IoT時代の安全安心に向けて

「『つながる世界の開発指針』の実践に向けた手引き[IoT高信頼化機能編]」の策定

SEC研究員　小崎 光義　SEC研究員　丸山 秀史　SEC調査役　宮原 真次

1 はじめに

IoT(Internet of Things)時代に向け、各国の様々な産業分野においてIoT機器や関連システムの開発が進んでいる。しかし、安全安心の基準が異なるシステムが相互接続することで、当初は想定していなかったリスクが顕在化することも懸念されている。

IPA/SECは、安全安心なIoTの開発に向けた着眼点を示した「つながる世界の開発指針」(以降、「開発指針」と略記)を2016年3月に策定した。この「開発指針」を参考にしながら開発するには、「具体的な機能の解説が必要」という声に応えるために、「開発指針」のうち技術面での対策が必要になる部分を更に具体化し、「『つながる世界の開発指針』の実践に向けた手引き[IoT高信頼化機能編]」(以降、「実践に向けた手引き」と略記)を2017年5月に策定した。

2 取り組みの概要

「開発指針」では、安全安心なIoTの実現に向けての着眼点と対策例を示した。その中で、例として挙げている対策は物理対策、人的対策、管理対策、技術対策から成るが、「実践に向けた手引き」では、これらのうち開発時に活用できる技術対策にフォーカスして解説することとし、次のような工夫により、開発者により具体的なイメージを持っていただくことを目指した。

(1) 設計段階から考慮して欲しい要件とIoT高信頼化機能の具体例を解説

(2) 分野間で連携するユースケースと、リスクや脅威、機能定義や機能配置の具体例を掲載

3 「実践に向けた手引き」の内容

3.1 安全安心なIoT機器・システムの開発の要件と機能

IoT機器・システムの安全安心を確保するための機能を「IoT高信頼化機能」と定義した。IoT機器・システムのライフサイクル(図1)を考慮すると、保守・運用時の視点で必要となる機能を設計時に作り込むことが重要である。例えば、運用中にシステムの障害が発生した場合、検知や回復に関する機能が必要であり、それらの機能を設計工程で作り込むなどの対処を実施する。保守・運用中の対策としては、「予防・検知・回復」の3つが必要であるが、更に、IoT機器・システムは環境や構成が絶えず変化することから、サービス開始や接続時、及びサービス終了や廃棄時の対策が必要であるので、「開始」と「終了」を追加し、開発者が

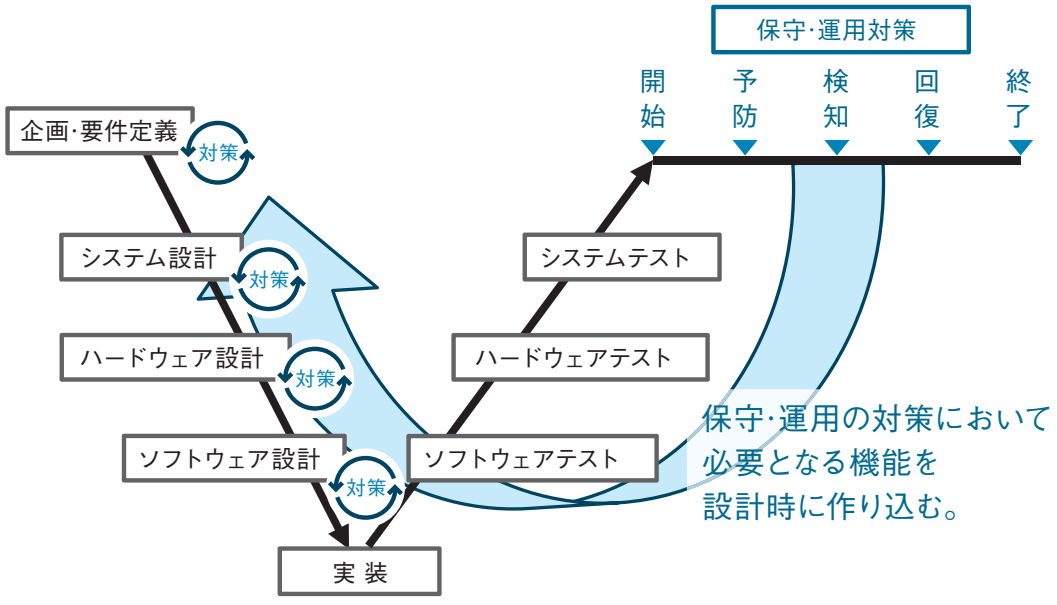

図1　ライフサイクル

設計段階から考慮すべき5つの要件を整理した。次に、それらの要件をソフトウェアで実装する場合に必要な12の機能要件に細分化し、更に、機能要件を実現するための具体的な23の機能を解説した(表1)。

