IoT 機器セキュリティ要件ガイドライン別冊

12 要件における解説編

－2021 年版－

生活機器を安全に利用できる社会の実現を目指して。

2021 年 6 月 18 日

一般社団法人 重要生活機器連携セキュリティ協議会

更新履歴

リビジョン	更新日	更新内容	策定
1,0	2019/12/27	2019 年版として新規作成	CCDS セキュリティ技術 WG
2.0	2021/6/18	2021 年版として下記改訂 ・2021 年要件の変更差分を反映 ・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	CCDS サーティフィケーション WG

目的

本解説書により IoT 機器セキュリティ要件ガイドライン(*1)への理解を深め、IoT 機器における
最低限の守るべき要件への対策や評価方法の検討に役立てる。

対象

ユーザ企業

IoT 機器を調達する際のセキュリティ評価ポイントを検討時

ベンダー企業

IoT 機器の開発時のセキュリティ訴求ポイントの検討時

特長

・「IoT 機器セキュリティ要件ガイドライン(*1)」の要件毎に要点を整理
・IoT デバイスからクラウドまでのシステム全体を対象
・IoT 機器における最低限の守るべき要件が疎かになった場合の具体的な事例、脅威を記載
・脅威に対する具体的な対策案を記載

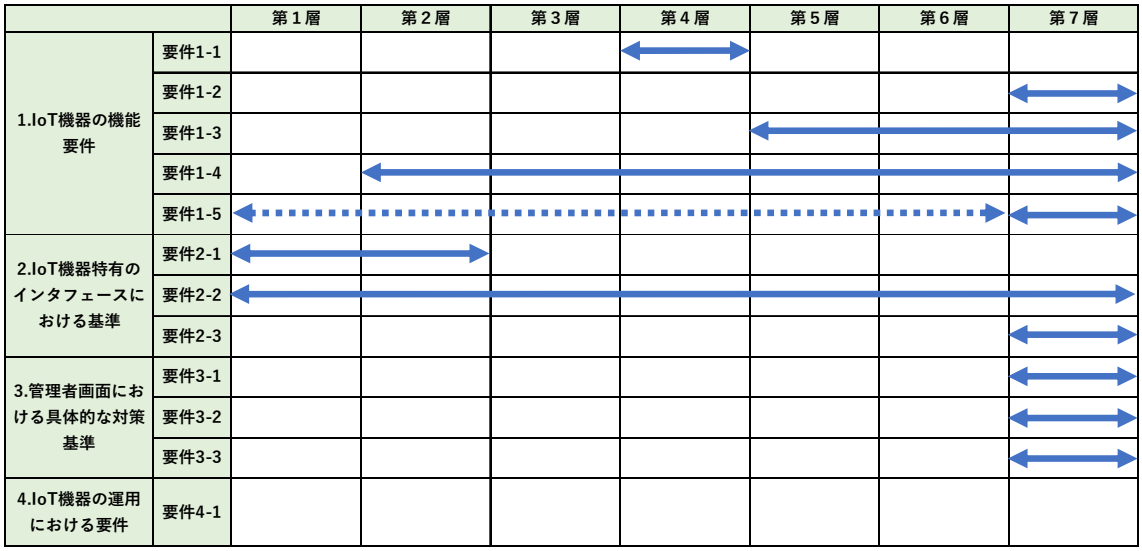
(*1) 一般社団法人 重要生活機器連携セキュリティ協議会
IoT 機器セキュリティ要件ガイドライン 2021 年版

(*1) 一般社団法人 重要生活機器連携セキュリティ協議会
IoT 機器セキュリティ要件 ガイドライン 2021 年版

◆OSI 7 階層

	レイヤー層
第 7 層	アプリケーション層
第 6 層	プレゼンテーション層
第 5 層	セッション層
第 4 層	トランスポート層
第 3 層	ネットワーク層
第 2 層	データリンク層
第 1 層	物理層

