SEC BOOKS

IPA Better Life with IT

# 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～

独立行政法人情報処理推進機構（IPA） 技術本部 ソフトウェア高信頼化センター（SEC）

# はじめに

IoT(Internet of Things)は、今や各産業界で生産性向上やビジネス革新などに、なくてはならない状況になりつつある。また、産業界を連携したIoTの新しいビジネスも生まれつつあり、IoTは本格的な活用の時代に入ったと考えられる。一方、IoTは、今までつながらなかったモノが様々な形態でつながり、IoT機器メーカやシステム開発企業が想定もしていない利用環境で使われることにより、安全安心を脅かす様々な事故や責任問題などの発生が懸念される。このため、IoTの開発においては、IoTの品質の確保に関して産業分野を横断した共通的な品質課題の認識と考慮すべき品質視点などが求められている。

このような状況の中で、IoT機器・システムの開発は、品質の説明責任、開発期間短縮、開発コスト削減に対する要求が一層厳しくなっている。IoT機器・システム開発は、設計や実装の効率化だけでなく、検証や評価も適切で効率的でなければ、開発コストが大きくなりコスト競争力が低下したり、利用者が期待する品質を確保できないことが懸念される。

こうした傾向に加えて、IoT機器・システムの検証や評価においては、多様な接続相手・セキュリティへの考慮や対策、長期利用を前提としライフサイクルを見通した考慮や対策を踏まえた品質確保の取組みが必要になる。具体的には、開発時に想定できなかったIoT機器・システムとの接続、ネットワークを介した攻撃への考慮や対策、ライフサイクルが異なる機器やシステム同士の接続、保守・運用中の維持・改善の継続といった点を踏まえ、適切な検証や評価によって品質を確保しなければならない。例えば、検証や評価が不十分なままでリリースすると、つながることによる思わぬ事故が発生し大きな社会問題となることでビジネスへのダメージが懸念される。

本書では、IoT機器・システムの品質をライフサイクルにわたり確保・維持するために、特に注意が必要となる部分を品質の視点・考慮ポイントとしてまとめた。本書を活用することにより、開発や品質保証に携わる関係者の理解を深め、関係者が品質確保の意識を持つことで検証や評価活動をスムーズに進める一助となることを目的としている。

# 【本書での扱い】

## (1) 用語定義

本書における用語の定義について以下に示す。なお、以下に特に明記していないものは、基本的に「つながる世界の開発指針」［1］に準ずるものとする。

表 1 本書における用語定義

| 用語 | 定義 | 備考 |
|---|---|---|
| 安全安心 | 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 | つながる世界の開発指針 |
| IoT<br>(Internet of Things) | 人々、システム、情報資源とインテリジェントなサービスとのインフラストラクチャであり、物理的および仮想的な世界の情報を処理し、それに反応することを可能にする | ISO/IEC DIS 20924 |
| IoT 機器<br>(IoT Device) | 以下の要素の単一または組み合わせであるコンポーネント:<br>- 物理エンティティに関する情報を提供するセンサー<br>- 物理エンティティを識別するために使用されるタグ<br>- 物理的実体の物理的状態を変更することができるアクチュエータ | 同上 |
| IoT システム<br>(IoT System) | センシング、作動、通信、および管理、ならびにアプリケーションおよびサービスをユーザに提供する機能から構成されるシステム | 同上 |
| テスト<br>(testing) | すべてのライフサイクルを通じて実施する静的、動的なプロセスにおいて、成果物が特定の要件を満足するかを判定し、目的に合致することを実証し、欠陥を見つけるため、ソフトウェアプロダクトや関連成果物に対し、計画、準備、評価をすること<br>(※評価には実行、報告を含む) | JSTQB ソフトウェアテスト標準用語集(JSTQB) [2] |
| テスト<br>(test) | 1 つ以上のテストケースのセット<br>(※本書において、「テスト」をこの意味で使用する場合には「テスト設計」や「テスト実施」のような用語で使用する) | 同上 |
| テストケース<br>(test case) | 入力値、実行事前条件、期待結果、そして、実行事後条件のセットで、特定のプログラムパスを用いることや特定の要件が満たされていることを検証することのような、特定の目的又はテスト条件のために開発されたもの | 同上 |
| テスト設計<br>(test design) | 概略的なテスト目的を具体的なテスト条件とテストケースに変換するプロセス | 同上 |

| 用語 | 定義 | 備考 |
|---|---|---|
| テスト実行<br>(test execution) | テスト対象のコンポーネントやシステムでテスト(test)を実行し、実行結果を出力するプロセス | 同上 |
| テスト実施 | テスト実行に加えてテストの準備や結果の確認を含む | 本書 |
| 妥当性確認<br>(validation) | 客観的証拠を提示することによって、特定の意図された用途又は適用に関する要求事項が満たされていることを確認すること | JIS Q9000:2015 |
| 検証<br>(verification) | 客観的証拠を提示することによって、規定要求事項が満たされていることを確認すること<br>(※下記の「検証・評価」という表現を繰り返す場合には、「検証」と略記することがある) | JIS Q9000:2015、本書 |
| 検証・評価 | 検証と妥当性確認<br>(※この対で利用する場合に限る) | 本書 |
| 欠陥(defect) | 意図された用途又は規定された用途に関する不適合 | JIS Q9000:2015 |
| 不具合 | 機器やシステムの状態が良くないこと | 本書 |
| 障害(fault) | 要求された機能を遂行する機能単位の能力の、縮退又は喪失を引き起こす、異常な状態 | JIS X 0014:1999 |
| 故障(failure) | 要求された機能を遂行する、機能単位の能力がなくなること | 同上 |

## (2) 略称一覧

本書で使用している略称の正式名称は以下のとおりである。

表 2 略称一覧

| 略語 | 名称 |
|---|---|
| AI | Artificial Intelligence |
| CCDS | Connected Consumer Device Security council |
| CPS | Cyber Physical System |
| CSAJ | Computer Software Association of Japan |
| DDoS | Distributed Denial of Service attack |
| DEOS | Dependability Engineering for Open Systems |
| DevOps | a clipped compound of "Development" and "Operations" |
| DFT | Design For Test/Testing/Testability |
| EDSA | Embedded Device Security Assurance |
| EoL | End of Life |
| GDPR | General Data Protection Regulation |
| GW | Gateway |
| ID | Identification |
| IEC | International Electrotechnical Commission |
| IEEE | The Institute of Electrical and Electronics Engineers, Inc. |

| 略語 | 名称 |
|---|---|
| IoT | Internet of Things |
| ISO | International Organization for Standardization |
| IVIA | IT Verification Industry Association |
| LED | Light Emitting Diode |
| JIS | Japanese Industrial Standards |
| JSTQB | Japan Software Testing Qualifications Board |
| LSI | Large Scale Integrated circuit |
| OSS | Open Source Software |
| OWASP | Open Web Application Security Project |
| PC | Personal Computer |
| PDCA | Plan-Do-Check-Act |
| RFID | Radio Frequency Identifier |
| PM2.5 | Particulate Matter 2.5 |
| SLA | Service Level Agreement |
| SoS | System of Systems |
| SQuaRE | Systems and software Quality Requirements and Evaluation |
| UC | Use Case |
| UI | User Interface |
| V&V | Verification and Validation |

# 目次

# 第1章
# 本書の背景と目的



本章では、様々な IoT 機器・システムがつながる世界において、品質確保の取組みが必要になっている背景や本書の目的、「つながる世界の開発指針」[1]に対する本書の位置付けについて説明する。

# 1.1 背景

今まで、IT 化があまり進んでいない農業や林業、水産業など第一次産業にも IoT の波が押し寄せており、第二次産業、第三次産業の分野とも連携が進みつつある。IoT は一つの産業内の連携にとどまらず、産業間を跨いで連携し、新しい価値を創生する時代が本格的に到来している。このような状況の中で、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で使われる。IoT は、SoS（System of Systems）と捉えることができ、日々、拡張し、変化していく特徴があり、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る。そのため、IoT の品質の確保が重要になるが、従来の延長線上では、解決できない様々な課題が存在する。特に、IoT の開発に経験が少ない分野や企業にとっては、何をどう考えれば品質を担保できるのか、手探りの状況であると考えられる。

IoT の品質の確保における代表的な課題としては、以下が想定される。

- 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
- 様々なモノがつながるときのセキュリティテストの考慮事項がわからない
- 様々なつながり方が想定され、テストの組み合わせが爆発する
- IoT の品質の説明責任が求められるが何をどうすれば良いかわからない
- IoT はライフサイクルが長く、かつ、システムや利用者が変化していくため、保守・運用でも品質を維持したいが考慮すべき事項がわからない

そこで、本書では、IoT が分野横断的に連携していくことを想定し、その品質を確保、維持改善するために考慮すべきポイントをまとめた。基本的な捉え方としては、IoT 機器・システム開発において、リリース前に品質を確保する考え方とリリース後の保守・運用で品質を維持・改善する考え方の 2 つでまとめた。

本書をまとめるにあたり、特に、IoT の特徴や性質に着目して、様々な分野の有識者の知見に基づく IoT の課題をベースに、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た。

# 1.2 IoT の特徴

## (1) 本書での IoT の捉え方

IoT とは ”Internet of Things”の略であり、1999 年に提唱した Kevin Ashton によればコンピュータが RFID やセンサーを用いて「モノ(Things)」から迅速かつ正確に情報収集を行うことで、省力化とともに、自らが世界を観察、特定、理解するようになる概念とのことである。しかし、現在の IoT は、収集した莫大なデータ（ビッグデータ）を用いて新しい知見を得たり、機器やシステムを制御することも重要な特徴となっている。

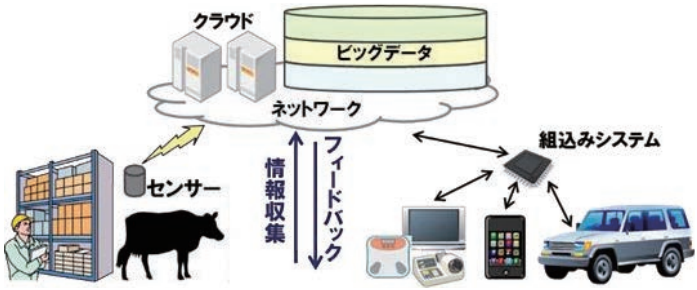
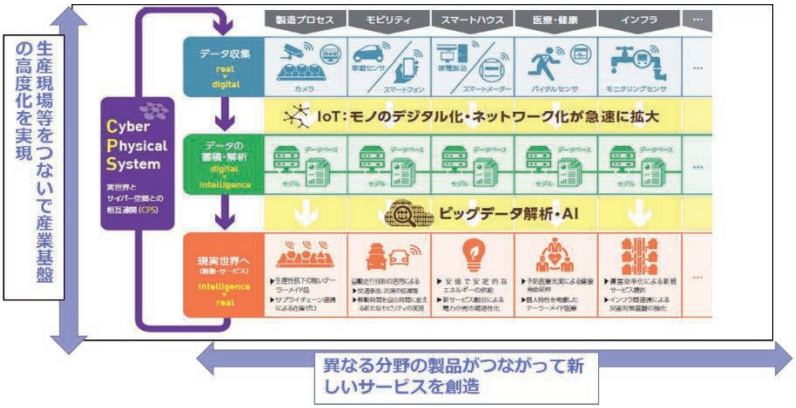



図 1-1 モノがつながる IoT

一方、経済産業省 産業構造審議会 商務流通情報分科会 情報経済小委員会の 2015 年の中間とりまとめ(案)（図 1-2）では、垂直方向の、生産現場をつないだ産業基盤の高度化と、水平方向の、異なる分野の製品がつながることによる新しいサービスの創造をイメージしている。本書での「つながる世界（≒ IoT）」はこの図全体の捉え方を想定している。

なお、本書では IoT の性質を表す場合には「IoT の特性」という用語を用いており、性質以外のものも含む場合には「IoT の特徴」という用語を用いている。




出典：経済産業省 産業構造審議会 商務流通情報分科会 情報経済小委員会 中間とりまとめ（案）に加筆

図 1-2 つながる世界のイメージ

## 1.3 目的

本書は、「つながる世界の開発指針」を基に開発される IoT 機器・システムの品質を確保するために、開発段階での品質の作り込みと保守・運用での品質の維持・改善に向けた考慮ポイントを示したものである。開発段階での品質の作り込みとしては、開発部門が作成した要求仕様や開発要件などの妥当性確認やテスト設計、テストの実施、および、検証・評価に関するマネジメントの考慮事項をまとめた。また、運用での品質の維持・改善としては、リリース後に発生する様々な変化や IoT 機器の故障、セキュリティ問題などに対応するための品質視点の考慮事項をまとめた。

本書は、IoT 機器・システムの品質に係わる人を主な読者としており、本書を活用することで、IoT のライフサイクルにわたり品質が担保できることを目指している。

本書をまとめるにあたり、以下を目指した。

(1) リリース前の品質の確保

IoT の品質確保では、品質保証関係者が開発の早期から妥当性確認のレビューなどに参画することが重要と考え、IoT の特徴などを考慮した指摘ができることを目指した。また、IoT のテストに関して、IoT 特有のテスト環境の準備やテスト設計ができることを目指して、テストを実施する上での考慮事項を示した。

(2) リリース後の品質の維持・改善

IoT はリリース後の変化が激しいこと（IoT 機器の増減によるシステム構成の変化やシステム連携、利用環境・利用者の変化など）から、運用での品質視点を示すことが重要と考え、IoT のライフサイクルにわたり安全安心を維持・改善するための考慮事項を示した。

本書を活用することで、IoT 開発で陥り易い考慮不足やテスト漏れを未然に防止することが可能となり、品質確保の重要性を認識することで、適正な経営資源を確保して安全安心な IoT を実現することを期待する。なお、本書では、IoT 機器・システム特有の品質確保に着目しており、一般的な品質確保については、各種の参考書や解説書を参照されたい［3］。

# 1.4 本書の位置付け

## (1) 開発指針との関係

IPA/SEC では、IoT の安全安心な実現に向けて、開発全般として考慮すべき事項を「つながる世界の開発指針」としてまとめた（第 1 版:2016 年 3 月公開、第 2 版:2017 年 6 月公開）。この開発指針は、主に開発者を対象に開発時に考慮して欲しい重要な事項をライフサイクル視点で、17 個の指針としてまとめたものである。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]」［4］として、2017 年 6 月に公開した。

本書は、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まとめたものである。

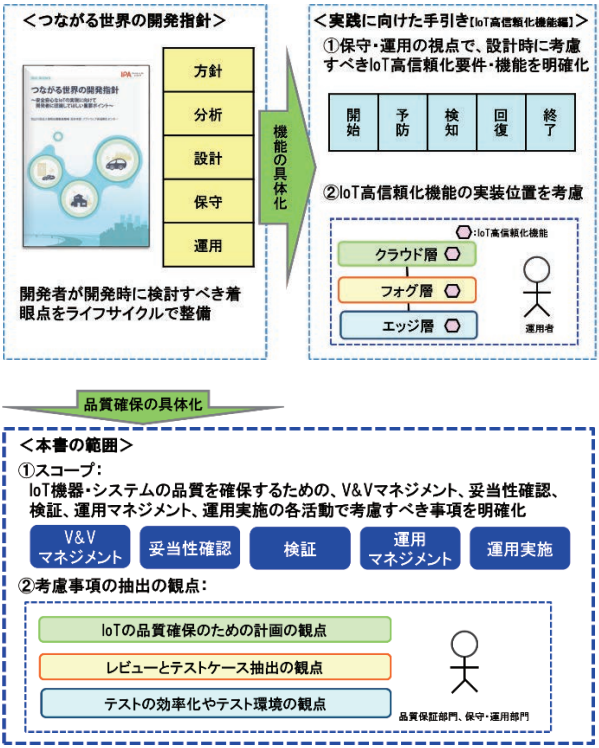



図 1-3 本書の位置付け

## (2) 開発プロセスとの関係

本書は、IoT 機器・システム開発の早期からの品質確保を目指すため、特定の開発プロセスに依存しないように記述しており、従来のウォーターフォール型の V 字開発や W 字開発、最近の新しい開発手法であるアジャイル開発、リーンソフトウェア開発、DevOps 開発などにも適用が可能と考えている。

## (3) 本書の活用方針

本書は、IoT の特徴を捉えて、IoT で特に留意が必要な品質確保の視点と考慮ポイントを記載している。

本書の活用に関して、以下を想定している。

- 第 3 章の視点や考慮ポイントは、必ず検討する。
- その対策の実施は、当事者の判断とする。

本書の具体的な適用事例に関しては、第 4 章で記載する。

## 1.5 想定する読者

本書で想定している対象読者を以下に示す。

### (1) 対象とする役割

本書では、品質の確保に関する役割を開発・保守時のテスト、運用に分類している（開発、保守、運用の範囲については 2.2.1 参照）。その役割を表 1-1 に示す。読者は幾つかの役割を持って活動していることを想定している。例えば開発者が開発時のテストと運用を行う場合は、それは開発・保守時のテストの役割と運用の役割の両方で活動することになると考えている。

表 1-1 対象とする役割

| 対象とする役割 | 役割の説明 |
|---|---|
| 開発・保守時のテストのマネジメント | 開発・保守におけるテストのプロジェクトの管理 |
| 開発・保守時のテスト | 開発・保守時の妥当性確認や検証による品質確保、および IoT 機器・システムの品質改善 |
| 運用マネジメント | 運用に関するプロジェクトの管理 |
| 運用 | IoT 機器・システムの品質維持、および運用改善 |

### (2) 役割ごとに特にお読みいただきたい箇所

役割ごとに、それぞれ特に読んでいただきたい箇所を表 1-2 に示す。

表 1-2 想定している読者と特にお読みいただきたい箇所

| 章＼読者の役割 | | 開発・保守時のテストのマネジメント | 開発・保守時のテスト | 運用マネジメント | 運用 |
|---|---|---|---|---|---|
| 第 1 章 | | ✔ | ✔ | ✔ | ✔ |
| 第 2 章 | | ✔ | ✔ | ✔ | ✔ |
| 第 3 章 | 3.1 | ✔ | ✔ | | |
| | 3.2～3.4 | | ✔ | | |
| | 3.5 | | | ✔ | ✔ |
| | 3.6 | | | | ✔ |
| 第 4 章 | | ✔ | ✔ | ✔ | ✔ |

なお、本書は、IoT 機器・システムの品質に係わる人を主な対象読者としているが、開発者や経営層にも参考になると考えており、一読を勧めたい。

# 第2章
# つながる世界の品質課題



本章では、つながる世界の品質課題とその対策をどのように導出したかについて、説明する。まず、IoT の品質を確保すべき開発・保守と運用の活動場面を想定し、これらの活動場面をスコープとして定義した。次に、このスコープを意識して IoT の品質に係わる課題意識やニーズを収集し、それらを IoT の特徴で分析し、検討すべき観点を整理した。そのスコープと観点の 2 つの軸を用いて、IoT の品質課題と対策を導き出した。

