IoT 分野共通セキュリティ要件
ガイドライン 2018 年度版（案）

一般社団法人
重要生活機器連携セキュリティ協議会

2018 年 11 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

■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(星一つ：★)を定義する。本要件は、つながる機器を用いた IoT サービスにおける最低限守るべき要件としても適用を想定する。共通要件には組み入れないが、各分野の特性に合わせて組み入れることが適切な要件についても参考として掲載する。認証要件には、セキュリティ強度や対策する難易度、脅威の影響度などの種々の観点における分類方法がある。

例えば、

共通要件：

★：つながる機器における最低限守るべき共通要件

分野毎に定義される要件：、

★★： 個々の機能に影響を及ぼす脆弱性要件

★★★：生命や財産に影響する脆弱性要件

として整理することができるが、

本要件定義では、

★：分野を問わず最低限守るべき要件

★★：各分野の機能特性に合わせて定義すべき要件

★★★：★★より個々の機能に従う要件

として整理している。

個々の共通要件については、以下の構成で記述している。

２．共通要件の構成

No.	対象認証レベル	認証要件	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	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 構文の排他が不十分であり、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）
2	★	Web 入力経由に	クロスサイ	[脅威の背景]

	（共通）	よるクロスサイトサイ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	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）
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	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）
4	★ （共通）	未使用ポートを外部より使用されないこと	不要サービスポートの解放	[脅威の背景] 機能やサービス上必要のないサービスポートを解放しておくことで、サイバー攻撃に悪用される恐れのある通信が可能となる。 [事例] ・Wi-Fi 無線ルータ、IP カメラ等
5	★ （共通）	システム運用上、必要なポートには、適切なアクセス認証方法（機器毎にユニークな ID/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/パスワード）で管理されていること	オープンサービスポートの不適切なアクセス管理	[脅威の背景] 解放されたサービスポートに対して、適切なアクセス管理が行われておらず、機器内の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
6	★ （共通）	・認証情報の設定変更が可能な	アクセスコードの不適	[脅威の背景] 機器やアプリケーションにアクセス

		こと ・初めて利用する際、設定変更を促すこと ・ID/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） ＊Web 管理画面アクセス時のID/パスワードを対象とし、認証鍵は対象外とする	切な実装（ハードコーディング、変更不可等）	用の ID/パスワード情報などを、ハードコーディングしているケースや、設定変更ができない実装により、ID/パスワードが危殆化してしまった場合の対応ができず、脆弱性につながる。 [事例] ・医療機関システム
7	★ （共通）	・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、容易に消去する機能を有すること ＊ただし、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	[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
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	Wi-Fi の通信方式が最新の方式ではない	[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
9	★ （共通）	・Bluetooth SIG 推奨の最新のペアリング方式が	Bluetooth のペアリング方式が最新	[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

		装備されていること	の方式ではない	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 桁の数字を入力による実装で多く、決め打ち攻撃で容易に破れてしまう。 [事例] ・Bluetooth 2.0+EDR 以前の機器
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 の不要なクラスの利用	[脅威の背景] 不要なデバイスクラスの実装により、BadUSB による攻撃を受ける可能性がある。 [事例] ・USB 実装機器全般
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できない	[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

３．本ガイドラインのアップデート時期

IoT 機器やサービスの拡がり状況に応じて、ガイドラインの見直しが必要である。攻撃の傾向や脆弱性の傾向などを参考に年に一度見直しを行う。