つながる世界の品質確保に向けたIPAの取組み
～IoTのリスクを認識し安全安心の対策を！～

IPA セミナー

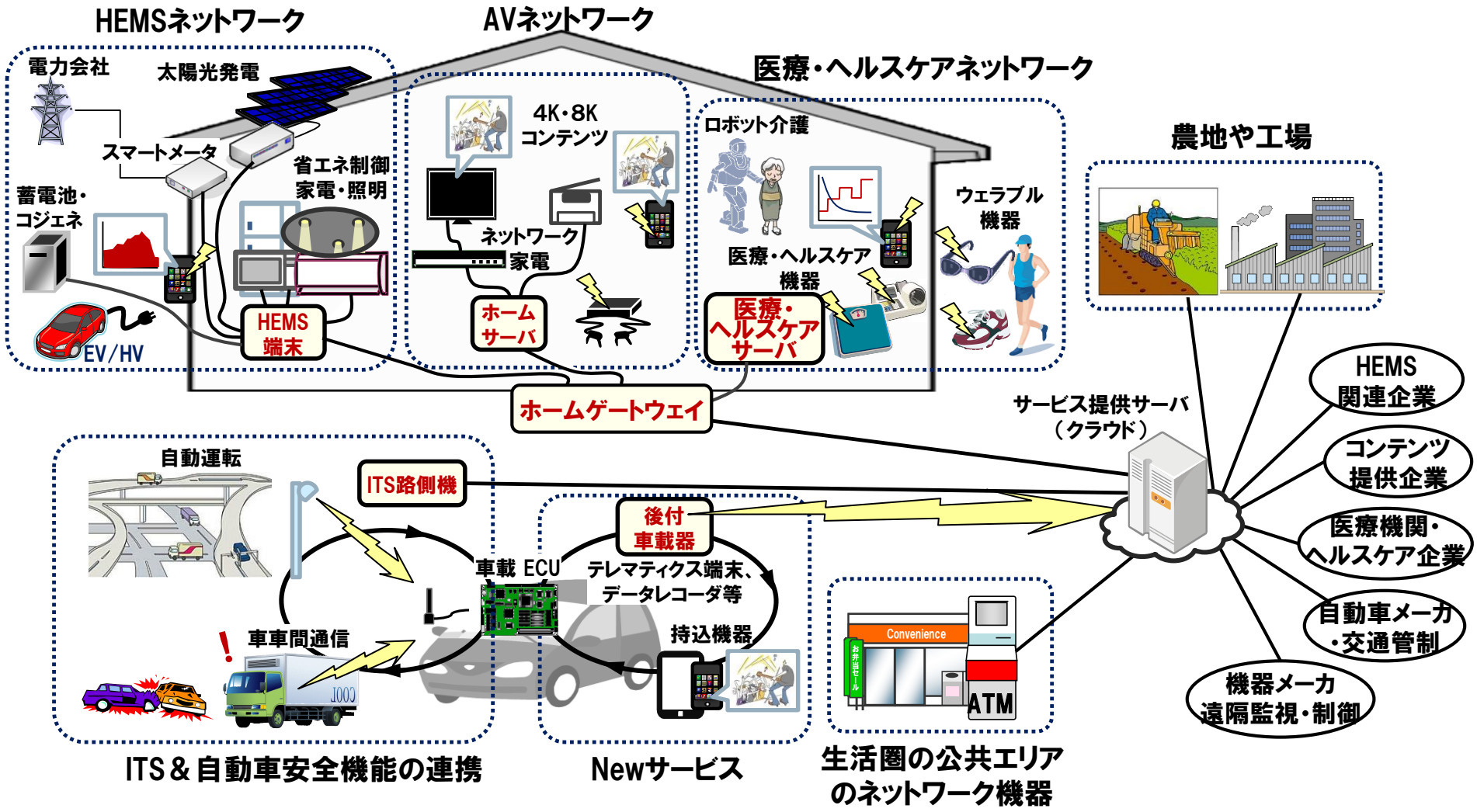
2019年2月13日

独立行政法人情報処理推進機構（IPA)
社会基盤センター　産業プラットフォーム部
調査役　宮原 真次

本日のお話

- IoTの活用事例の紹介
- IoT特有なリスク事例の紹介
- 安全・安心なIoTの実現に向けた対策
- つながる世界の品質確保チェックリストの紹介

IoT時代：様々なモノやサービスがつながる世界



出典：一般社団法人重要生活機器連携セキュリティ協議会「セキュアライフ2020」中の図に加筆

IoT事例：中小製造業の稼働状況の見える化

