# 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

Version 1.0

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）
スマートホームサブワーキンググループ

令和 3 年 4 月 1 日

# 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、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、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セキュリティに関する基本的な指針を示すものである。さら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、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。なお、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、対象は戸建住宅や共同住宅等の住宅である [1]。これら住宅では、企業のような専任の管理者がいない場合が一般的であり、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、添付 D に示す事例のように、IoT 機器の脆弱性、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ドアの開錠や空調などの家電の不正操作といったフィジカル空間のセーフティまで影響を及ぼす可能性もある。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、住宅の様々な IoT 機器がサイバー攻撃の対象となるため、

---

1 なお，本書で扱うスマートホームの形態には、戸建、共同住宅、持ち家、賃貸がある。戸建と共同住宅は、建物に含まれる住戸数によって決まる住宅の形態である。戸建は、建物が 1 つの住戸である住宅である。これに対して、複数の住戸で構成される建物を共同住宅（もしくは集合住宅）という。また、持ち家と賃貸は、住宅の所有によって決まる住宅の形態である。持ち家は、自己が所有し居住する住宅である。これに対して、賃貸は他人が所有する住宅を借りて居住する住宅の形態である。これら以外にも詳細な住宅の形態の違いはありうる。このように住宅といっても、それらの形態は異なり、所有者や管理の主体が区画によって異なることはありうる。このため、住まい手や所有者は注意が必要である。

セキュリティ対策が必要な機器の数は膨大となる。さらに、スマートホームには様々なステークホルダーが関与し、多様な脅威に対しステークホルダーがそれぞれで対応する必要がある上、建物と併用される IoT 機器は、長期に渡って利用されることから、継続的なセキュリティ確保が必要となる。

本ガイドラインは、市場が広がりつつあり、多岐にわたるサービスが予想される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。

なお、本ガイドラインでは、サイバーフィジカルシステムの一つであるスマートホームについて、主にサイバーセキュリティを強化するために、関係するステークホルダーが実施すべき基本的なセキュリティ指針を示すことを目的とする。個人情報やプライバシーの保護、不正侵入などに対する物理セキュリティ、データ連携時のセキュリティ、システム間連携時のセキュリティ、地震などの緊急時に必要となるセキュリティ等については考慮していない。セーフティについては、サイバー攻撃によって IoT 機器の動作に影響を及ぼすような一次的な影響については考慮した。それ以外の二次的な影響については今回のガイドラインでは考慮していない(例えば、断続的なサイバー攻撃によって、動力源を消費させ結果的にセーフティに影響を与える等である)。

## 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 [2]。

(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 家電や防犯カメラの製造元(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の事業者などがある。

(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ーと、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)

---

2 直接的なステークホルダー(一次ステークホルダー)だけでなく、一次ステークホルダーからの委託先、さらに再委託先等、契約等でセキュリティ・セーフティの対策が求められる関係者も対象である。

(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、施工業者などが挙げられる。

(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** [3]

区分所有型の共同住宅や団地において、共用スペース [4]に設置された IoT 機器や住棟内ネットワーク [5]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 [6]。

(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**

賃貸住宅の所有者(オーナー)や、所有者から管理業務を委託された管理委託会社等である。例えば、賃貸型の共同住宅の共用スペースに設置された機器や共用スペースのネットワーク回線の管理者である。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。

なお、賃貸型の戸建住宅の宅内 [7]や共同住宅の住戸内について、未入居の状況の場合には、所有者や管理受託会社が、戸建住宅や住戸 [8]を主体的に管理する。一方で、スマートホームの住まい手となる賃借人が入居した時点で管理の主体は賃借人となる。

(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(戸建住宅、共同住宅、持ち家、賃貸等の形態によらない)。主として IoT 機器を利用したサービスを受ける者である。

---

[3] 分譲共同住宅の管理組合や賃貸共同住宅の所有者(オーナー)と管理受託会社が締結する契約等に、共用スペースの IoT 機器やネットワーク回線等を管理する条項が含まれている場合には、原則として条項の内容に従う。

[4] 本書で示す共用スペースは、特に注意書きが無い限り、共同住宅等において共用で利用する箇所のみを指し、特定の住まい手が実質的に専用で利用する箇所は含めない。例えば、階段、エレベーターホールは共用スペースであるが、バルコニーや専用庭は共用スペースには含めない。定義は添付Eを参照されたい。

[5] 分譲共同住宅・団地の廊下や階段等の共用部分は、区分所有法でいうところの区分所有者が共同で所有するものである。このため、共用部分に設置された IoT 機器やネットワーク回線等は、原則として、区分所有者によって組織された管理組合が管理・運営する必要がある。共用部分の管理においては、その対象に応じた管理方法や責任範囲を検討する必要がある。

[6] 例えば、共同住宅の共用部分に設置された IoT 機器等がサイバー攻撃の対象となった場合、対応する主体が共用部分の所有者(分譲共同住宅の場合は全ての区分所有者)となることに留意が必要である。

[7] 本書では、戸建住宅における住宅内のことを指す。建物がある敷地内をいい、ベランダや庭を含む。

[8] 本書では、共同住宅における住宅内のことを指す。ベランダや専用庭などを含む。

## 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（2021 年 3 月）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」を実現するものであるとして、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は、直接的・間接的[9]に通信ネットワーク（インターネットなど）に接続する IoT 機器とサービスが連携するという基本的な IoT システムの特徴を備えているものとする。

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、そのネットワーク構成例や関連するステークホルダーについて、「1.3.1. 戸建住宅の例」、および「1.3.2. 共同住宅の例」を示す。なお、ここでのサービスは、IoT 機器を利用したスマートホーム向けのサービスのことである。以降、本書でのサービスは特に断りがない限り同じ意味で利用する。

### 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と、入居後に住まい手が IoT 機器やサービスを導入している場合のいずれかもしくはいずれも想定している。

なお、図 1 に示す宅内ネットワークは、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 のような表現としている。

---

[9] 直接的とは、例えばスマートメーターのよう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。

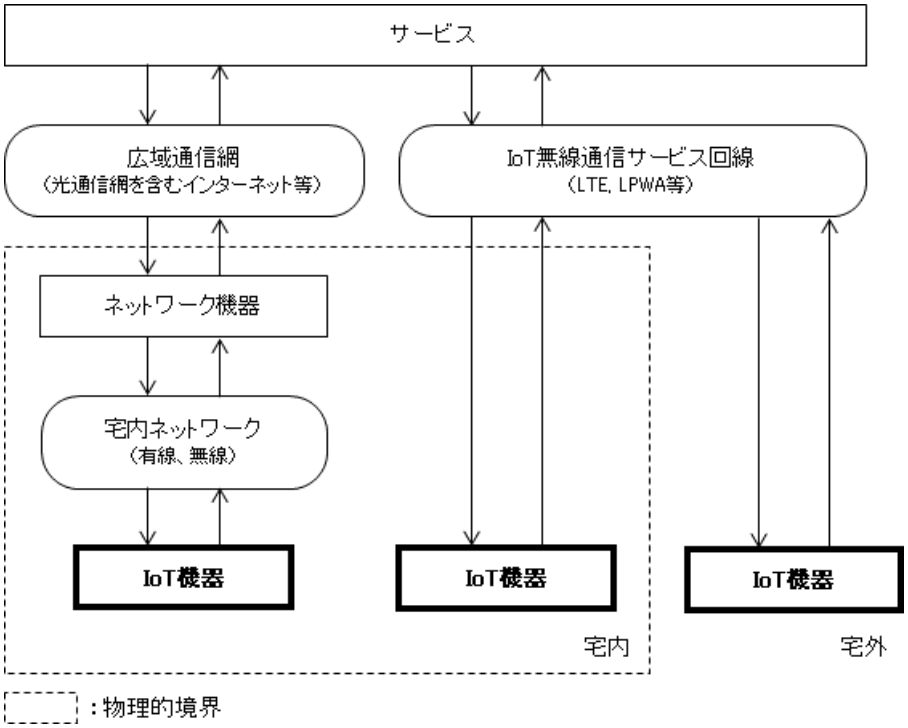


図 1.戸建住宅のネットワークの例

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<br>・ 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、<br>IoT 無線通信サービス回線 | （通信インフラ事業者） |
| 宅内ネットワークとネットワーク機器 | （スマートホームを供給する事業者から引き渡されるまで）<br>・ スマートホームを供給する事業者<br>（引き渡し後）<br>・ スマートホームの住まい手<br>・ 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 |
| IoT 機器 | （スマートホームを供給する事業者から引き渡されるまで、またはスマートホーム向け IoT 機器の事業者から購入するまで）<br>・ スマートホームを供給する事業者<br>・ スマートホーム向け IoT 機器の事業者<br>（引き渡し後または購入後）<br>・ スマートホーム向け IoT 機器の事業者<br>・ 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<br>・ 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<br>・ 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、共用スペース、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含め、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。

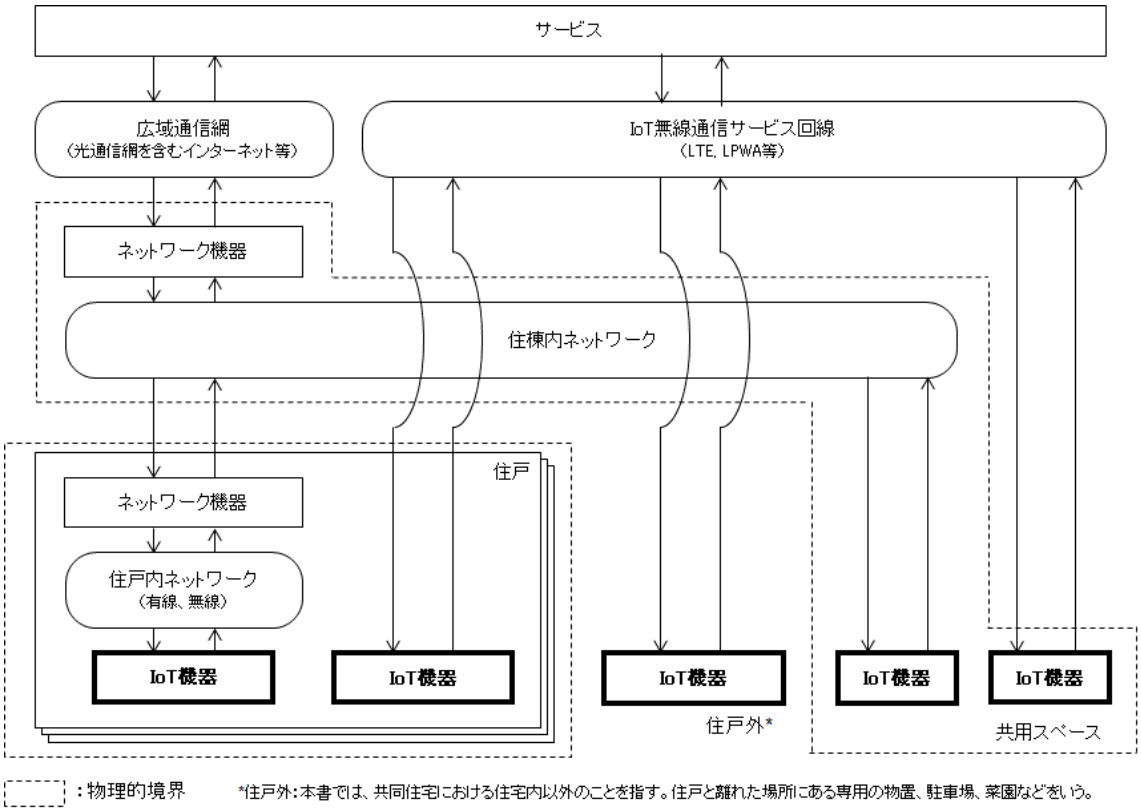


**図 2.共同住宅のネットワーク構成の例**

住まい手が IoT 機器を介し、また共同住宅の共用スペースの 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<br>・ 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、<br>IoT 無線通信サービス回線 | （通信インフラ事業者） |
| 住棟内ネットワークとネットワーク機器 [10] | （住棟内ネットワークが管理主体 [11]に引き渡されるまで）<br>・ スマートホームを供給する事業者<br>（引き渡し後）<br>・ 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<br>・ 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 |
| 共用スペースの IoT 機器 [12] | （共用スペースの IoT 機器の管理主体に引き渡されるまで、またはスマートホーム向け IoT 機器の事業者から購入するまで）<br>・ スマートホームを供給する事業者<br>・ スマートホーム向け IoT 機器の事業者<br>（引き渡し後または購入後）<br>・ スマートホーム向け IoT 機器の事業者<br>・ 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<br>・ 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<br>・ 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<br>・ 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 |
| 住戸内ネットワークとネットワーク機器 | （スマートホームを供給する事業者から引き渡されるまで）<br>・ スマートホームを供給する事業者<br>（引き渡し以降）<br>・ スマートホームの住まい手<br>・ 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<br>・ スマートホーム化された賃貸住宅の所有者または管理受託会社 |
| 住戸内の IoT 機器 | （スマートホームを供給する事業者から引き渡されるまで、またはスマートホーム向け IoT 機器の事業者から購入するまで）<br>・ スマートホームを供給する事業者 |

10 共同住宅では、機器の設置場所の違いで管理主体が異なり、責任の主体が曖昧になりがちである。例えば、共用スペースのルーターのファームウェアアップデートなどの対策は誰が責任主体なのかを明確にしておくことが望まれる。また、管理する機器についても、その機器の構成や機能等により行うべき具体的なセキュリティ対策が異なり、例えば、ルーター等の通信機器ではファームウェアのアップデートや強いパスワードの設定が必要である。一方で、分岐機器等の単純な装置では物理的な対策のみが必要となる。特に、どのような機器が共用スペースに設置されるかは契約する通信サービスに依存する。このため、共用スペースの管理者はどのような機器が存在し、セキュリティを確保する上でどのような管理をすべきかの確認が必要である。また、共用スペースには、管理用 PC なども設置されているケースもあり、そのセキュリティを確保することが必要である（ただし、共用スペースの管理用 PC については本書では考慮していない）。

11 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、またはスマートホーム化された賃貸住宅の所有者であるが、IoT 機器やネットワーク回線等の管理を契約等により管理受託会社等（場合によってはその下請け再委託先も含む）に委託する場合、管理受託会社等も管理主体となる。

12 共用スペースの IoT 機器とは、例えば、緊急地震速報の受信装置などである。

| 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<br>（引き渡し後または購入後）<br>・ スマートホームの住まい手<br>・ スマートホーム向け IoT 機器の事業者<br>・ 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<br>・ 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<br>・ 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（賃貸住宅で未入居の場合） |

## 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、それらの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等の IoT 機器が急速に増加している。これにより、IoT 機器と他の機器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ー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、各種 IoT 機器とサーバとの橋渡しを行う 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 5330 万世帯[13]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[14]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として生活に根付いているものもある。スマート家電等の IoT 機器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が報告されている。これらは、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。

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や脆弱性の具体的な事例を「添付 D サイバー攻撃と脆弱性等の事例」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つながるのかを整理している。

(1) 「通信基盤やサービス基盤」の事例
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つながる事例

(2) 「IoT 機器」の事例
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・財産の侵害などにつながる事例

---

[13] 出典 総務省統計局「日本の統計 2020」

[14] 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

(3) 「プライバシーに関わる情報」の事例

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、プライバシーの侵害などにつながる事例

なお、本ガイドラインでは、主に上記の「攻撃の対象」という観点に基づき脅威や脆弱性を抽出している。

## 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ワーキンググループ 1(制度・技術・標準化)の下で産業分野別に行われている検討のひとつとして位置付けられている。この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)では、Society 5.0(サイバー空間とフィジカル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)』[15]を策定した。

CPSF 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。

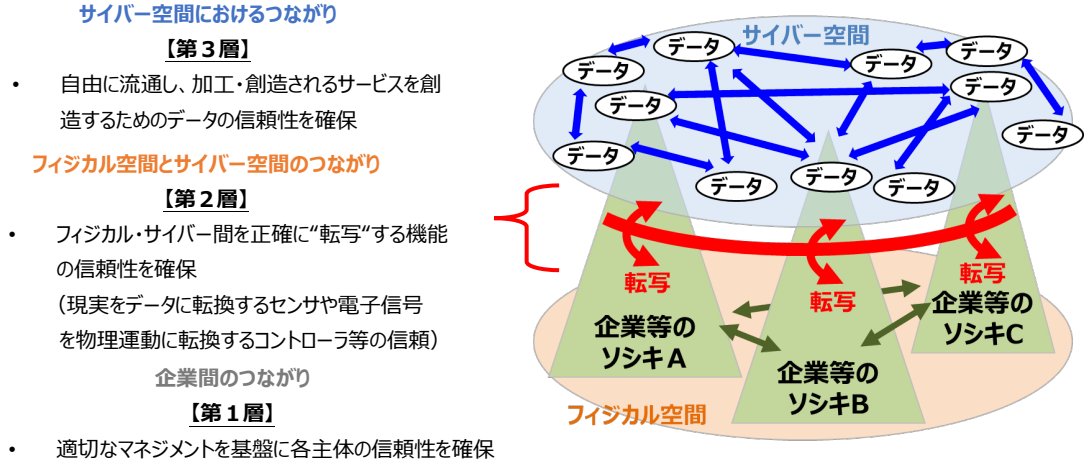


図 3.サイバー・フィジカル・セキュリティ対策フレームワーク(CPSF)の3層構造

[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、まとめたものである。

15 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)

