IoT 機器セキュリティ要件
適合基準ガイドライン 2023 年版
ver. 1.0

一般社団法人
重要生活機器連携セキュリティ協議会

2022 年 11 月 16 日

更新履歴

リビジョン	更新日	更新内容	策定
Draft1	2022/9/1	2023 版の要件に対応し、改定	CCDS
Draft2	2022/10/21	第 1 回諮問委員会での協議内容を反映	CCDS
1.0	2022/11/16	サーティフィケーション WG での意見募集、第 2 回諮問委員会の協議内容を反映し、1.0 版を策定	CCDS

目次

１．本書の目的

本ガイドラインは、「IoT 機器セキュリティ要件 2023 年版」に示されたセキュリティ要件に基づいて、具体的に守るべきセキュリティ機能要件を定義し、その機能要件において検査すべき内容と具体的な検査手法、合格基準について示すものである。

２．CCDS サーティフィケーションマークの対象

CCDS サーティフィケーションマークの付与対象は、インターネットプロトコルを使用可能なハードウェアインタフェース及びソフトウェアインタフェースを実装した機器及びシステムとなる。また IoT 機器において、脆弱性や攻撃が比較的多くみられる Wi-Fi、Bluetooth、USB のインタフェースを有する機器及びシステムについても対象とする（下記図 1～3 を参照）。

図１　対象インタフェースを実装したマーク対象製品の例１：ブロードバンドルータ

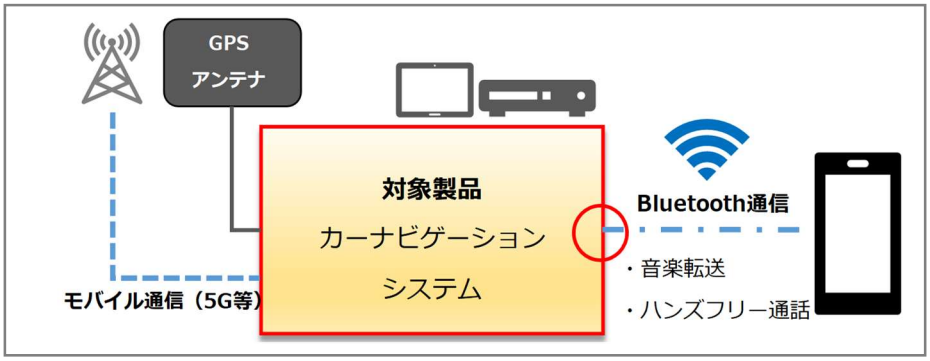

図２　対象インタフェースを実装したマーク対象製品の例２：カーナビゲーションシステム

図３　対象インタフェースを実装したマーク対象製品の例３：ウェブカメラ

３．CCDS サーティフィケーションマークの適合基準

CCDS サーティフィケーションマークの付与にあたっては、対象機器に対するリスクアセスメントが実施されていることを前提とし、７章記載のセキュリティ要件について、適合を必須とする（機能未実装となる要件を除く）。

適合基準は、必ず申請時に CCDS より提示された最新の検査ガイドラインを参照し、検査を行うこと。

また、電気通信事業法に基づく対象機器は、本書の適合基準とは別に、技術基準適合認定の取得が必要となる。

４．指定検証事業者への提出文書や資料

各セキュリティ要件に対する適合確認や、検査結果の証票として、以下の文書を指定検証事業者に提出する。対象機器の設計文書については、提出の必要はないが、マーク取得後の調査に備え、各社で保管しておくこと。

■１）ドキュメント検査において提出が必要な指定ドキュメント

1-1）システムの環境構成及び、要件を示す文書

申請対象機器が実際に運用される環境のシステム構成図を提出すること。

構成図において、他の機器との通信経路は、使用する通信規格や通信プロトコルを明示すること。なお申請者は、提出されたシステム環境構成・要件において申請対象機器が利用されることを保証すること。

1-2）申請対象機器の実装仕様に関するヒアリングシート

各セキュリティ要件において、合格基準への合致していることを示すため、別紙「様式１）CCDS-GR01-2023_適合ヒアリングシート（以下ヒアリングシート）」に必要事項を記載し、提出する。

⇒「様式１）CCDS-GR01-2023_適合ヒアリングシート」

表１　ヒアリングシートにおける記載内容一覧

対象要件	記載内容
1-1	・認証やアクセス制限の対応内容
1-1-1	・開放しているポート番号 ・ポートの利用用途 ・開放されるタイミング/条件
1-1-2	認証情報の設定変更に関する方針
1-2	データ保護に関する方針
1-2-1	設定情報、取得した情報の削除機能に関する方針
1-3	ソフトウェア更新の実装に関する方針
1-4-1	Wi-Fi の実装や認証方式に関する方針
1-4-2	Bluetooth の実装や認証方式、プロファイルに関する方針 OS・ソフトウェアのバージョンについて

1-4-3	USB の実装や利用するデバイスクラスに関する方針
1-4-4～1-4-6	Web 機能の実装に関する方針
2-1	製品の脆弱性に関する報告、相談窓口の対応状況 セキュリティサポート体制の対応状況
2-2	製品に関する文書管理の対応方針
2-3	利用者への情報提供ポリシー
3-1	監査証跡の記録、蓄積に関する実装方針
3-1-1	時間管理機能の実装方針

■２）実機検査において提出が必要な指定ドキュメント

2-1）実機動作を確認した際の動画や、静止画像

対象機器において実機動作を確認した際の、合格基準を満たしている事が証明可能な動画や、静止画像（画面のスクリーンショットや写真)。

2-2）参考検査ツールによる確認結果の出力ログ、レポート

参考検査ツールによる脆弱性スキャンの結果として表示される脆弱性一覧や、検出された脆弱性の個別レポート。参考検査ツールによる検査結果の出力ログなど。

2-3）様式２）検査手順書・結果表に対象機器の検査結果を記入し提出

セキュリティ要件に対する検査結果を指定の記入フォームに記載し、提出する。

・検査結果は OK/NG を明示すること。

・検査実施の日付、実施時のソフトウェアやファームウェアのバージョン、実施者の氏名を記載すること。

⇒「様式２）CCDS-GR01-2023_適合検査手順書・結果表」

５．提出文書の保管

指定検証事業者への提出書類として指定されている文書については、CCDS サーティフィケーションマークのエビデンスとして、申請者及び指定検証事業者は 3 年間保管するものとする。
※ただし、各企業の文書管理規定において、エビデンスの保管期限が 3 年を越える場合は、個社の規定に従うものとする。

６．適合基準の構成

6.1　対象となるセキュリティ要件

本書のセキュリティ要件は、「必須要件」と「推奨要件」に区分している。
「必須要件」は、一般利用者向けの IoT 機器/サービスにおいて対応が必要な要件であり、「推奨要件」は、より高度なセキュリティが要求される IoT 機器/サービスにおいて、必要な要件を定めている。

6.2　適合基準に記載する用語

本書の適合基準に記載する用語を以下に定義する。

表 2　適合基準における用語定義

用語	説明
特権ユーザ	機器のセキュリティ関連機能を含め、重要な構成変更を行う機能に対し、アクセスを許可されたユーザを示す。
監査証跡	対象機器やシステムの処理内容やプロセスを、時系列かつ連続的に記録したものを示す（＝監査ログ）。

6.3　適合基準の構成と観点

本書の適合対象とする IoT 機器セキュリティ要件_2023 年版（CCDS-GR01-2023）を表 3 に示す。
本書では上記セキュリティ要件に対する下記 A~B の観点で適合基準を示している。