以下に、IoT の品質課題の導出と対策に向けた検討のアプローチについて、解説する。

# 2.1 IoT の品質課題と解決に向けたアプローチ

本書における IoT の品質に関する課題の抽出と対策の検討のアプローチを図 2-1 に示す。

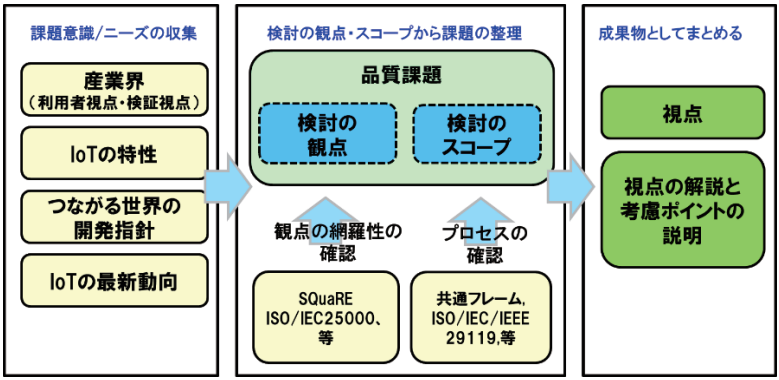



図 2-1 品質課題と解決に向けたアプローチ

## (1) スコープ

IoT は、ライフサイクルが長いという特徴があるため、開発時の品質確保だけでは不足であり、運用での品質の維持・改善が必要となる。そこで、開発・保守と運用に分けて、IoT の品質を検討するためのスコープを以下のように定義した。なお、本書では、保守はリリース後に開発担当者が実施する改修（改善）作業を表す。詳細は、2.2.1 で解説する。

【開発・保守】：V&V マネジメント、妥当性確認、検証

【運用】：運用マネジメント、運用実施

スコープの検討では、ISO/IEC 12207（ソフトウェアライフサイクルプロセス）に適合した共通フレーム [5]や ISO/IEC/IEEE 29119（ソフトウェアテスティング）を参考とした。

## (2) 課題意識/ニーズの収集と観点の整理

現場の意見として産業界から IoT の品質に係わる課題意識やニーズを収集した。この意見収集では、様々な分野の有識者を中心として、製品やシステム開発・保守に係わる意見とそれらの品質確保に係わる意見、さらに、運用に係わる意見など、約 100 件を収集した。それらに加えて IoT セキュリティガイドラ

イン［6］などで提唱されている IoT の特性や、IoT の品質に関連する業界ガイドや国際規格の最新の動向などを参考として、IoT の品質に係わる課題意識を抽出した。

次に、それらの課題意識を IoT の特徴で分析し、検討すべき観点を整理した。詳細は、2.2.2 で解説する。なお、この観点の検討では、ISO/IEC25000 シリーズ（SQuaRE）の品質特性を参考とした。

### (3) スコープと観点による課題の整理

上記で説明したスコープと観点の 2 つの軸を用いて、IoT で検討すべき品質課題を整理した。詳細は、2.2.3 で解説する。

### (4) 成果物としてのまとめ

整理した品質課題に対して、IoT の品質を確保する場面である開発・保守と運用で考慮すべき事項を検討し、対策としてまとめた。詳細は、第 3 章で解説する。

# ＜コラム 1＞IoT の特性

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

IoT の特性を挙げた例として、IoT セキュリティガイドライン［6］がある。IoT の品質を考えるときには、下記の IoT の特性を考慮することで、検証や評価のヒントが得られる。ここで示した着眼点は、IPA の解釈である。

**（性質 1）脅威の影響範囲・影響度合いが大きいこと**

着眼点：IoT では、IoT 機器・システムで発生した障害が拡散するため、障害の早期検知や防御・回復などの対策に着目する。

**（性質 2）IoT 機器のライフサイクルが長いこと**

着眼点：IoT は、10 年以上にわたり利用されることが想定され、長期間の利用による故障やセキュリティの劣化などの対策に着目する。

**（性質 3）IoT 機器に対する監視が行き届きにくいこと**

着眼点：IoT では、管理されないモノが勝手につながることがあり、セキュリティの脅威が増すため、セキュリティ対策に着目する。また、IoT 機器は屋外に設置されることがあり、離島や山岳地帯など保守員が簡単に踏み込めない場所などの監視やシステムの保全などの対策に着目する。

**（性質 4）IoT 機器側とネットワーク側の環境や特性の相互理解が不十分であること**

着眼点：IoT 機器側とネットワーク側の相互の理解不足により所要の安全や性能が満たされないケースが想定され、ネットワークと機器の接続環境に着目する。

**（性質 5）IoT 機器の機能・性能が限られていること**

着眼点：センサーなどのリソースが限られた IoT 機器では、セキュリティ対策が十分でないことも想定され、IoT 機器単体とシステム全体としてのセキュリティ対策に着目する。

**（性質 6）開発者が想定していなかった接続が行われる可能性があること**

着眼点：IoT では、様々な環境で利用されるため、様々な形態での接続が発生し、メーカ側が想定しないつながり方も起こり得る。そのため、IoT の様々な利用環境や利用者に着目する。

# 2.2 スコープと観点による課題の整理

## 2.2.1 スコープ

本書では、品質を確保すべき活動場面を想定し、開発・保守での品質確保と運用での品質維持・改善の活動をスコープとした。スコープとしては、図 2-2 に示すように、開発・保守での①V&V マネジメント、②妥当性確認、③検証、および運用での④運用マネジメント、⑤運用実施とした。なお、図 2-2 は、W 字開発プロセスを例として、活動をマップしているが、本書では、特定の開発プロセスを前提としていない。

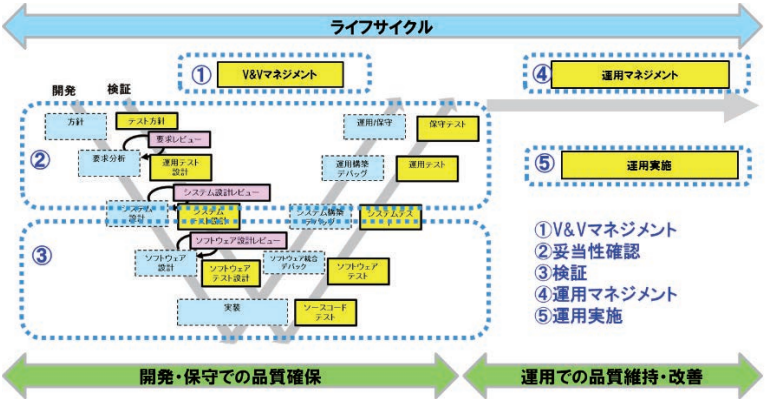



図 2-2 品質確認の活動の場面

### (1) V&V マネジメント

ここでは、IoT の開発・保守での妥当性確認や検証などのマネジメントを実施するときの場面で必要となる課題を検討した。この V&V マネジメントでは、検証や評価の方針、計画の策定、品質の説明責任、関係者間の合意形成などに関して扱うことにした。

### (2) 妥当性確認

ここでは、IoT 開発の要求や要件に関して、妥当性を確認する場面で必要となる課題を検討した。この妥当性確認では、利用者に本来提供したい価値が提供できるかの視点で、開発上流での要求仕様や開発要件のレビューと、実装後の確認に関して扱うことにした。

### (3) 検証

ここでは、IoT 機器・システムの設計関連の仕様を基に具体的なテスト設計とテスト実施の場面で必要となる課題を検討した。テスト設計では、IoT の特徴に着目したテストケースの抽出やテスト環境、テストのし易さ（DFT: Design For Test）に関して扱うことにした。テスト実施では、テストの効率化やテスト実施のエビデンスの保管に関して扱う。

### (4) 運用マネジメント

ここでは、IoT の品質の維持・改善のための運用に関する点検や診断、訓練などの場面で必要となる課題を検討した。この運用マネジメントでは、リリース後の構成の変化や利用環境・利用者の変化、脆弱性などの変化を想定した運用計画の立案とその運用計画の実施の評価と改善に関して扱うことにした。

### (5) 運用実施

ここでは、IoT の品質の維持・改善に着目して、運用を実践する場面で必要となる課題を検討した。この運用実施では、運用中に確認すべき機能やソフトウェア更新の適用時の考慮点などに関して扱うことにした。

## 2.2.2 観点

IoT の品質に関する約 100 件の課題認識を IoT の特徴を踏まえて分析し、以下の 3 つに分類した。

### (1) IoT の品質確保のための計画の観点

IoT は、様々な機器やシステムが連携して構成される特徴があるため、SoS を捉えた全体の品質確保、品質の説明責任、関係者との合意形成が重要となる。また、要件の妥当性確認やテストをどこまでやるのかなど、組織としての基本方針や検証・評価の計画立案などが重要となる。ここでは、IoT の品質確保のための組織の能力に焦点を当て、課題を検討した。

### (2) レビューとテストケース抽出の観点

IoT は、現場での知見がまだ少ないため、開発の要件そのものが利用者の要求を満たすものであることを客観的に確認する必要があり、開発時の要求仕様や開発要件などに対してレビューでの妥当性の確認が重要となる。特に、今ま

でつながっていなかったモノがつながることにより、セキュリティの脅威が増加することから、セキュリティの脅威分析の粒度や精度などの確認が重要となる。また、長期にわたって利用される多種多様な利用場面や、さらに IoT の変化に着目した保守や運用などの確認が必要となる。ここでは、IoT 機器・システムのプロダクト品質に焦点を当て、ISO/IEC25000 シリーズ（SQuaRE）の品質特性に着目して、テストケースの抽出に関して課題を検討した。

### (3) テストの効率化とテスト環境の観点

IoT の構成は、多種多様であり、様々な接続パターンや利用シーンがある。さらに、IoT の端末の最大接続や大量データ、異常データなどを組み合わせるとテストケースが爆発することが想定され、テストの効率化の観点が重要となる。また、それらのテストを実施するときのテスト環境が準備できないなどの問題もあり、テスト環境の整備の観点も重要となる。なお、品質の説明責任を果たすためにテストのエビデンスを残すことも必要となる。ここでは、テストの効率化とテスト環境の整備、およびテストのエビデンスに関して課題を検討した。

## 2.2.3 IoT の品質課題

上記のスコープと観点の 2 つの検討軸を基に、IoT の品質確保、維持・改善に関する品質課題を整理した。主な品質課題を以下に示す。

表 2-1 IoT の品質課題の整理

| 観点 / スコープ | IoT の品質確保のための計画の観点 | レビューとテストケース抽出の観点 | テストの効率化とテスト環境の観点 |
|---|---|---|---|
| V&V マネジメント | 課題1 | ― | ― |
| 妥当性確認 | ― | 課題2 | 課題2 |
| 検証（テスト設計） | ― | 課題3 | ― |
| 検証（テスト実施） | ― | ― | 課題4 |
| 運用マネジメント | 課題5 | ― | ― |
| 運用実施 | ― | 課題6 | ― |

**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**

- IoT は多種多様な購入品で構成される SoS であり全体の品質確保が必要
- IoT コンポーネントとしての品質の説明責任が必要

・関係者が多いため、品質の確保・維持に関する合意が必要
・IoT の品質確保について、何をどこまで確認するかの方針・計画が必要

**課題２：多種多様な IoT の要求や要件の妥当性の確認**

・IoT は様々な場所（離島、寒冷地、高地）で様々な人々が利用
・接続機種の増加やシステム連携などの変化でセキュリティの脅威が増加
・ライフサイクルも長いことが想定され、長期メンテナンスが必要
・IoT 開発の要求や要件が十分考慮されているかの妥当性の確認

**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**

・つながることによるセキュリティの脅威分析とその検証
・長期にわたって利用される多種多様な利用場面を想定した検証
・IoT の変化に着目した保守や運用機能の検証
・IoT の安全安心に係わる機能の検証（異常監視/検知、回復、性能など）

**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**

・テストケースの爆発に対するテスト効率化
・多種多様なテスト環境（負荷シミュレータ、各種ツール）の準備
・品質の説明責任が果たせるテストのエビデンスの取得と保管

**課題５：変化が激しい IoT の運用での品質維持・改善の計画**

・IoT の運用に関して、何をいつ、どのように実施するかの方針・計画
・リリース後の故障やセキュリティ異常の監視と対処
・利用者の使い方の変化に対する情報収集と品質の維持・改善
・法規制の変化や最新技術の動向調査による対応

**課題６：長期にわたる利用での品質の維持・改善**

・IoT の変化に対して、機能や性能が満足できているかの確認
・IoT の安全安心に係わる機能が正常に動作しているかの確認
・ソフトウェア更新がつながる相手に影響を与えないかの確認

# ＜コラム 2＞IoT 検証ガイドラインの動向

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

IoT の検証に関するガイド類は、これまであまり整備されていない状況であったが、セキュリティに関するガイドとして、OWASP の「IoT Testing Guides」［7］と重要生活機器連携セキュリティ協議会（CCDS）の「IoT セキュリティ評価検証ガイドライン」［8］を紹介する。

OWASP とは、Web をはじめとするセキュアなソフトウェア開発を促進する技術・プロセスに関する情報共有と普及啓発を目的としたコミュニティである。OWASP には、IoT のセキュリティについて扱うプロジェクトがあり、そこでは、「IoT Testing Guides」が整備されている。本ガイドは、IoT のテストにおいて物理的な面を含めたセキュリティに関するテストの考慮事項を 10 のカテゴリに分けて示している。また、セキュリティだけでなく、プライバシーについても言及されていることが大きな特徴である。

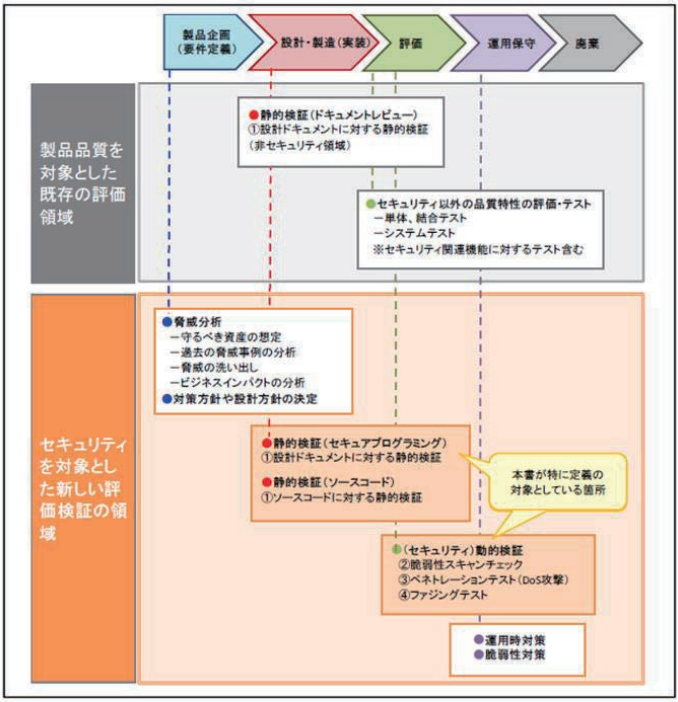
| Category |
|---|
| I1: Insecure Web Interface |
| I2: Insufficient Authentication/Authorization |
| I3: Insecure Network Services |
| I4: Lack of Transport Encryption |
| I5: Privacy Concerns |
| I6: Insecure Cloud Interface |
| I7: Insecure Mobile Interface |
| I8: Insufficient Security Configurability |
| I9: Insecure Software/Firmware |
| I10: Poor Physical Security |

IoT Testing Guides のカテゴリ

CCDS は日常生活で利用する機器のセキュリティ技術に関する調査研究を行っている国内の団体であり、「IoT セキュリティ評価検証ガイドライン」を公開している。本ガイドラインでは、IoT のセキュリティ検証についてプロセスを示し、さらに手法やツール、リスク評価について事例を挙げている。

また、国内の他の例として、IoT だけをターゲットとしたものではないが、IPA が「ファジング活用の手引き」［9］を、また、コンピュータソフトウェア

協会（CSAJ）が「ソフトウェア出荷判定セキュリティ基準チェックリスト」[10]を公開している。これらの、ガイド類は IoT のセキュリティの検証について具体的に検討する場合に参考になると考えている。




IoT セキュリティ評価検証ガイドラインのプロセス

# 第3章
# つながる世界の品質の確保、維持・改善の視点

本章では、第2章で抽出したIoTの6つの品質課題に対して、IoTの品質の確保、維持・改善をするために最低限、考慮すべきポイントを解説する。ここでは、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の視点について示した。

【視点1～10】：主に品質確保に係わる関係者が対象

この視点1～10は、IoT機器・システムの開発・保守時点で品質を確保するために、品質確保に係わる関係者が実施する妥当性確認や検証などに関しての視点と考慮ポイントを示した。ここでは、例えば、ソフトウェア更新の修正内容の妥当性確認や更新データの検証なども含まれる。

【視点11～13】：主に運用に係わる関係者が対象

この視点11～13は、運用で品質の維持・改善をするために、運用に係わる関係者が運用中に実施する点検、診断、訓練などに関しての視点と考慮ポイントを示した。ここでは、例えば、ソフトウェア更新の適用に関して、いつ誰がどのように実施するかなどの運用計画の立案と事前確認などが含まれる。

開発・保守と運用の関係は、完全に独立した組織が実施する場合やDevOpsのように密な連携もあり様々であるが、それぞれの活動場面として考慮すべき事項を記述した。なお、実際のトラブルシューティングや改善活動では、関係者と協調した連携が重要となるため、視点1の中で、関係者間での合意形成について、記述した。

品質の確保、維持・改善の視点一覧を表 3-1 に示す。

表 3-1 品質の確保、維持・改善の視点一覧

| | 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 | 3.1 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 | 3.2 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 | 3.3 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 |
| | | 3.4 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 | 3.5 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 | 3.6 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 |

# 3.1 IoT の品質確保のための検証・評価計画立案

IoT では、様々な種類の IoT 機器・システムがつながり、長期にわたり安全安心を維持することが求められる。IoT の品質を確保するためには、IoT 機器・システムの特徴を捉え、リスク対策を考慮した検証・評価方針を策定することが重要となる。さらに、その方針に基づいて、検証対象と検証範囲を定めて、IoT の検証が可能なスキルを有する人材の確保や検証を推進する体制を整備し、検証計画を立てる必要がある。ここでの検証とは、開発要件の妥当性確認やテスト設計時の開発側資料のレビュー（矛盾指摘など）も含まれる。また、IoT では、多種多様なベンダーからの調達や構築・運用など関係者が多くなると想定されることから、関係者間での責任範囲などの合意形成が必要であり、ステークホルダーへの品質の説明責任を果たせるような検証計画の策定が重要である。

本節では、開発段階での品質の確保を担う検証プロジェクトに要求される IoT の特徴を捉えた検証方針、検証計画の策定や品質の説明責任、関係者間の合意形成において考慮すべき視点について説明する。

# 【視点 1】IoT の社会的影響やリスクを想定する

## (1) 概説

IoT では、今まで単独で利用していた機器がネットワークにつながり、様々な環境で利用されることから、一旦、障害が発生したりマルウェアに感染すると、その影響は、甚大なものとなる可能性がある。2016 年 9 月に世界規模で発生したマルウェア「Mirai」では、家庭用ルータやデジタルビデオレコーダなどに 30 万件以上も感染し、大規模な DDoS 攻撃による甚大な被害が発生したと言われている［11］。

