スマートホームの安心・安全に向けた
サイバー・フィジカル・セキュリティ対策ガイドライン
（案）

産業サイバーセキュリティ研究会
スマートホーム SWG

令和２年７月

目次

1. はじめに

世の中の IT 化により、様々なライフスタイルやニーズに応じたサービスを IoT で実現するスマートホームは、IoT 機器の普及に伴い、急速な普及が見込まれている。

本ガイドラインは、スマートホームの提供事業者をはじめスマートホームの住まい手など幅広い関係者に、必要なセキュリティ対策をガイドすることで、スマートホームにおける安心で安全な暮らしを実現するための基本的な指針を示すものである。

さらに本ガイドラインは、スマートホームにおけるセキュリティ対策の考え方、ならびに各関係者が考慮すべき最低限のセキュリティ対策を示している。業種・業態に特化した、または詳細なセキュリティ対策の明示が必要な場合は、本ガイドラインや他のガイドラインを参考に、各々のセキュリティ対策を考案されたい。

1.1. ガイドラインを策定する目的

近年、サイバー空間とフィジカル空間を高度に融合させることにより、多様なニーズにきめ細かく対応したモノやサービスを提供し、経済的発展と社会的課題の解決を両立する超スマート社会である Society 5.0 への取り組みが進められている。

Society 5.0 では、フィジカル空間のセンサデバイスにより得られた膨大なデータがサイバー空間に集約され、データ群を解析・処理した結果がロボットなどを通して人間にフィードバックされることで、これまでに無かった新しい価値が産業や社会にもたらされる新たな「社会」を目指している。また、Society 5.0 の実現へ向け、様々なデータの「つながり」からの新たな製品やサービスなどのイノベーションが円滑に創出される産業社会、「Connected Industries」の形成も進められている。

本ガイドラインは、「Connected Industries」の重点分野の 1 つであるスマートライフ分野の核となるスマートホームに必要となるサイバーセキュリティ上の技術的な対策、および管理項目の明確化を目指すものである。

スマートホーム分野のガイドラインという観点では、実際の対象は一般住宅であり、IoT 機器やシステムのセキュリティを考慮した管理・運用がなされていないことが多い。また、IoT 機器の誤使用の可能性、サービスで必要となる個人情報の漏洩、サービスによってはサイバー攻撃が開錠や閉じ込めといったフィジカル空間の問題を引き起こす可能性もある。さらに、社会全体で考えると、IoT 機器が乗っ取られ踏み台として悪用されることも脅威となる。スマートホームでは、一般住宅の様々な IoT 機器がサイバー攻撃の対象となるため、その数は膨大となる。

本ガイドラインは、スマートホーム分野において、IoT 機器を通じた様々なサービスを受ける上で生じる、情報漏洩、サイバー攻撃、フィジカル空間への被害などに対するガイドを整備し、スマートホーム利用における住まい手の安心・安全の確保を目指す。

1.2. ガイドラインの対象者

本ガイドラインの対象者（ステークホルダー）は、以下の通りである。

(1) **スマートホーム向け IoT 機器の事業者**

スマートホーム向けの IoT 機器を開発・生産・販売する事業者である。例えば IoT 家電や監視カメラの製造元（ハードウェア開発業者、ソフトウェア開発業者）などがある。

(2) **スマートホーム向けの IoT 機器を遠隔から管理する事業者**

スマートホーム向けの IoT 機器を、インターネットなどの広域通信網を介して外部（遠隔）から管理する事業者である。例えば、IoT 機器のリモート設定支援サービスなどが含まれる。

(3) **スマートホーム向けのサービス事業者**

スマートホーム向けのサービスを開発・提供する事業者、およびサービスを提供するために連携する関連サービスの提供事業者である。例えば、テレビと連動した映像コンテンツ配信事業者や、その事業者が利用する事業者向けのクラウドサービスなどが挙げられる。

（サービスを行うサーバがクラウドで実現される場合には、クラウド上でデータを集約・分析する機能を提供するプラットフォーマと、そのデータに基づいてサービスを提供するサービサーが存在する）

(4) **スマートホームを供給する事業者**

IoT 機器の開発・生産は行わないが、IoT 機器や IoT 化された住宅設備を供給・設置する事業者である。例えば、スマートホームを提供するハウスメーカーやマンションデベロッパー、賃貸型の住宅の所有者（オーナー）などが挙げられる。

(5) **スマートホーム向けにメンテナンスやサポートを行う事業者**

スマートホーム向けのサービスや IoT 機器に関して、メンテナンスをはじめ、設置・設定・運用などを行う事業者である。これには、IoT 機器やサービスの選定、IoT 機器の交換・廃棄、解約などに関連する事業者を含む。例えば、IoT 機器の駆け付け修理サービスなどを提供する事業者が挙げられる。

(6) **スマートホーム化された分譲共同住宅・団地の管理組合や管理受託会社**

区分所有型の共同住宅や団地において、共用部分に設置された IoT 機器や共用部分のネットワーク回線を管理する者であり、IoT 機器を利用したサービスを受ける者としても位置付けられる。例えば、区分所有者によって組織された管理組合や、管理組合から管理業務を委託された管理受託会社が挙げられる。

(7) **スマートホーム化された賃貸住宅の所有者や管理受託会社**

賃貸型の共同住宅の共用部分に設置された機器や共用部分のネットワーク回線の管理者であり、IoT 機器を利用したサービスを受ける者としても位置付けられる。例えば、賃貸型の共同住宅の所有者（オーナー）や、所有者（オーナー）から管理業務を委託された管理受託会社が挙げられる。

(8) **スマートホームの住まい手**

スマートホームの居住者である。主として IoT 機器を利用したサービスを受ける者である。

1.3. 対象とするスマートホーム

本ガイドラインの作成時点（2019 年）時点で、国内外の文献調査を実施した範囲においては、スマートホームを明確に定義した国際規格は見つかっていない。現在、スマートホームの本格的な普及に向け各地で実証実験などが行われ、多くの事業者がスマートホームの具体化を進めている状況下においては、一意にスマートホームを定義することは極めて困難であると考えられる。

そこで本ガイドラインでは、スマートホームを「子育て世代、高齢者、単身者など、様々なライフスタイル／ニーズにあったサービスを IoT により実現する新しい暮らし」であるとして、IoT に対応した住宅設備・家電機器などが、サービスと連携することにより、住まい手や住まい手の関係者に便益が提供される住宅を、本ガイドラインの対象であるスマートホームとして独自に定義して取り扱う。

スマートホームにより提供される機能は多種多様となることが予想され、多くの場合、複数の機器やシステムによってスマートホームが構成されるものと考えられる。本ガイドラインが対象とするスマートホームの特徴は、直接的・間接的※に通信ネットワーク（インターネットなど）に接続する機器やサービスが連携するという点である。

※ 直接的とは、例えばスマートメーターの様に内部に通信機能を有し、ホームネットワークを介さずに通信ネットワークに接続するような接続形態を意味する。間接的とは、ホームネットワークなどの住居内の通信ネットワークに存在する通信機器を介して、インターネット等の広域通信ネットワークに接続するような接続形態を意味する。

一般的に、住宅はひとつの敷地に一世帯が居住する「戸建（個人住宅、専用住宅とも言う）」と、複数世帯が居住する「共同住宅」の2つに分類されることから、スマートホームのネットワーク構成例として、「図 1.戸建住宅のネットワークの例」、および「図 2.共同住宅のネットワーク構成の例」を示す。

1.3.1. 戸建住宅の例

戸建住宅のネットワーク構成例を「図 1.戸建住宅のネットワークの例」に示す。住宅の設計・施工によって、住宅設備などの IoT 機器が予め設置される場合もあるが、入居後に住まい手が IoT 機器やサービスを導入し、サービスを受けている状態を想定したものを示している。

なお、図 1 に示す宅内のネットワークは、複数のネットワークによる階層構造をとる場合もあるが、本ガイドラインにおいてはスマートホームのモデルを単純化するため、図 1 の様な表現としている。

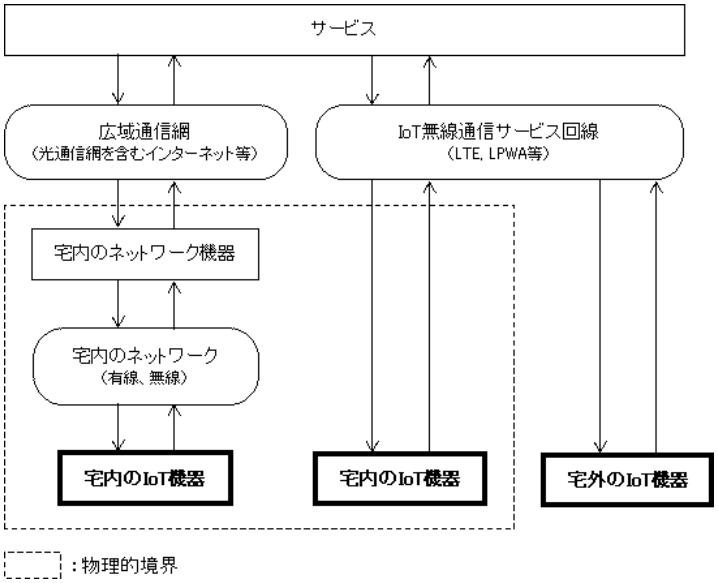

図 1.戸建住宅のネットワークの例

住まい手が、IoT 機器を介したサービスを受けている状態において、関連するステークホルダーを「表1　戸建住宅に関するステークホルダー」に示す。

表 1.戸建住宅に関するステークホルダー

サービス・機器等	関連するステークホルダー
サービス	・ スマートホーム向けのサービス事業者 ・ スマートホーム向けにメンテナンスやサポートを行う事業者
広域通信網, IoT 無線通信サービス回線	（通信インフラ事業者）
宅内のネットワーク	（スートホームを供給する事業者から引き渡されるまで） ・ スートホームを供給する事業者 （引き渡し後） ・ スマートホームの住まい手 ・ スマート向けにメンテナンスやサポートを行う事業者
IoT 機器	（引き渡されるまで） ・ スートホームを供給する事業者 ・ スマートホーム向け IoT 機器の事業者 （スートホームを供給する事業者から引き渡し後） ・ スマートホーム向け IoT 機器の事業者 ・ スマートホーム向けの IoT 機器を遠隔から管理する事業者 ・ スマートホーム向にメンテナンスやサポートを行う事業者 ・ スマートホームの住まい手

1.3.2.　共同住宅の例

共同住宅のネットワーク構成例を「図 2.共同住宅のネットワーク構成の例」に示す。共同住宅の設計・施工によって、共用部分、また住戸における住宅設備などの IoT 機器が予め設置される場合もあるが、入居後に住まい手が IoT 機器やサービスを導入し、サービスを受けている状態を想定したものを示している。

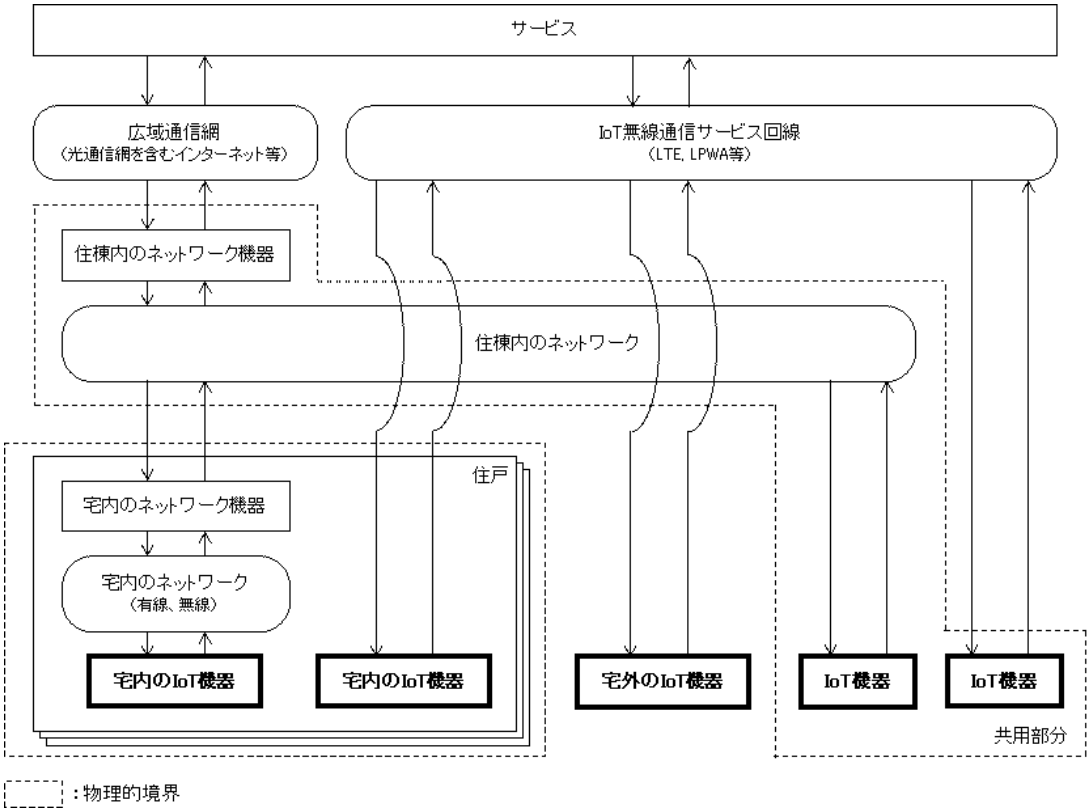

図 2.共同住宅のネットワーク構成の例

住まい手が IoT 機器を介し、また共同住宅の共用部分の IoT 機器を介して、サービスを受けている状態において、関連するステークホルダーを「表 2.共同住宅でのスマートホームに関するステークホルダー」に示す。

表 2.共同住宅でのスマートホームに関するステークホルダー

サービス・機器等	関連するステークホルダー
サービス	・ スマートホーム向けのサービス事業者 ・ スマートホーム向けにメンテナンスやサポートを行う事業者
広域通信網, IoT 無線通信サービス回線	（通信インフラ事業者）
共用部分のネットワーク	（共用部分のネットワークの管理主体[1]に引き渡されるまで） ・ スートホームを供給する事業者 （引き渡し後） ・ スマートホーム化された分譲共同住宅・団地の管理組合や管理受託会社 ・ スマートホーム化された賃貸住宅の所有者や管理受託会社
共用部分の IoT 機器[2]	（共用部分の IoT 機器の管理主体に引き渡されるまで） ・ スートホームを供給する事業者

1 管理主体とは、スマートホーム化された分譲共同住宅・団地の管理組合や管理受託会社、またはスマートホーム化された賃貸住宅の所有者や管理受託会社 である。

2 共用部分の IoT 機器とは、宅配ボックス（満庫通知）、緊急地震速報などである。

サービス・機器等	関連するステークホルダー
	・ スマートホーム向け IoT 機器の事業者 （引き渡し後） ・ スマートホーム向け IoT 機器の事業者 ・ スマートホーム向けの IoT 機器を遠隔から管理する事業者 ・ スマートホーム向けにメンテナンスやサポートを行う事業者 ・ スマートホーム化された分譲共同住宅・団地の管理組合や管理受託会社 ・ スマートホーム化された賃貸住宅の所有者や管理受託会社
住戸内のネットワーク	（スートホームを供給する事業者から引き渡されるまで） ・ スートホームを供給する事業者 （引き渡し以降） ・ スマートホームの住まい手 ・ スマートホーム向けにメンテナンスやサポートを行う事業者
住戸内の IoT 機器	（スートホームを供給する事業者から引き渡されるまで） ・ スートホームを供給する事業者 ・ スマートホーム向け IoT 機器の事業者 （引き渡し後） ・ スマートホームの住まい手 ・ スマートホーム向け IoT 機器の事業者 ・ スマートホーム向けの IoT 機器を遠隔から管理する事業者 ・ スマートホーム向にメンテナンスやサポートを行う事業者

1.4. ガイドライン作成の背景

1.4.1. スマートホームが社会にもたらすもの

持続可能な社会を構築するために、生活者や住空間などの情報を取り扱うシステムと住まい手、住まいのモノ・サービス提供者を含む全ての参加者が効率よく連携し、互いに支え合いながら限られた資源を最大限活かし、社会の幸せ、住まい手の幸せを実現する一つの形態であるスマートホームは、産業界においても新たな成長領域として大きく注目され、経済産業省がスマートホームの社会実装を見越したホームエネルギー管理システム（HEMS）の実証を行うなど、国内での市場形成・普及に向けて活動している状況にある。

スマートホームは、子育て世代、高齢者、単身者など、様々な住まい手のライフスタイル／ニーズにあったサービスを IoT 技術で実現する。家電・AV 機器・IT 機器など、あらゆる機器がネットワークに接続され、機器によって取得された住まい手の生活情報がクラウド上に集約・分析される。そして、クラウドサービスとつながる(連携する)ことで、住まい手に便利で快適な暮らしを提供する。さらには、高齢者世帯が増加していながら住宅や近隣住民・地域コミュニティによる互助・サポートが希薄化している社会状況にあって、公的・私的なサービスとしての支援（育児・見守りなど）が住まい手の健康管理やホームセキュリティの充実に繋がり、社会課題の解決・低減に大きく寄与すると考えられている。

スマートホームが、住まい手の生活情報と多様なサービスとをつなぐことで、住まいにおける新たな選択肢（社会サービス）が生まれ、社会課題の解決と住まい手の幸せの両方を実現することが期待されている。

1.4.2. スマートホームを取り巻く環境や状況

近年、IoT が普及したことによって、一般消費者の生活は大きく変化している。従来の家電製品や住設機器は、通信機能を持たないか、または専用のネットワークによるクローズドな環境内での通信が利用されている場合が多かった。

しかし、現在ではインターネット等の汎用な規格によるオープンなネットワークへの接続機能を有する家電や住設機器が急速に増加している。これにより、機器同士が相互に通信することで、様々な利便な機能が提供されている。例えば、スマートフォンやスマートスピーカの音声アシスタント機能によって、住宅内の AV 機器やスマート家電を操作し制御できるようになった。また、住設機器についても汎用の通信プロトコルの利用や、IoT ゲートウェイ装置によりインターネットなどオープンなネットワークからの制御が可能となった。

一方で、適切なセキュリティ対策がなされていない IoT 機器へのサイバー攻撃の事例が増加しており、多数の IoT 機器とサービスにより実現されるスマートホームに対するサイバーセキュリティ対策が急務となっている。

スマートホーム化により、従来よりもサイバー攻撃の対象となる住宅内の機器が拡大すると想定される。また、日本国内の世帯数はおよそ 5300 万世帯 [3]であり、攻撃対象の数も非常に膨大になると想定される。セキュリティレベルが一部でも低いところがあれば、攻撃が成功するため、大規模なサイバー攻撃の踏み台としてスマートホームが利用される懸念もある。

米国のある調査 [4]によれば、一部の製品やサービスは、セキュリティ上のリスクを認識しながらも利用せざるを得ない状況にあるまで生活に根付いているものもある。スマート家電や IoT は生活を便利にする反面、サイバーセキュリティ上のリスクも多く含んでおり、その対策が必要不可欠な状況にある。

1.4.3. サイバー攻撃の事例

IoT 機器が急激に普及する現在、一般の住宅向けの IoT 機器へのサイバー攻撃の事例や脆弱性も多数報告されており、スマートホームのセキュリティ対策に大きく関係すると考えられる。例えば無線 LAN や Bluetooth の脆弱性や、web インターフェースの脆弱性など、IoT 機器で標準的、広範囲に利用される通信技術に関する脆弱性であり、影響を受ける機器の種類と数量は極めて多いと想定されるものである。

---

[3] 平成 27 年国勢調査 / 総務省統計局

[4] IoT Value/Trust Paradox（IoT の価値と信用のパラドックス） /米 CISCO 社
スマート家電を含む IoT で収集され共有されるデータが安全だと信じていると回答した人は 9%。
一方、42%はリスクを認識しながらもデバイスやサービスの利用中止をしたくないと回答

本ガイドラインでは、読者の参考になるように、スマートホームで発生しうる脅威に関する脅威や脆弱性の、具体的な事例を「添付 D サイバー攻撃の事例」に示す。

なお、添付 D では、事例を「攻撃の対象」という観点で以下の 3 つに分類し、示される脅威や脆弱性の事例がどのような事象に繋がるのかを整理している。

1) スマートホームを構成する通信基盤やサービス基盤が不正にアクセスされ、システムの機能低下・停止や意図しない第三者攻撃への加担などに繋がる事例
2) スマートホームを構成する IoT 機器などが不正にアクセスされ、住設機器が不正に操作されたり、意図せず施錠が開錠されたりするなど、住居自体への物理的な損害や住まい手の生命・財産を侵害する事例
3) IoT 機器やサービスを通じて住まい手の位置情報やカメラ映像などの個人情報が不正に取得され、プライバシーや生命・財産の侵害に繋がる事例

1.5. サイバー・フィジカル・セキュリティ対策フレームワークとの関係

本ガイドラインを検討したワーキンググループは、産業サイバーセキュリティ研究会 WG1（制度・技術・標準化）の下で分野別検討組織に位置づけられている。この産業サイバーセキュリティ研究会 WG1（制度・技術・標準化）では、Society 5.0（仮想空間と現実空間を高度に融合させたシステムにより、経済発展と社会的課題の解決を両立する、人間中心の社会（Society））における新たなサプライチェーンの信頼性の確保に向けた『サイバー・フィジカル・セキュリティ対策フレームワーク（以下、CPSF）』[5]を策定した。

フレームワークでは、Society 5.0 へ向けた産業・社会の変化に伴うサイバー攻撃の脅威の増大に対し、リスク源（サイバーリスクを生じさせる原因となりうる要素）を適切に捉え、検討すべきセキュリティ対策を漏れなく提示するために、3 層構造アプローチを提示している。具体的には、「①企業間のつながり」「②フィジカル空間とサイバー空間のつながり」「③サイバー空間におけるつながり」の 3 層ごとに、インシデント・リスク源・対策要件を整理するとともに、セキュリティ対策要件ごとに対策例も提示している。