# 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 スマートホームにおけるセキュリティ上の脅威」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),(3)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・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。

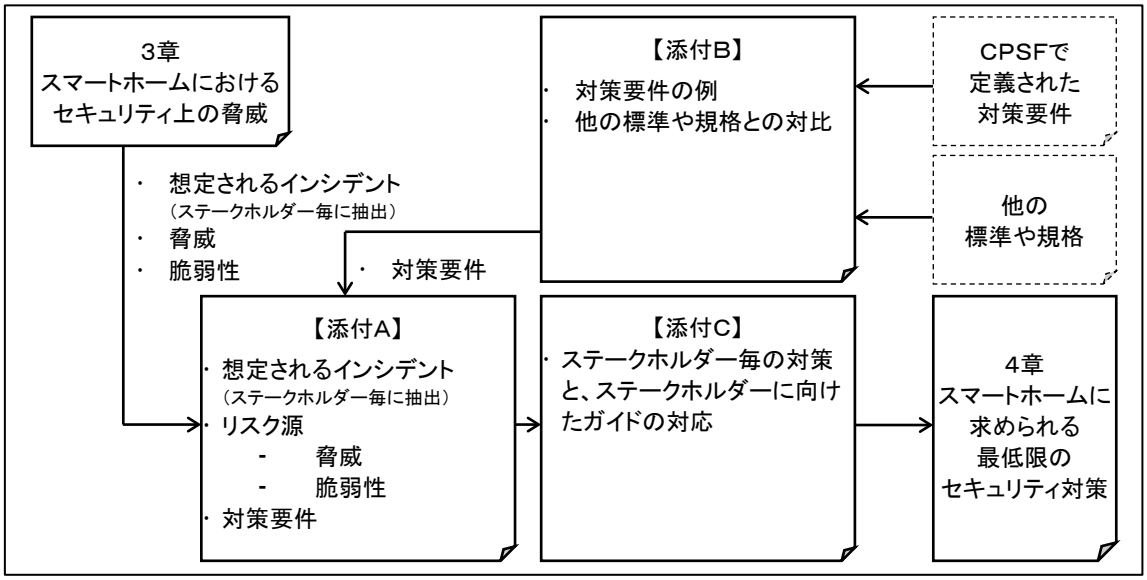


図 4.セキュリティ対策の検討

## 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、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<br>・ 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<br>・ 遠隔から IoT 機器を管理するシステムの脆弱性は、IoT 機器への不正な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<br>・ 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洩・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<br>・ 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洩、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 IoT 機器や通信機器 | ・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、IoT 機器や通信機器の設定およびメンテナンスは、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（共同住宅） | ・ 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 IoT 機器や通信機器の管理 | ・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 IoT 機器や通信機器の管理が、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 | ・ 住棟内ネットワーク及び住棟内ネットワークに接続された IoT 機器や通信機器の管理 | ・ 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 IoT 機器や通信機器の管理が、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 機器の選定、設置、設定により、影響を受ける可能性があるため<br>・ 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など、データの再利用防止が必要であるため |

# 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のユースケースでは、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念頭に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等の住宅や住まい手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について示す。

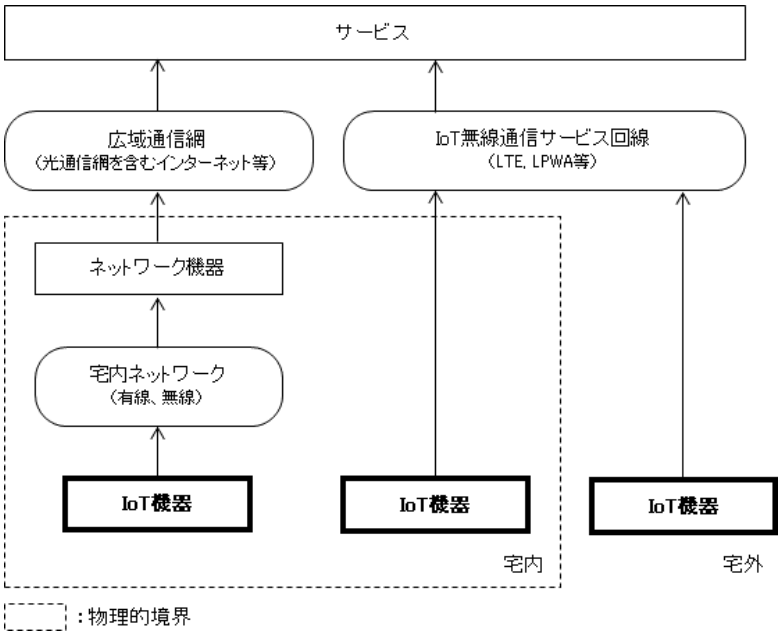


図 5.スマートホームからサイバー空間へ（戸建住宅の場合）

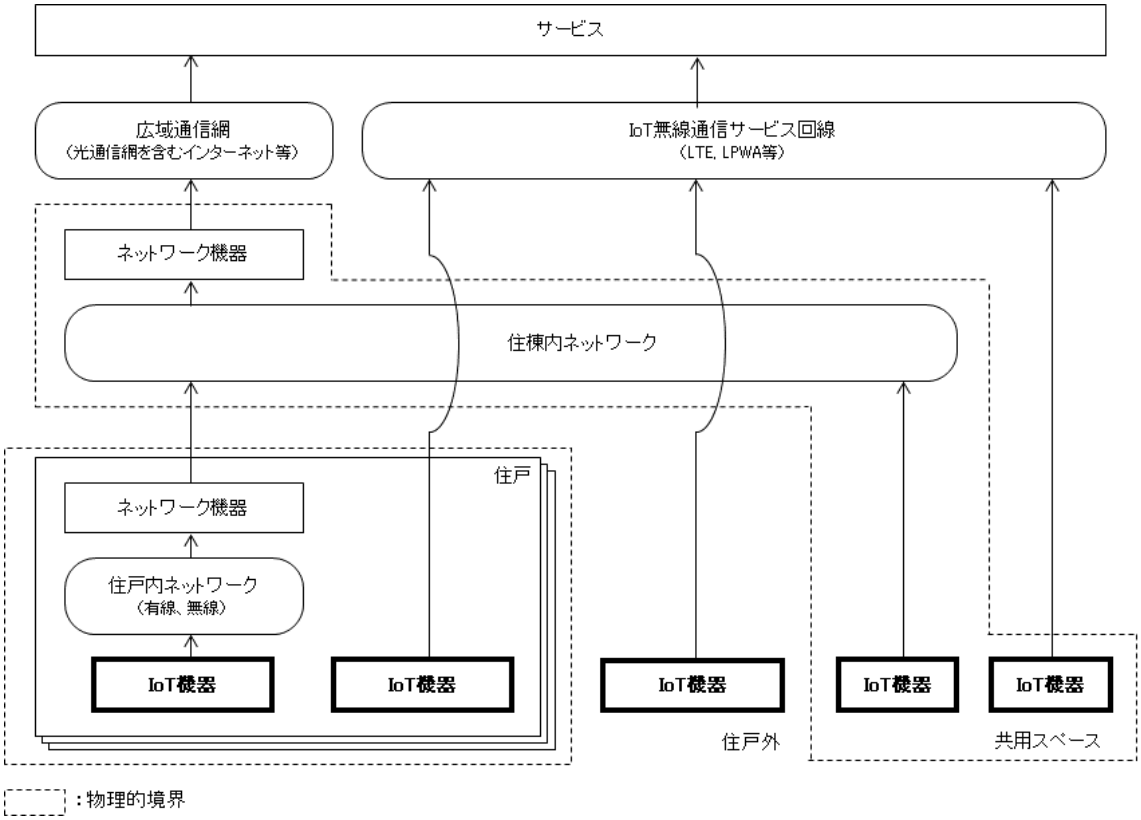


図 6.スマートホームからサイバー空間へ（共同住宅の場合）

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。<br>・ 戸建住宅のデータは、IoT 機器から、宅内ネットワーク、広域通信網と順に通過して、サービスに到達する経路となる。<br>・ 共同住宅の住宅内データは、住戸内の IoT 機器から、住戸内ネットワーク、住棟内ネットワーク [16]、広域通信網と順に通過して、サービスに到達する経路となる。<br>・ 共同住宅の共用スペースのデータは、共用スペースの IoT 機器から、住棟内ネットワーク、広域通信網と順に通過してサービスに到達する経路となる。<br>・ IoT 無線通信サービス回線を利用する場合には、データは、IoT 機器から IoT 無線通信サービス回線を通過してサービスに到達する経路となる。 |
| 前提条件 | 【戸建住宅の場合】<br>・ IoT 機器は、住まい手自身が購入、または/および、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。<br>【共同住宅の住戸の場合】 |

16 本書では、建物内に存在する共用スペースのネットワークのことを指す。共用スペースのネットワークは、住まい手が管理すべき住戸のネットワークとは異なる者が一般的に管理する。例えば、分譲住宅では、階段等の共用部分は、各住戸の住まい手が共同して所有・管理する位置付けであり、各住戸の住まい手から構成される管理組合が、共用部分の機器やネットワークを主体的に管理・運用する必要がある。

| | |
|---|---|
| | IoT 機器は、住まい手自身が購入、または/および、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。<br>【共同住宅の共用スペースの場合】<br>・ IoT 機器は、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。もしくは、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によって据え付けられることもある。<br>【IoT 機器共通】<br>・ なし。<br>【サービス】<br>・ 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】<br>2） デジタル情報に変換されたデータは、宅内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。 |
| | 【共同住宅の住戸の場合】<br>2） デジタル情報に変換されたデータは、住戸内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。 |
| | 【共同住宅の共用スペースの場合】<br>2） デジタル情報に変換されたデータは、住棟内ネットワークに送られ、住棟内ネットワーク、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】<br>2） 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。<br>・ 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。<br>・ 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。<br>・ 「添付 D サイバー攻撃と脆弱性等の事例」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窃取され、人体へのダメージや財産の侵害につながる。 |
| 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。<br>・ 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、宅内ネットワーク、および宅内ネットワークに接続されている IoT 機器以外の機器が、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 IoT 機器以外の機器、および住戸内ネットワーク、住戸内ネットワークに接続されている IoT 機器以外の機器が、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) |
| | ・ 戸建住宅の宅内ネットワーク、共同住宅の住戸内ネットワークに接続されている IoT 機器以外の機器および共同住宅の住棟内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) |
| | ・ スマートホーム向けのサービスを実行するサーバ等の機器の信頼性が低い、機器が攻撃を受ける、または脆弱性対策が行われていない。 | (U1_V.7) |
| | ・ スマートホーム向けのサービスを実行するサーバ等の機器の交換や廃棄時、機器内のデータ消去など、データの再利用が防止されていることを確認していない。 | (U1_V.8) |
| | ・ 住まい手などが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の交換時、個人情報などのデータ消去など、データの再利用が防止されていることが確認されていない。 | |
| | ・ スマートホーム向けの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。 | (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データを利用することでサービスを提供するモデルである。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イバー空間を通じて宅内や住戸内の IoT 機器を操作する、サイバー空間にある道路交通情報を受ける、地域情報を受けるなどの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、住まい手に対して 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。

