【技術報告】

IEC 62853 と「つながる世界の開発指針」の比較検討

2018 年 1 月 25 日

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

山浦 一郎、中川 雅通

1. はじめに

現代のシステムは、利用者の要求や使われ方の変化や外部環境の変化にさらされており、システム構築時に単一のステークホルダが全てを把握することができなくなってきている。

すなわち、現代のシステムは機能、構造、システム境界が時間的に変化しつづけるオープンシステム（開放系・変化系）であり、これに起因する不完全さと不確実さを完全に排除することができず、未来に障害となりうる要因を本質的に抱えている。

それら常に変化しつづける目的や環境に対応し、未知の障害をマネージし、サービスをできうる限り継続し、障害時には社会に対して説明責任を果たすための能力がシステムに求められている。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、この開放系対応力を「OSD：オープンシステムディペンダビリティ（Open Systems Dependability）」と呼び、OSD の研究、開発、実証、評価、標準化などを推進している。その１つとして OSD の国際標準である IEC62853 への取組みがある。

ただ IEC62853 は、広く OSD 達成のための要件を汎用的に定義したものであり、どの領域に適用すべきか、どのような手順、手法、ツールを用いるかなどは決めていない。そのため、実際のシステムの構築、運用に適用するには、その領域に合わせた標準、ガイドラインなどが必要となる。

一方、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) [2]では、IoT（Internet of Things）の進展にともない、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』ならではの機器やシステムに関わる企業が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」 [3]としてとりまとめている。

このように OSD と「つながる世界の開発指針」は、同じ問題意識のもと、異なるアプローチで課題に取り組んでいると言える。OSD はオープンシステムというパラダイムの変革をとらえた概念を構想し、その概念から求められる汎用的な要件を IEC62853 という国際規格にまとめようとしている。

一方、「つながる世界の開発指針」は、主に IoT 機器を開発する企業の経営者、開発者、運用者などに対して、彼らが直面する変革に対して、実際の活動に役に立つ指針をまとめている。

本報告では、IEC62853 の汎用のトップダウンの取組みと、「つながる世界の開発指針」の IoT 分野を想定したボトムアップの取組みを比較検討している。それにより、それら２つ取組みの共通する部分、同じ内容を違う観点でとらえている部分、一方では考慮や説明が不十分な部分などを明確にし、新たな気付きを得ることにより、現在のシステムの安全安心、ディペンダビリティの向上につなげたい。

2. OSD、IEC62853

現在の様々なシステムは、多くのシステムがつながり合い、変化しつづけるものとなってきている。そのため関係者によって見え方が違い、完全に把握することが困難になっている。そのような「境界，機能や構造が時とともに変化し，認識のされ方，記述のされ方が視点によって異なるようなシステム」がオープンシステムである。

オープンシステムでの不完全な情報下で、当初の期待外(Unanticipated)の状況、障害が起こっても、期待されるサービスをできるだけ継続することが必要である。そのようなディペンダビリティのことを、オープンシステムディペンダビリティ（OSD）と呼ぶ。OSD とは「システムの目的，目標，環境及び性能の変更に対応し，不断に説明責任を遂行することによって，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能力」のことである。

OSD について、国際標準案 IEC62853　Open System Dependability の作成プロジェクトが、IEC で進められている。そこでは、OSD の核となる視点として、4 つのプロセスビュー（合意形成、説明責任遂行、障害対応、変化対応）を定め、それにもとづく OSD 達成のための要求事項を提供している。2018 年 1 月現在、IEC62853 は、Final Draft International Standard 発行のための投票の準備段階にある。

以下、IEC62853 で取り組んでいる OSD の 4 つの視点について説明する。

2.1 OSD の核となる４つの視点（View）

■ 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

・ システムに関する合意事項の不履行がステークホルダや一般社会に及ぼす影響を同定し，合意事項の遂行を改善して，システムに関する確信と信用を保ち，潜在的な被害に対する補償を確実にする

■ 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，環境，目標及び目的が変化しても，システムの「目的にかなった(fit - for-purpose)」状態を維持する

3. つながる世界の開発指針

「つながる世界の開発指針」 [3]は、IoT の取組みがすすみ、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』ならではの機器やシステムに関わる企業が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」としてとりまとめた。」ものである。（ [3]　pp.1　はじめに　）

ここでの「安全安心」の定義は、単にセーフティだけでなく、セキュリティ、リライアビリティを含んだ概念であると説明されており（ [3]　pp.3）、OSD でのディペンダビリティの「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能力」の定義に近い、より大きな概念である。

