IoT 機器セキュリティ要件
ガイドライン 2021 年版
: CCDS-GR01-2021
Ver. 2.0

一般社団法人
重要生活機器連携セキュリティ協議会

2021 年 6 月 18 日

更新履歴

リビジョン	更新日	更新内容	策定
1.0 版	2020/11/24	1.0 版リリース	CCDS
2.0 版	2021/6/18	各セキュリティ要件の分類を整理し、要件番号の採番を変更。対応するガイドラインを最新の内容に更新	CCDS

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付与の対象

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ーフェースを実装した機器、及びシステムとなる。

３．IoT 機器セキュリティ要件

個々の IoT 機器セキュリティ要件については、表１に示す通りである。

表１　IoT 機器セキュリティ要件一覧

分類	No.	2019 年要件からの改定分類	サーティフィケーション要件	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	－	未使用な TCP/UDP ポートを外部より使用されないこと	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] ・ETSI EN 303 645　Cyber Security for Consumer Internet of Things: Baseline Requirements　関連案件 ”Minimize exposed attack surfaces” ・NISTIR 8259A　IoT Device Cybersecurity Capability Core Baseline 関連要件 ”Logical Access to Interfaces : The IoT device can restrict logical access to its local and network interfaces, and the protocols and services used by those interfaces, to authorized entities only.”
１．IoT 機器の機能要件	1-2	変更	システム運用上、必要な TCP/UDP セッションにおいて、適切な認証（機器毎にユニークな ID とパスワード）や通	CWE-287：不適切な認証（TCP/UDP ポートの不適切なアクセス管理）	[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

			信アクセス制御が行われていること。		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] ・ETSI EN 303 645　Cyber Security for Consumer Internet of Things: Baseline Requirements 関連案件 ”No universal default passwords” ・NISTIR 8259A　IoT Device Cybersecurity Capability Core Baseline 関連要件 ”Device Identification：The IoT device can be uniquely identified logically and physically.”
1．IoT 機器の機能要件	1-3	変更	・認証情報の設定変更が可能なこと（ハードコーディングされていないこと）	CWE-259：パスワードがハードコーディングされている問題（アクセスコードの不適切な実装・ハードコーディング、変更不可等）	[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] ・医療機関システム [参考] ・『IoT 機器のセキュリティ基準に係る技術基準適合認定』関連要件 ・『カリフォルニア州法』関連要件 ・ETSI EN 303 645　Cyber Security for Consumer Internet

					of Things: Baseline Requirements 関連案件 ” Minimize exposed attack surfaces”
1．IoT 機器の機能要件	1-4	－	・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 ・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	廃棄やリユースを想定した機能実装不備 ・該当 CWE なし	[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] ・ETSI EN 303 645　Cyber Security for Consumer Internet of Things: Baseline Requirements 関連案件 ” Make it easy for users to delete user data”
1．IoT 機器の機能要件	1-5	－	・ソフトウェア更新が可能なこと ・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	ソフトウェアアップデート機能の未実装 ・該当 CWE なし	[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] ・『IoT 機器のセキュリティ基準に係る技術基準適合認定』関連要件 ・ETSI EN 303 645　Cyber Security for Consumer Internet of

					Things: Baseline Requirements 関連案件 ”Keep software updated” ・NISTIR 8259A IoT Device Cybersecurity Capability Core Baseline 関連要件 ”Software Update : The IoT device’s software can be updated by authorized entities only using a secure and configurable mechanism.”
２．IoT 機器特有のインタフェースにおける基準	2-1	－	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	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] ・ETSI EN 303 645 Cyber Security for Consumer Internet of Things: Baseline Requirements 関連案件 ”Communicate securely”
２．IoT 機器特有のインタフェースにおける基準	2-2	要件追加	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 の脆弱性がないこと	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] ・ETSI EN 303 645　Cyber Security for Consumer Internet of Things: Baseline Requirements 関連案件 ” Communicate securely”
２．IoT 機器特有のインタフェースにおける基準	2-3	－	システム運用上、不要なクラスを認識できないこと	USB の不要なクラス利用 ・該当 CWE なし	[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
３．管理者画面における具体的な対策基準	3-1	－	Web 入力経由による SQL インジェクションの不具合がないこと	CWE-89：SQL 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た SQL 構文の無効化が不十分であり、セキュリティチェックの回避や、ステートメントの挿入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に利用される可能性がある。（CWE-TOP6） [事例] ・Wi-Fi 無線ルータ（CVE-2015-6319）

					[参考] ・ETSI EN 303 645　Cyber Security for Consumer Internet of Things: Baseline Requirements 関連案件 ” Validate input data”
3.管理者画面における具体的な対策基準	3-2	－	Web 入力経由によるクロスサイトリクエストフォージェリの不具合がないこと	CWE-352：クロスサイトリクエストフォージェリ	[脅威の背景] ユーザからのリクエストが、適切なフォーマットであるかを検証しないことで発生する脆弱性。攻撃者がクライアントを騙し、意図しないリクエストを Web サーバに送信させる可能性がある。（CWE-TOP7） [事例] ・Wi-Fi 無線ルータ（CVE-2014-7270） [参考] ・ETSI EN 303 645　Cyber Security for Consumer Internet of Things: Baseline Requirements 関連案件 ” Validate input data”
3.管理者画面における具体的な対策基準	3-3	－	Web 入力経由によるパストラバーサルの不具合がないこと	CWE-22：パストラバーサル	[脅威の背景] 外部入力からパス名を作成し、制限されているディレクトリへのアクセスを許してしまう脆弱性。（CWE-TOP11） [事例] ・IP カメラ（CVE-2017-7461） [参考] ・ETSI EN 303 645　Cyber Security for Consumer Internet of Things: Baseline Requirements 関連案件

					”Validate input data”
４．IoT 機器の運用における要件	4-1	新設	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）製品のセキュリティアップデートサポートサイトがあること	・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] ・ETSI EN 303 645　Cyber Security for Consumer Internet of Things: Baseline Requirements”関連案件 ”Implement a means to manage reports of vulnerabilities” NISTIR 8259　Foundational Cybersecurity Activities for IoT Device Manufactures　関連要件 ”Activity 6: Decide what to communicate to customers and how to communicate it.”

