CIAJ セキュリティ Information

つながる世界の品質確保に向けた手引き
～IoT 開発・運用における妥当性確認・検証の重要ポイント～

2018 年 5 月 18 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

近年、さまざまな分野において、IoT 機器・システムの開発・導入が進展しています。たとえば、産業分野においては、工場の製造システムをインターネットで外部に接続し、製造設備の保守の効率化や部品調達の迅速化などの生産性向上が図られています。また、生活分野においては、家電や自動車、住宅設備などがインターネットにつながることにより、多様なサービスが生まれ、利便性の向上が図られています。

一方、IoT 機器は、屋内／屋外、高地や寒冷地など、あらゆる環境での利用が想定されます。そして利用者も幼児から高齢者まで、幅広い層の利用が考えられます。

加えて、接続される機器の種類やその個数（接続数）など利用環境が日々刻々と変化するのも IoT システムならではの特徴です。よって、これらの状況を踏まえた新たな品質確保の視点が必要です。

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、2016 年 3 月、「つながる世界の開発指針」を公開しました。同書は IoT 製品の開発者が開発時に考慮すべきリスクや対策を指針として明確化したものです。さらに、この開発指針の考え方を具体的に開発者が実践できるように、IoT で考慮すべき高信頼化要件と機能をまとめ、「『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]」として 2017 年 6 月に公開しました。2018 年 3 月に公開した「つながる世界の品質確保に向けた手引き」は、IoT 機器・システムの品質を確保し、維持・改善するという側面から IoT の品質に係わる考慮事項を本件は 13 の品質確保の視点としてまとめたものです。

本書は、IPA 主催のつながる世界の品質指針検討 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。

IoT の品質確保における課題

IoT は様々な形態でシステムが構成され、IoT 機器は様々な場所や人々に使われます。IoT は日々拡張し、変化する特徴があり、品質の異なる様々なモノがつながることで、セキュリティリスクの増大などにより生命・財産への危害や社会的信用の失墜が懸念されます。そのため、IoT の品質確保が重要になりますが、IoT の開発に経験が少ない分野や企業では様々な課題があると考えられます。例えば、開発部門が IoT に不慣れなため IoT の特徴を考慮した設計ができない、品質保証部門が IoT 開発の早期から参画したいが IoT としてのレビューポイントが見いだせないといった課題です。

そこで、本書では特に IoT の特徴や性質に着目し、IoT 関係者が考慮すべき品質の確保や維持・改善に関する事項をまとめました。

IoT の品質確保、維持・改善の 13 の視点

開発・保守での品質の確保と運用での品質の維持・改善に分けて、開発・保守では、「V&V マネジメント」、「妥当性確認」、「検証（テスト計画、テスト実施）」と、運用では、「運用マネジメント」、「運用実施」の 5 つの活動場面において、13 の視点についてまとめています。

IoT の特徴や性質である、つながる機能や多種多様なつながり方での考慮すべき事項の例として視点 2、視点 4、視点 7 を紹介します。

	活動		品質の確保、維持・改善の視点
開発・保守	V&V マネジメント	IoT の品質確保のための検証・評価計画立案	【視点1】 IoT の社会的影響やリスクを想定する
	妥当性確認	利用者視点での要求の妥当性確認	【視点2】 つながる機能の要求仕様が利用者を満足させるか確認する
			【視点3】 実装した機能が利用者の要求を満たしているか評価する
	検証	IoT の特徴に着目したテスト設計	【視点4】 多種多様なつながり方での動作と性能に着目する
			【視点5】 多種多様な利用環境や使い方に着目する
			【視点6】 障害や故障、セキュリティ異常の検知と回復に着目する
			【視点7】 長期安定稼働の維持に着目する
			【視点8】 大規模・大量データのテスト環境構築とテスト効率化を検討する
			【視点9】 テストのし易さと実施可能性を検討する
		IoT の効率的なテスト実施	【視点10】 テストを効率的に実施し、エビデンスを残す
運用	運用マネジメント	IoT の品質を維持・改善するための運用計画立案	【視点11】 運用中の環境変化による影響やリスクを想定する
	運用実施	長期利用での品質維持と改善	【視点12】 運用中の環境変化を捉え、品質が維持されているか確認する
			【視点13】 ソフトウェアの更新時はつながる相手への影響を確認する

