や、**不利な側面**の指摘
- * <<con>>と表示
- * **反論の表現の一つ**

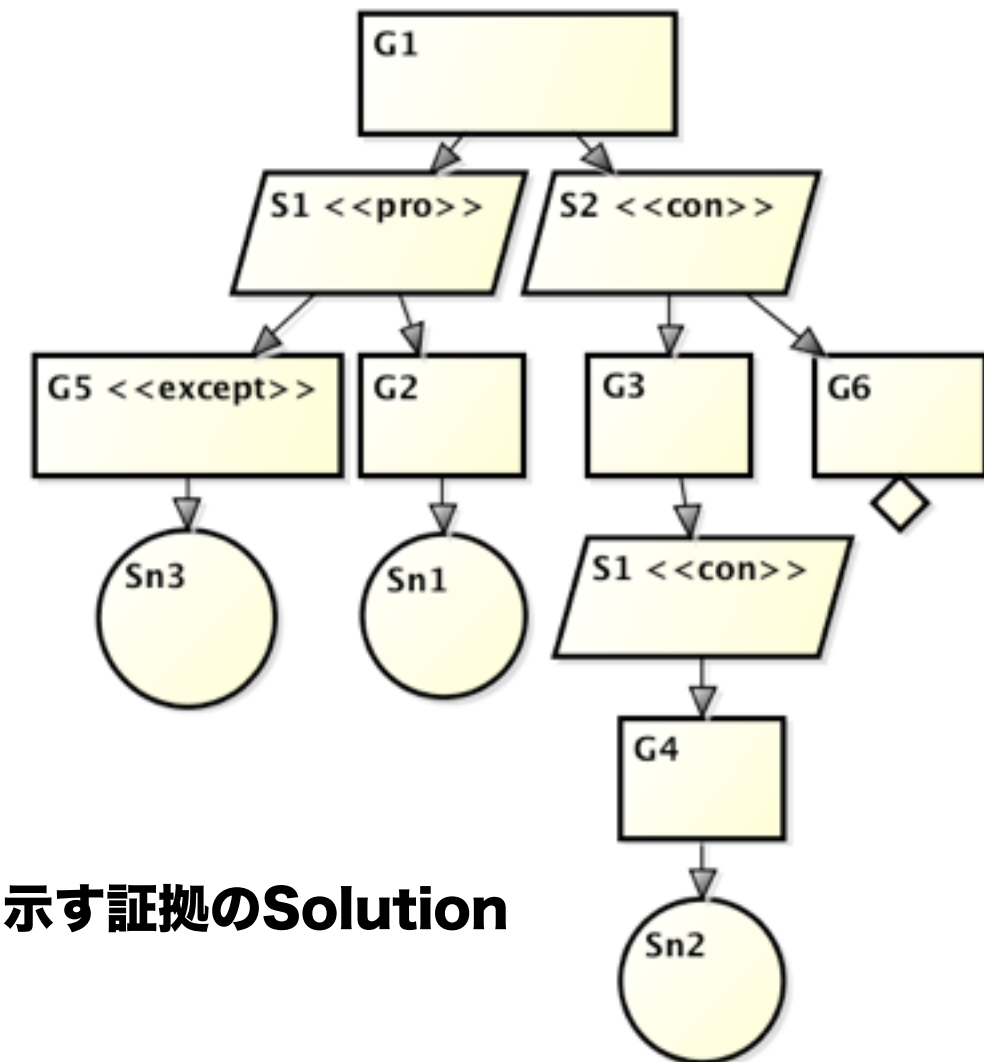
● Solution

▶ Pro (支持Solution)

- * Goalを支持する証拠を表す

▶ Con (反例Solution)

- * Goal が**成り立たない**、または、**適切ではない**ことを示す証拠のSolution
- * Goalの**反例**や、**不利な側面**の指摘
- * <<con>>と表示
- * **反論の表現の一つ**



Step 3: Strategy 及び Goal の状態

● Goal

▶ 受理 (Accepted)

