CCDS-SH02-2023
CCDS-SH03-2023

製品分野別セキュリティガイドライン
スマートホーム編 2023 年版
別紙セキュリティ要求事項

Ver. 1.0

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	2024/6/1	2023 版として要件、要求事項を改定し、別冊化し新規発行

■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。

© Connected Consumer Device Security Council Proprietary

目次

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が増加し、IoT 製品やサービス、サプライチェーンに対するサイバーセキュリティへの対策が国家の経済安全保障上の課題として取り上げられている。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。米国では 2022 年 9 月 14 日に制定された大統領令 14028 を皮切りに、コンシューマー向け IoT 製品のセキュリティ要求を示す文書として NIST IR8425 ″Profile of the IoT Core Baseline for Consumer IoT Products″[1]がリリースされ、ラベリング制度の検討が進められている。欧州では 2020 年にコンシューマー向け IoT 製品のセキュリティ標準を定義した ETSI EN 303 645 ″Cyber Security for Consumer Internet of Things: Baseline Requirements″[2]がリリースされた。また、“The Cyber Resilience Act(CRA)”による法制化の検討が進められている。一方、日本では、2022 年 11 月より経済産業省が IoT 製品を対象とした適合性評価制度の検討を開始しており、国内におけるセキュリティ対策の普及、促進が期待されている。

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 2014 年に設立され、継続的に IoT 製品のセキュリティに関する活動を行っている。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」[3]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。

2　スマートホームサービスにおけるセキュリティ要件

本書では、「「製品分野別セキュリティガイドラインスマートホーム編　2023 年版」にて記載したリスク分析・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。

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

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）[4]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 2.2 節記載のセキュリティ要求事項は、米国の NIST IR 8425 “Profile of the IoT Core Baseline for Consumer IoT Products”、欧州の標準規格 ETSI EN303 645 “CYBER; Cyber Security for Consumer Internet of Things: Baseline Requirements”を参考とし、スマートホーム分野としての必要可否を検討した上で定義を行った。

表 2-1 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 2-2　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 2-3 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	ESTI EN303 645	NIST IR8425	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分析すること。 ・リスク分析・評価結果を踏まえて、レベル２（★★）の適合に必要なセキュリティ対策の方針を策定、文書化すること	◎	◎	○ 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。	◎	◎	＝ CPS.SC-3 CPS.SC-4 CPS.SC-5 CPS.PT-3 CPS.DP-1 CPS.RP-2

R2-3	★★	サービス	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）	・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。	＝ 5.6-2 5.12-1	＝	＝ 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。	＝ 5.1-4	＝	＝ 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の削除を可能とすること。	＝ 5.11-1	＝	◎
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。	＝ 5.12-1	◎	◎
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。	＝ 5.3-8	＝	○ 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。 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	◎	◎	○ CPS.DS-7 CPS.MA-1
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。	◎	◎	○ 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。	◎	◎	○ CPS.DS-1 CPS.AE-1 CPS.AE-3 CPS.AE-4

				・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分析すること。 ・リスク分析・評価結果を踏まえて、レベル３（★★★）の適合に必要なセキュリティ対策の方針を策定し、文書化すること			CPS.AE-5 CPS.DP-1
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。	◎	◎	＝ 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。	◎	◎	○ CPS.AT-1 CPS.AC-2 CPS.IP-9

				※ISO/IEC27017：ISMS クラウドセキュリティ認証			
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。	＝ 5.10-1	＝	＝ 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	各サービス担当者のアクセス権限管理	・各サービス担当者によるスマートホームシステムへのアクセスに対して、適切なアクセス権限管理を行うこと。	＝ 5.6-7	＝	＝ 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インシデントレスポンス体制を構築し、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。	◎	◎	＝ 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

2.2　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。

なお、ホームゲートウェイ、スマートホーム対応機器群については、★★サービス、★★★サービスの要求事項を満たす前提として、CCDS サーティフィケーションレベル１（★）のセキュリティ要件、適合基準に準拠した対策を実施するものとする。

レベル１（★）のセキュリティ要件、適合基準は以下の文書を参照とする。

・IoT 機器セキュリティ要件ガイドライン 2023 年版_ver1.0(CCDS-GR01-2023)[5]

