

様々なモノがつながるIoT！
品質は大丈夫ですか？
～IoTの特徴を捉えた品質確保の勘所を紹介～

IPA 社会基盤センター
調査役 宮原 真次

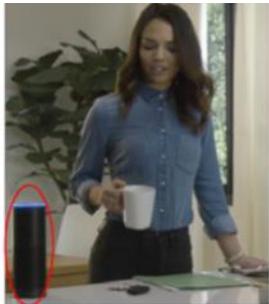
目次

- IoTの活用が進展！ リスクや課題もある！
- つながる世界の安全安心の実現に向けた
IoT開発の考慮事項
- つながる世界の品質確保に向けた重要ポイント

IoTの活用が進展！

■ 事例 1) 自動車と住宅の連携

- ・ 車内から自宅の玄関照明の点灯やガレージドアの開閉、スマート家電の操作
- ・ 自宅から車のエンジン始動やドアの施錠・開錠、燃料残量チェック、エアコン操作



■ 事例 2) 橋梁の保守・点検

- ・ 全国の橋梁は、高度成長期に作られたものが多く、老朽化。道路橋 約 70 万の 40% がもうすぐ寿命。
- ・ 橋にセンサーを取り付け、道路橋のひずみ、振動、傾斜、移動などの異常や損傷を検知

収集するデータ
● ひずみ
● 振動
● 傾斜
● 移動

活用方法
● 異常検出
● 保全計画策定



東京ゲートブリッジではセンサー（48個）により一秒あたり約2800程度のデータを測定。

【出典】 http://www.soumu.go.jp/main_content/000208995.pdf

【出典】 JETRO「ニューヨークだより2017年2月」

人命や財産を脅かすリスクも！

■セキュリティだけでなく人命や財産を脅かすリスク

監視カメラの映像がインターネット上に公開

利用者が気づかぬまま、WiFi等を通じてインターネットに接続



セキュリティ対策が不十分な**日本国内の多数の監視カメラ**の映像が**海外のインターネット上に公開**。
(ID、パスワードなどの初期設定が必要)

自動車へのハッキングによる遠隔操作

携帯電話網経由で遠隔地からハッキング



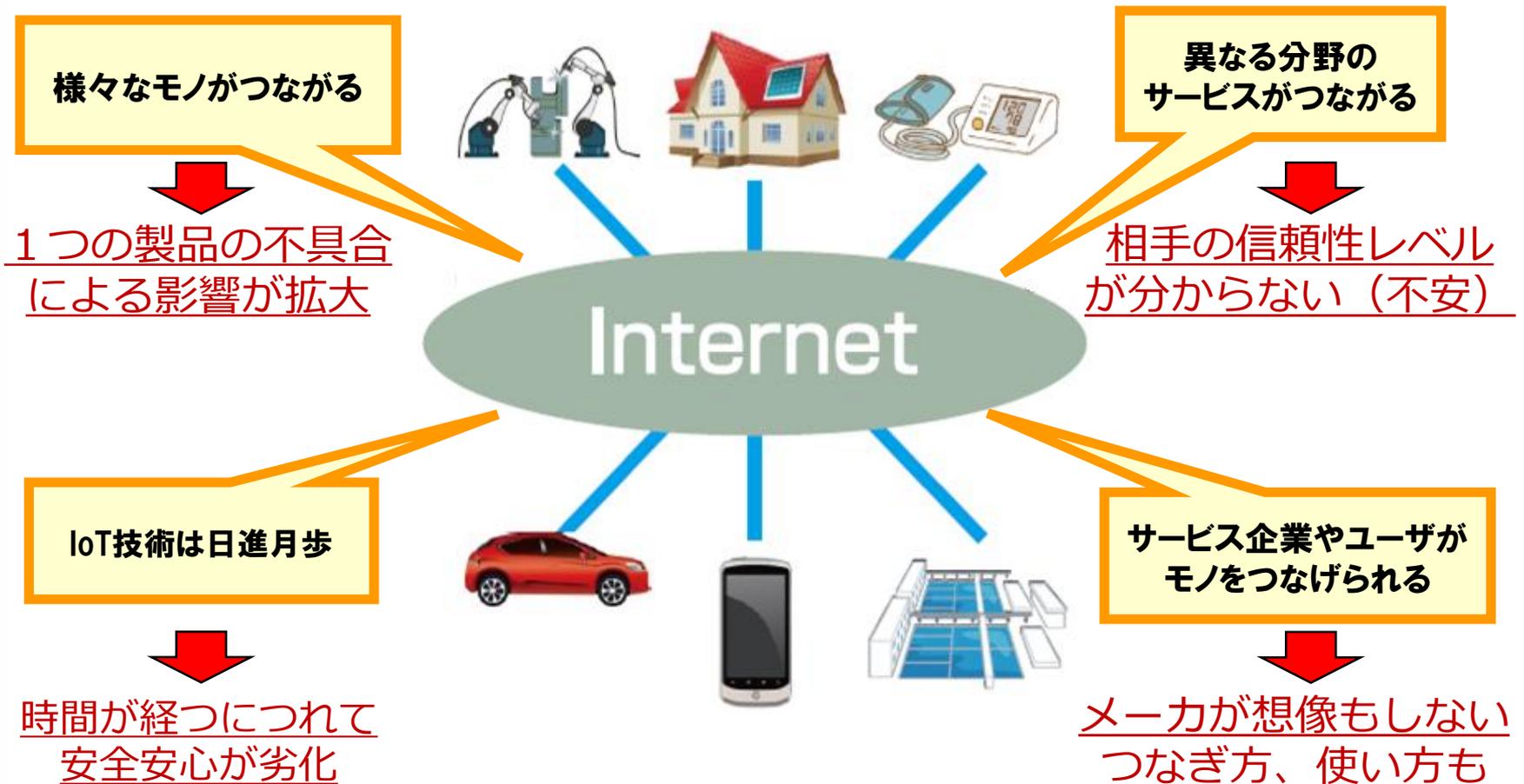
人命にも関わる事故が起こせることが証明され、自動車会社は**140万台にも及ぶリコール**を実施。

