別紙１

IoT セキュリティガイドライン
ver 1.0

平成　28 年　7月

IoT 推進コンソーシアム
総務省
経済産業省

はじめに

これまでインターネット等のネットワークに接続していなかった「モノ」が通信機能をもち、ネットワークに接続して動作する IoT(Internet of Things)が急速に普及している。2020 年にはこうしたネットワークに接続する「モノ」（IoT 機器）が 530 億個[1]に増加すると予測されており、これによりネットワークを経由した「モノ」へのサイバー攻撃の脅威が増大することが懸念される。IoT 機器やこれを組み合わせた IoT システムは、コネクテッドカーやスマートハウス等 10 年以上に渡って長期利用されるものや、センサー機器といったコンピューティングリソースに制約があるもの等、多様な性質を持った機器やネットワークで構成されており、この IoT システムやこれを利用したサービス特有の性質を踏まえたセキュリティ対策の検討は急務である。

平成 27 年 9 月に閣議決定されたサイバーセキュリティ戦略においても、IoT 機器やシステム、サービスのセキュリティが確保された形での新規事業の振興やガイドラインの策定などの制度整備、技術開発などを進めることとされている。今後、IoT を活用した革新的なビジネスモデルを創出していくとともに、国民が安全で安心して暮らせる社会を実現するために、こうした基盤整備は不可欠である。

本ガイドラインは、IoT 機器やシステム、サービスの供給者及び利用者を対象として、サイバー攻撃などによる新たなリスクが、モノやその利用者の安全や、個人情報・技術情報などの重要情報の保護に影響を与える可能性があることを認識したうえで、IoT 機器やシステム、サービスに対してリスクに応じた適切なサイバーセキュリティ対策を検討するための考え方を、分野を特定せずまとめたものである。本ガイドラインを活用することにより、IoT 機器やシステム、サービスの供給者や利用者が自己の役割を認識しつつ、分野ごとの性質に応じたセキュリティ確保の取組が促進されることを期待するものである。

[1]（出典）IHS Technology

目次

第1章

背景と目的

本章では、本ガイドライン策定の背景として、IoT の動向と脅威例及び IoT 特有の性質等を挙げ、具体的な脅威の事例や IoT 特有の性質を踏まえたセキュリティ対策の必要性について説明する。

また、本ガイドラインの目的として、業種を問わず IoT の関係者がセキュリティ確保上取り組むべき基本的な項目を示すとともに、IoT のセキュリティ確保のための取組について関係者間相互の認識の共有を促すための材料であることを説明する。加えて、本ガイドラインにおいて対象とする IoT のイメージについても示す。

1.1 ガイドラインの背景

1.1.1 IoT の動向と近年の脅威事例

近年、これまでインターネット等のネットワークに接続していなかった機器が通信機能をもち、ネットワークに接続して動作させることが一般化している。2020 年には、約 530 億個の IoT 機器がネットワークサービスに活用されると予測されている。2020 年時点での IoT 機器の普及分野は、ホームエネルギーマネジメントシステム（HEMS）をはじめとする消費者向けサービスが 52.7%と大半を占めると見込まれており、近年のセキュリティカンファレンスでは、HEMS 等の消費者向けサービスやコネクテッドカー等の自動車関連サービスに関連する IoT の脅威例が多数発表されている。また、既存の調査[2]では多くの IoT 機器のマルウェア感染や乗っ取りが判明しており、さらにその機器を悪用した DDoS 攻撃等の事例が多数発生している。このように、IoT 機器やシステムがネットワークにつながり、サイバー攻撃やシステム障害の発生によって安全に影響を及ぼしたり、個人の生活データなどの重要な情報が漏えいしたりする可能性がある。

表 1　分野別に見た IoT の脅威事例

（出典：総務省「M2M セキュリティ実証事業」成果を基に作成）

カテゴリー	サブカテゴリー	発表年・会議	概要
自動車関連サービス	・コネクテッドカー ・サブシステム	2015年 Black Hat USA	インターネットから自動車の遠隔操作を可能とする脆弱性を紹介。自動車のマルチメディアシステムのコントローラへインターネット経由で接続し、別のコントローラのファームウェアを書き換え、CAN(*1)バス上で不正なコマンドを送信することで、自動車のハンドルやエンジン等の遠隔操作に成功。
消費者向けサービス	・ホームエネルギーマネジメント（HEMS）	2014年 Black Hat USA	セキュアでないホームオートメーション開発の危険性の一例を紹介。ホテルの部屋にある機器・設備の通信に利用されているKNX(*2)net/IPプロトコルをキャプチャ・解析し、機器・設備を不正に遠隔操作することが可能。
産業別のサービス	・医療	2012年 Breakpoint Security Conference	ペースメーカー及び植込み型除細動器へのハッキングのデモを紹介。植込み型除細動器のワイヤレストランスミッタの脆弱性を利用し、近距離から植込み型除細動器に不正な動作を行わせることに成功。

(*1) CAN：Robert Bosch 社が 1986 年に公開した車載ネットワークプロトコル。1994 年国際標準規格（ISO 11898）に認定。

(*2) KNX：欧州の KNX 協会が 2002 年に公開したスマートハウスにおける通信プロトコル。2006 年国際標準規格（ISO/IEC 14543-3）に認定。

1.1.2 IoT 特有の性質とセキュリティ対策の必要性

IoT の動向と脅威事例を踏まえると、IoT の進展が企業活動や製品・サービスのイノベーションを加速する一方で、IoT 特有の性質と想定されるリスクをもつことから、これらの性質とリスクを踏まえたセキュリティ対策を行うことが必要である。一般的な IoT 機器特有の性質を次に挙げる。

【IoT 特有の性質】

（性質１）脅威の影響範囲・影響度合いが大きいこと

HEMS やコネクテッドカー等の IoT 機器はインターネット等のネットワークに接続していることから、ひとたび攻撃を受けると、IoT 機器単体に留まらずネットワークを介して関連する IoT システム・IoT サ

[2] https://www.usenix.org/system/files/conference/woot15/woot15-paper-pa.pdf

ービス全体へその影響が波及する可能性が高く、IoT 機器が急増していることによりその影響範囲はさらに拡大してきている。また、自動車分野、医療分野等において、IoT 機器の制御（アクチュエーション）にまで攻撃の影響が及んだ場合、生命が危険にさらされる場面さえも想定される。さらに、IoT 機器やシステムには重要な情報（例えば個人の生活データ、工場のデバイスから得た生産情報等）が保存されている場合もあり、こうしたデータの漏えいも想定される。

（性質２）IoT 機器のライフサイクルが長いこと

自動車の平均使用年数は 12～13 年程度と言われていたり、工場の制御機器等の物理的安定使用期間は 10 年～20 年程度のものが多く存在するなど、IoT 機器として想定されるモノには 10 年以上の長期にわたって使用されるものも多く、構築・接続時に適用したセキュリティ対策が時間の経過とともに危殆化することによって、セキュリティ対策が不十分になった機器がネットワークに接続されつづけることが想定される。

（性質３）IoT 機器に対する監視が行き届きにくいこと

IoT 機器の多くは、パソコンやスマートフォン等のような画面がないことなどから、人目による監視が行き届きにくいことが想定される。こうした場合、利用者には IoT 機器に問題が発生していることがわかりづらく、管理されていないモノが勝手にネットワークにつながり、マルウェアに感染することなども想定される。

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

IoT 機器側とネットワーク側それぞれが有する業態の環境や特性が、相互間で十分に理解されておらず、IoT 機器がネットワークに接続することによって、所要の安全や性能を満たすことができなくなる可能性がある。特に、接続するネットワーク環境は、IoT 機器側のセキュリティ要件を変化させる可能性があることに注意をすべきである。

（性質５）IoT 機器の機能・性能が限られていること

センサー等のリソースが限られた IoT 機器では、暗号等のセキュリティ対策を適用できない場合がある。

（性質６）開発者が想定していなかった接続が行われる可能性があること

IoT ではあらゆるものが通信機能を持ち、これまで外部につながっていなかったモノがネットワークに接続され、IoT 機器メーカやシステム、サービスの開発者が当初想定していなかった影響が発生する可能性がある。

1.2 ガイドラインの目的

本ガイドラインは、上記の IoT 特有の性質とセキュリティ対策の必要性を踏まえて、IoT 機器やシステム、サービスについて、その関係者がセキュリティ確保等の観点から求められる基本的な取組を、セキュリティ・バイ・デザイン[3]を基本原則としつつ明確化するものである。これによって、産業界による積極的な開発等の取組を促すとともに、利用者が安心して IoT 機器やシステム、サービスを利用できる環境を生み出すことにつなげることを目的とする。

なお、本ガイドラインの目的は、サイバー攻撃などによる被害発生時における IoT 機器やシステム、サービスの関係者間の法的責任の所在を一律に明らかにすることではなく、むしろ関係者が取り組むべき IoT のセキュリティ対策の認識を促すとともに、その認識のもと、関係者間の相互の情報共有を促すための材料を提供することである。

このため、本ガイドラインは、その対象者に対し、一律に具体的なセキュリティ対策の実施を求めるものではなく、その対象者において、守るべきものやリスクの大きさ等を踏まえ、役割・立場に応じて適切なセキュリティ対策の検討が行われることを期待するものである。

加えて、本ガイドラインでは、数多くの IoT 機器やシステム、サービスが、既に国民の日常生活に浸透していることから、一般利用者が注意すべき点についても記載する。

[3] セキュリティ・バイ・デザインとは、企画・設計段階からセキュリティを確保するための方策を指す。

1.3 ガイドラインの対象とするIoTのイメージ

1.3.1 IoTとは

IoTとは”Internet of Things”の略であり、ITU（国際電気通信連合）の勧告（ITU-T Y.2060(Y.4000)）では、「情報社会のために、既存もしくは開発中の相互運用可能な情報通信技術により、物理的もしくは仮想的なモノを接続し、高度なサービスを実現するグローバルインフラ」とされ、次のようなことが期待されている。

①. 「モノ（Things）」がネットワークにつながることにより迅速かつ正確な情報収集が可能となるとともに、リアルタイムに機器やシステムを制御することが可能となる。

②. カーナビや家電、ヘルスケアなど異なる分野の機器やシステムが相互に連携し、新しいサービスの提供が可能となる。

さらに、IoTは「モノ」がネットワークにつながって新しい価値を生むだけでなく、IoTが他のIoTとつながることでさらに新しい価値を生むという”System of Systems（SoS）”としての性質を持っている。SoSの特性とは、図１の１．～５．に示される通りである。

