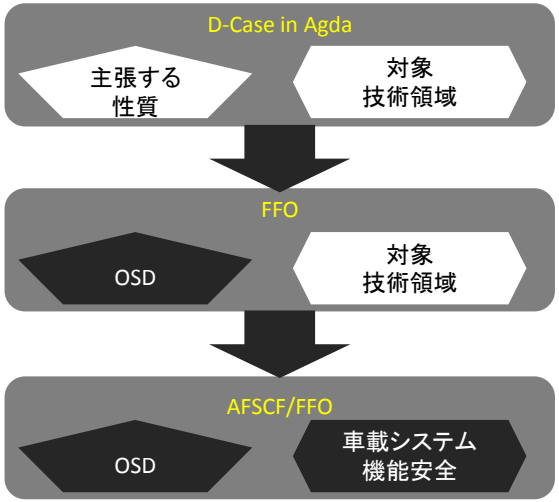
2014年度ソフトウェア工学分野の先導的研究支援事業

オープンシステムディペンダビリティのための形式アシュランスケースフレームワーク

Formal assurance case Framework
for Open systems dependability—FFO

木下佳樹（神奈川大学）

研究目標



システムライフサイクル(ISO15288)が
オープンシステム・ディペンダビリティを持つ
ことを主張する形式アシュランスケースの
フレームワーク

【研究目標1】オープンシステム・ディペンダビリティ一般のためのFFOの開発

- システムの技術領域には依らない。

【研究目標2】特定の技術領域におけるFFOの開発

- 技術領域を具体化（車載システム(AFSCF/FFO)、防災システム）

【研究目標3】事例研究による有効性評価

- 車載システムのアシュランスケーステンプレートへの評価

【研究目標4】FFOが依拠するシステムライフサイクル概念の確立

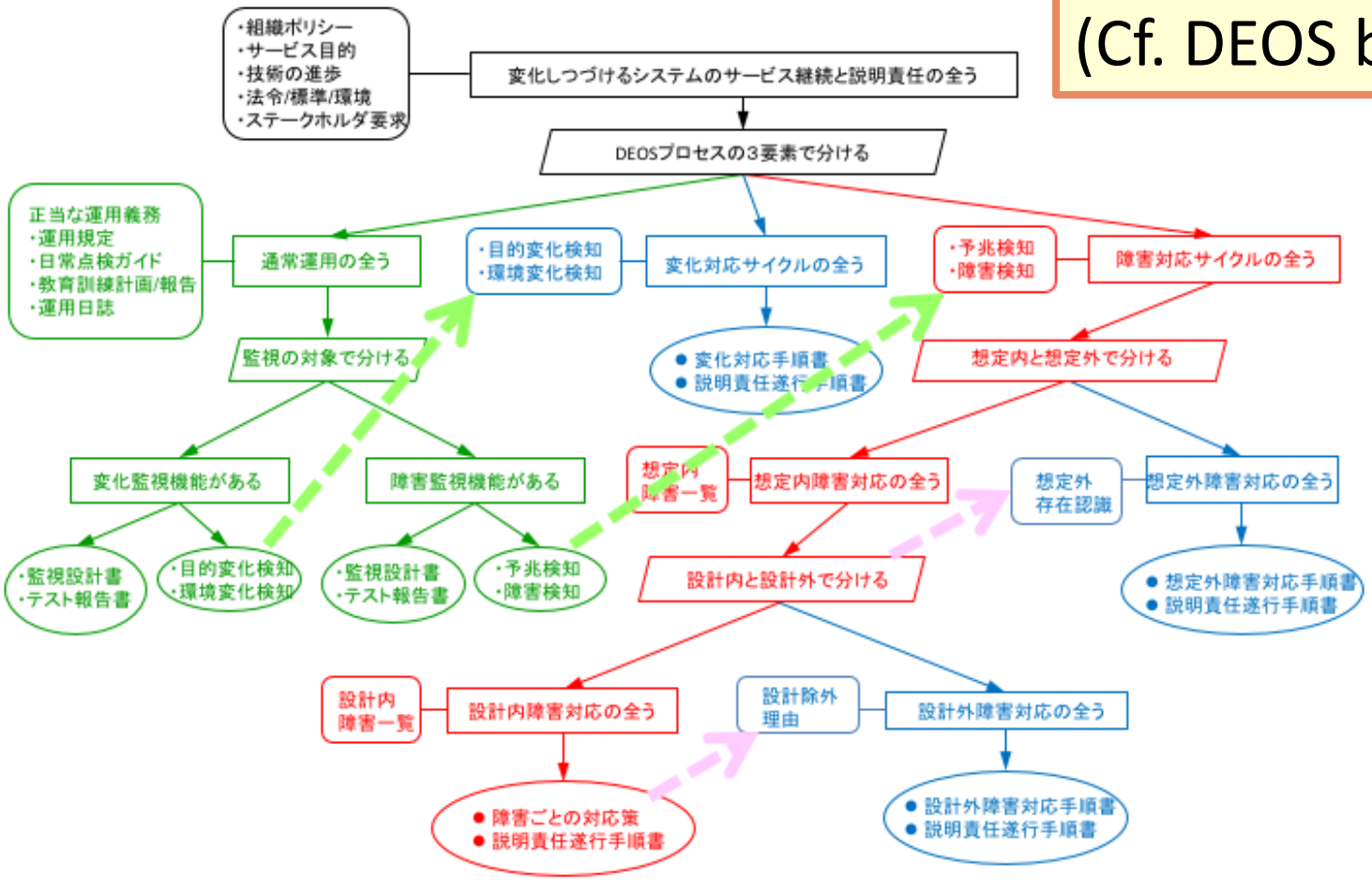
- 関連国際標準に準拠、また制定中の国際標準に成果を反映させる。

研究成果

1. FFO 基本パターン
   Formal assurance case **F**ramework for **O**pen systems dependability **Basic Pattern**
   【研究目標1】オープンシステム・ディペンダビリティー般のためのFFOの開発
2. FFO/AFSCF議論モデル
   FFO/Automobile **F**unctional **S**afety **C**ase **F**ramework
   【研究目標2】特定の技術領域におけるFFOの開発（車載システム）
3. 6W1Hモデル
   【研究目標2】特定の技術領域におけるFFOの開発（防災システム）
4. DPP議論モデル
   【研究目標2】特定の技術領域におけるFFOの開発（防災システム）
5. 導出パターン
   【研究目標3】事例研究による有効性評価
6. OSD ライフサイクルモデル
   【研究目標4】 FFOが依拠するシステムライフサイクル概念の確立

FFO Basic Pattern

DEOS基本構造
(Cf. DEOS book)



