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

令和元年10月29日

CCDS スマートホームWG

目次構成

1.1 スマートホーム分野における現状と課題

・スマートホーム分野は業界自体が黎明期にあり、明確なセキュリティ対策が存在していない。セキュリティガイドラインの策定にあたっては、スマートホームが利用されるユースケースを踏まえ、**生命や財産に対する影響を考慮した検討**や、**利用者が安心・安全にサービスを利用できるような具体的なセキュリティ対策案の提示**が必要となる。

・本書では、下記の関連ガイドラインを参考に、**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。**
- IoT推進コンソーシアム、「IoTセキュリティガイドライン」
- 経済産業省、「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）」
- 英国「Code of Practice for consumer IoT security」
- 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)

1.2 ガイドラインの対象範囲

・本書では、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）、住設機器を対象とする。

1.3 本書の対象者

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

・ガイドライン内にて使用する用語、略称を表1-1,1-2に整理

2.1 スマートホームサービスの定義

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ため、本ガイドラインではサービスを定義し、ユースケースの検証を行った。

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。

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。

2.1 スマートホームサービスの定義

■本書におけるサービス・システムの定義

①サービス

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

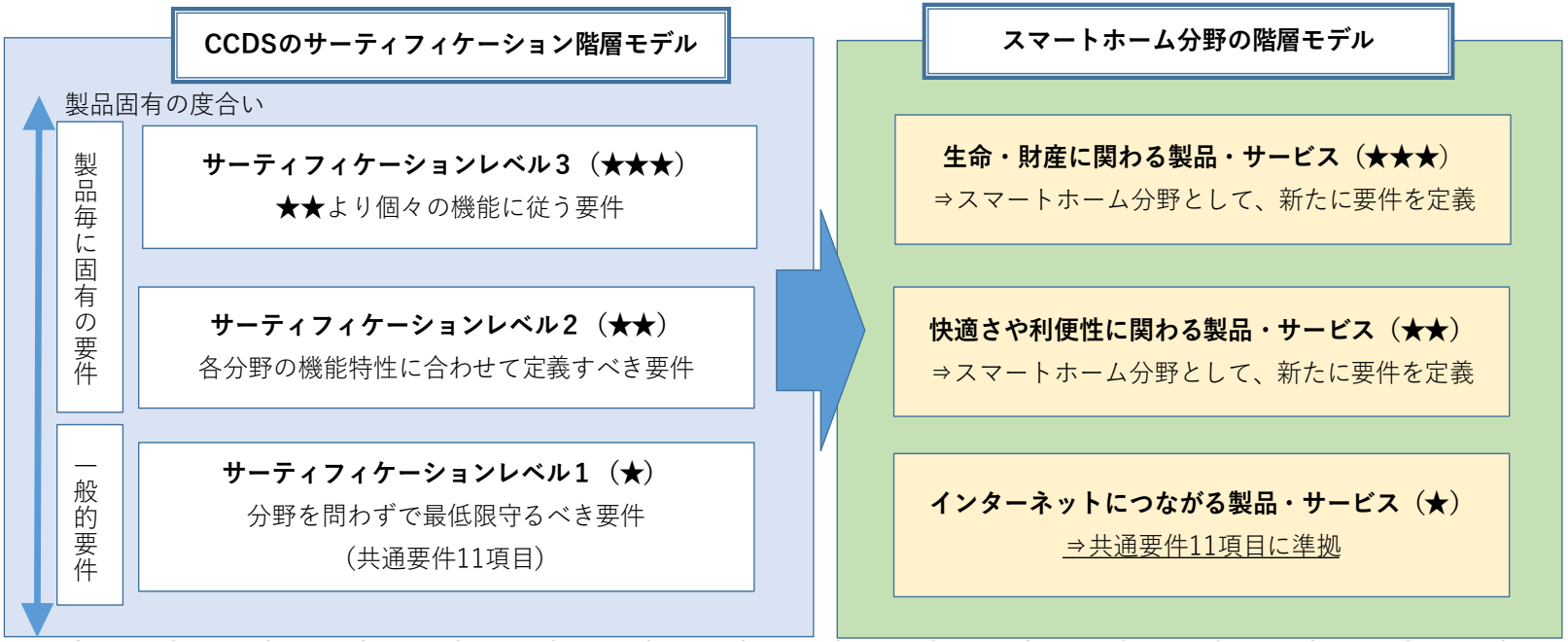
②システム

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

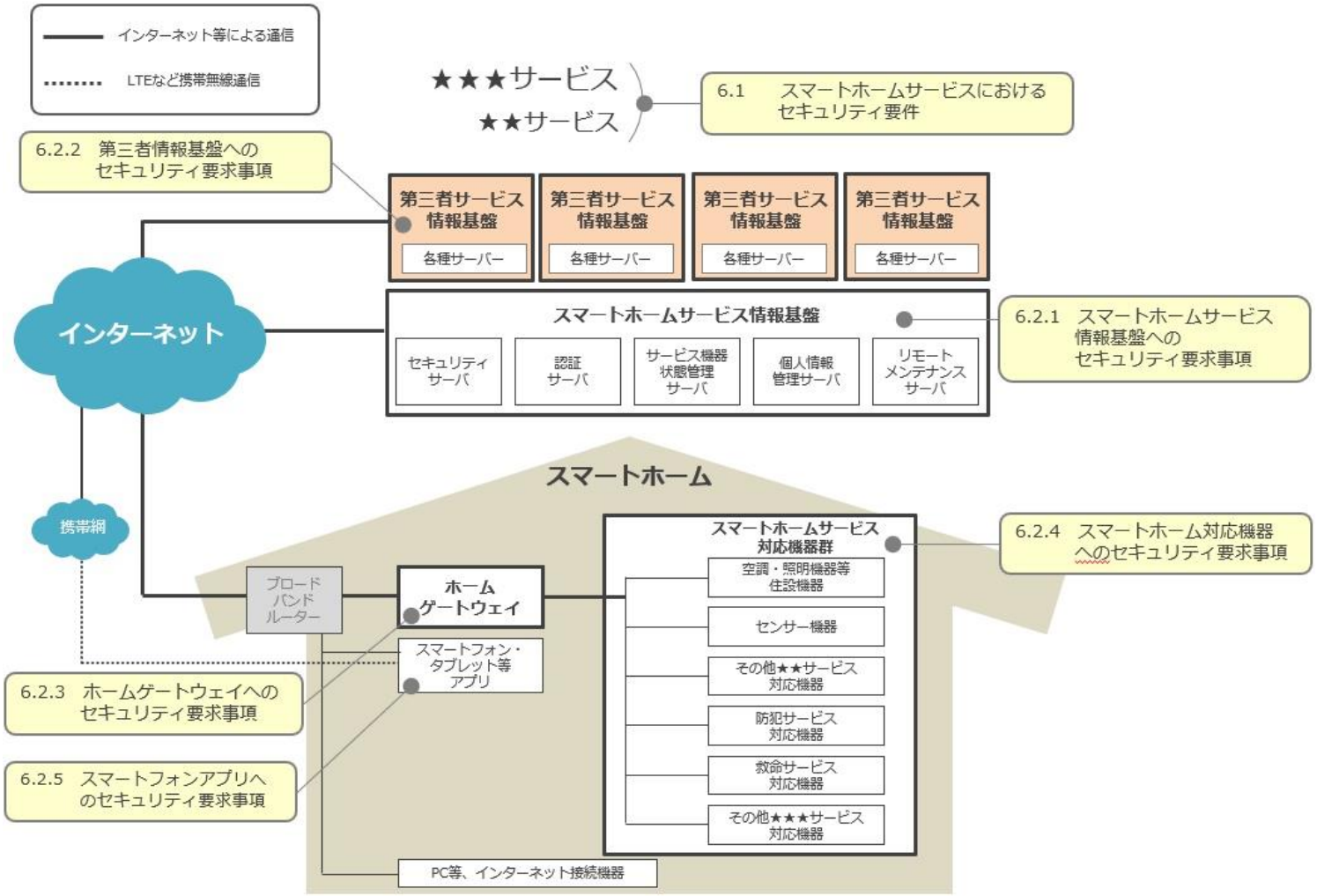
・サーティフィケーションのレベル階層の考え方はCCDSのサーティフィケーション階層モデルを踏襲。

