SEC BOOKS

つながる世界の開発指針

～安全安心なIoTの実現に向けて 開発者に認識してほしい重要ポイント～

第2版

独立行政法人情報処理推進機構 社会基盤センター

はじめに

近年、IoT（Internet of Things）への取組みが各国で進んでいる。しかし、今までつながっていなかったモノ、つながることを想定していないモノがつながることで安全安心に関するリスクも増大すると予想される。自動車や家電など10年以上使用される機器やシステムも多いため、IoTのリスクに対して早急に対策を行う必要がある。IoTのリスクに対して守るべきものを守れる機器やシステムを開発することは国際競争力の強化にも寄与すると期待される。

そこで、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)は、様々なモノがつながって新たな価値を創出していく『つながる世界』ならではの機器やシステムに関わる企業が安全安心に関して最低限考慮すべき事項を「つながる世界の開発指針」（以下「本開発指針」）としてとりまとめた。

本開発指針では、個別具体的な遵守基準ではなく、業界横断的な安全安心の取組みの方向性を示している。第4章の指針については、個別の対策は当事者の判断としても、必ず検討を実施していただきたい。

機器やシステムの開発に関わる企業の経営者、開発者及び保守者の方々に本開発指針を理解、実践いただくことにより、つながる世界の安全安心が実現されることを期待する。

表1 特に、お読みいただきたい読者

章		経営者	開発者	保守者
第1章		○	○	○
第2章			○	
第3章			○	
第4章	4.1	○	○	○
	4.2		○	
	4.3		○	
	4.4		○	○
	4.5		○	○
第5章			○	

改訂にあたって

本開発指針第 1 版では、IoT を構成する機器やシステムに着目し、つながる世界で安全安心を維持できるような機器やシステムが満たすべき十分な「製品品質」を実現するための指針を示した。それから一年、機器やシステムを用いた IoT サービスの進展を踏まえれば、使い方や利用環境が日々変化する状況で、実際にユーザに利用される際に提供されるユーザ経験・サービスの品質、すなわち「利用時の品質」の重要性も増していると考えられる。

そこで、IPA では、2016 年 9 月に利用時品質検討 WG［1］を設置し、つながる世界の「利用時の品質」のあり方や取組みの視点をとりまとめ、2017 年 3 月に WG 報告書［2］として公開した。また、WG 報告書に基づいて本開発指針の各指針を改訂し、この第 2 版を発行している。併せて、一部指針の見直しや参照情報のアップデートも行っている。

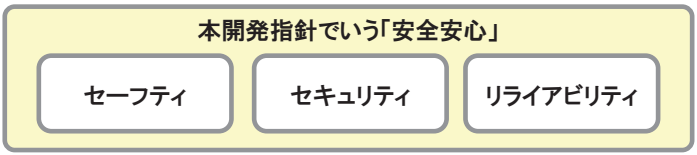
開発指針を読まれたことがない方もすでに活用されている方もぜひ第 2 版をご一読いただき、つながる世界の安全安心に役立てて頂きたいと考えている。なお、主な改訂は以下のとおりである。

改訂項目	主な改訂内容	
コラムの追加	＜コラム 2＞つながる世界の利用時の品質と安全安心（P26）	
指針の改訂	指針 1	解説追記、対策例追記、情報アップデート
	指針 2	解説追記、対策例追記、情報アップデート
	指針 4	解説追記、対策例追記
	指針 5	ポイント追加、解説追記、対策例追記
	指針 7	解説追記
	指針 11	ポイント追加、解説追記、対策例追記
	指針 13	解説追記
	指針 14	ポイント修正、解説追記、対策例追記
	指針 15	解説追記、対策例追記
	指針 16	解説追記、対策例追記
	指針 17	解説追記、対策例追記
付録	A5	「つながる世界の利用時の品質」視点一覧の追加

【本書での扱い】

(1) 安全安心の定義

本開発指針でいう「安全安心」は「セーフティ」「セキュリティ」及び「リライアビリティ」を含んだ概念である。以下にそれぞれの意味を示す。



用語	本開発指針での意味
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。
セーフティ	機器やシステムが、人間の生活または環境に対する潜在的なリスクを緩和する度合い(リスク回避性)。
セキュリティ	人間または他の機器やシステムが、認められた権限の種類及び水準に応じたデータアクセスの度合いを持てるように、機器やシステムが情報及びデータを保護する度合い。
リライアビリティ	明示された時間帯で、明示された条件下に、機器やシステムが明示された機能を実行する度合い。加えて、他の機器やシステムと適切に情報を交換しつながること(相互運用性)、その他の機器やシステムに有害な影響を与えないこと(共存性)なども含む。

出典:SQuaRE (ISO/IEC 25000 シリーズ)を参考

図 1 本開発指針における安全安心の意味

(2) IoT セキュリティガイドラインとの関係

IoT 推進コンソーシアムが発行した IoT セキュリティガイドラインに本開発指針（第 1 版）の内容が盛り込まれている。本開発指針の 2.2 で定義している「IoT コンポーネント」については、IoT セキュリティガイドラインでは「IoT 機器・システム」という用語が用いられている。

(3) 今後の検討事項

IoT では、データ品質やパーソナル情報の扱いに関する課題も想定されるが、本開発指針では対象としていない。

(4) 略称一覧

本開発指針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
ASIL	Automotive Safety Integrity Level
ATM	Automatic Teller Machine
AV	Audio Visual
BBF	Broadband Forum
BIOS	Basic Input/Output System
BITKOM	Bundesverband Informationswirtschaft, Telekommunikation und neue Medien
CAN	Controller Area Network
C2C-CC	CAR 2 CAR Communication Consortium
CCDS	Connected Consumer Device Security council
CD-ROM	Compact Disc Read Only Memory
CPS	Cyber Physical System
CSIRT	Computer Security Incident Response Team
DAF	Dependability Assurance Framework for Safety Sensitive Consumer Devices
DNS	Domain Name System
DRBFM	Design Review Based on Failure Model
D-Bus	Desktop Bus
EAL	Evaluation Assurance Level
ECU	Engine Control Unit
EDSA	Embedded Device Security Assurance
FA	Factory Automation
GSN	Goal Structuring Notation
HDD	Hard Disk Drive
HEMS	Home Energy Management System
ICT	Information and Communication Technology
ID	Identification
IEC	International Electrotechnical Commission
IEEE	The Institute of Electrical and Electronics Engineers, Inc.
I/F	Interface
IIC	Industrial Internet Consortium
IoT	Internet of Things
IPA	Information-technology Promotion Agency, Japan
ISAC	Information Sharing and Analysis Center
ISO	International Organization for Standardization
ITS	Intelligent Transport Systems
JPCERT	Japan Computer Emergency. Response Team Coordination
NIST	National Institute of Standards and Technology
OBD	On-Board Diagnostics

略語	名称
OCF	Open Connectivity Foundation
OS	Operating System
OSS	Open Source Software
POS	Point of Sales
PL	Performance Level
RFID	Radio Frequency Identifier
SAL	Security Assurance Levels
SIL	Safety Integrity Level
SMS	Short Message Service
SoS	System of Systems
SQuaRE	Systems and software Quality Requirements and Evaluation
TAL	Trust Assurance Levels
USB	Universal Serial Bus
VDMA	Verband Deutscher Maschinen– und Anlagenbau
ZVEI	Zentralverband Elektrotechnik– und Elektronikindustrie

目次

第1章
つながる世界と開発指針の目的

IoT（Internet of Things）とはあらゆる「モノ」が相互につながる世界であり、様々なメリットが期待されている。しかし、これまでつながっていなかった「モノ」は、以前からつながっていたサーバやパソコン等の情報機器と比較してセキュリティ対策が不十分であったり、つながることでセーフティ上の問題が発生したりする危険性がある。

本章では、つながる世界とそのリスクの説明、及びリスク低減に向けた本開発指針の目的を説明する。本章の流れを図 1-1 に示す。

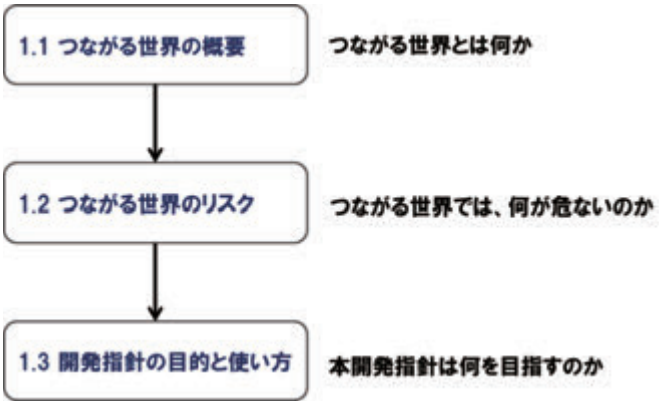


図 1-1 本章の流れ

1.1 つながる世界の概要

1.1.1 IoT とつながる世界

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 [3]。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、リアルタイムに機器やシステムを制御することも重要な特長となっている。

近年のカーナビや家電、ヘルスケアなどの機器にはコンピュータシステムが組み込まれ、情報収集、データ送受信、遠隔制御の機能を有するようになっている。これらの組込みシステムでは汎用 OS や通信規格が利用されるケースも多く、様々な「モノ」が容易に「つながる世界」の要因となっている。

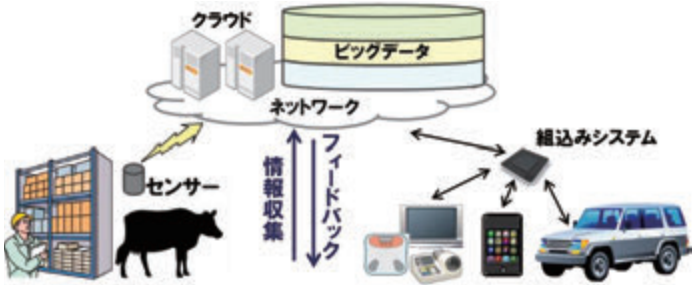


図 1-2 モノがつながる IoT

IoT については、複数のシステムが連携することでより大きなシステムとして新たな価値を実現する「System of Systems (SoS) 」の概念が参考となる。

System of Systems(SoS)の主要特性

1.構成要素の運用の独立性:個々のコンポーネントは独立かつそれ自体が役に立つように運用できる。
2.構成要素のマネジメントの独立性:コンポーネントは、個別に調達され，インテグレートされるとともに、SoS の中で独立に運用が可能である。
3.進化的開発:完成形ではなく、機能や目的が追加・削除・変更されながら進化する。
4.創発的振る舞い:コンポーネント単独では実現できない目的や機能を果たす。
5.地理的な分散:コンポーネントは広域に分散し、モノやエネルギーではなく、情報を交換する。

出典:”Architecting Principles for Systems-of-Systems” Mark W. Maier(訳:IPA)

本開発指針の「つながる世界」も、単に「モノ」同士がつながるだけではなく、独立に運用管理され単独でも有用な IoT が他の IoT とつながることにより進化し、より大きな IoT として新たな目的や機能を実現する SoS の世界をイメージしている。SoS の特性とは、図 1-3 の 1. ～5. に示される通りである。

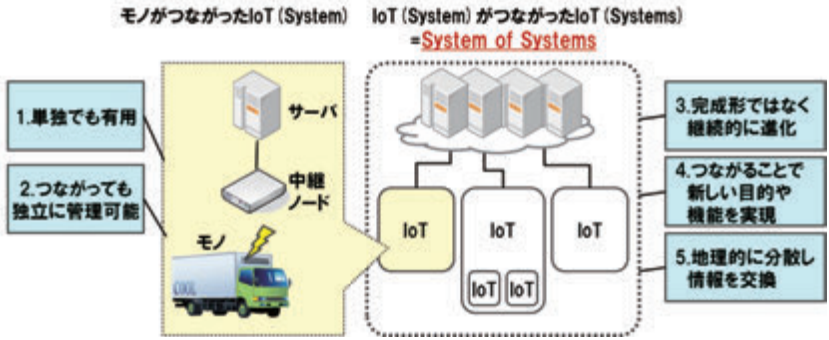
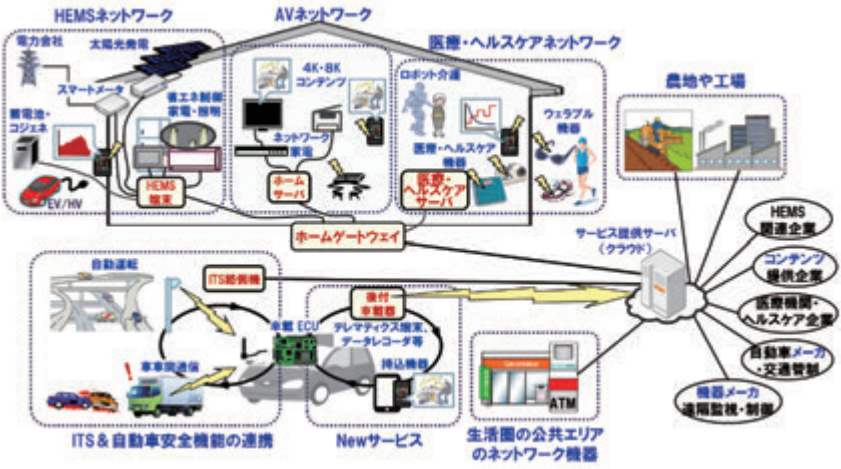


図 1-3 SoS 的な特徴を持った IoT＝「つながる世界」のイメージ

1.1.2 千変万化かつ巨大なインフラ

IoT につながる機器は 2020 年までに 250 億とも 500 億ともいわれており、家庭や公共空間、オフィス、工場、農地などに広がる巨大なインフラとなりつつある。IoT は企業や消費者を含む社会全体にとって重要なインフラといえる。

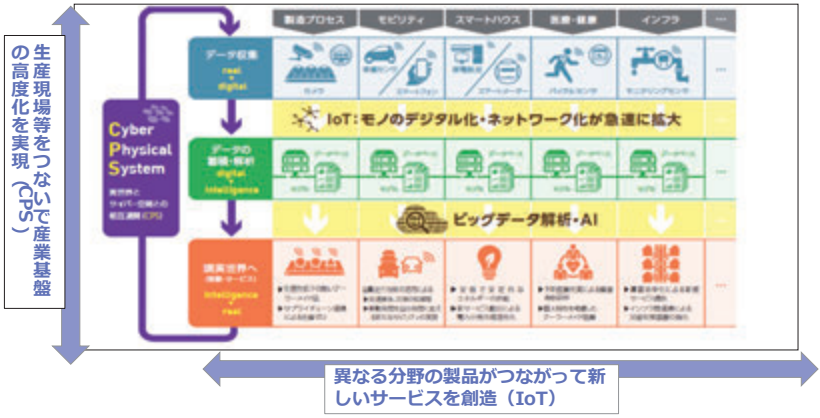


出典：一般社団法人重要生活機器連携セキュリティ協議会「セキュアライフ 2020」中の図に加筆

図 1-4 社会に広がるインフラとしての IoT

ただし、国で指定された「重要インフラ［4］」とは異なり、様々な機器やシステムが日々、サービス事業者や消費者によってつなげられたり、ウェアラブル機器や自動車などが移動しながらつながったりすることにより、その姿は常に変化している。このため、IoT の全体像を把握することは難しい。

経済産業省 産業構造審議会 商務流通情報分科会 情報経済小委員会は 2015 年、中間とりまとめ(案)において、産業基盤の高度化を図る Cyber Physical System (CPS)のイメージを公表している（図 1-5）。本図では、各分野における垂直型の CPS が IoT として横連携することでビッグデータ解析等により新たな価値を生み出すとするというイメージで整理している。すなわち、各分野の CPS が横連携することで IoT となり、そこで新しい価値が生まれるという意味で、前述の「System of Systems」の考え方が適用可能である。



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 1-5 CPS と IoT のイメージ

1.2 つながる世界のリスク

1.2.1 つながる世界のリスクの特徴

つながる世界には、従来の情報システムや重要インフラと異なり、以下のようなリスク要因がある。

(1) 想定しないつながりが発生する

近年の機器やシステムには汎用 OS や標準規格の通信インタフェースが使われており、メーカ以外の事業者でも容易に IoT サービスを構築できる上、ユーザが興味本位でつなげてしまうケースもある。このため、想定しないつながりが発生し、外部から攻撃を受けたり、情報が漏えいすることも懸念される。

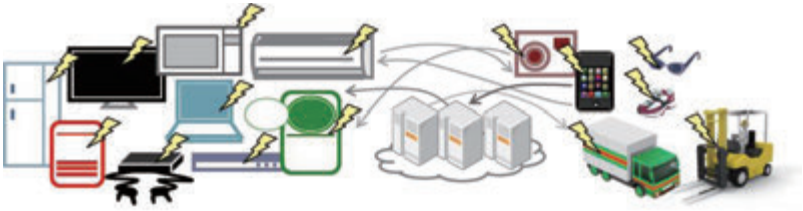


図 1-6 想定しないつながりが発生

(2) 管理されていないモノもつながる

企業の情報システムと異なり、IoT にはウェアラブル機器、駐車場の自動車、家庭の住宅設備や家電、廃棄される機器など、管理担当者がいないモノもつながる。このため、悪意がある者が直接、機器やシステムに不正なソフトウェアを埋め込んだり、廃棄された機器からデータやソフトウェアを読み出すことも比較的容易である。また、10 年以上経過し、適切に保守されていないものも混在することで、全体としての安全安心が低下する可能性もある。

図 1-7 メーカにより物理的に管理されない家庭や公共空間の機器やシステム

(3) 身体や財産への危害がつながりにより波及する

家電や自動車、ヘルスケアなどの機器やシステムの場合、事故や誤動作により身体や生命、財産に危険や損害（以下「危害」）を及ぼす可能性がある。ATMや自動販売機の場合は現金や商品の被害もありうる。単体であれば範囲も限定的であるが、IoTにつながることで被害が波及することも懸念される。

図 1-8 身体や生命、財産にも被害が及ぶ

(4) 問題が発生してもユーザにはわかりにくい

故障や破損など物理的な異常は分かりやすいが、ウイルス感染、設定ミスによる個人情報漏えいなど、ソフトウェア上の問題は目に見えない。無線経由での不正アクセスや誤接続も同様である。このようにIoTでは、つながることによる問題が発生しても、ユーザが気づかない可能性が高い。

図 1-9 目に見えないIoTのリスク

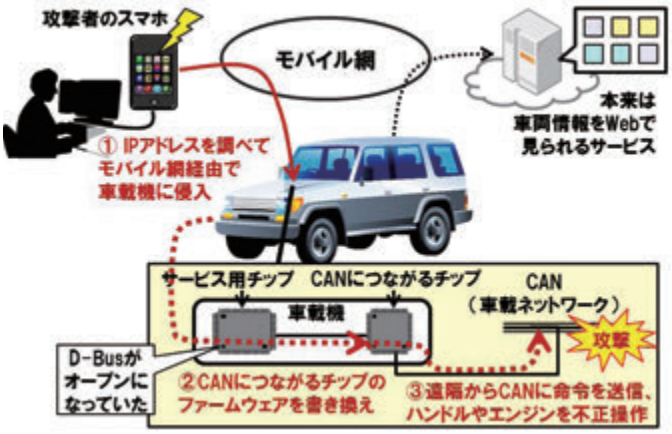
以上のように、IoTは社会全体に広がる重要なインフラであり、ユーザの身体や財産に危害を与える危険性もありながら、つながりの把握やリスクの発見、機器やシステムの管理が難しいなど、課題が多い。つながる機器やシステムの安全安心対策が必要である。

1.2.2 つながる世界のリスク例

ここでは、つながる世界におけるリスク例を紹介する。

(1) セーフティに影響を与えるリスク例

セキュリティ会議「Black Hat 2015」において、遠隔から車載器にアクセスし、走行中の自動車のハンドルやエンジンを不正に制御するデモが発表された。人命に関わる重大な危害が想定され、遠隔から姿を見られずに攻撃可能なことから実行のハードルも低く、リスクが高いと考えられる。本発表の後、対象車種 140 万台のリコールが行われている。



出典：一般社団法人重要生活機器連携セキュリティ協議会 生活機器の脅威事例集

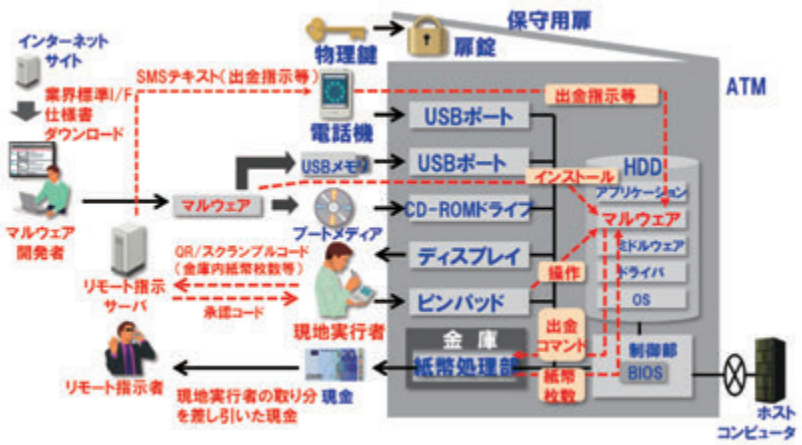
図 1-10 自動車に対する遠隔からの攻撃

主要な原因としては、モバイル網、車載器、車載ネットワーク、車両情報の表示サービスなどの構成要素が上記のような攻撃を想定していなかったことが挙げられる。このため、攻撃者がモバイル網から侵入し、車載器に不正アクセスし、チップのファームウェアを書き換え、車載ネットワークに不正な命令を送信するという一連の攻撃が成立している。つながる世界においては、構成要素のどこかで攻撃を止めることが必要である。

また、従来のセーフティは故意の攻撃を対象としていないため、つながる世界では外部からの攻撃がセーフティの機能に及ぼすリスクについても対応していく必要がある。

(2) セキュリティに影響を与えるリスク例

近年、海外では、保守用扉の物理鍵を不正に入手しATMの筐体を開けて電話機等を接続したり、ウイルスを感染させて現金を引き出す事例が発生している。現金盗難という明確な危害があり、実際にインシデントが発生していることからリスクが高いと考えられる。



出典：一般社団法人重要生活機器連携セキュリティ協議会資料より

図 1-11 ATMのリスク事例(海外のケース)

ATMについては、銀行が調達先を自由に選べるように仕様が共通化されており、ある機種を解析すれば他のメーカの機種も攻撃しやすいという特徴がある。特に近年のATMの多くは汎用OSを使用していることから、同OSに対応した機器をつなげた攻撃の対象になりやすいと想定される。

また、ATMに限らず、内部関係者が機器に不正なソフトウェアを組み込んだり、機器の設定や操作に関する情報を漏えいさせたりすれば、強固な機器でも対応しきれないと想定される。

つながる世界では、どのような機器やシステムにおいてもリスク対応が必要であるとともに、内部不正への対応も必要となる。

(3) リライアビリティに影響を与えるリスク例

近年、一部のメーカのテレビが視聴中または録画中に電源が OFF/ON を繰り返す不具合が発生した。あるメーカの発表によれば、原因はテレビ番組と併せて送信される特定放送データ（共通の番組表や特定機種のファームウェアアップデート用データなど）の中の他社データを正常に処理できなかったとのことで、不具合対応が必要な製品はそのメーカだけで 118 機種、最大約 162 万台であった［5］。

