DEOS要求マネジメント

名古屋大学　情報連携統括本部　情報戦略室
教授　山本修一郎

(株)NTTデータ　技術開発本部 システム科学研究所 所長 工学博士 山本修一郎

欧州を中心として、システムが重要安全性を満足することを示すためにアシュアランスケースが使用されている[1]。このため、アシュアランスケースは安全性ケース（safety case）と呼ばれていた。このアシュアランスケースを記述するための表記法は、欧州で約10年前から使用されているGSN（Goal Structuring Notation）である。今回は、このような安全性要求を確認するための実践的なゴール指向手法であるGSNに関連する話題を紹介しよう。

続きは本誌でご覧頂けます。→本誌を購入する
ご購入のお申込みは電話（03-3507-0560）でも承っております。

POWERED BY YAHOO! JAPAN
ウェブ検索
サイト内検索
ウェブ検索

60:要求とアーキテクチャ
61:要求と保守・運用
62:オープンソースソフトウェアと要求
63:要求工学のオープンな演習の試み

3月13日のプログラム

14:00～14:10　システムの高信頼化を保証する
　　ディペンダビリティケース研究構想の概要
14:10～14:30　議論パターン体系構築事例の紹介
14:30～15:00　TOGAF O-DAの概要と適用事例の紹介

15:00～15:10　休憩

15:10～15:40　ディペンダブル・オペレーションへの適用事例
15:40～16:00　ビジネスプロセスの高信頼性保証手法の紹介
16:00～16:20　テストの十分性保証手法の紹介
16:20～16:40　非機能要求グレードを用いたITサービスの
　　高信頼性保証事例の紹介

17:00～　　懇親会　シェ・ジロー

成果資料

- 議論パターンポケットガイド
- アシュアランスケース入門(+CD)
- 高信頼性エンタープライズアーキテクチャの取り組み
- ディペンダビリティケース適用のフロンティア2014

