IEC 62853と「つながる世界の開発指針」
Open Systems Dependabilityの観点からの考察

DEOS 協会 技術部会／パナソニック 中川 雅通　DEOS 協会 技術部会／富士ゼロックス 山浦 一郎
DEOS 協会 標準化部会／株式会社ソニーコンピュータサイエンス研究所 森田 直
DEOS 協会 標準化部会／神奈川大学 武山 誠　DEOS 協会 標準化部会／神奈川大学 木下 佳樹

変化に対応してサービスを継続できるシステムの指針として、OSD：Open Systems Dependability の考えに基づく国際標準 IEC 62853 が今年発行された。一方、IoT 分野の開発において安全安心の確保のための指針として「つながる世界の開発指針」がある。本稿では、OSD の概要と、「つながる世界の開発指針」を OSD の観点から考察した内容を紹介する。

1 はじめに

現在のシステムは、利用者の期待、環境、技術などの様々な変化に直面している。そのためシステムが長期間サービスを提供し続けるには、運用開始後でも変化に対応し、適応、成長し続けなければならない。変化によく対応できるシステムの提供、継続のために、一般社団法人ディペンダビリティ技術推進協会（DEOS 協会）※1 は「OSD：Open Systems Dependability」※2※3 の考え方を基本とし、その実用化研究、概念の普及、標準化などを推進している。その結果を反映し、対象分野によらない汎用の OSD 要件の国際標準 IEC 62853 Open Systems Dependability ※4 が今年発行された。

一方、IoT 分野、つまり様々なモノがつながって新たな価値を創出していく『つながる世界』では、安全安心の確保が問題となっている。独立行政法人情報処理推進機構 技術本部 ソフトウェア高信頼化センター（IPA/SEC）※5 は、IoT 分野の開発で安全安心に関して最低限考慮すべき事項を「つながる世界の開発指針」※6 としてまとめている。

OSD と「つながる世界の開発指針」は、つながり変化する世界で機能やサービスを継続して提供し続けるという共通の課題に取り組んでいる。本稿では、汎用の OSD の観点から、IoT 分野を対象とした「つながる世界の開発指針」を考察して得られた知見について報告する。詳細は、DEOS 協会の技術資料※7 に記載している。

2 OSDの概要

OSD では、従来別々に扱われていた開発と運用・保守を、変化に対応するための一体の活動として考える※8。運用の知見からの改善の開発なども含むこの活動は、システムライフサイクルの各ステージで独立して行われるものではない。密接に連携しフィードバックし合うステージすべてで継続して行われる、サービスを提供し続けるための活動である。OSD の要件は、合意形成、説明責任遂行、変化対応、障害対応の各目的を達成する 4 つの「プロセスビュー」のそれぞれが、ライフサイクル全体の中で実現されていることである。

2.1 OSD の 4 つのプロセスビュー

以下に OSD の核となる 4 つのプロセスビューの目的について説明する。

■ 合意形成プロセスビュー
- 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。

■ 説明責任遂行プロセスビュー
- 合意事項違反と、違反によってステークホルダと社会一般にもたらされる帰結（説明責任者に課される救済義務を含む）との間の対応関係を確立することで、合意実現の公算を増し、システムに対する確信と信用を保ち、潜在的な被害に対する救済措置を確保する。

■ 障害対応プロセスビュー
- 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。

■ 変化対応プロセスビュー
- 要求事項、環境、目標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。

2.2 4 つのプロセスビュー間の関係

これら 4 つは、独立してあるものではなく、お互いに関連し合っ

※1 一般社団法人　ディペンダビリティ技術推進協会, “DEOS協会,” http://deos.or.jp
※2 M. T. (ed.), Open Systems Dependability: Dependability Engineering for Ever-Changing Systems, Second Edition, CRC Press, 2015.
※3 所眞理雄(編), DEOS, 変化しつづけるシステムのためのディペンダビリティ工学, 近代科学社, 2014.
※4 IEC 62853 : 2018 Open systems dependability.
※5 IPA 独立行政法人 情報処理推進機構　ソフトウェア高信頼化, “IPA/SEC,” https://www.ipa.go.jp/sec/
※6 IPA/SEC, つながる世界の開発指針（第2版）, https://www.ipa.go.jp/sec/publish/tn16-002.html :IPA/SEC, 2017.
※7 DEOS協会技術部会, “IEC 62853と「つながる世界の開発指針」の比較検討,” http://deos.or.jp/link/obj/pdf/DEOS-TR-20180125.pdf
※8 DEOS協会, “はじめてみるIEC62853の実装,” DEOS協会, 2018, http://deos.or.jp/link/obj/pdf/Introduciton62853Implementation-DEOS20180605.pdf

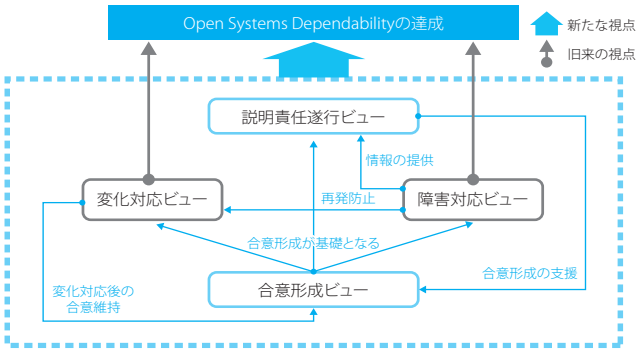

図 1　4 つのプロセスビューの関係

ている（図 1）。

合意形成はほかの 3 つのプロセスビューのベースになる。説明責任遂行はシステムに対する確信と信頼の根拠をステークホルダと社会一般に与え、また障害対応後と変化対応後の次の合意形成を支援する。障害対応は、再発防止のための変化対応を起動する。変化対応は、合意形成を再スタートさせて合意を維持し、システムを「目的にかなった」状態に保つ。合意は継続的に形成され維持されるべきものである。