・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、
★★・★★★サービスに対するセキュリティ対策方針やセキュリティ要件を検討。



2.3 システムモデルの定義

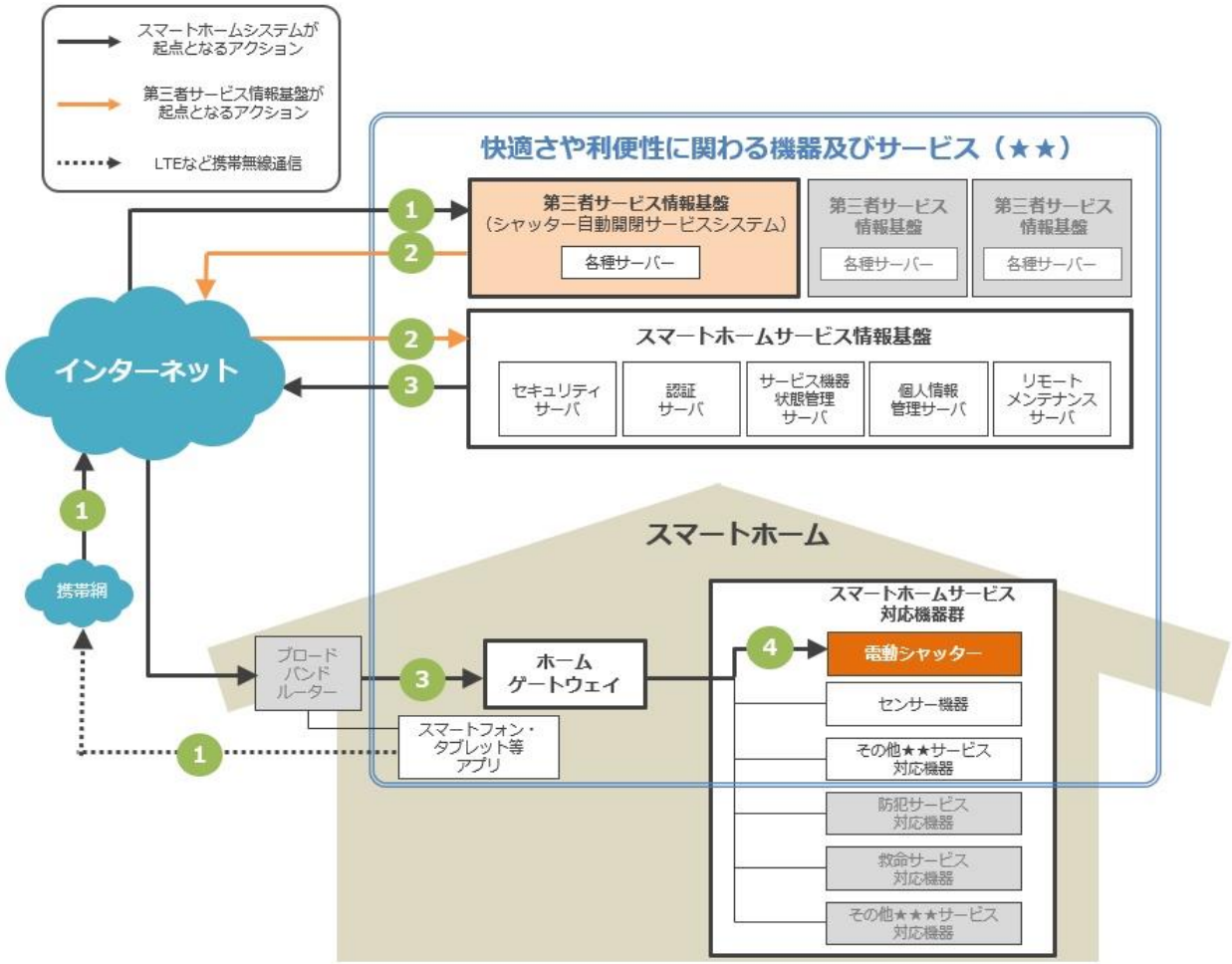
本書における各サービスのシステムモデル及び、セキュリティ要件/要求事項の　対応を以下の図にて示す。（節、項の番号はガイドライン本書に準拠）