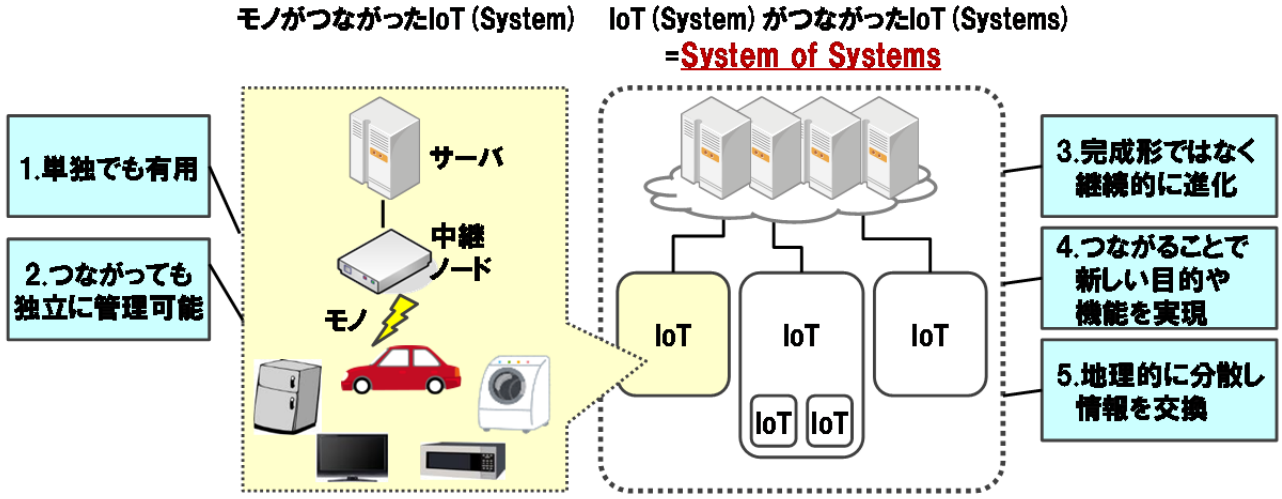


図 1 SoS的な特徴を持ったIoT＝「つながる世界」のイメージ

1.3.2 IoT機器・システム、サービスとは

IoTはつながることで新しい価値を生み出せる優位性を持つが、反面、機器等の確実な動作に関わる対象の構造が刻々と拡大・変化するため、対象の構造が変化した場合、安全に対する再評価を行うことが重要である。そこで、本ガイドラインでは、IoTを構成するネットワークに接続される機器や、その他の機器、システムを組み合わせて構成されるシステムを「IoT機器・システム」（IoTを構成する機器やシステムの総称）、これらの機器やシステムを活用して提供されるサービスを「サービス」として定義する。

1.4 対象読者

本ガイドラインで対象とする対象読者のイメージを以下に示す。

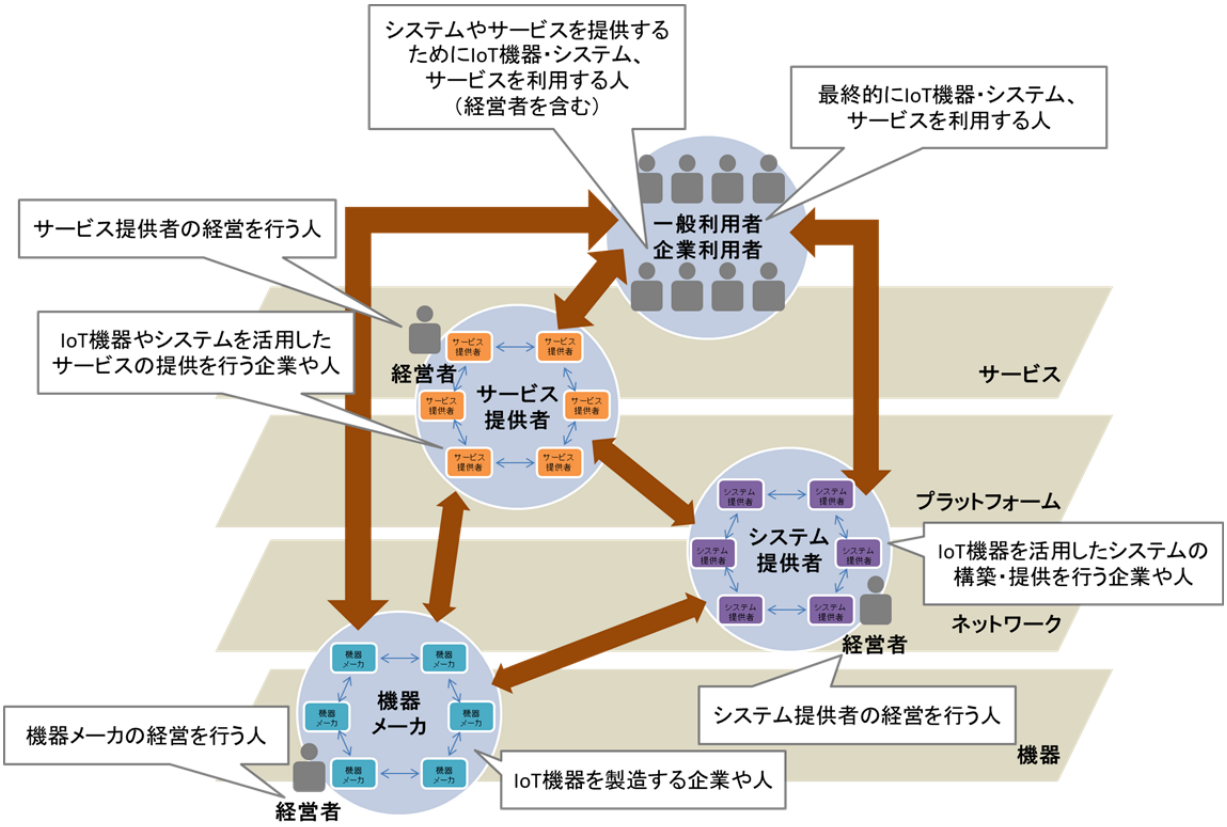


図 2 対象読者のイメージ

本ガイドラインの対象読者は以下を想定している。

- IoT 機器・システム、サービスの供給者及びその経営者
  - 機器メーカ
  - システム提供者
  - サービス提供者
- IoT 機器・システム、サービスの利用者
  - 企業利用者[4]
  - 一般利用者

IoT では複数の IoT 機器･システムやサービスを相互に利用して､機能やサービスを実現することも多く､システム提供者やサービス提供者はそれぞれが利用者であることも認識する必要がある。

[4]企業利用者については、IoT 機器・システム、サービスを自社の生産活動やサービス供給等ビジネスの中に組み込んでこれらの管理を行いつつ、利用している事業者を想定している。

それぞれの対象読者の例をいくつかの具体的なサービスに当てはめて示す。

表 1 対象読者の例

分野	サービス	供給者		システム・サービス提供者／企業利用者[5]	利用者
		経営者	機器メーカ		一般利用者
自動車	コネクテッドカーサービス	右記の機器メーカ、システム・サービス提供者の経営者	・自動車メーカ	・自動車メーカ ・ネットワーク事業者	・自動車の所有者、運転手
家電	HEMS	右記の機器メーカ、システム・サービス提供者の経営者	・HEMS 機器メーカ ・通信機器メーカ	・HEMS 事業者 ・住宅メーカ ・ネットワーク事業者	・居住者
医療	在宅医療サービス	右記の機器メーカ、システム・サービス提供者の経営者	・医療機器メーカ ・通信機器メーカ	・在宅医療サービス事業者 ・病院（システム管理部門） ・ネットワーク事業者	・患者及びその家族 ・医師 ・看護師 ・ケアマネージャ
工場	制御システム	右記の機器メーカ、システム、サービスの提供者／企業利用者の経営者	・制御機器メーカ ・制御用センサーメーカ	・工場のシステム構築者 ・工場の管理者 ・ネットワーク事業者	[6]

本ガイドラインを活用し、IoT におけるリスクの認識と具体的な対策の検討に資することを期待する。本ガイドラインは既に安全やセキュリティに関する基準や法律等が整備されている業界においても、他の分野の機器やシステム、サービスと連携する場合に参考となるものである。

[5] 企業利用者については、IoT 機器・システム、サービスを自社の生産活動やサービス供給等ビジネスの中に組み込んでこれらの管理を行いつつ、利用している事業者を想定している。

[6] 工場等の制御システムも IoT 機器・システムと接続されることで、ユーザ情報など一般利用者に影響を与えることも想定される。

1.5 ガイドラインの全体構成

第 1 章においては、本ガイドラインの背景や目的、ガイドラインの対象とする IoT、そして対象読者を示した。

第 2 章においては、以下に記載するとおり、IoT 機器・システム、サービスの供給者である経営者、機器メーカ、システム提供者・サービス提供者（一部、企業利用者を含む）を対象とした IoT セキュリティ対策の５指針を示す。IoT セキュリティ対策の５指針では、IoT のライフサイクル「方針」、「分析」、「設計」、「構築・接続」、「運用・保守」に沿って複数の要点を挙げ、要点ごとにポイントと解説、対策例を示す。なお、5 つの指針の内容については、「つながる世界の開発指針」（平成 28 年 3 月 独立行政法人情報処理推進機構）[7]を参考に、サービス提供者などへも対象者を広げ、より一般化したものである。

第 3 章においては、一般利用者向けの注意事項をルールとして記載する。

第 4 章においては、今後検討するべき事項を示す。

[7] http://www.ipa.go.jp/files/000051411.pdf

各章・節・要点ごとに想定している読者は以下の通りである。

表 2 章･節･要点ごとの対象読者

【凡例】〇：主な読者として想定

章・節			供給者（企業利用者含む）			利用者
			経営者	機器メーカ	システム・サービス提供者／企業利用者	一般利用者
はじめに			〇	〇	〇	〇
第１章			〇	〇	〇	〇
第２章	２．１ 方針･管理	要点 1	〇	〇	〇	
		要点 2	〇	〇	〇	
	２．２ 分析	要点 3	各要点のポイントについては、「概要」を参照のこと。	〇	〇	
		要点 4		〇	〇	
		要点 5		〇	〇	
		要点 6		〇	〇	
		要点 7		〇	〇	
	２．３ 設計	要点 8		〇	〇	
		要点 9		〇	〇	
		要点 10		〇	〇	
		要点 11		〇	〇	
		要点 12		〇	〇	
	２．４ 構築･接続	要点 13		〇	〇	
		要点 14			〇	
		要点 15			〇	
		要点 16		〇	〇	
	２．５ 運用･保守	要点 17		〇	〇	
		要点 18		〇	〇	
		要点 19		〇	〇	
		要点 20		〇	〇	
		要点 21			〇	
第３章						〇
第４章			〇	〇	〇	

第2章

IoT セキュリティ対策の 5 つの指針

本章は、IoT 機器の開発から IoT サービスの提供までの流れを、「方針」、「分析」、「設計」、「構築・接続」、「運用・保守」の 5 つの段階に分けた上で、それぞれの段階に対するセキュリティ対策指針を示した。さらに、指針ごとに具体的な要点を挙げ、ポイントと解説、対策例を記載する。

なお、既存の安全確保や性能に関する法令・規制要求事項が存在している分野については、それらを順守することが大前提である。その上で、それぞれの分野におけるリスクや事故発生時の対応を考慮し、実施の要否も含め、IoT セキュリティ対策を検討することが重要である。