各開発指針は、5 つの大項目と 17 の指針から構成されており、その内容を下記に示す。
（ [3]　pp.33　表 4-1 より）

表 1　つながる世界の開発指針一覧

	大項目	指針	
方針	4.1 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	4.2 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	4.3 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	4.4 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	4.5 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

4. IEC62853 と、つながる世界の開発指針の比較検討

「つながる世界の開発指針」の 5 つの大項目（方針、分析、設計、保守、運用）毎に、IEC62853 の 4 つのビュー（合意形成、変化対応、障害対応、説明責任）の内容と、「つながる世界の開発指針」のプラクティスと比較しながら、OSD の IoT 分野への適応について考察する。

以下に、IEC62853 の観点から、つながる世界のさらなる安全安心の実現に必要と思われることを、各指針毎に記載する。

※「指針＋番号」と記載したものは、「つながる世界の開発指針」の各開発指針を指すものとする。

4.1 方針：つながる世界の安全安心に企業として取り組む

安全安心に取り組むということを、企業経営者がステークホルダである従業員（開発者、保守、運用などの人員）、顧客、エンドユーザに周知することは、IEC62853 の合意形成、説明責任の観点からも重要である。

■ 指針 1「安全安心の基本方針を策定する」

IEC62853 の合意形成の観点からは、

- IEC62853 の合意形成で「共通理解と明示的合意」が求められているので、「周知」に加えて、共通理解および合意のレベルがわかるような記録が必要である。「社内に周知」として社内のステークホルダが示唆されているが、方針策定や分析において社外も含めてステークホルダを同定する必要がある。
- 本指針の「継続的に実現状況を把握し、見直していく」は、OSD の実現にとって重要である。ただし、その中に「共通理解と明示的合意」の維持が含まれている必要がある。また、「見直し」には合意達成プロセスの見直しも含まれるべきである。
- 合意に関する維持・管理の方針が必要。
- 指示・承認者の責任を明確にする必要がある。
- 「基本方針」が社内にて合意されたとする場合にその内容が妥当であり実現可能であることの理由が示される必要がある。

IEC62853 の説明責任の観点からは、

- IEC62853 の説明責任では、「意思決定を行うものと他のステークホルダに意思決定の結果を知らせ、フィードバックループが確立している」ことが求められている。本指針の「 経営者が基本方針を策定し、社内に周知する」だけでなく、逆の社内からのフィードバックを受けることも必要となる。IEC62853 での「説明責任」は、一方的に説明するだけなく、合意をとるための双方向のコミュニケーションを意図している。

■ 指針 2「安全安心のための体制・人材を見直す」

体制、人材の確保・育成などは、IEC62853 の求める共通理解の確立に通じる。明示的合意では書き尽くせない変化、障害への備えを重視する IEC62853 の実現においても考慮すべき項目である。

IEC62853 の合意形成の観点からは、

- 確保・育成される対象者もステークホルダであり、育成自体は「基本方針の周知」のレベルを「共通の理解と合意達成」に導くものである。
- 育成時に評価すれば、IEC62853 の「共通理解および合意のレベルの記録」の実現に通じる。
- 育成を「共通理解および合意」に位置づけるならば、その維持管理のためには、定期的な育成などが必要。
- 体制・環境や育成内容は継続的に見直される必要がある。

IEC62853 の変化対応の観点からは、

- 「変化への適応が準備されている」というアウトカムおよび、「必要な技術的支援が得られる」というアウトカムは、本指針の「体制や環境を整える」および「人材（開発担当者や保守担当者など）を確保・育成する」で与えられると考えられる。
- ただし、対象としている人材が開発担当者や保守担当者などとされているので、より統合的に関係者を考慮して対応を検討する必要がある。

IEC62853 の障害対応の観点からは、

- 障害対応のための体制や環境の整備は重要であり、実適用において考慮すべきである。
- IEC62853 でも強調されるように（IEC62853 6.4.1）、障害対応には、自動的に対応以外に、人による対応も含まれるので、本指針の対応する人材の確保、育成は大事であり、IEC62853 の実現において考慮すべきである。

IEC62853 の説明責任の観点からは、

- 「各主要意思決定事項について、その責任者あるいは責任組織が同定されている」ことが求められるが、同定だけでなく、つながる世界の開発指針にあるように、必要に応じて「体制の整備」、「人材の確保・育成」も、IEC62853 の実現において考慮すべきである。