IoT の品質を確保するためには、IoT 機器・システムがどのような環境で利用されるかを把握し、万一、問題が発生したときの社会的な影響やリスクを考慮し、検証・評価方針や検証・評価計画を策定することが重要である。また、ステークホルダーへの品質の説明責任を果たすことも重要になるが、IoT は様々なベンダーや構築業者が係わると想定され、構築に係わる関係者間の責任範囲などの合意形成も必要となる。

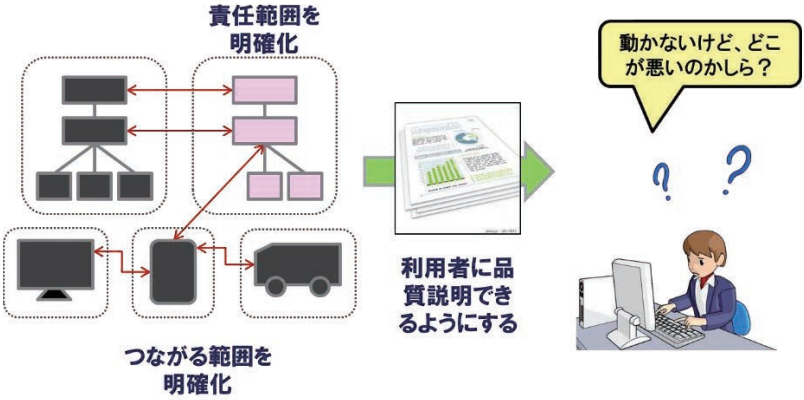



図 3-1 検証・評価計画を立てる

## (2) 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

IoT では、つながる相手に迷惑をかける可能性があるので、IoT 機器・システムがもたらす問題の重要性を意識し、リスクを考慮した検証方針を策定する。

① IoT 機器・システムの特徴の観点から検証方針を策定する。

IoT 機器・システムが利用される環境条件や利用者を考慮し、要求される品質を満たすべく方針を立てることが重要である。

1) IoT の特徴を考慮したテストの方針

- 利用者や利用環境を考慮したセキュリティやプライバシー対策のテスト
- 長期間利用に係わる保守・運用向け機能のテスト
- 大量データ、大量の機器、想定外の利用などに係わるテスト
- エッジ、フォグ、クラウドなど実装位置に係わるテスト

2) 利用分野、国内/海外などの利用場所を考慮した各種法規制の対応方針

- 国内の産業分野特有の安全規制や法律に係わる対応の方針

  例えば、製造物責任（PL）法、電気用品安全法、電気通信事業者法、個人情報保護法など。また、無線関係を扱う IoT では、電波法に関する小電力無線局や微弱無線局などの規則も考慮する。
- 海外の法律に係わる対応方針

  例えば、EU 一般データ保護規則（GDPR）など。

② 検証プロジェクトの要件の観点から検証方針を策定する。

IoT 機器・システムが適用される分野の特徴を捉えて、検証プロジェクトに要求される要件を分析し、品質を確保するための方針を立てることが重要である。以下に方針策定時の考慮点を示す。

1) 検証プロジェクト自体のリスク対策

以下のリスクを考慮し、対策を方針に盛り込む。

- つながる相手への影響が大きく検証漏れがもたらすリスク
- 検証環境が用意できないリスク

  例えば、IoT 機器台数やつながり方のバリエーション、環境条件を考慮
- 求められる人材が確保できないリスク

  例えば、セキュリティ、通信、デバイス特性などの知識が必要
- システムが複雑なので試験項目が多くなり検証期間が延びるリスク

2) 品質説明責任が果たせる範囲の明確化

品質の説明責任が果たせるように、品質確認の方針と品質プロセスを規定し、それらを順守することを盛り込む。

- IoT 機器・システム自体の品質目標の決定と承認手続きの明確化

例えば、IoT 機器・システムの品質目標を定め、検証の完了判定と合否判定を定め、責任者の承認を規定する。また、適用分野で必要となる公的な認証などを規定する。なお、調達品についても、どのように品質を確保するかを規定する。

・ 適正品質を確保するための方針の明確化

IoT 機器・システムの適用分野に要求される品質を確保することが重要であり、適正品質の確保を意識した妥当性確認と検証の方針を盛り込む。これにより、何をどの程度確認するかの範囲と深度が明確になる。

・ プロセスどおりに実施していることのエビデンスの確保

例えば、テストに関する記録や保管するドキュメント、検証部門の参画するタイミングなどを規定する。また、それらの品質記録のエビデンスが変更されないような保管方法を規定する。



**【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**

検証方針を具体化した検証計画を策定し、実施状況を管理することが重要である。一般的に検証計画では、検証対象・範囲、体制・要員、スケジュールをリスクやコストを意識しながら検討する。また、評価基準も計画段階で準備しておく必要がある。ここでは、IoT の特徴を考慮した検証計画を策定するときの考慮ポイントを示す。

① 検証対象・範囲

1) つながる相手との接続に着目した検証範囲の明確化

つなぐ機器の種類やプロトコル、つなぎ方など検証する範囲を定めて、異常時の振る舞いや相手への影響をどこまで確認するかなどを決める。また、今まで外部とつながっていなかったクローズドシステムとの連携や旧システムとの連携などでは、連携のリスクを評価し検証の範囲を決めることが必要である。

2) 多数の機器、多様な機器との接続検証環境の準備計画

自前で準備ができる環境と準備できない環境を整理し、必要に応じて外部のテストベッドなどの活用を検討する。また、大規模な環境の代わり

にシミュレータなどの活用を検討する。なお、テスト環境は、リリース後の障害の再現調査や機能拡張時およびソフトウェア更新時などの確認のために、確保しておくことが望ましい。テスト環境そのものが残せない場合は、テスト環境の構築手順書やテスト手順書などを残す。

3) 調達品の検証計画

自社製品やシステムの一部として調達品を利用する場合には、調達品に不具合がありその開発元に責任があったとしても、最終提供元の企業への責任が問われる可能性がある。IoT は、特に、SoS で構成され調達品が多用されることが想定されるので、調達品の品質をどこまで確認するかなどの検証計画を立てる。

② 体制・要員

IoT の検証に必要なスキルを有する検証要員を確保し、検証体制を整備する。例えば、以下の知識やスキルを有する検証要員が必要である。

1) IoT の特徴の理解

IoT を構成する IoT 機器、ネットワーク、クラウドなどの要素技術や IoT の特徴、IoT に潜むリスクなどの知識。例えば、「つながる世界の開発指針」［1］、「IoT セキュリティガイドライン」［6］などの理解。

2) セーフティ、セキュリティ上のリスクとそれに対応する機能の理解

例えば、「つながる世界のセーフティ＆セキュリティ設計入門」［12］、「『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］」［4］、セキュアコーディングなどの理解。

3) 自社だけで体制構築ができない場合、他社の協力についての検討

IoT の検証では、一般的な IoT やセキュリティ関連の知識以外に、無線に関する知識や適用分野の知識など専門知識も必要になる場合がある。また、大規模なシミュレータなどのツールを使用する場合では、使いこなせるスキルが必要になり、それらの専門スキルを有する社外の協力も検討する。

③ スケジュール

IoT の検証は、IoT の特徴や適用分野などを考慮することで、多岐にわたることが想定されるため、その検証スケジュールは、要員の確保や検証環境の手配・構築も含めて、十分な検討が必要である。例えば、以下を考慮する。

1)　構成の複雑性を考慮した検証スケジュール
2)　つながる相手との調整（検証範囲、手法など）に基づくスケジュール
3)　要員確保の遅延リスクを考慮したスケジュール
4)　検証環境の手配・構築の遅延リスクを考慮したスケジュール

④　評価基準の策定

評価基準の策定にあたっては、品質の重要項目を定め、満たすべきレベルを決めて、観測可能な数値化を行うことが重要である。また、自社の基準だけでなく、IoT の重要度を勘案して適用分野の業界規格や法規制などを考慮する必要がある。評価基準を考える上では、例えば、セキュリティに関するコモンクライテリアやセーフティに関する機能安全規格類、ISO/IEC25000 シリーズ(SQuaRE)の品質特性などが参考となる。IoT の安全安心に係わる品質の重点項目としては、例えば、セキュリティ、セーフティ、信頼性、性能、ユーザインタフェースなどがある。

⑤　ツールの検討と予算化

検証に必要と想定されるツール類を検討し、内製するものや調達するものを整理し、予算化しておくことが重要である。大規模な負荷シミュレータや擬似的な故障発生のツールなどは、高額になることもあり、この計画段階でテストツールやテスト環境などを調査し、概算しておく必要がある。



### 【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

ここでは、特に、IoT で重要となる品質説明責任に着目して、考慮ポイントを説明する。昨今、色々な分野で製造者やサービス事業者に対して、品質の説明責任が問われる時代になってきている。特に、セキュリティに関しては、国際的にメーカ責任が問われる時代になってきており、何をどのように確認したかを説明できることが求められる。IoT は、マルチベンダーによる多種多様な機器で構成されることが想定され、クレームや問題が発生したときには、責任の所在が特定できず、利用者に迷惑をかけることが懸念される。IoT の検証においては、利用者や関係者への品質の説明責任を果たすためのエビデンスを残すことが重要である。例えば、以下を考慮する。

①　製品のサプライチェーンを含めた品質の把握とエビデンス

調達品や OSS（オープンソースソフトウェア）などを含めたシステム全体の

品質を確認する仕組みを検討し、品質の把握とエビデンスとして残す記録、保管期限などを明確にする。また、セキュリティに関しては、蓄積された過去のソフトウェア資産や既存のシステムを流用する場合には、未対応の脆弱性などをどのように確認するかを明確にすることが重要である。

② つながる相手を意識した検証のエビデンス

IoT の検証として計画したテストに関して、テストの実施環境、実施項目、実施結果（合否判定）、実施日時、実施者などのエビデンスを残す。また、合否判定が正しかったことを立証する実行ログなどを残すことも重要である。

③ IoT のライフサイクルにわたって品質が維持できることの把握とエビデンス

IoT 機器の出荷後やシステムのリリース後の品質が維持できる範囲（例えば、品質保証 5 年など）を明確にし、品質が証明できるエビデンスを残す。なお、リリース後の機能追加や修正対応などで、品質確保ができる仕組みに整備し、実施したエビデンスを残すことも重要である。

④ 品質の要求レベルに応じたエビデンス

IoT は、生命や財産、社会に与える影響が大きいものがあり、適用分野における品質の要求に応じた品質に係わるエビデンスの確保が重要である。例えば、客観的な検証のエビデンスが求められる場合は、開発企業とは独立な第三者による検証が有効である。また、場合によっては、開発プロセスのプロセス監査の結果も必要となることがある。

⑤ 保証範囲を明確化したエビデンス

IoT は、様々なつながり方があるが、想定される利用環境などを踏まえて、開発時点でリスク分析を実施し、保証範囲を明確にする必要がある。その際には、どのような手法でリスク分析を実施し、そのリスク対策をどのような手法で確認したか関係者に説明できるエビデンスを残すことが重要である。加えて、保証範囲外においても、問題が発生する可能性がある重要な事項についてはそれらを明らかにする必要がある。

**【1-4】検証・評価の範囲を明確化し、関係者間の合意を促す**

IoT 開発では、品質の確保や品質の維持・改善には関係者間での合意形成が重要である。IoT は構成のバリエーションや利用シーンが多岐にわたるため、すべてのテストケースを確認することは困難が予想され、どの範囲まで検証するかなど関係者間での合意が必要である。また、IoT 機器・システムの開発段階での検証に関する計画やテスト結果の合否判断などは、依頼元との合意が重要となる。さらに、リリース後のトラブルシューティングを速やかに実施するためには、調達品の提供元や運用関係者などとの合意が重要である。例えば、以下の事項を考慮する。

① 検証に関する合意

検証に関する検証計画書やテスト設計書などは、テストを実施する前に依頼元とレビューを実施し、計画に対する正当性の確認を取る必要がある。また、テストケースの範囲を絞る場合、絞ることによるリスクを関係者で共有した上で範囲を設定することが望ましい。さらに、テスト結果の合否判定に関しても依頼元と協議し、事前に合否判定基準の合意を取るとともに、テスト実施後の結果の判定の妥当性に関して合意を取ることが望ましい。

② 問題解決に関する合意

調達品の提供元や製造ベンダーなどから品質に関する情報や障害および脆弱性に関する情報などを適宜、入手できるように合意を取ることが重要である。また、問題が起きたときの原因の特定と対処の迅速化のために、トラブルシューティングに関する協力体制を構築することが必要である。

## 3.2 利用者視点での要求の妥当性確認

IoT の開発経験が少ない企業や分野では、IoT で考慮すべき要求そのものが十分に検討されないまま、開発に着手するケースも考えられる。特に、新規に IoT に参入するベンチャー企業や今までネットワークにつながる製品を開発したことがない企業などでは、要求仕様や開発要件のレビュー不足によるリスクが高い製品開発となることが懸念される。IoT 機器・システムは、長期にわたり安全安心を維持することが求められるため、開発の上流で保守・運用を想定した製品・システム開発に関する要求仕様のレビューが重要となる。この要求仕様に関するレビューでは、IoT の特徴や製品・システムの適用分野を理解し、利用者に本来、提供したい価値が提供できるかの視点で妥当性について、客観的な立場で確認することが重要となる。また、IoT 機器・システムを実装した後の最終段階の確認として、要求に対する妥当性確認が必要であり、保守・運用の要件も含めた確認が重要である。

本節では、IoT 機器・システムの要求仕様や開発要件のレビューとその要件を実装した後の妥当性確認において、考慮すべき視点について説明する。なお、ここでは、利用者からの明示的な要求や要件だけではなく、利用者が安全安心に利用するため暗黙的なセーフティやセキュリティ要件、信頼性に関する要件なども対象としている。

# 【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

## (1) 概説

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る。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う。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た［1］。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する。

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る。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ある。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る。

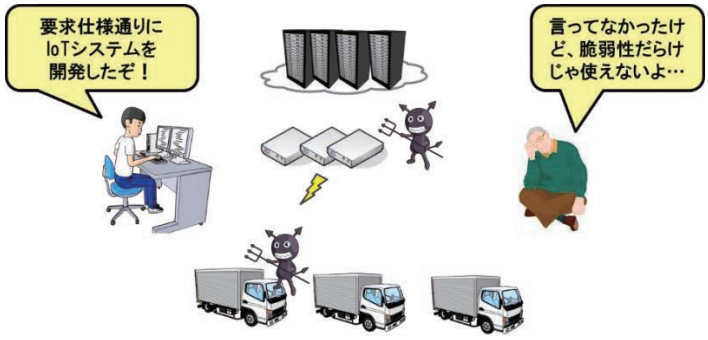



図 3-2 利用者視点で要求・要件の妥当性を確認

## (2) 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**

IoT 機器は、ネットワークにつながることにより、例えば、様々なデータをダウンロードできたり、アップロードできるようになり、それに伴う IoT 特有の機能が備わる。また、IoT は、多種多様な IoT 機器が色々なパターンでつながることから、性能差による問題や互換性、拡張性の問題が起こることが想定され、これらに着目した妥当性のレビューが重要である。

① IoT 特有の機能

IoT 機器としてネットワークにつながることによって付加された機能に着目して、レビューを実施する。例えば、IoT 機器にリモートアップデート機能が搭載されると仮定すると、リモートアップデートのための作業領域の最大サイズや更新回数の制限、更新の実施による本来の性能への影響などが考慮され、それらの見積値が妥当かどうかを確認する。また、リモートアップデート適用の失敗時の回復機能とその回復までの時間が妥当かなどを確認する。

② つながる機器の性能差

様々な機器がつながる場合、メーカの機器個体としての性能差や利用環境による性能差などに着目して、レビューを実施する。例えば、性能差が要件として明確になっているか、その性能差が IoT 全体として影響を及ぼさないか、また、利用者から見て、許容されるレベルかなどを確認する。

③ つながる機器の種類と接続数

つながる機器の種類やプロトコル、接続数が明確になっているか、また、今後、出てくると予想される機器やプロトコルの扱いに着目して、レビューを実施する。例えば、現状、サポート予定の機器やプロトコル、接続機器台数が利用者から見て妥当であるか、今後出てくると予想される機器やプロトコルの扱いが要件として明確になっているかなどを確認する。

④ 取り扱うデータの種類とデータ量

IoT として、取り扱うデータの種類とデータ量に着目して、レビューを実施する。例えば、取り扱うデータの種類、最大データ量が、今後の拡張や IoT 連携強化に対して妥当であるか、また、想定外のデータの取り扱いが明確になっているかなどを確認する。

⑤ つながる相手を含めた機能の充足性

開発要件が将来の拡張や IoT 連携強化を考慮しているかに着目して、レビューを実施する。例えば、拡張や連携機能として考慮している通信仕様や

サービス仕様が今後の技術の進展や利用者の拡大から見た場合、妥当であるかを確認する。また、外部のシステムとの連携などで、連携異常の監視が妥当であるかの確認も必要となる。

**【2-2】利用環境や利用者の使い方に着目する**

IoT は、様々な利用環境で使われ、その利用者も多岐にわたる。IoT 機器・システムの要求仕様や開発要件が利用シーンを意識して明確になっているか、その想定が妥当であるかのレビューが重要である。

① 利用環境や利用場面

利用者が IoT を使うときの利用環境や利用場面に着目して、レビューを実施する。例えば、利用場所として国内/海外、離島、寒冷地、高地などが考慮されているか。また、利用場面が、人命や財産、社会への影響が大きいときの考慮がされているか、緊急時の利用などが考慮されているかなど、それらの考慮が妥当であるかを確認する。なお、利用時のユーザ ID やパスワードが初期値の状態で利用されたときのリスク対策が考慮され、妥当であるかを確認する。

② 利用者の特性や役割

利用者は誰なのか、利用者の役割にも着目して、レビューを実施する。例えば、利用者の特性として、海外の習慣や慣習の違う人たちが使う場合や、幼児や高齢者、目や指先が不自由な方などの想定利用者が明確化され、それが妥当であるかを確認する。また、利用者の種類として、一般利用者、企業の利用者、運用者などを想定し、それらの特性の違いの認識や、利用者の利用スキルなどを考慮しているかを確認する。

③ 利用状況のフィードバック

インターネットにつながることで、利用者の利用環境や利用状況に関するデータをリアルタイムで収集可能であり、利用時の品質を改善することができることに着目して、レビューを実施する。また、収集した利用状況のデータの取り扱いがプライバシー保護や関連する法律や規制（欧州の GDPR など）を考慮しているかなどを確認する。

**【2-3】IoT のライフサイクルでの安全安心(セキュリティ、セーフティ、リライアビリティ)に着目する**

IoT は、ライフサイクルが長い特徴があり、利用期間の中で機器の故障やセキュリティ機能の劣化などが想定される。また、セキュリティレベルが異なるシステム連携によるセキュリティ脅威の増加、利用者や接続機器台数の増加による性能劣化や機能不全などが懸念される。IoT のライフサイクルでの安全安心を確保するための要件に対して、その妥当性のレビューが重要である。

① IoT 機器の障害や劣化

IoT は、生命や財産に係わる用途や産業や社会への影響が大きい用途があるため、高い信頼性が要求されることがある。IoT 機器の障害や劣化に対して、システムを継続するための信頼性に関する要件が明確であり、それが妥当であるかを確認する。例えば、障害の検知や障害が発生した部分の切り離し・回避、回復などの要件やシステムの継続・停止の要件などが妥当であるかを確認する。また、監視対象の機器や事象が明確化され、障害を特定するためのログの種類や量が妥当であるかなどを確認する。