3 OSDの観点からの「つながる世界の開発指針」の検討

「つながる世界の開発指針」[※6]は、5 つの大項目に分かれた 17 の指針から構成される（表 1）。

それらについて OSD の観点から検討を行った[※7]。そこで得られた知見を指針の大項目ごとに幾つか紹介する。

3.1 方針：つながる世界の安全安心に企業として取り組む

指針 1 にある「経営者が基本方針を策定し、社内に周知すると共に、継続的に実現状況を把握して見直す」は、OSD の説明責任遂行に求められる「意思決定者とほかのステークホルダに意思決定から生じた結果を知らせるフィードバックループの確立」の具体化の一つになる。

3.2 分析：つながる世界のリスクを認識する

指針 4 は「リスクの分析の結果を設計に反映する」ことを求めるが、OSD の説明責任の観点からは「抽出したリスクをステークホルダと共有する」ことも要求している。

3.3 設計：守るべきものを守る設計を考える

指針 12 の「安全安心を実現する設計の検証・評価を行う」は、OSD での「障害対応の遂行」につながる。OSD では「起きた障害の実態に即して設計時の仮定を見直す」、「なされた対応処理を評価する」ために、設計時だけでなく運用時にも検証・評価を行うことも要求している。

3.4 保守：市場に出た後も守る設計を考える

指針 13 の「自身がどのような状態かを把握し、記録する機能を設ける」は、OSD の変化対応での「環境、前提、リスクなどの変化で、システムの適応が必要となり得るものの識別」の実現につながり、同じ観点となっている。

表 1　つながる世界の開発指針一覧

	大項目	指針	
方針	3.1 つながる世界の安全安心に企業として取り組む	指針 1	安全安心の基本方針を策定する
		指針 2	安全安心のための体制・人材を見直す
		指針 3	内部不正やミスに備える
分析	3.2 つながる世界のリスクを認識する	指針 4	守るべきものを特定する
		指針 5	つながることによるリスクを想定する
		指針 6	つながりで波及するリスクを想定する
		指針 7	物理的なリスクを認識する
設計	3.3 守るべきものを守る設計を考える	指針 8	個々でも全体でも守れる設計をする
		指針 9	つながる相手に迷惑をかけない設計をする
		指針 10	安全安心を実現する設計の整合性をとる
		指針 11	不特定の相手とつなげられても安全安心を確保できる設計をする
		指針 12	安全安心を実現する設計の検証・評価を行う
保守	3.4 市場に出た後も守る設計を考える	指針 13	自身がどのような状態かを把握し、記録する機能を設ける
		指針 14	時間が経っても安全安心を維持する機能を設ける
運用	3.5 関係者と一緒に守る	指針 15	出荷後も IoT リスクを把握し、情報発信する
		指針 16	出荷後の関係事業者に守ってもらいたいことを伝える
		指針 17	つながることによるリスクを一般利用者に知ってもらう

3.5 運用：関係者と一緒に守る

指針 15、16 では、リスクや守ってもらいたいことの関係者への周知が重視されている。OSD の合意形成の観点からは、更に、何にどこまで対応するかなどについて関係者との「明示的合意」を双方向のコミュニケーションで確立することも要求している。

また、障害対応に対する、関係者、一般利用者へ、「実施した障害対応が、正しい対応であったか」の説明責任遂行も要求している。更に、合意をなぜ守らないといけないのか、守らないとどうなるかについて、普段から説明をして納得を得ることも要求している。

4 考察

「つながる世界の開発指針」は、IoT システムの開発から運用へのリニアな部分に焦点を置いている。「つながる」ことは、開発時には把握できない変化を運用時に受けるということでもある。よって、障害対応が開発時に完成することはなく、運用を通じた改善が重要となる。OSD では、運用時の予期外の障害を開発時と同様に分析し、分析結果に基づき再発防止に向けシステムを改変することにより、変化に対応することを要求している。IoT システムにもそのような OSD の障害対応、変化対応の要求事項を取り入れることで、サービスの継続性、安全・安心を向上できると考えられる。

一方、関係者（ステークホルダ）について、OSD の現規定では説明責任者か否かしか区別していないが、「つながる世界の開発指針」では、開発者、運用事業者、出荷後の関係事業者、廃棄事業者、直接ユーザ、間接ユーザ、受動的ユーザなどを想定してより具体的に指針を提示している。今後、OSD を特定分野向けに具体化する際の参考となる。

5 今後の展望

様々な分野のシステム、サービスが OSD の便益を享受できるようにするには、IEC 62853 をより具体的な分野別標準に展開し使いやすい形にしなければならない。本報告で紹介した検討は、その IoT 分野向けの一歩であり、今後、更に検討を深めて IoT 分野でのガイドライン策定や標準化に取り組みたい。