D-Case部会紹介

日本大学理工学部
応用情報工学科
松野裕
matsuno.yutaka@nihon-u.ac.jp

D-Case部会について

- 前身: JST CREST DEOSプロジェクトD-Caseコアチーム
  - 2009-2013
  - CRESTプロジェクト終了後、D-Case部会として活動中
- 目的：合意形成のための手法・ツール
  - 開発・運用を通じたアシュアランスケースによるディペンダビリティ合意形成

現在の参加者、企業

- 松野、高井さん（チェンジビジョン）、
  斎藤さん（ベリサーブ）、越山さん（日産、松野研博士課程）、
  堂向さん（NTTコムウェア）、（大村さん（日産））、
  松野研の学生(2名)
- 共同研究
  - 岡田さん(Tier4)、石川先生(NII)
- NDA手続き中(一社)
  - 要求と仕様の割り当ての手法としてD-Caseを検討

活動内容

- D-Caseに関する研究
  - 年、数本の論文を発表
- D-Caseワークショップ
  - 年に数回程度開催
  - 今年度は４月(Conpassで自由参加)と５月(社内)に開催
  - ベリサーブさんでの社内研修
- D-Caseツール(D-Case Communicator)開発

アシュアランスケース(Assurance Cases)

システム又は製品の特性（安全性、セキュリティ、信頼性、等）に関して、構造化された議論が明示的に、最上位の主張を下位の証拠及び前提条件に結びつけるもの

※そのうち、安全性に関連したものを
セーフティケース(Safety Case)と呼ばれる

セーフティケース、それを想定したGSNの使用は、機能安全、
自動運転開発の分野において推奨されている

- ISO26262
- SOTIF（ISO/PAS 21448, UL4600）

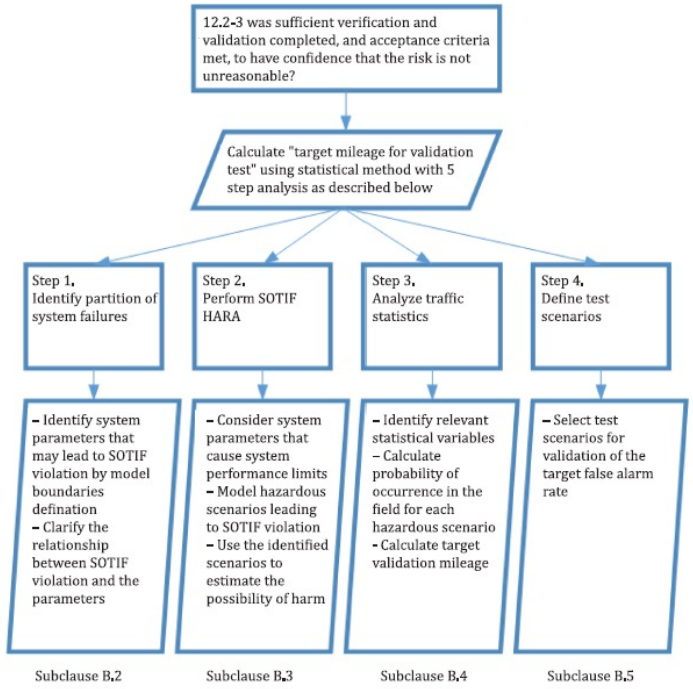


Figure B.1 — Overview of Annex B

ISO/PAS 21448

5.3.1 Interpretation of safety cases

The purpose of a safety case is to provide a clear, comprehensive and defensible argument, supported by evidence, that an item is free from unreasonable risk when operated in an intended context.

The guidance given here focuses on the scope of ISO 26262.

There are three principal elements of a safety case, namely:

— the requirements;

— the argument; and

— the evidence, i.e. ISO 26262 work products.

The relationship between these three elements, in the context of ISO 26262, is depicted in Figure 6.

Figure 6 — Key elements of a safety case (see [2])

5.2.1.3 HIGHLY RECOMMENDED:

a) Use of an established method to organize the safety case in a highly structured manner such as:
   1) OMG Structured Assurance Case Metamodel (SACM)
   2) Goal Structuring Notation (GSN)
   3) Claims Argument Evidence (CAE)
   4) Toulmin Analysis
b) Use of tool support to aid in safety case comprehension and navigation

ISO26262-10 2011

アシュアランスケース～

セーフティケースの事例

トヨタ、940億円で和解　米大規模リコール訴訟

2012/12/27付

保存 共有 印刷 その他

【ニューヨーク=杉本貴司】トヨタ自動車は26日、米国で「意図しない急加速」問題を巡る集団訴訟で、総額11億ドル（約940億円）を支払うことで原告と和解したと発表した。米自動車業界の和解としては史上最高額とみられる。同問題ではトヨタ側に過失がなかったことが証明されているが、訴訟長期化によるイメージ低下を避けるため異例の和解金支払いに踏み切る。今回の和解で大規模リコール（回収・無償修理）に伴う訴訟問題はおおむね決着する。

トヨタは「当社に過失はなかったが、訴訟を続ければ決着までに数年かかるとみられ、その間のイメージ低下を避けるため」に和解に踏み切ったと説明している。

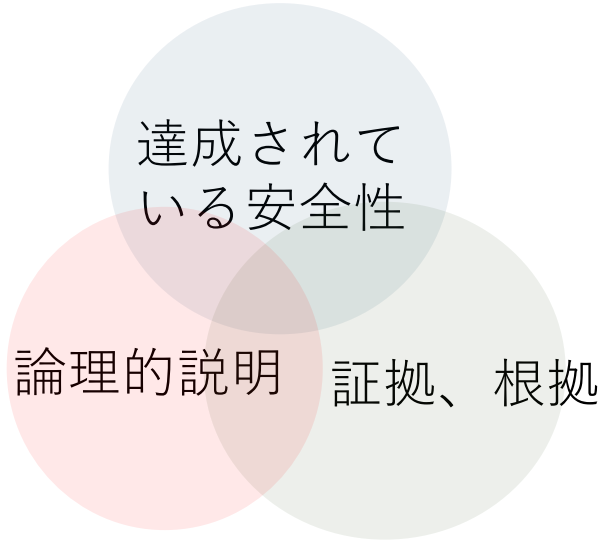
同問題では米運輸省などが当初、エンジンを制御する電子スロットルに問題があるとしたが、その後に米航空宇宙局（NASA）などの調査でトヨタ車に過失がなかったことが証明されている。トヨタも当初から過失を否定していたが、原告は一連の騒動で「車の価値が下落した」としてトヨタを訴えた。

トヨタは原告への支払いのほか、実際に車を売却したユーザーに下取り価格の下落分を補償費として支払う。安全対策としてブレーキとアクセルを同時に踏んだ場合にブレーキを優先するシステムも搭載する。11億ドルはこれらの合計額。

米国での大規模リコールに伴う集団訴訟は大きく3件。「トヨタの情報開示が問題で株価が下落した」とする投資家との間では和解が成立済み。残る訴訟は電子スロットルそのものに欠陥があるとするもので、トヨタは引き続き争う構え。当局から「シロ」判定を受けていることから敗訴になる可能性は低いと考えられている。