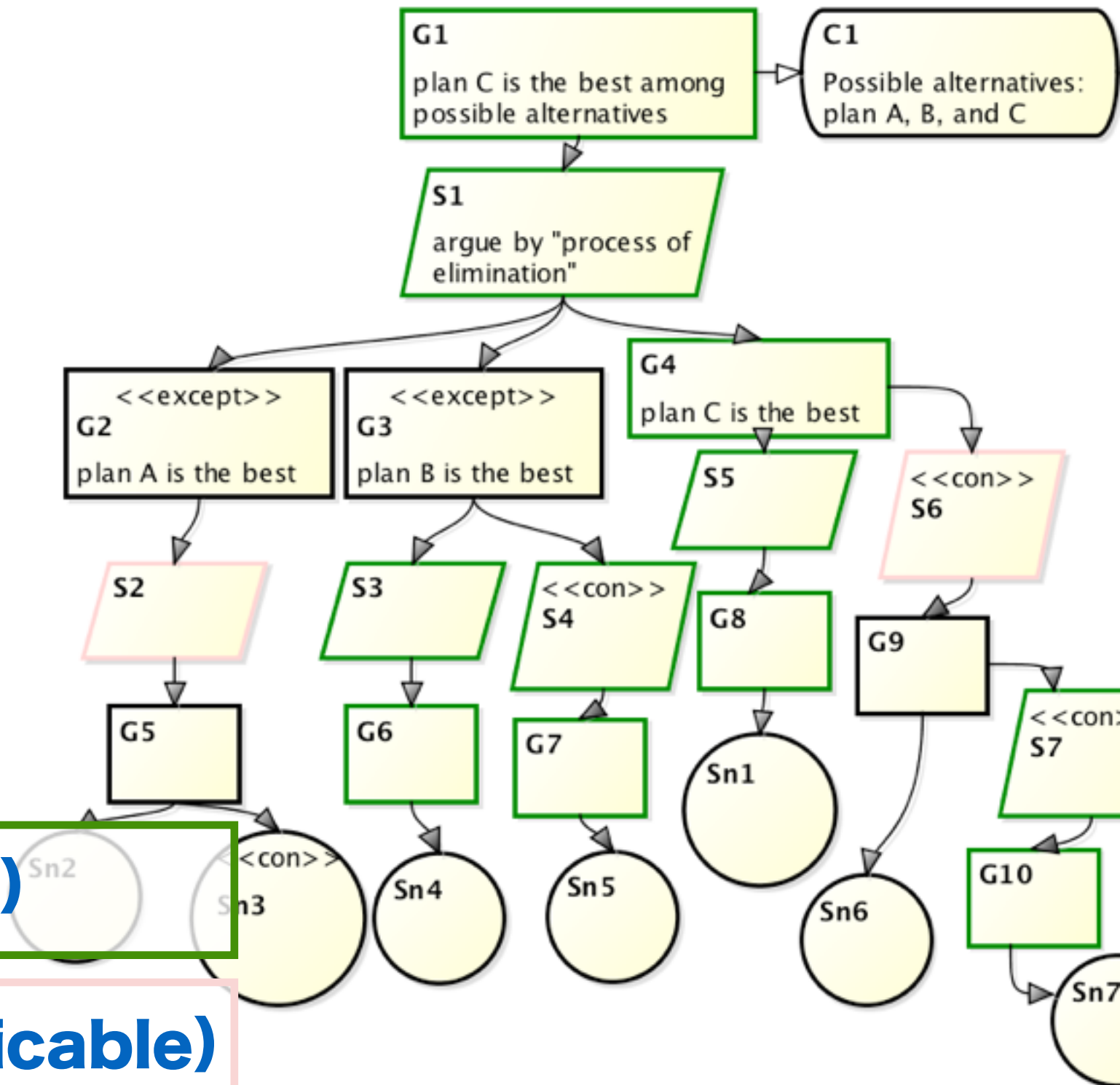
▶ 却下 (Rejected)

▶ 保留 (Stated)

● Strategy

▶ 適用可能 (applicable)

▶ 適用不可能 (not applicable)