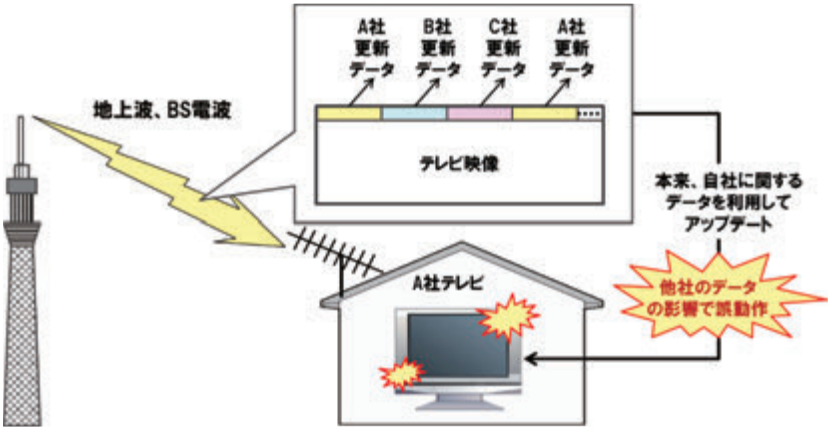


図 1-12　更新用データによるテレビの誤動作

別の事例では、ウイルス対策ソフトウェアのパターンファイルに不具合があり、パソコンの動作が極端に遅くなるというトラブルが発生した。土曜日であったため、企業の被害は新聞社や交通関係など限定されたが、それでも個人向けで約 16 万 1000 件、法人向けで約 1 万 3000 件の電話問い合わせが殺到、発生当初に対処できた件数はそのうち 4000 件程度とのことである［6］。

つながる世界では、パソコンだけでなく自動車や家電、その他、様々な機器やシステムがネットワークにつながるため、上記事例のように何らかの原因で一斉に利用できなくなれば生活に与える影響は大きい。ソフトウェアアップデートにおいては、ユーザが利用したいときに利用できる「リライアビリティ」に影響を与えないよう、十分な配慮が必要である。

1.3 開発指針の目的と使い方

(1) 開発指針の目的

本開発指針は、前述のリスクに対して、IoT 製品の開発時に考慮すべき安全安心に関わる事項を指針としてとりまとめたものである。各指針は、取組みの「ポイント」、背景の「解説」及び具体的な「対策例」から構成されている。すべてのポイントを検討することで、つながる世界のリスクを低減することを目的としている。機器やシステムの開発に関わる企業の経営者、開発者及び保守者の方々が本開発指針を活用することにより、つながる世界の安全安心が実現されることを期待する。

本開発指針の対象読者は主として機器やシステムに関わる企業の開発者であるが、開発者だけでは対応が難しい事項については経営者や保守者にも参照可能な内容としている。

図 1-13 開発指針の利用イメージ

(2) 開発指針の使い方

本開発指針の策定に当たっては、1.1 に示した IoT 及び SoS の概念を踏まえ、異なる業界の機器やシステムが横連携することによって新たな目的や機能を実現する世界を対象としている。このため、各業界での安全安心の取組み状況や先進事例を参考としつつ、企業の取組みポイントから業界連携に資する共通のポイントまで、広く記述している。

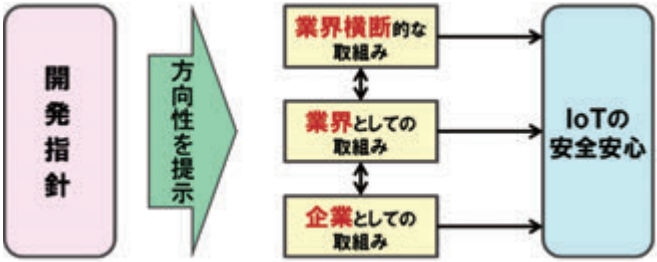


図 1-14 開発指針の対象

また、企業が現在の安全安心の取組み状況と指針との対応を確認できるよう、チェックリストも付録としている。

本開発指針の利活用方針は以下を想定している。

- 各指針のポイントは必ず検討する。
- 対策の実施は当事者の判断とする。実施する場合は各指針の対策例が参考となる。

既にセキュリティに関する基準等が整備されている業界の場合は、他の分野の機器やシステムとの連携の際に、参考とする。

具体的な利活用方法は以下を想定している。

- IoT 製品やシステムの開発時のチェックリストとして利用する。
- 指針で記述している事項は、検討時に企業や団体、業界の実情に合わせてカスタマイズして利用する。
- 内部での開発のみならず受発注の要件確認にも活用する。
- チェック結果を取組みのエビデンスとして活用する。

本開発指針の活用により各業界における IoT の安全安心の取組み及び異なる業界の連携が進み、つながる世界の安全安心が実現することを期待している。

第2章
開発指針の対象

IoT では、日々新たな機器やシステムが追加されていく一方で、自動車や家電など 10 年以上使われるものも存在する。また、IoT の規模は世界全体に広がるほど巨大であり、構成も日々変化するため、全体像を掴むことは難しい。本章では、そのような「つながる世界」に対して、どのような部分に対象を絞り、アプローチを行ったかを説明する。本章の流れを図 2-1 に示す。

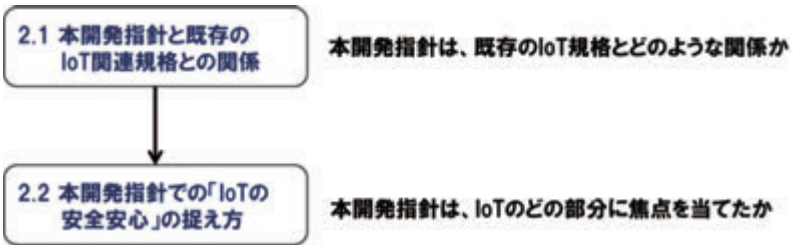


図 2-1 本章の流れ

2.1 本開発指針と既存の IoT 関連規格との関係

IoT については様々な団体で規格化が進められているが、大まかには業界・分野に共通的な「共通・汎用規格」と特定の業界や分野に依存する「業界別・特定規格」とに分類できる。前者としては IEEE、ISO/IEC、NIST、oneM2M 等があり、後者として Industrie4.0 や IIC がある。

表 2-1 主な汎用共通的な国際 IoT 規格、及び産業界における IoT 規格

	規格/団体	概要	主要参加メンバー等
共通・汎用規格	IEEE P2413	IoTにおいてドメイン横断のプラットフォームを検討	-
	ISO/IEC 30141	JTC1 SWG5 の後をうけて WG10 でリファレンスアーキテクチャを検討	-
	NIST CPS PWG	CPS の Framework 検討のための Public WG	-
	oneM2M	世界の主要 7 標準化団体の共同プロジェクト。従来の垂直統合型 M2M サービスを共通 PF で水平統合型に展開	Continua、HGI、OMA 等業界団体約 200 社
代表的な業界別・特定規格	Industrie 4.0	ドイツ政府が製造業のイノベーション政策として主導	Siemens 、Bosch 、SAP 等
	IIC	エネルギー、医療、製造、運輸、行政に焦点	GE 、AT&T 、IBM 、Cisco、Intel 等、約 150 社
	OCF	家庭、企業における多様なデバイス間の相互運用のための規格	Intel、サムスン電子、Cisco 、MS 、Qualcomm、LG 等
	HomeKit	iOS と機器をつなぐ規格	Apple 等、約 20 社

「業界別・特定規格」の安全安心に関する事項は業界の特性を反映しているため、他の業界が参考としにくい部分もある。逆に「共通・汎用規格」では、安全安心に関する事項も共通・汎用的な内容となっており、実践的なレベルとはいいがたい。

そこで本開発指針では、各業界別の実際のリスク例をベースに安全安心に関して実践的なレベルにまで踏み込みつつ、各業界で利用できるよう共通的・業界横断的なものとしてまとめることを目指した。図 2-2 にイメージを示す。

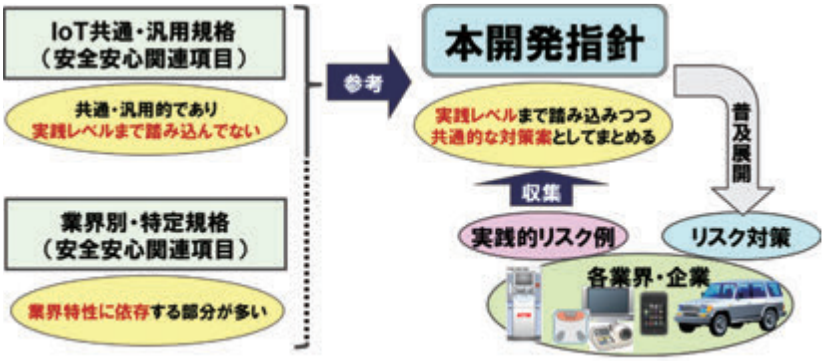


図 2-2 開発指針の位置づけ

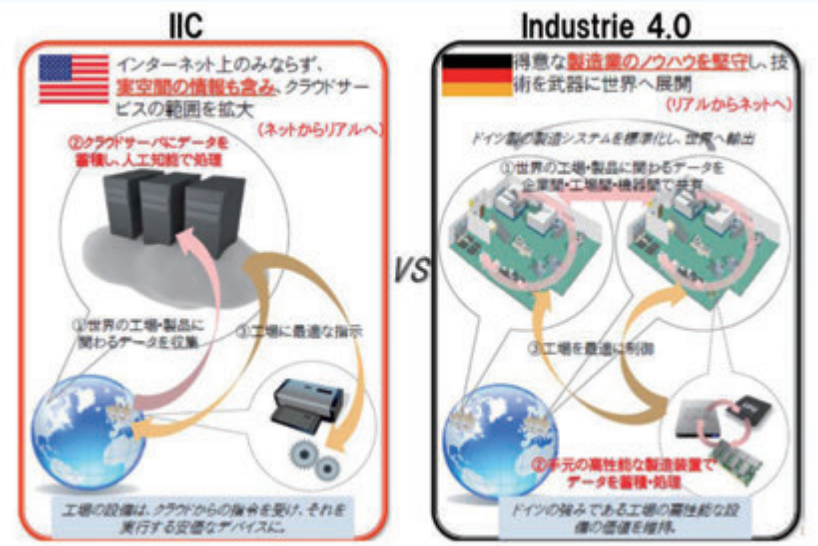
＜コラム1＞国際的な IoT 推進の動向

国際的な IoT 推進の主な取組み例として、ドイツ政府が推進する Industrie 4.0 及び米国企業コンソーシアム Industrial Internet Consortium（IIC）の概要及び特徴を紹介する。

Industrie 4.0 とはドイツ政府が推進する製造業の高度化を目指すプロジェクトである。第 4 次産業革命と称されている。その特徴は Cyber Physical System（CPS）をベースとした製造業の高度化である。BITKOM、VDMA、ZVEI の 3 団体がプラットフォーム事務局を設立し、推進している。

IIC は、Intel、IBM、Cisco Systems、GE、AT&T など 5 社によって産業市場における IoT の推進を目指して設立された団体である。IIC はエネルギー、医療、製造、運輸、行政等の領域を対象としている。IIC では IoT 向け規格の標準化団体に会員企業の要望を伝えることにより、IoT 規格の標準化やテストベッドによる検証環境構築の推進を目的としている。

Industrie 4.0 はドイツの機械産業の国際市場拡大、IIC は参加企業による IoT プラットフォームビジネスの市場創生が主要な目的と想定される。



出典：経済産業省「IoT によるものづくりの変革」より

Indsutire4.0 と IIC

2.2 本開発指針での「IoT の安全安心」の捉え方

2.2.1 「IoT コンポーネント」と「つながり」による分類

安全安心に関わる設計や評価は、機器やシステムの基本構成を基準に行われる場合が多い。しかし IoT は、1.1.1 で示したように IoT 同士がつながったり切り離されたりすることで刻々と構成が変化していくため、日々安全安心の設計の見直しや再評価が必要となり、現実的ではない。

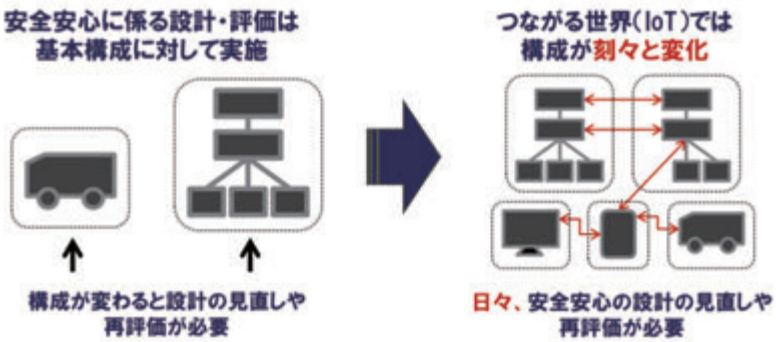


図 2-3 刻々と変化する「つながる世界(IoT)」の安全安心の設計・評価

本開発指針では、1.1.1 で示した SoS の最小単位、すなわち IoT を構成する機器やシステムのうち単独で目的や機能を果たすものを「IoT コンポーネント」と呼び、IoT は「IoT コンポーネント」と「つながり（ネットワークや情報通信等）」から構成されるものとする。その上で、「IoT コンポーネント」の安全安心の設計・評価により IoT 全体の安全安心を高める方策を検討する。

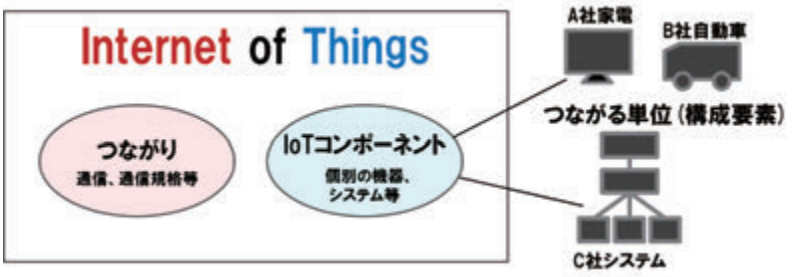


図 2-4 「IoT コンポーネント」と「つながり」により構成される IoT

2.2.2「IoT コンポーネント」の安全安心の捉え方

家電や自動車、省エネサービスなど個々の機器やシステム（IoT コンポーネント）の安全安心の設計や評価は、メーカやサービス提供企業が実施している。これに加え、IoT コンポーネントに対して、つながった場合でも安全安心を維持できる設計・評価を行えばインテグレータやユーザが IoT コンポーネントを組み合わせて利用する場合においても IoT 全体の安全安心を高められると期待される。この際には、設計内容やその条件を利用側に分かりやすく伝えることも必要である。

そこで本開発指針では、IoT コンポーネントがつながっても安全安心を維持するための設計やその内容・制限事項等の情報を関係者に伝えるための指針を示すこととした。

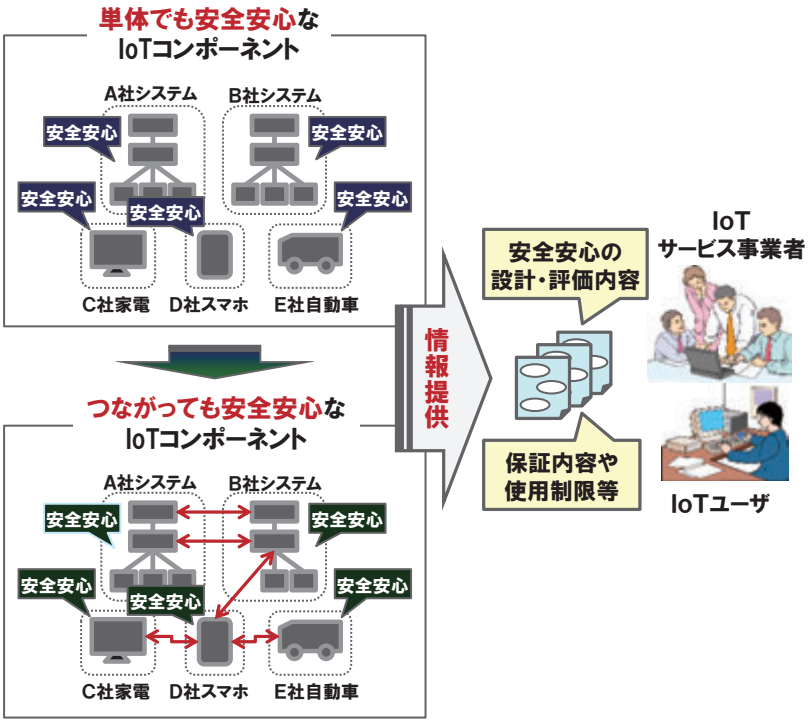


図 2-5 IoT コンポーネントの安全安心

2.2.3「IoT コンポーネント」の安全安心の二面性

IoT コンポーネントの安全安心を高めるためには本体を守る設計だけではなく、つながる他の IoT コンポーネントを守ることも重要となる。

IoT には安全安心の設計を行うことが難しい低機能・低価格の IoT コンポーネントや世代が古い IoT コンポーネントも混在すると想定される。この場合、他の IoT コンポーネントで攻撃を遮断するなどにより守ることが必要となる。また自らが故障したり、ウイルス感染した場合に、つながっている他の機器等に対して自らの異常動作を波及させないことも必要である。

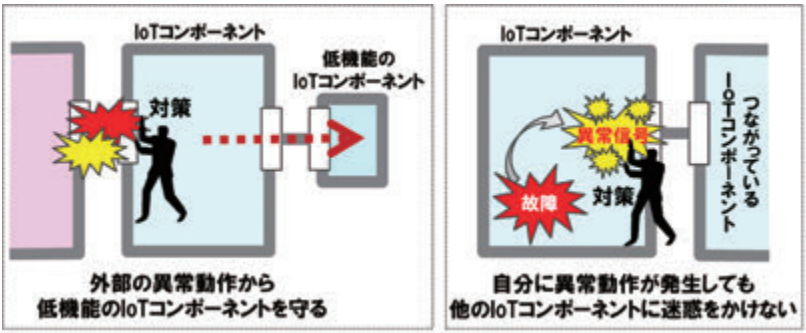


図 2-6 他の IoT コンポーネントの安全安心を実現するイメージ

以上のように、IoT コンポーネントの安全安心の設計には、自らを守る設計のほかに、つながる他の機器やシステムを守る設計も検討する必要がある。

2.2.4「つながり」の安全安心の捉え方

IoT の「つながり」の安全安心に関しては、通信セキュリティ、通信の安定性などが挙げられる。これらについては、表 2-1 で示した国際規格などで検討されているため、参照することにより国際的にも連携可能な安全安心対策の実現を目指すことが可能となる。

図 2-7「つながり」の検討方針

＜コラム2＞つながる世界の利用時の品質と安全安心

システムやソフトウェアの品質の国際規格であるSQuaRE（ISO/IEC 25000シリーズ）は、製品自体が備えている「製品品質」と併せて実際にユーザに利用される際の品質である「利用時の品質」を規定している。「利用時の品質」には多様な環境で多様なユーザが利用したときの満足度やリスクの回避などの特性が含まれている。企業においても「利用時の品質」を考慮して設計を行っていると思われるが、つながる世界では、想定外の環境で今までにない使い方をされる可能性があるため、長期にわたって満足感を維持したり、リスクを回避し続けることは容易でない。

利用時の品質を考えたつもりでも・・・・・つながる世界では想定外の使い方も！

つながる世界において安全安心を維持するためには、企画・設計段階からユーザを巻き込むことでユーザの利用環境に起因する製品品質の維持・リスクを最小限化するようなユーザ中心の設計を実現するとともに、市場に出した製品の利用状況や利用環境を把握・分析し、安全安心のための機能追加やアップデートを行うことが必要である。

また、技術的なリスク対策だけでなく、ユーザが「何がつながっているか」「自分の操作で何が起きるか」を直観的に理解できたり、実際の操作の結果を手元で確認できるような仕組みを製品に組み込むことにより、ユーザに安心をもたらす工夫も必要と考えられる。

本開発指針においても、上記のような「つながる世界の利用時の品質」を考慮した設計や運用が必要と考えられる。

第3章
つながる世界のリスク想定

巨大で常に変化する IoT に対して安全安心を実現する開発指針を策定するためには、その前提となるリスクについてもできる限り多様で特性が異なるものを想定することが望ましい。本章では、IoT をどのような軸で整理し、どのような手順でリスクを想定し、指針を策定したかを説明する。本章の流れを図 3-1 に示す。

図 3-1 本章の流れ

3.1 守るべきものの整理

一般に情報システムの「守るべきもの」としては「機能」と「情報」が挙げられるが、IoT コンポーネントの場合、自動車や建設機械のようにそれ自体の価値が高かったり、自動販売機や ATM のように商品や現金を内蔵するものもある。また、家電や医療機器、ウェアラブルデバイス、工作機械などは誤動作により人体や財産に危害を与えうるため、守るべきものの範囲は広くなる。図 3-2 に IPA が整理した IoT コンポーネントにおける守るべきものの例を示す。

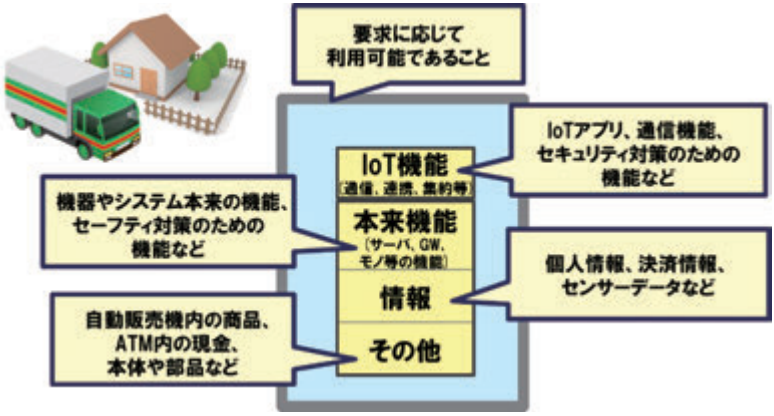


図 3-2 IoT コンポーネントにおける守るべきものの例

図中の守るべきものの意味は表 3-1 のとおりである。IoT とは、様々なモノが通信機能を持ちネットワークにつながる世界であるため、ここではモノの「本来機能」と通信等の「IoT 機能」に分けて整理している。

表 3-1 守るべきものの用語の意味

守るべきもの	用語の意味	リスク例
IoT 機能	機器やシステムが IoT につながるための機能。	IoT を介した不正アクセスやなりすまし、ウイルス感染など。
本来機能	「モノ(家電やセンサーなど)」本来の機能、セーフティ対策のための機能など。	セーフティ対策のための機能が攻撃され、故障時の被害を防げなくなるなど。
情報	ユーザの個人情報、収集情報、各機能の設定情報など。	設定変更による誤動作誘発、個人情報の漏えいなど。
その他	IoT コンポーネントが内蔵する物理的な価値。	現金、商品、本体・部品の盗難など。

3.2 つながりのパターンの整理

IoT については、機器やシステムのメーカだけでなく、IoT サービス事業者や先進的なユーザが様々なメーカの機器やサービスをつなぎ合わせて構築するケースが見られる。第三者がウイルスを注入するなどの攻撃のためにつなげる場合もある。また、有線／無線、固定的／動的（使用時に接続）など、つながり方も多様である。