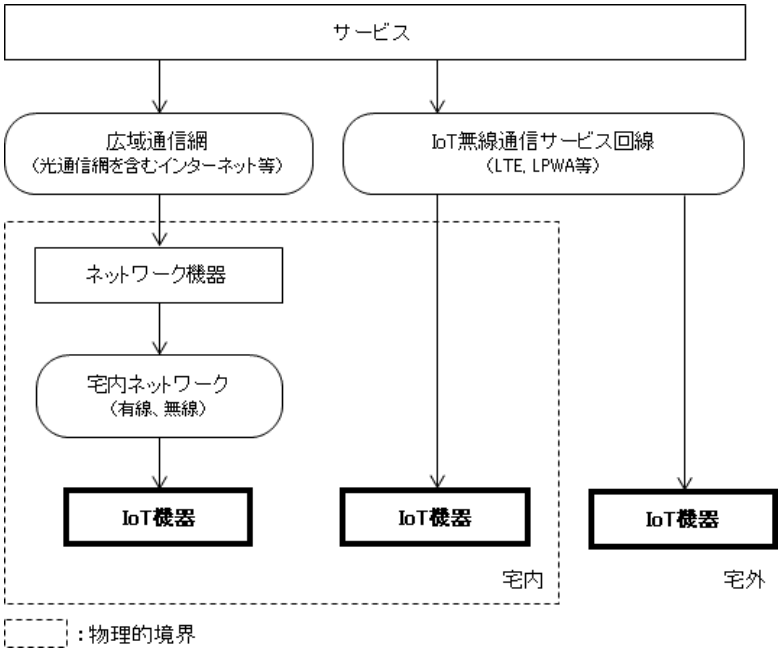


図 7.サイバー空間から IoT 機器へサービス提供（戸建住宅の場合）

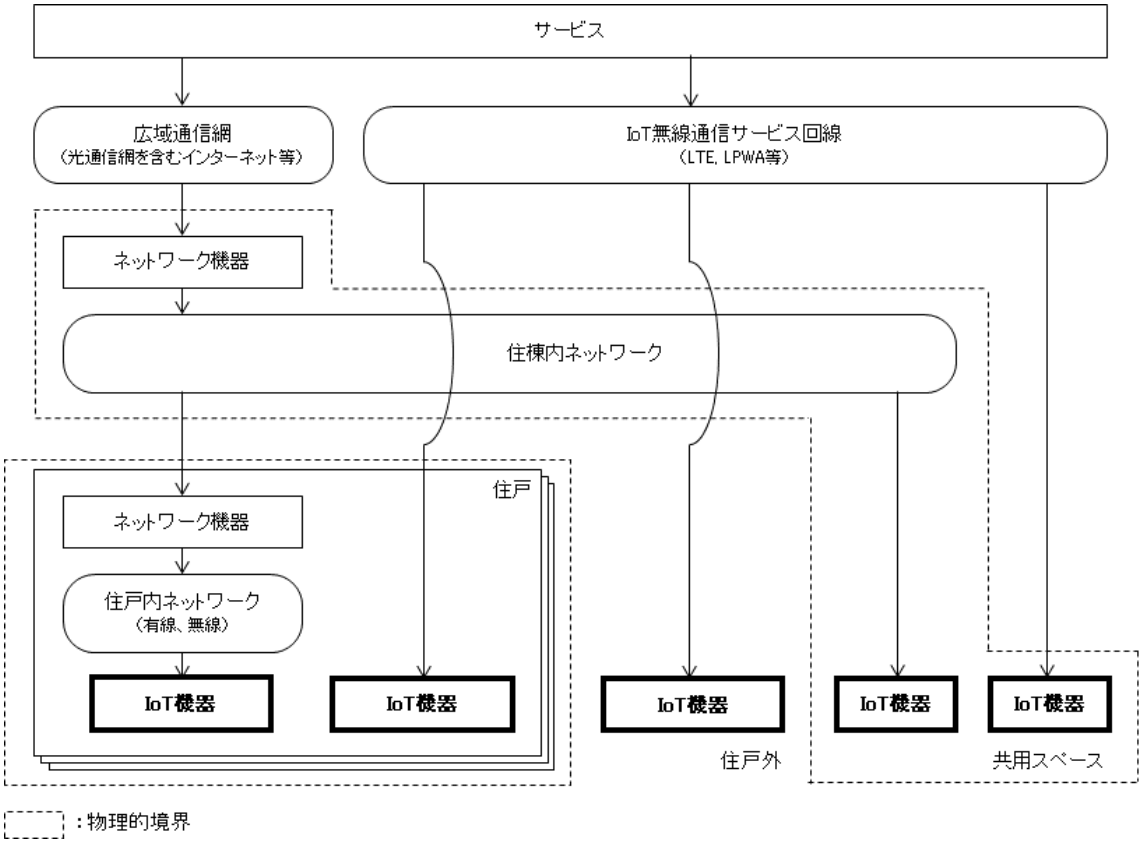


図 8.サイバー空間から IoT 機器へサービス提供（共同住宅の場合）

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。<br>・ 戸建住宅の IoT 機器に至るデータは、サイバー空間から、広域通信網、宅内ネットワークと順に通過して、IoT 機器に達する経路となる。<br>・ 共同住宅の住戸の IoT 機器に至るデータは、サイバー空間から、広域通信網、住棟内ネットワーク、住戸内ネットワークと順に通過して、IoT 機器に達する経路となる。<br>・ 共同住宅の共用スペースの IoT 機器に至るデータは、サイバー空間から、広域通信網、住棟内ネットワークと順に通過して、IoT 機器に達する経路となる。<br>・ IoT 無線通信サービス回線を利用する場合のデータは、サイバー空間から、IoT 無線通信サービス回線を通過して、IoT 機器に達する経路となる。 |
| 前提条件 | 【戸建住宅の場合】<br>・ IoT 機器は、住まい手自身が購入、または/および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。<br>【共同住宅の住戸の場合】<br>・ IoT 機器は、住まい手自身が購入、または/および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。<br>【共同住宅の共用スペースの場合】<br>IoT 機器は、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。もしくは/および、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によって据え付けられることもある。<br>【IoT 機器共通】<br>・ なし。<br>【サービス】<br>・ 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とおり正常に設定、運用されている。 |
| 基本フロー | 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。 |
| | 【戸建住宅の場合】<br>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、宅内ネットワークに送られ、IoT 機器が受け取る。 |
| | 【共同住宅の住戸内の場合】<br>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、住棟内ネットワーク、住戸内ネットワークに送られ、IoT 機器が受け取る。 |
| | 【共同住宅の共用スペースの場合】<br>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、住棟内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】<br>2) 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 | ・ 戸建住宅の宅内や共同住宅の住戸内の IoT 機器、共同住宅の共用スペースの 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ていない動作をする。<br>・ 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 サイバー攻撃と脆弱性等の事例」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、主に戸建住宅の宅内や共同住宅の住戸内や共用スペースで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。<br>・ 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 サイバー攻撃と脆弱性等の事例」の(1)に示されるように、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・停止や意図しない第三者攻撃への加担などにつながる。 |
| 脅威 | ・ IoT 機器が攻撃を受けることにより、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／意図しない動作をする。<br>・ 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。<br>・ 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)<br>IoT 機器が、戸建住宅や共同住宅の他の機器やシステムと連携する場合、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。<br>・ 暗号化されていない無線通信など、IoT 機器の脆弱性対策が行われていない。 (U2_V.2)<br>・ 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)<br>また、IoT 機器が、戸建住宅や共同住宅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。<br>・ 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)<br>・ 戸建住宅では、宅内ネットワーク、および宅内ネットワークに接続されている IoT 機器以外の機器が、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)<br>・ 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 IoT 機器以外の機器、住戸内ネットワーク、および住戸内ネットワークに接続された IoT 機器以外の機器が、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)<br>・ 戸建住宅の宅内ネットワークに接続されている IoT 機器以外の機器、共同住宅の住戸 IoT 機器以外の機器、住棟内ネットワークに接続されている IoT 機器以外の機器について、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。

## 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

戸建住宅と共同住宅の 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・売却・廃棄を扱う。また共同住宅における共用スペースの 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。

戸建住宅と共同住宅の IoT 機器におけるライフサイクルの想定シーンの以下の 2 つのケースについて、それぞれ別の表に整理する。

・宅内と住戸内の IoT 機器

・共同住宅の共用スペースの IoT 機器

【宅内と住戸内の IoT 機器】

| | |
|---|---|
| 概要 | 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 IoT 機器の更新やサービスの見直し、退去による IoT 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 | 【戸建住宅の場合】<br>・ スマートホームを供給する事業者により、予め宅内ネットワークや IoT 機器が据え付けられている場合がある。<br>【共同住宅の住戸の場合】<br>・ スマートホームを供給する事業者により、予め住戸内ネットワークや IoT 機器が据え付けられている場合がある。<br>・ 住棟内ネットワークと住戸ネットワーク回線は接続されており、共用スペースの IoT 機器や他の住戸の IoT 機器との通信と相互に影響しないように設定されている。<br>【サービス】<br>・ なし。<br>【IoT 機器共通】<br>・ なし。 |
| 基本フロー | 【IoT 機器の設置・設定】<br>1) 予め宅内ネットワーク、住戸内ネットワークや 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 IoT 機器以外の機器の設置・設定を行う。 |
| | 【転居等による IoT 機器の他者への譲渡】<br>1) 予め宅内ネットワーク、住戸内ネットワークや 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 機器を宅内や住戸内に残した状態で転居や販売を行う。 |
| | 【IoT 機器の更新】<br>1) 予め宅内ネットワーク、住戸内ネットワークや 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提供のポリシーの変更などにより、IoT 機器や IoT 機器以外の機器を交換する。 |
| | 【IoT 機器の廃棄】<br>1) 予め宅内ネットワーク、住戸内ネットワークや 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 IoT 機器以外の機器の返却や廃棄を行う。 |

【共同住宅の共用スペースにおける IoT 機器】

| | |
|---|---|
| 概要 | 共同住宅の共用スペースにおける IoT 機器の設置、設定、サービスの開始、IoT 機器の更新やサービスの見直し、IoT 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 | ・ IoT 機器やネットワーク設備は、一般的に、分譲共同住宅・団地の区分所有者または賃貸住宅の所有者への引き渡し前に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って据え付けられる。引き渡し後については、分譲共同住宅・団地の管理組合、または賃貸住宅の所有者等により IoT 機器が据え付けられる。<br>・ 住まい手（または住まい手同士）の決議によって、新たな機器を設置する場合もある。<br>・ 共用スペースの 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、共用スペースや住戸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】<br>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 IoT 機器以外の機器の設置・設定を行う。 |
| | 【IoT 機器の更新】<br>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提供のポリシーの変更などにより、IoT 機器や IoT 機器以外の機器を交換する。 |
| | 【IoT 機器の廃棄】<br>1) サービスの解約により事業者が、IoT 機器や IoT 機器以外の機器の返却や廃棄を行う。 |

戸建住宅と共同住宅の IoT 機器において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 | ・ 事業者のサービス提供のポリシーが開示されないことや正しく運用されないことなどの不備により、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。<br>・ 事業者のサービス提供の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洩する。<br>・ 利用者の個人情報が流出する。<br>・ 事業者のセーフティに関するサービス提供のポリシーが開示されないことや正しく運用されないことなどの不備により、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洩する。 |
| 脅威 | ・ | 事業者のサービス、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開示されないことや正しく運用されないことで、利用者に不利益が生じる。 |
| | ・ | 誤操作により、IoT 機器や IoT 機器以外の機器が意図しない動作をする。 |
| | ・ | 戸建住宅に新たに設置する 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、宅内ネットワーク、および宅内ネットワークに接続されている他の機器に干渉する。 |
| | ・ | 共同住宅の住戸に新たに設置する 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、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、住戸内ネットワーク、住戸内ネットワークに接続された新たに設置する IoT 機器以外の機器に干渉する。 |
| | ・ | 転居や販売・譲渡の際、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、またはポリシーどおりに運用されていない。 (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。<br>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。 (U3_V.2) |
| | ・ | IoT 機器が、十分なセーフティ機能を実装していない。<br>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。 (U3_V.3) |
| | ・ | 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。 (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、機器を利用している。 (U3_V.5) |
| | ・ | 戸建住宅では、宅内ネットワーク、および宅内ネットワークに接続されている IoT 機器以外の機器が、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。 (U3_V.6) |
| | ・ | 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 IoT 機器以外の機器、住戸内のネットワーク、住戸内ネットワークに接続されている IoT 機器以外の機器が、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。 (U3_V.7) |
| | ・ | サービスを実行するサーバ等の機器の信頼性が低い、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サーバ等の機器の交換や廃棄時のデータ消去など、データの再利用が防止されていることを確認していない。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。

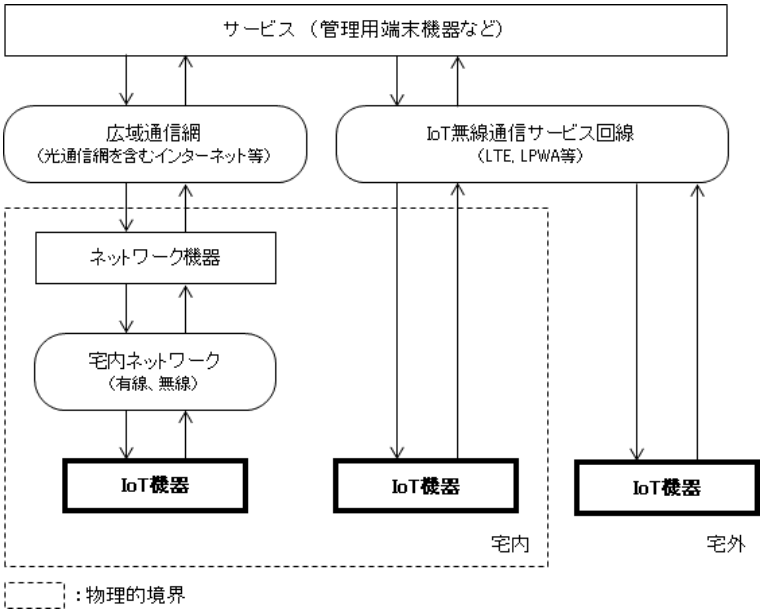


図 9.IoT 機器の外部管理（戸建住宅の場合）

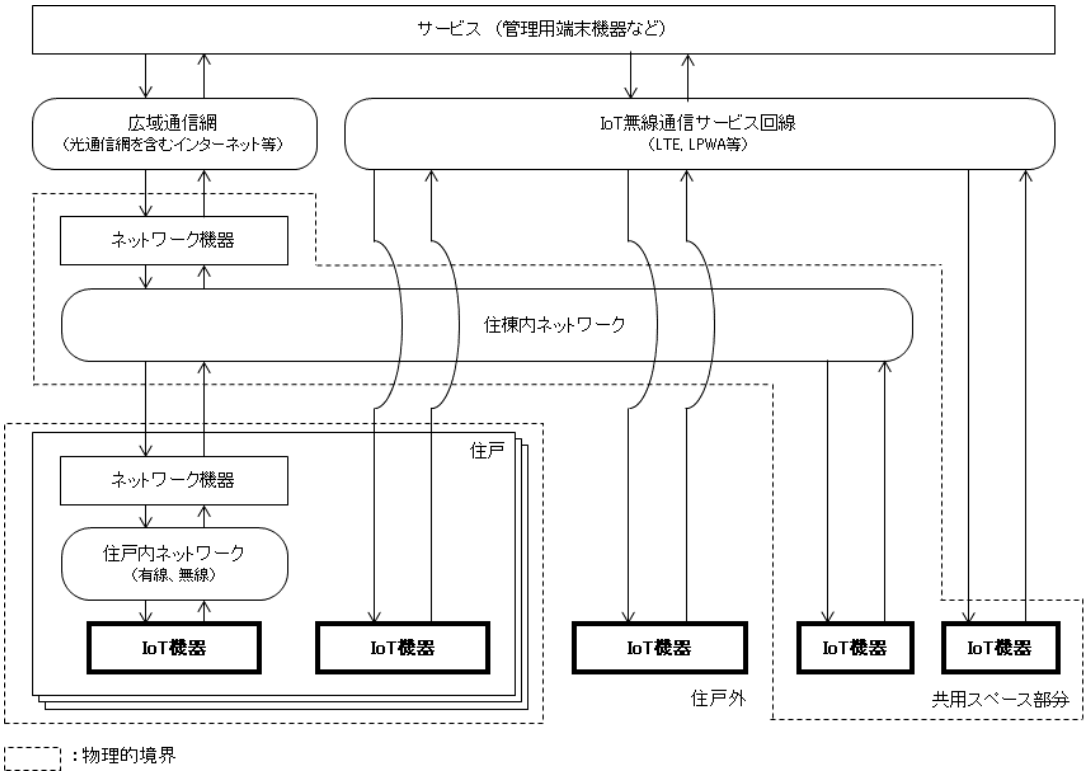


図 10.IoT 機器の外部管理（共同住宅の場合）

図9と図 10 を併せた想定シーンと脅威フロー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 | ・ なし |
| 基本フロー | 【IoT 無線通信サービス回線を利用しない場合】<br>以下の経路の4つの経路がありうる。<br>・ 戸建住宅の IoT 機器について、管理端末機器などからの IoT 機器の操作、設定のためのデータは、管理端末機器、広域通信網、宅内ネットワーク、IoT 機器の経路を経る。<br>・ 共同住宅の住戸内の IoT 機器について、管理端末機器などからの IoT 機器の操作、設定のためのデータは、管理端末機器、広域通信網、住棟内ネットワーク、住戸内のネットワーク、IoT 機器の経路を経る。<br>・ 共同住宅の共用スペースの IoT 機器について、管理端末機器などからの IoT 機器の操作、設定のためのデータは、管理端末機器、広域通信網、住棟内ネットワーク、IoT 機器の経路を経る。<br>・ 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を利用する場合】<br>・ 管理端末機器などからの IoT 機器の操作、設定のためのデータは、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。<br>・ 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。 |

図9と図10の想定シーンで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、意図しない動作をしたり人体に悪影響を及ぼしたりする。<br>・ IoT 機器が、宅内、住戸内や共用スペースの他の IoT 機器に干渉する。 |
| 脅威 | ・ IoT 機器が、乗っ取られる。<br>・ 管理端末装置と IoT 機器間の通信データが暴露される。<br>・ 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)<br>・ 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)<br>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。<br>・ 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)<br>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。<br>・ 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サーバや管理端末等の機器の交換や廃棄時の手続きがない、もしくは実施されない。 (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例は、「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 機器は出荷時や初期化状態から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、セキュアに利用するための情報を提供する

以下に、各項目を解説する。

### 4.1.1. IoT 機器は出荷時や初期化状態から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される可能性もある。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る。

サイバー攻撃によって引き起こされた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、セキュアに利用するための情報を提供する

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 機器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。

- 事業者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
- サービス提供や管理のポリシーを提示し遵守する

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。

以下に、各項目を解説する。

#### 4.2.1. 事業者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・保守を行うシステム、また運用・管理に利用しているサーバ等の機器が、サイバー攻撃の被害にあった場合、IoT 機器の管理・保守に影響するだけでなく、IoT 機器やサービスの利用に影響することとなり、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のシステム、または運用・管理に利用しているサーバ等の機器は、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。さらに、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、重要情報を再利用等できないよう適切に処理することが必要である。

#### 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むサービス提供のポリシー、および IoT 機器を開発・生産・販売する事業者が提供する設置方法・使用方法・機器内に保存される情報などの IoT 機器のガイドやポリシーを確認し、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 機器を開発・生産・販売する事業やスマートホーム向けのサービス事業者が示す用途・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. サービス提供や管理のポリシーを提示し遵守する

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、「サービス提供のポリシー」、サービスの利用環境・利用方法などを直接関係するステークホルダーに対して提示し遵守することが望ましい。

また、サービス提供時に取得する情報や外部に渡す(通信する)情報などの「管理のポリシー」も提示し、遵守することが望ましい。

直接関係するステークホルダーに対して、発生しうるインシデントや危害についても明確化し提示することが望ましい。

### 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を開発・提供する事業者および関連サービスの事業者は、以下の対策を行うことが望ましい。

- サービスを提供する事業者のシステムを適切に運用・管理する
- 管理のポリシーを提示し遵守する

以下に、各項目を解説する。

### 4.3.1. サービスを提供する事業者の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サーバ等の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やサーバ等の機器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。さらに、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サーバ等の機器の交換や廃棄時は、重要情報を再利用等できないよう適切に処理することが必要である。

### 4.3.2. 管理のポリシーを提示し遵守する

スマートホーム向けのサービスを提供する事業者は、サービス提供時に取得する情報や外部に渡す（通信する）情報などの「管理のポリシー」を提示し、遵守することが望ましい。

直接関係するステークホルダーに対して、発生しうるインシデントや危害についても明確化し提示することが望ましい。

スマートホーム向けのサービス事業者と直接関係するステークホルダーは、例えば、サービサーやプラットフォーマーなどとなる。セキュリティパッチ適用などのセキュリティ対策を実施する主体を契約等で明示することで、これらのステークホルダーとの責任の所在を明確にすることができる。

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

以下に、各項目を解説する。

### 4.4.1. 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、想定される用途・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耐タンパー機能の有無や、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つながる可能性がある。

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。

### 4.4.2. 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等がリフォームを実施する場合など、新たに設置する IoT 機器はその機器の種類（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。また IoT 機器を宅外[17]や住戸外といった、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。

## 4.5. 「（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」<br>「（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。

- **共用スペース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・運用を適切に行う**
- **機器やサービスの用途・用法を守る**