[5] サイバー・フィジカル・セキュリティ対策フレームワーク Version 1.0（平成 31 年 4 月 18 日）

サイバー空間におけるつながり

【第３層】

- 自由に流通し、加工・創造されるサービスを創造するためのデータの信頼性を確保

フィジカル空間とサイバー空間のつながり

【第２層】

- フィジカル・サイバー間を正確に“転写“する機能の信頼性を確保
  （現実をデータに転換するセンサや電子信号を物理運動に転換するコントローラ等の信頼）

企業間のつながり

【第１層】

- 適切なマネジメントを基盤に各主体の信頼性を確保

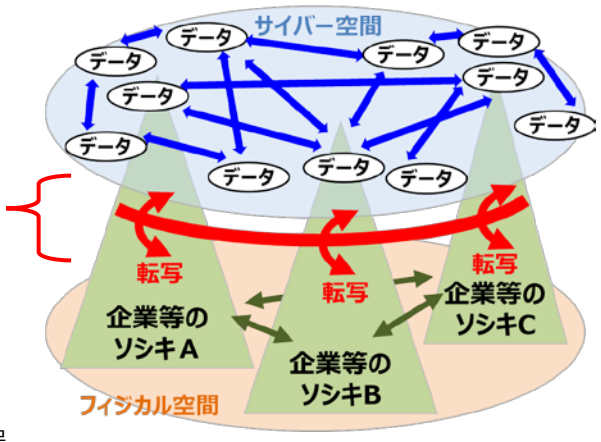

図 3.CPSF サイバー・フィジカル・セキュリティ対策フレームワークの3層構造

［引用］サイバー・フィジカル・セキュリティ対策フレームワーク/経済産業省

本ガイドラインは、CPSF で導出されたリスク源や対策要件を最大限に踏襲し、まとめるものである。

2. セキュリティ対策の検討の考え方

本章では、1章に示した「1.2 ガイドラインの対象者（ステークホルダー）」や「1.3 対象とするスマートホーム」を前提として、各ステークホルダーに向けたセキュリティ対策として表現するまでの考え方を示す。

2.1. 各ステークホルダーに対するセキュリティ対策を導出する流れ

本書は、以下の段階を踏んで、各ステークホルダーに対するセキュリティ対策のガイドを導出している。

(1) 「1.3 対象とするスマートホーム」に基づいて、セキュリティ上の脅威や想定されるインシデント、関連する脆弱性を検討する為の想定シーンと脅威を設定する。
→ 「3章 想定シーンと脅威」に示す

(2) (1)で設定した想定シーンと脅威より、想定されるインシデント、リスク源（脅威、脆弱性）を抽出し、ガイドラインの対象者（ステークホルダー）毎にまとめる。
→ 「添付A 機能／想定されるセキュリティインシデント／リスク源／対策要件」に結果を示す。

(3) 対策要件について対策例を示すと共に、対策例を他の標準や規格と対比する。
→ 「添付B 対策の整理と、国際規格などの各種規格との対応」に結果を示す。

(4) 2)で導出された脆弱性に基づいて、対象となるステークホルダー毎に対策要件を整理する。また、それぞれを要約し、各スークホルダーに必要な対策のガイドを導出する
→ 「添付C ステークホルダーに向けたガイドと対策要件の対応関係」に結果を示す。

(5) (4)にて、対象となるステークホルダー毎に導出したセキュリティ対策に対し、補足説明を加えて、ガイドライン文書として整理する。
→ 「4章 スマートホームに求められる最低限のセキュリティ対策」に示す。

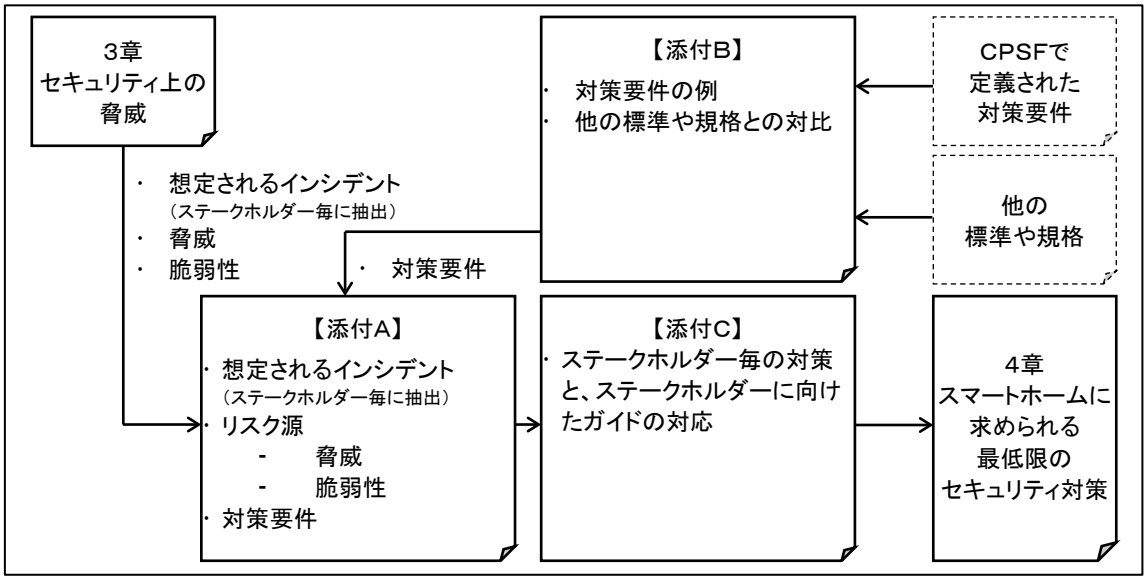

図 4.セキュリティ対策の検討

2.2. 脆弱性の要素

CPSF では、バリュークリエイションプロセスに関与する構成要素を「ソシキ」、「ヒト」、「モノ」、「データ」、「プロシージャ」、「システム」の6つの要素に分解し、その構成要素について各リスク源に対する対策要件および具体的な対策例を検討している。

本ガイドラインでは、これをスマートホームに適用するため以下の事由から要素を「管理面(ソシキ，ヒト，データ，プロシージャ)」と、「機器・システムの機能面(モノ，システム，データ)」に分けて分析している。

(1) ガイドラインとしてセキュリティ対策を整備するためには、「ソシキ」の分析対象である体制の有無、「ヒト」の能力、「プロシージャ」の手続き(社内規定など)は、事業者に依らず揃っていることが前提となる。しかしながら、各事業者の体制や業務プロセスが揃っている訳ではないため、「ソシキ」、「ヒト」、「プロシージャ」を、管理面として取り扱う。

(2) 「モノ」、「システム」については、ハードウェア(機器など)やソフトウェアで実現される機能、また複数のハードウェアやソフトウェアで構成するシステムについての機能面として取り扱う。これは理解を促すため、管理面に対する機能面という分類を示すことで理解を促すことも意図した。

(3) 「データ」については、「モノ」、「システム」により処理されるだけでなく、どのように取り扱われるか、管理面も問題となることから、機能面と管理面の両方で取り扱う。

2.3. 想定されるインシデントと脅威から脆弱性を抽出する観点

本ガイドラインでは、主として住まい手に影響を及ぼすリスク源を抽出することを想定して想定シーンと脅威を設定している。このリスク源をステークホルダー毎に示し、各ステークホルダーが個々にセキュリティ対策を図ることで、安心で安全なスマートホーム実現を目指していくものである。

各ステークホルダーにおけるリスク源の抽出に関する観点を下表にまとめる。

表 3.ステークホルダーとリスク源抽出の観点

ステークホルダー	リスク源抽出の観点	説明
スマートホーム向け IoT 機器の事業者	・ IoT 機器の機能	・ IoT 機器の機能に関する脆弱性が、住まい手に影響を及ぼしうるため
スマートホーム向けの IoT 機器を遠隔から管理する事業者	・ IoT 機器の管理 ・ 遠隔から IoT 機器を管理するシステム	・ IoT 機器の管理は、住まい手に影響を及ぼしうるため ・ 遠隔から IoT 機器を管理するシステムの脆弱性は、IoT 機器へのアクセスにつながることで、住まい手に影響を及ぼしうるため
スマートホーム向けのサービス事業者	・ 住まい手から収集したデータの取り扱い ・ IoT 機器の制御や、IoT 機器を通じた可視化などのデータの信頼性	・ 住まい手または住宅から収集したデータの漏えい・改ざんにより、住まい手やサービスに影響を及ぼしうるため ・ IoT 機器の制御のためのデータや、IoT 機器を通じた可視化などのデータの漏えい、改ざんは、住まい手に影響を及ぼしうるため

ステークホルダー	リスク源抽出の観点	説明
スマートホームを供給する事業者	・ スマートホームである住宅の施工時、またはリフォームなどの際における IoT 機器などの選定、設置	・ IoT 機器の選定や設置は、住まい手やサービスに影響を及ぼしうるため
スマートホーム向けにサポートやメンテナンスを行う事業者	・ 住戸内ネットワークに接続された機器	・住まい手が IoT 機器を通じてサービスを受けるためのサポートや IoT 機器の設定やメンテナンスは、住まい手やサービスに影響を及ぼしうるため
スマートホーム化された分譲共同住宅・団地の管理組合や管理受託会社	・ 共用部分のネットワーク、および共用部分のネットワークに接続された IoT 機器の管理	・共用部分のネットワーク、および共用部分のネットワークに接続された機器の管理が、住まい手に影響を及ぼしうるため
スマートホーム化された賃貸住宅の所有者や管理受託会社	・ 共用部分のネットワーク及び共用部分のネットワークに接続された IoT 機器の管理	・ 共用部分のネットワーク、および共用部分のネットワークに接続された機器の管理が、住まい手に影響を及ぼしうるため
スマートホームの住まい手	・ IoT 機器の選定、設置、設定実施、廃棄やサービスの解約の主体	・ IoT 機器内やスマートホーム向けのサービスに関連する事業者が保持している住まい手に関連した情報についてもデータ消去が必要であるため

3. スマートホームにおけるセキュリティ上の脅威

スマートホームにおける特徴的なリスク源（脅威、脆弱性）と、その対策要件の検討を行う上で必要となる想定シーンと脅威の整理を行う。

CPSF におけるスマートホームでは、スマートホームの特徴として「家電や防犯カメラ、健康器具などがインターネットに繋がり IoT 機器となっていく中で、日常生活に係るデータがネットワーク上でやりとりされるとともに、ネットワークを介して IoT 機器の操作も可能となる等、サイバーとフィジカルの転写機能の信頼が重要」、また「IoT 機器のメンテナンスや状態の管理について、明確な管理者が定まらないことが多い。」と示されている。

本ガイドラインでは、この特徴を考慮し、CPSF の観点から主として住まい手に影響を及ぼすリスク源を抽出することを想定して想定シーンと脅威を設定した。なお、本ガイドラインでは想定シーンを大きく2つの観点で示している。一つはデータに着目したシーンである。もう一方は、物理的なモノを含めた管理上の脅威である。

以下に、各々の想定シーンと脅威について解説する。

3.1. データと脅威

3.1.1. スマートホームからサイバー空間へのデータ転送

スマートホームのセンサデータをサイバー空間に送る想定シーンである。具体的には、IoT 機器が電力使用量や健康管理に関わるデータをサイバー空間に送り、サイバー空間に送られたデータの分析や加工が行われるというモデルにおいて、IoT 機器がデータをサイバー空間に送る部分を想定したものである。センサデータをサイバー空間に送る時のデータの流れを、戸建住宅と共同住宅のそれぞれで示す。

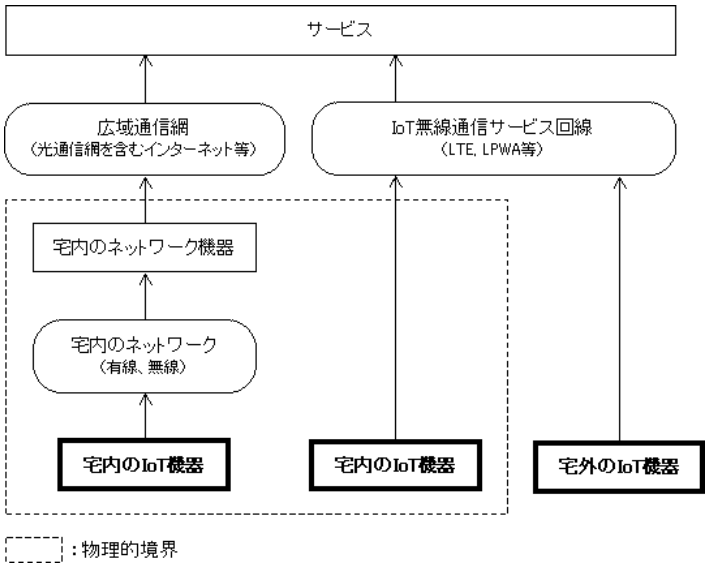

図 5.スマートホームからサイバー空間へ（戸建住宅の場合）

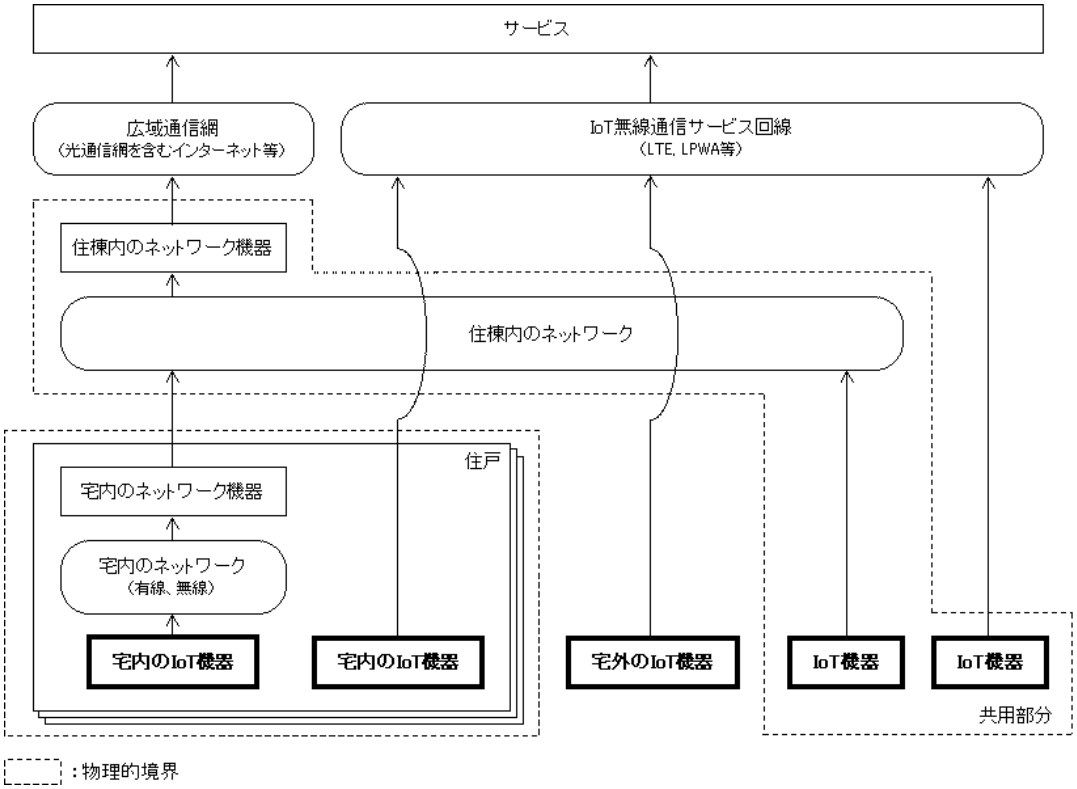

図 6.スマートホームからサイバー空間へ（共同住宅の場合）

想定シーンと脅威は以下の通りである。

概要	センサにより、スマートホームのデータ（家・住宅設備に関連するデータや住まい手に関連するデータ）をサイバー空間へ送る機能の想定シーンを整理する。 ・ 戸建住宅でのデータ経路は、IoT 機器、宅内のネットワーク、広域通信網、サービスの経路を経る。 ・ 共同住宅でのデータ経路は、住戸内においては、宅内 IoT 機器、宅内のネットワーク、住棟内ネットワーク、広域通信網、サービスの経路を経る。一方、共用部分においては、機器、住棟内のネットワーク、広域通信網を介してサービスにアクセスするか、機器から IoT 無線通信サービスを介してアクセスする。 ・ IoT 無線通信サービス回線を利用する場合のデータ経路は、IoT 機器、IoT 無線通信サービス回線、サービスとなる。
前提条件	・ 住戸内の IoT 機器は、住まい手自身が購入、または住まい手の入居前にスマートホームを供給する事業者により据え付けられている。 ・ 共用部分の IoT 機器は、分譲共同住宅・団地の管理組合や管理受託会社、または賃貸住宅の所有者や管理受託会社管理組合または管理受託会社によって据え付けられることもある。 ・ IoT 機器は想定された用途・用法に基づき設置、設定、運用され、フィジカル空間の物理事象を読み取り、一定のルールに基づいて正常にデジタル情報へ変換する。 ・ 戸建住宅では、宅内のネットワーク、および宅内のネットワークに接続されている他の機器は正常に設置、設定、運用されている。

	・ 共同住宅では、住棟内ネットワーク、住棟内ネットワークに接続されている他の機器、宅内のネットワーク、および宅内のネットワークに接続されている他の機器は正常に設置、設定、運用されている。 ・ センサデータを受け取るサービス、および他のサービスは正常に設定、運用されている。
基本フロー	1) IoT 機器により収集されたフィジカル空間の物理事象は、一定のルールに基づきデジタル情報に変換される。
	【戸建住宅の場合】 1) デジタル情報に変換されたデータは、宅内のネットワークに送られ、広域通信網回線を通じ、サイバー空間にあるサービスに送られる。
	【共同住宅(宅内の IoT 機器)の場合】 1) デジタル情報に変換されたデータは、宅内のネットワークに送られ、住棟内ネットワーク、ネットワーク広域通信網回線を通じ、サイバー空間にあるサービスに送られる。
	【共同住宅(共用部分の IoT 機器)の場合】 1) デジタル情報に変換された共用部分のデータは、住棟内のネットワークに送られ、ネットワーク広域通信網回線を通じ、サイバー空間にあるサービスに送られる。
	【IoT 無線通信サービスを利用する場合】 1) デジタル情報に変換されたデータは、IoT 無線通信サービス回線を通じ、サイバー空間にあるサービスに送られる。

想定されるインシデント、脅威、脆弱性について以下にまとめる。

想定されるインシデント	・ IoT 機器に対する攻撃により、センサデータを利用するサービスにおいて、正常に分析や加工ができない。 ・ IoT 機器からサイバー空間へ送られる個人情報などを含むデータが、通信経路において改ざんされ、センサデータを利用するサービスにおいて、正常に分析や加工ができない。 ・ IoT 機器からサイバー空間へ送られる個人情報などを含むデータが、通信経路において暴露される。 ・ 「添付 D サイバー攻撃の事例」の(3)に示すように、IoT 機器やサービスを通じて住まい手の個人情報などが搾取され、人体へのダメージや財産が侵害される。
脅威	・ IoT 機器が攻撃を受け、センサでの測定ができない/デジタル情報への変換ができない/データをサイバー空間へ送れないなど、センサデータをサイバー空間に送る機能が正しく動作しない。または、意図しないデータをサイバー空間に送る。 ・ IoT 機器からサイバー空間へ送るデータが通信経路において改ざんされる。 ・ IoT 機器からサイバー空間へ送るデータが通信経路において暴露される。
脆弱性	・ IoT 機器が、暗号通信など、十分なセキュリティ機能を実装していない。 (U1_V.1) ・ IoT 機器の脆弱性対策が行われていない。 (U1_V.2) ・ IoT 機器が、想定された用途・用法に基づき設置・設定・運用されていない。 (U1_V.3)

	・ 戸建住宅では、宅内のネットワーク、および宅内のネットワークに接続されている他の機器が、想定された用途・用法に基づき設置・設定・運用されていない。	(U1_V.4)
	・ 共同住宅の共用部分**に設置された IoT 機器では、住棟内ネットワーク、住棟内ネットワークに接続されている他の機器、宅内のネットワーク、宅内のネットワークに接続された他の機器が、想定された用途・用法に基づき設置・設定・運用されていない。**	(U1_V.5)
	・ 宅内のネットワークに接続されている他の機器、住棟内のネットワークに接続されている機器について、広域通信網への接続が管理されていない。	(U1_V.6)
	・ サービスを実行する機器の信頼性が低い、サーバ等の機器が攻撃を受ける、脆弱性対策が行われていない。	(U1_V.7)
	・ サービスを実行する機器の交換や廃棄時、IoT 機器内のデータ消去を確認していない。 ・ 利用していたサービスや、IoT 機器を遠隔から管理するシステムなど交換時、個人情報などのデータ消去が確認されていない。	(U1_V.8)
	・ サービスの運用において、個人情報を含むデータの管理ポリシーが提示されていない。	(U1_V.9)

※「脆弱性」部のカッコ内は、セキュリティ対策検討のための識別子（後述「添付 A」の想定利用シーンと脅威における脆弱性 ID）である。

3.1.2. サイバー空間からスマートホームへのデータ転送

IoT 機器が、サイバー空間よりデータを受けてサービスを提供するケースである。具体的には、スマートホームのセンサデータをサイバー空間で分析・加工した結果のデータ、またはサイバー空間にあるスマートホーム以外のデータについて IoT 機器を通じサービスを提供するモデルにおいて、サイバー空間のデータを受けることで IoT 機器がサービスを提供する部分を想定シーンとしたものである。

ここで、サイバー空間にあるスマートホーム以外のデータによるサービスの提供とは、例えばスマートフォンを操作することによりサーバ空間を通じて宅内の IoT 機器を操作する、道路交通情報を受ける、地域情報受けるなどによるサービス提供を意図したものである。