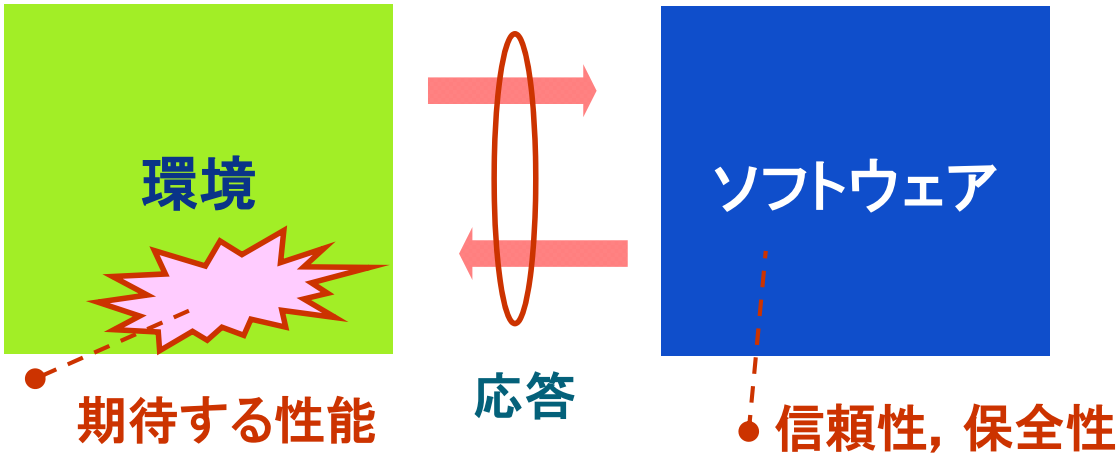
ディペンダビリティとは

人間行動
コンポーネント
法制度
自然物理現象

ディペンダビリティ

アベイラビリティ性能及びこれに影響を与える要因，すなわち信頼性性能，保全性性能及び保全支援能力を記述するために用いられる包括的な用語 JIS Z 8115

イベント

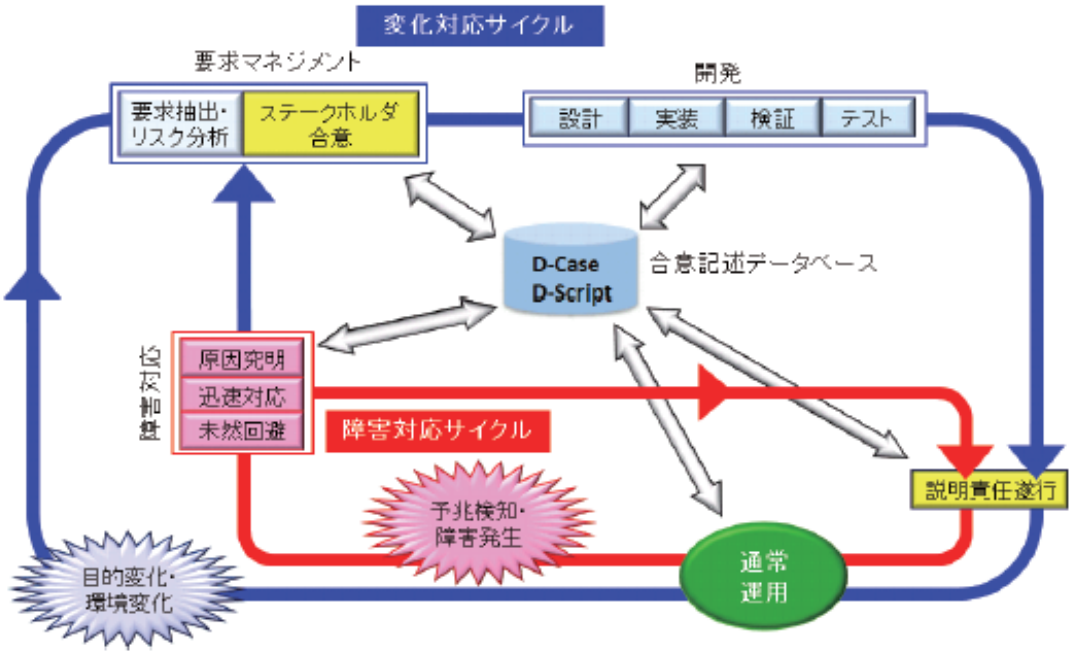


期待する性能

応答

信頼性，保全性

DEOSプロセス

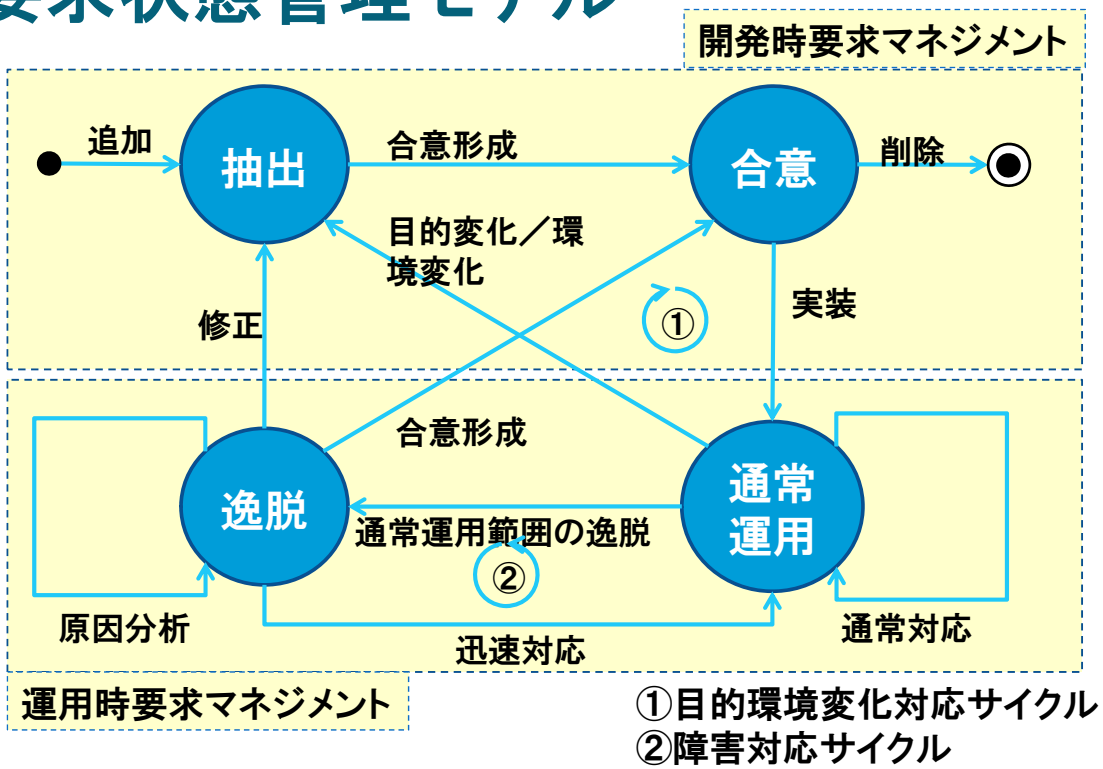


参考）DEOSプロジェクト, 2011 科学技術振興機構 White Paper DEOS-FY2011-WP-03J, *www.dependable-os.net/ja/topics/file/**White_Paper**_V3.0J.pdf*

要求マネジメント条件

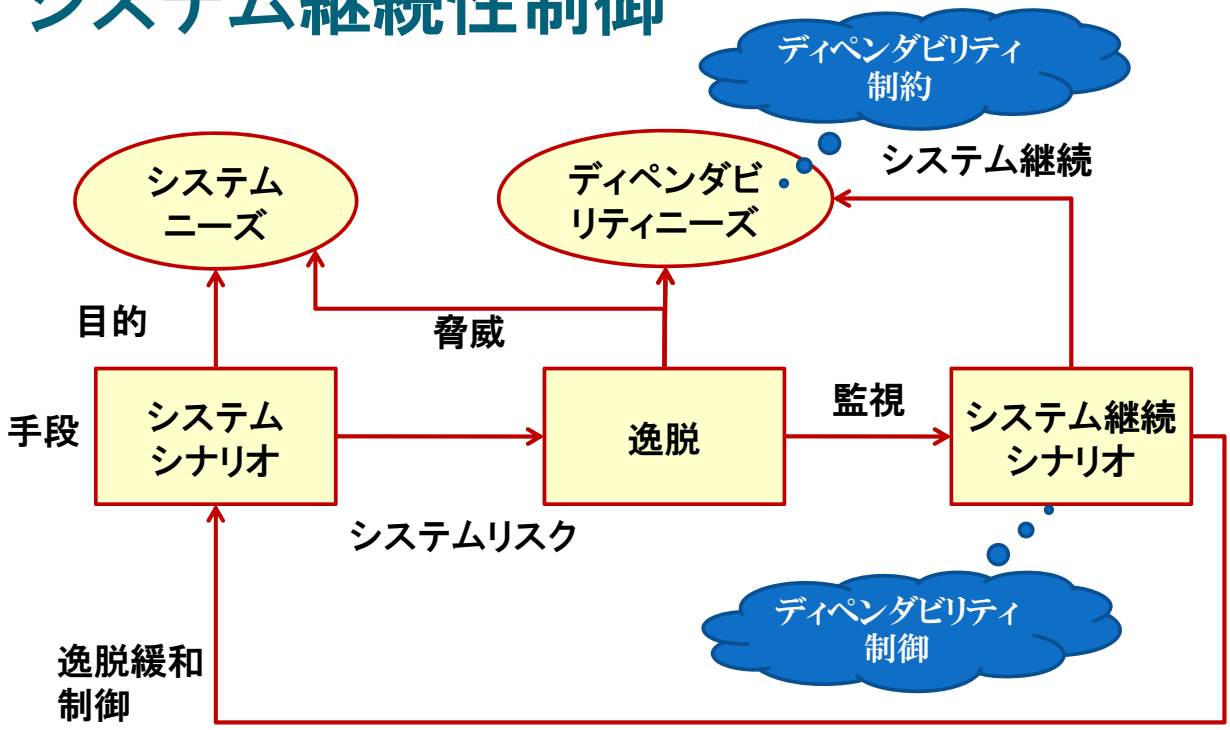
条件	説明
1	変化する要求に対してサービス継続性を保証できること
2	変化する要求に対して逐次、合意形成できること
3	変化する要求に対して常に説明責任を遂行できること