なお、分譲共同住宅・団地の管理組合および賃貸住宅の所有者が、IoT 機器やネットワーク回線等の管理を管理受託会社（場合によってはその下請け再委託先も含む）に委託する場合、セキュリティパッチ適用などのセキュリティ対策を実施する主体を契約等で明示することで、責任の所在を明確にすることができる。契約等に盛り込むセキュリティ対策の実施等については、業種・業態に応じて具体化する必要がある。

また、賃貸住宅の宅内や共同住宅の住戸内については、そこが未入居である場合には、住宅や住戸内を主体的に管理する必要がある。この場合に必要なセキュリティ対策は、4.6 項を参照されたい。

以下に、各項目を解説する。

---

17 本書では、戸建住宅における住宅内以外のことを指す。敷地外にある専用の物置、駐車場、菜園などをいう。

### 4.5.1. 共用スペース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・運用を適切に行う

共同住宅の共用スペースに設置される住棟内ネットワーク、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。特に、導入している機器等[18]に脆弱性が発見されていないかを定期的に調べることや、最新のセキュリティパッチの適用やファームウェアアップデートなどを行うことが望まれる。そのため、分譲共同住宅・団地の管理組合、賃貸住宅の所有者や、それぞれから管理を受託する会社が、メンテナンスやサポートを行う事業者やネットワーク接続業者等との契約において、保守の頻度・内容等を明確にすることが望まれる。

また、リフォームなどの際は、共用スペースに設置される住棟内ネットワークや 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の情報漏えいリスクもあるため、機器の種類や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 機器を交換することも考えられる。この場合においても機器の種類や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、共用スペースのセキュリティ事故発生時の対応フローや作業分担を、分譲住宅では管理組合が、賃貸住宅では所有者（オーナー）が、それぞれ契約先の管理受託会社、メンテナンスやサポートを行う事業者、ネットワーク接続業者等との契約で整合[19]しておくことが有効である。

また、建物の構造等の劣化に対応する大規模修繕を行う際に、ネットワークや IoT 機器の技術の進歩を勘案して、それらの交換や変更について検討することも望ましい。

### 4.5.2. 機器やサービスの用途・用法を守る

スマートホームを供給する事業者等が共用スペース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、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。

---

18 機器のソフトウェアやハードウェアに関する脆弱性はもちろん、機器を含む IoT システムを構成しているハードウェア（例えば共用部のルーター、管理室の PC、緊急地震速報の受信装置など）の確認も必要である。他には、機器を接続しているネットワークで利用しているプロトコルやクラウドサービス等にも脆弱性が発見されていないことを確認する。

19 共同住宅の共用部分の IoT 機器やネットワーク回線等の管理を管理受託会社等に委託する場合は、4.5.1 の内容の実施に関する事項だけでなく、セキュリティ事故発生時の対応フローや作業分担を、契約等に明記するべきである。例えば、分譲共同住宅の場合には管理組合と管理受託会社等との間で締結する契約等に明記すべきである。賃貸住宅の場合には住宅の所有者と管理受託会社等との間で締結する契約等に明記すべきである。

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、個人情報などの漏洩、物理的な被害、人体に対するダメージにつながるといった可能性がある。

また、用途・方法を守るには、ソフトウェアを常に最新の状態に維持することも含まれる。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、共用スペースの 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 機器やサービスの用途・用法を守って使う**
- **個人情報を自分で守る**

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、各事業者による個人情報を含む様々なデータ管理などのポリシーや、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、例えば以下のよう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 Web 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物や Web 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 IoT 機器の選定が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 機器やサービスの用途・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、個人情報の漏洩や、人体へのダメージにつながるなど、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、予め IoT 機器やサービスが設営されている場合においても、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、住まい手の意向に沿っ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. 個人情報を自分で守る

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・廃棄などの際は、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、データの再利用を防止することが望ましい。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ガイドを示した。

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 | 添付Dの事例の分類 | リスク源 | | | | 脆弱性の要素 | | 対策要件ID(*3) | 対策要件の例 | 関連するCPSFの対策要件ID(*4) |
|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | 脅威 | 脆弱性ID(*1) | 脆弱性 | 想定利用シーンにおける脆弱性ID(*2) | 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<br>・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<br>・サイ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<br>・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・エネルギーメーターなどに影響するものがある） | （１）、（２）、（３） | ・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やサービス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。<br>・IoT機器およびIoT機器を含むシステムが提供する機能、サービス、アプリケーション、アカウントについては出荷時点で明らかに不要な場合には、削除、無効化や停止を行うこと。また、出荷時点で不明な場合でも、必要に応じて停止、変更、削除や無効化が可能なようにすること。 | 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やパスワードが弱い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機器は個体毎に一意に識別できるようにすること。<br>・IoT機器およびIoT機器を含むシステムを安全に利用するために正当性の確認が必要な利用者やIoT機器の認証情報は、製品ライフサイクル全体でセキュリティ強度を高く維持できるような機能を実装すること。 | – |
| | | | | 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機器を含むシステムの構成要素管理の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機器を含む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。<br>・IoT機器およびIoT機器を含むシステムの企画・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機器およびIoT機器を含む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。<br>・IoT機器を含む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。<br>・IoT機器が提供する機能やデータへのローカル/リモートのアクセスについて、ユーザやロールに基づき閲覧や変更等の権限を管理し、認可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の改ざん検知や暗号化をする等、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機器およびIoT機器を含むシステムの動作仕様に基づき、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機器およびIoT機器を含むシステム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機器やネットワーク機器等の機能が停止する | （１）、（２） | ・IoT機器、ネットワーク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。<br>－ 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。<br>－ 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。<br>－ IoT機器を含む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・エネルギーメーターなどに影響する） | （２） | ・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機器およびIoT機器を含むシステム内に保存される情報や外部と通信する情報などを記載したガイドを提供すること。<br>・サポートする暗号化スイートや機器の状態等のセキュリティに関わる情報はIoT機器の管理者機能などを介して提供すること。 | – |
| | | | | 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 | （３） | ・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機器においてデータ消去（サニタイズ）するなど、データの再利用防止機能がない。 | U1_V.1, U2_V.1, U1_V.2, U2_V.2, U3_V.2, U4_V.2 | | ✓ | MO.12 | ・IoT機器およびIoT機器を含むシステムの廃棄時には、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）を消去（サニタイズ）するなど、データの再利用防止機能を実装すること。<br>・IoT機器およびIoT機器を含むシステムの廃棄時に、データを消去（サニタイズ）するなど、データの再利用を防止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 | 添付Dの事例の分類 | 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） | | | |
| 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 | （１） | ・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 | ・IoT機器に保存される鍵、認証情報や個人情報等の重要なデータを保護すること。<br>・耐タンパー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機器に保存される鍵、認証情報や個人情報等の重要なデータを保護すること。<br>・IoT機器およびIoT機器を含むシステム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、データ消去（サニタイズ）など、データの再利用を防止する手順がない | U1_V.1, U2_V.1, U1_V.2, U2_V.2, U3_V.2, U4_V.2, | | ✓ | MO.12 | ・IoT機器およびIoT機器を含むシステムの廃棄時には、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）を消去（サニタイズ）するなど、データの再利用防止機能を実装すること。<br>・IoT機器およびIoT機器を含むシステムの廃棄時に、データを消去（サニタイズ）するなど、データの再利用を防止する手順をガイドに示すこと。 | – |
| 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<br>（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、人体・健康・住宅・防犯・環境・利便性・エネルギーメーターなどに影響するものなどがある） | （２） | ・不正なエンティティによるインジェクション攻撃<br>・サイバー空間からの許容範囲外のインプットデータ<br>・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にも関わらず、機器が出荷される（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機器を含むシステムの構成要素管理の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機器を含む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。<br>・IoT機器およびIoT機器を含むシステムの企画・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IoT機器を含むシステムの企画・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 | 添付Dの事例の分類 | 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<br>・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<br>・サイバー空間から受け取ったデータに基づいて、IoT機器を制御したり、可視化したりする機能<br>・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・エネルギーメーターなどに影響する | （１）、（２）、（３） | ・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機器を遠隔から管理する事業者のシステムの脆弱性に対応すること。<br>・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提供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。<br>・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 | （３） | ・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消去（サニタイズ）など、データの再利用防止を行っていない | 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事業者のシステムを構成する機器（サーバー等）のデータを消去（サニタイズ）するなど、データの再利用を防止すること。 | – |
| | | | | | | | | | RMO.4 | ・スマートホーム向けのIoT機器を遠隔から管理する事業者のシステムは、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消去（サニタイズ）するなど、データの再利用を防止する機能を実装すること。<br>・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個人情報等を含むデータ管理などの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消去など、データの再利用が防止されていることを確認していない | 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事業者のシステムを構成する機器のリプレースや廃棄時に、データ消去（サニタイズ）するなど、データの再利用を防止すること。 | 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 | 添付Dの事例の分類 | 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<br>・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を含むデータを保管する機能<br>・センサデータを加工・分析する機能<br>・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・エネルギーメーターなどに影響する） | （１）、（２） | ・事業者の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 | ・事業者の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 | ・スマートホーム向けのサービス事業者のシステムが、十分なリソースで構成されていることを確認すること。<br>・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。 | – |
| | | | ・事業者の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 | ・事業者の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 | ・スマートホーム向けのサービス事業者の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。<br>・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 | （３） | ・事業者の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 | ・事業者の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 | ・スマートホーム向けのサービス事業者の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。<br>・スマートホーム向けのサービス事業者の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<br>・データを送受信する機能 | IoT機器を制御したり、可視化する機能などが、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・エネルギーメーターなどに影響する） | （２） | ・事業者の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、想定されていない動作が行われる | SV.3 | ・事業者の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 | ・スマートホーム向けのサービス事業者の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。<br>・スマートホーム向けのサービス事業者の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を含む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 | （３） | ・事業者の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 | ・事業者の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消去（サニタイズ）など、データの再利用が防止されていることを確認していない | U1_V.8, U2_V.9, U3_V.9 | ✓ | | SO.4 | ・スマートホーム向けのサービス事業者のシステムは、システム内部に保存されているユーザーデータを消去（サニタイズ）するなど、データの再利用を防止する機能を実装すること。<br>・スマートホーム向けのサービス事業者のシステムは、利用者がユーザーデータの削除を求めた場合に、データを消去（サニタイズ）するなど、データの再利用を防止する機能を提供すること。<br>・スマートホーム向けのサービス事業者の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、データ消去（サニタイズ）するなど、データの再利用を防止すること。 | 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）の管理の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 | ・住まい手に関する個人情報等を含むデータ管理など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 | 添付Dの事例の分類 | 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<br>・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<br>・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<br>・IoT機器を管理する | (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 | （３） | ・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<br>・センサーの測定値、閾値、設定の改ざん | HV.1 | ・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.1 | ・住宅（住戸）や共同住宅の共用スペースに設置するIoT機器の場合、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。<br>・耐タンパー性が必要な情報を取り扱う場合、IoT機器やIoT機器を含むシステムは、耐タンパーデバイスが組み込まれていることを確認すること。<br>・IoT機器やIoT機器を含むシステムのソフトウェアは完全性の検証が可能であることを確認すること。 | CPS.DS-8、CPS.DS-15 |
| | 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・エネルギーメーターなどに影響する | （１）、（２）、（３） | ・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.2 | ・住宅の新築時またはリフォーム・修繕時、住宅（住戸）や共同住宅の共用スペースに設置される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.2 | ・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。 | – |

## ■「(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 | 添付Dの事例の分類 | 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<br>・フィジカル空間の物理事象を読み取り、サイバー空間へ送る機能<br>・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<br>・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・エネルギーメーターなどに影響する | （１）、（２）、（３） | ・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にメンテナンスやサポート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提供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。<br>・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 | （３） | ・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、住居から転居する時、住宅に備え付けのIoT機器の個人情報などのデータ消去（サニタイズ）など、データの再利用の防止を行っていない | U3_V.1 | | ✓ | SMO.3 | ・住宅に備え付けのIoT機器のデータを消去（サニタイズ）するなど、データの再利用を防止すること。 | – |
| | | | | SMV.4 | ・スマートホーム向けサービスのメンテナンスやサポートを行う事業者の利用する機器のリプレースや廃棄時に、データ消去（サニタイズ）など、データの再利用が防止されていることを確認していない | 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メンテナンスやサポートを行う事業者のシステムのリプレースや廃棄時に、データ消去（サニタイズ）するなど、データの再利用を防止すること。 | 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、<br>「(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 | 添付Dの事例の分類 | 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<br>・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<br>・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<br>・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IoT機器で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るが、この動作により、人体・健康・住宅・防犯・環境・利便性・エネルギーメーターなどに影響する。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） | （１）、（２） | ・住戸内のネットワークに接続されたIoT機器が、住棟内ネットワークに接続されたIoT機器から攻撃される | CAV.1 | ・共用スペース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スペース設置のIoT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 | ・共用スペース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IoT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スペース設置の機器が、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 | ・住棟内ネットワークに接続されたIoT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、住棟内ネットワークに接続されたIoT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 | ・共同住宅の修繕時、新たに共用スペースまたは住戸部分に設置するIoT機器およびIoT機器を含むシステムの品質や信頼性が確認されていない。または、住棟内ネットワークに接続されたIoT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 | ・共同住宅の修繕時、共用スペースまたは住戸部分に導入されるIoT機器およびIoT機器を含むシステムは、目的とする特性に応じた品質や信頼性が確保されていることを確認すること。 | 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 | ・共同住宅の修繕時、共用スペースまたは住戸部分に設置されるIoT機器およびIoT機器を含むシステム内の個人情報などが漏洩する | （３） | ・共同住宅の修繕時、共用スペースまたは住戸部分に設置されるIoT機器およびIoT機器を含むシステムから住まい手の個人情報などが漏洩する | CAV.4 | ・共同住宅からの退去時、住戸に設置されたIoT機器およびIoT機器を含むシステム内のデータ消去（サニタイズ）など、データの再利用の防止を忘れる | U1_V.5, U2_V.6, U3_V.7 | ✓ | | CAO.4 | ・共同住宅からの退去時（利用者変更など）には、共用スペースおよび住戸に設置されたIoT機器やサービス内のデータを消去（サニタイズ）するなど、データの再利用を防止すること。 | CPS.IP-6 |
| | | | | CAV.5 | ・共同住宅の修繕時、共用スペースおよび住戸に設置された共用設備であるIoT機器およびIoT機器を含むシステム内のデータ消去（サニタイズ）など、データの再利用の防止を忘れる | U1_V.5, U2_V.6, U3_V.7 | ✓ | | CAO.5 | ・共同住宅の修繕時（IoT機器の変更やサービスのリプレースなど）には、共用スペースおよび住戸に設置されたIoT機器やサービス内のデータを消去（サニタイズ）するなど、データの再利用を防止すること。 | 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 | 添付Dの事例の分類 | 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<br>・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<br>・サイバー空間から受け取ったデータに基づいて、IoT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るが、この動作によりり、情報漏洩や不正な制御等、人体・健康・住宅・防犯・環境・利便性・エネルギーメーターなどに影響するものがある） | （１）、（２） | ・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機器を含むシステムを導入すること。<br>・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機器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提供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メンテナンスやサポートを行う事業者にメンテナンスやサポートを依頼すること。 | – |
| 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IoT機器を含むシステム内の個人情報などが漏洩する | （３） | ・転居、IoT機器の売却や廃棄の際に、IoT機器やIoT機器を含む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IoT機器を含むシステムの利用を終了する際に、IoT機器とIoT機器を含むシステム内のデータ消去（サニタイズ）など、データの再利用防止を忘れる | U2_V.10, U3_V.10 | ✓ | | CO.4 | ・利用を終了したIoT機器、利用を終了するとサービス内のデータを消去（サニタイズ）するなど、データの再利用を防止すること。 | CPS.IP-6 |

(*1)脆弱性ID：各脅威から導き出される脆弱性を識別するIDを示す　(*2)想定利用シーンにおける脆弱性ID：ガイドライン3章に明記した各想定シーンにおける脅威から導き出される脆弱性を識別するIDを示す　(*3)対策要件ID：各ステークホルダにおけるセキュリティ対策要件の例を識別するIDを示す
(*4)関連するCPSFの対策要件ID：対策要件IDと関連するCPSFのセキュリティ対策要件IDを示す