② セキュリティレベルの考慮と脆弱性への対応

IoT 機器・システムの適用分野におけるセキュリティレベルの要件が明確化されているか、それが妥当であるかを確認する。例えば、コモンクライテリア［13］もその参考になる。また、IoT 機器・システムが達成すべきレベルでのセキュリティ脅威分析が実施できていることの確認が重要である。この脅威分析では、必要に応じてセキュリティの専門家の意見が入っていることなども確認する。さらに、そのセキュリティ脅威分析の対策として、例えば、暗号化やアクセス認証などの技術水準の考慮が妥当かなども確認する。なお、セキュリティは時間とともに劣化する特性があるため、脆弱性への対応方針の考慮が妥当かなどを確認することも必要である。また、セキュリティ対策がセーフティ機能に影響することもあり得るため、セキュリティとセーフティの関係者が相互に影響を分析していることの確認も重要である。

③ システムの拡張による性能劣化・機能不全への対応

IoT は、時間の経過に伴い変化する特徴があり、それらの変化に対しての要件が明確化されているか、それが妥当であるかを確認する。例えば、IoT 機

器の種類や台数の増加による性能劣化、機能拡張やサービス連携の強化による機能不全、法規制の変化や利用者・利用環境の変化に対する機能不適合などへの対応方針や要件を確認する。

**【2-4】長期利用のための保守・運用に着目する**

IoT は、リリースした後に様々な変化が予想されるが、長期にわたり品質を維持・改善するための保守や運用の要件に対して、その妥当性のレビューが重要である。特に、IoT の保守・運用が安全安心に実施でき、かつ保守・運用が効率よく実施できるかに着目したレビューが必要である。

① IoT 機器・システムの障害対応や機能改善

IoT 機器・システムに不具合が発見されたり、脆弱性対策が必要になった場合の対応に関する要件が明確化され、それが妥当であるかを確認する。例えば、リモートアップデートなどの仕組みの要件や適用時の安全性、効率性を考慮しているかを確認する。また、IoT は様々な機器やシステムが多種多様なつながり方をするため、障害発生時の原因特定が困難になると想定され、障害の解析性を考慮しているかの確認も必要である。

② 安全安心に係わる監視機能の正常性の確認

安全安心に係わる監視機能により、IoT 全体の正常性が確認できることの要件、および、監視機能そのものが運用中に正常に動作することを確認するための要件が明確化され、それが妥当であるかを確認する。例えば、監視機能が IoT 全体のどの範囲をカバーしているか確認する。また、監視機能や回復機能、リモートアップデート機能などがシステム稼働中に正常動作するかを確認する仕組みがあるか、さらに、定期的に確認が必要な機能が明確になっているかなどを確認する。

③ IoT 機器の EoL や連携サービスの終了への対応

大量のセンサーなどを扱う IoT では、センサーの EoL（End of Life、製品が生産終了したこと）やバッテリ切れでの交換が大量に発生することが想定される。IoT 機器は、動作の保証期間が有限であるため、EoL やバッテリ期限を把握するための管理機能が必要である。また、連携したサービスも同様に終了することを想定し、サービス終了を把握する要件が明確化され、それが妥当であるかを確認する。

# 【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

## (1) 概説

開発段階で規定した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することが重要である。この評価では、実際の保守や運用を想定した多数のシナリオを用いることがある。これらのシナリオでは、装置の故障やセキュリティの劣化、大量の通信トランザクションなど、通常起こせない事象による評価も必要になる。そのため、評価環境として必要な擬似故障の発生ツールや大量の IoT 機器、大量データ発生のシミュレータなどの準備も必要となる。

ここでは、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。IoT としての市場への価値が提供できるかという判断になるため、大変重要である。

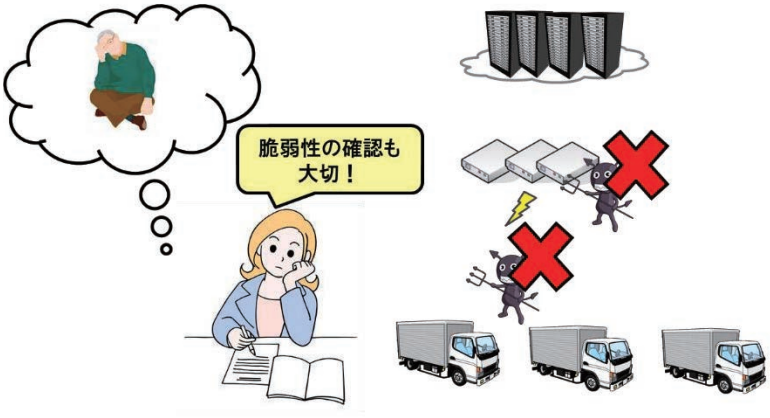



図 3-3 利用者の要求に合致していることを評価

## (2) 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**

IoT 機器・システムは、多種多様な使われ方をするため、その要求仕様や開発要件は、開発の上流でレビューが行われ、妥当性が確認される。しかし、開発段階の様々な制約や仕様の誤解などからすべての要件が的確に実装されていないかも知れない。そこで、要求仕様に基づく開発要件が確実に実装されているかの確認が重要である。なお、ここでは、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る。以下に、この妥当性確認の考慮点を示す。

① 評価シナリオの作成と合意

個々の機能を確認するのではなく、IoT 機器全体として、また、IoT システム全体として要件が満足しているかを確認するため、その評価のシナリオが重要となる。利用者の想定、使われるシーンや環境、使われる手順など、実際の利用場面（運用を含む）を考慮したシナリオを作成する必要がある。また、評価シナリオの十分性や判定基準も検討し、関係者間で合意することが必要である。なお、ここで確認する対象としては、視点２で挙げた妥当性確認の結果を反映したリスク低減策の確認も含むことが要求される。

② ツールの準備と評価要員の確保

安全安心に係わるセーフティ、セキュリティ、リライアビリティや性能などの要件を評価するために、例えば、負荷ツール、擬似故障発生ツール、ファジングツール、IoT 機器シミュレータ、ネットワークシミュレータなどのツールが必要となる。評価シナリオを実現するためのツール類の準備とツールを使いこなせるスキルを有する要員の確保が必要である。

③ 評価の実施と結果判断の合意

評価の実施においては、品質の説明責任が果たせるように評価結果のエビデンスを残すことが重要である。例えば、評価実施結果と合否判定結果、実行ログなどを残す。また、評価結果の判断が正しいことを関係者と協議し合意が必要であり、それらの合意形成の議事録などのエビデンスも残す。

# ＜コラム 3＞IoT 開発におけるレビューの勘所

国立大学法人名古屋大学　森崎　修司

普段のレビューではどのようにして欠陥を検出していますか？過去の情報や経験に頼ってレビューしている方が多いのではないでしょうか。組織標準や委託側から指定されたチェックリストがあり、それを使っているという方もいると思います。どちらの場合にも、過去にレビューで検出された欠陥や見逃された欠陥を参考にしています。

これから IoT への対応をはじめようとしている場合のように、対象ドメインでの実績がなく過去の経験に頼れない場合には、どうしたら良いでしょうか。本書のように欠陥がありそうな点や考慮が必要な点を集めた情報を参考にしたり知見を持っている方からアドバイスをもらったりするのが一般的な方法と言えます。

本来の目的が果たせるのかという視点から欠陥を見つける方法もあります。レビューでの欠陥検出を整理していくと、「こういう欠陥と同じような欠陥はないか」という具体的な欠陥を起点にして探す方法と、「こういう目的を果たそうとするときにそれを阻害する原因がないか」という保証内容を起点にして探す方法に大別できます。欠陥を起点にする方法が上述の過去の情報や経験に頼ったレビューです。機能定義漏れ、期待する性能が出ないといった過去の欠陥を起点にします。保証内容を起点とする場合、例えばスループットを一定内に抑えるという目的に対して、データの組み合わせやタイミングによっては非常に時間がかかる場合がある、スループットに影響を与える要因が多く簡単には予測できないといったことが阻害する原因になります。どちらの方法からでも同一の欠陥を検出できますが、実績が少ない場合には保証内容を考えることが欠陥検出につながることが多くあります。

IoT 開発では、センサーやデバイスからの情報を使って、利用者の利便性を高めたり、効率化して人手を介さなくても良いようにするといった目的があるはずです。そうした目的を阻害する要因がないかを確認します。例えば、センサーからの情報を使って消耗部品の予防保全を目的とする場合、予防保全のた

めに必要なデータの精度がある程度わかっている場合には、その精度を得るための仕組みや得られないときの対処方法が明らかになっているか確認します。他にも、ネットワークに接続されたセンサーやデバイスからの情報が正当な権限を持たない第三者によって改ざんされるといったことも保証内容を阻害する原因になります。


IoT 開発におけるレビューの勘所

## 3.3 IoT の特徴に着目したテスト設計

IoT では多数の機器・システムがつながり、その種類も様々である。また、IoT はライフサイクルが長く、その間の接続構成の変化が想定される。そのような IoT の特徴を考慮すると、単体の機器・システムよりもテスト実施が困難になることを認識しテスト設計を行う必要がある。例えば、テスト実施のためには膨大な数の組み合わせのテスト項目や大規模なテスト環境が必要となり、非現実的な場合もある。IoT では、テスト実施上の課題を検証担当者だけで解決するのではなく、開発担当者にテストのことを考慮した設計を求めることも重要である。なお、テスト設計時には、開発側の資料のレビューもあわせて実施し、論理の矛盾や曖昧な記述などの問題を早期に摘出することが重要である。

本節では、IoT の特徴やテスト環境に着目してテスト設計において考慮すべき視点について説明する。

# 【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

## (1) 概説

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る［14］。また、同じ IoT 機器でも様々なメーカの製品が存在し、そのつながり方も多様である。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る［15］。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る。

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ある。

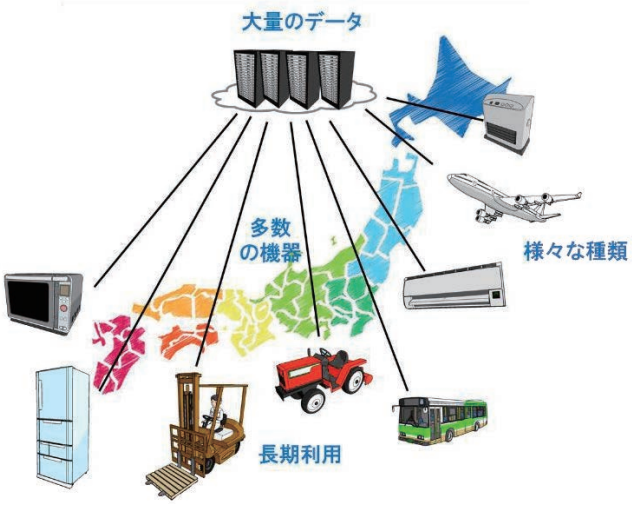



図 3-4 様々な種類の多数の機器の接続

## (2) 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**

① テスト設計時の考慮項目

IoT の特徴上、必要な機能や性能のテスト設計を行う場合に考慮すべき項目を以下に示す。

1) 最大接続数、データの最大量に関するテスト

IoT では多数の機器の接続や膨大な量のデータを扱う場合があり、境界条件に関するテストの中でも、特に想定される最大の接続数やデータの最大量に関するテストが重要である。また、これらの項目は、後述の性能に関するテストでも考慮が必要である。なお、設計仕様として IoT システムに接続可能なすべての種類の機器での動作確認は困難な場合があるので、動作確認済の機器をホワイトリストとして情報公開することも有効である。

2) 想定外のデータを取り扱う機能に関するテスト

IoT 機器の中には設計上想定していないデータを受け取る場合が考えられるため、そのようなデータを受け取った場合の処理についても確認する必要がある。例えば、想定外のデータとしてはデータの範囲やフォーマットの違いが考えられる。

3) つながる相手も含めた機能の充足性に関するテスト

IoT では、単体の機器のテストだけではなく、保証の範囲を確認し、機器やシステムが接続された状況において機能が充足できているか確認する必要がある。特に、つながり方の違いの考慮が必要である。これらを含めて、機器やシステム全体として所定の機能を実現しているかを確認することが望ましい。

4) 動作寿命に関するテスト

例えば、IoT では野外に設置されたセンサーなどのように電池交換なしでの長期間稼働が必要であり、消費電力に厳しい要求があるものがある。そのような機器やシステムの場合において、消費電力や電池寿命が設計範囲内か確認する必要がある。また、機器やシステムの中には常時稼働していないものもあり、省電力機能などを意識して待機中や稼働中など様々な動作パターンでの消費電力を確認するテストが必要である。

5) 性能に関するテスト

IoT では前述の最大接続数や最大データ量を取り扱う場合でも性能が満足するか確認する必要がある。例えばクラウドにおいて負荷に応じてオートスケールされる場合があるが、そのような場合にはオートスケール

の上限を把握してテスト設計を行う必要がある。また、つながる機器やシステム間で性能差がある場合、全体としては性能を満足していても、特定の箇所で性能が出ていないなどのボトルネックとなる箇所の把握も必要である。

② テストの実行性・効率性確認

1) テストの実行性

①で示したテスト実施のためには、多数の機器や大量のデータの用意が必要でテストが困難となる場合が想定される。そのため、接続性や性能の確認に必要なテスト環境の条件や仕様について明確にする必要がある。

2) テストの効率性

①で示したテスト実施のためには、膨大な数のつながるパターンやデータパターンなどの組み合わせによるテスト実施が必要となりテスト実施に長期間かかる場合が想定される。そのため、それらの実行期間を予測することが必要である。



**【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

IoT の互換性に関するテスト設計を行う場合に考慮すべき項目を以下に示す

1) 機能の互換性に関するテスト

IoT では様々な機器やシステムが接続されることが想定される。また、新規にシステムを構築するのではなく、既存の環境に追加する場合には、同一機器でも、様々なバージョンが存在する場合がある。そのため、テスト設計においては、様々な機器の種類（様々なバージョンを含む）を組み合わせたテスト設計が必要である。

2) 情報の互換性に関するテスト

機器の種類やバージョン以外にも、相互に情報の交換が可能かどうか互換性のテスト設計が必要である。また、これらの機器やシステムの中には、通信の規格に沿っていない場合があり、そのような機器と接続した場合の動作確認のテスト設計も必要である。

② テストの実行性・効率性

1)　テストの実行性

①で示したテスト実施のためには、機能や情報の互換性の確認に必要なテスト環境の用意が困難となる場合が想定される。そのための、テスト環境の条件や仕様について明確にする必要がある。

2)　テストの効率性

①で示したテスト実施のためには、多数のテスト対象機種やバージョンの組み合わせによるテスト実施が必要となりテスト実施に長期間かかる場合が想定される。そのため、テスト実行期間を予測することが必要である。

# 【視点 5】多種多様な利用環境や使い方に着目する

## (1) 概説

IoT では、利用者のスキルがシステム管理者レベルであったり一般利用者レベルであったり、同じシステムを提供しても使い易いと感じ取られる場合もあれば、逆の場合もある。また、移動する IoT 機器・システムなどの場合には、様々な利用環境（場所、シーンなど）の考慮も必要である。

上記のような IoT をテストすることを考えると、様々な利用者や利用環境を想定してテストすることが重要である。また、開発者による想定だけでなく、実際にどのように利用されているか利用状況を把握し、フィードバックして次版のテストに反映させることも必要である［16］。

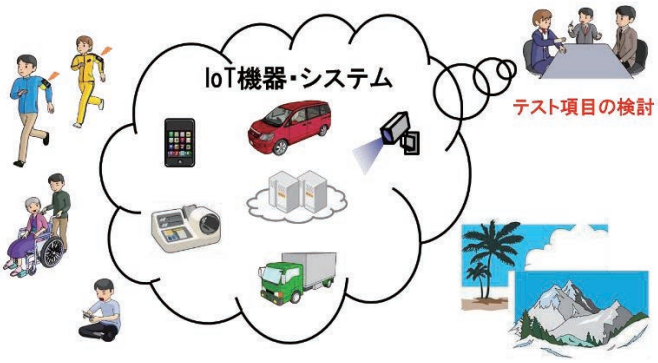



図 3-5 様々な利用環境や利用者の使い方に着目

## (2) 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**

① テスト設計時の考慮項目

利用者、利用状況、利用環境などを考慮したテスト設計を行う場合に考慮すべき項目を以下に示す。

1) 利用者、利用環境を想定したテスト

・ 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、管理者、運用者

これらは個別の項目でのテストではなく、組み合わせのテストの考慮も必要である。利用者に関しては、探索的なテストとして、仕様にはない利用者を想定したテストも考慮することが望ましい。

2) 利用状況把握やプライバシー保護に関するテスト
・ 利用状況把握：取得タイミング、取得箇所、取得データなど
・ プライバシー保護：暗号化、同意確認、匿名化などに関する保護対象データの種類・範囲など

② テストの実行性・効率性確認

1) テストの実行性

①で示したテスト実行のためには、想定した利用者や利用環境のすべては準備できない場合が想定される。そのため、利用者の立場で実利用に関する確認に必要なテスト環境の条件や仕様について明確にする必要がある。

2) テストの効率性

①で示したテスト実行のためには、膨大な数の利用環境パターンや利用シーンの組み合わせによるテスト実行が必要となりテスト実行に長期間かかる場合が想定される。そのため、実利用を想定したシーンのテストの組み合わせに関する実行期間を予測することが必要である。

# 【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

## (1) 概説

IoT では利用者による様々な機器・システムとの接続が行われるため、設計範囲外の機器との接続やデータ連携時にも意図された機能が維持できるか確認が必要である。

また、IoT システムの安全安心のためには機器・システムの障害/故障が発生しても意図した処理ができるか確認が必要である。しかしながら、障害/故障に関する機能のテストにおいて、実際にシステムの障害/故障を発生させることが困難な場合がある。

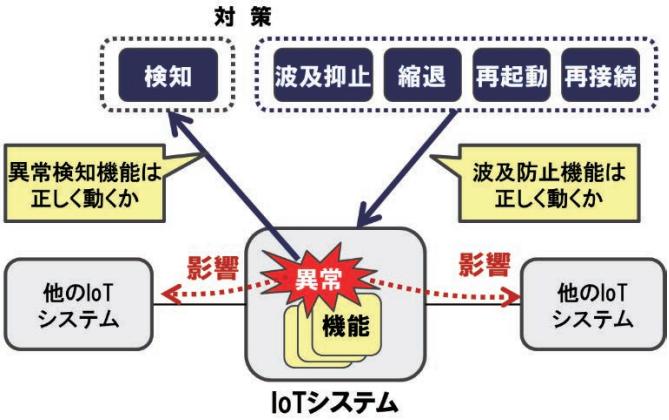



図 3-6 異常発生時の対策機能のテスト

セキュリティについては、IT システムと同様に、攻撃を受けた場合に検知して意図した処理ができるか、また、脆弱性が残っていないかなどのテストが必要である。それらのテストに加えて、特に、IoT ではセキュリティがセーフティに与える影響も含めてテストする必要がある。ただし、前述の障害/故障の発生同様に、実際に人体や財産に影響を与えるテストを実施することは多くの場合困難である。

