一般社団法人
ディペンダビリティ技術推進協会

技術部会
標準化部会

はじめてみる IEC62853の実装

～想定外を想定する矛盾から脱却する～

Open Systems Dependability

2018

はじめてみる IEC62853 の実装

～想定外を想定する矛盾から脱却する～

Open Systems Dependability

2018-04-09

DEOS 協会　技術部会・標準化部会

1. はじめに

本資料は、国際標準 IEC 62853 が規定する Open Systems Dependability (OSD)の概念を平易に説明し、その活用に向けた考え方を説明するものです。Dependability(総合信頼性)は、「要求された時にその要求通りに遂行するための能力」です。OSD ではこれに「総合品質」ともいうべき考え方が盛り込まれます。これは、合意の形成、説明責任の全う、障害対応、環境変化への対応をサービス継続に不可欠な四要因と認識し、一体化された運用保守と開発設計の反復でこれらに取り組む考え方(開放系総合信頼性)です。

従来の順次設計開発方式では、上流から下流に一度流した作業成果は完成品として手放せることが目指されました。OSD では、上流から下流に流れた水が海に入り、水蒸気となってまた上流に雨が降るような循環を意識します。例えば、システム仕様設計ではサービス提供者視点だけではなく運用者、利用者視点からの機能も組み込み、運用時にはそれを用いて運利用者からのフィードバックを得て、それを随時改善版の設計開発に繋げる、といった循環を確実にする体制の確立をシステム開発の当初から意識します。

OSD の実現には、常時、その時点でのシステム利害関係者は誰か、如何にシステムと運用開発体制が関係者間合意を満たしているか、等の実態を即座に提示できるツールの提供が重要となります。DEOS 協会が利用拡大を推進している D-ADD や D-Case はその候補となるものです。なお、利害関係者は運用者、利用者その他システムに影響を与える環境や関連機関などで、その捉え方や捉え誤りのリスクへの対処もまた合意の対象です。

急速に発展する現代の情報化社会で広範囲にサービスを提供し続けるには、一度完成したシステムでも利用者の期待、環境、技術の変化に応じて修正され成長し続けなければなりません。想定しなかった相手システムとの相互作用や新たな使われ方を生むネット接続の普遍化などにより、思いもよらない不具合に事後的に対処することも避けられなくなっています。これらは、素朴なウォーターフォール方式だけでは品質保証に限界が来ていることを示します。事前に設定したテスト項目通過をもってシステム完成とするための前提、つまり、将来的変化や不具合に関する開発者の事前の想定は十分である、努力次第で十分にできる、という前提に無理が生じているのです。

OSD は、各関係者がそれぞれの権利と義務を理解してリスクを共有し、より良いサービ

スの継続を維持し続けようとする活動に指針を与えます。新種の活動を求めるというより、サービス継続の四要因が満たされていることを自他に向けて明確化するという新たな視点から、今までの開発方式での活動を見直し改善する枠組みと言えます。IEC 62853 は、活動がもたらすべきアウトカムのリストを各要因について示し、その達成に向けたガイダンスを与えます。今までの活動の原型として ISO/IEC/IEEE 15288 が定めるライフサイクルプロセス達を採り、アウトカム達成向けて各活動を如何に用い、連携させ、必要な関係者間コミュニケーションを促す構造となすか、についてガイダンスが与えられます。

IEC 62853 を実際に利用するには、分野別規格として「実装」すること、「実装規格」とすることが必要と考えます。ここで「実装」とは、IEC 62853 では汎用に一般的な言葉で表現されたアウトカムやガイダンスを、分野に既存のプロセスや成果物の様式（仕様書、設計書、運用マニュアル等）の言葉で解釈し具体化することを通じて、業界での適合性の判定や手順化をよりしやすくした規格を策定することを意味します。

初めて見る人にも背景や経緯などを理解して頂き、本活動に協力していただきたいと思います。

2. 背景

Open System Dependability(OSD)の概念が生まれ、国際標準 IEC 62853 で採られた形で標準化されるにいたった背景について説明します。

2.1. 古典的な開発方式

古典的、基本的な開発方式（図 2.1）は、要求分析やリスク分析が最初にあり、開発、リリースの後は、通常運用が（廃棄まで）続く、という直線的な見方を中心とするものです。

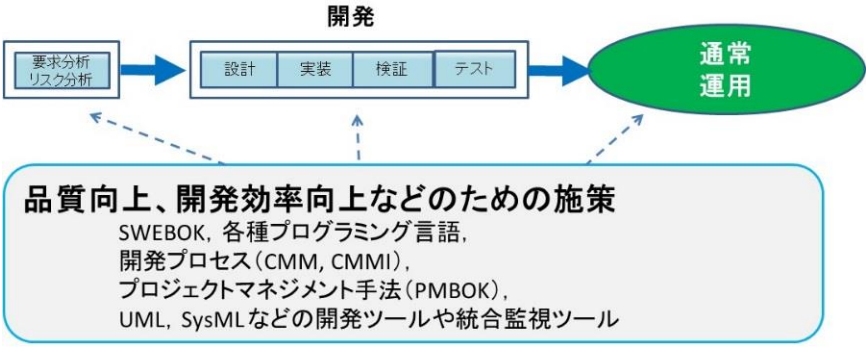


図 2.1 基本的な開発方式

この開発方式に蓄積された過去数十年にわたる世界中からの英知は、各現場で活用され、現在のソフトウェア工学の知識体系（SWBOK）やプロジェクトマネジメントの知識体系(PMBOK)、開発環境やツールなどに活かされています。

2.2. DEOS 二重サイクル

DEOS ライフサイクルモデルは、DEOS 協会が提唱している運用開発の方式です。古典的方式に対する近年の拡充の動向を踏まえ、特に、オープンシステムの課題（次節）の解決に向けて考案された方式です。ここでは、まず DEOS ライフサイクルモデルの原型となった「二重サイクル」について説明します。

古典的な想定とは異なり、現実には一度リリースされたシステムやサービスが、そのままで運用され続けることはありません。ユーザ動向などの要求の変化や、国際標準や技術動向などの環境の変化があるので、それらの変化に対応していく必要があるからです。

