JPCERT Coordination Center
電子署名者 : JPCERT Coordination Center
DN : c=JP, st=Tokyo, l=Chuo-ku, o=Japan Computer Emergency Response Team Coordination Center, cn=JPCERT Coordination Center, email=office@jpcert.or.jp
日付 : 2019.06.27 15:14:27 +09'00'

# IoT セキュリティチェックリスト

# 利用説明書

一般社団法人 JPCERT コーディネーションセンター

**2019 年 6 月 27 日**

JPCERT CC®

# 目次

## 1. はじめに

IoT (Internet of Things) とは、物理的な実体をもつ物の状態に関する情報を収集する監視アプリケーションや、収集された情報などをもとに物の状態を変える制御アプリケーションをネットワーク化された分散システムとして実現するという考え方である。それを応用した例として、広大な工場内の生産情報を効率的に収集するため、製造機械の温度計測や制御機能を持っていた個々のデバイスに対して新たに通信機能を持たせ、ネットワークと接続、クラウドサービス等と連携するようなシステムを構築し、情報の集約を行ったりすることが挙げられる。この例に見られるような、新たに通信機能を持たせたデバイスは「IoT デバイス」と呼ばれることがしばしばある。近年、そんな IoT デバイスや IoT の考え方をもとに構築したシステムは注目され、今後急速な普及が見込まれている。

例えば総務省[1]によれば、世界の IoT デバイス数の動向は、2017 年時点でスマートフォンや通信機器などの稼働数の多さに加え、今後、コネクテッドカーの普及により IoT 化の進展が見込まれる「自動車・輸送機器」、デジタルヘルスケアの市場が拡大している「医療」、スマート工場やスマートシティが拡大する「産業用途（工場、インフラ、物流）」などの高成長が予測されており、今後も増加傾向が続くとされている。

一方で、IoT デバイスや IoT の考え方をもとに構築されたシステムは、常時ネットワークに接続されており、多数の同じ IoT デバイスがネットワーク上に接続されているケースが多く、個々の IoT デバイスのセキュリティ管理の徹底が難しいことが多い。

常時ネットワークに多数の機器が接続されて、セキュリティ管理の徹底が難しいということでは、一般消費者向けのブロードバンドルータも IoT デバイスと同様である。ブロードバンドルータに関しては、2016 年頃より Mirai マルウエアによるセキュリティインシデント被害が多数報告された。管理コンソールの認証設定が甘かったり、脆弱性に対するパッチ適用が施されていないなど管理が不適切な機器が Mirai マルウエアに感染しやすい。IoT デバイスでも、普及すれば、Mirai マルウエアに類似した IoT デバイスを対象とするマルウエアが登場し、同様の感染被害が発生することが懸念されるのである。

IoT デバイス等のセキュアな稼働を確保して IoT を安全に利用するためには、IoT デバイス等自体が、脆弱性を持たない等、攻撃に対するセキュリティ的な耐性を備えていることが必要になる。

しかし、IoT デバイスの中には、新機能の作り込みに注意を奪われるあまり、Mirai に感染したブロードバンドルータと同様に、セキュリティ的な耐性に関する設計が忘れ去られているものが少なくない。こうした状況は、IoT デバイスのセキュリティ機能のチェックに簡易に使えるセキュリティチェックリストがあり、IoT デバイスの開発者が設計時にこれを利用するようになれば、大きく改善することが期待できる。

[1] 総務省 ：第 1 部　特集　人口減少時代の ICT による持続的成長(http://www.soumu.go.jp/johotsusintokei/whitepaper/ja/h30/html/nd111200.html)

また、利用者においても、IoT デバイスを使ってシステムを構築する際に、必要なセキュリティ的耐性を備えていることを確認した上で、システムを構成する製品を選定することが重要である。不適切な製品を選べば、サイバー攻撃を受けて、想定どおりにシステムが使えなくなったり、システムが第三者へのサイバー攻撃の踏み台として利用されたりしかねない。しかし、利用者側においても、主たる機能の実現に関心が集中し、セキュリティ上の検討を欠いたまま、構築プロジェクトが進んでいってしまう場合が少なくない。こうした事態も、IoT デバイスのセキュリティ機能のチェックに簡易に使えるチェックリストがあり、IoT デバイスの利用者がシステム構築時にこれを利用するようになれば、回避することが期待できる。

JPCERT/CC では、それらの課題を解決すべく、JNSA IoT セキュリティ WG や長崎県立大学の協力のもと、IoT セキュリティチェックリスト (以下、「チェックリスト」) を開発し公表することにした。チェックリストの開発にあたっては、IoT デバイスの開発者や利用者が簡易に使えるよう、実務的でスリムな内容とするように努めた。確認項目を必要最少限の基本的な項目のみに絞り込んだ上で、各項目について、確認事項と確認が必要な理由を書き込んだ一覧表としてまとめた。

また、本チェックリストでは、各確認項目について、IoT デバイスの開発者がチェックすべきことと、利用者がチェックすべきことを併記する体裁をとった。IoT デバイスの開発者には利用者が懸念する事項に、逆に、利用者には開発者が留意した事項に思いをはせていただくことにより双方の思いが噛み合い、安全な IoT 活用の実現に資するものと期待したからである。

一方で、チェックリストの記載をできるだけ簡潔にしたため、初めは使い方に戸惑うかも知れないと考え、チェックリストの使い方を説明した本書を用意することとした。本書では、第 2 章でチェックリストの全体概要を述べ、第 3 章でチェックリストの利用方法を、例を示しながら解説し、第 4 章では他のガイドと本チェックリストとの関係をまとめている. 本書をご一読の上、チェックリストをご活用いただければ幸いである。

