

IoTのリスクの認識と安全・安心の 実現に向けた対策

～IoT機器・システムの開発と品質確保の重要ポイントを紹介～

ET/IoT総合技術展2018 IPAセミナー
2018年11月16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の国の政策・方針（Connected Industriesの話）
- IoTは便利になるけど、リスクもあるよね！
- では、IoTの開発は、何をどう考えたらいいの？
 - 安全・安心なIoT開発の最低限のポイントを抑えよう！
- 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！

Connected Industries

～我が国産業が目指す姿(コンセプト)～

従来 事業所・工場、技術・技能等の電子データ化は進んでいるが、それぞれバラバラに管理され、連携していない

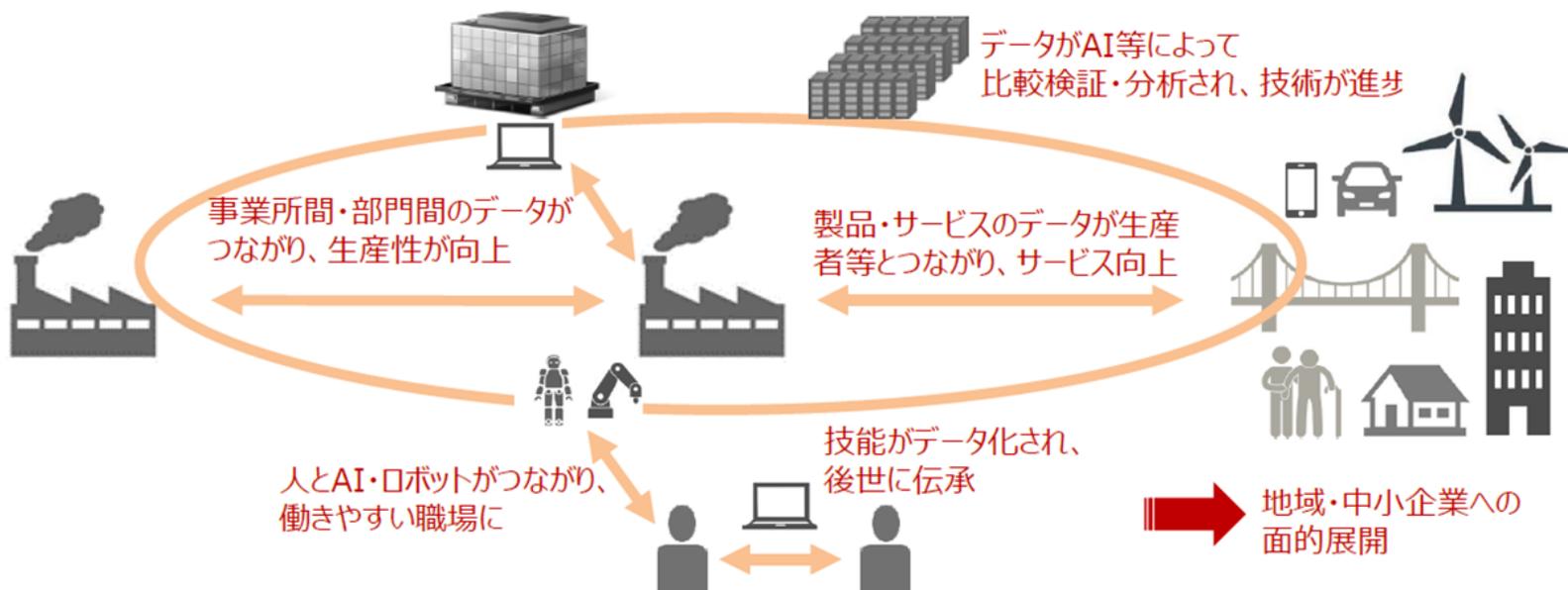
**産学官における
議論喚起・検討**

モビリティ、ものづくり、バイオ・素材、プラント保安、スマートライフなど分野別の取組

データ利活用、標準化、IT人材、サイバーセキュリティ、AI開発など横断的な取組

将来 データがつながり、有効活用されることにより、技術革新、生産性向上、技能伝承などを通じた課題解決へ

「Connected Industries」は、Made in Japan、産業用ロボット、カイゼン等続く、日本の新たな強みに



出典：METI「Connected Industries」東京イニシアティブ2017 平成29年10月2日

「Connected Industries」5つの重点取組分野

「自動走行・モビリティサービス」

- データ協調の在り方を早急に整理
- AI開発・人材育成の強化
- 物流等も含むモビリティサービスやEV化の将来像を見据えた取組



「ものづくり・ロボティクス」

- データ形式等の国際標準化
- サイバーセキュリティ・人材育成等の協調領域での企業間連携の強化
- 中小企業向けのIoTツール等の基盤整備



「バイオ・素材」

- 協調領域におけるデータ連携の実現
- 実用化に向けたAI技術プラットフォームの構築
- 社会的受容性の確保



「プラント・インフラ保安」

- IoTを活用した自主保安技術の向上
- 企業間のデータ協調に向けたガイドライン等の整備
- さらなる規制制度改革の推進



「スマートライフ」

- ニーズの掘り起こし、サービスの具体化
- 企業間アライアンスによるデータ連携
- データの利活用に係るルール整備



地域・中小企業の「Connected Industries」 取組み事例

- IoT、ロボット等の導入で生産性を向上させたり、単純作業や重労働を省力化し、労務費を削減。テレワークともあいまって、若者、女性、高齢者が働きやすくなる。→ **人手不足解消、働き方改革**
- 人工知能等によって「匠の技」を見える化し、若い職員のスキル習得を支援。→ **技能継承**
- 職人の技能や創造性をデータ化し、それを生産設備につなぐことで、多品種・単品・短納期加工を実現。新規顧客を獲得。→ **利益の拡大**
- 過疎地での高齢者の移動、遠隔地への荷物配送が可能に。歳をとってもクルマを安全に運転。将来的には、運転できない人も自動運転で目的地へ。→ **社会課題解決（安全運転・移動支援）**

事例1 旭鉄工

愛知県碧南市、自動車部品製造、従業員480名

- **カイゼン活動を加速するセンサーモニタリングシステム**を自社開発し、それを**生産設備につなぐこと**によって、部品製造プロセスの問題点を見える化。**生産性を短期で向上させ、労務費を大幅低減。**
- **単純作業を極力デジタル化**し、カイゼン活動の工夫といった人にしかできない仕事に従業員が取り組むことで、「**働き方改革**」も実現。

