

つながる世界の安全安心の実現に向けた取組み

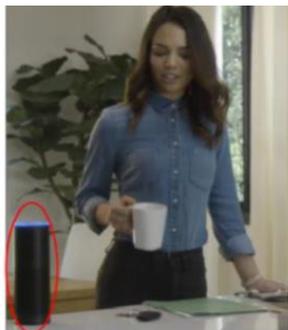
IPA/JEITA 共催セミナー in 仙台
2018年9月28日

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

- IoTは便利になるけど、リスクもあるよね？
- IoTの開発は、どうしたらいいのでしょうか？
 - 安全・安心なIoT開発のポイントを考えよう！
- IoTの品質確保は、従来とは、何が違うの？
 - IoTの特徴を意識して、品質確保を考えよう！

■ 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

東京ゲートブリッジ (恐竜橋)

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

加速度計

ひずみ計

温度計

変位計

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」

監視カメラの映像がインターネット上に公開

利用者が気づかないまま、WiFi等を通じてインターネットに接続



攻撃者



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



攻撃者

カーナビ経由でハンドル、ブレーキを含む制御全体を奪取。

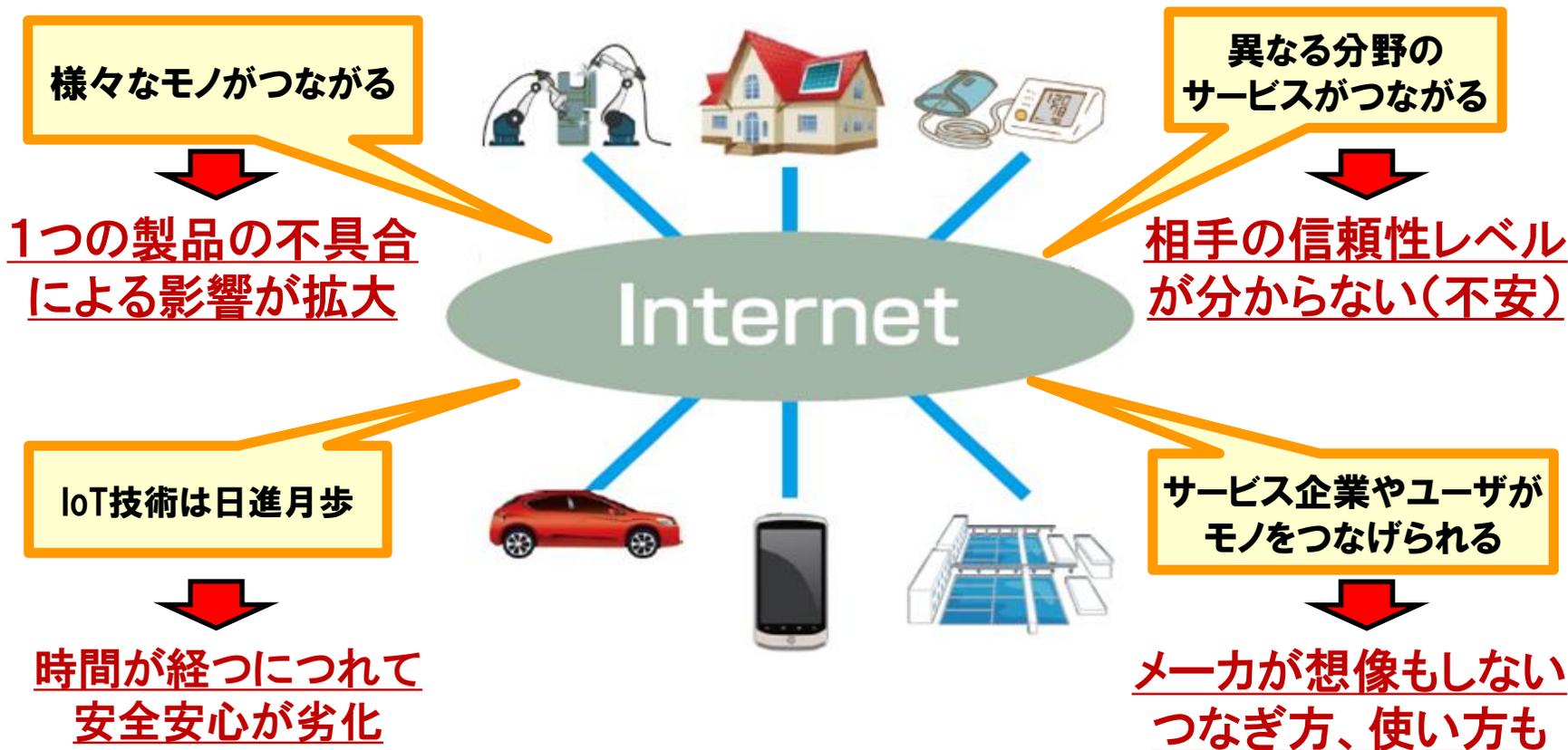


人命にも関わる事故が起こせることが証明され、自動車会社は**140万台にも及ぶリコール**を実施。

【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、製品供給者が想定しない、把握できない課題が発生



IoTの開発は、どうしたらいいのでしょうか？

- 安全・安心なIoT開発のポイントを
考えよう！



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	関係者と一緒を守る	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とってもらう

