製品分野別セキュリティガイドライン
スマートホーム編

Ver. 1.0

CCDS セキュリティガイドライン WG

スマートホーム WG

改訂履歴

版数	改訂日	改訂内容
Ver.0.1	2018/11/26	Draft 版として新規発行
Ver.1.0	2019/10/29	Draft 版を改定し、新規発行

■商標について

・本書に記載の会社名、製品名などは、各社の商標または登録商標です。

■おことわり

・本書に記載されている内容は発行時点のものであり、予告なく変更することがあります。

・本書の内容を CCDS の許可なく複製・転載することを禁止します。

© 2018-2019 Connected Consumer Device Security Council Proprietary

目次

1　はじめに 1

1.1　スマートホームのセキュリティの現状と課題 2

1.2　ガイドラインの対象範囲 4

1.3　本書の対象者 4

1.4　用語・略称 5

2　スマートホームサービスの定義とシステム構成 7

2.1　スマートホームサービスの定義 7

2.2　スマートホーム向け製品・サービスのセキュリティレベルの定義 8

2.3　システムモデルの定義 11

2.4　ユースケースの定義 14

2.4.1　★★サービスにおけるユースケース事例 14

2.4.2　★★★サービスにおけるユースケース事例 16

3　スマートホーム向け製品・サービスのリスク分析 18

3.1　リスク分析・評価の手順 18

3.2　保護すべき資産の抽出 19

3.3　想定される脅威の分析 21

3.3.1　スマートホームの製品・システム上の想定脅威 21

3.3.2　サイバーセキュリティ以外の想定脅威 25

3.4　想定される脅威の詳細分析 25

3.5　リスク値の計算 42

3.5.1　CVSS v3 によるリスク値の計算と課題 42

3.5.2　スマートホーム独自方式のリスク値計算の定義 44

3.5.3　スマートホーム独自方式でのリスク値計算の結果 55

3.6　リスク分析・評価のまとめ 66

3.7　セキュリティ対策の検討 66

4　想定されるセキュリティ上の脅威と対策指針 77

4.1　関係する要素の多様性 77

4.2　製品安全（セーフティ）への対応 77

4.3　機器の連携 78

4.4　利用者による IoT 機器の設置・撤去 78

4.5　スマートホームサービスにおけるセキュリティ対策指針の整理 79

5　スマートホームサービスのライフサイクルと　セキュリティへの取り組み 80

5.1　スマートホームサービスのライフサイクルにおけるフェーズの定義 80

5.2　サービスのライフサイクルにおけるセキュリティへの取組み 81

5.2.1　サービス企画フェーズ 81

5.2.2　設計・製造フェーズ 83

5.2.3　評価フェーズ 84

5.2.4　運用・保守フェーズ 84

5.2.5　サービス終了フェーズ 88

5.3　スマートホームのライフサイクルにおけるフェーズの定義 89

5.4　スマートホームのライフサイクルにおけるセキュリティへの取組み 90

5.4.1　設計フェーズ 90

5.4.2　生産・施工フェーズ 90

5.4.3　アフターフェーズ 92

5.4.4　リフォームフェーズ 93

5.4.5　転売フェーズ 94

5.4.6　解体フェーズ 95

6　スマートホームサービスにおけるセキュリティ要件 96

6.1　スマートホームサービスにおけるセキュリティ要件 96

6.2　システム・サービス対応機器群に求めるセキュリティ要求事項 104

6.2.1　スマートホームサービス情報基盤へのセキュリティ要求事項 105

6.2.2　第三者サービス情報基盤へのセキュリティ要求事項 111

6.2.3　ホームゲートウェイへのセキュリティ要求事項 112

6.2.4　スマートホームサービス対応機器へのセキュリティ要求事項 117

6.2.5　スマートフォンアプリへのセキュリティ要求事項 120

7　まとめ 121

引用/参考文献 122

図 2-1 スマートホーム向け製品・サービスの階層モデル 9

図 2-2 スマートホームサービスにおけるセキュリティ要件/要求事項の対応 10

図 2-3 スマートホームのシステムモデル図 12

図 2-4 スマートホームのユースケース（シャッター自動開閉サービス） 15

図 2-5 スマートホームのユースケース（駆けつけ防犯サービス） 16

図 3-1 スマートホームのシステムモデルにおける脅威分析事例 23

図 3-2 基本値（スマートホーム独自方式）の計算式 45

図 3-3 環境値（スマートホーム独自方式）の計算式 50

図 5-1 スマートホームサービスのライフサイクルにおけるフェーズ 80

図 5-2 スマートホームのライフサイクルにおけるフェーズ 89

表 1-1 用語一覧 5

表 1-2 略称一覧 6

表 2-1 本書におけるサービス・システムの定義 8

表 2-2 スマートホーム向け製品・サービスのサーティフィケーションレベル 9

表 2-3 システムモデル中の構成機器 13

表 2-4 スマートホームのユースケース（シャッター自動開閉サービス） 15

表 2-5 スマートホームのユースケース（駆けつけ防犯サービス） 17

表 3-1 リスク分析・評価の手順 18

表 3-2 スマートホームのシステム・製品を対象とした保護すべき資産の例 19

表 3-3 STRIDE+CCDS モデルによる脅威分類の一覧 22

表 3-4 STRIDE+CCDS モデルによる脅威分類事例 23
表 3-5 想定される脅威の詳細分析項目一覧..... 25
表 3-6 接続 I/F 項目..... 26
表 3-7 Who（誰がつなげたか）項目..... 27
表 3-8 Whom（何が危害をうけたか）項目..... 27
表 3-9 Where（どこで発生したか）項目..... 27
表 3-10 スマートホームサービス・第三者サービスの情報基盤に対する詳細脅威分析事例 29
表 3-11 ホームゲートウェイ・スマートホーム対応機器群・スマートフォンアプリに対する詳細脅威分析事例..... 34
表 3-12 CVSSv3 によるサービスのリスク値（★★、★★★共通）※抜粋 43
表 3-13 CVSSv3 によるリスク値計算の課題 44
表 3-14 スマートホーム独自方式の脆弱性評価基準..... 44
表 3-15 基本値を計算するパラメータ..... 46
表 3-16 生命・財産への影響（LP）..... 46
表 3-17 情報の重要度（II）..... 47
表 3-18 機密性（C)・完全性（I)・可用性（A）への影響..... 47
表 3-19 攻撃元区分（AV）..... 48
表 3-20 攻撃条件の複雑さ（AC）..... 48
表 3-21 攻撃に必要な特権レベル（PR）..... 48
表 3-22 ユーザ関与レベル（UI）..... 49
表 3-23 スコープ（S）..... 49
表 3-24 環境値を計算するパラメータ..... 51
表 3-25 緩和策後の生命・財産への影響（MLP）..... 52
表 3-26 緩和策後の情報の重要度（MII）..... 52
表 3-27 対象システムのセキュリティ要求度（CR/IR/AR）..... 52
表 3-28 緩和策後の機密性への影響（MC）..... 53
表 3-29 緩和策後の完全性への影響（MI）..... 53
表 3-30 緩和策後の可用性への影響（MA）..... 53
表 3-31 緩和策後の攻撃元区分（MAV）..... 53
表 3-32 緩和策後の攻撃条件の複雑さ（MAC）..... 53
表 3-33 緩和策後の攻撃に必要な特権レベル（MPR）..... 54
表 3-34 緩和策後のユーザ関与レベル（MUI）..... 54
表 3-35 緩和策後のスコープ（MS）..... 54
表 3-36 深刻度レベル分け..... 54

表 3-37 スマートホーム独自方式によるサービスのリスク値..... 55
表 3-38 シャッター自動開閉サービス（★★）のリスク値（セキュリティ対策前）... 56
表 3-39 防犯駆けつけサービス（★★★）のリスク値（セキュリティ対策前）..... 61
表 3-40 シャッター自動開閉サービス（★★）のリスク値（セキュリティ対策後）... 67
表 3-41 防犯駆けつけサービス（★★★）のリスク値（セキュリティ対策後）..... 72
表 5-1 スマートホームサービスにおけるフェーズの定義..... 81
表 5-2 サービス企画フェーズにおけるセキュリティへの取組み..... 82
表 5-3 設計・製造フェーズにおけるセキュリティへの取組み..... 83
表 5-4 評価フェーズにおけるセキュリティへの取組み..... 84
表 5-5 運用・保守フェーズでのセキュリティへの取組み..... 84
表 5-6 サービス終了フェーズでのセキュリティへの取組み..... 88
表 5-7 スマートホームにおけるフェーズの定義..... 89
表 5-8 設計フェーズでのセキュリティへの取組み..... 90
表 5-9 生産・施工フェーズにおけるセキュリティへの取組み..... 91
表 5-10 アフターフェーズにおけるセキュリティへの取組み..... 92
表 5-11 リフォームフェーズにおけるセキュリティへの取組み..... 93
表 5-12 転売フェーズにおけるセキュリティへの取組み..... 94
表 5-13 解体フェーズにおけるセキュリティへの取組み..... 95
表 6-1 セキュリティ要件及びセキュリティ要求事項における対応表記ルール 97
表 6-2　セキュリティ要件及びセキュリティ要求事項におけるナンバリングルール... 97
表 6-3 スマートホームサービスにおけるセキュリティ要件 98
表 6-4 スマートホームサービス情報基盤に対するセキュリティ要求事項..... 105
表 6-5 第三者サービス情報基盤に対するセキュリティ要求事項..... 111
表 6-6 ホームゲートウェイに対するセキュリティ要求事項..... 112
表 6-7 スマートホームサービス対応機器に対するセキュリティ要求事項..... 117
表 6-8 スマートフォンアプリに対するセキュリティ要求事項..... 120

1 はじめに

これまで製品業界ごとにセーフティ標準は策定されてきた。一方、サイバーセキュリティ標準をみると、組織運営に関する標準（ISO27001）と製品設計のセキュリティ評価・認証に関する標準（ISO15408）が策定されており、近年では、重要インフラストラクチャー（社会インフラに欠かせないプラントや施設）の制御システムを対象とした標準（IEC62443）も策定されている状況である。

Internet of Things（以下、IoT） の普及に伴い、身の回りにある生活機器が様々なネットワーク接続機能をもつことで、製品のセキュリティ懸念は増しているが、IoT 製品やサービスには欠かせないセキュリティ標準が生活機器に対しては未整備の状況である。欧米の動きをみると、各業界のセーフティ標準からセキュリティ標準を検討する動きが各所にみられる（英国の「Code of Practice for Consumer IoT Security」[21]や米国カリフォルニア州「接続される機器のセキュリティ法」（Senate Bill No.327 CHAPTER886）[1]など）。一方、日本においてもセキュリティに関する懸念は顕在化しており、検討すべき、という声は多いが、具体的検討に入っている分野はまだ少ない状況となっている。

このような状況の中で、一般社団法人 重要生活機器連携セキュリティ協議会（略称 CCDS。以下、CCDS）は設立された。本協議会では、生活機器セキュリティ標準の策定と、その標準に沿っていることを確認・検証した CCDS サーティフィケーションプログラムをセットにすることで、ユーザに安心して IoT 製品を使ってもらえる環境を整備することを目標に活動を行っている。

平成 28 年 7 月 5 日には IoT 推進コンソーシアム、経済産業省、総務省が「IoT セキュリティガイドライン」[2]として策定し、分野全体をカバーする共通事項を中心にまとめられた基本的な指針となっているが、CCDS では個々の製品分野において、具体的にセキュリティをカバーした設計・開発を進めるために、本分野別ガイドラインを策定した。

1.1　スマートホームのセキュリティの現状と課題

スマートホームとは、インターネット等に接続され、IoT に対応した住設・家電機器が設置された住宅であり、IoT・AI などの情報技術を活用して、利用者により安全・安心で快適な生活を提供する住まいである。

IoT 機器は、私達により身近なものになり、多種多様な方面で広がりを見せている。例えば家庭内に設置した住宅設備機器を遠隔で操作することを可能にすれば、家の施錠やシャッターの開閉、水回りの設備などをコントロールすることができる。IoT 機器の普及は著しく、今後はさらに増加すると想定されている。平成 28 年版情報通信白書[3]には、IHI Technology による推定を引用して、2015 年には世界で 約 54 億台であったコンシューマー向け IoT 機器が、2020 年には 2 倍以上の 125 億台になるとの予測が記載されている。

これらの IoT 機器は、インターネットに接続されていることで、様々なサービスの提供が可能であるが、同時に、情報セキュリティの脅威にさらされている。IoT 機器を標的としたマルウェアの存在も確認されており、その脅威は、生命や財産を脅かすものとなる可能性があることが危惧されている。

IoT 機器が攻撃を受ける要因は、利用者と提供者の二つの側面からみることができる。利用者に起因するものとしては、IoT 機器の初期設定での使用や、推測されやすいパスワードの設定、セキュリティへの知識不足などが挙げられる。提供者に起因するものとしては、初期設定で誰でもアクセスできてしまう設計や、利用者のセキュリティへの知識不足の想定が不十分であることなどである。

IoT 機器については、平成 28 年 3 月に独立行政法人情報処理推進機構（略称 IPA。以下、IPA）による「つながる世界の開発指針」[4]が公開され、IoT 機器の開発者が開発時に考慮すべきリスク・対策を指針として明確化された。また、平成 28 年 7 月には経済産業省及び総務省らによる「IoT セキュリティガイドライン」が公開され、IoT 機器やシステム、サービスのセキュリティ対策を検討するための考え方について提供者及び利用者を対象に提示された。例えば、IoT 機器の出荷後もセキュリティ上重要なアップデートを適切に実施することが挙げられている。

そして、CCDS が、ATM・IoT GW・車載器・オープン POS などの製品を横断したセキュリティサーティフィケーション制度である CCDS サーティフィケーションプログラムを準備中である。同プログラムでは、IoT 機器として満たすべき最低限のセキュリティ要件であるサーティフィケーションレベル１と、製品分野ごとに業界団体によって定義されるサーティフィケーションレベル２・３が定義されていて、自主評価と第三者認証によってセキュ

リティ要件を満たすことが確認された製品・サービスについて、サーティフィケーションレベル１にはサーティフィケーションマーク★、サーティフィケーションレベル２・３にはサーティフィケーションマーク★★、★★★が付与される仕組みの予定である。

このようにIoT機器が普及する一方、スマートホームはまだ黎明期で、住宅会社での取り組みも本格化しはじめた段階である。スマートホームのセキュリティもガイドライン策定には至っておらず、実証事業を通した検討がされてきた段階である。

例えば、平成28年度には総務省のIoTサービス創出支援事業として「スマートホームを想定した連携IoT機器のセキュリティ検証用テストベッドの構築」が実施された。同事業では、スマートホームのテストベッド環境を構築して、日常生活で使用するIoT機器のセキュリティ上の安全性を検証する実証事業が行われた。その結果を踏まえて、スマートホームにおけるIoTセキュリティ検証ガイドラインが策定されている。また、平成29年度には、経済産業省による「平成28年度補正　ＩｏＴを活用した社会システム整備事業（スマートホームに関するデータ活用環境整備推進事業)」が実施された。同事業では、実証実験の結果を踏まえて、スマートホーム分野のセキュリティ・製品安全対策指針（チェックリスト）が策定されている。

スマートホームのセキュリティガイドラインの策定に当たっては、IoT機器がどのような文脈で利用されるかを踏まえる必要がある。例えば、住宅とその利用者の生命・財産を守るためのIoT機器と、快適さ・便利さを改善するためのIoT機器は、それぞれのIoT機器と、それを操作するシステムに求められるセキュリティ要件が異なるはずである。しかし、前述の通り、住宅内に設置されるIoT機器は増加しているが、生命・財産に関わる領域にもセキュリティ面の安全性を十分に検討せずに導入される場合も見られる。このため、スマートホーム分野では、CCDSがセキュリティの認証を目的として定義したサーティフィケーションプログラムのサーティフィケーションレベル2および3について、保護すべき対象の重要度に応じてセキュリティ対策基準を策定し、それを満たすサービスにサーティフィケーションマーク★★、★★★を付与すべきである。利用者は、導入するスマートホームサービスのサーティフィケーションマークを確認することで、安心・安全なサービスであるか判断することができる。

本書では、IoT推進コンソーシアムの「IoTセキュリティガイドライン」[2]をもとにスマートホームホーム分野における構成要素・ライフサイクルを踏まえた具体的な対策指針を示すと共に、経済産業省の「サイバー・フィジカル・セキュリティ対策フレームワーク（CPSF)」[20]や英国の「Code of Practice for Consumer IoT Security」[21]、米国カリフォルニア州「接続される機器のセキュリティ法」(Senate Bill No.327 CHAPTER886)[1]に準拠し、スマートホーム分野としての必要可否を検討した上でセキュリティ要件の定義

を行う。また本書では、スマートホーム分野におけるセキュリティ対策として特徴的な事項を中心に検討するものとし、組織における情報セキュリティ管理やネットワークセキュリティ、またセーフティに関する対策等は対象としないため、他団体が定めた関連ガイドラインを参照されたい。

1.2　ガイドラインの対象範囲

本書は、スマートホーム環境による提供サービスや住宅（オフィス・施設・店舗などを除く個人向けの戸建て住宅・賃貸住宅・集合住宅を指す）、住設機器を対象とし、サービスやスマートホームの企画、設計、開発、運用に際して考慮すべきセキュリティの重要ポイントについて記載する。

1.3　本書の対象者

本書は、スマートホームサービスや住宅、住設機器の企画、設計、施工、運用に関わる企業の開発者を主な対象とし、各ライフサイクルにおいて考慮すべきセキュリティ対策の方針をガイドラインとしてまとめたものである。

本書の主な対象は、以下である。

1）住設機器の設計者、開発者、生産者、提供者
2）住設機器の運用保守を行う運用担当者
3）スマートホームの設計者、生産・施工者、監理者、現場監督者
4）スマートホームの運用保守を行う運用担当者

1.4 用語・略称

本書で使用されている用語について説明する。

表 1-1 用語一覧

用語	説明
住宅	人が住むための家。住居。すまい。本書ではオフィス、施設、店舗を除く、一般世帯向けの戸建て住宅、集合住宅、賃貸住宅等を指す。
住宅会社	住宅を企画、販売、設計、施工する会社。ハウスメーカー、工務店、ビルダー、設計事務所など。本書では、スマートホームの企画、販売、設計、施工、運用のいずれかを行う会社を指す。
スマートホーム	インターネット等の通信アーキテクチャを使用し、IoT に対応した住宅設備・家電機器が設置された住宅。
住設機器	住宅を構成する、または付随する設備。本書ではインターネット等とつながる住宅設備・家電を指す。住設と略記する場合もある。
ホームゲートウェイ	スマートホームに設置される通信機器。ホームゲートウェイは、宅内の住設・家電機器を外部のクラウドとセキュアに接続する役割も担う。
機器メーカークラウド	住設機器、家電メーカーが自社製品の管理・制御のために提供するクラウド。外部（例えば、第三者）に対し、対象機器の機能や情報へアクセスする API を提供する場合が多い。
現場監督	住宅の施工現場で、作業を指揮、監督すること。また、その人。
監理者	設計図通りに建物ができるよう、工事を指導・監督する人。
HEMS	Home Energy Management System。情報技術を活用して、一般家庭における家電などのエネルギー消費の見える化・効率化を図る管理システム。
エントリーポイント	スマートホームのサービス、IoT 機器、および通信経路において、外部からアクセス可能でセキュリティ上の脅威となりうる箇所。
ユーザインターフェース	利用者とスマートホームの間で情報をやり取りするための仕組み。スマートフォンのような画面表示と手入力によるものや、スマートスピーカーのような音声発話・認識によるものなど多様な方法がある。
デバイス	スマートホームに設置された住設機器・家電機器・センサーなどの IoT 機器。
リスク分析・評価	保護すべき資産と想定される脅威・被害を分析して、それらのリスク値（被害を受けた時の深刻度)からセキュリティ対策を定義するプロセス。

本書で使用されている略称について説明する。

表 1-2 略称一覧

略称	名称
API	Application Program Interface
CCDS	Connected Consumer Device Security council
CPU	Central Processing Unit
CSIRT	Computer Security Incident Response Team
CVSS	Common Vulnerability Scoring System
DoS	Denial of Service
ETSI	European Telecommunications Standards Institute
GW	Gateway
HEMS	Home Energy Management System
IEC	International Electrotechnical Commission
I/F	Interface
IoT	Internet of Things
IoT-GW	Internet of Things-Gateway
IP	Internet Protocol
IPA	Information-technology Promotion Agency
ISO	International Organization for Standardization
JPCERT/CC	Japan Computer Emergency Response Team Coordination Center
LAN	Local Area Network
OTA	Online Trust Alliance
OWASP	The Open Web Application Security Project
VPN	Virtual Private Network
WG	Working Group
Wi-Fi	Wireless Fidelity

2　スマートホームサービスの定義とシステム構成

スマートホーム分野において必要なセキュリティ対策を検討するにあたり、本章ではサービスの定義及び、サーティフィケーションとの関係の整理を行う。またスマートホームを構成するシステムを定義した上、サービスとして想定しているユースケースについても具体的な事例を提示する。

2.1　スマートホームサービスの定義

スマートホームに設置されたIoT機器の操作は、その状況によっては生命・財産に危害を及ぼす場合が考えられる。例えば、第三者によって脆弱性が悪用され、利用者による給湯器の設定が改ざんされた結果、火災や事故を誘発するケースや、電子的に管理された電子錠が不正に開錠され､盗難につながるケースなどが想定できる｡このようにスマートホーム分野では、サービスによって、提供機能やユースケース、対象機器が異なるため、保護すべき資産にも差異が生じる。特に生命・財産に影響する資産は、最優先で守られるべきであることを踏まえ、保護すべき資産の重要性に応じて、以下の２種類のサービスに分類を行った。

１）快適さや利便性に関わるサービス

宅内の住設機器や情報家電、センサー機器などがクラウド上のシステムと連携し、自動あるいは設定条件により制御され､利用者の快適さや利便性を向上させるサービスである。

サービス事例）

・空調・照明、電動シャッターなどのリモート制御や、スケジュール管理、センサー機器と連携した自動化等の製品・サービス

・電力測定や省エネなどの見える化に関わる製品・サービス

・日々の健康管理につながる製品・サービス　…など

２）生命・財産に関わるサービス

防犯用の監視カメラや電子錠、センサー機器、そして第三者サービス事業者に防犯システムや救命システム等の情報基盤と連携し、利用者の日々の安全や防犯、緊急時の救命措置にかかわるサービスである。

サービス事例）

・防犯や緊急時の救命にかかわる製品・サービス

・火災などの事故や怪我につながる恐れがあり厳格な管理が必要な製品・サービス　…など

以下に本書におけるサービス、システムの定義を示す。

表 2-1 本書におけるサービス・システムの定義

用語	定義
サービス	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、ハウスメーカー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や、機器やシステムのメーカー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などが想定される。
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「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システムなどが対象となる。また本書において、人による運用はシステムに含まれないものと定義する。

2.2 スマートホーム向け製品・サービスのセキュリティレベルの定義

CCDS は 2018 年 11 月に「IoT 分野共通セキュリティ要件ガイドライン 2018 年度版(案)」[5]をリリースした。このガイドラインでは、サーティフィケーション（認証）レベルを 3 階層のモデルとして定義し、それぞれ消費者にも分かりやすいよう★、★★、★★★と、星の数でセキュリティのレベルを表記する形式とした。また、第 1 階層の★レベルについては、「つながる機器最低限守るべき共通の要件」として、11 項目のセキュリティ要件を公開している。

スマートホーム分野においても、この階層モデルを踏襲し、最低限の基準である共通要件（★レベル）に準拠することを前提とした上で、★★レベルを「快適さや利便性に関わる製品・サービス」、★★★レベルを「生命・財産に関わる製品・サービス」と位置づけている。本書では★★、★★★の製品・サービスに対して、それぞれセキュリティ対策方針やセキュリティ要件の検討を行う。

スマートホーム分野におけるサーティフィケーション階層モデルを、図 2-1 に示す。

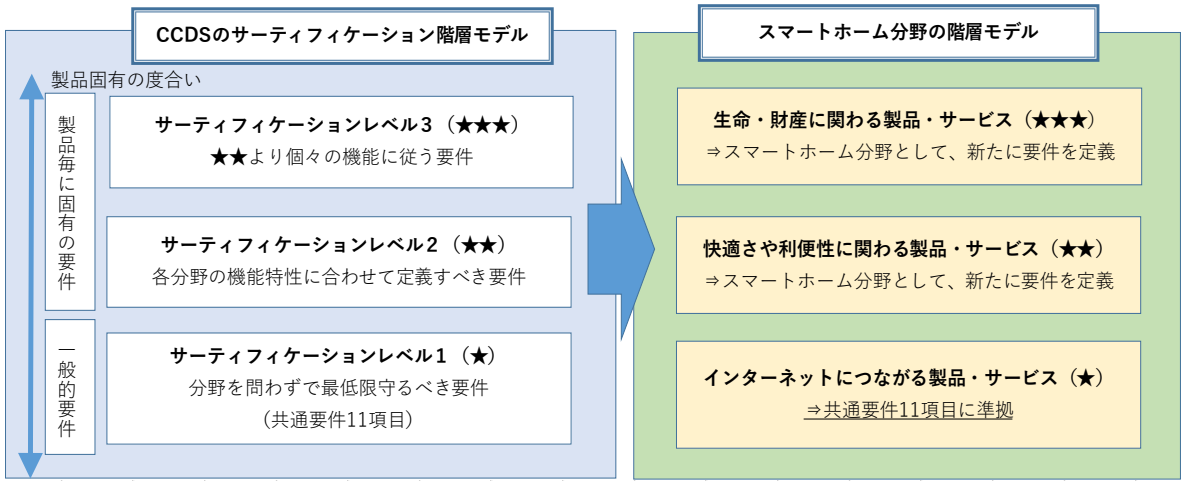

図 2-1 スマートホーム向け製品・サービスの階層モデル

また、それぞれのレベル定義を表 2-2 に示す。

表 2-2 スマートホーム向け製品・サービスのサーティフィケーションレベル

レベル	対応するサービス	説明
★★★	生命・財産に関わる製品・サービス（以下、★★★サービスとする）	★★レベルの要件に加え、生命・財産に影響を与える資産を保護する上で必要なセキュリティ対策を行う。
★★	快適さや利便性に関わる製品・サービス（以下、★★サービスとする）	★レベルの要件に加えて、快適さや利便性を実現する機能において必要なセキュリティ対策を行う。
★	インターネットにつながる製品・サービス	「IoT 分野共通セキュリティ要件ガイドライン」の共通要件１１項目に準拠する。

★★、★★★レベルにおけるサーティフィケーションは、スマートホームサービスを対象としており、5.5 節の「スマートホームサービスのセキュリティ要件」に対する適合性を検証するものである。

本書では、サービス全体として一定レベルのセキュリティ対策を保証するという考え方に基づくため、クラウド上のサービス情報基盤や、スマートホーム内の個別機器単体としてのセキュリティ対策を保証するものではない。従ってサービス情報基盤や機器に対して個別にサーティフィケーションの要件を定めることはしない。

ただし、サービス上の責任分界点を明確化するため、サービス情報基盤やスマートホーム内の個別機器については、5.6 節で定義した★★サービス、★★★サービスのセキュリ

ティ要求事項に準拠した対象を採用するものとする。例えば、同じ電子錠であっても、スマートフォンアプリの操作で開錠するようなユースケースであれば、「快適さや利便性に関わるサービス（★★）」に位置づけられ、 ★★サービスの要求事項に対する準拠が必要である。一方で宅内の異常通知に対して、最寄りの現場担当者が現地に駆け付け、遠隔開錠を行うユースケースであれば、 「生命・財産に関わるサービス（★★★）」 に位置づけられ、★★★サービスの要求事項に対する準拠が必要となる。