自社開発したモニタリングシステム

- ・低電力消費の無線技術により電気配線やLAN工事は不要。
- ・汎用のスマートフォン等で閲覧可能にすることで初期投資を抑制。



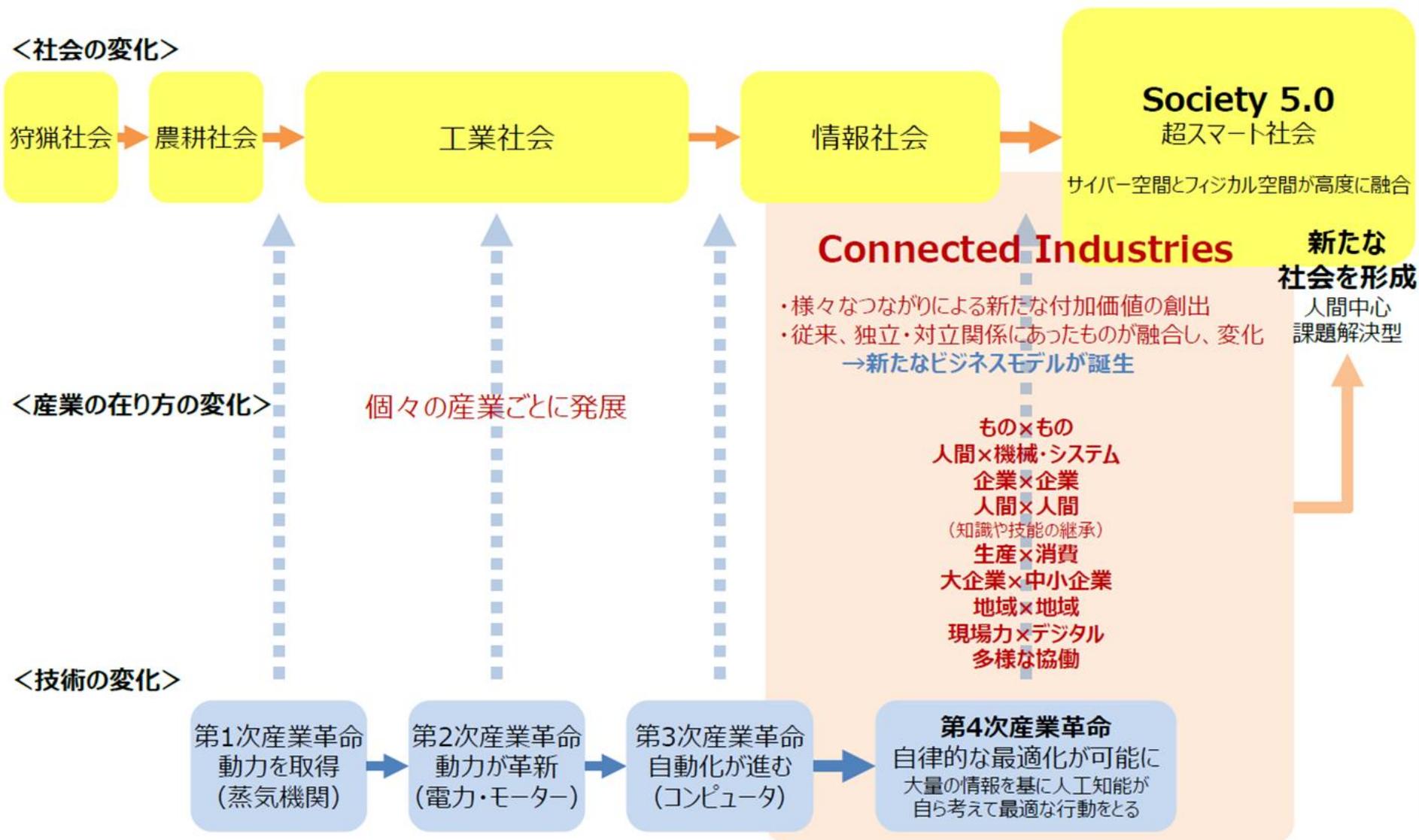
事例2 全国各地で実証実験を展開中

自動運転 福井県永平寺町、石川県輪島市（写真右上）、
沖縄県北谷町、茨城県日立市（写真右下）
ドローンによる荷物配送 福島県浜通り（写真左）



出典：METI「Connected Industries」東京イニシアティブ2017 平成29年10月2日

【参考】Society 5.0につながるConnected Industries

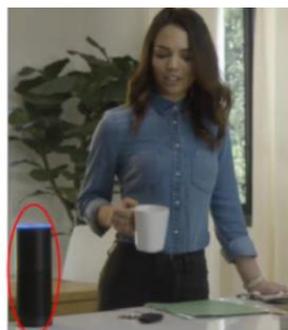


出典：METI「Connected Industries」東京イニシアティブ2017 平成29年10月2日

- IoTの国の政策・方針（Connected Industriesの話）
- **IoTは便利になるけど、リスクもあるよね！**
- では、IoTの開発は、何をどう考えたらいいの？
 - 安全・安心なIoT開発の最低限のポイントを抑えよう！
- 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」

つながる世界では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

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



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

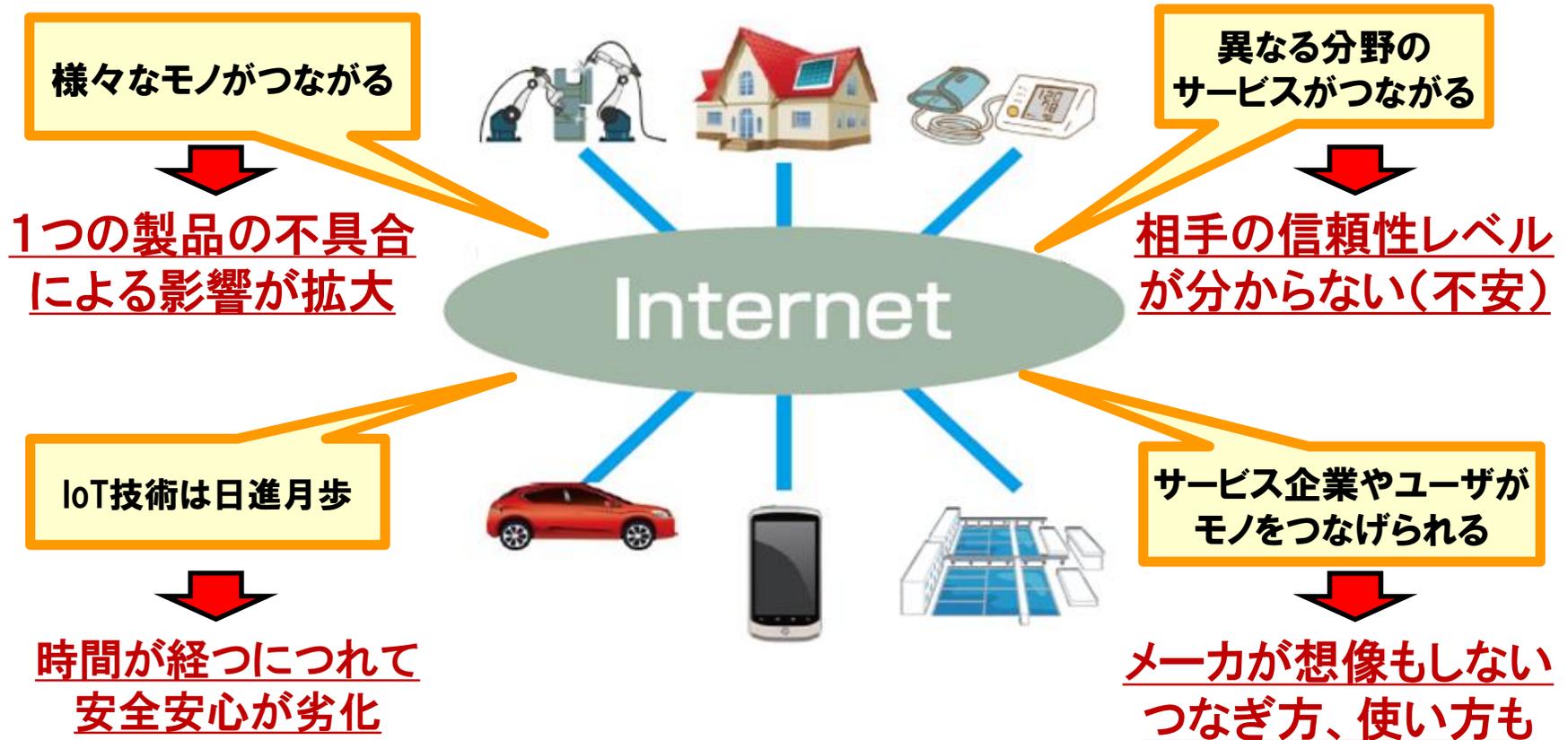


人命にも関わる事故が起こせることが証明され、自動車会社は**140万台にも及ぶリコール**を実施。

【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、製品供給者が想定しない、把握できない課題が発生



- IoTの国の政策・方針（Connected Industriesの話）
- IoTは便利になるけど、リスクもあるよね！
- **では、IoTの開発は、何をどう考えたらいいの？**
 - **安全・安心なIoT開発の最低限のポイントを抑えよう！**
- 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！