・A：申請対象機器の実装に対するドキュメントの確認
・B：実機動作の確認

表 3　CCDS IoT 機器セキュリティ要件_2023 年版（CCDS-GR01-2023）

分類	ID	セキュリティ要件 （サブセットの ID、セキュリティ要件）		要件の対象・目的
1）IoT 機器の機能要件	1-1	**アクセス制御及び認証**		識別、アクセス制御、 構成変更、権限管理、認証
		1-1-1	TCP/UDP ポートの無効化	
		1-1-2	認証情報の変更	
	1-2	**データ保護**		データ保護、 認証情報・鍵情報保護
		1-2-1	データ消去	
	1-3	**ソフトウェア更新**		運用中インシデント対応
	1-4	**特にインシデントが多く影響度が大きい要件**		
		1-4-1	Wi-Fi の認証方式	
		1-4-2	Bluetooth の対策	
		1-4-3	USB のアクセス制御	
		1-4-4	インジェクション対策	
2）IoT 機器の運用における要件	2-1	**連絡窓口・セキュリティサポート体制**		運用中インシデント対応
	2-2	**製品に関する文書管理**		セキュリティ対応状況の 明文化
	2-3	**利用者への情報提供**		運用サポート
3）IoT 機器の監査に関する要件	3-1	**ログの記録**		運用中インシデント管理
		3-1-1	時間管理機能	

6.4　ISO 認証取得による適合基準の充足

以下の ISO 認証を取得している場合、対象となる項目については適合基準を充足しているものとみなし、セキュリティ検査を省略することが可能となる。

表 4　2023 年版要件と ISO 認証規格との対応

※「○」が記載されている項目は、セキュリティ要件を充足とするものとみなし、検査を省略可能

分類	ID	セキュリティ要件		対象となる ISO 認証規格		
		（サブセットの ID、セキュリティ要件）		ISO9001	ISO27001	ISO15408[1]
1）IoT 機器の機能要件	1-1	アクセス制御及び認証				
		1-1-1	TCP/UDP ポートの無効化	－	－	○
		1-1-2	認証情報の変更			
	1-2	データ保護		－	－	－
		1-2-1	データ消去			
	1-3	ソフトウェア更新		－	－	○
	1-4	特にインシデントが多く影響度が大きい要件				
		1-4-1	Wi-Fi の認証方式	－	－	－
		1-4-2	Bluetooth の対策			
		1-4-3	USB のアクセス制御			
		1-4-4	インジェクション対策			
2）IoT 機器の運用における要件	2-1	連絡窓口・セキュリティサポート体制		－	○	－
	2-2	製品に関する文書管理		○	－	－

[1] ISO15408（Common Criteria）については、下記の特定用途機器 共通プロテクションプロファイルに適合した認証を取得している場合のみ、対象となる。また上記に適合している場合、該当要件については推奨要件までを充足するものとみなす。
参考）JISEC　特定用途機器　共通プロテクションプロファイル
https://www.ipa.go.jp/files/000079196.pdf

	2-3	**利用者への情報提供**		○	－	－
3）IoT 機器の監査に関する要件	**3-1**	**ログの記録**		－	－	○
		3-1-1	時間管理機能			

7．セキュリティ要件に対する適合基準

各セキュリティ要件に対する適合基準、検査方法を以下に示す。要件及び適合基準は、特定の条件が付帯されている場合を除き、AND 条件で適合を示すものとする。また実装例については、AND 条件、OR 条件の指定がない場合、申請対象機器の状況によって、選択可能な実装例を示している。

7.1-1　アクセス制御及び認証

対象セキュリティ要件			
分類	ID	セキュリティ要件	要件の対象目的
	サブセットの ID・要件		
1)IoT 機器の機能要件	**1-1**	**アクセス制御及び認証**	**識別、アクセス制御、構成変更、権限管理、認証**
必須要件	① ユーザ（一般ユーザ及び特権ユーザ）や他の IoT 機器によって、対象機器を一意に識別可能な ID を有すること。 ② システム運用上、利用が必要な TCP/UDP 通信については、ユーザや他の IoT 機器からのアクセスに対して、適切な認証、あるいはアクセス制御が行われていること。認証については、デフォルトパスワードは、機器毎に異なる一意の値を設定していること。 ③ ユーザ認証では連続したログイン試行による攻撃への対処として、一定回数を越えるログイン試行に対して特権ユーザあるいは機器の運用（保守）担当者へのアラート通知、あるいは対象アカウントを一定時間無効化する等の対策を行うこと。 ④ 機器のセキュリティ関連機能を含め、重要な構成変更を行う機能についてはユーザを識別、認証し、特権ユーザあるいは機器の運用（保守）担当者以外による機能の実行を制限すること。 ⑤ 障害等によるネットワークの停止後、他機器との接続において、アクセス制御や認証のプロセスを経由し、安全な状態での接続を再確立できること。 **【備考】** 上記②の「デフォルトパスワードは、機器毎に異なる一意の値を設定」については、代替手段として 7.1-1-2 項②に準拠し、初回起動時にユーザによるパスワード変更を必須としている場合は、適合基準を満たすものとする。	
推奨要件	―		
7.1-1A	**適合基準**		
検査手法	ドキュメントによる適合検査		
適合条件	**■必須要件** ・ 提出された指定ドキュメントの記載が、以下の条件に適合する場合、合格の判定が与えられる。 ① ユーザ（一般ユーザ及び特権ユーザ）や他の IoT 機器によって、対象機器を一意に識別可能な ID を有すること。		

	② TCP/UDP 通信では、認証をすること。もしくはアクセス制御によって通信先を制限すること。 ③ 連続したログイン試行による攻撃への対応を行うこと。 ④ 機器のセキュリティ関連機能を含め、重要な構成変更を行う機能へのアクセスは、ユーザまたは特権ユーザを識別し、認証する仕組みを有すること。 ⑤ 障害等によるネットワークの停止後、他機器との接続において、上記②の仕様に従った認証やアクセス制御やのプロセスを経由し、安全な状態での接続を再確立できること。 **【備考】** 上記②の認証については、認証に対応していないプロトコルもしくは、機器の動作に必要な設定を申請者が保証できない場合、例外とする。 例外となるプロトコルの例） - ARP、ICMP（TCP/UDP より下位のレイヤのプロトコルであるため） - DHCP、DNS、NTP（認証に対応していないプロトコルであるため） **■推奨要件** ・ 対象外
実装例	**実装例１）認証及びアクセス制御（必須要件②）** **【A）ユーザ ID とパスワードによるユーザ認証】（AND 条件）** ・ デフォルトパスワードは、MAC アドレス、Wi-Fi®SSID、機器のシリアル・型式番号・名前（略称）などの公開情報、及び固有名詞、単純なパターンの文字列など、容易に推測可能な値を設定していない。 ・ 設定可能なパスワードとして、8 文字以上かつ、英数小文字大文字を混在させることが可能な仕様となっている。 ・ デフォルトパスワードは、機器毎に異なる一意の値を設定している、もしくはパスワードを自動的に生成する仕組みを有する。 ・ パスワードを自動生成する仕組みを実装する場合、生成される値に明確な規則性がなく、類推しやすい値が含まれない仕様となっている。 **【備考】** ・ 英数小文字大文字の組み合わせによる実装が困難な場合には、パスワード長によって同等のエントロピー（値のランダム性）を確保すること。 **【B）機器認証】（OR 条件）** ・ デジタル証明書等を使用した標準的な認証方式に対応する。 ・ Web API の認証において OpenID Authentication※等の標準的な認証方式に対応する。 ※RFC 6749 “The OAuth 2.0 Authorization Framework”への準拠 **【C）多要素認証】**

