SEC BOOKS

「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

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)への取り組みが各国で進んでおり、IoT 機器や関連システム（IoT 機器・システム）がつながることによる価値創出を主要な戦略として位置づける企業も増えてきている。さらに、単一分野で IoT が普及すれば、利便性の向上やコスト削減のために分野を横断して相互乗り入れすることが見込まれる。しかし、すべての IoT 機器・システムをつないで相互に情報を共有したり制御したりすれば、IoT への取り組みは万全というわけではない。つながることにより生じる新たなリスクや脅威を熟慮した上で、安全安心に十分に配慮する必要がある。また、単一分野のみを対象とした IoT 機器・システムの開発においても、将来を見越して分野横断を意識した設計やロードマップを策定しなければ、IoT 機器・システムの再設計が必要になることをはじめ、寿命を縮める可能性が高まる。

IPA では、IoT の普及を見据え、安全安心が確保された信頼できる製品やシステムを開発するための「つながる世界の開発指針」を策定し 2016 年 3 月に公開した。「つながる世界の開発指針」では、つながることによって起こる事故やインシデントなどを未然に防ぐことを主眼に、指針ごとにポイント、解説、対策例を記載し、製品やシステム開発時において安全安心の確保のために考慮すべき着眼点を俯瞰的に示している。この開発指針を参考にしながら開発を進める際には具体例が必要という声に応えるために、本書では、開発指針の技術要件に対して、高信頼化実現のための機能レベルに具体化を図った。

本書は、IoT 機器・システムを実現しようとする開発者を対象読者とし、安全安心に寄与する機能を紹介する。具体的には、IoT の高信頼化の要件を提示し、それを実現するために求められる機能要件と機能をまとめた。また、本書で実施した分野間連携のリスク分析例も提示することで、開発者が自身の IoT 機器・システムの実装において活用できるようにした。

なお、本書の適用に当たっては、ここで提示した IoT 高信頼化機能のすべてを実装することを検討するのではなく、対象となる IoT 機器やシステムのリスクアセスメントを実施し、必要となる IoT 高信頼化機能を選択して、実装することを想定している。本書を実践することで、IoT の安全安心が実現できることを期待している。

【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」に順ずるものとする。

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
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、機能単位の能力が無くなること	同上
セキュリティ異常	不正／過失行為が発生し正常でない状態	
リスクアセスメント	リスク特定、リスク分析及びリスク評価のプロセス全体	JIS Q 31000
消去	ファイルの削除や、初期化（USB メモリのフォーマット等）では、復元することが可能な場合があるが、消去は完全にデータを読めなくする行為	
ログ	システムおよびネットワーク内で発生するイベント（事象）の記録	NIST SP800-92 コンピュータセキュリティログ管理ガイド
ログ収集	ログの生成、転送（通信）、保存（格納）、破棄までを示す。ログの分析は監視の一部とする	
信用性	相手の行為や情報の確からしさ	
信用度	信用性の度合い	

(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
ATM	Automatic Teller Machine
AV	Audio Visual
CSA	Cloud Security Alliance
CSMS	Cyber Security Management System
C2C-CC	CAR 2 CAR Communication Consortium
CRYPTEREC	Cryptography Research and Evaluation Committees

略語	名称
CRSS	CVSS based Risk Scoring System
CVSS	Common Vulnerability Scoring System
DoD	United States Department of Defense
EoL	End of Life
FIRST	Forum of Incident Response and Security Teams
GPS	Global Positioning System
GW	Gateway
HDD	Hard Disk Drive
HEMS	Home Energy Management System
IEEE	The Institute of Electrical and Electronics Engineers, Inc.
ID	Identification
IIC	Industrial Internet Consortium
IIRA	Industrial Internet Reference Architecture
I/F	Interface
IoT	Internet of Things
ISMS	Information Security Management System
JSAE	Society of Automotive Engineers of Japan
NC	Numerically Controlled
NIST	National Institute of Standards and Technology
NSA	National Security Agency
NTP	Network Time Protocol
OWASP	Open Web Application Security Project
PKI	Public Key Infrastructure
PM	Particulate Matter
POS	Point of Sales
POST	Power on Self Test
PV	Photovoltaics
RSMA	Risk Scoring Methodology for Automotive systems
SIAT	System Invariant Analysis Technology
USB	Universal Serial Bus
VPP	Virtual Power Plant

目次

第1章
背景と本書の目的

本章では、「つながる世界の開発指針」［1］について、さらに踏み込んだ実装に向けた手引きが必要となった背景や、本書の目的、および、「つながる世界の開発指針」に対する本書の位置づけを説明する。

1.1 背景

IoT 時代に向けて、国際標準やガイドラインの策定が分野別に進められている。国際標準やガイドラインは満たすべき要件を示すことが目的であるため、開発者はそれを実現する機能や機能配置を具体的に検討する必要がある。しかし、そうした具体的な公開情報は多くないのが実情である。

また、国際標準やガイドラインの整備が進み、その対象分野での IoT が普及すれば、次は、利便性の向上やコスト削減のために分野を横断した相互乗り入れが見込まれる。

そうした状況を考えれば、実際に分野を横断し相互乗り入れを前提とした開発を進める場合だけでなく、特定分野での標準やガイドラインに沿った開発を進める場合においても、分野間での相互接続、ロードマップの策定、将来を見据えた設計といった視点の高いグランドデザインが必要になる。そのためには、IoT 機器・システムをつなげる際に安全安心を確保するための機能（IoT 高信頼化機能）の必要性を理解し、その機能要件、機能定義のポイントを開発者が把握しておく必要がある。

本書では「つながる世界の開発指針」に示されている指針のうち技術面での対応が必要になる部分にフォーカスしている。既に IoT への対応が求められている機器・システムやサービスの開発、運用に携わる技術者だけでなく、これから IoT への対応が求められる機器・システムの開発に従事する開発者にとっても具体的な課題の認識、実現方法を考える際の手引きとなることを期待している。本書が対象読者である開発者の将来を見据えた設計につながり、国際競争力の強化に寄与することを目指す。

1.2 本書の目的

本書は、「つながる世界の開発指針」で示した技術要件を実装可能な機能レベルで具体化し、現場で実践するための手引きとして作成した。本書を適用することで、安全安心な IoT の実現を目指す。

本書では、IoT 高信頼化機能を実現しようとする開発者向けに、ライフサイクルや機能配置といった軸を示しながら高信頼化機能の機能要件と対応する具体的な機能を紹介する。また、近い将来に普及が見込まれる分野間での連携を視野に入れてもらうことにより、寿命が長く競争力の高い IoT 機器・システムを開発してもらえることを期待している。

本書では次のような工夫により、本書の対象読者がより具体的なイメージを持っていただくことを目指した。

(1) IoT 高信頼化機能の具体例とそれらの機能が満たすべき機能要件を説明する。これによって、読者がそれらを対応づけて理解することを助ける。

(2) IoT 機器・システムやサービスのライフサイクル、及び、エッジ、フォグ、クラウドといった機能配置を説明する。これによって、読者が実装方法や必要な機能を網羅的にイメージすることを助け、経済合理性や寿命を考慮した現実味のある検討を助ける。

(3) 本書をまとめるにあたって、ワーキンググループを構成する各分野の専門委員が議論した分野間を横断するユースケースとそこにおけるリスクや脅威、機能定義と機能配置の具体例を示す。これによって、読者が自身の開発対象におけるリスクや脅威を列挙すること、その対処を検討することを助ける。

1.3 本書の位置づけ

「つながる世界の開発指針」では、安全安心な IoT の実現に向けて、開発者に認識して欲しい重要なポイントをライフサイクルの視点で整理している。また、17 個の各指針において、対策の例をあげているが、実装すべき機能の具体化まではしていない。本書は、IoT 機器・システムが実際に使用される状況で起こり得るイベントについて，保守･運用の視点で設計時に考慮すべき IoT 高信頼化要件･機能を 5 つのカテゴリに分けて具体化するとともに、IoT における実装位置を考慮し整備したものである。

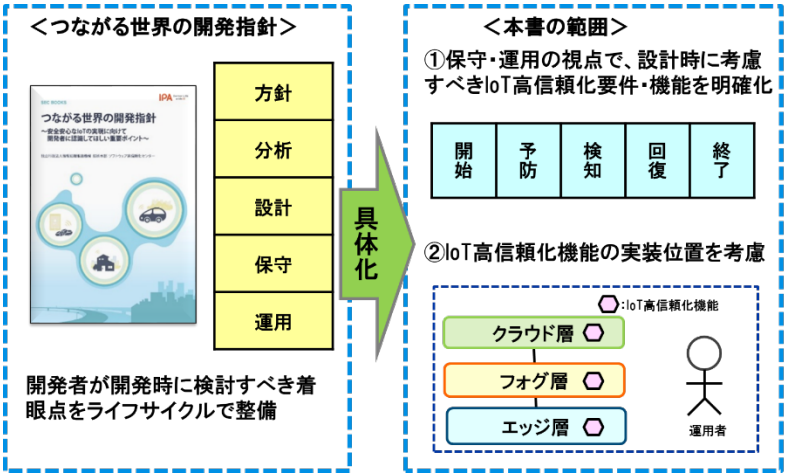


図 1-1 本書の位置づけ

第2章
IoT 高信頼化の考え方

IoT の高信頼化のためには、IoT 機器・システムがつながることによる脅威やハザードを想定し、それらに対する対策を講じることが必要である。特に IoT では、今後、分野間の連携が増加することが想定されるが、現時点では事例がすくなく検討が必要である。

本章では、「つながる世界の開発指針」をもとに IoT の脅威・ハザードや対策を整理した。特に、IoT の分野間連携については、より深く検討が必要と考えて、5 つの分野間連携のユースケースを作成して分析を行った。また、対策としては、機能の抽出のために技術対策に着目して整理を行った。このとき、機能抽出するための前提条件として、IoT 高信頼化機能の定義について明確化した。なお、抽出された機能について、開発者が設計する際に検討すべき視点として、保守・運用に着目した整理方法について説明する。

本書で整理した IoT 高信頼化要件は、主にソフトウェアで実装されることを想定しているが、ハードウェアでの実装や運用者（人）が一部カバーすることで実現しても良い。

2.1 IoT 高信頼化機能とは

「つながる世界の開発指針」では、IoT 機器・システムにおいて、守るべきものを IoT 機能、本来機能、情報、その他に分類している（2.4 参照）。IoT 高信頼化のためには、つながるための機能だけを高信頼化するだけでは不十分で、本来の機能もふくめて高信頼化しないと、高信頼化していない箇所の異常が、波及してしまうリスクがある。本書では、IoT 高信頼化機能は、IoT 機器・システムが相互につながる環境において、安全安心を確保するために必要な機能と捉え、IoT 機能、および本来機能の中に実装されるべきものとする。なお、ここでの「安全安心」とは、「つながる世界の開発指針」における解釈にしたがい、セーフティ、セキュリティ、リライアビリティを表すものである。

■ IoT高信頼化機能とは
IoT機器・システムが相互に連携する（つながる）環境において、安全安心を確保するための機能

図 2-1 に IoT 高信頼化機能の実装イメージを示す（具体的な内容については第 3 章で示す）。

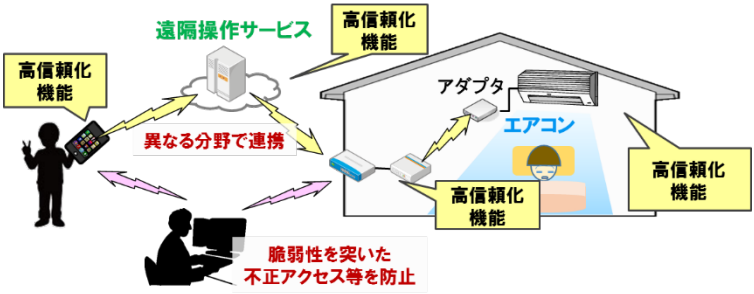


図 2-1 IoT 高信頼化機能の実装イメージ

2.2 IoT 高信頼化機能の抽出方法

IoT 高信頼化機能の抽出は、図 2-2 に示す 4 つのステップで実施した。

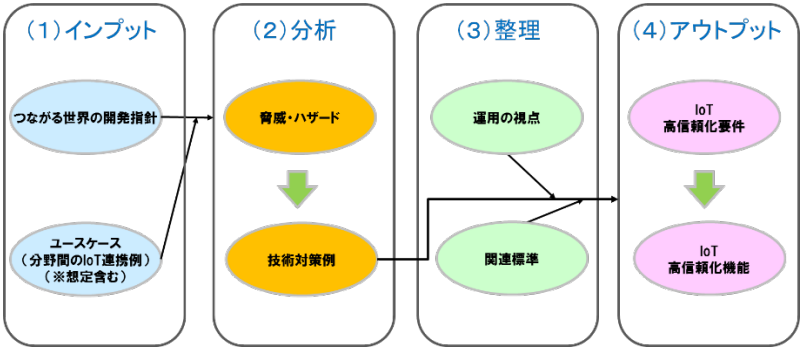


図 2-2 IoT 高信頼化機能抽出のステップ

(1) インプット

インプットとしては、「つながる世界の開発指針」に加えて、特に、分野間の IoT 連携を想定したユースケース（付録 A 参照）を導入した。

(2) 分析

IoT の脅威・ハザードの想定や対策について、「つながる世界の開発指針」で対策例としてあげているものと、分野間の IoT 連携に関するユースケースをもとに分析を行った。抽出された脅威・ハザード、及び技術対策例については付録 B 参照。

(3) 整理

脅威・ハザードを分析した結果、抽出した技術対策は、個々の技術対策となっており、必要な場面や、対策の必要性がわかりにくい。IoT 高信頼化機能が必要となる場面は保守・運用時である。そこで、開発者が保守・運用時の視点で必要となる機能を設計時に作りこむために、運用の軸で整理した（2.3 参照）。

さらに、IoT に関する標準類がすでに存在するため、そこに記述されている内容を調査し、逸脱しているものにならないように配慮した（付録 B 参照）。

(4) アウトプット

抽出した技術対策について、運用の視点を踏まえた IoT 高信頼化要件と、要件を実現するための IoT 高信頼化機能としてまとめた（第 3 章参照）。

なお、IoT 高信頼化機能は、「つながる世界の開発指針」の対策例とユースケース分析をもとに抽出したが、さらに検討の中で必要と考えられた機能も含んでいる。

2.3 IoT 高信頼化の分析と整理の考え方

2.3.1 基本モデルの想定

ユースケースを用いた脅威・ハザードの分析や、技術対策の実装を検討するために、IoT の基本モデル（IoT 構成イメージ）を想定した（図 2-3）。

本書では IoT 高信頼化機能の基本モデルを、エッジ層、フォグ層、クラウド層［2］に分類する（連携に関しての詳細は付録 A 参照）。エッジ層とはユーザの近くにエッジサーバを分散させ、距離を短縮することで移動するデータの量と距離を低減させる技術を利用する個別基盤である。データの処理（蓄積・分析）までは実施せず、リアルタイム性が必要な場合がある。フォグ層とは、クラウド層とエッジ層の間にある分散処理環境で、クラウドよりエッジに近い位置に広く分散したデータ処理装置を設置し、全体を統一のインターネットプロトコルで設計するネットワーク構造である。また、リアルタイム性が必要な場合がある。なお、フォグとは霧の意味であり、雲を意味するクラウドより、地上に近いことからこのネーミングがなされている。クラウド層はデータ処理（蓄積・分析）を実施し、リアルタイム性は重要視されない場合がある。

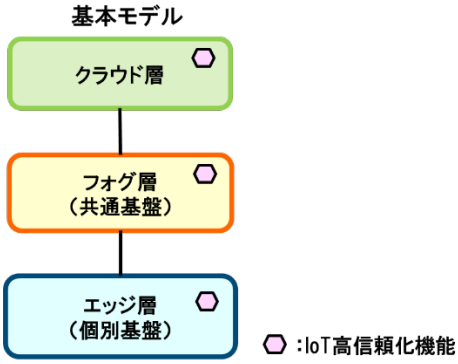


図 2-3　本書における IoT の基本モデル（IoT 構成イメージ）

IoT 高信頼化機能は、対象とする IoT 機器・システムの必要に応じて、エッジ層、フォグ層、クラウド層のいずれかに配置される。例えば、リソースの少ないエッジ層に負荷のかかる機能を配置できない場合は、上位のフォグ層やクラウド層でその機能を担保し、全体として IoT 高信頼化機能を実現できるようにする。

エッジ層、フォグ層、クラウド層のどこに、どのような IoT 高信頼化機能を最適に配置するのかをトータルに考えて設計することが IoT 時代の設計には求められる。本書の付録 A には、車両と住宅の連携、産業ロボットと電力管理の連携などの事例を記載している。それぞれの対象に即した IoT 高信頼化の機能の持ち方の参考としていただきたい。

2.3.2 保守・運用視点での要件の整理

IoT 高信頼化機能は、保守・運用時の視点で必要となる機能を設計時に作りこむことが重要である。例えば、運用中にシステムの障害が発生した場合、検知や回復に関する機能が必要であり、それらの機能を設計工程で作りこむなどの対処を実施する。

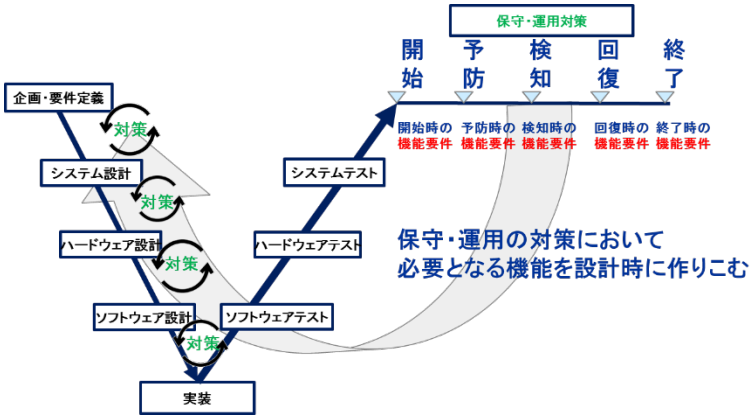


図 2-4 IoT 高信頼化を運用の視点でとらえたイメージ

IoT 高信頼化機能を実現するためには保守・運用中の対策としては、「予防・検知・回復 」の 3 つが必要である［3］。さらに、IoT 機器・システムは環境や構成が絶えず変化することから、サービス開始や接続時、及びサービス終了や廃棄時の対策が必要であるので、開始と終了を追加して「 開始・予防・検知・回復・終了」の 5 つに分類した。

(1)「開始」の対策

開始時に安全安心に接続できるためには、接続時に IoT 機器・システムにおいて目的に合致した初期設定や、利用者がサービスを利用開始する場合の許可

の状況などを確認することが必要である。なお、「開始」の捉え方ついては 2.3.3 に示す。

(2)「予防」の対策

稼働中の異常を未然に防ぐためには、IoT 機器・システムの安定稼働のための障害の予兆の把握、機能・資産の保護や、ソフトウェアのアップデートなどの事前対応を行うことが必要である。

(3)「検知」の対策

稼働中の異常を早期に検知するためには、IoT 機器・システムの障害/故障や、セキュリティ異常、競合状態などを検知し通知できる機能を備えていることが必要である。検知した内容について記録（ログ）を残しておき、異常の原因を特定することが必要である。

(4)「回復」の対策

IoT 機器・システムに、異常が発生しても被害の拡大を防ぎ、復旧できる機能を備えていることが必要である。回復の対策は構成情報管理、当座の回避、復旧、本格対処時の原因究明／対処に分けて考えることができる。

(5)「終了」の対策

IoT 機器やシステムが放置された場合の保護や、中古販売、廃棄時などに情報漏えいを防ぐための機能を備えていることが必要である。「終了」の捉え方については 2.3.3 に示す。

2.3.3「開始」と「終了」の捉え方

5 つのカテゴリの中で、「開始」と「終了」は、種々の捉え方があるため、その意味合いを整理する。例えば、「開始」では、システムを構築してサービスを最初に開始するカットオーバーとしての開始や利用者がサービス利用契約を締結して、使い始める時の開始などがある。また、ビジネスや教育現場（大学など）での共用端末や不特定多数がシェアして利用するレンタカーなどの共用 IoT 機器・システムの使い始めも「開始」として捉えることができる。本書では、「開始」と「終了」はいくつかの層があることを前提に考えた。ここで

