「頼れるシステム」への挑戦 設計・検証・説明の術を持て

あなたのシステムは「頼れる」存在か。それを検証し、説明できるか。「ディペンダビリティ(Dependability)」の確保とその検証はシステムに関わるプロフェッショナル全員が意識すべきことである。「安全や安心」を旗印に日本の産業が世界に出て行くには、この取り組みを避けては通れない。ディペンダビリティ検証方法の国際標準を作る動きが日本から出てきている。

いきなりだが表を見ていただきたい(**表**)。日経トレンディ12月号の特集「2013年ヒット商品ベスト30」に掲載された「2013年、社会にインパクトを与えた技術ベストテン」である。

日経BP社で技術系媒体を担当している専門記者200人が候補となる技術を挙げ、作家の山根一眞氏と日経ビジネス・日経トレンディ・日経WOMANの3編集長がベストテンを選んだ。候補に挙がった技術群については「テクノインパクトTrend」と銘打ってWebサイトのITproで紹介している。

ベストテンや候補に挙がった技術は「人や社会に優しい」という特徴を持つ。「優しい」は「気をつかう、情がこまやか、控え目、優美」を意味する。ベストテンや候補の多くは、人のそばに控え、細かい点に配慮し、人や社会を気づかう技術である。人とほぼ一体になって人を支援する技術もある。

表◉「テクノインパクトTrend」から選ばれた2013年の技術ベストテン。人や社会に配慮した「優しい」技術が多い

1位	イプシロンロケットの人工知能
2位	低価格「自動ブレーキ」
3位	ゲリラ雷雨予測技術
4位	高層ビル「赤ブリ」の解体技術
5位	身体機能を改善するロボットスーツ
6位	個人向け3Dプリンター
7位	直下地下切り替え工法
8位	無人がれき撤去技術
9位	新ディスプレイ「IGZO」
10位	Hadoop(ハドゥープ)

注)テクノインパクトTrendは日経BP社の技術専門記者200人が話題の技術を選ぶ企画。その中から選ばれたベストテンは日経トレンディ12月号に掲載された。

「優しい技術」は人の近くで使われるから「頼りがいのある技術」でなければならない。「ディペンダビリティ(Dependability)」を備えた技術ということである。ディペンダビリティのある技術やシステムは、安全かつ継続的に利用者が求める価値を提供できる。安全性や信頼性を保証するという意味で「システム・アシュアランス」と呼ぶこともある。

日本発の国際標準が登場

システムにディペンダビリティをもたらし、それを検証する方法を巡って、世界で検討が進められている。例えば、技術標準作りを手がけるオープングループは今年7月、「Dependability through Assuredness Standard(O-DA、安全・高信頼性検証国際標準)」を発表した。

O-DAは科学技術振興機構(JST)の「DEOS(Dependability Engineering for Open Systems)プロジェクト」の成果を取り入れている(69ページの「日本発の国際標準で世界に貢献」を参照)。

なぜ今、ディペンダビリティか

ディペンダビリティは安全性、信頼性、可用性、セキュリティといった特性を包含したものと言える。このため対象となるシステムによってディペンダビリティに含まれる特性は異なってくる。

人命に関わるシステムにおいてディペンダビリティを考えると、これまで通り、安全性を追求することになる。企業情報システムの場合、信頼性、可用性、セキュリティは引き続き重要だが、運用時の誤操作など人が間違うリスクも考慮しておかないと「頼りがいのある」システムにはならない。

ここへ来て諸特性に屋上屋を架すかのようにディペンダビリティが持ち出された理由は、従来より視野を広げて技術やシステムの「頼りがい」を検討しなければならなくなってきたからである(**図1**)。

車載端末や人に装着する端末をクラウドコンピューティングで結び、新サービスを提供するとしたら、端末とクラウド(サーバー)、ネットワークを含むシステムをディペンダブルにする必要がある。

図1◉ディペンダビリティ(Dependability)が重要視される理由

これまでディペンダビリティは産業機器と組み込みソフトウエアを主な対象として議論されてきたが、ネットワークやサーバーを含むエンタープライズシステムにおいても重要になってきたわけだ。

東日本大震災をきっかけに、安全性や信頼性に対する人々の意識はこれまで以上に高まっている。日本の産業界が世界で活躍していくためにも、ディペンダビリティ向上への取り組みが欠かせない。コスト競争を避け、日本生まれの製品やサービスの付加価値として「安全安心」を訴求しようとするなら、製品やサービスのディペンダビリティを高めなければならない。

そのためには製品あるいはシステムの全体像をしっかりとらえ、故障や事故の原因になる要素を設計・開発・利用の各段階で排除していくとともに、一連の対策を検証できるようにしておく必要がある。つまり「安全安心に力を入れています」と言ったとき、どう力を入れているのか、説明を求められるようになる。