	・　複数の認証要素を利用した多要素認証に対応する。 **【D）通信アクセス制御】※認証による対応が困難な場合** ・　対象機器の設定（例.Linux の場合 iptables など）の設定により、通信を許可する対象が制限されている。 －例）通信を許可する対象が IP アドレスなどで制限されている。 －例）通信を許可する対象が LAN 内の機器のみに制限されている。
	実装例２）連続したログイン試行攻撃への対応（OR 条件） ・　連続した認証の失敗時には、回数に応じた応答時間の遅延を設けている。 ・　認証の試行回数を制限し、制限回数を超過した場合、ログインを許可しない停止期間を設ける。 ・　認証の試行回数を制限し、制限回数を超過した場合、認証機能をロックする。 ・　暗号に関するベストプラクティスに基づき、認証値に適切なエントロピーを確保する。 ・　ログイン試行が連続した場合に、ユーザ（及び特権ユーザ）あるいは機器の運用（保守）担当者へ通知を行う
提出文書	CCDS が指定するドキュメントの提出
7.1-1B	**適合基準**
検査手法	実機による機能動作の適合性検査
適合条件	**■必須要件** ・　対象機器の実機検証結果が、以下の条件に適合する場合、合格の判定が与えられる。 ①　対象外：7.1-1A に基づきドキュメント検査を実施。 ②　接続機器やユーザアクセスによる認証及びアクセス制御の機能が、仕様に準拠し動作していること。 －設定された認証情報によるアクセスを認可し、それ以外の情報によるアクセスが不認可となっていること。 －仕様に準拠に従い、通信先のアクセス制御が適切に動作していること。 ③　検査手順例に基づくツール検査の結果、設定されたパスワードが解析不能な値となっていること。 ④　連続したログイン試行攻撃への対策機能について、仕様に準拠し正常に動作していること。 ⑤　対象外：7.1-1A に基づきドキュメント検査を実施。 **【備考】** ・　上記③、④については、B）機器認証、C）多要素認証、D）通信アクセス制御による対応が行われている場合は、実施対象外とする。 **■推奨要件** ・　対象外

実機検査手順例	上記③については通常の認証動作に加え、パスワード解析ツールにより、指定の辞書ファイルによるパスワードが認可されない事を確認する。 **【備考】** ・　参考ツール例：THC Hydra（Version9.3 以降） ・　検査用に指定された ID の辞書ファイルを利用すること ・　検査用に指定されたパスワード辞書を利用すること ※指定検証事業者が指定する独自辞書も利用可能とする ※連続したログイン試行攻撃への対応により、辞書ファイルによる実機検査が困難な場合は、パスワード解析ツールによる検査は対象外とする。（通常の認証動作の確認のみを行うものとする）
提出文書	CCDS が求める検査結果及び、検査ログの提出

7.1-1-1　TCP・UDP ポートの無効化

対象セキュリティ要件			
分類	ID	セキュリティ要件	要件の対象目的
	サブセットの ID・要件		
1)IoT 機器の機能要件	1-1	アクセス制御及び認証	識別、アクセス制御、
	1-1-1	TCP・UDP ポートの無効化	構成変更、権限管理、認証
必須要件	①　システム運用上、開放が不要な TCP・UDP ポートは停止しておくこと。 ②　システム運用上、開放が必要なポートについては、脆弱性検査により、所定の合格基準を満たしていることを提示すること。 **【備考】** 脆弱性検査については下記を対象とする。詳細な実施手順や条件については所定の合格基準を参照とする。 ・　TCP/UDP ポートに対するポートスキャンの実施。 ・　開放ポートに対する脆弱性診断（ネットワークスキャン）の実施。		
推奨要件	①　開放している TCP/UDP ポートを識別可能であり、開放/停止を変更できる機能を実装する。 ②　TCP/UDP ポートの開放/停止を変更する機能については、特権ユーザあるいは機器の運用（保守）担当者以外による実行を制限する。		
7.1-1-1A	適合基準		
検査手法	ドキュメントによる適合検査		
適合条件	**■必須要件** ・　提出された指定ドキュメントの記載が、以下の条件に適合する場合、合格の判定が与えられる。 ①　開放（LISTEN）している TCP・UDP ポートを明示し、対象のポート番号、利用用途、開放タイミングや条件が明らかにされていること。 ②　対象外：7.1-1-1B による実機検査を実施。 **■推奨要件** ・　提出された指定ドキュメントの記載が、以下の条件に適合する場合、合格の判定が与えられる。 ①　対象機器が以下の仕組みを有することが明示されている。 －開放している TCP・UDP ポートを機器側で識別可能な仕組みを有する。 －対象ポートは、停止と開放を変更する仕組みを有する。 ②　対象ポートの停止、開放を変更する仕組みは、特権ユーザあるいは機器の運用（保守）担当者以外による実行を制限可能であることが明示されている。		
実装例	－		
提出文書	CCDS が指定するドキュメントの提出		

7.1-1-1B	適合基準
検査手法	実機による機能動作の適合性検査
適合条件	**■必須要件** ・　対象機器の実機検証結果が、以下の条件に適合する場合、合格の判定が与えられる。 ①　ツールによるポートスキャンの結果が、指定ドキュメントに記載の情報と一致していること。 ③　開放ポートに対し、ツールによる既知の脆弱性検査を実施し、Severity7.0 以上のセキュリティ課題が検出されていないこと。 **【備考】** 上記②の脆弱性検査により、CVSSv3 基準 Severity7.0 以上の課題が検出された場合は、開発者を交えた課題の精査を行うこと。精査の結果、セキュリティ課題が下記のいずれかに該当する場合、精査結果の記録を添付することで、脆弱性の対象から除外し、合格条件を満たすものとする（OR 条件）。 1）誤検知である場合 ※検出された脆弱性に対応する機能が、未実装である場合など 2）運用対策を含む対策により、既に対策済みである場合 3）検出された脆弱性が実際の利用環境おいては、影響がない事を証明可能な場合。 4）Exploit Code を用いた実証テストを追加で実施し、攻撃が成功しない場合 **■推奨要件** ・　対象機器の実機検証結果が、以下の条件に適合する場合、合格の判定が与えられる。 ①　対象ポート停止させた際、ツールによるポートスキャンによって停止状態であることが確認できる。 ②　対象ポートの停止、開放を変更する仕組みが、特権ユーザあるいは機器の運用（保守）担当者以外による実行を制限されていることが確認できる。
実機検査手順例	**■必須要件** ①　ポートスキャンツールを使用し、0～65535 までの TCP/UDP ポートの調査を行う。 **【検査ツールのコマンド例（NMAP）】** ・　下記のコマンドで、TCP/UDP の全ポートをポート 1 から順にスキャンを行う。 nmap -r -sS -sU -Pn -p 0-65535 "IP アドレス" ②　脆弱性検査ツールを使用し、ネットワークの脆弱性スキャンを行う。 **【検査ツールの設定例（GVM）】** ・　Target の設定 －Port list：「All TCP and Nmap top 100 UDP」 ※ポートスキャンの結果、上記設定に含まれない UDP ポートが検出された場合には、UDP の対象ポートリストを追加して作成し、設定する。 ・　Scan Task の設定

	－Scanner：「OpenVAS Default」 －Scan Config：「Full and fast」 **【備考】** ・　参考ツール例 －ポートスキャン：NMAP（Ver7.93 以降） －脆弱性検査：GVM(OpenVAS)：Ver.21.4 以降、NVTs Version：検査時点で最新のバージョン ・　動作モードによって、開放されるポートの状態が変更となる場合は、それぞれのモードで不要なポートのスキャン及び、脆弱性検査を行う。
提出文書	CCDS が求める検査結果及び、検査ログの提出

7.1-1-2 認証情報の変更

対象セキュリティ要件			
分類	ID	セキュリティ要件	要件の対象目的
	サブセットの ID・要件		
1)IoT 機器の機能要件	1-1	アクセス制御及び認証	識別、アクセス制御、
	1-1-2	認証情報の変更	構成変更、権限管理、認証
必須要件	① 認証情報の設定変更を可能とし、ユーザ ID 及びパスワードなどの認証情報がハードコーディングされていないこと。 ② デフォルトパスワードが機器毎に異なる一意の値を設定できない場合、初回起動時にユーザによるパスワード変更を必須とする機能を実装すること。 ③ 認証情報の設定変更機能は、特権ユーザあるいは機器の運用（保守）担当者以外による機能の実行を制限すること。		
推奨要件	―		
7.1-1-2A	適合基準		
検査手法	・ ドキュメントによる適合検査		
適合条件	**■必須要件** ・ 提出された指定ドキュメントの記載が、以下の条件に適合する場合、合格の判定が与えられる。 ① 認証情報を変更可能な機能の実装及び、ユーザ ID 及びパスワードなどの認証情報がハードコーディングされていないこと明示されていること。 ② デフォルトパスワードが機器毎に異なる一意の値が設定されていること、もしくは初回起動時にユーザによるパスワード変更を必須とする機能の実装が明示されていること。 ③ 認証情報の変更機能が、特権ユーザあるいは機器の運用（保守）担当者以外による実行を制限されていることが明示されていること。 **【備考】** ・ 上記②、③については、7.1-1A 実装例に記載の「パスワードを自動生成する仕組み」、もしくは B）機器認証よる対応を実装する場合、本項の適合基準を満たすものとする。 ・ 本項については、7.1-1A 実装例記載の D）通信アクセス制御による対応が行われている場合は、実施対象外とする。 **■推奨要件** ・ 対象外		
実装例	―		
提出文書	CCDS が指定するドキュメントの提出		
7-.1-1-2B	適合基準		
検査手法	実機による機能動作の適合性検査		

