セキュリティ要件適合評価及びラベリング制度
特定分野システム（スマートホーム）向け
セキュリティ要件案（修正版）

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 SWG

令和 8 年 1 月

目次

エグゼクティブサマリー……5
1. はじめに……7
1.1. 特定分野システム(スマートホーム)の位置づけ……7
1.2. 検討体制について……8
1.3. 検討の進め方……8
2. スマートホームの構成……9
2.1. スマートホームのネットワーク構成……9
2.1.1. ネットワーク構成の基本類型……9
2.1.2. ネットワーク構成の応用類型……10
2.2. スマートホームの通信方式……11
2.2.1. 通信方式……11
2.2.2. 通信における認証方式……13
2.3. 利用が想定される機器……15
2.4. スマートホームのサービスとシステム……16
2.4.1. スマートホームのサービスとシステムの定義……16
2.4.2. ネットワーク構成の三類型に対応したスマートホームサービスの事例……17
2.4.3. スマートホームサービスの課題……18
3. セキュリティ脅威の検討……20
3.1. スマートホームの具体ユースケース……20
3.1.1. 想定する具体ユースケース……20
3.1.2. ネットワークシステム構成……22
3.1.3. 機能モジュールとデータベース構成……24
3.2. 具体ユースケースにおけるセキュリティ脅威分析……26
3.2.1. 保護するべき情報の抽出……26
3.2.2. アタックサーフェスと想定される脅威……28
3.3. その他想定される脅威について……31
3.3.1. 機器の初期ネットワーク設定……32
3.3.2. カスタマーエンジニアなどによるメンテナンス対応……32
3.3.3. 不要ポート……33
3.3.4. 製品廃棄・譲渡時の残存データ漏洩……33
3.3.5. 未知の脆弱性……33

3.4. 脅威への対策の基本方針 33
3.4.1. 想定する守るべき資産 33
3.4.2. 想定するアタックサーフェス 35
3.4.3. 想定される脅威 36
3.4.4. セキュリティ対策の基本方針 40
4. スマートホーム向け IoT 製品に求めるセキュリティ要件 41
4.1. セキュリティ要件の策定方法 42
4.1.1. 策定方法以外でのセキュリティ要件の補遺 43
4.2. ★1 に準ずるセキュリティ要件 43
4.2.1. 要件 1-1 （運用要件） 44
4.2.2. 要件 1-2 （技術要件） 45
4.2.3. 要件 1-3 （技術要件） 45
4.2.4. 要件 1-4 （運用要件） 46
4.2.5. 要件 1-5 （技術要件） 47
4.2.6. 要件 2-1 （運用要件） 47
4.2.7. 要件 3-1 （技術要件） 49
4.2.8. 要件 3-2 （技術要件） 49
4.2.9. 要件 3-3 （運用要件） 50
4.2.10. 要件 3-7 （技術要件） 51
4.2.11. 要件 3-8 （運用要件） 52
4.2.12. 要件 3-10 （技術要件） 52
4.2.13. 要件 3-14 （運用要件） 53
4.2.14. 要件 4-1 （技術要件） 54
4.2.15. 要件 5-1 （技術要件） 54
4.2.16. 要件 5-5 （技術要件） 55
4.2.17. 要件 5-7 （技術要件） 56
4.2.18. 要件 6-1 （技術要件） 57
4.2.19. 要件 9-1 （運用要件） 57
4.2.20. 要件 11-1 （技術要件） 58
4.2.21. 要件 17-2 （運用要件） 59
4.2.22. 要件 17-3 （運用要件） 60
4.2.23. 要件 17-5 （運用要件） 60
4.2.24. 要件 17-8 （運用要件） 61

4.2.25. 要件 17-10 （運用要件） 62
4.3. ★2 で追加するセキュリティ要件 63
4.3.1. 要件 4-2 （技術要件） 63
4.3.2. 要件 4-3 （技術要件） 64
4.3.3. 要件 4-4 （技術要件） 65
4.3.4. 要件 5-8 （運用要件） 66
4.3.5. 要件 8-2 （技術要件） 66
4.3.6. 要件 8-3 （運用要件） 67
4.3.7. 追加要件 （運用要件） 68
4.4. ★2 で追加するセキュリティ要件（BtoBtoC モデルを想定した運用対策） .. 68
4.4.1. 追加要件1 （運用要件） 69
4.4.2. 追加要件2（運用要件） 70
4.4.3. 追加要件3 （運用要件） 70
4.4.4. 追加要件4 （運用要件） 71
4.4.5. 追加要件5 （運用要件） 72
4.4.6. 追加要件6（運用要件） 72
4.4.7. 追加要件の課題（運用要件） 72
5. システムやサービスとしてのスマートホームに求めるセキュリティ要件 75
5.1. スマートホームサービスとシステム構成 75
5.2. セキュリティ要件の策定方法 75
5.3. 策定されたセキュリティ要件 77
5.3.1. スマートホームシステム・サービスの技術要件（機能要件） 77
5.3.2. スマートホームシステム・サービスの非技術要件（組織・運用要件） 79
付録 1. 参考文献 82
付録 2. 用語の意味・説明 83
付録 3. セキュリティ要件の分類 84

本ドキュメントに記載されている企業名および製品名は、それぞれの所有者の商標または登録商標である。特に断りのない限り、商標や登録商標の記号(™、®)は本文中では省略している。

エグゼクティブサマリー

スマートホームとは、住まい手のライフスタイルにあったサービスを IoT 技術で実現するものであり、住宅内に設置される家電・住宅設備・IoT 機器等がネットワークに接続され、機器 から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、そのようなデータを活用することで、便利で快適なサービスが住まい手に提供されるものである。一方で、家庭内には専任の管理者がおらず、セキュリティを考慮した管理・運用はなされていないことが多い。こうした中で IoT 機器がサイバー攻撃の対象となると、家電の不正操作や個人情報の漏洩、踏み台としての悪用など様々な脅威が起こりえる。

こうした脅威に対策するため、本報告書ではセキュリティ要件適合評価及びラベリング制度(JC-STAR)における特定分野の一つであるスマートホーム分野について、セキュリティ要件の考え方を示す。

セキュリティ要件の策定にあたって、まずはスマートホームを定義づけるネットワーク構成や利用される通信方式、想定される機器について検討した。また、家庭内で利用される様々な機器を用いて家全体でサービスを提供するユースケースとして、スマートホームシステムを定義した。

次にスマートホームで想定される具体ユースケースとして、エアコンの遠隔操作やモニター機能について脅威分析を実施した。結果として、IoT 機器および必須付随サービスとしてのモバイルアプリケーションやクラウドサービス、およびそれらの間の通信経路において、アップロードされるデータや、IoT 機器に対する制御指示、ダウンロードされるファームウェアの保護が必要であることが明らかになった。これを受けて、守るべき資産、アタックサーフェス、脅威や守るべき資産の関係性について、IoT 機器共通の JC-STAR★1制度と対比する形式で整理を行った。

ここまでの整理に基づいて、国内外セキュリティ要件の全体リストからスマートホーム分野として必要となる 32 項目（★1 制度準拠 25 項目、追加 6 項目、その他 1 項目）のセキュリティ要件を抽出した。このうち、JC-STAR★1 制度でも対象となっている 25 項目については、スマートホーム分野として解釈を行う際の補足を行った。さらに、家全体を一つのスマートホームシステムとして取り扱う場合のセキュリティ要件についても、システムとしてのセキュリティ要件を提示している米国 NIST IR 8425 を踏まえて、13 項目を策定した。

1. はじめに

ネットワーク技術の進化により、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 により実現するスマートホームは、国内外において急速に市場が伸長しており、大企業やスタートアップ等、あらゆる企業が参入をしている。

本報告書は、スマートホームに設置される IoT 家電や住宅設備といったネットワークに接続する様々な製品やサービスのセキュリティ確保に向けて、経済産業省及び独立行政法人情報処理推進機構セキュリティセンターにおいて、制度化が進められているセキュリティ要件適合評価及びラベリング制度(JC-STAR)における特定分野の一つであるスマートホーム分野の★2 に関するセキュリティ要件の考え方を示すことで、本制度の有効性を高めるために整備したものである。

また、スマートホーム市場に参入する様々な企業が本セキュリティ要件を遵守し、健全な市場形成を図るため、本報告書や他のガイドライン等を参考に各々のセキュリティ対策を考案されたい。

1.1. 特定分野システム（スマートホーム）の位置づけ

スマートホームとは、住まい手のライフスタイルにあったサービスを IoT 技術で実現するものであり、住宅内に設置される家電・住宅設備・IoT 機器等がネットワークに接続され、機器から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、そのようなデータを活用することで、便利で快適なサービスが住まい手に提供されるものである。（参考資料：令和 3 年 4 月 1 日「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」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）

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位置付けられ、様々な実証事業や業界アライアンスの構築等、国内での市場形成・普及に向けた動きが本格化している状況にある。

一方で、スマートホームのシステム導入・製品選定にあたっては、家庭内に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、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玄関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領域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、スマートホーム内の 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。加えて、スマートホームにおいては、ネットワークに接続する住宅の様々な IoT 機器がサイバー攻撃の対象となるため、セキュリティ対策が必要な製品の数は膨大となる。

スマートホームでは、住まい手も含めた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り、スマートホームに関連するネットワーク機器の利用者が安心して製品を選定できる基準が必要となってく

る。それゆえに、スマートホームを優先度の高い特定分野と位置付け、より高度なセキュリティ要件を具備することが不可欠となってくる。

1.2. 検討体制について

セキュリティ要件適合評価及びラベリング制度(JC-STAR)における★2 スマートホーム分野の検討に当たっては、産業サイバーセキュリティ研究会 WG1 の産業分野別にセキュリティ対策の標準モデルを検討するサブワーキンググループ(SWG)として設置がされている「スマートホーム SWG（事務局:一般社団法人 電子情報技術産業協会)」の枠組みを活用して、検討を行った。スマートホーム SWG には、11 社、8 団体、2 研究機関に加え、経済産業省がオブザーバとして参加し、合計 4 回の SWG の開催を行った。また、スマートホーム分野は、様々な機器や住宅そのものにも関連するため、一般社団法人電子情報技術産業協会、一般社団法人エコーネットコンソーシアム、一般社団法人住宅生産団体連合会、一般社団法人日本建材・住宅設備産業協会、一般社団法人重要生活機器連携セキュリティ協議会の住まいに関わる5団体にて連携し、幹事会を発足し、議論の取り纏め等を実施した。

1.3. 検討の進め方

スマートホーム分野は消費者向けに利用が拡大するため、★1 以上のセキュリティ要件の策定は必須であり、また、諸外国でも IoT 製品のセキュリティ対策に関する制度検討が進んでおり、我が国の IoT 製品がグローバルマーケットにおいても安心して受け入れられるよう、諸外国の取組み状況も踏まえて、共通的な物差しで製品のセキュリティ機能を評価・可視化し、利用者が求めるセキュリティ水準の IoT 製品を容易に選定できるようにしていく必要がある。また、スマートホーム分野においては、IoT 製品だけでなく、IoT 製品を利活用した多様なスマートホーム関連サービスが生まれていることから、当該サービスについてもセキュリティ要件を示す必要がある。

スマートホーム関連の各 IoT 製品類型に求めるセキュリティ要件の検討にあたっては、以下の手順で検討を進めており、当該検討結果について、次章以降に記載を行う。

なお、検討に当たっては、幹事会において原案を作成し、SWG にて説明を行い、SWG メンバーより、都度意見を募集する形で検討を進めてきた。

① スマートホームのネットワーク構成、通信方式、利用が想定される機器(IoT 製品を含む)等の特定

② スマートホームにおけるセキュリティ脅威の検討

③ スマートホーム関連の各 IoT 製品類型に求めるセキュリティ要件の検討(IoT 製品類型別)

2. スマートホームの構成

この章では、特定分野システムであるスマートホームについて、これを定義づけるネットワーク構成やそこで利用される通信方式、また利用が想定される機器について説明する。またスマートホーム分野では、様々な機器が利用される家全体を一つのシステムとして考慮するケースも存在する。

なお、JC-STAR 制度では、インターネットに直接接続されない製品も含め、インターネットプロトコル(IP)を使用する通信機能を持つ機器とともに、その付随サービスを含めた IoT 製品を制度の対象としている。スマートホーム編でもこの考え方を踏襲する。

2.1. スマートホームのネットワーク構成

スマートホームのネットワークは、各種機器、スマートフォンやタブレットなどの操作端末、クラウドサーバ、クラウドサーバと各種機器を中継するホームゲートウェイ(G/W)などから構成される。セキュリティの観点では、これら構成要素間でやりとりされるデータ・制御・ファームウェア(F/W)を如何にして保護するかが重要となってくる。この節では、スマートホームシステムのネットワーク構成を分類して整理する。

2.1.1. ネットワーク構成の基本類型

スマートホームの構成要素間の通信経路の構成によって、現状利用されているスマートホームシステムの基本的なネットワーク構成は、図 2-1 に示す 3 種類に類型化される。

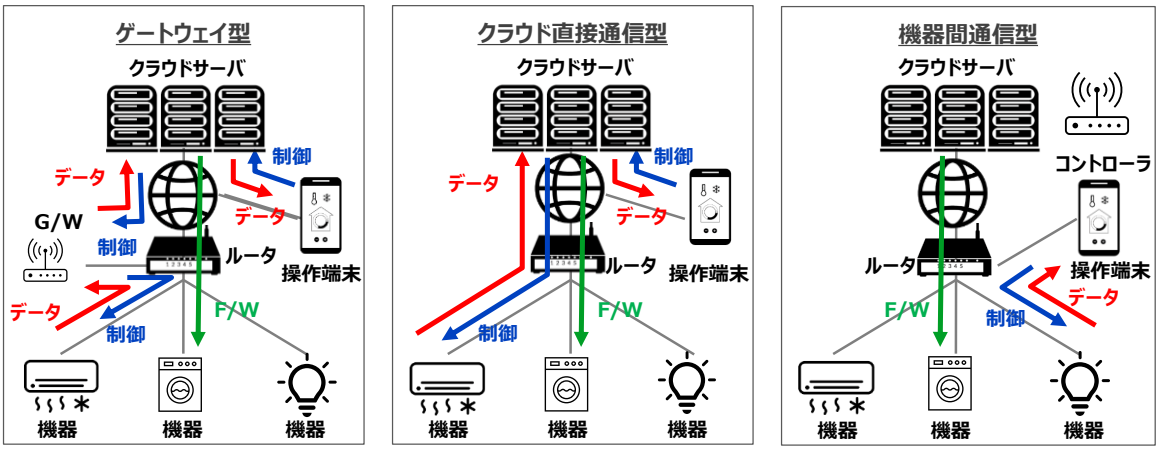


図 2-1 ネットワーク構成の基本類型

ゲートウェイ型では、各種機器は宅内の G/W と直接通信を行い、G/W はクラウドサーバと通信を行う。各種機器は G/W から直接制御されたり、宅外の操作端末からクラウドサーバと G/W を経由して遠隔制御される。また、各種機器のデータは、G/W により取得され G/W 内やクラウドサーバに保存される。宅外の操作端末は、クラウドサー

バに保存された各種機器のデータを取得したり、クラウドサーバと G/W を経由して各種機器からデータを取得する。

クラウド直接通信型では、各種機器は機器メーカ独自のクラウドサーバと直接通信を行う。各種機器はクラウドサーバから直接制御されたり、宅外の操作端末からクラウドサーバを経由して遠隔制御される。また、各種機器のデータは、クラウドサーバにより取得されクラウドサーバに保存される。さらに、宅外の操作端末は、クラウドサーバに保存された各種機器のデータを取得したり、クラウドサーバを経由して各種機器からデータを取得する。

機器間通信型では、各種機器は宅内の操作端末またはコントローラと直接通信を行う。各種機器は操作端末またはコントローラから直接制御される。また、各種機器のデータは、操作端末またはコントローラにより取得され、操作端末またはコントローラ内に保存される。

ファームウェアについては、いずれの類型においても、各種機器がクラウドサーバから取得する。

2.1.2. ネットワーク構成の応用類型

各スマートホームシステムは、前述のネットワーク構成の基本類型のうちのいずれかとなるが、各スマートホームシステム間で連携が行われるケースも存在するため、以下に応用類型として整理する。

図 2-2 に、各スマートホームシステムのクラウドサーバ間で連携を行う応用類型を「クラウド間連携型」として示す。各スマートホームシステムのクラウドサーバ間連携によって各種機器のデータを共有するとともに、相互に機器の制御を行う。図 2-2 では、各スマートホームシステムとしてゲートウェイ型とクラウド直接通信型の組み合わせ例を示しているが、ゲートウェイ型同士やクラウド直接通信型同士の組み合わせのケースもある。また、データ共有や機器制御が片方向のみとなるケースや、更にクラウドサーバ間を仲介する別のクラウドサーバを設けるケースもありえる。

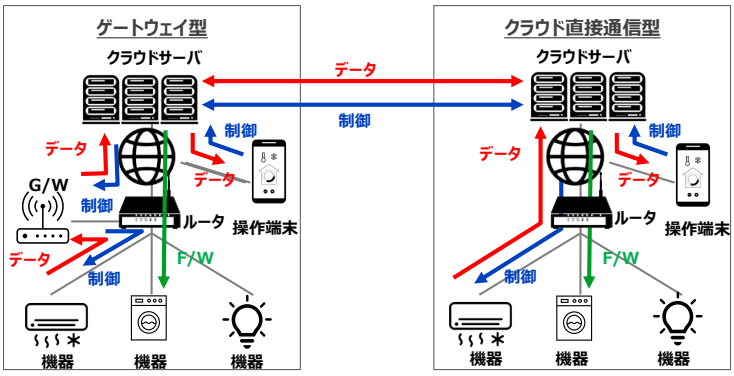


図 2-2 ネットワーク構成の応用類型（クラウド間連携型）

図 2-3 に、各スマートホームシステムのゲートウェイ間で連携を行う応用類型を「ゲートウェイ間連携型」として示す。各スマートホームシステムとしてゲートウェイ型とゲートウェイ型の組み合わせにおいて、ゲートウェイ間連携することで、データを共有するとともに、相互に機器制御を行う。

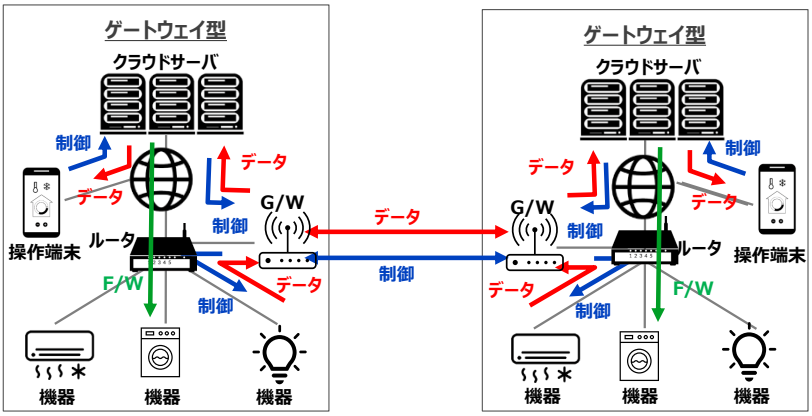


図 2-3 ネットワーク構成の応用類型（ゲートウェイ間連携型）

2.2. スマートホームの通信方式

この節では、スマートホームシステムで用いられる通信方式について整理する。

2.2.1. 通信方式

ネットワーク構成の基本類型で用いられる通信方式の例について図 2-4 に示す。G/W や操作端末と各種機器間の通信方式には、ECHONET Lite や Matter などが用いられている。また、G/W や操作端末、各種機器とクラウドサーバ間の通信には、基本的には各社独自の通信方式が用いられている。

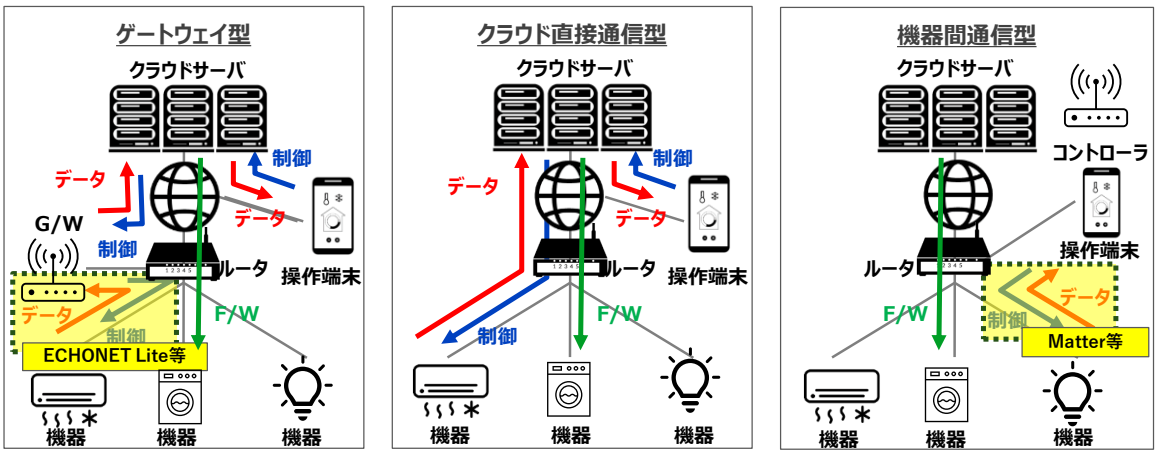


図 2-4 ネットワーク構成の基本類型で用いられる通信方式例

つづいて、ネットワーク構成の応用類型で用いられる通信方式について、図 2-5 に示す。クラウドサーバ間連携型では、共通仕様として ECHONET Lite Web API が用いられることが想定される。また、ゲートウェイ間連携型では、図には示していないが各社で選択する通信方式が用いられる。