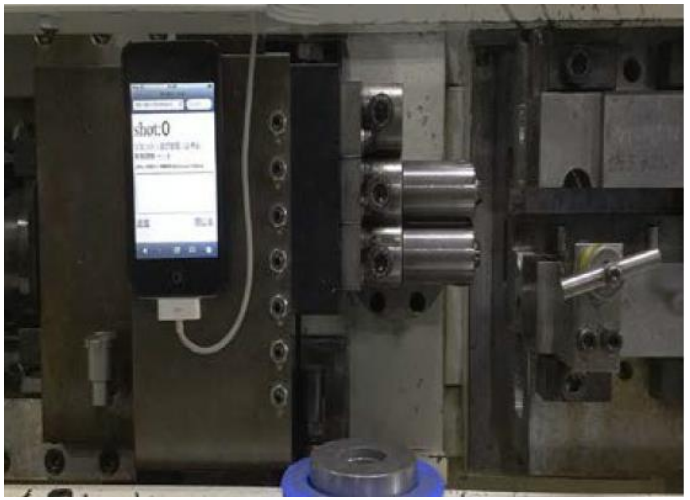
◆光センサーで工作機械の稼働情報を収集

・飯山精器(株) http://www.iiyamaseiki.co.jp/

三色灯の光をセンサで読み取り、稼働状況を蓄積。工作機械の電気的な信号を取得しないため、古い工作機械でも稼働状況を取得可能。配線などの複雑な作業も不要。

◆スマーフォンで工作機械の稼働情報を収集

・武州工業(株) http://www.busyu.co.jp/



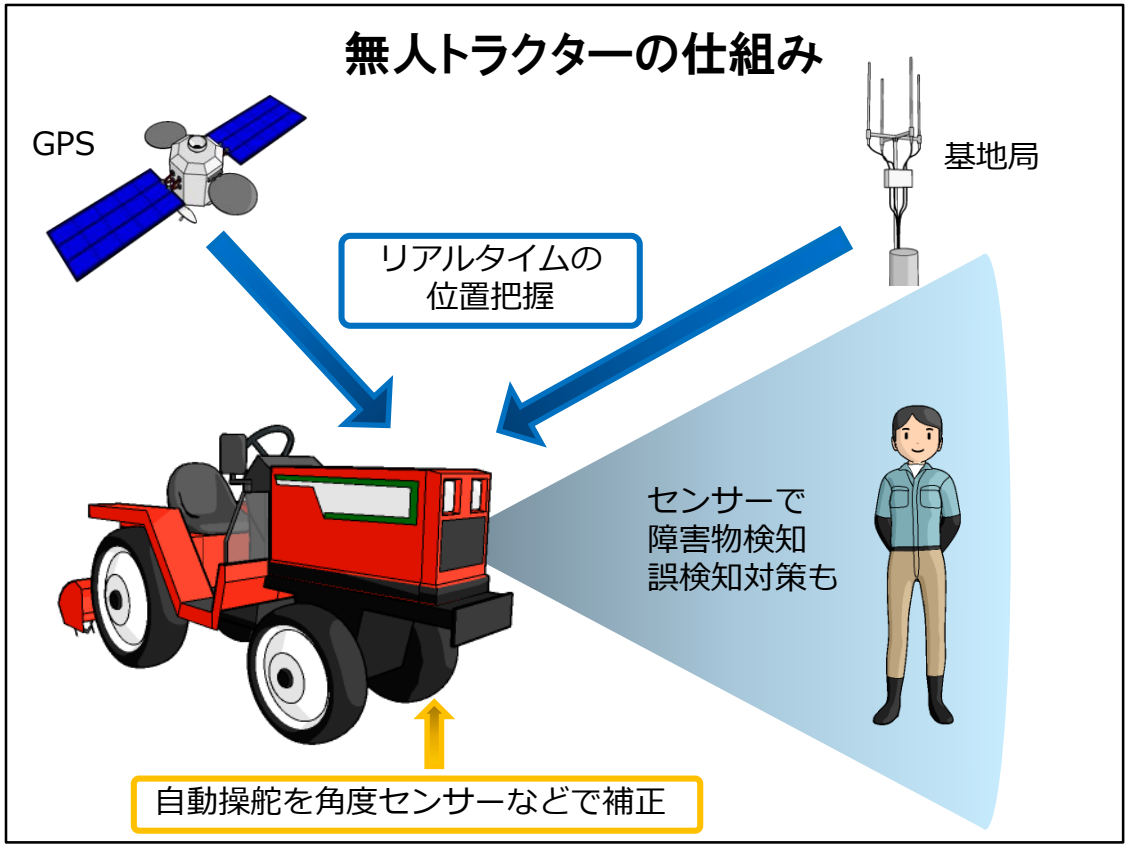
センサの代わりにスマートフォンを機械に設置し、内蔵された加速度センサで機械の稼働状況を把握。製造部品数の経時変化を見える化。

