ソフトウェアグループ

セーフティ＆セキュリティ設計とその見える化の推進

SEC 研究員
鈴木　基史

SEC 研究員
西尾　桂子

SEC 研究員
宮原　真次

1 背景と課題

複数の健康器具を組み合わせたヘルスケアサービスや、スマートフォンで家電を制御するサービスなど、異なる分野の製品やサービスを組み合わせた新たなサービスが始まっており、今後は、更に様々な製品などによる高度なつながるサービスが出現すると見込まれる（図１）。

こうした認識の下、2013 年度に実施した「ソフトウェア開発の取引構造（サプライチェーン）の実態にかかわる課題の調査」において抽出し整理した課題の中から、今後とくに対応が求められる「ユーザ組み合わせ型への変化」の課題とその対策案に沿った取り組みを 2014 年度より開始した。

【課題】

- ユーザ自ら製品・サービスを選択し、組み合わせて利用する形態が増え、利用時の品質を出荷時に想定して検査することが難しくなり、品質確定のタイミングが開発段階から利用段階にシフトした。
- 製品・サービスを提供する複数の企業の責任の所在があいまいになった。
- 組み合わせ利用によるセキュリティのリスクが増大した。
- 利用者が連携時のリスクを十分に理解できていない。

【対策案】

- 組み合わせ利用における動作保証範囲、提供者の責任範囲を明確にし、利用者に対して注意喚起も含む、分かりやすい説明を行う。
- 必要に応じて製品間の制御可否を行う仕組みを導入する。

2 課題への取り組み

つながる世界において、利用者がつながる製品やサービスを安全・安心に利用するために、サプライチェーンを構成する事業者が取り組むべき事項として、組み合わせ利用における動作保証範囲、提供者の責任範囲を明確にし、利用者に対して分かりやすく説明する仕組みが今後必要である。この仕組みの実現のためには、接続先システムの品質（とくに重要なのがセーフティとセキュリティの品質）の見える化[※1]が必要であり、このためにはセーフティ設計[※2]とセキュリティ設計[※3]が確実に実施されることが重要である。

実際に IPA/SEC で実施したアンケートでは、セーフティ設計とセキュリティ設計について、「具体的に何を

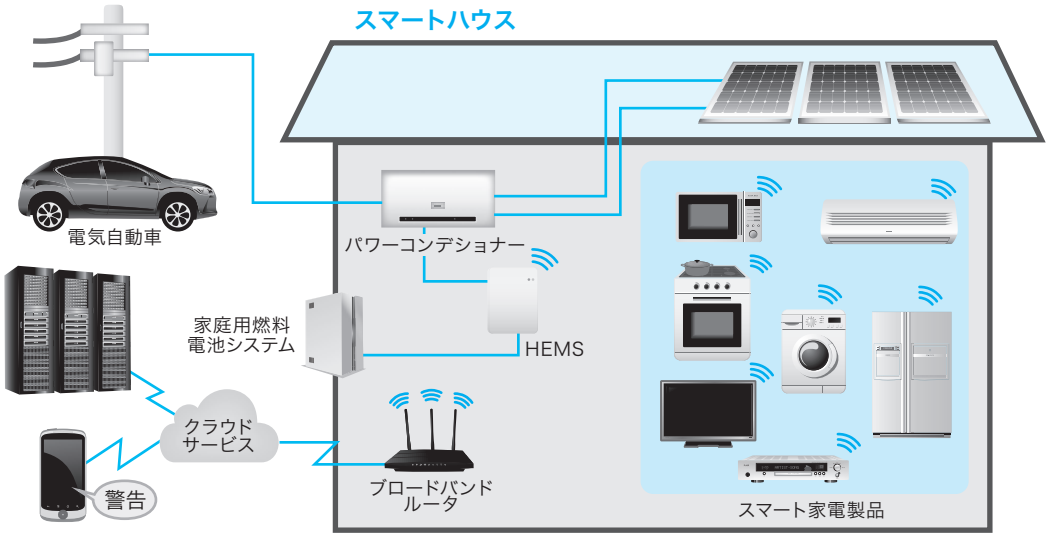

図１　製品やサービスを組み合わせて使用する「つながる世界」例

すれば良いかがわからない」「具体的なやり方が分からない」「何をどこまでやれば良いのか分からない」などの課題や、セーフティ設計とセキュリティ設計の見える化については、「チェックすべきポイントが理解されていないので何を見えるようにすべきか決めかねている」や「表記法がまだ固まっていない」などの多くの課題がある現状が見えてきたため、これらの課題に取り組む必要がある。

