

つながる世界に向けた取り組み

SEC ソフトウェアグループリーダー

SEC 研究員

中尾 昌善

宮原 真次

1 はじめに

今日、ソフトウェアが組み込まれた製品・システムは日常生活に無くてはならない社会基盤となってきた。更に、そのような製品・システム同士がネットワークを介してつながって、新しいサービスを生み出す世の中へと変遷しつつある。これをIPA/SECは「つながる世界」と呼んでいる。「つながる世界」は、次に示す2つの軸（図1の横軸と縦軸）から形成される。

(1) あらゆる製品・システムが、業界や企業を越えてつながり、新しいサービスや価値を創造する。例えば、スマートフォン（以後、スマホ）による自動車制御、家庭内の機器をつなげるスマートハウス、スマート家電などが考えられる（図1の横軸）。

(2) 利用される製品・システムから得られる各種データをビックデータとして収集・分析し、その結果を製品・システムの開発や制御にフィードバックする。例えば、電車の車両にセンサを装着し、電車の運行中に線路の保全データを収集し、劣化の予兆解析することで、線路の保全をタイムリーに実施するなどが考えられる（図1の縦軸）。

前者はIoT（Internet of Things）と呼ばれることもあるが、ここではインターネットに接続する場合だけでなく、あらゆる通信手段を用いてつながること、及びモノだけでなく、あらゆる製品やシステムをつながる対象としている点で、一般に用いられるIoTという用語を更に拡大して捉えている。

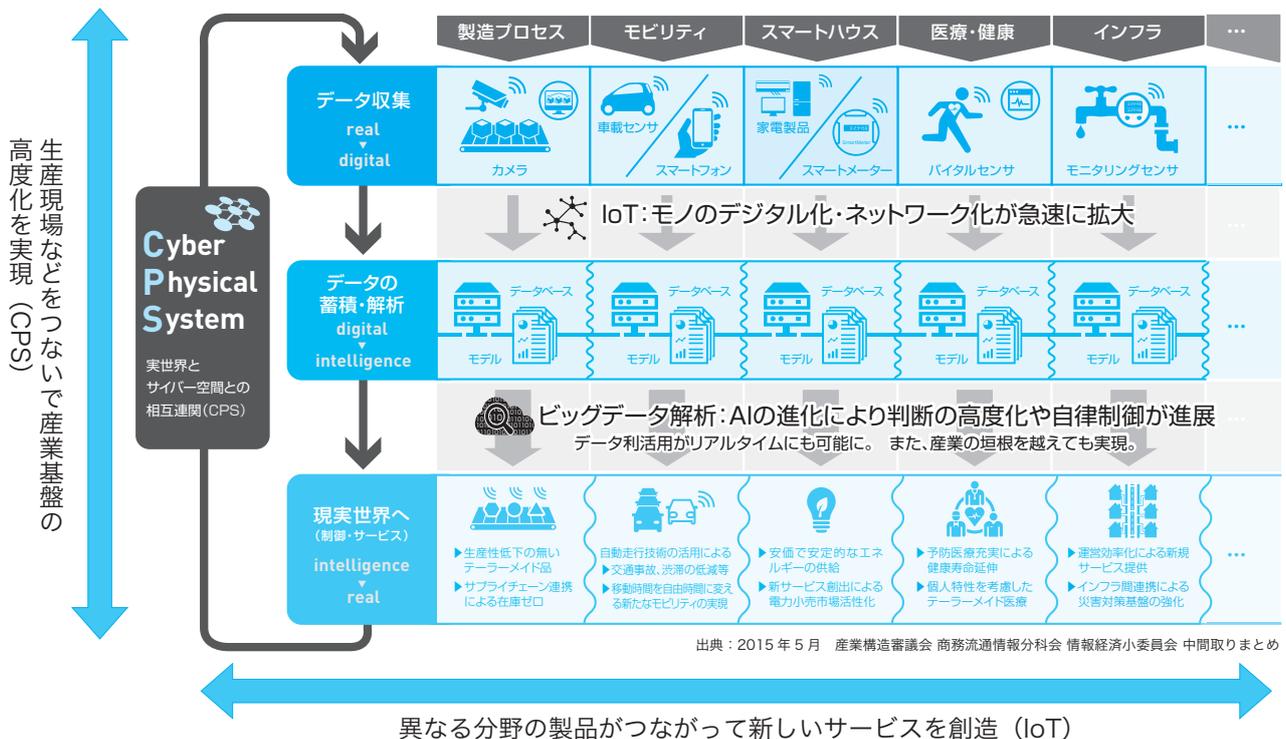


図1 つながる世界

後者は、実製品や実システムから得られるデータをもとに、その制御を行うという意味で、CPS (Cyber Physical System) またはデータ駆動型社会と呼ばれることもある。