適合条件	**■必須要件** ・　対象機器の実機検証結果が、以下の条件に適合する場合、合格の判定が与えられる。ただし、②については機器毎に異なる一意のパスワードを設定できない場合に限り、対応を必須とする。 ①　設定変更後、変更された認証情報によるアクセスを認可し、それ以外の情報によるアクセスが不認可となっていることが実機の動作により確認できること。 ②　デフォルトパスワードが機器毎に異なる一意の値を設定できない場合、初回起動時にユーザによるパスワード変更を必須とする機能が実装されていること。 ③　認証情報の変更機能は、特権ユーザあるいは機器の運用（保守）担当者以外による実行を制限されていること。 **■推奨要件** ・　対象外
実機検査手順例	実機を使用したシステムテストによって、確認を行なう。
提出文書	CCDS が求める検査結果及び、検査ログの提出

7.1-2 データ保護

対象セキュリティ要件			
分類	ID	セキュリティ要件	要件の対象目的
	サブセットの ID・要件		
1)IoT 機器の機能要件	1-2	データ保護	データ保護、認証情報・鍵情報保護
必須要件	① 機器本体のストレージ領域へ保存される情報資産については、不正なアクセスや変更から保護することができること。(SD カード等、ストレージメディアに格納するデータについても同様とする) ② 他の IoT 機器やサーバ(クラウド上のサーバを含む)へ送信される情報資産について、情報の漏えいや変更から保護することができること。 ③ 機器内に認証情報(パスワード、秘密鍵など)を保存する場合、ネットワーク経由での不正アクセス(改ざん、盗聴など)から保護された領域で管理すること 。 **【備考】** ・ 情報資産として取り扱うデータについては、製品/サービスごとにリスク分析を行い、対象となる情報を明確化しておく。		
推奨要件	① 暗号化及び改ざん防止対策を行い、採用する暗号方式や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。 ② 暗号化に使用する鍵や証明書は、不正なアクセスや変更から保護する。 **【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-0001-2012R7) - 「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) **【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) - 「CRYPTREC 暗号技術ガイドライン(軽量暗号)」(CRYPTREC GL-2003-2016JP) - 「暗号鍵設定ガイダンス」(CRYPTREC GL-3003-1.0) - 「暗号鍵管理システム設計指針(基本編)」(CRYPTREC GL-3002-1.0) - 「TLS 暗号設定ガイドライン」(CRYPTREC GL-3001-3.0.1)		
7.1-2A	適合基準		
検査手法	・ ドキュメントによる適合検査		
適合条件	**■必須要件** ・ 提出された指定ドキュメントの記載が、以下の条件に適合する場合、合格の判定が与えられる。		

	① 保護すべき情報資産が特定されており、不正なアクセスや変更からの保護対策が行われていること。 ② 他の IoT 機器やサーバ（クラウド上のサーバを含む）へ送信される情報資産について、情報の漏えいや変更に対する保護対策が行われていること。 ③ 機器内に認証情報（パスワード、秘密鍵など）がネットワーク経由での不正アクセス（改ざん、盗聴など）から保護されており、その保護対策が行われていること。 **■推奨要件** ・ 提出された指定ドキュメントの記載が、以下の条件に適合する場合、合格の判定が与えられる。 ① 採用する暗号方式や鍵管理の方法が、標準規格もしくはベストプラクティスに準拠していることが明示されている。 ② 暗号化に使用する暗号鍵や証明書が標準規格もしくはベストプラクティス（推奨要件に文書を例示）に準拠し、不正なアクセスや変更から保護されていることが明示されている。
実装例	**■必須要件** **実装例１）守るべき情報資産への保護対策（OR 条件）** ・ 守るべき情報資産の保護には、市場あるいは社内で実績のあるソフトウェア暗号方式もしくは、ハードウェア暗号方式が採用されている。 ・ 保存されるパスワードはハッシュ化により保護を行う。 ・ 個人情報は匿名加工情報あるいは、仮名加工情報に変換し、保存する。 **実装例２）送信データの保護対策** ・ 対象機器が、常に VPN 環境あるいは、物理専用線を経由した接続環境でのみ使用されている。 ・ 推奨要件記載のドキュメントに準拠し、TLS1.2 以上の暗号方式に対応する。 **■推奨要件** **実装例１）守るべき情報資への保護対策** ・ 守るべき情報資産が、仮想化技術もしくはセキュリティチップによるセキュア領域に保存されている。 ・ 推奨要件記載のドキュメントに準拠し、標準化あるいはベストプラクティスの暗号方式を採用する。 **実装例２）重要なセキュリティパラメータの保護実装例** ・ ETSI EN303 645 においては、パスワードや秘密鍵などを重要なセキュリティパラメータと定義し、下記のような安全なストレージ領域への保存を推奨している。 －信頼された実行環境（TEE： Trusted Execution Environment） －ハードウェアの暗号ストレージもしくはセキュアエレメンツ（SE： Secure Elements）

	－専用のセキュリティコンポーネント（DSC： Dedicated Security Components）、UICC（Universal Integrated Circuit Card） **【備考】** ・ 公開鍵は公開情報であるため、重要なセキュリティパラメータには区分されない。 ・ ストレージだけではなくメモリ上の重要なセキュリティパラメータも同様の実装による保護を推奨している。 **実装例３）通信経路の暗号方式の実装例** ・ 推奨要件記載（7.1-2 の推奨要件参照）のドキュメントに準拠し、TLS1.2 以上の暗号方式に対応する。
提出文書	CCDS が指定するドキュメントの提出
7.1-2B	**適合基準**
検査手法	実機による機能動作の適合性検査
適合条件	**■必須要件** ①～③　対象外：7.1-2A によるドキュメント検査を実施。 **■推奨要件** ・ 対象機器の実機検証結果が、以下の条件に適合する場合、合格の判定が与えられる。 ①　対象外：7.1-2A によるドキュメント検査を実施。 ②　通信経路の暗号化については、通信ログのキャプチャデータを取得し、ログ上の暗号スイートの表記が②の方式と一致する。
実機検査手順例	**■推奨要件　※適合条件③の検査手順例** ・ 通信ログのキャプチャデータを取得（Client Hello のパケット）し、記載されている暗号スィートが標準規格もしくはベストプラクティスに準拠していることを確認する。 **【暗号スィートの記載】** ・ TLS v1.2 まで： TLS_[鍵交換（Kx)]_[認証（Au)]_WITH_[共通鍵暗号（Enc)]_[ハッシュ（Hash/Mac)] ・ TLS v1.3 から： TLS_[AEAD 方式（Enc/Mac)]_[ハッシュ（Hash)]
提出文書	CCDS が求める検査結果及び、検査ログの提出

7.1-2-1　データ消去

対象セキュリティ要件			
分類	ID	セキュリティ要件	要件の対象目的
	サブセットの ID・要件		
1)IoT 機器の機能要件	1-2	データ保護	データ保護、認証情報・鍵情報保護
	1-2-1	データ消去	
必須要件	① 利用者の設定した情報、および機器が利用中に取得した情報は、容易に消去できる機能を有すること。 ② 情報消去後も、更新されたシステムソフトウェアは維持されること 。		
推奨要件	―		
7.1-2-1A	適合基準		
検査手法	ドキュメントによる適合検査		
適合条件	・ 提出された指定ドキュメントの記載が、以下の条件に適合する場合、合格の判定が与えられる。 ① 利用者が変更可能な設定値や、利用中に機器が取得した情報を消去可能な機能の実装が明示されていること。 ② 情報消去後も更新されたシステムソフトウェアバージョンの維持が明示されていること。		
実装例	―		
提出文書	CCDS が指定するドキュメントの提出		
7.1-2-1B	適合基準		
検査手法	実機による機能動作の適合性検査		
適合条件	**■必須要件** ・ 以下の条件に適合する場合、合格の判定が与えられる。 ① 利用者が変更可能な設定値や、利用中に機器が取得した情報を消去可能な機能が仕様通り動作していること。 ② 情報消去後も更新されたシステムソフトウェアバージョンの維持が確認できること。 **■推奨要件** ・ 対象外		
実機検査手順例	実機を使用したシステムテストによって、確認を行なう。		
提出文書	CCDS が求める検査結果及び、検査ログの提出		