要求状態管理モデル



①目的環境変化対応サイクル
②障害対応サイクル

システム継続性制御



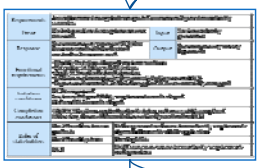
要求管理技法

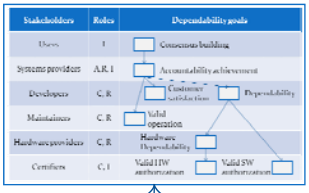
技法		説明
SCBC	サービス合意形成カード Service consensus building card	SCBCによりサービス要求を定義し，ステークホルダ間で合意する
DCB	ディペンダビリティ管理委員会 Dependability Control Board	DCB ではSCBCによる合意形成プロセスを管理する．DCB委員はステークホルダの代表者である
DC Map	ディペンダビリティ制御マップ Dependability Control Map	DC マップでは，ステークホルダの責務とディペンダビリティゴール間の依存関係を記述する
D-Case DB	D-Case データベース	D-Caseは，サービスのディペンダビリティ要求に対するディペンダビリティゴールを達成するために格納される
SRBS	サービスリスク分解構造 Service Risk Brake-down Structure	サービスリスク分解構造SRBSによって，階層的にリスクを分類する
SFT	サービス故障木Service Fault Tree	サービス故障木SFTにより故障の論理的な条件を定義する
SCS	サービス継続シナリオ Service Continuity Scenario	サービス継続シナリオSCSによって，ディペンダビリティ要求に対するリスクを緩和する．D-ScriptsによってSCS を実現する
SRMT	サービスリスク管理表 Service Risk Management Table	サービスリスク管理表SRMTにより，サービスイベントシナリオの確率と影響 に基づいてサービスリスクを定義する
SRSMT	サービス要求状態管理表 Service Requirements State Management Table	サービス要求状態管理表SRSMTでは，要求の開発時だけでなく，要求の運用中も含めて，サービス要求状態を管理する

名古屋大学

要求管理技法の関係

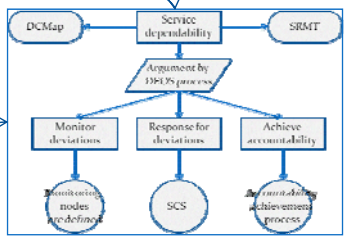
サービス合意形成カード
SCBC



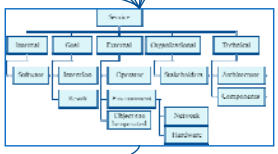


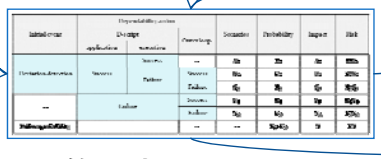
ディペンダビリティ制御マップ
DC Map

D-case

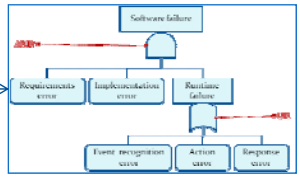


サービスリスク
分解構造
SRBS





サービスリスク管理表
SRMT



サービス故障木
SFT

名古屋大学

ディペンダビリティ制御マップ

ステークホルダ	役割	ディペンダビリティゴール
ユーザ	I	合意形成
システム提供者	A,R, I	説明責任遂行
開発者	C, R	顧客満足
保守者	C, R	保守の妥当性
ハードウェア提供者	C, R	ハードウェアディペンダビリティ
認定者	C, I	ハードウェア認定

