CCDS-SH02-2021
CCDS-SH03-2021

製品分野別セキュリティガイドライン
スマートホーム編 Appendix

Ver. 1.0

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.1.0	2019/10/29	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。

目次

1　本書の位置づけ

本書はCCDS「製品分野別セキュリティガイドライン スマートホーム編」のAppendixとして、以下の関連ガイドラインとの対応関係を整理した文書となる。

表 1-1 本書との対応関係を整理した関連ガイドライン

章	ガイドライン文書名	発行元
2	IoTセキュリティガイドライン	IoT推進コンソーシアム
3	サイバー・フィジカル・セキュリティ対策フレームワーク（CPSF）	経済産業省
4	Code of Practice for Consumer IoT Security	英国
5	「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

2　「IoT セキュリティガイドライン」との関係

本書は IoT 推進コンソーシアムが公開している「IoT セキュリティガイドライン」を詳細化した内容になっている。「IoT セキュリティガイドライン」と本書の対応を表 2-1 に示す。

表 2-1 IoT セキュリティガイドラインと本書の対応

IoT セキュリティガイドライン			本書での対応箇所	
大項目		指針	章番号	概要
方針・管理	方針 1 IoT の性質を考慮した基本方針を定める	要点 1 経営者が IoT セキュリティにコミットする	5.2.1 サービス企画フェーズ	・No.1　企業としての対応方針の策定
		要点 2 内部不正やミスに備える	5.2.3 評価フェーズ	・No.1 施工時の認証情報、セキュリティ設定の確認 ・No.2 脆弱性の有無のチェック
			5.4.2 生産・施工フェーズ	・No.2　使用機器等の発注 ・No.3　使用機器の管理・監督
			5.4.3　アフターフェーズ	・No.2　運用時の使われ方の定義 ・No.5　提供物管理
			5.4.4　リフォームフェーズ	・No.1　既導入機器との互換性確認
			5.4.5　転売フェーズ	・No.1　提供物管理
			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	・R2-3　構成機器に対する適切な初期設定（IoT 機器間の認証情報とアクセス制御） ・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 ・R3-6　脆弱性の有無のチェック ・R3-8　サービス提供におけ

				るインシデント対応
分析	方針 2 IoT のリスクを認識する	要点 3 守るべきものを特定する	3.2　保護すべき資産の抽出	・保護すべき資産の抽出
			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	・R2-1、R3-2　リスク分析・評価、セキュリティ対策方針の策定
		要点 4 つながることによるリスクを想定する	3.3　想定される脅威の分析	・想定される脅威の分析
			3.5　リスク値の計算	・リスク値の計算
			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	・R2-1、R3-2　リスク分析・評価、セキュリティ対策方針の策定
		要点 5 つながりで波及するリスクを想定する	3.4　想定される脅威の詳細分析	・想定される脅威の詳細分析
			3.5　リスク値の計算	・リスク値の計算
			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	・R2-1、R3-2　リスク分析・評価、セキュリティ対策方針の策定
		要点 6 物理的なリスクを認識する	3.4　想定される脅威の詳細分析	・想定される脅威の詳細分析
			3.5　リスク値の計算	・リスク値の計算
			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	・R2-1、R3-2　リスク分析・評価、セキュリティ対策方針の策定

		要点 7 過去の事例に並ぶ	3.4　想定される脅威の詳細分析	・想定される脅威の詳細分析
			3.5　リスク値の計算	・リスク値の計算
設計	方針 3 守るべきものを守る設計を考える	要点 8 個々でも全体でも守れる設計をする	4.1.3　機器の連携	・機器の連携
			4.1.5　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	・スマートホームサービスにおけるセキュリティ対策指針の整理
			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	・R2-1、R3-2　リスク分析・評価、セキュリティ対策方針の策定 ・R2-2、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
		要点 9 つながる相手に迷惑をかけない設計をする	5.2.1　サービス企画フェーズ	・No.3　サービス要件やシステムモデル、ユースケースの定義 ・No.6　セキュリティ対策方針の策定
			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	・R2-1、R3-2　リスク分析・評価、セキュリティ対策方針の策定 ・R2-2、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
		要点 10 安全安心を実現する設計の整合性をとる	5.2.1　サービス企画フェーズ	・No.3　サービス要件やシステムモデル、ユースケースの定義 ・No.6　セキュリティ対策方針の策定
			5.4.1　設計	・No.3　設計図書への表記・

			フェーズ	指示
			5.4.2　生産・施工フェーズ	・No.4　施工確認
			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	・R2-1、R3-2　リスク分析・評価、セキュリティ対策方針の策定 ・R2-2、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
		要点 11 不特定の相手とつなげられても安全安心を確保できる設計をする	4.1.3　機器の連携	・機器の連携
			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	・R2-3　構成機器に対する適切な初期設定(IoT 機器間の認証情報とアクセス制御) ・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
		要点 12 安全安心を実現する設計の検証・評価を行う	3　スマートホームサービスのリスク分析	・スマートホームサービスのリスク分析
			5.2.3　評価フェーズ	・No.2　脆弱性の有無のチェック
			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	・R2-1、R3-2　リスク分析・評価、セキュリティ対策方針の策定 ・R3-6　脆弱性の有無のチェック
			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	・SR3-SP-13　脆弱性スキャン、ペネトレーションテスト
			6.2.2　第三者サービス情報基盤へのセキュリティ	・SR3-PP-13　脆弱性スキャン、ペネトレーションテスト

			要求事項	
			6.2.3　ホームゲートウェイへのセキュリティ要求事項	・SR3-H-9　脆弱性スキャン・ペネトレーションテストの実施
			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	・SR3-D-5　脆弱性スキャン・ペネトレーションテストの実施
構築	方針 4 ネットワーク上での対策を考える	要点 13 自身がどのような状態かを把握し、記録する機能を設ける	5.2.4　運用・保守フェーズ	・No.2　ログ収集・データ分析
		要点 14 機能及び用途に応じて適切にネットワークを接続する	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	・R2-2、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 ・R2-3　構成機器に対する適切な初期設定（IoT 機器間の認証情報とアクセス制御）
		要点 15 初期設定に留意する	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	・R2-3　構成機器に対する適切な初期設定（IoT 機器間の認証情報とアクセス制御）
		要点 16 認証機能を導入する	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	・R2-3　構成機器に対する適切な初期設定（IoT 機器間の認証情報とアクセス制御） ・R2-4　サービス契約者の本人認証 ・R3-7　各サービス担当者のアクセス管理
			6.2.1　スマートホームサービス情報基盤へのセキュ	・SR2-SP-2　API における認証 ・SR2-SP-3　管理画面（提供サービスの概要表示や機能管