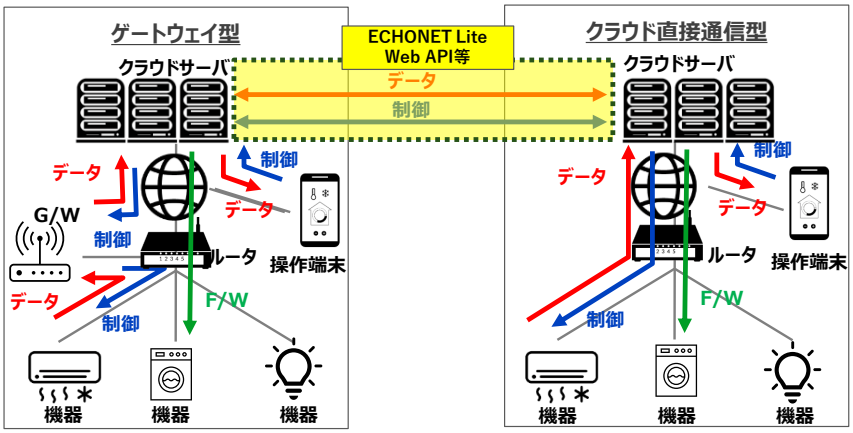


図 2-5 クラウド間連携型で用いられる通信方式例

2.2.2. 通信における認証方式

スマートホームシステムの各通信経路では、通信相手先の確認と通信路保護のために認証が行われる。認証方式は、認証トークンの違いにより表 2-1 認証方式に示すように機器認証、ユーザ認証、パスコード認証の三方式に大別される。

表 2-1 認証方式

認証方式	認証トークン	方式の例	特徴
機器認証	・秘密鍵 ・公開鍵証明書	・TLS Handshake ・DTCP-AKE	・認証と同時に鍵交換を行うのが一般的 ・以降の通信は交換した鍵で保護する ・片方向認証と双方向認証がある
ユーザ認証	・ユーザ ID ・パスワード*	・CHAP	・通信経路の保護が別途必要 ・パスワード漏洩のリスクがある ・リスク軽減のため、多要素認証を用いることもある
パスコード認証	パスコード	・SPAKE2 ・LESC ペアリング	・認証と同時に鍵交換を行うのが一般的 ・以降の通信は交換した鍵で保護する ・パスコード漏洩のリスクがあるため、初期設定など限定的なケースでのみ利用する

*) パスワードの代わりに、指紋や虹彩の特徴量など生体情報が利用されることもある

ここで、各通信経路と通信内容、認証方式の関係について整理する。図 2-6 に各通信経路とその経路番号を示す。表 2-2 に各通信経路の通信内容と通常利用される認証方式の関係を示す。

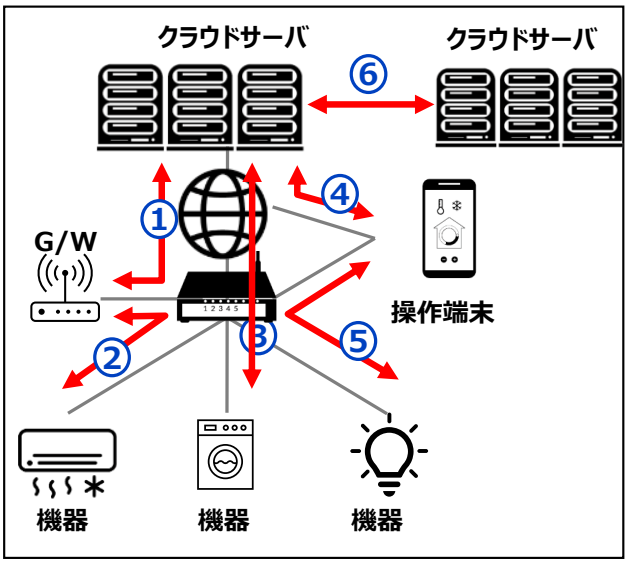


図 2-6 各通信経路と番号

表 2-2 通信経路と通信内容および認証方式の関係

経路番号	通信端点	通信内容	通常利用される認証方式
①	・サーバ ・G/W	・データ(G/W→サーバ) ・制御(サーバ→G/W)	・機器認証(片方向/双方向) ・ユーザ認証
		・F/W(サーバ→G/W)	・機器認証(双方向)
②	・G/W ・機器	・データ(機器→G/W) ・制御(G/W→機器)	・機器認証(双方向)
③	・サーバ ・機器	・データ(機器→サーバ) ・制御(サーバ→機器) ・F/W(サーバ→機器)	・機器認証(片方向/双方向) ・ユーザ認証
④	・サーバ ・操作端末	・データ(サーバ→操作端末) ・制御(操作端末→サーバ)	・機器認証(片方向) ・ユーザ認証
⑤	・操作端末 ・機器	・データ(機器→操作端末) ・制御(操作端末→機器)	・機器認証(双方向)
		・初期設定	・パスコード認証
⑥	・サーバ ・サーバ	・データ(サーバ→サーバ) ・制御(サーバ→サーバ)	・機器認証(双方向)

2.3. 利用が想定される機器

この節では、スマートホームで利用が想定される機器を整理する。表 2-3 に機器の分類と具体例を示す。ただし、全ての対象機器の網羅は困難であるため代表的な例の記載としている。なお、対象機器に該当する機器であっても IP 通信を行わない機器は、JC-STAR 制度の対象ではない。

表 2-3 利用が想定される機器

#	分類名	具体例	備考
a	住設機器	照明、電動シャッター、宅配ボックス、分電盤、空調換気扇、瞬間式給湯器	
b	エネマネ機器	電気温水器、ハイブリッド給湯機、燃料電池、蓄電池、太陽光発電、EV 充(放)電器、パワコンディショナー	特例計量器を含む
c	電気錠	玄関錠	
d	カメラ	ドアホンカメラ、ペットモニタ、ネットワークカメラ	公共空間に設置されるセキュリティカメラは除く※1
e	センサ	窓センサ、温湿度計	
f	アクチュエータ	電源タップ、カーテン開閉機、スマートスイッチ	
g	家電機器	エアコン、洗濯機、冷蔵庫、炊飯器、IH クッキングヒーター、掃除ロボ	
h	AV 機器	テレビ、レコーダ、デジタルカメラ、ビデオカメラ	コンテンツ配信は評価の対象外と考えられる※2
i	コントローラ	HEMS コントローラ、ドアホン、スマートリモコン	
j	ホームゲートウェイ(G/W)	HEMS コントローラ、スマートスピーカー	
k	健康・美容家電	体重計、電動歯ブラシ	薬機法などの対象外で、家電機器に準ずる

※) 薬機法の対象となる家庭用医療機器、別途制度検討されているスマートメータ(電力/ガス/水道)は、JC-STAR 制度 スマートホーム分野の対象外としている。

※1）公共空間などに設置される監視や防犯用途でのセキュリティカメラについては、スマートホーム分野とは別の製品類型として議論が進んでいるため、本報告書としては対象外とする。

※2）映像や音楽、静止画など各種コンテンツの通信経路上、およびストレージ上での取り扱いについては、著作権保護規格などでその保護についてルールが定められているため、スマートホーム分野における JC-STAR 制度での適合基準評価の範囲外と考えられる。

2.4. スマートホームのサービスとシステム

2.4.1. スマートホームのサービスとシステムの定義

① サービス

事業者が利用者に対して、機器やシステム及び、その運用を通じて、効用や満足等の価値を提供することを「サービス」と定義する。スマートホーム分野では、以下のケースなどを想定する。

- ハウスメーカが導入した機器やシステムを活用してサービス事業者となるケース
- 機器やシステムのメーカが自社の製品を活用してサービス事業者となるケース
- 第三者が他社のサービスや機器やシステムを活用してサービス事業者となるケース

上記のサービス事業者をまとめて本書では「サービス提供主体」と定義する。「サービス提供主体」は、顧客対応および品質保証を実施するために必ず存在し、不特定多数の機器を集めてスマートホームを構成した場合など、「サービス提供主体」が存在しないケースは対象外とする。

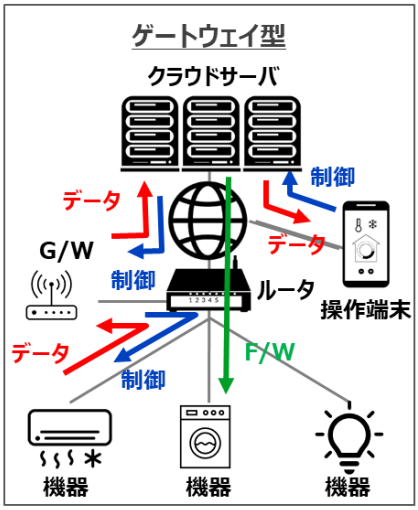
② スマートホームシステム

利用者にとっての価値を実現するために構成された機器の集合を「スマートホームシステム」と定義する。スマートホーム分野では宅内の IoT 機器環境や、サービス上必要なデータや制御を統合・管理するためのクラウドサーバなどが対象となる。ただし、人による運用はシステムに含まれないものと定義する。スマートホームシステムは基本的には 3 類型の通信方式で構成されており、★2 のセキュリティ要件を満たしているかをシステムの設計段階から検討する必要があり、責任分解をサービス提供主体と機器メーカ側との協議が必要となる。

サービス内容の制限は特に設けていないが、★2 のセキュリティ要件を満たしていること。

2.4.2. ネットワーク構成の三類型に対応したスマートホームサービスの事例

前述したネットワーク構成の三類型をもとに、それぞれのサービス事例を以下に示す。



・サービス例(HEMS サービス)

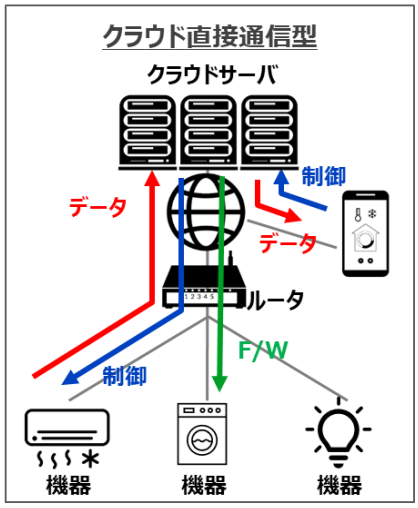
特徴:

・住宅内の各家電の制御・状態確認

・スマートフォンからの遠隔操作

・リアルタイムでの自家消費確認

快適で便利な生活を実現し、エネルギー管理が効率的に行われることで、利用者の節電意識を高めることができるサービスとなっている。



・サービス例(AI によるライフスタイル提案サービス)

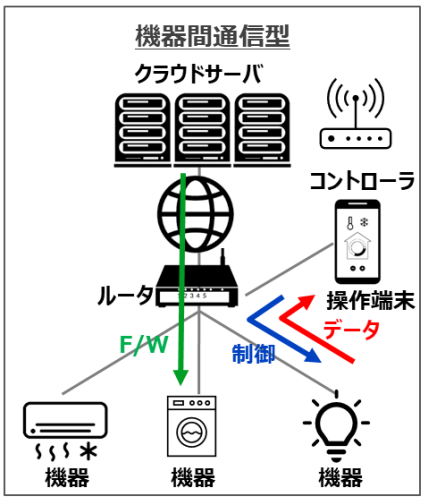
特徴:

・住宅内の各家電の制御・状態確認

・スマートフォンからの遠隔操作

・クラウド上 AI 分析によるライフスタイル提案

機器を利用すればするほど家族の好みや習慣を学習して利用に応じた使い方のアドバイスや最適なサービスをお勧めするサービスとなっている。



・サービス例(ホームオートメーションサービス)

特徴:

・音声アシスタントデバイスによるローカル制御

・音声コマンドによる操作

・スマートホームデバイスとの連携

スマートホームデバイスと簡単に連携でき、音声コマンドや自動化の設定により、利用者にとって快適な生活環境を提供するサービスとなっている。

2.4.3. スマートホームサービスの課題

利用者がスマートホームの技術を使って効用や満足等を得る場合に、利用する機器のセキュリティを担保することは当然ながら、システムや運用を含むサービス全体としての安全性も担保されなければならない。その観点から、つながる機器同士のセキュリティの安全性及びシステムとして利用するクラウドやスマートフォンなどの利用者接点を含め、システムやサービス全体としての対策が必要である。具体的には以下四つの課題を解決する必要がある。

① ステークホルダーの多様性

スマートホームサービスには、ハウスメーカ（サービス事業者）、機器メーカ（住設機器メーカや家電メーカなど）、システムインテグレータ（システムの設計や構築、運用、保守などの担当者）など、多様なステークホルダーが関係する。

例えば、機器同士やクラウドとの接続に利用される API に脆弱性があった場合、どのようにステークホルダー間で連携や責任分担を行うかが明確化されていないと、円滑なアップデート対応を阻害する可能性がある。顕在化されたセキュリティ課題に対して、ステークホルダー間における責任分解や対応指針を、サービスの統一的な基準として明確化しておく必要がある。

② ライフサイクルが異なる機器の混在

スマートホームサービスでは、住設機器（保証期間：5 年～10 年）や、家電機器（保証期間：1 年～3 年）など、ライフサイクルの異なる製品が混在している。機器のメンテナンスや更新ソフトウェアの提供、アフターサポートの対応期間など、対応方針が製品ごとに異なるため、利用者による管理が行き届きにくい。

例えばメンテナンスされずに残置された機器が、宅内ネットワークに対する攻撃の起点として利用される可能性もあり、「サービス提供主体」が定める機器の管理基準に従ったメンテナンス等、サービスとして機器の統一的な運用基準が必要となる。

③ 利用者（居住者や所有者）の変更や機器の移転

スマートホームサービスでは、利用者（居住者）の変更や機器（設備）の移転（廃棄・売却）を想定することが必要である。

例えば、住宅の売却による所有権の移転や、賃貸住宅では引っ越しによっても利用者の変更が行われる。機器や設備については、利用者が変更された後も継続して使用される場合もあれば、売却、廃棄される場合もある。

機器や設備、そしてクラウドサーバやモバイルアプリケーションなど、利用者の情報が記録される構成要素では、廃棄あるいは転売時に個人情報が漏洩しないよう、適切な権限管理や情報削除の対処等が必要となる。

④ インターネット経由での攻撃が把握しにくい

IoT 機器は一般利用者によって管理される場合が殆どであり、BOT 化や情報漏洩など、直接の影響が見えにくい攻撃には、対策が行き届きにくい。

スマートホームサービスでは、管理主体を明確に定義した上で、利用者への注意喚起を含むサービス全体を俯瞰したセキュリティ上の運用指針が必要となる。

3. セキュリティ脅威の検討

この章では、前章で定義づけた特定分野システムであるスマートホームについて、セキュリティ脅威を検討、分析していく。スマートホームでは様々な種類のネットワーク構成、通信方式、機器が利用されるため、これらを網羅的に分析することは難しい。そのため、ここでは具体的なユースケースや事例に基づいて、脅威分析を行う。これを踏まえて、守るべき資産を整理し、そのアタックサーフェスから想定される脅威をリストアップする。そのうえで、明確化された脅威に対する対策の基本方針を示す。

3.1. スマートホームの具体ユースケース

2.1 節で説明したネットワーク構成、2.2 節で説明した通信方式、2.3 節で説明した利用が想定される機器のように、スマートホームでは様々な機器が様々なネットワーク構成で接続され、その中では業界標準の複数の通信方式だけではなく、機器メーカやサービス事業者独自の通信方式も利用される。また、2.4 節で示したとおり、個々の機器だけではなく、家全体としてスマートホームシステムという観点でのサービスやユースケースも存在する。

このなかで、各機器からは各種センサで収集されるデータや、利用者の操作に応じた動作情報がネットワークを通じて、ゲートウェイやクラウドサーバ、スマートフォンで動作するモバイルアプリケーションに送信される。逆に、モバイルアプリケーションでの操作はネットワークを通じて、場合によってはゲートウェイやクラウドサーバを経由して、機器に伝達されて制御される。

さて、データや制御の種類はスマートホーム分野では多岐に渡る。業界標準の通信方式である ECHONET Lite や Matter でも各々数百種類を越えるデータや制御が定義されている。また、各社独自の通信方式でのデータや制御の種類は一般的には非公開であり、網羅的なセキュリティ脅威分析は難しい。

そこで、本章では以下に示す具体的なユースケースを想定して、セキュリティ脅威分析を実施する。

3.1.1. 想定する具体ユースケース

スマートホーム分野で幅広く利用されるユースケースとして、ネットワーク接続されたエアコンを本節では取り上げる。ここでは仮想的に、エアコンに対応するモバイルアプリケーションを利用することで、利用者は以下の三つの機能を利用できるものとする。

3.1.1.1. 遠隔操作

宅外からでも、自宅のエアコンを操作できる機能である。夏の暑い日や、冬の寒い日などに、帰宅する前からエアコンを動作させておくことで、帰宅した際には既に部屋を夏には涼しく、冬には暖かくしておくことができる。

図 3-1 エアコン遠隔操作のイメージ

3.1.1.2. モニター機能

昨今のエアコンでは、動作状況や室内温度に加えて、エアコンを効率的に動作させるために人センサを備えていることが一般的である。この人センサから収集される在不在のデータをモバイルアプリケーションで表示することで、自宅のリビングルームから、また場合によっては外出先からでも、例えば子供部屋にいる子供の状況をモバイルアプリケーションで確認することができる。

図 3-2 エアコン遠隔操作のイメージ

3.1.1.3. ファームウェア更新

利用者に提供する機能そのものではないが、ファームウェア更新も重要な機能の一つである。機能を新たに追加するようなケースに加えて、バグの修正や新たに判明した脆弱性への対応のためにもファームウェア更新が行われる。

3.1.2. ネットワークシステム構成

3.1.1 節で示した具体ユースケースを実現するためのネットワークシステム構成を図 3-3 に示す。このシステムでは、対象機器となるエアコンに加えて、利用者が遠隔制御を指示しモニター機能で状況を確認するためのモバイルアプリケーション、この二つを中継して機能を提供するためのクラウドサーバが必要となる。またこれらの間の通信経路上では、宅内のホームルータや、インターネット回線など様々な通信機器・サービスが存在する。以下では、機能毎にエアコン、モバイルアプリケーション、クラウドサーバがどのように動作していくか概略を説明する。

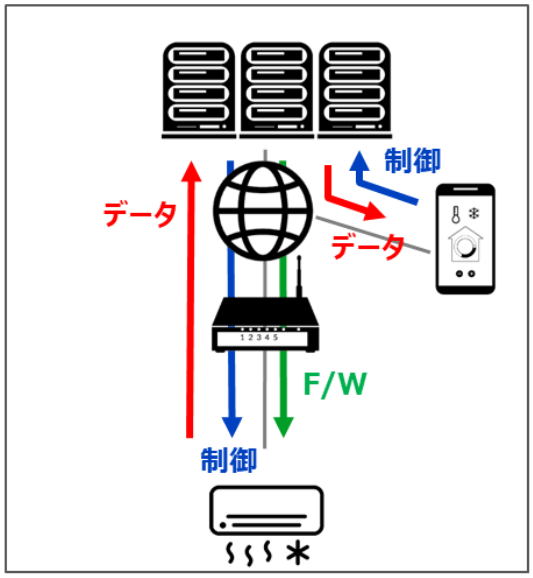


図 3-3 ネットワークシステム構成図

3.1.2.1. 遠隔操作の動作概略

1. 利用者はモバイルアプリケーションでユーザ ID とパスワードを入力し、クラウドサーバのシステムにログインする。
2. クラウドサーバ側では、ユーザ ID と機器 ID の対応を管理しており、ログインすることで操作対象となる機器のリストを利用者に提示する。
3. 利用者はモバイルアプリケーションで対象機器を選択し、電源 ON/OFF や冷暖動作モード変更、設定温度変更などを指示すると、クラウドサーバ経由でエアコンを制御する。

3.1.2.2. モニター機能の動作概略

1. 利用者はモバイルアプリケーションでユーザ ID とパスワードを入力し、クラウドサーバのシステムにログインする。
2. クラウドサーバ側では、ユーザ ID と機器 ID の対応を管理しており、ログインすることで操作対象となる機器のリストを利用者に提示する。
3. 利用者が対象機器を選択すると、対象機器からクラウドサーバ経由で収集された人センサのデータをモバイルアプリケーションで提示する。

3.1.2.3. ファームウェア更新の動作概略

1. エアコンは、定期的にクラウドサーバに対して、自身のファームウェアバージョンを通知して、ファームウェア更新の有無を確認
2. より新しいファームウェアが存在する場合には、クラウドサーバからファームウェアデータをダウンロードして、エアコンはファームウェアを更新する。

3.1.3. 機能モジュールとデータベース構成

3.1.2 節で示したネットワークシステム構成において、エアコン、モバイルアプリケーション、クラウドサーバで必要となる機能モジュールとデータベース構成を図 3-4 に示す。

以下では、エアコン、モバイルアプリケーション、クラウドサーバの各々毎に、機能モジュールとデータベース構成の概略を説明する。

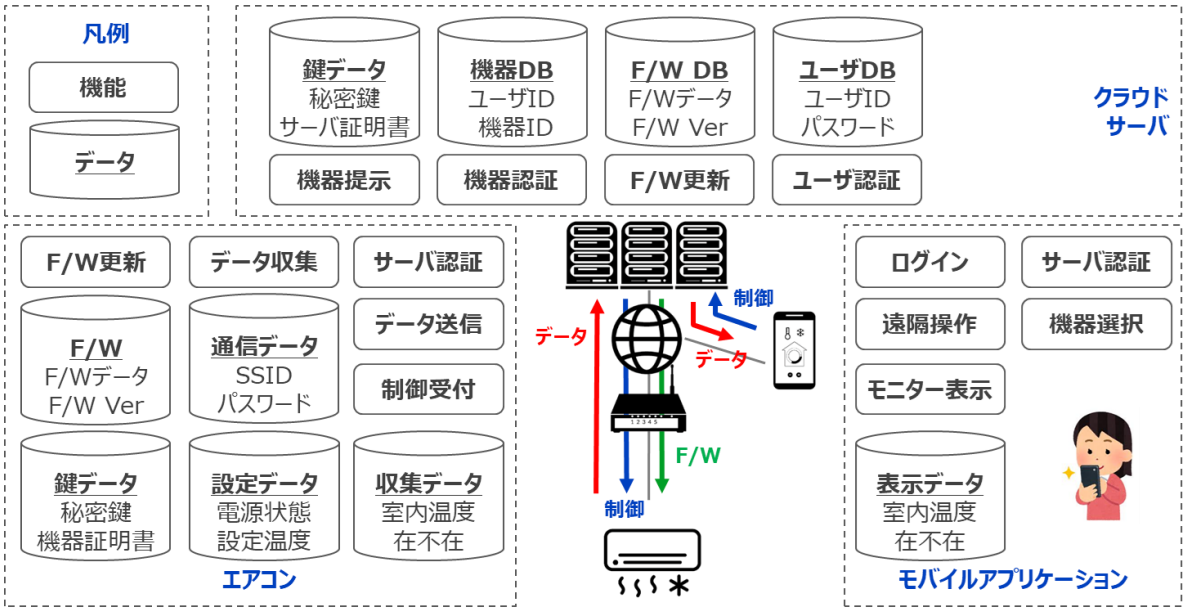


図 3-4 機能モジュールとデータベース構成図

3.1.3.1. エアコンの機能モジュールとデータベース構成

【機能モジュール】

1. **サーバ認証**:クラウドサーバとの通信において、通信相手となるクラウドサーバが正規のものであるかどうかを認証する。
2. **データ送信**:エアコンに設定されているデータや、各種センサから収集されるデータをクラウドサーバに送信する。
3. **制御受付**:クラウドサーバから通知される制御の指示を受け付け、実際にエアコンの ON/OFF や設定温度を変更する。
4. **データ収集**:**各種センサからデータを収集する。**
5. **ファームウェア更新**:定期的にクラウドサーバにファームウェア更新の有無を確認し、より新しいファームウェアが存在する場合には、クラウドサーバからファームウェアデータをダウンロードして、エアコンはファームウェアを更新する。(注:図ではファームウェアは F/W と略記する)