セキュリティ対策指針の一覧を以下に示す。

表 3 セキュリティ対策指針一覧

大項目	指針	要点
方針	指針1 IoT の性質を考慮した基本方針を定める	要点 1. 経営者が IoT セキュリティにコミットする
		要点 2. 内部不正やミスに備える
分析	指針2 IoT のリスクを認識する	要点 3. 守るべきものを特定する
		要点 4. つながることによるリスクを想定する
		要点 5. つながりで波及するリスクを想定する
		要点 6. 物理的なリスクを認識する
		要点 7. 過去の事例に学ぶ
設計	指針3 守るべきものを守る設計を考える	要点 8. 個々でも全体でも守れる設計をする
		要点 9. つながる相手に迷惑をかけない設計をする
		要点 10. 安全安心を実現する設計の整合性をとる
		要点 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
		要点 12. 安全安心を実現する設計の検証・評価を行う
構築・接続	指針4 ネットワーク上での対策を考える	要点 13. 機器等がどのような状態かを把握し、記録する機能を設ける
		要点 14. 機能及び用途に応じて適切にネットワーク接続する
		要点 15. 初期設定に留意する
		要点 16. 認証機能を導入する
運用・保守	指針5 安全安心な状態を維持し、情報発信・共有を行う	要点 17. 出荷・リリース後も安全安心な状態を維持する
		要点 18. 出荷・リリース後も IoT リスクを把握し、関係者に守ってもらいたいことを伝える
		要点 19. 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
		要点 20. IoT システム・サービスにおける関係者の役割を認識する
		要点 21. 脆弱な機器を把握し、適切に注意喚起を行う

2.1【方針】指針 1　IoT の性質を考慮した基本方針を定める

IoT 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、利用者の身体や生命、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があったり、長期間使われる機器も存在する一方で、全ての IoT 機器・システムまで監視が行き届きにくいこと、IoT 機器・システムの機能・性能が限られることもある。IoT のセキュリティ対策は、機器やシステムの開発企業のみならず、利用する企業にとっても存続にも関わる課題となっており、経営者がリスクを認識し経営者のリーダーシップで対策を推進する必要がある。

そこで本指針では、IoT のセキュリティ対策に企業の経営者を含めて認識しておくべき要点を記載する。

要点 1.経営者が IoT セキュリティにコミットする

要点 2.内部不正やミスに備える

要点1. 経営者が IoT セキュリティにコミットする

(1)ポイント

① 経営者は、「サイバーセキュリティ経営ガイドライン」を踏まえた対応を行う。IoT セキュリティ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。また、そのために必要な体制・人材を整備する。

(2)解説

IoT 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。

その上で、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。また、IoT においては、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。さらに、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。

このため、「サイバーセキュリティ経営ガイドライン」を踏まえ IoT セキュリティに関する基本方針を策定し、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。また、そのために必要な体制・人材を整備する。

(3)対策例

①組織としてセキュリティ対策に取り組む

- 経営層が「サイバーセキュリティ経営ガイドライン」を踏まえ、経営層のリーダーシップに基づいて IoT セキュリティに取り組むようにする。
  - －サイバーセキュリティ経営ガイドライン（平成 27 年 12 月 28 日経済産業省、独立行政法人情報処理推進機構） http://www.meti.go.jp/press/2015/12/20151228002/20151228002-2.pdf
- PDCA サイクルを回し、組織として IoT システム・サービスのリスクを認識し対策を行う体制を構築・維持する。リスクアセスメントの具体的な実施方法については、CSMS ユーザーズガイド等が参考になる。
  - －CSMS ユーザーズガイド（http://www.isms.jipdec.or.jp/csms/doc/JIP-CSMS111-08.pdf）

要点2. 内部不正やミスに備える

(1)ポイント

①IoT の安全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。IoT 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。

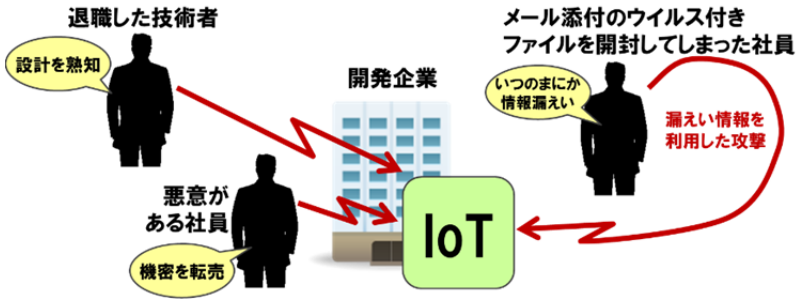


図 3 内部不正やミスによる影響

(3)対策例

①内部不正への対策例

IoT 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（下表）。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。
- IPA では「組織における内部不正防止ガイドライン」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 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	標的を隠す/排除する、利益をなくすことで犯行を防ぐ

（割に合わない）	
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

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。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。

2.2【分析】指針2　IoT のリスクを認識する

IoT のセキュリティ対策を行うには、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 IoT 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したりする可能性もある。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。

本指針では、IoT のリスクの認識として取り組むべき 5 つの要点を説明する。

要点 3.守るべきものを特定する

要点 4.つながることによるリスクを想定する

要点 5.つながりで波及するリスクを想定する

要点 6.物理的なリスクを認識する

要点 7.過去の事例に学ぶ

要点3. 守るべきものを特定する

(1)ポイント

① IoT の安全安心[8]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、財産を守る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、機器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。

つなげるための機能についても、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、IoT の安全安心の観点で、本来の機能やつなげるための機能についても守るべきものとして特定することが必要となる。

また、IoT 機器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。

(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 機器・システムが有する本来機能（自動車であれば「走る」、「曲がる」、「止まる」、エアコンであれば冷暖房といった機能）、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、ネットワークの設定情報等ネットワークに関係する事項も含め洗い出す。

2) 情報の洗い出し

IoT 機器・システムが収集するセンサーデータや個人情報（プライバシー含む）、所有する設計情報などの技術情報を洗い出す。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 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（商用コンテンツ利用時の著作権管理データおよびプライベートコンテンツ等）、コンテンツ利用履歴（コンテンツの利用履歴も保護することが重要）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、GPS で取得した位置情報等
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	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

[8] 本ガイドラインにおける「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」を含んだ概念であり、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。

設定情報	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（ファームウェアと呼ばれることもある）
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ガイドを基に作成

②守るべき機能や情報の洗い出し

従来の機器やシステムをIoT機器・システムとするために追加された通信、連携、集約などの機能や情報を洗い出す。特につなげるための機能の設定情報については、IoT サービスを構築・接続する事業者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。

要点4. 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 機器・システムとして使われる前提でリスクを想定する。
②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。インターネットから直接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。

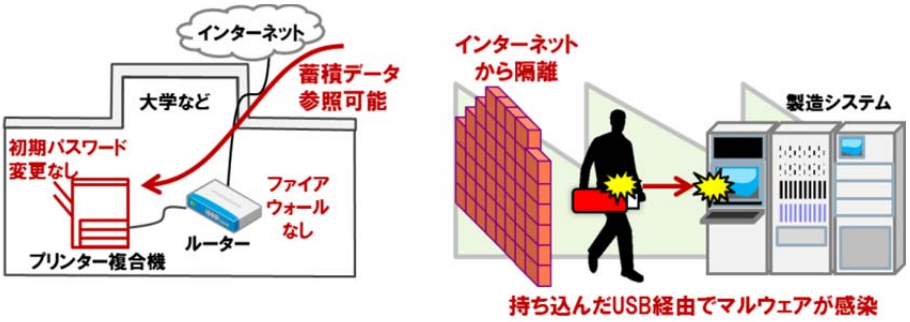


図 4 インターネットにつながらないと想定していたため発生したインシデント例

前者の事例はファイアウォールなどで制限さ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 機器・システム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。保守用ツールの悪用にも備える必要がある。

(3)対策例

①IoT 機器・システム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 機器・システム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 機器・システムとして利用される前提で設計、運用する。

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) 問題がある状況への対応

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。

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

3) ペネトレーションテストの実施

サイバー攻撃による不具合を防ぐため、攻撃者目線での機器やシステムの検証（いわゆるペネトレーションテスト）を行う。

②保守時のリスク、保守用ツールの悪用によるリスク

1) 保守時の攻撃リスクの想定

要点 2 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。

- 保守担当者の端末の管理が甘いことに起因するマルウェアの持ち込み
- 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

要点5. 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、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、対策のレベルが異なる IoT 機器・システムがつながることで全体的な対策のレベルが低下することも想定される。対策のレベルが低い IoT 機器・システム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 機器・システムのリスク想定や設計方針も異なると想定され、ネットワークへの接続パターンも考慮し、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。

(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 機器・システム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。

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たりす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。

②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

対策のレベルが異なる IoT 機器・システムがつながることで、対策レベルが低い IoT 機器・システムが攻撃の入り口になるリスクを想定する。また、対策レベルが低い IoT 機器・システムが接続された 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。

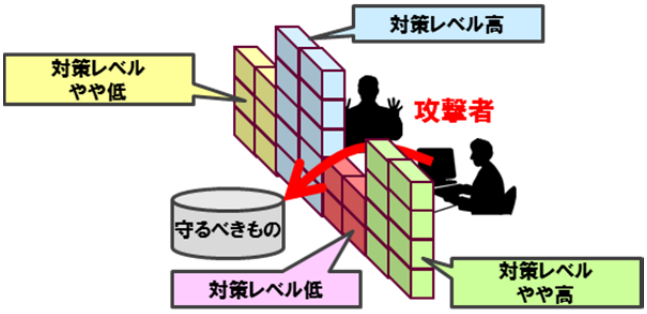


図 5 弱い部分からリスクが発生するイメージ

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 機器・システムのリスクが IoT 全体に波及する可能性を想定することも必要である。

要点6. 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

IoT 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 6　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)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 機器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操作され IoT サービスが誤動作するようなリスクを想定する。

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。

②不正な読み出しや書き換えの想定例

1) 廃棄された IoT 機器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 機器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。

2) IoT 機器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 機器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。

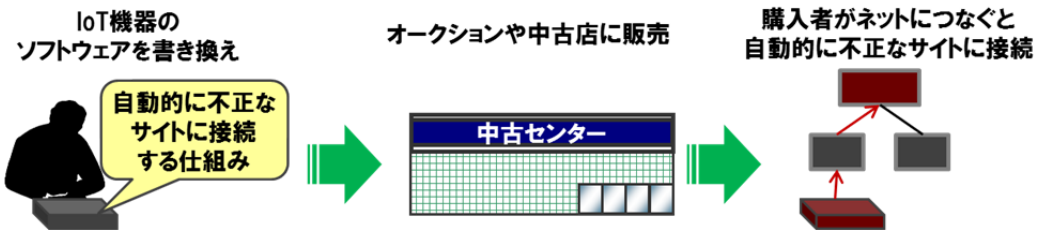


図 7　不正なサイトに接続する中古 IoT 機器が販売されるリスクの例

要点7. 過去の事例に学ぶ

(1)ポイント

① パソコン等の ICT の過去事例から攻撃事例や対策事例を学ぶ。
② IoT の先行事例から攻撃事例や対策事例を学ぶ。

(2)解説

IoT のセキュリティ対策を実施するにあたっては、過去どのような攻撃事例や対策事例があったかを学ぶことで、インシデントを未然に防ぐことやインシデント発生の際の対策の参考とすることができる。