これらサービスでは、IoT 機器単独でサービスを提供する場合と、複数の IoT 機器や他のシステムが連携してサービスを提供する場合がある。

サイバー空間で分析、加工されたデータによりサービスが提供される時のデータの流れを、戸建住宅と共同住宅でそれぞれ示す。

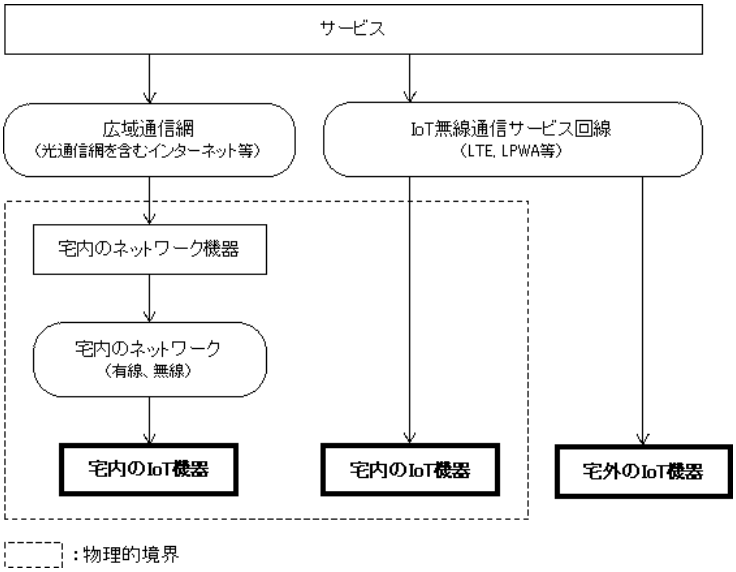

図 7.サイバー空間から IoT 機器へサービス提供（戸建住宅の場合）

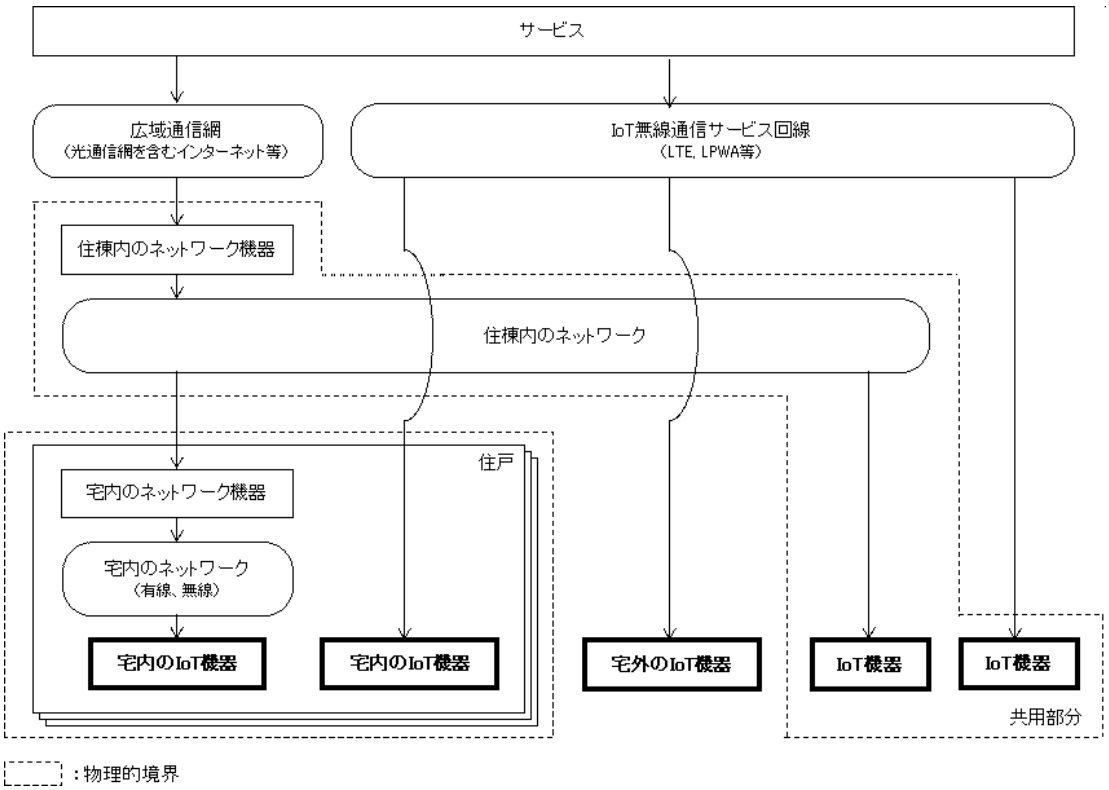

図 8.サイバー空間から IoT 機器へサービス提供（共同住宅の場合）

想定シーンと脅威は以下の通りである。

概要	スマートホームで収集されサイバー空間で分析・加工されたデータによるサービス、スマートホーム以外で収集されたデータによるサービス、住まい手や住まい手に関連する者がサイバー空間を介して IoT 機器などの操作を可能とするサービ

	スの想定シーンと脅威を整理する。 ・ 戸建住宅でのデータ経路は、サイバー空間より、広域通信網、宅内のネットワーク、IoT 機器の経路を経る。 ・ 共同住宅でのデータ経路は、サイバー空間、広域通信網、住棟内ネットワーク、宅内のネットワーク、IoT 機器の経路を経る。 ・ IoT 無線通信サービス回線を利用する場合のデータ経路は、サイバー空間、広域通信網、IoT 機器となる。
前提条件	・ 住戸内の IoT 機器は、住まい手自身が購入、または住まい手の入居前にスマートホームを供給する事業者により据え付けられている。 ・ 共用部分の IoT 機器は、分譲共同住宅・団地の管理組合や管理受託会社、または賃貸住宅の所有者や管理受託会社管理組合または管理受託会社によって据え付けられることもある。 ・ IoT 機器は、想定された用途・用法に基づき設置、設定、運用されており、サイバー空間から受け取るデータは IoT 機器が意図した通り処理される。 ・ 戸建住宅では、宅内のネットワーク、および宅内のネットワークに接続されている他の機器は正常に設置、設定、運用されている。 ・ 共同住宅では、住棟内ネットワーク、および住棟内ネットワークに接続されている他の機器は正常に設置、設定、運用されている。 ・ IoT 機器が他の機器やシステムと連携してサイバー空間からのデータをフィジカル情報へ変換される場合は、他の機器やシステムが想定された用途・用法に基づき設置、設定、運用されている。 ・ スマートホームで収集されたセンサデータを受け取るサービス、およびスマートホーム以外のデータによるサービスは意図された通り設定、運用されている。
基本フロー	1) サービスから、スマートホームの IoT 機器に向けてデータが伝送される。 【戸建住宅の場合】 1) サービスから、スマートホームの IoT 機器に向けてデータが伝送される。 2) サイバー空間から受け取るデータは、広域通信網を介し、宅内のネットワークに送られ、IoT 機器が受け取る。 【共同住宅の場合】 1) サービスまたは遠隔の機器から、スマートホームの IoT 機器に向けてデータが伝送される。 2) サイバー空間から受け取るデータは、広域通信網、住棟内ネットワークを介し、宅内のネットワークに送られ、IoT 機器が受け取る。 【IoT 無線通信サービスを利用する場合】 1) サイバー空間から受け取るデータは、IoT 無線通信サービス回線を介し、IoT 機器が受け取る。

想定されるインシデント、脅威、脆弱性について以下にまとめる。

想定されるインシデント	・ 住戸内の IoT 機器や共用部分の IoT 機器に対する攻撃により、サイバー空間から受け取ったデータ処理の如何に関わらず想定されない動作をする。 ・ サイバー空間から受け取るデータが通信経路において改ざんされ「添付 D サイバー攻撃の事例」の(2)に示すように、スマートホームを構成する IoT 機器などが不正にアクセスされ、主に住戸への物理的な損害や住まい手の人

	体へのダメージ、財産を侵害されるなど、想定されていない動作をする。 ・ サイバー空間から受け取るデータが、通信経路において暴露され、「添付 D サイバー攻撃の事例」の(1)に示される様に、スマートホームを構成する通信基盤やサービス基盤が不正にアクセスされ、システムの機能低下・停止など意図しない動作が行われるなど、情報が漏えいする。
脅威	・ IoT 機器が攻撃を受け、サイバー空間からデータを受け取れない/サイバー空間から受け取った通信データを処理できない/想定されない動作をする。 ・ サイバー空間から受け取る通信データが、通信経路において改ざんされる。 ・ サイバー空間から受け取る通信データが、通信経路において暴露される。
脆弱性	・ IoT 機器が、暗号通信など、十分なセキュリティ機能を実装していない。 (U2_V.1) IoT 機器が、住宅・住戸内の他の機器やシステムと連携する場合は、他の機器やシステムにおいても十分なセキュリティ機能が実装していない。 ・ 暗号化されていないによる無線通信など、IoT 機器の脆弱性対策が行われていない。 (U2_V.2) ・ IoT 機器が、十分なセーフティ機能を実装していない。 (U2_V.3) また、IoT 機器が、住宅・住戸内の他の機器やシステムと連携する場合は、他の機器やシステムにおいても十分なセーフティ機能が実装されていない。 ・ IoT 機器が、想定された用途・用法に基づき設置・設定・運用されていない。 (U2_V.4) ・ 戸建住宅では、宅内のネットワーク、および宅内のネットワークに接続されている他の機器が、想定された用途・用法に基づき設置・設定・運用されていない。 (U2_V.5) ・ 共同住宅の共用部分に設置された IoT 機器では、住棟内ネットワーク、住棟内ネットワークに接続されている他の機器、宅内のネットワーク、宅内のネットワークに接続された他の機器が、想定された用途・用法に基づき設置・設定・運用されていない。 (U2_V.6) ・ 宅内のネットワークに接続されている他の機器、住棟内のネットワークに接続されている機器について、広域通信網への接続が管理されていない。 (U2_V.7)

※「脆弱性」部のカッコ内は、セキュリティ対策検討のための識別子（後述「添付 A」の想定利用シーンと脅威における脆弱性 ID）である。

※セーフティとは、危害を引き起こすおそれがあると思われるハザードから守られている状態。（用語集 参照）

3.2. 物理的なモノを含めた管理上の脅威

3.2.1. IoT 機器のライフサイクル

IoT 機器のライフサイクルに関する想定シーンでは、入居などによる IoT 機器の設置・設定、リフォームなどによる IoT 機器の更新、転居や退去などによる IoT 機器の譲渡・転売・廃棄を扱う。また共同住宅における共用部分の IoT 機器については、共同住宅の完成時から IoT 機器の更新、さらに廃棄までを扱う。

【住戸内の IoT 機器】

概要	住宅への入居による IoT 機器の設置、設定、サービスの開始、リフォームなどによる機器の更新やサービスの見直し、退去による機器の廃棄やサービスの解約についての想定シーンを整理する。
前提条件	・ 戸建住宅・共同住宅のいずれの場合においても、スマートホームを供給する事業者により、予め宅内のネットワークや IoT 機器が据え付けられている場合がある。 ・ 共同住宅においては、棟内ネットワークと住戸間のネットワーク回線は接続されており、共用部分や他の住戸との通信と相互に影響しないように設定されている。 ・ スマートホーム向けのサービスを開発し提供する事業者により、サービスに関するセキュリティやプライバシーを含むサービス提供のポリシーが示されている。 ・ サービスを受けるために必要な IoT 機器には、個人情報やプライバシーを保護する機能を有している。
基本フロー	【IoT 機器の設置・設定】 1) 予め宅内のネットワークや IoT 機器が据え付けられている場合も含め、住まい手、またはスマートホーム向けサービスのサポートやメンテナンスを行う事業者が、サービスの提供を受けるため、サービスの契約、IoT 機器や他の機器の設置・設定を行う。
	【転居等による IoT 機器の他者への譲渡】 1) 宅内のネットワークや IoT 機器が据え付けられている場合も含め、住まい手または住宅の所有者が IoT 機器を住戸に残した状態で転居や転売を行う。
	【IoT 機器の更新】 1) 予め宅内のネットワークや IoT 機器が据え付けられている場合も含め、住まい手、またはスマートホーム向けのサービスのサポートやメンテナンスを行う事業者が、IoT 機器の故障やサービスポリシーの変更などにより、IoT 機器や他の機器を交換する。
	【IoT 機器の廃棄】 1) 予め宅内のネットワークや IoT 機器が据え付けられている場合も含め、住まい手、またはスマートホーム向けサービスのサポートやメンテナンスを行う事業者が、サービスを解約し、IoT 機器や他の機器の返却や廃棄を行う。

【共同住宅の共用部分における IoT 機器】

概要	共同住宅の共用部分における IoT 機器の設置、設定、サービスの開始、機器の更新やサービスの見直し、機器の廃棄やサービスの解約についての想定シーンを整理する。
前提条件	・ 共同住宅の共用部分においては、マンションデベロッパー等をはじめとするスマートホームを供給する事業者により、施工時からネットワークや IoT 機器が据え付けられている場合が基本となるが、分譲共同住宅・団地の管理組合や管理受託会社、または賃貸住宅の所有者や管理受託会社管理組合または管理受託会社によって据え付けられることもある。 ・ 住まい手（または住まい手同志）の決議によって、新たな機器を設置する場合もある。

	・ 共用部分の IoT 機器が住棟内ネットワークに接続される場合においては、共用部分や他の住戸との通信と相互に影響しないように設定されている。
基本フロー	【IoT 機器の設置・設定】 1) IoT 機器の設置としては、スマートホーム向けサービスのサポートやメンテナンスを行う事業者が、サービスの提供を受けるため、サービスの契約、IoT 機器や他の機器の設置・設定を行う。
	【IoT 機器の更新】 1) スマートホーム向けのサービスのサポートやメンテナンスを行う事業者が、IoT 機器の故障やサービスポリシーの変更などにより、IoT 機器や他の機器を交換する。
	【IoT 機器の廃棄】 1) 事業者が、サービスを解約し、IoT 機器や他の機器の返却や廃棄を行う。

想定されるインシデント、脅威、脆弱性について以下にまとめる。

想定されるインシデント	・ サービス提供のプライバシーポリシーが確認できないことにより、個人情報やプライバシーなどが住まい手の意思に反して利用される。 ・ サービスのセキュリティポリシーに不備があり、セキュリティ対策が不足し、事業者から情報が外部に漏えいする。 ・ 利用者の個人情報が流出する。 ・ セーフティに関するサービス提供のポリシーが提供されていないことにより、IoT 機器が利用者の想定と異なる動作をする。 ・ IoT 機器の交換時、交換される IoT 機器より個人情報やプライバシー情報が漏えいする。
脅威	・ サービス、および IoT 機器のセキュリティ、プライバシー、セーフティなどを含めたサービス提供のポリシーが確認できていない。 ・ 誤操作により、IoT 機器や他の機器が意図しない動作をする。 ・ 新たに設置する IoT 機器が、想定された用途・用法に基づき設置、設定されていないため、戸建住宅に設置された IoT 機器では、宅内のネットワーク、および宅内のネットワークに接続されている他の機器が、IoT 機器へ干渉する。 ・ 新たに設置する IoT 機器が、想定された用途・用法に基づき設置、設定されていないため、共同住宅では、住棟内ネットワーク、住棟内ネットワークに接続された機器、宅内のネットワーク、宅内のネットワークに接続された他の機器が、IoT 機器へ干渉する。 ・ 転居や転売の際、新たな利用者が前の利用者の情報（個人情報）が残存した状態で、IoT 機器やサービスを利用し続けてしまう。
脆弱性	・ サービス、および IoT 機器のセキュリティ、プライバシー、セーフティなどを含めたサービス提供のポリシーが提供されていない、または確認できていない。 (U3_V.1) ・ IoT 機器が、暗号通信など、十分なセキュリティ機能を実装していない。 (U3_V.2) IoT 機器が、他の機器やシステムと連携する場合は、他の機器やシステムにおいて十分なセキュリティ機能が実装されていない。 ・ IoT 機器が、十分なセーフティ機能が実装されていない。 (U3_V.3) IoT 機器が、他の機器やシステムと連携する場合は、他の機器

	やシステムにおいて十分なセーフティ機能が実装されていない。	
	・ IoT 機器が、想定された用途・用法に基づき設置・設定・運用がなされていない。	(U3_V.4)
	・ 不正アクセスやマルウェア感染などのインシデントに気が付かないまま、利用している。	(U3_V.5)
	・ 戸建住宅では、宅内のネットワーク、および宅内のネットワークに接続されている他の機器が、想定された用途・用法に基づき設置・設定・運用がなされていない。	(U3_V.6)
	・ 共同住宅の共用部分に設置された IoT 機器では、住棟内ネットワーク、住棟内ネットワークに接続されている他の機器、宅内のネットワーク、宅内のネットワークに接続された他の機器が、想定された用途・用法に基づき設置・設定・運用がなされていない。	(U3_V.7)
	・ サービスを実行する機器の信頼性が低い、サーバ等の機器が攻撃を受ける、脆弱性対策が行われていない。	(U3_V.8)
	・ サービスを実行する機器の交換や廃棄時のデータ消去を確認していない。IoT 機器を遠隔から管理するシステムなどで、管理する側に IoT 機器の設定情報や個人情報が残存する。	(U3_V.9)
	・ サービスの運用において、個人情報を含むデータ管理などのポリシーが提示されていない。	(U3_V.10)

※「脆弱性」部のカッコ内は、セキュリティ対策検討のための識別子（後述「添付 A」の想定利用シーンと脅威における脆弱性 ID）である。

3.2.2. IoT 機器の外部管理

スマートホーム向けサービスのサポートやメンテナンスを行う事業者は、IoT 機器の管理を行うが、この想定シーンでは、例えば外部から設定情報の更新や、IoT 機器のソフトウェアアップデートなど、管理者が行う作業を外部から行うケースを示したものである。

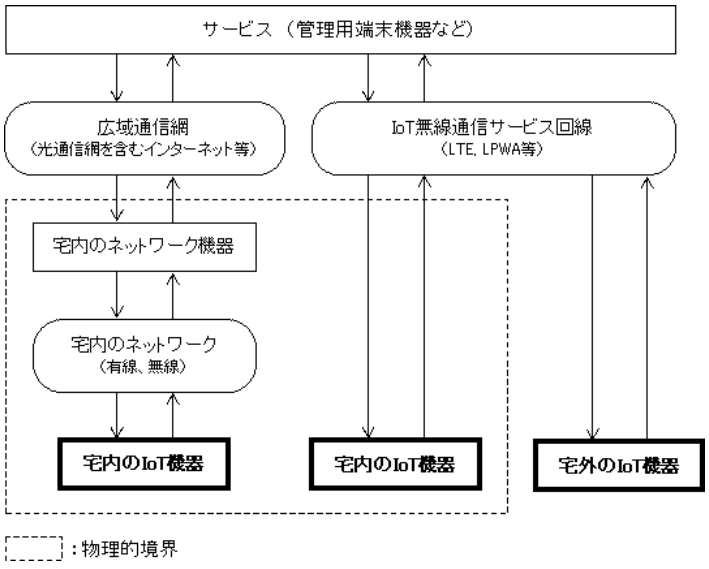

図 9.IoT 機器の外部管理（戸建住宅の場合）

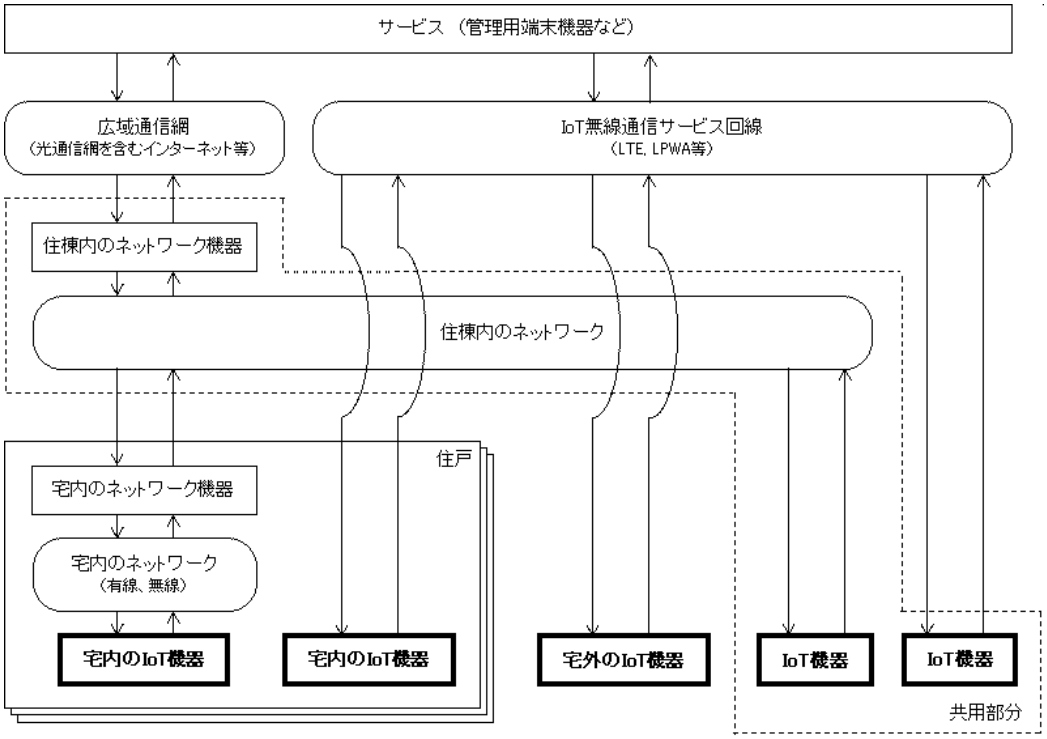

図 10.IoT 機器の外部管理（共同住宅の場合）

想定シーンと脅威は以下の通りである。

概要	管理端末機器などから、IoT 機器を操作、設定する想定シーンを整理する。
前提条件	・ 特定された管理端末装置のみが IoT 機器の管理を行うことができるように設計、または設定されている。 ・ 宅内のネットワーク、**住棟内のネットワーク、**IoT 無線通信サービス回線での通信データは、機密性や完全性が確保されている。
基本フロー	【宅内のネットワーク、住棟内のネットワーク、および広域通信網の場合】 1) 管理端末機器などから IoT 機器の操作、設定において、管理端末機器、広域通信網、宅内のネットワーク、IoT 機器の経路を経る。 2) 共同住宅においては、管理端末機器などから IoT 機器の操作、設定において、管理端末機器、広域通信網、住棟内のネットワーク、宅内のネットワーク、IoT 機器の経路を経る。 3) IoT 機器から管理端末装置などへの状態通知については、上記の真逆の経路となる。
	【IoT 無線通信サービス回線の場合】 1) 管理端末機器などから IoT 機器の操作、設定において、IoT 無線通信サービス回線を利用する場合は、管理端末機器から IoT 無線通信サービス回線を介して IoT 機器の経路を経る。 2) IoT 機器から管理端末装置などへの状態通知については、上記の真逆の経路となる。

