デジタルプラクティス　Vol.10 No.1(Jan. 2019)

特集号招待論文

開放系総合信頼性の標準化～CREST研究プロジェクトとIEC標準化の相互作用～

木下 佳樹[1]　武山 誠[1]　中川 雅通[2]　森田 直[3]　山浦 一郎[4]

[1]神奈川大学　[2]パナソニック　[3]ソニーCSL　[4]富士ゼロックス

システムは時とともに変化し，また，異なるステークホルダは異なる視点からシステムを見る．その結果，システムの記述は一般に不完全とならざるを得ない．これらの事実を出発点としてサービスを継続して提供する能力を考える総合信頼性（dependability）の研究が，DEOSプロジェクト（科学技術振興機構CREST制度「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」研究領域）において進められ，その成果として，開放系総合信頼性（open systems dependability）の概念がDEOSプロセスとして提出された．この概念は研究プロジェクト期間中に開始されたIEC TC56 Dependabilityによる標準化活動における議論によって洗練され，4つのプロセスビューとしてまとめられて国際標準IEC 62853 Open systems dependabilityとして2018年6月に発行された．

この国際標準は総合信頼性を説明責任達成によって担保する立場を取っている．たとえば，AI，IoT，セキュリティなどの分野においては，総合信頼性の達成には，要求されたときに要求どおりに遂行するだけでは不十分であると考えられる．そのため，総合信頼性の根拠として，要求仕様を満足することだけでなく，説明責任の達成が取り上げられている．説明責任達成を信頼性の根拠とするアプローチは，深層学習などのために，完全な要求仕様記述を前提とすることが適切でないシステムに対するアシュランス議論の枠組みとしてはたらくことが期待されている．この方向の標準化活動がIEC TC 56 WG 4 Information systemsおよびISO/IEC JTC 1/SC 7 Software and systems engineeringなどにおいて開始されつつある．

本稿では開放系総合信頼性の概要と，この概念を国際標準の体系にどのように組み込んだかについて解説し，合わせて，学界の研究プロジェクトから国際標準化活動まで一貫した活動を戦略的にどのように進めたかについて，研究活動マネジメントの視点から記す．

1. はじめに

現代社会ではさまざまな活動が「システム」の考えをもとに進められている．ここでのシステムは，情報科学，システム科学におけるもので，主要な国際標準では以下のように規定されている．自然科学におけるシステムとは，共通の背景を持つものの，異なるものである．

system
combination of interacting elements organized to achieve one or more stated purposes[8]
system,<in dependability>
set of interrelated items that collectively fulfil a requirement[1]

ここで，アイテムは，（サブ）システム，部品，構成品などを指す言葉である．また，システムには，付随する装置，設備，材料，道具，計算機プログラム，ファームウェア，技術文書，サービス，運用に必要な人員，支援などをすべて含むとされる．航空機システムや車載システムなどのように装置を中心に考え，その他の付随するものを含むと考えるシステムもあり，交通システム，食品流通システム，宇宙防衛システムなどのように，サービスを中心として考え，その実現のための装置その他を含むと考えるシステムもある．

さて，このようなシステムおよびシステムへの要求は時とともに変化する．また，異なるステークホルダは異なる視点，立場からシステムを利用し，要求を出す．あらゆる変化，あらゆる視点を考えに入れることは不可能であり，システムの記述は一般に不完全とならざるを得ない．このようなシステムは開放系（open system）と呼ばれる．開放系に特有の課題を解決する総合信頼性（dependability）は開放系総合信頼性（open systems dependability）と呼ばれる[9][4].

開放系総合信頼性の研究はDEOSプロジェクト（科学技術振興機構CREST制度「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」研究領域）において進められ，その成果として，開放系総合信頼性の概念がDEOSプロセスとして提出された．この概念は研究プロジェクト期間中に開始されたIEC TC56 Dependabilityによる標準化活動における議論によって洗練され，4つのプロセスビューとしてまとめられて国際標準IEC 62853 Open systems dependability[4]として2018年6月に刊行された．

開放系総合信頼性の達成には，従来考えられてきた「要求されたときに要求どおりに遂行する能力」だけでは不十分だと考えられる．そのため，開放系総合信頼性の根拠として，要求仕様を満足することだけでなく，説明責任の達成が取り上げられている．このアプローチは，完全な仕様記述を前提としない分野におけるアシュランス議論の枠組みとしてはたらくことが期待されており，この方向の関連活動がIEC TC 56 WG 4 Information systemsおよびISO/IEC JTC 1/SC 7 Software and systems engineeringにおいて開始されつつある．

本稿では開放系総合信頼性の概要と，この概念を国際標準の体系にどのように組み込んだかについて解説し，合わせて，学界の研究プロジェクトから国際標準化活動まで一貫した活動を戦略的にどのように進めたかについて，研究活動マネジメントの視点から記す．

2. 開放系総合信頼性とは

2.1 総合信頼性

総合信頼性（dependability）の国際標準における定義は

dependability, <of an item>
ability to perform when and as required[2]

である．伝統的な信頼性（reliability）を超えて，時を経ても首尾一貫して要求事項を満たし，

期待に応えていく，システムやその部品の能力が総合信頼性である[10].

サービス停止の頻度や製品故障などの頻度を系統的に減らし，その影響を最小限に抑えると総合信頼性が向上する．設計および設計能力の向上，故障の根本原因の除去，複雑なプロセスの簡素化，システム異常の緩和，耐故障性を持つ設計と利用，故障の回避と予防，保守活動管理，完整性（integrity）追求による利用者からの信用獲得などの活動を，システムライフサイクルを通じて展開することにより，総合信頼性を向上させることができる．

システムへの要求事項のうち，何らかの機能の遂行における信頼性，可用性，保守性，支援性（supportability）についての要求を，総合信頼性要求事項と呼ぶ．たとえば，自動車のブレーキの瞬間故障率がp未満となるようにせよ，というのは，ブレーキという機能の信頼性に関する要求だから総合信頼性要求事項である．また，ソフトウェアソースコードのインデンテーションを指定どおりに行え，という要求事項があったとすれば，これは保守性維持のための要求であるから総合信頼性要求事項と見ることができる．

総合信頼性要求事項には何か遂行すべき他の要求事項が付きものである．上記の場合，ブレーキに関する機能要求事項や，当該ソフトウェア全体の要求事項がそれにあたる．

総合信頼性には，信頼性，可用性，保守性などのような客観的な特性だけでなく，ある機能に関する信頼感のような主観的な特性も含まれる．

2.2 開放系

国際標準ではシステムが一般的に第1章のように定義され，システムには，その外との境界があるものとされる．システムの運用では境界の外からの資源が必要とされる場合もある．また，システムの利用や保守に関する条件も要求事項に記されているものとされる．そのうえで，システムのうち，特に開放系（open system）と捉えることのできるものが次のように定義されている．

> **open system**
> system whose boundaries, functions and structure change over time and is recognized and described differently from various points of view[5]

システムの内と外とに境界があり，その機能や構造が要求事項によって定義されている点では，開放系も普通のシステムと同じである．しかし開放系では，境界，機能，構造が時や視点によって変化するとされる．