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

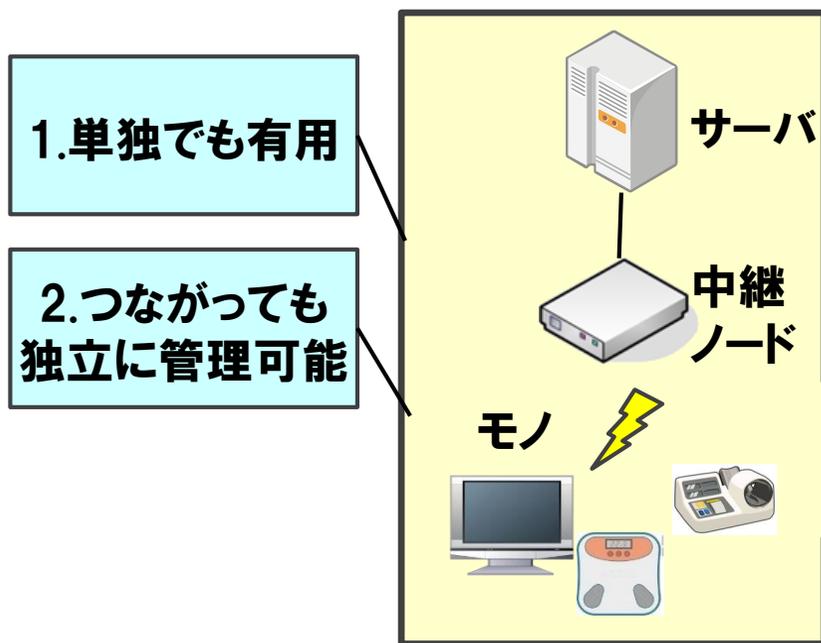
https://www.ipa.go.jp/sec/reports/20160511_2.html

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ほしいことを伝える
		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

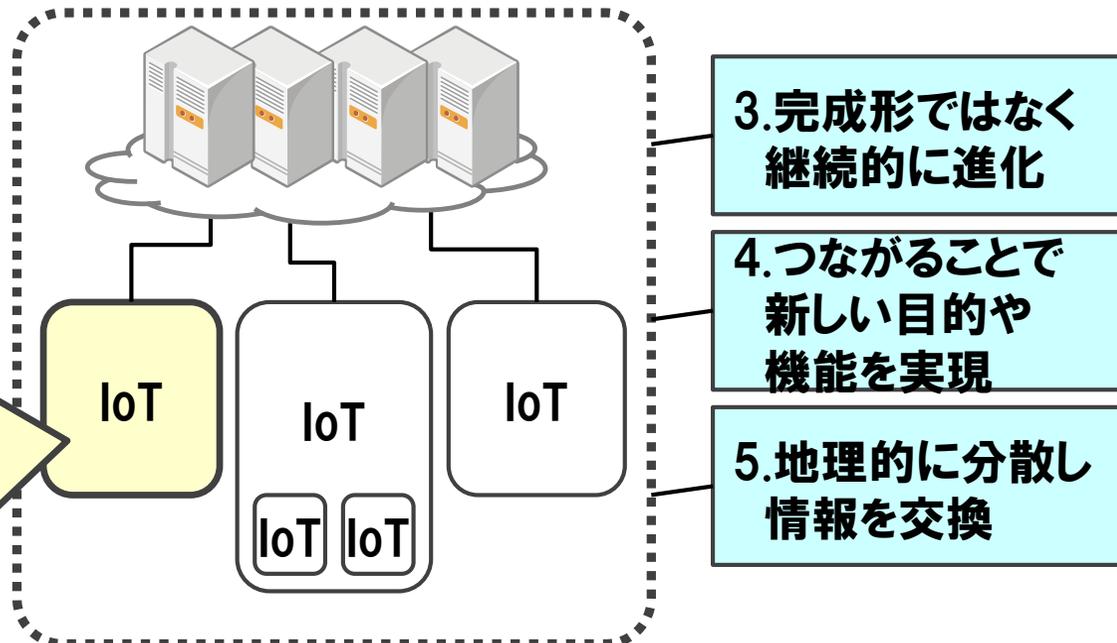
※IoTのネットワークに関する留意事項は、IoTセキュリティガイドラインを参照。
<http://www.meti.go.jp/press/2016/07/20160705002/20160705002.html>

- ◆ あらゆる「モノ」がネットワークにつながり、新しい価値を創生
- ◆ さらに、IoT同士がつながることで、新しい価値を創生

モノが繋がったIoT

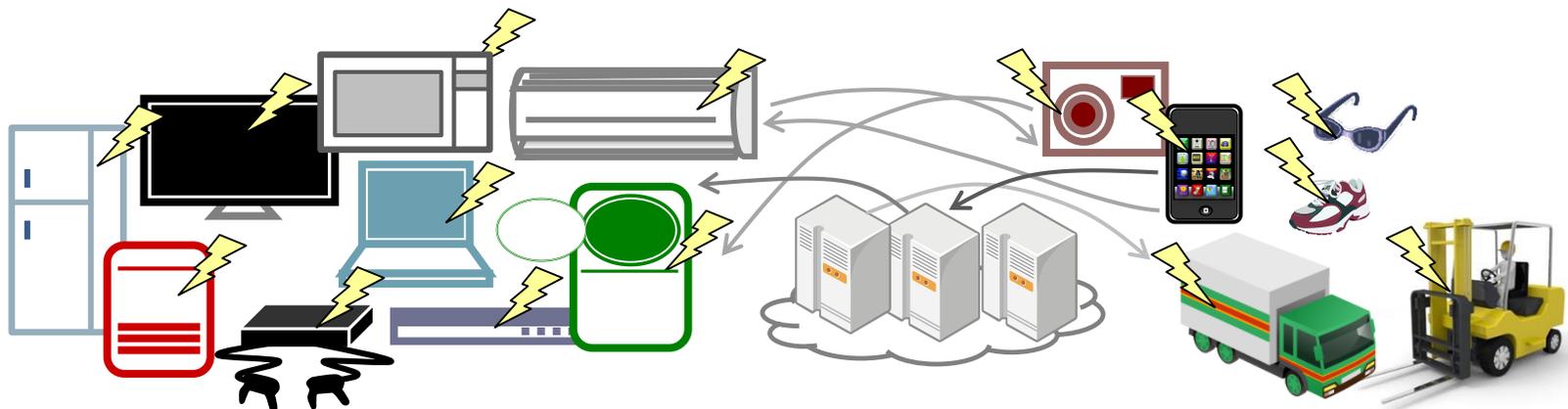


IoTが繋がったIoT (System of Systems)