は、厳密な意味の定義までは行わないが、そのように層に分けて捉えることを検討していただきたい。

＜「開始」の捉え方＞

① サービス提供者、利用者の機器・システムの入手時点
② サービス提供者、利用者がシステムを構築し、初期設定を行う時点
③ 利用者があるサービスの利用を開始する時点
（サービス提供者による日々のサービス提供などの開始を含む）

＜「終了」の捉え方＞

④ 利用者があるサービスの利用を終了する時点
（サービス提供者による日々のサービス提供などの終了を含む）
⑤ サービス提供者や、利用者がシステムを利用できない状況にする時点（システム解体含む）
⑥ サービス提供者や利用者が機器・システムを破棄する時点

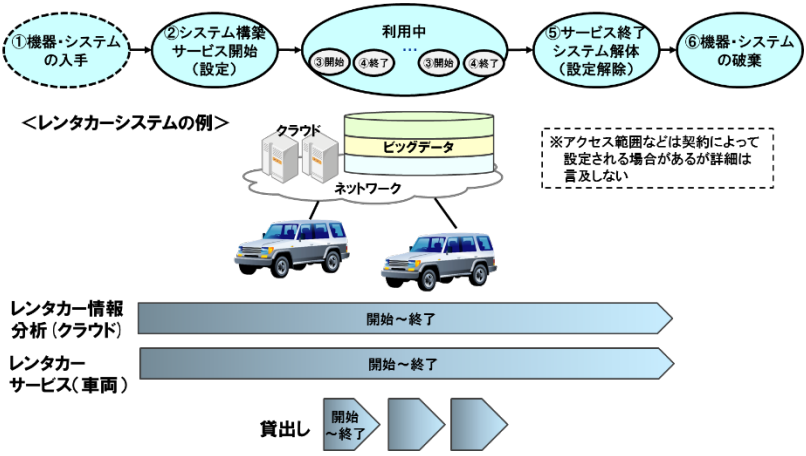


図 2-5 「開始」と「終了」の捉え方

2.4 IoT 高信頼化機能の活用の考え方

本書の IoT 高信頼化機能は、分野横断的に活用できることを想定し、各分野で広く適用していただくために、IoT の高信頼化を実現するために必要となる機能をまとめた（第 3 章）。この IoT 高信頼化機能の適用に当たっては、対象となる IoT 機器やシステムのリスクアセスメントを実施し、対策が必要となる IoT 高信頼化機能を選択して、実装を検討することを想定している。また、適用に当たっては、2.3.1 の 3 階層の基本モデルを考慮し、どの位置に実装するかなども含めて、IoT 高信頼化機能の選択の検討が必要である。

適用方法の詳細については、第 4 章で示す。

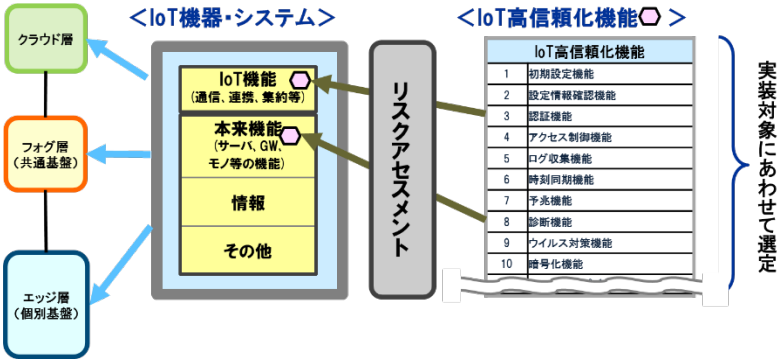


図 2-6 IoT 高信頼化機能の適用のイメージ

第3章
IoT 高信頼化機能

本章では、第 2 章で保守・運用の視点をもとに整理した IoT 高信頼化要件をさらに機能レベルに具体化し、IoT 高信頼化を実現するための機能要件と、実装時に活用するための IoT 高信頼化機能を整理した。さらに、IoT の特徴である障害や異常の広範囲な拡散や利用者・モノの接続が膨大、利用期間が長いなどの踏まえた実装上の考慮事項についても整理を行った。

IoT 高信頼化機能要件は実装時に必ず検討していただきたい内容であり、IoT 高信頼化機能は選択してご利用いただきたい。

なお、IoT 高信頼化機能については、基本的に必要と思われるものを抽出しているが、今後の技術の進歩、あるいは特定の分野によってさらに追加が必要となることが考えられる。

3.1 IoT 高信頼化要件・機能要件

表 3-1 に IoT 高信頼化要件・機能要件、および表 3-2 に IoT 高信頼化機能の一覧を示す。IoT 高信頼化機能要件の詳細は 3.1 で、IoT 高信頼化機能の詳細は 3.2 で説明する。なお、本章において、「必要である」、「望ましい」という表現は、検討していただく際の優先度を示している（「必要である」＞「望ましい」）。対策として実施するかどうかはリスクアセスメントの結果をもとに判断していただきたい。

表 3-1 IoT 高信頼化要件・機能要件一覧

IoT 高信頼化要件		IoT 高信頼化を実現するための機能要件	対応する IoT 高信頼化機能番号
開始	[要件 1]導入時や利用開始時に安全安心が確認できる	【機能要件1】初期設定が適切に行われ、その確認ができる	1、2
		【機能要件 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	3、4
予防	[要件 2]稼働中の異常発生を未然に防止できる	【機能要件 3】異常の予兆を把握できる	5、6、7、8、9
		【機能要件 4】守るべき機能・資産を保護できる	4、5、6、10
		【機能要件 5】異常発生に備えて事前に対処できる	11
検知	[要件 3]稼働中の異常発生を早期に検知できる	【機能要件 6】異常発生を監視・通知できる	12、13
		【機能要件 7】異常の原因を特定するためのログが取得できる	5、6
回復	[要件 4]異常が発生しても稼働の維持や早期の復旧ができる	【機能要件 8】構成の把握ができる	14
		【機能要件 9】異常が発生しても稼働の維持ができる	8、15、16、17
		【機能要件10】異常から早期復旧ができる	11、18、19、20
終了	[要件 5] 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	【機能要件11】自律的な終了や一時的な利用禁止ができる	18、21、22
		【機能要件12】データ消去ができる	23

表 3-2 IoT 高信頼化機能一覧

IoT 高信頼化機能			
1	初期設定機能	13	状態可視化機能
2	設定情報確認機能	14	構成情報管理機能
3	認証機能	15	隔離機能
4	アクセス制御機能	16	縮退機能
5	ログ収集機能	17	冗長構成機能
6	時刻同期機能	18	停止機能
7	予兆機能	19	復旧機能
8	診断機能	20	障害情報管理機能
9	ウイルス対策機能	21	操作保護機能
10	暗号化機能	22	寿命管理機能
11	リモートアップデート機能	23	消去機能
12	監視機能		

［要件1］導入時や利用開始時に安全安心が確認できる

(1) 概説

2016 年 1 月に、インターネットに接続された監視カメラのパスワードが未設定でのぞき見が可能となっているサイトがあるという問題が発生している[4]。このように、機器やシステム導入時に安全安心に係わる初期設定の不備による情報漏えいなどが発生することがあり、必要な初期設定が実施されているかの確認を支援する機能や、利用者がサービスの利用を開始するときに、利用が許可された者か、アクセスが可能なデバイスかなどの確認を支援する機能が必要である。

図 3-1 初期設定の必要性

(2) 要求される機能

【機能要件1】初期設定が適切に行われ、その確認ができる

システム構築時やサービスを開始する時は、安全安心に係わる初期設定が適切に行われ、その状態が確認できることが必要である。IoT では膨大な数の機器の設定や、様々な設置環境を考慮した通知方法などが必要であり、さらに安全安心な初期設定になっていることを確認できることが必要である。なお、一般的な管理者パスワード設定機能に加えて、個々の機器やシステムの初期設定が実施されていないと警告を発する機能や、システム全体においても現在の設定情報が分かりやすく確認できる機能などがあれば望ましい。

【IoT 高信頼化機能】初期設定機能[1]、設定情報確認機能[2]

【機能要件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

不正アクセスやデータ改ざんなどを防止するためには、利用者や機器などが接続される時に、本人や正しい機器であるかどうかを確認でき、設定された条件にしたがって利用許可を行うとともに許可されていない場合には利用を制限する機能が必要である。例えば、機器の機能単位に ID を付与（１つの機器に異なる種類のセンサーが複数設置され、それぞれにおいて ID が異なる場合がある）して認証する機能や利用範囲を限定するアクセス制御などの機能がある。なお、高度なセキュリティが必要な時は、PKI 認証や、生体認証などの機能、相互の信用度を確認して接続の可否判断をする機能などがあれば望ましい。

【IoT 高信頼化機能】認証機能[3]、アクセス制御機能[4]

(3) 実装上の考慮事項

①　接続する機器の増加への対応

IoT の機器数は 2020 年には 500 億個になると言われている。接続個数が膨大になり、管理テーブルの大きさなどのシステムのキャパシティを超えると、サービスの性能低下や制御不能になるリスクがある。これは特に、人命、財産、社会インフラなどに係る IoT 機器・システムの場合には深刻な問題となる。したがって、管理テーブルの大きさなどのキャパシティの設計を行う際には、接続個数の増加見込みなどを考慮する必要がある。

【IoT 高信頼化機能】初期設定機能[1]

②　リスク度合いに応じた権限設定

IoT の場合、保護すべき対象は情報資産だけでなく、人命、財産などに影響を与えるものになりうるため、リスク度合いに応じたアクセス権限の制限を設定する必要がある。

【IoT 高信頼化機能】認証機能[3] 、アクセス制御機能[4]

③　あらかじめ競合が予測できる場合の考慮

現在、利用している IoT 機器・システムを新たに別のサービスに接続する場合に、現在の状況と競合することが予測できる場合には、競合解決のための機能を考慮する必要がある（要件３　実装上の考慮事項②参照）。

④　接続時の信用度確認

認証機能やアクセス制御に加えて、相手の信用度を確認してサービスの提供範囲を判断することが必要な場合がある。例えば、工場のラインにおいて実績のない装置を組み込む際に、信用度を確認することでライン全体への悪影響が回避できる。信用度は、サービス開始時や接続の開始時に確認することが考えられる。信用度としては、品質保証レベル、セキュリティレベル、機能安全レベル、業界内の認定機関による情報などが考えられ、また、検討された例としては、C2C-CC にて議論中の Trust Assurance Level [5]などがある。

【IoT 高信頼化機能】認証機能(3)、アクセス制御機能(4)

［要件2］稼働中の異常発生を未然に防止できる

(1) 概説

IoT 機器・システムに異常が発生した場合には、他の接続された IoT 機器・システムに異常が波及することが想定される。IoT 機器・システムの安定稼働を維持するためには、異常の発生を予知し、未然に防止することが重要である。そのためには、異常の予兆を把握できる事象を想定し、予兆に必要な情報を取得し、判断基準に基づき対応の必要性（機器交換など）を判定し、通知することが必要である。特に、IoT では利用者などの関係者が多岐にわたるため、いつ、誰に、どのような手段で通知すべきかを検討することが必要である。

また、守るべきものを特定し改ざんや漏えいが出来ないようにガードをかけることが必要である。

さらに、長期間利用されることが想定される IoT 機器・システムでは、不具合や脆弱性などの既知の問題を事前に改修できることが望ましい。

図 3-2 予兆の把握、機能や資産の保護

(2) 要求される機能

【機能要件3】異常の予兆を把握できる

異常の予兆の対象となる事象を特定し、予兆の把握に必要な情報を取得・分析し、判断基準に基づき異常の発生を予測し、それを通知する機能が必要である。例えば、IoT 機器・システムの稼働中の各種情報をログとして収集し、故障に結びつくハードウェアの劣化状況、リソースの枯渇状況、セキュリティ異

常につながる状況にあるかなどを判断し、異常が発生する前に警告を出すことなどが考えられる。

また、異常発生の可能性が高い状態に陥っていない事を積極的に確認するために、ハードウェアの正常動作を確認する定期診断やIoT機器・システムのブート診断（POST）、セキュリティ異常を予防するためのウイルス対策機能などがあると望ましい。

【IoT高信頼化機能】ログ収集機能[5]、時刻同期機能[6]、予兆機能[7]、診断機能[8]、ウイルス対策機能[9]

【機能要件4】守るべき機能・資産を保護できる

セーフティやセキュリティの観点から守るべきものを特定し、それらを保護する機能とその保護状態が維持出来ていることを確認する機能が必要である。例えば、守るべきものとしては、「つながる世界の開発指針」では、「IoT機能」、「本来機能」、「情報」、「その他（ATM内の現金、自動販売機内の商品など）」に分類している。その中の「情報」としては、ユーザ情報や画像コンテンツ、機器情報、設定情報などがある。IoT機能はネットワークに接続するため、ネットワーク保護対策としてファイアウォール、暗号通信などが考えられる。本来機能、情報については、機能やデータの保護対策としてメモリプロテクション、暗号化、情報へのアクセス制限などが有効である。その他については物理的な鍵や開封時のアラームなどの対策が必要である（耐タンパー）。さらに、保護状態が維持出来ていることを確認できることが重要であり、ログ収集機能で考慮することが望ましい。

【IoT高信頼化機能】アクセス制御機能[4]、ログ収集機能[5]、時刻同期機能[6]、暗号化機能[10]

【機能要件5】異常発生に備えて事前に対処できる

IoT機器・システムを健全な状態に維持するためには、ハードウェアの劣化や性能不足、既知のソフトウェア不具合やセキュリティ脆弱性などの問題に出来る限り素早く対応することが必要である。そのためには、IoT機器・システムの寿命や既に分かっている問題に対してのハードウェア交換、リソース増強、ソフトウェアアップデートなどが必要である。特に、ソフトウェアアップ

デートについては、遠隔で改修できるリモートアップデート機能が望ましい。アップデートのデータそのものが改ざんされる可能性もあり、署名などの対策機能（セキュアアップデート）の考慮も必要である。また、改修した箇所については記録しておくことが望ましい。

なお、リモートアップデートは、異常発生する前の予防としての対策として位置づけているが、ソフトウェアの改修であり、回復の機能としても位置づけられる。

【IoT 高信頼化機能】リモートアップデート機能[11]

(3) 実装上の考慮事項

① 予兆の把握が難しい場合の対応

IoT 機器・システムの中には、常時接続されていない場合や、適用環境が変化する（移動含む）など予兆の把握が難しい場合がある。常時接続でない場合においては、定期的な接続を行い、そのタイミングでのログ収集や、環境が変化する場合においては、想定される環境のパターンを考慮しておくことが必要となる。

【IoT 高信頼化機能】ログ収集機能[5]

② 改修を可能にするための考慮

例えば脆弱性の改修を長期間にわたって行い続けることにより、領域の枯渇などリソース不足になって改修ができなくなる場合がある。IoT 機器・システムの改修を行うためには、必要なリソース（改修の作業領域など）の余地を残し、かつ、リソース不足になる前に警告することが望ましい。

【IoT 高信頼化機能】予兆機能[7]、リモートアップデート機能[11]

③ 性能への影響の考慮

1) 予兆の把握による負荷

IoT 機器・システムにおいて、大量のログ収集、ウイルスチェックや定期診断が負荷の増大につながる可能性がある。ログ生成タイミングの設定、ウイルスチェックや定期診断を利用時間の少ない時間帯に実行するためのスケジューリング機能や、実行優先度を下げて緩やかに実行するプライオリティ制御などの対策を考慮することが望ましい。

【IoT 高信頼化機能】ログ収集機能[5]、診断機能[8]、ウイルス対策機能[9]

2)改修による負荷

リモートアップデートを実施する場合は、対象機器に負荷がかかるため、1項と同様に、本来機能の遂行への影響を低減する対策が必要である。また、使用するネットワークの負荷が増加することに配慮した配信方法の検討が必要である。例えば、配信サーバ側では、対象となるデバイス数を管理し、ネットワークが過負荷にならないように一度に配信する個数を制限するなどの方法が考えられる。

【IoT 高信頼化機能】リモートアップデート機能[11]

3)ログ集約・予兆の性能

低リソースの IoT 機器（センサーなど）では、機器自身でログ分析が困難な場合があるため、集約装置にログを集約し、障害の予兆のためログ分析を実施する方法がある。このケースでは、集約装置では、予兆対象機器の個数や取得するログの量などを規定し、一度に予兆する個数を制限し、分割して予兆ができるような工夫があれば望ましい。

【IoT 高信頼化機能】ログ収集機能[5]、予兆機能[7]

［要件3］稼働中の異常発生を早期に検知できる

(1) 概説

IoT システムは、一般に多数のセンサーなどの IoT 機器で構成されることが多く、かつ、他の IoT システムと連携してサービスが提供され、複雑な構成となることがある。これらの複雑化した構成の中で、一部の IoT 機器の障害/故障やセキュリティ異常が連携システム全体に影響を及ぼすことが想定されるので、異常の早期発見と被疑箇所の特定が重要となる。そのためには、普段からのシステムの監視や異常の原因を切り分けるための動作ログを収集することが必要である。

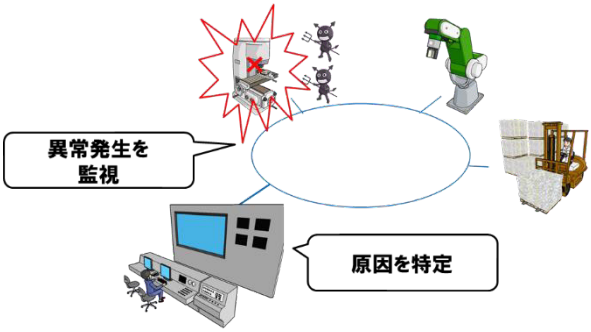


図 3-3 監視と原因特定

(2) 要求される機能

【機能要件6】異常発生を監視・通知できる

IoT 機器・システムの監視では、システムの各構成要素が保有する障害/故障やセキュリティ異常などの監視機能の能力を見極めて、システム全体としてもれなく監視が行き届くような設計が必要である。また、監視対象を明らかにして、その状態を逐次確認することが可能な状態可視化機能が必要である。なお、IoT の監視では、IoT 機器・システムの障害/故障やセキュリティ異常だけでなく、IoT 機器・システムなどに対する制御の競合が発生していないことを監視できる機能も必要である。制御の競合の検知については後述する。

【IoT 高信頼化機能】監視機能[12]、状態可視化機能[13]

【機能要件7】異常の原因を特定するためのログが取得できる

IoT 機器・システムは、複雑な構成をとることが多く、障害/故障やセキュリティ異常を切り分けるためのログが必要である。また、異なるベンダーの IoT 機器の組み合わせや異分野のシステム連携などでは、障害/故障やセキュリティ異常が発生した場合に障害の切り分けが困難となることも想定されるため、自社の IoT 機器・システムに問題がないことを証明するためにもログの収集機能が必要である。なお、ログ自体が改ざんされる可能性があり、ログの暗号化などの保護の対策機能が必要である。

また、IoT システムでは、多種多様の IoT 機器がつながることが想定されるが、各 IoT 機器の時刻にバラツキがあると取得したログの時刻が合わず、解析ができないケースが想定される。そのため、時刻同期の機能が必要となる。

【IoT 高信頼化機能】ログ収集機能[5]、時刻同期機能[6]

(3) 実装上の考慮事項

① 個々での異常検知ができない場合の考慮

例えば、多数のセンサーが接続されている場合に、個々のセンサーの障害を監視することが困難な場合がある。そのような場合に、複数のセンサーからあげられてくるセンシング値を比較し、「外れ値（統計において他の値から大きく外れた値）」などにより、センサーの異常の推測を行うことが考えられる。このように、個々の IoT 機器での異常検知ができない場合に、異常情報以外の値や複数の情報を用いて、異常を推測することが考えられる。

【IoT 高信頼化機能】監視機能[12]