7.1-3　ソフトウェア更新

対象セキュリティ要件			
分類	ID	セキュリティ要件	要件の対象目的
	サブセットの ID・要件		
1)IoT 機器の機能要件	1-3	ソフトウェア更新	運用中インシデント対応
必須要件	① ソフトウェア更新が可能なこと。 ② ソフトウェア更新された状態が電源 OFF 後も維持できること。 ③ ソフトウェアを更新後、バージョンの確認が行なえるなど、ソフトウェアのインストールが正常に完了したことを確認する手段を有すること。 ④ 更新対象のソフトウェアについては、更新プロセスを含め、改ざん等がなく、正規のソフトウェアだけをアップデートできることを申請者が保証すること（改ざんへの対策）。 **【備考】** ソフトウェア更新の実行は自動的に開始される方法、あるいは明示的に管理責任を有する保守員や特権ユーザが手動で実施する方法のどちらも要件を満たすものとする。		
推奨要件	① 更新用ソフトウェアをインストールする際、機器側でソフトウェアの真正性を検証する仕組みを有する（改ざんへの対策）。 ② 更新用ソフトウェアは、通信経路の暗号化、あるいは送信時にデータの暗号化を行う（データの保護）。 ③ ソフトウェア更新機能を無効化する機能を実装する場合は、特権ユーザあるいは機器の運用（保守）担当者以外による実行を制限する。 ④ アップデートに関する通知を有効または、無効に変更することが可能である。		
7.1-3A	適合基準		
検査手法	ドキュメントによる適合検査		
適合条件	**■必須要件** ・ 提出された指定ドキュメントの記載が、以下の条件に適合する場合、合格の判定が与えられる。 ① ソフトウェア更新の機能実装が明示されていること。 ② 電源 OFF 後も更新されたシステムソフトウェアバージョンの維持が明示されていること。 ③ ソフトウェアバージョンのインストールが正常に完了したことを確認可能な手段が明示されていること。 ④ ソフトウェアの更新プロセスや更新処理の真正性を確認可能な手段が明示されていること。		

	■推奨要件 ・ 提出された指定ドキュメントの記載が、以下の条件に適合する場合、合格の判定が与えられる。 ① 更新用ソフトウェアをインストールする際、機器側でソフトウェアの真正性を検証する仕組みの実装が明示されている。 ② 更新ソフトウェアの伝送は、通信経路の暗号化、あるいは送信時にデータの暗号化を行うことで保護されている。加えて採用する暗号方式や鍵管理の方法が、標準規格もしくはベストプラクティスに準拠していることが明示されている。 ③ ソフトウェア更新機能を無効化する機能を実装している場合において、特権ユーザあるいは機器の運用（保守）担当者以外による実行の制限が機能として明示されている。 ④ アップデートに関する通知を有効または無効に変更する機能の実装が明示されている。
実装例	**■必須要件** **実装例１）更新ソフトウェアの正常なインストール確認についての実装例** ・ インストールしたソフトウェアのバージョン情報を確認する機能を有する。 ・ インストール失敗時の状態を、ユーザに通知または表示する機能を有する。 **実装例２）ソフトウェアの真正性を保証する手段の例** ・ 社内で承認されたソフトウェアを、明示的に管理責任を有する運用（保守）担当者が直接更新操作を行う（運用対応の場合）。 **■推奨要件** **実装例１）機器側によるソフトウェアの真正性検証の実装例** ・ 更新ソフトウェアウェアをインストールする前に、付与された電子署名との照合を行い、改ざんを検知した場合にはインストールを中止する。 **実装例２）通信経路の暗号方式の実装例** ・ 推奨要記載のドキュメントに準拠し、TLS1.2 以上の暗号方式に対応する。
提出文書	CCDS が指定するドキュメントの提出
7.1-3B	**適合基準**
検査手法	実機による機能動作の適合性検査
適合条件	**■必須要件** ・ 対象機器の実機検証結果が、以下の条件に適合する場合、合格の判定が与えられる。 ① ソフトウェア更新の機能が仕様通り動作し、正常にソフトウェアの更新が可能となること。 ② ソフトウェア更新後に電源 OFF、ON を行った際、更新されたシステムソフトウェアのバージョンが維持されていること。

	③　ソフトウェアバージョンのインストールが正常に完了したことを確認可能な手段が仕様に準拠し、動作していること。 ④　対象外：7.1-3A によるドキュメント検査を実施。 **■推奨要件** ・　対象機器の実機検証結果が、以下の条件に適合する場合、合格の判定が与えられる。 ①　更新用ソフトウェアをインストールする際、機器側でソフトウェアの真正性を検証する仕組みが仕様に準拠し、正常に動作している。 ②　～④：対象外：7.1-3A によるドキュメント検査を実施。
実機検査手順例	**■推奨要件　※適合条件①の検査手順例** ①正規のソフトウェアのバイナリの一部を変更したデータを使用した場合に、更新が実行されず、また機器が正常に使用可能である。
提出文書	CCDS が求める検査結果及び、検査ログの提出

7.1-4　特にインシデントが多く影響度が大きい要件

7.1-4-1　Wi-Fi の認証方式

対象セキュリティ要件			
分類	ID	セキュリティ要件	要件の対象目的
	サブセットの ID・要件		
1)IoT 機器の機能要件	1-4	特にインシデントが多く影響度が大きい要件	―
	1-4-1	Wi-Fi の認証方式	
必須要件	① Wi-Fi Alliance ®（ワイファイ アライアンス）推奨の最新の認証方式が装備されていること。		
推奨要件	―		
7.1-4-1A	適合基準		
検査手法	ドキュメントによる適合検査		
適合条件	■必須要件 ・ 提出された指定ドキュメントの記載が、以下の条件に適合する場合、合格の判定が与えられる。 ① 指定ドキュメントにおいて、Wi-Fi の認証方式が下記基準を満たすことを明示していること。 【Wi-Fi 認証方式の適合基準】 －認証方式：WPA2 以上に対応 －暗号化プロトコル：CCMP と同等以上 －暗号化アルゴリズム：AES（128 ビット以上） －初期設定もしくは設定可能なパスワードとして、8 文字以上かつ、英数小文字大文字を混在させる仕様となっていること。 【備考】 ・ 英数小文字大文字の組み合わせによる実装が困難な場合には、鍵長によって同等のエントロピー（値のランダム性）を確保すること。 ■推奨要件 ・ 対象外		
実装例	―		
提出文書	CCDS が指定するドキュメントの提出		
7.1-4-1B	適合基準		
検査手法	実機による機能動作の適合性検査		
適合条件	■必須要件 ・ 対象機器の実機検証結果が、以下の条件に適合する場合、合格の判定が与えられる。		

	① WPA2 に準拠した認証が実装されており設定された認証情報によるアクセスを認可し、それ以外の情報によるアクセスが不認可となっていること。 **■推奨要件** ・ 対象外
実機検査手順例	上記①については、通常の認証動作に加え、Wi-Fi パスフレーズの解析ツールにより、指定の辞書ファイルによるパスワードが認可されない事を確認する。 【備考】 ・ 参考ツール例：aircrack-ng（Ver1.7 以降） ・ 検査用に指定されたパスワード辞書を利用すること ・ SSID はモニタ可能なため、辞書ファイルを使用しない。 ※指定検証事業者が指定する独自辞書も利用可能とする。
提出文書	CCDS が求める検査結果及び、検査ログの提出