【出典】「経済産業省の取組とIoTセキュリティガイドラインVer1.0の概要」、経済産業省

IoTのリスクを認識し、安全・安心への対策が急務！

つながる世界では様々な課題が存在

つながる世界では、製品供給者が想定しない、把握できない課題が発生



つながる世界の安全安心の実現に 向けたIoT開発の考慮事項

～ 経営者・開発者向けの開発指針を紹介 ～

つながる世界の開発指針の概要



IoT機器・システムの開発者、保守者、経営者に最低限検討して頂きたい安全・安心に関する事項をライフサイクル視点で整理

◆つながる世界の開発指針の内容

目次

第1章 つながる世界と開発指針の目的

第2章 開発指針の対象

第3章 つながる世界のリスク想定

第4章 つながる世界の開発指針（17個）

第5章 今後必要となる対策技術例

※指針は、ポイント、解説、対策例を記述

※開発指針を書籍化し、2016年5月11日に発刊
http://www.ipa.go.jp/sec/reports/20160511_2.html

大項目		指針
方針	つながる世界の安全安心に企業として取り組む	指針1 安全安心の基本方針を策定する
		指針2 安全安心のための体制・人材を見直す
		指針3 内部不正やミスに備える
分析	つながる世界のリスクを認識する	指針4 守るべきものを特定する
		指針5 つながることによるリスクを想定する
		指針6 つながりで波及するリスクを想定する
		指針7 物理的なリスクを認識する
設計	守るべきものを守る設計を考える	指針8 個々でも全体でも守れる設計をする
		指針9 つながる相手に迷惑をかけない設計をする
		指針10 安全安心を実現する設計の整合性をとる
		指針11 不特定の相手とつなげられても安全安心を確保できる設計をする
		指針12 安全安心を実現する設計の検証・評価を行う
保守	市場に出た後も守る設計を考える	指針13 自身がどのような状態かを把握し、記録する機能を設ける
		指針14 時間が経っても安全安心を維持する機能を設ける
運用	関係者と一緒に守る	指針15 出荷後もIoTリスクを把握し、情報発信する
		指針16 出荷後の関係事業者に守ってもらいたいことを伝える
		指針17 つながることによるリスクを一般利用者に知ってもらう

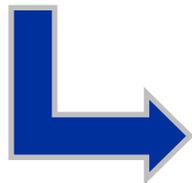
「つながる世界の開発指針」の実践に向けた手引き

- 開発指針のうち技術面での対策を具体化し、高信頼化実現に必要な機能を策定
- 2017年5月8日公開：以下のURLにpdf版掲載
<http://www.ipa.go.jp/sec/reports/20170508.html>