日本経済新聞
https://www.nikkei.com/article/DGXNASGM2700M_X21C12A2MM0000/

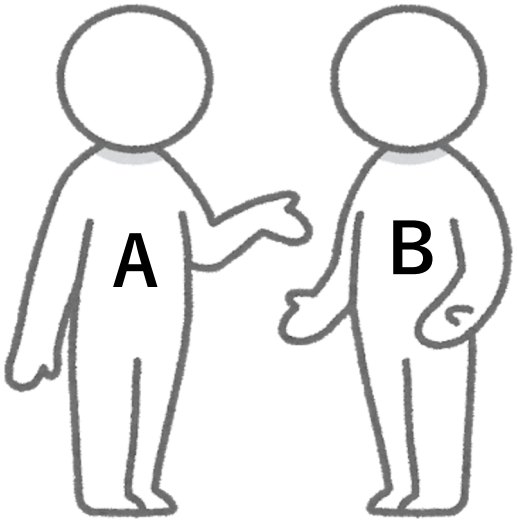
自動車のスロットル制御システム

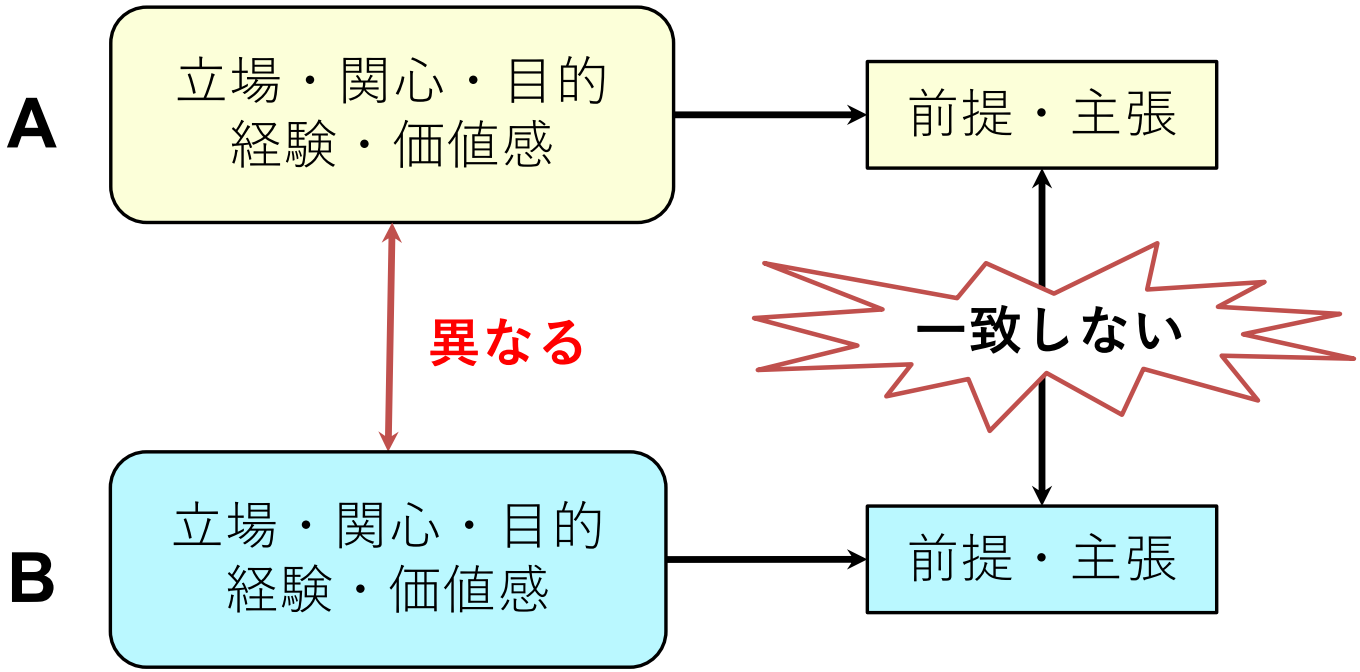


それらを明確に用意できていれば、もっと簡単に解決していた（*かもしれない*）

セーフティケースの重要性

D-Case目的: (ミニマムの)合意形成

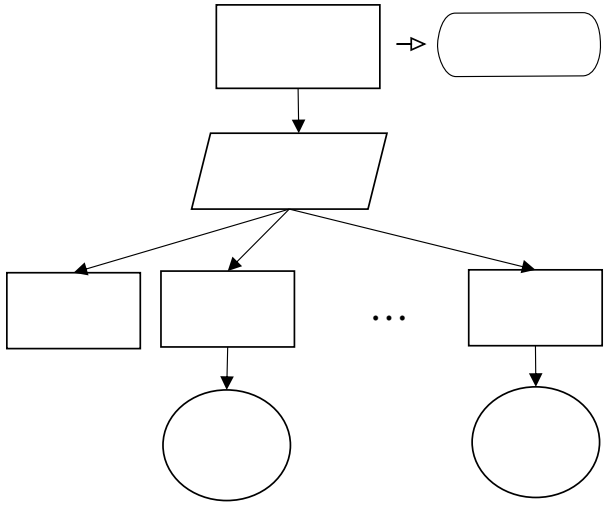




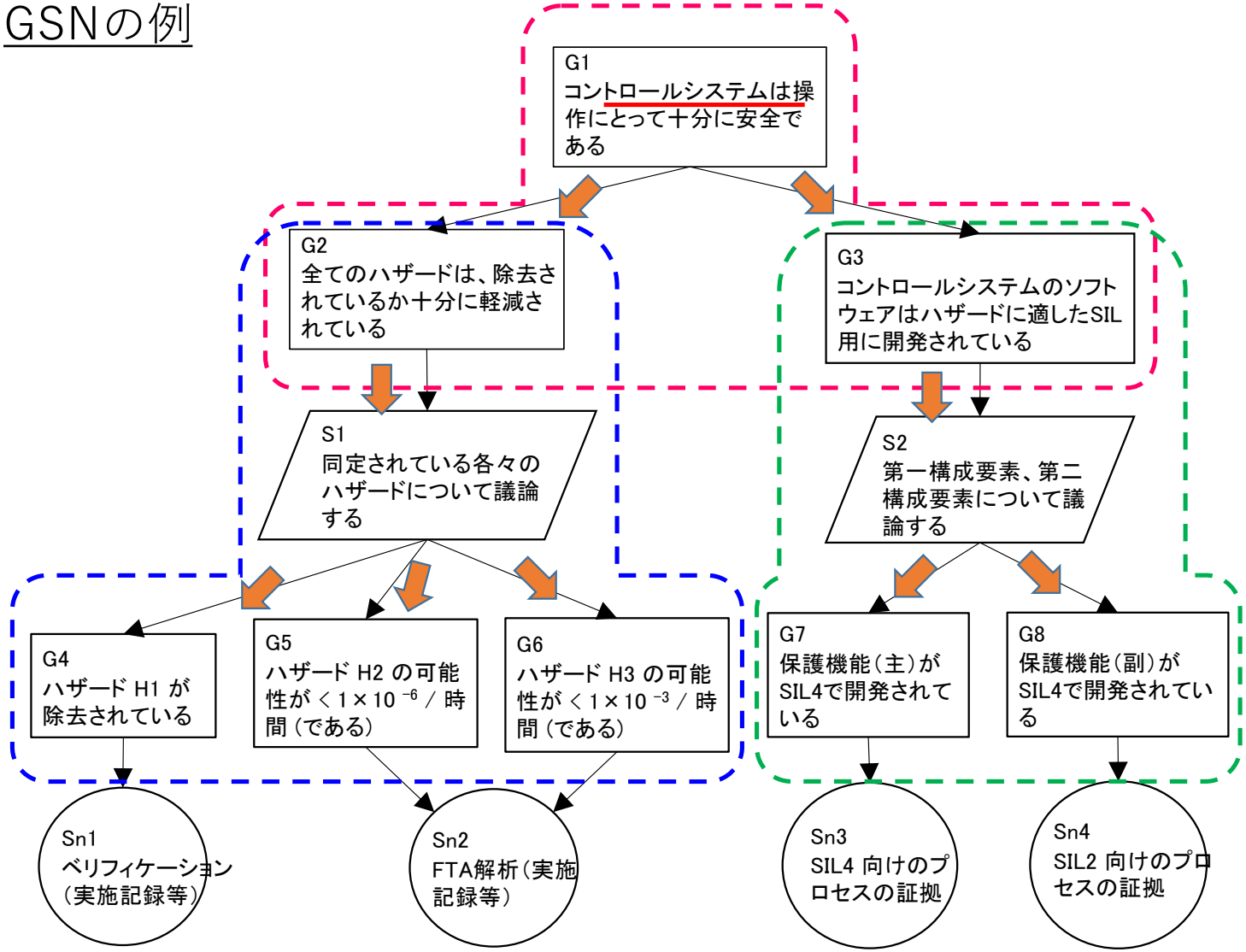
前提・主張を一致させる
→ 合意形成

GSN（Goal Structuring Notation）
アシュアランスケースの表記法の一つ
D-Caseでベースとして使う

・木構造である
・各要素は自然言語を用いて表現される



GSNの例



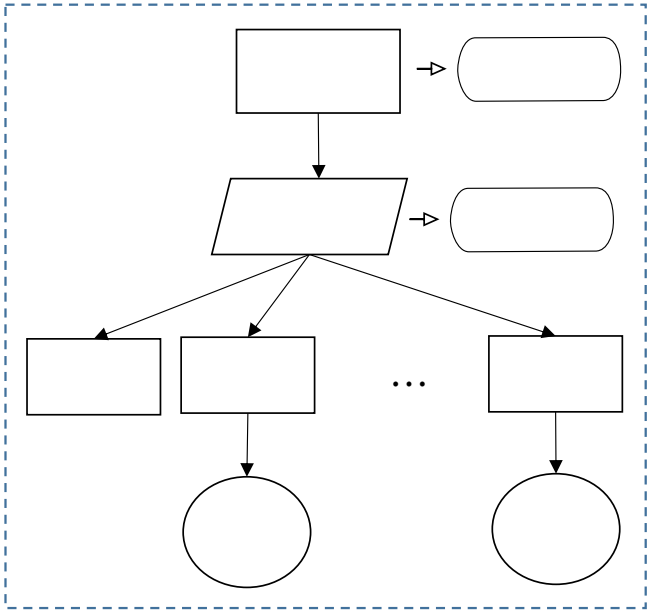
対象の分割、変換

階層的に詳細化し、説明している

John Rushby, The Interpretation and Evaluation of Assurance Cases

D-Caseの基本的な考え方

- GSN自体は基本的な構造、大きすぎないようにする
- コンテキストに要求分析結果、安全分析結果、テスト結果などのドキュメントをおく
- GSN自体は様々なドキュメントを紐付ける論理的な骨組みにとどめる
- 他のドキュメントがあれば、GSN自体はすぐ作れる（ようにする）



論証 before/after: before

- システムは安全です
  - リスク分析と試験は十分実施しました

機能	故障モード	故障シート	原因	直接の影響	システム全体への影響	検出の方法	現在の制御	ハザード	リスク	勧告