■ 指針 3「内部不正やミスに備える」

- 本方針の「内部不正やミス」は、IEC62853 では説明責任が問われる事象、障害対応での障害の１つとして考慮される。

また、本「方針」の各指針の実施全般について、説明責任達成、変化対応の観点から留意点を具体化することも有益となる（基本方針の合意形成過程の記録、各指針が合意に基づいて実施されていることの確認と記録、基本方針又は合意変更を要する変化の監視と変更への備え、等）

4.2 分析：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」

IEC62853 の変化対応の観点からは、

- IEC62853 において、「システムの適応が必要となりうるものが同定されている」という要求は、本指針の「守るべき本来機能や情報などを特定する」などで与えられると考えられる。また、IEC62853 においては環境、前提などの変化を認識するとともに、これも加味しての本指針の対応が必要となる。

IEC62853 の障害対応の観点からは、

- 本指針の「守るべき本来機能や情報などを特定する」は、IEC62853 の「障害発生時に保護されるべき主要機能が同定」の実現に通じる。
- 本指針の対策例でのユーザの分類（直接ユーザ、間接ユーザ、受動的ユーザ）は、IEC62853 でステークホルダを具体的に考える上で参考になる。

IEC62853 の説明責任の観点からは、

- 本指針では「リスクの分析の結果を設計に反映する」ということは書かれているが、IEC62853 が要求する「抽出したリスクをステークホルダと共有する」ことも必要である。

■ 指針 5「つながることによるリスクを想定する」

- 本方針の「つながることによるリスク」は、オープンシステムでも、必ず検討されるものである。IEC62853 の実現において、他のリスクと同様に分析、対応することが必要になる。

■ 指針 6「つながりで波及するリスクを想定する」

- 本指針の「つながりで波及するリスクを想定する」は、IEC62853 での障害対応において、「 対象システムへの被害だけでなく、連結された外部のシステムへの被害を想定する」の実現に通じる。

■ 指針 7 「物理的なリスクを認識する」

- 本方針の「物理的なリスク」である盗難、不正読み出し、転売なども、IEC62853 の実現において、他のリスクと同様に分析、対応することが必要である。

本「分析」の各指針の実施全般について、説明責任達成、変化対応の観点から導かれる留意点があることは、4.1 の「方針」と同様である。

4.3 設計：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」

本指針と IEC62853 の要求は相補的であり、併せた実現が望ましい（外部 I/F、内包リスク、物理的接触等、リスク箇所の具体的整理に基づく設計時の対策と、その前提が破れ・変化することに備える運用時も含めた対策の組み合わせ）。システム境界がオープンで変化するオープンシステムの場合での、個々、全体の考え方、インタフェースの定義などについては、検討が必要となる。また、「全体で守る」ためには、個々のシステムの説明責任達成が重要になる。全体で守るためのシステム間の情報伝達とそのための備えは、障害対応に関する説明責任達成の一部となる。

■ 指針 9「つながる相手に迷惑をかけない設計をする」

IEC62853 の説明責任の観点からは、

- 本指針の「異常を検知できる設計」や「検知したときの適切な振る舞いを検討」は、IEC62853 における「システムの適応が必要となりうるものが同定」や「管理」の実現につながる。検討結果や実施状況を、つながる相手に向けて常に説明できる体制も必要になる。

IEC62853 の合意形成の観点からは、

- 本指針は「異常検知時の適切な振る舞いとは」に関する合意形成の際のガイドとなる。一方、「つながる相手」を合意形成に関わるステークホルダとするか否か、無意識に繋がってしまう不特定の相手をどう扱うか、等について整理が必要になる。IEC62853 は特定の整理を定めないが、説明責任達成に耐えうる合意形成過程の記録が求められる。

IEC62853 の障害対応の観点からは、

- IEC62853 では、故障などへの対処を以下の三つに区分して考える。
  - i)　故障等の有無が監視され、故障等が起きた場合の処理が設計に組み込まれるもの
  - ii)　故障等の有無が監視されるが、故障等が起きた場合の処理は設計に組み込まれないもの
  - iii) 故障等の有無が監視されず、故障等が起きた場合の処理も設計に組み込まれないもの

  本指針でも i)、ii) に関しては「異常を検知する設計」、「異常を検知したときに適切な振る舞い」と記載されているが、iii) に対しては言及がない。たしかに監視も対応も設計に組み込まないので対応はできないため不要なようにも考えられるが、IEC62853 では、その場合でも「主要機能保護のためのデフォールト処理が組み込まれている」、「減災のための総括的な方策がなされている」必要があると記載している。これは個々の障害には対応しなくても、汎用の故障への