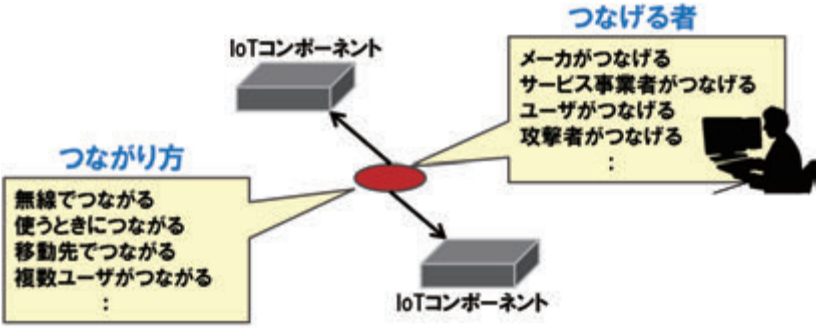


図 3-3 IoT コンポーネントのつながりの捉え方（イメージ）

以下に、IPA が想定したつながりのパターンの例を示す。IoT ではユーザ自身がつなげる場合もあり、つながり方も多種多様であるため、安全安心の維持が容易ではないと考えられる。

表 3-2 つながりのパターンの例

つながりのパターン		概要
つなげる者	メーカ	メーカが設計時に想定している接続。
	IoT サービス事業者	IoT サービスを構築するために機器やシステムを接続。中継システムの開発などにより、メーカが想定しない接続もありうる。
	ユーザ	機器やシステムを組み合わせて接続。個人輸入した機器や自作のスマホアプリなど、メーカが想定しない接続もありうる。
	攻撃者	攻撃のために、モバイルデバイスなどを接続。
つながり方	直接／間接	間接とは、ゲートウェイや集約装置を介して連携相手とつながるケース。
	有線／無線	無線については、携帯電話網、Wi-Fi、Wi-SUN など多様。
	固定的／動的	動的とは、必要時に接続するケース。移動先での接続も含む。
	専用／共用	共用とは、一つの機器を複数のユーザが利用するケース。
	複合的	上記の組み合わせ。

3.3 リスク箇所の整理

前節で整理した IoT コンポーネントの「守るべきもの」に対して、脅威やハザードを想定するとともに、どの場所で発生しうるかを整理した。IPA が想定した脅威やハザードが発生しうる箇所（以下「リスク箇所」）のイメージを図 3-4 に、想定される脅威やハザードの例を図 3-5 に示す。

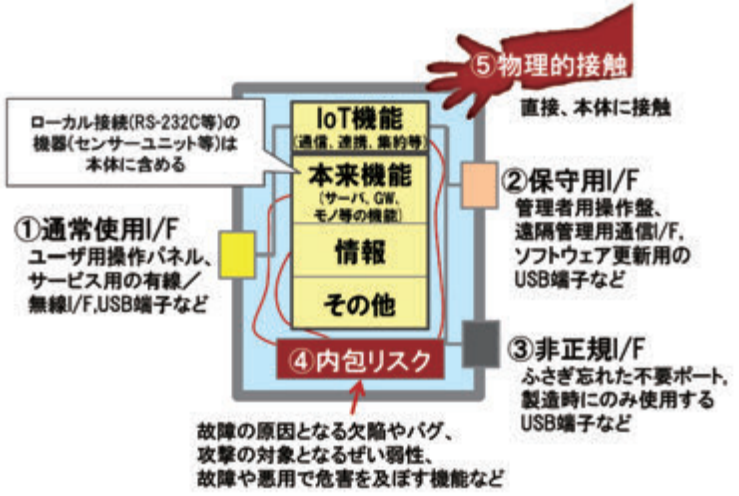


図 3-4 IoT コンポーネントのリスク箇所の例

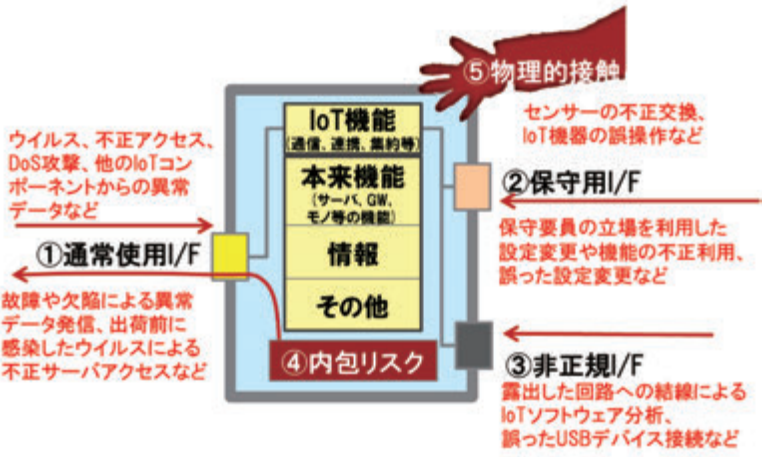


図 3-5 IoT コンポーネントに対する脅威やハザードの例

本節での検討を基に、次節において具体的なリスクの抽出を行う。

3.4 つながる世界のリスク分析の手順

一般に、セーフティのリスク分析については ISO/IEC Guide51、セキュリティについては ISO 31000 が参照されることが多いが、セキュリティに関してはその前に守るべき情報資産を洗い出す場合もある。そこで本開発指針では 3.1 の守るべきものの整理を行ったうえで、ISO/IEC Guide51 及び ISO 31000 を参考にリスク分析及び対策としての指針の策定を行った。図 3-6 に手順のイメージを示す。なお、図中の「ハザード」は身体や生命、財産、機能、情報などに被害をもたらす潜在的な要因のうちセーフティに関わるもの、「脅威」はセキュリティに関わるものを指している。

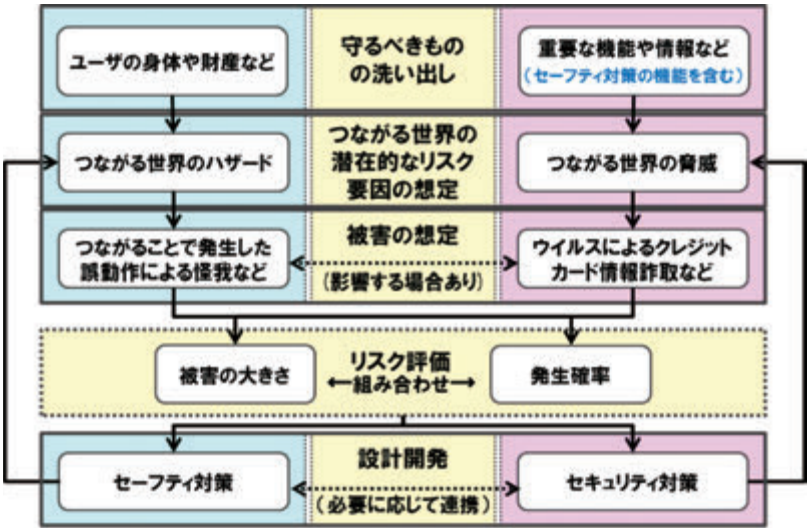
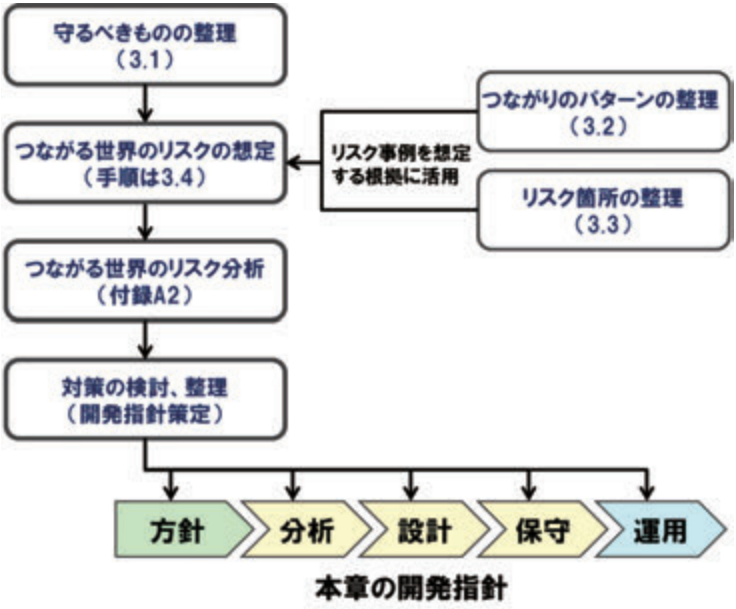


図 3-6 つながる世界のハザードと脅威の想定、リスク分析及び対策

リスクの想定においては、3.2 のつながりのパターン及び 3.3 のリスク箇所を多様的に選定することで、できる限り様々な特性を持つリスクを対処するように図っている（詳細は付録 A2 参照）。

第4章
つながる世界の開発指針

前章の手順により、関連業界の技術者、学術有識者の意見を頂きつつ、つながる世界のリスク対策を検討した。またその結果を「方針」、「分析」、「設計」、「保守」及び「運用」の各段階に整理し、開発指針としてとりまとめた。検討の流れを図 4-1 に示す。



（注）上図の開発指針において、緑は経営者、黄色は開発者、青は開発者が運用に向けて、それぞれ検討する内容であることを示す。

図 4-1 開発指針の策定の流れ

開発指針の一覧を表 4-1 に示す。また、各開発指針の概要について、以降で説明する。

表 4-1 検討して欲しい開発指針一覧

大項目		指針
方針	4.1 つながる世界の安全安心に企業として取り組む	指針 1 安全安心の基本方針を策定する
		指針 2 安全安心のための体制・人材を見直す
		指針 3 内部不正やミスに備える
分析	4.2 つながる世界のリスクを認識する	指針 4 守るべきものを特定する
		指針 5 つながることによるリスクを想定する
		指針 6 つながりで波及するリスクを想定する
		指針 7 物理的なリスクを認識する
設計	4.3 守るべきものを守る設計を考える	指針 8 個々でも全体でも守れる設計をする
		指針 9 つながる相手に迷惑をかけない設計をする
		指針 10 安全安心を実現する設計の整合性をとる
		指針 11 不特定の相手とつなげられても安全安心を確保できる設計をする
		指針 12 安全安心を実現する設計の検証・評価を行う
保守	4.4 市場に出た後も守る設計を考える	指針 13 自身がどのような状態かを把握し、記録する機能を設ける
		指針 14 時間が経っても安全安心を維持する機能を設ける
運用	4.5 関係者と一緒に守る	指針 15 出荷後も IoT リスクを把握し、情報発信する
		指針 16 出荷後の関係事業者に守ってもらいたいことを伝える
		指針 17 つながることによるリスクを一般利用者に知ってもらう

4.1 つながる世界の安全安心に企業として取り組む

つながる世界においては、自動車や家電、ヘルスケア、ATM・決済などの機器やシステムに誤動作や不正操作が発生することで、ユーザの身体や生命、財産などに危害が発生する危険性がある。またその影響はネットワークを介して広範囲に波及する可能性もある。つながる世界の安全安心は、機器やシステムの開発企業にとっては存続に関わる課題であるため、開発者のみならず経営者もリスクを認識する必要がある。

そこで本節では、つながる世界の安全安心に企業として取り組むべき 3 つの指針を説明する。

［指針1］安全安心の基本方針を策定する

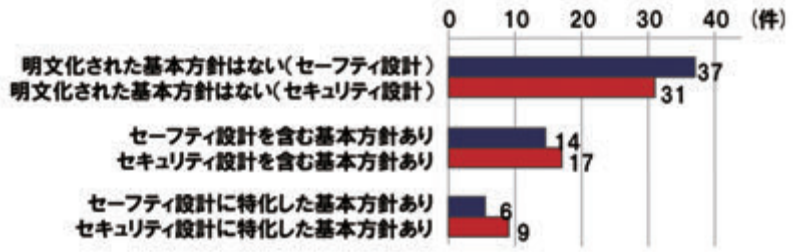
(1) ポイント

①経営者は、つながる世界の安全安心の基本方針を企業として策定し、社内に周知するとともに、継続的に実現状況を把握し、見直していく。

(2) 解説

つながる世界においては、リスクが多様化・波及し、企業の存続に関わる影響をもたらす可能性がある。また、そのリスク対策にはコストを要するため、開発現場の判断を超える場合も多いと想定される。そこで、経営が率先して対応方針を示すことが必要と考えられる。

しかしながら、先行してリスク対策に取り組んでいると想定した企業を対象に IPA が実施したアンケートでは、セーフティ/セキュリティの基本方針を策定している企業は半数以下という状況であった。つながる世界の安全安心に関する基本方針の策定と周知が急務である。



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

図 4-2 セーフティ/セキュリティの基本方針の策定状況

また、つながる世界の安全安心を高めるには、利用環境や使い方の変化によるリスクを回避するために利用時の品質の考慮が重要であり、基本方針の中に含めることも必要と考えられる。

以上のように、つながる世界に向けて安全安心に関わる基本方針を策定し、企業内への周知、遵守状況の把握及び見直しが必要である。

(3) 対策例

経営層が関与して、つながる世界の安全安心の基本方針を策定する。

①つながる世界の安全安心に向けた考慮すべき事項（例）

1) IoT に関わらず、企業が記載すべき項目例（内容は業種や業態による）

- 安全安心の対象（ユーザの生命や財産など）や対策の概要
- 安全安心な管理体制の確立および関連規程の整備・遵守
- 適切な人的・組織的・技術的対策および継続的な教育
- 問題が発生した場合の迅速な原因究明、被害の抑制及び再発防止
- 法令、国が定める指針、その他の社会的規範の遵守
- 社内への周知の方法、継続的な見直し及び改善　など

2) つながる世界で必要となる事項（内容は業種や業態による）

・経営視点でのセキュリティ対策

経済産業省／IPA「サイバーセキュリティ経営ガイドライン」[7]ではサイバー攻撃から企業を守る観点で経営者が認識すべき 3 原則などが示されている。

・企画・設計段階からの安全安心への取組み（Safety & Security by Design）

後付けでの安全安心対策はコスト面、効果面で課題が多いため、プロセスの早期から取り組む。また、ユーザの利用状況や利用環境を把握・分析し、安全安心に関わる利用時の品質を考慮した企画・設計を行う [2]。

・つながる世界でのサポート方針

刻々と変化するつながる世界において、出荷した機器やシステムの安全安心を維持する方針、さらに安全安心の保証の期限や使用制限などに関する方針を定める。

・つながる世界の安全安心対策の検証・評価の方針

つながる世界における外部からの影響や外部に影響を与えうる機能に対する安全安心の検証・評価（出荷判定条件を含む）の方針を定める。

・つながる世界の事故やインシデントへの迅速な対応方針

生活やビジネスを支えるインフラである IoT における事故やインシデント発生時の早期対応の方針を定める。

・継続的な実現状況の把握と見直し

想定外の問題が予想されるつながる世界において、安全安心の実現状況を把握するとともに、最新のリスクや安全安心の実現手段に関する情報を収集し、PDCA サイクルにより方針を見直していく。特にユーザ調査やフィードバック結果を分析し、利用時の品質向上の観点で企画・設計を見直す。

［指針2］安全安心のための体制・人材を見直す

(1) ポイント

①つながる世界における安全安心上の問題を統合的に検討できる体制や環境を整える。
②そのための人材（開発担当者や保守担当者など）を確保・育成する。

(2) 解説

つながる世界では想定外の問題が発生したり、影響が広域に波及したりする可能性があるため、緊急対応や原因分析、抜本的な対策を行う体制や、対策の検証・評価を行う環境が必要となる。

図 4-3 安全安心に関する問題への緊急対応の必要性

なお、つながる世界は様々な企業の機器やシステムにより構成されるため、企業が連携して対応に当たるための「体制の連携」も必要である。ユーザから意見を出していただける仕組みを作るとともに、つながる世界のトラブルやヒヤリハット事例を運用部門が収集し、企画・設計部門と連携して改善や予防に取り組むことも重要である。企画・設計の段階にユーザを巻き込み、早期にユーザの利用状況に起因する潜在リスクを回避するための措置を開発に取り入れる体制整備も有効である。また、知識や技術を活用して対応に当たる人材の確保・育成も必要となる。

(3) 対策例

①安全安心に関する体制や環境の例

安全安心の検討体制を連携させ、つながる世界での問題に統合的に対処可能な体制や環境を整備する。以下に例を示す。

1）製品安全管理体制の整備・維持・改善（組織体制）

経済産業省が公表した「製品安全に関する事業者ハンドブック（2012 年 6

月）」[8]の「1-3. 組織体制」において、「事業者は、製品安全に関する内部統制の目的を果たすために、企業内外における組織の役割と権限を明確化し、製品安全管理態勢の整備・維持・改善の観点から、組織のあり方を検証し続けることが必要である。」との推奨事項が示されている。

また第 4 章では「ステークホルダーとの連携・協働」として、消費者や販売事業者、設置事業者等との連携・協働による製品事故の未然防止、被害の波及防止策が示されている。

2) CSIRT（Computer Security Incident Response Team：シーサート）の設置

企業等の内部でインシデント対応や対策活動を行う組織の総称であり、関連団体でスタータキットも公開されている（指針 15、コラム 3 参照）。

3) 検証環境の整備・更新

リスク対策の効果を検証するために専用の環境を整備・更新することが望ましい。なお、個々の企業が整備するにはコストがかかるため、公的な検証の活用も有用である。

②人材育成に有用な情報源

1) つながる世界のセーフティ＆セキュリティ設計入門（IPA）

つながる世界における安全安心の実現に向けて、事故及びインシデント事例、セーフティ及びセキュリティの設計手法、関係者間での情報共有やユーザ説明に有用なセーフティ/セキュリティ設計品質の見える化手法などを紹介している [9]。

2) 情報セキュリティスキル強化に関する参考資料（IPA）

「IT のスキル指標を活用した情報セキュリティ人材育成ガイド」、「情報セキュリティスキルアップハンドブック」など人材育成に関わるガイドを公表 [10]。

3) IoT 開発におけるセキュリティ設計の手引き（IPA）

IoT のセキュリティ設計の脅威分析と対策検討をデジタルテレビ、ヘルスケア機器、スマートハウス及び自動車の事例を用いて説明 [11]。

4) つながる世界の利用時の品質（IPA）

IoT 製品・サービスの利用時の品質についての検討成果を公開。ユーザに起因するリスクの回避や安全のための機能をユーザが止めてしまわないための受容性などの観点も含まれている [2]。

5) 組込みシステムのセキュリティへの取組みガイド（2010 年度改訂版）（IPA）

組込みシステムのセキュリティ対策に関するガイド。改訂に当たり、IoT での活用が想定される IPv6 を利用した組込みシステムへの攻撃想定と対策などの記述を追加した [12]。

6) 自動車の情報セキュリティへの取組みガイド 第 2 版(IPA)

特に自動車に焦点を当てた組込みシステムのセキュリティガイド。欧州の先進事例を調査するとともに、モデルとして「IPA カー」を設定し、リスクの想定と対策の検討を行った。2017 年 3 月に第 2 版が公開されている [13]。

7) 情報処理技術者試験(IPA)

情報セキュリティマネジメント試験のほか組込みエンジニア向けのエンベデッドシステムスペシャリスト試験があり、セキュリティも範囲に含まれている [14]。また 2017 年度春期から情報処理安全確保支援士試験が開始された [15]。

［指針3］内部不正やミスに備える

(1) ポイント

①つながる世界の安全安心を脅かす内部不正の潜在可能性を認識し、対策を検討する。
②関係者のミスを防ぐとともに、ミスがあっても安全安心を守る対策を検討する。

(2) 解説

海外では、不満を持った退職者が遠隔から自動車の管理サービスを不正操作し、自動車を発進できなくしたり、ホーンを鳴らしたりする事件［16］や、銀行が管理するATMの物理鍵を複製し、その鍵を用いてATMの保守扉を開けてウイルスを感染させた上で、ATMのUSB端子にモバイルデバイスをつなげて現金を払い出させる事件が発生している［17］。つながる世界のサービスを構成する機器やシステムの設計や構造を熟知していたり、アクセス権限や鍵を不正に利用できたりする社員や退職者による「内部不正」への対策が必要である。

また悪意がない場合でも、標的型攻撃メールの添付ファイルを開封してウイルスに感染したり、持ち出した情報を紛失したりすることにより設計情報が漏えいするような「ミス」への対策が必要である。

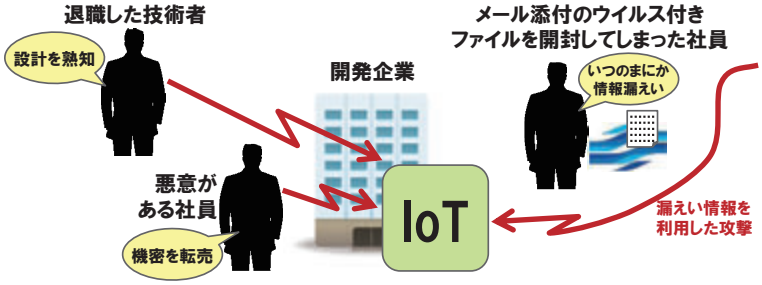


図 4-4 内部不正やミスによる影響

(3) 対策例

①内部不正への対策例

つながる世界での内部不正は他社の機器やシステム、ユーザにも多大な影響を与えるため、原因の理解と対策の必要性の認識が必要である。

・IPAの調査では、内部不正を行う主な原因や目的は、金銭詐取や転職を有利

にする目的や、仕事上の不満などとなっている。同調査における、企業社員に対する「不正をしたいと思う気持ちが高まると思う条件」のアンケート結果でも「不当だと思う解雇通告を受けた」、「条件のいい企業に対して有利に転職ができる」が上位となっている（表 4-2）。自社に照らし合わせて、社員が不正を起こさないように企業内の問題の是正や教育を進めることが必要である。

表 4-2 不正をしたいと思う気持ちが高まると思う条件（アンケート結果）

分類	順位	内容	割合※
動機・プレッシャー	1 位	不当だと思う解雇通告を受けた	30.0%
	2 位	条件のいい企業に対して有利に転職ができる	10.2%
	3 位	社内の人事評価に不満がある	8.2%
環境・機会	1 位	職場で頻繁にルール違反が繰り返されている	8.8%
	2 位	社内ルールや規則を違反した際、罰則がない	8.7%
	3 位	システム管理がずさんで、顧客情報を簡単に持ち出せることを知っている	8.4%
知識・経験	1 位	自分が情報システムの管理者ではないが、不正操作した証拠を消去することができる	9.8%
	2 位	社内の誰にも知られずに、顧客情報などの重要な情報を持ち出せる方法を知っている	9.5%
	2 位	これまでに顧客情報などの重要な情報を持ち出しても誰からも注意や指摘を受けなかった	9.5%

※内部不正行為への気持ちが高まると回答した回答者の割合。
出典：IPA 組織内部者の不正行為によるインシデント調査 [18]

・IPA では「組織における内部不正防止ガイドライン」[19]において、内部不正の基本 5 原則を公開している。本ガイドラインはつながる機器やシステムの内部不正リスクにも共通する事項が多いため、参照されたい。

表 4-3 内部不正の基本 5 原則

基本5原則	概要
犯行を難しくする（やりにくくする）	対策を強化することで犯罪行為を難しくする
捕まるリスクを高める（やると見つかる）	管理や監視を強化することで捕まるリスクを高める
犯行の見返りを減らす（割に合わない）	標的を隠す/排除する、利益をなくすことで犯行を防ぐ
犯行の誘因を減らす（その気にさせない）	犯罪を行う気持ちにさせないことで犯行を抑止する
犯罪の弁明をさせない（言い訳させない）	犯行者による自らの行為の正当化理由を排除する

出典：IPA 組織における内部不正防止ガイドライン[19]