7.1-4-2　Bluetooth の対策

対象セキュリティ要件			
分類	ID	セキュリティ要件	要件の対象目的
	サブセットの ID・要件		
1)IoT 機器の機能要件	1-4	特にインシデントが多く影響度が大きい要件	－
	1-4-2	Bluetooth の対策	
必須要件	① Bluetooth SIG 推奨の最新のペアリング方式が装備されていること。 ② Bluetooth における不要なプロファイルを認識しないこと。 ③ Bluetooth の Blueborne 脆弱性の脆弱性がないこと。		
推奨要件	－		
7.1-4-2A	適合基準		
検査手法	ドキュメントによる適合検査		
適合条件	■必須要件 ・ 提出された指定ドキュメントの記載が、以下の条件に適合する場合、合格の判定が与えられる。 ① ペアリング時の認証方式が以下への準拠を明示していること。 [Bluetooth Classic の場合] －Secure Simple Pairing(SSP モード)に準拠 [Bluetooth Low Energy の場合] －Bluetooth 4.2 以降の LE Secure Connections に準拠 ② 指定ドキュメントにおいて、実装している Bluetooth のプロファイルが以下の基準を満たすことを明示していること。 －利用するプロファイルが明示され、廃止されたプロファイルを利用していない。 －記載されたプロファイル以外は接続時に動作しないよう制限されている。 ③ 指定ドキュメントにおいて、Bluetooth 機能を有している機器が、次のバージョンの OS・ソフトウェアを利用していないことが明示されていること。 [Android] －セキュリティ パッチ レベル 2017 年 9 月を適用していない Android (CVE-2017-0781, CVE-2017-0782, CVE-2017-0783, CVE-2017-0785) [Linux] －kernel 4.13.2 以降 のバージョン －BlueZ 5.47 以降のバージョン [Windows] －2017 年 9 月マイクロソフトセキュリティ更新プログラムを適用していない Windows Vista 以降の Windows (CVE-2017-8628) [iOS, tvOS]		

	－iOS 9.3.5 およびそれ以前、AppleTV tvOS 7.2.2 およびそれ以前 （CVE-2017-14315） **【備考】** ・ 上記①については、SSP を実装していても、下記のモード及び認証方式を使用する場合は、適合条件を満たさないものとする。 A） Bluetooth Classic の場合 －セキュリティモード：「Mode 1:Non-Secure」 －認証方式：「Just works」 B）Bluetooth LE の場合 －セキュリティモード：「LE Security Mode 1:Level 1:セキュリティ無し」 ・ 上記②の廃棄されたプロファイルについては下記を参照。 Bluetooth SIG, Inc "Specifications and Test Documents List"[2] ※「Status：Withdrawn」が廃棄されたプロファイルとなる。 **■推奨要件** ・ 対象外
実装例	－
提出文書	CCDS が指定するドキュメントの提出
7-.1-4-2B	**適合基準**
検査手法	実機による機能動作の適合性検査
適合条件	**■必須要件** ・ 対象機器の実機検証結果が、以下の条件に適合する場合、合格の判定が与えられる。 ① 実機のマニュアル操作において、ペアリングの認証方式として Secure Simple Pairing(SSP)に準拠した動作を行い、正常にペアリングが可能であること。 ② 検査ツール（利用プロファイルの確認用ツール）によるスキャンを実施した結果として、指定ドキュメントに記載したプロファイル以外が検出されないこと。 ③ 検査ツール（脆弱性の確認用ツール）によるスキャンを実施した結果として、次の CVE に該当する脆弱性が検出されていないこと。 －CVE-2017-0782 －CVE-2017-0785 －CVE-2017-1000250 －CVE-2017-1000251 **■推奨要件** ・ 対象外

[2] Bluetooth SIG, Inc "Specifications and Test Documents List"
https://www.bluetooth.com/specifications/specs/?status=withdrawn&show_latest_version=0&show_latest_version=1&keyword=&filter=

実機検査手順例	① 対象機器とのペアリングをマニュアル操作で実施する。 ② 「sdptool」、「nRF connect for Mobile」等のツールを利用し、実装されているプロファイルを確認する。 ③ 適合条件に記載した各脆弱性の有無を PoC ツールにより確認する。 【備考】 ※上記③に記載した CVE の脆弱性は、脆弱性を実証するための PoC ツール（Proof of Concept）が Web 上で公開されており、同ツールでの検査をもって脆弱性の有無を検証する。
提出文書	CCDS が求める検査結果及び、検査ログの提出

7.1-4-3　USB のアクセス制御

対象セキュリティ要件			
分類	ID	セキュリティ要件	要件の対象目的
	サブセットの ID・要件		
1)IoT 機器の機能要件	1-4	特にインシデントが多く影響度が大きい要件	―
	1-4-3	USB のアクセス制御	
必須要件	①　USB インタフェースへの適切なアクセス制御及び、アクセス権限の制限を行うこと。		
推奨要件	①　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。 ②　USB 接続端子（ポート）は、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。		
7.1-4-3A	適合基準		
検査手法	ドキュメントによる適合検査		
適合条件	**■必須要件** ・　提出された指定ドキュメントの記載が、以下の条件に適合する場合、合格の判定が与えられる。 ①　USB インタフェースへの適切なアクセス制御及び、アクセス権限の制限が明示されていること。 **■推奨要件** ①　USB インタフェースの利用用途が明示されており、不要な USB 接続端子（ポート）が利用されていない。 ②　USB 接続端子（ポート）は、運用担当者以外が使用しにくい状態に対策されている。		
実装例	**■必須要件** **USB アクセス制御に関する実装例（OR 条件）** ・　利用する特定のデバイスクラスのみを有効化し、それ以外を無効化する。 －Windows のグループポリシーによる USB の利用制限 －専用ソフトウェアによる、USB ホワイトリストの設定 ・　外部ソリューションによる USB の保護 ・　USBGuard ソフトウェアフレームワークの利用（※Linux Red hat の場合）		
提出文書	CCDS が指定するドキュメントの提出		
7.1-4-3B	適合基準		
検査手法	実機による機能動作の適合性検査		
適合条件	－　※実機検査に該当する項目なし		
実機検査手順例	－		
提出文書	－		

7.1-4-4　インジェクション対策

対象セキュリティ要件			
分類	ID	セキュリティ要件	要件の対象目的
	サブセットの ID・要件		
1)IoT 機器の機能要件	1-4	特にインシデントが多く影響度が大きい要件	―
	1-4-4	インジェクション対策	
必須要件	① Web 入力経由によるインジェクションなどの脆弱性のうち、影響が大きい問題は、対策済みであること。		
推奨要件	―		
7.1-4-4A	適合基準		
検査手法	ドキュメントによる適合検査		
適合条件	**■必須要件** ・ 提出された指定ドキュメントの記載が、以下の条件に適合する場合、合格の判定が与えられる。 ① 対象機器において、http/https プロトコルを使用する設定や機能（Web 機能）の有無を明示し、Web 機能が実装されている場合には、7.1-4-4B の実機検査において、以下の脆弱性が未検出、あるいは対策済みであること。 [対象となる脆弱性] CWE-78：OS コマンドインジェクション CWE-89：SQL インジェクション CWE-352：クロスサイトリクエストフォージェリ（CSRF） CWE-22：パス・トラバーサル **【備考】** 本要件は対象機器が、機器単体もしくはシステム（クラウド連携、スマホ連携含む）において、http/https プロトコルを使用する設定や機能（Web 機能）が実装されている場合に限り、対応を必須とする。（未実装の場合は対応不要） **■推奨要件** ・ 対象外		
実装例	―		
提出文書	CCDS が指定するドキュメントの提出		
7.1-4-4B	適合基準		
検査手法	実機による機能動作の適合性検査		
適合条件	**■必須要件** ・ 対象機器の実機検証結果が、以下の条件に適合する場合、合格の判定が与えられる。		