FFO Basic Pattern

DEOS基本構造を
Agdaで形式化

```
module Argument where
open import Notation
open import Contexts
open import Evidence
open C-Global

main-case =
  let open C-トップレベル in
  変化しつづけるシステムのサービス継続と説明責任の全う
  by DEOSプロセスの3要素で分ける
     § (常に 通常運用の全う          by 通常運用ケース)
     § (常に 変化対応サイクルの全う by 変化対応ケース)
     § (常に 障害対応サイクルの全う by 障害対応ケース)
  where
  open C-トップレベル
  通常運用ケース : ∀(t : Time) → 通常運用の全う t
  通常運用ケース t =
    let open C-通常運用 t ; open E-通常運用 t in
    通常運用詳細化
    § (let open C-日常義務 ; open E-日常義務 in
      日常義務 が 果たされている
      by record { 運用日誌      = 運用日誌Ref
                ; 日常点検報告 = 日常点検報告Ref
                ; 教育訓練報告 = 教育訓練報告Ref })
    § (let open C-変化監視 in
      変化監視機能がある
      by ∧分解
         §  (目的・環境変化検知できる by 変化検知ケース)
         §  (変化対応に移行できる      by 変化対応への移行ケース))
    § (let open C-障害監視 in
      障害監視機能がある
      by ∧分解
         §  (障害（予兆）検知できる    by 障害検知ケース)
         §  (障害対応に移行できる      by 障害対応への移行ケース))
    where
    変化検知ケース =
      let open C-通常運用.C-変化監視 t ; open E-通常運用.E-変化監視 t in
      目的・環境変化検知できる
      by 証憑の吟味
         § (( 目的・環境変化検知 )機能証憑監査結果-型
           by 目的・環境変化検知-証憑監査結果Ref)
```

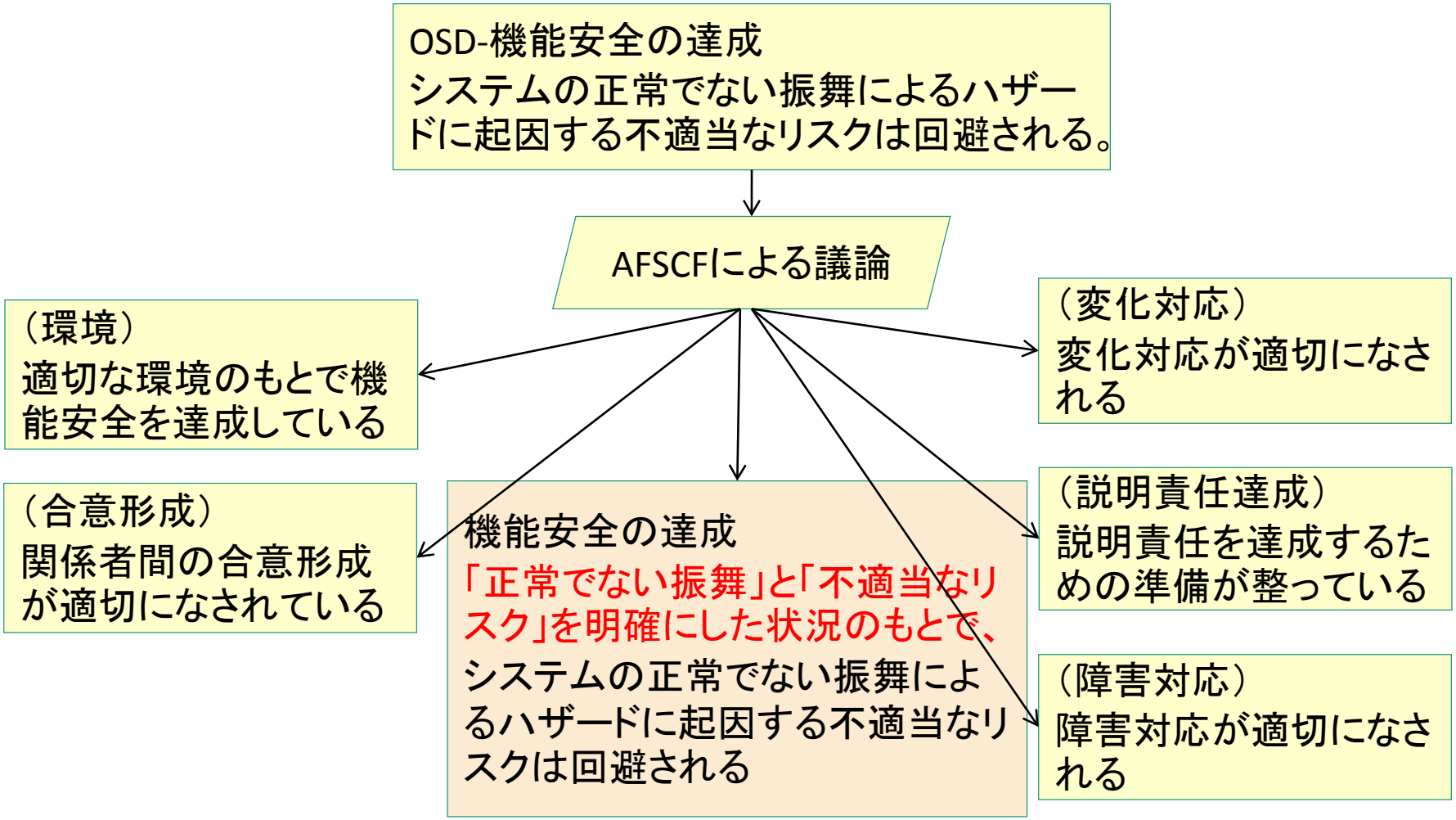
```
module Evidence where
open import Data.Product
open import Notation
open import Contexts
open C-Global
open C-トップレベル

module E-通常運用(t : Time) where
  open C-通常運用 t
  module E-日常義務 where
    open C-日常義務
    postulate
      運用日誌Ref      : 運用日誌-型
      日常点検報告Ref : 日常点検報告-型
      教育訓練報告Ref : 教育訓練報告-型
  module E-変化監視 where
    open C-変化監視
    postulate
      目的・環境変化検知-証憑監査結果Ref
                                  : ( 目的・環境変化検知 )機能証憑監査結果-型
      目的・環境変化検知-設計書Ref   : ( 目的・環境変化検知 )機能設計書-型
      目的・環境変化検知-開発履歴Ref : ( 目的・環境変化検知 )機能開発履歴-型
      目的・環境変化検知-テスト報告書Ref
                                  : ( 目的・環境変化検知 )機能テスト報告書-型
      目的・環境変化検知-運用証憑Ref : ( 目的・環境変化検知 )機能運用証憑-型
      変化対応移行-証憑監査結果Ref   : ( 変化対応移行 )機能証憑監査結果-型
      変化対応移行-設計書Ref         : ( 変化対応移行 )機能設計書-型
      変化対応移行-開発履歴Ref       : ( 変化対応移行 )機能開発履歴-型
      変化対応移行-テスト報告書Ref   : ( 変化対応移行 )機能テスト報告書-型
      変化対応移行-運用証憑Ref       : ( 変化対応移行 )機能運用証憑-型
  module E-障害監視 where
    open C-障害監視
    postulate
      障害（予兆）検知-証憑監査結果Ref
                                  : ( 障害（予兆）検知 )機能証憑監査結果-型
      障害（予兆）検知-設計書Ref     : ( 障害（予兆）検知 )機能設計書-型
      障害（予兆）検知-開発履歴Ref   : ( 障害（予兆）検知 )機能開発履歴-型
      障害（予兆）検知-テスト報告書Ref
                                  : ( 障害（予兆）検知 )機能テスト報告書-型
```