想定されるインシデント、脅威、脆弱性について以下にまとめる。

想定されるインシデント	・ IoT 機器が乗っ取られることにより、意図しない動作や人体に悪影響を及ぼす。 ・ IoT 機器が、宅内や共用部分の他の機器に干渉する
脅威	・ IoT 機器が、乗っ取られる。 ・ 管理端末装置と IoT 機器間の通信データが暴露される。 ・ 管理端末装置と IoT 機器間の通信データが改ざんされる。
脆弱性	・ IoT 機器が、予め許可された管理端末装置以外からの操作、設定が行える。 (U4_V.1) ・ IoT 機器が、十分なセキュリティ機能を実装していない。 (U4_V.2) IoT 機器が、他の機器やシステムと連携する場合は、他の機器やシステムにおいて十分なセキュリティ機能が実装されていない。 ・ IoT 機器が、十分なセーフティ機能を実装していない。 (U4_V.3) IoT 機器が、他の機器やシステムと連携する場合は、他の機器やシステムにおいて十分なセーフティ機能が実装されていない。 ・ サービスのサポートやメンテナンスを行うために利用する機器の交換や廃棄時の手続きがない。 (U4_V.4)

※「脆弱性」部のカッコ内は、セキュリティ対策検討のための識別子（後述「添付 A」の想定利用シーンにおける脆弱性 ID）である。

4. スマートホームに求められる最低限のセキュリティ対策

本章は、各ステークホルダーに必要となるセキュリティ対策のガイドを示す。

なお、各対象者（ステークホルダー）に向けた対策の具体内容は、「添付 A ステークホルダーにおける 機能／想定されるインシデント／リスク源／対策要件」、「添付 B 対策の整理と、国際規格などの各種規格との対応」、「添付 C ステークホルダーに向けたガイドと対策要件の対応関係」に示されている。必要に応じて参照されたい。

4.1. 「（1）スマートホーム向け IoT 機器の事業者」

スマートホーム向けの IoT 機器を開発・生産・販売する事業者は、以下の対策を行うことが望ましい。

- **IoT 機器は初期状態でセキュリティを確保する**
- **セーフティを考慮する**
- **ソフトウェアをアップデートするための仕組みを提供する**
- **利用者に IoT 機器の使い方や使用環境をガイドする**

以下に、各項目を解説する。

4.1.1. IoT 機器は初期状態でセキュリティを確保する

スマートホームは企業と違い、一般的にはセキュリティの専門家が関与することなく、無計画に IoT 機器やサービスが導入されることが想定される。また、提供者側の事業者の想定と異なる環境での IoT 機器とサービスの利用や、提供者側の事業者が想定しない設定や運用がなされる可能性も想定される。これらによりセキュリティリスクが生じる可能性が高い。このため、スマートホーム向け IoT 機器を提供する事業者は、IoT 機器の設計・開発段階からスマートホームの特性を考慮し、初期状態でセキュリティを確保することが望ましい。

4.1.2. セーフティを考慮する

スマートホームに設置される IoT 機器においては、たとえマルウェア感染や第三者による不正侵入が発生した場合にも、利用者の生命・財産に対するリスクを最小限にする仕組みを考慮しておくことが有効である。IoT 機器によっては、アクチュエータを持つ機器があるが、このような機器では、サイバー攻撃により引き起こされた異常な動作が物理的な被害を招くことが考えられ、この異常な動作を検知するために、一定期間証跡を残す仕組みや、異常な動作が発生しても安全側に倒れるような機能を実装することが望ましい。

4.1.3. ソフトウェアをアップデートするための仕組みを提供する

IoT 機器において、新たに発見された脆弱性に対応するため、IoT 機器のソフトウェアを適切にアップデートできる仕組みを具備することが望ましい。

4.1.4. 利用者に IoT 機器の使い方や使用環境をガイドする

スマートホーム向け IoT 機器を提供する事業者は、IoT 機器の誤操作や誤使用を防ぐため、「設置方法」、「使用環境」、「正しい使い方」、「IoT 機内に保存される情報」、「IoT 機器が外部と通信する情報」、「サポート期間」など、IoT 機器に関わるガイドやポリシーを提供することが望ましい。

また、このガイドには、発生しうるセキュリティインシデントや住まい手などへの危害についても記述しておくことが望ましい。

このガイドやポリシーは、住まい手だけではなく、IoT 機器を利用してサービスを提供する事業者、管理や保守を行う事業者にとっても有用である。

4.2. 「(2)スマートホーム向けの IoT 機器を遠隔から管理する事業者」「(5)スマートホーム向けにメンテナンスやサポートを行う事業者」

スマートホーム向け IoT 機器を遠隔から管理する事業者や、住まい手の住宅に出向き、スマートホーム向けにメンテナンスやサポートを行う事業者は、以下の対策を行うことが望ましい。

また、これらの事業者は、管理やサポートのためのシステムを開発して提供することも考えられる。管理やサポートのためのシステムを開発して提供する場合は、4.1 項、4.3 項もあわせて参照願いたい。

- **事業者側のシステムを適切に運用･管理する**
- **サービスと IoT 機器のガイドに従った保守･管理を行う**
- **管理のポリシーを提示し順守する**

以下に、各項目を解説する。

4.2.1. 事業者側のシステムを適切に運用･管理する

遠隔(外部)から IoT 機器の管理･保守が可能なシステム、また運用･管理に利用している機器が、サイバー攻撃の被害にあった場合、IoT 機器の管理･保守に影響するため、IoT 機器やサービスの利用に影響するばかりか、多くのサービス利用者に影響を及ぼしかねない。そのため、遠隔管理するための事業者側システムには、極めて高い品質や信頼性が確保されていること、また適切に脆弱性への手当を行うことが重要である。

また、このシステムに IoT 機器の利用者に関する個人情報などの重要情報が保存されている場合には、システムや機器の交換・廃棄時には、重要情報を適切に廃棄処理するこが必要である。

4.2.2. サービスと IoT 機器のガイドに従った保守・管理を行う

スマートホームのサービス事業者から提供されるサービスの利用方法・利用環境・サービスで取得する情報などを含めサービス提供のポリシー、および IoT 機器に関連する事業者が提供する設置方法・使用方法・機内に保存される情報などの IoT 機器ガイドを含むプライバシーポリシーを確認し、想定された用途・用法に基づき IoT 機器の管理・保守を行うことが重要である。

例えば、IoT 機器やサービスの提供者が示す用途・用法に従ってソフトウェアのアップデートを適切に行うことは、セキュリティの観点から重要である。IoT 機器やサービスのメンテナンスを行う事業者として、これらの事項も考慮することが望まれる。

4.2.3. 管理のポリシーを提示し順守する

スマートホーム向けの IoT 機器を遠隔から管理するサービス事業者や、スマートホーム向けにメンテナンスやサポートを行う事業者は、サービスに関わる「ポリシー」や「使用環境」、「正しい利用方法」、「取得する情報」、「外部に渡す（通信する）情報」などを順守する。また、利用者に対しては「プライバシーポリシー」を提示することが望ましい。また住まい手において、発生しうるインシデントについても記述しておくことが望ましい。

4.3. 「（3）スマートホーム向けのサービス事業者」

スマートホーム向けのサービス事業者は、以下の対策を行うことが望ましい。

- **サービスを提供するための事業者システムを適切に運用・管理する**
- **サービスのポリシーおよびサービスの利用方法を提供する**

以下に、各項目を解説する。

4.3.1. サービスを提供するための事業者システムを適切に運用・管理する

サービスを提供しているシステムや機器がサイバー攻撃の被害にあった場合、その影響はサービスの提供事業者のシステムに留まらず、そのサービスを利用する多くの利用者に対しても影響を及ぼす。そのため、事業者側のシステムは品質や信頼性が確保されていること、また適切に脆弱性への手当を行うことが望ましい。

また、住まい手の個人情報などの重要情報が保存されたシステムや機器の交換や廃棄時は、重要情報を適切に廃棄処理するこが必要である。

4.3.2. サービス提供に関わるポリシーと利用方法を提供する

スマートホーム向けのサービスを提供する事業者は、サービス提供に関わる「ポリシー」や、「正しい利用方法」、「利用環境」、「サービスで取得する情報」、「外部に渡す（通信する）情報」なども提供することが望ましい。

また、住まい手に対して、発生しうるインシデントや危害についても記述しておくことが望ましい。

4.4. 「（4）スマートホームを供給する事業者」

スマートホームを提供する事業者は、以下の対策を行うことが望ましい。

- **IoT 機器やサービスを正しく設置、設定する**
- **IoT 機器を正しく選定する**

以下に、各項目を解説する。

4.4.1. IoT 機器やサービスを正しく設置、設定する

住宅の新築時やスマートホームを提供する事業者がリフォームを実施する場合など、新たに設置する IoT 機器は機器の種類（機能）に応じたセキュリティレベルや品質を確保するため、ガイドに従った設置、施工を行うだけでなく、ネットワーク環境の整備も必要である。特に IoT 機器を住戸の外、住まい手以外の者も接触可能な場所に設置する場合は、不正な改造や不正なソフトウェアのインストール、ネットワークの不正利用防止について留意することが望ましい。

4.4.2. IoT 機器を正しく選定する

IoT 機器に関連する事業者が提供する使い方（ガイド）を参照し、想定された用途・用法に合致した IoT 機器を選定することが重要である。必要とされるセキュリティレベルに応じ、機密情報を保護するためのタンパ機能の有無や、ソフトウェアの完全性を保証する機能など、要件に合わせた機能を有することを確認する必要がある。仮にこれを考慮せず、想定されない設置・利用環境・設定で運用することは、本来発揮すべきセキュリティやセーフティに対する機能が有効に機能せず、住まい手のリスクに繋がる可能性がある。

また、適切に設置、施工するためのガイドを作成し、施工業者に展開することも重要である。

4.5. 「(6)スマートホーム化された分譲共同住宅・団地の管理組合や管理受託会社」
「(7)スマートホーム化された賃貸住宅の所有者や管理受託会社」

スマートホーム化された分譲共同住宅・団地の管理組合や管理組合から管理業務を受託する管理受託会社、スマートホーム化された賃貸住宅の所有者や所有者から管理業務を受託する管理受託会社は、以下の対策を行うことが望ましい。

- **共用部分や賃貸している住戸に設置する機器の選定と、機器やネットワークの管理・運用は適切に行う**
- **機器やサービスの用途・用法を守る**

以下に、各項目を解説する。

4.5.1. 共用部分や賃貸している住戸に設置する機器の選定と、機器やネットワークの管理・運用は適切に行う

共同住宅の共用部分に設置される住棟内のネットワーク、および機器は、機器の種類(機能)に応じ、適切に管理を行うことが望ましい。

また、リフォームなどの際は、共用部分に設置される住棟内のネットワークや IoT 機器に、品質が確保された機器を選定することが求められる。もし品質の低い機器を選定した場合には、住まい手の住戸に設置された IoT 機器に影響を及ぼしうるばかりか、住まい手の個人情報などを取り扱う製品からの漏えいリスクもあるため、機器の種類(機能)に応じたセキュリティレベルや品質の確保された機器を選定することが望ましい。

賃貸住宅、または賃貸している住戸のリフォームなどの際は、住戸内の IoT 機器を更新することも考えられる。この場合においても機器の種類(機能)に応じたセキュリティレベルや品質の確保された機器を選定することが望ましい。

なお共同住宅においては、運用の一環として、セキュリティ事故発生時の対応フローや作業分担を、住まい手同士(管理組合)や管理受託会社と整合しておくことが有効である。

4.5.2. 機器やサービスは用途・用法を守る

スマートホームを供給する事業者が共用部分に設置した機器を運用・管理する場合や、共用でサービス事業者によるサービスの提供を受ける場合、いずれの場合においても、提供事業者が想定する用途・方法を守った上で利用されているかどうかを確認することが重要である。

設定の不備や誤操作などにより、IoT 機器やサービスが利用者の意図しない動作となり、個人情報などの漏えい、物理的な被害、人体に対するダメージを負うといった可能性がある。

また、用途・方法を守るという観点で、ソフトウェアを常に最新の状態に維持するという観点も含まれる。ソフトウェアのアップデートを適切に行うことは、セキュリティの観点から重要であり、共用部分の IoT 機器に対しこれを考慮することが望まれる。

4.6. 「(8)スマートホームの住まい手」

スマートホームの住まい手は、以下の対策を行うことが望ましい。

- **信頼できる IoT 機器やサービスを選ぶ**
- **IoT 機器やサービスは用途・用法を守って使う**
- **個人情報は自分で守る**

以下に、各項目を解説する。

4.6.1. 信頼できる IoT 機器やサービスを選ぶ

IoT 機器やサービスを導入する際には、個人情報の取扱いポリシーや、セキュリティ対策に留意して、適切な製品やサービスを選択することが望ましい。住まい手が判断可能な選択のポイントとしては、例えば以下の様な項目が挙げられる。

- ソフトウェアのアップデート機能があるか
- 製品のセキュリティに関する最新情報がウェブサイトに掲載されているか
- 問い合わせ先があるか

住まい手自身で適切な IoT 機器・サービスを選択することが難しければ、家電量販店での配布やウェブサイト公開が行われている資料の活用など、住まい手の意向に沿った選定の可能な事業者に相談することも含めて、対応することが望ましい。

4.6.2. IoT 機器やサービスは用途・用法を守って使う

スマートホームで、IoT 機器やサービスを利用する際は、IoT 機器やサービスで想定された用途・方法で利用することが重要である。設定の不備や誤操作は、個人情報の漏えいや、人体へのダメージに繋がるなど、本来確保されているセキュリティやセーフティの機能に影響する可能性がある。これは、住まい手自身が IoT 機器やサービスを選定した場合だけでなく、IoT 機器やサービスが設営されている住戸を賃借した場合においても、設営されている IoT 機器やサービスで想定された用途・方法で利用することが重要である。

例えば、提供者の示す用途・用法に従ってソフトウェアのアップデートを適切に行うことは、セキュリティの観点から非常に重要である。もし、住まい手自身によるソフトウェアのアップデート実行や、IoT 機器やサービスの設定や管理が難しければ、住まい手の意向を代行した設定や管理が可能な事業者に相談することが望ましい。

4.6.3. 個人情報は自分で守る

スマートホームで利用されるIoT機器は、従来の住宅設備や家電と違い、個人情報やプライバシーに関わる情報を保有していることも多い。一方で、インターネットの普及に伴う個人売買の一般化で、IoT機器の譲渡や転売なども頻繁に行われている。

IoT機器の譲渡・転売・破棄などの際は、住まい手自身の個人情報を守るため、「データを消去する」などを確実に行うことが望ましい。もし、住まい手自身が適切な対応を取ることが難しければ、それを代行するサポート事業者に相談・依頼することも一つの選択肢である。

5. おわりに

本ガイドラインでは、スマートホームにおけるセキュリティ対策の考え方から、各ステークホルダーに必要な最低限のセキュリティ対策まで、最も基本的なセキュリティ対策の方針を示した。

一方、ガイドラインの冒頭に述べたように、スマートホームに必要なセキュリティ対策は幅広く、個別の業種・業態に応じて特化・詳細化することが有効である。特定の分野に特化したセキュリティ対策の検討が必要な際は、本ガイドラインや他のガイドライン等を参考に、セキュアな住環境の構築に向けたセキュリティ対策を考案されたい。

添付A

■「(1) スマートホーム向けIoT機器の事業者」における 機能／想定されるインシデント／リスク源／対策要件（1/2）

機能	想定されるインシデント	リスク源						対策要件ID	対策要件の例	関連するCPSFの対策要件ID
		脅威	脆弱性ID	脆弱性	想定利用シーンにおける脆弱性ID	脆弱性の要素 管理面（ソシキ, ヒト, データ, プロシージャ）	脆弱性の要素 機器・システムの機能面（モノ, システム, データ）			
下記の機能 ・フィジカル空間の物理事象を読み取り、デジタル情報へ変換し、サイバー空間へ送る機能 ・サーバー空間での処理の結果により、IoT機器を制御する等のためにサイバー空間から受ける機能 ・外部からの管理機能	事前に想定されていない動作をする（IoT機器およびIoT機器を含むシステムにより提供されるサービスや機器の種類により、想定されていない動作は異なり、情報漏洩や不正な制御といった、人体・健康・住宅・防犯・環境・利便性・エネルギーメータなどに影響するものがある）	・ソフトウェアの脆弱性やハードウェアの脆弱性を悪用してIoT機器内部に不正アクセスされる	MV.1	・利用されないネットワークポートなどが利用可能な状態のままとなっている	U1_V.1, U2_V.1, U1_V.2, U2_V.2, U3_V.2, U4_V.2	✓	✓	MO.1	・IoT機器およびIoT機器を含むシステムでの不要なネットワークポート、その他USBやシリアルポートなどを物理的または論理的に閉塞すること。	CPS.PT-2
			MV.2	・IoT機器およびIoT機器を含むシステムを利用するためのIDやパスワードが初期状態のままとなっている	U1_V.1, U2_V.1, U1_V.2, U2_V.2, U3_V.2, U4_V.2		✓	MO.2	・IoT機器およびIoT機器を含むシステムを利用するための初期パスワードを個体毎に異なるものとすること。または初期パスワードが機種によって同一である場合、パスワードを変更しない限り利用できないようにすること。	–
			MV.3	・受容できない既知のセキュリティリスクおよびセーフティに関するハザードが残存している	U1_V.1, U2_V.1, U1_V.2, U2_V.2, U2_V.3, U3_V.2, U4_V.2		✓	MO.3	・IoT機器およびIoT機器を含んだシステムの構成要素の管理におけるセキュリティルールが、実装方法を含めて有効かを確認するため、定期的にリスクアセスメントを実施し、IoT機器およびIoT機器を含んだシステムのライフサイクル全体に対し、受容できないセキュリティリスクおよび、セーフティに関するハザードに対応すること。 ・IoT機器およびIoT機器を含んだシステムの企画・設計の段階から、受容できない既知のセキュリティリスクおよび、セーフティに関するハザードが残存しないこと。	CPS.RA-4
			MV.4	・通信相手に対するアクセス制御が十分でない	U1_V.1, U2_V.1, U1_V.2, U2_V.2, U3_V.2, U4_V.1 U4_V.2		✓	MO.4	・IoT機器やシステムで通信相手に対するアクセス制限機能を実装すること。 ・システムを構成するネットワークへのアクセスを制限する機能を実装すること。	CPS.AC-4
			MV.5	・サービスを利用するためのパスワード等の認証情報が、ネットワーク上平文である	U1_V.1, U2_V.1, U1_V.2, U2_V.2 U3_V.2 U4_V.2		✓	MO.5	・サービスを利用するために必要となるパスワード等の認証情報は、平文のままネットワークに送出しないこと。	–
		・IoT機器およびIoT機器を含むシステムと、サービスを提供するサーバ等との通信データが改ざんされる	MV.6	・IoT機器およびIoT機器を含むシステムと、サービスを提供するサーバ等との通信が保護されていない。	U1_V.1, U2_V.1, U1_V.2, U2_V.2, U3_V.2, U4_V.2		✓	MO.6	・IoT機器およびIoT機器を含むシステムへの入力データやネットワーク間で転送される通信データ等のシステムに入力されるデータを検証する等、データの機密度や重要度に応じたデータ保護手段を提供すること。	–
		・IoT機器を含むシステムが、連携して動作しない	MV.7	・IoT機器を含むシステムを構築する際の設定や、動作の確認が不十分である	U1_V.3, U2_V.4, U3_V.4, U3_V.1, U3_V.3, U3_V.5, U4_V.3	✓		MO.7	・IoT機器に関する動作仕様に基づき、IoT機器の設定や確認方法および、利用方法に応じて、発生しうるセキュリティインシデントやインシデントの影響についてのガイドを提供すること。	–
		・新たに発見されたソフトウェアの脆弱性やハードウェアの脆弱性への対応ができない	MV.8	・IoT機器のソフトウェアやファームウェアをアップデートする機能が存在しないこと	U1_V.1, U2_V.1, U1_V.2, U2_V.2, U3_V.2, U4_V.2		✓	MO.8	・IoT機器のソフトウェアやファームウェアをアップデートする機能を実装し、受容できない既知のセキュリティリスクおよびセーフティに関するハザードに対応していくこと。	–
	IoT機器や通信機器等の機能が停止する	・IoTシステムを構成するIoT機器、通信機器等に対するサービス拒否攻撃	MV.9	・IoT機器を含むシステムに十分なリソース(処理能力、通信帯域、ストレージ容量)が確保されていない	U1_V.1, U2_V.1, U1_V.2, U2_V.2, U3_V.2, U4_V.2		✓	MO.9	・以下のようなリソースや資産保護の機能を実装すること。 - サービス拒否攻撃等のサイバー攻撃を受けた場合でも、資産を適切に保護する機能を実装すること。 - 通信断などにより機能やサービスを提供できない場合でも、資産を適切に保護する機能を実装すること。 - システムを構成するネットワークにアクセスを制限する機能を実装すること。	CPS.DS-6
	IoT機器を間違った使い方をする（IoT機器およびIoT機器を含むシステムにより提供されるサービスや機器の提供者が想定しない利用方法により顕在化する脆弱性により、情報漏洩や不正な制御が行われ、人体・健康・住宅・防犯・環境・利便性・エネルギーメータなどに影響する）	・IoT機器を利用するサービスや利用者が間違った使い方をする	MV.10	・IoT機器のセキュリティおよびセーフティに関するガイドが提供されていない	U1_V.3, U2_V.4, U3_V.4, U3_V.1, U3_V.3, U3_V.5, U4_V.3	✓		MO.10	・セキュリティ確保、セーフティ確保のために必要な事項だけでなく、IoT機器内に保存される情報やIoT機器が外部と通信する情報などについて記載してあるIoT機器のガイドを提供すること。	–
			MV.11	・IoT機器に対する設定ミスやエラーを考慮した設計がされてない	U1_V.1, U2_V.1, U1_V.2, U2_V.2, U2_V.3, U3_V.2, U4_V.2		✓	MO.11	・ミスやエラーを発生させないようなセットアップ機能や、ミスやエラーがあった場合には安全側に倒れるような機能を実装すること。	–
	廃棄されるIoT機器から情報が漏洩する	・IoT機器に登録された個人情報などの機微な情報やIoT機器が収集した情報などが機器内に残存した状態で廃棄される	MV.12	・IoT機器における情報削除機能（サニタイズ）がない。	U1_V.1, U2_V.1, U1_V.2, U2_V.2, U3_V.2, U4_V.2		✓	MO.12	・IoT機器の廃棄時には、内部に保存されているデータ（秘密鍵、電子証明書等の重要情報、個人情報等のプライバシー情報および、IoT機器が収集し蓄積する情報等）を削除または読み取りできない状態にする機能を実装すること。 ・IoT機器の廃棄時に、データを削除（または読み取りできない状態に）する手順をガイドに示すこと。	–
フィジカル空間の物理事象を読み取り、デジタル情報へ変換し、サイバー空間へ送る機能	(監視が行き届かない場所に設置される機器の運用中、あるいは廃棄後の盗難等の後)改ざんされたIoT機器がネットワーク接続され、故障や正確でないデータの送信等が発生する	・盗難等により不正な改造を施されたIoT機器がネットワークに不正接続されることにより、改ざんされたセンサーデータ等がサーバーに送られる	MV.13	・秘密鍵やアカウント情報など保護すべき情報を格納する領域に耐タンパー性がなく、物理的な改ざんを防げない	U1_V.1, U2_V.1, U1_V.2, U2_V.2, U3_V.2, U4_V.2		✓	MO.13	・耐タンパ性が必要な情報を取り扱う場合、耐タンパーデバイスを利用すること。	CPS.DS-8
			MV.14	・IoT機器のソフトウェアやファームウェアの完全性の検証手段がなく、ソフトウェア的な改ざんを防げない	U1_V.1, U2_V.1, U1_V.2, U2_V.2, U3_V.2, U4_V.2		✓	MO.14	・IoT機器にて稼働するソフトウェアの完全性を検証できること。	CPS.DS-10
			MV.15	・IoT機器の廃棄時に、データを削除（または読み取りできない状態に）する手順がない	U1_V.1, U2_V.1, U1_V.2, U2_V.2, U3_V.2, U4_V.2		✓	MO.12	・IoT機器の廃棄時には、内部に保存されているデータ（秘密鍵、電子証明書等の重要情報、個人情報等のプライバシー情報および、IoT機器が収集し蓄積する情報等）を削除または読み取りできない状態にする機能を実装すること。 ・IoT機器の廃棄時に、データを削除（または読み取りできない状態に）する手順をガイドに示すこと。	–