# 2. 本チェックリストの概要と利用すべき場面

## 2.1. 本チェックリストの概要

### 2.1.1. 構成

本チェックリストは、IoT の考え方に基づいて構築されるシステムの全体（以下、IoT システム）が、脅威の存在する環境においても安全に運用するため完備している必要がある 39 のセキュリティの機能をそれが必要な背景とともにまとめて、IoT システムを構成する製品の開発時および導入時の検討に使えるよう一覧表にしたものである。

本チェックリストを利用して、開発中または導入予定の IoT システムの評価を行う事により、その IoT システムのセキュリティを担保する上で必要な機能が備わっているかどうかの判断と更なる検討項目の洗い出しを行う事が出来る。

本チェックリストは次のように構成されている。

(1) IoT セキュリティチェックリスト
IoT システムに必要なセキュリティ機能が装備されていることを確かめるための 39 の確認項目のリスト

(2) IoT セキュリティチェックリスト解説図
IoT セキュリティチェックリストの確認項目についての理解を助けるための解説図集

(3) IoT セキュリティチェックリスト利用説明書 (本書)
IoT セキュリティチェックリストの利用方法についての解説書

### 2.1.2. 利用方法の概要

本チェックリストを用いたセキュリティ機能の評価は、次の 4 段階のステップに沿って進められる。

**ステップ 1： 評価対象の IoT デバイスに含まれる Primitive の決定**

評価を行う IoT デバイスがどの Primitive を持っているかを決定する。複数の Primitive を持っている場合もあることに注意されたい。なお、Primitive の詳細については 2.1.3 を参照して欲しい。

**ステップ 2： 評価する項目の決定**

IoT デバイスに要求される 39 のセキュリティ機能は、「ユーザ管理」、「ソフトウェア管理」、「セキュリティ管理」、「アクセス制御」、「不正な接続」、「暗号化」、「システム設定」、「通知」の 8 種類に大別

することができるが、本チェックリストでは、8 種類のうち一部についてだけ評価する利用も想定している。そのために、この段階で評価したい大項目を選択する。すべてを一通り確認したい場合は、全ての項目を選ぶ。

**ステップ 3：確認を要するチェックリストの部分の抽出**

チェックリストからの、ステップ 1 で特定した Primitive とステップ 2 で決めた大項目に関連する部分だけを残し、それ以外の部分を削除する。

**ステップ 4: セキュリティ機能の評価の実施**

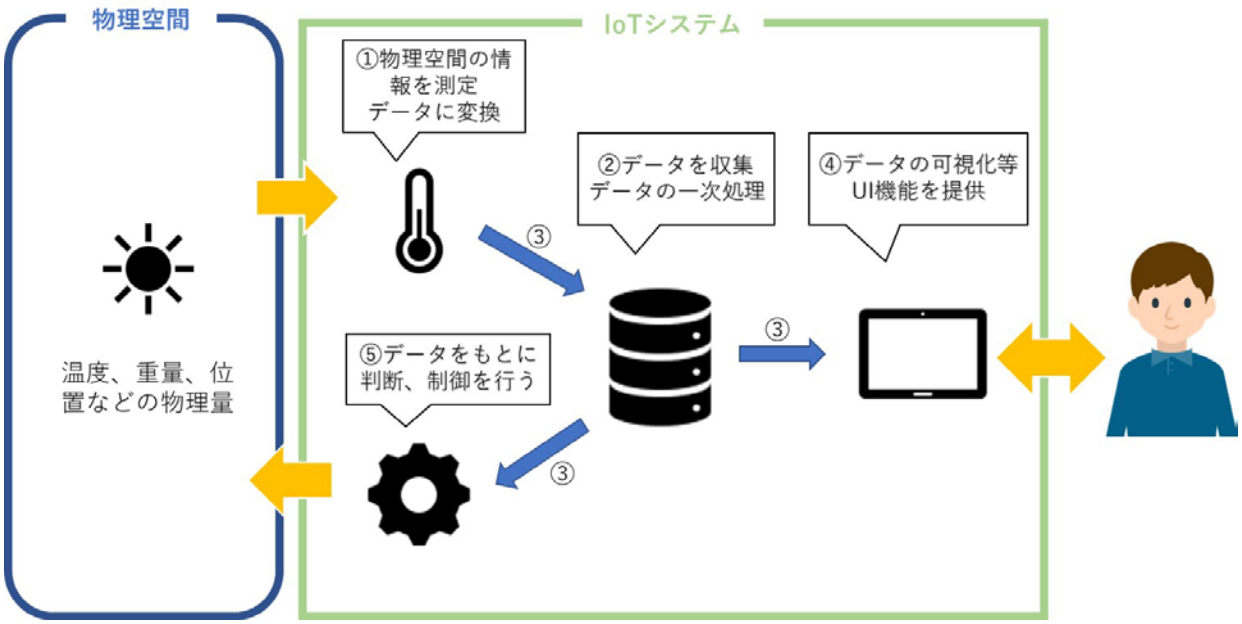
ステップ 3 で抽出されたチェックリストの部分に従って、IoT セキュリティチェックリスト解説図を参考としつつ、評価を行う。

さらに詳細な利用法については 3 章で紹介する。

### 2.1.3. IoT システムの構造と Primitive

本節では、チェックリストを利用する際にステップ 1 で決定される Primitive について述べる。

本チェックリストでは、IoT システムを汎用的に考察するために、機能や役割に応じて要素分解し、その構成要素を Primitive と呼ぶ。IoT システムは、物理空間の情報を収集し、その情報をもとに物の状態を変える制御を行っていることを踏まえると、一般に、[図 1]に示した構造に分解できる。