◆OSI 7 階層における CCDS の 11 要件の範囲



分類	1．IoT 機器の機能要件	
No	認証要件	脆弱性の種類
1-1	未使用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）

説明（脅威の背景）
[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.“

レイヤー
第 4 層 トランスポート層

経路
・有線 ・無線

モード
・初期設定モード ・管理者モード ・ユーザーモード

事例/脅威（対策しないとこうなると言う記載等）
不要なポートが解放されていると、攻撃者がそこを狙ってデバイスに不正アクセスし、次のような被害を与えます。

・不正なコマンドを実行して、データの改ざんや消去または、重要なファイルを盗み出して漏洩させたりします。
・プログラムを書き換えて、異常な動作をおこさせます。
・マルウェアを送り込んで、サービス不能攻撃などに利用します。
・他の通信機器などを狙って、マルウェアの拡散に利用します。

対応策（ケースバイケースの例を記入）
ポートスキャンを実施し、不要なポートや意図せずに解放されているポートがないか確認し、それらが確認された場合はポートを閉じるよう該当するサービスを停止などの処置を行います。 または、ファイアウォールの機能を用いて必要なポート以外は遮断します。

説明
ポートとはネットワークを介してデータを送受信する際の出入り口で、 デバイス上で起動している複数のアプリケーションやサービスごとに用意されており それぞれを識別するための番号が割り当てられています。 攻撃者は、このポートの開閉状態を調べる行為（ポートスキャン）によってデバイス上で起動しているアプリケーションやサービスの種類、それらバージョンに関する情報、使用しているＯＳに関する情報などを収集し、脆弱性などをついて侵入を図ります。 メンテナンス用として、または意図せずに Tcp ポート番号 23： Telnet などが解放状態であると、攻撃者はそこを狙って不正アクセスを試み、侵入してきます。 IoT 機器を主なターゲットとした「mirai」などマルウェアは、いくつかの経路で侵入を試み感染を拡大して大きな影響を及ぼします。 攻撃者からの不正アクセスを防ぐ上でも、不要なポートが解放されていないか確認し、必要なポート以外は閉じることが重要です。

分類	1．IoT 機器の機能要件	
No	認証要件	脆弱性の種類
1-2	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）や通信アクセス制御が行われていること。	CWE-287 ： 不 適 切 な 認 証（TCP/UDP ポートの不適切なアクセス管理）

説明（脅威の背景）
[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] ・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. “

レイヤー
第 7 層 アプリケーション層

経路
・ネットワーク ・USB ・シリアルポート ※いわゆるサービスポート全般に想定しうる。USB ポートとしているのは USB のデバイスクラスが有効で内部のサービスプログラムが有効の場合に攻撃を成立させることができてしまいます。

モード
初回出荷時

事例/脅威（対策しないとこうなると言う記載等）

■https://www.aterm.jp/support/tech/2016/0330.html

出荷後に発覚、いまだに残る（特にビジネスホテルに多い)。
WEB で管理画面が検索可能になっていた。認証設定なし。
https://github.com/jameshilliad/WECB-WZ
https://github.com/jameshilliad/WECB-VZ-GPL
上記を元にハッカーが基板のファームを解析。
FW のヘッダ等に署名がないため、改竄ファームを書き込む事が可能です。
出荷時に無効化したはずの telnet を有効にできるようになります。
プロセスとして無効化していただけで telnetd 自体は入っています。
MAC アドレスから計算すると（詳細割愛)、バックドアから root のシェルまで取得可能です。

説明
認証機能を実装し、製品出荷時には機器ごとに固有のパスワードを設定します。 初回利用時に強制的に認証の ID/Password を変更するような仕組みが望ましいです。 サービスポートを無効化するときはその機能そのものを利用できないようにプロセスごとファームウェアから取り除くのが望ましいです。 telnetd, sshd など、起動させていないから大丈夫ではなく、それすらも実体が存在せず起動できないのが望ましいです。 ただし、要件#2 が突破されない必要があります。