変化は，特定の目的に適応することだけでなく，システム自身の自律的な発展による変化も含む．いくつかの異なる機関にまたがったシステムでは，あちらこちらの変化が必ずしも協調しない形で進む．また，いわゆる学習を行うシステムでは，ユーザに見える機能も予測しがたい形で進化する．これらの場合には，制御の統治が十分に得られない場合があることから，開放系の典型的課題が発生する．

システムの変化や視点による相違を問題にしない場合も，もちろんあり得る．そのような場合には，システムを閉鎖系，closed systemなどと呼ぶのが適切であろう．

開放系には次のような特徴がある．

- 対象システムだけでなく，それを取り巻く環境を対象システムと同程度の比重で考えに入れなければならない（開放系では，境界の外にあって対象システムと関係するものたちが

重要な役割を果たす．これらのものをシステムの環境と呼ぶ）．
- 対象システム自身やその環境は不完全かつ不確定である．
- システムの仕様を完全に記すのは困難であることに加え，たえず変化していく開放系では，その困難は増すばかりである．したがって，システムを完全な形で記述するのが理想だと考えるのではなく，むしろ，システムの記述は不完全であることから出発して考える方が自然で実態に合っている．
- システムは不完全であるだけでなく不確定である．対象システム自体の設計や変更は，システムのステークホルダが掌握するが，対象システムが繋がっている外部システムや社会環境（法律など）などのシステム環境の変化は，ステークホルダが掌握できない．つまりシステムの環境は常に，定まったものではない（不確定である）という前提に立つのが現実的である．
- ブラックボックスの部品は，部品供給者によってその実体が入れ換えられる場合がある．その入れ換えの影響を部品の利用者側で制御するのは困難である．
- ステークホルダによる理解も不完全かつ不確定である．
- たとえシステムの記述が完全になされたとしても，ステークホルダによる理解が完全だとは限らない．ステークホルダたちが共通の理解を持つことは自明ではない．
- システムについて語るための語彙がステークホルダによって異なる．ある会社の業務システムについて，経営者が語るのと，会計部門担当者，情報処理技術者などが語るのとでは，語られる側面も用いられる用語も異なるため，これらのステークホルダ間の意思疎通を図ることは自明ではない．

なお，上に定めた用語open system中の‘open’の意味は，他の用語（Open Source Software，Open Systems Interconnection model等）での意味とは異なる．

開放系であるが故に発生する典型的な問題点をいくつか以下に列挙する．多くは従来から問題とされながら，従来の総合信頼性の建前的前提のもとでは対処し難かったものである．読者自身の経験したシステムのうち，下記の問題が上記の特徴により特に顕著になったものをもって「開放系とはどのようなものか」のイメージとすることができる．

- システムへの要求項目が曖昧である．
- いくつかのソフトウェアを組み合わせる場合，各ソフトウェア仕様の間に齟齬が生じる．
- SEや設計，テストなどの各開発チーム間の用語が相異なる．その結果，提出書類（要求，仕様書，設計書，試験報告書など）が互いに整合的でなくなったり，チーム間で文書の理解の仕方が相違する．
- 管理，運用，保守過程での変更や修正の記録もれや不達が生じる．
- 事業目的が変わる．
- 利用者環境が変わったり，システム性能への期待の度合いが変わる．
- 顧客数激増のためにユースケースが変わる．
- テクノロジー革新が起こる．
- 新たな国際標準や法令が施行される，あるいは既存のものが改訂される．
- オペーレータの能力が変わる．
- ネットワーク環境が変わる．しばしば思いがけない変化がある．
- 対象システムが外部からの悪意を持った攻撃にさらされる．
- ブラックボックス部分が更新される．

2.3 開放系総合信頼性

長期間にわたる変化や予期しなかった障害の下でも持続的にサービスを提供し，開放系の総合信頼性を向上させるためには，システムのライフサイクル全般にわたって絶え間ない改善活動を系統的に繰り返す必要がある．

開放系に対する総合信頼性管理は自明ではない．システムの仕様や要求事項，さらには目的までもが変化し得るため，明示的な合意事項に従った管理をするだけでは十分な総合信頼性管理ができないからである．システムおよびその環境について，ステークホルダの間で形成されている共通の理解に基づいて，場合によっては明示的な合意事項を超えた作業が必要である．開放系総合信頼性向上のためには，システムに関する前提が成り立たなくなったり，諸々の変化によって要求事項が無効になったりしたために障害が起こったとしても，システムに対する信頼を守ろうとするステークホルダの刻苦勉励が必要である．

また，システムは常に変化し発展するものである．したがって，総合信頼性管理の範囲を常に見直し修正して新たな合意文書を提供し続けるプロセスを明確にし，さらに新たな合意事項が説明責任の分担に関する合意につながるような管理が必要である．

障害の原因には，予期しなかったもの，予期できなかったものもある．当然ながら，これらを予防することはできない．したがって，システムの主要な機能を同定し，原因がなんであれ，それらの機能が働かなかった場合の結末を見越して，その結果の被害から迅速に復旧する，あるいは被害が出ないような冗長さをシステムに組み込んでおく，などの措置が必要である．

総合信頼性の能力‘ability to perform when and as required’のうち，特に開放系において必須でありながら実現が自明ではない部分をより明確にしたものが，国際標準で用語定義された「開放系総合信頼性（open systems dependability）」である．

> **open systems dependability**
> ability to accommodate changes in purpose, objectives, environment and actual performance and to achieve accountability continually, so as to provide expected services as and when required[6]

共通の理解はいわゆるBCP（Business Continuity Planning）の背景となるものといえる．しかし，開放系総合信頼性には，総合信頼性を保つために，場合によっては明示的に合意された事項を超える作業が，システムに関する共通の理解に基づいていることを前提に遂行されることが求められる．したがって，開放系総合信頼性の根拠を，明示された合意事項，つまり契約の内容や要求仕様書，非常時の対策会議開催要領などのみに求めるわけにはいかない．

開放系総合信頼性の究極の根拠は，説明責任に置かれる．事前に特定された説明責任者が，事前の合意に従って賠償，改善実施等を含む説明責任を達成する体制の保証が開放系総合信頼性達成のために不可欠である．

システムが求められる性質を満たすことの保証は常に不完全なものでしかなく，求められる性質はいずれ破綻するのが普通である．したがって，究極の根拠を，求められる性質が満たされることに置くのではなく，その性質が破綻した場合の説明責任に置くのが適切である．

システムの信頼性を説明責任に結びつけるこの考えは，少なくともこれまでの国際標準には見られないものであるが，開放系を対象とする場合には，避けられないアプローチだと考えられる．なお，このアプローチは求められた性質の保証をできる限り完全にする努力を否定せず，むしろその努力を当然の前提としたものである．

説明責任から，信頼性のための意思疎通（dependability communication）の必要性もおのずから導かれる．説明責任達成のためにシステムの利害関係者（stakeholders）は互いに協力しなければならない．