[図 1:　IoT システムの動き]

①は物理空間の状態を計測し測定データに変換し、そうしたデータを②が収集して一次処理した上で蓄積する。利用者は②に蓄積されたデータを閲覧したり設定したりできるが、そのためのインタフェースを実現するのが④である。また、⑤は、②に蓄積されたデータに基づいて、物の状態を変えるためのアクションを起こす役割を担っている。これらの機能は、ネットワーク上に分散して設置されるので、その間を結ぶ通信の機能③も必要になる。

本チェックリストでは、NIST SP800-183 にならって、①を Sensor、②を Aggregator、③を Communication Channel、④を e-Utility、⑤を Decision Trigger と呼び、①～⑤のような IoT システムを構成する基本単位を Primitive と呼ぶことにする。

| | |
|---|---|
| Sensor | 温度、加速度、重量、音、位置などを測定する機能・機器 |
| Aggregator | センサからのデータを集約する機能・機器 |
| Communication Channel | データの送受信を行うための通信路・ネットワーク |
| e-Utility | データを閲覧したり設定したりするインタフェース |
| Decision Trigger | データを計算し、その結果に基づいてアクションさせるための機能 |

なお、図 1 は単純化された模式図になっているが、実際の IoT システムにおいては、複数の Sensor を含んでいたり、Aggregator や e-Utility がエッジ環境とクラウド環境に分散して実現されていたり等の多様な形態をとるケースがあることにも留意されたい。また、データ収集だけで制御機能を持たないような IoT システムでは Decision Trigger が存在しない。

本チェックリストによる評価の対象となる IoT デバイスには、これらの Primitive のいずれか一つ、または複数の Primitive が実現されているはずである。どの Primitive が評価対象の IoT デバイス上で実現されているかは、それにより評価対象の IoT デバイスに必要なセキュリティ機能が異なるので、正しく見極める必要がある。

### 2.2. 本チェックリストを利用すべき場面

#### 2.2.1 製品開発者が本チェックリストを利用すべき場面とその効果

想定場面：

(A) IoT システムまたはそれを構成する一部となる製品の企画段階または初期の設計段階における基本機能を検討する際に、本チェックリストを利用して、必要なセキュリティ機能が盛り込まれているかどうかを検証する。

期待される効果：

- 製品開発の早い段階でチェックリストを利用することにより、必要不可欠なセキュリティ機能が装備されていることを体系的に確認し、問題点を早期に是正できる。

- 製品に持たせるセキュリティ機能の基準を作ることができ、その基準を他の開発する製品に展開することにより、自組織で開発する製品にて一定のセキュリティを担保できるようになる。
- 早期に問題点を見つけられることにより、開発プロセスの手戻りが減少し、製品が必要なセキュリティ機能を欠いたまま利用者の手に渡りサイバー攻撃を受けるリスクを低減することができる。

### 2.2.2. 製品利用者が本チェックリストを利用すべき場面とその効果

想定場面：

(A) 既存の製品を組み合わせて IoT システムを構築する際に、構築に利用する製品の候補が絞り込まれた段階で、候補製品が必要なセキュリティ機能を完備しているかどうかを確認する。

(B) 導入されている IoT システムを構成するそれぞれの製品について、必要なセキュリティ機能が稼働していることを確認し、仮に機能が欠けていた場合には新たに機器を追加するなどの対策方法を検討する。

期待する効果：

- (A)：セキュリティ機能が完備した製品を選択することにより、サイバー攻撃を受けるリスクを低減することができる。
- (B)：導入済みの IoT システムに不足している機能を割り出し、追加対策で補うことにより、必要なセキュリティ機能を欠いたままでの運用を改め、サイバー攻撃を受けるリスクを低減することができる。

# 3. チェックリストの利用方法

## 3.1. 製品開発者が使う場合のチェックリストの利用方法

### 3.1.1. チェックリストの構造

チェックリストは[図 2]のような表の形式をとっている。表の各行が個々のチェック項目に対応している。各チェック項目に対する各行は[表 1]に示した 9 つの欄で構成されている。


[図 2 IoT セキュリティチェックリスト]

[表 1　IoT セキュリティチェックリストの要素 ]

| No. | 項目名 | 説明 |
|---|---|---|
| ① | No. | チェック項目の番号 |
| ② | Primitive | 「2.1.3. IoT システムの構造と Primitive」にて説明した IoT の Primitive がそれぞれのイニシャルに対応している<br>（S：Sensor、A：Aggregator、E：e-Utility、<br>D：Decision Trigger、C：Communication Channel)<br>それぞれの Primitive において、その Primitive が確認すべきチェック項目には「〇」をつけている |
| ③ | 大項目 | 39 のチェック項目を次の 8 つの大項目のいずれかに分類したもの：<br>(1)ユーザ管理 (2)ソフトウェア管理 (3)セキュリティ管理(4)アクセス制御(5)不正な接続(6)暗号化(7)システム設定(8)通知 |
| ④ | 小項目 | |
| ⑤ | 本項目の目的 | チェック項目に対応するセキュリティ要件 |
| ⑥ | 開発する際に気を付けること | 製品開発者がチェックすべき事項。チェックした結果は回答欄に書き込む。 |
| ⑦ | 利用する際に気を付けること | 製品利用者がチェックすべき事項。チェックした結果は回答欄に書き込む。 |
| ⑧ | 回答欄 | チェック結果を書き込むための回答欄 |
| ⑨ | 回答の補足 | チェック結果が「OK」でなかった場合に、OK でなくとも問題なしと判断した理由を記載するための回答欄 |