【データベース】

1. **ファームウェア:**ファームウェアデータそのものを保持するとともに、そのファームウェアのバージョン情報を保持する。
2. **通信データ:**宅内のホームルータとの接続に必要となる、SSID やパスワードなどの情報を保持する。
3. **鍵データ:**クラウドサーバとの暗号化通信で必要となる、秘密鍵や機器証明書を保持する。
4. **設定データ:**エアコンの動作に関わる、電源状態（ON/OFF）や設定温度などを保持する。
5. **収集データ:**エアコンに備えられた各種センサ類から収集される、室内温度や人の在不在などの情報を保持する。

3.1.3.2. モバイルアプリケーションの機能モジュールとデータベース構成

【機能モジュール】

1. **ログイン:**利用者からユーザ ID とパスワードの入力を受け付けて、クラウドサーバのシステムにログインする。
2. **サーバ認証:**クラウドサーバとの通信において、通信相手となるクラウドサーバが正規のものであるかどうかを認証する。
3. **機器選択:**クラウドサーバから利用者が保有する機器のリストを受信してこれを表示し、利用者から操作対象機器の選択を受け付ける。
4. **遠隔操作:**操作対象となるエアコンに対して、電源の ON/OFF や設定温度の変更を指示する。
5. **モニター表示:**操作対象となるエアコンについて、クラウドサーバ経由で人の在不在などの情報を収集し、その収集結果を表示する。

【データベース】

1. **表示データ:**モニター表示機能で必要となる、人の在不在などの情報をキャッシュとして一時保管する。

3.1.3.3. クラウドサーバの機能モジュールとデータベース構成

【機能モジュール】

1. **機器提示:**ログインした利用者のユーザ ID に対応する機器 ID のリストを取得し、操作対象機器選択のためにモバイルアプリケーションに提示する。
2. **機器認証:**エアコンとの通信において、通信相手となるエアコンが正規のものであるかどうか、さらにその機器 ID を認証する。
3. **ファームウェア更新:**エアコンからの問合せを受けてファームウェア更新の有無を通知するとともに、より新しいファームウェアがある場合には、これをエアコンに対して提供する。
4. **ユーザ認証:**利用者がモバイルアプリケーションで入力したユーザ ID とパスワードで認証する。

なお、クラウドサーバについては、図 3-4 では機能モジュールとしては図示していないものの、遠隔動作およびモニター機能についてエアコンとモバイルアプリケーションの間の通信を仲介する機能も有している。

【データベース】

1. **鍵データ:** エアコンとの暗号化通信で必要となる、秘密鍵やサーバ証明書を保持する。
2. **機器データベース:** 利用者が保持する機器について、ユーザ ID と機器 ID の組み合わせとして保持する。(注:図ではデータベースは DB と略記する)
3. **ファームウェアデータベース:** 最新のファームウェアについて、ファームウェアデータそのものを保持するとともに、そのバージョン情報を保持する。
4. **ユーザデータベース:** 利用者について、ユーザ ID とパスワードの組み合わせとして保持する。

3.2. 具体ユースケースにおけるセキュリティ脅威分析

本節では、3.1 節で示した具体ユースケースに対して、セキュリティ上の脅威を分析していく。

3.2.1. 保護するべき情報の抽出

本節では、セキュリティ上の脅威の分析に先立って、保護するべき情報資産についてリストアップする。ここでは、エアコン、モバイルアプリケーション、クラウドサーバにおけるデータベースにおいて取り扱われる情報資産に加えて、モバイルアプリケーション、クラウドサーバで一時的に取り扱われる情報資産も保護するべき情報資産としてリストアップする。

また、エアコンとクラウドサーバ、クラウドサーバとモバイルアプリケーションの間の通信経路を流れる情報資産についてもリストアップを行う。

3.2.1.1. エアコンに関わる情報資産

番号	情報資産の場所	情報資産の名称
1	ファームウェア	ファームウェアデータ
2		ファームウェアバージョン
3	通信データ	SSID
4		パスワード(ルータ接続用)
5	鍵データ	機器秘密鍵
6		機器証明書
7	設定データ	電源状態
8		設定温度
9	収集データ	室内温度
10		在不在

3.2.1.2. モバイルアプリケーションに関わる情報資産

番号	情報資産の場所	情報資産の名称
11	表示データ	室内温度
12		在不在
13	(入力される一時情報)	SSID
14		パスワード(ユーザ認証用)
15		電源状態(例:ON の指示)
16		設定温度(例:18 度に設定指示)

3.2.1.3. クラウドサーバに関わる情報資産

番号	情報資産の場所	情報資産の名称
17	鍵データ	サーバ秘密鍵
18		サーバ証明書
19	機器データベース	ユーザ ID
20		機器 ID
21	ファームウェアデータベース	ファームウェアデータ(最新版)
22		ファームウェアバージョン(最新版)
23	ユーザデータベース	ユーザ ID
24		パスワード(ユーザ認証用)
25	(遠隔制御仲介時の一時情報)	電源状態(例:ON の指示)
26		設定温度(例:18 度に設定指示)
27	(モニター機能仲介時の一時情報)	室内温度
28		在不在

3.2.1.4. エアコンとクラウドサーバの通信に関わる情報資産

番号	情報資産の場所	情報資産の名称
29	(クラウドサーバから	電源状態(例:ON の指示)
30	エアコンへの通信)	設定温度(例:18 度に設定指示)
31		サーバ証明書
32		ファームウェアデータ(最新版)
33		ファームウェアバージョン(最新版)
34	(エアコンから	室内温度
35	クラウドサーバへの通信)	在不在
36		機器証明書

3.2.1.5. クラウドサーバとモバイルアプリケーションの通信に関わる情報資産

番号	情報資産の場所	情報資産の名称
37	（モバイルアプリケーションから	ユーザ ID
38	クラウドサーバへの通信）	パスワード（ユーザ認証用）
39		電源状態（例：ON の指示）
40		設定温度（例：18 度に設定指示）
41	（クラウドサーバからモバイル	室内温度
42	アプリケーションへの通信）	在不在

3.2.2. アタックサーフェスと想定される脅威

本節では、3.1.2 節で示したネットワーク構成を踏まえて、攻撃可能なポイントをアタックサーフェスとしてリストアップする。さらに、その各々のアタックサーフェスにおいて、想定される脅威の分析を行う。

脅威の分析にあたっては、Microsoft が提唱した脅威分析手法である STRIDE モデルを一般社団法人 重要生活機器連携セキュリティ協議会が拡張した STRIDE + CCDS モデルを利用する。STRIDE モデルでは 6 種類の脅威（なりすまし、データ改ざん、否認、情報の暴露、サービス不能、権限昇格）が定義され、それらを用いてシステムに及ぼされる脅威を分析する。これを拡張した STRIDE＋CCDS モデルでは、IoT 機器・システムを想定し、さらに 5 種類の脅威（不正アクセス、マルウェア感染、踏み台、不正改造、未知の脆弱性）が追加されている。

なお、一般的にリアルタイム OS で動作することが多いスマートホーム向けの IoT 機器では、OS 部分とアプリケーション部分が一体化したファームウェアとしてソフトウェアが構成されるケースが一般的である。また場合によっては、OS を利用せずにメインループのみでファームウェアを開発するケースもある。このようなリアルタイム OS を利用するケースや OS を全く使用しないケースでは、Linux、Windows のようなマルチタスク OS で不正なアプリケーションプログラムが実行されるマルウェア感染は起こりえない。その代わりに、ファームウェア全体が不正に改ざんされて配布されるケースや、実装上の不具合を突いて遠隔から送り込まれたデータがプログラムとして実行されてしまう遠隔コード実行が脅威となる。このため、脅威分析においてマルウェア感染の分類では、リアルタイム OS で動作する、または OS を利用しない IoT 機器での不正ファームウェア配布や遠隔コード実行による脅威を含める。

さてまずは、アタックサーフェスについては、ネットワーク構成を踏まえて図 3-5 に示す 5 つの箇所を想定する。

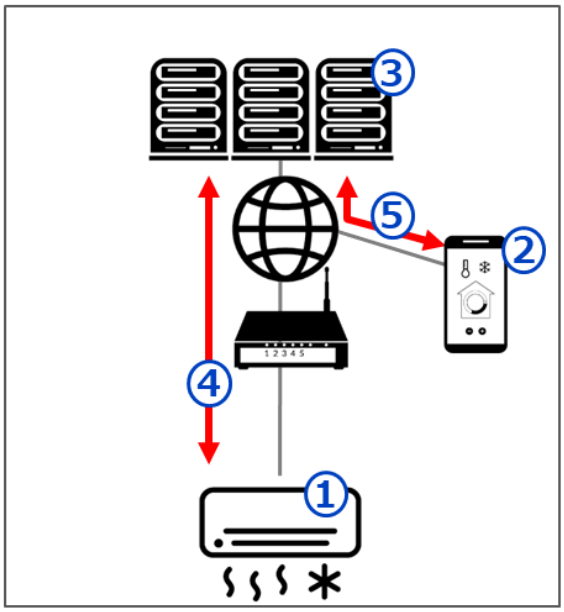


図 3-5 具体ユースケースで想定するアタックサーフェス

1. **エアコン**：IoT 機器そのものであり、攻撃の対象となり得る。
2. **モバイルアプリケーション**：IoT 機器を操作し、またその状態を確認するために利用するが、攻撃されることによってエアコンに対する不正な操作や、エアコンからの情報漏洩が起こりえる。
3. **クラウドサーバ**：ユーザ認証や機器認証も用いて、エアコンとモバイルアプリケーションの間の通信をセキュアに仲介するために利用するが、攻撃されることによってエアコンに対する不正な操作や、エアコンからの情報漏洩が起こりえる。
4. **エアコンとクラウドサーバ間の通信**：機器認証やサーバ認証も用いて制御の指示やアップロードされる収集データがセキュアに送受信されるが、改ざんや漏洩などの攻撃の対象となり得る。
5. **クラウドサーバとモバイルアプリケーションの間の通信**：ユーザ認証やサーバ認証も用いて制御の指示やアップロードされる収集データがセキュアに送受信されるが、改ざんや漏洩などの攻撃の対象となり得る。

3.2.2.1. エアコンに対する想定脅威

番号	脅威の分類	脅威の事例
1	データ改ざん	- エアコンの電源状態が書き換えられて、電源が勝手に OFF になってしまう。 - エアコンの設定温度が書き換えられて、暑い夏の日にエアコンが止まってしまう
2	情報の暴露	- エアコンの在不在の情報が漏洩する - エアコンの秘密鍵が漏洩する - エアコンに設定されている SSID・パスワードが漏洩する

3	マルウェア感染	- 不正なファームウェアが配布されて、正常なファームウェアが上書きされる - データ通信におけるデータ処理の不備を突いて、バッファオーバーフロー攻撃によって受信データの一部がコードとして実行される
4	なりすまし	- 秘密鍵、機器証明書の漏洩などにより、他の機器になりすまされる
5	不正アクセス	- 通信インタフェースなどから機器が不正にアクセスされる
6	踏み台	- 不正なファームウェアへの上書きなどによって、不正システムからの制御を受けて、他の機器への攻撃のために利用される

3.2.2.2. モバイルアプリケーションに対する想定脅威

番号	脅威の分類	脅威の事例
1	データ改ざん	- クラウドサーバを介してエアコンに送付される設定温度が書き換えられて、暑い夏の日にエアコンが止まってしまう
2	情報の暴露	- クラウドサーバを介してエアコンから収集される在不在の情報が漏洩する
3	マルウェア感染	- トロイの木馬などの手法で、ユーザ認証用のパスワード入力が盗まれる
4	なりすまし	- ユーザ ID やパスワードの漏洩などにより、他のユーザになりすまされる

3.2.2.3. クラウドサーバに対する想定脅威

番号	脅威の分類	脅威の事例
1	データ改ざん	- クラウドサーバを介してエアコンに送付される設定温度が書き換えられて、暑い夏の日にエアコンが止まってしまう - 機器データベースが改ざんされて、機器の所有者が不正攻撃者に書き換えられる
2	情報の暴露	- クラウドサーバを介してモバイルアプリケーションに送付される在不在の情報が漏洩する - ユーザデータベースに保存されているユーザ ID とパスワードが漏洩する
3	マルウェア感染	- クラウドサーバ自身がマルウェアに感染する - ファームウェアデータベースに保存されているファームウェアが不正に改ざんされる

4	なりすまし	-	秘密鍵、サーバ証明書の漏洩などにより、攻撃者によって正規サーバのようになりすまされる
5	不正アクセス	-	通信インタフェースなどからサーバが不正にアクセスされる
6	サービス不能	-	DoS 攻撃によって、クラウドサーバがダウンし、サービス提供が停止する

3.2.2.4. エアコンとクラウドサーバ間の通信に対する想定脅威

番号	脅威の分類	脅威の事例	
1	データ改ざん	-	通信経路上で、エアコンに送付される設定温度が書き換えられて、暑い夏の日にエアコンが止まってしまう
2	情報の暴露	-	通信経路上でエアコンから収集された在不在の情報が漏洩する
3	サービス不能	-	DoS 攻撃によって、エアコンとクラウドサーバ間の通信が阻害され、エアコンの電源 ON の制御指示が届かない
4	なりすまし	-	秘密鍵、サーバ証明書の漏洩などにより、他の機器になりすまされる

3.2.2.5. クラウドサーバとモバイルアプリケーション間の通信に対する想定脅威

番号	脅威の分類	脅威の事例	
1	データ改ざん	-	通信経路上で、クラウドサーバを介してエアコンに送付される設定温度が書き換えられて、暑い夏の日にエアコンが止まってしまう
2	情報の暴露	-	通信経路上でクラウドサーバを介してエアコンから収集された在不在の情報が漏洩する
3	サービス不能	-	DoS 攻撃によって、クラウドサーバとモバイルアプリケーション間の通信が阻害され、エアコンの電源 ON の制御指示が届かない
4	なりすまし	-	ユーザ ID やパスワードの漏洩などにより、他のユーザになりすましてログインされる

3.3. その他想定される脅威について

本節では、3.1 節で示した想定ユースケースでは現れないものの、スマートホーム向けの IoT 機器として特有の事情で想定しておくべき脅威について示していく。

3.3.1. 機器の初期ネットワーク設定

IoT 機器の利用開始にあたっては、ネットワーク設定が必要となることがある。Ethernet など有線接続であれば、一般的にはネットワーク設定は特に必要ない。一方で、Wi-Fi や Thread などの無線接続においては、SSID / XPANID とパスワードの設定が必要となる。このような初期ネットワーク設定作業は、住設機器では設置事業者が専用治具などを用いて行うこともある。一方で、利用者自らが量販店などで購入することが一般的な家電機器では、一般の利用者自らが初期ネットワーク設定を行うことが多い。

さて、スマートホーム分野の IoT 機器では、テレビなど一部の例外を除いて設定用のユーザインタフェースを持っていない。このため、SSID / XPANID とパスワードの設定は、WPS (Wi-Fi Protected Setup)などの方式を利用して実施される。更に近年では、モバイルアプリケーションを利用することで、より安全かつより判りやすく初期ネットワーク設定を行う方法が提供されている。

例えば、スマートホーム業界のグローバル標準規格である Matter では QR コードを用いた初期ネットワーク設定が導入されている。Matter 対応のモバイルアプリケーションでは、まず最初に IoT 機器に添付された QR コードをスキャンする。この QR コードには IoT 機器のモデル情報などに加えて、認証用のパスコードが含まれている。モバイルアプリケーションと IoT 機器のあいだでは、BLE (Bluetooth Low Energy)を用いて通信を行うが、この中でパスコードを用いての認証と鍵交換 (PAKE：Passcode Authentication and Key Exchange)を実施する。こうして確立された暗号通信経路上で、モバイルアプリケーションで入力された SSID / XPANID とパスワードが安全に IoT 機器側に通知される。

この機器の初期ネットワーク設定もアタックサーフェスとなりえる。例えば一部の IoT 機器では、電源投入と同時に BLE を用いた初期ネットワーク設定が開始される仕様となっており、万が一このような IoT 機器において添付されている QR コードが漏洩した場合には、BLE 通信が届く範囲内からであれば攻撃者が IoT 機器の初期ネットワーク設定を実施し、IoT 機器を自由に操作することが可能となる。

3.3.2. カスタマーエンジニアなどによるメンテナンス対応

冷蔵庫や洗濯機などの大型家電機器、またエアコン等住宅設備として取り付けられる機器では、販売店や機器メーカなどでの持ち込み修理は難しい。スマートホーム分野での IoT 機器が普及するにつれて、修理の前の事前状況確認や、一部ソフトウェアレベルでのメンテナンスについてはネットワーク経由で実施するケースが増えてきている。

これは、3.2.2.1 節で論じたエアコンに対する想定脅威の一部であるが、一般的な通信のためのインタフェースではなく、遠隔管理者用に特別な通信ポート・通信方式を用意している場合には注意が必要となる。

3.3.3. 不要ポート

スマートホーム分野の IoT 機器では、レコーダや HEMS (Home Energy Management System) ゲートウェイ機器など一部の例外を除いて、サーバとして機能することはない。このため、FTP (20 番)、SSH (22 番)、SMTP (25 番)や HTTP (80 番)などのシステムポートは閉じられていることが一般的である。

万が一、これらのシステムポートが開いていると、これがアタックサーフェスとして攻撃者に利用されかねない。なお、レコーダや HEMS ゲートウェイ機器のようにサーバとして機能する機器であっても、本当に必要なシステムポート以外は閉じておくべきなことは言うまでもない。

3.3.4. 製品廃棄・譲渡時の残存データ漏洩

昨今業務用 PC など IT の分野では、製品の廃棄時には HDD の論理的・物理的破壊など、データも修復不可能とすることが求められている。同様に、スマートホーム分野の IoT 機器についても、利用者が廃棄する際や他の利用者に譲渡する際には、残存データを消去するための仕組みが求められる。

なお、スマートホーム分野の IoT 機器では、利用者自身が廃棄を行うことを前提として、取扱説明書などで残存データの消去方法を説明するとともに、特殊な工具などは必要とせず、一般的な利用者でも対応可能な方法で消去が可能であることが求められる。

3.3.5. 未知の脆弱性

スマートホーム分野に限らず、昨今ソフトウェアのコードサイズが肥大化する IoT 製品共通の課題であるが、バグを完全に根絶した状態で製品を出荷することは難しい。また、製品の出荷後に採用する通信・暗号方式やオープンソースソフトウェアに脆弱性が判明するリスクを想定しておく必要がある。

3.4. 脅威への対策の基本方針

特定分野システムの IoT 製品における JC-STAR 制度活用ガイドでは、③IoT 製品類型に対する脅威分析の中で、1) 守るべき資産、 2) アタックサーフェス、 3) 脅威や守るべき資産との関係性、について整理するように求めている。

この節では、3.2 節で示した具体ユースケースにおけるセキュリティ脅威分析、また 3.3 節で示した IoT 機器特有の事情で考慮しておくべきその他の脅威を踏まえて、この整理を行う。

3.4.1. 想定する守るべき資産

表 3-1 に、全ての IoT 機器で共通の JC-STAR★1 で想定する守るべき資産と対比する形式で、スマートホーム分野★2 向けに想定する守るべき資産を示す。

表 3-1 想定する守るべき資産

IoT 製品において守るべき資産	★1 で想定する守るべき資産	スマートホーム分野★2 で想定する守るべき資産
1. IoT 機能 機器やシステムが IoT につながるための機能	・ 有線通信機能 ・ 無線通信機能	・ 有線通信機能 ・ 無線通信機能
2. 本来機能 「モノ」本来の機能、セキュリティ対策・セーフティ対策のための機能	・ セキュリティ機能	・ セキュリティ機能 ・ 制御指示
3. 情報 ユーザの個人情報、収集情報、各機能の設定情報など	・ 通信機能に関する設定情報 ・ セキュリティ機能に関する設定情報 ・ 機器の意図する使用において、機器が収集し、保存又は通信する、個人情報等の一般的に機密性が高い情報	・ 通信機能に関する設定情報 ・ セキュリティ機能に関する設定情報 ・ 機器が保存又は通信する、動作情報およびセンサ収集情報 ・ ユーザに関する設定情報 ・ 機器の初期ネットワーク設定情報 ・ 機器のファームウェア
4. その他の物理的資産 ユーザの健康・生命や IoT 機器が内蔵する物理的資産	－	－

以下、スマートホーム分野★2 向けの整理におけるポイントを記載する。

- ★1 で想定する守るべき資産をベースとして整理する。
- セーフティ対策を含む「モノ」本来の機能は対象外とするが、ネットワーク経由で送受信される「制御指示」については守るべき対象とする。スマートホーム分野で取り扱う IoT データ（機器の動作情報や、センサ収集情報）、およびこれらを加工したデータにおけるプライバシーの感じ方は人や時代によって変わり、機密性のレベル付けができないため、機器で取り扱う動作情報やセンサ収集情報は全て守るべき対象とする。
- ユーザ個人に関する設定情報に加え、機器の初期ネットワーク設定に関わる情報、機器のファームウェア自身も守るべき対象として 3. 情報の中に特記する。