②社員のミスや違反への対策例

近年、特定の企業や組織に対して、関係者や政府関係など信頼性が高い団体の担当者を名乗り、ウイルスを含む添付ファイル付のメールを送りつける攻撃（標的型攻撃メール）が急増している。ウイルスは情報漏えいのみならず、銀行勘定系システムに感染し、システムの不正操作を通じて ATM から金銭を払い出させるものもある。

図 4-5 実際にあった標的型攻撃メール

つながる機器やシステムの開発や保守の現場に関わらず、このような攻撃が流行していることを企業内に認知させることが重要である。しかし、標的型攻撃メールは非常に巧妙になっており、ついウイルスを含む添付ファイルを開封してしまう場合も多いため、企業内ネットワークの設計によりウイルスによる情報漏えいを防ぐ対策も必要である。

IPA では、ウイルス感染後のウイルスの動作を防ぎ、被害を最小限にとどめるための「『高度標的型攻撃』対策に向けたシステム設計ガイド」を公開している[20]。

4.2 つながる世界のリスクを認識する

つながる世界の安全安心の実現のためには、第3章で示したように守るべきものの特定とそれらに対するリスク分析が必要である。特につながる世界では、ネットワークでつながる他の機器にも影響を与えたり、つながることで想定外の問題が発生する可能性もある。このため、改めて守るべきものの特定やリスクの想定をやり直す必要がある。

そこで本節では、つながる世界のリスクの認識として取り組むべき4つの指針を説明している。

［指針4］守るべきものを特定する

(1) ポイント

①つながる世界の安全安心の観点で、守るべき本来機能や情報などを特定する。
②つなげるための機能（IoT 機能）についても、本来機能や情報の安全安心のために、守るべきものとして特定する。

(2) 解説

従来の機器やシステムは、エアコンであれば冷暖房のような固有の機能に加え、事故や誤動作が発生してもユーザの身体や生命、財産を防ぐための機能も備えている。機器やシステムが遠隔のサーバや他の家電とつながっても従来の安全安心を維持できるよう、これらの機能（本来機能）を守る必要がある。また、機能の動作に関わる情報や機器やシステムで生成される情報も、つながることで漏えいしないよう守る必要がある。IoT コンポーネントが収集するセンサーデータや個人情報などの守るべき情報の特定も必要である。つながる世界では、特に監視カメラやドライブレコーダに写る個人の撮像など受動的ユーザのプライバシーに対する配慮も必要である。

つなげるための機能（IoT 機能）についても、外部からの攻撃の入口になったり、誤動作の影響を外部に波及させないように守る必要がある。そこで、3.4 の図 3-6 に示したように、つながる世界の安全安心の観点で、本来の機能や IoT 機能について守るべきものを特定することが必要となる。

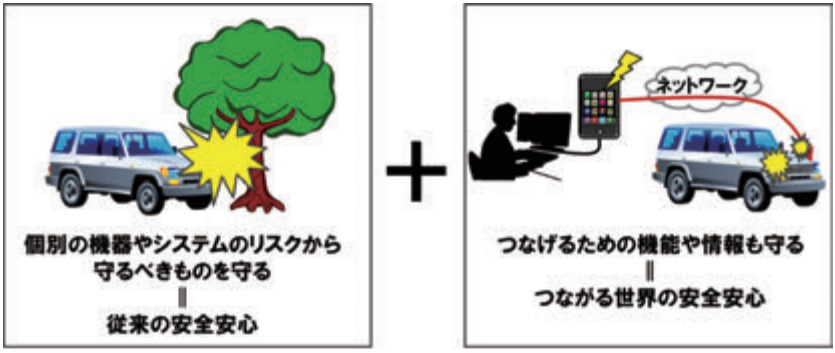


図 4-6　つながる世界で求められる安全安心

(3) 対策例

①守るべき本来機能や情報の洗い出し

1) 本来機能の洗い出し

IoT コンポーネントが有する本来機能（自動車であれば「走る」、「曲がる」、「止まる」といった機能）、生成されるセンサーデータ、ログ等の情報を洗い出す。遠隔操作など、つながりを利用した機能が追加されたり、その機能のために情報を生成したりするケースも想定されるため、根本的に洗い出す必要がある。

2) 情報の洗い出し

IoT コンポーネントが収集するセンサーデータやユーザの個人情報（プライバシー含む）などの情報を洗い出す。表 4-4 にユーザの分類を示す。

表 4-4 つながる世界のユーザの分類

名称	定義	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。 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。 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 b) 保守者，分析者，移植者，設置者 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。 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。 例1）見守りシステムで見守られる高齢者。 例2）監視カメラに写る通行人。	

（出典：IPA「つながる世界の利用時の品質」報告書）

IoT では、特に本人の意図に関わらず個人情報を収集される「受動的ユーザ」を考慮する。これについては IoT 推進コンソーシアムの「カメラ画像利活用ガイ

ドブック ver1.0 [21] [22]」が参考となる。

また、機能を構成するソフトウェアやその設定情報も読み出されて攻撃手法の考案に利用されたり、改ざんされて不正操作されるリスクがあるため、守るべきものとして洗い出す。

表 4-5 組込みシステムで守るべき情報の例

情報資産	説明
コンテンツ	音声、画像、動画等のマルチメディアデータ、コンテンツ利用履歴等
ユーザ情報	ユーザの個人情報（氏名/住所/電話番号/生年月日/クレジットカード番号等）、ユーザ認証情報、利用履歴・操作履歴等
機器情報	情報家電そのものに関する情報（機種、ID、シリアル ID 等）、機器認証情報等
ソフトウェアの状態情報	各ソフトウェアに固有の状態情報（動作状態、ネットワーク利用状態等）
ソフトウェアの設定情報	各ソフトウェアに固有の設定情報（動作設定、ネットワーク設定、権限設定、バージョン等）、設定変更の記録
ソフトウェア	OS、ミドルウェア、アプリケーション等
設計情報、内部ロジック	仕様・設計等の設計情報であり、ソフトウェアの解析や動作時に発する電磁波等から読み取られるロジックも含む

出典：IPA 組込みシステムのセキュリティへの取組みガイド [12]を基に作成

②守るべき IoT 機能や情報の洗い出し

従来の機器やシステムを IoT コンポーネントとするために追加された通信、連携、集約などの IoT 機能や情報を洗い出す。特に IoT 機能の設定情報については、IoT サービスを構築する事業が設定変更する場合もあるため、情報だけでなく設定機能も含めて、守るべきものとして洗い出す。

なお、洗い出した守るべきものは、必要に応じて重要度を整理する。

［指針5］つながることによるリスクを想定する

(1) ポイント

①クローズドなネットワーク向けの機器やシステムであっても、IoT コンポーネントとして使われる前提でリスクを想定する。
②つながる相手が偽物であることや、乗っ取られるリスクを想定する。
③保守時のリスク、保守用ツールの悪用によるリスクも想定する。

(2) 解説

2004 年には HDD レコーダーが踏み台にされるインシデント、2013 年、2015 年には複数メーカのプリンター複合機に蓄積されたデータがインターネットで公開状態となるというインシデントが発生した［23］。インターネットからアクセスできる環境での利用を想定しておらず、本体の初期パスワードを未設定のまま出荷したり、ユーザにパスワード変更を依頼していなかったことが原因と見られる。また、インターネットから隔離して運用されていた工場システムが、保守時に持ち込んだ USB メモリ経由でウイルスに感染した例もある［24］。

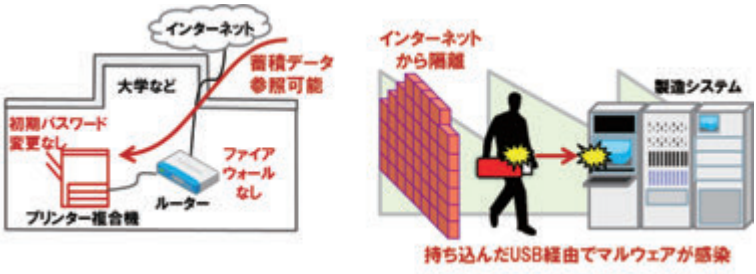


図 4-7　インターネットにつながらないと想定していたため発生したインシデント例

前者の事例はファイアウォールなどで守られた環境で使用する想定であったこと、後者の事例はインターネットから隔離していたことにより、ともに本体のセキュリティ対策が不十分であったと見られる。通信機能がある機器やシステムは利用環境の想定に関わらず、IoT コンポーネントとして使われる前提でリスクを想定する必要がある。また、年々新しい IoT やサービスが登場し、機器やシステムのつながりやユーザの使い方のパターンもべき乗級で増え、人や

環境との相互関係も複雑になる。そこで、人や環境を含めたリスク想定などを図ることが望ましい。

さらに、IoT コンポーネントが DNS への攻撃などにより不正な相手につなげられるリスクや、正規の相手であってもウイルスなどにより信頼できなくなるリスクもあるため、併せて想定する必要がある。

保守に関しては、自動車盗難防止システムの再設定機能を抜き出したツールがインターネットで販売され、自動車の窃盗に利用されている［25］。保守用ツールの悪用にも備える必要がある。

(3) 対策例

①IoT コンポーネントとしてのリスク想定

1）クローズドなネットワーク向けでも IoT コンポーネントとしてのリスクを想定

IoT につながる機能がある機器やシステムは、家庭や企業の LAN で使用する想定であっても IoT コンポーネントとして利用される前提で設計、運用する。

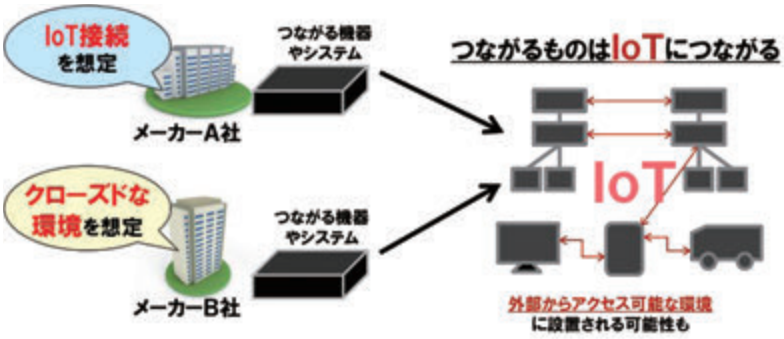


図 4-8　つながるものは IoT につながる

具体例を以下に示す。

- 出荷時の初期パスワードを同一にしない。また、推定されにくいものとする。
- ユーザ側でのパスワード変更を必須とし、パスワードの自動生成またはユーザが入力したパスワードの強度をチェックする。
- 一定回数以上の認証失敗に併せて機能制限をする。
- 必須でない場合はサーバ機能を持たせない。持つ場合は使用するポートを最小限とし、その他は使用不可とする。
- 内部の機能はすべて管理者権限とせず、適切なユーザ権限を割り当てる。

- 隔離されたネットワーク上の機器やシステムにウイルス対策ソフトウェアを入れたり、持ち込むパソコンや USB のウイルスチェックを行う。

2) 想定外の状況への対応

将来的には、機器やシステムの接続環境を確認し、問題がある場合には対策を促す機能を設けることが期待される。具体例としては、以下の状況を検知するとユーザに変更を促すメッセージを表示したり、サポート担当に通知したりする機能が挙げられる。

- 外部からアクセス可能な環境に設置されている場合
- 攻撃の可能性があった場合　など

3) 人や環境を含めたリスク分析手法の活用

機器・システム、人、環境などの相互作用を考慮してリスクを洗い出す手法として STAMP/STPA が挙げられる [26] [27]。本手法は、事故に至る原因はシステムを構成する機器等の故障や操作ミスだけではなく、人や環境を含めたシステムの安全性に関連する構成要素の相互作用から生み出されるものという考え方に基づいており、セキュリティにも適用可能である。

②つながる相手が偽物だったり、乗っ取られているリスクの想定

1) 不正な相手につながるリスクの想定

設定情報の書き換えにより不正なサーバにつながったり、意図せずに不正なアクセスポイントにつながるリスクを想定する。具体例を以下に示す。

- スマートフォンにダウンロードした偽アプリが無線ルータを乗っ取り、偽の DNS サーバを利用させることで不正なサーバに接続
- 公共機関等が設置している公衆 Wi-Fi と同じ SSID/共通パスワードを設定した不正なアクセスポイントに接続　など [28]

2) 正規のつながる相手が乗っ取られるリスクの想定

IoT コンポーネントがつながる正規の機器やシステムが乗っ取られたり、ウイルス感染するリスクを想定する。具体例を以下に示す。

- 標的型攻撃メールにより基幹システムがウイルス感染し、つながっている IoT コンポーネントに不正な命令を出すリスク　など

③保守時のリスク、保守用ツールの悪用によるリスクの想定

1) 保守時の攻撃リスクの想定

指針 3 に基づいて社員や関係会社に対して内部不正対策を図ったとしても、完全に抑制することは難しいと想定される。必要に応じて、内部不正の抑制に加え、保守時のリスクも想定する。具体的には、以下の例が挙げられる。

- 保守担当者による不正行為(不正なソフトウェアのインストールなど)
- 第三者による保守用 I/F の不正利用(非公開の保守モードの起動、ATM の物理鍵の入手など)

2) 保守用ツールの悪用リスクの想定

保守用ツールが不正利用されたり、改造されて攻撃されるリスクを想定する。具体的には、以下の例が挙げられる。

- 盗まれたり、横流しされた保守ツールの悪用(不正な設定変更など)
- 保守用ツールの脆弱性に対する攻撃(ウイルス感染など)
- 保守用ツールの設計情報の漏えいや分解・解析に基づく攻撃ツールの開発

［指針6］つながりで波及するリスクを想定する

(1) ポイント

①セキュリティ上の脅威や機器の故障の影響が、他の機器とつながることにより波及するリスクを想定する。
②特に、安全安心対策のレベルが低い機器やシステムがつながると、影響が波及するリスクが高まることを想定する。

(2) 解説

IoT では機器やシステムに故障が発生したり、ウイルスに感染したりした場合に、つながりを通じて影響が広範囲に伝播することが懸念される。機能停止すれば連携する機器やシステムに影響を与えるし、ウイルス感染で踏み台にされれば被害者から加害者に転じることとなる。機器やシステムが自分自身の異常状態や他の機器を攻撃していることを認識できない場合もありうる。また、IoT コンポーネントはその数が多い場合も想定したリスク認識が必要である。

さらに、安全安心対策のレベルが異なる IoT コンポーネントがつながることで全体的な安全安心対策のレベルが低下することも想定される。安全安心対策のレベルが低い IoT コンポーネントの脆弱性が攻撃の入口になったり、欠陥や誤設定が IoT 全体に影響を与える可能性もある。

異なる業界では IoT コンポーネントのリスク想定や安全安心の設計方針も異なると想定され、つながりで波及するリスクへの協調した対応が必要である。

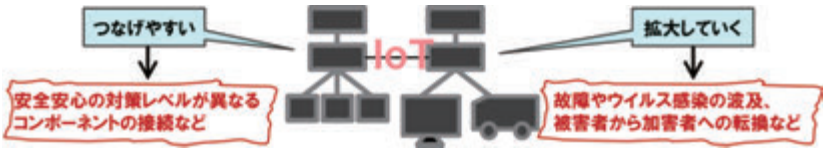


図 4-9 つながりによるリスクの増大例

(3) 対策例

①つながりにより波及するリスクの想定

1) 異常がつながりにより波及するリスクの想定

機器やシステムの異常が他の IoT コンポーネントに影響を与えるケース、ウイルスなどがつながりを介して IoT 全体に波及するケースなどを想定する。

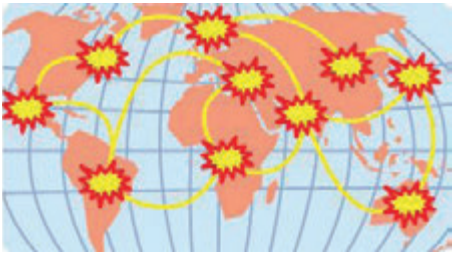


図 4-10 つながりを介して伝播するリスクのイメージ

被害を受けるケースだけでなく、機能停止することで連携する機器やシステムに影響を与えたり、ウイルス感染で踏み台にされることで被害者から加害者に転じるケースも想定する。また、機器やシステムが自分自身の異常状態や他の機器を攻撃していることを認識できないケースについても想定する。

2) 共同利用の機器やシステムを介して波及するリスクの想定

例えば、家庭用ロボットや表示デバイス、IP カメラなど、複数のサービス事業者の共同利用が想定される機器やシステムについて、操作が競合することで正常に動作しなくなる。また、共用のインタフェースがあると不正アクセスされた場合の影響が大きくなる。

図 4-11 共用機器のリスクのイメージ

②安全安心対策のレベルが低い機器やシステムがつながったことにより影響が波及するリスクが高まることの想定

安全安心対策のレベルが異なる IoT コンポーネントがつながることで、レベルが低い IoT コンポーネントが攻撃の入り口になるリスクを想定する。また、レベルが低い IoT コンポーネントが接続された IoT が別の IoT と接続することで全体的にリスクが波及することも想定する。

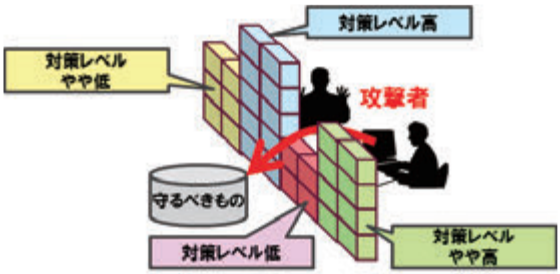


図 4-12 弱い部分からリスクが発生するイメージ

IoT は 1.1.1 で説明した System of Systems であるため、IoT 同士が接続してより大きな IoT を構成する中で、個々の IoT コンポーネントのリスクが IoT 全体に波及する可能性を想定する必要がある。

［指針7］物理的なリスクを認識する

(1) ポイント

①盗まれたり紛失した機器の不正操作や管理者のいない場所での物理的な攻撃に対するリスクを想定する。
②中古や廃棄された機器の情報などの読み出しやソフトウェアの書き換え・再販売などのリスクを想定する。

(2) 解説

つながる世界では、持ち歩いたり、家庭や公共空間などに設置された機器やシステムもIoTを構成するようになる。このため、盗まれたり紛失した機器が不正操作されたり、駐車場や庭、公共空間に設置された機器が第三者によって物理的に攻撃される危険性がある。また、廃棄した機器から情報が漏えいしたり、不正なソフトウェアを組み込んだ機器が中古販売される可能性もある。

図 4-13 メーカにより物理的に管理されない家庭や公共空間の機器やシステム（再掲）

つながる世界ではIoT製品・サービスの使い方や利用環境も変化していくため、実際のユーザの利用状況を把握・分析し、新たな物理的なリスクを想定することが必要である。

(3) 対策例

①物理的リスクの想定例

1）盗まれたり紛失したIoTコンポーネントに起因するリスクの想定
盗まれた機器が不正操作されたり、紛失して拾われた機器がいじられIoTサービスが誤動作したりするようなリスクを想定する。

図 4-14 紛失した IoT コンポーネントによる物理的リスクの例

2) 管理者のいない場所で物理的に攻撃されるリスクの想定

駐車場の自動車や庭に置かれた省エネ機器のカバーが開けられ、不正な機器をつなげられて遠隔操作されるなどのリスクを想定する。また、留守宅に侵入して家電の設定を変更し、不正なサイトに接続させるリスクも考えられる。

図 4-15 駐車場の車に攻撃される物理的リスクの例

②不正な読み出しや書き換えの想定例

1) 廃棄された IoT コンポーネントから守るべきものを読み出されるリスクの想定

廃棄された IoT コンポーネントのソフトウェアや設定を読み出してつながる仕組みを解析して IoT の攻撃に利用したり、個人情報を読み出し、なりすましにより不正アクセスするリスクを想定する。

図 4-16 廃棄された IoT コンポーネントを利用して攻撃されるリスクの例

2) IoT コンポーネントに不正な仕組みを埋め込み、中古販売されるリスクの想定

IoT コンポーネントのソフトウェアを不正なサイトに接続させるように書き換えてオークションに出したり、中古店に販売されるリスクを想定する。

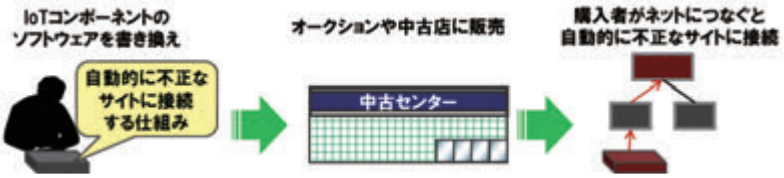


図 4-17 不正なサイトに接続する中古 IoT コンポーネントが販売されるリスクの例

4.3 守るべきものを守る設計を考える

限られた予算や人材でつながる世界の安全安心を実現するためには、守るべきものを絞り込んだり、特に守るべき領域を分離したりするほか、対策機能が低い IoT コンポーネントを連携する他の IoT コンポーネントで守ることも有効である。また、IoT サービス事業者やユーザが不特定の機器やシステムをつなげても安全安心を維持したり、異常が発生してもつながる相手に迷惑をかけない設計が望まれる。

本節では、上記の設計も含め、守るべきものを守る設計として取り組むべき 5 つの指針を説明している。

［指針8］個々でも全体でも守れる設計をする

(1) ポイント

①外部インタフェース経由／内包／物理的接触によるリスクに対して個々の IoT コンポーネントで対策を検討する。
②個々の IoT コンポーネントで対応しきれない場合は、それらを含む上位の IoT コンポーネントで対策を検討する。

(2) 解説

3.3 では、IoT コンポーネントにおいて発生するリスクとして「外部インタフェース（通常使用 I/F、保守用 I/F、非正規 I/F）経由のリスク」、「内包リスク」及び「物理的接触によるリスク」を挙げている。外部インタフェース経由のリスクとしては、DoS、ウイルス、なりすましなどの攻撃や他機器からの異常データが想定される。内包リスクとしては、潜在的な欠陥や誤設定、出荷前に不正に埋め込まれたマルウェアなど、物理的接触によるリスクとしては、家庭や公共空間に置かれた機器の持ち逃げ・分解、部品の不正な入れ替えなどが想定される。これらのリスクへの対策が必要である。

図 4-18 機器に対する物理的接触による攻撃

IoT コンポーネントにはセンサーなど性能が低いため単独では対策機能の実装が難しいものもある。その場合、それらを含む上位の IoT コンポーネントで守る対策を検討する。

(3) 対策例

①外部インタフェース経由／内包／物理的接触によるリスクへの対策

1）外部インタフェース経由のリスクへの対策
・通常使用 I/F 経由のリスクへの対策としては、利用者認証、メッセージデータの

正当性検証、ファジングツール等による脆弱性対策、ロギングなどが行われている [12]。

・保守用 I/F は保守・運用者用の I/F であるため、接続機器認証、利用者認証等の対策が見られる。特に重要な機器については、I/F を物理的な鍵で保護したり、二重鍵、生体認証、特殊なアダプター経由での接続などの例も増えている。