■ 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

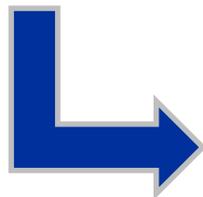
- 2017年5月8日公開:以下のURLからpdf版のダウンロード、書籍の購入

<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



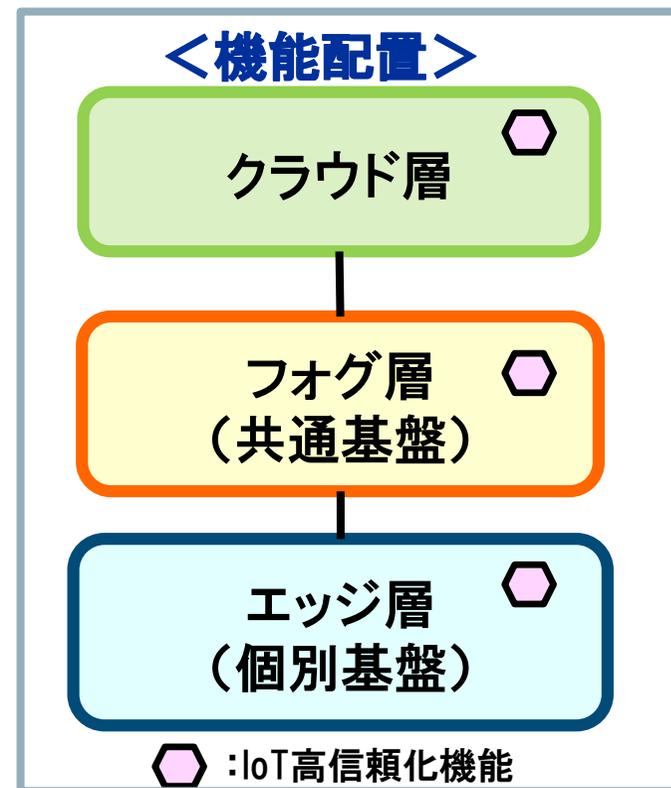
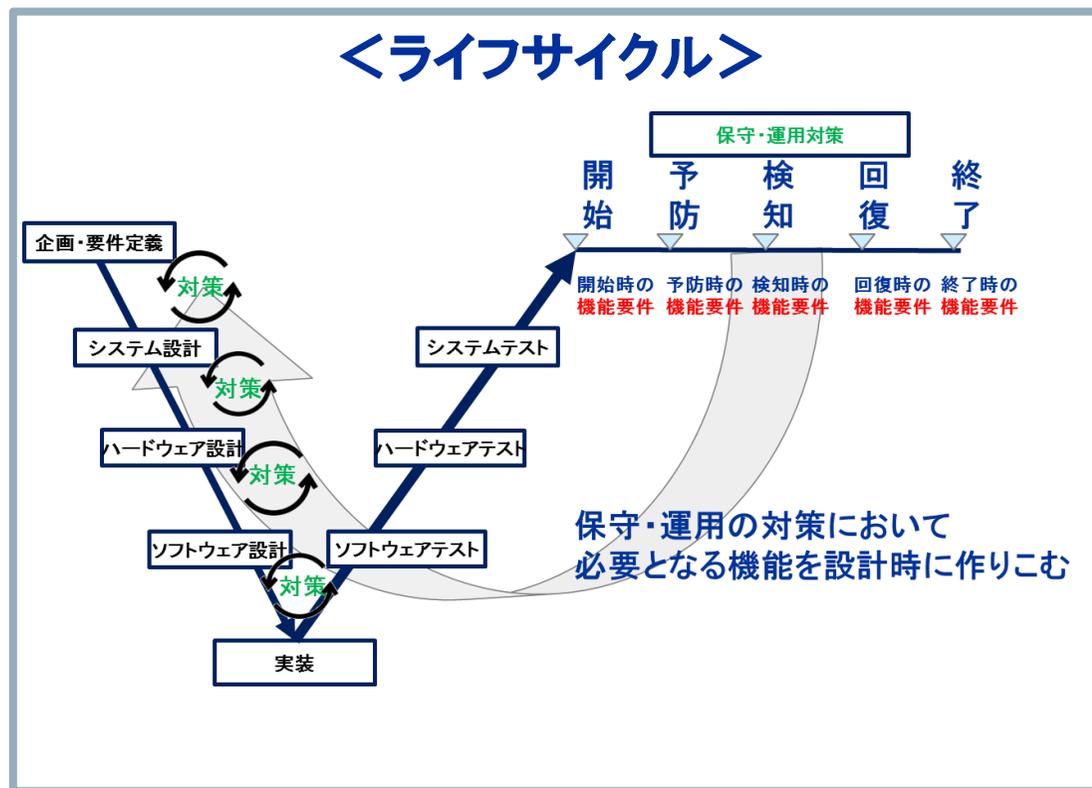
2017年5月

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機器・システムのライフサイクルを考慮し、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を目的に、IoTの**利用開始から予防・検知・回復、終了**の視点で、必要な機能を整理
 - **クラウド・フォグ・エッジ**等の機能配置を考慮
- 経済合理性や寿命を考慮し、全体として高信頼化を達成するための現実解を支援