【研究目標2】特定の技術領域におけるFFOの開発（車載システム）

FFO/AFSCF 議論モデル I

- AFSCF議論モデルの枠組を提案
- 機能安全の議論 (ISO26262適合)
  - 上位仕様を満たすか？「仕様設定の根拠」
  - 実装が仕様を満足しているか？「システムの仕様への適合性」
  - 手法、プロセス、ツールが適切か？「手法の適切さ」
  - 法令、安全文化に照らして適切か？「環境妥当性」
- 継続的変化対応を考慮したOSDの議論 (IEC62853適合)
  - 関係者間の合意形成 (Consensus Building)
  - 説明責任を果たすことができるか？ (Accountability Achievement)
  - 障害対応は適切か？ (Failure Response)
  - 変化対応は適切か？ (Change Accommodation)
- (AFSCF = Automotive Functional Safety Case Framework)

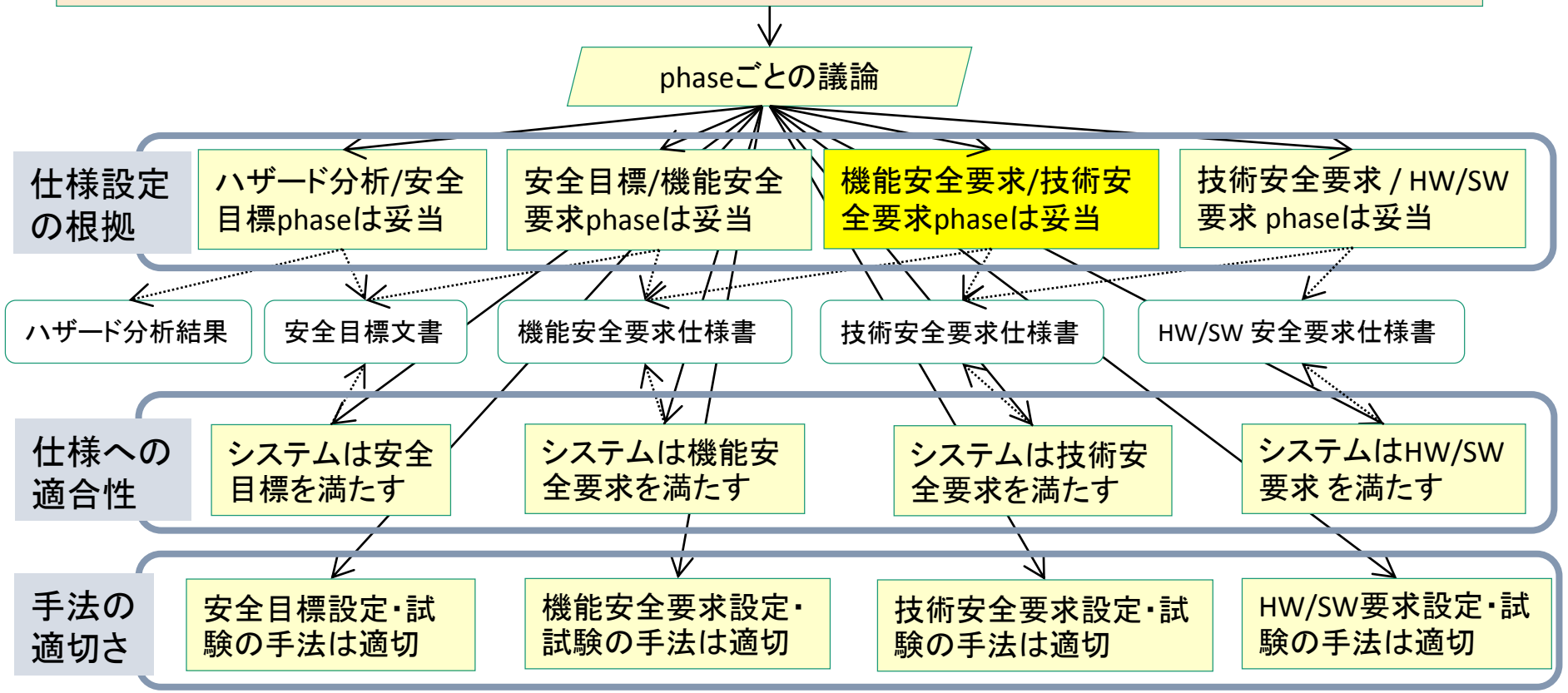
FFO/AFSCF 議論モデル II



【研究目標2】特定の技術領域におけるFFOの開発（車載システム）

FFO/AFSCF 議論モデル III

機能安全の達成
「正常でない振舞」と「不適当なリスク」を明確にした状況のもとで、
システムの正常でない振舞によるハザードに起因する不適当なリスクは回避される



6W1Hモデル I

- ISO/IEC/IEEE15288に基づくプロセス定義のためのモデル
- 6W1H…Who, What, Whom, When, Where, Why, How
  - Whoの記載によるタスク主体の明確化
  - Howは複数の6W1Hの集まりで構成される
    →プロセス/アクティビティ/タスクの階層構造を表現

【研究目標2】特定の技術領域におけるFFOの開発（防災システム）

6W1Hモデル II

No.	粒度	分類	6W1Hによる記述 Who	What	do	Whom	When	Where	Why	How
0	プロセス		市	飲料水等	供給	被災者等	発災時	避難所等		以下の手順で
1	アクティビティ	1.情報収集	市	給水の実施	判断	×	発災後	災害対策本部設置場所		収集した情報に基づき
2	タスク	1.情報収集	総務部被害調査班、特別調査班	水道の被害状況	調査	×		×		
3	タスク	1.情報収集	総務部被害調査班、特別調査班	水道の被害状況	報告	総合対策部総合調整班		×		
4	タスク	1.情報収集	土木復旧部	交通の状況	調査	×		×		
5	タスク	1.情報収集	土木復旧部	交通の状況	報告	総合対策部総合調整班		×		
6	タスク	1.情報収集	給水部	給水体制の進行状況等	調査	×		×		
7	タスク	1.情報収集	給水部	給水体制の進行状況等	報告	総合対策部総合調整班		×		
8	タスク	2.実施判断	災害対策本部	給水の実施	判断	×		災害対策本部設置場所		
9	アクティビティ		市	給水業務	準備	被災者等	実施判断後	市内各地		
10	タスク	3-1.水確保	総合対策部広報班	汲み置き	連絡	自主防災組織		×		
11	タスク	3-1.水確保	自主防災組織	汲み置き	呼びかけ	被災者等		×		
12	タスク	3-1.水確保	県企業庁平塚水道営業所	貯水量	確認	×		平塚配水池		
13	タスク	3-1.水確保	県企業庁平塚水道営業所	貯水量	連絡	災害対策本部		×		
14	タスク	3-1.水確保	協定締結事業者	飲料水の状況	確認	×		事業所		
15	タスク	3-1.水確保	協定締結事業者	飲料水の状況	連絡	災害対策本部		×		
16	タスク	3-1.水確保	給水部	非常用貯水タンクの状況	確認	×		非常用貯水タンク所在地		
17	タスク	3-1.水確保	給水部	非常用貯水タンクの状況	連絡	災害対策本部		×		
18	タスク	3-1.水確保	消防部	火災の状況	確認	×		災害対策本部		
19	タスク	3-1.水確保	給水部	臨時給水栓の設置	協議	消防部		×		
20	タスク	3-1.水確保	給水部、避難部	臨時給水栓	設置	×		消火栓所在地		
21	タスク	3-1.水確保	避難部	耐震性プールの水	ろ過	×		ろ水機利用場所		ろ水機を利用
22	タスク	3-1.水確保	県企業庁平塚水道営業所	配水管	復旧	×		配水管故障個		