また、提供するサービスが★★、★★★のいずれに該当するかについては、下記の手順に沿って、サービス事業者が判断を行う。

1）サービスの企画段階において、ユースケースを検討し、構成される機器やシステムから、暫定的に該当するサービスを仮定する。

2）ユースケースをもとにリスク分析を実施し、個人情報などの重要なデータの取り扱いの有無、および生命・財産への影響の有無を検討し、該当するサービスを決定する。

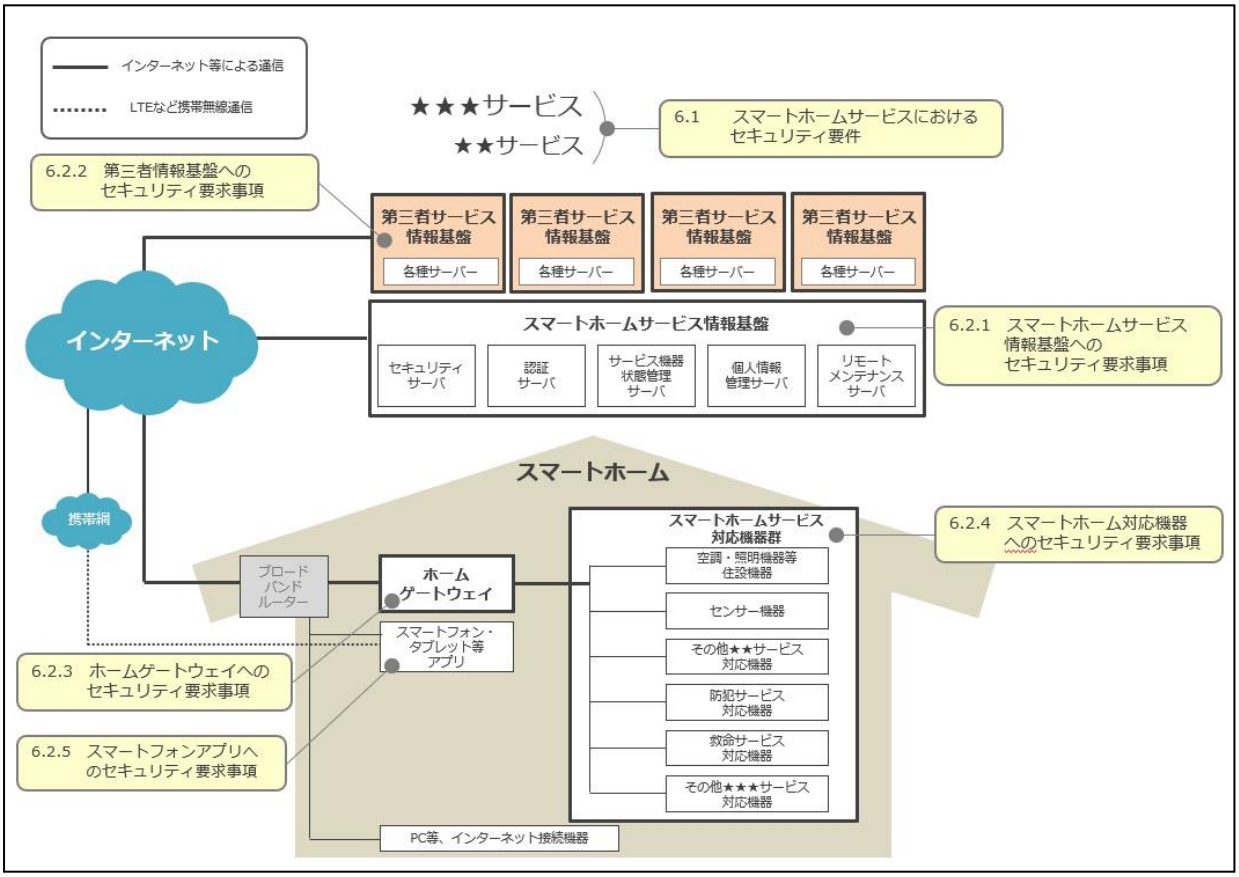

図 2-2 スマートホームサービスにおけるセキュリティ要件/要求事項の対応

なお、共通要件 11 項目の詳細は、「IoT 分野共通セキュリティ要件ガイドライン 2018 年度版（案）」[5]を参照のこと。

2.3　システムモデルの定義

スマートホームの基本的なシステムモデルを図 2-3 に示す。本モデルの検討では IPA の「IoT 開発におけるセキュリティ設計の手引き」の P59「図 5-3　スマートハウスの脅威と対策の検討例」を参考にした。

スマートホームに設置された機器を活用した利用者の生活を向上させるサービスを提供するために、その基盤となるスマートホームサービス情報基盤が構築される。スマートホームサービス情報基盤は、収集・蓄積したスマートホームや利用者の情報に応じて、宅内の機器を操作してサービスを実現する。機器の操作は、利用者が宅内・宅外から行う場合や、提供されるサービスによってはサービス事業者などの第三者が遠隔で操作する場合もある。

スマートホームサービス情報基盤からの機器の操作は、機器メーカークラウドから提供される API を利用する場合や、スマートホームサービス情報基盤から直接行う場合がある。後者の直接操作は、宅内ネットワークに接続された HEMS コントローラやエッジサーバを経由して行うため、スマートホームサービス情報基盤と宅内ネットワークをネットワークで接続する必要がある。特に生命・財産に関わる機器を操作する場合は、より安心・安全に機器を操作できるよう、宅内にホームゲートウェイを設置して、スマートホームサービス情報基盤との通信をセキュアにする。またホームゲートウェイは外部インターネットと、宅内スマートホーム環境の境界に位置し、セキュアゲートウェイとしての役割を担うため、一定のセキュリティ対策が保証されたサービス対応機器と、利用者が個別に追加した機器を区別できるような仕組みが望ましい。

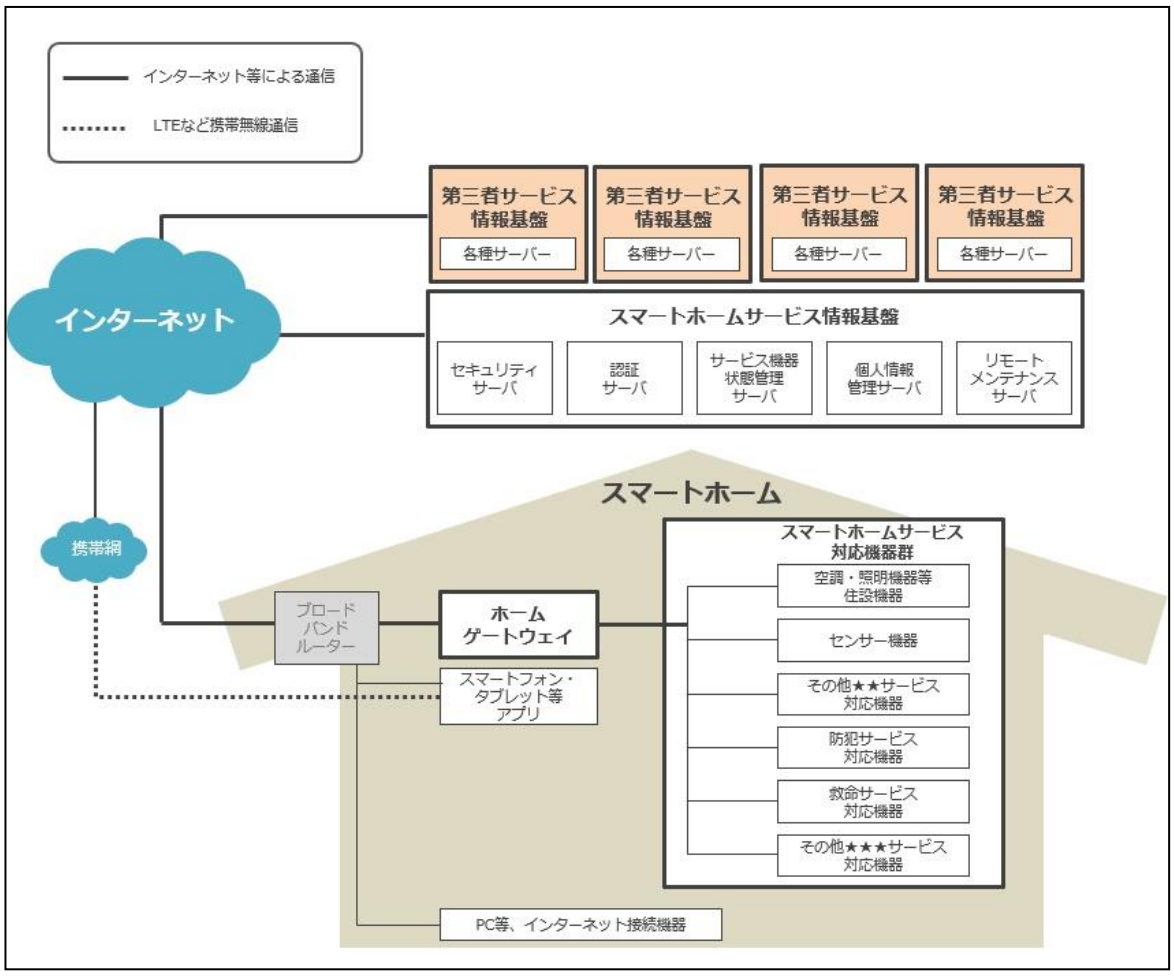

図 2-3 スマートホームのシステムモデル図

システムモデルの構成機器の説明を表 2-3 にまとめる。

表 2-3 システムモデル中の構成機器

名称	説明
■スマートホームサービス情報基盤 スマートホームを構成する機器の管理や、基本的なサービス提供用の情報システム。	
セキュリティサーバ	スマートホームサービス情報基盤のセキュリティ管理を行う。
認証サーバ	スマートホームサービス情報基盤の利用にあたり、利用者や運用者、ホームゲートウェイの認証を行う。
サービス機器状態管理サーバ	宅内のスマートホームサービス対応機器から送信された情報にもとづき、各機器の状態を管理する。
個人情報管理サーバ	スマートホームサービス情報基盤を利用する利用者のユーザ情報を管理する。
リモートメンテナンスサーバ	ホームゲートウェイやスマートホームサービス対応機器の更新用ソフトウェアの管理や更新時の配信を行う。
■スマートホーム	
ホームゲートウェイ	インターネットとスマートホームの間に設置され、セキュリティを担保し、情報基盤と住設機器・サービス対応機器を接続する。
空調・照明機器等 住宅設備機器（住設機器）	住宅に設置される空調設備・照明設備などの設備機器。
家電機器	一般家庭に設置されるテレビ・パソコン・冷蔵庫・洗濯機などの電気機器。
センサー機器	住宅の温度・湿度・人感などのセンサー機器。
その他★★サービス対応機器	HEMS 用コントローラや情報家電等、★★サービスに対応する上記以外の機器。
■第三者サービス情報基盤 防犯や救命サービスなど付加的なサービスを提供する上で連携するコールセンターなどの情報システム。	
各種サーバ（クラウド他）	サービス提供を行う上で必要な各種サーバが、クラウドなどに設置される。

2.4　ユースケースの定義

スマートホーム向けサービスの提供で利用する各種 IoT 機器(住設･家電機器､センサー)は、その利用用途によってサイバーセキュリティでの重要性が異なってくる。例えば、人感センサーは､生活を便利にするために利用される場合（例えば､室内扉の自動開閉）と、生命・財産に関わる場合（例えば、生死判定）では、後者においてより厳重なサイバーセキュリティ対策が求められる。「製品分野別セキュリティガイドライン IoT-GW 編_Ver2.0」[10]でも触れられているように､ユースケースによってリスクとなる要因､サイバーセキュリティの特徴・課題が異なるため、★★サービス、★★★サービスそれぞれのユースケース事例を定義した上で、セキュリティ対策の検討を行う。

2.4.1 ★★サービスにおけるユースケース事例

保護すべき資産が重要な情報の場合として、利用者ごとに設定されたスケジュールに応じて電動シャッターの自動開閉を行うサービス（以下、シャッター自動開閉サービス）のユースケースを用いる（図 2-4、表 2-4)。

本サービスは、利用者が操作するアプリから設定されたスケジュールに応じて、スマートホームサービス情報基盤から住宅に設置された電動シャッターを遠隔操作で制御するものである。電動シャッターの遠隔操作が個人情報と紐づくことで、例えば利用者の生活パターンや在宅情報など個人情報を知ることができる｡このため､本ユースケースは★★サービスに該当する。

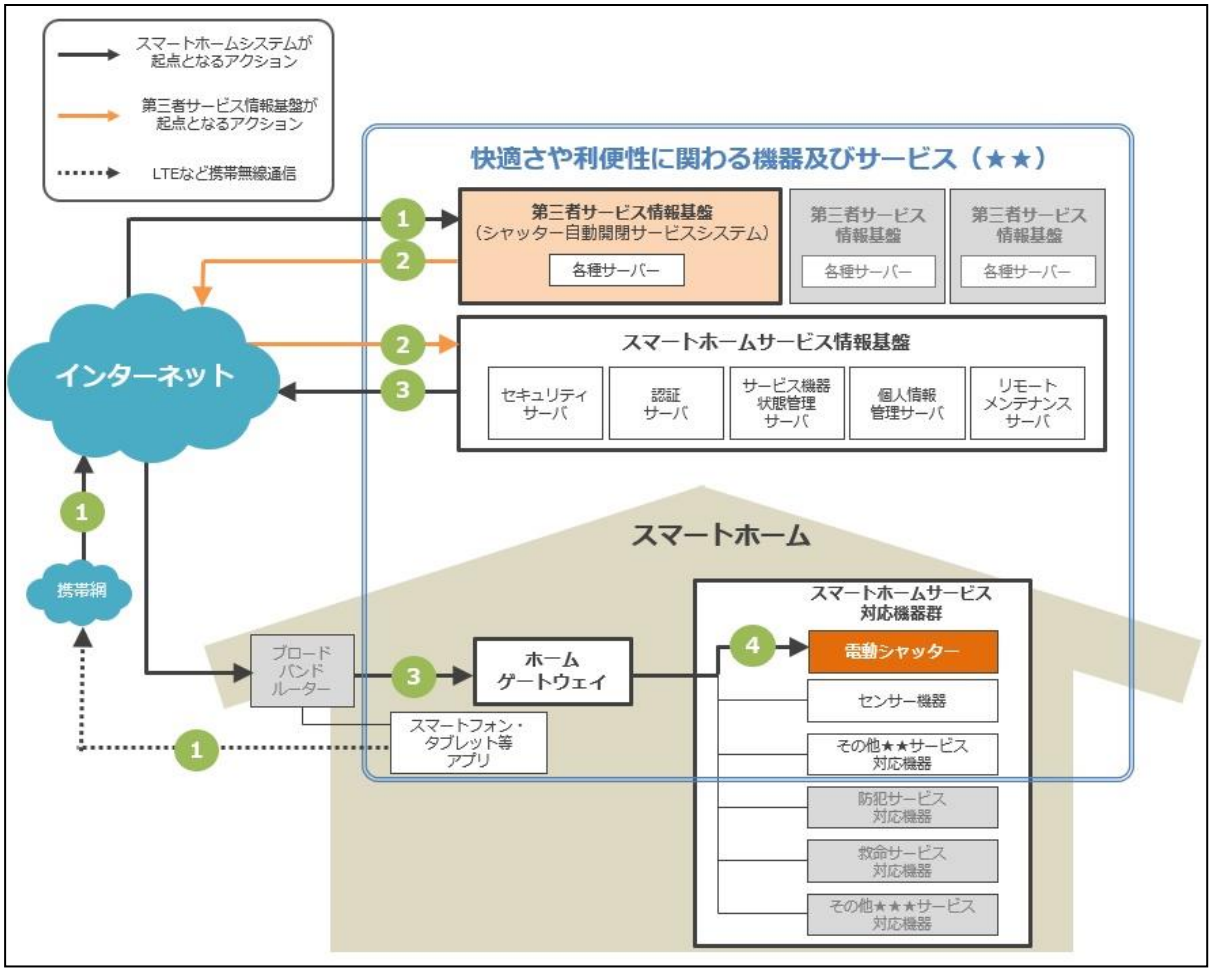

図 2-4 スマートホームのユースケース（シャッター自動開閉サービス）

表 2-4 スマートホームのユースケース（シャッター自動開閉サービス）

図番号	アクション	説明
1	開閉スケジュールの設定	利用者が操作するアプリから電動シャッターの開閉スケジュールが設定されると、シャッター自動開閉サービスシステムに利用者と紐づけてその内容が登録される。
2	電動シャッター開閉の指示	シャッター自動開閉サービスシステムは、指定された時刻になると、スマートホームサービス情報基盤に電動シャッターの開閉を指示する。
3	スマートホームサービス情報基盤から電動シャッター開閉の実行	電動シャッターの開閉を指示されたスマートホームサービス情報基盤は、電動シャッターの開閉を当該住宅のホームゲートウェイに指示する。
4	電動シャッターの開閉操作	ホームゲートウェイは、電動シャッターの開閉を行う。

2.4.2 ★★★サービスにおけるユースケース事例

保護すべき資産が生命・財産の場合として、住宅の異常検知時に駆けつける防犯サービス（以下、駆けつけ防犯サービス）のユースケースを用いる（図 2-5、表 2-5）

本サービスは、住宅に設置された防犯センサーで侵入などの異常を検知した際に、通知を受けた最寄りのスタッフが当該住宅に駆けつけて、コールセンターから遠隔操作で解錠された玄関から住宅内の状況を確認、必要に応じて対策を行うものである。

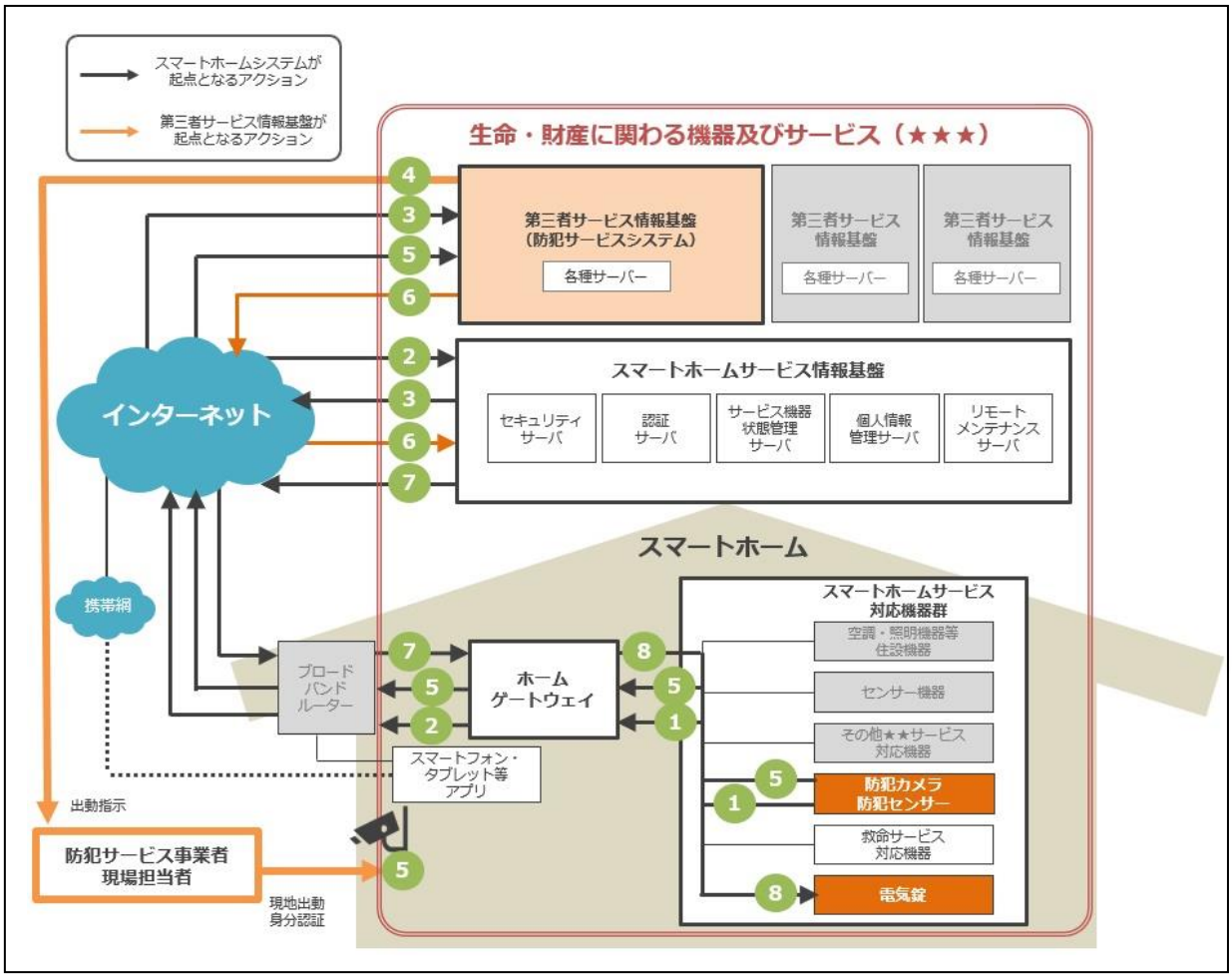

図 2-5 スマートホームのユースケース（駆けつけ防犯サービス）

表 2-5 スマートホームのユースケース（駆けつけ防犯サービス）

図番号	アクション	説明
1	防犯センサー・防犯カメラの異常検知	住宅に設置された防犯センサー・防犯カメラが、侵入などの異常を検知する。防犯センサー・防犯カメラの状態はホームゲートウェイで監視されていて、異常が発生次第検知される。
2	スマートホームサービス情報基盤への通知	住宅の異常検知は、セキュアな通信経路で、ホームゲートウェイからスマートホームサービス情報基盤に通知される。
3	防犯サービス事業者への通知	スマートホームサービス情報基盤は、防犯サービス事業者のコールセンターが監視する防犯サービスシステム画面に、住宅の異常検知を表示する。
4	現場担当者への出動指示	防犯サービス事業者は、異常を検知した住宅に出動するよう、最寄りの現場担当者に指示する。
5	現場担当者の到着確認	現場担当者が当該住宅に到着したこと、また到着した人物が正しい現場担当者であることを認証する。
6	電気錠解錠の指示	現場担当者の到着を確認したコールセンター担当者は、指示系統に従って承認を得た後、駆けつけ防犯サービス画面で当該住宅の玄関の電気錠を解錠する操作を行う。
7	スマートホームサービス情報基盤から電気錠解錠の実行	電気錠の解錠を指示されたスマートホームサービス情報基盤は、セキュアな通信経路で、電気錠の解錠を当該住宅のホームゲートウェイに指示する。
8	電気錠の解錠操作	ホームゲートウェイは、玄関の電気錠を解錠する。

3 スマートホーム向け製品・サービスのリスク分析

リスク分析・評価は、スマートホームに提供するサービスに存在するサイバーセキュリティ上のリスクと、それに対策するためのセキュリティ要件を定義するために行われる。リスク分析・評価では、サービス提供において守るべき情報資産とそれらに発生すると想定される脅威とそのリスク特性を洗い出し、脅威が発生したときの影響度を計算する。そして、分析したリスク特性と影響度から、リスクへの対策方法とその優先順位を判断する。

本章では、スマートホーム向けサービスにおけるサイバーセキュリティ上のリスク分析・評価について、その概要と手順を説明する。

3.1 リスク分析・評価の手順

スマートホーム向けサービスのリスク分析は、以下の流れで行う。以下では、各手順の詳細な内容を説明する。

表 3-1 リスク分析・評価の手順

No.	手順内容	説明
1	ユースケースの定義	分析・評価対象のシステムの構成要素と、その利用者、およびシステムと利用者のやりとりを定義する。
2	保護すべき資産の抽出	ユースケースに登場するシステムが扱う情報資産のうち、保護すべき対象を抽出する。
3	想定される脅威の分析	システムモデルをもとにエントリーポイントを特定し、想定される脅威を分析する。
4	想定される脅威の詳細分析	想定される脅威事例を検討し、詳細な分析を行う。
5	リスク値の計算	想定される脅威について、それが発生したときの影響度を表すリスク値を計算する。
6	セキュリティ対策の定義	リスク値による分析・評価結果から、サービスの提供にあたって取るべきセキュリティ対策を定義する。セキュリティ対策の定義にあたっては、インシデントの発生頻度、発生したときの影響度（リスク値）、また対策の実施にかかるコストを総合して検討する必要がある。

3.2　保護すべき資産の抽出

前節で定義したユースケースについて、保護すべき資産を洗い出す。スマートホームサービスを想定した場合、特に★★★サービスでは、緊急時の救命に関わる機能や、日々の防犯に関する機能の提供が攻撃によって阻害されることで、利用者の生命や財産に影響を与える可能性があるため、サービスを継続的に提供できること（＝可用性）が重要な保護資産として考えられる。また、スマートホームの製品・サービスを想定した場合、対象となる資産は、サービスを構成する要素（IoT 機器・クラウドなど）ごとに、それらが扱う情報、それらが提供する機能などから漏れなく導き出す必要がある。

以下表 3-2 に、保護すべき資産の例を列挙する。

表 3-2 スマートホームのシステム・製品を対象とした保護すべき資産の例

エントリーポイント	機器名	資産種別	保護すべき資産
スマートホームサービス情報基盤	セキュリティサーバ	一次資産（※1）	ハードウェア、ソフトウェア（セキュリティ機能それ自体）
			設定情報、ログ情報
	認証サーバ	一次資産	ハードウェア、ソフトウェア（機能それ自体）
		二次資産（※2）	認証情報
			暗号鍵
	サービス機器状態管理サーバ	一次資産	ハードウェア、ソフトウェア（機能それ自体）
			機器の状態管理情報
	個人情報管理サーバ	一次資産	ハードウェア、ソフトウェア（機能それ自体）
			個人情報（利用者の氏名、住所、電話番号等）
	リモートメンテナンスサーバ	一次資産	ハードウェア、ソフトウェア（機能それ自体）
			アップデートソフトウェア
スマートホームサービス情報基盤とインターネット間の通信経路	―	一次資産/二次資産	通信経路上のデータ
第三者サービス情報基盤	第三者サービス提供サービス用サーバ	一次資産	ハードウェア、ソフトウェア（機能それ自体）
			機器の状態管理情報
			個人情報（利用者の氏名、住所、電話番号等）
			設定情報、ログ情報

		二次資産	認証情報（認証キー）
			暗号鍵
第三者サービス情報基盤とインターネット間の通信経路	—	一次資産/二次資産	通信経路上のデータ
ホームゲートウェイ	ホームゲートウェイ	一次資産	ハードウェア、ソフトウェア（機能それ自体）
			設定情報、ログ情報
			個人情報（対象機器の実装機能に依存する）
		二次資産	認証情報
			暗号鍵
ホームゲートウェイとインターネット間の通信経路	—	一次資産/二次資産	通信経路上のデータ
スマートホームサービス対応機器群	空調・照明機器等	一次資産	ハードウェア、ソフトウェア（機能それ自体）
			制御信号
		二次資産	認証情報
	センサー機器	一次資産	ハードウェア、ソフトウェア（機能それ自体）
			センシングデータ
		二次資産	認証情報
	その他★★サービス対応機器	一次資産	ハードウェア、ソフトウェア（機能それ自体）
			制御信号
			センシングデータ
			個人情報（対象機器の実装機能に依存する）
		二次資産	認証情報
	防犯サービス対応機器	一次資産	ハードウェア、ソフトウェア（機能それ自体）
			制御信号
			センシングデータ
			個人情報（対象機器の実装機能に依存する）
		二次資産	認証情報
	救命サービス対応機器	一次資産	ハードウェア、ソフトウェア（機能それ自体）
			制御信号
			センシングデータ
			個人情報（対象機器の実装機能に依存する）