### 3.1.2.　チェックリストの使い方

**ステップ 1.**

開発を行う製品が IoT システム全体の中でどの Primitive にあたるかを特定する。
詳細については、「2.1.3. IoT システムの構造と Primitive」を参照

例えば、時計型ウェアラブルデバイスをチェック対象とする場合には、デバイス部分では、心拍数や歩数を図ることができ、Primitive としては Sensor に該当します、また、心拍数や歩数データを集約し、外部サーバと通信を行うため、Aggregator としての Primitive にも該当する。

**ステップ 2.**

用意されている 8 つの大項目（「ユーザ管理」、「ソフトウェア管理」、「セキュリティ管理」、「アクセス制御」、「不正な接続」、「暗号化」、「システム設定」、「通知」）のうち、確認したいセキュリティ機能の種類が定まっている場合、その対象の項目をチェック対象として選択する。
特定の種類の大項目を選ばない場合は、すべての項目について確認する。

例）ネットワークカメラの「アクセス制御」について、必要な機能の確認したい
→大項目「アクセス制御」の No.IV-1 ～ No.IV-4 について確認
ひととおりの項目について、確認したい
→No.I-1 ～ No.VIII-2 について確認

**ステップ 3.**

確認を要するチェックリストの部分の抽出

- ステップ 1 で特定した「Primitive」に○印がついているチェック項目だけを選び出す。○印のないチェック項目は無視する。
- ステップ 2 で選んだ大項目によって絞り込んだ No. 内で前項の「Primitive」に該当した小項目が確認すべきセキュリティの機能になる

**ステップ 4**

「開発する際に気を付けること」の欄に記載されている内容を実装予定、もしくは実装されているかを確認し、結果を「OK」または 「NG」で回答欄に書き込む。「開発する際に気を付けること」の欄に記載されている内容の意味が理解しにくい場合には「IoT セキュリティチェックリスト解説図」を参考として利用してほしい。「NG」と判定された場合には、その機能の実装が現実的に可能なのか、他の機能で代替可能か等を検討し、「回答の補足」に記載する。「回答の補足」の記載は、他の関係者への説明資料やマニュアル作成の際の参考になるだろう。

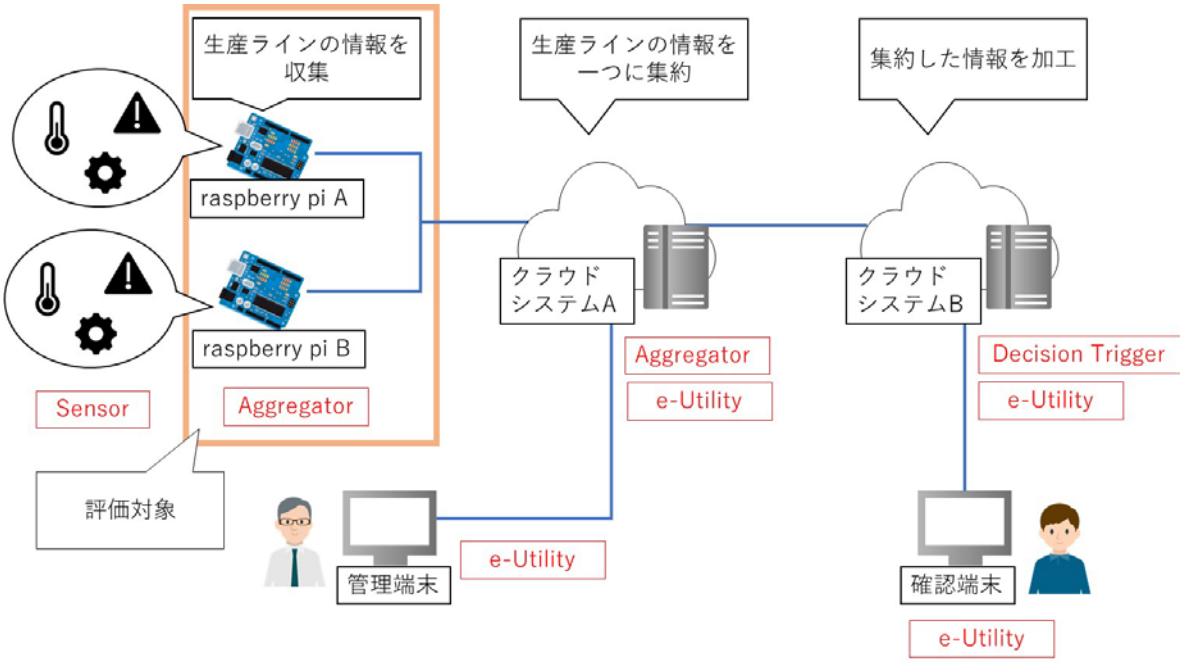
### 3.1.3. 適用事例

本チェックリストを用いた活用事例として、工場における生産情報収集システムのセキュリティについて、本チェックリストを用いて検討をするケースを紹介する。

#### 3.1.3.1. IoT セキュリティチェックリストの適用対象について

本システムは、製品 P の製造を行う製造ラインごとの生産情報を raspberry pi で収集し、それらの生産情報をクラウドシステム A で一つに集約し、その後、クラウドシステム B で情報を加工し、データ表示端末で生産情報を閲覧するものである。

[図 3]は､本システムを要素レベルにブレークダウンした構成図に､「2.1.3. IoT システムの構造と Primitive」を参考に要素ごとの分類を書き加えたものである。




[図 3　工場における生産情報収集システム ]

この生産情報収集システムの場合には、それぞれのクラウドシステムがユーザ用の画面表示機能を備えているため、クラウドシステム A では aggregator と e-Utility、クラウドシステム B では Decision Trigger と e-Utility と言うように複数の Primitive の役割を果たしていると考えられる。