なお，「説明責任」という日本語の単語の一般用語としてのニュアンスと，IEC 62853で定義されているaccountabilityの意味（これは英単語の一般用語としてのニュアンスを反映している）の違いについて注意しなければならない．IEC 62853における「説明責任」は，単に謝罪会見を開くというよりも，トラブル発生原因の合理的な説明を与える責任とトラブルによる損害の賠償責任，さらにそのための体制を普段から整え，明らかにし，納得を得ておくことを意味する．

2.4　4つの活動

開放系総合信頼性活動で，従来型の総合信頼性管理になかった課題は，予期しなかった障害や環境の変化があった場合のサービス継続のための努力をどのように行うか，である．予期しない障害や変化への対応なので，事後措置が中心である．しかし事後措置を迅速かつ円滑に進めるためのさまざまな事前措置を考えることはできる．以下の4つの活動によってそのような措置を事前，事後に講じることができる．

- **合意形成**　ステークホルダによる合意形成と理解促進の支援
  合意事項を明示することが必要なのは言うまでもない．
  明示された合意事項を超えて，システムに対する信頼を守る活動をステークホルダが展開するためには，システムや事業目的などに関する共通の理解を確立することが必要である．
  共通理解や合意事項の記述の枠組み（語彙とその基本的性質）の確立は，ステークホルダ間の正しいコミュニケーションを支援，促進するために必要である．
- **説明責任遂行**　システムライフサイクルプロセスに関する説明責任遂行の支援
  説明責任が曖昧であれば，障害発生後のシステム稼働が困難になる．
  合意事項達成のために最善を尽くし，達成できない場合の潜在的被害に対する補償を担保しておくことが必要である．
  その前提として，合意事項の不履行がステークホルダおよび一般社会に与える結末（影響）を明示しておかなければならない．
- **障害対応**　障害に対する短期的対応（応急措置）
  障害発生時に迅速かつ適切な措置をとって，サービスの中断や被害を極小化あるいは緩和することが必要である．これには，障害の予兆を検知してしかるべき方策を講じることも含まれる．ここでも，明示された合意事項を超えて，その場の状況に応じて最も便宜の得られる応急措置が求められる．
  いわゆるgraceful degradation（障害の程度に応じた劣化サービスの提供．これにより完全停止を可能な限り防ぐことができる）によって，最大限のサービスを継続することが求められる．
- **変化対応**　障害に対する中長期的な対応
  障害の原因となり得る要因を継続的に取り除き，常にシステムを改善し続けることが必要である．
  予期しなかった／できなかった障害の再発を防止する（二の矢を防ぐ）ために，必要に応じてシステムを改修する体制が事前に確立されている必要がある．
  環境や事業目的の変化に対応するためのシステム改修についても同様である．たとえば標準や法令の変化に対応しなければ，システムは社会的に認知されなくなっていく．

これら4つの活動は，互いに関連付けて進めていかねばならない．形成された合意は，他の3つの根拠となる．説明責任遂行活動は，形成された合意の実現を助けるばかりでなく，障害対応活動や変化対応活動の説明を提供することによって，システムへの社会からの信用を得る．障害

対応活動は説明責任遂行活動のための情報を提供するほか，障害の再発防止のための変化対応活動を引き起こす．変化対応活動は共通理解と明示的合意を変更する場合の合意形成活動を引き起こす．

これら4つはどれも，開放系に限らずどんなシステムの総合信頼性にも必要なことだが，特に，常に変化にさらされる開放系の総合信頼性管理においては不可欠なものである．

2.5 開放系総合信頼性標準化の意義

IEC 62853は，いわゆるガイダンス標準の1つである．望ましいシステム属性（性質）を明らかにし，達成に向けた方策を標準化する．通常の標準化は，関連業界で課題明確化の議論が進み種々の方策の実績が得る積まれた段階で，相互運用の円滑化等を目的に開始される．しかし，IEC 62853の標準化活動では，逆方向の効用，つまり，課題明確化と方策評価法の議論をそもそも開始するために必要な枠組みを与えることが意識された．共通認識と標準の存在自体が，開放系総合信頼性の達成に必要なためである．

標準は，「何についてどの程度のコストでどこまで対策すればよいのか」の議論に枠組みを与える。これは科学，論理のみでは線引きできず，利害関係者の判断，さらには社会全体の曖昧な通念による。枠組みなしには，開発側の無限責任，利用側の自己責任のみといった極論につながりやすい。IEC 62853は，前節の4つの活動の必要性と限界の共通認識を醸成し，その達成度を評価軸とする議論の開始を可能にする．

また開放系総合信頼性は個々のシステムや業界の個別の努力だけでは達成できないことも，標準化を先行させる必要性につながる。1つの対象システムの総合信頼性の議論には，サプライチェーンから提供されるサブシステム等だけではなく偶発的に連結しうる他システムの総合信頼性の議論も必然的にかかわる。 あらかじめ標準が準備されていることは，普段から連携しているとは限らない当事者間で議論を進めることを大きく助ける．

3. IEC 62853 Open systems dependability（開放系総合信頼性）の概要

前章では開放系総合信頼性を達成するために必要な活動を4つ提示した．これらの活動の要件を国際標準によって規定するためには，すでに存在するディペンダビリティやシステムライフサイクルプロセスに関連する国際標準の体系の中に開放系総合信頼性を位置付ける必要がある．本章では，IEC 62853 Open systems dependabilityによる位置付けを述べる．

3.1 システムライフサイクルプロセス

どんなシステムにもライフサイクルがある．国際標準におけるライフサイクルの定義は

> **life cycle**
> evolution of a system, product, service, project or other human-made entity from conception through retirement [7]

である．

ISO/IEC/IEEE 15288 System life cycle processesはライフサイクルを構成するプロセス（システムライフサイクルプロセス）を30個，4つのグループに分けて規定する．システムライフサイクルは，プロセス間の関連，組合せを定めて全体の活動を組織する．プロセスはアクティ

ビティから構成され，さらにアクティビティはいくつかのタスクからなる．特に，ISO/IEC/IEEE 15288は，ライフサイクルの活動をプロセス・アクティビティ・タスクの3つの階層構造で定め，以下の4つを与えることによって各ライフサイクルプロセスを規定する（**図1**）．つまり，1つのライフサイクルプロセスは，以下の4つを与えることによって規定されるとしている．

- プロセス名：プロセスの対象範囲を示唆する．
- 目的：プロセス実行の目的．
- アウトカム：プロセスが成功裏に遂行されたときに期待される，目に見える結果．
- アクティビティとタスクのリスト：アウトカム達成のために必要な要件，勧告あるいは取り得るアクション．