IoTの高信頼化の実現に向けた機能要件と機能

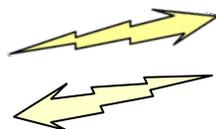
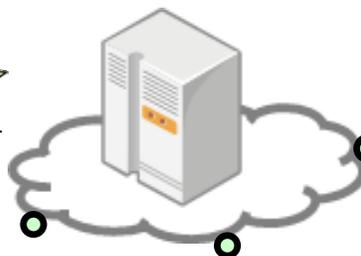
IoT高信頼化要件		IoT高信頼化のための12の機能要件	実装に向けた23の高信頼化機能
開始	導入時や利用開始時に安全安心が確認できる	1. 初期設定が適切に行われ、その確認ができる	初期設定機能、設定情報確認機能
		2. サービスを利用する時に許可されていることを確認できる	認証機能、アクセス制御機能
予防	稼働中の異常発生を未然に防止できる	3. 異常の予兆を把握できる	ログ収集機能、時刻同期機能、予兆機能、診断機能、ウイルス対策機能
		4. 守るべき機能・資産を保護できる	アクセス制御機能、ログ収集機能、時刻同期機能、ウイルス対策機能
		5. 異常発生に備えて事前に対処できる	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

(1) 利用開始時に守る！(接続時の考慮)

IoTデバイス



クラウドサービス



あれ？ デバイスの
パスワードが初期値の
ままだよね？ 警告しよう！
⇒**設定情報確認機能**

知らないデバイスが
つなげて来たけど
許可するの？
⇒**認証機能**

何か怪しいデバイス
の様なので使える機能を
制限しようか？
⇒**アクセス制御機能**

(2)利用中に守る！（予防、検知、回復の考慮）

IoTデバイス



クラウドサービス



脆弱性の問題が発覚！
早期に予防処置しよう！
⇒構成情報管理機能、
リモートアップデート機能

守るべきモノを特定し
どう守るか対策を入れよう！
⇒ウイルス対策機能、
暗号化機能

常時、ログを取って、
異常を監視しているし、
定期診断もしているから安心！
⇒ログ収集機能、監視機能
診断機能

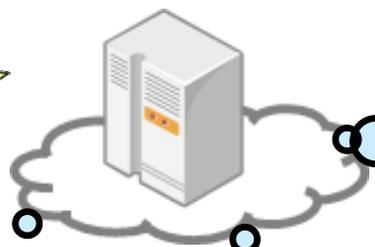
何か怪しい振る舞いだなあ～
乗っ取られた様だ！そのデバイスは
強制停止させよう！
⇒予兆機能、停止機能

(3)利用後も守る！(放置、リユース、廃棄時の考慮)

IoTデバイス



クラウドサービス



レンタカーを返したの？
個人情報消さないよね！
⇒消去機能、
(リモート消去)

盗難の連絡が入った！
そのデバイスは、
使えない様にしよう！
⇒操作保護機能

何年も放置されているなあ～
契約に従って、そのデバイスは
電源を落とすか！(野良IoT対策)
⇒停止機能
(リモート電源Off)

