スマートホーム IoT データプライバシーガイドライン

一般社団法人 電子情報技術産業協会
スマートホーム部会

令和 5 年 3 月

目次

第一部： 本ガイドラインの位置づけ

エクゼクティブサマリー

宅内外のあらゆる家電機器・住設機器・サービス等が生活データを中心に連携するスマートホームでは、利用者ニーズにあったサービスの高度化や社会課題の解決が期待されている。一方で、個人の生活領域に関連する膨大なデータが収集・利活用されるため、データの漏洩や不適切な取り扱いがあった場合には、利用者のプライバシーが侵害されることとなる。このため、事業者はプライバシーに関わるリスクを事前に予測して、その対策を取ることが不可欠となる。万が一、重大なプライバシー侵害を引き起こした場合には、損害賠償請求を受けることや、差止請求によって事業からの撤退を余儀なくされるというケースもあり得る。

データが個人情報に該当する場合には、事業者は個人情報保護法[1]を遵守した上で当該データを取り扱うことが当然の前提となる。しかしながら、家電機器や住設機器などから収集されるデータは個人情報には該当しない場合もあり、この場合には個人情報保護法のルールは適用されない。このような IoT データに対しても、利用者のプライバシー保護の観点で事業者が講ずべき措置が多数ある。

本ガイドラインでは、スマートホームで取り扱われる生活データの分類やスマートホーム向けサービスでのデータの利活用に関する考察を踏まえ、スマートホーム関連事業者に求められるルールを提示していく。ルールは以下の三つの要素から構成される。

① どのようなデータを、どのように取得して、どのような目的に利用するか、データのライフサイクルにわたって説明する際の記載項目および粒度に関するルール
② どのような場合に利用者からの同意取得を考慮する必要があるか、どのような方法で同意を取得するべきかに関するルール
③ 利用者自身が、データの開示や訂正・追加・削除、利用停止などのコントロールができる機能の提供に関するルール

本ガイドラインで提示するルールは、利用者に提示するべきプライバシーポリシーの作成時や、機器・サービス仕様の作成時などに活用できる。

また、プライバシー保護への取り組みは現場レベルの対策に留まらず、事業者全体として対策の実効性を確保するためにも、経営者やサプライチェーン全体を含めたガバナンスレベルでの対応も必要である。このため、プライバシーガバナンスの重要性や、プライバシーリスク評価の取り組みについても紹介する。

---

[1] 本ガイドラインでは、令和 2 年 6 月公布、令和 4 年 4 月施行の令和 2 年改正個人情報保護法を前提とする

1. はじめに

スマートホームとは、宅内外のあらゆる家電機器・住設機器・サービス等が生活データを中心に連携することで、利用者ニーズに合ったサービスの高度化、社会課題の解決につなげられると期待されている新たな成長市場である。テクノロジーの進化や低廉化を背景に、ネットワーク対応の家電機器をはじめとして、住宅内に多くのセンサーや情報をデジタル化する機器が設置されつつあり、スマートホームの急速な普及が見込まれている。

本ガイドラインは、インターネットに接続するスマートホーム関連機器の提供事業者をはじめ、スマートホームの住まい手に向けたサービス提供事業者などの幅広い関係者とスマートホームの住まい手である利用者との間の信頼関係を構築するため、スマートホームにおける生活データであるスマートホーム IoT データの取り扱い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、スマートホームに設置される様々な IoT 機器が収集するスマートホーム IoT データについて、個人情報保護やプライバシーに配慮しながら収集・活用するために、各関係者が考慮すべき最低限のあるべき姿を示している。

なお、業種・業態に特化した、または詳細な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、各々の対策を考案されたい。

1.1. スマートホームとは

1.1.1. スマートホームが社会にもたらすもの

本ガイドラインでは、スマートホームを「社会課題の解決と利用者の利便性向上の両立を達成するために、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もの」と独自に定義をする。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、国内外での市場形成・普及に向けて期待されている状況にある。

スマートホームでは、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 技術で実現することができる。家電機器・住設機器や 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収集された住まい手の生活データ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るなか、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、住まい手の生活データ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。

1.1.2. スマートホームを取り巻く環境や状況

近年、IoT 機器が普及したことによって、スマートホームの住まい手である一般利用者の生活は大きく変化している。従来の家電機器や住設機器は、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機器や住設機器等の 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、様々な利便性の高い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 機器や家電機器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 機器とクラウドとの橋渡しを行う 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。

スマートホーム市場の構築に向けては、上記のような IoT 機器から収集するスマートホーム IoT データを活用した戦略立案や実行は欠かせない一方、収集したスマートホーム IoT データを活用する場合には、利用者の個人情報・プライバシー情報を保護するべく、細心の注意を払わなければならない。スマートホーム市場が本格普及期に入ると、個人の生活領域に関連する膨大なスマートホーム IoT データが収集・利活用されることによって、プライバシーの侵害が起きるリスクも高まっていく。万が一、個人情報・プライバシー情報が利用者の想定外の方法で利用されたり漏洩したりした場合には、無関係な企業からプライベートな情報に基づく広告を受け取ったり、知人・友人に私生活の状況が知られたりするなど、利用者のプライバシーを侵害することとなる。このため、事業者はプライバシーに関わるリスクを事前に予測して、その対策を取ることが不可欠となる。

スマートホーム IoT データの内容は多様であり、プライバシーに関する様々な情報も含まれる。その中には個人情報保護法における個人情報に該当する情報もありえるが、個人情報に該当しなくても個人の権利利益の侵害につながりうる情報もありえる。前者の情報の利活用と保護は個人情報保護法により規律されるが、後者に関しては法的な保護義務がないとはいえ、その利用により個人の権利利益の侵害が起きるのであれば、事業者はその対策が求められるのは当然である。

また、スマートホーム IoT データの利活用において鍵となるのは、IoT 機器の利用者からの信頼である。これまでプライバシー対策は事業者にとってコストや手間と考える企業が多かった。しかし、そもそも適切なプライバシー対応は IoT 機器やそれのサービスにおける不可欠な品質であり、プライバシー対策を行うことは商品やサービスの品質の改善のひとつとして扱うべきである。実際、適切なプライバシー対応している IoT 機器やサービスは利用者の信頼につながり、それらの販売だけでなく、利用者からスマートホーム IoT データの取得も容易になる。

1.2. スマートホーム IoT データにおける課題

スマートホーム IoT データに対して利用者が懸念するのは、「どのようなデータが、どのような経路で集められているか分からないので、気が付かないうちに自分自身でプライバシーをさらけだしてしまっているのではないか。」という事であろう。一方で、法律用語で構成されている長文の利用規約やプライバシーポリシーが利用者から敬遠され、結果として事業者から利用者への説明が不十分なものとなっているという状況もある。

しかし、スマートホーム IoT データの取り扱いに関して説明が不十分なことで利用者に不信感を与えることは、IoT 機器やそのサービスの提供者にとって好ましいことではない。そこで、まずは「スマートホーム IoT データが受け入れられるための課題」を並べ、その解決に結びつけていきたい。

スマートホーム IoT データに対して利用者が不安に思うことを分解すると、以下の3点が挙げられる。

1）どのようなデータが集められるのか（収集・保有・利用される情報の性質）
2）そのデータをなぜ収集するのか（収集・保有・利用する目的）
3）そのデータがどのように取り扱われるのか（収集・保有・利用の方法）

1）どのようなデータが集められるのかについて、例えば、「バネ秤」と「IoT 機器」では利用者の理解が大きく違ってくる。「バネ秤」であれば重量を計測していることは誰にでも分かるが、「IoT 機器」は、音声や映像など多様なセンサーで多様な情報を取得することができることに加えて、何を計測しているか一見して分からないことから利用者の懸念が生まれる。また、設置するカメラやセンサー等が高解像度なものになっていけば、例えば指紋や虹彩のような現時点では読み取れない情報も認識されるようになるなど、機器の精度が上がれば「どのようなデータが集められるのか」も変わってくる。さらに、カメラ映像の分析技術が向上していけば、心拍数や喜怒哀楽などの感情を推測することもできるようになり、このような分析結果の情報が収集されることも考えられる。そして、そもそもスマートホーム IoT においては、居住する自宅内という完全に私的な領域で観察されたデータであることに留意する必要がある。

2）そのデータをなぜ収集するのかについて、購入したスマートホーム IoT 機器の事業者が提示する「データの利用目的」が曖昧であったり、収集されたデータが利用目的以外に取り扱われているか疑わしいなど、不安を感じる人は多いであろう。利用者としては、その製品を自身が使用するにあたって必要となる範囲であれば当然のものとして受容できても、その範囲を超える場合には自身にとっての利益（間接的・婉曲的なものも含めて）が無ければ、同意なく利用されることに納得できるものではない。

3）そのデータがどのように取り扱われるのかについては、スマートホーム IoT データの場合には、ネットワークの先で誰がデータを集めているか利用者には見えない。またデータが収集されるタイミングや、データがいつまで残るのか、どのような安全措置

のもとで保管されるのかについても、利用者には分からない。さらに、残されたデータは自分の家族にまで紐づけられてしまうかもしれない。利用者の残した情報が、利用者の子どもや孫にまで紐づけられて、そこに不利益が生じることになった場合には、警戒はより強まることであろう。

従って、スマートホーム IoT データの管理方法そのものについてや、サービス提供終了後のスマートホーム IoT データの取り扱いについても明確にしておく必要が出てくる。また、企業の破産や M&A によって当初知らされていた事業者以外に自身のスマートホーム IoT データが渡る可能性についても懸念する声があり、この可能性についても考慮が必要である。

本ガイドラインにおいては、上記のような課題を解決し、利用者からの信頼確保に向け、 スマートホーム IoT データのプライバシー情報保護を企図し、事業者側における利用者のスマートホームに関連するデータを収集・活用する際の取り扱いや、企業間連携に向けたデータ取り扱いに関するルールを規定するとともに、利用者にとって信用・信頼できるスマートホーム実現の一助とする。

1.3. 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。なお、本ガイドラインは一般利用者を対象として記載するものではないが、下記(1)～(4)の事業者は、一般利用者が重要なステークホルダーであることを意識して本ガイドラインを活用いただきたい。万が一プライバシー侵害にあたる事案が発生した場合に、直接的に影響を受けるのは一般利用者である。その結果として、損害賠償請求や差し止め請求、ブランド価値の毀損など、事業者も間接的に影響を受けることとなる。

また、本ガイドラインの活用に際しては、一般利用者のプライバシーに関する懸念を払拭するように努めるとともに、より便利なサービスの提供等を通じてプライバシーに関する受容性を向上していくことも重要である。

なお、各スマートホームの形態によっては、電気通信事業に該当する場合がある。

(1) スマートホーム向け IoT 機器の製造事業者

スマートホーム IoT データ収集を可能にする IoT 機器を開発・生産・販売する事業者。例えば家電機器や住設機器、各種センサー類等の製造元（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サービス提供事業者

宅内から収集されるスマートホーム IoT データを利活用し、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。例えば、ネットワークに接続した電気ポットを利用した見守りサービスの事業者や、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。

(3) スマートホーム関連データ取り扱い事業者

クラウド上でスマートホーム IoT データを含む各種データを集約・分析する機能を提供するプラットフォーム事業者や構築支援事業者。当該データに基づいてサービス等を提供するサービス事業者等。

本ガイドラインでは、一般利用者に直接向き合うこととなる上記(1)や(2)の事業者が注意すべき点を中心として取り纏めているが、スマートホーム IoT データを取り扱うその他の事業者もプライバシー侵害を引き起こすことのないよう本ガイドラインを参照されたい。

(4) その他 スマートホーム関連事業者

スマートホームを提供・販売・流通する事業者。(1)～(3)の事業者より委託を受け、利用者に対してプライバシーポリシーを明示したうえで、スマートホームをパッケージとして提供する場合も含まれる。

1.4. ガイドラインの活用方法

本ガイドラインは、クラウド上へスマートホーム IoT データをアップロードしたり、クラウドを介して遠隔制御されたりする IoT 機器や、アップロードされたスマートホーム IoT データを利用するサービスにおいて、事業者が利用者のプライバシーを適切に保護するための基本となる考え方を示すものである。このために、各事業者が提供する IoT 機器やサービスにおける利用規約や、スマートホーム IoT データの取り扱いに関するプライバシーポリシーを作成する際の指針として、本ガイドラインを活用することを想定している。また、データ送信に関するシステム設計や、同意取得および利用者によるデータのコントロール(自己コントロール性)の提供に関するユーザインタフェース設計の際の指針としても、本ガイドラインを活用することを想定している。

1.4.1. ガイドライン活用の効果

一般にクラウドに接続可能な IoT 機器から収集されうるスマートホーム IoT データは、IoT 機器の機能、その他新たな技術やサービス、環境の変化などにより、様々な用途に対応した利用形態のアップデートが想定される。また IoT 機器から収集されるスマートホーム IoT データは、その取り扱いに関してサービス事業者が提示するプライバシーポリシーに対する利用者からの同意を得てサービス事業者が収集し、プライバシーポリシーに定められた範囲内で使うことが前提となる。このため、IoT 機器からのスマートホーム IoT データにおけるプライバシー保護のための取り扱いは、利用者の不利益が無いように配慮しつつ、それらの変化に柔軟に対応していくことが求められ、サービス開始前に利用者が同意する利用規約やプライバシーポリシーについても、その方針に沿ってあわせて反映していくことが求められる。

利用者に安心して使っていただけるクラウドサービスシステムを提供するには、IoT 機器とクラウド間で行きかうスマートホーム IoT データを安全に管理し、健全に運用し、それを利用者に明確に提示し、必要に応じて同意を得ることが前提となる。また

IoT 機器の発売やサービス開始時点では存在していない新たなデータ活用方法の登場や、IoT 機器本体ソフトウェアのアップデートによる新規データ活用方法も想定した利用規約やプライバシーポリシーを作成し、また利用者に対するプライバシーポリシーの内容説明や、説明したプライバシーポリシーに対する同意の確認を行っていくことが求められる。

IoT 機器の商品仕様やそのサービス仕様についても、IoT 機器の電源を入れるだけで利用者の理解や同意無しにスマートホーム IoT データがクラウドにアップロードされることが無い様に配慮した仕様やユーザインタフェースであることが求められる。

本ガイドラインを参考にすることにより、IoT 機器の製造事業者やサービス提供事業者は、将来に対する「変化」を前提とした利用規約やプライバシーポリシーの策定、IoT 機器などのユーザインタフェース、及びサービス仕様の効率的・効果的な作成が可能となる。

またサービスを利用する利用者にとっても、本ガイドラインに記載された方針に配慮・設計された事業者の機器・サービスを選ぶことで、利用者自身のプライバシーに関わるスマートホーム IoT データを安心して事業者に提供することができるようになり、このスマートホーム IoT データを利用するサービスによるメリットを安心して享受出来るようになる。

1.4.2. 活用事例

ここでは、各 IoT 機器に関する仕様作成、及び IoT 機器に関するサービスの利用規約やプライバシーポリシーを策定する際に、それぞれのステップにおいて本ガイドラインを基に活用する事例を紹介する。

1.4.2.1. 利用規約やプライバシーポリシーの作成時

事業者は、IoT に関するサービスを利用者に提供する場合、事前にデータ活用の目的、用語の定義、適用範囲、対象となるデータ、データ利用する事業者名等について説明を行い、原則としてプライバシーポリシーに対する利用者の同意を取得することとなる。同時に、利用者の同意無しに IoT 機器から収集されるスマートホーム IoT データを機器の外部に送信しないことを明確にする必要がある。また、スマートホーム IoT データを第三者に提供する場合など、提供対象となるデータ、提供先の事業者名などについても事前に通知し同意を得ることとなる。本ガイドラインでは、IoTに関するサービスの利用規約やプライバシーポリシーの文言を作成する際に、参考となる推奨記載方針を規定する。

具体的には、各種センサーで収集されるスマートホーム IoT データは、利用者の同意無しにサーバ等に外部送信されることがないことを明記する。また外部送信されたスマートホーム IoT データは、サービス事業者が責任を持って、適切な暗号化やアクセス管理などによるセキュアな状態で保管するとともに、同意を得た利用目的以外では利用しないことを記載する。なお、同意の有効性については、6 章で述べる。