つながる世界の 開発指針



2016年3月



「つながる世界の 開発指針」の実践 に向けた手引き



2017年5月

① 設計段階から考慮して欲しい機能要件とIoT高信頼化機能の具体例を解説

② IoT機器・システムやサービスのライフサイクルを意識し、クラウド・フォグ・エッジ等の機能配置も考慮

③ IoTの分野間連携のユースケースによるリスクや脅威分析、対策として必要な機能や機能配置の具体例を提示

IoTの高信頼化の実現に向けた機能要件と機能

- IoT機器・システムやサービスのライフサイクルを考慮
- 保守・運用で起こり得る様々な安全安心を阻害する事象に対応できること
- IoTの利用開始から予防、検知、回復、終了の視点で能要件と実装に向けた機能を整理

IoT高信頼化要件		IoT高信頼化のための1 2の機能要件	実装に向けた2 3の高信頼化機能
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時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、ウイルス対策機能
		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、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

つながる世界の品質確保に向けた 重要ポイント

～ IoTの検証・評価で考慮すべき事項 ～

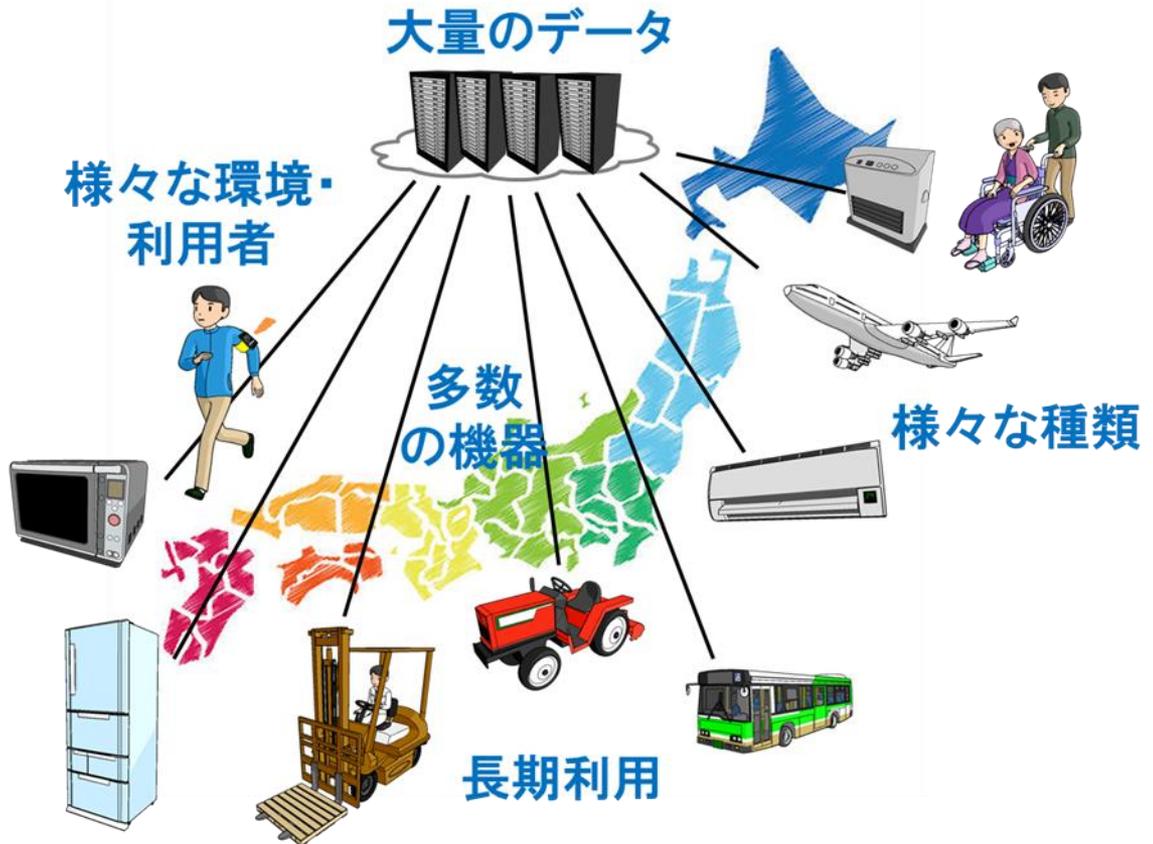
IoT時代では品質確保が重要に！

IoTの特徴

システムが日々変化！
接続される機器の種類や個数が膨大で、システムが日々刻々と変化

様々な環境で利用！
屋内/屋外、高地や寒冷地など様々な環境、幼児から高齢者まで幅広い層で利用

10年以上の長期利用！
自動車・家電製品・工場のシステムなど長期に利用



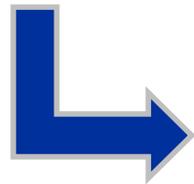
つながる世界の品質確保に向けた 手引き（概要）

- IoTの特徴を捉えて、IoTの品質確保で考慮すべき重要事項を13の視点として整理
- 開発者、保守者、品質保証者、運用者など品質に携わるすべての担当者が対象
- 2017年3月22日公開：以下のURLからpdf版ダウンロード
<https://www.ipa.go.jp/sec/reports/20180322.html>

つながる世界の 開発指針



2016年3月



2018年3月 公開

①IoTのライフサイクル全般で、品質を確保する活動を「V&Vマネジメント」「妥当性確認」「検証」「運用マネジメント」「運用実施」の5つに整理し、品質確保のための考慮事項を解説

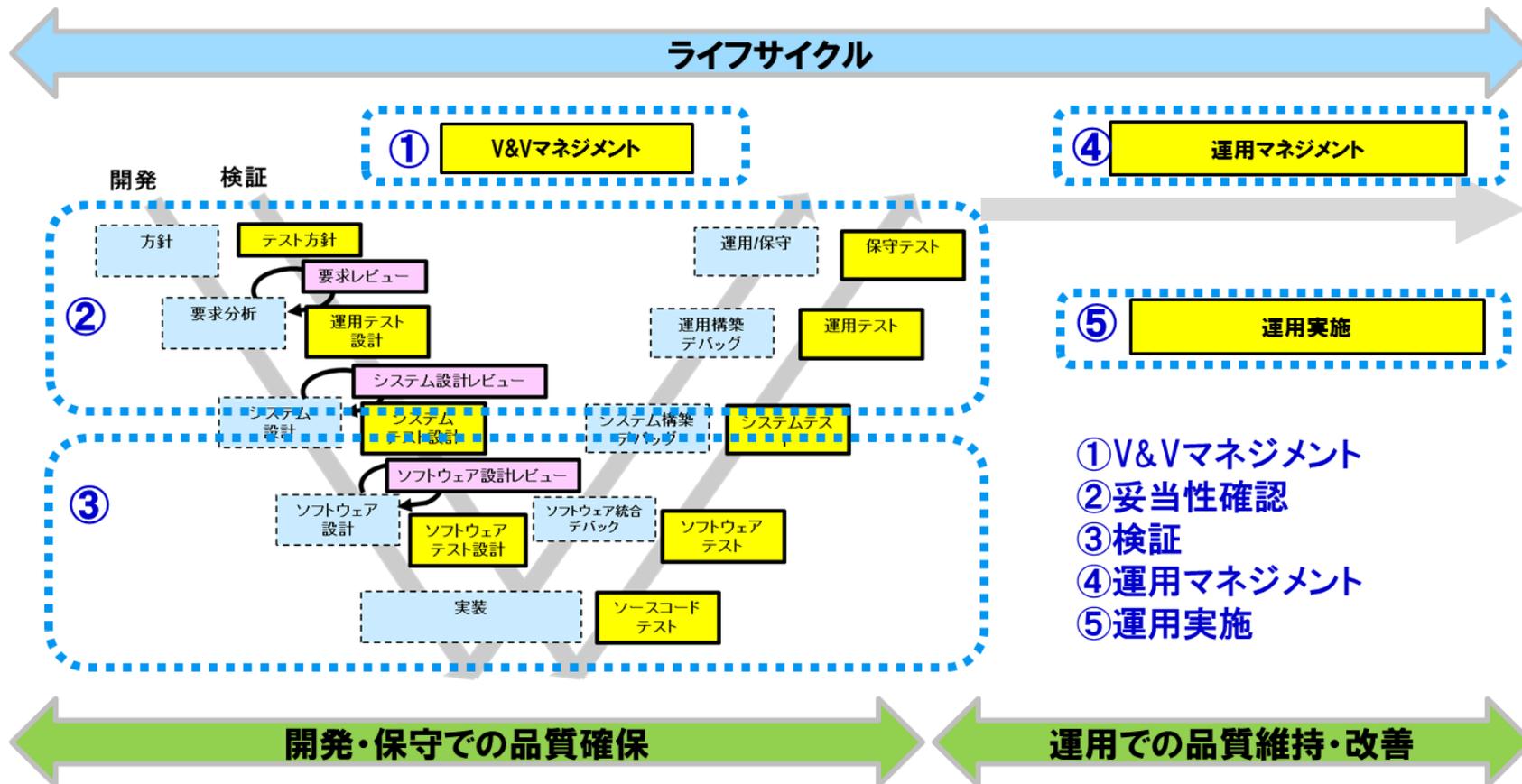
②IoTで実際に起こり得るIoTシステムの制御競合のケースを事例として、品質確保のための「13の視点」に基づき、適用検討事例を紹介