IoTの品質確保は、従来とは、何が違うの？

- **IoTの特徴を意識して、品質確保を
考えよう！**

IoTの特徴

システムが日々変化！

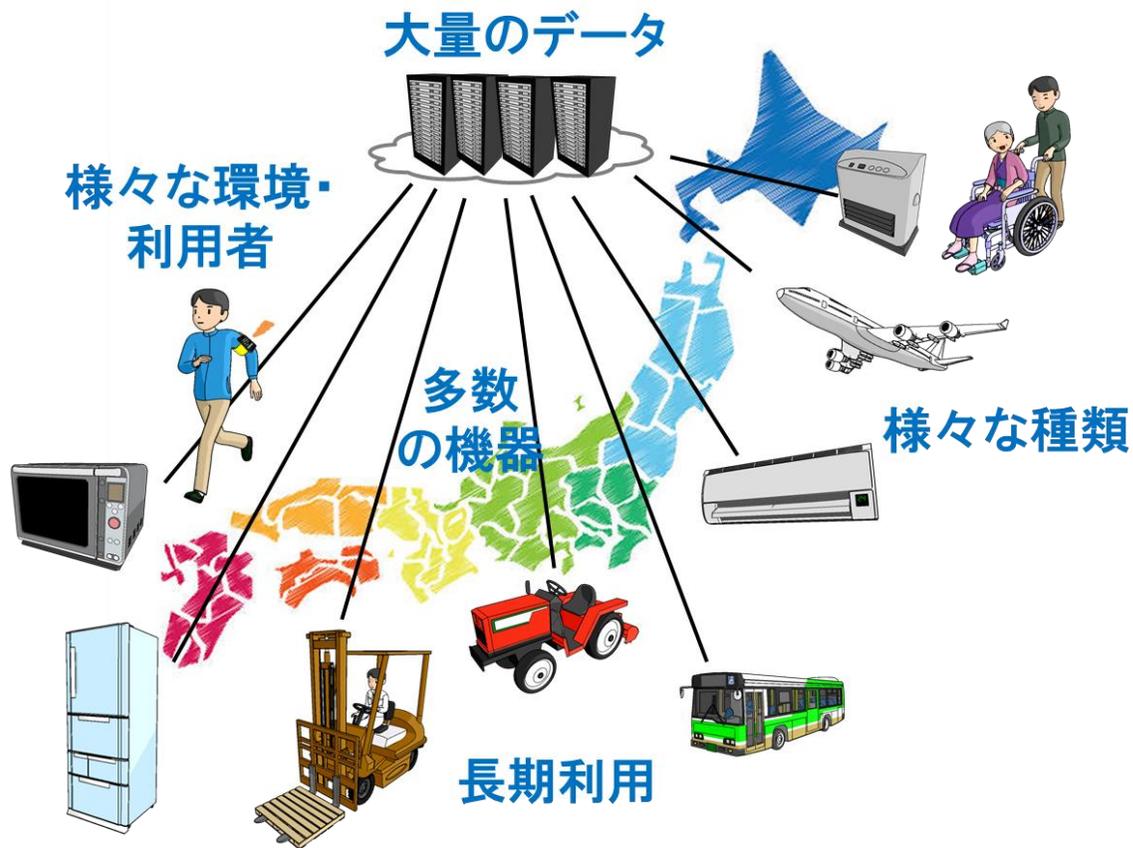
接続される機器の種類や個数が膨大で、システムが日々刻々と変化

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



- 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
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

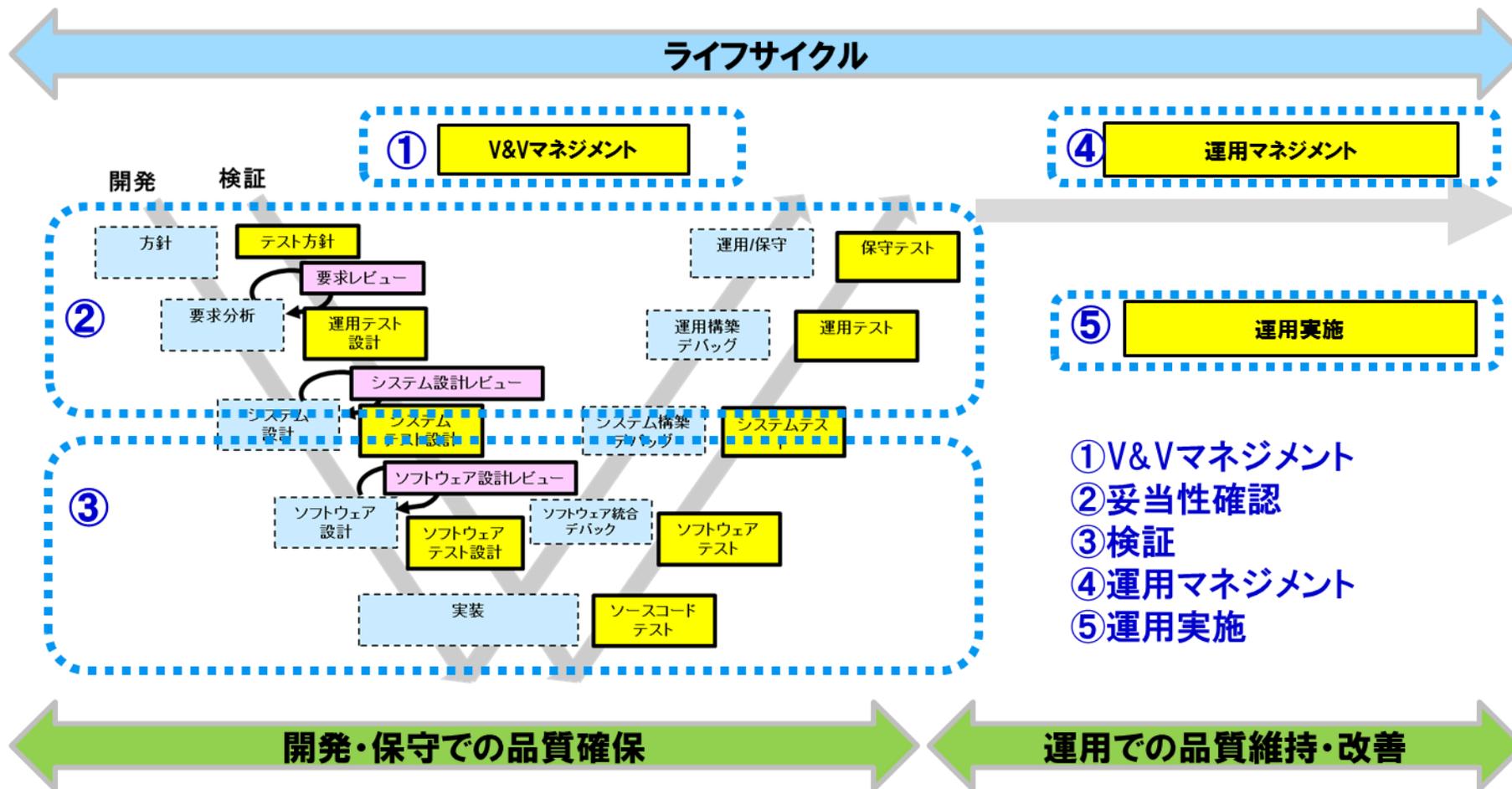
※V&V: Verification and Validation (検証と評価)