このつながる世界では、色々な製品・システムがつながって新しい製品・サービスが生み出され、我々の生活の益々の利便性向上や新しいビジネスの創出に寄与するものと期待されている。一方で、色々な品質の製品・システムが氾濫し、それが勝手につながってしまうと、安全上あるいはセキュリティ上の問題を引き起こす危険がある。そこで、IPA/SEC は本格的なつながる世界の到来に備えて、つながる世界に潜むリスクを防止する取り組みが必要と考えている。

2 つながる世界の特徴

つながる世界の特徴は、以下の点にあると考えられる。

- (1) 異なる分野の製品やシステムがつながる。
- (2) モノとモノが自律連携動作し、互いに影響を及ぼす可能性がある。
- (3) 制御などに利用するデータの信用が重要となる。
- (4) 試験対象が膨大化する。

これらの特徴に応じて、次のような仕組み作りの必要性が浮き彫りになると想定される (図2)。

- ① 分野間を安全・安心につなげる仕組み
- ② モノの自律連携における安全・安心を担保する仕組み (例：暴走防止など)
- ③ データの信用性を確認する仕組み

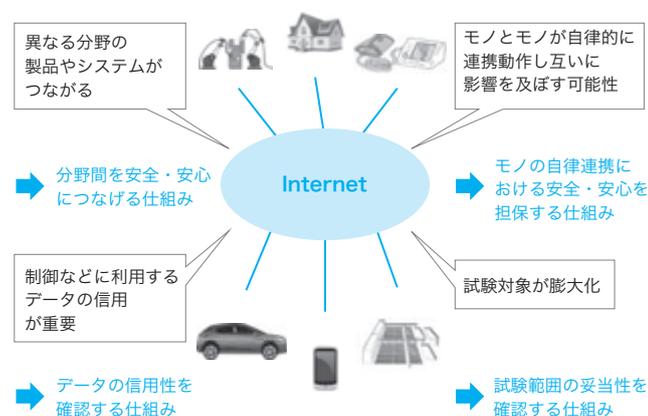


図2 つながる世界の特徴と必要となる仕組み

④ 試験範囲の妥当性を確認する仕組み

このうち、IPA/SEC では、2015 年度は①と②を中心に検討を行っている。③と④についても、2016 年度以降に順に検討していく予定である。

3 分野間を安全・安心につなげる仕組み

3.1 概論

分野間をつなげるプラットフォームの規格は、米国及び欧州を中心に議論されている。一方、国内では、分野内の規格としてホームネットワーク関連の ECONET-LITE や産業ロボット分野の ORiN などが存在し、分野間にも適用拡充する活動は緒についたばかりである。このプラットフォーム議論は既存の検討に委ねることとし、IPA/SEC は高信頼性の観点から寄与していくことを考えている。具体的には、つながる世界の品質の考え方やコンシューマデバイスの開発方法論などに関する取り組みを行っている。

3.2 つながる世界のソフトウェア品質ガイド

異なる業界や企業の製品をつなぎようとする時、品質に関する共通的な捉え方が必要である。今までその製品が属する分野でのみ通用していた品質の概念を持ち出しても、異なる分野の理解を得られるのは難しい。

そこで、IPA/SEC では、まずは品質理解の共通化を図ることが重要であると考えている。分野横断的な理解を得るには、品質定義に関する国際標準に従うことが妥当であり、その規格として存在する SQuaRE の採用を推進していこうとしている。SQuaRE の特徴は、品質はバグ含有量だけを指すものではなく、性能効率性や使用性などの幅広い観点での捉え方になっていることにある。この SQuaRE は、まだ必ずしも浸透しているわけではないので、その理解の手助けとするために、「つながる世界のソフトウェア品質ガイド」を作成した (図3)。