・IoT 機器セキュリティ要件_適合基準ガイドライン 2023 年版_ver1.0(CCDS-GRC01-2023)[6]

2.2.1 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 2-4 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	ESTI EN303 645	NIST IR8425	CPSF
SR2-SP-1	★★	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 における認証の仕組みは、報告されている脆弱性への対策を行うこと。	＝ 5.5-4	＝	○ CPS.AC-3 CPS.AC-9
SR2-SP-2	★★	スマートホームサービス情報基盤	サービス管理機能[1]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。	＝ 5.5-5	＝	＝ CPS.AC-3 CPS.AC-5 CPS.AC-6 CPS.AC-9
SR2-SP-3	★★	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。	＝ 5.5-5	＝	＝ CPS.AC-3 CPS.AC-5 CPS.AC-6 CPS.AC-9

[1] サービス管理機能は、ユーザ情報管理、宅内機器の状態管理などサービスの情報管理に使われる機能を指す。

SR2-SP-4	★★	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	正規のホームゲートウェイかどうかを識別、認証する仕組みを有すること。	＝ 5.5-4	＝	＝ CPS.AC-3 CPS.AC-9
SR2-SP-5	★★	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。	＝ 5.4-1	◎	＝ CPS.AC-3 CPS.AC-5 CPS.AC-6 CPS.AC-9
SR2-SP-6	★★	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、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。	＝ 5.3-1 5.3-2 5.3-7 5.3-8 5.3-9 5-3-10	＝	＝ 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に対し、脆弱性スキャン及び、検出された脆弱性への対策を行うこと。 ・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」[7]	○ 5.13-1	◎	○ 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。	○ 5.10-1	◎	＝ 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。	◎	◎	○ 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。	＝ 5.10-1	＝	＝ 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	情報基盤の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	○ 5.6-7	◎	○ 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	・情報基盤間との通信や、ホームゲートウェイとの通信は、通信経路の暗号化を行うこと。 ・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。 【暗号技術に関連するガイドライン】 -「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 暗号リスト)」（最終改訂: 2022 年 3 月 30 日、CRYPTREC LS-0001-2022）[8] -「暗号強度要件（アルゴリズム及び鍵長選択）に関する設定基準」（初版：2022 年 6 月、CRYPTREC LS-0003-2022）[9] 【上記ガイドラインの補足文書】 -「CRYPTREC 暗号技術ガイドライン（SHA-1）改定版」（CRYPTREC GL-2001-2013R1)[10]	○ 5.5-1	＝	○ CPS.DS-3

				- 「CRYPTREC 暗号技術ガイドライン(軽量暗号)」(CRYPTREC GL-2003-2016JP)[11] - 「暗号鍵設定ガイダンス」(CRYPTREC GL-3003-1.0)[12] - 「暗号鍵管理システム設計指針（基本編）」(CRYPTREC GL-3002-1.0)[13] - 「TLS 暗号設定ガイドライン」(CRYPTREC GL-3001-3.0.1)[14]			
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	・情報基盤が保持するデータにおいて、保護すべき資産に該当するものは暗号化による保護を行うこと。 ※保護すべき資産として取り扱うデータは、リスク分析の結果を踏まえ、対象を明確化すること。 ・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。 【暗号技術に関連するガイドライン】 - 「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 暗号リスト)」（最終改訂: 2022 年 3 月 30 日、CRYPTREC LS-0001-2022）[8] - 「暗号強度要件（アルゴリズム及び鍵長選択）に関する設定基準」（初版：2022 年 6 月、CRYPTREC LS-0003-2022）[9]	○ 5.4-1 5.8-1	＝	○ CPS.DS-2

				【上記ガイドラインの補足文書】 -「CRYPTREC 暗号技術ガイドライン（SHA-1）改定版」（CRYPTREC GL-2001-2013R1)[10] -「CRYPTREC 暗号技術ガイドライン(軽量暗号)」(CRYPTREC GL-2003-2016JP)[11] -「暗号鍵設定ガイダンス」(CRYPTREC GL-3003-1.0)[12] -「暗号鍵管理システム設計指針（基本編）」(CRYPTREC GL-3002-1.0)[13] -「TLS 暗号設定ガイドライン」(CRYPTREC GL-3001-3.0.1)[14]			
SR3-SP-11	★★★	スマートホームサービス情報基盤	鍵管理	・暗号化に使用する鍵や証明書は、以下のガイドラインを参考とし、不正なアクセスや変更から保護すること。 -「暗号鍵設定ガイダンス」(CRYPTREC GL-3003-1.0)[12] -「暗号鍵管理システム設計指針（基本編）」(CRYPTREC GL-3002-1.0)[13] -「TLS 暗号設定ガイドライン」(CRYPTREC GL-3001-3.0.1)[14]	＝ 5.5-7 5.5-8	＝	○ 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。	＝ 6-4	◎	＝ 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