- テストやセキュリティの専門分野、産業界などから有識者を招集し、検討WGを設置(活動期間:2017年7月~2018年3月)

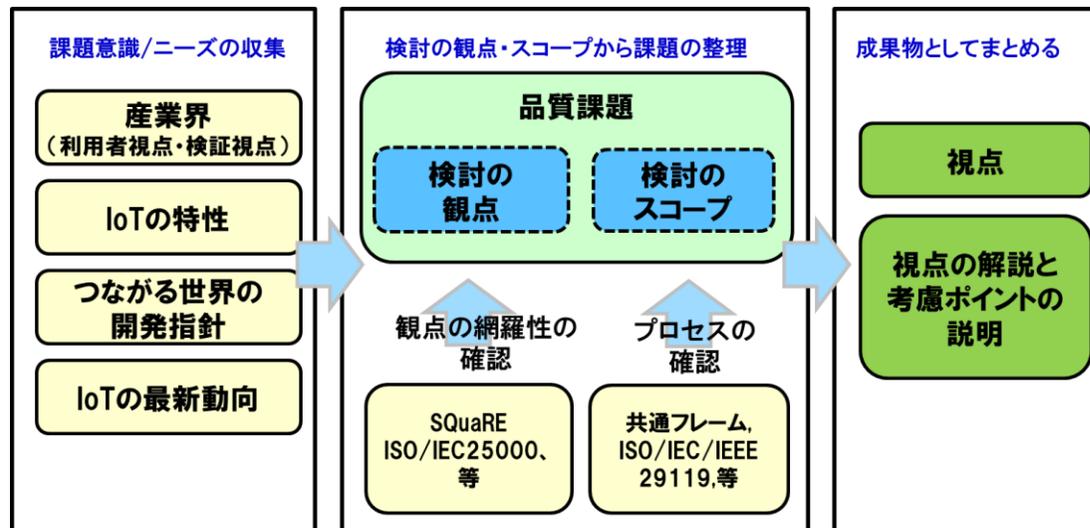
＜つながる世界の品質指針検討WG委員＞

	役割	氏名	所属
1	主査	森崎 修司	国立大学法人名古屋大学
2	委員	石川 博一	一般社団法人エコーネットコンソーシアム
3	委員	伊藤 公祐	一般社団法人 重要生活機器連携セキュリティ協議会(CCDS)
4	委員	亀井 健一	株式会社アイ・オー・データ機器
5	委員	後藤 祥文	デンソーテクノ株式会社
6	委員	五味 弘	一般社団法人電子情報技術産業協会(JEITA)/沖電気工業株式会社
7	委員	中道 泰隆	一般社団法人コンピュータソフトウェア協会(CSAJ)/ JBアドバンス・テクノロジー株式会社
8	委員	林 祥一	一般社団法人 IT検証産業協会(IVIA)/富士ゼロックス株式会社
9	委員	深川 義裕	新世代M2Mコンソーシアム/アンリツエンジニアリング株式会社
10	委員	松並 勝	DNV GL ビジネス・アシュアランス・ジャパン株式会社
11	委員	吉府 研治	一般社団法人情報通信ネットワーク産業協会(CIAJ)/日本電気株式会社

■ 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の品質に係わる課題意識を約100件収集
- 5つの品質確保の場面(スコープ)と品質確保の観点(テスト計画、テスト抽出、テスト環境、テスト実施など)の観点から品質課題を整理



