



第6回一般社団法人ディペンダビリティ技術推進協会総会・オープンシンポジウム

文部科学大臣表彰 科学技術賞(科学技術技術振興部門)受賞記念講演

開放系総合信頼性技術の 歩みと成果

2019年6月11日

所 眞理雄

(一社)ディペンダビリティ技術推進協会 理事長

(株)オープンシステムサイエンス研究所 代表取締役社長

時代背景



- 組み込みシステムの定義 (vs. PC)
 - 特定機能 機器に組み込み (vs. 汎用機能 機器とは別に存在)
 - 産業用機器、医療用機器、家庭用機器等
 - 小型・軽量、省電力、安定動作・誤動作防止
- 1961年 Minuteman、1965年 Apollo
- 1980年～
 - マイクロプロセッサの普及
- 1990年～
 - 組み込み機器産業の開始 μ ITRON、VxWorks, OS9, QNX
- 2000年～
 - 組み込み機器の発展 大規模組み込みシステム NetBSD, OpenBSD,
- 2005年～
 - 組み込み機器のバックエンドとの統合 組み込み用CE LINUX (Consumer Electronics Linux)、 Windows CE,
- 2015年～
 - IoT、自動運転、

DEOSプロジェクト(1)

- 2005年 JST研究開発戦略センター(CRDS)にてディペンダビリティの重要性が指摘され、「実用化を目指した組込みシステム用ディペンダブル・オペレーティングシステム」(略称DEOSプロジェクト)がCREST研究領域として採択され、研究総括に所眞理雄が就任した。
- 2006年に公募が開始され、審査を経て東京大学、筑波大学、慶應義塾大学、早稲田大学より合計5つの研究提案が採択され、同10月より具体的な研究が開始された。2008年には産業技術総合研究所、横浜国立大学、慶應義塾大学より合計4つの研究提案が採択され、総計9つに研究提案、100名近い研究者・大学院生の参加により、本研究領域の研究開発が行われた。

DEOSプロジェクト(2)

- 当初は各研究チームは「ディペンダブルなOS」の開発に注力。その後、いかにしてディペンダブルなライフサイクル・プロセスを達成するか、に議論が発展し、本研究領域全体の成果として、「オープンシステムディペンダビリティ(開放系総合信頼性)」の概念が提案された。
- 2013年10月に一般社団法人ディペンダビリティ技術推進協会(DEOS協会)が設立された。2014年3月にDEOSプロジェクトが終了し、その成果がDEOS協会に移管された。
- 2018年6月にIECによる国際標準IEC 62853 Open systems dependabilityが制定された。

これまでのディペンダビリティの概念



- 信頼性 (reliability): 一定の期間、要求された機能を与えられた条件のもとで実行する能力
- 1960 Reliability、RAS
- 1970 RASIS (reliability, availability, serviceability, integrity, security)
- 安全性 (safety): 規定された条件のもとで、生命、健康、財産またはその環境が危険にならないこと
- ディペンダビリティ (dependability) → 総合信頼性
- 安心性？

**これまでの工学的手法は、
対象を定義された領域とし、
構造、機能を固定し、
最適解を求める**

**その仮定の限りでは正しいが、
現場に導入したときに
その仮定が成立しているかどうか疑わしい
システム環境の変化が速い場合は特に困難**

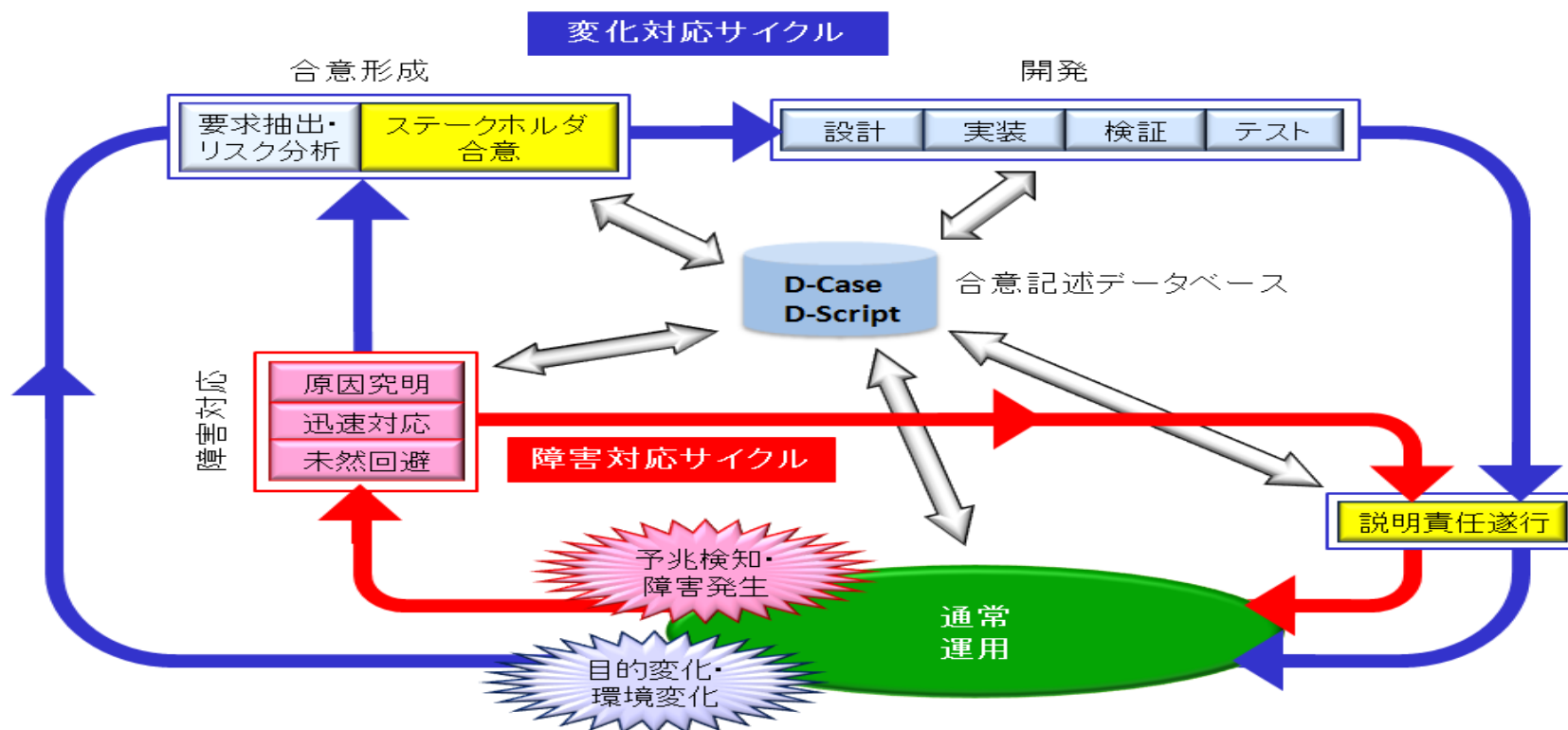
DEOSの先進性

DEOSの先進性

- 構成論的に開放系総合信頼性の実現をもとめず、ライフサイクルに対して漸近的にこれを実現することとした
- 総合信頼性の実現
 - 総合信頼性確保のための基本的な手段を、合意形成と説明責任とした
 - 合意形成の手法、記録(証憑)による合理的な説明の重要性の指摘
- 開放系対応
 - 開放系に対応するための基本的な手段を、変化対応サイクルと障害対応サイクルとした