ディペンダビリティ

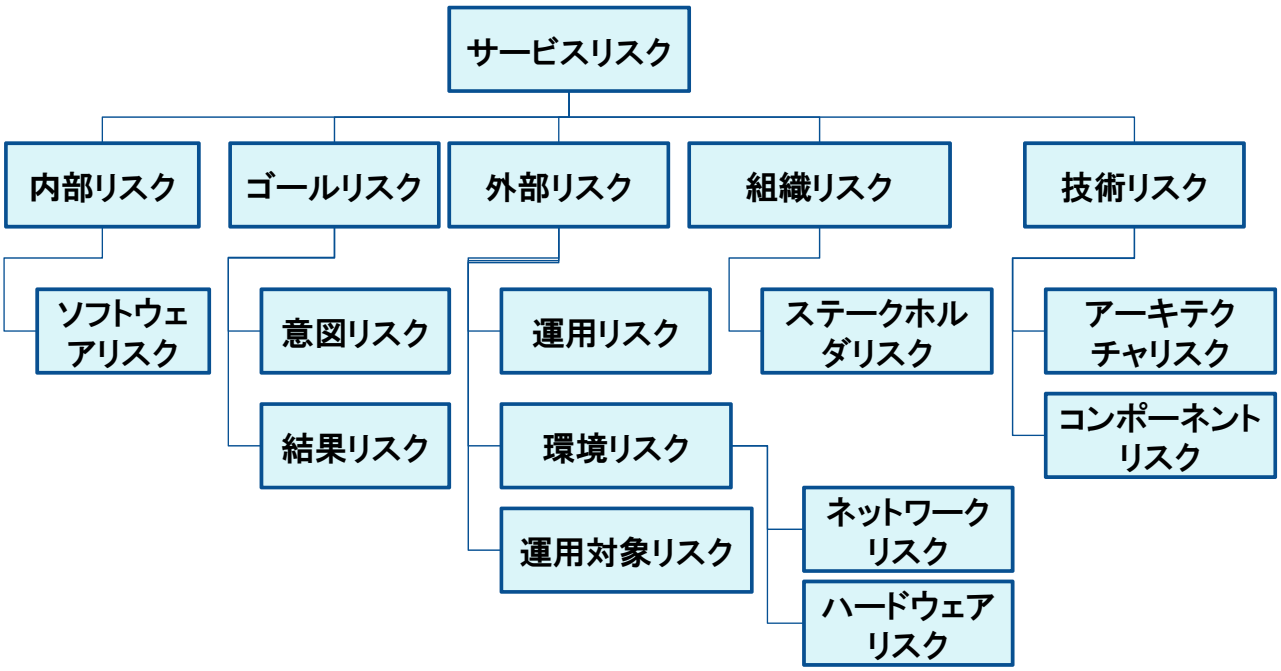
ソフトウェア認定

R: Responsible, A: Accountable, C: Consulted, I: Informed

サービス合意形成カード

要求	想定外の事象に対してサービス継続シナリオによってサービスを継続		
イベント	サービス要求の逸脱が発生	入力	サービス継続パラメータ
応答	サービス継続シナリオ(SCS)を適用することにより逸脱サービスを回復する	出力	サービス継続活動 ログ記録
機能要求	•サービス実行中に逸脱を検知する •逸脱に対処できるSCSを決定する •SCSを適用する •SCSの正常実行により，サービスの継続を確認する •SCSの適用で失敗して停止した場合，DCBにインシデントを通知する		
開始条件	DCB が設置されている サービス要求とディペンダビリティ要求が開発されている リスクとSCSが開発されている		
完了条件	妥当なSCSが逸脱に対して適用され正常に実行を完了する そうでない場合DCBに状況を報告する		
ステークホルダ役割	サービス提供者 製品提供者	サービス継続要求パラメータを定義 SCSの適用結果に合意．説明責任遂行	
	システム提供者	サービス継続シナリオを開発	
	ディペンダビリティ管理委員会	サービス継続要求と運用について合意形成	