■「(1) スマートホーム向けIoT機器の事業者」における 機能／想定されるインシデント／リスク源／対策要件（2/2）

機能	想定されるインシデント	リスク源						対策要件ID	対策要件の例	関連するCPSFの対策要件ＩＤ
		脅威	脆弱性ID	脆弱性	想定利用シーンにおける脆弱性ID	脆弱性の要素 管理面（ソシキ, ヒト, データ, プロシージャ）	脆弱性の要素 機器・システムの機能面（モノ, システム, データ）			
サイバー空間から受け取ったデータに基づいて、モノを制御したり、データを可視化したりする機能	正常動作・異常動作に関わらず、安全に支障をきたすような動作をする（提供されるサービスや機器の種類により、想定されていない動作は異なり、人体・健康・住宅・防犯・環境・利便性・エネルギーメータなどに影響するものなどがある）	・不正なエンティティによるインジェクション攻撃 ・サイバー空間からの許容範囲外のインプットデータ ・制御信号の改ざん	MV.16	・インプットされたデータを検証する仕組みが無い	U1_V.1, U2_V.1, U1_V.2, U2_V.2, U3_V.2, U4_V.2		✓	MO.15	・サイバー空間から受ける情報が悪質なコードを含んでおらず、許容範囲内であることを動作前に検証すること。	CPS.CM-3
			MV.17	・脆弱性が残存している（セキュリティリスクまたは/およびハザード）	U1_V.1, U2_V.1, U1_V.2, U2_V.2, U3_V.2, U4_V.2		✓	MO.3	・IoT機器およびIoT機器を含んだシステムの構成要素の管理におけるセキュリティルールが、実装方法を含めて有効かを確認するため、定期的にリスクアセスメントを実施し、IoT機器およびIoT機器を含んだシステムのライフサイクル全体に対し、受容できないセキュリティリスクおよび、セーフティに関するハザードに対応すること。 ・IoT機器およびIoT機器を含んだシステムの企画・設計の段階から、受容できない既知のセキュリティリスクおよび、セーフティに関するハザードが残存しないこと。	CPS.RA-4
			MV.18	・安全性が確保されていない	U1_V.1, U2_V.1, U1_V.2, U2_V.2, U3_V.2, U4_V.2		✓	MO.16	・IoT機器およびシステムの企画・設計の段階におけるアセスメントにて判明したセキュリティおよび関連するセーフティのリスクに対応すること。	CPS.RA-6

■「(2) スマートホーム向けのIoT機器を遠隔から管理する事業者」における 機能／想定されるインシデント／リスク源／対策要件

機能	想定されるインシデント	リスク源						対策要件ID	対策要件の例	関連するCPSFの対策要件ＩＤ
		脅威	脆弱性ID	脆弱性	想定利用シーンにおける脆弱性ID	脆弱性の要素 管理面（ソシキ, ヒト, データ, プロシージャ）	脆弱性の要素 機器・システムの機能面（モノ, システム, データ）			
下記機能の双方 ・フィジカル空間の物理事象を読み取り、デジタル情報へ変換し、サイバー空間へ送る機能 ・サイバー空間から受け取ったデータに基づいて、機器を制御したり、可視化したりする機能 ・外部からの管理機能	IoT機器およびIoT機器を含むシステムが不正に設定されまたは不正に利用され、情報漏洩や不正な制御等、人体・健康・住宅・防犯・環境・利便性・エネルギーメータなどに影響する	・スマートホーム向けのIoT機器を遠隔から管理する事業者のシステムがマルウェアに感染する	RMV.1	・スマートホーム向けのIoT機器を遠隔から管理する事業者のシステム（サーバーのOSやアプリケーション、ネットワーク機器等）が脆弱性に対応していない	U4_V.4		✓	RMO.1	・スマートホーム向けのIoT機器を管理する事業者のシステムの脆弱性に対応すること。 ・システムを構成するネットワークへのアクセスを制限する機能を導入すること。	–
		・スマートホームに設置されたIoT機器の設置・運用が正しく行われない	RMV.2	・IoT機器のガイドやサービスのポリシーを確認していない	U1_V.3, U2_V.4, U3_V.4	✓		RMO.2	・IoT機器の利用方法、設定方法、機器の内部に保存される情報などをIoT機器のガイドで確認すること。 ・サービスの利用方法、利用環境、サービスで取得する情報などを含め、サービス提供のポリシーを確認すること。	–
・IoT機器内に住まい手の個人情報などを保管する機能	住まい手の個人情報などが漏洩する	・スマートホーム向けのIoT機器を遠隔から管理する事業者のシステムを構成するサーバなどの機器のリプレースや廃棄時、ストレージ上のデータが残存している	RMV.3	・住まい手が、住居からの転居する時や、サービスの利用をやめるなどの住まい手からの要望があった時等、住宅に備え付けのIoT機器および、サーバーに保存される利用者の個人情報などのデータ削除（サニタイズ）を行っていない	U1_V.3, U2_V.4, U3_V.4	✓		RMO.3	・住まい手など利用者からの要求に応じ、住宅に備え付けのIoT機器とスマートホーム向けのIoT機器を遠隔から管理するシステムを構成する機器（サーバー等）のデータ削除（サニタイズ）を実施すること。	–
								RMO.4	・スマートホーム向けのIoT機器を遠隔から管理するシステムは、システム内部や管理対象のIoT機器に保存されているデータを削除または読み取りできない状態にする機能を実装すること。 ・スマートホーム向けのIoT機器を遠隔から管理するシステム内部や管理対象のIoT機器が取得する情報や外部に渡す（通信する）情報および、保存されているデータの内容を含むポリシーを提示すること。	–
			RMV. 4	・スマートホーム向けのIoT機器を遠隔から管理する事業者のシステムを構成するサーバなどのリプレースや廃棄時のデータ削除（サニタイズ）を確認していない	U3_V.1	✓		RMO.5	・スマートホーム向けのIoT機器を遠隔から管理するシステムを構成する機器のリプレースや廃棄時に、データ削除（サニタイズ）を行うこと。	CPS.IP-6

■「(3) スマートホーム向けのサービス事業者」における　機能／想定されるインシデント／リスク源／対策要件

機能	想定されるインシデント	リスク源				対策要件ID	対策要件の例	関連するCPSFの対策要件ＩＤ
		脅威	脆弱性ID	脆弱性	想定利用シーンにおける脆弱性ID	脆弱性の要素		
						管理面（ソシキ, ヒト, データ, プロシージャ）	機器・システムの機能面（モノ, システム, データ）	
下記の機能 ・住まい手がサービスを利用するために必要となる個人情報も含め、データを保管する機能 ・センサデータを加工・分析する機能 ・データを送受信する機能	サービスが提供できない（住まい手に対しては、サービスが停止することで、人体・健康・住宅・防犯・環境・利便性・エネルギーメータなどに影響する）	・システムを構成するサーバやネットワーク機器などへのサービス拒否攻撃を受け、システムが停止する	SV.1	・システムが十分なリソース(処理能力、通信帯域、ストレージ容量)を確保されていることを確認していない	U1_V.7, U2_V.8, U3_V.8	✓		SO.1	・システムが、十分なリソースで構成されていることを確認すること。 ・不要なアクセスや悪質なアクセスを受けるリスクを低減するための措置を講じること。	–
		・システムとしての動作不安定や、システムが停止する	SV.2	・システムを構成する機器の品質や信頼性を確認していないため、システムとして動作が不安定な状況となり、攻撃を受けるリスクが残存している	U1_V.7, U2_V.8, U3_V.8	✓		SO.2	・システムを構成するサーバやネットワーク機器などの品質や信頼性を確認すること。 ・不要なアクセスや悪質なアクセスを受けるリスクを低減するための措置を講じること。	–
	サービスに関するデータ（センサデータ、加工や分析されたデータ、住まい手の個人情報など）が漏洩する	・システムを構成するサーバやネットワーク機器などで対応されていない既知や未知の脆弱性を利用した攻撃により、情報漏洩が発生する	SV.3	・システムを構成するサーバやネットワーク機器などの脆弱性情報を確認していない等により、最新ソフトウェアへのアップデートやパッチ適用が行われず、脆弱な状態となる	U1_V.7, U2_V.8, U3_V.8	✓		SO.3	・システムを構成するサーバやネットワーク機器などの脆弱性が適切に対応されていることを確認すること。 ・システムを構成するネットワークへのアクセスを制限する機能を導入すること。	–
・センサデータを加工・分析する機能 ・データを送受信する機能	機器を制御したり、可視化などが、事前に想定されていない動作をする（住まい手に対しては、人体・健康・住宅・防犯・環境・利便性・エネルギーメータなどに影響する）	・システムを構成するサーバやネットワーク機器などで対応されていない既知や未知の脆弱性を利用した攻撃により、事前に想定されていない動作が行われる	SV.3	・システムを構成するサーバやネットワーク機器などの脆弱性情報を確認していない等により、最新ソフトウェアへのアップデートやパッチ適用が行われず、脆弱な状態となる	U1_V.7, U2_V.8, U3_V.8	✓		SO.3	・システムを構成するサーバやネットワーク機器などの脆弱性が適切に対応されていることを確認すること。 ・システムを構成するネットワークへのアクセスを制限する機能を導入すること。	–
・住まい手がサービスを利用するために必要となる個人情報も含め、データを保管する機能	サービスに関するデータ（センサデータ、加工や分析されたデータ、住まい手の個人情報など）が漏洩する	・システムを構成するサーバやネットワーク機器などの機器のリプレースや廃棄時、ストレージ上のデータが残存している	SV.4	・システムを構成するサーバやネットワーク機器などのリプレースや廃棄時のデータ削除（サニタイズ）を確認していない	U1_V.8, U2_V.9, U3_V.9	✓		SO.4	・サービスを提供するシステムは、システム内部に保存されているユーザーデータを削除または読み取りできない状態にする機能を実装すること。 ・サービスを提供するシステムは、利用者がユーザーデータの削除を求めた場合に、データを削除または読み取りできない状態にする機能を提供すること。 ・システム内で保持する個人情報(パスワード等)は必要に応じ、暗号化して保存する機能を実装すること。	–
								SO.5	・リプレースや廃棄時に、データ削除（サニタイズ）を行うこと。	CPS.IP-6
		・サービスを提供するシステム以外にも、サービスに関するデータ（センサデータ、加工や分析されたデータ、住まい手の個人情報など）が保管されている	SV.5	・サービスに関するデータ（センサデータ、加工や分析されたデータ、住まい手の個人情報など）の管理ポリシーが順守されていない	U1_V.9, U2_V.10, U3_V.10, U3_V.1	✓		SO.6	・住まい手に関するデータ保護などについてのポリシーを提示し、順守すること。	–

■「(4) スマートホームを供給する事業者」における　機能／想定されるインシデント／リスク源／対策要件

機能	想定されるインシデント	リスク源				対策要件ID	対策要件の例	関連するCPSFの対策要件ＩＤ
		脅威	脆弱性ID	脆弱性	想定利用シーンにおける脆弱性ID	脆弱性の要素		
						管理面（ソシキ, ヒト, データ, プロシージャ）	機器・システムの機能面（モノ, システム, データ）	
下記の機能 ・フィジカル空間の物理事象を読み取り、デジタル情報へ変換し、サイバー空間へ送る機能 ・サイバー空間から受け取ったデータに基づいて、モノを制御したり、データを可視化したりする機能 ・IoT機器を管理する	IoT機器の間違った設定などにより、情報漏洩や不正な制御等、人体・健康・住宅・防犯・環境・利便性・エネルギーメータなどに影響する	・スマートホームに設置されたIoT機器の設置・運用が正しく行われない	HV.1	・住宅の新築時またはリフォーム・修繕時、住宅（住戸）や集合住宅の共用部分に設置されるIoT機器およびIoT機器を含むシステムの設置状態や動作状況を適切に確認していない	U1_V.1, U2_V.1, U1_V.2, U2_V.2, U1_V.3, U2_V.4, U3_V.4, U1_V.4, U2_V.5, U3_V.6, U1_V.6, U2_V.7	✓		HO.1	・IoT機器に関する動作仕様に基づき、IoT機器の設定や利用方法から想定されるセキュリティインシデントや危害を回避や軽減するためのガイドやポリシーに従い設置と設定を行い、動作状況を確認すること。	–
	(監視が行き届かない場所に設置される機器の運用中、あるいは廃棄後の盗難等の後)改ざんされたIoT機器がネットワーク接続され、故障や正確でないデータの送信等が発生する	・盗難等により不正な改造を施されたIoT機器によるネットワーク接続 ・センサーの測定値、閾値、設定の改ざん	HV.2	・物理的な改ざんやソフトウェアやファームウェアの完全性について確認されていない	U1_V.1, U2_V.1, U1_V.2, U2_V.2, U3_V.2, U4_V.2	✓		HO.2	・住宅（住戸）や集合住宅の共用部分に設置するIoT機器およびIoT機器は、IoT機器やIoT機器を含むシステムに提供されるサービスの特性に応じ、セキュリティ機能およびセーフティ機能を確認すること。 ・耐タンパ性が必要な情報を取り扱う場合、耐タンパーデバイスが組み込まれたIoT機器やシステムであることを確認すること。 ・IoT機器やシステムのソフトウェアは完全性を検証可能なIoT機器やシステムであることを確認すること。	CPS.DS-8、CPS.DS-15

■「(5) スマートホーム向けにメンテナンスやサポートを行う事業者」における 機能／想定されるインシデント／リスク源／対策要件

機能	想定されるインシデント	リスク源				脆弱性の要素		対策要件ID	対策要件の例	関連するCPSFの対策要件ＩＤ
		脅威	脆弱性ID	脆弱性	想定利用シーンにおける脆弱性ID	管理面（ソシキ, ヒト, データ, プロシージャ）	機器・システムの機能面（モノ, システム, データ）			
下記機能の双方 ・フィジカル空間の物理事象を読み取り、間へ送る機能 ・サイバー空間から受け取ったデータに基づいて、モノを制御したり、データを可視化したりする機能 ・IoT機器を管理する	IoT機器およびIoT機器を含むシステムが不正に設定されまたは不正に利用され、情報漏洩や不正な制御等、人体・健康・住宅・防犯・環境・利便性・エネルギーメータなどに影響する	・スマートホーム向けサービスのサポートやメンテナンスを行う事業者の利用する機器のマルウェア感染	SMV.1	・スマートホーム向けサービスのサポートやメンテナンスを行う事業者の利用する機器の脆弱性が対応されていない	U4_V.4		✓	SMO.1	・スマートホーム向けサービスのサポートやメンテナンスを行う事業者のシステムの脆弱性に対応すること。	–
		・スマートホームに設置されたIoT機器の設置・運用が正しく行われない	SMV.2	・IoT機器のガイドやサービスのポリシーを確認していない	U1_V.3, U2_V.4, U3_V.4	✓		SMO.2	・IoT機器の利用方法、設定方法、機器の内部に保存される情報などをIoT機器のガイドで確認すること。 ・サービスの利用方法、利用環境、サービスで取得する情報などを含め、サービス提供のポリシーを確認すること。	–
・IoT機器内に住まいの手個人情報などを保管する機能	住まい手の個人情報などが漏洩する	・スマートホーム向けサービスのサポートやメンテナンスを行う事業者の利用する機器のリプレースや廃棄時、ストレージ上のデータが残存している	SMV.3	・住まい手が、住居からの転居する時、住宅に備え付けのIoT機器のデータ削除（サニタイズ）を行っていない	U3_V.1		✓	SMO.3	・住宅に備え付けのIoT機器のデータ削除（サニタイズ）を実施すること。	–
			SMV.4	・スマートホーム向けサービスのサポートやメンテナンスを行う事業者の利用する機器のリプレースや廃棄時のデータ削除（サニタイズ）していない	U1_V.8, U2_V.9, U3_V.9		✓	SMO.4	・スマートホーム向けサービスのサポートやメンテナンスを行う事業者の利用する機器のリプレースや廃棄時に、データ削除（サニタイズ）すること。	CPS.IP-6

■「(6) スマートホーム化された分譲共同住宅・団地の管理組合や管理受託会社」および、
「(7) スマートホーム化された賃貸住宅の所有者や管理受託会社」における 機能／想定されるインシデント／リスク源／対策要件

機能	想定されるインシデント	リスク源				脆弱性の要素		対策要件ID	対策要件の例	関連するCPSFの対策要件ＩＤ
		脅威	脆弱性ID	脆弱性	想定利用シーンにおける脆弱性ID	管理面（ソシキ, ヒト, データ, プロシージャ）	機器・システムの機能面（モノ, システム, データ）			
下記の機能 ・フィジカル空間の物理事象を読み取り、デジタル情報へ変換し、サイバー空間へ送る機能 ・サイバー空間から受け取ったデータに基づいて、モノを制御したり、データを可視化したりする機能 ・IoT機器を管理する	・事前に想定されていない動作をする（住戸内の機器により提供されるサービスの種類により、想定されていない動作は異なり、人体・健康・住宅・防犯・環境・利便性・エネルギーメータなどに影響する。また、住棟内ネットワークに接続された機器では、情報漏洩やデータが改ざんされる）	・住戸内のネットワークに接続された機器が、住棟内ネットワークに接続された機器から攻撃される	CAV.1	・共用部分における住棟内ネットワークが管理されていないまたは住棟内ネットワークに接続された共用部分設置の機器が管理されていないことでマルウェアに感染する	U1_V.5, U2_V.6, U3_V.7, U1_V.6, U2_V.7	✓		CAO.1	・共用部分における住棟内ネットワークおよび住棟内ネットワークに接続された機器を管理すること。	–
			CAV.2	・住棟内ネットワークに接続された共用部分設置の機器が、個々に外部のネットワークに接続され管理されていないことでマルウェアに感染する	U1_V.5, U2_V.6, U3_V.7, U1_V.6, U2_V.7	✓		CAO.2	・住棟内のネットワークに接続された機器の外部のネットワーク接続は、個々に管理するまたは住棟内のネットワークに接続された機器の外部のネットワーク接続を一元的に管理できるように構成すること。	–
			CAV.3	・集合住宅の修繕時、新たに共用部分または住戸部分に設置する機器およびシステムの品質や信頼性が確認されていないおよび住棟内ネットワークに接続された機器が管理されていない	U1_V.5, U2_V.6, U3_V.7, U1_V.6, U2_V.7	✓		CAO.3	・集合住宅の修繕時、共用部分または住戸部分に導入される機器およびシステムは、目的とする特性に応じた品質や信頼性の確保につき確認すること。	CPS.DS-14
IoT機器およびIoT機器を含むシステム内にデータを保存する機能	・集合住宅の修繕時、共用部分または住戸部分に設置される機器およびシステム内の個人情報などが漏洩する	・集合住宅の修繕時、共用部分または住戸部分に設置される機器およびシステムから住まい手の個人情報などが漏洩する	CAV.4	・集合住宅からの退去時、共用部分および住戸に設置された共用設備であるIoT機器内のデータ削除を忘れる	U1_V.5, U2_V.6, U3_V.7	✓		CAO.4	・集合住宅からの退去時、共用部分および住戸に設置された共用設備であるIoT機器内のデータを削除すること。	CPS.IP-6
			CAV.5	・集合住宅の修繕時、共用部分および住戸に設置された共用設備であるIoT機器内のデータ削除を忘れる	U1_V.5, U2_V.6, U3_V.7	✓		CAO.5	・集合住宅からの修繕時など、共用部分および住戸に設置された共用設備であるIoT機器の変更やサービスのリプレースの際には、IoT機器やサービス内のデータを削除すること。	CPS.IP-6