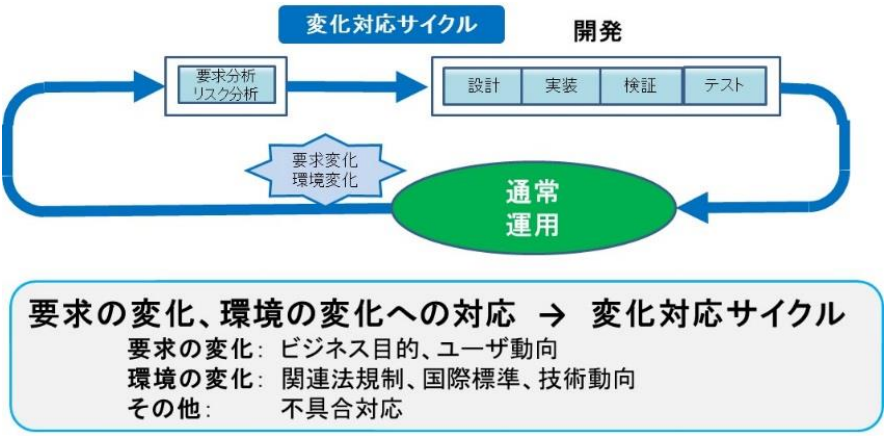


図 2.2 変化対応サイクル

このため、図 2.2 に示すようにバージョンアップを繰り返す「変化対応サイクル」によって変化に対応することを明確に意識しなくてはなりません。

また、通常運用中に障害が発生することは防ぎえず、迅速な対応ができるよう備えておく必要が有る、という認識も一般化してきました。要因には、上記の環境変化やシステムの大規模化、複雑化があります。図 2.2 のサイクルだけでは迅速な対応は望めないので、図 2.3 に示すような障害対応のための「障害対応サイクル」を別に予め準備しておく必要があります。

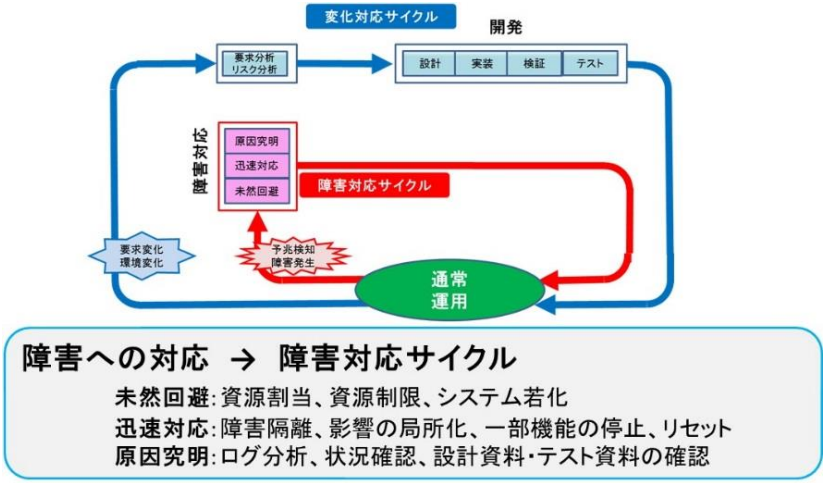


図 2.3 障害対応サイクル

全ての障害を完全に防ぐことはできないという認識は、同種の障害は繰り返さないよう、システムを継続的に改善していくことこそが肝要である、という考えにつながります。図 2.4 はこの考えを方式として明示するものです。障害対応本体の終了が、通常運用の再開だけでなく、再発防止措置をとる変化対応サイクルの開始とリンクされています。

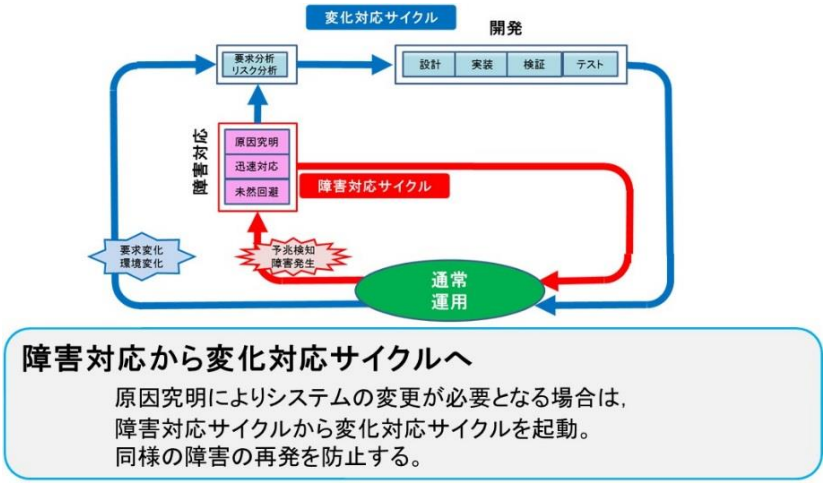


図 2.4 DEOS2重サイクル

2.3. オープンシステムの課題

安全で安心して利用できるような商品やサービスを提供し続けるうえで、システム開発の近年の状況には、古典的方式だけでは解決困難な様々な課題があります。

システムの大規模化により、新規に全てを開発することは稀になりました。例えば、多くのソフトウェアは他社製既存コンポーネントを組み合わせて開発されます。新規開発を基本とする古典的開発方式は現実的でなくなってきています。その結果、以下のような**システムの不完全さ**がでてきます。

- ブラックボックスソフトウェアやレガシーコードに因る仕様と動作の不一致
- 仕様記述やテストの「網羅性」の定義自体の不適切さ
- 各開発フェーズでの理解の不一致などによる各種ミス
- 管理、運用、保守における変更や修正の失敗

また、以下のような**システムを取り巻く環境の不確実さ**も、古典的には重視されてきませんでした（開発前／開発当初に解消できる、開発運用中も大きくは不変にできる、さもなければ廃棄、新規開発をすればよい、といった見方）。