出典：経済産業省 関東経済産業局
http://www.meti.go.jp/meti_lib/report/H28FY/000279.pdf

IoT事例：農業の人手不足対策

■ GPSとセンサーを活用した無人トラクター走行

- 2017年の農業就業人口は181万6000人と7年前に比べて約3割減
- 65歳以上の割合も66%と5ポイント上昇、働き手が不足し高齢化が進展



自動運転：GPSで現在地を把握。
精度を補うために、田んぼの側に簡易型の基地局を置き、ずれを補正。
±5cmの精度を実現。

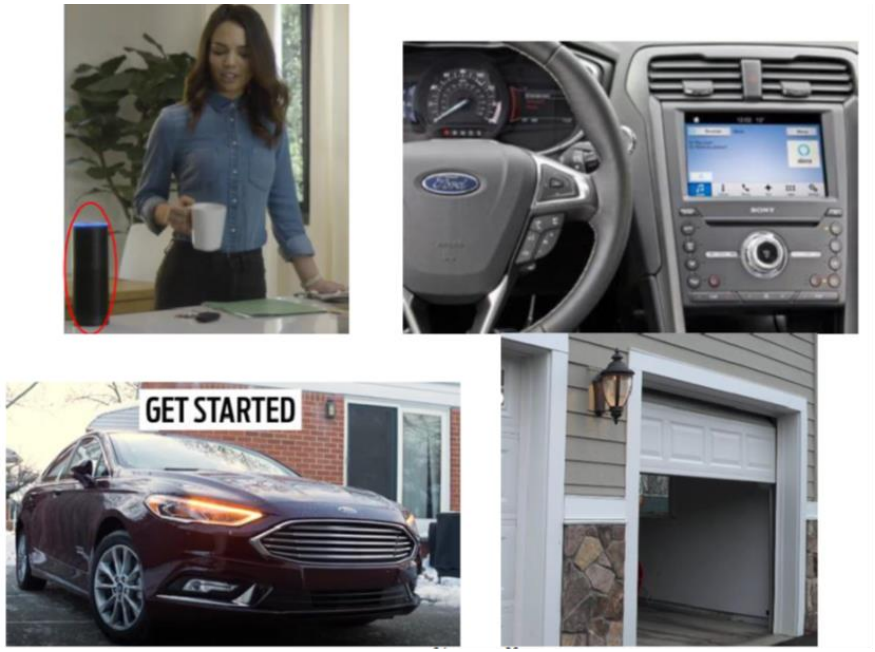
障害物検知：8台の超音波センサーと3台のレーザースキャナーを搭載。
障害物を検知すると即座に止まる。

出典：https://www.nikkei.com/article/DGXMZO26361490R30C18A1XA0000/?n_cid=SPTMG022　を基に作成

IoT事例：生活の利便性向上、社会インフラの異常検知

■ 自動車と住宅の連携

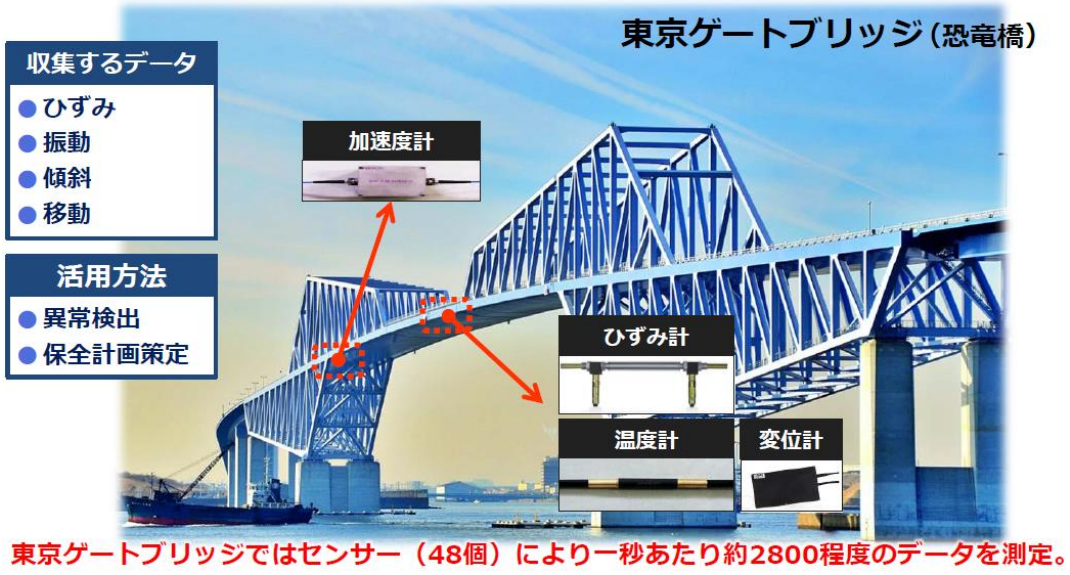
・車内から自宅の玄関照明の点灯やガレージドアの開閉、スマート家電の操作
・自宅から車のエンジン始動やドアの施錠・開錠、燃料残量チェック、エアコン操作



【出典】JETRO「ニューヨークだより2017年2月」

■ 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



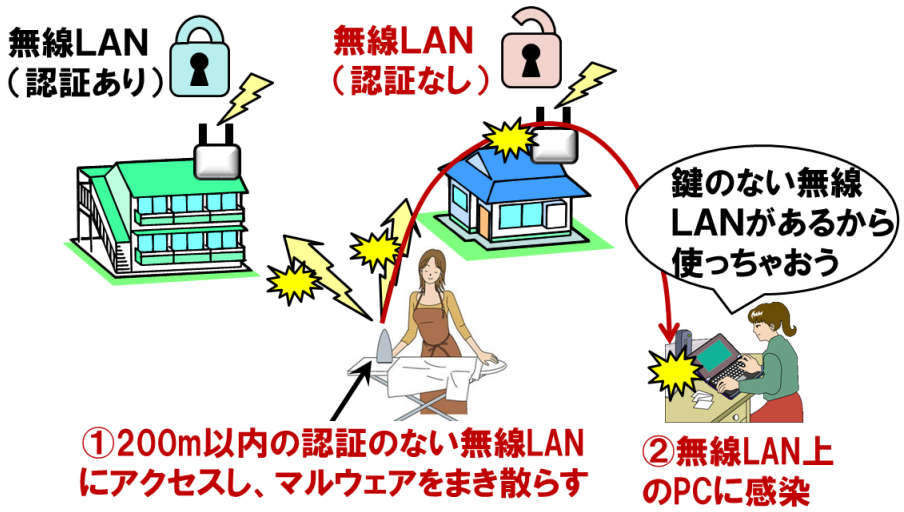
【出典】http://www.soumu.go.jp/main_content/000208995.pdf