3.4.2. 想定するアタックサーフェス

まずは図 3-6 に、JC-STAR★1 で想定するアタックサーフェスを特定分野システムの IoT 製品における JC-STAR 制度活用ガイドから引用する。

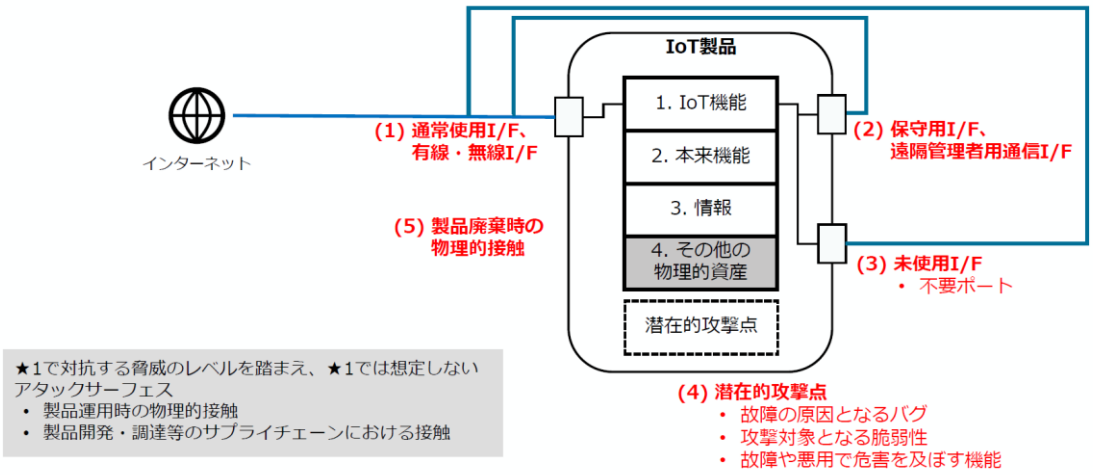


図 3-6 JC-STAR★1 で想定するアタックサーフェス

これを踏まえて対比する形式で、図 3-7 にスマートホーム分野★2 で想定するアタックサーフェスを示す。なお、ここでのアタックサーフェスは、3.2.2 節におけるアタックサーフェスとしてのエアコンについて、さらにインタフェース毎に詳細化したものとなる。

以下、スマートホーム分野★2 向けの整理におけるポイントを記載する。

- ★1 で想定するアタックサーフェスをベースとして整理する。
- ★1 と同様に、製品運用時の物理的接触や、製品開発・調達等のサプライチェーンにおける接触はアタックサーフェスとして想定しない。

- 通常インタフェースに加えて保守用インタフェースを含め、スマートホーム分野の IoT 機器を利用する利用者自身による悪用はアタックサーフェスとして想定しない。
- 3.3.1 節で示した、機器の初期ネットワーク設定に関わる機能についてもアタックサーフェスとして特記する。

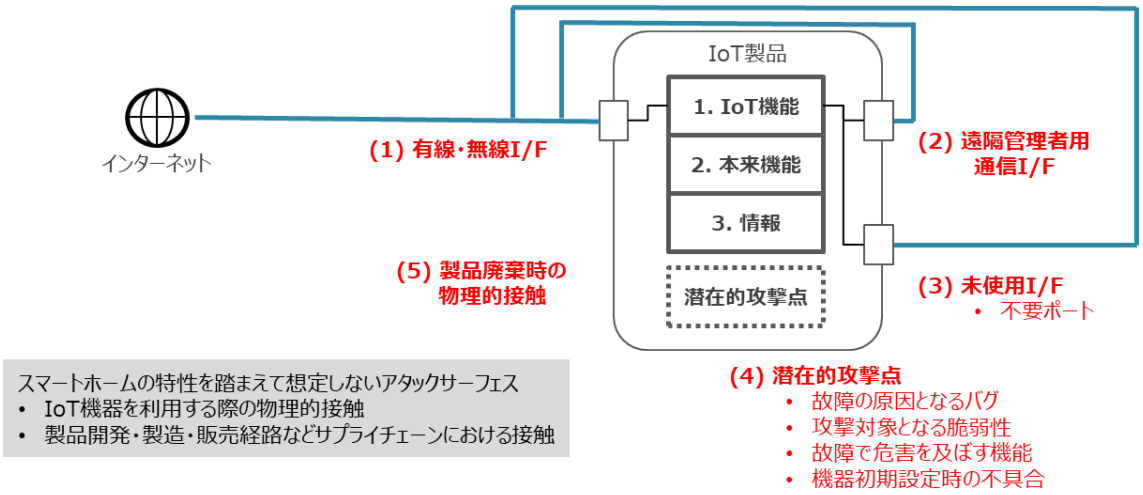


図 3-7 スマートホーム★2 で想定するアタックサーフェス

3.4.3. 想定される脅威

まずは図 3-8 に、JC-STAR★1 で想定される脅威を特定分野システムの IoT 製品における JC-STAR 制度活用ガイドから引用する。

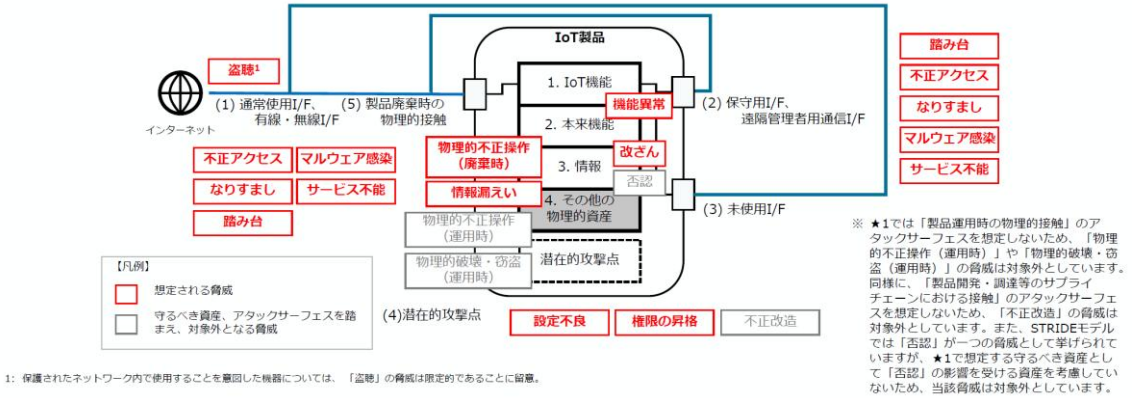


図 3-8 JC-STAR★1 で想定される脅威

これを踏まえて対比する形式で、図 3-9 にスマートホーム分野で想定される脅威を示す。

以下、スマートホーム分野向けの整理におけるポイントを記載する。

- ★1 で想定される脅威をベースとして整理する。
- ★1 と同様に、スマートホーム IoT 機器を利用する際の物理的接触をアタックサーフェスとして想定しないため、物理的な脅威（物理的不正操作、物理的破壊・窃盗、不正改造）は対象外とする。
- スマートホーム IoT 機器では、一般的にセキュリティに関する権限の概念がないため、権限の昇格や否認は対象外としている。なお、電気錠では、常時施錠・解錠が可能な居住者自身と、一時的にのみ施錠・解錠ができる訪問者（訪問介護員など）のようなケースがあるが、これは施錠・解錠機能が利用可能な条件の差異に基づくものであり、システム管理者と一般ユーザのようなセキュリティに関する権限とは異なる。
- マルウェア感染については、リアルタイム OS で動作することが多いスマートホーム IoT 機器の特性を踏まえて、不正ファームウェア配布と遠隔コード実行として記載する。

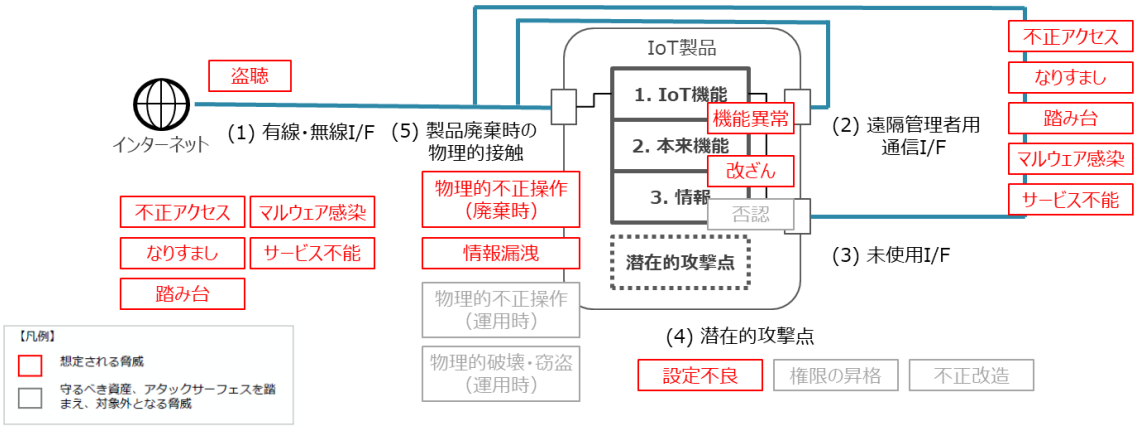


図 3-9 スマートホームで想定される脅威

さらに図 3-10 に、JC-STAR★1 で想定される脅威と守るべき資産との関係性を特定分野システムの IoT 製品における JC-STAR 制度活用ガイドから引用する。

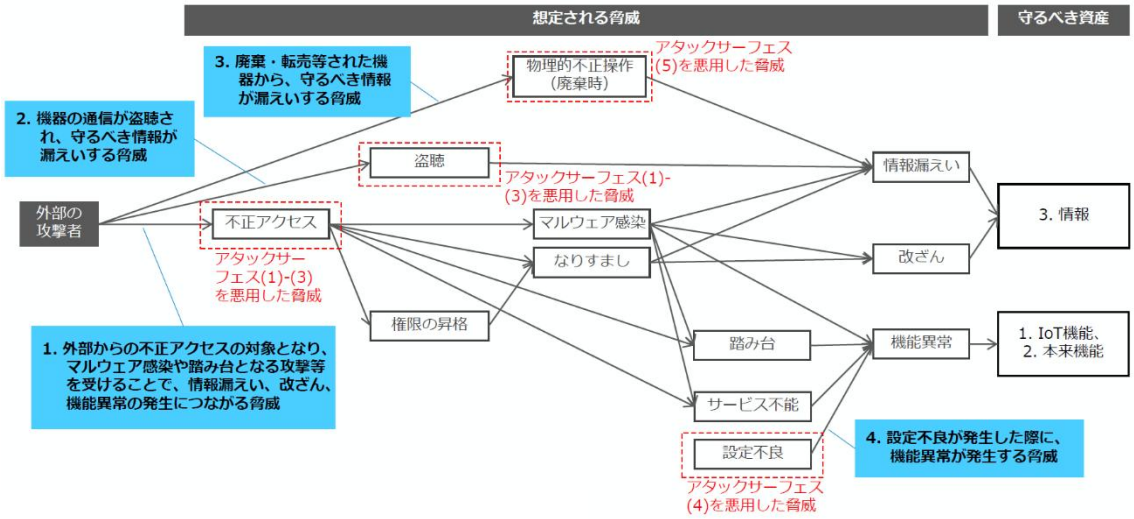


図 3-10 JC-STAR★1 で想定される脅威と守るべき資産との関係性

これを踏まえて対比する形式で、図 3-11 にスマートホーム分野で想定される脅威と守るべき資産との関係性を示す。

以下、スマートホーム分野向けの整理におけるポイントを記載する。

- スマートホーム IoT 機器の利用者自身による攻撃を想定しないため、ネット経由の攻撃者として明確化する。ただし、廃棄・転売等における攻撃は想定するため、このアタックサーフェスを想定して外部の攻撃者も残す。なお、以前の所有者が無自覚に、または悪意を持って機器の設定情報を残しておき、新たな所有者がその設定情報を初期化しなかった場合などには、以前の所有者による攻撃が考えられる。このような攻撃はネット経由の攻撃者による不正アクセス、なりすましと考えられる。
- スマートホーム IoT 機器では一般的に権限の概念がないため、想定される脅威において、権限の昇格を対象外とする。
- 制御指示が改ざんされることによって、IoT 機器としての本来機能が誤動作するリスクを示すために、想定される脅威である改ざんから、守るべき資産である本来機能に対する矢印を追加する。

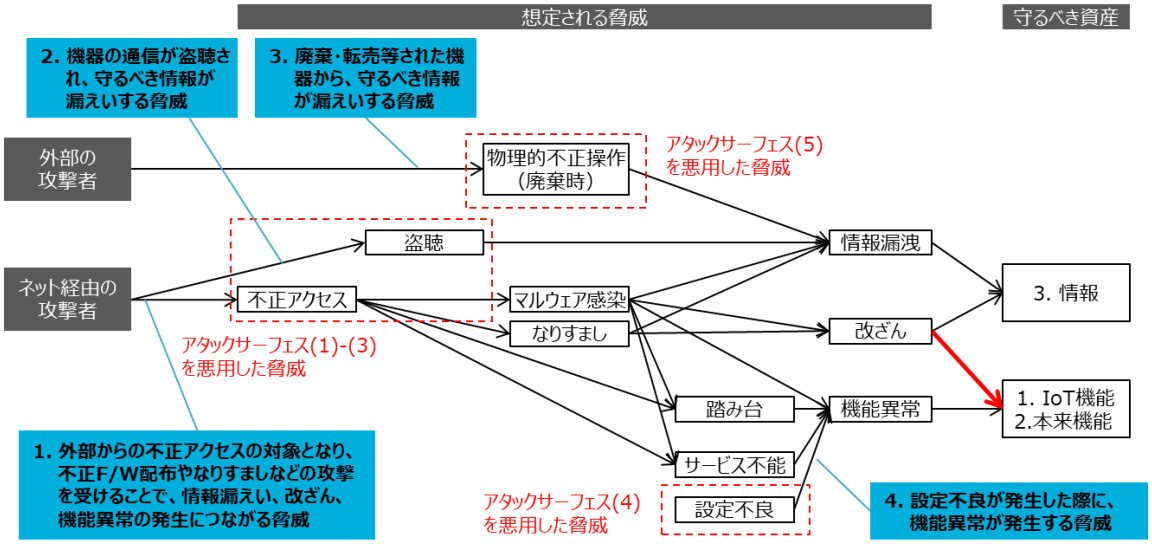


図 3-11 スマートホームで想定される脅威と守るべき資産との関係性

3.4.4. セキュリティ対策の基本方針

これまで、本章では具体ユースケースを想定してセキュリティ脅威分析を実施し、これを踏まえてスマートホーム分野における、1）守るべき資産、 2）アタックサーフェス、 3）脅威や守るべき資産との関係性、についての整理を進めてきた。

本章の締めくくりにあたって、スマートホーム分野におけるセキュリティ対策の基本方針としては以下を提示しておきたい。4 章以降では、この基本方針を踏まえて具体的なセキュリティ要件を規定していく。

スマートホーム IoT 機器、対応するモバイルアプリケーション、クラウドサービス、およびこれらを繋ぐ通信経路上において（以上、アタックサーフェス）、スマートホーム IoT 機器で取り扱う IoT データ、スマートホーム IoT 機器に対する制御指示、およびスマートホーム IoT 機器のファームウェア（以上、守るべき資産）を保護する。

このために、以下三項目をセキュリティ対策の基本方針とする。

- IoT 機器の通信経路を保護する
- IoT 機器のストレージを保護する
- IoT 機器のファームウェアを保護する

4. スマートホーム向け IoT 製品に求めるセキュリティ要件

IoT 機器は、例えばエアコンや洗濯機・冷蔵庫、電動シャッターや照明機器のように、単体で機器本来の機能を持つとともに、何らかのネットワークインタフェースを備えるものである。いっぽうで、2.1 節で示したスマートホームのネットワーク構成や、3.1 節で示した具体ユースケースで見たように、IoT 機器単体で利用されるわけではなく、モバイルアプリケーションやクラウドサービス[1]と組み合わせて利用されることもある。このように、スマートホーム向け IoT 製品は、IoT 機器とその必須付随サービスであるモバイルアプリケーションやクラウドサービスと組み合わせて利用されるケースもある。

さて、本書はスマートホーム向けの IoT 製品について、セキュリティ要件を定めるものである。いっぽうで、IoT 機器に対して求められるセキュリティ要件と、その必須付随サービスであるモバイルアプリケーションやクラウドサービスに求められるセキュリティ要件は、重複する内容もあれば、大きく異なるものものある。

3.4 節では IoT 機器に対して想定するアタックサーフェスや、想定される脅威を示した。これらの脅威に対策するための技術要件は IoT 機器特有のものとして、本章において提示していく。他方、モバイルアプリケーションやクラウドサービスにおける脅威に対策するための技術要件は大きく異なる。これは、組込向けの LSI でリアルタイム OS を利用することが一般的でハードウェアによるセキュリティ保護機構が重要な IoT 機器と、汎用 CPU で一般的なマルチタスク OS を利用することが一般的でソフトウェアによるセキュリティ対策が重要なモバイルアプリケーションやクラウドサービスで、考え方が大きく異なるためである。

なお、モバイルアプリケーションや、クラウドサービスにおけるセキュリティ対策はスマートホーム分野に限らず、各分野での共通的な課題となっている。このため、具体的な対策要件については、モバイルアプリケーションでは日本スマートフォンセキュリティ協会策定の「モバイルアプリケーション開発者の実施規範」、クラウドサービスでは経済産業省 商務情報政策局 情報セキュリティ政策室策定の「クラウドセキュリティガイドライン 活用ガイドブック （2013 年度版）」や総務省策定の「クラウドサービス提供における情報セキュリティ対策ガイドライン（第 3 版）」を参照されたい。

一方で、利用者に対する説明の方法や、開発プロセスにおけるセキュリティ観点での運用規定、脆弱性への対応方法については、IoT 機器での対応だけではなく、モバイルアプリケーションやクラウドサービスなどの必須付随サービスでも共通的に対応していくべきものである。このため、本書でも運用に関わるセキュリティ要件については、表 4-1 に示すとおり必須付随サービスにも適用していく。

表 4-1 IoT 機器と必須付随サービスに求められるセキュリティ要件

	IoT 機器	必須付随サービス
技術要件	本書で規定する	本書では対象外
運用要件	本書で規定する	本書で規定する

[1] JC-STAR★1 では必須付随サービスの一例として、物理的なサーバ実体を含まない「クラウドコンピューティング／ストレージ」としているが、本書では 2.1 節で示したネットワーク構成の類型で用いたクラウドサーバとの記載を踏まえて「クラウドサービス」と記載する。

また巻末の付録 2 に、以降で示す各要件について、技術要件・運用要件のいずれに分類されるか、また対象が IoT 機器のみなのか必須付随サービスであるモバイルアプリケーションやクラウドサービスも対象となるかについて表として整理する。

4.1. セキュリティ要件の策定方法

本節では、スマートホーム分野向けのセキュリティ要件の策定方法について説明する。要件策定にあたってベースとした文章は、経済産業省 産業サイバーセキュリティ研究会 ワーキンググループ 3 IoT 製品に対するセキュリティ適合性評価制度構築に向けた検討会の最終とりまとめにて、別添 1 として提示された全 101 項目のセキュリティ要件一覧である。この要件一覧は、ETSI EN 303 645 、NISTIR 8425 、EU CRA 、端末設備等規則等の国内外のセキュリティ要件の集合関係を踏まえ、重ね合わせの関係にあるセキュリティ要件の全体リストを整理したもの（いわゆるロングリスト）である。

まず、JC-STAR★1 は全ての IoT 機器共通に適用されるべきセキュリティ要件であることを鑑みて、JC-STAR★1 で該当するとした 25 項目については、スマートホーム分野向けのセキュリティ要件としても準ずるべきであるとした。なお、JC-STAR★1 は全ての IoT 機器共通のものとして策定されたセキュリティ要件であるため、スマートホーム分野向けとして要件の内容を考えた場合には、解釈が難しいケースもあった。このため、4.2 節において、スマートホーム分野向けとして必要となる補足を行っていく。

続いて、3.4.4 節で示したセキュリティ対策の基本方針である「通信経路の保護」「ストレージの保護」「ファームウェアの保護」に関連する 38 項目（JC-STAR★1 で該当の 12 項目を含む）を抽出した。具体的には、表 4-2 に示すように、セキュリティ要件のカテゴリ毎に、各基本方針との関連性を見て該当有無を判断した。

表 4-2 カテゴリ毎、基本方針毎の抽出結果

カテゴリ	通信経路の保護	ストレージの保護	ファームウェアの保護
3. ソフトウェアを最新の状態に保つ	-	-	関連する
4. 機密セキュリティパラメータをセキュアに保存する	-	関連する	-
5. セキュアに通信する	関連する	-	-
7. ソフトウェアの完全性を確実にする	-	-	関連する
8. 個人データがセキュアであることを確実にする	関連する	関連する	-
11. ユーザが簡単にデータを消去できるようにする	-	関連する	-

最後に、こうして得られた JC-STAR★1 で非該当の 26 項目のうちから、将来的な制度の国際連携を見据え、国際的に広く活用されている ETSI EN 303 645 の基準において必須（Mandatory）となっている以下の 6 項目をスマートホーム分野★2 において追加されるべき要件として抽出した。（各項目冒頭の番号は、上記ロングリストで付与されている要件番号）

- 4-2. ハードコードされた機器ごとに固有の ID がセキュリティ目的で製品で使用される場合、物理的、電気的、又はソフトウェアなどの手段による改ざんに耐えられるように実装しなければならない。
- 4-3. 製品のソフトウェアのソースコードにハードコードされた重要なセキュリティパラメータを使用してはならない。
- 4-4. ソフトウェアアップデートの完全性及び真正性チェック、及び製品のソフトウェアにおける関連サービスとの通信の保護に使用される重要なセキュリティパラメータは、機器ごとに固有でなければならず、製品のクラスに対する自動化された攻撃のリスクを低減するメカニズムで生成されるものとしなければならない。
- 5-8. 製造業者は、製品に関連する重要なセキュリティパラメータについて、セキュアな管理プロセスに従わなければならない。
- 8-2. 機器と関連サービス間で通信される機密の個人データの機密性は、技術の特性と使用法に適した暗号技術によって保護されなければならない。
- 8-3. 製品のすべての外部感知機能は、ユーザにとって明確で透明性のあるアクセス可能な方法で文書化されなければならない。

4.1.1. 策定方法以外でのセキュリティ要件の補遺

スマートホーム SWG では、4.1 節に示した方法でセキュリティ要件の一次案を策定したが、改めてロングリストを分析した結果、「【米国 NISTIR 8425】サイバーセキュリティの状態認識」については、攻撃やその兆候に関わるログの保存という要件としてはリストアップされておらず、「7. ソフトウェアの完全性を確実にする」「10. システムのテレメトリデータを検証・保護する」との要件とのみ対応づけられていることが判明した。