2.4 ユースケースの定義

本書における★★サービスの事例として「シャッター自動開閉サービス」のユースケースを以下に示す。

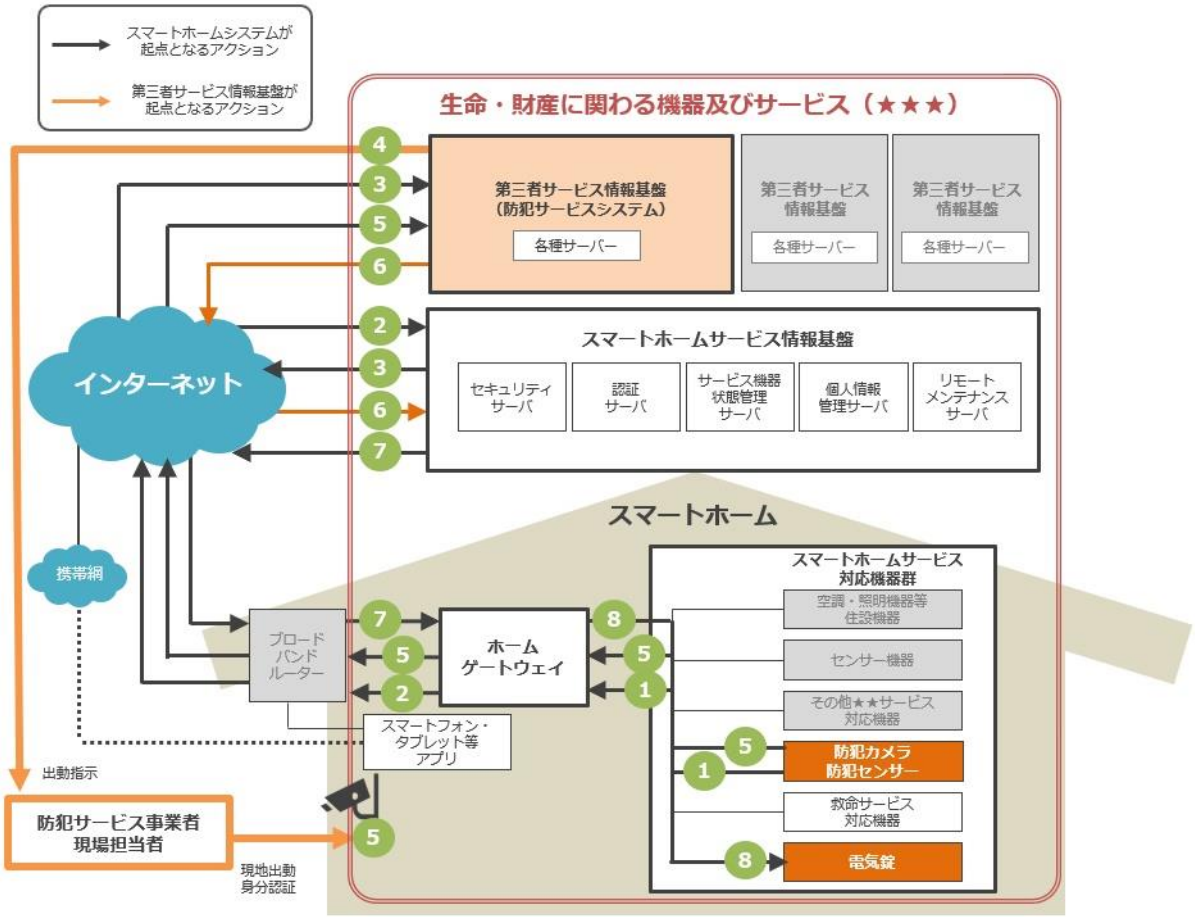
No	アクション
1	**開閉スケジュールの設定** 利用者が操作するアプリから電動シャッターの開閉スケジュールが設定されると、シャッター自動開閉サービスシステムに利用者と紐づけてその内容が登録される。
2	**電動シャッター開閉の指示** シャッター自動開閉サービスシステムは、指定された時刻になると、スマートホームサービス情報基盤に電動シャッターの開閉を指示する。
3	**電動シャッター開閉の実行** 電動シャッターの開閉を指示されたスマートホームサービス情報基盤は、電動シャッターの開閉を当該住宅のホームゲートウェイに指示する。
4	**電動シャッターの開閉操作** ホームゲートウェイは、電動シャッターの開閉を行う。