DEOSライフサイクルプロセス

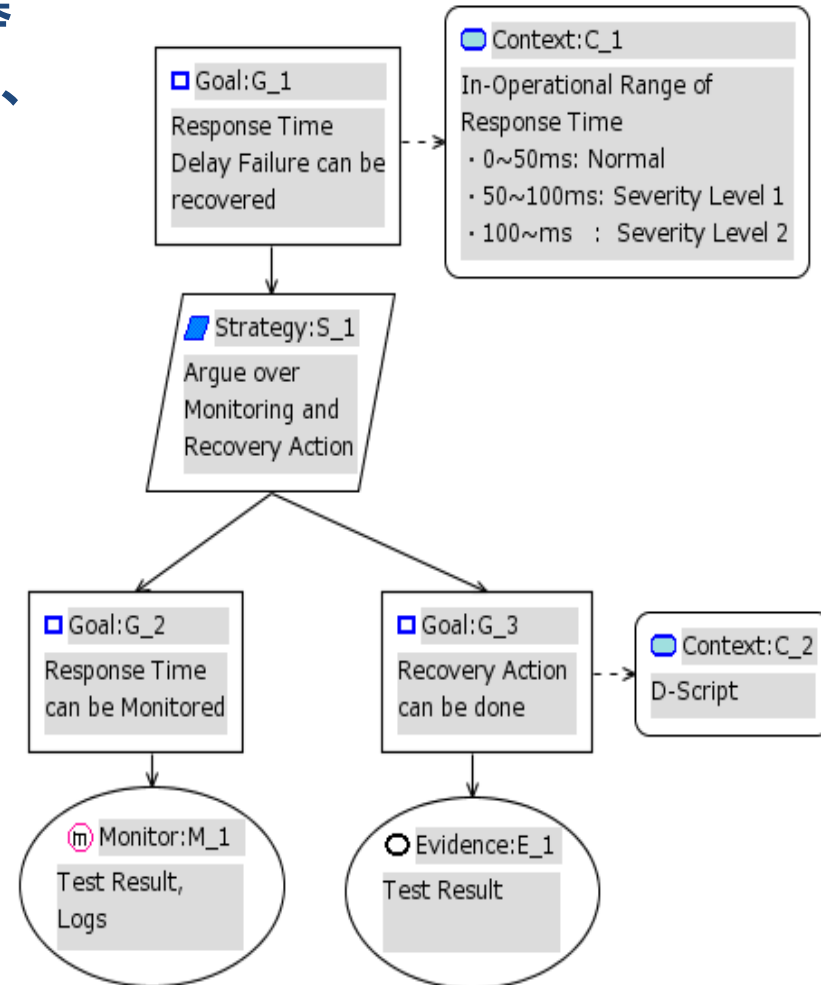
- 開発と運用の一体化
- 合意形成と説明責任の明確化によるディペンダビリティの担保
- 変化に対応するサイクルと障害に対応するサイクルからなる反復的なプロセス
- 再発防止のため、障害対応サイクルから変化対応サイクルへの経路



合意の形成と説明責任の遂行

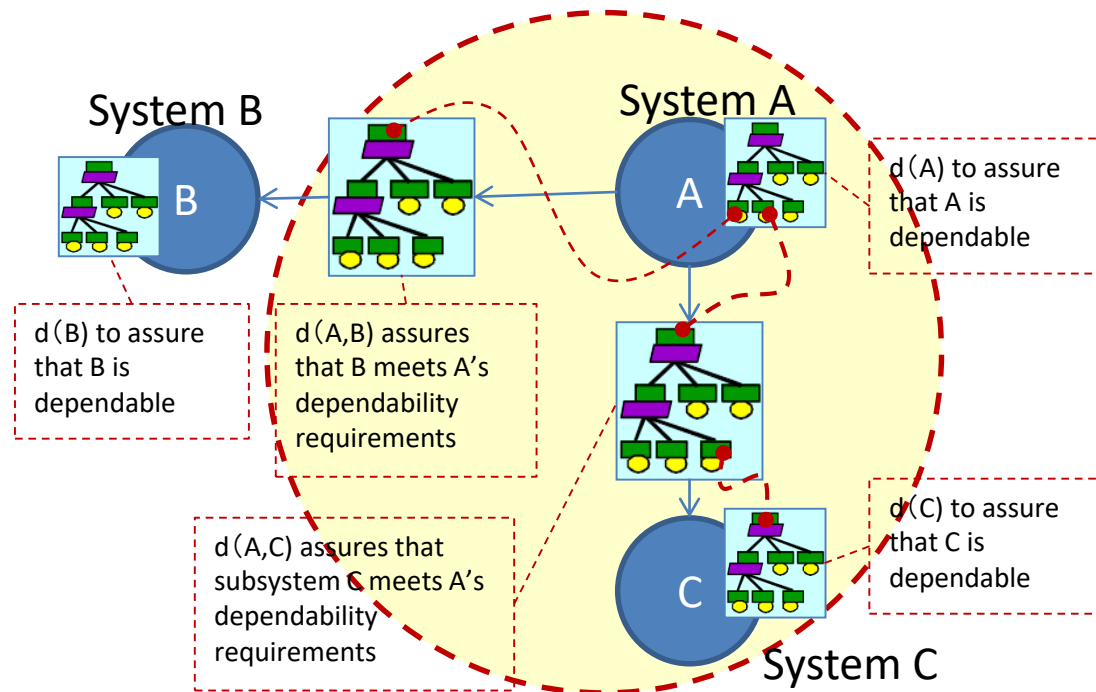


- 合意形成と説明責任の遂行のための基本的方法としてAssurance Caseを採用し、これを基にD-Case手法・記法を開発
- 論理構造の見える化と証憑の明示的な提示により、ステークホルダー間での合意内容の理解を容易にした
- 運用状況の記録も証憑の一つとして取り扱えるようにし、説明責任の遂行を容易にした