		二次資産	認証情報
ホームゲートウェイと対応機器間の通信経路	—	一次資産/二次資産	通信経路上のデータ ・制御信号、センシングデータ ・個人情報（対象機器の実装機能に依存する） ・認証情報
スマートフォンアプリ	—	一次資産	ソフトウェア（機能それ自体）
			制御信号
			スマーフォン内の個人情報や機微情報
		二次資産	認証情報
スマートフォンとホームゲートウェイ間の通信経路	—	一次資産/二次資産	通信経路上のデータ

※1、※2 注記）表において使用される一次資産、二次資産については、以下のように定義を行った。

・一次資産：保護すべき資産そのものを一次資産と定義。

・二次資産：一次資産を保護するために必要な暗号化対策や、認証に関する副次的な資産を二次資産と定義。

3.3 想定される脅威の分析

前節において抽出した保護すべき資産に対して、サイバーセキュリティ上の脅威を分析する。

3.3.1 スマートホームの製品・システム上の想定脅威

脅威の分析では、スマートホームのシステムモデルを用いて、エントリーポイント（攻撃可能なポイント）を抽出し、それぞれのエントリーポイントにおいて想定される脅威の分析を行う。本書では、Microsoft が提唱した脅威分析手法の STRIDE モデル[11]を CCDS が拡張した STRIDE＋CCDS モデル[12]を用いる。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。STRIDE はこれらの英語名称の頭文字から名づけられた）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。STRIDE＋CCDS モデルでは、IoT 機器・システムを想定し、さらに 5 種類の脅威が追加されている。

表 3-3 STRIDE+CCDS モデルによる脅威分類の一覧

種別	脅威	説明
STRIDE モデル	なりすまし	コンピューターに対し、他のユーザや機器を装うこと
STRIDE モデル	データ改ざん	権限なしでデータを改ざんし、データの完全性を失わせること
STRIDE モデル	否認	ユーザがあるアクションを行ったことを否認し、相手はこのアクションを証明する方法がないこと
STRIDE モデル	情報の暴露	アクセス権限を持たない個人に情報が公開されること
STRIDE モデル	サービス不能（DoS）	正規のユーザがサーバやサービスにアクセスできないよう妨害すること
STRIDE モデル	権限昇格	権限のないユーザがアクセス権限を得ること
CCDS による追加脅威	不正アクセス	アクセス権限を持たない者にアクセスされること
CCDS による追加脅威	マルウェア感染	他の機器への汚染源になる。ランサムウェアなどにより業務妨害を受けること
CCDS による追加脅威	踏み台	他の機器へ不正アクセス等を行う際の中継地点として使用されること
CCDS による追加脅威	不正改造	不正（違法）なハード、ソフトウェアの改造により、内部データを抜き取ったり、脆弱性の要因を組み込まれたりすること
CCDS による追加脅威	未知の脆弱性	まだ公知となっていない脆弱性や、新たな攻撃手法による脆弱性のこと

上記のモデルを踏まえて、保護すべき資産にどのような脅威が及ぶかを、システムモデルをもとに、エントリーポイント（攻撃可能なポイント）を対象に漏れなく検討する。下記図 3-1 が分析事例となるが、エントリ―ポイントについては、システムモデル上の機器や通信経路上に赤い印をつけ、①～⑩の番号（EP 番号）を記載することで表 3-4 と関連づけている。

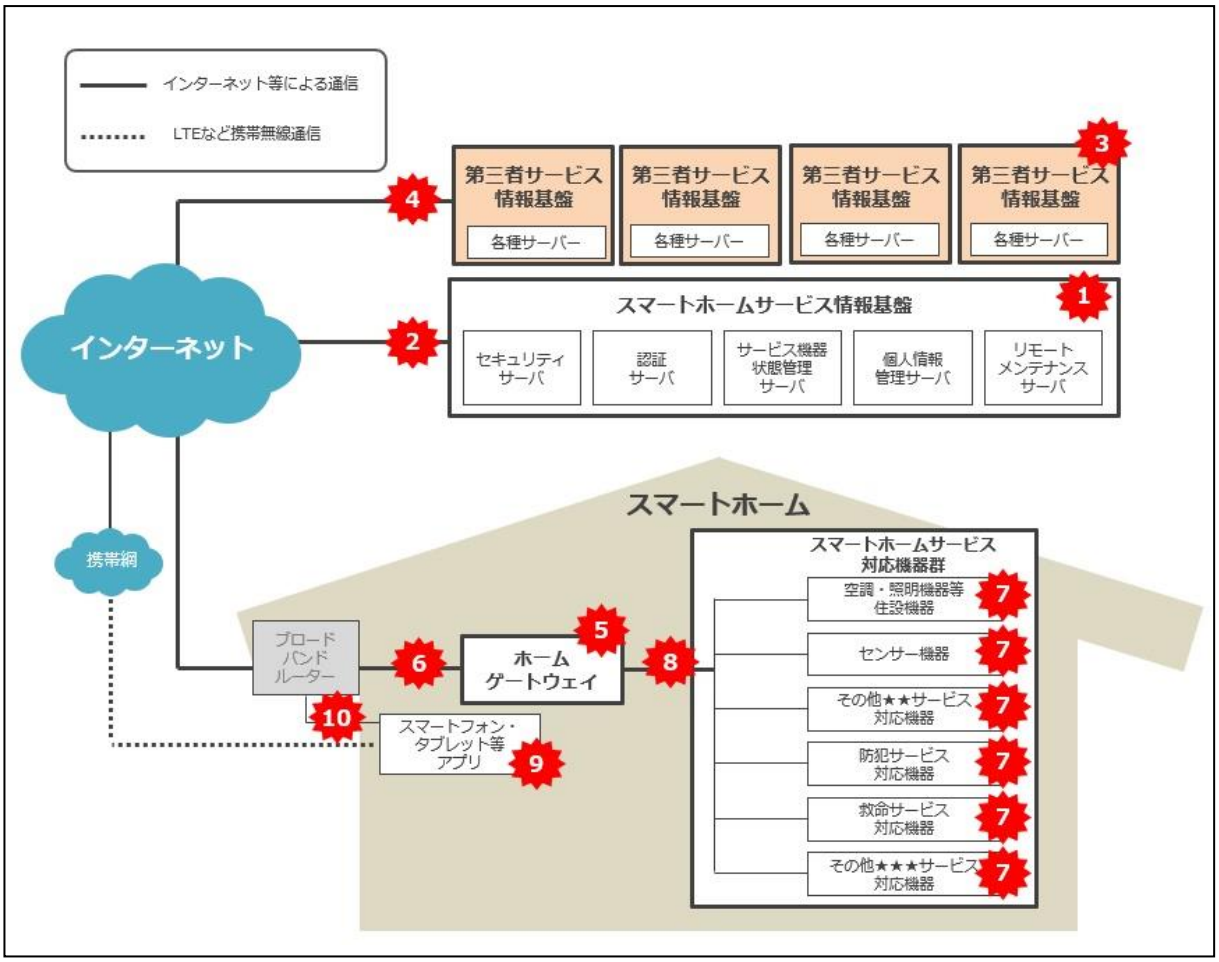

図 3-1 スマートホームのシステムモデルにおける脅威分析事例

表 3-4 STRIDE+CCDS モデルによる脅威分類事例

エントリーポイント	システムモデルにおけるエントリーポイントの番号（EP 番号）	STRIDE＋CCDS モデルによる脅威分類
スマートホームサービス情報基盤	EP①	不正アクセス
		情報の暴露
		データ改ざん
		なりすまし
		マルウェア感染
		サービス不能
スマートホーム情報基盤とインターネット間の通信経路	EP②	情報の暴露
第三者サービス情報基盤	EP③	不正アクセス
		情報の暴露

		データ改ざん
		なりすまし
		マルウェア感染
		サービス不能
第三者サービス情報基盤とインターネット間の通信経路	EP④	情報の暴露
ホームゲートウェイ	EP⑤	不正アクセス
		情報の暴露
		データ改ざん
		なりすまし
		マルウェア感染
		サービス不能
		踏み台
ホームゲートウェイとインターネット間の通信経路	EP⑥	情報の暴露
スマートホームサービス対応機器群	EP⑦	不正アクセス
		情報の暴露
		データ改ざん
		なりすまし
		マルウェア感染
		踏み台
スマートホームサービス対応機器群とホームゲートウェイ間の通信経路	EP⑧	なりすまし
		情報の暴露
スマートフォンアプリ	EP⑨	情報の暴露
		なりすまし
スマートフォンとホームゲートウェイ間の通信経路	EP⑩	なりすまし
		情報の暴露

3.3.2 サイバーセキュリティ以外の想定脅威

スマートホームサービスにおいて、可用性を重要な資産と位置付けた場合、サイバーセキュリティ以外の脅威についても検討を行う必要がある。具体的な事例としては、以下のような脅威が想定される。

・災害、火災等の事故
・ハードウェアの故障
・ソフトウェアの不具合
・運用担当者によるオペレーションミスや過失、内部不正
・メンテナンス作業（ソフトウェア、ハードウェアのアップデート）
・サービスに関連する事業者のサービス停止や事業撤退
・物理的な侵入によるハードウェア、ソフトウェアへの破壊行為

本書の５章では、本節のサイバーセキュリティ上の脅威分析結果と共に、上述のサイバーセキュリティ以外の脅威に対しても、対策すべき内容の検討を行う。

3.4 想定される脅威の詳細分析

前節までの分析結果を踏まえ、想定される攻撃の事例やリスク特性等を加え、更に詳細な分析を行う。

なお、リスク特性については、以下の記述する項目（表 3-5）を付与するものとする。

表 3-5 想定される脅威の詳細分析項目一覧

No.	項目	内容
想定される脅威の内容		
1	エントリーポイント	脅威が想定する対象のエントリーポイント（IoT 機器、クラウド）
2	保護すべき資産	脅威に晒される対象の資産（表 3-2 参照）
3	STRIDE+CCDS モデルによる脅威分類	想定される脅威の分類（表 3-3 参照）
4	想定される脅威の事例	想定される脅威の事例
リスク特性		
5	接続 I/F	脅威の侵入ルート（表 3-6 参照）
6	Who（誰がつなげたか）	エントリーポイントに接続した主体（表 3-7 参照）
7	Whom（何が危害をうけたか）	脅威が影響を与える対象（表 3-8 参照）

8	Where（どこで発生したか）	脅威が発生した箇所（表 3-9 参照）

接続 I/F に記載する項目を以下に示す。

表 3-6 接続 I/F 項目

A)有線接続による接続 I/F		
No.	項目	内容
1	Ethernet	CAT ケーブルを通信媒体とし 10Mbps～１Gbps のデータ伝送を行う規格であり、IEEE802.3 として規格化されている。
2	HD-PLC	2～30Mhz の周波数帯域を用いることで、複数の HDTV 映像通信を実現する高速 PLC の規格。
3	上記以外の有線通信	上記１、２以外の有線通信。
B)無線接続による接続 I/F		
No.	項目	内容
4	Wi-Fi	Wi-Fi(wireless fidelity)は、WiFi Aliance によって IEEE802.11 シリーズ（IEEE802.11a/IEEE802.11b）を利用した無線 LAN 機器間の相互接続性を認証されたこと（Wi-Fi Certified）を示す、ブランド名である。
5	Bluetooth	数 m から数十 m 程度の距離の情報機器間で、電波を使い簡易な情報のやりとりを行う使用される。
6	ZigBee	ZigBee とは、センサーネットワークを主目的とする近距離無線通信規格の一つであり、基礎部分の（電気的な）仕様は IEEE 802.15.4 として規格化されている。論理層以上の機器間の通信プロトコルについては「ZigBee Alliance」が仕様の策定を行っている。
7	Wi-SUN	Wi-SUN とは、Wireless Smart Utility Network の略で、IEEE802.15.4g 規格をベースに相互接続を有する無線通信規格を業界団体「Wi-SUN Alliance」が標準化を行ってきた規格。
8	特定小電力無線	ライフスタイルやビジネスシーンが多様化し、近距離間での簡易連絡用のコミュケーション手段を求める声が強くなった現代、比較的狭いサービスエリアにおける無線通信の需要は増加している。こうした背景から、「特定小電力無線局」に対する制度が作られ、総務省で定める一定の条件を満たした無線設備であれば、無線従事者規格も無線局免許も必要とせず、広く一般の人々が利用できる。
9	LTE/LTE-Advanced	デジタル携帯電話の通信方式。
10	上記以外の無線通信	上記 4～10 以外の無線通信。

参考）一般社団法人 情報通信技術委員会（TTC）の「TR-1043」、「TR-1064」を参考に CCDS で作成。

Who・Whom・Where に記述される内容は以下の通りである。これらは、IPA の「つながる世界の開発指針第 2 版」[14]に記載された「つながりのパターン」「守るべきもの」「リスク箇所」を参考に、スマートホーム向けサービス用に定義した。

表 3-7 Who（誰がつなげたか）項目

No.	項目	内容
1	機器メーカー	IoT 機器メーカーが設計時に想定している接続の場合。
2	サービス事業者	サービスを構築するために機器やシステムを接続した場合。これには、機器メーカーが設計時に想定していなかった接続が含まれる。
3	ユーザ（意図的）	ユーザによる意図的な接続の場合。
4	ユーザ（誤接続）	ユーザによる誤った接続の場合。
5	攻撃者	脆弱性を狙った悪意を持った接続の場合。
6	偶発的	接続を行うときに偶発的に接続された場合。

表 3-8 Whom（何が危害をうけたか）項目

No.	項目	内容
1	IoT 機能	IoT 機器がシステムに接続するために必要な機能(通信、セキュリティ対策など)
2	本来機能	IoT 機器やシステムが本来提供する機能
3	サービス	IoT 機器およびシステムが連携して提供されるサービス
4	情報	ユーザの個人情報、収集した機器情報、IoT 機器やシステムの設定情報
5	生命・財産	ユーザ自身の生命、ユーザの財産
6	その他	上記以外の対象

表 3-9 Where（どこで発生したか）項目

No.	項目	内容
1	通常使用 I/F	ユーザ用操作パネル、サービス用有線／無線 I/F、USB 端子など
2	保守用 I/F	管理者用操作パネル、遠隔管理用通信 I/F、ソフトウェア更新用 USB 端子など
3	非正規 I/F	ふさぎ忘れた不要ポート、製造時にだけ使用する USB 端子など
4	内包リスク	故障の原因となる欠陥・バグ、攻撃の対象となる脆弱性、故障・悪用などで危害を及ぼす機能など
5	物理的接触	直接、本体に接触（部品の不正交換・改造など）

上記の項目に沿って、スマートホームを構成するシステム、機器に対して脅威の詳細分析を実施した例を、下記表 3-10、表 3-11 に示す。

表 3-10 スマートホームサービス・第三者サービスの情報基盤に対する詳細脅威分析事例

エントリーポイント	EP 番号	保護すべき資産	STRIDE＋CCDS モデルによる脅威分類	想定される脅威の事例	接続 I/F 表 3-6	Who 表 3-7	Whom 表 3-8	Where 表 3-9
スマートホームサービス情報基盤	EP①	【一次資産】 ・ハードウェア、ソフトウェア（セキュリティ機能それ自体） ・設定情報、ログ情報 ・機器の状態管理情報 ・個人情報（利用者の氏名、住所、電話番号等） ・アップデートソフトウェア 【二次資産】 ・認証情報 ・暗号鍵	不正アクセス	サービス情報基盤に対する不正アクセス（既知の脆弱性を突いた攻撃）	Ethernet	攻撃者	★★ サービス ★★★ 生命・財産	通常使用 I/F
			情報の暴露	サービス情報基盤内のデータに対する情報窃取（アクセス制御、認証不備）	Ethernet	攻撃者	★★ 情報 ★★★ 情報	通常使用 I/F
			データ改ざん	サービス情報基盤のデータ、設定値の改ざん	Ethernet	攻撃者	★★ サービス ★★★ 生命・財産	通常使用 I/F
			なりすまし	API 経由の通信において第三者サービス情報基盤、ホームゲートウェイになりすまし、改ざんメッセージによる攻撃が行われる	Ethernet	攻撃者	★★ サービス ★★★ 生命・財産	通常使用 I/F

			マルウェア感染	サービス情報基盤のマルウェア感染（外部インターネット経由の攻撃）	Ethernet	攻撃者	★★ サービス ★★★ 生命・財産	通常使用 I/F
			サービス不能	DDoS（DoS）攻撃	Ethernet	攻撃者	★★ サービス ★★★ 生命・財産	通常使用 I/F
			情報の暴露	持ち込まれたストレージデバイスによる情報の暴露	上記以外の有線通信	サービス事業者	★★ 情報 ★★★ 情報	非正規 I/F
			マルウェア感染	持ち込まれたストレージデバイスによるマルウェア感染	上記以外の有線通信	サービス事業者	★★ サービス ★★★ 生命・財産	非正規 I/F
			情報の暴露	アップデート用のソフトウェアの情報窃取	Ethernet	攻撃者	★★ 情報 ★★★ 情報	保守用/IF
			データ改ざん	アップデート用のソフトウェアの改ざん	Ethernet	攻撃者	★★ サービス	保守用/IF

							★★★ 生命・財産	
スマートホーム 情報基盤と インターネット間 の通信経路	EP②	【一次資産/二次資産】 通信経路上のデータ	情報の暴露	中間者攻撃によるインターネット経路上の情報窃取	Ethernet	攻撃者	★★ 情報 ★★★ 情報	通常使用 I/F
第三者サービス 情報基盤	EP③	【一次資産】 ・ハードウェア、ソフトウェア（機能それ自体） ・設定情報、ログ情報 ・機器の状態管理情報 ・個人情報（利用者の氏名、住所、電話番号等） 【二次資産】 ・認証情報 ・暗号鍵	不正アクセス	サービス情報基盤に対する不正アクセス（既知の脆弱性を突いた攻撃）	Ethernet	攻撃者	★★ サービス ★★★ 生命・財産	通常使用 I/F
			情報の暴露	サービス情報基盤内のデータに対する情報窃取（アクセス制御、認証不備）	Ethernet	攻撃者	★★ 情報 ★★★ 情報	通常使用 I/F
			データ改ざん	サービス情報基盤のデータ、設定値の改ざん	Ethernet	攻撃者	★★ サービス ★★★ 生命・財産	通常使用 I/F
			なりすまし	API 経由の通信においてスマートホームサービス情報	Ethernet	攻撃者	★★ サービス	通常使用 I/F

				基盤になりすまし、改ざんメッセージによる攻撃が行われる			★★★ 生命・財産	
			マルウェア感染	サービス情報基盤のマルウェア感染（外部インターネット経由の攻撃）	Ethernet	攻撃者	★★ サービス ★★★ 生命・財産	通常使用 I/F
			サービス不能	DDoS（DoS）攻撃	Ethernet	攻撃者	★★ サービス ★★★ 生命・財産	通常使用 I/F
			情報の暴露	持ち込まれたストレージデバイスによる情報の暴露	上記以外の有線通信	ユーザ（意図的）	★★ 情報 ★★★ 情報	非正規 I/F
			マルウェア感染	持ち込まれたストレージデバイスによるマルウェア感染	上記以外の有線通信	ユーザ（意図的）	★★ サービス ★★★ 生命・財産	非正規 I/F
			情報の暴露	アップデート用のソフトウェアの情報窃取	Ethernet	攻撃者	★★ 情報	保守用/IF

							★★★ 情報	
			データ改ざん	アップデート用のソフトウェアの改ざん	Ethernet	攻撃者	★★ サービス ★★★ 生命・財産	保守用/IF
第三者サービス情報基盤とインターネット間の通信経路	EP④	【一次資産/二次資産】 通信経路上のデータ	情報の暴露	中間者攻撃によるインターネット経路上の情報窃取	Ethernet	攻撃者	★★ 情報 ★★★ 情報	通常使用 I/F

表 3-11 ホームゲートウェイ・スマートホーム対応機器群・スマートフォンアプリに対する詳細脅威分析事例

エントリーポイント	EP 番号	保護すべき資産	STRIDE＋CCDS モデルによる脅威分類	想定される脅威の事例	接続 I/F	Who	Whom	Where
ホーム ゲートウェイ	EP⑤	【一次資産】 ・ハードウェア、ソフトウェア（機能それ自体） ・設定情報、ログ情報 ・個人情報（利用者の氏名、住所、電話番号等） 【二次資産】 ・認証情報 ・暗号鍵	不正アクセス	ホームゲートウェイに対する不正アクセス（既知の脆弱性を突いた攻撃）	Ethernet	攻撃者	★★ 本来機能 ★★★ 本来機能	通常使用 I/F
					Ethernet	攻撃者	★★ サービス ★★★ 生命・財産	通常使用 I/F
			情報の暴露	ホームゲートウェイ内のデータ、設定値の情報窃取（アクセス制御、認証不備）	Ethernet	攻撃者	★★ 情報 ★★★ 情報	通常使用 I/F
			データ改ざん	ホームゲートウェイ内のデータ、設定値の改ざん	Ethernet	攻撃者	★★ 本来機能 ★★★ 本来機能	通常使用 I/F
					Ethernet	攻撃者	★★ サービス	通常使用 I/F

							★★★ 生命・財産	
			なりすまし	API 経由の通信において サービス情報基盤になりすまし、改ざんメッセージによる攻撃が行われる	Ethernet	攻撃者	★★ サービス ★★★ 生命・財産	通常使用 I/F
			マルウェア感染	ホームゲートウェイのマルウェア感染 （外部インターネット経由の攻撃）	Ethernet	攻撃者	★★ サービス ★★★ 生命・財産	通常使用 I/F
			サービス不能	DDoS（DoS）攻撃	Ethernet	攻撃者	★★ サービス ★★★ 生命・財産	通常使用 I/F
			情報の暴露	接続されたストレージデバイスによる情報の暴露	上記以外の有線通信	ユーザ （意図的）	★★ 情報 ★★★ 情報	通常使用 I/F
			マルウェア感染	接続されたストレージデバイスによるマルウェア感染	上記以外の有線通信	ユーザ （意図的）	★★ 本来機能 ★★★ 本来機能	通常使用 I/F

					上記以外の有線通信	ユーザ（意図的）	★★ サービス ★★★ 生命・財産	通常使用 I/F
			マルウェア感染	LAN 内接続機器からのマルウェア感染	Ethernet Wi-Fi 上記以外の無線通信	攻撃者	★★ 本来機能・情報 ★★★ 本来機能・情報	通常使用 I/F
					Ethernet Wi-Fi 上記以外の無線通信	攻撃者	★★ サービス ★★★ 生命・財産	通常使用 I/F
			踏み台	BOT 化等、攻撃の踏み台として悪用される	Ethernet	攻撃者	★★ IoT 機能 ★★★ IoT 機能	通常使用 I/F
	EP⑥	【一次資産/二次資産】 通信経路上のデータ	情報の暴露	中間者攻撃によるインターネット経路上の情報窃取	Ethernet	攻撃者	★★ 情報	通常使用 I/F

ホームゲートウェイとインターネット間の通信経路							★★★ 情報	
スマートホームサービス対応機器群	EP⑦	【一次資産】 ・ハードウェア、ソフトウェア（機能それ自体） ・制御信号 ・センシングデータ ・個人情報（利用者の氏名、住所、電話番号等） 【二次資産】 ・認証情報 ・暗号鍵	不正アクセス	機器に対する不正アクセス（既知の脆弱性を突いた攻撃）	Ethernet Wi-Fi 上記以外の有線通信/無線通信	攻撃者	★★ IoT 機能	通常使用 I/F
							★★★ IoT 機能	
					Ethernet Wi-Fi 上記以外の有線通信/無線通信	攻撃者	★★ サービス	通常使用 I/F
							★★★ 生命・財産	
			情報の暴露	機器内のデータ、設定値の情報窃取（アクセス制御、認証不備）	Ethernet Wi-Fi 上記以外の有線通信/無線通信	攻撃者	★★ 情報	通常使用 I/F
							★★★ 情報	

			データ改ざん	機器内のデータ、設定値の改ざん	Ethernet Wi-Fi 上記以外の有線通信/無線通信	攻撃者	★★ 本来機能	通常使用 I/F
							★★★ 本来機能	
					Ethernet Wi-Fi 上記以外の有線通信/無線通信	攻撃者	★★ サービス	通常使用 I/F
							★★★ 生命・財産	
			なりすまし	通信においてホームゲートウェイになりすまし、改ざんメッセージによる攻撃が行われる	Ethernet Wi-Fi 上記以外の有線通信/無線通信	攻撃者	★★ サービス	通常使用 I/F
							★★★ 生命・財産	
			情報の暴露	接続されたストレージデバイスによる情報の暴露 （USB インターフェース等の対応機器）	上記以外の有線通信	ユーザ （意図的）	★★ 情報	通常使用 I/F
							★★★ 情報	

			マルウェア感染	接続されたストレージデバイスによるマルウェア感染（USB インターフェース等の対応機器）	上記以外の有線通信	ユーザ（意図的）	★★ 本来機能・情報 ★★★ 本来機能・情報	通常使用 I/F
					上記以外の有線通信	ユーザ（意図的）	★★ サービス ★★★ 生命・財産	通常使用 I/F
			踏み台	BOT 化等、攻撃の踏み台として悪用される	Ethernet Wi-Fi 上記以外の有線通信/無線通信	攻撃者	★★ その他 ★★★ その他	通常使用 I/F
スマートホームサービス対応機器群とホームゲートウェイ間の通信経路	EP⑧	【一次資産/二次資産】 通信経路上のデータ ・制御信号、センシングデータ ・個人情報（対象機器の実装機能に依存する）	なりすまし	中間者攻撃による機器の制御信号のなりすまし	Wi-Fi 上記以外の無線通信	攻撃者	★★ 本来機能 ★★★ 本来機能	通常使用 I/F
					Wi-Fi	攻撃者	★★ サービス	通常使用 I/F

		・認証情報			上記以外の無線通信		★★★ 生命・財産	
			情報の暴露	中間者攻撃によるインターネット経路上の情報窃取	Wi-Fi 上記以外の無線通信	攻撃者	★★ 情報 ★★★ 情報	通常使用 I/F
スマートフォンアプリ	EP⑨	【一次資産】 ・ソフトウェア（機能それ自体） ・制御信号 ・スマーフォン内の個人情報や機微情報 【二次資産】 ・認証情報	情報の暴露	スマートフォンアプリの脆弱性によるデバイス内データの情報の暴露	Wi-Fi LTE/LTE-Advanced	ユーザ （意図的）	★★ 情報 ★★★ 情報	通常使用 I/F
			情報の暴露	スマートフォンアプリの不正ログインによる情報の暴露	Wi-Fi LTE/LTE-Advanced	攻撃者	★★ 本来機能 ★★★ 本来機能	通常使用 I/F
			なりすまし	スマートフォンアプリの不正ログインによる機器の不正操作（なりすまし）	Wi-Fi LTE/LTE-Advanced	攻撃者	★★ 本来機能 ★★★ 本来機能	通常使用 I/F
スマートフォンとホームゲートウェイ間の通信経路	EP⑩	【一次資産/二次資産】 通信経路上のデータ	なりすまし	中間者攻撃による機器の制御信号のなりすまし	Wi-Fi	攻撃者	★★ 本来機能 ★★★	通常使用 I/F

							本来機能	
			情報の暴露	中間者攻撃によるインターネット経路上の情報窃取	Wi-Fi	攻撃者	★★ 情報	通常使用 I/F
							★★★ 情報	

3.5　リスク値の計算

想定される脅威とそのリスク特性を分析後、それらのリスク値を計算する。リスク値の計算方法は、CVSS、The OWASP Risk Rating Methodology、ETSI TS102 165-1 など様々な方法が提案されている[15]。それらによって計算されたリスク値は、同じ脅威に対しても計算方法によって値が異なり、同じ方法で求めたリスク値の比較だけが意味をなす。そのため、スマートホーム向け製品・サービスのリスク値の計算方法を定義したら、その手法を使用し続ける必要がある。