#### 3.1.3.2. 「工場の生産情報収集システム」に対するチェックリストの適用

今回は本システムの raspberry Pi A と B について、チェックリストを利用した評価を行う。
仕様書を確認したところ、[表 2]に示した項目が「NG」と判定される結果となった。

[表 2　チェックリストによる該当項目 ]

| 大項目 | 小項目 |
|---|---|
| **ユーザ管理** | パスワードセキュリティオプション（二要素認証など） |
| | サービスやプロセスを起動するアカウントの権限管理 |
| | サービス連携 |
| **ソフトウェア管理** | ウイルス対策機能 |
| | 不正なデータ処理 |
| | データ転送量 |
| **セキュリティ管理** | セッション管理<br>(Cookie 設定) |
| | セッション管理<br>(URL リライティング) |
| | セッション管理<br>(ログイン時や重要な確定処理の時のセッション ID の払い出し) |
| **アクセス制御** | リモートアクセス用ポートのデフォルトポート |
| **不正な接続** | UPnP |
| **暗号化** | データの暗号化機能 |
| | 暗号化方式 |

上記の項目のうち、本システムにて扱う情報が社内の規定では、極秘情報扱いではないため、次の機能の実装は見送った

- ユーザ管理：パスワードセキュリティオプション（二要素認証など）
- 暗号化：データの暗号化機能

また、残りの項目のうち、実際に実装が可能であり、機能の追加の検討が必要と判断したものは次のとおりである

- ユーザ管理：サービス連携
- ソフトウェア管理：不正なデータ処理
- ソフトウェア管理：データ転送量
- セキュリティ管理：セッション管理(Cookie 設定)
- アクセス制御：リモートアクセス用ポートのデフォルトポート
- 暗号化：暗号化方式

### 3.2. 製品利用者が使う場合のチェックリストの利用方法

#### 3.2.1. 各項目のなまえ

チェックリストは[図 4]のような表の形式をとっている。表の各行が個々のチェック項目に対応している。各チェック項目に対する各行は[表 3]に示した 9 つの欄で構成されている。


| No. | Primitive A | B | C | D | 大項目 | 小項目 | 本項目の目的 | 開発する際に確認する項目 | 利用する際に確認する項目 | 回答欄 | 回答の補足 |
|---|---|---|---|---|---|---|---|---|---|---|---|
| I | 1 | ○ | ○ | ○ | ユーザ管理 | アカウントロックアウトメカニズム | 非正当な試行を不正に操作できないようにする | 連続した処理試行上のログイン失敗や多重ログインなどの挙動を検出したら、アカウントをロックし、ログインが不可になる機能を持たせる | アカウントロックに関する処理機構の内容を確認し、意味で設定したお回はアカウントがロックされることを確認する | | |
| | 2 | | ○ | ○ | | 一定期間利用されていないアカウントの強制失効オプション | 一定期間利用されていないアカウントからのログインをできないようにする | 設定した有効期限を超過したアカウントをロックする機能を持たせる | 有効期限後はアカウントが失効することを確認する | | |
| | 3 | | ○ | ○ | | パスワード強度の担保機能 | ブルートフォース、辞書攻撃などにより不正にログインされないようにする | 複数の文字種の利用や一定文字数以上などの条件を満たしたパスワードの作成できる機能を持たせる | 条件に満たないパスワードの設定ができないことを確認する | | |
| | 4 | | ○ | ○ | | パスワードセキュリティオプション（二要素認証など） | 非正当がシステムにログインすることを回避する | パスワードセキュリティオプションを利用できるようにする（例：二要素認証など） | パスワードセキュリティオプションが利用できることを確認する | | |
| | 5 | | ○ | ○ | | サービスやプロセスを駆動するアカウントの権限管理 | アカウント毎にはサービスやプロセスを動かす権限を設定してインシデント発生時の影響範囲をサービスやプロセスの範囲だけにする | サービスやプロセスの駆動はスーパーユーザを求めない作りにする | サービスやプロセス専用のユーザで動作することを確認する | | |
| | 6 | | ○ | ○ | | 共有ユーザアカウント | 用途に応じて適切な権限を付与できるようにする | アカウント管理機能を持たせる | 共有するアカウントが適切な権限と共有範囲で利用されていることを確認する | | |
| | 7 | | ○ | ○ | | 管理ユーザへの適切な権限付与 | 管理ユーザが必要な権限を使えるようにする | 権限を管理する機能を持たせる | 管理者ユーザが適切な権限を付与されている確認する | | |
| | 8 | | ○ | ○ | | 一般ユーザへの権限付与機能 | ユーザに必要な権限のみを使えるようにする | ユーザに権限を付与できる機能を持たせる | ユーザは権限が付与でき、権限に応じた利用ができることを確認する | | |
| | 9 | | ○ | ○ | | 認可制御機能 | 役割に応じたアクセス権を付与するできるようにする | アカウントの役割に応じたアクセス権を付与する機能を持たせる | 認可されていない機能や機能が利用できないことを確認する | | |
| | 10 | | ○ | ○ | | サービス連携 | ログイン情報が必要以上に他のサービスに渡らないようにする | サービス連携時に他のサービスに渡す情報をユーザに開示する機能を持たせる | 他のサービスに渡した情報が何かを確認する | | |
| II | 1 | | | ○ | ソフトウェア管理 | Webアプリケーションファイアウォール | Webアプリケーションファイアウォールを利用できるようにする | Webアプリケーションファイアウォールを利用できるようにする | Webアプリケーションファイアウォールを利用できることを確認する | | |
| | 2 | | ○ | ○ | | 製品に含まれるファイアウォール機能 | 製品に含まれるファイアウォールの機能を利用し、よりセキュアな状態にする | 製品に含まれるファイアウォール機能を利用できるようにする | 製品に含まれるファイアウォール機能が利用できることを確認する | | |
| | 3 | | ○ | ○ | | ソフトウェアバージョン | 脆弱性やバグ等に対応したバージョンのソフトウエアを利用し、セキュアな状態にする | ソフトウエアのアップデートを行う機能とバージョンを確認できる機能を持たせる | ソフトウエアのアップデートとバージョン確認ができることを確認する | | |
| | 4 | | ○ | ○ | | ウィルス対策機能 | 製品に含まれるウイルス対策機能を利用し、よりセキュアな状態にする | 製品に含まれるウイルス対策機能を利用できるようにする | 製品に含まれるウイルス対策機能が利用できることを確認する | | |
| | 5 | | ○ | ○ | | 不正なデータ処理 | システムが意図しない動作をしないようにする | 受け付けるデータを制限する機能を持たせる | - | | |
| | 6 | | ○ | ○ | | データ転送量 | システムのデータ転送量はDDoS攻撃などを考慮した設計にする | 受け付けるデータ転送量の制限を行うなどの機能を持たせる | 受け付けるデータ転送量を確認する | | |