Step 3: 状態の決定

● Strategy : 以下の通り

▶ 適用可能

Sub-goalは補題
のようなもの

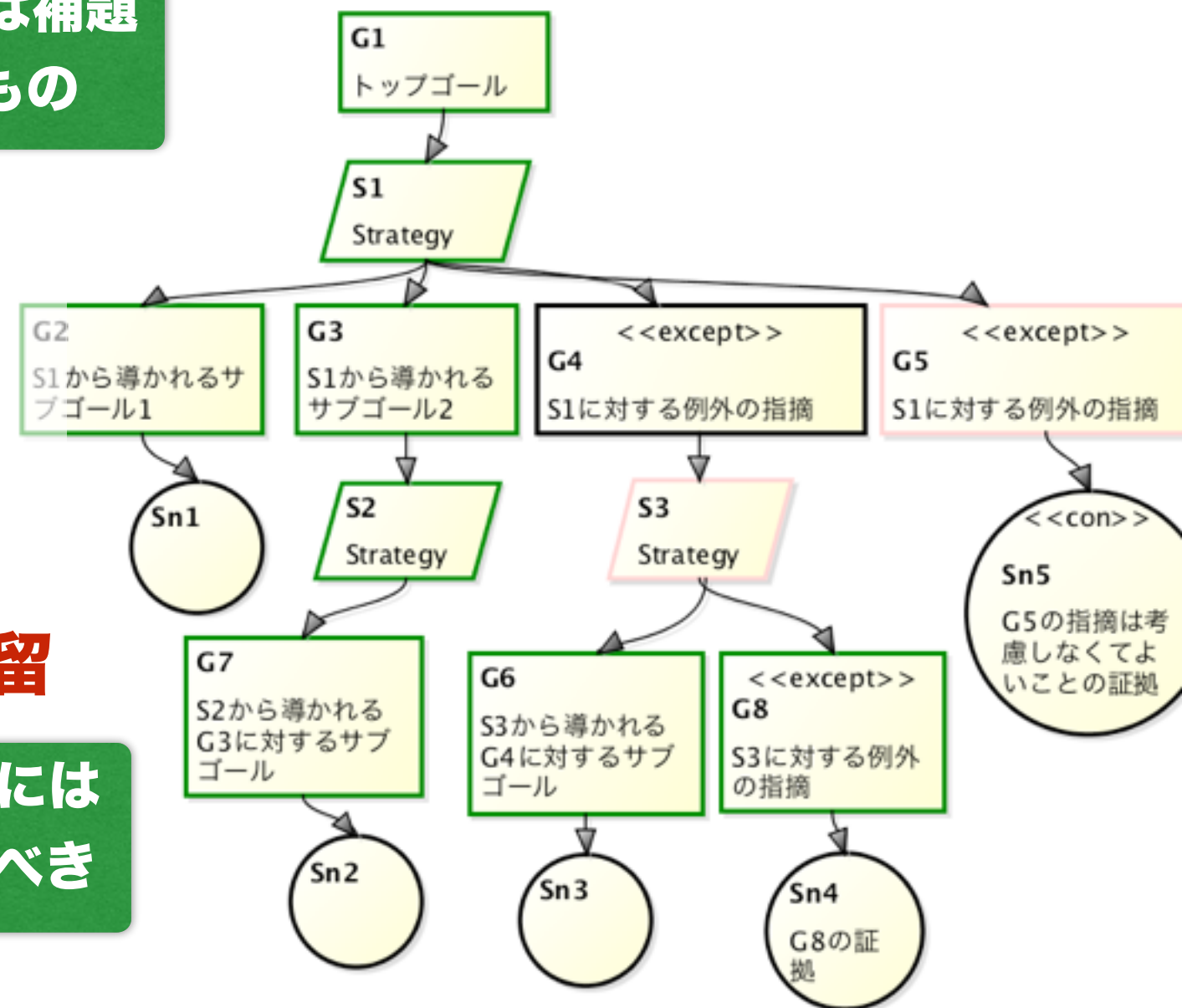
* 全ての通常Goalのsub
Goalが**受理**、かつ

* 全ての例外Goalの
subGoalが**却下**または**保留**

▶ 適用不可

指摘されたことには
全て答えておくべき

* 上記以外



● Goal : 評価基準 (Evaluation Standard) により決定

▶ わずかな立証 (scintilla of evidence)

1. 一つでも適用可能な支持Strategyがあれば受理

▶ 弁証法的妥当性 (dialectical validity)

1. 少なくとも一つ適用可能な支持Strategyをもち

2. 適用可能な反証Strategyがなければ受理

▶ 合理的な疑問の余地のない立証
(beyond a reasonable doubt)