サービスリスク分解構造



Ref: PMBOK 4th edition

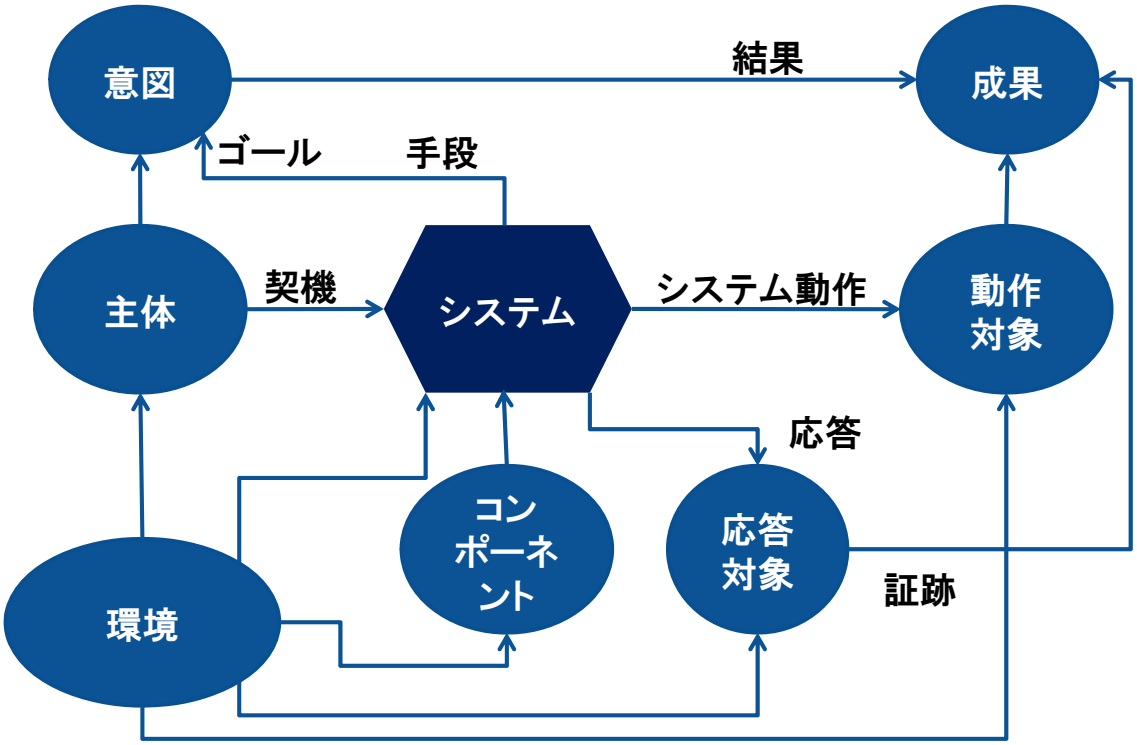
サービスリスク管理表

開始イベント	ディペンダビリティ活動			シナリオ識別子	確率	影響	リスク
	D-script		外部ループ				
	適用	実行					
逸脱検知	成功	成功	--	S_1	P_1	S_1	P_1S_1
		失敗	成功	S_2	P_2	S_2	P_2S_2
			失敗	S_3	P_3	S_3	P_3S_3
--	失敗		成功	S_4	P_4	S_4	P_4S_4
			失敗	S_5	P_5	S_5	P_5S_5
故障確率			--	--	P_3+P_5	S	PS

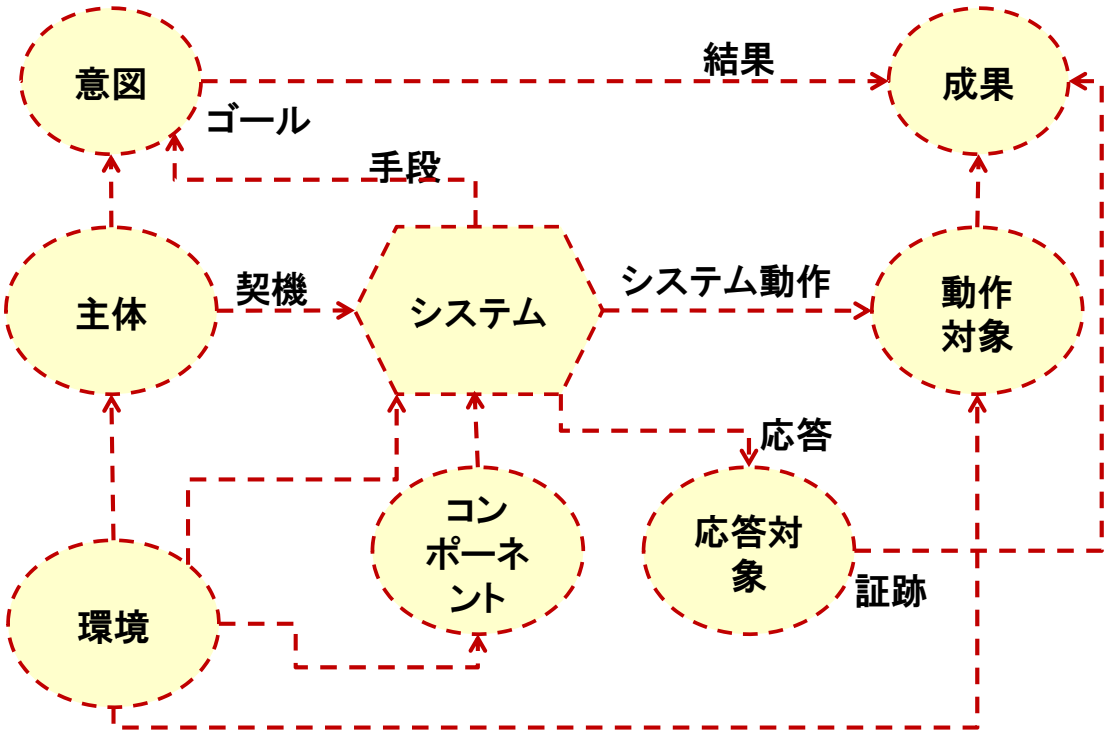
リスク分析活動

目的	システム要求リスクを分析し，システム継続シナリオを作成する		
入力	システム要求 ディペンダビリティ要求	出力	システム継続シナリオ
手順	•システム要求の逸脱を識別する •ディペンダビリティ要求を分析する •逸脱原因への対策を決定する •ディペンダビリティ要求を満足するシステム継続シナリオを作成する		
開始条件	リスク分析規則が定義されている サービス要求，ディペンダビリティ要求が定義されている		
完了条件	リスク分析規則に基づいて，システム要求とディペンダビリティ要求から，システム継続シナリオが抽出されている		
役割	システム，製品の提供者	システム要求とディペンダビリティ要求を提示する	
	システム提供者	システム継続シナリオを確認する	