**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(*1) | 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。<br>・IoT機器およびIoT機器を含むシステムが提供する機能、サービス、アプリケーション、アカウントについては出荷時点で明らかに不要な場合には、削除、無効化や停止を行うこと。また、出荷時点で不明な場合でも、必要に応じて停止、変更、削除や無効化が可能なようにすること。 | ・IoT機器およびIoT機器を含むシステム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。<br>・IoT機器およびIoT機器を含むシステムの使用しない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。<br>・IoT機器が提供する機能などについて出荷時点で明らかに不要な場合には、削除、無効化や停止を行う。また、出荷時点に不明な場合でも、IoT機器などの主たる機能の動作、安全やセキュリティ等に悪影響を及ぼさない範囲で利用者の使用方法や環境に応じて停止、変更、削除や無効化が可能なようにする。例えば、以下が考えられる。<br>- 不要なサービスの停止<br>- 不要な機能の無効化<br>- 不要なアプリケーションの削除<br>- デフォルトの管理者権限アカウントの変更<br>- 不要なアカウントの削除 | [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<br>[つながる世界の開発指針] 指針5<br>[Considerations for a Core IoT Cybersecurity Capabilities Baseline] Baseline候補 11、Baseline候補 12<br>[Code of Practice] Guidelines 6)<br>[ETSI EN 303 645] 4.6<br>[Baseline Security Recommendations for IoT] GP-TM-27、GP-TM-28、GP-TM-33、GP-TM-45 |
| MO.2 | ・IoT機器は個体毎に一意に識別できるようにすること。<br>・IoT機器およびIoT機器を含むシステムを安全に利用するために正当性の確認が必要な利用者やIoT機器の認証情報は、製品ライフサイクル全体でセキュリティ強度を高く維持できるような機能を実装すること。 | ・IoT機器には個体毎に異なる一意な識別子を割り当てる。<br>- 識別子とはMACアドレス、IoT機器管理システムの独自ID、アプリケーションID、証明書等である。<br>- 識別子も改ざんされないようにすることが望ましい。<br>・IoT機器およびIoT機器を含むシステムを安全に利用するために正当性の確認が必要な利用者やIoT機器のパスワード等の認証情報は、初期段階も含めて製品のライフライクル全体をとおしてセキュリティ強度を高く維持できるようにする(特にIoT機器は、初期段階に弱いパスワードが設定される問題が多い。初期段階でパスワード強度を上げるメカニズムが必要である）。<br>- 初期時点のパスワード強度を上げるための対策の例<br>-+ IoT機器には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。<br>—> 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ような文字列を使用するなど、IoT機器やサービスに応じた、パスワードの強度を満足することが必要である。<br>-+ 初期パスワードが個体毎に同一である場合、初回の利用時等にパスワードを変更しない限り利用できないようにする。<br>- 十分なセキュリティ強度であるかを確認できた場合のみパスワードを設定できるようにする。<br>- パスワード等の認証情報を変更できる機能を設け、パスワード強度が十分な場合にのみ変更できるようにする。<br>1）パスワードの強度（パスワードの最小長、弱いパスワードパターンのチェックや利用可能な文字種・文字の組み合わせなどによるパスワードの複雑さの確保など）をチェックする。<br>2) パスワード等の認証情報をの定期的な変更を促す機能を提供する場合にはデフォルトで無効にする。<br>・IoT機器の場合には、パスワード等の認証情報を定期的に変更させることは困難な場合が多い。特に「スマートホーム」の場合には定期的な変更は困難だと思われる。企業等の組織向けには規則上必要な場合もあり、定期的にパスワード等の認証情報の変更を促す機能を設ける。 | [IoTセキュリティガイドライン] 要点4、要点7、要点15<br>[つながる世界の開発指針] 指針5<br>[Code of Practice] Guidelines 1)<br>[ETSI EN 303 645] 4.1<br>[Baseline Security Recommendations for IoT] GP-TM-09、GP-TM-22 |
| MO.3 | ・IoT機器およびIoT機器を含むシステムの構成要素管理の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機器を含む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。<br>・IoT機器およびIoT機器を含むシステムの企画・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。<br>- リスクアセスメントはIoT機器およびIoT機器を含むシステムが使われる環境を想定して行う。<br>+ 例えば、セキュリティ関連のIoT機器が住宅外などの他者がアクセスしやすい場所に設置されることが想定される場合には、IoT機器にリセットボタンを備えるべきでないかもしれない。<br>・IoT機器およびIoT機器を含むシステムでサービスやプロセスを起動する場合には実行するプログラムの機能を最小化したり、それを実行するアカウントは必要最小限の特権となるように設計する。<br>・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。<br>・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。<br>・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・周知する。<br>- 例えば、MO.7の対策例に記載がある脆弱性情報を受け付ける窓口での情報は、すみやかに組織内に展開し、修正プログラムの提供等を行う。 | [IoTセキュリティガイドライン] 要点1、要点17、要点18<br>[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<br>[NISTIR 8228] Goal 1<br>[Considerations for a Core IoT Cybersecurity Capabilities Baseline] Baseline候補 2<br>[Code of Practice] Guidelines 2)、Guidelines 3)<br>[ETSI EN 303 645] 4.2、4.3<br>[Baseline Security Recommendations for IoT] GP-PS-06、GP-OP-04 |

| 対策要件ID(*1) | 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.4 | ・IoT機器およびIoT機器を含む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。<br>・IoT機器を含む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。<br>・IoT機器が提供する機能やデータへのローカル/リモートのアクセスについて、ユーザやロールに基づき閲覧や変更等の権限を管理し、認可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、以下のような機能を実装し、アクセスを制限する。<br>　- 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。<br>　- 通信元や通信先を制限する。<br>・制限方法は提供するIoT機器が利用される環境のセキュリティレベルや運用方法を考慮して検討する。<br>　- MACアドレスやIPアドレス等によるフィルタリングで相手先を制限してもよいし、パスワードや認証鍵、証明書等などを用いる認証技術を行ってもよい。<br>　- IoT機器がサーバに接続や通信する場合には、サーバをフィルタリングや認証した後に、接続や通信してもよい。<br>・証明書等を使ってサーバ認証を行う場合には、接続先のサーバが想定したものかを確認してもよい。例えば、信頼するCAの制限や、Certificate pinning等によって、受け入れる証明書を制限する。<br>・スマートホームのIoT機器は長期間使われる。このため、証明書を使う場合には、証明書の失効/変更も考慮する必要があることに注意する。<br>　- システムの要件によってはエンドツーエンドで相互認証できる機能を提供してもよい。<br>　- DHCPでIPを動的に割り当てる場合には、DNSスプーフィング対策として、DNSサーバの手動設定するオプション等を提供すべきである。<br>　- ユーザや通信先を認証する。<br>・IoT機器が提供する機能や保存しているデータ(アプリケーションやファームウェア等のプログラムも含む)へのローカルやリモートからの要求について、ユーザやロールに設定された権限に基づき、要求されたアクションを認可する機能を実装する。<br>　- 例えば、IoT機器にアクセスできるユーザを追加/削除したり、セキュリティ設定を変更するなどの機能を提供する場合には管理者の権限があるユーザのみに限定されるべきである。<br>・ログイン失敗、アクセス制限や認可に違反した場合などのセキュリティに関わるイベントは監査/イベントログとして記録する。<br>　- 予め設定した管理者等の連絡先(メール等)にアラート通知するなどの機能は、攻撃の早期発見につながりやすい。ただし、通知の頻度が高いと運用等に支障をきたすため、機能のオン/オフや送信する条件等の設定は変更可能にするのが望ましい。<br>　- これらのログは改ざんされたり、漏洩を防ぐために管理者のみにアクセスを許可する等のアクセス制御等の対策を行う。 | [IoTセキュリティガイドライン]　要点7、要点16<br>[ETSI EN 303 645]　4.1<br>[Considerations for a Core IoT Cybersecurity Capabilities Baseline]　Baseline候補 4<br>[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。<br>　- ID/パスワードだけではなく、認証した後に発行されるセッションIDなども保護すべき対象である。<br>　- パスワード等の認証情報を送る通信は、キャプチャされた通信の情報をそのまま再送されるリプレイ攻撃から保護するための対策も実装する。<br>　- 暗号技術を使う場合には、業界に認められた機関が発行するガイドライン等を参考にする（例えば、 CRYPTREC「CRYPTREC暗号リスト(電子政府推奨暗号リスト) 」、など） 。 | [IoTセキュリティガイドライン]　要点14、要点16<br>[NISTIR 8200]　※1<br>[Considerations for a Core IoT Cybersecurity Capabilities Baseline]　Baseline候補 5<br>[Code of Practice] Guidelines 5)<br>[ETSI EN 303 645]　4.5<br>[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の改ざん検知や暗号化をする等、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。<br>　- 一般的に、機密性を保護したい場合には、暗号化による秘匿だけでは対策として不十分である。改ざん検知などにより完全性を保護する必要がある。また、アプリケーションによっては送信先の認証も必要となる。<br>　- これらのネットワーク間で転送されるデータを保護したい場合には、暗号化だけでなく改ざん検知、認証、リプレイ対策も行えるTLS等のセキュアプロトコルの利用が推奨される。TLS以外にもIPsecなどの利用可能な技術は多いため、独自での開発はあまりせず、既存の技術の利用を検討する。<br>　- ただし、これらのセキュアプロトコルも過去の設計や実装で脆弱性が見つかっている。極力新しいバージョンの利用を推奨するとともに、これらのセキュアプロトコルをファームウェアアップデート等で更新可能なように設計することが望ましい。<br>　- 暗号技術を使う場合には、業界に認められた機関が発行するガイドライン等を参考にする（例えば、 CRYPTREC「CRYPTREC暗号リスト(電子政府推奨暗号リスト) 」、 CRYPTREC、IPA「SSL-TLS暗号設定ガイドライン v3.0.1」(2020年12月現在)など） 。<br>・送信するデータに機密性がない場合でも、完全性を保証する必要がある場合もある。そのような場合には改ざん検知等の暗号技術を使う。<br>・通信の後に発生する処理に応じて、キャプチャされた通信の情報をそのまま再送されるリプレイ攻撃から保護するための対策も実装する。<br>　- 例えば、受け取った後に重要な情報を書き換えたり、IoT機器が物理的に動作する等の処理では認証や認可の処理はもとより、リプレイ攻撃の対策が必要である。 | [IoTセキュリティガイドライン]　要点14、要点16<br>[NISTIR 8200]　※1<br>[Considerations for a Core IoT Cybersecurity Capabilities Baseline]　Baseline候補 5<br>[Code of Practice] Guidelines 5)、Guidelines 13)<br>[ETSI EN 303 645]　4.5<br>[Baseline Security Recommendations for IoT] GP-TM-39 |
| MO.7 | ・IoT機器およびIoT機器を含むシステムの動作仕様に基づき、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参照先の情報を提示する。<br>・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。<br>　- 脆弱性情報の窓口で受け付けた情報は、組織内の適切な部署に展開し、MO.3で実施している取り組みで対策を講じる。<br>・可能であれば、製品の製造/サポートの終了後にIoT機器の脆弱性の対応、更新が利用可能かなどについての製造者としての製品提供に関するサービスのポリシーもガイドに記載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、要点18、要点21<br>[つながる世界の開発指針]　指針16、指針17<br>[NISTIR 8259] Activity 5<br>[Code of Practice]　Guidelines 2)<br>[ETSI EN 303 645]　4.2<br>[Baseline Security Recommendations for IoT] GP-OP-02、GP-OP-05、GP-OP-06、GP-OP-07、GP-OP-08 |
| MO.8 | ・IoT機器およびIoT機器を含むシステム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。<br>・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。<br>　- 例えば、MO.3の取り組みで作成された修正プログラム等の展開が該当する。<br>・住宅に付帯するIoT機器については長期間利用されることが想定されるため、証明書等を使う場合には、それをオンラインで更新する仕組みを備えてもよい。<br>・自動更新や更新通知をサポートする場合には、ユーザがセキュリティ更新や更新通知のインストールを有効/無効/延期できるように設定できるようにしてもよい。<br>・修正プログラムの適用でIoT機器の基本機能が中断される場合には、ユーザに通知するべきである。 | [IoTセキュリティガイドライン]　要点17、要点21<br>[つながる世界の開発指針]　指針14、指針15、指針16<br>[NISTIR 8259] Activity 6<br>[Considerations for a Core IoT Cybersecurity Capabilities Baseline]　Baseline候補 2<br>[Code of Practice] Guidelines 3)<br>[ETSI EN 303 645]　4.3<br>[Baseline Security Recommendations for IoT] GP-TM-18、GP-TM-19、GP-TM-20 |

| 対策要件ID(*1) | 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.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。<br>- 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。<br>- 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。<br>- IoT機器を含む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。また、電力が失われた場合にも正常に回復する必要がある。<br>・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。<br>・サービス拒否攻撃に対しては、以下のような対策が考えられるのであわせて実施を検討する。<br>- ネットワークを分離し、通信元や通信先を制限する。<br>- 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。<br>・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。<br>・IoT機器は、時間が時刻サーバと同期できない場合でも、安全性を損なわない程度で動作する。 | [IoTセキュリティガイドライン] 要点7<br>[つながる世界の開発指針] 指針12<br>[NISTIR 8259] Activity 6<br>[Considerations for a Core IoT Cybersecurity Capabilities Baseline] Baseline候補 3、Baseline候補 4<br>[Code of Practice] Guidelines 9)、Guidelines 12)<br>[ETSI EN 303 645] 4.9、4.12<br>[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機器およびIoT機器を含むシステム内に保存される情報や外部と通信する情報などを記載したガイドを提供すること。<br>・サポートする暗号化スイートや機器の状態等のセキュリティに関わる情報はIoT機器の管理者機能などを介して提供すること。 | ・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情報等の処理内容、使用方法、使用者、使用目的等を開示する。<br>・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。もしくは 安全な構成を自動的にセットアップする機能を提供することが望ましい。<br>・セキュリティに関わる情報はIoT機器の管理者機能などを介して提供する。<br>- 例えば、サポートする暗号スイート、ファームウェアバージョン、ファイアウォールのステータス、リモート設定の有効/無効、ログイン試行のログ、起動中サービス、接続中のデバイスや利用インタフェースの情報（デバイスのIP、MACアドレスを含む）、システムステータスやログ等である。 | [IoTセキュリティガイドライン] 要点15、要点18<br>[つながる世界の開発指針] 指針15、指針16<br>[NISTIR 8259] Activity 6<br>[NISTIR 8267] ※2<br>[Considerations for a Core IoT Cybersecurity Capabilities Baseline] Baseline候補 9<br>[Code of Practice] Guidelines 8)、Guidelines 10)<br>[ETSI EN 303 645] 4.8、4.10<br>[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。<br>・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ような機能を提供する。<br>・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。もしくは、安全な構成を自動的にセットアップする機能を提供することが望ましい。<br>・導入の初期状態では、設定がセキュリティ側や安全側になるようなデフォルト設定とする。<br>- 例えば、通常は利用しない機能やサービス、運用や利用に注意が必要な機能やサービスはデフォルトで無効の状態とすることが望ましい（UPnPを無効にして出荷等）。<br>- 逆に、セキュリティ上や安全上で好ましい設定はデフォルトで有効にすることが望ましい（セキュリティに関する更新があることを通知するなど）。 | [IoTセキュリティガイドライン] 要点8<br>[つながる世界の開発指針] 指針8<br>[Code of Practice] Guidelines 12)、Guidelines 13)<br>[ETSI EN 303 645] 4.12、4.13<br>[Baseline Security Recommendations for IoT] GP-TM-54 |
| MO.12 | ・IoT機器およびIoT機器を含むシステムの廃棄時には、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）を消去（サニタイズ）するなど、データの再利用防止機能を実装すること。<br>・IoT機器およびIoT機器を含むシステムの廃棄時に、データを消去（サニタイズ）するなど、データの再利用を防止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情報等を消去（サニタイズ）するなど、データの再利用を防止する機能を提供する。<br>- 工場出荷や復元ポイントに再構成したりデバイスに収集されたデータを削除する機能の一部として動作する。<br>- これらの機能をリモートやローカルから攻撃者に悪用されて、容易にデータ消去がされないように、認可されたユーザのみが実行できるような設定や工夫を行う。<br>・パスワード等の認証情報を忘れたり、紛失することもあるため、ローカルでのハードウェアスイッチ等による工場出荷時の設定に戻す機能を備えることが望ましい。ただし、家の外に設置するようなIoT機器の場合には、工場出荷時の設定に戻すハードウェアスイッチが容易にアクセスできないようにする等の検討が必要である。 | [つながる世界の開発指針] 指針7<br>[NISTIR 8259] Activity 6<br>[Considerations for a Core IoT Cybersecurity Capabilities Baseline] Baseline候補 8<br>[Code of Practice] Guidelines 11)<br>[ETSI EN 303 645] 4.11 |
| MO.13 | ・IoT機器に保存される鍵、認証情報や個人情報等の重要なデータを保護すること。<br>・耐タンパー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。 | ・デバイスに格納されるソフトウェアに認証情報や鍵等を含めてハードコードしない。<br>・重要なデータは機密性や完全性を保護するために、暗号化/改ざん検知やアクセス制御等によってローカル/リモートからの攻撃者から保護する。<br>- 単純な難読化や独自開発した暗号手法は容易に破られる可能性が高い。<br>- 暗号技術は、業界に認められた機関が発行するガイドライン等を参考にする（例えば、「CRYPTREC暗号リスト(電子政府推奨暗号リスト)」など）。<br>・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情報等を保持する場合は、耐タンパー対策が施されたストレージに保存する。<br>・必要に応じて、IoT機器には、MMU(Memory Management Unit), TEE(Trusted Execution Environment)などのハードウェアレベルのセキュリティメカニズムを採用してもよい。 | [IoTセキュリティガイドライン] 要点8<br>[つながる世界の開発指針] 指針8<br>[Code of Practice] Guidelines 4)<br>[ETSI EN 303 645] 4.4<br>[Baseline Security Recommendations for IoT] GP-TM-01、GP-TM-02 |
| MO.14 | ・IoT機器に保存される鍵、認証情報や個人情報等の重要なデータを保護すること。<br>・IoT機器およびIoT機器を含むシステム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。<br>・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<br>[つながる世界の開発指針] 指針12<br>[Code of Practice] Guidelines 7)<br>[ETSI EN 303 645] 4.4、4.7<br>[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。<br>・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。 | [IoTセキュリティガイドライン] 要点16<br>[つながる世界の開発指針] 指針8<br>[NISTIR 8267] ※3<br>[Code of Practice] Guidelines 13)<br>[ETSI EN 303 645] 4.5、4.13<br>[Baseline Security Recommendations for IoT] GP-TM-42 |
| MO.16 | ・IoT機器およびIoT機器を含むシステムの企画・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。 | [IoTセキュリティガイドライン] 要点8<br>[つながる世界の開発指針] 指針10、指針12<br>[Baseline Security Recommendations for IoT] GP-TM-56、GP-TM-57 |