なお，ISO/IEC/IEEE 15288は特定のシステムライフサイクルを規定するものではない．

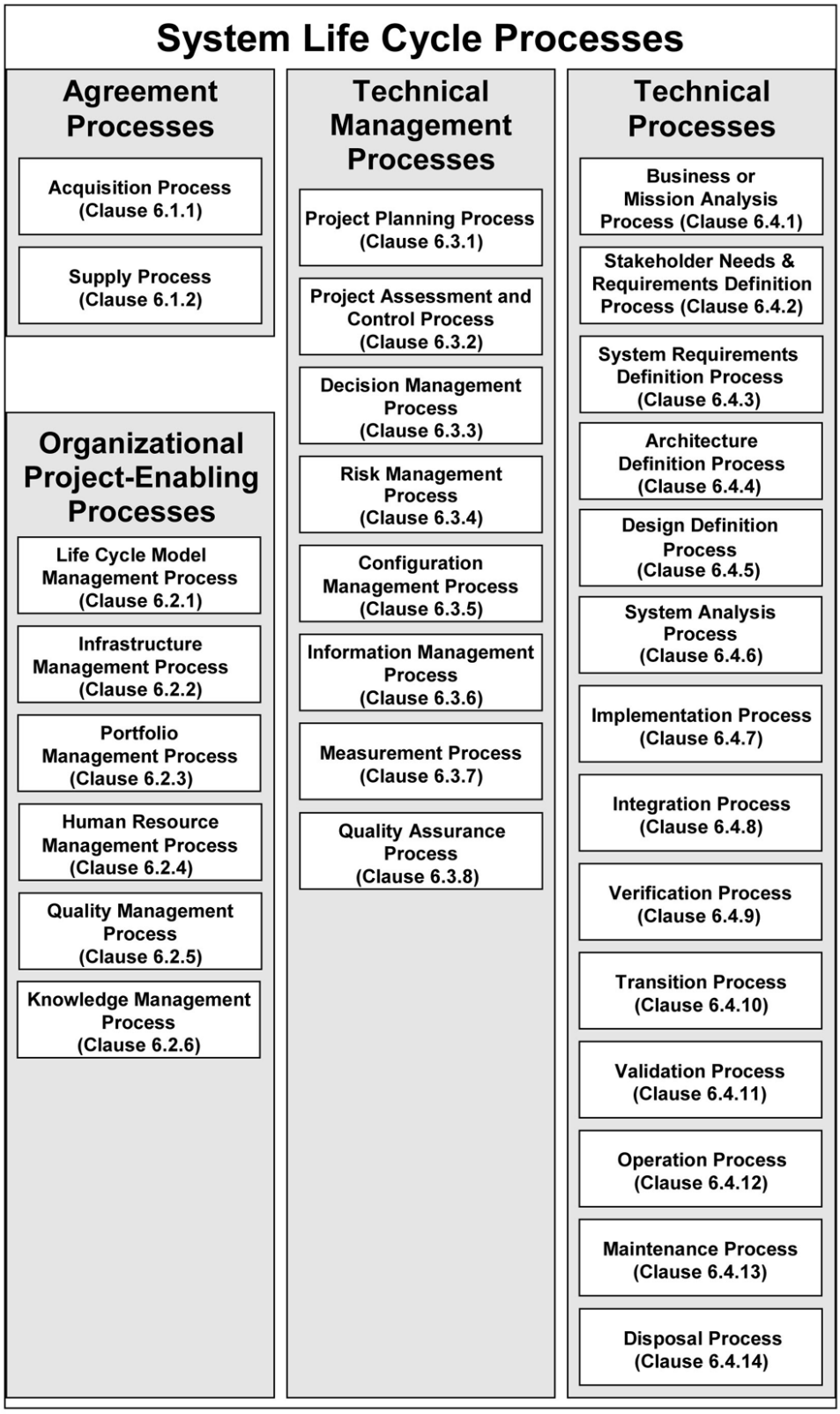

図1　ISO/IEC/IEEE 15288が規定するシステムライフサイクルプロセス
（ISO/IEC/IEEE 15288:2015 Figure 4）

3.2　プロセスビュー

開放系総合信頼性のための4つの活動を実現するために必要なタスクは，30個あるプロセスのあちこちに散らばっている．そこで，ISO/IEC/IEEE 15288:2015は，プロセスに加えて，プロセスビューと呼ばれる活動単位を説明している（Annex E. Process views）．たとえば合意形成に関係のある活動をひとまとめにするために，合意形成プロセスビューというものを考える．合意形成のために必要なアウトカムを設定し，それを実現するアクティビティやタスクを30のプ

ロセスのあちこちから引用してプロセスビューを規定する．アクティビティの集まり，という「実体」を持つプロセスに対し，その実体の別の「見せ方」を提供するのがプロセスビューだ，と見ることもできる（**図2**）．

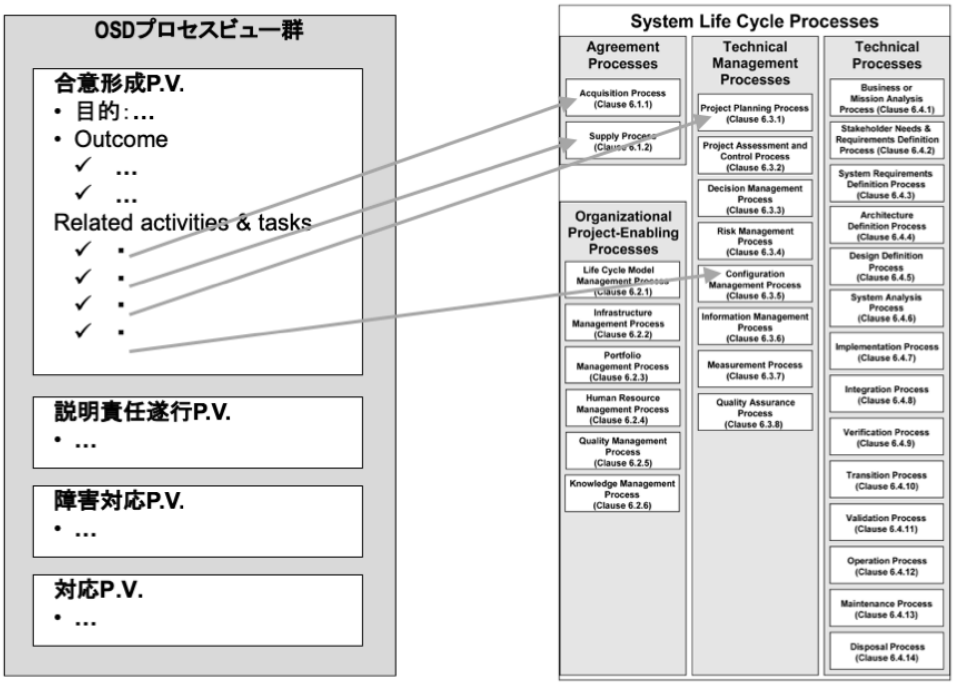

図2　OSDプロセスビューとシステムライフサイクルプロセスの関係

プロセスビューには，目的とアウトカムの記述はあるが，プロセスと違って，新たなアクティビティとタスクのリストはない．その代わりに，プロセスビューではISO/IEC/IEEE 15288に規定されているアクティビティやタスクを使ってアウトカムを達成する方法を規定する．つまり，1つのプロセスビューは

- プロセスビュー名．プロセスビューの対象範囲を示唆する
- 目的．プロセスビュー実行の目的
- アウトカム．プロセスビューが適切に遂行されるときに期待される，目に見える結果
- アウトカム達成のために用いるべきISO/IEC/IEEE 15288のアクティビティとタスクのリスト