1. 少なくとも一つ適用可能な支持Strategyをもち

2. 適用可能な反証Strategyがなく

3. 提出された支持Strategyがすべて適用可能であれば受理

- 一つのプロジェクト内で統一的な判断基準を与える
- 必要に応じた強さの評価基準を選択可能



<http://www.allmovie.com/movie/v5274>

ユースケース

(1)レビュー記録の構造化

(2)トレードオフや消去法に関する論証

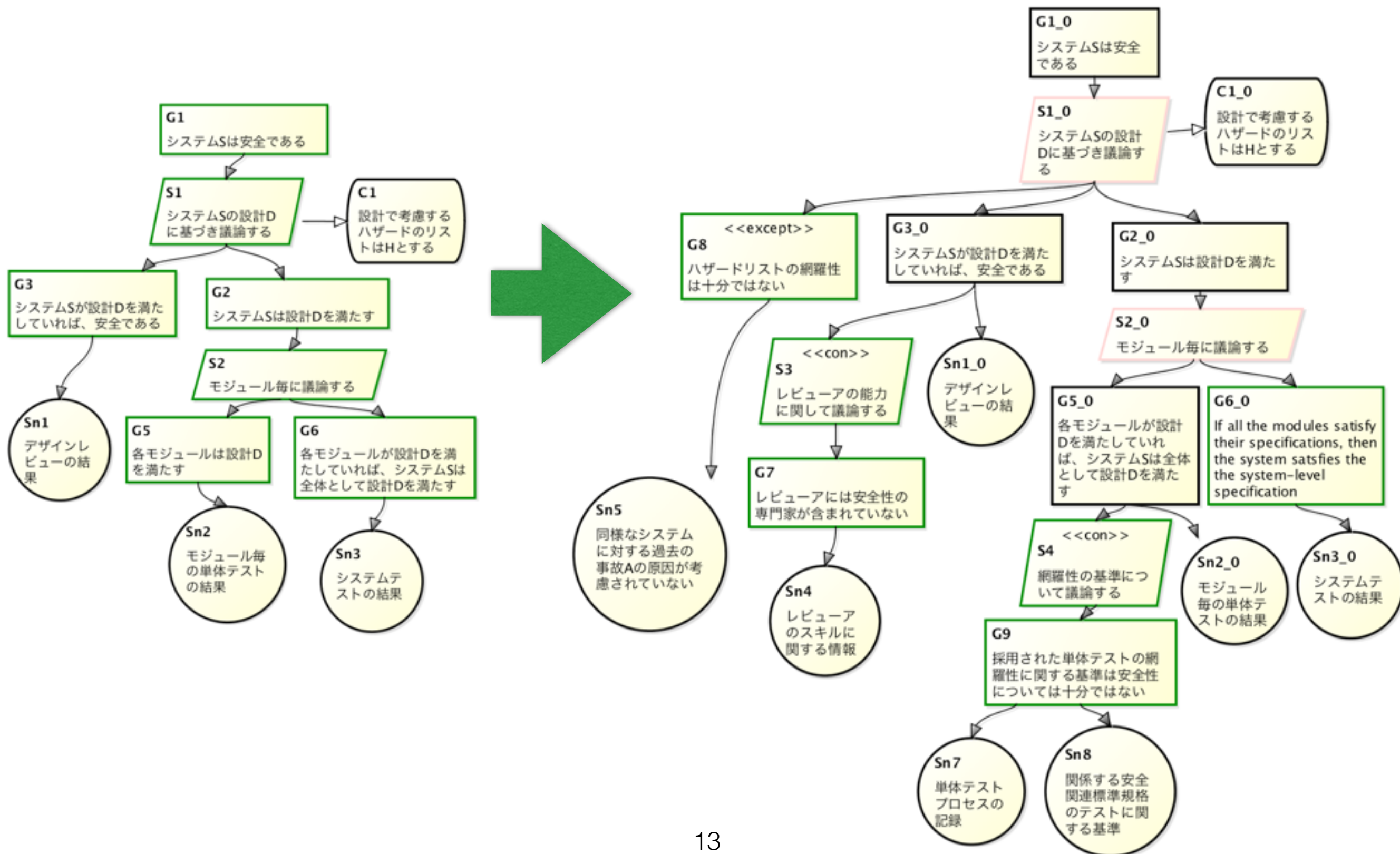
(3)変化への迅速対応

(4)意思決定