DPP議論モデル I

DPP: 以下の3つで構成される議論モデル

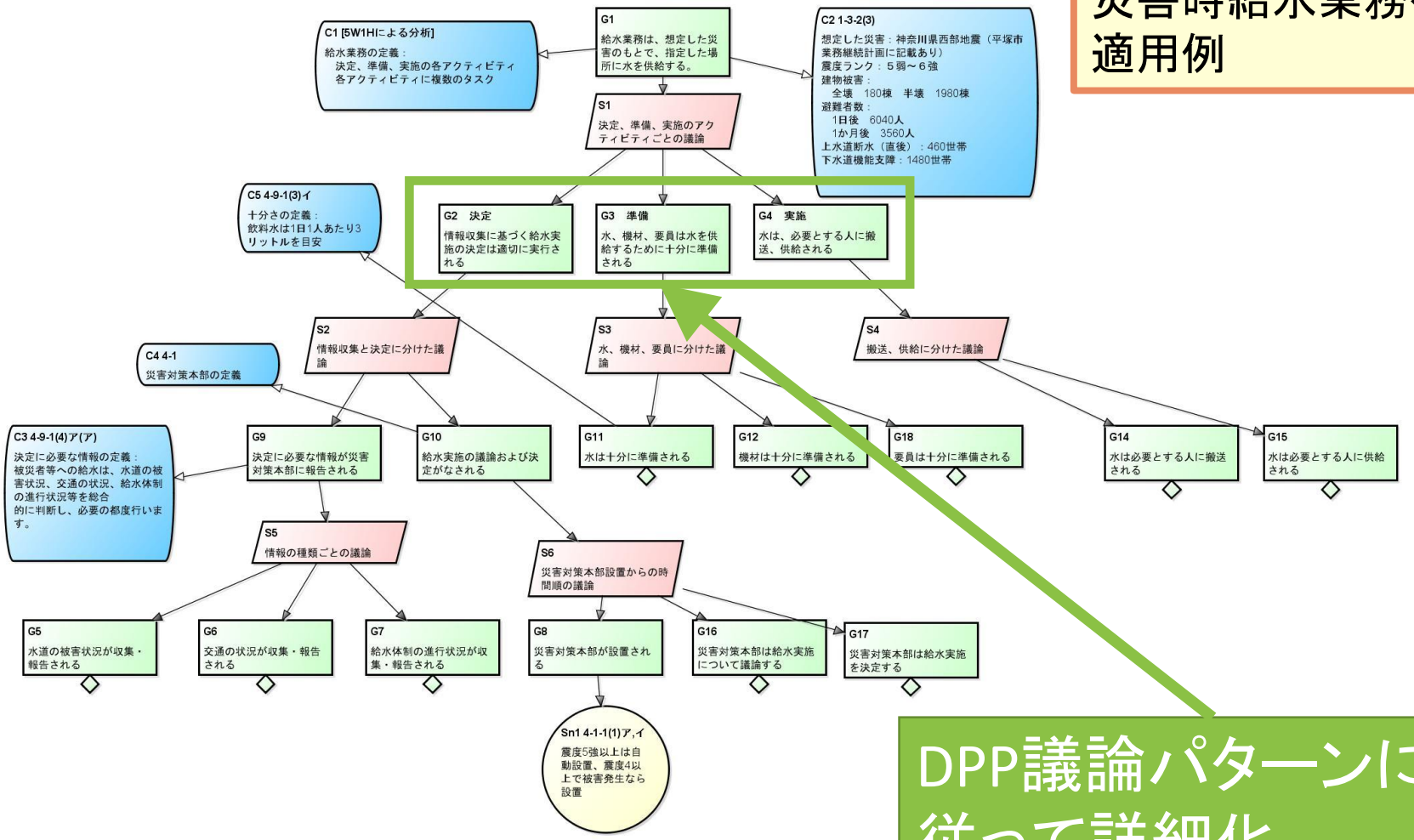
1. 決定（Decision）
2. 準備（Preparation）
3. 実施（Provision）

1. 決定（Decision）
   - 水道等の被害情報→給水実施の決定
   - 給水実施の情報→給水終了の決定
2. 準備（Preparation）
   - 水、運送用の車、人員等の手配
   - 需要と供給のバランスを考慮した輸送計画作成
3. 実施（Provision）
   - 計画に従った輸送
   - 避難所・公園等での供給