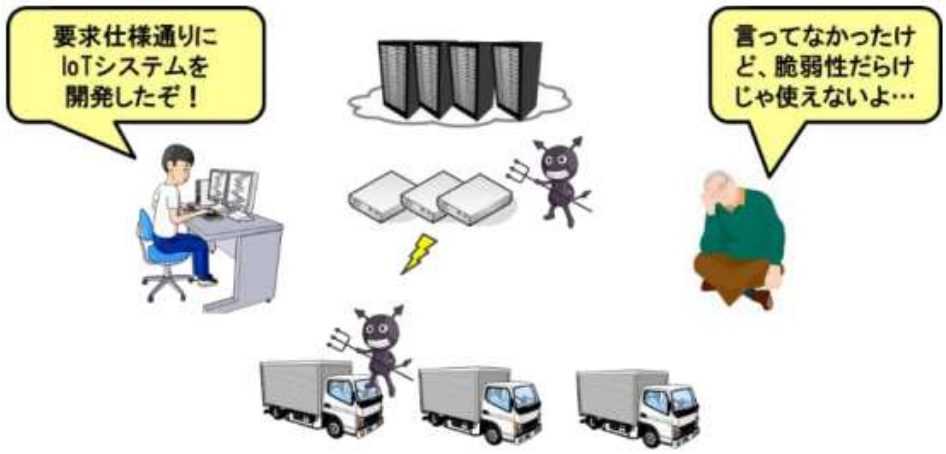
（出典：IPA 「つながる世界の品質確保に向けた手引き」）

つながる機能の要求仕様が利用者を満足させるか確認する（視点 2）

IoT の時代では、今までネットワークにつながっていなかった家電や自動車、住宅、工場の製造機器など様々な機器がネットワークにつながり、さらにそれらの分野間の連携が進むことで、大きな利便性が享受できるようになります。

しかし、一方で、多種なモノが多様な形でつながることを想定して製品・システムを開発しないと大きなリスクを伴います。2015 年の米国 Black Hat で、セキュリティの研究者から脆弱性を突いた攻撃により、自動車が遠隔から自由に操られた動画が公開されました。これは、今までつながらなかった自動車というモノが、車載器を通して外部のネットワークとつながったことによるリスクの増大の警鐘を意味します。

IoT は、利用者や利用環境が変化し、開発時点では想定外のモノが色々な形でつながるという特徴があります。これを踏まえて、IoT 機器・システムが本来提供したい価値を継続して提供できるかという視点で、要求仕様や開発要件のレビューが重要です。なお、要求仕様に直接書かれていない脆弱性対策などの暗黙的な要求も対象となります。



考慮ポイント

【2-1】IoT 特有の機能や性能、互換性や拡張性に着目する

・つながる機器の種類、性能差、取り扱うデータ、将来的な拡張性に関する要件を確認

【2-2】利用環境や利用者の使い方に着目する

・利用者や利用場面、利用者の役割などを想定しているか確認

【2-3】IoT のライフサイクルでの安全安心（注）に着目する

・機器の障害や劣化、セキュリティなどの要件を確認

【2-4】長期利用のための保守・運用に着目する

・リリース後の不具合や脆弱性対策、システムの正常稼働を確認する機能などの要件を確認

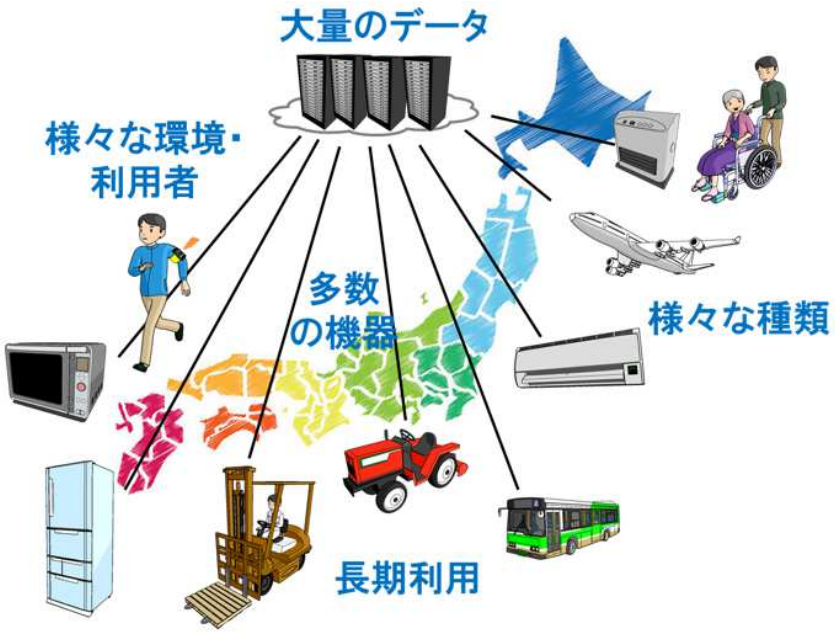
(注)対象とする機器やシステムのセーフティ、セキュリティ、リライアビリティが確保されていること