分類	1．IoT 機器の機能要件	
No	認証要件	脆弱性の種類
1-3	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）

説明（脅威の背景）
[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』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”

レイヤー
第 5~7 層

経路
ネットワーク

モード
初回出荷時

事例/脅威（対策しないとこうなると言う記載等）
機器やアプリケーションのアクセス用 ID/パスワードがハードコーディングされている場合や変更ができない場合、正規の利用者だけでなく、本来の利用者以外の攻撃者もその機器の ID/パスワードの入手さえできれば、機器に容易に不正侵入することが可能とな

ります。その結果、不正な操作や、情報漏洩につながるケースがあります。

IoT 機器の初期の ID/パスワード情報はインターネットでも容易に入手が可能です。
IoT 機器を対象とするマルウェアの多くは、IoT 機器の初期 ID/パスワードをリストとして保持し、リストを元に不正侵入を自動で試みるため、特にインターネットに接続している場合は短時間で不正侵入され、マルウェアに感染することがあります。
代表的なマルウェアとして MIRAI があり、多くの亜種が存在します。

説明
パスワードリスト型攻撃等による不正侵入やその後のマルウェア感染から守るためには、ハードコーディングのような ID/パスワードの変更ができない実装は適切ではありません。 ID/パスワードの変更ができることや、初回利用時に利用者にパスワードの設定変更を促す機能によって確実に初期パスワードから変更されることが望ましく、また、出荷時のパスワードが 1 台ずつ異なるような方法も効果があります。

分類	1．IoT 機器の機能要件	
No	認証要件	脆弱性の種類
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

説明（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”

レイヤー
第 2～7 層

経路
・機器への直接攻撃 ・ネットワークからの不正ログインによる漏洩、改ざん(リユース時)

モード
すべてのモードで起こり得ます。

事例/脅威（対策しないとこうなると言う記載等）
・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ります。 ・製品の開発時にリユースや廃棄後の対策まで検討しておくべきであり、情報が残ってしまうと個人情報漏洩等、会社にとって大きなリスクとなる可能性があります。

対応策（ケースバイケースの例を記入）
・対策例として、廃棄時用に情報の完全消去機能、リユース時用に不要な情報の削除機能を搭載します。

説明
・注意点として、単独では個人情報やプライバシー情報と認識されない情報であっても、複数組み合わせることで個人の特定や嗜好がわかる可能性があるため、利用中に変更される可能性のある情報は、更新されたシステムソフトウェアを除き、すべて削除することが望ましいです。 ・加えて、ファイルシステム上の消去では多くの場合情報の実体が削除されないため、情報の実体が書かれた箇所に対して乱数を書き込む等、情報の実体を確実に削除する必要があります。 ・また、情報の実体を削除したとしても、高度なハッカーであればフォレンジック等により再現できる可能性があるため、ファイルシステム全体を暗号化し、リユース時は出荷状態リセット、廃棄時はファイルシステム暗号化鍵の削除もしくはハードウェアの粉砕により対策することが望ましいです。

分類	1．IoT 機器の機能要件	
No	認証要件	脆弱性の種類
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

説明（脅威の背景）
[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.“

レイヤー
第 7 層 アプリケーション層

経路
・クラウド上 ・USB や CD 等の外部媒体

モード
初期設定/運用設定

事例/脅威（対策しないとこうなると言う記載等）
・アップデートの仕組み 　⇒ファームウェアのアップデート機能がない場合、経時変化により脆弱性が発見された場合の対処が行われない為、そこを突いて狙われウィルス感染等の可能性があります。

・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
⇒電源 OFF 時にソフトウェアが初期出荷状態に戻るデバイスの場合、瞬電等で意図しない電源 OFF が起きた際に管理者が初期出荷状態になった事を把握できません。
（アップデート時のクラウドやソフトウェアの認証の仕組み）
⇒アップデートするソフトが書き換えられていた場合、アップデートを実施しても正しく脆弱性の解決が行われず、悪意あるソフトがインストールされてしまいます。