			リティ要求事項	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 ・SR2-SP-4　サーバログイン時におけるユーザ認証の実施 ・SR2-SP-5　ホームゲートウェイの認証 ・SR2-SP-6　認証に必要な情報の管理
			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	・SR2-PP-2　API における認証 ・SR2-PP-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 ・SR2-PP-4　サーバログイン時におけるユーザ認証の実施 ・SR2-PP-5　ホームゲートウェイの認証 ・SR2-PP-6　認証に必要な情報の管理
			6.2.3　ホームゲートウェイへのセキュリティ要求事項	・SR2-H-2　認証 ・SR2-H-3　相互認証に必要な情報の管理
			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	・SR2-D-2　認証 ・SR2-D-3　相互認証に必要な情報の管理
			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	・SR2-A-1　利用者の認証

運用・保守	方針 5 情報発信・共有を行う	要点 17 出荷・リリース後も安全安心な状態を維持する	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	・R2-7 最新のソフトウェアへの定期的な更新 ・R2-8 更新ソフトウェアの運用手順及びバージョン管理
			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	・SR2-SP-7 セキュリティパッチの適用
			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	・SR2-PP-7 セキュリティパッチの適用
			6.2.3　ホームゲートウェイへのセキュリティ要求事項	・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
			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	・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
			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	・SR2-A-3　スマートフォンアプリのアップデート
		要点 18 出荷・リリース後も IoT リスクを把握し、関係者に守ってもらいたいことを伝える	5.4.2　生産・施工フェーズ	No.1　利用者同意 No.6　使用機器およびサービス利用方法の説明
			5.4.3　アフターフェーズ	・No.1　利用規約または取り扱い説明書の提供 ・No.2　運用時の使われ方の定義 ・No.3　ユーザへの注意喚起
			5.4.4　リフォームフェーズ	・No.2　機器廃棄方法の周知

			5.4.5　転売フェーズ	・No.2　機器廃棄方法の周知
			5.4.6　解体フェーズ	・No.1　機器廃棄方法の周知
			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	・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
		要点 19 つながることによるリスクを一般利用者に知ってもらう	5.4.3　アフターフェーズ	・No.1　利用規約または取り扱い説明書の提供 ・No.2　運用時の使われ方の定義 ・No.3　ユーザへの注意喚起
			5.4.4　リフォームフェーズ	・No.2　機器廃棄方法の周知
			5.4.5　転売フェーズ	・No.2　機器廃棄方法の周知
			5.4.6　解体フェーズ	・No.1　機器廃棄方法の周知
			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	・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
		要点 20 IoT システム・サービスにおける関係者の役割を認識する	5.2.1　サービス企画フェーズ	・No.3　サービス要件やシステムモデル、ユースケースの定義 ・No.6　セキュリティ対策方針の策定
			5.4.3　アフターフェーズ	・No.2　運用時の使われ方の定義
			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	・R2-1、R3-2　リスク分析・評価、セキュリティ対策方針の策定 ・R2-2、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 ・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
		要点 21 脆弱な機能を把握し、適切に注意喚起を行う	5.4.3　アフターフェーズ	・No.3　ユーザへの注意喚起 ・No.4　最新の脆弱性への対応 ・No.6　機器利用制限
			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	・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
一般利用者向け	ルール 1 問い合わせ窓口やサポートがない機器やサービスの購入・利用を控える		5.4.3　アフターフェーズ	・No.1　利用規約または取り扱い説明書の提供
	ルール 2 初期設定に気を付ける		5.4.3　アフターフェーズ	・No.1　利用規約または取り扱い説明書の提供 ・No.3　ユーザへの注意喚起
			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	・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
	ルール 3 使用しなくなった機器については電源を切る		5.4.3　アフターフェーズ	・No.6　機器利用制限
			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	・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
	ルール 4 機器を手放すときはデータを消す		5.4.4　リフォームフェーズ	・No.2　機器廃棄方法の周知
			5.4.5　転売フェーズ	・No.2　機器廃棄方法の周知
			5.4.6　解体	・No.1　機器廃棄方法の周知

		フェーズ	
		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	・R2-5　スマートホーム内で利用される個人情報の削除

3　「サイバー・フィジカル・セキュリティ対策フレームワーク」との関係

本書は経済産業省が公開している「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)」を参考に作成を行った。「サイバー・フィジカル・セキュリティ対策フレームワーク」と本書の対応を表 3-1 に示す。

表 3-1 サイバー・フィジカル・セキュリティ対策フレームワークと本書との対応

「サイバー・フィジカル・セキュリティ対策フレームワーク」			本書での対応箇所	
章番号	**対策要件 ID**	**対策要件**	**章番号**	**概要**
3.1.	CPS.AM	資産管理		
3.1.	CPS.AM-1	・システムを構成するハードウェア、ソフトウェア及びその管理情報(例：名称、バージョン、ネットワークアドレス、管理責任者、ライセンス情報)の一覧を作成し、適切に管理する。	5.4.2	生産・施工フェーズ No.2　使用機器等の発注 No.3　使用機器の管理・監督
3.1.	CPS.AM-2	・自組織が生産したモノのサプライチェーン上の重要性に応じて、トレーサビリティ確保のための特定方法を定める。	―	該当なし
3.1.	CPS.AM-3	・重要性に応じて、生産日時やその状態等について記録を作成し、一定期間保管するために生産活動の記録に関する内部規則を整備し、運用する。	―	該当なし

3.1.	CPS.AM-4	・組織内の通信ネットワーク構成図及び、データフロー図を作成し、適切に管理する。	5.2.1	サービス企画フェーズ No.4「リスク分析・評価とサービスレベルの定義」
3.1.	CPS.AM-5	・自組織の資産が接続している外部情報システムの一覧を作成し、適切に管理する。	5.2.1	サービス企画フェーズ No.4「リスク分析・評価とサービスレベルの定義」 No.6「セキュリティ対策方針の策定」
3.1.	CPS.AM-6	・リソース（例：モノ、データ、システム）を、機能、重要度、ビジネス上の価値に基づいて分類、優先順位付けし、管理責任を明確にした上で、業務上それらのリソースに関わる組織やヒトに伝達する。	3	スマートホーム向け製品・サービスのリスク分析
3.1.	CPS.AM-7	・自組織及び関係する他組織のサイバーセキュリティ上の役割と責任を定める。	5.2.1	サービス企画フェーズ No.6「セキュリティ対策方針の策定」
3.2.	CPS.BE	ビジネス環境		
3.2.	CPS.BE-1	・サプライチェーンにおいて、自組織が担う役割を特定し共有する。	5.2.1	サービス企画フェーズ No.6「セキュリティ対策方針の策定」
3.2.	CPS.BE-2	・あらかじめ定められた自組織の優先事業、優先業務と整合したセキュリティポリシー・対策基準を明確化し、自組織の取引に関係する者(サプライヤー、第三者プロバイダ等を含む)に共有する	5.2.2	設計・製造フェーズ No.2「開発及びソリューションの外部委託」