■「(8) スマートホームの住まい手」における 機能／想定されるインシデント／リスク源／対策要件

機能	想定されるインシデント	リスク源				脆弱性の要素		対策要件ID	対策要件の例	関連するCPSFの対策要件ＩＤ
		脅威	脆弱性ID	脆弱性	想定利用シーンにおける脆弱性ID	管理面（ソシキ, ヒト, データ, プロシージャ）	機器・システムの機能面（モノ, システム, データ）			
下記機能の双方 ・フィジカル空間の物理事象を読み取り、デジタル情報へ変換し、サイバー空間へ送る機能 ・サイバー空間から受け取ったデータに基づいて、機器を制御したり、可視化したりする機能	事前に想定されていない動作をする（IoT機器およびIoT機器を含むシステムにより提供されるサービスや機器の種類により、想定されていない動作は異なり、情報漏洩や不正な制御等、人体・健康・住宅・防犯・環境・利便性・エネルギーメータなどに影響するものがある）	・品質や信頼性の確保や維持が出来ていないIoT機器およびIoTを含むシステムを利用することで、サービスが意図通り提供されない	CV.1	・利用するIoT機器およびIoT機器を含むシステムが管理されておらず、品質や信頼性の確保や維持が出来ていないIoT機器およびIoTを含むシステムが利用されている	U1_V.1, U2_V.1, U1_V.2, U2_V.2, U1_V.3, U2_V.4, U3_V.4, U1_V.4, U2_V.5, U3_V.6, U1_V.6, U2_V.7	✓		CO.1	・品質や信頼性が確保されたIoT機器およびIoTを含むシステムを導入すること。 ・ソフトウェアアップデートなどにより品質や信頼性が維持されるIoT機器およびIoTを含むシステムを導入すること。	–
		・IoT機器およびIoT機器を含むシステムの設定が、想定された利用用途に基づくものとなっておらず、サービスが意図通り提供されない	CV.2	・IoT機器やサービスの利用や管理が理解できていない	U1_V.1, U2_V.1, U1_V.2, U2_V.2, U1_V.3, U2_V.4, U3_V.4, U2_V.10, U3_V.10	✓		CO.2	・IoT機器のガイドやサービスのポリシーを確認し利用や管理を行うこと。	–
								CO.3	・住まい手自ら対応が困難な場合は、スマートホーム向けのIoT機器を遠隔から管理する事業者もしくはスマートホーム向けサービスのサポートやメンテナンスを行う事業者にサポートやメンテナンスを依頼すること。	–
IoT機器およびIoT機器を含むシステム内にデータを保存する機能	・IoT機器およびシステム内の個人情報などが漏洩する	・転居、IoT機器の転売や廃棄の際に、IoT機器やシステム内のデータから住まい手の個人情報などが漏洩する	CV.3	・IoT機器やシステムの利用を終了する際に、IoT機器とシステム内のデータ削除を忘れる	U2_V.10, U3_V.10	✓		CO.4	・利用を終了したIoT機器とサービス内のデータを削除すること。	CPS.IP-6

添付B

■対策の整理と、国際規格などの各種規格との対応

・本項に記載の対策例はあくまで一例を示すものであって、他の実装方法を何ら否定するものではない。本資料は、サイバーとフィジカルの転写機能の信頼性、およびIoT機器の管理に関し、各組織の事業の特性やリスク分析の結果等に応じて、リスク対応を実施する際に参考とされたい。
・本項に記載する「国際規格などの各種規格との対応」は対策要件や、対策例として同等の内容が記載されている部分を抽出している。各組織の事業の特性やリスク分析の結果等に応じて、リスク対応を実施する際にあわせて参考とされたい。

対策要件ID	対策要件の例	対策例	国際規格などの各種規格との対応
MO.1	・IoT機器およびIoT機器を含むシステムでの不要なネットワークポート、その他USBやシリアルポートなどを物理的または論理的に閉塞すること。	・IoT機器の初期状態において、使用しないネットワークインタフェースは栓をするなどして物理的に閉塞、また利用しないネットワークポートは論理的に閉じること。 ・IoT機器の使用しないUSBポート、シリアルポートは栓をするなど物理的に閉塞すること。	[IoTセキュリティガイドライン] 要点4、要点8、要点9、要点15 [つながる世界の開発指針] 指針5 [Considerations for a Core IoT Cybersecurity Capabilities Baseline] Baseline候補 11、Baseline候補 12 [Code of Practice] Guidelines 6) [ETSI EN 303 645] 4.6 [Baseline Security Recommendations for IoT] GP-TM-27、GP-TM-28、GP-TM-33、GP-TM-45
MO.2	・IoT機器およびIoT機器を含むシステムを利用するための初期パスワードを個体毎に異なるものとすること。または初期パスワードが機種によって同一である場合、パスワードを変更しない限り利用できないようにすること。	・IoT機器およびIoT機器を含むシステムを利用するためのパスワードを個体毎に異なるものとすること。 ・初期パスワードが個体毎に同一である場合、これを変更しない限り利用できないようにすること。 １）パスワード品質（パスワード長、利用可能な文字種、文字の組み合わせなどによるパスワードの複雑さ） 予め個体毎に設定されているパスワード、または個体によらず同一パスワードが設定されている場合の変更については、IoT機器やサービスに応じた、パスワード品質を満足することが必要である。 ２）パスワードの初期値（IoT機器それぞれに個別の初期パスワードを付与） 予め個体毎に個別の初期パスワードを付与し、共通の初期パスワードを持たないような設計とすること。個別の初期パスワードは、個体の固有情報（例えばシリアル番号やMACアドレス）などから容易に推測できない様な文字列を使用するなど、IoT機器やサービスに応じた、パスワード品質を満足することが必要である。	[IoTセキュリティガイドライン] 要点4、要点7、要点15 [つながる世界の開発指針] 指針5 [Code of Practice] Guidelines 1) [ETSI EN 303 645] 4.1 [Baseline Security Recommendations for IoT] GP-TM-09、GP-TM-22
MO.3	・IoT機器およびIoT機器を含んだシステムの構成要素の管理におけるセキュリティルールが、実装方法を含めて有効かを確認するため、定期的にリスクアセスメントを実施し、IoT機器およびIoT機器を含んだシステムのライフサイクル全体に対し、受容できないセキュリティリスクおよび、セーフティに関するハザードに対応すること。 ・IoT機器およびIoT機器を含んだシステムの企画・設計の段階から、受容できない既知のセキュリティリスクおよび、セーフティに関するハザードが残存しないこと。	・IoT機器およびIoT機器を含むシステムを提供する組織は、構成要素の管理におけるセキュリティルールやポリシーを定め、定期的にリスクアセスメントを実施すること。 ・IoT機器およびIoT機器を含むシステムが実装しているオープンソースを含め、サードパーティの開発物を特定し、当該開発物に関する脆弱性情報を収集すること。 ・脆弱性検査ツールなどを利用した上で、IoT機器やIoT機器を含むシステムの特性に応じた脆弱性検査を行うこと。 ・既に住まい手が利用しているIoT機器やIoT機器を含むシステムにおいて受容できない脆弱性が発見された場合は、すみやかに脆弱性に対応した修正プログラム（ソフトウェアアップデート）を提供し、修正プログラムの適用手順の提示や、設定変更などによる緩和策、回避策の提示などの情報を公開すること。	[IoTセキュリティガイドライン] 要点1、要点17、要点18 [つながる世界の開発指針] 指針10、指針12、指針15、指針16、指針17 [NISTIR 8228] Goal 1 [Considerations for a Core IoT Cybersecurity Capabilities Baseline] Baseline候補 2 [Code of Practice] Guidelines 2)、Guidelines 3) [ETSI EN 303 645] 4.2、4.3 [Baseline Security Recommendations for IoT] GP-TS-06、GP-OP-04
MO.4	・IoT機器やシステムで通信相手に対するアクセス制限機能を実装すること。 ・システムを構成するネットワークへのアクセスを制限する機能を実装すること。	・IoT機器およびIoT機器を含むシステムは、例えば、以下の様な機能を実装し、アクセスを制限すること。 - ログイン認証失敗によるロックアウトや、安全性が確保できるまでログインを許可しないなど、IoT機器およびIoT機器を含むシステムに対する不正ログインを防ぐこと。 - 通信元や通信先を制限すること。 - ユーザや通信先を認証すること。	[IoTセキュリティガイドライン] 要点7、要点16 [ETSI EN 303 645] 4.1 [Considerations for a Core IoT Cybersecurity Capabilities Baseline] Baseline候補 4 [Baseline Security Recommendations for IoT] GP-TM-25
MO.5	・サービスを利用するために必要となるパスワード等の認証情報は、平文のままネットワークに送出しないこと。	・ネットワーク通信のデータを暗号化するなどID、パスワードなどを保護し、不正なアクセス、乗っ取り対策となる機能を実装すること。	[IoTセキュリティガイドライン] 要点14、要点16 [NISTIR 8200] ※1 [Considerations for a Core IoT Cybersecurity Capabilities Baseline] Baseline候補 5 [Code of Practice] Guidelines 5) [ETSI EN 303 645] 4.5 [Baseline Security Recommendations for IoT] GP-TM-39
MO.6	・IoT機器およびIoT機器を含むシステムへの入力データやネットワーク間で転送される通信データ等のシステムに入力されるデータを検証する等、データの機密度や重要度に応じたデータ保護手段を提供すること。	・ネットワーク通信のデータを暗号化するなど機密性を確保する機能を実装すること。 ・入力データを検証すること。	[IoTセキュリティガイドライン] 要点14、要点16 [NISTIR 8200] ※1 [Considerations for a Core IoT Cybersecurity Capabilities Baseline] Baseline候補 5 [Code of Practice] Guidelines 5)、Guidelines 13) [ETSI EN 303 645] 4.5 [Baseline Security Recommendations for IoT] GP-TM-39
MO.7	・IoT機器に関する動作仕様に基づき、IoT機器の設定や確認方法および、利用方法に応じて、発生しうるセキュリティインシデントやインシデントの影響についてのガイドを提供すること。	・脆弱性の情報や脆弱性により発生するセキュリティインシデントの情報を提供する。または、有用な情報を提供する外部のサイトへ誘導するようなポインタ情報を提示すること。 ・提供するIoT機器および、IoT機器を含むシステムの脆弱性情報を受け付ける窓口の情報を提示すること。	[IoTセキュリティガイドライン] 要点17、要点18、要点21 [つながる世界の開発指針] 指針16、指針17 [NISTIR 8259] Activity 5 [Code of Practice] Guidelines 2) [ETSI EN 303 645] 4.2 [Baseline Security Recommendations for IoT] GP-OP-02、GP-OP-05、GP-OP-06、GP-OP-07、GP-OP-08

対策要件ID	対策要件の例	対策例	国際規格などの各種規格との対応
MO.8	・IoT機器のソフトウェアやファームウェアをアップデートする機能を実装し、受容できない既知のセキュリティリスクおよびセーフティに関するハザードに対応していくこと。	・遠隔からの自動更新などの仕組みを提供すること。 ・修正プログラム（ソフトウェアアップデート）を提供し、修正プログラムの適用手順を提示すること。	[IoTセキュリティガイドライン] 要点17、要点21 [つながる世界の開発指針] 指針14、指針15、指針16 [NISTIR 8259] Activity 6 [Considerations for a Core IoT Cybersecurity Capabilities Baseline] Baseline候補 2 [Code of Practice] Guidelines 3) [ETSI EN 303 645] 4.3 [Baseline Security Recommendations for IoT] GP-TM-18、GP-TM-19、GP-TM-20
MO.9	・以下のようなリソースや資産保護の機能を実装すること。 - サービス拒否攻撃等のサイバー攻撃を受けた場合でも、資産を適切に保護する機能を実装すること。 - 通信断などにより機能やサービスを提供できない場合でも、資産を適切に保護する機能を実装すること。 - システムを構成するネットワークにアクセスを制限する機能を実装すること。	・IoT機器およびIoT機器を含むシステムは、ネットワークが失われた場合、可能な範囲でローカルでサービスを提供すること。 ・障害が予想よりも大きな影響を与える可能性があることを考慮して、攻撃に対する緩和機能を実装し、情報資産を保護すること。 ・サービス拒否攻撃に対しては、以下の様な対策が考えられるのであわせて実施を検討すること。 - ネットワークを分離し、通信元や通信先を制限すること。 - 誤った利用方法により適切にサービスが受けられていない可能性も考えられるので機能やサービスに対する設定をガイドすること。 ・IoT機器やサービスのソフトウェアの完全性を確認する機能を提供すること。	[IoTセキュリティガイドライン] 要点7 [つながる世界の開発指針] 指針12 [NISTIR 8259] Activity 6 [Considerations for a Core IoT Cybersecurity Capabilities Baseline] Baseline候補 3、Baseline候補 4 [Code of Practice] Guidelines 9)、Guidelines 12) [ETSI EN 303 645] 4.9、4.12 [Baseline Security Recommendations for IoT] GP-TM-15、GP-TM-16、GP-TM-17
MO.10	・セキュリティ確保、セーフティ確保のために必要な事項だけでなく、IoT機器内に保存される情報やIoT機器が外部と通信する情報などについて記載してあるIoT機器のガイドを提供すること。	・IoT機器およびIoT機器を含むシステムの利用者に対して、機器やシステム内部で管理する個人データ、個人データの処理内容、使用方法、使用者、目的等を開示すること。 ・住まい手等、IoT機器やサービスの利用者に対して、機器やシステムを安全にセットアップする手順を提供すること。 ・安全な構成を自動的セットアップする機能を提供することが望ましい。	[IoTセキュリティガイドライン] 要点15、要点18 [つながる世界の開発指針] 指針15、指針16 [NISTIR 8259] Activity 6 [NISTIR 8267] ※2 [Considerations for a Core IoT Cybersecurity Capabilities Baseline] Baseline候補 9 [Code of Practice] Guidelines 8)、Guidelines 10) [ETSI EN 303 645] 4.8、4.10 [Baseline Security Recommendations for IoT] GP-TM-10、GP-TM-11
MO.11	・ミスやエラーを発生させないようなセットアップ機能や、ミスやエラーがあった場合には安全側に倒れるような機能を実装すること。	・入力データを検証する機能により、不整合の発生を防ぐこと。 ・設定内容を検証する機能により、高いレベルのセキュリティを維持したり、設定内容に矛盾が生じた場合にはより安全な設定となる様な機能を提供すること。 ・住まい手等、IoT機器やサービスの利用者に対して、機器やシステムを安全にセットアップする手順を提供すること。 ・安全な構成を自動的セットアップする機能を提供することが望ましい。	[IoTセキュリティガイドライン] 要点8 [つながる世界の開発指針] 指針8 [Code of Practice] Guidelines 12)、Guidelines 13) [ETSI EN 303 645] 4.12、4.13 [Baseline Security Recommendations for IoT] GP-TM-54
MO.12	・IoT機器の廃棄時には、内部に保存されているデータ（秘密鍵、電子証明書等の重要情報、個人情報等のプライバシー情報および、IoT機器が収集し蓄積する情報等）を削除または読み取りできない状態にする機能を実装すること。 ・IoT機器の廃棄時に、データを削除（または読み取りできない状態に）する手順をガイドに示すこと。	・IoT機器およびIoT機器を含むシステムは、機器やサービス内部で保持する個人データを容易に削除できる機能を提供すること。	[つながる世界の開発指針] 指針7 [NISTIR 8259] Activity 6 [Considerations for a Core IoT Cybersecurity Capabilities Baseline] Baseline候補 8 [Code of Practice] Guidelines 11) [ETSI EN 303 645] 4.11
MO.13	・耐タンパ性が必要な情報を取り扱う場合、耐タンパーデバイスを利用すること。	・IoT機器およびIoT機器を含むシステムは、機器やサービス内部で機密度の高い重要な個人データ保持する場合は、耐タンパーな対策が施されたストレージに保存すること。	[IoTセキュリティガイドライン] 要点8 [つながる世界の開発指針] 指針8 [Code of Practice] Guidelines 4) [ETSI EN 303 645] 4.4 [Baseline Security Recommendations for IoT] GP-TM-01、GP-TM-02
MO.14	・IoT機器にて稼働するソフトウェアの完全性を検証できること。	・IoT機器は、製造元の公開キーなどにより、ソフトウェア更新の際の配布プログラムの完全性を検証すること。 ・IoT機器やサービスを提供するシステムが起動する際には、ソフトウェアの完全性を検証することが望ましい。	[IoTセキュリティガイドライン] 要点17 [つながる世界の開発指針] 指針12 [Code of Practice] Guidelines 7) [ETSI EN 303 645] 4.4、4.7 [Baseline Security Recommendations for IoT] GP-TM-03、GP-TM-04、GP-TM-05
MO.15	・サイバー空間から受ける情報が悪質なコードを含んでおらず、許容範囲内であることを動作前に検証すること。	・入力データを検証する機能により、不整合の発生を防ぐこと。 ・IoT機器は、製造元の公開キーなどにより、ソフトウェア更新の際の配布プログラムの完全性を検証すること。	[IoTセキュリティガイドライン] 要点16 [つながる世界の開発指針] 指針8 [NISTIR 8267] ※3 [Code of Practice] Guidelines 13) [ETSI EN 303 645] 4.5、4.13 [Baseline Security Recommendations for IoT] GP-TM-42
MO.16	・IoT機器およびシステムの企画・設計の段階におけるアセスメントにて判明したセキュリティおよび関連するセーフティのリスクに対応すること。	・IoT機器やサービスの設計段階で、既知の脆弱性検査ツールなどを利用し、IoT機器とサービスのセキュリティリスクを軽減すること。	[IoTセキュリティガイドライン] 要点8 [つながる世界の開発指針] 指針10、指針12 [Baseline Security Recommendations for IoT] GP-TM-56、GP-TM-57
RMO.1	・スマートホーム向けのIoT機器を管理する事業者のシステムの脆弱性に対応すること。 ・システムを構成するネットワークへのアクセスを制限する機能を導入すること。	・脆弱性検査ツールなどを利用した上で、システムの特性に応じた脆弱性検査を行うこと。 ・IoT機器のソフトウェア自動更新機能を有効化して運用すること。 ・ルータなどによりネットワークを分離し、通信元や通信先を制限すること。 ・ユーザや通信先を認証する機能を利用すること。 ・ログ機能によりIoT機器やネットワーク機器へのアクセスを記録すること。	[IoTセキュリティガイドライン] 要点7、要点8、要点13 [つながる世界の開発指針] 指針13、指針14 [NISTIR 8228] Goal 1 [Considerations for a Core IoT Cybersecurity Capabilities Baseline] Baseline候補 7 [Baseline Security Recommendations for IoT] GP-TM-18、GP-TM-19、GP-TM-56、GP-TM-57