2章 スマートホームサービスの定義とシステム構成（5）

No	アクション
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い、スマートホーム情報基盤へ解錠を指示する。
7	**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。

本書における★★★サービスの事例として「駆け付け防犯サービス」のユースケースを以下に示す。



3.1 リスク分析・評価の手順

・リスク分析・評価では、以下の手順にて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。

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

・本書のユースケースにおける保護すべき資産について、下記の通り抽出を行った。

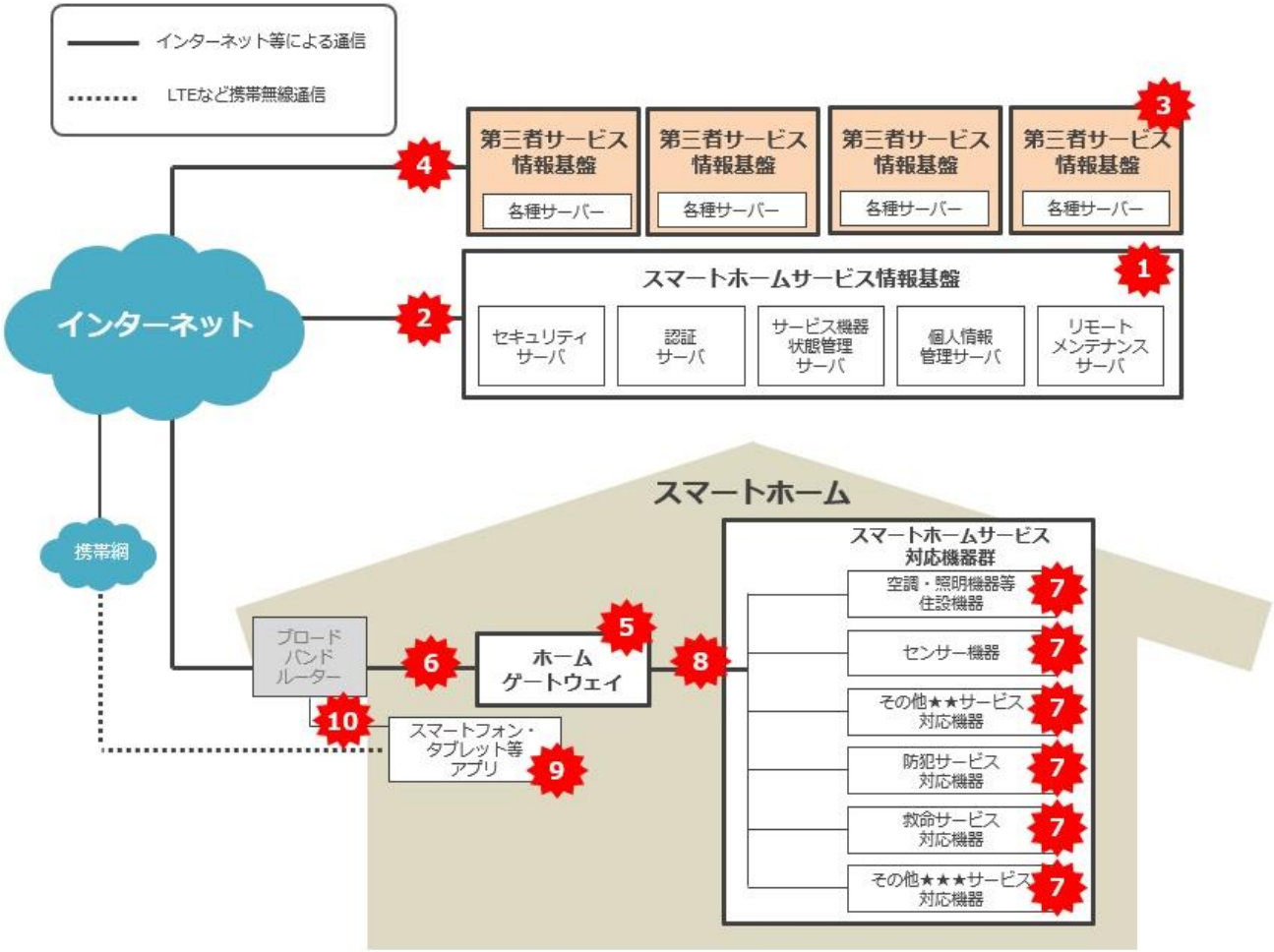
エントリーポイント	機器名	資産種別	保護すべき資産
スマートホーム サービス情報基盤	セキュリティサーバ	一次資産	ハードウェア、ソフトウェア（セキュリティ機能それ自体）
			設定情報、ログ情報
	認証サーバ	一次資産	ハードウェア、ソフトウェア（機能それ自体）
		二次資産	認証情報
			暗号鍵
	サービス機器状態管理サーバ	一次資産	ハードウェア、ソフトウェア（機能それ自体）
			機器の状態管理情報
	個人情報管理サーバ	一次資産	ハードウェア、ソフトウェア（機能それ自体）
			個人情報（利用者の氏名、住所、電話番号等）
	リモートメンテナンスサーバ	一次資産	ハードウェア、ソフトウェア（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

