CIAJ セキュリティ Information

IPA 発刊「『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]」のご紹介

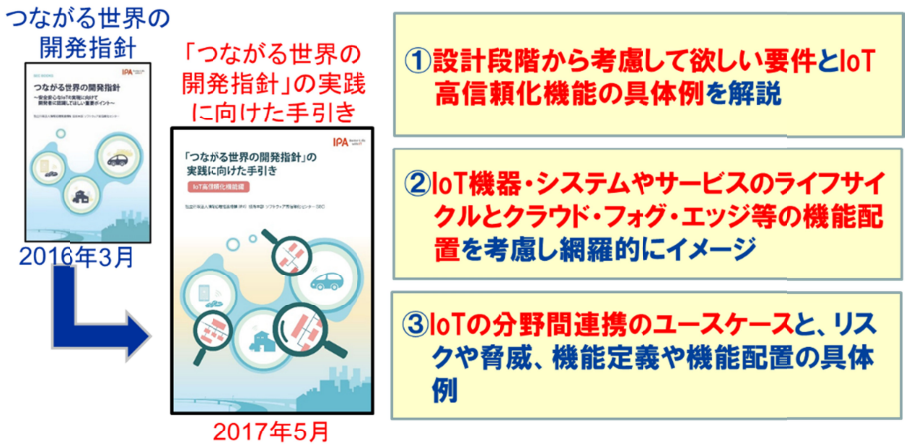
2017 年 6 月 14 日
CIAJ 通信ネットワーク機器セキュリティ分科会

はじめに

現在、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ます。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ます。

独立行政法人情報処理推進機構 ソフトウェア高信頼化センター(IPA/SEC)は、2017 年 5 月、「『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]」(以下、「本書」といいます) を公開しました。本書は、昨年 IPA/SEC から公開された『つながる世界の開発指針』で記載された指針のうち技術面での対策が必要になる部分をさらに具体化し、IoT 機器・システム開発時におけるセーフティ要件とセキュリティ要件、及びそれらを実現する機能を解説したものです。

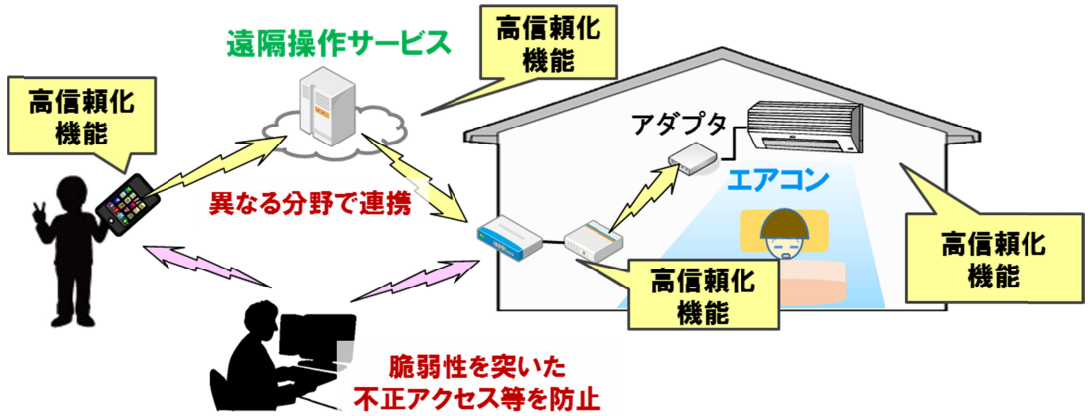
本書は、IPA 主催の IoT 高信頼化検討 WG で作成されましたが、本 WG に CIAJ も委員として参加し執筆に関わりましたので、本書の内容について紹介いたします。



(出典：IPA 「つながる世界の開発指針」の実践に向けた手引き 説明資料)

IoT の安全のために必要な機能

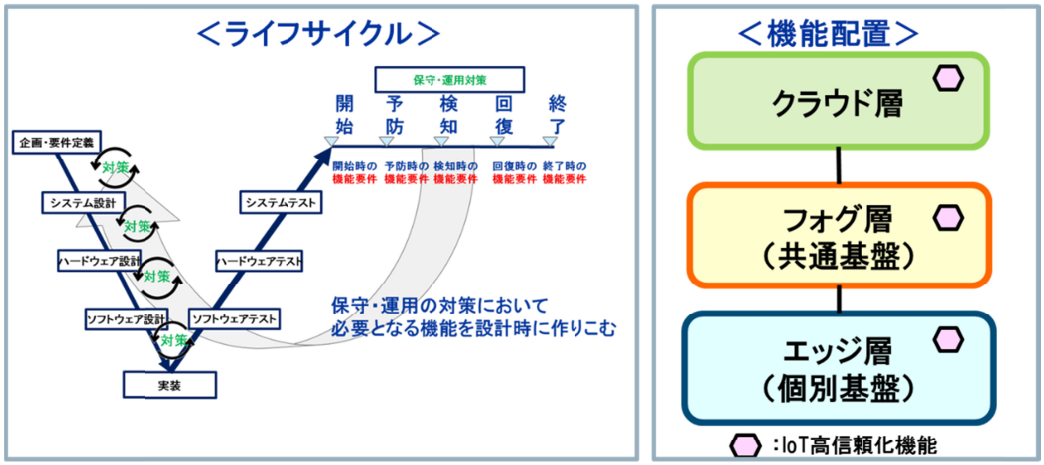
IoT の高信頼化のためには、IoT 機器・システムがつながることによる脅威やハザードを想定し、それらに対する対策を講じることが必要です。そのとき、つながるための機能だけを高信頼化するだけでは不十分で、本来の機能を含めて高信頼化しないと、高信頼化していない箇所の異常が波及してしまうリスクがあります。本書では、IoT 機器・システムが相互に連携する環境において、IoT 機能（つながる機能）および本来機能の中に実装される、安全安心を確保するための機能を「IoT 高信頼化機能」と呼んでいます。本書では、分野横断的に活用いただくことを想定して、IoT の信頼化を実現するために必要となる IoT 高信頼化機能をまとめています。