- 事業者の事業目的の変化による要求の変化
- 利用者の要求の変化、システムへの期待値の変化
- 利用動向の変化
- 技術の進歩
- 標準、規格の変更、新たな規制の出現
- オペレータの操作能力や習熟度の変化
- ネットワークを介した、環境との予期外の相互作用
- 外部からの意図的な攻撃

これらの**システムの不完全さ**や**システムを取り巻く環境の不確実さ**は、かなり以前から認識され対策が進められてきています。しかし、近年のシステムは「オープンシステム（開放

系）」としての側面を顕著に示すようになってきており、対応がさらに難しくなっています。

この開放系という意味でのオープンシステムは、システム境界が厳密には定義できない、システムの機能や構造が時間とともに変化する、という性質を持っています。クローズドシステム、つまりそのような性質は無視して差し支えないような古典的システムとの対比を図 2.5 に示します。

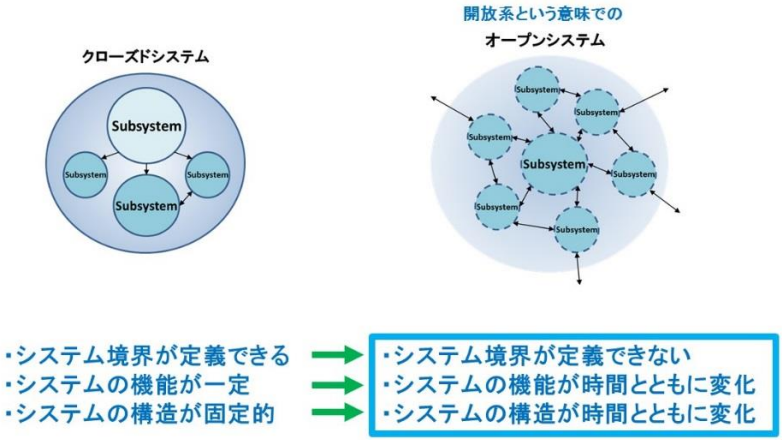


図 2.5 オープンシステムの性質

ここでは、オープンシステムを以下のように定義しています。

✓　「境界、機能と構造が時とともに変化するとともに、認識のされ方や記述のされ方も視点によって異なるようなシステム」

この性質は、要素還元主義ではオープンシステムは捉え難いことを意味します。長年の英知の結晶である各種工学手法の多くは、要素還元主義をベースにしたものです。クローズドシステムには十分有効に適用されてきた工学手法も、そのままではオープンシステムには適用できなくなってきています（図 2.6）。

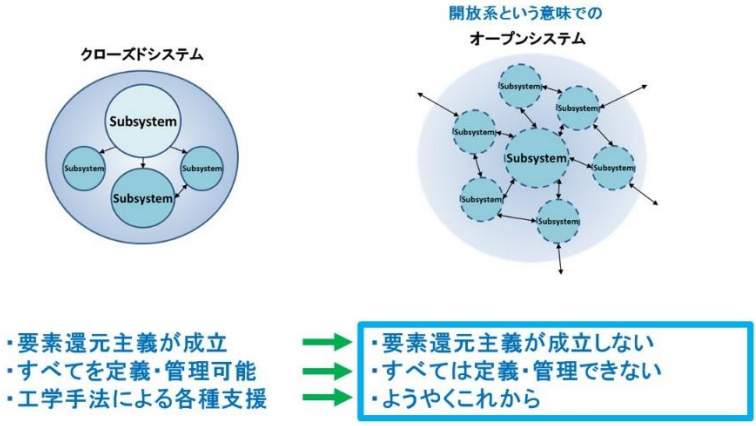


図 2.6 オープンシステムの課題

2.4. 課題の解決に向けて：DEOS ライフサイクルモデル

前節では、システムは以下の状況になってきていることを確認しました。

- 複雑化、大規模化していく。
- 環境とともに変化し続ける。
- オープンシステムとしての性質の程度とその影響がいや増す。

この状況で生じる問題に対して、私たちは日々改善し最大限の努力を継続しています。しかしながら、問題を“ゼロ”にすることは現実的には不可能です。

では、「できることは努力しかない」、「努力していることをもって十分とするしかない」でしょうか。

DEOS では、努力となお残る問題とについて**説明責任**を適切に果たし続けることがもうひとつ必須の要件と考えます。ここ数年で多くの組織も気づき始めていることと思われます。説明責任（accountability）には、問題を起こした場合にはその責任をとれる状態にあること、事前からそれが担保されていることが含まれます。

オープンシステムディペンダビリティ（OSD）の以下の定義はこの考え方を明示するものです。

✓　「期待されるサービスを求められた時に求められたように提供するために、システムの目的、目標、環境及び性能の変化に対応し、不断に説明責任を遂行する能力」

オープンシステムディペンダビリティ

1. システムの目的や環境の変化に（継続的に）対応
2. 利用者が期待するサービスを継続的に提供
3. 説明責任の遂行を継続的に支援

図 2.7 OSD

説明責任を適切、体系的に果たすためには、基準となる合意の**合意形成**にも注目する必要があります。DEOS 協会の提唱する DEOS ライフサイクルモデル（図 2.8）は、この合意形成や説明責任遂行を DEOS 二重サイクル（図 2.4）の中に組み込んだものです。