（出典：IPA 「つながる世界の品質確保に向けた手引き」）

多種多様なつながり方での動作と性能に着目する（視点 4）

IoT では 2020 年には約 300 億個の IoT 機器がネットワークに接続されることが予測されています。また、同じ IoT 機器でも様々なメーカーの製品が存在し、そのつながり方も多様です。さらに、航空機の IoT のようにエンジンをモニタリングし 1 回のフライトで約 0.5 テラ Byte ものデータを集めて燃費の改善のための解析が行われている例もあります。このように、IoT ではつながるモノの数が多く、種類やつながり方も様々で、データ量も多くなる傾向にあります。

上記のような IoT のテストの実施を考えると、大量の機器やシステムの接続や、その組み合わせの確認、また、要求される性能などを満足しているか確認が必要です。



（出典：IPA 「つながる世界の品質確保に向けた手引き」）

考慮ポイント

【4-1】多数の機器の接続や性能を考慮したテストを設計する

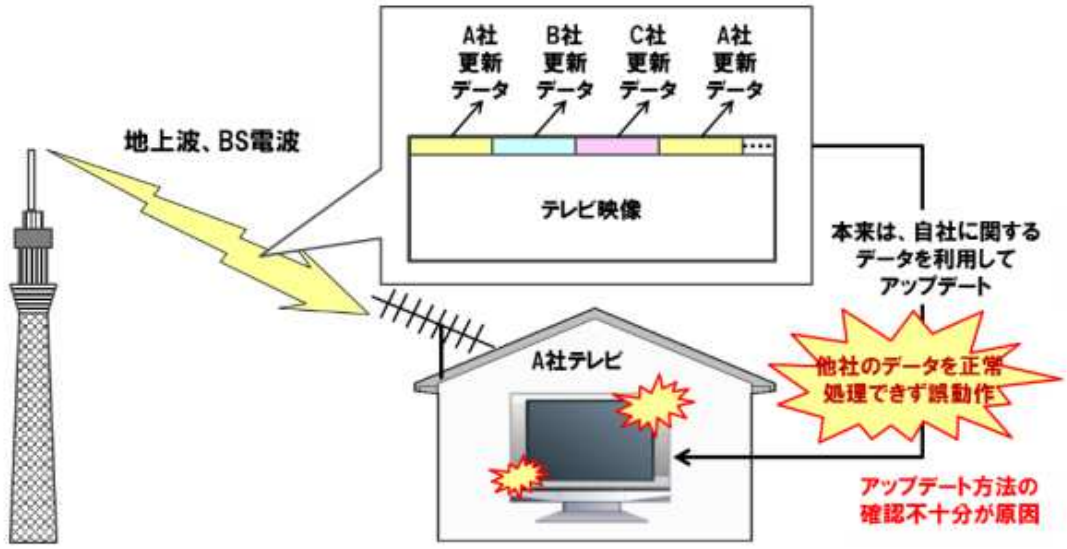
・最大接続数、データの最大量、想定外のデータ
・機器やシステムが実際に接続された状態での機能の充足性
・長期間稼働を可能にする消費電力や電池寿命
・性能評価（ピーク性能、オートスケール）、システム間の性能差による問題の有無

【4-2】多種類の機器との接続やシステム連携を考慮したテストを設計する

・機能の互換性（同一機種の異なるバージョン、同一仕様の異なるメーカー、等）
・情報の互換性（つながる機器の相互の情報交換、通信規格に準じてない機器、等）

長期安定稼働の維持に着目する（視点 7）

IoT 機器・システムの中には家電製品のように 5 年、10 年使用されるものや、工場のシステムのように 10 年以上使用されるものがあります。そのような機器やシステムをつながる環境において長期にわたって安全安心に利用できるようにするためには、ログなどが収集され障害が発生した場合に解析し、アップデートなどで不具合を修正できることの確認が必要です。一方、遠隔でのテレビのファームウェアアップデートに失敗し、テレビが OFF/ON を繰り返す不具合が発生した事例があります。このように、不具合を修正するためのアップデートの確認が不十分の場合、広範囲に影響を与える可能性があることを考慮する必要があります。



（出典：IPA 「つながる世界の品質確保に向けた手引き」）

考慮ポイント

【7-1】長期安定稼働のためのアップデートや必要なログの収集などのテストを設計する

- 障害解析に必要な機能の確認（ログの収集、転送など）
- アップデート機能の確認（セキュアな実施、アップデート失敗時のリカバリ、等）

おわりに

利用者が安心して利活用できる品質の IoT 機器・システムを提供するためには IoT 機器・システムの品質確保が必要です。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、品質確保に関する事項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、開発者だけではなく、保守者、品質保証者、運用者など、品質に携わるすべての皆様に是非ご活用いただければと思います。

著者：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　IoT 機器・システムの安全安心に向けた品質確保の手引きを公開
https://www.ipa.go.jp/sec/reports/20180322.html

・IPA　つながる世界の品質指針検討 WG
https://www.ipa.go.jp/sec/about/committee.html#024