3.2.	CPS.BE-3	・自組織が事業を継続する上での自組織及び関係する他組織における依存関係と重要な機能を特定する。	5.2.1	サービス企画フェーズ No.4「リスク分析・評価とサービスレベルの定義」 No.6「セキュリティ対策方針の策定」
			5.2.2	設計・製造フェーズ No.2「開発及びソリューションの外部委託」
3.3.	CPS.GV	ガバナンス		
3.3.	CPS.GV-1	・セキュリティポリシーを策定し、自組織及び関係する他組織のセキュリティ上の役割と責任、情報の共有方法等を明確にする。	5.2.1	サービス企画フェーズ No.1　企業としての対応方針の策定
3.3.	CPS.GV-2	・個人情報保護法、不正競争防止法等の国内外の法令や、業界のガイドラインを考慮した社内ルールを策定する。	5.2.1	サービス企画フェーズ No.2「企業としてのプライバシポリシーの策定」 No.5「関連法令への対応検討」
			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 SR3-SP-12「収集データ最小化」
			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 SR3-PP-12「収集データ最小化」 SR3-PP-14「個人情報の消去」
3.3.	CPS.GV-3	・各種法令や関係組織間だけで共有するデータの扱いに関する取決め等によって要求されるデータの保護の水準を的確に把握し、それぞれの要求を踏まえたデータの区分方法を整備し、ライフサ	3	スマートホーム向け製品・サービスのリスク分析
			5	スマートホームサービスの開発フェーズとセキュリティへの取り組み

		イクル全体に渡って区分に応じた適切なデータの保護を行う。		
3.3.	CPS.GV-4	・セキュリティに関するリスク管理を適切に行うために戦略策定、リソース確保を行う。	5	スマートホームサービスの開発フェーズとセキュリティへの取り組み
3.4.	CPS.RA	リスク評価		
3.4.	CPS.RA-1	・自組織の資産の脆弱性を特定し、対応する資産とともに一覧を文書化する。	5.2.1	サービス企画フェーズ No.4「リスク分析・評価とサービスレベルの定義」
3.4.	CPS.RA-2	・セキュリティ対策組織(SOC/CSIRT)は、組織の内部及び外部の情報源(内部テスト、セキュリティ情報、セキュリティ研究者等)から脆弱性情報/脅威情報等を収集、分析し、対応及び活用するプロセスを確立する。	5.2.4	運用・保守フェーズ No.16「サービス対応機器に対するインシデント対応」
3.4.	CPS.RA-3	・自組織の資産に対して想定されるセキュリティインシデントと影響及びその発生要因を特定し、文書化する。	5.2.1	サービス企画フェーズ No.4「リスク分析・評価とサービスレベルの定義」
3.4.	CPS.RA-4	・構成要素の管理におけるセキュリティルールが、実装方法を含めて有効かを確認するため、定期的にリスクアセスメントを実施する。	―	該当なし

		・IoT 機器及び IoT 機器を含んだシステムの企画・設計の段階から、受容できない既知のセキュリティリスクの有無を、セーフティに関するハザードの観点も踏まえて確認する。	6.2.5	スマートフォンアプリに対するセキュリティ要求事項 SR2-A-2「セキュア設計・コーディング」
3.4.	CPS.RA-5	・リスクを判断する際に、脅威、脆弱性、可能性、影響を考慮する。	3	スマートホーム向け製品・サービスのリスク分析
3.4.	CPS.RA-6	・リスクアセスメントに基づき、発生し得るセキュリティリスクに対する対応策の内容を明確に定め、対応の範囲や優先順位を整理した結果を文書化する。	5.2.1	サービス企画フェーズ No.6「セキュリティ対策方針の策定」
		・IoT 機器及び IoT 機器を含んだシステムの企画・設計の段階におけるアセスメントにて判明したセキュリティ及び関連するセーフティのリスクに対して適宜対応する。	5.2.1	サービス企画フェーズ No.6「セキュリティ対策方針の策定」
3.5.	CPS.RM	リスク管理戦略		

3.5.	CPS.RM-1	・自組織内におけるセキュリティリスクマネジメントの実施状況について確認し、組織内の適切な関係者（例：上級管理職）に伝達する。また、自組織の事業に関係する自組織及び他組織（例：業務委託先）の責任範囲を明確化し、関係する他組織によるセキュリティリスクマネジメントの実施状況を確認するプロセスを確立し、実施する。	5.2.1	サービス企画フェーズ No.1「企業組織としての対応方針の策定」
3.5.	CPS.RM-2	・リスクアセスメント結果及びサプライチェーンにおける自組織の役割から自組織におけるリスク許容度を決定する。	5.2.1	サービス企画フェーズ No.4「リスク分析・評価とサービスレベルの定義」
3.6.	CPS.SC	サプライチェーンリスク管理		
3.6.	CPS.SC-1	・取引関係のライフサイクルを考慮してサプライチェーンに係るセキュリティの対策基準を定め、責任範囲を明確化したうえで、その内容について取引先と合意する。	5.2.2	設計・製造フェーズ No.2「開発及びソリューションの外部委託」
			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 R2-2、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」
3.6.	CPS.SC-2	・自組織の事業を継続するに当たり、三層構造の各層において重要な役割を果たす組織やヒトを特定し、優先付けをし、評価する。	3	スマートホーム向け製品・サービスのリスク分析

3.6.	CPS.SC-3	・外部の組織との契約を行う場合、目的及びリスクマネジメントの結果を考慮し、自組織のセキュリティに関する要求事項に対して関係する他組織のセキュリティマネジメントが適合していることを確認する。	5.2.2	設計・製造フェーズ No.2「開発及びソリューションの外部委託」
			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 R2-2、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」
3.6.	CPS.SC-4	・外部の組織との契約を行う場合、目的及びリスクマネジメントの結果を考慮し、自組織のセキュリティに関する要求事項に対して関係する他組織の提供する製品・サービスが適合していることを確認する。	5.2.2	設計・製造フェーズ No.2「開発及びソリューションの外部委託」
			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 R2-2、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」
3.6.	CPS.SC-5	・取引先等の関係する他組織の要員の内、自組織から委託する業務に関わる者に対するセキュリティ上の要求事項を策定し、運用する。	5.2.2	設計・製造フェーズ No.2「開発及びソリューションの外部委託」
			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 R2-2、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」
3.6.	CPS.SC-6	・取引先等の関係する他組織が、契約上の義務を果たしていることを確認するために、監査、テスト結果、または他の形式の評価を使用して定期的に評価する。	5.2.3	評価フェーズ No.2「脆弱性の有無のチェック」
3.6.	CPS.SC-7	・取引先等の関係する他組織に対する監査、テストの結果、契約事項に対する不適合が発見された場合に実施すべきプロシージャを策定し、	－	該当なし