の4つを与えることによって規定される．目的とアウトカムを規定するだけで，実際の活動は既定のプロセスを参照するだけなので，プロセスビューは「バーチャルなプロセス」と見なすことができる．

3.3　総合信頼性管理

総合信頼性管理（dependability management）は，国際標準体系ではIEC 60300-1 Dependability management – Part 1: Guidance for management and application[1]によって規定されている．この標準は総合信頼性の標準体系で最上位に位置付けられるもので，総合信頼性の概念を規定するものとされている．

総合信頼性の国際標準を司るIECの技術委員会TC 56 Dependabilityにおいて，我が国のnational committeeから開放系総合信頼性の標準策定活動の開始が提起されたとき，委員会では，IEC 60300-1に，総合信頼性の中の開放系総合信頼性の位置付けが記されることが新標準

策定のために必要であるとの議論があった．2011年に開始されたIEC 60300-1の改訂作業の機会をとらえてその記述が付け加えられた．

> Systems are becoming more complex and can exhibit the characteristics of “open systems”, “systems of systems” or “unbounded or weakly bounded systems”. The systems can be managed by different parties that have different objectives and can be at different stages of the life cycle. This, together with the scale and complexity of the system makes it difficult for any stakeholder to comprehend the system as a whole and changes are thus less predictable and controllable. For that reason, it is crucial for stakeholders to understand and agree on the boundaries of their responsibilities and to assign accountability for implementation. Planning for dependability needs to take into account the potential for major failures and changes outside respective boundaries as well as inside.[3]（下線は著者による）

IECの総合信頼性に関する国際標準の体系において，IEC 62853 Open systems dependabilityは，IEC 60300-1のこの段落を詳細化し，発展させる標準として位置付けられている．

3.4　4つの活動のプロセスビュー

IEC 62853の3つの規範参照（normative reference）標準のうち，IEC 60010-192は総合信頼性に関する用語定義である．その他の2つとの関連を**図3**に図示した．

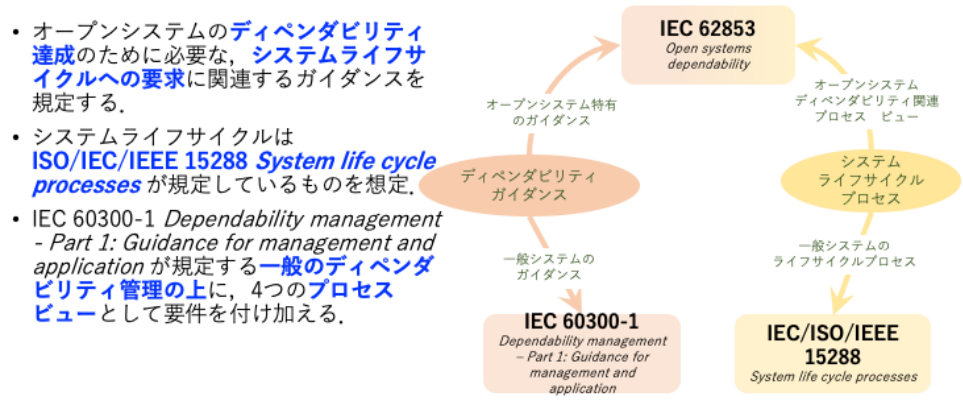

図3　IEC 62853とIEC 60300-1, IEC／ISO/IEEE 15288

IEC 62853は開放系総合信頼性向上のための4つの活動それぞれに対して1つづつ，プロセスビューを規定する．各プロセスビューで，そのプロセスビューのアウトカムの達成に，ISO/IEC/IEEE 15288に規定されたプロセス，アクティビティ，タスクがどのようにかかわるかが示されている．

- 合意形成プロセスビュー
  合意形成プロセスビューの目的はシステム，システムの目的，目標，環境，性能，ライフサイクル，およびこれらの変化に関する共通理解と明示的合意を確立し，維持することである（**図4**）．

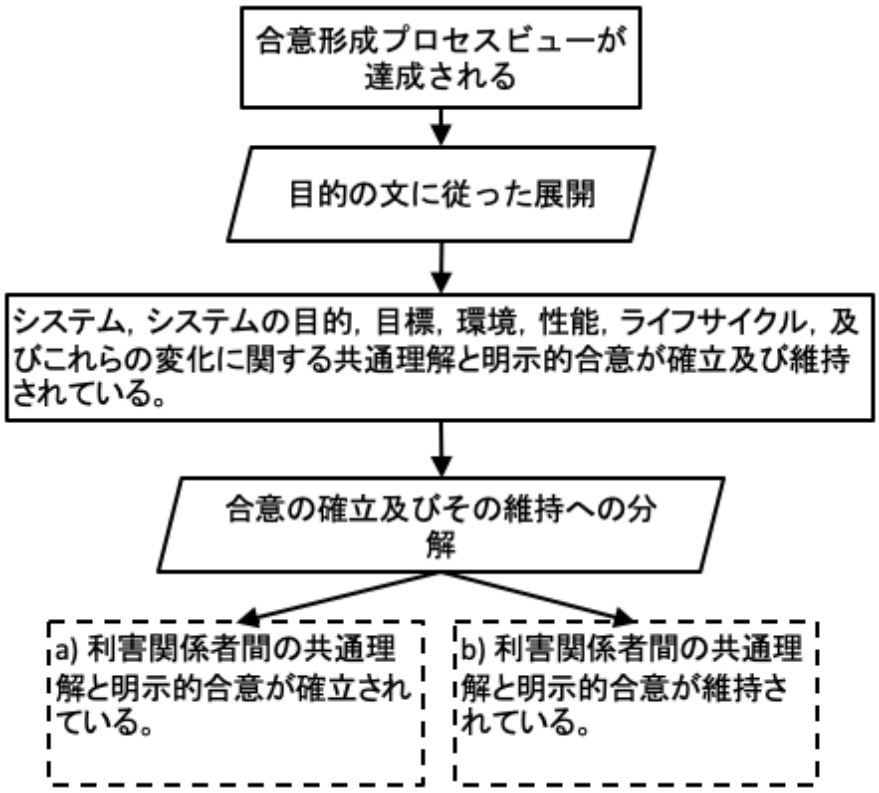

図4　合意形成

- 説明責任遂行プロセスビュー
  合意形成プロセスビューで確立された明示的合意事項に対して違反が生じた場合，その違反を原因とする何らかの帰結が，利害関係者および社会一般にもたらされる．ここで，「違反」は，故意や過失によるものだけではなく，自然災害などの不可抗力に起因するものも含めて考えられる（**図5**）．