IoTは、つながりにより拡大するリスクも発生！

◆ 想定しないつながりが発生する



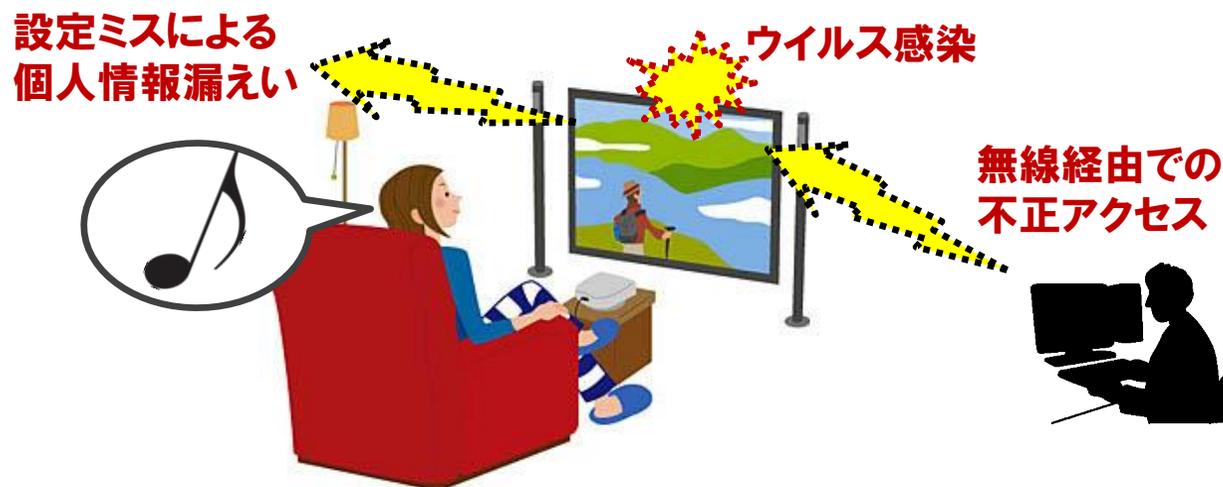
◆ 管理されていないモノもつながる



◆ 身体や財産への危害にもつながる、危害がつながりにより波及する



◆ 問題が発生してもユーザにはわかりにくい



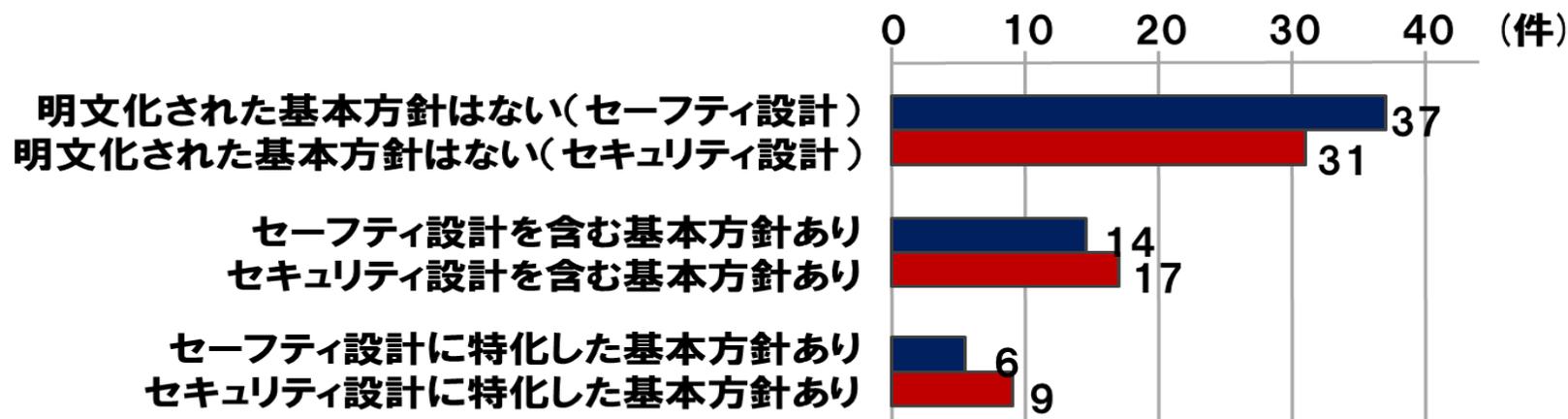
◆ 方針: つながる世界の安全安心に企業として取り組む

IoT時代の安全安心へのリスクは、経営問題となる可能性を認識し、企業の経営層に組織として取り組んでもらいたい事項をまとめた！

基本方針を策定する

体制・人材を見直す

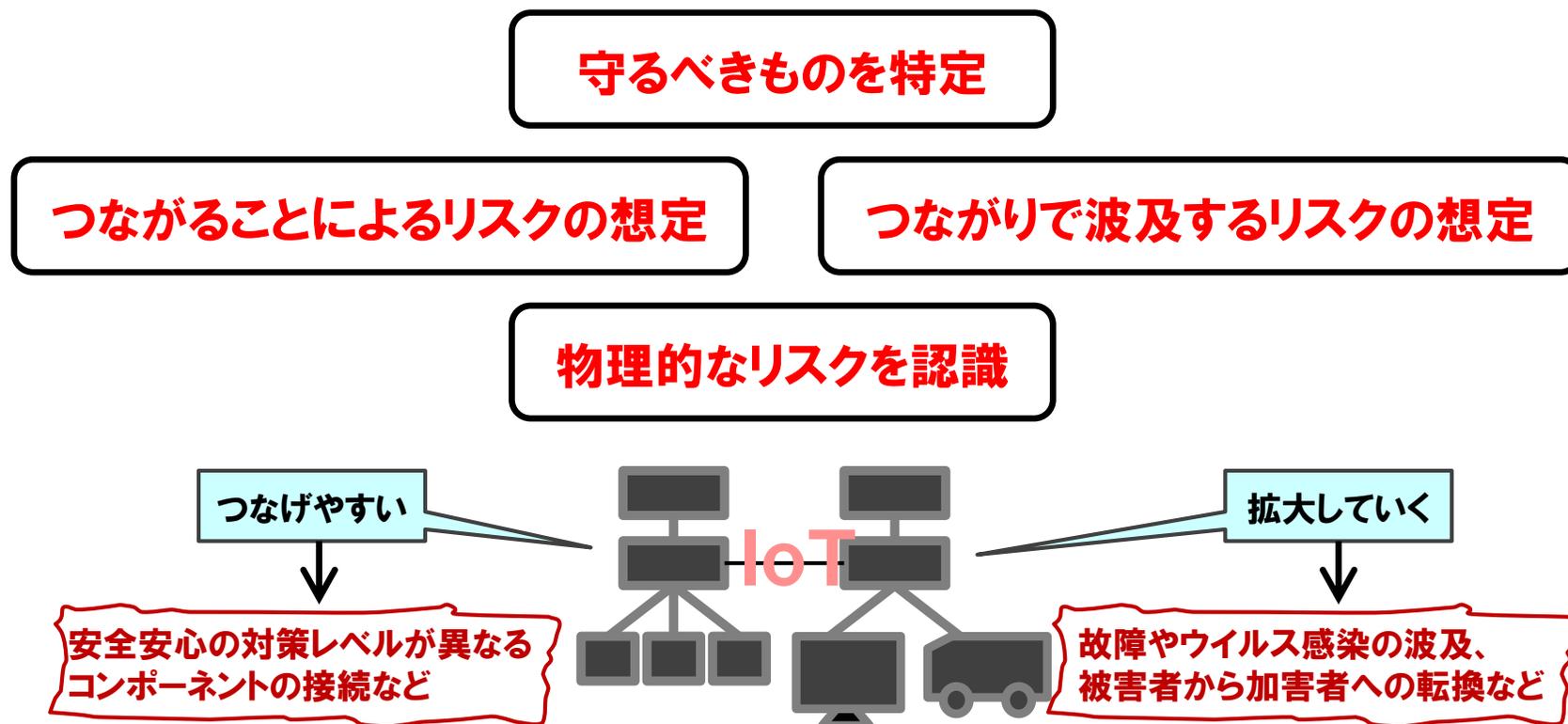
内部不正やミスに備える



出典:IPA セーフティ設計・セキュリティ設計に関する実態調査結果IPAアンケートより

◆ 分析: つながる世界のリスクを認識する