	① 脆弱性スキャンツールによる既知の脆弱性検査を行い、下記 URL に一覧表示される CVE-ID に該当する脆弱性が検出されないこと。 [URL] https://nvd.nist.gov/vuln/search [検索条件] Search Type: Advanced Category: OS Command Injection SQL Injection Cross-Site Request Forgery (CSRF) Path Traversal **【備考】** 上記①の脆弱性検査により、該当するセキュリティ課題が検出された場合は、開発者を交えた課題の精査を行うこと。精査の結果、セキュリティ課題が下記のいずれかに該当する場合、精査結果の記録を添付することで、脆弱性の対象から除外し、合格条件を満たすものとする（OR 条件)。 1）誤検知である場合 ※検出された脆弱性に対応する機能が、未実装である場合など 2）運用対策を含む対策により、既に対策済みである場合 3）検出された脆弱性が実際の利用環境おいては、影響がない事を証明可能な場合。 4）Exploit Code を用いた実証テストを追加で実施し、攻撃が成功しない場合 **■推奨要件** ・ 対象外
実機検査手順例	① 脆弱性検査ツールを使用し、ネットワークの脆弱性スキャンを行う。 **【検査ツールの設定例（GVM)】** ・ Target の設定 －Port list :「All TCP and Nmap top 100 UDP」 ※ポートスキャンの結果、上記設定に含まれない UDP ポートが検出された場合には、UDP の対象ポートリストを追加して作成し、設定する。 ・ Scan Task の設定 －Scanner :「OpenVAS Default」 －Scan Config :「Full and fast」 **【備考】** ・ 参考ツール例 : GVM(OpenVAS) : Ver.21.4 以降、NVTs Version : 検査時点で最新のバージョン ・ 動作モードによって、開放されるポートの状態が変更となる場合は、それぞれのモードで脆弱性検査を行う。

提出文書	CCDS が求める検査結果及び、検査ログの提出

7.2-1　連絡窓口・セキュリティサポート体制

対象セキュリティ要件			
分類	ID	セキュリティ要件	要件の対象目的
	サブセットの ID・要件		
2)IoT 機器の運用における要件	2-1	連絡窓口・セキュリティサポート体制	運用中インシデント対応
必須要件	①　製品の脆弱性に関する連絡窓口があり、公開していること。 ②　タイムリーな製品のセキュリティアップデートを行う仕組みを有すること。		
推奨要件	－		
7.2-1A	適合基準		
検査手法	ドキュメントによる適合検査		
適合条件	**■必須要件** ・　提出された指定ドキュメントの記載が、以下の条件に適合する場合、合格の判定が与えられる。 ①　製品の脆弱性に関する連絡、問い合わせ用の窓口が整備され、一般に公開されていること。 ②　表面化した対象製品のセキュリティ課題に対して、タイムリーなアップデートが可能な体制及び、プロセスが整備されていること。 **■推奨要件** ・　対象外		
対応例	**製品の脆弱性に関する連絡窓口の例）** ・　連絡、相談先のメールアドレスや、電話番号の掲載、あるいはウェブサイト上で送信フォームなどが整備され、製品利用者に限らず、誰もが問題を連絡可能な仕組みがある。 **セキュリティアップデートの体制、プロセスの例）** ・　PSIRT あるいは、同等の役割を担当する体制を有し、脆弱性の情報収集、トリアージや分析、改善や対策を行うプロセスが整備されている。 ・　上記に加え、アップデートによる対応が必要な課題については、タイムリーな対応が可能な仕組みが整備されている。		
提出文書	CCDS が指定するドキュメントの提出		
7.2-1B	適合基準		
検査手法	実機による機能動作の適合性検査		
適合条件	－　※実機検査に該当する項目なし		
実機検査手順例	－		
提出文書	－		

7.2-2　製品に関する文書管理

対象セキュリティ要件			
分類	ID	セキュリティ要件	要件の対象目的
	サブセットの ID・要件		
2)IoT 機器の運用における要件	2-2	製品に関する文書管理	セキュリティ対応状況の明文化
必須要件	① 製品のライフサイクルを通じて、サイバーセキュリティに関する情報を明確化し、文書として記録、更新を含め管理を行うこと。		
推奨要件	―		
7.2-2A	適合基準		
検査手法	ドキュメントによる適合検査		
適合条件	**■必須要件** ・ 提出された指定ドキュメントの記載が、以下の条件に適合する場合、合格の判定が与えられる。 ① 製品のセキュリティ対応の状況について、対応例と比較し、適切な文書管理が行われていること。 **■推奨要件** ・ 対象外		
対応例	**製品に関する文書管理の例)** ・ **製品構成の把握とサイバーセキュリティ機能の明確化：** ーシステムモデルにおいてはソフトウェア構成及び、ハードウェア構成を明確にすると共に、各機能（サイバーセキュリティ上の機能を含む）を明示すること。 ・ **物理的な使用環境の明確化：** ーユースケースにおいては、物理的な使用環境（設置場所等）や関係するアクター（ステークホルダー）についても明示しておくこと。 ・ **責任分解点の明確化：** ー製品の要件を踏まえ、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。 ・ **保守：** ー保守、メンテナンス業務の要件や手順及び、サイバーセキュリティ上の考慮事項を定義し、文書化する。また、外部委託を行う場合は、委託先の選定要件を定義する。		
提出文書	CCDS が指定するドキュメントの提出		
7.2-2B	適合基準		
検査手法	実機による機能動作の適合性検査		
適合条件	― ※実機検査に該当する項目なし		

実機検査手順例	－
提出文書	－

7.2-3　利用者への情報提供

対象セキュリティ要件			
分類	ID	セキュリティ要件	要件の対象目的
	サブセットの ID・要件		
2)IoT 機器の運用における要件	2-3	利用者への情報提供	運用サポート
必須要件	① 初期設定の方法など、利用上、情報セキュリティ面に影響が生じる設定や使用方法については、安全に利用できる手順を利用者に明示すること。 ② 製品のソフトウェア更新の内容や必要性、更新を行わない場合の影響などを利用者へ周知すること。 ③ 想定される事故や障害に対して、免責事項を利用者へ周知すること。 ④ 対象製品やサービスのサポート期限やサポート終了時の方針を利用者に通知すること。 ⑤ 機器内にデータが残留したまま廃棄することで想定されるリスクや、データ消去を含む機器の安全な廃棄方法を利用者へ周知すること。		
推奨要件	―		
7.2-3A	適合基準		
検査手法	ドキュメントによる適合検査		
適合条件	**■必須要件** ・ 提出された指定ドキュメントの記載が、以下の条件に適合する場合、合格の判定が与えられる。 ① 初期設定の方法など、利用上、情報セキュリティ面に影響が生じる設定や使用方法について、安全に利用できる手順を利用者に明示していること。 ② 製品のソフトウェア更新の内容や必要性、更新を行わない場合の影響などを利用者へ周知する方針が明示されていること。 ③ 想定される事故や障害に対して、免責事項を利用者へ周知する方針が明示されていること。 ④ 対象製品やサービスのサポート期限やサポート終了時の方針を利用者に通知するプロセスが明確に明確であること。 ⑤ 機器内にデータが残留したまま廃棄することで想定されるリスクや、データ消去を含む機器の安全な廃棄方法を利用者へ周知する明示されていること。 **■推奨要件** ・ 対象外		
対応例	**利用者への情報提供の例）** **① 情報セキュリティ面に影響が生じる設定や使用方法の開示例** ・ ユーザ ID 及びパスワード変更の実施手順や、パスワード変更時に特定しにくい値を用		