[図 4 IoT セキュリティチェックリスト ]

[表 3　IoT セキュリティチェックリストの要素 ]

| No. | 項目名 | 説明 |
|---|---|---|
| ① | No. | チェック項目の番号 |
| ② | Primitive | 「2.1.3. IoT システムの構造と Primitive」にて説明した IoT システムの Primitive がそれぞれのイニシャルに対応している<br>( S：Sensor、A：Aggregator、E：e-Utility、<br>D：Decision Trigger、C：Communication Channel)<br>それぞれの Primitive において、その Primitive が確認すべきチェック項目には「〇」をつけている |
| ③ | 大項目 | 39 のチェック項目を次の 8 つの大項目のいずれかに分類したもの：<br>(1)ユーザ管理 (2)ソフトウェア管理 (3)セキュリティ管理(4)アクセス制御(5)不正な接続(6)暗号化(7)システム設定(8)通知 |
| ④ | 小項目 | |
| ⑤ | 本項目の目的 | チェック項目に対応するセキュリティ要件 |
| ⑥ | 開発する際に気を付けること | 製品開発者がチェックすべき事項。チェックした結果は回答欄に書き込む。 |
| ⑦ | 利用する際に気を付けること | 製品利用者がチェックすべき事項。チェックした結果は回答欄に書き込む。 |
| ⑧ | 回答欄 | チェック結果を書き込むための回答欄 |
| ⑨ | 回答の補足 | チェック結果が「OK」でなかった場合に、OK でなくとも問題なしと判断した理由を記載するための回答欄 |

### 3.2.2.　本チェックリストの使い方

**ステップ 1.**

利用する製品が IoT システム全体の中でどの Primitive にあたるかを特定する。
詳細については、「2.1.3. IoT システムの構造と Primitive」を参照

例えば、時計型ウェアラブルデバイスをチェック対象とする場合には、デバイス部分では、心拍数や歩数を図ることができ、Primitive としては Sensor に該当する、また、心拍数や歩数データを集約し、外部サーバと通信を行うため、Aggregator としての Primitive にも該当する。

**ステップ 2.**

用意されている 8 つの大項目（「ユーザ管理」、「ソフトウェア管理」、「セキュリティ管理」、「アクセス制御」、「不正な接続」、「暗号化」、「システム設定」、「通知」）のうち、確認したいセキュリティ機能の種類が定まっている場合、その対象の項目をチェック対象として選択する。
特定の種類の大項目を選ばない場合は、すべての項目について確認する。

例）ネットワークカメラの「アクセス制御」について、必要な機能の確認したい

→大項目「アクセス制御」の No.IV-1 ～ No.IV-4 について確認

ひと通りの項目について、確認したい

→No.I-1 ～ No.VIII-2 について確認

**ステップ 3.**

確認を要するチェックリストの部分の抽出

- ステップ 1 で特定した「Primitive」に〇印がついているチェック項目だけを選び出す。

〇印のないチェック項目は無視する。

- ステップ 2 で選んだ大項目によって絞り込んだ No. 内で前項の「Primitive」に該当した小項目が確認すべきセキュリティの機能になる

**ステップ 4.**

評価対象が「利用する際に気を付けること」に記載されている内容を満たしているかどうかを確認する。

- 「利用する際に気を付けること」に記載の内容が製品に搭載されているか確認
- 項目の内容については、IoT セキュリティチェックリストに添付の「IoT セキュリティチェックリスト解説図」を参考に確認する