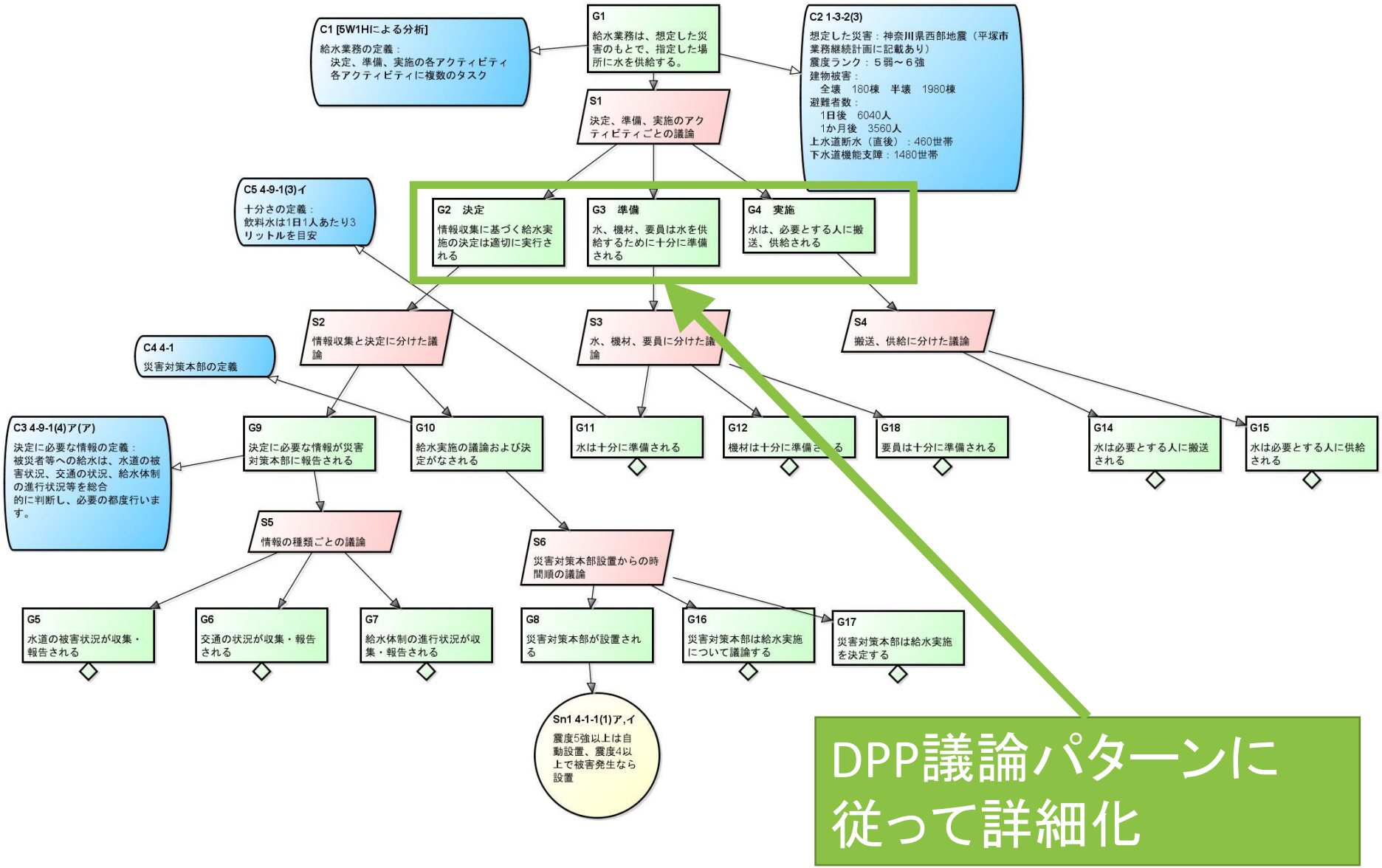
【研究目標2】特定の技術領域におけるFFOの開発（防災システム）

DPP議論モデルII

DPPの
災害時給水業務への
適用例



DPP議論パターンに
従って詳細化


C1 [5W1Hによる分析]
給水業務の定義：
決定、準備、実施の各アクティビティ
各アクティビティに複数のタスク
G1
給水業務は、想定した災害のもとで、指定した場所に水を供給する。
C2 1-3-2(3)
想定した災害：神奈川県西部地震（平塚市業務継続計画に記載あり）
震度ランク：５弱～６強
建物被害：
全壊　180棟　半壊　1980棟
避難者数：
1日後　6040人
1か月後　3560人
上水道断水（直後）：460世帯
下水道機能支障：1480世帯
S1
決定、準備、実施のアクティビティごとの議論
C5 4-9-1(3)イ
十分さの定義：
飲料水は1日1人あたり3リットルを目安
G2　決定
情報収集に基づく給水実施の決定は適切に実行される
G3　準備
水、機材、要員は水を供給するために十分に準備される
G4　実施
水は、必要とする人に搬送、供給される
S2
情報収集と決定に分けた議論
S3
水、機材、要員に分けた議論
S4
搬送、供給に分けた議論
C4 4-1
災害対策本部の定義
C3 4-9-1(4)ア(ア)
決定に必要な情報の定義：
被災者等への給水は、水道の被害状況、交通の状況、給水体制の進行状況等を総合的に判断し、必要の都度行います。
G9
決定に必要な情報が災害対策本部に報告される
G10
給水実施の議論および決定がなされる
G11
水は十分に準備される
G12
機材は十分に準備される
G18
要員は十分に準備される
G14
水は必要とする人に搬送される
G15
水は必要とする人に供給される
S5
情報の種類ごとの議論
S6
災害対策本部設置からの時間順の議論
G5
水道の被害状況が収集・報告される
G6
交通の状況が収集・報告される
G7
給水体制の進行状況が収集・報告される
G8
災害対策本部が設置される
G16
災害対策本部は給水実施について議論する
G17
災害対策本部は給水実施を決定する
Sn1 4-1-1(1)ア,イ
震度5強以上は自動設置、震度4以上で被害発生なら設置
DPP議論パターンに従って詳細化

導出パターン I

- 上位フェーズへの要求から下位フェーズへの要求を「導出する根拠」の「パターン」を抽出した。
- パターンは以下の項目よりなる
  a. 上位要求仕様のパターン
  b. 下位要求仕様のパターン
  c. パターンの適用条件
- パターンを個々の場合に「適用」して仕様を導出する。
- 「仕様」を導出すると同時に「導出する根拠」の記述も得られる。

【研究目標3】事例研究による有効性評価

導出パターンII

導出パターンの例

a. 上位要求仕様のパターン
<機能ブロック>の<故障>を判別できる<情報>を出力する

b. 下位要求仕様のパターン
<システムブロック1>の<故障1>を判別できる<情報1>を出力する
…
<システムブロックn>の<故障n>を判別できる<情報n>を出力する
（n個の要求。nは上位の<機能ブロック>と<故障>によって決まる）