IoTの世界では、つながっていなかったモノがつながることで想定外の問題が発生することや障害が波及するリスクなどの検討が必要！



◆ 設計: 守るべきものを守る設計を考える

IoT機器にはリソースが小さいモノもあり、全体で守ることが重要。
また、障害の波及防止や接続相手の信用確認する仕組みも重要！

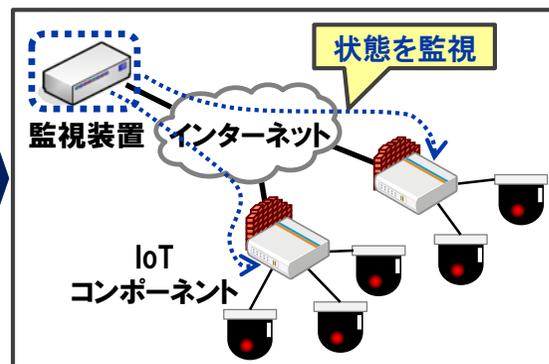
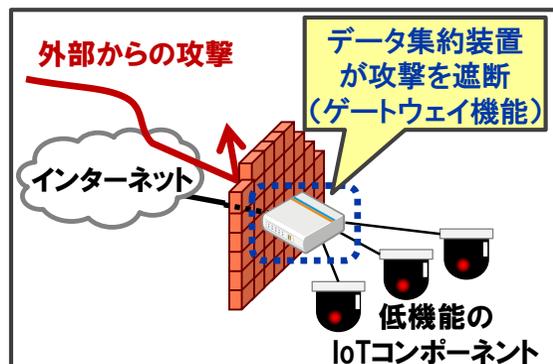
個々でも全体でも守る

つながる相手に迷惑を掛けない

不特定の相手とつながられても
安全安心を確保

安全安心の設計の整合を取る

安全安心の設計の検証・評価の実施

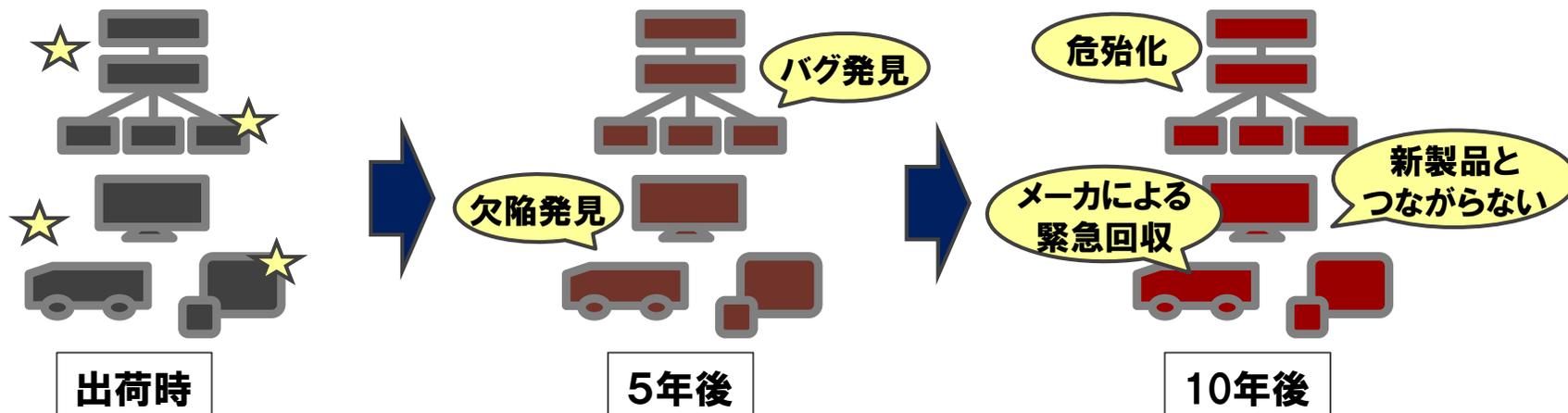


◆ 保守:市場に出た後も守る設計を考える

IoT機器には、10年以上も利用されるものも多く、故障やセキュリティ機能の劣化などの対策が必須。自分自身の状態を常に把握する機能や健全性を保つためにソフトウェアのアップデート機能は重要！