衝突緩和制動	指示の失敗	N/A	コンピュータ ソフトウェア 配線	衝突緩和制動	衝突回避を下げたまま飛行	センサー		衝突による ダメージ	4C	
	早まって指示	N/A	コンピュータ	もし衝突緩和が下がっていれば、衝突緩和が早まって上がる	地上走行や離陸時に衝突緩和が上がる	センサー		地上走行時 にダメージ	2C	
			ソフトウェア							
衝突緩和制動	指示の失敗	N/A	コンピュータ ソフトウェア 配線	衝突緩和を下げることができない	航空機は、衝突緩和をあげたまま、着陸しなければならない	センサー		衝突時のダメージ又は損失	2C	
	早まった指示	N/A	コンピュータ ソフトウェア	もし衝突緩和が上がっていれば、衝突緩和が早まって下がる	着陸装置を下げたまま飛行	センサー		墜落による ダメージ	2C	
組込み試験	実施の失敗	N/A	コンピュータ ソフトウェア 電気系統の故障	衝突緩和の故障の未検出	使用したとき、警告無しで、操縦または誤解をしない	なし		取り得るお安全な状態	4C	
	誤って実施される	N/A	コンピュータ ソフトウェア 電気系統の故障	組込み試験のデータ不正	警告無しまたは、着陸装置の状態に応じた誤った警告	なし		取り得るお安全な状態	4C	
システム導器の制御	実施の失敗	N/A	コンピュータ ソフトウェア 電気系統の故障	組込み試験のデータが報告されない	障害状態を警告しない	パイロットによる検出		なし	4D	
	誤って実施される	N/A	コンピュータ ソフトウェア 電気系統の故障	組込み試験のデータが誤って報告される	障害状態を警告しない、または、誤った警告を発する	パイロットによる検出		なし	4D	
組込み試験の結果の記録	実施の失敗	N/A	コンピュータ ソフトウェア 電気系統の故障	組込み試験のデータが記録されない	障害状態を記録しない	データ分析		なし	4D	
	誤って実施される	N/A	コンピュータ ソフトウェア 電気系統の故障	組込み試験のデータが誤って記録される	障害状態を記録しない、または、誤って記録する	データ分析		なし	4D	