該当する場合には、「回答欄」にチェックし、該当しない場合には、その理由について「回答の補足」に記載を行う。

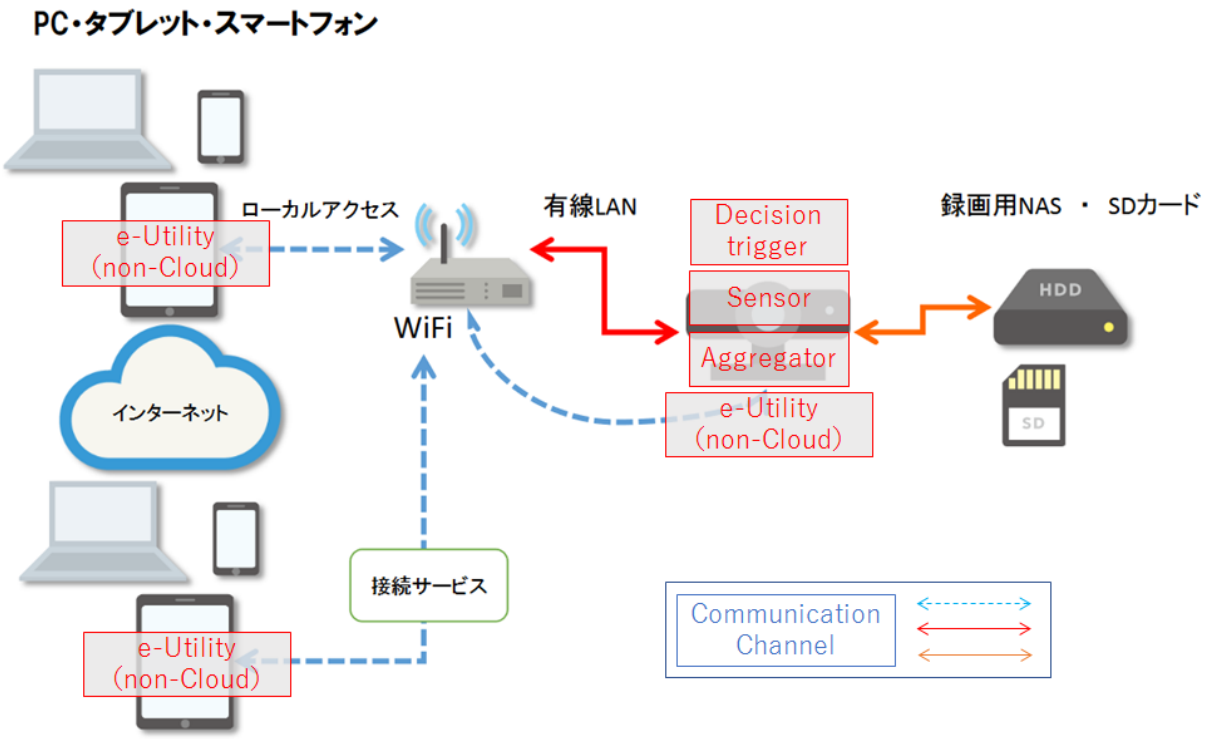
- チェック項目にチェックがつかなかった項目について、その機能は製品にとって開発する際に実装が現実的に可能なのか、他の機能にて補完可能か等、検討し、「回答の補足」に記載を行い、他者への説明資料やマニュアル作成の際の参考資料に活用する

### 3.2.3. 活用事例

本チェックリストを用いた活用事例として、防犯の目的で遠隔地より自宅を監視するために、市販のネットワークカメラの導入を考える利用者が、導入製品に必要なセキュリティ対策を検討する際に評価を行ったケースを紹介する。

#### 3.2.3.1. IoT セキュリティチェックリストの適用対象について

今回の評価にて分類したネットワークカメラの機能ごとの構成を以下の図に示す。
なお、[図 5]は JNSA が発行した「コンシューマ向け IoT セキュリティガイド」の Web カメラの例を参照している。




[図 5　ネットワークカメラにおける Primitive 別分類]

参考：日本ネットワークセキュリティ協会（JNSA）「コンシューマ向け IoT セキュリティガイド」

例に挙げたネットワークカメラの構成では、カメラ自体が多くの機能を備えていることから、複数の Primitive を割り当てることができると考えている。

- Web カメラ (Sensor, Aggreator, eUtility, Decision Trigger)
- スマートフォン、PC (eUtility)
- Wifi, 内部バス (Communication Channel)

### 3.2.3.2. 「ネットワークカメラ」に対するチェックリストの適用

今回の例ではネットワークカメラの e-Utility 部分に対してチェックリストを利用した評価を行った。[表 4]は、導入を検討しているネットワークカメラのユーザマニュアルを参照し、チェックリストに挙げられている機能の搭載の有無について確認を行い、その結果、搭載されていなかった項目を挙げているものである。

[表 4　チェックリストによる該当項目 ]

| 大項目 | 小項目 |
|---|---|
| **ユーザ管理** | 有効期限切れパスワードへの強制失効オプション |
| | パスワード強度の担保機能 |
| | パスワードセキュリティオプション（二要素認証など） |
| | サービスやプロセスを起動するアカウントの権限管理 |
| **ソフトウェア管理** | 製品に含まれるファイアウォール機能 |
| | ウイルス対策機能 |
| **アクセス制御** | 管理されていない物理手段によるアクセス |
| | リモートアクセス用ポートのデフォルトポート |
| | 無線通信におけるセキュリティ(WPS) |
| **不正な接続** | ネットワークポートの制限 |
| | UPnP |

上記の結果を踏まえて、評価を行ったネットワークカメラの導入の際に併せて、検討を行いたい項目について、3 つ挙げることにした。

(1) 認証機能の強化について

ネットワークカメラ上の認証機能の設定は多くの製品で不十分なこと事が多い。例えば、出荷時の認証パスワードがすべての機器で同じ安易なものが設定されており、そのパスワードがインターネット上で公開されている製品も存在している。開発者はすべての機器に同一のパスワードが設定されてしまう点についても考慮する必要もあるが、機器に設定できるパスワードを強固なものしか設定できないような仕様を検討する必要がある。また、二要素認証等の実装による認証の強化も検討したい。また、利用者も同様にパスワードを強固なものに設定できる製品や、二要素認証等のオプションを選択できる製品を選択し、適切に設定していく必要がある。

