IoT 分野共通セキュリティ要件
ガイドライン 2019 年版
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

2020 年 2 月 26 日

更新履歴

リビジョン	更新日	更新内容	策定
Draft	2018/11/26	新規作成	CCDS
Draft2	2019/3/8	共通要件検討 WG における指摘事項の修正	CCDS
1.0 版	2019/4/11	1.0 版リリース	CCDS
2.0 版	2020/2/26	2.0 版リリース	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．共通要件

個々の共通要件については、以下の通りである。

No.	対象レベル	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	★（共通）	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] ・“UK Code of Practice for consumer IoT security”該当要件 13. Validate input data（入力データを検証する）
2	★（共通）	Web 入力経由によるクロスサイ	CWE-352 ： クロスサイ	[脅威の背景] ユーザからのリクエストが、適切な

		トリクエストフォージェリの不具合がないこと	トリクエストフォージェリ	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] ・“UK Code of Practice for consumer IoT security”該当要件 13. Validate input data（入力データを検証する）
3	★ （共通）	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] ・“UK Code of Practice for consumer IoT security”該当要件 13. Validate input data（入力データを検証する）
4	★ （共通）	未使用の 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] ・“UK Code of Practice for consumer IoT security”該当要件 6. Minimise exposed attack

				surfaces（攻撃対象となる場所を最小限に抑える）
5	★ （共通）	システム運用上、必要なTCP/UDP ポートには、適切なアクセス認証方法（機器毎にユニークなID とパスワード、もしくは外部公開の恐れのない管理されたID とパスワード）で管理されていること	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] 開放されたTCP/UDP ポートに対して、適切なアクセス管理が行われておらず、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] ・“UK Code of Practice for consumer IoT security”該当要件 6. Minimise exposed attack surfaces（攻撃対象となる場所を最小限に抑える）
6	★ （共通）	・認証情報の設定変更が可能なこと ・初めて利用する際、設定変更を促す機能を有すること ・ID とパスワードはハードコーディングをしないこと（初期パスワードは共通でも可とする）	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、ID とパスワード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』該当要件 ・『カリフォルニア州法』該当要件 ・“UK Code of Practice for consumer IoT security”該当要件 1. No Default Password（初期パスワードの利用禁止、認証情報を設定しないと使えないこと）
7	★	・利用者の設定	廃棄やリユ	[脅威の背景]

	（共通）	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	ースを想定した機能実装不備 ・該当 CWE なし	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] ・“UK Code of Practice for consumer IoT security”該当要件 8. Ensure that personal data is protected（個人データの保護を徹底する） 11. Make it easy for consumers to delete personal data（消費者が個人データを容易に削除できるように配慮する）
8	★ （共通）	Wi-Fi 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] ・“UK Code of Practice for consumer IoT security”該当要件 5. Communicate securely（安全に通信する
9	★ （共通）	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	CWE-287：適切でない認証（最新の Bluetooth	[脅威の背景] 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

			ペアリング機能の未実装）	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。 [事例] ・Bluetooth 2.0+EDR 以前の機器 [参考] ・“UK Code of Practice for consumer IoT security”該当要件 5. Communicate securely（安全に通信する）
10	★ （共通）	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 [参考] ・“UK Code of Practice for consumer IoT security”該当要件 6. Minimise exposed attack surfaces（攻撃対象となる場所を最小限に抑える）
11	★ （共通）	・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』該当要件 ・“UK Code of Practice for consumer IoT security”該当要件

				3. Keep software updated（ソフトウェア更新を保持する） 9. Make systems resilient to outages（停電時のシステムの継続性を確保する）