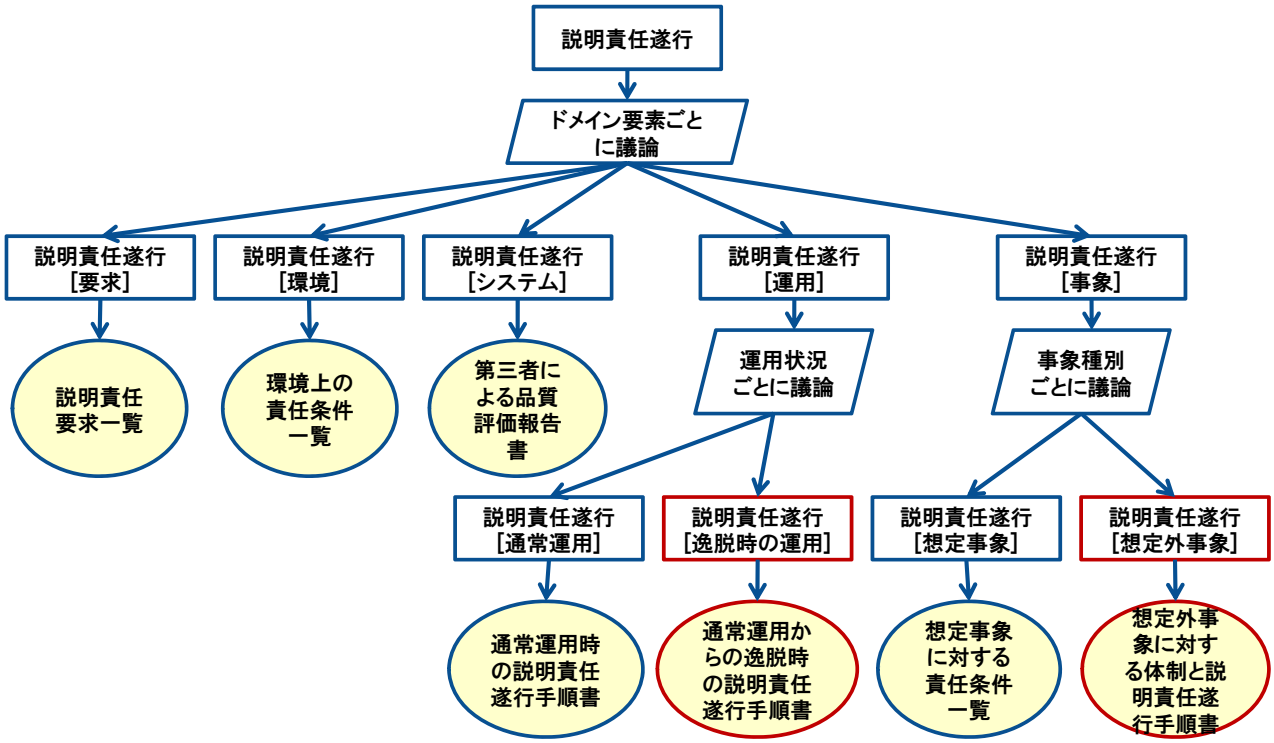
システムの動作シナリオ



システムリスク



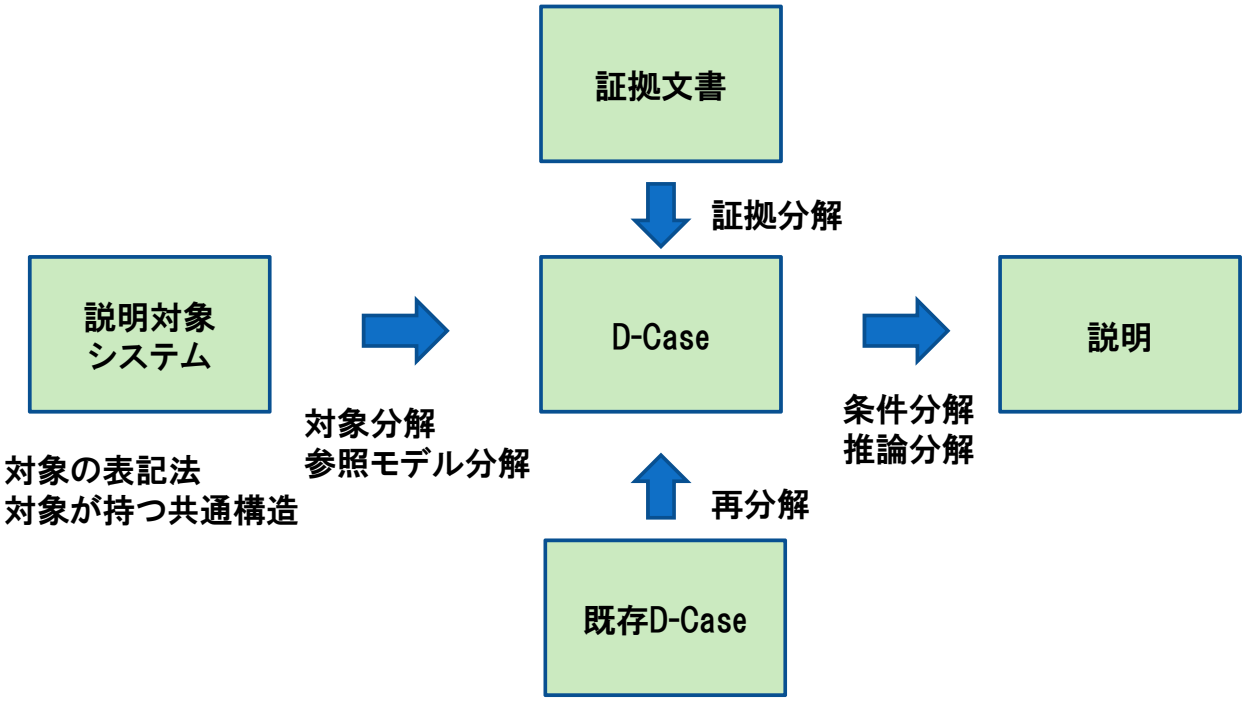
合意された要求の実現と説明責任遂行



D-Caseの全体構成例

TOGAF/ O-DA		O-DA/ D-Case	D-Case パターン
IT開発プロセス	要件定義	要件定義 D-Case	
	設計	設計D-Case	
	製造	製造D-Case	
	試験	試験D-Case	
サービス開発運用プロセス	サービス戦略	サービス戦略D-Case	
	サービス設計	サービス設計D-Case	
	サービス移行	サービス移行D-Case	
	サービス運用	サービス運用D-Case	
	継続的サービス改善	サービス改善D-Case	