対策要件ID	対策要件の例	対策例	国際規格などの各種規格との対応
RMO.2	・IoT機器の利用方法、設定方法、機器の内部に保存される情報などをIoT機器のガイドで確認すること。 ・サービスの利用方法、利用環境、サービスで取得する情報などを含め、サービス提供のポリシーを確認すること。	・IoT機器のガイドに従い利用方法を確認し、IoT機器がセキュリティレベルを維持できる利用方法、設定内容で運用すること。 ・IoT機器のサービス提供のポリシーと内容を確認し、適切に運用する。例えば、ソフトウェアアップデートの提供期間を確認したうえで、利用期間を決定するなどが考えられる。 ・IoT機器のガイドに従い利用方法を確認し、IoT機器内に保存する情報と情報の廃棄方法など廃棄の際に必要な手順を定めたうえで運用すること。	[IoTセキュリティガイドライン] 要点18、要点19 ※5 [つながる世界の開発指針] 指針16、指針17 ※5 [Considerations for a Core IoT Cybersecurity Capabilities Baseline] Baseline候補 2
RMO.3	・住まい手など利用者からの要求に応じ、住宅に備え付けのIoT機器とスマートホーム向けのIoT機器を遠隔から管理するシステムを構成する機器（サーバー等）のデータ削除（サニタイズ）を実施すること。	・住宅に備え付けのIoT機器から、機器やサービス内部で保持する個人データを削除すること。	[IoTセキュリティガイドライン] 要点18、要点19 [つながる世界の開発指針] 指針7 [Considerations for a Core IoT Cybersecurity Capabilities Baseline] Baseline候補 8 [Code of Practice] Guidelines 11) [ETSI EN 303 645] 4.11 [Baseline Security Recommendations for IoT] GP-TM-14
RMO.4	・スマートホーム向けのIoT機器を遠隔から管理するシステムは、システム内部や管理対象のIoT機器に保存されているデータを削除または読み取りできない状態にする機能を実装すること。 ・スマートホーム向けのIoT機器を遠隔から管理するシステム内部や管理対象のIoT機器が取得する情報や外部に渡す（通信する）情報および、保存されているデータの内容を含むポリシーを提示すること。	・IoT機器およびIoT機器を含むシステムは、機器やサービス内部で保持する個人データを容易に削除できる機能を提供すること。 ・システムやサービスを構成する機器内部で保持する個人情報などの個人データは住まい手などの利用者の要求に応じて容易に削除できる機能を提供すること。 ・スマートホーム向けのIoT機器を遠隔から管理するシステムが取得する情報や外部に渡す（通信する）情報および、保存されているデータの内容を含むポリシーを提示すること。	[IoTセキュリティガイドライン] 要点18、要点19 [つながる世界の開発指針] 指針7 [Considerations for a Core IoT Cybersecurity Capabilities Baseline] Baseline候補 8 [Code of Practice] Guidelines 11) [ETSI EN 303 645] 4.11 [Baseline Security Recommendations for IoT] GP-TM-14
RMO.5	・スマートホーム向けのIoT機器を遠隔から管理するシステムを構成する機器のリプレースや廃棄時に、データ削除（サニタイズ）を行うこと。	・システムやサービスを構成する機器内部で保持する個人データを含む全データを削除すること。	[IoTセキュリティガイドライン] 要点18、要点19 [つながる世界の開発指針] 指針7 [Considerations for a Core IoT Cybersecurity Capabilities Baseline] Baseline候補 8 [Code of Practice] Guidelines 11) [ETSI EN 303 645] 4.11 [Baseline Security Recommendations for IoT] GP-TM-14
SO.1	・システムが、十分なリソースで構成されていることを確認すること。 ・不要なアクセスや悪質なアクセスを受けるリスクを低減するための措置を講じること。	・障害が予想よりも大きな影響を与える可能性があることを考慮して、攻撃に対する緩和機能を実装し、情報資産の保護が可能なリソースを有することを確認すること。 ・ファイアウォール装置やWAF機能等によるネットワーク分離や通信元や通信先を制限すること。	[IoTセキュリティガイドライン] 要点７、要点8 [つながる世界の開発指針] 指針13 [ETSI EN 303 645] 4.5、4.9 [Baseline Security Recommendations for IoT] GP-TM-46、GP-TM-51
SO.2	・システムを構成するサーバやネットワーク機器などの品質や信頼性を確認すること。 ・不要なアクセスや悪質なアクセスを受けるリスクを低減するための措置を講じること。	・サービスを提供するためのシステムを構成するサーバやネットワーク機器のベンダーの品質体制を確認すること。 ・ネットワークを分離し、通信元や通信先を制限すること。 ・ログ機能によりシステムを構成するサーバやネットワーク機器へのアクセスを記録すること。	[IoTセキュリティガイドライン] 要点７、要点13 [つながる世界の開発指針] 指針13 [Considerations for a Core IoT Cybersecurity Capabilities Baseline] Baseline候補 7
SO.3	・システムを構成するサーバやネットワーク機器などの脆弱性が適切に対応されていることを確認すること。 ・システムを構成するネットワークへのアクセスを制限する機能を導入すること。	・サービスを提供するためのシステムを構成するサーバやネットワーク機器の情報公開体制、脆弱性対応の体制を確認すること。 ・ネットワークを分離し、通信元や通信先を制限すること。	[つながる世界の開発指針] 指針14
SO.4	・サービスを提供するシステムは、システム内部に保存されているユーザーデータを削除または読み取りできない状態にする機能を実装すること。 ・サービスを提供するシステムは、利用者がユーザーデータの削除を求めた場合に、データを削除または読み取りできない状態にする機能を提供すること。 ・システム内で保持する個人情報(パスワード等)は必要に応じ、暗号化して保存する機能を実装すること。	・システムやサービスを構成する機器内部で保持する個人情報などの個人データは住まい手などの利用者の要求に応じて容易に削除できる機能を提供すること。 ・個人情報などの重要なデータは暗号化して保存すること。	[つながる世界の開発指針] 指針14 [Code of Practice] Guidelines 4)、Guidelines 11) [ETSI EN 303 645] 4.4、4.11
SO.5	・リプレースや廃棄時に、データ削除（サニタイズ）を行うこと。	・システムやサービスを構成する機器内部で保持する個人データを含む全データを削除すること。	[IoTセキュリティガイドライン] 要点18、要点19 [つながる世界の開発指針] 指針7 [Considerations for a Core IoT Cybersecurity Capabilities Baseline] Baseline候補 8 [Code of Practice] Guidelines 11) [ETSI EN 303 645] 4.11 [Baseline Security Recommendations for IoT] GP-TM-14
SO.6	・住まい手に関するデータ保護などについてのポリシーを提示し、順守すること。	・住まい手等、IoT機器やサービスの利用者に対して、機器やシステム内部で管理する個人データ、個人データの処理内容、使用方法、使用者、目的等に関する規定を制定し、規定に従い運用すること。	[IoTセキュリティガイドライン] 要点18、要点19 [つながる世界の開発指針] 指針7 [NISTIR 8259] Activity 6 [Code of Practice] Guidelines 8) [ETSI EN 303 645] 4.8 [Baseline Security Recommendations for IoT] GP-TM-14
HO.1	・IoT機器に関する動作仕様に基づき、IoT機器の設定や利用方法から想定されるセキュリティインシデントや危害を回避や軽減するためのガイドやポリシーに従い設置と設定を行い、動作状況を確認すること。	・住宅（住戸）や集合住宅の共用部分に設置するIoT機器は、設定したガイドやポリシーに従い適切に設置し、設定を行うこと。 ・住宅（住戸）や集合住宅の共用部分に設置したIoT機器は、ガイドやポリシーに従った動作が行われていることを確認すること。	[IoTセキュリティガイドライン] 要点6 [つながる世界の開発指針] 指針1

対策要件ID	対策要件の例	対策例	国際規格などの各種規格との対応
HO.2	・住宅（住戸）や集合住宅の共用部分に設置するIoT機器およびIoT機器は、IoT機器やIoT機器を含むシステムに提供されるサービスの特性に応じ、セキュリティ機能およびセーフティ機能を確認すること。 ・耐タンパ性が必要な情報を取り扱う場合、耐タンパーデバイスが組み込まれたIoT機器やシステムであることを確認すること。 ・IoT機器やシステムのソフトウェアは完全性を検証可能なIoT機器やシステムであることを確認すること。	・住宅（住戸）や集合住宅の共用部分に設置するIoT機器およびネットワーク機器は、機能や性能の他、ベンダーの品質体制、情報公開体制および、保守体制を含めて選定すること。 ・IoT機器に関する動作仕様に基づき、IoT機器の設定や利用方法から想定されるセキュリティインシデントや危害を回避や軽減するためのガイドやポリシーを制定し、ガイドやポリシーに従った設置マニュアルや設定マニュアルなどのガイドを作成すること。 ・住宅（住戸）や集合住宅の共用部分に設置するIoT機器内部で機密度の高い重要なデータ保持する場合は、耐タンパー対策が施されたストレージに保存する機器を選定すること。 ・IoT機器やシステムは、ソフトウェアの完全性を検証可能な機種を選定すること。	[IoTセキュリティガイドライン] 要点7、要点14、要点18、要点19 [つながる世界の開発指針] 指針1 [NISTIR 8228] Goal 1 [Code of Practice] Guidelines 4)、Guidelines 8)、Guidelines 12) [ETSI EN 303 645] 4.4、4.8、4.12 [Baseline Security Recommendations for IoT] GP-TM-13
SMO.1	・スマートホーム向けサービスのサポートやメンテナンスを行う事業者のシステムの脆弱性に対応すること。	・脆弱性検査ツールなどを利用した上で、システムの特性に応じた脆弱性検査を行うこと。 ・IoT機器のソフトウェア自動更新機能を有効化して運用することを検討すること。	[IoTセキュリティガイドライン] 要点8 [つながる世界の開発指針] 指針8 [Code of Practice] Guidelines 4) [ETSI EN 303 645] 4.4、4.12 [Baseline Security Recommendations for IoT] GP-TM-01、GP-TM-02
SMO.2	・IoT機器の利用方法、設定方法、機器の内部に保存される情報などをIoT機器のガイドで確認すること。 ・サービスの利用方法、利用環境、サービスで取得する情報などを含め、サービス提供のポリシーを確認すること。	・IoT機器のガイドに従い利用方法を確認し、IoT機器がセキュリティレベルを維持できる利用方法、設定内容で運用すること。 ・IoT機器のサービス提供のポリシーと内容を確認し、ソフトウェアアップデートの設定、ソフトウェアアップテートの提供期間を確認し、利用期間を定めたうえで運用すること。 ・IoT機器のガイドに従い利用方法を確認し、IoT機器内に保存する情報と情報の廃棄方法など廃棄の際に必要な手順を定めたうえで運用すること。 ・構成要素の管理におけるセキュリティルールやポリシーを定め、定期的にリスクアセスメントを実施すること。	[IoTセキュリティガイドライン] 要点1、要点18、要点19 ※5 [つながる世界の開発指針] 指針16、指針17 ※5
SMO.3	・住宅に備え付けのIoT機器のデータ削除（サニタイズ）を実施すること。	・住宅に備え付けのIoT機器やシステムが内部に保持するデータ（転居する住まい手の個人データなど）を削除すること。	[IoTセキュリティガイドライン] 要点8 [つながる世界の開発指針] 指針12、指針14、指針16 [Considerations for a Core IoT Cybersecurity Capabilities Baseline] Baseline候補 8 [Code of Practice] Guidelines 11) [ETSI EN 303 645] 4.11 [Baseline Security Recommendations for IoT] GP-TM-18、GP-TM-19、GP-TM-56、GP-TM-57
SMO.4	・スマートホーム向けサービスのサポートやメンテナンスを行う事業者の利用する機器のリプレースや廃棄時に、データ削除（サニタイズ）すること。	・機器内部で保持する個人データを含む全データを削除すること。	[IoTセキュリティガイドライン] 要点18、要点19 [つながる世界の開発指針] 指針7 [Considerations for a Core IoT Cybersecurity Capabilities Baseline] Baseline候補 8 [Code of Practice] Guidelines 11) [ETSI EN 303 645] 4.11 [Baseline Security Recommendations for IoT] GP-TM-14
CAO.1	・共用部分における住棟内ネットワークおよび住棟内ネットワークに接続された機器を管理すること。	・共用部分における住棟内ネットワーク、および住棟内ネットワークに接続された機器の接続情報やソフトウェアバージョンを定期的に確認し、最新化された状態を維持すること。 ・構成要素の管理におけるセキュリティルールやポリシーを定め、定期的にリスクアセスメントを実施すること。 ・機器は管理された区画に設置するなど物理的な対策を行うこと。 ・機器が無線LANなどのアクセス手段を利用する場合は、暗号化などによるアクセス制限を行うこと。 ・機器へのアクセスをログに記録して管理すること。 ・構成要素のガイドなどから保守期間を確認し、更新計画の作成と計画に従った更新を行うこと。	[IoTセキュリティガイドライン] 要点6、要点13、要点18、要点19 ※5 [つながる世界の開発指針] 指針7、指針13、指針14、指針15、指針16、指針17 ※5 [NISTIR 8228] Goal 1 [Security for IoT Sensor Networks] ※4 [Considerations for a Core IoT Cybersecurity Capabilities Baseline] Baseline候補 7 [Code of Practice] Guidelines 3) [ETSI EN 303 645] 4.3
CAO.2	・住棟内のネットワークに接続された機器の外部のネットワーク接続は、個々に管理するまたは住棟内のネットワークに接続された機器の外部のネットワーク接続を一元的に管理できるように構成すること。	・外部ネットワークに接続された機器の接続先情報や通信プロトコルなど接続方式を定期的に確認し、最新化された状態を維持すること。 ・構成要素の管理におけるセキュリティルールやポリシーを定め、定期的にリスクアセスメントを実施すること。	[IoTセキュリティガイドライン] 要点1、要点14 [つながる世界の開発指針] 指針13、指針14、指針15 [NISTIR 8228] Goal 1 [Security for IoT Sensor Networks] ※4 [Code of Practice] Guidelines 5) [ETSI EN 303 645] 4.5
CAO.3	・集合住宅の修繕時、共用部分または住戸部分に導入される機器およびシステムは、目的とする特性に応じた品質や信頼性の確保につき確認すること。	・住宅（住戸）や集合住宅の共用部分に設置するIoT機器およびネットワーク機器は、機能や性能の他、ベンダーの品質体制、情報公開体制および、保証体制を含めて選定すること。	[IoTセキュリティガイドライン] 要点15 [つながる世界の開発指針] 指針1 [Security for IoT Sensor Networks] ※4
CAO.4	・集合住宅からの退去時、共用部分および住戸に設置された共用設備であるIoT機器内のデータを削除すること。	・共用部分および住戸に設置された共用設備であるIoT機器から、機器やサービス内部で保持する個人情報などのデータを削除すること。	[IoTセキュリティガイドライン] 要点18、要点19 ※5 [つながる世界の開発指針] 指針7 [Security for IoT Sensor Networks] ※4 [Considerations for a Core IoT Cybersecurity Capabilities Baseline] Baseline候補 8 [Code of Practice] Guidelines 11) [ETSI EN 303 645] 4.11 [Baseline Security Recommendations for IoT] GP-TM-14

対策要件ID	対策要件の例	対策例	国際規格などの各種規格との対応
CAO.5	・集合住宅からの修繕時など、共用部分および住戸に設置された共用設備であるIoT機器の変更やサービスのリプレースの際には、IoT機器やサービス内のデータを削除すること。	・共用部分および住戸に設置された共用設備であるIoT機器から、機器やサービス内部で保持する個人情報などのデータを削除すること。	[IoTセキュリティガイドライン] 要点18、要点19 ※5 [つながる世界の開発指針] 指針7 [Security for IoT Sensor Networks] ※4 [Considerations for a Core IoT Cybersecurity Capabilities Baseline] Baseline候補 8 [Code of Practice] Guidelines 11) [ETSI EN 303 645] 4.11 [Baseline Security Recommendations for IoT] GP-TM-14
CO.1	・品質や信頼性が確保されたIoT機器およびIoTを含むシステムを導入すること。 ・ソフトウェアアップデートなどにより品質や信頼性が維持されるIoT機器およびIoTを含むシステムを導入すること。	・IoT機器やサービスを提供するベンダーの品質体制を確認すること。 ・IoT機器やサービスを提供するベンダーの脆弱性情報の開示やソフトウェアアップデートの実施体制および、サポート期間を確認すること。 ・ネットワークを分離し、通信元や通信先を制限すること。	[IoTセキュリティガイドライン] 要点18、要点19、ルール1 ※5 [つながる世界の開発指針] 指針16、指針17 ※5
CO.2	・IoT機器のガイドやサービスのポリシーを確認し利用や管理を行うこと。	・IoT機器のガイドやサービスのポリシーを確認し、適切な利用や管理を行うこと。 ・IoT機器やシステムがソフトウェアの自動アップデート機能を提供する場合には、自動アップデートを有効化すること。	[IoTセキュリティガイドライン] 要点18、要点19、ルール1、ルール2 ※5 [つながる世界の開発指針] 指針16、指針17 ※5 [ETSI EN 303 645] 4.3、4.11
CO.3	・住まい手自ら対応が困難な場合は、スマートホーム向けのIoT機器を遠隔から管理する事業者もしくはスマートホーム向けサービスのサポートやメンテナンスを行う事業者にサポートやメンテナンスを依頼すること。	・住まい手自ら管理が困難な場合は、スマートホーム向けのIoT機器を遠隔から管理する事業者、またはスマートホーム向けサービスのサポートやメンテナンスを行う事業者にサポートやメンテナンスに依頼すること。	[IoTセキュリティガイドライン] ルール1、ルール2、ルール3、ルール4 [ETSI EN 303 645] 明確な指示はないが、IoT製品やサービスが意図した機能を提供するために必要なデジタル サービスを求めている。
CO.4	・利用を終了したIoT機器とサービス内のデータを削除すること。	・転居やIoT機器の買い替え、転売、廃棄などIoT機器を利用しなくなった場合、IoT機器の初期化等によりデータを削除すること。 ・サービスの利用を中止した場合、サービスからデータを削除すること。	[IoTセキュリティガイドライン] 要点18、要点19、ルール4 ※5 [つながる世界の開発指針] 指針7 [Considerations for a Core IoT Cybersecurity Capabilities Baseline] Baseline候補 8 [Code of Practice] Guidelines 11) [ETSI EN 303 645] 4.11

必要に応じ、「国際規格などの各種規格との対応」に示されていないドキュメントについても参照戴きたい。例えば「NISTIR 8228」の分類は、「1.デバイスのセキュリティの保護に関するリスク軽減」、「2.データセキュリティの保護に関するリスク軽減」、「3.個人のプライバシー保護のためのリスク軽減」となっており、記載のある項目以外についても関連する項目は多いと考えられる。

※1：[NISTIR 8200]では、要件や対策例として明確に示されていないが、消費者向けのIoT機器の脅威の例に通信内容の盗聴が示されている。

※2：[NISTIR 8267]では、多くのIoT機器が起動時等に複数のIPアドレスと通信する事が示されている。このような複数の通信先との通信内容についても明記する必要がある。

※3：[NISTIR 8267]では、多くのIoT機器はスマートフォン用の専用アプリケーション（コンパニオンアプケーション）を利用することが示されている。よって、IoT機器やシステムには、スマートフォンのコンパニオンアプケーションが含まれると判断すべきである。ただし、本対策ガイドラインはスマートホーム向けであり、スマートフォンのOSやアプリケーションは対象外としている。

※4：[Security for IoT Sensor Networks]は、ビル管理システムを対象としたドキュメントであり、ドキュメント全体を参照し、記載されている要件を満足するようなIoT機器やサービスを導入すること。

※5：[IoTセキュリティガイドライン] 要点18、要点19および、[つながる世界の開発指針] 指針16、指針17は、提供者が利用者に向けた情報発信についての記載であるが、利用者側がこれを受けて適切な対応を行う必要がある。

添付C

■「(1) スマートホーム向けIoT機器の事業者」に向けたガイドと対策要件の対応関係

ガイド	対策要件ID	対策要件の例
IoT機器は初期状態で、セキュリティを確保する	MO.1	・IoT機器およびIoT機器を含むシステムでの不要なネットワークポート、その他USBやシリアルポートなどを物理的または論理的に閉塞すること。
	MO.2	・IoT機器およびIoT機器を含むシステムを利用するための初期パスワードを個体毎に異なるものとすること。または初期パスワードが機種によって同一である場合、パスワードを変更しない限り利用できないようにすること。
	MO.3	・IoT機器およびIoT機器を含んだシステムの構成要素の管理におけるセキュリティルールが、実装方法を含めて有効かを確認するため、定期的にリスクアセスメントを実施し、IoT機器およびIoT機器を含んだシステムのライフサイクル全体に対し、受容できないセキュリティリスクおよび、セーフティに関するハザードに対応すること。 ・IoT機器およびIoT機器を含んだシステムの企画・設計の段階から、受容できない既知のセキュリティリスクおよび、セーフティに関するハザードが残存しないこと。
	MO.4	・IoT機器やシステムで通信相手に対するアクセス制限機能を実装すること。 ・システムを構成するネットワークへのアクセスを制限する機能を実装すること。
	MO.5	・サービスを利用するために必要となるパスワード等の認証情報は、平文のままネットワークに送出しないこと。
	MO.6	・IoT機器およびIoT機器を含むシステムへの入力データやネットワーク間で転送される通信データ等のシステムに入力されるデータを検証する等、データの機密度や重要度に応じたデータ保護手段を提供すること。
	MO.12	・IoT機器の廃棄時には、内部に保存されているデータ（秘密鍵、電子証明書等の重要情報、個人情報等のプライバシー情報および、IoT機器が収集し蓄積する情報等）を削除または読み取りできない状態にする機能を実装すること。 ・IoT機器の廃棄時に、データを削除（または読み取りできない状態に）する手順をガイドに示すこと。
	MO.13	・耐タンパ性が必要な情報を取り扱う場合、耐タンパーデバイスを利用すること。
	MO.14	・IoT機器にて稼働するソフトウェアの完全性を検証できること。
	MO.15	・サイバー空間から受ける情報が悪質なコードを含んでおらず、許容範囲内であることを動作前に検証すること。
セーフティを考慮する	MO.9	・以下のようなリソースや資産保護の機能を実装すること。 - サービス拒否攻撃等のサイバー攻撃を受けた場合でも、資産を適切に保護する機能を実装すること。 - 通信断などにより機能やサービスを提供できない場合でも、資産を適切に保護する機能を実装すること。 - システムを構成するネットワークにアクセスを制限する機能を実装すること。
	MO.11	・ミスやエラーを発生させないようなセットアップ機能や、ミスやエラーがあった場合には安全側に倒れるような機能を実装すること。
	MO.16	・IoT機器およびシステムの企画・設計の段階におけるアセスメントにて判明したセキュリティおよび関連するセーフティのリスクに対応すること。
ソフトウェアをアップデートするための仕組みを提供する	MO.8	・IoT機器のソフトウェアやファームウェアをアップデートする機能を実装し、受容できない既知のセキュリティリスクおよびセーフティに関するハザードに対応していくこと。
利用者に対しIoT機器の正しい使い方や使用環境をガイドする	MO.7	・IoT機器に関する動作仕様に基づき、IoT機器の設定や確認方法および、利用方法に応じて、発生しうるセキュリティインシデントやインシデントの影響についてのガイドを提供すること。
	MO.10	・セキュリティ確保、セーフティ確保のために必要な事項だけでなく、IoT機器内に保存される情報やIoT機器が外部と通信する情報などについて記載してあるIoT機器のガイドを提供すること。