専門の管理者が常時監視を行うことが望ましい商用 IT システムやネットワークシステムとは異なり、一般の利用者が用いるスマートホーム向けの機器では、管理者による監視は望み得ない。このため、攻撃に関わりうるログの保存と、そのアップロード、必要に応じての専門家によるログ解析が重要となる。

このため、NIST IR 8425 の要件である「Cyber Security State Awareness」について、特に攻撃やその兆候に関わるログの保存という観点で、スマートホーム分野でのセキュリティ要件として追加する。

4.2. ★1 に準ずるセキュリティ要件

本節では、4.1 節に示した策定方法において★1 に準じて★2 でも求められるとしたセキュリティ要件について、スマートホーム分野向けとして必要となる具体的な要件についての補足を行う。このため、4.2.x.1 の各小節では★1 における要件を参考とし

て引用し、4.2.x.2 の各小節でスマートホーム分野における背景を説明する。そのうえで、4.2.x.3 の各小節でスマートホーム分野★2 における要件を示す。

なお、セキュリティ要件に基づいて、適合基準および評価ガイドを策定するにあたっては、★1 での適合基準及び評価ガイドをベースとしつつも、スマートホーム向けとしての再検討が求められる。

4.2.1. 要件 1-1 （運用要件）

4.2.1.1. ★1 における要件

【カテゴリ】

汎用のデフォルトパスワードを使用しない

【要件】

パスワードが使用され、工場出荷時のデフォルト以外の状態にある製品において、すべてのパスワードは、機器ごとに固有であるか、又はユーザによって定義されるものでなければならない。

4.2.1.2. スマートホーム分野における要件に関する補足

スマートホーム向けの IoT 機器は、キーボードやタッチパネルなどのユーザインタフェースを持たないことが多い。このため、必須付随サービスとしてのモバイルアプリケーションで、利用者がユーザ ID とパスワードを入力し、IoT 機器またはクラウドサービスでユーザ認証を行うことが一般的である。

一方で、ネットワーク接続設定など IoT 機器の初期設定は、対応するモバイルアプリケーションを用いて実施することが一般的であり、この際には IoT 機器とモバイルアプリケーションのあいだでパスワードやパスコードを利用した認証が行われる。この際の認証としては、例えば IoT 機器が Wi-Fi のアクセスポイントモードとして動作し、SSID とパスワードを利用して接続してくるモバイルアプリケーションとのあいだで WPA（Wi-Fi Protected Access）を用いて認証する方法がある。また、他の例としては Bluetooth Low Energy における LE Secure Connection でのペアリングにおいて、IoT 機器に予め設定されたパスコードと、IoT 機器に添付されるシールや同梱されるドキュメントで示されるパスコードをモバイルアプリケーションで入力して、相互にパスコード認証を行う方法などがある。

4.2.1.3. スマートホーム分野★2 における要件

【機器の要件】

パスワード（アクセスポイントモードとして動作する際のパスワードを含む）またはパスコードが使用され、工場出荷時のデフォルト以外の状態にある IoT 機器において、すべてのパスワードまたはパスコードは、IoT 機器ごとに固有であるか、又はユーザによって定義されるものでなければならない。

【クラウドサービスの要件】

クラウドサービスで IoT 機器のユーザの認証のためにパスワードが使用される場合、パスワードはユーザによって定義されるものでなければならない。

4.2.2. 要件 1-2 （技術要件）

4.2.2.1. ★1 における要件

【カテゴリ】

汎用のデフォルトパスワードを使用しない

【要件】

プリインストールされた固有のパスワードを使用する場合、自動化された攻撃への耐性をもつために、パスワードは十分なランダム性を保有しなければならない。

4.2.2.2. スマートホーム分野における要件に関する補足

4.2.1.2 節で補足したように、キーボードやタッチパネルなどのユーザインタフェースを持たないスマートホーム向けの IoT 機器では、ユーザ認証は行われないことが多い。一方で、IoT 機器の初期ネットワーク接続設定時にはパスワードやパスコードを利用した認証が行われる。

なお、パスコードについては、入力の容易性を鑑みて、一般的には数字 6 桁以上とされている。また、表示手段に制限がある場合などで数字 6 桁以上の入力が難しい場合には、他の手段も利用される。

4.2.2.3. スマートホーム分野★2 における要件

【機器の要件】

IoT 機器でプリインストールされた固有のパスワードまたはパスコードを使用する場合、自動化された攻撃への耐性をもつために、パスワード・パスコードは十分なランダム性を保有しなければならない。

4.2.3. 要件 1-3 （技術要件）

4.2.3.1. ★1 における要件

【カテゴリ】

汎用のデフォルトパスワードを使用しない

【要件】

製品に対してユーザを認証するために使用される認証メカニズムは、製品用途の特性等に適した想定するリスクを低減できる技術を使用していなければならない。

4.2.3.2. スマートホーム分野における要件に関する補足

4.2.1.2 節で補足したように、キーボードやタッチパネルなどのユーザインタフェースを持たないスマートホーム向けの IoT 機器では、ユーザ認証は行われないことが多い。一方で、IoT 機器の初期ネットワーク接続設定時にはパスワードやパスコードを利用した認証が行われる。

4.2.3.3. スマートホーム分野★2 における要件

【機器の要件】

IoT 機器に対してユーザを認証するために使用される認証メカニズム、および IoT 機器の初期ネットワーク設定時に IoT 機器と設定用モバイルアプリケーションとのあいだで利用される認証メカニズムは、製品用途の特性等に適した想定するリスクを低減できる技術を使用していなければならない。

4.2.4. 要件 1-4 （運用要件）

4.2.4.1. ★1 における要件

【カテゴリ】

汎用のデフォルトパスワードを使用しない

【要件】

製品に対するユーザ認証において、製品は使用される認証値を変更するためのシンプルなメカニズムを、ユーザ又は管理者に提供しなければならない。

4.2.4.2. スマートホーム分野における要件に関する補足

4.2.1.2 節で補足したように、キーボードやタッチパネルなどのユーザインタフェースを持たないスマートホーム向けの IoT 機器では、ユーザ認証は行われないことが多いことに注意する必要がある。

4.2.4.3. スマートホーム分野★2 における要件

【機器の要件】

IoT 機器に対するユーザ認証がある場合には、IoT 機器は使用される認証値を変更するためのシンプルなメカニズムを、ユーザ又は管理者に提供しなければならない。

【モバイルアプリケーションの要件】

モバイルアプリケーションを入力手段とするユーザ認証において、モバイルアプリケーションは使用される認証値を変更するためのシンプルなメカニズムを、ユーザ又は管理者に提供しなければならない。

4.2.5. 要件 1-5 （技術要件）

4.2.5.1. ★1 における要件

【カテゴリ】

汎用のデフォルトパスワードを使用しない

【要件】

機器が、制約のある機器ではない場合、ネットワークを介して行われる認証に対する総当たり攻撃等のブルートフォース攻撃が実行できないようにするメカニズムを保有しなければならない。

4.2.5.2. スマートホーム分野における要件に関する補足

特になし。

4.2.5.3. スマートホーム分野★2 における要件

【機器の要件】

IoT 機器が、制約のある機器ではない場合、ネットワークを介して行われる認証に対する総当たり攻撃等のブルートフォース攻撃が実行できないようにするメカニズムを保有しなければならない。

4.2.6. 要件 2-1 （運用要件）

4.2.6.1. ★1 における要件

【カテゴリ】

脆弱性の報告を管理するための手段を導入する

【要件】

製造業者は、脆弱性開示ポリシーを公開しなければならない。このポリシーには、少なくとも以下が含まれていなければならない

・問題を報告するための連絡先情報

・以下のタイムラインに関する情報

1) 最初の受領確認

2) 報告された問題が解決されるまでの状況の更新

4.2.6.2. スマートホーム分野における要件に関する補足

スマートホーム向けの IoT 機器は、IoT 機器単体ではなく必須付随サービスとしてのモバイルアプリケーションやクラウドサービスとともに利用されることが多い。脆弱性については、必ずしも IoT 機器だけに発生するものではなく、モバイルアプリケーショ

ンやクラウドサービスにも発生しうる。このため、本要件については、スマートホーム分野★2 では必須付随サービスについても適用されるべきである。

また、スマートホーム向けの IoT 機器は製造業者自身のブランドで直接、または販売店を通じて一般の利用者に販売されるケースもあれば、製造業者とは別の事業者のブランドで販売されるケースもある。例えば、ハウスメーカが機器メーカから製品を購入し、ハウスメーカのブランドとしてスマートホームシステム全体を提供するようなケースがある。この例では、一般の利用者に対して脆弱性情報を直接的に開示することとなるのは、ハウスメーカである。このため、★1 における要件で記載されている製造業者は、IoT 機器や必須付随サービスの提供事業者と読み替えられるべきである。

なお、IoT 機器の提供事業者が脆弱性情報を開示するためには、製造業者もまた IoT 機器の提供事業者に対して脆弱性情報を開示する必要がある。

4.2.6.3. スマートホーム分野★2 における要件

【機器の要件】

IoT 機器の提供事業者は、IoT 機器に関する脆弱性開示ポリシーを公開しなければならない。このポリシーには、少なくとも以下が含まれていなければならない

・問題を報告するための連絡先情報

・以下のタイムラインに関する情報

1) 最初の受領確認

2) 報告された問題が解決されるまでの状況の更新

【モバイルアプリケーションの要件】

IoT 機器の提供事業者がモバイルアプリケーションを提供する場合には、提供事業者はモバイルアプリケーションの脆弱性開示ポリシーを公開しなければならない。このポリシーには、少なくとも以下が含まれていなければならない

・問題を報告するための連絡先情報

・以下のタイムラインに関する情報

1) 最初の受領確認

2) 報告された問題が解決されるまでの状況の更新

【クラウドサービスの要件】

IoT 機器の提供事業者がクラウドサービスを提供する場合には、提供事業者はクラウドサービスの脆弱性開示ポリシーを公開しなければならない。このポリシーには、少なくとも以下が含まれていなければならない

・問題を報告するための連絡先情報

・以下のタイムラインに関する情報

1) 最初の受領確認

2) 報告された問題が解決されるまでの状況の更新

4.2.7. 要件 3-1 （技術要件）

4.2.7.1. ★1 における要件

【カテゴリ】

ソフトウェアを最新の状態に保つ

【要件】

製品に含まれる特定のソフトウェアコンポーネントについて、アップデート可能にしなければならない。

4.2.7.2. スマートホーム分野における要件に関する補足

スマートホームにおける IoT 機器は、クラウド上のサービスに接続する機能を備えるため、外部からの不正なアクセスなどの危険に晒される環境に置かれている。このため、IoT 機器では、外部との通信をつかさどる通信モジュールに関しては、不正な侵入を許さないためのソフトウェア開発を行い、アップデートによる不正アクセス防止に対応していく必要がある。

このため、IoT 機器側にはその通信モジュール内のハードウェア部分に、信頼できる接続先から、最新の不正アクセスに対応したファームウェアをダウンロード、または外部メモリなどからインストールを行い、必要最低限のメモリ空間をアップデートしていく仕組みが必要不可欠となる。

4.2.7.3. スマートホーム分野★2 における要件

【機器の要件】

IoT 機器のクラウド上のサービスに接続する機能をつかさどる通信モジュールのファームウェアについて、アップデート可能にしなければならない。

4.2.8. 要件 3-2 （技術要件）

4.2.8.1. ★1 における要件

【カテゴリ】

ソフトウェアを最新の状態に保つ

【要件】

機器が、制約のある機器でない場合、アップデートをセキュアにインストールするためのアップデートメカニズムを備えていなければならない。

4.2.8.2. スマートホーム分野における要件に関する補足

スマートホームにおけるIoT機器は、クラウド上のサービスに接続する機能を備えるため、外部からの不正なアクセスなどの危険に晒される環境に置かれている。このため製造業者は既知の攻撃に対し、様々なセキュリティ対策を行い出荷するが、今日、クラウドを通した様々な攻撃は常に新たなものが現れており、購入時のままでは安全な状態を維持できないことになる。また、このセキュリティ対策ソフトウェアは外部から不正なプログラムをインストールされないように、信頼される手段をもってセキュアにインストールするための仕組みが必要となる。

このため、スマートホームにおけるIoT機器は、クラウドからの新たな攻撃に関して対策を行なったIoT機器の通信モジュールファームウェアを、クラウド、あるいはモバイルアプリケーションや外部メモリなどから、セキュアにアップデートする機能を持っていなければならない。

4.2.8.3. スマートホーム分野★2における要件

【機器の要件】

IoT機器が、制約のある機器でない場合、通信モジュールファームウェアのアップデートをセキュアにインストールするためのアップデートメカニズムを備えていなければならない。

4.2.9. 要件 3-3 （運用要件）

4.2.9.1. ★1における要件

【カテゴリ】

ソフトウェアを最新の状態に保つ

【要件】

製品においてアップデートメカニズムが実装されている場合、そのアップデートは、ユーザが簡単に適用できるものでなければならない。

4.2.9.2. スマートホーム分野における要件に関する補足

スマートホームにおけるIoT機器には、表示画面を持ち、IoT機器本体の操作でアップデート可能な機器のほか、表示画面を持たず操作ボタンも数少なく、外部機器を利用してアップデートを行う機器など様々なバリエーションがある。そのためIoT機器本体のキー操作でアップデートを行うには、機器の仕様に応じて、音や表示などでその操作をガイドするなど、ユーザが簡単に操作できる仕様が望ましい。また、外部メモリなどの外部媒体を挿入する場合は、その接続位置がアップデート操作を妨げない位置に配置するなどの配慮が必要となる。

また、モバイルアプリケーションを利用したアップデートでは、最新アップデート情報があることの告知やその内容を明確にし、ユーザが理解しやすい操作でアップデートを遠隔で行える配慮が望ましい。

スマートホームにおけるIoT機器のアップデート操作に関しては機器の本来の役割を妨げてはならず、実施前にユーザへの告知や、許諾を得る形態が望ましい。自動的にアップデートする方法を使う場合は、特にその事前告知などの配慮や許諾が重要となる。

4.2.9.3. スマートホーム分野★2における要件

【機器の要件】

IoT機器において通信モジュールのファームウェアアップデートメカニズムが実装されている場合、そのアップデートは、ユーザが簡単に適用できるものでなければならない。

4.2.10. 要件 3-7 （技術要件）

4.2.10.1. ★1における要件

【カテゴリ】

ソフトウェアを最新の状態に保つ

【要件】

製品においてアップデートメカニズムが実装されている場合、セキュアなアップデートメカニズムを容易にするために、ベストプラクティスの暗号技術を使用しなければならない。

4.2.10.2. スマートホーム分野における要件に関する補足

スマートホーム向けIoT機器で、通信モジュールのファームウェアアップデートをセキュアに行う場合、その実現には、暗号化技術が求められる。しかしながらIoT機器には、高性能なSoCが搭載されていることは稀であるため、その機器の用途、価格などのバランスを考慮した最適な暗号化技術を選択する必要がある。特に住宅設備機器や生活家電等、利用期間が長いIoT機器においては、特に将来を見据えた暗号強度を採用することや、暗号化技術の更新に対応できる設計が望ましい。

4.2.10.3. スマートホーム分野★2における要件

【機器の要件】

IoT機器において通信モジュールのファームウェアアップデートメカニズムが実装されている場合、セキュアなアップデートメカニズムを容易にするために、ベストプラクティスの暗号技術を使用しなければならない。

4.2.11. 要件 3-8 （運用要件）

4.2.11.1. ★1 における要件

【カテゴリ】

ソフトウェアを最新の状態に保つ

【要件】

製品においてアップデートメカニズムが実装されている場合、セキュリティアップデートは、適時でなければならない。

4.2.11.2. スマートホーム分野における要件に関する補足

スマートホーム向け IoT 機器は他の機器同様、攻撃の踏み台となる可能性があり、脆弱性情報のレベル、リスクに応じて適時通信モジュールのファームウェアアップデート対応を行うことが求められる。脆弱性が見つかるなどアップデートが必要なった場合は、リスク回避のためなるべく早い段階でアップデートを行う必要性がある。

すなわち、IoT 機器のセキュリティに関するソフトウェアの最新情報を常時ユーザが確認できるほか、本体やモバイルアプリケーションなどから、その必要性をユーザに明確に知らせることが必要となる。重大なセキュリティ課題が発生した際には、IoT 機器の通信モジュールのファームウェアの更新を強く促す配慮が必要となる。ユーザの事前了承を得て、自動アップデートを行うなどの仕様は、最適な手段と言える。

そのため、IoT 機器の提供事業者は、常に通信モジュールにおける脆弱性情報を確認し、対策必要なファームウェアアップデートの必要がある場合はなるべく早く市場に対策ファームを提供できるよう、体制を事前に整えておく必要性がある。最新アップデート情報の公開方法に関しても明確にユーザに告知しておくことが望ましい。

4.2.11.3. スマートホーム分野★2 における要件

【機器の要件】

IoT 機器において通信モジュールファームウェアのアップデートメカニズムが実装されている場合、セキュリティアップデートは、適時でなければならない。

4.2.12. 要件 3-10 （技術要件）

4.2.12.1. ★1 における要件

【カテゴリ】

ソフトウェアを最新の状態に保つ

【要件】

製品においてアップデートメカニズムが実装され、ソフトウェアアップデートがネットワークインタフェースを介して配信される場合、製品は、信頼関係を介して各アップデートの真正性及び完全性を検証しなければならない。

4.2.12.2. スマートホーム分野における要件に関する補足

スマートホームにおける IoT 機器で、通信モジュールのファームウェアアップデートがネットワークインタフェースを介して行う場合、ユーザが確実に自分の利用する IoT 機器と認識出来る状況で接続を行った、信頼できるクラウドサーバ、モバイルアプリケーションなど、それらのサービスやアプリから機器状況の確認、ファームウェアアップデートの必要性確認、アップデート操作を行えることが重要となる。

4.2.12.3. スマートホーム分野★2 における要件

【機器の要件】

IoT 機器においてアップデートメカニズムが実装され、ソフトウェアアップデートがネットワークインタフェースを介して配信される場合、IoT 機器は、信頼関係を介して各アップデートの真正性及び完全性を検証しなければならない。

4.2.13. 要件 3-14 （運用要件）

4.2.13.1. ★1 における要件

【カテゴリ】

ソフトウェアを最新の状態に保つ

【要件】

製品のモデル名称は、製品上のラベル又は物理的インタフェースを介して、ユーザに対して明確に認識可能でなければならない。

4.2.13.2. スマートホーム分野における要件に関する補足

スマートホーム向けの IoT 機器の通信モジュールファームウェアアップデートは、複数の同種の機器が存在する場合、また接続設定をユーザ以外に、IoT 機器の設置事業者やメンテナンス業者によって行われる場合があるため、アップデートする IoT 機器に対応したソフトウェアを正確にアップデートできるように、アップデート対象となる IoT 機器のモデル名称、及びアップデートソフトウェアのファイル名を誤認識しないよう、明確に識別可能とする必要がある。

また、スマートホーム向けの IoT 機器は、ユーザが容易に確認できない場所に設置される場合がある。このため、必須付随サービスとしてのモバイルアプリケーションやウェブ UI で、製品情報を確認できることが望ましい。

さらに、複数の同種の機器がある場合は、その他の区別できる記号を付加表示する手段を用意する事が望ましい。（例：Wi-Fi の MAC アドレス等）

4.2.13.3. スマートホーム分野★2 における要件

【機器の要件】

IoT 機器のモデル名称は、IoT 機器上のラベル又は物理的インタフェースを介して、ユーザに対して明確に認識可能でなければならない。

4.2.14. 要件 4-1 （技術要件）

4.2.14.1. ★1 における要件

【カテゴリ】

機密セキュリティパラメータをセキュアに保存する

【要件】

製品のストレージにある機密セキュリティパラメータは、製品によってセキュアに保存されなければならない。

4.2.14.2. スマートホーム分野における要件に関する補足

製品のストレージにおいて、機密セキュリティパラメータとして守るべき情報資産は、3.4.1 節で提示したとおり、以下の四種類である。なお、ファームウェアについては、4.2.12 節で別途論じているため、ここでは守るべき情報資産から割愛する。

- 通信機能に関する設定情報
- セキュリティ機能に関する設定情報
- 機器が保存する、動作情報またはセンサ収集情報
- ユーザに関する設定情報
- 機器の初期ネットワーク設定情報

なお、IoT 機器での処理の都合上、一時的にキャッシュやメモリ等に保存する情報資産については、処理終了後又は合理的期間経過後の自動消去するなどのセキュリティ対策を実施することを条件として、守るべき情報資産の対象外となる。

4.2.14.3. スマートホーム分野★2 における要件

【機器の要件】

IoT 機器のストレージにある守るべき情報資産は、IoT 機器によってセキュアに保存されなければならない。

4.2.15. 要件 5-1 （技術要件）

4.2.15.1. ★1 における要件

【カテゴリ】

セキュアに通信する

【要件】

製品は、ベストプラクティスの暗号技術を使用してセキュアに通信をしなくてはならない。

4.2.15.2. スマートホーム分野における要件に関する補足

スマートホーム向け IoT 機器では、クラウドとの通信、あるいは機器との通信において、セキュアに通信を行う必要があり、その実現には、暗号化技術が求められる。しかしながら IoT 機器には、高性能な SoC が搭載されていることは稀であるため、その機器の用途、価格などのバランスを考慮した最適な暗号化技術を選択する必要がある。住宅設備機器や生活家電等、利用期間が長い IoT 機器においては、特に将来を見据えた暗号強度を採用することや、暗号化技術の更新に対応できる設計が望ましい。

4.2.15.3. スマートホーム分野★2 における要件

【機器の要件】

IoT 機器は、ベストプラクティスの暗号技術を使用してセキュアに通信をしなくてはならない。

4.2.16. 要件 5-5 （技術要件）

4.2.16.1. ★1 における要件

【カテゴリ】

セキュアに通信する

【要件】

ネットワークインタフェースを介してセキュリティに関連する設定の変更を可能にする製品の機能は、認証後にのみアクセス可能でなければならない。ただし、製品が依存するネットワークサービスプロトコルで、製品の動作に必要な設定を製造業者が保証できない場合は、例外とする。

4.2.16.2. スマートホーム分野における要件に関する補足

スマートホーム向け IoT 機器では、クラウドとの通信、あるいは他の機器との通信においてセキュアに通信を行うが、そのセキュリティに関する設定は決められた内容で使用される場合が多く、セキュリティに関する設定を変更する機能は無いか、限定された範囲である事がほとんどである。 さらに、それら設定であっても、IoT 機器単体ではなく必須付随サービスとしてのモバイルアプリケーションで行う場合もある。