また、スマートホーム向け製品・サービスのリスク値の計算では、その利用用途、特に生命・財産への影響の有無を考慮すべきである。

3.5.1 CVSS v3 によるリスク値の計算と課題

スマートホーム向け製品・サービスのリスク分析・評価は、これまでに実施されたことがなく、既存の分析手法が存在しない。本ガイドラインの作成にあたり、リスク分析・評価手法の調査・検討を行い、まず情報セキュリティの脆弱性評価で標準的に利用される CVSS v3[16][17]によるリスク値の計算を試行した。

セキュリティ対策を行う前の脅威のリスク値は、CVSS 基本値を用いるものとする。以下に、★★サービス、★★★サービスで想定される脅威に対して、CVSS v3 によるリスク値を示す。

表 3-12 CVSSv3 によるサービスのリスク値（★★、★★★共通）※抜粋

脅威事例				基本値												
エントリーポイント	EP番号	脅威分類	脅威事例	攻撃元区分	攻撃条件の複雑さ	攻撃に必要な特権レベル	利用者の関与	影響の想定範囲（スコープ）	機密性への影響	完全性への影響	可用性への影響	生命・財産への影響	情報の重要度	リスク値	リスク値ランク
スマートホームサービス情報基盤	EP①	不正アクセス	サービス情報基盤に対する不正アクセス（既知の脆弱性を利用）	ネットワーク	高	不要	不要	変更なし	高	高	高	なし	なし	8.1	重要
		情報の暴露	サービス情報基盤内のデータに対する情報窃取（アクセス制御、認証不備）	ネットワーク	低	低	不要	変更なし	高	なし	なし	なし	なし	6.5	警告
		データ改ざん	サービス情報基盤のデータ、設定値の改ざん	ネットワーク	高	不要	不要	変更なし	高	高	高	なし	なし	8.1	重要
		マルウェア感染	サービス情報基盤のマルウェア感染（外部インターネット経由の攻撃）	ネットワーク	高	不要	不要	変更なし	高	高	高	なし	なし	8.1	重要
		サービス不能	DDoS（DoS）攻撃	ネットワーク	低	不要	不要	変更なし	なし	なし	高	なし	なし	7.5	重要
		情報の暴露	持ち込まれたストレージデバイスによる情報漏洩	物理	低	低	要	変更なし	高	なし	なし	なし	なし	4.1	警告
		マルウェア感染	持ち込まれたストレージデバイスによるマルウェア感染	物理	低	低	要	変更なし	高	高	高	なし	なし	6.4	警告
		情報の暴露	アップデート用のソフトウェアの情報窃取	ネットワーク	高	不要	不要	変更なし	高	高	高	なし	なし	8.1	重要
		データ改ざん	アップデート用のソフトウェアの改ざん	ネットワーク	高	不要	不要	変更なし	高	高	高	なし	なし	8.1	重要
スマートホームサービス情報基盤情報基盤とインターネット間の通信経路	EP②	情報の暴露	中間者攻撃によるインターネット経路上の情報窃取	隣接	高	低	不要	変更なし	高	なし	なし	なし	なし	4.8	警告

この計算結果を踏まえ、スマートホーム分野において CVSS v3 を適用した場合の課題を示す。

表 3-13 CVSSv3 によるリスク値計算の課題

課題	内容
①保護すべき資産の重要度をリスク計算結果に反映できない	CVSS は保護すべき資産の重要性をリスクファクターとして含んでいないため、個人情報の漏洩など、★★サービスにおいて影響が大きい資産が含まれる場合の脅威であってもリスク計算結果に反映されない。
②生命・財産への影響をリスク計算結果に反映できない	CVSS はインシデントが機密性、完全性、可用性に対して与える影響度を重要なリスクファクターとして計算するため★★★サービスで懸念されるような生命・財産に対する影響をリスク計算結果に反映できない。

CVSS の設計上、スマートホーム分野に適用した場合、上記①、②の課題があり、実際の計算結果でも★★サービス、★★★サービスにおいて、リスク値に差異は生じていない。

そのため本書では CVSS v3 を土台に、スマートホーム向け製品・サービスのセキュリティ特性を考慮した独自のリスク値の計算方法（以下、スマートホーム独自方式）を新たに定義する。

3.5.2 スマートホーム独自方式のリスク値計算の定義

CVSS v3 を踏まえて、スマートホーム向けの製品・サービスのリスク値の計算方法（スマートホーム独自方式）を定義する。スマートホーム独自方式では、以下の 2 つの値を用いてサービスの脆弱性を評価する。

表 3-14 スマートホーム独自方式の脆弱性評価基準

No.	項目	内容
1	基本値	脆弱性そのものの深刻度を表す値で、セキュリティ対策を実施する前の評価に用いる。 • 攻撃の難易度と、システムのセキュリティ特性である機密性・完全性・可用性に対する影響、およびスマートホーム向け製品・サービスのセキュリティ特性である生命・財産への影響の有無、個人情報などの情報の重要度を評価して計算する。 • 基本値は、脆弱性固有の深刻度を表していて、脆弱性を取り巻く時間的変化や利用環境での対策状況に拠らない。
2	環境値	実際のサービスの提供システムにおける脆弱性の深刻度を表す値で、セキュリティ対策を実施した後の評価に用いる。 • サービスの提供環境における攻撃の難易度、攻撃による影響度を、セキュリティ対策の状況などを踏まえて再評価して、環境値を計算する。

これらの基本値、環境値は、以下に示す計算式で求められ、0.0（深刻度が最低）から 10.0（深刻度が最高）までの数値（0.1 刻み）で表される。

これらの基本値・環境値の計算式において、スマートホーム向け製品・サービスに特有のセキュリティ特性（生命・財産への影響、扱う情報の重要度）を評価するパラメータを CVSS v3 に追加して、CVSS v3 のリスク値を計算する影響度にかかる係数（図 3-2、図 3-3）として用いる。具体的には、製品・サービスに脅威が及ぼされたとき生命・財産への影響があれば影響度が 1.5 倍に、また製品・サービスが個人情報保護法に定義された個人情報を扱う場合は影響度が 1.2 倍に算出される（表 3-16、表 3-17、表 3-25、表 3-26）。詳細は、後述の基本値および環境値の計算式を参照のこと。

(1) 基本値の計算式

基本値の計算式を以下に示す。

(1)影響度
調整前影響度 = 1 - (1-C)×(1-I)×(1-A)
影響度(スコープ変更なし)= 6.42×調整前影響度×LP×II
影響度(スコープ変更あり)= (7.52×(調整前影響度-0.029) - 3.25×(調整前影響度-0.02)^{15}) ×LP×II

(2)攻撃容易性
攻撃容易性 = 8.22×AV×AC×PR×UI

(3)基本値
影響度がゼロ以下の場合　基本値 = 0
影響度がゼロよりも大きい場合
・スコープ変更なし
基本値 = 影響度＋攻撃容易性（※）
・スコープ変更あり
基本値 = 1.08×(影響度＋攻撃容易性)（※）
（※）小数点第二位を切り上げ。10.0 を超える場合は 10.0 とする。

図 3-2 基本値（スマートホーム独自方式）の計算式

計算式に登場する LP/II、C/I/A および AV/AC/PR/UI は表 3-15 で定義される。LP と II はスマートホーム向け製品・サービスに特有のパラメータで、それぞれ生命・財産への影響と、個人情報などの情報の重要度を表す。他のパラメータは CVSS v3 で定義されるパラメータと同一である。

表 3-15 基本値を計算するパラメータ

No.	項目	内容
1	生命・財産への影響（LP）	脆弱性への攻撃が生命・財産に影響を及ぼす可能性を評価する。
2	情報の重要度（II）	脆弱性への攻撃が情報に影響を及ぼす場合に、その情報の重要度（個人情報等）を評価する。
3	機密性への影響（C）	脆弱性を攻撃された際に、対象とする影響想定範囲の情報が漏洩する可能性を評価する。
4	完全性への影響（I）	脆弱性を攻撃された際に、対象とする影響想定範囲の情報が改ざんされる可能性を評価する。
5	可用性への影響（A）	脆弱性を攻撃された際に、対象とする影響想定範囲の業務が遅延・停止する可能性を評価する。
6	攻撃元区分（AV）	脆弱性のあるコンポーネントをどこから攻撃可能であるかを評価する。
7	攻撃条件の複雑さ（AC）	脆弱性のあるコンポーネントを攻撃する際に必要な条件の複雑さを評価する。
8	攻撃に必要な特権レベル（PR）	脆弱性のあるコンポーネントを攻撃する際に必要な特権のレベルを評価する。
9	ユーザ関与レベル（UI）	脆弱性のあるコンポーネントを攻撃する際に必要なユーザ関与レベルを評価する。
10	スコープ（S）	脆弱性のあるコンポーネントへの攻撃による影響範囲を評価する。

それぞれの項目が取り得る値を、以下に示す。

表 3-16 生命・財産への影響（LP）

項目	内容	値
あり（Y）	脅威が発生した場合、生命・財産への影響がある。	1.5
なし（N）	脅威が発生しても、生命・財産への影響がない。	1.0

表 3-17 情報の重要度（II）

項目	内容	値
高（H）	以下に示した重要な情報が含まれる。 個人情報保護法（第二条）に定められた個人情報とは、生存する個人に関する情報で、次のいずれかに該当するもの。 ・ 当該情報に含まれる氏名、生年月日その他の記述等により特定の個人を識別することができるもの。他の情報と容易に照合することができ、それにより特定の個人を識別することができることとなるものを含む。 ・ 個人識別符号（その情報単体でも特定の個人を識別できるもの）が含まれるもの。 ➢ 身体の一部の特徴を電子計算機のために変換した符号 ➢ サービス利用や書類において対象者ごとに割り振られる符号	1.2
なし（N）	重要な情報は含まれない。	1.0

表 3-18 機密性（C）・完全性（I）・可用性（A）への影響

項目	高（H）	低（L）	なし（N）
機密性（C）	脅威が発生した場合に、利用者の情報、システムの重要な情報がすべて参照可能であり、影響が全体におよぶ。	脅威が発生した場合に、利用者の情報、システムの重要な情報が部分的に参照可能であり、影響が限定的である。	脅威が発生しても、利用者やシステムの情報が参照されることがなく、影響が発生しない。
	値： 0.56	値： 0.22	値： 0.0
完全性（I）	脅威が発生した場合、利用者の情報、システムの重要な情報が改ざん可能であり、影響が全体におよぶ。	脅威が発生した場合、利用者やシステムの情報が改ざん可能であるが、重要な情報は改ざんできなく、影響が限定的である。	脅威が発生しても、利用者やシステムの情報が改ざんされることがなく、影響が発生しない。
	値： 0.56	値： 0.22	値： 0.0
可用性（A）	脅威が発生した場合に、サービスの提供を完全に停止させることが可能である。	脅威が発生した場合に、サービスの提供を一時的に停止させたり、遅延させたりすることが可能である。	脅威が発生しても、サービスの提供が停止・遅延することがなく、影響が発生しない。
	値： 0.56	値： 0.22	値： 0.0

表 3-19 攻撃元区分（AV）

項目	内容	値
ネットワーク（N）	攻撃対象をネットワーク経由でリモートから攻撃可能である。 ・インターネットからスマートホームサービス情報基盤を攻撃 ・インターネットから GW を攻撃	0.85
隣接（A）	攻撃対象を隣接ネットワークから攻撃する必要がある。 ・スマートホームサービス情報基盤のネットワークに接続して攻撃 ・GW が接続された無線ルータの無線 LAN に接続して攻撃 ・GW の LAN 端子・無線 LAN に接続して攻撃	0.62
ローカル（L）	攻撃対象をローカル環境から攻撃する必要がある。 ・スマートホームサービス情報基盤のサーバにログインして攻撃 ・GW のシリアルコンソールに接続して攻撃	0.55
物理（P）	攻撃対象を物理アクセス環境から攻撃する必要がある。 ・GW に設けられた JEM-A 端子（HA 端子）、USB 端子などの物理端子に接続して攻撃	0.20

表 3-20 攻撃条件の複雑さ（AC）

項目	内容	値
低（L）	特別な攻撃条件を必要とせず、攻撃対象を常に攻撃可能である。	0.77
高（H）	攻撃者以外に依存する攻撃条件が存在する。 例えば、次のいずれかの条件に合致する場合などが該当する。 ・攻撃者は、設定情報、シーケンス番号、共有鍵など、攻撃対象の情報収集が事前に必要となる。 ・攻撃者は、競合が発生する条件、ヒープスプレイを成功させるための条件など、攻撃を成功させるための環境条件を明らかにする必要がある。 ・攻撃者は、中間者攻撃のため環境が必要となる。	0.44

表 3-21 攻撃に必要な特権レベル（PR）

項目	内容	値	
		スコープ変更なし	スコープ変更あり
不要（N）	特別な権限を有する必要はない。	0.85	
低（L）	コンポーネントに対する基本的な権限を有していれば良い。	0.62	0.68
高（H）	コンポーネントに対する管理者権限相当を有する必要がある。	0.27	0.50

表 3-22 ユーザ関与レベル（UI）

項目	内容	値
不要（N）	ユーザが何もしなくても脆弱性が攻撃される可能性がある。	0.85
要（R）	リンクのクリック、ファイル閲覧、設定の変更など、ユーザ動作が必要である。	0.62

また、スコープ変更あり／スコープ変更なしは、表 3-23 で定義される。

表 3-23 スコープ（S）

項目	内容
変更なし（U）	影響範囲が攻撃対象と同じ認証の範囲に属するシステムである。 例えば、アクセストークンを共有するシステムへの不正アクセスは、変更なしのスコープである。
変更あり（C）	影響範囲が攻撃対象と認証が異なるシステムへと、範囲を越えた攻撃が可能である。

(2) 環境値の計算式

環境値の計算式を以下に示す。

(1)緩和策後影響度

緩和策後調整前影響度 = min [(1 -(1 - MC×CR)×(1 - MI×IR)×(1 - MA×AR)), 0.915]

◎スコープ変更なし

緩和策後影響度= 6.42×緩和策後調整前影響度×MLP×MII

◎スコープ変更あり

緩和策後影響度= (7.52×(緩和策後調整前影響度-0.029)

- 3.25×(緩和策後調整前影響度-0.02)^{15}) ×MLP×MII

(2)緩和策後攻撃容易性

緩和策後攻撃容易性 = 8.22×MAV×MAC×MPR×MUI

(3)環境値

緩和策後影響度がゼロ以下の場合　環境値 = 0

緩和策後影響度がゼロよりも大きい場合

◎スコープ変更なし

緩和策後基本値 = 緩和策後影響度＋緩和策後攻撃容易性（※1）

環境値 = 緩和策後基本値×E×RL×RC（※2）

◎スコープ変更あり

緩和策後基本値 = 1.08×(緩和策後影響度＋緩和策後攻撃容易性)（※1）

環境値 = 緩和策後基本値×E×RL×RC（※2）

（※1）小数点第二位を切り上げ。10.0 を超える場合は 10.0 とする。

（※2）小数点第二位を切り上げ。

E：攻撃される可能性、RL：利用可能な対策のレベル、RC：脆弱性情報の信頼性の値は、通常の現状評価値の計算方法から変更がないため、CVSSv3[16][17]を参照。

図 3-3 環境値（スマートホーム独自方式）の計算式

計算式に登場する MLP/MI、CR/IR/AR、MC/MI/MA および MAV/MAC/MPR/MUI は表 3-24 で定義される。ここで、MLP/MII はそれぞれ生命・財産への影響と、個人情報などの情報の重要度を表し、基本値における LP と II に対応する。他のパラメータは CVSS v3 で定義されるパラメータと同一である。

表 3-24 環境値を計算するパラメータ

No.	項目	内容
生命・財産の影響、情報の重要度		
1	緩和策後の生命・財産への影響（MLP）	脆弱性への攻撃が生命・財産に影響を及ぼす可能性を再評価する。
2	緩和策後の情報の重要度（MII）	脆弱性への攻撃が情報に影響を及ぼす場合に、その情報の重要度（個人情報等）を再評価する。
対象システムのセキュリティ要求度		
3	機密性（CR）	対象システムにおける、機密性の重要度を評価する。
4	完全性（IR）	対象システムにおける、完全性の重要度を評価する。
5	可用性（AR）	対象システムにおける、可用性の重要度を評価する。
環境条件を加味した基本評価の再評価		
6	緩和策後の機密性への影響（MC）	脆弱性を攻撃された際に、対象とする影響想定範囲の情報が漏えいする可能性を再評する。
7	緩和策後の完全性への影響（MI）	脆弱性を攻撃された際に、対象とする影響想定範囲の情報が改ざんされる可能性を再評価する。
8	緩和策後の可用性への影響（MA）	脆弱性を攻撃された際に、対象とする影響想定範囲の業務が遅延・停止する可能性を再評価する。
9	緩和策後の攻撃元区分（MAV）	脆弱性のあるコンポーネントをどこから攻撃可能であるかを再評価する。
10	緩和策後の攻撃条件の複雑さ（MAC）	脆弱性のあるコンポーネントを攻撃する際に必要な条件の複雑さを再評価する。
11	緩和策後の攻撃に必要な特権レベル（MPR）	脆弱性のあるコンポーネントを攻撃する際に必要な特権のレベルを再評価する。
12	緩和策後のユーザ関与レベル（MUI）	脆弱性のあるコンポーネントを攻撃する際に必要なユーザ関与レベルを再評価する。
13	緩和策後のスコープ（MS）	脆弱性のあるコンポーネントへの攻撃による影響範囲を再評価する。

それぞれの項目が取り得る値を、以下に示す。

表 3-25 緩和策後の生命・財産への影響（MLP）

項目	内容	値
未評価（X）	評価しない（基本値の計算と同じ項目を用いる）	
あり（Y）	基本値の計算に用いる定義と同じ（表 3-16 を参照）	1.5
なし（N）		1.0

表 3-26 緩和策後の情報の重要度（MII）

項目	内容	値
未評価（X）	評価しない（基本値の計算と同じ項目を用いる）	
高（H）	基本値の計算に用いる定義と同じ（表 3-17 を参照）	1.2
なし（N）		1.0

表 3-27 対象システムのセキュリティ要求度（CR/IR/AR）

項目	未評価（X）	高（H）	中（M）	低（L）
機密性（CR）	この項目を評価しない。	機密性が失われると、壊滅的な影響がある。	機密性が失われると、深刻な影響がある。	機密性が失われても、一部の影響に留まる。
	値： 1.0	値： 1.5	値： 1.0	値： 0.5
完全性（IR）	この項目を評価しない。	完全性が失われると、壊滅的な影響がある。	完全性が失われると、深刻な影響がある。	完全性が失われても、一部の影響に留まる。
	値： 1.0	値： 1.5	値： 1.0	値： 0.5
可用性（AR）	この項目を評価しない。	可用性が失われると、壊滅的な影響がある。	可用性が失われると、深刻な影響がある。	可用性が失われても、一部の影響に留まる。
	値： 1.0	値： 1.5	値： 1.0	値： 0.5

表 3-28 緩和策後の機密性への影響（MC）

項目	内容	値
未評価（X）	評価しない（基本値の計算と同じ項目を用いる）	
高（H）	基本値の計算に用いる定義と同じ（表 3-18 の「機密性」を参照）	0.56
低（L）		0.22
なし（N）		0.0

表 3-29 緩和策後の完全性への影響（MI）

項目	内容	値
未評価（X）	評価しない（基本値の計算と同じ項目を用いる）	
高（H）	基本値の計算に用いる定義と同じ（表 3-18 の「完全性」を参照）	0.56
低（L）		0.22
なし（N）		0.0

表 3-30 緩和策後の可用性への影響（MA）

項目	内容	値
未評価（X）	評価しない（基本値の計算と同じ項目を用いる）	
高（H）	基本値の計算に用いる定義と同じ（表 3-18 の「可用性」を参照）	0.56
低（L）		0.22
なし（N）		0.0

表 3-31 緩和策後の攻撃元区分（MAV）

項目	内容	値
未評価（X）	評価しない（基本値の計算と同じ項目を用いる）	
ネットワーク（N）	基本値の計算に用いる定義と同じ（表 3-19 を参照）	0.85
隣接（A）		0.62
ローカル（L）		0.55
物理（P）		0.20

表 3-32 緩和策後の攻撃条件の複雑さ（MAC）

項目	内容	値
未評価（X）	評価しない（基本値の計算と同じ項目を用いる）	
低（L）	基本値の計算に用いる定義と同じ（表 3-20 を参照）	0.77

高（H）		0.44

表 3-33 緩和策後の攻撃に必要な特権レベル（MPR）

項目	内容	値	
		スコープ変更なし	スコープ変更あり
未評価（X）	評価しない（基本値の計算と同じ項目を用いる）		
不要（N）	基本値の計算に用いる定義と同じ（表 3-21 を参照）	0.85	
低（L）		0.62	0.68
高（H）		0.27	0.50

表 3-34 緩和策後のユーザ関与レベル（MUI）

項目	内容	値
未評価（X）	評価しない（基本値の計算と同じ項目を用いる）	
不要（N）	基本値の計算に用いる定義と同じ（表 3-22 を参照）	0.85
要（R）		0.62

表 3-35 緩和策後のスコープ（MS）

項目	内容
未評価（X）	評価しない（基本値の計算と同じ項目を用いる）
変更なし（U）	基本値の計算に用いる定義と同じ（表 3-23 を参照）
変更あり（C）	

(3) 深刻度レベル分け

スマートホーム独自方式では、CVSS v3 と同じく、深刻度のレベル分けを以下の通りに設定している。

表 3-36 深刻度レベル分け

深刻度	緊急	重要	警告	注意	なし
スコア	9.0～10.0	7.0～8.9	4.0～6.9	0.1～3.9	0

(4) スマートホーム独自方式によるリスク値の計算

表 3-37 に本方式によるリスク値の計算結果を示す。

表 3-37 スマートホーム独自方式によるサービスのリスク値

①CVSSv3 算定例：スマートホーム独自方式未適用

脅威事例				基本値									
エントリーポイント	EP番号	脅威分類	脅威事例	攻撃元区分	攻撃条件の複雑さ	攻撃に必要な特権レベル	利用者の関与	影響の想定範囲（スコープ）	機密性への影響	完全性への影響	可用性への影響	リスク値	リスク値ランク
スマートホームサービス情報基盤	EP①	不正アクセス	サービス情報基盤に対する不正アクセス（既知の脆弱性を利用）	ネットワーク	高	不要	不要	変更なし	高	高	高	8.1	重要

②CVSSv3 算定例：スマートホーム独自方式適用（情報の重要度に影響あり）

脅威事例				基本値											
エントリーポイント	EP番号	脅威分類	脅威事例	攻撃元区分	攻撃条件の複雑さ	攻撃に必要な特権レベル	利用者の関与	影響の想定範囲（スコープ）	機密性への影響	完全性への影響	可用性への影響	生命・財産への影響	情報の重要度	リスク値	リスク値ランク
スマートホームサービス情報基盤	EP①	不正アクセス	サービス情報基盤に対する不正アクセス（既知の脆弱性を利用）	ネットワーク	高	不要	不要	変更なし	高	高	高	なし	高	9.3	緊急

③CVSSv3 算定例：スマートホーム独自方式適用（情報の重要度、生命・財産に影響）

脅威事例				基本値											
エントリーポイント	EP番号	脅威分類	脅威事例	攻撃元区分	攻撃条件の複雑さ	攻撃に必要な特権レベル	利用者の関与	影響の想定範囲（スコープ）	機密性への影響	完全性への影響	可用性への影響	生命・財産への影響	情報の重要度	リスク値	リスク値ランク
スマートホームサービス対応機器群	EP②	不正アクセス	機器に対する不正アクセス（既知の脆弱性を利用）	ネットワーク	高	不要	不要	変更なし	高	高	高	あり	高	10	緊急

まず上記①はスマートホーム独自方式を適用しない既存の CVSSv3 によるリスク評価例であり、リスク値は 8.1（重要）と判定されている。次に上記②では、同じ想定脅威に対して、★★サービスとして個人情報が取り扱われるユースケースを想定すると、リスク値は 9.3（緊急）と判定されている。更に上記③では、同じ想定脅威に対して、★★★サービスとして個人情報や生命・財産に影響が想定されるユースケースを想定した場合には、リスク値が 10（緊急）と判定された。

以上のように既存の CVSSv3 と比較し、保護すべき資産に個人情報が加わった場合や、生命・財産に影響が生じる場合の脅威事例についても、評価結果として差異を表現することが可能となった。

3.5.3 スマートホーム独自方式でのリスク値計算の結果

前節で定義したスマートホーム独自方式を用いて、インシデントのそれぞれのリスク値を計算する。シャッター自動開閉サービス（★★）と防犯駆けつけサービス（★★★）の計算結果を、それぞれ表 3-38 と表 3-39 に示す。

表 3-38 シャッター自動開閉サービス（★★）のリスク値（セキュリティ対策前）

脅威事例				基本値											
エントリーポイント	EP番号	脅威分類	脅威事例	攻撃元区分	攻撃条件の複雑さ	攻撃に必要な特権レベル	利用者の関与	影響の想定範囲（スコープ）	機密性への影響	完全性への影響	可用性への影響	生命・財産への影響	情報の重要度	リスク値	リスク値ランク
スマートホームサービス情報基盤	EP①	不正アクセス	サービス情報基盤に対する不正アクセス（既知の脆弱性を利用）	ネットワーク	高	不要	不要	変更なし	高	高	高	なし	高	9.3	緊急
		情報の暴露	サービス情報基盤内のデータに対する情報窃取（アクセス制御、認証不備）	ネットワーク	低	低	不要	変更なし	高	なし	なし	なし	高	7.2	重要
		データ改ざん	サービス情報基盤のデータ、設定値の改ざん	ネットワーク	高	不要	不要	変更なし	高	高	高	なし	高	9.3	緊急
		なりすまし	API経由の通信において第三者サービス情報基盤、ホームゲートウェイになりすまし、改ざんメッセージによる攻撃が行われる	ネットワーク	高	不要	不要	変更なし	低	高	高	なし	高	8.8	重要
		マルウェア感染	サービス情報基盤のマルウェア感染（外部インターネット経由の攻撃）	ネットワーク	高	不要	不要	変更なし	高	高	高	なし	高	9.3	緊急
		サービス不能	DDoS（DoS）攻撃	ネットワーク	低	不要	不要	変更なし	なし	なし	高	なし	なし	7.5	重要
		情報の暴露	持ち込まれたストレージデバイスによる情報漏洩	物理	低	低	要	変更なし	高	なし	なし	なし	高	4.9	警告
		マルウェア感染	持ち込まれたストレージデバイスによるマルウェア感染	物理	低	低	要	変更なし	高	高	高	なし	高	7.6	重要
		情報の暴露	アップデート用のソフトウェアの情報窃取	ネットワーク	高	不要	不要	変更なし	高	高	高	なし	高	9.3	緊急
		データ改ざん	アップデート用のソフトウェアの改ざん	ネットワーク	高	不要	不要	変更なし	高	高	高	なし	高	9.3	緊急
スマートホームサービス情報基盤情報基盤とインターネット間の通信経路	EP②	情報の暴露	中間者攻撃によるインターネット経路上の情報窃取	隣接	高	低	不要	変更なし	高	なし	なし	なし	高	5.5	警告