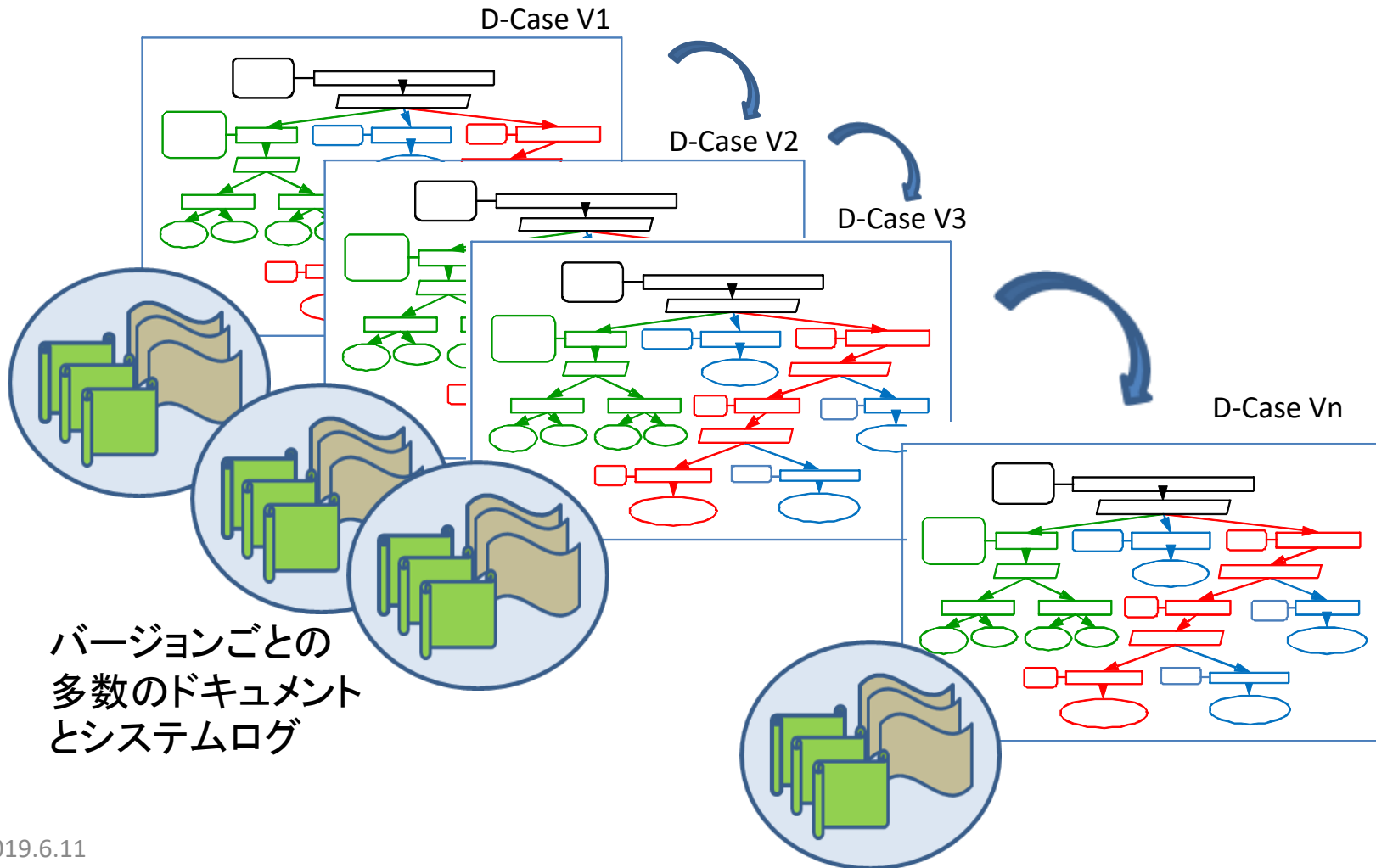
外部システムとの接続

- 所有者・管理者が異なるシステムとの接続においても総合信頼性を確保するための接続ノードを導入した



合意の記録と履歴の管理

- 合意の記述やシステム状態の履歴を保存し、説明責任を遂行するための統合データベース D-ADD を開発した



D-ADDによる 文書・履歴の 一元管理

D-ADD:

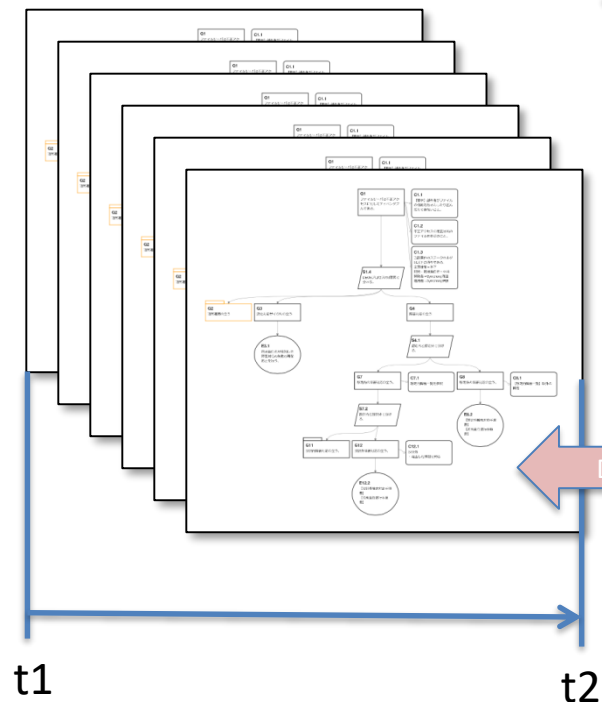
契約書、仕様、開発、テストの情報
ステークホルダーの合意記録と一貫性の担保



t1

上流

下流



t1

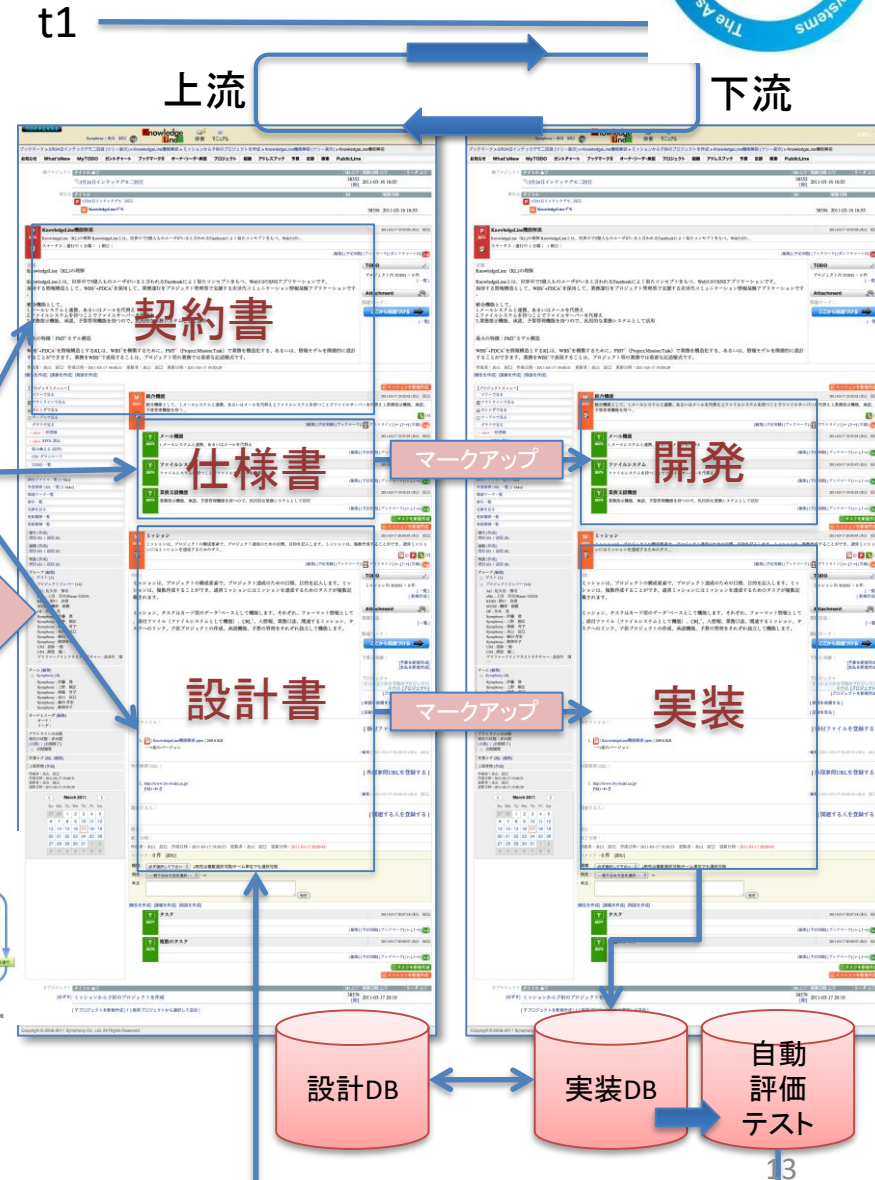
D-Case更新管理

t2

D-Case:
アシュアランスケースの合意状態を示す

- D-Caseの変更・構成管理をD-ADDで実現
- D-Caseの変更要求をD-ADDで記録
- D-Caseの時間変化の理由をD-ADDからトレース
- D-Case/D-ADDにて証憑を提示(マークアップ)