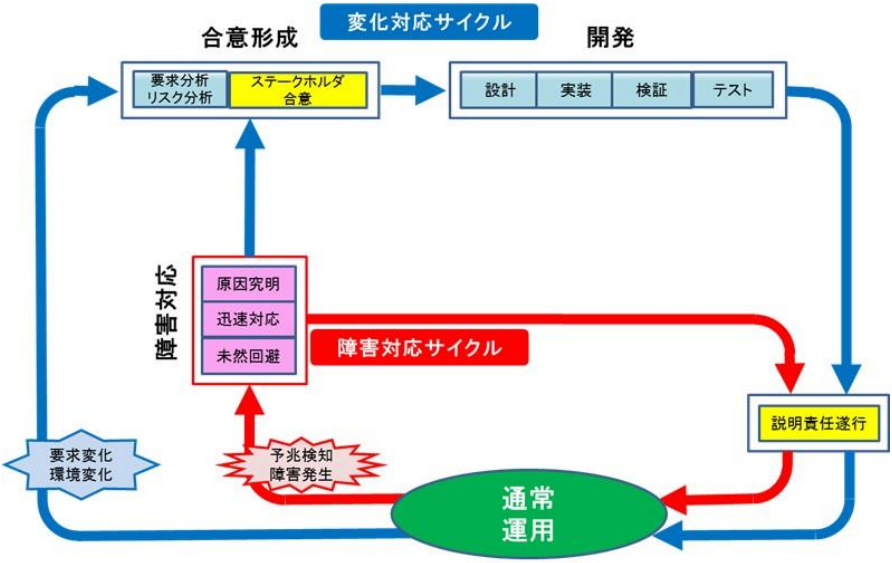


図 2.8 DEOS ライフサイクルモデル

動きの概要は二重サイクルと同様ですが、運用開始前には説明責任遂行の体制が確立されていること、そのための準備が開発初頭からなされ、その後も常に維持されることが特徴です。

開発初頭の合意形成では、開発に直接かかわるシステム要件等に加え、根底にある理念・目的、各利害関係者の負う説明責任、運用中の障害対応の計画等についても合意されます。

合意に基づいた開発後、運用開始前の事前の説明責任遂行には、合意の妥当性、システムの合意適合性、障害対応計画の対外的説明等を通じて、運用開始への一般的納得を得ることが含まれます。

運用中の障害発生時には、障害対応計画の実施に加え、予期外の障害に対して理念・目的に適った臨機応変の対応もとられます。

障害対応後、運用再開前の説明責任遂行では、障害と対応の説明に加え、合意で障害に対して定めていた債務が履行され（始め）ます。また障害対応後には、再発防止をする次版システムに関する合意形成も開始されます。

次版の開発後、その運用前には防止策や体制の改善について改めて一般的納得を得るための説明がなされます。運用中の要求変化や環境変化により開始される対応版次版システムについても同様です。

ここでの、**合意形成**、**説明責任遂行**、**変化対応**および**障害対応**は独立したものではなく、お互いに関連しあっています。責任を果たす必要が生じた時点で、初めて準備を始めるのではなく、合意形成の段階ですでに説明責任への準備が始まっています。

これら**合意形成**、**説明責任遂行**、**変化対応**および**障害対応**のそれぞれで、どのようなアウトカムが達成されるべきかを規定し、達成に向けたガイドラインを与えているのが国際標準 IEC 62853 です。

3. IEC 62853 の目指すもの

IEC 62853 が目指すものは、サービスを提供するシステムが、サービスを要求された時に要求された様に機能することはもとより、運用開始後に要求が変化する時その変化にも対応できる仕組みを持ち、その仕組みが適切に働くことに対する責任の所在も提示されて

いることです。

従来の信頼性関連標準の多くは、要求や環境が静的に固定されていることを前提にシステム開発と運用・保守を別々の対象としてきました。OSD は、運用とその知見からの改善も含め動的変化に対応する運用・開発体制全体に対象範囲と関係者を拡大し、それら関係者の行動規範の枠組みも組み込んだ概念です。そしてまた過去の知見に頼る静的な要求を基にした開発行為から、未来の要求にも対応可能な動的開発を可能とする仕組みをも要求しています。

システムのライフサイクルにおけるステージを分断して緻密化するというよりも、各ステージが密接に連携しフィードバックしあいながら一体として機能しサービスを提供し続ける、継続した活動を構築することがことに求められます。

活動に関するガイドラインは、ステージ別ではなく、合意形成、説明責任遂行、変化対応、障害対応の各目的別に「プロセスビュー」として与えられます。各プロセスビューは、明文化された目的、実施に成功した場合に期待されるアウトカム、アウトカム達成に向けて各種ライフサイクルプロセスを如何に用いるかのガイドから成ります。ライフサイクルプロセスは、すでに国際規格として確立されている ISO/IEC/IEEE 15288 で規定されているものから選ばれています。IEC 62853 は、ISO/IEC/IEEE 15288 の要求事項から OSD の達成に重要な項目を選んで 4 つのプロセスビューとしてまとめ直したものと見ることもできます。そのうえで、必要な項目をシステムに関わる人たちが充当する仕組み、およびその充当された情報群をまとめ上げ説明責任遂行に必要な情報として提示できる仕組みの実現を要求しているといえます。

IEC 62853 の要求の表現では、以下の様な言葉が用いられています。IEC の公式で汎用な定義文言とは別に DEOS における意図を強調した説明は次のようになります。

- オープンシステム
  - 環境変化に対する動的平衡を考慮したシステム
- システムライフサイクル
  - システムが新陳代謝しながら世代を超えて継続し続けるための適応サイクル
- ステークホルダ
  - 発注者、開発者、運用者、保守担当、利用者、等の関連する利害関係者を幅

広く含めた範囲でステークホルダを捉えている

- ディペンダビリティケース
  - 総合信頼性(Dependability*1)要求を実現していることの根拠となる論理的整合性のある説明構造とその証拠とがリンクされた論証書類
- プロセスビュー
  - ディペンデビリティケースに基づいて夫々のステークホルダが関係する、システムに対する機能限界、性能限界、責任分界の提示に必要な要件の集合
- アウトカム
  - 各プロセスビューが要求する活動内容の結果

4. IEC62853 の４つのプロセスビュー

IEC 62853 は OSD を達成するために、四つのプロセスビューを規定しています。各プロセスビューの目的と、実施に成功した場合に期待されるアウトカムに関する規定の抄訳を以下に示します。

4.1. 合意形成

目的　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、及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。

アウトカム

a) システム等に関して、ステークホルダ間で共通の理解と明示的合意が確立されている。
   1) 誰がシステムのステークホルダか明確にされている。
   2) 記述や判断の枠組として、全てのステークホルダに分かる枠組がひとつ確立されている。枠組には、語彙（用語集）やシステムの環境に関する基本的仮定が含まれる。
   3) 枠組みの中で、各ステークホルダはシステムの目的等とそれらの変化について