脅威事例				基本値											
エントリーポイント	EP番号	脅威分類	脅威事例	攻撃元区分	攻撃条件の複雑さ	攻撃に必要な特権レベル	利用者の関与	影響の想定範囲（スコープ）	機密性への影響	完全性への影響	可用性への影響	生命・財産への影響	情報の重要度	リスク値	リスク値ランク
第三者サービス情報基盤	EP③	不正アクセス	サービス情報基盤に対する不正アクセス （既知の脆弱性を利用）	ネットワーク	高	不要	不要	変更なし	高	高	高	なし	なし	8.1	重要
		情報の暴露	サービス情報基盤内のデータに対する情報窃取（アクセス制御、認証不備）	ネットワーク	低	低	不要	変更なし	高	なし	なし	なし	なし	6.5	警告
		データ改ざん	サービス情報基盤のデータ、設定値の改ざん	ネットワーク	高	不要	不要	変更なし	高	高	高	なし	なし	8.1	重要
		なりすまし	API経由の通信においてスマートホームサービス情報基盤になりすまし、改ざんメッセージによる攻撃が行われる	ネットワーク	高	不要	不要	変更なし	低	高	高	なし	なし	7.7	重要
		マルウェア感染	サービス情報基盤のマルウェア感染（外部インターネット経由の攻撃）	ネットワーク	高	不要	不要	変更なし	高	高	高	なし	なし	8.1	重要
		サービス不能	DDoS（DoS）攻撃	ネットワーク	低	不要	不要	変更なし	なし	なし	高	なし	なし	7.5	重要
		情報の暴露	持ち込まれたストレージデバイスによる情報漏洩	物理	低	低	要	変更なし	高	なし	なし	なし	なし	4.1	警告
		マルウェア感染	持ち込まれたストレージデバイスによるマルウェア感染	物理	低	低	要	変更なし	高	高	高	なし	なし	6.4	警告
		情報の暴露	アップデート用のソフトウェアの情報窃取	ネットワーク	高	不要	不要	変更なし	高	高	高	なし	なし	8.1	重要
		データ改ざん	アップデート用のソフトウェアの改ざん	ネットワーク	高	不要	不要	変更なし	高	高	高	なし	なし	8.1	重要
第三者サービス情報基盤とインターネット間の通信経路	EP④	情報の暴露	中間者攻撃によるインターネット経路上の情報窃取	隣接	高	低	不要	変更なし	高	なし	なし	なし	なし	4.8	警告

脅威事例				基本値											
エントリーポイント	EP番号	脅威分類	脅威事例	攻撃元区分	攻撃条件の複雑さ	攻撃に必要な特権レベル	利用者の関与	影響の想定範囲（スコープ）	機密性への影響	完全性への影響	可用性への影響	生命・財産への影響	情報の重要度	リスク値	リスク値ランク
ホームゲートウェイ	EP⑤	不正アクセス	ホームゲートウェイに対する不正アクセス （既知の脆弱性を利用）	ネットワーク	高	不要	不要	変更なし	高	高	高	なし	なし	8.1	重要
		情報の暴露	ホームゲートウェイ内のデータ、設定値の情報窃取（アクセス制御、認証不備）	ネットワーク	低	低	不要	変更なし	高	なし	なし	なし	なし	6.5	警告
		データ改ざん	ホームゲートウェイ内のデータ、設定値の改ざん	ネットワーク	高	不要	不要	変更なし	高	高	高	なし	なし	8.1	重要
		なりすまし	API経由の通信においてサービス情報基盤になりすまし、改ざんメッセージによる攻撃が行われる	ネットワーク	高	不要	不要	変更なし	低	高	高	なし	なし	7.7	重要
		マルウェア感染	ホームゲートウェイのマルウェア感染（外部インターネット経由の攻撃）	ネットワーク	高	不要	不要	変更なし	高	高	高	なし	なし	8.1	重要
		サービス不能	DDoS（DoS）攻撃	ネットワーク	低	不要	不要	変更なし	なし	なし	高	なし	なし	7.5	重要
		情報の暴露	接続されたストレージデバイスによる情報漏洩	物理	低	低	要	変更なし	高	なし	なし	なし	なし	4.1	警告
		マルウェア感染	接続されたストレージデバイスによるマルウェア感染	物理	低	低	要	変更なし	高	高	高	なし	なし	6.4	警告
		マルウェア感染	LAN内接続機器からのマルウェア感染	隣接	低	不要	不要	変更なし	高	高	高	なし	なし	8.8	重要
		踏み台	BOT化等、攻撃の踏み台として悪用される	ネットワーク	低	低	不要	変更あり	なし	なし	なし	なし	なし	3.2	注意
ホームゲートウェイとインターネット間の通信経路	EP⑥	情報の暴露	中間者攻撃によるインターネット経路上の情報窃取	隣接	高	低	不要	変更なし	高	なし	なし	なし	なし	4.8	警告

脅威事例				基本値											
エントリーポイント	EP番号	脅威分類	脅威事例	攻撃元区分	攻撃条件の複雑さ	攻撃に必要な特権レベル	利用者の関与	影響の想定範囲（スコープ）	機密性への影響	完全性への影響	可用性への影響	生命・財産への影響	情報の重要度	リスク値	リスク値ランク
スマートホームサービス対応機器群	EP⑦	不正アクセス	機器に対する不正アクセス（既知の脆弱性を利用）	ネットワーク	高	不要	不要	変更なし	高	高	高	なし	なし	8.1	重要
		情報の暴露	機器内のデータ、設定値の情報窃取（アクセス制御、認証不備）	ネットワーク	低	低	不要	変更なし	高	なし	なし	なし	なし	6.5	警告
		データ改ざん	機器内のデータ、設定値の改ざん	ネットワーク	高	不要	不要	変更なし	高	高	高	なし	なし	8.1	重要
		なりすまし	通信においてホームゲートウェイになりすまし、改ざんメッセージによる攻撃が行われる	ネットワーク	高	不要	不要	変更なし	低	高	高	なし	なし	7.7	重要
		情報の暴露	接続されたストレージデバイスによる情報漏洩（USBインターフェース等の対応機器）	物理	低	低	要	変更なし	高	なし	なし	なし	なし	4.1	警告
		マルウェア感染	接続されたストレージデバイスによるマルウェア感染（USBインターフェース等の対応機器）	物理	低	低	要	変更なし	高	高	高	なし	なし	6.4	警告
		踏み台	BOT化等、攻撃の踏み台として悪用される	ネットワーク	低	低	不要	変更あり	低	なし	なし	なし	なし	5	警告
スマートホームサービス対応機器群とホームゲートウェイ間の通信経路	EP⑧	なりすまし	中間者攻撃による機器の制御信号のなりすまし	隣接	高	低	不要	変更あり	低	高	高	なし	なし	7.9	重要
		情報の暴露	中間者攻撃によるインターネット経路上の情報窃取	隣接	高	低	不要	変更なし	高	なし	なし	なし	なし	4.8	警告

脅威事例				基本値											
エントリーポイント	EP番号	脅威分類	脅威事例	攻撃元区分	攻撃条件の複雑さ	攻撃に必要な特権レベル	利用者の関与	影響の想定範囲（スコープ）	機密性への影響	完全性への影響	可用性への影響	生命・財産への影響	情報の重要度	リスク値	リスク値ランク
スマートフォンアプリ	EP⑨	情報の暴露	スマートフォンアプリの脆弱性によるデバイス内データの情報漏洩	ネットワーク	高	不要	不要	変更あり	高	なし	なし	なし	高	7.6	重要
		情報の暴露	スマートフォンアプリの不正ログインによる情報漏洩	ネットワーク	低	低	不要	変更なし	高	なし	なし	なし	高	7.2	重要
		なりすまし	スマートフォンアプリの不正ログインによる機器の不正操作(なりすまし)	ネットワーク	低	低	不要	変更あり	なし	なし	高	なし	なし	7.7	重要
スマートフォンとホームゲートウェイ間の通信経路	EP⑩	なりすまし	中間者攻撃による機器の制御信号のなりすまし	隣接	高	低	不要	変更あり	低	高	高	なし	なし	7.9	重要
		情報の暴露	中間者攻撃によるインターネット経路上の情報窃取	隣接	高	低	不要	変更なし	高	なし	なし	なし	高	5.5	警告

※リスク評価計算の前提

・自動シャッター開閉サービスのユースケースに基づき、スマートホームサービス対応機器群については、個人情報の蓄積・伝送を行わないものとする。

表 3-39 防犯駆けつけサービス（★★★）のリスク値（セキュリティ対策前）

脅威事例				基本値											
エントリーポイント	EP番号	脅威分類	脅威事例	攻撃元区分	攻撃条件の複雑さ	攻撃に必要な特権レベル	利用者の関与	影響の想定範囲（スコープ）	機密性への影響	完全性への影響	可用性への影響	生命・財産への影響	情報の重要度	リスク値	リスク値ランク
スマートホームサービス情報基盤	EP①	不正アクセス	サービス情報基盤に対する不正アクセス （既知の脆弱性を利用）	ネットワーク	高	不要	不要	変更なし	高	高	高	あり	高	10	緊急
		情報の暴露	サービス情報基盤内のデータに対する情報窃取（アクセス制御、認証不備）	ネットワーク	低	低	不要	変更なし	高	なし	なし	なし	高	7.2	重要
		データ改ざん	サービス情報基盤のデータ、設定値の改ざん	ネットワーク	高	不要	不要	変更なし	高	高	高	あり	高	10	緊急
		なりすまし	API経由の通信において第三者サービス情報基盤、ホームゲートウェイになりすまし、改ざんメッセージによる攻撃が行われる	ネットワーク	高	不要	不要	変更なし	低	高	高	あり	高	10	緊急
		マルウェア感染	サービス情報基盤のマルウェア感染（外部インターネット経由の攻撃）	ネットワーク	高	不要	不要	変更なし	高	高	高	あり	高	10	緊急
		サービス不能	DDoS（DoS）攻撃	ネットワーク	低	不要	不要	変更なし	なし	なし	高	あり	なし	9.3	緊急
		情報の暴露	持ち込まれたストレージデバイスによる情報漏洩	物理	低	低	要	変更なし	高	なし	なし	なし	高	4.9	警告
		マルウェア感染	持ち込まれたストレージデバイスによるマルウェア感染	物理	低	低	要	変更なし	高	高	高	あり	高	10	緊急
		情報の暴露	アップデート用のソフトウェアの情報窃取	ネットワーク	高	不要	不要	変更なし	高	高	高	なし	高	9.3	緊急
		データ改ざん	アップデート用のソフトウェアの改ざん	ネットワーク	高	不要	不要	変更なし	高	高	高	あり	高	10	緊急
スマートホームサービス情報基盤情報基盤とインターネット間の通信経路	EP②	情報の暴露	中間者攻撃によるインターネット経路上の情報窃取	隣接	高	低	不要	変更なし	高	なし	なし	なし	高	5.5	警告

脅威事例				基本値											
エントリーポイント	EP番号	脅威分類	脅威事例	攻撃元区分	攻撃条件の複雑さ	攻撃に必要な特権レベル	利用者の関与	影響の想定範囲（スコープ）	機密性への影響	完全性への影響	可用性への影響	生命・財産への影響	情報の重要度	リスク値	リスク値ランク
第三者サービス情報基盤	EP③	不正アクセス	サービス情報基盤に対する不正アクセス （既知の脆弱性を利用）	ネットワーク	高	不要	不要	変更なし	高	高	高	あり	高	10	緊急
		情報の暴露	サービス情報基盤内のデータに対する情報窃取（アクセス制御、認証不備）	ネットワーク	低	低	不要	変更なし	高	なし	なし	なし	高	7.2	重要
		データ改ざん	サービス情報基盤のデータ、設定値の改ざん	ネットワーク	高	不要	不要	変更なし	高	高	高	あり	高	10	緊急
		なりすまし	API経由の通信においてスマートホームサービス情報基盤になりすまし、改ざんメッセージによる攻撃が行われる	ネットワーク	高	不要	不要	変更なし	低	高	高	あり	高	10	緊急
		マルウェア感染	サービス情報基盤のマルウェア感染（外部インターネット経由の攻撃）	ネットワーク	高	不要	不要	変更なし	高	高	高	あり	高	10	緊急
		サービス不能	DDoS（DoS）攻撃	ネットワーク	低	不要	不要	変更なし	なし	なし	高	あり	なし	9.3	緊急
		情報の暴露	持ち込まれたストレージデバイスによる情報漏洩	物理	低	低	要	変更なし	高	なし	なし	なし	高	4.9	警告
		マルウェア感染	持ち込まれたストレージデバイスによるマルウェア感染	物理	低	低	要	変更なし	高	高	高	あり	高	10	緊急
		情報の暴露	アップデート用のソフトウェアの情報窃取	ネットワーク	高	不要	不要	変更なし	高	高	高	なし	高	9.3	緊急
		データ改ざん	アップデート用のソフトウェアの改ざん	ネットワーク	高	不要	不要	変更なし	高	高	高	あり	高	10	緊急
第三者サービス情報基盤とインターネット間の通信経路	EP④	情報の暴露	中間者攻撃によるインターネット経路上の情報窃取	隣接	高	低	不要	変更なし	高	なし	なし	なし	高	5.5	警告

脅威事例				基本値											
エントリーポイント	EP番号	脅威分類	脅威事例	攻撃元区分	攻撃条件の複雑さ	攻撃に必要な特権レベル	利用者の関与	影響の想定範囲（スコープ）	機密性への影響	完全性への影響	可用性への影響	生命・財産への影響	情報の重要度	リスク値	リスク値ランク
ホームゲートウェイ	EP⑤	不正アクセス	ホームゲートウェイに対する不正アクセス （既知の脆弱性を利用）	ネットワーク	高	不要	不要	変更なし	高	高	高	あり	高	10	緊急
		情報の暴露	ホームゲートウェイ内のデータ、設定値の情報窃取（アクセス制御、認証不備）	ネットワーク	低	低	不要	変更なし	高	なし	なし	なし	高	7.2	重要
		データ改ざん	ホームゲートウェイ内のデータ、設定値の改ざん	ネットワーク	高	不要	不要	変更なし	高	高	高	あり	高	10	緊急
		なりすまし	API経由の通信においてサービス情報基盤になりすまし、改ざんメッセージによる攻撃が行われる	ネットワーク	高	不要	不要	変更なし	低	高	高	あり	高	10	緊急
		マルウェア感染	ホームゲートウェイのマルウェア感染（外部インターネット経由の攻撃）	ネットワーク	高	不要	不要	変更なし	高	高	高	あり	高	10	緊急
		サービス不能	DDoS（DoS）攻撃	ネットワーク	低	不要	不要	変更なし	なし	なし	高	あり	なし	9.3	緊急
		情報の暴露	接続されたストレージデバイスによる情報漏洩	物理	低	低	要	変更なし	高	なし	なし	なし	高	4.9	警告
		マルウェア感染	接続されたストレージデバイスによるマルウェア感染	物理	低	低	要	変更なし	高	高	高	あり	高	10	緊急
		マルウェア感染	LAN内接続機器からのマルウェア感染	隣接	低	不要	不要	変更なし	高	高	高	あり	高	10	緊急
		踏み台	BOT化等、攻撃の踏み台として悪用される	ネットワーク	低	低	不要	変更あり	なし	なし	なし	なし	なし	3.2	注意
ホームゲートウェイとインターネット間の通信経路	EP⑥	情報の暴露	中間者攻撃によるインターネット経路上の情報窃取	隣接	高	低	不要	変更なし	高	なし	なし	なし	高	5.5	警告

脅威事例				基本値											
エントリーポイント	EP番号	脅威分類	脅威事例	攻撃元区分	攻撃条件の複雑さ	攻撃に必要な特権レベル	利用者の関与	影響の想定範囲（スコープ）	機密性への影響	完全性への影響	可用性への影響	生命・財産への影響	情報の重要度	リスク値	リスク値ランク
スマートホームサービス対応機器群	EP⑦	不正アクセス	機器に対する不正アクセス（既知の脆弱性を利用）	ネットワーク	高	不要	不要	変更なし	高	高	高	あり	高	10	緊急
		情報の暴露	機器内のデータ、設定値の情報窃取（アクセス制御、認証不備）	ネットワーク	低	低	不要	変更なし	高	なし	なし	なし	高	7.2	重要
		データ改ざん	機器内のデータ、設定値の改ざん	ネットワーク	高	不要	不要	変更なし	高	高	高	あり	なし	10	緊急
		なりすまし	通信においてホームゲートウェイになりすまし、改ざんメッセージによる攻撃が行われる	ネットワーク	高	不要	不要	変更なし	低	高	高	あり	なし	10	緊急
		情報の暴露	接続されたストレージデバイスによる情報漏洩（USBインターフェース等の対応機器）	物理	低	低	要	変更なし	高	なし	なし	なし	高	4.9	警告
		マルウェア感染	接続されたストレージデバイスによるマルウェア感染（USBインターフェース等の対応機器）	物理	低	低	要	変更なし	高	高	高	あり	高	10	緊急
		踏み台	BOT化等、攻撃の踏み台として悪用される	ネットワーク	低	低	不要	変更あり	低	なし	なし	なし	なし	5	警告
スマートホームサービス対応機器群とホームゲートウェイ間の通信経路	EP⑧	なりすまし	中間者攻撃による機器の制御信号のなりすまし	隣接	高	低	不要	変更あり	低	高	高	あり	なし	10	緊急
		情報の暴露	中間者攻撃によるインターネット経路上の情報窃取	隣接	高	低	不要	変更なし	高	なし	なし	なし	高	5.5	警告

脅威事例				基本値											
エントリーポイント	EP番号	脅威分類	脅威事例	攻撃元区分	攻撃条件の複雑さ	攻撃に必要な特権レベル	利用者の関与	影響の想定範囲（スコープ）	機密性への影響	完全性への影響	可用性への影響	生命・財産への影響	情報の重要度	リスク値	リスク値ランク
スマートフォンアプリ	EP⑨	情報の暴露	スマートフォンアプリの脆弱性によるデバイス内データの情報漏洩	ネットワーク	高	不要	不要	変更あり	高	なし	なし	なし	高	7.6	重要
		情報の暴露	スマートフォンアプリの不正ログインによる情報漏洩	ネットワーク	低	低	不要	変更なし	高	なし	なし	なし	高	7.2	重要
		なりすまし	スマートフォンアプリの不正ログインによる機器の不正操作(なりすまし)	ネットワーク	低	低	不要	変更あり	なし	なし	高	なし	なし	7.7	重要
スマートフォンとホームゲートウェイ間の通信経路	EP⑩	なりすまし	中間者攻撃による機器の制御信号のなりすまし	隣接	高	低	不要	変更あり	低	高	高	なし	なし	7.9	重要
		情報の暴露	中間者攻撃によるインターネット経路上の情報窃取	隣接	高	低	不要	変更なし	高	なし	なし	なし	高	5.5	警告

3.6　リスク分析・評価のまとめ

本章では、スマートホーム向け製品・サービスのリスク分析・評価の概要と手順を説明した。その過程で、スマートホーム向け製品・サービスのリスク値の計算において、生命・財産への影響と個人情報など取り扱う情報の重要度を反映するために、独自の計算方法を定義した。

スマートホーム独自方式で 2.4.1 節および 2.4.2 節のユースケースに適用した結果、生命・財産に影響を及ぼす脅威や、個人情報を扱う脅威のリスク値に反映されることを確認した。

3.7　セキュリティ対策の検討

リスク値を計算した結果、深刻度が高い脅威から、セキュリティ対策を検討する。セキュリティ対策は、「IoT 開発におけるセキュリティ設計の手引き」[6]の「表 3-6・表 3-7　対策候補一覧」、「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 2 版）」[9]の「Annex 2 物理的・技術的対策編 対策項目一覧表」や、OTA[18]、OWASP[19]等のフレームワークを参照して設定する。また、対策の検討にあたっては、インシデントの発生頻度、発生したときの影響度、対策の実施にかかるコスト等も考慮すべきである。本書において検討したセキュリティ対策の内容については、4 章以降で述べるものとする。

またセキュリティ対策を定義した後に CVSS の環境評価値を評価することで、対策の妥当性や費用対効果を確認することができる。

シャッター自動開閉サービス（★★）と防犯駆けつけサービス（★★★）の計算結果を、それぞれ表 3-40 と表 3-41 に示す。

表 3-40 シャッター自動開閉サービス（★★）のリスク値（セキュリティ対策後）

脅威事例				環境値													
エントリーポイント	EP番号	脅威分類	脅威事例	機密性の要求度	完全性の要求度	可用性の要求度	緩和対策後の攻撃元区分	緩和対策後の攻撃条件の複雑さ	緩和対策後に必要な特権レベル	緩和対策後の利用者の関与	緩和対策後の影響の想定範囲	緩和対策後の機密性への影響	緩和対策後の完全性への影響	緩和対策後の可用性への影響	緩和対策後の生命・財産への影響	緩和対策後の情報の重要度	リスク値	リスク値ランク
スマートホームサービス情報基盤	EP①	不正アクセス	サービス情報基盤に対する不正アクセス（既知の脆弱性を利用）	高	高	高	ネットワーク	高	不要	不要	変更なし	低	低	低	なし	高	7.7	重要
		情報の暴露	サービス情報基盤内のデータに対する情報窃取（アクセス制御、認証不備）	高	高	低	ネットワーク	高	高	不要	変更なし	低	低	なし	なし	高	5	警告
		データ改ざん	サービス情報基盤のデータ、設定値の改ざん	高	高	高	ネットワーク	高	不要	不要	変更なし	低	低	低	なし	高	7.7	重要
		なりすまし	API経由の通信において第三者サービス情報基盤、ホームゲートウェイになりすまし、改ざんメッセージによる攻撃が行われる	低	高	高	ネットワーク	高	不要	不要	変更なし	低	低	低	なし	高	6.9	警告
		マルウェア感染	サービス情報基盤のマルウェア感染（外部インターネット経由の攻撃）	高	高	高	ネットワーク	高	不要	不要	変更なし	低	低	低	なし	高	7.7	重要
		サービス不能	DDoS（DoS）攻撃	低	低	高	ネットワーク	低	不要	不要	変更なし	なし	なし	低	なし	なし	6.1	警告
		情報の暴露	持ち込まれたストレージデバイスによる情報漏洩	高	低	低	物理	低	高	要	変更なし	低	なし	なし	なし	高	2.8	注意
		マルウェア感染	持ち込まれたストレージデバイスによるマルウェア感染	高	高	高	物理	低	高	要	変更なし	低	低	低	なし	高	5.6	警告
		情報の暴露	アップデート用のソフトウェアの情報窃取	高	高	高	ネットワーク	高	不要	不要	変更なし	低	低	低	なし	高	7.7	重要
		データ改ざん	アップデート用のソフトウェアの改ざん	高	高	高	ネットワーク	高	不要	不要	変更なし	低	低	低	なし	高	7.7	重要
スマートホームサービス情報基盤情報基盤とインターネット間の通信経路	EP②	情報の暴露	中間者攻撃によるインターネット経路上の情報窃取	高	高	低	隣接	高	高	不要	変更なし	低	なし	なし	なし	高	3.1	注意

脅威事例				環境値														
エントリーポイント	EP番号	脅威分類	脅威事例	機密性の要求度	完全性の要求度	可用性の要求度	緩和対策後の攻撃元区分	緩和対策後の攻撃条件の複雑さ	緩和対策後に必要な特権レベル	緩和対策後の利用者の関与	緩和対策後の影響の想定範囲	緩和対策後の機密性への影響	緩和対策後の完全性への影響	緩和対策後の可用性への影響	緩和対策後の生命・財産への影響	緩和対策後の情報の重要度	リスク値	リスク値ランク
第三者サービス情報基盤	EP③	不正アクセス	サービス情報基盤に対する不正アクセス （既知の脆弱性を利用）	高	高	高	ネットワーク	高	不要	不要	変更なし	低	低	低	なし	なし	6.8	警告
		情報の暴露	サービス情報基盤内のデータに対する情報窃取（アクセス制御、認証不備）	高	高	低	ネットワーク	高	高	不要	変更なし	低	低	なし	なし	なし	4.3	警告
		データ改ざん	サービス情報基盤のデータ、設定値の改ざん	高	高	高	ネットワーク	高	不要	不要	変更なし	低	低	低	なし	なし	6.8	警告
		なりすまし	API経由の通信においてスマートホームサービス情報基盤になりすまし、改ざんメッセージによる攻撃が行われる	低	高	高	ネットワーク	高	不要	不要	変更なし	低	低	低	なし	なし	6.1	警告
		マルウェア感染	サービス情報基盤のマルウェア感染（外部インターネット経由の攻撃）	高	高	高	ネットワーク	高	不要	不要	変更なし	低	低	低	なし	なし	6.8	警告
		サービス不能	DDoS（DoS）攻撃	低	低	高	ネットワーク	低	不要	不要	変更なし	なし	なし	低	なし	なし	6.1	警告
		情報の暴露	持ち込まれたストレージデバイスによる情報漏洩	高	低	低	物理	低	高	要	変更なし	低	なし	なし	なし	なし	2.4	注意
		マルウェア感染	持ち込まれたストレージデバイスによるマルウェア感染	高	高	高	物理	低	高	要	変更なし	低	低	低	なし	なし	4.8	警告
		情報の暴露	アップデート用のソフトウェアの情報窃取	高	高	高	ネットワーク	高	不要	不要	変更なし	低	低	低	なし	なし	6.8	警告
		データ改ざん	アップデート用のソフトウェアの改ざん	高	高	高	ネットワーク	高	不要	不要	変更なし	低	低	低	なし	なし	6.8	警告
第三者サービス情報基盤とインターネット間の通信経路	EP④	情報の暴露	中間者攻撃によるインターネット経路上の情報窃取	高	高	低	隣接	高	高	不要	変更なし	低	なし	なし	なし	なし	2.7	注意

脅威事例				環境値													
エントリーポイント	EP番号	脅威分類	脅威事例	機密性の要求度	完全性の要求度	可用性の要求度	緩和対策後の攻撃元区分	緩和対策後の攻撃条件の複雑さ	緩和対策後に必要な特権レベル	緩和対策後の利用者の関与	緩和対策後の影響の想定範囲	緩和対策後の機密性への影響	緩和対策後の完全性への影響	緩和対策後の可用性への影響	緩和対策後の生命・財産への影響	緩和対策後の情報の重要度	リスク値	リスク値ランク
ホームゲートウェイ	EP⑤	不正アクセス	ホームゲートウェイに対する不正アクセス （既知の脆弱性を利用）	高	高	高	ネットワーク	高	不要	不要	変更なし	低	低	低	なし	なし	6.8	警告
		情報の暴露	ホームゲートウェイ内のデータ、設定値の情報窃取（アクセス制御、認証不備）	高	高	低	ネットワーク	高	高	不要	変更なし	低	低	なし	なし	なし	4.3	警告
		データ改ざん	ホームゲートウェイ内のデータ、設定値の改ざん	高	高	高	ネットワーク	高	不要	不要	変更なし	低	低	低	なし	なし	6.8	警告
		なりすまし	API経由の通信においてサービス情報基盤になりすまし、改ざんメッセージによる攻撃が行われる	低	高	高	ネットワーク	高	不要	不要	変更なし	低	低	低	なし	なし	6.1	警告
		マルウェア感染	ホームゲートウェイのマルウェア感染（外部インターネット経由の攻撃）	高	高	高	ネットワーク	高	不要	不要	変更なし	低	低	低	なし	なし	6.8	警告
		サービス不能	DDoS（DoS）攻撃	低	低	高	ネットワーク	低	不要	不要	変更なし	なし	なし	低	なし	なし	6.1	警告
		情報の暴露	接続されたストレージデバイスによる情報漏洩	高	低	低	物理	低	高	要	変更なし	低	なし	なし	なし	なし	2.4	注意
		マルウェア感染	接続されたストレージデバイスによるマルウェア感染	高	高	高	物理	低	高	要	変更なし	低	低	低	なし	なし	4.8	警告
		マルウェア感染	LAN内接続機器からのマルウェア感染	高	高	高	隣接	低	不要	不要	変更なし	低	低	低	なし	なし	7.4	重要
		踏み台	BOT化等、攻撃の踏み台として悪用される	低	低	低	ネットワーク	低	高	不要	変更あり	なし	なし	なし	なし	なし	2.3	注意
ホームゲートウェイとインターネット間の通信経路	EP⑥	情報の暴露	中間者攻撃によるインターネット経路上の情報窃取	高	高	低	隣接	高	高	不要	変更なし	低	なし	なし	なし	なし	2.7	注意