課題1: IoTの品質の説明責任が果たせる体制整備や関係者との合意形成

課題2: 多種多様なIoTの要求や要件の妥当性の確認

課題3: つながることを意識したテスト項目の抽出とテスト計画

課題4: テストの組み合わせの爆発を抑えるテストの効率化

課題5: 変化が激しいIoTの運用での品質維持・改善の計画

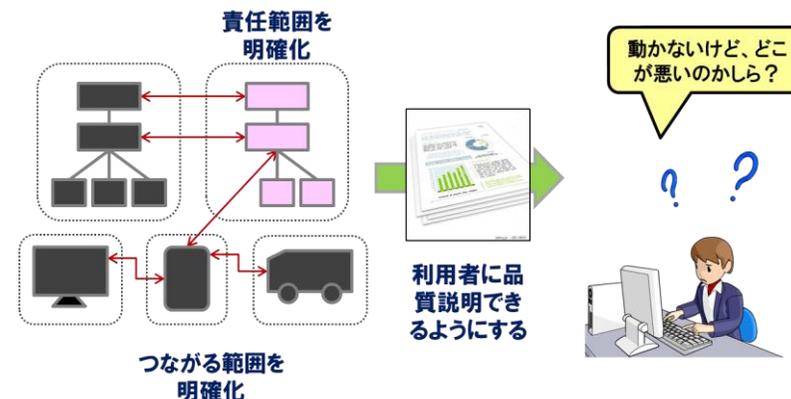
課題6: 長期にわたる利用での品質の維持・改善

■ 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

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

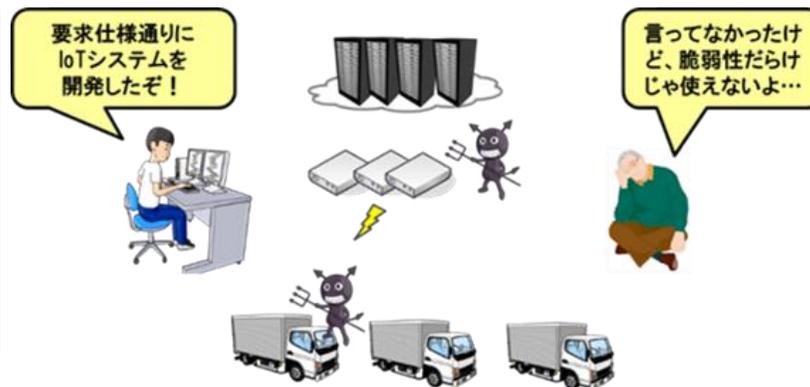
- ・依頼元や調達品の提供元などの関係者と合意を得るための仕組みを考慮

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

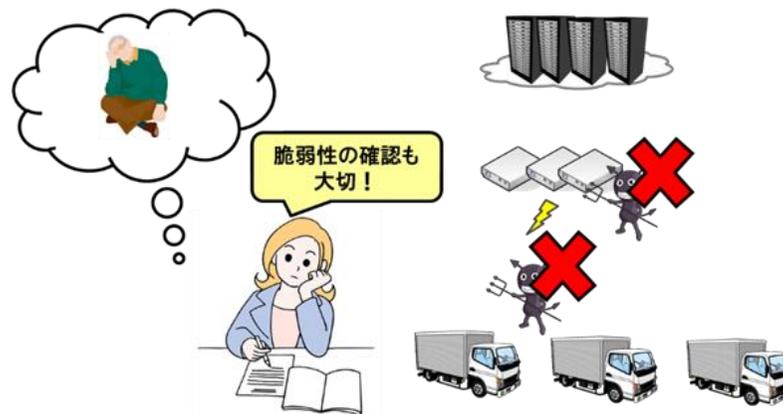
(注) 本書における定義：対象とする機器やシステムのセーフティ、セキュリティ、リライアビリティが確保されていること

妥当性確認（要求仕様に対する実装の確認）

【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

概要

- 開発要件が確実に実装されていることを利用者視点で評価
 - ・ 脆弱性対策などの暗黙的な要求も対象
- IoTのライフサイクルにわたる安全安心の確認と利用者の継続的利用における満足が得られることを確認する必要がある



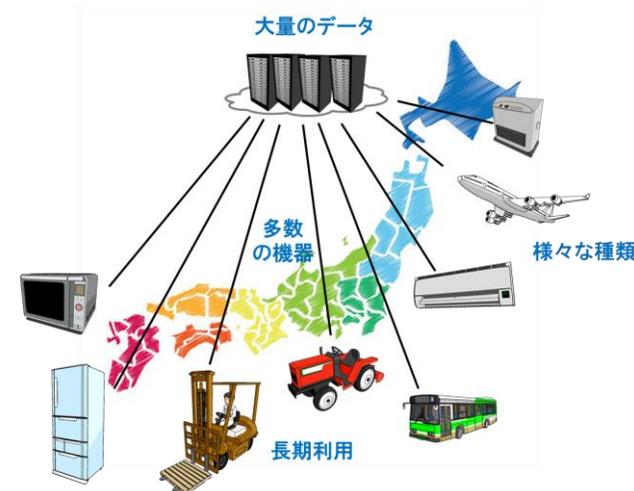
考慮ポイント

【3-1】 IoTの機能が要求を満足できるレベルで実装できていることを評価する

- ・ 利用者の想定、使われるシーン、実際の利用場面を想定してシナリオを作成
- ・ 評価環境の構築に必要なツールの準備と、ツールを使いこなす評価要員の確保
- ・ 評価を実施し、評価結果の判断が正しいことを関係者と合意