対応策（ケースバイケースの例を記入）
・[MUST]機器のファームウェアアップデートの機能を、機器の管理者（ユーザーやメーカー保守員）が操作できる機能として提供すること。 ・[MUST]ファームウェアアップデートおよび機器の設定値の変更時はただちに不揮発領域に書き込み、電源 OFF 後も状態を維持すること。 ・[SHOULD]現在のファームウェアバージョンを表示する機能を有するべきです。(管理画面等でファームウェアバージョンを表示するなど) ・[WANT]ファームウェアアップデート機能は、ダウングレードを許可しないことが望ましいです。ダウングレード機能を提供する場合、ボタン押下等の機器の物理操作を伴うなど、ネットワークのみで完結しない仕組みを提供すべきです。 ・[WANT]オンラインでファームウェアが自動配信され自動的にアップデートする機能があると望ましいです。 ・[WANT]ファームウェアに電子署名を付与するなど、ファームウェアの正当性と完全性を検証する機能を付与することが望ましいです。

説明
・アップデートが公開された際に、アップデートを実施する仕組みがあること。 （アップデートするソフトの信頼性が重要で、どこからアップデートするかによるソフトの信頼性を得る必要があります。つまり、アップデートするソフトの信頼性を確認する仕組みがある商品でなければなりません。）

分類	２．IoT 機器特有のインタフェースにおける基準	
No	認証要件	脆弱性の種類
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）

説明（脅威の背景）
[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”

レイヤー
第 1～2 層

経路
・無線からの攻撃(アクセスポイント(AP)のなりすまし、接続機器のなりすまし) ※ AP に対する有線ポートからの攻撃は、アクセスポイントの脆弱性のため対象外とします。

モード
・無線での通信時に起こり得ます。

事例/脅威（対策しないとこうなると言う記載等）
・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ます。これにより、AP のなりすましによる情報漏洩や、不正な接続機器の AP への接続が起こり得ます。 ・Wi-Fi アライアンスが推奨しない方式(WEP 等)を使用すると、脆弱性により情報漏洩等のリスクが存在します。

対応策（ケースバイケースの例を記入）
・Wi-Fi アライアンスが推奨する方式(WPA2, WPA3 等)を使用し、推奨しない方式(WEP 等)は搭載しません。

説明
・Wi-Fi アライアンスが推奨する方式(WPA2, WPA3 等)であっても、脆弱性が発見されることがあります(ex. KRACKs, Dragonblood)。このため、CVE や JVN, NVD 等の脆弱性データベースを定期的に監視し、使用する方式に脆弱性が発見された場合、修正ソフトウェアを適用する必要があります。

分類	２．IoT 機器特有のインタフェースにおける基準	
No	認証要件	脆弱性の種類
2-2	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）

説明（脅威の背景）
[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”

レイヤー
第 1～7 層

経路
・Bluetooth インタフェース ※ハードウェア、ソフトウェアの両側面での対応が出来ていないと攻撃を成立させることは可能です。

モード
・無線での通信時に起こり得ます。

事例/脅威（対策しないとこうなると言う記載等）
・ペアリングしていないケースがほとんどです。悪質な場合、専用アプリと称してアプリなしではペアリングできないような事を説明書に記載して実際には認証なしで接続可能になっていたものもあります。 ・ペアリング時に認証を行っている場合でも、Bluetooth 2.0+EDR 以前の 4 桁の PIN コード認証では値を特定される危険性があります。 ・実際の利用上、不要なプロファイルを実装することで、攻撃を受けた場合に、制御可能な機能が増え、影響が大きくなります。 ・OS バージョンが古い機器では、Blueborne の脆弱性が潜在している可能性があり、遠隔の第三者によって、機器に関連する情報やユーザの個人情報が取得されたり、機器上で任意のコードを実行されたりする可能性があります。 参考）様々な Bluetooth 実装に複数の脆弱性 - JVN https://jvn.jp/vu/JVNVU95513538/