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 サービス対応機器群	空調・照明機器	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
		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★2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

3.3 想定される脅威の分析

・２章で定義した★★・★★★サービスのユースケースを事例として、システムモデルにおいて脅威分析を実施。

※システムモデル上の機器や通信経路において、攻撃の可能性がある箇所（エントリーポイント）に、赤い印を付け、それぞれ番号を記載。
各番号における具体的な想定脅威は次ページに記載。



3章 スマートホーム向け製品・サービスのリスク分析（4）

・システムモデルにおいて抽出した各エントリーポイントにおける想定脅威を以下に示す。

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

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番号	STRIDE＋CCDSモデルによる脅威分類
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

3.4 想定される脅威の詳細分析

・上記結果をもとに、各エントリーポイントに対する詳細な脅威分析を実施。
（分析結果は、ガイドライン本書を参照）

3.5 リスク値の計算

・サービスのユースケースに対する想定脅威の深刻度を数値化する手法として、本書ではCVSSv3に基づき、リスク値の算出を行ったが、スマートホーム分野に適用する際には、下記の課題がある。

– 課題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

– 課題②：生命・財産への影響をリスク計算結果に反映できない

・本書では、上記課題への対応として、
「情報の重要度(II)」と「生命・財産への影響（LP）」というリスクファクターを追加し、独自の算出方式を定義している。

3.5 リスク値の計算

情報の重要度（II）の計算値

項目	内容	値
高（H）	以下に示した重要な情報が含まれる。 ①　個人情報保護法（第二条）に定められた個人情報 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

生命・財産への影響（LP）の計算値

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

■スマートホーム独自方式でのリスク値計算の結果

・スマートホーム分野独自の算出方式を使用した結果、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。以下がその結果となる。

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	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

3.6 リスク分析・評価のまとめ

・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。
また、スマートホーム独自方式の適用により、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

・セキュリティ対策の検討に向けて、スマートホーム独自方式を使用し、シャッター自動開閉サービス（★★）と防犯駆けつけサービス（★★★）の想定脅威に対して、それぞれリスク対策後の評価を行い、改善後の数値算定を実施した。

（リスク値の計算結果については、ガイドライン本書を参照）

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

- 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。

⇒ 個々のIoT機器とサービスの観点に分けて、セキュリティ対策を検討。

4.2 製品安全（セーフティ）への対応

- 電気用品安全法（電安法）
- 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）
- 製造物責任法（PL法）や消費生活用製品安全法（消安法）

⇒ 「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」などの原則を遵守する。

4.3 機器の連携

– IoTは連携先の機器のセキュリティ対策の水準が不透明であり、複数の機器が連携する場合、対策水準の低い機器が攻撃の入り口となりやすい。

⇒ 個別の機器に対して、それぞれにセキュリティ要求事項を示す。

4.4 利用者によるIoT機器の設置・撤去

– 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。

⇒ 個別の機器の対策状況をサーティフィケーションマーク取得により担保。

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

– 上記のスマートホーム分野の特徴を踏まえ、セキュリティ対策指針のポイントを整理

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

・**サービス事業者を対象としたスマートホームサービス**の開発ライフサイクルを「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　に分類を行った。