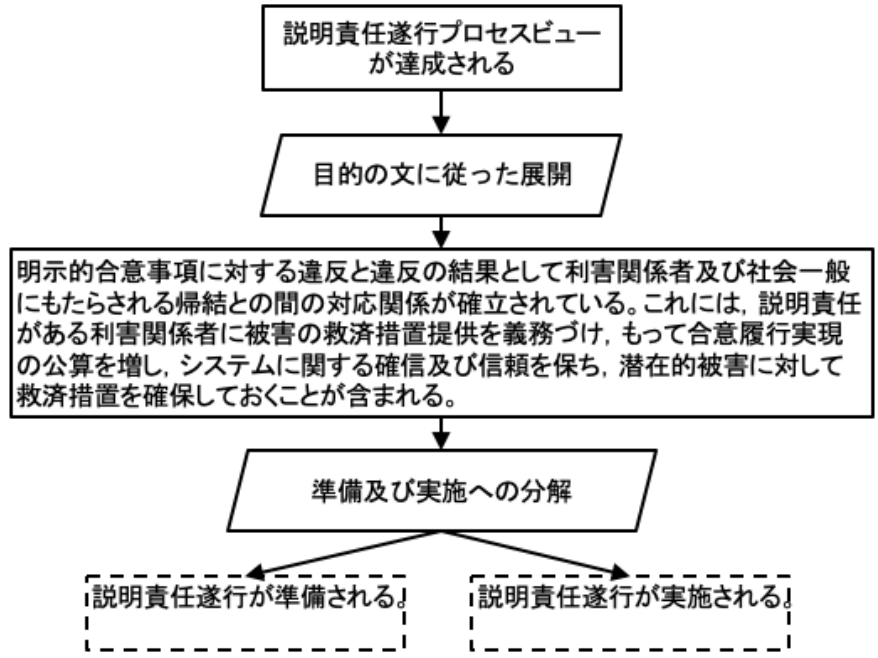

図5　説明責任遂行

説明責任遂行プロセスビューの目的は，明示的合意事項への違反とその帰結との間の対応関係を確立することである．これには，説明責任を持つ利害関係者に対して被害の救済措置提供を義務づけ，それによって合意実現の可能性を増やし，システムに関する確信と信

頼を保ち，潜在的被害に対して救済措置を確保することが含まれる．

- 障害対応プロセスビュー
  障害対応プロセスビューの目的は，障害に際してもサービス中断と損害を最小にとどめ，その状況のもとで最も適切なやり方で，可能な限りサービス提供を続けることである（**図6**）．

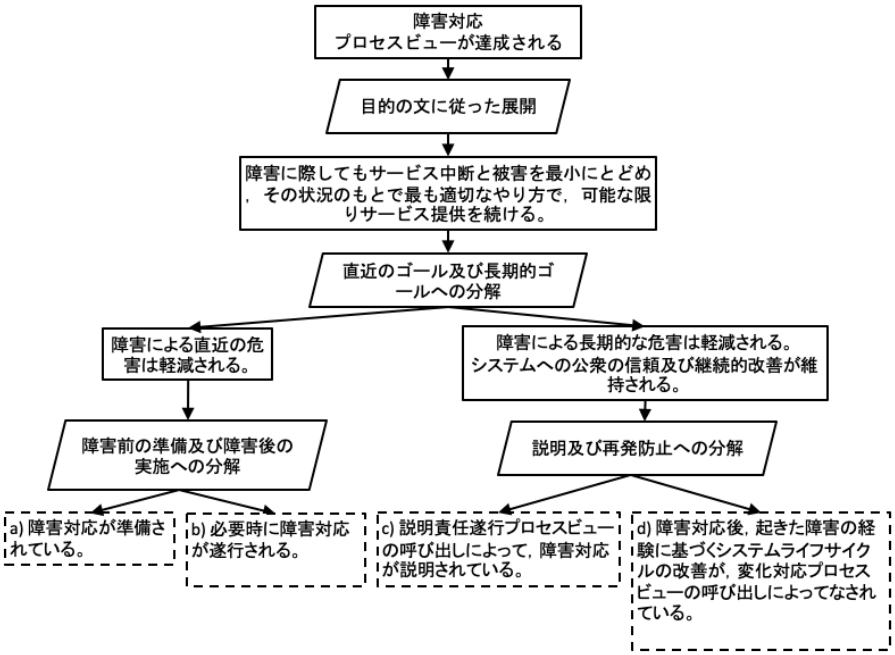

図6　障害対応

- 変化対応プロセスビュー
  変化対応プロセスビューの目的は，要求，環境，目標および目的が変化しても，システムを「目的にかなった（fit-for-purpose）」状態に維持することである（**図7**）．

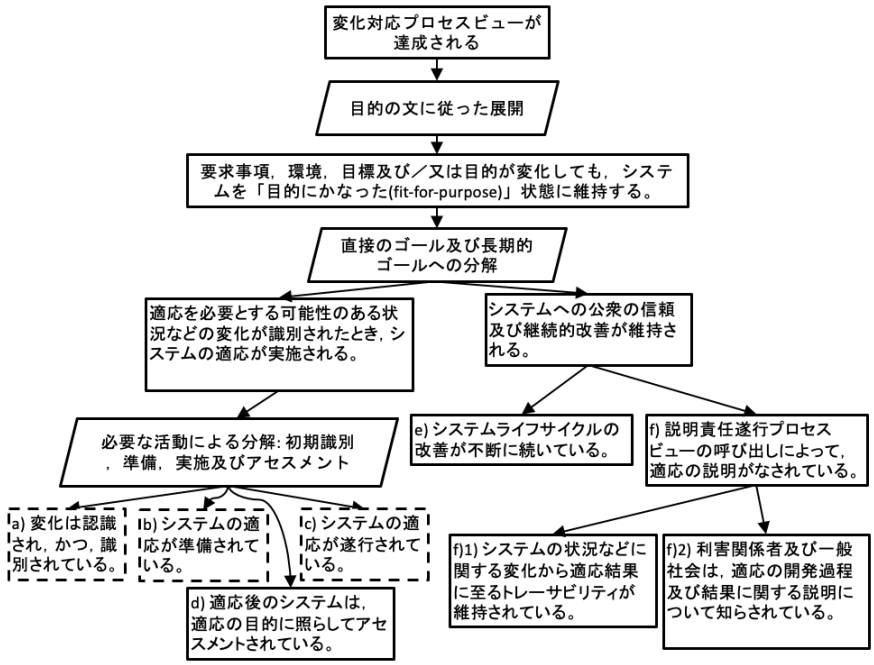

図7　変化対応

4. 国際標準策定までの実際

4.1 標準化の経緯

本節では，JST CRESTのDEOS研究領域に設けられた研究プロジェクト「利用者指向ディペンダビリティの研究」における国際標準化活動を紹介する．

標準が開放系総合信頼性獲得のための1つの重要な要素として位置付けられるため，研究活動の一部として，標準開発を行うこととなった．まず，デジュール標準とするかデファクト標準とするかの選択が必要であった．開放系総合信頼性の場合，この概念自体が研究途上にあること，安全性におけるGuide 51やリスク管理におけるGuide 73のような基本的標準の開発から始めなければならないこと，などから，デジュール標準開発を選択することとした．