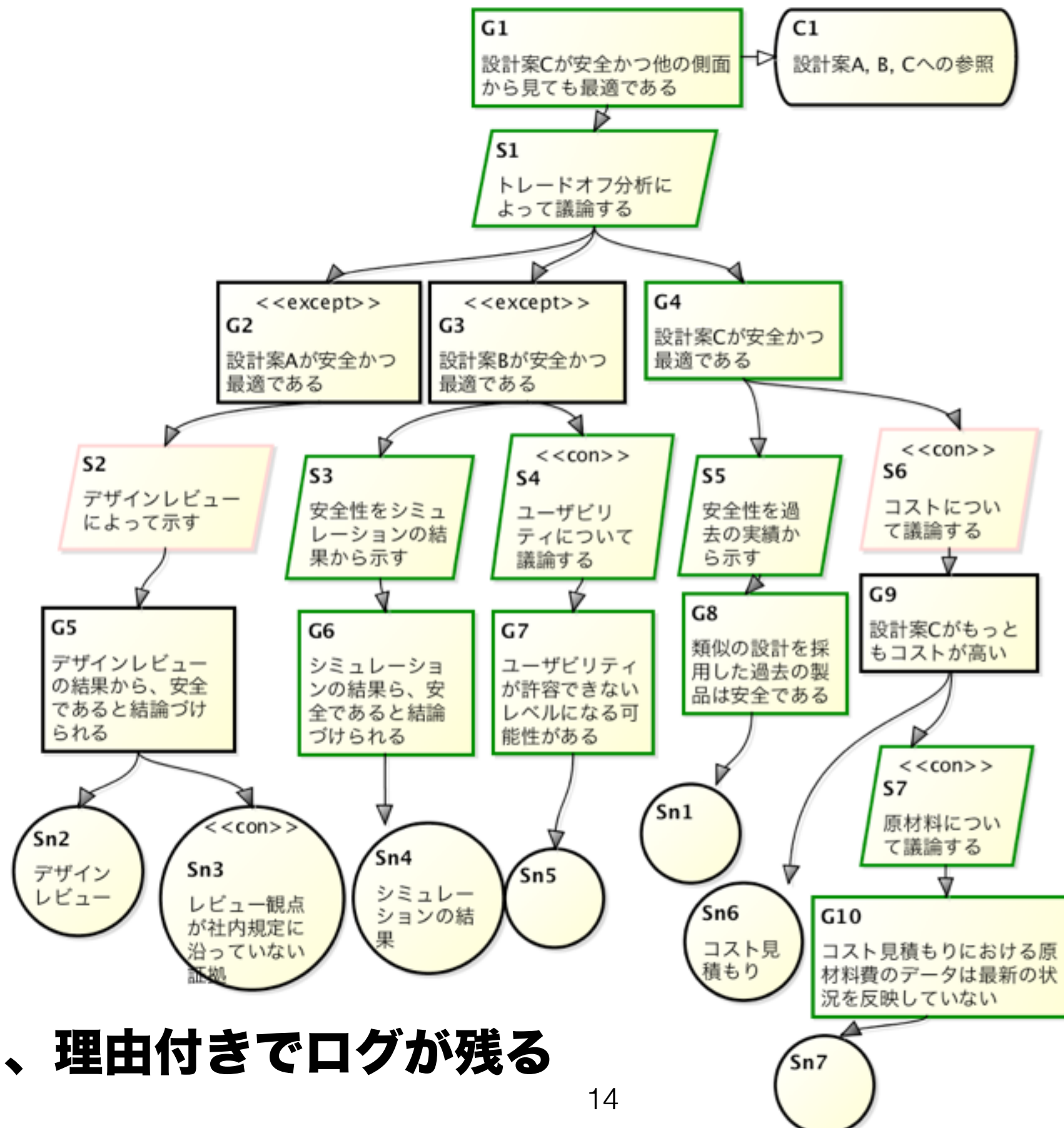
(5)D-Caseの評価

(6)モニターノードとの組み合わせ

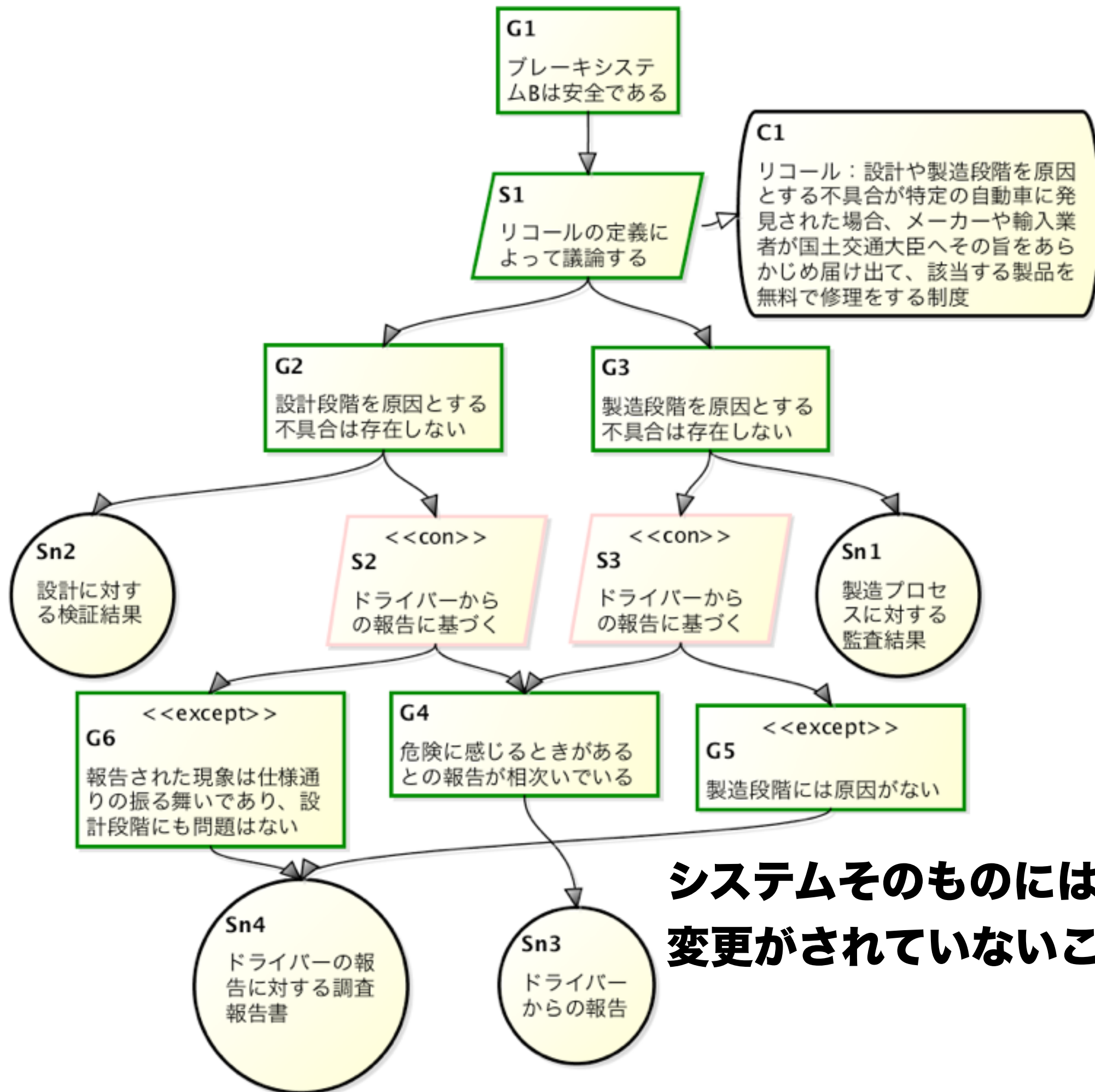
レビュー記録の構造化



トレードオフに関する議論