システム安全の考えを活かす

ディペンダビリティを追求するには「視野を広げて技術やシステムの『頼りがい』を検討」する必要があると述べたが、その際に「システム安全(System Safety)」の考え方と手法が参考になる。航空、宇宙、軍事、原子力といった分野のクリティカルなシステムの安全性を追求するシステム安全は次の原理に基づいており、それら

は情報システムにも有用である。

- 概念開発と要件定義といった初期段階から安全を考慮する。
- システム全体を扱い、人間、機械、環境といった構成要素間の相互作用に着目する。
- 分析と定性的手法を重視する。
- 設計におけるトレードオフと対立を重視する。
- エンジニアリングにとどまらず、管理者・設計者・操作者の態度、政治や世論などにも関心を持つ。

以上の原理はシステム安全の教科書として知られる「セーフウェア　安全・安心なシステムとソフトウェアを目指して」(**写真**)から抜粋した。これらは情報システムの世界においても以前から重要だと指摘されているものの、なかなか実践できない。つまりディペンダビリティへの近道はない。

ちなみに「セーフウェア」の著者ナンシー・レブソン氏は「(ディペンダビリティのように)複数の特性を一つの抽象概念にまとめようとする試みは見当違い」と指摘している。ディペンダビリティの指標を作り、それだけを使って管理しても意味がない。前述した通り、「システムによってディペンダビリティに含まれる特性は異なる」から、それらを明確にし、優先順位を付けて対策に取り組む必要がある。

写真◉システム安全の教科書として知られる「セーフウェア」(ナンシー・G・レブソン著、松原友夫監訳・訳)

大きなシステムとして把握

システム安全の考え方を参考にして、ディペンダビリティ向上のために取り組むべきことをまとめると次の4点になる(**図2**)。

第1に、対象を広義のシステムとしてとらえる。第2に、リスクを洗い出し、設計段階から除去していく。システム安全の場合、ハザード(事故をもたらし得るシステムの状態)に注目する。第3に、利用段階でリスクやハザードを監視する。記録(エビデンス)を残し、取り組みについて説明できるようにする。

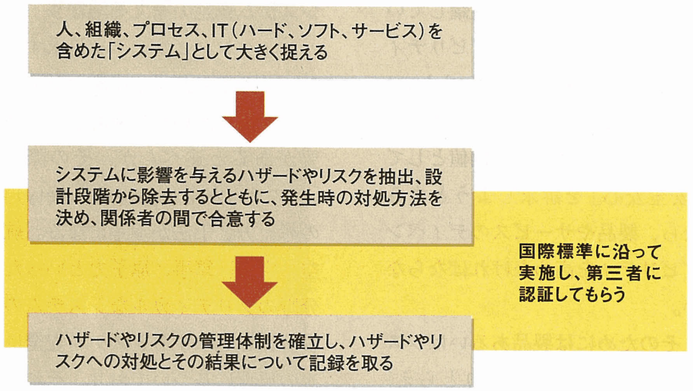
第4に、以上の取り組みを国際標準に沿って進め、しかるべき取り組みかどうか第三者に認証してもらうことが望ましい。

国際標準や第三者認証についてはISO(国際標準化機構)やIEC(国際電気標準会議)が定めた品質や安全に関する規格が製品や技術分野ごとにある。例えば、開発プロセスの改善や、安全装置を使う安全性(機能安全と呼ぶ)を対象にしたものがある。

7月にオープングループが発表した「安全・高信頼性検証国際標準(O-DA)」は分野を限定せず、あらゆるシステムを対象にしており、エンタープライズ・アーキテクチャ(EA)とD-Caseという手法を推奨、設計・検証・説明ができるようにしている。

O-DAは日本のDEOSプロジェクトが提案しているやり方を取り入れた。それは、反復的プロセスによる漸近的な解決を目指すというものである。システムを取り巻く環境や要件は変化し続けるから、ディペンダビリティを維持するには、システム自身を継続的に進化させる必要がある。

図2◉ディペンダビリティ向上のために取り組むべきこと



日本発の国際標準で世界に貢献

オープングループ日本代表
グローバル情報社会研究所社長
藤枝 純教

オープンな技術の標準作りや認証を手がける非営利団体、オープングループ(The Open Group)は7月15日、「Dependability through Assuredness Standard(O-DA、安全・高信頼性検証国際標準)」を発表した。

O-DAは製品やサービス、情報システムなどの安全・高信頼性(Dependability)を保証(Assure)するために、開発者や提供者が実施すべき活動のフレームワークを定めたものである(**図A**)。