| 対策要件ID(*1) | 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.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の脆弱性に対応すること。<br>・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。<br>・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。<br>・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。<br>・ユーザや通信先を認証する機能を利用する。<br>・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。 | [IoTセキュリティガイドライン] 要点7、要点8、要点13<br>[つながる世界の開発指針] 指針13、指針14<br>[NISTIR 8228] Goal 1<br>[Considerations for a Core IoT Cybersecurity Capabilities Baseline] Baseline候補 7<br>[Baseline Security Recommendations for IoT] GP-TM-18、GP-TM-19、GP-TM-56、GP-TM-57 |
| 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。<br>・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。<br>・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）。<br>・IoT機器のガイドを確認し、IoT機器内に保存される情報の内容（個人情報が含まれるか否かなど）、その情報の廃棄方法などの必要な手順を定めたうえで運用する。 | [IoTセキュリティガイドライン] 要点18、要点19 ※5<br>[つながる世界の開発指針] 指針16、指針17 ※5<br>[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事業者のシステムを構成する機器（サーバー等）のデータを消去（サニタイズ）するなど、データの再利用を防止すること。 | ・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情報等を消去（サニタイズ）するなど、データの再利用を防止する。 | [IoTセキュリティガイドライン] 要点18、要点19<br>[つながる世界の開発指針] 指針7<br>[Considerations for a Core IoT Cybersecurity Capabilities Baseline] Baseline候補 8<br>[Code of Practice] Guidelines 11)<br>[ETSI EN 303 645] 4.11<br>[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事業者のシステムは、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消去（サニタイズ）するなど、データの再利用を防止する機能を実装すること。<br>・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個人情報等を含むデータ管理などの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情報等を消去（サニタイズ）するなど、データの再利用を防止する機能を提供する。<br>・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等のデータは住まい手などの利用者の要求に応じて消去（サニタイズ）するなど、データの再利用を防止する機能を提供する。<br>・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。 | [IoTセキュリティガイドライン] 要点18、要点19<br>[つながる世界の開発指針] 指針7<br>[Considerations for a Core IoT Cybersecurity Capabilities Baseline] Baseline候補 8<br>[Code of Practice] Guidelines 11)<br>[ETSI EN 303 645] 4.11<br>[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事業者のシステムを構成する機器のリプレースや廃棄時に、データ消去（サニタイズ）するなど、データの再利用を防止すること。 | ・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等を含む全データの消去（サニタイズ）など、データの再利用を防止する。 | [IoTセキュリティガイドライン] 要点18、要点19<br>[つながる世界の開発指針] 指針7<br>[Considerations for a Core IoT Cybersecurity Capabilities Baseline] Baseline候補 8<br>[Code of Practice] Guidelines 11)<br>[ETSI EN 303 645] 4.11<br>[Baseline Security Recommendations for IoT] GP-TM-14 |
| SO.1 | ・スマートホーム向けのサービス事業者のシステムが、十分なリソースで構成されていることを確認すること。<br>・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。<br>・ファイアウォール装置やWAF機能等によりネットワーク分離や通信元・通信先を制限する。 | [IoTセキュリティガイドライン] 要点７、要点8<br>[つながる世界の開発指針] 指針13<br>[ETSI EN 303 645] 4.5、4.9<br>[Baseline Security Recommendations for IoT] GP-TM-46、GP-TM-51 |
| SO.2 | ・スマートホーム向けのサービス事業者の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。<br>・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。<br>・ネットワークを分離し、通信元や通信先を制限する。<br>・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。 | [IoTセキュリティガイドライン] 要点７、要点13<br>[つながる世界の開発指針] 指針13<br>[Considerations for a Core IoT Cybersecurity Capabilities Baseline] Baseline候補 7 |
| SO.3 | ・スマートホーム向けのサービス事業者の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。<br>・スマートホーム向けのサービス事業者の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。<br>・ネットワークを分離し、通信元や通信先を制限する。 | [つながる世界の開発指針] 指針14 |
| SO.4 | ・スマートホーム向けのサービス事業者のシステムは、システム内部に保存されているユーザーデータを消去（サニタイズ）するなど、データの再利用を防止する機能を実装すること。<br>・スマートホーム向けのサービス事業者のシステムは、利用者がユーザーデータの削除を求めた場合に、データを消去（サニタイズ）するなど、データの再利用を防止する機能を提供すること。<br>・スマートホーム向けのサービス事業者の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等のデータは住まい手などの利用者の要求に応じて消去（サニタイズ）するなど、データの再利用を防止する機能を提供する。<br>・個人情報等の重要なデータは暗号化して保存する。 | [つながる世界の開発指針] 指針14<br>[Code of Practice] Guidelines 4)、Guidelines 11)<br>[ETSI EN 303 645] 4.4、4.11 |
| SO.5 | ・リプレースや廃棄時に、データ消去（サニタイズ）するなど、データの再利用を防止すること。 | ・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等を含む全データを消去（サニタイズ）するなど、データの再利用を防止する。 | [IoTセキュリティガイドライン] 要点18、要点19<br>[つながる世界の開発指針] 指針7<br>[Considerations for a Core IoT Cybersecurity Capabilities Baseline] Baseline候補 8<br>[Code of Practice] Guidelines 11)<br>[ETSI EN 303 645] 4.11<br>[Baseline Security Recommendations for IoT] GP-TM-14 |
| SO.6 | ・住まい手に関する個人情報等を含むデータ管理など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情報等のデータの処理内容、使用方法、使用者、使用目的等に関する規定を制定し、規定に従い運用する。 | [IoTセキュリティガイドライン] 要点18、要点19<br>[つながる世界の開発指針] 指針7<br>[NISTIR 8259] Activity 6<br>[Code of Practice] Guidelines 8)<br>[ETSI EN 303 645] 4.8<br>[Baseline Security Recommendations for IoT] GP-TM-14 |

| 対策要件ID(*1) | 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.1 | ・住宅（住戸）や共同住宅の共用スペースに設置するIoT機器の場合、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。<br>・耐タンパー性が必要な情報を取り扱う場合、IoT機器やIoT機器を含むシステムは、耐タンパーデバイスが組み込まれていることを確認すること。<br>・IoT機器やIoT機器を含むシステムのソフトウェアは完全性の検証が可能であることを確認すること。 | ・住宅（住戸）や共同住宅の共用スペースに設置する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。<br>・IoT機器の動作仕様に基づき、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・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を作成する。<br>・住宅（住戸）や共同住宅の共用スペースに設置するIoT機器内部で機密度の高い重要なデータを保持する場合は、耐タンパー対策が施されたストレージを選定する。<br>・IoT機器やIoT機器を含むシステムは、ソフトウェアの完全性が検証可能な機種を選定する。 | [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<br>[つながる世界の開発指針] 指針1<br>[NISTIR 8228] Goal 1<br>[Code of Practice] Guidelines 4)、Guidelines 8)、Guidelines 12)<br>[ETSI EN 303 645] 4.4、4.8、4.12<br>[Baseline Security Recommendations for IoT] GP-TM-13 |
| HO.2 | ・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）や共同住宅の共用スペースに設置する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。<br>・住宅（住戸）や共同住宅の共用スペースに設置した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。 | [IoTセキュリティガイドライン] 要点6<br>[つながる世界の開発指針] 指針1 |
| SMO.1 | ・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、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のシステムの特性に応じた脆弱性検査を行う。<br>・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。 | [IoTセキュリティガイドライン] 要点8<br>[つながる世界の開発指針] 指針8<br>[Code of Practice] Guidelines 4)<br>[ETSI EN 303 645] 4.4、4.12<br>[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。<br>・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。<br>・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。<br>・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。<br>・構成要素の管理におけるセキュリティルールや管理のポリシーを定め、定期的にリスクアセスメントを実施する。 | [IoTセキュリティガイドライン] 要点1、要点18、要点19 ※5<br>[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機器のデータを消去（サニタイズ）するなど、データの再利用を防止すること。 | ・住宅に備え付けのIoT機器やIoT機器を含むシステムの内部に保持するデータ（転居する住まい手の個人情報など）を消去（サニタイズ）するなど、データの再利用を防止する。 | [IoTセキュリティガイドライン] 要点8<br>[つながる世界の開発指針] 指針12、指針14、指針16<br>[Considerations for a Core IoT Cybersecurity Capabilities Baseline] Baseline候補 8<br>[Code of Practice] Guidelines 11)<br>[ETSI EN 303 645] 4.11<br>[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メンテナンスやサポートを行う事業者のシステムのリプレースや廃棄時に、データ消去（サニタイズ）するなど、データの再利用を防止すること。 | ・機器内部で保持する個人情報等含む全データを消去（サニタイズ）するなど、データの再利用を防止する。 | [IoTセキュリティガイドライン] 要点18、要点19<br>[つながる世界の開発指針] 指針7<br>[Considerations for a Core IoT Cybersecurity Capabilities Baseline] Baseline候補 8<br>[Code of Practice] Guidelines 11)<br>[ETSI EN 303 645] 4.11<br>[Baseline Security Recommendations for IoT] GP-TM-14 |
| CAO.1 | ・共用スペース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IoT機器を管理すること。 | ・共用スペース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。<br>・機器管理におけるセキュリティルールや管理のポリシーを定め、定期的にリスクアセスメントを実施する。<br>・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。<br>・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。<br>・機器へのアクセスをログに記録して管理する。<br>・機器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。 | [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<br>[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<br>[NISTIR 8228] Goal 1<br>[Security for IoT Sensor Networks] ※4<br>[Considerations for a Core IoT Cybersecurity Capabilities Baseline] Baseline候補 7<br>[Code of Practice] Guidelines 3)<br>[ETSI EN 303 645] 4.3 |
| CAO.2 | ・住棟内ネットワークに接続されたIoT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、住棟内ネットワークに接続されたIoT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。<br>・機器管理におけるセキュリティルールや管理のポリシーを定め、定期的にリスクアセスメントを実施する。 | [IoTセキュリティガイドライン] 要点1、要点14<br>[つながる世界の開発指針] 指針13、指針14、指針15<br>[NISTIR 8228] Goal 1<br>[Security for IoT Sensor Networks] ※4<br>[Code of Practice] Guidelines 5)<br>[ETSI EN 303 645] 4.5 |
| CAO.3 | ・共同住宅の修繕時、共用スペースまたは住戸部分に導入されるIoT機器およびIoT機器を含むシステムは、目的とする特性に応じた品質や信頼性が確保されていることを確認すること。 | ・住宅（住戸）や共同住宅の共用スペースに設置する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。 | [IoTセキュリティガイドライン] 要点15<br>[つながる世界の開発指針] 指針1<br>[Security for IoT Sensor Networks] ※4 |
| CAO.4 | ・共同住宅からの退去時（利用者変更など）には、共用スペースおよび住戸に設置されたIoT機器やサービス内のデータを消去（サニタイズ）するなど、データの再利用を防止すること。 | ・共用スペースおよび住戸に設置されたIoT機器から、機器やサービス内部で保持する個人情報等のデータを消去（サニタイズ）するなど、データの再利用を防止する。 | [IoTセキュリティガイドライン] 要点18、要点19 ※5<br>[つながる世界の開発指針] 指針7<br>[Security for IoT Sensor Networks] ※4<br>[Considerations for a Core IoT Cybersecurity Capabilities Baseline] Baseline候補 8<br>[Code of Practice] Guidelines 11)<br>[ETSI EN 303 645] 4.11<br>[Baseline Security Recommendations for IoT] GP-TM-14 |

| 対策要件ID(*1) | 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 | ・共同住宅の修繕時（IoT機器の変更やサービスのリプレースなど）には、共用スペースおよび住戸に設置されたIoT機器やサービス内のデータを消去（サニタイズ）するなど、データの再利用を防止すること。 | ・共用スペースおよび住戸に設置されたIoT機器から、機器やサービス内部で保持する個人情報等のデータを消去（サニタイズ）するなど、データの再利用を防止する。 | [IoTセキュリティガイドライン] 要点18、要点19 ※5<br>[つながる世界の開発指針] 指針7<br>[Security for IoT Sensor Networks] ※4<br>[Considerations for a Core IoT Cybersecurity Capabilities Baseline] Baseline候補 8<br>[Code of Practice] Guidelines 11)<br>[ETSI EN 303 645] 4.11<br>[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機器を含むシステムを導入すること。<br>・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機器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。<br>・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。<br>・ネットワークを分離し、通信元や通信先を制限する。 | [IoTセキュリティガイドライン] 要点18、要点19、ルール1 ※5<br>[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提供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提供のポリシーを確認し、適切な利用や管理を行う。<br>・IoT機器やIoT機器を含む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。 | [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<br>[つながる世界の開発指針] 指針16、指針17 ※5<br>[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メンテナンスやサポートを行う事業者にメンテナンスやサポートを依頼すること。 | ・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もしくはスマートホーム向けサービスのメンテナンスやサポートを行う事業者にメンテナンスやサポートを依頼する。 | [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 |
| CO.4 | ・利用を終了したIoT機器、利用を終了するとサービス内のデータを消去（サニタイズ）するなど、データの再利用を防止すること。 | ・転居やIoT機器の買い替え、売却、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消去（サニタイズ）するなど、データの再利用を防止する。<br>・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。 | [IoTセキュリティガイドライン] 要点18、要点19、ルール4 ※5<br>[つながる世界の開発指針] 指針7<br>[Considerations for a Core IoT Cybersecurity Capabilities Baseline] Baseline候補 8<br>[Code of Practice] Guidelines 11)<br>[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（コンパニオンアプリケーション）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リ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。

(*1)対策要件ID：各ステークホルダにおけるセキュリティ対策要件の例を識別するIDを示す

**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(*1) | 対策要件の例 |
|---|---|---|
| IoT機器は出荷時や初期化状態から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。<br>・IoT機器およびIoT機器を含むシステムが提供する機能、サービス、アプリケーション、アカウントについては出荷時点で明らかに不要な場合には、削除、無効化や停止を行うこと。また、出荷時点で不明な場合でも、必要に応じて停止、変更、削除や無効化が可能なようにすること。 |
| | MO.2 | ・IoT機器は個体毎に一意に識別できるようにすること。<br>・IoT機器およびIoT機器を含むシステムを安全に利用するために正当性の確認が必要な利用者やIoT機器の認証情報は、製品ライフサイクル全体でセキュリティ強度を高く維持できるような機能を実装すること。 |
| | MO.3 | ・IoT機器およびIoT機器を含むシステムの構成要素管理の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機器を含む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。<br>・IoT機器およびIoT機器を含むシステムの企画・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機器およびIoT機器を含む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。<br>・IoT機器を含む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。<br>・IoT機器が提供する機能やデータへのローカル/リモートのアクセスについて、ユーザやロールに基づき閲覧や変更等の権限を管理し、認可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の改ざん検知や暗号化をする等、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機器およびIoT機器を含むシステムの廃棄時には、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）を消去（サニタイズ）するなど、データの再利用防止機能を実装すること。<br>・IoT機器およびIoT機器を含むシステムの廃棄時に、データを消去（サニタイズ）するなど、データの再利用を防止する手順をガイドに示すこと。 |
| | MO.13 | ・IoT機器に保存される鍵、認証情報や個人情報等の重要なデータを保護すること。<br>・耐タンパー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機器に保存される鍵、認証情報や個人情報等の重要なデータを保護すること。<br>・IoT機器およびIoT機器を含むシステム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。<br>- 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。<br>- 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。<br>- IoT機器を含む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IoT機器を含むシステムの企画・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機器およびIoT機器を含むシステム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IoT機器の使い方や使用環境をガイドする、セキュアに利用するための情報を提供する | MO.7 | ・IoT機器およびIoT機器を含むシステムの動作仕様に基づき、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機器およびIoT機器を含むシステム内に保存される情報や外部と通信する情報などを記載したガイドを提供すること。<br>・サポートする暗号化スイートや機器の状態等のセキュリティに関わる情報はIoT機器の管理者機能などを介して提供すること。 |