		運用する。		
3.6.	CPS.SC-8	・自組織が、関係する他組織及び個人との契約上の義務を果たしていることを証明するための情報(データ)を収集、安全に保管し、必要に応じて適当な範囲で開示できるようにする。	―	該当なし
3.6.	CPS.SC-9	・サプライチェーンにおけるインシデント対応活動を確実にするために、インシデント対応活動に関係する者の間で対応プロセスの整備と訓練を行う。	5.2.4	運用・保守フェーズ No.16「サービス提供上のインシデント対応」
3.6.	CPS.SC-10	・取引先等の関係する他組織との契約が終了する際(例：契約期間の満了、サポートの終了)に実施すべきプロシージャを策定し、運用する。	―	該当なし
3.6.	CPS.SC-11	・サプライチェーンに係るセキュリティ対策基準及び関係するプロシージャ等を継続的に改善する。	―	該当なし
3.7.	CPS.AC	アイデンティティ管理、認証及びアクセス制御		
3.7.	CPS.AC-1	・承認されたモノとヒト及びプロシージャの識別情報と認証情報を発効、管理、確認、取消、監査するプロシージャを確立し、実施する。	5.6	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

3.7.	CPS.AC-2	・IoT 機器、サーバ等の設置エリアの施錠、入退室管理、生体認証等の導入、監視カメラの設置、持ち物や体重検査等の物理的セキュリティ対策を実施する。	5.2.4	運用・保守フェーズ No.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）」 No.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）」
			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 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」 R3-7「各サービス担当者のアクセス管理」
			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 SR3-PP-15「各サービス担当者のアクセス管理」
3.7.	CPS.AC-3	・無線接続先(ユーザーや IoT 機器、サーバ等)を正しく認証する。	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 R2-4「サービス契約者の本人認証」 R3-7「各サービス担当者のアクセス管理」

			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 SR2-SP-2「API における認証」 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」 SR2-SP-4「サーバログイン時におけるユーザ認証の実施」 SR2-SP-5「ホームゲートウェイの認証」 SR2-SP-6「認証に必要な情報の管理」
			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 SR2-PP-2「API における認証」 SR2-PP-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」 SR2-PP-4「サーバログイン時におけるユーザ認証の実施」 SR2-PP-5「ホームゲートウェイの認証」 SR2-PP-6「認証に必要な情報の管理」 SR3-PP-15「各サービス担当者のアクセス管理」
			6.2.3	ホームゲートウェイへのセキュリティ要求事項 SR2-H-2「認証」 SR2-H-3「相互認証に必要な情報の管理」

			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 SR2-D-2「認証」 SR2-D-3「相互認証に必要な情報の管理」
			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 SR2-A-1「利用者の認証」
3.7.	CPS.AC-4	・一定回数以上のログイン認証失敗によるロックアウトや、安全性が確保できるまで再ログインの間隔をあける機能を実装する等により、IoT 機器、サーバ等に対する不正ログインを防ぐ。	－	該当なし
3.7.	CPS.AC-5	・職務及び責任範囲(例:ユーザー/システム管理者)を適切に分離する。	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 R2-4「サービス契約者の本人認証」 R3-7「各サービス担当者のアクセス管理」
			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 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」 SR2-SP-4「サーバログイン時におけるユーザ認証の実施」 SR2-SP-6「認証に必要な情報の管理」

			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 SR2-PP-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」 SR2-PP-4「サーバログイン時におけるユーザ認証の実施」 SR2-PP-6「認証に必要な情報の管理」 SR3-PP-15「各サービス担当者のアクセス管理」
3.7.	CPS.AC-6	・特権を持つユーザーのシステムへのネットワーク経由でのログインに対して、想定されるリスクも考慮して、信頼性の高い認証方式（例：二つ以上の認証機能を組み合わせた多要素認証）を採用する。	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 R2-4「サービス契約者の本人認証」
			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 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」 SR2-SP-4「サーバログイン時におけるユーザ認証の実施」 SR2-SP-6「認証に必要な情報の管理」

			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 SR2-PP-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」 SR2-PP-4「サーバログイン時におけるユーザ認証の実施」 SR2-PP-6「認証に必要な情報の管理」
3.7.	CPS.AC-7	・データフロー制御ポリシーを定め、それに従って適宜ネットワークを分離する （例：開発・テスト環境と実運用環境、IoT 機器を含む環境と組織内の他の環境）等してネットワークの完全性を保護する。	5.2.1	サービス企画フェーズ No.4「リスク分析・評価とサービスレベルの定義」 No.6「セキュリティ対策方針の策定」
3.7.	CPS.AC-8	・IoT 機器、サーバ等が実施する通信は、適切な手順で識別されたエンティティ（ヒト/モノ/システム等）との通信に限定する。	5.2.1	サービス企画フェーズ No.4「リスク分析・評価とサービスレベルの定義」 No.6「セキュリティ対策方針の策定」
			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 SR3-SP-8「サーバセキュリティ対策」
			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 SR3-PP-8「サーバセキュリティ対策」

		・IoT 機器やユーザーによる構成要素(モノ/システム等)への論理的なアクセスを、取引のリスク(個人のセキュリティ、プライバシーのリスク及びその他の組織的なリスク)に見合う形で認証・認可する。	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 R2-4「サービス契約者の本人認証」 R3-7「各サービス担当者のアクセス管理」
3.7.	CPS.AC-9		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 SR2-SP-2「API における認証」 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」 SR2-SP-4「サーバログイン時におけるユーザ認証の実施」 SR2-SP-5「ホームゲートウェイの認証」 SR2-SP-6「認証に必要な情報の管理」

			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 SR2-PP-2「API における認証」 SR2-PP-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」 SR2-PP-4「サーバログイン時におけるユーザ認証の実施」 SR2-PP-5「ホームゲートウェイの認証」 SR2-PP-6「認証に必要な情報の管理」 SR3-PP-15「各サービス担当者のアクセス管理」
			6.2.3	ホームゲートウェイへのセキュリティ要求事項 SR2-H-2「認証」 SR2-H-3「相互認証に必要な情報の管理」
			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 SR2-D-2「認証」 SR2-D-3「相互認証に必要な情報の管理」
			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 SR2-A-1「利用者の認証」

3.8.	CPS.AT	意識向上及びトレーニング		
3.8.	CPS.AT-1	・自組織の全ての要員に対して、セキュリティインシデントの発生とその影響を抑制するために割り当てられた役割と責任を遂行するための適切な訓練、教育を実施し、その記録を管理する。	5.2.4	運用・保守フェーズ No.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)」 No.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)」
			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 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」
3.8.	CPS.AT-2	・自組織におけるセキュリティインシデントに関係し得る、セキュリティマネジメントにおいて重要度の高い関係他組織の担当者に対して、割り当てられた役割を遂行するための適切な訓練(トレーニング)、セキュリティ教育を実施し、その記録を管理する。	5.2.4	運用・保守フェーズ No.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)」 No.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)」 No.12「第三者サービス情報基盤の運用堅牢化③(遠隔開錠操作)」
			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 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」
3.8.	CPS.AT-3	・自組織の要員や、重要度の高い関係他組織の担当者に対する、セキュリティに係る訓練、教育の内容を改善する。	－	該当なし
3.9.	CPS.DS	データセキュリティ		
3.9.	CPS.DS-1	・組織間で保護すべき情報を交換する場合、当該情報の保護に係るセキュリティ要件について、事前に組織間で取	5.5	スマートホームサービスのセキュリティ要件
			5.6	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