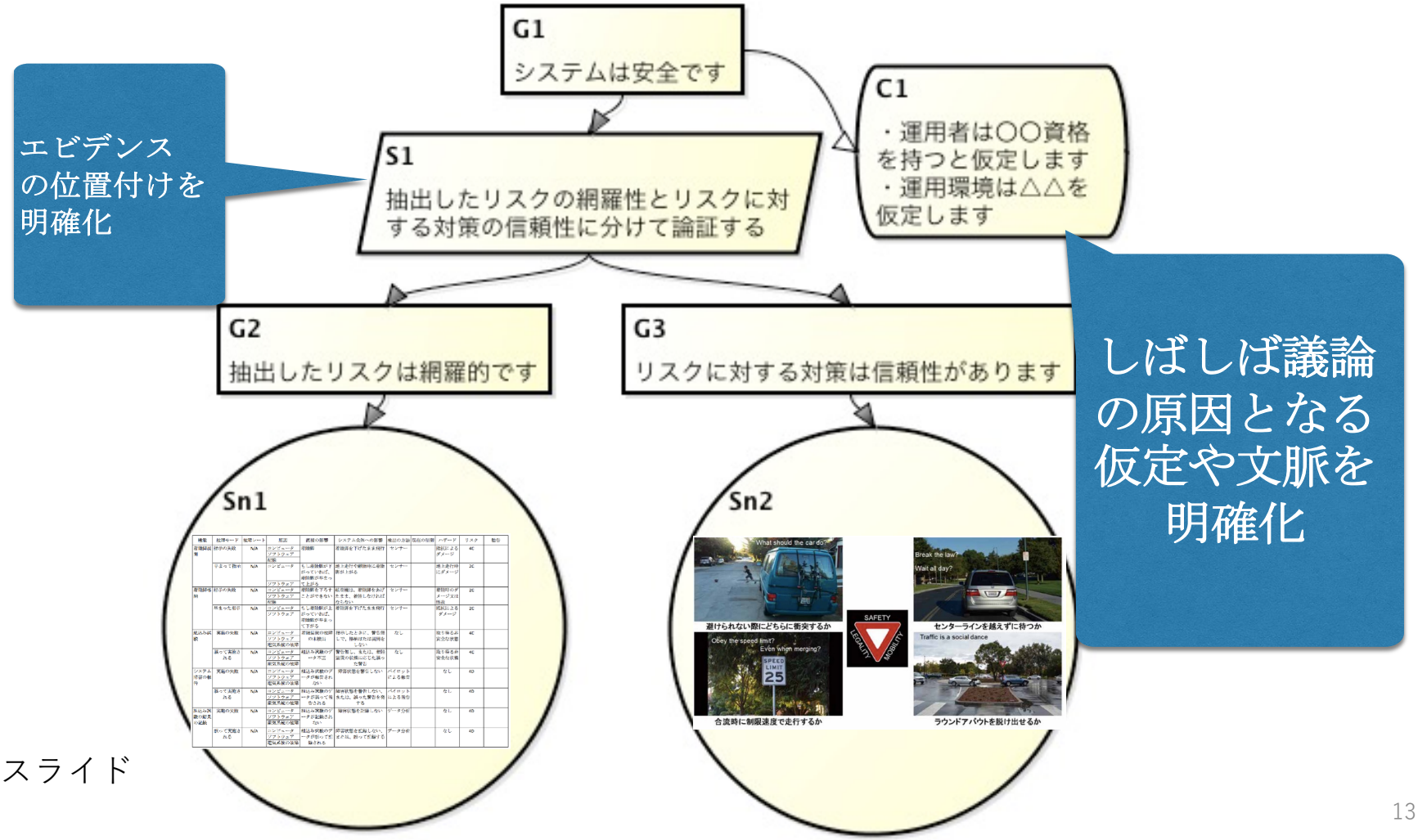
リスク分析結果

試験結果

高井さんのスライド

http://www.its-jp.org/wp-content/uploads/2015/03/World-ITS-initiatives_2016.pdf

論証 before/after: after



高井さんのスライド

Conpassでの D-Case ワークショップ （社会人博士の越山さん）

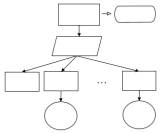
Connpassを使い一般公募（15名　参加）

説明と演習の様子（ワークショップ#2）

全体説明

GSN（Goal Structuring Notation）とは …

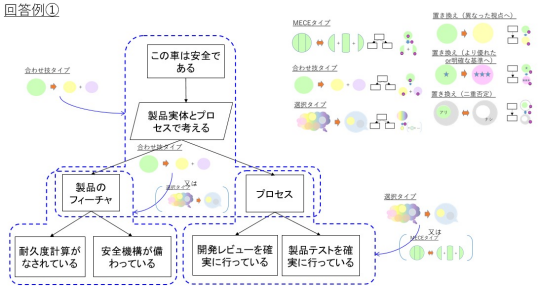
・木構造の構造化言語である。
・各要素は「自然言語」を用いて表現される



各要素（自然言語）どうしの関係を論理的に示すことができる。

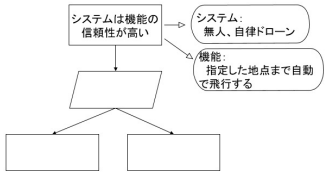
全体演習

回答例①



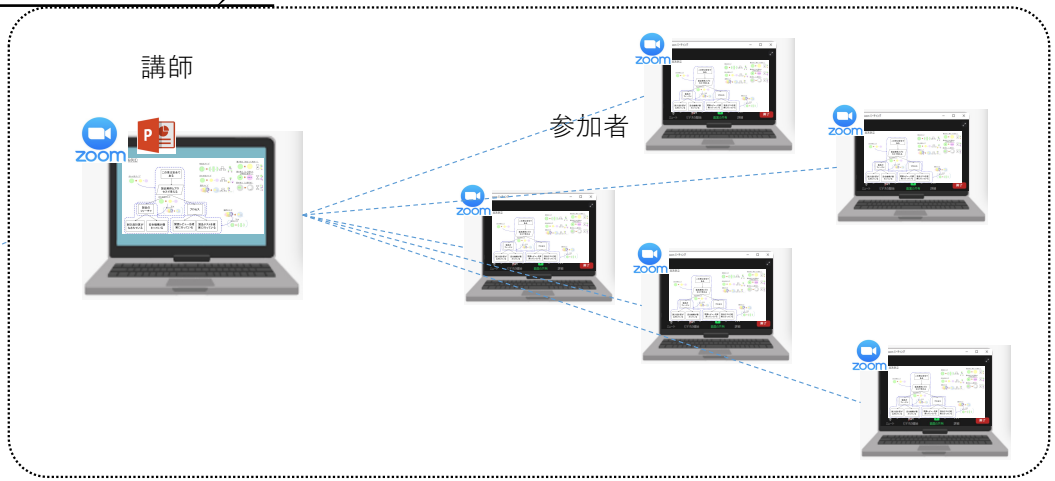
個別演習

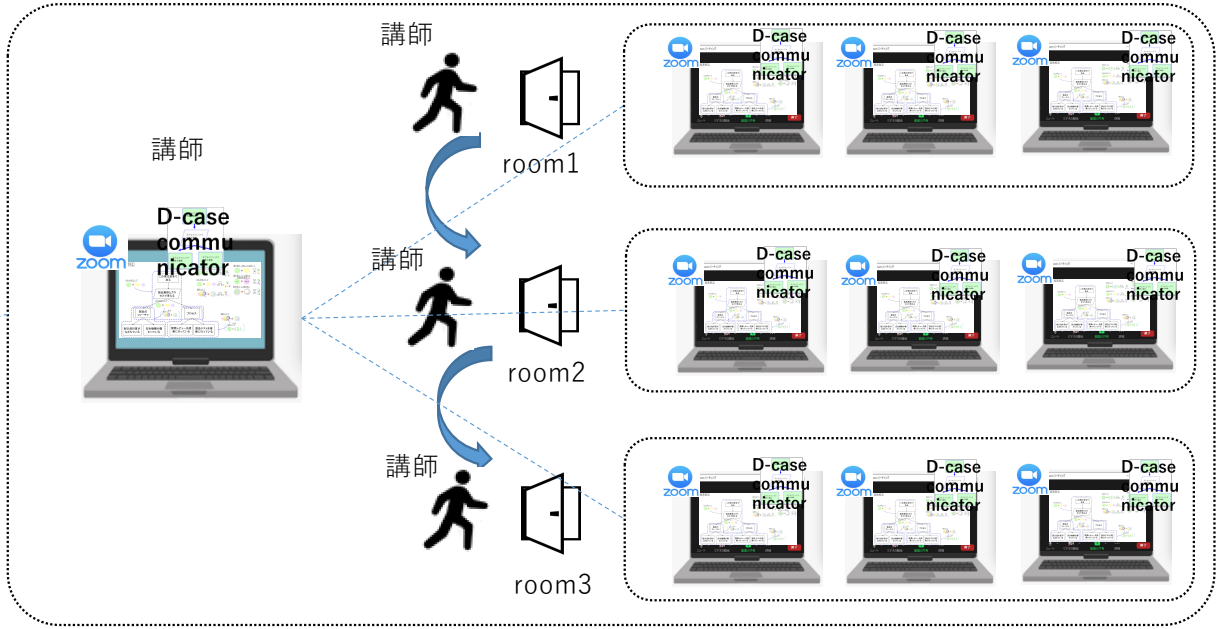
・次のGSNのサブゴールを完成させてください。
・６パターンのいずれかが当てはまるかを考えてみてください。