② 競合への考慮

IoT では、各種サービスが複雑に連携するケースが想定され、一つの IoT 機器・システムが同時に複数のサービスから相反する指示を受けることがある。例えば、住宅の中で、快適サービスからは、暑くなってきたので窓を開ける指示と、一方、防犯サービスでは、窓を閉める指示が出されるなど、制御が競合する場合がある。競合の状況が検知できることが重要であり、競合状況としては、互いに正常な指示の競合だけでなく、一方が不正な指示による競合も想定が必要となる。

次に、競合の検知後の対策として、人による判断と自動判断が考えられる。後者については、環境条件を考慮したシナリオによる優先度制御が有効と考えられる。

【IoT 高信頼化機能】監視機能[12]

③　セキュリティ攻撃の分析

管理者権限（ID）でのログイン失敗や、攻撃回数のチェックなどを実施し、異常値は警告を発するなどの検討が必要である。

【IoT 高信頼化機能】監視機能[12]

④　IoT 構成の変化のチェック

意図しない IoT 機器・システムの設置、接続や紛失を確認し、警告を発するなどの検討が必要である。

【IoT 高信頼化機能】監視機能[12]、構成情報管理機能[14]

⑤　誤検知の対策

重要なデータに係る異常の誤検知をしてしまい、誤ってシステムが停止するなどのリスクを防止する方法としては、複数のデータを組み合わせて異常を検知する方法が考えられる。しかしながら、すべての情報に対して複数のデータを組み合わせて検知することはコストの増加につながるので、重要なデータに係る異常に絞って検知することが考えられる。

【IoT 高信頼化機能】監視機能[12]

⑥　ログの量や種類が多いことの考慮

複数ベンダーの機器が混在する IoT では、ログ収集は、原因特定のためには必要であるが、必要なログが無くて分析できないケースがある。ログ設計では、何をするためにどんなログが必要かをあらかじめ見極め、必要なログが消えないようなログ収集方式の検討が必要である。ログを収集する機器の数が多い場合は、ログの格納領域が不足することが想定される。そのような場合には、ログのローテーションや、最新の障害情報などの重要な情報については選択して格納することが望ましい。また、ログの種類が多い場合は、障害、セキュリティ異常に関するものなど重要なものは確実に保存されるようにすることが望ましい。また、障害ログなどにおいて、同じログが多発する場合には圧縮することが考えられる。さらに、当該機器やシステムでは収集できない情報については、つながっている相手から入手する方法も考えられる。

【IoT 高信頼化機能】ログ収集機能[5]

［要件4］異常が発生してもシステム稼働の維持や早期の復旧ができる

(1) 概説

IoT 機器・システムは、交通監視システムや災害監視システムなど社会インフラに適用されるケースもあり、高いシステム稼働率が要求されることもある。IoT 機器・システムに障害が発生した場合は、システムの稼働を維持するための対策やシステム停止など重度な障害に対する復旧の対策が必要である。また、つながっている他の IoT 機器・システムへの被害の拡大を防ぐ対策も必要である。稼働を維持する対策としては、例えば、障害箇所の切り替えや縮退、隔離、ネットワークの遮断などがある。復旧対策としては、当該機器・システムのリセット・リブートやデータ復旧、ロールバックなどが考えられる。なお、IoT システムでは特にシステム構成が頻繁に変化する可能性があるため、最新のシステム構成を把握しておくことが必要である。

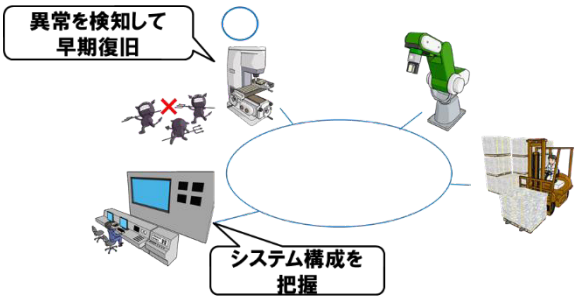


図 3-4 検知と早期復旧

(2) 要求される機能

【機能要件8】構成の把握ができる

IoT システムは、日々変化することが想定され、障害などが発生した際に、切り替えや縮退などによる処理の継続や、あるいは異常状態からの復旧（自動復旧含む）やその原因分析を行うために、構成情報管理が必要である。構成情報管理としては、システムを構成しているハードウェアやソフトウェアの種

類・バージョン、接続情報、状態情報などを管理することが必要である。特に、多数台の IoT 機器接続や自律分散システムにおいては、構成情報を定期的に自動取得できることが望ましい。

【IoT 高信頼化機能】構成情報管理機能[14]

【機能要件9】異常が発生しても稼働の維持ができる

障害が発生した場合に、一部の IoT 機器や機能を切り離す縮退や、セキュリティ異常の発生したアプリケーションや IoT 機器の隔離などによって処理を継続できる機能が必要である。また、重要なシステムでは、障害/故障に対して堅固であることが求められ、冗長構成によって処理を継続できる機能が必要である。なお、冗長構成の予備系などの通常は使用されていない機能や機器については、定期的な動作確認を実施することが望ましい。

【IoT 高信頼化機能】診断機能[8]、隔離機能[15]、縮退機能[16]、冗長構成機能[17]

【機能要件10】異常から早期復旧ができる

障害が発生し処理の継続が困難な場合には、当該 IoT 機器・システムの自動停止や、人や監視サーバなどからの当該 IoT 機器・システムの停止、ネットワークからの切り離しなどの機能が必要となる。IoT 機器・システムの停止や、ネットワークから切り離された場合には、早期に復旧させることが必要となる。復旧においては、リブート、ネットワークの再接続の機能が必要であり、特に、遠隔地などにある IoT 機器・システムでは、リモート操作でそれらの再接続操作ができることが望ましい。さらに、データが壊れていないかを確認する機能や、必要に応じてデータをロールバックする機能などがあると望ましい。なお、障害の原因特定のために、復旧の前に、障害に関する重要な情報を退避する機能も必要である。

これらの当座の対策に加えて、原因を分析・特定し、ソフトウェアに不具合がある場合には、リモートアップデート等で改修することも必要である。

【IoT 高信頼化機能】リモートアップデート機能[11]、停止機能[18]、復旧機能[19]、障害情報管理機能[20]

(3) 実装上の考慮事項

① 変化する構成情報への対応

IoT では構成が変化する可能性が高いため、構成情報の把握が困難な場合が想定される。そのため、静的な構成情報の管理だけでなく、動的に構成情報を把握できる機能の考慮が必要である。

【IoT 高信頼化機能】構成情報管理機能(14)

② 縮退運転時の考慮

IoT システムは、複数のベンダーやシステム構築者、サービス提供者など多くの関係者で構成されるため、縮退運転時や、縮退運転からの復旧時には、関係者間の情報連携が重要である。そこで、縮退運転中であるという状態を周囲へ伝える仕組みを考慮することが望ましい。また、縮退運転から復旧した場合にも、同様の考慮をすることが望ましい。

【IoT 高信頼化機能】縮退機能(16)

③ 復旧時の同期確認に係る考慮

復旧時には、システムやアプリケーションの立ち上げだけではなく、データの復旧やユーザ状態の復旧などの多くの処理が必要である。そこでは、起動順序の同期やデータの整合性を考慮しなければならない場合が想定される。例えば、多数の IoT 機器から構成されるシステムで大規模障害が発生し、電源投入からの復旧が必要になる場合があるが、一度に多数の機器の電源を投入すると電力供給量を超えて、電力投入を失敗するケースがある。電力供給量を見積もり、一定の台数単位に順番に電源を投入する方法があると望ましい。

【IoT 高信頼化機能】復旧機能(19)

④ 部分的に回復しない場合の考慮

IoT システムの復旧において、関係する IoT 機器が多数あるときは、正常に立ち上がらない IoT 機器が出てくることが想定される。したがって、復旧が完了したときは、管理すべき対象の IoT 機器がすべて正常に立ち上がり、使える状態になっていることの確認が必要である。また、システム間連携時は、相手のシステムと正常に連携出来ていることを相互に確認することが望ましい。

【IoT 高信頼化機能】復旧機能(19)

［要件5］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

(1) 概説

利用者が、あるサービス単位の利用を終了する場合、利用者が正常な終了を指示し忘れる可能性がある。その際には、機器の稼働状態の放置、盗難などにより事故や情報漏えいなどが発生するリスクがある。したがって、利用者が正常な終了手順を忘れにくくするとともに、忘れた際に IoT 機器・システムが稼働状態のまま放置されても、安全を保つことが必要である。

また、共用端末など頻繁に利用者が変化する場合は、ID、パスワードなどの設定情報や、様々な情報が格納されたままでは、セキュリティ異常が発生する可能性がある。したがって、消去する対象を定めて、確実に消去を実施できる対策が必要である。さらに、IoT システムを解体した後に、IoT 機器を中古販売や破棄業者に渡す場合においては、情報が漏えいするリスクがあるため、内部に格納された情報を確実に消去できる対策が必要である。

図 3-5 データ消去の必要性

(2) 要求される機能

【機能要件11】自律的な終了や一時的な利用禁止ができる

IoT 機器・システムは、遠隔から操作されることが考えられ、終了させたつもりでも操作ミスや通信の異常などにより、稼働状態のままとなる場合が想定される。例えば、エアコンのつけっぱなしなどが発生する。また、スマートフォンの置き忘れや盗難時には、他人により異常操作されるリスクがある。その対策として、長期間稼働状態のままの場合に自律的に終了する機能や、放置や

盗難時において、一時的に利用禁止にする操作保護機能が必要である（遠隔ロック等）。さらに、IoT 機器・システムの使用期間や稼働時間満了時には利用者に通知できると望ましい。

【IoT 高信頼化機能】停止機能[18]、操作保護機能[21]、寿命管理機能[22]

【機能要件12】データ消去ができる

IoT では、モバイル端末の中古利用や共有で使用するケース、また乗用車のレンタルなど利用者が変化する場合があり、利用終了時には情報を消去することが求められている。また、IoT サービスをとりやめて、IoT 機器を破棄する場合にも、格納されていた情報の消去機能が必要である。

【IoT 高信頼化機能】消去機能[23]

(3) 実装上の考慮事項

① 自律的な終了/停止の無条件実施の可否に関する考慮

自律的な終了や停止は、安全を保つために有効な場合だけでなく、逆に安全を脅かす場合もありうるため、条件の設定ができるような機能の考慮が必要である。

【IoT 高信頼化機能】停止機能[18]

② データの完全な消去

設定の初期化や、保存したデータを削除しただけでは、データの復元が可能となる場合がある。例えば、HDD などは、通常の削除処理として実行されるファイルアロケーションテーブルのクリアだけでは、復元が可能な場合があるため、ランダムなデータの上書きなど IoT 機器の用途に応じた消去機能が必要である。データの消去については、実装上の位置や情報漏えいリスクに応じた機能を考慮する必要がある。

【IoT 高信頼化機能】消去機能[23]

③ 使用期間や稼働時間の考慮

IoT 機器・システムは、多種多様のセンサーなどで構成され、日々増減する場合やライフサイクルが長いことから、デバイスの寿命管理が煩雑となる。この問題を解決するには、IoT 機器自身にて使用期間管理や稼働時間管理などの寿命を管理し、事前通知する機能が必要である。

【IoT 高信頼化機能】寿命管理機能[22]

3.2 IoT 高信頼化機能

IoT 高信頼化機能要件の実現のために利用できる IoT 高信頼化機能を示す（一覧は前述の表 3-2 に記載）。

(1) 初期設定機能

目的	システムの構築・接続時や利用開始時に必要な設定が実施されるようにする。
説明	初期設定機能には以下のような機能がある。 ・ 各種情報の範囲設定 ・ 管理者権限、利用者権限などのパスワード設定（デフォルトパスワードからの変更機能、強固なパスワード設定を促すガイド機能含む） ・ アクセス制御の設定 ・ 不要なポート・サービスの停止 ・ ソフトウェアのアップデートの設定 ・ 信用度に関する情報の設定　など 未設定の場合には、システムの利用を開始できないようにする
参考	

(2) 設定情報確認機能

目的	機器・システムの設定情報の確認を行う
説明	設定情報確認機能には以下のような機能がある。 ・ システムの構築・接続時や利用開始時に、個々の機器やシステムの初期設定が適切に実施されていない場合の警告 ・ システム全体において設定情報をわかりやすく確認
参考	

(3) 認証機能

目的	利用者、機器などを一意に識別し、本人、あるいは、正しいものであるかどうかを確認する。
説明	認証方式には以下のような方式がある。 ・ 接続する IoT 機器のなりすまし防止 　– IoT 機器の識別子による認証 　– クライアント証明書による認証 　– メッセージ認証 ・ 利用者のなりすまし防止 　– ID・パスワードによる認証 　– IC カードなどの所有物による認証 　– 生体認証 ・ 接続する相手のシステム・サービスのなりすまし防止 　– 接続する相手のシステム・サービス相互で鍵・電子証明書等を使用した認証 上記の、いくつかの方式を組み合わせた多要素認証などの方式もある。 また、一定回数以上の認証に失敗した場合にロックする機能などがある。
参考	・ [IoT 推進コンソーシアム]IoT セキュリティガイドライン http://www.meti.go.jp/press/2016/07/20160705002/20160705002-1.pdf ・ [CSA]IoT 早期導入者のためのセキュリティガイダンス https://www.cloudsecurityalliance.jp/newsite/wp-content/uploads/2016/02/Security_Guidance_for_Early_Adopters_of_the_Internet_of_Things_J_160224.pdf ・ [CRYPTREC]電子政府推奨暗号の利用方法に関するガイドブック http://www.cryptrec.go.jp/report/c07_guide_final.pdf

(4) アクセス制御機能

目的	守るべきものを保護するために、守るべきものに対する操作を制限する。
説明	アクセス制御は認証によって識別された ID に基づいて、守るべきものに対する操作を許可、または拒否する。 アクセス制御方式には、以下のような方式がある。 ・ 任意アクセス制御（DAC） ・ 強制アクセス制御（MAC） ・ ロールベースアクセス制御（RBAC）
参考	

(5) ログ収集機能

目的	機器やシステム上で発生した事象を追跡可能とするために、発生したイベントに関する情報を蓄積する。
説明	ログ収集機能には以下のような機能が含まれる。 ・ 特定のイベントに関連した記録をするための情報に関するログ生成 ・ リソースの少ない IoT 機器などの場合に、他の機器へのセキュアなログ転送 ・ ログの保存 – ログの保存においては、リソースが限られている場合のローテーションやログ喪失防止のためのバックアップがある – 保存したログの保護にはアクセス制御、暗号化、追記のみ可能とするなどの方法がある ・ 不要となったログの破棄 記録する内容の例 ・ セキュリティ解析用：攻撃、ユーザ認証、データアクセス、構成管理情報更新、アプリケーション実行、ログの記録開始・停止、通信、扉の開閉、チェックサム、移動履歴 ・ セーフティ解析用：故障情報（ハードウェア/ソフトウェア） ・ リライアビリティ解析用：結果情報、状態情報、動作環境情報（温度、湿度、CPU 負荷、ネットワーク負荷、リソース使用量等）、ソフトウェアの更新
参考	[NIST] SP800-92 コンピュータセキュリティログ管理ガイド http://www.ipa.go.jp/files/000025363.pdf

(6) 時刻同期機能

目的	機器・システム間で時刻を合わせる。
説明	時刻同期には、基準となる絶対時刻に合わせる方式と、つながる機器・システム間で相対的な時刻のずれがないように合わせる方式があり、例えば以下のような方式がある。 ・ 絶対時刻にあわせる方式 – 10ms 程度の精度の NTP ・ 相対的な時刻に合わせる方式 – 1 μs 以下の精度の IEEE1588 PTP – 無線 LAN における時刻同期のための IEEE802.11 TSF
参考	・NTP http://www.ntp.org/ ・IEEE1588 PTP(Precision Time Protocol) ・IEEE802.11 TSF(Timing Synchronization Function) ・IEEE802.1 TSN（Time Sensitive Networking） ・IEEE802.15.4 Time-slotted communication model https://standards.ieee.org/から購入が必要

(7) 予兆機能

目的	近い将来に異常となることが見込まれることを予測し、正常な範囲内でも対応を促す。
説明	予兆として把握すべき事象を定め、必要な情報を取得・分析し、判断基準に基づき異常の発生を予測し、通知する。予兆の把握には機械学習などを活用して、例えば下記のような状態の変化を把握する方法がある。 ・ 周期的な状態の傾向の変化 ・ 状態の推移の傾向の変化 ・ 相関関係の高い複数の状態の関係の変化
参考	・ システムの異常予兆を検知するリアルタイム監視ソリューション https://www.fujitsu.com/jp/documents/about/resources/publications/magazine/backnumber/vol67-2/paper04.pdf ・ インバリアント解析技術（SIAT）を用いたプラント故障予兆監視システム http://jpn.nec.com/techrep/journal/g14/n01/pdf/140126.pdf

(8) 診断機能

目的	異常発生の可能性が高い状態に陥っていないかをテストなどにより積極的に確認する。
説明	診断機能には以下のような機能がある。 ・ 機器やシステムを起動し、オンラインになる前にハードウェアの正常性の確認を行うブート診断 ・ オンラインになってから、一定の期間ごとに正常性の確認を行う定期診断 なお、冗長構成などで普段動作していない箇所の診断も考慮する。
参考	[IPA]組込みシステムのセキュリティへの取組みガイド http://www.ipa.go.jp/files/000013968.pdf

(9) ウイルス対策機能

目的	ウイルス感染の被害を防止する。
説明	ウイルス対策には、検出（侵入、実行、潜伏を含む）、駆除がある。検出には以下のような方式がある。 ・ ホワイトリスト方式 – 特にリソースの少ない IoT 機器の場合においては、登録されたソフトウェアのみ実行を許可することで、未知のウイルスの実行を防止する。 ・ ブラックリスト方式 – ウイルスチェックには、既知のウイルスをパターンファイルに登録し侵入、実行、潜伏を検出する。 ブラックリスト方式は、リソースが少ない場合には実装が難しいことが想定される。
参考	制御システム向けの端末防御技術「ホワイトリスト型ウイルス対策」とは？ http://monoist.atmarkit.co.jp/mn/articles/1404/07/news004.html

(10)　暗号化機能

目的	機器やシステムに格納されたデータ、または通信経路上のデータを、暗号技術を用いて電子署名や暗号化を行う。
説明	暗号化機能の詳細は参考に示す文献に記述されている。 暗号化する際は、適切なセキュリティ強度を持った暗号アルゴリズム、鍵長の使用や、鍵の適切な管理が必要となる。リソースの限られたデバイスにも実装可能な「軽量暗号」も開発されている。 暗号化機能は、認証や改ざん検知などでも用いられる。
参考	・ [IPA]IoT 開発におけるセキュリティ設計の手引き https://www.ipa.go.jp/files/000052459.pdf ・ [CRYPTREC] 電子政府推奨暗号の利用方法に関するガイドブック http://www.cryptrec.go.jp/report/c07_guide_final.pdf ・ [CRYPTREC] 暗号技術調査 WG（軽量暗号）報告書 https://www.cryptrec.go.jp/estimation/techrep_id2406.pdf

(11) リモートアップデート機能

目的	ソフトウェアの不具合や脆弱性を改修するために、遠隔で更新を行う。
説明	リモートアップデート機能には以下のような機能が含まれる。 ・アップデートファイルの暗号化、署名 ・改修した箇所の記録(ログ収集機能) ・アップデートスケジューリング ・アップデート優先度設定 ・アップデート、及び失敗した場合のバージョンダウン アップデートは遠隔での実行に限らないが、IoT 機器・システムでは、特に離れた場所での保守が見込まれるため、リモートアップデート機能に注目した。
参考	

(12) 監視機能

目的	機器・システムの異常を検知する。
説明	監視機能には以下のような機能がある。 ・ 異常の検知機能 – 障害/故障の検知(ログ分析含む) – セキュリティ異常の検知(ログ分析含む) – 制御の競合の検知 等 ・ 検知した異常の通知機能
参考	

(13) 状態可視化機能

目的	機器・システムの稼働状態を表示する。
説明	状態可視化機能には以下のような機能がある。 ・ 最新の稼働状態の表示 ・ 時系列での稼働状態の表示 ※監視機能の一部と捉える考え方もある
参考	