インターネット等のネットワークに接続する場合、ネットワーク経由で攻撃を受ける等の脅威が生じる。IoT に対する攻撃は、ICT で過去に行われた攻撃手法を用いたものも多く発生しており、パソコン等の ICT で発生した攻撃事例や対策等を参考にし、IoT におけるセキュリティ対策を検討することが有効である。また、先行する IoT で発生した攻撃事例、その対策事例についてもセキュリティ対策の参考とする。

IoT のセキュリティインシデントの先行事例としては、適切なセキュリティ対策を施されていない複合機や Web カメラに対して、第三者がインターネット経由で不正にアクセスできる状態になっていることが明らかになった。このような IoT の先行的な攻撃事例を受けて、IPA や IoT 機器メーカ等から供給者や利用者に向けたセキュリティ対策に関する注意喚起がなされている。

(3)対策例

① パソコン等の ICT の攻撃事例と対策事例

パソコンにおける攻撃事例を以下に示す。

パソコンでは、2001 年頃に悪質で影響力の大きいマルウェアが複数発見され、企業内のローカルネットワークだけではなく、インターネットサービスプロバイダのメールサーバがダウンしたり、ルータが膨大なトラフィックを処理しきれなくなり正常な通信ができなくなる、等の影響が発生した。

パソコン等、ICT におけるセキュリティ対策の具体例を以下に示す。

1) ファイアウォール機能の強化
不必要な通信を行わないよう、不要なサービス、パケットを遮断する。

2) 更新プログラムの自動インストール
セキュリティホールを素早く修正して攻撃者の侵入を防ぐ。

3) ウイルス対策ソフトのインストールの強制
ウイルス対策ソフトがインストールされているか否かを自動的にチェックし、インストールされていない場合にはインストールを強制する。

4) マルウェアに侵入されてもマルウェアの起動を防ぐ仕組みの実装
実行可能なプログラムを事前に登録し、プログラムの起動を制御することで、万が一マルウェアが侵入してもその起動を水際で防ぐ。(ホワイトリスト技術)

② IoT の先行事例における攻撃事例と対策事例

IoT の先行事例における攻撃事例を以下に示す。

複数の大学の複合機がインターネットから参照できる状態になっており、複合機へのアクセスにファイアウォールがなく ID・パスワードを初期設定から変更していない場合、外部から容易に複合機に蓄積されたデータへのアクセスが可能であった。

また、適切なセキュリティ対策を施していない世界中の Web カメラ(カフェ、店舗、モール、工場、寝室等 73,000 台分)の映像を供給者や利用者に無断で公開できてしまうことが明らかになった。

IoT 機器をネットワークへ新たに接続する際のセキュリティ対策の具体例を以下に示す。

1) 不要なインターネット接続の停止

インターネット接続する必要のない IoT 機器については、インターネット接続を行わない。

2) ファイアウォールの設置

インターネット接続する IoT 機器のうち、複合機等ファイアウォールにより外部からのアクセス制御が有効なものについては、ファイアウォールの設置を行う。

3) パスワードの変更

パスワードを IoT 機器出荷時の初期設定から変更し、悪意のある第三者からのなりすましによる不正アクセスを防ぐ。

2.3【設計】指針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 IoT のセキュリティ対策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 機器・システムを連携する他の IoT 機器・システム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セキュリティを維持したり、異常が発生してもつながる相手に迷惑をかけたりしない設計が望まれる。

本指針では、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 つの要点を説明する。

要点 8.個々でも全体でも守れる設計をする

要点 9.つながる相手に迷惑をかけない設計をする

要点 10.安全安心を実現する設計の整合性をとる

要点 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

要点 12.安全安心を実現する設計の検証・評価を行う

要点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 機器・システムで対策を検討する。
②個々の IoT 機器・システムで対応しきれない場合は、それらを含む上位の IoT 機器・システムで対策を検討する。

(2)解説

IoT 機器・システムにおいて発生するリスクとしては、「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」が挙げられる。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。

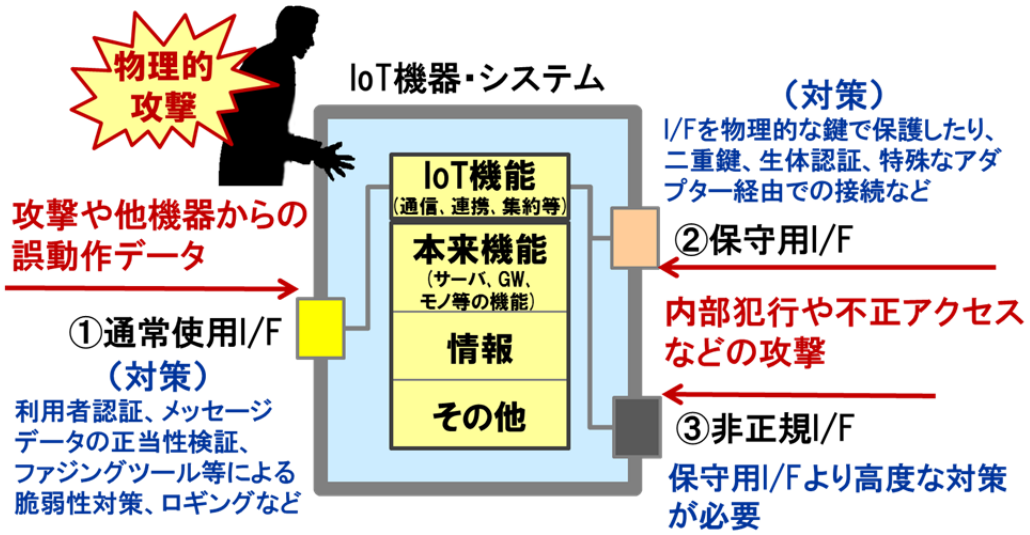


図 8　外部インタフェースのリスクへの対策

内包リスクとは機器やシステムの設計や仕様、設定等においてセキュリティ上の問題が存在することであり、具体的には、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が想定される。また、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。

IoT 機器・システム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 機器・システム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。
- 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。

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。
- 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 機器・システム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。下表に例を示す。

表 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クリア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 機器・システム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 機器・システムを上位の IoT 機器・システムで守る対策

性能が不十分でセキュリティ機能を載せられない IoT 機器・システムは、下図のようにそれらを含む「上位の IoT 機器・システム」で守る対策を検討する。

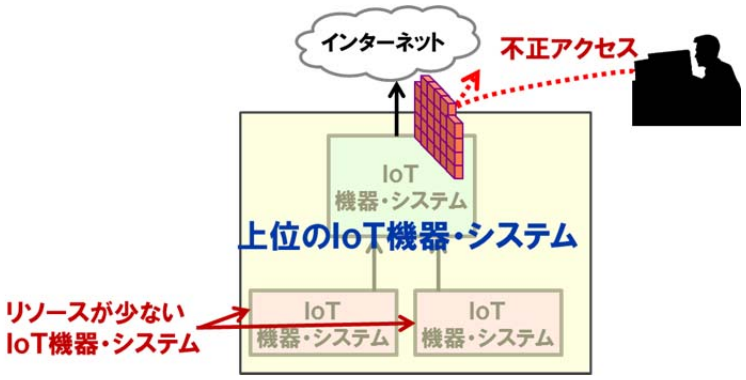


図 9　上位の IoT 機器・システムで守るイメージ

- IoT 機器・システムが通信でつながる接点を考慮する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 機器・システムにより、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。
- 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 機器・システムの開発者は、当該 IoT 機器・システム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。

要点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 機器・システム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 機器・システムに波及する可能性があり、それを防ぐために当該 IoT 機器・システム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 機器・システム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 機器・システムの機能を利用していた他の IoT 機器・システム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。

(3)対策例

①異常状態の検知と波及防止

1) 異常状態の検知

異常状態の検知は、まず各 IoT 機器・システム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 機器・システム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 機器・システム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 機器･システムの監視
  複数の IoT 機器･システム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いる。
- IoT 機器･システム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 機器･システムの性能に応じて監視方法を適切に設計する。

2) 異常状態の影響の波及抑止

- IoT 機器･システムが自身の異常な状態を検知した場合、それが他の IoT 機器･システム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 機器･システムの異常を検知した場合は、その内容によって当該 IoT 機器･システム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異常発生時の復旧方法

1) 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

2) IoT 機器・システムの再起動・再接続

- 状況によっては、当該 IoT 機器・システム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 機器・システム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機器・システムについては、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。

3) IoT 機器・システムの復旧力／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。[9]

[9] 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 の準備体制）、ISO/IEC 27001（情報セキュリティ）で標準規格が策定されている。他にも、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。

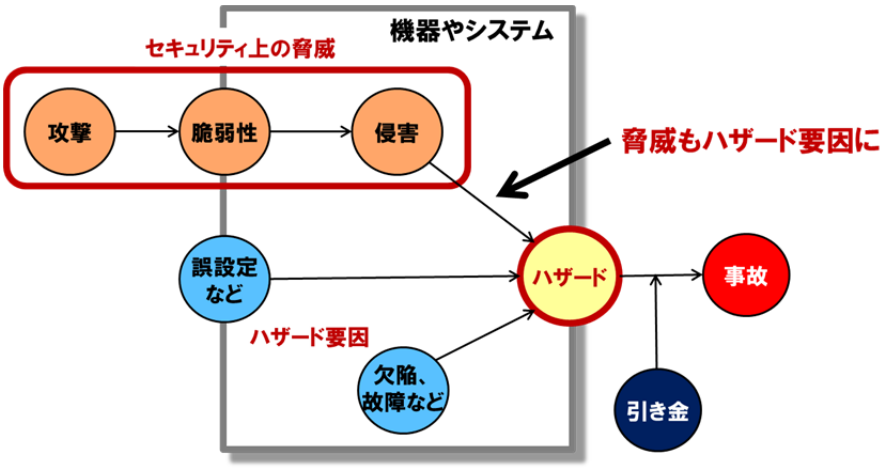
要点10. 安全安心を実現する設計の整合性をとる

(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 機器・システム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。特に、セーフティ機能が攻撃された場合は、システムダウンや事故につながりかねず注意が必要である。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 10 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。

また、既に安全を確保するための安全規制等が存在する場合[10]には、それらに従って安全を確保することが大前提である。

(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。
- 見える化することで、開発者のみならず、経営者、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。

[10]安全規制等の例
一般製品：製造物責任法(PL 法)、医療機器：薬機法、自動車：道路運送車両法、高圧ガスプラント：高圧ガス保安法

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。
- 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。

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。
- 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：設計者が変更点・変化点に着目し、心配点をしっかり洗い出して設計的対応を考えた上、有識者、専門家を交え多くの知見からデザインレビューして未然防止を図る手法） 等が挙げられる。
- IoT 化することにより発現する最大のリスクは、IoT 機器の機能について、設計上想定された結果を保証できなくなることであり、サイバー攻撃やシステム障害が起こりうることを考慮する必要がある。全てのリスクをゼロにすることは難しいものの IoT 機器・システムの設計時には、対策を前もって体系的に検討するとともに、結果が保証できなくなる事態に陥った際、現行法令要求が求める安全を確保するため、安全な状態に遷移させることが必要である。（Fail Safe、Fail As Is 等）