この SQuaRE は、まだ必ずしも浸透しているわけではないので、その理解の手助けとするために、「つながる世界のソフトウェア品質ガイド」を作成した (図3)。

◀ 図3 つながる世界のソフトウェア品質ガイド

この「つながる世界のソフトウェア品質ガイド」は、ソフトウェア品質ガイド編とSQuaRE品質モデル活用リファレンス編の2部構成である。前者は、製品・サービスを提供する事業者が理解しておくべき品質に関する基本的な知識を分野事例を交えて紹介しており、後者は、国際規格SQuaREの活用方法についてわかりやすく解説している。

3.3 コンシューマデバイスの開発方法論の標準化

コンシューマデバイスとは、自動車、家庭用のサービスロボット、スマートハウス（スマート家電）など、一般の利用者が使用する機器のことである。IPA/SECは、このコンシューマデバイスの開発方法論の国際標準案を、国立研究開発法人産業技術総合研究所、トヨタ自動車株式会社、富士通株式会社、電気通信大学との共同で、OMG（Object Management Group：オブジェクト指向の標準化推進のための国際的な業界団体）に提案してきた。その結果、2015年3月にOMGの国際標準規格として成立した。今回の標準規格の特徴は、次の通りである。

- ① 対象がコンシューマデバイス全般であること
- ② ディペンダビリティ向上のための仕組みに関する規格であること
- ③ 日本流のすり合わせ開発の方法論を汎用的な開発方法論として提案していること

今後のつながる世界では、コンシューマデバイス間の連携は欠かせぬものになると想定され、その開発方法に関して我が国からの規格提案が認められたことの意義は大きく、本規格が各産業界で適用され、日本の国際競争力向上につながる事を期待する（図4）。

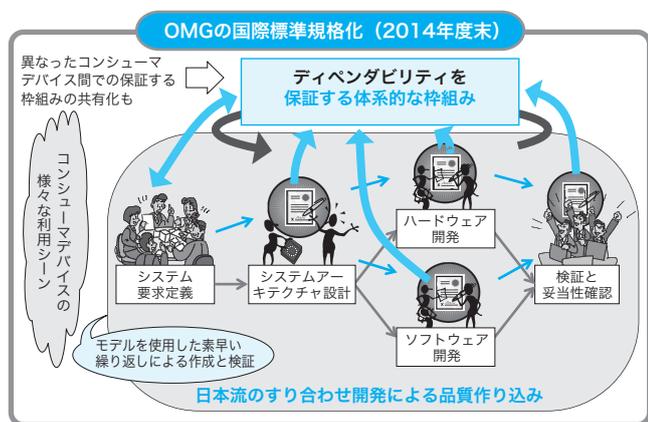


図4 日本流のすり合わせ開発による品質作り込み

4 自律連携における安全・安心を担保する仕組み

4.1 概論

自律連携とは、モノとモノが直接つながって、独自の判断により、互いに制御したり、データを交換したりすることである。換言すれば、モノ（機械）にすべてを委ねてしまうことになるため、想定外の事象が発生すれば、それが正しい動作を行わなくなり、人間の判断が関与できない事態が想定される。このような潜在リスクを極小化し、安全・安心を担保するための対策は多岐にわたるが、IPA/SECはその中でもセーフティ設計とセキュリティ設計を一定水準以上に保つことが重要であると考えている。そのために実施している活動は、次の通りである。

4.2 つながる世界のセーフティ&セキュリティ設計入門

例えば、スマホで自動車の自動駐車を制御するというサービスが実現されるかもしれない。スマホは主に通信やエンターテイメントで利用される製品だが、一方で自動車は人の命を預かるという、レベルの厳しい信頼性の設計要件を備えた製品である。2つを接続するとなると、おのずと、それらを接続しても問題ないかという確認が必要になる。設計要件が異なるこれらを接続する際に想定されるリスクとしては、別のスマホから自動車が乗っ取られてしまうという盗難の危惧や、スマホ操作中のハングアップにより動作中の自動車が暴走して事故を起こすという危険も考えられる（図5）。