そのため、セキュリティに関連する設定の変更を可能にする機能は、不正アクセスを防ぎ、システムの安全性を確保するため、認証状態を適切に管理し、認証後にのみアクセス可能となるよう保護が必要である。

そこで、スマートホーム向け IoT 機器のセキュリティに関連する設定の変更では、次のポイントに留意し信頼性を確保し、実装することが必要である。

・ セキュリティ機能のエンフォースメント:

設定変更に関するポリシーやルールを IoT 機器の通信モジュールソフトウェアレベルで強制することで、ユーザが意図しない変更を行うリスクを減少させる

- リカバリ機能:
  設定変更が不正に行われた場合やアップデート処理が異常となった場合に備えて、設定を元に戻せる機能の実装

4.2.16.3. スマートホーム分野★2 における要件

【機器の要件】

ネットワークインタフェースを介してセキュリティに関連する設定の変更を可能にする IoT 機器の設定変更機能は、認証後にのみアクセス可能でなければならない。ただし、IoT 機器が依存するネットワークサービスプロトコルで、IoT 機器の動作に必要な設定を製造業者が保証できない場合は、例外とする。

4.2.17. 要件 5-7 （技術要件）

4.2.17.1. ★1 における要件

【カテゴリ】

セキュアに通信する

【要件】

ネットワークインタフェースを介してセキュリティに関連する設定の変更を可能にする製品は、リモートアクセス可能なネットワークインタフェースを介して通信される重要なセキュリティパラメータの機密性を保護しなければならない。

4.2.17.2. スマートホーム分野における要件に関する補足

スマートホーム向け IoT 機器では、クラウドとの通信、あるいは機器との通信においてセキュアに通信を行うが、そのセキュリティに関する設定は決められた内容で使用される場合が多く、セキュリティに関する設定を変更する機能は無いか、限定された範囲である事がほとんどである。その上で、ネットワークインタフェースを通して、これらの設定を変更する場合、必須付随サービスとしてのモバイルアプリケーションとの間の通信でのみ実施され、その通信では、重要なセキュリティパラメータの機密性を保護する必要がある。

4.2.17.3. スマートホーム分野★2 における要件

【機器の要件】

ネットワークインタフェースを介してセキュリティに関連する設定の変更を可能にするスマートホーム向け IoT 機器では、リモートアクセス可能なネットワークインタフェース

を介して通信される重要なセキュリティパラメータの機密性を保護しなければならない。

4.2.18. 要件 6-1 （技術要件）

4.2.18.1. ★1 における要件

【カテゴリ】

露出した攻撃面を最小化する

【要件】

すべての未使用の物理的インタフェース及び論理的インタフェースは無効化しなければならない。

4.2.18.2. スマートホーム分野における要件に関する補足

スマートホーム向け IoT 機器では、クラウドとの通信機能と、宅内での機器間通信機能の両方をもつ機器があり、宅内通信機能を使用しない場合は、宅内通信用システムポートは閉じ、逆にクラウドとの通信を使用しない場合は、クラウドとの通信用システムポートは閉じるなどの措置を講じ、使用する事を判定する期間を除き、常時、未使用のシステムポートが開いていることのないようにする必要がある。

また、スマートホーム向け IoT 機器の開発段階において TCP・UDP ポートや USB ポートでのアクセスを開発目的で使用することがあり、また、サービス・メンテナンスのためにこのようなアクセスが可能な機器もある。このような場合は、IoT 機器出荷時にはこれらのポートを無効化することが必要となる。

4.2.18.3. スマートホーム分野★2 における要件

【機器の要件】

IoT 機器では、すべての未使用の物理的インタフェース及び論理的インタフェースは無効化しなければならない。

4.2.19. 要件 9-1 （運用要件）

4.2.19.1. ★1 における要件

【カテゴリ】

停止に対してレジリエントなシステムにする

【要件】

データネットワークと電源の停止の可能性を考慮して、レジリエンスを製品とサービスに組み込まなければならない。

4.2.19.2. スマートホーム分野における要件に関する補足

スマートホーム向け IoT 機器では、データネットワークの切断や、電源の停止からの復帰時には自動的にサービスを再開させる必要がある。ネットワーク切断中もスマートホーム対応機器は、正常に動作し、復帰時にはクラウドと自動的に同期をとり、サービスに支障が発生しないように対応する。通信途中にネットワーク切断や電源切断がされた場合は、本体側に直前までの必要な情報を保存しておき、復旧時に再送するなどの配慮された設計が望ましい。

4.2.19.3. スマートホーム分野★2 における要件

【機器の要件】

IoT 機器では、データネットワークと電源の停止の可能性を考慮して、レジリエンスを製品とサービスに組み込まなければならない。

【クラウドサーバの要件】

IoT 機器の提供事業者は、必須付随サービスであるクラウドサーバに関してデータネットワークの停止の可能性を考慮して、レジリエンスをサーバに組み込まなければならない。

4.2.20. 要件 11-1 （技術要件）

4.2.20.1. ★1 における要件

【カテゴリ】

ユーザが簡単にデータを消去できるようにする

【要件】

ユーザが、簡単な方法で製品からユーザデータを消去できるような機能を提供されなければならない。

4.2.20.2. スマートホーム分野における要件に関する補足

スマートホーム向け IoT 機器が保持するセキュリティ上の設定値、機密情報、プライバシー情報等の削除機能を実装していない、もしくは消去の方法が複雑であった場合、廃棄時やリユース時に機密情報やセキュリティ設定値、プライバシー情報などが漏洩する可能性がある。スマートホーム分野では、IoT 機器の提供・設定サービス等複数事業者が関わる機会が多いと考えられることから、ユーザのみならず設置事業者が簡単に機器・アプリ・クラウドの関連情報を消去できることが求められる。

4.2.20.3. スマートホーム分野★2 における要件

【機器の要件】

IoT 機器の提供事業者は、ユーザや設置事業者等が簡単な方法で IoT 機器のユーザデータを消去できるような手段を提供しなければならない。

4.2.21. 要件 17-2 （運用要件）

4.2.21.1. ★1 における要件

【カテゴリ】

製品に関する情報提供を行う

【要件】

製造業者は、製品をセキュアに設定・利用・廃棄する方法について、ユーザに提供しなければならない。

4.2.21.2. スマートホーム分野における要件に関する補足

脅威の背景として、機器やアプリケーションが保持するセキュアな設定・利用・廃棄のための機能を有していても、その情報提供が行われない場合、機密情報やセキュリティ設定値、プライバシー情報などが漏洩する可能性がある。スマートホーム分野では、IoT 機器の提供・設定サービス等、複数事業者が関わる機会が多いと考えられることから、ユーザや設置事業者等が簡単に機器・アプリ・クラウドの設定・利用・廃棄方法を把握できることが求められる。

たとえば、

・安全に利用できる手順を設置事業者等に明示することや製品のソフトウェア更新の内容や必要性、更新を行わない場合の影響などを設置事業者等へ周知すること想定される事故や障害に対して、免責事項を設置事業者等へ周知すること

・機器のサポート期限・終了方針を設置事業者等に通知すること

・機器内にデータが残留したまま廃棄することで想定されるリスクや、データ消去を含む機器の安全な廃棄方法を設置事業者等に周知すること

などがある

4.2.21.3. スマートホーム分野★2 における要件

【機器の要件】

IoT 機器の提供事業者は、IoT 機器をセキュアに設定・利用・廃棄する方法について、ユーザや設置事業者に提供しなければならない。

【モバイルアプリケーションの要件】

IoT 機器の提供事業者は、必須付随サービスとしてのモバイルアプリケーションをセキュアに設定・利用・削除する方法について、ユーザや設置事業者に提供しなければならない。

4.2.22. 要件 17-3 （運用要件）

4.2.22.1. ★1 における要件

【カテゴリ】

製品に関する情報提供を行う

【要件】

アップデートメカニズムが実装されている場合、製造業者は、セキュリティアップデートが必要であることを、そのアップデートによって軽減されるリスクに関する情報とともに、認識可能で明らかな方法でユーザに通知しなければならない。

4.2.22.2. スマートホーム分野における要件に関する補足

IoT 機器の提供事業者は、IoT 機器にセキュティティアップデートが必要な場合、アップデートの重要性/免責事項やサポート情報を適切な方法で通知出来ることが必要となる。もしくは、アップデートの内容をクラウドサーバないしはモバイルアプリケーション上で確認することを促す表示を行わなければならない。その場合、想定される事故や障害に対して、免責事項を利用者へ提供しなければならない。

また、対象機器やサービスのサポート期限やサポート終了時の方針をユーザや設置事業者に通知しなければならない。

さらに、IoT 機器の提供事業者は、ユーザインタフェース上の通知又は電子メールを介して、アップデートが必要であることをユーザや設置事業者に通知するなどをおこなう。

4.2.22.3. スマートホーム分野★2 における要件

【機器の要件】

IoT 機器の提供事業者は、IoT 機器にセキュリティアップデートが必要であることを、そのアップデートによって軽減されるリスクに関する情報とともに、認識可能で明らかな方法でユーザや設置事業者に通知しなければならない

4.2.23. 要件 17-5 （運用要件）

4.2.23.1. ★1 における要件

【カテゴリ】

製品に関する情報提供を行う

【要件】

製造業者は、ユーザが製品を廃棄する手順について、指定された方法でユーザに提供しなければならない。

4.2.23.2. スマートホーム分野における要件に関する補足

機器内にデータが残留したまま廃棄することで想定されるリスクや、データ消去を含む機器の安全な廃棄方法をユーザや設置事業者へ周知しなければならない。

IoT 機器の提供事業者は、IoT 機器や、IoT 機器に付随するモバイルアプリケーション、クラウドサーバにおいて、データが残留したまま、IoT 機器を廃棄することで想定されるリスクと合わせ、データ消去方法をアプリ UI もしくはマニュアル等で周知しなければならない。

4.2.23.3. スマートホーム分野★2 における要件

【機器の要件】

IoT 機器の提供事業者は、ユーザが IoT 機器を廃棄する手順について、指定された方法でユーザや設置事業者に提供しなければならない。

【モバイルアプリケーションの要件】

IoT 機器の提供事業者は、ユーザが IoT 機器を廃棄する場合のモバイルアプリケーションのデータを削除する手順について、指定された方法でユーザや設置事業者に提供しなければならない。

4.2.24. 要件 17-8 （運用要件）

4.2.24.1. ★1 における要件

【カテゴリ】

製品に関する情報提供を行う

【要件】

製造業者は、定められたサポート期間を、ユーザにとって明確で透明性のある方法で公表しなければならない。

4.2.24.2. スマートホーム分野における要件に関する補足

製品を購入する際、ユーザへはその製品のソフトウェアアップデートのサポート期間を明確に伝えることが必要である。ユーザがその製品をいつまで安心してネットワークに接続して使用し続けることが出来るか確認できるようにしておくことはセキュリティを確保する上で重要である。

例えば、製品上のユーザインタフェースを介して、もしくは製品に具備された QR コードなどのタグをスキャンすることでその製品のソフトウェアアップデートのサポート期間を確認できること等の方法が考えられる。

4.2.24.3. スマートホーム分野★2 における要件

【機器の要件】

IoT 機器の提供事業者は、自らが定めたサポート期間を、ユーザや設置事業者にとって明確で透明性のある方法で公表しなければならない

【モバイルアプリケーションの要件】

IoT 機器の提供事業者は、必須付随サービスであるモバイルアプリケーションの自ら定めたサポート期間を、ユーザや設置事業者にとって明確で透明性のある方法で公表しなければならない

【クラウドサーバの要件】

IoT 機器の提供事業者は、必須付随サービスであるクラウドサーバの定められたサポート期間を、ユーザや設置事業者にとって明確で透明性のある方法で公表しなければならない

4.2.25. 要件 17-10 （運用要件）

4.2.25.1. ★1 における要件

【カテゴリ】

製品に関する情報提供を行う

【要件】

製造業者は、セキュリティリスクを引き起こす可能性がある製品の利用状況に関する情報について、指定された方法でユーザに提供しなければならない。

4.2.25.2. スマートホーム分野における要件に関する補足

ユーザや設置事業者がスマートホーム向け IoT 機器で、セキュリティに関わる機器やモバイルアプリケーションやサービスの設定を行う場合には、安全に使用するための設定方法や使用方法をユーザや設置事業者に明示することが求められる。

また、製品を使用する上で想定される事故や障害および免責事項について消費者に明示することが求められる。

たとえば、初期設定の方法など、利用上、サイバーセキュリティを確保するための設定や使用方法について、安全に利用できる手順をユーザや設置事業者に明示しなければならない。

あるいは、想定される事故や障害に対して、免責事項をユーザや設置事業者へ明示しなければならない。さらに、製造業者またはサービス提供主体は、サポート終了後に機器やサービスを使い続ける場合のリスク（新たな脆弱性が修正されないなど）について、ユーザや設置事業者へ周知しなければならない。その際、継続利用する場

合のオフライン化・買い替え・廃棄などの選択肢や対策方法を案内することが望ましい。

4.2.25.3. スマートホーム分野★2 における要件

【機器の要件】

IoT 機器の提供事業者は、セキュリティリスクを引き起こす可能性がある IoT 機器の利用状況に関する情報について、明確な方法でユーザや設置事業者に提供しなければならない。

【モバイルアプリケーションの要件】

IoT 機器の提供事業者は、セキュリティリスクを引き起こす可能性があるモバイルアプリケーションの利用状況に関する情報について、指定された方法でユーザや設置事業者に提供しなければならない。

【クラウドサーバの要件】

IoT 機器の提供事業者は、セキュリティリスクを引き起こす可能性があるクラウドサーバの利用状況に関する情報について、指定された方法でユーザや設置事業者に提供しなければならない。

4.3. ★2 で追加するセキュリティ要件

本節では、4.1 節に示した策定方法においてスマートホーム向けとして★2 で新たに追加するセキュリティ要件について説明する。このため、4.3.x.1 の各小節ではロングリストにおける要件を参考として引用し、4.3.x.2 の各小節でスマートホーム分野における背景を説明する。そのうえで、4.3.x.3 の各小節でスマートホーム分野★2 における要件を示す。

なおこれらのセキュリティ要件は、★1 では存在しないものであり、新たに適合基準および評価ガイドの検討が必要となる。

4.3.1. 要件 4-2 （技術要件）

4.3.1.1. ロングリストにおける要件

【カテゴリ】

機密セキュリティパラメータをセキュアに保存する

【要件】

ハードコードされた機器ごとに固有の ID がセキュリティ目的で製品で使用される場合、物理的、電気的、及びソフトウェアなどの手段による改ざんに耐えられるように実装しなければならない。

4.3.1.2. スマートホーム分野における要件に関する補足

スマートホーム分野の IoT 機器には複数種類の固有 ID が付与されることがある。製造番号は固有 ID の一例である。また、クラウドサービスとの通信用に機器証明書が付与されている場合には、この証明書が X.509v3 形式である場合に記載されている Certificate Serial Number や Common Name が固有 ID に該当する。

機器証明書を改ざんやなりすましから保護するためには、機器証明書に署名を付与するとともに、機器証明書に記載される公開鍵に対応する秘密鍵を漏洩や改ざんから保護する必要がある。秘密鍵は、例えばセキュアな OTP（One Time Programable）領域に格納するなどして、物理的、電気的、又はソフトウェアによる漏洩や改ざんに耐えられるように実装されることが多い。

なお、3.4.2 節で論じたとおり、製品運用時の物理的接触や、製品開発・調達等のサプライチェーンにおける接触はアタックサーフェスとして想定しない一方で、製品廃棄時の物理的接触はアタックサーフェスとして想定する。このため、ソフトウェアによる改ざんに加えて、物理的又は電気的な手段による改ざん、および改ざんに伴う他の機器へのなりすましについて耐えられる必要がある。

4.3.1.3. スマートホーム分野★2 における要件

【機器の要件】

ハードコードされた IoT 機器ごとに固有の身元情報がセキュリティ目的で IoT 機器で使用される場合、物理的、電気的、又はソフトウェアなどの手段による改ざんに耐えられるように実装しなければならない。

4.3.2. 要件 4-3 （技術要件）

4.3.2.1. ロングリストにおける要件

【カテゴリ】

機密セキュリティパラメータをセキュアに保存する

【要件】

製品のソフトウェアのソースコードにハードコードされた重要なセキュリティパラメータを使用してはならない。

4.3.2.2. スマートホーム分野における要件に関する補足

スマートホーム分野の IoT 機器で利用される重要なセキュリティパラメータの一例は、クラウドサービスなどとの通信において利用される機器固有の秘密鍵である。また、初期ネットワーク設定時に IoT 機器がアクセスポイントモードで動作する際のパスワードも重要なセキュリティパラメータに該当する。

こうした重要なセキュリティパラメータがソースコードの中にハードコードされると、容易に解析されてしまうこととなる。また、単純な難読化（obfuscation）や暗号化をしたとしても、容易に解析されてしまうことが知られている。このためソースコードには、重要なセキュリティパラメータを記載してはならない。

4.3.2.3. スマートホーム分野★2 における要件

【機器の要件】

IoT 機器のソフトウェアのソースコードに重要なセキュリティパラメータをハードコードしてはならない。

4.3.3. 要件 4-4 （技術要件）

4.3.3.1. ロングリストにおける要件

【カテゴリ】

機密セキュリティパラメータをセキュアに保存する

【要件】

ソフトウェアアップデートの完全性及び真正性チェック、及び製品のソフトウェアにおける関連サービスとの通信の保護に使用される重要なセキュリティパラメータは、機器ごとに固有でなければならず、製品のクラスに対する自動化された攻撃のリスクを低減するメカニズムで生成されるものとしなければならない。

4.3.3.2. スマートホーム分野における要件に関する補足

IoT 機器とモバイルアプリケーションやクラウドサービスなど必須付随サービスとの通信、あるいは IoT 機器間での通信を保護するためには、通信経路において機器認証を行ったうえで暗号化通信を行うことが求められる。この際に IoT 機器側で保持する機器証明書および対応する秘密鍵が固有であることを本要件は求めている。

ソフトウェアアップデートの完全性及び真正性をチェックするためには、ファームウェアに公開鍵暗号方式による署名を付与しておき、IoT 機器側では公開鍵を用いて署名検証を行うことで完全性及び真正性をチェックすることが一つの方法である。この場合には、IoT 機器側で用いる公開鍵は、IoT 機器毎に固有にするべき重要セキュリティパラメータに該当しないことに注意されたい。これ以外の方法でソフトウェアアップデートの完全性及び真正性をチェックする場合には、その際に利用する重要なセキュリティパラメータは機器毎に固有で無ければならない。

4.3.3.3. スマートホーム分野★2 における要件

【機器の要件】

ファームウェアアップデートの完全性及び真正性チェック、及びモバイルアプリケーションやクラウドサービスなど必須付随サービスとの通信の保護に使用される重要なセキュリティパラメータは、IoT 機器ごとに固有でなければならず、IoT 機器のクラスに対する自動化された攻撃のリスクを低減するメカニズムで生成されるものとしなければならない。

4.3.4. 要件 5-8 （運用要件）

4.3.4.1. ロングリストにおける要件

【カテゴリ】

セキュアに通信する

【要件】

製造業者は、製品に関連する重要なセキュリティパラメータについて、セキュアな管理プロセスに従わなければならない。

4.3.4.2. スマートホーム分野における要件に関する補足

重要なセキュリティパラメータの管理プロセスについては、標準のセキュアな管理プロセスが推奨される。

4.3.4.3. スマートホーム分野★2 における要件

【機器の要件】

IoT 機器の提供事業者は、IoT 機器に関連する重要なセキュリティパラメータについて、セキュアな管理プロセスに従わなければならない。

4.3.5. 要件 8-2 （技術要件）

4.3.5.1. ロングリストにおける要件

【カテゴリ】

個人データがセキュアであることを確実にする

【要件】

機器と関連サービス間で通信される機密の個人データの機密性は、技術の特性と使用法に適した暗号技術によって保護されなければならない。

4.3.5.2. スマートホーム分野における要件に関する補足

保護すべき情報資産が特定されており、不正なアクセスや変更からの保護対策が行われていることが求められる。

IoT 機器やモバイルアプリケーション、クラウドサーバにおいて、ストレージ領域へ保存される情報資産については、不正なアクセスや変更から保護することができること。(SD カード等、ストレージメディアに格納するデータについても同様とする)。

また、他の機器やクラウドサーバに送信される情報資産について、情報の漏えいや変更から保護することができること。

IoT 機器に置いて、認証情報(パスワード、秘密鍵など)を保存する場合、ネットワーク経由での不正アクセス(改ざん、盗聴など)から保護された領域で管理すること 。

暗号化に使用する鍵や証明書は、不正なアクセスや変更から保護しなければならない。

「機密の個人データ」とは、その開示が個人に害を及ぼす可能性が高いデータである。「機密の個人データ」として扱われるものは、製品やユースケースによって異なるが、例えば、家庭用セキュリティカメラのビデオストリーム、支払い情報、通信データの内容、タイムスタンプ付きの位置データなどがある。

4.3.5.3. スマートホーム分野★2 における要件

【機器の要件】

IoT 機器と他の IoT 機器や必須付随サービスとの間で通信される IoT データ(機器の動作情報やセンサ収集情報)の機密性は、技術の特性と使用法に適した暗号技術によって保護されなければならない。

4.3.6. 要件 8-3 (運用要件)

4.3.6.1. ロングリストにおける要件

【カテゴリ】

個人データがセキュアであることを確実にする

【要件】

製品のすべての外部感知機能は、ユーザにとって明確で透明性のあるアクセス可能な方法で文書化されなければならない。

4.3.6.2. スマートホーム分野における要件に関する補足

例えば、外部感知機能は、光学センサまたは音響センサである場合がある。センサが光学・音響をセンシングし利用可能であれば、その旨を、ユーザにとって明確で透明性のあるアクセス可能な方法で文書化されなければならない。

4.3.6.3. スマートホーム分野★2 における要件

【機器の要件】

IoT 機器の提供事業者は、機器のすべての外部感知機能を、ユーザにとって明確で透明性のあるアクセス可能な方法で提示すること

4.3.7. 追加要件 （運用要件）

4.3.7.1. ロングリストにおける要件

【カテゴリ】

対応するカテゴリ無し

【要件】

対応する要件なし。なお、本追加要件は NIST IR 8425 の Cybersecurity State Awareness に記載される内容に基づいて追加するものである。