要点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

① IoT 機器・システム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)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 が普及するにともない、利用されている機器のメーカが意図していない不特定の機器が、インテグレータや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。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、同じメーカの製品同士でも、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。

(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。

- 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。
- 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。

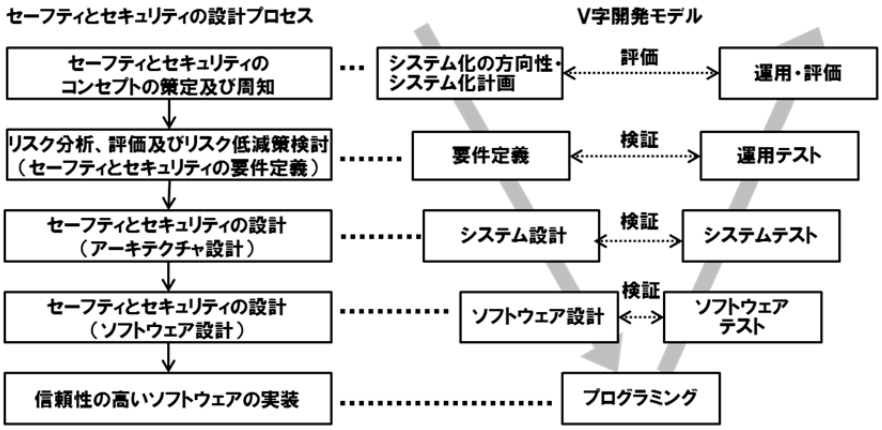
要点12. 安全安心を実現する設計の検証・評価を行う

(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を実現する設計の検証・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。下図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 11 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 機器・システムについては、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 IoT 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

各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（例えば、自動車分野であれば ISO26262、産業機械分野であれば IEC62061 等）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。

- 製品セキュリティに関する国際規格
  - 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 ATM、車載器（カーナビ等）などのセキュリティ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。

2.4【構築・接続】指針 4　ネットワーク上での対策を考える

多様な機能・性能を持つ機器・システムが相互に接続される IoT では、機器のみにセキュリティ対策をゆだねるのでは無く、IoT 機器・システム及びネットワークの両面からセキュリティ対策を考えることが重要である。

本指針では、システム・サービスの構築・接続時に取り組むべき４つの要点を説明する。

要点 13.　機器等がどのような状態かを把握し、記録する機能を設ける

要点 14.　機能及び用途に応じて適切にネットワーク接続する

要点 15　初期設定に留意する

要点 16.　認証機能を導入する

要点13. 機器等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 機器等の状態や他の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

様々な機器やシステムがつながった状態では、何がどのように接続し、機器やネットワーク上の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。異常の発生を検知・分析して、原因を明らかにしたり、対策を検討したりするためには、個々の IoT 機器・システムがそれぞれの状態や他機器との通信状態を収集・把握することが必要である。また、発生した異常の原因究明を行う際に必要となることから、収集した情報はログとして適切に記録することが必要である。このとき、ログとして保管しても、攻撃者等によりその内容を不正に消去・改ざんされてしまうと対策が打てなくなってしまうことから、正しく記録できるよう対策を講じる必要がある。

また、IoT 機器・システムの中にはセンサーなど低機能のものも含まれており、単独で大量のログの管理や、ログの暗号化などの対策を行うことが難しい場合がある。そのような機器については、他にログを管理するための機器を用意するなどの対策を行う必要がある。

(3)対策例

①機器等の状態や他の機器との通信状態を把握して記録

- 各 IoT 機器・システム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リソースは有限であるため、保管方針を策定する。
- 関連する IoT 機器・システム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。
- 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 機器・システム全体で考慮する。
- ログの記録が IoT 機器・システム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 機器・システムにおいて、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 機器・システム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 機器・システム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。

要点14. 機能及び用途に応じて適切にネットワーク接続する

(1)ポイント

① 機能及び用途に応じてネットワーク接続の方法を検討し、構築・接続する。
② ネットワーク接続の方法を検討する際には、IoT 機器の機能・性能のレベルも考慮する。

(2)解説

提供する IoT システム・サービスの機能及び用途、IoT 機器の機能・性能等を踏まえ、ネットワーク構成やセキュリティ機能の検討を行い、IoT システム・サービスを構築・接続する必要がある。

機能及び用途に応じて有線接続・無線接続のどちらを選択するかを検討した上で、セキュリティ対策を実施する必要がある。また、機能・性能が限られた IoT 機器については、IoT 機器単体で必要なセキュリティ対策を実現することが困難なため、IoT システム・サービス全体でセキュリティを確保することが必要である。

(3)対策例

①機能及び用途に応じたネットワーク接続

機能・性能レベルの異なる IoT 機器が混在する環境を前提として、IoT システム・サービス全体でのセキュリティを確保できる設計を行い、構築・接続する必要がある。

1) ネットワーク接続の基本方針
セキュリティ対策が適用された IoT 機器をインターネットへ接続することとし、セキュリティ対策が適用されていない IoT 機器の接続や不必要なネットワーク接続は行わないように留意する。なお、IoT システム・サービスとして必要な IoT 機器のみをインターネットへ接続するよう留意する。

2) 認証機能の適用
有線接続・無線接続やセキュアなゲートウェイ経由の接続等それぞれの環境においてパスワード認証等の認証機能によるセキュリティ対策を実施する。具体的な認証機能については、要点 16 に記載する。

3) 暗号機能の適用
有線接続・無線接続やセキュアなゲートウェイ経由の接続等それぞれの環境において暗号機能によるセキュリティ対策を実施する。暗号機能の適用にあたっては、適切な暗号アルゴリズム、ハッシュ関数を採用することに留意し、総務省・経済産業省の「CRYPTREC 暗号リスト（電子政府推奨暗号リスト）」を参照し、採用する技術が危殆化していないか、利用中に危殆化する恐れがないかを確認する。
CRYPTREC 暗号リスト（電子政府推奨暗号リスト）：http://www.cryptrec.go.jp/list.html
暗号機能適用の具体例を以下に示す。

- 有線接続では TLS、無線接続では WPA2 等のネットワーク暗号化を適用する等、ネットワークの通信路のデータの盗聴や改ざんへの対策を行う。
- クラウド上のデータ蓄積形態に応じて、ファイルの暗号化やデータベースの暗号化を適用する等、クラウド上のデータの盗難や不正アクセスへの対策を行う。特に暗号鍵等の高い機密性が求められるデータは、必要に応じて HSM 等の専用の暗号装置や TEE、TPM 等の暗号技術の利用等を検討する。

4) 第三者適合性評価制度
システム・サービス提供者は、ISMS 適合性評価制度等の第三者適合性評価制度による認証を受けた信頼性の高いシステム・サービスの利用を検討する。

②IoT 機器の機能・性能レベルの考慮

センサー等の機能・性能が限られた IoT 機器では、暗号等のセキュリティ対策を適用できない場合がある。こうした制約のある IoT 機器のセキュリティを確保する場合には、IoT 機器単体でのセキュリティ対策のみならず、機器、ネットワーク、プラットフォーム、サービス等の階層ごとにセキュリティ対策の役

割を分担し、IoT システム・サービス全体でセキュリティを確保することが必要である。

例えば、セキュリティ対策の困難な IoT 機器をネットワークに接続する場合、インターネットへつながる手前でセキュアなゲートウェイを経由させる等、セキュリティを確保する手段を講じる。

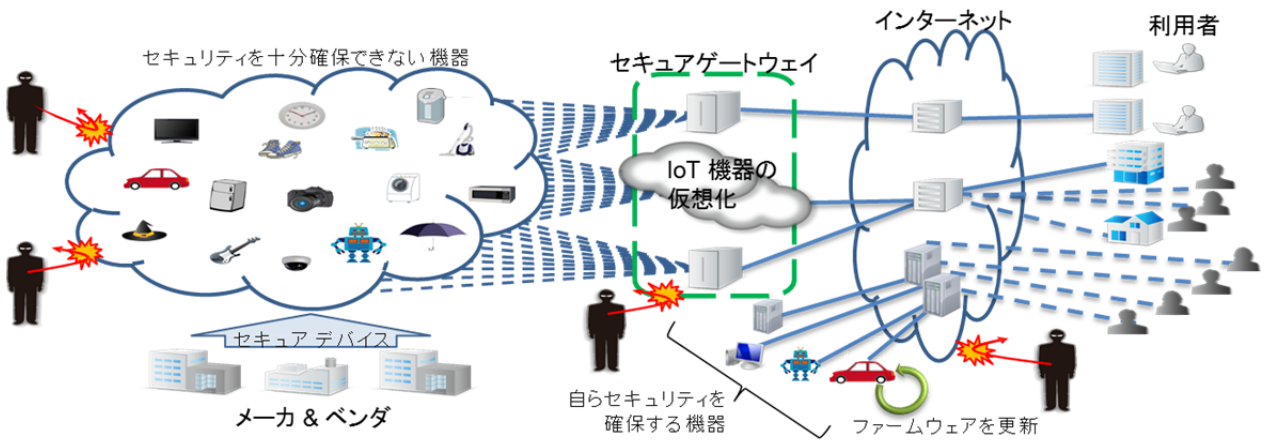


図 12 セキュアなゲートウェイを経由する接続イメージ

要点15. 初期設定に留意する

(1)ポイント

① IoT システム・サービスの構築・接続時や利用開始時にセキュリティに留意した初期設定を行う。
② 利用者へ初期設定に関する注意喚起を行う。

(2)解説

IoT システム・サービスの提供者がシステム・サービスを構築・接続したり、その提供を開始するにあたって、悪意のある攻撃者が容易に攻撃可能であるような脆弱なシステム・サービスとならないよう、できる限り脆弱性に留意したセキュアな設定とすることが必要である。また、利用者へ初期設定に関する注意喚起を行う必要がある。

(3)対策例

①IoT システム・サービス構築・接続時のセキュリティに留意した初期設定

IoT システム・サービスの提供者として、管理者権限等のパスワードの設定・管理の徹底や不要なサービス・ポートの停止等を行い、初期設定に留意する。

1) パスワードの適切な設定・管理
管理者権限、利用者権限のパスワード設定及び管理を適切に行うことで、なりすましによる悪意のある第三者からの不正アクセスを防止する。
具体例を以下に示す。
- パスワードを初期設定のままとせず、適切に変更(変更後の文字数、文字種別等にも留意)し、第三者に知られないよう厳重に管理する。
- パスワードを権限のないユーザと共有しない。
- パスワードを他システム・サービスと使いまわししない。