自身の状態を把握し記録する機能を設ける

時間が経っても安全安心を維持する機能を設ける



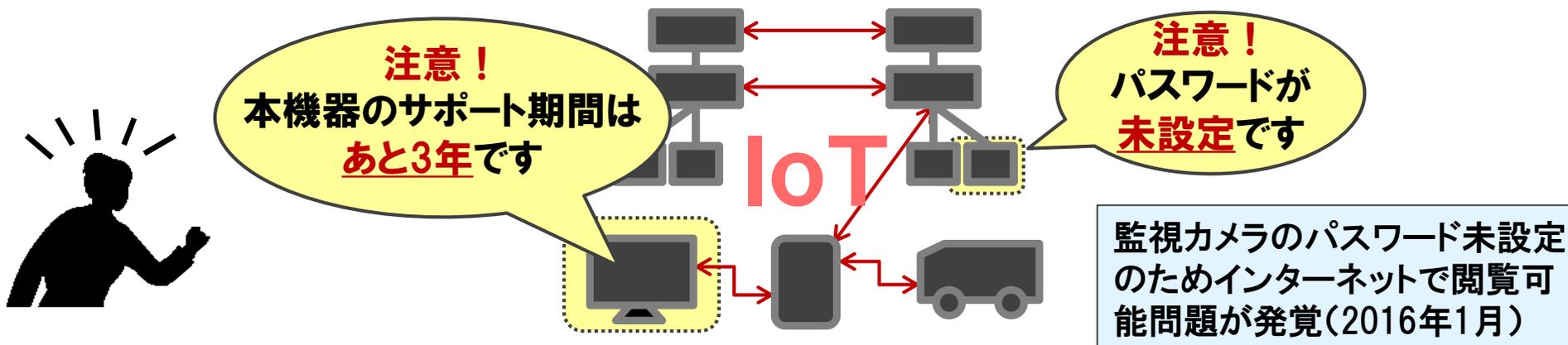
◆ 運用：関係者と一緒に守る

ログインパスワードの未設定問題やサポート期限切れ問題、廃棄時の個人情報・機密情報漏れ問題など運用に関わる懸念事項が多数あり、関係事業者との連携が重要！

出荷後もIoTリスクを把握し、情報発信する

関係事業者に守ってもらいたいこと伝える

一般利用者につながるリスクを伝える



■ 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

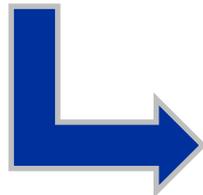
- 2017年5月8日公開:以下のURLからpdf版のダウンロード、書籍の購入

<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



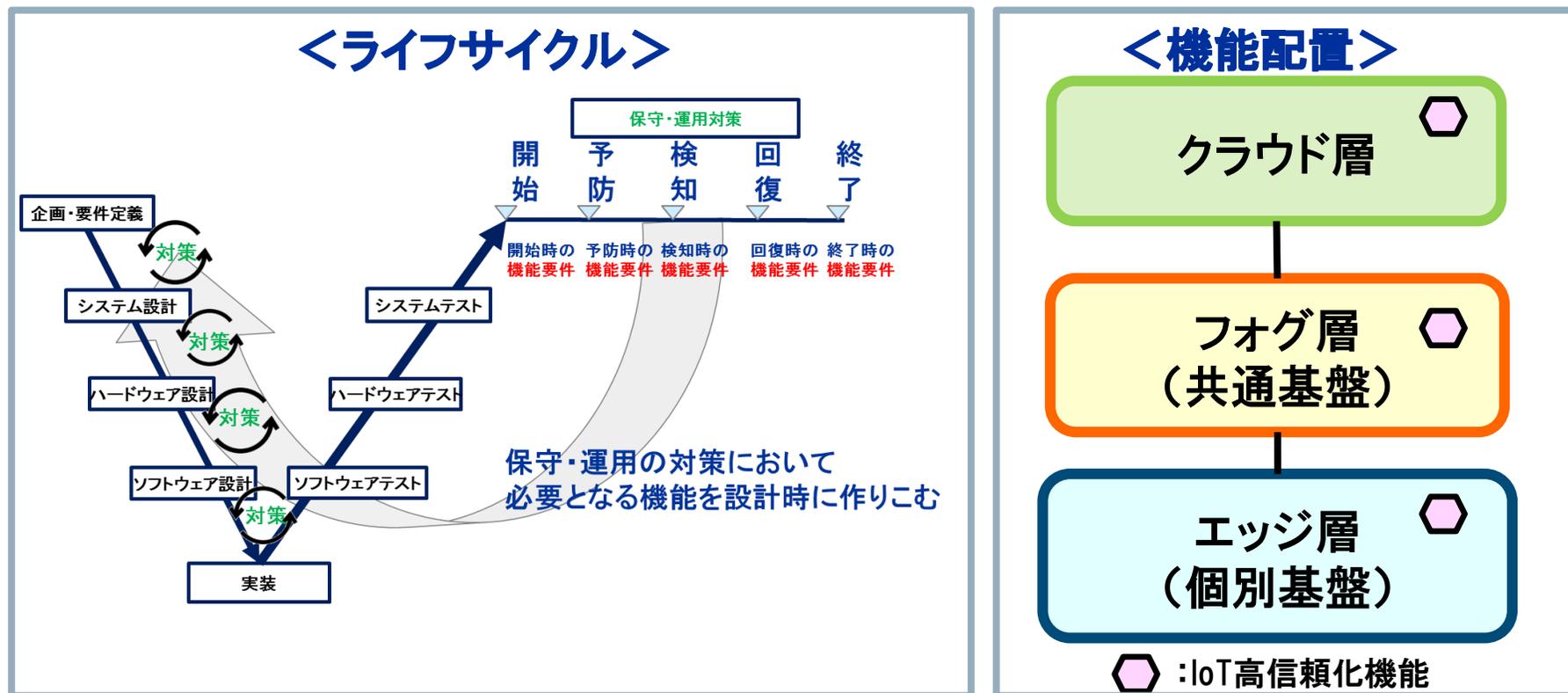
2017年5月

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

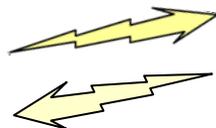
IoT高信頼化要件		IoT高信頼化のための12の機能要件	実装に向けた23の高信頼化機能
開始	導入時や利用開始時に安全安心が確認できる	1. 初期設定が適切に行われ、その確認ができる	初期設定機能、設定情報確認機能
		2. サービスを利用する時に許可されていることを確認できる	認証機能、アクセス制御機能
予防	稼働中の異常発生を未然に防止できる	3. 異常の予兆を把握できる	ログ収集機能、時刻同期機能、予兆機能、診断機能、ウイルス対策機能
		4. 守るべき機能・資産を保護できる	アクセス制御機能、ログ収集機能、時刻同期機能、ウイルス対策機能
		5. 異常発生に備えて事前に対処できる	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

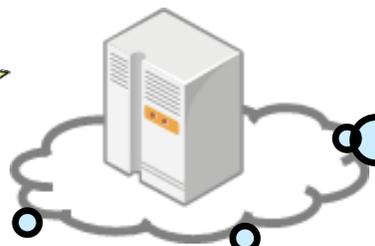
何か怪しい振る舞いだなあ～
乗っ取られた様だ！そのデバイスは
強制停止させよう！
⇒予兆機能、停止機能

(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？
個人情報消さないかね！
⇒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の国の政策・方針（Connected Industriesの話）
- IoTは便利になるけど、リスクもあるよね！
- では、IoTの開発は、何をどう考えたらいいの？
 - 安全・安心なIoT開発の最低限のポイントを抑えよう！
- **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！**