(2) 外部からのアクセスの制限

ネットワークカメラは、利用者が意図せず外部からアクセス可能な状態になっていることがある。攻撃者はそういった機器のリモートアクセス用のデフォルトポートを狙い、マルウエア感染を行うことがあるため、利用者は外部からのアクセスの制御やリモートアクセス用のポートを変更することを検討する。また、UPnP（ユニバーサルプラグアンドプレイ）などの機能により NAT 環境下でもインターネットから到達可能な場合があるため、注意が必要である。開発者は、外部からのアクセスの制御機能やリモートアクセス用のポートを変更機能、UPnP の無効を行えるような仕様を検討する必要がある。

(3) 製品に含まれる機能の活用

利用可能ならばファイアウォール機能やウイルス策機能も対策として検討する必要がある。製品のスペックによっては e-Utility での実装が難しい場合もあるが、そういった場合にも、例えば、e-Utility 以外の場所での実装も検討を考える。また、攻撃者の動向として、既知のセキュリティ上の問題を執拗に攻撃対象としてくると思われるため、開発者は脆弱性などが公開された際に修正を行うためのファームウエアの更新機能を実装し利用者も適宜、確実にアップデートを行う必要がある。

## 4. 本チェックリストと他ガイド等との関係

本チェックリストの小項目は、IoT に関するセキュリティ評価資料以外に IT 向けのセキュリティ評価資料を参考に作成されている。IoT システムは既存 IT の技術を利用しつつ構成されているケースが考えられ、例えば、製品に含まれる e-Utility などに実装されるインタフェースが、Web アプリケーションや、API によるアクセスなど、通信プロトコルが Web とよく似た実装となっているといったことがあり、IT 向けのセキュリティ評価が参考になると考えるためである。

チェックリストでは、数多くある IoT / IT 向けのセキュリティ評価資料の中でも、特に具体的なセキュリティ評価の方法の記載されている次の文章を主な参考とした

IoT Security Guidance
OWASP
https://www.owasp.org/index.php/IoT_Security_Guidance

The Penetration Testing Execution Standard
Penetration Testing Execution Standard Group
http://www.pentest-standard.org/index.php/Main_Page

上記の 2 つの資料から、共通する項目を基準項目として検討を行った。これらの資料は、IT および IoT のセキュリティを考える上で、特に基本的な項目がまとめられており、項目の中にはそれぞれの資料の中で共通しているものが多く存在する。そのため、これら共通項目は注目度が高く優先して実施することが望まれるのではないかと考える。

しかし、本文書では、これらの項目はすべてが満たされなければならない要求・要件ではないと考えている。すなわち、注目度が高いことから、優先的に対策を講じるなどの議論や検討が必要とされている推奨項目であると考えている。

なぜならば、製品やシステムによっては、その他に求められる規格などの要件や、項目に重み付けがあるなど考えられるためで、チェックリストを適用する際には、それらの他の要件とも併せて検討することが望ましい。

また、チェックリストでは IoT システムのセキュリティに対する基本的な検討項目をまとめたが、問題によっては、セキュリティに対する要件による解決ではなく、セーフティに対する要件によって解決を図ることが優先できる場合も考えられる。本文書では、セキュリティとセーフティを併せて検討することが適切であるとの立場から、どちらを優先するということでなく、並行して検討し、最終的に製品やシステムに対して適切に対策が施されている状況を作り、確認することを推奨する。

## 謝辞

本文書の検討およびチェックリストの作成にあたり、JNSA IoT セキュリティ WG リーダ　松岡 正人氏、公立大学法人長崎県立大学　加藤 雅彦 教授との協力を得て検討を行った。また、論点について、JNSA IoT セキュリティ WG メンバーをはじめ、多数の協力者のアドバイスを受けて検討した。本文書に関わっていただいたすべての方々に対して、改めて御礼申し上げる。

## 参考文献


・IoT Security Guidance
OWASP
https://www.owasp.org/index.php/IoT_Security_Guidance

・The Penetration Testing Execution Standard
Penetration Testing Execution Standard Group
http://www.pentest-standard.org/index.php/Main_Page

・NIST Special Publication 800-183 Networks of ‘Things
NIST
https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-183.pdf

・NIST SP 800-160 Systems Security Engineering: Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems
NIST
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-160.pdf

・コンシューマ向け IoT セキュリティガイド
日本ネットワークセキュリティ協会(JNSA)
https://www.jnsa.org/result/iot/

・Overview of the Internet of things
International Telecommunication Union (ITU)
https://www.itu.int/ITU-T/recommendations/rec.aspx?rec=y.2060

・IoT セキュリティガイドライン[ver 1.0]
経済産業省／総務省
http://www.meti.go.jp/press/2016/07/20160705002/20160705002.html

・つながる世界の開発指針[第 2 版]
独立行政法人情報処理推進機構（IPA）
https://www.ipa.go.jp/sec/reports/20160324.html

・The STRIDE Threat Model
Microsoft
https://msdn.microsoft.com/en-us/library/ee823878(v=cs.20).aspx

・The WASC Threat Classification v2.0
WASC Projects
http://projects.webappsec.org/w/page/13246978/Threat%20Classification

・OWASP Testing Guide v4 Table of Contents
OWASP
https://www.owasp.org/index.php/OWASP_Testing_Guide_v4_Table_of_Cont

・引用・転載・再配布等の際は、広報（pr@jpcert.or.jp）にご連絡ください。
・本文書内に記載されている情報により生じるいかなる損失または損害に対して、JPCERT/CC は責任を負うものではありません。
・本チェックリストは、すべての設問項目を達成することで、何らかの基準や国際標準を保証したり、IoT セキュリティ対策が万全であることを意味するものではございません。予めご了承ください。