		り決める。	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 R2-1、R3-2「リスク分析・評価、セキュリティ対策方針の策定」
3.9.	CPS.DS-2	・情報を適切な強度の方式で暗号化して保管する。	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 SR3-SP-10「データ暗号化」
			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 SR3-PP-10「データ暗号化」
			6.2.3	ホームゲートウェイへのセキュリティ要求事項 SR3-H-6「データ暗号化」
3.9.	CPS.DS-3	・IoT 機器、サーバ等の間、サイバー空間で通信が行われる際、通信経路を暗号化する。	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 SR3-SP-9「通信経路暗号化」
			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 SR3-PP-9「通信経路暗号化」
			6.2.3	ホームゲートウェイへのセキュリティ要求事項 SR-H-4「外部インターネットとの通信経路暗号化」 SR-H-5「LAN 内接続機器との通信経路暗号化」
			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 SR-D-2「LAN 内接続機器との通信経路暗号化」
3.9.	CPS.DS-4	・情報を送受信する際に、情報そのものを暗号化して送受信する。	－	該当なし

3.9.	CPS.DS-5	・送受信データ、保管データの暗号化等に用いる鍵を、ライフサイクルを通じて安全に管理する。	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 SR3-SP-11「鍵管理」
			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 SR3-PP-11「鍵管理」
			6.2.3	ホームゲートウェイへのセキュリティ要求事項 SR3-H-7「鍵管理」
			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 SR3-D-3「鍵管理」
3.9.	CPS.DS-6	・サービス拒否攻撃等のサイバー攻撃を受けた場合でも、資産を適切に保護し、攻撃による影響を最小限にできるよう、構成要素において十分なリソース(例：ヒト、モノ、システム)を確保する。	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 SR3-SP-5「DoS 対策」
			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 SR3-PP-5「DoS 対策」
3.9.	CPS.DS-7	・IoT 機器、通信機器、回線等に対し、定期的な品質管理、予備機や無停電電源装置の確保、冗長化、故障の検知、交換作業、ソフトウェアの更新を行う。	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 R2-7「最新のソフトウェアへの定期的な更新」 R2-8「更新ソフトウェアの運用手順及びバージョン管理」 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」
			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 SR2-SP-7「セキュリティパッチの適用」

			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 SR2-PP-7「セキュリティパッチの適用」
			6.2.3	ホームゲートウェイへのセキュリティ要求事項（★★サービス SR2-H-4「機器の稼働監視、障害監視」 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」
			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 SR2-D-4「可用性に考慮した通信I/F」 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」
			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 SR2-A-3「スマートフォンアプリのアップデート」
3.9.	CPS.DS-8	・保護すべき情報を扱う、あるいは自組織にとって重要な機能を有する機器を調達する場合、耐タンパーデバイスを利用する。	－	該当なし
3.9.	CPS.DS-9	・自組織外への不適切な通信を防ぐため、保護すべき情報を自組織外へ送信する通信を適切に制御する。	－	該当なし
3.9.	CPS.DS-10	・IoT 機器、サーバ等にて稼動するソフトウェアの完全性を組織が定めるタイミングで検証し、不正なソフトウェアの起動を防止する。	－	該当なし

3.9.	CPS.DS-11	・送受信・保管する情報に完全性チェックメカニズムを使用する。	－	該当なし
3.9.	CPS.DS-12	・ハードウェアの完全性を検証するために完全性チェックメカニズムを使用する。	－	該当なし
3.9.	CPS.DS-13	・IoT 機器やソフトウェアが正規品であることを定期的(起動時等)に確認する。	－	該当なし
3.9.	CPS.DS-14	・データの取得元、加工履歴等をライフサイクルの全体に渡って維持・更新・管理する。	－	該当なし
3.9.	CPS.DS-15	・計測の可用性、完全性保護によるセンシングデータの信頼性確保のために、計測セキュリティの観点が考慮された製品を利用する。	－	該当なし
3.10.	CPS.IP	情報を保護するためのプロセス及び手順		
3.10.	CPS.IP-1	・IoT 機器、サーバ等の初期設定手順(パスワード等)及び設定変更管理プロセスを導入し、運用する。	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 R2-3「構成機器に対する適切な初期設定（IoT 機器間の認証情報とアクセス制御）」
			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 SR2-SP-1「共通要件への対応」※共通要件 No.6 対応事項
			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 SR2-SP-1「共通要件への対応」※共通要件 No.6 対応事項

			6.2.3	ホームゲートウェイへのセキュリティ要求事項 SR2-SP-1「共通要件への対応」※共通要件 No.6 対応事項
			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 SR2-SP-1「共通要件への対応」※共通要件 No.6 対応事項
3.10.	CPS.IP-2	・IoT 機器、サーバ等の導入後に、追加するソフトウェアを制限する。	―	該当なし
3.10.	CPS.IP-3	・システムを管理するためのシステム開発ライフサイクルを導入する。	5.2.3	設計・製造フェーズ No.2「開発及びソリューションの外部委託」
3.10.	CPS.IP-4	・構成要素(IoT 機器、通信機器、回線等)に対し、定期的なシステムバックアップを実施し、テストする。	―	該当なし
3.10.	CPS.IP-5	・無停電電源装置、防火設備の確保、浸水からの保護等、自組織の IoT 機器、サーバ等の物理的な動作環境に関するポリシーや規則を満たすよう物理的な対策を実施する。	―	該当なし
3.10.	CPS.IP-6	・IoT 機器、サーバ等の廃棄時には、内部に保存されているデータ及び、正規 IoT 機器、サーバ等を一意に識別する ID(識別子)や重要情報(秘密鍵、電子証明書等)を削除又は読み取りできない状態にする。	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 SR2-SP-1「共通要件への対応」※共通要件 No.7 対応事項
			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 SR2-SP-1「共通要件への対応」※共通要件 No.7 対応事項

			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 SR3-PP-14「個人情報の消去」
			6.2.3	ホームゲートウェイへのセキュリティ要求事項 SR2-SP-1「共通要件への対応」※共通要件 No.7 対応事項
			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 SR2-SP-1「共通要件への対応」※共通要件 No.7 対応事項
3.10.	CPS.IP-7	・セキュリティインシデントへの対応、内部及び外部からの攻撃に関する監視／測定／評価結果から教訓を導き出し、資産を保護するプロセスを改善する。	5.2.4	運用・保守フェーズ No.16「サービス対応機器に対するインシデント対応」
			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 R3-8「サービス提供におけるインシデント対応」
3.10.	CPS.IP-8	・保護技術の有効性について、適切なパートナーとの間で情報を共有する。	5.2.2	設計・製造フェーズ No.2「開発及びソリューションの外部委託」
3.10.	CPS.IP-9	・人の異動に伴い生じる役割の変更に対応した対策にセキュリティに関する事項（例：アクセス権限の無効化、従業員に対する審査）を含める。	5.2.4	運用・保守フェーズ No.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）」 No.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）」 No.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）」 No.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）」 No.12「第三者サービス情報基盤の運用堅牢化③（遠隔開錠操作）」