2019.6.11



13

意識の変化

- 2009.8 トヨタ アクセルペダル リコール
- 2011.3.11 福島原発事故
- 「想定外」にどのように対処するか
 - 「想定外」をなくすようにしらみつぶしに起こりうる状況を想定し、対応を考えておく
 - 事故が起こった場合には、出来るだけのことをやっていたこと(善管注意義務を果たしていた)ことを示す。

DEOSプロジェクトで行っていたことへの
理解が得られるようになってきた。

開放系総合信頼性とは？

開放系総合信頼性 とは(1)



- 総合信頼性？

- Dependabilityの日本語訳(JIS Z 8115 ディペンダビリティ)
- (for an item) “ability to perform as and when required”
「アイテムが要求された時に、その要求通りに遂行するための能力」。ここで、「アイテム」は製品だけでなくサービスも含まれる。
- 「信頼性」の上位概念で、アベイラビリティ、信頼性、回復可能性、保全性、保全支援機能を含む。適用によっては耐久性、安全性およびセキュリティのような他の特性を含むことがある。

(益田昭彦、JIS Z 8115 ディペンダビリティ(信頼性)用語の現状と将来、電子情報通信学会基礎・境界ソサイエティ、Fundamentals Review Vol. 9 No.4 pp.318-329 2016年4月参照)

開放系総合信頼性 とは(2)

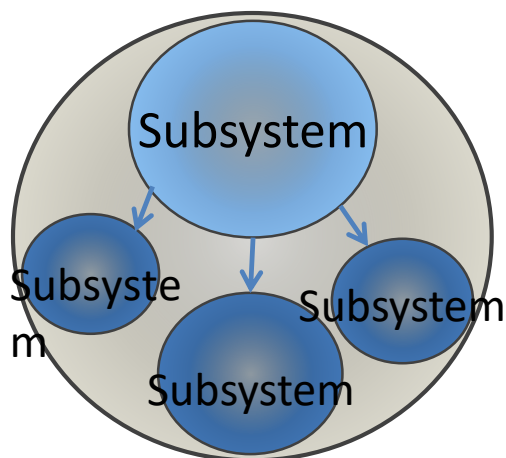
• 開放系？

- Open Systemsの日本語訳
- 閉鎖系 (Closed Systems)の対語

閉鎖系

機能、構造、境界が固定
境界が明確に定義できる

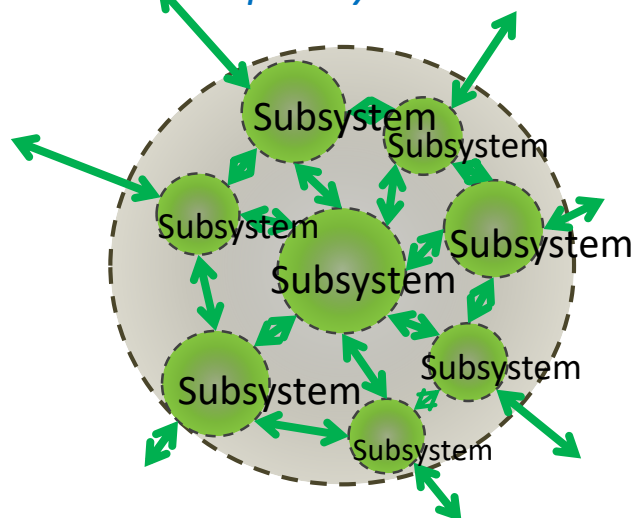
Closed Systems



開放系

機能、構造、境界が変化
境界明確に定義できない

Open Systems



開放系総合信頼性 とは(3)



- 開放系総合信頼性はOpen Systems Dependabilityの日本語訳
- 「総合信頼性」の概念を「開放系」環境下で展開

開放系総合信頼性は対象とする系のライフサイクルに亘る総合信頼性の最適解を求める

隣接する系を含む環境や目的の変化に対し説明可能な形で総合信頼性を確保する

IEC 62853

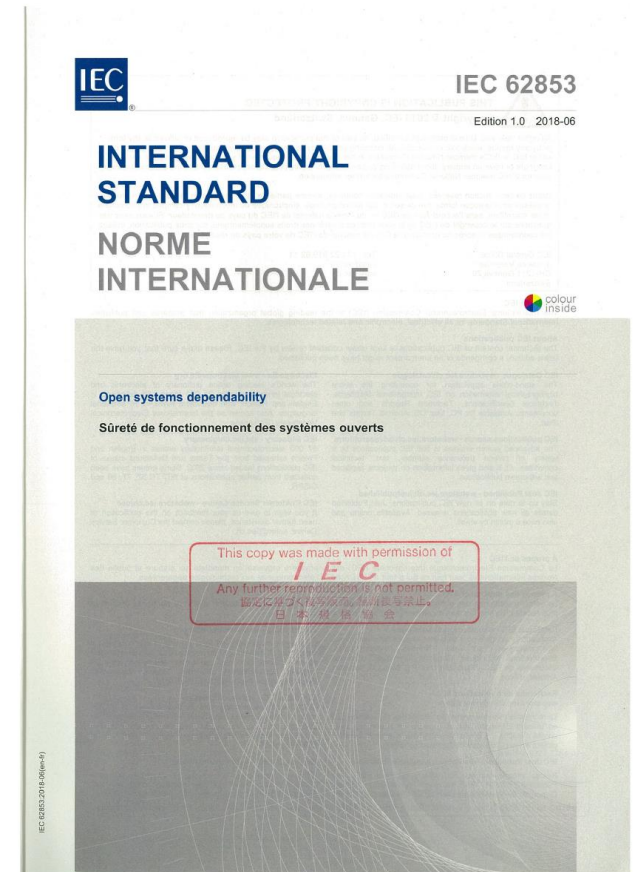
Open systems dependability

IEC62853 Open systems dependability (開放系総合信頼性)



2018年06月13日出版
日本語訳は暫定

1. スコープ
2. 引用規格
3. 用語と定義
4. オープンシステムディペンダビリティ(以下OSD)
 1. オープンシステムとは
 2. オープンシステムに係るディペンダビリティの課題
 3. 目的
 4. OSDの達成
 5. OSD関連する概念
5. 規格適合性
6. OSDを達成するためのプロセスビュー
 1. 一般
 2. 合意形成プロセスビュー
 3. 説明責任達成プロセスビュー
 4. 障害対応プロセスビュー
 5. 変化対応プロセスビュー
7. 付録A OSDライフサイクルモデルの例
8. 付録B ディペンダビリティケースのためのテンプレートの例



IEC 62853 の先進性

- 「開放系」の考え方と文言を初めて国際標準に導入した。
- DEOSの4つのプロセスをプロセスビューの形で定式化した
 - 合意形成プロセスビュー
 - 説明責任達成プロセスビュー
 - 障害対応プロセスビュー
 - 変化対応プロセスビュー

