IoT 機器セキュリティ要件
ガイドライン 2025 年版
: CCDS-GR01-2025
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

2024 年 10 月 7 日

更新履歴

リビジョン	更新日	更新内容	策定
1.0 版	2024/10/7	1.0 版策定	CCDS

■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。

１．本書の目的

本ガイドラインは、つながる機器における最低限守るべき要件(対策レベル：★星一つ)を定義する。本要件は、つながる機器を用いた IoT 機器、及びシステムにおける最低限守るべき要件としての適用を想定する。

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．IoT 機器セキュリティ要件

本書の IoT 機器セキュリティ要件_2025 年版（CCDS-GR01-2025）を一覧として表 1 に示す。また個々の IoT 機器セキュリティ要件の詳細については、表 2 に示す。

表 1　CCDS IoT 機器セキュリティ要件_2025 年版（CCDS-GR01-2025）一覧

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	認証及びアクセス制御		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	

表２　個別の IoT 機器セキュリティ要件詳細

ID	SubID	改定分類	セキュリティ要件		脆弱性の種類	説明（脅威の背景・事例）
１．IoT 機器の機能要件						
1-1	―	変更	認証及びアクセス制認	**■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 TCP/UDP 通信を介した守るべき情報資産へのアクセスは、認証に基づく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及びアクセス制御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。	CWE-287：不適切な認証 CWE-264 ： 認可・権限・アクセス制御	**[脅威の背景]** システム運用上、必要な開放ポートに対して、TCP/UDP セッションでの適切な認証あるいは通信アクセス制御が行われておらず、機器内データの情報漏洩や、権限昇格（管理機能の掌握）等の問題を生じる可能性がある。 **[事例]** ・Wi-Fi 無線ルータ、IP カメラ等 **[参考]** **技術基準適合認定（電気通信事業法令）関連要件** ・規則第 34 条の 10 第 1 号関係 アクセス制御機能 ・同第 4 号関係 電力供給停止時のアクセス制御機能、ソフトウェア維持の機能 **NIST IR8425 関連要件** #1 Asset Identification #2 Product Configuration #4 Interface Access Control

ID	SubID	改定分類	セキュリティ要件		脆弱性の種類	説明（脅威の背景・事例）
				■推奨要件 ―		**ETSI EN 303 645 関連要件** 5.1 No universal default passwords 5.4 Securely store sensitive security parameters 5.5 Communicate securely 5.9 Make systems resilient to outages **セキュリティ要件適合評価及びラベリング制度（JC-STAR）** ＃2、＃4
1-1	1-1-1	変更	TCP・UDP ポートの無効化	**■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。 **■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。	CWE-671：セキュリティに対する管理者制御の欠如（不要な TCP、UDP ポート開放）	**[脅威の背景]** 機能やサービス上必要のない TCP/UDP ポートを開放しておくことで、サイバー攻撃に悪用される恐れがある通信が可能となる。 **[事例]** ・Wi-Fi 無線ルータ、IP カメラ等 **[参考]** **NIST IR8425 関連要件** ※明示される関連要件なし **ETSI EN 303 645 関連要件** 5.6 Minimize exposed attack surfaces **セキュリティ要件適合評価及びラベリング制度（JC-STAR）**

ID	SubID	改定分類	セキュリティ要件		脆弱性の種類	説明（脅威の背景・事例）
				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。		＃13
1-1	1-1-2	変更	認証情報の変更	**■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。 ④ 通信や電源に異常が発生した際、復旧後に設定変更された認証情報を維持していること。 ■推奨要件	CWE-259：パスワードがハードコーディングされている問題 CWE-255：証明書・パスワード管理	**[脅威の背景]** 機器やアプリケーションにアクセスする際の ID とパスワード情報などの認証情報が、ハードコーディングしているケースや、設定変更を不可とする実装により、認証情報が危殆化してしまった場合に対応がとれず、脆弱性につながる。 **[事例]** ・Wi-Fi 無線ルータ、IP カメラ、医療機関システム等 **[参考]** **技術基準適合認定（電気通信事業法令）関連要件** 規則第 34 条の 10 第 2 号関係 アクセス制御機能に係る識別符号の初期状態変更を促す機能 **NIST IR8425 関連要件**

ID	SubID	改定分類	セキュリティ要件		脆弱性の種類	説明（脅威の背景・事例）
				－		#2 Product Configuration #4 Interface Access Control **ETSI EN 303 645 関連要件** 5.1 No universal default passwords 5.4 Securely store sensitive security parameters **セキュリティ要件適合評価及びラベリング制度（JC-STAR）** ＃1、＃3、＃14
1-2	－	新規	データ保護	**■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は、不正なアクセスによる情報の漏洩や改ざんから保護されていること。 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、情報の漏えいや改ざん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による情報の漏洩や改ざんから保護された領域で管理す	CWE-200：情報漏洩 CWE-310：暗号の問題 CWE-255：証明書・パスワード管理	**[脅威の背景]** 本体ストレージやメモリ領域、通信経路において暗号化等のデータ保護対策に不備や脆弱性があり、情報の漏洩につながる。また暗号化に使用される証明書の管理方法の不備や脆弱性から、データ解析につながる可能性がある。 **[事例]** ・Windows、Linux 等の OS、OpenSSL 等のソフトウェアモジュール、医療機器用の画像ビューアなど多数 **[参考]** **NIST IR8425 関連要件** #3 Data Protection