IoTの特徴

システムが日々変化！

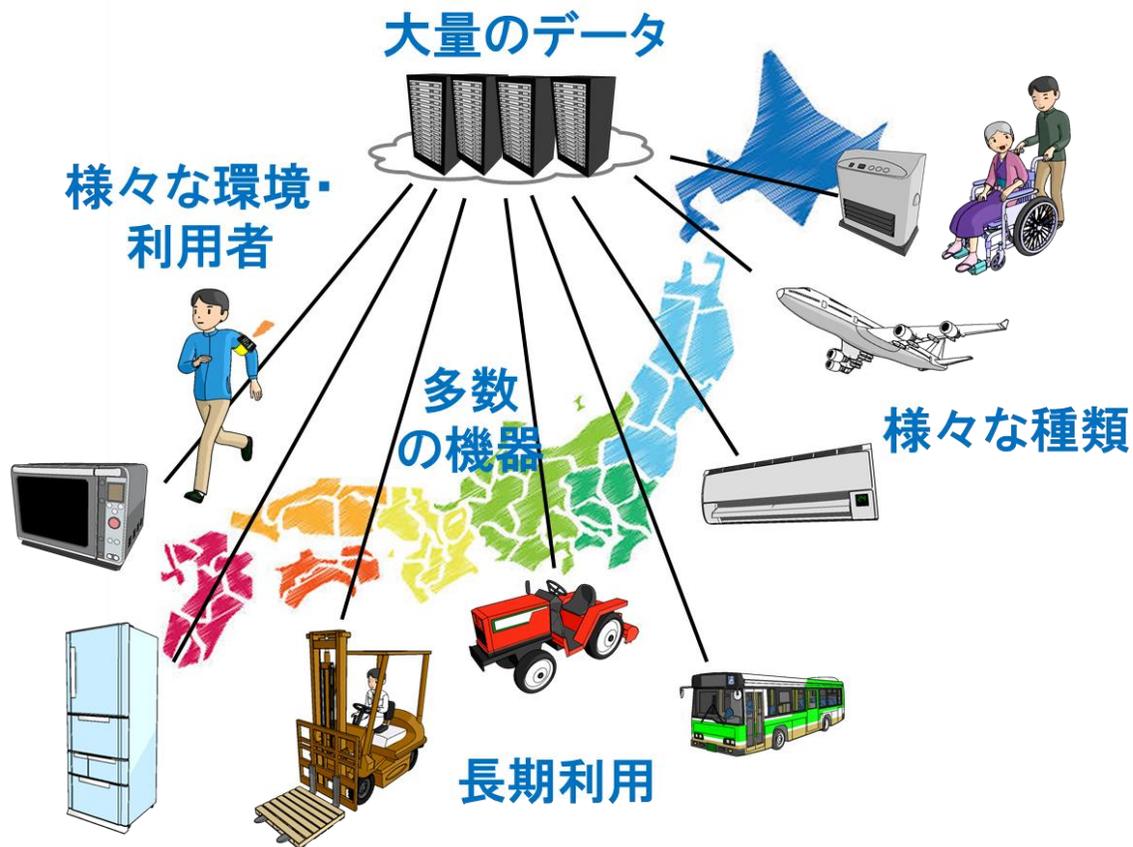
接続される機器の種類や個数が膨大で、システムが日々刻々と変化

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

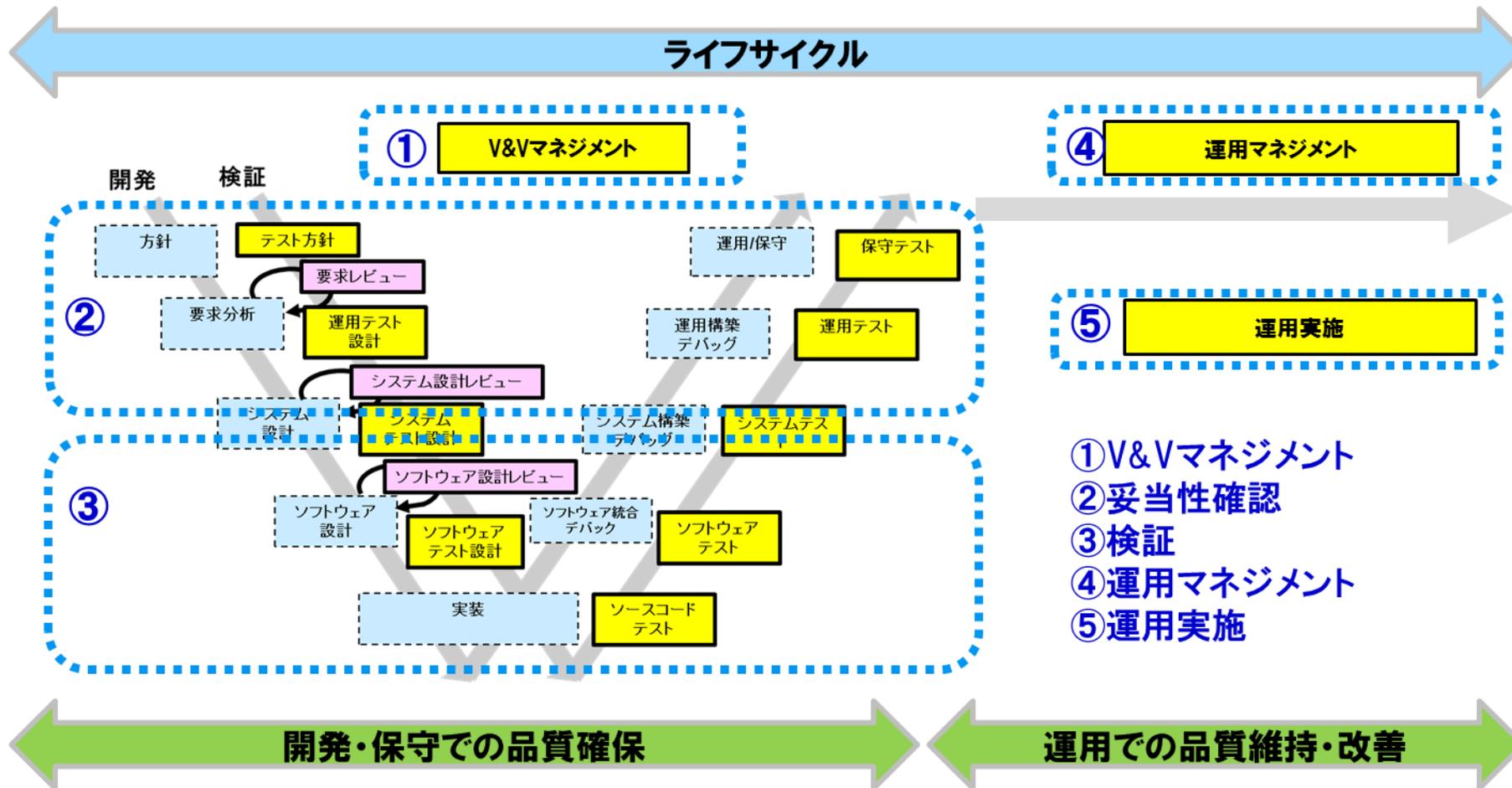
③開発・運用の現場で活用できる品質確保チェックリストを同時公開

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

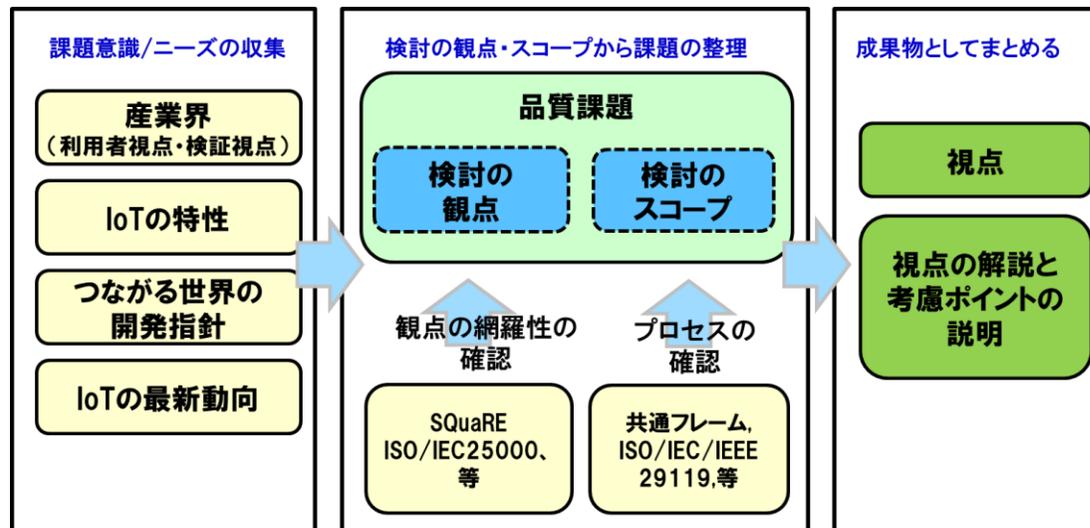
検証: 正しく作っているか

評価: 正しいものを作っているか(妥当性確認)