1.4.2.2. サービス利用仕様作成時

利用者が、事業者の提供する IoT に関するサービスを利用する場合、スマートフォンや PC などのサービスアプリケーション等を介して利用規約やプライバシーポリシーの説明を受けたり、必要に応じて同意を与えたりすることとなる。その際アプリケーションの確認画面において、デフォルトで同意確認の選択欄が設定された状態で仕様が提供された場合、利用者が確定キーを連続押しするなどの操作を行うと、設定内容を確認できないまま、意図しない同意決定操作を強いることになってしまう。

利用規約やプライバシーポリシーへの同意欄には、初期状態では選択されていない状態とし、利用者の積極的な意図による選択操作を必須とするなど、事業者はサービス仕様を注意深く規定することが求められる。同時に利用規約やプライバシーポリシーの内容については、必ず利用者がサービスの利用前に、本文全体内容を確認できる仕様とすることが求められる。

また、利用者が IoT 機器の提供するサービス利用を必要としなくなり、利用を終了する際は、その手順をわかりやすい仕様で提供することが求められる。さらに、サービスの利用を終了した際には、速やかにスマートホーム IoT データの事業者への提供を中止するなど、プライバシーに配慮した仕様であることも求められる。

1.4.2.3. 機器データ送信仕様作成時

操作データやセンサー情報などのスマートホーム IoT データを外部送信する機能を持つ IoT 機器では、利用者からの同意なしに機器からスマートホーム IoT データをクラウドに送信させることがない仕様とすることが求められる。本ガイドラインでは、IoT 機器メーカが、本体仕様を策定する際に、機器からのスマートホーム IoT データを外部送信するまでのインタフェース仕様例等、機器データ送信仕様を設計する際の方針を規定する。

IoT 機器は、クラウドに接続することで可能となるサービスの内容や利用者メリットを設定アプリケーション内の説明以外にも、カタログや商品パッケージへの印刷、本体に説明ラベルを添付するなどの方法で利用者に伝えることが望ましい。また、IoT 機器がネットワークに接続されている状態を表示する手段（無線 LAN インジケータ等）を有し、接続中に IoT 機器のスマートホーム IoT データが外部送信されている状態であることを明確に示すことが求められる。同時に、外部送信されてサーバなどに保存されたスマートホーム IoT データは、プライバシーポリシーに記載されたサービス範囲内でのみ利用し、利用者本人と、サービス事業者（プライバシーポリシーに記載の委託先を含む）以外は使用できないように、安全に運用することが求められる。

また今後、利用者の手元に届く前に、ネットワークに繋がる通信設定などが事前になされた状態で配送される場合が想定される。その際も、使用前に利用者への説明なしに機器からの各種スマートホーム IoT データ、及びネットワークからの制御情報等が事業者に渡ることが無いように配慮された仕様とすることが求められる。

1.4.2.4. IoT 機器の設置時

住設機器などでは、IoT 機器をサービス提供事業者が設置するケースもある。このような IoT 機器がセンサーを備える場合には、その設置場所により関わりうるプライバシーの内容が変わってくることとなる。

このため、サービス提供事業者はサービス利用仕様で想定される設置場所に機器を設置する必要がある。設置上の都合などにより、サービス利用仕様で想定されていない設置場所に機器を設置する事となる場合には、利用者への説明や注意喚起を行うことが望ましい。

2. スマートホーム IoT データの概要

この章では本ガイドラインにおいて取り扱うスマートホーム IoT データの定義や分類について述べる。

2.1. スマートホーム IoT データの定義

2.1.1. IoT データとスマートホーム IoT データの関係性

既に述べた通り、現在数多くの IoT 機器が製造され、様々な分野で IoT データが活用されている。今後高成長が期待される IoT 機器の分野として、ネットワーク接続された家電機器・住設機器やIoT化された電子機器が増加する「コンシューマー」、デジタルヘルスケアの市場が拡大する「医療」、スマート工場やスマートシティが拡大する「産業用途」（工場、インフラ、物流）、コネクテッドカーの普及によりIoT化が進む「自動車・宇宙分野」が挙げられる。スマートホームは「コンシューマー」の領域に分類され、今後高い成長が見込まれている。

本ガイドラインで取り扱うスマートホーム IoT データとは、スマートホームで利用される IoT 機器が生み出す、あるいは収集するデータであり、スマートホームに属する領域に関わるものである。

2.1.2. スマートホーム IoT データとは

IoT データには、河川の橋梁のゆがみを計測するセンサー情報等のインフラの維持・高度化を支えるものや、物流を支える自動走行等に関するデータも含まれる。しかしながら、こうした IoT データは前述の「産業用途」や「自動車・宇宙分野」に該当し、本ガイドラインの対象データには含めない。

本ガイドラインでは家電機器や住設機器等が収集する、住まい手である利用者の暮らす環境データや利用者の行為から収集するデータ、あるいは利用者に直接提供するサービスのデータといったものを狭義のスマートホーム IoT データと捉え、その取り扱いについて述べるものである。具体的には以下の様な機器から収集されるデータを想定したものである。

スマートホーム IoT データを生み出す機器　例　：

・IoT 家電（冷蔵庫、エアコン等）

・IoT 住設機器（電動シャッター、インターホン、風呂・トイレ等）

・IoT ガジェット（温度計、カーテン開閉機等）

・ウェアラブル機器/スマートウォッチ

・HEMS 機器

・電気/ガス/水道　スマートメータ

・家庭用　ヘルスケア機器（体重計/体組成計等）

これらの機器は住まい手の暮らしに密着し、住まい手に対し機器としての利便性を提供するものであり、それらの機器が収集するスマートホームIoTデータは住まい手の動作や状況等の情報を知り得るものである。

2.1.3. 個人情報保護法との関係

スマートホーム IoT データの中には、個人情報保護法の定める個人情報に該当するものが存在する。例えば、映像音声データのように特定の個人が識別できる可能性があるケースや、特定の個人に関する情報である健康情報（体重など）のようなケースについては、個人情報に該当することがあり得る。また、それ自体個人情報ではないようなスマートホーム IoT データであったとしても、住所氏名など個人識別可能な情報とスマートホーム IoT データを紐付けて管理している場合にも、このスマートホーム IoT データは個人情報となりうる。また、スマートホーム IoT データは個人情報保護法の定める個人関連情報に該当し得る。スマートホーム IoT データを第三者提供する場合に、提供先で個人情報と紐付けて利用する場合には、個人関連情報の第三者提供制限の義務に留意する必要がある。

スマートホーム IoT データが個人情報または個人関連情報に該当する場合には、事業者は個人情報保護法を遵守した上で当該スマートホーム IoT データを取り扱うことが当然の前提となる。一方で、個人情報保護法の義務の対象とならないスマートホーム IoT データに対しては、個人情報保護法のルールは適用されない。しかしながら、このようなスマートホーム IoT データに対しても、利用者のプライバシー保護の観点で事業者が講ずべき措置が多数ある。本ガイドラインでは、個人情報に該当しないスマートホーム IoT データの取扱いを対象とする。

2.1.4. 対象外データ

スマートホーム IoT データの類型には、多様な項目が含まれているが、一部機器は、宅内外に設置され、データが収集される可能性があるものの、本ガイドラインの対象外とする。具体的には以下に類するデータである。

・テレビ視聴履歴
・宅外監視カメラ
・医療情報

これらのデータについては法規制に則り他の文書でその取り扱いについて議論が進められ、文書化が行われているため、そちらの文書を参照することとする。

● テレビ視聴履歴

総務省において、地上波や衛星、ケーブル放送用のテレビ視聴履歴の利活用に向けたガイドライン整備が進んでいるため、対象外とする。但し、インターネットに接続するテレビの普及によって、各世帯の視聴番組や視聴時間帯などのデータが収集されていることから、視聴履歴のガイドラインが公開された時点で、参照するか、または整合性を持った形で本ガイドライン中に記載をしていくか検討を行うものとする。

● 宅外監視カメラ

宅外監視カメラ(主として防犯用途)は、不特定多数の個人情報が記録される可能性が高く、肖像権侵害やプライバシー侵害を生じるおそれの高い分野である。しかしながら、本分野においては、先行した検討がなされている他、防犯目的で収集されるカメラ画像の取扱い指針等は各市区町村で条例が制定されていることから[2]、今回のガイドラインでは対象外とする[3]。但し、利用者および家族が対象となる宅内の映像・音声(ベビーモニタなど)については、対象とする。また、ドアホンについては呼び鈴が押された場合のみに記録することを前提として対象に含めるものとする。

● 医療情報

医薬品医療機器等法(旧薬事法)に基づいて認定される医療機器については、本WG 外の専門家の意見を要するため、対象外とする。但し、医療機器に該当しない、健康家電(体重計など)からの収集情報、環境データを用いたヘルスケアに関わる情報は対象に含めるものとする。

表 1. ガイドライン対象外となるデータと参照文献

項目	参照先文書
テレビ視聴履歴	○個人情報保護委員会／総務省 放送受信者等の個人情報保護に関するガイドライン https://www.ppc.go.jp/files/pdf/broadcast_recipient_GL.pdf

2 駅や空港等での顔識別機能付きカメラシステムの利用に関しては、個人情報保護委員会が、「犯罪予防や安全確保のためのカメラ画像利用に関する有識者検討会」を設置して、包括的に整理を行っている。また、自治体においては、防犯カメラを対象にする単独条例が、令和4年2月末時点で少なくとも 43 市区町村で制定されている。地方自治研究機構「防犯カメラに関する条例」(2022 年 3 月 6 日)参照。

3 経済産業省・総務省が「カメラ画像利活用ガイドブック ver.3.0」を策定しており、防犯カメラ目的や、特定の個人を識別する目的で取得されるカメラ画像の利活用は対象外とされている。

	○一般社団法人　放送セキュリティセンター (SARC) 「オプトアウト方式で取得する非特定視聴履歴の取扱いに関するプラクティス（ver2.0）」 https://www.sarc.or.jp/NEWS/hogo/20200731.html
宅外監視カメラ	○経済産業省／総務省 「カメラ画像利活用ガイドブック ver3.0」 https://www.meti.go.jp/press/2021/03/20220330001/20220330001.html ※防犯目的で取得されるカメラ画像の取扱いは各市区町村で制定されている「防犯カメラの設置に関するガイドライン」等を参照。
医療情報	○個人情報保護委員会 「医療・介護関係事業者における個人情報の適切な取扱いのためのガイダンス」 https://www.ppc.go.jp/personalinfo/legal/iryoukaigo_guidance/ ○3省2ガイドライン 「医療情報システムの安全管理に関するガイドライン」 「医療情報を取り扱う情報システム・サービスの提供事業者における安全管理ガイドライン」 https://www.mhlw.go.jp/stf/shingi/0000516275.html https://www.meti.go.jp/policy/mono_info_service/healthcare/teikyoujigyousyagl.html ○経済産業省 「医療情報を受託管理する情報処理事業者向けガイドライン」 https://www.meti.go.jp/policy/it_policy/privacy/iryouglv2.pdf ○総務省 「クラウドサービス事業者が医療情報を取り扱う際の安全管理に関するガイドライン」 https://www.soumu.go.jp/main_content/000567229.pdf

2.2. スマートホーム IoT データの類型

これまで記述したようにスマートホーム IoT データは、様々な IoT 機器から生成されるデータであり、これらのデータ種別は今後増加する見込みである。様々なスマートホ

ーム向けの IoT 機器が生まれるだけでなく、すでに IoT 化された機器においても技術の進歩により従来とは異なるスマートホーム IoT データを収集するようになることが考えられる。そのため、1 種類の機器毎にスマートホーム IoT データの取扱い指針を示すことはすぐに指針とのズレを生むことが考えられる。また、1つのデータ種別においても、同じデータ項目であっても収集する機器によって収集頻度、精度等が異なることが想定され、プライバシーの観点から考えられる懸念の程度は異なることが考えられる。

そのため、本ガイドラインでは1機種毎、1 つのデータ種別毎といった考え方ではなく、収集されるスマートホーム IoT データをプライバシーに与える影響を考慮した 10 種類のカテゴリに分けて考える。また、データの利用目的についても 8 種類のカテゴリに分類する。このスマートホーム IoT データのカテゴリと利用目的のカテゴリに基づき、データの取扱いについて、利用者への説明や同意の取得方法、あるいは利用者によるデータのコントロール性（自己コントロール性）について事業者が具備すべき事項について次章以降に取りまとめる。

2.2.1. スマートホーム IoT データのカテゴリ

本ガイドラインではスマートホームIoTデータを以下のデータカテゴリに分類した。本カテゴリは本ガイドライン作成時のカテゴリ分類であり、今後の IoT 機器の発展やデータ分析技術の進展により、カテゴリの項目や具体例の属するカテゴリは変わる可能性がある。

なお、個別の機器を特定できる情報のなかで IP アドレスや MAC アドレス、Cookie などについては、IoT 機器とそれに伴う IoT サービスが電気通信事業に相当する場合は、電気通信事業法に基づく対応が求められることがあるので、注意されたい。

表 2. スマートホーム IoT データ　データ分類カテゴリ

#	カテゴリ名	内容説明	対象データの具体例
1	映像音声	個人識別可能なカメラ映像、マイク音声など	宅内モニタ映像、ドアホン集音、エアコン熱画像
2	健康情報	体重や血圧など、個人の健康データ	体重計計測値、血圧計計測値
3	扉窓開閉状態	住宅開口部の開閉状態が判るデータ	窓センサ、電子錠開閉状態
4	生活リズム	宅内での生活行動が判るデータ	炊飯器予約時間、トイレ人感センサ
5	在不在状態	住人の在・不在が判るデータ	冷蔵庫開閉、照明ON/OFF
6	生活志向	衣食住の生活スタイルや嗜好が判るデータ	電子レンジメニュー選択、湯温設定
7	家族構成	住人の人数や子供の有無などが判るデータ	チャイルドロック、洗濯機メニュー
8	地域特定	住居の場所（地域）が特定できるデータ	室外気温、電波状態（SSID）
9	故障診断	機器そのものの状態が推定できるデータ	モータ回転数、機器内部温度
10	個体特定	個別の機器を特定できる情報	IPアドレス、MACアドレス

2.2.2. データ分類カテゴリの考え方

前記データ分類カテゴリは対象となるスマートホーム IoT データによって、利用者のどのようなプライバシー情報を知り得るかという観点でカテゴリを定義している。

例えば、対象データの具体例に記載されている照明 ON/OFF では、この照明が室内灯であれば、ON/OFF をした際にそこに人が存在していること、またその操作履歴の蓄積データからは不在の可能性が高い時間帯等の算出が可能となることから、カテゴリは”在不在状態”と分類している。同じ照明器具の ON/OFF 情報においてもトイレに設置された照明器具の ON/OFF データであれば、ON/OFF 操作時間帯に人が存在していただけでなく、生活リズムや疾患の可能性等も分かり得る可能性が出てくる。また、単独のスマートホーム IoT データだけでは無く、複数のスマートホーム IoT データを組み合わせて加工分析することによっても、異なる種類のプライバシー情報を知り得る可能性があることにも留意する必要がある。

このようにスマートホーム IoT データから知り得るプライバシー情報は、具体的な対象データやそのデータが収集される頻度や期間、データをどのように加工するかと合わせて考慮する必要がある。スマートホーム IoT データを取り扱う事業者は、上記の 10 種類のカテゴリを参考としながら、利用するスマートホーム IoT データからどのようなプライバシー情報がわかり得るのかを十分に熟慮した上で、プライバシー保護のために必要な取り組みを行うことが求められる。

2.2.3. スマートホーム IoT データの利用目的カテゴリ

本ガイドラインではスマートホーム IoT データの利用目的を以下の 8 つのカテゴリに分類した。本カテゴリは本ガイドライン作成時に想定される利用目的でカテゴリを作成しており、今後の関連法の改正や国際情勢等の要因からカテゴリの追加や更新を必要とすることが考えられる。

表 3. スマートホーム IoT データ利用目的カテゴリ

	#	カテゴリ名	内容説明	具体利用事例
第三者提供無	一	申込サービス提供	利用者が申し込んだサービス提供のため	出先での遠隔確認・制御
	二	カスタマサポート	不具合などが発生した場合の対応のため	修理時の故障原因分析
	三	開発・分析	製品開発や、マーケティング分析のため*1	バグ解析
	四	関連プロモーション	当該製品そのもの、および関連する宣伝のため	調理器具用食材の推奨
第三者提供有	五	申込サービス提供	利用者が申し込んだ連携サービス提供のため	電気ポットの駆けつけサービス
	六	法に基づく例外	裁判所命令などによる開示	犯罪捜査のため
	七	開発・分析	関連製品の開発や、マーケティング分析のため*2	冷凍食品の消費分析
	八	関連プロモーション	当該製品のデータに基づく、第三者による宣伝のため	広告目的での第三者販売