③開発・運用の現場で活用できる品質確保チェックリストを同時公開

※V&V：Verification and Validation（検証と評価）

IoTの品質確保、維持・改善のスコープ

- 品質確保の5つの場面を想定し、そこで考慮すべき重点事項を整理



IoTの品質確保、維持・改善の13の視点

■ IoTの開発・保守から運用までライフサイクルの品質に係わる重要事項を整理

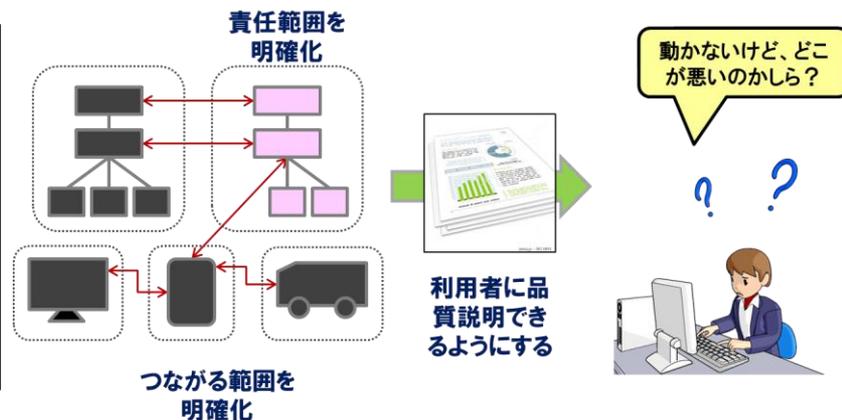
	活動	品質の確保、維持・改善の視点	
開発・保守	V&Vマネジメント	IoTの品質確保のための検証・評価計画立案 【視点1】IoTの社会的影響やリスクを想定する	
	妥当性確認	利用者視点での要求の妥当性確認	【視点2】つながる機能の要求仕様が利用者を満足させるか確認する
			【視点3】実装した機能が利用者の要求を満たしているか評価する
	検証	IoTの特徴に着目したテスト設計	【視点4】多種多様なつながり方での動作と性能に着目する
			【視点5】多種多様な利用環境や使い方に着目する
			【視点6】障害や故障、セキュリティ異常の検知と回復に着目する
			【視点7】長期安定稼働の維持に着目する
			【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

V&Vマネジメント（検証方針・計画立案）

【視点1】IoTの社会的影響やリスクを想定する

概要

- IoTでは障害が発生すると影響が拡散し、甚大な被害となる可能性がある
（例）マルウェア「Mirai」（注1）の事例では大規模なDDoS（注2）攻撃による被害が発生
- 問題が発生したときの社会的な影響やリスクを考慮し、品質の説明責任が果たせる検証・評価計画の策定が重要