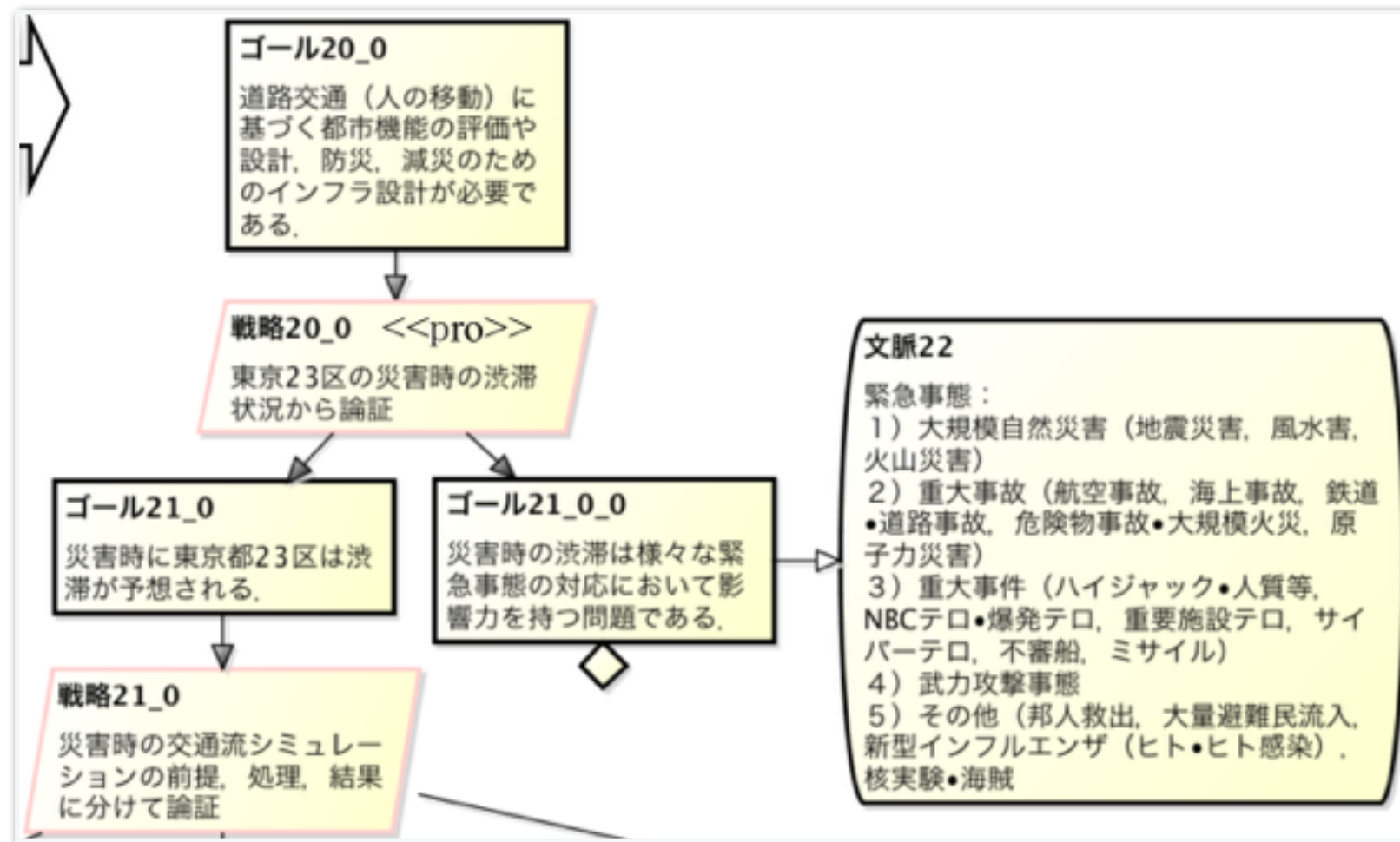
却下案も、理由付きでログが残る



**システムそのものには
変更がされていないことに注意**

政策分野における意思決定

- 東京大学において、防災計画の妥当性確認のため、提案表記法によるケーススタディを実施中(*1)