(*1) ：仮名加工情報としての取り扱いを想定する
(*2) ：統計化情報または匿名加工情報としての第三者提供を想定する

2.2.4. 利用目的カテゴリの考え方

利用目的カテゴリは収集したスマートホーム IoT データをどのようなタイプの目的で利用するかについて、利用者から見てスマートホーム IoT データの利用目的が推定しやすいかどうか、さらにその利用目的が妥当と判断しやすいかどうかという観点から分類したものである。本カテゴリの策定意図は、同じスマートホーム IoT データであっても利用目的が異なれば利用者にとってデータ提供の受容性は大きく異なるためである。

例えば、掃除機の使用データを故障検知や適切な省エネ動作のためにデータ提供をするということと、第三者による出張掃除サービスのプロモーションを行うためにデータを提供することでは、利用者の受容性は異なっている。

このように利用目的によってデータ提供に係る利用者の受容性は大きく異なることから、収集するスマートホーム IoT データがどのようなプライバシーに関する情報がわかり得るのかということと合わせ、どのような目的でスマートホーム IoT データを利用するのかといった両面からの判断が必要になる。スマートホーム IoT データを取り扱う事業者は、当該スマートホーム IoT データの分類カテゴリに照らして、提示した利用目的で当該スマートホーム IoT データを利用した場合に、利用者が当該利用をどう捉えるかを考慮し、同意取得の方法、同意取得にあたっての説明内容等を判断する必要がある。

2.3. スマートホーム IoT データの取り扱い

スマートホーム IoT データを取り扱う事業者はそのスマートホーム IoT データから知り得るプライバシー情報や、利用者に示した利用目的に応じて適切にスマートホーム IoT データを取り扱う必要がある。本ガイドラインではその取り扱いについて、前節で述べたデータ分類カテゴリおよび利用目的カテゴリにあわせて、スマートホーム IoT データを取り扱う事業者が行うべき内容を利用者に対して行う説明・同意および自己コントロール性の観点から、対応上の代表的なケースとして取りまとめた。各ケースにおいて事業者が守るべき具体的なルールの内容は 5 章以降で記載する。なお、実際のプライバシーポリシーでは、複数のカテゴリに分類されるスマートホーム IoT データに対して、同じく複数のカテゴリに属する利用目的で利用することが想定される。このため、具体的なスマートホーム IoT データの内容、およびその利用目的に対して、実際にどのような説明や、同意の取得、自己コントロール性の提供を行うかは、本節で示した代表的なケースを参考として、各事業者にて判断頂きたい。

A）対象データと利用目的の関係性が判りやすいケース

例えば、照明の ON/OFF データを用いて、外出先での消し忘れ確認や、防犯用途で帰宅前に照明を点灯しておくようなケースである。対象データの内容とその利用目的が、一般の利用者にも想像しやすく、そのスマートホーム IoT データを利用することが自明である場合が該当する。

このケースを基本として、以降のケースでは説明や同意の取得、自己コントロール性の提供について注意すべき事項を記載していく。

B）対象データと利用目的の関係性が判りにくいケース

例えば、冷蔵庫の電力消費量を長期間にわたって収集して分析することで故障の予兆を検知し、電子メールなどを通じて点検や買い換えを促すケースである。一般の利用者にとっては、収集するスマートホーム IoT データの内容と利用目的との関係性が想像しにくい場合が該当する。

このようなケースでは、対象データと利用目的の関係性について、プライバシーポリシーの中で説明することが求められる。特に、複数の対象データを用いる場合や、収集が高頻度な場合、長期間にわたって収集する場合、対象データを加工分析する場合には、対象データの種類・収集頻度・収集期間・加工分析方法などを説明する必要がある。

C）対象データそのものがプライバシーに注意を要するケース

例えば、ベビーモニターのカメラ映像や、体重計での計測値など、個人に直接紐付きうるスマートホーム IoT データでプライバシーに注意を要するケースである。単体データとして注意を要するケースだけでは無く、収集の頻度や期間、加工の方法などによっても、プライバシーに注意を要する場合がありうる。

このようなケースでは、収集の対象となるスマートホーム IoT データや、加工の結果得られる情報をプライバシーポリシーに明記することが必要となる。また、利用者が十分に理解した上でスマートホーム IoT データを収集することが必要である。さらに、利用者がプライバシーに大きく影響すると感じるスマートホーム IoT データが収集された場合に、後からでも削除ができるような自己コントロール性を提供していくことも必要となる。

D）想定しにくい利用目的で対象データを利用するケース

例えば、プロモーションや広告用途など、利用者によっては対象データを利用して欲しくないと感じる利用目的に対象データを利用するケースである。家電機器・住設機器本来の機能には直接関連しない利用目的であって、利用者にとって想定しづらい利用目的である場合が該当する。

このようなケースでは、利用者が利用目的を十分に理解した上でスマートホーム IoT データを利用するために、分かりやすい説明を提供することが必要である。また、利用目的を誤解して同意してしまうことや、実際に利用する中で不満を感じることも想定されるため、後からでも当該利用目的のために対象データの利用を停止できるような自己コントロール性を提供していくことも必要となる。

E）対象データを第三者に提供するケース

例えば、電気ポットの利用状況を第三者であるサービス事業者に提供し、利用者の体調不良が疑われる場合にはサービス事業者が自宅まで駆けつけるサービスを提供するケースである。利用目的の内容如何に関わらず、対象データを個人識別が可能な状態で第三者提供する場合に該当する。

このようなケースでは、プライバシーポリシーにおいて、提供先の第三者の名称、提供するスマートホーム IoT データの内容、提供先での利用目的を明確化することが求められる。また、利用者が十分に理解した上で第三者提供を始めるために、明確な同意を取得することが必要となる。

2.4. 留意点

本ガイドラインでは IoT 家電などから収集されるスマートホーム IoT データにおける状況を勘案して取り扱いルールを策定しており、一部のルールについては、個人情報に該当するスマートホーム IoT データに対しても有益に適用することができる。具体的には、以下の各項目については、個人情報保護法を遵守することを前提として、本ガイドラインで定める取り扱いルールに従う必要がある。

- 5.1 節（同意の取得）、5.2 節（用語の説明）、5.3 節（対象データの説明）、5.4 節（利用目的の説明）における、説明項目として記載すべき内容の粒度
- 5.1 節（同意の取得）における、同意取得の対象者に関する注意事項
- 6.1 節（同意取得方法）における、IoT 機器のユーザインタフェースに応じた同意取得の方法
- 6.2 節（同意取得を考慮する必要のあるタイミング）について、データ収集開始時、および追加データの収集開始時における同意取得の推奨

3. スマートホーム事業者に求められる取り組み

スマートホーム市場においては、前章で説明したスマートホーム IoT データを活用し、様々なサービス開発等が行われ、利用者に提供されることが想定されるが、スマートホーム IoT データのデータライフサイクルは以下の**図 1** のようになる。

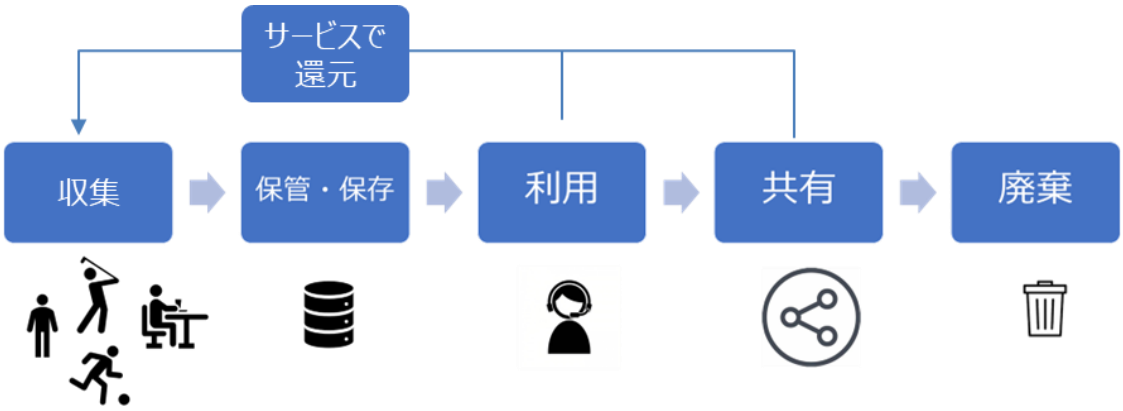

図 1 スマートホーム IoT データのデータライフサイクル

利用者が IoT 機器を利用することでスマートホーム IoT データが取得され、スマートホーム事業者はこれを保管・保存した上で利用し、また必要に応じて関連する他のスマートホーム事業者に共有する。このスマートホーム IoT データの利用や共有を通じて、利用者にはサービスとして還元される。最終的にスマートホーム IoT データが不要となった段階で廃棄される。

しかしながら、利用者の立場に立つと、日々の日常生活や機器の稼働情報をデータ化し、スマートホーム事業者に提供していくことになるため、どのようなデータが収集され、そのデータが何に利用されるのか、また、自らのデータが適切に管理されているかどうかを不安に感じてしまう。

また、スマートホーム IoT データの利用目的や利用方法について理解をしたとしても、一方的にスマートホーム IoT データが収集されてしまえば、スマートホーム事業者への不信感を募らせてしまうことにもつながる。

さらに、スマートホーム事業者がスマートホーム IoT データを収集した後にも、利用者のスマートホーム IoT データの利用状況について、しっかりと知る方法が担保されなければ、スマートホーム事業者に対して不満を感じることにもなる。

以降、本ガイドラインの 5 章から 7 章では、利用者からの不安・不信・不満といった“不”の部分を解消し、スマートホーム事業者が利用者からの信頼を確保するうえで、必須の項目となりうるスマートホームIoTデータに関する説明・同意取得・自己コントロール性の在り方について説明をしていく。

スマートホーム事業者は、利用者の日々の暮らしのデータを扱うことから、法令遵守はもちろんのこと、利用者に配慮したデータ管理やガバナンス体制の構築が必要となってくる。

4. 代表的な利用目的の分類

本ガイドラインの第二部で具体的なルールを示す前に、本章ではスマートホーム IoT データの代表的な利用目的について分類する。

4.1. 本来サービスのためスマートホーム IoT データを利用するケース

2.2.3 節で示した利用目的カテゴリの中で「一」に相当するケースである。

機器のパンフレットや取扱説明書、スマホアプリの概要説明などで謳われる本来サービスのためにスマートホーム IoT データを利用するケースである。例えば、エアコンの消し忘れを外出先から確認したり、逆に帰宅前に暖房・冷房機能を動作させて快適な状態にしたりなど、利用者本人やその家族のためにスマートホームの住空間としての安全性・快適性を高めるためのサービスが該当する。このケースでは、利用者が予めサービス内容に納得したうえでサービスを開始することが想定されるため、当該サービスを提供するためにスマートホーム IoT データを利用することに対する受容性は高いと考えられる。ただし、サービス内容を十分に理解せず、または誤解して利用を開始してしまうことも考えられるため、注意が必要である。

4.2. 連携サービスのためスマートホーム IoT データを提供するケース

2.2.3 節で示した利用目的カテゴリの中で「五」に相当するケースである。

機器のパンフレットや取扱説明書、スマホアプリの概要説明、第三者が提示するサービスのパンフレットや契約書などで謳われる本来サービスであるが、サービス提供のために第三者へのスマートホーム IoT データ提供が必要となるケースである。第三者としては、警備会社などの一般民間企業に加えて、医療機関や介護施設、地方自治体などがありえる。これらの第三者にスマートホーム IoT データを提供することにより、IoT 家電機器や住設機器などだけでは提供できない、実世界での見守りサービスや医療・健康サービス、行政サービスなどが提供される。

このケースでも、利用者が予めサービス内容に納得した上で利用を開始すると想定されるため、第三者提供を伴わない場合と同様に、スマートホーム IoT データの利用に対する受容性は高いものと考えられる。

4.3. カスタマサポートのためスマートホーム IoT データを利用するケース

2.2.3 節で示した利用目的カテゴリの中で「二」に相当するケースである。

機器に関する利用者からの問い合わせ対応、故障時の修理対応のためにスマートホーム IoT データを利用するケースである。実際に質問事項や不具合が発生するまでは、スマートホーム IoT データを利用することの必要性が判りにくいため、スマートホーム IoT データの利用について懇切丁寧な説明が必要となる。

4.4. 内部での開発・分析のためスマートホーム IoT データを利用するケース

2.2.3 節で示した利用目的カテゴリの中で「三」に相当するケースである。

スマートホーム IoT データは、本来サービスやカスタマサポートのように利用者自身へのサービス提供のために利用するだけではなく、IoT 機器のメーカやサービス提供事業者が、機器やサービスを改善していくためにも利用される。また、内部での分析結果は、利用者個々人を対象とするサービスとしてではなく、広く一般を対象としたマーケティング用途に利用されることもありうる。

内部での開発・分析のためにスマートホーム IoT データを利用する場合には、必ずしも特定の個人を識別する必要性はない。このため、スマートホーム IoT データが個人情報保護法で定める個人情報ではない場合には、製品・サービスの向上のための内部利用のみであることを前提として、スマートホーム IoT データの利用に対する受容性は比較的高いと考えられる。ただし、事業者での内部での開発・分析だけのためにスマートホーム IoT データを収集することは望ましくはなく、利用者自身に価値を還元するサービスを提供することが望ましい。

4.5. 第三者の開発・分析のためスマートホーム IoT データを提供するケース

2.2.3 節で示した利用目的カテゴリの中で「七」に相当するケースである。

事業者内での開発・分析だけではなく、IoT 機器から収集されるスマートホーム IoT データは、その IoT 機器に関係する商品の開発・分析のためにも有用なケースがある。例えば、電子レンジなどの調理家電であれば、冷凍食品などの食料品の開発/分析のために、スマートホーム IoT データを利用することが想定される。

このようなケースでは必ずしも特定の個人を識別する必要性や IoT 機器一台毎のスマートホーム IoT データを提供する必要性はない。このため、事業者内部でも提供先においても、特定の個人が識別できないように匿名化されたデータや、多数の IoT 機器から得られたスマートホーム IoT データを統計化したデータとしての提供で十分である。

4.6. 関連プロモーションのためスマートホーム IoT データを利用するケース

2.2.3 節で示した利用目的カテゴリの中で「四」に相当するケースである。

スマートホーム IoT データは、その収集対象となる IoT 機器に関連する消耗品や補修部品、新規サービスのプロモーションに利用されることもあり得る。さらには、収集対象となる IoT 機器のみならず、同一事業者内の他の IoT 機器やサービスのプロモーションにも利用されうる。また、場合によっては他の事業者からの委託を受けて、特定の IoT 機器やサービスの利用者向けにプロモーションを行うことも想定される。この際のプロモーションとしては、特定の機器やその機器を利用する個人を対象とした、いわゆるターゲティング広告となることもある。なお、他の事業者からの委託を受ける場合も含めて、プロモーションの主体者はスマートホーム IoT データを収集する事業者であり、スマートホーム IoT データの管理や利活用に関する責任は当該事業者が負うこととなる。

スマートホーム IoT データを利用することで、事業者にとっては、効果の高いプロモーションが実施できる。一方で利用者にとっては、有益な情報提供として捉えられるケースもあれば、必要性を感じられない情報提供となることもありえる。

4.7. プロモーション用途で第三者にスマートホーム IoT データを提供するケース

2.2.3 節で示した利用目的カテゴリの中で「八」に相当するケースである。

事業者内でのプロモーション用途での利用だけではなく、利用者の同意のうえでスマートホーム IoT データを第三者に提供し、第三者がプロモーション用途に利用するケースも想定される。特に、第三者が保有する別のデータと、特定の IoT 機器から収集されたスマートホーム IoT データが統合して利用されるケースも想定される。これらのケースでは、プロモーションの主体者は第三者であるが、スマートホーム IoT データの管理や利活用については提供元の事業者と提供先の第三者の双方の共同責任となる。

提供を受ける第三者側では、スマートホーム IoT データを利用することで、効果の高いプロモーションが期待される。一方で利用者にとっては、例え一度は同意していたとしても第三者から提供される他のサービスがない場合やあってもメリットが不十分な場合には、第三者によるスマートホーム IoT データの利用に疑問を抱かせることとなる。