・非正規 I/F はデバッグ用途などに用いるもので高い権限を持つ場合が多いため、他の I/F と比較してより高度なセキュリティ機能が求められる。

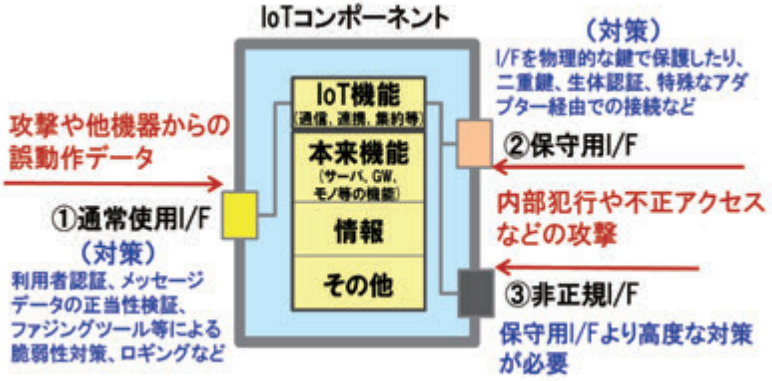


図 4-19 外部インタフェースのリスクへの対策

2) 内包リスクへの対策

・部品やソフトウェアの外部調達においては、設計データや品質データを入手し、不正な埋め込みや品質上の問題がないことを確認する対策が行われている [9]。

・コンテンツを扱う機器では、内部のデータやソフトウェアの正当性チェック、生成データの妥当性チェックなど、実行時に対策を行う例がある。また、重要なデータについては暗号化等の秘匿対策を行っている。

・内蔵時計を持つ機器では、外部の信頼できるシステムを利用した定期的な時刻補正、時計機能の耐タンパー性の強化を行っている。また、複数の IoT コンポーネントが関連するケースでは、それらの間で時刻同期を行う対策が見られる。

・スマートフォン等のオープンなプラットフォーム上で動作するソフトウェアの開発では、ソースコードのセキュリティ検査ツール等により脆弱性対策が行われている。

3) 物理的接触によるリスクへの対策

機器が盗みだされて分解されても内包するデータやソフトウェアを読み出されないようにする。表 4-6 に例を示す。

表 4-6 物理的接触によるリスクへの対策例(耐タンパー性)

対策の種別	対策例
ハードウェアや構造設計による対策	- 機器を分解すると配線が切断されたり、インタフェースが破壊されたりすることで解析を妨げる設計 - 不要な非正規 I/F や露出した配線の除去 - 専用認証デバイスを接続しないと内部にアクセスできない設計 - 漏えい電磁波から内部処理を推定させないための電磁シールド - チップや配線の内装化
データやソフトウェア設計による対策	- 盗難、紛失時に遠隔から端末をロックする機能の実装 - ソフトウェアの難読化、暗号化 - 機密データの暗号化、使用時のメモリなど在中時間の短縮 - 実行時のメモリ上でのプログラムやデータの改ざんの防止

レンタルや中古、廃棄された機器などに残されたデータの読み出しを防止するために、スマートフォン等では不揮発記憶域上のデータを消去する機能が実装されている。

4) 守るべきものの重要度に応じたセキュリティ対策

機器やシステムの全てを守るのではなく、守るべきものに応じて対策を行うことでコストの低減が可能である。

・IoT コンポーネントを構成する機器やシステムを物理的または仮想的なゲートウェイにより複数の領域(以下「ドメイン」)に分割し、異常発生の影響の範囲を局所化したり、重要な機能を多重のゲートウェイにより守ることが可能である。

・決済にともなう重要な情報はセキュリティレベルが高い周辺機器で読取及び暗号化を行い、そのままサーバ送信することで機器本体に重要情報を残さない方法がある。セキュリティ強化と対策・管理コストの低減を両立することが可能で、POS 業界において標準化が進められている。

②対策が不十分な IoT コンポーネントを上位の IoT コンポーネントで守る対策

性能が不十分でセキュリティ機能を載せられない IoT コンポーネントは、下図のようにそれらを含む「上位の IoT コンポーネント」で守る対策を検討する。

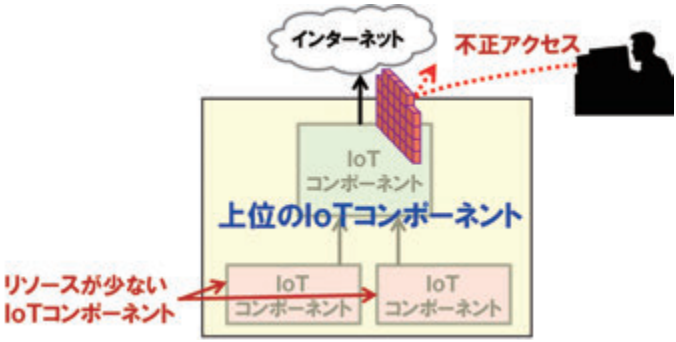


図 4-20 上位の IoT コンポーネントで守るイメージ

・IoT コンポーネントが通信でつながる接点を絞り込むとともにゲートウェイを設け、攻撃を遮断する設計を行う。

・さらに、監視機能を有する他の IoT コンポーネントにより、機器やシステムを監視し異常検知や原因推定を行う。家電の遠隔管理のための標準仕様として Broadband Forum (BBF)の TR-069 がある [29]。

図 4-21 対策機能が低い IoT コンポーネントの対策のイメージ

なお、製品の仕様上の制約等により十分な対策をとれない IoT コンポーネントの開発者は、当該 IoT コンポーネント使用時のリスクへの対策で考慮すべき事項をマニュアルや使用手引書等で明示する必要がある。

［指針9］つながる相手に迷惑をかけない設計をする

(1) ポイント

①IoT コンポーネントの異常を検知できる設計を検討する。
②異常を検知したときの適切な振る舞いを検討する。

(2) 解説

ソフトウェア／ハードウェアの不具合や攻撃などによる異常な動作が発生した場合、影響の波及を防ぐために、まず異常な状態を検知できるようにする必要がある。また、異常な状態が検知された場合、内容によっては影響が他の IoT コンポーネントに波及する可能性があり、それを防ぐために当該 IoT コンポーネントをネットワークから切り離す等の対策の検討が必要である。

IoT コンポーネントのネットワークからの切り離しや機能の停止が発生した場合、その IoT コンポーネントの機能を利用していた他の IoT コンポーネントやユーザへの影響を抑えるために、状況に応じて早期に復旧するための設計が必要となる。

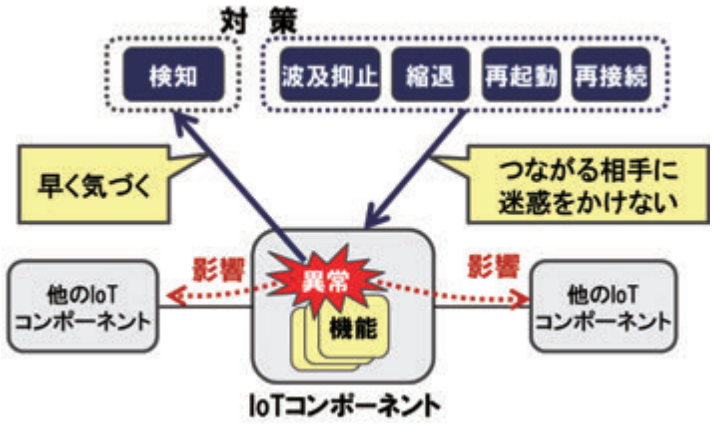


図 4-22 機能の切り離しと復旧のイメージ

(3) 対策例

①異常状態の検知

異常状態の検知は、まず各 IoT コンポーネントが個々に行っておく必要がある。ただし、仕様や異常の状態によっては IoT コンポーネントが自身の異常を検知できないケースがある。このケースに対しては、IoT コンポーネントのログ情報を監視サーバが参照することによって異常状態を検知する対策例がある。

ログによる監視の例を以下に示す。

・連携した複数の IoT コンポーネントの監視

複数の IoT コンポーネントの連携が重視されるケースでは、監視システムが関連したコンポーネントの処理結果の整合性を確認して異常を検知する方法がある。異常の検知ではより効果的な方法の検討が進んでおり、5.2 でその動向を記載している。

・IoT コンポーネントの監視による負荷の増加の抑制

ログ監視ではサーバ側の CPU や記憶域、ネットワーク帯域などの資源を消費することになるため、監視対象システムの規模や IoT コンポーネントの性能に応じて監視方法を適切に設計する必要がある。図 4-23 に例を示す。

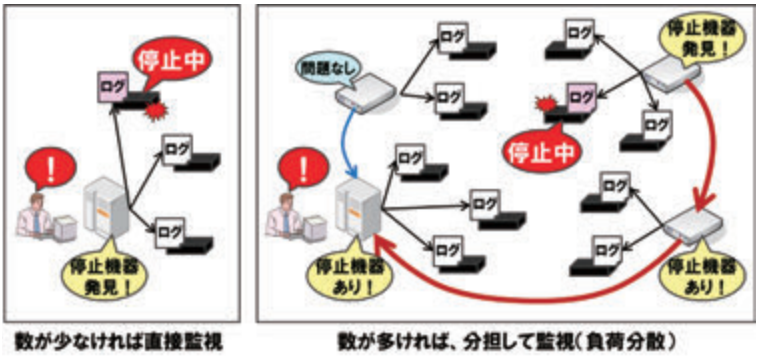


図 4-23 IoT コンポーネントの性能を考慮した監視方法の例

②異常発生時の波及防止や復旧

1) 異常状態の影響の波及抑止

・IoT コンポーネントが自身の異常な状態を検知した場合、それが他の IoT コンポーネントに影響を及ぼす可能性がある場合は、自身を停止、あるいはネットワークから切り離すことにより、影響の波及を抑止する。

・監視サーバが IoT コンポーネントの異常を検知した場合は、その内容によって当該 IoT コンポーネントに停止やネットワーク切断を指示したり、ルータ等を利用し強制的にネットワークから切り離す。

2) 異常が発生した機能の縮退

発生した異常が機能に限定されていると判断される場合はその機能の実行のみ制限し、他の機能は実行可能としておく。機能を制限する対応の例を以下に示す。

- 当該機能の受信ポートのみ閉鎖する
- 当該機能を実行するプロセスのみ停止する
- 環境設定により当該機能が必ずエラーを返すようにする

3) IoT コンポーネントの再起動・再接続

・状況によっては、当該 IoT コンポーネントを再起動することで異常な状態が解消され、復旧するケースがある。再起動は、異常検知を契機として IoT コンポーネント自身で行うケースと、監視サーバ等の外部から行うケースとがある。

・異常を波及させないために切り離された IoT コンポーネントをその運用方針や機能に応じた手順で復旧し、ネットワークに再接続する。

4) IoT コンポーネントの復旧力／回復力

・システムやサービスの復旧力／回復力はレジリエンスという概念で扱われ、IoT の分野でも重視されてきている。レジリエンスについては、主要な標準規格で取り上げられており、対策を検討する上で参考とすることができる。（コラム 3 参照）

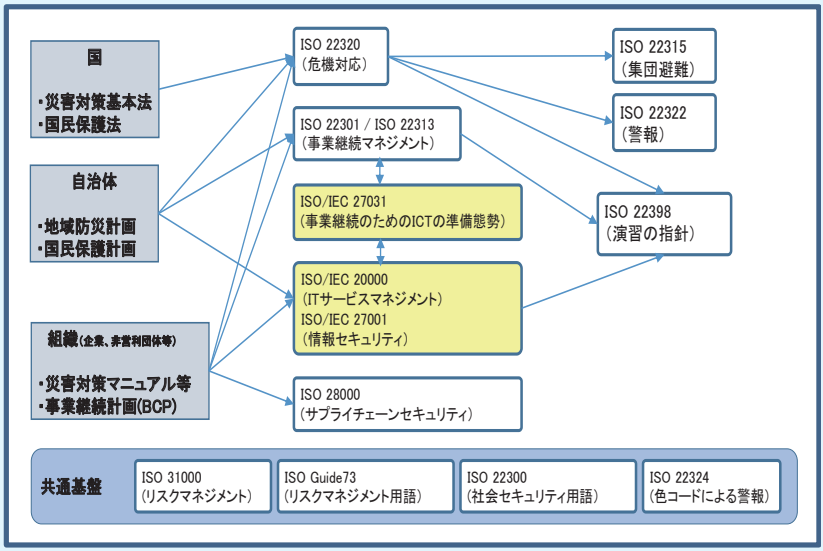
＜コラム3＞　異常からの回復力（レジリエンス）

近年、予測し難い変化や混乱が発生したときでも、それに対応し、最小限の機能を維持しながら迅速に元の状態に回復する能力が重視されておりレジリエンス（resilience）と呼ばれている。IoT においても、セキュリティ・セーフティの対策を行ってもシステムに障害や誤りが発生する可能性をゼロにはできないため、レジリエンスへの対応が必要となる。IoT 関連規格における取組み状況は以下のとおりである。

- NIST CPS Framework では、セキュリティ・プライバシー・セーフティ・リライアビリティと並んでレジリエンスが信用性の要素になっている。
- IIC の”Industrial Internet Reference Architecture”でも、主要項目として取り上げられている。

ISO ではレジリエンスに関連した標準化が進んでおり、ICT／IT システムの分野では、ISO/IEC 27031（事業継続のための ICT の準備態勢）、ISO/IEC 20000（IT サービスマネジメント）、ISO/IEC 27001（情報セキュリティ）で標準規格が策定されている。レジリエンスに関連する標準規格とその相互関係を図に示す。

今後、IoT におけるレジリエンスの標準化動向が注目される。



出典：レジリエンス協会　レジリエンスに関連する国際規格とその相互関係　を基に作成

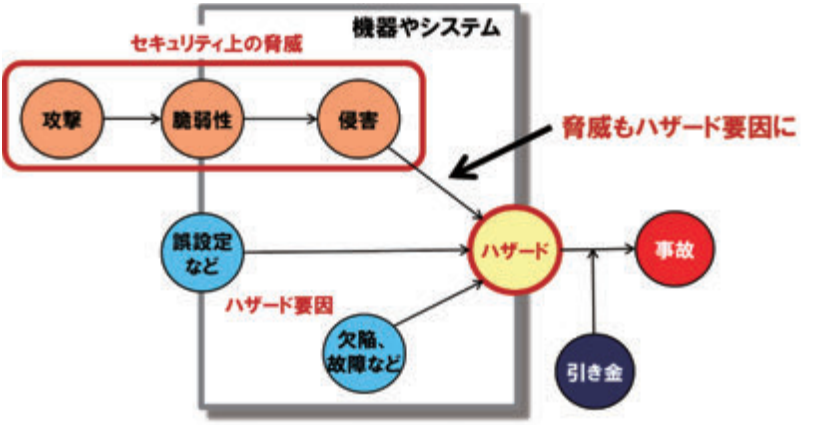
［指針10］安全安心を実現する設計の整合性をとる

(1) ポイント

①安全安心を実現するための設計を見える化する。
②安全安心を実現するための設計の相互の影響を確認する。

(2) 解説

セキュリティ上の脅威がセーフティのハザード要因となるケースがある。例えば、第三者による IoT コンポーネントへの不正侵入によりソフトウェアやデータの改ざんが行われた場合、何らかのきっかけで誤動作を引き起こす可能性がある。また、セキュリティ機能を実装することでセーフティ関連も含めた本来機能の性能に影響を与える可能性もある。それらの対策が適切に行われているかどうかを確認するために、セーフティとセキュリティの設計の「見える化」が有効である。



出典：SESAMO プロジェクト「SECURITY AND SAFETY MODELLING FOR EMBEDDED SYSTEMS」を基に作成

図 4-24 セキュリティ上の問題がセーフティに影響を与えるモデル

セーフティとセキュリティの設計品質の確認では、ハザードや脅威とそれらから引き起こされるリスク対応だけでなく、セーフティとセキュリティの相互の影響を確認する必要がある。その際には、それらの相互の影響を可視化し、異なる部署・異なる企業の技術者間で設計の整合性を確認することを容易にする対策も有効である。

(3) 対策例

①安全安心の設計の見える化

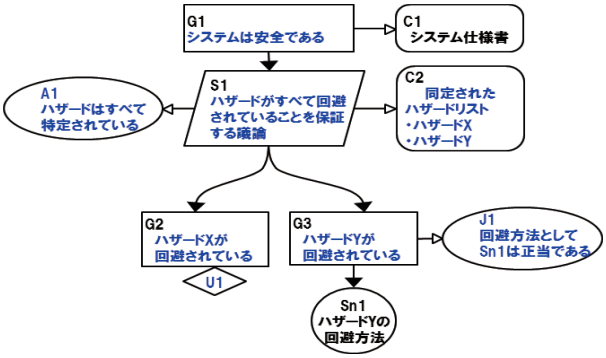
・設計の「見える化」とは、設計における分析、設計、評価などのプロセスを経緯や根拠も含めて可視化することであり、セーフティとセキュリティの技術者間での相互の設計品質の共有に有用と期待される。また、既存の機能を新製品に流用する場合の設計品質の理解や評価にも活用可能である。

出典:つながる世界のセーフティ&セキュリティ設計入門

図 4-25 ソフトウェアの設計品質の見える化

・見える化することで、開発者のみならず、経営層、発注元、外注先などに対するセーフティやセキュリティの設計品質の説明及び合意にも活用することが可能である。万一、事故が発生した場合でも、慌てて状況を確認したり、資料を整えることもなく、被害者に対する説明責任を果たすことが可能である。

・見える化の方法は開発対象や開発環境に応じて様々なものが考案され、活用されている。図 4-26 によく知られた見える化の一手法である GSN の表記例を示す。設計の見える化の詳細は「つながる世界のセーフティ&セキュリティ設計入門」を参照されたい [9]。



出典:つながる世界のセーフティ&セキュリティ設計入門

図 4-26 GSN での表記例

・消費者向けデバイスのディペンダビリティを実現するための国際規格として、セーフティ/セキュリティ設計を見える化し、すり合わせながら開発するためのメタ規格 ”Dependability Assurance Framework for Safety Sensitive Consumer Devices （DAF）”がある [30]。

②セーフティとセキュリティの相互の影響の確認

セキュリティ対策においては、守るべき機能（本来機能やセーフティ関連機能）を特定し、脅威とリスクの分析を行う必要がある。以下に検討の例を示す。

・守るべき機能（要件）に対する脅威・リスク分析、セキュリティ対策検討、効果及び守るべき機能への影響の分析・評価を行い、評価結果が受容可能でない場合には再分析・再検討を行う。

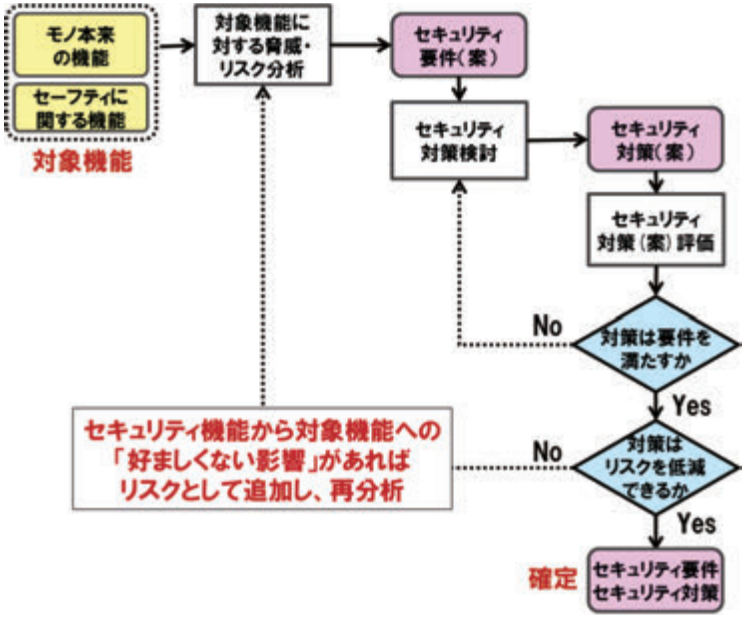


図 4-27 セキュリティ評価・分析・対策のフロー

・守るべき機能の規模が大きい場合、セキュリティ対策の影響分析を漏れなく行うことが複雑になる。この場合の影響分析手法の例としては、DRBFM（Design Review Based on Failure Model） 等が挙げられる [31]。

［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

(1) ポイント

①IoT コンポーネントがつながる相手やつながる状況に応じてつなぎ方を判断できる設計を検討する。
②危険なつなぎ方をしにくい設計や危険なつなぎ方に気づくような設計を検討する。

(2) 解説

機器のメーカで接続して動作確認をしていない機器の組み合わせであっても、業界の標準規格の機能を持つ機器を接続して利用できることが多い。そのため IoT が普及するに従い、利用されている機器のメーカが意識していない不特定の機器が、インテグレータや先進ユーザによってつなげられて利用されるケースが増えている。

図 4-28 不特定の機器とのつながり

この状況においては、信頼性の低い機器が接続された場合に、秘密情報が簡単に漏えいしたり、あるいは想定していない動作が引き起こされてしまう可能性がある。また、同じメーカ同士の製品でも、時間が経つにつれて後から出荷された型式やバージョンが増え、接続動作確認が行われていないケースも増加する。つながる相手やつながる状況に応じてつなぎ方を判断する設計を検討する必要がある。

また、ユーザや機器設置の担当者が危険な機器をつなげないように導く設計も必要である。ユーザ経験や利用環境を把握・分析し、説明書きやシール、機器本体による警告などにより工夫していくことが考えられる。

(3) 対策例

①つながる相手やつながる状況を確認しその内容に応じてつながり方を判断する設計

他の機器と接続する際、相手のメーカ、年式、準拠規格といった素性に関する情報を確認し、その内容に応じて接続可否を判断する設計が考えられる。また、接続相手の素性に応じて提供機能や情報の範囲を変更することにより、リスクを許容範囲に抑えながらつながりを広げる設計が考えられる。

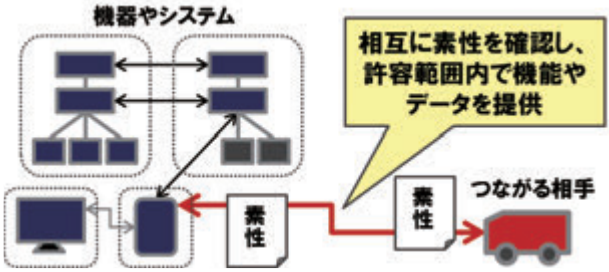


図 4-29 相手の素性により提供機能や情報を変更

・同じメーカの機器であればフルにつながり、同じ業界団体に属する企業の機器であれば一定のレベルまでつながるといった形で制限していくことが考えられる。

・つながる相手が相応の権限を有する機器と確認できた場合のみ重要な機能を利用させることでセキュリティレベルを高める方法もあり、例えば海外 ATM では保守時などにおける不正な端末での操作を防ぐ目的で利用されている。

・一方で、つながる範囲が広いほど IoT におけるビジネスチャンスやユーザの利便性が高まると期待されることから、異なる業界の企業、ビジネス上のつながりがない企業の機器であっても安全安心に関連する標準規格に準拠していれば最低限の機能や情報提供を行うことも考えられる。今後必要になると考えられる対策技術例について、第 5 章を参照されたい。

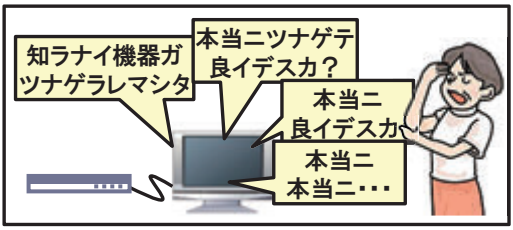
なお、異常なケースが発生するときの機器の接続形態や状況・利用形態に関する情報を蓄積し、異常発生の予防に活用していく試みも進められている。詳細は第 5 章を参照されたい。