ID	SubID	改定分類	セキュリティ要件		脆弱性の種類	説明（脅威の背景・事例）
				ること。 **■推奨要件** ① 暗号化に使用する鍵や証明書は、標準規格もしくはベストプラクティスに準拠し、不正なアクセスや変更から保護されている。 **【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)		**ETSI EN 303 645 関連要件** 5.4 Securely store sensitive security parameters 5.5 Communicate securely 5.8 Ensure that personal data is secure **セキュリティ要件適合評価及びラベリング制度（JC-STAR）** ＃11、＃12

ID	SubID	改定分類	セキュリティ要件		脆弱性の種類	説明（脅威の背景・事例）
				- 「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)		
1-2	1-2-1	変更なし	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** ー	CWE-226:リソース内の機密情報が再利用前に削除されない	**[脅威の背景]** 機器やアプリケーションが保持するセキュリティ上の設定値、機密情報、プライバシー情報等の削除機能を実装しておらず、廃棄時やリユース時に機密情報やセキュリティ設定値、プライバシー情報などが漏洩する可能性がある。 **[事例]** ・PC、USB メモリスマートフォン **[参考]** **NIST IR8425 関連要件** ※明示される関連要件なし **ETSI EN 303 645 関連要件** 5.11 Make it easy for users to delete user

ID	SubID	改定分類	セキュリティ要件		脆弱性の種類	説明（脅威の背景・事例）
						data **セキュリティ要件適合評価及びラベリング制度（JC-STAR）** ＃15
1-3	ー	変更	ソフトウェア更新	**■必須要件** ① ユーザにとって、容易かつ分かりやすい方法で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完全性を確認可能な手段が明示されていること。 **■推奨要件** ① 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）。	CWE-1277: ファームウェアがアップデート可能となっていない	**[脅威の背景]** ソフトウェアやファームウェアに脆弱性が見つかった場合に、更新を行う機能が実装されていない事で、セキュリティホールを突かれた攻撃を受ける可能性がある。 **[事例]** ・Wi-Fi 無線ルータ、IP カメラ等 **[参考]** **技術基準適合認定（電気通信事業法令）関連要件** 規則第 34 条の 10 第 3 号関係 ソフトウェアの更新の機能 **NIST IR8425 関連要件** #5 Software Update **ETSI EN 303 645 関連要件** 5.3 Keep software updated 5.4 Securely store sensitive security parameters

ID	SubID	改定分類	セキュリティ要件		脆弱性の種類	説明（脅威の背景・事例）
				② 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。 ③ 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。		5.7 Ensure software integrity **セキュリティ要件適合評価及びラベリング制度（JC-STAR）** ＃6、＃7、＃8、#14
1-4	1-4-1	変更なし	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** －	CWE-326：強度を持った暗号化方式で保護していない問題（最新の Wi-Fi 通信方暗号化機能の未実装）	**[脅威の背景]** Wi-Fi 機器において使用される通信暗号化の方式が最新のものではなく脆弱な暗号化プロトコルや、暗号化アルゴリズムが使用されている。 **[事例]** ・Wi-Fi 無線ルータ **[参考]** **NIST IR8425 関連要件** #4 Interface Access Control **ETSI EN 303 645 関連要件** 5.5 Communicate securely **セキュリティ要件適合評価及びラベリング制度（JC-STAR）** ※該当なし

ID	SubID	改定分類	セキュリティ要件		脆弱性の種類	説明（脅威の背景・事例）
1-4	1-4-2	変更なし	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** ―	CWE-287：適切でない認証（最新の Bluetooth ペアリング機能の未実装）	**[脅威の背景]** ① Bluetooth 2.0+EDR 以前の仕様では、ペアリングする機器同士が、共通の「PIN コード」と呼ばれる数字を入力する方式となっている。一般的には「0000」など、4 桁の数字入力による実装が多く、値の決め打ちで攻撃されてしまい、容易にセキュリティが破られる。 ② 不要な Bluetooth のプロファイル実装により、攻撃を受ける可能性がある。 ③ Blueborne の脆弱性が内在している機器を利用することで、第三者に機器を自由に操作されてしまう可能性がある。 **[事例]** ・Bluetooth 2.0+EDR 以前の機器 ・Bluetooth 機能を実装し、Blueborne の脆弱性が潜在する恐れのある OS バージョンを使用している機器 **[参考]** **NIST IR8425 関連要件** #4 Interface Access Control **ETSI EN 303 645 関連要件**