4.8. 個人情報保護法に準じて例外的に第三者提供するケース

2.2.3 節で示した利用目的カテゴリの中で「六」に相当するケースである。

個人情報の場合には、裁判所の命令に基づく場合や、人の生命、身体や財産保護のために必要があって同意の取得が困難な場合など、個人情報保護法の定めに応じて例外的に第三者提供が認められるケースがある。スマートホーム IoT データについても同様の対応が想定される。

なお、たとえプライバシーポリシーに本利用目的を記載していたとしても、スマートホーム IoT データを開示することによって、プライバシー侵害を引き起こすこともある。実際にスマートホーム IoT データを提供するにあたっては、法務関係者や弁護士に相談するなど、十分な注意を払うべきである。

第二部：具体ルール

第二部ではスマートホーム事業者に求められる具体ルールについて記載していく。その際に、本ガイドラインとして必須と考える要件については「必要である」または「必要がある」と記載する。必ずしも必須ではないが、本ガイドラインとして推奨する要件については「望ましい」と記載する。また、本ガイドラインとしての禁止事項については「してはならない」と記載する。

表 4. 本ガイドラインにおける要件の表記

記載方法	要件の対応条件
必要である 必要がある	本ガイドラインとして、記載されている要件への対応を必須とする（shall）
望ましい	本ガイドラインとして、記載されている要件への対応を推奨とし、事業者に判断を委ねる（should）
してはならない	本ガイドラインとして、記載されている禁止事項に対応しないことを必須とする（shall not）

なお、推奨する要件に関する対応の是非は各事業者において判断する事となる。その際には、利用者観点でのプライバシーリスク評価が肝要であり、そのリスクが高いと判断する場合には推奨要件にも対応するべきである。プライバシーリスク評価については、8.3 節を参照されたい。万が一、利用者のプライバシーが侵害される事態となった場合には、1.3 節でも述べたように、損害賠償請求や差し止め請求が起きうることも判断の際には念頭におくべきである。

5. 通知・公表・説明に関するガイドライン

スマートホーム IoT データを取り扱う事業者は、どのようなデータを、どのように取得して、どのような目的に利用するかを、データのライフサイクル全般にわたって通知・公表・説明し、原則として同意を得た上で利活用する**必要がある**。本章では、説明事項として最低限記載すべき項目と、内容説明として最低限満足すべき記載粒度についてのガイドラインを記載する。記載すべき項目としては、①同意の取得、②用語の説明、③対象データの説明、④利用目的の説明、⑤業務委託、⑥共同利用の6項目である。

5.1. 同意の取得

スマートホーム IoT データの収集において同意を取得する場合に、プライバシーポリシーなどでの説明が必要となる内容・項目について記載する。

「1.4　ガイドラインの活用方法」に記載の通り、スマートホーム IoT データを利用者から収集する場合には、原則として事前に利用者による同意を取得するオプトイン方式であることが**必要である**。なお、6.1 節で論じるとおり、同意ボタンのクリックや同意する旨の署名等の典型的な場合以外にも、利用者の行為がオプトインの同意として認められる場合がある。

スマートホーム IoT データとして収集する情報とその利用目的については、できる限り具体的に、その情報に関して特定できるように箇条書きなどで説明し、利用者が同意して良いかを適切に判断できる情報にする**必要がある**。5.3 の対象データの説明、5.4 の利用目的の説明を参照されたい。例えば、空調機が機器の制御に利用しているセンサー情報であれば、空調機の室外機の外気温情報を長期間収集・分析することにより、室外機の設置された地域の地理情報を類推して活用できる可能性があるが、そのようなスマートホーム IoT データを活用する場合には、収集したスマートホーム IoT データの活用方法について利用者に説明することが求められる。

通知・説明・公表する場所は、製品の取扱説明書、スマートフォンアプリのトップページ、利用者が最初に到達する Web ページなどスマートホーム IoT 機器の利用者が、その内容について適切に確認できる場所に記載することが**必要である**。

また、スマートホーム IoT データは個人情報保護法にいう「個人関連情報」に該当する場合があるため、第三者提供においては、個人情報に該当しないスマートホーム IoT データであっても提供先において、他の情報と突合することにより個人情報になることが想定されるスマートホーム IoT データについては、個人情報保護法に従った対応が**必要である**。例えば、図 2 に示すように、エアコンのセンサー情報と空気清浄機のセンサー情報を組み合わせることにより「個人情報を推定可能」と判断する場合には、A 社でのデータ利用に対する利用者からの事前同意をもって、センサー情報を利用する必要がある。また、B 社は A 社へのスマートホーム IoT データの提供にあたって、A 社が個人情報を推定するかどうかを確認し、A社が個人情報を推定する場合には、A 社に対するデータ提供について個人情報保護法に従った対応が求められる。

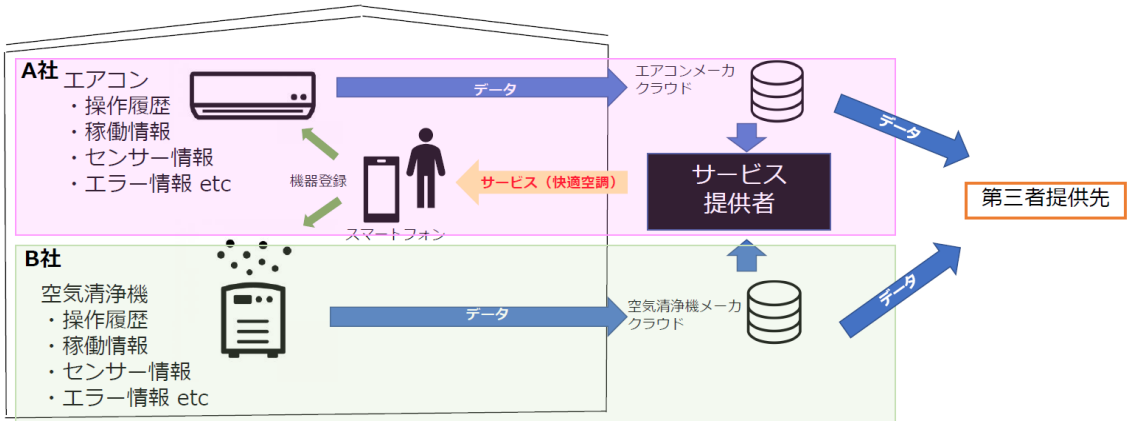

図 2 複数機器のデータによるプライバシー情報の推定

次に、事業者が同意取得を求める利用者の範囲について記載する。一人で利用するケースが多いスマートフォンとは異なり、テレビ受信機と同様に、スマートホーム IoT 機器はスマートホームに在住する世帯の構成員（家族、同居人など）が共用することが一般的である。このため、「放送分野の個人情報保護に関する認定団体指針」が示すように、代表となる利用者が世帯の構成員に対してスマートホーム IoT データが収集・利用されることを周知し了解を得る必要があることを代表となる利用者に注意喚起したうえで、代表となる利用者本人から同意を取得する必要がある。

なお、技術の高度化により、共用している機器のスマートホーム IoT データから世帯の構成員を識別し、収集したスマートホーム IoT データを利用して、個々の構成員を対象としたサービスや情報提供を行う場合には、構成員からの直接の同意取得やサービスの利用停止も必要である。

なお、同意取得の方法、タイミングとしては、Web サイトの参照や、スマートフォンアプリによる同意などの方法があるが、詳細は 6 章の同意取得に関するガイドラインに記載する。

5.2. 用語の説明

利用者に提示するプライバシーポリシーに記載する用語は、利用者がスマートホーム IoT データの扱いに関して、正しく理解するために必要であり、図などを用いて、わかりやすく記載することが望ましい。用語については、主に三種類の用語の解説が必要である。一つは技術的な用語に対する説明である。IoT は広く普及しているが、IT 技術者だけが理解できるような用語については、その収集されるデータの中身と、それによるデータの取り扱い方について明確化する必要がある。例えば、Cookie や IP アドレス、MAC アドレス、証明書シリアル番号などはその代表例であり、利用者はその仕組みまで理解する必要はないが、それによってどのようなスマートホーム IoT データが収集され、どのように利用されるかを、わかりやすく説明することが求められる。二つ目は、各企業独自に定義した機器のシリーズ名称や、機能名、サービス名称などに対する説明であり、利用規約の中で用いられる用語である。三つ目は、法律用語につ

いてである。同意取得の説明文の中に記載するケースは少ないが、例えば、仮名加工情報といった用語などについては、氏名等を削除した情報であり、他の情報と照合しない限り特定の個人を識別できないなど、補足した記載の仕方が求められる。

また、用語の解説に加えて、スマートホーム IoT データのフロー（入力から出力までの流れ）についても、図などを用いて説明することが望ましい。例えば、利用者による操作やセンサーによる IoT 機器でのデータ収集を起点として、クラウドへのアップロード、委託先や第三者提供先へのデータ提供、その先での利用者に対する IoT サービスとしての還元まで、データの流れとサービスの提供を説明することが求められる。

5.3. 対象データの説明

プライバシーポリシーでは、IoT 機器が取り扱うスマートホーム IoT データについて、これをリストアップして利用者に提示する必要がある。また、スマートホーム IoT データの利用方法によっては、どのようなプライバシーに対する影響が起きうるかが分かりにくいケースがある。例えば、ペットモニターの録画映像を外出先から確認するサービスを提供している場合には、宅内の様子というプライバシー情報がサービス事業者に収集されうることは一般の利用者にも自明である。一方で、日々のエアコンの動作状況から生活リズムにあわせた自動最適制御を行うサービスを提供している場合には、起床時間や就寝時間などの生活リズムがサービス事業者に収集されうることは一般の消費者には予想がつかないと考えられる。スマートホーム IoT データの利用方法に応じて、一般の利用者にも理解可能な表現で、二次加工データを含めて、プライバシーに対する影響が明確になるように記載する必要がある。

上記を実現するために、スマートホーム IoT データは以下観点に留意して記載することが求められる。

- **対象となるデータの内容を判りやすく記載すること**

2.2.1 節のスマートホーム IoT データのカテゴリ分類も考慮した上で、対象となるスマートホーム IoT データの名称を、一般の利用者にも判りやすい表現で記載する必要がある。

必ずしも詳細に個々のデータの内容を記載する必要は無いが、プライバシー影響度合いの異なるカテゴリ分類を跨がるような過度の大括りはしてはならない。例えば、生活リズムの特定に繋がるような人感センサーと、故障診断用途に利用する機器内温度センサーの両方を備える IoT 機器において、この両者を「センサーデータ」と大括りにするような記載は避けなければならない。

- **データ収集の方法を示すこと**

スマートホーム IoT データは、IoT 機器や対応するスマホアプリなどから様々な方法で収集される。また、収集されたスマートホーム IoT データは IoT 機器やスマホアプリ内部に留まることもあれば、サービス事業者の管理するサーバに外部送信されて管理されることもある。対象となるデータ毎に、以下に例示するようなデータ収集の方法に

ついて記載することが**必要である**。なお、以下の方法は網羅的なものではなく、各 IoT 機器の特徴に応じて適切な方法を記載することが**望ましい**。

- 利用者自身が、IoT 機器やスマホアプリで入力したデータ
- IoT 機器の製造時に予め付与されているデータ
- IoT 機器に備えられたセンサーが、自動的に収集したデータ
- 利用者操作のタイミングで、IoT 機器に備えられたセンサーが収集したデータ
- IoT 機器の内部動作ログデータ
- サービス事業者の管理するサーバに外部送信されるデータ

また、データの名称から自明なケースについては、必ずしもデータ収集の方法を明記する必要は無い。例えば、MAC アドレスは製造時に予め付与されているデータであることが明白なため、改めてデータの収集方法を記載する必要は無い。

- **データ収集の期間や頻度、精度を示すこと**

スマートホーム IoT データは、その収集期間が長期間にわたる場合や、頻度が極めて高い場合、高精度である場合には、そのプライバシーに対する影響も比例して高くなるケースが存在する。例えば、照明機器の ON/OFF データは、単独では単に在不在を示すだけの情報であるが、数週間単位で蓄積されれば、在宅時間の傾向を示す情報となり得る。また、例えば冷蔵庫の電力消費量も数分単位での計測であれば、在不在を示すような情報となり得る。精度についても、画像データが高精度になれば、虹彩や指紋、心拍数など個人に関わるバイタルデータが収集されうる情報となる。

このために、長期間にわたる収集や、頻繁な収集、高精度な収集でプライバシーに対する影響が高まる場合には、その期間や頻度・精度についても記載することが**望ましい**。

なお、必ずしも全ての対象となるスマートホーム IoT データに対して期間や頻度、精度を示す必要は無く、例えば利用者で入力されたデータについては、頻度が自明であることから明示的な記載の必要は無い。

- **どのようなプライバシー情報を知り得るか明確にすること**

2.2.2 節で例示したとおり、同じ機器からのスマートホーム IoT データであってもその設置場所や、収集頻度・蓄積期間によって、スマートホーム IoT データのカテゴリは変化しうる。また収集したスマートホーム IoT データをそのまま利用するのではなく、AI 処理などで加工して取り扱う場合にも、スマートホーム IoT データのカテゴリは変化しうる。

収集した原データをどのような機能を実現するために利用するのかに応じて、その際に知り得るプライバシー情報の内容について判るように記載する**必要がある**。なお、将来の機能追加や変更を想定して記載を行う必要は無いが、加工方法の追加や変更によって、従来と異なるカテゴリのプライバシー情報を知り得る場合には、同意の再取得が必要となるケースもある。詳細については、6.2.4 節を参照のこと。

また、IoT 機器の設置場所についてサービス利用仕様で想定する場所があるにも関わらず想定外の場所に設置する場合には、サービス提供事業者はプライバシーポリシ

ーなどで利用者への説明や注意喚起を行うことが望ましい。例えば、ペットの見守り用途で利用するペットモニターについて、脱衣所に設置するようなことがあれば、利用者本人が望まない映像情報が収集されることについて注意喚起を行うべきである。

5.4. 利用目的の説明

プライバシーポリシーでは、対象となるスマートホーム IoT データに関する説明とともに、その利用目的についても説明をすることが必要である。同じスマートホーム IoT データを利用するとしても、それを本来サービス目的で利用するのか、それともプロモーション目的で第三者に提供するのかによって、求められる説明内容は大きく異なる。なお、複数の利用目的がある場合には、プライバシーポリシーでは、その全てを記載することが必要である。

以下では、4 章で提示した利用目的の類型毎に、利用目的を記載するにあたって留意すべき事項を示していく。なお、本ガイドラインでの利用目的の類型は網羅的なものではなく、ここに記載されていない利用目的でスマートホーム IoT データを利用する場合には、プライバシー侵害にならないように十分に配慮した上で、類似のケースを参考としながら利用目的を適切に記載することが求められる。

5.4.1. 本来サービスのためスマートホーム IoT データを利用するケース

スマートホーム IoT データの利用に対する受容性は高いものと考えられ、利用者がスマートホーム IoT データの利用目的を理解できるように記載することが必要である。パンフレットなどで謳われている本来サービスの内容を簡潔に示し、この目的で利用することを利用者が理解できるように記載する。

なお、スマートホーム IoT データをそのまま利用するのではなく、AI 処理などで二次加工したうえで利用する場合には、スマートホーム IoT データとその利用目的の関係性が、一般の利用者には判りにくいケースも考えられる。このような場合には、AI 処理によって得られるプライバシー情報の内容について説明することなどで、スマートホーム IoT データと利用目的の関係性を明確化することが望ましい。

また、サービス内容を十分に理解せず、または誤解してサービス利用を開始してしまうこともありえるため、7.3 節で記載する利用停止に関する自己コントロール性を提供することも必要である。

5.4.2. 連携サービスのためスマートホーム IoT データを提供するケース

第三者提供を伴わない場合と同様に受容性は高いものと考えられ、利用者がスマートホーム IoT データの利用目的を理解できるように記載することが必要である。なお、第三者提供を伴うため、別途同意取得に関する記載（6.2.2 節）も参照のこと。また、5.4.1 節の場合と同様に不十分な理解や誤解に基づいて利用を開始してしまった場合に備え、第三者提供の停止を可能としておくことが望ましい。