脅威事例				環境値														
エントリーポイント	EP番号	脅威分類	脅威事例	機密性の要求度	完全性の要求度	可用性の要求度	緩和対策後の攻撃元区分	緩和対策後の攻撃条件の複雑さ	緩和対策後に必要な特権レベル	緩和対策後の利用者の関与	緩和対策後の影響の想定範囲	緩和対策後の機密性への影響	緩和対策後の完全性への影響	緩和対策後の可用性への影響	緩和対策後の生命・財産への影響	緩和対策後の情報の重要度	リスク値	リスク値ランク
スマートホームサービス対応機器群	EP⑦	不正アクセス	機器に対する不正アクセス（既知の脆弱性を利用）	高	高	高	ネットワーク	高	不要	不要	変更なし	低	低	低	なし	なし	6.8	警告
		情報の暴露	機器内のデータ、設定値の情報窃取（アクセス制御、認証不備）	高	高	低	ネットワーク	高	高	不要	変更なし	低	なし	なし	なし	なし	2.9	注意
		データ改ざん	機器内のデータ、設定値の改ざん	高	高	高	ネットワーク	高	不要	不要	変更なし	低	低	低	なし	なし	6.8	警告
		なりすまし	通信においてホームゲートウェイになりすまし、改ざんメッセージによる攻撃が行われる	低	高	高	ネットワーク	高	不要	不要	変更なし	低	低	低	なし	なし	6.1	警告
		情報の暴露	接続されたストレージデバイスによる情報漏洩（USBインターフェース等の対応機器）	高	低	低	物理	低	高	要	変更なし	低	なし	なし	なし	なし	2.4	注意
		マルウェア感染	接続されたストレージデバイスによるマルウェア感染（USBインターフェース等の対応機器）	高	高	高	物理	低	高	要	変更なし	低	低	低	なし	なし	4.8	警告
		踏み台	BOT化等、攻撃の踏み台として悪用される	低	低	低	ネットワーク	低	高	不要	変更あり	なし	なし	なし	なし	なし	2.3	注意
スマートホームサービス対応機器群とホームゲートウェイ間の通信経路	EP⑧	なりすまし	中間者攻撃による機器の制御信号のなりすまし	高	高	高	物理	高	高	不要	変更あり	低	低	低	なし	なし	5.8	警告
		情報の暴露	中間者攻撃によるインターネット経路上の情報窃取	高	高	低	隣接	高	高	不要	変更なし	低	なし	なし	なし	なし	2.7	注意

脅威事例				環境値														
エントリーポイント	EP番号	脅威分類	脅威事例	機密性の要求度	完全性の要求度	可用性の要求度	緩和対策後の攻撃元区分	緩和対策後の攻撃条件の複雑さ	緩和対策後に必要な特権レベル	緩和対策後の利用者の関与	緩和対策後の影響の想定範囲	緩和対策後の機密性への影響	緩和対策後の完全性への影響	緩和対策後の可用性への影響	緩和対策後の生命・財産への影響	緩和対策後の情報の重要度	リスク値	リスク値ランク
スマートフォンアプリ	EP⑨	情報の暴露	スマートフォンアプリの脆弱性によるデバイス内データの情報漏洩	高	高	高	ローカル	高	不要	不要	変更あり	低	なし	なし	なし	高	4.5	警告
		情報の暴露	スマートフォンアプリの不正ログインによる情報漏洩	高	高	高	ネットワーク	低	高	不要	変更なし	なし	なし	低	なし	高	3.8	注意
		なりすまし	スマートフォンアプリの不正ログインによる機器の不正操作(なりすまし)	高	高	高	ネットワーク	低	高	不要	変更あり	なし	なし	低	なし	なし	5	警告
スマートフォンとホームゲートウェイ間の通信経路	EP⑩	なりすまし	中間者攻撃による機器の制御信号のなりすまし	高	高	高	物理	高	高	不要	変更あり	低	低	低	なし	なし	5.8	警告
		情報の暴露	中間者攻撃によるインターネット経路上の情報窃取	高	高	低	隣接	高	高	不要	変更なし	低	なし	なし	なし	高	3.1	注意

※リスク評価計算の前提

・自動シャッター開閉サービスのユースケースに基づき、スマートホームサービス対応機器群については、個人情報の蓄積・伝送を行わないものとする。

・機密性、完全性、可用性に対する影響については、本書のセキュリティ要件あるいはセキュリティ要求事項に準拠することを前提として、緩和対策後の影響を「低」に設定している。

・生命・財産に対する影響については、本書のセキュリティ要件あるいはセキュリティ要求事項に準拠することを前提として、緩和対策後の影響を「なし」に設定している。

・情報の重要度については、セキュリティ対策を実施後も保護すべき資産は引き続き存在するため、緩和対策後であっても値の変更は行っていない。

表 3-41 防犯駆けつけサービス（★★★）のリスク値（セキュリティ対策後）

脅威事例				環境値														
エントリーポイント	EP番号	脅威分類	脅威事例	機密性の要求度	完全性の要求度	可用性の要求度	緩和対策後の攻撃元区分	緩和対策後の攻撃条件の複雑さ	緩和対策後に必要な特権レベル	緩和対策後の利用者の関与	緩和対策後の影響の想定範囲	緩和対策後の機密性への影響	緩和対策後の完全性への影響	緩和対策後の可用性への影響	緩和対策後の生命・財産への影響	緩和対策後の情報の重要度	リスク値	リスク値ランク
スマートホームサービス情報基盤	EP①	不正アクセス	サービス情報基盤に対する不正アクセス（既知の脆弱性を利用）	高	高	高	ネットワーク	高	不要	不要	変更なし	低	低	低	なし	高	7.7	重要
		情報の暴露	サービス情報基盤内のデータに対する情報窃取（アクセス制御、認証不備）	高	高	低	ネットワーク	高	高	不要	変更なし	低	低	なし	なし	高	5	警告
		データ改ざん	サービス情報基盤のデータ、設定値の改ざん	高	高	高	ネットワーク	高	不要	不要	変更なし	低	低	低	なし	高	7.7	重要
		なりすまし	API経由の通信において第三者サービス情報基盤、ホームゲートウェイになりすまし、改ざんメッセージによる攻撃が行われる	低	高	高	ネットワーク	高	不要	不要	変更なし	低	低	低	なし	高	6.9	警告
		マルウェア感染	サービス情報基盤のマルウェア感染（外部インターネット経由の攻撃）	高	高	高	ネットワーク	高	不要	不要	変更なし	低	低	低	なし	高	7.7	重要
		サービス不能	DDoS（DoS）攻撃	低	低	高	ネットワーク	低	不要	不要	変更なし	なし	なし	低	なし	なし	6.1	警告
		情報の暴露	持ち込まれたストレージデバイスによる情報漏洩	高	低	低	物理	低	高	要	変更なし	低	なし	なし	なし	高	2.8	注意
		マルウェア感染	持ち込まれたストレージデバイスによるマルウェア感染	高	高	高	物理	低	高	要	変更なし	低	低	低	なし	高	5.6	警告
		情報の暴露	アップデート用のソフトウェアの情報窃取	高	高	高	ネットワーク	高	不要	不要	変更なし	低	低	低	なし	高	7.7	重要
		データ改ざん	アップデート用のソフトウェアの改ざん	高	高	高	ネットワーク	高	不要	不要	変更なし	低	低	低	なし	高	7.7	重要
スマートホームサービス情報基盤情報基盤とインターネット間の通信経路	EP②	情報の暴露	中間者攻撃によるインターネット経路上の情報窃取	高	高	低	隣接	高	高	不要	変更なし	低	なし	なし	なし	高	3.1	注意

脅威事例				環境値														
エントリーポイント	EP番号	脅威分類	脅威事例	機密性の要求度	完全性の要求度	可用性の要求度	緩和対策後の攻撃元区分	緩和対策後の攻撃条件の複雑さ	緩和対策後に必要な特権レベル	緩和対策後の利用者の関与	緩和対策後の影響の想定範囲	緩和対策後の機密性への影響	緩和対策後の完全性への影響	緩和対策後の可用性への影響	緩和対策後の生命・財産への影響	緩和対策後の情報の重要度	リスク値	リスク値ランク
第三者サービス情報基盤	EP③	不正アクセス	サービス情報基盤に対する不正アクセス （既知の脆弱性を利用）	高	高	高	ネットワーク	高	不要	不要	変更なし	低	低	低	なし	高	7.7	重要
		情報の暴露	サービス情報基盤内のデータに対する情報窃取（アクセス制御、認証不備）	高	高	低	ネットワーク	高	高	不要	変更なし	低	低	なし	なし	高	5	警告
		データ改ざん	サービス情報基盤のデータ、設定値の改ざん	高	高	高	ネットワーク	高	不要	不要	変更なし	低	低	低	なし	高	7.7	重要
		なりすまし	API経由の通信においてスマートホームサービス情報基盤になりすまし、改ざんメッセージによる攻撃が行われる	低	高	高	ネットワーク	高	不要	不要	変更なし	低	低	低	なし	高	6.9	警告
		マルウェア感染	サービス情報基盤のマルウェア感染（外部インターネット経由の攻撃）	高	高	高	ネットワーク	高	不要	不要	変更なし	低	低	低	なし	高	7.7	重要
		サービス不能	DDoS（DoS）攻撃	低	低	高	ネットワーク	低	不要	不要	変更なし	なし	なし	低	なし	なし	6.1	警告
		情報の暴露	持ち込まれたストレージデバイスによる情報漏洩	高	低	低	物理	低	高	要	変更なし	低	なし	なし	なし	高	2.8	注意
		マルウェア感染	持ち込まれたストレージデバイスによるマルウェア感染	高	高	高	物理	低	高	要	変更なし	低	低	低	なし	高	5.6	警告
		情報の暴露	アップデート用のソフトウェアの情報窃取	高	高	高	ネットワーク	高	不要	不要	変更なし	低	低	低	なし	高	7.7	重要
		データ改ざん	アップデート用のソフトウェアの改ざん	高	高	高	ネットワーク	高	不要	不要	変更なし	低	低	低	なし	高	7.7	重要
第三者サービス情報基盤とインターネット間の通信経路	EP④	情報の暴露	中間者攻撃によるインターネット経路上の情報窃取	高	高	低	隣接	高	高	不要	変更なし	低	なし	なし	なし	高	3.1	注意

脅威事例				環境値														
エントリーポイント	EP番号	脅威分類	脅威事例	機密性の要求度	完全性の要求度	可用性の要求度	緩和対策後の攻撃元区分	緩和対策後の攻撃条件の複雑さ	緩和対策後に必要な特権レベル	緩和対策後の利用者の関与	緩和対策後の影響の想定範囲	緩和対策後の機密性への影響	緩和対策後の完全性への影響	緩和対策後の可用性への影響	緩和対策後の生命・財産への影響	緩和対策後の情報の重要度	リスク値	リスク値ランク
ホームゲートウェイ	EP⑤	不正アクセス	ホームゲートウェイに対する不正アクセス （既知の脆弱性を利用）	高	高	高	ネットワーク	高	不要	不要	変更なし	低	低	低	なし	高	7.7	重要
		情報の暴露	ホームゲートウェイ内のデータ、設定値の情報窃取（アクセス制御、認証不備）	高	高	低	ネットワーク	高	高	不要	変更なし	低	低	なし	なし	高	5	警告
		データ改ざん	ホームゲートウェイ内のデータ、設定値の改ざん	高	高	高	ネットワーク	高	不要	不要	変更なし	低	低	低	なし	高	7.7	重要
		なりすまし	API経由の通信においてサービス情報基盤になりすまし、改ざんメッセージによる攻撃が行われる	低	高	高	ネットワーク	高	不要	不要	変更なし	低	低	低	なし	高	6.9	警告
		マルウェア感染	ホームゲートウェイのマルウェア感染（外部インターネット経由の攻撃）	高	高	高	ネットワーク	高	不要	不要	変更なし	低	低	低	なし	高	7.7	重要
		サービス不能	DDoS（DoS）攻撃	低	低	高	ネットワーク	低	不要	不要	変更なし	なし	なし	低	なし	なし	6.1	警告
		情報の暴露	接続されたストレージデバイスによる情報漏洩	高	低	低	物理	低	高	要	変更なし	低	なし	なし	なし	高	2.8	注意
		マルウェア感染	接続されたストレージデバイスによるマルウェア感染	高	高	高	物理	低	高	要	変更なし	低	低	低	なし	高	5.6	警告
		マルウェア感染	LAN内接続機器からのマルウェア感染	高	高	高	隣接	低	不要	不要	変更なし	低	低	低	なし	高	8.3	重要
		踏み台	BOT化等、攻撃の踏み台として悪用される	低	低	低	ネットワーク	低	高	不要	変更あり	なし	なし	なし	なし	なし	2.3	注意
ホームゲートウェイとインターネット間の通信経路	EP⑥	情報の暴露	中間者攻撃によるインターネット経路上の情報窃取	高	高	低	隣接	高	高	不要	変更なし	低	なし	なし	なし	高	3.1	注意

脅威事例				環境値														
エントリーポイント	EP番号	脅威分類	脅威事例	機密性の要求度	完全性の要求度	可用性の要求度	緩和対策後の攻撃元区分	緩和対策後の攻撃条件の複雑さ	緩和対策後に必要な特権レベル	緩和対策後の利用者の関与	緩和対策後の影響の想定範囲	緩和対策後の機密性への影響	緩和対策後の完全性への影響	緩和対策後の可用性への影響	緩和対策後の生命・財産への影響	緩和対策後の情報の重要度	リスク値	リスク値ランク
スマートホームサービス対応機器群	EP⑦	不正アクセス	機器に対する不正アクセス（既知の脆弱性を利用）	高	高	高	ネットワーク	高	不要	不要	変更なし	低	低	低	なし	高	7.7	重要
		情報の暴露	機器内のデータ、設定値の情報窃取（アクセス制御、認証不備）	高	高	低	ネットワーク	高	高	不要	変更なし	低	なし	なし	なし	高	3.3	注意
		データ改ざん	機器内のデータ、設定値の改ざん	高	高	高	ネットワーク	高	不要	不要	変更なし	低	低	低	なし	なし	6.8	警告
		なりすまし	通信においてホームゲートウェイになりすまし、改ざんメッセージによる攻撃が行われる	低	高	高	ネットワーク	高	不要	不要	変更なし	低	低	低	なし	なし	6.1	警告
		情報の暴露	接続されたストレージデバイスによる情報漏洩（USBインターフェース等の対応機器）	高	低	低	物理	低	高	要	変更なし	低	なし	なし	なし	高	2.8	注意
		マルウェア感染	接続されたストレージデバイスによるマルウェア感染（USBインターフェース等の対応機器）	高	高	高	物理	低	高	要	変更なし	低	低	低	あり	高	8.3	重要
		踏み台	BOT化等、攻撃の踏み台として悪用される	低	低	低	ネットワーク	低	高	不要	変更あり	なし	なし	なし	なし	なし	2.3	注意
スマートホームサービス対応機器群とホームゲートウェイ間の通信経路	EP⑧	なりすまし	中間者攻撃による機器の制御信号のなりすまし	高	高	高	物理	高	高	不要	変更あり	低	低	低	あり	なし	8.5	重要
		情報の暴露	中間者攻撃によるインターネット経路上の情報窃取	高	高	低	隣接	高	高	不要	変更なし	低	なし	なし	なし	高	3.1	注意

脅威事例				環境値														
エントリーポイント	EP番号	脅威分類	脅威事例	機密性の要求度	完全性の要求度	可用性の要求度	緩和対策後の攻撃元区分	緩和対策後の攻撃条件の複雑さ	緩和対策後に必要な特権レベル	緩和対策後の利用者の関与	緩和対策後の影響の想定範囲	緩和対策後の機密性への影響	緩和対策後の完全性への影響	緩和対策後の可用性への影響	緩和対策後の生命・財産への影響	緩和対策後の情報の重要度	リスク値	リスク値ランク
スマートフォンアプリ	EP⑨	情報の暴露	スマートフォンアプリの脆弱性によるデバイス内データの情報漏洩	高	高	高	ローカル	高	不要	不要	変更あり	低	なし	なし	なし	高	4.5	警告
		情報の暴露	スマートフォンアプリの不正ログインによる情報漏洩	高	高	高	ネットワーク	低	高	不要	変更なし	なし	なし	低	なし	高	3.8	注意
		なりすまし	スマートフォンアプリの不正ログインによる機器の不正操作(なりすまし)	高	高	高	ネットワーク	低	高	不要	変更あり	なし	なし	低	なし	なし	5	警告
スマートフォンとホームゲートウェイ間の通信経路	EP⑩	なりすまし	中間者攻撃による機器の制御信号のなりすまし	高	高	高	物理	高	高	不要	変更あり	低	低	低	なし	なし	5.8	警告
		情報の暴露	中間者攻撃によるインターネット経路上の情報窃取	高	高	低	隣接	高	高	不要	変更なし	低	なし	なし	なし	高	3.1	注意

※リスク評価計算の前提

・機密性、完全性、可用性に対する影響については、本書のセキュリティ要件あるいはセキュリティ要求事項に準拠することを前提として、緩和対策後の影響を「低」に設定している。

・生命・財産に対する影響については、本書のセキュリティ要件あるいはセキュリティ要求事項に準拠することを前提として、緩和対策後の影響を「なし」に設定している。

・情報の重要度については、セキュリティ対策を実施後も保護すべき資産は引き続き存在するため、緩和対策後であっても値の変更は行っていない。

4 想定されるセキュリティ上の脅威と対策指針

本章ではスマートホーム分野において、セキュリティに影響を及ぼす特徴的な事項を整理し、セキュリティ対策指針の検討を行う。

4.1 関係する要素の多様性

2 章で説明したシステムモデルの通り、スマートホームの構成要素は多種多様であり、セキュリティ上の脅威と対策を検討する方針が見えにくい問題がある。

この問題に対しては、スマートホームの構成要素が、利用者に提供する価値の面から、個々の IoT 機器と、それらを活用したサービスに大きく分けられる点に着目して、個々の IoT 機器とサービスの観点に分けて検討することで対応する。

本ガイドラインでは、スマートホームが提供するサービスについては、システムモデルに対してセキュリティ上の脅威と対策を検討し、評価する。また、個別の IoT 機器は、それぞれのガイドラインを作成して、同様に脅威と対策の検討と評価を行う。

4.2 製品安全（セーフティ）への対応

IoT 機器を含めた電気用品の遠隔操作は、電気用品安全法（電安法）の技術基準別表第八の１（２）ロ[7]において、「手元操作が最優先されること」「遠隔操作による動作が確実に行われるよう、操作結果のフィードバック確認ができること」などの構造を備えることが規定されている。また、平成 30 年 3 月には、国立研究開発法人 産業技術総合研究所と株式会社ミサワホーム総合研究所によって、機能安全に関する基本規格 IEC 61508（電気・電子・プログラマブル電子安全関連の機能安全）の原則に従って、スマートホームで同時に動作する複数の機器・システムの機能安全を規定する国際標準の提案が国際電気標準会議（IEC）に出され、承認されている[8]。他にも、製造物責任法（PL 法）や消費生活用製品安全法（消安法）に該当する IoT 機器の場合、遠隔操作がそれらの法令を遵守しているか確認が必要である。

また、スマートホームサービス情報基盤および関係するクラウドに何らかの障害が発生してサービスの提供が停止した場合でも、その影響を最小限に留めるように、フェイルセーフ・フェイルソフトなどの製品安全が講じられている必要がある。

4.3　機器の連携

スマートホームには多数の IoT 機器が設置されるが、これらの機器は単独で動作するだけでなく、互いに連携して動作する場合がある。

しかし、異なる機器が連携する場合、次の 3 点の課題がある。①連携先の機器のセキュリティ対策の内容・水準が適切であるか不明であり、全体として適切なセキュリティ対策が取られているか判断できない。②セキュリティ水準の異なる複数の機器が連携する場合、システム上、セキュリティ上の安全性が最も低い水準の機器が攻撃の入り口となる可能性があるため、全ての構成機器を視野に入れた対策が必要である。③本書のユースケースで提示したようにサービスを対象とした場合、システムや機器の開発並びに第三者サービスとの連携において、複数の企業がマルチベンダーとして参画するため、セキュリティ上の責任分解点が明示しにくい点がある。これは同時に、サービス事業者の立場から、他社に対してセキュリティ対策基準を提示しにくいという課題にもつながる。

上記の課題への対策としては、新規サービスの企画段階において、サービスを構成するシステムモデルを対象に、リスク分析・評価を実施することが必要である。リスク分析結果を踏まえ、サービス情報基盤やホームゲートウェイ、住設機器に対して、個別にセキュリティ対策基準として要件事項を示すことで、構成システム全体のセキュリティ品質の向上を促すことができる。また、同時に参画する企業の責任分界点についても明示することができる。

4.4　利用者によるIoT機器の設置・撤去

住宅に設置される建材・住設機器は、住宅会社が設定する調達基準（例えば、JIS、内装建材の F☆☆☆☆、防犯建物部品の CP マークなど）を満たす製品が採用される。スマートホームの場合は、セキュリティ対策を有する製品であることを確認する必要があり、それを満たした機器が設置されると考えられる。

しかし、住宅が住宅会社から利用者に引き渡された後に、利用者が独自に選んだ機器が後付け設置される可能性がある。このような機器については、製品に取られているセキュリティ対策の内容・水準が不明であることも考えられる。このような機器の設置により、スマートホームのセキュリティ水準が引き下げられる場合が想定される。このため、利用者が独自に設置する機器を含めたスマートホームのセキュリティを担保する方法を考える必要がある。

この問題に対しても、CCDS サーティフィケーションプログラムによるサーティフィケーションマーク制度で対策できる。利用者は機器に表示されたサーティフィケーションマークを目安として、自身で IoT 機器を購入して設置できる。このような機器はサーティフィケーションプログラムで定義されたセキュリティ要件を満たしているため、設置後のスマートホームのセキュリティ水準は担保される。

4.5 スマートホームサービスにおけるセキュリティ対策指針の整理

スマートホーム向けサービスの提供には、スマートホームサービス情報基盤と、第三者サービス事業者の情報基盤も関係する。サービス情報基盤のクラウドシステムは、システム面だけでなく、それを運用する体制（人、運用環境、運用手順等）もセキュリティ対策を検討する必要がある。また、スマートホームサービス情報基盤は、生命・財産に影響がある情報を扱ったり、実際に機器を制御したりする可能性がある。また、場合によっては利用者の不在時に第三者に制御を許可することもあり得る。

したがって、スマートホームサービスでは、なりすましや情報の暴露、不正アクセスなどの脅威に留意すべきである。次に考慮点を挙げる。

- クラウド上のシステムとしてサービス情報基盤については、十分なセキュリティ対策を講じること。
- サービスの運用施設に物理的セキュリティ対策や人・運用環境・運用手順についてもセキュリティ対策を講じること。
- サービスを構成するシステム、機器は IoT 分野共通セキュリティ要件ガイドラインの共通要件★を満たしていること。また、★★サービス、★★★サービスを構成するシステム、機器については、それぞれがセキュリティ対策基準（6 章）を満たしていること。
- 各サービス情報基盤（スマートホーム情報基盤と第三者サービス情報基盤のどちらも含む）によるホームゲートウェイの認証、ホームゲートウェイによるスマートホーム対応機器の認証を実施すること。
- 各サービス情報基盤とホームゲートウェイ間、各サービス情報基盤間の通信経路は、セキュアな通信手段、プロトコルとすること。
- 不正な操作が行われたときに、その操作元・操作内容を追跡できるよう、機器の操作ログを採取すること。

5 スマートホームサービスのライフサイクルとセキュリティへの取り組み

本章ではスマートホームのセキュリティ対策においては、IoT 機器のライフサイクル（購入、故障、転売、廃棄）による機器の入れ替わりだけでなく、IoT 機器が変わらずその利用者が変わる場合も考慮する必要がある。

5.1 スマートホームサービスのライフサイクルにおけるフェーズの定義

本節ではサービス事業者を対象としたスマートホーム開発のライフサイクルにおけるセキュリティ対策を定義する。スマートホームサービスの開発ライフサイクルは、大きく「サービス企画」、「設計・製造」、「評価」、「運用・保守」、「サービス終了」の５フェーズに分類される。提供するスマートホームサービスにおいて十分なセキュリティを確保するには、各フェーズにおいて企業としての方針・計画策定や、法令順守すべき要件、人、運用環境・運用手順等の幅広い範囲において十分な対策を施し、提供サービスのセキュリティ品質を確実なものとするべきである。

図 5-1 スマートホームサービスのライフサイクルにおけるフェーズ

表 5-1 スマートホームサービスにおけるフェーズの定義

フェーズ	説明
サービス企画	サービスのコンセプト、要件定義、ユースケース定義、想定システムモデルにもとづくリスク分析・評価等を行う。
設計・製造	サービス企画フェーズの決定内容をもとに、サービスを構成するシステムや機器の設計、実装、製造を行う（あるいは外部委託を行う）。
評価	サービス提供において、障害やインシデントが発生しないよう、施工担当者による設置確認や使用機器の管理、監督を行う。
運用・保守	利用者へのサービス提供期間中のサービス運用や保守、インシデントへの対応等を行う。
サービス終了	サービス終了に伴い、ユーザへの周知や新規サービスへの移行手続き、収集した個人情報の破棄等を行う。

5.2 サービスのライフサイクルにおけるセキュリティへの取組み

前節で概説したライフサイクルの各フェーズにおいて実施すべきセキュリティへの取組みを説明する。

5.2.1 サービス企画フェーズ

ここではサービス企画におけるフェーズにおけるセキュリティへの取り組みを以下に示す。

表 5-2 サービス企画フェーズにおけるセキュリティへの取組み

No.	項目	説明
1	企業組織としての対応方針の策定	・企業組織として、サイバーセキュリティに対するリスクマネジメントの体制やルールの策定を行う。
2	企業組織としての個人情報管理ポリシーの策定	・個人情報保護の観点から、収集する個人情報の定義や管理ポリシーの策定を行う。
3	サービス要件やシステムモデル、ユースケースの定義	・提供サービスの要件を踏まえ、システムモデルやユースケースの定義を行う。システムモデルにおいては、サービス事業者と外部委託先等、提携する企業との責任分解点を明確化する。
4	リスク分析・評価とサービスレベルの定義	・リスク分析・評価を行い、保護すべき資産と想定される脅威およびリスク値の評価を行う。 ・リスク分析・評価の過程で、個人情報などの重要なデータの取り扱いの有無、および生命・財産への影響の有無を検討して、サービスのサーティフィケーションレベル（★★、★★★）を定義する。
5	関連法令への対応検討	スマートホームサービス上、関連法令に関して対応が必要な項目を抽出し、機器及びシステム上の対策内容を検討する。
6	セキュリティ対策方針の策定	・リスク分析・評価結果を踏まえて、必要なセキュリティ対策の方針を策定する。またセーフティに関するハザードの観点を踏まえ、可用性等についても考慮した検討を行う。
7	サービスとしての免責事項の定義	・提供サービスにおいて想定される障害に対して、免責事項を定義する。 （例えば、災害や火災等の事故発生時に伴う停電など）