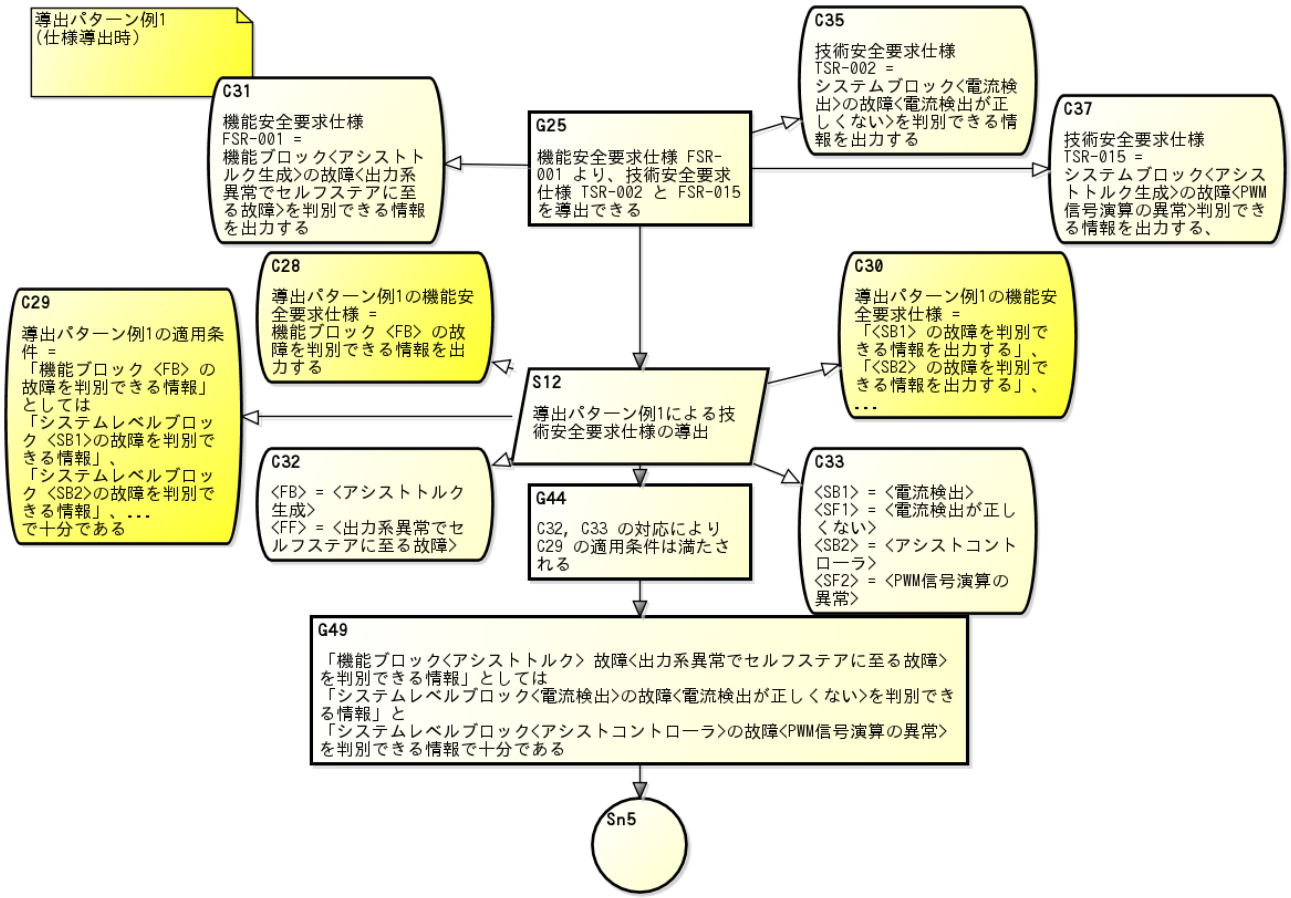
c. パターンの適用条件
<機能ブロック>の<故障>を判別するためには
<システムブロック1>の<故障1>を判別できる<情報1>
…
<システムブロックn>の<故障n>を判別できる<情報n>
のn個の情報があれば十分である