5.4.3. カスタマサポートのためスマートホーム IoT データを利用するケース

実際に質問事項や不具合が発生するまではその必要性が判りにくいため、利用目的として具体的なカスタマサポートの内容について記載することが必要である。

5.4.4. 内部での開発・分析のためスマートホーム IoT データを利用するケース

特定の個人が識別できない方法で、内部での開発や分析のために利用することを説明する記載が必要である。

例えば、洗濯機の機能毎の利用状況分析結果に応じてテレビコマーシャルの内容を検討する場合には、利用状況を統計データとしてマスマーケティング用途に利用することの説明が求められる。

5.4.5. 第三者の開発・分析のためスマートホーム IoT データを提供するケース

特定の個人が識別できないように匿名化されたデータや、多数の IoT 機器からのスマートホーム IoT データを統計化したデータとして提供することを前提として、第三者側での開発・分析用途などのために第三者に提供することを説明する記載が必要である。なお、匿名化されたデータとして提供する場合には、提供される情報の項目について特定の個人が識別できない理由とともに説明する必要がある。

5.4.6. 関連プロモーションのためスマートホーム IoT データを利用するケース

単に利用目的としてプロモーション用途であることを記載するだけではなく、どのようなスマートホーム IoT データに基づいたどのようなプロモーションを実施するかを説明するための記載があることが望ましい。例えば、食品メーカからの委託を受けて、電子レンジで冷凍食品を温めた場合に、新製品の冷凍食品の広告を出す場合には、電子レンジの調理メニューの選択に基づいてプロモーションを行うとの説明が求められる。

収集されたスマートホーム IoT データに加えて、外部から第三者提供されたデータを特定の IoT 機器から収集されたスマートホーム IoT データと統合して利用する場合には、そこから読み取れるプライバシー情報のカテゴリも変わりうる。そのため、第三者提供されたデータを統合して利用する場合には、統合して利用することについても記載をしておく必要がある。なお、統合の結果読み取れるプライバシー情報の内容についても記載しておくことが望ましい。

5.4.7. プロモーション用途でスマートホーム IoT データを提供するケース

単に利用目的としてプロモーション用途で第三者に提供することを記載するだけではなく、どのような第三者に対して提供するのか、どのような種類のスマートホーム IoT データを提供するのか、について記載することが必要である。また、スマートホーム IoT データを AI 処理などで二次加工した情報を提供する場合には、その二次加工によって得られるプライバシー情報の内容について記載することも必要である。なお、第三者提供を伴うため、別途同意取得に関する記載も参照のこと。

5.4.8. 個人情報保護法に準ずる例外的な第三者提供

必ずしも個人情報とはならないスマートホーム IoT データであったとしても、プライバシーポリシーにおける利用目的として、個人情報保護法に準じて例外的に第三者提供する可能性を記載しておくことが望ましい。

5.5. 業務委託

他社に業務委託をする際には、各種の情報を適切に取り扱うよう、委託先企業名、委託するスマートホーム IoT データの内容などを明確にした二者間契約を締結する必要がある。二社間での委託契約書においては、委託元名・委託先名、委託するスマートホーム IoT データの内容、守秘義務、漏洩時の責任・保証など、委託先が負うべき義務について明確に規定することが必要である。

プライバシーポリシーでは、業務委託に関する状況について、利用者に説明することが望ましい。

5.6. 共同利用

個人情報保護法における個人情報の共同利用と同様に、利用者から得る情報を自社以外の事業者と共同利用する場合は、共同利用されるスマートホーム IoT データの項目、利用する事業者、利用目的等（共同利用事項）をあらかじめ、利用者に通知し、又は利用者が容易に知り得る状態に置くことを記載する必要がある。共同利用事項は次のとおりである。

- スマートホーム IoT データの項目
- 共同利用する者(=企業)の範囲
- 共同利用する目的
- 共同利用する情報の管理について責任を有する者の氏名又は名称及び住所（法人の場合はその代表者の氏名）
- スマートホーム IoT データの収集方法

個人データの共同利用の場合、法により本人の同意が要求されないのは（個人情報保護法 27 条 5 項）、本人から見て、当該個人データを提供する事業者と一体のものとして取り扱われることに合理性がある範囲で、当該個人データが共同して利用されるからである。したがって、共同利用者として認められるのは、グループ企業や親子会社といった客観的な一体性のある範囲に限られる。この点はスマートホーム IoT データの共同利用においても同様である。共同利用事項を通知し又は容易に知り得る状態に置く方法等の手続きは、個人情報保護法の共同利用に準じるものとする。

共同利用に関しては、予め明記された企業が共同して適切なデータ管理について、責任をもって行うことが前提となる。

共同利用に関しては、参加する企業の列挙の仕方、撤退時/企業統合時など共同利用者の状況変化が起きた場合のスマートホーム IoT データの扱い、責任についても明確にしておくことが望ましい。

5.7. その他留意事項

ISO/IEC29184（オンラインでのプライバシーに関する通知と同意）に従って考慮すべき内容として下記に列挙する。

① 言語

日本語による記載だけではなく、国内に居住されているスマートホーム IoT 機器を利用する日本語以外の母国語を使われる方にも通知、同意を求めている内容について理解できるよう複数の言語で記載（表示）することが望ましい。

② アクセシビリティ

加齢による影響を含む様々な種類の視覚障がいを持つ利用者を考慮し、文字の大きさ、文字色などについて配慮すべきであるが、さらに進んだ考え方として、音声による案内などがあってもよい。

③ データの所在

スマートホーム IoT データを保管、利用する地理的位置及び法域について、収集したスマートホーム IoT データが国外に送信、蓄積され、国外で利用される場合や、国内で収集したスマートホーム IoT データを海外に移転する場合など、国、法域を超える場合には、利用者に通知することが望ましい。

また、総務省の「プラットフォームサービスに関する研究会　中間とりまとめ （令和 3 年 9 月） https://www.soumu.go.jp/main_content/000769270.pdf」には、通知・同意取得にあたっては、「サービスの利用タイミングに合わせたタイムリーな通知」が利用者の理解や安心に資する工夫として記載されている。

サービスの利用開始時・アカウント作成時における通知とは別に、適宜利用者が認識しやすいタイミングで通知（ポップアップ、プッシュ通知等）を行うといった工夫をすること、さらに、利用者が同意した内容を確認することや、同意の撤回を容易にするためのプライバシー設定の工夫も有効であり、こういった工夫は同意取得に関する将来的にあるべき姿である。

図 3 は、**図 1** で示したスマートホーム IoT データのライフサイクルにおいて、どのタイミングでタイムリーな通知を行うべきかを概念的に示したものである。サービスの利用を開始し実際にスマートホーム IoT データを収集する前に説明を行うだけではなく、サービスでの還元時に適宜収集データの内容やその利用目的について注意喚起を行うことや、廃棄の際にスマートホーム IoT データの取り扱い内容について重ねて説明することが望ましい。

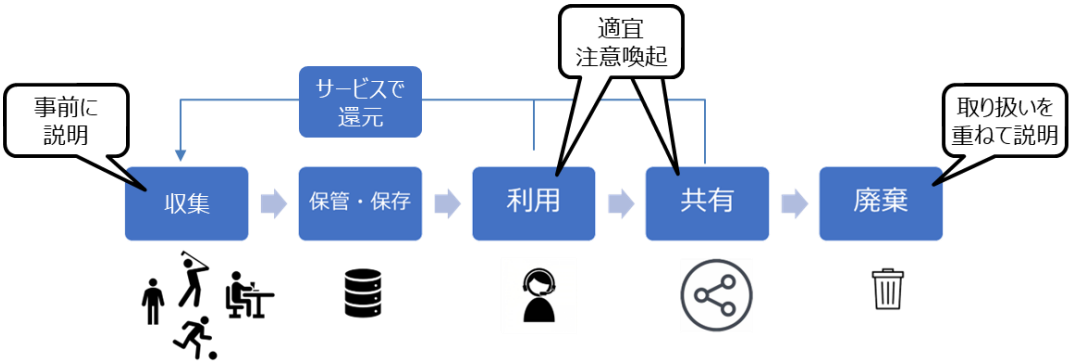

図 3 サービスの利用タイミングに合わせたタイムリーな通知

6. 同意取得に関するガイドライン

5 章で示したとおり、スマートホーム IoT データを取り扱う事業者はプライバシーポリシーなどでスマートホーム IoT データの取り扱いについて説明し、原則として同意を得ることが求められる。本章では、個人情報ではないスマートホーム IoT データを取り扱う事業者が、どのような場合に同意取得を考慮するべきであり、各事業者において同意取得する判断を行った場合には、どのような方法で取得するべきかについて、ガイドラインを記載する。

同意が有効であるためには、1) 同意が強制されておらず自由性・任意性がある、2) データの利用目的が特定されている、3) 5 章記載のガイドラインに従って十分に説明されている、4) 同意の行為が明確である、ことが求められる。

同意取得に関しての最終決定は事業者が行うものであるが、各事業者においては、収集するスマートホーム IoT データが、2.2.1 節に示したデータの類型から見てプライバシーに対する影響が高い情報になるかどうかや、4 章で考察した利用目的の類型、その他事業者の利用者への情報提供方針、法令遵守の観点を十分に考慮したうえで、同意取得の必要性及びその同意取得方法やタイミングを判断することが求められる。本章では、個人情報ではないスマートホーム IoT データを取り扱う事業者が、同意取得の同意取得方法やタイミングを選択するためのガイドラインを記載する。

6.1. 同意取得方法

同意の取得方法には、契約文書へ署名する最も確実な方法から、シュリンクラップ契約のような封を破いて取り出した時点で契約に同意したとみなす本用途としては不適切な方法まで、いくつかのレベルが存在する。

本ガイドラインでは以下の表に示すように、IoT 機器のユーザインタフェースに応じて考えられる同意取得方法の例をリストアップし、①明確な意思確認を行う同意、②自然な操作の流れの中での同意、③不適切な同意取得方法の三段階にレベル分けを行った。

表 5.　同意取得方法の例とレベル分け

#	プライバシーポリシーの提示方法	同意の取得方法	レベル
1	販売前に契約書などの一部として書面で提示	書類に対して署名	①明確な意思確認を得る同意
2	機器が持つ or 接続されるディスプレイで提示	チェックボックスにチェックした上で、同意ボタン押下	
3	対応するスマホアプリで提示	チェックボックスにチェックした上で、同意ボタン押下	
4	機器に同梱される取扱説明書などで提示	説明書記載の特定操作を実施	
5	機器が持つ or 接続されるディスプレイで提示	機器の指示に従ってネットワーク接続	②自然な操作の流れの中での同意
6	機器が持つ or 接続されるディスプレイで提示	単純な同意ボタン押下	
7	対応するスマホアプリで提示	スマホアプリの指示に従ってネットワーク接続	
8	対応するスマホアプリで提示	単純な同意ボタン押下	
9	機器に同梱される取扱説明書などで提示	説明書の記載に従ってネットワーク接続	
10	機器に同梱される取扱説明書などで提示	電源を投入（ネットワークは自動的に接続）	③不適切な同意取得方法
11	外箱などに印刷	開封	

① 明確な意思確認を得る同意

表5中の1から4は、書面や IoT 機器のディスプレイ、スマートフォンのアプリケーション等にプライバシーポリシーを提示し、それに対する明確な意思確認を行う同意取得方法である。本ガイドラインでは、これらの同意取得方法を、利用者がプライバシーポリシーを理解したうえで、明確な意思をもって同意したと考えられるものとしてレベル分けを行った。尚、2、3、の方法は、ユーザインタフェースの性質上、事前の同意取得だけでなく変更時の同意取得にも適用可能であるが、1、4の方法は、事前の同意取得のみに適用可能である。

なお、4 については、取扱説明書などにおいて、プライバシーポリシーを提示する箇所と、機器の特殊操作を説明する箇所を隣接しておく必要がある。また、特殊操作については、例えば特定の 5 つのボタンを予め定められた順番で押下したうえでそのうちの 3 つのボタンのみを 10 秒以上押下するなど、通常の利用では起こりえない操作とすることが必要である。

② 自然な操作の流れの中での同意

表中の5から9は、IoT 機器のディスプレイやスマートフォンのアプリケーション、取扱説明書等にプライバシーポリシーを提示し、単純な同意ボタンの押下や IoT 機器のネットワーク接続設定を行う操作により同意取得を行う方法である。本ガイドラインでは、これらの同意取得方法を、プライバシーポリシーを提示したうえで、IoT 機器の自然な操作の流れの中で同意が取得されるものとしてレベル分けを行った。ただし、ネットワーク接続によってスマートホーム IoT データの収集が始まることが、プライバシーポリシーでの説明などを通じて一般の利用者にも十分に理解可能なことが必要である。理解可能であれば、明確な同意行為があったと見做すことができる。

例えば、天気予報表示機能付きのスマート室温計が、ネットワーク接続とともに天気予報の情報をダウンロードするだけではなく、プライバシーポリシーでの説明もなく計測した室温をサーバにアップロードしているとすれば、一般の利用者には理解困難と考えられる。

尚、6、8の方法は、ユーザインタフェースの性質上、事前の同意取得だけでなく変更時の同意取得にも適用可能であるが、5、7、9の方法は、ネットワーク接続をもって同意の意思表示とする方法のため、事前の同意取得のみに適用可能である。

③ 不適切な同意取得方法

表中の10、11は、取扱説明書や IoT 機器の外箱等にプライバシーポリシーを提示し、シュリンクラップ契約のように電源の投入や製品包装の開封をもって同意の意思表示とみなす方法である。本ガイドラインとしては、これらの方法は同意取得と見做してはならないと考える。このため、本ガイドラインでは、不適切なものとしてレベル分けを行った。

6.2. 同意取得を考慮する必要のあるタイミング

個人情報保護法が定める同意取得が必要な場合の内、第三者提供時、利用目的の追加・変更時、共同利用するデータ項目や共同利用する者の範囲の変更時について、本ガイドラインでは個人情報ではないスマートホーム IoT データにおいても、同意取得が**必要である**。加えて、データ収集開始時や後から追加でデータを収集する場合にも、原則として同意取得が**必要である**。

以下の表 6 に本ガイドラインで整理した、同意取得を考慮する必要のあるタイミングを示す。

表 6. 同意取得を考慮する必要のあるタイミング

#	タイミング	説明
1	データ収集開始時	機器をネットワークに接続して、データ収集を開始する前
2	第三者提供時	第三者に対してデータを提供する前
3	追加データの収集開始時	機器から新たな種類のデータを追加で収集開始する前
4	利用目的の追加・変更時	収集しているデータについて、その利用目的の追加・変更時
5	共同利用の変更時	データ項目や、共同利用する者の範囲を変更する場合

6.2.1. データ収集開始時

IoT 機器をネットワークに接続してスマートホーム IoT データの収集を開始する前に、原則として同意を取得することが**必要である**。

スマートホーム IoT データの収集タイミングでは、収集・利用が開始される前に本人の同意が得られることから、それに基づきスマートホーム IoT データの利活用を実施することが可能であるという特徴がある。

データ収集開始時の同意取得方法としては、**①明確な意思確認を得る同意**に分類される方法、**②自然な操作の流れの中での同意**に分類される方法が選択できる。

各事業者においては、対象となるスマートホーム IoT データの分類カテゴリ、その利用目的のカテゴリに応じて、適切な方法を選択する**必要がある**。

6.2.2. 第三者提供時

5.4.2 節に記載の連携サービスのためにスマートホーム IoT データを提供するケース、5.4.7 節に記載のプロモーション用途でスマートホーム IoT データを提供するケースにおいて、提供元で個人情報ではなく、提供先においても個人情報として取り扱わないスマートホーム IoT データを第三者提供するケースが該当する。

何れのケースにおいてもスマートホーム IoT データがプライバシーに配慮すべきデータであることを踏まえて、第三者に対してスマートホーム IoT データを提供する前に、同意を取得する**必要がある**。

各事業者において同意取得する判断を行った場合には、**①明確な意思確認を得る同意**に分類される方法で同意を取得することが**必要である**。

6.2.3. 追加データの収集開始時

IoT 機器から新たな種類のスマートホーム IoT データを追加で収集開始する前に、原則として同意を取得することが**必要である**。例えば、遠隔からの IoT 機器のアップデートによって、その IoT 機器から新たな種類のスマートホーム IoT データを収集する場合や、ある IoT 機器が他の機器から収集されるデータを後から連携して利用する場合等が該当する。