「情報システムのディペンダビリティ」は，国際標準活動においては隙間（ニッチ）にある．この国際標準化を行うには，情報システムの国際標準を所掌するISO/IEC JTC 1 Information technology/SC 7 Software and systems engineering/WG 7 Life cycle managementで行うか，あるいはディペンダビリティの国際標準を所掌するIEC TC 56で行うかの2つの選択肢があった．我々はまずは2つの委員会ともに参加することとした．SC 7には合計3名，TC 56には最終的に合計4名（IEC 62853開発プロジェクトTC 56/PT 4.8参加者は3名，それを管轄するTC 56/WG 4への参加者が別に1名）の関係者が参加した（開発最終段階にWG 4への参加者がさらに2名増えて3名となった）．また，本活動がSC 7とTC 56の2つの委員会に関係することから，これらの間のリエゾンオフィサーを派遣し，両委員会での活動の連絡促進に努めた．さらに，2013年からは，著者の1人（木下）がTC 56の小委員会の1つWG 4 Information systemsのコンビナー（主査）を務め，TC 56全体の運営に参加した．

2010年当時は，開放系総合信頼性の概念はまだ研究途上で十分に成熟したものとはいえず，「open systems dependability（開放系総合信頼性）」の言葉さえ確定していなかった．その状況の下で，国際標準における総合信頼性およびアシュランスに関連する標準の体系を調査し，プロジェクトの成果を国際標準として策定する方策を探った．

我々の活動からコンビナーが就任したこともあり，国際標準開発の場の2つの選択肢のうち，TC 56での開発を選択することとして，TC 56国内委員会を通じて2012年夏に開発開始の提案（NWIP, New Work Item Proposal）をTC 56に提出した．投票の結果，2013年初頭にNWIPが承認され，著者の1人（木下）をプロジェクトリーダとして開発プロジェクトチームPT 4.8が発足した．その後，5年強の開発期間に草稿がCD （Committee Draft），CDV, （Committee Draft for Vote）, FDIS （Final Draft International Standard） の段階を通過して，国際標準（IS）が2018年6月13日に発行された．

IECにおける標準のデフォールトの開発期間よりも2年強長くかかってしまい，何度か開発期間延長の手続きを経なければならなかった．開放系総合信頼性の概念を確立させ，熟した草稿ができてからプロジェクトを開始しておれば，（公式の）開発期間を短くし，手続きを簡素化できたと思われる．しかしながら，公式のプロジェクト開始をいつにするかの判断は難しい判断である．TC 56における草稿改善の議論によって開放系総合信頼性の概念がより明確になっていった場合が多々あるけれども，草稿改善の議論は公式の開発期間開始前にはなかなか始められないからである．

IEC TC 56とISO/IEC JTC 1/SC 7/WG 7の両方に参加したことは有意義であった．IEC 62853を発行したのはIEC TC 56である．一方，ISO/IEC JTC 1/SC 7/WG 7への参加は，後述するように，IEC 62853 Open systems dependabilityをIECの他のディペンダビリティ関連標準と関連付け，体系の中に適切に位置付ける上で有効に働いている．

4.2 IEC 62853への懸念とその解決

IEC 62853の開発当初は，少なくとも3つの懸念があった．1つ目の懸念は“open systems dependability”が，TC 56の標準の意味でのdependabilityと乖離してしまうのではないかというものである．これに対しては，IEC 62853開発開始と前後して，当時改訂が進められていたTC 56の基本標準IEC 60300-1 Dependability management – Part 1: Guidance for management and applicationの中に，open systems dependabilityの必要性をすでに埋め込んでおき，IEC 62853はIEC 60300-1のそのパラグラフの詳細化である，という位置付けを行った．これによって懸念は解消したようである．このことは，ディペンダビリティ標準体系全般を見渡した活動がIEC 62853の開発に有効に働いたことを示している．IEC 62853のように，過去に標準化されていなかった新しい基本概念を含む標準を開発する場合には，その分野の標準体系全体に関連する総合的な活動が必要である．IEC 62853の開発プロジェクトにを提案してそれを遂行するだけの狭い範囲の活動では成功しなかったかもしれない．

2つ目はこの標準がISO/IEC/IEEE 15288のライフサイクルプロセスを補う形（プロセスビュー）で記されることへの反対である．ライフサイクルの考えのもとにディペンダビリティを考えることに異論はなかったが，ライフサイクルの具体的なプロセスは，ISO/IEC/IEEE 15288に限らず，いろいろな定義があるから，1つの定義にのみ依存するべきではない，という意見があった．実はそのような反対は，根拠が薄い．ISO/IEC/IEEE 15288はISO/IECの標準体系の中でまさにシステムライフサイクルプロセスを定義するものとして位置付けられているからである．日本からそのような説明を試みたのはもちろんだが，最終的にこの反対がなくなったのは，ISO/IEC/IEEE 15288の上にディペンダビリティ標準を確立する方針が，日本からだけでなく，オーストラリアや英国などの他の有力な国によっても積極的に支持されたこと，またISO/IEC/IEEE 15288の内容の理解が進んだこと，などによると思われる．

3つ目の懸念は，この標準が伝統的な故障解析やリスク解析などのように解析学や統計学に基づく定量的な基準を提供しないことへのものであった．しかし，対象システムのディペンダビリティ属性は定量的な解析法が不明な場合も多く，むしろそのような場合に，定性的であってもできるだけ有効な総合信頼性獲得および保証の手段を提供するのが本標準の目的である．現在でも，このことの納得が十分行き渡っているとはいえないが，これは本質的な論点であり，今後も繰り返し説明を続ける必要がある．

4.3 関連する国際標準への波及

IEC 62853は本年（2018年）6月に発行されたばかりであり，その策定の社会的影響について考察するには時期尚早だが，5年以上にわたって続けられた策定活動は，すでにいくつかの影響，効果を生んでいる．

まずIEC TC 56内部では，開放系への考慮がディペンダビリティ標準開発を，今後目指すべき方向を示すものと捉えられている．TC 56ではこれまでディペンダビリティが対象とする属性（reliability, availability, maintenability, supportability）の整理が議論され，また有力な応用としてasset management systemが取り上げられてきた．しかし開放系が強調する変化と

多様性が，IoT, SoS, ブラックボックスなどの昨今のホットな話題に共通する課題であることの理解が広がるにつれ，今後の計画の大きな柱の1つとして開放系がリスク管理などとともにリストアップされている．

IEC 62853がとった，ISO/IEC/IEEE 15288 System life cycle processesの上にディペンダビリティ標準を開発するアプローチは，現在改訂準備が進められているIEC 60300-1 の次期バージョンに取り入れられつつある．この標準は上述のように，TC 56のディペンダビリティ標準全般の基本と位置付けられており，今後のディペンダビリティ国際標準に大きく影響していくと見られている．

IECの外に目を移すと，車載ソフトウェアにおける自動運転の信頼性のための基準としてIEC 62853に注目する向きが一般社団法人ディペンダビリティ技術推進協会（DEOS協会）自動車応用部会などにあり，今後の動きに注目される．さらに，Lloyd's Register Foundation（LRF）によるInternational research programmeであるAssuring Autonomy（York大学John McDarmidt教授が総括）の研究プロジェクトTIGARS （Towards Identifying Gaps in Autonomy in Road vehicleS, 2018-09～2019-12）でもIEC 62853を基準とすることが考慮されている．