共通の理解を持つ。これには、システムに関する仮定やステークホルダの責任についての理解が含まれる。

4) 利益相反を解決できるよう、合意が得られない場合の仲裁手続きが事前に合意されている。

5) 明示的合意が a)3)の理解に基づいて作られ、記録されている。記録には、合意形成過程の説明と、合意事項を適切かつ実現可能であるとする理由づけが含まれる。

6) ステークホルダ間での合意文書の解釈の差異は十分に小さい。

7) 以上のアウトカムは、全ステークホルダに対して公正でかつ各々の利害の釣合いに十分留意した方法で達成されている。

b) ステークホルダ間で共通の理解と明示的合意が維持されている。

1) 合意変更管理のポリシーが確立されている。

2) 事業目標、ステークホルダのニーズ、システム、環境などが変化しても明示的合意は維持される。

3) 事業目標、ステークホルダのニーズ、システム、環境などが変化したときには、合意達成のプロセスが見直される。

4) ディペンダビリティケースの構築と承認に関する責任が定められている。

5) 合意達成の事実と合意内容、合意形成過程の説明、合意内容を適切かつ実現可能であるとする理由づけがディペンダビリティケースに記録されている。

4.2. 説明責任

目的　説明責任遂行プロセスビューの目的は、合意事項違反と違反の結果として利害関係者及び社会一般にもたらされる帰結との間の対応関係を確立することである。これには、説明責任者に被害の救済を義務づけ、もって合意履行の公算を増し、システムに関する確信と信用を保ち、潜在的な被害に対して救済措置を確保しておくことが含まれる。

アウトカム

a) システムライフサイクルとそのリスクをコントロールする主要な意思決定事項は何かが

明確にされている。プロセスとプロセスビューのアウトカムを左右する決定事項は、主要意思決定事項に数えられる。

b) 各主要意思決定事項について、説明責任を負う者又は組織が定められている。

c) 各合意事項について、失敗又は違反の原因となりうる主要意思決定事項はどれかが明確にされている。

d) 各合意違反について、説明責任者以外のステークホルダと社会一般に対する影響のアセスメントが行われている。

e) 各合意違反について、説明責任者にもたらされる帰結と、他のステークホルダや社会一般の得る補償とについて合意がなされている。

f) 意思決定での決定から生じた結果は、予期されたものも予期されなかったものも幅広くシステム全体にわたって監視され、アセスされている。これには、合意違反の監視も含まれる。

g) 意思決定者と他のステークホルダに、とられた決定とアクションから生じた結果を知らせるフィードバックループが確立している。

h) 合意違反があった場合、違反の説明責任者は他のステークホルダと社会一般に対して遅滞なく補償を行う。

i) 十分かつ的確な情報が、説明責任者から他のステークホルダと社会一般に対して遅滞なく提供される。

   1) 利害関係者からのシステムに関する正当な情報請求には、速やかに有効かつ十分な返答が与えられる。

   2) システムに関して提供された情報について、利害関係者は根拠のある確信と信頼を持つ。

   3) 故障後には、十分かつ的確な情報が選定され、対象システムの利害関係者、接続先システムの利害関係者、公衆に対し提供される。

   4) システム要求、システムへの期待、システム記述、およびシステム性能の変化に関する情報も同様に選定され、提供される。

   5) システムに関する要求、期待、記述、性能の間の齟齬に関する情報も、見つかり次第同様に選定され、提供される。

4.3. 障害対応

目的　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被害を最小にとどめ、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。

アウトカム

a)　障害対応が準備されている。

1)　サービス継続性確保のために保護されるべき主要機能は何かが明確にされている。

2)　主要機能の保護について、サービス継続のために達せられるべき保護目的が明確にされている。

3)　主要機能に影響する障害要因、エラー、障害及びこれらの前兆が明確にされている。

4)　a)3)の障害等について、影響度と起こりやすさが分析されている。

5)　a)3)の障害等への対応について、サービス継続のために達せられるべき対応目的が定義され、合意されている。

6)　a)3)の各障害等について、以下のいずれの種類の対応をとるかが選択されている。

i)　監視対象とし、特定の対応処理を設計に組み込んで備える。

ii)　監視対象とするが、設計で備えることはしない。

iii)　監視対象とせず、設計で備えることもしない。

7)　主要機能を a)6)i)に属する障害等から保護する特定の対応処理と、a)6)ii)または a)6)iii)に属する障害等から保護するデフォールト対応処理が開発されている。

8)　原因不明の障害からの被害を減らすための総括的な方策が開発されている。

b)　障害発生時には、障害対応が遂行される。

1)　障害等が発生した場合には検知される。

2)　実際起きた障害等について、実態に即した原因分析と影響度分析が行われ

る。

3) 障害等への a)5)の対応目的は、実情に照らして調整される。

4) a)6)i)に属する障害等に対しては特定の対応処理が、a)6)ii)または a)6)iii)に属するものに対してはデフォールト対応処理が、それぞれ実行される。

5) 実際起きた障害等で a)6)ii)または a)6)iii)属するものへの対応処理は、デフォールト対応処理以外に事後的にも考案される。

6) 障害等への対応処理は、被害を悪化させたり、さらなる被害のリスクを増加させたりしない。

7) 対象システムおよび接続された他システムに対する被害が全体として減じられる。

8) 検知された障害への対応処理のアセスメントが、b)3)で調整された目的に照らして行われる。

c) 説明責任遂行プロセスビューの呼び出しによって、障害対応が説明されている。

1) 障害による被害への補償が、合意に基づいてなされている。

2) システムに対する確信と信用が維持されている。

3) 障害対応に関する説明情報がステークホルダ及び一般社会に対して提供されている。この情報には以下が含まれる。

i) a)3)で明確にした障害等全体の範囲が適切であったことの説明

ii) 検知された障害等への対応処理計画が適切であったことの説明

iii) 検知された障害等の影響度分析の結果

iv) 障害への対応処理の結果とそのアセスメント

4) 説明責任遂行プロセスビューに対して必要な情報が提供されている。

d) 障害対応後、起きた障害の経験に基づくシステムライフサイクルの改善が、変化対応プロセスビューの呼び出しによってなされている。

1) 改善の目的が定義され、合意されている。

2) 変化対応プロセスビューに対して必要な情報が提供されている。

4.4. 変化対応

目的　変化対応プロセスビューの目的は、要求、環境、目標及び／又は目的が変化しても、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。