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

・３章のリスク分析・評価結果を踏まえて各フェーズにおけるセキュリティ対策方針を定義。

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

・**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）のライフサイクルを「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　に分類を行った。

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

・３章のリスク分析・評価結果を踏まえて各フェーズにおけるセキュリティ対策方針を定義。

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

・これまでに検討を行ったセキュリティ対策の取り組みを踏まえ、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。

・★★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。

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）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。

・セキュリティ要件は、英国の「Code of Practice for consumer IoT security」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)についても準拠した対策となる。

■補足）本書におけるセキュリティ要件（要求事項）の選定プロセス

① ★★、★★★のユースケースにおけるリスク分析・評価を行い、想定される脅威の抽出とリスク評価値の算出を実施。

② CCDS、IPAの関連ガイドラインや、CPSFをもとに想定脅威に対する対策候補を要件案として列挙。

③ 列挙した要件案に対して、機器・システムベンダーに精査いただき、コストや技術面を踏まえた対応可否や、要件の過不足を検討。
（リスク分析結果をもとに、セキュリティ品質に支障を生じない範囲で、対応が現実的ではない要件の除外、追加の必要がある要件を追加）

④ 英国の「Code of Practice for consumer IoT security」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)を参考に、要件（要求事項）の対応状況のチェックを実施。

■セキュリティ要件における関連ガイドラインとの対応の前提
※P.30以降の要求事項についても同様の前提となる。

①下記３種の関連ガイドラインとの対応関係を示している。

略称	ガイドライン文書名
UK	英国「Code of Practice for consumer IoT security」
SB327	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)
CPSF	「サイバー・フィジカル・セキュリティ対策フレームワーク」

②各要件、要求事項の対応状況については、下記の記号により対応関係を示している。

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。

6章 スマートホームサービスのセキュリティ要件（4）

スマートホームサービスにおけるセキュリティ要件（★★）：９項目

No.	項目	内容	UK	SB 327	CP SF
R2-1	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	◎	◎	○
R2-2	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（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。	◎	◎	＝
R2-3	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。	＝	◎	＝
R2-4	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。	＝	◎	＝
R2-5	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。	＝	◎	◎
R2-6	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。	＝	◎	◎

次ページに続く→

6章 スマートホームサービスのセキュリティ要件（5）

No.	項目	内容	UK	SB 327	CP SF
R2-7	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（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。			
R2-8	更新ソフトウェアの運用手順及びバージョン管理	・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。	＝	◎	○
		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	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。			

6章 スマートホームサービスのセキュリティ要件（6）

スマートホームサービスにおけるセキュリティ要件（★★★）：８項目

No.	項目	内容	UK	SB 327	CP SF
R3-1	★★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	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。			
R3-3	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（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。			
R3-4	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			
R3-5	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。	＝	◎	＝
R3-6	脆弱性の有無のチェック	・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。	◎	◎	○
R3-7	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。	◎	◎	＝
R3-8	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。			

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

・これまでに検討を行ったセキュリティ対策の取り組みを踏まえ、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。

・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、リスク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の選定基準は、セキュリティ要件と同様となる。

・セキュリティ要求事項は、英国の「Code of Practice for consumer IoT security」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)」についても準拠した対策となる。

6章 スマートホームサービスのセキュリティ要件（8）

スマートホームサービス情報基盤におけるセキュリティ要求事項（★★）：７項目

No.	項目	内容	UK	SB 327	CP SF
SR2-SP-1	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。	＝	＝	＝
SR2-SP-2	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。	◎	◎	○
SR2-SP-3	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。	◎	◎	＝
SR2-SP-4	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。	◎	◎	＝
SR2-SP-5	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。	◎	◎	＝
SR2-SP-6	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。	◎	◎	＝
SR2-SP-7	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。	＝	◎	＝

6章 スマートホームサービスのセキュリティ要件（9）

スマートホームサービス情報基盤におけるセキュリティ要求事項（★★★）：１３項目

No.	項目	内容	UK	SB 327	CP SF
SR3-SP-1	★★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	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	◎	◎	○
SR3-SP-3	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]	○	◎	○
SR3-SP-4	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。	○	◎	＝
SR3-SP-5	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。	＝	◎	○
SR3-SP-6	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。	○	◎	＝
SR3-SP-7	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。	◎	◎	○
SR3-SP-8	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	○	◎	○