4.3.7.2. スマートホーム分野における要件に関する補足

専門の管理者が常時監視を行うことが望ましい商用ITシステムやネットワークシステムとは異なり、一般の利用者が用いるスマートホーム向けの機器では、管理者による監視は望み得ない。このため、攻撃に関わりうるログの保存と、そのアップロード、必要に応じての専門家によるログ解析が重要となる。

4.3.7.3. スマートホーム分野★2 における要件

【機器の要件】

IoT 機器への攻撃、および IoT 機器を用いた攻撃に関わりうる IoT 機器の状態について、IoT 機器は収集して記録すること。IoT 機器が接続されているサーバなどに記録する形態でも良い。

4.4. ★2 で追加するセキュリティ要件（BtoBtoC モデルを想定した運用対策）

4.3 節までは、製造業者が IoT 製品に対して実施する対策を記述したが、ビジネスモデルによっては、対策を実施する主体が異なる場合がある。

製造業者による IoT 製品のビジネモデルでは、店頭やオンラインで直接利用者に販売する形態、すなわち BtoC モデルが一般的である。BtoC モデルでは、IoT 機器の製造業者が対策の主体者となる。

一方でスマートホーム分野においては、OEM や ODM などで IoT 機器が他の企業（ハウスメーカや、住宅内の IoT 機器を使ってサービスを提供するスマートホームの提供事業者。以降、「スマートホームの提供事業者」と呼ぶ）を経由して利用者に提供される形態が存在する（BtoBtoC モデル）。スマートホームの提供事業者は、自身が管理するスマートフォンアプリやクラウドサーバとの連携によってスマートホーム製品（サービス）を構成し、利用者に新たな付加価値を提供している。

BtoBtoC モデルでは、製造業者とスマートホームの提供事業者との間で企業間取引（BtoB）が成立するものの、IoT 製品のセキュリティに関する運用対応については明確な基準がなく、両社間での責任の所在が曖昧になりやすい。例えば、スマートホームに含まれる IoT 製品の更新ソフトウェアの提供主体や、インシデント発生時の対応に関する役割分担などを、製造業者とスマートホームの提供事業者の間で確認し、合意しておくことで、最終的な利用者の安全を守ることにもつながる。本節では、スマートホーム IoT 製品（スマートホーム IoT 機器と、その必須付随サービス）、製品が扱う情報の管理プロセスを含むものとし、以下の運用要件を記載する。

・ソフトウェアの更新プロセス、リリース、バージョン管理

・利用者変更に伴う情報の初期化や変更などの対応

・既知の脆弱性の有無を診断するプロセスの整備

・インシデントレスポンスの体制、プロセス構築

具体的な運用対策については、★1 の要件項目をもとに BtoBtoC モデルにおける不足事項を要件化するものとする。なお、本節の要件の主体者は BtoBtoC モデルにおいて顧客にスマートホーム製品を提供するスマートホームの提供事業者である。本節に記載する追加要件は、製造業者が満たす必要はない。

4.4.1. 追加要件1 （運用要件）

- **スマートホーム IoT 製品（スマートホーム IoT 機器と、その必須付随サービス）はスマートホームの提供事業者が主体となり、製造業者と連携し、最新のソフトウェアへと更新可能な体制とプロセスを構築すること。**
-

4.4.1.1. ★1における関連要件

3-8. 製品においてアップデートメカニズムが実装されている場合、セキュリティアップデートは、適時でなければならない。

4.4.1.2. スマートホーム分野における要件に関する補足

スマートホーム IoT 製品の必須付随サービスは、スマートホームの提供事業者が主体となり、円滑な実施体制やプロセスを整備しておく必要がある。必須付随サービスに関する脆弱性の報告は、スマートホームの提供事業者が情報を集約し、影響範囲の特定及び、アップデート計画を進めることが望ましい。

スマートホームの提供事業者は、更新されたソフトウェアによる不具合や脆弱性が見つかった場合に備え、対応方針（ソフトウェアを古いバージョンに更新（ロールバック）するなどの手段や手順）を整備しておくこと。

※文書化する場合の例

ソフトウェア開発ポリシー、品質管理規程、開発手順書/リリース管理手順書、保守・メンテナンス作業手順書など

4.4.2. 追加要件2（運用要件）

- スマートホームの提供事業者は製造業者と連携し、スマートホーム IoT 製品（IoT 機器と、その必須付随サービス）のソフトウェアについて、リリースまでの運用手順やバージョンの管理の仕組みを明確化すること。

1）更新ソフトウェアをリリースする際の管理、運用手順

2）更新ソフトウェアの更新内容と対応バージョンの履歴管理

4.4.2.1. ★1における関連要件

3-8. 製品においてアップデートメカニズムが実装されている場合、セキュリティアップデートは、適時でなければならない。

4.4.2.2. スマートホーム分野における要件に関する補足

スマートホーム IoT 製品の必須付随サービスは、スマートホームの提供事業者が主導し、更新ソフトウェアのリリースや、バージョン管理の対応方針を明確化する必要がある。

※文書化する場合の例）

ソフトウェア開発ポリシー、品質管理規程、開発手順書/リリース管理手順書、保守・メンテナンス作業手順書など

※補足）CI 環境等のシステムを用いて管理が行われる場合も、その旨の記述が対象文書に記載されていること。

4.4.3. 追加要件3 （運用要件）

- スマートホーム IoT 機器の提供において、利用者の変更が想定される場合（例えばリース契約による提供など）、情報資産の漏洩や、脆弱な状態にある機器の利用を防ぐために、スマートホームの提供事業者は運用プロセスにおいて、下記の対応を行った上で、新しい利用者への引継ぎが行われることが明示されていること。

1）設定及び収集、蓄積した情報の初期化を行うこと。

2）設置工事後、次の利用者がサービス運用を開始するまでに、IoT 機器を最新の状態へとソフトウェアアップデートすること。

3）必須付随サービス（クラウドサービス）については、蓄積された情報資産の管理をスマートホームの提供事業者が行い、情報の削除や変更を含む、管理対応の仕組みを有すること。

4.4.3.1. ★1における関連要件

3-1. 製品に含まれる特定のソフトウェアコンポーネントについて、アップデート可能にしなければならない。

11-1. ユーザが、簡単な方法で製品からユーザデータを消去できるような機能を提供しなければならない。

4.4.3.2. スマートホーム分野における要件に関する補足

スマートホーム IoT 製品では、リース契約や譲渡などにより、利用者の変更が行われる場合がある。利用者の変更後も、スマートホーム IoT 機器が転用される場合は、スマートホームの提供事業者によるメンテナンスが必要となる。

※文書化する場合の例

初期設定/インテグレーション手順書、システム運用手順書など

4.4.4. 追加要件4 （運用要件）

- **スマートホームの提供事業者は、インシデントレスポンスの体制構築の一環として、IoT 機器から収集したログデータの分析を行う体制や手順が定められていること。**

4.4.4.1. ★1における関連要件

2-1. 製造業者は、脆弱性開示ポリシーを公開しなければならない。このポリシーには、少なくとも以下が含まれていなければならない。

・問題を報告するための連絡先情報

・以下のタイムラインに関する情報

1)最初の受領確認

2)報告された問題が解決されるまでの状況の更新

4.4.4.2. スマートホーム分野における要件に関する補足

ログデータの分析はセキュリティインシデントだけでなく、ネットワーク及びシステム障害の原因究明にも対応できる体制、プロセスを整備し、必須付随サービスを含むスマートホーム IoT 製品の総合的なレジリエンス向上につながることが望ましい。

※文書化する場合の例

システム運用管理規程、ログ運用手順書、情報セキュリティ規程など

4.4.5. 追加要件5 （運用要件）

- スマートホームの提供事業者は製造業者と連携し、スマートホーム IoT 製品（IoT 機器と、その必須付随サービス）に対して、既知の脆弱性の有無を診断するプロセスおよび実施ポリシーを整備すること。
- 実施方法や判断基準、実行頻度は、スマートホームの提供事業者が設定するものとする。

4.4.5.1. ★1における関連要件

2-1. 製造業者は、脆弱性開示ポリシーを公開しなければならない。このポリシーには、少なくとも以下が含まれていなければならない。

・問題を報告するための連絡先情報

・以下のタイムラインに関する情報

1)最初の受領確認

2)報告された問題が解決されるまでの状況の更新

4.4.5.2. スマートホーム分野における要件に関する補足

スマートホーム IoT 製品では、既知の脆弱性が対策されないまま潜在することで、必須付随サービスを含む製品全体の脅威につながる恐れがある。IoT 製品の運用に影響しない開発環境もしくはテスト環境において、定期的な脆弱性診断を実施することで、インシデント発生の予防措置を行う。

スマートホーム IoT 製品については必須付随サービスを含め、スマートホームの提供事業者が既知の脆弱性診断に関する計画を主導し、対応する。

また、運用中の必須付随サービス（クラウドサービス）では、ペネトレーションテストなど規模の大きい検査や診断は実施困難であることが想定されるため、比較的対応が容易な、脆弱性診断の手法を例示する。

※クラウドサービスに対する既知の脆弱性検査例

- クラウドサービス：コンテナイメージ内のソフトウェアに対して、脆弱性スキャンツールによる既知の脆弱性検査を実施する。

※文書化する場合の例

ソフトウェア開発ポリシー、品質管理規程、開発手順書/リリース管理手順書など

4.4.6. 追加要件6（運用要件）

- スマートホームの提供事業者は、発生した想定外のセキュリティリスクに対応するため、製造業者と連携したインシデントレスポンス体制を構築し、事後対策及び再発防止策を検討するための仕組みを整備すること。
- 脆弱性の報告については、外部組織（JPCERT/CC 等）と連携し、適切な対応を行うこと。

4.4.6.1. ★1における関連要件

2-1. 製造業者は、脆弱性開示ポリシーを公開しなければならない。このポリシーには、少なくとも以下が含まれていなければならない。

・問題を報告するための連絡先情報

・以下のタイムラインに関する情報

1)最初の受領確認

2)報告された問題が解決されるまでの状況の更新

4.4.6.2. スマートホーム分野における要件に関する補足

スマートホームの提供事業者は、セキュリティインシデント発生に備え、インシデントレスポンスの対応方針を整備しておくことで、事後対応の迅速化、及び再発防止を図る。スマートホーム IoT 製品については必須付随サービスを含め、スマートホームの提供事業者がインシデントレスポンスの体制、プロセス構築を主導し、対応する。

インシデントレスポンスの対応指針として、明確化しておくべき項目を以下に例示する。

1)対象サービスにおける「インシデント」の定義。

2)「想定外のインシデント」に対して責任を持つ部署/担当者の整理。

3)組織内で発生したインシデント対応について、全体の統括を行う部署またはチーム等の整理。

4)インシデント発生時における、組織内の報告フローの整理。また報告を受けたものが、どのような判断基準で対応や上位への報告を行うかを定義。

5)インシデントの発見者が報告を行うタイミングや報告書式の定義。

6)インシデント対応に用いるツールやインフラが整備され、利用ルールの定義。

7)全てのインシデントに関する対応記録が保持、管理される仕組みの定義。

8)JPCERT/CC や ISAC など、社外の CSIRT 関連組織との連携方針の定義。

※文書化する場合の例

情報セキュリティ規程、インシデント対応計画書/手順書など

4.4.7. 追加要件の課題（運用要件）

・本制度は第三者による認証制度ではなく、スマートホーム提供事業者による自己評価・自己宣言を前提とした制度である。このため、各要件への適合確認にあたっては、第三者監査レベルの証跡提出を求めるものではなく、事業者自身の責任において要件を満たしていることを確認・宣言することを基本としている。

・BtoBtoC モデルにおけるスマートホーム提供事業者が本章で定義する各要件を満たすためには、製造業者から一定の情報提供を受ける必要がある。しかしながら、本章に記載した運用要件の多くは、製造業者におけるセキュリティ運用や組織体制等に関わる内容であり、企業機密情報として管理されている、もしくは社内の職制・業務分掌として明文化された資料が存在しない場合が多いことが確認されている。このため、これらの内容を文書として提示・提出することを一律に求めることは実運用上困難である。

・以上を踏まえ、各要件への適合を示す証跡については文書提出に限定せず、当該要件に対応する仕組みやプロセスが製造業者において実際に存在していることを、スマートホーム提供事業者と製造業者の間で確認し、相互に合意していることをもって、要件を満たしていることを示すことを可能とする。その確認・合意の結果は、チェックリスト等の形式により整理・記録することで足りるものとする。

・なお、万一セキュリティ事故が発生した場合には、スマートホーム提供事業者は、事前に確認・合意していた各要件の内容およびその確認方法について説明責任を負うものとし、製造業者はその説明に必要な範囲で当該仕組みやプロセスの内容を示すことが求められる。その内容に製造業者の内部機密情報が含まれる場合、製造業者はスマートホーム提供事業者を介さず直接関係機関に示すことを可能とする。これは事故発生時に新たな文書提出義務を課すものではなく、あらかじめ確認・合意していた内容の妥当性を説明するためのものである。

・以上を考慮した場合、今後以下の点について検討が必要である。

1）本章 4.4 では BtoBtoC モデルを想定した要件を記述しているが、BtoC モデルにおいても同様に適用可能な要件が存在するため、4.2 章および 4.3 章の該当項目との整合性を整理する必要がある。その際、章構成の再整理や統合も含めた検討が必要である。

2）各項目において「スマートホーム提供事業者と製造業者間で確認、合意できていること」としているが、具体的にどのような情報や確認方法をもって確認・合意とみなすかについては整理されていない。チェックリストの記載粒度や確認観点の例示など、実務上の運用を支援するための補足整理が今後の課題である。

5. システムやサービスとしてのスマートホームに求めるセキュリティ要件

この章では、家全体を一つのスマートホームシステムとして取り扱う場合のセキュリティ要件を示す。本章記載のスマートホームシステム及びサービスのセキュリティ要件は、★2レベルよりも厳しい基準(★3レベル相当)を想定している。また、サービス提供主体は、JC-STAR 制度の★2 ラベルを取得した IoT 製品でスマートホームシステムを構成し、構成したスマートホームの管理、運用におけるセキュリティ要件を満たす必要がある。

5.1. スマートホームサービスとシステム構成

本章で対象とするスマートホームのシステム・サービス要件の対象を下記の図 5-1 に示す。スマートホームシステム・サービスの管理、運用において、セキュリティ上考慮すべき事項を抽出し、後述の要件として定義を行う。

またスマートホームの構成機器については、サービス提供主体(サービス事業者や機器メーカ等)が利用を想定している機器のみを対象とし、利用者が個別に追加した機器(PC やその他のインターネット接続機器等)については対象外とする。

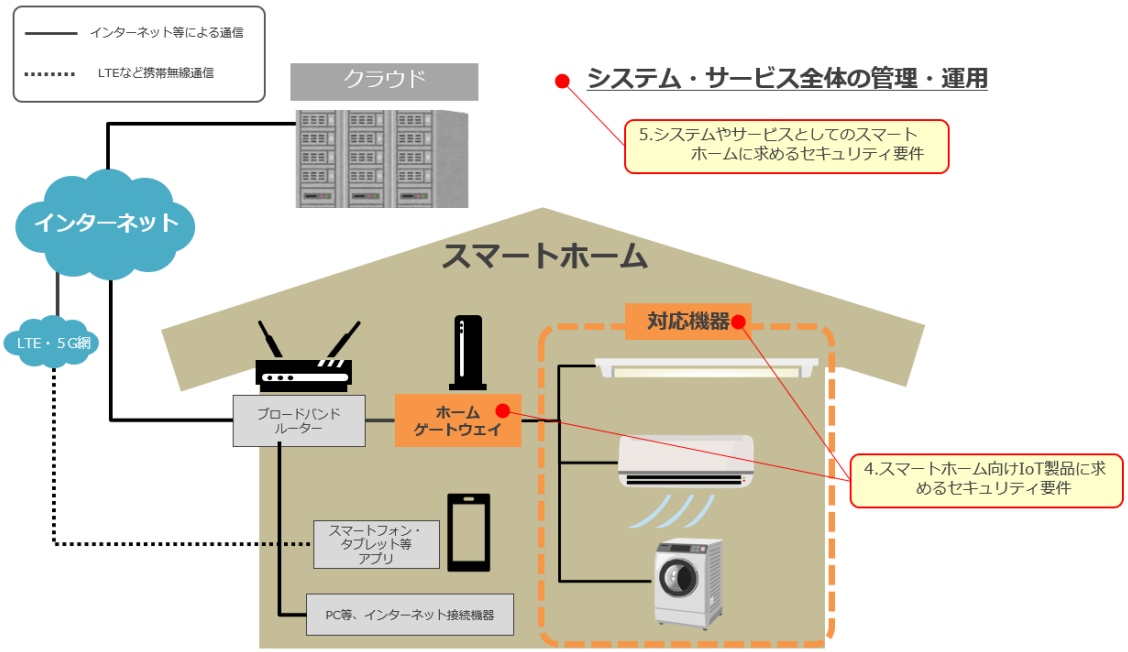


図 5-1_スマートホームのシステム・サービス要件の対象

5.2. セキュリティ要件の策定方法

スマートホームシステムを安全に運用し、かつ安全なサービスを利用者に提供するためには、機器のセキュリティ要件をサポートする非技術的な要件も求められる。本書では、求められるスマートホームシステム・サービス要件の検討にあたり、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 2023 年版 別紙セキュリティ要求

事項 Ver.1.0」[2]よりスマートホームサービスにおけるセキュリティ要件及び、経済産業省のロングリスト要件、さらにロングリストの参照先である NISTIR 8425 ” Profile of the IoT Core Baseline for Consumer IoT Products”を参考とした。NISTIR 8425 は、サービス提供主体に求められる運用プロセス上の非技術要件の参考として"IoT Product Non-Technical Supporting Capabilities"を中心に参照した。また、同文書は IoT 機器を対象とした文書であるため、スマートホームサービスにおけるユースケースや現状課題から求められる要件を選定し、サービスに適用する上で解釈を加えている(図 5-2 参照)。

参照した NISTIR 8425 とスマートホームシステム・サービス要件との対応を、表 5-1 に掲載する。

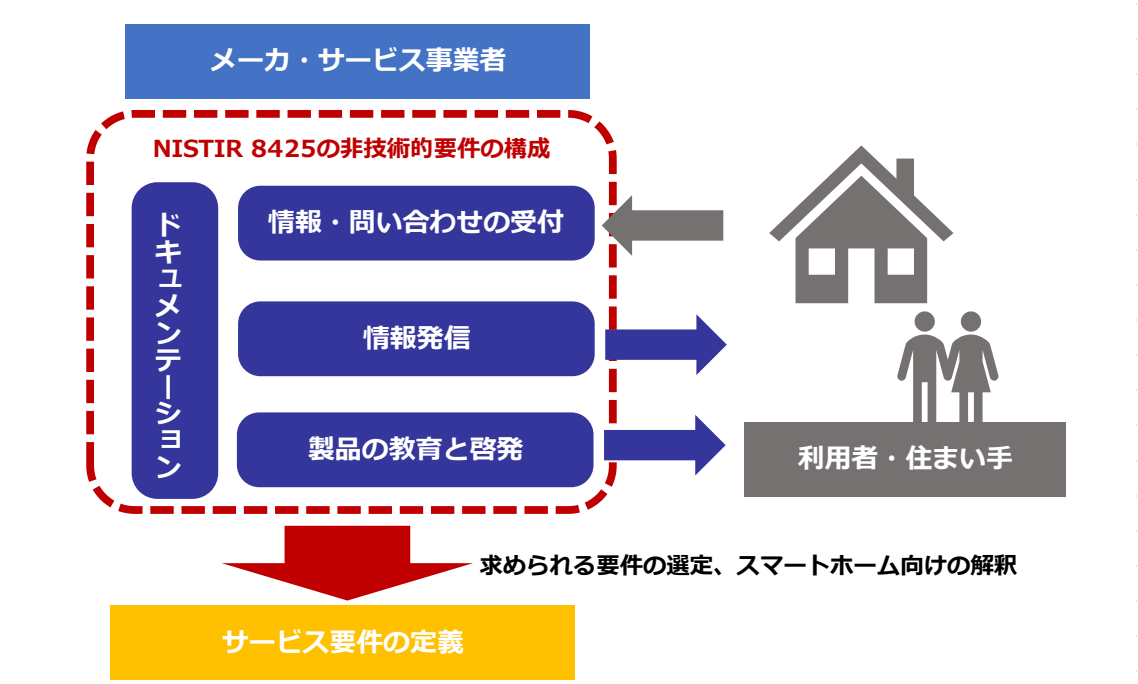


図 5-2_NISTIR 8425 の非技術要件の構成とサービス要件の関連[3]

表 5-1_スマートホームシステム・サービス要件とロングリスト、NISTIR 8425 の対応

#	スマートホームシステム・サービス要件	ロングリストの要件	NIST IR8425 の関連項目
スマートホームシステム・サービスの技術要件（機能要件）			

[2] https://www.ccds.or.jp/public/document/other/CCDS_SecGuide-Smarthome_Annex-Req_2023_v1.0_jpn.pdf

[3] 出典)NISTIR 8259B Figure 1 を参考にスマートホーム SEG にて作図
https://csrc.nist.gov/pubs/ir/8259/b/final

1	スマートホームシステム構成要素間のデータ保護	5-1. 製品は、ベストプラクティスの暗号技術を使用してセキュアに通信をしなくてはならない。	IoT Product Capabilities ・Data Protection：1,3 ・Interface Access Control：1
2	サービス契約者の本人認証	1-3. 製品に対してユーザを認証するために使用される認証メカニズムは、製品用途の特性等に適した想定するリスクを低減できる技術を使用していなければならない。	IoT Product Capabilities ・Interface Access Control：1
3	サービス管理担当者のアクセス権限管理	6-7. ソフトウェアは、セキュリティと機能の両方を考慮し、必要最小限の権限で実行しなければならない。	IoT Product Capabilities ・Product Configuration：1,2
スマートホームシステム・サービスの非技術要件（組織・運用要件）			
1	一定のセキュリティ基準を満たした IoT 製品の利用	18-1. 製造業者は、セキュリティ要件を満たすために用いた手段に関するデータを文書化しなければならない。	IoT Product Non-Technical Supporting Capabilities ・Documentation：c
2	スマートホームの安全な利用方法に関するガイダンス	12-1. 製品の設置及び保守は、ユーザによる決定を最小限とし、ユーザビリティに関するセキュリティのベストプラクティスに従わなくてはならない。 12-2. 製造業者は、使用する製品がセキュアにセットアップされているかどうかを確認する方法について、ユーザにガイダンスを提供しなければならない。	IoT Product Non-Technical Supporting Capabilities ・Documentation：d-vii ・Information and Query Reception：b ・Product Education and Awareness：a-i～a-ii
3	サービス管理担当者のアクセス権限管理	6-7. ソフトウェアは、セキュリティと機能の両方を考慮し、必要最小限の権限で実行しなければならない。	IoT Product Non-Technical Supporting Capabilities ・Documentation：a-iii