- IoTの活用事例の紹介
- **IoT特有なリスク事例の紹介**
- 安全・安心なIoTの実現に向けた対策
- つながる世界の品質確保チェックリストの紹介

リスク事例：知らないうちにつながってしまうリスク

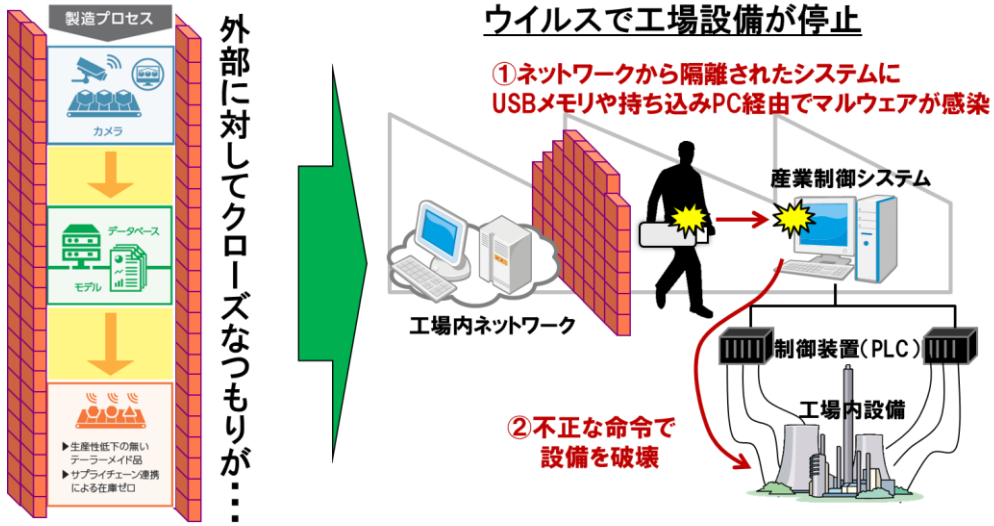
知らないうちに「つながってしまう」

ロシアで、中国製アイロンの中に近隣200m以内の無線LANにアクセスし、ウイルスを撒き散らすチップが埋め込まれていることが発見された。



つながらないつもりが「つながってしまう」

製造工場内のネットワークは外部に接続していないので安全と認識していたが、製造機器の保守などでUSBやPCを持ち込んだ時にウイルス感染したケースがある。



出典：一般社団法人 重要生活機器連携セキュリティ協議会「生活機器の脅威事例集」

IoTのリスクは身近なものと認識しましょう！

リスク事例：人命や財産を脅かすリスクも！

監視カメラの映像がインターネット上に公開

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よる遠隔操作

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！

- IoTの活用事例の紹介
- IoT特有なリスク事例の紹介
- **安全・安心なIoTの実現に向けた対策**
- つながる世界の品質確保チェックリストの紹介

つながる世界の安全安心に向けたIPAの取組み

セーフティ＆
セキュリティ
設計入門
2015年10月
発行

報告書：分野間実証実験
2017年5月 公開

実証

実践に向けた手引き
2017年6月 発行

具体化

開発指針
2016年5月 発行

拡充

第2版：利用時の品質を
製品開発の考慮点に追
加2017年6月 発行

課題2：設計手法
セーフティやセキュリティのリスク分析や設計の手法が分からない

課題3：開発指針
経営者や開発者がIoT開発時に考慮すべき事項が分からない

課題4：利用時品質
IoTは利用者が多岐にわたり、利用環境も変化、対応への考慮点

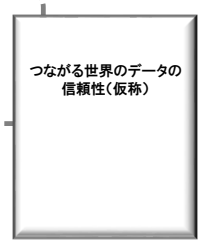
つながる世界の安全安心の実現

課題1：品質モデル
分野毎に品質の捉え方が異なり、品質に関する議論が出来ない

課題5：品質指針
変化が激しいIoTの品質をどう担保すれば良いか分からない

課題6：データ信頼性
CPSやAIで使うデータ自身の信頼性、信憑性に懸念

ソフトウェア品質ガイド
2015年5月 発行



検討中

（ﾃﾞｰﾀ流通推進協議会等と協調）

報告書：つながる世界の品質確保に向けた手引き
（IT検証産業協会と共創） 2018年6月 発行

報告書：つながる世界の
利用時の品質
（HCD-Netと共創）
2017年3月 公開

本日の
テーマ

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
併せて、開発指針チェックリストも公開
https://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

※IoTのネットワークに関する留意事項は、IoTセキュリティガイドラインを参照。
http://www.meti.go.jp/press/2016/07/20160705002/20160705002.html

「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からpdf版のダウンロード、書籍の購入**
  https://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高信頼化要件		IoT高信頼化のための12の機能要件	実装に向けた23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