追加データの収集開始時の同意取得方法としては、**①明確な意思確認を得る同意**に分類される方法、**②自然な操作の流れの中での同意**に分類される方法が選択できる。

予め全ての収集データを想定したプライバシーポリシーをデータ収集開始前に提示できればよいが、そうではない場合に追加データの収集が必要となるため、変更時の同意取得が可能なユーザインタフェースを備えた同意取得方法で、同意を取得することが**望ましい**。

各事業者においては、対象となるスマートホーム IoT データの分類カテゴリ、その利用目的のカテゴリに応じて、適切な方法を選択する**必要がある**。

6.2.4. 利用目的の追加・変更時

スマートホーム IoT データがプライバシーに配慮すべきデータであることを踏まえて、収集しているスマートホーム IoT データの利用目的を追加・変更する際には、同意を再取得することが**必要である**。

利用目的の追加・変更については、個人情報保護法ガイドライン（通則編）に記載の通り、「変更後の利用目的が変更前の利用目的からみて、社会通念上、本人が通常予期し得る限度と客観的に認められる範囲内」であれば、必ずしも同意の取得は必要ではなく、通知または公表のみでの対応としてもよい。

但し、スマートホーム IoT データの利用方法として、収集データと利用目的の紐づけや、どのような分析を行うかといった収集データの分析方法についても利用目的の一部であり、収集データと利用目的の紐づけを追加・変更する場合や、収集データの分析方法を追加・変更する場合などが、利用目的の追加・変更となり得る可能性があることに注意されたい。特に、収集データの分析方法を追加・変更することで、収集した原データを用いて実現される機能が追加／変更され、その際に知りうるプライバシー情報のカテゴリが以前と異なるものとなる場合には、利用目的の追加・変更となる可能性が高い。また、スマートホーム IoT データの利用目的を変更する場合には、同意の再取得を得たあとに収集されたスマートホーム IoT データのみを新たな利用目的で利用することが**望ましい**。つまり、同意の再取得を得る前に収集したデータについても新たな利用目的で利用する場合には、提示する更新版のプライバシーポリシーで説明することが求められる。

各事業者においては、個人情報保護法ガイドライン（通則編）に記載の、社会通念上、本人が通常予期し得る限度と客観的に認められる範囲の変更かどうかを判断基準の参考とし、同意取得の適否を判断する**必要がある**。

各事業者において同意取得する判断を行った場合には、**①明確な意思確認を得る同意**に分類される方法で同意を取得することが**必要である**。この際には、収集データと利用目的の紐づけや収集データの分析方法についても、利用目的の記載の中で具体的に特定することが**望ましい**。

6.2.5. 共同利用の変更時

スマートホーム IoT データがプライバシーに配慮すべきデータであることを踏まえて、共同利用するデータ項目や、共同利用を行う者の範囲を変更する際には、同意を再取得することが**必要である**。

各事業者において同意取得する判断を行った場合には、**①明確な意思確認を行う同意**に分類される方法で同意を取得する**必要がある**。

7. 利用者の自己コントロール性の担保について

個人情報保護法で定める個人情報の場合には、開示請求、訂正・削除・追加請求、利用停止請求への対応が法律として定められている。これは、利用者が自身で自身の個人情報をコントロールできるようにすることによって、利用者が安心して個人情報を提供できるようにするためである。

個人情報と同様に、スマートホーム IoT データについても、自己コントロール性を提供することによって、利用者が安心してスマートホーム IoT データを提供できるようになるとの効果が期待できる。このため、事業者には、自己コントロール性を利用者に提供するとともに、その旨をプライバシーポリシーで記載することが**必要である**。

また、昨今ではダッシュボードと呼ばれる、自己コントロール性を一括して提供するためのユーザインタフェースが提唱されており、将来的にはダッシュボードを提供していくことが**望ましい**。

また、スマートホーム IoT データの開示・訂正や利用停止に加えて、利用者がサービス提供を必要としなくなった際は、会員としてのサービス利用を全面的に停止するサービス退会の機能を提供することも**必要である**。

7.1. スマートホーム IoT データの情報開示請求について

機器から得られるスマートホーム IoT データが個人情報保護法の対象外となるスマートホーム IoT データの場合でも、そのデータ提供元の個人からの請求があった場合には、原則として、対象データが個人情報である場合と同様に、個人に関わるスマートホーム IoT データを開示する**必要がある**。一方で、必ずしも個人情報保護法で定める個人情報ではないスマートホーム IoT データについては、例外を考慮すべき点もある。本節ではこのような例外について規定する。

7.1.1. 個人に関わる情報開示の条件確認について

個人情報に対して情報開示の請求があった場合には、その個人情報の中に含まれる氏名や住所など個人を識別可能な情報によって、請求者が本人であることを確認可能である。しかしながら、スマートホーム IoT データが個人情報でない場合などには、氏名や住所などによる本人確認を行うことができない。

このような状況であったとしても、各種請求への対応時には、機器・サービスの利用者”本人” であると確信するに足る技術的な確認が**必要である**。情報開示の際には、秘密鍵/証明書による機器認証や、ID/パスワードでの利用者認証で、スマートホーム IoT データの生成元となった機器やサービスの利用者”本人”であることを確認するなど、事業者各々の責任で対応する**必要がある**。

また、スマートホーム IoT 機器が利用者本人だけではなくスマートホームに在住する世帯の構成員の情報も収集している場合、情報開示の請求は世帯の構成員の情報を開示することとなる可能性があることから、世帯の構成員の了解を得たものであるかを利用者“本人”に対して確認することが**望ましい**。

7.1.2. 開示されるスマートホーム IoT データの範囲について

利用者より収集するスマートホーム IoT データの活用については、各種スマートフォン用アプリやサービスで提示している範囲での利用が多くを占める。このため利用者からの開示要求があったとしても、当該アプリやサービスでのデータ提示機能で対応可能な場合には、利用者に対してこれらの利用方法の説明を案内することで対応が可能である。

アプリやサービスでのデータ提示機能がない場合には、無償または必要な手数料を徴収した上で、請求者がデータ提供の”本人”であることを確認の上、書面または電子データで提供する事が望ましい。

なお、利用者が直接的に目に触れることがない機器内部動作ログについては、開示の対象外としても良い。ただし、利用者自身による操作や入力した内容については、内部動作ログに代わる代替データの提供等で開示請求に対応する必要がある。

また、個人情報保護法では、個人情報であったとしても、以下のケースに該当する場合には、必ずしも開示請求に対応する必要は無いと定められている。

- 本人又は第三者の生命、身体、財産その他の権利利益を害するおそれがある場合
- 当該個人情報取扱事業者の業務の適正な実施に著しい支障を及ぼすおそれがある場合
- 他の法令に違反することとなる場合

スマートホーム IoT データについても、上記のようなケースに該当する場合には、必ずしも開示請求に対応する必要は無い。

7.1.3. 第三者提供記録の扱いについて

スマートホーム IoT データについて、提供先で個人に紐付け可能な状態で第三者提供する場合には、提供先・提供内容などを含む第三者提供記録についても、スマートホーム IoT データそのものと同様に開示することが望ましい。

7.2. スマートホーム IoT データの訂正・追加・削除について

スマートホーム IoT データは機器操作履歴や各種センサーの収集データであり、その収集情報がリアルタイムにアプリ表示に反映されない等、一概に表示誤りとは言えない場合が発生する。このような場合、利用者からの逐一の訂正や追加要求に応じることが正しい対応とは言えないため、訂正・追加・削除請求への対応は特に本ガイドラインでは規定しない。

※個人情報保護法ガイドライン（通則編）に、「利用目的からみて訂正等が必要ではない場合、保有個人データが誤りである旨の指摘が正しくない場合には、訂正等を行う必要はない。」との記載があり、このケースに該当すると考えられる。

例えば、洗濯機の誤操作により「洗濯開始」が記録されるケースや、人感センサーの誤検出で「14:00 在宅」が記録されるケースなどが想定される。ただし、その場合も実

際に何等かの操作やセンサー反応がある場合、センシングデータとしては正しい情報である。このため、ガイドラインとしては利用者からの訂正、削除請求などに応じる表記は規定しないものとする。

ただし、機器誤操作やセンサー誤検出により、利用者の想定とは異なるスマートホーム IoT データが収集されるケースに備え、訂正・追加・削除機能の仕組みを提供することが**望ましい**。

また、サービスアプリケーションに機器状態表示機能を有する場合、収集したスマートホーム IoT データと、リアルタイムな表示との一致性等にずれが生じるなど、100%の精度が保証出来ない場合があることについて、利用者マニュアルなどで利用者への説明が必要なことは記載しておくことが**望ましい**。

7.3. サービスの利用停止について

利用者がスマートホーム IoT データを用いたサービスの利用が不要となった場合、その利用停止や会員からの脱会などが「容易に行える仕様」の提供が**必要である**。スマートフォンや本体表示画面などの操作仕様を策定する場合、その導線は「設定」「会員情報」等、わかりやすい名称のメニュー内に配置することが**望ましい**。その際、サービスの利用を停止することで、停止されるデータ送出やサービス内容も明確に利用者に伝えることが**必要である**。

なお、サービスの利用停止は、原則として機器・サービスの利用者”本人”から受け付けることが求められる。“本人”以外の世帯の構成員から利用停止を受け付ける場合には、“本人”の同意が必要である旨注意喚起する**必要がある**。但し、共用している機器のスマートホーム IoT データから世帯の構成員を識別し、収集したスマートホーム IoT データを利用して、個々の構成員を対象としたサービスや情報提供を行っている場合には、世帯の構成員が同意を撤回する場合に備えて、各構成員が直接サービスの利用停止をできるようにすることが**望ましい**。

7.3.1. サービス利用を停止した場合のスマートホーム IoT データの扱いについて

利用者がスマートホーム IoT データを用いたサービス利用を停止した場合の対応について以下に記載する。

① IoT 機器からのデータ送出も停止する**必要がある**。
② サービス利用の停止までに利用者より収集したスマートホーム IoT データは、各企業での利用を停止することが**望ましい**。
③ サービス利用が停止され、時間が経過したスマートホーム IoT データについては削除することが**望ましい**。
④ スマートホーム IoT データを第三者に提供している場合には、提供先に対して上記①～③の対応を要求することが**望ましい**。

また、利用者が IoT 機器の利用をとり止めたあとで、この IoT 機器を中古品として他

者に譲渡や転売することも考えられる。各企業で収集済みのスマートホーム IoT データについては上述のとおりであるが、IoT 機器の中にスマートホーム IoT データが残っているケースも想定される。このようなケースでは、利用者の想定範囲外でスマートホーム IoT データが第三者に漏洩する可能性がある。こうした漏洩を防ぐために、IoT 機器では機器内部で管理するスマートホーム IoT データを削除する機能を搭載するとともに、削除機能について取扱説明書などに記載して利用者への注意喚起を図ることが望ましい。

7.4. その他留意事項

近年の企業では、保管する個人情報を本人が把握、管理できる手段を用意し、ID に紐づけて保管されているデータのコピーを収集することや、ID の無効化や削除をすること、ID に関連付けられたデータの完全な削除を可能にしている。また、データの解析に利用する項目についても、本人が個別に ON/OFF を設定することが可能になっている。

また、総務省の「プラットフォームサービスに関する研究会　中間とりまとめ （令和 3 年 9 月） https://www.soumu.go.jp/main_content/000769270.pdf 」には、①個別同意、②プライバシー設定の工夫について記載されている。①の個別同意は、取り扱う情報の種類や利用目的、第三者提供先等について、個別に利用者が同意できるフォーマットを提供することについて記載されているが、この個別同意フォーマットについては、利用者全体の 64%が利用したいと回答している。

また、②のプライバシー設定は、利用者がサービス利用にあたり、同意した内容を確認することや同意を撤回（オプトアウト）することを容易にさせるための設定を一覧的に設定、管理することを可能とする画面（ダッシュボード）を提供することについても記載されているが、このプライバシー設定についても、利用者全体の 67%が利用したいと回答している。これらの回答から考えると、スマートホームIoTデータにおける利用者の自己コントロール性について、①個別同意フォーマットや②プライバシー設定の機能を実装することは、利用者だけではなく、提供する企業にとっても利用者から信頼されるという点で将来あるべき工夫であると言える。

8. プライバシー情報管理に関するガバナンス体制

IoT 機器やそれに伴うサービスの多様性から、本ガイドラインの指針は事業者の判断による部分が多い。逆にいえば、事業者が IoT 機器からスマートホーム IoT データを適切に収集し、そのスマートホーム IoT データを適切に利用することが前提になる。従って、事業者がプライバシー保護内容を適切に判断して、それを実施することが求められる。一方で、個人情報とは異なり、スマートホーム IoT データなどを含むプライバシーに関する情報の範囲は広いため、すべからく保護していると、事業者のビジネスは進まなくなる。さらに IoT 機器の種別や相違はもちろん、同じスマートホーム IoT データであっても事業者自身の業態や保有するスマートホーム IoT データ、そしてサービスによっても、求められるプライバシー保護の範囲や方法は異なるため、本ガイドラインに準拠するとしても、事業者それぞれが保護すべきプライバシーに関する情報とその保護方法を適切に判断することが求められる。また、短期的にはプライバシー保護と企業としての利益追求が相反するケースも想定され、継続的にプライバシー保護を運用していくためには、事業者自身が適切な規律を定めてその実施を担保することが求められる。このため、事業者自身でプライバシーに関わるガバナンスを定めることが重要となる。

これまで記載をしてきたように、スマートホームの利用者からの信頼確保に向けては、スマートホーム IoT データの取り扱いに関する事業者からの丁寧な説明、同意取得、自己コントロール性の確保が、サービス設計の段階から必要となる。一方で、製品の開発や設計時における現場レベルの対策に留まらず、事業者全体として対策の実効性を確保するためにも、経営者やサプライチェーン全体を含めたガバナンスレベルでの対応も必須となる。

経済産業省と総務省は、分野・産業の壁を超えてデータに関する取引を活性化することを目的として、「企業のプライバシーガバナンスモデル検討会」（座長：佐藤一郎）を設置し、「DX 時代における企業のプライバシーガバナンスガイドブック」を公表した。

同ガイドブックでは事業者におけるプライバシー保護に関わる取り組みとして、プライバシー対応を事業者にとってコストではなく、商品やサービスの品質の改善と位置づけている。実際に、適切なプライバシー対応は他の事業者に対する重要な差別化要素となりうる。IoT を含めてデータの利用が重視される状況においては、利用者から有用なデータの提供を受けた事業者は、AI を含めて高次なデータ利用が可能となる。そのためには利用者の信頼を得ることで、利用者が安心してデータを事業者に提供できることと、事業者がその信頼に応えることが早道である。

そうした事業者におけるプライバシーの取り組みに関わる変化を受けて、ガイドブックでは、経営者が取り組むべき三要件、プライバシーガバナンスの重要事項が記載されており、個々の企業の状況に応じて柔軟に利用をしていくことが望ましい。詳細については、本ガイドブックを参照頂きたい。

8.1. 経営者が取り組むべき三要件

企業の経営者には、プライバシー問題への対応を競争力の要素として、重要な経営戦略上の課題として捉えるとともに、コーポレートガバナンスとそれを支える内部統制の仕組みを企業内に構築・運用することが求められる。プライバシーガバナンス実現のために、経営者が実施すべきことは、以下の3点である。

① プライバシーガバナンスに係る姿勢の明文化

利用者のプライバシーを守っていくことは、これからの経営上の重要事項の１つと認識し、組織の一貫した対応を可能とするプライバシー保護の軸となる基本的な考え方や、プライバシーリスクに能動的に対応していく姿勢を明文化し、組織内外に知らしめることが必要である。

明文化の具体的な形としては、宣言の形をとったプライバシーステートメントや、組織全体での行動原則などを策定するケース等がある。

②プライバシー保護責任者の指名

経営者は、組織全体のプライバシー問題への対応の責任者を担当幹部として指名し、経営者が姿勢を明文化した内容を踏まえて、その実践を行うための責任を遂行させることが必要である。

③プライバシーへの取組に対するリソース投入

経営者は、姿勢を明文化した内容の実践のため、必要十分な経営資源（ヒト・モノ・カネ）を投入することが求められる。プライバシー問題に対応するための体制を構築し、そこに十分な人員を配置することや、人材育成、新たな人材の確保を実施することが必要である。