5.2.2 設計・製造フェーズ

生産・施工フェーズにおけるセキュリティへの取り組みを以下に示す。

表 5-3 設計・製造フェーズにおけるセキュリティへの取組み

No.	項目	説明
1	開発委託先の体制の確認	・機器やシステムの開発委託を行う場合は、委託先の開発体制がセキュリティ・バイ・デザインに基づく品質管理を行っている事を確認する。 例） ・静的評価：セキュア設計、コーディングレビューの実施 ・動的評価：各種セキュリティテストの実施　…など
2	開発及びソリューションの外部委託	・提供サービスにおいて新たな機器の開発やソリューションが必要となった場合、開発やソリューションの外部委託先へは、提供サービスの認証レベルに応じたセキュリティ要求事項を提示し、準拠することを必須とする。 ・具体的なセキュリティ対策の内容については、本書の下記項目を参照する。 6.2　システム･サービス対応機器群に求めるセキュリティ要求事項

5.2.3 評価フェーズ

評価フェーズにおけるセキュリティへの取り組みを以下に示す。

表 5-4 評価フェーズにおけるセキュリティへの取組み

No.	項目	説明
1	施工時の認証情報、セキュリティ設定の確認	・スマートホーム施工時には、認証情報やセキュリティ設定が適切にインテグレーションされていることを確認すること。
2	脆弱性の有無のチェック	・各サービス情報基盤とホームゲートウェイ、スマートホーム対応機器に対して、既知の脆弱性の有無のチェックを行うこと。
3	スマートホームの生産・施工時の対応	※その他、評価フェーズの対策内容としては、下記スマートホームのライフサイクルにおける生産・施工フェーズを参照すること。 5.4.2　生産・施工フェーズ No.2 使用機器等の発注 No.3 使用機器等の管理・監督 No.4 施工確認

5.2.4 運用・保守フェーズ

運用・保守フェーズでのセキュリティへの取り組みを以下に示す。

表 5-5 運用・保守フェーズでのセキュリティへの取組み

No.	項目	説明
1	サービス契約者の本人認証	・サービスを提供するシステム（各サービス情報基盤、スマートホームの環境）は、サービス契約を行った本人（あるいは本人の許可を得た者）のみが利用可能とするため、認証する機能を有すること。
2	ログ収集・データ分析	・サービスを運用するシステムは、不正アクセス等のインシデント対策として、ログ収集機能を有し、また収集したログデータの分析が可能な運用体制を有すること。
3	データ削除機能の実装	・個人情報保護の観点から、サービスを運用するシステム上の

		データについては、削除機能を実装すること。
4	現場担当者の認証	・★★★サービスについては、異常検知の通報を受け、住宅に到着した現場担当者が正しい身分であるかどうかを認証する仕組みあるいは機能を有すること。
5	スマートホームサービス情報基盤の運用堅牢化①（データアクセス）	・サービス情報基盤について、下記の運用堅牢化対策を行う 1）データアクセスの手順・ルールの定義 2）データアクセス範囲の最小化 3）データアクセスログの監査 4）運用担当者のセキュリティ教育 ※いずれも下記の認証取得あるいは、認証基準に準じた運用体制を保持していること。 －ISO/IEC27017：ISMS クラウドセキュリティ認証
6	スマートホームサービス情報基盤の運用堅牢化②（サーバログイン）	・サービス情報基盤について、下記の運用堅牢化対策を行う 1）ログイン情報の管理手順・ルールの定義 2）ログイン情報の発行対象の範囲を最小化 3）運用担当者のセキュリティ教育 ※いずれも下記の認証取得あるいは、認証基準に準じた運用体制を保持していること。 －ISO/IEC27017：ISMS クラウドセキュリティ認証
7	スマートホームサービス情報基盤の運用ルーム堅牢化①（入室制限）	・許可を得ていない要員がサーバルームやオペレーションルームへ入室できないよう ID カード等で管理を行うこと。 ※下記の認証取得あるいは、認証基準に準じた運用体制を保持していること。 －ISO/IEC27017：ISMS クラウドセキュリティ認証
8	スマートホームサービス情報基盤の運用ルーム堅牢化②（デバイスの持ち込み	・サーバルームやオペレーションルームへの入室時は、ストレージデバイス、スマートフォン、PC 等の持ち込みを制限し、厳格な管理を行うこと。 ※下記の認証取得あるいは、認証基準に準じた運用体制を保持していること。

	制限）	－ISO/IEC27017：ISMS クラウドセキュリティ認証
9	スマートホームサービス情報基盤の運用ルーム堅牢化③ （入退室履歴管理）	・サーバルームやオペレーションルームへの入退室は監視カメラや ID カードの履歴によって、記録を行うこと。 ※下記の認証取得あるいは、認証基準に準じた運用体制を保持していること。 －ISO/IEC27017：ISMS クラウドセキュリティ認証
10	第三者サービス情報基盤の運用堅牢化① （データアクセス）	・サービス情報基盤（※）について、下記の運用堅牢化対策を行う １）データアクセスの手順・ルールの定義 ２）データアクセス範囲の最小化 ３）データアクセスログの監査 ４）運用担当者のセキュリティ教育 ※第三者サービス情報基盤の事例としては、コールセンターのシステム等が該当する。 ※いずれも下記の認証取得あるいは、認証基準に準じた運用体制を保持していること。 －ISO/IEC27017：ISMS クラウドセキュリティ認証
11	第三者サービス情報基盤の運用堅牢化② （サーバログイン）	・サービス情報基盤について、下記の運用堅牢化対策を行う １）ログイン情報の管理手順・ルールの定義 ２）ログイン情報の発行対象の範囲を最小化 ３）運用担当者のセキュリティ教育 ※第三者サービス基盤の事例としては、コールセンターのシステム等が該当する。 ※いずれも下記の認証取得あるいは、認証基準に準じた運用体制を保持していること。 －ISO/IEC27017：ISMS クラウドセキュリティ認証
12	第三者サービス情報基盤の運用堅牢化③	・第三者サービス情報基盤が防犯・救命に関連する機器操作を行う場合は、下記の対策を行うこと。

	（遠隔開錠操作）	１）防犯・救命に関連する機器操作の運用手順定義 ２）防犯・救命に関連する機器操作の運用ログ監査 ３）防犯・救命に関連するオペレーターのセキュリティ教育 ※第三者サービス情報基盤の事例としては、コールセンターのシステム等が該当する。 ※いずれも下記の認証取得あるいは、認証基準に準じた運用体制を保持していること。 －ISO/IEC27017：ISMS クラウドセキュリティ認証
13	第三者サービス情報基盤の運用ルーム堅牢化① （入室制限）	・許可を得ていない要員がサーバルームやオペレーションルームへ入室できないよう ID カード等で管理を行うこと。 ※第三者サービス情報基盤の事例としては、コールセンターのシステム等が該当する。 ※下記の認証取得あるいは、認証基準に準じた運用体制を保持していること。 －ISO/IEC27017：ISMS クラウドセキュリティ認証
14	第三者サービス情報基盤の運用ルーム堅牢化② （デバイスの持ち込み制限）	・サーバルームやオペレーションルームへの入室時は、ストレージデバイス、スマートフォン、PC 等の持ち込みを制限し、厳格な管理を行うこと。 ※第三者サービス情報基盤の事例としては、コールセンターのシステム等が該当する。 ※下記の認証取得あるいは、認証基準に準じた運用体制を保持していること。 －ISO/IEC27017：ISMS クラウドセキュリティ認証
15	第三者サービス情報基盤の運用ルーム堅牢化③ （入退室履歴管理）	・サーバルームやオペレーションルームへの入退室は監視カメラや ID カードの履歴によって、記録を行うこと。 ※第三者サービス情報基盤の事例としては、コールセンターのシステム等が該当する。 ※下記の認証取得あるいは、認証基準に準じた運用体制を保持していること。

		－ISO/IEC27017：ISMS クラウドセキュリティ認証
16	サービス提供上の インシデント対応	・サービス提供において発生した想定外のリスクに対応するための CSIRT を組織し、インシデントの対応を行い、再発防止対策を行う。 ・また、脆弱性の報告については、JPCERT/CC 等の組織と連携し、適切な対応を行うこと。
17	スマートホームサービス の運用保守対応	※上記以外の運用保守フェーズの対策内容としては、下記スマートホーム開発のアフターフェーズ、リフォームフェーズを参照すること。 5.4.3 アフターフェーズ 5.4.4 リフォームフェーズ

5.2.5 サービス終了フェーズ

サービス終了フェーズでのセキュリティへの取り組みを以下に示す。

表 5-6 サービス終了フェーズでのセキュリティへの取組み

No.	項目	説明
1	サービス終了の通知	・提供サービスの終了にあたっては、利用者保護の観点から、サービス利用停止までに 1 年間程度の期間を定め、利用者に事前周知を行うこと。また代替サービスの説明を含め、利用者に適切な説明を行うこと。
2	収集した個人情報の破棄	・提供サービスの終了時には個人情報の管理ポリシーに沿って、収集した個人情報の破棄を行うこと。但し、代替サービスへの移行が行われる場合には、利用者による同意を前提とし、継続して個人情報のサービス利用が行なえるものとする。
3	機器廃棄方法の周知	※機器廃棄方法の周知フェーズについては、下記スマートホーム開発の解体フェーズを参照すること。 5.4.6 解体フェーズ No.1 機器廃棄方法の周知

5.3　スマートホームのライフサイクルにおけるフェーズの定義

本節ではサービス事業者及びシステム運用ベンダーを対象としたスマートホーム（住宅）のライフサイクルにおけるセキュリティ対策を定義する。住宅のライフサイクルは、大きく「設計」、「生産・施工」、「アフター」、「リフォーム」、「転売」「解体」の６フェーズに分類される。提供するスマートホームサービスにおいて十分なセキュリティを確保するには、各フェーズにおいて十分な対策を施し、製品のセキュリティ品質を確実なものとするべきである。

図 5-2 スマートホームのライフサイクルにおけるフェーズ

表 5-7 スマートホームにおけるフェーズの定義

フェーズ	説明
設計	IoT 住宅設備を含めたスマートホーム住宅の設計を行う
生産・施工	IoT 住宅設備を含めたスマートホーム住宅の生産、施工を行う
アフター	施工後に家主が居住を開始し、スマートホーム住宅の情報活用、運用、メンテナンスを行う
リフォーム	スマートホーム住宅のリフォームを行う
転売	スマートホーム住宅の家主の変更を行う
解体	スマートホーム住宅の使用を終了し、解体を行う

5.4　スマートホームのライフサイクルにおけるセキュリティへの取組み

前節で概説したライフサイクルの各フェーズにおいて実施すべきセキュリティへの取組みを説明する。

5.4.1 設計フェーズ

設計フェーズにおけるセキュリティへの取り組みを以下に示す。

表 5-8 設計フェーズでのセキュリティへの取組み

No.	項目	説明
1	サービス選定	・利用者に対してサービス内容を説明し、利用するサービスの同意を得る。
2	設置機器の選定	・提供サービスの認証レベルに応じて、セキュリティ対策基準を満たした機器の選定を行う ・具体的なセキュリティ対策の内容については、本書の下記項目を参照する。 6.2　システム・サービス対応機器群に求めるセキュリティ要求事項
3	設計図書への表記・指示	・使用機器を設計図書（システム系統図など）へもれなく表記する。

5.4.2 生産・施工フェーズ

生産・施工フェーズにおけるセキュリティへの取り組みを以下に示す。

表 5-9 生産・施工フェーズにおけるセキュリティへの取組み

No.	項目	説明
1	利用者同意取得	・サービスの利用者（利用者）に対し、個人情報等の取り扱いについて説明し、同意を得る。 ・責任分界点の明示および説明を実施する。 ・サービスにおける免責事項について説明を行い、利用者の同意を得る。
2	使用機器等の発注	・設計図書との整合性を確認する（ホームゲートウェイ、センサー、配線、など)。
3	使用機器等の管理・監督	・不正な機器の導入がないか、使用機器に不具合がないか、を確認する。 ・施工時に、宅内に設置される機器が、サービスに対応するセキュリティ要件を満たした機種（品名・型番）であることを確認する。
4	施工確認	・契約者、使用機器、オプションの状況を確認する。 ・施工時および施工後の設計図書、発注明細との整合性確認および監理を行う（※ただし、写真等での記録も可とする)。 ・使用機器等の施工後の動作確認を行う。 ・システム全体の正常性確認を行う。
5	提供物確認	・キー、カード等の払い出し数と引き渡し数を突き合わせる。
6	使用機器およびサービス利用方法の説明	・使用機器およびサービス利用方法の説明 ・使用機器やサービスの利用方法について、利用者に説明する。
7	利用規約	・免責事項、不具合時の対応方法やサービス事業者の連絡先などを記載する。

5.4.3 アフターフェーズ

アフターフェーズでのセキュリティにおける取り組みを以下に示す。

表 5-10 アフターフェーズにおけるセキュリティへの取組み

No.	項目	説明
1	利用規約または取扱説明書の提供	・サービス提供上の免責事項は、利用規約または取扱説明書に明示し、利用者へ提示すること。 ・利用者へ、提供サービスのセキュリティ対策方針を提示すること。
2	運用時の使われ方の定義	・スマートホーム内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する。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、サービスの目的や提供機能について、周知すること。
3	ユーザへの注意喚起	・不審な機器が接続されている場合や、機器の異常動作が見られる場合には、速やかにサービス事業者へ連絡するよう取扱説明書に記載を行う。 ・初期設定値の利用や、設定ミスによりセキュリティ上、脆弱な状態となる事が想定されるケースについては、取扱説明書にてユーザに注意喚起を促すこと。
4	最新の脆弱性への対応	・使用している OS、boot プログラム、アプリケーションに脆弱性がないかどうかを、脆弱性関連情報を常にウォッチし、関連する脆弱性が報告された場合、アップデートプログラムを提供する。 ・サービス利用者に対して、更新された最新のプログラムが存在することを通知し、脆弱性の影響についての注意喚起及び、プログラムのアップデート手順を周知する。
5	提供物管理	・キー、カード等の払い出し数と引き渡し数を突き合わせる。 ・紛失時に提供物の情報を更新する。
6	機器利用制限	・今現在十分と考えられているアルゴリズムや鍵長も、将来的には不十分になる可能性があり、ユーザへある時点で機器利用の停止を推奨することを検討する。

		・利用期間が長いと想定されるホームゲートウェイ においては、サービス事業者として保守期間を明確化し、マニュアルや HP 上でユーザに周知する。

5.4.4 リフォームフェーズ

リフォームフェーズにおけるセキュリティへの取り組みを以下に示す。

ただし、リフォームにおける設計および生産・施工フェーズについては、表 5-8 および表 5-9 を参照。

表 5-11 リフォームフェーズにおけるセキュリティへの取組み

No.	項目	説明
1	既導入機器との互換性確認	・使用機器等の追加・入替えおよび情報の追加・更新を行う際、既導入機器類に影響を及ぼさないか確認する。
2	機器廃棄方法の周知	※下記は、リフォーム時の利用者（入居者）変更に伴い、機器の廃棄が行われる場合の対策となる。 ・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脅威、リスクを取扱説明書等で明示し、利用者へ注意喚起を促すこと。 ・廃棄時には機器の設定やメモリ内のデータを初期化(工場出荷状態)することを取扱説明書等で推奨する。 ・破壊し廃棄することを推奨する場合には、各自治体の規則に従って廃棄処分する旨を取扱説明書等で利用者に明示する。 ・サービス事業者は、防犯に関する機器（電子錠やドアロック等）を廃棄する際、廃棄を行う事業者に対して、データの初期化を求めること。

5.4.5 転売フェーズ

転売フェーズにおけるセキュリティへの取り組みを以下に示す。

表 5-12 転売フェーズにおけるセキュリティへの取組み

No.	項目	説明
1	提供物管理	・キー、カード等の払い出し数と引き渡し数を突き合わせる。
2	機器廃棄方法の周知	※下記は、転売時の利用者（入居者）変更に伴い、機器の廃棄が行われる場合の対策となる。 ・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脅威、リスクを取扱説明書等で明示し、利用者へ注意喚起を促すこと。 ・廃棄時には機器の設定やメモリ内のデータを初期化(工場出荷状態)することを取扱説明書等で推奨する。 ・破壊し廃棄することを推奨する場合には、各自治体の規則に従って廃棄処分する旨を取扱説明書等で利用者に明示する。 ・サービス事業者は、防犯に関する機器（電子錠やドアロック等）を廃棄する際、廃棄を行う事業者に対して、データの初期化を求めること。
3	転売後の管理	・次利用者へ免責事項とセキュリティ上の注意事項を周知する。 ・セキュリティ上の注意事項については、表 4-4 アフターフェーズの下記項目を参照。 －取扱説明書の提供 －ユーザへの注意喚起 －最新の脆弱性への対応 －機器利用制限

5.4.6 解体フェーズ

解体フェーズにおけるセキュリティへの取り組みを以下に示す。

表 5-13 解体フェーズにおけるセキュリティへの取組み

No.	項目	説明
1	機器廃棄方法の周知	・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脅威、リスクを取扱説明書等で明示し、利用者へ注意喚起を促すこと。 ・廃棄時には機器の設定やメモリ内のデータを初期化(工場出荷状態)することを取扱説明書等で推奨する。 ・破壊し廃棄することを推奨する場合には、各自治体の規則に従って廃棄処分する旨を取扱説明書等で利用者に明示する。 ・サービス事業者は、防犯に関する機器（電子錠やドアロック等）を廃棄する際、廃棄を行う事業者に対して、データの初期化を求めること。

6　スマートホームサービスにおけるセキュリティ要件

本章では、これまでに検討を行ったリスク分析・評価の結果や、セキュリティ対策の取り組みを踏まえ、スマートホーム分野のサーティフィケーションプログラムに求められるサービスのセキュリティ要件及び、各構成要素に求められるセキュリティ要求事項の定義を行う。

6.1　スマートホームサービスにおけるセキュリティ要件

本節では、サーティフィケーションプログラムにおいて、対応を必須とするサービスのセキュリティ要件を定義する。

★★サービス及び★★★サービスに対する要件は、それぞれ以下の基準で選定を行った。

１）★★サービスの要件

・全てのスマートホームサービスを安全、安心かつ安定して提供するために必須事項となる要件。

※リスク評価結果をもとに深刻度が高い脅威に対して、対費用効果の高い対策を中心に選定。

２）★★★サービスの要件

・生命や財産、個人情報の保護を行うために、より厳格な対策が必要なサービスに求められる要件。

※リスク評価結果をもとにサイバー・フィジカル・セキュリティ対策フレームワーク（CPSF）[20]と照合の上、コストや対費用効果を考慮し、実装可能な項目を選定。

また本節のセキュリティ要件と 6.2 節記載のセキュリティ要求事項は、英国の「Code of Practice for Consumer IoT Security」[21]及び、米国カリフォルニア州「接続される機器のセキュリティ法」(Senate Bill No.327 CHAPTER886)[1]についても準拠した対策となる。

表 6-1 セキュリティ要件及びセキュリティ要求事項における対応表記ルール

記号	対応状況
◎	関連ガイドラインでは検討されていないが、本ガイドラインは定義している。
○	関連ガイドラインよりも、本ガイドラインでは更に詳細なディティールまで定義している。
＝	要件、要求事項の概要は、ほぼ関連ガイドラインに対応している。

本書におけるセキュリティ要件及びセキュリティ要求事項は、下記のルールに沿ってナンバリングを行っている。

[要件/要求事項]［レベル]-［種別]-［No.］

表 6-2　セキュリティ要件及びセキュリティ要求事項におけるナンバリングルール

カテゴリ	名称	英語表記	ナンバリングルール
要件/要求事項	要件	Requirements	R
	要求事項	Secondary Requirements	SR
レベル	レベル 2	Level2	2
	レベル 3	Level3	3
種別	スマートホームサービス情報基盤	Smarthome Service Information Platform	SP
	第三者サービス情報基盤	Service Provider Information Platform	PP
	ホームゲートウェイ	Home Gateway	H
	スマートホーム対応機器群	Smart home compatible devices	D
	スマートフォンアプリ	Smartphone application	A

表 6-3 スマートホームサービスにおけるセキュリティ要件

No.	レベル	対象	項目	内容	UK	SB327	CPSF
R2-1	★★	サービス	リスク分析・評価、セキュリティ対策方針の策定	・サービスを対象とした・リスク分析・評価を行い、保護すべき資産と想定される脅威およびリスク値の評価を行うこと。 ・リスク分析・評価の過程で、個人情報などの重要なデータの取り扱いの有無、および生命・財産への影響の有無を検討して、サービスの認証レベル（★★）を定義する。 ・リスク分析・評価結果を踏まえて、必要なセキュリティ対策の方針を策定すること	◎	◎	○ CPS.DS-1 CPS.AE-1 CPS.AE-3 CPS.AE-4 CPS.AE-5 CPS.DP-1
R2-2	★★	サービス	セキュリティ要求事項を満たした機器、システムの使用	・サービスを提供するシステム（各サービス情報基盤、スマートホーム内の機器やスマートフォンアプリ）は、★★サービスの要求事項を満たした機器、システムによって構成すること。 ・スマートホーム施工時には、宅内に設置される機器が、★★サービスの要求事項を満たした機種（品名・型番）であることを確認すること。	◎	◎	＝ CPS.SC-3 CPS.SC-4 CPS.SC-5 CPS.PT-3 CPS.DP-1 CPS.RP-2
R2-3	★★	サービス	IoT 機器間の認証情報とアクセス制御の初期設定	・サービス利用開始時に、IoT 機器間の認証情報あるいはアクセス制御が適切に初期設定されていることを確認すること。	＝ UK6	◎	＝ CPS.IP-1

R2-4	★★	サービス	サービス契約者の本人認証	・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の認証を行い、転売時には利用者の認証情報の変更を行うこと。	＝ UK12	◎	＝ CPS.AC-6 CPS.AC-9
R2-5	★★	サービス	スマートホーム内で利用される個人情報や蓄積情報の削除	・スマートホーム内で利用される機器については、転売時や廃棄を想定し、利用者自身が登録した個人情報及び蓄積情報の削除を可能とすること。	＝ UK8	◎	◎
R2-6	★★	サービス	スマートホームの安全な利用方法に関するガイダンス	・スマートホーム内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、サービスの目的や提供機能について、周知すること。	＝ UK12	◎	◎
R2-7	★★	サービス	最新のソフトウェアへの定期的な更新	・サービスを提供するシステム（各サービス情報基盤、スマートホーム内の機器）は最新のソフトウェアへと定期的な更新を行うこと。 ・上記において脆弱性が報告された場合には、速やかに更新用ソフトウェアの提供を行うこと。	＝ UK3	◎	○ CPS.DS-7 CPS.MA-1
R2-8	★★	サービス	更新ソフトウェアの運用手順及びバージョン管理	・各サービス情報基盤やスマートホーム内の機器に対するソフトウェア更新の運用手順を明確化し、バージョン管理を行うこと。	＝ UK3 UK7	◎	○ CPS.DS-7 CPS.MA-1

				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			
R2-9	★★	サービス	転売時のスマートホーム構成機器に対する初期化及びアップデート	・転売時には、スマートホーム内の構成機器に対して、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際に、最新の状態へのソフトウェアアップデートを行うこと。	＝ UK3 UK8	◎	○ CPS.DS-7 CPS.MA-1
R3-1	★★★	サービス	★★サービス要件への対応	・★★サービスに対するセキュリティ要件を満たしていること	※★★参照		
R3-2	★★★	サービス	リスク分析・評価、 セキュリティ対策方針の策定	・サービスを対象とした・リスク分析・評価を行い、保護すべき資産と想定される脅威およびリスク値の評価を行うこと。 ・リスク分析・評価の過程で、個人情報などの重要なデータの取り扱いの有無、および生命・財産への影響の有無を検討して、サービスの認証レベル（★★★）を定義する。	◎	◎	○ CPS.DS-1 CPS.AE-1 CPS.AE-3 CPS.AE-4 CPS.AE-5 CPS.DP-1

				・リスク分析・評価結果を踏まえて、必要なセキュリティ対策の方針を策定すること			
R3-3	★★★	サービス	セキュリティ要求事項を満たした機器、システムの使用	・サービスを提供するシステム（各サービス情報基盤、スマートホーム内の機器）は、★★★サービスの要求事項を満たした機器、システムによって構成すること。 ・スマートホーム施工時には、宅内に設置される機器が、★★★サービスの要求事項を満たした機種（品名・型番）であることを確認すること。	◎	◎	＝ CPS.SC-3 CPS.SC-4 CPS.SC-5 CPS.PT-3 CPS.DP-1 CPS.RP-2
R3-4	★★★	サービス	クラウドサービス運用における情報セキュリティ管理	・サービス事業者によるクラウドサービスの運用において、情報セキュリティ管理の仕組みを有していること。 ・第三者サービスとの連携を行う場合は、連携先のサービス事業者が、信頼できる情報セキュリティ管理の仕組みを有しているかどうか、確認を行うこと。 ・下記の認証取得あるいは、認証基準に準じた運用体制を保持していること。 ※ISO/IEC27017：ISMS クラウドセキュリティ認証	◎	◎	○ CPS.AT-1 CPS.AC-2 CPS.IP-9

R3-5	★★★	サービス	ログ収集・データ分析	・サービスを提供するシステムは、インシデント対策として、ログ収集機能を有し、また収集したログデータの分析が可能な運用体制を有すること。	＝ UK10	◎	＝ CPS.MA-2 CPS.PT-1 CPS.CM-2 CPS.CM-5 CPS.AN-2
R3-6	★★★	サービス	脆弱性の有無のチェック	・各サービス情報基盤とホームゲートウェイ、スマートホーム対応機器に対して、既知の脆弱性の有無のチェックを行うこと。実施する方法やタイミングは、提供サービスに応じて、個別に設定するものとする。	◎	◎	○ CPS.CM-7
R3-7	★★★	サービス	緊急通報時の現場担当者の認証	・★★★サービスについては、緊急時の通報を受け、住宅に到着した現場担当者が正しい身分であるかどうかを認証する仕組みあるいは機能を有すること。	◎	◎	＝ CPS.AC-2 CPS.AC-3 CPS.AC-5 CPS.AC-9

R3-8	★★★	サービス	サービス提供における インシデント対応	・サービス提供において発生した想定外のリスクに対応するための CSIRT を組織し、インシデントの対応を行い、再発防止対策を行う。 ・また、脆弱性の報告については、JPCERT/CC 等の組織と連携し、適切な対応を行うこと。	＝ UK2	◎	＝ CPS.IP-7 CPS.IP-10 CPS.AE-2 CPS.RP-4 CPS.CO-1 CPS.AN-2 CPS.AN-3 CPS.MI-1 CPS.IM-1 CPS.IM-2

6.2　システム・サービス対応機器群に求めるセキュリティ要求事項

本節では、各サービス情報基盤や、ホームゲートウェイ、スマートホーム対応機器群、スマートフォンアプリの機器及びシステムベンダーを対象にセキュリティ上の要求事項を定義する。セキュリティ要求事項は、責任分界点を定める目安として機器やシステム毎に定義しているが、必須事項ではない。個別の機器やシステムでの対応が難しい場合には、脅威分析結果をもとに別の構成要素にて対応を行い、サービス全体として一定のセキュリティ品質を満たすことを目的としている。