これらのことを踏まえて、IoT の検証においては、擬似障害によるテストや、シミュレータの活用などの対策が必要となる。

## (2) 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**

① テスト設計時の考慮項目

設計範囲外の機器の接続やデータ連携、故障や異常に対するテスト設計を行う場合に考慮すべき項目を以下に示す。

1) 設計範囲外の機器の接続、異常データ発生に関するテスト

設計時に想定されている機器・システムだけでなく、設計範囲外の機器・システムが接続されたと仮定して設計された処理（エラーとして処理するなど）を発生させ、意図された機能が維持できることを確認することが必要である。また、つながる相手から正常なデータを受けるだけでなく異常なデータを受けた場合の処理の確認も必要である。

2) 機器・システムの障害・故障や通信の障害発生時の対応処理のテスト

一部の機器・システムの障害・故障や通信の障害を発生させて、設計された処理（検知、回復など）が動作するか確認が必要である。

3) 長期間の利用に関するテスト

長期間の利用を想定した場合、ソフトウェアとしてはデータ量の増加などによる資源枯渇や、ハードウェアとしては機器の劣化などの確認が考えられる。なお、SSD やフラッシュメモリーなど書き換え回数の制限がある機器は、リリース後に十分書き込みができるように、テスト時には制限回数に気を付けて、書き込み回数を抑えるなどの考慮が必要である。

4) 複数の IoT システムの競合に関するテスト

１つの IoT システムの中では正常な動作であっても、複数の IoT システムを接続した場合に、矛盾した処理となることが想定される［4］。このように競合が発生した場合においても優先度制御などにより意図された機能が実行できるか確認が必要である。

② テストの実行性・効率性確認

1) テストの実行性

①で示したテスト実行のためには、障害/故障、異常状態、競合状態など

の発生が必要でテストが困難となる場合が想定される。そのため、障害/故障、異常状態、競合状態などを発生させるテスト環境の条件や仕様について明確にする必要がある。

2) テストの効率性

①で示したテスト実行のためには、様々な構成での障害/故障、異常状態、競合状態などの組み合わせによるテスト実行が必要となりテスト実行に長期間かかる場合が想定される。そのため、テストの組み合わせに関する実行期間を予測することが必要である。



**【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**

① テスト設計時の考慮項目

1) セキュリティ攻撃の検知や脆弱性に関するテスト

IT システムと同様に、セキュリティに関して、侵入テスト、脆弱性のテスト、またファジングテストなどを行うことが必要である。なお、特に、IoT での利活用を想定していなかった過去の資産ソフトウェアやシステムを転用した場合や OSS などを活用した場合は、システムの脆弱性評価を検討することが重要である。これらのセキュリティに関するテストについては、CCDS の IoT セキュリティ評価検証ガイドライン［8］が参考になる。

2) 要求されたセキュリティやセーフティのレベルに必要なテスト

コモンクライテリアや EDSA ［17］、また機能安全などで定められたレベルについての要求がある場合は当該規格に従ってテストを行う必要がある。

3) セキュリティやセーフティのレベルが異なるシステム間のテスト

IoT では、制御システムと情報システムの接続など、セキュリティやセーフティのレベルが異なるシステム間の接続が想定される。個々のシステムのレベルに関するテストに加えて、システム全体として異なるレベルの機器が混在している場合の対応について、設計している内容を確認してテストすることが必要である。

4) セキュリティがセーフティに与える影響のテスト

従来はつながっていなかった機器やシステムがつながるようになった場合、もともと具備していたセーフティの機能に加えてセキュリティの対策が実施されることがある。そのような場合に、セキュリティ対策の追加によって、セーフティ機能の動作が損なわれないか確認が必要である。

5) 個人情報や企業の機密情報などの初期化のテスト

IoT 機器やシステムの破棄や譲渡時は、個人情報や企業の機密情報などを消去する必要があり、これらの情報を初期化する機能についてテストを行う。

② テストの実行性・効率性確認

1) テストの実行性

①で示したテスト実行のためには、セキュリティやセーフティに関する異常を発生させることが必要であるが、例えば人命や財産に影響を与えたりテストが困難となる場合が想定される。そのため、セキュリティやセーフティに関する異常を発生させるテスト環境の条件や仕様について明確にする必要がある。

2) テストの効率性

①で示したテスト実行のためには、網羅的な脆弱性の確認や、様々な規格への適合の確認が必要となりテスト実行に長期間かかる場合が想定される。そのため、脆弱性や規格への適合性について効率的に確認するためのツールの検討が必要である。

# 【視点 7】長期安定稼働の維持に着目する

## (1) 概説

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る。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ある。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る［1］。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であると、広範囲に影響を与える場合があることを考慮する必要がある。

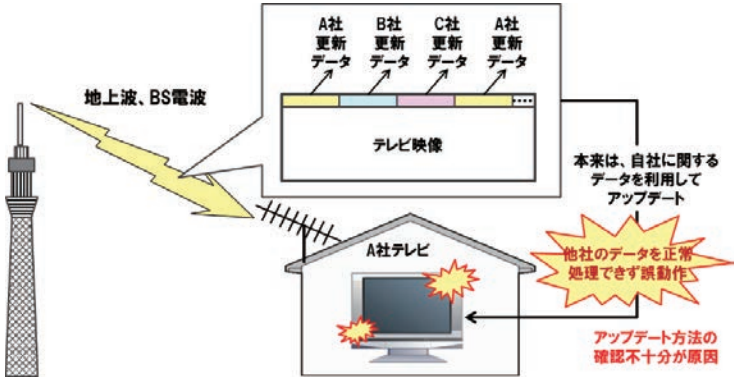



図 3-7 更新用データによるテレビの誤動作

## (2) 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**

① テスト設計時の考慮項目

IoT の長期利用における保守に関するテスト設計を行う場合に考慮すべき項目を以下に示す。

1) 障害解析に必要な機能の確認

機器・システムの障害、通信の異常や、セキュリティの攻撃を発生させ

て、必要なログが収集できるか確認が必要である。特にリソースの少ない IoT 機器の場合など、格納できるログの最大値に達した場合の処理の確認や、セキュアにログを転送するための機能などの確認が必要である。

2) アップデート機能の確認

アップデートが正しくセキュアに実施できるか確認する必要がある。特に IoT では管理者が常時監視していない場合があるため、自動アップデートが失敗した場合などに、自動的に従来バージョンで復帰するなど致命的な状態にならないことを確認することが必要である。

また、同時アップデートの最大数での確認を行い、ネットワークやシステムに与える負荷が設計範囲内であるかどうか確認が必要である。

② テストの実行性・効率性確認

1) テストの実行性

①で示したテスト実行のためには、ログ確認のために必要な障害の発生や、アップデート時の最大負荷の発生が困難となる場合が想定される。そのため、ログ確認のための障害やアップデートの負荷を発生させるテスト環境の条件について明確にする必要がある。

2) テストの効率性

①で示したテスト実行のためには、様々な通信の異常パターンやセキュリティの攻撃パターンでのテストが必要となりテスト実行に長期間かかる場合が想定される。そのため、通信の異常パターンやセキュリティの攻撃を発生させるためのツールの検討が必要である。

# 【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

## (1) 概説

視点 4 から視点 7 の「テストの実行性・効率性」では、テストに必要なテスト環境の条件や効率化に向けたツールなどを検討した。ここでは、それらの要件をまとめて、対策として考慮すべき事項について説明する。視点 4 から視点 7 に示した内容に基づいてテストすることを考えると、テスト環境の検討を後回しにすると準備が間に合わなくなったり、場合によっては開発の終盤になって見積もり以上にテスト環境の構築のためにコストがかかってしまうリスクがある。そのため、テスト環境についてはテスト設計段階から考慮することが必要である。また、IoT では、特にテストの種類や組み合わせが膨大な数になることも見込まれるためテスト効率化が重要である。


図 3-8 テスト設計段階からテスト環境や効率化を検討

## (2) 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**

① テスト環境の考慮事項

以下のような事項を考慮して、各テストで必要となるテスト環境を整理し、テスト環境の設計およびテスト環境構築手順、各種機材の操作手順の作成を行う。

1)　多数の機器が接続可能なテスト環境を検討
- 最大接続数を超えた機器
- 設計範囲内の様々な種類の機器、および設計範囲外の機器
- 様々な種類のネットワーク

2)　大量データや想定外のデータに関するテスト環境を検討
- 最大データ量
- 想定外のデータ

3)　障害/故障の発生に関するテスト環境の検討
- ハードウェア、ソフトウェア、ネットワークの障害／故障

4)　セキュリティ異常の発生に関するテスト環境の検討
- 機器・システム、ネットワーク、およびそれらで扱われるデータのセキュリティ

5)　その他のテスト環境の検討
- 時間短縮のための加速度テスト環境
- 性能の測定に関するテスト環境
- センサーなど省電力が要求される機器の電力の測定

②　手配できない場合の代替手段

1)　シミュレータやツールの手配
- 多数台接続や大量データのシミュレータ
- ハードウェアやソフトウェアの擬似的な異常の発生ツール
- ペネトレーション（侵入）、脆弱性スキャン、ファジングなどのツール

2)　テストできる場所やテストベッドの手配
- 他者が有するテスト設備の利用の検討（公的機関や業界が用意しているテスト環境など）

**【8-2】効率的なテスト方法を検討する**

注：下記に掲載した個々の検証手法の詳細については専門書を参考にしていただきたい。

①　テストの効率化

1)　テストの爆発の抑制（項目数の削減）

・ 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検討

2) テストの類似項目の整理

・ 同値分割などの手法の活用

・ テスト全体を眺めて、同様なテストや統合可能なテストを整理

3) テストの工数削減

・ テストデータの自動生成、テストプログラムの自動生成、テスト実行の自動化などを検討する。

4) 回帰テストの容易化

・ 効率的に回帰テストが可能な構成やツールの検討

# 【視点 9】テストのし易さと実施可能性を検討する

## (1) 概説

テスト設計の各視点の中でのテスト実行性や効率性の確認を行った結果として、開発担当者が設計した内容に対して効率的にテストが実施できない、あるいはテストが困難という場合も生じる。それらをそのままにしてテスト設計を行うと、計画以上にテストの期間がかかったり、テストが実行できないリスクがある。そのような場合に、テスト設計だけで解決を図るのではなく、開発に反映させることを検討することが重要である。


図 3-9 テストのために設計から見直す

## (2) 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**

テスト設計を実施する場合に、効率的なテストの実施が難しい場合や、テストが非常に困難な場合、設計内容について開発担当者に確認し、テストし易さや、テスト実行可能性を考慮した設計について考慮してもらえるよう開発担当者へ提案することが必要である［18］。

① テスト容易化設計（DFT）の提案

テストの容易化のための設計は、もともとはLSIの設計で検討された方法であるが［19］、ソフトウェア開発においても同様の考えは必要であり、IoTの場合は特に、以下の点に考慮することが必要である。

1) 設計時に制御や監視に関するインタフェースの統一・集約

機器やシステムが複雑に連携することが想定されるので、設計時に制御や監視に関するインタフェースを統一したり、集約したりすることが必要である。

2) アーキテクチャのモジュール化

アーキテクチャをモジュール化しテストの考慮範囲を局所化することが必要である。

3) テストに必要な機能の組込み

テスト実施時に外部からの障害発生が困難な場合があり、あらかじめ擬似障害を発生させるハードウェアやソフトウェアを組み込んでおくことも必要である。

4) その他のテスト容易化のための考慮内容

その他一般的に、実行時の異常な値の検出を容易化するためのアサーションやプログラム中に満たすべき要件を記述する Design by Contract などの活用も考えられる。

② テストが困難である場合の提案

1) 設計内容の見直しの提案

用意することができない数や種類の機器が必要であったり、利用の手配ができない場所が含まれていて、それらに対して、代替手段で対応できない場合には、検証（役割）の担当者は設計されている仕様について開発担当者へ設計内容の見直しを提案することが考えられる。

2) 保証する内容の見直しの提案

AI やビッグデータ解析などを活用していてテストの手法が技術的に確立できていない場合（例：センサー情報を集めて天気予報を行う IoT システムの場合、予報が正しいかどうか確認が困難）に、システムとして保証する内容について、検証（役割）の担当者は開発担当者へ保証する内容の見直しを提案することが考えられる（精度までは保証しないなど）。

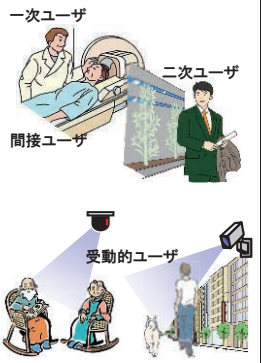
# ＜コラム 4＞受動的ユーザ

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

本書では IoT 機器・システムを利用する者を「利用者」と呼んでいる。しかし、単に「利用者」と言っても IoT 機器・システムとの係わり方は多様である。また、直接 IoT 機器・システムを利用しないが、間接的にその影響を受けている者もいる。

IPA/SEC では 2017 年 3 月につながる世界における「利用時の品質」について検討し、報告書［20］を公開している。そこでは、「ユーザ」という用語を用いているが、本書では「利用者」に相当する。上記の報告書の中では、ISO/IEC25000 シリーズ(SQuaRE)を参考にしてユーザの分類をした。先に述べた、間接的に影響を受けている者として、「間接ユーザ」と「受動的ユーザ」を分類したのが下の表である。つながる世界では、本人が意図せずに IoT 機器・システムによってサービスを提供されたり、逆に情報を取得されたりすることが増大する可能性がある。IoT 機器・システムの仕様検討や検証・評価の際は、これらの間接的にその影響を受けている者の存在も考慮すべきである。

**ユーザの分類**

| 名称 | 定義 | 左記のユーザ例のイメージ |
|---|---|---|
| 直接ユーザ | システムとインタラクションする人。一次ユーザと二次ユーザに区別される。 |  |
| 一次ユーザ | 主目標を達成するためにシステムとインタラクションする人。<br>例）医療機器を操作する技師。 | |
| 二次ユーザ | 支援を提供する人。例えば，次の人を言う。<br>a) コンテンツプロバイダ，システム管理者及び／又はシステム上級管理者，並びにセキュリティ管理者<br>b) 保守者，分析者，移植者，設置者<br>例）医療機器の保守担当者。 | |
| 間接ユーザ | システムと直接インタラクションしないが，出力を受け取る人。<br>例）医療機器で検査される患者。 | |
| 受動的ユーザ | 本人の意図に関わらずシステムの影響を受ける人。<br>例1）見守りシステムで見守られる高齢者。<br>例2）監視カメラに写る通行人。 | |

出典：つながる世界の利用時の品質～IoT 時代の安全と使いやすさを実現する設計～、IPA/SEC

## 3.4 IoT の効率的なテスト実施

テストの実施のためには、前節でテスト設計された内容に従ったテスト環境の構築が必要である。また、テストは限られた期間内で完了させることが必要であり、特に有償の機材やテストベッドなどを活用する場合、テストの効率化が重要である。さらに、リリース後のトラブル発生時に品質に関する説明を求められる場面を想定すると、テストのエビデンスを残しておくことが重要である。

本節では、IoT のテスト環境の整備や効率化に着目したテスト実施において考慮すべき視点について説明する。

# 【視点 10】テストを効率的に実施し、エビデンスを残す

## (1) 概説

テスト環境の利用や要員の確保には制約があり、3.3 でテスト設計されたものを、テスト実施時に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の検討を行い効率的にテストを実施することが重要である。また、IoT では様々な機器やシステムが連携されているため、障害発生時にそれぞれの機器やシステムに問題がないか説明を求められることが想定される。このような場合を想定しテストの結果のエビデンスを残すことが重要である。

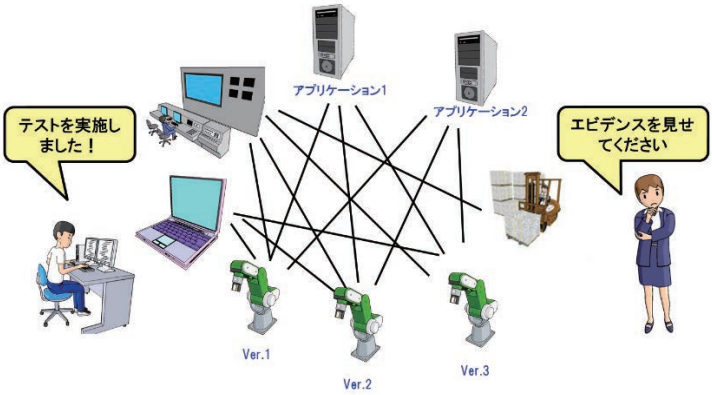



図 3-10 テストのエビデンスを残す

## (2) 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**

① テスト効率化の考慮項目

以下の事項を考慮したテスト実施の効率化が必要である。

1) テスト環境に着目したテストの実行順序

テスト設計した内容に沿ってテストを実施できる環境を構築するには、様々な機器やシステム、ネットワークと、それらを設置可能な場所をテストに必要な期間において確保する必要がある。機器やシステムを代替

するためのシミュレータなどが必要な場合、それらの機材の手配や、自社だけでテスト環境が構築できない場合はテストベッドの手配などが考えられる。しかしながら、こうした機材やテストベッドなどを利用するにはコストがかかる。そのため、手配した環境でしか実施できないテストを優先的に実施し、手配する期間を短縮できるようにテストの実行順序を考慮する必要がある。

2) 対象となる機器やシステムの組み合わせ

3.3 で設計した個別のテストを無計画に実施するのではなく、同じ組み合わせ（機器の構成）下で実行されるものをまとめることにより準備の時間を短縮できる可能性がある。特に、テスト設計で作成したシナリオごとにテスト環境が異なる場合など組み合わせを考慮した複数のテストをまとめることが望ましい。



**【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**

① テスト実施上の考慮項目

1) 品質の説明責任を果たすためのエビデンス

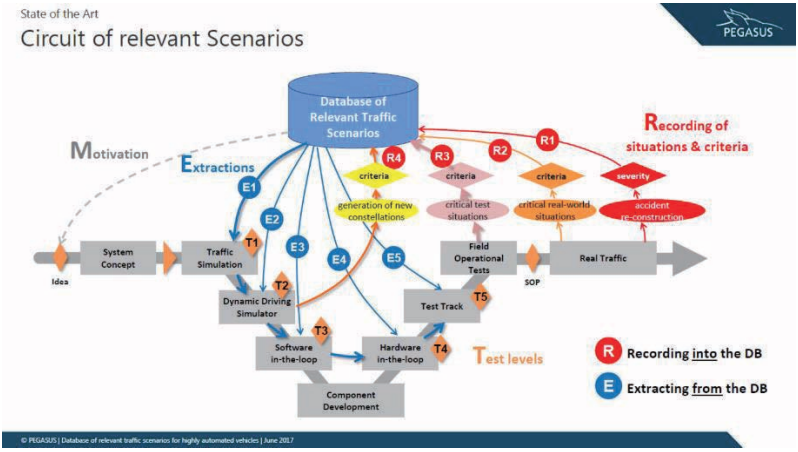
テストの結果をエビデンスとして残すことは重要である。IoT では特に、リリース後のトラブル発生時に品質に関する説明を求められることが想定されるため、保証範囲における実施結果を説明できることが重要である。テストのエビデンスを残す場合に合否判定の結果だけでなく、合否を判断した仕様との差や性能差などの付加情報を残しておくと、説明が求められた場合に活用できることが想定される。