サブゴールの数は追加してもかまいません。
パターンは当てはまるだけ、挙げてください。

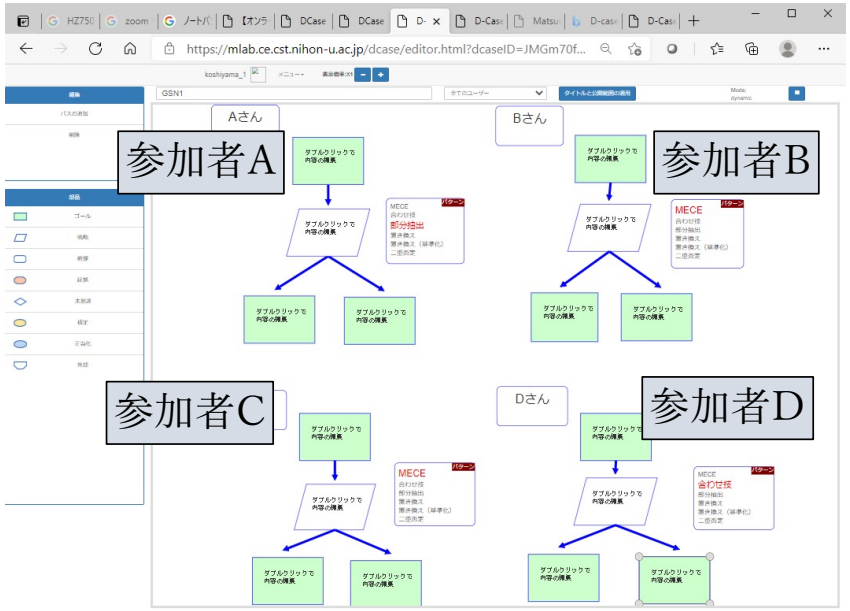
（個別演習 ＝グループ演習）

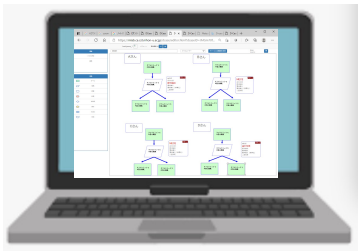


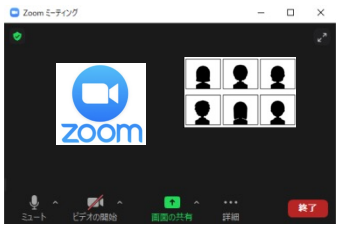


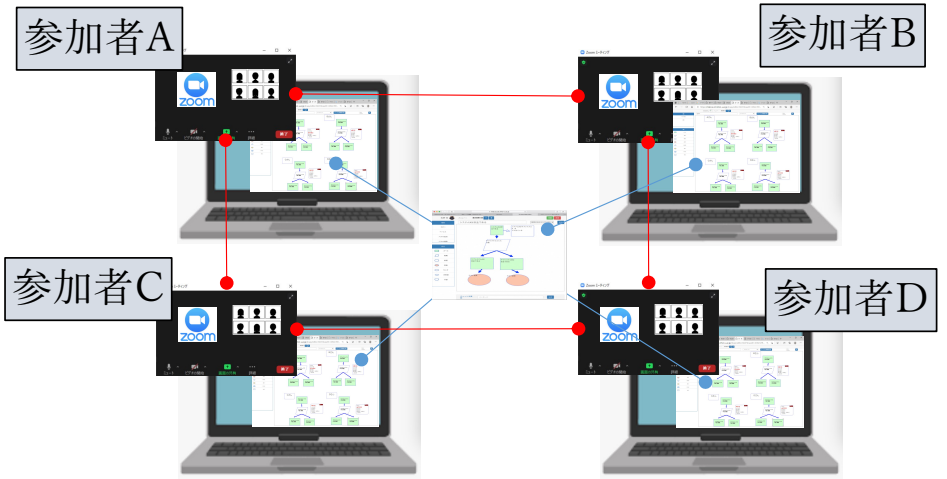
グループ演習の様子（ワークショップ#2）

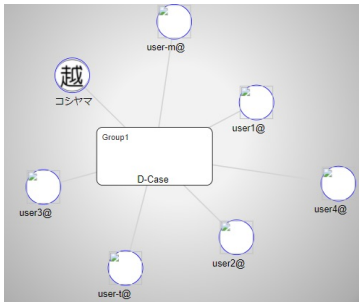
あるグループ内の様子











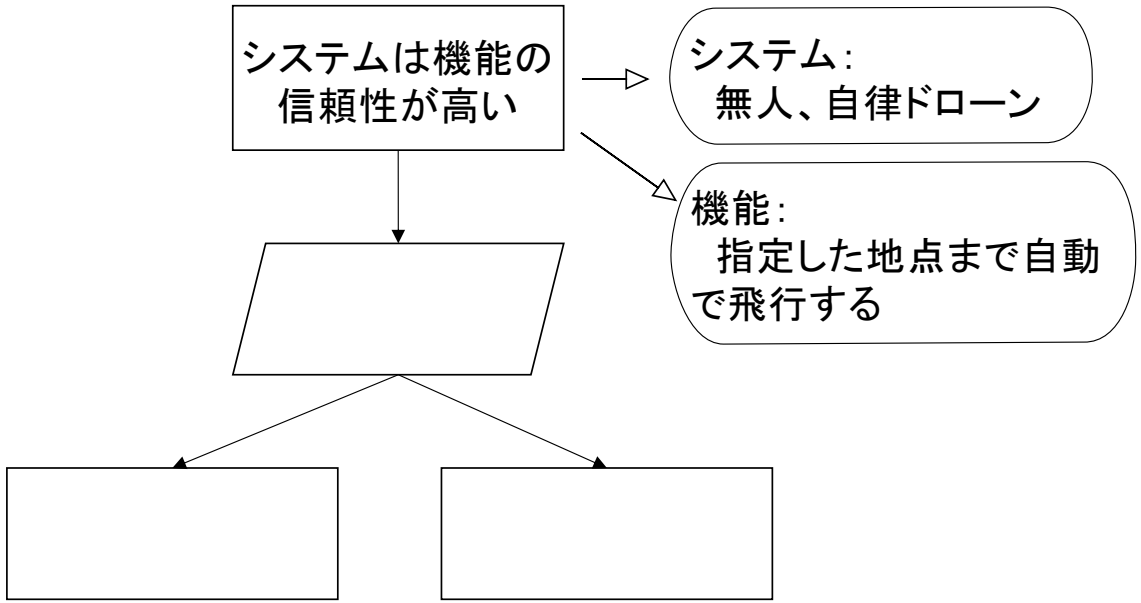
D-Case Communicator http://mlab.ce.cst.nihon-u.ac.jp/project/dcomm/