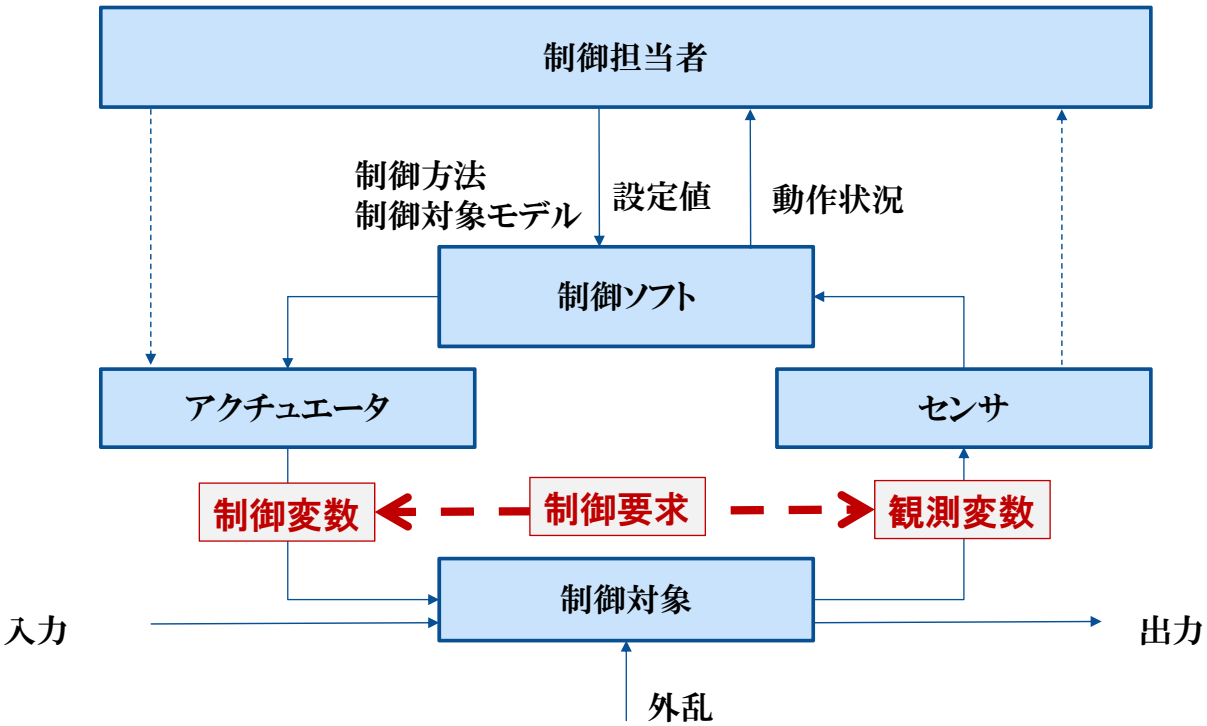
議論分解パターンの構成



議論分解パターンの事例

パターン 分類	説明
記述法 15	アーキテクチャ, 機能, 属性, 完全化, プロセス, プロセス依存関係 , 階層化, データフロー図, ビュウ, ユースケース, 要求, 状態遷移, 運用要求, シーケンス図, ビジネスモデル
参照モデル 10	DEOS プロセス,リスク, 組み込みシステム, コモンクライテリア, 要求テンプレート, システム境界, 欠陥モード, 非機能要求グレード, テストケース, 問題フレーム
条件 7	ECA, 条件判断, 代替案選択 , 矛盾解消, 平衡化, 改善, 明確化
推論 5	帰納法, 消去法, 否定推論, 反駁
証拠 11	法制度, 形式的証明, モデル検査, 試験成績書, 合意文書, レビュ報告書, シミュレーション, 評価報告書, 説明書, モニタノード, 文書
再利用 2	水平分解、垂直分解

STAMP 階層的制御構造



連載 要求工学 第20回 ソフトシステム方法論 再考 (その1)