対策として、いわば基礎体力のようなものとしての設計を要請している。本指針の解説にある「異常からの回復力（レジリエンス）」の概念に近いものと考えられる。このような汎用の障害対策もオープンシステムでは重要であると考える。

・ 「つながる相手に迷惑を掛けない」ことは、IEC62853 が求める「対象システムへの被害だけでなく、連結された外部のシステムへの被害も含めて、全体としての減災がなされている」ことに直結する。

■ 指針 10「安全安心を実現する設計の整合性をとる」

IEC62853 の合意形成の観点からは

・ 本方針の「設計の見える化」は、ステークホルダの「共通理解と明示的合意」を達成する上で必要である。
・ 本方針の「見える化」の提示対象（合意すべきステークホルダ）を明確にして「共通理解と明示的合意」を達成する必要がある。
・ また、設計の承認や責任を明確にする必要がある。

IEC62853 の障害対応の観点からは

・ IEC62853 では「 対象システムへの被害だけでなく、連結された外部のシステムへの被害も含めて、全体としての減災がなされている」と書かれているが、そのステップとして、本指針では、「設計の見える化」、「設計の相互の影響を確認」と具体的に書かれており、参考となる。

■ 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」

・ 設計時に想定できない「不特定の相手」すべてとつなげられても「安全安心を確保」するのは困難である。本指針は、その中でも可能な限り完全な想定と対策をすることで、安全安心を設計時に確保する考え方と言える。IEC62853 では、設計時の対策に加え、運用と開発の反復による漸進的改善の体制があることをもって安全安心の確保とする考え方がとられる。「減災のための総括的な方策」を含め最大限対策を実施したうえでなお失敗する可能性に注目し、その経験に基づいた変化対応によって再発防止を含む改善を施す体制を予め整備しておくことが求められる。

■ 指針 12「安全安心を実現する設計の検証・評価を行う」

・ 本指針の「安全安心を実現する設計の検証・評価」は、IEC62853 における「変化対応の遂行」の実現につながる。
・ 本指針での設計時の評価だけでなく、IEC62853 では、「検知された障害の処理が行われた時に、目的に照らして評価している」とあり、運用時にも検証、評価を行うことも必要となる。

また、方針における合意に基づいて、本「設計」の各指針を実施する必要がある。

4.4 保守：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」

・ 本指針の「自身の状態や他機器との通信状況を把握して記録」は、IEC62853 の変化対応における「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うるものの同定」の実現につながる。

■ 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」

・ 本指針は IEC62853 における将来を見据えた変化対応に備えることにつながる。

本「設計」の各指針の実施全般について、説明責任達成、変化対応の観点から導かれる留意点があることは、4.1 の「方針」と同様である。

4.5 運用：関係者と一緒に守る

IEC62853 は、ステークホルダとして、社内、顧客などの直接の関係者だけでなく、広く関連する人、組織を想定している。本方針で、社内関係者だけではなく、一般利用者（エンドユーザ）、運用事業者、出荷後の関係事業者など社外のステークホルダも意識されているのは、IEC62853 の実現に通じる。

■ 指針 15「出荷後も IoT リスクを把握し、情報発信する」

IEC62853 の合意形成の観点からは

・ 情報を提供し理解・合意を得るべきステークホルダを明確にする必要がある。
・ 「共通理解および合意のレベルの記録」が必要。
・ 「最新情報を常に収集・分析する」という継続的な活動が重要。
・ 「最新情報を常に収集・分析する」の結果の「共通理解および合意」も継続的に進める必要がある。（合意の維持が可能となる）

IEC62853 の変化対応の観点からは

・ 本指針の「①欠陥や脆弱性、事故やインシデントの最新情報を常に収集・分析する」は、IEC62853 における「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うるものの同定」の実現につながる。

・ 本指針の「②必要に応じて社内や関係事業者、情報提供サイトなどへリスクの情報を発信し共有する」は、IEC62853 の変化対応における「i) ステークホルダは、適応の必要、適応の選択枝とそれらの影響などの情報を得ている」および「 ii)ステークホルダは、変化後の状況でも合意形成の交渉に関して必要な支援を得ている」の実現につながる。

IEC62853 の説明責任の観点からは

・ IEC62853 での「システムへの要求、期待、記述、性能などの変化に関する情報の中から適切なものが選ばれて、対象システムのステークホルダ、連結した他のシステムのステークホルダや公衆に対して提供される」の実現につながる。

■ 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」

IEC62853 の合意形成の観点からは

・ ただ単に周知するだけでなく、関係業者が、なにを、どこまで対応するかについての「合意」を得ることが必要。
・ 「共通理解および合意のレベルの記録」が必要。
・ 伝える内容は変化対応などにより常に変化していくので継続的な活動が必要。