			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 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」
3.10.	CPS.IP-10	・脆弱性修正措置計画を作成し、計画に沿って構成要素の脆弱性を修正する。	5.2.4	運用・保守フェーズ No.16「サービス対応機器に対するインシデント対応」
			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 R3-8「サービス提供におけるインシデント対応」
3.11.	CPS.MA	保守		
3.11.	CPS.MA-1	・IoT 機器、サーバ等のセキュリティ上重要なアップデート等を、必要なタイミングに管理されたツールを利用して適切に履歴を記録しつつ実施する。	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 R2-7「最新のソフトウェアへの定期的な更新」 R2-8「更新ソフトウェアの運用手順及びバージョン管理」 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」
			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 SR2-SP-7「セキュリティパッチの適用」
			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 SR2-PP-7「セキュリティパッチの適用」
			6.2.3	ホームゲートウェイへのセキュリティ要求事項 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」

			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 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」
			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 SR2-A-3「スマートフォンアプリのアップデート」
		・可能であれば、遠隔地からの操作によってソフトウェア(OS、ドライバ、アプリケーション)を一括して更新するリモートアップデートの仕組みを備えたIoT 機器を導入する。	－	該当なし
3.11.	CPS.MA-2	・自組織のIoT 機器、サーバ等に対する遠隔保守を、適用先のモノ、システムのオーナー部門による承認を得て、ログを記録し、不正アクセスを防げる形で実施する。	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 R3-5「ログ収集・データ分析」
			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 SR3-SP-6「ログ採取・分析」
			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 SR3-PP-6「ログ採取・分析」
			6.2.3	ホームゲートウェイへのセキュリティ要求事項 SR3-H-8「ログ採取・分析」
3.12.	CPS.PT	保護技術		
3.12.	CPS.PT-1	・セキュリティインシデントを適切に検知するため、監査記録／ログ記録の対象を決	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 R3-5「ログ収集・データ分析」

		定、文書化し、そうした記録を実施して、レビューする。	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 SR3-SP-6「ログ採取・分析」
			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 SR3-PP-6「ログ採取・分析」
3.12.	CPS.PT-2	・IoT 機器、サーバ等の本体に対して、不要なネットワークポート、USB、シリアルポート等を物理的または論理的に閉塞することで、IoT 機器、サーバ等の機能を必要最小限とする。	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 SR2-SP-1「共通要件への対応」※共通要件 No.4 対応事項 SR3-SP-8「サーバセキュリティ対策」
			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 SR2-PP-1「共通要件への対応」※共通要件 No.4 対応事項 SR3-PP-8「サーバセキュリティ対策」
			6.2.3	ホームゲートウェイへのセキュリティ要求事項 SR2-H-1「共通要件への対応」※共通要件 No.4 対応事項 SR2-H-5「USB 接続端子の対策」
			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 SR2-D-1「共通要件への対応」※共通要件 No.4 対応事項 SR2-D-5「USB 接続端子の対策」
3.12.	CPS.PT-3	・ネットワークにつながることを踏まえた安全性を実装する IoT 機器を導入する。	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 R2-2、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」

			6.2.1	スマートホームサービスにおけるセキュリティ要件 SR3-SP-2「外部インターネットからの不正アクセス防止」 SR3-SP-7「マルウェア対策」
			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 SR3-PP-2「外部インターネットからの不正アクセス防止」 SR3-PP-7「マルウェア対策」
			6.2.3	ホームゲートウェイへのセキュリティ要求事項 SR3-H-2「外部インターネットからの不正アクセス防止」
3.13.	CPS.AE	異変とイベント		
3.13.	CPS.AE-1	・ネットワーク運用のベースラインと、ヒト、モノ、システム間の予測される情報の流れを特定し、管理するプロシージャを確立し、実施する。	5.2.1	サービス企画フェーズ No.4「リスク分析・評価とサービスレベルの定義」
			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 R2-1、R3-2「リスク分析・評価、セキュリティ対策方針の策定」
3.13.	CPS.AE-2	・セキュリティ管理責任者を任命し、セキュリティ対策組織(SOC/CSIRT)を立ち上げ、組織内でセキュリティ事象を検知・分析・対応する体制を整える。	5.2.4	運用・保守フェーズ No.16「サービス提供上のインシデント対応」
			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 R3-8「サービス提供におけるインシデント対応」
3.13.	CPS.AE-3	・セキュリティ事象の相関の分析及び外部の脅威情報と比較した分析を行う手順を	5.2.1	サービス企画フェーズ No.4「リスク分析・評価とサービスレベルの定義」

		実装することで、セキュリティインシデントを正確に特定する。	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 R2-1、R3-2「リスク分析・評価、セキュリティ対策方針の策定」
3.13.	CPS.AE-4	・関係する他組織への影響を含めてセキュリティ事象がもたらす影響を特定する。	5.2.1	サービス企画フェーズ No.4「リスク分析・評価とサービスレベルの定義」
			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 R2-1、R3-2「リスク分析・評価、セキュリティ対策方針の策定」
3.13.	CPS.AE-5	・セキュリティ事象の危険度の判定基準を定める。	5.2.1	サービス企画フェーズ No.4「リスク分析・評価とサービスレベルの定義」
			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 R2-1、R3-2「リスク分析・評価、セキュリティ対策方針の策定」
3.14.	CPS.CM	セキュリティの継続的なモニタリング		
3.14.	CPS.CM-1	・組織内のネットワークと広域ネットワークの接点において、ネットワーク監視・制御、アクセス監視・制御を実施する。	5.2.4	運用・保守フェーズ No.2「ログ収集・データ分析」
3.14.	CPS.CM-2	・IoT 機器、サーバ等の重要性を考慮し、適切な物理的アクセスの設定及び記録、監視を実施する。	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 R3-5「ログ収集・データ分析」
			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 SR3-SP-4「不正侵入検知と遮断」 SR3-SP-6「ログ採取・分析」

			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 SR3-PP-4「不正侵入検知と遮断」 SR3-PP-6「ログ採取・分析」
			6.2.3	ホームゲートウェイへのセキュリティ要求事項 SR2-H-4「機器の稼働監視、障害監視」
3.14.	CPS.CM-3	・指示された動作内容と実際の動作結果を比較して、異常の検知や動作の停止を行うIoT 機器を導入する。	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 SR3-SP-4「不正侵入検知と遮断」
			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 SR3-PP-4「不正侵入検知と遮断」
			6.2.3	ホームゲートウェイへのセキュリティ要求事項 SR2-H-4「機器の稼働監視、障害監視」
		・サイバー空間から受ける情報が悪質なコードを含んでおらず、許容範囲内であることを動作前に検証する。	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 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」
			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 SR3-PP-3「Web アプリケーションの脆弱性を悪用した攻撃対策」
			6.2.3	ホームゲートウェイへのセキュリティ要求事項 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」
3.14.	CPS.CM-4	・サイバー空間から受ける情報の完全性及び真正性を動作前に確認する。	－	該当なし