2.2.2 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 2-5 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	ESTI EN303 645	NIST IR8425	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 2.2.1 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 2.2.1 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。	＝ 5.11-1 5.11-2	＝	＝ CPS.GV-2 CPS.IP-6

SR3-PP-15	★★★	第三者サービス情報基盤	各サービス担当者のアクセス管理	・各サービス担当者によるサービス情報基盤へのアクセスに対して、適切なアクセス管理を行うこと。	＝ 5.6-7	＝	＝ CPS.AC-2 CPS.AC-3 CPS.AC-5 CPS.AC-9

2.2.3 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 2-6 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	ESTI EN303 645	NIST IR8425	CPSF
SR2-H-1	★★	ホームゲートウェイ	IoT 機器セキュリティ要件（レベル１）への対応	IoT 機器セキュリティ要件（レベル１）に対応し、適合基準を満たしていること。	＝	＝	＝ CPS.IP-1 CPS.IP-6 CPS.PT-2
SR2-H-2	★★	ホームゲートウェイ	認証	・接続する対応機器が正規の機器かどうかを識別、認証する仕組みを有すること。	＝ 5.5-4 5.5-5	＝	＝ CPS.AC-3 CPS.AC-9

SR2-H-3	★★	ホームゲートウェイ	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。	＝ 5.5-7 5.5-8	＝	○ 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	○ 5.10-1	◎	＝ 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	＝ 5.6-3	◎	○ 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、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。	○ 5.3-1 5.3-2 5.3-7	＝	＝ CPS.DS-7 CPS.MA-1

					5.3-8 5.3-9 5-3-10		
SR3-H-1	★★★	ホームゲートウェイ	ホームゲートウェイのレベル２要求事項への対応	・ホームゲートウェイのレベル２要求事項に対応し、適合基準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対策を行い、脆弱性スキャンを実施すること。 ※IPA「安全なウェブサイトの作り方」[7]	○ 5.13-1	◎	○ CPS.CM-3
SR3-H-4	★★★	ホームゲートウェイ	通信経路の暗号化	・情報基盤（クラウド）及び、接続する対応機器との通信に情報資産が含まれる場合、通信経路の暗号化を行うこと。 ・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。 【暗号技術に関連するガイドライン】	○ 5.5-1	＝	○ CPS.DS-3

				-「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 暗号リスト)」（最終改訂: 2022 年 3 月 30 日、CRYPTREC LS-0001-2022）[8] -「暗号強度要件（アルゴリズム及び鍵長選択）に関する設定基準」（初版：2022 年 6 月、CRYPTREC LS-0003-2022）[9] 【上記ガイドラインの補足文書】 -「CRYPTREC 暗号技術ガイドライン（SHA-1）改定版」（CRYPTREC GL-2001-2013R1)[10] -「CRYPTREC 暗号技術ガイドライン(軽量暗号)」(CRYPTREC GL-2003-2016JP)[11] -「暗号鍵設定ガイダンス」(CRYPTREC GL-3003-1.0)[12] -「暗号鍵管理システム設計指針（基本編）」(CRYPTREC GL-3002-1.0)[13] -「TLS 暗号設定ガイドライン」(CRYPTREC GL-3001-3.0.1)[14]			
SR3-H-5	★★★	ホームゲートウェイ	データの暗号化	・ホームゲートウェイが保持するデータにおいて、保護すべき資産に該当するものは暗号化による保護を行うこと。	○ 5.4-1 5.8-1	＝	○ CPS.DS-2