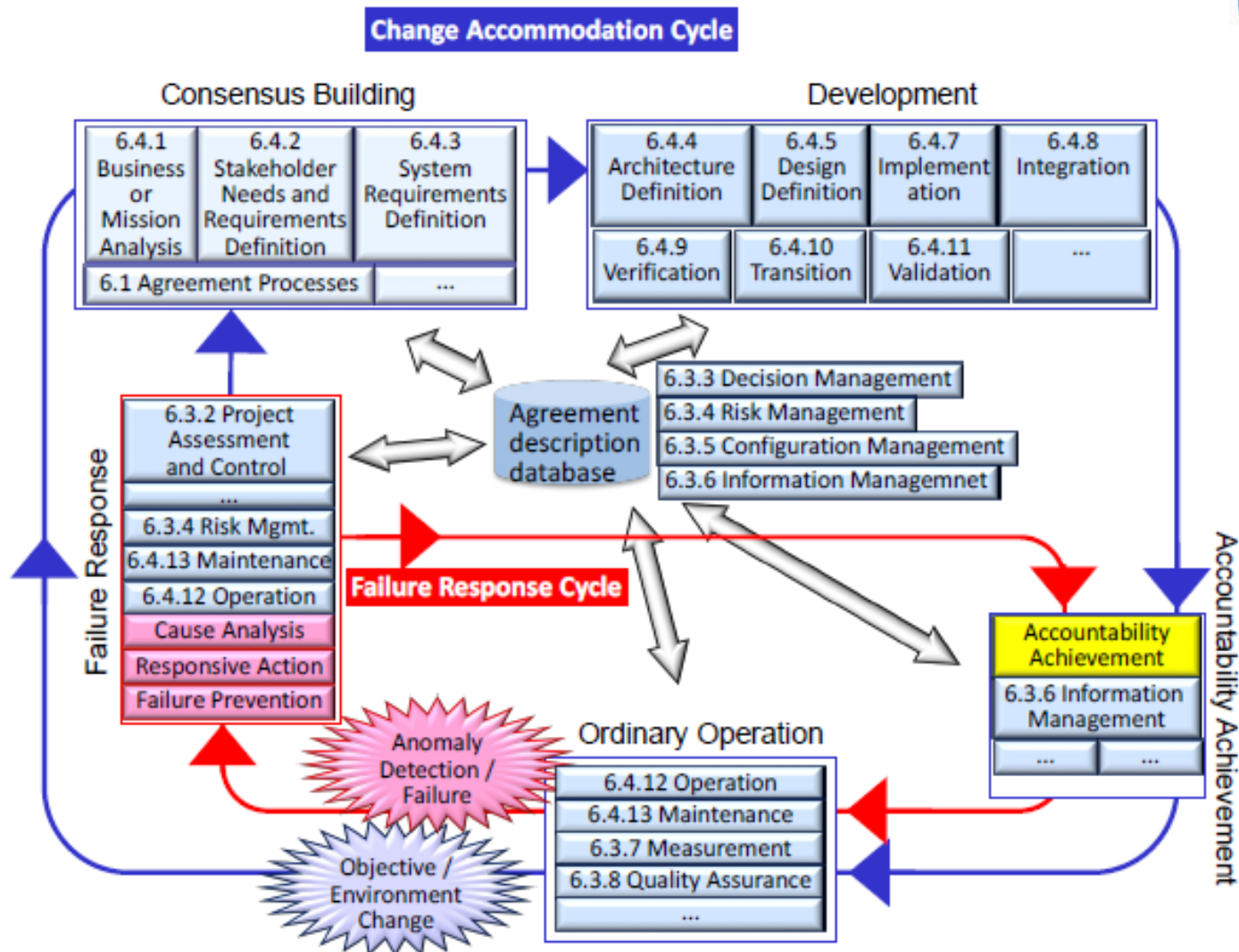


Figure A.1 – DEOS life cycle model ([1], adjusted)

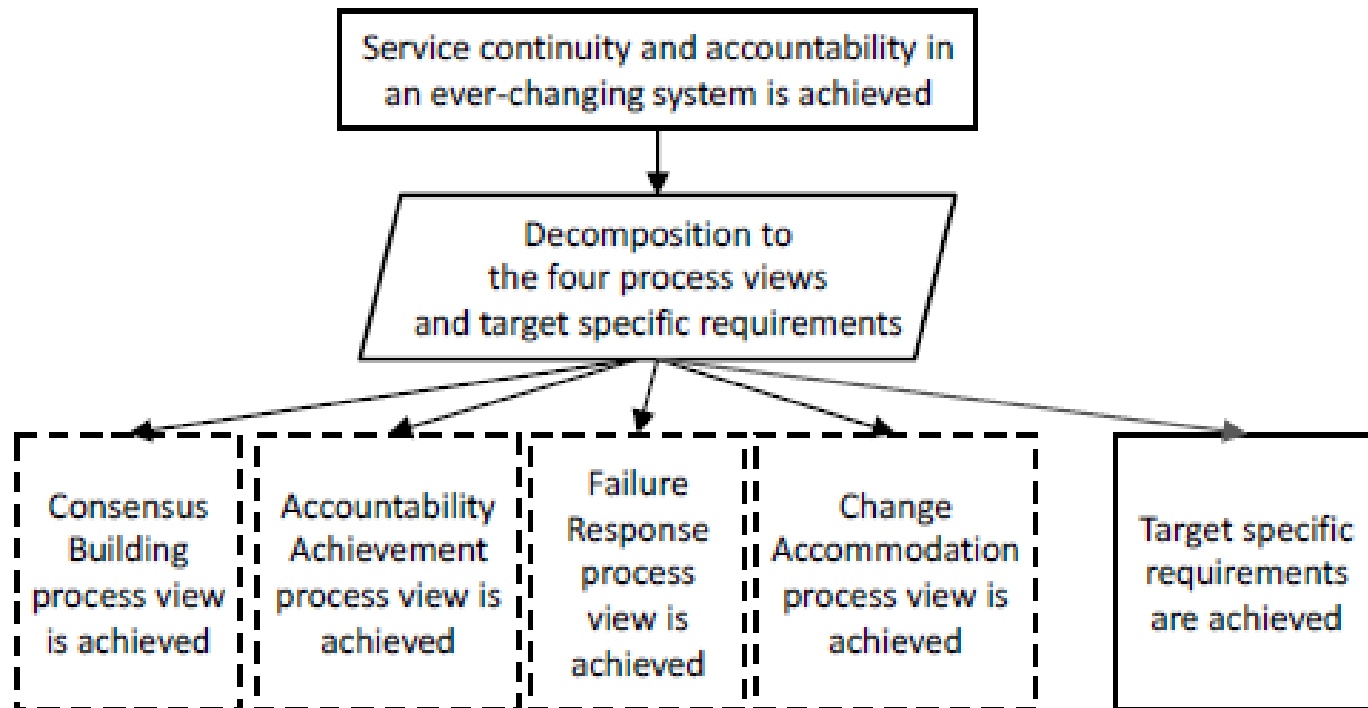


Figure B.1 – Overall argument

関連する技術・考え方

- **PDCA**

- Plan、Do、Check、Actionによる継続的改善

- **システムズエンジニアリング**

- 「システムの実現を成功させることができる 複数の専門分野にまたがるアプローチおよび 手段」
(INCOSE SE Handbook, 2000)