また、テスト実施した結果については、開発担当者を交えて確認することが必要である。特に使用性など主観的な判断が行われる場合はテスト設計時になるべく曖昧にならないようにするだけでなく、体感など、判断した内容について、開発担当者を交えて確認することが重要である。なお、利用者の誤使用を避けるために、テストの確認結果などから使用できる範囲や条件をマニュアルなどに明示することも重要である。

# ＜コラム 5＞自動運転に向けた新たな検証の枠組み

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

独国の自動車産業界を中心に、自動運転車の型式認証を想定して、実利用・実運用情報を活用する新たな検証・妥当性確認の枠組み構築を目指す Pegasus プロジェクトが 2016 年末よりスタートした。IoT や AI を活用した新しい概念の製品・サービスでは、実利用時・実運用時の利用形態・利用状況を開発時に適切に想定するのが困難である。そのため、開発者の想定した範囲を超えた利用による想定外の障害や事故が発生するリスクが従来製品・サービスと比べて高い。AI を搭載する自動運転車も同様の課題を抱えている。実際、海外では開発時に想定しない状況での事故が発生している。




出典： 独 Pegasus プロジェクト公開資料より抜粋

http://www.pegasus-projekt.info/en/information-material?file=files/tmpl/pdf/AVT%20Symposium%202017%20Database%20traffic%20scenarios_Folien.pdf

**独 Pegasus プロジェクトが構想する検証の枠組み**

Pegasus プロジェクトでは、実利用・実運用情報から、クリティカルな利用・運用情報、事故が発生した利用情報・運用情報を抽出し、検証のための利

用・運用シナリオをデータベースに蓄積（図中Rの箇所）。データベースの利用・運用シナリオを開発時（含む更新・保守）の検証に用いることで、障害・事故の再発防止を確実にしていく（図中Eの箇所）。企業の枠を超えて産業界全体でデータベースを共有することにより、1社で発生した障害・事故を産業界全体でも再発させない枠組みである。Pegasusプロジェクトの基本的な考え方は自動車分野以外にも適用可能で、新しい概念の製品・サービスの社会的受容性の醸成・確保にも有効である。

## 3.5 IoT の品質を維持・改善するための運用計画立案

IoT 機器・システムは、開発段階で妥当性評価や検証により、リリース前に品質を確保するが、IoT はリリース後も様々な変化が想定され、運用時の品質の維持が重要となる。ここでの運用時の品質とは、IoT 機器・システムが本来提供する機能や性能などの品質維持に係わる事項と、ソフトウェア更新時の手順確認などの運用オペレーションの品質維持に係わる事項との 2 つと捉えることができる。IoT の運用時の品質を維持するためには、時間の経過とともに変化する様々な事象を想定し、点検や診断、保守のための修正・改善や訓練などの計画の策定が必要となる。

本節では、IoT の運用時の品質の維持・改善に向けた計画の策定において考慮すべき視点について説明する。

# 【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

## (1) 概説

IoT は、リリース前には想定していなかった IoT 機器のつながりや利用環境の変化、IoT 機器の EoL や連携サービスの停止・終了などがあり得るため、その運用への影響などの確認が必要となる。また、利用者が使う本来の機能が正常に動作していることに加え、IoT の安全安心に係わる異常監視機能などが意図した動作をしているかの診断、装置の切り替え機能など正常時には動作しない機能の定期的な点検や訓練が必要となる。また、IoT 機器・システムの動作に重要な影響を与えるソフトウェアの不具合や脆弱性の対応などの更新の適用は、運用プロセスの策定とリスクを考慮した適用順序、利用者への事前告知などが必要である。

IoT の品質を維持するためには、時間の経過とともに変化する要素を洗い出し、それらの状況をいつどのように確認するかの運用計画の立案が重要である。また、運用品質が維持されていることを定期的に評価し、運用品質の状態を確認することも重要である。

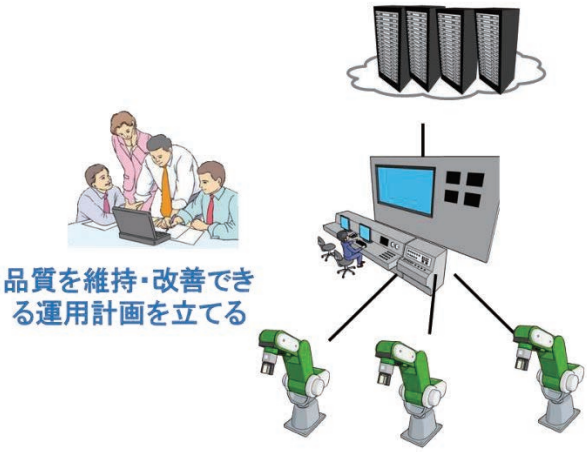



図 3-11 変化を想定した運用計画を立てる

## (2) 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**

IoT の運用においては、①リリース後の変化要素を洗い出し、その影響を考慮した改善を行うこと、②定期的な品質の確認・点検作業を行うこと、③不具合の発生などを想定して対応プロセスを確立しておくこと、④情報公開やクレーム対応が重要である。

① リリース後の変化要素の洗い出し

IoT は、リリース後に様々な変化が起こり得るが、それらをできるだけ網羅的に想定することが、重要である。また、運用を担う組織として、IoT の変化を想定し対策を練ることができる人材の確保が必要である。特に、セキュリティの脅威は、時間の経過とともに増加する傾向があるため、システム更新時や新たなシステム連携時などに脅威分析をやり直すことを計画することが必要となる。

② 定期的な品質の確認・点検作業の計画

リリース後の変化要素に対して、運用時の品質を維持するための点検や診断、訓練に関して、いつ誰がどのように実施するかの実行計画を立てる。適用に必要なツール類や要員（スキル）、標準実施時間、標準スケジュールなどを検討する。なお、計画どおりに実施できないときや対応が遅れるときを想定し、社会や利用者に与える影響やリスクを考慮することが必要である。

③ 不具合の発生などを想定した対応プロセスの確立

リリース後の不具合などの発生に対して、迅速に対応できるプロセスの確立が重要である。例えば、IoT の関係者との役割を明確にし、問い合わせルートの確立や協力体制の合意なども必要である。また、不具合の影響レベルごとの利用者への連絡方法なども決めておく必要がある。

④ 情報公開やクレーム対応

利用者からの情報公開請求やクレームに関して、どのような対応を取るかについて、対応プロセスとエスカレーション（事業責任者などへの連絡）のルールを決めておくことが重要である。また、IoT は、マルチベンダー機器で構成されることが多いため、利用者の立場で解決となる解を提供できることが望まれる。

**【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**

IoT の運用計画が適切に実行され、運用品質が維持できていることの評価が重要である。また、その評価の結果を運用計画や関係者にフィードバックし、PDCA サイクルをまわすことが必要である。

① 運用品質の評価項目の抽出と評価基準の策定

運用品質に係わる事項を洗い出し、それらの事項を評価するための基準を定めることが重要である。例えば、一般的に運用品質としては、インシデント対応や SLA（Service Level Agreement）などがあるが、IoT の特徴を捉えて運用に関する品質項目を定め、何をどのように測定し判定するかなどの評価基準を設定しておくことが必要である。

② 運用品質の評価とフィードバック

運用品質の評価項目を定期的に測定し、運用品質が維持されていることを評価基準に従って確認する。IoT では、関係者が多いため、運用での評価結果を関係者へフィードバックすることも重要である。なお、運用品質の評価結果から、クレームや障害対応などの短期改善項目を把握するだけではなく、利用者が継続的に利用できる状況にあるかなど長期改善項目を把握し、次期開発などにフィードバックすることも重要となる。例えば、DEOS 協会では、企画・開発から保守・運用に関して、変化に着目したオープンシステムディペンダビリティの国際規格（IEC62853）の制定と、それを基にした DEOS ライフサイクルモデルを定義しており、その具体的な展開のための活動を行っている。［21］

## 3.6 長期利用での品質維持と改善

IoT のリリース後における品質を維持するためには、前節で述べた運用での計画を確実に実施することが重要である。

本節では、IoT の実利用の場面における IoT 機器・システムの機能の維持と変化への対応などにおいて考慮すべき視点について説明する。

# 【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

## (1) 概説

IoT では、リリース後に想定外の IoT 機器の接続やセキュリティの劣化などが起こり得るため、運用での点検や診断、訓練などが重要である。特に、IoT 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働いていることの確認が重要となる。2015 年 12 月に発生したウクライナ発電所を狙った「BlackEnergy」［22］と呼ばれるマルウェアによる攻撃では、まず、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した。その影響で、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 万人に影響が出たと言われている。この例のように、悪意ある攻撃者の攻撃パターンも高度化しており、安全安心に係わる監視機能などが正常に動作していることの確認が重要になってきている。

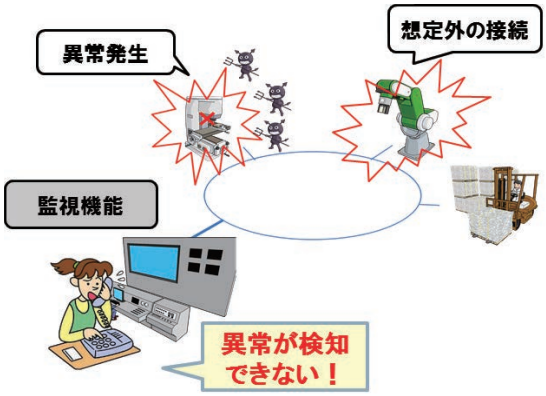



図 3-12 異常検知機能の維持確認は重要！

IoT のリリース後の品質を維持するためには、視点 11 で策定した運用時の検証計画を確実に実施することが重要である。視点 12 では、特に、IoT 機器・システムの利用環境の変化や技術動向の把握、安全安心に係わる機能の確認に着目して、考慮ポイントを説明する。

## (2) 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**

IoT の利用環境の変化と最新の技術動向を把握し、その影響を確認し必要に応じて対応する。

① 利用環境の変化の把握と対処

利用環境の変化への影響を確認し、対応が必要である。

例えば、IoT 特有の変化としては、以下が想定される。

- 想定外の利用者や IoT 機器の接続（悪意がある場合を含めて）
- 利用者の拡大や連携サービスの拡大による性能への影響
- IoT 機器の EoL や連携サービスの停止・終了（想定外も含む）
- 経年変化による IoT 機器の故障やセキュリティ異常
- 構成部品のセキュリティパッチやソフトウェア修正
- IoT 機器・システムの拡大による脅威（脅威分析の再実施）
- 自らの変化によるつながる相手への影響

② 技術情報の変化の把握と対処

IoT 機器・システムが利用している OSS を含むソフトウェアなどの更新情報や脆弱性情報、法改正などのルール変更は、開発側と運用側が連携して両方で確認することが望ましい。それらの変化が IoT 機器・システムに影響がないか確認し必要に応じて対処を行う。特に、プライバシー情報を扱う IoT では、国内外の法規制が変化する可能性もあり、対応が必須になる場合もある。

**【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**

IoT のライフサイクルにおいて、利用者に提供している機能や性能が満足できているか、安全安心に係わる機能が目的を達成できる状態にあるか確認する。なお、この運用状況の確認において、利用者に影響する問題や改善点が見つかれば、速やかに関係者に連絡し、フィードバックを行うことが重要である。

① 利用者に提供している機能・性能の確認

本来、利用者に約束している機能や性能が満足できる状況にあることを確

認し、必要に応じて情報公開する。例えば、利用状況を定期的に取得し、機能面や性能面の状態を分析し、稼働状況の Web 公開や利用者へ通知する。特に、利用者への影響の有無の確認として、セキュリティ攻撃や IoT 機器の故障などが起きていないことを監視する必要がある。

また、IoT では、ID やパスワードをデフォルトのままで利用すると外部からの侵入などのリスクが高いため、利用者に正しい設定を行うよう促すことが重要である。2016 年 1 月に世界中のネットワークカメラがパスワード未設定により、見放題になっていることがロシアのサイトから公表され、大きな問題となった。

② 安全安心に係わる機能の確認

安全安心に係わる機能の中には、正常時に動作しているものだけでなく、異常時しか動作しないものもあるため、定期的な動作の確認が必要である。例えば、IoT の障害監視機能、ログ収集機能、ウイルス対策機能、診断機能、縮退機能、停止機能などがあり、これらの機能が維持できていることの確認が必要である。また、利用者の稼働には直接影響しないデータのバックアップ機能などが正常に動作していることの確認も必要である。なお、IoT 機器・システムの更新や他システムとの連携強化などの変化があるときは、脆弱性を確認するテストなどを実施することも有効である。特に、UI を公開していない IoT 機器においても、無防備なバックドアなどが容易に推測できる状態で存在しないか確認することが望ましい。

# 【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

## (1) 概説

IoT は、新しいビジネス分野や産業分野で適用が進むと想定され、スモールスタートで知見を獲得しながら拡大していくケースも多いと考えられる。この場合は、仕様変更や機能追加など、アップデートが繰り返されるため、利用者や他の接続されている機器への影響などの確認が重要となる。さらに、IoT のシステム連携などが進展すると自システムの変更がつながる相手に対して、どのような影響があるかの確認も重要となる。

IoT のリリース後の不具合対応や機能追加などのアップデートでは、つながる相手や利用者への影響を事前に把握し、影響がないことを確認することが求められる。

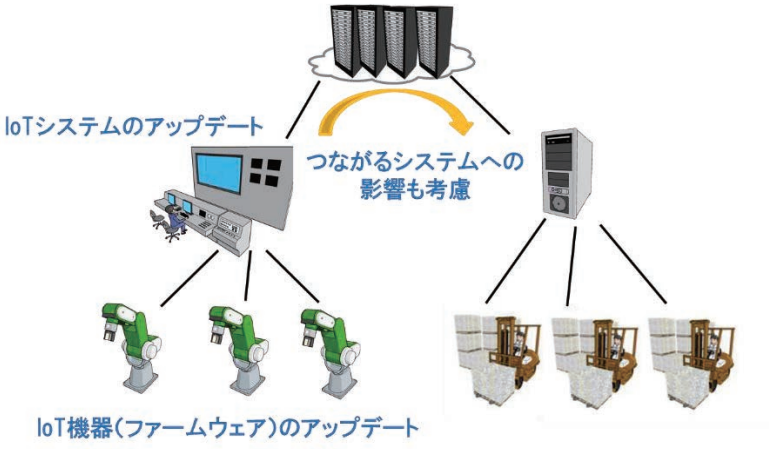



図 3-13 アップデート時は他への影響も考慮

## (2) 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**

IoT の不具合修正や機能拡張などのソフトウェア更新では、適用現場の状況を把握し、つながる相手への影響を確認することが重要である。一般にソフト

ウェアの更新データの確認は、開発側で実施されるが、現地の環境や構成に依存する場合もあり、運用側での検証も必要である。

① 接続相手への影響確認

IoT は多種多様な IoT 機器や様々なつながり方があるため、通信プロトコルのバージョン変更や新規プロトコルを追加する場合などでは、つながっている機器や利用者への影響を確認する必要がある。また、つながる相手との処理性能の差の拡大による影響など、性能に着目した確認も重要である。ただし、実環境での確認にはリスクがあるため、実環境に近い確認環境をいかに準備するかが、ポイントとなる。

② 多数台つながっている場合の影響確認

IoT 機器が多数台つながっている場合は、通信路の帯域性能の影響も考慮して、ソフトウェア更新の適用の順序やタイミングを決めることが重要である。また、適用の手順を事前に確認し、適用要員のスキルや理解度も含めて問題がないことを検証しておくことも重要である。

③ アップデート失敗への考慮

ソフトウェア更新は、現地の様々な条件により、アップデートが失敗する場合や更新により動作が不安定になる場合もあり、そのときのリカバリーの手順を事前確認しておくことが重要である。特に、人命や財産、社会的な影響が大きい IoT では、早急な回復が求められ、ソフトウェア適用失敗時のリカバリーや原状回復の手順の確認が重要である。

④ 運用手順の訓練

IoT の品質維持に関する様々な運用手順に関しては、定期的な実施訓練が必要である。例えば、障害が発生したときの回復手順やアップデートの適用手順、アップデート失敗時の回復手順などがある。また、IoT の様々な変化に対して、運用手順の定期的な見直しも必要となる。

# 第4章
# 本書の適用検討事例

本章では、本書でまとめた IoT の品質を確保、維持・改善するための「考慮ポイント」を、想定したユースケースに適用し、本事例による特徴的な IoT の考慮ポイントを示した。

# 4.1 戸締り競合制御システムの開発への適用

ここでは、想定するユースケースに対して、本書の視点・考慮ポイントを適用した事例を示す。適用したシステムについては、「『つながる世界の開発指針』の実践に向けた手引き」［4］付録 A UC4 を参照されたい。

## 4.1.1 システム概要

### (1) 想定するユースケース

既に快適性制御システムを導入し現在運用中のスマートホームに、新たに防災/防犯システムを追加導入することになったユースケースを想定する。快適性制御システムは A 社が提供したが、防災/防犯システムは B 社が提供し運用することとなった。A 社製の快適性制御システムと B 社製の防災/防犯システムという異なる IoT システムが、スマートホーム内で並行して運用される。B 社が防災/防犯システムを独自に（A 社の協力を得ないで）開発し、導入運用する場合について検討した。

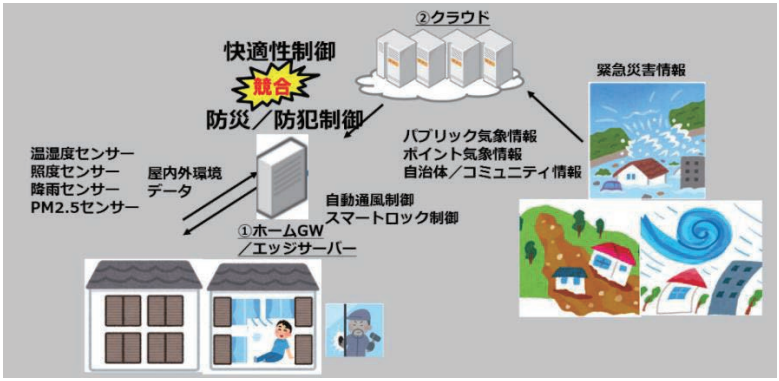



図 4-1 スマートホーム

### (2) 快適性制御システムの機能概要

屋内外の環境状態に合わせ屋内を快適な状態に保つ IoT システムであり、下記の制御を行う。

- 温湿度センサー、照度センサー、降雨センサー、PM2.5 センサーなどによる空調制御、日差し制御、自動通風制御
- 屋外のスマートフォンからクラウド経由での空調機の電源 ON/OFF 制御