図5 接続先は信頼できるか

つながる世界の安全・安心のためには、異分野製品とつながることを想定したセーフティ設計・セキュリティ設計を行っておくことが必要であり、つなげる際には互いの製品の信頼性を確認することが重要である。そのため、自身が行った設計を「見える化」（ドキュメント化）しておくことが必要不可欠になる。

ところで、セーフティ設計・セキュリティ設計の実態調査を行ったところ、その必要性はほぼ 100% 認識しつつも、経営層の関与は 30% 弱という結果であった(図6)。

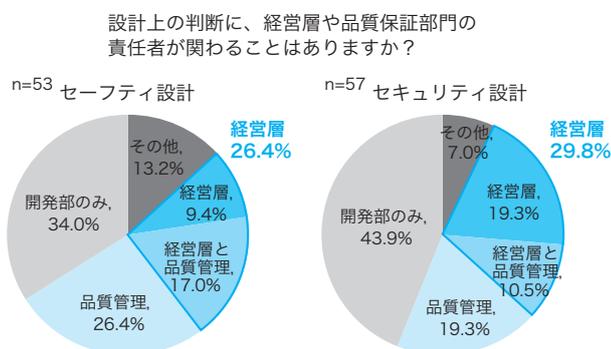


図6 セーフティ設計・セキュリティ設計に関する経営層の関与の割合

事故やインシデントが発生すると、損害賠償や企業の信用失墜といった経営リスクにつながるため、安全・安心にかかわる設計の基本方針の策定など経営層の関与が重要であると考えられる。セーフティ設計・セキュリティ設計は、表面上に見える製品やサービスの機能とは異なり、下支えする要件のため、開発現場の判断だけではコストやリソースをかけにくく、それらの推進のためにはやはり経営層の積極的なリーダーシップが不可欠と考えられる。

このような課題認識のもとに、セーフティ設計・セキュリティ設計の実施、見える化の推進、経営層の関与の必要性を解説した入門書として「つながる世界のセーフティ&セキュリティ設計入門」を作成した(図7)。



◀ 図7
つながる世界のセーフティ&セキュリティ設計入門

4.3 つながる世界の開発指針検討WGの開催

つながる世界を実現するには、セーフティ・セキュリティ・信頼性などの確保が必要であり、それらの要件を実現することを前提として新しい製品やサービスの創出が期待される。しかし、異なる分野の製品・サービスのつながりを考える場合、どのようにリスクを捉え、どの

ようなセーフティ・セキュリティ・信頼性を担保すればよいのか分からない状況である。そこで、IPA/SECは業界横断的な開発指針を作成することを目的として、「つながる世界の開発指針検討WG」を開催している。

このWGは、幾つかの業界の識者の方々へ出席いただき、その中のコンセンサスとして意見をとりまとめるものであり、あまねく業界に意見を伺うのは、次の段階としている。

つながる世界特有のリスクとしては、次のようなものが想定される。

- つながることを想定していなかったが、勝手につながってしまう。あるいは、間違っつないでしまう。
- 悪意者がつなげてしまう。
- 悪影響が周囲のつながる環境に波及的に拡大する。

それらへの対策として、IoT製品の開発者が考慮すべき事項を中心に、経営者や運用者・利用者が考慮すべき事項も含めて、開発指針として作成予定である。

4.4 システムズエンジニアリングへの取り組み

IPA/SECではつながる世界は、アメーバ状にシステムが拡大していく世界と捉えている。そこでは、色々な環境条件や要因により様々なことが発生するため、総合的な設計の考え方が必要になると考えている。そのアプローチとして、最近話題になりつつあるシステムズエンジニアリングは、課題解決のヒントを与えてくれるものではないかと推測している。そこで、IPA/SEC内にシステムズエンジニアリングに取り組むチームを立ち上げ、その見識を高めると共に、産業界へ貢献していきたいと考えている。具体的な取り組み内容は、今後詳細化していく。

5 おわりに

つながる世界は、利用者にとっては新たな製品やサービスによる更なる利便性向上への期待感があり、産業界にとっても新たなビジネス創出の鍵として捉えられている。一方で、勝手に色々なものがつながってしまうことは、安全・安心上の問題を引き起こすという危惧がある。IPA/SECは、高信頼性の観点から、引き続きこれらの課題へ取り組んでいく。