IoTの特徴を意識した品質確保が重要に！

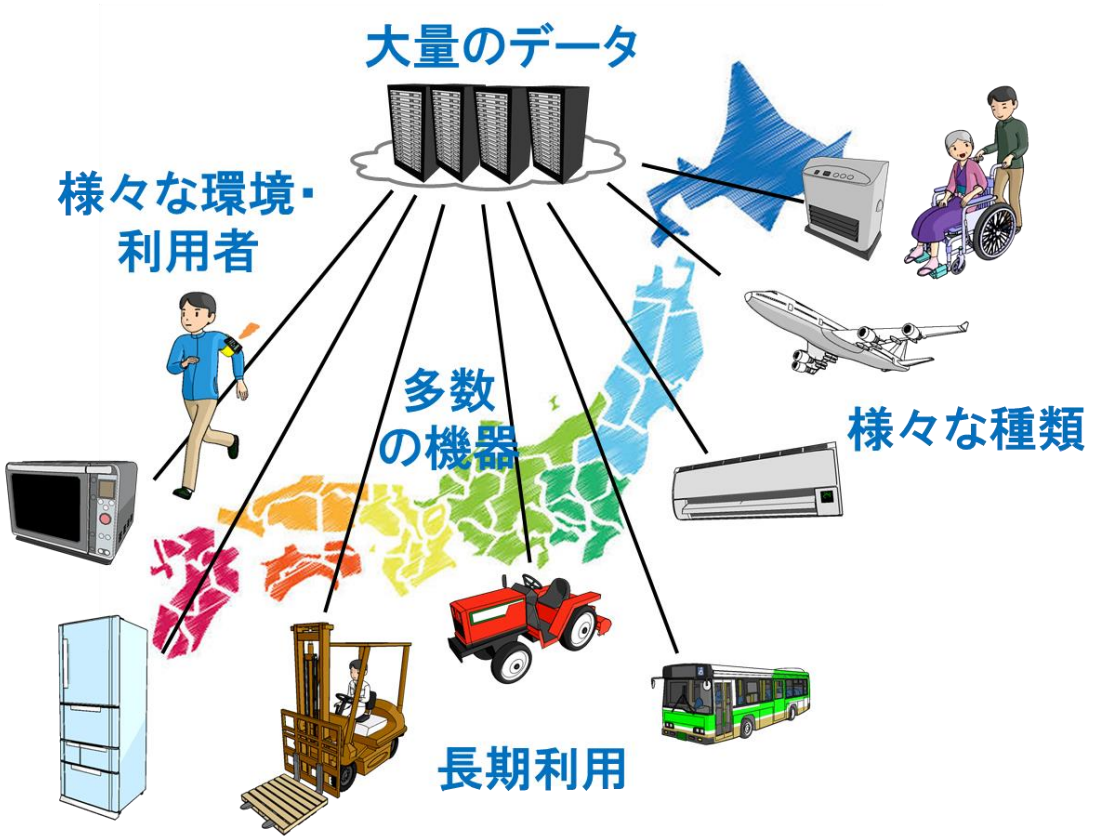
従来の製品・システムの壊れにくい/ダウンしない、性能が良い、使いやすい、デザインが良いなどの品質に加えて、IoTならではの特徴を意識した品質の考慮が必要！

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
- 2018年3月22日公開：以下のURLからpdf版のダウンロード、書籍の購入
  https://www.ipa.go.jp/sec/reports/20180322.html

つながる世界の開発指針

2016年3月

つながる世界の品質確保に向けた手引き

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

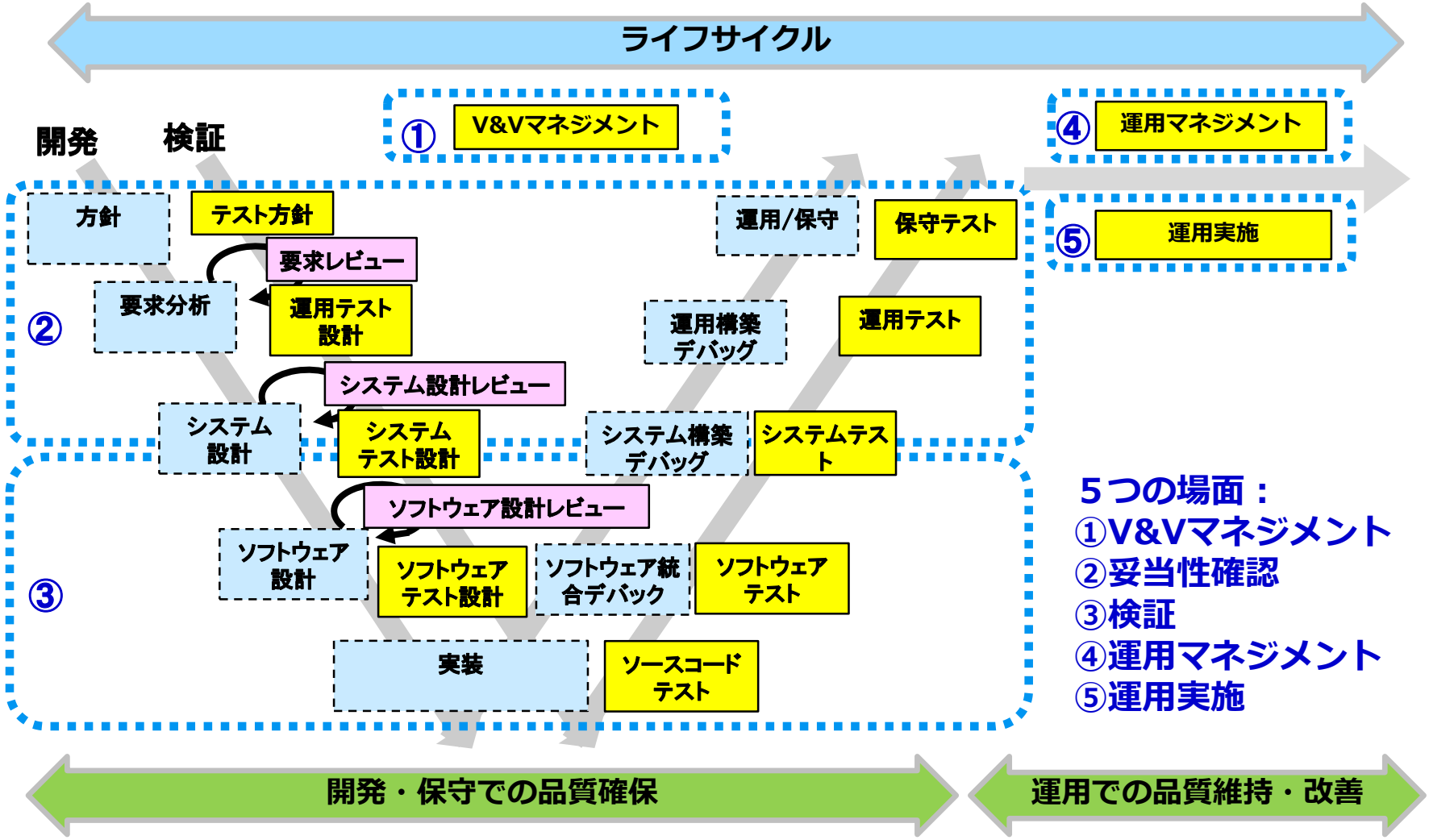
②IoTで実際に起こり得るIoTシステムの制御競合のケースを事例として、品質確保のための「13の視点」に基づき、適用検討事例を紹介