2) アクセス制御の適用
ファイアウォール等により、適切なアクセス制御を行うことで、外部からの不正アクセスを防止する。

3) ソフトウェアのアップデート
IoT 機器の出荷時からシステム・サービスのリリースまでにIoT 機器メーカからファームウェア等のアップデート版が公開されている可能性がある。そのため、システム・サービスのリリース時にアップデート版の公開有無について確認し、公開されている場合、IoT システム・サービスの提供者はアップデートの要否を判断した上で、問題ない場合はアップデートを行う。なお、アップデート版の取得は、必ず IoT 機器メーカ等の信頼できる Web サイトからダウンロードする等、信頼できる経路で、電子署名等を利用して改ざんされていないことを検証したものを取得することに留意する。

4) 不要なサービス・ポートの停止
認証やアクセス制御、ソフトウェアアップデート以外のセキュリティ対策として、TELNET 等の不要なネットワークサービスやポートを停止することで、外部からの不正アクセスを防止する。
具体例を以下に示す。
- 不要なネットワークサービスがないか点検・確認し、不要なネットワークサービスは停止する。
- サービスに必要のない不要なポートがオープンとなっていないか点検・確認し、不要なポートは停止する。

②利用者への初期設定に関する注意喚起

IoT システム・サービスの提供者の立場から、利用者に初期設定に関する注意喚起を行う。

1) パスワードの変更
IoT 機器の出荷時の初期パスワードを変更することを利用者へ注意喚起する。初期パスワードの変更が

行われなければ、機能を制限するなどの対策も有効である。

2) ファイアウォールの設置

複合機等ファイアウォールの設置が有効な IoT 機器・システムに関しては、ファイアウォールの設置を行うことを利用者へ注意喚起する。

要点16. 認証機能を導入する

(1)ポイント

① IoT システム・サービス全体でセキュリティの確保を実現する認証機能を適用する。
② IoT 機器の機能・性能の制約を踏まえた適切な認証方式を使用する。

(2)解説

不正な IoT 機器が正規の IoT 機器のようになりすますことで、利用したユーザのプライバシー情報が漏えいしたり、不正なユーザが正規のユーザになりすますことで、IoT 機器が乗っ取られて不正な動作を引き起こす可能性がある。また、ネットワークの通信路やクラウド上のプラットフォームのデータが盗聴され、ユーザのプライバシー情報が漏えいする可能性がある。そうしたなりすましや盗聴等の脅威への対策として、認証や暗号化等の仕組みの導入が必要である。

(3)対策例

①IoT システム・サービス全体でセキュリティの確保を実現する認証機能

IoT システム・サービス全体でセキュリティの確保を実現する認証機能を適用する。
具体例を以下に示す。

- 接続する IoT 機器のなりすましへの対策を行う。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、メッセージ認証等を行い、また、不正な IoT 機器からの接続拒否設定も行う。
- 利用者のなりすましへの対策を行う。利用者を識別する ID・パスワード、IC カード、生体認証等による認証を行う。
- 接続する相手のシステム・サービスのなりすましへの対策を行う。接続する IoT 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を行う。

②IoT 機器の機能・性能の制約を踏まえた適切な認証方式

取り扱う情報の種類に応じ、IoT 機器及びネットワークの機能・性能に制約があっても、データの改ざんや漏えいを防ぐことのできる認証技術を採用する。
具体例を以下に示す。

- 暗号を用いた認証の適用
  IoT 機器のファームウェア更新時には、過失または故意によって、ファームウェアの改ざん等の脅威が想定される。そうした脅威に対して IoT 機器のファームウェアを正しく更新するためには、更新データの正当性を担保する必要がある。IoT 機器及びネットワークの機能・性能に制約のある環境下において確実なアップデートを実現するためには、暗号を用いた機器認証、ユーザ認証やファームウェア検証等が有効である。

2.5【運用・保守】指針 5
安全安心な状態を維持し、情報発信・共有を行う

IoT では多様な機器が存在し 10 年以上の長期間利用される機器やシステムも想定される。そのため、機器の故障だけでなく、危殆化等によるセキュリティ対策状況の劣化やネットワーク環境の変化など、多くの環境変化が考えられ、機器やシステム、サービスの出荷やリリース後についてもセキュリティ対策を考えることが重要である。

本指針では、市場に出た後も想定し、IoT 機器・システム、サービスに関わる関係者が取り組むべき５つの要点を説明する。

要点 17.　出荷・リリース後も安全安心な状態を維持する

要点 18.　出荷・リリース後も IoT リスクを把握し、関係者に守ってもらいたいことを伝える

要点 19.　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

要点 20.　IoT システム・サービスにおける関係者の役割を認識する

要点 21.　脆弱な機器を把握し、適切に注意喚起を行う

要点17. 出荷・リリース後も安全安心な状態を維持する

(1)ポイント

① IoT システム・サービスの提供者等は、IoT 機器のセキュリティ上重要なアップデート等を必要なタイミングで適切に実施する方法を検討し、適用する。

(2)解説

IoT 機器には製品出荷後に脆弱性が発見されることがあるため、脆弱性を対策した対策版のソフトウェアを IoT 機器へ配布・アップデートする手段が必要である。

IoTシステム・サービスの提供者等は、IoTシステム・サービスの分野ごとの特徴を踏まえて、IoT 機器のセキュリティ上重要なアップデートを必要なタイミングで適切に実施する方法を検討し、適用する必要がある。

なお、本指針は IoT 機器に対して常に最新のアップデートを適用せよ、という趣旨ではなく、セキュリティ上重要なアップデートを適切に行って、IoT 機器を安全安心な状態に保つことを推奨するものである。

(3)対策例

①IoT 機器のアップデート

IoT システム・サービスの提供者等は、IoT システム・サービスの分野ごとの特徴を踏まえて、IoT 機器のセキュリティ上重要なアップデートを必要なタイミングで適切に実施する方法を検討し、適用する。

1) アップデート方法の検討

IoT システム・サービスの環境を考慮したアップデート方法を検討する。例えば、リモート経由もしくは USB 等の媒体の利用等について検討する。USB 等の媒体を利用する場合は、アップデート時にウイルスチェック等を行い、ウイルス混入を防止する。

また、IoT 機器のファームウェア等のアップデートを自動的に行って問題ないかどうかを判断する。

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を検討する。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）を可能とする方法を検討する。

なお、アップデートを遠隔で行う場合には、アップデート機能が乗っ取られ悪用されないよう、アップデート機能のセキュリティ対策を講じることも重要である。

2) アップデート等の機能の搭載

アップデートの実施ができるよう、IoT 機器にアップデート機能を搭載する。

具体例を以下に示す。

- IoT 機器が自動または手動によりファームウェア等をアップデートできる機能を搭載する。
- IoT 機器が離れた場所にある場合には、遠隔でアップデートできる機能を搭載する。
- アップデート対象となる IoT 機器のなりすましを防止するために、IoT 機器の認証やアップデートファイルの暗号化を行うことも検討する。また、必要に応じ、暗号の危殆化に対応した鍵管理システムの導入を検討する。
- 一般利用者が使用するような IoT 機器については、電源オフ・オンでファームウェアのアップデートができるような簡易な機能を搭載することも検討する。

3) アップデートの実施

1)で検討した結果に従い、ファームウェア等のアップデートを行う。なお、アップデート版の取得は、必ず IoT 機器メーカ等の信頼できる Web サイトからダウンロードする等、信頼できる経路で、電子署名等を利用した改ざんされていないことを検証したものを取得することに留意する。

要点18. 出荷・リリース後も IoT リスクを把握し、関係者に守ってもらいたいことを伝える

(1)ポイント

① 脆弱性情報を収集・分析し、ユーザや他のシステム・サービスの供給者・運用者に情報発信を行う。
② セキュリティに関する重要な事項を利用者へあらかじめ説明する。
③ 出荷・リリース後の構築・接続、運用・保守、廃棄の各ライフサイクルで関係者に守ってもらいたいことを伝える。

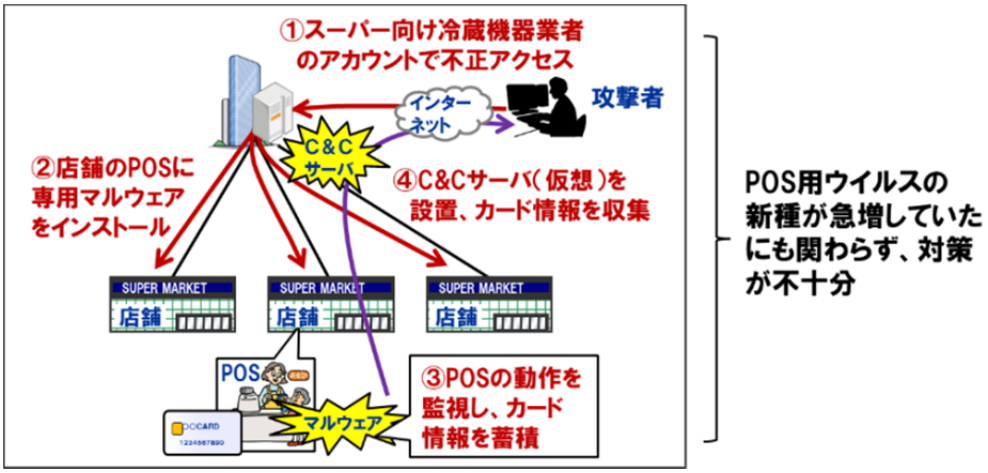
(2)解説

提供するシステム・サービスに関わる脆弱性情報がないか、脆弱性情報を収集・分析し、ユーザや他のシステム・サービス提供者に情報発信を行う必要がある。

また、IoT システム・サービス提供者は、システム・サービスの提供条件や利用上の注意等の中にセキュリティに関する留意事項を記載し、利用者に対してシステム・サービスの利用開始前に説明する必要がある。

IoT では、出荷後に想定外の問題が発生するリスクもある。例えば、2013 年に米国大手小売業が POS 用ウイルスに感染し、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事例がある。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。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。

IoT 機器メーカ及びシステム・サービス提供者は、これらの問題に早急に対応するために、関係者と協力し継続的に情報収集・分析する必要がある。



出典:CCDS 生活機器の脅威事例集を基に作成

図 13 POS 端末に対する攻撃事例

また、IoT 機器・システムは出荷・リリース後、構築・接続、運用・保守にて長期にわたって利用される。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。

- 構築・接続時
  - 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
  - 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た継続利用
  - 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

上記の問題は、設計時等の対策だけでは対応が難しいため、構築・接続、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。

(3)対策例

①脆弱性情報の収集・分析と情報発信

脆弱性情報を収集・分析し、ユーザや他のシステム・サービス提供者に情報発信を行い、ファームウェアアップデート等の必要な対策を行う必要がある。なお、アップデート版の取得は、必ず IoT 機器メーカ等の信頼できる Web サイトからダウンロードする等、信頼できる経路で、電子署名等を利用して改ざんされていないことを検証したものを取得することに留意する。