ワークショップ演習
（６パターンは、越山さんが提案しているGSNパターン）

・次のGSNのサブゴールを完成させてください。
・６パターンのいずれかが当てはまるかを考えてみてください。

（30分間）

（2~3階層程度が目安）

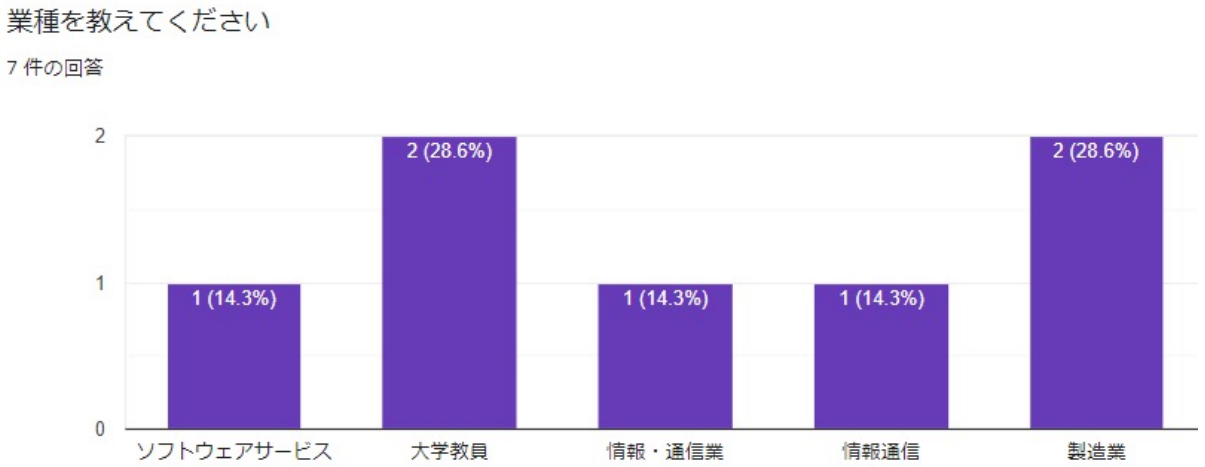


サブゴールの数は追加してもかまいません。
パターンは当てはまるだけ、挙げてください。

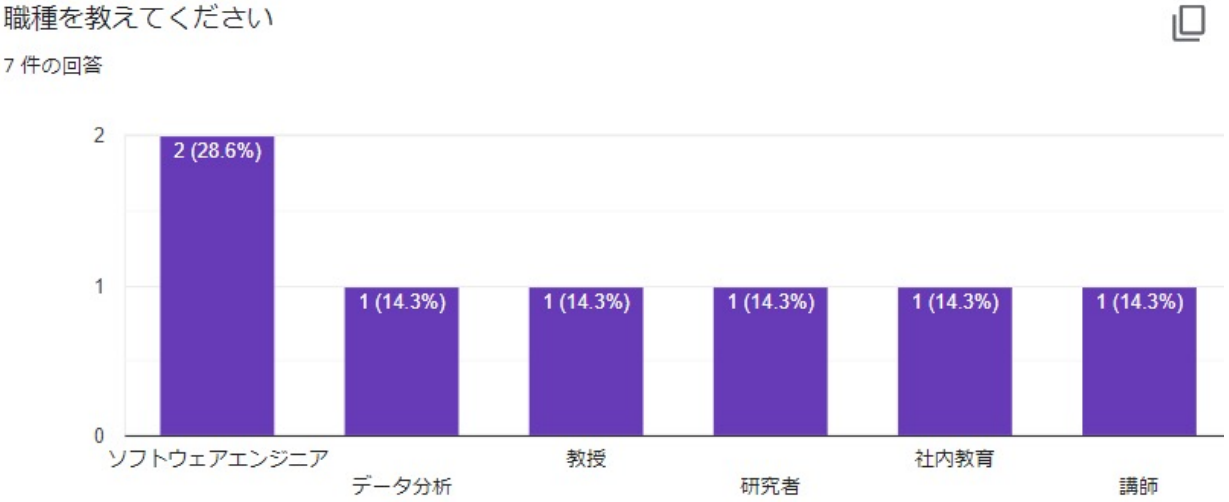
コンテキストも適宜使用してください。

アンケート結果

設問1)



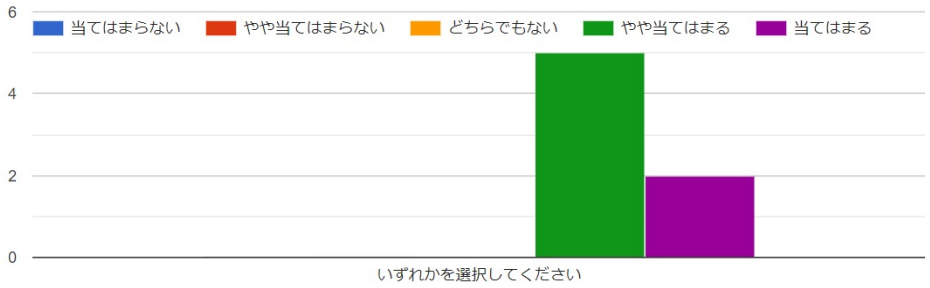
設問2)



アンケート結果

設問3)

説明はわかりやすかったですか？



設問4)

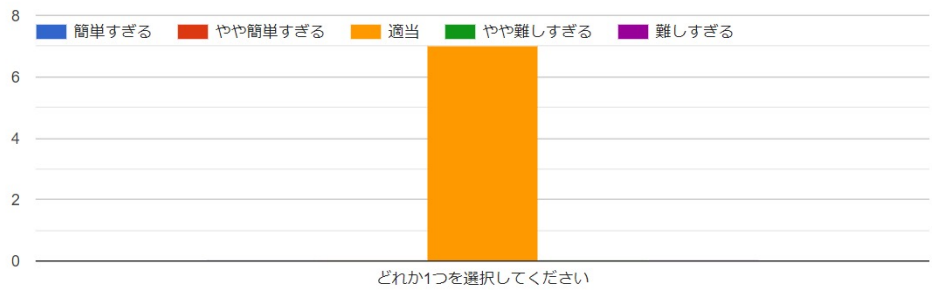
説明について分かり易かった（又は分かりづらかった）点を具体的に教えてください。

3 件の回答

- PPTは最初にいただけると有難いです
- 最初は漠然としていましたが、実際に全体演習、その後個別演習になったことで、具体的なイメージがつきやすくなりました。
- 最初、パターンを理解するのに時間がかかった