## (3) 防災/防犯システムへの要求項目

地震、台風、ゲリラ豪雨などの災害に対応でき、空き巣や強盗などの犯罪に備える IoT システムを開発、保守・運用する。

- 夜になったら窓・雨戸を閉める。玄関扉を施錠する。
- 自治体などからの緊急災害の避難指示や地震速報などが出た場合、避難経路確保のために窓・雨戸を開放し玄関扉の鍵を解錠する。
- 台風やゲリラ豪雨、竜巻の予報が発生した場合、窓・雨戸を閉める。
- 屋外侵入を感知したら、窓・雨戸を閉め玄関扉を施錠し、警備会社に通報する。
- 玄関扉鍵のこじ開けを感知したら、警備会社に通報する。
- 玄関扉の鍵の施錠・解錠はスマートフォンから手動でもできる。
- 並行して運用される既存のサービスに影響を与えないようにする。
- IoT のセキュリティを確保する。

ただし、窓・雨戸は開閉のみで閉めるとロックされ、玄関扉は鍵の解錠・施錠のみで扉の開閉は人が行うこととする。

## (4) 想定される脅威/被害

① 窓、雨戸、玄関鍵などの制御の競合

1) 防災/防犯システムと快適性制御システム間の競合

快適性制御システムからの晴天時の窓・雨戸の開放

防災/防犯システムからの屋外侵入者感知時の窓・雨戸の戸締り

2) 防災/防犯システム内の競合（宅内と外部システム連携）

外部システムからの緊急災害時の避難経路確保のための窓・雨戸の開放、玄関扉解錠

防災/防犯システムからの屋外侵入者感知時の窓・雨戸の戸締り、玄関扉施錠

3) 外部システムからの矛盾する情報による防災/防犯システム内の競合

外部システムからの地震速報受信時の避難経路確保のための窓・雨戸の開放、玄関扉解錠

外部システムからの竜巻情報受信時の窓・雨戸の戸締り、玄関扉施錠

② 他システムとの無線の影響

防災/防犯システムの Wi-Fi 2.4GHz 帯域通信と他システムの異なる無線

通信（Bluetooth のオーディオシステムなど）の干渉

③　ホーム GW および防災/防犯コントローラの脆弱性脅威

制御ソフトウェアへの悪意のある攻撃により、窓・雨戸・玄関扉鍵の開閉制御が不能になる

④　クラウドサーバのサービス停止

- クラウドサーバからパブリック気象情報・ポイント気象情報・自治体/コミュニティ情報の提供が停止
- クラウドサーバのログデータ蓄積機能が停止

⑤　通信データ改ざん

- クラウドサーバとホーム GW 間の通信データ改ざん
- ホーム GW と防災/防犯コントローラ間の通信データ改ざん
- 防災/防犯コントローラと窓・雨戸・玄関扉鍵などの制御機器間の通信データ改ざん

## (5) システム構成

前記の情報を基に防災/防犯システムを追加した構成図を図 4-2 に示す。赤枠で示した部分が、新規に追加される部分である。

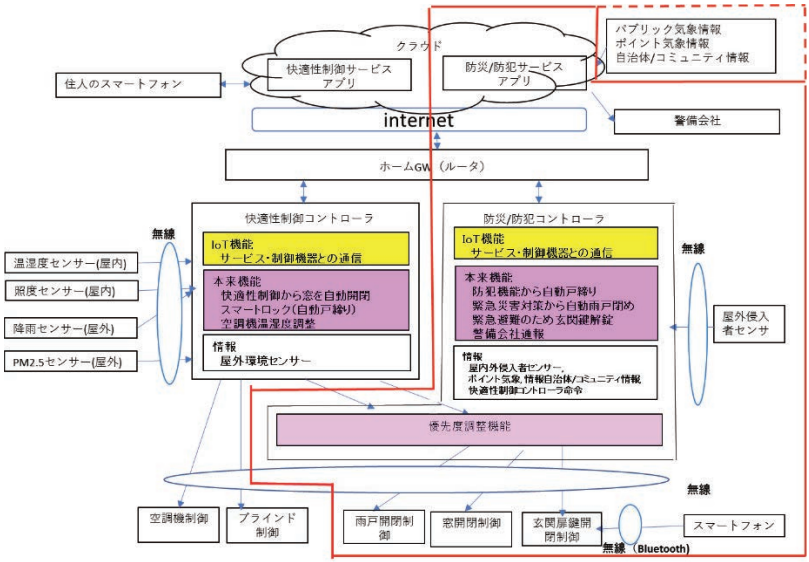



図 4-2 システム構成

### (6) システムの開発チームと検証チームの想定

開発チームは、新規に発足した他事業部門との混成チームであり、IoT 開発の経験が少ないメンバーで構成されていると想定。また、検証チームは、IoT の知識や検証スキルは有するが、無線ネットワークの検証スキルを有するメンバーはいないと想定。

## 4.1.2 適用検討事例

本ユースケースのシステムの品質確保、維持・改善のために本書の第 3 章で記載した視点・考慮ポイントを検討した結果を以下に示す。なお、ここでは、本事例として考慮すべき特徴的な事項のみを掲載する。抽出した事項の一覧は付録 A に掲載する。

### (1) V&V マネジメント（視点 1 の 1-1、1-2 を検討）

① 検証・評価方針（視点 1:1-1）

本 IoT システムの特徴や開発チームおよび検証チームの特性を考慮し、以下の検証・評価の方針とした。

1) 検証チームの参加のタイミング

本開発は、防災/防犯を目的とした社会的な影響が大きいプロジェクトであること、および、開発チームが IoT の開発経験が少ないことが判明したため、システムの早期品質確保、開発の効率化を目指し、開発要件や要求仕様のレビューなどの上流工程から参画することにした。なお、テストプロセスとしては、検証業界で定義している IVIA のテスト標準工程[23]を採用する。

2) 検証・評価の重点ポイント

本 IoT システムの特徴と社会的な影響を考慮し、以下の 3 つを検証・評価の重点ポイントとした。

・ 既存の快適性制御システムと新規に追加する防災/防犯システムの IoT デバイスの競合や干渉に着目する。雨戸や窓、玄関扉の IoT デバイスは、両方のシステムから制御され、競合が発生するため、優先度調整機能を設けており、そこに着目する。また、快適性制御システムの温度や降雨センサーなどは、無線で接続されており、新規に追加する防災/防犯システムの屋外侵入センサーとの干渉が起こり得るため、既存

のシステムとの影響に着目する。

- 防災/防犯システム自体のセキュリティ対策に着目する。本システムは、家屋の災害や空き巣などの犯罪の予防が使命であるため、本システムそのものの機能を守ることが重要である。本システムの脅威分析やリスク対策、脆弱性などのセキュリティに着目する。
- パブリック気象情報や自治体/コミュニティ情報などの外部システムとの連携に着目する。例えば、パブリック気象情報システムとの連携において、悪意ある改ざんなどで誤った情報が送られて来ると、利用者に悪影響を及ぼす可能性があるため、なりすましなどを防止するためのシステム相互間の認証やアクセス制御などに着目する。

② 検証・評価計画（視点 1:1-2）

1) 検証対象・範囲

- 上記①で挙げた「検証・評価の重点ポイント」を中心に、妥当性確認と検証を実施する。また、本システムは、稼働後の品質を維持するために、保守性や運用性に着目して、機能や性能の保証に関する検証を実施する。
- 制御機器やセンサーなどの購入品について、品質評価基準を調査し、B 社の基準との準拠性を確認する。電波法などの認定基準があるものは認定の取得を確認する。

2) 体制・要員の確保

- 今回の検証チームは、IoT の知識や検証スキルがあるが、無線ネットワークに関する知識を有する検証要員がいないことから、外部の無線ネットワークの検証専門エンジニアを確保することにした。

3) テスト環境

- 社内設備では準備ができない大規模なテスト環境は、公的機関や業界が用意しているスマートホームの実験環境を利用する。なお、テスト環境の利用に関して、借用設備の費用なども概算し、検証・評価の費用として計上する。

## (2) 妥当性確認（視点 2 を検討）

① IoT 特有の機能や性能（視点 2:2-1）

- 既存システムで制御している扉や窓の IoT デバイスの競合を避けるため

に新規に開発する優先度調整機能が、利用者の意思や生命・財産に与える影響を考慮した優先制御ができるかについて、開発要件を網羅的に確認する。

・新規に開発する屋外侵入センサーが、既存の屋外センサーなどの無線による制御と競合しないことを仕様上、考慮していることを確認する。

・外部連携システムの休止や停止の想定や、さらに、自システムへの影響についての対応要件を確認する。

② 利用環境や利用者の使い方（視点 2:2-2）

・利用者についてはシステムを操作できない高齢者や幼児も想定し、受動的ユーザ（コラム 4 参照）の安全を意識したシステムになっていることを確認する。

③ ライフサイクルでの安全安心の確保（視点 2:2-3）

・本システムは、人命や財産に影響を与える可能性があるため、開発システムが達成すべきセキュリティレベルが明確になっているか、また、システムとしてのセキュリティの脅威分析とその対策が明確であることを確認する。

④ 運用時のトラブルシューティング（視点 2:2-4）

・本システムは、既存システムや外部システムとの連携があるため、障害の切り分けが難しいことが想定される。運用時の障害の解析性を向上させるために、ログの強化を提案する。例えば、ホーム GW とクラウド・制御機器・センサー間の通信ログを仕様に盛り込む。

## (3) 検証（視点 4、視点 6 を検討）

① IoT 特有の機能と構成（視点 4:4-1、4-2）

・複数の機器が追加/取り外しされることや、長期間使用されることを考慮した検証を行う。

・センサー類の追加などを考慮して、仕様上の最大台数にて動作や管理に支障がないことを検証する。その際、PC やスマートフォンなどシステム以外の無線 LAN 機器および Bluetooth 機器が動作している環境で問題が発生しないことを検証する。

・機器ごとにデータの精度が異なるケースを想定し、許容誤差や不定データを受け取った場合について検証する。

・制御システムの競合テストにおいて、イベントが同時に発生した場合でも優先順位が守られることを検証する。

② IoT の障害/故障やセキュリティ異常（視点 6:6-1、6-2）

・外部システムとつながることによって高度なシステム連携となることから、クラウドやネットワークの停止・停電などを考慮した検証を行う。

・容易に追加/取り外しができるセンサー機器を使用しているため、使用を停止する場合（譲渡、廃棄、故障）において、セキュリティの脅威（個人情報の流出など）やセーフティを考慮した機能となっていることを検証する。

・異常時やエラー発生時に適時利用者にアラートを出せるかについて、検証する。

## (4) 運用マネジメント（視点 11 を検討）

① 運用計画（視点 11:11-1、11-2）

・他システムとの相互影響があるため、運用責任範囲を定め、不具合発生時の連携方法を明確にしておく。

・防災/防犯システムと快適性制御システムが相互に影響する機能である優先度調整機能が正常に動作することを運用中に確認する方法を検討し、定期確認の計画に盛り込む。

## (5) 運用実施（視点 12、13 を検討）

① リリース後も機能が維持されていることの確認（視点 12）

・防災/防犯システムと快適性制御システム以外のシステムの導入や想定外の GW が接続されていないか、利用環境の変化を確認する。

・運用計画に従って、定期的にシステム間の競合を制御する優先度調整機能に影響が出ていないことを、ログなどから確認する。

② システムの不具合対応や機能改善（視点 13）

・ソフトウェアを更新する場合、運用計画に基づきテストを実施するとともに、ソフトウェアの更新が失敗した場合を想定し、復旧方法や他システムへの影響を最小限にするための対応方法を確認する。

# おわりに

IoT の世界では、様々な機器やシステムがつながることにより、これまでになかった便利な世界が期待される。一方で、IoT の安全安心を確保しないと社会が混乱するリスクがある。独立行政法人情報処理推進機構 技術本部 ソフトウェア高信頼化センター(IPA/SEC)では、リスクに対応するために「つながる世界の開発指針」を策定し、開発者が考慮して欲しい重要なポイントを明確化してきた。

一方、産業界では、IoT 機器・システムの開発が進められつつあるが、IoT の品質確保について正面から解説したガイド類は見当たらず、現状は、IoT セキュリティに関するものがわずかに存在する程度である。IoT の品質確保が現場任せになっており、企業、業界、あるいは業界横断で取り組むための共通的な考えを示すことで、IoT のリスクを低減できると考えた。

そこで、IPA/SEC では、IoT 機器・システムの品質の確保において特に注意が必要となる項目を視点や考慮ポイントとしてまとめることにした。これにより、IoT 機器・システムに携わるステークホルダーが品質への理解を深め、安全安心な IoT の実現を支援することを目指した。検討を進めるにあたっての課題は、「品質」の捉え方が有識者間で異なることであった。そこで、検討の最初の段階で、「品質」について検討するスコープを合意し、そのスコープの範囲内で課題やニーズを収集して整理することで、視点や考慮ポイントを導き出すことができた。IoT 機器・システムの開発や品質確保に係わる方々が本書を実践することで、IoT の品質の確保、維持・改善活動の一助となることを期待する。なお、本書の第 3 章で記載した品質確保の視点や考慮ポイントをチェックリスト化したので活用していただきたい [24]。

本書は、関連するガイド類の動向、IoT サービスの発展などの状況を把握しながら、今後も適宜、アップデートしていく予定である。

最後に本書の策定にあたり、この WG の主査、および多大なるご支援をいただいた検討メンバーの方々に感謝の意を表す。

# 付録 A.IoT 検証ユースケース詳細

第 4 章で説明した既存の快適性制御システムと新規に開発する防災/防犯システムの IoT 検証ユースケース（スマートホームの戸締り競合制御）における考慮ポイントの詳細を表に示す。

考慮ポイント欄の文頭記号の意味

(競) IoT 特有の競合に関するもの
(セ) IoT 特有のセキュリティに関するもの
(連) IoT 特有の外部連携に関するもの
(他) IoT 特有であり上記以外のもの
(考) IoT 特有ではないが IoT でも考慮が必要なもの

表 A-1 検証ユースケース考慮ポイント詳細

| 番号 | 考慮ポイント |
|---|---|
| 1-1 | **(1)IoT の特徴を考慮した製品リスクを分析し対応する検証・評価方針を策定する**<br>本開発システムの特徴と社会的な影響を考慮し、以下の 3 つを検証・評価の重点ポイントとする。<br>・既存の快適性制御システムと新規防災/防犯システムの IoT デバイスの競合<br>・新規防災/防犯システム自体のセキュリティ対策<br>・パブリック気象情報や自治体/コミュニティ情報などの外部システムとの連携<br>(競) 本システムの本来機能である、クラウドサービスアプリケーションからの気象・防災情報および室外侵入センサーからの情報により、窓・雨戸の開閉および玄関扉鍵の開閉を制御する機能が、利用者の要求どおりに正しく動作することを検証する。<br>つながることによって起こる他のシステムへの影響（快適性制御システムと併設した場合、そのシステムに影響を与えないこと/そのシステムから影響を受けないこと）を検証する。本事例では、目的の異なる別々のシステム、機能または外部連携情報が、同一の IoT 機器を制御するために制御の競合が起こり、利用者に影響が及ぶリスクがある。本システムでは、窓、雨戸、玄関扉鍵の開閉制御の競合が、次の場合に起きると推定され、制御の優先度（高い順に人命を守る、財産を守る、快適性を確保する）に従って正しく処理されることを検証する。<br>・本システムと快適性制御システム間での競合<br>・本システム内の防災機能と防犯機能間での競合<br>・本システム内の外部連携情報間での競合<br>本システムの無線帯域通信（Wi-Fi 2.4GHz 帯）と他システムの異なる無線通信（Bluetooth のオーディオシステムなど）の影響を検証する。影響には電波の混雑や干渉によるレスポンス低下・タイムアウトなどを考慮する。<br>(セ)(連) つながることにより起こる脅威やハザードに対する、安全安心の品質を検証する。脅威・ハザードには、ホーム GW および防災/防犯コントローラの脆弱性脅威、クラウドサーバのサービス停止（気象・防災情報などの提供停止、ログ蓄積機能停止）、各コンポーネント間の通信データ改ざん（クラウドサーバとホーム GW 間、 |

| | |
|---|---|
| | ホーム GW と防災/防犯コントローラ間、防災/防犯コントローラと窓・雨戸・玄関扉鍵の制御機器間）、脆弱性脅威の安全性への波及、コンポーネントの障害が他コンポーネントに及ぼす影響などを考慮する。<br>**(2)IoT の特徴を考慮したプロジェクトリスクを分析し対応する検証・評価方針を策定する**<br>（他） 本システムの早期品質確保および開発効率化に寄与するために、検証プロセスとして、検証/品質保証部門が上流から参画できる IVIA のテスト標準工程を採用し、要求のレビューから出荷前の検証および評価までを実施する。<br>開発チームは IoT の開発経験が少ないことから、要求仕様レビュー工程から参加し、開発要件や要求仕様のレビューを行う。<br>本システムは長期にわたり運用され、出荷後は周辺環境の変化が予測されるので、保守・運用時の品質維持に必要な機能も検証対象とする。<br>**(3)法規制、準拠する標準およびガイド・基準を調査適用する**<br>（他） 防災/防犯システムに関する電波法が適用されていることを検証する。 |
| 1-2 | **(1)重点項目の検証・評価計画を立てる**<br>（他） 重点検証項目としてセーフティ、セキュリティ、リライアビリティ、互換性に関する項目を検証する計画を立てる。<br>（他） 制御機器やセンサーなどの調達品について、品質基準（ECHONET Lite 規格や無線通信規格など）を調査し、準拠性を確認する。認証基準があるものは認証取得を評価基準とする。また、IoT 製品は長期にわたり使用されるため保証期間、保守期間も確認する。<br>（競） 本システムが既存の快適性制御システムと相互に影響を受けないこと、および相互に影響を与えないことを検証する計画を立てる。<br>**(2)品質確保のリスク管理項目を設定し評価する**<br>（他） 製品リスク<br>調達品（制御装置、センサー）の品質リスク、外部連携（パブリック気象情報、ポイント気象情報、自治体/コミュニティ情報）のインタフェースに係わる品質リスクを評価する。<br>（他） 検証プロジェクトリスク<br>検証環境が整わないときのリスク、専門検証技術者がいないときのリスクを評価する。<br>**(3)具体的な検証・評価計画を立てる**<br>（競） IoT 機器（制御機器）の制御の競合について、既存 IoT システムとの競合および自システム内の競合について全組み合わせをテストする計画を立て、優先度に基づいて処理されることを検証する。<br>（競） IoT 機器の無線通信の混雑や干渉について、本システムが既存の IoT システムと相互に影響を受けないこと/相互に影響を与えないことを検証する計画を立てる。<br>（セ） ホーム GW や防災/防犯コントローラのリスク分析（脆弱性に対する脅威分析）と対策を検証する計画を立てる。<br>（セ） クラウドサーバのサービス停止と通信データの改ざん時の対策を検証する計画を立てる。<br>（セ） 制御機器やセンサーなどの IoT 機器のリユース時のセキュリティ対策や廃棄後のセキュリティ対策を検証する計画を立てる。<br>（競） 制御機器などの IoT 機器が他の機器から影響を受けないこと/他の機器に影響を与えないことを検証する計画を立てる。<br>（連） 本システムの外部連携情報（気象・防災情報）が正しいこと（システム間認証やアクセス制御など）を検証する計画を立てる。 |