■ 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

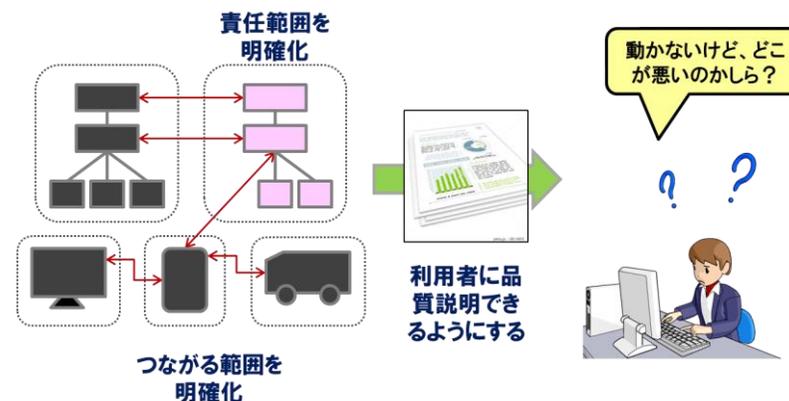
■ IoTの開発・保守から運用までライフサイクルで品質を確保、維持・改善

	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

【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

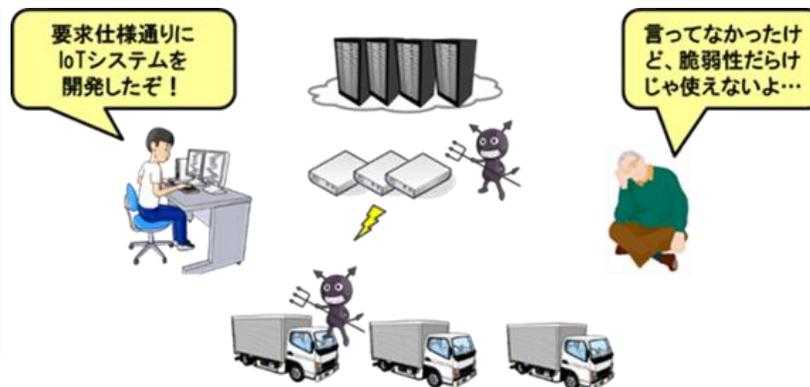
【1-4】検証・評価の範囲を明確化し、関係者間の合意を促す

- ・ 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

【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

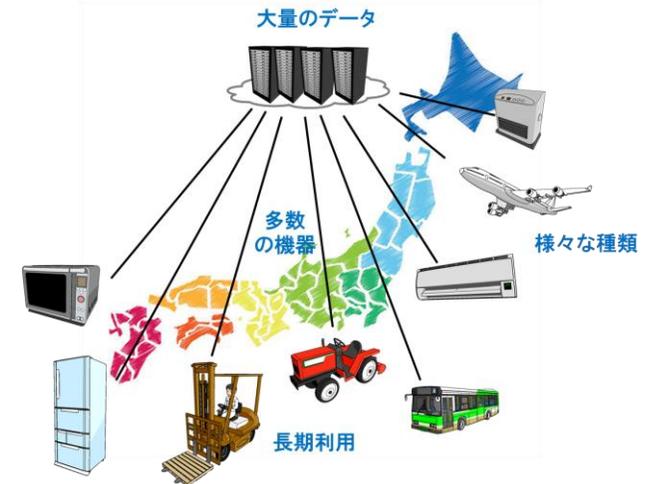
- ・ リリース後の不具合や脆弱性対策、システムの正常稼働を確認する機能などの要件を確認

(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

【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

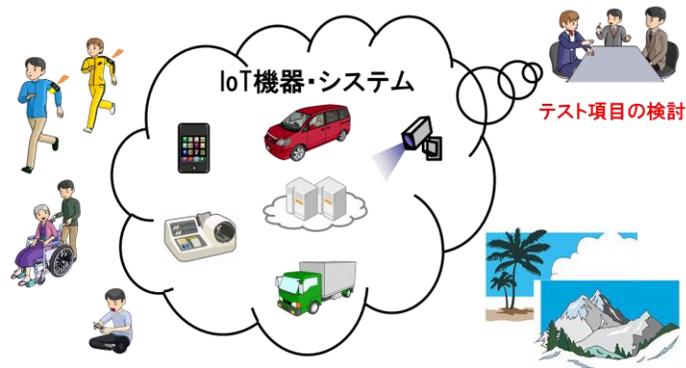
【4-2】 多種類の機器との接続やシステム連携を考慮したテストを設計する

- ・ 機能の互換性（同一機種の変化するバージョン、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

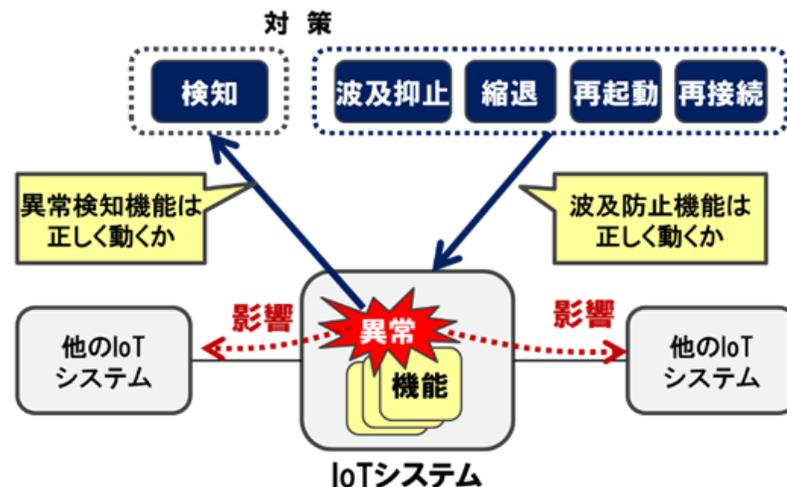
【5-1】 利用者、利用状況、利用環境などを考慮したテストを設計する

- 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

【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

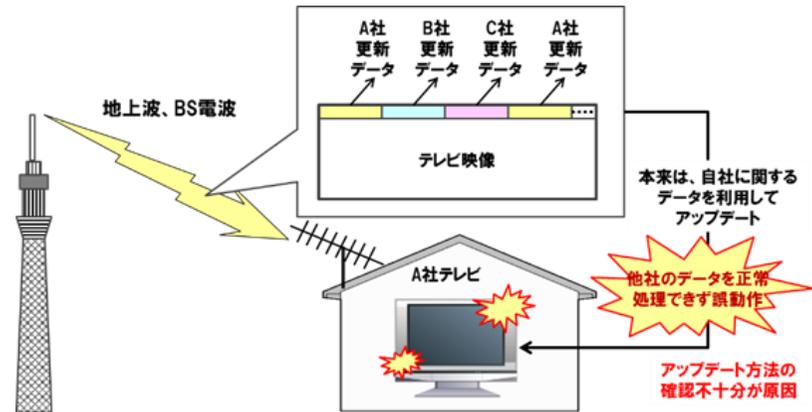
【6-2】 つながることによるセキュリティの脅威やそれがセーフティに及ぼす影響を考慮したテストを設計する

- ・ 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

【視点7】 長期安定稼働の維持に着目する

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）

【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）

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、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。

【参考】中小規模向けIoTの品質確認チェックリストIPA

◆従来、144項目あった確認項目が、24項目に集約！（2018年11月公開予定）

IPA

中小規模向けIoTの品質確認

- 自己診断チェックリスト -

独立行政法人情報処理推進機構
社会基盤センター

IoTの特徴を捉えた品質確認の
ポイントが簡単にわかります！！

IoTの特徴

- 様々なモノやシステムがつながる
- 接続される機器の種類や個数など、システムが柔軟に変化する
- 様々な利用者が様々な利用環境で使う
- 自動車・家電製品・工場のシステムなど長期に利用される

自己診断チェックリスト			
	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制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化して、リスクとコストを算定しながら、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、テストの合格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)	メーカー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？	
テストの実施	(13)	つながることによるセキュリティの脅威やそれがセキュリ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？	
	(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？	
運用計画	(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)	合格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？	
運用実施	(20)	運用中に起こり得るシステムの機能や性能を変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？	
	(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？	

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に提案し、正式プロジェクト発足(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。