（出典：IPA 「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］）

IoT では、機器・システムの出荷やリリース後、10 年以上の長期間利用されるものも想定されます。そのため、技術やネットワーク環境の変化など多くの環境変化が考えられることを踏まえた上で、市場に出た後も想定してセキュリティ対策を考えることが重要です。機器・システムの出荷やリリース後、つまり保守・運用時に必要となる高信頼化機能は、設計時の時点で作り込むことが重要になります。本書では、IoT 機器・システムやサービスのライフサイクルを考慮し、保守・運用の視点で、サービス開始や接続時からサービス終了や廃棄時までの間に求められる対策を、予防・検知・回復に分けて整理しています。

また、本書では、脅威・ハザードの分析や、技術対策の実装を検討するために、IoT 構成を 3 層（エッジ層、フォグ層、クラウド層）に分けた IoT の基本モデルを想定しています。これら 3 層のどこにどのような IoT 機能を配置するのか、トータルに考えて設計することが求められます。例えば、リソースの少ないエッジ層においては、負荷のかかる機能を配置できない場合があり、その場合は上位のフォグ層やクラウド層でその機能を担保し、全体として IoT 高信頼化機能を実現できるようにします。本書では、IoT の基本モデルにおける IoT 高信頼化機能の配置を考慮しており、経済合理性や寿命を考慮した現実的な検討を支援します。



（出典：IPA 「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］）

IoT 高信頼化要件・機能要件

本書では、設計段階から必ず検討して欲しい要件を、「IoT 高信頼化要件」として記載しています。IoT 高信頼化要件は、保守運用における 5 つの視点「開始」「予防」「検知」「回復」「終了」で整理し、それをさらに 12 の機能要件に細分化しています。それぞれの要件については、要件の具体的な説明に加え、実装にあたって考慮すべき事項についても記載しています。

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	初期設定が適切に行われ、その確認ができる	1、2
		サービスを利用する時に許可されていることを確認できる	3、4
予防	稼働中の異常発生を未然に防止できる	異常の予兆を把握できる	5、6、7、8、9
		守るべき機能・資産を保護できる	4、5、6、10
		異常発生に備えて事前に対処できる	11
検知	稼働中の異常発生を早期に検知できる	異常発生を監視・通知できる	12、13
		異常の原因を特定するためのログが取得できる	5、6
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	構成の把握ができる	14
		異常が発生しても稼働の維持ができる	8、15、16、17
		異常から早期復旧ができる	11、18、19、20
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	自律的な終了や一時的な利用禁止ができる	18、21、22
		データ消去ができる	23

（出典：IPA 「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］）

IoT 高信頼化機能

本書では、IoT 高信頼化機能要件を実現するために利用可能な、23 の具体的な機能（例：初期設定や認証など）も紹介しています。一般的な機能においても、例えば機器の認証や軽量暗号、ホワイトリストによるウイルス対策について述べているなど、IoT について考慮した内容としています。

IoT高信頼化機能					
1	初期設定機能	9	ウイルス対策機能	17	冗長構成機能
2	設定情報確認機能	10	暗号化機能	18	停止機能
3	認証機能	11	リモートアップデート機能	19	復旧機能
4	アクセス制御機能	12	監視機能	20	障害情報管理機能
5	ログ収集機能	13	状態可視化機能	21	操作保護機能
6	時刻同期機能	14	構成情報管理機能	22	寿命管理機能
7	予兆機能	15	隔離機能	23	消去機能
8	診断機能	16	縮退機能		

（出典：IPA 「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］）

おわりに

IoT の安全安心のためには、セキュリティ、セーフティ、リライアビリティの考慮が必要です。本書は、「つながる世界の開発指針」では具体化されていなかった、安全安心な IoT の要件や必要な機能を具体化したものです。「つながる世界の開発指針」とあわせて、開発者の皆様に是非ご活用いただければと思います。

文責：吉府　研治（よしふ　けんじ）　日本電気株式会社
プロフィール
日本電気株式会社
サイバーセキュリティ戦略本部
シニアエキスパート、CISSP、CISA

【参考文献】

・IPA　開発者向け、安全安心な IoT 機器・システム開発のための「『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］」の公開
http://www.ipa.go.jp/sec/reports/20170508.html

・IPA　IoT 高信頼化検討 WG
http://www.ipa.go.jp/sec/about/committee.html#021