3.14.	CPS.CM-5	・セキュリティ事象を適切に検知できるよう、外部サービスプロバイダとの通信内容をモニタリングする。	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 R3-5「ログ収集・データ分析」
			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 SR3-SP-4「不正侵入検知と遮断」 SR3-SP-6「ログ採取・分析」
			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 SR3-PP-4「不正侵入検知と遮断」 SR3-PP-6「ログ採取・分析」
3.14.	CPS.CM-6	・機器等の構成管理では、ソフトウェア構成情報、ネットワーク接続状況(ネットワーク接続の有無、アクセス先等)及び他のソシキ、ヒト、モノ、システムとの情報の送受信状況について、継続的に管理する。	－	該当なし
3.14.	CPS.CM-7	・自組織の管理しているIoT機器、サーバ等に対して、定期的に対処が必要な脆弱性の有無を確認する。	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 R3-6「脆弱性の有無のチェック」
			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 SR3-SP-13「脆弱性スキャン、ペネトレーションテスト」
			6.2.2	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 SR3-PP-13「脆弱性スキャン、ペネトレーションテスト」
			6.2.3	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 SR3-H-9「脆弱性スキャン、ペネトレーションテスト」

			6.2.4	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 SR3-D-5「脆弱性スキャン、ペネトレーションテスト」
3.15.	CPS.DP	検知プロセス		
3.15.	CPS.DP-1	・セキュリティ事象の説明責任を果たせるよう、セキュリティ事象検知における自組織とサービスプロバイダが担う役割と負う責任を明確にする。	5.2.1	サービス企画フェーズ No.1「企業組織としての対応方針の策定」 No.2「企業組織としてのプライバシポリシーの策定」 No.3「サービス要件やシステムモデル、ユースケースの定義」 No.7「サービスとしての免責事項の定義」
			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 R2-1、R3-2「リスク分析・評価、セキュリティ対策方針の策定」 R2-2、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」
3.15.	CPS.DP-2	・監視業務では、地域毎に適用される法令、通達や業界標準等に準拠して、セキュリティ事象を検知する。	－	該当なし
3.15.	CPS.DP-3	・監視業務として、セキュリティ事象を検知する機能が意図したとおりに動作するかどうかを定期的にテストし、妥当性を検証する。	－	該当なし
3.15.	CPS.DP-4	・セキュリティ事象の検知プロセスを継続的に改善する。	－	該当なし

3.16.	CPS.RP	対応計画		
3.16.	CPS.RP-1	・セキュリティインシデント発生後の対応の内容や優先順位、対策範囲を明確にするため、インシデントを検知した後の組織／ヒト／モノ／システムの対応手順（セキュリティ運用プロセス）をあらかじめ定義し、実装する。	－	該当なし
3.16.	CPS.RP-2	・セキュリティ運用プロセスにおいて、取引先等の関係する他組織との連携について手順と役割分担を定め、運用する。	5.2.1	サービス企画フェーズ No.3「サービス要件やシステムモデル、ユースケースの定義」
			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 R2-2、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」
3.16.	CPS.RP-3	・自然災害時における対応方針及び対応手順を定めている事業継続計画又は緊急時対応計画の中にセキュリティインシデントを位置づける。	－	該当なし
3.16.	CPS.RP-4	・セキュリティインシデント発生時に被害を受けた設備にて生産される等して、何らかの品質上の欠落が生じていることが予想されるモノ（製品）に対して適切な対応を行う。	5.2.4	運用・保守フェーズ No.16「サービス提供上のインシデント対応」
			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 R3-8「サービス提供におけるインシデント対応」
3.17.	CPS.CO	伝達		
3.17.	CPS.CO-1	・セキュリティインシデント発生後の情報公表時のルールを策定し、運用する。	5.2.4	運用・保守フェーズ No.16「サービス提供上のインシデント対応」

			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 R3-8「サービス提供におけるインシデント対応」
3.17.	CPS.CO-2	・事業継続計画又は緊急時対応計画の中に、セキュリティインシデントの発生後、組織に対する社会的評価の回復に取り組む点を位置づける。	－	該当なし
3.17.	CPS.CO-3	・復旧活動について内部及び外部の利害関係者と役員、そして経営陣に伝達する点を、事業継続計画又は緊急時対応計画の中に位置づける。	－	該当なし
3.18.	CPS.AN	分析		
3.18.	CPS.AN-1	・セキュリティインシデントの全容と、推測される攻撃者の意図から、自組織及び関係する他組織を含む社会全体への影響を把握する。	－	該当なし
3.18.	CPS.AN-2	・セキュリティインシデント発生後に、デジタルフォレンジックを実施する。	5.2.4	運用・保守フェーズ No.16「サービス提供上のインシデント対応」
			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 R3-5「ログ収集・データ分析」 R3-8「サービス提供におけるインシデント対応」
			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 SR3-SP-6「ログ採取・分析」
			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 SR3-PP-6「ログ採取・分析」

3.18.	CPS.AN-3	・検知されたセキュリティインシデントの情報は、セキュリティに関する影響度の大小や侵入経路等で分類し、保管する。	5.2.4	運用・保守フェーズ No.16「サービス提供上のインシデント対応」
			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 R3-8「サービス提供におけるインシデント対応」
3.19.	CPS.MI	低減		
3.19.	CPS.MI-1	・セキュリティインシデントによる被害の拡大を最小限に抑え、影響を低減する対応を行う。	5.2.4	運用・保守フェーズ No.16「サービス提供上のインシデント対応」
			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 R3-8「サービス提供におけるインシデント対応」
3.20.	CPS.IM	改善		
3.20.	CPS.IM-1	・セキュリティインシデントへの対応から教訓を導き出し、セキュリティ運用プロセスを継続的に改善する。	5.2.4	運用・保守フェーズ No.16「サービス提供上のインシデント対応」
			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 R3-8「サービス提供におけるインシデント対応」
3.20.	CPS.IM-2	・セキュリティインシデントへの対応から教訓を導き出し、事業継続計画又は緊急時対応計画を継続的に改善する。	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 R3-8「サービス提供におけるインシデント対応」

4 「Code of Practice for Consumer IoT Security」との関係

本書は英国が発行した「Code of Practice for Consumer IoT Security」に対する要件の準拠を確認している。「Code of Practice for Consumer IoT Security」と本書の対応を表 4-1 に示す。