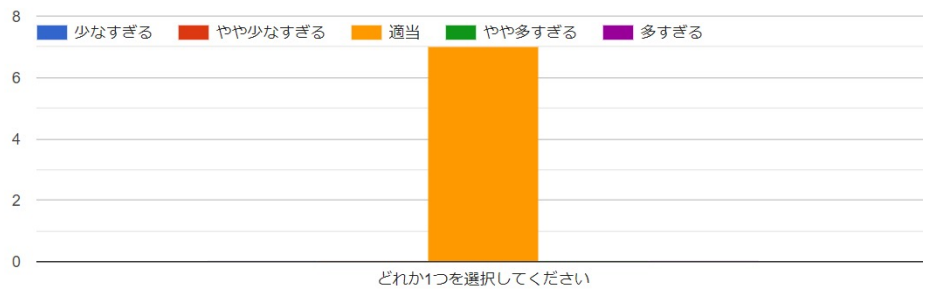
設問5)

演習の難易度はいかがでしたか？



設問6)

演習の量はいかがでしたか？



アンケート結果

設問13)

全体を通して、ご意見ご感想等がありましたらお願いします。

5 件の回答

参加してよかったです。QAML経由です。

GSN自体を初耳の状態で参加しましたが、概要はよくわかりました。信頼性を重視したソフトウェア開発を行う予定なので、実践してみたいと思います。ありがとうございます。

わかりやすい説明でした。演習があってよかったです。ゴール分割にはORがあるのですね。１６枚目のスライドではAND分割しかないように見えたので奇異に思っていました。どうも有難うございます。

MECEは簡単なようで難しい
GSNの知識更新ができました。ありがとうございました。

このような講習は初めて参加しましたが、演習を通してイメージがつきやすくなりました。また、演習に対して個別に解説をしてくださったことで、自分の理解度がわかり、勉強になりました。ありがとうございました。

ベリサーブさんでのD-Case研修

合意形成研修の概要

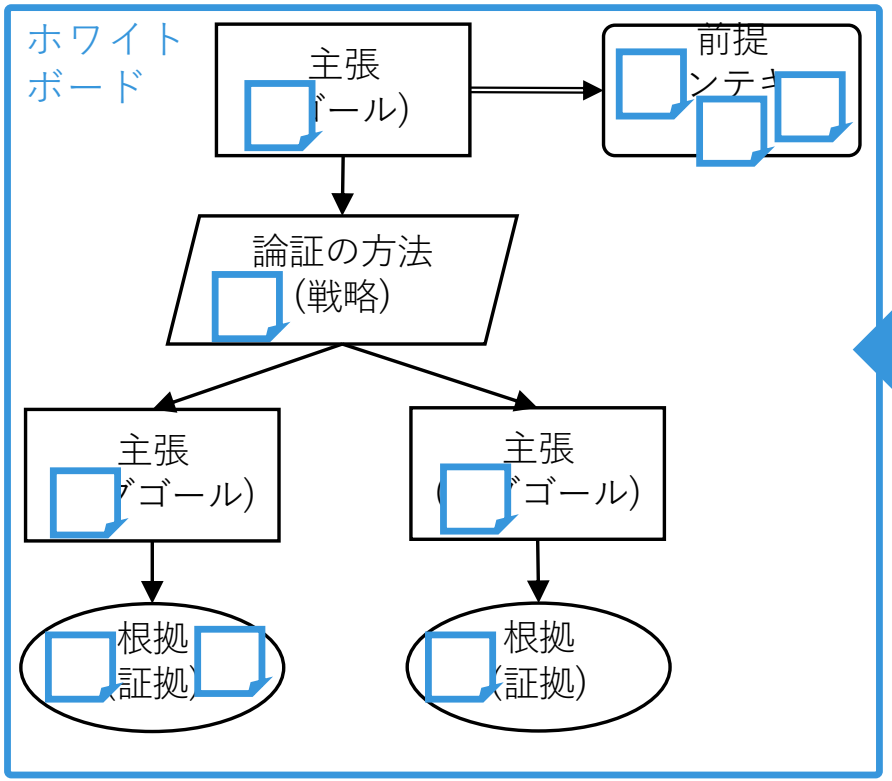
VERISERVE

- **実施日：2021/05/27**
- **研修時間：16:00～21:00 5時間**
- **参加者：9名（当日1名欠席のため）**
- **講師：講師1名、TA1名、運営側2名**
- **実施形態：オンライン（Zoom）**
  - 初めてのオンライン（試行的なことも含め）のため、人数制限（10人）で開催
  - 導入編は、講義＋練習（D-Caseステンシルを用いたD-Case作成の練習）
  - 演習編は、講義＋チーム演習（ブレークアウトセッションでの2チームで実施）
    - 講師・受講者のコミュニケーションを重視しているため、基本的にビデオをONで参加を依頼
    - チームごとに講師またはTAが付く形で演習を実施
    - メインセッション ⇔ ブレークアウトセッションの移動等はすべて運営側スタッフが対応
    - 演習は、D-Caseステップごとにチーム内で議論しながら進める形
    - 書記が代表してD-Caseステンシルで描画し、その画面をチームで共有して実施
      - Office365の共有は、あえて使用していない