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）
検証：正しく作っているか
評価：正しいものを作っているか（妥当性確認）

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

IPA

- IoTの開発・保守から運用までライフサイクルで品質を確保、維持・改善

	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

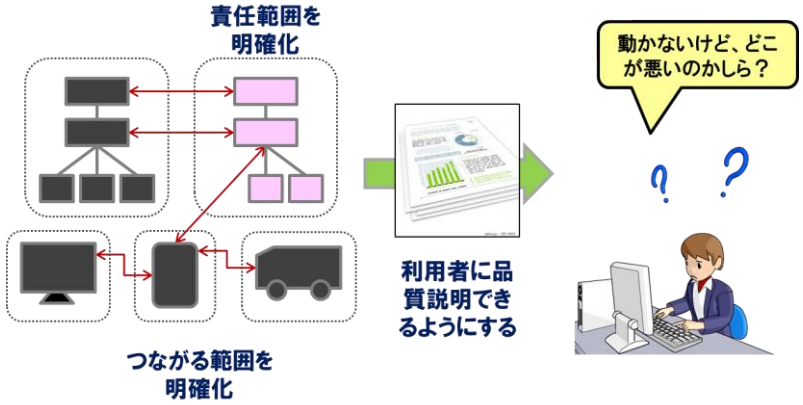
V&Vマネジメント（検証方針・計画立案）

【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合意を得るための仕組みを考慮

妥当性確認（要求仕様のレビュー）

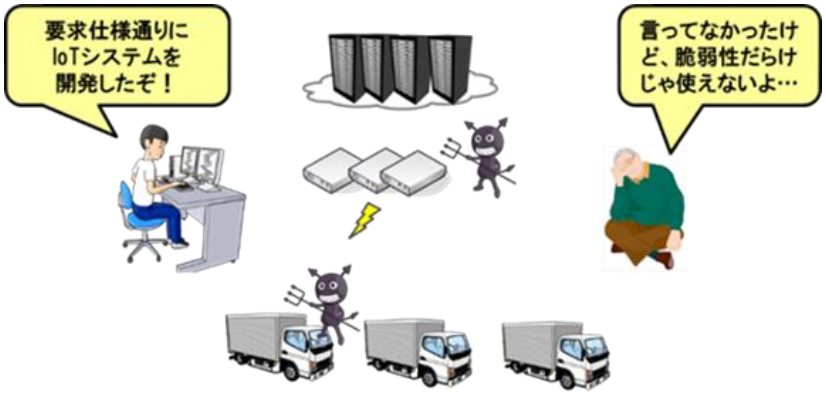
【視点2】 つながる機能の要求仕様が利用者を満足させるか確認する

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

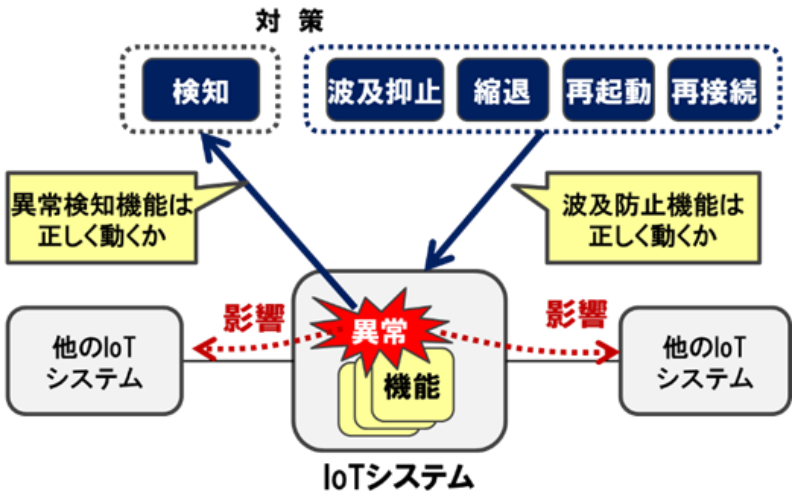
（注） 本書における定義：対象とする機器やシステムのセーフティ、セキュリティ、リライアビリティが確保されていること