★★サービス及び★★★サービスに対する要求事項は、それぞれ以下の基準で選定を行った。

１）★★サービスの要求事項

・全てのスマートホームサービスを安全、安心かつ安定して提供するために必須事項のとなる要求事項。

※リスク評価結果をもとに、深刻度が高い脅威に対して、対費用効果の高い対策を中心に選定。

２）★★★サービスの要求事項

・生命や財産、個人情報の保護を行うために、より厳格な対策が必要なサービスに求められる要求事項。

※リスク評価結果をもとに CPSF と照合の上、コストや対費用効果を考慮し、実装可能な項目を選定。

6.2.1 スマートホームサービス情報基盤へのセキュリティ要求事項

スマートホーム情報基盤に対するセキュリティ上の要求事項を以下に示す。（エントリーポイント：EP①～EP②）

表 6-4 スマートホームサービス情報基盤に対するセキュリティ要求事項

No.	レベル	対象	項目	内容	UK	SB327	CPSF
SR2-SP-1	★★	スマートホームサービス情報基盤	共通要件への対応	・IoT 分野共通セキュリティガイドラインの共通要件★と同等の対策を満たしていること。	＝ UK1 UK6 UK13	＝ 1798.91.05	＝ CPS.IP-1 CPS.IP-6 CPS.PT-2
SR2-SP-2	★★	スマートホームサービス情報基盤	API における認証	・API における認証を実装し、認証情報の無効化と再発行が可能な認証方式を有すること。 ・API における認証については、報告されている脆弱性への対策を行うこと。	◎	◎	○ CPS.AC-3 CPS.AC-9
SR2-SP-3	★★	スマートホームサービス情報基盤	管理画面（提供サービスの概要表示や機能管理を行うインターフェース）ログイン時におけるユーザ認証の実施	・ログインユーザ（オペレータ）に対する認証を行う仕組みを有すること。 ・総当たり攻撃対策を行い、危殆化が疑われる場合には値の変更が可能な実装とすること。	◎	◎	＝ CPS.AC-3 CPS.AC-5 CPS.AC-6 CPS.AC-9

SR2-SP-4	★★	スマートホームサービス情報基盤	サーバログイン時におけるユーザ認証の実施	・ログインユーザ（オペレータ）に対する認証を行う仕組みを有すること。 ・総当たり攻撃対策を行い、危殆化が疑われる場合には値の変更が可能な実装とすること。	◎	◎	＝ CPS.AC-3 CPS.AC-5 CPS.AC-6 CPS.AC-9
SR2-SP-5	★★	スマートホームサービス情報基盤	ホームゲートウェイの認証	ホームゲートウェイに対する認証を行う仕組みを有すること。	◎	◎	＝ CPS.AC-3 CPS.AC-9
SR2-SP-6	★★	スマートホームサービス情報基盤	認証に必要な情報の管理	・認証に必要な情報が漏洩しないような仕組みを実装すること。	◎	◎	＝ CPS.AC-3 CPS.AC-5 CPS.AC-6 CPS.AC-9
SR2-SP-7	★★	スマートホームサービス情報基盤	セキュリティパッチの適用	・使用している OS、boot プログラム、サーバソフト、データベース、アプリケーション、その他オープンソースライブラリに脆弱性が発見され、セキュリティパッチが公開された場合は、テストを実施した上で、セキュリティパッチの適用を行うこと。	＝ UK3	◎	＝ CPS.DS-7 CPS.MA-1
SR3-SP-1	★★★	スマートホームサービス情報基盤	★★サービス要件への対応	・★★サービスのサービス基盤に対するセキュリティ要求事項を満たしていること。	※★★参照		

SR3-SP-2	★★★	スマートホームサービス情報基盤	外部インターネットからの不正アクセス防止	・外部インターネットからのアクセスに対して、不正アクセスを防止する機能を有すること。 例）ファイアウォールによる防御機能	◎	◎	○ CPS.PT-3
SR3-SP-3	★★★	スマートホームサービス情報基盤	Webアプリケーションの脆弱性を悪用した攻撃対策	・外部ネットワークから行われるWebアプリケーションの脆弱性を悪用した攻撃対策を行うこと。 例）WAF機能 ・ウェブサイト、ウェブアプリケーションが実装される場合には、下記ガイドラインに準拠した脆弱性対策を行うこと。 ※「安全なウェブサイトの作り方」[28]	○ UK13	◎	○ CPS.CM-3
SR3-SP-4	★★★	スマートホームサービス情報基盤	不正侵入検知と遮断	・ホストや通信回線を監視し、不正侵入を検知した場合に管理者へ通知を行う侵入検知と、不正アクセスや不正侵入の通信を遮断する機能を実装すること。	○ UK10	◎	＝ CPS.CM-2 CPS.CM-3 CPS.CM-5
SR3-SP-5	★★★	スマートホームサービス情報基盤	DoS対策	・サーバやネットワークなどのリソースに過剰な負荷を掛けたり、脆弱性を突くことによる(D)DoS攻撃を想定し、負荷試験の実施及び一定レベルの負荷に耐える設計とすること。	＝ UK9	◎	○ CPS.DS-6

SR3-SP-6	★★★	スマートホームサービス情報基盤	ログ採取・分析	・操作履歴、状態履歴などを記録して、インシデント発生時に分析が行えること。	○ UK10	◎	＝ CPS.MA-2 CPS.PT-1 CPS.CM-2 CPS.CM-5 CPS.AN-2
SR3-SP-7	★★★	スマートホームサービス情報基盤	マルウェア対策	サーバを対象としてアンチマルウェア/ウィルス対策を行うこと。	◎	◎	○ CPS.PT-3
SR3-SP-8	★★★	スマートホームサービス情報基盤	サーバセキュリティ対策	・下記の基本的なサーバセキュリティ対策を実施すること。 1）不要なサービスの停止、アプリケーションの削除 2）デフォルトの管理者権限アカウントの変更 3）不要なアカウントの削除	○ UK6	◎	○ CPS.AC-8 CPS.PT-2
SR3-SP-9	★★★	スマートホームサービス情報基盤	通信経路暗号化	・スマートホームサービス情報基盤との通信や、ホームゲートウェイとの通信に対しては、通信経路の暗号化を行うこと。 ※もしくは専用線やVPN等により通信経路の対策を行い、セキュリティ強度の高い構成とすること。 ※但し、★★サービスの要求事項「認証」において、認証付き暗号の実装が行われる場合は、通信経	○ UK5	◎	○ CPS.DS-3

				路暗号化の要求事項を同時に満たすものであるため、当該要求事項の対応は不要とする。 ※暗号技術については、以下を参考にガイドラインに準拠した実装とすること。 「SSL-TLS 暗号設定ガイドライン_V2.0」[22] 「電子政府における調達のために参照すべき暗号のリスト」[23]もしくは「CRYPTREC 暗号技術ガイドライン(軽量暗号)」[24]			
SR3-SP-10	★★★	スマートホームサービス情報基盤	データの暗号化	・保護すべき資産に対する暗号化を行う。 ※保護すべき資産の対象については、本書 3.2 節、表 3-2 を参照とするものとする。 ※暗号化すべき資産については、サービスやユースケースを踏まえて重要度の高いものを対象とする。 ※暗号技術については、以下を参考にガイドラインに準拠した実装とすること。 「SSL-TLS 暗号設定ガイドライン_V2.0」[22] 「電子政府における調達のために参照すべき暗号のリスト」[23]	○ UK4 UK8	◎	○ CPS.DS-2

SR3-SP-11	★★★	スマートホームサービス情報基盤	鍵管理	・通信経路暗号化やデータの暗号化に用いる鍵の管理を適切に行うこと。 ※鍵管理の方法については、以下を参考にガイドラインに準拠した実装とすること。 「NIST SP (Special Publications) 800-57」[25] 「SSL/TLS 暗号設定ガイドライン改定及び鍵管理ガイドライン作成のための調査・検討－調査報告書－」[26]	○ UK4	◎	○ CPS.DS-5
SR3-SP-12	★★★	スマートホームサービス情報基盤	収集データ最小化	・データの収集を必要最小限に留める実装とすること。	◎	◎	＝ CPS.GV-2
SR3-SP-13	★★★	スマートホームサービス情報基盤	脆弱性スキャン、ペネトレーションテスト	定期的な脆弱性スキャン、ペネトレーションテストを実施し、脆弱性の有無をチェックすること。実施するタイミングは、提供サービスに応じて、個別に設定するものとする。	◎	◎	○ CPS.CM-7

6.2.2 第三者サービス情報基盤へのセキュリティ要求事項

第三者サービス情報基盤に対するセキュリティ要求事項を以下に示す。(エントリーポイント：EP③～EP④)

表 6-5 第三者サービス情報基盤に対するセキュリティ要求事項

No.	レベル	対象	項目	内容	UK	SB327	CPSF
SR2-PP-1 ～ SR2-PP-7	★★	第三者サービス情報基盤	共通要件への対応 ～ セキュリティパッチの適用	※スマートホームサービス情報基盤に対するセキュリティ要件と同一の対策を実施すること。 ※要求事項の詳細は 6.2.1 節の SR2-SP-1～SR2-SP-7 を参照すること。	※スマートホーム情報基盤を参照		
SR3-PP-1 ～ SR3-PP-13	★★★	第三者サービス情報基盤	★★サービス要件への対応 ～ 脆弱性スキャン、ペネトレーションテスト	※スマートホームサービス情報基盤に対するセキュリティ要件と同一の対策を実施すること。 ※要求事項の詳細は 6.2.1 節の SR3-SP-1～SR3-SP-13 を参照すること。	※スマートホーム情報基盤を参照		
SR3-PP-14	★★★	第三者サービス情報基盤	個人情報の消去	・収集した個人情報は不要にとなった時点、あるいはサービス事業者より削除要請を受けた際に削除可能な機能を実装すること。	＝ UK8	◎	＝ CPS.GV-2 CPS.IP-6
SR3-PP-15	★★★	第三者サービス情報基盤	緊急通報時の現場担当者の認証	・提供サービスのユースケースに応じて、住宅に到着した現場担当者が正しい身分であるかどうかを認証する機能を有すること。	◎	◎	＝ CPS.AC-2 CPS.AC-3 CPS.AC-5 CPS.AC-9

6.2.3 ホームゲートウェイへのセキュリティ要求事項

ホームゲートウェイに対するセキュリティ要求事項を以下に示す。(エントリーポイント：EP⑤～EP⑥)

表 6-6 ホームゲートウェイに対するセキュリティ要求事項

No.	レベル	対象	項目	内容	UK	SB327	CPSF
SR2-H-1	★★	ホームゲートウェイ	共通要件への対応	・IoT 分野共通セキュリティガイドラインの共通要件★を満たしていること。	＝ UK1 UK6 UK13	＝ 1798.91.05	＝ CPS.IP-1 CPS.IP-6 CPS.PT-2
SR2-H-2	★★	ホームゲートウェイ	認証	・接続機器との相互認証を行う仕組みを有すること。	◎	◎	＝ CPS.AC-3 CPS.AC-9
SR2-H-3	★★	ホームゲートウェイ	相互認証に必要な情報の管理	・相互認証に必要な情報が漏洩しないような仕組みを実装すること。	◎	◎	○ CPS.AC-3 CPS.AC-9
SR2-H-4	★★	ホームゲートウェイ	機器の稼働監視、障害監視	以下事項について、サービス対応機器群を対象とした稼働監視、障害監視を行うこと。 1）機器の死活管理 2）不正な機器の接続	○ UK10	◎	＝ CPS.DS-7 CPS.CM-2 CPS.CM-3

SR2-H-5	★★	ホームゲートウェイ	USB 接続端子の対策	・USB 接続端子（ポート）は、不用意な接続によるリスクの軽減策として、運用担当者以外が使用しにくい状態とするよう対策を行うこと。またサービス上、不要な USB 接続端子については、実装を行わないこと。 例） USB 接続端子について物理的なカバーを用いて対策を行う　…など	◎	◎	○ CPS.PT-2
SR2-H-6	★★	ホームゲートウェイ	報告された脆弱性に対する更新ソフトウェアの提供	・使用している OS、boot プログラム、アプリケーションに脆弱性が報告された場合には、テストを実施した上で、速やかに更新用ソフトウェアの提供を行うこと。	＝ UK3	◎	＝ CPS.DS-7 CPS.MA-1
SR3-H-1	★★★	ホームゲートウェイ	★★サービス要件への対応	・★★サービスの同機器に対するセキュリティ要求事項を満たしていること	※★★参照		
SR3-H-2	★★★	ホームゲートウェイ	外部インターネットからの不正アクセス防止	・外部インターネットからのアクセスに対して、不正アクセスを防止する機能を有すること。 例）ファイアウォールによる防御機能	◎	◎	○ CPS.PT-3
SR3-H-3	★★★	ホームゲートウェイ	Web アプリケーションの脆弱性を悪用した攻撃対策	・Web アプリケーションや WebAPI を使用した設定・動作の管理機能が実装されている場合や、サーバ機能を実装している場合には、下記ガイドラインに準拠した脆弱性対策を行うこと。 ※「安全なウェブサイトの作り方」[28]	○ UK13	◎	○ CPS.CM-3

SR3-H-4	★★★	ホームゲートウェイ	外部インターネットとの通信経路暗号化	・外部インターネットとの通信は、通信経路の暗号化を行うこと ※但し、★★サービスの要求事項 No.2「認証」において、認証付き暗号の実装が行われる場合は、通信経路暗号化の要求事項を同時に満たすものであるため、当該要求事項の対応は不要とする。 ※暗号技術については、以下を参考にガイドラインに準拠した実装とすること。 「SSL-TLS 暗号設定ガイドライン_V2.0」[22] 「電子政府における調達のために参照すべき暗号のリスト」[23]もしくは「CRYPTREC 暗号技術ガイドライン(軽量暗号)」[24]	○ UK5	◎	○ CPS.DS-3
SR3-H-5	★★★	ホームゲートウェイ	LAN 内接続機器との通信経路暗号化	・LAN 内接続機器との通信は、通信経路の暗号化を行うこと。 ※ホームゲートウェイと LAN 内の機器が、有線で接続される場合には、対象外とする。 ※但し、★★サービスの要求事項 No.2「認証」において、認証付き暗号の実装が行われる場合は、通信経路暗号化の要求事項を同時に満たすものであるため、当該要求事項の対応は不要とする。 ※暗号技術については、以下を参考にガイドラインに準拠した実装とすること。	○ UK5	◎	○ CPS.DS-3

				「SSL-TLS 暗号設定ガイドライン_V2.0」[22] 「電子政府における調達のために参照すべき暗号のリスト」[23]もしくは「CRYPTREC 暗号技術ガイドライン(軽量暗号)」[24]			
SR3-H-6	★★★	ホームゲートウェイ	データの暗号化	・保存された保護すべき資産に対する暗号化を行う。 ※保護すべき資産の対象については、本書 3.2 節、表 3-2 を参照とするものとする。 ※暗号化すべき資産については、サービスやユースケースを踏まえて重要度の高いものを対象とする。 ※暗号技術については、以下を参考にガイドラインに準拠した実装とすること。 「SSL-TLS 暗号設定ガイドライン_V2.0」[22] 「電子政府における調達のために参照すべき暗号のリスト」[23]もしくは「CRYPTREC 暗号技術ガイドライン(軽量暗号)」[24]	○ UK4 UK8	◎	○ CPS.DS-2
SR3-H-7	★★★	ホームゲートウェイ	鍵管理	・通信経路暗号化やデータの暗号化に用いる鍵の管理を適切に行うこと。 ※鍵管理の方法については、以下を参考にガイドラインに準拠した実装とすること。 「NIST SP (Special Publications) 800-57」	○ UK4	◎	○ CPS.DS-5

				[25] 「SSL/TLS 暗号設定ガイドライン改定及び鍵管理ガイドライン作成のための調査・検討－調査報告書－」[26]			
SR3-H-8	★★★	ホームゲートウェイ	ログ採取・分析	・アクセスログを蓄積し、インシデントが発生した際に、サービス情報基盤側での分析を可能とすること。	◎	◎	＝ CPS.MA-2
SR3-H-9	★★★	ホームゲートウェイ	脆弱性スキャン・ペネトレーションテストの実施	・新規製品の開発完了時および、ソフトウェアのバージョンアップ時には、脆弱性スキャン、ペネトレーションテストを実施し、脆弱性の有無をチェックすること。	◎	◎	○ CPS.CM-7

6.2.4 スマートホームサービス対応機器へのセキュリティ要求事項

スマートホームサービス対応機器に対するセキュリティ要求事項を以下に示す。(エントリーポイント：EP⑦～⑧)

表 6-7 スマートホームサービス対応機器に対するセキュリティ要求事項

No.	レベル	対象	項目	内容	UK	SB327	CPSF
SR2-D-1	★★	スマートホーム対応機器群	共通要件への対応	・IoT 分野共通セキュリティガイドラインの共通要件★を満たしていること	＝ UK1 UK6 UK13	＝ 1798.91.05	＝ CPS.IP-1 CPS.IP-6 CPS.PT-2
SR2-D-2	★★	スマートホーム対応機器群	認証	・接続機器との相互認証を行う仕組みを有すること。	◎	◎	＝ CPS.AC-3 CPS.AC-9
SR2-D-3	★★	スマートホーム対応機器群	相互認証に必要な情報の管理	・相互認証に必要な情報が漏洩しないような仕組みを実装すること。	◎	◎	＝ CPS.AC-3 CPS.AC-9

SR2-D-4	★★	スマートホーム対応機器群	USB 接続端子の対策	・USB 接続端子（ポート）は、不用意な接続によるリスクの軽減策として、運用担当者以外が使用しにくい状態とするよう対策を行うこと。またサービス上、不要な USB 接続端子については、実装を行わないこと。 例） USB 接続端子について物理的なカバーを用いて対策を行う　…など	◎	◎	○ CPS.PT-2
SR2-D-5	★★	スマートホーム対応機器群	報告された脆弱性に対する更新ソフトウェアの提供	・機器のソフトウェアやファームウェアに脆弱性が報告された場合には、テストを実施した上で、速やかに更新用ソフトウェアの提供を行うこと。	＝ UK3	◎	＝ CPS.DS-7 CPS.MA-1
SR3-D-1	★★★	スマートホーム対応機器群	★★サービス要件への対応	・★★サービスの同機器に対するセキュリティ要求事項を満たしていること。	※★★参照		

SR3-D-2	★★★	スマートホーム対応機器群	LAN 内接続機器との通信経路暗号化	・LAN 内接続機器との通信は、通信経路の暗号化を行うこと。 ※有線で接続される場合は、当該要求事項の対応は不要とする。 ※但し、★★サービスの要求事項 No.2「認証」において、認証付き暗号の実装が行われる場合は、通信経路暗号化の要求事項を同時に満たすものであるため、当該要求事項の対応は不要とする。 ※暗号技術については、以下を参考にガイドラインに準拠した実装とすること。 「SSL-TLS 暗号設定ガイドライン_V2.0」[22] 「電子政府における調達のために参照すべき暗号のリスト」[23]もしくは「CRYPTREC 暗号技術ガイドライン(軽量暗号)」[24]	○ UK5	◎	○ CPS.DS-3
SR3-D-3	★★★	スマートホーム対応機器群	鍵管理	・通信経路暗号に用いる鍵の管理を適切に行うこと。	＝ UK4	◎	＝ CPS.DS-5
SR3-D-4	★★★	スマートホーム対応機器群	可用性に考慮した通信 I/F	ホームゲートウェイとの接続方法は、提供サービスに応じて可用性に考慮した実装を選択すること。	◎	◎	＝ CPS.DS-7
SR3-D-5	★★★	スマートホーム対応機器群	脆弱性スキャン・ペネトレーションテストの実施	・新規製品の開発完了時および、ソフトウェアのバージョンアップ時には、脆弱性スキャン、ペネトレーションテストを実施し、脆弱性の有無をチェックすること。	◎	◎	○ CPS.CM-7

6.2.5 スマートフォンアプリへのセキュリティ要求事項

スマートフォンアプリに対するセキュリティに対するセキュリティ要求事項を以下に示す。（エントリーポイント：EP⑨～EP⑩）

※現時点では、該当要求事項は★★のみ。

表 6-8 スマートフォンアプリに対するセキュリティ要求事項

No.	レベル	対象	項目	内容	UK	SB327	CPSF
SR2-A-1	★★	スマートフォンアプリ	利用者の認証	・アプリケーション利用時に多要素認証によるセキュリティ対策を行うこと。	◎	◎	＝ CPS.AC-3 CPS.AC-9
SR2-A-2	★★	スマートフォンアプリ	セキュア設計・コーディング	・下記のガイドラインに準拠し、セキュリティを考慮した設計、コーディングを行うこと。 ※「Android アプリのセキュア設計・セキュアコーディングガイド」[27]	◎	◎	＝ CPS.RA-4
SR2-A-3	★★	スマートフォンアプリ	スマートフォンアプリのアップデート	・スマートフォンアプリに影響のあるセキュリティホールや不具合が確認された場合には、速やかにアップデートソフトウェアのリリースを行うこと	＝ UK3	◎	＝ CPS.DS-7 CPS.MA-1

7 まとめ

本ガイドラインでは、一般的なスマートホームのシステムモデルと、その脅威と対策を検討する例としてユースケースを提示した。その後、スマートホーム向け製品・サービスの分類と、スマートホームの特徴がセキュリティに及ぼす影響を考察して、ユースケースに対する脅威と対策の分析・評価を行った。また、スマートホームサービスとスマートホーム（住宅）を対象に、開発ライフサイクルにおけるセキュリティ対策をまとめた。そして、最後にスマートホームのサービスや、システム・機器に求められるセキュリティ対策を整理し、セキュリティ要件、要求事項として提示を行った。

今後、スマートホームが普及して、スマートホーム向け製品・サービスが増加することが見込まれるが、その企画・設計・開発に本ガイドラインが適切な対策を取る一助となれば幸いである。

また、本ガイドラインで示したスマートホーム独自方式によるリスク値の計算では、生命・財産への影響と取り扱う情報の重要度を考慮したが、それ以外のスマートホーム特有のセキュリティ特性を取り込む必要があるか今後の検討が必要である。また、本ガイドラインで示したリスク分析・評価の手順は実施に時間がかかる課題があり、今後の改良が必要である。

今後は、それらの課題への対応を含めて、内容の更なる充実化を図るだけでなく、新しいスマートホーム向け製品・サービスへの対応や、新しい攻撃手法への対応など、時代の変化に応じたガイドラインの改訂も行いたい。

本書はスマートホーム分野を対象としたセキュリティガイドラインとして作成したが、想定される脅威やライフサイクルにおけるセキュリティの取組みなど、他の分野でも応用できるところがあると考えられる。様々な製品・サービスの開発プロセスにおいてセキュリティ対策を考慮するにあたり、本ガイドラインを積極的に活用して欲しい。

引用/参考文献

[1] カリフォルニア州「SB-327 Information privacy: connected devices.」
http://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180SB327

[2] IoT セキュリティガイドライン、IoT 推進コンソーシアム・総務省・経済産業省
http://www.meti.go.jp/press/2016/07/20160705002/20160705002-1.pdf

[3] 平成 28 年版情報通信白書 第 1 部 第 2 章 第 1 節 1 p.80、総務省
http://www.soumu.go.jp/johotsusintokei/whitepaper/ja/h28/pdf/n2100000.pdf

[4] つながる世界の開発指針　～安全安心な IoT の実現に向けて開発者に認識してほしい重要ポイント～、独立行政法人情報処理推進機構　技術本部　ソフトウェア高信頼化センター
https://www.ipa.go.jp/files/000051411.pdf

[5] IoT 分野共通セキュリティ要件ガイドライン 2018 年度版（案）、CCDS 共通要件検討 WG
https://www.ccds.or.jp/public/document/other/IoT 分野共通セキュリティ要件ガイドライン 2018 年度版（案）.pdf

[6] IoT 開発におけるセキュリティ設計の手引き、IPA
https://www.ipa.go.jp/security/iot/iotguide.html

[7]「別表第八 電気用品安全法施行令（昭和三十七年政令第三百二十四号）別表第一第六号から第九号まで及び別表第二第七号から第十一号までに掲げる交流用電気機械器具並びに携帯発電機」
http://www.meti.go.jp/policy/consumer/seian/denan/kaishaku/gijutsukijunkaishaku/beppyoudai8.pdf

[8]「国際標準化の新規開発提案が承認される」、国立研究開発法人産業技術総合研究所
https://www.aist.go.jp/aist_j/news/nr20180330.html

[9] 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 2 版）、総務省
http://www.soumu.go.jp/menu_news/s-news/01cyber01_02000001_00001.html

[10] 製品分野別セキュリティガイドライン IoT-GW 編 Ver.2.0、CCDS セキュリティガイドライン WG ホーム GW SWG
https://www.ccds.or.jp/public/document/other/CCDS 製品分野別セキュリティガイドライン_IoT-GW 編_Ver2.0.pdf

[11] STRIDE：Microsoft が提唱する脅威の分類手法
https://docs.microsoft.com/ja-jp/azure/security/azure-security-threat-modeling-tool-threats

[12] 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、CCDS セキュリティ技術ワーキンググループ
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

[13] インシデントとは、JPCERT/CC
https://www.jpcert.or.jp/aboutincident.html

[14] つながる世界の開発指針第 2 版、IPA
https://www.ipa.go.jp/sec/reports/20170630.html

[15] IoT セキュリティ評価検証ガイドライン Rev1.0、CCDS
https://www.ccds.or.jp/public/document/other/guidelines/CCDS_IoT セキュリティ評価検証ガイドライン_rev1.0.pdf

[16] Common Vulnerability Scoring System v3.0: Specification Document, FIRST (the Forum of Incident Response and Security Teams)
https://www.first.org/cvss/specification-document

[17] 共通脆弱性評価システム CVSS v3 概説、IPA
https://www.ipa.go.jp/security/vuln/CVSSv3.html

[18] IoT Security & Privacy Trust Framework v2.5、OTA
https://www.internetsociety.org/wp-content/uploads/2018/05/iot_trust_framework2.5a_Japanese.pdf

[19] Top 10 IoT Vulnerabilities (2014)、OWASP
https://www.owasp.org/index.php/Top_10_IoT_Vulnerabilities_(2014)

[20] サイバー・フィジカル・セキュリティ対策フレームワーク Version1.0、経済産業省

https://www.meti.go.jp/press/2019/04/20190418002/20190418002-2.pdf

[21] Code of Practice for Consumer IoT Security、GOV.UK

https://www.gov.uk/government/publications/code-of-practice-for-consumer-iot-security

[22] SSL-TLS 暗号設定ガイドライン Ver2.0、IPA

https://www.ipa.go.jp/security/ipg/documents/ipa-cryptrec-gl-3001-2.0.pdf

[23] 電子政府における調達のために参照すべき暗号のリスト、CRYPTREC

https://www.cryptrec.go.jp/list/cryptrec-ls-0001-2012r4.pdf

[24] CRYPTREC 暗号技術ガイドライン(軽量暗号)、CRYPTREC

https://www.cryptrec.go.jp/report/cryptrec-gl-2003-2016jp.pdf

[25] NIST SP800-57 Part1 鍵管理における推奨事項（第一部：一般事項）、アメリカ国立標準技術研究所（NIST）※翻訳：IPA

https://www.ipa.go.jp/files/000055491.pdf

[26] SSL/TLS 暗号設定ガイドライン改定及び鍵管理ガイドライン作成のための調査・検討－調査報告書－、IPA

https://www.ipa.go.jp/files/000067459.pdf

[27] Android アプリのセキュア設計・セキュアコーディングガイド、JSSEC

https://www.jssec.org/dl/android_securecoding.pdf

[28] 安全なウェブサイトの作り方、IPA

https://www.ipa.go.jp/files/000017316.pdf

編著者（敬称略）

主　査　　積水ハウス株式会社

副　査　　株式会社 LIXIL

スマートホーム WG

株式会社アルファ
積水ホームテクノ株式会社
日本システムウエア株式会社
文化シヤッター株式会社
リンナイ株式会社
株式会社マストトップ

ガイドライン監修委員会

委員長　一般社団法人 重要生活機器連携セキュリティ協議会　代表理事
荻野 司

委員　　北陸先端科学技術大学院大学　先端科学技術研究科　教授
丹　康雄

横浜国立大学 大学院環境情報研究院/先端科学高等研究院 准教授
吉岡 克成