(14) 構成情報管理機能

目的	機器・システムを構成している情報を管理する。
説明	構成情報管理機能では以下のような情報を管理する。 ・ ハードウェアの種類・バージョン ・ ソフトウェアの種類・バージョン ・ システムを構成している機器の証明書更新状況 ・ 接続情報(ネットワーク構成、電源関連 等) ・ 利用可、利用不可などの情報 等
参考	[IPA]技術参照モデル(TRM) 第 5 章「技術ドメイン解説」クイックリファレンス https://www.ipa.go.jp/files/000025495.pdf

(15) 隔離機能

目的	異常の発生したアプリケーションや機器・システムを、他の正常なアプリケーション、機器・システムから遮断する。
説明	隔離機能には以下のような機能がある。 ・ アプリケーションの隔離 – ウイルス感染を検知した場合に、アプリケーションを実行できないように隔離（ウイルス対策機能参照） ・ 機器・システムの隔離 – セキュリティポリシーに沿っていない場合や、異常を検知した場合に機器を切り離し、場合によっては接続を隔離ネットワークへ切り替え　など
参考	[日経 BP] 検疫ネットワークを実現する方式 http://itpro.nikkeibp.co.jp/article/lecture/20070522/271750/

(16) 縮退機能

目的	システムの一部に障害が発生しても、機能や性能を制限し、稼働を完全に停止することを防ぐ。
説明	縮退機能には以下のような機能がある。 ・ 複数の機器で構成されている場合に、1つの機器に障害が発生してもその機器を切り離して、処理を継続する機能 – 例えば、多数のセンサーが接続されていて、あるセンサーが異常となった場合は、それを切り離す機能 ・ 性能を制限しても処理を継続する機能 – 例えば、通信において、回線状態が悪化して本来のスピードで通信が行えない場合に、自動的に低速モードに切り替えて通信を継続する機能
参考	[IPA]インターネットサーバーの安全性向上策に関する調査 https://www.ipa.go.jp/security/fy14/contents/high-availability/guide.html

(17) 冗長構成機能

目的	システム、あるいはシステムを構成する機器などを複数用意することにより、一つのシステムや機器に障害が発生しても全体としては機能や性能を維持する。
説明	冗長構成機能には以下のような機能がある。 ・ ある機能を単一の機器ではなく、予備系を含めた複数台の機器で構成する機能 ・ 異常時の切り替えを判断する機能 ・ 異常時の切り替え機能 ・ 切り戻し機能
参考	[IPA]インターネットサーバーの安全性向上策に関する調査 https://www.ipa.go.jp/security/fy14/contents/high-availability/guide.html

(18) 停止機能

目的	機器・システムが放置され処理の継続が危険な場合や、異常の発生により処理の継続が困難な場合などに、機器・システムを停止する。
説明	停止機能には以下のような機能がある。 ・ 自律的停止 – 利用終了すべきときに放置された場合などで、一定の条件下における機器・システムの自律的な停止 ・ 人または監視装置などからの停止(遠隔停止指示含む) – セキュリティ異常や障害/故障などが発生した場合の強制的な停止
参考	

(19) 復旧機能

目的	障害が発生し処理の継続が困難な場合に、機器・システムを処理の継続可能な状態に戻す。
説明	復旧機能には以下のような機能がある。 ・ リブート – 機器・システムによるリブート、人または監視装置などからの機器・システムのリブート ・ ネットワーク再接続 ・ データロールバック – 正常に機能していた時点までのデータの復元
参考	

(20) 障害情報管理機能

目的	障害の解析に必要な情報を収集し管理する。
説明	障害情報管理機能には以下のような機能がある。 ・ 障害種別と障害時に収集する情報のマッピング機能 ・ 障害発生時に機器・システムの障害情報を退避 – 障害発生時にリブートなど必要になる場合、解析よりもリブートが優先させることを想定し、障害情報を一時的に消えないメモリ領域に退避などしてリブート後に収集する。 ・ 障害情報の履歴管理機能
参考	[IPA]技術参照モデル(TRM) 第 5 章「技術ドメイン解説」クイックリファレンス https://www.ipa.go.jp/files/000025495.pdf

(21) 操作保護機能

目的	機器・システムの放置や盗難により、不正な操作をされる可能性がある状態にあるときに操作を受け付けない。
説明	操作保護機能には以下のような機能がある。 ・ 操作のロックと解除 – 機器・システムの自律的なロックや、人または監視装置などからのロック – 機器・システムの直接操作によるロックと遠隔ロック – 上記のロックの解除 ・ 難読化 – 画面情報などを利用者以外からは読み難くする機能
参考	[IPA]IoT 開発におけるセキュリティ設計の手引き https://www.ipa.go.jp/files/000052459.pdf

(22) 寿命管理機能

目的	稼働時間や使用期間を過ぎた利用を防止する。
説明	寿命管理機能には以下のような機能がある。 ・ 稼働時間管理 – 累積稼働時間が使用可能時間内であることの管理 ・ 使用期間管理 – メーカーが保証する使用期間内であることの管理 ・ EoL の事前通知機能 – 累積稼働時間や使用期間が期限に到達する前の事前通知 ※：ハードウェア、ソフトウェアの両方が対象
参考	

(23) 消去機能

目的	機器やシステムを破棄するときなどの情報の漏えいを防止する。
説明	ファイルの削除や、初期化（USB メモリのフォーマット等）では、特殊な方法で復元することが可能な場合がある。ここでいう消去は、完全にデータを読めなくすることである。消去機能では設定した情報や、保存したデータを消去する。 消去機能では磁気的に記憶された情報を完全に消去する必要があり、例えば以下のような方式がある。 ・ NSA 方式 ・ DoD 方式 ・ Peter Gutmann 方式　など
参考	・ NSA/CSS Policy manual 9-12 https://www.nsa.gov/resources/everyone/media-destruction/assets/files/storage-device-declassification-manual.pdf ・ DoD 方式（DoD5220.22-M） http://www.dss.mil/documents/odaa/nispom2006-5220.pdf ・ Secure Deletion of Data from Magnetic and Solid-State Memory https://www.cs.auckland.ac.nz/~pgut001/pubs/secure_del.html

＜コラム1＞ ヘルスケアと IoT

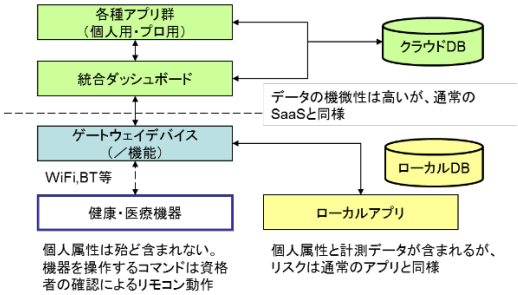
一般社団法人電子情報技術産業協会　鹿妻　洋之

【ウェアラブル健康機器から考えてみよう】

本来、ヘルスケアは医療と健康を幅広く包含する言葉ですが、日本国内においては、医療機器と健康機器には大きな規制上の差が存在しています。このコラムでは、一般にイメージを持ちやすい健康機器・サービスにおける IoT について、まずお話ししたいと思います。

ヘルスケア IoT で、まず思い浮かぶのはウェアラブル健康機器ではないでしょうか。手首に装着するバンド型のもので、活動量・歩数・活動パターン・睡眠等を計測する機能が備わっています。この中には、表示機能を持たないものもあり、計測されたデータは、スマートフォンなどの汎用端末に送付して、アプリ上で管理することになります。計測データを汎用端末に送付して管理する健康機器というように定義を広げていくと、血圧計・体重体組成計・体温計といった見慣れた機器が加わってきます。これらのデータを個別の専用アプリで管理することもありますが、多くの場合、複数カテゴリのデータを統合的に管理するアプリケーションがそれを担うことになります。このような使い方の中で気になるのは、機器からのデータが想定外の場所に送信、記録されてしまうことです。機器内部に個人属性に関連するような情報が記録されていることは少ないため、誤送信とそれに伴う消去でデータ欠損の可能性はあるものの、個人情報漏えいの可能性は少ないと言えます。

次に、このように統合されたデータは、どのように使用されるか考えてみましょう。一般的な IoT の世界では、集約されたデータは自動的に解析され、何らかのフィードバック制御に使用されることが多いわけですが、健康分野においては、若干状況が異なります。フィードバックをかける対象となる人間自体の系としての複雑さ、医師法等に定められる医療行為とみなされないための制約などから、分析等までとどめておくか、有資格者による確認作業の後で各種制御コマンドを発行することが主流となっています。この考え方は、医療分野に近い保健指導の現場や慢性疾患患者の重症化予防に用いられるシステムでも見ることができます。

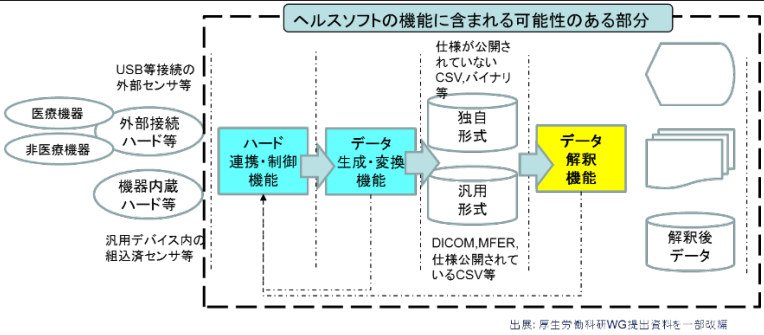


ヘルスケアデータの管理

【どのようなリスクが考えられるのか】

健康機器等と連携して汎用機器上で利用されるソフトウェアは、ヘルスソフトウェアと呼ばれています。このヘルスソフトウェアには、大きく分けて以下の三つの機能が実装されています（①ハード連携・制御機能、②データ生成・変換機能、③データ解釈機能）。ソフトとしての価値の中心は③の部分であるものの、リスクは各機能に存在しています。

ハード連携・制御機能	・センサー（医療機器等）に対して、誤った指示を発行する。 ・機器に対して指示した内容が、医療機器本来の機能に影響を与える。
データ生成・変換機能	・データ生成時点において、センサーからの情報劣化が生じ、次プロセスにおける解釈に誤謬を生じる。 ・データが欠損する。（特段の指示がある場合を除く）
データ解釈機能	・解釈した結果が、医学的な意味を有する。 ・解釈した結果に基づくメッセージを実行した場合に、利用者（患者等）に対して、悪影響を及ぼす



ヘルスソフトウェアの機能

第4章
IoT 高信頼化機能の適用

3 章では、IoT を高信頼化するための要件や機能を整理した。本章では、IoT 高信頼化要件、及び IoT 高信頼化機能として整理した内容を IoT 機器・システムの開発への適用手順を示す。適用は、主に次の 4 つの手順からなる。

(1) 開発の対象 IoT 機器・システムの基本モデル（図 2-3）へのマッピング
(2) リスクアセスメント
(3) リスク対策の決定
(4) IoT 高信頼化機能による対策

4.1 IoT 機器・システムへの適用手順

4.1.1 開発対象の基本モデルへのマッピング

本書では、図 2-3 に示した基本モデル、すなわちクラウド、フォグ、エッジの 3 階層モデルを前提としている。IoT 高信頼化機能の IoT 機器・システムへの適用に際しては、どの層に実装するかが重要になるため、まず開発対象をこのモデルにマッピングしておくことが必要である。

4.1.2 リスクアセスメント

4.1.1 で示したモデル化された開発対象となる IoT 機器・システムに対してセーフティ、セキュリティの観点からリスクアセスメントを行う必要がある。図 4-1 は、「つながる世界の開発指針」で示しているリスクアセスメント（守るべきものの洗い出し～リスク評価）の手順である。

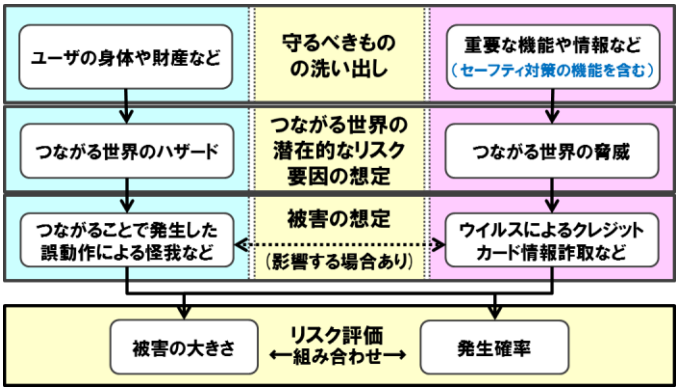


図 4-1 リスクアセスメントの手順

(1) 守るべきものの洗い出し

「つながる世界の開発指針」の指針 4 を参考にして、守るべきものの洗い出しを行う。守るべきものの例としては、指針 4 に記載されているものや、さらにそれを詳細化した付録 A のユースケース分析の事例であげているものなどがある。

(2) つながる世界の潜在的なリスク要因や被害の想定

「つながる世界の開発指針」の指針 5～7 を参考に、つながることによるリスクや、つながりで波及するリスク、物理的なリスクを想定する。基本モデルと「つながる世界の開発指針」の IoT 機器・システムの構成をもとに、該当する連携モデル、つながり方、対象とする機器やシステムを想定し、リスクを想定する。

リスクの想定においては、様々な利用環境や利用方法を網羅的に考えることが必要である。例えば、離島や遠隔地など、人が出向いて保守することが容易でない場所に設置されることなども想定する必要がある。

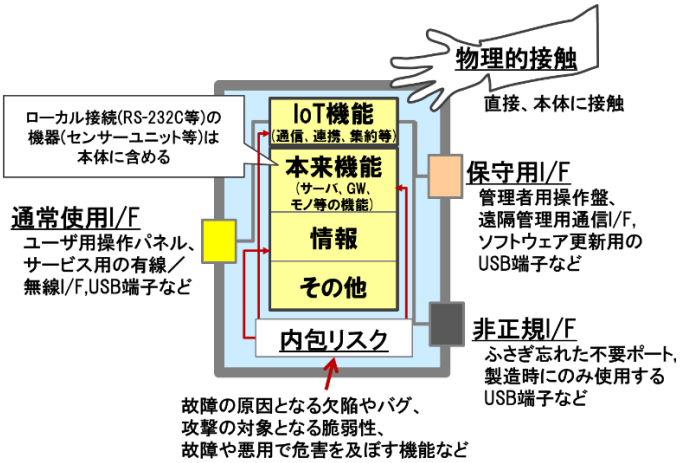


図 4-2 リスク箇所の例

(3) リスク評価

想定された各種リスクについて、被害の大きさと発生確率の両面から評価を行う。リスク評価についてはコラム 2 参照。

具体的なハザード分析や脅威分析の手法については、「つながる世界のセーフティ&セキュリティ設計入門」［6］が参考になる。

4.1.3 リスク対策の決定

4.1.2 で洗い出したリスクに対して、その対策方法を検討する。対策方法の検討に際しては、それをどのレベルまで対策するかという方針が前提として必

要となる。その方針にしたがって、表 3-1 で示した要件 1 から 5 の IoT 高信頼化要件について対策方法を定めていただきたい。

対策方法としては、ソフトウェアでの実装（IoT 高信頼化機能による対策）、ハードウェアでの実装、運用者（人）によるカバーなどが考えらえる。もちろん、被害が小さい場合や、発生確率が低い場合など、対策を実施しないことも考えられる（リスクの受容）。いずれの対策を実施するかは、被害の大きさや発生確率だけでなく、コスト、組織の方針、技術的実現性などを踏まえて優先度を考慮し、決定する必要がある。

対策を決定する際には、個別に検討を行うのではなく、全体として整合をとって検討する必要がある。検討の結果、IoT 機器・システムのハードウェア資源（CPU やメモリ、ネットワーク等）に制約があり IoT 高信頼化機能を実装していない場合、あるいは IoT 高信頼化機能を実装していない機器やシステムを接続する場合、それらを守ることができる構成を検討する必要がある。

4.1.4 IoT 高信頼化機能による対策

4.1.3 では、リスク対策を、ソフトウェアでの実装（IoT 高信頼化機能による対策）、ハードウェアでの実装、運用者（人）によるカバーなどに分類した。このうち、ソフトウェアでの実装（IoT 高信頼化機能による対策）について述べる。

ソフトウェアでリスク対策を行うには、そのソフトウェアがもつ機能要件を考える必要がある。それは、4.1.3 で示した IoT 高信頼化要件のうち、ソフトウェアでの対策を考えた要件を満たすものでなければならない。それらが IoT 高信頼化機能要件である。その IoT 高信頼化機能要件を満たす機能例として主なものを示したものが表 3-2 に示した IoT 高信頼化機能である。この中から、必要な機能を選択してご活用いただきたい。

4.2 IoT 高信頼化機能の検討例

付録 A でとりあげたユースケース分析事例の中で、車両と住宅の連携システム（UC１）をもとに IoT 高信頼化機能を検討した例を示す。UC1 において、基本モデルへのマッピング、およびリスクアセスメントのうち守るべきものの洗い出し、リスクの要因の想定、被害の想定までを行っている。そこで、これらを踏まえたリスク評価を実施し、以後の対策検討に至る例を示す。

(1) リスク評価実施例

UC１は自動車が関連する事例なので、リスク評価方法としては CCDS の「製品分野別セキュリティガイドライン」［7］を参考にして CRSS を用いた。表 4-1 では、CRSS の評価を行う前の準備として、対象機器（住宅内の音声認識装置、車両内の音声操作システム、クラウド）に対する６つのリスク特性（分野固有・共通、脅威の分類、接続 I/F、誰がつなげたか、何が危害を受けたか、どこで発生したか）について明確化した。表 4-2 は、それらの特性に基づいて、CRSS で定義されている評価区分（攻撃元区分、攻撃条件の複雑さ、攻撃前の認証要否、機密性への影響、完全性への影響、可用性への影響）について評価を実施した結果である。この例では、リスク評価結果は、Critical（対策が必要）を赤、Major（要注意）をオレンジで表している。Minor（早急な対策は不要）はなかった。

リスク評価をするにあたって、UC1 では、車両、住宅、クラウドのサーバそれぞれがシステムであるが、それらがつながっている場合、あるシステムの異常が他のシステムへ影響を与えてしまうことの考慮が必要である。そこで、全体を１つのシステムとして捉えて、車両、住宅、クラウドを部分とすることで、それぞれの部分に脆弱性があれば、システム全体にどのような影響があるかを考慮した。

表 4-1 CRSS を用いたリスク評価の例（前半）

No.	想定脅威	想定被害	対象機器	分野固有・共通	脅威の分類	接続I/F（侵入ルート）	who 誰がつなげたか	whom 何が危害をうけたか	where どこで発生したか
1	車／音声操作システムウイルス感染（※システム全体のうち、車が攻撃される）	異常操作による人体への悪影響(e.g.大音量)	車載器	分野固有	ウイルス感染	USB	ユーザー（意図的）	身体や財産	サービス用I/F
2	家／音声認識装置からの異常操作情報（※システム全体のうち、家が攻撃される）	交通事故(e.g.エンジン停止)	宅内機器	共通	不正利用	3G/GSM	攻撃者	身体や財産	サービス用I/F
3	他の家／音声認識装置からの誤操作情報（※他のシステムから、自システムの車が攻撃される）	交通事故(e.g.エンジン停止)	車載器	分野固有	不正利用	3G/GSM	メーカーや関連企業	身体や財産	サービス用I/F
4	家／音声認識装置ウイルス感染（※システム全体のうち、家が攻撃される）	異常操作による人体への悪影響(e.g.過剰な光)、住居・家財の災害(e.g.火事・盗難)	宅内機器	共通	ウイルス感染	USB	ユーザー（意図的）	身体や財産	サービス用I/F
5	車／音声操作システムからの異常操作情報（※システム全体のうち、車が攻撃される）	同上	車載器	分野固有	不正利用	3G/GSM	攻撃者	身体や財産	サービス用I/F
6	他の車／音声操作システムからの誤操作情報（※他のシステムから、自システムの家が攻撃される）	同上	宅内機器	共通	不正利用	3G/GSM	攻撃者	身体や財産	サービス用I/F
7	クラウドサーバの情報漏洩	個人情報の悪用	サーバ	共通	情報漏えい	インターネット	攻撃者	データ	サービス用I/F
8	クラウドサーバのサービス停止	連携機能の停止	サーバ	共通	DoS攻撃	インターネット	メーカーや関連企業	本来機能	サービス用I/F
9	通信データの改ざん、なりすまし	異常操作による人体への悪影響(e.g.大音量) 交通事故(e.g.エンジン停止)	サーバ	共通	盗聴	インターネット	攻撃者	本来機能	サービス用I/F
10	車／盗難	個人情報の悪用	車載器	分野固有	情報漏えい	USB	攻撃者	データ	物理的接触
11	車／廃棄時の情報漏えい	個人情報の悪用	車載器	分野固有	情報漏えい	USB	攻撃者	データ	物理的接触