				※保護すべき資産として取り扱うデータは、リスク分析の結果を踏まえ、対象を明確化すること。 ・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。 【暗号技術に関連するガイドライン】 -「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 暗号リスト)」（最終改訂: 2022 年 3 月 30 日、CRYPTREC LS-0001-2022）[8] -「暗号強度要件（アルゴリズム及び鍵長選択）に関する設定基準」（初版：2022 年 6 月、CRYPTREC LS-0003-2022）[9] 【上記ガイドラインの補足文書】 -「CRYPTREC 暗号技術ガイドライン（SHA-1）改定版」（CRYPTREC GL-2001-2013R1)[10] -「CRYPTREC 暗号技術ガイドライン(軽量暗号)」(CRYPTREC GL-2003-2016JP)[11] -「暗号鍵設定ガイダンス」(CRYPTREC GL-3003-1.0)[12]			

				-「暗号鍵管理システム設計指針（基本編）」(CRYPTREC GL-3002-1.0)[13] -「TLS 暗号設定ガイドライン」(CRYPTREC GL-3001-3.0.1)[14]			
SR3-H-6	★★★	ホームゲートウェイ	鍵管理	・暗号化に使用する鍵や証明書は、以下のガイドラインを参考とし、不正なアクセスや変更から保護すること。 -「暗号鍵設定ガイダンス」(CRYPTREC GL-3003-1.0)[12] -「暗号鍵管理システム設計指針（基本編）」(CRYPTREC GL-3002-1.0)[13] -「TLS 暗号設定ガイドライン」(CRYPTREC GL-3001-3.0.1)[14]	＝ 5.5-7 5.5-8	＝	○ CPS.DS-5
SR3-H-7	★★★	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。	＝ 5.10-1	＝	＝ CPS.MA-2
SR3-H-8	★★★	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。	○ 5.10-1	◎	○ CPS.CM-7

2.2.4 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 2-7 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	ESTI EN303 645	NIST IR8425	CPSF
SR2-D-1	★★	スマートホーム対応機器群	IoT 機器セキュリティ要件（レベル１）への対応	・IoT 機器セキュリティ要件（レベル１）に対応し、適合基準を満たしていること	＝	＝ 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	・ホームゲートウェイからの認証要求に応答する仕組みを有すること。	＝ 5.5-4 5.5-5	＝	＝ CPS.AC-3 CPS.AC-9
SR2-D-3	★★	スマートホーム対応機器群	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。	＝ 5.5-7	＝	＝ 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	＝ 5.6-3	◎	○ 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。	○ 5.3-1 5.3-2 5.3-7 5.3-8 5.3-9 5-3-10	＝	＝ CPS.DS-7 CPS.MA-1
SR3-D-1	★★★	スマートホーム対応機器群	対応機器のレベル２要求事項への対応	・対応機器のレベル２要求事項に対応し、適合基準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、通信に情報資産が含まれる場合、通信経路の暗号化を行うこと。 ・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。	○ 5.5-1	＝	○ CPS.DS-3

				【暗号技術に関連するガイドライン】 -「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 暗号リスト)」（最終改訂: 2022 年 3 月 30 日、CRYPTREC LS-0001-2022）[8] -「暗号強度要件（アルゴリズム及び鍵長選択）に関する設定基準」（初版：2022 年 6 月、CRYPTREC LS-0003-2022）[9] 【上記ガイドラインの補足文書】 -「CRYPTREC 暗号技術ガイドライン（SHA-1）改定版」（CRYPTREC GL-2001-2013R1)[10] -「CRYPTREC 暗号技術ガイドライン(軽量暗号)」(CRYPTREC GL-2003-2016JP)[11] -「暗号鍵設定ガイダンス」(CRYPTREC GL-3003-1.0)[12] -「暗号鍵管理システム設計指針（基本編）」(CRYPTREC GL-3002-1.0)[13] -「TLS 暗号設定ガイドライン」(CRYPTREC GL-3001-3.0.1)[14]			

SR3-D-3	★★★	スマートホーム対応機器群	鍵管理	・暗号化に使用する鍵や証明書は、以下のガイドラインを参考とし、不正なアクセスや変更から保護すること。 -「暗号鍵設定ガイダンス」(CRYPTREC GL-3003-1.0)[12] -「暗号鍵管理システム設計指針（基本編）」(CRYPTREC GL-3002-1.0)[13] -「TLS 暗号設定ガイドライン」(CRYPTREC GL-3001-3.0.1)[14]	＝ 5.5-7 5.5-8	＝	＝ 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。	＝ 5.9-3	◎	＝ 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