検証（テスト設計）

【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

概要

- **機器・システムとの接続が行われるため、障害/故障が波及したり、セキュリティ攻撃を受ける可能性がある**
- ⇨ 障害/故障が発生しても意図された機能が維持できるか確認する
- ⇨ セキュリティについて、セーフティに与える影響を含めて確認する



考慮ポイント

【6-1】障害/故障や異常の検知、復旧などの異常処理や長期利用に係わるテストを設計する

- 設計範囲外の機器接続や異常データ発生時の処理
- 機器の障害/故障、通信の障害発生時の処理
- 長期間利用時、複数システムによる競合時の処理

【6-2】つながることによるセキュリティの脅威やそれがセーフティに及ぼす影響を考慮したテストを設計する

- セキュリティ攻撃の検知、セキュリティ/セーフティ規格による要求事項への準拠の確認レベルが異なるシステム間の接続、セキュリティがセーフティに与える影響の確認

- IoTの活用事例の紹介
- IoT特有なリスク事例の紹介
- 安全・安心なIoTの実現に向けた対策
- **つながる世界の品質確保チェックリストの紹介**

つながる世界の品質確保チェックリスト

IPA

- 手引きで記載した考慮事項に関して開発・保守、運用の現場での活用を効率化
  - 事業内容や開発の実態に合せてカスタマイズしてご利用ください！
  - URL：https://www.ipa.go.jp/files/000064878.xlsx

チェック項目について、対象とするかどうかを検討

対象とした項目について、実施状況を記入

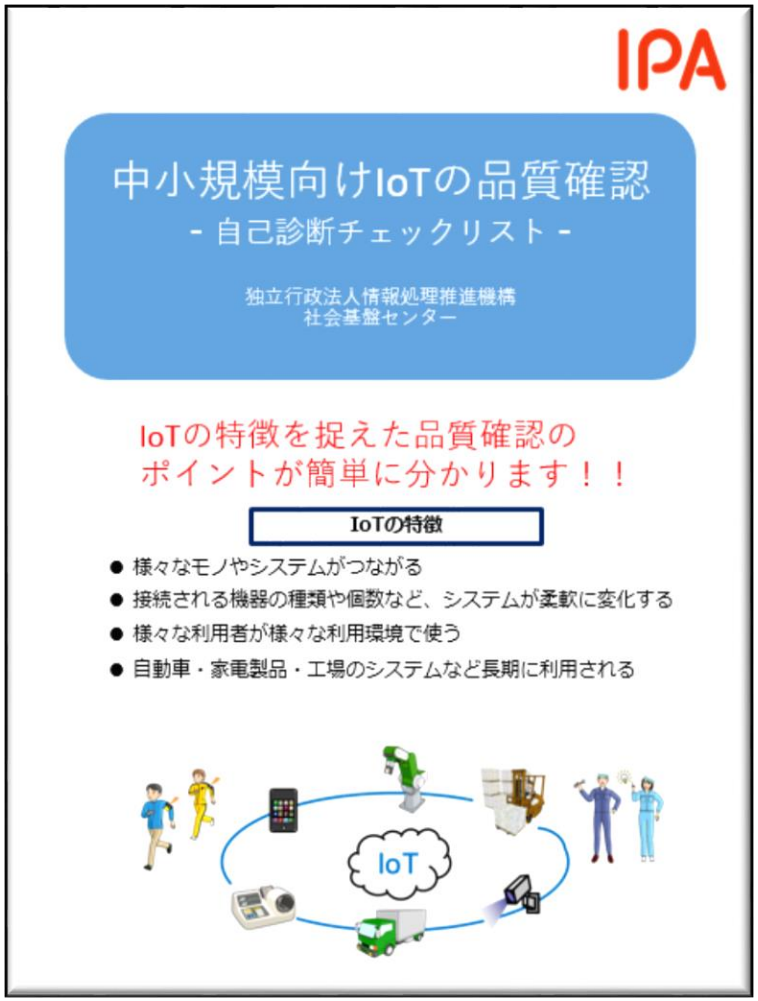
計画書やテスト結果などのエビデンスを記載

考慮ポイントとチェック項目			対象の検討	実施状況（対象と決めた場合）	エビデンス（対象と決めた場合）	確認日
【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						
	① テスト設計時の考慮項目					
	4-1-1-1	最大接続数、データの最大量に関するテストが考慮されているか？	対象	検討中		
	4-1-1-2	想定外のデータを取り扱う機能に関するテストが考慮されているか？	対象	未着手		
	4-1-1-3	様々なつながり方でつながる相手も含めた機能の充足性に関するテストが考慮されているか？	対象	未着手		
	4-1-1-4	動作寿命や消費電力に関するテストが考慮されているか？	対象外			
	4-1-1-5	IoT全体としての性能の満足性や性能のボトルネック、性能バランスに関するテストが考慮されているか？	対象	未着手		
	② テストの実行性・効率性確認					
	4-1-2-1	実行性に関して、接続性や性能の確認に必要なテスト環境の条件や仕様が明確であるか？				
	4-1-2-2	効率性に関して、つながるパターンやデータパターンなどの組み合わせテストの実行時間を予測しているか？				
【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						
	① テスト設計時の考慮項目					
	4-2-1-1	同一機種の各種バージョンでの機能の互換性に関するテストが考慮されているか？				
	4-2-1-2	同一仕様の各種メーカーでの機能の互換性に関するテストが考慮されているか？				
	4-2-1-3	システム連携などでの相互の情報の交換に関するテスト（異常データも含む）が考慮されているか？				
	② テストの実行性・効率性確認					
	4-2-2-1	実行性に関して、機能や情報の互換性の確認に必要なテスト環境の条件や仕様が明確であるか？				
	4-2-2-2	効率性に関して、テスト対象機種やバージョンの組み合わせテストの実行時間を予測しているか？				
【5-1】利用者、利用状況、利用環境などを考慮したテストを設計する						
	① テスト設計時の考慮項目					
	5-1-1-1	利用者の特性・スキル、利用場所、利用シーンなどを想定したテストが考慮されているか？				
	5-1-1-2	利用状況把握機能とプライバシー保護機能に係わるテストが考慮されているか？				
	② テストの実行性・効率性確認					
	5-1-2-1	実行性に関して、実利用に関する確認に必要なテスト環境の条件や仕様が明確であるか？				
	5-1-2-2	効率性に関して、実利用を想定したシーンの組み合わせテストの実行期間を予測しているか？				