表 4-2 CRSS を利用したリスク評価の例（後半）

			CRSS（CVSSの応用）								
No.	想定脅威	想定被害	AV 攻撃元区分	AC 攻撃条件の複雑さ	Au 攻撃前の認証要否	攻撃容易性	C 機密性への影響	I 完全性への影響	A 可用性への影響	影響度	リスク値
1	車／音声操作システムウイルス感染（※システム全体のうち、車が攻撃される）	異常操作による人体への悪影響(e.g.大音量)	ローカル	低	単一	3.14	甚大	甚大	甚大	10.00	6.77
2	家／音声認識装置からの異常操作情報（※システム全体のうち、家が攻撃される）	交通事故(e.g.エンジン停止)	隣接	中	単一	4.41	甚大	甚大	軽微	9.54	7.04
3	他の家／音声認識装置からの誤操作情報（※他のシステムから、自システムの車が攻撃される）	交通事故(e.g.エンジン停止)	ネットワーク	中	複数	5.49	軽微	軽微	軽微	6.44	5.36
4	家／音声認識装置ウイルス感染（※システム全体のうち、家が攻撃される）	異常操作による人体への悪影響(e.g.過剰な光)、住居・家財の災害(e.g.火事・盗難)	ローカル	低	単一	3.14	甚大	甚大	甚大	10.00	6.77
5	車／音声操作システムからの異常操作情報（※システム全体のうち、車が攻撃される）	同上	ネットワーク	中	複数	5.49	甚大	甚大	軽微	9.54	7.55
6	他の車／音声操作システムからの誤操作情報（※他のシステムから、自システムの家が攻撃される）	同上	ネットワーク	中	複数	5.49	軽微	軽微	軽微	6.44	5.36
7	クラウドサーバの情報漏洩	個人情報の悪用	ネットワーク	高	複数	3.15	甚大	なし	なし	6.87	4.57
8	クラウドサーバのサービス停止	連携機能の停止	ネットワーク	高	複数	3.15	なし	なし	甚大	6.87	4.57
9	通信データの改ざん、なりすまし	異常操作による人体への悪影響(e.g.大音量) 交通事故(e.g.エンジン停止)	ネットワーク	高	複数	3.15	甚大	甚大	軽微	9.54	6.45
10	車／盗難	個人情報の悪用	ローカル	中	単一	2.70	甚大	なし	甚大	9.21	6.00
11	車／廃棄時の情報漏えい	個人情報の悪用	ローカル	中	単一	2.70	甚大	なし	なし	6.87	4.35

(2) IoT 高信頼化機能による対策検討例

表 4-2 に示したリスク評価結果に対して、方針として Critical（対策は必須）赤（C で表記）と Major（要注意）オレンジ（M で表記）について、対策を行うことを考えた。すなわち、表に示した全項目への対策が必要であった。

次に、この対策を実施するにあたり、ハードウェアや運用（人）での対策が必要な点もあるが、ここではソフトウェアでの対策に着目して検討を行った。

表 4-3 では、IoT 高信頼化機能要件を検討するにあたって、前述のリスク評価の内容をマッピングして必要な対策を検討した。

表 4-3 IoT 高信頼化機能の適用例

IoT 高信頼化機能要件	主に関連するリスク（リスク番号）	優先度	対策	対策として適用できる主な機能
【機能要件 1】初期設定が適切に行われ、その確認ができる	他の家/音声認識装置からの操作(3)	M	正当性が確認できるように設定を行う（機能要件 2 の対策に関連）	初期設定機能
	他の車/音声操作システムからの操作(6)	M		
【機能要件 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	他の家/音声認識装置からの操作(3)	M	正当性を確認し正当でない場合は通信遮断、ユーザ通知	認証機能 アクセス制御機能
	他の車/音声操作システムからの操作(6)	M		
【機能要件 3】異常の予兆を把握できる	車/音声操作システムウイルス感染(1)	M	ウイルス感染を防止する	ウイルス対策機能
	家/音声認識装置ウイルス感染(4)	M		
【機能要件 4】守るべき機能・資産を保護できる	情報漏えい(7)、通信データの改ざん、なりすまし(9)	M	データを保護する	暗号化機能 認証機能（メッセージ）
【機能要件 5】異常発生に備えて事前に対処できる	家/音声認識装置からの異常操作(2)	C	脆弱性を潰し不正操作されないようにする	リモートアップデート機能（ローカルなアップデート含む）
	車/音声操作システムからの異常操作(5)	C		
【機能要件 6】異常発生を監視・通知できる	※	―	異常の監視を行う	監視機能
【機能要件 7】異常の原因を特定するためのログが取得できる	※	―	ログを収集する	ログ収集機能
【機能要件 8】構成の把握ができる	※	―	構成情報管理を行う	構成情報管理機能
【機能要件 9】異常が発生しても稼働の維持ができる	クラウドサーバのサービス停止(8)	M	障害部分の切り離しや障害時に待機系に切り替える	縮退機能 冗長構成機能

【機能要件 10】異常から早期復旧ができる	※	―	異常からの復旧機能を用意する	停止機能 復旧機能
【機能要件 12】自律的な終了や一時的な利用禁止ができる	車/盗難(10)	M	盗難された時に操作をロックする	操作保護機能
【機能要件 12】データ消去ができる	車/廃棄時の情報漏えい(11)	M	廃棄時にデータを消去する	消去機能

※：リスクに対して共通的に必要な項目

＜コラム2＞対策に取り掛かる前にリスク評価

重要生活機器連携セキュリティ協議会(CCDS)　伊藤　公祐

システムやサービスには様々なリスク要因（脆弱性）が潜んでいます。システムを開発する際、セーフティとセキュリティそれぞれの観点で開発対象となるシステムの脅威分析を行うことは、そのシステムの信頼性を高次元で確立するための、設計フェーズでの重要な作業となります。

様々なガイドブックでセキュリティ対策といえば「まず脅威分析をしましょう」とあるので、脅威の洗い出しをされたことのある方は多いかと思います。ではリストアップされた脅威をすべて潰すべく、対策の検討を即始めるべきでしょうか？挙げられた脅威すべてを対処していては、時間もコストも膨大にかかり、IoT サービスの実現は不可能となります。

そこで優先して対処すべき脅威と脆弱性を浮き彫りにする方法が「リスク評価」です。様々な脅威すべてがユーザやサービス提供者にとって致命的なリスクにつながるとは限りません。リスク評価は、それぞれの脅威がどのようなリスクにつながるかを想定し、サービス提供上、起きてはならない重大なリスクを浮き彫りにして、対策すべき脅威の優先順位を見える化するものです。

リスク評価手法には、評価の視点の違いでいくつかありますが、ここでは、代表的な 2 つの手法を紹介します。

1）CVSS

非営利団体 FIRST が推進する脆弱性の評価システムで、情報セキュリティの世界では標準的な評価手法です。脆弱性ごとに ①基本評価値、②現状評価値、③環境評価値の 3 つのパラメータを設定し、計算式により値を求めることで、深刻度を見える化することができます。現在 version 3 が公開されています。

・リスク計算式：http://jvndb.jvn.jp/cvss/v3/ja.html

評価基準	説明
1)基本評価基準 (Base Metrics)	「機密性」、「完全性」、「可用性」に対する影響から評価
2)現状評価基準 (Temporal Metrics)	攻撃コードの出現有無や対策情報が利用可能といった基準で評価
3)環境評価基準 (Environment Metrics)	二次的被害の大きさや、対象製品の使用状況といった基準で評価

深刻度	スコア
緊急	9.0～10.0
重要	7.0～8.9
警告	4.0～6.9
注意	0.1～3.9
なし	0

［CRSS］・・・CVSS の自動車業界向けに特化された手法
自動車技術会（JSAE）が、CVSS(v2)をベースに人命、安全への影響を考慮して作成［7］。

2）OWASP Risk Rating Methodology

ウェブアプリケーションセキュリティをとりまく課題解決を目的としたオープンコミュニティ OWASP によって開発された脆弱性の評価手法です。

・リスク計算式： Risk Severity = ((①+②)/2) X ((③+④)/2)

特徴：リスクファクタに、技術的な観点のほか、金銭等の資産損失やブランド・信用棄損が含まれており、ビジネス面の深刻度を評価できる。

①Threat Agent ①-1:Skill Level ①-2:Motive ①-3:Opportunity ①-4:Size	③Technical Impact ③-1:Loss of confidentiality ③-2:Loss of integrity ③-3:Loss of availability ③-4:Loss of accountability
②Vulnerability ②-1:Ease of discovery ②-2:Ease of exploit ②-3:Awareness ②-4:Intrusion detection	④Business Impact ④-1:Financial damage ④-2:Reputation damage ④-3:Non compliance ④-4:Privacy violation

この他、例えば自動車システム向けには、リスク発生可能性と影響度の２つの側面から評価する RSMA や、企業のレピュテーションリスクや事業生産性への影響まで考慮する OCTAVE Allegro といったものもあります。重大なリスクを見逃さないためにも、できるだけ複数の手法でリスク評価することをお勧めします。例えば、企業イメージの損失を重要視したいのに、その指標がない評価手法で評価したことで対策効果がまったく現れない、という CCDS での検討事例も実際にありました。

評価作業は大変ですが、リスク評価の利点は以下のように様々あります。

1)列挙された脅威の深刻度が数値的に定量化でき、可視化できる
2)対策を打つべき脅威の優先度を深刻度から判断しやすくなる
3)設計の早い段階で脅威への対策検討ができる
4)対策を打った後のシステムに対し、再度リスク評価をすることで、打った対策によるリスク低減効果を検証できる（＝対策の導入コストの妥当性が判断できる）
5)開発者と品質管理者の間で、評価の根拠を通じてリスクの考え方を共有しやすくなる。

このようにリスク評価は、企業にとって技術的にも、ビジネス的にも妥当なセキュリティ対策を見極める重要な設計プロセスになります。

おわりに

IoT の世界では、さまざま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、開発者が考慮してほしい重要なポイントを明確化してきた。

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 高信頼化のために、考慮すべき事項には参考となる具体的な要件が存在せず、現場任せになっており、具体的な高信頼化の機能要件が求められていた。特に、IoT の特徴である分野間連携で必要となる高信頼化機能要件は、明確化されていなかった。

そこで、IPA/SEC では、開発現場で IoT 機器・システムを開発するときに実装すべき高信頼化機能要件を提示することで、各産業界における IoT の高信頼化を実現する場合の共通的な対策を策定することとした。ところが、IoT の高信頼化について、WG の委員間で捉え方が大きく異なっていた。意見の集約ために、保守・運用の視点からの設計時の考慮事項や、分野間連携のユースケースをもとに IoT の構成における実装位置について、WG において長時間にわたる審議をいただき、それにより本書をとりまとめることができた。IoT 機器・システムの開発者の方々が「つながる世界の開発指針」を実践し、IoT 高信頼化のための機能を開発する際に、本書が一助となることを期待する。

なお、本書については、関連規格の動向、IoT サービスの発展、新たなリスクの登場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対して、多大なるご支援を頂いた WG メンバーの方々に感謝の意を表す。

付録 A. IoT のユースケース分析

2.2 で示したように、本書での IoT 高信頼化機能は、いくつかの典型的なユースケース分析から導いた（IoT 高信頼化機能の適用例ではなく、導出のためのユースケースである）。

IoT が進展し、異なる分野の連携がなされることで、様々なリスクの発生が見込まれる。そこで、IoT の実装状況のイメージの共有や異なる分野の連携に着目したリスクを考えるために連携モデルを明確化し、洗い出したリスクをもとに求められる IoT 高信頼化機能を抽出した。

(1) 連携モデル

脅威・ハザードの分析や、技術対策の実装を検討するにあたって、IoT の異なる分野での連携モデルとして、連携する層別にクラウド連携(CC)モデル、フォグ連携(FC)モデル、エッジ連携(EC)モデルを想定した。エッジ連携モデルは個別基盤どうしの連携を指す。フォグ連携モデルはフォグ層を介した連携であり、配下にあるエッジ層との連携は含めるが、クラウド層との連携は含まない。クラウド連携モデルはクラウド層を介した連携であり、配下にあるフォグ層、エッジ層との連携も含む。

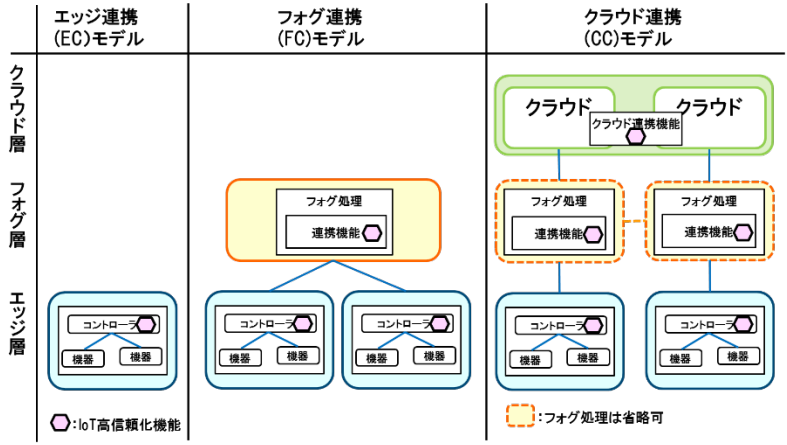


図 A-1 連携モデル

(2) ユースケースと連携モデルの関係

ユースケースの洗い出しに関しては、現状実現できるものと今後想定されるものから表 A-1 に示す 5 つのユースケースを作成して分析を行った。なお、分析においては「つながる世界の開発指針」を活用しているので、「IoT コンポーネント」（IoT 機器・システムのうち単独で目的や機能を果たすもの）という用語を用いている。連携モデルについて、それぞれのユースケースにおいて、１つの連携モデルに該当するのではなく、複数のモデルの要素を含むことがわかった。ここでは、各ユースケースの特徴をもっとも示す連携モデルを想定して、連携機能のリスクを中心に分析を行った。

表 A-1 ユースケースと連携モデルの関係

ユースケース		EC モデル	FC モデル	CC モデル	補足説明
UC1	車両と住宅の連携			◎	クラウドが活用されており、リアルタイム性は要求されないので CC モデル。
UC2	VPP と分散型電源監視サービスとの連携	○		◎	複数のサービスの連携を実施する。HEMS サーバ機能がクラウド上にあるモデルと需要家機器内にあるモデルがあり前者を CC モデルとして選定。
UC3	宅内機器連携	◎			HEMS のデバイスやコントローラ間の連携 フォグやクラウドまでは利用しない
UC4	戸締り競合制御	◎	○	○	ホーム GW／エッジサーバ内の複数の制御ソフト間で競合解決
UC5	産業ロボットと電力管理の連携	○	◎		複数のサービスを連携し、判断の応答性が重視されるフォグ連携システムとして選定

（※：○は各モデルに該当する場合で、◎はそのうち分析まで行ったもの）

UC1. 車両と住宅の連携におけるリスク分析

株式会社デンソー　中垣　良夫

(1) 連携対象

車両（車）と住宅（家）

(2) 概要

車両の運転者は車内から車載の音声操作システムを通じて（家のクラウドベースの音声認識サービスに接続）、車庫の扉を開閉する、玄関の照明を点灯／消灯する、ホームセキュリティを ON/OFF するなど家（自宅）の照明、サーモスタット、セキュリティシステムなどを制御する。反対に住居者が自宅のソファでくつろぎながら家のクラウドベースの音声認識サービスを経由して、車両エンジンの始動/停止、ドアの施錠/解錠、燃料残量チェックする。

(3) 連携形態

クラウド連携モデル

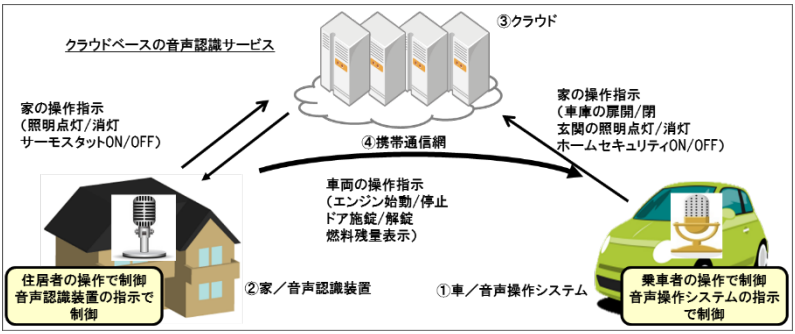


図 A-2　連携形態

(4) 特徴

この連携の特徴は携帯通信網などを通じたクラウドサービスを利用して、車両と住宅という異なる分野のサービスを連携させていることである。IoT 接続により家と離れた場所にある車とをリアルタイムでつなげ、様々な遠隔操作が可能となる。

ただし、車から誤った遠隔操作で家にアクセスして火災になるなどの事故や運転中の車への攻撃によって、運転者の意図しない運転操作が行われ、人命にかかわる重大な事故が発生するなどのセキュリティのリスクがある。

(5) IoT コンポーネントの構造分析

図 A-3 に示すように、家の住居者はクラウドから車/音声操作システムによる操作情報を入手し、車の運転者はクラウドに接続し、家/音声認識装置による操作情報を入手できる。

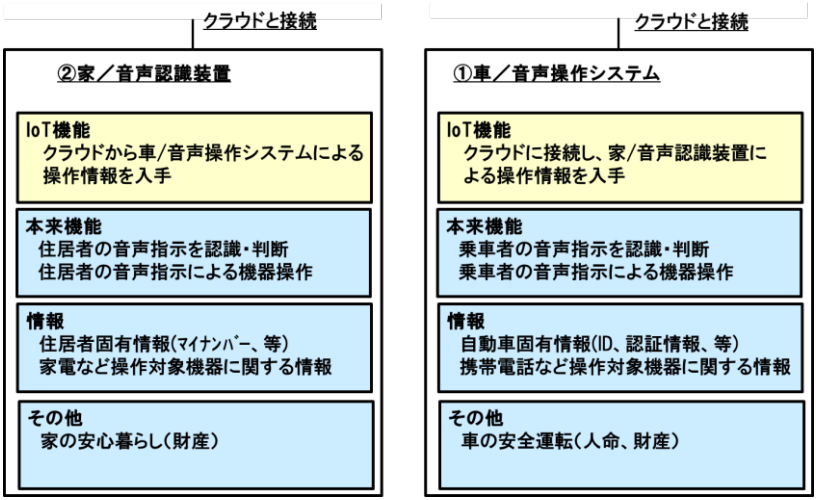


図 A-3 IoT コンポーネントの構造分析

(6) 想定される脅威／被害と主要な要因、課題

想定されるリスクと主要な要因を以下に示す。

表 A-2 想定される脅威/被害

場所	想定される脅威/被害	主要な要因、課題
①	車／音声操作システムウイルス感染 異常操作による人体への悪影響(e.g.大音量)、交通事故(e.g.エンジン停止)	車／音声操作システムの脆弱性
①	家／音声認識装置からの異常操作情報 同上	家／音声認識装置の脆弱性 車と家を繋ぐ通信経路の脆弱性
①	他の家／音声認識装置からの誤操作情報 同上	車／音声操作システムへの接続機器の未認証
①	車／音声操作システムの断続的なサービス停止 正常操作情報が認識出来ず、誤操作による人体への悪影響、交通事故	車／音声操作システムの故障・製品寿命
②	家／音声認識装置ウイルス感染 異常操作による人体への悪影響(e.g.過剰な光)、住居・家財の災害(e.g.火事・盗難)	家／音声認識装置の脆弱性
②	車／音声操作システムからの異常操作情報 同上	車／音声操作システムの脆弱性 家と車を繋ぐ通信経路の脆弱性
②	他の車／音声操作システムからの誤操作情報 同上	家／音声認識装置への接続機器の未認証
②	家／音声認識装置の断続的なサービス停止 正常操作情報が認識出来ず、誤操作による人体への悪影響、住居・家財の災害	家／音声認識装置の故障・製品寿命
③	クラウドサーバのサービス停止、情報漏えい	サーバシステムの脆弱性
④	通信データの改ざん、なりすまし	通信網の脆弱性