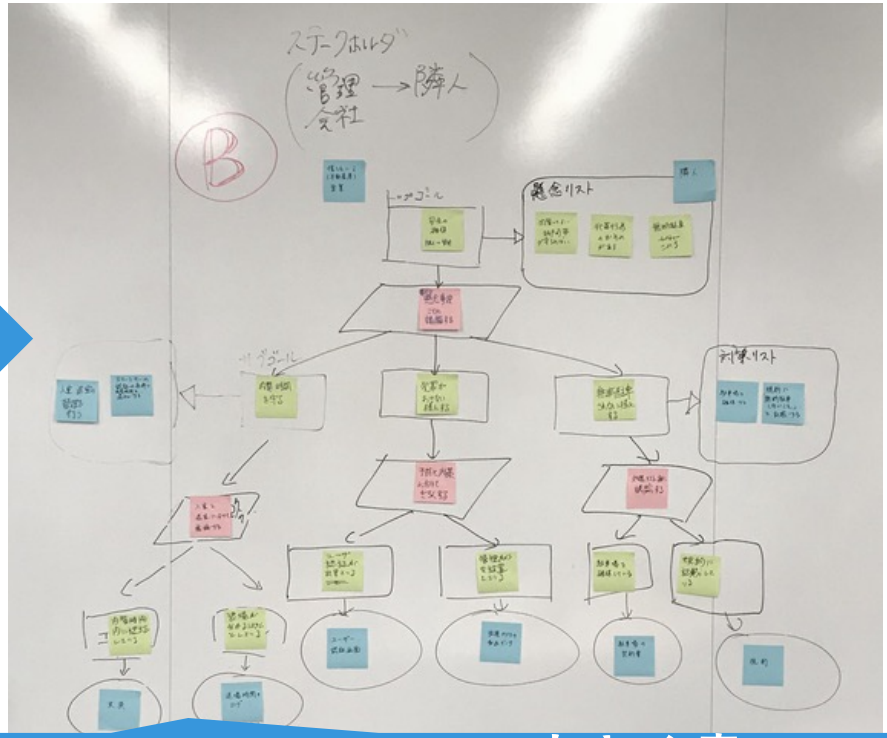
演習教材の例

VERISERVE

➢付箋紙のメモをホワイトボードに張り付け、D-Caseを作成します



こんなイメージです！

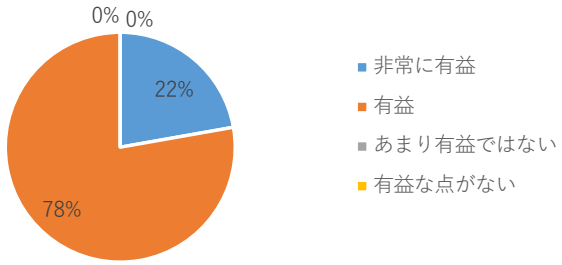


付箋メモの文字は可能な範囲で**大きく書いて**ください！

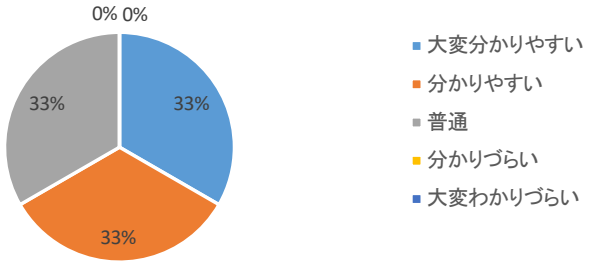
アンケート結果

VERISERVE

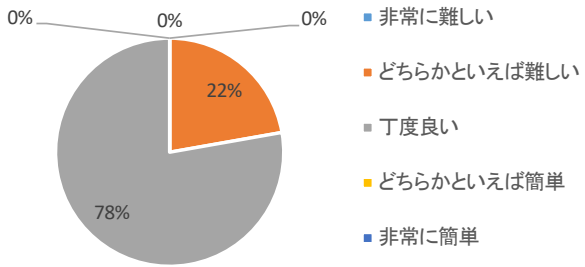
研修は有益だったか



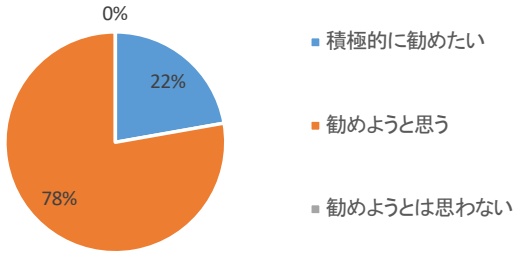
説明や資料の分かりやすさ



演習問題のレベルは



他の人に勧めるか



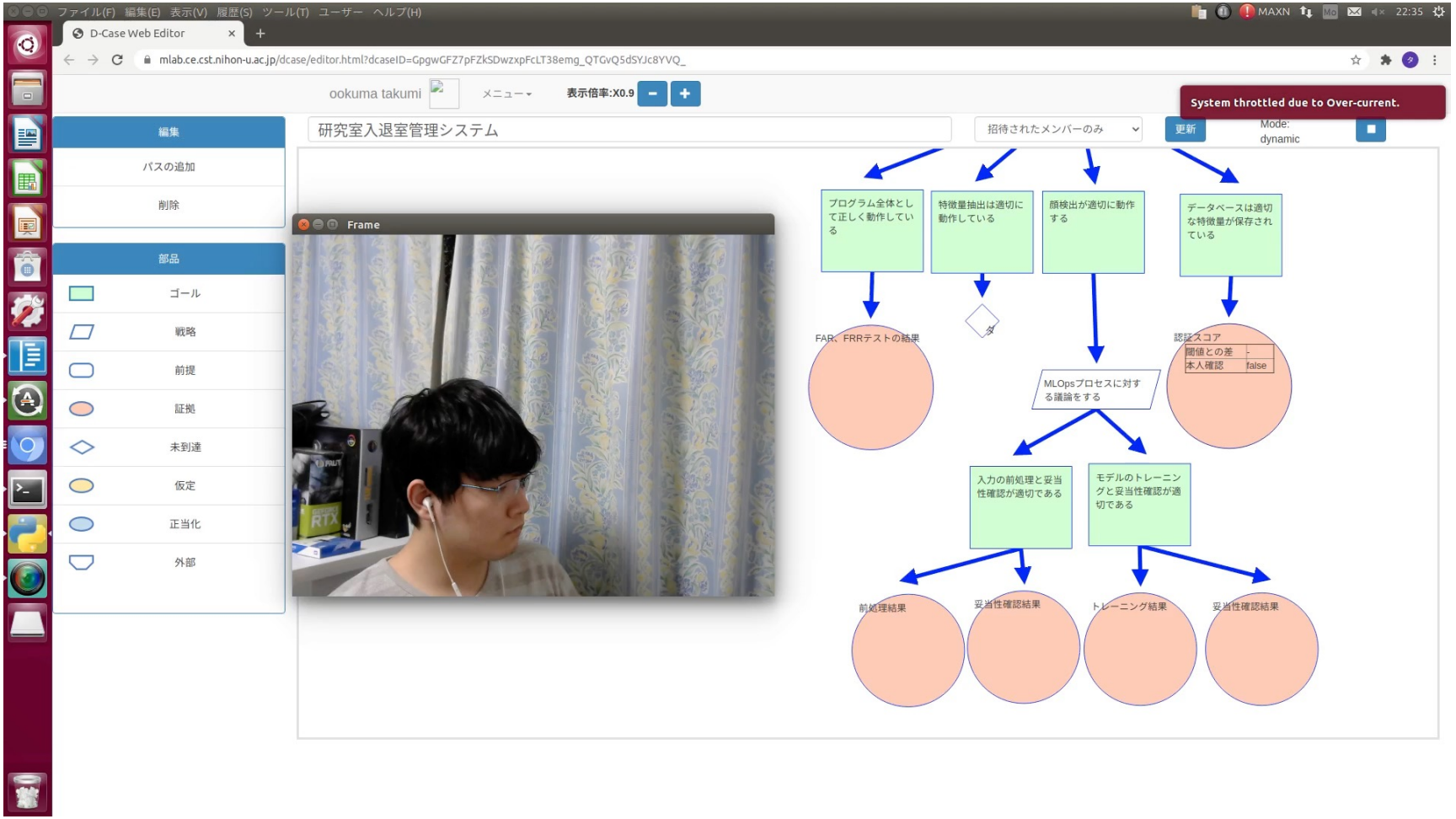
D-Caseツール開発

開発と運用がリンクした D-Caseを用いた合意形成に必要なツール要件

- 他のツールとの連携
  - Astah System Safetyとの連携を試作
- 変化対応
  - Gitの機能(Commit, Fork)を参考に、簡単な変更管理機能を試作
- 運用時のモニタリング情報の取得

科研基盤C(2021-2023)
DevOpsアシュアランスケースによる機械学習システムのディペンダビリティ保証

顔認証システムでのモニタリングデモ



ご参加の案内

- 企業内での安全性などの合意形成やコミュニケーションに課題がある、興味がおありでしたらぜひご参加ください
  - 社内でのD-Caseワークショップもご興味ありましたらご連絡ください

- 問い合わせ先：松野
  - matsuno.yutaka@nihon-u.ac.jp

はじめての D-Case