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5】 多種多様な利用環境や使い方に着目する

概要

- 利用者のスキルレベルの想定が難しい
 - 移動する機器は利用シーンによって評価結果が異なる
- ⇒ 様々な利用者や利用環境を想定したテスト設計が必要



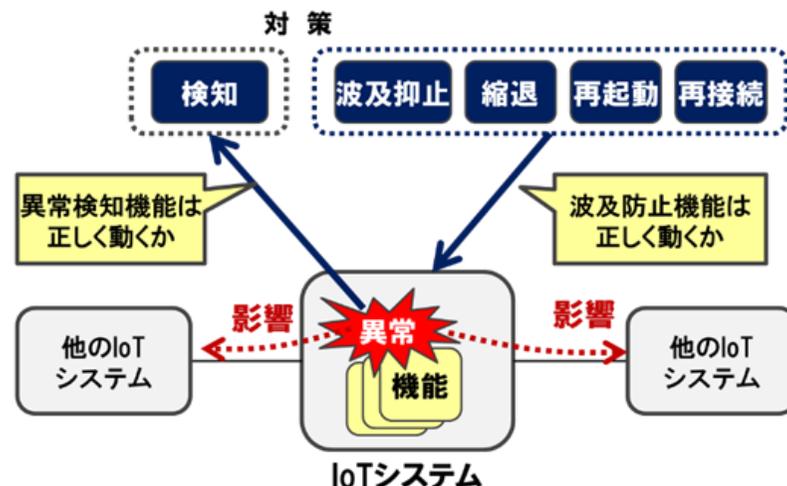
考慮ポイント

【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

- ・ 利用者の特性：年齢、性別、身体特性、言語、習慣の違い
- ・ 利用場所：国内/海外、離島、寒冷地、高地
- ・ 利用シーン：朝/夕、順光/逆光、晴/雨/雪
- ・ 利用者のスキル：システム管理レベル/利用者レベル
- ・ 利用者の役割：一般利用者、企業利用者、運用者

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

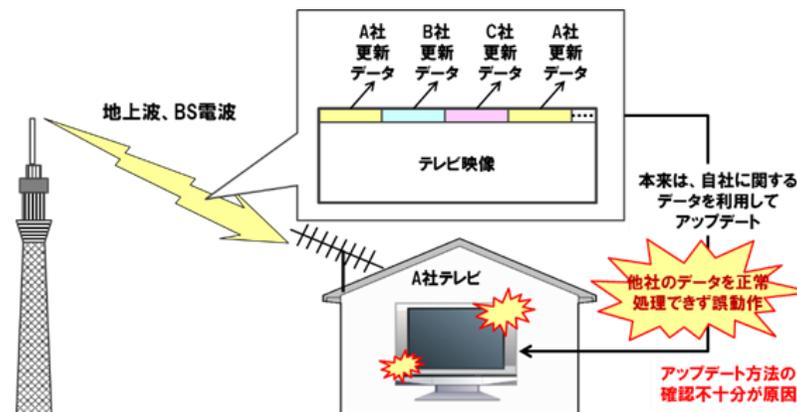
【6-2】 つながることによるセキュリティの脅威やそれがセーフティに及ぼす影響を考慮したテストを設計する

- 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

【視点7】 長期安定稼働の維持に着眼する

概要

- IoT機器・システムの中には長期間使用されるものがある
 - ⇒ 障害発生時の原因解析と、不具合を修正するアップデート機能などの確認が必要
 - ⇒ 一方で、アップデート自身の確認不足により、広範囲に影響を与える場合があることにも考慮が必要（右図）



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）

概要

- 視点4から視点7のテストを実施するためのテスト環境やテスト効率化について、テスト設計段階から考慮することが必要



考慮ポイント

【8-1】 多数の機器の接続や、大量のデータを想定したテスト環境を検討する

- 設計範囲内および範囲外の機器接続（接続数、機器の種類、ネットワークの種類）
- 設計範囲内および範囲外のデータ（データ数、種類）
- 障害/故障発生時のテスト（ハードウェア、ソフトウェア、ネットワーク）
- セキュリティ上の異常発生に関するテスト
- その他（加速度テスト環境、等）

【8-2】 効率的なテスト方法を検討する

- テスト爆発の抑制：直交表、オールペア法、HAYST法、原因結果グラフ技法などの活用
- テスト類似項目の整理：同値分割、統合可能なテストの整理
- テスト工数削減：テストデータやテストプログラムの自動生成、テスト実行の自動化
- 回帰テストの容易化：効率的な回帰テスト実行の構成やツール検討

【視点9】 テストのし易さと実施可能性を検討する

概要

- 開発担当者が設計した内容では効率的にテストできない場合やテスト困難な場合がある
- ⇒ 開発側への仕様変更の提案を検討することが重要



考慮ポイント

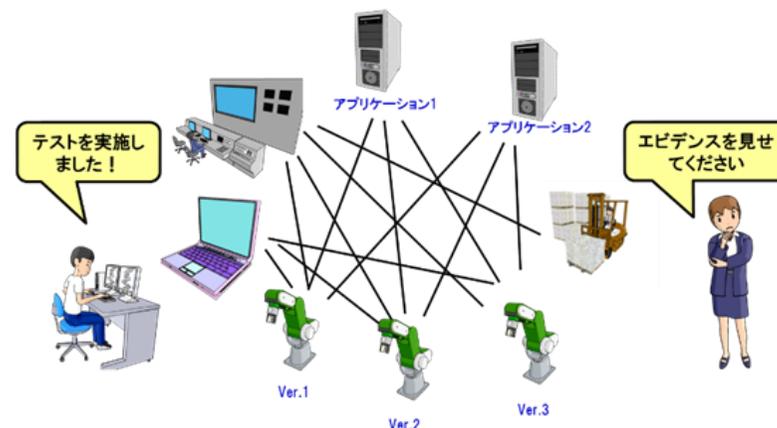
【9-1】 テストし易さ、テスト実行性を満たすための対策を開発へ反映させる

- テスト容易化設計^(注)の提案
 - ✓ 制御や監視に関するインタフェースの統一・集約
 - ✓ アーキテクチャのモジュール化
 - ✓ テストに必要な機能の組込み（疑似障害発生、等）
- テストが困難である場合の提案
 - ✓ 環境が用意できず代替手段もない場合は、設計内容の見直しを提案
 - ✓ AIやビッグデータなどテスト手法が技術的に確立できていない場合は、保証範囲の見直しを提案