(7) 想定される対策

想定されるリスクに対する対策を以下に示す。

表 A-3 想定されるリスクに対する対策

場所	想定される脅威/被害	対策	連携モデル	備考
①	車／音声操作システム	クラウドで繋がる機器(車／音声操作システム)の信用性を確認	CC	認証機能、アクセス制御機能

	ウイルス感染	し、信頼出来ない場合はシステム停止、及びユーザ通知		監視機能、ログ収集機能 停止機能
①	家／音声認識装置からの異常操作情報	クラウドで繋がる機器（家／音声認識装置）から正常操作情報であるか確認し、異常を検知した場合はシステム停止、及びユーザ通知	CC	異常検知機能 監視機能、ログ収集機能 停止機能
①	他の家／音声認識装置からの操作情報	クラウドで繋がる機器（家／音声認識装置）の正当性を確認し、正当でない場合は通信遮断、及びユーザ通知	CC	認証機能、アクセス制御機能 構成情報管理機能 監視機能、ログ収集機能 強制遮断機能
①	車／音声操作システムの断続的なサービス停止	定期的に正しく動作しているか確認、及び累積稼働時間を管理し、異常を検知した場合はシステム停止、及びユーザ通知	CC	診断機能 寿命管理機能 監視機能、ログ収集機能 停止機能
②	家／音声認識装置ウイルス感染	クラウドで繋がる機器（家／音声認識装置）の信用性を確認し、信頼出来ない場合はシステム停止、及びユーザ通知	CC	認証機能、アクセス制御機能 監視機能、ログ収集機能 停止機能
②	車／音声操作システムからの異常操作情報	クラウドで繋がる機器（車／音声操作システム）から正常操作情報であるか確認し、異常を検知した場合はシステム停止、及びユーザ通知	CC	異常検知機能 監視機能、ログ収集機能 停止機能
②	他の車／音声操作システムからの操作情報	クラウドで繋がる機器（車／音声操作システム）の正当性を確認し、正当でない場合は通信遮断、及びユーザ通知	CC	認証機能、アクセス制御機能 構成情報管理機能 監視機能、ログ収集機能 強制遮断機能
②	家／音声認識装置の断続的なサービス停止	定期的に正しく動作しているか確認、及び累積稼働時間を管理し、異常を検知した場合はシステム停止、及びユーザ通知	CC	診断機能 寿命管理機能 監視機能、ログ収集機能 停止機能
③	クラウドサーバのサービ	一般的な冗長構成技術等で対応	–	–

	ス停止、情報漏えい			
④	通信データの改ざん、なりすまし	一般的な暗号化技術等で対応	–	–

(8) IoT 高信頼化機能と実装位置

①（機器）認証機能/アクセス制御機能

クラウドで繋がる機器の信用性・正当性の確認

・車/音声操作システム、及び家/音声認識装置はクラウドに接続

・クラウドで繋がる機器の信用性、及び正当性を確認

・車は家/音声認識装置を接続先として組み込む、また家は車/音声操作システムを接続先として組み込む。

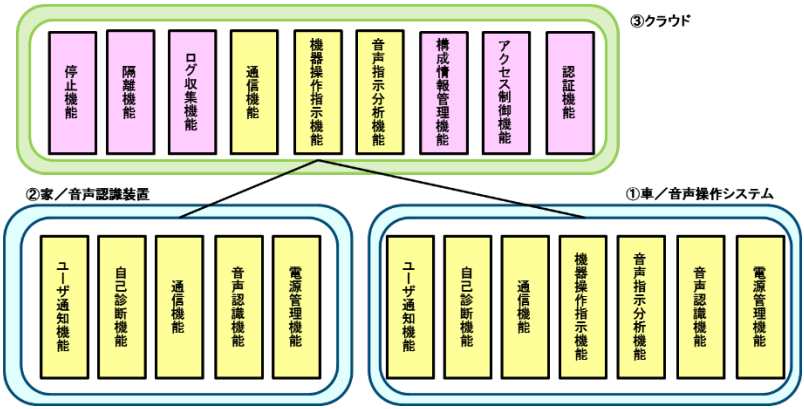


図 A-4 クラウドで繋がる機器の信用性・正当性の確認

②監視機能（異常検知）

クラウドで繋がる機器の操作情報の信用性の確認

・車/音声操作システム、及び家/音声認識装置はクラウドに接続

・クラウドで繋がる機器の操作情報の信用性を確認

・車は家/音声認識装置を接続先として組み込む、また家は車/音声操作システムを接続先として組み込む。

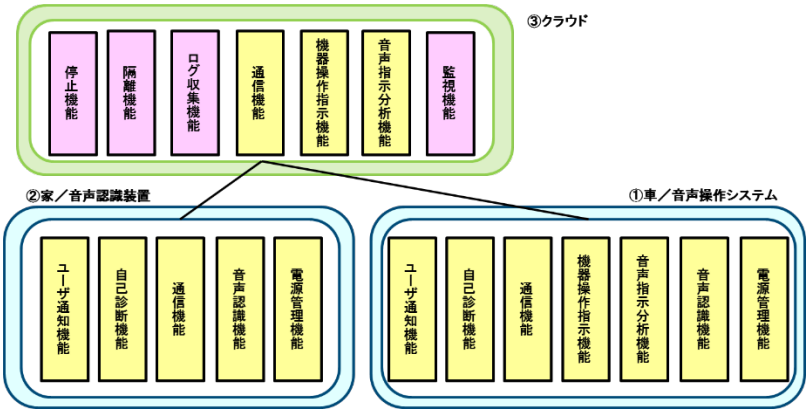


図 A-5 クラウドで繋がる機器の操作情報の信用性の確認

③診断機能/寿命管理機能

クラウドで繋がる機器の信用性の確認

・車/音声操作システム、及び家/音声認識装置はクラウドに接続

・クラウドで繋がる機器の動作状態の確認、及び累積稼働時間を管理

・車は家/音声認識装置を接続先として組み込む、また家は車/音声操作システムを接続先として組み込む。

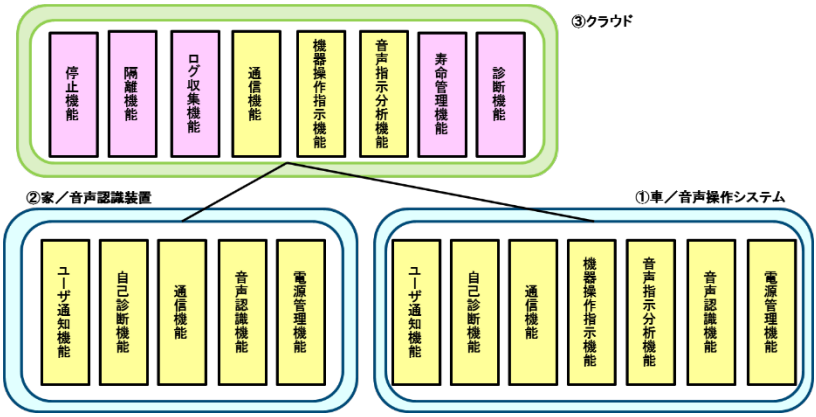


図 A-6 クラウドで繋がる機器の信用性の確認

UC2. VPP と分散型電源監視サービスとの連携におけるリスク分析

一般社団法人日本電機工業会　辻　和隆

(1) 連携対象

VPP（Virtual Power Plant）と分散型電源監視サービス

(2) 概要

VPP では、アグリゲーターが、家庭などの電力需要家側に分散して設置された太陽光発電システムや燃料電池、蓄電システムなどの分散型電源システムを通信で制御することで、仮想的な大型発電設備や大型蓄電システムとしての運用を行い、系統電力逼迫時の電力供給や余剰電力発生時の需給調整などのサービスを送配電事業者に提供する。この際、一般家庭など比較的小容量の分散型電源について，HEMS サーバと HEMS コントローラよりなる HEMS が、太陽光発電の発電量予測や蓄電池の充電状態などに基づいて、蓄電池の充放電や需要機器の運転を実施し、アグリゲーターの要求に応じた電力供給や電力消費を実現する。

一方、分散型電源監視サービスは、例えば太陽光発電システムの発電状況や蓄電システムの充放電状況を監視して、異常通知や気象情報に基づく発電量予測、蓄電池の充放電可能容量の確認などのサービスを提供する。

(3) 連携形態

クラウド連携モデル

HEMS は、複数のサービスと連携する機能と需要家側に設置された ECHONET Lite 機器からの情報収集と制御を行う HEMS コントローラ機能よりなり、サービス及び ECHONET Lite 機器との連携を実現するシステムと定義される［8］。

サービス連携機能はサーバ上に配置される場合と需要家側の機器に搭載される場合があるが、ここでは HEMS サーバはクラウド上にあり、需要家側に設置された HEMS コントローラと連携している形態を考える。

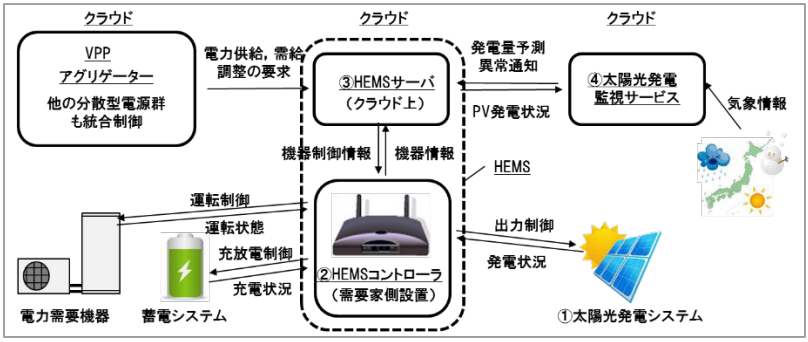


図 A-7 連携形態

(4) 特徴

この連携の特徴は、インターネットなどを通じたクラウドサービスと HEMS を利用して、分散型電源を統合制御する VPP と太陽光発電システムや蓄電システムの異常検知や太陽光発電の発電量予測などを行う監視システムという異なる分野のサービスを連携させていることである。これにより、例えば太陽光発電の発電量予測や蓄電池の充放電可能容量に基づいて各需要家の機器を最適制御してアグリゲーターの要求に対応する事が可能となる。

ただし、誤った発電量予測や機器異常の通知などにより、アグリゲーターの要求に対する不履行や太陽光発電の不要停止などの事故が発生するリスクがあり、特に、分散型電源を大量に統合制御する VPP においては、系統電力の安定性に支障を来すような重大な事故につながるリスクも考えられる。

(5) IoT コンポーネントの構造分析

以下では、VPP と太陽光発電監視システムとの連携を例に検討を行う。図 A-8 のように、HEMS は VPP アグリゲーターから電力の供給や消費に関する要求を入手し、太陽光発電監視システムから発電量予測や機器異常通知を入手する。HEMS はこれらの情報に基づいて太陽光発電システムやその他の ECHONET Lite 機器の制御を行い、太陽光発電システムは HEMS を介して監視システムに発電状況を送付する。

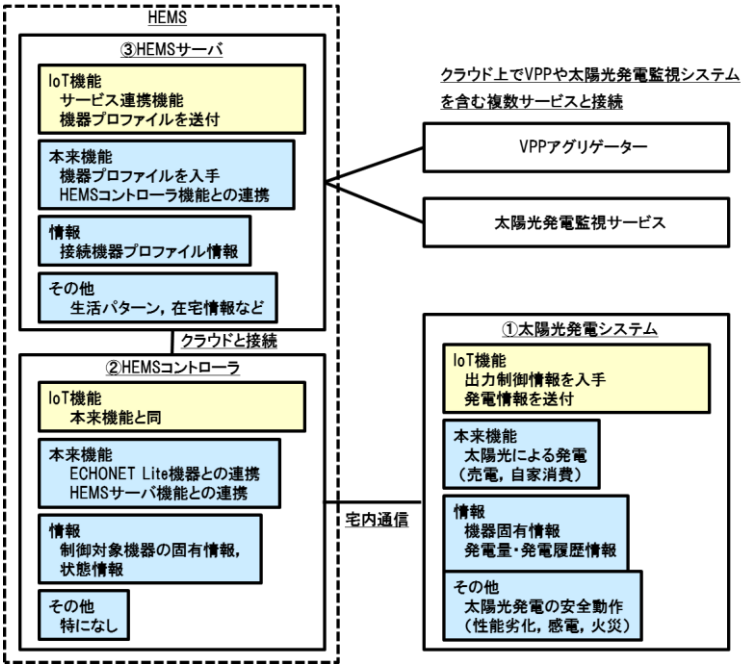


図 A-8 IoT コンポーネントの構造分析

(6) 想定される脅威／被害と主要な要因、課題

想定されるリスクと主要な要因を以下に示す。

表 A-4 想定される脅威/被害

場所	想定される脅威/被害	主要な要因、課題の例
①	太陽光発電システムの機能不全 未認定アプリや他のコントローラからの異常な制御/間違った制御による機器の機能不全（不要な発電抑制，VPP の要求不履行）	太陽光発電システムの脆弱性 品質レベルの低い未認定アプリや他コントローラとの接続 通信相手の優先度未設定
②	HEMS コントローラへの不正アクセス、なりすまし 誤った機器情報による不要制御，VPP 不履行 誤った制御情報による不要制御，VPP 不履行	HEMS コントローラの脆弱性 非暗号化での通信 通信相手の未確認
②	HEMS コントローラのウイルス感染 異常な機器制御，VPP 要求不履行 HEMS サーバへの誤った機器情報送信による不要制御の発生，VPP 要求の不履行	HEMS コントローラの脆弱性

②③	通信データの改ざん 誤った機器情報による不要制御，VPP 不履行 誤った制御情報による不要制御，VPP 不履行	サーバ/コントローラ間通信の脆弱性
③	HEMS サーバへの不正アクセス、なりすまし 異常な制御情報による不要制御，VPP 不履行 誤った機器情報による監視システムの誤作動	PV 監視システム/HEMS サーバ間通信の脆弱性 HEMS サーバ/コントローラ間通信の脆弱性
③	HEMS サーバのウイルス感染 異常な機器制御，VPP 要求不履行 誤った機器情報による監視システムの誤作動	HEMS サーバの脆弱性

(7) 想定される対策

想定されるリスクに対する対策を以下に示す。

表 A-5 想定されるリスクに対する対策

場所	想定される脅威/被害	対策	連携モデル	備考
①	太陽光発電システムの機能不全	・機器認証により通信相手を認証し，その結果共有した鍵を利用してメッセージ認証を行うことで，未認定アプリやコントローラの接続排除/機能制限を行う ・ユーザ承認により接続相手(コントローラ)を制限する	EC	(機器)認証機能 メッセージ認証機能 アクセス制御機能
②	HEMS コントローラへの不正アクセス、なりすまし	・機器認証により通信相手を認証し，その結果共有した鍵を利用してメッセージ認証を行う ・安全性や機器の故障に係わる異常制御への応答拒否	CC	(機器)認証機能 メッセージ認証機能 監視機能
②	HEMS コントローラのウイルス感染	・コントローラの OS,セキュリティソフト更新 ・接続先の確認(機器認証)	CC	(機器)認証機能
②③	通信データの改ざん	・SSL 通信による暗号化 ・ログ蓄積によるデータ照合	CC	暗号化機能 ログ収集機能
③	HEMS サーバへの不正アクセス、なりすまし	・連携サーバの機器認証 ・第三者機関による，情報の照合や，機器の一斉故障，一斉メンテナンスなどの異常指示の監視と通知	CC	(機器)認証機能 監視機能 ログ収集機能

③	HEMS サーバのウイルス感染	・サーバの OS,セキュリティソフト更新 ・ネットワーク機器のセキュリティアップデート ・接続先の確認(機器認証)	CC	(機器)認証機能

(8) IoT 高信頼化機能と実装位置

①機器認証機能/メッセージ認証機能/アクセス制御機能

宅内ネットワークで繋がる相手機器の信用性の確認

・繋がる相手機器が，意図した機器である事を確認し承認

・HEMS コントローラ，太陽光発電システムはお互いの正当性を確認

・相手機器との通信内容の暗号化およびメッセージ認証

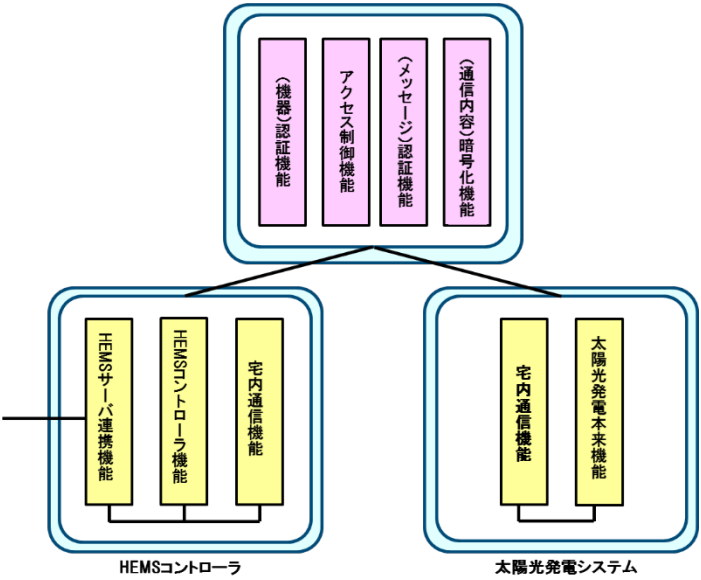


図 A-9 宅内ネットワークで繋がる相手機器の信用性の確認

②機器認証/暗号化/ログ収集機能

HEMS サーバ/HEMS コントローラ間の信用性の確認

・繋がる相手機器が，意図した機器である事を確認し承認

・HEMS サーバ，HEMS コントローラはお互いの正当性を確認

・相手機器との通信内容の暗号化

・機器制御情報と機器動作の照合による確認と誤動作要因の解析

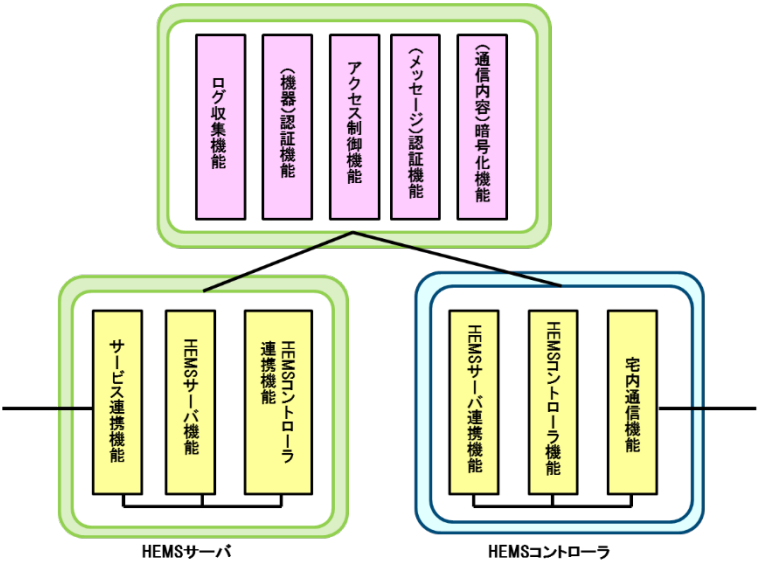


図 A-10 HEMS サーバ/HEMS コントローラ間の信用性の確認

UC3. 宅内機器連携におけるリスク分析

一般社団法人エコーネットコンソーシアム　村上　隆史

(1) 連携対象

コントローラと宅内機器

(2) 概要

家庭内のさまざまな白物家電製品、住設機器、センサーネットワークに適用可能な、比較的低速、低容量で安価な設備系のネットワークにより、さまざまなメーカーの設備機器、センサーや、コントローラが相互接続され、これらが有機的な連携をすることで、省エネルギー、高齢者、在宅介護などに対応した、安全安心で、快適、人に、地球に配慮したネットワークシステムが実現可能となる。