## ■「(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機器を遠隔から管理する事業者のシステムの脆弱性に対応すること。<br>・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事業者のシステムは、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消去（サニタイズ）するなど、データの再利用を防止する機能を実装すること。<br>・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個人情報等を含むデータ管理などの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。<br>・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。 |
| サービス提供や管理のポリシーを提示し遵守する | 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事業者のシステムを構成する機器（サーバ等）のデータを消去（サニタイズ）するなど、データの再利用を防止すること。 |
| | RMO.4 | ・スマートホーム向けのIoT機器を遠隔から管理する事業者のシステムは、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消去（サニタイズ）するなど、データの再利用を防止する機能を実装すること。<br>・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個人情報等を含むデータ管理などの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事業者のシステムを構成する機器のリプレースや廃棄時に、データ消去（サニタイズ）するなど、データの再利用を防止すること。 |

## ■「(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事業者のシステムを適切に運用・管理する | SO.1 | ・スマートホーム向けのサービス事業者のシステムが、十分なリソースで構成されていることを確認すること。<br>・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 | ・スマートホーム向けのサービス事業者の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。<br>・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 | ・スマートホーム向けのサービス事業者の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。<br>・スマートホーム向けのサービス事業者の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 | ・スマートホーム向けのサービス事業者のシステムは、システム内部に保存されているユーザーデータを消去（サニタイズ）するなど、データの再利用を防止する機能を実装すること。<br>・スマートホーム向けのサービス事業者のシステムは、利用者がユーザーデータの削除を求めた場合に、データを消去（サニタイズ）するなど、データの再利用を防止する機能を提供すること。<br>・スマートホーム向けのサービス事業者の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、データ消去（サニタイズ）するなど、データの再利用を防止すること。 |
| 管理のポリシーを提示し遵守する | SO.6 | ・住まい手に関する個人情報等を含むデータ管理など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機器を正しく選定する | HO.1 | ・住宅（住戸）や共同住宅の共用スペースに設置するIoT機器の場合、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。<br>・耐タンパー性が必要な情報を取り扱う場合、IoT機器やIoT機器を含むシステムは、耐タンパーデバイスが組み込まれていることを確認すること。<br>・IoT機器やIoT機器を含むシステムのソフトウェアは完全性の検証が可能であることを確認すること。 |
| IoT機器やサービスを正しく設置、設定する | HO.2 | ・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。 |

## ■「(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にメンテナンスやサポートを行う事業者のシステムの脆弱性に対応すること。 |
| サービスとIoT機器のガイドに従った保守・管理を行う | 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。<br>・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。 |
| サービス提供や管理のポリシーを提示し遵守する | SMO.3 | ・住宅に備え付けのIoT機器のデータを消去（サニタイズ）するなど、データの再利用を防止すること。 |
| | SMO.4 | ・スマートホーム向けサービスのメンテナンスやサポートを行う事業者のシステムのリプレースや廃棄時に、データ消去（サニタイズ）するなど、データの再利用を防止すること。 |

## ■「(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 |
|---|---|---|
| 共用スペース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・運用を適切に行う | CAO.1 | ・共用スペース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IoT機器を管理すること。 |
| | CAO.2 | ・住棟内ネットワークに接続されたIoT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、住棟内ネットワークに接続されたIoT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 | ・共同住宅からの退去時（利用者変更など）には、共用スペースおよび住戸に設置されたIoT機器やサービス内のデータを消去（サニタイズ）するなど、データの再利用を防止すること。 |
| | CAO.5 | ・共同住宅の修繕時（IoT機器の変更やサービスのリプレースなど）には、共用スペースおよび住戸に設置されたIoT機器やサービス内のデータを消去（サニタイズ）するなど、データの再利用を防止すること。 |
| 機器やサービスの用途・用法を守る | CAO.3 | ・共同住宅の修繕時、共用スペースまたは住戸部分に導入されるIoT機器およびIoT機器を含むシステムは、目的とする特性に応じた品質や信頼性が確保されていることを確認すること。 |

## ■「(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機器を含むシステムを導入すること。<br>・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機器を含むシステムを導入すること。 |
| IoT機器やサービスの用途・用法を守って使う | CO.2 | ・IoT機器のガイドやサービス提供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メンテナンスやサポートを行う事業者にメンテナンスやサポートを依頼すること。 |
| 個人情報を自分で守る | CO.4 | ・利用を終了したIoT機器、利用を終了するサービス内のデータを消去（サニタイズ）するなど、データの再利用を防止すること。 |

(*1)対策要件ID：各ステークホルダにおけるセキュリティ対策要件の例を識別するIDを示す

## 添付D サイバー攻撃と脆弱性等の事例

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、攻撃により影響が及ぶ対象が何かとの観点より「(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つの分類に関連付けて整理した。

また、添付 A の想定されるインシデントに添付 D のこの3分類との対応関係も明記した。

(1) 「通信基盤やサービス基盤」の事例

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つながる事例

1) 無線 LAN 機器等の脆弱性や設定不備

2) Bluetooth 機器の脆弱性

3) HEMS コントローラーの脆弱性や誤使用

7) Web サービスに収集された IoT 機器情報の漏洩

(2) 「IoT 機器」の事例

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・財産の侵害などにつながる事例

3) HEMS コントローラーの脆弱性や誤使用

4) 照明システムへの侵入

5) ロボット掃除機の脆弱性

6) 自動車の脆弱性

(3) 「プライバシーに関わる情報」の事例

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、プライバシーの侵害などにつながる事例

1) 無線 LAN 機器等の脆弱性や設定不備

5) ロボット掃除機の脆弱性

7) Web サービスに収集された IoT 機器情報の漏洩

8) スマートスピーカーの不正操作

以下に各事例を示す。なお、本書では紙面の都合から記載事項は概要程度に留めた。詳細は、出典先の資料等を参考されたい。

### 1) 無線 LAN 機器等の脆弱性や設定不備

ホームゲートウェイとして一般的に利用されている無線 LAN 機器(Wi-Fi ルーター)において、Wi-Fi で利用される WPA2 の暗号化プロトコルに複数の脆弱性が発見された。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。

また、Wi-Fi ルーターが悪意のある攻撃により管理画面をのっとられ管理用パスワードや DNS 情報などの設定情報が書き換えられる事例も確認されている。ルーターなどを設置した際には、初期パスワードからの変更、ファームウェアの最新化が必要と改めて警鐘が鳴らされた事例でもあった。

家庭内や共同住宅の共用スペースに設置される Wi-Fi ルーターやネットワークカメラなどを起点とした大規模な DDoS 攻撃も確認された。これは「Mirai(ミライ)」というマルウェアに感染したネットワークカメラなどの IoT 機器で構築されたボットネットによる攻撃であったと見られている。IoT 機器の利用時に必要となるユーザ名とパスワード(ログイン情報)として、“root”や“password”といった汎用的な単語を初期設定としている製品がある。初期設定のままで利用することが非常に危険であることが本件でも知らしめた事例であった。

ネットワークカメラの脆弱性から、海外のウェブサイト上にリアルタイムのカメラ映像が公開されていることが判明し、プライバシー情報の漏洩として大きなインパクトを与えた事例もあった。

出典:WPA2 における複数の脆弱性について(IPA)

https://www.ipa.go.jp/security/ciadr/vul/20171017_WPA2.html,(参照 2021-02-05)

出典:Wi-Fi ルータの DNS 情報の書換え後に発生する事象について(NICT)

https://blog.nicter.jp/2018/03/router-dns-hack/,(参照 2021-02-05)

出典:ネットワークカメラや家庭用ルータ等の IoT 機器は利用前に必ずパスワードの変更を(IPA)

https://www.ipa.go.jp/security/anshin/mgdayori20161125.html,(参照 2021-02-05)

### 2) Bluetooth 機器の脆弱性

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 搭載機器を乗っ取られる可能性があり、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。

出典:Bluetooth の実装における複数の脆弱性について(IPA)

https://www.ipa.go.jp/security/ciadr/vul/20170914_blueborne.html,(参照 2021-02-05)

### 3) HEMS コントローラーの脆弱性や誤使用

HEMS コントローラーに、任意のコマンド実行、管理者パスワードの変更の脆弱性が発見され、脆弱性を修正したファームウェアの配布が実施された事例があった。さらに、同製品に対して、機器内に保存した情報やファイルへの不正アクセス、接続した機器の不正操作等を可能とする脆弱性が発見され、脆弱性を修正したファームウェアの配布が実施された。当該製品には、ファームウェアの自動更新機能が搭載されていたが、自動更新機能をオフにしている利用者も想定し、手動で更新する方法の情報提供が実施された。

また、スマートホームの情報を一元管理する HEMS コントローラーがインターネットに接続されている場合、外部の第三者から不正アクセスされる可能性についての報告もあった。当該 HEMS コントローラーはホームルーターを介してインターネット接続することを前提としていたが、30 世帯以上でインターネットに直結していたため、HEMS のモニター画面が見える状態になっており、第三者に情報を見られたり、家庭内機器を遠隔操作されたりする恐れがあった。

出典：IoT 開発におけるセキュリティ設計の手引き 5.3 章（IPA）

https://www.ipa.go.jp/files/000052459.pdf,(参照 2021-02-05)

### 4) 照明システムへの侵入

ビルの照明をハッキングし、屋外から見える窓の照明を使って巨大なパズルゲームにした。ハッキングは公開のもと、デモンストレーションとして行われ、実際に窓照明によって作られた巨大な画面の上から下へと、照明によって色付けされたブロックが流れ落ちる様子が、動画としても残されている。攻撃として行われた内容自体は、いたずらのデモンストレーションであり、実害の無いものだが、実在のビルの照明のシステムを実際に乗っ取り、自由に制御できることを示したものであり、実行する内容次第では、例えば照明を落としてその間に何らかの犯罪を行うなど、実害をもたらすような攻撃も可能であることを示したものであった。

出典：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 2.2 章（経済産業省）

https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_seido/wg_building/pdf/20190617_01.pdf,(参照 2021-02-05)

### 5) ロボット掃除機の脆弱性

ロボット掃除機の一部機種に脆弱性があり、第三者から不正に操作されるおそれがあった。この掃除機はスマートフォンから操作可能であり、操作に利用する無線 LAN に攻撃者がアクセス可能であると、この脆弱性を悪用して掃除機を乗っ取られる。さらにカメラ搭載モデルの場合、室内を覗き見され、プライバシー侵害となるおそれがあった。本脆弱性に対応するセキュリティパッチが提供され、利用者に対しパッチ適用が呼びかけられた事例であった。

出典：情報セキュリティ 10 大脅威 2018「IoT 機器の不適切な管理」（IPA）

https://www.ipa.go.jp/files/000065376.pdf,(参照 2021-02-05)

### 6) 自動車の脆弱性

大手自動車メーカーが、自動車の脆弱性の通知を受け、その対策を実施した事例である。カーナビやエンターテイメントシステムを提供する車載機器の脆弱性を用いて、偽の携帯電話ネットワークから SMS を送付する等の操作により、ドアの開錠や任意コード実行等の操作が行えたものであった。

出典:『第 2 層:フィジカル空間とサイバー空間のつながり』の信頼性確保に向けたセキュリティ対策検討タスクフォースの検討の方向性(自動車の脆弱性に関する Black Hat USA 2019 での報告)(経済産業省)

https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_seido/wg_bunyaodan/dainiso/pdf/002_03_00.pdf,(参照 2021-02-05)

### 7) Web サービスに収集された IoT 機器情報の漏洩

Web サイト(クラウドサービス)の脆弱性を狙った攻撃による不正アクセスから、プライバシー情報を含む個人情報の漏洩が多数報告されている。Web サイトの脆弱性を狙ったゼロデイ攻撃による不正アクセスを受けた事例もあった。今後、住まい手の健康情報を IoT 機器で収集しクラウドで管理するモデルが遠隔医療などで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。

出典:情報セキュリティ 10 大脅威 2017「ウェブサービスからの個人情報の窃取」(IPA)

https://www.ipa.go.jp/security/vuln/10threats2017.html,(参照 2021-02-05)

### 8) スマートスピーカーの不正操作

各メーカーから音声アシスタント搭載スピーカーが発売されている。これらは、スマートスピーカーと呼ばれ、対話型の音声操作に対応した AI アシスタントが利用可能である。インターネットを介した検索、音楽の再生、家電の操作、AI との会話などと多岐にわたる機能がある。一方で、インターネットに接続されていることから、ハッキングされることで家庭内のプライバシーに関わる音声が盗聴されるリスクやエアコン等他の IoT 機器の不正操作などのリスクの警鐘が鳴らされている。

出典:ここからセキュリティ!情報セキュリティ・ポータルサイト IoT のセキュリティ(IPA)

https://www.ipa.go.jp/security/kokokara/,(参照 2021-02-05)

# 添付E 用語集

あ行

- アクチュエータ [英] Actuator
  電気や油圧などのエネルギーやコンピュータの信号を、物理的運動に変換し、機器を動かす駆動装置のこと。メカトロニクスにおいて中心的な役割を果たす。
- 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)、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。
- IPA [英] Information-technology Promotion Agency, Japan
  独立行政法人情報処理推進機構の略称。国家試験である情報処理技術者試験なども実施している機関である。
- インシデント [英] Incident
  望まない単独若しくは一連のサイバーセキュリティ事象、または予期しない単独若しくは一連のサイバーセキュリティ事象であって、事業運営を危うくする確率およびサイバーセキュリティを脅かす確率が高いもの。
- OEM [英] Original Equipment Manufacturer
  他社ブランドの製品を製造すること。「相手先ブランド名製造」などと訳される。

か行

- 可用性 [英]Availability
  認可された主体が要求したときに、アクセス及び使用が可能である特性。
- 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、主体またはプロセスに対し、情報を使用させず、また開示しない特性。
- 共用スペース
  共用スペースとは、区分所有法(建物の区分所有等に関する法律)における「共用部分」を意味せず、一般的に共用で使用されるスペースをいう。共用部分にはバルコニーのような住まい手が実質的に専用利用する箇所も含まれる。本書では、そのような管理主体が住まい手の部分は共用スペースには含めない。共用スペースの例示となる箇所は、「共用部分」における例示箇所と同じである。本書の読み手を意識し、本書では、分譲と賃貸に共通する言葉として用いる。
- 共用部分
  区分所有法における共用部分をいい、分譲マンションなどの区分所有建物で、専有部分以外の建物部分や付属部分のことをいう。例えば、エントランス、共用廊下、階段、エレベーターホール、機械室、車庫などの建物部分やエレベーター設備、電気設備、給排水設備、インターネット通信設備などの建物の付属部分をいう。