（注1） <https://www.ipa.go.jp/files/000057382.pdf>

（注2） DDoS : Distributed Denial of Service attack（分散型サービス妨害攻撃）

考慮ポイント

【1-1】IoTの特徴を考慮した検証・評価の方針を策定する

- ・ 適用分野/社会的影響、法規制、プロジェクト自体のリスク、調達品の品質などを考慮

【1-2】つながる範囲を明確化してリスク・コストを意識しながら検証・評価計画を策定する

- ・ 検証評価の範囲、要員、スケジュール、評価基準、予算などを考慮

【1-3】つなぐ相手や利用者に対して品質を説明できるようにする

- ・ 調達品を含めた検証結果のエビデンスを残し、利用者や関係者に対する説明責任を考慮

【1-4】検証・評価の範囲を明確化し、関係者間の合意を促す

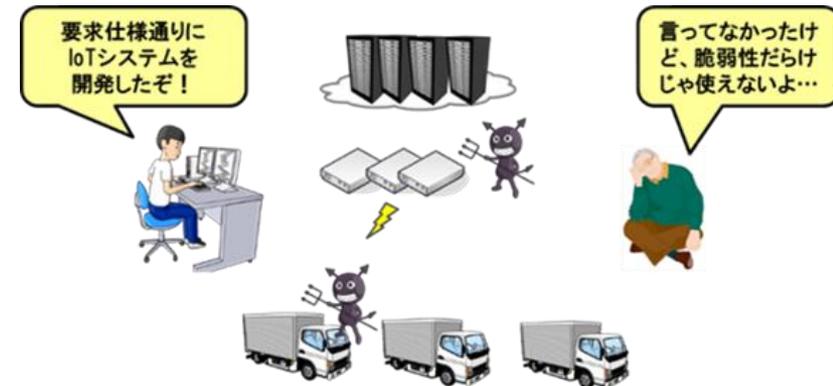
- ・ 依頼元や調達品の提供元などの関係者との合意を得るための仕組みなどを考慮

妥当性確認（要求仕様のレビュー）

【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

概要

- IoTでは利用者や利用環境の想定が難しい
 - 多様な利用者や利用環境の変化に対して、本来提供したい価値を継続して提供できるか、要求仕様そのものの妥当性を確認する
 - ・ 要求仕様に明確に書かれていない暗黙的な要求も対象とする



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

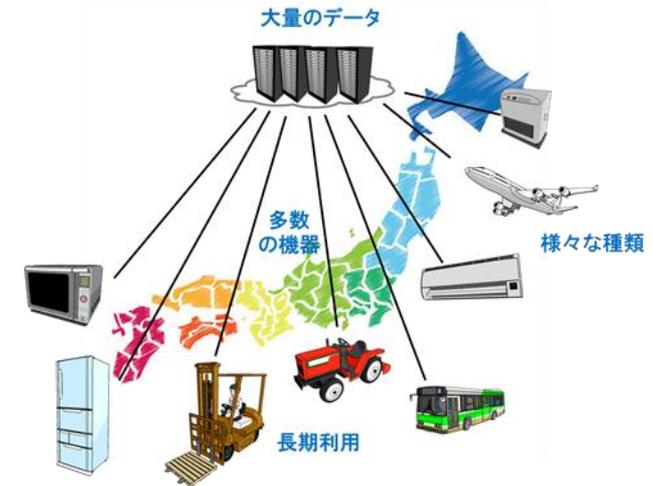
(注) 本書における定義：対象とする機器やシステムのセーフティ、セキュリティ、リライアビリティが確保されていること

検証（テスト計画）

【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

概要

- IoTは、様々な種類の多数の機器が接続され、つながり方も様々
- 大量のデータを扱い、製品の寿命が長く、省電力が要求されるものもある
- 大量の機器・システムの接続やその組み合わせ、性能などを確認できるテスト設計が必要



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）

【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

概要

- リリース前には想定していないIoT機器の接続、利用環境の変化、IoT機器のEoL（注）や連携サービスの停止・終了などのリスクがある
- 機能の正常動作、安全安心に係わる異常監視機能などの診断、正常時には動作しない装置の切り替え機能などの定期的な点検や訓練が必要

（注）EoL：End of Life（製品の生産終了）



考慮ポイント

【11-1】 運用期間において品質を維持するための計画を策定する

- ・ リリース後の変化要素の洗い出し
- ・ 定期的な品質の確認・点検作業の計画
- ・ 不具合の発生などを想定した対応プロセスの確立
- ・ 利用者からの情報公開請求やクレームへの対応