- 総合的思考

将来に向けて

現在の具体的課題(1)

- 設計・開発と運用が同時進行するシステムの総合信頼性の担保
- 派生開発に関連する総合信頼性の担保
- 個別に(他社により)に開発され、他社により運営されるシステムとの接続において不具合が生じた場合、いかに自社システムが無実であることを証明するか。(例えば、巨大サーバーとの接続やIoTにおけるセンサーからの情報)
- 事故が起こった時の説明責任をどのように果たしたらよいか(例えば自動車走行系、医療行為)
- 今後、特に、人工知能やビッグデータに依存するシステムの不具合時の説明責任をどのように果たすか

現在の具体的課題(2)

IoT、AI …… (技術)

自動運転、医療システム…… (システム)

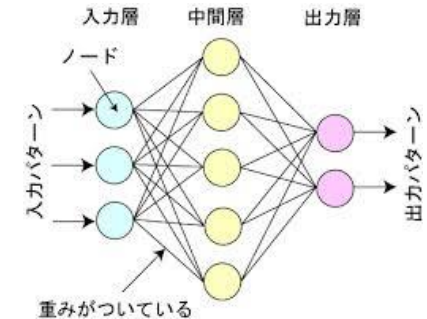
Industry 4.0、Society 5.0 (社会インフラ)

- 生活の基本的なインフラストラクチャであるためディペンダビリティ(総合信頼性)が極めて重要
- オーナシップが異なるサブシステムからなり、変化しつづける統合システム
- AI(人工知能)系のシステムではシステムの挙動が学習データに依存する

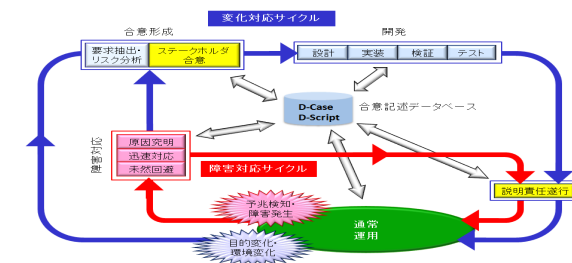
説明責任の全うが可能なシステム

AI(人工知能)系のシステムでは システムの挙動が学習データに依存する

- なぜシステムがそのような動作をするのかを論理的に説明することができない。リアルタイムで学習する場合には、更に問題は複雑になる。
- データの精度(誤差)や誤データ、偽データに対する対応が必要となる。
- ヨーロッパではAIシステムに対する説明責任を問う方向の議論が進んでいる。
- 必然的にプライバシーの問題が関係する
- AIシステムの学習データと動作の記録と監視による説明責任の全うが必要になるであろう。

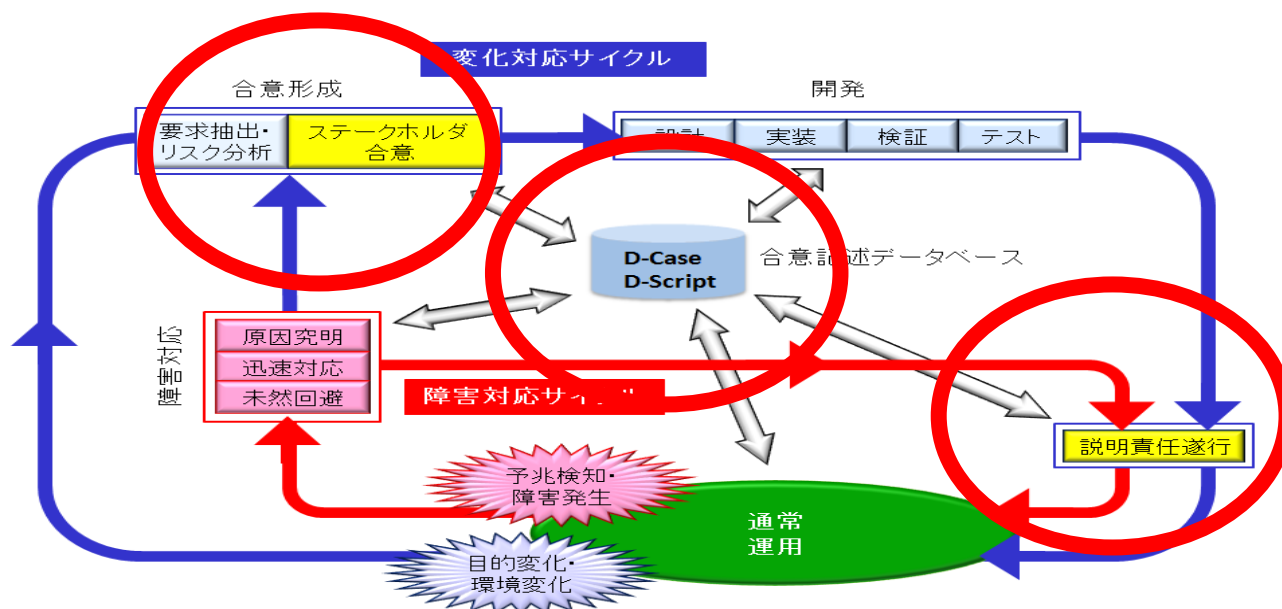


学習データの
精度、誤デー
タ、偽データ



説明責任を中心にした考え方

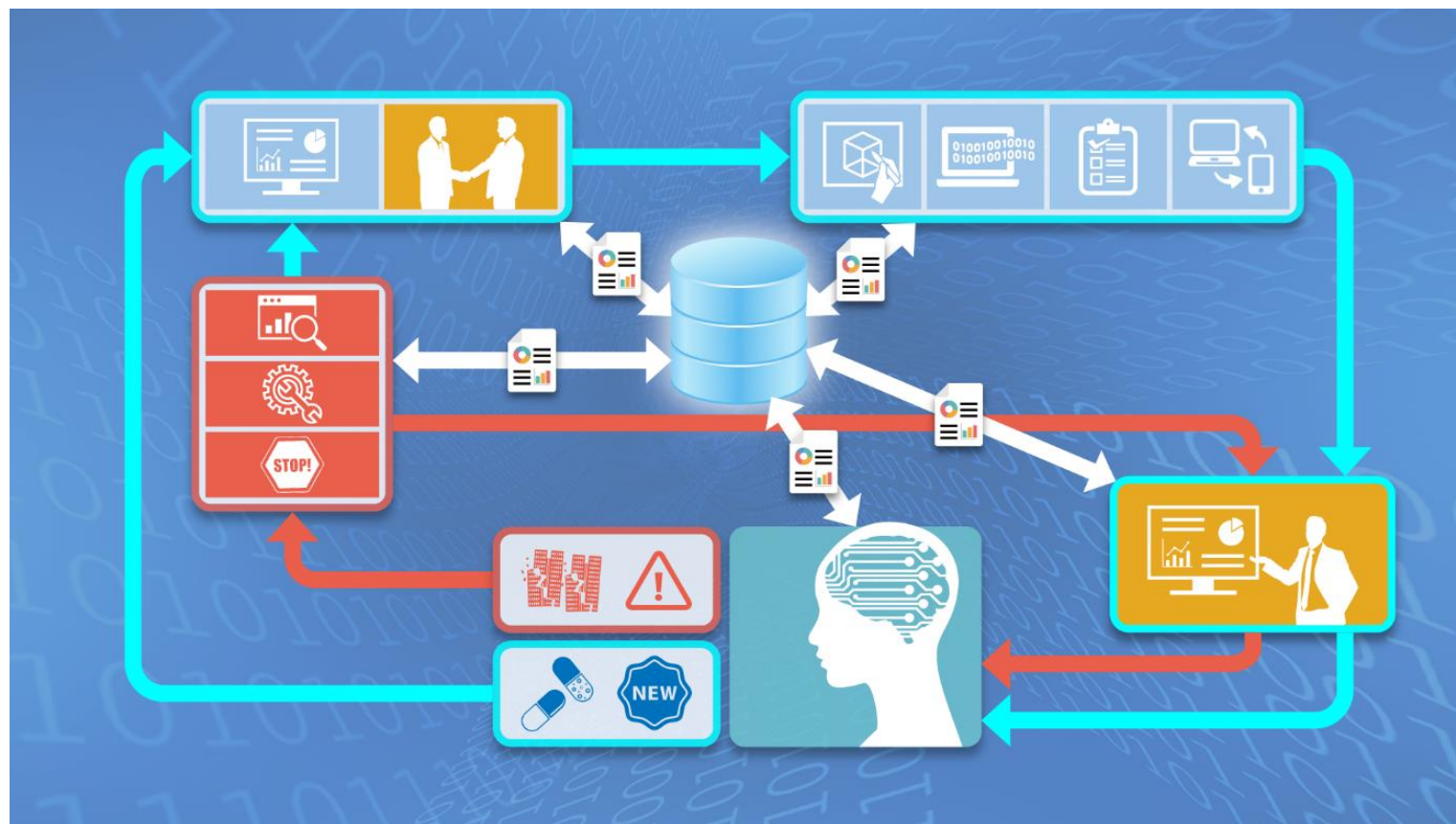
- 合意の形成と、合意ならびにシステム状態の記録による説明責任の全う
 - 自動運転システム
 - ドイツPEGASUSプロジェクトの例、状況が無限にある
 - 医療システム
 - 理化学研究所 医科学イノベーションハブ推進プログラムの例
 - 健康医療データベース、機器、操作、治験