- 区分所有者
  分譲マンションのように独立した各部分から構成されている建物を「区分所有建物」という。 この区分所有建物において、建物の独立した各部分のことを「専有部分」という。 区分所有者とは、この専有部分を所有する者のことである。区分所有法における区分所有者である。
- 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。
- 戸建
  本書では、一戸建住宅を指す。長屋のうち、共用の機器やネットワークをもたない形式は戸建に含む。
- 広域通信網　[英] Wide Area Network（WAN）
  地理的に離れた地点間を結ぶ通信ネットワーク。建物内や敷地内を結ぶ LAN と対比される用語で、通信事業者が設置・運用する回線網をいう。
- 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
  電子的な情報の漏洩や改ざんをはじめ、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 Space
  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、または認可されてないアクセスや使用の試み。
- サニタイズ　[英] Sanitize
  本書で扱うサニタイズは、保存されたデータを簡単に取り出したり再現したりできないという合理的な保証を得るために記憶媒体からデータを削除するプロセスのことである。例えば、ファイルシステム上のデータを単にコマンド等で削除するのではなく、媒体上のデータの格納領域を非機密データで何度となく上書きすることや、保存媒体を分解、焼却、粉砕、細断、溶解などによって物理的に破壊することである。なお、プログラムにおいて入力されたデータから危険なコードやデータを変換または除去して無害化する処理のこともサニタイズという。例えば、Web サイトの入力フォームから、悪意のあるコードが入力され、その文字列が実行されることで様々な被害に遭う可能性があり、この入力値に対しサニタイズを行い、悪意のあるコードを無害化することで、攻撃へ対処する。
- 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。
- サービス拒否攻撃
  サービス拒否攻撃の説明は、「DoS 攻撃」、「DDoS 攻撃」の項を参照。
- 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。
- 住戸
  本書では、共同住宅における住宅内のことを指す。ベランダや専用庭などを含む。
- 住戸外
  本書では、共同住宅における住宅内以外のことを指す。住戸と離れた場所にある専用の物置、駐車場、菜園などをいう。
- 住棟
  本書では、マンションや団地の棟を指し、複数の住戸で構成される建物をいう。
- 信頼性 [英] Trustworthiness
  信頼また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または影響されると認知している、あらゆる人または組織。
- スマートメーター [英] Smart Meter
  通信機能を持つ電子式電力量計である。従来の電力量計とは異なり、スマートメーターは通信回線を利用して電力会社に使用量を送信できる。
- 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、資産または管理策の弱点。
- ゼロデイ攻撃 [英] Zero-Day Attack
  脆弱性の修正プログラムが開発ベンダーより提供される前に行われるサイバー攻撃。
- 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。
- 専有部分
  区分所有法における専有部分をいい、分譲マンションなどの区分所有建物において、区分所有者が単独で所有している部分のことをいう。一般的には住戸部分をいうが、天井・床・壁などコンクリート躯体部分で囲まれた内部空間となる。これに対して、区分所有建物において、区分所有者全体で所有している部分は「共用部分」という。
- Society 5.0
  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

- 耐タンパー機能 [英] Tamper Resistant
  機器や装置、ソフトウェアなどの内部構造・データ処理メカニズムや記録されたデータなどが、外部から不当に解析、読み取り、改変されにくいようにする機能。
- 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。
- 宅内
  本書では、戸建住宅における住宅内のことを指す。建物がある敷地内をいい、ベランダや庭を含む。
- 宅外
  本書では、戸建住宅における住宅内以外のことを指す。敷地外にある専用の物置、駐車場、菜園などをいう。
- 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
  Web 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。
- WPA [英] Wi-Fi Protected Access
  無線 LAN 製品の普及促進を図ることを目的とした業界団体の Wi-Fi Alliance が策定したセキュリティプロトコルで WPA、WPA2、WPA3 がある。

な行

- NICT [英] National Institute of Information and Communications Technology
  国立研究開発法人情報通信研究機構の略称。情報通信分野を専門とする公的研究機関。経済成長の原動力である情報通信技術の研究開発の推進などを実施している。

は行

- ハザード [英] Hazard
  ハザードは、危険の原因・危険物・障害物などを意味し、潜在的危険性をいう。
- 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、相互に関連するまたは相互に作用する、論理的また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、予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。一般的に「指針、方針」を示す際に本件の表記を利用する。
  - 管理のポリシー
    IoT 機器を管理することを意図したポリシー（指針、方針）を示す際に本件の表記を利用する。主に、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などを表記したい場合に利用する。
  - サービス提供のポリシー
    「サービス提供」を意図したポリシー（指針、方針）を示す際に本件の表記を利用する。主に、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のサービスなどを表記したい場合に利用する。プライバシーに関わるサービスで取り扱うデータに関する指針・方針も含む。
  - 個人情報を含むデータ管理などのポリシー
    「個人情報」を含むデータの管理のポリシー（指針、方針）を示す際に本件の表記を利用する。主に、住まい手を意識した際に本件表記を利用する。

## ま行

- マルウェア　[英] Malware
  許可されていないプログラム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。
- Mirai
  ネットワークカメラやホームルーターといった家庭内のオンライン機器（IoT デバイス）を主要ターゲットとしているマルウェア。感染すると遠隔操作できるボット化し、大規模なネットワーク攻撃(DDoS 攻撃)に使われる。亜種も多数存在している。

## 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囲のネットワークも含む。
- LTE　[英] Long Term Evolution
  携帯電話の 4G(4th Generation)の通称で第 4 世代移動通信システムのこと。

- LPWA　[英] Low Power Wide Area
  通信速度は数 kbps から数百 kbps 程度と携帯電話システムと比較して低速なものの、一般的な電池で数年から数十年にわたって運用可能な省電力性や、数 km から数十 km もの通信が可能な広域性を有している。IoT の構成要素の 1 つとして注目されている。
- リスク　[英] Risk
  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
  それ自体また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。
- ルーター　[英] Router
  異なるネットワーク間を中継する装置。本書では広域通信網（インターネット等）にアクセスするために家庭内または組織内のネットワーク（LAN）の中継を行う装置を指す。

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「Society 5.0」、「Connected Industries」によって拡張したサプライチェーン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,( 参 照 2021-02-05) |

- 「IoT セキュリティガイドライン」

| | |
|---|---|
| 発行元 | IoT 推進コンソーシアム・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/,(参照 2021-02-05)<br>https://www.soumu.go.jp/main_content/000428393.pdf,(参照 2021-02-05) |

- 「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,(参照 2021-02-05) |

## 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スペースに対するセキュリティ対策の参考となる。 |
| 参照先 | https://www.meti.go.jp/press/2019/06/20190617005/20190617005_01.pdf,(参照 2021-02-05) |

- 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 | スマートホームサービスや住宅、住設機器の企画、設計、施工、運用に関わる企業の開発者を主な対象とし、各ライフサイクルにおいて考慮すべきセキュリティ対策の方針をガイドラインとしてまとめたものである。スマートホーム向け製品やサービスのセキュリティ上のリスク分析・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,(参照 2021-02-05)<br>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,(参照 2021-02-05)<br>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,(参照 2021-02-05) |

**その他参考文献**

- NISTIR 8200(Draft) Interagency Report on Status of International Cybersecurity Standardization for the Internet of Things (IoT)

| | |
|---|---|
| 発行元 | National Institute of Standards and Technology<br>(米国国立標準技術研究所) |
| 概要 | コネクティッドカー、消費者向け IoT 機器、ヘルス IoT 機器、スマートビル、スマート製造を対象とし、IoT のサイバーセキュリティの目的、リスク、脅威の分析および IoT サイバーセキュリティの国際標準化状況を整理し、読者へ発信することを目的としている。 |
| 参照先 | https://csrc.nist.gov/publications/detail/nistir/8200/draft,(参照 2021-02-05) |

- NISTIR 8228 Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks

| | |
|---|---|
| 発行元 | National Institute of Standards and Technology<br>(米国国立標準技術研究所) |
| 概要 | IoT 機器利用におけるサイバーセキュリティのリスクだけでなく、プライバシーリスクも IoT 機器のリスクとし、これらに関して考慮すべき事項を記載している。 |
| 参照先 | https://csrc.nist.gov/publications/detail/nistir/8228/final,(参照 2021-02-05) |

- NISTIR 8259(DRAFT) Recommendations for IoT Device Manufacturers: Foundational Activities and Core Device Cybersecurity Capability Baseline (2nd Draft)

| | |
|---|---|
| 発行元 | National Institute of Standards and Technology<br>(米国国立標準技術研究所) |
| 概要 | IoT 機器メーカーが行うべき 6 つのアクティビティを、IoT 機器を市場に出す前のフェーズ(4 つのアクティビティ)と、IoT 機器を市場に出した後のフェーズ(2 つのアクティビティ)に分けて整理している。IoT機器のサイバーセキュリティ対策基準については、NISTIR 8228 と同等の内容を推奨している。 |
| 参照先 | https://csrc.nist.gov/publications/detail/nistir/8259/archive/2020-01-07,(参照 2021-02-05) |

- NISTIR 8259A IoT Device Cybersecurity Capability Core Baseline

| | |
|---|---|
| 発行元 | National Institute of Standards and Technology<br>(米国国立標準技術研究所) |
| 概要 | 物理的なアクチュエータやセンサー機能を持つとともに、ネットワークインタフェースでインターネットに接続される機器を対象とし、Core Baseline として、ネットワークに接続される IoT 機器が最低限満たすべき要件を記載している。 |
| 参照先 | https://csrc.nist.gov/publications/detail/nistir/8259a/final,(参照 2021-02-05) |

- NISTIR 8267(Draft) Security Review of Consumer Home Internet of Things (IoT) Products

| | |
|---|---|
| 発行元 | National Institute of Standards and Technology<br>(米国国立標準技術研究所) |
| 概要 | 仕様書や Web サイトの情報などの公開情報からのセキュリティ機能調査と、製品を実際に動作させた状態でのセキュリティ機能を観察することによる調査を行ない、セキュリティ機能上の課題を明らかにしている。 |
| 参照先 | https://csrc.nist.gov/publications/detail/nistir/8267/draft,(参照 2021-02-05) |

- Security for IoT Sensor Networks : Building Management Case Study (DRAFT)

| | |
|---|---|
| 発行元 | National Institute of Standards and Technology<br>(米国国立標準技術研究所) |
| 概要 | IoT センサーネットワークの一般的なコンポーネント毎に脅威およびセキュリティ要件を整理している。ビル管理システムを例とした IoT センサーネットワークへの脅威シナリオおよびサイバーセキュリティ対策要件を示している。 |
| 参照先 | https://csrc.nist.gov/publications/detail/white-paper/2019/02/01/security-for-iot-sensor-networks/draft,(参照 2021-02-05) |

- Considerations for a Core IoT Cybersecurity Capabilities Baseline(DRAFT)

| | |
|---|---|
| 発行元 | National Institute of Standards and Technology<br>(米国国立標準技術研究所) |
| 概要 | あらゆる IoT 機器がサポートすべき 12 のサイバーセキュリティ機能を提案している。12 のサイバーセキュリティ機能には、IoT 機器の管理(物理的、ソフトウェア、ファームウェア)、アクセス制御、データおよび通信データの暗号化、イベントログの記録などが挙げられている。このベースラインは、個々のセクター、業種別のより詳細なベースラインを開発するための基礎として役立つ。 |
| 参照先 | https://www.nist.gov/system/files/documents/2019/02/01/final_core_iot_cybersecurity_capabilities_baseline_considerations.pdf,(参照 2021-02-05) |

- Code of Practice for Consumer IoT Security

| | |
|---|---|
| 発行元 | Government of UK, Department for Digital, Culture, Media & Sport<br>(英国デジタル・文化・メディア・スポーツ省) |
| 概要 | IoT のセキュリティにおけるベストプラクティスを、成果に焦点を当てて 13 項目のガイドラインに集約している。また、本プラクティスは「ETSI EN 303 645」のもとにもなっている文献である。 |
| 参照先 | https://www.gov.uk/government/publications/code-of-practice-for-consumer-iot-security,(参照 2021-02-05) |

- Draft ETSI EN 303 645 CYBER; Cyber Security for Consumer Internet of Things

| | |
|---|---|
| 発行元 | European Telecommunications Standards Institute<br>(欧州電気通信標準化機構) |
| 概要 | 本標準は消費者向けの IoT 機器に関するセキュリティ上の課題を解決するためのものではなく、重要で広範なセキュリティの課題に対処する技術的な制御と組織のポリシーに焦点をあてている。 |
| 参照先 | https://www.etsi.org/deliver/etsi_en/303600_303699/303645/02.00.00_20/en_303645v020000a.pdf,(参照 2021-02-05) |

- IEC63168

| | |
|---|---|
| 発行元 | IEC（国際電気標準会議、The International Electro technical Commission） |
| 概要 | スマート化対応機器・システムを導入していくと、複数の動作の組み合わせ、周囲の状況などにより思わぬ不具合が生じる可能性があり、このようなリスクの低減を目的に IEC 63168 の標準化が進められている。 |
| 参照先 | https://www.iec.ch/dyn/www/f?p=103:23:0::::FSP_ORG_ID:11827,（参照 2021-02-05） |

- IoT Security Foundation, IoT Security Compliance Framework

| | |
|---|---|
| 発行元 | IoT Security Foundation（IoT セキュリティ財団） |
| 概要 | ハイパーコネクティッドデジタルの世界では広い範囲でセキュリティ上の不安がある。このような背景をもとに、IoT Security Foundation は「IoT の保護および採用を支援し、その利益を最大化すること」を使命としており、支援の一つとして本フレームワークを発行している。 |
| 参照先 | https://www.iotsecurityfoundation.org/tag/iot-security-compliance-framework/,(参照 2021-02-05) |

- Baseline Security Recommendations for IoT

| | |
|---|---|
| 発行元 | European Network and Information Security Agency<br>(欧州ネットワーク・情報セキュリティ機関) |
| 概要 | IoT のセキュリティおよび安全性の確保は、IoT 機器自身だけでなく、クラウドなどのバックエンドのサーバやサービス、アプリケーション、保守ツールや診断ツールなどの全ての関連システムのセキュリティと安全性に掛かっている。また、IoT は技術的側面だけでなく、法的、政治的、規制的側面でも、幅広く複雑な問題を提起している。 |
| 参照先 | https://www.enisa.europa.eu/publications/baseline-security-recommendations-for-iot,(参照 2021-02-05) |

- The C2 Consensus on IoT Device Security Baseline Capabilities

| | |
|---|---|
| 発行元 | CSDE: Council to Secure the Digital Economy |
| 概要 | 技術内容に特化した IoT デバイスセキュリティにおいて、様々な団体・規格等から抽出した 13 項目の共通機能項目を策定している。各機能の留意点をまとめたもの。具体的な対策は参照先ドキュメントへのマッピングを記載している。 |
| 参照先 | https://securingdigitaleconomy.org/wp-content/uploads/2019/09/CSDE_IoT-C2-Consensus-Report_FINAL.pdf,（参照 2021-02-05） |

- SoK: Security Evaluation of Home-Based IoT Deployments

| | |
|---|---|
| 発行元 | 2019 IEEE Symposium on Security and Privacy (SP) |
| 概要 | 家庭用の IoT システムのセキュリティに関する調査により、攻撃ベクトル(脆弱性)、対策方法、ステークホルダーの傾向を分析。さらに、市場にある 45 個の製品に関して製品評価を実施し、存在する脆弱性、実施されている対策を洗い出している。 |
| 参照先 | https://alrawi.github.io/static/papers/alrawi_sok_sp19.pdf,（参照 2021-02-05） |

- BSI TR-03148 Secure Broadband Router 1.1

| | |
|---|---|
| 発行元 | Federal Office for Information Security |
| 概要 | エンドユーザーに提供される OS とサービスを備えたハードウェアコンポーネントとしてのルーターを対象とし、工場出荷時の設定と初期化された状態のルーターへの機能要件を明記している。 |
| 参照先 | https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR03148/TR03148.html,(参照 2021-02-05) |

- IoT **分野共通セキュリティ要件ガイドライン** 2019 **年版** ver2.0

| | |
|---|---|
| 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（略称 CCDS） |
| 概要 | IoT 機器に対するミニマムリクワイアメント（最低限のセキュリティ要件）として、多くの IoT 機器で対応できるよう、全 11 の要件が定義されている。<br>国内外のセキュリティ標準と比較し、Bluetooth や USB に関する要件が含まれている点が特徴となる。 |
| 参照先 | https://www.ccds.or.jp/certification/documents.html,(参照 2021-02-05) |

- 2010 **年度版 情報家電におけるセキュリティ対策 検討報告書**

| | |
|---|---|
| 発行元 | 独立行政法人 情報処理推進機構 |
| 概要 | 2010 年当時の状況において、今後普及が進んでいく情報家電機器におけるセキュリティ課題と業界としての取り組みの方向性についてまとめられている。<br>そのうえで、既に普及しつつあったネットワーク接続されるデジタルテレビを対象として、具体的なセキュリティ対策についてリストアップされている。 |
| 参照先 | https://www.ipa.go.jp/security/fy22/reports/electronic/,(参照 2021-02-05) |

- IoT **セキュリティチェックリスト**

| | |
|---|---|
| 発行元 | JPCERT コーディネーションセンター（JPCERT/CC） |
| 概要 | ioT 機器に存在すべきセキュリティ機能についてチェックリスト化している。各要件は IoT 機器が提供する機能に基づいて、必要な機能が絞り込めるようになっている。 |
| 参照先 | https://www.jpcert.or.jp/research/IoT-SecurityCheckList.html,(参照 2021-02-05) |

- **ネットワークカメラシステムにおける情報セキュリティ対策要件チェックリスト 第** 2 **版**

| | |
|---|---|
| 発行元 | 独立行政法人情報処理推進機構<br>特定用途機器情報セキュリティ対策検討委員会 |
| 概要 | IoT 機器に存在すべきセキュリティ機能についてチェックリスト化している。各要件は IoT 機器が提供する機能に基づいて、必要な機能が絞り込めるようになっている。 |
| 参照先 | https://www.ipa.go.jp/security/jisec/choutatsu/nwcs/checklist_nwc.pdf,( 参照 2021-02-05) |