2.2.5 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 2-8 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	ESTI EN303 645	NIST IR8425	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。 A)Android アプリ - JSSEC『Android アプリのセキュア設計・セキュアコーディングガイド』[15] B)iOS アプリ - Apple『Secure Coding Guide Section:App security』[16] C)Web アプリケーション（PWA） IPA『安全なウェブサイトの作り方』[7]	◎	◎	＝ 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	＝ 5.3-1 5.3-2 5.3-7 5.3-8 5.3-9 5-3-10	＝	＝ CPS.DS-7 CPS.MA-1

3 まとめ

本ガイドライン別紙では、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。

引用/参考文献

[1] NIST IR8425 ″Profile of the IoT Core Baseline for Consumer IoT Products″, NIST
https://nvlpubs.nist.gov/nistpubs/ir/2022/NIST.IR.8425.pdf

[2] ETSI EN 303 645 ″Cyber Security for Consumer Internet of Things: Baseline Requirements″, ETSI
https://www.etsi.org/deliver/etsi_en/303600_303699/303645/02.01.01_60/en_303645v020101p.pdf

[3] 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
https://www.soumu.go.jp/main_content/000428393.pdf

[4] 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/policy/netsecurity/wg1/CPSF_ver1.0.pdf

[5] IoT 機器セキュリティ要件ガイドライン 2023 年版_ver1.0(CCDS-GR01-2023)、CCDS サーティフィケーション WG
https://www.ccds.or.jp/public/document/other/CCDS_SecGuide-IoTReq_2023_v1.0_jpn.pdf

[6] IoT 機器セキュリティ要件_適合基準ガイドライン 2023 年版_ver1.0(CCDS-GRC01-2023)、CCDS サーティフィケーション WG
https://www.ccds.or.jp/public/document/other/CCDS_SecGuide-IoTReq_Criteria_2023_v1.0_jpn.pdf

[7]「安全なウェブサイトの作り方」、IPA
https://www.ipa.go.jp/security/vuln/websecurity/about.html

[8]「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 暗号リスト)」(最終改訂: 2022 年 3 月 30 日、CRYPTREC LS-0001-2022) , CRYPTREC
https://www.cryptrec.go.jp/list/cryptrec-ls-0001-2022.pdf

[9]「暗号強度要件（アルゴリズム及び鍵長選択）に関する設定基準」（初版：2022 年 6 月、CRYPTREC LS-0003-2022），CRYPTREC
https://www.cryptrec.go.jp/list/cryptrec-ls-0003-2022.pdf

[10]「CRYPTREC 暗号技術ガイドライン（SHA-1）改定版」(CRYPTREC GL-2001-2013R1)，CRYPTREC
https://www.cryptrec.go.jp/report/cryptrec-gl-2001-2013r1.pdf

[11]「CRYPTREC 暗号技術ガイドライン(軽量暗号)」(CRYPTREC GL-2003-2016JP)，CRYPTREC
https://www.cryptrec.go.jp/report/cryptrec-gl-2003-2016jp.pdf

[12]「暗号鍵設定ガイダンス」(CRYPTREC GL-3003-1.0)，CRYPTREC
hhttps://www.cryptrec.go.jp/report/cryptrec-gl-3003-1.0.pdf

[13]「暗号鍵管理システム設計指針（基本編）」(CRYPTREC GL-3002-1.0)，CRYPTREC
https://www.cryptrec.go.jp/report/cryptrec-gl-3002-1.0.pdf

[14]「TLS 暗号設定ガイドライン」(CRYPTREC GL-3001-3.0.1)，CRYPTREC
https://www.ipa.go.jp/sec/reports/20170630.html

[15]「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/report/securecoding.html

[16]"Apple Platform Security Section: App sectity"，Apple
https://help.apple.com/pdf/security/en_GB/apple-platform-security-guide-b.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 参画企業

旭化成ホームズ株式会社
株式会社アルファ
積水化学工業株式会社
積水ホームテクノ株式会社
文化シヤッター株式会社
大和ハウス工業株式会社
日本システムウエア株式会社
ミサワホーム株式会社
リンナイ株式会社
YKK AP 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