表 4-1 Code of Practice for Consumer IoT Security と本書との対応

「Code of Practice for Consumer IoT Security」		本書での対応箇所	
No.	要件	章番号	概要
UK1	デフォルトパスワードを使用しない	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 SR2-SP-1「共通要件への対応」※共通要件 No.6
		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 SR2-PP-1「共通要件への対応」※共通要件 No.6
		6.2.3	ホームゲートウェイへのセキュリティ要求事項 SR2-H-1「共通要件への対応」※共通要件 No.6
		6.2.4	スマートホーム対応機器へのセキュリティ要求事項 SR2-D-1「共通要件への対応」※共通要件 No.6
UK2	脆弱性の情報公開ポリシを策定する	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 R2-8「サービス提供におけるインシデント対応」
UK3	ソフトウェアを定期的に更新する	6.1	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 R2-7「最新のソフトウェアへの定期的な更新ウェアの提供」 R2-8「更新ソフトウェアの運用手順及びバージョン管理」 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」
		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 SR2-SP-1「共通要件への対応」※共通要件 No.11

			SR2-SP-7「セキュリティパッチの適用」
		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 SR2-PP-1「共通要件への対応」※共通要件 No.11 SR2-PP-7「セキュリティパッチの適用」
		6.2.3	ホームゲートウェイへのセキュリティ要求事項 SR2-H-1「共通要件への対応」※共通要件 No.11 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」
		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 SR2-D-1「共通要件への対応」※共通要件 No.11 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」
		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 SR2-A-3「スマートフォンアプリのアップデート」
UK4	認証情報とセキュリティ上重要な情報を安全に保存する	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 SR3-SP-10「データ暗号化」 SR3-SP-11「鍵管理」
		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 SR3-PP-10「データ暗号化」 SR3-PP-11「鍵管理」
		6.2.3	ホームゲートウェイへのセキュリティ要求事項 SR3-H-6「データ暗号化」 SR3-H-7「鍵管理」
		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 SR3-D-3「鍵管理」
UK5	安全に通信する	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 SR3-SP-9「通信経路暗号化」

		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 SR2-PP-1「共通要件への対応」※共通要件 No.8,9 SR3-PP-9「通信経路暗号化」
		6.2.3	ホームゲートウェイへのセキュリティ要求事項 SR2-H-1「共通要件への対応」※共通要件 No.8,9 SR3-H-4「外部インターネットとの通信経路暗号化」 SR3-H-5「LAN 内接続機器との通信経路暗号化」
		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 SR2-D-1「共通要件への対応」※共通要件 No.8,9 SR3-D-2「LAN 内接続機器との通信経路暗号化」
UK6	攻撃対象になる場所を最低限に抑える	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 R2-3「構成機器に対する適切な初期設定（IoT 機器間の認証情報とアクセス制御）」
		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 SR2-SP-1「共通要件への対応」※共通要件 No.4,5,10 SR3-SP-8「サーバセキュリティ対策」
		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 SR2-PP-1「共通要件への対応」※共通要件 No.4,5,10 SR3-PP-8「サーバセキュリティ対策」
		6.2.2	ホームゲートウェイへのセキュリティ要求事項 SR2-H-1「共通要件への対応」※共通要件 No.4,5,10
		6.2.3	スマートホーム対応機器へのセキュリティ要求事項 SR2-D-1「共通要件への対応」※共通要件 No.4,5,10

UK7	ソフトウェアの整合性を確認する	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 R2-8「更新ソフトウェアの運用手順及びバージョン管理」
UK8	個人データの保護を徹底する	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 R2-5「スマートホーム内で利用される個人情報の削除」 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」
		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 SR2-SP-10「データ暗号化」
		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 SR3-PP-10「データ暗号化」 SR3-PP-14「個人情報の消去」
		6.2.3	ホームゲートウェイへのセキュリティ要求事項 SR3-H-6「データ暗号化」
UK9	機能停止時の復旧性を確保する	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 SR3-SP-5「DoS 対策」
		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 SR3-PP-5「DoS 対策」
UK10	システムの遠隔データを監視する	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 R3-5「ログ収集・データ分析」
		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 SR3-SP-4「不正侵入検知と遮断」 SR3-SP-6「ログ採取・分析」

		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 SR3-PP-4「不正侵入検知と遮断」 SR3-PP-6「ログ採取・分析」
		6.2.3	ホームゲートウェイへのセキュリティ要求事項 SR3-H-4「機器の稼働監視、障害監視」
UK11	消費者が個人データを用意に削除できるように配慮する	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 R2-5「スマートホーム内で利用される個人情報の削除」
UK12	デバイスの設置とメンテナンスを用意にできるように配慮する	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 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」
UK13	入力データを検証する	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 SR2-SP-1「共通要件への対応」※共通要 No.1,2,3 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」
		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 SR2-PP-1「共通要件への対応」※共通要 No.1,2,3 SR3-PP-3「Web アプリケーションの脆弱性を悪用した攻撃対策」
		6.2.3	ホームゲートウェイへのセキュリティ要求事項 SR2-H-1「共通要件への対応」※共通要件 No.1,2,3 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」

5　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」との関係

本書は米国カリフォルニア州で法案として可決された「接続される機器のセキュリティ法」に対する要件の準拠を確認している。「接続される機器のセキュリティ法」と本書の対応を表 5-1 に示す。

表 5-1 接続される機器のセキュリティ法と本書との対応

「接続される機器のセキュリティ法」		本書での対応箇所	
No.	要件	章番号	概要
1	インターネットに接続する機器の製造者は当該機器に、合理的なセキュリティ機能または以下のすべてを備えたものとする。 １．デバイスの性質と機能に適し、 ２．収集、保管、または送信できる情報に適し、 ３．不正なアクセス、破壊、使用、変更、または開示から、機器および機器に含まれるすべての情報を保護する設計	※注釈	下記の★★～★★★サービスにおけるセキュリティ要件及びセキュリティ要求事項において、個人情報を含む保護すべき資産の保護、機器やユーザの認証、通信経路の暗号化、ソフトウェア更新等の対策を定義し、左記の対策を満たすものと判断している。
		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
		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
		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
		6.2.3	ホームゲートウェイへのセキュリティ要求事項
		6.2.4	スマートホーム対応機器へのセキュリティ要求事項
		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
2	ローカルエリアの外で認証を実施する機器は、以下のいずれかを満たす場合に、合理的なセキュリティ機能を備えているとみなす。 １．あらかじめプログラムされたパスワードは、製造された各機器に固有のものであること ２．当該機器は、初回アクセスが許可される前にユーザーが新しい認証手段を生成しなければならないセキュリティ機能を有していること	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 SR2-SP-1「共通要件への対応」※共通要件 No.6
		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 SR2-PP-1「共通要件への対応」※共通要件 No.6
		6.2.3	ホームゲートウェイへのセキュリティ要求事項 SR2-H-1「共通要件への対応」※共通要件 No.6
		6.2.4	スマートホーム対応機器へのセキュリティ要求事項 SR2-D-1「共通要件への対応」※共通要件 No.6