8.2. プライバシーガバナンスの重要項目

プライバシーガバナンスを機能させるには、各部門の情報を集約し、事業におけるプライバシー問題を見つけるとともに、対象となる事業の目的の実現とプライバシーリスクマネジメントを可能な限り両立させるために、対応策を多角的に検討することが必要となる。当該目的を実現するため、指名されたプライバシー保護責任者を中心として、中核となるプライバシー保護組織を企業内に設けることが望ましい。

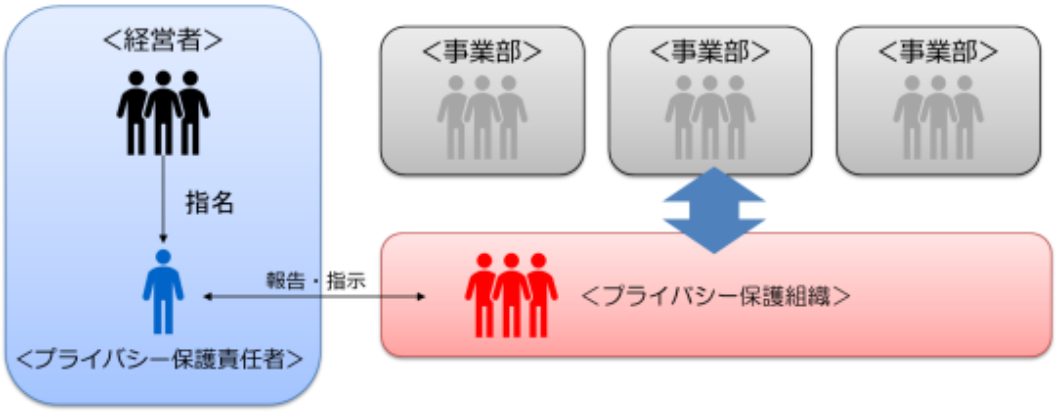

図 4 プライバシー保護の体制の構築

また、プライバシー問題に関しては、利用者や社会の受け止めの変化などを常に把握するとともに、企業がイノベーション創出やプライバシーリスクマネジメントに、いかに能動的に取り組んでいるのか、実際の問題が生じてしまった場合の対応をどのように行うのかという点について、利用者をはじめとして、ビジネスパートナー、グループ企業、投資家・株主・関係行政機関・業界団体等のステークホルダーと継続的にコミュニケーションを実施し、信頼を確保していくことが重要である。

さらに、プライバシーガバナンスに係る体制や運用を実質的に機能させていくためには、経営者が姿勢を明文化した内容について、組織全体へ浸透させ、プライバシーリスクを適切に対応できるような企業文化を組織全体で醸成していくことが不可欠である。企業に所属する従業員一人一人が、一個人や一消費者として当たり前のようにプライバシーに関する問題意識をもっていることが重要である。このような従業員が、スマートホーム IoT データの利活用に対する利用者の意識や不安、求めている情報や取組等についての理解を深め、社会と向き合った丁寧な対応をしていく状態が最も望ましい姿である。

8.3. プライバシーリスク評価の取組み

スマートホーム IoT データの利活用による新たな企業価値の創出のためには、事業者はプライバシー侵害を含めて利用者の権利利益の侵害を起こさないことを大前提として、利用者や社会からの信頼を高めることを念頭に、イノベーションの促進とリスクの適切な管理の両面に積極的に取り組む必要がある。

スマートホーム IoT データの利活用によって、プライバシーを侵害されるリスクを負うのは利用者（データ主体）である。そのため、事業者が利用者のプライバシーを侵害するリスクに適切に対応するためには、まず①利用者目線で当該リスクを特定し、評価する必要がある。また、個別のサービスやプロダクトとは別に、プライバシーに影響を及ぼし得る新しい技術やスマートホーム IoT データの利活用に対する②社会の受容水準やその変化を知っておくこと、受容性を向上させることも有用になる。

①利用者目線のリスクの特定については、個別のサービスやプロダクトの企画・開発段階、またローンチ後にいかに利用者などの意見を取り入れられるかが重要になってくる。そのための取り組みの事例としては、主に以下の取り組みが考えられる。

・テストマーケティングの際に利用者からプライバシーの観点でも意見を貰う。

・カスタマーサービス部門等に集まるお客様からの声を分析、法令対応だけでなく企画・開発部門にもフィードバックしてインプットとする。

・外部の有識者に意見を求める（定期的な会議体で実施している企業もあれば、個別のサービスやプロダクト、問題点について都度相談している企業など様々である）。

・開発担当の事業部門と技術部門だけで検討するのではなく、法務・コンプライアンス・サステナビリティなどの関連部門からも意見を貰う。

・利用者と直接的なコミュニケーションの実施。例えば、スマートシティに関する事例では、住民説明会を開催して直接説明し、利用者から意見を貰うケースもある。

また、プライバシーリスクに対する評価の方法として、国際規格などが策定されており、当該標準等の活用も有効となりえる[4] 。

なお、②社会の受容水準に関する調査としては、定量調査・パネル調査などで個別に実施するケースもあり、自社及び業界内で常に情報を収集していくことも重要となる。受容性を向上させるためには、継続的なプライバシーへの取り組みによって、利用者からの信頼を得ることを基本とした上で、収集したスマートホーム IoT データを活用して利用者により便利なサービスを提供するなどの経済的なメリットを提供していくことも効果がある。

[4] 例えば、ISO/IEC 29134（PIA ガイドライン）およびこれに基づく国内規格 JIS X 9251:2021 では、個人に対するプライバシー影響の重大度、組織に対する全体的な影響を捉えた上で、プライバシーリスクの相対的な優先順位付けを実施する、プライバシーリスク評価の考え方を示している。

9. おわりに

当協会のスマートホーム部会では「生活者に、安心・安全、健康、快適、便利なサービスを提供する新たなスマートライフ市場の構築に向け、住宅・住宅設備機器・家電・IT 通信機器・サービス等の住まいに関わるあらゆるモノを連携し、業界・業種の枠を超えたスマートホーム実現に資する取組みを行う」ということを目的として、活動を推進している。利用者一人一人にあわせた便利なサービスを提供していくためには、スマートホーム IoT データを利活用していくことが重要である。

スマートホーム IoT データを利活用するには、まずは利用者からスマートホーム IoT データを提供してもらう必要がある。当協会の独自調査でも、プライバシー保護に関する懸念が、スマートホームでの IoT 機器利用を阻害する要因の一つになっていることが判明している。

本ガイドラインで示した各種の要件に対して、スマートホームに関わる機器やサービスの提供事業者が真摯に取り組むことで、プライバシー保護に関する利用者の懸念を払拭することが可能となる。これにより、利用者からより多くのスマートホーム IoT データを提供いただけるようになり、さらに便利なサービスを提供することでスマートホームの付加価値を向上していくことができる。

スマートホームに関わる機器やサービスの提供事業者においては、利用者のプライバシー保護に関する懸念を払拭し、より便利なサービスをより多くの利用者にお届けするための一助として本ガイドラインを活用いただきたい。

プライバシーの捉え方は歴史とともに変化している。本ガイドラインは部会に属する家電機器メーカ・サービス事業者を中心に執筆したが、それ以外に学術有識者や弁護士、消費者団体の関係者による会議を複数回開催して、IoT 機器におけるプライバシーに関して多様な見地から意見を頂きながらとりまとめた。ただし、今後も利用者や社会のプライバシー意識の変化に応じて随時見直しが必要となる。また、個人情報保護法についても、いわゆる三年ごと見直しが規定されており、本ガイドラインについても、同様のタイミングで見直していくことが必要である。

スマートホーム分野で生じるプライバシーリスクや課題、ベストプラクティスとなり得る取り組みについては、スマートホーム部会における普及啓発活動を通じて随時情報共有を図っていく。本ガイドラインの読者におかれては、本ガイドラインで示したルールだけではなく、最新の事例も踏まえた上で、利用者のプライバシー保護に関する懸念の払拭に努められたい。

付録1. 参考文献

- 「オプトアウト方式で取得する非特定視聴履歴の取扱いに関するプラクティス（ver2.0）」

発行元	一般社団法人　放送セキュリティセンター（SARC）
概要	視聴者のプライバシーに配慮して、適正に視聴関連情報を活用するための取扱いについて整理したもの。
参照先	https://www.sarc.or.jp/NEWS/hogo/20200731.html

- 「放送受信者等の個人情報保護に関するガイドライン」

発行元	個人情報保護委員会・総務省
概要	視聴者特定視聴履歴その他の放送受信者等の個人情報の適正な取扱いに関し、受信者情報取扱事業者の遵守すべき義務等の内容をまとめたもの。
参照先	https://www.ppc.go.jp/files/pdf/broadcast_recipient_GL.pdf

- 「カメラ画像利活用ガイドブック ver3.0」

発行元	経済産業省／総務省
概要	経済産業省・総務省は、商用目的でカメラ画像を利活用するにあたり必要な配慮事項を整理し、配慮事項のポイントを写真やイラストを盛り込んだ具体例を通して解説している。
参照先	https://www.meti.go.jp/press/2021/03/20220330001/20220330001.html

- 「医療・介護関係事業者における個人情報の適切な取扱いのためのガイダンス」

発行元	個人情報保護委員会／厚生労働省
概要	病院、診療所、薬局、介護保険法に規定する居宅サービス事業を行う者等の事業者等が行う個人情報の適正な取扱いの確保に関する活動を支援するための具体的な留意点・事例等を示すもの。
参照先	https://www.ppc.go.jp/personalinfo/legal/iryoukaigo_guidance/

- 「医療情報システムの安全管理に関するガイドライン」

発行元	厚生労働省
概要	医療情報システムの安全管理や e-文書法への適切な対応を行うため、技術的及び運用管理上の観点から所要の対策を示したもの
参照先	https://www.mhlw.go.jp/stf/shingi/0000516275.html

- 「医療情報を取り扱う情報システム・サービスの提供事業者における安全管理ガイドライン」

発行元	経済産業省
概要	総務省「クラウドサービス事業者が医療情報を取り扱う際の安全管理に関するガイドライン」、および経済産業省「医療情報を受託管理する情報処理事業者における安全管理ガイドライン」が定める要件を整理・統合したもの。
参照先	https://www.meti.go.jp/policy/mono_info_service/healthcare/teikyoujigyousyagl.html

- 「医療情報を受託管理する情報処理事業者向けガイドライン」

発行元	経済産業省
概要	法令に保存義務が規定されている診療録及び診療諸記録の電子媒体による保存に関するガイドライン（紙等の媒体による外部保存を含む）、及び医療・介護関連機関における個人情報保護のための情報システム運用管理ガイドラインを示したもの。
参照先	https://www.meti.go.jp/policy/it_policy/privacy/iryouglv2.pdf

- 「クラウドサービス事業者が医療情報を取り扱う際の安全管理に関するガイドライン」

発行元	総務省
概要	医療機関等による委託に基づいて医療情報を取り扱うクラウドサービス事業者に対して、厚生労働省ガイドラインに示される必要な安全管理対策について示したもの。
参照先	https://www.soumu.go.jp/main_content/000567229.pdf

- 「個人情報の保護に関する法律についてのガイドライン（通則編）」

発行元	個人情報保護委員会
概要	事業者が個人情報の適正な取扱いの確保に関して行う活動を支援すること、及び当該支援により事業者が講ずる措置が適切かつ有効に実施されることを目的として、個人情報の保護に関する法律に基づき具体的な指針として定めるもの。
参照先	https://www.ppc.go.jp/personalinfo/legal/guidelines_tsusoku/

- 「電気通信事業における個人情報保護に関するガイドライン」及び「電気通信事業における個人情報保護に関するガイドラインの解説」

発行元	個人情報保護委員会・総務省
概要	電気通信事業を行う者に対し、通信の秘密に属する事項その他の個人情報の適正な取扱いについてできるだけ具体的な指針を示すことにより、その範囲内での自由な流通を確保して電気通信役務の利便性の向上を図るとともに、利用者の権利利益を保護することを目的として、個人情報保護法及び電気通信事業法の関連規定に基づき具体的な指針として定めるもの。
参照先	https://www.soumu.go.jp/main_sosiki/joho_tsusin/d_syohi/telecom_perinfo_guideline_intro.html

- 「電気通信事業参入マニュアル[追補版]」

発行元	総務省
概要	電気通信事業を営む者が電気通信事業法への理解を深め、法令遵守に資するため、電気通信事業法の用語、適用を判断するための考え方及び具体的な事例等を体系的にまとめたもの。
参照元	「電気通信事業参入マニュアル[追補版]」 https://www.soumu.go.jp/main_content/000477428.pdf 「電気通信事業参入マニュアル[追補版]ガイドブック」 https://www.soumu.go.jp/main_content/000799137.pdf

- 「DX 時代における企業のプライバシーガバナンスガイドブック」

発行元	経済産業省／総務省
概要	パーソナルデータの利活用において、プライバシーへの配慮はますます重要になってきており、プライバシーガバナンスの構築は不可欠となる。その実践にあたっての取組みを、参考となる具体的事例を交えながら解説したもの。
参照先	https://www.meti.go.jp/press/2021/02/20220218001/20220218001.html

- 「プライバシーガバナンスに関する調査結果」

発行元	経済産業省・総務省
概要	プライバシーガバナンスに親和性のある取組を実施している企業 16 社・団体に対してヒアリングを実施し、経営者が取り組むべき 3 要件、プライバシーガバナンスの重要項目に基づき、整理したもの。
参照先	https://www.meti.go.jp/press/2021/03/20220318014/20220318014.html

- 「プラットフォームサービスに関する研究会　中間とりまとめ」

発行元	総務省
概要	利用者情報の適切な取扱いの確保に関して、プラットフォーム事業者等の具体的な方策の在り方や今後の検討の具体的な方向性を示したもの。
参照先	https://www.soumu.go.jp/main_content/000769270.pdf

- 「JIS X 9251:2021 情報技術―セキュリティ技術―プライバシー影響評価のためのガイドライン」

発行元	日本産業標準調査会(JISC)
概要	潜在的なプライバシーへの影響を事前に評価(PIA:Privacy Impact Assessment)するための有効な方法／手段を示した国際標準 ISO/IEC 29134:2017 Information technology – Security techniques – Guidelines for privacy impact assessment の JIS 版。
参照先	https://www.jipdec.or.jp/library/report/20210225-2.html (PIA とは何か？PIA の進め方とポイントを解説、一般財団法人日本情報経済社会推進協会)

- 「PIA の取組の促進について ―PIA の意義と実施手順に沿った留意点―」

発行元	個人情報保護委員会
概要	PIA（Privacy Impact Assessment、個人情報保護評価）を促進する上で、事業者、消費者、認定個人情報保護団体をはじめとする関係団体等の関係者向けに、PIA の意義や手順をまとめたもの。
参照先	「PIA の取組の促進について―PIA の意義と実施手順に沿った留意点―（概要）」（個人情報保護委員会、2021 年） https://www.ppc.go.jp/files/pdf/pia_overview.pdf ・「PIA の取組の促進について―PIA の意義と実施手順に沿った留意点―」（個人情報保護委員会、2021 年） https://www.ppc.go.jp/files/pdf/pia_promotion.pdf

- 「情報信託機能の認定スキームの在り方に関する検討会とりまとめ」

発行元	総務省
概要	テレマティクス機器、IoT 機器等の世帯等の複数の構成員が利用する情報収集機器等から取得されるデータを利用する場合の構成員の同意が得られていることの確認や利用停止の求めの取扱いについて配慮事項を纏めている。
参照先	https://www.soumu.go.jp/main_content/000764119.pdf

- 「放送分野の個人情報保護に関する認定団体指針」

発行元	一般財団法人 放送セキュリティセンター
概要	放送分野ガイドラインから委ねられている視聴者特定視聴履歴及び視聴者非特定視聴履歴の取扱いを中心に、同ガイドラインを補足する規範を定めている。
参照先	https://www.sarc.or.jp/documents/www/hogo/touroku/hogo_shishin.pdf