例えば、居住者の在不在を検知して、エアコンや照明を効率良く動かすことで、無駄なエネルギー消費を抑えるのみならず、今後、普及拡大が予想される太陽光発電や燃料電池で作り出したエネルギーを蓄電池や電気自動車に蓄えておき、家庭内のエネルギー消費が多い夜間などの時間帯に利用することで、自然エネルギーを有効に活用できる。このように、設備系ネットワークは、創エネ設備、蓄エネ設備、エネルギー消費設備を効率的に動かすことで、地球環境にやさしい効率的なエネルギーマネジメントシステムを構築することができる。

（ECHONET Lite 規格書 Ver.1.12 第 1 部より抜粋）［9］

(3) 連携形態

エッジ連携モデル

太陽光発電（PV）の発電状況と、蓄電池の充電可能量を HEMS コントローラが知り、蓄電池の充電制御を行うことで、PV による発電分を自家消費によりエネルギーを有効に活用するモデルを具体例として記載する。

本モデルの利用方法は以下のとおりである。

- HEMS コントローラが太陽光発電システムから発電状況を取得する。
- HEMS コントローラが蓄電池から充電可能量を取得する。

・ 充電している状況、もしくは出力制御の状況である場合、HEMS コントローラは蓄電池に対して、充電要求を送信し、需要家内で効率よく電力を使用する。

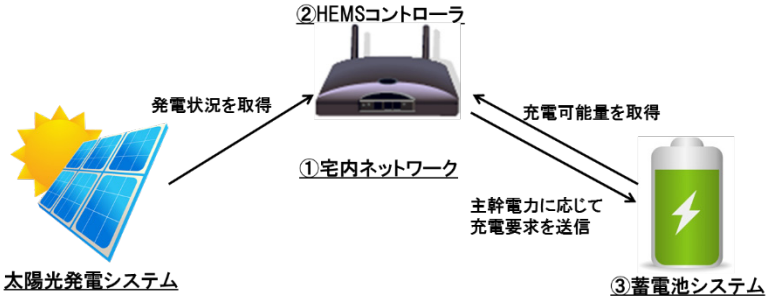


図 A-11 連携形態

(4) 特徴

この連携の特徴は、ユーザが Ethernet や Wi-Fi などの宅内ネットワークを通じて、HEMS コントローラを介して太陽光発電システムと蓄電池システムなどといった宅内の異なる機器を連携させているところである。本モデルの例では、太陽光発電システムの情報を活用し、蓄電池システムの充電制御を行うことで電力を有効活用することが可能となる。

HEMS コントローラと太陽光発電システム及び蓄電池システムとの相互接続を実現するための通信仕様が ECHONET Lite である。ECHONET Lite においては、相互接続性を高めるために通信仕様の仕様適合性を試験する「ECHONET Lite 規格適合性認証」と、ECHONET Lite の具体的な使用方法を機器ごとに規定した仕様の適合性を試験する「アプリケーション通信インタフェース仕様適合性認証」とを規定している。

一方で、ECHONET Lite は軽装かつ容易な通信仕様であるため、上記適合性認証を取得せずに、相互接続性の信頼度が低い機器が市場に投入される可能性もある。このような状況に対して、ユーザの声として「通信信頼性の高い HEMS コントローラから安全に機器を操作したい」、サービス／機器提供者の声として「通信信頼性の高い機器を組み合せて、ユーザメリットの高い機器操作を実現したい」といった意見が挙がっている。

(5) IoT コンポーネントの構造分析

図 A-12 のように、ユーザは宅内の各種機器に対して HEMS コントローラを介した操作ができる。また、HEMS コントローラを介して各種機器の状態情報や固有情報を入手できる。

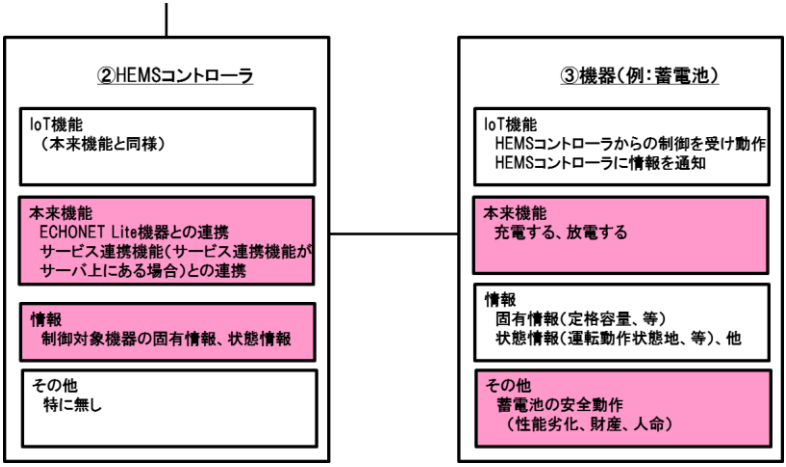


図 A-12 IoT コンポーネントの構造分析

(6) 想定される脅威／被害と主要な要因、課題

想定されるリスクと主要な要因を以下に示す。

表 A-6 想定される脅威/被害

場所	想定される脅威/被害	主要な要因、課題の例
②③	未認定アプリからの接続 PC/スマホの未認定アプリから機器への異常な制御/間違った制御により機器の機能不全につながる。	品質レベルの低い未認定アプリとの接続
②③	許可していない機器からの接続 他のコントローラから機器への異常な制御/間違った制御/（主コントローラにとって）邪魔な制御などによる機器の機能不全につながる。	通信相手の優先度未設定、品質レベルの低い他コントローラとの接続
②③	不正制御 第三者による Ethernet/Wi-Fi などへの不正アクセス・誤接続による意図しない機器の制御（実装間違いなどによる不正パケットの送信含む）	Wi-Fi のセキュリティ設定不備、非暗号化での通信、通信相手の未確認
①	プライバシ情報漏えい Ethernet/Wi-Fi などへの不正アクセスによりプライバシ情報、機器の状態などを盗聴される	Wi-Fi のセキュリティ設定不備、非暗号化での通信

(7) 想定される対策

想定されるリスクに対する対策を以下に示す。

表 A-7 想定されるリスクに対する対策

場所	想定される脅威/被害	対策	連携モデル	備考
②③	未認定アプリからの接続	・ 機器認証の仕組みにより通信相手を認証し、その結果共有した鍵を利用してメッセージ認証を行うことで、未認定アプリ/コントローラの接続排除/機能制限を行う。	EC	(機器)認証機能 (メッセージ)認証機能
②③	許可していない機器からの接続	・ アクセス制御により接続相手(コントローラ)を制限する	EC	アクセス制御機能
②③	不正制御	・ アクセス制御により誤接続を防ぐ ・ 機器認証の仕組みにより通信相手を認証し、その結果共有した鍵を利用してメッセージ認証を行う	EC	(機器)認証機能 (メッセージ)認証機能 アクセス制御機能
①	プライバシ情報漏えい	・ 機器認証の仕組みにより通信相手を認証し、その結果共有した鍵を利用して通信内容の暗号化を行う	EC	(機器)認証機能 (通信内容)暗号化機能

(8) IoT 高信頼化機能と実装位置

①認証機能/アクセス制御機能/暗号化機能

宅内ネットワークで繋がる相手機器の信用性の確認

・繋がる相手機器が、ユーザが意図した機器であることを確認し承認

・HEMS コントローラ、制御対象となる機器はお互いの正当性（規格適合性認証の有無など）を確認

・正当性が確認できた相手機器との通信内容の暗号化および（メッセージ）認証を行う。

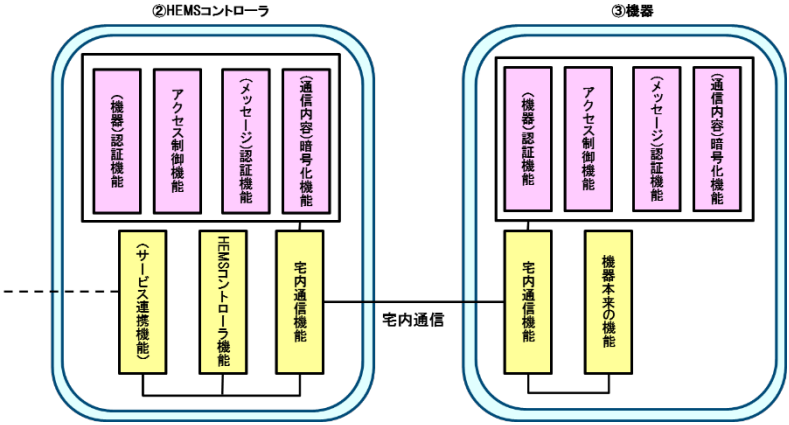


図 A-13 宅内ネットワークで繋がる相手機器の信用性の確認

UC4. 戸締り競合制御におけるリスク分析

YRP 研究開発推進協会 /一般社団法人 WSN-ATEC　柘植　晃

(1) 連携対象

住宅（宅内複数システムの競合）

(2) 概要

住宅宅内の複数システムが同時に動作する場合の競合として、以下のような快適性制御のための自動通風システムと緊急災害、防犯対策システムとの競合事例について述べる。

① 快適性制御のための自動通風窓開閉システム
温湿度センサー、照度センサー、PM2.5 センサーなどによる空調制御、自動通風制御

② 緊急災害・防犯対策システム
ポイント気象情報、戸外侵入者センサーなどによる防災、防犯システム制御

(3) 連携形態

エッジ連携モデル

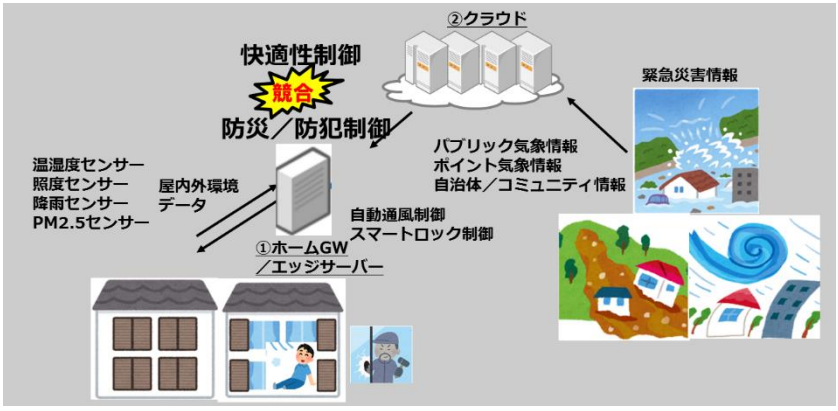


図 A-14　連携形態

快適性制御のための自動通風システムの雨戸、窓などを開く制御と、緊急災害、防犯システムからの雨戸、窓などの戸締り制御が競合する。また緊急災害

時は緊急避難のために玄関を解錠するべきであるが、防犯システムの施錠制御と競合する場合が想定される。

(4) 特徴

この競合の例は単なる一例に過ぎず、同様の競合事例が他にも多く想定される。例えば、ビデオ予約システムで AV 機器の電源を入れる制御と節電システムによって電源オフを制御するなどの動作が競合するなどが考えられる。一般的にはそれぞれ個別に設計されたシステムが混在し、同一の操作対象を制御する場合に、それぞれのシステム個別で設計されたものが同一操作対象を同時に制御するために想定外の操作競合が発生してしまう。

(5) IoT コンポーネントの構造分析

本事例の場合は、以下の図のように宅内のホーム GW、またはホームエッジサーバなどの内部での競合である。

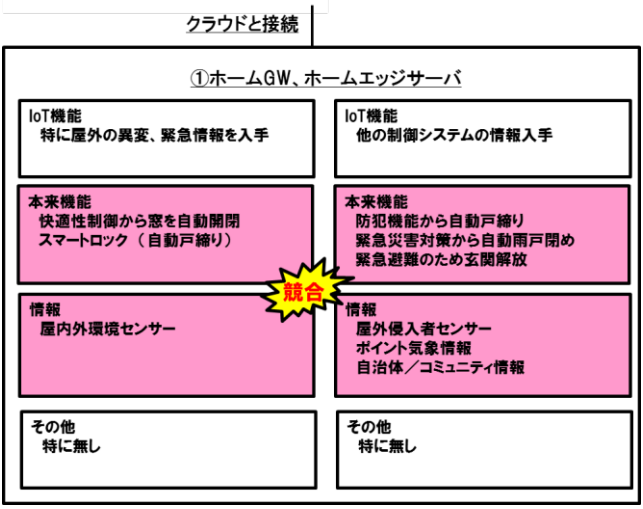


図 A-15 IoT コンポーネントの構造分析

(6) 想定される脅威／被害と主要な要因、課題

以下に、本事例における想定される脅威／被害と主な要因、課題について述べる。

表 A-8 想定される脅威/被害

場所	想定される脅威/被害	主要な要因、課題の例
①	ホーム GW／エッジサーバ 快適性のため窓を開ける制御と防犯／防災のための窓・雨戸を閉める制御とが競合し、安全安心が損なわれる。	複数の制御ロジックが競合
①	ホーム GW／エッジサーバ ウイルス感染 制御ソフトウェアへの悪意のある攻撃により本来の窓・雨戸・玄関などの戸締り制御が乗っ取られる。	ホーム GW／エッジサーバの脆弱性
②	クラウドサーバのサービス停止	
③	通信データの改ざん	

(7) 想定される対策

表 A-9 に本事例における想定される対策について述べる。

表 A-9 想定されるリスクに対する対策

場所	想定される脅威/被害	対策	連携モデル	備考
①	ホーム GW／エッジサーバ	快適性のため窓を開ける制御と防犯／防災のための窓・雨戸を閉める制御とが競合する際に、優先度を判断する上位レイヤの制御機能を追加し、安心・安全性を優先する。	EC	監視機能（競合解決機能）
①	ホーム GW／エッジサーバ	ホーム GW／エッジサーバ制御ソフトウェアにおける悪意のある侵入者からの攻撃に対するセキュリティ対策	EC	監視機能（侵入防止機能）
②	クラウドサーバのサービス停止	一般的な冗長構成技術等で対応	−	−
③	通信データの改ざん	一般的な暗号化技術等で対応	−	−

(8) IoT 高信頼化機能と実装位置

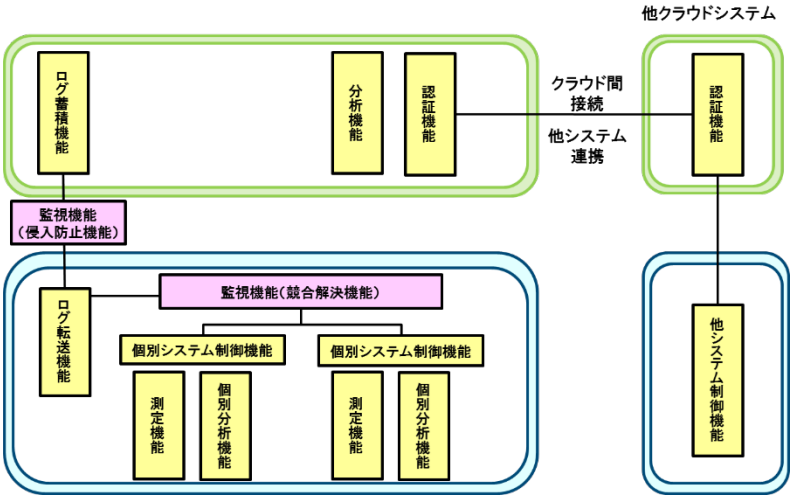


図 A-16 複数の制御システムの競合解決

上記のように宅内に存在する複数の制御システムが同時に動作する場合、宅内外のあらゆる状況を総合的に判断してまず人命最優先、次に財産を守る、その上で快適性、エンターテイメントというスーパーバイザー的な制御システムが必要である。

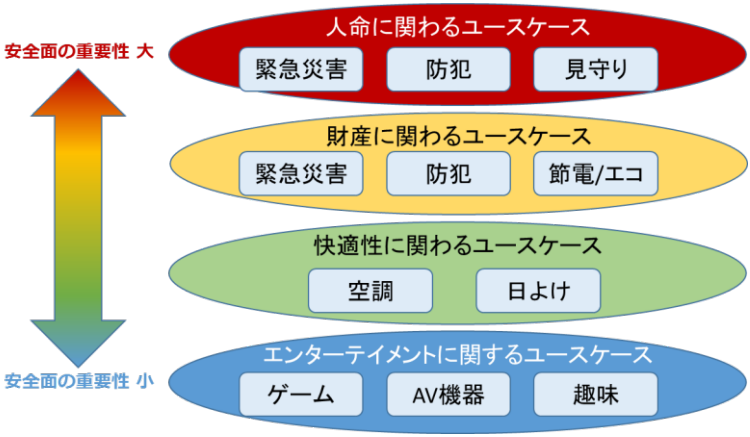


図 A-17 競合制御における優先度の考え方

図 A-18 にその優先度カテゴリのイメージおよび、競合解決するためのホームエッジサーバのアーキテクチャイメージを示す。今後将来的に新たな制御システムが追加されることも想定しながら、いかなる場合もまず人命優先→財産を守る→快適性→エンターテイメントという優先度を総合的に判断しながら被害を最小限に抑えるシステムが必要である。そのために各システムをプラグイン的に組合せが可能でどのようなシステムが組合せられても全体最適を図るスーパーバイザー的な競合制御が必要である。

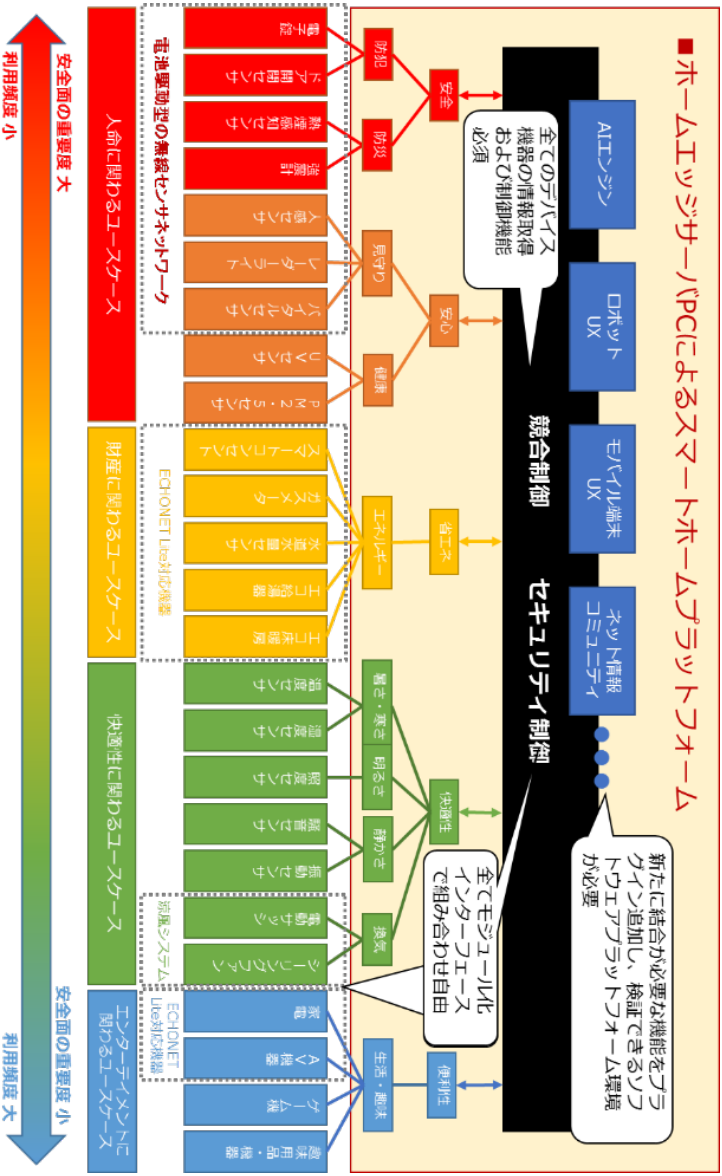


図 A-18 優先度カテゴリのイメージ

UC5. 産業ロボットと電力管理の連携におけるリスク分析

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

(1) 連携対象

産業ロボットシステムと電力管理システム

(2) 概要

中小企業の経営者が小規模工場内の設備を監視・操作する場面を想定する。ここでの生産監視システムは、以下の機能を有するものとする。

・異常検知

　産業ロボットシステムの稼働情報と電力管理システムの電力情報を連携して産業ロボットシステムと電力管理システムの異常をより確実に検知する。

・工場のファシリティ制御

　産業ロボットの稼働状況に応じて電力管理システムの空調や照明などの機器を制御する。

(3) 連携形態

フォグ連携システム

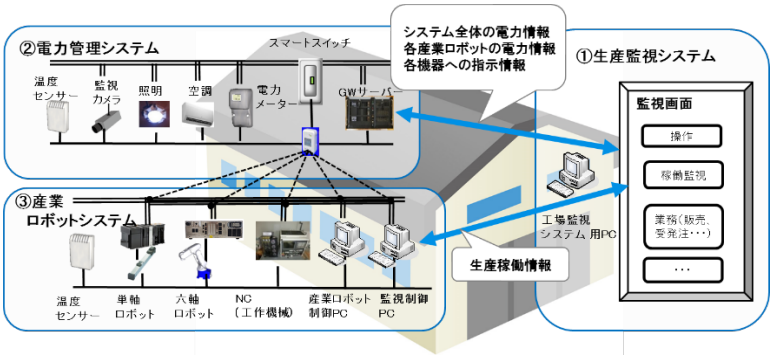


図 A-19　連携形態

(4) 特徴

本システムは、工場内の電力を監視して電力消費を制御する電力管理システム、産業ロボットやNC装置を制御して生産物の加工を行う産業ロボットシステム、並びに両システムを監視して操作する生産監視システムから構成されている。