5. 研究と標準化の相互作用について

開放系総合信頼性の標準化は，1.5節に記した理由で実現技術の確立に先行した。これは，研究と標準化の関係の在り方に関して近年顕著になってきた要請の表れの1つである．

古き良き時代には，研究と標準化は専ら科学技術活動の異なるフェーズで行われるものであった．新しい知見が研究され，研究が一段落した段階で実用化がなされ，機能は同一だが性能や信頼性が異なりまた互換性もない製品が乱立し始めて初めて標準化が求められ，標準化活動がなされた．現在でも，物質に関する科学技術では，この考えが有効な場面が多く見られる．しかし，情報に関する科学技術では，この図式が有効でない場合がしばしば見受けられる．情報技術に関する国際標準化会議では，研究途上の課題を解決するための国際標準が議論されることが増えてきた．

たとえば自律システム（AI，深層学習を含むシステムなど）のアシュランスに関して，研究と国際標準化の両方にまたがる活動がいくつか，本稿執筆時において進行している．自律システムおよびアシュランスについて，個別には研究の歴史もあり，技術展開のために標準化すべき事柄もある．しかし，自律システム，とくにAIや深層学習を含むシステムのアシュランスについては，理論の枠組みも明確でなく，研究がこれからようやく始まろうとしている段階であると思われる．機能安全に関するIEC 61508の初版では，深層学習のような発見的手法は安全システムに用いるべきではないとされ，明確に除外されていたほどである．

ところが，ISO/IEC JTC 1/SC 7 Software and systems engineeringではstudy group on autonomous systems and potential areas for standardizationがたてられ，自律システムのintegrity levelの必要性について議論が進んでいる．この活動は，一定の研究成果が出て社会のコンセンサスが得られたことを標準化しようとしている，というよりも，標準化の立場から要請される今後の研究テーマを議論していると見る方がよい．

一方，Lloyd's Register Foundationは昨年，Assuring Autonomy国際研究領域（International Programme）を開始したが，その研究プロジェクト公募では，標準化活動による規制を通じてアシュランスを実現することを明示的に要求している．ISO/IEC JTC 1/SC 7の活動とは逆に，こちらでは研究活動の立場から標準化活動への参加が求められている例と見ることができる．

上記はシステムアシュランスの分野において研究と標準化が相互に作用しあっている例だが，科学研究活動の成果が一般社会に直接影響を及ぼす場合が増えている現代では今後，同様の相互作用が他の分野でも見られることが増えていくと思われる．そこでは，研究と標準化は表裏一体で，相互作用しながら並行して進められるべきという了解が形成されつつあると考えられる．

翻って，CRESTにおけるDEOSプロジェクトを見ると，上記のISO/IECやLRFの活動に10年先行して，2008年の活動初期から標準化プロジェクトを研究領域のプロジェクトの1つとして位置付け，研究と標準化を並行して進められてきた．研究領域総括は当初，「研究者に標準化活動を求めても，同意してくれないかもしれない」と危惧していたが，それに同意するグループが現れて，今日に至っている．その結果，国際標準が刊行されただけでなく，開放系総合信頼性の概念が整理され，かつ，補強された．これは意図された研究と標準化の相乗作用であった．

謝辞　開放系総合信頼性に関する研究を開始した所眞理雄氏と所氏が領域総括を務められたDEOS研究領域（科学技術振興機構CREST制度「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」研究領域）がなければIEC 62853は策定されませんでした．この研究領域の「コアチーム」および研究領域のプロジェクトの1つ「利用者指向ディペンダビリティの研究」によってIEC 62853の原型が作られました．後者の研究プロジェクトをホストしたのは産業技術総合研究所および神奈川大学でした．

DEOS研究プロジェクト終了後に本格化したIECにおける国際標準策定活動を支えたのは情報処理推進機構ソフトウェア工学分野の先導的研究支援事業による研究プロジェクト「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」と（株）シンフォニーとの共同研究であり，これらをホストしたのは神奈川大学でした．

また，DEOS研究プロジェクト終了後，研究成果の普及活動を展開しているディペンダビリティ技術推進協会での産業界と学界にまたがる議論，意見交換はIEC 62853の内容をより現実的になものにしました．

筆者の一部がプロジェクトリーダやプロジェクトメンバ（エキスパート）として策定に携わったIEC TC 56 PT 4.8におけるIEC 62853の草稿検討作業にあたってはValter Roll, Jean Cross, Leigh Appleyardの諸氏は特に有益な意見を寄せられました．

本論文の共同推敲を編集委員として担当された細野繁氏は，単なる推敲の範囲を超えて，本論文をより論理的にし，かつ読みやすくするための積極的な提案を多々寄せられました．

以上，記して深甚の感謝の意を表します．

参考文献

1）IEC 60050-192:2015, 192-01-03.
2）IEC 60050-192:2015, 192-01-22.
3）IEC 60300-1:2014 Ed.3 Dependability Management - Part 1: Guidance for Management and Application, 4.3 (2014).

4）IEC 62853 Ed.1 Open Systems Dependability (2018).
5）IEC 62853 Ed.1 Open Systems Dependability, 3.12 (2018).
6）IEC 62853 Ed.1 Open Systems Dependability, 3.13 (2018).
7）ISO/IEC/IEEE 15288:2015 System Life Cycle Processes, 4.1.23 (2015).
8）ISO/IEC/IEEE 15288:2015 System Life Cycle Processes, 4.1.46 (2015).
9）Tokoro, M. (ed.) : Open Systems Dependability Dependability Engineering for Ever-Changing Systems, Second Edition, CRC Press (2015).
10) 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, IEICE Fundamentals Review, Vol.9, No.4, pp.318–329 (2016).

木下 佳樹（正会員）yoshiki@kanagawa-u.ac.jp
神奈川大学理学部情報科学科教授．神奈川大学プログラミング科学研究所所長．IEC TC 65 Dependability WG 4 Information Systems Convenor. ISO/IEC JTC 1/SC 7/WG 7 Expert.（一社）ディペンダビリティ技術推進協会理事.

武山 誠（非会員）makoto-takeyama@kanagawa-u.ac.jp
神奈川大学プログラミング科学研究所研究員．IEC/TC 56 Dependability/WG 3, WG 4 expert．同国内対応委員会WG 3委員，WG 4幹事．（一社）ディペンダビリティ技術推進協会標準化部会会員.

中川 雅通（非会員）nakagawa.masamichi@jp.panasonic.com
パナソニック株式会社 オートモーティブ＆インダストリアルシステムズ社 技術本部.（一社） ディペンダビリティ技術推進協会理事.

森田 直（非会員）morita@scl.sony.co.jp
株式会社ソニーコンピュータサイエンス研究所．OESプロジェクト　オーブンシステムストラテジスト．IEC TC56 Dependability WG4 Information Systems Expert．IEC SyC LVDC Expert.（一社）ディペンダビリティ技術推進協会標準化部会副主査.

山浦 一郎（非会員）ichiro.yamaura@fujixerox.co.jp
富士ゼロックス（株）．（一社）ディペンダビリティ技術推進協会理事，技術部会主査.

採録決定：2018年10月10日
編集担当：細野 繁（日本電気株式会社）