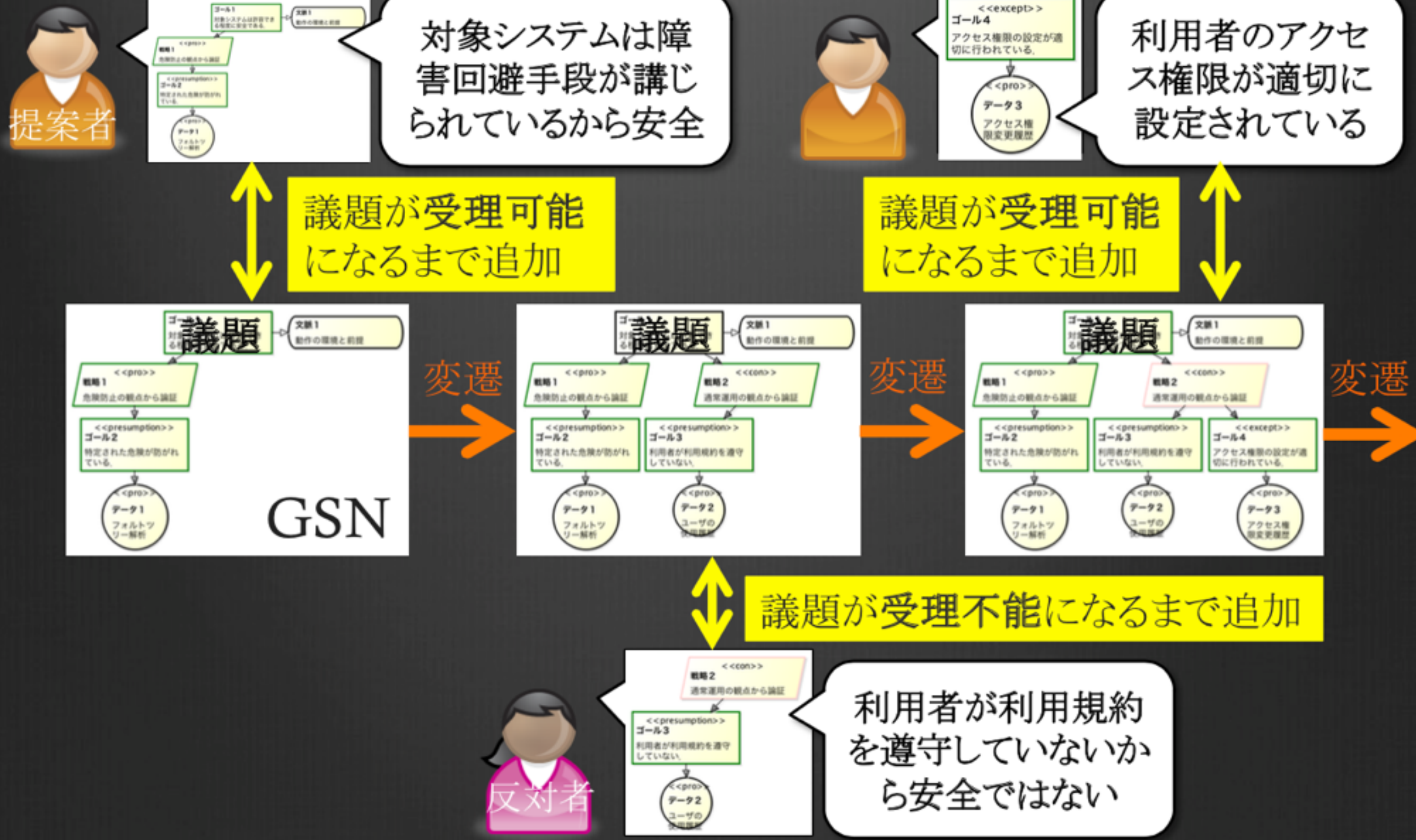


(*1) より引用

- 木藤らはこの中で合意形成をとともなう
議論の構築プロセスを提案中

(*1) 木藤、大澤 “撤回可能付きゴール構造表記法を介したレジリエンス議論の促進”，第6回 システム創成学学術講演会，2014.

(*1) より引用



(*1) 木藤、大澤 “撤回可能付きゴール構造表記法を介したレジリエンス議論の促進”, 第6回 システム創成学学術講演会, 2014.

結論と考察

- **D-Caseに反論を記述可能な補助的表記法を導入(*1)**
 - ▶ **撤回可能付きGSN(defeasible GSN)とよぶ**
- **受理/却下/保留を決定する意味を与えることにより
迅速な変化対応が可能**
- **却下された選択肢も記録できるため
トレードオフや消去法による議論も記述可能**
- **反論を記述できるため、**確証バイアス**を避ける道を提供**
- **評価基準を選択できるため、**D-Caseの系統的な評価法**
与える道を開く**

(*1) Toshinori Takai and Hiroyuki Kido. A supplemental notation of gsn aiming for dealing with changes of assurance cases. In 2014 IEEE International Symposium on Software Reliability Engineering Workshops, Workshop on Open Systems Dependability (WOSD), pages 461–466, Naples, November 2014.

今後の課題と展開

● 課題

- ▶ モニターノードとの組み合わせによるD-Caseの運用プロセスへの応用
- ▶ D-Caseのリファクタリングのタイミングを含むプロセスガイドラインの提供
- ▶ アシュアランスケースの信用度評価への応用
 - * 支持、反証、証拠などの強さの導入
- ▶ 実践的なケーススタディ

● 期待する展開

- ▶ D-Case標準への反映
- ▶ D-Case教育シラバスへの反映