生産監視システムは、電力管理システムが取得した電力情報と産業ロボットシステムが取得した生産稼働情報を連携させて、工場内システムの異常監視と省電力のための制御を行う。

このシステムでは、電力管理システムでのセンサー類の機器のなりすましや取得された情報の改ざん等によって、工場内システムの異常監視並びに省電力制御が誤動作する可能性がある。また、産業ロボットシステムと電力管理システムの個々の判断により、同一の機器に対して相反する指示が出された場合、各制御の目的が達成されないことに加え、機器の故障などに結び付くケースが考えられる。

(5) IoTコンポーネントの構造分析

①生産監視システム

電力管理システムから産業ロボットの電力情報を、産業ロボットシステムからは生産稼働情報をそれぞれ入手し、それらの整合性を確認することにより異常検知を行う。

②電力管理システム

システム全体の消費電力が上限値を超えないように、電力の使用状況を監視して必要に応じて電力使用量を抑える制御を行う。

③産業ロボットシステム

与えられた指示に従い、製造物の加工を自動的に行う。その中で、生産管理のための生産稼働情報を取得しておく。

電力管理システム内の空調に対して指示を送り、ロボットや産業用機器の動作や作業者に適した温度制御を行う。

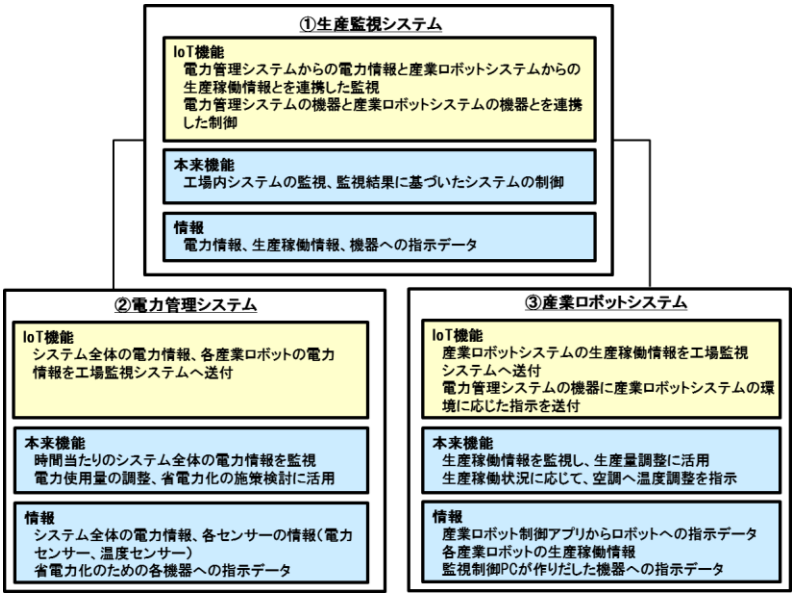


図 A-20 IoT コンポーネントの構造分析

(6) 想定される脅威／被害と主要な要因、課題

想定されるリスクと主要な要因を以下に示す。

表 A-10 想定される脅威/被害

場所	想定される脅威／被害	主要な要因、課題
①②③	システム全体の電力情報や各産業ロボットの電力情報の改ざん 産業ロボットシステムの生産稼働情報の改ざん ／異常を検知できないことによるシステムダウン 想定外の動作の継続による故障増加 想定外の動作の継続による消費電力増加 過剰生産、過小生産	PC、GW サーバ上のハードウェア/ソフトウェアの耐タンパー性の低さ LAN 上に流しているデータを保護していない
②	電力メーター、電力センサーのなりすまし 不正内包した機器の接続 ／異常を検知できないことによるシステムダウン	正規の GW サーバの確認方法がない 正規の電力メーター、電力センサーの確認方法がない
①③	産業ロボットシステムの監視プログラムの改ざん、なりすまし ／異常を検知できないことによるシステムダウン	正規の監視プログラムの確認方法がない

②③	相反する指示(例 空調のパワーオン、パワーオフ)の競合 ／空調の故障による生産性の低下	独立した2つのシステムでは、優先する状態が異なるケースがある (電力制御システムでは消費電力の上限に達しないようにすることを優先、産業ロボットシステムは、作業者や機器にとって適切な温度に調整することを優先)
①②③	内部不正、ウイルスによる PC・GW サーバの時刻改ざん ／異常発生時の調査費用増加	PC, GW サーバの時刻設定機能のアクセス制御が不十分

(7) 想定される対策

想定されるリスクに対する対策を以下に示す。

表 A-11 想定されるリスクに対する対策

場所	想定される脅威／被害	対策	連携モデル	備考
①②③	システム全体の電力情報や各産業ロボットの電力情報の改ざん 産業ロボットシステムの生産稼働情報の改ざん ／異常を検知できないことによるシステムダウン 想定外の動作の継続による故障増加 想定外の動作の継続による消費電力増加 過剰生産、過小生産	・PC 上プログラムのアクセス制御と耐タンパー性強化により、メモリ上のデータの改ざんを防止 ・電力情報、生産稼働情報にダイジェスト情報や署名をつけて正当性チェックをおこない、改ざんを検知	FC	・アクセス制御機能 ・(耐タンパー性) ・監視機能(セキュリティ異常の検知)
②	電力メーター、電力センサーのなりすまし 不正内包した機器の接続 ／異常を検知できないことによるシステムダウン	・GW サーバによる電力メーター、電力センサーの機器認証により、なりすましを検知	EC	・認証機能(機器認証) ・監視機能(セキュリティ異常の検知)
①③	産業ロボットシステムの監視プログラムの改ざん、なりすまし	・PC 上プログラムのアクセス制御と耐タンパー性強化により、メモリ上のプログ	FC	・アクセス制御機能 ・(耐タンパー性)

	／異常を検知できないことによるシステムダウン	ラム並びにデータの改ざんを防止 ・工場監視システムによるPC上プログラムの認証、産業ロボット制御プログラムとの相互認証により、なりすましを検知		・監視機能（セキュリティ異常の検知） ・認証機能（プログラム認証）
②③	相反する指示（例　空調のパワーオン、パワーオフ）の競合 ／空調の故障による生産性の低下	・空調に対する指示を監視して、相反する指示が一定時間連続して出されていたら異常としてアラームをあげる	FC	・監視機能（競合の検知）
①②③	内部不正、ウイルスによる PC・GW サーバの時刻改ざん ／異常発生時の調査費用増加	・各 PC で、NTP、GPS 等を使った時刻合わせを適度に短い時間間隔で実施	FC	・時刻同期機能

(8) IoT 高信頼化機能と実装位置

①アクセス制御機能/監視機能/認証機能

生産監視システム、電力管理システム、産業ロボットシステムで、異常監視の脅威に対する対策として、アクセス制御機能、監視機能（セキュリティ異常の検知）、認証機能（機器認証、プログラム認証）を組み込む。なお、監視機能や機器を制御する機能を実現するプログラム及びデータの改ざん防止対策として、それらに耐タンパー性をもたせることが考えられる。

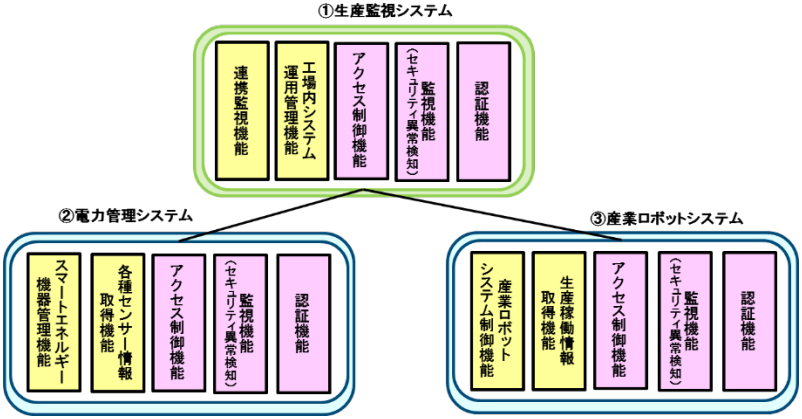


図 A-21 異常監視の脅威に対する対策

②監視機能（競合の検知）

生産監視システムで、電力管理システムでの電力制御を目的とした空調への指示と産業ロボットシステムでの製造環境の温度制御を目的とした空調への指示との競合を検知するための対策として、監視機能（競合の検知）を組み込む。

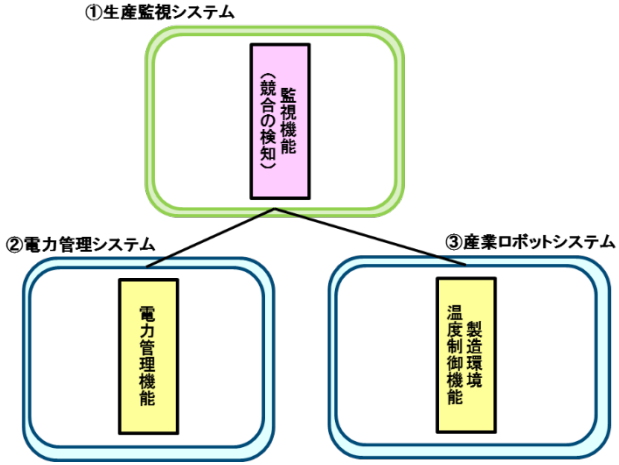


図 A-22 競合の検知

③時刻同期機能

生産監視システム、電力管理システム、産業ロボットシステムで、各システムでの監視対象事象の検知時刻の信頼性を確保するために、時刻同期機能を組み込む。

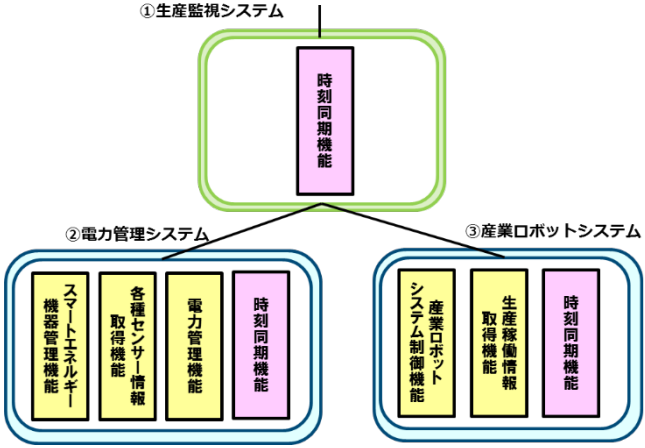


図 A-23 時刻同期

付録 B. IoT 高信頼化に向けた分析／整理

(1) 脅威と対策のまとめ

第 2 章で言及した IoT 高信頼化に向けた分析/整理において、「つながる世界の開発指針」、及びユースケースをもとに抽出した脅威・ハザードおよび技術対策のカテゴリをまとめたものを表 B-1 に示す。

脅威・ハザードに対する対策としては物理対策、人的対策、管理対策、技術対策が考えられる。IoT 高信頼化機能は技術対策であるため、それらの対策の中の技術対策に着目して整理を行った。技術対策は設計、保守（のための設計）、運用（のための設計）が中心であるが、分析においてもリスク分析の結果として必要な対策が示されているものを含めている。

表 B-1　脅威と対策のまとめ

	指針 No.	指針	脅威・ハザードの種類	主な技術対策（機能）
方針	指針1	安全安心の基本方針を策定する	（対象外）	（対象外）
	指針 2	安全安心のための体制・人材を見直す	（対象外）	（対象外）
	指針 3	内部不正やミスに備える	（対象外）	（対象外）
分析	指針 4	守るべきものを特定する	（対象外）	（対象外）
	指針 5	つながることによるリスクを想定する	不正アクセス	認証機能、アクセス制御機能、監視機能（不正アクセス）
			ウイルス感染	ウイルス対策機能
			設定誤り	初期設定機能
	指針 6	つながりで波及するリスクを想定する	制御の競合	監視機能（競合の検知）
	指針 7	物理的なリスクを認識する	（対象外）	（対象外）

設計	指針 8	個々でも全体でも守れる設計をする	不正利用	認証機能（ユーザ認証、生体認証、機器認証）
			データ改ざん	暗号化機能 （メッセージ）認証機能
			時刻改ざん	時刻同期機能
			想定外装置からの誤アクセス	認証機能、アクセス制御機能、構成情報管理機能
			ウイルス感染	ウイルス対策機能
	指針 9	つながる相手に迷惑をかけない設計をする	異常の波及	監視機能（障害/故障監視、通知） 隔離機能 停止機能 診断機能
			サービス停止	縮退機能 冗長構成機能 復旧機能
	指針 10	安全安心を実現する設計の整合性をとる	（対象外）	（対象外）
	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	信頼性の低い機器と接続	アクセス制御機能 （信用度の確認）
	指針 12	安全安心を実現する設計の検証・評価を行う	（対象外）	（対象外）
保守	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	故障 不正アクセス	予兆機能 監視機能（障害/故障監視、通知） ログ収集機能
	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	脆弱性	リモートアップデート機能
運用	指針 15	出荷後もIoTリスクを把握し、情報発信する	（対象外）	（対象外）
	指針 16	出荷後の関係事業者に守ってもらいたいことを伝える	初期設定の不備	初期設定機能
			サポート期間の終了	寿命管理機能
	指針 17	つながることによるリスクを一般利用者に知ってもらう	リユース・廃棄時の情報漏えい	消去機能

(2) 関連標準/ガイド類

2.2 で示した IoT 高信頼化機能の抽出において、参考とした IoT に関する標準やガイド類について以下に示す。

表 B-2 IoT 高信頼化機能の抽出で参考とした関連標準/ガイド類

規格/ガイド	団体	内容
Industrial Internet of Things Volume G4:Security Framework [10]	IIC	インダストリアル IoT におけるセキュリティ対策技術やプロセスをまとめたフレームワーク。
IoT 早期導入者のためのセキュリティガイダンス [11]	CSA	IoT を導入する組織のためのセキュリティ管理策を提示。
コンシューマ向け IoT セキュリティガイド [12]	日本ネットワークセキュリティ協会	ベンダーとして IoT デバイスを提供する際にセキュリティについて検討すべきことを提示。 直行する2つの軸で、脅威、対策を整理。 ・ 利用開始(導入初期) – 平常運用時 – 買い替え(廃棄) ・ 放置(野良状態) – 平常運用時 – 異常発生時
IoT 開発におけるセキュリティ設計の手引き [13]	IPA セキュリティセンター	IoT 機器、およびその使用環境で想定されるセキュリティ脅威と対策を提示。
IoT Security Guidelines [14]	GSMA	IoT のセキュアな製品やサービス、ネットワーク運用者向けの指針。
製品分野別セキュリティガイドライン [7]	CCDS	車載・IoT ゲートウェイ・金融端末(ATM)・決済端末(POS)の4分野の製品分野別セキュリティガイドライン。

付録 C. 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] 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　分散戦略 WG, “中間とりまとめ,” [オンライン]. Available: http://www.meti.go.jp/report/whitepaper/data/pdf/20161129001_01.pdf.

[3] 高田　信彦、南　俊博, 情報セキュリティ教科書, 東京電機大学出版局, 2008.

[4] 一般社団法人重要生活機器連携セキュリティ協議会, “重要生活機器の脅威の事例集　Ver.1.2,” [オンライン]. Available: https://www.ccds.or.jp/public/document/other/CCDS_CaseStudies_v1_2.pdf.

[5] 一般財団法人日本自動車研究所, “平成 26 年度　戦略的イノベーション創造プログラム　V2X (Vehicle to X) システムに係わるセキュリティ技術の海外動向等の調査,” [オンライン]. Available: http://www.meti.go.jp/meti_lib/report/2015fy/000326.pdf.

[6] 独立行政法人情報処理推進機構, “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/files/000055007.pdf.

[7] 一般社団法人重要生活機器連携セキュリティ協議会, “製品分野別セキュリティガイドライン,” [オンライン]. Available: https://www.ccds.or.jp/public_document/index.html.

[8] 一般社団法人日本電機工業会　HEMS 専門委員会, “外部システムとの連携における HEMS の定義,” [オンライン]. Available: http://www.meti.go.jp/committee/kenkyukai/energy_environment/energy_resource/pdf/004_03_03.pdf.

[9] 一般社団法人エコーネットコンソーシアム, “ECHONET Lite 規格書,” [オンライン]. Available: https://echonet.jp/spec_g/#standard-01.

[10] Industrial Internet Consortium, “Industrial Internet of Things Volume G4: Security Framework,” [オンライン]. Available: https://www.iiconsortium.org/pdf/IIC_PUB_G4_V1.00_PB.pdf.

[11] 一般社団法人日本クラウドセキュリティアライアンス, “IoT 早期導入者のためのセキュリティガイダンス(日本語バージョン),” [オンライン]. Available: https://www.cloudsecurityalliance.jp/newsite/wp-content/uploads/2016/02/Security_Guidance_for_Early_Adopters_of_the_Internet_of_Things_J_160224.pdf.

[12] 特定非営利活動法人日本ネットワークセキュリティ協会, “コンシューマ向け IoT セキュリティガイド,” [オンライン]. Available: http://www.jnsa.org/result/iot/.

[13] IPA, “IoT 開発におけるセキュリティ設計の手引き,” [オンライン]. Available: https://www.ipa.go.jp/files/000052459.pdf.

[14] GSM Association, “IoT Security Guidelines,” [オンライン]. Available: http://www.gsma.com/connectedliving/future-iot-networks/iot-security-guidelines/.

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) IoT 高信頼化検討 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	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）
	鹿妻　洋之	一般社団法人電子情報技術産業協会（JEITA）
	柘植　晃	YRP 研究開発推進協会 /一般社団法人 WSN-ATEC
	辻　和隆	一般社団法人日本電機工業会
	中垣　良夫	株式会社デンソー
	村上　隆史	一般社団法人エコーネットコンソーシアム
	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
IPA/SEC	中尾　昌善	
	宮原　真次	
	金子　朋子	
	小崎　光義	
	丸山　秀史	

「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］

平成 29 年 6 月 15 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　松本 隆明
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 http://www.ipa.go.jp/sec/

ISBN 978-4-905318-52-1　Printed in Japan

ISBN978-4-905318-52-1
C3055 ¥278E

定価：本体278円+税

IPA 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-TN17-002