説明
・ペアリング時に認証を行い、Secure Simple Pairing(SSP)など最新の規格に準拠した認証方式を実装していることが求められます。 ・設計段階で実装が必要なプロファイルを明確に定義し、必要最低限のプロファイルのみを実装します。また、利用を許可しないプロファイルについては、接続時に動作しないよう制限を行います。 ・公開された脆弱性情報を確認し、Blueborne の脆弱性が潜在する可能性のある OS・ソフトウェアバージョンを利用しないようにします。また、製品リリース前に、POC ツールなどを活用し、脆弱性スキャンを実施しておくことが望ましいです。

分類	2．IoT 機器特有のインタフェースにおける基準	
No	認証要件	脆弱性の種類
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

説明（脅威の背景）
[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

レイヤー
第 7 層 アプリケーション層

経路
USB ポート

モード
初期出荷設定/運用設定

事例/脅威（対策しないとこうなると言う記載等）
・HID(キーボード、マウス等) 　例えば、利用者が USB メモリとして接続した際に、USB 内にトロイ木馬化した悪意のコードが仕込まれていると、機器の HID が有効であれば乗っ取られてしまいます。 ・Bluetooth 　マルウェアと組み合わせて Buletooth の通信機能を持たせ、外部との接続を可能にし、外部に情報を送ります。 ・マスストレージ（USB メモリー、カードリーダー等） 　USB 機能を持ってない様なデバイスを挿すと、マルウェアが仕込まれていた場合、マストストレージの機能を悪用して実行されてしまいます。

対応策（ケースバイケースの例を記入）
・[MUST]機器が利用可能な USB デバイスクラスを設計資料で明確にすること。 ・[MUST]利用可能な USB デバイスクラスは、機器の要件上最低限のものとすること。

・[MUST]利用を許可しないデバイスクラスのドライバを除去するなどにより、利用を許可しないデバイスクラスの機器を繋いでも認識しないようにすること。

説明
USB ポートのデバイスクラスが初期状態のままで、使用しないデバイスを挿した場合にそのまま使用できる状態は攻撃を受ける可能性があるので、使用するデバイスのみを認識する様にしなければいけません。

分類	3．管理者画面における具体的な対策基準	
No	認証要件	脆弱性の種類
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

説明（脅威の背景）
[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ります。（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”

レイヤー
第 7 層　アプリケーション層

経路
経路には依存しない

モード
モードに依存しない

事例/脅威（対策しないとこうなると言う記載等）
●IoT 機器の接続設定時の攻撃事例 ・IoT 機器の接続設定機能等において、SQL インジェクションの脆弱性が存在した場合、ID/PW によるログイン認証機能、IoT 機器の登録検索機能等にて、入力ボックスに不正な SQL 構文を入力することによる当該機器の情報流出（IoT 機器の MAC アドレス、IoT 機器の識別情報）や、データベースに不正な情報を登録することによる監理者パスワードの設定等の情報改ざんの恐れがあります。 ●IoT 機器で動作する組込みソフトへの攻撃事例 ・IoT 機器の制御をつかさどる組込ソフトにおいて、SQL インジェクションの脆弱性が

存在すると、IoT 機器の管理者に関する機微な情報（ID/PW 等）の流出や改ざん、IoT 機器への乗っ取りといった恐れがあります。乗っ取られた IoT 機器は、新たな攻撃を引き起こす機器となり得ます。
・IoT 機器内のデータベースにある設定情報や制御情報を改ざんすることにより、IoT 機器が意図していない動作や挙動をするといった脅威があります。