中小規模向けIoTの品質確認チェックリスト

IPA

◆144項目のチェック項目を24項目に簡易化！



自己診断チェックリスト

対策済／一部対策済／検討中／未着手／対象外

	No.	チェック内容	チェック欄
検証・評価計画	(1)	IoT機器・システムとしての特徴や産業分野の規則など守らなければならない事項などの観点から検証・評価方針を策定していますか？	
	(2)	つながる範囲を明確にして、リスクとコストを意識しながら、検証・評価計画を策定していますか？	
	(3)	検証・評価の結果として残すべき記録（テストの実施環境、実施項目、テスト結果、実行ログなど）が明確になっていますか？	
	(4)	検証・評価計画書やテスト設計書、テストの合否判定の結果に対する合意方法や、トラブルシューティングに関する協力について、関係者間で決めていますか？	
要求仕様レビュー	(5)	IoT特有の機能、性能、将来の拡張を考慮して、要求仕様の妥当性をレビューしていますか？	
	(6)	利用者や利用環境を網羅的に考慮して、要求仕様の妥当性をレビューしていますか？	
	(7)	IoT機器の障害や劣化による影響、セキュリティ対策など、安全安心を考慮して、要求仕様の妥当性をレビューしていますか？	
	(8)	IoT機器・システムを長期的に安定して稼働させるための保守・運用を考慮して、要求仕様の妥当性をレビューしていますか？	
テスト設計	(9)	接続する機器の最大接続数やデータの最大量を考慮したテストや、性能テストを設計していますか？	
	(10)	メーカやバージョンが異なる機器と接続するときの機能の互換性や、システム連携の情報の互換性を考慮したテストを設計していますか？	
	(11)	利用者の特性・スキル、利用場所、利用シーンなどを想定したテストを設計していますか？	
	(12)	機器の故障やシステム障害の発生を想定したテストを設計していますか？	
	(13)	つながることによるセキュリティの脅威やそれがセーフティに及ぼす影響を考慮したテストを設計していますか？	
	(14)	障害解析に必要なログの収集や転送を行う機能、アップデートに関する機能（セキュアな転送、失敗時の回復、負荷・性能など）のテストを設計していますか？	
テスト実施	(15)	テスト設計で抽出したテストを確実に実施するために必要なテスト環境は準備できていますか？	
	(16)	テスト設計で抽出したテストを効率化するための手段を検討していますか？	
	(17)	テストの実行順序や組み合わせを考慮してテストをしていますか？	
	(18)	合否判断の根拠となるエビデンスを残し、テスト実施結果を開発チームと確認していますか？	
	(19)	IoTの機能が当初の目的や目標を満足しているか総合評価し、評価結果を関係者と合意していますか？	
運用計画	(20)	運用中に起こり得るシステムの機能や性能を劣化させる事項を予測し、それらの発生を把握するような監視方法と発生時の対応プロセスを決めていますか？	
	(21)	機能や性能が利用者の視点で目標を達成できているか評価し、評価結果を関係者と共有し、開発にフィードバックするプロセスを決めていますか？	
運用実施	(22)	リリース後の利用環境の変化や最新の技術情報を把握し、対応していますか？	
	(23)	利用者が利用する機能と安全安心に関する機能が正常に維持できていることを、確認していますか？	
	(24)	ソフトウェアの更新時は、接続先システムに影響を与えないことを確認していますか？	

2018年11月公開　ダウンロードURL: https://www.ipa.go.jp/ikc/reports/20181113.html

品質確保チェックリストの用途、適用後の気づき

➢ IoT製品・システム開発の品質確認に適用

・新規製品開発やエンハンス時、障害対策後の品質確認
・PoC(Proof of Concept：概念実証)の要件確認、量産移行時の品質確認
・クローズドなシステムから外部システムに連携拡張する時の品質確認

➢ IoT製品・システムの発注/調達時の確認に適用

・発注時の購入仕様の品質確認条件や受入検査事項
・調達品の品質確認

➢ 品質コンサルや第三者検証の確認に適用

・お客様への検証/評価コンサルの素材
・検証業務の受託案件の品質確認

◆ケアしていない確認項目があり、参考になった。危機感を感じた。
◆開発と検証チームが一体となって取り組む必要があることを改めて認識できた。
◆開発の上流工程で利用することで品質向上に繋がるという認識が強くなった。

つながる世界シリーズの書籍、及び
チェックリストのご活用を
宜しくお願い致します。

ご清聴ありがとうございました。