次ページに続く→

6章 スマートホームサービスのセキュリティ要件（10）

スマートホームサービス情報基盤におけるセキュリティ要求事項（★★★）

No.	項目	内容	UK	SB 327	CP SF
SR3-SP-9	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	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]	○	◎	○
SR3-SP-11	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]	○	◎	○
SR3-SP-12	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。	◎	◎	＝
SR3-SP-13	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。	◎	◎	○

6章 スマートホームサービスのセキュリティ要件（11）

第三者サービス情報基盤におけるセキュリティ要求事項

★★：7項目、　★★★：１５項目

No.	レベル	項目	内容	UK	SB 327	CP SF
SR2-PP-1 ～ SR2-PP-7	★★	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	★★★	★★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	★★★	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。	＝	◎	＝
SR3-PP-15	★★★	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。	◎	◎	＝

6章 スマートホームサービスのセキュリティ要件（12）

ホームゲートウェイにおけるセキュリティ要求事項（★★）：６項目

No.	項目	内容	UK	SB 327	CP SF
SR2-H-1	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。	＝	＝	＝
SR2-H-2	認証	・接続機器との相互認証を行う仕組みを有すること。	◎	◎	＝
SR2-H-3	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。	◎	◎	○
SR2-H-4	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	○	◎	＝
SR2-H-5	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	◎	◎	○
SR2-H-6	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。	＝	◎	＝

6章 スマートホームサービスのセキュリティ要件（13）

ホームゲートウェイにおけるセキュリティ要求事項（★★★）：９項目

No.	項目	内容	UK	SB327	CPSF
SR3-H-1	★★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	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	◎	◎	○
SR3-H-3	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]	○	◎	○
SR3-H-4	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]	○	◎	○
SR3-H-5	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。 「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]	○	◎	○

次ページに続く→

6章 スマートホームサービスのセキュリティ要件（14）

ホームゲートウェイにおけるセキュリティ要求事項（★★★）

No.	項目	内容	UK	SB 327	CP SF
SR3-H-6	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]	○	◎	○
SR3-H-7	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]	○	◎	○
SR3-H-8	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。	◎	◎	＝
SR3-H-9	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。	◎	◎	○

6章 スマートホームサービスのセキュリティ要件（15）

スマートホーム対応機器におけるセキュリティ要求事項（★★）：５項目

No.	項目	内容	UK	SB 327	CP SF
SR2-D-1	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	＝	＝	＝
SR2-D-2	認証	・接続機器との相互認証を行う仕組みを有すること。	◎	◎	＝
SR2-D-3	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。	◎	◎	＝
SR2-D-4	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	◎	◎	○
SR2-D-5	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。	＝	◎	＝

6章 スマートホームサービスのセキュリティ要件（16）

スマートホーム対応機器におけるセキュリティ要求事項（★★★）：５項目

No.	項目	内容	UK	SB 327	CP SF
SR3-D-1	★★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	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]	○	◎	○
SR3-D-3	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。	＝	◎	＝
SR3-D-4	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。	◎	◎	＝
SR3-D-5	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。	◎	◎	○

6章 スマートホームサービスのセキュリティ要件（17）

スマートフォンアプリにおけるセキュリティ要求事項（★★）：３項目

No.	項目	内容	UK	SB327	CPSF
SR2-A-1	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。	◎	◎	＝
SR2-A-2	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]	◎	◎	＝
SR2-A-3	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	＝	◎	＝

※★★★に該当する要求事項なし。

7章 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。

・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。

Appedix

・本ガイドラインでは、IoTセキュリティに関連する下記ガイドラインとの対比を整理している。

（詳細はガイドライン本書を参照）

- 「IoTセキュリティガイドライン」、IoT推進コンソーシアム
- 「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)」、経済産業省
- 「Code of Practice for consumer IoT security」、英国
- 「接続される機器のセキュリティ法」(Senate Bill No.327　CHAPTER886)、米国 カリフォルニア州