5.3. 策定されたセキュリティ要件

5.3.1. スマートホームシステム・サービスの技術要件（機能要件）

5.3.1.1. スマートホームシステム・サービスの技術要件1

【タイトル】

スマートホームシステム構成要素間のデータ保護

【対応すべき背景や課題】

スマートホームサービスのシステム構成機器間におけるデータ保護については、多くのステークホルダーが関係するため、責任分解が曖昧になりやすい。データの受け

渡しに共通で利用される Web API や、電子証明書などの管理責任の主体を明確に定義する必要がある。

【要件】

- **スマートホームサービスを提供するスマートホームシステムは、構成要素間の通信経路において、データ保護対策を行うこと。さらに、データの受け渡しに使用される Web API や電子証明書の管理責任の主体を明確に定義し、各ステークホルダーの責任を明確化すること。**

【スマートホーム分野における要件の補足】

構成要素には、2.1 で示す通り、対応機器だけなく、クラウドサーバやモバイルアプリケーションが含まれる。

異なる構成要素間でデータ送受信を実現するためには、一例として共通の Web API を利用することが想定される。Web API を活用する場合、スマートホームシステム全体のメンテナンス性を確保する上で、Web API の管理責任はサービス提供主体が担うことが望ましい。この場合、Web API はサービス提供主体により配布され、定められた利用許諾に従い、ステークホルダー各社で利用される。

各構成要素における保護対策の実装については、TLS による暗号化が一般的だが、対策手法はこれに限定しない。ただし、暗号化技術については CRYPTREC 発行のガイドライン等によって推奨されたベストプラクティスを採用する。その他の対策手法を用いる場合には、市場で実績のあるデータ保護のソリューションを採用すること。

電子証明書など、構成要素間の認証やデータ保護に利用される情報については、サービス提供主体が一元管理を行うことが望ましい。例えば、各構成機器において、定期的な証明書の更新が必要な場合には、サービス提供主体より、ステークホルダー各社へ通知を行い、スマートホームシステムとして一貫した対応を行う。

5.3.1.2. スマートホームシステム・サービスの技術要件2

【タイトル】

サービス契約者の本人認証

【対応すべき背景や課題】

スマートホームサービスでは、住宅の所有権の移転（転売）や、賃貸契約の解消（退去）などにより、利用者の変更が想定される。現在の利用者がサービス契約者と異なる可能性もあるため、サービス契約者の本人認証を機能として実装する必要がある。

【要件】

- **スマートホームサービス利用時には、サービス契約を締結している利用者を識別、認証及びアクセス管理の仕組みを有すること。**

【スマートホーム分野における要件の補足】

サービス契約者の認証には、一般的に操作端末のモバイルアプリケーションを利用することが想定される。モバイルアプリケーションを利用した認証の場合、例えば、電話回線や SMS による認証コード通知を用いた多要素認証によって、セキュリティ強度を高める工夫を行うこと。

5.3.1.3. スマートホームシステム・サービスの技術要件3

【タイトル】

サービス管理担当者のアクセス権限管理

【対応すべき背景や課題】

スマートホームサービスの管理を行う上で、サービス提供主体の管理担当者（オペレータ含む）が管理用のクラウドサーバにアクセスすることが想定される。万一、管理担当者のなりすましによって、クラウドサーバに不正アクセスされてしまうと、個人情報の窃取やバックドアとなるマルウェア感染など、深刻な影響を受ける可能性がある。サイバー攻撃を防ぐために、クラウドサーバ側でサービス管理担当者を適切に識別、認証し、アクセス管理する仕組みが求められる。

【要件】

- **サービス管理担当者（オペレータ含む）がクラウドサーバ等のスマートホームシステムへアクセスする際、担当者の識別や認証及び、アクセス管理の仕組みを有すること。**

【スマートホーム分野における要件の補足】

スマートホームサービスのクラウドサーバは、構成要素間の認証や、アップデートファイルの提供、設備や機器の制御や状態の記録、監視、利用顧客の情報管理など、多様な機能が求められ、扱われる情報も機密性が高い。多機能なサーバに対して、効率的に認証の仕組みを導入する場合には、クラウド事業者がサービスとして提供している認証機能を利用することが想定される。

5.3.2. スマートホームシステム・サービスの非技術要件（組織・運用要件）

5.3.2.1. スマートホームシステム・サービスの非技術要件1

【タイトル】

一定のセキュリティ基準を満たしたIoT製品の利用

【対応すべき背景や課題】

スマートホームシステムの構成において、一部でも脆弱な製品が存在することで、外部からの攻撃の入り口となり、スマートホームシステム全体の脅威となる可能性がある。

【要件】

- サービス提供主体は、サービスの利用に必要な構成要素を、モデル名や型式番号、JC-STAR制度の★レベルなどによって明確化すること。
- スマートホームシステムは、JC-STAR制度の★２のセキュリティ要件を満たしているIoT製品によって構成されること。
- 上記の**スマートホーム**システムの構成及び手順は文書化されていること。

【スマートホーム分野における要件の補足】

サービス提供主体は、スマートホーム施工時に宅内に設置されるIoT機器が、★２ラベルを取得した製品（または★２要件を満たしている製品）かどうかを確認する手順を、運用プロセスに含めるべきである。

5.3.2.2. スマートホームシステム・サービスの非技術要件2

【タイトル】

スマートホームの安全な利用方法に関するガイダンス

【対応すべき背景や課題】

宅内のスマートホームシステムは、利用者によってサービス対象に含まれない機器の追加や、想定外の使用方法により障害やインシデントの原因となる可能性がある。サービス提供主体は、適切な利用手順を提示するとともに、責任範囲外となる事項についても、利用者へ明示すべきである。

【要件】

- 宅内スマートホームシステムの機器構成や設定については、利用者による変更を認めない範囲を明示し、該当する範囲については、利用者が無断で変更しないよう注意喚起を促すこと。
- 利用者が想定外の用途で機器を使用しないよう、提供機能の利用手順や、セキュリティ上の安全な利用方法について、周知すること。
- 上記対応手順は文書化され、ウェブページやマニュアル等を用いて利用者に情報提示されること。

【スマートホーム分野における要件の補足】

サービス提供主体は、利用者による使用を前提としていない管理機能について、アクセスの方法や設定手順等を開示すべきではない。また、サービス上想定されていない機器の追加や使用については、免責事項として提示しておく事が望ましい。

・免責事項の例）

－サービス対象としていない機器を利用者が追加した場合、追加の機器で発生した問題はサービス上の免責事項に相当し、利用者側の責任のもとで使用する旨、記載を行う。またセキュリティ上の危険性がある旨、注意喚起を促す。

サービス提供主体は、サービスの対象となるIoT製品やスマートホームシステムに障害が発生した場合の問い合わせ先を、ウェブページやマニュアル等に明示すべきである。

5.3.2.3. スマートホームシステム・サービスの非技術要件3

【タイトル】

サービス管理担当者のアクセス権限管理

【対応すべき背景や課題】

スマートホームサービスの管理を行う上で、サービス提供主体の管理担当者（オペレータ含む）が管理用のクラウドサーバにアクセスすることが想定される。万一、管理担当者のなりすましによって、クラウドサーバに不正アクセスされてしまうと、個人情報の窃取やバックドアとなるマルウェア感染など、深刻な影響を受ける可能性がある。サイバー攻撃を防ぐために、サービス管理担当者のアカウント管理は適切に運用されることが求められる。

【要件】

- サービス管理担当者には**最小権限の原則に従い、**適切なアクセス権限を設定し、定期**的な権限のレビュー及び、不要権限の削除を実施すること**。
- 上記の方針、手順は文書化されていること。

【スマートホーム分野における要件の補足】

5.3.1.3. スマートホームシステム・サービスの技術要件3についてもあわせて参照すること。

付録1. 参考文献

- 「STRIDE モデル」

発行元	Microsoft Corporation
概要	Microsoft 社が提唱する脅威分析手法
参照先	https://docs.microsoft.com/ja-jp/azure/security/azure-security-threat-modeling-tool-threats

- 「STRIDE + CCDS モデル」

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	STRIDE モデルを拡張した脅威分析手法
参照先	https://www.ccds.or.jp/public/document/other/CCDS_IoT システム調達のためのセキュリティ要件フレームワーク.pdf

- 「特定分野システムの IoT 製品における JC-STAR 制度活用ガイド」

発行元	経済産業省　商務情報政策局 サイバーセキュリティ課
概要	特定の分野や業界において類似の汎用的な構成で利用されるシステムに組み込まれて調達され、利用されるような IoT 製品に対するセキュリティ要件を定め、IoT 製品に対するセキュリティ要件適合評価及びラベリング制度の活用を検討する際に参考となる情報
参照先	https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_cybersecurity/iot_security/20241106.html

付録2. 用語の意味・説明

以下に記載のない用語については、独立行政法人情報処理推進機構（IPA）から令和 6 年 12 月に発行された、「セキュリティ要件適合評価及びラベリング制度（JC-STAR）★1 レベル適合基準・評価手法」（文章番号：JST-CR-01-01-2024R1）の Appendix. A 用語集、および「セキュリティ要件適合評価及びラベリング制度（JC-STAR）★1 評価ガイド」（文章番号：JST-EG-01-01-2024）の Appendix. A 用語説明に記載の意味および説明に従う。

用語	意味
スマートホーム IoT 機器	IoT 機器のうちで、スマートホーム分野で利用されるもの。 注 1：スマートホーム IoT 機器は、一般の消費者が住宅内において使用される。
スマートホーム IoT 製品	スマートホーム IoT 機器と、その必須付随サービス

付録3. セキュリティ要件の分類

番号	分類	要件内容	要件内容
1-1	運用要件	IoT 機器	パスワード（アクセスポイントモードとして動作する際のパスワードを含む）またはパスコードが使用され、工場出荷時のデフォルト以外の状態にある IoT 機器において、すべてのパスワードまたはパスコードは、IoT 機器ごとに固有であるか、又はユーザによって定義されるものでなければならない。
		クラウド サービス	クラウドサービスで IoT 機器のユーザの認証のためにパスワードが使用される場合、パスワードはユーザによって定義されるものでなければならない。
1-2	技術要件	IoT 機器	IoT 機器でプリインストールされた固有のパスワードまたはパスコードを使用する場合、自動化された攻撃への耐性をもつために、パスワード・パスコードは十分なランダム性を保有しなければならない。
1-3	技術要件	IoT 機器	IoT 機器に対してユーザを認証するために使用される認証メカニズム、および IoT 機器の初期ネットワーク設定時に IoT 機器と設定用モバイルアプリケーションとのあいだで利用される認証メカニズムは、製品用途の特性等に適した想定するリスクを低減できる技術を使用していなければならない。
1-4	運用要件	IoT 機器	IoT 機器に対するユーザ認証がある場合には、IoT 機器は使用される認証値を変更するためのシンプルなメカニズムを、ユーザ又は管理者に提供しなければならない。
		モバイル アプリケーション	モバイルアプリケーションを入力手段とするユーザ認証において、モバイルアプリケーションは使用される認証値を変更するためのシンプルなメカニズムを、ユーザ又は管理者に提供しなければならない。
1-5	技術要件	IoT 機器	IoT 機器が、制約のある機器ではない場合、ネットワークを介して行われる認証に対する総当たり攻撃等のブルートフォース攻撃が実行できないようにするメカニズムを保有しなければならない。

2-1	運用要件	IoT 機器	IoT 機器の提供事業者は、IoT 機器に関する脆弱性開示ポリシーを公開しなければならない。このポリシーには、少なくとも以下が含まれていなければならない ・問題を報告するための連絡先情報 ・以下のタイムラインに関する情報 1) 最初の受領確認 2) 報告された問題が解決されるまでの状況の更新
		モバイル アプリケーション	IoT 機器の提供事業者がモバイルアプリケーションを提供する場合には、提供事業者はモバイルアプリケーションの脆弱性開示ポリシーを公開しなければならない。このポリシーには、少なくとも以下が含まれていなければならない ・問題を報告するための連絡先情報 ・以下のタイムラインに関する情報 1) 最初の受領確認 2) 報告された問題が解決されるまでの状況の更新
		クラウド サービス	IoT 機器の提供事業者がクラウドサービスを提供する場合には、提供事業者はクラウドサービスの脆弱性開示ポリシーを公開しなければならない。このポリシーには、少なくとも以下が含まれていなければならない ・問題を報告するための連絡先情報 ・以下のタイムラインに関する情報 1) 最初の受領確認 2) 報告された問題が解決されるまでの状況の更新
3-1	技術要件	IoT 機器	IoT 機器のクラウド上のサービスに接続する機能をつかさどる通信モジュールのファームウェアについて、アップデート可能にしなければならない。

3-2	技術要件	IoT 機器	IoT 機器が、通信モジュールファームウェアのアップデートをセキュアにインストールするためのアップデートメカニズムを備えていなければならない。
3-3	運用要件	IoT 機器	IoT 機器において通信モジュールのファームウェアアップデートメカニズムが実装されている場合、そのアップデートは、ユーザ或いは管理者が簡単に適用できるものでなければならない。
3-7	技術要件	IoT 機器	IoT 機器において通信モジュールのファームウェアアップデートメカニズムが実装されている場合、セキュアなアップデートメカニズムを容易にするために、ベストプラクティスの暗号技術を使用しなければならない。
3-8	運用要件	IoT 機器	IoT 機器において通信モジュールファームウェアのアップデートメカニズムが実装されている場合、セキュリティアップデートは、適時でなければならない。
3-10	技術要件	IoT 機器	IoT 機器においてアップデートメカニズムが実装され、ソフトウェアアップデートがネットワークインタフェースを介して配信される場合、IoT 機器は、信頼関係を介して各アップデートの真正性及び完全性を検証しなければならない。
3-14	運用要件	IoT 機器	IoT 機器のモデル名称は、IoT 機器上のラベル又は物理的インタフェースを介して、ユーザに対して明確に認識可能でなければならない。
4-1	技術要件	IoT 機器	IoT 機器のストレージにある守るべき情報資産は、IoT 機器によってセキュアに保存されなければならない。
4-2	技術要件	IoT 機器	ハードコードされた IoT 機器ごとに固有の身元情報がセキュリティ目的で IoT 機器で使用される場合、物理的、電気的、又はソフトウェアなどの手段による改ざんに耐えられるように実装しなければならない。
4-3	技術要件	IoT 機器	IoT 機器のソフトウェアのソースコードに重要なセキュリティパラメータをハードコードしてはならない。
4-4	技術要件	IoT 機器	ファームウェアアップデートの完全性及び真正性チェック、及びモバイルアプリケーションやクラウドサービスなど必須付随サービスとの通信の保護に使用される重要なセ

			キュリティパラメータは、IoT 機器ごとに固有でなければならず、IoT 機器のクラスに対する自動化された攻撃のリスクを低減するメカニズムで生成されるものとしなければならない。
5-1	技術要件	IoT 機器	IoT 機器は、ベストプラクティスの暗号技術を使用してセキュアに通信をしなくてはならない。
5-5	技術要件	IoT 機器	ネットワークインタフェースを介してセキュリティに関連する設定の変更を可能にする IoT 機器の設定変更機能は、認証後にのみアクセス可能でなければならない。ただし、IoT 機器が依存するネットワークサービスプロトコルで、IoT 機器の動作に必要な設定を製造業者が保証できない場合は、例外とする。
5-7	技術要件	IoT 機器	ネットワークインタフェースを介してセキュリティに関連する設定の変更を可能にするスマートホーム向け IoT 機器では、リモートアクセス可能なネットワークインタフェースを介して通信される重要なセキュリティパラメータの機密性を保護しなければならない。
5-8	運用要件	IoT 機器	IoT 機器の提供事業者は、IoT 機器に関連する重要なセキュリティパラメータについて、セキュアな管理プロセスに従わなければならない。
6-1	技術要件	IoT 機器	IoT 機器では、すべての未使用の物理的インタフェース及び論理的インタフェースは無効化しなければならない。
8-2	技術要件	IoT 機器	IoT 機器と他の IoT 機器や必須付随サービスとの間で通信される IoT データ(機器の動作情報やセンサ収集情報)の機密性は、技術の特性と使用法に適した暗号技術によって保護されなければならない。
8-3	運用要件	IoT 機器	IoT 機器の提供事業者は、機器のすべての外部感知機能を、ユーザにとって明確で透明性のあるアクセス可能な方法で提示すること。
9-1	運用要件	IoT 機器	IoT 機器では、データネットワークと電源の停止の可能性を考慮して、レジリエンスを製品とサービスに組み込まなければならない。

		クラウド サービス	IoT 機器の提供事業者は、必須付随サービスであるクラウドサービスに関してデータネットワークの停止の可能性を考慮して、レジリエンスをサーバに組み込まなければならない。
11-1	技術要件	IoT 機器	IoT 機器の提供事業者は、ユーザや設置事業者等が簡単な方法で IoT 機器のユーザデータを消去できるような手段を提供しなければならない。
17-2	運用要件	IoT 機器	IoT 機器の提供事業者は、IoT 機器をセキュアに設定・利用・廃棄する方法について、ユーザや設置事業者に提供しなければならない。
		モバイル アプリケーション	IoT 機器の提供事業者は、必須付随サービスとしてのモバイルアプリケーションをセキュアに設定・利用・削除する方法について、ユーザや設置事業者に提供しなければならない。
17-3	運用要件	IoT 機器	IoT 機器の提供事業者は、IoT 機器にセキュリティアップデートが必要であることを、そのアップデートによって軽減されるリスクに関する情報とともに、認識可能で明らかな方法でユーザや設置事業者に通知しなければならない。
17-5	運用要件	IoT 機器	IoT 機器の提供事業者は、ユーザが IoT 機器を廃棄する手順について、指定された方法でユーザや設置事業者に提供しなければならない。
		モバイル アプリケーション	IoT 機器の提供事業者は、ユーザが IoT 機器を廃棄する場合のモバイルアプリケーションのデータを削除する手順について、指定された方法でユーザや設置事業者に提供しなければならない。
17-8	運用要件	IoT 機器	IoT 機器の提供事業者は、自らが定めたサポート期間を、ユーザや設置事業者にとって明確で透明性のある方法で公表しなければならない。
		モバイル アプリケーション	IoT 機器の提供事業者は、必須付随サービスであるモバイルアプリケーションの自ら定めたサポート期間を、ユーザや設置事業者にとって明確で透明性のある方法で公表しなければならない。

		クラウド サービス	IoT 機器の提供事業者は、必須付随サービスであるクラウドサーバの定められたサポート期間を、ユーザや設置事業者にとって明確で透明性のある方法で公表しなければならない。
17-10	運用要件	IoT 機器	IoT 機器の提供事業者は、セキュリティリスクを引き起こす可能性がある IoT 機器の利用状況に関する情報について、明確な方法でユーザや設置事業者に提供しなければならない。
		モバイル アプリケーション	IoT 機器の提供事業者は、セキュリティリスクを引き起こす可能性があるモバイルアプリケーションの利用状況に関する情報について、指定された方法でユーザや設置事業者に提供しなければならない。
		クラウド サーバ	IoT 機器の提供事業者は、セキュリティリスクを引き起こす可能性があるクラウドサーバの利用状況に関する情報について、指定された方法でユーザや設置事業者に提供しなければならない。
追加 1	運用要件	IoT 機器	IoT 機器への攻撃、および IoT 機器を用いた攻撃に関わりうる IoT 機器の状態について、IoT 機器は収集して記録すること。IoT 機器が接続されているサーバなどに記録する形態でも良い。
追加 2	運用要件	IoT 機器及び、その必須付随サービス	・スマートホーム IoT 製品（スマートホーム IoT 機器と、その必須付随サービス）は IoT 製品の提供事業者により、最新のソフトウェアへと更新可能な体制とプロセスを構築すること。
追加 3	運用要件	IoT 機器及び、その必須付随サービス	・IoT 製品の提供事業者はスマートホーム IoT 製品（スマートホーム IoT 機器と、その必須付随サービス）のソフトウェアについて、リリースまでの運用手順の明確化及び、バージョンの管理を行うこと。

追加 4	運用要件	IoT 機器及び、その必須付随サービス	・スマートホーム IoT 機器の提供において、利用者の変更が想定される場合（例えばリース契約による提供など）、情報資産の漏洩や、脆弱な状態にある機器の利用を防ぐために、IoT 製品の提供事業者は下記の対応を行った上で、新しい利用者への引継ぎを行うこと。 1）設定及び収集、蓄積した情報の初期化を行うこと。 2）設置工事後、次の利用者がサービス運用を開始するに、IoT 機器を最新の状態へとソフトウェアアップデートすること。 3）必須付随サービス（クラウドサービス）については、蓄積された情報資産の管理を IoT 製品の提供事業者が行うこと。クラウドサービスの管理に外部の事業者が関係する場合、提供事業者は外部の事業者と連携し、情報の削除や変更指示を含む、管理対応を行うこと。
追加 5	運用要件	IoT 機器及び、その必須付随サービス	・IoT 製品の提供事業者は、インシデントレスポンスの体制構築の一環として、IoT 機器から収集したログデータの分析を行う体制や手順を定め、運用を行うこと。
追加 6	運用要件	IoT 機器及び、その必須付随サービス	・IoT 製品の提供事業者は、スマートホーム IoT 製品（スマートホーム IoT 機器と、その必須付随サービス）に対して、既知の脆弱性の有無を診断するプロセスを整備すること。 ・実施方法や判断基準、実行頻度は、IoT 製品の提供事業者が個別に設定するものとする。
追加 7	運用要件	IoT 機器及び、その必須付随サービス	・IoT 製品の提供事業者は、発生した想定外のセキュリティリスクに対応するため、ステークホルダーと連携したインシデントレスポンス体制を構築し、事後の対応及び、再発防止対策を行うこと。

			・脆弱性の報告については、外部組織（JPCERT/CC 等）と連携し、適切な対応を行うこと。

1