| | |
|---|---|
| | **(4)テスト環境を整備し維持する**<br>（他） 本システムのテスト環境は、公的機関や業界が用意している、スマートホーム実証実験環境（快適性制御システムも稼働している環境）を利用する。 また、手動で操作できるクラウドダミーサーバを構築する。これらにより、動作検証のコスト削減と効率化を図る。 テスト環境は運用期間中も維持できるよう管理する。<br>**(5)検証要員を確保する**<br>（考） 本検証チームには、無線ネットワークの知識を有する検証要員がいないため、無線ネットワークがわかる検証専門エンジニアを確保する。 |
| 1–3 | **(1)品質の説明責任を果たすために、客観性・専門性の観点を考慮する**<br>（考） 本システムは、セキュリティ対策に不備があると人命や財産に影響を与えるため、セキュリティ対策の検証・評価は、客観性および専門性を考慮し、外部の第三者による検証を実施し品質説明のエビデンスを保持する。<br>（考） 上記エビデンスは、防災/防犯システムの供給責任者が、各構成要素の品質、システム全体の品質を説明できるレベルのものを保管する。 |
| 2–1 | **(1)つながることによって起こる IoT 機器（窓、雨戸、玄関扉鍵）への競合についての対応を含めて開発要件が正しいことを確認する**<br>（競） 既存の快適性制御システムは通気のために窓の開閉を自動で行うものである。一方、本システムは防災/防犯のために窓、雨戸などを自動で閉めることがあり、快適性制御システムの窓・雨戸の開放と相反する動作が発生し得る。そのため、両システム間の競合を調整する機能を設けている。この調整機能に関して、競合条件が網羅的に考慮されていることを確認する。<br>同様の競合は自らのシステム内の防災機能と防犯機能の間でも発生し得るし、さらには防災機能の中でも地震速報と竜巻情報間といった外部連携システム間からもたらされる情報による判断の間で競合し得る。これらの競合に対する調整のための要件が正しいことも確認する。<br>（競） 既存の屋外センサーなど無線による制御が、新規に開発する屋外侵入センサーと競合しないことを仕様上、考慮していることを確認する。<br>**(2)外部システムが正常動作していない場合のリスクが分析されていて、またその低減策が組織的に合意されているか確認する**<br>（連） 外部連携システムの休止や停止を想定しているか、さらに、自システムにどのような影響があるかなど対応要件を確認する。<br>（連） 外部サービスや接続される機器すべてについて、その品質要件（性能、故障率、寿命などについての）が明確になっていることを確認する。 |
| 2–2 | **(1)利用者を想定した上で守るべきものやリスクを特定し、その分析結果や対応方針が要件に反映されているかを確認する**<br>（他） 利用者はシステムを操作できない高齢者や幼児も想定し、受動的ユーザ（コラム4参照）の安全を意識したシステムになっていることを確認する。防災/防犯システムを解除しなくとも、物理的な鍵が中からは容易に開けられるなど、閉じ込め事故が発生しないなどの安全に配慮した仕様になっていることを確認する。<br>（考） コントローラの操作性、インタフェースのわかり易さについて、高齢者や身体障害者の方々にも配慮しているかを確認する。<br>本システムがどんな機能があるかを利用者が容易に理解でき、適切な判断ができる仕様になっているか、説明やナビゲーションに対する要求、利用者が操作を容易に覚えるための工夫、誤った操作をしない、または誤っても前の操作に復帰できる機能などの要求、端末やインタフェース自体の見栄え、わかり易さに関する要求、様々な年齢層、心身特性および能力差への配慮に対する要求、言語対応に関する要求を確認する。 |

| | |
|---|---|
| 2–3 | **(1)セキュリティの確保を確認する**<br>（セ） 本システムは人命や財産に影響を与える可能性があるため、開発システムが達成すべきセキュリティレベルが明確になっているか、システムとしてセキュリティの脅威分析とその対策が明確であることを確認する。 |
| 2–4 | **(1)運用時のリスクを検討し、トラブルシューティングの容易化を提案する**<br>（他） 本システムは既存システムや外部システムとの連携があるため、障害の切り分けが難しいことが想定される。運用時の障害の解析性の向上を目指し、ホームGW とクラウド・制御機器・センサー間の通信ログを仕様に盛り込むことを提案する。 |
| 3–1 | **(1)要求（暗黙的要求を含む）が実装されていること、およびその満足度合いを動的テストで評価する**<br>（考） 利用者要求から評価のシナリオを作成し、利用者要求が網羅されていることを関係者と合意する。<br>「防災/防犯システム」製品として要求を実現できたのか見極めを行う（Proof of Concept）。 見極めは、テスト結果やテスト完了報告などの文書によるものだけでなく、実物の評価環境などを関係者で確認して合意する。<br>**(2)リスクの低減を動的テストでも確認する**<br>（競） 地震速報と竜巻情報の同時到達といった、リスクの原因として考えられていた競合状態を実際に発生させる条件を作り出し、ハザードに至らないことを確認する。 |
| 4–1 | **(1)IoT デバイスのつながり方やデータに着目してテスト設計する**<br>（他） センサーが追加、取り外しされること、および両システムが長期間利用されることを考慮したテスト設計を行う。<br>（競） 仕様上の最大台数にて動作や管理に支障がないことを検証する。その際、PC やスマートフォンなどシステム以外の無線 LAN 機器および Bluetooth 機器が動作している環境で問題が発生しないことを検証する。<br>（考） 調達品である無線モジュールが電波法に適合していることを書類確認する。（エビデンスも入手）<br>（他） 機器ごとにデータの精度が異なるケースを想定し許容誤差や不定データを受け取った場合について検証する。 |
| 4–2 | **(1)他のシステムとの競合やシステム内の競合について、テスト設計する**<br>（競） 両システムの競合テストにて、人命＞財産＞快適性の優先度で処理されることを検証する。<br>（競） 快適性制御システムへ影響を与えないことおよび他の無線 LAN 機器や Bluetooth 機器へ影響を与えないこと/受けないことを検証する。<br>（競） 競合が発生するケースについて予め決定した仕様に基づいて動作することを検証する。<br>a)システム内競合−宅内システム内<br>地震と強盗侵入が同時に発生した場合に鍵の施錠と解錠の競合<br>・屋外侵入センサーが侵入者を感知すると窓および玄関の鍵を施錠する。<br>・地震速報により雨戸を開け、玄関および窓の鍵を解錠する。<br>b) システム間競合−外部システム連携<br>竜巻と地震が同時に発生した場合に雨戸の開閉についての競合<br>・竜巻情報から防災/防犯システムが雨戸および窓を閉める。<br>・地震速報から防災/防犯システムが窓を解錠し雨戸を開ける。<br>c)システム間競合<br>快適性制御システムによる通風時に強盗侵入で窓の施錠と解錠の競合<br>・快適性制御システムが晴天・適温時に通風として窓を開ける。<br>・防災/防犯システムが侵入者を感知し窓および玄関を施錠する。 |

| | |
|---|---|
| 5-1 | **(1)本システムの利用環境に着目して、テスト設計する**<br>(競) 同環境で存在し得ると思われる機器がある状態で動作し、影響を受けない/与えないこと。ゲーム機、Bluetooth スピーカー、スマートフォン、PC の同時使用にて検証する。<br>(競) 隣家のシステムと競合しないこと、機器追加時にも競合しないことを検証する。<br>センサーなどを追加する場合について、同じ型番の各種環境センサーを初期状態で通電(購入直後)しても、試験対象のホーム GW と各種環境センサーの接続には影響しないことを検証する。<br>(競) 無線方式が干渉して使用できない状態にならないかを検証する。<br>Wi-SUN など方式の違う無線環境を用意して相互に問題がないことを検証する。<br>(セ) 開閉対象のドアが開いていてそのままだと施錠できない状態にて、施錠の指示を受けたときの動作仕様を基に、施錠できないことをアラートする仕様として動作を検証する。<br>(連) 外部サービス(緊急災害など)からの戸締り制御について、クラウドからの指示により実際に窓の開閉を行うまでの許容時間の検証を行う。<br>(連) 緊急避難の玄関解錠について、クラウドからの指示により実際に玄関の解錠を行うまでの許容時間の検証を行う。 |
| 6-1 | **(1)本システムの異常検知とその異常処理に着目して、テスト設計する**<br>(連) 各種動作状態でクラウドを切断されたときにセンサー信号を基に、人命優先となっていることを検証する。復帰したときにはクラウドの情報と突き合わせ正常動作していることの検証を行う。<br>(他) 通信不通時・故障時・寿命時・停電からの復帰時の検証を行う。<br>回線が不通時にはセンサー信号を基に、人命優先として動作することを検証する。<br>センサーおよびアクチュエータが故障/寿命時には故障のアラートを利用者に知らせることを検証する。<br>停電からの復帰時にセンサーおよびクラウドに自動接続し正常動作することおよび再起動したことを利用者に通知することを検証する。 |
| 6-2 | **(1)セキュリティ対策に着目して、テスト設計する**<br>(考) 使用停止方法のテスト(譲渡時・廃棄時・故障時)<br>セキュリティの観点から廃棄時に個人情報/設定の初期化ができることおよびマニュアルに説明があることを検証する。<br>(セ) スマートフォンによる施錠・解錠方法がセキュリティホールにならないことを検証する。また、スマートフォン紛失時などの緊急解錠方法がセキュリティホールにならないことについても検証する。<br>(セ) インターネットにポート解放する機器は攻撃にさらされることへの対策を検証。<br>(考) 不要な空ポートがないか検証する。<br>(考) 一般的なネットワーク脆弱性テスト(ツール利用など)の検証を行う。<br>(考) 出荷時パスワードが短い/全個体一緒/未設定ということがないか検証する。<br>(考) デフォルトパスワードのまま利用できない仕組みであることを検証する。<br>(セ) セキュリティおよびセーフティについては単体だけではなくシステム全体としての検証を行う。 |

| | |
|---|---|
| 7-1 | **(1)長期利用での品質維持に着目して、テスト設計する**<br>(考) ログなどのデバッグ機能・障害解析機能の検証を行う。<br>(考) アップデート機能の検証を行う。<br>・アップデートが正常にできるか、その後システムに自動認識されるか。<br>・アップデート中の動作や機能・性能に対する影響の検証。<br>・アップデート失敗時に安全性、回復性の検証。<br>・同時アップデートでネットワークやシステムが過負荷とならないことの検証。 |
| 8-1 | **(1)テスト環境を検討する**<br>(他) テスト環境は、開発チームの IoT 実験設備に擬似的なクラウド環境を構築するとともに、スマートホーム業界の設備や公的機関の設備を利用する。公的機関としては、例えば、東京大学 COMMA ハウス(http://www.commahouse.iis.u-tokyo.ac.jp/)や神奈川工科大学 HEMS 認証支援センター(http://sh-center.org/)などを活用する。 |
| 8-2 | **(1)テストの効率化を検討する**<br>(考) 各種機能について、テスト要素とテスト変数(条件や環境)の抽出・組み合わせを検討し、作成した組み合わせ表のテストを効率的に実施できる検証環境と手順を計画する。<br>同値分割、境界値分析、直交表、オールペア法などを使い効率化を図るとともに重要性の高い機能については漏れなく検証する。 |
| 9-1 | **(1)テストが困難なケースについて設計でも考慮してもらうよう開発に提案する**<br>(考) ログ収集機能、擬似障害発生方法、加速度試験を実施する方法について提案し設計に盛り込んでもらう。 |
| 10-2 | **(1)テスト結果の合否判定の曖昧性を排除する**<br>(考) 使い勝手など使用性の主観的な判断については開発担当者を交えて確認し、曖昧な部分をなくすようにする。 |
| 11-1 | **(1)リリース後の変化に対応できる運用計画を立案する**<br>(セ) 本システムの更新タイミングや外部のシステムとの連携時に、セキュリティの脅威分析を見直す計画を盛り込む。<br>**(2)定期的な品質の確認・点検作業を計画する**<br>(競) 他システムと相互に影響する機能である優先度調整機能が正常に動作することを運用中に確認する方法を検討し、定期確認の計画に盛り込む。<br>**(3)不具合の発生などを想定した対応プロセスを確立する**<br>(考) 他システムとの相互影響があるため、システム間での運用の責任範囲を定める。また、つながることによる被害の拡大を防ぐため、不具合発生時の連携方法を明確にしておく。<br>(競) 他システムとの優先度調整機能の接続箇所について責任分界点を定め、脆弱性問題によりウイルス感染などのセキュリティ問題が顕在化した場合には、優先度調整機能でネットワーク遮断を行うように手順化する。 |
| 11-2 | **(1)運用品質の評価項目の抽出と評価基準を策定する**<br>(競) 運用時に想定される脅威を計測するために、優先度調整機能におけるシステム間の競合発生頻度を監視すべき指標として定義する。 |
| 12-1 | **(1)利用環境の変化を把握し対処する**<br>(他) 本防災/防犯システムと既存の快適性制御システム以外のシステムが導入されていないか、センサー接続用の無線ネットワークに想定外のセンサーや GW などが接続されていないかを定期的に確認する。 |

| | |
|---|---|
| 12-2 | **(1)安全安心に係わる機能の確認を行う**<br>（競） 運用計画に従って、定期的にシステム間の競合を制御する優先度調整機能に影響が出ていないことを、ログなどから確認する。 |
| 13-1 | **(1)システムの不具合対応や機能改善を行う**<br>（考） ソフトウェアを更新する場合、運用計画に基づきテストを実施するとともに、ソフトウェアの更新が失敗した場合を想定し、復旧方法や他システムへの影響を最小限にするための対応方法を確認する。 |

# 付録 B.参考文献


[1] IPA, “つながる世界の開発指針,” [オンライン]. Available: https://www.ipa.go.jp/sec/publish/tn16-002.html.

[2] JSTQB 技術委員会, “ソフトウェアテスト標準用語集（日本語版）,” [オンライン]. Available: http://jstqb.jp/dl/JSTQB-glossary.V2.3.J02.pdf.

[3] IPA, “SEC BOOKS,” [オンライン]. Available: https://www.ipa.go.jp/sec/publish/index.html.

[4] IPA, “「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],” [オンライン]. Available: https://www.ipa.go.jp/sec/publish/tn17-002.html.

[5] IPA, “共通フレーム 2013,” [オンライン]. Available: https://www.ipa.go.jp/sec/publish/tn12-006.html.

[6] IoT 推進コンソーシアム, “IoT セキュリティガイドライン ver1.0,” [オンライン]. Available: http://www.meti.go.jp/press/2016/07/20160705002/20160705002-1.pdf.

[7] OWASP, “IoT Testing Guides,” [オンライン]. Available: https://www.owasp.org/index.php/IoT_Testing_Guides.

[8] CCDS, “IoT セキュリティ評価検証ガイドライン Rev1.0,” [オンライン]. Available: https://www.ccds.or.jp/public/document/other/guidelines/CCDS_IoT セキュリティ評価検証ガイドライン_rev1.0.pdf.

[9] IPA, “ファジング活用の手引き,” [オンライン]. Available: https://www.ipa.go.jp/files/000057652.pdf.

[10] CSAJ, “ソフトウェア出荷判定セキュリティ基準チェックリスト,” [オンライン]. Available: http://www.csaj.jp/NEWS/committee/security/160713_sec-release-decision.html.

[11] IPA, “IoT における脅威と対策,” [オンライン]. Available: https://www.ipa.go.jp/files/000057382.pdf.

[12] IPA, “つながる世界のセーフティ＆セキュリティ設計入門,” [オンライン]. Available: https://www.ipa.go.jp/sec/publish/tn15-001.html.

[13] IPA, “コモンクライテリア,” [オンライン]. Available: https://www.ipa.go.jp/security/jisec/cc/index.html.

[14] 総務省, “平成 29 年版　情報通信白書,” [オンライン]. Available: http://www.soumu.go.jp/johotsusintokei/whitepaper/ja/h29/html/nc133100.html.

[15] 八山　幸司, “ニューヨークだより　2015 年 8 月,” [オンライン]. Available: https://www.ipa.go.jp/files/000047543.pdf.

[16] IPA, “つながる世界の利用時の品質,” [オンライン]. Available: https://www.ipa.go.jp/files/000058465.pdf.

[17] CSSC 認証ラボラトリー, “ISASecure EDSA 認証とは,” [オンライン].

Available: http://www.cssc-cl.org/jp/about_edsa/index.html.

[18] B. Linders, “テスト容易性のためのシステム設計,” [オンライン]. Available: https://www.infoq.com/jp/news/2014/11/designing-systems-testability.

[19] Wikipedia, “Design for testing,” [オンライン]. Available: https://en.wikipedia.org/wiki/Design_for_testing.

[20] IPA, “つながる世界の利用時の品質,” [オンライン]. Available: https://www.ipa.go.jp/files/000058465.pdf.

[21] DEOS 協会, “IEC 62853 と「つながる世界の開発指針」の比較検討,” [オンライン]. Available: http://deos.or.jp/link/obj/pdf/DEOS-TR-20180125.pdf.

[22] JPCERT, “制御システムセキュリティの 現在と展望 2016,” [オンライン]. Available: https://www.jpcert.or.jp/present/2016/20160217_CSC-JPCERT01.pdf.

[23] IVIA, “IT 検証標準工法ガイド Ver.1.1,” [オンライン]. Available: https://www.ivia.or.jp/dl_ctg003/.

[24] IPA, “つながる世界の品質確保チェックリスト,” [オンライン]. Available: https://www.ipa.go.jp/sec/publish/tn18-001.html.

本書は、独立行政法人情報処理推進機構(IPA) 技術本部 ソフトウェア高信頼化センター(SEC) つながる世界の品質指針検討 WG において作成しました。

## 編著者 (敬称略)


| | | |
|---|---|---|
| 主　査 | 森崎　修司 | 国立大学法人名古屋大学 |
| 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 |
| | 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) |
| | 亀井　健一 | 株式会社アイ・オー・データ機器 |
| | 後藤　祥文 | デンソーテクノ株式会社 |
| | 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 |
| | 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 アドバンスト・テクノロジー株式会社 |
| | 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 |
| | 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 |
| | 松並　勝 | DNV GL ビジネス・アシュアランス・ジャパン株式会社 |
| | 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 |
| 事務局 | 末田　信 | 一般社団法人 IT 検証産業協会 (IVIA) /株式会社ブイラボ |
| | 大濱　裕史 | 一般社団法人 IT 検証産業協会 (IVIA) /NTT アドバンステクノロジ株式会社 |
| | 表　憲一 | 一般社団法人 IT 検証産業協会 (IVIA) /株式会社富士通コンピュータテクノロジーズ |
| | 中尾　昌善 | IPA/SEC |
| | 宮原　真次 | IPA/SEC |
| | 小崎　光義 | IPA/SEC/日本電気株式会社 |
| | 西尾　桂子 | IPA/SEC |

**SEC BOOKS**

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～

平成 30 年 6 月 4 日　1 版 1 刷発行

監修者　独立行政法人情報処理推進機構(IPA) 技術本部
ソフトウェア高信頼化センター(SEC)

発行人　片岡 晃

発行所　独立行政法人情報処理推進機構(IPA)
〒113-6591
東京都文京区本駒込 2-28-8
文京グリーンコートセンターオフィス
URL https://www.ipa.go.jp/sec/



ISBN 978-4-905318-59-0　Printed in Japan

ISBN978-4-905318-59-0
C3055 ￥278E


定価：本体278円+税


独立行政法人 情報処理推進機構
技術本部 ソフトウェア高信頼化センター

SEC-TN18-001