対応策（ケースバイケースの例を記入）
・Web サイトや組込みソフトを開発する場合には、IPA サイトを参考にした上、必要なセキュリティ対策を実施し、脆弱性を作りこまないように開発することが望ましく、開発を委託する場合にも、自社で開発する場合と同様に、セキュリティ対策の実施を開発委託先へ要求することが望ましいです。 ・具体的に、SQL インジェクションへの対策として、静的プレースホルダを使用して SQL 文を組み立てることを推奨します。静的プレースホルダを使用できない場合、外部から入力されたデータをエスケープすることでも対応できますが、エスケープのみで対応する場合、データベースの仕様により対策漏れが出やすいため推奨されません。 ・製品開発、もしくは開発委託品の検収の際には、ツールを利用した脆弱性検査を行い、セキュリティ実装の対応状況を確認することが望ましいです。 ・製品リリース後、新たな脆弱性が発見される可能性があるので、定期的に脆弱性検査を行うことが望ましいです。

説明
・一般的には SQL インジェクションとは、Web アプリケーション上での SQL 構文に対して対策を問われるが、Web アプリケーションに限らず、IoT 機器に組み込まれ、動作をつかさどる組込みソフトに関して、外部からの入力あるいは出力時に、想定しない SQL による命令を実行させ、データベースを不正に操作する攻撃にも対策が必要です。

分類	3．管理者画面における具体的な対策基準	
No	認証要件	脆弱性の種類
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	クロスサイトリクエストフォージェリ

説明（脅威の背景）
[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ります。（CWE-TOP7）可能性があります。 [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”

レイヤー
第 7 層　アプリケーション層

経路
経路には依存しない

モード
初期設定モード・管理者モードなど Web アプリを利用できるモード全般

事例/脅威（対策しないとこうなると言う記載等）
クロスサイトリクエストフォージェリの脆弱性が IoT 機器上に存在すると、該当の IoT 機器上に存在する Web アプリで定義された処理が、利用者が意図せず実行されてしまう恐れがあります。 ■意図しない設定の変更 例）アイ・オー・データ製ネットワークカメラにおける脆弱性（JVN#65411235） ・監視カメラの録画データ公開先などが書き換えられてしまいます。 ・管理者パスワードを書き換えられてしまいます。 ・ルータの設定変更により外部からの侵入経路を設けられてしまいます。

■意図しない処理の実行
・決済端末上で不正な取引が計上されてしまいます。
・スマートキーが解錠されてしまいます。

対応策（ケースバイケースの例を記入）
基本的な対策としては、捏造されたコンテンツによって生成された HTTP リクエストであるか否かを区別できるような、ユニークな照合情報（トークン）を HTTP リクエストに埋め込むことです。 （1）hidden トークン HTTP リクエストに照合情報を埋め込み、この照合情報とセッションで保持していた照合情報が等しいかどうかをチェックします。 トークンに用いる値としてはセッション ID があるが、暗号論的擬似乱数生成器による乱数（nonce）を用いる方法もあります。 （2）HTTP ヘッダートークン（X-CSRF-TOKEN） HTTP ヘッダの中の POST パラメータ”X-CSRF-TOKEN”などを用いることで、照合情報が合致しているかをチェックします。 （3）Origin リクエストヘッダ リクエストヘッダに付加した Origin フィールドに含まれるドメインがアクセスを許可した対象ドメインであるかをチェックします。

説明
・Web アプリに対して適切な権限を持たないユーザが、意図しない処理（設定変更・大量の処理等）を埋め込んだ URL や実行ファイルを、正当に Web アプリを利用できる権限を持っているユーザに対し巧妙にカモフラージュさせることなどで実行させた結果、適切なユーザが保持するセッション上で Web アプリの設定をはじめとする意図しない処理を実行することが可能となる脆弱性です。 設定画面や実行画面を外部公開しているのと同等のリスクと考え、十分な対策を講じることが望ましいです。

分類	3．管理者画面における具体的な対策基準	
No	認証要件	脆弱性の種類
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

説明（脅威の背景）
[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。（CWETOP11） [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”