アウトカム

a) 変化は認識され、明確にされている。

1) システムの置かれた状況、前提、リスクなどに関する変化で、システムの適応を必要としうるものが明確にされている。

2) 予期外の故障を含め、予期外の事象を検知したときは、その原因となったシステム及び／又は環境に関する変化が明確にされる。この明確化は障害対応プロセスビューによって引き起こされる場合もある。

3) 破壊的変化は認識され、管理される。

注記　破壊的変化とは、有意義な適応が既存のステークホルダでは不可能または実現困難なものを指す。必要な適応のコストが、現状の合意での説明責任者が事業的に耐えうる限界を超える場合はこれに含まれる。

b) システムの適応が準備されている。

1) システムの「目的にかなった」状態に対する変化の影響のアセスメントがなされ、変化と影響との間の関係が記録されている。

2) 「目的にかなった」状態を維持する適応の目的が定義されている。これには以下が含まれる。

i) 適応の必要性、選択肢とそれぞれの帰結についての情報がステークホルダに与えられている。

ii) 変化した状況の下での合意形成の交渉に必要な支援が、利害関係者に与えられている。

iii) 障害対応プロセスビューによって開始された適応によって、障害の再発が防止されている。

iv) 適応の目的が定義されている。

3) 合意形成プロセスビューの呼び出しによって、適応の目的が合意され、合意文

書の改訂に反映されている。

c) システムの適応が遂行されている。
   1) 適応過程が技術的に支援されている。
   2) 過去の経験による知識が効果的に用いられている。
   3) 目的を実現する適応形質が定義される。
   4) 適応形質が開発される。
   5) 既存サービスの中断と接続先他システムへの悪影響を最小とするように、適応後のサービスが展開される。
d) 適応後のシステムは、適応の目的に照らしてアセスメントされている。
e) システムライフサイクルの改善が不断に続いている。
f) 説明責任遂行プロセスビューの呼び出しによって、適応の説明がなされている。
   1) システムの状況等に関する変化から適応結果に至るトレーサビリティが維持されている。
   2) 適応の過程と結果に関する説明が、ステークホルダ及び社会一般に対して提供されている。

5. ４つのプロセスビュー間の関係

ここまで、IEC62853 で規定されている4つのプロセスビューに関して説明してきました。これらは、独立してあるものではなく、お互いに関連し合っています。これを図 5.1 に示します。

合意形成は他の3つのプロセスビューのベースになっています。説明責任遂行の体制整備により、説明責任者には合意履行への努力が動機づけられ、他のステークホルダと社会一般にはシステムへの確信と信頼への根拠が与えられます。さらに、障害対応後と変化対応後の説明責任遂行は次の合意形成を支援します。障害対応は説明責任遂行のために情報を提供するとともに、再発防止のための変化対応を起動します。変化対応は、現状の合意に環境の変化を反映させる合意形成を再スタートさせて合意を維持し、システムを「目的に適った」状態に保ちます。合意は継続的に形成され維持されるべきものです。

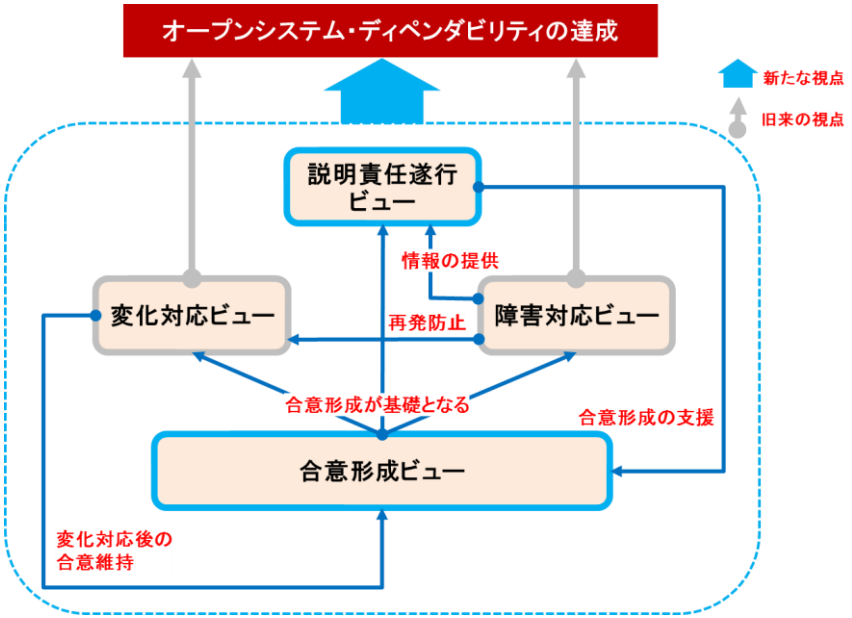


図 5.14つのプロセスビューの関係

5.1. プロセスビューとプロセスの関係

前述のように IEC 62853 のプロセスビューは、ISO/IEC/IEEE 15288 のプロセス、要求を、OSD の視点でまとめ直したものです。したがって、IEC 62853 は、新規にプロセス、活動を追加するものではなく、従来のライフサイクルの各プロセス、活動に対して、OSD の観点での明確化、強化を促すものになります。

表 5.1 に、ISO/IEC/IEEE 15288 の 30 のプロセスと、IEC62853 の 4 つのプロセスビューとの関連を示します。この表からも判るように、4つのプロセスビューは、それぞれシステムライフサイクル全体に広く関係しています。