このパターンの妥当性についてのメタな議論の欄も必要。

【研究目標3】事例研究による有効性評価

導出パターン III

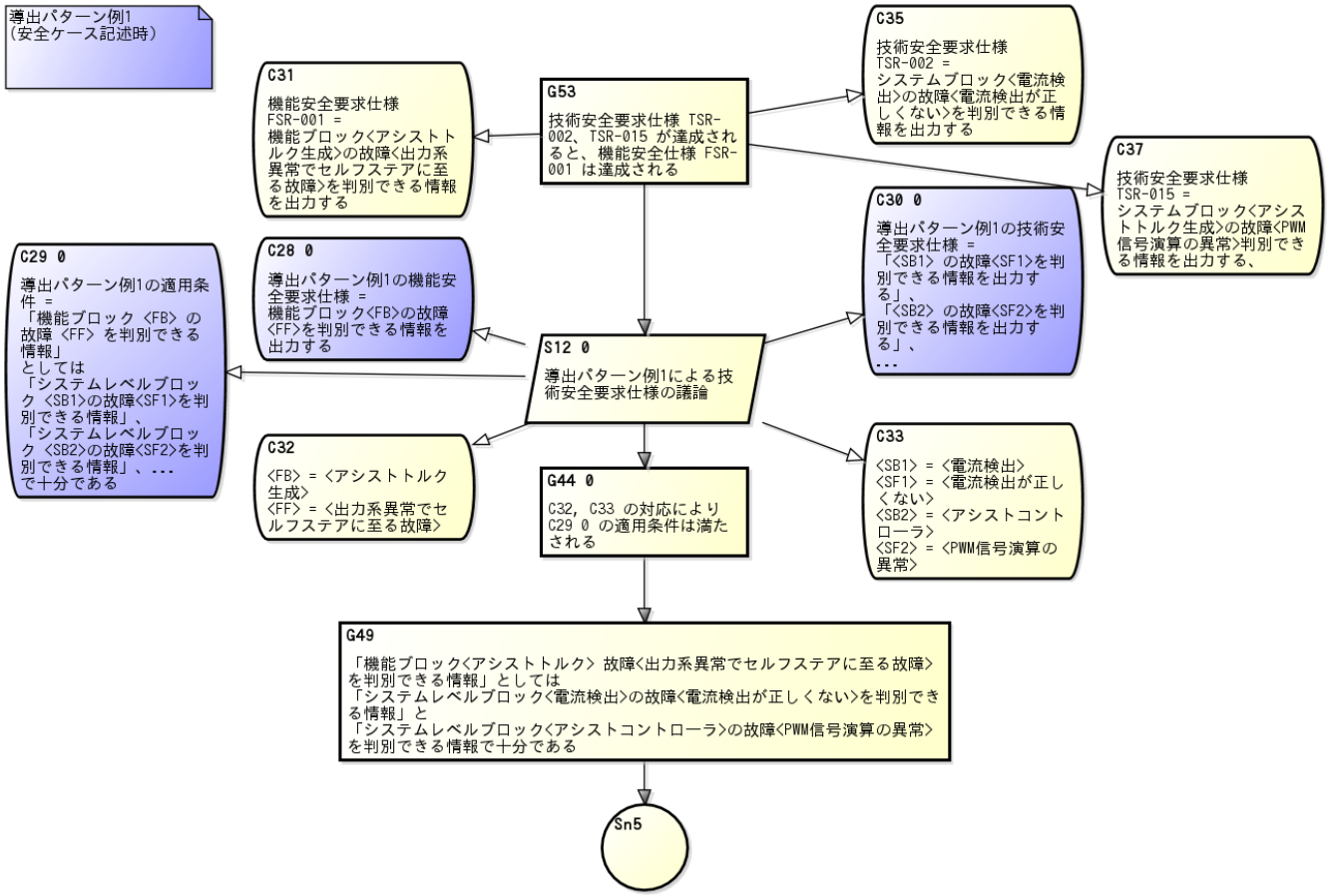
導出パターンの
仕様導出への適用例



【研究目標3】事例研究による有効性評価

導出パターン IV

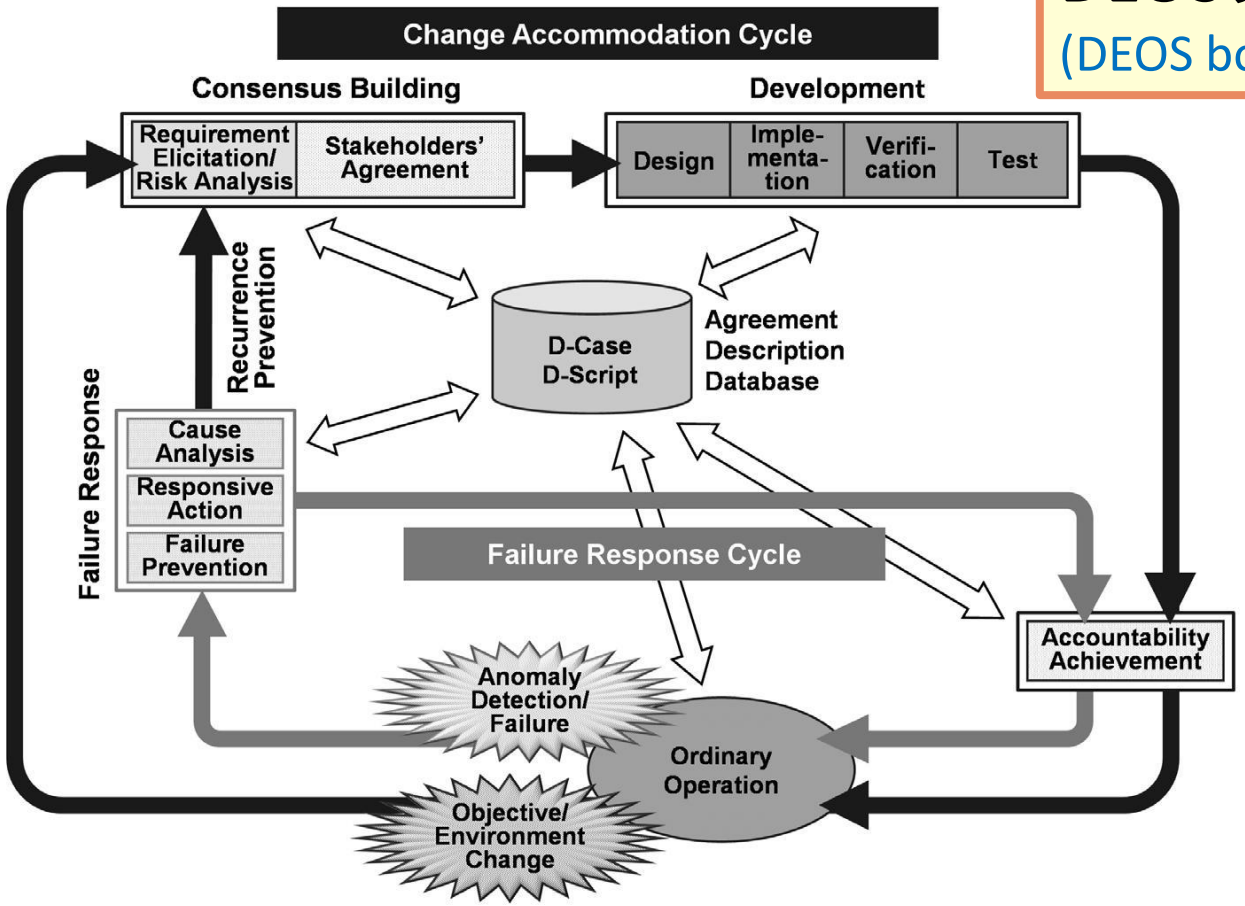
導出パターンの
安全ケース導出への適用例



【研究目標4】FFOが依拠するシステムライフサイクル概念の確立

OSDライフサイクルモデル I

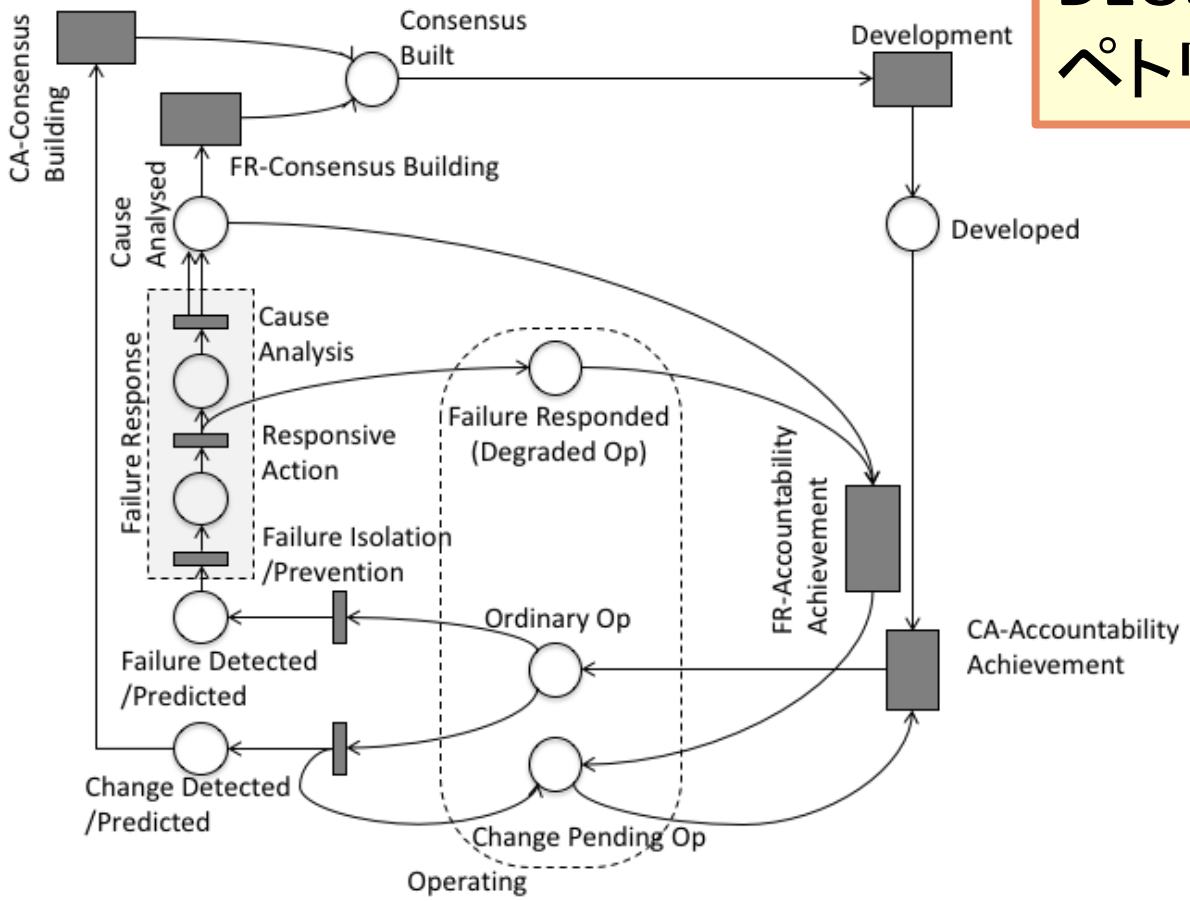
DEOSプロセス
(DEOS bookより)