具体例を以下に示す。

1) 脆弱性情報の収集・分析

- IoT システム・サービスの運用中に発生した脆弱性情報やインシデント情報を収集・分析する。
  - 自社が提供する IoT 機器・システム、サービスの基本的な構成情報の把握・管理
  - 入手した脆弱性情報やインシデント情報について、自社が提供する IoT 機器・システム、サービスへの影響を調査
  - 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
- 現場と接している関係者が把握した脆弱性情報やインシデント情報を IoT 機器メーカや IoT システム・サービス提供者にフィードバックする仕組みも検討する。
- IoT 機器メーカや公的機関、ISAC 等が発信している情報の収集・分析を行う。以下に情報の収集先の例を示す。

表 7 脆弱性情報等の収集先の例

	名称	概要
国内の収集先	JPCERT/CC	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) - 同 データベース(JVN iPedia) 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)	業界ごとでインシデント、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。
	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。
海外の収集先	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。
	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。

※OSS の脆弱性情報については、個別に開発者や関係者等で構成される団体（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) 情報発信

構成情報と脆弱性情報がマッチングした場合、関係者へ情報発信を行う必要がある。なお、一般利用者と情報連携できる窓口・チャネルとしてポータルサイトでの情報提供サービスを活用することも検討する。

発信先の例を以下に示す。

- 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。
- JPCERT/CC
- ISAC

外部への情報発信・共有する際には、影響が及ぶ関係者を見極め、発信先を選定し、発信方法やタイミングに留意する。

対策の目処がないまま脆弱性情報を公開することはゼロデイ攻撃を受けるなど新たなリスクを発生させるため、情報発信・共有するタイミングや発信先は慎重に検討する。

・JPCERT/CC 脆弱性関連情報取扱いガイドライン（https://www.jpcert.or.jp/vh/vul-guideline2014.pdf）

②セキュリティに関する重要事項の事前説明

IoT システム・サービス提供者は、重要事項説明等（サービスの提供条件や利用上の注意等）の中にセキュリティに関する留意事項を記載し、利用者に対してシステム・サービスの利用開始前に説明する。

説明方法の具体例を以下に示す。

1) Web での情報公開
2) サービス約款・マニュアル等への記載
3) IoT 機器・システムが画面を有する場合は、画面での表示

③出荷・リリース後の各ライフサイクルで関係者に守ってもらいたいことの伝達

各ライフサイクルにおいて関係者に守ってもらいたいことの例を以下に示す。

1) 構築・接続時の対策
   - 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 機器・システム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
   - 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 14 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・秘密情報の未消去への対応
  - 個人情報・秘密情報が IoT 機器・システム内に存在することを周知徹底
  - 未消去に関するリスクの解説
  - 個人情報・秘密情報を完全に消去するためのプログラムの搭載

要点19. 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や守ってもらいたいことを一般利用者に伝える。

(2)解説

一般利用者が不用意なつなぎ方や不正な使い方をすると、不正に遠隔操作されたり、異常動作する等のリスクが高まる。

また、IoT 機器メーカ及び IoT システム・サービス提供者が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・リリース時には想定できなかったリスクが発生する可能性もあるため、そのようなリスクの存在を一般利用者に伝える必要がある。

IoT 機器を利用する際には、その利便性だけではなく、リスクがあることも一般利用者に周知する必要がある。一般利用者に対して、IoT 機器・システムを不用意につなげたり、不正な使い方をしないことを周知するとともに、IoT 機器・システムの脆弱性対策の必要性を説明し、協力を得ることが必要である。

(3)対策例

①不用意なつなぎ方によるリスクや守ってもらいたいことの一般利用者への周知

一般利用者が不用意なつなぎ方や不正な使い方をすると、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高まる。そのため、リスクを一般利用者に周知する。

具体例を以下に示す。

1) 一般利用者への周知方法

- IoT 機器が画面を有する場合、起動時の画面への表示
- マニュアルへの記載(IoT 機器メーカ及びシステム・サービス提供者から一般利用者への周知)
- 保証書への記載
- 自社 Web サイトへの掲載

2) 一般利用者へ周知する内容

- 推奨する(動作保証がされている)つなぎ方
- アップデート実施
- 自動アップデート機能がある場合の出荷時のデフォルト設定
- 無線 LAN(Wi-Fi 等)のセキュリティキーなどのセキュリティ設定
- 他者が推定しにくいパスワード設定

- 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、個人情報・秘密情報を完全に消去するためのプログラムの利用

なお、周知の際には第 3 章「一般利用者のためのルール」に記載の一般利用者向けのルールを参照した上で、利用者への適切な周知を行う事が望ましい。

要点20. IoT システム・サービスにおける関係者の役割を認識する

(1)ポイント

① IoT 機器メーカや IoT システム・サービス提供者及び一般利用者の役割を整理する。

(2)解説

インシデントが発生してから誰がどのような対応をするのか初めて協議するようでは、セキュリティ対策が後手に回り、被害の影響が大きくなる可能性がある。また、事前に役割を明確化しておかないことに起因する、関係者間の連携不足も懸念される。

サービス開始時までにあらかじめシステム・サービス提供者が関係者間の役割分担を明確にし、それぞれの役割を正しく理解してもらえるよう努めておく必要がある。

IoT においては、自動車・医療機器・スマート家電・スマートホーム等の分野ごとに想定されるインシデントやリスクは大きく異なってくるため、分野ごとに関係者の役割を整理して理解しておくことが必要である。例えば、自動車分野では、IoT 機器メーカが自動車メーカ、IoT システム・サービス提供者が TSP 等のネットワーク事業者や自動車メーカ、一般利用者が自動車の所有者、運転手等となっている。同様に、医療分野では、IoT 機器メーカが医療機器メーカや通信機器メーカ、IoT システム・サービス提供者がネットワーク事業者や在宅医療サービス事業者、一般利用者が患者及びその家族、医師、看護師、ケアマネージャ等となっている。

このように、IoT においては、多くの関係者が存在し、かつ、複雑な関係となっているため、あらかじめ関係者の役割を整理して理解しておくことが必要である。

(3)対策例

①IoT 機器メーカや IoT システム・サービス提供者及び利用者の役割の整理

IoT 機器メーカ及び IoT システム・サービス提供者は、分野ごとに想定されるインシデントのシナリオを検討し、リスクの特定を行った上で、関係者ごとの役割を整理する。 整理した役割については、IoT システム・サービス提供者が公開する Web や配布するドキュメント（サービス約款・マニュアル等）、提供する IoT 機器の画面等に記載・表示を行い、関係者に対してサービス開始までに周知し、システム・サービスの利用者が確認した上で、サービスの利用が開始できるような仕組みを整備する。

要点21. 脆弱な機器を把握し、適切に注意喚起を行う

(1)ポイント

① ネットワーク上で IoT 機器を把握する仕組みを構築し、脆弱性を持つ IoT 機器の特定を行う。
② 脆弱性を持つ IoT 機器を特定した場合には、該当する IoT 機器の管理者へ注意喚起を行う。

(2)解説

IoT 機器に脆弱性がある場合には、その脆弱性を突いたサイバー攻撃が行われる可能性がある。そのため、IoT システム・サービスの提供者が、提供しているシステム・サービスのために設置した IoT 機器のうち、脆弱性を持つものがネットワーク上に存在していないかどうかを確認することが被害の抑制に有効である。そのためには、新たに設置する IoT 機器だけではなく、既存の IoT 機器を含めて、機器の情報を把握する手段を整備もしくは利用し、脆弱性を持つ機器を特定する必要ある。また、脆弱性が把握された場合には、該当する IoT 機器の管理者に対して、注意喚起を実施する必要がある。

(3)対策例

① 脆弱性を持つ IoT 機器を把握する仕組みの構築及び該当する IoT 機器の特定

ネットワーク上の IoT 機器の情報を把握する仕組みを整備もしくは利用し、その情報から脆弱性を持つ IoT 機器を特定する。

具体例を以下に示す。

- 提供するシステム・サービスのために設置した IoT 機器について、ネットワーク上で調査を行い、ファームウェアのバージョン情報等から脆弱性が存在しないか把握する。
- IoT 機器の管理者・設置場所についても把握する。例えば、IoT 機器の設置場所については、正しい設置場所から不正に移動されていないか確認することも考えられる。

② 脆弱性が把握された場合の注意喚起の実施

脆弱性が把握された場合には、事前に関係者間で合意した役割に従って、IoT 機器の管理者に対して適切に注意喚起を実施する。注意喚起の内容には、IoT 機器のファームウェアアップデートやネットワーク接続からの切り離し等に関するものが含まれる。

具体例を以下に示す。

- T-ISAC-J による注意喚起
  市販されている一部のブロードバンドルータにおいて、本来 LAN 側からのみアクセス可能な管理画面が WAN 側からもアクセス可能な脆弱性が存在し、さらに、ルータの管理者 ID・パスワードが出荷時の共通的な設定から変更されていないものがインターネットに接続されるという状況の中、海外からのサイバー攻撃に利用され、不正アクセスやフィッシング等の被害が発生した。
  こうした被害を受けて、T-ISAC-J では、ルータ等のネットワーク機器が保有する脆弱性と脅威に関して、インターネット経由で脆弱性を有する機器の調査を行い、脆弱性保有機器検出の精度向上と利用者特定の効率化を図りながら、インターネット接続サービスの一般利用者に対する注意喚起を実施し、最終的にインターネット上の脆弱性保有ルータ数の削減を実現した。

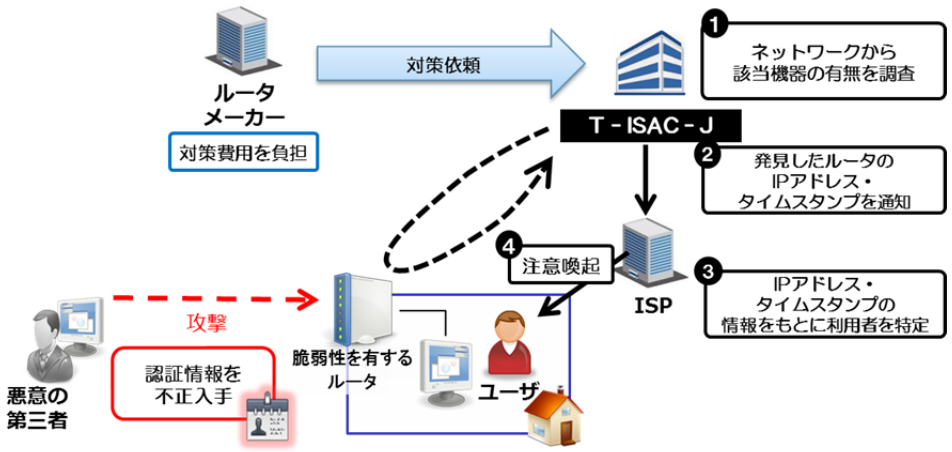


図 15 ルータの脆弱性を突いた攻撃への注意喚起

- JPCERT/CC による注意喚起
  JPCERT/CC の情報提供サイトにおいて、「注意喚起」ページ等を設け、システム・サービスの提供者等に対して注意喚起を実施している。