例えば、IEC62853 の 6.2 の合意形成プロセスビューは、ISO/IEC/IEEE15288 の 6.1 合意プロセスだけに関係するのではありません。6.3.1 プロジェクト計画プロセスや、6.4.3 システム要求分析プロセス、6.4.11 妥当性確認プロセスなど、システムの計画、開発、検証などのライフサイクルのそれぞれの段階毎に、適切に合意形成し、結果を確認することを求めています。

			IEC62853 プロセスビュー			
			6.2 合意形成	6.3 説明責任	6.4 障害対応	6.5 変化対応
ISO/IEC/IEEE 15288 プロセス	6.1 合意プロセス	6.1.1 取得プロセス	✔	✔	✔	✔
		6.1.2 供給プロセス	✔	✔	✔	✔
	6.2 組織的プロジェクト実現プロセス	6.2.1 ライフサイクルモデル管理プロセス	✔	✔	✔	✔
		6.2.2 インフラストラクチャ管理プロセス				✔
		6.2.3 ポートフォリオ管理プロセス		✔	✔	✔
		6.2.4 人的資源管理プロセス			✔	
		6.2.5 品質管理プロセス	✔	✔	✔	✔
		6.2.6 知識マネジメントプロセス	✔	✔		
	6.3 技術マネジメントプロセス	6.3.1 プロジェクト計画プロセス	✔	✔		✔
		6.3.2 プロジェクトアセスメント・制御プロセス	✔	✔	✔	✔
		6.3.3 意思決定管理プロセス	✔	✔		✔
		6.3.4 リスク管理プロセス		✔	✔	✔
		6.3.5 構成管理プロセス		✔		✔
		6.3.6 情報管理プロセス	✔	✔		✔
		6.3.7 測定プロセス		✔		✔
		6.3.8 品質保証プロセス	✔	✔		✔
	6.4 技術プロセス	6.4.1 ビジネス解析、ミッション解析プロセス	✔	✔		✔
		6.4.2 利害関係者要求定義プロセス	✔	✔	✔	✔
		6.4.3 システム要求分析プロセス	✔	✔	✔	✔
		6.4.4 アーキテクチャ設計プロセス	✔	✔	✔	✔
		6.4.5 設計定義プロセス		✔	✔	✔
		6.4.6 システム解析プロセス		✔	✔	✔
		6.4.7 実装プロセス		✔	✔	✔
		6.4.8 統合プロセス		✔	✔	✔
		6.4.9 検証プロセス	✔	✔	✔	✔
		6.4.10 移行プロセス		✔	✔	✔
		6.4.11 妥当性確認プロセス	✔	✔	✔	✔
		6.4.12 運用プロセス		✔	✔	✔
		6.4.13 保守プロセス		✔	✔	✔
		6.4.14 廃棄プロセス		✔	✔	✔

表 5.1

6. IEC62853 はどのように使えるか

- IEC 62853 はガイダンス文書
  - IEC 62853 の要求を如何に解釈して実現したかを明示することで、製品の運用開発体制やサービスがどういう意味で OSD を達成していると言えるのかについて、より明確にコミュニケーションを図ることが可能になります。
  - 一方、独自に解釈する部分が大きいままでは「標準に準拠している」の一言から得られる結論や信認も大きくありません。IEC 62853 は、各業界の実情に合わせて合意される解釈を「実装規格として実装」し、実効的な適合性認証を認証機関から得られるようにする体制づくりの土台として利用できます。
- 業界毎の OSD 実装規格の策定
  - 夫々の事業領域に合わせ、IEC 62853 のガイダンスに沿った実装規格を関連団体で策定することが必要です。これには、既存のライフサイクルでガイダンスの解釈と適用の実践を試み、必要な仕組みを具体的に開発して組み込み、妥当性を検討する作業が含まれます。国を超えた活動が OSD 実装規格の効力を増すことになります。
- 分野別 OSD 実装規格の認証体制の確立
  - 実装規格の効力の確保には、それに基づく評価・認証を行う機関自体の評価、権威付け、つまり、適切な権威による認証機関の「認定」も必要になります。評価、認証の活動に関する既存の汎用ガイドに加えて、IEC 62853 が「認証機関の活動は OSD の目的に適ったものである」と認定するための仕組づくりに活用されます。
- 認定された認証機関による OSD 実装規格への適合性評価認証
  - 企業は、製品の運用開発体制やサービスが実装規格に適合した活動を行なっている証拠を認定された認証機関に提示して評価認証を受けることで、「OSD を達成している」ことについて自らの確信と他者からの信頼、信認を得られるようになります。
- 適合性評価認証は期限付き

- 認証はその時の環境をベースに評価されるため環境変化に合わせた運用ができているか再評価する必要があり、定期的な再認定の仕組みも必須となります。

7. IEC62853 の状況および他の国際標準との関係

IEC 62853 Open systems dependability は IEC TC 56/PT 4.8 によって開発されました。TC 56 Dependability は、dependability（総合信頼性）に関する国際標準を所掌する Technical Committee で、

- WG 1 Dependability terminology
- WG 2 Dependability techniques
- WG 3 Management and Systems
- WG 4 Information systems

の 4 つの Working Groups (WG)から構成されています。WG の他に、新たな標準開発の作業項目が開始されるとそのために Project Team (PT)が設けられ、また、既存標準の改定のために Maintenance Team (MT)が設けられています。

TC 56 による dependability 関連の標準を体系化しようとする試みが行われてきました。技術の進歩によって、既存の体系からはみ出す標準が必要になりますから、体系化の試みは終わることなく続いています。特に大掛かりな体系の見直しが 2017 年から始まっています。それによると、

- IEC 60300 Dependability management – Part 1: Guidance for management and application

によって dependability の概念規定を与え、その仕様や評価を

- IEC 60300 Dependability management – Part 3-4: Application guide – Guide to the specification of dependability requirements

によって規定し、これらの上に立って reliability, availability, maintainability, supportability (RAMS) などの dependability を構成する属性に関する各論を規定する標準群があります。また、

- IEC 61025 Fault Tree Analysis (FTA)
- IEC 60812 Analysis techniques for system reliability - Procedure for failure mode and

effects analysis (FMEA)