レイヤー
第 7 層　アプリケーション層

経路
ネットワーク

モード
初回出荷時

事例/脅威（対策しないとこうなると言う記載等）
パストラバーサルにより、本来アクセスさせてはいけないファイルに対するアクセスを許してしまいます。適切な対処がされていない場合、パスワードを記載したファイルや、本来公開すべきではないファイルにアクセスされます。 影響としては、ID/パスワードが保存されたファイルの漏えい、個人情報が含まれるファイルの漏えい等の事例が実際にあります。

説明
パストラバーサルはディレクトリトラバーサルとも呼ばれ、本来アクセスを許可していないファイルへのアクセスができてしまう問題です。Web 入力時に直接パスやファイル

名を指定できるような場合に、「../」等を入力することで、上位のパスにあるファイルにアクセスできる場合があります。
対策例：
・直接パスやファイル名を入力させること避けます。
例えば test.txt を返す処理の場合には、入力値として test.txt を受けるのではなく、「テスト」を選択させるような方法が望ましいです。
・入力値を正規化し、不要な指定は削除します。
「../」のような文字列を入力値から取り除く正規化がありますが、この場合、パーセントエンコードされた「%2e%2e%2f」（内部的には「../」と同じ）などの文字を正確に取り除けないケースがあるため、かなり慎重な実装が必要となります。
・適切なアクセス権の付与
アクセスを許可しないパスに対して適切なアクセス権を付与し、不正な入力に対してアクセスできないようにすることも重要となります。
・重要なファイルを Web サーバのドキュメントルート配下に置かないで下さい。
Web サーバのドキュメントルート下に重要なファイルを保存する場合、適切にアクセス権が付与されていないとファイルが漏えいすることがあるため、特に Web サーバ上で直接利用する必要がないものは、別のパスに置くことが望ましいです。

分類	4．IoT 機器の運用における要件	
No	認証要件	脆弱性の種類
4-1	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

説明（脅威の背景）
[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.“

レイヤー
対象外　※機器の運用フェーズ

経路
対象外

モード
対象外

事例/脅威（対策しないとこうなると言う記載等）
・欧米では IoT 機器においても、セキュリティ対策の不備による訴訟が増加しており、既にセキュリティインシデント発生時の対応は、企業の社会的責任として認識されつつあります。脆弱性報告の相談窓口を明示（公開）していない場合、セキュリティ上の問題に気づくことができず、時間の経過と共に、事態がより深刻化する可能性があります。 ・万一、製品に脆弱性が発見された場合にも、ソフトウェアのアップデートにより、修正を行うことが可能ですが、被害を最小限に抑えるためには、製品の利用ユーザに対して、セキュリティアップデートの必要性や実施手順を明確に周知しておく必要があります。

説明
・対象機器において脆弱性やサイバーセキュリティへの影響が懸念される問題が見つかった場合に、報告先となる窓口の情報を公開します。こうした情報は利用者だけでなく、ホワイトハッカーなど、善意の第三者からも有益な情報が得られる可能性があり、問題発生後、迅速な対応を行う上で非常に有効です。 ・セキュリティアップデートのサポートにおいては、利用ユーザに対し、一例として以下のような情報の提供が必要です。 ※セキュリティアップデートの情報提供例 ①アップデートの内容：不具合や脆弱性の修正なのか、機能追加なのか、など ②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など ③アップデートの方法・手順：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）など

■　２０１９年版　制　作　■

利用部会：セキュリティ技術 WG

第一版（2019 年 12 月）

主　　査：富士ソフト株式会社
副 主 査：大日本印刷株式会社
メンバー：トレンドマイクロ株式会社
株式会社ラック
日本シノプシス合同会社
パナソニック アドバンストテクノロジー株式会社
株式会社ソリトンシステムズ
株式会社メタテクノ
日本ダイレックス株式会社
日本プロセス株式会社
マクニカネットワークス株式会社
NTT コミュニケーションズ株式会社
独立行政法人 製品評価技術基盤機構
アイビーシー株式会社
株式会社アリス
アライドテレシス株式会社

オブザーバー：CCDS　荻野　司
横浜市　福田　次郎
アドバイザー：　江川　将偉