【11-2】 利用者視点で運用品質が維持されているかを評価する

- ・ 運用品質の評価項目の抽出と評価基準の策定
- ・ 定期的な運用品質の評価と関係者へのフィードバック

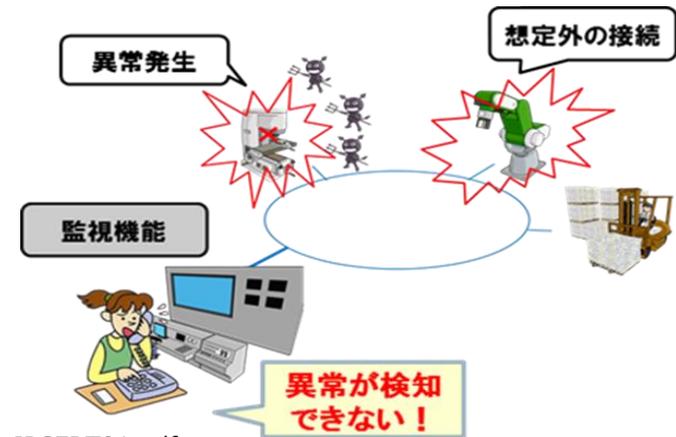
運用実施（長期利用での品質維持）

【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

概要

- リリース後に想定外のIoT機器接続やセキュリティ劣化が発生する可能性がある
 - ・ 「BlackEnergy」^(注)では、復旧活動を妨害する補助的攻撃が行われ、遠隔操作や監視機能を無効化され、復旧が長期化した。
- 機器の故障やセキュリティ異常を検知するための機能が正常動作している事の確認が重要

(注) https://www.jpcert.or.jp/present/2016/20160217_CSC-JPCERT01.pdf



考慮ポイント

【12-1】 リリース後の利用環境の変化と脆弱性などの技術情報を把握する

- ・ 利用環境の変化の把握（想定外の利用者、機器の故障やセキュリティの異常、等）
- ・ 技術方法の変化の把握（脆弱性情報、OSSなどの更新情報、法規制の変化、等）

【12-2】 利用者が直接利用する機能と安全安心に係わる機能が維持されているかを確認する

- ・ 利用者に約束している機能や性能の状況を確認し利用者へ情報提供
- ・ 安全安心に係わる機能の定期的な確認（障害監視、ウイルス対策、縮退・停止機能、等）

「つながる世界の開発指針」の展開

政府施策への展開

- IoT推進コンソーシアムのIoTセキュリティガイドラインへの展開 (2016/7)
- ERABサイバーセキュリティガイドラインへの展開(2017/4)
- その他の政府レベルのガイドラインへの展開

国際標準化

- 国内外の産業界や海外の研究機関と連携した国際標準化
- JTC1/SC27,SC41に提案 (2018/5)

海外連携

- 米NISTと連携したIoTについての検討
- 独IESEと連携した実証実験

産業界への普及

- CCDS 4分野の分野別セキュリティガイドライン (2016/6)
- チェックリスト化、社内ルール化への支援(2017/3)
- その他の分野別ガイドラインの策定への支援

スコープ拡大

- IoT高信頼化に向けた機能要件と機能のまとめ(2017/5)
- 利用時品質のまとめ (HCD-netとの共創) (2017/3)
- IoTの品質確保の検討 (IVIA,CCDS等と共創) (2018/3)
- データ品質の検討 (データ流通推進協議会等と協調予定)



第2版:利用時の品質を製品開発の考慮点に追加(2017/6)

つながる世界シリーズの活用に向けて

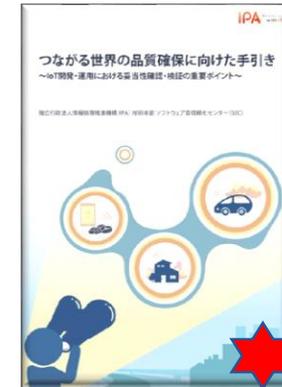
開発指針



実践に向けた手引き



品質確保に向けた手引き



企業や産業界に展開

★ チェックリストも公開

◆ 企業

- ・ 開発標準に盛り込む
- ・ 受発注時のチェック
- ・ 社内教育
- ・ お客様へのコンサル

◆ 産業界

- ・ 開発ガイドライン
- ・ 品質ガイドライン
- ・ ユーザ/会員の講習会
- ・ ユーザへの説明

つながる世界シリーズ : https://www.ipa.go.jp/sec/our_activities/iot.html

「ITSS+（プラス）」のお知らせ

第4次産業革命に向けた

スキル変革の羅針盤 ITSS+

ITSS+

IoTソリューション領域

アジャイル領域

データサイエンス領域

セキュリティ領域

学び直し

スキル強化

ITスキル標準（ITSS）

情報システムユーザー
スキル標準（UISS）

詳しくはこちら！

ITSS+



<http://www.ipa.go.jp/jinzai/itss/itssplus.html>

**つながる世界シリーズの書籍、
チェックリストの
ご活用をよろしくお願い致します！**

ご清聴、ありがとうございました。

【参考】 つながる世界の安全安心の実現に向けた取組み（書籍、報告書）