ID	SubID	改定分類	セキュリティ要件		脆弱性の種類	説明（脅威の背景・事例）
						5.6 Minimize exposed attack surfaces **セキュリティ要件適合評価及びラベリング制度（JC-STAR）** ＃13
1-4	1-4-3	変更	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。	CWE-284：不適切なアクセス制御	**[脅威の背景]** 不要なデバイスクラスの実装により、マルウェアなどによる攻撃を受ける可能性がある。 **[事例]** ・USB 実装機器全般 **[参考]** **NIST IR8425 関連要件** #4 Interface Access Control **ETSI EN 303 645 関連要件** 5.6 Minimize exposed attack surfaces **セキュリティ要件適合評価及びラベリング制度（JC-STAR）** ＃13
1-4	1-4-4	変更	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。	CWE-78：OS コマンドインジェクション	**[脅威の背景]** ユーザからの入力に含まれるコマンドの挿入やパス名の操作により、バックエンドのデータベースを改ざんやシステムコマンドの実行、セキュリティチェックの回避等に利用される可

ID	SubID	改定分類	セキュリティ要件		脆弱性の種類	説明（脅威の背景・事例）
				■推奨要件 －	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	能性がある。 **[事例]** ・Wi-Fi 無線ルータ（CVE-2015-6319） ・Wi-Fi 無線ルータ（CVE-2014-7270） ・IP カメラ（CVE-2017-7461） **[参考]** **NIST IR8425 関連要件** #4 Interface Access Control **ETSI EN 303 645 関連要件** 5.13 Validate input data **セキュリティ要件適合評価及びラベリング制度（JC-STAR）** ※該当なし
２．IoT 機器の運用における要件						
2-1	－	変更		**■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体制、プロセスを整備し、その概要を公開すること。 **■推奨要件**	該当 CWE なし	**[背景]** IoT 機器を対象とした国内外のセキュリティ標準において、製品を提供する事業者に対する組織体制や運用に関する基準が示されている。 **[参考]** **NIST IR8425 関連要件** #8 Information and Query Reception **ETSI EN 303 645 関連要件**

ID	SubID	改定分類	セキュリティ要件		脆弱性の種類	説明（脅威の背景・事例）
				－		5.2 Implement a means to manage reports of vulnerabilities 5.3 Keep software updated **セキュリティ要件適合評価及びラベリング制度（JC-STAR）** ＃5
2-2	－	新規	製品に関する文書管理	**■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** －	該当 CWE なし	**[背景]** IoT 機器を対象とした国内外のセキュリティ標準において、製品を提供する事業者に対する組織体制や運用に関する基準が示されている。 **[参考]** **NIST IR8425 関連要件** #7 Documentation **ETSI EN 303 645 関連要件** ※明示される関連要件なし **セキュリティ要件適合評価及びラベリング制度（JC-STAR）** ＃9
2-3	－	新規	利用者への情報提供	**■必須要件** ① 初期設定の方法など、利用上、サイバーセキュリティ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	該当 CWE なし	**[背景]** IoT 機器を対象とした国内外のセキュリティ標準において、製品を提供する事業者に対する組織体制や運用に関する基準が示されている。

ID	SubID	改定分類	セキュリティ要件		脆弱性の種類	説明（脅威の背景・事例）
				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 アップデートを行わない場合に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** ―		**[参考]** **NIST IR8425 関連要件** #9 Information Dissemination #10 Product Education and Awareness **ETSI EN 303 645 関連要件** 5.2 Implement a means to manage reports of vulnerabilities 5.3 Keep software updated 5.11 Make it easy for users to delete user data 5.12 Make installation and maintenance of devices easy **セキュリティ要件適合評価及びラベリング制度（JC-STAR）** ＃16
３． IoT 機器の監査に関する要件						
3-1	―	新規	ログの記録	**■必須要件** ― **■推奨要件**	CWE-778：不十分なロギング	**[背景]** 製品のインシデントレスポンス対応やセキュリティ監査において、事後の分析や対応検討のためには、ログデータ（監査証跡）の取得や記録が必要となる。IoT 機器を対象とした国内外

ID	SubID	改定分類	セキュリティ要件		脆弱性の種類	説明（脅威の背景・事例）
				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。 ③ 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。		のセキュリティ標準においても、サイバーセキュリティの状態認識を目的としたログの記録が要件に組み込まれている。 **[参考]** **NIST IR8425 関連要件** #6 Cybersecurity State Awareness **ETSI EN 303 645 関連要件** 5.2 Implement a means to manage reports of vulnerabilities 5.7 Ensure software integrity **セキュリティ要件適合評価及びラベリング制度（JC-STAR）** ※該当なし
3-1	3-1-1	新規	時間管理機能	**■必須要件** － **■推奨要件**	該当 CWE なし	**[背景]** ログデータ（監査証跡）の時系列に沿った記録、事後の分析過程において、発生日時の適切な時間管理が求められる。

ID	SubID	改定分類	セキュリティ要件		脆弱性の種類	説明（脅威の背景・事例）
				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。		**[参考]** **NIST IR8425 関連要件** ※明示される関連要件なし **ETSI EN 303 645 関連要件** ※明示される関連要件なし **セキュリティ要件適合評価及びラベリング制度（JC-STAR）** ※該当なし