医科学イノベーションハブ 推進プログラム(理化学研究所)



<http://www.riken.jp/research/labs/mih/>

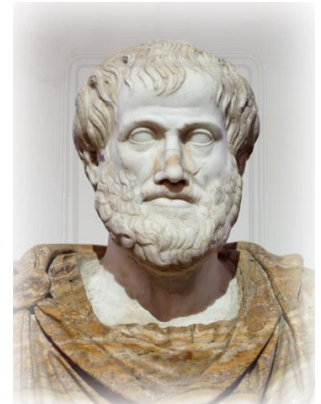


閉鎖系科学から 開放系科学へ

閉鎖系科学から開放系科学へ(1)



- 元来、学問は全体を見ていた(e.g. アリストテレス)。常に状況に依存していたので、基本原理を抽出しにくかった
- 中世になると、すべての物は神によって作られ、最初から存在し、変化しない、と考えられるようになった
- デカルトの還元主義により、基本原理の解明が進み、近代科学が勃興し、産業革命へと導いた。



René Descartes
1596 –1650



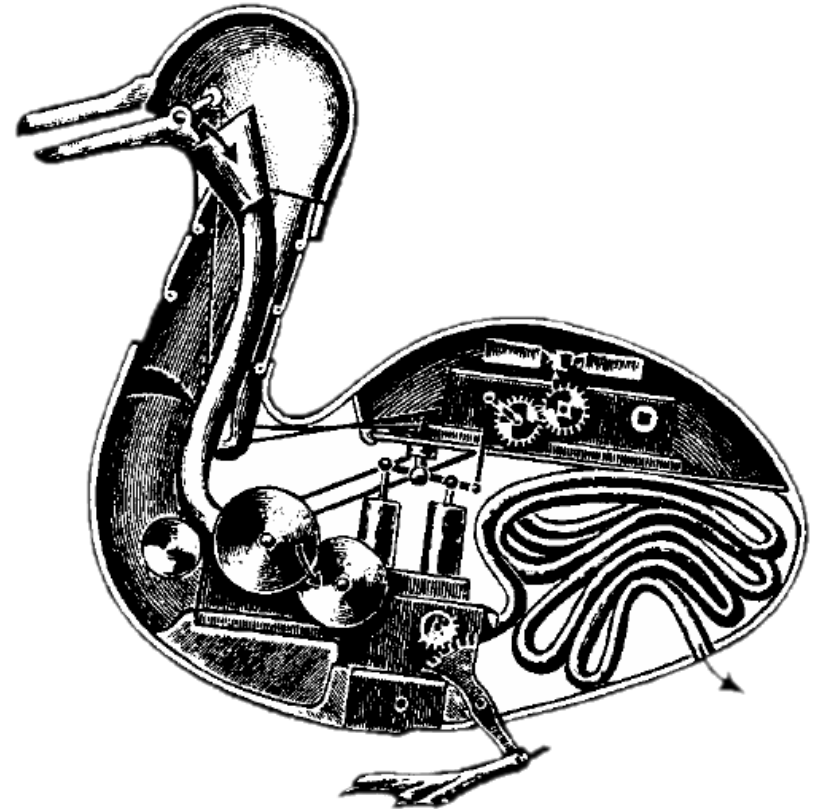
方法序説、1637

1. 明証的に真であると認めたもの以外は受け入れない
2. 問題を小さな部分に分ける
3. 単純なものから始めて複雑なものへ
4. 見落としが無いかなすべてを見直す

要素還元主義 (reductionism)

外界からの遮断
領域が定義可能

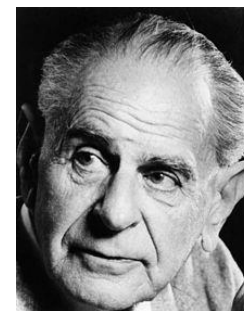
単純な問題群への分割
問題が分割可能



閉鎖系科学から開放系科学へ(2)



- 研究分野が細分化、時間軸を伴う全体的視野の欠如(生物・生命、社会)、現実世界への応用における問題(環境・持続可能性)
- オープンシステム的な見方の勃興(ポパー、クーン、ベルタランフィ、など)
- 身近な課題が発生: 巨大人工システム(インターネット、IoT、人工知能、自動運転、医療)