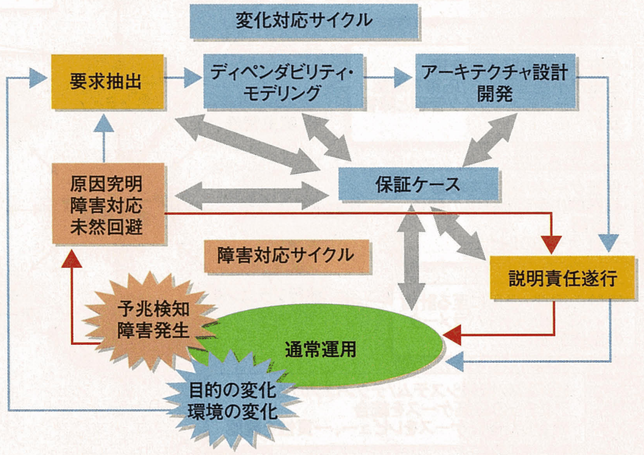
このフレームワークは、科学技術振興機構(JST)がかねてより進めてきた「DEOS(Dependability Engineering for Open Systems)プロジェクト(研究総括はソニーコンピュータサイエンス研究所の所眞理雄エグゼクティブアドバイザー/ファウンダー)」の研究成果に基づいており、O-DAは「日本発」の国際標準になっている。

O-DAは航空機・原子力発電・自動車・鉄道の管制・食品・ヘルスケア・スマート系など人の安全に関わるシステムはもちろん、通信・銀行など一般企業の持続性を担保するシステムの高信頼性管理にも適用できる。

ここでいうシステムは、製品や技術(ハードウエア、ソフトウエア)と、それを操作あるいは利用する人や組織まで含む。人命に関わる深刻な事故やトラブルの原因を調べると、人の操作ミスや勘違いであることが多い。

システムの安全・高信頼性を保つためには、人の操作まで含めたリスクを抽出し、設計・開発段階できるようにしている。

図A◉オープングループが発表した「安全・高信頼性検証国際標準(Dependability through Assuredness Standard)」のフレームワーク



出所：Open Group Standard Dependability through Assuredness(O-DA)Framework。用語を和訳するにあたり科学技術振興機構(JST)のDEOSプロジェクトの用語を参考にした。

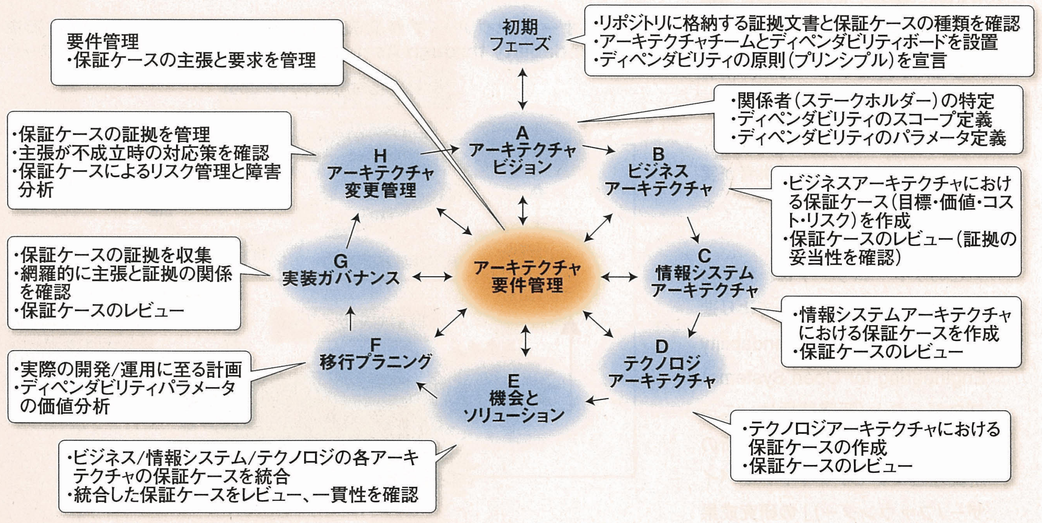
からリスクを排除していく必要がある。システムを動かしてから、目的や置かれた環境が変わったら見直さなければならない（図Aの変化対応サイクル）。

さらにシステムの運用時にリスクが顕在化した場合の対策を用意しておく（図Aの障害対応サイクル）。事前にあらゆるリスクを想定できないから、想定外の障害が起きた際には被害を最小限に抑える対策を講じつつ、システムを再設計するサイクルを回す。

これらのサイクルが確かに機能していることを保証するために次の2点が必要になる。第1に、システムに関わる関係者（ステークホルダー）が議論して決めた対策とその根拠を「保証ケース」と呼ぶ文書に残す。こうすることでステークホルダーたちはシステムに対し、責任（Accountability）をとれる。