2.1 セーフティ・セキュリティ設計の見える化推進のための調査結果

そこで、IPA/SEC では、4 分野（自動車、スマートフォン、ヘルスケア、スマート家電）の先進的な取り組みを行っている企業におけるセーフティ設計とセキュリティ設計の実施状況について明らかにするために、「セーフティ・セキュリティ設計の見える化推進のための調査」を実施した。調査においては各企業で使われているセーフティとセキュリティの分析手法・対策手法と共に、セーフティ設計とセキュリティ設計の見える化の手法・技術についても調査を行った。

調査結果からは、ほとんどの人がセーフティ設計とセキュリティ設計の両方が必要だと考えていると分かった一方で、担当部門では「製品のセーフティ設計」または「製品のセキュリティ設計」に関する明文化された基本方針を持っていないとの回答が半数以上を占めており、セーフティ設計とセキュリティ設計について十分に普及していないことも明らかとなった。

2.2 ワーキンググループ（WG）より得られた知見

前述の課題解決に向け、セーフティ設計とセキュリティ設計及びその設計品質の見える化の普及のために、これらの分野の有識者から成る「サプライチェーンにおける品質の見える化 WG」を設置した。

WG 活動を進めるに従って、セーフティ設計に関しては、過去からの確立した設計手法があるものの、セキュリティ設計に関しては、まだ新しい分野のため公開情報が少なく、標準的な設計手法（分析・対策）の確立には至っておらず、独自の手法も多く使われていることが分かってきた。また、同じ業界の中でも、セーフティ分野とセキュリティ分野とでは使用する用語の意味や使い方が違うということも明らかになった。さらに、セーフティ設計とセキュリティ設計を統合したプロセスはまだ確立されているとは言えない状況であることも分かった。

このような状況の中、WG 委員からの意見などを踏まえ、セーフティとセキュリティの分析・対策手法を中心に初心者にも分かりやすい内容のガイドブックとして、「つながる世界のセーフティ & セキュリティ設計入門」の作成を行った。

2.3 ガイドブックの特徴

今回作成したガイドブックは以下の特徴を持つ。

① セーフティ設計、セキュリティ設計、その設計品質の見える化の 3 つを 1 冊のガイドブックに整理
② セーフティ設計とセキュリティ設計の分析・対策などの手法を初心者に分かりやすく解説
③ アシュアランスケースの表記法を設計品質の見える化手法として紹介

前半の 1 ～ 3 章は、セーフティ設計とセキュリティ設計の必要性をマネージャ層にも理解してもらえるような内容になっている。例えば、2 章ではセーフティ設計にかかわる事故事例やセキュリティ設計にかかわるインシデント事例を掲載している。また、後半の 4 ～ 6 章では、前述のセーフティ・セキュリティ設計の見える化推進のための調査結果から、実際の開発現場で使われている分析、対策、見える化の手法を中心に解説しているので、ソフトウェア技術者の参考になる内容となっている。

「つながる世界のセーフティ＆セキュリティ設計入門」
（2015 年発行予定）

・セーフティ＆セキュリティ設計、その設計品質の見える化を 1 冊のガイドブックに整理
・セーフティ設計とセキュリティ設計の分析・対策手法を初心者に分かり易く解説
・アシュアランスケース表記法を見える化手法として紹介

1 章 つながるシステムのセーフティとセキュリティ
2 章 事故及びインシデント事例
3 章 セーフティとセキュリティのための開発プロセス
4 章 ソフトウェア技術者のためのセーフティ設計
5 章 ソフトウェア技術者のためのセキュリティ設計
6 章 ロジカルな設計品質の説明

図 2　ガイドブックの特徴と目次

3 今後の取り組み

2014 年度はセーフティ設計とセキュリティ設計の重要性を紹介したプレセミナーを開催した（2015 年 3 月）。2015 年度は、本ガイドブックに基づいたセミナーを行い、セーフティ設計とセキュリティ設計及びその見える化の普及を図っていく予定である。

【脚注】

※ 1　対象システム（製品）の設計品質（セーフティやセキュリティなど）が設計において確保されていることを、エビデンスを使って論理的に第三者に分かるように説明

※ 2　設計の段階での安全の作りこみ。そのためのリスク分析とリスク低減

※ 3　設計の段階で脆弱性の低減や脅威への対策を考慮。そのためのリスク分析とリスク低減