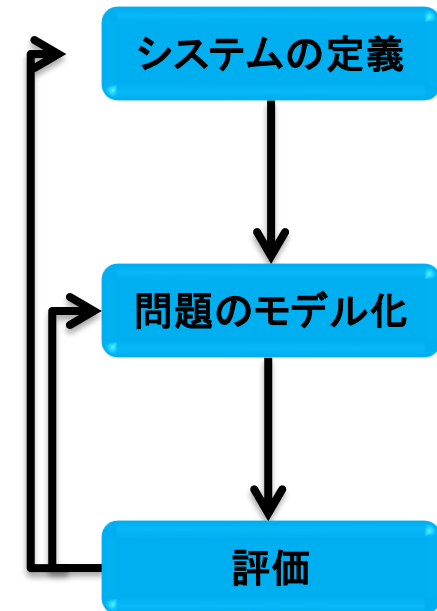


オープンシステムサイエンス

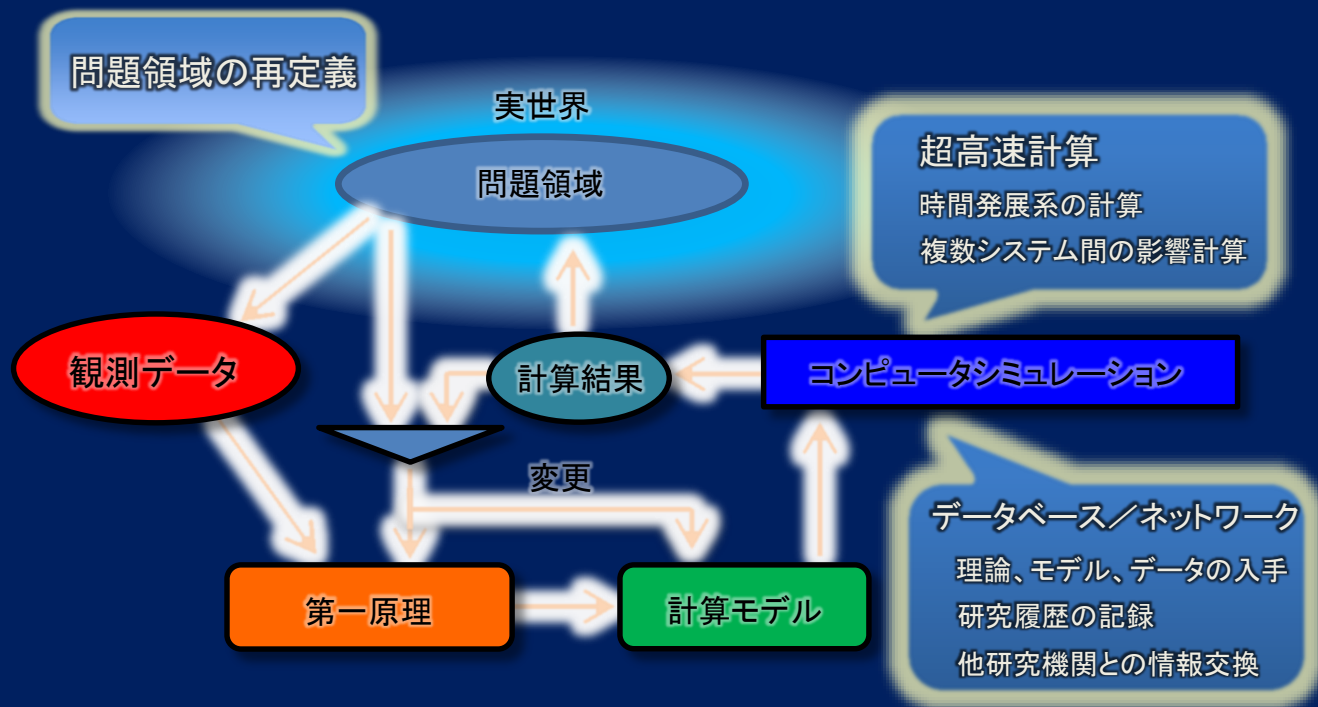
所 2016



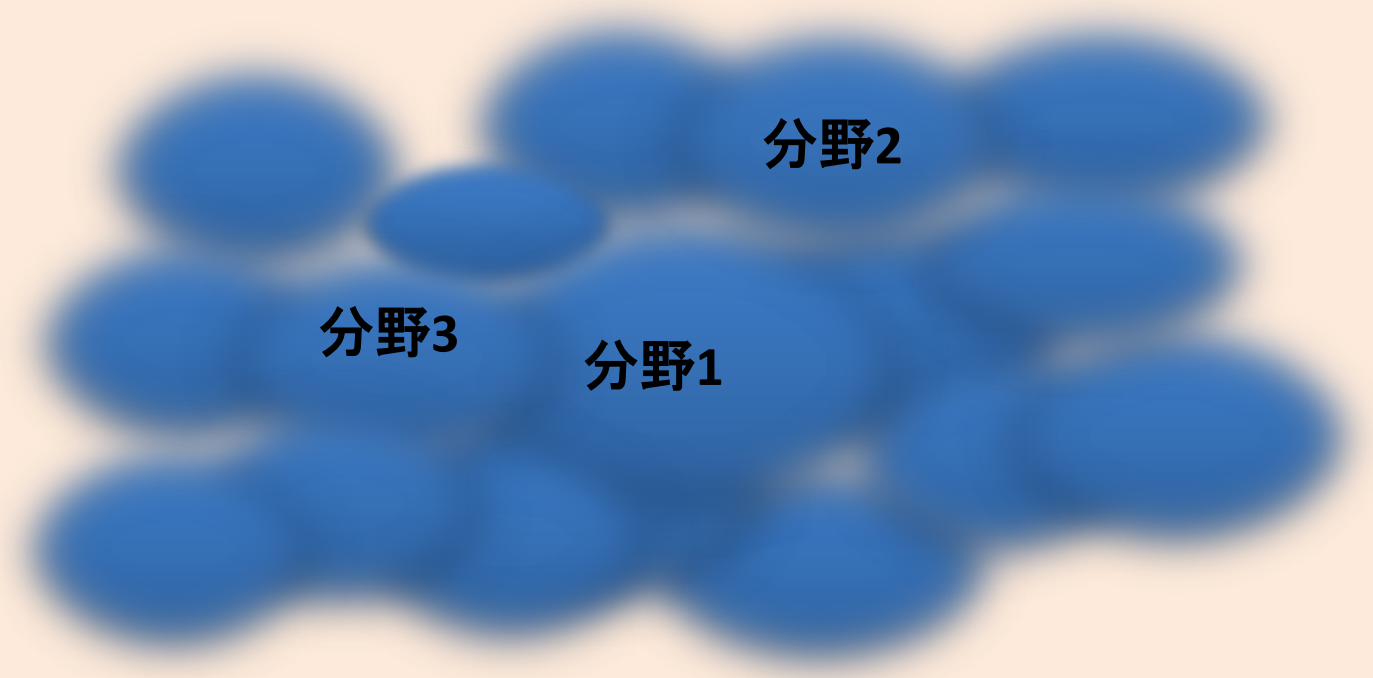
1. 問題が存在する領域(システム)を暫定的に定義する
2. 問題をモデル化する
3. モデルの振る舞いが時間経過とともに
 1. 自己矛盾を起こすことがないか
 2. 実システムの挙動と乖離することがないかを調査する
4. もしも許容範囲を超えた矛盾や乖離があれば
 1. 問題のモデルを変更
 2. 必要に応じて問題領域(システム)を変更してモデルを再構築する
5. 満足する結果が得られるまでこれを繰り返す



オープンシステムサイエンスと シミュレーション



統合プラットフォームによる 総合的問題解決



技術的課題

人工知能

Iot

ビッグデータ

セキュリティ

安全性

プライバシー

...

社会受容性

倫理的課題

まとめ

- DEOS/IEC62853は開放系科学の方法論の具体的な形であり、ソフトウェアシステムに限らず、多くの分野に適用できる。
- シミュレーション技術との統合により、社会システム設計、環境設計、企業経営など、新たな分野への適用が可能である。
- AIシステムを含む今後の社会インフラの設計・構築・運用における重要な規範を提供できる。
- 技術的課題に加え、倫理的課題が重要になる。

開放系科学方法論 (Open Systems Science)

開放系総合信頼性 (Open Systems Dependability)

IEC 62853 Open Systems Dependability

ご清聴ありがとうございました



一般社団法人 ディペンダビリティ技術推進協会

IEC 62853 Open systems dependability
を推進します。

引き続きご支援をよろしくおねがいします