②危険なつなぎ方をしにくい設計や危険なつなぎ方に気づくような設計

危険なつなぎ方やつなぎ間違いを洗い出す手法として「ミスユースケース」図の作成が有効である。これは、仕様に沿った正規の使い方（ユース）と脅威となる使い方（ミスユース。正規ユーザによる行為、悪意のない行為も含む。）を同一のユースケース図に表現するもので、脆弱性や危険な操作の可能性を明らかにするとともに、その対策が正規の使い方を阻害しないかを確認できる。

上記で洗い出した危険なつなぎ方に対して、ユーザに警告する機能の搭載も考えられる。例えば、不正な IoT に誤ってつなげようとしたときに自動的にブロックしたり、ユーザに警告を出して確認させたりすることが挙げられる。これによりリスクを回避するとともに、ユーザにどのような場合が危険であるかを認知させ、リスクを予防する効果も期待される。

ただし、頻繁に警告が出されるようではユーザがこの機能を停止してしまう可能性もあり、バランスが重要である。



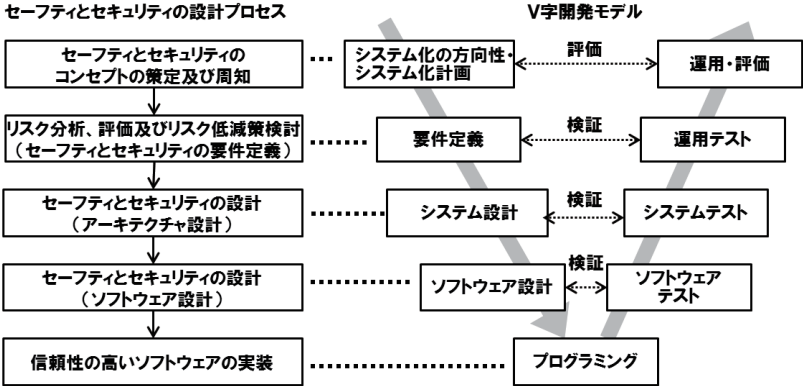
［指針12］安全安心を実現する設計の検証・評価を行う

(1) ポイント

①つながる機器やシステムは、IoT ならではのリスクも考慮して安全安心の設計の検証・評価を行う。

(2) 解説

機器やシステムにおいて、設計が実現されていることを検証・評価するスキームとしてはV字開発モデルが挙げられる。図 4-30 にセーフティとセキュリティの設計における V 字開発モデルの例を示す。



出典:つながる世界のセーフティ＆セキュリティ設計入門

図 4-30 セーフティ及びセキュリティの設計における検証・評価

IoT コンポーネントについては、単独では問題がないのに、つながることにより想定されなかったハザードや脅威が発生する可能性もある。安全安心の要件や設計が満たされているかの「検証」だけでなく、安全安心の設計がつながる世界において妥当であるかの「評価」を実施することが必要となる。

(3) 対策例

①検証・評価への反映項目例

1) 各指針の反映

本開発指針の第 3 章に記載した守るべきもの、つながり方、リスク箇所を検討した上で、1 から 17 の指針の内容を反映し、必要な事項を評価に反映する。

2) 機器やシステムの安全安心対策のレベルに応じた検証・評価

安全安心に関しては一部業界において国際規格が制定されており、その要求事項が企業内での検証・評価の項目抽出に活用可能である。また規格に基づく第三者認証により、安全安心対策のレベルの客観的評価も実施されている。

・セーフティに関する国際規格

セーフティを実現する機能に関しては、機能安全規格 IEC 61508 及びその派生規格が制定されている。IEC 61508 についてはセカンドエディションでセキュリティに関する事項も追加されている。

・コモンクライテリア（ISO/IEC 15408）

情報セキュリティの観点から情報技術に関連した機器やシステムが適切に設計され、正しく実装されていることを評価する規格で、国際協定に基づき認証された機器やシステムは加盟国においても有効と認められる。

・EDSA(Embedded Device Security Assurance)認証

制御機器を対象としたセキュリティ評価制度であり、ソフトウェア開発の各フェーズにおけるセキュリティ評価、セキュリティ機能の実装評価及び通信の堅牢性テストの 3 つの評価項目からなる。

・その他

国際規格が整備されていない分野では民間による第三者評価も有効であり、米国では ICSA Labs、NSS Labs 等のセキュリティ評価機関が通信機器等の評価を実施している。国内では一般社団法人重要生活機器連携セキュリティ協議会（CCDS）が製品分野別のセキュリティガイドラインや検証評価ガイドラインを作成している。

3) 既知のハザードや脅威への対策が取れていることの確認

IoT に関しては、今後、普及するに従って新たなハザードや脅威が発生すると想定される。運用関係者等と連携、最新の情報を把握し、評価に反映する（指針 15 参照）。

4.4 市場に出た後も守る設計を考える

つながる世界では、自動車や家電のように 10 年以上も利用される機器やシステムも多く、故障やセキュリティ機能の劣化などによる誤動作や不正操作から機器やシステムを守ることが必要となる。そのためには自分自身の状態を適切に把握し、判断したり、ソフトウェアのアップデートにより安全安心に関する機能の更新を行うことも必要となる。

そこで本節では、市場に出た後も守る設計として取り組むべき 2 つの指針を説明している。

［指針13］自身がどのような状態かを把握し、記録する機能を設ける

(1) ポイント

①自身の状態や他機器との通信状況を把握して記録する機能を検討する。
②記録を不正に消去・改ざんされないようにする機能を検討する。

(2) 解説

様々な機器やサービスがつながった状態では、どこで何が発生しているかを把握することは容易ではない。異常が発生した場合に検知し、分析して原因を明らかにし、対策を検討するためには、個々の IoT コンポーネントがそれぞれの状態や他機器との通信状態を把握するとともに、ログとして記録することが必要である。その際、ユーザの操作履歴や利用環境などのデータも自動的に収集することができれば、不用意な操作やつなぎ方に起因する脆弱性を明らかにしたり、想定外の利用方法やその頻度を把握して次の製品開発に役立てたりすることも可能となる。なお、ログにはユーザのプライバシーに関するものも含まれる場合があるため、考慮が必要である。

また、それらのデータが攻撃者等により消去・改ざんされてしまうと対策が打てなくなるため、セキュアに保管することが必要である。

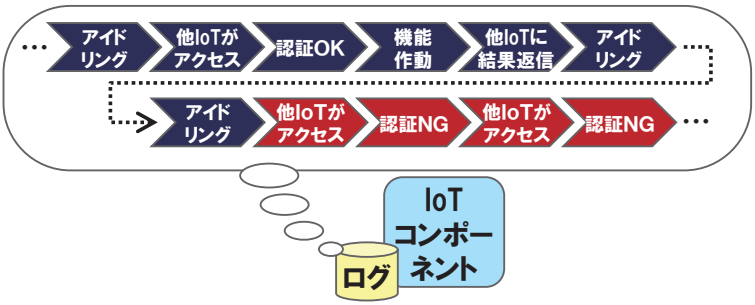


図 4-31 IoT コンポーネントにおけるログ（動作履歴）

なお、IoT コンポーネントの中にはセンサーなど低機能のものも含まれており、単独での大量のログの管理や、ログ暗号化 などの対策が難しい場合がある。そのような機器については、他にログを管理ための機能を有する IoT コンポーネントを用意して対策を行う必要がある。

(3) 対策例

①自身の状態や他機器との通信状態を把握して記録

・各 IoT コンポーネントで動作をログとして記録する。

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

・ログを保管するための資源は有限であるため、保管方針を策定する。

・関連する IoT コンポーネント間でログの記録時間が整合するように、時刻の同期を行う [32]。

・ログに記録するタイミングは機器ごとに設計するのではなくて、IoT コンポーネント全体で考慮する。

・ログの記録が IoT コンポーネントの保全のためであることをマニュアル等に記載する。

②記録の不正な消去、改ざんの防止

・IoT コンポーネントにおいて、ログに対してアクセス権限の設定、暗号化を行う方法がある。

・IoT コンポーネントにおいて収集したデータを定期的に、ログを保管する機能を有する IoT コンポーネントや専用の装置等に送信する方法がある。

・ログへの書き込みは追記のみ可能な仕組みを用意している例もある [33]。

［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

(1) ポイント

①経年で増大するリスクや変化する使い方・利用環境に対し、アップデートなどで安全安心を維持する機能を検討する。

(2) 解説

IoT の製品サービスは経年により、欠陥の発見、セキュリティ機能の劣化、新製品とつながらないといった問題が発生しうる。例えば、セキュリティに関しては、秘密鍵や乱数 SEED の推定、ソフトウェアの解析、設計情報等の流出によりリスクが高まることも考えられる。また、つながる世界では使い方や利用環境が急速に変化していくことが予想され、誤操作や危険なつなぎ方を防ぐための操作性改善や機能追加が必要と考えられる。

図 4-32 経年で増大するリスク

これらの対応を行うために、アップデートなどの機能の導入を検討する必要がある。ただし、アップデートの不具合により IoT コンポーネントの動作に異常が生じたり、アップデート処理のために IoT コンポーネントの性能が低下したり、多数の IoT コンポーネントの同時アップデートによりネットワーク帯域が不足したりするリスクがあるため、充分な考慮が必要である。

なお、アップデート以外にも、時間が経っても安全安心を維持する方法として、動的な構成変更や拡張性などを考慮した作り方がある。

(3) 対策例

①アップデートなどで安全安心を維持する機能

1) アップデートなどの機能

・IoT コンポーネントが自動／手動、直接／遠隔により操作性改善や機能追加、不具合対策、秘密鍵更新などの処理を行えるアップデート機能を搭載する。

・アップデート機能をなりすましで利用されないように、アップデートファイルの暗号化や署名を利用する方法が考えられる。

・セキュリティ対策が不十分となった機器の機能を制限する対策に利用されている例もある。

2) アップデートなどによる影響の低減

・アップデート中の性能低下やネットワーク帯域の不足により機能や安全性への影響が予測される場合にはアップデート日時設定や帯域制御を可能とする方法が考えられる。また、他の IoT コンポーネントと連携して稼動している場合等は、アップデート手順の設計を実施する方法が考えられる。

・自動アップデート後に動作しなくなった場合の自動バージョンダウン（特に自動アップデートの場合）を可能とする方法が考えられる。

・アップデート後の性能ダウンを防止するために、事前検証を確実に行うことが考えられる。

・アップデート時のウイルス混入を防止する。USB でアップデートする場合は USB のチェックを徹底する。通常ネットワークに接続していないコンポーネントはセキュリティ対策を実施されていない可能性が高いのでアップデートだけのためにネットワークに接続することは避けることが望ましい。

3) IoT コンポーネントの利用場所の把握など

・IoT コンポーネントに深刻な不具合が発見された場合、出荷からかなりの年月が経過していても迅速かつ確実に対応するために、ユーザの承諾を得た上で IoT コンポーネントの利用場所を把握したり、メッセージを表示したり、停止させる設計が考えられる。

・IoT コンポーネントが中古販売された場合を考慮し、利用場所の移動を認識すると所有者に再度、承諾を得るような設計も考えられる。

4.5 関係者と一緒に守る

つながる世界の安全安心を守るためには、機器やシステムの開発者だけでなく、関係事業者や一般利用者といった様々な関係者の協力が必要である。関係事業者とは、保守者や運用者、販売店、異なる企業や分野の機器やシステムを組み合わせてサービスを提供するインテグレータ、それらのユーザである企業利用者などである。つながる世界の安全安心を実現するためには、それらの関係者と連携して情報を把握したり、情報発信することが必要となる。

そこで本節では、関係者と一緒に守るために取り組むべき 3 つの指針を説明している。

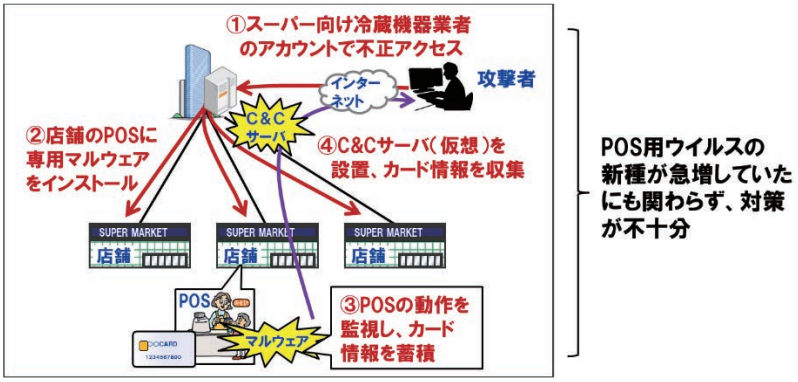
［指針15］出荷後もIoTリスクを把握し、情報発信する

(1) ポイント

①欠陥や脆弱性、事故やインシデントの最新情報を常に収集・分析する。
②必要に応じて社内や関係事業者、情報提供サイトなどへリスクの情報を発信し共有する。

(2) 解説

つながる世界では、出荷後に想定外の問題が発生する場合がある。2013 年に米国大手小売業の POS がウイルスに感染し、4 千万人のクレジット・デビッドカード情報及び 7 千万人の顧客情報が漏えいした（図 4-33）。2011 年頃から POS 用ウイルスの新種が急増していたにも関わらず、対策が不十分であった可能性がある［34］。また、2014 年の Heartbleed など、広く普及しているオープンソースソフトウェア（以下「OSS」）に重大な脆弱性が発見された例もある。特に、セキュリティ上の脅威がセーフティの機能に影響を与える場合、予期せぬ事故が発生する可能性もある。



出典：CCDS 生活機器の脅威事例集を基に作成

図 4-33 POS 端末に対する攻撃事例

開発者はこれらの問題に早急に対応するために、継続的に情報収集・分析するとともに、必要に応じて情報発信する必要がある。また、ユーザからのフィードバックは、利用状況の把握や障害の原因特定にも有用であるため、積極的

に利用時の品質向上に活用することが望ましい。なお開発者が行える情報収集やリスク対策には限度があるため、関係者の協力が必要である。

(3) 対策例

①事故やインシデントの情報収集・分析の例

・世の中で発生している事故やインシデントの情報を収集・分析する。

－入手した情報の自社製品への影響を調査

－関連する問題が自社製品に見つかったときには、つながっている外部への影響も調査

－外部への影響が想定される情報のうち、発信が必要なものを選定

上記に加え、現場と接している関係者が把握した事故やインシデントの情報を開発者にフィードバックする仕組みも重要である。

・情報収集は以下が参考になる。分析は 4.2 を参照のこと。

表 4-7 情報提供サイト等の事例

名称		概要
国内の事例	JPCERT コーディネーションセンター	国際的なセキュリティ緊急対応組織として長年にわたり、脅威に関する情報収集や対応を行ってきた中立的組織であり、IPA と共同で脆弱性情報を集約・公開している。 - 脆弱性対策情報ポータルサイト（JVN）[35] - 同 データベース（JVN iPedia）[36] 日々発見される脆弱性対策情報を蓄積することで幅広く利用されることを目的として、JVN に掲載される脆弱性対策情報のほか、国内外問わず公開された脆弱性対策情報を広く公開対象とし、データベースとして蓄積。OSS の脆弱性情報も取得可能。
	ISAC(Information Sharing and Analysis Center)	インシデント、脅威及び脆弱性に関する業界独自の情報共有、会員同士の情報交換などを行っている（コラム 4 参照）。
	IPA：情報セキュリティ 10 大脅威	有識者により各年に発生した最も重大な脅威を公表し、警戒を促している [37]。
海外の事例	Black Hat	コンピュータセキュリティの国際的なカンファレンスであり、最先端の攻撃事例や対策方法の研究事例が発表されている [38]。
	Cyber Treat Alliance	米国のセキュリティ企業が設立した組織であり、最新の情報共有を図るとともに、ホワイトペーパーなどを公表している [39]。

・OSS については個別に開発者や関係事業者などで構成される団体（OSS コミュニ

ティ）があり、バグ情報の共有や修正パッチ作成なども行われている。コミュニティの Web サイトなどで情報収集が可能である。

②つながるリスクの情報発信の例

①で収集し分析した情報はリスクとして必要に応じて発信・共有する。

- 社内で担当を決め、実施する。
- 外部へ情報発信・共有する場合は注意が必要である。

対策例として下記が考えられる。

1) CSIRT（Computer Security Incident Response Team：シーサート）

コンピュータセキュリティインシデントへの緊急対応や対策活動を行う。企業内に CSIRT を設置し、社内や顧客からの報告を受け、緊急対策を行うとともに、他社の CSIRT とともに対策の連携を図る例が見られる（コラム 4 参照）。

2) JPCERT コーディネーションセンター、ISAC への発信

①を参照。

3) 外部への情報発信・共有時の注意点

・伝える相手の選定

つながっている先やユーザなど、影響が及ぶ範囲を見極める。

・伝え方とタイミング

対策の目処がないままリスクの情報を公開することはゼロディ攻撃を受けるなど新たなリスクを発生させるので慎重に検討する。前述した ISAC も業界企業間の情報共有の場として有用である。

＜コラム4＞セキュリティの組織対策 CSIRT と ISAC

セキュリティ対策に有用な組織的対策として、緊急対応等を行う CSIRT 及び業界内でのインシデント情報共有等を図る ISAC が挙げられる。

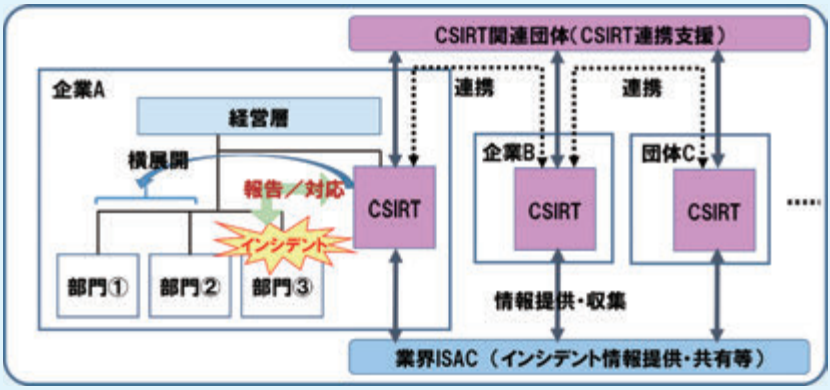
1）企業内で活躍する緊急対応チーム：CSIRT

CSIRT（Computer Security Incident Response Team：シーサート）はコンピュータセキュリティインシデントへの緊急対応や対策活動を行う組織の総称であり、インターネット上の問題の監視、インシデント対応及びその支援、分析や教育、研究開発など様々な活動を行う。近年、企業等の内部に設置し、自社や顧客への緊急対応を行う動きがある。日本シーサート協議会において企業内 CSIRT の設置のためのスタータキットを公開している［40］。

2）業界内の情報共有の場：ISAC

ISAC（Information Sharing and Analysis Center：アイザック）とは、インシデント、脅威及び脆弱性に関する業界独自の情報共有と分析・会員同士の情報交換を行う組織の総称である。日本国内では金融 ISAC［41］や ICT-ISAC［42］が設立されている。

両者のイメージを下図に示す。



CSIRT と ISAC

セーフティに関しては、企業の受付窓口や ISO 10393（消費者製品リコール－供給者のためのガイドライン）などの基準整備も進んでいる。セキュリティにおいても、CSIRT や ISAC の活用など企業連携や情報共有により、新しい脅威に対して迅速かつ効率的に対応することが期待される。

［指針16］出荷後の関係事業者に守ってもらいたいことを伝える

(1) ポイント

①導入、運用、保守、廃棄で守ってもらいたいことを直接それらの業務に関わっている担当者や外部の事業者に伝える。

(2) 解説

IoT コンポーネントは出荷後、一連の導入、運用、保守にて長期にわたって利用される。また、その後リユースされることもあるが、最後は廃棄されることになる。この間、以下のような安全安心上の問題が想定される。

・導入時
  - ファイアウォールの無い環境への設置
  - ログイン用パスワードの未設定

・運用・保守時
  - 経年によるセキュリティ機能の劣化、新たな脆弱性の発見
  - 他者が推定可能なパスワード設定やソフトウェアアップデート未実施
  - サポート期間が未通知、またはサポート期間を過ぎても継続利用
  - システムや機器に設計された復旧機能でも回復が困難な障害の発生

・リユース・廃棄時
  - 内包する個人情報・秘密情報の未消去
  - 不正改造された IoT コンポーネントの譲渡や中古販売への対応

上記の問題は、企画・設計・開発時の対策だけでは対応が難しいため、導入・運用・保守・廃棄時の関係事業者に対して対応を求める必要がある。図 4-34 に製品・サービスのライフサイクル例と本指針の対象範囲を示す。

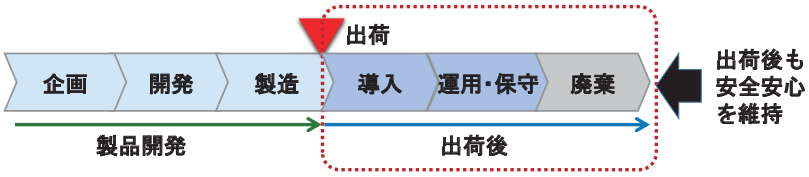


図 4-34 製品・サービスのライフサイクル例

(3) 対策例

①出荷後も安全安心を維持するために、以下の対策を検討し、直接それらの業務に関わっている担当者や外部の関係者に周知を図る。

1) 導入時の対策

・ファイアウォールの無い環境への設置に対する対応

- 外部ネットワークに接続する際の必須事項の伝達(ファイアウォール内への設置等)

・ログイン用パスワードの未設定への対応

- ID・パスワードの初期設定値から変更すべきことの伝達

2) 運用・保守時の対策

・IoT コンポーネントのセキュリティ機能の劣化や新たな脆弱性への対応

- ソフトウェアのアップデート機能の利用促進(指針14参照)

・他者が推定しにくいパスワード設定やソフトウェアアップデート未実施への対応

- 運用訓練の実施、徹底管理の依頼
- 自動アップデート機能の設定依頼

・サポート期間未通知、サポート期間超過利用への対応

- サポート期間の通知とサポート期間終了の予告及び通知
- 自社 Web ページでの掲載、機器やシステム上のメッセージ表示
- サポート期間終了後もつなげたまま利用するとリスクが高いケースでは、技術的にネットワークへの接続を制限

図 4-35 サポート期間の通知

・システムや機器に設計された復旧機能でも回復が困難な障害への対応

- ソフトウェアや暗号鍵などの管理システムからの再構成の検討依頼
- システム的な復旧が不可能な場合の手作業による復旧手順の検討依頼
- 予備の機器・部品やシステムの調達方法と配備の検討依頼

3) リユース・廃棄時の対策

・内包する個人情報・秘密情報への対応

- 個人情報・秘密情報が IoT コンポーネント内に存在することの周知徹底
- 未消去に関するリスクの解説
- データを消去する機能の搭載（指針 8 参照）

・不正改造された IoT コンポーネントの譲渡や中古販売への対応

–ソフトウェア、設定、マニュアルなどの改ざんなどのリスクの中古販売会社やユーザへの周知

–改ざんの有無の確認方法やクリーニングツールの販売会社やユーザへの提供

- 中古販売会社による上記ツールを用いたクリーニング実施保証　など

［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

(1) ポイント

①不用意なつなぎ方や不正な使い方をすると、自分だけでなく、他人に被害を与えたり、環境に悪影響を与えたりするリスクがあることを一般利用者に伝える。
②安全安心を維持していくために一般利用者に守ってもらいたいことを伝える。