第3章

一般利用者のためのルール

本章では、一般利用者のためのルールを記載します。

インターネットに接続する IoT（※1）機器が世の中に普及・増加し、一般利用者の方も日常生活の中で IoT 機器を利用するようになってきています。

IoT 機器を適切に取り扱わないと、IoT 機器の利用に不都合が生じるだけでなく、インターネット経由で機器が操作され、自分（所有者）やその家族等になりすまして不正利用されたり、自分や家族等のプライバシー情報が漏れたり、IoT 機器が悪用されて他の利用者に迷惑をかける、あるいは、犯罪に巻き込まれたりする可能性もあります。

そういったリスクの多くは、IoT 機器を利用する際に、簡単な注意を払うだけで回避することができます。

ここでは、一般利用者が IoT セキュリティ対策として留意すべき４つのルールをまとめましたので、これらに気を付けながら IoT 機器を安全に利用しましょう。

（※1）：IoT とは、”Internet of Things”の略で、「モノのインターネット」と呼ばれています。これまでインターネットに接続されてきたパソコンやスマートフォンに加えて、自動車や家電など様々なモノがインターネットにつながるようになってきています。IoT 機器とは、そうしたインターネットにつながるモノを指します。

ルール１）問合せ窓口やサポートがない機器やサービスの購入・利用を控える

- インターネットに接続する機器やサービスの問合せ窓口やサポートがない（もしくはサポート期限が切れた）場合、何か不都合が生じたとしても、適切に対処することが困難になります。また、インターネットに接続する機器のアップデート（※2）を適切に行うこともできないため、安全な状態で継続して機器やサービスを利用することができなくなります。（問合せ窓口やサポートがある機器やサービスの購入・利用を行って、機器の異常等、何か不都合が生じた場合は、問合せ窓口やサポートの連絡先へ直ちに知らせてください。）
- 問合せ窓口やサポートがない（もしくはサポート期限が切れた）機器やサービスの購入・利用は行わないようにしましょう。

（※2）：機器のアップデートとは、機器の不具合の改善や不正利用の防止を目的として、機器をインターネット経由で最新の状態に更新することです。

ルール２）初期設定に気をつける

- インターネットに接続する機器のパスワードが他の人に漏れると、インターネット経由で機器が乗っ取られ、自分（所有者）やその家族等になりすまして不正利用される恐れがあります。
- 機器を初めて使う際には、ID、パスワードの設定を行いましょう。パスワードの設定では、機器購入時のパスワードのままとしない、他の人とパスワードを共有しない、他のパスワードを使い回さない、生年月日等他の人が推測しやすいものは使わない等の点に気をつけましょう。
- インターネットに接続する機器の取扱説明書等を読んで、取扱説明書等の手順に従って、自分でアップデートを実施してみましょう。

ルール３）使用しなくなった機器については電源を切る

- 使用しなくなった機器や不具合が生じた機器をインターネットに接続した状態のまま放置すると、知らず知らずのうちにインターネット経由で機器が乗っ取られ、不正利用される恐れがあります。
- 使用しなくなった機器や不具合が生じた機器は電源を切りましょう。
  例えば、使用しなくなった Web カメラ（※3）やルータ（※4）等をそのまま放置せず、電源をコンセントから抜きましょう。

（※3）：Web カメラとは、インターネットに接続することができるカメラです。
（※4）：ルータとは、パソコンやスマート家電等の機器をインターネットへ接続させるための情報通信機器です。

ルール４）機器を手放す時はデータを消す

- 機器を捨てる、売る、貸し出すなど、機器を手放す場合は、機器に記憶されている情報の削除を行わないと、自分や家族等の利用者情報が漏洩する恐れがあります。
- 機器を手放す際は、自分や家族等の利用者のプライバシー情報が漏れないよう、情報を確実に削除しましょう。

第4章
今後の検討事項

本ガイドラインは、産学官で IoT の利活用を促進するため、「IoT 推進コンソーシアム」において、セキュリティ確保等の観点から求められる基本的かつ横断的に適用可能な取組を明らかにするため取りまとめた。IoT は、国民の日常生活から日本経済を支える社会基盤まで様々な分野に浸透し、将来にわたり利用が拡大していくこと、また新たな IoT 機器やサービスの出現が想定されることから、引き続き必要な検討を行っていくことが必要である。その項目例として以下を挙げる。

具体的な検討事項を下記に挙げる。

- リスク分析に基づく分野別の対策について
  IoT は、様々な分野に浸透していくことになるが、その分野それぞれにおいて求められるセキュリティのレベルは、自ずと異なってくる。例えば、簡易な情報サービスに使用される IoT 機器と、工場や社会インフラシステム等の安全に関わる分野で使用される IoT 機器では、求められるセキュリティレベル、セキュリティ対策の目的、優先度が異なる。多くの IoT 機器が利用されている、もしくは利用が想定される分野では、具体的な IoT の利用シーンを想定し、詳細なリスク分析を行った上で、その分野の性質、特徴に応じた対策を検討する必要がある。また、対策実施の判断が行えるよう、対策に掛かる費用と得られる効果を比較・評価するための手法等についての検討も必要である。

- 法的責任関係について
  IoT は、「1.4 対象読者」で示したとおり、機器メーカ、システム提供者、サービス提供者等、複数の関係者が相互に連携し、利用者にサービスが提供されることが多い。例えば、サイバー攻撃により被害が生じた場合、費用負担の観点も含めて誰がその対処を行うかなど、責任の在り方については、今後出現する IoT サービスの形態や、IoT が利用されている分野において規定されている法律等に応じて整理を行っていく必要がある。

- IoT 時代のデータ管理の在り方について
  IoT システムでは、企業の技術情報や、利用者のプライバシーを含む個人情報等のデータを取得・保持・管理・利用・廃棄を行う者又は場所が、サービスの形態により変わってくる。IoT システムの特徴を踏まえつつ、個人情報や技術情報等の重要なデータを適切に取得・保持・管理・利用・廃棄を行うことが必要であり、その具体的な方法について検討していく必要がある。

- IoT に対する総合的なセキュリティ対策について
  IoT 社会の健全な発展の実現には、既に実施されている、情報処理推進機構（IPA）のソフトウェアの脆弱性情報の発信・共有などの取組、情報通信研究機構（NICT）の IoT に対するサイバー攻撃の観測などのサイバーセキュリティの研究開発の取組、JPCERT/CC のコンピュータセキュリティのインシデントに関する報告の受付、対応などの取組、Telecom ISAC Japan(ICT ISAC Japan)の ICT 分野にお

けるサイバー攻撃に関する情報共有・分析などの取組に加え、一般利用者に対する IoT 機器のマルウェア感染に関する注意喚起などの取組について、官民連携による強化を検討する。

本ガイドラインは、上記のような検討事項の取り込みや、IoT を取り巻く社会的な動向、脆弱性・脅威事象の変化、対策技術の進歩等を踏まえて、今後、必要に応じて改訂を行っていく必要がある。

付録

本ガイドライン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 8 略称一覧

略語	名称
ATM	Automated Teller Machine 現金自動預け払い機
CCDS	Connected Consumer Device Security Council 一般社団法人重要生活機器連携セキュリティ協議会
CRYPTREC	Cryptography Research and Evaluation Committees 電子政府推奨暗号の安全性を評価・監視し、暗号技術の適切な実装法・運用法を調査・検討するプロジェクト
CSIRT	Computer Security Incident Response Team コンピュータセキュリティにかかるインシデントに対処するための組織
CSMS	Cyber Security Management System 制御システムセキュリティにおけるサイバーセキュリティマネジメントシステム
DAF	Dependability Assurance Framework for Safety-Sensitive Consumer Devices 一般利用者が使用する機器の信頼性を確保するための開発方法論
DoS	Denial of Service 提供するサービスを妨害したり停止させる攻撃
DDoS	Distributed Denial of Service 標的となるコンピュータに対して複数のマシンから大量の処理負荷を与えることでサービスを妨害したり停止させる攻撃
DRBFM	Design Review Based on Failure Mode 故障モードに基づく設計レビュー
EDSA	Embedded Device Security Assurance 組込み機器セキュリティ保証
HEMS	Home Energy Management System 家庭用エネルギー管理システム
HSM	Hardware Security Module 鍵管理や暗号化などのセキュリティ機能を提供する専用のハードウェア
ID	Identifier システムの利用者を識別するために用いられる番号等の識別子
IEC	International Electrotechnical Commission 国際電気標準会議
I/F	Interface コンピュータ等と他のコンピュータ・周辺機器等を接続するための規格や仕様（本ガイドラインでは、IoT 機器・システムと他の IoT 機器・システムを接続するための規格や仕様）
IoT	Internet of Things 情報社会のために、既存もしくは開発中の相互運用可能な情報通信技術により、物理的もしくは仮想的なモノを接続し、高度なサービスを実現するグローバルインフラ
IPA	Information-technology Promotion Agency, Japan 独立行政法人情報処理推進機構

略語	名称
ISAC	Information Sharing and Analysis Center 情報セキュリティ関連情報を共有・分析するセンター
ISMS	Information Security Management System 情報セキュリティマネジメントシステム
ISO	International Organization for Standardization 国際標準化機構
ISP	Internet Service Provider インターネットサービスプロバイダ
JPCERT/CC	Japan Computer Emergency Response Team Coordination Center 一般社団法人 JPCERT コーディネーションセンター 日本国内における情報セキュリティを脅かす事象（インシデント）への対応を推進する CSIRT 活動を国際的に連携する組織
JVN	Japan Vulnerability Notes 日本で使用されているソフトウェアなどの脆弱性関連情報とその対策情報を提供し、情報セキュリティ対策に資することを目的とする脆弱性対策情報ポータルサイト
LAN	Local Area Network 企業内、大学内、家庭内等の限定された範囲の中でコンピュータ等を接続した情報通信ネットワーク
NICT	National Institute of Information and Communications Technology 国立研究開発法人情報通信研究機構
OS	Operating System コンピュータを制御し、アプリケーションソフトウェア等がコンピュータ資源を利用可能にするための基本となるソフトウェア
OSS	Open Source Software ソースコードが無償で公開され、複製、再配布、改良等の自由が認められているソフトウェア
POS	Point of Sales 販売時点情報管理
SoS	System of Systems 異なる複数のシステムが互いに複雑な関係を持つシステム
TEE	Trusted Execution Environment IC カード管理技術の標準化組織の１つである Global Platform が定義する、認証された実行環境とそれに関わる API（アプリケーションプログラミングインタフェース）の仕様
T-ISAC-J	Telecom-ISAC Japan 一般財団法人日本データ通信協会 テレコム・アイザック推進会議 平成 28 年 7 月からは一般社団法人「ICT-ISAC」が業務を発展的に継承して活動
TLS	Transport Layer Security データを送受信する一対の機器間で通信を暗号化し、なりすまし等を防ぐセキュリティプロトコル
TPM	Trusted Platform Module コンピュータのマザーボードなどに装着される、セキュリティ関連の処理機能を実装した LSI チップ
TSP	Telematics Services Provider テレマティクスサービス（車両向けの無線通信サービス）を提供する企業
WAN	Wide Area Network 通信事業者が提供する広域通信網
WPA2	Wi-Fi Protected Access 2 WPA（Wi-Fi Protected Access）のセキュリティ強度を向上させ、AES 暗号に対応した無線 LAN の暗号化方式