	いるなど、セキュリティ上、安全な初期設定の方法をマニュアルやウェブページ等で周知する。 **② セキュリティアップデートの情報提供例** ・ セキュリティアップデートについては、以下の情報をウェブページやメール等で情報周知を行う。 **[アップデートの目的]** －機能の追加や変更なのか、あるいは不具合や脆弱性の修正なのかを提示 **[不具合や脆弱性の情報]** －発生する問題の概要と利用者への影響を提示 －問題が発生するソフトウェア/ファームウェアバージョン情報を提示 **[アップデートの方法・手順]** －自動更新かマニュアル操作による更新が必要なのかを提示 －マニュアル操作による更新の場合は、具体的な手順や、アップデートプログラムの入手先（ウェブリンクや URL）を提示 －アップデートにより機器の機能に影響が出る場合、あるいは機器のアップデートの実施が困難である場合は、その理由や対処方法を提示 **[アップデートの実行者]** －利用者側で行うのか、製品提供側（運用あるいは保守担当者など）で行うのかを提示 **③ 想定される事故や障害に対して、免責事項を利用者へ周知** ・ 想定される事故や障害発生時に、製品サポートの範囲として対応すべき内容と、サポート対象外となる免責事項を区別し、利用者へ事前の契約やマニュアル、ウェブページ等で周知を行う。 **④ 対象製品やサービスのサポート期限やサポート終了時の方針周知** ・ 対象製品のサポートの対応期限や、サポート終了時の事前告知期間、サポート終了後の利用者に求める対応について、利用者へ事前の契約やマニュアル、ウェブページ等で周知を行う。 ※上記について、周知を行う方針が整備されている。 **⑤ 機器内にデータが残留したまま廃棄することのリスク、安全な廃棄方法の周知** ・ データ消去を実行せずに廃棄した場合に、残留するデータ（特に認証情報や個人情報）とそれが漏洩した場合のリスク、安全な廃棄を行う上で事前に実施すべき内容についてマニュアル、ウェブページ等で周知を行う。
提出文書	CCDS が指定するドキュメントの提出
7.2-3B	**適合基準**
検査手法	実機による機能動作の適合性検査
適合条件	－ ※実機検査に該当する項目なし
実機検査手順例	－
提出文書	－

7.3-1　ログの記録

対象セキュリティ要件			
分類	ID	セキュリティ要件	要件の対象目的
	サブセットの ID・要件		
3) IoT 機器の監査に関する要件	3-1	ログの記録	運用中インシデント管理
必須要件	－		
推奨要件	① 監査証跡の取得機能、蓄積機能を実装し、特権ユーザあるいは機器の運用（保守）担当者）による監査証跡の読み出しを可能とする。 ② 監査証跡については監査に必要な容量を確保※し、監査証跡の保存容量を超過した場合には、古い記録から順次上書きするなど、管理上の対策を行う。 ② 監査証跡は不正な情報削除や変更を防止する対策を行う。 **【備考】** ・ 監査証跡の蓄積は、機器またはサーバ側のいずれか（あるいは双方）が有するものとする。 ・ 必要な容量については、製品ごとの利用用途を踏まえ、別途検討を行うこと。		
7.3-1A	適合基準		
検査手法	ドキュメントによる適合検査		
適合条件	**■必須要件** ・ 対象外 **■推奨要件** ・ 提出された指定ドキュメントの記載が、以下の条件に適合する場合、合格の判定が与えられる。 ① 監査証跡の取得機能、蓄積機能が実装されている。加えて監査証跡の読み出しが権ユーザあるいは機器の運用（保守）担当者）のみ可能であることが明示されている。 ② 監査証跡については監査に必要な容量が仕様定義され、保存容量が超過した場合の管理対策が明示されている。 ③ 監査証跡は、不正な情報削除や変更を防止する対策が明示されている。		
実装例	**取得すべき監査証跡の例）** ・ 監査証跡は、以下のイベントに対して種別や発生日時を記録する。 －ログイン試行（成功時、失敗時）の記録 －閾値を越えるログイン試行の記録と、それに対する機器側の対応の記録 （7.1-1A の実装例２を参照） －保存容量の上限に達した場合の記録、それに対する機器側の対応の記録 （最新の監査証跡を保存する際、削除を行った過去の監査証跡の記録など）		

	－初期状態における管理者識別失敗時の記録 －管理機能の利用記録 －ソフトウェア改ざん検出時の記録 －時間変更時の記録（変更前と変更後の時刻を含む）
提出文書	CCDS が指定するドキュメントの提出
7.3-1B	**適合基準**
検査手法	実機による機能動作の適合性検査
適合条件	**■必須要件** ・　対象外 **■推奨要件** ・　対象機器の実機検証結果が、以下の条件に適合する場合、合格の判定が与えられる。 ①　対象機器より読み出された監査証跡が記録されている。 ②　～③：対象外：7.3-1A によるドキュメント検査を実施
実機検査手順例	－
提出文書	CCDS が求める検査結果及び、検査ログの提出

7.3-1-1　時間管理機能

対象セキュリティ要件			
分類	ID	セキュリティ要件	要件の対象目的
	サブセットの ID・要件		
3) IoT 機器の監査に関する要件	3-1	ログの記録	運用中インシデント管理
	3-1-1	時間管理機能	
必須要件	―		
推奨要件	① セキュリティイベントの監査証跡の発生日時を記録するため、時間管理機能を有する。 **【備考】** ・ 時間管理機能は、機器またはサーバ側のいずれかが有することで、イベントの発生日時が管理できれば要件を満たすものとする。		
7.3-1-1A	適合基準		
検査手法	ドキュメントによる適合検査		
適合条件	**■必須要件** ・ 対象外 **■推奨要件** ・ 提出された指定ドキュメントの記載が、以下の条件に適合する場合、合格の判定が与えられる。 ① セキュリティイベント監査証跡の発生日時を記録するための時間管理機能の実装が、明示されている。		
実装例	―		
提出文書	CCDS が指定するドキュメントの提出		
7.3-1-1B	適合基準		
検査手法	実機による機能動作の適合性検査		
適合条件	**■必須要件** ・ 対象外 **■推奨要件** ・ 対象機器の実機検証結果が、以下の条件に適合する場合、合格の判定が与えられる。 ① 対象機器より読み出された監査証跡において、発生日時が正常に記録されている。		
実機検査手順例	実機を使用したシステムテストによって、確認を行なう。		
提出文書	CCDS が求める検査結果及び、検査ログの提出		

８．本ガイドラインとの関連文書

本ガイドラインに記載したセキュリティ要件と、表 5 に示す海外のセキュリティ文書との比較、対応状況については、別紙「ANNEX1_海外セキュリティガイドライン・標準への対応」を参照のこと。

表 5　ANNEX1 で比較対象とする海外文書

発行機関	発行	文書名
NIST	2022 年 9 月	NIST IR 8425 "Profile of the IoT Core Baseline for Consumer IoT Products"
ETSI	2020 年 6 月	ETSI EN 303 645 v2.1.1 "Cyber Security for Consumer Internet of Things: Baseline Requirements"
EUROPEAN COMMISSION	2022 年 9 月	"ANNEXES to the PROPOSAL FOR A REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUCIL"

本ガイドラインに記載している検査方法については、「CCDS IoT セキュリティ評価検証ガイドライン」[3]を併せて参照のこと。

[3] 「CCDS IoT セキュリティ評価検証ガイドライン 第 1 版」
https://www.ccds.or.jp/public_document/index.html#Verification_guidelines1.0

９．参考文献

本書における参考文献を以下に示す。

【１．暗号技術に関連するガイドライン】

https://www.cryptrec.go.jp/list.html

「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-0001-2012R7）
https://www.cryptrec.go.jp/list/cryptrec-ls-0001-2012r7.pdf

「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）
https://www.cryptrec.go.jp/list/cryptrec-ls-0003-2022.pdf

【２．上記ガイドラインの補足文書】

https://www.cryptrec.go.jp/op_guidelines.html

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

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

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

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

「TLS 暗号設定ガイドライン」(CRYPTREC GL-3001-3.0.1)
https://www.cryptrec.go.jp/report/cryptrec-gl-3001-3.0.1.pdf

【３．海外のセキュリティ要件文書・標準】

NIST IR 8425 "Profile of the IoT Core Baseline for Consumer IoT Products" (NIST)
https://csrc.nist.gov/publications/detail/nistir/8425/final

ETSI EN 303 645 v2.1.1 "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

"ANNEXES to the PROPOSAL FOR A REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUCIL"(EUROPEAN COMMISSION)
https://trade.ec.europa.eu/doclib/docs/2021/december/tradoc_159967.pdf

【４．CCDS 関連ガイドライン】

「CCDS IoT セキュリティ評価検証ガイドライン 第１版」
https://www.ccds.or.jp/public_document/index.html#Verification_guidelines1.0