(2) 解説

一般利用者が家電に非正規のアダプターを取り付けたり、赤外線リモコンを改造することにより、家電の遠隔操作を行う例が見られる。そのようなつなぎ方をすると、不正に遠隔操作されたり、異常動作するなどのリスクが高まる。

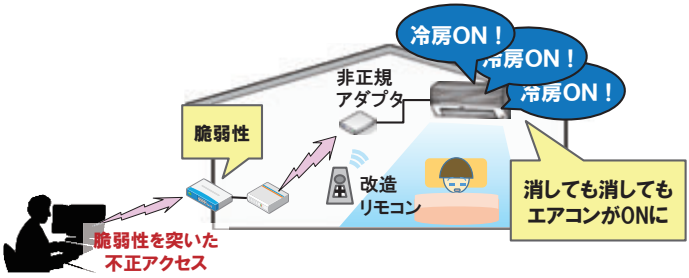


図 4-36　一般利用者の不正改造によるリスク例

また、各種リスク対策を行い許容できる範囲までリスクを低減したとしても一般利用者に影響を与えるリスクが潜在していたり、出荷時には想定できなかったが経年で増大するリスクもありうる（指針 14 参照）ので、それらを一般利用者に伝える必要がある。

つながる世界は便利ではあるがリスクもあることを一般利用者に周知し、機器やシステムを不用意につなげないことを伝えるとともに、IoT コンポーネントの不具合・脆弱性対策の必要性を理解、協力いただくことが必要である。例えばスマートフォンの脆弱性はソフトウェアのアップデートで対応することが多いため、一般利用者に実施を促す必要がある。

一般利用者への周知状況を把握、分析し、周知方法の改善を図る。

(3) 対策例

①不用意なつなぎ方によるリスク周知の例

1)伝え方

- オープニングの操作画面での表示
- マニュアルへの例示記載（開発者、運用者から一般利用者への周知）
- 保証書への記載
- 自社 Web サイトでの掲載（IPA の掲載例 [43]）

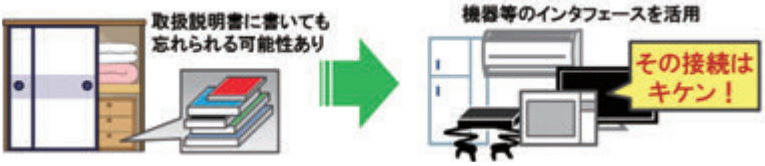


図 4-37 機器やシステムのユーザインタフェースを活用した警告

2)伝える内容例

- 推奨する（動作保証がされている）つなぎ方など

②一般利用者に実施していただきたいことの周知の例

一般利用者に協力いただきたいこと、注意いただきたいことを伝える。また、一般利用者への周知状況を把握、分析し、周知方法の改善に向け PDCA サイクルを回す。

1)伝え方- オープニングの操作画面での表示

- マニュアルへの例示記載（開発者、運用者から一般利用者への周知）
- 自社 Web サイトでの掲載 など

2)伝える内容例

- アップデート実施の推奨
- 自動アップデート機能がある場合は出荷時にデフォルトが ON となっていること
- 無線 LAN（Wi-Fi など）のセキュリティキーなどのセキュリティの設定
- 他者が推定しにくいパスワード設定の推奨
- リユース・廃棄時の個人情報や秘密情報の流出対策として、データを消去する機能の周知（指針 8 参照）

第5章
今後必要となる対策技術例

第 4 章の開発指針の対策例については、現時点で技術的に確立できているものを中心に記載している。しかしながら、つながる世界の安全安心を確保するためには、さらに高度な研究が必要となる。本章では現時点では技術的に確立されていないが、今後必要になることが想定される対策技術の例について記載する。

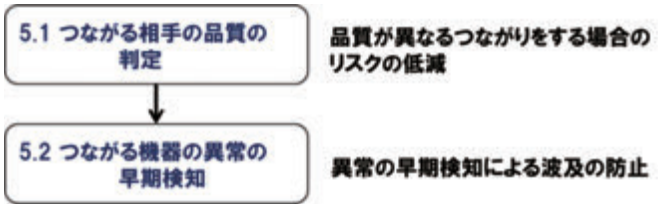


図 5-1 本章の流れ

5.1 つながる相手の品質の判定

つながる世界では、出荷した IoT コンポーネントやサービスを開始したシステムがサービス事業者やユーザによって手を加えられ、メーカが想定しない使い方やつなぎ方になる可能性がある。また、異なる分野の IoT コンポーネントがつながるようになると、それぞれ品質に関する考え方やルールが異なるために想定していた品質を維持できなくなるリスクがある。さらに、このような状況であるにもかかわらず、ユーザがリスクに気づかないまま利用してしまうことも懸念される。

本章では、異なる相手とつながる場合のリスクを低減するために、以下の手順により情報群を整理・交換し、相手の品質を確認する対策を提案する。

1. つながる相手の品質を確認するための情報群の整理
2. 接続時の情報群の交換・判断、結果の通知

なお、つながる相手と情報交換を行うためには、相手の認証やセキュアな通信手段の確保が必要であるが、ここでは「実現されている」という前提で考える。

(1) 品質確認のための情報群の整理

- セーフティ、セキュリティ、リライアビリティに関する情報について交換・確認できる必要がある。以下に情報群として活用可能な情報例を記載する。
  - ・セキュリティレベル（EAL、SAL（EDSA）等）
  - ・機能安全のレベル（SIL、ASIL、PL 等）
  - ・業界内の認定機関による情報
  - ・稼働率・回復力
  - ・企業の体制（関連規格認証取得等）、品質保証の情報
- 情報群を交換する範囲としては、同じ企業内、特定の分野内、さらには異分野間でも交換できるものとする。ただし、異分野間の場合には、汎用的な共通交換情報を定めることは困難であるため、接続する製品やサービス間でどのような情報を交換するかをあらかじめ議論して定める必要がある。

図 5-2 情報群のイメージ

(2) 情報群の交換・判断、結果の通知

- IoT コンポーネントを接続するための情報群の交換及び品質の確認方法としては、以下の２つが挙げられる。

・静的な情報交換：オフラインで情報群を確認（装置や部品選定時）

- 市場に出ている IoT コンポーネントについて、人手により情報群による品質の確認、接続の可否やサービスの提供範囲の決定、及び結果一覧のサーバへの保存を行う。
- IoT コンポーネントが他と接続する際、サーバ上の結果一覧を参照し、相手との接続の可否やサービスの提供範囲を確認する。

・動的な情報交換：オンラインで情報群を確認（接続時）

- IoT コンポーネントに自分の情報群を保存し、他の IoT コンポーネントと接続する際に情報群を交換、相手の品質を確認し、自律的に接続可否やサービスの提供範囲の判断を行う。

いずれも場合も、相手に判断結果を通知するとともに、交換した情報群や判断結果を記録する。本件の例については付録 A3 参照。

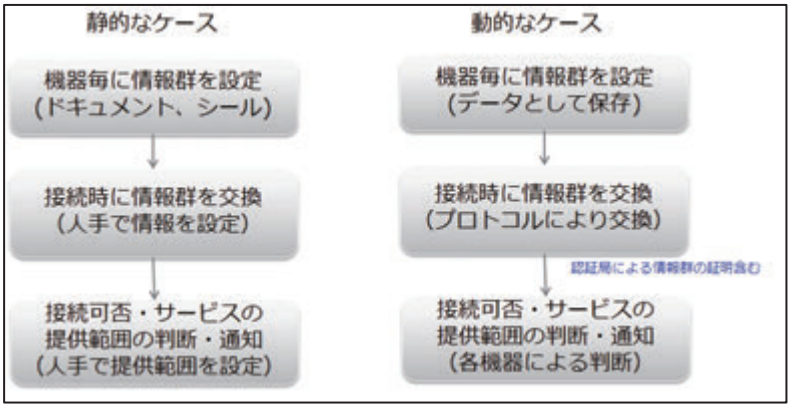


図 5-3 静的・動的な情報交換・判断

5.2 つながる機器の異常の検知

つながる相手に迷惑をかけないためには、それぞれの IoT コンポーネントが守るべきものを守る（被害者とならない工夫）とともに、IoT コンポーネントの異常の波及を防止すること（加害者とならない工夫）が必要となる。具体的には、IoT コンポーネントが暴走して異常な通信を続けることでネットワークの負荷が上がったり、マルウェアに感染して他の IoT コンポーネントにも伝播してしまうような状態を早期に発見し、対応する仕組みが重要である。

つながる世界では、小さな異常が波及・蓄積することで全体として大きな影響が発生する可能性がある。しかし、個々の IoT コンポーネントに内包された小さい異常は見逃されやすい。また、工場のラインのようにしばしば大規模な組み替えが発生するケースでは異常判定基準の策定に手間がかかる。

そこでここでは、正常な動作を記録することで自動的に異常判定基準を策定し、実際の動作と比較することで異常検知を行う手法を想定した。

(1) 正常な動作の記録

- あらかじめ静的に記録をとる方法と、動的に記録する方法がある。静的な記録としては人手により正常な動作を記録する方法が、動的な記録としては通常の動作を記録し続け、機械学習等により正常な状態を認識する方法が考えられる。
- 動作を記録する範囲として、単体の IoT コンポーネントの動作を記録する方法と、複数の IoT コンポーネントの動作の記録をとる方法がある。

(2) 正常な動作との比較

- 異常の検知
  - ・正常な動作との値の範囲の比較により異常を検知する。IoT コンポーネント単体の場合は、その動作が正常の範囲内かどうかをチェックし、複数の IoT コンポーネントの場合には、相互の関係として異常かどうかまでチェックを行う。
- 予兆の検知
  - ・異常ではないが、近い将来に異常となることが見込まれる場合には、正常な範囲内でも検知して対応することで、より効果的に異常の波及を防止することが可能となる。

・ 予兆の検知には、機械学習等を活用して状態の変化を検知する方法がある。例えば、周期的な状態の傾向の変化や、状態の推移の傾向の変化、または相関関係の高い複数の IoT コンポーネントの状態の関係の変化をチェックする方法等が考えられる。

異常の検知の例については付録 A4 参照。

おわりに

つながる世界においては、家電や自動車などあらゆる「モノ」がネットワークにつながることにより、消費者のみならず開発者すら想定しないリスクが発生すると懸念される。しかも機器やシステムのリスクには、つながりを介して広範囲に波及したり、人命や財産に危害を与えるものもあり、早急な対応が必要である。そこで、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、機器やシステムに関わる企業が安全安心に関して最低限考慮すべき事項を指針としてとりまとめることとした。

IoT 自体が発展途上である状況においてこのような指針を策定することは困難が予想されたが、IoT を構成する機器やシステム（IoT コンポーネント）の安全安心に焦点を絞るとともに、有識者による WG において長時間にわたる審議をいただくことにより、本開発指針としてとりまとめることができた。機器やシステムの開発者の方々がつながる世界のリスク対応に取り組んでいただく際に、本開発指針が一助となることを期待する。

なお、開発指針については、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。引き続き、開発指針の更新状況に注意を払っていただきたい。

最後に本開発指針の策定に対して、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.

A1. 本開発指針の活用方法（チェックリスト）

本書では、様々な業種がつながり新しいサービスやビジネスが創生されるIoT時代に向けて、業界内及び業界間を安全安心につなぐために最低限、考慮すべき共通事項を開発指針・ポイントとしてまとめた。以下に、この開発指針を有効かつ効果的に使っていただくためのチェックリストの例を示す。

表 A-1 開発指針チェックリストの例

対象製品名称： **記入者部署・氏名：**

	指針	ポイント	チェックポイント	…
記載例	［指針1］安全安心の基本方針を策定する	①経営者は、つながる世界の安全安心の基本方針を企業として策定し、社内に周知するとともに、継続的に実現状況を把握し、見直していく。	1)つながる世界のセーフティに係る基本方針は策定／周知／実現状況把握／見直しされているか	…
			2)つながる世界のセキュリティに係る基本方針は策定／周知／実現状況把握／見直しされているか	…
方針	［指針1］安全安心の基本方針を策定する	①経営者は、つながる世界の安全安心の基本方針を企業として策定し、社内に周知するとともに、継続的に実現状況を把握し、見直していく。	1)つながる世界の**セーフティ**に係る基本方針は策定／周知／実現状況把握／見直しされているか	
			2)つながる世界の**セキュリティ**に係る基本方針は策定／周知／実現状況把握／見直しされているか	
	［指針2］安全安心のための体制・人材を見直す	①つながる世界における安全安心上の問題を統合的に検討できる体制や環境を整える。	1)問題の検討や対策のための**体制**は整えられているか	
			2)問題への対策を検証・評価するための**環境**は整えられているか	
		②そのための人材（開発担当者や保守担当者など）を確保・育成する。	3)**人材の確保**を行っているか	
			4)**人材の育成**を行っているか	
	［指針3］内部不正やミスに備える	①つながる世界の安全安心を脅かす内部不正の潜在可能性を認識し、対策を検討する。	1)社員が**内部不正**に走る要因を把握しているか	
			2)内部不正の**抑制や対策**を検討しているか	
		②関係者のミスを防ぐとともに、ミスがあっても安全安心を守る対策を検討する。	3)関係者の**ミスを防ぐ**対策を検討しているか	
			4)**ミスがあっても**安全安心を**守る**対策を検討しているか	

A2. 開発指針の導出手順

開発指針の策定においては、第 3 章で整理したつながりのパターンを横軸、IoT のリスク例を縦軸にとり、リスク分析を行った。ただし、各パターンの組み合わせを網羅するためには膨大なリスク例が必要となるため、各パターンの要素がいずれかのリスク例に含まれるようにリスク例を導出した。なお、IoT の事例は多くなく、リスク例も少ない。そこで、既存の IoT のリスク事例では不足していたため、一部のリスク例は想定したものとなっている。整理のイメージを図 A-1 に示す。

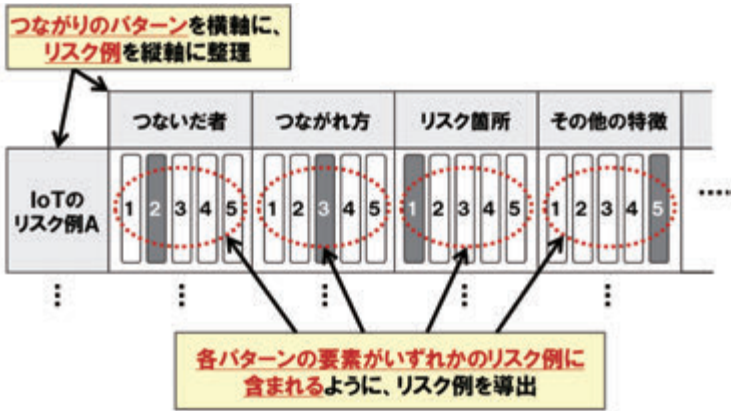


図 A-1　つながりのパターンと IoT のリスク例の整理

次に、各リスク例が発生した原因を分析し、IoT に着目した課題／問題を整理した。結果を表 A-2 に示す。

「IoT に着目した課題／問題」としては、「ファイアウォールに守られたクローズドな環境への設置を想定していた」という問題や「意図しないつながりにおいても、安全安心を維持する必要がある」という課題など、様々なモノに「つながる」という IoT の特性に起因したものを挙げている。また、保守用 USB 端子からの攻撃、内部関係者による犯行、アップデート機能の不正利用など、セキュリティ技術者でなければ想定しにくい課題も多い。セキュリティ上の脅威がセーフティ上のハザードにつながる事例もあり、安全安心としての対応の必要性も明らかになっている。

表 A–2 IoTリスクの分析表

WHAT 何が起きたか		WHO 誰がつなげたか						HOW どのようにつなげたか					WHOM 何が危害を受けたか					WHERE どこで発生したか					WHEN どの段階で発生したか					WHY なぜ発生したか	
機器種別	リスク例	メーカーや関連企業	サービス事業者	ユーザ（意図的）	ユーザ（誤接続）	攻撃者	偶発的	直接的	間接的	固定的	動的	複合的	IoT機能	本来機能	データ	身体や財産	その他	通常使用I／F	メンテナンス用I／F	非正規I／F	内包	物理的接触	企画・設計・開発	製造・出荷	運用（供給側）	運用（ユーザ側）	廃棄・リサイクル	主要な原因	IoTに着目した課題/問題
プリンター複合機	インターネットに接続することを想定していないプリンター複合機の蓄積データが公開状態に。初期パスワードも文書で公開。	○								○					○				○							○		インターネット接続の想定不足 初期パスワードの変更依頼不足 初期パスワードを記載した文書の公開	ファイアウォールに守られた環境への設置を想定していた。
ATM	物理鍵を不正に入手しATMの保守用扉を開けてウイルスを感染させるとともに、さらに電話機等を取り付け、その電話機等にメールを送ることで現金引き出した。					○		○			○					○（現金）			○			○				○		攻撃事例の把握、共有不足 保守用扉のアクセス管理不足 保守用インタフェースの開放 ATM端末のウイルス感染	攻撃者に保守用扉を開けられたり、保守用USB端子に電話機等をつなげられるリスクの想定が不十分であった。
IoT全般	（想定事例）IoT同士がつながるうちに、想定されたないIoTまでつながり、情報が漏えいした。						○								○			○						○				個々のIoTの管理不足 つながりの全体像を把握する機能なし	意図しないつながりにおいても、安全安心を維持する必要がある。
IoT機器	（想定事例）拾ったIoT機器をいじっていたら遠隔機能が動作し、ユーザの財産に損害を与えた。				○						○			○		○		○							○			ユーザ認証機能の不足 不自然な操作に対する確認の不足	拾得者などによる意図しない利用に対しても、安全安心を考える必要がある。
自動車	ローンが滞ったユーザの自動車を遠隔からロックしたり、ホーンをならすサービスが元従業員に不正利用。		○							○				○				○							○			アカウントの管理不足 異常な利用を防ぐ仕組みの不足	内部犯行を想定していなかった。
車載器	モバイル網経由で車載器にアクセス、チップのファームウェアを書き換え、車載ネットワークに制御命令を送信、自動車のハンドルやブレーキを遠隔制御。	○				○			○		○			○					○	○					○			モバイル網のアクセス管理不足 スマホ－車載器間通信の非保護 車載器権限の認証なし アップデートファイルの暗号化なし 自動車制御系へのアクセス管理不足	・守るべきものが守られていなかった。 ・セキュリティの問題がセーフティに与える影響の想定が不十分であった。 ・遠隔アップデート機能のセキュリティが不十分であった。
IoT機器	工場の検査時にウイルス感染、出荷され、IoT接続された際に感染が広がった。			○				○									○（製品）				○			○					工場でのセキュリティ検査不足 ウイルスチェック機能なし 異常時の自律制御機能なし	つながる相手に影響を与えないという配慮が不足していた。
IoT機器	（想定事例）廃棄・リサイクルされた機器をつなげたら、前の所有者のIoT設定が残っていてサーバにつながってしまった。				○					○	○						○	○									○	廃棄・リサイクル時の設定消去なし	廃棄・リサイクル時の対策を検討する必要がある。
IoT全般	（想定事例）災害時に、災害対策用のIoTが一斉に立ち上がり、無線が輻輳、IoTが使用できなくなった。						○				○	○	○	○				○							○			社会全体としてのIoTの把握不足	周囲及び自己の現在の状態を把握し、対応する必要がある。
POS	センターサーバに不正アクセス、POS端末にウイルスを感染させ、顧客の決済情報を不正に収集。		○			○			○	○					○			○							○			攻撃事例の把握、共有不足 センターサーバのアクセス管理不足 POS端末のウイルス感染	自社に関連する機器への攻撃が増大していたのに、対策していなかった。
家電	（想定事例）ユーザが家庭用の家電操作機器の通信を中継・延長し、遠隔から家電を操作したところ家族が事故にあった。			○						○						○		○								○		ユーザのリスク認識不足	ユーザにつながる世界のリスクを認知させる必要がある。

以上の分析を元に「対策の方向性」を導出した。ここでいう「対策の方向性」とは、実際の被害事例や想定事例の原因を基に IoT に着目した課題／問題を導出し、それらに対応するための方向性を整理したものである。本プロセスのイメージを図 A-2 に示す。

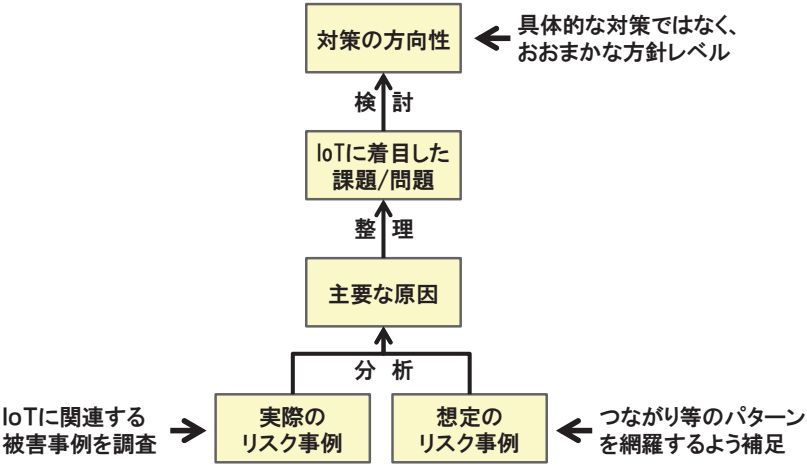


図 A-2 「対策の方向性」の導出プロセスのイメージ

上図のとおり、「対策の方向性」の導出はボトムアップ的なアプローチである。結果を表 A-3 に示す。

表 A-3 IoT に着目した課題から対策の方向性の導出

WHAT		WHY	
何が起きたか		なぜ発生したか	
機器種別	リスク例	主要な原因	IoTに着目した課題/問題
プリンター複合機	インターネットに接続することを想定していないプリンター複合機の蓄積データが公開状態に。初期パスワードも文書で公開。	インターネット接続の想定不足	ファイアウォールに守られたクローズドな環境への設置を想定していた。
		初期パスワードの変更依頼不足	
		初期パスワードを記載した文書の公開	
ATM	物理鍵を不正に入手しATMの保守用扉を開けてウイルスを感染させるとともに、さらに電話機等を取り付け、その電話機等にメールを送ることで現金引き出した。	攻撃事例の把握、共有不足	攻撃者に保守用扉を開けられたり、保守用USB端子に電話機等をつなげられるリスクの想定が不十分であった。
		保守用扉のアクセス管理不足	
		保守用インタフェースの開放	
		ATM端末のウイルス感染	
IoT全般	(想定事例)IoT同士がつながるうちに、想定されたないIoTまでつながり、情報が漏えいした。	個々のIoTの管理不足	意図しないつながりにおいても、安全安心を維持する必要がある。
		つながりの全体像を把握する機能なし	
IoT機器	(想定事例)拾ったIoT機器をいじっていたら遠隔機能が動作し、ユーザの財産に損害を与えた。	ユーザ認証機能の不足	拾得者などによる意図しない利用に対しても、安全安心を考える必要がある。
		不自然な操作に対する確認の不足	
自動車	ローンが滞ったユーザの自動車を遠隔からロックしたり、ホーンをならすサービスが元従業員に不正利用。	アカウントの管理不足	内部犯行を想定していなかった。
		異常な利用を防ぐ仕組みの不足	
車載器	モバイル網経由で車載器にアクセス、チップのファームウェアを書き換え、車載ネットワークに制御命令を送信、自動車のハンドルやブレーキを遠隔制御。	モバイル網のアクセス管理不足	・守るべきものが守られていなかった。 ・セキュリティの問題がセーフティに与える影響の想定が不十分であった。 ・遠隔アップデート機能のセキュリティが不十分であった。
		スマホー車載器間通信の非保護	
		車載器権限の認証なし	
		アップデートファイルの暗号化なし	
		自動車制御系へのアクセス管理不足	
IoT機器	工場の検査時にウイルス感染、出荷され、IoT接続された際に感染が広がった。	工場でのセキュリティ検査不足	つながる相手に影響を与えないという配慮が不足していた。
		ウイルスチェック機能なし	
		異常時の自律制御機能なし	
IoT機器	(想定事例)廃棄・リサイクルされた機器をつなげたら、前の所有者のIoT設定が残っていてサーバにつながってしまった。	廃棄・リサイクル時の設定消去なし	廃棄・リサイクル時の対策を検討する必要がある。
IoT全般	(想定事例)災害時に、災害対策用のIoTが一斉に立ち上がり、無線が輻輳、IoTが使用できなくなった。	社会全体としてのIoTの 把握不足	周囲及び自己の現在の状態を把握し、対応する必要がある。
POS	センターサーバに不正アクセス、POS端末にウイルスを感染させ、顧客の決済情報を不正に収集。	攻撃事例の把握、共有不足	自社に関連する機器への攻撃が増大していたのに、対策していなかった。
		センターサーバのアクセス管理不足	
		POS端末のウイルス感染	
家電	(想定事例)ユーザが家庭用の家電操作機器の通信を中継・延長し、遠隔から家電を操作したところ家族が事故にあった。	ユーザのリスク認識不足	ユーザにつながる世界のリスクを認知させる必要がある。