- IEC 61882 Hazard and operability studies (HAZOP studies) - Application guide

などの、ツールや方法論に関する標準群をおく、と考えられています。

以上が「古典的な」dependability 管理に関する標準体系ですが、近年に至って、risk management や system life cycle など、システム工学的な dependability の取り扱いが必要となり、

- IEC/ISO 31010 Risk management -- Risk assessment techniques
- IEC 60300-3-3:2017 Dependability management - Part 3-3: Application guide - Life cycle costing

などの標準が策定されています。これらはシステム工学などの新しい技術から 60300-1 を補うものとして位置付けられており、IEC 62853 もそのような標準の一つとされています。

IEC 62853 は IEC 60300-1 を補うものとして位置付けられていますが、それだけではなく、システムライフサイクルの基本標準と位置付けられている

- ISO/IEC/IEEE 15288 Systems and software engineering -- System life cycle processes

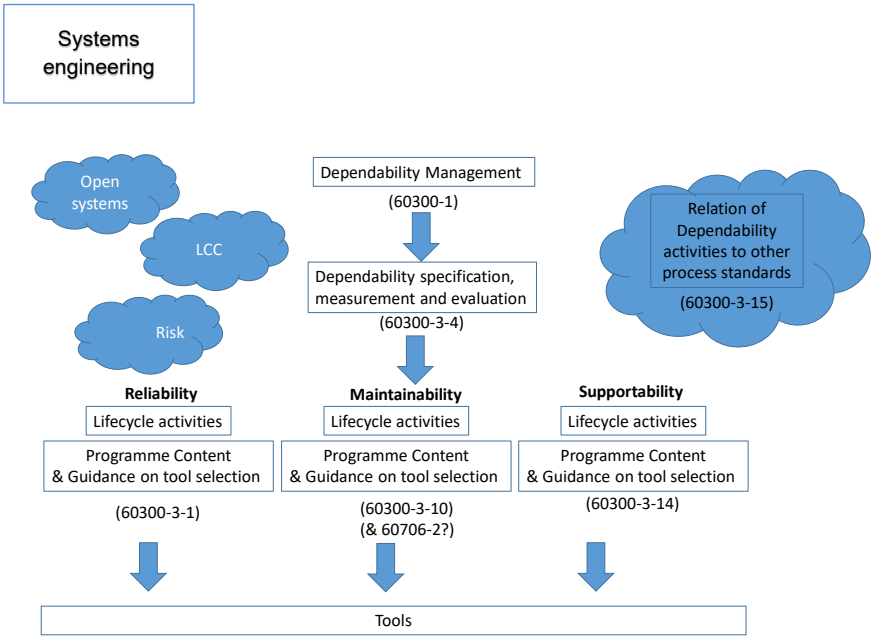
を normative reference とする標準でもあります。また、IEC 62853 への適合性主張のためにはアシュランスケース提出が必要とされるところから、

- ISO/IEC 15026 Systems and software engineering - Systems and software assurance - Part 2: Assurance case

とも密接に関連します。これら二つは ISO/IEC JTC 1 Information technology SC 7 Software and systems engineering が策定、保守している標準です。

IEC 62853 は科学技術振興機構（JST）の研究領域「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」（領域総括：所眞理雄）の研究プロジェクトの一つ「利用者指向ディペンダビリティの研究」（研究代表者：木下佳樹）の研究成果を基にして、IEC TC 56 の我が国の国内委員会が提案し、TC 56 内に設けられた PT 4.8 によって策定されたもので、我が国発祥の日の丸標準といえるものです。2018 年 4 月現在、IEC 62853 は Final Draft International Standard (FDIS) が各国委員会に配布され、承認投票が行われている段階にあります。IEC 規定では、承認投票後のスケジュールが細かく定め

られており、それによると 5 月終わりには FDIS 承認の可否が投票によって決定し、承認された場合には 7 月には国際標準として出版されることになります。



8. おわりに

ここまで IEC 62853 がどの様に生まれ、どの様な問題に取り組みどの様な対応をしてきたかを説明してきました。しかしながら IEC 62853 はあくまでもガイドラインであり、どの様に活用するかは各業界団体の合意によって作成される実装規格が実行力を持つのです。サービス提供者と開発者の視点でなく、運用者やサービス利用者が相互に関係しながら権限の行使と責任の全うに合意し、批判や非難し合うのではなく改善提案をしながらシステムを成長させ快適なサービスが利用できる様にするものです。

結果責任に合意することは難しいことですが、その時点でやるべき事が為されているかどうか適切にそれぞれのレベルで確認できる仕組みを構築する事で OSD(開放系総合信

頼性)が確保できるものと考えます。

IEC 62853 で要求されたガイドラインを独自解釈し、それに沿って仕様書や設計書、評価結果報告書、等々多くの書類を適切に構成して作成し保存しメンテナンスし規格要求に沿って実現したと表現することは可能ですが、分野ごとに認証された実装規格に沿って必要な資料を作成し集約することが重要です。そしてその集約された情報の中から、短い時間で必要な情報を必要なステークホルダに提示できるようにするには IT 技術を活用したツール群が必要となると考えます。その IT ツールのひとつは前述した実装規格に沿うように開発されたデータベースとなるかもしれません。そしてそのデータベースには各ステークホルダが開示できる情報と知的財産として確保したい情報とを分ける機能なども組み込まれるでしょう。

皆さんと共に、このガイドラインに沿う事業領域ごとの OSD 実装規格開発を行い、適切なツールを開発し実際に使い**始めてみる**事が次のステップであると考えます。
是非みなさまも DEOS 協会に参加いただき日本発の国際規格を業界ごとの使える規格として実装し日本から安心出来る商品やサービスを開発・販売・運用しながら国際社会に貢献しようではありませんか。

編著者（敬称略）

森田　直	株式会社 ソニーコンピュータサイエンス研究所
木下佳樹	神奈川大学
武山誠	神奈川大学
中川雅通	パナソニック 株式会社
山浦 一郎	富士ゼロックス 株式会社

The Association of Dependability Engineering for Open Systems

DEOS