付録2. 用語の説明・定義

用語	説明・定義
利用者	スマートホーム IoT 機器や、スマートホーム IoT データを活用したサービスの利用者
利用目的	スマートホーム IoT 機器から収集されるスマートホーム IoT データの利用目的
家電機器	冷蔵庫や洗濯機、エアコンなど、家庭で利用される電子機器。家電量販店などで利用者が購入し、必要に応じて販売事業者が設置工事を行った上で、家庭内で利用される。
住設機器	ブレーカーやダウンライト、ドアホンなど、住宅の設備として機能する電子機器。一般的には、住宅の一部としてハウスビルダーやマンションデベロッパー、不動産事業者などから購入する。
個人情報	個人情報の保護に関する法律（平成十五年法律第五十七号）の第二条で定められる、生存する個人に関する情報
プライバシーポリシー	どのようなデータを収集するのか、収集したデータをどのように扱うのか、サービス事業者が利用者に対して提示する規範。
利用規約	機器やサービスの利用に関して、提供者の義務や権利、利用者が遵守しなければならない内容などを定めたもの。
外部送信	機器に対する利用者の操作履歴や、機器に搭載されたセンサーによって収集されたデータについて、インターネットなどの公衆回線を通じて外部機器に送信する行為。
第三者提供	データを収集した事業者が、他の事業者に対してデータを提供する行為。

付録3. チェックリスト

本チェックリストでは、5 章から 7 章で「必要である」「必要がある」「望ましい」「してはならない」と記載したルールについてリストとして提示する。ただし、単なる例示として記載している箇所については、本チェックリストでは割愛した。プライバシーポリシーの作成時や、機器・サービス仕様の作成時などのチェックリストとして活用されたい。

なお、ルールが適用される条件や、例外事項、注意点などについては、本文の関連する記載を確認すること。

番号	記載箇所	ルール内容
1	5 章直下	スマートホーム IoT データを取り扱う事業者は、どのようなデータを、どのように取得して、どのような目的に利用するかを、データのライフサイクル全般にわたって通知・公表・説明し、原則として同意を得た上で利活用する**必要がある**。
2	5.1 節	スマートホーム IoT データを利用者から収集する場合には、原則として事前に同意を取得するオプトイン方式であることが**必要である**。
3	5.1 節	スマートホーム IoT データとして収集する情報とその利用目的については、できる限り具体的に、その情報に関して特定できるように箇条書きなどで説明し、利用者が同意して良いかを適切に判断できる情報にする**必要がある**。
4	5.1 節	通知・説明・公表する場所は、製品の取扱説明書、スマートフォンアプリのトップページ、利用者が最初に到達する Web ページなどスマートホーム IoT 機器の利用者が、その内容について適切に確認できる場所に記載することが**必要である**。
5	5.1 節	第三者提供においては、個人情報に該当しないスマートホーム IoT データであっても提供先において、他の情報と突合することにより個人情報になることが想定されるスマートホーム IoT データについては、個人情報保護法に従った対応が**必要である**。
6	5.1 節	代表となる利用者が世帯の構成員に対してスマートホーム IoT データが収集・利用されることを周知し了解を得る必要があることを代表となる利用者に注意喚起したうえで、代表となる利用者本人から同意を取得する**必要がある**。
7	5.1 節	共用している機器のスマートホーム IoT データから世帯の構成員を識別し、収集したスマートホーム IoT データを利用して、個々の構成員を対象としたサービスや情報提供を行う場合には、構成員からの直接の同意取得やサービスの利用停止も**必要である**。

8	5.2 節	利用者に提示するプライバシーポリシーに記載する用語は、利用者がスマートホーム IoT データの扱いに関して、正しく理解するために必要であり、図などを用いて、わかりやすく記載することが**望ましい**。
9	5.2 節	IT 技術者だけが理解できるような用語については、その収集されるデータの中身と、それによるデータの取り扱い方について明確化する**必要がある**。
10	5.2 節	スマートホーム IoT データのフロー（入力から出力までの流れ）についても、図などを用いて説明することが**望ましい**。
11	5.3 節	プライバシーポリシーでは、IoT 機器が取り扱うスマートホーム IoT データについて、これをリストアップして利用者に提示する**必要がある**。
12	5.3 節	スマートホーム IoT データの利用方法に応じて、一般の利用者にも理解可能な表現で、二次加工データを含めて、プライバシーに対する影響が明確になるように記載する**必要がある**。
13	5.3 節	対象となるスマートホーム IoT データの名称を、一般の利用者にも判りやすい表現で記載する**必要がある**。
14	5.3 節	プライバシー影響度合いの異なるカテゴリ分類を跨がるような過度の大括りは**してはならない**。
15	5.3 節	対象となるデータ毎に、以下に例示するようなデータ収集の方法について記載することが**必要である。**
16	5.3 節	以下の方法は網羅的なものではなく、各 IoT 機器の特徴に応じて適切な方法を記載することが**望ましい**。
17	5.3 節	長期間にわたる収集や、頻繁な収集、高精度な収集でプライバシーに対する影響が高まる場合には、その期間や頻度・精度についても記載することが**望ましい**。
18	5.3 節	収集した原データをどのような機能を実現するために利用するのかに応じて、その際に知り得るプライバシー情報の内容について判るように記載する**必要がある**。
19	5.3 節	IoT 機器の設置場所についてサービス利用仕様で想定する場所があるにも関わらず想定外の場所に設置する場合には、サービス提供事業者はプライバシーポリシーなどで利用者への説明や注意喚起を行うことが**望ましい**。
20	5.3 節	プライバシーポリシーでは、対象となるスマートホーム IoT データに関する説明とともに、その利用目的についても説明をすることが**必要である**。
21	5.3 節	複数の利用目的がある場合には、プライバシーポリシーでは、その全てを記載することが**必要である。**

22	5.4.1 節	利用者がスマートホーム IoT データの利用目的を理解できるように記載することが**必要である**。
23	5.4.1 節	AI 処理によって得られるプライバシー情報の内容について説明することなどで、スマートホーム IoT データと利用目的の関係性を明確化することが**望ましい**。
24	5.4.1 節	サービス内容を十分に理解せず、または誤解してサービス利用を開始してしまうこともありえるため、7.3 節で記載する利用停止に関する自己コントロール性を提供することも**必要である**。
25	5.4.2 節	利用者がスマートホーム IoT データの利用目的を理解できるように記載することが**必要である**。
26	5.4.2 節	不十分な理解や誤解に基づいて利用を開始してしまった場合に備え、第三者提供の停止を可能としておくことが**望ましい。**
27	5.4.3 節	実際に質問事項や不具合が発生するまではその必要性が判りにくいため、利用目的として具体的なカスタマサポートの内容について記載することが**必要である**。
28	5.4.4 節	特定の個人が識別できない方法で、内部での開発や分析のために利用することを説明する記載が**必要である**。
29	5.4.5 節	特定の個人が識別できないように匿名化されたデータや、多数の IoT 機器からのスマートホーム IoT データを統計化したデータとして提供することを前提として、第三者側での開発・分析用途などのために第三者に提供することを説明する記載が**必要である**。
30	5.4.5 節	匿名化されたデータとして提供する場合には、提供される情報の項目について特定の個人が識別できない理由とともに説明する**必要がある。**
31	5.4.6 節	どのような場合にどのようなスマートホーム IoT データに基づいたプロモーションを実施するかを説明するための記載があることが**望ましい**。
33	5.4.6 節	第三者提供されたデータを統合して利用する場合には、統合して利用することについても記載をしておく**必要がある**。
34	5.4.6 節	統合の結果読み取れるプライバシー情報の内容についても記載しておくことが**望ましい**。
35	5.4.7 節	どのような第三者に対して提供するのか、どのような種類のスマートホーム IoT データを提供するのか、について記載することが**必要である**。
36	5.4.7 節	スマートホーム IoT データを AI 処理などで二次加工した情報を提供する場合には、その二次加工によって得られるプライバシー情報の内容について記載することも**必要である**。

37	5.4.8 節	個人情報保護法に準じて例外的に第三者提供する可能性を記載しておくことが**望ましい**。
38	5.5 節	他社に業務委託をする際には、各種の情報を適切に取り扱うよう、委託先企業名、委託するスマートホーム IoT データの内容などを明確にした二者間契約を締結する**必要がある**。
39	5.5 節	二社間での委託契約書においては、委託元名・委託先名、委託するスマートホーム IoT データの内容、守秘義務、漏洩時の責任・保証など、委託先が負うべき義務について明確に規定することが**必要である**。
40	5.5 節	プライバシーポリシーでは、業務委託に関する状況について、利用者に説明することが**望ましい**。
41	5.6 節	共同利用されるスマートホーム IoT データの項目、利用する事業者、利用目的等（共同利用事項）をあらかじめ、利用者に通知し、又は利用者が容易に知り得る状態に置く記載する**必要がある**。
42	5.6 節	参加する企業の列挙の仕方、撤退時/企業統合時など共同利用者の状況変化が起きた場合のスマートホーム IoT データの扱い、責任についても明確にしておくことが**望ましい**。
43	5.7 節	通知、同意を求めている内容について理解できるよう複数の言語で記載（表示）することが**望ましい**。
44	5.7 節	収集したスマートホーム IoT データが国外に送信、蓄積され、国外で利用される場合や、国内で収集したスマートホーム IoT データを海外に移転する場合など、国、法域を超える場合には、利用者に通知することが**望ましい**。
45	5.7 節	サービスでの還元時に適宜収集データの内容やその利用目的について注意喚起を行うことや、廃棄の際にスマートホーム IoT データの取り扱い内容について重ねて説明することが**望ましい**。
46	6.1 節	取扱説明書などにおいて、プライバシーポリシーを提示する箇所と、機器の特殊操作を説明する箇所を隣接しておく**必要がある**。
47	6.1 節	特殊操作については、例えば特定の 5 つのボタンを予め定められた順番で押下したうえでそのうちの 3 つのボタンのみを 10 秒以上押下するなど、通常の利用では起こりえない操作とすることが**必要である**。
48	6.1 節	ネットワーク接続によってスマートホーム IoT データの収集が始まることが、プライバシーポリシーでの説明などを通じて一般の利用者にも十分に理解可能なことが**必要である**。

49	6.1 節	本ガイドラインとしては、これらの方法は同意取得と見做**してはならない**と考える。
50	6.2 節	第三者提供時、利用目的の追加・変更時、共同利用するデータ項目や共同利用する者の範囲の変更時について、本ガイドラインでは個人情報ではないスマートホーム IoT データにおいても、同意取得が**必要である**。
51	6.2 節	データ収集開始時や後から追加でデータを収集する場合にも、原則として同意取得が**必要である**。
52	6.2.1 節	IoT 機器をネットワークに接続してスマートホーム IoT データの収集を開始する前に、原則として同意を取得することが**必要である**。
53	6.2.1 節	対象となるスマートホーム IoT データの分類カテゴリ、その利用目的のカテゴリに応じて、適切な方法を選択する**必要がある**。
54	6.2.2 節	スマートホーム IoT データがプライバシーに配慮すべきデータであることを踏まえて、第三者に対してスマートホーム IoT データを提供する前に、同意を取得する**必要がある**。
55	6.2.2 節	各事業者において同意取得する判断を行った場合には、**①明確な意思確認を得る同意**に分類される方法で同意を取得することが**必要である**。
56	6.2.3 節	IoT 機器から新たな種類のスマートホーム IoT データを追加で収集開始する前に、原則として同意を取得することが**必要である**。
57	6.2.3 節	変更時の同意取得が可能なユーザインタフェースを備えた同意取得方法で、同意を取得することが**望ましい**。
58	6.2.3 節	対象となるスマートホーム IoT データの分類カテゴリ、その利用目的のカテゴリに応じて、適切な方法を選択する**必要がある**。
59	6.2.4 節	収集しているスマートホーム IoT データの利用目的を追加・変更する際には、同意を再取得することが**必要である**。
60	6.2.4 節	スマートホーム IoT データの利用目的を変更する場合には、同意の再取得を得たあとに収集されたスマートホーム IoT データのみを新たな利用目的で利用することが**望ましい**。
61	6.2.4 節	個人情報保護法ガイドライン（通則編）に記載の、社会通念上、本人が通常予期し得る限度と客観的に認められる範囲の変更かどうかを判断基準の参考とし、同意取得の適否を判断する**必要がある**。
62	6.2.4 節	各事業者において同意取得する判断を行った場合には、**①明確な意思確認を得る同意**に分類される方法で同意を取得することが**必要である**。

63	6.2.4 節	収集データと利用目的の紐づけや収集データの分析方法についても、利用目的の記載の中で具体的に特定することが**望ましい**。
64	6.2.5 節	共同利用するデータ項目や、共同利用を行う者の範囲を変更する際には、同意を再取得することが**必要である**。
65	6.2.5 節	各事業者において同意取得する判断を行った場合には、**①明確な意思確認を行う同意**に分類される方法で同意を取得する**必要がある**。
66	7 章直下	事業者には、自己コントロール性を利用者に提供するとともに、その旨をプライバシーポリシーで記載することが**必要である**。
67	7 章直下	昨今ではダッシュボードと呼ばれる、自己コントロール性を一括して提供するためのユーザインタフェースが提唱されており、将来的にはダッシュボードを提供していくことが**望ましい**。
68	7 章直下	利用者がサービス提供を必要としなくなった際は、会員としてのサービス利用を全面的に停止するサービス退会の機能を提供することも**必要である**。
69	7.1 節	データ提供元の個人からの請求があった場合には、原則として、対象データが個人情報である場合と同様に、個人に関わるスマートホーム IoT データを開示する**必要がある**。
70	7.1.1 節	各種請求への対応時には、機器・サービスの利用者”本人” であると確信するに足る技術的な確認が**必要である**。
71	7.1.1 節	情報開示の際には、秘密鍵/証明書による機器認証や、ID/パスワードでの利用者認証で、スマートホーム IoT データの生成元となった機器やサービスの利用者”本人”であることを確認するなど、事業者各々の責任で対応する**必要がある**。
72	7.1.1 節	スマートホーム IoT 機器が利用者本人だけではなくスマートホームに在住する世帯の構成員の情報も収集している場合、情報開示の請求は世帯の構成員の情報を開示することとなる可能性があることから、世帯の構成員の了解を得たものであるかを利用者“本人”に対して確認することが**望ましい**。
73	7.1.2 節	アプリやサービスでのデータ提示機能がない場合には、無償または必要な手数料を徴収した上で、請求者がデータ提供の本人であることを確認の上、書面または電子データで提供する事が**望ましい**。
74	7.1.2 節	利用者自身による操作や入力した内容については、内部動作ログに代わる代替データの提供等で開示請求に対応する**必要がある**。

75	7.1.3 節	提供先で個人に紐付け可能な状態で第三者提供する場合には、提供先・提供内容などを含む第三者提供記録についても、スマートホーム IoT データそのものと同様に開示することが**望ましい**。
76	7.2 節	機器誤操作やセンサー誤検出により、利用者の想定とは異なるスマートホーム IoT データが収集されるケースに備え、訂正・追加・削除機能の仕組みを提供することが**望ましい**。
77	7.2 節	100%の精度が保証出来ない場合があることについて、利用者マニュアルなどで利用者への説明が必要なことは記載しておくことが**望ましい**。
78	7.3 節	利用者がスマートホーム IoT データを用いたサービスの利用が不要となった場合、その利用停止や会員からの脱会などが「容易に行える仕様」の提供が**必要である**。
79	7.3 節	スマートフォンや本体表示画面などの操作仕様を策定する場合、その導線は「設定」「会員情報」等、わかりやすい名称のメニュー内に配置することが**望ましい**。
80	7.3 節	サービスの利用を停止することで、停止されるデータ送出やサービス内容も明確に利用者に伝えることが**必要である**。
81	7.3 節	“本人”以外の世帯の構成員から利用停止を受け付ける場合には、“本人”の同意が必要である旨注意喚起する**必要がある**。
82	7.3 節	共用している機器のスマートホーム IoT データから世帯の構成員を識別し、収集したスマートホーム IoT データを利用して、個々の構成員を対象としたサービスや情報提供を行っている場合には、世帯の構成員が同意を撤回する場合に備えて、各構成員が直接サービスの利用停止をできるようにすることが**望ましい**。
83	7.3.1 節	IoT 機器からのデータ送出も停止する**必要がある**。
84	7.3.1 節	サービス利用の停止までに利用者より収集したスマートホーム IoT データは、各企業での利用を停止することが**望ましい**。
85	7.3.1 節	サービス利用が停止され、時間が経過したスマートホーム IoT データについては削除することが**望ましい**。
86	7.3.1 節	スマートホーム IoT データを第三者に提供している場合には、提供先に対して上記①～③の対応を要求することが**望ましい**。
87	7.3.1 節	IoT 機器では機器内部で管理するスマートホーム IoT データを削除する機能を搭載するとともに、削除機能について取扱説明書などに記載して利用者への注意喚起を図ることが**望ましい**