これにより合意の維持が可能となる。

IEC62853 の説明責任の観点からは

・ 関係事業者との合意の各事項について、その責任者と守られなかった場合の責任者の責務・非責任者に対する救済等を定めておく必要がある。
・ 障害が生じたときに、関係者、一般利用者への説明責任が重要であると考える。IEC62853 では、障害時には、対象システムのステークホルダのみならず、連結した他のシステムのステークホルダや公衆に対して、適切な情報の提供する必要がある。
・ 本方針の「廃棄」と安全安心の関係についての考え方も、重要な視点であると考える。

IEC62853 の障害対応の観点からは

・ 本指針の「導入、運用、保守、廃棄」に関わる「担当者や外部の事業者」への対策の周知は障害対応にも重要である。IEC62853 では、障害対応を誰が実施するかについて具体的な要求はないが、一般には障害によって破られる合意事項の責任者であり、本指針の実施は必要な合意事項と実施者の具体化につながる。

■ 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」

IEC62853 の合意形成の観点からは

- 一般利用者の「共通理解および合意のレベルの記録」は困難であるが、責任を持つステークホルダ間で、その「伝え方」で十分であるかを合意する必要がある。
- 伝える内容は変化対応などにより常に変化していくので継続的な活動が必要。

IEC62853 の説明責任の観点からは

- 本指針での、一般利用者へのリスク、守ってもらいたいとことを伝えるだけでなく、IEC62853 における「実施した障害対応が、正しい対応であったかの説明」や、なぜ守らないといけないのかという理由（「不履行による影響」）の説明も必要。

また、方針における合意に基づいて、本「運用」の各指針を実施する必要がある。

5. 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、運用時に開発時には把握していない変化を受けることになる。そのため常に変化することを前提とした障害対応は、開発時だけでなく運用時での対応も必要となる。たとえば運用時の障害も開発時と同様に分析し、必要とあればシステムを改変するなど、変化に対応することも必要である。そのような IEC62853 の障害対応、変化対応の要求事項を IoT システムにも取り入れることで、さらにサービスを継続的に提供できるシステムとなると考えられる。

また提供するサービスや機能なども常に進化するので、方針策定、リスク分析、システム開発、システム運用の各段階において、適時、関係者に継続的に説明を行い、合意をとっていく必要がある。IEC62853 での説明責任、合意形成の考え方を IoT システムのライフサイクルに取り入れる必要があると考える。IEC62853 での説明責任は、単に障害時に説明を行うということだけなく、このように通常の開発時にも、関係者の理解を得ることにより開発を手戻りなくスムーズに進められるためにも有用である。

一方、実際のシステムの開発、運用などにおいては、「つながる世界の開発指針」に書かれているように、それを担う体制、人材が重要である。IEC62853 では明示的には書かれていない体制、人材についても、OSD の観点からの検討が必要であると考える。

また IEC62853 では関係者を「ステークホルダ」とのみ記しているが、「つながる世界の開発指針」では、開発者だけでなく、運用事業者、出荷後の関係事業者、廃棄事業者などの想定や、ユーザもユーザを直接ユーザ、間接ユーザ、受動的ユーザに詳細に想定している。これらの具体的なステークホルダのとらえ方は、今後、OSD を IoT 分野などへ適応する場合の参考になると思われる。

6. 今後の展望

今後、OSD が様々な分野のシステム、サービスで活用されるためには、IEC62853 を、各分野毎に適したより具体的な分野規格に展開していく必要がある。OSD の活用が期待される分野として IoT 分野が考えられる。本報告の IoT 分野の「つながる世界の開発指針」への IEC62853 の適用の検討はその一歩であり、今後、さらなる検討を深めて IoT 分野での OSD の分野規格、ガイドラインなどの構築を検討したい。

7. 謝辞

本報告をまとめるにあたり、当初から議論、レビューに参加頂き多大なご助言を頂きました、ディペンダビリティ技術推進協会の武山 誠氏、木下 佳樹氏（標準化部会 主査）、森田 直氏（標準化部会 副主査）、田丸 喜一郎氏（DEOS 協会 理事）をはじめとする関係各位に深く感謝申し上げます。

8. 引用文献

[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,” [オンライン]. Available: http://deos.or.jp.

[2] 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,” [オンライン]. Available: https://www.ipa.go.jp/sec/.

[3] IPA/SEC, つながる世界の開発指針（第 2 版）, https://www.ipa.go.jp/sec/reports/20160324.html: IPA/SEC, 2017.