対象読者 / 対策の方向性	対策されるべき課題		
	経営者	開発者	保守者
つながりによるリスクを想定する	基本方針が策定されていない。	リスクが想定されていない。	
物理的なリスクを認識する		リスクが想定されていない。	
知らない相手でも安全安心につなげられる設計をする		意図しない使われ方やつながりを考慮できていない。	
内部不正や情報漏えいに備える	社員のモラルや訓練、リスク想定が不足している。		
安全安心の設計の整合性を確認する		双方の技術者が連携できていない。	
個々でも全体でも守れる設計をする		IoTとしての守るべきものと守り方が明確でない。	
時間が経っても安全安心を維持する		アップデート機能の安全性が不足している。	アップデート機能の不正利用を防げない。
つながる相手に迷惑かけない設計をする		自身の問題の他への波及を止められない。	自身の問題の他への波及を止められない。
廃棄・リサイクル時の機密漏えいに備える		廃棄・リサイクル時の機密漏えい対策が不十分。	廃棄・リサイクル時の機密漏えい対策が不十分。
自身がどのような状態かを把握・記録する	緊急対応体制が整備できていない。	自身の問題を検知できない。	自身の問題を検知できない。
最新のIoTリスクを把握・情報共有する			最新のリスクを把握できていない。
ユーザにつながることによるリスクを知ってもらう			ユーザがつなげるリスクを防げない。

A3. つながる相手の品質判定の例

第 5 章で示した今後必要となる品質判定の例を示す。

(1) 車載システムにおける信用保証レベルを利用した動的な品質判定

車載システムの信用保証レベルとして、C2C-CC で提案された TAL がある。車々間の通信において、証明書を用いて送信されたメッセージの正当性の検証を行っても元々のデータの信用は保証されているわけではない。発信者の情報をどれだけ信用して良いかを示す指標として TAL を定義し、自動車がどのレベルのセキュリティ基準を満たしているかを、その開発時に認証しておくものである。TAL では 0〜4 のレベルが設定されており、その信頼性レベルを認証局に保証してもらうことで、車々間通信における送信元の保証にむけて検討されている［44］。

Trust Ass. Level (TAL)	Requirements			Implications		
	Minimum Target of Evaluation (TOE)	Minimum Evaluation Assurance Level (EAL)	Minimum (Hardware) Security Functionality	Prevented (Internal) Attacker acc. to CC	Potential Security Implications	C2X Use Case Examples
0	None	None	None	None	Not reliable against security attacks in general	Some limited e.g. using trusted C2I infrastructures
1	+ ITS Station software	EAL 3	Only software security mechanisms	Basic	Not reliable against simple hardware attacks (e.g., offline flash manipulation)	Non-safety, but most privacy relevant use cases
2	+ ITS Station hardware	EAL 4	+ dedicated hardware security, i.e., secure memory & processing)	Enhanced Basic	Not reliable against more sophisticated hardware attacks (e.g., side-channel attacks)	C2C-CC day one use cases (e.g., passive warnings and helpers)
3	+ private network of ECUs	EAL 4+ (AVA_VAN.4 vulnerability resistance)	+ basic tamper resistance	Moderate	C2X box secure as stand alone device, but without trustworthy invehicle inputs	Safety relevant relying not only on V2X inputs
4	+ relevant in-vehicle sensors and ECUs	EAL 4+ (AVA_VAN.5 vulnerability resistance)	+ moderate – high tamper resistance	Moderate–High	C2X box is trustworthy also regarding all relevant in-vehicle inputs	All

Minimum Level

出典：S. Goetz and H. Seudié: “Operational Security”, C2C-CC 2012

図 A-3　C2C-CC にて議論中の Trusted Assurance Level

(2) FA 分野における認証情報を利用した動的な品質判定

１つの分野内での品質判定の例として、産業用ロボット（以下「ロボット」）を使い、認定情報を利用して動的な判定を IPA/SEC にて実施した例がある。本件の例では、認定情報を有しているロボットとそうでないものの混在を考慮した判定方法を採用している。

1)品質の不明確な機器を利用することによるリスク

ロボットが使われる環境においても、システム内の接続機器のマルチベンダー化が進んでおり、発注したシステムの中に品質の低い機器が接続されている可能性がある。この品質の低い機器がシステムに影響を与えて安全性のリスクが大きくなる可能性が予想され、品質の低いロボットを接続しないための対処を行った。

2)品質の不明確な機器による安全性のリスクの回避

ロボットの品質を認定してその認定情報を発行する公の機関を想定する。ロボットはその機関から発行された認定情報を情報群として内部に埋め込んでおき接続時に動的な判断を実施するようにした。このとき、実際にはロボットの中には、上記対応される新バージョンと、対応されない旧バージョンが存在する。そこで以下の対応を実施した。

・旧バージョン

入力データであるロボット固有情報の中のロボット識別情報のリザーブ域に手動で認定情報をいれておく。

・新バージョン

ロボットのファーム更新機能によりロボット識別情報のリザーブ域に認定情報をいれておく。ロボットを制御する統合アプリケーションではロボットとのコネクションを開設するとき、ロボットが新バージョンのときはロボットの認定情報の有無をチェックし、認定情報がなかった場合はエラーをログに出力してロボットを動作させず、システム全体としては停止するようにする。

この実施例では、旧バージョンのロボットを使用し、手動で設定された認証情報を確認した。

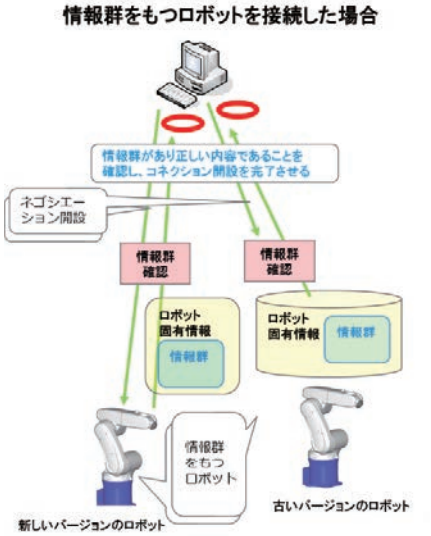


図 A-4　品質に関する情報群を用いたロボットの接続の判定

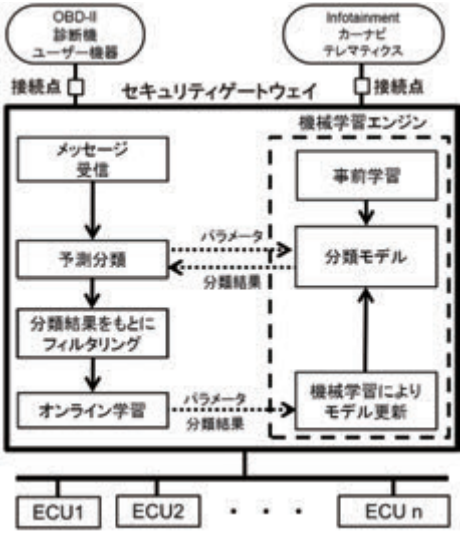
A4. つながる機器の異常検知の例

第 5 章で示した今後必要となるつながる機器の異常検知の例を示す。

(1) 車載 LAN のセキュリティゲートウェイにおける機械学習を用いた動的ルール生成による異常検知

車載 LAN については、カーナビやテレマティクス端末などの車載器を経由して外部から侵入したり、不正な機器をつなげる攻撃の研究事例が散見される。近年、車載 LAN 上のゲートウェイに認証機能を持たせる動きもあるが、長期利用される自動車においてセキュリティ機能を保守することは容易ではない。

本研究事例は，車載 LAN 上のゲートウェイ上に機械学習を用いた動的なルールによるフィルタリング機能を設置し、外部からの攻撃を検知するものである。具体的には、車載 LAN 上の正常なトラフィック（メッセージ群）から初期ルールを、攻撃メッセージを加えたトラフィックから攻撃を検出するルールを生成する。さらに、機械学習アルゴリズムにより動的にルールを更新することで、攻撃メッセージの検出率及び誤検知率を改善するものである。



出典：広島市立大学 伊達友裕，CCDS 井上博之「車載 LAN のセキュリティゲートウェイにおける機械学習を用いた動的ルール生成」, SCIS2016

図 A–5　セキュリティゲートウェイの動作

本研究により、攻撃のパターンが変化しても機械学習で動的にルールを更新することにより攻撃を検知することが期待される。また、攻撃の検知を強化す

ると正常なメッセージまで誤検知する可能性が高まるという課題については、他の対策においても参考となる。

(2) FA 分野における定型的な動作パターンとの比較による異常検知

IPA/SEC にて、産業用ロボットにおいて異常状態を検知し、異常動作を抑止する実証実験を行った例がある。

ロボットとセルコントロール用 PC との間でやりとり可能なデータは年々多様化並びに複雑化しており、ネットワークを経由してシステムや他の機器とより柔軟に接続することが可能となっている。しかしその反面、運用上のミスやアプリケーションの不具合等により誤ったデータが発生するリスクが高まっている。実証実験では、ロボットの正常動作のパターンを記憶しておき、実動作が正常動作のパターンを逸脱する場合を異常状態として捉え、異常状態を検知したときはロボットを停止させる、といった対策を実施し、比較的容易な方法で異常検知と異常動作抑止の仕組みを実現している。

1)ロボット制御アプリの異常状態の検知

セルコントロール PC からロボットを制御するケースにおいて、セルコンの不具合（人的運用ミス、ウイルスなど）により、セルコンからロボットに従来のシーケンスにはない誤ったティーチングポイント（座標データ）への移動指令が行われた場合やセルコントロール以外のアプリケーションの不具合などにより、ロボットのティーチングポイントの内容が書き換えられた場合、重大な問題が引き起こされる可能性がある。

そこで、ロボット制御アプリから出力されるロボットのティーチングポイントを監視して、万が一ロボットに想定外の動作をさせるような指示が出された場合はそれを早期に検知し、必要に応じてロボットの制御を止めることにより、重大な問題の発生を防ぐ対策を実施した。

2)ロボットの異常状態検知のための対策

動作異常検知を行う場合、次の3つ状態を監視する方法が考えられる。

- ロボットのティーチングポイント
- ロボットの状態遷移
- 複数のロボット間の制御の時間軸のタイミング

本実施例では、ロボット制御アプリから出されるティーチングポイントを監視し、正常時の値と異なった値が検知されたときは異常な値と認識し、ロボットの動作を停止させる対処を行っている。

①前準備で、ロボットが正常に動作しているときの一連のティーチングポイントのデータを採取し、それらを正常値としてティーチングポイントの比較用ログファイルに出力しておく。

②システムが動作している状況において、ロボットに指示されたティーチングポイントを適切な時間幅で監視し、①で採取した比較用ログファイルの正常な値と比較する。また、監視したティーチングポイントを動作ログとして表示・格納し、異常と判断されたときのティーチングポイントの値を示せるようにしておく。

③異常が発生する。

④監視中のティーチングポイントが比較用ログファイルの中の正常な値に含まれていないことを確認して異常と判断し、ロボットを含むシステム全体を停止させる。同時に異常検知をコンソール画面で表示する。

⑤ロボットを正しく動作するように回復させる。

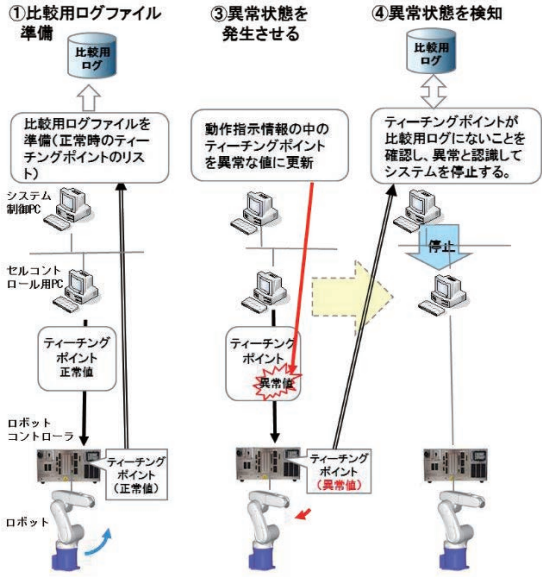


図 A-6　ロボットの動作パターンの比較による異常検知

A5.「つながる世界の利用時の品質」視点一覧

つながる世界の開発指針の改訂（第 2 版）にあたって参考とした「つながる世界の利用時の品質」報告書［2］で挙げられた視点一覧を表 A-4 に示します。

表 A-4 視点一覧

区分	視点	
組織文化	視点 1	つながる世界の利用時の品質を意識する
	視点 2	他部門と連携して取り組む文化を作る
	視点 3	自社や顧客の責任者の意識を変える
	視点 4	利用時の品質向上に関わる人材を育成する
把握・分析	視点 5	ユーザの特性や経験、文化、利用環境を考慮する
	視点 6	ユーザ経験を収集・分析・評価する
	視点 7	間接・受動的ユーザやプライバシーにも配慮する
	視点 8	利用状況や利用環境の変化の影響を考慮する
設計	視点 9	企画・設計段階からユーザを巻き込む
	視点10	ユーザを安全な操作に導く設計をする
	視点11	第三者に機能や情報を使わせない設計をする
	視点12	操作結果やメッセージを確実に伝える設計をする
保守・運用	視点13	ユーザや関係者からフィードバックを得る仕組みを作る
	視点14	知見を開発時及び出荷後の利用時の品質向上に活用する
	視点15	つながるリスクの周知と安全設定の仕組みを作る

付録B. 参考文献

[1] IPA, “「利用時品質検討ワーキング・グループ」を発足,”
https://www.ipa.go.jp/sec/info/20160927.html.

[2] IPA, “「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～」を公開,” http://www.ipa.go.jp/sec/reports/20170330.html.

[3] K. Ashton, “That ’Internet of Things’ Thing,”
http://www.rfidjournal.com/articles/view?4986.

[4] 内閣サイバーセキュリティセンター（NISC）, “重要インフラ一覧表,”
http://www.nisc.go.jp/active/infra/pdf/cc_ceptoar.pdf.

[5] 総合電機メーカー, “液晶テレビ受信不具合について,”
http://www.mitsubishielectric.co.jp/oshirase/20150409/.

[6] ITMedia, “原因は「二重の人為的ミス」 ,”
http://www.itmedia.co.jp/news/articles/0504/24/news008.html.

[7] 経済産業省／IPA, “サイバーセキュリティ経営ガイドライン,”
http://www.meti.go.jp/press/2015/12/20151228002/20151228002.html.

[8] 経済産業省, “製品安全に関する事業者ハンドブック,”
http://www.meti.go.jp/product_safety/producer/jigyouhandbook.html.

[9] IPA, “つながる世界のセーフティ&セキュリティ設計入門,”
https://www.ipa.go.jp/sec/reports/20151007.html.

[10] IPA, “情報セキュリティスキル強化についての取り組み,”
http://www.ipa.go.jp/jinzai/hrd/security/index.html.

[11] 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/security/iot/iotguide.html.

[12] IPA, “組込みシステムのセキュリティへの取組みガイド（2010年度改訂版）,”
https://www.ipa.go.jp/security/fy22/reports/emb_app2010.

[13] IPA, “自動車の情報セキュリティへの取組みガイド 第2版,”
http://www.ipa.go.jp/security/iot/emb_car2.html.

[14] IPA, “情報処理技術者試験 試験区分一覧,”
https://www.jitec.ipa.go.jp/1_11seido/seido_gaiyo.html.

[15] IPA, “国家資格「情報処理安全確保支援士」,” http://www.ipa.go.jp/siensi/.

[16] WIRED, “Hacker Disables More Than 100 Cars Remotely,”
http://www.wired.com/2010/03/hacker-bricks-cars/.

[17] ITmedia, “ATMを狙うマルウェア、携帯メールで現金引き出す,”
http://www.itmedia.co.jp/enterprise/articles/1403/26/news037.html.

[18] IPA, “組織内部者の不正行為によるインシデント調査,”
http://www.ipa.go.jp/security/fy23/reports/insider/.

[19] IPA, “組織における内部不正防止ガイドライン,”
https://www.ipa.go.jp/security/fy24/reports/insider/.

[20] IPA, “『高度標的型攻撃』対策に向けたシステム設計ガイド,”
https://www.ipa.go.jp/security/vuln/newattack.html.

[21] IoT推進コンソーシアム/データ流通促進WG/カメラ画像利活用SWG.
http://www.iotac.jp/wg/data/.

[22] IoT 推進コンソーシアム, “カメラ画像利活用ガイドブック ver1.0,” 31 1 2017. http://www.meti.go.jp/press/2016/01/20170131002/20170131002-1.pdf.

[23] 朝日新聞 Digital, “ネット接続の複合機など、データ丸見え　大学など２６校,” http://www.asahi.com/articles/ASHDD3SMNHDDPTIL006.html.

[24] 日本放送協会「クローズアップ現代」, “サイバー攻撃の恐怖　狙われる日本のインフラ,” http://www.nhk.or.jp/gendai/kiroku/detail02_3221_all.html.

[25] 愛知県, “愛知県安全なまちづくり条例,” https://www.pref.aichi.jp/police/syokai/houritsu/sekou-kaisei/seian-s/machizukuri.html.

[26] IPA, “はじめての STAMP/STPA ～システム思考に基づく新しい安全性解析手法～,” http://www.ipa.go.jp/sec/reports/20160428.html.

[27] IPA, “はじめての STAMP/STPA（実践編）～システム思考に基づく新しい安全性解析手法～,” https://www.ipa.go.jp/sec/reports/20170324.html.

[28] IPA, “公衆無線 LAN 利用に係る脅威と対策,” https://www.ipa.go.jp/files/000051453.pdf.

[29] Broadband Forum, “TR-069 CPE WAN Management Protocol v1.1,” https://www.broadband-forum.org/technical/download/TR-069_Amendment-2.pdf.

[30] IPA, “コンシューマデバイスの信頼性確保に向けた取組み～開発方法論の国際標準化に向けて～,” https://www.ipa.go.jp/sec/reports/20130930.html.

[31] 多田直弘, モノづくりにおける実践の DRBFM―より高い品質をめざした未然防止手法のすすめ, 夕月書房, 2014.

[32] 丸文株式会社, “ネットワークにおける時刻同期の重要性,” http://www.marubun.co.jp/product/network/ntp/qgc18e0000010oqg-att/symmetricom_wp_1.pdf.

[33] 一般社団法人電子情報技術産業協会(JEITA), “WORM 技術と暗号化技術,” http://home.jeita.or.jp/is/committee/tech-std/std/201104/tape_system_08.pdf.

[34] 一般社団法人重要生活機器連携セキュリティ協議会, “生活機器の脅威事例集,” https://www.ccds.or.jp/public_document.html.

[35] “脆弱性対策情報ポータルサイト（JVN）,” http://jvn.jp/.

[36] “脆弱性対策情報データベース（JVN iPedia）,” http://jvndb.jvn.jp/.

[37] IPA, “情報セキュリティ 10 大脅威 2017,” https://www.ipa.go.jp/security/vuln/10threats2017.html.

[38] Black Hat, https://www.blackhat.com/.

[39] Cyber Threat Alliance, http://www.cyberthreatalliance.org/.

[40] 日本シーサート協議会. http://www.nca.gr.jp/.

[41] 一般社団法人金融 ISAC. http://www.f-isac.jp/.

[42] 一般社団法人 ICT-ISAC, https://www.ict-isac.jp/.

[43] IPA, “【注意喚起】家庭内における無線 LAN のセキュリティ設定の確認を,” https://www.ipa.go.jp/security/topics/alert270612.html.

[44] 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,” 3 2015. http://www.meti.go.jp/meti_lib/report/2015fy/000326.pdf.

本開発指針は、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) つながる世界の開発指針検討 WG において作成しました。また、改訂にあたって利用時品質検討 WG (主査黒須 正明) [1]の検討成果[2]を参考としました。

編著者 (敬称略)

主　査	高田 広章	名古屋大学
副主査	後藤　厚宏	情報セキュリティ大学院大学
委　員	飯島　雅人	株式会社ミサワホーム総合研究所
	木村　利明	一般財団法人機械振興協会　技術研究所
	緒方　日佐男	日立オムロンターミナルソリューションズ株式会社
	荻野　司	一般社団法人重要生活機器連携セキュリティ協議会
	奥原　雅之	富士通株式会社
	梶本　一夫	パナソニック株式会社
	高橋　裕一	株式会社日立製作所　情報・通信システム社
	長谷川　勝敏	一般社団法人組込みイノベーション協議会
	早川　浩史	株式会社デンソー
	松並　勝	一般社団法人日本スマートフォンセキュリティ協会
	三上　清一	株式会社 JVC ケンウッド
事務局	中尾　昌善	IPA／SEC
	宮原　真次	IPA／SEC
	小崎　光義	IPA／SEC
	遠山　真	IPA／SEC
	西尾　桂子	IPA／SEC
	丸山　秀史	IPA／SEC

2018年7月組織再編により「社会基盤センター」が設立されました。
これまでソフトウェア高信頼化センターで行ってきた事業は
「社会基盤センター」が引き続き推進しています。

SEC BOOKS
つながる世界の開発指針
～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ポイント～

2016年5月11日　1版1刷発行
2016年9月9日　1版2刷発行
2017年6月30日　2版1刷発行
2018年9月14日　2版2刷発行

監修者　独立行政法人情報処理推進機構(IPA)
社会基盤センター

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
https://www.ipa.go.jp/ikc/

ISBN 978-4-905318-55-2　Printed in Japan

ISBN978-4-905318-55-2
C3055 ¥278E

定価：本体278円+税

IPA 独立行政法人情報処理推進機構
社会基盤センター

SEC-TN17-003

古紙パルプ配合率80％再生紙を使用

この印刷物は、印刷用の紙へ
リサイクルできます。