また、IoT機器・システムについて、その機能配置として、エッジ層、フォグ層、クラウド層から成るIoTの構成(図2)を想定した。例えば、エッジ層では、リソースが少なく、コストがかけられないことが想定され、一律にIoT高信頼化機能を実装することが難しいので、それらのIoT特有の条件を考慮するためのポイントを解説した。更に、リスクアセスメントを行って必要な機能を搭載する手順についても解説を行った。

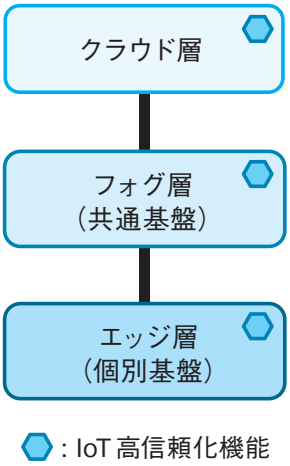

図2　IoTの構成

このように、ライフサイクルと機能配置の二つの軸で整理することにより、開発者が実装方法や必要な機能の網羅的な検討や、経済合理性や寿命を考慮した現実味のある検討に活用できると考えている。

3.2 ユースケースと、リスクや脅威、機能定義や機能配置の具体例

IoTの分野間の連携に着目した5つのユースケース(①車両と住宅の連携、②VPP(Virtual Power Plant)と分散型電源監視サービスとの連携、③宅内機器連携、④戸締り競合制御、⑤産業ロボットと電力管理の連携)を掲載した。

例えば、「戸締り競合制御」の例では、一つの住宅環境制御IoTシステムに、目的が相反する複数の制御系機能が接続された場合のリスク分析を行っている。この例では、複数の制御の競合の検知が監視機能として必要であることを説明している。

4 おわりに

「実践に向けた手引き」を活用いただくことによりIoTの安全・安心に寄与できると考えている。これまで、IoTに関連する各企業、業界団体、業界横断的団体に対して「開発指針」の普及展開を行ってきたが、今後は具体的な現場での活用に向けて本書を紹介していく予定である。「開発指針」は、多数のIoT関連の民間事業者が参画する「IoT推進コンソーシアム」が策定している「IoTセキュリティガイドライン」で採用されており、また、「IoTセキュリティガイドライン」は今後の国際標準化の提案のベースとしての活用が見込まれる。本書は国際標準化に向けた提案においてテクニカルリファレンスとしての提案も視野に入れて進めていく予定である。

「実践に向けた手引き」は以下のWebサイトで公開しているので、積極的に活用いただきたい。

https://www.ipa.go.jp/sec/reports/20170508.html

表1　IoT高信頼化の要件と機能

IoT高信頼化要件		IoT高信頼化を実現するための機能要件	対応するIoT高信頼化機能
開始	導入時や利用開始時に安全安心が確認できる	1. 初期設定が適切に行われ、その確認ができる	初期設定機能、設定情報確認機能
		2. サービスを利用するときに許可されていることを確認できる	認証機能、アクセス制御機能
予防	稼働中の異常発生を未然に防止できる	3. 異常の予兆を把握できる	ログ収集機能、時刻同期機能、予兆機能、診断機能、ウイルス対策機能
		4. 守るべき機能・資産を保護できる	アクセス制御機能、ログ収集機能、時刻同期機能、暗号化機能
		5. 異常発生に備えて事前に対処できる	リモートアップデート機能
検知	稼働中の異常発生を早期に検知できる	6. 異常発生を監視・通知できる	監視機能(競合の検知を含む)、状態可視化機能
		7. 異常の原因を特定するためのログが取得できる	ログ収集機能、時刻同期機能
回復	異常が発生しても稼働の維持や早期の復旧ができる	8. 構成の把握ができる	構成情報管理機能
		9. 異常が発生しても稼働の維持ができる	診断機能、隔離機能、縮退機能、冗長構成機能
		10. 異常から早期復旧ができる	リモートアップデート機能、停止機能、復旧機能、障害情報管理機能
終了	利用の終了やシステム・サービス終了後も安全安心が確保できる	11. 自律的な終了や一時的な利用禁止ができる	停止機能、操作保護機能、寿命管理機能
		12. データ消去ができる	消去機能