第2に、設計や保証ケースの記述をオープンな標準にそって実施する。第三者に安全性・高信頼性を検証してもらえるし、設計から運用に至るプロセスに盛り込んだ知恵を他の組織やプロジェクトで再活用する道が開ける。

図B◉エンタープライズ・アーキテクチャの中でディペンダビリティを検討する方法



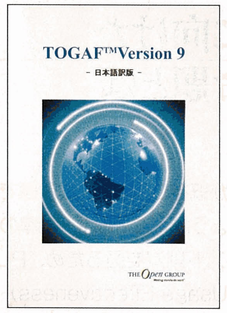
出所：Open Group Standard Dependability through Assuredness（O-DA）Framework。日本語の説明文は『TOGAF Version9（日本語訳版）』、オープングループ日本代表の藤枝純教ならびに名古屋大学情報連携統括本部の山本修一郎教授の説明資料に基づく。

O-DAはフレームワークを示したものであり、手法までは規定しないが、オープングループが提供しているエンタープライズ・アーキテクチャ（EA）作成標準TOGAF（**写真**）と、DEOSプロジェクトが開発した手法D-Caseを推奨している（図Bと図C）。

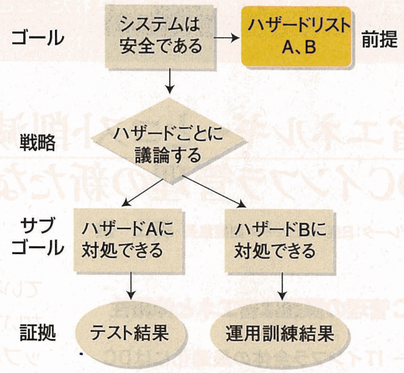
TOGAFは何らかの目的を持ったシステムのアーキテクチャ（設計情報）を記述するためのものであり、情報システムだけが対象ではない。図Bに示した、AからHに至るプロセスを通じて、ビジネスアーキテクチャ（システムの目標・価値・コストなど）、情報システムアーキテクチャ（データとアプリケーション）などを作成し、それぞれについて安全・高信頼性の保証ケースを作成していく。

保証ケースを書くにあたって、DEOSプロジェクトは、英国で開発されたGSN（Goal Structuring Notation）を拡張した表記法を用いる。図Cで示したように、ゴール、そのための戦略、証拠の関係を図で記述していくものである。「ハザード」とは安全を脅かしうる状態や条件を指す。

写真◉オープングループのエンタープライズ・アーキテクチャ作成標準「TOGAF Version9（日本語訳版）」



図C◉保証ケース記述の一例



出所：電気通信大学情報システム学研究科の松野裕助教によるD-Case説明資料

7月に発表されたO-DAは第1版であり、今後2年をかけて、保証ケースを格納するリポジトリ、リアルタイムシステムのためのプロセス、複数システムにおけるディペンダビリティの定義、などを盛り込んでいく。

それと並行して、安全と高信頼性が求められるシステムに関わる企業や団体が、TOGAFのプロセスの上に立ったO-DA1.0を使って安全・高信頼性を検証する取り組みを進め、実践結果を世界に発信いただくことが不可欠である。「日本の安全・高信頼性」というブランドの価値を高めていくには、オープンな世界標準に沿った取り組みとその発信が必須になる。

12月にはDEOSプロジェクトの成果物の普及と標準化推進を目的とする『ディペンダビリティ技術推進協会』が設立される予定である。オープングループは同協会と連携しつつ、O-DAの普及を進めていきたい。

ディペンダビリティに取り組むには、対象を大きなシステムとして捉え、リスクをはっきり示して対策を立て、国際標準を意識する必要がある。3点とも日本勢は苦手としてきたが、日本発のO-DAが登場したことをきっかけにして、様々な製品やサービス、システムのディペンダビリティを高める取り組みを進めたいところだ。

ただし、自動車、航空、鉄道、化学プラント、原子力発電などにおいては安全の国際規格があり、これらに関わる企業は対処に追われている。この実態を踏まえると、まずはスマートシティのような新しいシステム領域から、ディペンダビリティの向上と検証に取り組むことになるのではないか。

第一歩は情報システムに関わる技術者がディペンダビリティを意識することだ。「セーフウェア」の著者レブソン氏は次のように苦言を呈している。「ソフト技術者はめったにコンピュータの向こう側のことを思い描こうとしない。通常、彼らは安全に対する影響をほとんど考慮に入れずにソフトを作る」。

（谷島 宣之＝日経BPイノベーションICT研究所）