(注) DFT : Design for Test/Testing/Testability

概要

- テストの項目を1から順番通りに実施すると効率的でない場合がある
 - ⇒ 手配できた環境や要員に合わせてテストの実行順序や組み合わせを検討して効率化
- 機器・システムの障害発生時に問題ないか説明を求められることがある
 - ⇒ テスト結果のエビデンスを残す



考慮ポイント

【10-1】 テスト環境に着目し、テストの実行順序や組み合わせを考慮したテストを実施する

- テスト環境の準備状況に合わせてテスト実行順序を考慮
- 同じ機器やシステムの組み合わせによるテストをまとめて実行

【10-2】 合否判定結果だけでなく、判定理由を含めてエビデンスとして残す

- リリース後のトラブル発生時に品質の説明責任を果たすための準備が重要
- テスト結果と合否判定の根拠となった情報を含めてエビデンスとして残す

概要

- リリース前には想定していないIoT機器のつながり、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

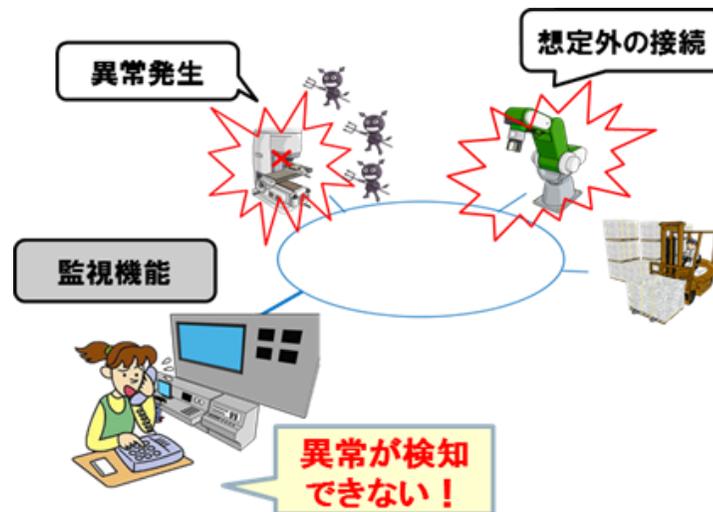
運用実施（長期利用での品質維持）

【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

IPA

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た。何が起きているかの把握が遅れ、復旧までに6時間を要し40～70万人に影響が出た
- ⇒ 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に動作していることの確認が重要



(注) https://www.jpccert.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

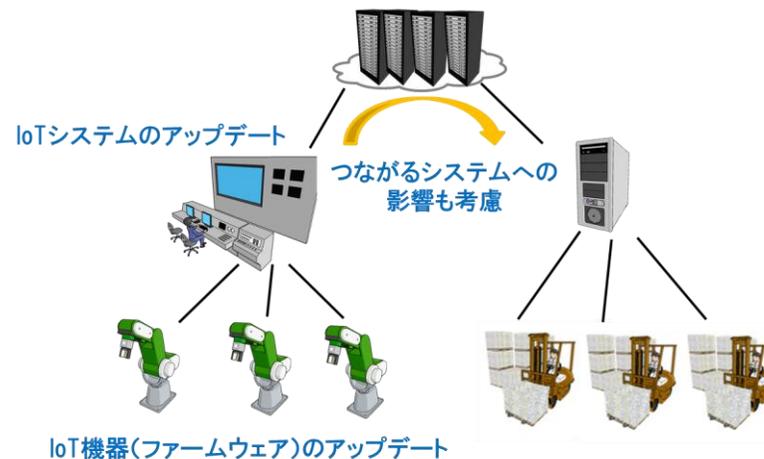
- 利用環境の変化の把握（想定外の利用者、機器の故障やセキュリティの異常、等）
- 技術方法の変化の把握（脆弱性情報、OSSなどの更新情報、法規制の変化、等）

【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）

概要

- 運用開始後も仕様変更や機能追加に対応するためのアップデートが繰り返されるケースが想定される
- ⇒ 自システムへの影響のみならず、つながる相手への影響の有無に関して十分な事前確認が必要



考慮ポイント

【13-1】 ソフトウェアの更新時は接続相手の性能などに影響を与えない適用手順であることを確認する

- 接続相手への影響確認（通信プロトコル変更、性能差の拡大による影響、等）
- 多数台つながっている場合の影響確認（通信路の帯域性能を考慮した更新タイミング、等）
- アップデート失敗への考慮（リカバリー手順の確認、等）
- 運用手順の訓練（障害発生や更新時の手順を定期的に確認、変化に対応した手順の見直し、等）

つながる世界の品質確保チェックリスト

- 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わ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	同一機種の種類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？				

➤ 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の品質確認
- PoC(Proof of Concept:概念実証)の要件の確認
- 試作開発品から量産開発品に移行する時の品質確認
- 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
- 障害発生時の原因分析と対策後の品質確認

➤ IoT製品・システムの発注確認に適用

- 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

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。