■「(2) スマートホーム向けのIoT機器を遠隔から管理する事業者」に向けたガイドと対策要件の対応関係

ガイド	対策要件ID	対策要件の例
事業者側のシステムを適切に運用・管理する	RMO.1	・スマートホーム向けのIoT機器を管理する事業者のシステムの脆弱性に対応すること。 ・システムを構成するネットワークへのアクセスを制限する機能を導入すること。
	RMO.4	・スマートホーム向けのIoT機器を遠隔から管理するシステムは、システム内部や管理対象のIoT機器に保存されているデータを削除または読み取りできない状態にする機能を実装すること。 ・スマートホーム向けのIoT機器を遠隔から管理するシステム内部や管理対象のIoT機器が取得する情報や外部に渡す（通信する）情報および、保存されているデータの内容を含むポリシーを提示すること。
サービスとIoT機器のガイドに従った保守・管理を行う	RMO.2	・IoT機器の利用方法、設定方法、機器の内部に保存される情報などをIoT機器のガイドで確認すること。 ・サービスの利用方法、利用環境、サービスで取得する情報などを含め、サービス提供のポリシーを確認すること。
管理のポリシーを提示し順守する	RMO.3	・住まい手など利用者からの要求に応じ、住宅に備え付けのIoT機器とスマートホーム向けのIoT機器を遠隔から管理するシステムを構成する機器（サーバー等）のデータ削除（サニタイズ）を実施すること。
	RMO.4	・スマートホーム向けのIoT機器を遠隔から管理するシステムは、システム内部や管理対象のIoT機器に保存されているデータを削除または読み取りできない状態にする機能を実装すること。 ・スマートホーム向けのIoT機器を遠隔から管理するシステム内部や管理対象のIoT機器が取得する情報や外部に渡す（通信する）情報および、保存されているデータの内容を含むポリシーを提示すること。
	RMO.5	・スマートホーム向けのIoT機器を遠隔から管理するシステムを構成する機器のリプレースや廃棄時に、データ削除（サニタイズ）を行うこと。

■「(3) スマートホーム向けのサービス事業者」に向けたガイドと対策要件の対応関係

ガイド	対策要件ID	対策要件の例
サービスを提供するための事業者システムを適切に運用・管理する	SO.1	・システムが、十分なリソースで構成されていることを確認すること。 ・不要なアクセスや悪質なアクセスを受けるリスクを低減するための措置を講じること。
	SO.2	・システムを構成するサーバやネットワーク機器などの品質や信頼性を確認すること。 ・不要なアクセスや悪質なアクセスを受けるリスクを低減するための措置を講じること。
	SO.3	・システムを構成するサーバやネットワーク機器などの脆弱性が適切に対応されていることを確認すること。 ・システムを構成するネットワークへのアクセスを制限する機能を導入すること。
	SO.4	・サービスを提供するシステムは、システム内部に保存されているユーザーデータを削除または読み取りできない状態にする機能を実装すること。 ・サービスを提供するシステムは、利用者がユーザーデータの削除を求めた場合に、データを削除または読み取りできない状態にする機能を提供すること。 ・システム内で保持する個人情報(パスワード等)は必要に応じ、暗号化して保存する機能を実装すること。
	SO.5	・リプレースや廃棄時に、データ削除（サニタイズ）を行うこと。
サービスのポリシーおよびサービスの利用方法を提供する	SO.6	・住まい手に関するデータ保護などについてのポリシーを提示し、順守すること。

■「(4) スマートホームを供給する事業者」に向けたガイドと対策要件の対応関係

ガイド	対策要件ID	対策要件の例
IoT機器やサービスを正しく設置、設定する	HO.1	・IoT機器に関する動作仕様に基づき、IoT機器の設定や利用方法から想定されるセキュリティインシデントや危害を回避や軽減するためのガイドやポリシーに従い設置と設定を行い、動作状況を確認すること。
セキュアでセーフティなIoT機器を選定する	HO.2	・住宅（住戸）や集合住宅の共用部分に設置するIoT機器およびIoT機器は、IoT機器やIoT機器を含むシステムに提供されるサービスの特性に応じ、セキュリティ機能およびセーフティ機能を確認すること。 ・耐タンパ性が必要な情報を取り扱う場合、耐タンパーデバイスが組み込まれたIoT機器やシステムであることを確認すること。 ・IoT機器やシステムのソフトウェアは完全性を検証可能なIoT機器やシステムであることを確認すること。

■「(5) スマートホーム向けにメンテナンスやサポートを行う事業者」に向けたガイドと対策要件の対応関係

ガイド	対策要件ID	対策要件の例
事業者側のシステムを適切に運用・管理する	SMO.1	・スマートホーム向けサービスのサポートやメンテナンスを行う事業者のシステムの脆弱性に対応する。
サービスととIoT機器のガイドに従った保守・管理を行う	SMO.2	・IoT機器の利用方法、設定方法、機器の内部に保存される情報などをIoT機器のガイドで確認すること。 ・サービスの利用方法、利用環境、サービスで取得する情報などを含め、サービス提供のポリシーを確認すること。
プライバシーポリシーを提示し順守する	SMO.3	・住宅に備え付けのIoT機器のデータ削除（サニタイズ）を実施すること。
	SMO.4	・スマートホーム向けサービスのサポートやメンテナンスを行う事業者の利用する機器のリプレースや廃棄時に、データ削除（サニタイズ）すること。

■「(6) スマートホーム化された分譲共同住宅・団地の管理組合や管理受託会社」および、「(7) スマートホーム化された賃貸住宅の所有者や管理受託会社」に向けたガイドと対策要件の対応関係

ガイド	対策要件ID	対策要件の例
共用部分や賃貸している住戸に設置する機器の選定と、機器やネットワークの管理・運用は適切に行う	CAO.1	・共用部分における住棟内ネットワークおよび住棟内ネットワークに接続された機器を管理すること。
	CAO.2	・住棟内のネットワークに接続された機器の外部のネットワーク接続は、個々に管理するまたは住棟内のネットワークに接続された機器の外部のネットワーク接続を一元的に管理できるように構成すること。
	CAO.4	・集合住宅からの退去時、共用部分および住戸に設置された共用設備であるIoT機器内のデータを削除すること。
	CAO.5	・集合住宅からの修繕時など、共用部分および住戸に設置された共用設備であるIoT機器の変更やサービスのリプレースの際には、IoT機器やサービス内のデータを削除すること。
機器・ 機器やサービスの用途・用法を守る	CAO.3	・集合住宅の修繕時、共用部分または住戸部分に導入される機器およびシステムは、目的とする特性に応じた品質や信頼性の確保につき確認すること。

■「(8) スマートホームの住まい手」に向けたガイドと対策要件の対応関係

ガイド	対策要件ID	対策要件の例
信頼できるIoT機器やサービスを選ぶ	CO.1	・品質や信頼性が確保されたIoT機器およびIoTを含むシステムを導入すること。 ・ソフトウェアアップデートなどにより品質や信頼性が維持されるIoT機器およびIoTを含むシステムを導入すること。
IoT機器やサービスは用途・用法を守る	CO.2	・IoT機器のガイドやサービスのポリシーを確認し利用や管理を行うこと。
	CO.3	・住まい手自ら対応が困難な場合は、スマートホーム向けのIoT機器を遠隔から管理する事業者もしくはスマートホーム向けサービスのサポートやメンテナンスを行う事業者にサポートやメンテナンスを依頼すること。
個人情報は自分で守る	CO.4	・利用を終了したIoT機器とサービス内のデータを削除すること。

添付D サイバー攻撃の事例

スマートホームで利用されると考えられる機器のうち、現時点の普及率が高く身近な製品やサービスで発生したサイバー攻撃や脆弱性の事例を示す。

なお、これらの事例は脅威分析に利用する目的で、攻撃の対象という観点より「1）通信基盤やサービス基盤」「2）IoT 機器」「3）プライバシーに関わる情報」という、3つの分類で整理した。

1） スマートホームを構成する通信基盤やサービス基盤が不正にアクセスされ、システムの機能低下・停止や意図しない第三者攻撃への加担などに繋がる事例
   (1) 無線 LAN 機器
   (2) Bluetooth 機器
   (3) スマートホームコントローラ
   (4) ウェブカメラ

2） スマートホームを構成する IoT 機器などが不正にアクセスされ、主に住居自体への物理的な損害や住まい手の生命・財産を侵害に繋がる事例
   (5) 照明
   (6) 掃除ロボット
   (7) 自動車

3） IoT 機器やサービスを通じて住まい手の個人情報である位置情報やカメラ映像が不正に取得され、プライバシーや生命・財産の侵害に繋がる事例
   (8) クラウドサービス
   (9) おしゃべり人形

(1) 無線 LAN 機器 (2017 年)

主に Wi-Fi で利用される暗号化プロトコルの WPA2 に、プロトコル上の脆弱性が複数発見された。この脆弱性が悪用されると、IoT 機器をはじめとする端末とアクセスポイント間の通信を傍受されるリスクがあるため、公開当初は情報が錯綜し、市場に混乱をきたした事例である。今では後継の暗号化プロトコルに移行しつつあるが、WPA3 などは WPA2 との互換性から、ダウングレード攻撃の攻撃手法も指摘されている。

(2) Bluetooth 機器 (2017 年)

近距離無線通信技術である Bluetooth に複数の脆弱性が発見された。これを悪用されると、スマートフォンなど Bluetooth 搭載機器を乗っ取ることが可能であり、コード実行・不正な情報取得といったリスクがある。また、Bluetooth が有効にさえなっていれば攻撃対象となりうる脆弱性のため、スマート家電をはじめとする様々な IoT 機器に影響が及ぶ事例である。なお、本脆弱性の修正プログラムはリリース済であるものの、アップデートが困難な環境にある機器等は依然としてリスクを残していると考えられる。

(3) スマートホームコントローラ （2019 年）

某セキュリティ企業により、スマートホームコントローラの重大な脆弱性が複数報告された。具体的には、ホームオートメーションに広く採用される Z-Wave という無線通信プロトコルや管理パネルの Web インターフェース、クラウド基盤などが対象であるとされた。これらの脆弱性を組み合わせることで、コントローラに正規でないプログラムをダウンロードさせることができ、例えばAV機器の音量や第三者によるスマート家電の操作等が行えるとされた事例である。

(4) IP カメラ/web カメラ （2018 年～）

家庭内や公共の場所に設置されるIPカメラ（web カメラ）に対して、多くの脆弱性が報告されている。脆弱性の種類としても、アクセス制御に関する事項をはじめさまざまであるが、遠隔からの制御の乗っ取りや、情報の改ざんなど複数の被害が想定される。また所有者が気付かない状態で、意図せず DoS 攻撃や DDoS 攻撃に悪用されサイバー攻撃の加害者になるリスクもある。近年では、カメラを含む IoT 機器を標的にして世界的に感染が広がったマルウェア Mirai の事例もあり、大きな課題となっている。

(5) 照明 （2016 年）

IoT 機能を有する照明機器に脆弱性が報告された。実際は研究目的で行った実証で顕在化したものであるが、実際に電球のスイッチを入／切するマルウェアを開発したという事例である。この脆弱性を利用して一度侵入を許すと、ZigBee の通信機能を利用して、通信エリア内にある他の機器に感染を広げることができることから、スマートホームやスマートシティという将来像において、大きな脅威となり得る事例である。

(6) 掃除ロボット（2017 年）

海外製のロボット掃除機にセキュリティ上の脆弱性が報告された。Wi-Fi 通信と屋内を動き回って監視するモニタリング機能を持つこの掃除機に対して、デバイスの MAC アドレスを知ることにより、システム管理者の権限を乗っ取ることができる脆弱性であった。不正な制御や操作だけでなく、プライバシー侵害のリスクにもつながる事例である。なお、このロボット掃除機は OEM 供給によって他ブランドでも販売されていたこともあり、影響の範囲が広範囲に及んだ事例でもあった。

(7) 自動車

コンピュータによって電子制御される自動車の脆弱性が複数指摘されている。代表的な事例として、米国で行われた自動運転の安全実験が挙げられる。走行中に外部から遠隔操作し、車外の離れた場所から車のコントロールを奪ってしまった初めてのこの実例は、これまでの走行中の車内による実験例とは一線を画していた。他にも以下のような複数の事例が報告されており、今後も大きな課題となる可能性がある。

・スマートフォンのアプリ経由で位置情報の取得やドアロック解除される事例

・Wi-Fi を介して盗難防止アラーム解除や車載ネットワークに不正アクセスされる事例
・スマートフォン専用アプリの脆弱性で、エアコン制御などが行われる事例

(8) クラウドサービス （2018 年）

国内のある自治体において、集団検診の予約などを行うインターネットサイト上に登録された個人情報が流出した事例である。市が管理するクラウドサービスから、名前や電話番号、性別、住所、医療保険種別（個人の健康情報）が流出したこの事例は、直接 IoT 機器やスマートホームと関連する事例ではない。しかしながら、今後、住まい手の健康情報をクラウドで管理するモデルが遠隔医療等に活用されるシーンが想定され、スマートホームのセキュリティ観点で脅威となりうる事例と考えられる。

(9) おしゃべり人形 （2017 年）

欧州の一国において、事実上の「スパイ機器」となっているとして、インターネット接続された玩具（おしゃべり人形）のある製品を使用禁止にした事例である。この玩具は Bluetooth を利用して音声の伝達を行う機能を持つ。しかし暗号化や秘匿化の考慮がなされていなかったため、無線が届く範囲であれば盗聴や録音が可能であったとして、国家が警鐘を鳴らした事例である。

添付E 用語集

あ行

- **IoT** [英] Internet of Things
  IoT とは、従来インターネットに接続されていなかった様々なモノ（センサ機器、駆動装置（アクチュエーター）、建物、車、電子機器など）が、ネットワークを通じてサーバやクラウドサービスに接続され、相互に情報交換をする仕組み。
- **IoT 機器** [英] Internet of Things Device
  センシング、またはアクチュエーティングを通じてフィジカル空間と相互作用し、通信する機器。スマート家電など通信機能を有する機器を示す場合もある。本来は、IoT 機器とはセンサまたはアクチュエータを指す。
- **インシデント** [英] Incident
  望まない単独若しくは一連の事象、又は予期しない単独若しくは一連の事象であって、事業運営を危うくする確率および脅かす確率が高いもの。

か行

- **完全性** [英] Integrity
  正確さ、および完全さの特性。
- **機密性** [英] Confidentiality
  認可されていない個人、主体又はプロセスに対し、情報を使用させず、また開示しない特性。
- **脅威** [英] Threat
  システムや組織に損害を与える可能性がある、望ましくないインシデントの潜在的な原因。
- Connected Industry
  「もの×もの」「人間×機械・システム」「企業×企業」「人間×人間（知識や技能の継承）」「生産×消費」「大企業×中小企業」「地域×地域」「現場力×デジタル」などの多様な協働を通じて、様々なつながりによる新たな付加価値の創出、および従来、独立・対立関係にあったものが融合し、変化することで新たなビジネスモデルが誕生する産業社会のこと。

さ行

- **サイバーセキュリティ** [英] Cyber Security
  電子的な情報の漏えいや改ざんをはじめ、期待されていた IT システムや制御システムなどの機能が果たされないといった不具合が生じないようにすること。
- **サイバー空間** [英] Cyber
  コンピュータ・システムやネットワークの中に広がる仮想空間。デジタル化されたデータを活用して価値を生み出す。
- **サイバー攻撃** [英] Cyber Attack
  資産の破壊、暴露、改ざん、無効化、盗用、又は認可されてないアクセスや使用の試み。
- **サービス** [英] Service
  組織と顧客との間で実行される、少なくとも一つの活動を伴う組織のアウトプット。
- **サプライチェーン** [英] Supply Chain
  複数の開発者間でリンクされたリソース・プロセスで、製品とサービスについて、調達に始まり設計・開発・製造・加工・販売および購入者への配送に至る一連の流れ。

- **識別子** [英] Identifier
  ある主体を他の主体と明確に区別する情報。
- **ZigBee**
  センサネットワーク、IoT、家電の遠隔制御に用いられる近距離無線通信規格。
- **信頼性** [英] Reliability
  信頼又は信用に値する特性。IoT の文脈では、IoT 実装のライフサイクル全体の中でセキュリティ、プライバシー、セーフティ、リライアビリティ、およびレジリエンスを保証するための信頼、または信用に値する特性を指す。
- **ステークホルダー** [英] StakeHolder
  意思決定若しくは活動に影響を与え、影響されることがある又は影響されると認知している、あらゆる人又は組織。
- **脆弱性** [英] Vulnerability
  一つ以上の脅威によって付け込まれる可能性のある、資産又は管理策の弱点。
- **セーフティ（安全性）** [英] Safety
  危害を引き起こすおそれがあると思われるハザードから守られている状態。
- **センサ** [英] Sensor
  音・光・温度・圧力などの物理量を検出して信号に変える装置。IoT では 1 つ以上の物理的な主体の 1 つ以上の特性を測定し、ネットワーク経由で送信可能なデジタルデータを出力する IoT 機器を指す。
- **Society5 .0**
  サイバー空間（仮想空間）とフィジカル空間（現実空間）を高度に融合させたシステムにより、経済発展と社会的課題の解決を両立する、人間中心の社会。狩猟社会（Society 1.0）、農耕社会（Society 2.0）、工業社会（Society 3.0）、情報社会（Society 4.0）に続く、新たな社会を指すもので、第5期科学技術基本計画において我が国が目指すべき未来社会の姿として初めて提唱された。

た行

- **ダウングレード攻撃** [英] Downgrade attack
  古いバージョンとの下位互換性を持たせた通信プロトコルにおいて、互換性のある動作をさせた場合に古いバージョンが持つ脆弱性を利用した攻撃が可能なことを利用した攻撃手法。
- **DDos 攻撃** [英] Distributed Denial of Service attack
  DoS 攻撃を発展させ、複数のコンピュータや IoT 機器を利用することで、DoS 攻撃を大規模化、高度化した攻撃手法。攻撃の高度化の例としては、多数の IoT 機器を利用することで、DoS 攻撃に対する防御措置を無効化し被害を与えるなどがある。
- **DoS 攻撃** [英] Denial of Service attack
  ウェブサービスを提供しているサーバに対する大量アクセスや、大量のメールを特定のメールサーバに送信するなどにより、ネットワークとサーバを過負荷な状態に陥らせ円滑なサービスを妨害、または過負荷な状態で利用可能となる脆弱性を狙う攻撃手法。

な行

は行

- **フィジカル空間** [英] Physical space

現実の世界。サイバー空間と物質から構成される世界とを区別するための表現。

- Bluetooth
  約 10m 以下の範囲で通信が可能な、IoT、家電制御、スマートフォンや住設機器の間での情報交換や制御に用いられる近距離無線通信規格。
- **プロセス** [英] Process
  インプットをアウトプットに変換する、相互に関連する又は相互に作用する、論理的又は物理的な一連の活動。
- **プロトコル** [英] Protocol
  複数の主体が滞りなく信号やデータ、情報を相互に伝送できるよう、あらかじめ決められた約束事や手順の集合のこと。
- HEMS [英]Home Energy Management System
  家庭内で使うエネルギーを管理し、エネルギー利用の効率化や、節約するための管理システム。太陽光パネルの発電状況や、サービス提供事業者からのインフォメーションなどの表示機能を有するものがある。
- **ポリシー** [英] Policy
  トップマネジメントによって正式に表明された組織のセ意図や方向付け、およびそのような意図や方向付けに基づいて対策を行うために組織が定めた規定。

ま行

- **マルウェア** [英] Malware
  許可されていないプロセスの実施を試みることによって、情報システムの機密性・完全性・可用性に悪影響をもたらすソフトウェア、またはファームウェア。セキュリティ上の被害を及ぼすウイルス、スパイウエア、ボットなどの悪意を持ったプログラムを指す総称。

や行

ら行

- LAN [英] Local Area Network
  家庭内や組織内部のネットワークを示すことが多い。建物内部などの限られた範
- **リスク** [英] Lisk
  不具合が生じ、それによって自組織や取引先などの関係する他組織の目的、または社会全体に何らかの影響が及ぶ可能性。
- **リスク源** [英] Risk Source
  それ自体又は他との組合せにより、リスクを生じさせる力を本来潜在的にもっている要素。
- **ルータ** [英] Router
  広域通信網（インターネット等）とアクセスを行うために家庭内または組織内のネットワーク（LAN）の中継を行う装置。

わ行

- Wi-Fi
  米国の Wi-Fi アライアンスが規定する無線 LAN に関する規格。無線 LAN の国際標準である IEEE 802.11 規格に準拠した製品のうち、相互接続が確認されたもの。

添付 F 参考文献

ガイドライン本文中で参照

- 「サイバー・フィジカル・セキュリティ対策フレームワーク」

発行元	経済産業省
概要	経済産業省が「Society5.0」、「Connected Industries」によって拡張したサプライチェーンの概念に求められるセキュリティへの対応指針を整理したもの。
参照先	https://www.meti.go.jp/press/2019/04/20190418002/20190418002.html

- 「IoT セキュリティガイドライン」

発行元	IoT 推進コンソーシア・総務省・経済産業省
概要	IoT 機器全体をカバーする共通事項を中心にまとめられている。
参照先	http://www.IoTac.jp/ https://www.soumu.go.jp/main_sosiki/joho_tsusin/security/enduser/security01 https://www.meti.go.jp/press/2016/07/20160705002/20160705002.html

- 「つながる世界の開発指針」

発行元	独立行政法人情報処理推進機構／社会基盤センター
概要	IoT 機器における開発者視点から、セキュリティ対策がまとめられている。
参照先	https://www.ipa.go.jp/sec/publish/tn16-002.html

あわせて読むことを推奨

- ビルシステムにおけるサイバー・フィジカル・セキュリティ対策ガイドライン

発行元	産業サイバーセキュリティ研究会　ワーキンググループ 1(制度・技術・標準化) ビルサブワーキンググループ
概要	ビルシステムを構成する全てのサブシステムにおける共通的なセキュリティ対策を整理したもの。マンション等の共用部分に対するセキュリティ対策の参考となる。
参照先	本文:https://www.meti.go.jp/press/2019/06/20190617005/20190617005_01.pdf

- CCDS 分野別セキュリティガイドライン_スマートホーム編

発行元	一般社団法人 重要生活機器連携セキュリティ協議会
概要	スマートホーム分野におけるセキュリティ上のリスク分析、およびリスク評価によりスマートホームを構成する機器のセキュリティについて整理し、脅威のレベルや保護すべき情報資産の重要度に応じ 3 段階に分類したもの。
参照先	https://www.ccds.or.jp/public/document/other/CCDS 製品分野別セキュリティガイドライン_スマートホーム編_Ver.1.0.pdf https://www.ccds.or.jp/public/document/other/CCDS 製品分野別セキュリティガイドライン-概要説明資料_スマートホーム編_Ver.1.0.pdf https://www.ccds.or.jp/public/document/other/CCDS 製品分野別セキュリティガイドライン_スマートホーム編_Appendix_Ver.1.0.pdf