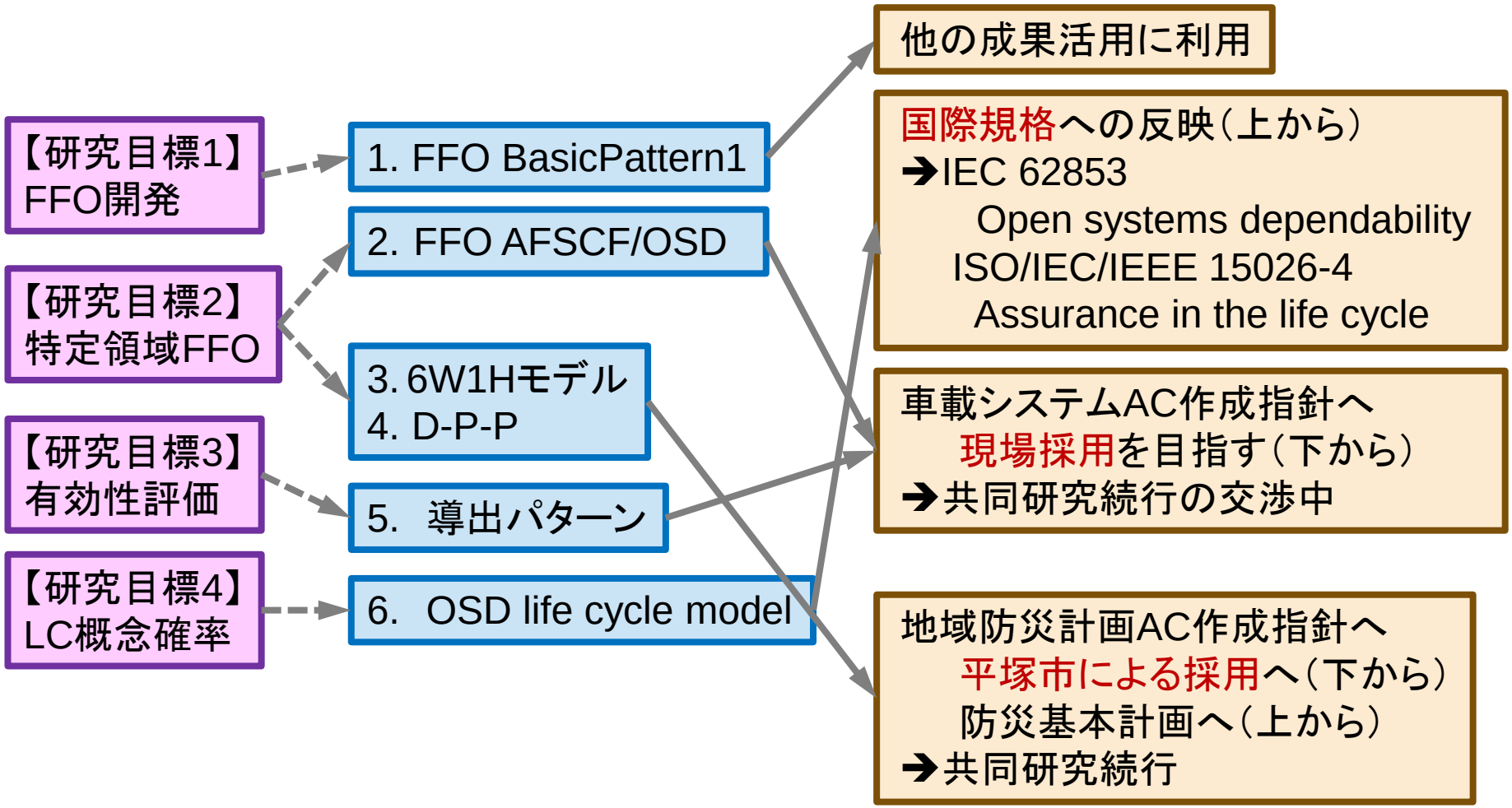
【研究目標4】FFOが依拠するシステムライフサイクル概念の確立

OSDライフサイクルモデルII

DEOSプロセスを
ペトリネットで定式化



成果の活用見込み


【研究目標1】
FFO開発
【研究目標2】
特定領域FFO
【研究目標3】
有効性評価
【研究目標4】
LC概念確率
1. FFO BasicPattern1
2. FFO AFSCF/OSD
3. 6W1Hモデル
4. D-P-P
5. 導出パターン
6. OSD life cycle model
他の成果活用に利用
国際規格への反映（上から）
➔IEC 62853
Open systems dependability
ISO/IEC/IEEE 15026-4
Assurance in the life cycle
車載システムAC作成指針へ
現場採用を目指す（下から）
➔共同研究続行の交渉中
地域防災計画AC作成指針へ
平塚市による採用へ（下から）
防災基本計画へ（上から）
➔共同研究続行

研究成果の発表、投稿、引用等

著書

- Makoto Takeyama, “D-Case Integrity Checking Tool and Formal Assurance Case”, Chapter 6 of Open Systems Dependability, Mario Tokoro (ed.), 2nd edition, CRC Press, 2015.
- Yoshiki Kinoshita, “Standardisation of Open Systems Dependability”, Chapter 10 of Open Systems Dependability, Mario Tokoro (ed.), 2nd edition, CRC Press, 2015.

口頭発表

- 武山誠「DEOSライフサイクルモデルについて」システムアシュランス研究会、2015-07-21、神奈川大学プログラミング科学研究所
- 木下佳樹「 DEOS標準化動向」システムアシュランス研究会、2014-07-18、神奈川大学プログラミング科学研究所
- 木下佳樹「IEC TC56 Dependability 活動報告」システムアシュランス研究会、2014-12-18、神奈川大学プログラミング科学研究所
- 木下佳樹「 IEC 62853 オープンシステムズディペンダビリティの最新動向」システムアシュランス研究会、2015-07-21、神奈川大学プログラミング科学研究所
- Yoshiki Kinoshita, “Open systems dependability standardization activity in IEC TC56”, WOSD (Workshop on Open Systems Dependability, IEEE ISSRE workshop), 2015-11-03, Washington DC.
- 武山誠「ディペンダビリティ技術の国際標準化動向とDEOS 」、DEOSシンポジウム, 2014-06-25, 慶應大学日吉キャンパス
- 木下佳樹「 DEOS関連国際標準の動向（IEC62853:Open Systems Dependability） 」、DEOSシンポジウム, 2015-06-17, 慶應大学日吉キャンパス
- Shuji Kinoshita, “Towards Assurance Arguments of Local Disaster Management Plans”, ASSURE (International Workshop on Assurance Cases for Software-intensive Systems, SAFECOMP workshop), 2015-09-22, Delft.
- Yoshiki Kinoshita, “The Role of Argumentation in Certification and Safety Risk Management”, ASSURE (International Workshop on Assurance Cases for Software-intensive Systems), 2015-09-22, Delft.
- 木下修司「平塚市地域防災計画の整合性検査」、DSW (ディペンダブルシステムワークショップ、ソフトウェア科学会)、2014-12-18、熱海
- 中原早生「AFSCF自動車機能安全議論について」、DSW (ディペンダブルシステムワークショップ、ソフトウェア科学会)、2015-12-17、熱海
- 木下修司「地域防災計画のアシュランス議論に向けて」、DSW (ディペンダブルシステムワークショップ、ソフトウェア科学会)、2015-12-17、熱海