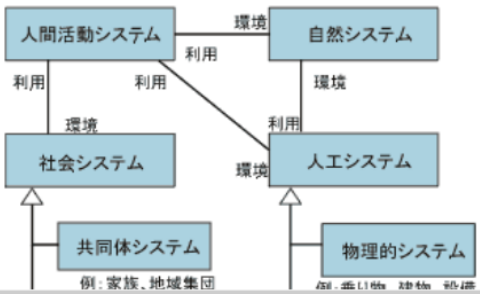
NTTデータ
技術開発本部
副本部長
山本修一郎

概要

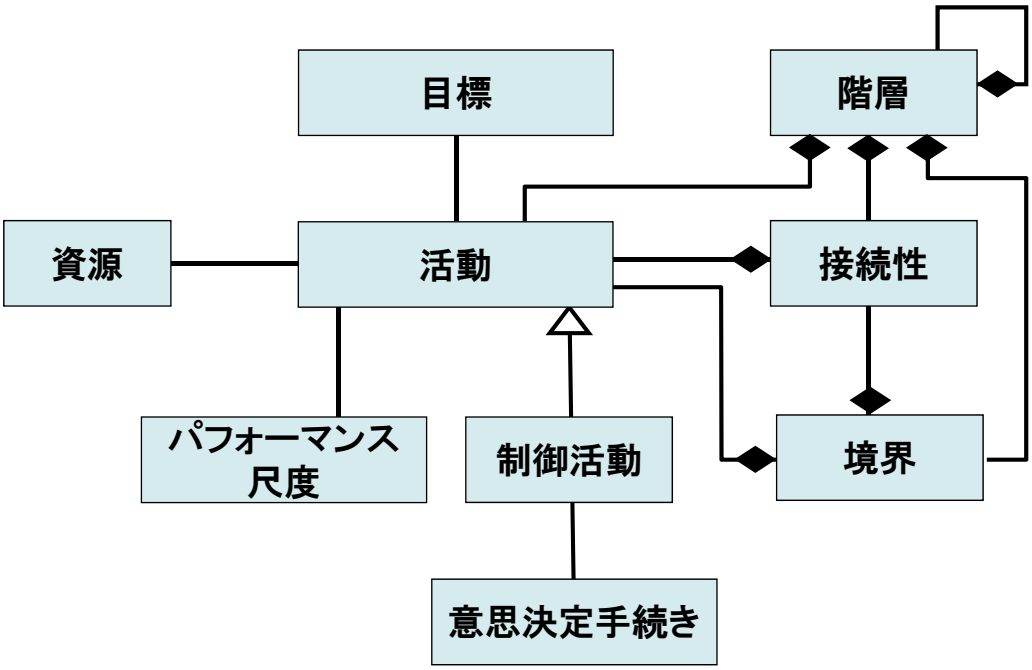
チェックランドのソフトシステム方法論（SSM）が最近再び注目されてきている。そこで今回から数回に分けてSSMの現代的な意義について要求工学の視点から考察していく。今回はその第1回としてウィルソンの「システム仕様の分析学」(1990, 日本語訳は1996)[1]第２章システム言語に基づいて、SSMの基礎となる人間活動システムの「基本定義」や「概念モデル」について紹介する。

システムの分類

まずSSMが分析の対象とするシステムをみておこう。システムは図１に示すように自然システム、人工システム、社会システム、そして人間活動システムの4つに分類されている[1]。自然システムは物理的なシステムであり、人間の意思決定によって制御できる範囲を超えているとさ



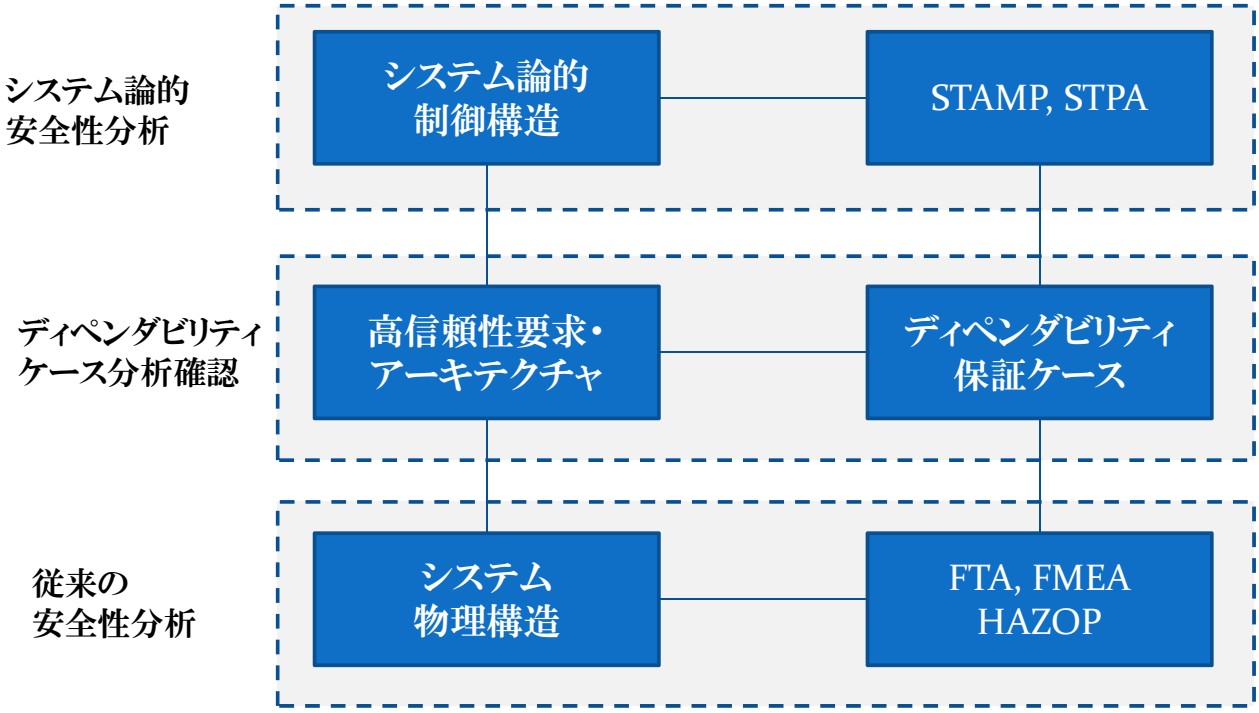
チェックランドの形式システムモデルの構造



システム論の制御条件

条件	説明
ゴール条件	制御主体が、目標値や満たすべき制約条件などのゴールを持つ
活動条件	外乱に際して既定義の限界または安全制約内にプロセスが操作されることを保証するようにシステム状態を制御する
モデル条件	制御主体が制御対象システムのモデルを持つ
観測条件	プロセス状態についてのフィードバック情報から制御主体がシステム状態を確認する

安全性分析手法の統合化



まとめ

- DEOS要求マネジメント
- STAMP/STPA
- 安全性分析保証技法の統合化